Acronis

acronis.com

サイバープロテクション

24.03

ユーザー ガイド

リビジョン: 2024/04/10

目次

Cyber Protectionの使用を開始する

アカウントのアクティブ化

管理者によってアカウントが作成されると、エンドユーザーの電子メールアドレスに承認メールが送信されます。承認メールには次の情報が含まれます。

- **ログイン。**これは、ログインに使用するユーザー名です。ログイン情報は、アカウントのアクティベーションページにも表示されます。
- **[アカウントを有効化]** ボタンボタンをクリックして、アカウントのパスワードを設定します。パスワードは9文字以上にしてください。パスワードの詳細情報については、"パスワード要件"（19ページ）を参照してください。

管理者が二要素認証を有効にしている場合、自分のアカウントに二要素認証を設定するように促されます。詳細については、"二要素認証"（19ページ）を参照してください。

パスワード要件

ユーザーアカウントのパスワードは9文字以上にする必要がありますまた、パスワードの複雑さもチェックされ、以下のいずれかのカテゴリに分類されます。

- 弱
- 中
- 強

9文字以上であっても、脆弱性のあるパスワードを保存することはできません。ユーザー名、ログイン名、ユーザーのEメールアドレス、またはユーザーアカウントが属するテナント名が繰り返し出現するパスワードは、いずれの場合でも脆弱であると見なされます。頻繁に使用されるパスワードも脆弱であると見なされます。

パスワードの強度を高めるには、文字数を増やします。数字、大文字、小文字、記号など、さまざまな種類の文字を使用することは必須ではありませんが、これらを組み合わせることで、より強力で短いパスワードを作成できます。

二要素認証

二要素認証（2FA）はアカウントへの不正アクセスに対して追加の保護を提供します。二要素認証がセットアップされると、Cyber Protectコンソールへのログインにパスワード（第1要素）とワンタイムコード（第2要素）の入力が必要になります。ワンタイムコードは、ユーザーの携帯電話またはユーザーに属する他のデバイスにインストールが必要な特別なアプリケーションによって生成されます。ログイン名とパスワードが別のユーザーに知られたとしても、第2要素デバイスにアクセスできなければログインすることはできません。

ユーザーのアカウントに二要素認証を設定するには

管理者が組織で二要素認証を有効にしている場合は、アカウントに二要素認証を設定する必要があります。Cyber Protectコンソールにログインしている間に管理者が二要素認証を有効にした場合、現在のセッションの有効期限が切れたタイミングで構成する必要があります。

前提条件

- 管理者により、組織用の二要素認証が有効化されています。

ユーザーのアカウントに二要素認証を設定するには

1. モバイルデバイスに認証アプリをインストールします。
   認証アプリの例:
   - Twilio Authy
   - Microsoft Authenticator
   - Google Authenticator
2. 認証アプリを使用してQRコードをスキャンし、認証アプリに表示される6桁のコードを **[二要素認証の設定]** ウィンドウに入力します。
3. **[次へ]** をクリックします。
   二要素認証デバイスを紛失した場合や認証アプリをアンインストールした場合のアカウントへのアクセスを復元する手順が表示されます。
4. PDFファイルを保存または印刷します。

   注意
   PDFファイルを安全な場所に保存するか、印刷して参照できるようにしてください。これがアクセスを復元する最も有効な方法です。

5. Cyber Protectコンソールのログインページへ戻り、生成されたコードを入力します。
   ワンタイムコードの有効期限は30秒間です。30秒以上待つ場合は、次に生成されたコードを使用します。

次回のログイン時に、**[このブラウザを信頼する...]** チェックボックスを選択できます。この場合、このマシンでこのブラウザを使用して次回以降ログインする際には、コードは必要ありません。

注意
このチェックボックスはオフのままにしておくことをお勧めします。そうでない場合、アカウントの二要素認証へのアクセスが失われます。

新しいデバイスで二要素認証（2FA）を復元するには

以前設定したモバイル認証アプリにアクセスできる場合

1. 新しいデバイスに認証アプリをインストールします。
2. デバイスで二要素認証を構成した際に保存したPDFファイルを使用します。このファイルには、認証アプリをアクロニスアカウントに再度リンクする際に認証アプリに入力する必要がある、32桁のコードが含まれています。

重要
コードが動作しない場合は、認証アプリの時刻がデバイスと同期されていることを確認してください。

セットアップ中にPDFファイルを保存していなかった場合:

a. **[二要素認証をリセット]** をクリックして、モバイル認証アプリに表示されているワンタイムパスワードを入力します。
b. 画面の指示に従います。

以前設定したモバイル認証アプリにアクセスできなかった場合

1. 新しいモバイルデバイスを用意します。
2. 保存されたPDFファイルを使用して、新しいデバイスをリンクします（デフォルトのファイル名は `cyberprotect-2fa-backupcode.pdf`）。
3. バックアップからアカウントへのアクセス権を復元します。バックアップがモバイルアプリでサポートされていることを確認してください。
4. アプリでサポートされている場合は、別のモバイルデバイスから同じアカウントでアプリを開きます。

プライバシー設定

プライバシー設定は、個人情報の収集、使用、開示についての意思を示すのに役立ちます。

ユーザーがCyber Protect Cloudを使用している国やサービスを提供しているCyber Protect Cloudデータセンターによっては、Cyber Protect Cloudの初回起動時に、Cyber Protect CloudでGoogle Analyticsを使用することに同意するかどうかを確認するよう求められる場合があります。

Google Analyticsは、匿名化されたデータを収集することで、ユーザーの行動に対する理解を深め、Cyber Protect Cloudでのユーザーエクスペリエンスを向上させるサポートを提供します。

Cyber Protect Cloudの初回起動時に、Google Analyticsを有効化または拒否した場合、後からいつでもその設定を変更できます。

Google Analyticsを有効または無効にするには

1. Cyber Protectコンソールで、**[アカウントの管理]** をクリックします。
2. 右上にあるアカウントアイコンをクリックします。
3. **[現在のプライバシー設定]** を選択します。**[現在のプライバシー設定]** ウィンドウが表示されます。
4. **Google Analyticsデータ収集**セクションで、次のボタンのいずれかをクリックします。
   - **[オン]**: Google Analyticsを有効化
   - **[オフ]**: Google Analyticsを無効化

Cookieを削除する方法セクションでは、ブラウザ内でクッキーを制御および管理する方法が説明されています。

注意
Google Analyticsセクションが表示されない場合、お住まいの国ではGoogle Analyticsが使用されていないことを意味します。

試用期間中に最初に表示される **[製品内オンボーディングとインタラクティブ型のヘルプ]** セクションでは、将来的にプログラムの改善や新機能に関する情報の受信を停止または継続することができます。この機能はデフォルトで有効になっていますが、トグルを**オフ**に切り替えて無効にできます。

Cyber Protectionサービスへのアクセス

アカウントを有効化した後、Cyber Protectコンソールまたは管理ポータルからログインして、Cyber Protectionサービスにアクセスできます。

Cyber Protectコンソールにログインするには

1. Cyber Protectionサービスのログインページに移動します。
2. ログイン情報を入力して **[次へ]** をクリックします。
3. パスワード入力してから **[次へ]** をクリックします。
4. （複数のCyber Protect Cloudサービスを使用する場合）**[サイバープロテクション]** をクリックします。
   Cyber Protectionサービスへのアクセス権を持つユーザーのみが、Cyber Protectコンソールに直接ログインできます。

   サイバープロテクション以外のサービスにアクセスできる場合、右上にある  アイコンを使用してサービスを切り替えることができます。管理者もこのアイコンを使用して、管理ポータルに切り替えることができます。

Cyber Protectコンソールのタイムアウト時間は、アクティブセッションに対しては24時間、アイドルセッションに対しては1時間です。

右上のアカウントアイコンをクリックして、Webインターフェースの言語を変更できます。

管理ポータル経由でCyber Protectコンソールにアクセスするには

1. 管理ポータルで **[監視]** > **[使用状況]** へ進みます。
2. **[Cyber Protect]** の下で **[保護]** を選択してから、**[サービスを管理]** をクリックします。
   または、**[クライアント]** の下でカスタマーを選択してから、**[サービスの管理]** をクリックします。

これにより、Cyber Protectコンソールにリダイレクトされます。

重要
カスタマーの管理モードが**セルフサービス**の場合、代わりにサービスを管理することはできません。カスタマーモードを**サービスプロバイダーによる管理対象**に変更し、サービスを管理できるのはカスタマー管理者のみです。

パスワードをリセットする手順

1. Cyber Protectionサービスのログインページに移動します。
2. ログイン情報を入力して **[次へ]** をクリックします。
3. **[パスワードをお忘れですか？]** をクリックします。
4. **[送信する]** をクリックしてその先の手順を知らせてもらうようリクエストします。
5. 受信したEメールの手順に従います。
6. 新しいパスワードを設定します。

ソフトウェア要件

推奨 Web ブラウザ

Cyber ProtectコンソールはTLS 1.2プロトコルを使用し、以下のWebブラウザをサポートしています。

- Google Chrome 29以降
- Mozilla Firefox 23以降
- Opera 16以降
- Microsoft Edge 25以降
- macOSおよびiOSオペレーティングシステムで稼働するSafari 8以降

他のWebブラウザ（他のオペレーティングシステムで稼働するSafariブラウザなど）では、ユーザーインターフェースが正しく表示されないか、一部の機能が使用できない場合があります。

サポートされるオペレーティング システムと環境

Windowsエージェント

このエージェントには、ウイルス対策およびマルウェア対策保護とURLフィルタリングのコンポーネントが含まれています。 オペレーティングシステムでサポートされている機能の詳細については、「"オペレーティングシステムでサポートされる保護機能"（43ページ）」を参照してください。

- Windows XP Professional SP1（x64）、SP2（x64）、SP3（x86）
- Windows Server 2003 SP1/2003 R2以降 – StandardおよびEnterpriseエディション (x86、x64)
- Windows Small Business Server 2003/2003 R2
- Windows Server 2008、Windows Server 2008 SP2* - Standard、Enterprise、Datacenter、Webの各エディション（x86、x64）
- Windows Small Business Server 2008, Windows Small Business Server 2008 SP2*
- Windows 7: すべてのエディション

注意

Windows 7でCyber Protectionを使用するには、プロテクションエージェントをインストールする前に、Microsoftが提供する次のアップデートプログラムをインストールする必要があります。

- Windows 7拡張セキュリティアップデートプログラム（ESU）
- KB4474419
- KB4490628

必要なアップデートの詳細については、このナレッジベースの記事を参照してください。

- Windows Server 2008 R2* - Standard、Enterprise、Datacenter、Foundation、Web の各エディション
- Windows Home Server 2011*
- Windows MultiPoint Server 2010*/2011*/2012
- Windows Small Business Server 2011* - すべてのエディション
- Windows 8/8.1 – Windows RTエディションを除くすべてのエディション（x86、x64）
- Windows Server 2012/2012 R2: すべてのエディション
- Windows Storage Server 2003/2008/2008 R2/2012/2012 R2/2016
- Windows 10 - Home、Pro、Education、Enterprise、IoT Enterprise、LTSC（旧称: LTSB）の各エディション
- Windows Server 2016: Nano Server以外のすべてのインストールオプション
- Windows Server 2019: Nano Server以外のすべてのインストールオプション
- Windows 11 - すべてのエディション
- Windows Server 2022: Nano Server以外のすべてのインストールオプション

注意

このバージョンのWindowsでCyber Protectionを使用するには、プロテクションエージェントのインストールに先立ち、Microsoft KB4474419で提供されている、SHA2コード署名サポートアップデートをインストールする必要があります。

SHA2コード署名サポートアップデートに関する問題については、こちらのナレッジベースの記事を参照してください。

SQLエージェント、Active Directoryエージェント、Exchangeエージェント（データベースバックアップとアプリケーション認識型バックアップ用）

各エージェントは上記の一覧で示すオペレーティングシステムとサポートされているバージョンのアプリケーションを実行するコンピュータにインストールできます。

データ漏洩防止エージェント

デバイス制御

- Microsoft Windows 7 Service Pack 1以降
- Windows Server 2008 R2以降

- macOS 10.15 (Catalina)
- macOS 11.2.3（Big Sur）
- macOS 12 (Monterey)
- macOS 13 (Ventura)

注意
データ損失防止macOSエージェントは、x64プロセッサのみをサポートしています。ARMベースのAppleシリコンプロセッサはサポートされていません。

データ漏洩防止

- Microsoft Windows 7 Service Pack 1以降
- Windows Server 2008 R2以降

注意
データ漏洩防止エージェントはMacエージェントの一部であるため、サポートされていないmacOSシステムにインストールされる可能性があります。この場合、Cyber Protectコンソールでは、コンピューターにデータ漏洩防止エージェントがインストールされている状態が表示されますが、デバイス制御およびデータ損失防止機能は動作しません。デバイス制御機能は、データ漏洩防止エージェントをサポートしているmacOSシステムでのみ動作します。

Advanced Data Loss Preventionエージェント

- Microsoft Windows 7 Service Pack 1以降
- Windows Server 2008 R2以降

File Sync & Shareエージェント

サポート対象のオペレーティングシステムについては、『Cyber Files Cloudユーザーガイド』を参照してください。

Exchangeエージェント（メールボックスバックアップ用）

- Windows Server 2008: Standard、Enterprise、Datacenter、Webの各エディション（x86、x64）
- Windows Small Business Server 2008
- Windows 7: すべてのエディション
- Windows Server 2008 R2: Standard、Enterprise、Datacenter、Foundation、Web の各エディション
- Windows MultiPoint Server 2010/2011/2012
- Windows Small Business Server 2011: すべてのエディション
- Windows 8/8.1 – Windows RTエディションを除くすべてのエディション（x86、x64）
- Windows Server 2012/2012 R2: すべてのエディション
- Windows Storage Server 2008/2008 R2/2012/2012 R2
- Windows 10: Home、Pro、Education、Enterpriseの各エディション

- Windows Server 2016: Nano Server以外のすべてのインストールオプション
- Windows Server 2019: Nano Server以外のすべてのインストールオプション
- Windows 11 - すべてのエディション
- Windows Server 2022: Nano Server以外のすべてのインストールオプション

Microsoft 365エージェント

- Windows Server 2008 - Standard、Enterprise、Datacenter、Foundation、Webの各エディション（x64のみ）
- Windows Small Business Server 2008
- Windows Server 2008 R2: Standard、Enterprise、Datacenter、Foundation、Web の各エディション
- Windows Home Server 2011
- Windows Small Business Server 2011: すべてのエディション
- Windows 8/8.1: Windows RTエディションを除くすべてのエディション（x64のみ）
- Windows Server 2012/2012 R2: すべてのエディション
- Windows Storage Server 2008/2008 R2/2012/2012 R2/2016（x64のみ）
- Windows 10: Home、Pro、Education、Enterpriseの各エディション（x64のみ）
- Windows Server 2016 – Nano Server以外のすべてのインストールオプション（x64のみ）
- Windows Server 2019 – Nano Server 以外のすべてのインストールオプション（x64 のみ）
- Windows 11 - すべてのエディション
- Windows Server 2022: Nano Server以外のすべてのインストールオプション

Oracle エージェント

- Windows Server 2008R2 – Standard、Enterprise、Datacenter、Webの各エディション（x86、x64）
- Windows Server 2012R2 – Standard、Enterprise、Datacenter、Webの各エディション（x86、x64）
- Linux - Linuxエージェントによってサポートされているすべてのカーネルとディストリビューション（下記参照）

MySQL/MariaDBエージェント

- Linux - Linuxエージェントによってサポートされているすべてのカーネルとディストリビューション（下記参照）

Linuxエージェント

このエージェントには、ウイルス対策およびマルウェア対策保護とURLフィルタリングのコンポーネントが含まれています。 オペレーティングシステムでサポートされている機能の詳細については、「"オペレーティングシステムでサポートされる保護機能"（43ページ）」を参照してください。

次のLinuxディストリビューションとカーネルのバージョンは明示的なテストの対象となっています。ただし、Linuxディストリビューションまたはカーネルのバージョンが以下のリストに掲載されていない場合でも、Linuxオペレーティングシステムの仕様により、必要なすべてのシナリオにおいて正しく動作する可能性があります。

Cyber Protectionの使用中に、特定のLinuxディストリビューションとカーネルのバージョンの組み合わせで問題が発生した場合は、さらなる調査のために、サポートチームに連絡してください。

2.6.9から5.19のカーネルとglibc 2.3.4以降を搭載したLinux（以下のx86とx86_64のディストリビューションが含まれます）。

- Red Hat Enterprise Linux 4.x, 5.x, 6.x, 7.x, 8.x*, 9.0*, 9.1*, 9.2*, 9.3*
- Ubuntu 9.10, 10.04, 10.10, 11.04, 11.10, 12.04, 12.10, 13.04, 13.10, 14.04, 14.10, 15.04, 15.10, 16.04, 16.10, 17.04, 17.10, 18.04, 18.10, 19.04, 19.10, 20.04, 20.10, 21.04, 21.10, 22.04, 22.10, 23.04
- Fedora 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 37, 38
- SUSE Linux Enterprise Server 10, 11, 12, 15

重要
Btrfsによる構成は、SUSE Linux Enterprise Server 12およびSUSE Linux Enterprise Server 15ではサポートされていません。

- Debian 4.x, 5.x, 6.x, 7.0, 7.2, 7.4, 7.5, 7.6, 7.7, 8.0, 8.1, 8.2, 8.3, 8.4, 8.5, 8.6, 8.7, 8.8, 8.11, 9.0, 9.1, 9.2, 9.3, 9.4, 9.5, 9.6, 9.7, 9.8, 10, 11
- CentOS 5.x, 6.x, 7.x, 8.x*
- CentOS Stream 8*, 9*
- Oracle Linux 5.x、6.x、7.x、8.x*、9.0*、9.1*、9.2* - Unbreakable Enterprise KernelとRed Hat Compatible Kernelの両方

注意
セキュアブートが有効なOracle Linux 8.6以降にプロテクションエージェントをインストールする場合、カーネルモジュールに手動で署名する必要があります。カーネルモジュールに署名する方法の詳細については、こちらのナレッジベースの記事を参照してください。

- CloudLinux 5.x, 6.x, 7.x, 8.x*
- ClearOS 5.x, 6.x, 7.x
- AlmaLinux 8.x*,9.0*, 9.1*, 9.2*
- Rocky Linux 8.x*, 9.0*, 9.1*, 9.2*, 9.3*
- ALT Linux 7.0

*バージョン8.4以降、4.18から5.19までのカーネルでのみサポートされています。

Macエージェント

このエージェントには、ウイルス対策およびマルウェア対策保護とURLフィルタリングのコンポーネントが含まれています。 オペレーティングシステムでサポートされている機能の詳細については、「"オペレーティングシステムでサポートされる保護機能"（43ページ）」を参照してください。

x64およびARMアーキテクチャ（Apple M1およびM2などのAppleシリコンプロセッサで採用）の両方がサポートされています。

注意
Appleシリコンプロセッサを搭載するMacに、IntelベースMacのディスクレベルバックアップをリカバリすることはできません。ファイルおよびフォルダをリカバリできます。

- macOS High Sierra 10.13
- macOS Mojave 10.14
- macOS Catalina 10.15
- macOS Big Sur 11
- macOS Monterey 12
- macOS Ventura 13
- macOS Sonoma 14

重要
バージョンC23.07以降のCyber Protect Cloudでは、次のオペレーティングシステムがサポートされません:OS X Yosemite 10.10、OS X El Capitan 10.11、macOS Sierra 10.12。

互換性を確保し、Cyber Protect Cloudの全機能を使用できるようにするために、オペレーティングシステムをサポート対象のバージョンにアップグレードすることを強くお勧めします。

VMwareエージェント（仮想アプライアンス）

このエージェントは、ESXi ホストで実行する仮想アプライアンスとして提供されます。

VMware ESXi 4.1, 5.0, 5.1, 5.5, 6.0, 6.5, 6.7, 7.0, 8.0

エージェント for VMware（Windows）

このエージェントは、上記のWindowsエージェントのオペレーティングシステムで実行するWindowsアプリケーションとして提供されます。ただし次の例外があります。

- 32ビットオペレーティングシステムはサポートされません。
- Windows XP、Windows Server 2003/2003 R2、Windows Small Business Server 2003/2003 R2はサポートされません。

Hyper-Vエージェント

- Windows Server 2008（x64のみ）with Hyper-Vのロール: Server Coreインストールモードを含む
- Windows Server 2008 R2 with Hyper-Vのロール: Server Coreインストールモードを含む
- Microsoft Hyper-V Server 2008/2008 R2
- Windows Server 2012/2012 R2 with Hyper-Vのロール: Server Coreインストールモードを含む
- Microsoft Hyper-V Server 2012/2012 R2
- Windows Server 8、8.1（x64のみ）（Hyper-V使用）
- Windows 10: Pro、Education、Enterpriseエディション（Hyper-V使用）

- Windows Server 2016 with Hyper-Vのロール: Nano Server以外のすべてのインストールオプション
- Microsoft Hyper-V Server 2016
- Windows Server 2019 with Hyper-Vのロール: Nano Server以外のすべてのインストールオプション
- Microsoft Hyper-V Server 2019
- Windows Server 2022: Nano Server以外のすべてのインストールオプション

Virtuozzoエージェント

- Virtuozzo 6.0.10, 6.0.11, 6.0.12, 7.0.13, 7.0.14
- Virtuozzo Hybrid Server 7.5

Virtuozzo Hybrid Infrastructureエージェント

Virtuozzo Hybrid Infrastructure 3.5, 4.0, 4.5, 4.6, 4.7, 5.0, 5.1, 5.2, 5.3, 5.4, 6.0

Scale Computing HC3エージェント

Scale Computing Hypercore 8.8, 8.9, 9.0, 9.1, 9.2, 9.3

oVirtエージェント

Red Hat Virtualization 4.2, 4.3, 4.4, 4.5

Synologyエージェント

DiskStation Manager 6.2.x、7.x

Synologyエージェントでは、x86_64プロセッサを搭載したNASデバイスのみがサポートされています。ARMプロセッサはサポートされていません。

Cyber Protectモニタ

- Windows 7以降
- Windows Server 2008 R2以降
- Macエージェントがサポートするすべてのバージョン

サポートされる Microsoft SQL Server のバージョン

- Microsoft SQL Server 2022
- Microsoft SQL Server 2019
- Microsoft SQL Server 2017
- Microsoft SQL Server 2016
- Microsoft SQL Server 2014
- Microsoft SQL Server 2012
- Microsoft SQL Server 2008 R2

- Microsoft SQL Server 2008
- Microsoft SQL Server 2005

上述のSQLサーバーのバージョンでは、SQL Server Expressエディションもサポートされています。

注意
Microsoft SQLバックアップは、NFTS、REFS、およびFAT32ファイルシステム上で実行されているデータベースに対してのみサポートされています。ExFatはサポートされていません。

サポートされるMicrosoft Exchange Serverのバージョン

- Microsoft Exchange Server 2019: すべてのエディション。
- Microsoft Exchange Server 2016: すべてのエディション。
- Microsoft Exchange Server 2013: すべてのエディション、累積的な更新プログラム1（CU1）以降。
- Microsoft Exchange Server 2010 - すべてのエディション、すべてのサービスパック。メールボックスのバックアップとデータベースバックアップからの粒度復元は、Service Pack 1（SP1）以降でサポートされています。
- Microsoft Exchange Server 2007 - すべてのエディション、すべてのサービスパック。メールボックスのバックアップとデータベースバックアップからの粒度復元はサポートされていません。

サポートされる Microsoft SharePoint のバージョン

Cyber Protectionは、Microsoft SharePointの以下のバージョンをサポートします。

- Microsoft SharePoint 2013
- Microsoft SharePoint Server 2010 SP1
- Microsoft SharePoint Foundation 2010 SP1
- Microsoft Office SharePoint Server 2007 SP2*
- Microsoft Windows SharePoint Services 3.0 SP2*

* これらのバージョンと一緒に SharePoint Explorer を使用するには、データベースを接続する SharePoint 復元ファームが必要です。

データの展開元のバックアップとデータベースは、SharePoint Explorer がインストールされている場所と同じ SharePoint バージョンのものである必要があります。

サポート対象の Oracle データベースのバージョン

- Oracle データベース バージョン 11g（すべてのエディション）
- Oracleデータベースバージョン 12c（すべてのエディション）
- Oracleデータベースバージョン19c（すべてのエディション）
- Oracleデータベースバージョン21c（すべてのエディション）

単一インスタンスの設定のみがサポートされます。

サポート対象の SAP HANA バージョン

物理マシンまたは VMware ESXi 仮想マシン上で実行される RHEL 7.6 にインストールされた HANA 2.0 SPS 03。

SAP HANA は、ストレージスナップショットを使用したマルチテナントデータベースコンテナの復元をサポートしていないため、このソリューションは、テナントデータベースが 1 つだけの SAP HANA コンテナをサポートします。

サポートされるMySQLのバージョン

- 5.5.x - Community Server、Enterprise、Standard、およびClassicの各エディション
- 5.6.x - Community Server、Enterprise、Standard、およびClassicの各エディション
- 5.7.x - Community Server、Enterprise、Standard、およびClassicの各エディション
- 8.0.x - Community Server、Enterprise、Standard、およびClassicの各エディション

サポートされるMariaDBのバージョン

- 10.0.x
- 10.1.x
- 10.2.x
- 10.3.x
- 10.4.x
- 10.5.x
- 10.6.x
- 10.7.x

サポートされる仮想環境プラットフォーム

次の表では、各種仮想環境プラットフォームがどのようにサポートされているのかについてまとめています。

エージェントベースとエージェントレスのバックアップの違いについては、"エージェントベースのバックアップとエージェントレスバックアップ"（65ページ）を参照してください。

注意
下表に記載されていない仮想化プラットフォームまたはバージョンを使用している場合でも、**エージェントベースのバックアップ（ゲストOS内部からのバックアップ）**方法は、必要なすべてのシナリオにおいて正常に動作する可能性があります。エージェントベースのバックアップで問題が発生した場合は、さらなる調査のために、サポートチームまでお問い合わせください。

VMware

プラットフォーム	エージェントレスバックアップ（ハイパーバイザーレベルのバックアップ）	エージェントベースのバックアップ（ゲストOS内のバックアップ）
VMware vSphereバージョン:4.1、5.0、5.1、5.5、6.0、6.5、6.7、7.0、8.0 **VMware vSphere のエディション:** VMware vSphere Essentials* VMware vSphere Essentials Plus* VMware vSphere Standard* VMware vSphere Advanced VMware vSphere Enterprise VMware vSphere Enterprise Plus	サポート対象 **[デバイス]** > **[追加]** > **[仮想化ホスト]** > **[VMware ESXi]** > **[Windowsでのインストール用エージェント]** または、 **[デバイス]** > **[追加]** > **[仮想化ホスト]** > **[VMware ESXi]** > **[仮想アプライアンス（OVF）]** をクリックします。	サポート対象 **[デバイス]** > **[追加]** > **[ワークステーション]**/**[サーバー]** > **[Windows]**/**[Linux]**
VMware vSphere Hypervisor（Free ESXi）**	サポート対象外	サポート対象 **[デバイス]** > **[追加]** > **[ワークステーション]**/**[サーバー]** > **[Windows]**/**[Linux]**
VMware サーバー（VMware 仮想サーバー） VMware Workstation VMware ACE VMware Player	サポート対象外	サポート対象 **[デバイス]** > **[追加]** > **[ワークステーション]**/**[サーバー]** > **[Windows]**/**[Linux]**

*これらのエディションでは、仮想ディスク用HotAdd転送がvSphere 5.0以降でサポートされています。バージョン4.1ではバックアップの実行は遅くなります。

** この製品は Remote Command Line Interface（RCLI）へのアクセスが読み取り専用モードに制限されているため、ハイパーバイザ レベルでのバックアップは、vSphere Hypervisor ではサポートされません。エージェントは、プロダクト キーが入力されていなければ、vSphere Hypervisor の評価期間中は動作します。プロダクト キーが入力されると、エージェントは動作を停止します。

注意
Cyber Protect Cloudでは、vSphereのメジャーバージョン内のアップデートが正式にサポートされます。

例えば、vSphere 8.0のサポートには、特に明記されていない限り、このバージョン内のすべてのアップデートのサポートが含まれます。つまり、vSphere 8.0 Update 1は、当初リリースされたvSphere 8.0とともにサポートされています。

特定のVMware vSphereバージョンがサポートされることで、対応するバージョンのvSANもサポートされます。たとえば、vSphere 8.0がサポートされている場合、vSAN 8.0もサポートされています。

制限事項

- **フォールト トレラント コンピュータ**
  エージェント for VMwareでは、VMware vSphere 6.0以降でフォールト トレランスが有効になっている場合のみ、フォールト トレラント コンピュータをバックアップします。それ以前のvSphereバージョンからアップグレードした場合、各コンピュータのフォールト トレランスを無効にして有効にすれば機能します。以前のvSphereバージョンを使用している場合、ゲスト オペレーティング システムにエージェントをインストールします。
- **独立ディスクおよび RDM**
  エージェント for VMware では、物理互換モードの Raw Device Mapping（RDM）ディスクや独立ディスクをバックアップは行いません。この場合、エージェントはこれらのディスクをスキップして、警告をログに追加します。この警告を回避するには、保護計画から独立ディスクと物理互換モードのRDMを除外します。これらのディスクやディスクのデータをバックアップする場合、ゲスト オペレーティング システムにエージェントをインストールします。
- **In-guest iSCSI接続**
  VMwareエージェントはゲストオペレーティングシステム内で動くiSCSIイニシエータによって接続されたLUNボリュームをバックアップしません。ESXiハイパーバイザーはそのようなボリュームを認識しないので、そのボリュームはハイパーバイザースナップショットに含まれず、警告なしにバックアップから省かれます。これらのボリュームやボリュームのデータをバックアップする場合、ゲストオペレーティングシステムにエージェントをインストールします。
- **暗号化仮想コンピュータ**（VMware vSphere 6.5で導入）
  - 暗号化された仮想コンピュータは暗号化されていない状態でバックアップされます。暗号化が不可欠である場合、保護計画作成時にバックアップの暗号化を有効にします。
  - 復元された仮想コンピュータは常に復号化されます。復元が完了後に手動で暗号化を有効にできます。
  - 暗号化仮想コンピュータをバックアップする場合には、エージェント for VMwareが実行されている仮想コンピュータも暗号化することをお勧めします。そうしないと、操作に想定されているより時間がかかる可能性があります。vSphere Web Clientでエージェントのコンピュータに**VM暗号化ポリシー**を適用します。
  - 暗号化仮想コンピュータは、エージェントにSAN転送モードを設定してもLAN経由でバックアップされます。VMwareが暗号化仮想ディスクのバックアップにSAN転送をサポートしないため、エージェントはNBD転送にフォールバックします。

- **セキュアブート**
  - VMWare仮想マシン:（VMware vSphere 6.5で導入）**セキュアブート**は仮想マシンが新しい仮想マシンとして復元された後に無効になります。復元が完了後に手動でこのオプションを有効にできます。この制限事項はVMwareに適用されます。
  - Hyper-V仮想マシン:すべてのGEN2 VMにおいては、仮想マシンが新しい仮想マシンまたは既存の仮想マシンにリカバリされた後、セキュアブートが無効になります。
- VMware vSphere 7.0では、**ESXi設定のバックアップ**はサポートされていません。
- **論理ボリューム使用でマシンがサポートされる操作**

  WindowsのLDM（ダイナミックディスク）やLinuxのLVMなど、論理ボリュームを使用するワークロードのバックアップと復元は、一部の制限付きでサポートされます。その制限の詳細については、"論理ボリューム使用でサポートされる操作"（55ページ）を参照してください。

Microsoft

プラットフォーム	エージェントレスバックアップ（ハイパーバイザーレベルのバックアップ）	エージェントベースのバックアップ（ゲストOS内のバックアップ）
Windows Server 2008（x64）（Hyper-V 使用） Windows Server 2008 R2（Hyper-V 使用） Microsoft Hyper-V Server 2008/2008 R2 Windows Server 2012/2012 R2（Hyper-V 使用） Microsoft Hyper-V Server 2012/2012 R2 Windows Server 8、8.1（x64）（Hyper-V 使用） Windows 10（Hyper-V 使用） Windows Server 2016 with Hyper-V: Nano Server以外のすべてのインストールオプション Microsoft Hyper-V Server 2016 Windows Server 2019 with Hyper-V: Nano Server以外のすべてのインストールオプション Microsoft Hyper-V Server 2019 Windows Server 2022 with Hyper-V: Nano Server以外のすべてのイン	サポート対象 **[デバイス]** > **[追加]** > **[仮想化ホスト]** > **[Hyper-V]**	サポート対象 **[デバイス]** > **[追加]** > **[ワークステーション]**/**[サーバー]** > **[Windows]**/**[Linux]**

プラットフォーム	エージェントレスバックアップ（ハイパーバイザーレベルのバックアップ）	エージェントベースのバックアップ（ゲストOS内のバックアップ）
ストールオプション		
Microsoft Virtual PC 2004, 2007 Windows Virtual PC	サポート対象外	サポート対象 **[デバイス]** > **[追加]** > **[ワークステーション]**/**[サーバー]** > **[Windows]**/**[Linux]**
Microsoft Virtual Server 2005	サポート対象外	サポート対象 **[デバイス]** > **[追加]** > **[ワークステーション]**/**[サーバー]** > **[Windows]**/**[Linux]**

注意
Storage Spaces Direct（S2D）搭載のハイパーコンバージドクラスター上で動作するHyper-V仮想マシンがサポートされています。Storage Spaces Directは、バックアップストレージとしてもサポートされています。

制限事項

- **パス スルー ディスク**
  Hyper-Vエージェントは、パス スルー ディスクをバックアップしません。バックアップ中、エージェントはこれらのディスクをスキップして、警告を追加します。警告を回避するには、保護計画からパススルーディスクを除外します。これらのディスクやディスクのデータをバックアップする場合、ゲスト オペレーティング システムにエージェントをインストールします。
- **Hyper-Vゲストクラスタリング**
  Hyper-Vエージェントは、Windows Serverフェールオーバークラスターのノードである Hyper-V仮想マシンのバックアップをサポートしません。ホストレベルのVSSスナップショットでは、外部のクォーラムディスクをクラスターから一時的に切断することもできます。これらのマシンをバックアップする場合、ゲストオペレーティングシステムにエージェントをインストールします。
- **In-guest iSCSI接続**
  Hyper-Vエージェントはゲストオペレーティングシステム内で動くiSCSIイニシエータによって接続されたLUNボリュームをバックアップしません。Hyper-Vハイパーバイザーはそのようなボリュームを認識しないので、そのボリュームはハイパーバイザースナップショットに含まれず、警告なしにバックアップから省かれます。これらのボリュームやボリュームのデータをバックアップする場合、ゲストオペレーティングシステムにエージェントをインストールします。
- **セキュアブート**
  すべてのGEN2 VMにおいては、仮想マシンが新しい仮想マシンまたは既存の仮想マシンにリカバリされた後、セキュアブートが無効になります。
- **論理ボリューム使用でマシンがサポートされる操作**

WindowsのLDM（ダイナミックディスク）やLinuxのLVMなど、論理ボリュームを使用するワークロードのバックアップと復元は、一部の制限付きでサポートされます。その制限の詳細については、"論理ボリューム使用でサポートされる操作"（55ページ）を参照してください。

- **アンパサンド記号を含むVHD/VHDXファイル名**

  Windows Server 2016以降を実行しているHyper-Vホストでは、VHD/VHDXファイルの名前にアンパサンド記号（&）が含まれている場合、Hyper-V 2012 R2またはそれ以前のバージョンで作成されたレガシー仮想マシン（バージョン5.0）をバックアップできません。

  このようなマシンをバックアップできるようにするには、Hyper-V Managerで、対応する仮想ディスクを仮想マシンから取り外し、VHD/VHDXファイル名を編集してアンパサンド記号を削除してから、ディスクを仮想マシンに再度接続します。

- **Microsoft WMIサブシステムでの依存関係**

  Hyper-V仮想マシンのエージェントレスバックアップは、Microsoft WMIサブシステム、特に`Msvm_VirtualSystemManagementService` クラスに依存しています。WMIクエリが失敗すると、バックアップも失敗します。`Msvm_VirtualSystemManagementService` クラスの詳細については、Microsoftのドキュメントを参照してください。

Scale Computing

プラットフォーム	エージェントレスバックアップ（ハイパーバイザーレベルのバックアップ）	エージェントベースのバックアップ（ゲストOS内のバックアップ）
Scale Computing Hypercore 8.8, 8.9, 9.0, 9.1, 9.2, 9.3	サポート対象 **[デバイス]** > **[追加]** > **[仮想化ホスト]** > **[Scale Computing HC3]**	サポート対象 **[デバイス]** > **[追加]** > **[ワークステーション]**/**[サーバー]** > **[Windows]**/**[Linux]**

制限事項

論理ボリューム使用でマシンがサポートされる操作

WindowsのLDM（ダイナミックディスク）やLinuxのLVMなど、論理ボリュームを使用するワークロードのバックアップと復元は、一部の制限付きでサポートされます。その制限の詳細については、"論理ボリューム使用でサポートされる操作"（55ページ）を参照してください。

Citrix

プラットフォーム	エージェントレスバックアップ（ハイパーバイザーレベルのバックアップ）	エージェントベースのバックアップ（ゲストOS内のバックアップ）
Citrix XenServer/Citrix Hypervisor 4.1.5, 5.5, 5.6, 6.0, 6.1, 6.2, 6.5, 7.0, 7.1, 7.2, 7.3, 7.4, 7.5, 8.0, 8.1, 8.2	サポート対象外	完全仮想化（HVM）ゲストのみがサポートされます。準仮想化（PV）ゲストはサポート対象外です。

プラットフォーム	エージェントレスバックアップ（ハイパーバイザーレベルのバックアップ）	エージェントベースのバックアップ（ゲストOS内のバックアップ）
		[デバイス] > **[追加]** > **[仮想化ホスト]** > **[Citrix XenServer]** > **[Windows]**/**[Linux]**

Red Hat および Linux

プラットフォーム	エージェントレスバックアップ（ハイパーバイザーレベルのバックアップ）	エージェントベースのバックアップ（ゲストOS内のバックアップ）
Red Hat Enterprise Virtualization (RHEV) 2.2, 3.0, 3.1, 3.2, 3.3, 3.4, 3.5, 3.6 Red Hat Virtualization (RHV) 4.0, 4.1	サポート対象外	サポート対象 **[デバイス]** > **[追加]** > **[ワークステーション]**/**[サーバー]** > **[Windows]**/**[Linux]**
Red Hat Virtualization（oVirtによる管理）4.2、4.3、4.4、4.5	サポート対象 **[デバイス]** > **[追加]** > **[仮想化ホスト]** > **[Red Hat Virtualization（oVirt）]**	サポート対象 **[デバイス]** > **[追加]** > **[ワークステーション]**/**[サーバー]** > **[Windows]**/**[Linux]**
Kernel-based Virtual Machine（KVM）	サポート対象外	サポート対象 **[デバイス]** > **[追加]** > **[KVM]** > **[Windows]**/**[Linux]**
Red Hat Enterprise Linux 7.6, 7.7またはCentOS 7.6、7.7上で動作する、oVirt 4.3で管理されるカーネルベースの仮想マシン（KVM）。	サポート対象 **[デバイス]** > **[追加]** > **[仮想化ホスト]** > **[Red Hat Virtualization（oVirt）]**	サポート対象 **[デバイス]** > **[追加]** > **[ワークステーション]**/**[サーバー]** > **[Windows]**/**[Linux]**
Red Hat Enterprise Linux 8.xまたはCentOS Stream 8.x上で動作する、oVirt 4.4で管理されるカーネルベースの仮想マシン（KVM）。	サポート対象 **[デバイス]** > **[追加]** > **[仮想化ホスト]** > **[Red Hat Virtualization（oVirt）]**	サポート対象 **[デバイス]** > **[追加]** > **[ワークステーション]**/**[サーバー]** > **[Windows]**/**[Linux]**
Red Hat Enterprise Linux 8.xまたはCentOS Stream 8.x上で動作する、oVirt 4.5で管理されるカーネルベースの仮想マシン（KVM）	サポート対象 **[デバイス]** > **[追加]** > **[仮想化ホスト]** > **[Red Hat Virtualization（oVirt）]**	サポート対象 **[デバイス]** > **[追加]** > **[ワークステーション]**/**[サーバー]** > **[Windows]**/**[Linux]**

制限事項

論理ボリューム使用でマシンがサポートされる操作

WindowsのLDM（ダイナミックディスク）やLinuxのLVMなど、論理ボリュームを使用するワークロードのバックアップと復元は、一部の制限付きでサポートされます。その制限の詳細については、"論理ボリューム使用でサポートされる操作"（55ページ）を参照してください。

Parallels

プラットフォーム	エージェントレスバックアップ（ハイパーバイザーレベルのバックアップ）	エージェントベースのバックアップ（ゲストOS内のバックアップ）
Parallels Workstation	サポート対象外	サポート対象 **[デバイス]** > **[追加]** > **[ワークステーション]**/**[サーバー]** > **[Windows]**/**[Linux]**
Parallels Server 4 Bare Metal	サポート対象外	サポート対象 **[デバイス]** > **[追加]** > **[ワークステーション]**/**[サーバー]** > **[Windows]**/**[Linux]**

Oracle

プラットフォーム	エージェントレスバックアップ（ハイパーバイザーレベルのバックアップ）	エージェントベースのバックアップ（ゲストOS内のバックアップ）
Oracle Virtualization Manager（oVirtベース）*4.3	サポート対象 **[デバイス]** > **[追加]** > **[仮想化ホスト]** > **[Red Hat Virtualization（oVirt）]**	サポート対象 **[デバイス]** > **[追加]** > **[ワークステーション]**/**[サーバー]** > **[Windows]**/**[Linux]**
Oracle VM Server 3.0, 3.3, 3.4	サポート対象外	完全仮想化（HVM）ゲストのみがサポートされます。準仮想化（PV）ゲストはサポート対象外です。 **[デバイス]** > **[追加]** > **[仮想化ホスト]** > **[Oracle]** > **[Windows]**/**[Linux]**
Oracle VM VirtualBox 4.x	サポート対象外	サポート対象 **[デバイス]** > **[追加]** > **[仮想化ホ**

プラットフォーム	エージェントレスバックアップ（ハイパーバイザーレベルのバックアップ）	エージェントベースのバックアップ（ゲストOS内のバックアップ）
		スト] > [**Oracle**] > [**Windows**]/[**Linux**]

*Oracle Virtualization Managerは、oVirtエージェントによってサポートされます。

制限事項

論理ボリューム使用でマシンがサポートされる操作

WindowsのLDM（ダイナミックディスク）やLinuxのLVMなど、論理ボリュームを使用するワークロードのバックアップと復元は、一部の制限付きでサポートされます。その制限の詳細については、"論理ボリューム使用でサポートされる操作"（55ページ）を参照してください。

Nutanix

プラットフォーム	エージェントレスバックアップ（ハイパーバイザーレベルのバックアップ）	エージェントベースのバックアップ（ゲストOS内のバックアップ）
NutanixAcropolisハイパーバイザー(AHV)20160925.xから20180425.x	サポート対象外	サポート対象 [**デバイス**] > [**追加**] > [**仮想化ホスト**] > [**Nutanix AHV**] > [**Windows**]/[**Linux**]

Virtuozzo

プラットフォーム	エージェントレスバックアップ（ハイパーバイザーレベルのバックアップ）	エージェントベースのバックアップ（ゲストOS内のバックアップ）
Virtuozzo 6.0.10, 6.0.11, 6.0.12	サポート対象 [**デバイス**] > [**追加**] > [**仮想化ホスト**] > [**Virtuozzo**]	仮想マシンのみがサポートされています。コンテナはサポート対象外です。 [**デバイス**] > [**追加**] > [**ワークステーション**]/[**サーバー**] > [**Windows**]/[**Linux**]
Virtuozzo 7.0.13, 7.0.14	Ploopコンテナのみがサポートされています。仮想マシンはサポート対象外です。 [**デバイス**] > [**追加**] > [**仮想化ホスト**] > [**Virtuozzo**]	仮想マシンのみがサポートされています。コンテナはサポート対象外です。 [**デバイス**] > [**追加**] > [**ワークステーション**]/[**サーバー**] >

プラットフォーム	エージェントレスバックアップ（ハイパーバイザーレベルのバックアップ）	エージェントベースのバックアップ（ゲストOS内のバックアップ）
		[Windows]/[Linux]
Virtuozzo Hybrid Server 7.5	サポート対象 [デバイス] > [追加] > [仮想化ホスト] > [Virtuozzo]	仮想マシンのみがサポートされています。コンテナはサポート対象外です。 [デバイス] > [追加] > [ワークステーション]/[サーバー] > [Windows]/[Linux]

制限事項

論理ボリューム使用でマシンがサポートされる操作

WindowsのLDM（ダイナミックディスク）やLinuxのLVMなど、論理ボリュームを使用するワークロードのバックアップと復元は、一部の制限付きでサポートされます。その制限の詳細については、"論理ボリューム使用でサポートされる操作"（55ページ）を参照してください。

Virtuozzo Hybrid Infrastructure

プラットフォーム	エージェントレスバックアップ（ハイパーバイザーレベルのバックアップ）	エージェントベースのバックアップ（ゲストOS内のバックアップ）
Virtuozzo Hybrid Infrastructure 3.5, 4.5, 4.6, 4.7, 5.0, 5.1, 5.2, 5.3, 5.4, 6.0	サポート対象 [デバイス] > [追加] > [仮想化ホスト] > [Virtuozzo Hybrid infrastructure]	サポート対象 [デバイス] > [追加] > [ワークステーション]/[サーバー] > [Windows]/[Linux]

制限事項

- **外付けiSCSIストレージ上のディスクを使用したVMのエージェントレスバックアップ**
  VMディスクが（VHIクラスターに接続された）外部iSCSIボリュームに配置されている場合、Virtuozzo Hybrid InfrastructureからVMをバックアップすることはできません。
- **論理ボリューム使用でマシンがサポートされる操作**
  WindowsのLDM（ダイナミックディスク）やLinuxのLVMなど、論理ボリュームを使用するワークロードのバックアップと復元は、一部の制限付きでサポートされます。その制限の詳細については、"論理ボリューム使用でサポートされる操作"（55ページ）を参照してください。

Amazon

プラットフォーム	エージェントレスバックアップ（ハイパーバイザーレベルのバックアップ）	エージェントベースのバックアップ（ゲストOS内のバックアップ）
Amazon EC2インスタンス	サポート対象外	サポート対象 **[デバイス]** > **[追加]** > **[ワークステーション]**/**[サーバー]** > **[Windows]**/**[Linux]**

Microsoft Azure

プラットフォーム	エージェントレスバックアップ（ハイパーバイザーレベルのバックアップ）	エージェントベースのバックアップ（ゲストOS内のバックアップ）
Azure仮想コンピュータ	サポート対象外	サポート対象 **[デバイス]** > **[追加]** > **[ワークステーション]**/**[サーバー]** > **[Windows]**/**[Linux]**

暗号化ソフトウェアとの互換性

ファイルレベル暗号化ソフトウェアによって暗号化されるデータのバックアップと復元には制限がありません。

ディスクレベルの暗号化ソフトウェアは、オンザフライでデータを暗号化します。これは、バックアップに含まれるデータが暗号化されていないためです。ディスクレベルの暗号化ソフトウェアは多くの場合、ブート レコード、パーティション テーブル、またはシステム テーブルなどのシステム領域の一部を変更します。こうした要素は、ディスクレベルバックアップと復元、リカバリされたシステムの起動とSecure Zoneへのアクセスに影響を与えます。

次のディスクレベル暗号化ソフトウェアで暗号化されたデータをバックアップできます。

- Microsoft BitLocker Drive Encryption
- McAfee Endpoint Encryption
- PGP Whole Disk Encryption

信頼できるディスクレベルの復元を確保するには、次の一般的なルールとソフトウェア固有の推奨事項に従ってください。

一般的なインストール ルール

プロテクションエージェントをインストールする前に、暗号化ソフトウェアをインストールすることを強く推奨します。

Secure Zoneの使用方法

Secure Zoneは、ディスクレベル暗号化で暗号化しないでください。Secure Zoneは次の方法でのみ使用できます。

1. 暗号化ソフトウェアをインストールしてから、エージェントをインストールします。
2. Secure Zoneを作成します。
3. ディスクまたはそのボリュームを暗号化する際はSecure Zoneを除外します。

共通バックアップ ルール

オペレーティング システムで、ディスクレベルのバックアップを実行できます。

ソフトウェア固有の復元手順

Microsoft BitLocker Drive Encryption

BitLocker で暗号化されたシステムを復元するには

1. ブータブル メディアから起動します。
2. システムを復元します。復元されたデータが復号化されます。
3. 復元されたシステムを再起動します。
4. BitLocker を有効にします。

パーティションが複数あるディスクのパーティション 1 つのみを復元する場合は、オペレーティング システム上で実行してください。ブータブル メディア上で復元すると、復元されたパーティションが Windows で検出されない場合があります。

McAfee Endpoint Encryption および PGP Whole Disk Encryption

暗号化されたシステム パーティションの復元が可能なのは、ブータブル メディアを使用する場合だけです。

復元されたシステムを起動できない場合は、Microsoft サポート技術情報（https://support.microsoft.com/kb/2622803）の記事の手順に従ってマスター ブート レコードを再構築してください。

Dell EMC Data Domainストレージの機能

Dell EMC Data Domainデバイスをバックアップストレージとして使用することができます。

このストレージでは、例えば**常に完全**など、定期的に完全バックアップを作成するバックアップスキームの使用をお勧めします。利用可能なバックアップスキームの詳細については、"バックアップ スキーム"（406ページ）を参照してください。

保持ロック（ガバナンスモード）がサポートされています。保持ロックが有効化されている場合、当該のストレージをバックアップ先として使用するプロテクションエージェントのマシンに、`AR_RETENTION_LOCK_SUPPORT`環境変数を追加する必要があります。

注意
Macエージェントでは、保持ロックが有効化されたDell EMC Data Domainストレージはサポートされていません。

AR_RETENTION_LOCK_SUPPORT環境変数を追加するには

Windowsの場合

1. プロテクションエージェントが稼働するマシンに管理者としてログインします。
2. **コントロールパネル**で、[**システムとセキュリティ**] > [**システム**] > [**システムの詳細設定**] に進みます。
3. [**詳細**] **タブ**で、[**環境変数**] をクリックします。
4. [**システム環境変数**] パネルで [**新規**] をクリックします。
5. [**新しいシステム変数**] ウィンドウで、以下の新しい変数を追加します。
   - 変数名:AR_RETENTION_LOCK_SUPPORT
   - 変数の値:1
6. [**OK**] をクリックします。
7. [**環境変数**] ウィンドウで [**OK**] をクリックします。
8. コンピュータを再起動します。

Linuxの場合

1. プロテクションエージェントが稼働するマシンに管理者としてログインします。
2. /sbinディレクトリに移動し、acronis_mmsファイルを開いて編集します。
3. export LD_LIBRARY_PATH行の上に以下の行を追加します。

   ```
   export AR_RETENTION_LOCK_SUPPORT=1
   ```

4. acronis_mmsファイルを保存します。
5. コンピュータを再起動します。

仮想アプライアンスで

1. 仮想アプライアンスに管理者としてログインします。
2. /binディレクトリに移動し、autostartファイルを開いて編集します。
3. export LD_LIBRARY_PATH行の下に以下の行を追加します。

   ```
   export AR_RETENTION_LOCK_SUPPORT=1
   ```

4. autostartファイルを保存します。
5. 仮想アプライアンスマシンを再起動します。

オペレーティングシステムでサポートされる保護機能

このトピックでは、Cyber Protect Cloudの保護機能について扱います。バックアップと復元の機能は取り上げられていません。

保護機能は、プロテクションエージェントがインストールされたマシンのみでサポートされます。Hyper-Vエージェント、VMwareエージェント、Virtuozzo Hybrid Infrastructureエージェント、Scale Computingエージェント、またはoVirtエージェントなどによるエージェントレスモードでバックアップされた仮想マシンでは利用できません。

適用されるライセンスモデルによっては、一部の機能で追加のライセンスが必要になる場合があります。

サポートされるオペレーティングシステムとバージョン

Windows

特定の機能セットについて特に記載がない限り、以下のWindowsバージョンがサポートされています。

- Windows 7 Service Pack 1以降
- Windows Server 2008 R2 Service Pack 1以降

注意
Windows 7の場合、プロテクションエージェントをインストールする前に、Microsoftが提供する次のアップデートプログラムをインストールする必要があります。

- Windows 7拡張セキュリティアップデートプログラム（ESU）
- KB4474419
- KB4490628

必要なアップデートの詳細については、このナレッジベースの記事を参照してください。

Linux

サポートされているLinuxディストリビューションとそのバージョンは、機能セットによって異なり、各表の下部に掲載されています。

macOS

サポートされているmacOSのバージョンは、機能セットによって異なり、各表の下部に掲載されています。

機能セット	Windows	Linux	macOS
既定の保護計画			
リモートワーカー	はい	いいえ	いいえ
オフィスワーカー（サードパーティのウイルス対策）	はい	いいえ	いいえ
オフィスワーカー（Cyber Protectウイルス対策）	はい	いいえ	いいえ
Cyber Protect Essentials（Cyber Protect Essentials Editionのみ）	はい	いいえ	いいえ
サポート対象のWindowsバージョンについては、"サポートされるオペレーティングシステムとバージョン"			

機能セット	Windows	Linux	macOS
既定の保護計画			
（44ページ）を参照してください。			

機能セット	Windows	Linux	macOS
フォレンジックバックアップ			
メモリダンプの収集	はい	いいえ	いいえ
動作中のプロセスのスナップショット	はい	いいえ	いいえ
ローカルイメージフォレンジックバックアップの公証	はい	いいえ	いいえ
クラウドイメージフォレンジックバックアップの公証	はい	いいえ	いいえ
サポート対象のWindowsバージョンについては、"サポートされるオペレーティングシステムとバージョン"（44ページ）を参照してください。			

機能	Windows	Linux	macOS
継続的データ保護（CDP）			
ファイルとフォルダのCDP	はい	いいえ	いいえ
アプリケーショントラッキングによる変更ファイルのCDP	はい	いいえ	いいえ
サポート対象のWindowsバージョンについては、"サポートされるオペレーティングシステムとバージョン"（44ページ）を参照してください。			

機能セット	Windows	Linux	macOS
自動検出とリモートインストール			
ネットワークベースの検出	はい	いいえ	いいえ
Active Directoryベースの検出	はい	いいえ	いいえ
テンプレートベースの検出（ファイルからマシンをインポート）	はい	いいえ	いいえ
デバイスの手動追加	はい	いいえ	いいえ
サポート対象のWindowsバージョンについては、"サポートされるオペレーティングシステムとバージョン"（44ページ）を参照してください。			

機能セット	Windows	Linux	macOS
Active Protection			
プロセスインジェクト検出	はい	いいえ	いいえ
影響を受けたファイルのローカルキャッシュからの自動復元	はい	はい	はい
Acronisバックアップファイルの自己防御	はい	いいえ	いいえ
Acronisソフトウェアの自己防御	はい	いいえ	はい (Active Protectionおよびマルウェア対策コンポーネントのみ)
信頼できる/ブロックされているプロセスの管理	はい	いいえ	はい
プロセス/フォルダの除外	はい	はい	はい
プロセスの動作に基づくランサムウェア検出（AIベース）	はい	はい	はい
プロセスの動作に基づくクリプトマイニングプロセス検出	はい	いいえ	いいえ
外付けドライブ保護（HDD、フラッシュドライブ、SDカード）	はい	いいえ	はい
ネットワークフォルダの保護	はい	はい	はい
サーバー側保護機能	はい	いいえ	いいえ
Zoom、Cisco WebEx、Citrix Workspace、Microsoft Teamsの保護	はい	いいえ	いいえ
サポート対象のオペレーティングシステムとバージョンの詳細については、"サポートされるプラットフォーム"（796ページ）を参照してください。			

機能セット	Windows	Linux	macOS
ウイルスおよびマルウェア対策保護			
完全統合型のActive Protection機能	はい	いいえ	いいえ
リアルタイムのマルウェア対策保護	はい	はい（高度なマルウェア対策機能パック付	はい (Advancedマルウェア対策パック付属)

機能セット	Windows	Linux	macOS
ウイルスおよびマルウェア対策保護			
		属）	
ローカル署名ベースの検出によるAdvancedリアルタイムマルウェア対策保護	はい	はい	はい
ポータブル実行可能ファイルの静的分析	はい	いいえ	はい*
オンデマンドマルウェア対策スキャン	はい	はい**	はい
ネットワークフォルダの保護	はい	はい	いいえ
サーバー側保護機能	はい	いいえ	いいえ
アーカイブファイルのスキャン	はい	いいえ	はい
リムーバブルドライブのスキャン	はい	いいえ	はい
新規ファイルと変更ファイルのみスキャン	はい	いいえ	はい
ファイル/フォルダの除外	はい	はい	はい***
プロセスの除外	はい	いいえ	はい
挙動分析エンジン	はい	いいえ	はい
エクスプロイト防御	はい	いいえ	いいえ
検疫	はい	はい	はい
検疫自動クリーンアップ	はい	はい	はい
URLフィルタ処理（http/https）	はい	いいえ	いいえ
全社レベルのホワイトリスト	はい	いいえ	はい
ファイアウォール管理****	はい	いいえ	いいえ
Microsoft Defender Antivirus管理*****	はい	いいえ	いいえ
Microsoft Security Essentials管理	はい	いいえ	いいえ
Windows Security Centerでのウイルスおよびマルウェア対策保護の登録と管理	はい	いいえ	いいえ
サポート対象のオペレーティングシステムとバージョンの詳細については、"サポートされるプラットフォーム"（796ページ）を参照してください。			

* ポータブル実行可能ファイルの静的分析は、macOSでのスケジュールされたスキャンでのみサポートされています。

** 開始条件は、Linuxのオンデマンドスキャンではサポートされていません。

*** ファイル/フォルダ除外は、macOSでのリアルタイム保護またはスケジュールスキャンによるスキャンを行わないファイルとフォルダを指定する場合にのみサポートされます。

****Windows 8以降でファイアウォールの管理がサポートされています。Windows Serverはサポート対象ではありません。

*****Microsoft Defender Antivirusの管理はWindows 8.1以降でサポートされています。

機能セット	Windows	Linux	macOS
脆弱性診断			
オペレーティングシステムとそのネイティブアプリケーションの脆弱性診断	はい	はい******	はい
サードパーティ製アプリケーションの脆弱性診断	はい	いいえ	はい
サポート対象のオペレーティングシステムとバージョンの詳細については、"サポート対象のMicrosoft製品とサードパーティ製品"（924ページ）、"サポートされているLinux製品"（927ページ）、"サポート対象のApple製品とサードパーティ製品"（926ページ）を参照してください。			

******脆弱性診断は、https://lists.centos.org/pipermail/centos-announce/、https://lists.centos.org/pipermail/centos-cr-announceなどの公式のセキュリティアドバイザリが提供されているかどうかによって異なります。

機能セット	Windows	Linux	macOS
パッチ管理			
パッチの自動承認	はい	いいえ	いいえ
パッチの自動インストール	はい	いいえ	いいえ
パッチのテスト	はい	いいえ	いいえ
パッチの手動インストール	はい	いいえ	いいえ
パッチのスケジューリング	はい	いいえ	いいえ
フェイルセーフのパッチ適用: 保護計画の一環としてパッチをインストールする前のマシンバックアップ	はい	いいえ	いいえ
バックアップ実行時のマシン再起動のキャンセル	はい	いいえ	いいえ
サポート対象のWindowsバージョンについては、"サポートされるオペレーティングシステムとバージョン"（44ページ）を参照してください。			

機能	Windows	Linux	macOS
データ保護マップ			
重要ファイルの調整可能定義	はい	いいえ	いいえ
保護されていないファイルを見つけるためのマシンスキャン	はい	いいえ	いいえ
保護されていないロケーションの概要	はい	いいえ	いいえ
データ保護マップウィジェットから保護アクション（**[すべてのファイルを保護]** アクション）を開始する機能	はい	いいえ	いいえ
サポート対象のWindowsバージョンについては、"サポートされるオペレーティングシステムとバージョン"（44ページ）を参照してください。			

機能セット	Windows	Linux	macOS
ディスク状態			
HDDとSSDのAIベースヘルス制御	はい	いいえ	いいえ
サポート対象のWindowsバージョンについては、"サポートされるオペレーティングシステムとバージョン"（44ページ）を参照してください。			

機能	Windows	Linux	macOS
Acronisサイバープロテクションオペレーションセンター（CPOC）のアラートに基づくスマート保護計画			
脅威フィード	はい	いいえ	いいえ
修復ウィザード	はい	いいえ	いいえ
サポート対象のWindowsバージョンについては、"サポートされるオペレーティングシステムとバージョン"（44ページ）を参照してください。			

機能セット	Windows	Linux	macOS
バックアップスキャン			
バックアップ計画の一部として実行するイメージバックアップのマルウェア対策スキャン	はい	いいえ	いいえ
マルウェアを検出するためのクラウドでのイメージバックアップスキャン	はい	いいえ	いいえ
暗号化されたバックアップのマルウェアスキャン	はい	いいえ	いいえ
サポート対象のWindowsバージョンについては、"サポートされるオペレーティングシステムとバージョン"（44ページ）を参照してください。			

機能セット	Windows	Linux	macOS
安全な復元			
ウイルスおよびマルウェア対策保護機能による復元プロセス中のマルウェアスキャン	はい	いいえ	いいえ
暗号化されたバックアップの安全な復元	はい	いいえ	いいえ
サポート対象のWindowsバージョンについては、"サポートされるオペレーティングシステムとバージョン"（44ページ）を参照してください。			

機能セット	Windows	Linux	macOS
リモートデスクトップ接続			
NEAR経由での接続	はい	はい	はい
RDP経由での接続	はい	いいえ	いいえ
Apple画面共有経由での接続	いいえ	いいえ	はい
Webクライアント経由での接続	はい	いいえ	いいえ
クイックアシスト経由での接続	はい	はい	はい
リモートアシスタンス	はい	はい	はい
ファイル転送	はい	はい	はい
スクリーンショット送信	はい	はい	はい
サポート対象のオペレーティングシステムとバージョンの詳細については、"サポートされるプラットフォーム"（961ページ）を参照してください。			

機能セット	Windows	Linux	macOS
#CyberFitスコア			
#CyberFitスコアステータス	はい	いいえ	いいえ
#CyberFitスコアのスタンドアロンツール	はい	いいえ	いいえ
#CyberFitスコアの推奨事項	はい	いいえ	いいえ
サポート対象のWindowsバージョンについては、"サポートされるオペレーティングシステムとバージョン"（44ページ）を参照してください。			

機能セット	Windows	Linux	macOS
データ漏洩防止			
デバイス制御	はい	いいえ	macOS 10.15以降またはmacOS 11.2.3以降が動作するIntelプロセッサ搭載のMacをサポートして言います。 ARMベースのAppleシリコンプロセッサ（Apple M1/M2など）はサポートされていません。
Advanced Data Loss Prevention	はい	いいえ	いいえ
サポート対象のWindowsバージョンについては、"サポートされるオペレーティングシステムとバージョン"（44ページ）を参照してください。			

機能セット	Windows	Linux	macOS
管理オプション			
Cyber Protectエディションのプロモーションのためのアップセルシナリオ	はい	はい	はい
Webベースの集中リモート管理コンソール	はい	はい	はい
サポートされるオペレーティングシステムとバージョン:プラットフォームに依存しません。			

機能セット	Windows	Linux	macOS
保護オプション			
リモートワイプ	はい	いいえ	いいえ
Windows 10以降でサポートされています。			

機能セット	Windows	Linux	macOS
Cyber Protectモニタ			
Cyber Protectアプリ	はい	いいえ	はい
Zoomの保護ステータス	はい	いいえ	いいえ
Cisco Webexの保護ステータス	はい	いいえ	いいえ
Citrix Workspaceの保護ステータス	はい	いいえ	いいえ
Microsoft Teamsの保護ステータス	はい	いいえ	いいえ
サポート対象のWindowsバージョンについては、"サポートされるオペレーティングシステムとバージョン"（44ページ）を参照してください。 macOSの場合、Cyber Protectモニタは、Macエージェントをインストールできるすべてのバージョンでサポートされています。詳細については、"Macエージェント"（27ページ）を参照してください。			

機能セット	Windows	Linux	macOS
ソフトウェアインベントリ			
ソフトウェアインベントリのスキャン	はい	いいえ	はい
ソフトウェアインベントリの監視	はい	いいえ	はい
サポート対象のWindowsバージョンについては、"サポートされるオペレーティングシステムとバージョン"（44ページ）を参照してください。 macOSの場合、ソフトウェアインベントリはバージョン10.13.x～13.xでサポートされています。			

機能セット	Windows	Linux	macOS
ハードウェアインベントリ			
ハードウェアインベントリのスキャン	はい	いいえ	はい
ハードウェアインベントリの監視	はい	いいえ	はい
サポート対象のWindowsバージョンについては、"サポートされるオペレーティングシステムとバージョン"（44ページ）を参照してください。 macOSの場合、ハードウェアインベントリはバージョン10.13.x～13.xでサポートされています。			

サポートされるファイル システム

保護エージェントは、エージェントがインストールされているオペレーティングシステムからアクセスできれば、どのファイルシステムでもバックアップできます。たとえば、エージェント for Windows

は、対応するドライバがWindowsにインストールされていれば、ext4ファイル システムをバックアップして復元することができます。

次の表には、バックアップと復元が可能なファイル システムについてまとめてあります（ブータブル メディアは復元のみサポート）。制限事項はエージェントとブータブル メディアの両方に適用されます。

ファイル システム	サポートするエージェントまたはブータブル メディア			制限事項
	エージェント	Windowsおよび Linux用ブータブル メディア	Mac用ブータブル メディア	
FAT16/32	全エージェント	+	+	制限なし
NTFS	全エージェント	+	+	
ext2/ext3/ext4	全エージェント	+	-	
HFS+	エージェント for Mac	-	+	
APFS	エージェント for Mac	-	+	• サポート対象は macOS High Sierra 10.13 以降 • 別のマシンやベアメタルに復元する場合は、ディスクの設定を手動で再作成する必要があります。
JFS	Linuxエージェント	+	-	• ファイルフィルタ（包含/除外）はサポートされていません • 高速増分/差分バックアップを有効にできません
ReiserFS3	Linuxエージェント	+	-	
ReiserFS4	Linuxエージェント	+	-	• ファイルフィルタ（包含/除外）はサポートされていません • 高速増分/差分バックアップを有効にできません • 復元中はボリュームのサイズ変更不可
ReFS	全エージェント	+	+	• ファイルフィルタ（包含/除外）はサポートされていません • 高速増分/差分バックアップを有

ファイル システム	サポートするエージェントまたはブータブル メディア			制限事項
	エージェント	WindowsおよびLinux用ブータブル メディア	Mac用ブータブル メディア	
				効にできません • 復元中はボリュームのサイズ変更不可 • ReFSバックアップからのファイル復元中は、内容のみが復元されます。アクセス制御リスト（ACL）とalternate streamは復元されません。スパースファイルは通常のファイルとして復元されます。
XFS	全エージェント	+	+	• ファイルフィルタ（包含/除外）はサポートされていません • 高速増分/差分バックアップを有効にできません • 復元中はボリュームのサイズ変更不可 • XFSファイルシステムでは、高速増分バックアップモードはサポートされていません。XFSボリュームのクラウドへの増分バックアップと差分バックアップは、高速増分モードを使用した同等のext4バックアップと比べて大幅に遅延する場合があります。
Linux Swap	Linuxエージェント	+	-	制限なし
exFAT	全エージェント	+ バックアップが exFAT フォーマットで保存されている場合、ブータブルメ	+	• ディスク/ボリュームのバックアップのみがサポートされます • ファイルフィルタ（包含/除外）はサポートされていません • 個別のファイルはバックアップから復元できません

ファイル システム	サポートするエージェントまたはブータブル メディア			制限事項
	エージェント	Windowsおよびlinux用ブータブル メディア	Mac用ブータブル メディア	
		ディアを復元に使用することはできません		

認識されないファイルシステムやサポートされていないファイルシステム（Btrfsなど）のドライブをバックアップするときは、ソフトウェアが自動的にセクターバイセクターノードに切り替えられます。次のファイル システムの場合、セクタ単位のバックアップが可能です。

- ブロックベース
- 単一ディスク内
- 標準MBR/GPTパーティション スキームがある

ファイル システムが上記の要件を満たさない場合、バックアップできません。

データの重複除外

Windows Server 2012以降では、NTFSボリュームのデータの重複除外機能を有効にできます。データの重複除外を実行すると、ボリュームのファイルのフラグメントのうち重複しているものが 1 回しか保存されないため、使用する領域が小さくなります。

データの重複除外が有効になっているボリュームのバックアップとリカバリはディスクレベルで制限なく実行できます。Acronis VSSプロバイダーを使用する場合を除き、ファイルレベルのバックアップがサポートされます。ディスクバックアップからファイルをリカバリするには、バックアップから仮想マシンを実行するか、Windows Server 2012以降を実行しているマシンでバックアップをマウントし、マウントされたボリュームからファイルをコピーします。

Windows Serverのデータ重複除去機能は、Acronis Backupの重複除外機能とは関係ありません。

論理ボリューム使用でサポートされる操作

WindowsのLDM（ダイナミックディスク）やLinuxのLVMなど、論理ボリュームを使用するワークロードのバックアップと復元は、次の制限付きでサポートされます。

バックアップ

エージェントベースバックアップは、ワークロードにインストールされたプロテクション エージェント、またはブータブルメディアによって作成されるバックアップです。

エージェントレスバックアップは仮想マシンにのみ利用可能です。エージェントレスバックアップは、環境内のすべての仮想マシンをバックアップおよび復元できるエージェントによってハイパーバイザーレベルで実行されます。保護対象の仮想マシンには個別のエージェントはインストールされません。

エージェントベースとエージェントレスのバックアップの違いについては、"エージェントベースのバックアップとエージェントレスバックアップ"（65ページ）を参照してください。

エージェントベースのバックアップ	エージェントレスバックアップ
• 論理ボリュームがボリューム単位でバックアップされる。 • ファイルフィルタ（包含/除外）がサポートされている。	• ディスク上で論理ボリュームが検出されると、ディスクはセクタ単位（RAW）モードでバックアップされる。ディスクのパーティション構造は分析されず、ボリュームイメージは個別には保存されない。 • 直接選択でもポリシールールの使用でも、個々のLDMまたはLVMボリュームをバックアップソースとして選択できない。保護プランの**[バックアップ対象]**セクションで使用できるのは、**[マシン全体]**のみ。 • ファイルフィルタ（包含/除外）はサポートされていない。構成された包含または除外は無視される。

復元

エージェントベースの復元は、ワークロードにインストールされたエージェント、またはブータブルメディアによって実行される復元です。

エージェントレス復元は、仮想マシンのみをターゲットとしてサポートします。このエージェントレス復元は、環境内のすべての仮想マシンをバックアップおよび復元できるエージェントによってハイパーバイザーレベルで実行されます。バックアップを復元するターゲットマシンを手動で作成する必要はありません。

	エージェントベースのバックアップから	エージェントレスバックアップから
エージェントベースの復元	• ボリュームごとの復元が可能。 • ファイルとフォルダの復元が可能。	• ボリュームごとの復元はできない。 • ファイルとフォルダの復元が可能。
エージェントレス復元	• マシンのマイグレーション（P2V、V2P、V2V）はサポートされていない。エージェントベースのバックアップからデータを復元するには、ブータブルメディアを使用する。 • 「**VMとして実行**」操作がサポートされていない。 • ファイルとフォルダの復元が可能。	• ボリュームごとの復元はできない。 • マシン全体の復元が可能。 • ファイルとフォルダの復元が可能。 • 「**VMとして実行**」操作がサポートされている。仮想マシンを起動可能にするには、起動順序を変更する必要がある。詳細については、このナレッジベースの記事を参照。

	エージェントベースのバックアップから	エージェントレスバックアップから
		• 次の仮想マシンの種類への変換をサポート: ◦ VMware ESXi ◦ Microsoft Hyper-V ◦ Scale Computing HC3

Cyber Protectionエージェントのインストールと配置

インストールする前に

手順1

バックアップアップ対象にインストールするエージェントを選択します。利用可能な選択肢の詳細については、「どのエージェントが必要ですか？」を参照してください。

手順2

エージェントをインストールするのに十分な空き領域がハードドライブにあることを確認してください。必要な領域の詳細については、「"エージェントのシステム要件"（66ページ）」を参照してください。

手順3

プログラムの設定をダウンロードします。ダウンロードリンクを確認するには、**[すべてのデバイス]** > **[追加]** の順にクリックします。

[デバイスの追加] ページには、Windowsにインストールする各エージェントのウェブ インストーラがあります。ウェブ インストーラとは、インターネットからメインのプログラムの設定をダウンロードして、一時ファイルに保存する小さい実行可能ファイルのことです。このファイルは、インストール後すぐに削除されます。

プログラムの設定をローカルに保存する場合は、**[デバイスの追加]** ページの下にあるリンクを使用して、Windowsにインストールするすべてのエージェントを含むパッケージをダウンロードします。32ビットと64ビットの両方のパッケージがあります。これらのパッケージでは、インストールするコンポーネントのリストをカスタマイズできます。このパッケージを使えば、グループ ポリシーを使用した無人インストールなども実施できます。この高度な設定については、"グループポリシーによるエージェントの配置"（163ページ）で詳しく説明しています。

Microsoft 365エージェントのセットアッププログラムをダウンロードするには、右上にあるアカウントアイコンをクリックし、その後 **[ダウンロード]** > **[Microsoft 365エージェント]** の順にクリックします。

Linux および macOS のインストールは、通常の設定プログラムから実行します。

Cyber Protectionサービスにマシンを登録するため、プログラムの設定にはすべてインターネット接続が必要です。インターネット接続がない場合、インストールできません。

手順4

Cyber Protect機能には、Microsoft Visual C++ 2017再頒布可能パッケージが必要です。既にマシンにインストールされていることを確認するか、エージェントをインストールする前にインストールしてください。Microsoft Visual C++のインストール後に再起動が必要になる場合があります。Microsoft Visual C++の再頒布可能パッケージは、https://support.microsoft.com/help/2999226/update-for-universal-c-runtime-in-windowsから入手できます。

手順5

ネットワークセキュリティシステムのファイアウォールや他のコンポーネント（プロキシサーバーなど）で次のTCPポートを使用した送信接続が許可されていることを確認します。

- ポート**443**および**8443**
  これらのポートは、Cyber Protectコンソールへのアクセス、エージェントの登録、証明書のダウンロード、ユーザー承認、クラウドストレージからのファイルのダウンロードに使用されます。
- ポート範囲**7770**～**7800**
  エージェントはこれらのポートを使用して管理サーバーと通信します。
- ポート**44445**および**55556**
  エージェントはバックアップ時および復元時のデータ転送にこれらのポートを使用します。

ネットワークでプロキシサーバが有効な場合は、"プロキシサーバー設定の構成"（72ページ）を参照し、プロテクションエージェントを実行する各マシンでこれらの設定を構成する必要があるかどうかを判断してください。

クラウドからエージェントを管理するために必要な最小インターネット接続速度は、1Mbit/s です（クラウドへのバックアップに許容されるデータ転送速度と混乱しないように注意してください）。ADSLなどの低帯域幅接続テクノロジを使用する場合、この点を考慮してください。

VMware仮想マシンのバックアップとレプリケーションに必要なTCP ポート

- ポート**443**
  VMwareエージェント（Windowsと仮想アプライアンスの両方）は、このポートをESXiホスト/vCenterサーバーに接続してVMの管理操作を実行します。この操作には、バックアップ、復元、VMレプリケーションの操作におけるvSphere上のVMの作成、アップデート、および削除が含まれます。
- ポート**902**
  VMwareエージェント（Windowsと仮想アプライアンスの両方）は、このポートをESXiホストに接続してNFC接続を確立し、バックアップ、復元、VMレプリケーションの操作においてVMディスクでのデータの読み書きを行います。
- ポート**3333**
  VMレプリケーションのターゲットであるESXiホスト/クラスターにおいてVMwareエージェント（仮想アプライアンス）が実行されている場合、VMレプリケーショントラフィックがポート**902**で直接ESXiホストに送られることはありません。トラフィックはソースとなるVMwareエージェントから、

ターゲットとなるESXiホスト/クラスターのVMwareエージェント（仮想アプライアンス）のTCPポート**3333**に向かいます。

元のVMディスクからデータを読み込むソース側のVMwareエージェントは、別の場所にあっても構いません。また、仮想アプライアンスとWindowsのどちらでも構いません。

VMレプリケーションデータをターゲット側のVMwareエージェント（仮想アプライアンス）で受け付けるサービスは、「レプリカディスクサーバー」と呼ばれます。このサービスでは、VMレプリケーション中のトラフィックの圧縮と重複除外などのWAN最適化技術が応用されており、これにはレプリカのシーディングが含まれます（「初期レプリカのシード」を参照）。ターゲット側のESXiホストにVMwareエージェント（仮想アプライアンス）が存在しない場合、このサービスは利用できないため、レプリカのシーディングのシナリオもサポートされません。

Downloaderコンポーネントに必要なポート

Downloaderコンポーネントは、コンピューターにアップデートを配信し、それらを他のDownloaderインスタンスに配布する役割を果たします。コンピューターをDownloaderエージェントに切り替えるエージェントモードで、実行することができます。Downloaderエージェントはインターネットからアップデートをダウンロードして、他のコンピューターに対するアップデートの配布元として機能します。Downloaderが動作するには、次のポートが必要です。

- TCPおよびUDP（受信）ポート**6888**
  トレントピアツーピアのアップデートのために、BitTorrentプロトコルによって使用されます。
- UDPポート**6771**
  ローカルピア検出ポートとして使用されます。ピアツーピアのアップデートにも使用されます。
- TCPポート**18018**
  異なるモードで動作するアップデータ間の通信に使用されます。アップデータモードとアップデータエージェントモードです。
- TCPポート**18019**
  アップデータとプロテクションエージェント間の通信に使用されるローカルポートです。

手順6

プロテクションエージェントをインストールするマシンで、以下のローカルポートが他のプロセスに使用されていないことを確認します。

- 127.0.0.1:**9999**
- 127.0.0.1:**43234**
- 127.0.0.1:**9850**

注意
ファイアウォール内で上記のポートを開く必要はありません。

プロテクションエージェントで使用されるポートの変更

ご使用の環境では、プロテクションエージェントで必要な一部のポートが他のアプリケーションによって使用されている場合があります。競合を回避するためには、次のファイルを修正して、プロテクショ

ンエージェントで使用されるポートを変更することができます。

- Linuxの場合: `/opt/Acronis/etc/aakore.yaml`
- Windowsの場合: `\ProgramData\Acronis\Agent\etc\aakore.yaml`

エージェント

エージェントの選択は、何をバックアップするかによって異なります。次の表に、判断に役立つ情報をまとめています。

Windowsの場合、Exchangeエージェント、SQLエージェント、Active Directoryエージェント、Oracleエージェントとともに、Windowsエージェントもインストールする必要があります。つまり、 SQLエージェントをインストールした場合は、エージェントがインストールされたマシン全体をバックアップできるようになります。

VMwareエージェント（Windows）およびHyper-Vエージェント（Windows）をインストールする場合、Windowsエージェントもインストールすることをお勧めいたします。

Linuxの場合、Oracleエージェント、MySQL/MariaDBエージェント、Virtuozzoエージェントを使用するには、Linuxエージェント（64ビット）もインストールする必要があります。これらのエージェントは、Linuxエージェント（64-bit）のセットアップファイルにバンドルされています。

バックアップ対象	インストールするエージェント	インストール先
物理コンピュータ		
Windows OSの物理コンピュータ	Windowsエージェント	バックアップ対象のマシン。
Linux OSの物理コンピュータ	Linuxエージェント	
macOS を実行している物理マシン	エージェント for Mac	
データベース		
SQLデータベース	SQL エージェント	Microsoft SQL Serverを実行しているコンピュータ。
MySQL データベース	MySQL/MariaDB エージェント （Linuxエージェント（64-bit）のセットアップファイルにバンドル済み）	MySQL Serverを実行しているマシン
MariaDBデータベース	MySQL/MariaDB エージェント	MariaDB Serverを実行しているマシ

	（Linuxエージェント（64-bit）のセットアップファイルにバンドル済み）	ン
Exchangeデータベース	Exchangeエージェント	Microsoft Exchange Serverのメールボックスの役割を実行しているマシン。*
Oracle データベース	Oracle エージェント （Linuxの場合、Linuxエージェント（64-bit）のセットアップファイルにバンドル済み）	Oracleデータベースを実行しているマシン。
クラウドツークラウドワークロード		
Microsoft 365メールボックス （クラウドエージェントまたはローカルエージェント）	クラウドエージェント （インストールの必要なし）	この機能は、データセンターに配置されたクラウドエージェントで利用可能です。詳細については、"Microsoft 365クラウドエージェントを使用する"（593ページ）を参照してください。
	エージェント for Office 365	インターネットに接続されているWindowsマシン詳細については、"ローカルにインストールされたOffice 365エージェントの使用"（589ページ）を参照してください。
Microsoft 365 OneDriveファイルおよびSharePoint Onlineサイト	クラウドエージェント （インストールの必要なし）	この機能は、データセンターに配置されたクラウドエージェントで利用可能です。詳細

		については、"Microsoft 365クラウドエージェントを使用する"（593ページ）を参照してください。
Google Workspace Gmailメールボックス、Googleドライブのファイル、共有ドライブのファイル	クラウドエージェント （インストールの必要なし）	この機能は、データセンターに配置されたクラウドエージェントで利用可能です。詳細については、"Google Workspaceデータの保護"（625ページ）を参照してください。
Active Directory		
Active Directoryドメインサービスを実行しているコンピュータ	エージェント for Active Directory	ドメインコントローラ
仮想コンピュータ		
VMware ESXi仮想コンピュータ	エージェント for VMware（Windows）	vCenter Serverおよび仮想マシンのストレージに接続できるWindowsマシン。**
	エージェント for VMware（仮想アプライアンス）	ESXiホスト。
Hyper-V仮想コンピュータ	Hyper-Vエージェント	Hyper-Vホスト
Scale Computing HC3仮想マシン	Scale Computing HC3エージェント（仮想アプライアンス）	Scale Computing HC3ホスト。
Red Hat Virtualization仮想マシン（oVirtによる管理）	oVirtエージェント（仮想アプライアンス）	Red Hat Virtualizationホスト上。
Virtuozzo仮想マシンおよびコンテナ***	Virtuozzoエージェント	Virtuozzoホスト

	（Linuxエージェント（64-bit）のセットアップファイルにバンドル済み）	
Virtuozzo Hybrid Infrastructure仮想マシン	Virtuozzo Hybrid Infrastructureエージェント（仮想アプライアンス）	Virtuozzo Hybrid Infrastructureホスト上。
Amazon EC2でホストされている仮想コンピュータ	物理マシンと同様****	バックアップ対象のマシン。
Windows Azureでホストされている仮想コンピュータ		
Citrix XenServer 仮想コンピュータ		
Red Hat Virtualization (RHV/RHEV), not managed by oVirt		
カーネルベースの仮想マシン（KVM）は、oVirtにより管理されません		
Oracle仮想マシンは、oVirtにより管理されません		
Nutanix AHV仮想マシン		
Red Hat Virtualization (RHV/RHEV)は、oVirtにより管理されます	oVirtエージェント（仮想アプライアンス）	仮想化ホストの場合。
カーネルベースの仮想マシン（KVM）は、oVirtにより管理されます		
Oracle仮想マシンは、oVirtにより管理されます		
モバイル デバイス		
Androidを実行するモバイル デバイス	Android用モバイルアプリ	バックアップ対象のモバイル デバイス。
iOSを実行するモバイル デバイス	iOS用モバイルアプリ	

*インストールの過程で、Exchangeエージェントはマシンに十分な空き領域が存在するかどうかをチェックします。粒度復元の過程では、最も大きなExchangeデータベースの15パーセントに等しい空き領域が一時的に必要になります。

**ESXiでSAN 接続ストレージが使用されている場合は、このエージェントを同じSAN接続マシンにインストールします。エージェントは、ESXiホストやLANを経由せずにストレージから仮想コンピュータを直接バックアップします。詳細な指示については、"エージェント for VMware - LAN フリー バックアップ"（671ページ）を参照してください。

***Virtuozzo 7では、Ploopコンテナのみがサポートされています。仮想マシンはサポート対象外です。

****外部エージェントでバックアップされている場合、マシンは仮想マシンと見なされます。エージェントがゲスト システムでインストールされている場合、バックアップおよび復元操作は、物理コン

ピュータの場合と同じです。ただし、Cyber ProtectionがCPUID命令を使用して仮想マシンを識別できる場合は、その仮想マシンに仮想マシンのサービスクォータが割り当てられます。ダイレクトパススルー、またはCPUの製造元IDが表示されないようにする他のオプションを使用している場合、物理マシンのサービスクォータのみを割り当てることができます。

エージェントベースのバックアップとエージェントレスバックアップ

エージェントベースのバックアップでは、すべての保護されているマシンにプロテクションエージェントをインストールする必要があります。エージェントベースのバックアップは、すべての物理および仮想マシンでサポートされています。必要なエージェントの種類とインストール先については、"エージェント"（61ページ）を参照してください

エージェントレスバックアップは一部の仮想化プラットフォームでサポートされており、物理マシンでは利用できません。エージェントレスバックアップに必要なプロテクションエージェントは1つだけで、仮想化環境の専用マシンにインストールします。このエージェントでは環境内の他のすべての仮想マシンがバックアップされます。仮想環境プラットフォームごとのサポートされるバックアップの種類については、"サポートされる仮想環境プラットフォーム"（31ページ）を参照してください。

仮想環境プラットフォームによっては、仮想アプライアンスが利用できます。仮想アプライアンス（VA）は、プロテクションエージェントを含む事前設定された仮想マシンです。仮想アプライアンスは、.ovf、.ova、または.qcowなど、ハイパーバイザー固有の形式で利用可能です。

どのタイプのバックアップが必要ですか？

以下のような必要性がある場合には、エージェントベースのバックアップをお勧めします。

- ウイルスおよびマルウェア対策、パッチ管理、リモートデスクトップ接続など、追加の保護機能。これらの機能の詳細については、"オペレーティングシステムでサポートされる保護機能"（43ページ）を参照してください。
- テナントレベルで分離した仮想マシン。例えば、テナント内のユーザーが自分のバックアップのみにアクセスできるようにするためなど。
- ゲストオペレーティングシステムにリカバリできるファイルレベルのバックアップ。

以下のような必要性がある場合には、エージェントレスのバックアップをお勧めします。

- 機能バックアップのみで、追加の保護機能は不要。
- シンプルな管理: 単一のエージェントをインストールして構成するだけで、複数の仮想マシンをバックアップできる。
- リソースの使用量を最小限に抑える必要がある。単一の専用エージェントを利用することで、環境内の各仮想マシンに複数のエージェントをインストールするよりも、CPUとRAMの使用量を抑える。
- LANフリーバックアップなど、特定のバックアップ設定。この機能の詳細については、"エージェント for VMware - LAN フリー バックアップ"（671ページ）を参照してください。
- 設定のオーバーヘッドが少ない。専用エージェントで、ゲスト オペレーティング システムに関係なく、ハイパーバイザーレベルで仮想マシンをバックアップする。

エージェントのシステム要件

エージェント	インストールに必要なディスク領域
Windowsエージェント	1.2GB
Linuxエージェント	2GB
エージェント for Mac	1GB
SQLエージェントとWindowsエージェント	1.2GB
ExchangeエージェントとWindowsエージェント	1.3GB
データ漏洩防止エージェント	500MB
Microsoft 365エージェント	500MB
Active DirectoryエージェントとWindowsエージェント	2GB
VMwareエージェントとWindowsエージェント	1.5GB
Hyper-VエージェントとWindowsエージェント	1.5GB
VirtuozzoエージェントとLinuxエージェント	1GB
Virtuozzo Hybrid Infrastructureエージェント	700MB
OracleエージェントとWindowsエージェント	2.2GB
OracleエージェントとLinuxエージェント	2GB
MySQL/MariaDBエージェントとLinuxエージェント	2GB

バックアップ操作（バックアップの削除を含む）には、バックアップのサイズ1TBあたり約1GBのRAMが必要です。エージェントが処理するデータの量や種類により、メモリ消費量は増減する場合があります。

注意
サイズが非常に大きいバックアップセット（4TB以上）のバックアップを行う場合、RAMの使用量は増加する可能性があります。

x64システムの場合、ブータブルメディアによる処理と再起動によるディスク復元には、2GB以上のメモリが必要です。

第11世代のIntel CoreやAMD Ryzen 7などの最新プロセッサを搭載したワークロードでは、CETテクノロジーがサポートされており、これとの競合を回避するため、データ損失防止エージェントの一部の機

能が無効になっています。このようなCPUを搭載したシステムで、デバイスコントロールとAdvanced DLPの機能を利用できる環境を次の表に示します。

機能	デバイス制御	Advanced DLP
ローカルチャネル		
リムーバブルストレージ	使用不可	はい
暗号化リムーバブルストレージ	はい	使用不可
プリンター	使用不可	いいえ
リダイレクトされるマッピング済みドライブ	使用不可	はい
リダイレクトされるクリップボード	使用不可	いいえ
ネットワーク通信		
SMTP Eメール	使用不可	はい
Microsoft Outlook（MAPI）	使用不可	はい
IBM Notes	使用不可	いいえ
Webメール	使用不可	はい
インスタントメッセージ（ICQ）	使用不可	いいえ
インスタントメッセージ（Viber）	使用不可	いいえ
インスタントメッセージ（IRC、Jabber、Skype、Viber）	使用不可	はい
ファイル共有サービス	使用不可	はい
ソーシャルネットワーク	使用不可	はい
ローカルネットワークファイル共有（SMB）	使用不可	はい
Webアクセス（HTTP/HTTPS）	使用不可	はい
ファイル転送（FTP/FTPS）	使用不可	はい
データ転送の許可リスト		
デバイスタイプの許可リスト	使用不可	はい
ネットワーク通信の許可リスト	使用不可	はい
リモートホストの許可リスト	使用不可	はい
アプリケーションの許可リスト	使用不可	はい
周辺デバイス		
リムーバブルストレージ	はい	はい

暗号化リムーバブルストレージ	はい	はい
プリンター	いいえ	いいえ
MTP接続のモバイルデバイス	いいえ	いいえ
Bluetoothアダプタ	はい	はい
光学ドライブ	はい	はい
フロッピードライブ	はい	はい
Windowsクリップボード	いいえ	いいえ
スクリーンショットのキャプチャ	いいえ	いいえ
リダイレクトされるマッピング済みドライブ	はい	はい
リダイレクトされるクリップボード	いいえ	いいえ
Cyber Protectエージェントの自己防御機能		
一般エンドユーザーからの保護	はい	はい
ローカルシステム管理者からの保護	はい	はい

Linuxパッケージ

必要なモジュールを Linuxカーネルに追加するには、セットアッププログラムに次の Linuxパッケージが必要です。

- カーネルのヘッダーまたはソースを持つパッケージ。パッケージのバージョンは、カーネルのバージョンに一致している必要があります。
- GNU コンパイラ コレクション（GCC）コンパイラ システム（GCCはカーネルがコンパイルされたバージョンである必要があります）
- makeツール
- perlインタプリタ。
- 4.15以降で、CONFIG_UNWINDER_ORC=yで設定される、カーネルのビルドのための`libelf-dev`、`libelf-devel`、または`elfutils-libelf-devel`ライブラリ。Fedora 28など一部のディストリビューションでは、カーネルのヘッダーとは別にインストールする必要があります。

これらのパッケージの名前は、Linux ディストリビューションによって異なります。

Red Hat Enterprise Linux、CentOS、および Fedora では、通常、パッケージはセットアッププログラムによってインストールされます。その他のディストリビューションで、パッケージがインストールされていない場合や、必要なバージョンがインストールされていない場合は、パッケージをインストールする必要があります。

必要なパッケージが既にインストールされていることを確認

パッケージが既にインストールされていることを確認するには、次の手順を実施します。

1. カーネルのバージョンと必要な GCCバージョンを確認するには、次のコマンドを実行します。

   ```
   cat /proc/version
   ```

   このコマンドにより、次のような行が返されます。`Linux version 2.6.35.6`および`gcc version 4.5.1`
2. makeツールと GCC コンパイラがインストールされているかどうかを確認するには、次のコマンドを実行します。

   ```
   make -v
   gcc -v
   ```

   gccの場合、コマンドによって返されるバージョンが手順1の`gcc version`と同じであることを確認します。**make**については、コマンドが実行されることを確認します。
3. カーネルモジュールを作成するパッケージの適切なバージョンがインストールされているかどうかを確認します。
   - Red Hat Enterprise Linux、CentOS、および Fedora で次のコマンドを実行します。

     ```
     yum list installed | grep kernel-devel
     ```
   - Ubuntu の場合、次のコマンドを実行します。

     ```
     dpkg --get-selections | grep linux-headers
     dpkg --get-selections | grep linux-image
     ```

   どちらの場合でも、パッケージのバージョンが手順1の`Linux version`と同じであることを確認します。
4. 次のコマンドを実行して、perl インタプリタがインストールされているかどうか確認します。

   ```
   perl --version
   ```

   perl のバージョンに関する情報が表示された場合、インタプリタはインストールされています。
5. Red Hat Enterprise Linux、CentOS、およびFedoraでは、次のコマンドを実行して`elfutils-libelf-devel`がインストールされているかどうかを確認します。

   ```
   yum list installed | grep elfutils-libelf-devel
   ```

   ライブラリのバージョンに関する情報が表示される場合、ライブラリはインストールされています。

レポジトリからのパッケージのインストール

次の表では、さまざまな Linux ディストリビューションで必要なパッケージをインストールする方法について説明します。

Linuxディストリビューション	パッケージ名	インストール方法

Red Hat Enterprise Linux	**kernel-devel gcc make elfutils-libelf-devel**	セットアップ プログラムは、Red Hatのサブスクリプションを使用して、自動的にパッケージをダウンロードしてインストールします。
	perl	次のコマンドを実行します。 `yum install perl`
CentOS Fedora	**kernel-devel gcc make elfutils-libelf-devel**	セットアップ プログラムは、自動的にパッケージをダウンロードしてインストールします。
	perl	次のコマンドを実行します。 `yum install perl`

Ubuntu
Debian
	linux-headers linux-image gcc make perl	次のコマンドを実行します。
		`sudo apt-get update`
		`sudo apt-get install linux-headers-$(uname -r)`
		`sudo apt-get install linux-image-$(uname -r)`
		`sudo apt-get install gcc-<package version>`
		`sudo apt-get install make`
		`sudo apt-get install perl`

SUSE Linux
OpenSUSE
	kernel-source gcc make perl	`sudo zypper install kernel-source`
		`sudo zypper install gcc`
		`sudo zypper install make`
		`sudo zypper install perl`

パッケージはディストリビューションのレポジトリからダウンロードされ、インストールされます。

他の Linux ディストリビューションについては、必要なパッケージの正確な名前およびインストール方法に関してディストリビューションのドキュメントを参照してください。

手動のパッケージインストール

次の場合には、パッケージを**手動で**インストールする必要があります。

- コンピュータに Red Hatの有効なサブスクリプションまたはインターネット接続がない場合。
- プログラムの設定がカーネルのバージョンに対応する**kernel-devel**または**gcc**バージョンを見つけることができない場合。利用できる**kernel-devel**がご使用のカーネルより新しい場合は、カーネルをアップデートするか一致する**kernel-devel**バージョンを手動でインストールする必要があります。
- 必要なパッケージが既にローカル ネットワークにあるため、自動的な検索とダウンロードに時間をかけないようにする場合。

ローカル ネットワークまたは信頼されているサードパーティのウェブ サイトからパッケージを入手して、次のようにインストールします。

- Red Hat Enterprise Linux、CentOS、または Fedora で、ルートユーザーとして次のコマンドを実行します。

```
rpm -ivh PACKAGE_FILE1 PACKAGE_FILE2 PACKAGE_FILE3
```

- Ubuntu の場合は、次のコマンドを実行します。

```
sudo dpkg -i PACKAGE_FILE1 PACKAGE_FILE2 PACKAGE_FILE3
```

例:Fedora 14にパッケージを手動でインストールする

32 ビットコンピュータの Fedora 14 に必要なパッケージをインストールするには、次の手順に従います。

1. カーネルのバージョンと必要な GCC バージョンを確認するには、次のコマンドを実行します。

   ```
   cat /proc/version
   ```

   このコマンドの出力には、次の内容が含まれます。

   ```
   Linux version 2.6.35.6-45.fc14.i686
   gcc version 4.5.1
   ```

2. このカーネルのバージョンに対応する**kernel-devel**および**gcc**パッケージを取得します。

   ```
   kernel-devel-2.6.35.6-45.fc14.i686.rpm
   gcc-4.5.1-4.fc14.i686.rpm
   ```

3. Fedora 14用の**make**パッケージを取得します。

   ```
   make-3.82-3.fc14.i686
   ```

4. ルートユーザーとして次のコマンドを実行して、パッケージをインストールします。

   ```
   rpm -ivh kernel-devel-2.6.35.6-45.fc14.i686.rpm
   rpm -ivh gcc-4.5.1.fc14.i686.rpm
   rpm -ivh make-3.82-3.fc14.i686
   ```

これらすべてのパッケージは、1つのrpmコマンドで指定できます。インストールするこれらのパッケージの一部では、依存性を解決するために、追加パッケージのインストールが必要になることがあります。

プロキシサーバー設定の構成

保護エージェントはHTTP/HTTPSプロキシサーバー経由でデータを伝送できます。このサーバーは、スキャンやHTTPトラフィックによる介入なしで、HTTPトンネルを介して動作する必要があります。Man-in-the-middleプロキシはサポートされていません。

インストール中にエージェントはクラウドに自ら登録するため、エージェントのインストール中にまたはあらかじめ、プロキシサーバー設定を構成する必要があります。

Windows 用

[コントロールパネル] > **[インターネットオプション]** > **[接続]** でプロキシサーバーが構成されている場合、プログラムの設定はレジストリからプロキシサーバー設定を読み取り、これらを自動的に使用します。

以下のタスクを実行する場合は、この手順を使用します。

- エージェントのインストール前にプロキシ設定を行います。
- エージェントのインストール後にプロキシのアップデートを行います。

エージェントのインストール中にプロキシ設定構成するには、"Windowsでプロテクションエージェントをインストールする"（76ページ）を参照してください。

注意

この手順は、http-proxy.yamlファイルがマシンに存在しない場合にのみ有効です。マシンにhttp-proxy.yamlファイルが存在する場合、aakore.yamlファイルの設定より優先されるため、ファイルのプロキシ設定をアップデートする必要があります。

%programdata%\Acronis\Agent\var\aakore\http-proxy.yamlファイルは、Cyber Protectionモニタを使用してプロキシサーバー設定を構成するときに作成されます。詳細については、"Cyber Protectモニタのプロキシサーバー設定の構成"（302ページ）を参照してください。

http-proxy.yamlファイルを開くには、WindowsのAdministratorsグループのメンバーである必要があります。

プロキシ設定を構成するには

1. 新しいテキスト文書を作成し、メモ帳などのテキストエディタで開きます。
2. 次の行をコピーしてファイルに貼り付けます。

```
Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SOFTWARE\Acronis\Global\HttpProxy]
"Enabled"=dword:00000001
"Host"="proxy.company.com"
"Port"=dword:000001bb
```

```
"Login"="proxy_login"
"Password"="proxy_password"
```

3. proxy.company.com はご使用のプロキシサーバーホスト名/IPアドレスで置換し、000001bbはポート番号の16進値で置換します。たとえば、000001bbはポート443です。
4. プロキシサーバーで認証が必要な場合は、proxy_loginとproxy_passwordをプロキシサーバー資格情報と置き換えます。必要ない場合は、ファイルからこれらの行を削除します。
5. proxy.regとして文書を保存します。
6. ファイルを管理者として実行します。
7. Windowsレジストリを編集することを確認します。
8. このワークロードにエージェントがインストールされていない場合は、ここでインストールします。ワークロードにエージェントが既にインストールされている場合は、次の手順に進みます。
9. テキストエディタで%programdata%\Acronis\Agent\etc\aakore.yamlファイルを開きます。
   このファイルを開くには、WindowsのAdministratorsグループのメンバーである必要があります。
10. **env**セクションを探し（または作成し）、以下の行を追加します。

```
env:
    http-proxy: proxy_login:proxy_password@proxy_address:port
    https-proxy: proxy_login:proxy_password@proxy_address:port
```

11. proxy_loginとproxy_passwordをプロキシサーバー資格情報と置き換えます。また、proxy_address:portをプロキシサーバーのアドレスとポート番号に置き換えます。
12. **[スタート]** メニューで **[実行]** をクリックし、「**cmd**」と入力してから **[OK]** をクリックします。
13. 以下のコマンドを実行してaakoreサービスを再起動します。

```
net stop aakore
net start aakore
```

14. 以下のコマンドを実行してエージェントを再起動します。

```
net stop mms
net start mms
```

macOS の場合

以下のタスクを実行する場合は、この手順を使用します。

- エージェントのインストール前にプロキシ設定を行います。
- エージェントのインストール後にプロキシのアップデートを行います。

エージェントのインストール中にプロキシ設定構成するには、"macOSでプロテクションエージェントをインストールする"（81ページ）を参照してください。

プロキシ設定を構成するには

1. /Library/Application Support/Acronis/Registry/Global.configファイルを作成し、Text Editなどのテキストエディタで開きます。

2. 次の行をコピーしてファイルに貼り付けます。

```
<?xml version="1.0" ?>
<registry name="Global">
    <key name="HttpProxy">
        <value name="Enabled" type="Tdword">"1"</value>
        <value name="Host" type="TString">"proxy.company.com"</value>
        <value name="Port" type="Tdword">"443"</value>
        <value name="Login" type="TString">"proxy_login"</value>
        <value name="Password" type="TString">"proxy_password"</value>
    </key>
</registry>
```

3. proxy.company.com はご使用のプロキシサーバーホスト名/IPアドレスで置換し、443はポート番号の10進値で置換します。
4. プロキシサーバーで認証が必要な場合は、proxy_loginとproxy_passwordをプロキシサーバー資格情報と置き換えます。必要ない場合は、ファイルからこれらの行を削除します。
5. ファイルを保存します。
6. このワークロードにエージェントがインストールされていない場合は、ここでインストールします。ワークロードにエージェントが既にインストールされている場合は、次の手順に進みます。
7. テキストエディタで/Library/Application Support/Acronis/Agent/etc/aakore.yamlファイルを開きます。
8. **env**セクションを探し（または作成し）、以下の行を追加します。

```
env:
    http-proxy: proxy_login:proxy_password@proxy_address:port
    https-proxy: proxy_login:proxy_password@proxy_address:port
```

9. proxy_loginとproxy_passwordをプロキシサーバー資格情報と置き換えます。また、proxy_address:portをプロキシサーバーのアドレスとポート番号に置き換えます。
10. **[アプリケーション]** > **[ユーティリティ]** > **[ターミナル]** に移動します。
11. 以下のコマンドを実行してaakoreサービスを再起動します。

```
sudo launchctl stop aakore
sudo launchctl start aakore
```

12. 以下のコマンドを実行してエージェントを再起動します。

```
sudo launchctl stop acronis_mms
sudo launchctl start acronis_mms
```

Linux用

--http-proxy-host=ADDRESS --http-proxy-port=PORT --http-proxy-login=LOGIN --http-proxy-password=PASSWORDパラメータを使用してインストールファイルを実行します。プロテクションエージェントのインストール後にプロキシ設定をアップデートするには、以下の手順を使用します。

プロキシ設定を構成するには

1. テキストエディタで/etc/Acronis/Global.configファイルを開きます。
2. 次のいずれかを実行します。
   - エージェントインストール中にプロキシ設定を指定した場合は、次のセクションを見つけます。

     ```
     <key name="HttpProxy">
         <value name="Enabled" type="Tdword">"1"</value>
         <value name="Host" type="TString">"ADDRESS"</value>
         <value name="Port" type="Tdword">"PORT"</value>
         <value name="Login" type="TString">"LOGIN"</value>
         <value name="Password" type="TString">"PASSWORD"</value>
     </key>
     ```

   - エージェントのインストール時にプロキシ設定が指定されていない場合は、以下の行をコピーし、<registry name="Global">...</registry>タグの間のファイルに貼り付けます。

     ```
     <key name="HttpProxy">
         <value name="Enabled" type="Tdword">"1"</value>
         <value name="Host" type="TString">"ADDRESS"</value>
         <value name="Port" type="Tdword">"PORT"</value>
         <value name="Login" type="TString">"LOGIN"</value>
         <value name="Password" type="TString">"PASSWORD"</value>
     </key>
     ```

3. ADDRESSは新しいプロキシサーバーホスト名/IPアドレスで置換し、PORTはポート番号の10進値で置換します。
4. プロキシサーバーで認証が必要な場合は、LOGINとPASSWORDをプロキシサーバー資格情報と置き換えます。必要ない場合は、ファイルからこれらの行を削除します。
5. ファイルを保存します。
6. /opt/acronis/etc/aakore.yamlファイルをテキストエディタで開きます。
7. **env**セクションを探し（または作成し）、以下の行を追加します。

   ```
   env:
       http-proxy: proxy_login:proxy_password@proxy_address:port
       https-proxy: proxy_login:proxy_password@proxy_address:port
   ```

8. proxy_loginとproxy_passwordをプロキシサーバー資格情報と置き換えます。また、proxy_address:portをプロキシサーバーのアドレスとポート番号に置き換えます。
9. 以下のコマンドを実行してaakoreサービスを再起動します。

   ```
   sudo service aakore restart
   ```

10. 任意のディレクトリでコマンドを実行してエージェントを再起動します。

    ```
    sudo service acronis_mms restart
    ```

ブータブルメディアの場合

ブータブルメディアで作業する場合、プロキシサーバーを介してクラウドストレージにアクセスしなければならない場合があります。プロキシサーバーを構成するには、**[ツール]** > **[プロキシサーバー]** をクリックして、プロキシサーバーホスト名/IPアドレス、ポート、および資格情報を構成します。

プロテクションエージェントをインストールする

「サポート対象のオペレーティングシステムと環境」に挙げられているいずれかのオペレーティングシステムを実行するマシンにエージェントをインストールできます。Cyber Protect機能をサポートしているオペレーティングシステムについては、「Cyber Protect機能がサポートされているオペレーティングシステム」を参照してください。

プロテクションエージェントをダウンロードする

エージェントをインストールする前に、Cyber Protectコンソールからエージェントのインストールファイルをダウンロードする必要があります。

保護対象のワークロードを追加している間にエージェントをダウンロードするには

1. Cyber Protectコンソールで、**[デバイス]** > **[すべてのデバイス]** に進みます。
2. 右上の **[デバイスの追加]** をクリックします。
3. **[デバイスの追加]** パネルで、**[リリースチャネル]** ドロップダウンメニューから、エージェントのバージョンを選択します。
   - **前回のリリース** - 以前にリリースされたバージョンのエージェントをダウンロードします。
   - **最新** - 利用可能な最新バージョンのエージェントをダウンロードします。
4. 追加するワークロードのオペレーティングシステムに対応するエージェントを選択します。
   [名前を付けて保存] ダイアログが開きます。
5. （Apple Siliconプロセッサーを搭載したMac（Apple M1など）のみ）**[キャンセル]** をクリックします。開いた **[Macの追加]** パネルで、**ARMインストーラのダウンロード**リンクをクリックします。
6. エージェントのインストールファイルの保存ロケーションを選択して、［**保存**］をクリックします。

エージェントをダウンロードして後で使用するには

1. Cyber Protectコンソールの右上隅で、**ユーザー**アイコンをクリックします。
2. **[ダウンロード]** をクリックします。
3. **[ダウンロード]** ダイアログで、**[リリースチャネル]** ドロップダウンメニューから、エージェントのバージョンを選択します。
   - **前回のリリース** - 以前にリリースされたバージョンのエージェントをダウンロードします。
   - **最新** - 利用可能な最新バージョンのエージェントをダウンロードします。
4. 利用可能なインストーラのリストをスクロールして、必要なエージェントインストーラを探します。その後、その行の最後にあるダウンロードアイコンをクリックします。
   [名前を付けて保存] ダイアログが開きます。
5. エージェントのインストールファイルの保存ロケーションを選択して、［**保存**］をクリックします。

Windowsでプロテクションエージェントをインストールする

前提条件

保護計画の対象となるワークロードに必要なエージェントをダウンロードします。"プロテクションエージェントをダウンロードする"（76ページ）をご覧ください。

Windowsエージェントをインストールするには

1. コンピュータがインターネットに接続されていることを確認します。
2. 管理者権限でログオンし、インストーラを起動します。
3. （オプション）[**インストール設定のカスタマイズ**] をクリックし、以下を希望する場合は適切な変更を加えます。
   - インストールするコンポーネントを変更するには（例えば、Cyber Protection Monitorやコマンドラインツールのインストールを無効にしたり、マルウェア対策保護やURLフィルタリング用エージェントをインストールしたりするには）。

     注意
     Windowsマシンで、マルウェア対策保護機能を利用するには、マルウェア対策保護エージェントのインストールが必要であり、URLフィルタリング機能を利用するには、URLフィルタリングエージェントのインストールが必要です。これらのエージェントは、保護計画で**ウイルスおよびマルウェア対策保護**や**URLフィルタリング**のモジュールが有効になっている場合、保護対象のワークロードに自動的にインストールされます。

   - Cyber Protectionサービスでワークロード登録のメソッドを変更するには。[**サービスコンソールを使用します**]（デフォルト）から [**資格情報を使用します**] や [**登録トークンを使用します**] に切り替えることが可能です。
   - インストールパスを変更する場合。
   - エージェントサービスを実行するユーザーアカウントを変更する場合:詳細については、"Windowsマシンのログオンアカウントの変更"（84ページ）を参照してください。
   - プロキシサーバーのホスト名/IPアドレス、ポート、および資格情報を確認または変更する場合。Windowsでプロキシサーバーが有効な場合は、自動的に検出、使用されます。
4. [**インストール**] をクリックします。
5. （VMwareエージェントをインストールする場合のみ）仮想マシンをバックアップおよびリカバリする、vCenter ServerまたはスタンドアロンESXiホストのアドレスとアクセス認証を指定して、[**完了**] をクリックします。

   管理者ロールを割り当てられた既存のアカウントを使用するのではなく、vCenter ServerまたはESXiホストにアクセスするための専用アカウントを使用することをお勧めします。専用アカウントに必要な権限の詳細については、"VMware エージェント - 必要な権限"（681ページ）を参照してください。
6. （ドメインコントローラでインストールする場合のみ）エージェントサービスを実行するユーザーアカウントを指定して、[**完了**] をクリックします。これは、セキュリティ上の理由で、プログラムの設定はドメインコントローラ上で新しいアカウントを自動作成できないためです。

注意
このユーザーアカウントには、**サービスとしてログオン**の権限を指定する必要があります。ドメインコントローラーのマシン上にプロファイルフォルダを作成するには、該当のマシンでこのアカウントが既に使用されている必要があります。

読み取り専用ドメインコントローラーに対するエージェントインストールの詳細については、こちらのナレッジベースの記事を参照してください。

7. 手順3でデフォルトの登録方法 **[サービスコンソールを使用します]** を保持した場合は、登録画面が表示されるのを待ってから、次の手順に進みます。それ以外の場合、追加の操作は不要です。
8. 次のいずれかを実行します。
   - 企業管理者アカウントでログインする場合、自分の会社のワークロードを登録します。
     a. **[ワークロードを登録]** をクリックします。
     b. 開いたブラウザウィンドウで、Cyber Protectコンソールにサインインしてから、登録の詳細を確認します。
     c. **[アカウントの登録]**リストで、ワークロードを登録するユーザーアカウントを選択します。
     d. **[コードを確認]** をクリックしてから、**[登録を確認]** をクリックします。
   - パートナー管理者アカウントでログインする場合、カスタマーのワークロードを登録します。
     a. **[ワークロードを登録]** をクリックします。
     b. 開いたブラウザウィンドウで、Cyber Protectコンソールにサインインしてから、登録の詳細を確認します。
     c. **[アカウントの登録]**リストで、ワークロードを登録するカスタマーのユーザーアカウントを選択します。
     d. **[コードを確認]** をクリックしてから、**[登録を確認]** をクリックします。
   - **[登録情報を表示]** をクリックします。セットアッププログラムには登録リンクと登録コードが表示されます。現在のマシンでワークロードの登録を完了できない場合は、登録リンクとコードをコピーし、別のマシンで登録の手順を実行してください。この場合は、登録フォームに登録コードを入力する必要があります。登録コードの有効期限は 1 時間です。
     または、**[すべてのデバイス]** > **[追加]** をクリックし、下にスクロールして **[コードによる登録]** を表示し、**[登録]** をクリックして、登録フォームにアクセスできます。

     注意
     登録を確認するまで、プログラムの設定を終了しないでください。登録を再開するには、プログラムの設定を再開して、インストール手順を繰り返す必要があります。

     その結果ワークロードは、Cyber Protectコンソールへのログインに使用されたアカウントに割り当てられます。
   - コマンドラインを使用してワークロードを手動で登録してください。その方法については、「"ワークロードの手動登録と登録解除"（116ページ）」を参照してください
9. （コンプライアンスモードを使用しているテナントのアカウントにエージェントが登録されている場合）暗号化パスワードを設定してください。

Linuxでプロテクションエージェントをインストールする

インストールする前に

- 保護計画の対象となるマシンに必要なエージェントをダウンロードします。["プロテクションエージェントをダウンロードする"（76ページ）]をご覧ください。
- 必要なLinuxパッケージがコンピュータにインストールされていることを確認します。
- SUSE Linuxにエージェントをインストールする場合、必ずsudoの代わりにsu -を使用してください。そうでない場合、Cyber Protectコンソールからエージェントを登録しようとすると、以下のエラーが発生します。**Webブラウザの起動に失敗しました。表示できません。**
  SUSEなど一部のLinuxディストリビューションでは、sudoを使用する際にDISPLAY変数が渡されず、インストーラからグラフィカル ユーザーインターフェース（GUI）経由でブラウザを開くことができません。

インストール

Linuxエージェントをインストールするには、少なくとも2GBの空きディスク領域が必要です。

Linuxエージェントをインストールする

1. コンピュータがインターネットに接続されていることを確認します。
2. ルートユーザーとして、インストールファイルが配置されているディレクトリに移動し、ファイルを実行可能な状態にしてから実行します。

   ```
   chmod +x <installation file name>
   ```

   ```
   ./<installation file name>
   ```

   ネットワーク内でプロキシサーバが有効な場合、インストールファイルを実行するときに、サーバーホスト名/IPアドレスとポートを以下の形式で指定します。 `--http-proxy-host=ADDRESS --http-proxy-port=PORT --http-proxy-login=LOGIN --http-proxy-password=PASSWORD`。
   Cyber Protectionサービスにマシンを登録するデフォルトの方法を変更する場合は、次のいずれかのパラメータを使用してインストールファイルを実行します。
   - `--register-with-credentials`: インストール時にユーザー名とパスワードを確認する場合
   - `--token=STRING`: 登録トークンを使用する場合
   - `--skip-registration`: 登録をスキップする場合
3. インストールするエージェントのチェック ボックスを選択します。次のエージェントを使用できます。
   - Linuxエージェント
   - Virtuozzoエージェント
   - Oracle エージェント
   - MySQL/MariaDBエージェント

Virtuozzoエージェント、Oracleエージェント、およびMySQL/MariaDBエージェントの場合は、Linuxエージェント （64ビット）もインストールする必要があります。

4. 手順 2 でデフォルトの登録方法を保持した場合は、次の手順に進みます。それ以外の場合は、Cyber Protectionサービスのユーザー名とパスワードを入力するか、トークンでマシンが登録されるまで待ちます。
5. 次のいずれかを実行します。
   - 企業管理者アカウントでログインする場合、自分の会社のワークロードを登録します。
     a. **[ワークロードを登録]** をクリックします。
     b. 開いたブラウザウィンドウで、Cyber Protectコンソールにサインインしてから、登録の詳細を確認します。
     c. **[アカウントの登録]**リストで、ワークロードを登録するユーザーアカウントを選択します。
     d. **[コードを確認]** をクリックしてから、**[登録を確認]** をクリックします。
   - パートナー管理者アカウントでログインする場合、カスタマーのワークロードを登録します。
     a. **[ワークロードを登録]** をクリックします。
     b. 開いたブラウザウィンドウで、Cyber Protectコンソールにサインインしてから、登録の詳細を確認します。
     c. **[アカウントの登録]**リストで、ワークロードを登録するカスタマーのユーザーアカウントを選択します。
     d. **[コードを確認]** をクリックしてから、**[登録を確認]** をクリックします。
   - **[登録情報を表示]** をクリックします。セットアッププログラムには登録リンクと登録コードが表示されます。現在のマシンでワークロードの登録を完了できない場合は、登録リンクとコードをコピーし、別のマシンで登録の手順を実行してください。この場合は、登録フォームに登録コードを入力する必要があります。登録コードの有効期限は 1 時間です。

     または、**[すべてのデバイス]** > **[追加]** をクリックし、下にスクロールして **[コードによる登録]** を表示し、**[登録]** をクリックして、登録フォームにアクセスできます。

     注意
     登録を確認するまで、プログラムの設定を終了しないでください。登録を再開するには、プログラムの設定を再開して、インストール手順を繰り返す必要があります。

     その結果ワークロードは、Cyber Protectコンソールへのログインに使用されたアカウントに割り当てられます。
   - コマンドラインを使用してワークロードを手動で登録してください。その方法については、「"ワークロードの手動登録と登録解除"（116ページ）」を参照してください
6. （コンプライアンスモードを使用しているテナントのアカウントにエージェントが登録されている場合）暗号化パスワードを設定してください。
7. UEFIセキュアブートがマシンで有効になっている場合、インストールの後にシステムを再起動するように促されます。使用するパスワード（root ユーザーまたは「Acronis 」のいずれか）を確実に覚えておいてください。

注意
インストール時には、カーネルモジュールの署名に使用する新しいキーが生成されます。マシンを再起動して、この新しいキーをマシンオーナーキー（MOK）リストに登録する必要があります。新しいキーを登録しないと、現在のエージェントを操作できません。エージェントのインストール後にUEFIセキュアブートを有効にした場合は、エージェントを再インストールする必要があります。

8. インストールの完了後、次のいずれかを実行します。
   - 前の手順でシステムの再起動をするよう促された場合、**[再起動]** をクリックします。
     システム再起動中に、MOK（マシン所有者キー）の管理を選択し、**[MOK を登録]** を選択し、前の手順で推奨されたパスワードを使用してキーを登録します。
   - それ以外の場合は **[終了]** をクリックします。

トラブルシューティングに関する情報は、`/usr/lib/Acronis/BackupAndRecovery/HOWTO.INSTALL`ファイルを参照してください。

macOSでプロテクションエージェントをインストールする

前提条件

保護計画の対象となるワークロードに必要なエージェントをダウンロードします。"プロテクションエージェントをダウンロードする"（76ページ）をご覧ください。

Macエージェント（x64またはARM64）をインストールするには

1. コンピュータがインターネットに接続されていることを確認します。
2. インストールファイル（.dmg）をダブルクリックします。
3. インストールディスクイメージがオペレーションシステムにマウントされるのを待ちます。
4. **[インストール]** をダブルクリックします。
5. プロキシサーバーがネットワークで有効になっている場合は、メニューバーの **[保護エージェント]** をクリックし、**[プロキシサーバー設定]** をクリックして、プロキシサーバーのホスト名/IPアドレス、ポート、資格情報を指定します。
6. 資格情報を求められた場合は、管理者の資格情報を入力します。
7. **[続行]** をクリックします。
8. 登録画面が表示されるまで待ちます。
9. 次のいずれかを実行します。
   - 企業管理者アカウントでログインする場合、自分の会社のワークロードを登録します。
     a. **[ワークロードを登録]** をクリックします。
     b. 開いたブラウザウィンドウで、Cyber Protectコンソールにサインインしてから、登録の詳細を確認します。
     c. **[アカウントの登録]**リストで、ワークロードを登録するユーザーアカウントを選択します。
     d. **[コードを確認]** をクリックしてから、**[登録を確認]** をクリックします。

- パートナー管理者アカウントでログインする場合、カスタマーのワークロードを登録します。
  a. **[ワークロードを登録]** をクリックします。
  b. 開いたブラウザウィンドウで、Cyber Protectコンソールにサインインしてから、登録の詳細を確認します。
  c. **[アカウントの登録]**リストで、ワークロードを登録するカスタマーのユーザーアカウントを選択します。
  d. **[コードを確認]** をクリックしてから、**[登録を確認]** をクリックします。
- **[登録情報を表示]** をクリックします。セットアッププログラムには登録リンクと登録コードが表示されます。現在のマシンでワークロードの登録を完了できない場合は、登録リンクとコードをコピーし、別のマシンで登録の手順を実行してください。この場合は、登録フォームに登録コードを入力する必要があります。登録コードの有効期限は 1 時間です。
  または、**[すべてのデバイス]** > **[追加]** をクリックし、下にスクロールして **[コードによる登録]** を表示し、**[登録]** をクリックして、登録フォームにアクセスできます。

  注意
  登録を確認するまで、プログラムの設定を終了しないでください。登録を再開するには、プログラムの設定を再開して、インストール手順を繰り返す必要があります。

  その結果ワークロードは、Cyber Protectコンソールへのログインに使用されたアカウントに割り当てられます。
- コマンドラインを使用してワークロードを手動で登録してください。その方法については、「"ワークロードの手動登録と登録解除"（116ページ）」を参照してください

10. （コンプライアンスモードを使用しているテナントのアカウントにエージェントが登録されている場合）暗号化パスワードを設定してください。
11. macOSのバージョンがMojave10.14.x以降の場合は、保護エージェントにフルディスクアクセスを付与してバックアップ操作を有効にします。
    詳細については、「サイバープロテクションエージェントに対する'Full Disk Access'権限の付与（64657）」を参照してください。
12. リモートデスクトップ機能を使用するには、接続エージェントに必要なシステム許可を付与します。詳細については、"接続エージェントに必要なシステム許可を付与する"（82ページ）を参照してください。

接続エージェントに必要なシステム許可を付与する

macOSワークロードでリモートデスクトップのすべての機能を有効にするには、フルディスクアクセスの許可に加えて、接続エージェントに次の許可を付与する必要があります。

- 画面収録 - NEARを介したmacOSワークロードの画面収録を有効にします。この許可が付与されるまで、すべてのリモート制御接続は拒否されます。
- アクセシビリティ - NEARを介した制御モードでのリモート接続を可能にします
- マイク - NEARを介したリモートのmacOSワークロードからローカルワークロードへのサウンドリダイレクトを可能にします。サウンドリダイレクト機能を有効にするには、ワークロードにサウンドキャプチャドライバがインストールされている必要があります。詳細については、"リモート音声の

リダイレクト"（963ページ）を参照してください。

- 自動化 - ごみ箱を空にする操作を有効にします

macOSワークロード上でエージェントを起動すると、エージェントにこれらの許可が付与されているかどうかが確認され、必要に応じて許可を求められます。

画面収録の許可を付与するには

1. Cyber Protectエージェントの、**[必要なシステム権限を付与する]** ダイアログで、**[システム許可を設定]** をクリックします。
2. **[システム許可]** ダイアログで、**[画面収録の許可を要求]** をクリックします。
3. **[システム環境設定を開く]** をクリックします。
4. **接続エージェント**を選択します。

リモートでワークロードにアクセスしようとしたときにエージェントに許可が付与されていない場合、[画面収録の許可を要求] ダイアログが表示されます。ダイアログに応答できるのは、ローカルユーザーだけです。

アクセシビリティの許可を付与するには

1. Cyber Protectエージェントの、**[必要なシステム権限を付与する]** ダイアログで、**[システム許可を設定]** をクリックします。
2. **[システム許可]** ダイアログで、**[アクセシビリティの許可を要求]** をクリックします。
3. **[システム環境設定を開く]** をクリックします。
4. ウィンドウの左下にあるロックアイコンをクリックして、ロック解除の状態に変更します。変更を行うには、管理者パスワードの入力が必要です。
5. **接続エージェント**を選択します。

マイクの許可を付与するには

1. 接続エージェントの、**[必要なシステム許可を付与する]** ダイアログで、**[システム許可を設定]** をクリックします。
2. **[システム許可]** ダイアログで、**[マイクの許可を要求]** をクリックします。
3. **[OK]** をクリックします。

注意
また、エージェントに付与された許可でワークロードの音声をリダイレクトしたい場合、macOSワークロードにサウンドキャプチャドライバをインストールする必要があります。詳細については、"リモート音声のリダイレクト"（963ページ）を参照してください。

自動化の許可を付与するには

1. 接続エージェントの、**[必要なシステム許可を付与する]** ダイアログで、**[システム許可を設定]** をクリックします。
2. **[システム許可]** ダイアログで、**[自動化の許可を要求]** をクリックします。

Windowsマシンのログオンアカウントの変更

[コンポーネントの選択] 画面で、**[エージェントサービスのログオンアカウント]** を指定してサービスが実行されるアカウントを決定します。次のいずれかを選択できます。

- **サービスユーザーアカウントを使用する**（エージェントサービスのデフォルト）
  サービスユーザーアカウントは、サービスの実行に使用される Windows のシステムアカウントです。この設定の利点は、ドメインのセキュリティポリシーがそれらのアカウントのユーザー権限に影響を及ぼさないことです。デフォルトでは、エージェントは**ローカルシステム**のアカウントで実行されます。
- **新しいアカウントを作成する**
  エージェントのアカウント名は「Agent User」になります。
- **次のアカウントを使用する**
  ドメインコントローラー上にエージェントをインストールする場合は、エージェントに既存のアカウント（または同じアカウント）を指定するようシステムから求められます。セキュリティ上の理由で、システムはドメインコントローラー上に新しいアカウントを自動作成しません。
  ドメインコントローラー上でセットアッププログラムを実行する際に指定するユーザーアカウントには、**サービスとしてログオン**する権限を付与する必要があります。ドメインコントローラーのマシン上にプロファイルフォルダを作成するには、該当のマシンでこのアカウントが既に使用されている必要があります。
  読み取り専用ドメインコントローラーに対するエージェントインストールの詳細については、こちらのナレッジベースの記事を参照してください。

[新しいアカウントを作成する] または **[次のアカウントを使用する]** のオプションを選択する場合は、ドメインのセキュリティポリシーが、関連するアカウントの権限に影響を及ぼさないようにしてください。インストール中に割り当てられたユーザー権限がアカウントからなくなると、コンポーネントが不適切な動作をする、またはまったく動作しなくなる場合があります。

ログオンアカウントで必要な権限

保護エージェントは、WindowsマシンのManaged Machine Service（MMS）として稼働します。エージェントを実行するアカウントは、エージェントを正しく実行するのに必要な権限を持っていなければなりません。それで、MMSユーザーに以下の権限を割り当てる必要があります。

1. **Backup Operators**グループと**Administrators**グループに追加します。ドメインコントローラーでは、**Domain Admins**グループにユーザーを追加する必要があります。
2. **フルコントロール**を`%PROGRAMDATA%\Acronis`フォルダ（Windows XPおよびServer 2003では`%ALLUSERSPROFILE%\Application Data\Acronis`）とそのサブフォルダすべてに許可します。
3. 次のキーにある特定のレジストリキーに対して **[フルコントロール]** を許可します。`HKEY_LOCAL_MACHINE\SOFTWARE\Acronis`。
4. 以下のユーザー権限を割り当てます。
   - サービスとしてログオン
   - プロセスのメモリクォータの調整

- プロセスレベルトークンの置き換え
- ファームウェアの環境値の修正

ユーザー権限を割り当てる方法

ユーザー権限を割り当てるには、以下の手順を実行します（この例では **[サービスとしてログオン]** ユーザー権限を使用していますが、他のユーザー権限の場合も手順は同じです）。

1. 管理権限を持つアカウントを使用してコンピューターにログオンします。
2. **[コントロールパネル]** から **[管理ツール]** を開くか、Win+Rを押してから**control admintools**と入力してEnterを押して、**[ローカルセキュリティポリシー]** を開きます。
3. **[ローカルポリシー]** を展開し、**[ユーザー権限の割り当て]** をクリックします。
4. 右側のペインで **[サービスとしてログオン]** を右クリックして、**[プロパティ]** を選択します。
5. 新しいユーザーを追加するために、**[ユーザーまたはグループの追加]** ボタンをクリックします。
6. **[ユーザー、コンピューター、サービスアカウントまたはグループの選択]** ウィンドウで、対象のユーザーを見つけて入力し、**[OK]** をクリックします。
7. **[サービスとしてログオンのプロパティ]** で **[OK]** をクリックし、変更内容を保存します。

重要
[サービスとしてログオン] ユーザー権限に追加したユーザーが **[ローカルセキュリティポリシー]** の **[サービスとしてログオンを拒否する]** のリストに含まれていないことを確認してください。

インストール完了後、手動でログオンアカウントを変更しないことをお勧めします。

コンポーネントの動的なインストールとアンインストール

エージェントバージョン15.0.26986（2021年5月リリース）以降で保護されているWindowsワークロードでは、以下のコンポーネントが動的に、つまり保護計画で必要とされるときにのみインストールされます。

- URLフィルタリング用エージェント—URLフィルタリング機能の動作に必要です。
- マルウェア対策保護エージェント - マルウェア対策保護機能を動作させるために必要です。
- データ損失防止エージェント - デバイス制御機能の動作に必要です。

デフォルトでは、これらのコンポーネントはインストールされません。以下のモジュールが有効になっている計画でワークロードが保護されるようになると、それぞれのコンポーネントが自動的にインストールされます。

- ウイルスおよびマルウェア対策保護
- URLフィルタ処理
- デバイス制御

同様に、マルウェア対策保護、URLフィルタリング、デバイス制御機能を必要とする保護計画が存在しなくなった場合は、それぞれのコンポーネントが自動的にアンインストールされます。

コンポーネントの動的なインストールまたはアンインストールは、保護計画を変更してから最大で10分を要します。ただし、以下の処理が実行中の場合、その処理が終了した後に動的インストールまたはアンインストールが開始されます。

- バックアップ
- 復元
- バックアップのレプリケーション
- 仮想マシンへのレプリケーション
- レプリカのテスト
- バックアップから仮想マシンを実行する（ファイナライズを含む）
- ディザスタリカバリフェールオーバー
- ディザスタリカバリフェールバック
- スクリプトの実行（サイバースクリプト機能の場合）
- パッチのインストール
- ESXi構成バックアップ

無人インストールまたはインストール解除

Windows での無人インストールまたはインストール解除

Windowsでは、以下の方法で無人インストールやインストール解除を行うことができます。

- セットアッププログラムのEXEファイルを使用し、コマンドラインでインストールパラメータを指定します。
- セットアッププログラムから展開したMSIファイルを使用し、以下のいずれかの方法でインストールパラメータを指定します。
  - MSTファイルで
  - コマンドラインで直接

EXEファイルによる無人インストールとインストール解除

このタイプの無人インストールでは、セットアッププログラムをダウンロードし、必要なインストールパラメータを指定してコマンドラインから起動します。使用できるパラメータについては、"無人インストール用パラメータ（EXE）"（89ページ）を参照してください。

事前にインストールパッケージ、MSI、MSTファイルを展開する必要はありません。

エージェントとコンポーネント（EXE）のインストールとアンインストール

EXEファイルを使用して無人インストールを実行するには、セットアッププログラムを実行し、コマンドラインでインストールパラメータを指定します。

セットアッププログラムをダウンロードするには、Cyber Protectコンソールで、右上にあるアカウントアイコンをクリックしてから、**[ダウンロード]** をクリックします。ダウンロードリンクは、**[デバイスの追加]** ペインにもあります。

エージェントとコンポーネントをインストールするには

1. 管理者としてコマンドラインインターフェイスを起動し、セットアッププログラムのEXEファイルに移動します。
2. セットアッププログラムを起動し、インストールパラメータを指定するには、以下のコマンドを実行します：

   ```
   <file path>/<EXE file><PARAMETER 1>=<value 1> ... <PARAMETER N>=<value n>
   ```

   パラメータを区切るにはスペースを使用し、パラメータの値を区切るにはカンマ（スペースなし）を使用します。例:

   ```
   C:\Users\Administrator\Downloads\AgentForWindows_web.exe --add-
   components=agentForWindows,agentForSql,commandLine --install-dir="C:\Program
   Files\BackupClient" --reg-address=https://eu2-cloud.company.com --reg-token=34F6-
   8C39-4A5C --quiet
   ```

   利用可能なパラメータとその値を確認するには、"無人インストール用パラメータ（EXE）"（89ページ）を参照してください。

例

- Windowsエージェント、マルウェア対策エージェント、URLフィルタリング用エージェント、コマンドラインツール、Cyber Protect Monitorをインストールする。 ユーザー名とパスワードを使用してCyber Protectionサービスにワークロードを登録する操作。

  ```
  C:\Users\Administrator\Downloads\AgentForWindows_web.exe --add-
  components=agentForWindows,agentForAmp,commandLine,trayMonitor --install-
  dir="C:\Program Files\BackupClient" --agent-account=system --reg-
  address=https://cloud.company.com --reg-login=johndoe --reg-password=johnspassword
  ```

- Windowsエージェント、コマンドラインツール、Cyber Protect Monitorのインストール。Windowsでエージェントサービスの新しいログオンアカウントを作成する操作。トークンを使用してCyber Protectionサービスにワークロードを登録する操作。

  ```
  C:\Users\Administrator\Downloads\AgentForWindows_web.exe --add-
  components=agentForWindows,commandLine,trayMonitor --install-dir="C:\Program
  Files\BackupClient" --agent-account=new --reg-address=https://eu2-cloud.company.com -
  -reg-token=34F6-8C39-4A5C
  ```

- Windowsエージェント、コマンドラインツール、Oracleエージェント、Cyber Protect Monitorのインストール。ユーザー名とパスワードを使用してCyber Protectionサービスにマシンを登録する操作。

  ```
  C:\Users\Administrator\Downloads\AgentForWindows_web.exe --add-
  components=agentForWindows,commandLine,agentForOracle,trayMonitor --install-
  dir="C:\Program Files\BackupClient" --language=en --agent-account=system --reg-
  address=https://cloud.company.com --reg-login=johndoe --reg-password=johnspassword
  ```

- Windowsエージェント、コマンドラインツール、Cyber Protect Monitorのインストール。ユーザーインターフェイスの言語をドイツ語に設定。トークンを使用してCyber Protectionサービスにマシンを登録する操作。HTTPプロキシを設定する操作。

```
C:\Users\Administrator\Downloads\AgentForWindows_web.exe --add-
components=agentForWindows,commandLine,agentForOracle,trayMonitor --install-
dir="C:\Program Files\BackupClient"--language=de --agent-account=system --reg-
address=https://eu2-cloud.company.com --reg-token=34F6-8C39-4A5C --http-proxy-
address=https://my-proxy.company.com:80 --http-proxy-login=tomsmith --http-proxy-
password=tomspassword
```

インストールしたコンポーネントを削除するには

1. コマンドラインインターフェイスを管理者として起動し、`%ProgramFiles%\BackupClient\RemoteInstall`に移動します。
2. 次のコマンドを実行します。

   ```
   web_installer.exe --remove-components=<value 1>,<value 2> --quiet
   ```

   利用可能なパラメータとその値を確認するには、"無人インストール用パラメータ（EXE）"（89ページ）を参照してください。

例

- Cyber Protectモニタのアンインストール。

```
C:\Program Files\BackupClient\RemoteInstall\web_installer.exe --remove-
components=trayMonitor --quiet
```

エージェントをアンインストールするには

1. コマンドラインインターフェイスを管理者として起動し、`%Program Files%\Common Files\Acronis\BackupAndRecovery`に移動します。
2. 次のコマンドを実行します。

   ```
   Uninstaller.exe --quiet --delete-all-settings
   ```

   利用可能なパラメータとその値を確認するには、"無人インストール用パラメータ（EXE）"（89ページ）を参照してください。

例

- Windowsエージェントとそのすべてのコンポーネントをアンインストールします。すべてのログ、タスク、構成の設定を削除します。

```
C:\Program Files\Common Files\Acronis\BackupAndRecovery\Uninstaller.exe --quiet --
delete-all-settings
```

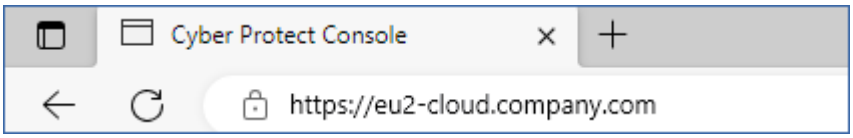
- パスワードで保護されたWindowsエージェントとそのすべてのコンポーネントをアンインストールします。すべてのログ、タスク、構成の設定を削除します。

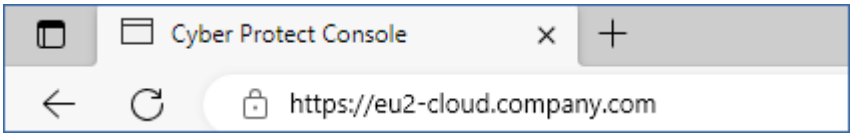
```
C:\Program Files\Common Files\Acronis\BackupAndRecovery\Uninstaller.exe --anti-tamper-password=<password> --quiet --delete-all-settings
```

無人インストール用パラメータ（EXE）

次の表は、EXEファイルを使用した無人インストールのパラメータをまとめたものです。

パラメータ	説明
一般的なパラメータ	
--add-components=<コンポーネント1,コンポーネント2,...,コンポーネントN>	インストールするコンポーネント。利用できるコンポーネントの詳細なリストについては、"無人インストール用コンポーネント（EXE）"（93ページ）を参照してください。 複数のコンポーネントを指定する場合は、カンマで区切ってください。カンマの前後にスペースを挿入しないでください。 既にインストールされているコンポーネントを指定すると、セットアッププログラムのバージョンとインストールされているコンポーネントのバージョンに応じて、これらのコンポーネントが修復またはアップデートされます。 このパラメータを指定しない場合、インストールを実行するマシンに応じて、デフォルトのコンポーネントセットがインストールされます。例えば、SQLエージェントは、MS SQL Serverが動作するマシンにのみインストールされます。
--install-dir=<パス>	選択したコンポーネントがインストールされるフォルダ。指定されたフォルダが存在しない場合、フォルダが作成されます。 このパラメータを指定しない場合、デフォルトのフォルダが使用されます。C:\Program Files\BackupClient。
--log-dir=<パス>	インストールログを保存するフォルダです。 このパラメータを指定しない場合、デフォルトのフォルダ（%ProgramData%\Acronis\InstallationLogs）が使用されます。
--language=<コード>	製品の言語。 次の値を使用できます: en、bn、bg、cs、da、de、es、fr、ko、id、it、hi、hu、ms、nl、ja、nb、pl、pt、pt_BR、ru、fi、sr、sv、th、tr、vi、zh、zh_TW。 このパラメータを指定せず、インストールを実行するマシンのシステム言語が上に記載されている場合は、システム言語が使用されます。それ以外の場合はenに設定されます。
--quiet	グラフィカルユーザーインターフェイスを表示せずにセットアッププログラムを実行するには、このパラメータを使用します。 --register-onlyパラメータと併用しないでください。

パラメータ	説明
--help	このパラメータを使用すると、コマンドラインで使用できるすべてのパラメータのリストとその説明が表示されます。
--fss-onboarding-auto-start	このパラメータを--quietパラメータと併用すると、無人インストール後にFile Sync & Shareオンボードウィザードが表示されます。
登録パラメータ	
--registration={skip | by-credentials | by-token | device-flow}	このパラメータを使用して、インストール後のエージェントの登録方法を選択します。 登録をスキップするには、skipと指定します。後で、--register-onlyパラメータを使用して、エージェントを登録することができます。 資格情報を使用してエージェントを登録するには、by-credentialsを指定し、--reg-loginと--reg-passwordパラメータを使用します。また、使用できるのは--reg-loginおよび--reg-passwordパラメータのみのため、--registration=by-credentialsの指定はオプションになります。 エージェントを登録トークンで登録するには、by-tokenを指定し--reg-tokenパラメータを使用します。また、--reg-tokenパラメータのみ使用できるため、--registration=by-tokenの指定はオプションになります。 OAuth 2.0プロトコルを使用してエージェントを登録するには、device-flowを指定します。インストールが完了すると、登録ページが自動的に開きます。 --registration=device-flowを使用する場合、--reg-addressパラメータの値として正確なデータセンターのアドレスを指定します。これは、Cyber Protectionサービスに**ログインした後**に表示されるURLです。例えば、https://eu2-cloud.company.comです。  --registration=device-flowと--quietパラメータを併用しないでください。
--reg-address=<url>	Cyber ProtectionサービスのURL。このパラメータは、--reg-loginと--reg-passwordの両パラメータと併用することも、--reg-tokenパラメータと併用することもできます。 • これを--reg-loginおよび--reg-passwordの両パラメータと併用する場合、Cyber Protectionサービスへの**ログイン**に使用するアドレスを指定します。例えばhttps://cloud.company.com:  のようになります。 • これを--reg-tokenパラメータと併用する場合は、実際のデータセンターのア

パラメータ	説明
	ドレスをそのまま指定してください。これは、Cyber Protectionサービスに**ログインした後**に表示されるURLです。たとえば、`https://eu2-cloud.company.com`です。  `https://cloud.company.com`を`--reg-token`パラメータと併用しないでください。

`--reg-login=<ログイン>`
 	
`--reg-password=<パスワード>`
	エージェントをCyber Protectionサービスに登録するアカウントの資格情報です。パートナー管理者アカウントは使用できません。
	
	これらのパラメータを使用する場合、`--registration`パラメータの指定は任意となります。
	
	これらのパラメータ`--reg-token`パラメータと併用しないでください。

`--reg-token=<トークン>`	登録トークン。 登録トークンは、12桁の文字列を3つのセグメントに分けてハイフンで区切る形式になっています。登録トークンを生成する方法の詳細については、"登録トークンの生成"（164ページ）を参照してください。 このパラメータを使用する場合、`--registration`パラメータの指定は任意となります。 このパラメータを`--reg-login`および`--reg-password`パラメータと併用しないでください。
`--register-only`	インストールをスキップし、OAuth 2.0プロトコル(device-flow)を使用してエージェントを登録するには、このパラメータを使用します。 インストールが完了すると、登録ページが自動的に開きます。 `--register-only`と`--quiet`パラメータを併用しないでください。
エージェント サービスのログイン アカウント	

`--agent-account={system | new | custom}`
 	
または、
 	
`--agent-account-login=<ログイン>`
 	
`--agent-account-password=<パスワード>`
	このパラメータを使用して、エージェントサービスを実行するログオンアカウントを指定します。ログオンアカウントの詳細については、"Windowsマシンのログオンアカウントの変更"（84ページ）を参照してください。
	
	ローカルシステムアカウントを使用するには、`--agent-account=system`を指定するか、コマンドで`--agent-account`パラメータを指定しないようにします。
	
	自動的に作成される新しいログオンアカウント**Acronis Agent User**でエージェントサービスを実行するには、`new`を指定します。
	
	エージェントサービスを既存のアカウントで実行させるには、`--agent-account-login`および`--agent-account-password`パラメータを使用してアカウント資格情報を指定します。この場合、`--agent-account=custom`パラメータの指定は任意とな

パラメータ	説明
	ります。
vCenter/ESXiパラメータ	
--esxi-address=<ホスト>	vCenter ServerまたはESXiホストのホスト名またはIPアドレス。 このパラメータは、VMwareエージェントをインストールするときに使用します。
--esxi-login=<ログイン> --esxi-password=<パスワード>	vCenter ServerまたはESXiホストへのアクセス認証情報。 これらのパラメータは、VMwareエージェントをインストールするときに使用します。
プロキシパラメータ	
--http-proxy={none | system | custom}	このパラメータを使用して、クラウドストレージへのバックアップとクラウドストレージからの復元に使用するHTTPプロキシサーバーを指定します。 プロキシサーバー接続を無効にするには、--http-proxy=noneを指定します。 システム全体のプロキシサーバーを使用するには、--http-proxy=systemを指定するか、コマンドで--http-proxyパラメータを指定しないようにします。 別のプロキシサーバーを使用するには、--http-proxy-address、--http-proxy-login、--http-proxy-passwordパラメータを使用して、プロキシサーバーアドレスと資格情報を指定します。この場合、 --http-proxy=customパラメータの指定は任意です。
--http-proxy-address=<ホスト>:<ポート>	カスタムHTTPプロキシサーバーのホスト名またはIPアドレスとポート。
--http-proxy-login=<ログイン>	カスタムHTTPプロキシサーバーへのログイン。
--http-proxy-password=<パスワード>	カスタムHTTPプロキシサーバーのパスワード。
インストール解除パラメータ	
--remove-components=<コンポーネント1,コンポーネント2,...,コンポーネントN>	アンインストールするコンポーネント。利用できるコンポーネントの詳細なリストについては、"無人インストール用コンポーネント（EXE）"（93ページ）を参照してください。 複数のコンポーネントを指定する場合は、カンマで区切ってください。カンマの前後にスペースを挿入しないでください。

パラメータ	説明
	重要 このパラメータを使用すると、コンポーネントのみをアンインストールできます。製品を完全にアンインストールするには、Windowsの [コントロールパネル] > [プログラムと機能] で製品を選択し、**[アンインストール]** をクリックします。
`--delete-all-settings`	このオプションパラメータは、`--remove-components`パラメータを使用して、すべての製品ログ、タスク、構成設定を削除する場合に使用します。
`--anti-tamper-password=<パスワード>`	Windowsエージェントをアンインストールしたりそのコンポーネントを変更したりするにはパスワードが求められます。

無人インストール用コンポーネント（EXE）

以下の表は、EXEファイルによる無人インストールに使用できるコンポーネントをまとめたものです。値の名前を使用して、`--add-components`パラメータの値を指定します。

詳細については、"無人インストール用パラメータ（EXE）"（89ページ）"無人インストール用パラメータ（MSI）"（98ページ）を参照してください

値の名前	コンポーネントの説明
`agentForWindows`	Windowsエージェント
`agentForSas`	File Sync & Shareエージェント
`agentForAd`	エージェント for Active Directory
`agentForAmp`	マルウェア対策保護エージェントおよびURLフィルタリング用エージェント
`agentForDlp`	データ漏洩防止エージェント
`agentForEsx`	エージェント for VMware（Windows）
`agentForExchange`	Exchangeエージェント
`agentForHyperV`	Hyper-Vエージェント
`agentForOffice365`	エージェント for Office 365
`agentForOracle`	Oracle エージェント
`agentForSql`	SQL エージェント
`commandLine`	コマンドラインツール
`mediaBuilder`	ブータブルメディアビルダー
`trayMonitor`	Cyber Protectモニタ
`all`	この値は、すべてのコンポーネントを組み合わせたものです。

値の名前	コンポーネントの説明
allAgents	この値は、すべてのエージェントを組み合わせたものです。

MSIファイルによる無人インストールとインストール解除

このタイプの無人インストールには、Windows Installer（Msiexecプログラム）を使用します。セットアッププログラムのグラフィカルユーザーインターフェイスを使用して、事前にインストールパッケージとMSIファイルを展開します。

MSIファイルでコンポーネントをインストールする場合、MST変換ファイルを使用して、インストールパラメータをカスタマイズできます。MSIファイルとMSTファイルの組み合わせの使用方法の詳細については、"エージェントとコンポーネントのインストール（MSIとMSTの組み合わせ）"（95ページ）を参照してください。Active Directoryドメインでこのインストール方法を使用すると、Windowsグループポリシーを使用してプロテクションエージェントをインストールできます。詳細については、"グループポリシーによるエージェントの配置"（163ページ）を参照してください。

また、コマンドラインから手動でインストールパラメータを指定することもできます。この場合、MSTファイルは必要ありません。詳細については、"例"（96ページ）を参照してください。

MSI、MST、およびCABファイルの展開

セットアッププログラムのグラフィカルユーザーインターフェイスを実行して、インストールパッケージとMSI、MST、およびCABファイルを展開します。

MSI、MST、およびCABファイルを展開するには

1. セットアッププログラムのグラフィカルユーザーインターフェイスを実行し、**[無人インストールの.mstおよび.msiを作成]** をクリックします。
2. **[インストールする項目]** で、インストールするコンポーネントを選択してから、**[完了]** をクリックします。
   これらのコンポーネントのインストールパッケージは、CABファイルとしてセットアッププログラムから展開されます。
3. **[登録の設定]** で **[資格情報を使用します]** か **[登録トークンを使用します]** を選択します。選択に応じて資格情報または登録トークンを指定し、**[完了]** をクリックします。
   登録トークンを生成する詳細な方法については、"登録トークンの生成"（164ページ）を参照してください。
4. （ドメインコントローラーでインストールする場合のみ）**エージェントサービスのログオンアカウント**で、**[次のアカウントを使用する]** を選択します。エージェントサービスを実行するユーザーアカウントを指定して、**[完了]** をクリックします。これは、セキュリティ上の理由で、プログラムの設定はドメインコントローラ上で新しいアカウントを自動作成できないためです。

注意
このユーザーアカウントには、**サービスとしてログオン**の権限を指定する必要があります。ドメインコントローラーのマシン上にプロファイルフォルダを作成するには、該当のマシンでこのアカウントが既に使用されている必要があります。

読み取り専用ドメインコントローラーに対するエージェントインストールの詳細については、こちらのナレッジベースの記事を参照してください。

5. MSTファイルに追加される他のインストール設定を確認または変更し、**[実行]** をクリックします。
6. MSI、MST、CABファイルが展開されるフォルダを選択し、**[生成]** をクリックします。

エージェントとコンポーネントのインストール（MSIとMSTの組み合わせ）

MSTファイルを使用して、MSIファイルのインストール設定をカスタマイズします。Windowsグループポリシーを通じて複数のマシンにエージェントをインストールする場合は、MSIとMSTの組み合わせを使用します。詳細については、"グループポリシーによるエージェントの配置"（163ページ）を参照してください。

MSIファイルとMSTファイルでコンポーネントをインストールするには

1. MSIファイルとMSTファイルを展開します（"MSI、MST、およびCABファイルの展開"（94ページ）を参照）。
2. コンポーネントをインストールするマシンのコマンドラインインターフェイスで、以下のコマンドを実行します。

```
msiexec /i <MSI file> TRANSFORMS=<MST file>
```

例:

```
msiexec /i BackupClient64.msi TRANSFORMS=BackupClient64.msi.mst
```

エージェントとコンポーネントのインストールとアンインストール（MSIと直接選択）

MSIファイルを実行し、インストールするコンポーネントを手動で選択して、コマンドラインでインストールパラメータを指定します。この場合、MSTファイルは必要ありません。

エージェントとコンポーネントをインストールするには

1. MSIファイルとインストールパッケージ（CABファイル）を展開します（"MSI、MST、およびCABファイルの展開"（94ページ）を参照）。
   このインストール方法では、MSIファイルとCABファイルのみが必要です。MSTファイルは必要ありません。
2. マシンのコマンドラインインターフェイスで、以下のコマンドを実行します。

```
msiexec /i <MSI file><PARAMETER 1>=<value 1> ... <PARAMETER N>=<value n>
```

パラメータを区切るにはスペースを使用し、パラメータの値を区切るにはカンマ（スペースなし）を使用します。例:

```
msiexec.exe /i BackupClient64.msi
ADDLOCAL=MmsMspComponents,BackupAndRecoveryAgent,CommandLineTool,TrayMonitor
TARGETDIR="C:\Program Files\BackupClient" REGISTRATION_ADDRESS=https://eu2-
cloud.company.com REGISTRATION_TOKEN=34F6-8C39-4A5C
```

利用可能なパラメータとその値を確認するには、"無人インストール用パラメータ（MSI）"（98ページ）を参照してください。

例

- Windowsエージェント、マルウェア対策エージェント、URLフィルタリング用エージェント、コマンドラインツール、Cyber Protect Monitorをインストールする。 ユーザー名とパスワードを使用してCyber Protectionサービスにワークロードを登録する操作。

```
msiexec.exe /i BackupClient64.msi /l*v my_log.txt /qn
ADDLOCAL=MmsMspComponents,BackupAndRecoveryAgent,AmpAgentFeature,CommandLineTool,Tray
Monitor TARGETDIR="C:\Program Files\BackupClient" REBOOT=ReallySuppress MMS_USE_
SYSTEM_ACCOUNT=1 REGISTRATION_ADDRESS=https://cloud.company.com REGISTRATION_
LOGIN=johndoe REGISTRATION_PASSWORD=johnspassword
```

- Windowsエージェント、コマンドラインツール、Cyber Protect Monitorのインストール。Windowsでエージェントサービスの新しいログオンアカウントを作成する操作。トークンを使用してCyber Protectionサービスにワークロードを登録する操作。

```
msiexec.exe /i BackupClient64.msi /l*v my_log.txt /qn
ADDLOCAL=MmsMspComponents,BackupAndRecoveryAgent,CommandLineTool,TrayMonitor
TARGETDIR="C:\Program Files\BackupClient" REBOOT=ReallySuppress MMS_CREATE_NEW_
ACCOUNT=1 REGISTRATION_ADDRESS=https://eu2-cloud.company.com REGISTRATION_TOKEN=34F6-
8C39-4A5C
```

- Windowsエージェント、コマンドラインツール、Oracleエージェント、Cyber Protect Monitorのインストール。ユーザー名とbase64でエンコードされたパスワードを使用してCyber Protectionサービスにマシンを登録する操作。パスワードに記号や空白が含まれている場合、エンコードが必要になる場合があります。パスワードをエンコードする方法の詳細については、"特殊文字やブランクスペースを使用したパスワード"（120ページ）を参照してください。

```
msiexec.exe /i BackupClient64.msi /l*v my_log.txt /qn
ADDLOCAL=MmsMspComponents,BackupAndRecoveryAgent,CommandLineTool,OracleAgentFeature,T
rayMonitor TARGETDIR="C:\Program Files\BackupClient" REBOOT=ReallySuppress CURRENT_
LANGUAGE=en MMS_USE_SYSTEM_ACCOUNT=1 REGISTRATION_ADDRESS=https://cloud.company.com
REGISTRATION_LOGIN=johndoe REGISTRATION_PASSWORD_ENCODED=am9obnNwYXNzd29yZA==
```

- Windowsエージェント、コマンドラインツール、Cyber Protect Monitorのインストール。トークンを使用してCyber Protectionサービスにマシンを登録する操作。HTTPプロキシを設定する操作。

```
msiexec.exe /i BackupClient64.msi /l*v my_log.txt /qn
ADDLOCAL=MmsMspComponents,BackupAndRecoveryAgent,CommandLineTool,TrayMonitor
TARGETDIR="C:\Program Files\BackupClient" REBOOT=ReallySuppress CURRENT_LANGUAGE=en
MMS_USE_SYSTEM_ACCOUNT=1 REGISTRATION_ADDRESS=https://eu2-cloud.company.com
```

```
REGISTRATION_TOKEN=34F6-8C39-4A5C HTTP_PROXY_ADDRESS=https://my-proxy.company.com
HTTP_PROXY_PORT=80 HTTP_PROXY_LOGIN=tomsmith HTTP_PROXY_PASSWORD=tomspassword
```

インストールしたコンポーネントを削除するには

1. MSIファイルとインストールパッケージ（CABファイル）を展開します（"MSI、MST、およびCABファイルの展開"（94ページ）を参照）。
   このインストール方法では、MSIファイルとCABファイルのみが必要です。MSTファイルは必要ありません。
2. マシンのコマンドラインインターフェイスで、以下のコマンドを実行します。

   ```
   msiexec /i <MSI file><REMOVE>=<value 1>,<value 2> REBOOT=ReallySuppress /qn
   ```

   利用可能なパラメータとその値を確認するには、"無人インストール用パラメータ（MSI）"（98ページ）を参照してください。

例

- Cyber Protectモニターを削除します。

```
msiexec.exe /i BackupClient64.msi /l*v uninstall_log.txt REMOVE=TrayMonitor
REBOOT=ReallySuppress /qn
```

エージェントをアンインストールするには

1. MSIファイルとインストールパッケージ（CABファイル）を展開します（"MSI、MST、およびCABファイルの展開"（94ページ）を参照）。
   このインストール方法では、MSIファイルとCABファイルのみが必要です。MSTファイルは必要ありません。
2. マシンのコマンドラインインターフェイスで、以下のコマンドを実行します。

   ```
   msiexec /x <MSI file> /l*v uninstall_log.txt DELETE_ALL_SETTINGS=1
   REBOOT=ReallySuppress /qn
   ```

   利用可能なパラメータとその値を確認するには、"無人インストール用パラメータ（MSI）"（98ページ）を参照してください。

例

- Windowsエージェントとそのすべてのコンポーネントをアンインストールします。すべてのログ、タスク、構成の設定を削除します。

```
msiexec.exe /x BackupClient64.msi /l*v uninstall_log.txt DELETE_ALL_SETTINGS=1
REBOOT=ReallySuppress /qn
```

- パスワードで保護されたWindowsエージェントとそのすべてのコンポーネントをアンインストールします。すべてのログ、タスク、構成の設定を削除します。

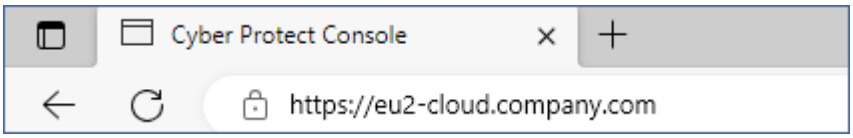
```
msiexec.exe /x BackupClient64.msi /l*v uninstall_log.txt ANTI_TAMPER_
PASSWORD=<password> DELETE_ALL_SETTINGS=1 REBOOT=ReallySuppress /qn
```

無人インストール用パラメータ（MSI）

次の表は、MSIファイルを使用した無人インストールのパラメータをまとめたものです。

追加のmsiexecパラメータを使用することもできます。例えば、/qnを使ってGUIエレメントが表示されないようにします。msiexecパラメータの詳細については、Microsoftの文書を参照してください。

パラメータ	説明
一般的なパラメータ	
ADDLOCAL=<コンポーネント1,コンポーネント2,..., コンポーネントN>	インストールするコンポーネント。利用できるコンポーネントの詳細なリストについては、"無人インストール用コンポーネント（MSI）"（101ページ）を参照してください。 複数のコンポーネントを指定する場合は、カンマで区切ってください。カンマの前後にスペースを挿入しないでください。 **注意** インストールするすべてのコンポーネントのインストールファイルを展開する必要があります。展開する方法の詳細については、"MSI、MST、およびCABファイルの展開"（94ページ）を参照してください。
TARGETDIR=<パス>	選択したコンポーネントがインストールされるフォルダ。指定されたフォルダが存在しない場合、フォルダが作成されます。 このパラメータを指定しない場合、デフォルトのフォルダが使用されます。C:\Program Files\BackupClient。
REBOOT=ReallySuppress	マシンを再起動せずにコンポーネントをインストールしたい場合は、このパラメータを指定します。
/l*v <ログファイル>	冗長ログを保存するには、このパラメータを指定します。このログは、インストールの問題を調査する場合に必要となります。
CURRENT_LANGUAGE=<言語ID>	製品の言語。 次の値を使用できます: en、bn、bg、cs、da、de、es、fr、ko、id、it、hi、hu、ms、nl、ja、nb、pl、pt、pt_BR、ru、fi、sr、sv、th、tr、vi、zh、zh_TW。 このパラメータを指定せず、インストールを実行するマシンのシステム言語が上に記載されている場合は、システム言語が使用されます。それ以外の場合はenに設定されます。
SKIP_SHA2_KB_CHECK={0,1}	このパラメータを使用して、Microsoftが提供するSHA2コード署名サポートアップデートプログラム（KB4474419）のマシンへのインストール状況を確認するかどうかを選択します。この確認は、このアップデートが必要なオペレーティングシステムでのみ実行されます。ご利用のオペレーティングシステムで必要かどうかについては、"サポートされるオペレーティング システムと環境"（23ページ）

パラメータ	説明
	を参照してください。 このパラメータの値を1に設定して使用すると、確認を省略できます。 パラメータを指定しないか、値を0に設定した場合、SHA2コード署名サポートアップデートがマシンで見つからないと、インストールが失敗します。
FSS_ONBOARDING_AUTO_START={0,1}	無人インストール後にオンボードウィザードを表示するには、このパラメータを1に設定します。 このパラメータを指定しないか、値を0に設定すると、オンボードウィザードは表示されません。
登録パラメータ	
REGISTRATION_ADDRESS	Cyber ProtectionサービスのURL。このパラメータは、REGISTRATION_LOGINおよびREGISTRATION_PASSWORDの両パラメータと併用することも、REGISTRATION_TOKEN単体と併用することもできます。 • これをREGISTRATION_LOGINおよび REGISTRATION_PASSWORDの両パラメータと併用する場合、Cyber Protectionサービスへの**ログイン**に使用するアドレスを指定します。たとえば、https://cloud.company.comです。  • これをREGISTRATION_TOKENパラメータと併用する場合は、実際のデータセンターのアドレスをそのまま指定してください。これは、Cyber Protectionサービスに**ログインした後**に表示されるURLです。たとえば、https://eu2-cloud.company.comです。  https://cloud.company.comをREGISTRATION_TOKENパラメータと併用しないでください。
REGISTRATION_LOGIN REGISTRATION_PASSWORD	エージェントをCyber Protectionサービスに登録するアカウントの資格情報です。パートナー管理者アカウントは使用できません。 これらのパラメータREGISTRATION_TOKENパラメータと併用しないでください。
REGISTRATION_PASSWORD_ENCODED	base64でエンコードされた、エージェントをCyber Protectionサービスに登録するアカウントのパスワードです。パスワードのエンコード方法の詳細については、"特殊文字やブランクスペースを使用したパスワード"（120ページ）を参照してください。
REGISTRATION_TOKEN	登録トークン。 登録トークンは、12桁の文字列を3つのセグメントに分けてハイフンで区切る形式になっています。登録トークンを生成する方法の詳細については、"登録トークン

パラメータ	説明
	の生成"（164ページ）を参照してください。 このパラメータをREGISTRATION_LOGINおよびREGISTRATION_PASSWORDパラメータと併用しないでください。
REGISTRATION_REQUIRED={0,1}	このパラメータを使用して、登録に失敗した場合の処理を選択します。 値を1に設定している場合、インストールも失敗します。値を0に設定しているか、パラメータを指定しないと、登録に失敗してもインストールは正常に完了します。
エージェント サービスのログイン アカウント	
MMS_USE_SYSTEM_ACCOUNT={0,1}	**ローカルシステム**ログオンアカウントでサービスを実行するには、このパラメータの値を1にします。 ログオンアカウントの詳細については、"Windowsマシンのログオンアカウントの変更"（84ページ）を参照してください。
MMS_CREATE_NEW_ACCOUNT={0,1}	このパラメータの値を1にすると、エージェントサービスは自動的に作成される新しいログオンアカウント**Acronis Agent User**で実行されます。
MMS_SERVICE_USERNAME=<ユーザー名> MMS_SERVICE_PASSWORD=<パスワード>	エージェントサービスが実行される既存のログオンアカウントを指定するには、これらのパラメータを使用します。
vCenter/ESXiパラメータ	
SET_ESX_SERVER={0,1}	このパラメータは、VMwareエージェントをインストールするときに使用します。 値を0に設定すると、VMwareエージェントは、vCenter ServerまたはESXiホストに接続されません。 値を1に設定している場合、次のパラメータを指定します。ESX_HOST、EXI_USER、ESX_PASSWORD。
ESX_HOST=<ホスト名>	vCenter ServerまたはESXiホストのホスト名またはIPアドレス。
ESX_USER=<ユーザー名> ESX_PASSWORD=<パスワード>	vCenter ServerまたはESXiホストへのアクセス認証情報。
プロキシパラメータ	
HTTP_PROXY_ADDRESS=<IPアドレス> HTTP_PROXY_PORT=<ポート>	これらのパラメータを使用して、エージェントが使用するHTTPプロキシサーバーを指定します。 プロキシサーバーを使用しない場合は、これらのパラメータを指定しないでください。

パラメータ	説明
HTTP_PROXY_LOGIN=<ログイン> HTTP_PROXY_PASSWORD=<パスワード>	HTTPプロキシサーバーの資格情報。 プロキシサーバーで認証が求められる場合は、これらのパラメータを使用します。
インストール解除パラメータ	
REMOVE={<**コンポーネントのリスト**>|ALL}	アンインストールするコンポーネント。 複数のコンポーネントを指定する場合は、カンマで区切ってください。カンマの前後にスペースを挿入しないでください。 すべての製品コンポーネントを削除するには、値をALLに設定します。
DELETE_ALL_SETTINGS={0,1}	すべての製品ログ、タスク、構成設定を削除するには、値を1に設定します。 REMOVEパラメータを使用する場合、このオプションパラメータを使用します。
ANTI_TAMPER_PASSWORD=<**パスワード**>	Windowsエージェントをアンインストールしたりそのコンポーネントを変更したりするにはパスワードが求められます。

無人インストール用コンポーネント（MSI）

以下の表は、MSIファイルによる無人インストールに使用できるコンポーネントをまとめたものです。値の名前を使用して、ADDLOCALパラメータの値を指定します。詳細については、"無人インストール用パラメータ（MSI）"（98ページ）を参照してください。

値の名前	コンポーネントの説明	一緒にインストールする必要があるもの	ビット数
AgentFeature	エージェントのコアコンポーネント		32 ビット/64 ビット
MmsMspComponents	バックアップのコアコンポーネント	AgentFeature	32 ビット/64 ビット
BackupAndRecoveryAgent	Windowsエージェント	MmsMspComponents	32 ビット/64 ビット
AmpAgentFeature	Agent for Antimalware protection	BackupAndRecoveryAgent	32 ビット/64 ビット
UrlFilteringAgentFeature	Agent for URL Filtering	BackupAndRecoveryAgent	32 ビット/64 ビット

DlpAgentFeature	データ漏洩防止エージェント	BackupAndRecoveryAgent	32 ビット/64 ビット
SasAgentFeature	File Sync & Share エージェント	TrayMonitor	32 ビット/64 ビット
ArxAgentFeature	Exchangeエージェント	MmsMspComponents	32 ビット/64 ビット
ArsAgentFeature	SQL エージェント	BackupAndRecoveryAgent	32 ビット/64 ビット
ARADAgentFeature	エージェント for Active Directory	BackupAndRecoveryAgent	32 ビット/64 ビット
ArxOnlineAgentFeature	Microsoft 365 エージェント	MmsMspComponents	32 ビット/64 ビット
OracleAgentFeature	Oracle エージェント	BackupAndRecoveryAgent	32 ビット/64 ビット
AcronisESXSupport	VMware ESX(i) エージェント（Windows）	BackupAndRecoveryAgent	64 ビット
HyperVAgent	Hyper-Vエージェント	BackupAndRecoveryAgent	32 ビット/64 ビット
CommandLineTool	コマンドラインツール		32 ビット/64 ビット
TrayMonitor	Cyber Protectモニタ	AgentFeature	32 ビット/64 ビット
BackupAndRecoveryBootableComponents	ブータブルメディアビルダー		32 ビット/64 ビット

Linux での無人インストールまたはインストール解除

このセクションでは、Linuxを実行しているマシンで保護エージェントのインストールとアンインストールをコマンドラインによって無人モードで実行する方法を説明します。

エージェントをインストールするには

1.ターミナルを開きます。

2.次のいずれかを実行します。

- コマンドラインでパラメータを指定してインストールを開始する場合は、以下のコマンドを実行します。

  ```
  <package name> -a <parameter 1> ... <parameter N>
  ```

  ここで、<package name> は、インストールパッケージの名前です（.i686 または .x86_64 ファイル）。すべての有効なパラメータと値の説明については、"無人インストールまたはインストール解除のパラメータ"（104ページ）を参照してください。
- 別のテキストファイルで指定したパラメータを使用してインストールを開始する場合は、以下のコマンドを実行します。

  ```
  <package name> -a --options-file=<path to the file>
  ```

  コマンドラインに機密情報を入力したくない場合は、この方法が便利です。この場合は、別のテキストファイルで構成設定を指定して、自分だけがそのファイルにアクセスできるようにしておきます。各パラメータを1行ごとに記述し、その後にパラメータの値を入力します（以下の例を参照）。

  ```
  --rain=https://cloud.company.com
  --login=johndoe
  --password=johnspassword
  --auto
  ```

  または、

  ```
  -C
  https://cloud.company.com
  -g
  johndoe
  -w
  johnspassword
  -a
  --language
  en
  ```

  コマンドラインとテキストファイルの両方で同じパラメータを指定する場合は、コマンドラインの値が優先されます。

3. UEFI セキュアブートがマシンで有効になっている場合、インストールの後にシステムを再起動するように促されます。使用するパスワード（ルートユーザーまたは「acronis」のパスワード）を覚えてお

いてください。システム再起動中に、MOK（マシン所有者キー）の管理オプションで、**[MOKを登録]**を選択し、推奨されたパスワードを使用してキーを登録します。

エージェントのインストール後にUEFIセキュアブートを有効にした場合は、手順3を含むインストールを繰り返します。そうでない場合、バックアップは失敗します。

エージェントをアンインストールするには

1. ターミナルを開きます。
2. 次のいずれかを実行します。
   - エージェントをアンインストールして、すべてのログ、タスクおよび設定を削除するには、次のコマンドを実行します。

     ```
     /usr/lib/Acronis/BackupAndRecovery/uninstall/uninstall -a
     ```

   - エージェントをアンインストールして、そのIDを保持する（たとえば、後でエージェントをインストールする予定がある場合）には、次のコマンドを実行します。

     ```
     /usr/lib/Acronis/BackupAndRecovery/uninstall/uninstall -a --no-purge
     ```

   - インストールファイルを使用してエージェントをアンインストールするには、次のコマンドを実行します。

     ```
     <package name> -a -u
     ```

     ここで、<package name> は、インストールパッケージの名前です（.i686 または .x86_64 ファイル）。すべての有効なパラメータと値の説明については、"無人インストールまたはインストール解除のパラメータ"（104ページ）を参照してください。

     注意
     このコマンドは、インストールパッケージがインストールされたエージェントと同じバージョンであり、/usr/lib/Acronis/BackupAndRecovery/uninstall/uninstallが破損しているかアクセスできない場合にのみ使用します。

無人インストールまたはインストール解除のパラメータ

このセクションでは、Linuxでの無人モードのインストールやアンインストールで使用するパラメータについて説明します。

無人インストールの最小構成には、-aと登録パラメータ（--loginと--passwordや、--rainと--tokenなど）が含まれます。その他のパラメータを使用してインストールをカスタマイズすることも可能です。

インストールパラメータ

基本パラメータ

{-i |--id=}<コンポーネントのリスト>

インストールするコンポーネントをスペース文字なしのカンマ区切りで指定します。.x86_64インストールパッケージには、以下のコンポーネントが用意されています。

コンポーネント	コンポーネントの説明
BackupAndRecoveryAgent	Linuxエージェント
AgentForPCS	Virtuozzoエージェント
OracleAgentFeature	Oracle エージェント
MySQLAgentFeature	MySQL/MariaDBエージェント

このパラメータを指定しない場合、上記のすべてのコンポーネントがインストールされます。

Virtuozzoエージェント、Oracleエージェント、およびMySQL/MariaDBエージェントを使用するには、Linuxエージェントもインストールする必要があります。

.i686インストールパッケージには、BackupAndRecoveryAgentしか入っていません。

`{-a|--auto}`

ユーザーの干渉なしでインストールと登録のプロセスが完了します。このパラメータを使用する場合は、エージェントをCyber Protectionサービスに登録するアカウントを指定する必要があります。そのためには、`--token`パラメータを使用するか、`--login`と`--password`の両パラメータを使用します。

`{-t|--strict}`

このパラメータを指定した場合は、インストール中に警告が発生するとインストールが失敗します。このパラメータを指定しない場合は、警告が発生してもインストールは正常に完了します。

`{-n|--nodeps}`

インストール時に必要なLinuxパッケージが存在しない場合でも無視されます。

`{-d|--debug}`

インストールログを詳細モードで書き込みます。

`--options-file=<ロケーション>`

インストールパラメータをコマンドラインではなくテキストファイルから読み取ります。

`--language=<言語ID>`

製品の言語。使用できる値:`en`、`bg`、`cs`、`da`、`de`、`es`、`fr`、`hu`、`id`、`it`、`ja`、`ko`、`ms`、`nb`、`nl`、`pl`、`pt`、`pt_BR`、`ru`、`fi`、`sr`、`sv`、`tr`、`zh`、`zh_TW`。
このパラメータを指定しない場合は、システム言語に基づいて製品の言語が定義されます（ただし、その言語が上記のリストに含まれていることが条件です）。そうでない場合は、製品の言語が英語（`en`）に設定されます。

登録パラメータ

次のいずれかのパラメータを指定します。

- `{-g|--login=}<`**ユーザー名**`>` と `{-w|--password=}<`**パスワード**`>`

  エージェントをCyber Protectionサービスに登録するアカウントの資格情報です。パートナー管理者アカウントは使用できません。

- `--token=<`**トークン**`>`

  登録トークンは、12桁の文字列を3つのセグメントに分けて各セグメントをハイフンで区切る形式になっています。Cyber Protectコンソールで登録トークンを生成できます（「グループポリシーによるエージェントの配置」を参照）。

  `--token`パラメータは、`--login`、`--password`、`--register-with-credentials`パラメータと一緒に使用できません。

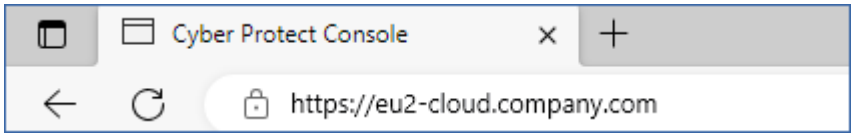
  - `{-C|--rain=}<`**サービスアドレス**`>`

    Cyber ProtectionサービスのURL。

    登録のために`--login`パラメータと`--password`パラメータを使用するのであれば、このパラメータを明示的に組み込む必要はありません。インストーラがデフォルトで正しいアドレス（Cyber Protectionサービスへの**ログイン**で使用するアドレス）を使用するからです。例:

    ただし、`{-C|--rain=}`と`--token`パラメータを一緒に使用する場合は、実際のデータセンターのアドレスをそのまま指定する必要があります。これは、Cyber Protectionサービスに**ログインすると**表示されるURLです。例:

- `--register-with-credentials`

  このパラメータを指定すると、インストーラのグラフィカルインターフェースが起動します。登録を完了するために、エージェントをCyber Protectionサービスに登録するアカウントのユーザー名とパスワードを入力します。パートナー管理者アカウントは使用できません。

- `--skip-registration`

  エージェントをインストールするものの、Cyber Protectionサービスには後で登録する場合、このパラメータを使用します。詳細については、「マシンの手動登録」を参照してください。

その他のパラメータ

`--http-proxy-host=<`**IPアドレス**`>`および`--http-proxy-port=<`**ポート**`>`

エージェントがクラウドからのバックアップと復元や管理サーバーへの接続に使用するHTTPプロキシサーバーです。これらのパラメータを指定しない場合は、プロキシサーバーは使用されません。

`--http-proxy-login=<`**ログイン**`>` および`--http-proxy-password=<`**パスワード**`>`

HTTPプロキシサーバーの資格情報。サーバーで認証が求められる場合は、これらのパラメーターを使用します。

--tmp-dir=<**ロケーション**>

インストール時に一時ファイルを保管するフォルダを指定します。デフォルトのフォルダは**/var/tmp**です。

{-s|--disable-native-shared}

システムにすでに再頒布可能ライブラリが存在する場合でも、インストール時にそのライブラリを使用します。

--skip-prereq-check

snapapiモジュールのコンパイルに必要なパッケージがすでにインストールされているかどうかをチェックしません。

--force-weak-snapapi

インストーラはsnapapiモジュールをコンパイルしません。その代わりに、あらかじめ用意されているモジュールを使用します（そのモジュールはLinuxカーネルに完全に対応しない可能性があります）。このオプションの使用はお勧めしません。

--skip-svc-start

インストール後にサービスを自動的に開始しません。このパラメータは通常、--skip-registrationと一緒に使用します。

情報パラメータ

{-?|--help}

パラメータの説明を表示します。

--usage

コマンドの使用法についての簡単な説明を表示します。

{-v|--version}

インストールパッケージのバージョンを表示します。

--product-info

製品名とインストールパッケージのバージョンを表示します。

--snapapi-list

あらかじめ用意されている有効なsnapapiモジュールを表示します。

--components-list

インストーラコンポーネントを表示します。

レガシー機能のパラメータ

以下は、レガシーコンポーネントagent.exeに関連したパラメータです。

{-e|--ssl=}<**パス**>

SSL通信用のカスタム証明書ファイルのパスを指定します。

{-p|--port=}<**ポート**>

agent.exeが接続をlistenするポートを指定します。デフォルトのポートは9876です。

インストール解除パラメータ

{-u|--uninstall}

製品をインストール解除します。

--purge

製品をアンインストールし、ログやタスクや構成設定を削除します。--purgeパラメータを使用する場合、--uninstallパラメータを明示的に指定する必要はありません。

例

- Linuxエージェントをインストールする操作（登録はしない）。

```
./Cyber_Protection_Agent_for_Linux_x86_64.bin -i BackupAndRecoveryAgent -a --skip-registration
```

- LinuxエージェントとVirtuozzoエージェントとOracleエージェントをインストールし、資格情報を使用して登録する操作。

```
./Cyber_Protection_Agent_for_Linux_x86_64.bin -a --login=johndoe --password=johnspassword
```

- OracleエージェントとLinuxエージェントをインストールし、登録トークンを使用して登録する操作。

```
./Cyber_Protection_Agent_for_Linux_x86_64.bin -i BackupAndRecoveryAgent,OracleAgentFeature -a --rain=https://eu2-cloud.company.com --token=34F6-8C39-4A5C
```

- 別のテキストファイルに記述した構成設定を使用して、LinuxエージェントとVirtuozzoエージェントとOracleエージェントをインストールする操作。

```
./Cyber_Protection_Agent_for_Linux_x86_64.bin -a --options-file=/home/mydirectory/configuration_file
```

- Linuxエージェント、Virtuozzoエージェント、およびOracleエージェントをアンインストールし、すべてのログやタスクや構成設定を削除する操作。

```
./Cyber_Protection_Agent_for_Linux_x86_64.bin -a --purge
```

macOSの無人インストールとインストール解除

このセクションでは、コマンドラインを使用した無人モードで、macOSを実行しているマシン上のプロテクションエージェントをインストール、登録、アンインストールする方法について説明します。

必要な許可

Macワークロードで無人インストールを開始する前に、ワークロードのmacOSでプライバシー設定のポリシーコントロールを変更して、アプリアクセスとカーネルおよびシステム拡張機能を許可する必要があります。これにより、Cyber Protectionエージェントのインストールが可能になります。 "macOSでの無人インストールに必要な許可"（110ページ）を参照してください。

PPPCペイロードを配置した後、以下の手順に進むことができます。

インストールファイル（.dmg）をダウンロードする手順

1. Cyber Protectコンソールで **[デバイス]** > **[すべてのデバイス]** に進みます。
2. **[追加]** をクリックして、**[Mac]** をクリックします。

エージェントをインストールするには

1. ターミナルを開きます。
2. インストールファイル（.dmg）をマウントする一時ディレクトリを作成します。

   ```
   mkdir <dmg_root>
   ```

   ここで、<dmg_root>は自分で選択した名前になります。
3. .dmgファイルをマウントします。

   ```
   hdiutil attach <dmg_file> -mountpoint <dmg_root>
   ```

   ここで、<dmg_file>はインストールファイルの名前です。たとえば、**Cyber_Protection_Agent_for_MAC_x64.dmg**と指定します。
4. インストーラを実行します。
   - CyberProtect_AgentForMac_x64.dmgやCyberProtect_AgentForMac_arm64.dmgなどのMac用のフルインストーラを使用する場合、以下のコマンドを実行してください。

     ```
     sudo installer -pkg <dmg_root>/Install.pkg -target LocalSystem
     ```

     注意
     File Sync & Shareの自動オンボーディングを有効にする必要がある場合は、代わりに以下のコマンドを実行してください。このオプションでは、管理者パスワードが要求されます。

     ```
     open <dmg_root>/Install.app --args --unattended --fss-onboarding-auto-start
     ```

   - CyberProtect_AgentForMac_web.dmgなどのMac用のユニバーサルインストーラを使用する場合、

以下のコマンドを実行してください。

```
sudo <dmg_root>/Install.app/Contents/MacOS/cyber_installer -a
```

5. インストールファイル（.dmg）のマウントを解除します。

```
hdiutil detach <dmg_root>
```

例

```
mkdir mydirectory
```

```
hdiutil attach /Users/JohnDoe/Cyber_Protection_Agent_for_MAC_x64.dmg -mountpoint
mydirectory
```

```
sudo installer -pkg mydirectory/Install.pkg -target LocalSystem
```

```
hdiutil detach mydirectory
```

エージェントをアンインストールするには

1. ターミナルを開きます。
2. 次のいずれかを実行します。
   - エージェントのインストール解除を行うには、次のコマンドを実行します。

     ```
     sudo /Library/Application\ Support/BackupClient/Acronis/Cyber\ Protect\ Agent\
     Uninstall.app/Contents/MacOS/AgentUninstall /confirm
     ```

   - エージェントをアンインストールして、すべてのログ、タスクおよび設定を削除するには、次のコマンドを実行します。

     ```
     sudo /Library/Application\ Support/BackupClient/Acronis/Cyber\ Protect\ Agent\
     Uninstall.app/Contents/MacOS/AgentUninstall /confirm /purge
     ```

macOSでの無人インストールに必要な許可

Macワークロードで無人インストールを開始する前に、ワークロードのmacOSでプライバシー設定のポリシーコントロールを変更して、アプリアクセスとカーネルおよびシステム拡張機能を許可する必要があります。これにより、Cyber Protectionエージェントのインストールが可能になります。カスタムPPPC（プライバシー設定のポリシーコントロール）ペイロードの配置、またはワークロードのグラフィカルユーザーインターフェースの環境設定で、これを実行できます。以下の許可が必要です。

macOS 11（Big Sur）以降での要件

タブ	セクション	フィールド	値

プライバシー設定のポリシーコントロール	アプリアクセス	ID	com.acronis.backup

		IDの種類	バンドルID
		コードの要件	identifier "com.acronis.backup" and anchor apple generic and certificate 1[field.1.2.840.113635.100.6.2.6] /* exists */ and certificate leaf[field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf[subject.OU] = ZU2TV78AA6
		アプリまたはサービス	SystemPolicyAllFiles
		ACCESS	許可
	アプリアクセス	ID	com.acronis.backup.aakore
		IDの種類	バンドルID
		コードの要件	identifier "com.acronis.backup.aakore" and anchor apple generic and certificate 1[field.1.2.840.113635.100.6.2.6] /* exists */ and certificate leaf[field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf[subject.OU] = ZU2TV78AA6
		アプリまたはサービス	SystemPolicyAllFiles
		ACCESS	許可
	アプリアクセス	特定済み	com.acronis.backup.activeprotection
		IDの種類	バンドルID
		コードの要件	identifier "com.acronis.backup.activeprotection" and anchor apple generic and certificate 1[field.1.2.840.113635.100.6.2.6] /* exists */ and certificate leaf[field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf[subject.OU] = ZU2TV78AA6
		アプリまたはサービス	SystemPolicyAllFiles
		ACCESS	許可
	アプリアクセス	ID	cyber-protect-service
		IDの種類	バンドルID
		コードの要件	identifier "cyber-protect-service" and anchor apple generic and certificate 1[field.1.2.840.113635.100.6.2.6] /* exists */ and certificate leaf[field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf[subject.OU] = ZU2TV78AA6
		アプリまたはサービス	SystemPolicyAllFiles
		ACCESS	許可

システム拡張		ユーザーがシステム拡張を承認できるようにする	有効、
	許可されたチームIDおよびシステム拡張	表示名	Acronisサイバープロテクションエージェントのシステム拡張
		システム拡張の種類	許可されたチームID
		チームID	ZU2TV78AA6

macOSバージョン11以前の要件

タブ	セクション	フィールド	値

プライバシー設定のポリシーコントロール	アプリアクセス	ID	com.acronis.backup

		IDの種類	バンドルID
		コードの要件	identifier "com.acronis.backup" and anchor apple generic and certificate 1[field.1.2.840.113635.100.6.2.6] /* exists */ and certificate leaf[field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf[subject.OU] = ZU2TV78AA6
		アプリまたはサービス	SystemPolicyAllFiles
		ACCESS	許可
	アプリアクセス	ID	com.acronis.backup.aakore
		IDの種類	バンドルID
		コードの要件	identifier "com.acronis.backup.aakore" and anchor apple generic and certificate 1[field.1.2.840.113635.100.6.2.6] /* exists */ and certificate leaf[field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf[subject.OU] = ZU2TV78AA6
		アプリまたはサービス	SystemPolicyAllFiles
		ACCESS	許可
	アプリアクセス	特定済み	com.acronis.backup.activeprotection
		IDの種類	バンドルID
		コードの要件	identifier "com.acronis.backup.activeprotection" and anchor apple generic and certificate 1[field.1.2.840.113635.100.6.2.6] /* exists */ and certificate leaf[field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf[subject.OU] = ZU2TV78AA6
		アプリまたはサービス	SystemPolicyAllFiles
		ACCESS	許可
	アプリアクセス	ID	cyber-protect-service
		IDの種類	バンドルID
		コードの要件	identifier "cyber-protect-service" and anchor apple generic and certificate 1[field.1.2.840.113635.100.6.2.6] /* exists */ and certificate leaf[field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf[subject.OU] = ZU2TV78AA6
		アプリまたはサービス	SystemPolicyAllFiles
		ACCESS	許可

承認されたカーネル拡張		ユーザーがカーネル拡張を承認できるようにする	有効、
		レガシーカーネル拡張を標準ユーザーが承認できるようにする（macOS 11以降）	有効、
	承認されたチームIDおよびカーネル拡張	承認されたチームID - 表示名	Acronisサイバープロテクションエージェントのカーネル拡張
		チームID	ZU2TV78AA6
		カーネル拡張のバンドルID	• com.acronis.systeminterceptors • com.acronis.ngscan • com.acronis.notifyframework
システム拡張		ユーザーがシステム拡張を承認できるようにする	有効、
	許可されたチームIDおよびシステム拡張	表示名	Acronisサイバープロテクションエージェントのシステム拡張
		システム拡張の種類	許可されたチームID
		チームID	ZU2TV78AA6

ワークロードの手動登録と登録解除

ワークロードにプロテクションエージェントをインストールすると、自動的にCyber Protectionサービスに登録されます。プロテクションエージェントをアンインストールすると、ワークロードは自動的に登録解除され、Cyber Protectコンソールで表示されなくなります。

また、コマンドラインインターフェースを使用して、手動でワークロードを登録することもできます。自動登録に失敗した場合や、ワークロードを新しいテナントや新しいユーザーアカウント移動させたい場合などに、手動登録が必要になります。

ユーザー名とパスワードを使用してワークロードを登録するには

Windowsの場合

コマンドラインで以下のコマンドを実行します。

```
"%ProgramFiles%\BackupClient\RegisterAgentTool\register_agent.exe" -o register -t cloud
-a <service address> -u <user name> -p <password>
```

例:

```
"C:\ProgramFiles\BackupClient\RegisterAgentTool\register_agent.exe" -o register -t cloud
-a https://cloud.company.com -u johndoe -p johnspassword
```

Linuxの場合

コマンドラインで以下のコマンドを実行します。

```
sudo "/usr/lib/Acronis/RegisterAgentTool/RegisterAgent" -o register -t cloud -a <service
address> -u <user name> -p <password>
```

例:

```
sudo "/usr/lib/Acronis/RegisterAgentTool/RegisterAgent" -o register -t cloud -a
https://cloud.company.com -u johndoe -p johnspassword
```

macOSの場合

コマンドラインで以下のコマンドを実行します。

```
sudo "/Library/Application Support/BackupClient/Acronis/RegisterAgentTool/RegisterAgent"
-o register -t cloud -a <service address> -u <user name> -p <password>
```

例:

```
sudo "/Library/Application Support/BackupClient/Acronis/RegisterAgentTool/RegisterAgent"
-o register -t cloud -a https://cloud.company.com -u johndoe -p johnspassword
```

注意
ワークロードを登録するアカウントのユーザー名とパスワードを使用します。パートナー管理者アカウントは使用できません。

サービスアドレスは、Cyber Protectionサービスへの**ログイン**に使用するURLです。例えば、`https://cloud.company.com`です。

重要
パスワードに記号やブランクスペースが含まれている場合は、"特殊文字やブランクスペースを使用したパスワード"（120ページ）を参照してください。

重要
macOS 10.14以降を使用している場合、プロテクションエージェントにフルディスクアクセスの権限を付与してください。これを実行するには、[**アプリケーション**] > [**ユーティリティ**] に移動して、[**Cyber Protectエージェントアシスタント**] を実行します。アプリケーションウィンドウの指示に従います。

登録トークンを使用してワークロードを登録するには

Windowsの場合

コマンドラインで以下のコマンドを実行します。

```
"%ProgramFiles%\BackupClient\RegisterAgentTool\register_agent.exe" -o register -t cloud
-a <service address> --token <registration token>
```

例:

```
"C:\ProgramFiles\BackupClient\RegisterAgentTool\register_agent.exe" -o register -t cloud
-a https://au1-cloud.company.com --token 3B4C-E967-4FBD
```

Linuxの場合

コマンドラインで以下のコマンドを実行します。

```
sudo "/usr/lib/Acronis/RegisterAgentTool/RegisterAgent" -o register -t cloud -a <service
address> --token <registration token>
```

例:

```
sudo "/usr/lib/Acronis/RegisterAgentTool/RegisterAgent" -o register -t cloud -a
https://eu2-cloud.company.com --token 34F6-8C39-4A5C
```

macOSの場合

コマンドラインで以下のコマンドを実行します。

```
sudo "/Library/Application Support/BackupClient/Acronis/RegisterAgentTool/RegisterAgent"
-o register -t cloud -a <service address> --token <registration token>
```

例:

```
sudo "/Library/Application Support/BackupClient/Acronis/RegisterAgentTool/RegisterAgent"
-o register -t cloud -a https://us5-cloud.company.com --token 9DBF-3DA9-4DAB
```

重要
macOS 10.14以降を使用している場合、プロテクションエージェントにフルディスクアクセスの権限を付与してください。これを実行するには、[**アプリケーション**] > [**ユーティリティ**] に移動して、[**Cyber Protectエージェントアシスタント**] を実行します。アプリケーションウィンドウの指示に従います。

仮想アプライアンス

1. 仮想アプライアンスのコンソールで、CTRL+SHIFT+F2キーでコマンドラインインターフェイスが開きます。
2. コマンド プロンプトで、次のコマンドを実行します。

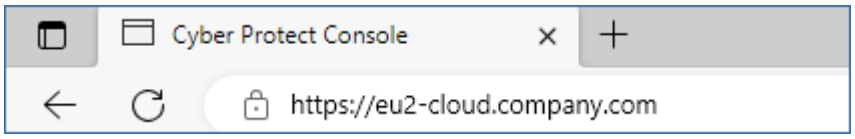
   ```
   register_agent -o register -t cloud -a <service address> --token <registration token>
   ```

例:

```
register_agent -o register -t cloud -a https://eu2-cloud.company.com --token 34F6-8C39-4A5C
```

3. Alt+F1キーを押して、アプライアンスのグラフィカルインターフェイスに戻ります。

注意
登録トークンを使用する場合は、実際のデータセンターのアドレスをそのまま指定しなければなりません。これは、Cyber Protectionサービスに**ログインした後**に表示されるURLです。たとえば、`https://eu2-cloud.company.com`です。



ここでは`https://cloud.company.com`を使用しないでください。

登録トークンは、12桁の文字列を3つのセグメントに分けて各セグメントをハイフンで区切る形式になっています。登録トークンを生成する詳しい方法については、"登録トークンの生成"（164ページ）を参照してください。

ワークロードの登録を解除するには

Windowsの場合

コマンドラインで以下のコマンドを実行します。

```
"%ProgramFiles%\BackupClient\RegisterAgentTool\register_agent.exe" -o unregister
```

例:

```
"C:\ProgramFiles\BackupClient\RegisterAgentTool\register_agent.exe" -o unregister
```

Linuxの場合

コマンドラインで以下のコマンドを実行します。

```
sudo "/usr/lib/Acronis/RegisterAgentTool/RegisterAgent" -o unregister
```

macOSの場合

コマンドラインで以下のコマンドを実行します。

```
sudo "/Library/Application Support/BackupClient/Acronis/RegisterAgentTool/RegisterAgent" -o unregister
```

仮想アプライアンス

1. 仮想アプライアンスのコンソールで、CTRL+SHIFT+F2キーでコマンドラインインターフェイスが開きます。
2. コマンド プロンプトで、次のコマンドを実行します。

```
register_agent -o unregister
```

3. Alt+F1キーを押して、アプライアンスのグラフィカルインターフェイスに戻ります。

ワークロードを別のテナントに移動

ワークロードを別のテナントに移動する処理は、ネイティブではサポートされていません。回避策として、ワークロードの登録を解除し、別のテナントに登録することができます。適用された保護計画はすべてそのワークロードから取り消され、元のテナントのクラウドストレージにあるバックアップへのアクセスも失われます。

新しいテナントまたは新しいユーザーアカウントでワークロードを登録する方法については、"ワークロードの登録を変更する"（121ページ）を参照してください。

特殊文字やブランクスペースを使用したパスワード

パスワードに特殊文字やブランクスペースが含まれている場合は、コマンドラインで入力するときにパスワードを引用符で囲んでください。

例えば、Windowsでは以下のコマンドを実行します。

コマンドテンプレート:

```
"%ProgramFiles%\BackupClient\RegisterAgentTool\register_agent.exe" -o register -t cloud
-a <service address> -u <user name> -p <"password">
```

コマンド例:

```
"C:\ProgramFiles\BackupClient\RegisterAgentTool\register_agent.exe" -o register -t cloud
-a https://cloud.company.com -u johndoe -p "johns password"
```

このコマンドでエラーが発生する場合、base64形式でパスワードをエンコードします（https://www.base64encode.org/を参照）。その後コマンドラインで、-bパラメータまたは--base64パラメータを使用して、そのエンコードしたパスワードを指定します。

例えば、Windowsでは以下のコマンドを実行します。

コマンドテンプレート:

```
"%ProgramFiles%\BackupClient\RegisterAgentTool\register_agent.exe" -o register -t cloud
-a <service address> -u <user name> -b -p <encoded password>
```

コマンド例:

```
"C:\ProgramFiles%\BackupClient\RegisterAgentTool\register_agent.exe" -o register -t
cloud -a https://cloud.company.com -u johndoe -b -p am9obnNwYXNzd29yZA==
```

ワークロードの登録を変更する

ワークロードの現在の登録内容を変更するには、新しいテナントまたは新しいユーザーアカウントから登録する必要があります。

重要
ワークロードの登録を変更すると、そのワークロードに適用されているすべての保護計画が取り消されます。ワークロードの保護を継続するには、新しい保護計画を適用します。

ワークロードを新しいテナントに登録すると、ワークロードから元のテナントのクラウドストレージにあるバックアップへのアクセスが失われます。クラウドストレージ以外のバックアップには、引き続きアクセスできます。

ワークロードの登録を変更するには、コマンドラインを使用するか、GUIインストーラを使用します。コマンドラインを使用する場合、エージェントのアンインストールは不要です。

ワークロードの登録を変更するには

コマンドラインを使用する

1. プロテクションエージェントの登録を解除します（"ワークロードの登録を解除するには"（119ページ）を参照）。
2. プロテクションエージェントを新しいテナントまたは新しいユーザーアカウントから登録します（"ユーザー名とパスワードを使用してワークロードを登録するには"（116ページ）または"登録トークンを使用してワークロードを登録するには"（117ページ）を参照）。

GUIインストーラを使用する

1. プロテクションエージェントをアンインストールします。
2. プロテクションエージェントをインストールして、新しいテナントまたは新しいユーザーアカウントから登録します。

エージェントをインストールおよび登録する方法については、"プロテクションエージェントをインストールする"（76ページ）を参照してください。

マシンの自動検出

自動検出を使用すると、次のことが可能になります。

- Active Directoryドメインやローカルネットワーク内のマシンを検出して、プロテクションエージェントのインストールやマシンの登録を自動化します。
- 複数のマシンにプロテクションエージェントをインストールし、アップデートできます。
- 大規模なActive Directoryドメイン内におけるリソースのプロビジョニングやマシン管理の負荷を軽減するために、Active Directoryとの同期を使用できます。

前提条件

自動検出を実行するには、ローカルネットワークまたはActive Directoryドメイン内に、プロテクションエージェントがインストールされたマシンが1台または複数台必要です。このエージェントは、検出エージェントとして使用されます。

重要
検出エージェントとして使用可能なのは、Windowsマシンにインストールされているエージェントのみです。現在の環境に検出エージェントが存在しない場合、**[デバイスを追加]** パネルの **[複数のデバイス]** オプションを使用することはできません。

エージェントのリモートインストールは、Windowsを搭載したマシンでのみサポートされています（Windows XPはサポートされていません）。Windows Server 2012 R2を実行しているマシンでリモートインストールを実行するには、このマシンにWindows Update KB2999226をインストールする必要があります。

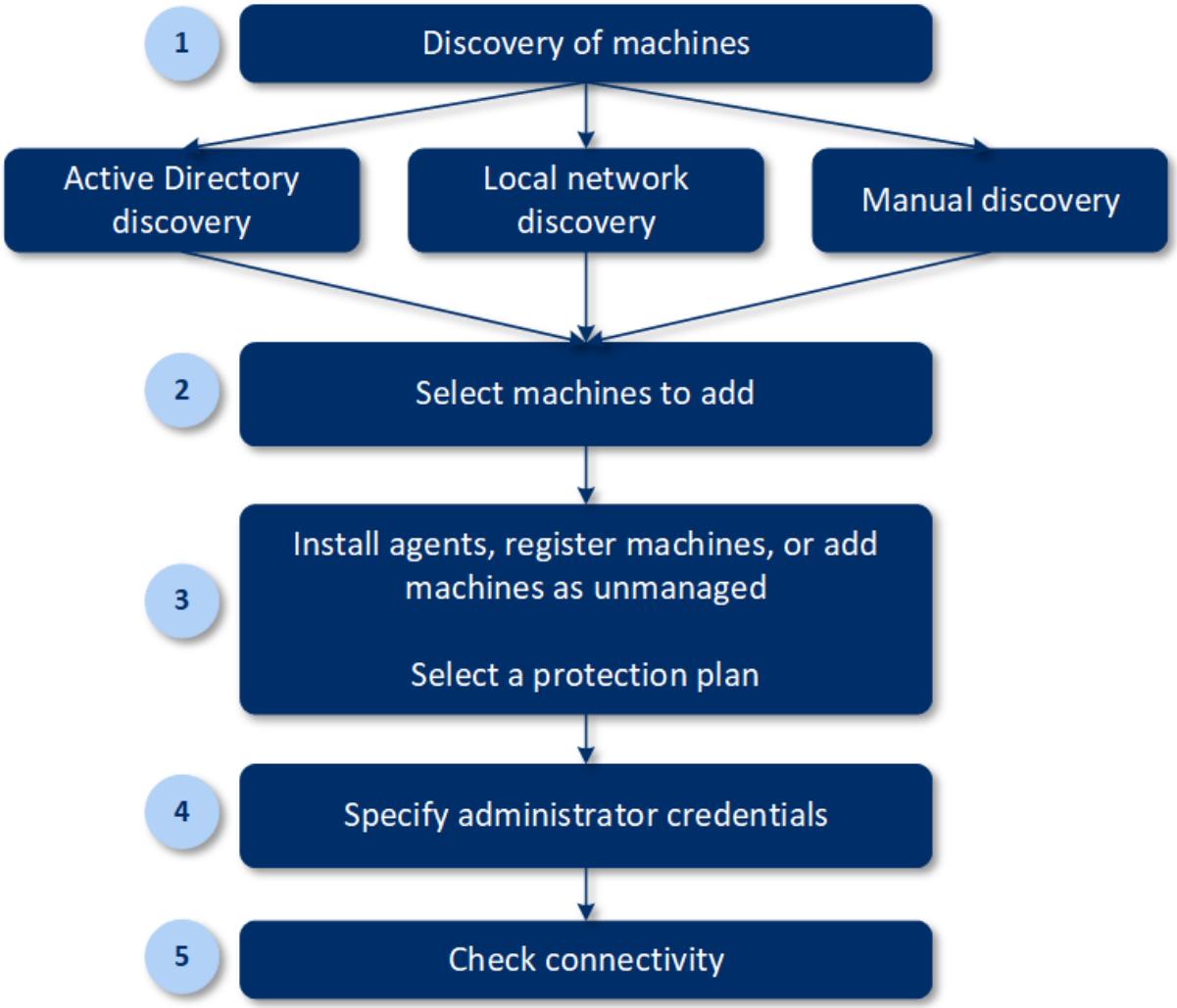
自動検出の仕組み

ローカルネットワーク検出において検出エージェントは、NetBIOS検出、Webサービス検出（WSD）、ARP（Address Resolution Protocol）テーブルを使用して、ネットワーク内の各マシンについて以下の情報を収集します。

- 名前（短縮/NetBIOSホスト名）
- 完全修飾ドメイン名（FQDN）
- ドメイン/ワークグループ
- IPv4/IPv6アドレス
- MACアドレス
- オペレーティングシステム（名前/バージョン/ファミリー）
- マシンカテゴリ（ワークステーション/サーバー/ドメインコントローラー）

Active Directory検出において検出エージェントは、上記のリストに加えて、マシンの組織単位（OU）に関する情報や、マシンの名前やオペレーティングシステムに関する詳細な情報を収集します。ただし、IPアドレスやMACアドレスは収集されません。

次の図は、自動検出のプロセスをまとめたものです。



1. 検出方法を選択します。
   - Active Directoryの検出
   - ローカルネットワークの検出
   - 手動検出 - マシンのIPアドレスまたはホスト名を使用するか、ファイルからマシンの一覧をインポートする

   Active Directory検出やローカルネットワーク検出の結果は、プロテクションエージェントがインストールされているマシンを除外します。

   手動検出中に、既存のプロテクションエージェントがアップデートされ、再登録されます。エージェントが登録されているのと同じアカウントを使用して自動検出を実行すると、エージェントは必ず最新バージョンにアップデートされます。別のアカウントを使用して自動検出を実行すると、エージェントは最新バージョンにアップデートされ、アカウントが属するテナントに再登録されます。
2. テナントに追加するマシンを選択します。
3. これらのマシンを追加する方法を選択します:
   - プロテクションエージェントと追加コンポーネントをマシンにインストールし、それらをCyber Protectコンソールに登録する。

- Cyber Protectコンソールでマシンを登録する（プロテクションエージェントが既にインストールされている場合）。
- プロテクションエージェントをインストールせずに、マシンを**非管理対象マシン**としてCyber Protectコンソールに追加する。

プロテクションエージェントをインストールするマシン、またはCyber Protectコンソールに登録するマシンに既存の保護計画を適用することもできます。

4. 選択したマシンの管理者資格情報を指定する。
5. 指定した資格情報でマシンに接続できることを確認します。

Cyber Protectコンソールに表示されるマシンは、次のカテゴリに分類されます。

- **検出済み** - 検出されたが、プロテクションエージェントがインストールされていないマシン。
- **管理対象** - プロテクション エージェントがインストールされたマシン。
- **保護されていない** - 保護計画が適用されていないマシン。保護されていないマシンには、保護計画が適用されていない検出済みマシンと管理対象のマシンの両方が含まれます。
- **保護されているマシン** - 保護計画が適用されたマシン。

エージェントのリモートインストールの仕組み

1. 検出エージェントは、検出ウィザードで指定されたホスト名、IPアドレス、および管理者の資格情報を使用してターゲットマシンに接続し、`web_installer.exe`ファイルをこれらのマシンにアップロードします。
2. `web_installer.exe`ファイルは、ターゲットマシンにおいて無人モードで実行されます。
3. ウェブインストーラーは、クラウドから追加のインストールパッケージを取得し、`msiexec`コマンドを使用してそれらをターゲットマシンにインストールします。
4. インストールが完了すると、コンポーネントはクラウドに登録されます。

注意
エージェントサービスの実行には、追加の許可が必要となるため、ドメインコントローラーエージェントのリモートインストールはサポートされていません。

自動検出と手動検出の実行

検出を始める前に、前提条件を満たしているかどうか確認します。

注意
エージェントサービスの実行には、追加の許可が必要となるため、ドメインコントローラー追加時の自動検出はサポートされていません。

マシンの検出手順

1. Cyber Protectコンソールで **[デバイス]** > **[すべてのデバイス]** に進みます。
2. **[追加]** をクリックします。
3. **[複数のデバイス]** で、**[Windowsのみ]** をクリックします。検出ウィザードが開きます。

4. （組織が部署に分かれている場合）部署を選択します。部署と子部署に関連付けられたエージェントを **[検出エージェント]** から選択できるようになります。
5. マシン検出のためスキャンを実行する検出エージェントを選択します。
6. 検出方法を選択します。
   - **Active Directoryを検索**。検出エージェントのあるマシンがActive Directoryドメインのメンバーであることを確認してください。
   - **ローカルネットワークをスキャン**。選択した検出エージェントでマシンを検出できなかった場合は、別の検出エージェントを選択してください。
   - **手動で指定するか、ファイルからインポート**。追加するマシンを手動で決定するか、テキストファイルからインポートします。
7. （検出方法にActive Directoryが選択されている場合）マシンの検索方法を選択します。
   - **組織単位（OU）リスト内**。追加するマシンのグループを選択します。
   - **LDAP方言クエリ**。LDAP方言クエリを使用してマシンを選択します。**[ベースを検索]** は検索する場所を指定します。**[フィルタ]** にはマシン選択の条件を指定できます。
8. 選択した検出方法に応じて、以下のいずれかのアクションを実行します。

検出方法	アクション
Active Directoryを検索	検出されたマシンの一覧から、追加するマシンを選択します。
ローカルネットワークをスキャン	検出されたマシンの一覧から、追加するマシンを選択します。

手動で指定するか、ファイルからインポート	マシンのIPアドレスかホスト名を指定します。または、テキストファイルからマシンリストをインポートします。ファイルには1行ごとにIPアドレス/ホスト名が含まれている必要があります。次にファイルの例を示します。
	`156.85.34.10`
	`156.85.53.32`
	`156.85.53.12`
	`EN-L00000100`
	`EN-L00000101`
	マシンのアドレスを手動で追加するか、ファイルからインポートした後、追加されたマシンに対してエージェントがpingを実行し、可用性を確認します。

9. 検出後に必ず実行するアクションを選択します。

オプション	説明
エージェントのインストールとマシ	**[コンポーネントの選択]** をクリックして、マシンにインストールするコンポーネントを選択できます。詳細については、"インストールするコンポーネントの選択"（129ページ）を参照してください。

オプション	説明
ンの登録	
エージェント サービスのログオンアカウント	この設定は、**[コンポーネントの選択]**画面で使用できます。 この設定によって、サービスが実行されるアカウントが決まります。 次のいずれかのオプションを選択できます。 • **サービスユーザーアカウントを使用する**（エージェントサービスのデフォルト） サービスユーザーアカウントは、サービスの実行に使用される Windows のシステムアカウントです。この設定の利点は、ドメインのセキュリティポリシーがそれらのアカウントのユーザー権限に影響を及ぼさないことです。デフォルトでは、エージェントは**ローカルシステム**のアカウントで実行されます。 • **新しいアカウントを作成する** エージェントのアカウント名は「Agent User」になります。 • **次のアカウントを使用する** ドメインコントローラー上にエージェントをインストールする場合は、エージェントに既存のアカウント（または同じアカウント）を指定するようシステムから求められます。セキュリティ上の理由で、システムはドメインコントローラー上に新しいアカウントを自動作成しません。 **[新しいアカウントを作成する]** または **[次のアカウントを使用する]** のオプションを選択する場合は、ドメインのセキュリティポリシーが、関連するアカウントの権限に影響を及ぼさないようにしてください。インストール中に割り当てられたユーザー権限がアカウントからなくなると、コンポーネントが不適切な動作をする、またはまったく動作しなくなる場合があります。
インストールされたエージェントでマシンを登録	マシンにエージェントが既にインストールされていて、Cyber Protectionでの登録のみ必要な場合、このオプションを使用します。マシンでエージェントが見つからない場合、**非管理**マシンとして追加されます。
非管理マシンとして追加	このオプションを選択すると、エージェントはマシンにインストールされません。コンソールでマシンを表示できるようになり、後からエージェントのインストールや登録を実行できます。
必要に応じてマシンを再起動	このオプションは、**[エージェントのインストールとマシンの登録]** が選択されていると表示されます。 このオプションを選択すると、インストールを完了するのに必要な回数だけ、マシンが再起動されます。 次のいずれかの場合に、マシンの再起動が必要になります。 • 前提条件のインストールが完了し、インストールを続行するには再起動が必要な場合。 • 前提条件のインストールが完了したが、インストール中に一部のファイルがロックされたため、再起動が必要な場合。 • インストールが完了したが、以前インストールされた他のソフトウェアの再起動が必要な場合。

オプション	説明
ユーザーのログイン中は再起動しない	このオプションは、**[必要に応じてマシンを再起動]** が選択されている場合に表示されます。 このオプションを選択すると、ユーザーがシステムにログインしていれば、マシンは自動的に再起動されません。例えば、インストールで再起動が必要になったときにユーザーが作業中であれば、システムは再起動されません。 前提条件がインストールされているにもかかわらず、ユーザーがログイン中であるために再起動が実行されなかった場合は、エージェントのインストールを完了させるため、マシンを再起動してインストールを再度開始する必要があります。 エージェントがインストールされた後、マシンが再起動されなかった場合は、マシンを再起動する必要があります。
マシンを登録する場所のユーザー	（組織内にユニットがある場合）マシンを登録するユニットまたは下位ユニットのユーザーアカウントを選択します。 （パートナーテナントレベルで自動検出を実行する場合）管理するカスタマーテナントの一覧で、ツリー構造を展開し、マシンを登録するユーザーアカウントを選択します。 （顧客管理者として自動検出を実行する場合）**[エージェントのインストールとマシンの登録]** または **イ[ンストールされたエージェントでマシンを登録]** を選択した場合、マシンに保護計画を適用するオプションもあります。複数の保護計画が存在する場合、使用するものを選択できます。

10. すべてのマシンに管理者権限を持つユーザーの資格情報を指定します。

重要
エージェントのリモートインストールが準備なしで機能するのは、組み込みの管理者アカウント（オペレーティングシステムのインストール時に最初に作成されたアカウント）の資格情報を指定した場合のみです。カスタム管理者の資格情報を複数指定する場合は、追加の準備手順を手動で実行する必要があります（"マシンを準備してリモートインストールする手順"（127ページ）を参照）。

11. すべてのマシンへの接続をシステムがチェックします。接続に失敗したマシンがある場合、それらのマシン用の資格情報を変更できます。

マシン検出が開始されると、対応するタスクの状況を **[監視]** > **[アクティビティ]** > **[マシンの検出]** アクティビティで確認できるようになります。

マシンを準備してリモートインストールする手順

- Windows 7以降のリモートのマシンで正常にインストールするには、マシン上で、**[コントロールパネル]** > **[フォルダオプション]** > **[表示]** > **[共有ウィザードの使用]**に進み、このオプションを無効にする必要があります。
- Active Directoryドメインのメンバーになっていないリモートのマシンに正常にインストールするには、該当のマシンでユーザーアカウント制御（UAC）を無効化する必要があります。無効化する方法の詳細については、「ユーザーアカウント制御（UAC）の要件」の「UACを無効化する方法」を参照してください。

- デフォルトでは、Windowsマシンへのリモートインストールには、ビルトインの管理者アカウントの資格情報が必要です。別の管理者アカウントの資格情報を使用してリモートインストールを実行するには、ユーザーアカウント制御（UAC）のリモート制限を無効化する必要があります。無効化する方法の詳細については、「ユーザーアカウント制御（UAC）の要件」の「UACのリモート制限を無効化する方法」を参照してください。
- [ファイルとプリンタの共有] が、リモートのコンピュータで [有効] になっている必要があります。このオプションにアクセスするには
  - Windows 2003 Serverが実行されているマシンの場合: **[コントロールパネル]** > **[Windowsファイアウォール]** > **[例外]** > **[ファイルとプリンタの共有]** を選択します。
  - Windows Server 2008、またはWindows 7以降が実行されているマシンの場合: **[コントロールパネル]** > **[Windowsファイアウォール]** > **[ネットワークと共有センター]** > **[共有の詳細設定の変更]** を選択します。
- Cyber Protectionのリモートインストールには、TCPポート445、25001、および43234が使用されます。

  [ファイルとプリンタの共有] を有効にすると、ポート445が自動的に開かれます。ポート 43234 および 25001 は、Windows ファイアウォールによって自動的に開かれます。Windows ファイアウォール以外のファイアウォールを使用する場合、これらの 3 つのポートが受信要求と送信要求の両方に対して開かれている（例外に追加されている）ことを確認してください。

  リモートインストールが完了すると、ポート25001は、Windowsファイアウォールによって自動的に閉じられます。今後エージェントをリモートでアップデートする場合は、ポート 445 と 43234 は開いたままにしておく必要があります。ポート25001は、アップデートのたびにWindowsファイアウォールによって自動的に開閉されます。別のファイアウォールを使用する場合は、3 つのポートをすべて開いたままにしておいてください。

ユーザー アクセス制御（UAC）の要件

Windows 7以降を実行し、Active Directoryドメインのメンバーになっていないマシンで、集中管理操作（リモートインストールを含む）を行うには、UACとUACのリモート制限が無効になっている必要があります。

UAC を無効にする手順は、次のとおりです。

オペレーティング システムに応じて次のいずれかを実行します。

- **Windows 8より前のWindowsオペレーティングシステム:**

  [コントロールパネル] > **[表示方法:小さいアイコン]** > **[ユーザーアカウント]** > **[ユーザーアカウント制御設定の変更]** を選択し、スライダを **[通知しない]** に移動します。次にコンピュータを再起動します。
- **任意のWindowsオペレーティングシステム**:
  1. レジストリ エディタを開きます。
  2. 次のレジストリキーを見つけます。**HKEY_LOCAL_MACHINE¥Software¥Microsoft¥Windows¥CurrentVersion¥Policies¥System**
  3. **EnableLUA**の設定値を**0**に変更します。
  4. コンピュータを再起動します。

UACのリモート制限を無効にする手順は、次のとおりです。

1. レジストリ エディタを開きます。
2. 次のレジストリキーを見つけます。**HKEY_LOCAL_MACHINE¥SOFTWARE¥Microsoft¥Windows¥CurrentVersion¥Policies¥System**
3. **LocalAccountTokenFilterPolicy**の設定値を**1**に変更します。
   LocalAccountTokenFilterPolicyの値が存在しない場合は、 DWORD（32ビット）として作成します。この値の詳細については、Microsoftのドキュメント（https://support.microsoft.com/en-us/help/951016/description-of-user-account-control-and-remote-restrictions-in-windows）を参照してください。

注意
セキュリティ上の理由から、管理処理（リモートインストールなど）を終了した後、両方の設定を元の状態に戻すことをお勧めします。**EnableLUA**=**1**および**LocalAccountTokenFilterPolicy**=**0**

インストールするコンポーネントの選択

必須コンポーネントと追加コンポーネントについては、次のテーブルに説明されています。

コンポーネント	説明
必須コンポーネント	
Windowsエージェント	このエージェントはディスク、ボリューム、ファイルをバックアップします。Windowsマシンにインストールされます。必ずインストールされます。オプションではありません。
その他のコンポーネント	
データ漏洩防止エージェント	このエージェントを使用すると、保護計画の下にあるマシンのローカルおよびリダイレクトされた周辺デバイス、ポート、クリップボードへのユーザーアクセスを制限することができます。選択された場合にインストールされます。
マルウェア対策およびURLフィルタ処理	このコンポーネントにより、保護計画でウイルス対策およびマルウェア対策保護モジュールとURLフィルタリングモジュールが利用可能になります。インストールしないことを選択した場合でも、これらのモジュールのいずれかがマシンの保護計画で有効になっていれば、後で自動的にインストールされます。
Hyper-Vエージェント	このエージェントはHyper-V仮想マシンをバックアップします。Hyper-Vホストにインストールされます。選択された場合、マシンでHyper-Vロールが検出された場合にインストールされます。
SQL エージェント	このエージェントはSQL Serverデータベースをバックアップします。Microsoft SQL Serverを実行中のマシンにインストールされます。選択された場合、およびマシンにアプリケーションが検出された場合にインストールされます。
Exchangeエージェント	このエージェントはExchangeデータベースとメールボックスをバックアップします。Microsoft Exchange Serverのメールボックスロールを実行中のマシンにインストールされます。選択された場合、およびマシンにアプリケーションが検出された場合にインストールされます。

エージェント for Active Directory	このエージェントはActive Directoryドメインサービスのデータをバックアップします。ドメインコントローラにインストールされます。選択された場合、およびマシンにアプリケーションが検出された場合にインストールされます。
エージェント for VMware（Windows）	このエージェントはVMware仮想マシンをバックアップします。vCenter Serverにネットワークアクセス可能なWindowsマシンにインストールされます。選択された場合にインストールされます。
Microsoft 365 エージェント	このエージェントはMicrosoft 365メールボックスをローカルにバックアップします。Windowsマシンにインストールされます。選択された場合にインストールされます。
Oracle エージェント	このエージェントはOracleデータベースをバックアップします。Oracle Databaseを実行中のマシンにインストールされます。選択された場合にインストールされます。
Cyber Protectionモニタ	このコンポーネントによって、ユーザーは通知領域内で実行中のタスクの実行を監視できます。Windowsマシンにインストールされます。選択された場合にインストールされます。 Windows 7 Service Pack 1以降、Windows 2008 Server R2 Service Pack 1以降をサポートします。

検出されたマシンの管理

検出プロセス実行後、検出されたマシンを **[デバイス]** > **[非管理マシン]** で確認できます。

このセクションは、使用された検出方法によってサブセクションに分かれています。マシンのパラメータの完全なリストを下に掲載します（パラメータは検出方法により異なります）。

名前	説明
名前	マシンの名前です。マシンの名前を検出できなかった場合は、IPアドレスが表示されます。
IPアドレス	マシンのIPアドレスです。
検出の種類	マシンの検出に使用された検出方法です。
組織単位（OU）	マシンが所属する、Active Directory内の組織単位（OU）です。この列は、**[非管理マシン]** > **[Active Directory]** でマシンの一覧を表示する場合にのみ表示されます。
オペレーティングシステム	マシンにインストールされたオペレーティングシステムです。

[例外] セクションには、検出プロセスでスキップさせるマシンを追加できます。たとえば、特定のマシンを検出させなくてよい場合、それらのマシンをこのリストに追加できます。

マシンを **[例外]** に追加するには、リストでマシンを選択し、**[例外に追加]** をクリックします。マシンを **[例外]** から削除するには、**[非管理マシン]** > **[例外]** に移動してマシンを選択し、**[例外から削除]** をクリックします。

Cyber Protectionで検出されたマシンにプロテクションエージェントをインストールし、一群のマシンを登録するには、それらをリストから選択し、**[インストールと登録]** をクリックします。開いたウィザードでは、一群のマシンに保護計画を割り当てることができます。

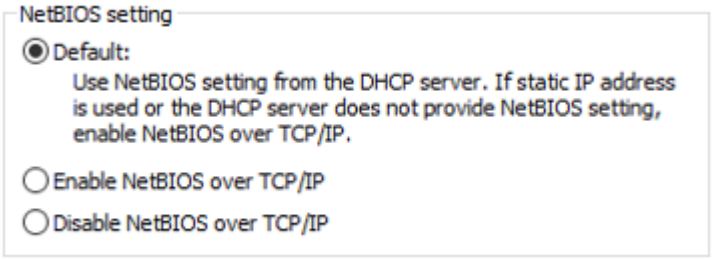
保護エージェントがマシンにインストールされると、それらのマシンが **[デバイス]** > **[エージェントがインストールされているマシン]** セクションに表示されます。

保護ステータスを確認するには、**[監視]** > **[概要]** に移動して **[保護ステータス]** ウィジェットまたは **[検出済みマシン]** ウィジェットを追加します。

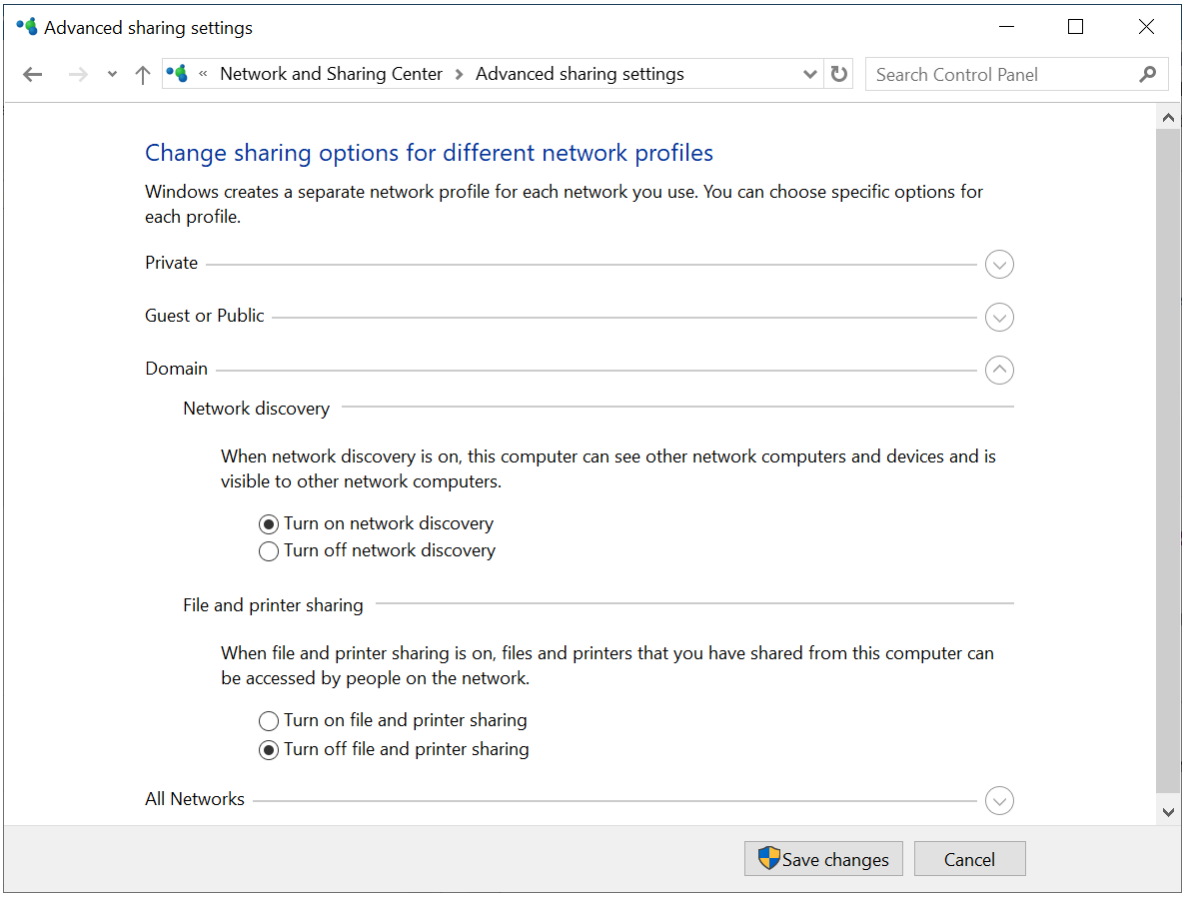
トラブルシューティング

自動検出機能に問題が発生した場合、次の点をチェックしてみてください。

- NetBIOS over TCP/IPが有効になっている、またはデフォルトに設定されているかを確認します。



- 「コントロールパネル¥ネットワークと共有センター¥共有の詳細設定」でネットワーク検出をオンにします。



- 検出を実行するマシンと検出先のマシンでFunction Discovery Provider Hostサービスが実行されていることを確認します。

- 検出先のマシンでFunction Discovery Resource Publicationサービスが実行されていることを確認します。

エージェント for VMware（仮想アプライアンス）の配置

開始する前に

エージェントのシステム要件

デフォルトでは、仮想アプライアンスには4GBのRAMと2個のvCPUが割り当てられ、ほとんどの操作にはこれで最適かつ十分です。

バックアップの作成速度を向上させ、RAMメモリの不足に関連する障害を回避するため、より高い負荷が想定されるケースでは、これらのリソースを16GBのRAMと4個のvCPUに増設することをお勧めします。例えば、バックアップトラフィックが1秒間に100MBを超えると予想される場合（10ギガビットネットワークなど）や、大容量ハードディスク（500GB以上）を搭載した複数の仮想マシンを同時にバックアップする場合は、割り当てリソースを増やしてください。

アプライアンス自体の仮想ディスクが占有するのは最大6GBです。ディスク形式がシックかシンかは無関係で、アプライアンスのパフォーマンスに影響しません。

いくつのエージェントが必要ですか。

1台の仮想アプライアンスでvSphere環境全体を保護できますが、ベストプラクティスは、vSphereクラスターごと（クラスターがない場合はホストごと）に1台の仮想アプライアンスをデプロイすることです。これは、アプライアンスがバックアップされたディスクをHotAddトランスポートを使用して接続でき、そのためバックアップトラフィックがあるローカルディスクから別のローカルディスクに向けられるため、バックアップを高速化できます。

仮想アプライアンスとVMwareエージェント（Windows）が同じvCenter Serverに接続されているか、または異なるESXiホストに接続されている場合、両方を同時に使用するのは正常です。1つのエージェントがESXiに直接接続されていて、別のエージェントがこのESXiを管理するvCenter Serverに接続されているケースは避けてください。

複数のエージェントがある場合、ローカル接続のストレージの使用（仮想アプライアンスに追加された仮想ディスクでのバックアップの保存）はお勧めしません。考慮事項については、"ローカルに接続されたストレージの使用"（674ページ）を参照してください。

エージェントの自動DRSを無効にする

仮想アプライアンスがvSphereクラスターにデプロイされている場合、それに対する自動vMotionを無効にします。クラスターDRS設定で、個々の仮想マシン自動化レベルを有効にして、仮想アプライアンスの **[自動化レベル]** を **[無効]** に設定します。

OVFテンプレートの配置

1. **[すべてのデバイス]** > **[追加]** > **[VMware ESXi]** > **[仮想アプライアンス（OVF）]** をクリックします。

   .zipアーカイブがマシンにダウンロードされます。
2. .zipアーカイブを展開します。フォルダには1つの.ovfファイルと2つの.vmdkファイルがあります。
3. vSphereクライアントを実行するマシンからこれらのファイルにアクセスできることを確認してください。
4. vSphereクライアントを起動し、vCenter Serverにログインします。
5. OVFテンプレートを配置します。
   - ストレージを構成するときは、共有データストアを選択します（存在する場合）。アプライアンスのパフォーマンスに影響しないため、ディスク形式がシックかシンかは無関係です。
   - ネットワーク接続を構成するとき、エージェントがクラウドで正しく登録されるように、インターネット接続が可能なネットワークを選択します。

仮想アプライアンスの設定

仮想アプライアンスを配置してから、vCenter ServerまたはESXiホストとCyber Protectionサービスにアクセスできるように構成を実行する必要があります。

仮想アプライアンスを構成する手順は、次のとおりです。

1. vSphereクライアントで、仮想アプライアンスマシンのコンソールを開きます。
2. ネットワーク接続が構成されたことを確認します。

   接続はDHCP（Dynamic Host Configuration Protocol）経由で自動的に構成されます。

   デフォルトの構成を変更するには、**[エージェントオプション]** 以下の **[eth0]** フィールドで **[変更]** をクリックして、ネットワーク設定を指定します。
3. 仮想アプライアンスをvCenter ServerまたはESXiホストに接続します。
   a. **[エージェントオプション]** 以下の **[vCenter/ESX(i)]** フィールドで **[変更]** をクリックして、次の値を指定します。
      - （vCenter Serverを使用する場合）vCenter Serverの名前またはIPアドレス。
      - （vCenter Serverを使用していない場合）仮想マシンをバックアップしてリカバリするESXiホストの名前またはIPアドレス。バックアップを高速化するには、同じホスト上に仮想アプライアンスを配置します。
      - アプライアンスがvCenter ServerまたはESXiホストに接続するために必要な資格情報。

        管理者ロールを割り当てられた既存のアカウントを使用するのではなく、vCenter ServerまたはESXiホストにアクセスするための専用アカウントを使用することをお勧めします。専用アカウントに必要な権限の詳細については、"VMware エージェント - 必要な権限"（681ページ）を参照してください。

   b. **[接続を確認]** をクリックして、設定が正しいことを確認します。
   c. **[OK]** をクリックします。
4. 以下のいずれかの方法で、アプライアンスをCyber Protectionサービスに登録します。

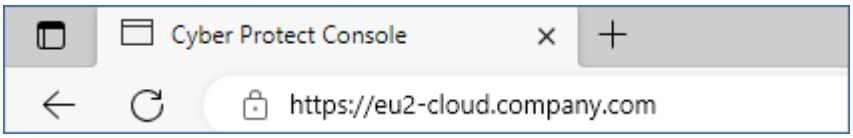
- （二要素認証を導入していないテナントのみ）グラフィカルインターフェイスでアプライアンスを登録します。
  a. **[エージェントオプション]** 以下の **[管理サーバー]** フィールドで、**[変更]** をクリックします。
  b. **[サーバー名/IP]** フィールドで **[クラウド]** を選択します。
     Cyber Protectionサービスのアドレスが表示されます。別途指示がある場合を除き、このアドレスは変更しないでください。
  c. **[ユーザー名]** および **[パスワード]** フィールドで、Cyber Protectionサービスのアカウントの資格情報を指定します。仮想アプライアンスとアプライアンスが管理する仮想マシンは、このアカウントに登録されます。
  d. **[OK]** をクリックします。
- コマンドラインインターフェイスでアプライアンスを登録します。

  注意
  この方法では、登録トークンが必要です。登録トークンを生成する方法の詳細については、"登録トークンの生成"（164ページ）を参照してください。

  a. CTRL+SHIFT+F2キーでコマンドラインインターフェイスが開きます。
  b. 次のコマンドを実行します。

  ```
  register_agent -o register -t cloud -a <service address> --token <registration token>
  ```

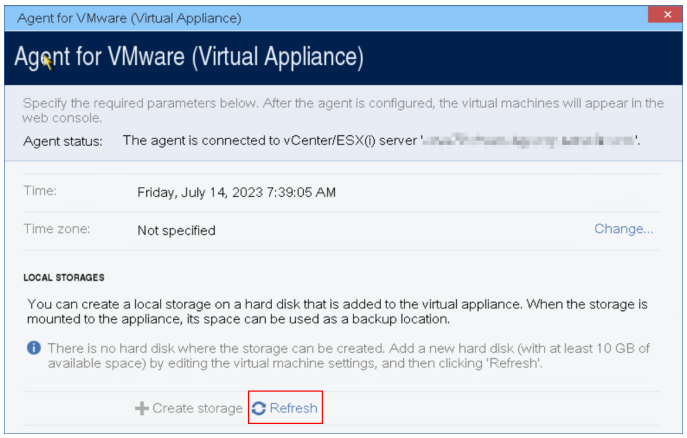
  注意
  登録トークンを使用する場合は、実際のデータセンターのアドレスをそのまま指定しなければなりません。これは、Cyber Protectコンソールに**ログインした後**に表示されるURLです。たとえば、`https://eu2-cloud.company.com`です。

  ここでは`https://cloud.company.com`を使用しないでください。

  c. Alt+F1キーを押して、アプライアンスのグラフィカルインターフェイスに戻ります。

5. （オプション） ローカルストレージを追加します。
   a. vSphereクライアントで、仮想アプライアンスに仮想ディスクを接続します。仮想ディスクには少なくとも10GBの空き容量が必要です。
   b. アプライアンスのグラフィカルユーザーインターフェイスで、**[リフレッシュ]** をクリックします。



[ストレージを作成] ボタンがアクティブになります。

c. **[ストレージを作成]** をクリックします。

d. ストレージのラベルを指定して、**[OK]** をクリックします。

e. **[はい]** をクリックしてこの選択内容を確認します。

6. （ネットワークでプロキシサーバーが有効にされている場合）プロキシサーバーを構成します。

a. CTRL+SHIFT+F2キーでコマンドラインインターフェイスが開きます。

b. **/etc/Acronis/Global.config**ファイルをテキストエディタで開きます。

c. 次のいずれかを実行します。

- エージェントインストール中にプロキシ設定を指定した場合は、次のセクションを見つけます。

```
<key name="HttpProxy">
    <value name="Enabled" type="Tdword">"1"</value>
    <value name="Host" type="TString">"ADDRESS"</value>
    <value name="Port" type="Tdword">"PORT"</value>
    <value name="Login" type="TString">"LOGIN"</value>
    <value name="Password" type="TString">"PASSWORD"</value>
</key>
```

- それ以外の場合は、上記の内容をコピーして、ファイルの`<registry name="Global">...</registry>`タグの間に貼り付けます。

d. `ADDRESS`は新しいプロキシサーバーホスト名/IPアドレスで置換し、`PORT`はポート番号の10進値で置換します。

e. プロキシサーバーで認証が必要な場合は、`LOGIN`と`PASSWORD`をプロキシサーバー資格情報と置き換えます。必要ない場合は、ファイルからこれらの行を削除します。

f. ファイルを保存します。

g. ファイル**/opt/acronis/etc/aakore.yaml**をテキストエディタで開きます。

h. **env**セクションを探し（または作成し）、以下の行を追加します。

```
env:
    http-proxy: proxy_login:proxy_password@proxy_address:port
    https-proxy: proxy_login:proxy_password@proxy_address:port
```

i. proxy_loginとproxy_passwordをプロキシサーバー資格情報と置き換えます。また、proxy_address:portをプロキシサーバーのアドレスとポート番号に置き換えます。

j. rebootコマンドを実行します。

注意

プロキシの背後に配置された仮想アプライアンスをアップデートできるようにするには、アプライアンスのconfig.yamlファイル（/opt/acronis/etc/va-updater/config.yaml）を編集し、ファイルの最下行に以下の行を追加して、現在の環境で固有の値を入力します。

```
httpProxy: http://<proxy_login>:<proxy_password>@<proxy_address>:<port>
```

例:

```
httpProxy: http://mylogin:mypassword@192.168.2.300:8080
```

Scale Computing HC3 エージェント（仮想アプライアンス）の配置

開始する前に

このアプライアンスはScale Computing HC3クラスターで配置する事前構成済みの仮想マシンです。クラスターのすべての仮想マシンのサイバープロテクションを管理できるプロテクション エージェントが含まれています。

エージェントのシステム要件

デフォルトでは、エージェントを含む仮想マシンは2基のvCPUと4GiBのRAMを使用します。これらの設定で、ほとんどの処理に十分対応できますが、Scale Computing HC3 Webインターフェースで仮想マシンを編集することも変更できます。

バックアップの作成速度を向上させ、RAMメモリの不足に関連する障害を回避するため、より高い負荷が想定されるケースでは、これらのリソースを4個のvCPUと8GiBのRAMに増設することをお勧めします。例えば、バックアップトラフィックが1秒間に100MBを超えると予想される場合（10ギガビットネットワークなど）や、大容量ハードディスク（500GB以上）を搭載した複数の仮想マシンを同時にバックアップする場合は、割り当てリソースを増やしてください。

アプライアンスの仮想ディスクのサイズは約9GBです。

いくつのエージェントが必要ですか。

単一のエージェントでクラスター全体を保護できます。ただしバックアップトラフィックの帯域幅負荷を分散する必要がある場合は、クラスター内に複数のエージェントを含めることができます。

クラスター内に複数のエージェントがある場合、仮想マシンはエージェント間で自動的に均等に配分されるため、各エージェントでほぼ同数のマシンを管理することになります。

エージェント間で負荷の不均衡が20%に達すると、自動で再配分が実行されます。これは、マシンまたはエージェントを追加または削除した後に発生する可能性があります。たとえば、スループットを向上させるためにより多くのエージェントが必要で、追加の仮想アプライアンスをクラスターに配置する必要があるとします。Management Serverは、最も適したコンピュータを新しいエージェントに割り当てます。これにより、古いエージェントの負荷は軽減されます。エージェントを管理サーバーから削除すると、エージェントに割り当てられたマシンは残りのエージェント間で再配分されます。ただし、エージェントが破損したり、Scale Computing HC3 クラスターから手動で削除されたりした場合には、この再配分は実行されません。再配分は、このようなエージェントをCyber Protectコンソールから削除しなければ開始されません。

どのエージェントが特定のマシンを管理しているかを確認するには

1. Cyber Protectコンソールで **[デバイス]** をクリックし、**[Scale Computing]** を選択します。
2. 表の右上にあるギアアイコンをクリックして 、**[システム]** の下にある **[エージェント]** チェックボックスを選択します。
3. 表示される列でエージェントの名前を確認してください。

QCOW2テンプレートのデプロイ

1. Cyber Protectionアカウントにログインします。
2. **[デバイス]** > **[すべてのデバイス]** > **[追加]** > **[Scale Computing HC3]** の順にクリックします。.zipアーカイブがマシンにダウンロードされます。
3. ZIPアーカイブを展開し、.qcow2ファイルと.xmlファイルを**ScaleAppliance**という名前のフォルダに保存します。
4. **ScaleAppliance**フォルダをネットワーク共有にアップロードし、Scale Computing HC3クラスターがそのフォルダにアクセスできることを確認します。
5. **VMの作成/編集**ロールを割り当てられた管理者として、Scale Computing HC3クラスターにログインします。Scale Computing HC3仮想マシンでの操作に必要なロールの詳細については、「"Scale Computing HC3 エージェント – 必要なロール"（140ページ）」を参照してください。
6. Scale Computing HC3 Webインターフェースで、**ScaleAppliance**フォルダから仮想マシンのテンプレートをインポートします。
   a. **[HC3 VMをインポート]** アイコンをクリックします。
   b. **[HC3 VMをインポート]** ウィンドウで以下を指定します。
      - 新しい仮想マシンの名前。
      - **ScaleAppliance**フォルダが配置されているネットワーク共有。
      - このネットワーク共有にアクセスするために必要なユーザー名とパスワード。
      - （オプション） 新しい仮想マシンのドメインタグ。
      - ネットワーク共有上の**ScaleAppliance**フォルダのパス。
   c. **[インポート]** をクリックします。

配置が完了したら、仮想アプライアンスを構成する必要があります。構成の方法については、「"仮想アプライアンスの設定"（138ページ）」を参照してください。

注意
クラスターで複数の仮想アプライアンスが必要な場合は、上記の手順を繰り返して、追加の仮想アプライアンスを配置します。Scale Computing HC3 Webインターフェースの **[VMのクローンを作成する]** オプションを使用して、既存の仮想アプライアンスのクローンを作成しないでください。

仮想アプライアンスの設定

仮想アプライアンスを配置した後、保護するScale Computing HC3クラスターとCyber Protectionサービスの両方に到達できるよう設定が必要です。

仮想アプライアンスを構成する手順は、次のとおりです。

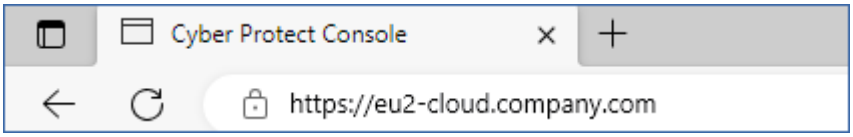
1. Scale Computing HC3 アカウントにログインします。
2. 構成したい仮想アプライアンスを選択し、**コンソール**アイコンをクリックします。
3. **[eth0]** フィールドで、アプライアンスのネットワークインターフェースを設定します。
   自動で割り当てられたDHCPアドレス（あれば）が、仮想マシンが使用するネットワーク内で有効であるかを確認するか、手動で割り当てます。アプライアンスが使用するネットワークの数に応じて、1つまたは複数のインターフェースを構成する場合があります。
4. **[Scale Computing]** フィールドで **[変更]** をクリックして、Scale Computing HC3クラスターのアドレスとアクセス用の資格情報を指定します。
   a. **[サーバー名/IP]** フィールドで、クラスターのDNS名またはIPアドレスを入力します。
   b. **[ユーザー名]** と **[パスワード]** のフィールドに、Scale Computing HC3管理者アカウントの資格情報を入力します。
      このアカウントにScale Computing HC3仮想マシンでの操作に必要なロールが割り当てられていることを確認してください。これらのロールの詳細については、「"Scale Computing HC3 エージェント – 必要なロール"（140ページ）」を参照してください。
   c. **[接続を確認]** をクリックして、設定が正しいことを確認します。
   d. **[OK]** をクリックします。
5. 以下のいずれかの方法で、アプライアンスをCyber Protectionサービスに登録します。
   - （二要素認証を導入していないテナントのみ）グラフィカルインターフェイスでアプライアンスを登録します。
     a. **[エージェントオプション]** 以下の **[管理サーバー]** フィールドで、**[変更]** をクリックします。
     b. **[サーバー名/IP]** フィールドで **[クラウド]** を選択します。
        Cyber Protectionサービスのアドレスが表示されます。別途指示がある場合を除き、このアドレスは変更しないでください。
     c. **[ユーザー名]** および **[パスワード]** フィールドで、Cyber Protectionサービスのアカウントの資格情報を指定します。仮想アプライアンスとアプライアンスが管理する仮想マシンは、このアカウントに登録されます。
     d. **[OK]** をクリックします。
   - コマンドラインインターフェイスでアプライアンスを登録します。

注意
この方法では、登録トークンが必要です。登録トークンを生成する方法の詳細については、"登録トークンの生成"（164ページ）を参照してください。

a. CTRL+SHIFT+F2キーでコマンドラインインターフェイスが開きます。
b. 次のコマンドを実行します。

```
register_agent -o register -t cloud -a <service address> --token <registration token>
```

注意
登録トークンを使用する場合は、実際のデータセンターのアドレスをそのまま指定しなければなりません。これは、Cyber Protectコンソールに**ログインした後**に表示されるURLです。たとえば、`https://eu2-cloud.company.com`です。



ここでは`https://cloud.company.com`を使用しないでください。

c. Alt+F1キーを押して、アプライアンスのグラフィカルインターフェイスに戻ります。

6. （オプション）**[名前]** フィールドで **[変更]** をクリックして、**localhost**となる仮想アプライアンスのデフォルト名を編集します。この名前はCyber Protectコンソールに表示されます。
7. （オプション）**[時間]** フィールドで **[変更]** をクリックして、ロケーションのタイムゾーンを選択し、該当する時刻にスケジュールされた処理が実行されることを確認します。
8. （ネットワークでプロキシサーバーが有効にされている場合）プロキシサーバーを構成します。
   a. CTRL+SHIFT+F2キーでコマンドラインインターフェイスが開きます。
   b. **/etc/Acronis/Global.config**ファイルをテキストエディタで開きます。
   c. 次のいずれかを実行します。
      - エージェントインストール中にプロキシ設定を指定した場合は、次のセクションを見つけます。

```
<key name="HttpProxy">
    <value name="Enabled" type="Tdword">"1"</value>
    <value name="Host" type="TString">"ADDRESS"</value>
    <value name="Port" type="Tdword">"PORT"</value>
    <value name="Login" type="TString">"LOGIN"</value>
    <value name="Password" type="TString">"PASSWORD"</value>
</key>
```

      - それ以外の場合は、上記の内容をコピーして、ファイルの`<registry name="Global">...</registry>`タグの間に貼り付けます。
   d. `ADDRESS`は新しいプロキシサーバーホスト名/IPアドレスで置換し、`PORT`はポート番号の10進値で置換します。

e. プロキシサーバーで認証が必要な場合は、LOGINとPASSWORDをプロキシサーバー資格情報と置き換えます。必要ない場合は、ファイルからこれらの行を削除します。
f. ファイルを保存します。
g. ファイル**/opt/acronis/etc/aakore.yaml**をテキストエディタで開きます。
h. **env**セクションを探し（または作成し）、以下の行を追加します。

```
env:
    http-proxy: proxy_login:proxy_password@proxy_address:port
    https-proxy: proxy_login:proxy_password@proxy_address:port
```

i. proxy_loginとproxy_passwordをプロキシサーバー資格情報と置き換えます。また、proxy_address:portをプロキシサーバーのアドレスとポート番号に置き換えます。
j. rebootコマンドを実行します。

注意
プロキシの背後に配置された仮想アプライアンスをアップデートできるようにするには、アプライアンスのconfig.yamlファイル（/opt/acronis/etc/va-updater/config.yaml）を編集し、ファイルの最下行に以下の行を追加して、現在の環境で固有の値を入力します。

```
httpProxy: http://<proxy_login>:<proxy_password>@<proxy_address>:<port>
```

例:

```
httpProxy: http://mylogin:mypassword@192.168.2.300:8080
```

Scale Computing HC3クラスター内の仮想マシンを保護するには

1. Cyber Protectionアカウントにログインします。
2. **[デバイス]** > **[Scale Computing HC3]** > <クラスター> の順に移動するか、**[デバイス]** > **[すべてのデバイス]** でマシンを検索します。
3. マシンを選択し、保護計画を適用します。

Scale Computing HC3 エージェント – 必要なロール

このセクションでは、Scale Computing HC3仮想マシンでの操作に必要なロールについて説明します。

操作	ロール
仮想マシンのバックアップ	バックアップ VM 作成/編集 VM 削除
既存の仮想マシン にリカバリする	バックアップ VM 作成/編集 VM 電源管理

	VM 削除 クラスター設定
新しい仮想マシンに復元する	バックアップ VM 作成/編集 VM 電源管理 VM 削除 クラスター設定

Virtuozzo Hybrid Infrastructureエージェント（仮想アプライアンス）の配置

開始する前に

このアプライアンスはVirtuozzo Hybrid Infrastructureで配置する事前構成済みの仮想マシンです。Virtuozzo Hybrid Infrastructureクラスターのすべての仮想マシンのサイバープロテクションを管理できるプロテクションエージェントが含まれています。

注意
[仮想マシンのボリュームシャドウコピーサービス（VSS）] バックアップオプションが有効化されているバックアップが、アプリケーションに関する一貫性のある状態で適切に実行およびデータキャプチャされるようにするには、Virtuozzoゲストツールが保護された仮想マシンにインストールされており最新の状態であることを確認します。

エージェントのシステム要件

仮想アプライアンスを配置する際には、vCPUsとRAMがさまざまに事前定義された組み合わせ（フレーバー）の中から選択できます。また、独自のフレーバーを作成することもできます。

ほとんどの操作で、2個のvCPUと4GBのRAM（ミディアムフレーバー）が十分かつ最適です。バックアップの作成速度を向上させ、RAMメモリの不足に関連する障害を回避するため、より高い負荷が想定されるケースでは、これらのリソースを4個のvCPUと8GBのRAMに増設することをお勧めします。例えば、バックアップトラフィックが1秒間に100MBを超えると予想される場合（10ギガビットネットワークなど）や、大容量ハードディスク（500GB以上）を搭載した複数の仮想マシンを同時にバックアップする場合は、割り当てリソースを増やしてください。

いくつのエージェントが必要ですか。

単一のエージェントでクラスター全体を保護できます。ただしバックアップトラフィックの帯域幅負荷を分散する必要がある場合は、クラスター内に複数のエージェントを含めることができます。

クラスター内に複数のエージェントがある場合、仮想マシンはエージェント間で自動的に均等に配分されるため、各エージェントでほぼ同数のマシンを管理することになります。

エージェント間で負荷の不均衡が20%に達すると、自動で再配分が実行されます。これは、マシンまたはエージェントを追加または削除した後に発生する可能性があります。たとえば、スループットを向上させるためにより多くのエージェントが必要で、追加の仮想アプライアンスをクラスターに配置する必要があるとします。Management Serverは、最も適したコンピュータを新しいエージェントに割り当てます。これにより、古いエージェントの負荷は軽減されます。エージェントを管理サーバーから削除すると、エージェントに割り当てられたマシンは残りのエージェント間で再配分されます。ただし、エージェントが破損したり、Virtuozzo Hybrid Infrastructureのノードから手動で削除されたりした場合には、この再配分は実行されません。再配分は、このようなエージェントをCyber ProtectionのWebインターフェースから削除しなければ開始されません。

どのエージェントが特定のマシンを管理しているかを確認するには

1. Cyber Protectコンソールで **[デバイス]** をクリックし、**[Virtuozzo Hybrid Infrastructure]** を選択します。
2. 表の右上にあるギアアイコンをクリックして 、**[システム]** の下にある **[エージェント]** チェックボックスを選択します。
3. 表示される列でエージェントの名前を確認してください。

制限事項

- Virtuozzo Hybrid Infrastructureアプライアンスはリモートで配置できません。
- 仮想マシンのアプリケーション認識型バックアップはサポートされていません。

Virtuozzo Hybrid Infrastructureのネットワーク構成

仮想アプライアンスの配置と構成に先立ち、Virtuozzo Hybrid Infrastructureでのネットワーク構成が必要です。

Virtuozzo Hybrid Infrastructureエージェント（仮想アプライアンス）のネットワーク要件

- 仮想アプライアンスでは、2つのネットワークアダプタが必要です。
- 仮想アプライアンスは、次のネットワークトラフィックタイプでVirtuozzoネットワークに接続する必要があります。
  - 計算API
  - VM のバックアップ
  - ABGWパブリック
  - VMパブリック

ネットワークの構成の詳細については、Virtuozzo文書の「コンピュートクラスターの要件」を参照してください。

Virtuozzo Hybrid Infrastructureのユーザーアカウント構成

仮想アプライアンスを構成するには、Virtuozzo Hybrid Infrastructureのユーザーアカウントが必要です。このアカウントには、**デフォルト**ドメインの**管理者**ロールが割り当てられます。ユーザーの詳細に

ついては、Virtuozzo Hybrid Infrastructure文書の「管理者パネルユーザーの管理」を参照してください。このアカウントに、**デフォルト** ドメインのすべてのプロジェクトへのアクセス権が付与されていることを確認してください。

デフォルトドメインのすべてのプロジェクトへのアクセス権を付与するには

1. システム管理者用の環境ファイルを作成します。これを行うには、OpenStackコマンドラインインターフェースを使用して、Virtuozzo Hybrid Infrastructureクラスターで次のスクリプトを実行します。このインターフェースへの接続方法の詳細については、Virtuozzo Hybrid Infrastructure文書の「OpenStackコマンドラインインターフェースへの接続」を参照してください。

   ```
   su - vstoradmin
   kolla-ansible post-deploy
   exit
   ```

2. 環境ファイルを使用して、さらにOpenStackコマンドを認証します。

   ```
   . /etc/kolla/admin-openrc.sh
   ```

3. 次のコマンドを実行します。

   ```
   openstack --insecure user set --project admin --project-domain Default --domain
   Default <username>
   openstack --insecure role add --domain Default --user <username> --user-domain
   Default compute --inherited
   ```

   ここで<username>は、**デフォルト**ドメインの**管理者**ロールが割り当てられたVirtuozzo Hybrid Infrastructureアカウントになります。仮想アプライアンスは、**デフォルト**ドメインに属するいずれかの子プロジェクトで仮想マシンをバックアップまたは復元するために、このアカウントを使用します。

例

```
su - vstoradmin
kolla-ansible post-deploy
exit
. /etc/kolla/admin-openrc.sh
openstack --insecure user set --project admin --project-domain Default --domain Default
johndoe
openstack --insecure role add --domain Default --user johndoe --user-domain Default
compute --inherited
```

デフォルトドメインではないドメインの仮想マシンでバックアップを管理するには、次のコマンドを実行します。

異なるドメインのすべてのプロジェクトへのアクセス権を付与するには

```
openstack --insecure role add --domain <domain name> --inherited --user <username> --
user-domain Default admin
```

この<domain name>は、<username>アカウントにアクセス権を付与するプロジェクトのドメインになります。

例

```
openstack --insecure role add --domain MyNewDomain --inherited --user johndoe --user-
domain Default admin
```

プロジェクトへのアクセスを許可した後、アカウントに割り当てられているロールを確認します。

割り当てられたロールを確認するには

```
openstack --insecure role assignment list --user <username> --names
```

ここで<username>は、Virtuozzo Hybrid Infrastructureアカウントになります。

例

```
openstack --insecure role assignment list --user johndoe --names -c Role -c User -c
Project -c Domain
+--------------+-----------------+---------+-------------+
| Role         | User            | Project | Domain      |
+--------------+-----------------+---------+-------------+
| admin        | johndoe@Default |         | MyNewDomain |
| compute      | johndoe@Default |         | Default     |
| domain_admin | johndoe@Default |         | Default     |
| domain_admin | johndoe@Default |         | Default     |
+--------------+-----------------+---------+-------------+
```

この例では、ページに合わせてコマンド出力を簡略化するために、`-c Role`、`-c User`、`-c Project`、`-c Domain`オプションが使用されます。

すべてのプロジェクトでアカウントに割り当てられている有効なロールを確認するには、次のコマンドも実行します。

すべてのプロジェクトで有効なロールを確認するには

```
openstack --insecure role assignment list --user <username> --names --effective
```

ここで<username>は、Virtuozzo Hybrid Infrastructureアカウントになります。

例

```
openstack --insecure role assignment list --user johndoe --names --effective  -c Role -c
User -c Project -c Domain
+--------------+-----------------+-----------------+---------+
| Role         | User            | Project         | Domain  |
+--------------+-----------------+-----------------+---------+
```

```
| domain_admin | johndoe@Default |                 | Default |
| compute      | johndoe@Default | admin@Default   |         |
| compute      | johndoe@Default | service@Default |         |
| domain_admin | johndoe@Default | admin@Default   |         |
| domain_admin | johndoe@Default | service@Default |         |
| project_user | johndoe@Default | service@Default |         |
| member       | johndoe@Default | service@Default |         |
| reader       | johndoe@Default | service@Default |         |
| project_user | johndoe@Default | admin@Default   |         |
| member       | johndoe@Default | admin@Default   |         |
| reader       | johndoe@Default | admin@Default   |         |
| project_user | johndoe@Default |                 | Default |
| member       | johndoe@Default |                 | Default |
| reader       | johndoe@Default |                 | Default |
+--------------+-----------------+-----------------+---------+
```

この例では、ページに合わせてコマンド出力を簡略化するために、`-c Role`、`-c User`、`-c Project`、`-c Domain`オプションが使用されます。

QCOW2テンプレートのデプロイ

1. Cyber Protectionアカウントにログインします。
2. **[デバイス]** > **[すべてのデバイス]** > **[追加]** > **[Virtuozzo Hybrid Infrastructure]** の順にクリックします。

   .zipアーカイブがマシンにダウンロードされます。
3. .zipアーカイブを展開します。展開すると、.qcow2のイメージファイルが入っています。
4. Virtuozzo Hybrid Infrastructureアカウントにログインします。
5. Virtuozzo Hybrid Infrastructureの計算クラスターへの.qcow2イメージファイル追加は、以下の手順で行います。
   - **[計算]** > **[仮想マシン]** > **[イメージ]** タブで、**[イメージを追加]** をクリックします。
   - **[イメージを追加]** ウィンドウで、**[参照]** をクリックして.qcow2ファイルを選択します。
   - イメージ名を指定し、OSの種類に **[Generic Linux OS]** タイプを選択した上で、**[追加]** をクリックします。
6. **[計算]** > **[仮想マシン]** > **[仮想マシン]** タブで、**[仮想マシンを作成]** をクリックします。開いたウィンドウで、以下のパラメータを指定します。
   - 新しい仮想マシンの名前。
   - **[配置元]** で、**[イメージ]** を選択します。
   - **[イメージ]** ウィンドウで、アプライアンスの.qcow2イメージファイル選択し、**[完了]** をクリックします。
   - **[ボリューム]** ウィンドウでは、ボリュームを追加する必要はありません。システムディスクに自動で追加されるボリュームで十分です。
   - **[フレーバー]** ウィンドウで、vCPUsとRAMの任意の組み合わせを選択し、**[完了]** をクリックします。通常はvCPUが2つと4GiBのRAMで十分です。

- **[ネットワークインターフェース]** ウィンドウで **[追加]** をクリックします。パブリックタイプの仮想ネットワークインターフェースを選択した上で、**[追加]** をクリックします。そのインターフェースが **[ネットワークインターフェース]** リストに表示されます。
  複数の物理ネットワーク（したがって、パブリックタイプの仮想ネットワークが複数ある）でセットアップを行う場合は、この手順を繰り返し、必要な仮想ネットワークを選択します。

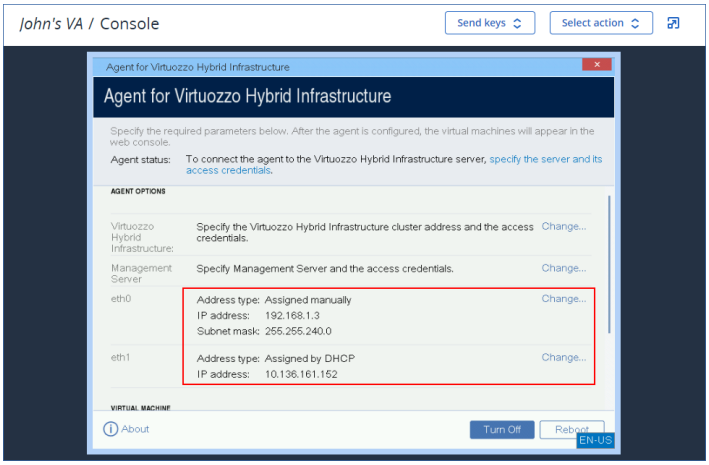
7. **[完了]** をクリックします。
8. **[仮想マシンを作成]** ウィンドウに戻り、**[デプロイ]** をクリックして、仮想マシンを作成し起動します。

仮想アプライアンスの設定

Virtuozzo Hybrid Infrastructureエージェント（仮想アプライアンス）を配置した後、仮想アプライアンスが、保護対象のVirtuozzo Hybrid InfrastructureクラスターとCyber Protectionクラウドサービスの両方に到達できるように設定する必要があります。

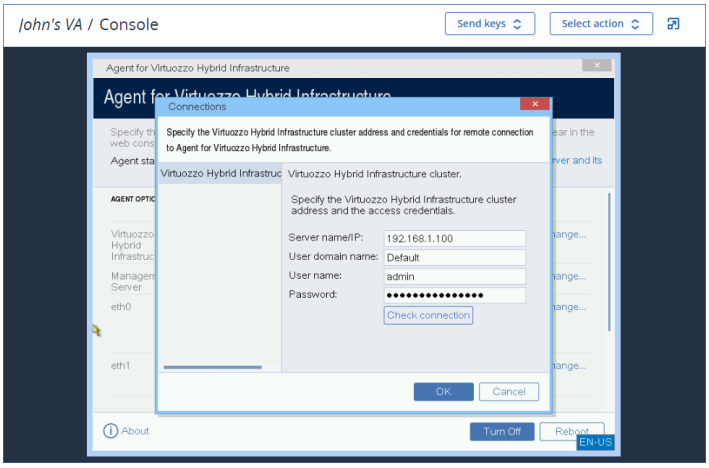
仮想アプライアンスを構成する手順は、次のとおりです。

1. Virtuozzo Hybrid Infrastructureアカウントにログインします。
2. **[計算]** > **[仮想マシン]** > **[仮想マシン]** タブで、作成した仮想マシンをクリックします。次に、**[コンソール]** をクリックします。
3. アプライアンスのネットワークインターフェースを設定します。構成するインターフェースが複数ある場合がありますが、これは、アプライアンスが使用する仮想ネットワークの数によって異なります。自動で割り当てられたDHCPアドレス（あれば）が、仮想マシンが使用するネットワーク内で有効であるかを確認するか、手動で割り当てます。



4. Virtuozzoクラスターのアドレスと資格情報を指定します。
   - Virtuozzo Hybrid InfrastructureクラスターのFQDNまたはIPアドレスを指定します。これは、クラスター管理ノードのアドレスです。デフォルトのポート5000が自動で設定されます。別のポートを使用する場合は、手動で指定する必要があります。
   - **[ユーザードメイン名]** フィールドで、Virtuozzo Hybrid Infrastructureで使用しているドメインを指定します。たとえば、**デフォルト**を指定します。
     ドメイン名では大文字と小文字が区別されます。

- **[ユーザー名]** と **[パスワード]** のフィールドに、指定したドメインで**管理者**のロールを持つVirtuozzo Hybrid Infrastructureユーザーアカウントの資格情報を入力します。ユーザー、ロール、ドメインの詳細については、「Virtuozzo Hybrid Infrastructureのユーザーアカウント構成」を参照してください。



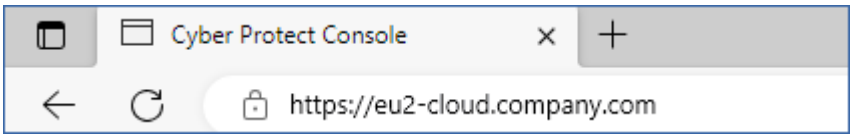
5. 以下のいずれかの方法で、アプライアンスをCyber Protectionサービスに登録します。
   - （二要素認証を導入していないテナントのみ）グラフィカルインターフェイスでアプライアンスを登録します。
     a. **[エージェントオプション]** 以下の **[管理サーバー]** フィールドで、**[変更]** をクリックします。
     b. **[サーバー名/IP]** フィールドで **[クラウド]** を選択します。
        Cyber Protectionサービスのアドレスが表示されます。別途指示がある場合を除き、このアドレスは変更しないでください。
     c. **[ユーザー名]** および **[パスワード]** フィールドで、Cyber Protectionサービスのアカウントの資格情報を指定します。仮想アプライアンスとアプライアンスが管理する仮想マシンは、このアカウントに登録されます。
     d. **[OK]** をクリックします。
   - コマンドラインインターフェイスでアプライアンスを登録します。

     注意
     この方法では、登録トークンが必要です。登録トークンを生成する方法の詳細については、"登録トークンの生成"（164ページ）を参照してください。

     a. CTRL+SHIFT+F2キーでコマンドラインインターフェイスが開きます。
     b. 次のコマンドを実行します。

```
register_agent -o register -t cloud -a <service address> --token <registration token>
```

注意
登録トークンを使用する場合は、実際のデータセンターのアドレスをそのまま指定しなければなりません。これは、Cyber Protectコンソールに**ログインした後**に表示されるURLです。たとえば、`https://eu2-cloud.company.com`です。



ここでは`https://cloud.company.com`を使用しないでください。

c. Alt+F1キーを押して、アプライアンスのグラフィカルインターフェイスに戻ります。

6. （ネットワークでプロキシサーバーが有効にされている場合）プロキシサーバーを構成します。
   a. CTRL+SHIFT+F2キーでコマンドラインインターフェイスが開きます。
   b. **/etc/Acronis/Global.config**ファイルをテキストエディタで開きます。
   c. 次のいずれかを実行します。
      - エージェントインストール中にプロキシ設定を指定した場合は、次のセクションを見つけます。

```
<key name="HttpProxy">
    <value name="Enabled" type="Tdword">"1"</value>
    <value name="Host" type="TString">"ADDRESS"</value>
    <value name="Port" type="Tdword">"PORT"</value>
    <value name="Login" type="TString">"LOGIN"</value>
    <value name="Password" type="TString">"PASSWORD"</value>
</key>
```

      - それ以外の場合は、上記の内容をコピーして、ファイルの`<registry name="Global">...</registry>`タグの間に貼り付けます。
   d. `ADDRESS`は新しいプロキシサーバーホスト名/IPアドレスで置換し、`PORT`はポート番号の10進値で置換します。
   e. プロキシサーバーで認証が必要な場合は、`LOGIN`と`PASSWORD`をプロキシサーバー資格情報と置き換えます。必要ない場合は、ファイルからこれらの行を削除します。
   f. ファイルを保存します。
   g. ファイル**/opt/acronis/etc/aakore.yaml**をテキストエディタで開きます。
   h. **env**セクションを探し（または作成し）、以下の行を追加します。

```
env:
    http-proxy: proxy_login:proxy_password@proxy_address:port
    https-proxy: proxy_login:proxy_password@proxy_address:port
```

   i. `proxy_login`と`proxy_password`をプロキシサーバー資格情報と置き換えます。また、`proxy_address:port`をプロキシサーバーのアドレスとポート番号に置き換えます。
   j. `reboot`コマンドを実行します。

注意

プロキシの背後に配置された仮想アプライアンスをアップデートできるようにするには、アプライアンスのconfig.yamlファイル（/opt/acronis/etc/va-updater/config.yaml）を編集し、ファイルの最下行に以下の行を追加して、現在の環境で固有の値を入力します。

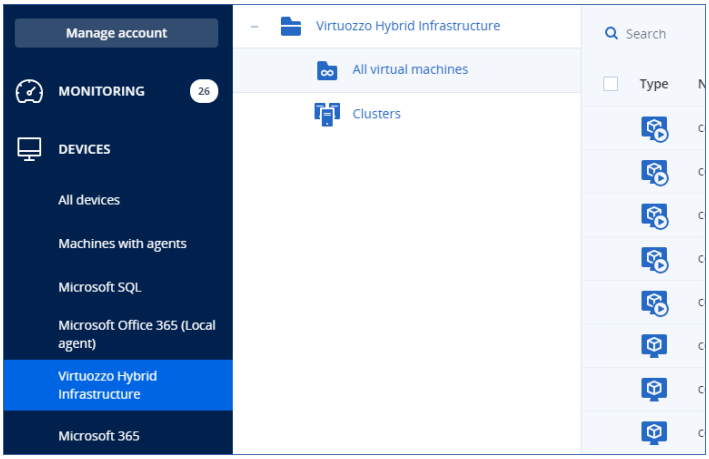
```
httpProxy: http://<proxy_login>:<proxy_password>@<proxy_address>:<port>
```

例:

```
httpProxy: http://mylogin:mypassword@192.168.2.300:8080
```

Virtuozzo Hybrid Infrastructureクラスター内の仮想マシンを保護する手順

1. Cyber Protectionアカウントにログインします。
2. **[デバイス]** > **[Virtuozo Hybrid Infrastructure]** > <お使いのクラスター> > **[デフォルトプロジェクト]** > **[管理者]** の順に移動するか、**[デバイス]** > **[すべてのデバイス]** でマシンを検索します。
3. マシンを選択し、保護計画を適用します。



oVirt（仮想アプライアンス）エージェントをデプロイ中

開始する前に

このアプライアンスはRed Hat Virtualization/oVirtデータセンターで配置する事前構成済みの仮想マシンです。アプライアンスには、データセンターに存在するすべての仮想マシンのサイバープロテクションを管理できるプロテクションエージェントが含まれています。

エージェントのシステム要件

デフォルトでは、エージェントを含む仮想マシンは2基のvCPUと4GiBのRAMを使用します。これらの設定で、ほとんどの処理に十分対応できますが、Red Hat Virtualization/oVirt管理ポータルで編集することもできます。

バックアップの作成速度を向上させ、RAMメモリの不足に関連する障害を回避するため、より高い負荷が想定されるケースでは、これらのリソースを4個のvCPUと8GiBのRAMに増設することをお勧めします。例えば、バックアップトラフィックが1秒間に100MBを超えると予想される場合（10ギガビットネットワークなど）や、大容量ハードディスク（500GB以上）を搭載した複数の仮想マシンを同時にバックアップする場合は、割り当てリソースを増やしてください。

アプライアンスの仮想ディスクのサイズは8GiBです。

いくつのエージェントが必要ですか。

単一のエージェントでデータセンター全体を保護できます。ただしバックアップトラフィックの帯域幅負荷を分散する必要がある場合は、データセンター内に複数のエージェントを含めることができます。

データセンター内に複数のエージェントがある場合、仮想マシンはエージェント間で自動的に配分されるため、各エージェントでほぼ同数のマシンを管理することになります。

エージェント間で負荷の不均衡が20%に達すると、自動で再配分が実行されます。これは、マシンまたはエージェントを追加または削除した後に発生する可能性があります。たとえば、スループットを向上させるためにより多くのエージェントが必要で、追加の仮想アプライアンスをデータセンターに配置する必要があるとします。Management Serverは、最も適したコンピュータを新しいエージェントに割り当てます。これにより、古いエージェントの負荷は軽減されます。エージェントを削除すると、エージェントに割り当てられたマシンが残りのエージェントの間で再配分されます。ただし、エージェントが破損したり、Red Hat Virtualization/oVirt管理ポータルから手動で削除されたりした場合には、この再配分は実行されません。再配分は、このようなエージェントをCyber Protectコンソールから削除しなければ開始されません。

どのエージェントが特定のマシンを管理しているかを確認するには

1. Cyber Protectコンソールで **[デバイス]** をクリックし、**[oVirt]** を選択します。
2. 表の右上にあるギアアイコンをクリックして 、**[システム]** の下にある **[エージェント]** チェックボックスを選択します。
3. 表示される列でエージェントの名前を確認してください。

制限事項

以下の操作は、Red Hat Virtualization/oVirt仮想マシンではサポートされていません。

- アプリケーション認識型バックアップ
- バックアップから仮想コンピュータを実行する
- 仮想コンピュータのレプリケーション
- Changed Block Tracking

OVAテンプレートの配置

1. Cyber Protectionアカウントにログインします。
2. **[デバイス]** > **[すべてのデバイス]** > **[追加]** > **[Red Hat Virtualization（oVirt）]** の順にクリックします。

.zipアーカイブがマシンにダウンロードされます。

3. ZIPアーカイブを展開します。アーカイブには.ovaファイルが1つ含まれています。
4. 保護したいRed Hat Virtualization/oVirtデータセンターのホストに、.ovaファイルをアップロードします。
5. 管理者としてRed Hat Virtualization/oVirt管理ポータルにログインします。仮想マシンでの操作に必要なロールの詳細については、「"oVirtエージェント - 必要なロールとポート"（154ページ）」を参照してください。
6. ナビゲーションメニューから、**[計算]** > **[仮想マシン]** を選択します。
7. メインテーブルの上にある縦の省略記号アイコン  をクリックしてから、**[インポート]** をクリックします。
8. **[仮想マシンをインポート]** ウィンドウで以下の手順を実行します。
   a. **[データセンター]** で、保護したいデータセンターを選択します。
   b. **[ソース]** で、**[仮想アプライアンス（OVA）]** を選択します。
   c. **[ホスト]** で、.ovaファイルをアップロードしたホストを選択します。
   d. **[ファイルパス]** で、.ovaファイルを含むディレクトリへのパスを指定します。
   e. **[読み込み]** をクリックします。
      .ovaファイルのoVirt仮想アプライアンステンプレートが、**ソース上の仮想マシン**パネルに表示されます。
      テンプレートがこのパネルに表示されない場合は、ファイルへの正しいパスが指定されていること、ファイルが破損していないこと、およびホストにアクセスできることを確認してください。
   f. **ソース上の仮想マシン**で、oVirt仮想アプライアンステンプレートを選択し、右矢印をクリックします。
      テンプレートは、**[インポートする仮想マシン]** パネルに表示されます。
   g. **[次へ]** をクリックします。
9. 新しいウィンドウで、アプライアンス名をクリックして、次の設定を構成します。
   - **[ネットワークインターフェース]** タブで、ネットワークインターフェースを構成します。
   - （オプション）**[一般]** タブで、エージェントを使用して仮想マシンのデフォルト名を変更します。

これで配置は完了です。次に、仮想アプライアンスを構成する必要があります。構成の方法については、「"仮想アプライアンスの設定"（152ページ）」を参照してください。

注意
データセンターに複数の仮想アプライアンスが必要な場合は、上記の手順を繰り返して、追加の仮想アプライアンスを配置します。Red Hat Virtualization/oVirt管理ポータルの **[VMのクローンを作成する]** オプションを使用して、既存の仮想アプライアンスのクローンを作成しないでください。

仮想アプライアンスをダイナミックグループバックアップから除外するには、Cyber Protectコンソールの仮想マシンのリストでも仮想アプライアンスを除外する必要があります。これを除外するには、Red Hat Virtualization/oVirt管理ポータルで、エージェントを含む仮想マシンを選択し、その仮想マシンにタグ`acronis_virtual_appliance`を割り当てます。

仮想アプライアンスの設定

仮想アプライアンスを配置した後、oVirtエンジンとCyber Protectionサービスの両方に到達できるよう設定が必要です。

仮想アプライアンスを構成する手順は、次のとおりです。

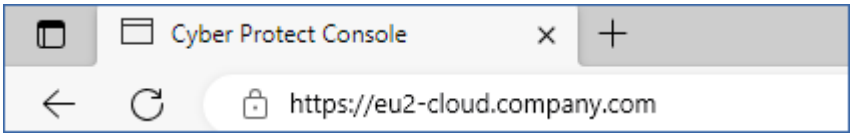
1. Red Hat Virtualization/oVirt管理ポータルにログインします。
2. 構成したい仮想アプライアンスを選択し、**コンソール**アイコンをクリックします。
3. **[eth0]** フィールドで、アプライアンスのネットワークインターフェースを設定します。
   自動で割り当てられたDHCPアドレス（あれば）が、仮想マシンが使用するネットワーク内で有効であるかを確認するか、手動で割り当てます。アプライアンスが使用するネットワークの数に応じて、1つまたは複数のインターフェースを構成する場合があります。
4. **[oVirt]** フィールドで **[変更]** をクリックして、oVirtエンジンのアドレスとアクセス用の資格情報を指定します。
   a. **[サーバー名/IP]** フィールドで、エンジンのDNS名またはIPアドレスを入力します。
   b. **[ユーザー名]** と **[パスワード]** のフィールドに、このエンジンの管理者資格情報を入力します。
      この管理者アカウントに、Red Hat Virtualization/oVirt仮想マシンでの操作に必要なロールがあることを確認してください。これらのロールの詳細については、「"oVirtエージェント - 必要なロールとポート"（154ページ）」を参照してください。
      oVirtエンジンのシングルサインオン（SSO）プロバイダーが、Keycloakになっている場合（oVirt 4.5.1のデフォルト）、ユーザー名を指定するときにKeycloak形式を使用します。例えば、デフォルトの管理者アカウントを`admin@internal`ではなく、`admin@ovirt@internalsso`のように指定します。
   c. （オプション）**[接続の確認]** をクリックして、指定した資格情報が正しいかどうかを確認します。
   d. **[OK]** をクリックします。
5. 以下のいずれかの方法で、アプライアンスをCyber Protectionサービスに登録します。
   - （二要素認証を導入していないテナントのみ）グラフィカルインターフェイスでアプライアンスを登録します。
     a. **[エージェントオプション]** 以下の **[管理サーバー]** フィールドで、**[変更]** をクリックします。
     b. **[サーバー名/IP]** フィールドで **[クラウド]** を選択します。
        Cyber Protectionサービスのアドレスが表示されます。別途指示がある場合を除き、このアドレスは変更しないでください。
     c. **[ユーザー名]** および **[パスワード]** フィールドで、Cyber Protectionサービスのアカウントの資格情報を指定します。仮想アプライアンスとアプライアンスが管理する仮想マシンは、このアカウントに登録されます。
     d. **[OK]** をクリックします。
   - コマンドラインインターフェイスでアプライアンスを登録します。

注意
この方法では、登録トークンが必要です。登録トークンを生成する方法の詳細については、"登録トークンの生成"（164ページ）を参照してください。

a. CTRL+SHIFT+F2キーでコマンドラインインターフェイスが開きます。
b. 次のコマンドを実行します。

```
register_agent -o register -t cloud -a <service address> --token <registration token>
```

注意
登録トークンを使用する場合は、実際のデータセンターのアドレスをそのまま指定しなければなりません。これは、Cyber Protectコンソールに**ログインした後**に表示されるURLです。たとえば、`https://eu2-cloud.company.com`です。



ここでは`https://cloud.company.com`を使用しないでください。

c. Alt+F1キーを押して、アプライアンスのグラフィカルインターフェイスに戻ります。

6. （オプション）**[名前]** フィールドで **[変更]** をクリックして、**localhost**となる仮想アプライアンスのデフォルト名を編集します。この名前はCyber Protectコンソールに表示されます。
7. （オプション）**[時間]** フィールドで **[変更]** をクリックして、ロケーションのタイムゾーンを選択し、該当する時刻にスケジュールされた処理が実行されることを確認します。
8. （オプション）（ネットワークでプロキシサーバーが有効にされている場合）プロキシサーバーを構成します。
   a. CTRL+SHIFT+F2キーでコマンドラインインターフェイスが開きます。
   b. **/etc/Acronis/Global.config**ファイルをテキストエディタで開きます。
   c. 次のいずれかを実行します。
      - エージェントインストール中にプロキシ設定を指定した場合は、次のセクションを見つけます。

```
<key name="HttpProxy">
    <value name="Enabled" type="Tdword">"1"</value>
    <value name="Host" type="TString">"ADDRESS"</value>
    <value name="Port" type="Tdword">"PORT"</value>
    <value name="Login" type="TString">"LOGIN"</value>
    <value name="Password" type="TString">"PASSWORD"</value>
</key>
```

      - それ以外の場合は、上記の内容をコピーして、ファイルの`<registry name="Global">...</registry>`タグの間に貼り付けます。
   d. `ADDRESS`は新しいプロキシサーバーホスト名/IPアドレスで置換し、`PORT`はポート番号の10進値で置換します。

e. プロキシサーバーで認証が必要な場合は、LOGINとPASSWORDをプロキシサーバー資格情報と置き換えます。必要ない場合は、ファイルからこれらの行を削除します。
f. ファイルを保存します。
g. ファイル/**opt**/**acronis**/**etc**/**aakore.yaml**をテキストエディタで開きます。
h. **env**セクションを探し（または作成し）、以下の行を追加します。

```
env:
    http-proxy: proxy_login:proxy_password@proxy_address:port
    https-proxy: proxy_login:proxy_password@proxy_address:port
```

i. proxy_loginとproxy_passwordをプロキシサーバー資格情報と置き換えます。また、proxy_address:portをプロキシサーバーのアドレスとポート番号に置き換えます。
j. rebootコマンドを実行します。

注意
プロキシの背後に配置された仮想アプライアンスをアップデートできるようにするには、アプライアンスのconfig.yamlファイル（/opt/acronis/etc/va-updater/config.yaml）を編集し、ファイルの最下行に以下の行を追加して、現在の環境で固有の値を入力します。

```
httpProxy: http://<proxy_login>:<proxy_password>@<proxy_address>:<port>
```

例:

```
httpProxy: http://mylogin:mypassword@192.168.2.300:8080
```

Red Hat Virtualization/oVirtデータセンターの仮想マシンを保護するには

1. Cyber Protectionアカウントにログインします。
2. [**デバイス**] > [**oVirt**] > <クラスター> の順に移動するか、[**デバイス**] > [**すべてのデバイス**] でマシンを検索します。
3. マシンを選択し、保護計画を適用します。

oVirtエージェント - 必要なロールとポート

必要なロール

oVirtエージェントの配置と操作には、次のロールが割り当てられた管理者アカウントが必要です。

oVirt/Red Hat Virtualization 4.2および4.3/Oracle Virtualization Manager 4.3

- DiskCreator
- UserVmManager
- TagManager
- UserVmRunTimeManager
- VmCreator

oVirt/Red Hat Virtualization 4.4、4.5

- SuperUser

必要なポート

oVirtエージェントは、仮想アプライアンスの構成時に指定したURLを使用してoVirtエンジンに接続します。通常、エンジンURLの形式は次のとおりです:`https://ovirt.company.com`。この場合、HTTPSプロトコルとポート443が使用されます。

デフォルト以外のoVirt設定では、別のポートが必要になる場合があります。URL形式を分析することで、正しいポートを見つけることができます。例:

oVirtエンジンのURL	ポート	プロトコル
`https://ovirt.company.com/`	443	HTTPS
`http://ovirt.company.com/`	80	HTTP
`https://ovirt.company.com:1234/`	1234	HTTPS

バックアップはHotAddモードで実行されるため、ディスクの読み取り/書き込み操作用に追加のポートは必要ありません。

Synologyエージェントの配置

開始する前に

Synologyエージェントを使用すると、Synology NASデバイスとの間でファイルやフォルダのバックアップを実行できます。共有、フォルダ、およびファイルに対するNAS固有のプロパティとアクセス許可は保持されます。

Synologyエージェントは、NASデバイス上で実行されます。このため、バックアップのレプリケーション、検証、クリーンアップなどのオフホストデータ処理操作に、デバイスのリソースを利用できます。これらの処理の詳細については、"オフホストのデータ処理"（193ページ）を参照してください。

注意
Synologyエージェントでは、x86_64プロセッサを搭載したNASデバイスのみがサポートされています。ARMプロセッサはサポートされていません。

バックアップは、NASデバイスの元のロケーションまたは新しいロケーションにリカバリしたり、該当のデバイスを介してアクセス可能なネットワークフォルダにリカバリしたりできます。クラウドストレージ内のバックアップは、Synologyエージェントがインストールされている非オリジナルのNASデバイスにリカバリすることもできます。

利用可能なバックアップソースとバックアップ先の概要について、以下の表に示します。

バックアップ元	バックアップする項目 （バックアップソース）	バックアップの保存先 （バックアップ先）
ファイル/フォルダ	ローカルフォルダ*	クラウドストレージ
		ローカルフォルダ*
	ネットワークフォルダ （SMB）**	ネットワークフォルダ （SMB）**
		NFSフォルダ

* NASデバイスに接続されているUSBドライブを含む。

注意
暗号化されたフォルダはサポートされていません。これらのフォルダは、Cyber Protection グラフィカルユーザーインターフェイスに表示されません。

** Synology DiskStation Manager 6.2.3以降で動作するエージェントの場合のみ、SMBプロトコル経由で外部ネットワーク共有をバックアップソースまたはバックアップ先として利用できます。ホストされたネットワーク共有を含め、Synology NASにホストされているデータは、制限なくバックアップできます。

制限事項

- Synologyエージェントでは、x86_64プロセッサを搭載したNASデバイスのみがサポートされています。ARMプロセッサはサポートされていません。
- バックアップされた暗号化共有は、非暗号化ボリュームとしてリカバリされます。
- **ファイル圧縮**オプションが有効化されたバックアップ共有は、このオプションが無効にされた状態でリカバリされます。
- Synology NASデバイスに復元できるのは、Agent for Synologyによって作成されたバックアップのみです。

セットアップ プログラムのダウンロード

Synologyエージェントのセットアッププログラムは、SPKファイルとして入手できます。

Synology 7.xエージェント

セットアッププログラムをダウンロードするには

1. Cyber Protectコンソールで、**[デバイス]** > **[すべてのデバイス]** に進みます。
2. 右上の **[追加]** をクリックします。
3. **ネットワーク接続ストレージ（NAS）**以下で、**[Synology]** をクリックします。
   現在のマシンに、セットアッププログラムがダウンロードされます。

Synology 6.xエージェント

セットアッププログラムをダウンロードするには

1. Cyber Protectコンソールで、**[デバイス]** > **[すべてのデバイス]** に進みます。
2. 右上の **[追加]** をクリックします。
3. **ネットワーク接続ストレージ（NAS）**以下で、**[Synology]** をクリックします。
   Synology 7.xエージェントのセットアッププログラムがマシンにダウンロードされます。
   ダウンロードプロセスを安全に停止するか、ダウンロードしたファイルを無視することができます。
4. **[Synology 6.xエージェントをダウンロード]** をクリックします。
   Synology 6.xエージェントのセットアッププログラムがマシンにダウンロードされます。

Synologyエージェントのインストール

Synologyエージェントをインストールするには、Synology DiskStation ManagerでSPKファイルを実行します。

注意
Synologyエージェントでは、x86_64プロセッサを搭載したNASデバイスのみがサポートされています。ARMプロセッサはサポートされていません。

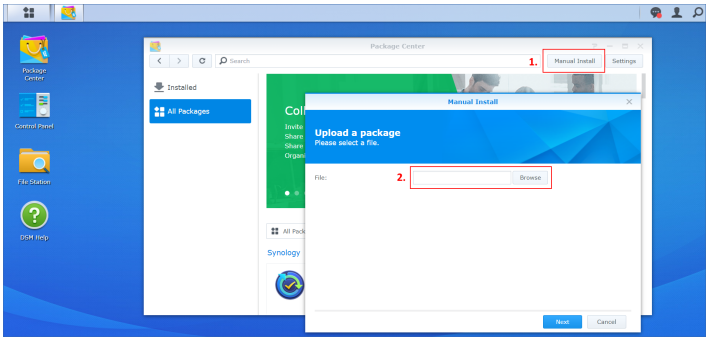
Synology 7.xエージェント

前提条件

- NASデバイスでは、DiskStation Manager 7.xが実行されています。
- 自分が、NASデバイスの**管理者グループ**のメンバーになっていること。
- エージェントをインストールするNASのボリュームに、少なくとも200MBの空き容量があること。
- マシンでSSHクライアントが使用可能である。この文書では、例としてPuttyを使用します。

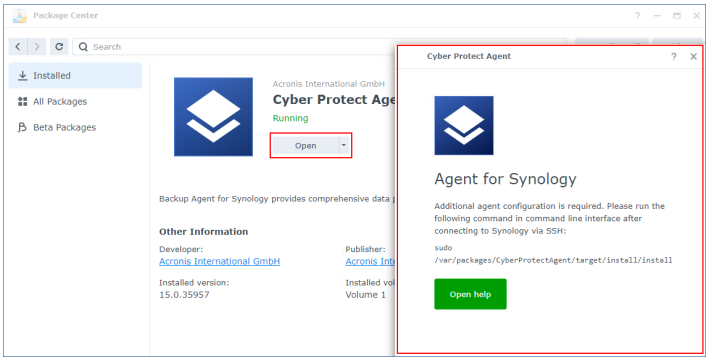
Synologyエージェントをインストールするには

1. Synology DiskStation Managerにログインします。
2. **パッケージセンター**を開きます。
3. **[手動インストール]** をクリックしてから、**[参照]** をクリックします。



4. Cyber Protectコンソールでダウンロードした SPKファイルを選択し、**[次へ]** をクリックします。
   サードパーティ製のソフトウェアパッケージをインストールするという警告が表示されます。このメッセージは標準インストール手順の一部です。

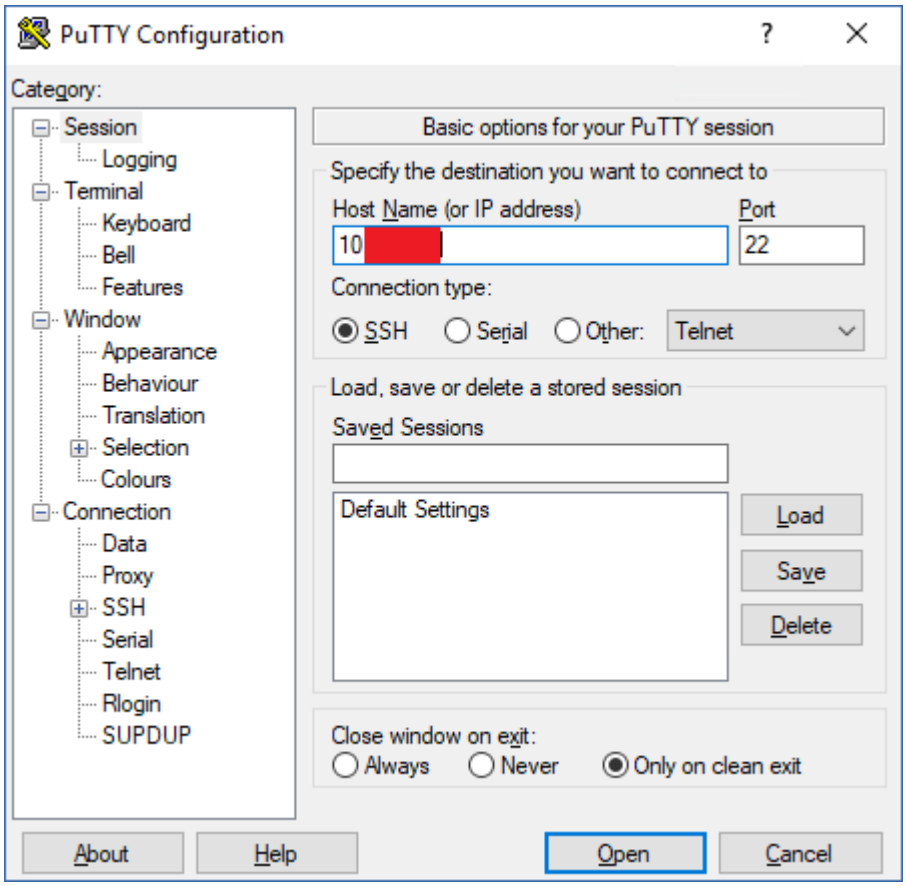
5. パッケージをインストールすることを確認するには、[**同意**] をクリックします。
6. エージェントをインストールするボリュームを選択してから、[**次へ**] をクリックします。
7. 設定を確認し、[**完了**] をクリックします。
8. Synology DiskStation Manager**パッケージセンター**で、Cyber Protect Synologyエージェントを開き、次の画面が表示されることを確認します。



9. Synology DiskStation Managerの**コントロールパネル**で、[**ターミナルとSNMP**] に移動し、NASデバイスへのSSHアクセスを有効にします。
10. SSHクライアント(この例ではPutty)を使用して、NASデバイスで**インストール**スクリプトを実行します。

    このスクリプトにより、エージェントを構成するために必要なDSM7.0以降へのルートアクセスが有効になります。

    a. Puttyを起動し、Synology NASデバイスのIPアドレスまたはホスト名を指定します。



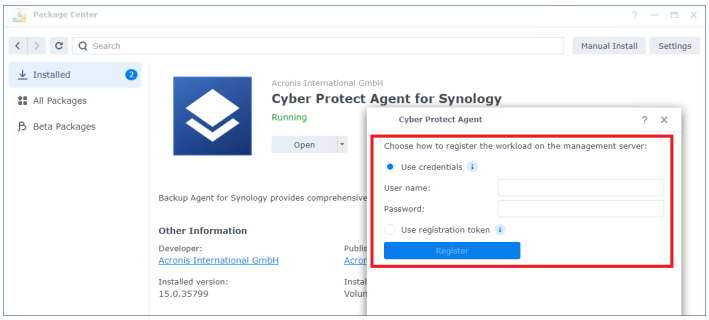
b. **[開く]** をクリックし、Synology DSM管理者としてログインします。

c. 次のコマンドを実行します。

```
sudo /var/packages/CyberProtectAgent/target/install/install
```

スクリプトの開始後、Cyber Protectionサービスが初期化されるまで15秒間待ちます。

11. Synology DiskStation Managerの**コントロールパネル**で、**[ターミナルとSNMP]** に移動し、NASデバイスへのSSHアクセスを無効にします。SSHアクセスは必須ではなくなります。
12. Synology DiskStation Manager**パッケージセンター**で、Cyber Protect Synologyエージェントを開きます。
13. 登録メソッドを選択します。



- （資格情報を使用してエージェントを登録するには）
  - **[ユーザー名]** および **[パスワード]** フィールドで、エージェントが登録されるアカウントの資格情報を指定します。このアカウントは、パートナー管理者アカウントにはできません。
- （登録トークンを使用してエージェントを登録するには）
  - **[登録アドレス]**には、正確なデータセンターのアドレスを指定します。正確なデータセンターのアドレスとは、`https://us5-cloud.acronis.com`など、Cyber Protectコンソールにログインした後に表示されるURLです。

    注意
    データセンターのアドレスを含まないURL形式は使用しないでください。例えば、`https://cloud.acronis.com`を使用することはできません。

  - **[トークン]**フィールドで登録トークンを指定します。
    登録トークンを生成する詳細な方法については、"登録トークンの生成"（164ページ）を参照してください。

14. **[登録]** をクリックします。

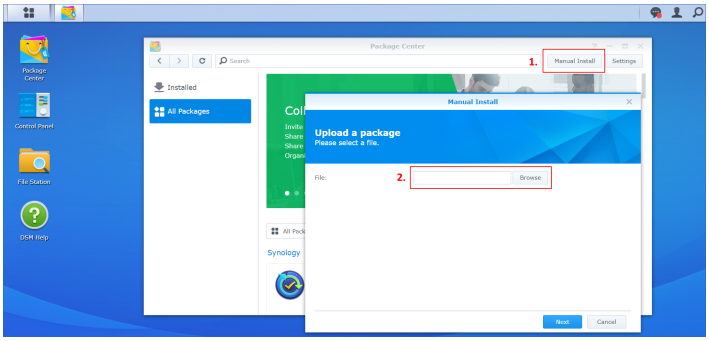
Synology 6.xエージェント

前提条件

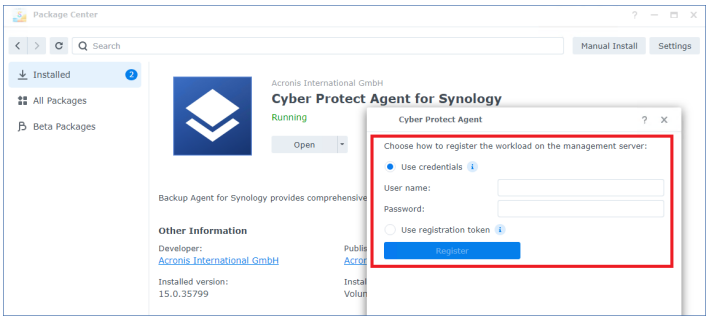
- NASデバイスでは、DiskStation Manager 6.2.xが実行されています。
- 自分が、NASデバイスの**管理者グループ**のメンバーになっていること。
- エージェントをインストールするNASのボリュームに、少なくとも200MBの空き容量があること。

Synologyエージェントをインストールするには

1. Synology DiskStation Managerにログインします。
2. **パッケージセンター**を開きます。
3. **[手動インストール]** をクリックしてから、**[参照]** をクリックします。



4. Cyber Protectコンソールでダウンロードした.SPKファイルを選択し、**[次へ]** をクリックします。
   デジタルシグネチャのないパッケージをインストールするという警告が表示されます。このメッセージは標準インストール手順の一部です。
5. パッケージをインストールすることを確認するには、**[はい]** をクリックします。
6. エージェントをインストールするボリュームを選択してから、**[次へ]** をクリックします。
7. 設定を確認し、**[適用]** をクリックします。
8. Synology DiskStation Manager**パッケージセンター**で、Cyber Protect Synologyエージェントを開きます。
9. 登録メソッドを選択します。



- （資格情報を使用してエージェントを登録するには）
  - **[ユーザー名]** および **[パスワード]** フィールドで、エージェントが登録されるアカウントの資格情報を指定します。このアカウントは、パートナー管理者アカウントにはできません。
- （登録トークンを使用してエージェントを登録するには）
  - **[登録アドレス]**には、正確なデータセンターのアドレスを指定します。正確なデータセンターのアドレスとは、`https://us5-cloud.acronis.com`など、Cyber Protectコンソールにログインした後に表示されるURLです。

    注意
    データセンターのアドレスを含まないURL形式は使用しないでください。例えば、`https://cloud.acronis.com`を使用することはできません。

  - **[トークン]**フィールドで登録トークンを指定します。

登録トークンを生成する詳細な方法については、"登録トークンの生成"（164ページ）を参照してください。

10. **[登録]** をクリックします。

登録完了後、Synology NASデバイスが、**[デバイス]** > **[ネットワーク接続ストレージ]** タブのCyber Protectコンソールに表示されます。

NASデバイスのデータをバックアップするには、保護計画を適用します。

Synologyエージェントのアップデート

Synology 6.xエージェントを新しいバージョンのSynology 6.xエージェントにアップデートできます。同様に、Synology 7.xエージェントを Synology 7.xエージェントの新しいバージョンにアップデートすることもできます。

エージェントをアップデートするには、Synology DiskStation Managerで新しいバージョンのセットアッププログラムを実行します。エージェントの元の登録、その設定、保護対象のワークロードに適用される計画が保持されます。

注意
Cyber Protectコンソールからエージェントをアップデートすることはできません。

Synology 6.xエージェントからSynology 7.xエージェントへのアップグレードは、古いエージェントをアンインストールし、新しいエージェントをインストールする方法のみがサポートされます。この場合、すべての保護計画は取り消しになり、手動で再適用する必要があります。

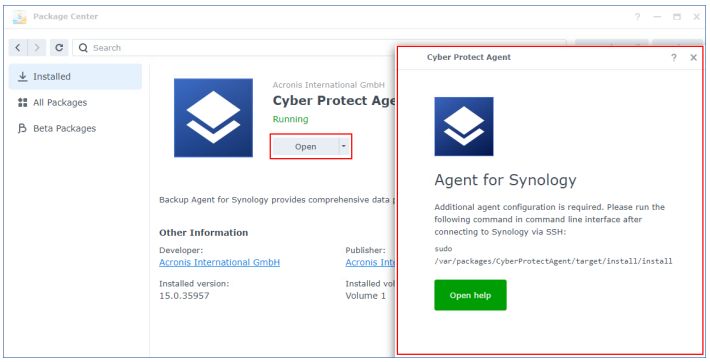
Synology 7.xエージェント

前提条件

- 自分が、NASデバイスの**管理者グループ**のメンバーになっていること。
- エージェントをインストールするNASのボリュームに、少なくとも200MBの空き容量があること。
- マシンでSSHクライアントが使用可能である。この文書では、例としてPuttyを使用します。

Synologyエージェントをアップデートするには

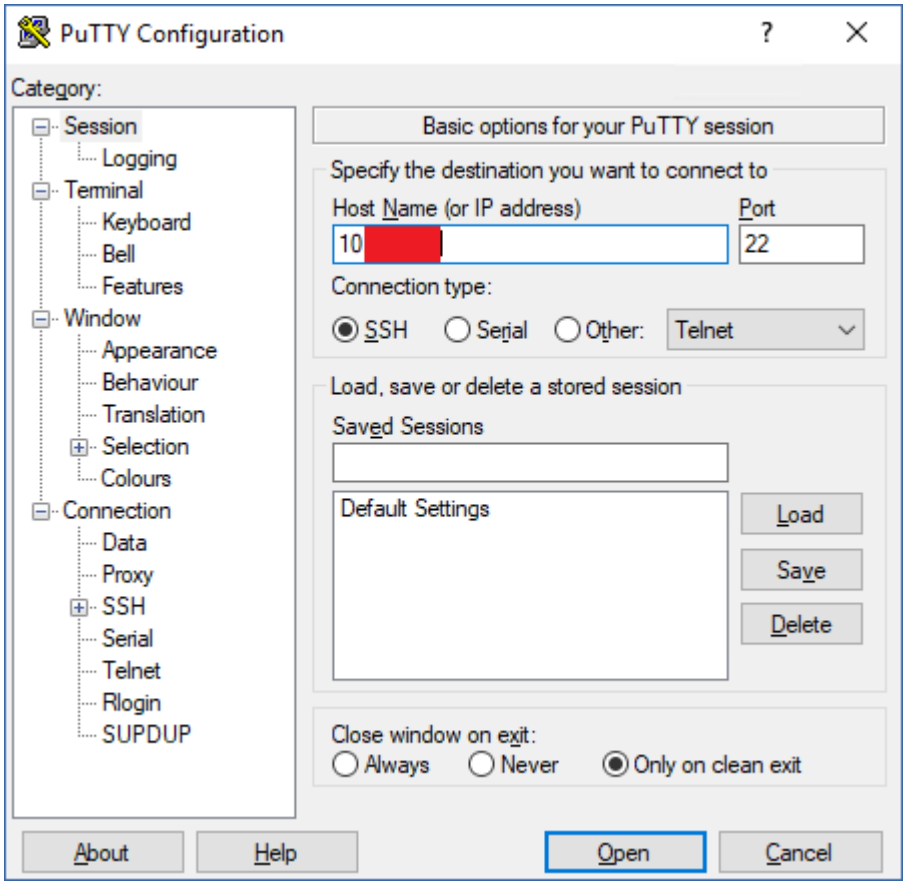
1. DiskStation Managerで、**[パッケージセンター]**を開きます。
2. **[手動インストール]** をクリックしてから、**[参照]** をクリックします。
3. Cyber Protectコンソールでダウンロードした、Synology 7.xエージェント用の新しいSPKファイルを選択し、**[次へ]** をクリックします。
   サードパーティ製のソフトウェアパッケージをインストールするという警告が表示されます。このメッセージは標準インストール手順の一部です。
4. パッケージをインストールすることを確認するには、**[同意]** をクリックします。
5. 設定を確認し、**[完了]** をクリックします。
6. Synology DiskStation Manager**パッケージセンター**で、Cyber Protect Synologyエージェントを開き、次の画面が表示されることを確認します。



7. Synology DiskStation Managerの**コントロールパネル**で、[**ターミナルとSNMP**] に移動し、NASデバイスへのSSHアクセスを有効にします。
8. SSHクライアント(この例ではPutty)を使用して、NASデバイスで**インストール**スクリプトを実行します。

   このスクリプトにより、エージェントを構成するために必要なDSM7.0以降へのルートアクセスが有効になります。

   a. Puttyを起動し、Synology NASデバイスのIPアドレスまたはホスト名を指定します。



   b. [**開く**] をクリックし、Synology DSM管理者としてログインします。

   c. 次のコマンドを実行します。

```
sudo /var/packages/CyberProtectAgent/target/install/install
```

9. Synology DiskStation Managerの**コントロールパネル**で、[**ターミナルとSNMP**] に移動し、NASデバイスへのSSHアクセスを無効にします。SSHアクセスは必須ではなくなります。

Synology 6.xエージェント

前提条件

- 自分が、NASデバイスの**管理者グループ**のメンバーになっていること。
- エージェントをインストールするNASのボリュームに、少なくとも200MBの空き容量があること。

Synologyエージェントをアップデートするには

1. DiskStation Managerで、[**パッケージセンター**]を開きます。
2. [**手動インストール**] をクリックしてから、[**参照**] をクリックします。
3. Cyber Protectコンソールでダウンロードした、Synology 6.xエージェント用の新しいSPKファイルを選択し、[**次へ**] をクリックします。
   デジタルシグネチャのないパッケージをインストールするという警告が表示されます。このメッセージは標準インストール手順の一部です。
4. パッケージをインストールすることを確認するには、[**はい**] をクリックします。
5. 設定を確認し、[**適用**] をクリックします。

グループポリシーによるエージェントの配置

Windowsグループポリシーを使用して、WindowsエージェントをActive Directoryドメインのメンバーとなっているマシンに集中的にインストール（または配置）できます。

このセクションでは、グループポリシーオブジェクトを設定して、ドメイン全体またはその組織単位（OU）のコンピュータにエージェントを配置する方法について説明します。

コンピュータがドメインにログオンするたびに、適用されるグループポリシーオブジェクトによって、エージェントが確実にインストールされ登録されます。

前提条件

- Active Directoryドメインと、Microsoft Windows Server 2003以降を実行しているドメインコントローラがある。
- 設定者がこのドメインの**Domain Admins**グループのメンバーである。
- **Windowsのすべてのエージェント**のセットアッププログラムがダウンロードされている。
  セットアッププログラムをダウンロードするには、Cyber Protectコンソールで、右上にあるアカウントアイコンをクリックしてから、[**ダウンロード**] をクリックします。ダウンロードリンクは、[**デバイスの追加**] ペインにもあります。

グループポリシー経由でエージェントを配置するには

1. 登録トークンを生成します（"登録トークンの生成"（164ページ）を参照）。
2. .mstファイル、.msiファイル、.cabファイルを作成します（"変換ファイルを作成してインストールパッケージを抽出する"（166ページ）を参照）。

3. グループポリシーオブジェクトのセットアップを実行します（"グループ ポリシー オブジェクトの設定"（167ページ）を参照）。

登録トークンの生成

登録トークンは、Cyber Protectコンソールにユーザーの資格情報を保存することなく、ユーザーの個人情報をエージェントのプログラムの設定に渡します。これにより、ユーザーはログインしなくても、自分のアカウントに任意の台数のマシンを登録でき、また、保護計画をワークロードに適用できます。

注意
保護計画は、マシン登録中には自動的に適用されません。保護計画の適用は別のタスクです。

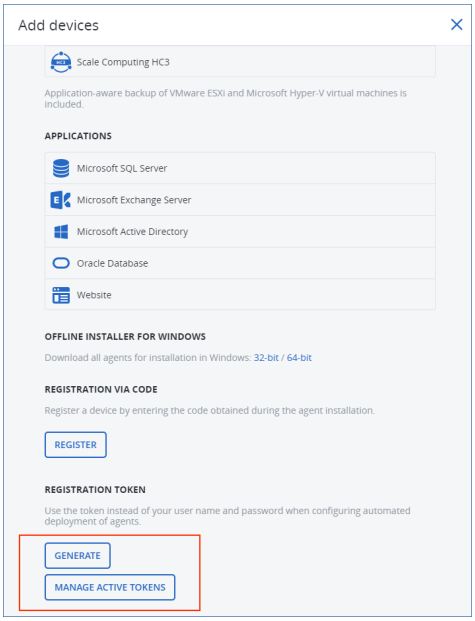
セキュリティ上の理由から、トークンには変更可能な有効期間が設定されています。デフォルトの有効期間は3日間です。

ユーザーは、自分のアカウントに対してのみ登録トークンを生成できます。管理者は、管理しているテナントのすべてのユーザーアカウントに対して登録トークンを生成できます。

登録トークンを生成するには

ユーザーの場合

1. Cyber Protectコンソールにログインします。
2. **[デバイス]** > **[すべてのデバイス]** > **[追加]** の順にクリックします。
   右側に **[デバイスの追加]** ペインが開きます。
3. 下にスクロールして **[登録トークン]** を表示し、**[生成]** をクリックします。

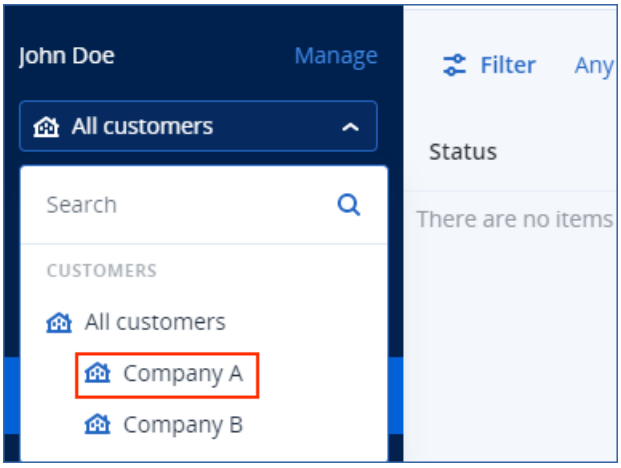


4. トークンの有効期間を指定します。
5. **[トークンを生成]** をクリックします。
6. **[コピー]** をクリックして、トークンをデバイスのクリップボードにコピーするか、トークンをメモします。

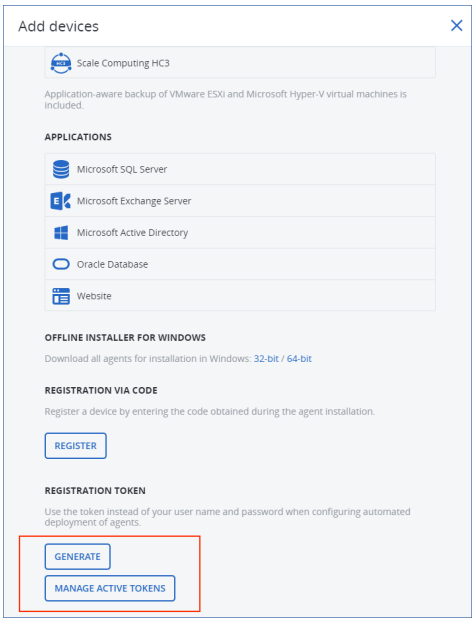
管理者の場合

1. Cyber Protectコンソールに管理者としてログインします。
   既に管理ポータルにサインインしている場合は、**[監視]** > **[使用状況]** からCyber Protectコンソールに移動して、**[保護]** タブ以下の **[サービスを管理]** をクリックします。

   （パートナー管理者がカスタマーテナントを管理している場合）Cyber Protectコンソールで、トークンを生成したいユーザーのテナントを選択します。**すべてのカスタマー**レベルではトークンを生成することはできません。



2. **[デバイス]** の下で、**[すべてのデバイス]** > **[追加]** をクリックします。
   右側に **[デバイスの追加]** ペインが開きます。
3. 下にスクロールして **[登録トークン]** を表示し、**[生成]** をクリックします。



4. トークンの有効期間を指定します。
5. トークンを生成したいユーザーを選択します。

> **注意**
> トークンを使用すると、ワークロードはここで選択したユーザーアカウントで登録されます。

6. （オプション）トークンのユーザーが、追加したワークロードに保護計画を適用したり取り消したりできるようにするには、ドロップダウンリストから計画を選択します。
   なお追加されたワークロードに対し、保護計画を適用する、または取り消すスクリプトを実行する必要があります。詳細については、こちらのナレッジベースの記事を参照してください。
7. **[トークンを生成]** をクリックします。
8. **[コピー]** をクリックして、トークンをデバイスのクリップボードにコピーするか、トークンをメモします。

登録トークンを表示または削除するには

1. Cyber Protectコンソールにログインします。
2. **[デバイス]** > **[すべてのデバイス]** > **[追加]** の順にクリックします。
3. 下にスクロールして **[登録トークン]** を表示し、**[アクティブなトークンを管理]** をクリックします。
   右側に、テナントで生成されたアクティブなトークンを含むリストが表示されます。

> **注意**
> セキュリティ上の理由から、**[トークン]** 列ではトークン値の最初の2文字のみが表示されます。

4. （トークンを削除するには）トークンを選択して **［削除］** をクリックします。

変換ファイルを作成してインストールパッケージを抽出する

Windowsグループポリシーでプロテクションエージェントを配置するには、変換ファイル（.mst）、インストールパッケージ（.msiおよび.cabファイル）が必要です。

注意
以下の手順では、デフォルトの登録オプションであるトークンによる登録を使用します。登録トークンを生成する方法については、"登録トークンの生成"（164ページ）を参照してください。

.mstファイルを作成し、インストールパッケージ（.msiファイル、.cabファイル）を展開するには

1. Active Directoryドメイン内の任意のマシンで、管理者としてログインします。
2. インストールパッケージを保存する共有フォルダを作成します。共有フォルダにドメインユーザーがアクセスできるようにします。たとえば、デフォルトの共有設定を **[Everyone]** のままにします。
3. エージェントのセットアッププログラムを実行します。
4. **[無人インストールの .mst および .msi を作成]** をクリックします。
5. **[インストールする項目]** で、インストールに含めるコンポーネントを選択してから、**[完了]** をクリックします。
6. **登録の設定**で、**[指定]** をクリックし、登録トークンを入力し、**[完了]** をクリックします。
   登録方法を **[登録トークンを使用]**（デフォルト）から **[資格情報を使用]** または **[登録をスキップ]** に変更できます。**[登録をスキップ]** オプションは、ワークロードを後から手動で登録することを前提としています。
7. .mstファイルに追加されるインストール設定を確認または変更し、**[実行]** をクリックします。
8. **ファイルを保存する**には、作成した共有フォルダへのパスを指定します。
9. **[生成]** をクリックします。

その結果、.mstファイル、.msiファイル、.cabファイルが作成され、指定した共有フォルダにコピーされます。

次に、Windowsグループポリシーオブジェクトをセットアップします。この方法については、"グループ ポリシー オブジェクトの設定"（167ページ）を参照してください。

グループ ポリシー オブジェクトの設定

この手順では、"変換ファイルを作成してインストールパッケージを抽出する"（166ページ）で作成したインストールパッケージを使用して、グループポリシーオブジェクト（GPO）をセットアップします。このGPOにより、ドメイン内のマシンにエージェントが配置されます。

グループポリシーオブジェクトを設定するには

1. ドメイン管理者としてドメインコントローラにログインします。
   ドメインに複数のドメインコントローラがあるときは、いずれかのドメインにドメイン管理者としてログオンします。
2. （組織単位（OU）にエージェントを配置する場合）エージェントを配置する組織単位（OU）が、ドメイン内に存在していることを確認します。
3. Windowsの **[スタート]** メニューで、**[管理ツール]** をポイントしてから、**[グループポリシーの管理]**（Windows Server 2003の場合は **[Active Directoryユーザーとコンピューター]**）をクリックします。

4. （Windows Server 2008以降の場合）ドメイン名または組織単位（OU）名を右クリックし、**[このドメインに GPO を作成し、このコンテナにリンクする]** をクリックします。
5. （Windows Server 2003の場合）ドメイン名または組織単位（OU）名を右クリックし、**[プロパティ]** をクリックします。ダイアログボックスで、**[グループポリシー]** タブをクリックし、**[新規作成]** をクリックします。
6. 新しいグループポリシーオブジェクトに **[Windows エージェント]**という名前を付けます。
7. **[Window エージェント]** グループポリシーオブジェクトを編集用に開きます。
   - （Windows Server 2008以降の場合）**[グループポリシーオブジェクト]** でグループポリシーオブジェクトを右クリックし、**[編集]** をクリックします。
   - （Windows Server 2003の場合）グループポリシーオブジェクトをクリックし、**[編集]** をクリックします。
8. グループポリシーオブジェクトエディタのスナップインで、**[コンピュータの構成]** を展開します。
9. （Windows Server 2012以降の場合）**[ポリシー]** > **[ソフトウェアの設定]** の順に展開します。
10. （Windows Server 2003およびWindows Server 2008 の場合）**[ソフトウェアの設定]** を展開します。
11. **[ソフトウェアインストール]** を右クリックし、**[新規作成]** をポイントし、**[パッケージ]** をクリックします。
12. 作成した共有フォルダにあるエージェントの.msiインストールパッケージを選択し、**[開く]** をクリックします。
13. **[ソフトウェアの展開]** ダイアログボックスで、**[詳細設定]** をクリックし、**[OK]** をクリックします。
14. **[変更]** タブで、**[追加]** をクリックして、作成した共有フォルダの.mstファイル選択します。
15. **[OK]** をクリックして、**[ソフトウェアの展開]** ダイアログボックスを閉じます。

仮想アプライアンスへのSSH接続

メンテナンス目的で仮想アプライアンスにリモートアクセスするときは、Secure Socket Shell（SSH）接続を使用します。

Secure Shellデーモンを起動する

仮想アプライアンスへのSSH接続を許可するには、アプライアンス上でSecure Shellデーモン（sshd）を起動します。

Secure Shallデーモンを起動するには

1. ハイパーバイザーソフトウェアで、仮想アプライアンスのコンソールを開きます。
2. アプライアンスのグラフィカルユーザーインターフェイスでCTRL+SHIFT+F2キーを押すと、コマンドラインインターフェイスが開きます。
3. 次のコマンドを実行します。

   ```
   /bin/sshd
   ```

4. （アプライアンスへの最初の接続時のみ）**ルート**ユーザーのパスワードを設定します。

パスワードの設定方法については、"仮想アプライアンス上でルートパスワードを設定する"（169ページ）を参照してください。

注意
SSH接続を使用しないときは、Secure Shellデーモンを停止することをお勧めします。

仮想アプライアンス上でルートパスワードを設定する

仮想アプライアンスでSSH接続を確立する前に、アプライアンスのルートパスワードを設定する必要があります。

ルートパスワードを設定するには

1. ハイパーバイザーソフトウェアで、仮想アプライアンスのコンソールを開きます。
2. アプライアンスのグラフィカルユーザーインターフェイスでCTRL+SHIFT+F2キーを押すと、コマンドラインインターフェイスが開きます。
3. 次のコマンドを実行します。

   ```
   passwd
   ```

4. パスワードを指定してから、エンターを押します。
   パスワードは、少なくとも9文字以上で構成する必要があり、複雑性スコアは3以上でなければなりません。複雑性スコアは自動的に計算されます。より高いスコアを達成するためには、特殊記号、大文字と小文字、数字の組み合わせを使用してください。
5. パスワードを確認してから、エンターを押します。

SSHクライアントを介して仮想アプライアンスにアクセスする

前提条件

- リモートのマシンにはSSHクライアントが必要です。以下の手順では、例としてWinSCPクライアントを使用します。必要に応じて手順を変更すれば、任意のSSHクライアントを使用することもできます。
- 仮想アプライアンス上でSecure Shellデーモン（sshd）を開始する必要があります。詳細については、"Secure Shellデーモンを起動する"（168ページ）を参照してください。

WinSCPを介して仮想アプライアンスにアクセスする

1. リモートのマシンで、WinSCPを開きます。
2. **[セッション]** > **[新しいセッション]** をクリックします。
3. **[ファイルプロトコル]**で、**[SCP]** を選択します。
4. **[ホスト名]**で、仮想アプライアンスのIPアドレスを指定します。
5. **ユーザー名**と**パスワード**で、**ルート**と**ルート**ユーザーのパスワードを指定します。
6. **[ログイン]** をクリックします。

仮想アプライアンス上のすべてのディレクトリのリストが表示されます。

エージェントのアップデート

すべてのエージェントを手動でアップデートする場合、Cyber Protectコンソール経由で実行する方法と、インストールファイルをダウンロードして実行する方法があります。

以下のエージェントの自動アップデートを構成できます。

- Windowsエージェント
- Linuxエージェント
- エージェント for Mac
- File Sync & ShareCyber Files Cloudエージェント

エージェントを自動でアップデートする場合、またCyber Protectコンソールを使用して手動でアップデートする場合のいずれでも、以下のロケーションに4.2GBの空き容量が必要となります。

- Linuxの場合 - ルートディレクトリ
- Windowsの場合 - エージェントがインストールされているボリューム

macOSでエージェントをアップデートするには、ルートディレクトリ5GBの空き容量が必要です。

注意
（VMwareエージェント、Scale Computingエージェント、Virtuozzo Hybrid Infrastructureエージェント、RHV（oVirt）エージェントなど、仮想アプライアンスの形式で提供されるすべてのエージェント向け）

プロキシの背後で動作している仮想アプライアンスの自動アップデートまたは手動アップデートを実行するには、各アプライアンス上でプロキシサーバーを以下のように構成する必要があります。

`/opt/acronis/etc/va-updater/config.yaml`ファイルで、次の行をファイルの最終行に追加し、環境に応じた適切な値を入力します:

```
httpProxy: http://proxy_login:proxy_password@proxy_address:port
```

エージェントの手動アップデート

エージェントのアップデートには、Cyber Protectコンソールを使用する方法と、インストールファイルをダウンロードして実行する方法があります。

以下のバージョンの仮想アプライアンスは、Cyber Protectコンソールを使用してアップデートする必要があります。

- VMwareエージェント（仮想アプライアンス）: バージョン12.5.23094以降。
- Virtuozzo Hybrid Infrastructureエージェント（仮想アプライアンス）: バージョン12.5.23094以降。

以下のバージョンのエージェントは、Cyber Protectコンソールを使用してアップデートすることもできます。

- Windowsエージェント、VMwareエージェント（Windows）、Hyper-Vエージェント: バージョン12.5.21670以降。

- Linuxエージェント: バージョン12.5.23094以降。
- 他のエージェント: バージョン12.5.23094以降。

エージェントのバージョンを確認するには、Cyber Protectコンソールでマシンを選択して、**[詳細]** をクリックします。

それらのエージェントの旧バージョンをアップデートするには、最新バージョンを手動でダウンロードしてインストールします。ダウンロードリンクを確認するには、**[すべてのデバイス]** > **[追加]** の順にクリックします。

前提条件

WindowsマシンでCyber Protect機能を使用するには、Microsoft Visual C++ 2017再頒布可能パッケージが必要です。既にマシンにインストールされていることを確認するか、エージェントをアップデートする前にインストールしてください。インストール後に再起動が必要になる場合があります。Microsoft Visual C++の再頒布可能パッケージは、MicrosoftのWebサイト（https://support.microsoft.com/help/2999226/update-for-universal-c-runtime-in-windows）から入手できます。

Cyber Protectコンソールを使用してエージェントをアップデートするには

1. **[設定]** > **[エージェント]** の順にクリックします。
   ソフトウェアにより、コンピュータのリストが表示されます。古いバージョンのエージェントが適用されているコンピュータには、オレンジ色の感嘆符が示されます。
2. アップデート対象のコンピュータを選択します。このコンピュータはオンラインである必要があります。
3. **[エージェントのアップデート]** をクリックします。

注意
アップデートの間、進行中のバックアップはすべて失敗します。

12.5.23094より前のバージョンのVMwareエージェント（仮想アプライアンス）のアップデート手順

1. **[設定]** > **[エージェント]** > アップデートするエージェント > **[詳細]** の順にクリックし、**割り当てられた仮想マシン**セクションを調べます。アップデートの後にこれらの設定を再入力する必要があります。
   a. **[自動割り当て]** スイッチの位置を書き留めます。
   b. どの仮想マシンが手動でエージェントに割り当てられているかを調べるため、**[割り当て済み:]** リンクをクリックします。ソフトウェアにより、割り当てられた仮想マシンのリストが表示されます。**[エージェント]** 列で、エージェント名の後に「(M)」がついたマシンをメモしておきます。
2. 「エージェントのアンインストール」の説明に従ってVMwareエージェント（仮想アプライアンス）を削除します。エージェントは再インストールする予定ですが、手順5では **[設定]** > **[エージェント]** からエージェントを削除します。
3. 「OVFテンプレートの配置」の説明に従って、VMwareエージェント（仮想アプライアンス）をデプロイします。

4. 「仮想アプライアンスの設定」の説明に従ってVMwareエージェント（仮想アプライアンス）を設定します。

   ローカル接続されたストレージを再構築したい場合、手順7で以下のように実行します。

   a. ローカルストレージが含まれるディスクを仮想アプライアンスに追加する。

   b. **[更新]** > **[ストレージの作成]** > **[マウント]** をクリックする。

   c. ソフトウェアによって、ディスクの元の**ドライブ文字**と**ラベル**が表示されます。それらは変更しないでください。

   d. **[OK]** をクリックします。

5. **[設定]** > **[エージェント]** > アップデートするエージェント > **[詳細]** の順にクリックし、ステップ1で書き留めた設定を再構築します。仮想マシンが手動でエージェントに割り当てられている場合、「仮想マシンのバインド」の記述通りにそれらを再度割り当てます。

   エージェントの設定が完了すると、古いエージェントに適用されていた保護計画が自動的に新しいエージェントに再適用されます。

6. アプリケーション認識型バックアップが有効になっている計画では、ゲストOSの資格情報の再入力が必要になります。計画を編集し、資格情報を再入力します。

7. ESXi設定をバックアップする計画では、「ルート」パスワードの再入力が必要になります。計画を編集し、パスワードを再入力します。

マシンでサイバープロテクション定義を更新する

1. **[設定]** > **[エージェント]** の順にクリックします。
2. サイバープロテクションの定義をアップデートするマシンを選択し、**[定義のアップデート]** をクリックします。マシンがオンラインでなければなりません。

エージェントにアップデートロールを割り当てる

1. **[設定]** > **[エージェント]** の順にクリックします。
2. アップデートロールを割り当てるマシンを選択して、**[詳細]** をクリックします。次に、**[サイバープロテクション定義]** セクションで、**[このエージェントを使用してパッチとアップデートをダウンロードし、配布します]** を有効にします。

   注意

   アップデータロールを割り当てられているエージェントでは、Windowsのサードパーティ製品についてのみパッチのダウンロードおよび配信が可能です。Microsoft製品の場合、アップデータエージェントによるパッチ配信はサポートされていません。

エージェントでキャッシュデータを消去する

1. **[設定]** > **[エージェント]** の順にクリックします。
2. キャッシュのデータ（古いアップデートファイルとパッチ管理データ）を消去するマシンを選択し、**[キャッシュの消去]** をクリックします。

エージェントの自動アップデート

複数のワークロードの管理を容易にするために、Windowsエージェント、Linuxエージェント、Macエージェントの自動アップデートを構成することができます。自動アップデートの対象となるのは、

エージェントバージョン15.0.26986（2021年5月リリース）以降です。以前のエージェントは、まず手動で最新バージョンにアップデートする必要があります。

自動アップデートは、以下のオペレーティングシステムを搭載したマシンでサポートされています。

- Windows XP SP 3以降
- Red Hat Enterprise Linux 6以降、CentOS 6以降
- OS X 10.9 Mavericks以降

自動アップデートの設定は、データセンターレベルで事前構成されています。社内管理者は、社内または部署内のすべてのマシン、または個別マシンに対して、これらの設定をカスタマイズすることができます。カスタム設定が適用されていない場合は、上位レベルの設定が順次使用されます。

1. Cyber Protectionデータセンター
2. 社内（カスタマーテナント）
3. ユニット
4. コンピュータ

例えば、部署の管理者は、部署内のすべてのマシンにカスタムの自動アップデート設定を行うことができますが、この設定は、社内レベルでマシンに適用される設定と異なる場合があります。また、管理者は、部署内の1台または複数の個別マシンに対して異なる設定を適用することができます。この場合、そのマシンには部署の設定や社内の設定が適用されません。

自動アップデートを有効にした後、以下のオプションを構成することができます。

- **アップデートチャネル**
  アップデートチャネルにより、エージェントのどのバージョンを使用するか（最新のバージョン、または前回のリリースから最も新しいバージョン）を定義します。
- **メンテナンス期間**
  メンテナンス期間により、アップデートをインストールできるタイミングを定義します。メンテナンス期間を無効にすると、アップデートはいつでも実行できるようになります。
  有効なメンテナンス期間内であっても、エージェントが以下のいずれかの処理を行っている間はアップデートはインストールされません。
  - バックアップ
  - 復元
  - バックアップのレプリケーション
  - 仮想マシンへのレプリケーション
  - レプリカのテスト
  - バックアップから仮想マシンを実行する（ファイナライズを含む）
  - ディザスタリカバリフェールオーバー
  - ディザスタリカバリフェールバック
  - スクリプトの実行（サイバースクリプト機能の場合）
  - パッチのインストール
  - ESXi構成バックアップ

自動アップデートの設定をカスタマイズするには

1. Cyber Protectコンソールで **[設定]** > **[エージェント]** に進みます。
2. 設定するスコープを選択します。
   - すべてのマシンの設定を変更するには、**[デフォルトのエージェントアップデート設定を編集する]** をクリックします。
   - 特定のマシンの設定を変更するには、対象となるマシンを選択し、**[エージェントアップデート設定]** をクリックします。
3. 必要に応じて設定を構成して **[適用]** をクリックします。

自動アップデート設定のカスタマイズを削除するには

1. Cyber Protectコンソールで **[設定]** > **[エージェント]** に進みます。
2. 設定するスコープを選択します。
   - すべてのマシンでカスタマイズされた設定を削除するには、**[デフォルトのエージェントアップデート設定を編集する]** をクリックします。
   - 特定のマシンのカスタマイズされた設定を削除するには、対象となるマシンを選択し、**[エージェントアップデート設定]** をクリックします。
3. **[デフォルトの設定にリセット]** をクリックしてから、**[適用]** をクリックします。

自動アップデートのステータスを確認するには

1. Cyber Protectコンソールで **[設定]** > **[エージェント]** に進みます。
2. 表の右上にあるギアアイコンをクリックして、**[自動アップデート]** のチェックボックスが選択されていることを確認します。
3. **[自動アップデート]** の列に表示されているステータスを確認します。

BitLockerで保護されたワークロードでのエージェントのアップデート

Startup Recovery Managerに変更を加えるエージェントのアップデートは、BitLockerとStartup Recovery Managerの両方が有効になっているワークロードではBitLockerに干渉します。この場合、再起動後にBitLocker復元キーが必要になります。この問題を解消するには、エージェントをアップデートする前にBitLockerを一時停止するか、無効にしてください。

影響を受けるエージェントのバージョン:

- 23.12.36943（2023年12月リリース）

アップデートによるStartup Recovery Managerに対する変更の有無は、プロテクションエージェントのリリースノートでも確認できます。

BitLockerおよびStartup Recovery Managerが有効なワークロードでエージェントをアップデートするには

1. エージェントをアップデートするワークロードで、BitLockerを一時停止するか、無効にします。
2. エージェントをアップデートします。

3. ワークロードを再起動します。
4. BitLockerを有効にします。

エージェントの不正なインストール解除または変更の防止

保護計画の**パスワードによる保護**設定を有効にすることで、Windowsエージェントを不正なインストール解除や変更から保護できます。この設定は、**自己防御機能**設定が有効な場合に限り利用可能です。

パスワードによる保護を有効にする手順

1. 保護計画では、**ウイルス対策およびマルウェア対策保護**モジュール（Cyber Backup Editionの**Active Protection**モジュール）を拡張します。
2. **[自己防御機能]** をクリックして、**[自己防御機能]** スイッチが有効になっていることを確認します。
3. **[パスワードによる保護]** スイッチを有効にします。
4. 開いたウィンドウで、保護されたWindowsエージェントのコンポーネントをアンインストールまたは変更するために必要なパスワードをコピーします。
   このパスワードは一意であり、このウィンドウを閉じるとリカバリできなくなります。このパスワードを紛失したり忘れたりした場合は、保護計画を編集して新しいパスワードを作成できます。
5. **[閉じる]** をクリックします。
6. **自己防御機能**ペインで、**[完了]** をクリックします。
7. 保護計画を保存します。

この保護計画が適用されるマシンでは、パスワードによる保護が有効になります。パスワードによる保護は、Windowsエージェントのバージョン15.0.25851以降でのみ使用できます。このコンピュータはオンラインである必要があります。

パスワードによる保護を有効にした保護計画は、macOSを実行しているマシンに適用できますが、保護が提供されることはありません。Linuxを実行しているマシンにそのような計画を適用することはできません。

また同じWindowsマシンに対し、パスワードによる保護が有効になっている複数の保護計画を適用することはできません。発生する可能性のある競合を解決する方法については、「計画の競合の解決」を参照してください。

既存の保護計画のパスワードを変更するには

1. 保護計画では、**ウイルス対策およびマルウェア対策保護**モジュール（Cyber Backup Editionの**Active Protection**モジュール）を拡張します。
2. **[自己防御機能]** をクリックします。
3. **[新しいパスワードの作成]** をクリックします。
4. 開いたウィンドウで、保護されたWindowsエージェントのコンポーネントをアンインストールまたは変更するために必要なパスワードをコピーします。
   このパスワードは一意であり、このウィンドウを閉じるとリカバリできなくなります。このパスワードを紛失したり忘れたりした場合は、保護計画を編集して新しいパスワードを作成できます。

5. **[閉じる]** をクリックします。
6. **自己防御機能**ペインで、**[完了]** をクリックします。
7. 保護計画を保存します。

エージェントのアンインストール

ワークロードからエージェントをアンインストールすると、ワークロードは自動的にCyber Protectコンソールから削除されます。ネットワークの問題などの理由により、エージェントのアンインストール後もワークロードが表示される場合、コンソールから手動でこのワークロードを削除してください。この方法については、"Cyber Protectコンソールからワークロードを削除する"（325ページ）を参照してください。

注意
エージェントを削除しても、計画やバックアップは削除されません。

エージェントをアンインストールするには

Windows

1. エージェントが稼働するマシンに管理者としてサインインします。
2. **[コントロールパネル]** で、**[プログラムと機能]**（Windows XPでは **[プログラムの追加と削除]**）に移動します。
3. **Acronis Cyber Protect**を右クリックして、**[アンインストール]** を選択します。
4. （パスワードで保護されたエージェントの場合）エージェントをアンインストールするために必要なパスワードを指定して、**[次へ]** をクリックします。
5. （オプション）**[ログと構成の設定を削除する]** チェックボックスをオンにします。
   エージェントを再インストールする場合は、このチェックボックスをオフにします。チェックボックスを選択してエージェントを再インストールする場合、このワークロードはCyber Protectコンソール内で重複する可能性があります。また古いバックアップの関連付けが削除される可能性があります。
6. **[アンインストール]** をクリックします。

Linux

1. エージェントが稼働するマシンで、ルートユーザーとして`/usr/lib/Acronis/BackupAndRecovery/uninstall/uninstall`を実行します。
2. （オプション）**[製品のログ、タスク、格納域および構成の設定を削除する]** チェックボックスをオンにします。
   エージェントを再インストールする場合は、このチェックボックスをオフにします。チェックボックスを選択してエージェントを再インストールする場合、このワークロードはCyber Protectコンソール内で重複する可能性があります。また古いバックアップの関連付けが削除される可能性があります。
3. 操作を確定します。

macOS

1. エージェントが稼働するマシンで、インストール用の.dmgファイルをダブルクリックします。
2. インストールディスクイメージがオペレーティングシステムシステムにマウントされるのを待ちます。
3. イメージ内で、**[アンインストール]** をダブルクリックします。
4. 資格情報を求められた場合は、管理者の資格情報を入力します。
5. 操作を確定します。

Windowsエージェントにバンドルされたコンポーネントをアンインストールするには

Windowsエージェントをアンインストールせずに、Windowsエージェントにバンドルされている個別のコンポーネント（例: Cyber Protectモニタ、データ損失防止エージェント、ブータブルメディアビルダーなど）を個別にアンインストールできます。

1. エージェントが稼働するマシンに管理者としてサインインします。
2. セットアッププログラムを実行し、**[インストールされたコンポーネントを修正]** をクリックします。
3. アンインストールするコンポーネントの横にあるチェックボックスをオフにして、**[完了]** をクリックします。

VMwareエージェント（仮想アプライアンス）を削除するには

1. vSphereクライアントを使用してvCenter Serverにログインします。
2. （仮想アプライアンスがオンの場合）仮想アプライアンスを右クリックしてから、**[電源]** > **[電源オフ]** をクリックします。操作を確定します。
3. （仮想アプライアンスが仮想ディスク上でローカルに接続されているストレージを使用しており、そのディスク上にデータを保持したい場合）仮想アプライアンスから仮想ストレージを削除します。
   a. 仮想アプライアンスを右クリックし、**[設定の編集]** をクリックします。
   b. ストレージが存在するディスクを選択してから、**[削除]** をクリックします。
   c. **[削除オプション]** で、**[仮想マシンから削除]** をクリックします。
   d. **[OK]** をクリックします。
   その結果、ディスクがデータストアに保持されます。ディスクを別の仮想アプライアンスに接続することができます。
4. 仮想アプライアンスを右クリックし、**[ディスクから削除]** をクリックします。操作を確定します。
5. （オプション）（このアプライアンスを再度使用する予定がない場合）Cyber Protectコンソールで、**[バックアップストレージ]** > **[ロケーション]** をクリックし、ローカル接続のストレージに対応するロケーションを削除します。

保護の設定

Cyber Protectionの一般的な保護設定を変更するには、Cyber Protectコンソールで **[設定]** > **[保護]** に移動します。

コンポーネントの自動アップデート

デフォルトでは、すべてのエージェントからインターネット接続が可能であり、アップデートをダウンロードできます。

管理者は、利用している環境内で1つまたは複数のエージェントを選択し、それらのエージェントにアップデータの役割を割り当てることで、ネットワークの帯域幅のトラフィックを最小限に抑えることができます。これにより、専用のエージェントがインターネットに接続し、アップデート情報をダウンロードできます。他のすべてのエージェントは、ピアツーピア技術を使用して専用のアップデータエージェントに接続し、そこからアップデートプログラムをダウンロードします。

アップデータの役割を割り当てられていないエージェントは、環境内に専用のアップデータエージェントが存在しない場合や、専用のアップデータエージェントとの接続が約5分間にわたって確立できない場合に、インターネットに接続します。

アップデータエージェントは、ウイルス対策およびマルウェア対策保護、脆弱性診断、およびパッチ管理のためのアップデートおよびパッチを配布しますが、エージェントバージョンのアップデートは含まれません。

注意
アップデータロールを割り当てられているエージェントでは、Windowsのサードパーティ製品についてのみパッチのダウンロードおよび配信が可能です。Microsoft製品の場合、アップデータエージェントによるパッチ配信はサポートされていません。

エージェントにアップデータの役割を割り当てる前に、エージェントが動作するマシンが十分に強力であり、安定した高速インターネット接続と十分なディスク容量を備えていることを確認してください。

アップデータの役割に対応するマシンを準備するには

1. アップデータの役割を有効にする計画のエージェントマシンで、次のファイアウォールルールを適用します。
   - すべてのファイアウォールプロファイル（パブリック、プライベート、ドメイン）で、TCPポート18018および6888に対する「updater_incoming_tcp_ports」の着信（受信）接続を許可する。
   - すべてのファイアウォールプロファイル（パブリック、プライベート、ドメイン）で、UDPポート6888に対する「updater_incoming_udp_ports」の着信（受信）接続を許可する。
2. Acronisエージェントコアサービスを再起動します。
3. ファイアウォールサービスを再起動します。

これらのルールを適用せず、ファイアウォールを有効にしている場合、ピアエージェントがクラウドからアップデートプログラムをダウンロードします。

保護エージェントにアップデートロールを割り当てる

1. Cyber Protectコンソールで **[設定]** > **[エージェント]** に進みます。
2. アップデートロールを割り当てるエージェントがインストールされているマシンを選択します。
3. **[詳細]** をクリックしてから、**[このエージェントを使用してパッチとアップデートをダウンロードし、配布します]** スイッチを有効化します。

ピアツーピアアップデートは以下のように動作します。

1. アップデートロールのエージェントがスケジュールに従ってサービスプロバイダーからのインデックスファイルを確認し、コアコンポーネントをアップデートします。
2. アップデートロールのエージェントがアップデートのダウンロードを開始し、すべてのエージェントに配布します。

環境内の複数のエージェントにアップデータの役割を割り当てることができます。つまり、アップデータの役割を割り当てられたエージェントがオフラインの場合、この役割を割り当てられた他のエージェントが定義更新のソースとして動作します。

スケジュールに従ってCyber Protectionの定義をアップデートする

[スケジュール] タブでは、次の各コンポーネントに対してCyber Protectionの定義の自動アップデートスケジュールを設定できます。

- マルウェア対策
- 脆弱性診断
- パッチ管理

定義アップデートの設定を変更するには、**[設定]** > **[保護]** > **[保護定義のアップデート]** > **[スケジュール]** に移動します。

スケジュールの種類:

- **日単位** - 週のどの曜日に定義をアップデートするかを指定します。
  開始時刻 - 定義をアップデートする時刻を選択します。
- **時間単位** - アップデートスケジュールを時間単位でより細かく指定します。
  次の間隔で実行 – アップデートを実行する期間を指定します。
  開始時刻 ...**終了時刻** – アップデートの特定の時間範囲を指定します。

オンデマンドでCyber Protectionの定義をアップデートする

特定のマシンのCyber Protectionの定義をオンデマンドでアップデートする

1. Cyber Protectコンソールで **[設定]** > **[エージェント]** に進みます。
2. 保護定義をアップデートするマシンを選択し、**[定義のアップデート]** をクリックします。

キャッシュストレージ

キャッシュデータのロケーションは以下の通りです。

- Windowsマシン:`C:\ProgramData\Acronis\Agent\var\atp-downloader\Cache`
- Linuxマシン: `/opt/acronis/var/atp-downloader/Cache`
- macOSマシン: `/Library/Application Support/Acronis/Agent/var/atp-downloader/Cache`

キャッシュストレージの設定を変更するには、**[設定]** > **[保護]** > **[保護定義のアップデート]** > **[キャッシュストレージ]** に移動します。

[古いアップデートファイルとパッチ管理データ] で、キャッシュデータを削除するまでの経過時間を指定します。

エージェントの最大キャッシュストレージサイズ（GB）：

- **アップデートロール** - アップデートロールを持つマシンのキャッシュのストレージサイズを指定します。
- **その他のロール** - その他のマシンのキャッシュのストレージサイズを指定します。

注意
Cyber Protectionでは、検出されたマルウェアのサンプルを収集し、追加分析を行うことで、ソフトウェアの改善に役立てています。この設定は、**[保護]** タブの **[マルウェアのサンプルを収集し、CPOCにアップロード]** トグルを無効にすることで、いつでも変更できます。

マシンのサービスクォータの変更

サービスクォータは、保護計画が最初にマシンに適用されるときに、自動的に割り当てられます。

保護されているマシンの種類、オペレーティングシステム、必要な保護レベル、クォータの可用性に応じて、もっとも適切なクォータが割り当てられます。組織内でもっとも適切なクォータが利用できない場合、次善に適切なクォータが割り当てられます。例えば、もっとも適切なクォータが**Webホスティングサーバー**であるものの、それが利用できない場合、**サーバー**のクォータが割り当てられます。

クォータ割り当ての例:

- Windows ServerまたはLinuxサーバーのオペレーティングシステム（Ubuntuサーバーなど）を実行する物理マシンには、**サーバー**クォータが割り当てられます。
- WindowsまたはLinuxデスクトップオペレーティングシステム（Ubuntuデスクトップなど）を実行する物理マシンには、**ワークステーション**クォータが割り当てられます。
- Hyper-Vロールが有効化されたWindows 10を実行する物理マシンには、**ワークステーション**クォータが割り当てられます。
- 仮想デスクトップインフラ上で動作し、プロテクションエージェントがゲストオペレーティングシステム内にインストールされているデスクトップマシン（例:Windowsエージェント）には、**仮想マシン**クォータが割り当てられます。このタイプのマシンの場合、**仮想マシン**クォータが使用できないときに、**ワークステーション**クォータを使用することもできます。
- 仮想デスクトップインフラ上で動作し、エージェントレスモード（VMwareエージェントまたはHyper-Vエージェントなど）でバックアップされるデスクトップマシンには、**仮想マシン**クォータが割り当てられます。
- Hyper-VまたはvSphereサーバーには、**サーバー**クォータが割り当てられます。
- cPanelまたはPleskが動作するサーバーには、**Webホスティングサーバー**クォータが割り当てられます。また、Webホスティングサーバークォータが使用できない場合、Webサーバーが実行されているマシンのタイプに応じて、**仮想マシン**または**サーバー**クォータを使用することもできます。
- アプリケーション認識型バックアップの場合、ワークステーションであっても**サーバー**クォータが必要です。

元の割り当ては後から手動で変更できます。たとえば、同じマシンにさらに高度な保護計画を適用するには、マシンのサービスクォータをアップグレードする必要が生じる場合があります。その保護計画で必要となる機能が、現在割り当てられているサービスクォータでサポートされていない場合、保護計画は失敗します。

また、クォータの割り当てが行われた後に、より適切なクォータを購入した場合は、サービスクォータを変更できます。例えば、仮想マシンに**ワークステーション**クォータが割り当てられている場合がこれに相当します。**仮想マシン**クォータを購入した後、元の**ワークステーション**クォータではなく、購入したクォータをマシンに手動で割り当てることができます。

また、現在割り当てられているサービスクォータを解放して、それを別のマシンに割り当てることもできます。

個別マシンまたはマシンのグループのサービスクォータを変更できます。

個別マシンのサービスクォータを変更するには

1. Cyber Protectコンソールで **[デバイス]** に進みます。
2. 対象のマシンを選択して、**[詳細]** をクリックします。
3. **[サービスクォータ]** セクションで、**[変更]** をクリックします。
4. **[クォータの変更]** ウィンドウで、希望するサービスクォータまたは **[クォータなし]** を選択し、**[変更]** をクリックします。

マシンのグループのサービスクォータを変更するには

1. Cyber Protectコンソールで **[デバイス]** に進みます。
2. 複数のマシンを選択し、**[クォータの割り当て]** をクリックします。
3. **[クォータの変更]** ウィンドウで、希望するサービスクォータまたは **[クォータなし]** を選択し、**[変更]** をクリックします。

ご利用の環境にインストールされているCyber Protectionサービス

Cyber Protectionでは、使用中のCyber Protectionオプションに応じて、以下の一部またはすべてのサービスがインストールされます。

Windowsにインストールされるサービス

サービス名	用途
Acronis Managed Machine Service	バックアップ、復元、レプリケーション、保持、ベリファイ機能を提供します
Acronis Scheduler2 Service	特定のイベント発生時にスケジュールされたタスクを実行します
Acronis Active Protection Service	ランサムウェアに対する保護を提供します

Acronis Cyber Protection Service	マルウェア対策保護機能を提供します

macOSにインストールされるサービス

サービス名と場所	用途
/Library/LaunchDaemons/com.acronis.aakore.plist	エージェントと管理コンポーネント間の通信サービス
/Library/LaunchDaemons/com.acronis.cyber-protect-service.plist	マルウェアの検出機能を提供
/Library/LaunchDaemons/com.acronis.mms.plist	バックアップおよび復元機能を提供
/Library/LaunchDaemons/com.acronis.schedule.plist	スケジュールされたタスクを実行

エージェントログファイルを保存する

エージェントのログを.zipファイルに保存できます。不明の理由でバックアップが失敗した場合、テクニカルサポートの担当者から、エージェントのログ取得を依頼する場合があります。

デフォルトではログの情報は過去3日間について最適化されますが、この期間を変更することもできます。

エージェントのログを取得するには

1. 次のいずれかを実行します。
   - **[デバイス]** で、ログ取得の対象となるマシンを選択し、**[アクティビティ]** をクリックします。
   - **[設定]** > **[エージェント]** で、ログ取得の対象となるマシンを選択し、**[詳細]** をクリックします。
2. （オプション） システム情報が含まれるデフォルトの期間を変更するには、**[システム情報の収集]** ボタンの横にある矢印をクリックし、期間を選択します。
3. **[システム情報の収集]** をクリックします。
4. Webブラウザ上でメッセージが表示されたら、ファイルの保存先を指定します。

サイトツーサイトOpen VPN - 追加情報

復元サーバーを作成する場合、サーバーで**稼働中のネットワークのIPアドレス**を構成し、**テストIPアドレス**を行います。

フェールオーバーを実行し（仮想マシンをクラウドで稼働させ）、仮想マシンにログインしてサーバーのIPアドレスを確認します。**稼働中のネットワークのIPアドレス**が表示されているはずです。

テストフェールオーバーを実行する場合、テストサーバーへのアクセスには、**テストIPアドレス**を使用する必要があります。このIPアドレスは、復元サーバーの構成でのみ表示されます。

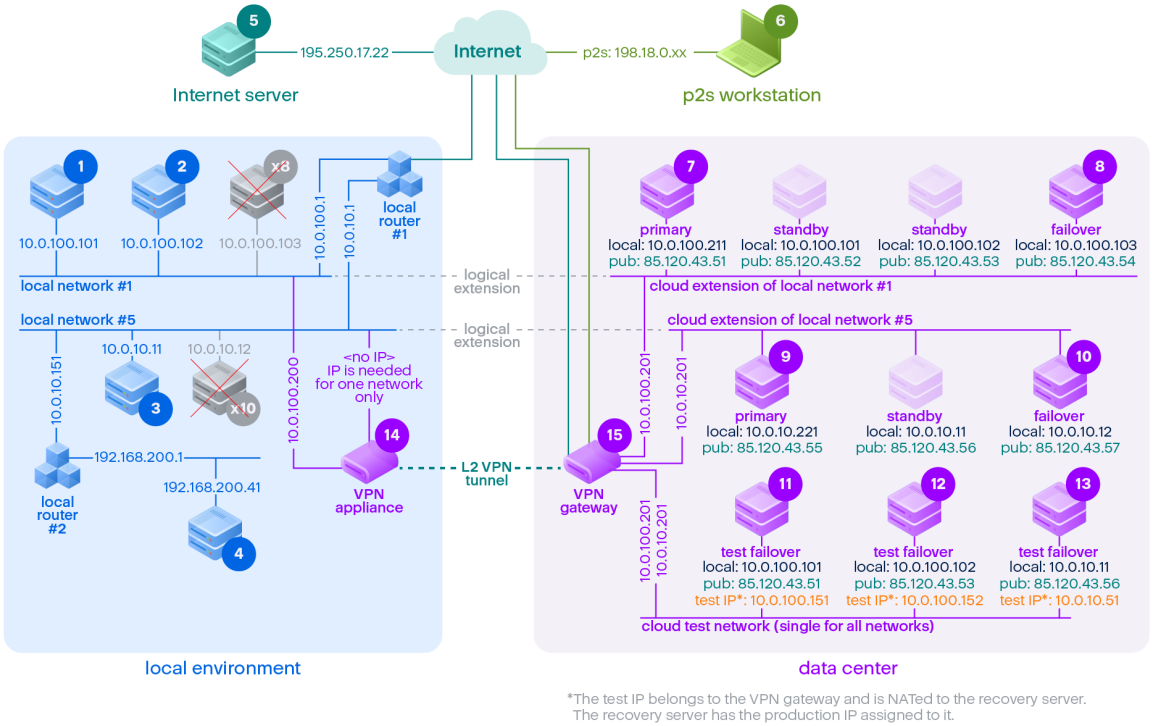
ローカルサイトからテストサーバーにアクセスするには、**テストIPアドレス**を使用する必要があります。

注意

サーバーのネットワーク構成には、常に**稼働中のネットワークのIPアドレス**が表示されます（テストサーバーは、稼働中のサーバーの状態をミラーリングするため）。これは、テスト用IPアドレスがテストサーバーではなく、VPNゲートウェイに属していて、NATにより稼働中のIPアドレスに変換されるためです。

次の図は、サイト間Open VPN構成の例を示しています。ローカル環境の一部のサーバーは、フェールオーバーを使用してクラウドにリカバリされます（ネットワークインフラストラクチャへの影響はありません）。

1. カスタマーが以下の方法によりディザスタリカバリを有効化しました:
   a. VPNアプライアンス（14）を構成し、それを専用のクラウドVPNサーバー（15）に接続する
   b. 一部のローカルサーバーをディザスタリカバリで保護する（1、2、3、x8、x10）
      ローカルサイトの一部のサーバー（4など）は、VPNアプライアンスへの接続がないネットワークに接続されています。このようなサーバーは、ディザスタリカバリで保護されていません。
2. 一部のサーバー（異なるネットワークに接続）は、ローカルサイトで動作しています:（1、2、3、4）
3. 保護済みのサーバー（1、2、3）は、テストフェールオーバーでテストされています（11、12、13）
4. ローカルサイトの一部のサーバーは、利用できません（x8、x10）。これらは、フェールオーバーの実行後、クラウドで利用可能になります（8および10）。
5. クラウド環境では、異なるネットワークに接続されたいくつかのプライマリサーバー（7、9）が利用できます
6. （5）は、パブリックIPアドレスを持つインターネット上のサーバーです
7. （6）はポイントツーサイトVPN接続（p2s）でクラウドに接続されているワークステーションです



この例では、**From:**列のサーバーから**To:**列のサーバーに対して、以下のような接続設定が利用できます（たとえば、「ping」）。

	[終了日:]	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**
[開始時刻:]		ローカル	ローカル	ローカル	ローカル	インターネット	p2s	プライマリ	フェールオーバー	プライマリ	フェールオーバー	テストフェールオーバー	テストフェールオーバー	テストフェールオーバー	VPNアプライアンス	VPNサーバー
1	ローカル		ダイレクト	ローカルルーター1経由	ローカルルーター2経由	ローカルルーター1およびインターネット経由	いいえ	トンネル:local経由 ローカルルーター1およびインターネット:pub経由	トンネル:local経由 ローカルルーター1およびインターネット:pub経由	トンネル:local経由 ローカルルーター1およびインターネット:pub経由	トンネル:local経由 ローカルルーター1およびインターネット:pub経由	トンネル経由:NAT（VPNサーバー） ローカルルーター1およびインターネット:pub経由	トンネル経由:NAT（VPNサーバー） ローカルルーター1およびインターネット:pub経由	ローカルルーター1およびトンネル経由:NAT（VPNサーバー） ローカルルーター1およびインターネット:pub経由	ダイレクト	いいえ

	[終了日:]	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
2	ローカル	ダイレクト		ローカルルーター1経由	ローカルルーター2経由	ローカルルーター1およびインターネット経由	いいえ	トンネル:local経由 ローカルルーター1およびインターネット:pub経由	トンネル:local経由 ローカルルーター1およびインターネット:pub経由	トンネル:local経由 ローカルルーター1およびインターネット:pub経由	トンネル:local経由 ローカルルーター1およびインターネット:pub経由	トンネル経由:NAT（VPNサーバー） ローカルルーター1およびインターネット:pub経由	トンネル経由:NAT（VPNサーバー） ローカルルーター1およびインターネット:pub経由	ローカルルーター1およびトンネル経由:NAT（VPNサーバー） ローカルルーター1およびインターネット:pub経由	ダイレクト	いいえ
3	ローカル	ローカルルーター1経由	ローカルルーター1経由		ローカルルーター2経由	ローカルルーター1およびインターネット経由	いいえ	トンネル:local経由 ローカルルーター1およびイン	トンネル:local経由 ローカルルーター1およびイン	トンネル:local経由 ローカルルーター1およびイン	トンネル:local経由 ローカルルーター1およびイン	トンネル経由:NAT（VPNサーバー） ローカル	トンネル経由:NAT（VPNサーバー） ローカル	ローカルルーター1およびトンネル経由:NAT（VPN	ローカルルーター経由	いいえ

	[終了日:]	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
								ターネット:pub経由	ターネット:pub経由	ターネット:pub経由	ターネット:pub経由	ルーター1およびインターネット:pub経由	ルーター1およびインターネット:pub経由	サーバー） ローカルルーター1およびインターネット:pub経由		
4	ローカル	ローカルルーター2およびルーター1経由	ローカルルーター2およびルーター1経由	ローカルルーター2経由		ローカルルーター2、およびルーター1、およびインターネット経由	いいえ	ローカルルーター2およびトンネル経由:ローカル ローカルルーター2、およびローカルルーター1、およ	ローカルルーター2およびトンネル経由:ローカル ローカルルーター2、およびローカルルーター1、およ	ローカルルーター2およびトンネル経由:ローカル ローカルルーター2、およびローカルルーター1、およ	ローカルルーター2およびトンネル経由:ローカル ローカルルーター2、およびローカルルーター1、およ	トンネル経由:NAT（VPNサーバー） ローカルルーター2、およびルーター1、およびインターネット:	トンネル経由:NAT（VPNサーバー） ローカルルーター2、およびルーター1、およびインターネット:	トンネル経由:NAT（VPNサーバー） ローカルルーター2、およびルーター1、およびインターネット:	ローカルルーター2経由	いいえ

	[終了日:]	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
								びインターネット:pub経由	びインターネット:pub経由	びインターネット:pub経由	びインターネット:pub経由	pub経由	pub経由	pub経由		
5	インターネット	いいえ	いいえ	いいえ	いいえ		使用不可	インターネット:pub経由	インターネット:pub経由	インターネット:pub経由	インターネット:pub経由	インターネット:pub経由	インターネット:pub経由	インターネット:pub経由	いいえ	いいえ
6	p2s	いいえ	いいえ	いいえ	いいえ	インターネット経由		p2s VPN（VPNサーバー）:local経由 インターネット:pub経由	p2s VPN（VPNサーバー）:local経由 インターネット:pub経由	p2s VPN（VPNサーバー）:local経由 インターネット:pub経由	p2s VPN（VPNサーバー）:local経由 インターネット:pub経由	p2s VPN経由-NAT（VPNサーバー） インターネット:pub経由	p2s VPN経由-NAT（VPNサーバー） インターネット:pub経由	p2s VPN経由-NAT（VPNサーバー） インターネット:pub経由	いいえ	いいえ
7	プライマリ	トンネル経由	トンネル経由	トンネルおよびローカ	トンネルおよびローカ	インターネット経由（VPNサーバー経由）	いいえ		クラウドダイレクト:local	トンネルおよびローカルルーター1:local経由	トンネルおよびローカルルーター1:local経由	VPNサーバー経由:NAT	VPNサーバー経由:NAT	トンネルおよびローカルルーター1経由:NAT	いいえ	DHCPおよびDNSプロトコルのみ

	[終了日:]	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
				ルーター1経由	ルーター1/2経由											
8	フェールオーバー	トンネル経由	トンネル経由	トンネルおよびローカルルーター1経由	トンネルおよびローカルルーター1/2経由	インターネット経由（VPNサーバー経由）	いいえ	クラウドダイレクト: local		トンネルおよびローカルルーター1: local経由	トンネルおよびローカルルーター1: local経由	VPNサーバー経由:NAT	VPNサーバー経由:NAT	トンネルおよびローカルルーター1経由:NAT	いいえ	DHCPおよびDNSプロトコルのみ
9	プライマリ	トンネルおよびローカルルー	トンネルおよびローカルルー	トンネル経由	トンネル経由	インターネット経由（VPNサーバー経由）	いいえ	トンネルおよびローカルルーター1: local経由	トンネルおよびローカルルーター1: local経由		クラウドダイレクト: local	トンネルおよびローカルルーター1経由:NAT	トンネルおよびローカルルーター1経由:NAT	VPNサーバー経由:NAT	いいえ	DHCPおよびDNSプロトコルのみ

	[終了日:]	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
		ター1経由	ター1経由													
10	フェールオーバー	トンネルおよびローカルルーター1経由	トンネルおよびローカルルーター1経由	トンネル経由	トンネル経由	インターネット経由（VPNサーバー経由）	いいえ	トンネルおよびローカルルーター1:local経由	トンネルおよびローカルルーター1:local経由	クラウドダイレクト:local		トンネルおよびローカルルーター1経由:NAT	トンネルおよびローカルルーター1経由:NAT	VPNサーバー経由:NAT	いいえ	DHCPおよびDNSプロトコルのみ
11	テストフェールオーバー	いいえ	いいえ	いいえ	いいえ	インターネット経由（VPNサーバー経由）	いいえ	いいえ	いいえ	いいえ	いいえ		クラウドダイレクト:local	VPNサーバー:local経由（ルーティング）	いいえ	DHCPおよびDNSプロトコルのみ
12	テストフェールオーバー	いいえ	いいえ	いいえ	いいえ	インターネット経由（V	いいえ	いいえ	いいえ	いいえ	いいえ	クラウドダイレクト:local		VPNサーバー:local経由（ル	いいえ	DHCPおよびDNSプ

	[終了日:]	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
						PNサーバー経由）								ーティング）		ロトコルのみ
13	テストフェールオーバー	いいえ	いいえ	いいえ	いいえ	インターネット経由（VPNサーバー経由）	いいえ	いいえ	いいえ	いいえ	いいえ	VPNサーバー: local経由（ルーティング）	VPNサーバー: local経由（ルーティング）		いいえ	DHCPおよびDNSプロトコルのみ
14	VPNアプライアンス	ダイレクト	ダイレクト	ローカルルーター1経由	ローカルルーター2経由	インターネット経由（ローカルルーター1）	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ		いいえ
15	VPNサーバー	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	

オンプレミス管理サーバーのライセンス管理

オンプレミス管理サーバーを有効化する方法、またはオンプレミス管理サーバーにライセンスを割り当てる方法の詳細については、『Cyber Protectユーザーガイド』の「ライセンス」セクションを参照してください。

保護の対象と方法を定義する

管理タブ

注意
この機能を利用できるかどうかは、現在のアカウントで有効になっているサービスクォータによって異なります。

作成したすべての計画は、コンソールの **[管理]** タブで利用できます。

以下のセクションがあります。

- **保護計画**
- **リモート管理計画**
- **スクリプト計画**
- **計画の監視**
- **スクリプトのリポジトリ**
- **クラウドアプリケーションバックアップ**
- **バックアップスキャン**
- **バックアップのレプリケーション**
- **ベリファイ**
- **クリーンアップ**
- **VMへの変換**
- **VMレプリケーション**

計画ステータス

保護計画とVMレプリケーション計画の場合、ステータスバーには以下のようにステータスが色分けされて表示されます。

- OK（緑）
- 警告（オレンジ）
- エラー（濃いオレンジ）
- 重大（赤）
- 計画が実行中（青）
- 計画が無効（グレー）

ステータスバーをクリックし、計画が適用されているすべてのワークロードに関する計画ステータスの詳細を表示します。

特定のステータスをクリックすると、そのステータスのすべてのワークロードのリストが表示されます。

保護計画

[管理] > **[保護計画]** タブでは、既存の保護計画に関する情報の確認、保護計画に関する操作の実行、新しい計画の作成が可能です。

保護計画に関する詳細については、"保護計画とモジュール"（209ページ）を参照してください。

クラウドアプリケーションのバックアップ計画

[管理] > **[クラウドアプリケーションバックアップ]** タブには、クラウドツークラウドバックアップ計画が表示されます。これらの計画では、クラウド内で実行され、クラウドストレージをバックアップロケーションとして使用するエージェントにより、クラウド内で実行されているアプリケーションをバックアップします。

このセクション内では、以下の操作を実行できます。

- バックアップ計画の作成、表示、実行、停止、編集、および削除
- 各バックアップ計画に関連するアクティビティを表示
- 各バックアップ計画に関連するアラートを表示

クラウドアプリケーションバックアップの詳細については、以下を参照してください。

- Microsoft 365データの保護
- Google Workspaceデータの保護

クラウドからクラウドへのバックアップの手動実行

Cyber Protectionサービスが中断されるのを避けるため、手動のクラウドツークラウドバックアップの実行回数は、Microsoft 365またはGoogle Workspaceの各組織について1時間当たり10回までに制限されています。この回数に達すると、許可される実行回数は1時間に1回にリセットされ、その後は1時間当たり合計10回の実行に達するまで、1時間ごとに1回の追加の実行が可能になります（例：1時間目は10回の実行、2時間目は1回の実行、3時間目は2回の実行）。

デバイスのグループ（メールボックス、ドライブ、サイト）、または10個を超えるデバイスを含むグループに適用されたバックアップ計画は、手動で実行できません。

バックアップスキャンの計画

バックアップのマルウェア（ランサムウェアを含む）をスキャンするには、バックアップスキャン計画を作成します。

重要
バックアップスキャン計画は、一部のワークロードとバックアップストレージではサポートされていません。詳細については、"制限事項"（841ページ）を参照してください。

バックアップスキャン計画を作成する手順

1. Cyber Protectコンソールで **[管理]** > **[バックアップスキャン]** に進みます。
2. **[計画の作成]** をクリックします。
3. 計画の名前と以下のパラメータを指定します。
   - **スキャンの種類**:
     - **クラウド** - このオプションは変更できません。自動的に選択されたクラウドエージェントが、バックアップスキャンを実行します。
   - **スキャン対象のバックアップ**:
     - **ロケーション** - スキャンするバックアップセットのロケーションを選択します。
     - **バックアップ** - スキャンするバックアップセットを選択します。
   - **スキャン対象**:
     - **マルウェア** - このオプションは変更できません。スキャンでは、選択したバックアップセットにおけるマルウェア（ランサムウェアを含む）の有無が確認されます。
   - **暗号化** - 暗号化されたバックアップセットをスキャンするために、暗号化パスワードを指定します。ロケーションまたは複数のバックアップセットを選択しているにも関わらず、指定したパスワードがバックアップセットと一致しない場合、アラートが作成されます。
   - **スケジュール** - このオプションは変更できません。クラウドストレージでは、自動的にスキャンが開始されます。
4. **[作成]** をクリックします。

その結果、バックアップスキャン計画が作成され、クラウドエージェントにより指定されたロケーションまたはバックアップセットを対象にマルウェアのスキャンが実行されます。

オフホストのデータ処理

注意
この機能は、Advanced Backupパックの一部として**Advanced Backup - Servers**または**Advanced Backup - NASの**クォータが有効になっているカスタマーテナントで使用できます。

レプリケーション、検証、クリーンアップは通常、バックアップを実行するプロテクション エージェントによって実行されます。このため、バックアッププロセスが完了した後でも、エージェントが実行されているマシンにさらに負荷がかかります。マシンの負荷を軽減するには、オフホストデータ保護計画、つまりレプリケーション、検証、クリーンアップ、および仮想マシンへの変換のための個別の計画を作成します。

オフホストデータ保護計画で、以下のことが可能です。

- バックアップとオフホストデータ保護操作に異なるエージェントを選択する
- ネットワークの帯域幅の消費を最小限に抑えるため、オフピークの時間帯にオフホストデータ処理操作をスケジュールする
- オフホストデータ処理専用のエージェントをインストールしない場合に、オフホストデータ処理操作を営業時間外にスケジュールする

注意
オフホストデータ処理計画は、プロテクション エージェントがインストールされているマシンの時間設定（タイムゾーンを含む）に従って実行されます。仮想アプライアンス（Agent for VMware、Agent for Scale Computing HC3など）の場合、エージェントのグラフィカルユーザーインターフェイスでタイムゾーンを設定できます。

バックアップのレプリケーション

注意
この機能は、Advanced Backupパックの一部として**Advanced Backup - Servers**または**Advanced Backup - NASの**クォータが有効になっているカスタマーテナントで使用できます。

バックアップのレプリケーションで、バックアップが別のロケーションにコピーされます。オフホストデータ処理操作のため、バックアップのレプリケーション計画で構成されます。

バックアップのレプリケーションは、保護計画の一部にすることもできます。このオプションの詳細については、"レプリケーション"（428ページ）を参照してください。

バックアップのレプリケーション計画の作成

オフホストデータ処理としてバックアップのレプリケートを実行するために、バックアップのレプリケーション計画を作成します。

バックアップのレプリケーション計画を作成する

1. Cyber Protectコンソールで、**[管理]** > **[バックアップのレプリケーション]** をクリックします。
2. **[計画の作成]** をクリックします。
3. **[エージェント]** で、レプリケーションを実行するエージェントを選択します。
   ソースロケーションとレプリケーションロケーションの両方にアクセスできるエージェントを選択できます。
4. **[レプリケートする項目]** で、レプリケートするアーカイブまたはバックアップロケーションを選択します。
   アーカイブとロケーションを切り替えるには、右上隅の **[ロケーション]** / **[バックアップ]** スイッチを使用します。
   複数の暗号化されたアーカイブを選択した場合、それらの暗号化パスワードは同じでなければなりません。異なる暗号化パスワードを使用しているアーカイブがある場合は、別個の計画を作成します。
5. **[レプリケーション先]** で、レプリケーションのロケーションを指定します。
6. **[レプリケーション方法]** で、レプリケートするバックアップ（別名: 復元ポイント）を選択します。
   次から選択できます。
   - **すべてのバックアップ**
   - **完全バックアップのみ**
   - **最後のバックアップのみ**

これらのオプションの詳細については、"レプリケーション対象"（195ページ）を参照してください。

7. **[スケジュール]** で、レプリケーションのスケジュールを構成します。
   バックアップのレプリケーション計画のスケジュールを構成する際は、バックアップのレプリケーションが開始されるときに、最後にレプリケートされたバックアップが元のロケーションで利用可能な状態になっていることを確認してください。もし、このアーカイブが元のロケーションで利用できない場合（例: 保持ルールによって削除された場合）、全体のバックアップセットが完全バックアップとしてレプリケートされます。これは非常に時間がかかる可能性があり、追加のストレージスペースを消費します。
8. **[保持ルール]** で、ターゲットロケーションの保持ルールを指定します。
   次から選択できます。
   - **バックアップの数**
   - **バックアップ世代**（月単位、週単位、日単位、時間単位のバックアップ）
   - **バックアップの合計サイズ別**
   - **バックアップを無期限に保存する**

     注意
     このオプションを選択すると、ストレージの使用量が増えます。不要なバックアップは手動で削除する必要があります。
9. （**[レプリケートする項目]** で暗号化されたアーカイブが選択されている場合）、**[バックアップパスワード]** スイッチを有効にして、暗号化パスワードを入力してください。
10. （オプション） 計画のオプションを変更するには、ギアアイコンをクリックしてから、必要に応じてオプションを構成します。
11. **[作成]** をクリックします。

レプリケーション対象

注意
ロケーション全体のレプリケーションやバックアップセットの全バックアップのレプリケーションなど、一部のレプリケーション処理には非常に時間がかかる場合があります。

個別のバックアップセットまたはバックアップロケーション全体のレプリカを作成できます。バックアップロケーションのレプリカを作成する場合、ロケーションに存在するすべてのバックアップセットのレプリカが作成されます。

バックアップセットは、バックアップ（復元ポイントとも呼ばれる）で構成されています。レプリカを作成するバックアップを選択する必要があります。

次から選択できます。

- **すべてのバックアップ**
  レプリケーション計画が実行されるたびに、バックアップセット内のすべてのバックアップについてレプリカが作成されます。

- **完全バックアップのみ**
  レプリカが作成されるのは、バックアップセット内の完全バックアップのみです。
- **最後のバックアップのみ**
  タイプ（フル、差分、または増分）に関わらず、バックアップセット内の最新のバックアップについてのみ、レプリカが作成されます。

ニーズと使用するバックアップスキームに応じて、オプションを選択してください。例えば、**常に増分（単一ファイル）**バックアップスキームを使用していて、最新の増分バックアップのみをレプリケートする場合は、バックアップのレプリケーション計画で **[前回のバックアップのみ]** を選択します。

次の表は、各バックアップスキームでどのバックアップのレプリカが作成されるかをまとめたものです。

	常に増分（単一ファイル）	常に完全	週単位で完全、日単位で増分	月単位で完全、週単位で差分、日単位で増分（GFS）
すべてのバックアップ	バックアップセット内のすべてのバックアップ	バックアップセット内のすべてのバックアップ	バックアップセット内のすべてのバックアップ	バックアップセット内のすべてのバックアップ
完全バックアップのみ	最初のバックアップ（フルバックアップ）のみ	すべてのバックアップ	毎週1件のバックアップ*	毎月1件のバックアップ*
前回のバックアップ	バックアップセット内の最新のバックアップ*	バックアップセット内の最新のバックアップ*	バックアップセット内の最新のバックアップ（タイプに関わらず）*	バックアップセット内の最新のバックアップ（タイプに関わらず）*

*バックアップのレプリケーション計画のスケジュールを構成する際は、バックアップのレプリケーションが開始されるときに、最後にレプリケートされたバックアップが元のロケーションで利用可能な状態になっていることを確認してください。もし、このアーカイブが元のロケーションで利用できない場合（例: 保持ルールによって削除された場合）、全体のバックアップセットが完全バックアップとしてレプリケートされます。これは非常に時間がかかる可能性があり、追加のストレージスペースを消費します。

サポートされるロケーション

次の表は、バックアップのレプリケーション計画でサポートされるバックアップロケーションをまとめたものです。

バックアップロケーション	ソースとしてサポートされる	ターゲットとしてサポートされる
クラウドストレージ	+	+
ローカルフォルダ	+	+
ネットワークフォルダ	+	+

バックアップロケーション	ソースとしてサポートされる	ターゲットとしてサポートされる
パブリッククラウド	+	+
NFSフォルダ	–	–
Secure Zone	–	–

ベリファイ

注意
この機能は、Advanced Backupパックの一部として**Advanced Backup - Servers**または**Advanced Backup - NASの**クォータが有効になっているカスタマーテナントで使用できます。

バックアップを検証して、そのバックアップからデータをリカバリできることを検証します。

オフホストデータ処理としてバックアップを検証するために、検証計画を作成します。いずれかを作成する方法については、"検証計画の作成"（198ページ）を参照してください。

以下の検証メソッドが利用可能です。

- チェックサムのベリファイ
- 仮想マシンとして実行
  - VMハートビート
  - スクリーンショット検証

1つまたは複数のメソッドを選択できます。複数の検証メソッドを選択した場合、それぞれの検証メソッドが連続して実行されます。メソッドの詳細については、"VMハートビート"（201ページ）を参照してください。

バックアップセットまたはバックアップロケーションを検証できます。バックアップロケーションの検証では、そのロケーション内のすべてのバックアップセットが検証されます。

サポートされるロケーション

サポートされているバックアップロケーションと検証メソッドを次の表に示します。

注意
パブリッククラウドからアーカイブ全体を読み取るには膨大なコストがかかるため、検証オプションはパブリッククラウドのバックアップでは使用できません。

バックアップロケーション	チェックサムのベリファイ	仮想マシンとして実行	
		VMハートビート	スクリーンショット検証
クラウドストレージ	+	+	+

バックアップロケーション	チェックサムのベリファイ	仮想マシンとして実行	
		VMハートビート	スクリーンショット検証
ローカルフォルダ	+	+	+
ネットワークフォルダ	+	+	+
NFSフォルダ	–	–	–
Secure Zone	–	–	–

検証ステータス

検証が成功したバックアップに、緑のドットと**検証済み**というラベルが表示されます。

検証に失敗した場合、バックアップには赤いドットが表示されます。使用した検証メソッドのいずれかで問題が発生した場合、検証は失敗となります。検証計画の構成に誤りがある場合、こういった結果が生じます。例えば、正しくないホスト上の仮想マシンに**VMハートビート**メソッドが使用されている場合などがこれに当たります。

バックアップの検証ステータスは、新しい検証操作が実行されるごとにアップデートされます。各検証メソッドのステータスは個別にアップデートされます。そのため、いずれかの検証メソッドで失敗したバックアップの検証は、同じ検証メソッドが成功するまで失敗と表示されます。つまり、直近の検証操作で以前失敗した方法が使用されず、これが正常に完了した場合でも、失敗の表示が継続します。

検証ステータスを確認する方法の詳細については、"バックアップの検証ステータスを確認する"（203 ページ）を参照してください。

検証計画の作成

オフホストデータ処理としてバックアップセットを検証するために、検証計画を作成します。

検証計画を作成するには

1. Cyber Protectコンソールで、**[管理]** > **[検証]** をクリックします。
2. **[計画の作成]** をクリックします。
   新しい検証計画のテンプレートが開きます。
3. （オプション） 計画名を変更するには、デフォルト名をクリックします。
4. **エージェント**で、検証を実行するエージェントを選択し、**[OK]** をクリックします。
   バックアップから仮想マシンを実行して検証を行う場合は、VMwareエージェントまたはHyper-Vエージェントが動作するマシンを選択します。それ以外の場合は、バックアップロケーションにアクセスできる任意のマシンを選択します。
5. **検証する項目**で、検証するバックアップセットを選択してください。
   a. 右上角の**[ロケーション]**または**[バックアップ]**をクリックして、計画のスコープ（各バックアップセットまたはロケーション全体）を選択します。

選択したバックアップが暗号化されている場合、すべてのバックアップで同じ暗号化パスワードを使用する必要があります。異なる暗号化パスワードを使用しているバックアップがある場合は、別個の計画を作成します。

b. **[追加]** をクリックします。

c. 検証計画のスコープに応じて、ロケーション、またはロケーションとバックアップセットを選択し、**[完了]** をクリックします。

d. **[完了]** をクリックします。

6. **検証の対象**で、選択したバックアップセット内で検証するバックアップ（別称:復元ポイント）を選択します。次から選択できます。
   - **すべてのバックアップ**
   - **最後のバックアップのみ**
7. **検証方法**で、検証メソッドを選択します。
   次のオプションから1つまたは2つを選択します。
   - **チェックサムのベリファイ**
   - **仮想コンピュータとしての実行**

   メソッドの詳細については、"VMハートビート"（201ページ）を参照してください。
8. （**チェックサムのベリファイ**を選択している場合）**[完了]** をクリックします。
9. （**仮想マシンとしての実行**を選択している場合）。このメソッドの設定を構成します。
   a. **[ターゲットマシン]** で、仮想マシンのタイプ（ESXiまたはHyper-V）、ホスト、マシン名のテンプレートを選択して、**[OK]** をクリックします。
   デフォルトの名前は **[マシン名]_validate** です。

   b. **[データストア]**（ESXiの場合）または **[パス]**（Hyper-Vの場合）で、仮想マシンのデータストアを選択します。

   c. **仮想マシンとしての実行**で利用可能な検証メソッドのどちらかまたは両方を選択します。
      - **VMハートビート**
      - **スクリーンショット検証**

   d. （オプション） **[VM設定]** をクリックして、仮想マシンのメモリサイズとネットワーク接続を変更します。
   デフォルトでは、仮想マシンはネットワークに接続されていません。また、仮想マシンのメモリサイズは、元のマシンと同じです。

   e. **[完了]** をクリックします。
10. （オプション） 検証計画テンプレートで、**[スケジュール]** をクリックして、構成を実行します。
11. （**[検証する項目]** で選択されているバックアップセットが暗号化されている場合）**[バックアップパスワード]** スイッチを有効にして、暗号化パスワードを入力します。
12. （オプション） 計画のオプションを変更するには、ギアアイコンをクリックします。
13. **[作成]** をクリックします。

これにより、検証計画の準備が整い、構成済みのスケジュールに従って実行されます。計画を直ちに実行するには、**[管理]** > **[検証]** で計画を選択し、**[今すぐ実行]** をクリックします。

計画の開始後、Cyber Protectコンソールの **[監視]** > **[アクティビティ]** で、実行中のアクティビティをチェックし、詳細情報を掘り下げて確認できます。

検証計画には複数のバックアップが含まれる場合があり、1つのバックアップを複数の検証計画で検証できます。

注意
すべてのバックアップは、単一の検証タスクによって順番に1つずつ処理されます。

特定のエージェントで一度に実行できる検証タスクは1つだけです。異なるエージェントによって実行される場合、複数の検証タスクを並行して実行できます。2つのタスクを同時に実行するには、2つのエージェントが必要で、3つのタスクの場合は、3つのエージェントが必要（以後同様）です。

次の表は、検証アクティビティで考えられるステータスをまとめたものです。

アクティビティ結果	単一のバックアップを含む計画	複数のバックアップを含む計画
成功	すべての検証メソッドが正常に完了	すべてのバックアップで、すべての検証メソッドが正常に完了
警告を伴い正常に完了	なし	少なくとも1つのバックアップのバックアップメソッドで問題が発生しました
失敗	少なくとも1つのバックアップメソッドで問題が発生しました	すべてのバックアップの少なくとも1つのバックアップメソッドで問題が発生しました

検証メソッド

検証計画では、以下の検証メソッドが利用可能です。

- チェックサムのベリファイ
- 仮想マシンとして実行
  - VMハートビート
  - スクリーンショット検証

チェックサムのベリファイ

チェックサム検証経由の検証では、バックアップからリカバリ可能なすべてのデータブロックについてチェックサムが計算され、バックアップ処理中に書き込まれた該当のデータブロックについて元のチェックサムとの比較が行われます。ただし、クラウドストレージに配置されたファイルレベルのバックアップのベリファイだけは例外となります。これらのバックアップは、バックアップに保存されたメタデータの整合性をチェックすることで検証されます。

チェックサム検証経由の検証プロセスは、サイズの小さい増分バックアップや差分バックアップの場合でも一定の時間がかかります。これは、検証処理において特定のバックアップに物理的に含まれるデータだけでなく、リカバリが必要なすべてのデータ、つまり過去のバックアップについても検証が必要になる場合があるからです。

チェックサム検証による検証が成功すれば、高確率でデータ復元を実行できます。ただしこのメソッドによる検証で、復元プロセスに影響を与えるすべての要素が確認される訳ではありません。

オペレーティングシステムをバックアップする場合は、必要に応じて以下の追加操作の幾つかを実行することをお勧めいたします。

- ブータブルメディア以下にあるテスト復元を予備のハードドライブに移動する。
- ESXiまたはHyper-V環境で、バックアップから仮想マシンを実行する。
- 仮想マシンとして実行の検証メソッドが有効になっている**検証計画を実行する。**

仮想マシンとして実行

この方法は、オペレーティングシステムを含むディスクレベルバックアップにのみ実行できます。これを使用するには、ESXiホストまたはHyper-Vホストと、このホストを管理するプロテクションエージェント（VMwareエージェントまたはHyper-Vエージェント）が必要です。

仮想マシンとして実行検証メソッドには、以下のバリエーションがあります。

- VMハートビート
- スクリーンショット検証

少なくとも1つの項目を選択する必要があります。

VMハートビート

この検証メソッドでは、エージェントがバックアップから仮想マシンを実行し、VMware ToolsまたはHyper-V Integration Serviceに接続し、ハートビート応答をチェックして、オペレーティングシステムが正常に開始されていることが確認されます。接続が失敗した場合、エージェントは 2 分ごとに接続を試みます（合計 5 回）。接続が一度も成功しなかった場合、ベリファイは失敗します。

検証計画と検証対象のバックアップの数に関わらず、検証を実行するエージェントは、一度に1つの仮想マシンを実行します。ベリファイの結果が判明すると、エージェントは仮想マシンを削除して次の仮想マシンを実行します。

注意
このバックアップ検証メソッドは、VMware仮想マシンのバックアップがESXiホスト上の仮想マシンとして実行されており、さらにHyper-V仮想マシンのバックアップがHyper-Vホスト上の仮想マシンとして実行されている場合にのみ使用可能です。

スクリーンショット検証

この検証メソッドでは、エージェントがバックアップから仮想マシンを起動して、仮想マシンが起動している間にスクリーンショットが作成されます。マシンインテリジェンス（MI）モジュールによりスクリーンショットが確認され、そこにログイン画面があれば、バックアップが検証済みとマークされます。

スクリーンショットは復元ポイントに添付され、検証の実行から1年間、Cyber Protectコンソールでダウンロードできます。スクリーンショットの確認方法の詳細については、"バックアップの検証ステータスを確認する"（203ページ）を参照してください。

ユーザーアカウントで通知が有効になっている場合、バックアップの検証ステータスについて、スクリーンショットが添付されたEメールが送信されます。通知の詳細については、「ユーザー向け通知設定の変更」を参照してください。

スクリーンショット検証は、エージェントバージョン15.0.30971（2022年11月リリース）以降でサポートされています。

注意
スクリーンショット検証は、GUIベースのログイン画面が採用されているWindowsおよびLinuxシステムのバックアップでもっとも効果的です。このメソッドは、コンソールのログイン画面が使用されるLinuxシステムには最適化されていません。

VMハートビートとスクリーンショット検証のタイムアウトの変更

バックアップを仮想マシンとして実行し検証する場合、仮想マシンを起動してからハートビート要求を送信するまでのタイムアウト、またはスクリーンショットを取得するまでのタイムアウトを構成できます。

デフォルトの期間は以下の通りです。

- 1分 - ローカルフォルダまたはネットワーク共有に保存されたバックアップの場合
- 5分 - クラウドに保存されたバックアップの場合

VMwareエージェントまたはHyper-Vエージェントの設定ファイルを編集することで変更可能です。

タイムアウトを変更するには

1. 構成ファイルを編集用に開きます。このファイルは以下のロケーションにあります:
   - Windowsで実行されているVMwareエージェントまたはHyper-Vエージェント:`C:\Program Files\BackupClient\BackupAndRecovery\settings.config`
   - VMwareエージェント（仮想アプライアンス）:`/bin/mms_settings.config`
     仮想アプライアンス上の設定ファイルにアクセスする方法の詳細については、"仮想アプライアンスへのSSH接続"（168ページ）を参照してください。
2. `<validation>`に進み、必要に応じてローカルバックアップとクラウドバックアップの値を変更します。

```
<validation>
<run_vm>
<initial_timeout_minutes>
<local_backups>1</local_backups>
<cloud_backups>5</cloud_backups>
</initial_timeout_minutes>
</run_vm>
</validation>
```

3. 構成ファイルを保存します。

4. エージェントを再起動します。
   - （Windowsで実行されているVMwareエージェントまたはHyper-Vエージェントの場合）コマンドプロンプトで次のコマンドを実行します。

     ```
     net stop mms
     ```

     ```
     net start mms
     ```

   - （VMwareエージェント（仮想アプライアンス）の場合）エージェントを含む仮想マシンを再起動します。

エラー発生時の再試行回数を構成する

検証の成功数を最大化するために、エラーで終了した検証処理の自動再試行を構成することができます。

自動再試行を構成するには

1. 検証計画の作成時に、ギアアイコンをクリックします。
2. **[オプション]** ペインで、**[エラーの処理]** を選択します。
3. **[エラーが発生した場合は再試行する]** 以下の **[はい]** をクリックします。
4. **[試行回数]** では、エラーが発生した場合の最大再試行回数を構成します。
   検証処理は、正常に終了するか、再試行回数が上限に達するまで繰り返し実行されます。
5. **[試行間隔]** で、再試行が行われる間隔のタイムアウトを構成します。
6. **[完了]** をクリックします。

バックアップの検証ステータスを確認する

バックアップの検証ステータスは、**[デバイス]** タブまたは **[バックアップストレージ]** タブで確認できます。

また、各検証メソッドのステータスを確認したり、スクリーンショット検証メソッドで取得されたスクリーンショットをダウンロードしたりできます。

ステータスの挙動の詳細については、"検証ステータス"（198ページ）を参照してください。

バックアップの検証ステータスを確認するには

デバイス

1. Cyber Protectコンソールで **[デバイス]** > **[すべてのデバイス]** に進みます。
2. バックアップの検証ステータスを確認するワークロードを選択し、**[復元]** をクリックします。
3. （複数のバックアップ先がある場合）バックアップロケーションを選択します。
4. ステータスを確認するバックアップを選択します。

バックアップストレージ

1. Cyber Protectコンソールで、**[バックアップストレージ]** に移動します。
2. バックアップセットが保管されているロケーションを選択します。

3. バックアップセットを選択してから、**[バックアップを表示]** をクリックします。
4. 検証ステータスを確認したいバックアップを選択します。

クリーンアップ

クリーンアップは、期限切れのバックアップを保持ルールに従って削除する操作です。この処理はエージェントとワークロードにのみ適用され、クラウドツークラウドバックアップには適用されません（手動でのみ削除可能）。

注意
この機能は、Advanced Backupパックの一部として**Advanced Backup - Servers**または**Advanced Backup - NASの**クォータが有効になっているカスタマーテナントで使用できます。

サポートされるロケーション

クリーンアップ計画では、NFSフォルダ、およびSecure Zoneを除くすべてのバックアップロケーションがサポートされます。

クリーンアップ計画を作成するには

1. Cyber Protectコンソールで、**[管理]** > **[クリーンアップ]** をクリックします。
2. **[計画の作成]** をクリックします。
3. **[エージェント]** で、クリーンアップを実行するエージェントを選択します。
   バックアップロケーションにアクセスできる任意のエージェントを選択できます。
4. **[クリーンアップする項目]** で、クリーンアップするアーカイブまたはバックアップロケーションを選択します。
   アーカイブとロケーションを切り替えるには、右上隅の **[ロケーション]** / **[バックアップ]** スイッチを使用します。
   複数の暗号化されたアーカイブを選択した場合、それらの暗号化パスワードは同じでなければなりません。異なる暗号化パスワードを使用しているアーカイブがある場合は、別個の計画を作成します。
5. **[スケジュール]** で、クリーンアップのスケジュールを構成します。
6. **[保持ルール]** で、保持ルールを指定します。
   次から選択できます。
   - **バックアップの数**
   - **バックアップ世代**（月単位、週単位、日単位、時間単位のバックアップ）
   - **バックアップの合計サイズ別**
7. （**[レプリケートする項目]** で暗号化されたアーカイブが選択されている場合）、**[バックアップパスワード]** スイッチを有効にして、暗号化パスワードを入力してください。
8. （オプション） 計画のオプションを変更するには、ギアアイコンをクリックしてから、必要に応じてオプションを構成します。
9. **[作成]** をクリックします。

仮想コンピュータへの変換

仮想マシンへの変換は、ディスクレベルバックアップでのみ可能です。バックアップにシステムボリュームが含まれ、オペレーティングシステムの起動に必要なすべての情報が含まれている場合は、生成される仮想マシンはそれ自体で起動できます。それ以外の場合は、仮想ディスクを別の仮想マシンに追加できます。

注意
ネイティブのScale Computing VMレプリケーション機能でレプリケートされたVMはバックアップできません。

仮想マシンに別個の変換計画を作成し、その計画を手動でまたはスケジュールにより実行することができます。

前提条件と制限については、「"変換に関する注意点"（206ページ）」を参照してください。

注意
この機能は、Advanced Backupパックの一部として**Advanced Backup - Servers**または**Advanced Backup - NASの**クォータが有効になっているカスタマーテナントで使用できます。

仮想マシンへの変換計画の作成

1. **[管理]** > **[VMへの変換]** をクリックします。
2. **[計画の作成]** をクリックします。
   新しい計画テンプレートが表示されます。
3. （オプション） 計画名を変更するには、デフォルト名をクリックします。
4. **[変換先]** で、ターゲット仮想マシンの種類を選択します。**次のいずれかを選択できます**:
   - **VMware ESXi**
   - **Microsoft Hyper-V**
   - **Scale Computing HC3**
   - **VMware Workstation**
   - **VHDXファイル**

     注意
     ストレージスペースを節約するため、毎回のVHDXファイルまたはVMware Workstationへの変換においては、前回の変換時に作成されたターゲットロケーションのVHDX/VMDKファイルが上書きされます。
5. 次のいずれかを実行します。
   - （VMware ESXi、Hyper-V、およびScale Computing HC3の場合）**[ホスト]** をクリックし、ターゲットホストを選択して、新しいマシン名のテンプレートを指定します。
   - （その他の仮想マシンタイプの場合）**[パス]** において、仮想マシンファイルとファイル名テンプレートの保存先を指定します。

   デフォルトの名前は **[マシン名]_converted**です。

6. **[エージェント]** をクリックし、変換を実行するエージェントを選択します。
7. **[変換する項目]** をクリックして、この計画で仮想マシンに変換するバックアップを選択します。
   右上の **[ロケーション]**/**[バックアップ]** スイッチを使用することによって、バックアップの選択とロケーション全体の選択を切り替えることができます。
   選択したバックアップが暗号化されている場合、すべてのバックアップで同じ暗号化パスワードを使用する必要があります。異なる暗号化パスワードを使用しているバックアップがある場合は、別個の計画を作成します。
8. [VMware ESXiとHyper-Vのみ] **[データストア]**（ESXi）または **[パス]**（Hyper-V）をクリックしてから、仮想マシンのデータストア（ストレージ）を選択します。
9. （VMware ESXiおよびHyper-Vのみ）ディスクプロビジョニングモードを選択します。デフォルトの設定は、VMware ESXiの場合は **[シン]**、Hyper-Vの場合は **[容量可変]** です。
10. （オプション）（VMware ESXi、Hyper-V、およびScale Computing HC3の場合）**[VM設定]** をクリックして仮想マシンのメモリサイズ、プロセッサー数、またはネットワーク接続数を変更します。
11. （オプション）**[スケジュール]** をクリックし、スケジュールを変更します。
12. **[変換する項目]** で選択されているバックアップが暗号化されている場合は、**[バックアップパスワード]** スイッチを有効にして、暗号化パスワードを入力してください。それ以外の場合は、この手順をスキップします。
13. （オプション）計画のオプションを変更するには、ギアアイコンをクリックします。
14. **[作成]** をクリックします。

変換に関する注意点

サポートされている仮想マシンの種類

バックアップの仮想マシンへの変換は、バックアップを作成した同じエージェント、または別のエージェントによって行われます。

VMware ESXi、Hyper-V、またはScale Computing HC3への変換を実行するには、それぞれESXi、Hyper-V、またはScale Computing HC3ホストと、このホストを管理するプロテクションエージェント（VMwareエージェント、Hyper-Vエージェント、またはScale Computing HC3エージェント）が必要になります。

VHDXファイルへの変換は、ファイルがHyper-V仮想マシンへ仮想ディスクとして接続されるものとみなします。

次の表は、**VMへの変換**操作で作成できる仮想マシンのタイプをまとめたものです。表の行は、変換された仮想マシンのタイプを示しています。列には、変換を実行するエージェントが表示されます。

VM の種類	エージェント for VMware	Hyper-V エージェント	Windows エージェント	Linux エージェント	エージェント for	Scale Computing HC3 エージェント	oVirt（KVM）エージェント	Virtuozzo Hybrid Infrastructureエージェント	Virtuozzo エージェント

					Mac				
VMware ESXi	+	–	–	–	–	–	–	–	–
Microsoft Hyper-V	–	+	–	–	–	–	–	–	–
VMware Workstation	+	+	+	+	–	–	–	–	–
VHDX ファイル	+	+	+	+	–	–	–	–	–
Scale Computing HC3	–	–	–	–	–	+	–	–	–

制限事項

- NFSに保存されているバックアップは変換できません。
- Secure Zoneに保存されているバックアップは、同じマシン上で実行中のエージェントによってのみ変換できます。
- Linux論理ボリューム（LVM）を含むバックアップは、VMwareエージェント、Hyper-VエージェントまたはScale Computing HC3エージェントによって作成され、同じハイパーバイザーを対象としている場合にのみ変換できます。クロスハイパーバイザー変換はサポートされていません。
- WindowsマシンのバックアップをVMware WorkstationまたはVHDXファイルへ変換する際、作成される仮想マシンは、変換を実行するマシンからCPUの種類を継承します。その結果、対応するCPUドライバがゲストオペレーティングシステムにインストールされます。CPUの種類が異なるホストを起動すると、ゲストシステムにドライバエラーが表示されます。このドライバを手動でアップデートします。

定期的に実行される仮想マシンへの変換とバックアップからの仮想マシンの実行

どちらの操作でも、元のマシンに障害が発生した場合に数秒で起動できる仮想マシンを使用できます。

定期的に実行される仮想マシンへの変換は、CPUとメモリリソースを消費します。仮想マシンのファイルは、データストア（ストレージ）の領域を常時使用します。これは、変換に本番ホストを使用する場合は、実用的ではないことがあります。ただし、仮想マシンのパフォーマンスは、ホストのリソースによってのみ制限されます。

バックアップから仮想マシンを実行する場合、仮想マシンの実行中にのみリソースが消費されます。データストア（ストレージ）の領域は、仮想ディスクに変更を保持する目的でのみ必要です。ただし、

ホストは仮想ディスクに直接アクセスせず、バックアップからデータを読み取るエージェントと通信するため、仮想マシンの実行速度が遅くなる可能性があります。また、仮想マシンは一時的なものです。

仮想マシンに対し定期的に実行される変換の動作

定期的に実行される変換の動作は、仮想マシンの作成場所によって異なります。

- **仮想マシンを一連のファイルとして保存する場合:** 変換が行われるたびに、仮想マシンが新しく再作成されます。
- **仮想化サーバー上に仮想マシンを作成する場合:** 増分または差分バックアップが変換されると、新しい仮想マシンが再作成される代わりに、既存の仮想マシンが増分的にアップデートされます。通常、こちらの変換の方が高速です。ネットワーク トラフィックと、変換を実行するホストの CPU リソースが節約されます。仮想コンピュータのアップデートができない場合は、仮想コンピュータが新しく再作成されます。

次に、両方の動作について詳しく説明します。

仮想コンピュータを一連のファイルとして保存する場合

最初の変換の結果、新しい仮想マシンが作成されます。その後に変換するごとに、このコンピュータが最初から作成されます。最初に、古いコンピュータの名前が一時的に変更されます。次に、新しい仮想コンピュータが、古いコンピュータの変更前の名前で作成されます。この処理が成功すると、古いコンピュータが削除されます。この処理が失敗すると、新しいコンピュータは削除され、古いコンピュータの名前が変更前に戻されます。このように、変換処理は常に 1 台のコンピュータで実行されますが、変換中は、古いコンピュータを保持するための追加のストレージ領域が必要になります。

仮想サーバー上に仮想コンピュータを作成する場合

最初の変換では、新しい仮想マシンが作成されます。その後の変換の動作は次のとおりです。

- 本セクションで既に説明したとおり、最後の変換以降の完全バックアップが存在する場合、仮想マシンが新しく再作成されます。
- 完全バックアップが存在しない場合、既存の仮想マシンが、最後の変換以降に行われた変更内容を反映するようにアップデートされます。アップデートができない場合（中間スナップショットを削除した場合など。以下を参照してください）、仮想コンピュータが新しく再作成されます。

中間スナップショット

変換された仮想マシンを安全にアップデートできるようにするために、ソフトウェアはこのマシンの中間ハイパーバイザースナップショットを保存します。スナップショットの名前は「**Replica...**」であり、この名前を保持する必要があります。

「**Replica…**」スナップショットは、最新の変換結果に対応しています。マシンの状態を元に戻したい場合、このスナップショットにアクセスします。たとえば、マシンの使用中に、そのマシンに対して行った変更内容を取り消したい場合などです。

変換されたScale Computing HC3仮想マシンの場合、追加の**ユーティリティスナップショット**が作成されます。Cyber Protectionサービスのみで使用されます。

保護計画とモジュール

データを保護するため、保護計画を作成し、それをワークロードに適用する必要があります。

保護計画は、さまざまな保護モジュールで構成されています。必要なモジュールを有効化し、その設定を構成して、特定のニーズに合った保護計画を作成できます。

次のモジュールを使用できます。

- バックアップ:データソースをローカルまたはクラウドストレージにバックアップできます。
- "ディザスタリカバリを実装する"（714ページ）:クラウドサイトにマシンの正確なコピーを作成し、破損した元のマシンからクラウド内の復元サーバーにワークロードを切り替えられます。
- ウイルスおよびマルウェア対策保護:内蔵のマルウェア対策ソリューションにより、ワークロードを確認します。
- エンドポイント検知と応答（EDR）。気づかれなかった攻撃など、ワークロード上の不審なアクティビティを検知し、インシデントを生成します。これにより、攻撃がどのように発生したか、どのように再発を防止するかについての情報を得られます。
- URLフィルタリング: 悪意あるURLへのアクセスやダウンロードコンテンツをブロックすることで、インターネット経由の脅威からマシンを保護できます。
- Windows Defender Antivirus:Windows Defender Antivirusの設定を管理して環境を保護します。
- Microsoft Security Essentials:Microsoft Security Essentialsの設定を管理して環境を保護します。
- 脆弱性診断:マシンにインストールされたWindows、Linux、macOSの各製品、またMicrosoftおよびmacOSのサードパーティ製品の脆弱性を自動的にチェックし、使用者に知らせます。
- パッチ管理:マシン上のWindows、Linux、macOSの各製品、またMicrosoftおよびmacOSのサードパーティ製品に対するパッチとアップデートをインストールして、検出された脆弱性を解決します。
- データ保護マップ:データを検出して重要なファイルの保護ステータスをモニタリングできます。
- デバイス制御ユーザーが現在のマシンでの使用を許可または禁止するデバイスを指定できます。
- Advanced Data Loss Prevention:データフローポリシーに基づき、周辺デバイス（プリンタやリムーバブルストレージなど）からの機密データの漏洩、ならびに内部および外部ネットワーク転送を介した機密データの漏洩を防止できます。

保護計画の作成

以下の方法で保護計画を作成できます。

- **[デバイス]** タブでの操作。1つまたは複数の保護対象のワークロードを選択し、保護計画を作成します。
- **[管理]** > **[保護計画]** タブでの操作。 保護計画を作成し、計画を適用する1つまたは複数のワークロードを選択します。

保護計画を作成すると、ワークロードの種類に応じて適用可能なモジュールのみが表示されます。

複数のワークロードに保護計画を適用できます。また、同じワークロードに複数の保護計画を適用することもできます。競発生し得る競合については、「"計画の競合の解決"（215ページ）」を参照してください。

保護計画を作成するには

デバイス

1. Cyber Protectコンソールで **[デバイス]** > **[すべてのデバイス]** に進みます。
2. 保護するワークロードを選択して、**[保護]** をクリックします。
3. （すでに適用済みの計画の場合）**[計画を追加]** をクリックします。
4. **[計画の作成]** > **[保護]** をクリックします。
   保護計画パネルが開きます。
5. （オプション） 保護計画の名前を変更するには、鉛筆のアイコンをクリックし、新しい名前を入力します。
6. （オプション） 計画のモジュールを有効化または無効化するには、モジュール名の横にあるスイッチを切り替えます。
7. （オプション） モジュールを構成するには、モジュールをクリックして展開し、必要な構成を変更します。
8. 準備ができたら、**[作成]** をクリックします。

注意
暗号化を使用して保護計画を作成するには、暗号化パスワードを指定します。詳細については、「"暗号化"（430ページ）」を参照してください。

[管理] > **[保護計画]**

1. Cyber Protectコンソールで、**[管理]** > **[保護計画]** に移動します。
2. **[計画の作成]** をクリックします。
   保護計画のテンプレートが開きます。
3. （オプション）保護計画の名前を変更するには、鉛筆のアイコンをクリックし、新しい名前を入力します。
4. （オプション）計画のモジュールを有効化または無効化するには、モジュール名の横にあるスイッチを切り替えます。
5. （オプション）モジュールを構成するには、モジュールをクリックして展開し、必要な構成を変更します。
6. （オプション） 計画を適用するワークロードを選択するには、**[デバイスの追加]** をクリックします。

注意
どのワークロードにも適用せずに、計画を作成することができます。計画を編集することで、後でワークロードを追加できます。ワークロードを計画に追加する方法については、"ワークロードへの保護計画の適用"（212ページ）を参照してください。

7. 準備ができたら、**[作成]** をクリックします。

注意
暗号化を使用して保護計画を作成するには、暗号化パスワードを指定します。詳細については、「"暗号化"（430ページ）」を参照してください。

モジュールをオンデマンドで実行（**バックアップ**、**ウイルス対策およびマルウェア対策保護**、**脆弱性診断**、**パッチ管理**、**データ保護マップ**など）するには、**[今すぐ実行]** をクリックします。

ハウツービデオ「最初の保護計画を作成する」をご覧ください。

ディザスタリカバリモジュールの詳細については、「"ディザスタリカバリ保護計画の作成"（720ページ）」を参照してください。

デバイス制御モジュールの詳細については、「"デバイス制御モジュールを動作させる"（353ページ）」を参照してください。

保護計画を使用した操作

保護計画を作成した後、その保護計画で以下のアクションを実行できます。

- ワークロードまたはデバイスグループに計画を適用する。
- 計画名を変更します。
- 計画を編集する。
  計画に含まれるモジュールの有効化/無効化、および設定の変更が可能です。
- 計画を有効または無効にします。
  無効化された計画は、該当の計画が適用されているワークロードでは実行されません。
  このアクションは、後から同じワークロードを同じ計画で保護する予定の管理者にとって利便性があります。計画がワークロードから取り消されることはなく、計画を再度有効化することですぐに保護を復元できます。
- ワークロードで計画を取り消します。
  取り消された計画は、ワークロードに適用されなくなります。
  この操作は、同じ計画を再利用して同じワークロードを保護する必要のない管理者にとって利便性があります。取り消された計画で提供される保護を復元するには、その計画の名前を知っている必要があります。利用可能な計画のリストから該当の計画を選択して、各ワークロードに計画を再度適用します。
- 計画を停止します。
  この操作により、計画が適用されるすべてのワークロードで実行中のすべてのバックアップ操作が停止されます。計画のスケジュールに従って、バックアップが再開されます。
  マルウェア対策スキャンはこの操作の影響を受けず、スケジュール構成に従って実行されます。
- 計画のクローンを作成します。
  既存の計画の完全なコピーを作成できます。新しい計画は、どのワークロードにも割り当てられません。
- 計画をエクスポートおよびインポートします。

計画をJSONファイルとしてエクスポートし、後でインポートし直すことができます。これにより、手動で新しい計画を作成し、構成を実行する手間を省くことができます。

注意
インポートできるのは、Cyber Protection 9.0（2020年3月リリース）で作成した保護計画だけです。以前のバージョンで作成した計画には、Cyber Protection 9.0以降との互換性がありません。

- 計画の詳細を確認します。
- 計画に関連するアクティビティやアラートを確認できます。
- 計画を削除します。

ワークロードへの保護計画の適用

ワークロードを保護するには、対象のワークロードに保護計画を適用する必要があります。

[デバイス] タブと **[管理]** > **[保護計画]** タブで計画を適用できます。

デバイス

1. 保護対象である、1つまたは複数のワークロードを選択します。
2. **[保護]** をクリックします。
3. （選択したマシンに保護計画が既にに適用されている場合）**[計画の追加]** をクリックします。
4. 使用可能な保護計画の一覧が表示されます。
5. 適用する保護計画を選択して、**[適用]** をクリックします。

[管理] > **[保護計画]**

1. Cyber Protectコンソールで、**[管理]** > **[保護計画]** に移動します。
2. 適用する保護計画を選択します。
3. **[編集]** をクリックします。
4. ［**デバイスの管理**］をクリックします。
5. **[デバイス]** ウィンドウで **[追加]** をクリックします。
6. 計画を適用するワークロードを選択して、**[追加]** をクリックします。
7. **[デバイス]** ウィンドウで **[完了]** をクリックします。
8. 保護計画パネルで、**[保存]** をクリックします。

保護計画をデバイスグループに適用する方法については、「"グループに計画を適用する"（352ページ）」を参照してください。

保護計画の編集

計画の編集時には、計画に含まれるモジュールの有効化/無効化、および設定の変更が可能です。

保護計画の編集は、適用されるすべてのワークロードに対して、または選択されたワークロードに限定して実行できます。

[デバイス] タブと **[管理]** > **[保護計画]** タブで計画を編集できます。

デバイス

1. 計画を適用する1つまたは複数のワークロードを選択します。
2. **[保護]** をクリックします。
3. 編集する保護計画を選択します。
4. 計画名の横にある省略記号のアイコン（...）をクリックして、**[編集]** をクリックします。
5. 編集したいモジュールをクリックし、必要に応じて構成します。
6. **[保存]** をクリックします。
7. （計画を適用先としてすべてのワークロードを選択していない場合）編集スコープを選択します。
   - 適用先におけるすべてのワークロードの計画を編集する場合は、**[変更をこの保護計画に適用（他のデバイスに影響します）]** をクリックします。
   - 選択したワークロードについてのみ計画を変更する場合は、**[選択したデバイスの新しい保護計画だけを作成]** をクリックします。
     この場合、選択したワークロードから既存の計画が取り消されます。構成済みの設定で新しい保護計画が作成され、これらのワークロードに適用されます。

[管理] > [保護計画]

1. Cyber Protectコンソールで、**[管理]** > **[保護計画]** に移動します。
2. 編集する保護計画を選択します。
3. **[編集]** をクリックします。
4. 編集したいモジュールをクリックし、必要に応じて設定を構成します。
5. **[保存]** をクリックします。

注意
[管理] > **[保護計画]** タブから計画を編集すると、計画が適用されているすべてのワークロードに影響します。

保護計画の取り消し

計画を取り消すと、1つまたは複数のワークロードから計画が削除されます。この計画が適用された他のワークロードは引き続き保護対象となります。

[デバイス] タブおよび **[管理]** > **[保護計画]** タブで計画を取り消せます。

デバイス

1. 計画を取り消すワークロードを選択します。
2. **[保護]** をクリックします。
3. 取り消す保護計画を選択します。
4. 計画名の横にある省略記号のアイコン（...）をクリックして、**[取り消し]** をクリックします。

[管理] > [保護計画]

1. Cyber Protectコンソールで、**[管理]** > **[保護計画]** に移動します。
2. 取り消す保護計画を選択します。
3. **[編集]** をクリックします。
4. ［**デバイスの管理**］をクリックします。

5. **[デバイス]** ウィンドウで、計画を取り消すワークロードを選択します。
6. **[削除]** をクリックします。
7. **[デバイス]** ウィンドウで **[完了]** をクリックします。
8. 保護計画テンプレートで、**[保存]** をクリックします。

保護計画の有効化と無効化

有効化された計画はアクティブになり、適用されたワークロード上で実行されます。無効化された計画は非アクティブになります。ワークロードには引き続き適用されますが、ワークロード上で実行されることはありません。

[デバイス] タブから保護計画を有効または無効にすると、選択したワークロードにのみ影響します。

[管理] > **[保護計画]** タブから保護計画を有効化または無効化すると、計画が適用されているすべてのワークロードに影響します。複数の保護計画を有効化または無効化することもできます。

デバイス

1. 計画を無効にするワークロードを選択します。
2. **[保護]** をクリックします。
3. 無効化する保護計画を選択します。
4. 計画名の横にある省略記号のアイコン（...）をクリックして、それぞれ **[有効化]** または **[無効化]** をクリックします。

[管理] > **[保護計画]**

1. Cyber Protectコンソールで、**[管理]** > **[保護計画]** に移動します。
2. 有効/無効にする1つまたは複数の保護計画を選択します。
3. **[編集]** をクリックします。
4. それぞれ、**[有効化]** または **[無効化]** をクリックします。

注意
この操作は、既に希望する変更状態になっている保護計画には影響しません。たとえば、選択した計画に有効なものと無効なものがある場合、**[有効化]** をクリックすると、選択したすべての計画が有効になります。

保護計画の削除

計画を削除すると、その計画はすべてのワークロードから取り消され、Cyber Protectコンソールから削除されます。

[デバイス] タブと **[管理]** > **[保護計画]** タブから計画を削除できます。

デバイス

1. 削除する保護計画が適用されたいずれかのワークロードを選択します。
2. **[保護]** をクリックします。

3. 削除する保護計画を選択します。
4. 計画名の横にある省略記号のアイコン（...）をクリックして、**[削除]** をクリックします。

[管理] > **[保護計画]**

1. Cyber Protectコンソールで、**[管理]** > **[保護計画]** に移動します。
2. 削除する保護計画を選択します。
3. **[削除]** をクリックします。
4. **[計画の削除を確定します]** チェックボックスを選択して内容を確認し、**[削除]** をクリックします。

計画の競合の解決

同じワークロードに複数の保護計画を適用することが可能です。たとえば、**ウイルスおよびマルウェア対策**モジュールのみを有効化して構成した保護計画と、**バックアップ**モジュールのみを有効化して構成した別の保護計画を適用することができます。

異なるモジュールを有効化した保護計画を組み合わせることができます。また、**バックアップ**モジュールのみが有効な複数の保護計画を組み合わせることも可能です。ただし、他のモジュールが複数の計画で有効になっている場合は、競合が発生します。計画を適用するには、まず、競合を解決する必要があります。

新しい計画と既存の計画の競合

新しい計画が既存の計画と競合する場合、以下のいずれかの方法で解決できます。

- 新しい計画を作成および適用し、競合する既存の計画を無効化します。
- 新しい計画を作成し、無効化します。

個別計画とグループ計画の競合

個別の保護計画が、デバイスグループに適用されているグループ計画と競合する場合、次のいずれかの方法で解決できます。

- デバイスグループからワークロードを削除し、個別の保護計画を適用します。
- 既存のグループ計画を編集するか、新しいグループ計画をデバイスグループに適用します。

ライセンスの問題

場合により保護計画モジュールで、保護対象のワークロードに特定のサービスクォータを割り当てる必要があります。割り当てられたサービスクォータが適切でない場合、それぞれのモジュールが有効になっている保護計画を実行、アップデート、または適用することはできません。

ライセンスの問題を解決するには、以下のいずれかを実行します。

- 現在割り当てられているサービスクォータでサポートされていないモジュールを無効化し、保護計画の使用を継続します。
- 割り当てられたサービスクォータを手動で変更します。この方法については、「"マシンのサービスクォータの変更"（180ページ）」を参照してください。

既定の保護計画

既定の保護計画は、事前構成されたテンプレートであり、ワークロードに適用することで、迅速な保護を実現することができます。既定の保護計画を使用すれば、一から新しい保護計画を作成する必要がなくなります。

既定の保護計画を初めて適用すると、テンプレートがテナントにコピーされ、計画内のモジュールと設定を編集できるようになります。

以下の既定の計画が用意されています:

- Cyber ProtectEssentials
  基本的な保護機能とファイルレベルのバックアップを提供する計画です。
- リモートワーカー
  リモートワークのユーザー向けに最適化された計画です。より頻繁に発生するタスク（バックアップ、マルウェア対策保護、脆弱性診断など）、より厳密な保護操作、最適化されたパフォーマンスと電源オプションを提供します。
- オフィスワーカー（サードパーティのウイルス対策）
  この計画は、オフィスで業務を行い、サードパーティのウイルス対策ソフトウェアを利用することが多いユーザー向けに最適化されています。この計画では、**ウイルスおよびマルウェア対策保護**モジュールが無効にされます。
- オフィスワーカー（Acronisウイルス対策）
  この計画は、オフィスで業務を行い、Acronisのウイルス対策ソフトウェアを利用することが多いユーザー向けに最適化されています。

既定の保護計画の比較

モジュールとオプション	**既定の保護計画**			
	Cyber ProtectEssentials	**リモートワーカー**	**オフィスワーカー（サードパーティのウイルス対策）**	**オフィスワーカー（Acronisウイルス対策）**
バックアップ	使用可能	使用可能	使用可能	使用可能
バックアップの対象 バックアップする項目	ファイル/フォルダ [すべてのプロファイル フォルダ]	コンピュータ全体	コンピュータ全体	コンピュータ全体
継続的データ保護（CDP）	無効	有効	無効	無効
バックアップ先	クラウドストレージ	クラウドストレージ	クラウドストレージ	クラウドストレージ
スケジュール	月曜日から金曜日の	月曜日から金曜日の	月曜日から金曜日の	月曜日から金曜日の

モジュールとオプション	既定の保護計画			
	Cyber ProtectEssentials	リモートワーカー	オフィスワーカー（サードパーティのウイルス対策）	オフィスワーカー（Acronisウイルス対策）
	午後11:00	午前12:00 追加で有効にされたオプションと開始条件: • マシンの電源が入っていないため実行されなかったタスクを起動時に実行する • スリープモードや休止モードから起動して、スケジュールされたバックアップを開始する • バッテリー電源を節約:バッテリー駆動時は開始しない • 従量制課金の接続時には開始しない	午後11:00	午後11:00
バックアップスキーム	常に増分	常に増分	常に増分	常に増分
保持する期間	期間を制限せずにバックアップを保持する	月単位:12か月 週単位:4週間 日単位:7日	月単位:12か月 週単位:4週間 日単位:7日	月単位:12か月 週単位:4週間 日単位:7日
バックアップオプション	バックアップオプション	既定のオプション（次の点が付加）: • パフォーマンスとバックアップウィンドウ（緑のセット）: CPUの優先度:低 出力速度:50%	バックアップオプション	バックアップオプション
ウイルスおよびマルウェア	使用可能	使用可能	使用できません	使用可能

モジュールとオプション	既定の保護計画			
	Cyber ProtectEssentials	リモートワーカー	オフィスワーカー（サードパーティのウイルス対策）	オフィスワーカー（Acronisウイルス対策）
対策保護				
Active Protection	オフ	オフ	–	オフ
高度なマルウェア対策機能	曜日	曜日	–	曜日
ネットワークフォルダの保護	曜日	曜日	–	曜日
サーバー側保護機能	オフ	オフ	–	オフ
自己保護	曜日	曜日	–	曜日
クリプトマイニングプロセス検出	曜日	曜日	–	曜日
検疫	検疫されたファイルを30日後に削除	検疫されたファイルを30日後に削除	–	検疫されたファイルを30日後に削除
振る舞い検知エンジン	検疫	検疫	–	検疫
エクスプロイト防御	プロセスの通知と停止	プロセスの通知と停止	–	プロセスの通知と停止
リアルタイム保護	検疫	検疫	–	検疫
スケジュールスキャン	クイックスキャン:検疫 日曜日から土曜日の午後02:20 完全スキャン: オフ	クイックスキャン:オフ 完全スキャン:検疫 日曜日から土曜日の午後01:55 追加で有効にされたオプションと開始条件: • マシンの電源が	–	クイックスキャン:検疫 日曜日から土曜日の午後02:20 完全スキャン:オフ

モジュールとオプション	既定の保護計画			
	Cyber ProtectEssentials	リモートワーカー	オフィスワーカー（サードパーティのウイルス対策）	オフィスワーカー（Acronisウイルス対策）
		入っていないため実行されなかったタスクを起動時に実行する • スリープモードや休止モードから起動して、スケジュールされたバックアップを開始する • バッテリー電源を節約:バッテリー駆動時は開始しない		
除外	なし	なし	–	なし
URLフィルタ処理	使用可能	使用可能	使用可能	使用可能
悪意あるWebサイトへのアクセス	常にユーザーに確認	ブロック	常にユーザーに確認	常にユーザーに確認
フィルタリングするカテゴリ	バックアップオプション	バックアップオプション	バックアップオプション	バックアップオプション
除外	なし	なし	なし	なし
脆弱性診断	使用可能	使用可能	使用可能	使用可能
脆弱性診断スコープ	Microsoft製品、Windowsサードパーティ製品	Microsoft製品、Windowsサードパーティ製品	Microsoft製品、Windowsサードパーティ製品	Microsoft製品、Windowsサードパーティ製品
スケジュール	午後01:15（月曜日のみ）	午後02:20（月曜日のみ）	午後01:15（月曜日のみ）	午後01:15（月曜日のみ）
パッチ管理	使用可能	使用可能	使用可能	使用可能
Microsoft製品	すべてのアップデート	すべてのアップデート	すべてのアップデート	すべてのアップデート
Windowsサー	メジャーアップデー	メジャーアップデー	メジャーアップデー	メジャーアップデー

モジュールとオプション	既定の保護計画			
	Cyber ProtectEssentials	リモートワーカー	オフィスワーカー（サードパーティのウイルス対策）	オフィスワーカー（Acronisウイルス対策）
ドパーティ製品	トのみ	トのみ	トのみ	トのみ
スケジュール	午後03:10（月曜日のみ）	月曜日から金曜日の午後02:20	午後03:10（月曜日のみ）	午後03:10（月曜日のみ）
アップデート前のバックアップ	オフ	曜日	オフ	オフ
データ保護マップ	使用できません	使用可能	使用可能	使用可能
拡張子と例外ルール	–	デフォルトのオプションと、以下の追加拡張子: **イメージ** • .jpeg • .jpg • .png • .gif • .bmp • .ico • .wbmp • .xcf • .psd • .tiff • .dwg **音声と動画** • .avi、 • .mov、 • .mpeg、 • .mpg、 • .mkv • .wav • .aif • .aifc • .aiff • .au	デフォルトのオプション（66種類の拡張子を検出）	デフォルトのオプション（66種類の拡張子を検出）

モジュールとオプション	既定の保護計画			
	Cyber ProtectEssentials	リモートワーカー	オフィスワーカー（サードパーティのウイルス対策）	オフィスワーカー（Acronisウイルス対策）
		• .snd • .mid • .midi • .mpga • .mp3 • .oga • .flac • .opus • .spx • .ogg • .ogx • .mp4		
スケジュール	–	月曜日から金曜日の午後03:35	月曜日から金曜日の午後03:40	月曜日から金曜日の午後03:40

注意
デフォルトの保護計画のモジュール数は、ご利用のCyber Protectionライセンスによって異なる場合があります。

既定の保護計画を適用する

既定の保護計画は、設定のテンプレートであり、編集できません。既定の計画を初めて適用すると、テンプレートが構成済みの保護計画としてテナントにコピーされ、選択したワークロードで有効になります。

保護計画の管理は、**[管理]** > **[保護計画]** タブで保護計画を表示してから実行します。

既定の保護計画を初めて適用するには

1. Cyber Protectコンソールで **[デバイス]** > **[すべてのデバイス]** に進みます。
2. 保護するワークロードを選択します。
3. **[保護]** をクリックします。
4. いずれかのデフォルト計画を選択して、**[適用]** をクリックします。

既定の保護計画を編集する

既定の保護計画は、初回の適用後に編集できます。

適用された既定の保護計画を編集するには

1. Cyber Protectコンソールで、**[管理]** > **[保護計画]** に移動します。
2. 編集する計画を選択し、**[編集]** をクリックします。
3. この計画に含まれるモジュールまたはオプションを変更し、**[保存]** をクリックします。

重要
一部変更できないオプションがあります。

ホスティングコントロールパネル統合に関する個別保護計画

DirectAdmin、cPanel、Pleskを使用するWebホスティングサーバーでホスティングコントロールパネルの統合を有効化すると、Cyber Protectionサービスの自動処理により、各ワークロードのユーザーアカウント以下に個別の保護計画が作成されます。この保護計画は、保護計画の作成を開始した特定のワークロードと関連付けられます。取り消したり、他のワークロードに割り当てたりすることはできません。

個別の保護計画の利用を停止するには、Cyber Protectコンソールから削除します。個別の保護計画は、名前の横にある の記号で識別できます。

ホスティングコントロールパネル統合を使用する複数のWebホスティングサーバーを保護する保護計画が必要な場合、Cyber Protectコンソールで通常の保護計画を作成し、これらのワークロードを割り当てることができます。ただし、複数のWebホスティングコントロールパネルで共有されている保護計画の修正は、必ずCyber Protectコンソールから実行します。統合機能の内部から実行することはできません。

マシンの#CyberFitスコア

#CyberFitスコアは、セキュリティ評価とスコアリングメカニズムにより、マシンのセキュリティ状態を評価します。#CyberFitスコアでは、IT環境にあるセキュリティギャップとエンドポイントへのオープン型攻撃ベクトルを特定し、改善を図るために推奨されるアクションをレポート形式で提供します。この機能は、すべてのCyber Protectエディションでご利用いただけます。

#CyberFitスコア機能は次のシステムでサポートされています。

- Windows 7（最初のバージョン）以降
- Windows Server 2008 R2以降

仕組み

マシンにインストールされている保護エージェントでセキュリティ評価を行い、マシンの#CyberFitスコアを計算します。マシンの#CyberFitスコアは定期的に自動で再計算されます。

#CyberFitスコアリングのメカニズム

次のメトリクスに基づいて、マシンの#CyberFitスコアが計算されます。

- マルウェア対策保護0-275
- バックアップ保護0-175

- ファイアウォール0-175
- 仮想プライベートネットワーク（VPN）0-75
- フルディスクの暗号化0-125
- ネットワークセキュリティ0-25

マシンの#CyberFitスコア最高値は850です。

メトリクス	評価対象	ユーザーへの推奨事項	スコアリング
マルウェア対策	エージェントは、マルウェア対策ソフトウェアがマシンにインストールされているかどうかを確認します。	検査結果 • マルウェア対策保護が有効です（+275ポイント） • マルウェア対策保護が導入されていません。システムが危険にさらされている可能性があります（0ポイント） #CyberFitスコアによる推奨事項 セキュリティリスクから継続的に保護するために、ご使用のマシンにマルウェア対策ソリューションをインストールして有効にしてください。 推奨されるマルウェア対策ソリューションの一覧については、AV-TestまたはAV-ComparativesなどのWebサイトを参照してください。	275 - マルウェア対策ソフトウェアがマシンにインストールされています 0 - マルウェア対策ソフトウェアがマシンにインストールされていません
バックアップ	エージェントにより、バックアップソリューションがマシンにインストールされているかどうかが確認されます。	検査結果 • データはバックアップソリューションによって保護されています（+175ポイント） • バックアップソリューションが見つかりませんでした。データが危険にさらされている可能性があります（0ポイント） #CyberFitスコアによる推奨事項 データ損失やランサムウェア攻撃を防止するために、定期的にデータをバックアップすることをお勧めします。次のようなバックアップソリューションを使用することを検討してください。 • Acronis Cyber Protect / Cyber Backup / True Image • Windows Serverバックアップ（Windows Server 2008 R2以降）	175 - バックアップソリューションがマシンにインストールされています 0 - バックアップソリューションがマシンにインストールされていません
ファイアウォール	ご利用の環境でファイアウォールが利用可能で有効	検査結果	100 - Windows パブリックファ

	化されているかをエージェントが確認します。 エージェントで、以下の操作を実施します。 1.パブリックファイアウォールがオンになっているか、Windowsファイアウォールとネットワーク保護機能をチェックします。 2.プライベートファイアウォールがオンになっているか、Windowsファイアウォールとネットワーク保護機能をチェックします。 3.Windowsのパブリックファイアウォールとプライベートファイアウォールが無効になっている場合に、サードパーティ製ファイアウォールソリューション/エージェントをチェックします。	• パブリックおよびプライベートネットワークのファイアウォールが有効、またはサードパーティ製のファイアウォールソリューションが見つかりました（+175ポイント） • パブリックネットワークのファイアウォールのみが有効です（+100ポイント） • プライベートネットワークのファイアウォールのみが有効です（+75ポイント） • ファイアウォールが有効ではありません。ネットワーク接続は安全ではありません（0ポイント） #CyberFitスコアによる推奨事項 パブリックおよびプライベートネットワークでファイアウォールを有効にし、システムへの悪意のある攻撃に対するセキュリティ保護を強化することをお勧めします。次に、セキュリティのニーズとネットワークアーキテクチャに従って、Windowsファイアウォールを設定するための詳細なガイドを示します。 エンドユーザー/従業員向けのガイド: PCでWindows Defenderファイアウォールを設定する方法 PCでWindowsファイアウォールを設定する方法 システム管理者およびエンジニア向けガイド: Advanced SecurityでWindow Defender Firewallをデプロイする方法 Windowsファイアウォールでの詳細ルール作成方法	イアウォールが有効です 75 - Windowsプライベートファイアウォールが有効です 175 - Windowsパブリックおよびプライベートファイアウォールが有効であるか、 サードパーティ製のファイアウォールソリューションが有効です 0 - Windowsファイアウォール、サードパーティ製ファイアウォールソリューションのいずれも有効化されていません
仮想プライベートネットワーク（VPN）	エージェントは、VPNソリューションがマシンにインストールされているかどうか、またVPNが有効化されて実行されているかどうか確認します。	検査結果 • VPNソリューションが導入されているため、パブリックおよび共有ネットワークで安全にデータを送受信できます（+75ポイント） • VPNソリューションが見つかりませんでした。パブリックおよび共有ネットワークへの接続が安全ではありません（0ポイント） #CyberFitスコアによる推奨事項 企業ネットワークと機密データにアクセスする際にはVPNを使用することをお勧めします。特に、カフェ、図書館、空港などの場所で無料のインターネットアクセスを使用する場合には、	75 - VPNが有効で実行されています 0 - VPNが有効ではありません

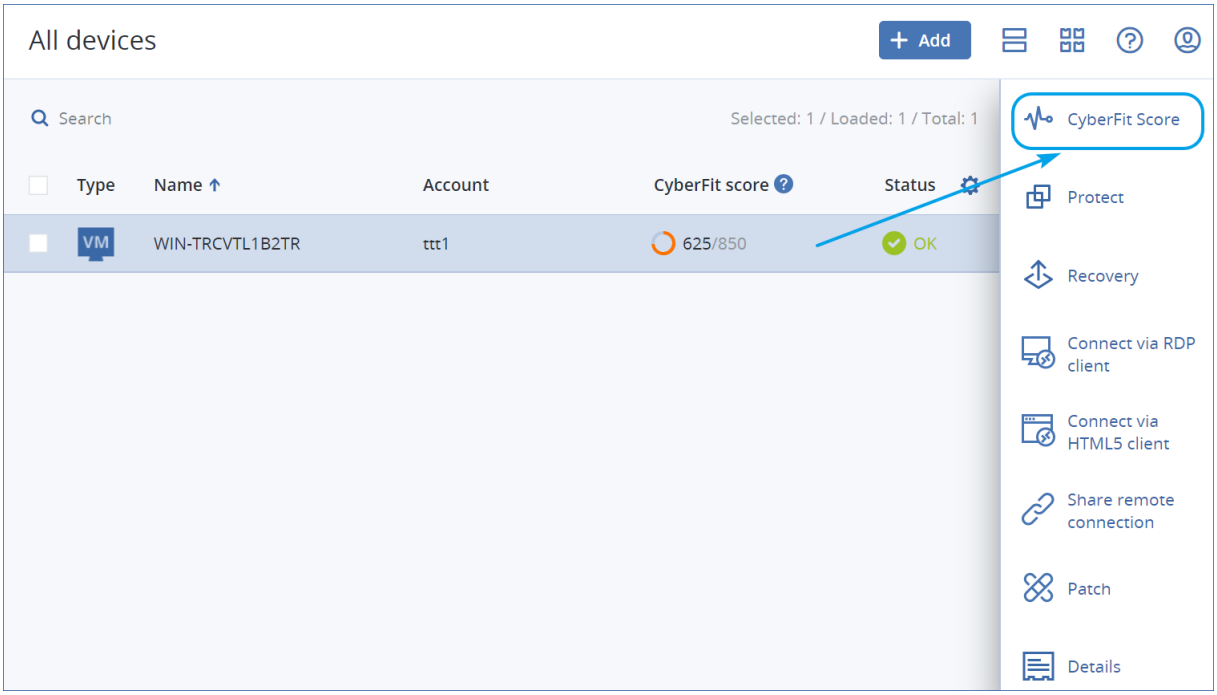
		通信を安全にプライベートに保つためにVPNを使用することが重要です。次のようなVPNソリューションを使用することを検討してください。 • Acronis法人向けVPN • OpenVPN • Cisco AnyConnect • NordVPN • TunnelBear • ExpressVPN • PureVPN • CyberGhost VPN • Perimeter 81 • VyprVPN • IPVanish VPN • Hotspot Shield VPN • Fortigate VPN • ZYXEL VPN • SonicWall GVPN • LANCOM VPN	
ディスク暗号化	エージェントは、マシンのディスク暗号化が有効であるかどうかを確認します。 エージェントは、Windows BitLockerがオンになっているかどうかを確認します。	検査結果 • フルディスク暗号化が有効です。マシンは物理的な改ざんに対して保護されています（+125ポイント） • 一部のハードディスクのみが暗号化されています。マシンが物理的な改ざんのリスクにさらされている可能性があります（+75ポイント） • ディスク暗号化が見つかりませんでした。マシンが物理的な改ざんのリスクにさらされています（0ポイント） #CyberFitスコアによる推奨事項 Windows BitLockerをオンにして、データとファイルの保護を強化することをお勧めします。 ガイドWindowsでデバイス暗号化をオンにする方法	125 - すべてのディスクが暗号化されています 75 - 少なくとも1基のディスクが暗号化されていますが、暗号化されていないディスクもあります 0 - ディスクが暗号化されていません
ネットワークセキュリティ（リモートサー	エージェントは、マシンがリモートサーバーへの送信NTLMトラフィックを制限しているかどうかを確認し	検査結果 • リモートサーバーへの送信NTLMトラフィックが拒否されました。資格情報は保護されています（+25ポイント）	25 - 送信NTLMトラフィックがすべて拒否に設定されています

バーへの送信NTLMトラフィック）	ます。	• リモートサーバーへの送信NTLMトラフィックが拒否されていません。資格情報は公開される危険にさらされている可能性があります（0ポイント） #CyberFitスコアによる推奨事項 セキュリティ保護を強化するため、リモートサーバーへのすべての送信NTLMトラフィックを拒否することをお勧めします。NTLM設定を変更し、例外を追加する方法については、以下のリンクを参照してください。 ガイドリモートサーバーへの送信NTLMトラフィック制限	0 - 送信NTLMトラフィックが別の値に設定されています

メトリクスそれぞれの合計ポイントに基づくマシンの#CyberFitスコア合計が、以下のエンドポイント保護レベルを示す評価結果のいずれかに当てはめられます。

- 0 - 579 - 脆弱
- 580 - 669 - 普通
- 670 - 739 - 良好
- 740 - 799 - 非常に良好
- 800 - 850 - 優れている

Cyber Protectコンソールでマシンの#CyberFitスコアを確認するには、**[デバイス]** > **[すべてのデバイス]** に進みます。デバイスの一覧で、**[#CyberFitスコア]** 列にスコアが表示されています。マシンの[#CyberFitスコア] スキャンを実行することでもセキュリティ状態を確認できます。

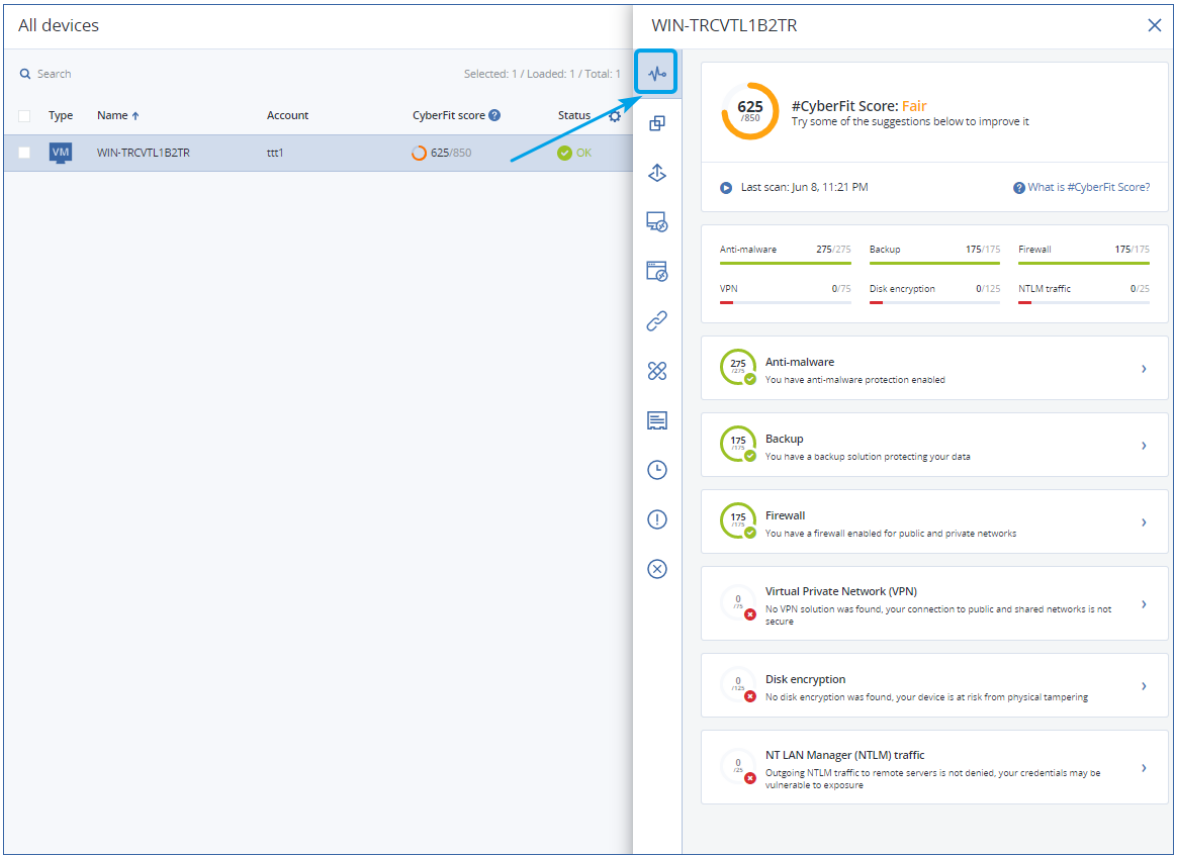


対応するウィジェットとレポートのページでも、#CyberFitスコアの情報を確認できます。

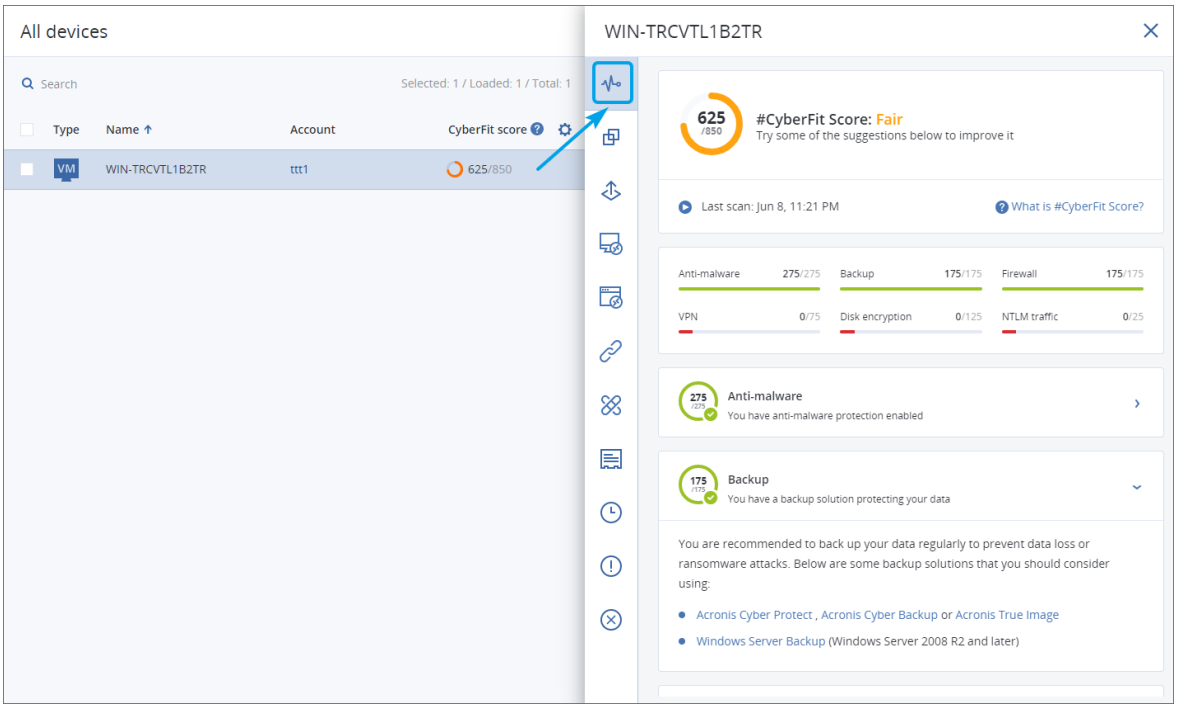
#CyberFitスコアスキャンの実行

#CyberFitスコアスキャンを実行する

1. Cyber Protectコンソールで **[デバイス]** に進みます。
2. マシンを選択して、**[#CyberFitスコア]** をクリックします。
3. これまでに一度もマシンのスキャンを行ったことがない場合は、**[初回スキャンを実行]** をクリックします。
4. スキャンが完了すると、マルウェア対策、バックアップ、ファイアウォール、仮想プライベートネットワーク（VPN）、ディスク暗号化、NT LAN Manager（NTLM）トラフィックなど、6つの評価メトリクスによるスコアと共に、マシンの合計#CyberFitスコアが表示されます。



5. セキュリティ構成の改善につながる可能性のある、各メトリクスでスコア向上を図る方法を確認するには、対応するセクションを展開して推奨事項をお読みください。



6. 推奨事項に対処してから、#CyberFitスコア合計のすぐ下にある矢印アイコンをクリックすると、マシンの#CyberFitスコアをいつでも再計算できます。

サイバースクリプト処理

サイバースクリプトによって、スクリプトで、ソフトウェアのインストール、設定の変更、サービスの開始または停止、アカウントの作成など、環境内のWindowsおよびmacOSマシン上のルーチン操作を自動化できます。そのため、このような操作に費やす時間を短縮し、手動で実行する際のエラーのリスクを減らすことができます。

サイバースクリプトは、カスタマーレベルの管理者/ユーザーだけでなく、パートナー管理者（サービスプロバイダー）も利用可能です。管理者の異なるレベルの詳細については、"マルチテナントサポート"（318ページ）を参照してください。

スクリプトを使用できるようにするには、事前に承認する必要があります。**サイバー管理者**ロールを付与された管理者のみが、新しいスクリプトを承認し、テストすることができます。スクリプトステータスの変更については、"スクリプトステータスの変更"（239ページ）を参照してください。

ユーザー ロールによって、スクリプトとスクリプト計画で実行できる操作が異なります。ロールの詳細については、"ユーザーロールとサイバースクリプトの権限"（229ページ）を参照してください。

前提条件

- サイバースクリプト機能を利用するには、Advanced Managementパックが必要です。
- スクリプトの編集、スクリプトの実行、スクリプト計画の作成など、サイバースクリプトのすべての機能を利用するには、アカウントの二要素認証を有効にする必要があります。

制限事項

- 以下のスクリプト言語をサポートしています。
  - PowerShell
  - Bash
- サイバースクリプト処理は、プロテクションエージェントがインストールされているターゲットマシンでのみ実行可能です。

サポートされるプラットフォーム

サイバースクリプト処理は、WindowsおよびmacOSワークロードで使用できます。

次の表に、サポートされるバージョンを示します。

オペレーティングシステム	バージョン
Windows	Windows 7 SP1以降 - すべてのエディション
	Windows 8/8.1 – Windows RTエディションを除くすべてのエディション（x86、x64）
	Windows 10 - Home、Pro、Education、Enterprise、IoT Enterpriseエディション
	Windows 11
	Windows Server 2008 R2 SP1以降: Standard、Enterprise、Datacenter、Foundation、Web の各エディション
	Windows Server 2012/2012 R2: すべてのエディション
	Windows Server 2016
	Windows Server 2019
	Windows Server 2022
	Windows Storage Server（2008 R2、2012、2012 R2、2016）
macOS	macOS Mojave 10.14
	macOS Catalina 10.15
	macOS Big Sur 11
	macOS Monterey 12

ユーザーロールとサイバースクリプトの権限

スクリプトとスクリプト計画で実行できる操作は、スクリプトのステータスとユーザーのロールによって異なります。

管理者は、自分のテナントとその子テナント内のオブジェクトを管理できます。上位の管理者レベルのオブジェクトがある場合、そのオブジェクトを閲覧したりアクセスしたりすることはできません。

高レベルの管理者が自分のワークロードに適用したスクリプト計画の場合、低レベルの管理者に付与されるのは読み取り専用のアクセス権のみです。

以下のロールには、サイバースクリプトに関する権限が付与されます。

- **社内管理者**
  このロールにより、管理者に対しすべてのサービスに対する完全な権限が付与されます。サイバースクリプトに関しては、サイバー管理者ロールと同じ権限が付与されます。
- **サイバー管理者**
  このロールには、テナントで使用できるスクリプトの承認や、**テスト**ステータスでスクリプトを実行する機能など、完全な許可が付与されます。
- **管理者**
  このロールには、承認されたスクリプトを実行したり、そのスクリプトを使用するスクリプト計画を作成/実行したりするための、限定的な許可が付与されます。
- **読み取り専用管理者**
  このロールには、テナントで使用されるスクリプトと保護計画を表示することができる、限定的な許可が付与されます。
- **ユーザー**
  このロールには、承認されたスクリプトを実行したり、そのスクリプトを使用するスクリプト計画を作成/実行したりするための、限定的な許可が付与されます。この操作は、ユーザーのマシン上でのみ実行できます。

スクリプトのステータスとユーザーロールに応じて実行できるすべての操作を次の表にまとめました。

ロール	目的	スクリプトのステータス		
		下書き	テスト中	承認済み
サイバー管理者 **社内管理者**	スクリプト計画	編集（計画からドラフトのスクリプトを削除） 削除 取り消し 無効にする 停止	作成 編集 適用 有効にする 実行 削除 取り消し 無効にする 停止	作成 編集 適用 有効にする 実行 削除 取り消し 無効にする 停止
	スクリプト	作成	作成	作成

		編集 ステータスを変更 クローンを作成 削除 実行をキャンセル	編集 ステータスを変更 実行 クローンを作成 削除 実行をキャンセル	編集 ステータスを変更 実行 クローンを作成 削除 実行をキャンセル
管理者 **ユーザー**（それぞれが所有するワークロード）	スクリプト計画	表示 取り消し 無効にする 停止	表示 実行をキャンセル	作成 編集 適用 有効にする 実行 削除 取り消し 無効にする 停止
	スクリプト	作成 編集 クローンを作成 削除 実行をキャンセル	表示 クローンを作成 実行をキャンセル	実行 クローンを作成 実行をキャンセル
読み取り専用管理者	スクリプト計画	表示	表示	表示
	スクリプト	表示	表示	表示

スクリプト

スクリプトは、実行時に解析され、ターゲットマシンで実行される命令セットです。スクリプトは、反復的なタスクや複雑なタスクを自動化するための便利な解決策を提供します。

サイバースクリプト処理によって、定義済みのスクリプトを実行したり、カスタムスクリプトを作成したりできます。利用可能なすべてのスクリプトは、**[管理]** > **[スクリプトリポジトリ]** で確認できます。定義済みのスクリプトは、**[ライブラリ]** セクションにあります。テナントに作成またはクローン作成したスクリプトは、**[マイスクリプト]** セクションにあります。

スクリプトは、スクリプト計画に含めるか、**[スクリプトのクイック実行]** 処理を実行することで使用できます。

注意
承認されたスクリプトは、テナントで作成されたもの、またはテナントにクローンされたもののみ使用できます。スクリプトがスクリプトリポジトリから削除された場合、または **[下書き]** ステータスの場合、スクリプトは実行されません。スクリプト操作の詳細の確認やキャンセルは、**[監視]** > **[アクティビティ]** で行えます。

次の表は、スクリプトのステータスによって可能な操作の詳細をまとめたものです。

ステータス	実行可能な操作
下書き	新しく作成したスクリプトと、リポジトリにクローンを作成したスクリプトは、**[下書き]** ステータスになる。これらのスクリプトを実行したり、スクリプト計画に含めたりすることはできない。
テスト中	**サイバー管理者**ロールを付与された管理者は、これらのスクリプトを実行し、スクリプト計画に含めることができる。
承認済み	これらのスクリプトを実行し、スクリプト計画に含めることができる。

スクリプトのステータス変更や、承認済みスクリプトの削除を実行できるのは、**サイバー管理者**ロールを付与された管理者のみです。詳細については、"スクリプトステータスの変更"（239ページ）を参照してください。

スクリプトの作成

手動でコードを書いてスクリプトを作成できます。

スクリプトを作成するには

1. Cyber Protectコンソールで **[管理]** > **[スクリプトリポジトリ]** に進みます。
2. **[マイ スクリプト]** で、**[AIを利用してスクリプトを作成]** をクリックします。
3. メインのペインで、スクリプトの本体を書き込みます。

重要
スクリプトを作成する際は、処理ごとに終了コードのチェックを入れてください。そうでない場合、失敗した処理が無視され、**[監視]** > **[アクティビティ]** のステータスが、誤って **[成功]** と表示される可能性があります。

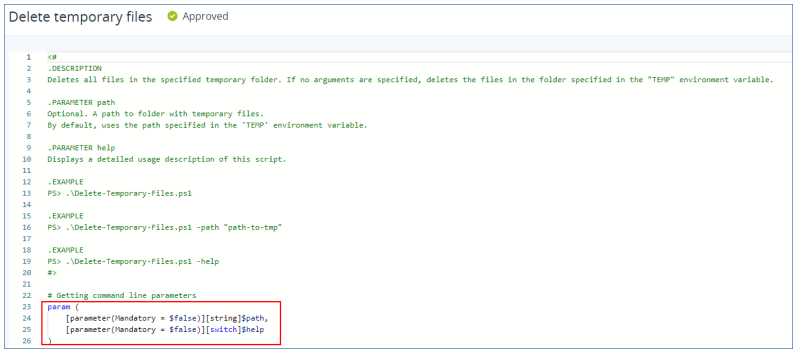
4. スクリプト設定を指定します。

設定	説明
スクリプト名	スクリプト名。このフィールドは自動的に入力され、値を変更可能。
説明	スクリプトの説明。この設定はオプション。 （AIによって生成されたスクリプトの場合）このフィールドはスクリプト生成時に自動的に入力されます。AIによって入力された説明は編集できます。

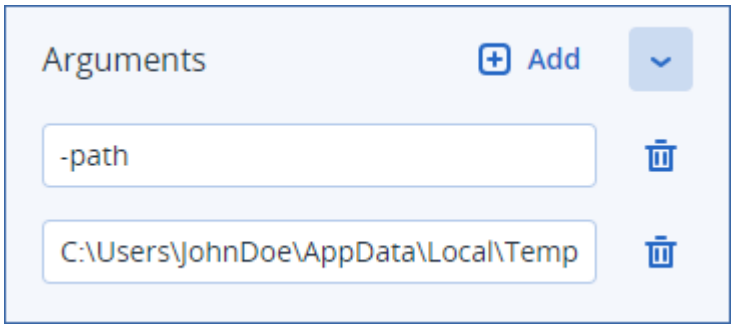
設定	説明
言語	スクリプト言語。次の値を使用可能。 • **PowerShell**。デフォルト値。 • **Bash** （AIによって生成されたスクリプトの場合）この設定はスクリプト生成前に設定される。
オペレーティングシステム	スクリプトが実行されるターゲットワークロードにインストールされているオペレーティングシステム。次の値を使用可能。 • **Windows**。デフォルト値。 • **macOS** （AIによって生成されたスクリプトの場合）この設定はスクリプト生成前に設定される。
ステータス	スクリプトのステータス。 • **下書き**。新しく作成したスクリプトと、リポジトリにクローンを作成したスクリプトは、[**下書き**] ステータスになる。**下書き**スクリプトを実行したり、スクリプト計画に含めたりすることはできない。 • **テスト**。**サイバー管理者**のロールを付与された管理者のみ、スクリプトステータスの [**テスト**] への変更、スクリプトの [**テスト**] ステータスでの実行、そのようなスクリプトを使用したスクリプト計画の実行の各操作が可能。 • **承認**。**承認済み** スクリプトを実行し、スクリプト計画に含めることができる。 スクリプトのステータス変更や、承認済みスクリプトの削除を実行できるのは、**サイバー管理者**ロールを付与された管理者のみです。詳細については、"スクリプトステータスの変更"（239ページ）を参照してください。
タグ	タグでは大文字と小文字が区別されず、最大32文字まで使用可能。丸括弧、角括弧、カンマ、スペースは使用不可。 この設定はオプション。 （AIによって生成されたスクリプトの場合）**AI生成**タグは、スクリプト生成時に自動的に追加される。手動でこのタグの削除、タグの追加が可能。

5. （資格情報を必要とするスクリプトのみ）資格情報を指定します。
   シングルの資格情報（トークンなど）またはペアになった資格情報（ユーザー名とパスワードなど）を使用することができます。
6. （引数を必要とするスクリプトのみ）以下のように引数とその値を指定します。
   a. [**追加**] をクリックします。
   b. 最初の[**引数を追加**] フィールドで、引数を指定します。
   c. [**追加**] をクリックします。
   d. 表示される2番目のフィールドで、引数の値を指定します。

注意
引数は、スクリプト本体ですでに定義されている場合にのみ指定可能です。



例:



e. 複数の引数を追加する必要がある場合は、上記の手順を繰り返してください。

7. **[保存]** をクリックします。

スクリプトは **[下書き]** ステータスでリポジトリに保存されます。

サイバー管理者ロールを持つ管理者がスクリプトのステータスを **[承認済み]** に変更するまで、スクリプトを使用できません。詳細については、"スクリプトステータスの変更"（239ページ）を参照してください。

管理している別のテナントでスクリプトを使用するには、そのテナントにスクリプトのクローンを作成する必要があります。詳細については、"スクリプトのクローン作成"（237ページ）を参照してください。

AIを利用したスクリプトの作成（ScriptPilot）

注意
ScriptPilotにはAdvanced Managementパックが必要です。

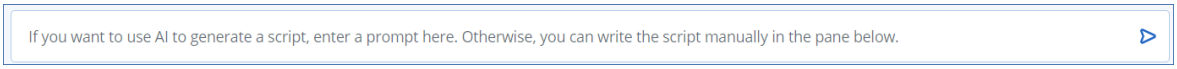
ScriptPilotを使用すると、AIを利用してプロンプトを強力なスクリプトに変換し、時間と労力を節約できます。この機能は以下の方法で使用できます。

- AIにスクリプトをゼロから生成するよう求めるプロンプトを入力する。
- プロンプトを入力して、スクリプト本体に入力したコードをAIが確認して完成させるように求める。この機能は、複雑なコードに取り組むときに活用できます。

ScriptPilotはOpenAIのGPT-4モデルを使用しています。ScriptPilotで組織は1暦月あたり最大100スクリプトまで無料で作成できます。

AIを利用してスクリプトを作成するには

1. Cyber Protectコンソールで **[管理]** > **[スクリプトリポジトリ]** に進みます。
2. **[マイ スクリプト]** で、**[AIを利用してスクリプトを作成]** をクリックします。
3. プロンプトにスクリプトで実行する内容の説明を入力します。入力する説明は、できるだけ明確に詳しくしてください。

   例:

   ```
   I need a script that deletes Temporary files for all users (including user profiles + Windows Temps) and disable Windows Update Service to allow the script to run
   ```

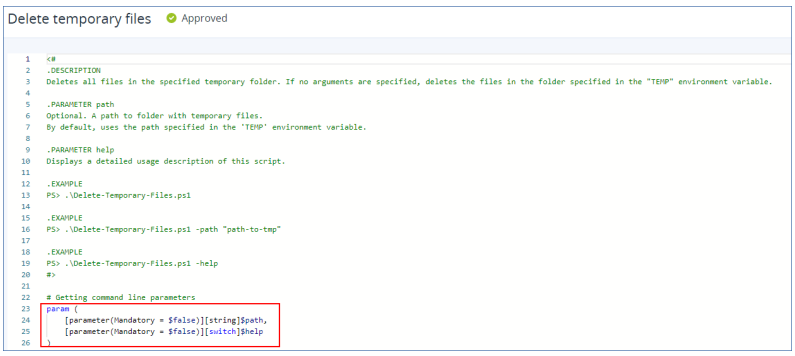
4. プロンプトで矢印ボタンをクリックします。
5. 確認ウィンドウで言語とオペレーティングシステムを選択し、**[生成]** をクリックします。
   AIが生成したスクリプトがメインペインに表示されます。スクリプトの名前と説明は、スクリプトと一致するようにAIによって自動生成されます。**AIが生成した**タグは、スクリプトに自動的に割り当てられます。
6. AIが生成したスクリプトを確認し、必要に応じて手動で編集します。
7. 必要に応じて、スクリプトの設定を編集します。

設定	説明
スクリプト名	スクリプト名。このフィールドは自動的に入力され、値を変更可能。
説明	スクリプトの説明。この設定はオプション。 （AIによって生成されたスクリプトの場合）このフィールドはスクリプト生成時に自動的に入力されます。AIによって入力された説明は編集できます。
言語	スクリプト言語。次の値を使用可能。 • **PowerShell**。デフォルト値。 • **Bash** （AIによって生成されたスクリプトの場合）この設定はスクリプト生成前に設定される。
オペレーティングシステム	スクリプトが実行されるターゲットワークロードにインストールされているオペレーティングシステム。次の値を使用可能。 • **Windows**。デフォルト値。 • **macOS** （AIによって生成されたスクリプトの場合）この設定はスクリプト生成前に設定される。
ステータス	スクリプトのステータス。 • **下書き**。新しく作成したスクリプトと、リポジトリにクローンを作成したスクリプトは、**[下書き]** ステータスになる。**下書き**スクリプトを実行したり、スクリプト計画に含めたり

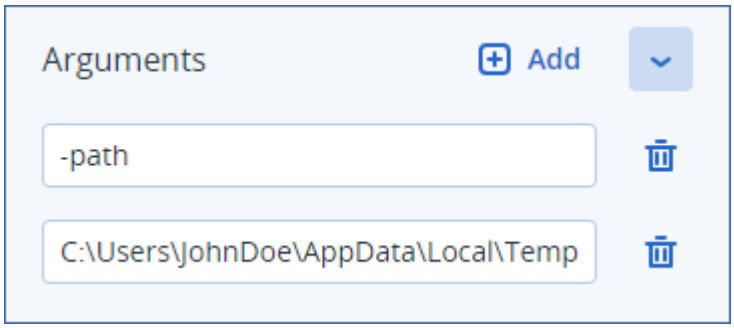
設定	説明
	することはできない。 • **テスト。サイバー管理者**のロールを付与された管理者のみ、スクリプトステータスの **[テスト]** への変更、スクリプトの **[テスト]** ステータスでの実行、そのようなスクリプトを使用したスクリプト計画の実行の各操作が可能。 • **承認。承認済み** スクリプトを実行し、スクリプト計画に含めることができる。 スクリプトのステータス変更や、承認済みスクリプトの削除を実行できるのは、**サイバー管理者**ロールを付与された管理者のみです。詳細については、"スクリプトステータスの変更"（239ページ）を参照してください。
タグ	タグでは大文字と小文字が区別されず、最大32文字まで使用可能。丸括弧、角括弧、カンマ、スペースは使用不可。 この設定はオプション。 （AIによって生成されたスクリプトの場合）**AI生成**タグは、スクリプト生成時に自動的に追加される。手動でこのタグの削除、タグの追加が可能。

8. （オプション）（資格情報を必要とするスクリプトのみ）資格情報を指定します。
   シングルの資格情報（トークンなど）またはペアになった資格情報（ユーザー名とパスワードなど）を使用することができます。
9. （引数を必要とするスクリプトのみ）以下のように引数とその値を指定します。
   a. **[追加]** をクリックします。
   b. 最初の**[引数を追加]** フィールドで、引数を指定します。
   c. **[追加]** をクリックします。
   d. 表示される2番目のフィールドで、引数の値を指定します。

注意
引数は、スクリプト本体ですでに定義されている場合にのみ指定可能です。



例:



e. 複数の引数を追加する必要がある場合は、上記の手順を繰り返してください。

10. **[保存]** をクリックします。

    スクリプトは **[下書き]** ステータスでリポジトリに保存されます。

    サイバー管理者ロールを持つ管理者がスクリプトのステータスを **[承認済み]** に変更するまで、スクリプトを使用できません。詳細については、"スクリプトステータスの変更"（239ページ）を参照してください。

    管理している別のテナントでスクリプトを使用するには、そのテナントにスクリプトのクローンを作成する必要があります。詳細については、"スクリプトのクローン作成"（237ページ）を参照してください。

スクリプトのクローン作成

次のような場合にスクリプトのクローンを作成する必要があります。

- **ライブラリ**のスクリプトを使用する前。この場合、まずスクリプトを **[マイスクリプト]** セクションにクローンを作成する必要があります。
- 親テナントで作成したスクリプトをその子テナントやユニットにクローンしたい場合。

スクリプトのクローンを作成するには

1. **スクリプトリポジトリ**で、クローンを作成したいスクリプトを見つけます。
2. 次のいずれかを実行します。
   - （**マイスクリプト**からスクリプトのクローンを作成する場合）スクリプト名の横にある省略記号（...）のアイコンをクリックして、**[クローン]** をクリックします。
   - （**ライブラリ**からスクリプトのクローンを作成する場合）選択したスクリプト名の横にある **[クローン]** をクリックします。
3. **[スクリプトのクローンを作成]** のポップアップで、**[ステータス]** ドロップダウンリストから次のいずれかのスクリプトステータスを選択します。
   - **下書き**（デフォルト） - このステータスの場合、スクリプトをすぐに実行することはできません。
   - **テスト** - このステータスの場合、スクリプトを実行できます。
   - **承認済み** - このステータスの場合、スクリプトを実行できます。
4. （複数のテナントまたはユニットを管理している場合）スクリプトのクローンを作成する場所を選択します。

   [スクリプトのクローンを作成] ダイアログボックスには、管理可能なテナントとAdvanced Managementパックが適用されたテナントのみが表示されます。

その結果、スクリプトのクローンが作成され、選択したテナントまたはユニットの**マイスクリプト**セクションに表示されます。ユニットを含まない単一のテナントのみを管理している場合、スクリプトは自動的に**マイスクリプト**セクションにコピーされます。

重要
オリジナルでないテナントにスクリプトをクローンする場合、スクリプトが使用する資格情報はコピーされません。

スクリプトの編集または削除

注意
ユーザー ロールによって、スクリプトとスクリプト計画で実行できる操作が異なります。ロールの詳細については、"ユーザーロールとサイバースクリプトの権限"（229ページ）を参照してください。

スクリプトを編集するには

1. **スクリプトリポジトリ**で、**マイスクリプト**に移動して、編集したいスクリプトを見つけます。
2. スクリプト名の横にある省略記号（...）のアイコンをクリックして、**[編集]** をクリックします。
3. スクリプトを編集してから、**[保存]** をクリックします。
4. （スクリプト計画で使用されるスクリプトを編集する場合）**[スクリプトを保存]** をクリックして選択を確認します。

   注意
   スクリプト計画の次回実行時には、最新バージョンのスクリプトが使用されます。

スクリプトのバージョン

以下に示すスクリプトの属性のいずれかを編集する場合、新しいバージョンのスクリプトが作成されます。

- スクリプト本文
- スクリプト名
- 説明
- スクリプトの言語
- 資格情報
- 引数

他の属性を変更する場合は、編集内容が現在のバージョンのスクリプトに追加されます。バージョンとそれらを比較する方法の詳細については、"スクリプトのバージョンの比較"（239ページ）を参照してください。

注意
スクリプトのステータスは、**[ステータス]** フィールドの値を変更したときのみアップデートされます。サイバー管理者のロールを付与された管理者のみが、スクリプトのステータスを変更できます。

スクリプトを削除するには

1. **スクリプトリポジトリ**で、**マイスクリプト**に移動して、削除したいスクリプトを見つけます。
2. スクリプト名の横にある省略記号（...）のアイコンをクリックして、**[削除]** をクリックします。
3. **[削除]** をクリックします。
4. （スクリプト計画で使用されるスクリプトを削除する場合）**[スクリプトを保存]** をクリックして選択を確認します。

注意
削除されたスクリプトを使用するスクリプト計画は、実行できません。

スクリプトステータスの変更

新しいスクリプトが作成され、**[下書き]** 状態にある場合は、ステータスが **[承認済み]** に変更されるまで使用できません。ユースケースによっては、スクリプトが承認されるまでの一定期間、ステータスが **[テスト]** になる場合があります。

注意
ユーザー ロールによって、スクリプトとスクリプト計画で実行できる操作が異なります。ロールの詳細については、"ユーザーロールとサイバースクリプトの権限"（229ページ）を参照してください。

前提条件

- ユーザーは、**サイバー管理者**ロールが割り当てられている管理者である。
- 対応する状態のスクリプトを使用できる。

スクリプトステータスを変更するには

1. **スクリプトリポジトリ**で **[マイスクリプト]** に移動します。
2. スクリプト名の横にある省略記号（...）のアイコンをクリックして、**[編集]** をクリックします。
3. **[ステータス]** ドロップダウンリストで、ステータスを選択します。
4. **[保存]** をクリックします。
5. （承認済みスクリプトのステータスを変更する場合）変更を確定するには、**[スクリプトを保存]** をクリックします。

注意
スクリプトのステータスが**ドラフト**にダウングレードされた場合は、それを使用するスクリプト計画の実行に失敗します。
サイバー管理者ロールを付与された管理者のみが、**テスト**ステータスのスクリプトと、そのスクリプトを含むスクリプト計画を実行できます。

スクリプトのバージョンの比較

スクリプトの2つのバージョンを比較し、以前のバージョンに戻すことができます。また、特定のバージョンの作成者と作成時期を確認することもできます。

スクリプトのバージョンを比較するには

1. **スクリプトリポジトリ**で、**マイスクリプト**に移動して、バージョンを比較したいスクリプトを見つけます。
2. スクリプト名の横にある省略記号（...）のアイコンをクリックして、**[バージョン履歴]** をクリックします。
3. 比較したい2つのバージョンを選択して、**[バージョンを比較]** をクリックします。
   スクリプトの本体、引数、資格情報などに変更があった場合は、ハイライト表示されます。

以前のバージョンに戻すには

1. **[スクリプトのバージョンを比較]** ウィンドウで、**[このバージョンに戻す]** をクリックします。
2. **[以前のバージョンに戻す]** のポップアップで、**[ステータス]** ドロップダウンリストからスクリプトステータスを選択します。

選択したバージョンが復元され、バージョン履歴に最新のバージョンとして保存されます。

スクリプトを復元するには、**[バージョン履歴]** ウィンドウからバージョンを選択し、**[復元]** ボタンをクリックすることも可能です。

重要
スクリプトは、**[テスト]** または **[承認済み]** のステータスのみで実行できます。詳細については、"スクリプトステータスの変更"（239ページ）を参照してください。

スクリプト処理の出力のダウンロード

スクリプト処理の出力を.zipファイル形式でダウンロードできます。**標準出力**とstderrの2種類のテキストファイルが含まれています。**標準出力**では、正常に終了したスクリプト処理の結果を確認できます。stderrファイルには、スクリプト処理中に発生したエラーの情報が含められます。

出力ファイルをダウンロードするには

1. Cyber Protectコンソールで、**[監視]** > **[アクティビティ]** に進みます。
2. 出力のダウンロードを実行する、サイバースクリプト処理のアクティビティをクリックします。
3. **[アクティビティの詳細]** 画面で、**[出力をダウンロード]** をクリックします。

スクリプトのリポジトリ

スクリプトリポジトリは、**[管理]** タブの下で見つけることができます。リポジトリでは、スクリプトの名前と説明をキーワードにして検索を実行できます。また、フィルタを使用したり、スクリプトの名前やステータスでソートしたりすることもできます。

スクリプトを管理するには、スクリプト名の横にある省略記号（...）のアイコンをクリックしてから、任意の操作を選択します。または、スクリプトをクリックし、開いた画面のボタンを使用します。

スクリプトリポジトリには、以下のセクションが含まれています。

- **マイスクリプト**
  ここでは、現在の環境で直接利用可能なスクリプトを見つけることができます。オリジナルで作成したスクリプトと、ここでクローンしたスクリプトがあります。

このセクションのスクリプトは、次の条件で検索によってフィルタリングできます。
  - タグ
  - ステータス
  - 言語
  - オペレーティングシステム
  - スクリプトの所有者
- **ライブラリ**
  ライブラリには定義済みのスクリプトが含まれており、**マイスクリプト**セクションでクローンを作成した後、現在の環境で使用できます。これらのスクリプトについては、検査とクローン作成のみ実行できます。
  このセクションのスクリプトは、次の条件で検索によってフィルタリングできます。
  - タグ
  - 言語
  - オペレーティングシステム
  詳細については、「ベンダーによって認証されたスクリプト（70595）」を参照してください。

スクリプト計画

スクリプト計画では、複数のワークロードに対するスクリプトの実行、スクリプト実行に関するスケジュールの設定、また追加の設定を行うことができます。

作成したスクリプト計画とワークロードに適用されたスクリプト計画は、**[管理]** > **[スクリプト計画]** で確認できます。ここでは、計画を実行するロケーション、オーナー、ステータスを確認できます。

クリック可能なバーに、スクリプト計画のステータスが以下のように色分けして表示されます。

- 実行中（青）
- 互換性を確認中（ダークグレイ）
- 無効（ライトグレイ）
- OK（緑）
- 重要なアラート（赤）
- エラー（オレンジ）
- 警告（黄色）

バーをクリックすると、計画がどのようなステータスで、また何件のワークロードで運用されているかがわかります。各ステータスをクリックすることもできます。

[スクリプト計画] タブで、次の操作を行うことで計画を管理できます。

- 実行
- 停止
- 編集
- 名前の変更
- 無効にする
- 有効にする

- クローンを作成
- エクスポート: 計画の構成はJSON形式でローカルのマシンにエクスポートされます。
- 削除

スクリプト計画の可視性と、その計画で実行可能なアクションは、計画の所有者/ユーザーのロールによって異なります。例えば、社内管理者は、ワークロードに適用されているパートナー所有のスクリプト計画に対する可視性のみを有しています。これらの計画で操作を実行することはできません。

スクリプト計画を作成および管理できるユーザーの詳細については、"ユーザーロールとサイバースクリプトの権限"（229ページ）を参照してください。

スクリプト計画を管理するには

1. Cyber Protectコンソールで **[管理]** > **[スクリプト計画]** に進みます。
2. 管理する計画を見つけ、その横にある省略記号（...）をクリックします。
3. 任意の操作を選択してから、画面の指示に従います。

スクリプト計画の作成

以下の方法でスクリプト計画を作成できます。

- **[デバイス]** タブで
  ワークロードを選択して、それらに対するスクリプト計画を作成します。
- **[管理]** > **[スクリプト計画]** タブで
  スクリプト計画を作成し、計画を適用するワークロードを選択します。

[デバイス] タブでスクリプト計画を作成するには

1. Cyber Protectコンソールで **[デバイス]** > **[エージェントがインストールされているマシン]** に進みます。
2. スクリプト計画を適用するワークロードまたはデバイスグループを選択し、それぞれについて **[保護]** または **[保護グループ]** をクリックします。
3. （すでに適用済みの計画の場合）**[計画を追加]** をクリックします。
4. **[計画の作成]** > **[スクリプト計画]** をクリックします。
   スクリプト計画のテンプレートを開きます。
5. （オプション） スクリプト計画名を変更するには、鉛筆のアイコンをクリックします。
6. **[スクリプトを選択]** をクリックして使用するスクリプトを選択し、**[完了]** をクリックします。

   注意
   自分の承認済みスクリプトを、必ず **[スクリプトリポジトリ]** > **[マイスクリプト]** から使用します。**テスト**ステータスでスクリプトを使用することができるのは、**サイバー管理者ロール**を割り当てられた管理者のみです。ロールの詳細については、"ユーザーロールとサイバースクリプトの権限"（229ページ）を参照してください。

7. スクリプト計画のスケジュールと開始条件を構成します。

8. ターゲットワークロードのどのアカウントでスクリプトを実行するかを選択します。次から選択できます。
   - システムアカウント（macOS、これはルートアカウントです）
   - 現在ログインしているアカウント
9. ターゲットワークロード上でスクリプトを実行できる、時間の長さを指定します。
   設定された時間内にスクリプトの実行が終了しない場合、サイバースクリプト処理は失敗します。
   指定できる最小値は1分、最大値は1440分です。
10. （PowerShellスクリプトのみ）PowerShellの実行ポリシーを構成します。
    このポリシーの詳細については、Microsoftの文書を参照してください。
11. **[作成]** をクリックします。

[スクリプト計画] タブでスクリプト計画を作成するには

1. Cyber Protectコンソールで **[管理]** > **[スクリプト計画]** に進みます。
2. **[計画の作成]** をクリックします。
   スクリプト計画のテンプレートを開きます。
3. （オプション） 新しい計画を適用するワークロードまたはデバイスグループを選択するには、**[ワークロードを追加]** をクリックします。
   a. **[エージェントがインストールされているマシン]** をクリックしてリストを展開し、任意のワークロードまたはデバイスグループを選択します。
   b. **[追加]** をクリックします。
   パートナーレベルでデバイスグループを作成する方法については、"[デバイス] タブ"（313ページ）を参照してください。

   注意
   また、計画を作成した後にワークロードまたはデバイスグループを選択することもできます。

4. （オプション） スクリプト計画名を変更するには、鉛筆のアイコンをクリックします。
5. **[スクリプトを選択]** をクリックして使用するスクリプトを選択し、**[完了]** をクリックします。

   注意
   自分の承認済みスクリプトを、必ず **[スクリプトリポジトリ]** > **[マイスクリプト]** から使用します。**テスト**ステータスでスクリプトを使用することができるのは、**サイバー管理者ロール**を割り当てられた管理者のみです。ロールの詳細については、"ユーザーロールとサイバースクリプトの権限"（229ページ）を参照してください。

6. スクリプト計画のスケジュールと開始条件を構成します。
7. ターゲットワークロードのどのアカウントでスクリプトを実行するかを選択します。次から選択できます。
   - システムアカウント（macOS、これはルートアカウントです）
   - 現在ログインしているアカウント
8. ターゲットワークロード上でスクリプトを実行できる、時間の長さを指定します。
   設定された時間内にスクリプトの実行が終了しない場合、サイバースクリプト処理は失敗します。

指定できる最小値は1分、最大値は1440分です。

9. （PowerShellスクリプトのみ）PowerShellの実行ポリシーを構成します。
   このポリシーの詳細については、Microsoftの文書を参照してください。
10. **[作成]** をクリックします。

スケジュールと開始条件

スケジュール

スクリプト計画は、1回または繰り返し実行するように設定できます。またスケジュールに従って起動させたり、特定のイベントが発生したときに起動させたりすることもできます。

次から選択できます。

- 1回だけ実行
  このオプションでは、計画が実行される日付と時間を構成する必要があります。
- 時刻でスケジュール
  このオプションにより、毎時、毎日、または毎月実行するスクリプト計画を構成できます。
  スケジュールを一時的に有効にしたい場合は、**[日付範囲内に実行]** チェックボックスにチェックを入れ、スケジュール済みの計画が実行される期間を設定します。
- システムへのユーザーログイン時
  特定のユーザーのみがスクリプト計画をトリガーするか、ログイン中の任意のユーザーがトリガーするかを選択できます。
- ユーザーがシステムからログオフするとき
  特定のユーザーのみがスクリプト計画をトリガーするか、ログオフ中の任意のユーザーがトリガーするかを選択できます。
- システムの起動時
- システムがシャットダウンされたとき

  注意
  このスケジューリングオプションは、システムアカウントで実行されるスクリプトにのみ有効です。

- システムがオンラインになったとき

開始条件

開始条件により、スケジュールされている計画に柔軟性を持たせることができます。複数の条件を設定した場合、計画を開始するには、すべての条件が同時に満たされる必要があります。

開始条件は、**[今すぐ実行]** オプションにより、手動で計画を実行した場合には有効になりません。

条件	説明
ワークロードがオンラインの場合にのみ実行	このスクリプトは、ターゲットのワークロードがインターネットに接続されているときに実行されます。

条件	説明
ユーザーがアイドル状態	この条件は、マシンでスクリーンセーバーが実行されているかマシンがロックされている場合に一致します。
ユーザーのログオフ	この条件では、ターゲットワークロードのユーザーがログオフするまで、スケジュール済みのスクリプト計画を延期することができます。
期間の範囲内に収める	この条件では、スクリプト計画は指定された時間間隔内に限って開始されます。例えばこの条件を使用して、「**ユーザーのログオフ**」の条件を制限することができます。
バッテリー電源を節約	この条件により、バッテリー残量が少ないためにスクリプト計画が中断されないようにできます。次から選択できます。 • バッテリー駆動時は開始しない マシンが電源に接続されている場合のみ、計画が開始されます。 • バッテリーレベルが以下の値より高い場合に開始する マシンが電源に接続されているか、バッテリーレベルが指定した値よりも高い場合に計画を開始します。
従量制課金の接続時には開始しない	この条件では、ターゲットのワークロードが従量制接続でインターネットにアクセスしている場合に、計画が開始されないようにできます。
以下のWi-Fiネットワークに接続している場合は開始しない	この条件では、ターゲットのワークロードが、指定されたいずれかのワイヤレスネットワークに接続している場合に、計画が開始されないようにできます。この条件を使用するには、制限対象となるネットワークのSSIDを指定する必要があります。 この制限は、名前の文字列の中に指定した名前が含まれるすべてのネットワークに適用されます（大文字と小文字は区別されません）。例えば、ネットワーク名に「phone」と指定すると、デバイスが次のいずれかのネットワークに接続されている場合、計画は開始されません。「JohnのiPhone」、「phone_wifi」、または「my_PHONE_wifi」。
デバイスのIPアドレスをチェック	この条件では、ターゲットのワークロードにおけるいずれかのIPアドレスが、指定されたIPアドレスの範囲内または範囲外である場合、計画が開始されないようにできます。 次から選択できます。 • 以下のIPレンジの範囲外の場合に開始する • 以下のIPレンジの範囲内の場合に開始する IPv4 アドレスのみがサポートされています。
開始条件を満たさない場合でも、タスクを実行	このオプションでは、他の条件に関係なく、計画が実行される時間間隔を設定できます。その他の条件に一致するか、指定された期間が終了するかのどちらか早い時点で計画が開始されます。 このオプションは、スクリプト計画が一度だけ実行されるように構成されている場合は利用できません。

計画のターゲットワークロードの管理

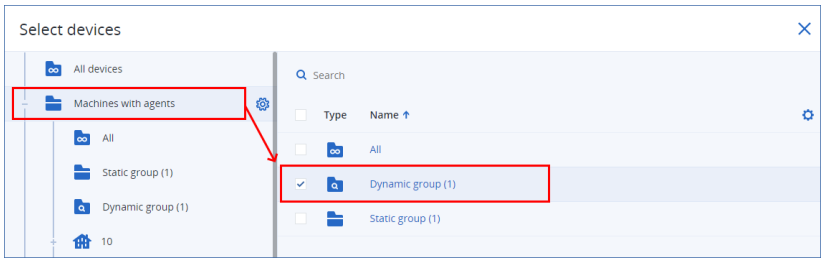
スクリプト計画を適用するワークロードまたはデバイスグループは、計画の作成中、または作成後に選択することができます。

パートナー管理者は、異なるカスタマーのワークロードに同じ計画を適用したり、異なるカスタマーのワークロードを含むデバイスグループを作成したりできます。パートナーレベルで静的または動的デバイスグループを作成する方法については、"[デバイス] タブ"（313ページ）を参照してください。

計画に初期ワークロードを追加するには

1. Cyber Protectコンソールで **[管理]** > **[スクリプト計画]** に進みます。
2. ターゲットのワークロードを指定する計画の名前をクリックします。
3. **[ワークロードを追加]** をクリックします。
4. 任意のワークロードまたはデバイスグループを選択し、**[追加]** をクリックします。

注意
デバイスグループを選択するには、その親レベルをクリックし、メインペインで、その名前の横のチェックボックスを選択します。

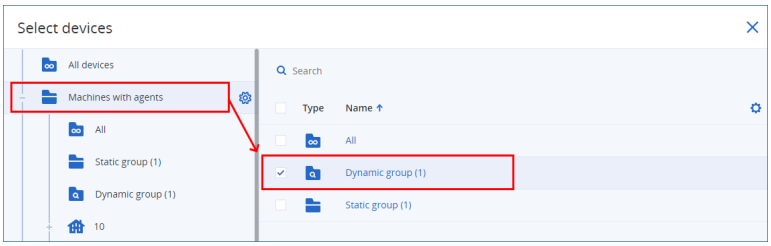


5. 編集した計画を保存するには、**[保存]** をクリックします。

計画の既存のワークロードを管理するには

1. Cyber Protectコンソールで **[管理]** > **[スクリプト計画]** に進みます。
2. 変更したいターゲットのワークロードを含む計画の名前をクリックします。
3. **[ワークロードを管理]** をクリックします。
   [デバイス] 画面には、現在スクリプト計画が適用されているワークロードの一覧が表示されます。（複数のテナントを管理している場合、ワークロードはテナントごとにソートされます。
   - 新しいワークロードまたはデバイスグループを追加するには、**[追加]** をクリックします。
     a. 任意のワークロードまたはデバイスグループを選択します。管理しているすべてのテナントからワークロードを追加できます。

注意
デバイスグループを選択するには、その親レベルをクリックし、メインペインで、その名前の横のチェックボックスを選択します。



b. **[追加]** をクリックします。

- ワークロードまたはデバイスグループを削除するには、それらを選択してから **[削除]** をクリックします。

4. **[完了]** をクリックします。
5. 編集した計画を保存するには、**[保存]** をクリックします。

各管理レベルの計画

各レベルの管理者が参照/管理できる計画の概要を次の表に示します。

管理者	管理レベル	計画	権限
パートナー管理者	パートナーレベル	独自の計画	フルアクセス
		カスタマー計画（ユニットの計画を含む）	フルアクセス
		ユニット計画	フルアクセス
	カスタマーレベル （サービスプロバイダーが管理するカスタマーの場合）	このカスタマーのワークロードに適用されるパートナー計画	読み取り専用
		カスタマー計画（ユニットの計画を含む）	フルアクセス
		ユニット計画	フルアクセス
	ユニットレベル （サービスプロバイダーが管理するカスタマーの場合）	このユニットのワークロードに適用されるパートナー計画	読み取り専用
		このユニットのワークロードに適用されるカスタマー計画	読み取り専用
		ユニット計画	フルアクセス

管理者	管理レベル	計画	権限
企業管理者	カスタマーレベル	このカスタマーまたはユニットのワークロードに適用されるパートナー計画	読み取り専用
		カスタマー計画（ユニットの計画を含む）	フルアクセス
		ユニット計画	フルアクセス
	ユニットレベル	このユニットのワークロードに適用されるパートナー計画	読み取り専用
		このユニットのワークロードに適用されるカスタマー計画	読み取り専用
		ユニット計画	フルアクセス
部署管理者	ユニットレベル	このユニットのワークロードに適用されるパートナー計画	読み取り専用
		このユニットのワークロードに適用されるカスタマー計画	読み取り専用
		ユニット計画	フルアクセス

重要
計画の所有者は、その計画が作成されたテナントになります。従って、パートナー管理者がカスタマーテナントレベルで計画を作成した場合、カスタマーテナントがその計画の所有者となります。

スクリプト計画の互換性の問題

ワークロードにスクリプト計画を適用すると、互換性の問題が発生する場合があります。以下のような互換性の問題が考えられます:

- 互換性のないオペレーティングシステム - この問題は、ワークロードのオペレーティングシステムがサポートされていない場合に発生します。
- サポートされていないエージェント - この問題は、ワークロード上のプロテクションエージェントのバージョンが古く、サイバースクリプト処理機能がサポートされていない場合に発生します。
- クォータの不足 - この問題は、選択したワークロードに割り当てる十分なサービスクォータがテナントに存在しない場合に発生します。

150件以下のワークロードを個別に選択して、スクリプト計画を適用する場合、計画を保存する前に、既存の競合を解決するよう通知が表示されます。競合を解決するには、競合の根本原因を取り除くか、影響を受けるワークロードを計画から削除します。詳細については、"スクリプト計画の互換性の問題を解決する"（249ページ）を参照してください。競合を解決せずに計画を保存すると、互換性のないワークロードに対して計画が自動的に無効にされ、アラートが表示されます。

スクリプト計画が150件を超えるワークロードまたはデバイスグループに適用されている場合、保存された後、互換性が確認されます。互換性のないワークロードに対しては、計画が自動的に無効になり、アラートが表示されます。

スクリプト計画の互換性の問題を解決する

互換性の問題の原因に応じ、新しいスクリプト計画を作成するプロセスの一環として、互換性の問題を解決するための各操作を実行できます。

注意
互換性の問題を解決するために計画からワークロードを削除する場合、デバイスグループの一部となっているワークロードを削除することはできません。

互換性の問題を解決するには

1. **[問題をレビュー]** をクリックします。
2. （互換性がないオペレーティングシステムの互換性の問題を解決するには）
   a. **[互換性がないオペレーティングシステム]** タブで、削除するワークロードを選択します。
   b. **[計画からワークロードを削除]** をクリックします。
   c. **[削除]** をクリックしてから、**[閉じる]** をクリックします。
3. （計画からワークロードを削除して、サポートされていないエージェントの互換性の問題を解決するには）
   a. **[サポートされていないエージェント]** タブで、削除するワークロードを選択します。
   b. **[計画からワークロードを削除]** をクリックします。
   c. **[削除]** をクリックしてから、**[閉じる]** をクリックします。
4. （エージェントのバージョンをアップデートして、サポートされていないエージェントとの互換性の問題を解決するには）**[エージェントリストに移動]** をクリックします。

   注意
   このオプションを使用できるのは、カスタマー管理者のみです。

5. （計画からワークロードを削除して、クォータの不足を伴う互換性の問題を解決するには）
   a. **[クォータの不足]** タブで、削除するワークロードを選択します。
   b. **[計画からワークロードを削除]** をクリックします。
   c. **[削除]** をクリックしてから、**[閉じる]** をクリックします。
6. （テナントのクォータを増やして、クォータの不足による互換性の問題を解決するには）

   注意
   このオプションを使用できるのは、パートナー管理者のみです。

   a. **[クォータの不足]** タブで、**[管理ポータルに移動]** をクリックします。
   b. カスタマーのサービスクォータを増やします。

スクリプトのクイック実行

スクリプトは、スクリプト計画に含めることなく、すぐに実行できます。この操作は、150を超えるワークロード、オフラインワークロード、またはデバイスグループでは使用できません。

ターゲットのワークロードには、スクリプトのクイック実行機能をサポートするサービスクォータが割り当てられます。また、そのテナントでAdvanced Managementパックが有効になっている必要があります。テナント内で利用可能な場合は、適切なサービスクォータが自動的に割り当てられます。

注意
自分の承認済みスクリプトを、必ず **[スクリプトリポジトリ]** > **[マイスクリプト]** から使用します。**テスト**ステータスでスクリプトを使用することができるのは、**サイバー管理者ロール**を割り当てられた管理者のみです。ロールの詳細については、"ユーザーロールとサイバースクリプトの権限"（229ページ）を参照してください。

以下の方法でクイック実行を開始できます。

- **[デバイス]** タブから
  1つまたは複数のワークロードを選択してから、実行するスクリプトを選択します。
- **[管理]** > **[スクリプトリポジトリ]** タブから
  スクリプトを選択してから、1つまたは複数のターゲットワークロードを選択します。

[デバイス] タブからスクリプトを実行する

1. Cyber Protectコンソールで **[デバイス]** > **[すべてのデバイス]** に進みます。
2. スクリプトを実行するワークロードを選択し、**[保護]** をクリックします。
3. **[スクリプトのクイック実行]** をクリックします。
4. **[スクリプトを選択]** をクリックして使用するスクリプトを選択し、**[完了]** をクリックします。
5. ターゲットワークロードのどのアカウントでスクリプトを実行するかを選択します。次から選択できます。
   - システムアカウント（macOS、これはルートアカウントです）
   - 現在ログインしているアカウント
6. ターゲットワークロード上でスクリプトを実行できる、時間の長さを指定します。
   設定された時間内にスクリプトの実行が終了しない場合、サイバースクリプト処理は失敗します。
   1分から1440分までの値を使用できます。
7. （PowerShellスクリプトのみ）PowerShellの実行ポリシーを構成します。
   このポリシーの詳細については、Microsoftのドキュメントを参照してください。
8. **[今すぐ実行]** をクリックします。

[スクリプトリポジトリ] タブからスクリプトを実行するには

1. Cyber Protectコンソールで **[管理]** > **[スクリプトリポジトリ]** に進みます。
2. 実行するスクリプトを選択し、**[スクリプトのクイック実行]** をクリックします。
3. **[ワークロードを追加]** をクリックして、ターゲットのワークロードを選択し、**[追加]** をクリックします。

4. **[スクリプトを選択]** をクリックして使用するスクリプトを選択し、**[完了]** をクリックします。
5. ターゲットワークロードのどのアカウントでスクリプトを実行するかを選択します。次から選択できます。
   - システムアカウント（macOS、これはルートアカウントです）
   - 現在ログインしているアカウント
6. ターゲットワークロード上でスクリプトを実行できる、時間の長さを指定します。
   設定された時間内にスクリプトの実行が終了しない場合、サイバースクリプト処理は失敗します。
   1分から1440分までの値を使用できます。
7. （PowerShellスクリプトのみ）PowerShellの実行ポリシーを構成します。
   このポリシーの詳細については、Microsoftのドキュメントを参照してください。
8. **[今すぐ実行]** をクリックします。

コラボレーションおよびコミュニケーションアプリケーションの保護

Zoom、Cisco Webex Meetings、Citrix Workspace、Microsoft Teamsは、ビデオ/Web会議およびコミュニケーションで広く使用されるようになっています。Cyber Protectionサービスでは、コラボレーションツールを保護できます。

Zoom、Cisco Webex Meetings、Citrix Workspace、Microsoft Teamsの保護設定は類似しています。次の例では、Zoomの構成を検討します。

Zoom保護を設定する

1. コラボレーションアプリケーションがインストールされているマシンで、保護エージェントをインストールします。
2. Cyber Protectコンソールにログインし、次のモジュールのいずれかが有効である保護計画を適用します。
   - **ウイルスおよびマルウェア対策保護**（**自己防御機能**および**Active Protection**設定が有効）- Cyber Protectエディションのいずれかを使用している場合。
   - **Active Protection**（**自己防御機能**設定が有効） - Cyber Backup Editionのいずれかを使用している場合。
3. （オプション）自動アップデートインストールについては、保護計画の**パッチ管理**モジュールを構成してください。

結果として、次のアクティビティを含め、Zoomアプリケーションが保護されます。

- Zoomクライアントのアップデートを自動的にインストール
- コードインジェクションからZoomプロセスを保護
- Zoomプロセスによる不審な動作を防止
- Zoomに関連するドメインの追加から「ホスト」ファイルを保護

現在の保護レベルについて理解する

監視

[監視] タブでは、現在の保護レベルに関する重要な情報を提供します。以下のダッシュボードが含まれています。

- **概要**
- **アクティビティ**
- **アラート**
- **脅威フィード**（詳細については、"脅威フィード"（293ページ）を参照してください）

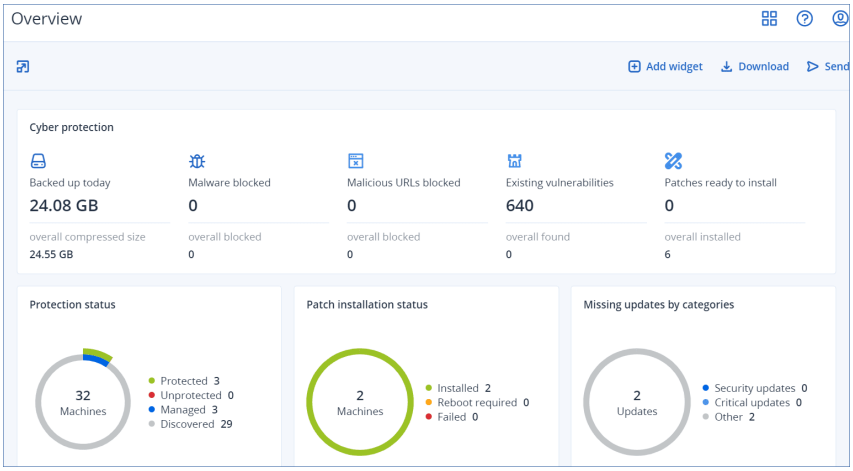
概要ダッシュボード

[概要] ダッシュボードには、Cyber Protectionサービスに関連する操作の概要を示すカスタマイズ可能なウィジェットが多数用意されています。他のサービスのウィジェットは、将来のリリースで利用可能になります。

ウィジェットは、5分間隔でアップデートされます。ウィジェットには、クリックすることによって、問題を調査し、トラブルシューティングを実行できる要素が含まれています。ダッシュボードの現在の状態は、.pdf または/および .xlsx 形式でダウンロードできる他、電子メールで送信するようにも設定できます。

表、円グラフ、棒グラフ、一覧表、ツリー図として表示されるさまざまなウィジェットから選択できます。同じ種類の複数のウィジェットを異なるフィルタで追加することができます。

[監視] > **[送信する]** にある **[ダウンロード]** ボタンと **[送信]** ボタンは、Cyber Protectionサービスの Standard Editionでは利用できません。



ダッシュボード上のウィジェットを再配置します

名前をクリックしてウィジェットをドラッグアンドドロップします。

ウィジェットを編集します

ウィジェット名の横にある鉛筆アイコンをクリックします。ウィジェットを編集するときには、ウィジェットの名前を変更したり、時間範囲を変更したり、フィルタを設定したり、行をグループ化したりできます。

ウィジェットを追加します

[ウィジェットの追加] をクリックし、次のいずれかの操作を行います。

- 追加するウィジェットをクリックします。ウィジェットはデフォルト設定に追加されます。
- ウィジェットを追加する前に編集するには、ウィジェットが選択されているときに [カスタマイズ] をクリックします。ウィジェットを編集したら、**[完了]** をクリックします。

ウィジェットを削除します

ウィジェット名の横にある X 記号をクリックします。

アクティビティダッシュボード

アクティビティダッシュボードでは、現在と過去のアクティビティの概要が表示されます。デフォルトでは、保持期間は 90 日です。

アクティビティダッシュボードの表示をカスタマイズするには、ギアアイコンをクリックして、表示する列を選択します。

アクティビティの進行状況をリアルタイムで確認するには、**[自動的にリフレッシュ]** チェックボックスを選択します。ただし、複数のアクティビティで更新が頻繁に発生する場合、管理サーバーのパフォーマンスが低下します。

リストにあるアクティビティを以下の条件で検索することができます。

- **デバイス名**
  アクティビティが実行されているそのマシンです。
- **開始者**
  アクティビティを開始したアカウントです。

次のプロパティを使用してアクティビティをフィルタすることもできます。

- **ステータス**
  たとえば、成功、失敗、進行中、キャンセルなどです。
- **種類**
  たとえば、計画の適用、バックアップの削除、ソフトウェアアップデートのインストールなどです。
- **時間**
  たとえば、直近のアクティビティ、過去24時間のアクティビティ、デフォルト保持期間内における特定の期間のアクティビティなどです。

アクティビティの詳細を表示するには、リストからこのアクティビティを選択し、**[アクティビティの詳細]** パネルで **[すべてのプロパティ]** をクリックします。使用可能なプロパティの詳細については、開発者ネットワークポータルのアクティビティおよびタスクAPIのリファレンスを参照してください。

アラートダッシュボード

アラートダッシュボードには、現在のすべてのアラートが表示されます。重大またはエラーアラートがリストアップされます。これらは通常、何らかの理由で正常に完了しなかったバックアップタスクなどに関連しています。

ダッシュボードでアラートをフィルタリングするには

1. [**表示**] ドロップダウンリストから、次の基準のいずれかを選択します。
   - **アラート重大度**
   - **アラートのカテゴリ**
   - **アラートタイプ**
   - **監視タイプ**
   - **日付範囲: ...から...まで**
   - **ワークロード**
   - **計画**
   - **顧客**
2. [**アラートのカテゴリ**] を選択した場合は、[**カテゴリ**] ドロップダウンリストから、表示するアラートのカテゴリを選択します。
3. フィルタリングせずにすべてのアラートを表示したい場合は、[**すべてのアラートタイプ**] をクリックします。

各アラート内で、以下の操作を実行できます:

- [**デバイス**] リンクをクリックして関連するデバイスのアラートにアクセスする。
- アラートの [**トラブルシューティング**] セクションの提案を確認し、それを実行する。
- [**ソリューションを検索**] をクリックして、関連文書とナレッジベース記事にアクセスする。サポートの効果を高めるため、**ソリューションを検索**機能で、リクエストに現在のアラートの詳細を事前入力します。

ダッシュボードでアラートを並べ替えるには

アラートテーブルで、以下の列名の横にある矢印ボタンをクリックします:

- **アラート重大度**
- **アラートタイプ**
- **作成済み**
- **アラートのカテゴリ**
- **ワークロード**
- **計画**

アラートタイプ

アラートは以下のアラートタイプに対して生成されます:

バックアップアラート

警告	説明	アラートを解決する方法
バックアップに失敗しました	バックアップの実行中に解決可能なエラーが発生した場合や、システムのシャットダウンによりバックアップが中断された場合、アラートが生成されます。	失敗したバックアップ操作のログを確認します:ワークロードをクリックして選択し、[**アクティビティ**] をクリックしてから、ログ内の警告を見つけます。メッセージには、ソフトウェアから通知される問題の根本原因が示されています。
バックアップが警告を伴って正常に終了しました。	バックアップが警告を伴い完了した場合、アラートが生成されます。	VMへの変換、レプリケーション、または検証計画のログを確認します。これらの処理中に問題が発生すると、「アクティビティが失敗しました」または「アクティビティが警告を伴い終了しました」というアラートが生成されます。
バックアップがキャンセルされました	ユーザーによってバックアップアクティビティが手動でキャンセルされるたびに、アラートが生成されます。	手動でバックアップを開始するには、[今すぐ実行] をクリックするか、次回にスケジュールされた実行のタイミングまで待機します。
バックアップウィンドウが閉じているため、バックアップがキャンセルされました	バックアップオプションで指定された期間に収まらないことが原因でバックアップアクティビティが実行されなかった場合、アラートが生成されます。	スケジュールを再構成するか、[**パフォーマンスとバックアップ**] ウィンドウで、バックアップ計画のオプションを編集できます。製品のセクションを展開して、指示をご覧ください。
バックアップ待機中です。	このアラートは、スケジューリングの競合が発生し、2件のバックアップタスクが同時に開始される場合に生成されます。この場合、2件目のバックアップタスクは、1件目のタスクが終了するか停止されるまでキューに入れられます。	バックアップが予定時間内にスケジュール通りに実行されていることを確認し、可能な限りスケジューリングの競合を回避します。
バックアップが応答していませ	実行中のバックアップの進行状	この問題はルックアップが原因となって

警告	説明	アラートを解決する方法
ん	況がしばらく表示されず、フリーズの可能性がある場合、アラートが生成されます。	いる場合があります。必要なトラブルシューティング情報を収集するには、こちらの記事の手順を実行してください。
バックアップが開始しませんでした	スケジュール済みのバックアップが原因不明の理由で開始できなかった場合、アラートが生成されます。	Acronis Backup製品の最新ビルドを使用していることを確認してください。 • バックアップ開始時にエージェントマシンが利用可能な場合は、次の手順を実行します: 1. バックアップタスクの開始時間を編集します。 2. それでもアラートが表示される場合は、バックアップタスクを再作成します。 3. 新しく作成したバックアップタスクでもアラートが発生する場合は、アクロニスサポートにお問い合わせください。 • エージェントがオフラインの場合: 1. バックアップ中はマシンの電源を切らないでください。 2. マシンの電源が切られていない場合は、Acronis Managed Machine Serviceが稼働していることを確認してください:[スタート] -> [検索] -> 「services.msc」と入力 -> Acronis Managed Machine Serviceに移動します。サポートが必要な場合は、アクロニスサポートに連絡してください。
バックアップ ステータスが不明です	スケジュール済みのバックアップ時刻にバックアップエージェントがオフラインだった場合、アラートが生成されます。リソース バックアップのステータスは、バックアップ エージェントがオンラインになるまで不明です。	1. エージェントがオフラインになる予定かどうかを確認します（例えば、管理サーバーネットワークの外にあるノートブックの場合）。 2. エージェントがオフラインにならない場合は、Acronis Managed Machine Serviceが実行されていることを確認してください:[スタート] -> [検索] -> 「services.msc」と入力 -> Acronis Managed Machine Serviceに移動して、ステータスを確認します。サービスが停止している場合は、開始します。

警告	説明	アラートを解決する方法
バックアップが見つかりません	（最終バックアップからの日数）日以上バックアップが成功しなかった場合、アラートが生成されます。	
バックアップは破損しています	検証アクティビティが正常に完了し、バックアップの破損が検出されると、アラートが生成されます。	「破損したバックアップに関する問題のトラブルシューティング」の記事に記載されている手順に従ってください。 アーカイブ破損の根本原因の特定にサポートが必要な場合は、アクロニスサポートにお問い合わせください。
継続的データ保護が失敗しました	バックアップの継続的な保護に失敗した場合、アラートが生成されます。	次の制限事項を確認してください: 1. 継続的データ保護は、NTFSファイルシステムと次のオペレーティングシステムでのみサポートされます。 • デスクトップ:Windows 7以降 • サーバー:Windows Server 2008 R2以降 2. CDPでは、保存先として**Acronis Secure Zone**はサポートされていません。 3. WindowsにマウントされているNFSフォルダはサポートされていません。 4. 継続的レプリケーションはサポートされていません: 保護計画に2つのロケーションがある場合、CDPスライスは第一保存先にのみ作成され、変更は次回のバックアップで第二保存先にレプリケートされます。 5. ネットワークソースからローカルの保護対象フォルダ内に変更が適用された場合（ユーザーがネットワークからフォルダにアクセスした場合など）、CDPで変更は検出されません。 6. ファイルが使用されている場合、例えばExcelファイルに何らかの変更が加えられている場合、CDPで変更は検出されません。CDPによって変更が検出されるようにするには、変更を保存してファイルを閉じます。
Hyper-Vホストの構成が無効です	同じホスト名を持つHyper-VホストにHyper-V用のエージェン	このアカウントの異なる子部署の下に、Hyper-V用のこれらのエージェントを登録して、競合を回避する必要があります。

警告	説明	アラートを解決する方法
	トが2つ以上インストールされている場合、アラートが生成されます（同じアカウントレベルではサポートされていない）。	
ベリファイが失敗しました	バックアップの検証プロセスが完了できない場合、アラートが生成されます。	失敗した操作のログを確認します:マシンをクリックして選択し、**[アクティビティ]**をクリックし、ログ内の警告を見つけます。メッセージには、ソフトウェアから通知される問題の根本原因が示されています。
クラウドストレージのバックアップを新しい形式に移行できませんでした	クラウドストレージのバックアップを新しい形式に移行できない場合、アラートが生成されます。	Acronis Cyber Backup Advancedアーカイブのマイグレーションについては、こちらを参照してください。 Acronis Cyber Backupアーカイブのマイグレーションについては、こちらを参照してください。 アクロニスサポートに連絡する前に、migrate_archivesツールを使用して以下のレポートを収集してください: **migrate_archives.exe --account=<Acronisアカウント> --password=<パスワード> --subaccounts=All > report1.txt** **migrate_archives.exe --cmd=finishUpgrade --account=<Acronisアカウント> --password=<パスワード> > report2.txt**
暗号化パスワードが見つかりません。	データベースの暗号化キーが正しくない、破損している、または見つからない場合、アラートが生成されます。	パスワードを失くしたり忘れたりした場合に、暗号化されたバックアップをリカバリする方法はありません。保護対象のデバイスに、ローカルでこの暗号化パスワードを設定する必要があります。保護計画で暗号化パスワードを設定することはできません。詳細については、「暗号化パスワードの設定」を参照してください。
アップロードは保留中です	スケジュール済みの確認で、バックアップ計画によりクラウドアーカイブに転送された物理データがストレージにアップロードされないことが検出され	

警告	説明	アラートを解決する方法
	た場合、アラートが生成されます。	
バックアップの復元に失敗しました	ファイルやシステムバックアップのリカバリを試みた際に復元操作が失敗すると、アラートが生成されます。	バックアップが失敗した正確な日付を特定し、正常な最終バックアップで復元を試みます。

ディザスタリカバリアラート

警告	説明	アラートを解決する方法
ストレージクォータを超過しました	ディザスタリカバリストレージのソフトクォータを超過した場合、アラートが生成されます	クォータを増やすか、クラウドストレージから一部のアーカイブを削除します。
クォータに達しました	以下の場合にアラートが生成されます: • クラウドサーバーのソフトクォータを超過している。 • コンピュートポイントのソフトクォータを超過している。 • パブリックIPアドレスのソフトクォータを超過している。	
ストレージのクォータを超過しています	ディザスタリカバリストレージのハードクォータを超過した場合、アラートが生成されます。 このストレージは、プライマリサーバーと復元サーバーで使用されます。この制限値（クォータ）の追加容量に達した場合、プライマリサーバーとリカバリサーバーの作成や、既存プライマリサーバーのディスクの追加/拡張は実行できなくなります。この制限値（クォータ）の追加容量を超過した場合、フェールオーバーの開始や、停止したサーバーの起動が行えなくなります。実行中のサーバーは引き続き実行されます。	
クォータを超過しています	以下の場合にアラートが生成されます: • クラウドサーバーのハード	デバイスクォータを追加購入するか、保護する必要がなくなったデバイスのバックアップタスクを無効にすること

警告	説明	アラートを解決する方法
	クォータを超過している。 • コンピュートポイントのハードクォータを超過している。 • パブリックIPアドレスのハードクォータを超過している。	を検討してください。
フェールオーバーエラー	フェールオーバー操作が送信された後にシステムで問題が発生した場合、アラートが生成されます。	1. 復元サーバーで **[編集]** をクリックします。詳細については、「復元サーバーの作成」を参照してください。 2. 復元サーバーのCPU/RAMを減少させます。 3. フェールオーバーを再試行します。
フェールオーバーエラーをテスト	テスト操作が送信された後でシステムに問題が発生する場合、アラートが生成されます。	1. 復元サーバーで **[編集]** をクリックします。詳細については、「復元サーバーの作成」を参照してください。 2. 復元サーバーのCPU/RAMを減少させます。 3. フェールオーバーを再試行します。 **注意** 稼働中のネットワークのIPアドレスに、DHCPサーバーの設定と同一のIPアドレスが指定されていることを確認していください。
フェールバック エラー	フェールバックが初期化された後、システムに問題が発生する場合、アラートが生成されます。	バックアップストレージのリストに誤ったロケーションが表示されます: 名前の代わりに数字が表示され（通常、ロケーション名は既存のエンドユーザー名のいずれかと一致する）、このロケーションは作成されていません。誤ったロケーションを削除します: 1. Cyber Protectコンソールで、バックアップストレージに移動します。 2. ロケーションを探し、十字（x）アイコンをクリックして削除します。 3. [削除] をクリックしてこの選択内

警告	説明	アラートを解決する方法
		容を確認します。 4. フェールオーバーを再試行します。
フェールバックがキャンセルされました	ユーザーによりフェールバックがキャンセルされるとアラートが生成されます。	コンソールから手動でアラートを解除します。
VPN接続エラー	ユーザー操作以外の理由でVPN接続に障害が発生した場合、アラートが生成されます。VPNアプライアンスによるステータスのレポートが古くなっています。	Acronis VPNアプライアンスの配置および接続で問題が発生した場合は、アクロニスサポートにお問い合わせください。 以下の情報をEメールで送信してください: • エラーメッセージのスクリーンショット（ある場合） • Acronis VPN アプライアンスのCLIインターフェースのスクリーンショット • Acronis Backup Cloudのデータセンターおよびグループの名前。
（VPNに接続できない）接続ゲートウェイに接続できません	DRサービスから接続ゲートウェイに接続できない場合、アラートが生成されます。接続ゲートウェイによるステータスのレポートが古くなっています。	Acronis VPNアプライアンスの配置および接続で問題が発生した場合は、アクロニスサポートにお問い合わせください。 以下の情報をEメールで送信してください: • エラーメッセージのスクリーンショット（ある場合） • Acronis VPN アプライアンスのCLIインターフェースのスクリーンショット • Acronis Backup Cloudのデータセンターおよびグループの名前
DRのIPの再割り当てが必要	VPNアプライアンスによりネットワークの変更が検出された場合、アラートが生成されます。	IPアドレスが再度割り当てられます。詳細については、「IPアドレスの再割り当て」を参照してください。
接続ゲートウェイの問題	クラウドでVPNサーバーの配置に失敗する場合、アラートが生成されます。	接続検証ツールを使用し、出力にエラーがないかを確認します。 ファイアウォールやマルウェア対策ソフトウェアのアプリケーション制御を

警告	説明	アラートを解決する方法
		通じて、Acronisのソフトウェアを許可します。
プライマリサーバー作成の失敗	エラーによりプライマリサーバーが作成されなかった場合、アラートが生成されます。	
復元サーバー作成の失敗	エラーにより復元サーバーが作成されなかった場合、アラートが生成されます。	復元サーバーがソフトウェア要件に適合していることを確認してください。
プライマリサーバーを削除	プライマリサーバーが削除された場合、アラートが生成されます。	
サーバー復元の失敗	プライマリサーバーまたは復元サーバーをリカバリできなかった場合、アラートが生成されます。	詳細を検索します。エラーメッセージが具体的でないまたは不明瞭（「内部エラー」など）な場合は、**[ディザスタリカバリ]** → **[サーバー]** に移動し、該当するマシンをクリックして選択し、**[アクティビティ]** をクリックします。アクティビティをクリックし、CTRLを押しながらアクティビティを左クリックします。これで、すべてのアクティビティの横に省略記号（...）が表示されるようになります。**[タスクアクティビティ情報]** をクリックして選択します。
バックアップに失敗しました	クラウドサーバー（プライマリまたは本番フェールオーバー状態のサーバー）のバックアップに失敗した場合、アラートが生成されます。	1. バックアップロケーションの接続を検証します。 2. バックアップストレージデバイス（ローカルバックアップ）を確認します。
ネットワーク制限の超過	クラウドネットワークの最大数（5系統のネットワーク）に達する場合、アラートが生成されます。	
ランブックの障害	ランブックが実行できなかった場合、アラートが生成されます。	製品の動作には影響しないため、無視しても差し支えありません。詳細については、「ランブックの作成」を参照してください。
ランブックの警告	ランブックの実行が警告を伴い完了した場合、アラートが生成されます。	製品の動作には影響しないため、無視しても差し支えありません。詳細については、「ランブックの作成」を参照してください。

警告	説明	アラートを解決する方法
ランブックのユーザーインタラクションが必要	ランブックがユーザーインタラクションを待機している場合、アラートが生成されます。	製品の動作には影響しないため、無視しても差し支えありません。詳細については、「ランブックの作成」を参照してください。
インターネットトラフィックのブロック	管理者によりインターネットトラフィックがブロックされた場合、アラートが生成されます。	
インターネットトラフィックのブロック解除	管理者によりインターネットトラフィックのブロックが解除された場合、アラートが生成されます。	
ローカルネットワークの重複	同一な、または重複したローカルネットワークが検出された場合、アラートが生成されます。	
ライセンス切り替えにおけるサーバークォータの不足	クラウドサーバーのクォータが十分でない場合、アラートが生成されます。	• テナントおよびユーザーに、物理サーバー用のWebホスティングサーバークォータまたはサーバークォータがあることを確認してください。 • テナントおよびユーザーに、仮想サーバー用のWebホスティングサーバークォータまたは仮想マシンクォータがあることを確認してください。仮想サーバーでは、サーバクォータは使用できません。
ライセンス切り替えにおける提供項目の不適合	ディザスタリカバリストレージの提供項目が無効になっている場合、アラートが生成されます。	詳細については、ディザスタリカバリクォータを参照してください。
ライセンス切り替えエラー	ディザスタリカバリのアップグレードでエラーが発生した場合、アラートが生成されます。	
ライセンス切り替えにおけるコンピュートポイントの不足	利用可能なコンピュートポイントが存在しない場合、アラートが生成されます。	管理ポータルで、コンピュートポイントのハードクォータを確認して増加させます。
ライセンス切り替えにおけるサーバー提供項目の不適合	クラウドサーバーの提供項目が無効になっている場合、アラートが生成されます。	
ポリシーで問題が発生し復元サーバーを作成できない	ディザスタリカバリインフラストラクチャのセットアップ中にエ	インターネットアクセスプロパティを含まない復元サーバーを手動で作成し

警告	説明	アラートを解決する方法
	ラーが発生した場合、アラートが生成されます。	ます。詳細については、「復元サーバーの作成」を参照してください
バックアッププロセッサの自動テストフェールオーバーが再スケジュール済み	自動テストフェールオーバーの実行が再スケジュールされた場合、アラートが生成されます。	
バックアッププロセッサの自動テストフェールオーバーがタイムアウトに到達	自動テストフェールオーバーの処理がタイムアウトした場合、アラートが生成されます。 **注意** 自動テストフェールオーバーが実行されるたびに、チャージ可能なコンピュートポイントが消費されます。	
バックアッププロセッサの自動テストフェールオーバーの全般的な問題	直近にスケジュールされた、復元サーバーの自動テストフェールオーバーを実行できなかった場合、アラートが生成されます。	1. 復元サーバーのテストフェールオーバーを手動で開始します。詳細については、「テストフェールオーバーの実行」を参照してください。 2. 自動テストフェールオーバーが実行される次回のスケジュール日まで待機する
フェールバックデータ転送エラー	フェールバックのデータ転送に失敗した場合、アラートが生成されます。	
フェールバックの失敗	フェールバックでエラーが発生した場合、アラートが生成されます。	バックアップストレージのリストに誤ったロケーションが表示されます: 名前の代わりに数字が表示され（通常、ロケーション名は既存のエンドユーザー名のいずれかと一致する）、このロケーションは作成されていません。誤ったロケーションを削除します: 1. Cyber Protectionで、バックアップストレージに移動します。 2. ロケーションを探し、十字（x）アイコンをクリックして削除します。 3. **[削除]** をクリックしてこの選択内容を確認します。 フェールオーバーを再試行します。

警告	説明	アラートを解決する方法
フェールバック確認の失敗	フェールバックの確認が失敗した場合、アラートが生成されます。	
フェールバックマシンのスイッチオーバーの準備完了	マシンのスイッチオーバーの準備が整っている場合、アラートが生成されます。	
フェールバックのスイッチオーバーの完了	スイッチオーバーが正常に完了した場合、アラートが生成されます。	コンソールから手動でアラートを解除します。
フェールバックのターゲットエージェントのオフライン	エージェントがオフラインの場合、アラートが生成されます。	

マルウェア対策保護アラート

警告	説明	アラートを解決する方法
不審なリモート接続アクティビティが検出されました	リモート接続からランサムウェアが検出された場合、アラートが生成されます。	コンソールから手動でアラートを解除します。
不審なアクティビティが検出されました	ワークロードでランサムウェアが検出された場合、アラートが生成されます。	コンソールから手動でアラートを解除します。でアラートのアクティベートを解除します。 Active Protection計画で指定したオプションに応じて、悪意のあるプロセスが停止され、プロセスによって行われた変更が元に戻される場合があります。また操作が未実行のため、この問題を手動で解決しなければならない場合もあります。 どのプロセスがファイルを暗号化しているのか、どのファイルが影響を受けているのかについて、アラートの詳細を確認してください。 ファイルを暗号化するプロセスが許可されていると判断した場合（偽陽性アラート）、このプロセスを信頼できるプロセスに追加します: 1. Active Protection計画を開きます。 2. **[編集]** をクリックして、設定を変更します。 3. **[信頼できるプロセス]** で、ランサムウェアと見なされない信頼済みプロセスを指定します。実行可能なプロセスのフルパスを、ドライブ文字を先頭にして指定します。 例:C:¥Windows¥Temp¥er76s7sdkh.exe。
クリプトマイニングアクティビティが検	ワークロードで悪意のあるクリプトマイナーが検出された	コンソールから手動でアラートを解除します。

警告	説明	アラートを解決する方法
出されました	場合、アラートが生成されます	
MBR の防御:不審なアクティビティが検出され、一時停止されました	ワークロードでランサムウェアが検出された場合（具体的には、MBR/GPTパーティションがランサムウェアによって変更されている場合）、アラートが生成されます。	コンソールから手動でアラートを解除します。
サポートされていないネットワークパスが指定されています	管理者によって提供された復元パスがローカルフォルダパスでない場合、アラートが生成されます。	ネットワークフォルダ保護用のローカルパス（復元パス）を指定します。コンソールから手動でアラートを解除する
Active Protection計画に有害な重要プロセスが追加されます	重要なプロセスが、保護除外リストでブロック対象プロセスとして追加されると、アラートが生成されます。	コンソールから手動でアラートを解除します。
Active Protectionポリシーを適用できませんでした	Active Protectionポリシーの適用に失敗した場合、アラートが生成されます。	エラーメッセージを確認して、Active Protectionポリシーを適用できない理由を確認します。
セキュアゾーン:権限のない処理を検出しブロックしました	ワークロードでランサムウェアが検出された場合（ASZパーティションがランサムウェアによって変更されている場合）、アラートが生成されます。	コンソールから手動でアラートを解除します。
Active Protectionサービスが実行されていません	Active Protectionサービスがクラッシュしているか、実行されていない場合、アラートが生成されます。	エラーメッセージを確認して、Active Protectionサービスが実行されていない理由を確認します。
Active Protectionサービス使用不可	ドライバに互換性がないか、ドライバが存在しないため、Active Protectionサービスを使用できない場合、アラートが生成されます。	Windowsのイベントログで、Acronis Active Protectionサービス（acronis_protection_service.exe）がクラッシュしていないかどうかを確認してください。
別のセキュリティソリューションとの競合	別のセキュリティソリューションとの競合の検出により、マシン「{{resourceName}}」でActive Protectionが利用できない場合、アラートが生成され	**解決策1**:Acronisのリアルタイム保護を使用する場合は、マシンでサードパーティ製のウイルス対策をアンインストールしてください。 **解決策2**:サードパーティ製のウイルス対策を使用したい場合は、保護計画のAcronisリアルタイム保護、URLフィルタリング、Windows Defenderウイ

警告	説明	アラートを解決する方法
	ますActive Protection を有効化するには、競合するセキュリティソリューションを無効化するかアンインストールしてください。	ルス対策を無効にしてください。
検疫アクションが失敗しました	検出されたマルウェアがマルウェア対策により隔離されなかった場合、アラートが生成されます。	エラーメッセージで、隔離が失敗した理由を確認します。
不審なプロセスの検出	振る舞い検知エンジンによってマルウェア（プロセスタイプ）が検出された場合、アラートが生成されます。検出されたマルウェアは隔離されます。	コンソールから手動でアラートを解除します。
不審なプロセスの検出（ただし隔離なし）	振る舞い検知エンジンによってマルウェア（プロセスタイプ）が検出された場合、アラートが生成されます。検出されたマルウェアは隔離されません。	コンソールから手動でアラートを解除します。
マルウェアを検出しブロックしました（ODS）	スケジュール済みスキャンによってマルウェアが検出された場合、アラートが生成されます。検出されたマルウェアは隔離されます。	コンソールから手動でアラートを解除します。
マルウェアを検出しブロックしました（RTP）	リアルタイム保護によってマルウェアが検出された場合、アラートが生成されます。検出されたマルウェアは隔離されます。	コンソールから手動でアラートを解除します。
バックアップでマルウェアが検出されました	バックアップスキャン中にマルウェアが検出された場合、アラートが生成されます。	コンソールから手動でアラートを解除します。
リアルタイムマルウェア対策保護とセキュリティ製品の間で競合が検出されました	Windowsセキュリティセンターでマルウェア対策を登録できなかった場合、アラートが生成されます。	サードパーティのセキュリティ製品を無効化/アンインストールするか、保護計画のリアルタイムマルウェア対策保護を無効にします。
Microsoft Security	Microsoft Security Essentials	エラーメッセージで、Microsoft Security

警告	説明	アラートを解決する方法
Essentials モジュールを実行できませんでした	モジュールの実行に失敗した場合、アラートが生成されます。	Essentialsモジュールの実行に失敗した理由を確認します。
サードパーティ製のウイルス対策ソフトウェアがインストールされているため、リアルタイム保護が利用できません	サードパーティのウイルス対策でリアルタイム保護が有効になっているために、リアルタイム保護をオンにできなかった場合、アラートが生成されます。	サードパーティのセキュリティ製品を無効化/アンインストールするか、保護計画のリアルタイムマルウェア対策保護を無効にします。
ドライバに互換性がないか、ドライバが存在しないため、リアルタイム保護を使用できません	ドライバに互換性がないか、ドライバが存在しないため、リアルタイム保護を使用できない場合、アラートが生成されます。	エラーメッセージで、Acronisがワークロードでドライバのインストールに失敗した理由を確認します。
サイバープロテクション（またはActive Protection）サービスの応答がありません	コンソールからのヘルスチェックpingに対して、サイバープロテクションサービスからの応答があった場合、アラートが生成されます。	コンソールから手動でアラートを解除します。
セキュリティ定義のアップデートに失敗しました	セキュリティ定義のアップデートに失敗した場合、アラートが生成されます。	エラーメッセージで、セキュリティ定義のアップデートが失敗した理由を確認します。
Tamper Protectionが有効化済み	Tamper Protectionが有効になっているため、Microsoft Defenderの設定を変更できない場合、アラートが生成されます。	WindowsワークロードのTamper Protection設定を無効化します。
Windows Defenderのモジュールの実行に失敗しました	Windows Defenderモジュールの実行に失敗した場合、アラートが生成されます。	エラーメッセージで、Windows Defenderモジュールの実行に失敗した理由を確認します。
Windows Defenderは、サードパーティのウイルス対策ソフトウェアによってブロックされました	サードパーティのウイルス対策がマシンにインストールされているため、Windows Defenderがブロックされている場合、アラートが生成されます。	サードパーティのセキュリティ製品を無効化またはアンインストールします。
グループポリシーの競合	Microsoft Defenderがグループポリシーで制御されているため、設定を変更できない場合、アラートが生成されま	Windowsワークロードのグループポリシー設定を無効化します。

警告	説明	アラートを解決する方法
	す。	
Microsoft Security Essentialsにより、マシンをマルウェアから保護するための操作が行われました	Microsoft Security Essentialによりマルウェアが削除/隔離された場合、アラートが生成されます。	コンソールから手動でアラートを解除します。
Microsoft Security Essentialsによりマルウェアが検出されました	Microsoft Security Essentialsにより、マルウェアもしくはその他の望ましくないソフトウェアが検出された場合、アラートが生成されます。	コンソールから手動でアラートを解除します。

ライセンスアラート

警告	説明	アラートを解決する方法
まもなくストレージのクォータに達します	使用率が80%以下になった場合（クリーンアップまたはクォータのアップグレード後）、アラートが生成されます。	追加のストレージを購入するか、クラウドストレージの空き領域を確保することを検討してください。
ストレージのクォータを超過しました	ストレージクォータの利用率が100%に達した場合、アラートが生成されます。	追加のストレージスペースを購入してください。詳細については、「追加のクラウドストレージを購入する」を参照してください。
ワークロードのクォータに到達	提供項目の使用量が0より大きく、クォータ制限を超過しているものの、クォータ制限と追加容量の合計以下である場合、アラートが生成されます。	
ワークロードのクォータを超過	提供項目の使用量がクォータと追加容量の合計を上回っている場合、アラートが生成されます。	
ワークロードに、バックアップ計画を適用するためのクォータがありません（リソースにサービスクォータがない）	以下の場合にアラートが生成されます: • クォータは手動で削除されました: **[デバイス]** > **[詳細]** > **[サービスクォータ]** に移動し、**[変更]** をクリックしてから、**[クォータなし]** オプションを選択します。 • 管理コンソールの提供項目が無効	

警告	説明	アラートを解決する方法
	化されています。 • 管理コンソールの提供項目で、クォータと追加容量の合計値が、現在の使用量を下回りました。	
割り当てられたクォータがあるワークロードを保護できません	提供項目が条件を満たしておらず、以下が必要な場合、アラートが生成されます。 • ダイナミックグループ。 • グループに割り当てられたバックアップ計画。 • ダイナミックグループに該当するリソースを追加する（同じバックアップ計画を適用できない何らかの特性を持つリソースを含む）。	
サブスクリプションライセンスの期限切れです	ライセンス/メンテナンス期限に関する日次チェックでライセンスサーバーに問い合わせを行い、ライセンスの期限が切れているという応答があった場合、アラートが生成されます。	サブスクリプションの有効期限が切れると、追加のサブスクリプションの更新まで、復元を除くすべての製品機能がブロックされます。バックアップされたデータには、復元のために引き続きアクセスできます。新しいライセンスを購入します。 **注意** 新しいサブスクリプションを購入したにもかかわらず、引き続きサブスクリプションの有効期限が切れているというメッセージが表示される場合は、アクロニスアカウントから新しいサブスクリプションをインポートする必要があります。管理コンソールで、[設定] -> [ライセンス] に進み、右上隅にある [同期] をクリックします。サブスクリプションは自動的には同期されません。
サブスクリプションライセンスの有効期間がまもなく終了します	ライセンス/メンテナンス期限に関する日次チェックでライセンスサーバーに問い合わせを行い、ライセンスの期限が30日以内に切れるという応答があった場合、アラートが生成されます。	新しいサブスクリプションの購入を検討します。

URLフィルタ処理アラート

警告	説明	アラートを解決する方法
悪意のあるURLがブロックされました	URLフィルタリングによって悪意のあるURLがブロックされる場合、アラートが生成されます。	URLフィルタリングの設定を確認します。URLフィルタリングにより、URLフィルタ処理設定でブロック対象とされているページがブロックされています。
悪意のあるURLの警告が無視されました	URLフィルタリングで悪意のあるURLをブロックすることを選択した場合、アラートが生成されます。	URLフィルタリングの設定を確認します。
URLフィルタリングとセキュリティ製品の間で競合が検出されました	他のセキュリティ製品との競合により、URLフィルタリングを有効にすることができない場合、アラートが生成されます。	URLフィルタリングの設定を確認します。
Web サイト URL がブロックされました	URLフィルタリングのブロック対象カテゴリに指定されたすべての基準を満たすURLがある場合、アラートが生成されます。	URLフィルタリングの設定を確認します。

EDRアラート

警告	説明	アラートを解決する方法
インシデントの検出	インシデントが作成されたり、既存のインシデントのステータスがアップデートされたりした場合、アラートが生成されます。	このアラートにより、新しいインシデントが発生したことや古いインシデントがアップデートされたことを通知します。アラートを表示し、閉じることができます。必要に応じ、詳細な調査のためにインシデントを開くこともできます。
IOC（Indicators of Compromise）の検出	新しいIndicators of Compromise（IOC）がEDR IOC脅威検索サービスによって検出された場合、アラートが生成されます。	このアラートにより、1つまたは複数のワークロードでIOCが検出されたことを通知します。アラートを表示してからアラート内のリンクをクリックして、IOCの詳細を表示できます。
ネットワークからワークロードを分離できませんでした	ユーザーがマシンをネットワークから分離する操作をトリガーし、分離操作が失敗した場合に、アラートが	必要な操作を実行します。

警告	説明	アラートを解決する方法
	生成されます。	
ワークロードをネットワークに再接続できませんでした	ユーザーがマシンをネットワークに再接続する操作をトリガーし、操作が失敗した場合に、アラートが生成されます。	必要な操作を実行します。
Windows Defenderのファイアウォール設定が変更されました	分離されたマシンのファイアウォール設定が変更された場合、アラートが生成されます。	このアラートにより、分離されたマシンのファイアウォールの詳細が変更されたことを通知します。このアラートは情報提供のみであり、参照後にアラートを閉じることができます。

デバイス制御アラート

警告	説明	アラートを解決する方法
デバイス制御とデータ損失防止は、限定された機能で実行されます（CPUの非互換性が検出されました）。	CETテクノロジーに対応したCPUを持つ物理マシンでDeviceLockエージェントが起動した場合、アラートが生成されます。	影響を受けるマシンでオプションを無効にして、アラートを回避してください。
macOS Venturaでは、デバイス制御機能はまだサポートされていません。	DeviceLockエージェントが物理的なmacOS Venturaマシンで開始され、デバイス制御を伴う保護計画がエージェントに適用された場合、アラートが生成されます。DeviceLockドライバに起因するカーネルパニックの問題があるバージョンにのみ、適用されます。	
転送を許可された機密データ	機密コンテンツの転送が許可されている場合、アラートが生成されます。	
正当に転送された機密データ	機密コンテンツの転送が正当化されている場合、アラートが生成されます。	
転送を拒否された機密データ	機密コンテンツの転送がブロックされている場合、アラートが生成されます。	
データ漏洩防止の観察モードの結果を確認する	観察の結果を確認するタイミングで、アラートが生成されます: • Advanced DLP Packのライセンスが適用されていません。 • 少なくとも1つのワークロードに適	

警告	説明	アラートを解決する方法
	用された保護計画で観察モードが有効化されてから1ヵ月が経過しました。 • 前回に同様のアラートが発生してから1ヵ月が経過し、観察モードでのDLPを使用したことが検出されました。	
ユーザーのセキュリティ識別子が変更された	既知のユーザー名のSIDがアップデートされた場合、アラートが生成されます。これは、ドメイン外部のPCにOSを再インストールした場合に発生する場合があります。	
周辺デバイスへのアクセスがブロックされました。	サポートされているデバイスの一部の操作（読み取り/書き込み操作）がブロックされた場合に、アラートが生成されます。	
リモートSSLリソースに接続できません。	リモートSSLリソースへのアクセスが、そのリソースで使用されている追加のハンドシェイク防止機能によってブロックされた場合、アラートが生成されます。	リソースをリモートホストの許可リストに追加します。

システムアラート

警告	説明	アラートを解決する方法
エージェントは古くなっています	エージェントのバージョンが古い場合、アラートが生成されます。	エージェントリストに移動して、エージェントのアップデートを開始します。
自動アップデートの失敗	エージェントの自動アップデートが失敗した場合、アラートが生成されます。	手動アップデートを試行してください。
新しいエージェントをインストールした後、デバイスを再起動する必要があります	リモートインストールが成功した後に再起動が必要な場合、アラートが生成されます。	ワークロードを再起動します。
アクティビティが失敗しました	アクティビティが失敗した場合、アラートが生成されます。	マシン上のすべてのAcronisサービスを再起動します。
アクティビティが警告を伴って正常に終了しました。	アクティビティは成功しているものの、何らかの警告が発生した場合、アラートが生成されます。	

警告	説明	アラートを解決する方法
アクティビティが応答していません	アクティビティの実行中に応答がなくなった場合、アラートが生成されます。	
計画の配置に失敗しました	保護計画の配置が失敗した場合、アラートが生成されます。	
ユーザー名の SID への変換に失敗しました	スケジュールSIDの変換に失敗した場合、アラートが生成されます。	

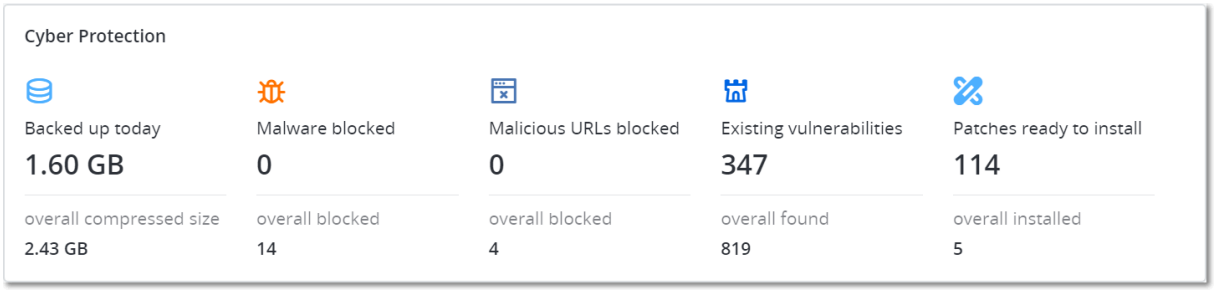
アラートウィジェット

アラートウィジェットでは、ワークロードに関連するアラートについて以下の情報を確認できます。

フィールド	説明
直近5件のアラートウィジェット	直近5件のアラートのリストです。
アラート概要履歴	アラートの重大度、アラートの種類、時間範囲ごとにアラートを表示するグラフィカルなウィジェットです。
アクティブアラート概要	アラートの重大度やアラートの種類ごとにアクティブアラートを表示し、その合計数を表示するグラフィカルなウィジェットです。
アラート履歴	過去のアラートを表形式で表示します。
アクティブアラートの詳細	アクティブアラートを表形式で表示します。

サイバープロテクション

このウィジェットは、バックアップのサイズ、ブロックされたマルウェア、ブロックされたURL、検出された脆弱性、インストールされているパッチに関する全体的な情報を示します。



上側の行では、以下の現在の統計情報を表示します。

- **本日実行済みのバックアップ** - 過去24時間の復元ポイントのサイズの合計
- **ブロックされたマルウェア** - ブロックされたマルウェアに関する現在有効なアラートの数
- **ブロックされたURL** - ブロックされたURLに関する現在有効なアラートの数

- **既存の脆弱性** - 現時点で存在する脆弱性の数
- **インストール可能なパッチ** - 現在インストール可能なパッチの数

下側の行では、以下の全体的な統計情報を表示します。

- すべてのバックアップの圧縮サイズ
- マシン全体でブロックされたマルウェアの合計数
- マシン全体でブロックされたURLの合計数
- マシン全体で検出された脆弱性の合計数
- マシン全体でインストールされたアップデート/パッチの合計数

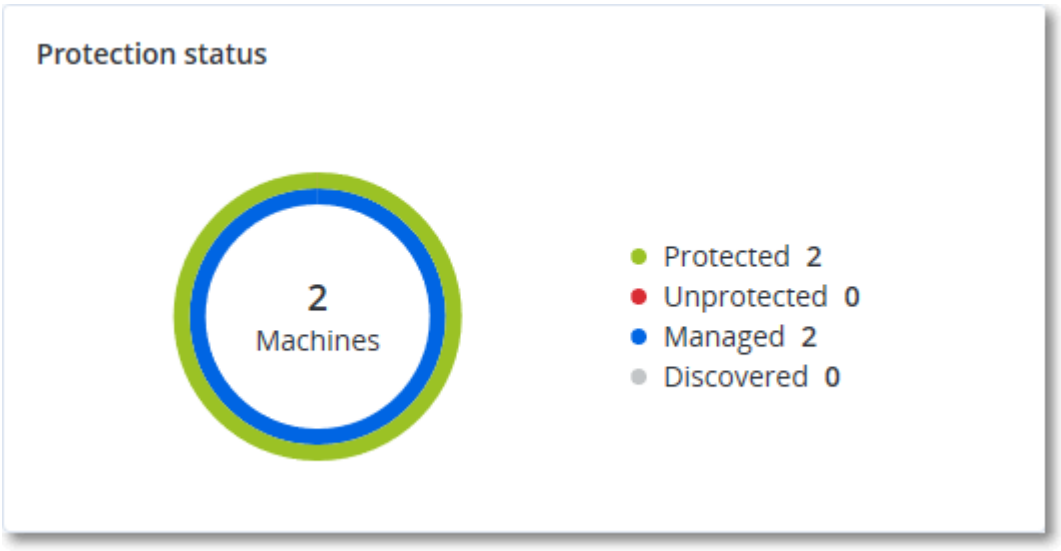
保護ステータス

このウィジェットはすべてのマシンについて現在の保護ステータスを表示します。

マシンは次のいずれかのステータスになります。

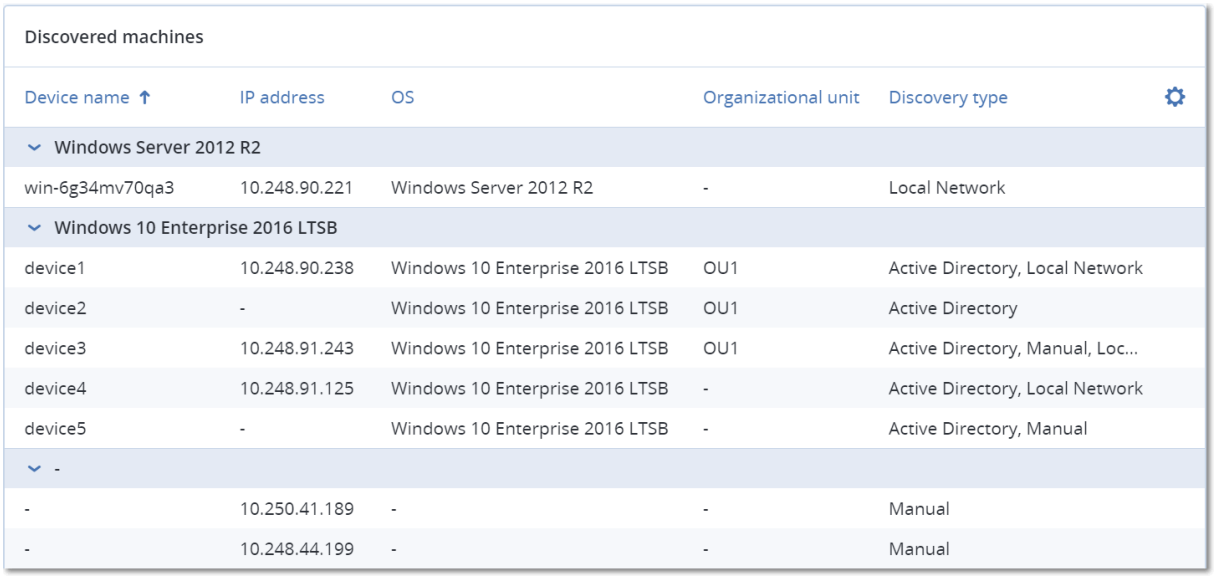
- **保護対象** - 保護計画が適用されているマシン。
- **保護対象外** - 保護計画が適用されていないマシン。これらには、保護計画が適用されていない検出済みマシンと管理対象のマシンの両方が含まれます。
- **管理対象** - プロテクションエージェントをインストール済みのマシン。
- **検出済み** - プロテクションエージェントを未インストールのマシン。

マシンのステータスをクリックすると、ステータスの詳細情報を含むマシンのリストにリダイレクトされます。



検出されたマシン

このウィジェットには指定された時間内に検出されたマシンのリストが表示されます。



Discovered machines

Device name	IP address	OS	Organizational unit	Discovery type
Windows Server 2012 R2				
win-6g34mv70qa3	10.248.90.221	Windows Server 2012 R2	-	Local Network
Windows 10 Enterprise 2016 LTSB				
device1	10.248.90.238	Windows 10 Enterprise 2016 LTSB	OU1	Active Directory, Local Network
device2	-	Windows 10 Enterprise 2016 LTSB	OU1	Active Directory
device3	10.248.91.243	Windows 10 Enterprise 2016 LTSB	OU1	Active Directory, Manual, Loc...
device4	10.248.91.125	Windows 10 Enterprise 2016 LTSB	-	Active Directory, Local Network
device5	-	Windows 10 Enterprise 2016 LTSB	-	Active Directory, Manual
-				
-	10.250.41.189	-	-	Manual
-	10.248.44.199	-	-	Manual

エンドポイント検知と応答（EDR）ウィジェット

エンドポイント検知と応答（EDR）には7種類のウィジェットがあり、これらはすべて **[概要]** ダッシュボードからアクセスできます。これらのウィジェットのうち3種類は、EDR機能内にデフォルトで表示されています（"インシデントを確認する"（874ページ）を参照）。

次の7種類のウィジェットが利用可能です。

- ワークロードごとの上位インシデントディストリビューション
- 脅威のステータス（EDRに表示）
- インシデント重大度の履歴（EDRに表示）
- セキュリティインシデントのMTTR
- セキュリティインシデントのバーンダウン
- タクティクス別の検出（EDRに表示）
- ワークロードのネットワークステータス

ワークロードごとの上位インシデントディストリビューション

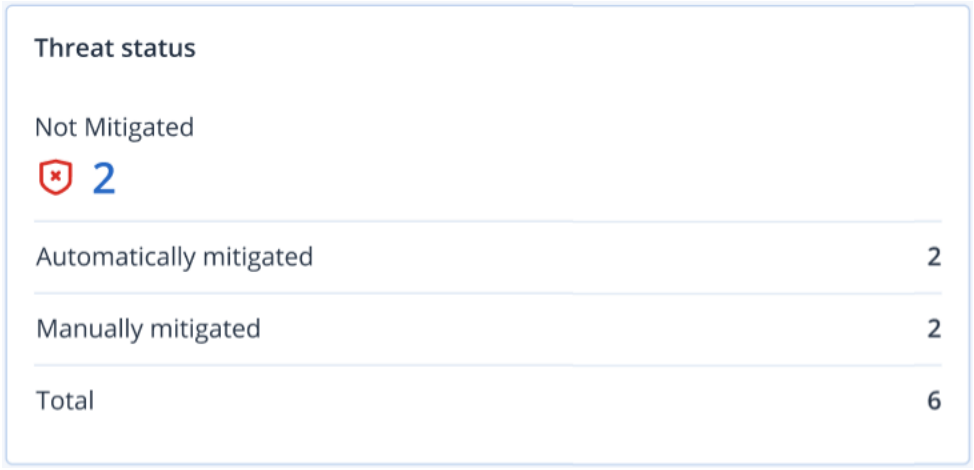
このウィジェットには、インシデントの数が多い、上位5つのワークロードが表示されます（**[すべて表示]** をクリックすると、ウィジェットの設定に応じてフィルタリングされたインシデントのリストにリダイレクトされます）。

ワークロード行にホバーすると、インシデントに関する現在の調査ステータスの内訳が表示されます。調査ステータスは、**開始前**、**調査中**、**閉鎖済み**、**偽陽性**の順に表示されます。続いて、詳細に分析したいワークロードをクリックすると、ウィジェットの設定に応じてインシデントのリストがリフレッシュされます。

脅威のステータス

このウィジェットでは、すべてのワークロードに存在する現在の脅威のステータスが表示されます。また、現時点で脅威が軽減されておらず、調査が必要なインシデントの数が強調表示されます。ウィジェットにはさらに、（手動で、またはシステムにより自動で）軽減措置が適用されたインシデントの数も表示されます。

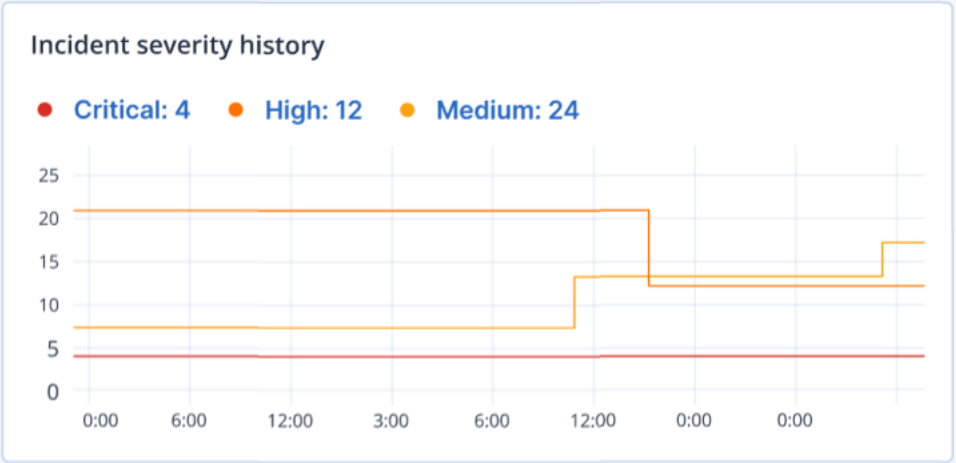
軽減されていないインシデントを表示するため、フィルタリングされたインシデントリストを表示するには、**[軽減されていない]** の数字をクリックします。



インシデント重大度の履歴

このウィジェットでは、攻撃の進展が重大度ごとに表示されるので、関連した一連の攻撃を表示するのに役立ちます。スパイクが存在する場合、組織への攻撃が進行中であることを示している可能性があります。

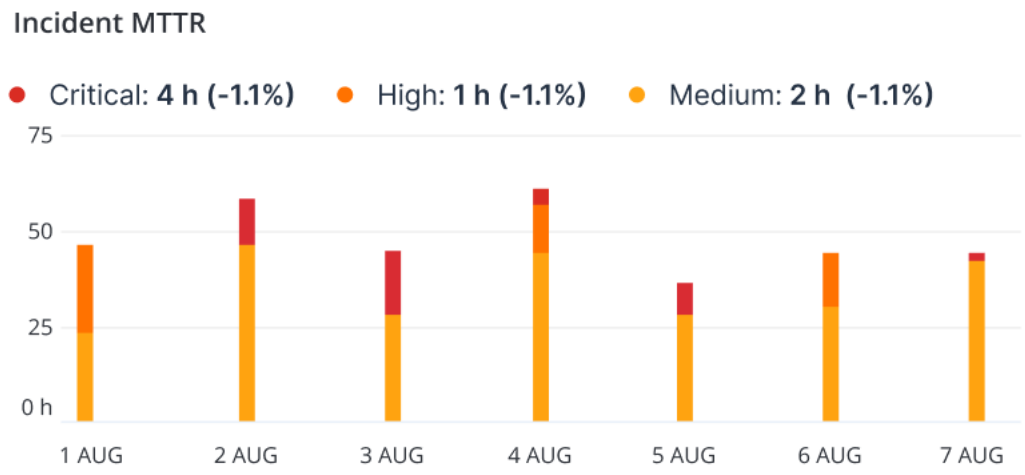
グラフにカーソルをホバーすると、過去24時間（デフォルト期間）における特定時点のインシデント履歴の内訳が表示されます。関連するインシデントのリストを表示するには、重大度レベル（**重大**、**高**、**中**）をクリックします。選択した重大度レベルに一致するインシデントでフィルタリング済みのインシデントリストにリダイレクトされます。



セキュリティインシデントのMTTR

このウィジェットでは、セキュリティインシデントの平均解決時間を表示します。これは、インシデントの調査や解決のスピードを示しています。

列をクリックすると、重要度（**重大**、**高**、**中**）別のインシデントの内訳と、重要度レベル別の解決に要した時間が表示されます。括弧内の%数値により、前期比での増減が表わされます。

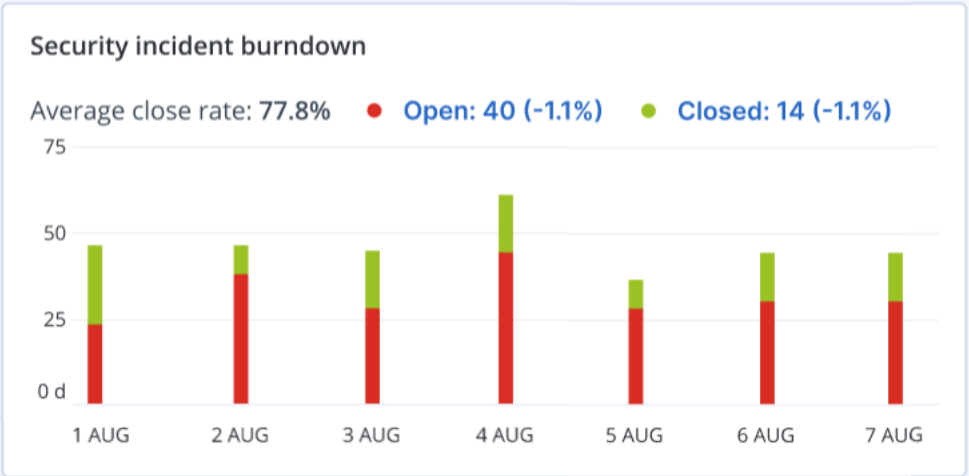


セキュリティインシデントのバーンダウン

このウィジェットでは、インシデントがクローズ状態になるまでの効率性が表示されます。この効率性は、オープン状態のインシデントの数と、一定期間内にクローズされたインシデントの数の比較により表わされます。

列をホバーすると、選択した日付におけるクローズ状態およびオープン状態のインシデントの内訳が表示されます。[オープン] の値をクリックすると、現在オープンな状態のインシデント（**調査中**または**開始前**ステータス）を表示するフィルタが適用されたインシデントリストが表示されます。[クローズ] の値をクリックすると、現在オープンな状態ではないインシデント（**閉鎖済み**または**偽陽性**のステータス）を表示するフィルタが適用されたインシデントリストが表示されます。

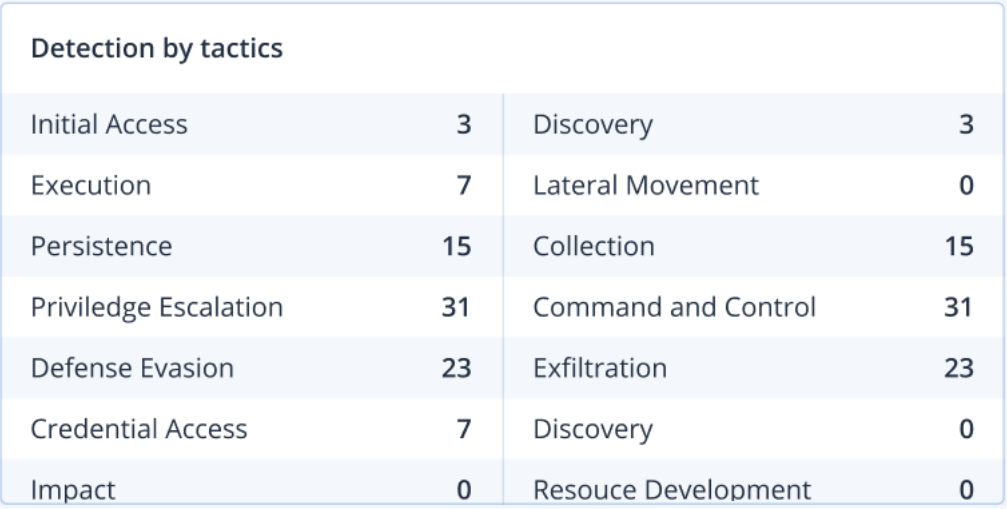
括弧内の%数値により、前期比での増減が表わされます。



タクティクスによる検出

このウィジェットでは、選択した期間中のインシデントで特定の攻撃手法が発見された回数が表示されます。

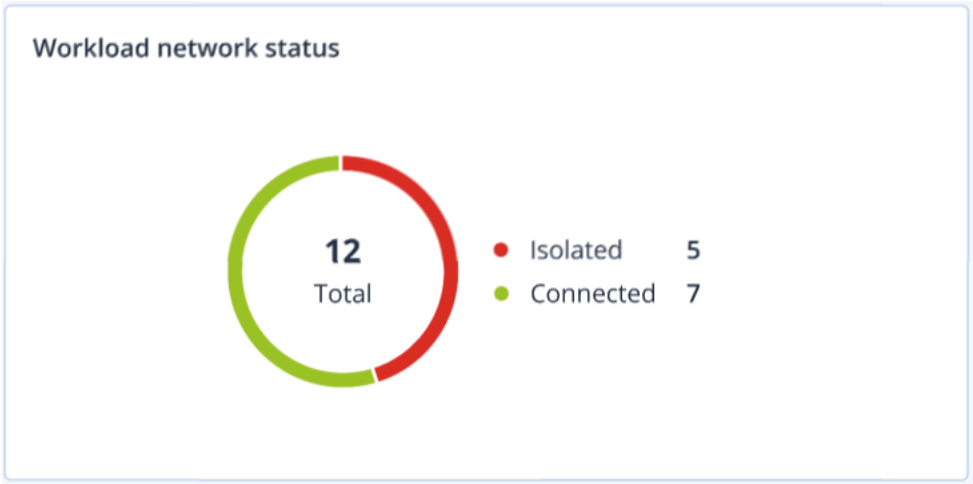
前の期間より増加している場合は緑色の数値で、減少している場合は赤色の数値で表示されます。以下の例では、特権昇格およびコマンドと制御攻撃が前の期間より増加しています。これは、資格情報管理の分析とセキュリティの強化が必要であることを示唆しています。



ワークロードのネットワークステータス

このウィジェットでは、ワークロードの現在のネットワーク状態が表示され、分離されているワークロードの数と接続済みのワークロードの数が示されます。

[分離済み] の値をクリックすると、エージェントリストを含むワークロード（コンソールの**[ワークロード]** メニュー以下）が表示されます。このリストには、分離済みのワークロードを表示するフィルタが適用されています。[接続済み] の値をクリックすると、接続済みのワークロードを表示するフィルタが適用されたエージェントリストとワークロードが表示されます。



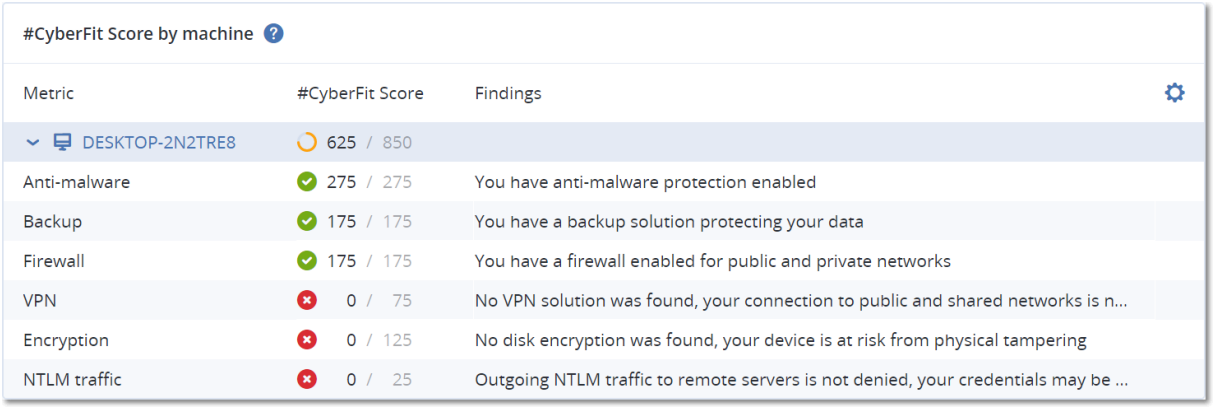
マシンごとの #CyberFit スコア

このウィジェットは、各マシンの合計#CyberFitスコア、その複合スコア、および次の各メトリクスに関する評価結果を示します。

- マルウェア対策
- バックアップ
- ファイアウォール
- VPN
- 暗号化
- NTLMトラフィック

各メトリクスのスコアを改善するには、レポートに記載された推奨事項を確認します。

#CyberFitスコアの詳細については、「マシンの#CyberFitスコア」を参照してください。



ディスク状態監視

ディスク状態の監視は、現在のディスク状態のステータスに関する情報と予測情報を提供し、ディスク障害に関連して発生する可能性のあるデータ損失を防ぐことができます。HDDおよびSSDディスクがサポートされています。

制限事項

- ディスク状態の予測はWindowsを実行するマシンのみをサポートします。
- 物理マシンのディスクのみを監視します。仮想マシンのディスクは監視対象ではなく、ディスク状態ウィジェットに表示されません。
- RAID構成はサポートされていません。ディスク状態ウィジェットには、RAIDが実装されたマシンに関する情報は含まれていません。
- NVMe SSDはサポートされていません。

ディスク状態は、次のいずれかのステータスで示されます。

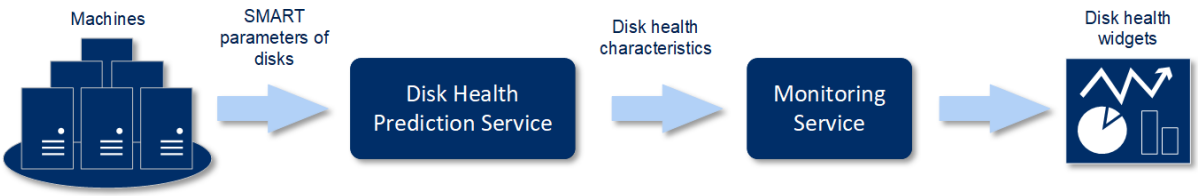
- **OK**
  ディスク状態が70～100%です。
- **警告**
  ディスク状態が30～70%です。
- **重大**
  ディスク状態が0～30%です。
- **ディスクデータの計算中**
  現在のディスク状態と予測を計算中です。

仕組み

ディスク状態予測サービスは、AI ベースの予測モデルです。

1. プロテクションエージェントがディスクのSMARTパラメータを収集して、このデータをディスク状態予測サービスに渡します。
   - SMART 5 - リアロケートされたセクタの数です。
   - SMART 9 - 通電時間です。
   - SMART 187 - 報告された未修正エラーです。
   - SMART 188 - コマンドタイムアウトです。
   - SMART 197 - 現在保留されているセクタの数です。
   - SMART 198 - オフラインの未修正セクタの数です。
   - SMART 200 - 書き込みエラー発生率です。
2. ディスク状態予測サービスは、受信したSMARTパラメータを処理して予測を実行し、次のようにディスク状態の特性を提供します:
   - ディスク状態の現在のステータス:OK、警告、重大。
   - ディスク状態の予測: 陰性、安定、陽性。
   - ディスク状態の予測は百分率で示されます。

   予測期間は1か月間です。
3. 監視サービスはこれらの特性情報を受信し、Cyber Protectコンソールのディスク状態ウィジェットに関連情報を表示します。



ディスク状態ウィジェット

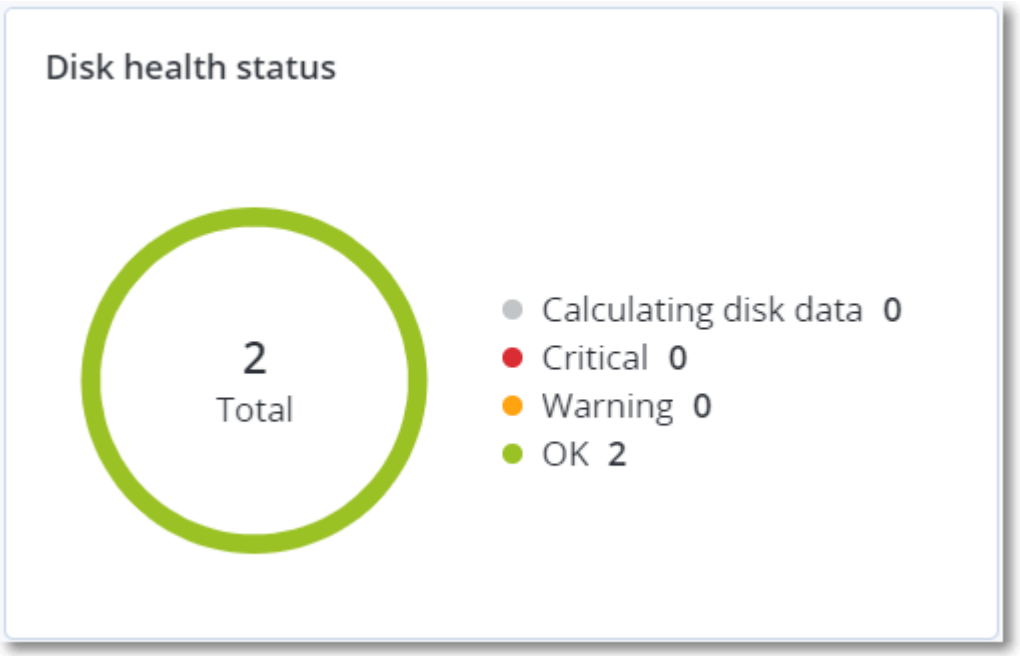
ディスク状態の監視結果は、Cyber Protectコンソールで利用できる以下のウィジェットに表示されます。

- **ディスク状態の概要**は、階層の詳細情報を含むツリー図ウィジェットです。階層は、ツリーをたどるようにして切り替えることができます。
  - マシンレベル
    選択したカスタマーのマシンに関する、ディスク状態ステータスの要約情報を表示します。最も重大なディスクステータスのみが表示されます。他のステータスは、該当するブロックにマウスを移動（ホバー）することでツールの先端に表示されます。マシンのブロックサイズは、該当するマシンの全ディスクの合計サイズによって異なります。マシンのブロックの色は、見つかったもっとも重大なディスクステータスによって異なります。

- ディスクレベル
  選択済みのマシンに現在搭載されている全ディスクのディスク状態ステータスを表示します。各ディスクブロックには、以下のいずれかのディスク状態予測とその確率がパーセンテージで表示されます。
  - 低下傾向
  - 安定傾向

- 改善傾向

- **ディスク状態ステータス**は、円グラフウィジェットで各ステータス別にディスクの数を示します。



ディスク状態アラート

30分間隔でディスク状態のチェックが実行されるとともに、対応するアラートが1日に1回生成されます。ディスク状態が**警告**から**重大**に変化する場合、必ずアラートが生成されます。

アラート名	重大度	ディスク状態ステータス	説明
ディスク障害が生じる可能性があります	警告	(30 – 70)	このマシン上の<ディスク名>ディスクは、今後故障する可能性があります。できるだけ早くこのディスクのフルイメージバックアップを実行し、新しいディスクに交換してからイメージをリカバリしてください。
ディスク障害が差し迫っています	重大	(0 – 30)	このマシンの<ディスク名>ディスクは、故障が差し迫った重大な状態にあります。ストレスが加わるとディスクが故障する可能性があるため、現時点ではこのディスクのイメージバックアップは推奨できません。今すぐこのディスクの最も重要なファイルをすべてバックアップして、交換してください。

データ保護マップ

注意
この機能は、Advanced Backupパックで利用可能です。

データ保護マップ機能により、重要なすべてのデータを確認できます。また拡大縮小できるツリー形式のビューで、すべての重要なファイルについて数量、サイズ、ロケーション、保護ステータスの詳細を確認できます。

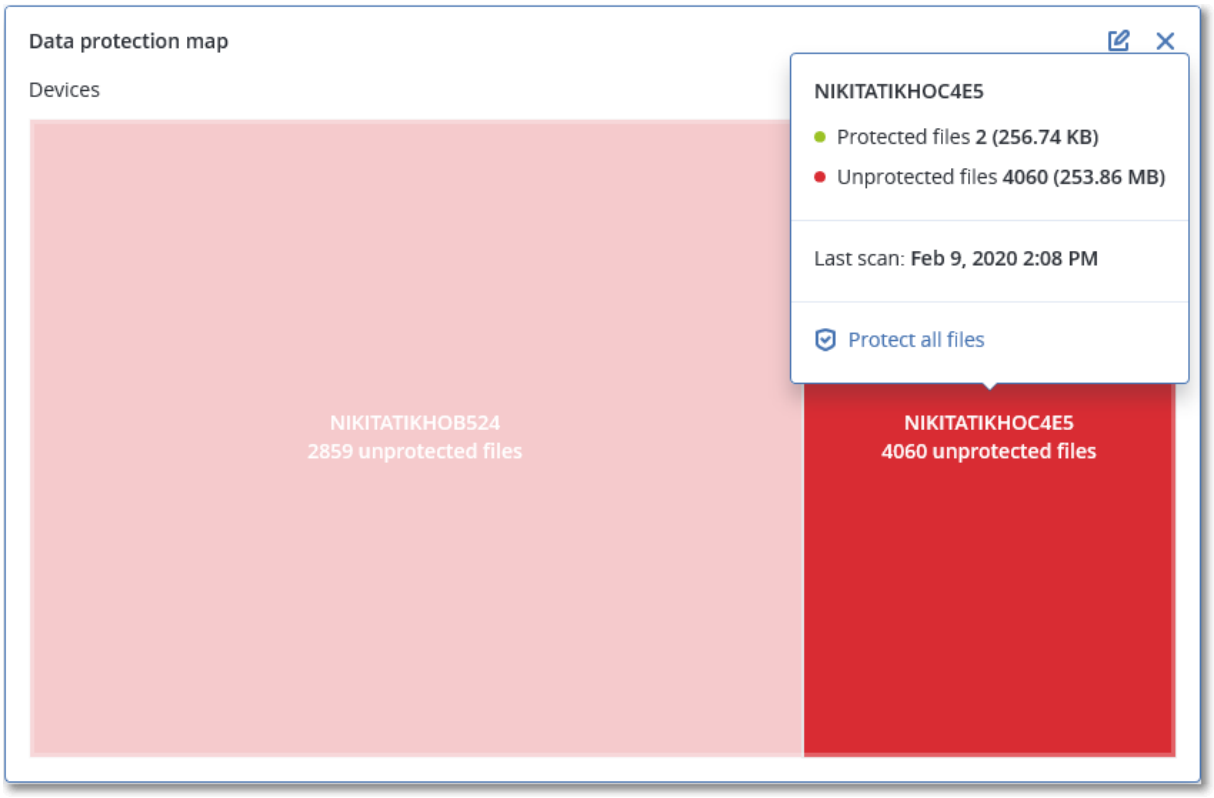
各ブロックのサイズは、カスタマー/マシンに属する重要なすべてのファイルの合計数/サイズによって異なります。

ファイルは次のいずれかの保護ステータスになります。

- **重大** - 選択済みのマシン/ロケーションにおける既存のバックアップの設定で、バックアップ対象に指定されていない拡張子を持つ保護非対象のファイルが、51～100%存在します。
- **低** - 選択済みのマシン/ロケーションにおける既存のバックアップの設定で、バックアップ対象に指定されていない拡張子を持つ保護非対象のファイルが、21～50%存在します。
- **中** - 選択済みのマシン/ロケーションにおける既存のバックアップの設定で、バックアップ対象に指定されていない拡張子を持つ保護非対象のファイルが、1～20%存在します。
- **高** - 選択済みのマシン/ロケーションで、すべてのファイルが保護（バックアップ）対象に指定された拡張子を有しています。

データ保護確認の結果は、データ保護マップウィジェットの監視ダッシュボードで確認できます。ツリーマップウィジェットにはマシンレベルの詳細が表示されます。

- マシンレベル - 選択済みのカスタマーのマシンごとに重要なファイルの保護ステータスに関する情報を表示します。



保護されていないファイルを保護するには、ブロックにマウスを移動（ホバー）して、**[すべてのファイルを保護]** をクリックします。ダイアログウィンドウで、保護されていないファイルの数とそのロケーションについての情報を見つけることができます。それらを保護するには、**[すべてのファイルを保護]** をクリックします。

CSV形式で詳細レポートをダウンロードすることもできます。

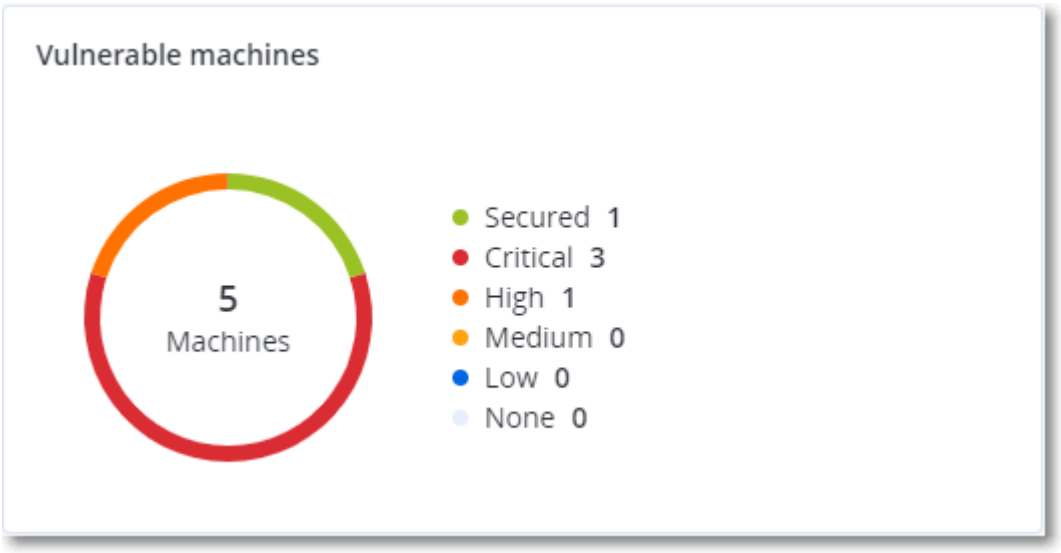
脆弱性診断ウィジェット

脆弱性のあるマシン

このウィジェットは脆弱性の重大度別に脆弱なマシンを表示します。

見つかった脆弱性は、共通脆弱性評価システム（CVSS）v3.0に従って、次の重大度レベルのいずれかで示されます。

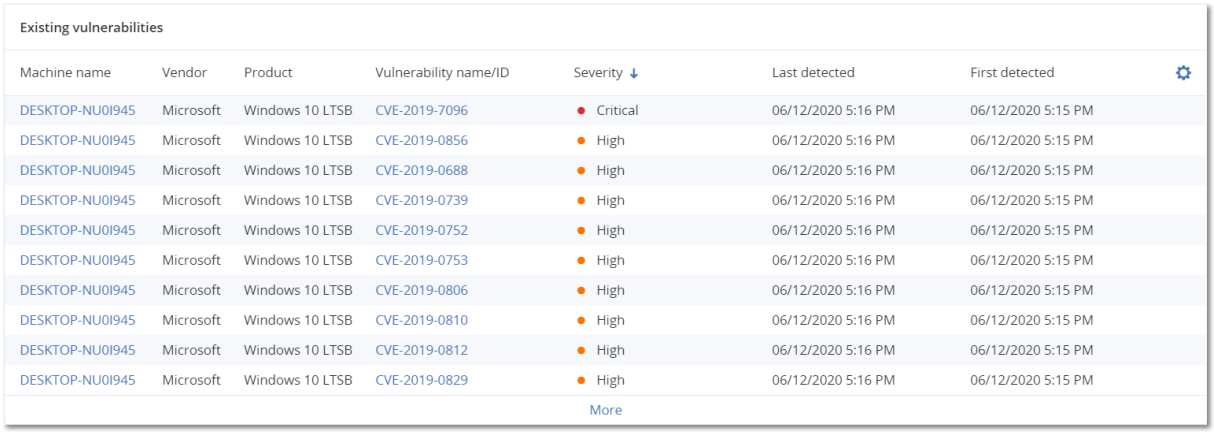
- セキュア: 脆弱性が見つからない
- 重大:9.0 - 10.0 CVSS
- 高:7.0 - 8.9 CVSS
- 中:4.0 - 6.9 CVSS
- 低:0.1 - 3.9 CVSS
- なし:0.0 CVSS



既存の脆弱性

このウィジェットは、マシンに現時点で存在する脆弱性を表示します。[**既存の脆弱性**] ウィジェットには、タイムスタンプが表示される2つの列があります。

- **最初の検出** - マシンで最初に脆弱性が検出された日時。
- **最後の検出** - マシンで最後に脆弱性が検出された日時。


Existing vulnerabilities

Machine name	Vendor	Product	Vulnerability name/ID	Severity	Last detected	First detected
DESKTOP-NU0I945	Microsoft	Windows 10 LTSB	CVE-2019-7096	Critical	06/12/2020 5:16 PM	06/12/2020 5:15 PM
DESKTOP-NU0I945	Microsoft	Windows 10 LTSB	CVE-2019-0856	High	06/12/2020 5:16 PM	06/12/2020 5:15 PM
DESKTOP-NU0I945	Microsoft	Windows 10 LTSB	CVE-2019-0688	High	06/12/2020 5:16 PM	06/12/2020 5:15 PM
DESKTOP-NU0I945	Microsoft	Windows 10 LTSB	CVE-2019-0739	High	06/12/2020 5:16 PM	06/12/2020 5:15 PM
DESKTOP-NU0I945	Microsoft	Windows 10 LTSB	CVE-2019-0752	High	06/12/2020 5:16 PM	06/12/2020 5:15 PM
DESKTOP-NU0I945	Microsoft	Windows 10 LTSB	CVE-2019-0753	High	06/12/2020 5:16 PM	06/12/2020 5:15 PM
DESKTOP-NU0I945	Microsoft	Windows 10 LTSB	CVE-2019-0806	High	06/12/2020 5:16 PM	06/12/2020 5:15 PM
DESKTOP-NU0I945	Microsoft	Windows 10 LTSB	CVE-2019-0810	High	06/12/2020 5:16 PM	06/12/2020 5:15 PM
DESKTOP-NU0I945	Microsoft	Windows 10 LTSB	CVE-2019-0812	High	06/12/2020 5:16 PM	06/12/2020 5:15 PM
DESKTOP-NU0I945	Microsoft	Windows 10 LTSB	CVE-2019-0829	High	06/12/2020 5:16 PM	06/12/2020 5:15 PM

More

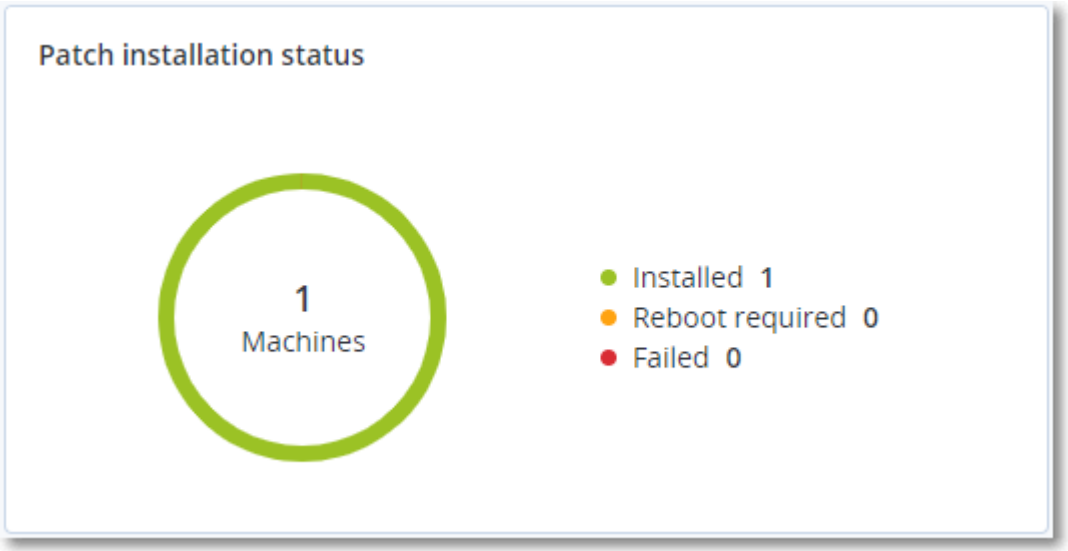
パッチインストールウィジェット

パッチの管理機能に関連する4種類のウィジェットがあります。

パッチインストールステータス

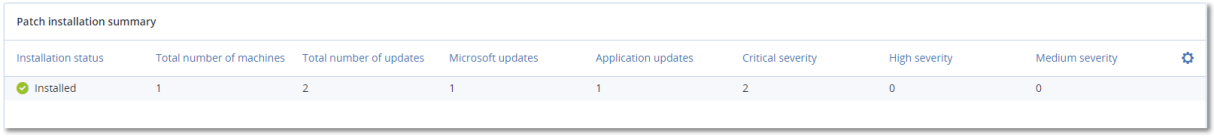
このウィジェットは、パッチインストールステータスでグループ化したマシンの数を表示します。

- **インストール済み** - 利用可能なすべてのパッチがマシンにインストール済み
- **再起動が必要** - パッチのインストール後にマシンの再起動が必要
- **失敗** - マシンでパッチインストールが失敗



パッチインストール概要

このウィジェットは、パッチインストールステータスによるマシンのパッチの概要を表示します。



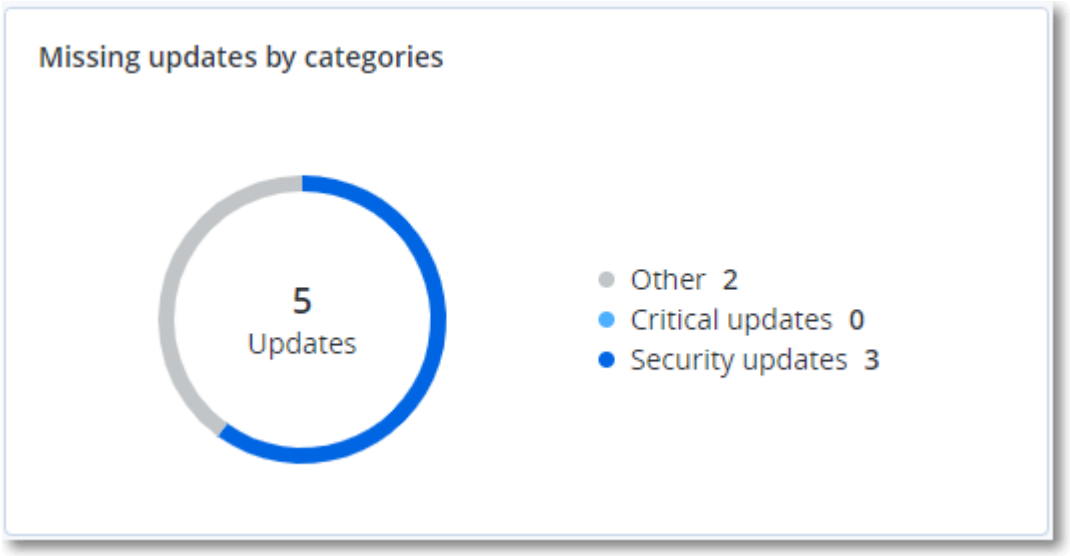
パッチインストール履歴

このウィジェットは、マシンのパッチに関する詳細を表示します。

カテゴリ別の未適用アップデート

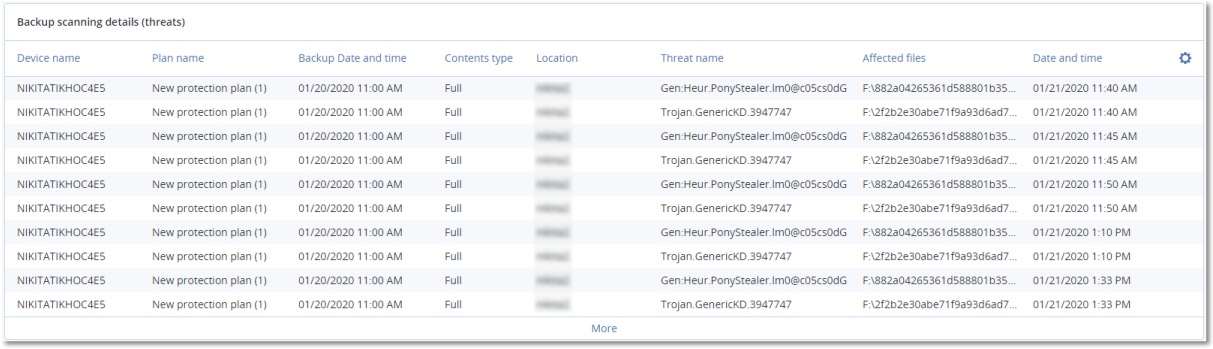
このウィジェットは、見つからないアップデートの数をカテゴリ別に表示します。次のカテゴリで表示されます。

- セキュリティアップデート
- 重要なアップデート
- その他



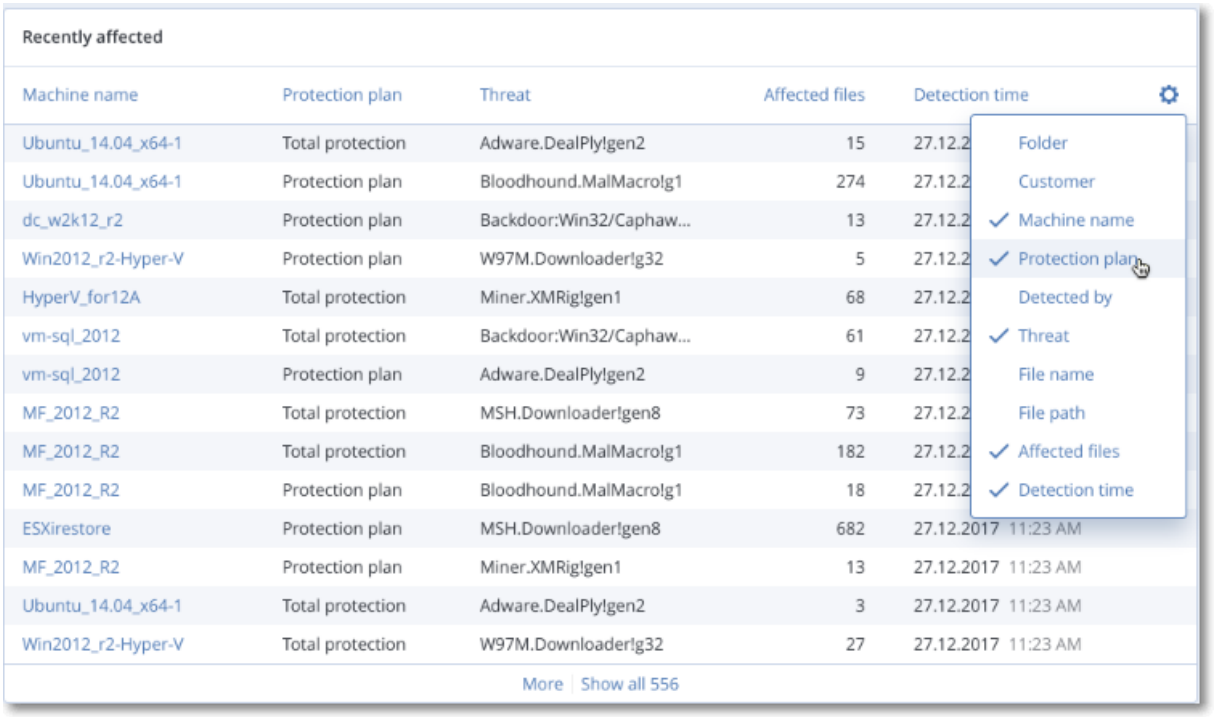
バックアップスキャンの詳細

このウィジェットは、バックアップで検出された脅威に関する詳細を表示します。



最近影響を受けたもの

このウィジェットには、ウイルス、マルウェア、ランサムウェアなどの脅威の影響にさらされているワークロードの詳細情報が表示されます。検出された脅威の情報、脅威が検出された時間、影響を受けたファイルの数などを確認できます。



最近影響を受けたワークロードのデータをダウンロードする

最近影響を受けたワークロードのデータをダウンロードし、CSVファイルを生成して、指定した受信者に送信できます。

最近影響を受けたワークロードのデータをダウンロードするには

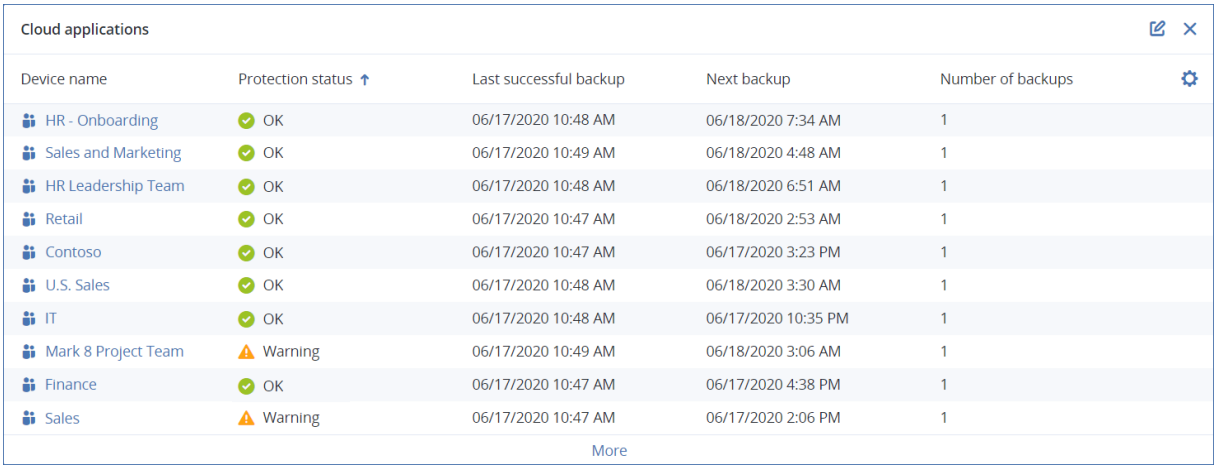
1. **[最近影響を受けたもの]** ウィジェットで、**[データをダウンロード]** をクリックします。
2. **[対象期間]** フィールドに、データをダウンロードする日数を入力します。入力可能な最大日数は200日です。
3. **[受信者]** フィールドに、すべての受信者のEメールアドレスを入力します。Eメールには、CSVファイルをダウンロードするためのリンクが記載されます。
4. **[ダウンロード]** をクリックします。
   システムにより、指定した期間に影響を受けたワークロードのデータを含む、CSVファイルの作成が開始されます。CSVファイルの作成が完了すると、システムにより受信者にEメールが送信されます。各受信者はその後、CSVファイルをダウンロードできるようになります。

クラウドアプリケーション

このウィジェットは、クラウドツークラウドのリソースに関する詳細を表示します。

- Microsoft 365ユーザー（メールボックス、OneDrive）
- Microsoft 365グループ（メールボックス、グループサイト）
- Microsoft 365のパブリックフォルダ
- Microsoft 365サイトコレクション
- Microsoft 365 Teams

- Google Workspaceユーザー（Gmail、Googleドライブ）
- Google Workspace共有ドライブ

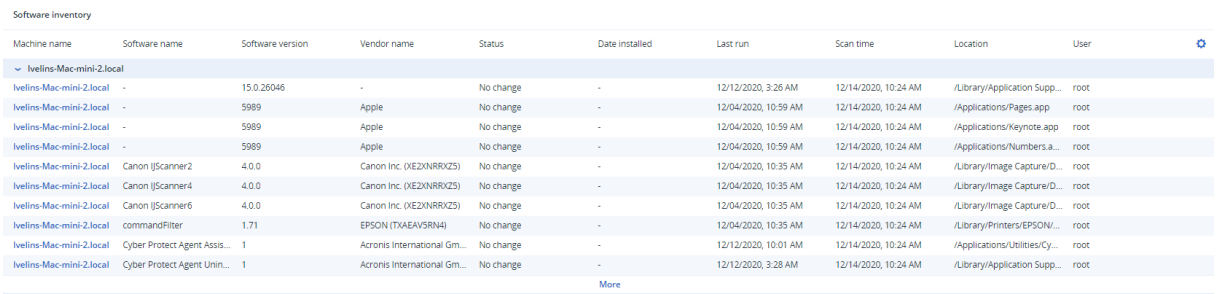


クラウドツークラウドのリソースに関する追加の情報は、以下のウィジェットでも利用可能です。

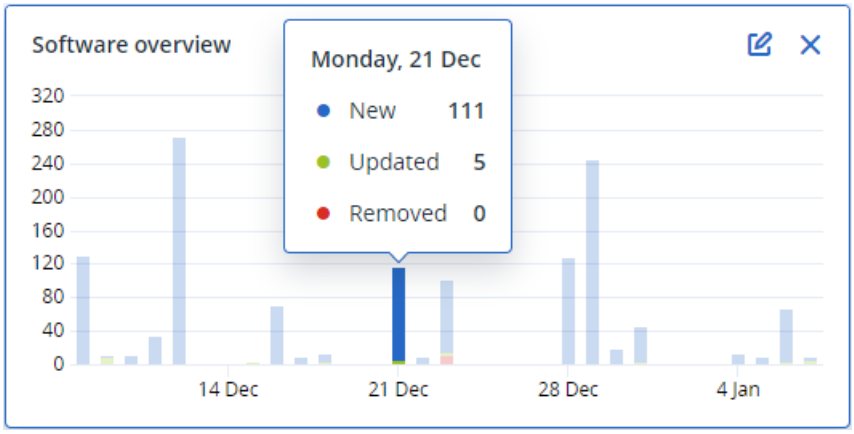
- アクティビティ
- アクティビティ一覧
- 直近 5 件のアラート
- アラート履歴
- アクティブアラート概要
- アラート概要履歴
- アクティブアラートの詳細
- ロケーションサマリー

ソフトウェアインベントリウィジェット

ソフトウェアインベントリテーブルウィジェットには、組織内のWindowsおよびmacOSデバイスにインストールされているすべてのソフトウェアに関する詳細情報が表示されます。



ソフトウェアの概要ウィジェットには、指定した期間（7日、30日、または当月）に組織内のWindowsおよびmacOSデバイスで新規導入、アップデート、および削除されたアプリケーションの数が表示されます。



チャートの特定のバーにホバーすると、次の情報を含むツールチップが表示されます。

新規 - 新しくインストールされたアプリケーションの数です。

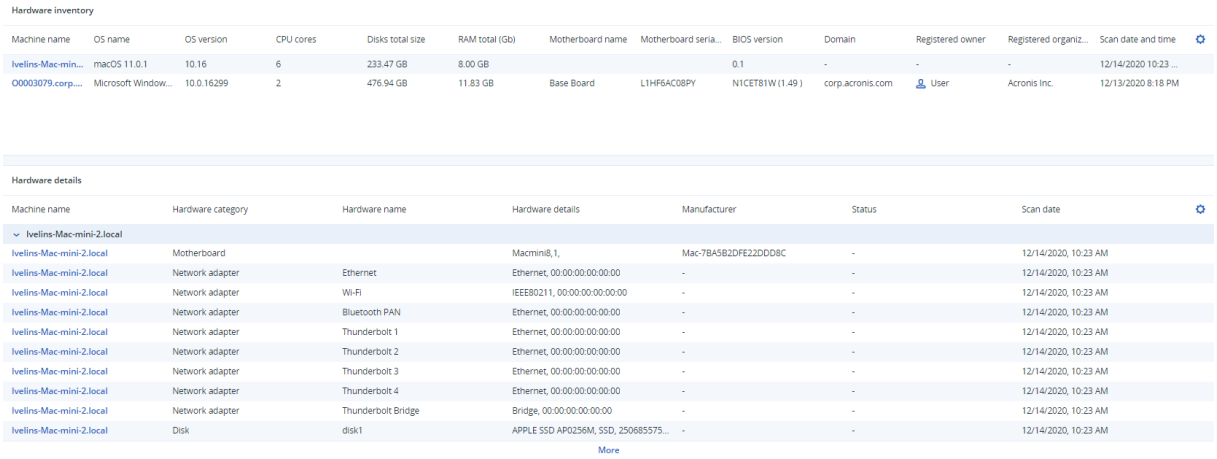
アップデート済み - アップデートされたアプリケーションの数です。

削除済み -削除されたアプリケーションの数です。

特定のステータスを示すバーの一部をクリックすると、**[ソフトウェア管理]** -> **[ソフトウェアインベントリ]** ページにリダイレクトされます。ページ内の情報は、対応する日付とステータスでフィルタリングされます。

ハードウェアインベントリウィジェット

ハードウェアインベントリおよび**ハードウェアの詳細**テーブルウィジェットには、組織内の物理的および仮想的なWindows/macOSデバイスにインストールされているすべてのハードウェアに関する情報が表示されます。


Hardware inventory

Machine name	OS name	OS version	CPU cores	Disks total size	RAM total (Gb)	Motherboard name	Motherboard seria...	BIOS version	Domain	Registered owner	Registered organiz...	Scan date and time
Ivelins-Mac-min...	macOS 11.0.1	10.16	6	233.47 GB	8.00 GB			0.1	-	-	-	12/14/2020 10:23 ...
O0003079.corp....	Microsoft Window...	10.0.16299	2	476.94 GB	11.83 GB	Base Board	L1HF6AC08PY	N1CET81W (1.49)	corp.acronis.com	User	Acronis Inc.	12/13/2020 8:18 PM

Hardware details

Machine name	Hardware category	Hardware name	Hardware details	Manufacturer	Status	Scan date
Ivelins-Mac-mini-2.local						
Ivelins-Mac-mini-2.local	Motherboard		Macmini8,1,	Mac-7BA5B2DFE22DDD8C	-	12/14/2020, 10:23 AM
Ivelins-Mac-mini-2.local	Network adapter	Ethernet	Ethernet, 00:00:00:00:00:00	-	-	12/14/2020, 10:23 AM
Ivelins-Mac-mini-2.local	Network adapter	Wi-Fi	IEEE80211, 00:00:00:00:00:00	-	-	12/14/2020, 10:23 AM
Ivelins-Mac-mini-2.local	Network adapter	Bluetooth PAN	Ethernet, 00:00:00:00:00:00	-	-	12/14/2020, 10:23 AM
Ivelins-Mac-mini-2.local	Network adapter	Thunderbolt 1	Ethernet, 00:00:00:00:00:00	-	-	12/14/2020, 10:23 AM
Ivelins-Mac-mini-2.local	Network adapter	Thunderbolt 2	Ethernet, 00:00:00:00:00:00	-	-	12/14/2020, 10:23 AM
Ivelins-Mac-mini-2.local	Network adapter	Thunderbolt 3	Ethernet, 00:00:00:00:00:00	-	-	12/14/2020, 10:23 AM
Ivelins-Mac-mini-2.local	Network adapter	Thunderbolt 4	Ethernet, 00:00:00:00:00:00	-	-	12/14/2020, 10:23 AM
Ivelins-Mac-mini-2.local	Network adapter	Thunderbolt Bridge	Bridge, 00:00:00:00:00:00	-	-	12/14/2020, 10:23 AM
Ivelins-Mac-mini-2.local	Disk	disk1	APPLE SSD AP0256M, SSD, 250685575...	-	-	12/14/2020, 10:23 AM

More

ハードウェアの変更テーブルウィジェットには、指定した期間（7日、30日、または当月）に組織内の物理的および仮想的なWindows/macOSデバイスで追加、削除、および変更されたハードウェアに関する情報が表示されます。

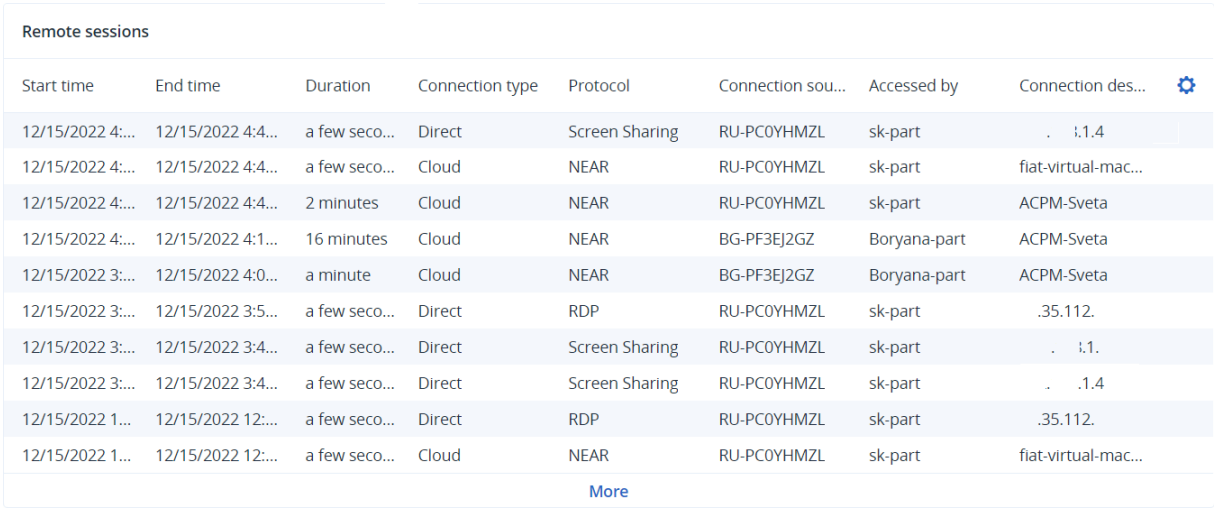
Hardware changes

Machine name	Hardware category	Status	Old value	New value	Modification date and time
DESKTOP-0FF9TTF					
DESKTOP-0FF9TTF	Network adapter	Changed	Oracle Corporation, Ethernet 802.3,...	Oracle Corporation, Ethernet 802.3, ...	01/11/2021 9:28 AM
DESKTOP-0FF9TTF	Network adapter	New	-	Realtek Semiconductor Corp., Ether...	01/04/2021 2:37 PM
DESKTOP-0FF9TTF	Motherboard	New	-	LENOVO, Torronto 5C1, PF0PJB10	01/04/2021 2:37 PM
DESKTOP-0FF9TTF	GPU	New	-	Intel(R) HD Graphics Family	01/04/2021 2:37 PM
DESKTOP-0FF9TTF	Disk	New	-	(Standard disk drives), WDC WD10JP...	01/04/2021 2:37 PM
DESKTOP-0FF9TTF	Network adapter	New	-	Cisco Systems, Ethernet 802.3, 00:0...	01/04/2021 2:37 PM
DESKTOP-0FF9TTF	Network adapter	New	-	Oracle Corporation, Ethernet 802.3, ...	01/04/2021 2:37 PM
DESKTOP-0FF9TTF	RAM	New	-	Samsung, 985D7122, 4.00 GB	01/04/2021 2:37 PM
DESKTOP-0FF9TTF	Network adapter	New	-	TAP-NordVPN Windows Provider V9...	01/04/2021 2:37 PM
DESKTOP-0FF9TTF	RAM	New	-	Micron, 00000000, 4.00 GB	01/04/2021 2:37 PM

More

リモートセッションウィジェット

このウィジェットでは、リモートデスクトップとファイル転送セッションの詳細が表示されます。



Remote sessions

Start time	End time	Duration	Connection type	Protocol	Connection sou...	Accessed by	Connection des...
12/15/2022 4:...	12/15/2022 4:4...	a few seco...	Direct	Screen Sharing	RU-PC0YHMZL	sk-part	. .1.4
12/15/2022 4:...	12/15/2022 4:4...	a few seco...	Cloud	NEAR	RU-PC0YHMZL	sk-part	fiat-virtual-mac...
12/15/2022 4:...	12/15/2022 4:4...	2 minutes	Cloud	NEAR	RU-PC0YHMZL	sk-part	ACPM-Sveta
12/15/2022 4:...	12/15/2022 4:1...	16 minutes	Cloud	NEAR	BG-PF3EJ2GZ	Boryana-part	ACPM-Sveta
12/15/2022 3:...	12/15/2022 4:0...	a minute	Cloud	NEAR	BG-PF3EJ2GZ	Boryana-part	ACPM-Sveta
12/15/2022 3:...	12/15/2022 3:5...	a few seco...	Direct	RDP	RU-PC0YHMZL	sk-part	.35.112.
12/15/2022 3:...	12/15/2022 3:4...	a few seco...	Direct	Screen Sharing	RU-PC0YHMZL	sk-part	. .1.
12/15/2022 3:...	12/15/2022 3:4...	a few seco...	Direct	Screen Sharing	RU-PC0YHMZL	sk-part	. .1.4
12/15/2022 1...	12/15/2022 12:...	a few seco...	Direct	RDP	RU-PC0YHMZL	sk-part	.35.112.
12/15/2022 1...	12/15/2022 12:...	a few seco...	Cloud	NEAR	RU-PC0YHMZL	sk-part	fiat-virtual-mac...

More

スマート保護

脅威フィード

Acronisサイバープロテクションオペレーションセンター（CPOC）は、セキュリティアラートを生成して、関連する地域だけに送信します。セキュリティアラートによって、データ保護に影響を及ぼす世界規模のイベント（マルウェア、脆弱性、自然災害、公衆衛生など）に関する情報を確認できます。脅威フィードによって知らされるあらゆる潜在的な脅威についての情報を活用し、そうした脅威を回避することも可能になります。

注意
この機能を利用できるかどうかは、現在のアカウントで有効になっているサービスクォータによって異なります。

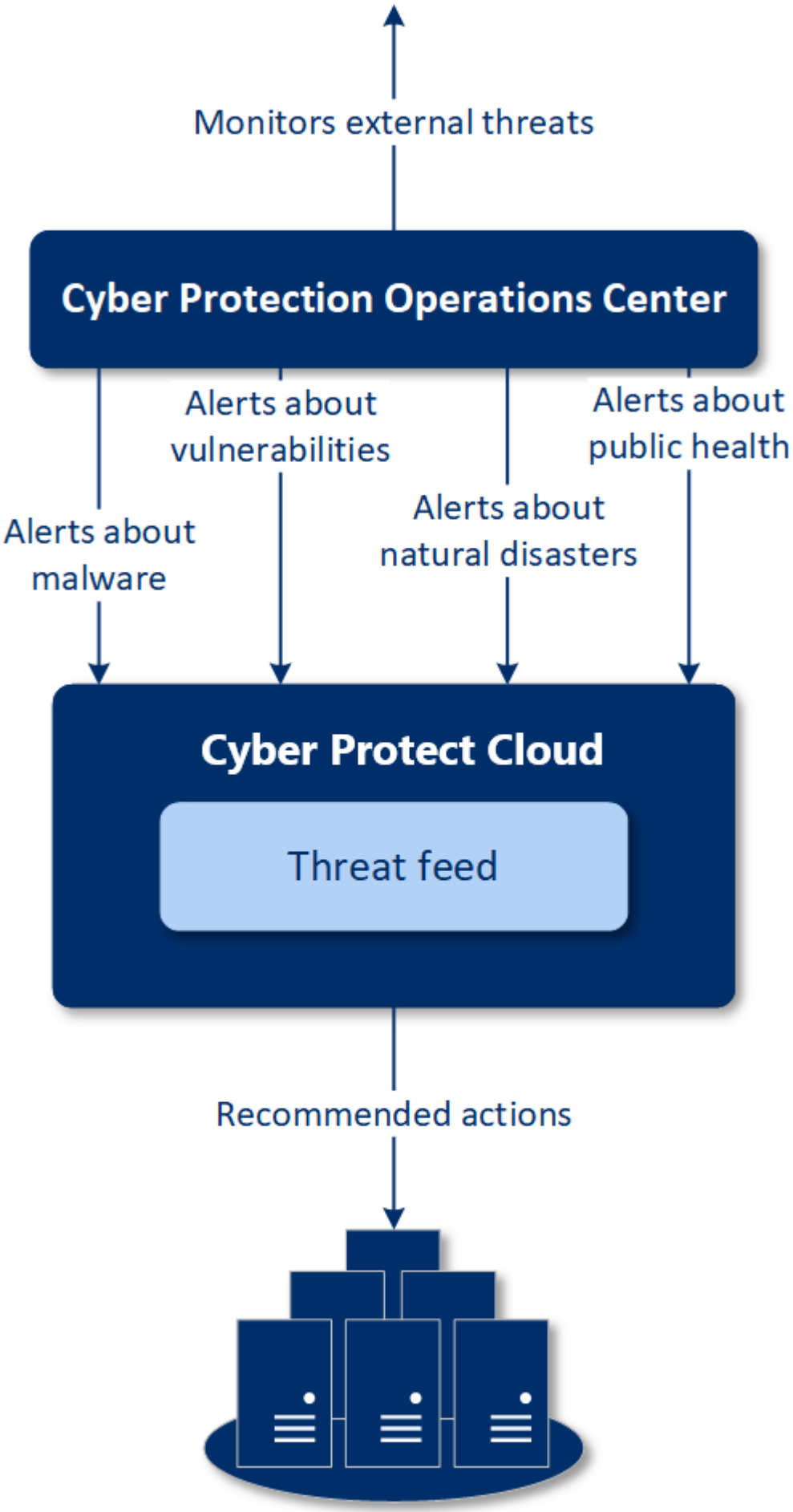
セキュリティアラートは、セキュリティエキスパートによって提供される次の一連のアクションによって解決できます。また一部のセキュリティアラートは、今後の脅威について知らせるだけで推奨アクションはありません。

注意
マルウェアアラートは、マルウェア対策保護エージェントがインストールされているマシンに対してのみ生成されます。

仕組み

Acronisサイバープロテクションオペレーションセンターは、外部からの脅威を監視して、マルウェア、脆弱性、自然災害、公衆衛生などの脅威に関するアラートを生成します。Cyber Protectコンソールの**脅威フィード**セクションでこれらすべてのアラートを確認できます。アラートの種類に応じて、それぞれ該当する推奨アクションを実行できます。

脅威フィードの主要ワークフローを下図に示します。



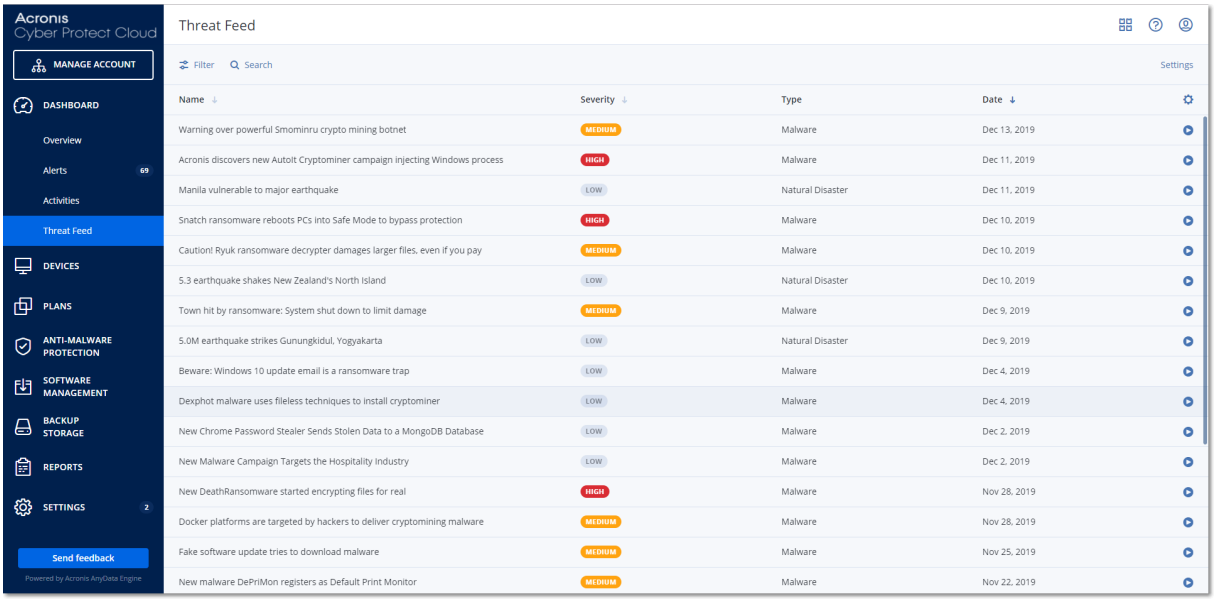
Acronisサイバープロテクションオペレーションセンターから受け取ったアラートに関する推奨アクションを開始するには、以下の手順を実行します。

1. Cyber Protectコンソールで **[監視]** > **[脅威フィード]** に進み、既存のセキュリティアラートがあるかどうかを確認します。
2. リストからアラートを選択して、詳細情報を確認します。
3. **[開始]** をクリックして、ウィザードを起動します。
4. 実行するアクションと、アクションを適用するマシンを有効にします。以下のアクションがあります。
   - **脆弱性診断** - マシンをスキャンして脆弱性があるかどうかを調べます
   - **パッチ管理** - 選択したマシンにパッチをインストールします
   - **マルウェア対策保護** - 選択したマシンの完全スキャンを実行します

     注意
     このアクションは、マルウェア対策保護のエージェントがインストールされているマシンでのみ使用できます。

   - **保護されているマシンや保護されていないマシンのバックアップ** - 保護されているワークロードや保護されていないワークロードをバックアップします。
     （クラウドとローカルのアクセス可能なすべてのロケーションで）ワークロードのバックアップがまだ存在しない場合、または既存のバックアップが暗号化されている場合、システムにより以下の形式の名前で完全バックアップが作成されます:

     `%workload_name%-Remediation`
     デフォルトのバックアップ先は、Cyber Protect Cloudストレージですが、処理を開始する前に別のロケーションを設定することもできます。
     暗号化されていないバックアップが既に存在する場合は、システムにより、既存のアーカイブに増分バックアップが作成されます。
5. **[開始]** をクリックします。
6. **[アクティビティ]** ページで、アクティビティが正常に実行されたことを確認します。



すべてのアラートの削除

以下の期間が過ぎると、脅威フィードからの自動クリーンアップが実行されます。

- 自然災害 - 1週間
- 脆弱性 - 1カ月
- マルウェア - 1カ月
- 公衆衛生 - 1週間

データ保護マップ

データ保護マップ機能で実行できること

- マシンに保管されているデータの詳細情報（分類、ロケーション、保護ステータス、追加情報）を取得すること。
- データが保護されているかどうかを確認すること。データがバックアップ（バックアップモジュールを有効にした保護計画）で保護されていると、そのデータは保護されていると見なされます。
- データ保護のアクションを実行すること。

仕組み

1. まず、データ保護マップのモジュールを有効にした保護計画を作成します。
2. その後、計画を実行し、データが検出され、解析されたら、データ保護マップウィジェットでデータ保護の状況を可視化できます。
3. **[デバイス]** > **[データ保護マップ]** に進んで、保護されていないファイルに関する情報をデバイスごとに確認することも可能です。
4. デバイスで検出された保護されていないファイルを保護するためのアクションを実行できます。

検出された保護されていないファイルの管理

検出された保護されていない重要なファイルを保護するには、以下の手順を実行します。

1. Cyber Protectコンソールで **[デバイス]** > **[データ保護マップ]** に進みます。
   デバイスのリストで、保護されていないファイルの数やサイズに関する全般的な情報をデバイスごとに確認したり、最新のデータ検出の状況を調べたりできます。
   特定のマシンにあるファイルを保護するには、省略記号のアイコンをクリックし、**[すべてのファイルを保護]** をクリックします。計画のリストにリダイレクトされます。そのリストで、バックアップモジュールを有効にした保護計画を作成できます。
   保護されていないファイルがある特定のデバイスをリストから削除するには、**[次回のデータ検出まで非表示]** をクリックします。
2. 特定のデバイスにある保護されていないファイルの詳細情報を表示するには、そのデバイスの名前をクリックします。
   拡張子ごと、ロケーションごとに、保護されていないファイルの数が表示されます。保護されていないファイルのうち、どの拡張子のファイルの情報を確認するかを指定するために、検索フィールドで拡張子を定義します。

3. 保護されていないファイルをすべて保護するには、[**すべてのファイルを保護**] をクリックします。計画のリストにリダイレクトされます。そのリストで、バックアップモジュールを有効にした保護計画を作成できます。

保護されていないファイルの情報をレポート形式で取得するには、[**CSV形式で詳細レポートをダウンロード**] をクリックします。

データ保護マップの設定

データ保護マップのモジュールを組み込んだ保護計画を作成する方法については、「保護計画の作成」を参照してください。

データ保護マップのモジュールでは、以下の設定を指定できます。

スケジュール

データ保護マップのタスクを実行するスケジュールを作成するために、さまざまな設定を定義できます。

フィールド	説明
次のイベントを使ってタスクの実行スケジュールを設定します	この設定は、タスクがいつ実行されるかを定義します。 次の値を使用できます。 • **時刻でスケジュール** - これはデフォルト設定です。タスクは指定した時間に実行されます。 • **システムへのユーザーログイン時** - デフォルトでは、いずれかのユーザーがログインするとタスクが開始されます。特定のユーザーアカウントのみがタスクをトリガーできるように、この設定を変更できます。 • **システムへのユーザーログオフ時** - デフォルトでは、いずれかのユーザーがログオフするとタスクが開始されます。特定のユーザーアカウントのみがタスクをトリガーできるように、この設定を変更できます。 **注意** このタスクは、システムのシャットダウン時には実行されません。シャットダウンとログオフは、スケジューリング構成における別個のイベントです。 • **システムの起動時** - オペレーティングシステムが起動するときにタスクが実行されます。 • **システムのシャットダウン時** - オペレーティングシステムがシャットダウンするときにタスクが実行されます。
スケジュールの種類	このフィールドは、[**次のイベントを使ってタスクの実行スケジュールを設定**] で [**時刻でスケジュール**] を選択した場合に表示されます。 次の値を使用できます。

フィールド	説明
	• **月単位** - タスクを実行する該当月と、その月内の週または日を選択します。 • **日単位** - これはデフォルト設定です。タスクを実行する週中の日を選択しします。 • **時間単位** - タスクを実行する週中の日、繰り返しの回数、時間間隔を選択しします。
開始時刻	このフィールドは、[**次のイベントを使ってタスクの実行スケジュールを設定**] で [**時刻でスケジュール**] を選択した場合に表示されます。 タスクを実行する正確な時間を選択します。
日付範囲内に実行	このフィールドは、[**次のイベントを使ってタスクの実行スケジュールを設定**] で [**時刻でスケジュール**] を選択した場合に表示されます。 設定したスケジュールが有効な日付範囲を指定します。
ユーザーアカウントを指定し、そのアカウントがオペレーティングシステムにログインしたときにタスクを開始	このフィールドは、[**次のイベントを使ってタスクの実行スケジュールを設定**] で [**システムへのユーザーログイン時**] を選択した場合に表示されます。 次の値を使用できます。 • **任意のユーザー** - いずれかのユーザーがログインしたときにタスクを開始させたい場合は、このオプションを使用します。 • **次のユーザー** - 指定したユーザーアカウントのログインでタスクを開始させたい場合は、このオプションを使用します。
ユーザーアカウントを指定し、そのアカウントがオペレーティングシステムからログアウトしたときにタスクを開始	このフィールドは、[**次のイベントを使ってタスクの実行スケジュールを設定**] で [**システムへのユーザーログオフ時**] を選択した場合に表示されます。 次の値を使用できます。 • **任意のユーザー** - いずれかのユーザーがログアウトしたときにタスクを開始させたい場合は、このオプションを使用します。 • **次のユーザー** - 指定したユーザーアカウントのログアウトでタスクを開始させたい場合は、このオプションを使用します。
開始条件	すべての条件を定義して、同時に満たされたときにタスクを実行する条件を指定します。 マルウェア対策スキャンの開始条件は、**バックアップモジュール**の開始条件に類似しています。「開始条件」を参照してください。 以下のような追加の開始条件を定義できます。 • **時間枠内でタスク開始時間を分散する** - このオプションを使用すると、タスクを実行する時間枠を設定して、ネットワークのボトルネックを回避できます。遅延時間を、時間または分単位で指定できます。たとえばデフォルトの開始時間が10:00 AMで、遅延を60分とした場

フィールド	説明
	合、タスクは10:00 AMから11:00 AMの間に開始されます。 • **マシンの電源が入っていないため実行されなかったタスクを起動時に実行する** • **タスク実行中はスリープモードや休止モードに入らない** - このオプションは、Windowsを実行しているマシンに対してのみ有効です。 • **開始条件を満たさない場合でも、次の時間の経過後にタスクを実行** - 他の開始条件にかかわらずタスクが実行されるまでの時間を指定します。 **注意** 開始条件は、Linuxではサポートされていません。

拡張子と例外ルール

[拡張子] タブでファイル拡張子のリストを定義すると、その拡張子のファイルはデータ検出時に重要と見なされ、保護されているかどうかがチェックされます。以下の形式で拡張子を定義してください。

```
.html, .7z, .docx, .zip, .pptx, .xml
```

[例外ルール] タブで、データの検出時に保護ステータスを確認しないファイルやフォルダを定義できます。

- **[隠しファイルとフォルダ]** - 選択すると、データの検査時に隠しファイルと隠しフォルダがスキップされます。
- **[システムファイルとフォルダ]** - 選択するとデータの検査時に、システムファイルとシステムフォルダがスキップされます。

アクティビティタブ

[アクティビティ] タブには、過去90日間のアクティビティが表示されます。

ダッシュボードでアクティビティをフィルタリングするには

1. **[デバイス名]** フィールドで、アクティビティが実行されているマシンを指定します。
2. **[ステータス]** ドロップダウンリストから、ステータスを選択します。たとえば、成功、失敗、進行中、キャンセルなどです。
3. **[リモート操作]** ドロップダウンリストから、操作を選択します。たとえば、計画の適用、バックアップの削除、ソフトウェアアップデートのインストールなどです。
4. **[最新]** フィールドで、アクティビティの期間を設定します。例えば、直近のアクティビティ、過去24時間のアクティビティ、過去90日間内における特定の期間のアクティビティなどです。
5. パートナー管理者として **[アクティビティ]** タブにアクセスする場合、自分が管理している特定のカスタマーのアクティビティをフィルタリングできます。

[アクティビティ] タブの表示をカスタマイズするには、ギアアイコンをクリックして、表示する列を選択します。アクティビティの進行状況をリアルタイムで確認するには、**[自動的にリフレッシュ]** チェックボックスを選択します。

実行中のアクティビティをキャンセルするには、その名前をクリックし、**[詳細]** 画面で **[キャンセル]** をクリックします。

リストにあるアクティビティを以下の条件で検索することができます。

- デバイス名
  アクティビティが実行されているそのマシンです。
- 開始者
  アクティビティを開始したアカウントです。

リモートデスクトップアクティビティは、以下のプロパティでフィルタリングできます：

- 作成する計画
- 計画の適用
- 計画の取り消し
- 計画の削除
- リモート接続
  - RDP経由のクラウドリモートデスクトップ接続
  - NEAR経由のクラウドリモートデスクトップ接続
  - Apple画面共有経由のクラウドリモートデスクトップ接続
  - Webクライアント経由のリモートデスクトップ接続
  - クイックアシスト経由のリモートデスクトップ接続
  - RDP経由の直接リモートデスクトップ接続
  - Apple画面共有経由の直接リモートデスクトップ接続
  - ファイル転送
  - クイックアシスト経由でのファイル転送
- リモート操作
  - ワークロードをシャットダウンしています
  - ワークロードを再起動しています
  - ワークロードのリモートユーザーをログアウトしています
  - ワークロードのユーザーのごみ箱を空にしています
  - ワークロードをスリープ状態にしています

Cyber Protectモニタ

Cyber Protect Monitorには、WindowsエージェントまたはMacエージェントがインストールされているマシンの保護ステータス情報が表示されます。また、ユーザーはバックアップ暗号化構成のプロキシサーバの設定を行えます。

File Sync & Shareエージェントがマシンにインストールされると、Cyber Protect MonitorはFile Sync & Shareサービスへのアクセスを提供します。File Sync & Share機能は、ユーザーが自身のFile Sync & Share アカウントにサインインし、個人用同期フォルダを選択する必須のオンボーディング後にアクセス可能です。File Sync & Shareエージェントの詳細については、Cyber Files Cloudユーザーガイドを参照してください。

重要
Cyber Protectモニタには、Cyber ProtectionまたはFile Sync & Shareサービスの管理者権限を持っていないユーザーでもアクセスできます。

次の表に、管理者権限を付与されていないユーザーが可能な操作をまとめています。

インストールされているエージェント	ユーザーが可能な操作	ユーザーができない操作
WindowsエージェントまたはMacエージェント	• デフォルトの保護計画をマシンに適用する • マシンの保護ステータスを確認する • Active Protectionの通知を受け取る • マシンのバックアップを一時停止する • プロキシサーバの設定を構成する • バックアップ暗号化設定を変更する **警告** Cyber Protect Monitorで暗号化設定を変更すると、保護計画の設定が上書きされ、マシンのすべてのバックアップに影響します。このため、この操作により、一部の保護計画が失敗する場合があります。詳細については、"暗号化"（430ページ）を参照してください。 パスワードを失くしたり忘れたりした場合に、暗号化されたバックアップをリカバリする方法はありません。	• カスタム保護計画を適用する • すでに適用されている保護計画を管理する
WindowsエージェントとSync & Shareエージェント MacエージェントとSync & Shareエージェント	• ローカルの同期フォルダとFile Sync & Shareアカウント間でのコンテンツの同期 • 同期操作を一時停止する • 同期フォルダを変更する • 同期できないファイルタイプを確認する	• 同期できないファイルタイプを編集する

Cyber Protectモニタのプロキシサーバー設定の構成

Cyber Protectモニタのプロキシサーバー設定を構成できます。この設定は、マシンにインストールされているすべてのエージェントに影響します。

プロキシサーバーの設定を構成するには

1. Cyber Protectモニタを開き、右上隅にあるギアアイコンをクリックします。
2. **[設定]** をクリックしてから、**[プロキシ]** をクリックします。

3. **[プロキシサーバを使用する]** スイッチを有効にし、プロキシサーバーアドレスとポートを入力します。
4. （プロキシサーバーへのアクセスがパスワードで保護されている場合）**[パスワードが必要]** スイッチを有効にし、プロキシサーバーにアクセスするためのユーザー名とパスワードを入力します。
5. **[保存]** をクリックします。
   プロキシサーバーの設定は、`http-proxy.yaml`ファイルに保存されます。

レポート

注意
この機能を利用できるかどうかは、現在のアカウントで有効になっているサービスクォータによって異なります。

操作に関するレポートには、ダッシュボードウィジェットの任意のセットを含めることができます。すべてのウィジェットには企業全体のサマリ情報が表示されます。

ウィジェットのタイプに応じ、レポートには時間範囲のデータ、または参照時やレポート生成時のデータが含まれます。"ウィジェットの種類に応じたレポートのデータ"（306ページ）をご覧ください。

すべての履歴ウィジェットで、同じ時間範囲のデータが表示されます。この範囲はレポート設定で変更できます。

デフォルトのレポートを使用したり、カスタムレポートを作成したりできます。

レポートをダウンロードできます。またXLSX（Excel）またはPDF形式によりEメールで送信することもできます。

デフォルトレポートのセットは、Cyber Protectionサービスのエディションによって異なります。デフォルトのレポートの一覧は次のとおりです。

レポート名	説明
マシンごとの #CyberFit スコア	各マシンのセキュリティメトリクスと構成の評価に基づき、#CyberFit スコアと、改善するための提案が表示されます。
アラート	指定された期間に発生したアラートを表示します。
バックアップスキャンの詳細	バックアップ内に検出された脅威に関する詳細を表示します。
日次のアクティビティ	指定された期間中に実行されたアクティビティの概要を表示します。
データ保護マップ	マシン上にあるすべての重要なファイルの数、サイズ、ロケーション、保護ステータスの詳細を表示します。
検出された脅	影響を受けたマシンの詳細情報として、ブロックされた脅威の数、および正常なマシンと脆弱

威	なマシンの数を表示します。
検出されたマシン	組織のネットワーク内で見つかったすべてのマシンを一覧表示します。
ディスク状態の予測	HDD/SSDが故障するタイミングの予測と現在のディスクのステータスを示します。
既存の脆弱性	組織内のOSとアプリケーションの既存の脆弱性を一覧表示します。このレポートには、一覧にある各製品について、ネットワーク内で影響を受けたマシンの詳細情報が表示されます。
ソフトウェアインベントリ	社内のデバイスにインストールされているソフトウェアに関する情報を表示します。
ハードウェアインベントリ	社内のデバイスで使用可能なハードウェアに関する情報を表示します。
パッチ管理概要	未適用のパッチ、インストール済みのパッチ、適用可能なパッチの一覧を表示します。レポートを掘り下げることで、未適用/インストール済みパッチの情報およびシステム全体の詳細情報が得られます。
概要	指定された期間に保護されたデバイスの概要を表示します。
週単位のアクティビティ	指定された期間中に実行されたアクティビティの概要を表示します。
リモートセッション	リモートデスクトップとファイル転送セッションの詳細が表示されます。

レポートの操作

レポートを表示するには、その名前をクリックします。

新しいレポートを追加するには

1. Cyber Protectコンソールで **[レポート]** に進みます。
2. 使用可能なレポートのリスト以下で、**[レポートを追加]** をクリックします。
3. （定義済みレポートを追加するには）定義済みレポートの名前をクリックします。
4. （カスタムレポートを追加するには）**[カスタム]** をクリックしてから、レポートにウィジェットを追加します。
5. （オプション） ウィジェットをドラッグアンドドロップして並べ替えます。

レポートを編集するには

1. Cyber Protectコンソールで **[レポート]** に進みます。
2. レポートのリストで、編集するレポートを選択します。
   以下の方法があります。
   - レポート名を変更します。
   - レポートですべてのウィジェットの時間範囲を変更します。

- レポートの受信者と、レポートを送信するタイミングを指定します。使用可能な形式は、PDFとXLSXです。

レポートを削除するには

1. Cyber Protectコンソールで **[レポート]** に進みます。
2. レポートのリストで、削除するレポートを選択します。
3. 省略記号アイコン（...）をクリックして、**[削除]** をクリックします。
4. **[削除]** をクリックしてこの選択内容を確認します。

レポートのスケジュールを設定するには

1. Cyber Protectコンソールで **[レポート]** に進みます。
2. レポートのリストで、スケジュールを設定するレポートを選択してから、**[設定]** をクリックします。
3. **[スケジュール済み]** スイッチを有効にします。
   - 受信者のEメールアドレスを指定します。
   - レポートの形式を選択します。

     注意
     PDFファイルでは最大1,000件、XLSXファイルでは最大10,000件までエクスポートできます。
     PDFファイル、XLSXファイルのタイムスタンプには、ご利用のマシンのローカル時間が使用されます。

   - レポートの言語を選択します。
   - スケジュールを構成します。
4. **[保存]** をクリックします。

レポートをダウンロードするには

1. Cyber Protectコンソールで **[レポート]** に進みます。
2. レポートのリストでレポートを選択してから、**[ダウンロード]** をクリックします。
3. レポートの形式を選択します。

レポートを送信するには

1. Cyber Protectコンソールで **[レポート]** に進みます。
2. レポートのリストでレポートを選択してから、**[送信する]** をクリックします。
3. 受信者のEメールアドレスを指定します。
4. レポートの形式を選択します。
5. **[送信する]** をクリックします。

レポート構造をエクスポートするには

1. Cyber Protectコンソールで **[レポート]** に進みます。
2. レポートのリストでレポートを選択します。
3. 省略記号アイコン（...）をクリックして、**[エクスポート]** をクリックします。

これにより、レポート構造はJSONファイルとしてマシンに保存されます。

レポートデータをダンプするには

このオプションを使用すると、カスタムされた期間のすべてのデータをフィルタリングせずにCSVファイルにエクスポートし、そのCSVファイルをEメール受信者に送信できます。

注意
CSVファイルで最大150,000項目をエクスポートできます。CSVファイルのタイムスタンプには、協定世界時（UTC）が使用されます。

1. Cyber Protectコンソールで **[レポート]** に進みます。
2. レポートのリストで、データをダンプするレポートを選択します。
3. 省略記号アイコン（...）をクリックして、**[データをダンプ]** をクリックします。
4. 受信者のEメールアドレスを指定します。
5. **[時間範囲]** で、データをダンプするカスタムの期間を指定します。

   注意
   長期間を対象とするCSVファイルの準備には、時間を要する場合があります。

6. **[送信する]** をクリックします。

ウィジェットの種類に応じたレポートのデータ

ダッシュボードのウィジェットは、表示するデータの範囲に応じて2つの種類があります。

- 参照時やレポート作成時に、実際のデータを表示するウィジェット。
- 履歴データを表示するウィジェット。

レポートの設定で特定の期間のデータをダンプするように日付範囲を構成した場合、選択された時間範囲は、履歴データを表示するウィジェットにのみ適用されます。参照した時点の実際のデータを表示するウィジェットの場合、時間範囲のパラメータは適用されません。

次の表は、使用可能なウィジェットとそのデータ範囲の一覧です。

ウィジェット名	ウィジェットやレポートに表示されるデータ
マシンごとの #CyberFit スコア	実際の値
直近 5 件のアラート	実際の値
アクティブアラートの詳細	実際の値
アクティブアラート概要	実際の値
アクティビティ	履歴レポート
アクティビティ一覧	履歴レポート
アラート履歴	履歴レポート
攻撃手法の統計	履歴レポート

バックアップスキャンの詳細（脅威）	履歴レポート
バックアップステータス	履歴レポート - 列内の**合計実行数**と**正常に完了した実行数** 実際の値 - その他のすべての列について
ブロックされたURL	実際の値
クラウドアプリケーション	実際の値
Cyber protection	実際の値
データ保護マップ	履歴レポート
デバイス	実際の値
検出されたマシン	実際の値
ディスク状態の概要	実際の値
物理デバイスごとのディスク状態	実際の値
既存の脆弱性	履歴レポート
ハードウェアの変更	履歴レポート
ハードウェアの詳細	実際の値
ハードウェアインベントリ	実際の値
アラート概要履歴	履歴レポート
インシデント重大度の履歴	履歴レポート
ロケーションサマリー	実際の値
カテゴリ別の未適用アップデート	実際の値
未保護	実際の値
パッチインストール履歴	履歴レポート
パッチインストールステータス	履歴レポート
パッチインストール概要	履歴レポート
保護ステータス	実際の値
最近影響を受けたもの	履歴レポート
リモートセッション	履歴レポート
セキュリティインシデントのバーンダウン	履歴レポート
セキュリティインシデントのMTTR	履歴レポート
ソフトウェアインベントリ	実際の値

ソフトウェアの概要	履歴レポート
脅威のステータス	実際の値
脆弱性のあるマシン	実際の値
ワークロードのネットワークステータス	実際の値

Cyber Protectコンソールでワークロードを管理する

このセクションでは、Cyber Protectコンソールでワークロードを管理する方法について説明します。

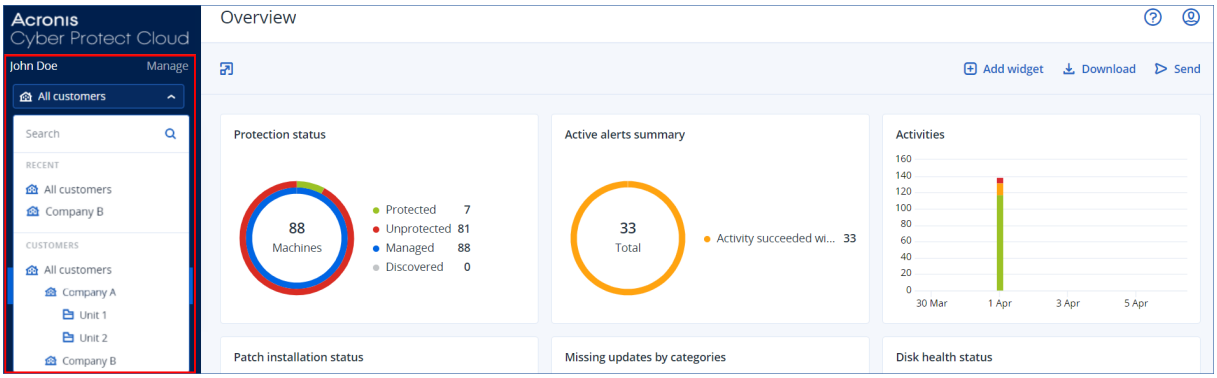
Cyber Protectコンソール

Cyber Protectコンソールでは、ワークロードや計画の管理、保護設定の変更、レポートの構成、バックアップストレージの確認を行うことができます。

Cyber Protectコンソールでは、File Sync & Shareやウイルスおよびマルウェア対策保護、パッチ管理、デバイス制御、脆弱性診断といった、別のサービス機能を利用することができます。それらのサービスや機能の種類と数は、ご利用のCyber Protectionライセンスによって異なります。

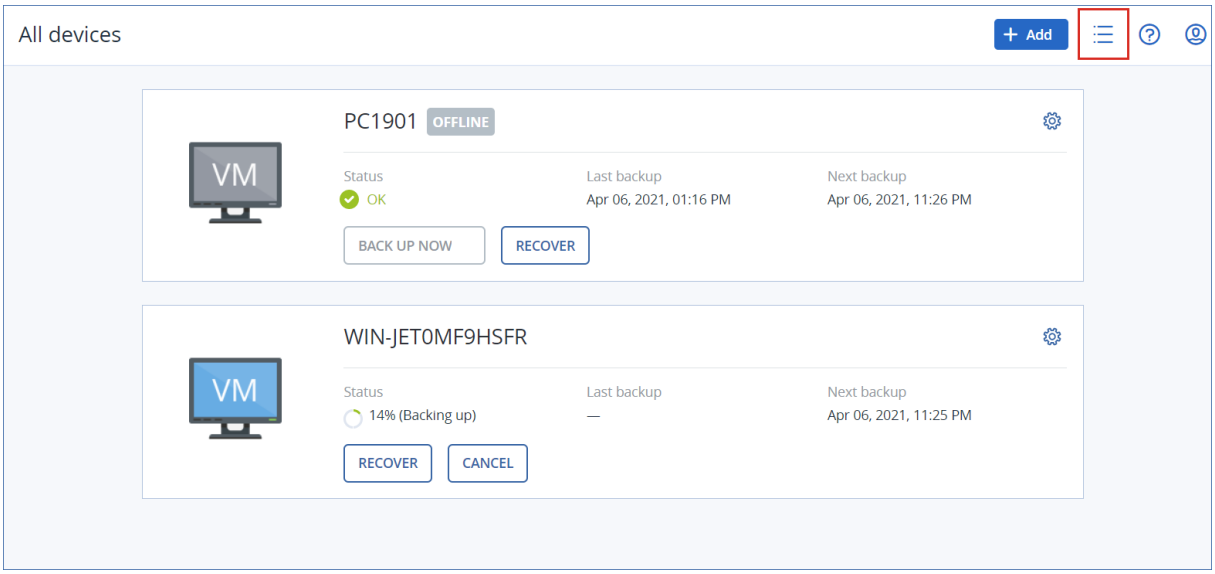
保護に関する重要な情報が掲載されているダッシュボードを確認するには、**[監視]** > **[概要]** に移動します。

アクセス許可に応じて、1つまたは複数のカスタマーテナントまたはテナント内のユニットの保護を管理できます。階層レベルを切り替えるには、ナビゲーションメニューのドロップダウンリストを使用します。アクセスできるレベルのみが表示されます。管理ポータルに移動するには、**[管理]** をクリックします。

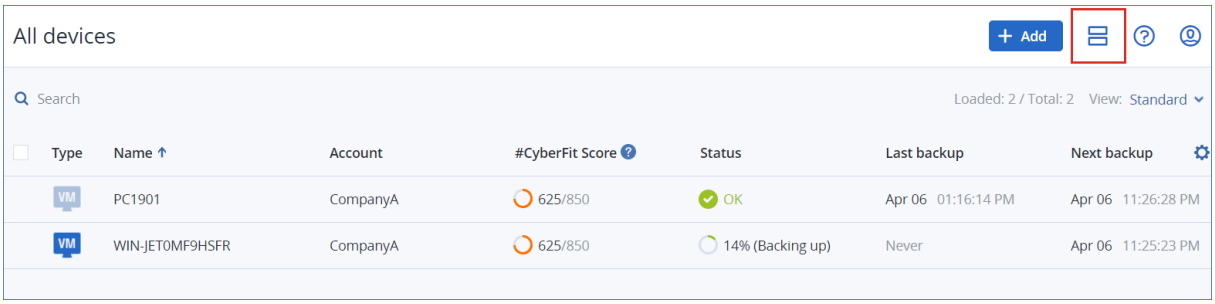


[デバイス] セクションでは、シンプルなテーブルビューが利用できます。表示を切り替えるには、右上隅にある該当するアイコンをクリックします。

簡易表示では、数件のワークロードのみが表示されます。



ワークロードの数が多くなると自動的に、表形式が有効になります。



どちらの表示形式の場合も、同じ機能、同じ操作が実行できます。このドキュメントでは、一覧表示での操作について説明します。

ワークロードがオンラインまたはオフラインに切り替わる場合、Cyber Protectコンソール上にそのステータスが反映されるまでに時間がかかります。ワークロードのステータスは1分ごとに確認されます。対応するマシンにインストールされているエージェントでデータ転送が発生せず、確認に対する応答が5回連続で返ってこない場合、ワークロードはオフラインとして表示されます。ステータスの確認に対してワークロードからの応答があるか、データ転送が開始されると、オンラインステータスに復帰したものとして表示されます。

Cyber Protectコンソールの新機能

Cyber Protect Cloudの新しい機能が利用可能になった場合、Cyber Protectコンソールにログインすると、これらの機能について簡単な説明が記載されたポップアップウィンドウが表示されます。

また、コンソールのメインウィンドウの左下にある「**新機能**」のリンクをクリックすることで、新機能の説明を確認できます。

新機能が存在しない場合、**新機能**のリンクは表示されません。

パートナー管理者としてCyber Protectコンソールを使用する

パートナー管理者は、Cyber Protectコンソールをパートナーテナント（**すべてのカスタマー**）レベルまたは顧客テナントレベルで使用できます。

パートナーテナント（**すべてのカスタマー**）レベル

パートナーテナント（**すべてのカスタマー**）レベルでは、以下のアクションを実行できます。

- すべての管理対象カスタマーテナントのワークロードに対するスクリプト計画を管理する。
  異なるカスタマーのワークロードに同じスクリプト計画を適用したり、異なるカスタマーのワークロードを含むデバイスグループを作成したりできます。パートナーレベルで静的または動的デバイスグループを作成する方法については、"パートナーレベルの静的デバイスグループ作成"（313ページ）および"パートナーレベルの動的デバイスグループ作成"（314ページ）を参照してください。スクリプトとスクリプト計画については、"サイバースクリプト処理"（228ページ）を参照してください。
- すべての管理対象カスタマーテナントのワークロードの監視計画を作成します。
- すべての管理対象カスタマーテナントのワークロードのリモート管理計画を作成します。
- 個々のカスタマーのインシデント画面にアクセスするのではなく、1つのインシデント管理インターフェイスで、すべてのカスタマーのテナントのエンドポイント検知と応答（EDR）のインシデントを表示および管理します。
- すべての管理対象カスタマーテナントについてマシンの自動検出を実行します。

カスタマーテナントレベル

パートナー管理者は、このレベルにおいて、社内管理者と同じ権限を持ち、その代理として作業を実行できます。

テナントレベルの選択

Cyber Protectコンソールで作業するテナントレベルを選択できます。

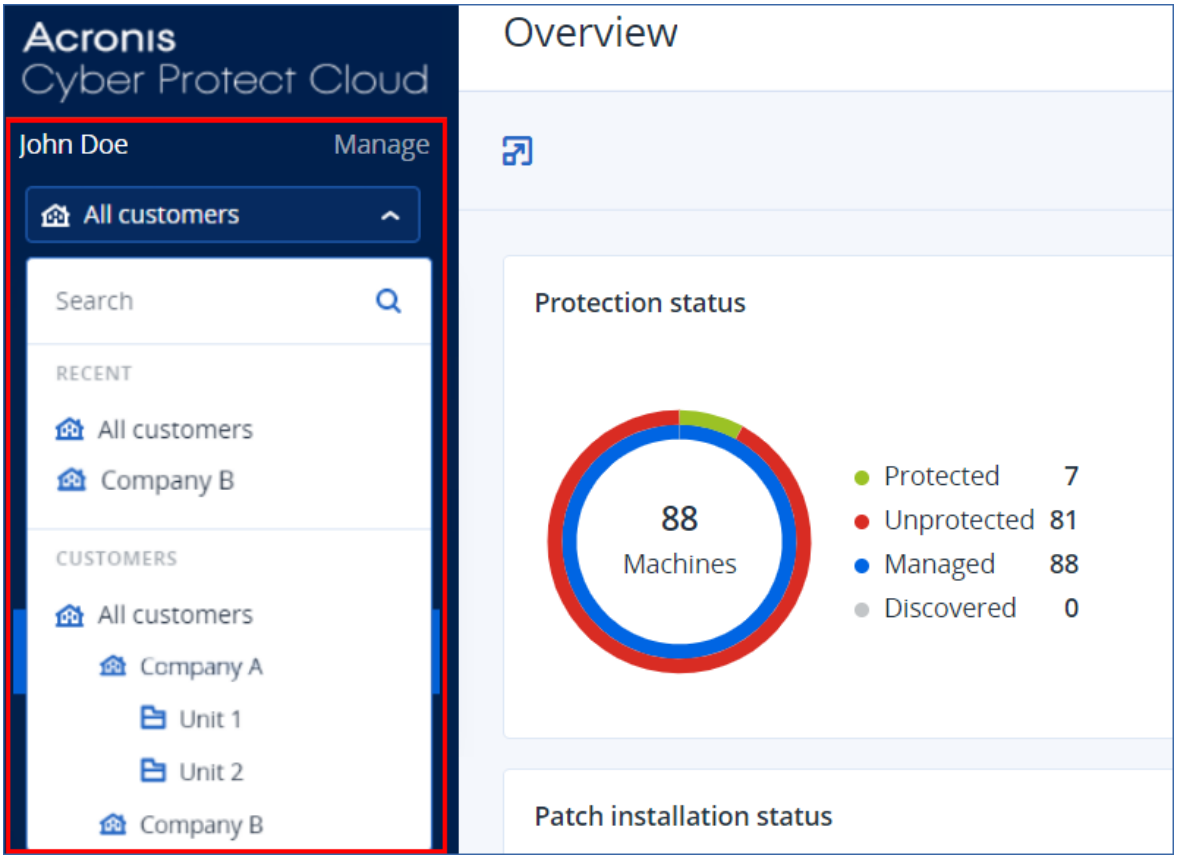
前提条件

- Cyber Protectコンソールと管理ポータルの両方にアクセスする権限がある。
- 複数のテナントやユニットを管理できる。

Cyber Protectコンソールでテナントレベルを選択するには

1. 左側のナビゲーションメニューで、顧客テナント名の横にある矢印をクリックします。
2. 次のオプションからひとつを選択します。
   - パートナーレベルで作業を実行するには、**[すべてのカスタマー]** を選択します。
   - カスタマーまたはユニットレベルで作業を実行するには、そのカスタマーまたはユニットの名前

を選択します。



Cyber Protectコンソールのパートナーテナントレベル

パートナーテナント（**すべてのカスタマー**）レベルでCyber Protectコンソールを使用する場合、カスタマイズされたビューが利用できます。

[アラート] および **[アクティビティ]** タブで、パートナー関連の追加フィルタが利用できます。一方、**[デバイス]** および **[管理]** タブからは、パートナー管理者がアクセスできる機能またはオブジェクトにのみアクセス可能です。

[アラート] タブ

ここでは、管理しているすべてのカスタマーからのアラートを確認および検索したり、以下の条件に従ってフィルタリングしたりすることができます。

- デバイス
- 顧客
- 計画

それぞれの条件に対して、複数の項目を選択できます。

[アクティビティ] タブ

ここでは、管理しているすべてのテナントのアクティビティ、または特定のカスタマーのテナントアクティビティを確認できます。

カスタマー、ステータス、時間、タイプでアクティビティをフィルタリングできます。

このレベルでは、以下のタイプのアクティビティが自動的に事前選択されます。

- 計画の適用
- 保護計画の作成
- 保護計画
- 計画の取り消し
- スクリプト処理

[デバイス] タブ

[エージェントがインストールされているマシン] タブでは、管理対象のカスタマーテナントに属するすべてのワークロードが表示され、1つまたは複数のテナントからワークロードを選択することができます。また、複数のテナントのワークロードを含むデバイスグループを作成することもできます。

重要
パートナー（**すべてのカスタマー**）レベルで作業する場合、デデバイスに対して実行できる操作には制限があります。例えば、以下の操作は実行できません。

- 顧客のデバイス上の既存の保護計画を確認および管理する。
- 新しい保護計画を作成する。
- バックアップを復元する。
- ディザスタリカバリを使用する。
- Cyber Protection Desktopの機能を使用する。

これらの操作を行うには、カスタマーレベルで作業します。

[ソフトウェア管理] タブ

カスタマーのワークロードに対してソフトウェアインベントリースキャンが有効な場合、ソフトウェアのスキャンの結果を確認できます。

特定の顧客のワークロードを表示する

パートナー管理者は、自分が管理するカスタマーテナントに属するワークロードを表示できます。

特定の顧客のワークロードを表示するには

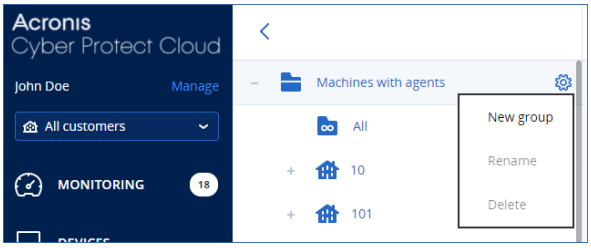
1. Cyber Protectコンソールで **[デバイス]** > **[エージェントがインストールされているマシン]** に進みます。
2. ツリーで **[エージェントがインストールされているマシン]** をクリックしてリストを展開します。
3. ワークロードを表示・管理する顧客の名前をクリックします。

パートナーレベルの静的デバイスグループ作成

パートナー（**すべてのデバイス**）レベルで静的デバイスグループを作成できます。

パートナーレベルで静的デバイスグループを作成するには

1. Cyber Protectコンソールで **[デバイス]** > **[エージェントがインストールされているマシン]** に進みます。
2. **[エージェントがインストールされているマシン]** の横にあるギアアイコンをクリックしてから、**[新しいグループ]** をクリックします。



3. グループの名前を指定します。
4. （オプション） 説明を追加します。
5. **[OK]** をクリックします。

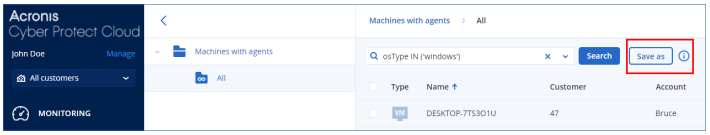
パートナーレベルの動的デバイスグループ作成

パートナー（**すべてのデバイス**）レベルで動的デバイスグループを作成できます。

パートナーレベルで動的デバイスグループを作成するには

1. Cyber Protectコンソールで **[デバイス]** > **[エージェントがインストールされているマシン]** に進みます。
2. ツリーで **[エージェントがインストールされているマシン]** をクリックしてリストを展開します。
3. **[すべて]** をクリックします。
4. 検索フィールドで動的デバイスグループを作成する条件を指定してから、**[検索]** をクリックします。

   利用可能な検索条件の詳細については、"非クラウドツークラウドワークロードの属性を検索する"（337ページ）および"クラウドツークラウドワークロードの属性を検索する"（336ページ）を参照してください。
5. **[名前を付けて保存]** をクリックしてから、グループの名前を指定します。



6. （オプション） 説明を追加します。
7. **[OK]** をクリックします。

パートナーテナントレベルでのマシンの自動検出の実行

パートナーテナント（**すべてのカスタマー**）レベルでマシンの自動検出を実行できます。

前提条件

顧客のローカルネットワークまたはActive Directoryドメイン内に、プロテクションエージェントがインストールされたマシンが1台以上ある。

重要

Windowsマシンにインストールされたエージェントのみが、ディスカバリーエージェントにできます。顧客の環境にディスカバリーエージェントがない場合、**[デバイスの追加]** パネルの**[複数のデバイス]** オプションを使用できません。

エージェントサービスの実行には、追加の許可が必要となるため、ドメインコントローラー追加時の自動検出はサポートされていません。

エージェントのリモートインストールは、Windowsを搭載したマシンでのみサポートされています（Windows XPはサポートされていません）。Windows Server 2012 R2を実行しているマシンでリモートインストールを実行するには、このマシンにWindows Update KB2999226をインストールする必要があります。

パートナーテナントレベルでマシンの自動検出を実行するには

1. Cyber Protect コンソールで、**[すべてのカスタマー]** を選択します。
2. **[デバイス]** > **[すべてのデバイス]** に移動します。
3. **[追加]** をクリックします。
4. **[複数のデバイス]** で、**[Windowsのみ]** をクリックします。検出ウィザードが開きます。
5. 顧客テナントを選択し、マシン検出のスキャンを実行するディスカバリーエージェントを選択します。
6. 検出方法を選択します。
   - **Active Directoryを検索**。検出エージェントのあるマシンがActive Directoryドメインのメンバーであることを確認してください。
   - **ローカルネットワークをスキャン**。選択した検出エージェントでマシンを検出できなかった場合は、別の検出エージェントを選択してください。
   - **手動で指定するか、ファイルからインポート**。追加するマシンを手動で決定するか、テキストファイルからインポートします。
7. （検出方法にActive Directoryが選択されている場合）マシンの検索方法を選択します。
   - **組織単位（OU）リスト内**。追加するマシンのグループを選択します。
   - **LDAP言語クエリ**。LDAPダイアレクトクエリを使用してマシンを選択します。**[ベースを検索]** は検索する場所を指定します。**[フィルタ]** にはマシン選択の条件を指定できます。

8. 選択した検出方法に応じて、以下のいずれかのアクションを実行します。

検出方法	アクション
Active Directoryを検索	検出されたマシンの一覧から、追加するマシンを選択します。
ローカルネットワークをスキャン	検出されたマシンの一覧から、追加するマシンを選択します。

手動で指定するか、ファイルからインポート	マシンのIPアドレスかホスト名を指定します。または、テキストファイルからマシンリストをインポートします。ファイルには1行ごとにIPアドレス/ホスト名が含まれている必要があります。次にファイルの例を示します。
	`156.85.34.10`
	`156.85.53.32`
	`156.85.53.12`
	`EN-L00000100`
	`EN-L00000101`
	マシンのアドレスを手動で追加するか、ファイルからインポートした後、追加されたマシンに対してエージェントがpingを実行し、可用性を確認します。

9. 検出後に必ず実行するアクションを選択します。

オプション	説明
エージェントのインストールとマシンの登録	**[コンポーネントの選択]** をクリックして、マシンにインストールするコンポーネントを選択できます。詳細については、"インストールするコンポーネントの選択"（129ページ）を参照してください。
エージェント サービスのログオンアカウント	この設定は、**[コンポーネントの選択]**画面で使用できます。 この設定によって、サービスが実行されるアカウントが決まります。 次のいずれかのオプションを選択できます。 • **サービスユーザーアカウントを使用する**（エージェントサービスのデフォルト） サービスユーザーアカウントは、サービスの実行に使用される Windows のシステムアカウントです。この設定の利点は、ドメインのセキュリティポリシーがそれらのアカウントのユーザー権限に影響を及ぼさないことです。デフォルトでは、エージェントは**ローカルシステム**のアカウントで実行されます。 • **新しいアカウントを作成する** エージェントのアカウント名は「Agent User」になります。 • **次のアカウントを使用する** ドメインコントローラー上にエージェントをインストールする場合は、エージェントに既存のアカウント（または同じアカウント）を指定するようシステムから求められます。セキュリティ上の理由で、システムはドメインコントローラー上に新しいアカウントを自動

オプション	説明
	作成しません。 **[新しいアカウントを作成する]** または **[次のアカウントを使用する]** のオプションを選択する場合は、ドメインのセキュリティポリシーが、関連するアカウントの権限に影響を及ぼさないようにしてください。インストール中に割り当てられたユーザー権限がアカウントからなくなると、コンポーネントが不適切な動作をする、またはまったく動作しなくなる場合があります。
インストールされたエージェントでマシンを登録	マシンにエージェントが既にインストールされていて、Cyber Protectionでの登録のみ必要な場合、このオプションを使用します。マシンでエージェントが見つからない場合、**非管理**マシンとして追加されます。
非管理マシンとして追加	このオプションを選択すると、エージェントはマシンにインストールされません。コンソールでマシンを表示できるようになり、後からエージェントのインストールや登録を実行できます。
必要に応じてマシンを再起動	このオプションは、**[エージェントのインストールとマシンの登録]** が選択されていると表示されます。 このオプションを選択すると、インストールを完了するのに必要な回数だけ、マシンが再起動されます。 次のいずれかの場合に、マシンの再起動が必要になります。 • 前提条件のインストールが完了し、インストールを続行するには再起動が必要な場合。 • 前提条件のインストールが完了したが、インストール中に一部のファイルがロックされたため、再起動が必要な場合。 • インストールが完了したが、以前インストールされた他のソフトウェアの再起動が必要な場合。
ユーザーのログイン中は再起動しない	このオプションは、**[必要に応じてマシンを再起動]** が選択されている場合に表示されます。 このオプションを選択すると、ユーザーがシステムにログインしていれば、マシンは自動的に再起動されません。例えば、インストールで再起動が必要になったときにユーザーが作業中であれば、システムは再起動されません。 前提条件がインストールされているにもかかわらず、ユーザーがログイン中であるために再起動が実行されなかった場合は、エージェントのインストールを完了させるため、マシンを再起動してインストールを再度開始する必要があります。 エージェントがインストールされた後、マシンが再起動されなかった場合は、マシンを再起動する必要があります。
マシンを登録する場所のユーザー	（組織内にユニットがある場合）マシンを登録するユニットまたは下位ユニットのユーザーアカウントを選択します。 （パートナーテナントレベルで自動検出を実行する場合）管理するカスタマーテナントの一覧で、ツリー構造を展開し、マシンを登録するユーザーアカウントを選択します。 （顧客管理者として自動検出を実行する場合）**[エージェントのインストールとマシンの登**

オプション	説明
	録] または **イ[ンストールされたエージェントでマシンを登録**] を選択した場合、マシンに保護計画を適用するオプションもあります。複数の保護計画が存在する場合、使用するものを選択できます。

10. すべてのマシンに管理者権限を持つユーザーの資格情報を指定します。

重要
エージェントのリモートインストールが準備なしで機能するのは、組み込みの管理者アカウント（オペレーティングシステムのインストール時に最初に作成されたアカウント）の資格情報を指定した場合のみです。カスタム管理者の資格情報を定義する場合は、"前提条件"（314ページ）に記載された追加の準備手順を実行する必要があります。

11. すべてのマシンへの接続をシステムがチェックします。接続に失敗したマシンがある場合、それらのマシン用の資格情報を変更できます。

マシン検出起動後は、対応するタスクの状況を **[監視]** > **[アクティビティ]** > **[マシンの検出]** アクティビティで確認できます。

マルチテナントサポート

Cyber Protectionサービスはマルチテナントをサポートしており、以下のレベルで管理されます。

- （サービスプロバイダー向け）パートナーテナント（**すべてのカスタマー**）レベル
  このレベルは、カスタマーのテナントを管理するパートナー管理者のみが利用可能です。
- カスタマーテナントレベル
  このレベルは、社内管理者により管理されます。
  パートナー管理者は、自分が管理するカスタマーテナントでもこのレベルで作業できます。パートナー管理者は、このレベルにおいて、カスタマー管理者と同じ権限を有し、その代理として作業を実行できます。
- ユニットレベル
  このレベルは、ユニット管理者、および親カスタマーテナントの社内管理者によって管理されます。
  親カスタマーテナントを管理するパートナー管理者もこのユニットレベルにアクセスできます。パートナー管理者は、このレベルにおいて、カスタマー管理者と同じ権限を持ち、その代理として作業を実行できます。

管理者は、自分のテナントとその子テナント内のオブジェクトを管理できます。上位の管理者レベルのオブジェクトがある場合、そのオブジェクトを閲覧したりアクセスしたりすることはできません。

例えば社内管理者は、カスタマーテナントレベルとユニットレベルの両方で保護計画を管理できます。ユニット管理者は、ユニットレベルの自分の保護計画のみを管理できます。ユニット管理者は、カスタマーテナントレベルの保護計画を管理することはできず、カスタマー管理者がユニットレベルで作成した保護計画も管理することはできません。

また、パートナー管理者は、自分が管理するカスタマーテナントでスクリプト計画を作成し、適用することができます。このようなテナントの社内管理者の場合、パートナー管理者がワークロードに適用するスクリプト計画に対しては、読み取り専用のアクセス権のみが付与されています。一方、カスタマー管理者は、独自のスクリプトや保護計画を作成し、それらを適用することができます。

ワークロード

ワークロードとは、物理マシン、仮想マシン、メールボックス、データベースインスタンスなど、あらゆるタイプの保護対象リソースのことです。Cyber Protectコンソールでワークロードは、計画（保護計画、バックアップ計画、またはスクリプト計画）を適用できるオブジェクトとして表示されます。

ワークロードによっては、プロテクションエージェントをインストールするか、仮想アプライアンスを配置する必要があります。エージェントは、グラフィカルユーザーインターフェイスを使用してインストールすることも、コマンドラインインターフェイスを使用してインストールすることもできます（無人インストール）。無人インストールを使用すると、インストール手順を自動化できます。 プロテクションエージェントをインストールする方法については、"Cyber Protectionエージェントのインストールと配置"（58ページ）を参照してください。

仮想アプライアンス（VA）は、プロテクションエージェントを含む既製の仮想マシンです。仮想アプライアンスを使用すると、プロテクションエージェントをインストールすることなく、同じ環境内の他の仮想マシンをバックアップできます（エージェントレスバックアップ）。仮想アプライアンスは、.ovf、.ova、または.qcowなど、ハイパーバイザー固有の形式で提供されます。 どの仮想環境プラットフォームがエージェントレスバックアップをサポートしているかの詳細については、"サポートされる仮想環境プラットフォーム"（31ページ）を参照してください。

重要
エージェントは、少なくとも30日に1回はオンラインである必要があります。この条件を満たさない場合、計画は取り消され、ワークロードは保護対象ではなくなります。

ワークロードの種類とそれぞれのエージェントを、以下の表に示します。

ワークロードの種類	エージェント	例（非網羅的リスト）
物理コンピュータ	プロテクションエージェントは、保護されているマシンそれぞれにインストールされます。	ワークステーション ノートブック サーバー
仮想コンピュータ	仮想環境プラットフォームに応じて、以下のバックアップメソッドを利用できます: • エージェントベースのバックアップ - プロテクションエージェントは、すべての保護されているマシンにインストールされます。 • エージェントレスバックアップ - プロテクションエージェントは、	VMware仮想マシン Hyper-V仮想コンピュータ カーネルベースの

ワークロードの種類	エージェント	例 （非網羅的リスト）
	ハイパーバイザーホストまたは専用仮想マシン上にインストールされるか、仮想アプライアンスとして配置されます。このエージェントでは、環境内のすべての仮想マシンがバックアップされます。	仮想マシン（KVM）は、oVirtにより管理されます。
Microsoft 365 Business ワークロード Google Workspace ワークロード	これらのワークロードは、インストール不要のクラウドエージェントによってバックアップされます。 クラウドエージェントを使用するには、Cyber Protectコンソールに Microsoft 365またはGoogle Workspace組織を追加する必要があります。 さらに、ローカルのOffice 365エージェントも利用可能です。これはインストールが必要で、Exchange Onlineのメールボックスのバックアップにのみ使用できます。 ローカルエージェントとクラウドエージェントの違いについては、"Microsoft 365データの保護"（584ページ）を参照してください。 .	Microsoft 365メールボックス Microsoft 365 OneDrive Microsoft Teams SharePointサイト Googleメールボックス Google Drive
アプリケーション	特定のアプリケーションのデータは、SQLエージェント、Exchangeエージェント、MySQL/MariaDBエージェント、Active Directoryエージェントなどの専用エージェントによってバックアップされます。	SQL Serverデータベース MySQL/MariaDB データベース Oracle データベース Active Directory
モバイル デバイス	モバイルアプリは、保護対象のデバイスにインストールされます。	AndroidまたはiOS デバイス
Web サイト	これらのWebサイトは、インストール不要のクラウドエージェントによってバックアップされます。	SFTPまたはSSHプロトコルでアクセスしたWeb サイト

必要なエージェントの種類とインストール先については、"エージェント"（61ページ）を参照してください

Cyber Protectコンソールにワークロードを追加する

ワークロードの保護を開始するには、まず対象のワークロードをCyber Protectコンソールに追加します。

注意
アカウントのサービスクォータに応じて、追加できるワークロードのタイプが異なります。特定のワークロードのタイプが見つからない場合、**デバイスの追加**ペインでグレイアウトされています。

パートナー管理者は、管理ポータルで必要なサービスクォータを有効化できます。詳細については、"パートナー管理者への情報"（325ページ）を参照してください。

ワークロードを追加するには

1. Cyber Protectコンソールにログインします。
2. **[デバイス]** > **[すべてのデバイス]** に進み、**[追加]** をクリックします。
   右側に **[デバイスの追加]** ペインが開きます。
3. リリースチャンネルを選択します。
4. 追加したいワークロードタイプをクリックし、選択した特定のワークロードの指示に従います。

次の表に、ワークロードのタイプと必要な操作を示します。

追加するワークロード	必要な操作	必要な手順
複数のWindowsマシン	現在の環境で自動検出を実行します。 自動検出を実行するには、ローカルネットワークまたはActive Directoryドメイン内に、プロテクションエージェントがインストールされたマシンが1台または複数台必要です。このエージェントは、検出エージェントとして使用されます。	"自動検出と手動検出の実行"（124ページ）
Windowsワークステーション Windowsサーバー	Windowsエージェントをインストールします。	"Windowsでプロテクションエージェントをインストールする"（76ページ） または、 "Windows での無人インストールまたはインストール解除"（86ページ）
macOSワークステーション	macOSエージェントをインストールします。	"macOSでプロテクションエージェントをインストールする"（81ページ） または、 "macOSの無人インストールとインストール解除"（109ページ）
Linuxサーバー	Linuxエージェントをインストールします。	"Linuxでプロテクションエージェントをインストールする"（79ページ） または、 "Linux での無人インストールまたは

追加するワークロード	必要な操作	必要な手順
		インストール解除"（103ページ）
モバイル デバイス （iOS、Android）	モバイルアプリをインストールします。	"モバイル デバイスの保護"（577ページ）
クラウドツークラウドワークロード		
Microsoft 365 Business	Cyber ProtectコンソールにMicrosoft 365組織を追加し、クラウドエージェントを使用して、Exchange Onlineのメールボックス、OneDriveファイル、Microsoft Teams、SharePointサイトを保護します。 または、ローカルのOffice 365エージェントをインストールすることもできます。Exchange Onlineメールボックスのバックアップのみを提供します。 ローカルエージェントとクラウドエージェントの違いについては、"Microsoft 365データの保護"（584ページ）を参照してください。	"Microsoft 365データの保護"（584ページ）
Google Workspace	Google Workspace組織をCyber Protectコンソールに追加し、クラウドエージェントを使用してGmailメールボックスとGoogleドライブファイルを保護します。	"Google Workspaceデータの保護"（625ページ）
仮想コンピュータ		
VMware ESXi	現在の環境にVMwareエージェント（仮想アプライアンス）を配置します。	"エージェント for VMware（仮想アプライアンス）の配置"（132ページ）
	VMwareエージェント（Windows）をインストールします。	"Windowsでプロテクションエージェントをインストールする"（76ページ） または、 "Windows での無人インストールまたはインストール解除"（86ページ）
Virtuozzo Hybrid Infrastructure	Virtuozzo Hybrid Infrastructureエージェント （仮想アプライアンス）を現在の環境に配置します。	"Virtuozzo Hybrid Infrastructureエージェント（仮想アプライアンス）の配置"（141ページ）
Hyper-V	Hyper-Vエージェントをインストールしま	"Windowsでプロテクションエージェ

追加するワークロード	必要な操作	必要な手順
	す。	ントをインストールする"（76ページ） または、 "Windows での無人インストールまたはインストール解除"（86ページ）
Virtuozzo	Virtuozzoエージェントをインストールします。	"Linuxでプロテクションエージェントをインストールする"（79ページ） または、 "Linux での無人インストールまたはインストール解除"（103ページ）
KVM	Windowsエージェントをインストールします。	"Windowsでプロテクションエージェントをインストールする"（76ページ） または、 "Windows での無人インストールまたはインストール解除"（86ページ）
	Linuxエージェントをインストールします。	"Linuxでプロテクションエージェントをインストールする"（79ページ） または、 "Linux での無人インストールまたはインストール解除"（103ページ）
Red Hat仮想環境（oVirt）	現在の環境にoVirtエージェント（仮想アプライアンス）を配置します。	"oVirt（仮想アプライアンス）エージェントをデプロイ中"（149ページ）
Citrix XenServer	Windowsエージェントをインストールします。	"Windowsでプロテクションエージェントをインストールする"（76ページ） または、 "Windows での無人インストールまたはインストール解除"（86ページ）
	Linuxエージェントをインストールします。	"Linuxでプロテクションエージェントをインストールする"（79ページ） または、 "Linux での無人インストールまたはインストール解除"（103ページ）
Nutanix AHV	Windowsエージェントをインストールし	"Windowsでプロテクションエージェ

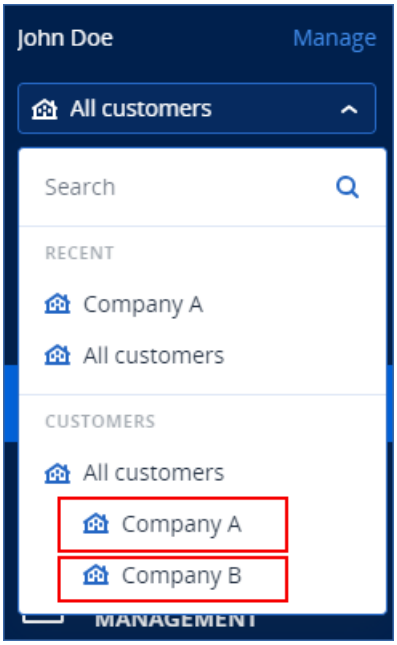
追加するワークロード	必要な操作	必要な手順
	ます。	ントをインストールする"（76ページ） または、 "Windows での無人インストールまたはインストール解除"（86ページ）
	Linuxエージェントをインストールします。	"Linuxでプロテクションエージェントをインストールする"（79ページ） または、 "Linux での無人インストールまたはインストール解除"（103ページ）
Oracle VM	Windowsエージェントをインストールします。	"Windowsでプロテクションエージェントをインストールする"（76ページ） または、 "Windows での無人インストールまたはインストール解除"（86ページ）
	Linuxエージェントをインストールします。	"Linuxでプロテクションエージェントをインストールする"（79ページ） または、 "Linux での無人インストールまたはインストール解除"（103ページ）
Scale Computing HC3	現在の環境にScale Computing HC3エージェント（仮想アプライアンス）を配置します。	"Scale Computing HC3 エージェント（仮想アプライアンス）の配置"（136ページ）
ネットワーク接続ストレージ		
Synology	現在の環境にSynologyエージェント（仮想アプライアンス）を配置します。	"Synologyエージェントの配置"（155ページ）
アプリケーション		
Microsoft SQL Server	SQLエージェントをインストールします。	"Windowsでプロテクションエージェントをインストールする"（76ページ） または、 "Windows での無人インストールまたはインストール解除"（86ページ）
Microsoft Exchange Server	Exchangeエージェントをインストールします。	
Microsoft Active Directory	Active Directoryエージェントをインストールします。	
Oracleデータベース	Oracleエージェントをインストールしま	"Oracle データベースの保護"（650

追加するワークロード	必要な操作	必要な手順
	す。	ページ）
Web サイト	Webサイトへの接続を構成します。	"Webサイトとホスティングサーバーの保護"（657ページ）

利用可能なプロテクションエージェントとインストールロケーションについては、"エージェント"（61ページ）を参照してください

パートナー管理者への情報

- 必要なサービスクォータが管理ポータルで有効になっていない場合、ワークロードタイプが**デバイスの追加**ペインに表示されないことがあります。各ワークロードに必要なサービスクォータの詳細については、パートナー管理者ガイドの「提供項目の有効化/無効化」を参照してください。
- パートナー管理者として、**すべてのカスタマー**レベルでワークロードを追加することはできません。ワークロードを追加するには、各カスタマーテナントを選択します。



Cyber Protectコンソールからワークロードを削除する

保護する必要がなくなったワークロードは、Cyber Protectコンソールから削除できます。この手順はワークロードのタイプによって異なります。

または、保護対象のワークロード上でエージェントをアンインストールすることもできます。エージェントをアンインストールすると、保護対象のワークロードは自動的にCyber Protectコンソールから削除されます。

重要

Cyber Protectコンソールからワークロードを削除すると、そのワークロードに適用されているすべての計画が取り消されます。ワークロードを削除しても、計画やバックアップは削除されず、プロテクションエージェントはアンインストールされません。

次の表に、ワークロードのタイプと必要な操作を示します。

削除するワークロード	必要な操作	必要な手順
物理マシンと仮想マシン		
プロテクションエージェントがインストールされた物理または仮想マシン	1. Cyber Protectコンソールからワークロードを削除します。 2. （オプション）プロテクションエージェントをアンインストールします。	"Cyber Protectコンソールからワークロードを削除するには"（328ページ） （プロテクションエージェントを含むワークロード）
ハイパーバイザーレベルでバックアップされる仮想マシン（エージェントレスバックアップ）	1. Cyber Protectコンソールで、プロテクションエージェントがインストールされたマシンを削除します。このエージェントによってバックアップされたすべての仮想マシンは、コンソールから自動的に削除されます。 2. （オプション）プロテクションエージェントをアンインストールします。	"Cyber Protectコンソールからワークロードを削除するには"（328ページ） （プロテクションエージェントを含まないワークロード）
クラウドツークラウドワークロード		
Microsoft 365 Businessワークロード Google	Cyber ProtectコンソールからMicrosoft 365またはGoogle Workspace組織を削	"Cyber Protectコンソールからワークロードを削除するには"（328ページ） （クラウドツークラウドワークロード）

削除するワークロード	必要な操作	必要な手順
Workspaceワークロード	除します。該当する組織のすべてのリソースは、コンソールから自動的に削除されます。	
モバイル デバイス		
Androidデバイス iOSデバイス	1. Cyber Protectコンソールからモバイルデバイスを削除します。 2. （オプション）モバイルデバイスでアプリをアンインストールします。	"Cyber Protectコンソールからワークロードを削除するには"（328ページ） （モバイルデバイス）
ネットワーク接続ストレージ		
Synology	1. Cyber Protectコンソールからワークロードを削除します。 2. （オプション）プロテクションエージェントをアンインストールします。	"Cyber Protectコンソールからワークロードを削除するには"（328ページ） （プロテクションエージェントを含むワークロード）
アプリケーション		
Microsoft SQL Server Microsoft Exchange Server Microsoft Active Directory Oracleデータベース	1. Cyber Protectコンソールで、プロテクションエージェントがインストールされたマシンを削除します。このエージェントによってバックアップされたオブジェクトは、コンソールから自動的に削除されます。 2. （オプション）	"Cyber Protectコンソールからワークロードを削除するには"（328ページ） （プロテクションエージェントを含まないワークロード）

削除するワークロード	必要な操作	必要な手順
	プロテクションエージェントをアンインストールします。	
Web サイト	Cyber Protectコンソールから Webサイトを削除します。	"Cyber Protectコンソールからワークロードを削除するには"（328ページ） （Webサイト）

Cyber Protectコンソールからワークロードを削除するには

プロテクションエージェントを含むワークロード

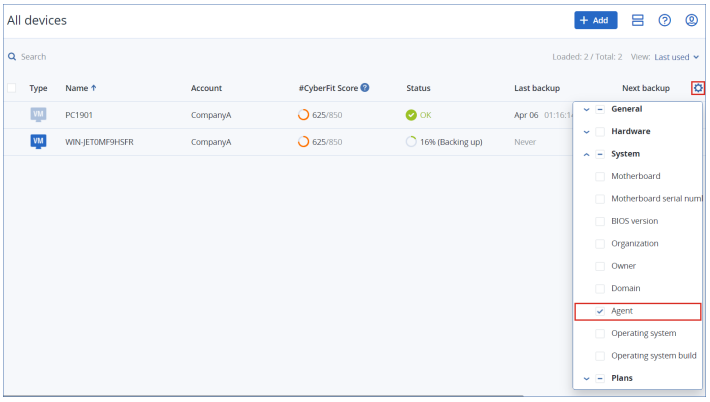
このワークロードのタイプを直接削除できます。

1. Cyber Protectコンソールで、**[デバイス]** > **[すべてのデバイス]** に進みます。
2. 削除対象である、1つまたは複数のワークロードの横にあるチェックボックスを選択します。
3. **[操作]** ペインで、**[削除]** をクリックします。
4. **[削除]** をクリックしてこの選択内容を確認します。
5. （オプション） エージェントをアンインストールします（"エージェントのアンインストール"（176ページ）を参照）。

プロテクションエージェントを含まないワークロード

このワークロードのタイプを削除するには、プロテクションエージェントがインストールされたマシンを削除する必要があります。

1. Cyber Protectコンソールで **[デバイス]** > **[すべてのデバイス]** に進みます。
2. 右上にあるギアアイコンをクリックしてから、**[エージェント]** チェックボックスを選択します。



エージェント列が表示されます。

3. **エージェント**列で、プロテクションエージェントがインストールされているマシンの名前をチェックします。
4. Cyber Protectコンソールで、プロテクションエージェントがインストールされたマシンの横にあるチェックボックスを選択します。

5. **[操作]** ペインで、**[削除]** をクリックします。
6. **[削除]** をクリックしてこの選択内容を確認します。
7. （オプション） エージェントをアンインストールします（"エージェントのアンインストール"（176 ページ）を参照）。

クラウドツークラウドワークロード

クラウドエージェントによってバックアップされたワークロードを削除するには、Cyber Protectコンソールから Microsoft 365または Google Workspace組織を削除します。

1. Cyber Protectコンソールで、**[デバイス]** > **[Microsoft 365]** または **[デバイス]** > **[Google Workspace]** に移動します。
2. Microsoft 365または Google Workspace組織の名前をクリックします。
3. **[操作]** ペインで、**[グループを削除]** をクリックします。
4. **[削除]** をクリックして、操作を確定します。

モバイルデバイス

1. Cyber Protectコンソールで、**[デバイス]** > **[すべてのデバイス]** に進みます。
2. 削除対象であるワークロードの横にあるチェックボックスを選択します。
3. **[操作]** ペインで、**[削除]** をクリックします。
4. **[削除]** をクリックしてこの選択内容を確認します。
5. （オプション） モバイルデバイスからアプリをアンインストールします。

Web サイト

1. Cyber Protectコンソールで、**[デバイス]** > **[すべてのデバイス]** に進みます。
2. 削除対象であるワークロードの横にあるチェックボックスを選択します。
3. **[操作]** ペインで、**[削除]** をクリックします。
4. **[削除]** をクリックしてこの選択内容を確認します。

デバイスグループ

デバイスグループを使用すると、グループ計画で複数の類似したワークロードを保護することができます。この計画はグループ全体に適用され、グループのメンバーから取り消すことはできません。

1つのワークロードを複数のグループのメンバーにすることができます。デバイスグループに含まれるワークロードも、個別の計画で保護できます。

デバイスグループには、同じ種類のワークロードのみを追加できます。例えば、**[Hyper-V]**では、Hyper-V仮想マシンのグループのみを作成できます。**[エージェントがインストールされているマシン]** では、エージェントがインストールされているマシンのグループのみを作成できます。

すべてのタイプのグループ（ルートグループの**すべてのデバイス**、または**[エージェントがインストールされているマシン]** > **[すべて]**、**[Microsoft 365]** > （自分の組織） > **[ユーザー]** > **[すべてのユーザー]** などのビルトイングループ）内にデバイスグループを作成することはできません。

ビルトイングループとカスタムグループ

ビルトイングループ

Cyber Protectコンソールでワークロードを登録すると、ワークロードは、**[デバイス]** タブのビルトインルートグループのいずれか（**エージェントがインストールされているマシン**、**Microsoft 365**、または **Hyper-V**）に表示されます。

登録されたすべての非クラウドツークラウドワークロードは、**[すべてのデバイス]** ルートグループにも表示されます。テナントの名前を付けた別のビルトインルートグループには、クラウドツークラウド以外のすべてのワークロードとこのテナント内のすべてのユニットが含まれます。

ルートグループを削除また編集することはできません。またルートグループに計画を適用することもできません。

ルートグループの中には、1つまたは複数のレベルのビルトインサブグループが含まれるものがあります。**[エージェントがインストールされているマシン]** > **[すべて]**、**[Microsoft 365]** > （自分の組織） > **[Teams]** > **[すべてのチーム]**、**[Google Workspace]** > （自分の組織） > **[共有デバイス]** > **[すべての共有デバイス]** などです。

ビルトインサブグループを編集または削除することはできません。

カスタム グループ

異なる保護設定や保護スケジュールを必要とするワークロードが存在する可能性があるため、ビルトイングループ内のすべてのワークロードを保護するという方法が有効でない場合があります。

ルートグループの一部、例えば**エージェントがインストールされているマシン**、**Microsoft 365**、**Google Workspace**で、カスタムサブグループを作成することができます。これらのサブグループには、静的なものと動的なものがあります。

カスタムグループは、編集、名前の変更、削除が可能です。

静的グループとダイナミックグループ

以下の種類のカスタムグループを作成できます。

- 固定
- 動的

静的グループ

静的グループには、手動で追加したワークロードが含まれます。

静的グループのコンテンツは、ワークロードを明示的に追加または削除したときにのみ変更されます。

例:自社の経理部門向けの静的グループを作成し、経理担当者のマシンをこのグループに手動で追加します。グループ計画を適用すると、そのグループ内のマシンが保護されるようになります。新しい経理担当者が入社した場合は、新しい担当者のマシンを手動で静的グループに追加する必要があります。

ダイナミックグループ

ダイナミックグループには、特定の条件に一致するワークロードが含められます。これらの条件は、属性（例: `OsType`）、その値（例: `Windows`）、および検索演算子（例: `IN`）を含む検索クエリを作成することであらかじめ定義しておきます。

これにより、Windowsオペレーティングシステムが動作するすべてのマシンのダイナミックグループや、Microsoft 365組織でEメールアドレスが`john`で始まるすべてのユーザーを含むダイナミックグループなどを作成できます。

合致する属性と値を持つすべてのワークロードは自動的にグループに追加され、そのような属性または値を失ったワークロードは自動的にグループから削除されます。

例 1:経理部門に属するマシンのホスト名には、経理という単語が含まれています。名前に経理が含まれるマシンを検索し、検索結果をダイナミックグループとして保存します。その後、保護計画をこのグループに適用します。新しい経理担当者が入社した場合、その経理担当者のマシンの名前には経理という名前が含められ、Cyber Protectコンソールでそのマシンを登録すると同時に、自動的にダイナミックグループに追加されます。

例 2:経理部門が独立したActive Directoryの組織単位（OU）を確立しました。経理のOUを必須属性として指定し、検索結果をダイナミックグループとして保存します。その後、保護計画をこのグループに適用します。新しい経理担当者が入社した場合は、担当者のマシンがActive Directory OUに追加され、Cyber Protectコンソールに登録されると同時に、ダイナミックグループに追加されます（操作の順番を問わず）。

クラウドツークラウドグループと非クラウドツークラウドグループ

クラウドツークラウドグループには、クラウドエージェントによってバックアップされたMicrosoft 365やGoogle Workspaceのワークロードが含まれています。

非クラウドツークラウドグループには、その他のすべてのワークロードタイプが含まれます。

デバイスグループでサポートされている計画

次の表は、デバイスグループに適用できる計画をまとめたものです。

グループ	適用可能な計画	計画のロケーション
クラウドツークラウドワークロード（Microsoft 365およびGoogle Workspaceワークロード）	バックアップ計画	**[管理]** > **[クラウドアプリケーションバックアップ]**
非クラウドツークラウドワークロード	保護計画	**[管理]** > **[保護計画]**
	リモート管理計画	**[管理]** > **[リモート管理計画]**
	スクリプト計	**[管理]** > **[スクリプト計画]**

グループ	適用可能な計画	計画のロケーション
	画	

Microsoft 365またはGoogle Workspace組織をコンソールに追加すると、Microsoft 365/Google Workspaceユーザー、OneDrive/Google Drive共有、Microsoft Teams、またはAzure ADグループなどのクラウドリソースが、すぐにCyber Protectコンソールに同期されるようになります。それ以降に組織の変更があった場合は、1日に1回実行される同期で反映されます。

変更をすぐに同期する必要がある場合は、Cyber Protectコンソールで、**[デバイス]** > **[Microsoft 365]** または **[デバイス]** > **[Google Workspace]** に移動して、必要な組織を選択し、**[リフレッシュ]** をクリックします。

静的グループの作成

空の静的グループを作成し、そこにワークロードを追加できます。

また、ワークロードを選択し、選択したワークロードから新しい静的グループを作成することもできます。

すべてのタイプのグループ（ルートグループの**すべてのデバイス**、または**[エージェントがインストールされているマシン]** > **[すべて]**、**[Microsoft 365]** > （自分の組織） > **[ユーザー]** > **[すべてのユーザー]** などのビルトイングループ）内にデバイスグループを作成することはできません。

静的グループの作成するには

メインウィンドウで:

1. **[デバイス]** をクリックして、新しい静的グループを作成するワークロードを含むルートグループを選択します。
2. （オプション） ネストされたグループを作成するには、既存の静的グループに移動します。

   注意
   ネストされた静的グループの作成は、クラウドツークラウドワークロードでは利用できません。

3. グループツリー以下の **[+新しい静的グループ]** をクリックするか、**[操作]** ペインで **[新しい静的グループ]** をクリックします。
4. 新しいグループ名を指定します。
5. （オプション） グループのコメントを追加します。
6. **[OK]** をクリックします。

グループツリーで:

1. **[デバイス]** をクリックして、新しい静的グループを作成するワークロードを含むルートグループを選択します。
2. 静的グループを作成するグループの名前の横にある、ギアアイコンをクリックします。

注意
ネストされた静的グループの作成は、クラウドツークラウドワークロードでは利用できません。

3. **[新しい静的グループ]** をクリックします。
4. 新しいグループ名を指定します。
5. （オプション） グループのコメントを追加します。
6. **[OK]** をクリックします。

選択項目から:

1. **[デバイス]** をクリックして、新しい静的グループを作成するワークロードを含むルートグループを選択します。

注意
すべてのタイプのグループ（ルートグループの**すべてのデバイス**、または**[エージェントがインストールされているマシン]** > **[すべて]**、**[Microsoft 365]** > （自分の組織） > **[ユーザー]** > **[すべてのユーザー]** などのビルトイングループ）内にデバイスグループを作成することはできません。

2. 新しく作成するグループに対応するワークロードの横のチェックボックスを選択し、**[グループに追加]** をクリックします。
3. フォルダツリーで、新しいグループの親レベルを選択し、**[新しい静的グループ]** をクリックします。

注意
ネストされた静的グループの作成は、クラウドツークラウドワークロードでは利用できません。

4. 新しいグループ名を指定します。
5. （オプション） グループのコメントを追加します。
6. **[OK]** をクリックします。
   新しいグループがフォルダツリーに表示されます。
7. **[完了]** をクリックします。

静的グループへのワークロードの追加

最初にターゲットグループを選択し、そのグループにワークロードを追加できます。

または、最初にワークロードを選択してから、グループに追加することも可能です。

静的グループにワークロードを追加するには

最初にターゲットグループを選択

1. **[デバイス]** をクリックし、ターゲットグループに移動します。
2. ターゲットグループを選択してから、**[デバイスを追加]** をクリックします。
3. フォルダツリーで、必要なワークロードを含むグループを選択します。
4. 追加するワークロードの横のチェックボックスを選択し、**[追加]** をクリックします。

最初にワークロードを選択する

1. **[デバイス]** をクリックして、必要なワークロードを含むルートグループを選択します。
2. 追加するワークロードの横のチェックボックスを選択し、**[グループに追加]** をクリックします。
3. フォルダツリーでターゲットグループを選択してから、**[完了]** をクリックします。

ダイナミックグループの作成

検索クエリで定義した特定の属性を持つワークロードを検索して、ダイナミックグループを作成します。検索結果をダイナミックグループとして保存します。

ダイナミックグループの検索と作成にサポートされている属性は、クラウドツークラウドワークロードと非クラウドツークラウドワークロードで異なります。サポートされている属性の詳細については、「"非クラウドツークラウドワークロードの属性を検索する"（337ページ）」および「"クラウドツークラウドワークロードの属性を検索する"（336ページ）」を参照してください。

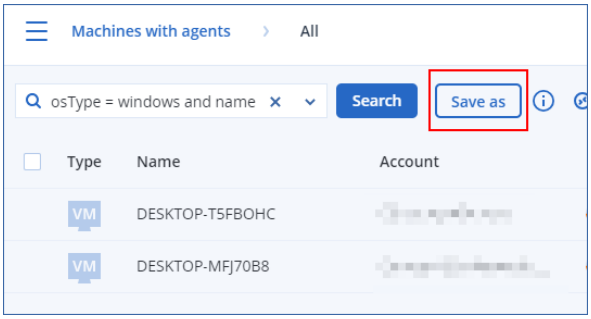
ダイナミックグループは、それぞれのルートグループに作成されます。ネストされたダイナミックグループはサポート対象外です。

すべてのタイプのグループ（ルートグループの**すべてのデバイス**、または**[エージェントがインストールされているマシン]** > **[すべて]**、**[Microsoft 365]** >（自分の組織）> **[ユーザー]** > **[すべてのユーザー]** などのビルトイングループ）内にデバイスグループを作成することはできません。

ダイナミックグループを作成するには

非クラウドツークラウドワークロード

1. **[デバイス]** をクリックして、新しいダイナミックグループを作成するワークロードを含むグループを選択します。
2. サポートされている検索属性と演算子を使用して、ワークロードを検索します。
   単一のクエリで、次の複数の属性および演算子を使用できます。サポートされている属性の詳細については、「"非クラウドツークラウドワークロードの属性を検索する"（337ページ）」を参照してください。
3. 検索フィールドの横の **[名前を付けて保存]** をクリックします。



注意

特定のレベルでダイナミックグループを作成することが許可されていない場合、例えば、ルート グループで **[デバイス]** > **[すべてのデバイス]** で、**[名前を付けて保存]** ボタンは使用できません。

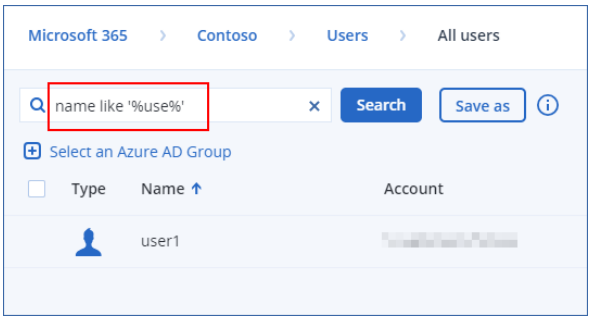
別のレベル（ **[デバイス]** > **[エージェントがインストールされているマシン]** >**[すべて]**など）を選択し、上記の手順を繰り返します。この検索では、**[エージェントがインストールされているマシン]** > **[すべて]** 内ではなく、**[エージェントがインストールされているマシン]** 内でダイナミックグループを作成できます。

4. 新しいグループ名を指定します。
5. （オプション） **[コメント]** フィールドに、新しいグループの説明を追加します。
6. **[OK]** をクリックします。

クラウドツークラウドワークロード

1. **[デバイス]** をクリックし、**[Microsoft 365]** または **[Google Workspace]** を選択します。
2. 新しいダイナミックグループを作成するワークロードを含むグループ（**[ユーザー]** > **[すべてのユーザー]**など）を選択します。
3. サポートされている検索属性と演算子を使用するか、特定のActive DirectoryグループからMicrosoft 365ユーザーを選択して、ワークロードを検索します。

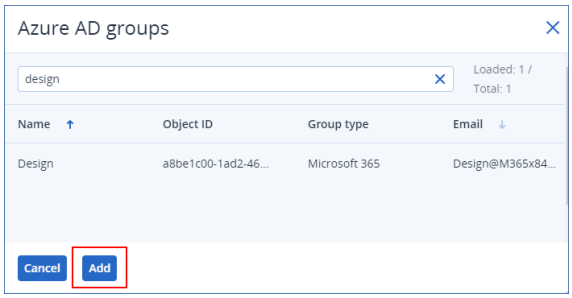
   単一のクエリで、次の複数の属性および演算子を使用できます。サポートされている属性の詳細については、「"クラウドツークラウドワークロードの属性を検索する"（336ページ）」を参照してください。



4. （**[Microsoft 365]** > **[ユーザー]** のみ）特定のActive Directoryグループからユーザーを選択するには、次の操作を実行します。
   a. **[ユーザー]** > **[すべてのユーザー]** に移動します。
   b. **[Azure ADグループを選択]** をクリックします。

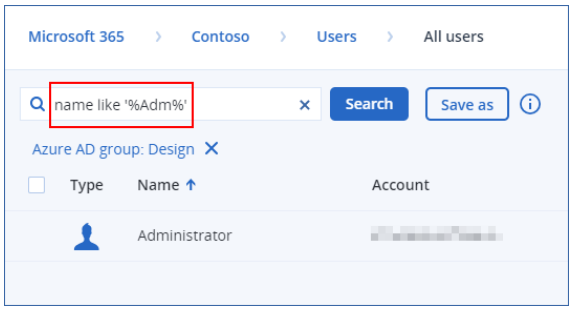
      組織内のActive Directoryグループのリストが開きます。

      このリストでは、特定のグループを検索したり、名前またはEメールでグループを並べ替えたりできます。
   c. 必要なActive Directoryグループを選択し、**[追加]** をクリックします。



d. （オプション） 選択したActive Directoryグループで特定のユーザーを含めたり除外したりするには、サポートされている検索属性と演算子を使用して検索クエリを作成します。

単一のクエリで、次の複数の属性および演算子を使用できます。サポートされている属性の詳細については、「"クラウドツークラウドワークロードの属性を検索する"（336ページ）」を参照してください。



5. 検索フィールドの横の **[名前を付けて保存]** をクリックします。

注意

特定のレベルでダイナミックグループを作成することが許可されていない場合、例えば、ルート グループの **[Microsoft 365]** > 自分の組織 > **[ユーザー]** などで、**[名前を付けて保存]** は使用できません。

別のレベル（**[Microsoft 365]** > 自分の組織 > **[ユーザー]** > **[すべて]**など）を選択し、上記の手順を繰り返します。この検索では、**[ユーザー]** > **[すべて]** 内ではなく、**[Microsoft 365]** > 自分の組織 > **[ユーザー]** 内でダイナミックグループを作成できます。

6. 新しいグループ名を指定します。
7. （オプション） **[コメント]** フィールドに、新しいグループの説明を追加します。
8. **[OK]** をクリックします。

クラウドツークラウドワークロードの属性を検索する

次の表は、Microsoft 365およびGoogle Workspaceワークロードの検索クエリで使用できる属性をまとめたものです。

他の種類のワークロードが検索クエリでどの属性を使用できるかについては、"非クラウドツークラウドワークロードの属性を検索する"（337ページ）を参照してください。

属性	意味	以下で使用できます:	検索クエリの例	グループ作成でサポートされているか
name	Microsoft 365またはGoogle Workspaceのワークロードの表示名	すべてのクラウドツークラウドリソース	name = 'My Name' name LIKE '*nam*'	はい
email	Microsoft 365ユーザー/グループ、またはGoogle Workspaceユーザーのメールアドレス	Microsoft 365 > グループ Microsoft 365 > ユーザー Google Workspace > ユーザー	email = 'my_group_email@mycompany.com' email LIKE '*@company*' email NOT LIKE '*enterprise.com'	はい
siteName	Microsoft 365グループに関連付けられたサイトの名前	Microsoft 365 > グループ	siteName = 'my_site' siteName LIKE '*company.com*support*'	はい
url	Microsoft 365グループまたはSharePointサイトのWebアドレス	Microsoft 365 > グループ Microsoft 365 > サイトコレクション	url = 'https://www.mycompany.com/' url LIKE '*www.mycompany.com*'	はい

非クラウドツークラウドワークロードの属性を検索する

次の表は、非クラウドツークラウドワークロードの検索クエリで使用できる属性をまとめたものです。

クラウドツークラウドのワークロードの検索クエリでどの属性を使用できるかについては、"クラウドツークラウドワークロードの属性を検索する"（336ページ）を参照してください。

属性	意味	検索クエリの例	グループ作成でサポートされているか
一般			
name	ワークロードの名前の例: • 物理コンピュータのホスト名 • 仮想コンピュータの名前	name = 'en-00'	はい

属性	意味	検索クエリの例	グループ作成でサポートされているか
	• データベース名 • メールボックス用の電子メールアドレス		
id	デバイスID デバイスIDを取得するには、**[デバイス]** でデバイスを選択し、**[詳細]** > **[すべてのプロパティ]** をクリックします。 IDは [id] フィールドに表示されます。	id != '4B2A7A93-A44F-4155-BDE3-A023C57C9431'	はい
resourceType	ワークロードのタイプ。 設定可能な値: • 'machine' • 'exchange' • 'mssql_server' • 'mssql_instance' • 'mssql_database' • 'mssql_database_folder' • 'msexchange_database' • 'msexchange_storage_group' • 'msexchange_mailbox.msexchange' • 'msexchange_mailbox.office365' • 'mssql_aag_group' • 'mssql_aag_database' • 'virtual_machine.vmww' • 'virtual_machine.vmwesx' • 'virtual_host.vmwesx' • 'virtual_cluster.vmwesx' • 'virtual_appliance.vmwesx' • 'virtual_application.vmwesx' • 'virtual_resource_pool.vmwesx'	resourceType = 'machine' resourceType in ('mssql_aag_database', 'mssql_database')	はい

属性	意味	検索クエリの例	グループ作成でサポートされているか
	• 'virtual_center.vmwesx' • 'datastore.vmwesx' • 'datastore_cluster.vmwesx' • 'virtual_network.vmwesx' • 'virtual_data_center.vmwesx' • 'virtual_machine.vmww' • 'virtual_cluster.mshyperv' • 'virtual_machine.mshyperv' • 'virtual_host.mshyperv' • 'virtual_network.mshyperv' • 'virtual_folder.mshyperv' • 'virtual_data_center.mshyperv' • 'datastore.mshyperv' • 'virtual_machine.msvs' • 'virtual_machine.parallelsw' • 'virtual_host.parallelsw' • 'virtual_cluster.parallelsw' • 'virtual_machine.rhev' • 'virtual_machine.kvm' • 'virtual_machine.xen' • 'bootable_media'		
chassis	シャーシのタイプ。 設定可能な値: • laptop • desktop • server • other • unknown	chassis = 'laptop' chassis IN ('laptop', 'desktop')	はい
ip	IPアドレス（物理マシンのみ）。	ip RANGE ('10.250.176.1','10.250.176.50')	はい

属性	意味	検索クエリの例	グループ作成でサポートされているか

comment	デバイスへのコメント。これは、自動または手動で指定できます。
	
	デフォルト値:
	
	• Windowsを実行する物理マシンでは、Windowsのコンピューターの説明がコメントとして自動的にコピーされます。この値は15分間隔で同期されます。
	• その他のデバイスでは空白です。
	
	注意
	コメントフィールドに手動で追加したテキストがある場合、自動同期は無効になります。同期を再び有効にするには、このテキストをクリアします。
	
	現在のワークロードの自動同期コメントをリフレッシュするには、**Windowsサービス**のManaged Machine Serviceを再起動するか、コマンドプロンプトで次のコマンドを実行します。
	
	`net stop mms`
	
	`net start mms`
	
	デバイスのコメントを表示するには、**[デバイス]** からデバイスを選択し、**[詳細]** をクリックし、次に **[コメント]** セクションを見つけます。
	
	手動でコメントを追加または変
		`comment = 'important machine'`
		
		`comment = ''`（コメントのないすべてのマシン）
			はい

属性	意味	検索クエリの例	グループ作成でサポートされているか
	更するには、**[追加]** または **[編集]** をクリックします。 プロテクション エージェントがインストールされているデバイスの場合、2つの独立したコメントフィールドがあります。 • エージェントのコメント ◦ Windowsを実行する物理マシンでは、Windowsのコンピューターの説明がコメントとして自動的にコピーされます。この値は15分間隔で同期されます。 ◦ その他のデバイスでは空白です。 **注意** コメントフィールドに手動で追加したテキストがある場合、自動同期は無効になります。同期を再び有効にするには、このテキストをクリアします。 • デバイスのコメント ◦ エージェントのコメントが自動で指定されている場合、内容がデバイスのコメントにコピーされます。エージェントのコメントを手動で追加しても、デバイスのコメントにコピーされることはありません。 ◦ デバイスのコメントは、エージェントのコメントにコピーされません。		

属性	意味	検索クエリの例	グループ作成でサポートされているか
	デバイスには、いずれかまたは両方の指定済みコメントを付加できます。また、両方とも空白にして付加することもできます。両方のコメントが指定されている場合、デバイスのコメントが優先されます。 コメントを表示するには、**[設定]** > **[エージェント]** 以下からエージェントを含むデバイスを選択し、**[詳細]** をクリックしてから、**[コメント]** セクションを見つけます。 デバイスのコメントを表示するには、**[デバイス]** からデバイスを選択し、**[詳細]** をクリックし、次に **[コメント]** セクションを見つけます。 手動でコメントを追加または変更するには、**[追加]** または **[編集]** をクリックします。		
isOnline	ワークロードの可用性 設定可能な値: • true • false	isOnline = true	いいえ
hasAsz	セキュアゾーンの可用性 設定可能な値: • true • false	hasAsz = true	はい
tzOffset	協定世界時（UTC）からのタイムゾーンオフセット（分単位）。	tzOffset = 120 tzOffset > 120 tzOffset < 120	はい

属性	意味	検索クエリの例	グループ作成でサポートされているか
CPU、メモリ、ディスク			
cpuArch	CPUのアーキテクチャ。 設定可能な値: • 'x64' • 'x86'	cpuArch = 'x64'	はい
cpuName	CPU名。	cpuName LIKE '%XEON%'	はい
memorySize	RAMのサイズ（MB単位）。	memorySize < 1024	はい
diskSize	ハードドライブのサイズ（GBまたはMB単位、物理マシンのみ）。	diskSize < 300GB diskSize >= 3000000MB	いいえ
オペレーティングシステム			
osName	オペレーティングシステム名	osName LIKE '%Windows XP%'	はい
osType	オペレーティングシステム名 設定可能な値: • 'windows' • 'linux' • 'macosx'	osType = 'windows' osType IN ('linux', 'macosx')	はい
osArch	オペレーティングシステムのアーキテクチャ。 設定可能な値: • 'x64' • 'x86'	cpuArch = 'x86'	はい
osProductType	オペレーティングシステムの製品の種類。 設定可能な値: • 'dc' ドメインコントローラを表します。	osProductType = 'server'	はい

属性	意味	検索クエリの例	グループ作成でサポートされているか
	注意 Windowsサーバーでドメインコントローラーのロールが割り当てられると、osProductTypeが「server」から「dc」に変わります。このようなマシンは、「osProductType = 'server'」の検索結果には含まれません。 • 'server' • 'workstation'		
osSp	オペレーティングシステムのサービスパック。	osSp = 1	はい
osVersionMajor	オペレーティングシステムのメジャーバージョン。	osVersionMajor = 1	はい
osVersionMinor	オペレーティングシステムのマイナーバージョン。	osVersionMinor > 1	はい
エージェント			
agentVersion	インストールされている保護エージェントのバージョン。	agentVersion LIKE '12.0.*'	はい
hostId	保護エージェントの内部ID。 プロテクションエージェントのIDを取得するには、[**デバイス**]でデバイスを選択し、[**詳細**]>[**すべてのプロパティ**]をクリックします。agentプロパティの「id」の値を確認します。	hostId = '4B2A7A93-A44F-4155-BDE3-A023C57C9431'	はい
virtualType	仮想マシンの種類: 設定可能な値: • 'vmwesx' VMware仮想マシン。 • 'mshyperv'	virtualType = 'vmwesx'	はい

属性	意味	検索クエリの例	グループ作成でサポートされているか
	Hyper-V仮想マシン。 • 'pcs' Virtuozzo仮想マシン。 • 'hci' Virtuozzo Hybrid Infrastructure仮想マシン。 • 'scale' Scale Computing HC3仮想マシン。 • 'ovirt' oVirt仮想マシン		
insideVm	エージェントがインストールされている仮想マシン。 設定可能な値: • true • false	insideVm = true	はい
ロケーション			
tenant	デバイスが属しているテナント名。	tenant = 'Unit 1'	はい
tenantId	デバイスが属しているテナントのID。 テナントのIDを取得するには、**[デバイス]** でデバイスを選択し、**[詳細]** > **[すべてのプロパティ]** をクリックします。このIDは[ownerId]フィールドに表示されます。	tenantId = '3bfe6ca9-9c6a-4953-9cb2-a1323f454fc9'	はい
ou	指定したActive Directoryの組織単位（OU）に属するデバイス。	ou IN ('RnD', 'Computers')	はい
ステータス			
state	デバイスの状態 設定可能な値:	state = 'backup'	いいえ

属性	意味	検索クエリの例	グループ作成でサポートされているか
	• 'idle' • 'interactionRequired' • 'canceling' • 'backup' • 'recover' • 'install' • 'reboot' • 'failback' • 'testReplica' • 'run_from_image' • 'finalize' • 'failover' • 'replicate' • 'createAsz' • 'deleteAsz' • 'resizeAsz'		
status	保護ステータス 設定可能な値: • ok • warning • error • critical • protected • notProtected	status = 'ok' status IN ('error', 'warning')	いいえ
protectedByPlan	特定のIDを持つ保護計画によって保護されているデバイス。 計画IDを表示するには、**[管理]** > **[保護計画]** で計画を選択し、**[ステータス]** 列のバーをクリックしてから、ステータス名をクリックします。新しい計画IDによる検索が作成されます。	protectedByPlan = '4B2A7A93-A44F-4155-BDE3-A023C57C9431'	いいえ
okByPlan	特定のIDを持つ保護計画によって保護されている、ステータスが **[OK]** のデバイス。	okByPlan = '4B2A7A93-A44F-4155-BDE3-A023C57C9431'	いいえ

属性	意味	検索クエリの例	グループ作成でサポートされているか
errorByPlan	特定のIDを持つ保護計画によって保護されている、ステータスが [**エラー**] のデバイス。	errorByPlan = '4B2A7A93-A44F-4155-BDE3-A023C57C9431'	いいえ
warningByPlan	特定のIDを持つ保護計画によって保護されている、ステータスが [**警告**] のデバイス。	warningByPlan = '4B2A7A93-A44F-4155-BDE3-A023C57C9431'	いいえ
runningByPlan	特定のIDを持つ保護計画によって保護されている、ステータスが [**実行中**] のデバイス。	runningByPlan = '4B2A7A93-A44F-4155-BDE3-A023C57C9431'	いいえ
interactionByPlan	特定のIDを持つ保護計画によって保護されている、ステータスが [**ユーザーの応答が必要**] のデバイス。	interactionByPlan = '4B2A7A93-A44F-4155-BDE3-A023C57C9431'	いいえ
lastBackupTime*	最後にバックアップが作成された日時 形式はYYYY-MM-DD HH:MMです。	lastBackupTime > '2023-03-11' lastBackupTime <= '2023-03-11 00:15' lastBackupTime is null	いいえ
lastBackupTryTime*	最後にバックアップの作成が試行された日時 形式はYYYY-MM-DD HH:MMです。	lastBackupTryTime >= '2023-03-11'	いいえ
nextBackupTime*	次回バックアップの時刻 形式はYYYY-MM-DD HH:MMです。	nextBackupTime >= '2023-08-11'	いいえ
lastVAScanTime*	最後に脆弱性診断が正常に実行された日時 形式はYYYY-MM-DD HH:MMです。	lastVAScanTime > '2023-03-11' lastVAScanTime <= '2023-03-11 00:15' lastVAScanTime is null	はい
lastVAScanTryTime*	最後に脆弱性診断の作成が試行された日時。 形式はYYYY-MM-DD HH:MMです。	lastVAScanTimeTryTime >= '2022-03-11'	はい
nextVAScanTime*	次回の脆弱性診断の日時。 形式はYYYY-MM-DD HH:MMです。	nextVAScanTime <= '2023-08-11'	はい

属性	意味	検索クエリの例	グループ作成でサポートされているか
network_status	エンドポイント検知と応答（EDR）のネットワーク分離ステータス。 設定可能な値: • connected • isolated	network_status= 'connected'	はい

注意
時間と分の値をスキップすると、開始時刻はYYYY-MM-DD 00:00と見なされ、終了時刻はYYYY-MM-DD 23:59:59と見なされます。例えば、lastBackupTime = 2023-01-20の場合、検索結果には、lastBackupTime >= 2023-01-20 00:00とlastBackup time <= 2023-01-20 23:59:59の間のすべてのバックアップが含まれることになります。

検索演算子

次の表に、検索クエリで使用できる演算子を示します。

単一のクエリで複数の演算子を使用することができます。

演算子	サポート対象:	意味	例
AND	すべてのワークロード	論理積演算子	name like 'en-00' AND tenant = 'Unit 1'
OR	すべてのワークロード	論理和演算子	state = 'backup' OR state = 'interactionRequired'
NOT	すべてのワークロード	論理否定演算子	NOT(osProductType = 'workstation')
IN	すべて	この演算子は、値のリス	osType IN ('windows', 'linux')

演算子	サポート対象:	意味	例
(<value1>,... <valueN>)	のワークロード	トに式と一致する値があるかどうかを確認します。	
NOT IN	すべてのワークロード	この演算子は、IN演算子の逆の意味を持ちます。	NOT osType IN ('windows', 'linux')
LIKE 'wildcard pattern'	すべてのワークロード	この演算子は、式がこのワイルドカードパターンと一致するかどうかを確認します。 例えば次のようなワイルドカード演算子を使用できます。 • *または%: アスタリスクおよびパーセント記号は、0、1つまたは複数の文字を表します。 • _: アンダースコアは、1つの文字を表します。	name LIKE 'en-00' name LIKE '*en-00' name LIKE '*en-00*' name LIKE 'en-00_'
NOT LIKE 'wildcard pattern'	すべてのワークロード	この演算子は、LIKE演算子の逆の意味を持ちます。 例えば次のようなワイルドカード演算子を使用できます。 • *または%: アスタリスクおよびパーセント記号は、0、1つまたは複数の文字を表します。 • _: アンダースコアは、1つの文字を表します。	NOT name LIKE 'en-00' NOT name LIKE '*en-00' NOT name LIKE '*en-00*' NOT name LIKE 'en-00_'
RANGE (<starting_value>, <ending_value>)	すべてのワークロード	この演算子は、式が値の範囲内かどうか確認します（包含的）。 英数字の文字列を含む検	ip RANGE('10.250.176.1','10.250.176.50') name RANGE('a','d') このクエリでは、A、B、Cで始まるすべての名前

演算子	サポート対象:	意味	例
		索クエリでは、ASCIIコードのソート順が使用されますが、大文字と小文字は区別されません。	（Alice、Bob、Claireなど）をフィルタにかけることができます。ただし、Dは1文字の場合のみ条件を満たすので、DianaやDonなどDで始まる複数の文字数の名前は対象外となります。 同じ結果を得るために、以下のクエリも使用できます。 `name >= 'a' AND name <= 'd'`
=または==	すべてのワークロード	等しいことを表す演算子	`osProductType = 'server'`
!=または<>	すべてのワークロード	等しくないことを表す演算子	`id != '4B2A7A93-A44F-4155-BDE3-A023C57C9431'`
<	非クラウドツークラウドワークロード	小なりを表す演算子	`memorySize < 1024`
>	非クラウドツークラウドワークロード	大なりを表す演算子。	`diskSize > 300GB`
<=	非クラウドツークラウドワークロード	以下を表す演算子	`lastBackupTime <= '2022-03-11 00:15'`
>=	非クラウドツークラウドワークロード	以上を表す演算子	`nextBackupTime >= '2022-08-11'`

ダイナミックグループを編集する

ダイナミックグループの編集は、グループの内容を定義する検索クエリを変更することで実行します。

Active Directoryをベースとしたダイナミックグループでは、Active Directoryのグループを変更することもできます。

ダイナミックグループを編集するには

検索クエリを変更する:

1. **[デバイス]** をクリックし、編集するダイナミックグループに移動して選択します。
2. グループの名前の横にあるギアアイコンをクリックして、**[編集]** をクリックします。または、**[操作]** ペインで **[編集]** をクリックします。
3. 検索属性やその値、検索演算子を変更して検索クエリを変更し、**[検索]** をクリックします。
4. 検索フィールドの横の **[保存]** をクリックします。

Active Directoryグループを変更する:

注意
この手順は、Active Directoryに基づくダイナミックグループに適用されます。Active Directoryベースのダイナミックグループは、**[Microsoft 365]** > **[ユーザー]** でのみ利用可能です。

1. **[デバイス]** をクリックして、**[デバイス]** > **[Microsoft 365]** > （自分の組織） > **[ユーザー]** に進みます。
2. 編集するダイナミックグループを選択します。
3. グループの名前の横にあるギアアイコンをクリックして、**[編集]** をクリックします。または、**[操作]** ペインで **[編集]** をクリックします。
4. 以下のいずれかの操作を実行して、グループの内容を変更できます:
   - 既に選択されているActive Directoryグループの名前をクリックし、開いたリストから新しいActive Directoryグループを選択し、変更します。
   - 検索クエリを編集してから、**[検索]** をクリックします。
     検索対象は、現在選択されているActive Directoryグループに限定されます。
5. 検索フィールドの横の **[保存]** をクリックします。

また、編集した内容を現在のグループに上書きせずに保存することもできます。編集した構成を新しいグループとして保存するには、検索フィールドの横にある矢印ボタンをクリックし、**[名前を付けて保存]** をクリックします。

グループの削除

デバイスグループを削除すると、そのグループに適用されているすべての計画が取り消されます。他の計画が適用されない場合、グループ内のワークロードは、保護されていない状態になります。

デバイスグループを削除するには

1. **[デバイス]** をクリックし、削除するグループに移動します。
2. グループの名前の横にあるギアアイコンをクリックして、**[削除]** をクリックします。
3. **[削除]** をクリックしてこの選択内容を確認します。

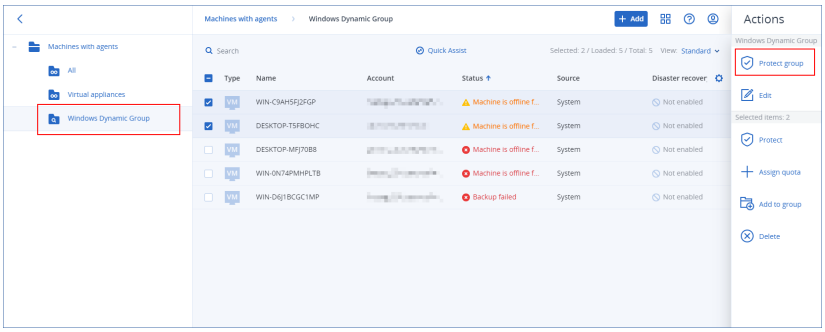
グループに計画を適用する

先にグループを選択し、そのグループに計画を割り当てることで、グループに計画を適用できます。

また、編集用に計画を開いてから、グループを追加することも可能です。

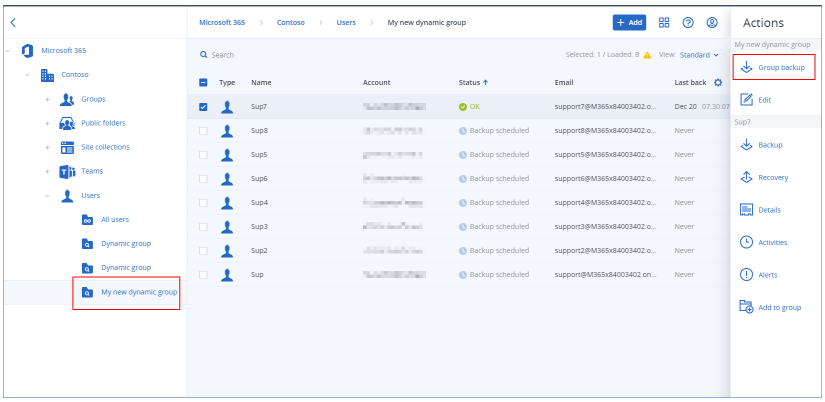
グループに計画を適用するには

1. **[デバイス]** をクリックし、計画を適用するグループに移動します。
2. （非クラウドツークラウドワークロードの場合）**[グループの保護]** をクリックします。



適用可能な計画のリストが表示されます。

3. （クラウドツークラウドワークロードの場合）**[グループバックアップ]** をクリックします。



適用可能なバックアップ計画のリストが表示されます。

4. （既存の計画を適用するには）計画を選択してから、**[適用]** をクリックします。
5. （新しい計画を作成するには）、**[計画の作成]** をクリックして、計画のタイプを選択してから新しい計画を作成します。

   利用可能な計画のタイプと作成方法については、"デバイスグループでサポートされている計画"（331ページ）を参照してください。

注意
クラウドツークラウドデバイスグループに適用されるバックアップ計画は、1日に1回実行されるように自動的にスケジュールされます。これらの計画は、**[今すぐ実行]** をクリックしてオンデマンドで実行することはできません。

グループから計画を取り消す

先にグループを選択し、そこから計画を取り消すことで、グループから計画を取り消すことができます。

または、編集用に計画を開き、そこからグループを削除することもできます。

グループから計画を取り消すには

1. **[デバイス]** をクリックし、計画を取り消したいグループに移動します。
2. （非クラウドツークラウドワークロードの場合）**[グループの保護]** をクリックします。
   グループに適用される計画のリストが表示されます。
3. （クラウドツークラウドワークロードの場合）**[グループバックアップ]** をクリックします。
   グループに適用されるバックアップ計画のリストが表示されます。
4. 取り消す計画を選択します。
5. （非クラウドツークラウドワークロードの場合）省略記号アイコンをクリックして、**[取り消し]** をクリックします。
6. （クラウドツークラウドワークロードの場合）ギアアイコンをクリックして、**[取り消し]** をクリックします。

デバイス制御モジュールを動作させる

デバイス制御モジュール[1]は、Cyber Protectionサービス保護計画の一環として、保護された各コンピューター上のデータ漏洩防止エージェント[2]の機能的サブセットを利用します。これにより、ローカルコンピューターのチャネルを介したデータの不正アクセスおよび送信を検出し、防止します。リムーバブルメディア、プリンタ、仮想デバイスやリダイレクトデバイス、Windowsクリップボードを使用したデータ交換など、多岐にわたるデータ漏洩経路をきめ細かく制御します。

---

[1]デバイス制御モジュールは保護計画の一環として、保護された各コンピューター上のデータ漏洩防止エージェントの機能的サブセットを活用して、ローカルコンピューターのチャネルを介したデータの不正アクセスおよび送信を検出し、防止します。制御の対象となるのは、周辺デバイスやポートへのユーザーアクセス、文書の印刷、クリップボードのコピー/貼り付け操作、メディアのフォーマットや取り出し操作、ローカルに接続されたモバイルデバイスとの同期などです。デバイス制御モジュールは、保護されたコンピューター上でユーザーに対してアクセスが許可されるデバイスやポートの種類、そしてユーザーがそれらのデバイスに対して実行できる操作をコンテキストに基づききめ細かく制御します。

[2]データ漏洩防止システムのクライアントコンポーネントで、コンテキストとコンテンツ分析技術を組み合わせて適用し、集中管理されたデータ漏洩防止ポリシーを実施することで、秘匿データ、保護データ、または機密データに対する、不正使用、送信、および保存からホストコンピューターを保護します。サイバープロテクションは、フル機能のデータ漏洩防止エージェントを提供しています。ただし、保護されたコンピューター上のエージェントの機能は、サイバープロテクションのライセンスで利用可能なデータ漏洩防止機能のセットに制限されており、そのコンピューターに適用されている保護計画に依存しています。

このモジュールは、ワークロード単位でライセンスが付与される、Cyber Protect Essentials、Cyber Protect Standard、Cyber Protect Advanced Editionで利用できます。

注意
Windowsマシンでは、デバイスコントロール機能を利用するには、データ漏洩防止エージェントのインストールが必要です。保護対象となっているワークロードの保護計画で**デバイス制御**モジュールが有効になっていれば、自動的にインストールされます。

デバイス制御モジュールは、エージェントのデータ漏洩防止[1]機能に依拠して、保護されているコンピューター上におけるデータアクセスおよび転送操作に対するコンテキスト制御を強制的に適用します。制御の対象となるのは、周辺デバイスやポートへのユーザーアクセス、文書の印刷、クリップボードのコピー/貼り付け操作、メディアのフォーマットや取り出し操作、ローカルに接続されたモバイルデバイスとの同期などです。データ漏洩防止エージェントには、デバイス制御モジュールのすべての集中管理および管理コンポーネント向けのフレームワークが含まれています。このため、デバイス制御モジュールで保護を実行するために、データ漏洩防止エージェントをすべてのコンピューターにインストールする必要があります。エージェントは、保護対象のコンピューターに適用される保護計画から取得したデバイス制御設定に基づいて、ユーザーのアクションを許可、制限、または拒否します。

デバイス制御モジュールは、保護対象のコンピューターで直接使用されている場合、また保護対象のコンピューター上でホストされている仮想環境でリダイレクトされている場合の両方で、さまざまな周辺デバイスへのアクセスを制御します。Microsoftリモートデスクトップサーバー、Citrix XenDesktop/XenApp/XenServer、およびVMware Horizonでリダイレクトされたデバイスを認識します。また、VMware Workstation/Player、Oracle VM VirtualBox、またはWindows Virtual PC上で実行されているゲストオペレーティングシステムのクリップボードと、保護対象のコンピューター上で実行されているホストオペレーティングシステムのクリップボード間のデータコピー操作を制御することができます。

デバイス制御モジュールは、以下のオペレーティングシステムを実行しているコンピューターを保護することができます。

デバイス制御

- Microsoft Windows 7 Service Pack 1以降
- Windows Server 2008 R2以降
- macOS 10.15 (Catalina)
- macOS 11.2.3（Big Sur）
- macOS 12 (Monterey)
- macOS 13 (Ventura)

注意
データ損失防止macOSエージェントは、x64プロセッサのみをサポートしています。ARMベースのAppleシリコンプロセッサはサポートされていません。

[1]組織内外の正当な権限を持たない使用者による、秘匿データ、保護データ、および機密データへの偶発的ならびに意図的な開示やアクセス、または信頼済みでない環境への移転を検知し、それらを防止することを目的とした、統合技術と組織的な対策を導入したシステムです。

データ漏洩防止

- Microsoft Windows 7 Service Pack 1以降
- Windows Server 2008 R2以降

注意
データ漏洩防止エージェントはMacエージェントの一部であるため、サポートされていないmacOSシステムにインストールされる可能性があります。この場合、Cyber Protectコンソールでは、コンピューターにデータ漏洩防止エージェントがインストールされている状態が表示されますが、デバイス制御およびデータ損失防止機能は動作しません。デバイス制御機能は、データ漏洩防止エージェントをサポートしているmacOSシステムでのみ動作します。

Hyper-Vでのデータ漏洩防止エージェントの使用制限について

データ漏洩防止エージェントをHyper-Vクラスター内のHyper-Vホストにインストールすると、主にクラスター共有ボリューム（CSV）を使用するHyper-VクラスターでBSOD問題が発生する可能性があります。インストールは行わないでください。

以下のバージョンのHyper-Vエージェントを使用している場合は、データ漏洩防止エージェントを手動で削除する必要があります。

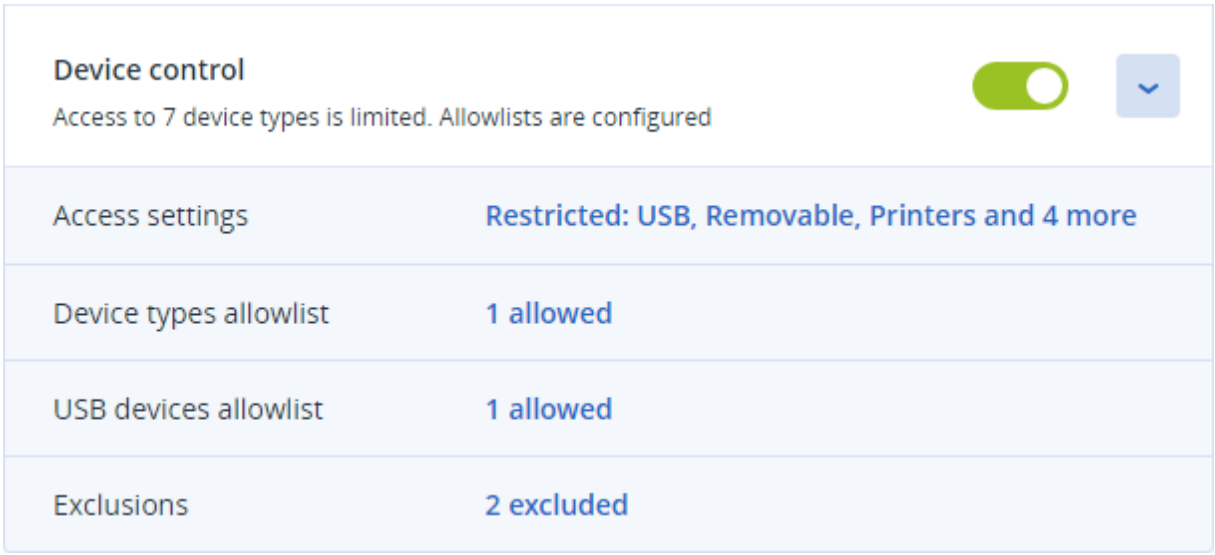
- 15.0.26473（C21.02）
- 15.0.26570（C21.02 HF1）
- 15.0.26653（C21.03）
- 15.0.26692（C21.03 HF1）
- 15.0.26822（C21.04）

データ漏洩防止エージェントを削除するには、Hyper-Vホスト上でインストーラを手動で実行し、データ漏洩防止エージェントのチェックボックスをオフにするか、以下のコマンドを実行してください。

```
<installer_name> --remove-components=agentForDlp -quiet
```

デバイス制御モジュールは、Cyber Protectコンソールの保護計画の **[デバイス制御]** セクションで有効にして構成できます。手順については、「デバイス制御を有効化または無効化する手順」を参照してください。

[デバイス制御] セクションには、モジュールの設定の概要が表示されます。



- アクセス設定 - 制限された（拒否または読み取り専用の）アクセスが存在する場合は、デバイスタイプとポートの概要を表示します。そうでない場合は、すべてのデバイスタイプが許可されていることを表示します。この概要をクリックして、アクセス設定を表示または変更します（「アクセス設定を表示または変更する手順」を参照してください）。
- デバイスタイプの許可リスト - デバイスのアクセス制御から除外することで許可されるデバイスのサブクラスの数を表示します（存在する場合）。存在しない場合は、許可リストが空であることが表示されます。この概要をクリックして、許可されたデバイスサブクラスの選択を表示または変更します（「デバイスサブクラスをアクセス制御から除外する手順」を参照してください）。
- USBデバイスの許可リスト - デバイスのアクセス制御から除外することで許可されるUSBデバイス/モデルの数を表示します（存在する場合）。存在しない場合は、許可リストが空であることが表示されます。この概要をクリックして、許可されたUSBデバイス/モデルのリストを表示または変更します（「個別のUSBデバイスをアクセス制御から除外する手順」を参照してください）。
- 除外 - Windowsクリップボード、スクリーンショットのキャプチャ、プリンタ、およびモバイルデバイスに設定されているアクセス制御の除外数を示します。

デバイス制御の使用

このセクションでは、デバイス制御モジュールを使用する際の基本的なタスクの扱い方をステップバイステップで説明します。

デバイス制御を有効化または無効化する

保護計画を作成する際に、デバイス制御を有効にできます。既存の保護計画を変更して、デバイス制御を有効または無効にすることができます。

デバイス制御を有効化または無効化するには

1. Cyber Protectコンソールで **[デバイス]** > **[すべてのデバイス]** に進みます。
2. 以下のいずれかの手順を実行して、保護計画パネルを開きます。

- 新しい保護計画を作成する場合は、保護されているマシンを選択して、**[保護]** をクリックしてから、**[計画の作成]** をクリックします。
- 既存の保護計画を変更する場合は、保護されているマシンを選択して、**[保護]** をクリックしてから、保護計画の名前の横にある省略記号（...）をクリックします。その後、**[編集]** をクリックします。

3. 保護計画パネルで、**[デバイス制御]** 領域に移動し、**[デバイス制御]** を有効化または無効化します。
4. 次のいずれかの手順を実行します。
   - 保護計画を作成する場合は、**[作成]** をクリックします。
   - 保護計画を編集する場合は、**[保存]** をクリックします。

または、[管理] タブから保護計画パネルにアクセスすることもできます。ただし、この機能はCyber Protectionサービスのすべてのエディションで利用できるわけではありません。

macOSでのデバイスコントロールモジュールの使用を有効化する

保護計画のデバイス制御設定は、保護対象のワークロードでデバイス制御ドライバが読み込まれた後にのみ有効になります。このセクションでは、macOSでデバイス制御ドライバを読み込んで、デバイス制御モジュールを使えるようにする方法について説明します。この操作は1回限りのもので、エンドポイントのマシンで管理者権限が必要となります。

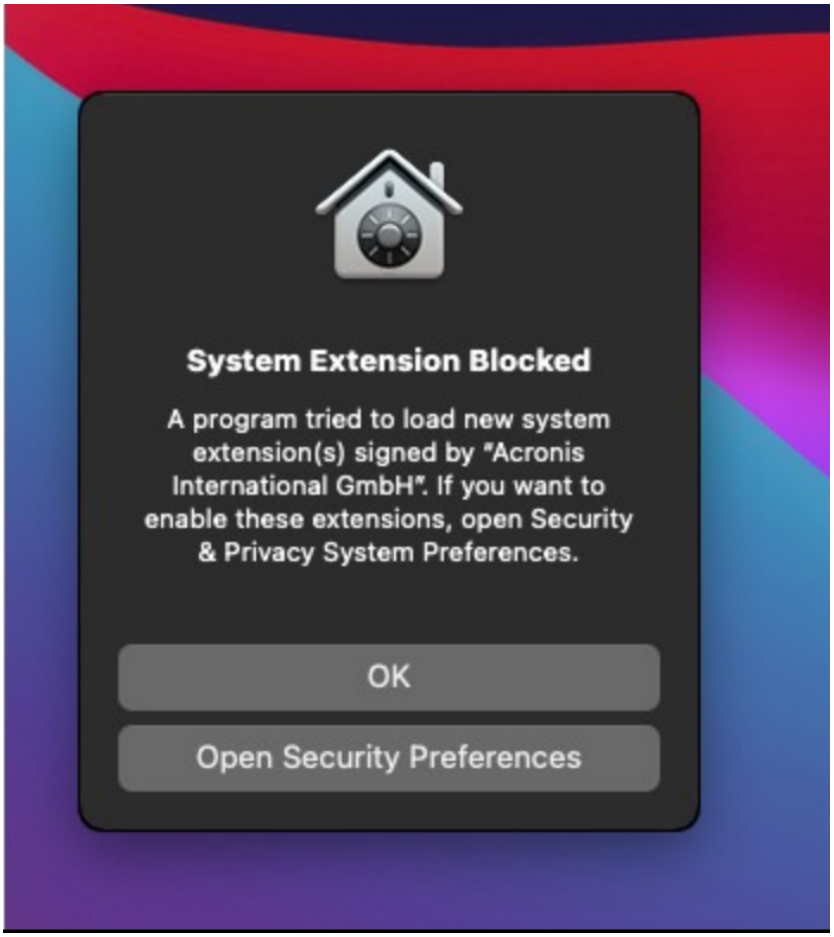
サポートされているmacOSバージョン:

- macOS 10.15（Catalina）以降
- macOS 11.2.3（Big Sur）以降
- macOS 12.2（Monterey）以降
- macOS 13.2（Ventura）以降

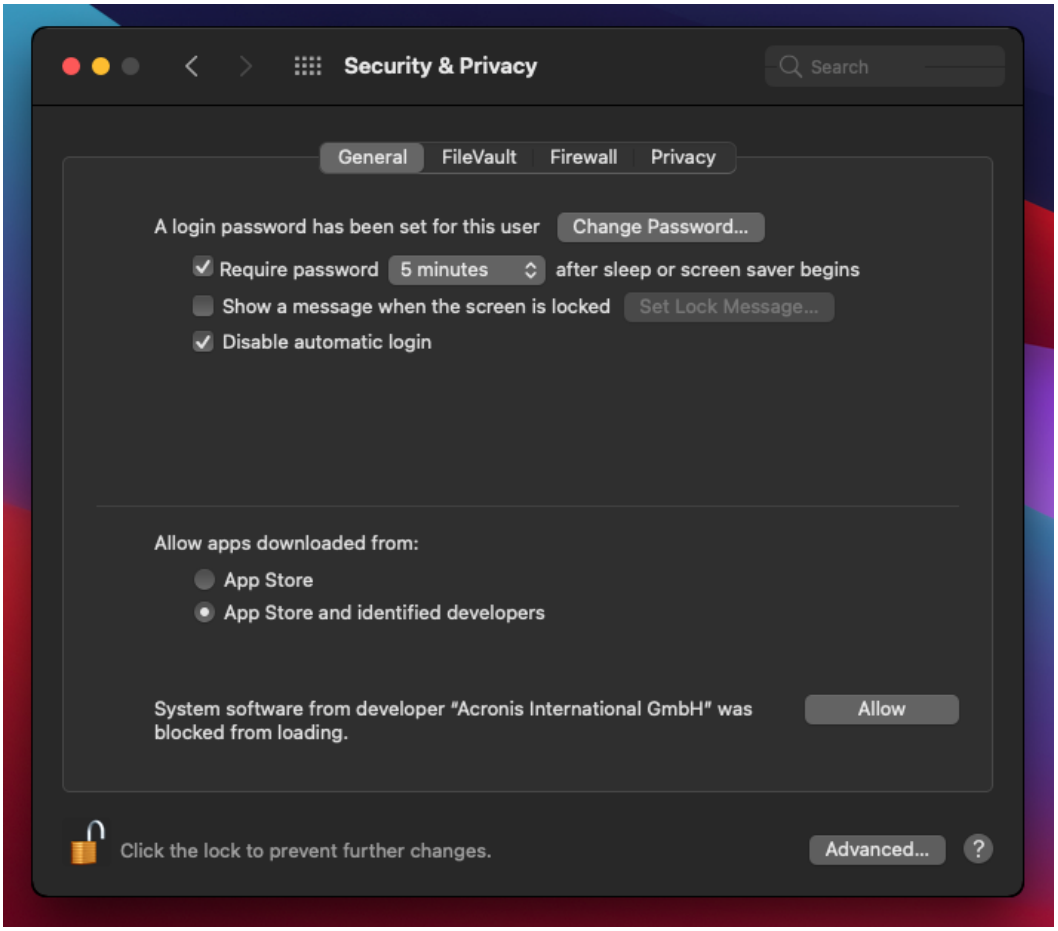
macOSでデバイス制御モジュールの使用を有効化するには

1. 保護したいマシンにMacエージェントをインストールします。
2. 保護計画でデバイス制御設定を有効にします。
3. 保護計画を適用します。

4. 保護対象のワークロードに「システム拡張がブロックされました」という警告が表示されます。**[セキュリティ環境設定を開く]** をクリックします。



5. 表示される **[セキュリティとプライバシー]** ペインで、**[App Storeと特定の開発者]** を選択し、**[許可]** をクリックします。



6. 表示されるダイアログで **[再起動]** をクリックすると、ワークロードが再起動され、デバイス制御設定が有効化されます。

注意
デバイス制御設定を一度無効にしてから再度有効にしている場合、この手順を繰り返す必要はありません。

アクセス設定の表示または変更

保護計画パネルから、デバイス制御モジュールのアクセス設定を管理することができます。このようにして、特定のタイプのデバイスについてアクセスを許可/拒否したり、通知やアラートを有効化/無効化したりすることができます。

アクセス設定を表示または変更するには

1. 保護計画の保護計画パネルを開き、該当の計画でデバイス制御を有効にします（「デバイス制御を有効化または無効化する手順」を参照）。
2. **[デバイス制御]** スイッチの横にある矢印アイコンをクリックして設定を展開し、**[アクセス設定]** の横にあるリンクをクリックします。
3. 表示される[アクセス設定の管理] ページで、必要に応じてアクセス設定を確認または変更します。

注意
デバイス制御とAdvanced DLPの両方を使用してワークロードを保護する場合、デバイス制御で構成されたアクセス設定が上書きされる可能性があります。 "保護計画でのAdvanced Data Loss Preventionの有効化"（853ページ）を参照してください。

OS通知とサービスアラートを有効化または無効化する

アクセス設定を管理する際に、許可されていない操作を実行しようとしたユーザーに通知するOS通知とサービスアラートを有効または無効にすることができます。

OS通知を有効化または無効化する

1. 「アクセス設定を表示または変更する手順」に従ってください。
2. [アクセス設定の管理] ページで、**[ブロックされたデバイスのタイプやポートを使用しようとした場合、エンドユーザーに対しOSからの通知を表示する]** のチェックボックスをオンまたはオフにします。

サービスアラートを有効化または無効化する

1. 「アクセス設定を表示または変更する手順」に従ってください。
2. [アクセス設定の管理] ページで、任意のデバイスタイプ（複数可）について、**[アラートの表示]** チェックボックスを選択または解除します。

[アラートの表示] チェックボックスは、アクセスが制限されているデバイスタイプ（読み取り専用またはアクセス拒否）でのみ使用できます。スクリーンショットのキャプチャは対象外です。

デバイスのサブクラスをアクセス制御から除外する

保護計画パネルで、アクセス制御から除外するデバイスのサブクラスを選択できます。これにより、デバイス制御のアクセス設定に関わらず、それらのデバイスへのアクセスが許可されます。

デバイスのサブクラスをアクセス制御から除外するには

1. 保護計画の保護計画パネルを開き、該当の計画でデバイス制御を有効にします（「デバイス制御を有効化または無効化する手順」を参照）。
2. **[デバイス制御]** スイッチの横にある矢印アイコンをクリックして設定を展開し、**[デバイスタイプの許可リスト]** の横にあるリンクをクリックします。
3. 表示される[許可リストの管理] ページで、アクセス制御から除外するデバイスのサブクラスの選択を表示または変更します。

個別のUSBデバイスをアクセス制御から除外する

保護計画パネルで、アクセス制御から除外するUSBデバイスやUSBデバイスのモデルを個別に指定できます。これにより、デバイス制御のアクセス設定に関わらず、それらのデバイスへのアクセスが許可されます。

USBデバイスをアクセス制御から除外するには

1. 保護計画の保護計画パネルを開き、該当の計画でデバイス制御を有効にします（「デバイス制御を有効化または無効化する手順」を参照）。
2. **[デバイス制御]** スイッチの横にある矢印アイコンをクリックして設定を展開し、**[USBデバイスの許可リスト]** の横にあるリンクをクリックします。
3. 表示される [許可リストの管理] ページで、**[データベースから追加]** をクリックします。
4. 表示される [USB機器選択] ページで、[USBデバイスデータベース] に登録されているデバイスの中から目的のデバイスを選択します。
5. **[許可リストに追加]** ボタンをクリックします。

USBデバイスをアクセス制御から除外するには

1. 保護計画の保護計画パネルを開き、該当の計画でデバイス制御を有効にします（「デバイス制御を有効化または無効化する手順」を参照）。
2. **[デバイス制御]** スイッチの横にある矢印アイコンをクリックして設定を展開し、**[USBデバイスの許可リスト]** の横にあるリンクをクリックします。
3. 表示された [許可リストの管理] ページで、任意のUSBデバイスを示すリスト項目の末尾にある削除アイコンをクリックします。

データベースでUSBデバイスを追加または削除する

特定のUSBデバイスをアクセス制御から除外するには、USBデバイスデータベースに追加する必要があります。そのデータベースから選択することで、デバイスを許可リストに追加することができます。

次の手順は、デバイス制御機能が有効になっている保護計画に適用されます。

USBデバイスをデータベースに追加するには

1. 編集するデバイスの保護計画を開きます。
   保護計画名の横にある省略記号（...）をクリックして、**[編集]** をクリックします。

   注意
   計画でデバイス制御を有効にして、デバイス制御設定にアクセスできるようにする必要があります。

2. **[デバイス制御]** スイッチの横にある矢印アイコンをクリックして設定を展開し、**[USBデバイスの許可リスト]** の横にあるリンクをクリックします。
3. 表示される **[USBデバイスの許可リスト] ページ**で、**[データベースから追加]** をクリックします。
4. 表示される [USBデバイスデータベースの管理] ページで、**[データベースから追加]** をクリックします。
5. 表示される **[USBデバイスを追加]** ダイアログで、USBデバイスが接続されているマシンをクリックします。
   コンピューターのリストには、オンラインのマシンのみが表示されます。
   USBデバイスのリストは、データ漏洩防止エージェントがインストールされているマシンについてのみ表示されます。
   USBデバイスはツリービューに一覧表示されます。ツリーの最上位レベルは、デバイスモデルを表します。2番目のレベルは、該当モデルの特定のデバイスを表します。

デバイスの説明の横にある青いアイコンは、デバイスが現在コンピューターに接続されていることを示しています。デバイスがコンピューターに接続されていない場合は、アイコンがグレーアウトして表示されます。

6. データベースに追加するUSBデバイスのチェックボックスを選択し、**[データベースに追加]** をクリックします。
   選択したUSBデバイスがデータベースに追加されます。
7. 終了するか、保護計画を保存します。

コンピューターの詳細パネルからデータベースにUSBデバイスを追加するには

注意
この手順は、オンライン状態であり、データ漏洩防止エージェントがインストールされているデバイスのみに適用されます。オフラインのコンピューター、またはデータ漏洩防止エージェントがインストールされていないコンピューターのUSBデバイスのリストを表示することはできません。

1. Cyber Protectコンソールで **[デバイス]** > **[すべてのデバイス]** に進みます。
2. 任意のUSBデバイスが接続されているコンピューターを選択し、右側のメニューで **[インベントリ]** をクリックします。
   コンピューターの詳細パネルが開きます。
3. コンピューターの詳細パネルで、**[USBデバイス]** タブをクリックします。
   選択したコンピューターで認識されているUSBデバイスのリストが開きます。
   USBデバイスはツリービューに一覧表示されます。ツリーの最上位レベルは、デバイスモデルを表します。2番目のレベルは、該当モデルの特定のデバイスを表します。
   デバイスの説明の横にある青いアイコンは、デバイスが現在コンピューターに接続されていることを示しています。デバイスがコンピューターに接続されていない場合は、アイコンがグレーアウトして表示されます。
4. データベースに追加するUSBデバイスのチェックボックスを選択し、**[データベースに追加]** をクリックします。

サービスアラートからデータベースにUSBデバイスを追加するには

1. Cyber Protectコンソールで、**[監視]** > **[アラート]** に進みます。
2. USBデバイスへのアクセスが拒否されていることを通知する、デバイス制御アラートを検索します。
3. アラートのシンプルビューで、**[このUSBデバイスを許可]** をクリックします。
   これにより、USBデバイスがアクセス制御から除外され、以後も参照できるようデータベースに追加されます。

デバイスのリストをデータベースにインポートしてUSBデバイスを追加するには

データベースに、USBデバイスの一覧を含んだJSONファイルをインポートできます。"USBデバイスのリストをデータベースにインポートします"（373ページ）をご覧ください。

データベースからUSBデバイスを削除するには

1. 編集するデバイスの保護計画を開きます。
   保護計画名の横にある省略記号（...）をクリックして、**[編集]** をクリックします。

   注意
   計画でデバイス制御を有効にして、デバイス制御設定にアクセスできるようにする必要があります。

2. **[デバイス制御]** スイッチの横にある矢印をクリックして設定を展開し、**[USBデバイスの許可リスト]** 行をクリックします。
3. 表示される [許可リストの管理] ページで、**[データベースから追加]** をクリックします。
4. データベースからUSBデバイスを選択するページで、データベースに追加するUSBデバイスを示すリスト項目の末尾にある省略記号（...）をクリックします。それから **[削除]** をクリックし、削除を確定します。
   USBデバイスがデータベースから削除されます。
5. 終了するか、保護計画を保存します。

デバイス制御アラートを表示

デバイス制御モジュールでは、拒否されたユーザーが特定のデバイスタイプを使用しようとするとアラートを生成して通知するように構成できます（「OS通知とサービスアラートを有効化または無効化する」を参照してください）。これらのアラートを表示するには、次の手順を実行します。

デバイス制御アラートを表示するには

1. Cyber Protectコンソールで、**[監視]** > **[アラート]** に進みます。
2. 以下のステータスのアラートを探します:「周辺デバイスへのアクセスがブロックされました」。

詳細については、「デバイス制御のアラート」を参照してください。

アクセス設定

[アクセス設定] ページでは、特定のタイプのデバイスについてアクセスを許可/拒否したり、OS通知やデバイス制御アラートを有効化/無効化したりすることができます。

注意
デバイス制御とAdvanced DLPの両方を使用してワークロードを保護する場合、デバイス制御で構成されたアクセス設定が上書きされる可能性があります。 "保護計画でのAdvanced Data Loss Preventionの有効化"（853ページ）を参照してください。

アクセス設定では、以下のデバイスタイプとポートへのユーザーアクセスを制限することができます。

- **リムーバブル**（デバイスタイプによるアクセス制御） - コンピューターに接続するための何らかのインターフェース（USB、FireWire、PCMCIA、IDE、SATA、SCSIなど）を備えたデバイスで、オペレーティングシステムによってリムーバブルストレージデバイスとして認識されるものです（例:USBメモリ、カードリーダー、光磁気ドライブなど）。デバイス制御では、USB、FireWire、PCMCIAを介して接続されたすべてのハードドライブがリムーバブルデバイスとして分類されます。また、該当

のデバイスでホットプラグ機能がサポートされていて、インストール済みかつ稼働中のオペレーティングシステムが含まれていない場合、一部のハードドライブ（通常はSATAとSCSI）がリムーバブルデバイスとして分類されます。

保護されたコンピューター上で、リムーバブルデバイスへのフルアクセスや読み取り専用アクセスを許可したり、アクセスを拒否したりできます。これにより、リムーバブルデバイスとの間のデータコピー処理を制御することができます。アクセス権は、BitLockerまたはFileVault（HFS+ファイルシステムのみ）で暗号化されているデバイスには影響しません。

このデバイスタイプは、WindowsとmacOSの両方でサポートされています。

- **暗号化されたリムーバブル**（デバイスタイプによるアクセス制御）- BitLocker（Windows）またはFileVault（macOS）ドライブ暗号化で暗号化されたリムーバブルデバイス。

  macOSでは、HFS+（HFS Plus、Mac OS拡張、HFS拡張とも呼ばれる）ファイルシステムを使用する暗号化リムーバブルドライブのみがサポートされます。APFSファイルシステムを使用して暗号化されたリムーバブルドライブは、リムーバブルドライブとして扱われます。

  保護されたコンピューター上で、暗号化されたリムーバブルデバイスへのフルアクセスや読み取り専用アクセスを許可したり、アクセスを拒否したりできます。これにより、暗号化されたリムーバブルデバイスとの間のデータコピー処理を制御することができます。アクセス権は、BitLockerまたはFileVault（HFS+ファイルシステムのみ）で暗号化されているデバイスにのみ影響します。

  このデバイスタイプは、WindowsとmacOSの両方でサポートされています。

- **プリンタ**（デバイスタイプによるアクセス制御） - コンピューターに接続するための何らかのインターフェース（USB、LPT、Bluetoothなど）を備えた物理プリンタ、またはネットワーク上のコンピューターからアクセスするプリンタです。

  保護されたコンピューター上で、プリンタへのアクセスを許可または拒否して、任意のプリンタによる文書の印刷を制御できます。

  注意

  プリンタのアクセス設定を**拒否**に変更した場合、新しく構成されたアクセス設定を適用するには、プリンタにアクセスするアプリケーションとプロセスを再起動する必要があります。アクセス設定が正しく適用されるようにするには、保護されたワークロードを再起動します。

  このデバイスタイプは、Windowsでのみサポートされています。

- **クリップボード**（デバイスタイプによるアクセス制御） - Windowsのクリップボードです。

  保護されたコンピューター上で、クリップボードへのアクセスを許可または拒否して、Windowsクリップボードを介したデータのコピー/貼り付けを制御できます。

  注意

  クリップボードのアクセス設定を**拒否**に変更した場合、新しく構成されたアクセス設定を適用するには、クリップボードにアクセスするアプリケーションとプロセスを再起動する必要があります。アクセス設定が正しく適用されるようにするには、保護されたワークロードを再起動します。

  このデバイスタイプは、Windowsでのみサポートされています。

- **スクリーンショットのキャプチャ**（デバイスタイプによるアクセス制御）- 画面全体、アクティブなウィンドウ、または画面の選択した部分でスクリーンショットのキャプチャを有効にします。

保護されたコンピューターで、スクリーンショットキャプチャへのアクセスを許可または拒否して、スクリーンショットキャプチャを制御できます。

注意
スクリーンショットキャプチャのアクセス設定を**拒否**に変更した場合、新しく構成されたアクセス設定を適用するには、スクリーンショットキャプチャにアクセスするアプリケーションとプロセスを再起動する必要があります。アクセス設定が正しく適用されるようにするには、保護されたワークロードを再起動します。

このデバイスタイプは、Windowsでのみサポートされています。

- **モバイルデバイス**（デバイスタイプによるアクセス制御） - コンピューターに接続するための何らかのインターフェース（USB、IP、Bluetooth）により、メディア転送プロトコル（MTP）を介してコンピューターと通信するデバイス（Androidベースのスマートフォンなど）です。
  保護されたコンピューター上で、モバイルデバイスへのフルアクセスや読み取り専用アクセスを許可したり、アクセスを拒否したりできます。これにより、MTPベースのモバイルデバイスとの間におけるデータコピー処理を制御することができます。

注意
モバイルデバイスのアクセス設定を**読み取り専用**または**拒否**に変更した場合、新しく構成されたアクセス設定を適用するには、モバイルデバイスにアクセスするアプリケーションとプロセスを再起動する必要があります。アクセス設定が正しく適用されるようにするには、保護されたワークロードを再起動します。

このデバイスタイプは、Windowsでのみサポートされています。

- **Bluetooth**（デバイスタイプによるアクセス制御） - コンピューターに接続するための何らかのインターフェース（USB、PCMCIAなど）を備える、外部および内部のBluetoothデバイスです。この設定は、このタイプのデバイスを使用したデータ交換ではなく、このタイプのデバイスの使用自体を制御します。
  保護されたコンピューター上で、Bluetoothへのアクセスを許可または拒否することができます。これによって任意のBluetoothデバイスの使用を制御できます。

注意
macOSでは、Bluetoothのアクセス権は、Bluetooth HIDデバイスに影響しません。iMacやMac Proのハードウェアでワイヤレス HIDデバイス（マウスやキーボード）が無効化されるのを防ぐため、これらのデバイスへのアクセスは常に許可されています。

このデバイスタイプは、WindowsとmacOSの両方でサポートされています。

- **光学ドライブ**（デバイスタイプによるアクセス制御） - コンピューターに接続するための何らかのインターフェース（IDE、SATA、USB、FireWire、PCMCIAなど）を備える、外付けおよび内蔵のCD/DVD/BDドライブ（ライターを含む）です。
  保護されたコンピューター上で、光学ドライブへのフルアクセスや読み取り専用アクセスを許可したり、アクセスを拒否したりできます。これにより、光学ドライブとの間におけるデータコピー処理を制御することができます。
  このデバイスタイプは、WindowsとmacOSの両方でサポートされています。

- **フロッピードライブ**（デバイスタイプによるアクセス制御） - コンピューターに接続するための何らかのインターフェース（IDE、USB、PCMCIAなど）を備える、外部および内部のフロッピードライブです。一部のモデルのフロッピードライブは、オペレーティングシステムによりリムーバブルドライブとして認識されます。その場合、デバイス制御もこれらのドライブをリムーバブルデバイスとして認識します。

  保護されたコンピューター上で、フロッピードライブへのフルアクセスや読み取り専用アクセスを許可したり、アクセスを拒否したりできます。これにより、フロッピードライブとの間におけるデータコピー処理を制御することができます。

  このデバイスタイプは、Windowsでのみサポートされています。
- **USB**（デバイスインターフェースによるアクセス制御） - USBポートに接続されているすべてのデバイス（ハブを除く）です。

  保護されたコンピューター上で、USBポートへのフルアクセスや読み取り専用アクセスを許可したり、アクセスを拒否したりできます。これにより、USBポートに接続されたデバイスとの間におけるデータコピー処理を制御することができます。

  このデバイスタイプは、WindowsとmacOSの両方でサポートされています。
- **FireWire**（デバイスインターフェースによるアクセス制御） - FireWire（IEEE 1394）ポートに接続されているすべてのデバイス（ハブを除く）です。

  保護されたコンピューター上で、FireWireポートへのフルアクセスや読み取り専用アクセスを許可したり、アクセスを拒否したりできます。これにより、FireWireポートに接続されたデバイスとの間におけるデータコピー処理を制御することができます。

  このデバイスタイプは、WindowsとmacOSの両方でサポートされています。
- **リダイレクトされたデバイス**（デバイスインターフェースによるアクセス制御） - 仮想アプリケーション/デスクトップセッションにリダイレクトされた、マップ済みドライブ（ハードドライブ、リムーバブルドライブ、光学ドライブ）、USBデバイス、クリップボードです。

  このデバイスコントロールは、保護されたWindowsコンピューター上でホストされているMicrosoft RDS、Citrix XenDesktop、Citrix XenApp、Citrix XenServer、およびVMware Horizon仮想環境で、Microsoft RDP、Citrix ICA、VMware PCoIP、およびHTML5/WebSocketsリモートプロトコルを介してリダイレクトされたデバイスを認識します。また、VMware Workstation/Player、Oracle VM VirtualBox、またはWindows Virtual PC上で実行されているゲストオペレーティングシステムのWindowsクリップボードと、保護されているWindowsコンピューター上で実行されているホストオペレーティングシステムのクリップボード間のデータコピー操作を制御することができます。

  このデバイスタイプは、Windowsでのみサポートされています。

  リダイレクトされたデバイスへのアクセスは、以下のように設定できます。
  - **マップ済みドライブ** - 保護されたコンピューター上で、ホスト済みセッションにリダイレクトされたハードドライブ、リムーバブルドライブ、または光学ドライブへのフルアクセスや読み取り専用アクセスを許可したり、アクセスを拒否したりできます。これにより、これらのデバイスとの間のデータコピーを制御します。
  - **クリップボード受信** - 保護されたコンピューター上で、ホスト済みのセッションへのアクセスを許可または拒否し、クリップボードを介したデータコピーを制御します。

注意
クリップボード受信のアクセス設定を**拒否**に変更した場合、新しく構成されたアクセス設定を適用するには、クリップボードにアクセスするアプリケーションとプロセスを再起動する必要があります。アクセス設定が正しく適用されるようにするには、保護されたワークロードを再起動します。

- **クリップボード送信** - 保護されたコンピューター上で、ホスト済みのセッションからのアクセスを許可または拒否し、クリップボードを介したデータコピーを制御します。

注意
クリップボード送信のアクセス設定を**拒否**に変更した場合、新しく構成されたアクセス設定を適用するには、クリップボードにアクセスするアプリケーションとプロセスを再起動する必要があります。アクセス設定が正しく適用されるようにするには、保護されたワークロードを再起動します。

- **USBポート** - 保護されたコンピューター上で、ホスト済みセッションにリダイレクトされた任意のUSBポートへのアクセスを許可または拒否して、USBポートに接続されているデバイスとの間のデータコピーを制御します。

デバイス制御の設定は、すべてのユーザーに同様に影響します。たとえば、保護されたコンピューター上でリムーバブルデバイスへのアクセスを拒否すると、対象のデバイスとの間でのユーザーによるデータコピーを防止できます。アクセス制御から除外することで、個別のUSBデバイスへのアクセスを選択的に許可することができます（「デバイスタイプの許可リスト」と「USBデバイスの許可リスト」を参照）。

デバイスへのアクセスが、タイプレベルとインターフェースレベルの両方で制御されている場合、インターフェースレベルで設定されたアクセス拒否が優先されます。例えば、USBポートへのアクセスが拒否されている場合（デバイスインターフェースレベル）、USBポートに接続されたモバイルデバイスへのアクセスは、モバイルデバイスへのアクセスの許可/拒否（デバイスタイプレベル）に関わらず拒否されます。このようなデバイスへのアクセスを許可するには、そのインターフェースとデバイスタイプの両方を許可する必要があります。

注意
macOSで使用する保護計画に、Windowsでのみサポートされているデバイスタイプの設定が含まれている場合、macOSではこれらのデバイスタイプの設定は無視されます。

重要
リムーバブルデバイス、暗号化されたリムーバブルデバイス、プリンタ、またはBluetoothデバイスがUSBポートに接続されていて、それらのデバイスへのアクセスが許可されている場合は、これらの許可がUSBインターフェースレベルで設定されたアクセス拒否より優先されます。このようなデバイスタイプを許可する場合、USBポートへのアクセスが拒否されているかどうかに関わらず、デバイスへのアクセスが許可されます。

OS通知およびサービスアラート

ブロックされたデバイスのタイプや保護されたコンピューターを使用しようとした場合、エンドユーザーに対しOSからの通知を表示するように、デバイス制御を構成できます。アクセス設定で **[ブロックされたデバイスタイプまたはポートを使用しようとした場合にエンドユーザーにOS通知を表示する]** チェックボックスが選択されている場合、エージェントは、以下のイベントのいずれかが発生したときに、保護されたコンピューターの通知領域にポップアップメッセージを表示します。

- USBまたはFireWireポートでデバイスを使用しようとしましたが拒否されました。この通知は、インターフェースレベル（USBポートへのアクセスを拒否する場合など）またはタイプレベル（リムーバブルデバイスの使用を拒否する場合など）で拒否された、USBまたはFireWireデバイスをユーザーが使用しようとした場合に表示されます。この通知により、指定されたデバイス/ドライブに対するユーザーのアクセスが許可されていないことを知らせます。
- 特定のデバイスからデータオブジェクト（ファイルなど）をコピーしようとしましたが拒否されました。この通知は、フロッピードライブ、光学ドライブ、リムーバブルデバイス、暗号化済みリムーバブルデバイス、モバイルデバイス、リダイレクトされたマップ済みドライブ、およびリダイレクトされたクリップボードの受信データに対する読み取りアクセスを拒否するときに表示されます。この通知により、指定されたデバイスから指定されたデータオブジェクトへのユーザーによるアクセスが許可されていないことを知らせます。

  また、Bluetooth、FireWireポート、USBポート、リダイレクトされたUSBポートへの読み/書きアクセスを拒否した場合には、読み取り拒否の通知が表示されます。
- 特定のデバイスに対してデータオブジェクト（ファイルなど）をコピーしようとしましたが拒否されました。この通知は、フロッピードライブ、光学ドライブ、リムーバブルデバイス、暗号化済みリムーバブルデバイス、モバイルデバイス、ローカルクリップボード、スクリーンショットのキャプチャ、プリンタ、リダイレクトされたマップ済みドライブ、およびリダイレクトされたクリップボードの送信データに対する書き込みアクセスを拒否するときに表示されます。この通知により、ユーザーには、指定されたデバイスに対する指定されたデータオブジェクトの送信が許可されていないことを知らせます。

ユーザーが、保護されたコンピューター上でブロック対象のデバイスタイプにアクセスしようとする場合にアラートが発生し、Cyber Protectコンソールにログとして保存するようにできます。アクセス設定の **[アラートの表示]** チェックボックスを選択することで、デバイスのタイプ（スクリーンショットのキャプチャを除く）やポートごとにアラートを有効化できます。たとえば、リムーバブルデバイスへのアクセスが読み取り専用に制限されており、そのデバイスタイプで **[アラートの表示]** チェックボックスが選択されている場合、保護されたコンピューターのユーザーがリムーバブルデバイスにデータをコピーしようとするたびにアラートが発生し、ログとして保存されます。詳細については、「デバイス制御のアラート」を参照してください。

OS通知とサービスアラートを有効化または無効化する手順も参照してください。

デバイスタイプの許可リスト

[デバイスタイプの許可リスト] ページでは、デバイスのアクセス制御から除外するデバイスサブクラスを選択できます。これにより、デバイス制御モジュールのアクセス設定に関わらず、対象のデバイスへ

のアクセスが許可されます。

デバイス制御モジュールでは、拒否されたデバイスタイプの中で、特定のサブクラスのデバイスに対するアクセスを許可するオプションが提供されます。このオプションは、特定タイプのすべてのデバイスを拒否します。対象となるタイプのデバイスで一部のサブクラスを除外することができます。例えば、USBキーボードとマウスを同時に使用できるようにした上で、すべてのUSBポートへのアクセスを拒否する必要がある場合などに便利です。

デバイス制御モジュールを構成するときに、どのデバイスサブクラスをデバイスアクセス制御から除外するかを指定することができます。デバイスが、除外対象のサブクラスに属している場合、該当のデバイスタイプやポートが拒否対象になっているかどうかに関わらず、そのデバイスへのアクセスが許可されます。次に挙げるデバイスのサブクラスをデバイスアクセス制御から選択的に除外することができます。

- **USB HID（マウス、キーボードなど）** - これを選択すると、USBポートが拒否対象になっていても、USBポートに接続されたヒューマンインターフェースデバイス（マウス、キーボードなど）にアクセスできます。デフォルトでは、この項目が選択されているため、USBポートへのアクセスを拒否してもキーボードやマウスが無効にならないよう設定されています。
  WindowsとmacOSの両方をサポートしています。
- **USBおよびFireWireネットワークカード** - これを選択すると、USBポートやFireWireポートが拒否対象になっていても、USBまたはFireWire（IEEE 1394）ポートに接続されたネットワークカードにアクセスできます。
  WindowsとmacOSの両方をサポートしています。
- **USBスキャナおよび静止画デバイス** - これを選択すると、USBポートが拒否対象になっている場合でも、USBポートに接続されたスキャナおよび静止画デバイスにアクセスできます。
  は、Windowsでのみサポートされます。
- **USBオーディオデバイス** - これを選択すると、USBポートが拒否対象になっている場合でも、USBポートに接続されたヘッドセットやマイクなどのオーディオデバイスにアクセスできます。
  は、Windowsでのみサポートされます。
- **USBカメラ** - これを選択すると、USBポートが拒否対象になっている場合でも、USBポートに接続されたWebカメラにアクセスできます。
  は、Windowsでのみサポートされます。
- **Bluetooth HID（マウス、キーボードなど）** - これを選択すると、Bluetoothが拒否対象になっていても、Bluetooth経由で接続されたヒューマンインターフェースデバイス（マウス、キーボードなど）にアクセスできます。
  は、Windowsでのみサポートされます。
- **アプリケーション内のクリップボードでのコピー/貼り付け操作** - これを選択すると、クリップボードの使用が拒否されていても、同一のアプリケーション内でクリップボードを介してデータをコピー/貼り付けできます。
  は、Windowsでのみサポートされます。

注意
適用される保護計画で、サポートされていないデバイスサブクラスの設定が構成されている場合、これらの設定は無視されます。

デバイスタイプを許可する場合は、次のことを考慮してください。

- デバイスタイプの許可リストでは、デバイスのサブクラス全体のみを許可できます。特定のデバイスモデルを許可することはできませんが、同じサブクラスの他のすべてのデバイスを拒否することはできます。例えば、USBカメラをデバイスのアクセス制御から除外することで、モデルやベンダーに関わらず、すべてのUSBカメラの使用を許可します。個別のデバイス/モデルを許可する方法については、「USBデバイスの許可リスト」を参照してください。
- デバイスタイプは、デバイスサブクラスのクローズドリストからのみ選択できます。許可するデバイスのサブクラスが異なっている場合、デバイスタイプの許可リストを使用して許可することはできません。例えば、USBスマートカードリーダーのようなサブクラスは許可リストに追加できません。USBポートの使用が拒否されている場合に、USBスマートカードリーダーを許可するには、「USBデバイスの許可リスト」の指示に従ってください。
- デバイスタイプの許可リストは、標準のWindowsドライバを使用するデバイスに対してのみ有効です。デバイス制御では、独自のドライバを搭載した一部のUSBデバイスのサブクラスが認識されない場合があります。このため、デバイスタイプの許可リストを使用して、そのようなUSBデバイスへのアクセスを許可することはできません。この場合は、デバイス/モデルごとにアクセスを許可することができます（「USBデバイスの許可リスト」を参照してください）。

USBデバイスの許可リスト

許可リストは、他のデバイス制御設定に関わりなく、特定のUSBデバイスの使用を許可するために利用します。許可リストに個別のデバイスやデバイスモデルを追加して、それらのデバイスのアクセス制御を無効にすることができます。例えば、ユニークIDを使用してモバイルデバイスを許可リストに追加すると、他のUSBデバイスが拒否されていても、その特定のデバイスの使用は許可されます。

[デバイスタイプの許可リスト] ページでは、デバイスのアクセス制御から除外するUSBデバイスやUSBデバイスのモデルを個別に指定できます。これにより、デバイス制御モジュールのアクセス設定に関わらず、対象のデバイスへのアクセスが許可されます。

許可リストでデバイスを識別する方法は2つあります。

- デバイスのモデル - 特定モデルのすべてのデバイスを一括して識別します。各デバイスモデルは、ベンダーID（VID）と製品ID（PID）で識別されます（例: USB¥VID_0FCE&PID_E19E）。
  このVIDとPIDの組み合わせでは、特定のデバイスを識別するのではなく、デバイスモデル全体を識別します。デバイスモデルを許可リストに追加することで、そのモデルのデバイスへのアクセスが許可されます。例えばこの方法では、特定モデルのUSBプリンタの使用を許可することができます。
- ユニークデバイス - 特定のデバイスを識別します。各ユニークデバイスは、ベンダーID（VID）、製品ID（PID）、およびシリアルナンバーで識別されます（例: USB¥VID_0FCE&PID_E19E¥D55E7FCA）。
  すべてのUSBデバイスにシリアルナンバーが割り当てられているわけではありません。製造時にデバイスに対しシリアルナンバーが割り当てられている場合に限り、デバイスをユニークデバイスとして許可リストに追加することができます。例えば、ユニークなシリアルナンバーが割り当てられているUSBメモリなどです。

デバイスを許可リストに追加するには、まずデバイスをUSBデバイスデータベースに追加する必要があります。そのデータベースから選択することで、デバイスを許可リストに追加することができます。

許可リストは、**USBデバイス許可リスト**という別の設定ページで管理されています。リストの各項目は、デバイスまたはデバイスモデルを表しており、次のフィールドがあります。

- **説明** - USBデバイスを接続するときに、オペレーティングシステムにより特定の説明が割り当てられます。USBデバイスのデータベースでデバイスの説明を変更することができます（「USBデータベースの管理」ページを参照）。
- **デバイスタイプ** - リスト項目がユニークなデバイスを表す場合は「ユニーク」と表示され、デバイスのモデルを表す場合は「モデル」と表示されます。
- **読み取り専用** - これを選択すると、デバイスからのデータ受信のみが可能になります。デバイスが読み取り専用アクセスをサポートしていない場合、デバイスへのアクセスはブロックされます。このチェックボックスをオフにすると、制限なくデバイスにアクセスできるようになります。
- **再初期化** - これを選択すると、新しいユーザーがログオンしたときにデバイスの切断/再接続をシミュレートします。一部のUSBデバイスでは、正常な動作のために再初期化が必要になる場合があります。そのようなデバイス（マウス、キーボードなど）では、このチェックボックスをオンにすることを推奨します。また、データストレージデバイス（USBメモリ、光学ドライブ、外付けハードドライブなど）については、このチェックボックスをオフにしておくことをお勧めします。
  デバイス制御では、独自のドライバを搭載した一部のUSBデバイスを再初期化できない場合があります。このようなデバイスにアクセスできない場合、USBポートからUSBデバイスを取り外して、再び挿入する必要があります。

注意
[再初期化] フィールドはデフォルトでは非表示になっています。表に表示するには、表の右上にあるギアアイコンをクリックして **[再初期化]** チェックボックスを選択します。

注意
[読み取り専用] および **[再初期化]** フィールドは、macOSではサポートされていません。適用される保護計画で、これらのフィールドが構成されている場合、それらは無視されます。

許可リストでデバイス/モデルを追加また削除するには、次の手順を実行します。

- リストの上の **[データベースから追加]** をクリックし、USBデバイスデータベースに登録されているデバイスの中から目的のデバイスを選択（複数可）します。選択したデバイスがリストに追加され、その設定を構成したり、変更を確認したりできます。
- **[このUSBデバイスを許可]** をクリックすると、USBデバイスへのアクセスが拒否されたことを通知するアラートが表示されます（「デバイス制御アラート」を参照）。これにより、デバイスが許可リストとUSBデバイスデータベースに追加されます。
- リスト項目の最後にある削除アイコンをクリックします。この操作により、それぞれのデバイス/モデルを許可リストから削除します。

USBデバイスのデータベース

デバイス制御モジュールは、USBデバイスのデータベースを保持しており、そこからデバイスを除外リストに追加することができます（「USBデバイスの許可リスト」を参照）。これらの方法のいずれかでUSBデバイスをデータベースに登録することができます。

- 除外リストにデバイスを追加するときに表示されるページでデバイスを追加します（「USBデバイスのデータベース管理ページ」を参照）。
- Cyber Protectコンソールにある、コンピューターのインベントリペインの [USBデバイス] タブからデバイスを追加します（「コンピューターのUSBデバイスリスト」を参照）。
- USBデバイスへのアクセスを拒否するアラートからデバイスを許可します（「デバイス制御アラート」を参照）。

関連項目「データベースでUSBデバイスを追加または削除する手順」を参照してください。

USBデバイスのデータベース管理ページ

USBデバイスの許可リストを設定する際に、データベースからデバイスを追加するオプションを利用できます。このオプションを選択すると、管理ページにデバイスのリストが表示されます。このページでは、データベースに登録されているすべてのデバイスを一覧表示したり、許可リストに追加するデバイスを選択したりできます。また以下の操作を行うことができます。

デバイスをデータベースに登録します

1. ページ上部の **[データベースに追加]** をクリックします。
2. 表示される **[USBデバイスを追加]** ダイアログで、USBデバイスが接続されているマシンを選択します。
   コンピューターのリストには、オンラインのマシンのみが表示されます。
   USBデバイスのリストは、データ漏洩防止エージェントがインストールされているマシンについてのみ表示されます。
   USBデバイスはツリービューに一覧表示されます。ツリーの最上位レベルは、デバイスモデルを表します。2番目のレベルは、該当モデルの特定のデバイスを表します。
   デバイスの説明の横にある青いアイコンは、デバイスが現在コンピューターに接続されていることを示しています。デバイスがコンピューターに接続されていない場合は、アイコンがグレーアウトして表示されます。
3. 登録するUSBデバイスのチェックボックスを選択し、**[データベースに追加]** をクリックします。

デバイスの説明を変更します

1. **USBデバイスのデータベース**ページで、デバイスを示すリスト項目の末尾にある省略記号（...）をクリックしてから、**[編集]** をクリックします。
2. 表示されるダイアログボックスで説明を変更します。

データベースからデバイスを削除します

1. デバイスを示すリスト項目の末尾にある省略記号（...）をクリックします。
2. **[削除]** をクリックして、削除を確定します。

ページ上のリストでは、各デバイスについて以下の情報が提供されています。

- **説明** - 可読性のあるデバイスの識別情報です。必要に応じて説明を変更することができます。
- **デバイスタイプ** - リスト項目がユニークなデバイスを表す場合は「ユニーク」と表示され、デバイスのモデルを表す場合は「モデル」と表示されます。ユニークなデバイスには、ベンダーID（VID）と

製品ID（PID）に加え、シリアルナンバーが必要になります。一方、デバイスモデルはVIDとPIDの組み合わせで識別されます。

- **ベンダーID**、**製品ID**、**シリアルナンバー** - これらの値を組み合わせて、USB¥VID_<ベンダーID>&PID_<製品ID>¥<シリアルナンバー>の形式により、デバイスIDが構成されます。
- **アカウント** - このデバイスが属するテナントを示します。これは、デバイスをデータベースに登録するために使用されたユーザーアカウントが属するテナントです。

注意
この列はデフォルトでは非表示になっています。表に表示するには、表の右上にあるギアアイコンをクリックしてから [**アカウント**] を選択します。

一番左の列は、許可リストに追加するデバイスを選択するために使用します。追加するデバイスごとにチェックボックスを選択して、[**許可リストに追加**] ボタンをクリックします。すべてのチェックボックスを選択または解除するには、列のヘッダーにあるチェックボックスをクリックします。

デバイスのリストを検索したり、フィルタリングしたりすることができます。

- ページ上部の [**検索**] をクリックし、検索用の文字列を入力します。デバイスの説明が入力した文字列と一致する場合、リストに表示されます。
- [**フィルタ**] をクリックし、表示されるダイアログボックスでフィルタを構成して適用します。リスト表示の対象は、フィルタを構成する際に選択したタイプ、ベンダーID、製品ID、アカウントを持つデバイスに限定されます。フィルタをキャンセルしてすべてのデバイスをリストに表示するには、[**デフォルトにリセット**] をクリックします。

データベース内のUSBデバイスのリストをエクスポートします

データベースに追加されたUSBデバイスのリストをエクスポートできます。

1. 編集するデバイスの保護計画を開きます。
2. [**デバイス制御**] スイッチの横にある矢印アイコンをクリックして設定を展開し、[**USBデバイスの許可リスト**] 行をクリックします。
3. [USBデバイスの許可リスト] ページで、[**データベースから追加**] をクリックします。
4. 表示される [USBデバイスデータベースの管理] ページで、[**エクスポート**] をクリックします。
   標準の [参照] ダイアログが開きます。
5. ファイルを保存するロケーションを選択し、必要に応じて新しいファイル名を入力して、[**保存**] をクリックします。

USBデバイスのリストがJSONファイルにエクスポートされます。

エクスポートされたJSONファイルを編集して、デバイスを追加または削除したり、デバイスの説明に一括変更を適用したりできます。

USBデバイスのリストをデータベースにインポートします

Cyber ProtectコンソールからUSBデバイスを追加する代わりに、USBデバイスのリストをインポートできます。リストはJSON形式のファイルです。

注意
JSONファイルに記述されているデバイスが含まれていないデータベースに、JSONファイルをインポートできます。重複するエントリをインポートすることはできないため、変更されたファイルをエクスポート元のデータベースにインポートするには、最初にデータベースをクリアする必要があります。USBデバイスのリストをエクスポートして変更を加え、クリーンアップを実行せずに同じデータベースにインポートしようとすると、インポートは失敗します。

1. 編集するデバイスの保護計画を開きます。
2. **[デバイス制御]** スイッチの横にある矢印アイコンをクリックして設定を展開し、**[USBデバイスの許可リスト]** 行をクリックします。
3. [USBデバイスの許可リスト] ページで、**[データベースから追加]** をクリックします。
4. 表示される [USBデバイスデータベースの管理] ページで、**[インポート]** をクリックします。
   [ファイルからUSBデバイスをインポート] ダイアログが開きます。
5. インポートするファイルをドラッグアンドドロップするか参照します。

Cyber Protectコンソールで、リストの中に、データベースに存在する重複エントリが含まれているかどうかが確認されます。該当する場合それらはスキップされます。データベースの中に存在しないUSBデバイスが追加されます。

コンピューターに搭載されているUSBデバイスのリスト

Cyber Protectコンソールにある、コンピューターのインベントリパネルには、**[USBデバイス]** タブがあります。コンピューターがオンライン状態で、コンピューターにデータ漏洩防止エージェントがインストールされている場合、**[USBデバイス]** タブには、そのコンピューターに接続されたことのあるすべてのUSBデバイスのリストが表示されます。

USBデバイスはツリービューに一覧表示されます。ツリーの最上位レベルは、デバイスモデルを表します。2番目のレベルは、該当モデルの特定のデバイスを表します。

リストには、各デバイスに関する以下の情報が掲載されています。

- **説明** - USBデバイスを接続するときに、オペレーティングシステムにより説明が割り当てられます。この説明は、可読性のあるデバイスの識別情報を提供します。
  デバイスの説明の横にある青いアイコンは、デバイスが現在コンピューターに接続されていることを示しています。デバイスがコンピューターに接続されていない場合は、アイコンがグレーアウトして表示されます。
- **デバイスID** - オペレーティングシステムがデバイスに割り当てた識別子です。この識別子は、以下の形式となります。USB¥VID_<ベンダーID>&PID_<製品ID>¥<シリアルナンバー>（<シリアルナンバー>はオプションです）。例：USB¥VID_0FCE&PID_ADDE¥D55E7FCA（シリアルナンバーのあるデバイス）、USB¥VID_0FCE&PID_ADDE（シリアルナンバーのないデバイス）。

USBデバイスのデータベースにデバイスを追加するには、目的のデバイスのチェックボックスを選択し、**[データベースに追加]** ボタンをクリックします。

アクセス制御からのプロセスの除外

Windowsクリップボード、スクリーンショットのキャプチャ、プリンタ、およびモバイルデバイスへのアクセスは、プロセスに挿入されたフックによって制御されます。プロセスがフックされていない場合、これらのデバイスへのアクセスは制御されません。

注意
プロセスをアクセス制御から除外する機能は、macOSではサポートされていません。適用される保護計画で、除外されるプロセスのリストが構成されている場合、それは無視されます。

除外ページで、フックされないプロセスのリストを指定できます。指定されたプロセスに対しては、クリップボード（ローカルおよびリダイレクト）、スクリーンショットのキャプチャ、プリンタ、およびモバイルデバイスのアクセス制御が適用されなくなります。

たとえば、プリンタへのアクセスを拒否する保護計画を適用してから、Microsoft Wordアプリケーションを起動したとします。このアプリケーションから印刷を実行してもブロックされます。ただし、Microsoft Wordプロセスを除外リストに追加すると、アプリケーションはフックされません。これにより、Microsoft Wordからの印刷はブロックされませんが、他のアプリケーションからの印刷は引き続きブロックされます。

プロセスを除外に追加するには

1. 編集するデバイスの保護計画を開きます。
   保護計画名の横にある省略記号（...）をクリックして、**[編集]** をクリックします。

   注意
   計画でデバイス制御を有効にして、デバイス制御設定にアクセスできるようにする必要があります。

2. **[デバイス制御]** スイッチの横にある矢印をクリックして設定を展開し、**[除外]** 行をクリックします。
3. **除外**ページの **[プロセスとフォルダ]** 行で、**[+追加]** をクリックします。
4. アクセス制御から除外するプロセスを追加します。
   たとえば、`C:\Folder\subfolder\process.exe` と指定します。
   ワイルドカードを使用できます。
   - *は任意の文字数の文字と置き換わります。
   - ?は1文字と置き換わります。

   例:

   ```
   C:\Folder\*
   *\Folder\SubFolder?\*
   *\process.exe
   ```
5. チェックマークをクリックしてから、**[完了]** をクリックします。
6. 保護計画で、**[保存]** をクリックします。
7. 除外したプロセスを再起動して、フックが適切に削除されていることを確認します。

除外されたプロセスは、クリップボード、スクリーンショットのキャプチャ、プリンタ、およびモバイルデバイスのアクセス設定に関わらず、それらのデバイスにアクセスできます。

除外からプロセスを外すには

編集するデバイスの保護計画を開きます。

保護計画名の横にある省略記号（...）をクリックして、**[編集]** をクリックします。

注意
計画でデバイス制御を有効にして、デバイス制御設定にアクセスできるようにする必要があります。

1. **[デバイス制御]** スイッチの横にある矢印をクリックして設定を展開し、**[除外]** 行をクリックします。
2. **除外**ページで、除外から外したいプロセスの横にある、ごみ箱アイコンをクリックします。
3. **[完了]** をクリックします。
4. 保護計画で、**[保存]** をクリックします。
5. プロセスを再開して、フックが適切に挿入されていることを確認します。

保護計画のアクセス設定は、除外から外したプロセスに適用されます。

除外でプロセスを編集するには

1. 編集するデバイスの保護計画を開きます。
   保護計画名の横にある省略記号（...）をクリックして、**[編集]** をクリックします。

   注意
   計画でデバイス制御を有効にして、デバイス制御設定にアクセスできるようにする必要があります。

2. **[デバイス制御]** スイッチの横にある矢印をクリックして設定を展開し、**[除外]** 行をクリックします。
3. **除外**ページで、編集するプロセスの横にある**編集**アイコンをクリックします。
4. 変更を適用し、チェックマークをクリックして確認します。
5. **[完了]** をクリックします。
6. 保護計画で、**[保存]** をクリックします。
7. 影響を受けるプロセスを再起動して、変更が正しく適用されていることを確認します。

デバイス制御アラート

デバイス制御では、制御対象のデバイスタイプ、ポート、またはインターフェイスにアクセスしようとするユーザーの行動をトラックすることで、イベントログを保持します。特定のイベントについてアラートが発生するようにして、Cyber Protectコンソールにログとして保存するようにできます。例えば、デバイス制御モジュールでは、ユーザーが対象となるデバイスにデータをコピーしようとしたとき、またはそのようなデバイスからデータをコピーしようとしたときに、アラートをログに記録して、リムーバブルデバイスの使用を防止するように構成することができます。

デバイス制御モジュールを構成するときに、デバイスのタイプ（スクリーンショットのキャプチャを除く）またはポートの下に列挙されているほとんどのアイテムのアラートを有効化できます。アラートが有効になっている場合、ユーザーが許可されていない操作を実行しようとするたびにアラートが発生します。たとえば、リムーバブルデバイスへのアクセスが読み取り専用に制限されており、そのデバイスタイプで **[アラートの表示]** オプションが選択されている場合、保護されたコンピューターのユーザーがリムーバブルデバイスにデータをコピーしようとするたびにアラートが生成されます。

Cyber Protectコンソールでアラートを確認するには、**[監視]** > **[アラート]** に進みます。各デバイス制御アラートの内部で、コンソールはそれぞれのイベントに関する以下の情報を提供します。

- **タイプ** - 警告。
- **ステータス** - 「周辺デバイスへのアクセスがブロックされました」と表示されます。
- **メッセージ** - 「'<コンピューター名>'の'<デバイスタイプまたはポート>'に対するアクセスがブロックされました」と表示されます。例えば、「'accountant-pc'の'Removable'に対するアクセスがブロックされました」となります。
- **日付と時刻** - イベントが発生した日付と時刻です。
- **デバイス** - イベントが発生したコンピューター名です。
- **計画名** - イベントが発生した保護計画の名前です。
- **ソース** - イベントに関係するデバイスタイプとポートです。例えば、拒否対象のユーザーがリムーバブルデバイスにアクセスしようとした場合、このフィールドには「Removable」デバイスが読み込まれます。
- **アクション** - イベントの原因となった操作です。例えば、拒否対象のユーザーがデバイスにデータをコピーしようとした場合、このフィールドは「Write」を読み取ります。詳細については、「アクションフィールドの値」を参照してください。
- **名前** - ユーザーがコピーしようとしたファイルや、ユーザーが使用しようとしたデバイスなど、イベントのターゲットオブジェクトの名前です。ターゲットオブジェクトが特定できない場合は表示されません。
- **情報** - USBデバイスのデバイスIDなど、イベントのターゲットデバイスに関する追加情報です。ターゲットデバイスに関する追加情報がない場合は表示されません。
- **ユーザー** - イベントの原因となったユーザーの名前です。
- **プロセス** - イベントの原因となったアプリケーションの実行可能ファイルへの完全修飾パスです。場合によっては、パスの代わりにプロセス名が表示されることがあります。プロセス情報が存在しない場合は表示されません。

アラートがUSBデバイス（リムーバブルデバイスおよび暗号化されたリムーバブルデバイスを含む）に適用される場合、管理者はそのデバイスをアラートから直接許可リストに追加して、デバイス制御モジュールによってその特定デバイスへのアクセスが制限されないようにすることができます。**[このUSBデバイスを許可する]** をクリックすると、該当のUSBデバイスが、デバイス制御モジュールの構成で許可リストに追加され、さらに参照用としてUSBデバイスデータベースに追加されます。

関連項目「デバイス制御アラートを表示する手順」も参照してください。

アクションフィールドの値

アラート**アクション**フィールドには、以下の値を含めることができます。

- **読み取り** - デバイスまたはポートからデータを取得します。
- **書き込み** - データをデバイスまたはポートに送信します。
- **フォーマット** - デバイスに直接アクセス（フォーマット、チェックディスクなど）します。ポートの場合は、そのポートに接続されているデバイスに適用されます。
- **イジェクト** - システムからデバイスを削除するか、デバイスからメディアを取り出します。ポートの場合は、そのポートに接続されているデバイスに適用されます。
- **印刷** - プリンタに文書を送信します。
- **オーディオをコピー** - ローカルクリップボードを介してオーディオデータをコピーまたはペーストします。
- **ファイルをコピー** - ローカルクリップボードを介してファイルをコピーまたはペーストします。
- **イメージのコピー** - ローカルクリップボードを介して画像をコピーまたはペーストします。
- **テキストをコピー** - ローカルクリップボードを介してテキストをコピーまたはペーストします。
- **未確認コンテンツのコピー** - ローカルクリップボードを介して他のデータをコピーまたはペーストします。
- **RTFデータ（イメージ）のコピー** - リッチテキスト形式によりローカルクリップボードを介してイメージをコピーまたはペーストします。
- **RTFデータ（ファイル）のコピー** - リッチテキスト形式によりローカルクリップボードを介してファイルをコピーまたはペーストします。
- **RTFデータ（テキスト、イメージ）のコピー** - リッチテキスト形式によりローカルクリップボードを介してイメージを伴うテキストをコピーまたはペーストします。
- **RTFデータ（テキスト、ファイル）のコピー** - リッチテキスト形式によりローカルクリップボードを介してファイルを伴うテキストをコピーまたはペーストします。
- **RTFデータ（イメージ、ファイル）のコピー** - リッチテキスト形式によりローカルクリップボードを介してファイルを伴うイメージをコピーまたはペーストします。
- **RTFデータ（テキスト、イメージ、ファイル）のコピー** - リッチテキスト形式によりローカルクリップボードを介してイメージとファイルを伴うテキストをコピーまたはペーストします。
- **削除** - デバイス（リムーバブルデバイス、モバイルデバイスなど）からデータを削除します。
- **デバイスアクセス** - 一部のデバイスまたはポートへのアクセス（Bluetoothデバイス、USBポートなど）。
- **受信オーディオ** - リダイレクトされたクリップボードを介して、クライアントコンピューターからホストされたセッションにオーディオデータをコピーまたはペーストします。
- **受信ファイル** - リダイレクトされたクリップボードを介して、クライアントコンピューターからホストされたセッションにファイルをコピーまたはペーストします。
- **受信イメージ** - リダイレクトされたクリップボードを介して、クライアントコンピューターからホストされたセッションにイメージをコピーまたはペーストします。
- **受信テキスト** - リダイレクトされたクリップボードを介して、クライアントコンピューターからホストされたセッションにテキストをコピーまたはペーストします。
- **受信未確認コンテンツ** - リダイレクトされたクリップボードを介して、クライアントコンピューターからホストされたセッションに他のデータをコピーまたはペーストします。

- **受信RTFデータ（イメージ）** - リッチテキスト形式によりリダイレクトされたクリップボードを介して、クライアントコンピューターからホストされたセッションにイメージをコピーまたはペーストします。
- **受信RTFデータ（ファイル）** - リッチテキスト形式によりリダイレクトされたクリップボードを介して、クライアントコンピューターからホストされたセッションにファイルをコピーまたはペーストします。
- **受信RTFデータ（テキスト、イメージ）** - リッチテキスト形式によりリダイレクトされたクリップボードを介して、クライアントコンピューターからホストされたセッションにイメージを伴うテキストをコピーまたはペーストします。
- **受信RTFデータ（テキスト、ファイル）** - リッチテキスト形式によりリダイレクトされたクリップボードを介して、クライアントコンピューターからホストされたセッションにファイルを伴うテキストをコピーまたはペーストします。
- **受信RTFデータ（イメージ、ファイル）** - リッチテキスト形式によりリダイレクトされたクリップボードを介して、クライアントコンピューターからホストされたセッションにファイルを伴うイメージをコピーまたはペーストします。
- **受信RTFデータ（テキスト、イメージ、ファイル）** - リッチテキスト形式によりリダイレクトされたクリップボードを介して、クライアントコンピューターからホストされたセッションにイメージとファイルを伴うテキストをコピーまたはペーストします。
- **挿入** - USBデバイスまたはFireWireデバイスを接続します。
- **送信オーディオ** - リダイレクトされたクリップボードを介して、ホストされたセッションからクライアントコンピューターにオーディオデータをコピーまたはペーストします。
- **送信ファイル** - リダイレクトされたクリップボードを介して、ホストされたセッションからクライアントコンピューターにファイルをコピーまたはペーストします。
- **送信イメージ** - リダイレクトされたクリップボードを介して、ホストされたセッションからクライアントコンピューターにイメージをコピーまたはペーストします。
- **送信テキスト** - リダイレクトされたクリップボードを介して、ホストされたセッションからクライアントコンピューターにテキストをコピーまたはペーストします。
- **送信未確認コンテンツ** - リダイレクトされたクリップボードを介して、ホストされたセッションからクライアントコンピューターに他のデータをコピーまたはペーストします。
- **送信RTFデータ（イメージ）** - リッチテキスト形式によりリダイレクトされたクリップボードを介して、ホストされたセッションからクライアントコンピューターにイメージをコピーまたはペーストします。
- **送信RTFデータ（ファイル）** - リッチテキスト形式によりリダイレクトされたクリップボードを介して、ホストされたセッションからクライアントコンピューターにファイルをコピーまたはペーストします。
- **送信RTFデータ（テキスト、イメージ）** - リッチテキスト形式によりリダイレクトされたクリップボードを介して、ホストされたセッションからクライアントコンピューターにイメージを伴うテキストをコピーまたはペーストします。
- **送信RTFデータ（テキスト、ファイル）** - リッチテキスト形式によりリダイレクトされたクリップボードを介して、ホストされたセッションからクライアントコンピューターにファイルを伴うテキストをコピーまたはペーストします。

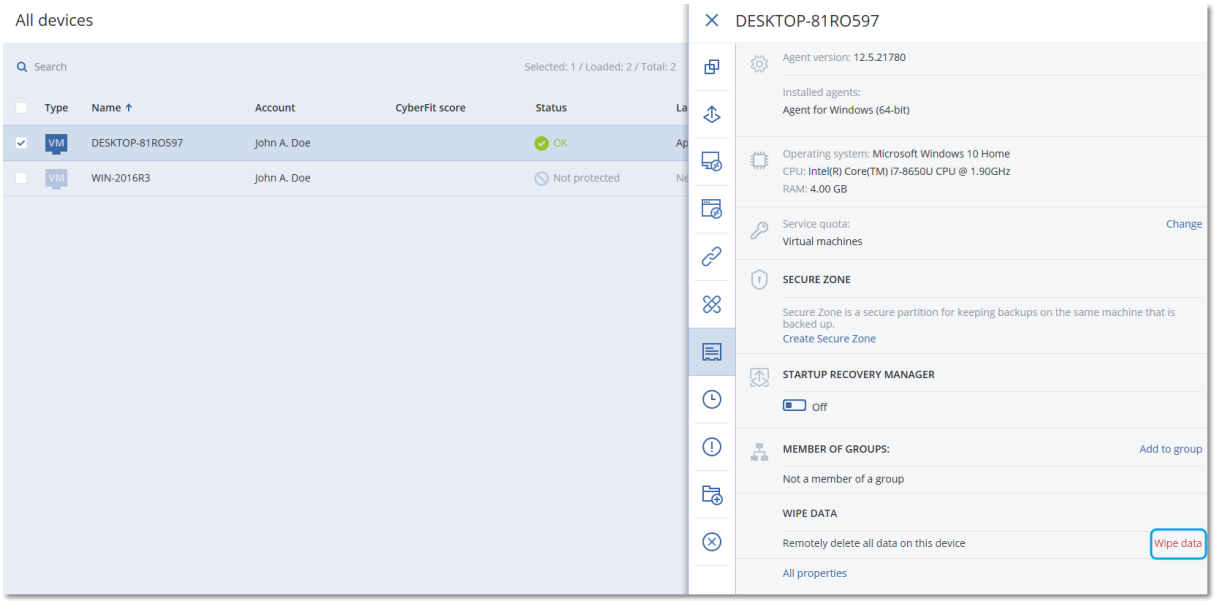
- **送信RTFデータ（イメージ、ファイル）** - リッチテキスト形式によりリダイレクトされたクリップボードを介して、ホストされたセッションからクライアントコンピューターにファイルを伴うイメージをコピーまたはペーストします。
- **送信RTFデータ（テキスト、イメージ、ファイル）** - リッチテキスト形式によりリダイレクトされたクリップボードを介して、ホストされたセッションからクライアントコンピューターにイメージとファイルを伴うテキストをコピーまたはペーストします。
- **名前の変更** - デバイス上（リムーバブルデバイス、モバイルデバイスなど）のファイルの名前を変更します。

マネージドワークロードでデータをワイピングする

注意
Advanced Securityパックでは、リモートワイプ機能が利用できます。

リモートワイプでは、マシンが紛失したり盗まれたりした場合に、Cyber Protectionサービス管理者とマシン所有者が管理対象のマシンのデータを削除できます。このため、機密情報への不正アクセスが防止されます。

リモートワイプは、Windowsバージョン10以降が実行されているマシンでのみ使用できます。ワイプコマンドを受信するには、マシンをオンにし、インターネットに接続する必要があります。



マシンからデータをワイプするには

1. Cyber Protectコンソールで **[デバイス]** > **[すべてのデバイス]** に進みます。
2. ワイプするデータがあるマシンを選択します。

   注意
   一度に1台のマシンからデータをワイプできます。

3. **[詳細]** をクリックしてから、**[データのワイプ]** をクリックします。

選択したマシンがオフラインの場合、[**データのワイプ**] オプションは使用不可になります。

4. 選択内容を確認入力します。
5. このマシンのローカル管理者の資格情報を入力してから、[**データのワイプ**] をクリックします。

注意
[**監視**] > [**アクティビティ**] では、ワイピングの詳細と操作を開始したユーザーを確認できます。

CyberAppワークロード

CyberAppワークロードは、独立ソフトウェアベンダー（ISV）によって作成され、CyberApp統合が有効になると、Cyber Protectコンソールに表示されます。以下の条件を満たす必要があります。

- CyberAppで**ワークロードと操作**拡張ポイントが有効化されている。
- CyberAppで少なくとも1つの**ワークロードタイプ**が定義されている。
- 独立ソフトウェアベンダー（ISV）がホストする接続サービスでは、CyberAppワークロードがAcronisプラットフォームに追加され、またアップデートされるようにする。

ベンダーポータルとCyberAppsの作成の詳細については、『ベンダーポータルユーザーガイド』を参照してください。

集約ワークロード

物理ワークロードには、Cyber Protectエージェントと1つまたは複数のCyberAppエージェントが同時にインストールされている場合があります。この場合、同じワークロードが**すべてのデバイス**画面に複数表示され、Acronisワークロードと各CyberAppワークロードに別々のレコードが表示されます。ワークロードの自動マージが有効になっており、ベンダーポータルまたはCyber Protectコンソールから構成されている場合、システムによりAcronisワークロードのホストアドレスとMACアドレスが比較され、表示されているワークロードは、1件の集約ワークロードにマージされます。また、Cyber Protectコンソールでワークロードを手動でマージしたり、マージを解除したりできます。

CyberAppワークロードの動作

Cyber Protectコンソールにビルトインされている標準的な操作とは別に、CyberAppワークロードがコンソールに表示された後でこれらの操作を実行できます。ワークロードを手動で統合ワークロードにマージし、CyberAppで設定されたカスタム操作を実行します。

マージ

前提条件

- テナントでさまざまなソースからのワークロードを利用できます。

Acronisワークロードを1つまたは複数のCyberAppワークロードに手動でマージして、単一の集約ワークロードにすることができます。

手動でワークロードを集約ワークロードにマージするには

1. **すべてのデバイス**画面で、マージしたいワークロードを選択します。

   注意
   AcronisワークロードとCyberAppワークロードなど、異なるソースからワークロードを選択した場合、マージ操作が表示されます。

2. **[ワークロードをマージ]** をクリックします。

カスタム操作を実行

前提条件

- テナントで、**ワークロード操作**が定義されているCyberApp統合が有効になっている。

カスタム操作とは、CyberAppで構成された操作のことであり、テナントのCyberApp統合を有効にすると、対応するCyberAppワークロードで利用できるようになります。

カスタム操作を実行するには

1. **[すべてのデバイス]** 画面で、ワークロードをクリックします。
2. **[統合アプリ保護]** をクリックします。
3. 操作をクリックします。

集約ワークロードの動作

Cyber Protectコンソールにビルトインされている標準的な操作とは別に、集約ワークロードに対して、詳細の表示、ソースワークロードのマージ解除、CyberAppsで構成されたカスタム操作の実行の各処理を行えます。

詳細の表示

前提条件

- 少なくとも1つの集約ワークロードがテナントで利用可能です。

集約ワークロードの詳細を表示するには

1. **すべてのデバイス**画面で、集約ワークロードをクリックします。
2. **[詳細]** をクリックします。
   集計ワークロードの詳細は、タブごとに分割されています。各タブには、各ワークロードの詳細が表示されます。

結合解除

前提条件

- 少なくとも1つの集約ワークロードがテナントで利用可能です。

集約ワークロードのマージを解除すると、デバイスリストに表示されなくなります。代わりに、集約ワークロードにマージされた各ソースワークロードの個別エントリが表示されます。

集約ワークロードのマージを解除するには

1. **すべてのデバイス**画面で、マージを解除したい集約ワークロードをクリックします。
2. **[ソースワークロードの結合を解除]** をクリックします。
3. 確認ウィンドウで **[結合解除]** をクリックします。

カスタム操作を実行

前提条件

- テナントで、**ワークロード操作**が定義されているCyberApp統合が少なくとも1件有効になっている。

カスタム操作とは、CyberAppで構成された操作のことであり、テナントのCyberApp統合を有効にすると、対応するCyberAppワークロードで利用できるようになります。

カスタム操作を実行するには

1. **[すべてのデバイス]** 画面で、ワークロードをクリックします。
2. **[統合アプリ保護]** をクリックします。
3. 利用可能なカスタム操作に応じて、以下のいずれかを実行します。
   - 集約ワークロードにCyberAppワークロードが1件のみ存在する場合は、操作をクリックします。
   - 集約ワークロードに複数のCyberAppワークロードが存在する場合は、CyberAppの名前をクリックしてから、操作をクリックします。

最終ログインユーザーを検索

管理者がデバイスを管理するには、どのユーザーがデバイスにログインしているか、および過去にログインしていたかを特定する必要があります。この情報は、ダッシュボードやワークロードの詳細に表示されます。

最終ログイン情報の表示を有効化または無効化するには、リモート管理計画で設定を変更します。

オンラインダッシュボードで次の操作を実行します。

1. **[デバイス]** をクリックします。**[すべてのデバイス]** ウィンドウが表示されます。
2. **最終ログイン**列には、各デバイスに最後にログインしたユーザーの名前が表示されます。
3. **最終ログイン時刻**列には、各デバイスで最後のユーザーログインがあった時間が表示されます。

デバイスの詳細で次の操作を実行します。

1. **[デバイス]** をクリックします。**[すべてのデバイス]** ウィンドウが表示されます。
2. 詳細を確認したいデバイスをクリックします。
3. **詳細**アイコンをクリックします。選択したデバイスに最後にログインしたユーザー名と、日付および時刻が **[最終ユーザーログイン]** セクションに表示されます。

注意
[最終ユーザーログイン] セクションには、デバイスにログインしたユーザーが最大5件まで表示されます。

ダッシュボードで最終ログイン列と最終ログイン時刻列の表示/非表示を切り替えるには

1. **[デバイス]** をクリックします。**[すべてのデバイス]** ウィンドウが表示されます。
2. 右上隅のギアアイコンをクリックし、**[一般]** セクションで以下のいずれかを実行します。
   - ダッシュボードに表示する場合は、**最終ログイン**および**最終ログイン時刻**列を有効にします。
   - ダッシュボードで非表示にする場合は、**最終ログイン**および**最終ログイン時刻**列を無効にします。

ワークロード/ファイルのバックアップを復元および管理する

バックアップモジュールでは、物理マシン、仮想マシン、ファイル、データベースのクラウドストレージまたはローカルストレージへのバックアップと復元を行えます。

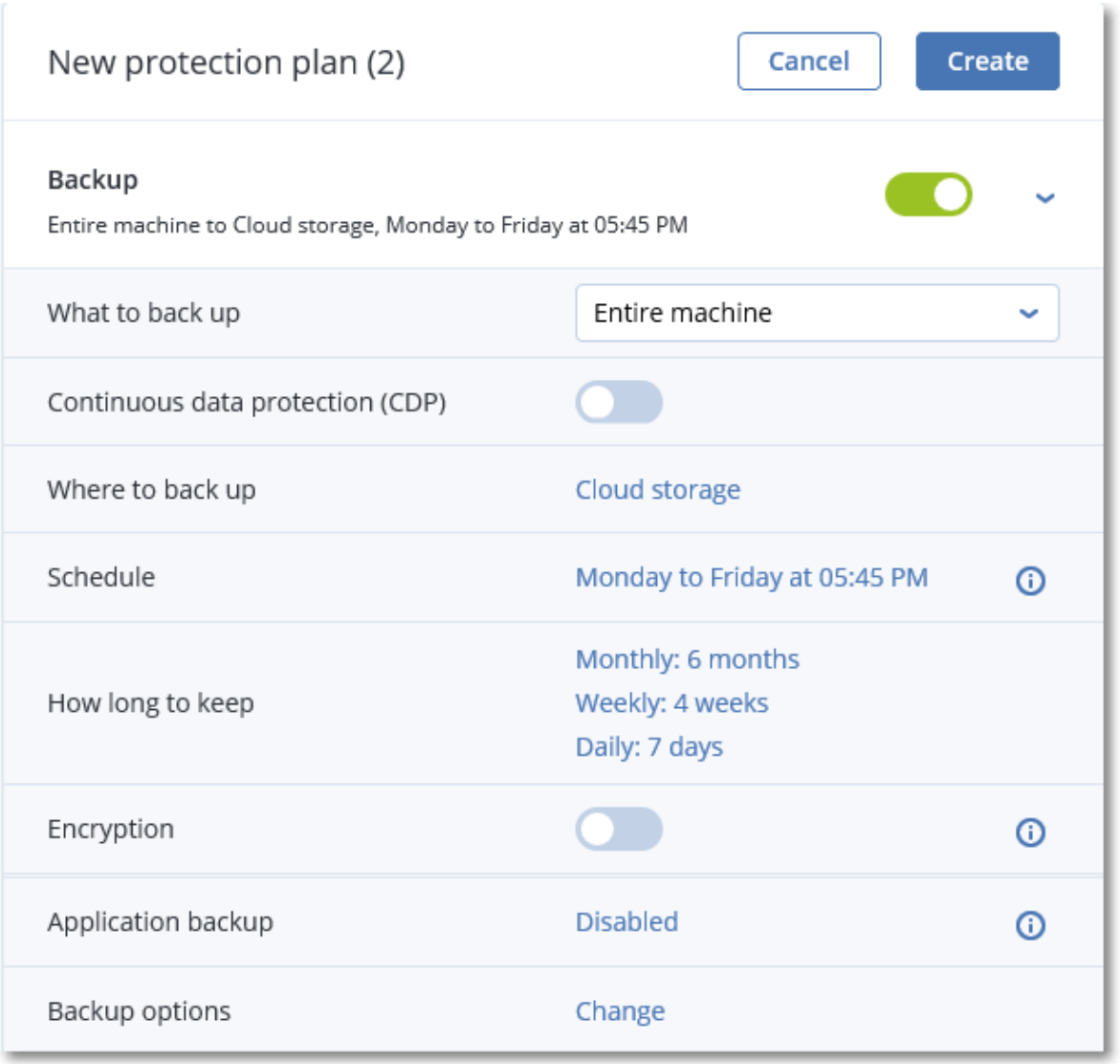
バックアップ

バックアップモジュールを有効にした保護計画は、マシン上でデータを保護する方法を指定したルールのセットです。

保護計画は、計画の作成時に複数のマシンに適用できます。後から適用することもできます。

バックアップモジュールを有効にした最初の保護計画の作成

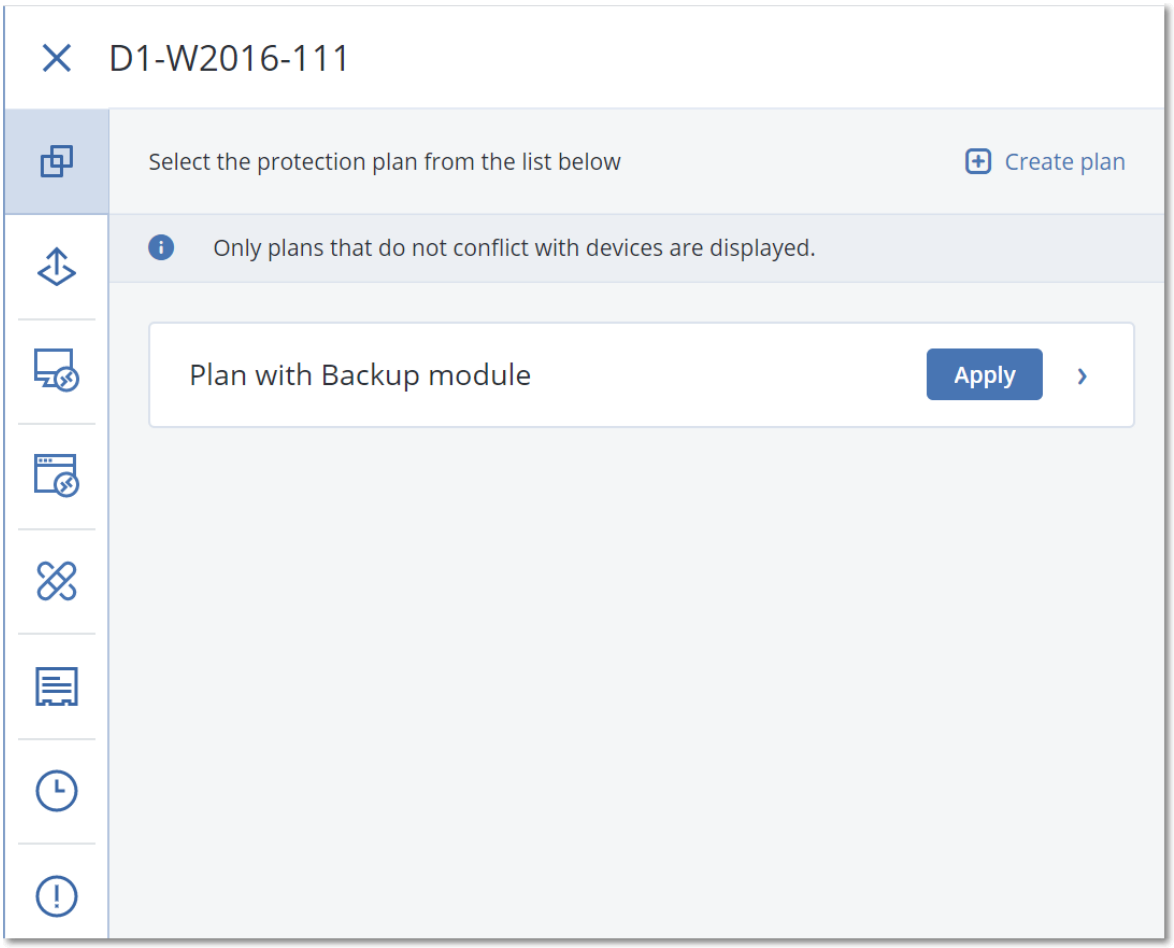
1. バックアップ対象のコンピュータを選択します。
2. **[保護]** をクリックします。
   マシンに適用されている保護計画が表示されます。どの計画もまだ適用されていないマシンの場合、適用可能なデフォルトの保護計画が表示されます。必要に応じてこの計画の設定を調整することも、新しい計画を作成することもできます。
3. 新しい計画を作成するには、**[計画の作成]** をクリックします。**[バックアップ]** モジュールを有効にしてから設定を展開します。



4. （オプション）保護計画名を変更するには、デフォルト名をクリックします。
5. （オプション）バックアップモジュールのパラメータを変更するには、保護計画パネルの該当する設定をクリックします。
6. （オプション）バックアップオプションを変更するには、**[バックアップオプション]** の横にある **[変更]** をクリックします。
7. **[作成]** をクリックします。

既存の保護計画を適用する手順

1. バックアップ対象のコンピュータを選択します。
2. **[保護]** をクリックします。選択したマシンに共通の保護計画が既に適用されている場合は、**[計画の追加]** をクリックします。
   以前に作成された保護計画が表示されます。



3. 適用する保護計画を選択します。
4. **[適用]** をクリックします。

保護計画のチートシート

次の表は、使用可能な保護計画の設定内容を示しています。この表を使用して、要件に最も適した保護計画を作成してください。

バックアップ対象	バックアップする項目 選択方法	バックアップ先	スケジュール バックアップ スキーム	保存期間
ディスク/ボリューム（物理マシン[1]）	直接選択 ポリ	クラウド ローカルフォルダ	常に増分（単一ファイル） 常に完全	バックアップ経過時間に基づく（バックアップ 設定ごとに1つのルール）

[1]オペレーティングシステムにインストールされたエージェントによってバックアップされるマシン。

	シールール ファイルフィルタ	ネットワークフォルダ NFS* Secure Zone**	週単位で完全、日単位で増分 月単位で完全、週単位で差分、日単位で増分（GFS） カスタム（F-D-I）	バックアップの数 バックアップの合計サイズ別*** 無期限に保存
ディスク/ボリューム（仮想マシン[1]）	ポリシールール ファイルフィルタ	クラウド ローカルフォルダ ネットワークフォルダ NFS*		
ファイル（物理マシンのみ[2]）	直接選択 ポリシールール ファイルフィルタ	クラウド ローカルフォルダ ネットワークフォルダ NFS* Secure Zone**	常に増分（単一ファイル） 常に完全 週単位で完全、日単位で増分 月単位で完全、週単位で差分、日単位で増分（GFS） カスタム（F-D-I）	
ESXi構成	直接選択	ローカルフォルダ ネットワークフォルダ NFS*		
Webサイト（ファイルとMySQLデータベース）	直接選択	クラウド	—	

[1]VMwareエージェントやHyper-Vエージェントなどの外部エージェントによってハイパーバイザーレベルでバックアップされる仮想マシン。 エージェントがインストールされている仮想マシンは、バックアップの観点から物理マシンとして扱われます。
[2]オペレーティングシステムにインストールされたエージェントによってバックアップされるマシン。

<table>
<tr><td colspan="2">システム状態</td><td rowspan="3">直接選択</td><td rowspan="3">クラウド
ローカルフォルダ
ネットワークフォルダ</td><td rowspan="3">常に完全
週単位で完全、日単位で増分
カスタム（F-I）</td></tr>
<tr><td colspan="2">SQLデータベース</td></tr>
<tr><td colspan="2">Exchangeデータベース</td></tr>
<tr><td rowspan="6">Microsoft 365</td><td>メールボックス
（ローカルのMicrosoft 365エージェント）</td><td>直接選択</td><td>クラウド
ローカルフォルダ
ネットワークフォルダ</td><td>常に増分（単一ファイル）- SQLデータベースのみ</td></tr>
<tr><td>メールボックス
（Microsoft 365クラウドエージェント）</td><td rowspan="3">直接選択</td><td rowspan="4">クラウド</td><td rowspan="4">1日最大6回のバックアップ</td></tr>
<tr><td>パブリック フォルダ</td></tr>
<tr><td>Teams</td></tr>
<tr><td>OneDriveファイル</td><td>直接選択</td></tr>
<tr><td>SharePoint Onlineデータ</td><td>ポリシールール</td></tr>
<tr><td rowspan="3">Google Workspace</td><td>Gmail メールボックス</td><td>直接選択</td><td rowspan="3">クラウド</td><td rowspan="3">1日最大6回のバックアップ</td></tr>
<tr><td>Google ドライブのファイル</td><td>直接選択</td></tr>
<tr><td>共有ドライブファイル</td><td>ポリシールール</td></tr>
</table>

* Windowsでは、NFS共有へのバックアップは使用できません。

** Macでは、Secure Zoneを作成できません。

*** **バックアップの合計サイズ別**保持ルールは、**[常に増分（単一ファイル）]** バックアップスキームが指定されている場合、またはクラウドストレージにバックアップする場合には使用できません。

バックアップ対象の選択

マシン全体を選択する

マシン全体のバックアップとは、リムーバブルディスクを除くすべてのディスクをバックアップすることを意味します。ディスクバックアップの詳細については、「"ディスクまたはボリュームの選択"（390ページ）」を参照してください。

制限事項

- 暗号化されたAPFSボリュームがロックされている場合、ディスクレベルバックアップはサポートされません。マシン全体のバックアップにおいて、このようなボリュームはスキップされます。
- デフォルトでは、OneDriveのルートフォルダはバックアップ操作から除外されています。特定のOneDrive ファイルやフォルダのバックアップを選択すると、それらの対象がバックアップされます。デバイス上でファイルが利用できない場合、バックアップセット内に無効な内容が含められます。

ディスクまたはボリュームの選択

ディスクレベルバックアップには、ディスクのコピーまたはパッケージ化されたボリュームが含まれます。ディスクレベルバックアップから、ディスク、ボリューム、フォルダ、ファイルをリカバリすることができます。

保護計画内の個々のワークロードごとにバックアップするディスクまたはボリュームを選択（直接選択）することも、複数のワークロードに対してポリシールールを構成することもできます。さらに、ファイルフィルタを構成することで、特定のファイルをバックアップから除外したり、特定のファイルのみをバックアップに含めることができます。詳細については、"ファイルフィルタ（除外/包含）"（450ページ）を参照してください。

ディスクまたはボリュームを選択するには

直接選択

直接選択は、物理マシンのみで使用できます。

1. **[バックアップの対象]** で、**[ディスク/ボリューム]** を選択します。
2. **[バックアップする項目]** をクリックします。
3. **[バックアップする項目]** で、**[直接]** を選択します。
4. 保護計画に含まれるそれぞれのワークロードで、バックアップするディスクまたはボリュームの横にあるチェックボックスを選択します。
5. **[完了]** をクリックします。

ポリシールールを使用する

1. **[バックアップの対象]** で、**[ディスク/ボリューム]** を選択します。
2. **[バックアップする項目]** をクリックします。

3. **[バックアップする項目]** で、**[ポリシールールを使用]**を選択します。
4. 事前に定義されたルールを選択するか、独自のルールを入力するか、両方を組み合わせます。

   利用できるポリシールールの詳細については、"ディスクとボリュームのポリシールール"（392ページ）を参照してください。

   保護計画に含まれているすべてのワークロードにポリシールールが適用されます。

   指定されたルールがワークロードに適用できない場合、そのワークロードのバックアップは失敗します。
5. **[完了]** をクリックします。

制限事項

- 暗号化されたAPFSボリュームがロックされている場合、ディスクレベルバックアップはサポートされません。マシン全体のバックアップにおいて、このようなボリュームはスキップされます。
- デフォルトでは、OneDriveのルートフォルダはバックアップ操作から除外されています。特定のOneDrive ファイルやフォルダのバックアップを選択すると、それらの対象がバックアップされます。デバイス上でファイルが利用できない場合、バックアップセット内に無効な内容が含められます。
- 物理マシンに接続されたディスクをiSCSIプロトコルでバックアップできます。ただし、VMwareエージェントまたはHyper-Vエージェントでの iSCSI接続ディスクをバックアップする場合は制限事項があります。詳細については、"制限事項"（33ページ）を参照してください。

ディスクまたはボリュームのバックアップに保存される内容

ディスクまたはボリュームのバックアップには、ディスクまたはボリュームの**ファイルシステム**全体と、オペレーティングシステムを起動するうえで必要なすべての情報が保存されます。これらのバックアップからはディスクまたはボリュームの全体を復元することも、個別のフォルダやファイルを復元することもできます。

セクタ単位（RAWモード）のバックアップ オプションをオンにすると、ディスクバックアップにディスクのセクタがすべて保存されます。セクタ単位のバックアップは、認識されないまたはサポートされないファイル システムや他の独自のデータ形式を使用しているディスクをバックアップするときに使用できます。

Windows

ボリューム バックアップには、隠しファイル、システム ファイルなどの属性に関係なく、選択されたボリュームのすべてのファイルとフォルダ、ブート レコード、存在する場合はファイル アロケーション テーブル（FAT）、マスタ ブート レコード（MBR）を含むハード ディスクのルート トラックとゼロ トラックが保存されます。

ディスク バックアップには、ベンダの保守パーティションなどの隠しボリュームを含む、選択されたディスクのすべてのボリュームと、マスタ ブート レコードを含むゼロ トラックが保存されます。

次の項目は、ディスクまたはボリュームのバックアップ（およびファイルレベルのバックアップ）には含まれません。

- スワップ ファイル（pagefile.sys）およびコンピュータが休止状態になったときに RAM の内容を保存するファイル（hiberfil.sys）。リカバリ後は、それらのファイルが適切な場所にサイズ 0 で再作成されます。
- バックアップがオペレーティングシステムの下で実行された場合（ブータブルメディアではなく、またはハイパーバイザレベルでの仮想コンピュータのバックアップではなく）：
  - Windows シャドウ ストレージ。このストレージのパスは、レジストリキー**HKEY_LOCAL_MACHINE¥SYSTEM¥CurrentControlSet¥Control¥BackupRestore¥FilesNotToBackup**にあるレジストリ値**VSS Default Provider**で指定されます。これは、Windows Vista以降のオペレーティングシステムでは、Windowsの復元ポイントがバックアップされないことを意味します。
  - **ボリュームシャドウコピーサービス（VSS）**バックアップ オプションが有効の場合、**HKEY_LOCAL_MACHINE¥SYSTEM¥CurrentControlSet¥Control¥BackupRestore¥FilesNotToSnapshot**レジストリキーに指定されているファイルとフォルダ。

Linux

ボリューム バックアップには、属性に関係なく、選択されたボリュームのすべてのファイルとディレクトリ、ブート レコード、ファイル システム スーパー ブロックが保存されます。

ディスク バックアップにはすべてのディスク ボリュームとマスタ ブート レコードを含むゼロ トラックが保存されます。

Mac

ディスクまたはボリュームのバックアップには、選択したディスクまたはボリュームの全ファイルおよびディレクトリと、ボリュームレイアウトの説明が保存されます。

次のアイテムは除外されます。

- システムメタデータ、たとえばファイルシステムジャーナルやSpotlightインデックス
- ゴミ箱
- Time Machineバックアップ

物理的には、Mac上のディスクとボリュームはファイルレベルでバックアップされます。ディスクおよびボリュームバックアップからのベアメタル復元は可能ですが、セクタ単位のバックアップモードは使用できません。

ディスクとボリュームのポリシールール

バックアップするディスクまたはボリュームを選択するときに、保護対象のワークロードのオペレーティングシステムに応じて、次のポリシールールを使用できます。

Windows

- `[All Volumes]` では、マシン上のすべてのボリュームが選択されます。
- ドライブ文字（`C:\` など）には、指定されたドライブ文字のボリュームを選択します。

- [Fixed Volumes (physical machines)] では、リムーバブルメディア以外の物理マシンの全ボリュームが選択されます。固定ボリュームには、SCSI、ATAPI、ATA、SSA、SAS、SATAの各デバイスおよび RAIDアレイ上のボリュームがあります。
- [BOOT+SYSTEM] では、システムおよびブートボリュームが選択されます。これは、オペレーティングシステムをリカバリするための最小限の組み合わせです。
- [Disk 1] は、マシンの最初のディスクを選択し、そのディスク上のボリュームすべてを含みます。別のディスクを選択するには、該当する番号を入力します。

Linux

- [All Volumes] では、マシンでマウントされたすべてのボリュームが選択されます。
- /dev/hda1は、最初のIDEハードディスクの最初のボリュームを選択します。
- /dev/sda1は、最初のSCSIハードディスクの最初のボリュームを選択します。
- /dev/md1は、最初のソフトウェア RAIDハードディスクを選択します。
- その他のベーシックボリュームを選択するには、/dev/xdyNを指定します。
  - 「x」はディスクの種類に対応します。
  - 「y」はディスク番号に対応します（「a」は 1 番目のディスク、「b」は 2 番目のディスクなど）
  - 「N」はボリューム番号です。
- 論理ボリュームを選択するには、rootアカウントでls /dev/mapperコマンドを実行した後に表示されるパスを指定します。

  例:

  ```
  [root@localhost ~]# ls /dev/mapper/
  control vg_1-lv1 vg_1-lv2
  ```

  この出力は、vg_1ボリュームグループに属するlv1とlv2の2つの論理ボリュームを示しています。これらのボリュームをバックアップするには、次を指定します。

  /dev/mapper/vg_1-lv1

  /dev/mapper/vg-l-lv2

macOS

- [All Volumes] では、マシンでマウントされたすべてのボリュームが選択されます。
- [Disk 1] は、マシンの最初のディスクを選択し、そのディスク上のボリュームすべてを含みます。別のディスクを選択するには、該当する番号を指定します。

ファイルまたはフォルダの選択

ファイルレベルのバックアップを使用して、特定のデータ（例えば、現在のプロジェクトのファイル）のみを保護します。ファイルレベルのバックアップはディスクレベルバックアップよりも小さいため、ストレージスペースを節約できます。

重要
ファイルレベルのバックアップからオペレーティングシステムをリカバリすることはできません。

保護計画内の個々のワークロードごとにバックアップするファイルまたはフォルダを選択（直接選択）することも、複数のワークロードに対してポリシールールを構成することもできます。さらに、ファイルフィルタを構成することで、特定のファイルをバックアップから除外したり、特定のファイルのみをバックアップに含めることができます。詳細については、"ファイルフィルタ（除外/包含）"（450ページ）を参照してください。

ファイルまたはフォルダを選択するには

直接選択

1. **[バックアップの対象]** で、**[ファイル/フォルダ]** を選択します。
2. **[バックアップする項目]** で **[指定]** をクリックします。
3. **[バックアップする項目]** で、**[直接]** を選択します。
4. 保護計画のワークロードごとにバックアップするファイルまたはフォルダを指定します。
   a. **[ファイルとフォルダの選択]** をクリックします。
   b. **[ローカル フォルダ]** または **[ネットワークフォルダ]** をクリックします。
      選択したマシンからネットワークフォルダへのアクセス環境が必要です。
      ソースとして**ネットワークフォルダ**を選択すると、NetAppデバイスなどのネットワーク接続ストレージ（NAS）からデータをバックアップできます。すべてのベンダーのNASデバイスがサポートされています。
   c. フォルダツリーで、必要なファイルまたはフォルダに移動します。
      または、それらのパスを指定し、矢印ボタンをクリックします。
   d. （共有フォルダの場合）プロンプトが表示されたら、共有フォルダへのアクセス認証情報を指定します。
      匿名アクセスでのフォルダのバックアップはサポートされていません。
   e. 必要なファイルとフォルダを選択します。
   f. **[完了]** をクリックします。

ポリシールールを使用する

1. **[バックアップの対象]** で、**[ファイル/フォルダ]** を選択します。
2. **[バックアップする項目]** で **[指定]** をクリックします。
3. **[バックアップする項目]** で、**[ポリシールールを使用]**を選択します。
4. 事前に定義されたルールを選択するか、独自のルールを入力するか、両方を組み合わせます。
   利用できるポリシールールの詳細については、"ファイルおよびフォルダのポリシールール"（395ページ）を参照してください。
   保護計画に含まれているすべてのワークロードにポリシールールが適用されます。
   指定されたルールがワークロードに適用できない場合、そのワークロードのバックアップは失敗します。
5. **[完了]** をクリックします。

制限事項

- エージェントがインストールされた物理マシンまたは仮想マシンをバックアップする際に、ファイルやフォルダを選択できます（エージェントベースのバックアップ）。ファイルレベルのバックアップは、エージェントレスモードでバックアップする仮想マシンでは使用できません。これらのバックアップタイプの違いについては、"エージェントベースのバックアップとエージェントレスバックアップ"（65ページ）を参照してください。
- デフォルトでは、OneDriveのルートフォルダはバックアップ操作から除外されています。特定のOneDrive ファイルやフォルダのバックアップを選択すると、それらの対象がバックアップされます。デバイス上でファイルが利用できない場合、バックアップセット内に無効な内容が含められます。
- iSCSIプロトコルで物理マシンに接続されたディスク上にあるファイルやフォルダをバックアップできます。VMwareエージェントまたはHyper-Vエージェントで iSCSI接続ディスクのデータをバックアップする場合は、いくつかの制限事項があります。

ファイルおよびフォルダのポリシールール

バックアップするファイルまたはフォルダを選択するときに、保護対象のワークロードのオペレーティングシステムに応じて、次のポリシールールを使用できます。

Windows

- ファイルまたはフォルダへのフルパス。例: `D:\Work\Text.doc`または`C:\Windows`など。
- 事前に定義されたルール:
  - `[All Files]` は、マシン上のすべてのボリュームのすべてのファイルを選択します。
  - `[All Profiles Folder]` では、すべてのユーザープロファイルが存在するフォルダが選択されます。例: `C:\Users`または`C:\Documents and Settings`など。
- 環境変数：
  - `%ALLUSERSPROFILE%`では、すべてのユーザープロファイルの共通データが存在するフォルダが選択されます。例: `C:\ProgramData`または`C:\Documents and Settings\All Users`など。
  - `%PROGRAMFILES%`では、`Program Files`フォルダが選択されます。例: `C:\Program Files`。
  - `WINDIR%`では、`Windows`フォルダが選択されます。例: `C:\Windows`。

  他の環境変数を使用したり、環境変数とテキストを組み合わせて使用したりすることができます。例えば、Program Filesフォルダ内のJavaフォルダを選択するには、`%PROGRAMFILES%\Java`を指定します。

Linux

- ファイルまたはディレクトリへのフルパス。

  例えば、`/home/usr/docs`にマウントされているボリューム`/dev/hda3`上の`file.txt`ファイルをバックアップするには、`/dev/hda3/file.txt`または`/home/usr/docs/file.txt`を指定します。
- 事前に定義されたルール:
  - `[All Profiles Folder]` では、`/home`が選択されます。デフォルトでは、すべてのユーザープロファイルはこのフォルダに保存されます。

- `/home`は、共通ユーザーのホームディレクトリを選択します。
- `/root`は、rootユーザーのホームディレクトリを選択します。
- `/usr`は、ユーザーに関連するすべてのプログラムのディレクトリを選択します。
- `/etc`は、システム構成ファイルのディレクトリを選択します。

macOS

- ファイルまたはディレクトリへのフルパス。
  例:
  - ユーザーのデスクトップ上の`file.txt`をバックアップするには、`/Users/<`**ユーザー名**`>/Desktop/file.txt`を指定します。
  - ユーザーの**デスクトップ**、**ドキュメント**および**ダウンロード**フォルダをバックアップするには、`/Users/<`**ユーザー名**`>/Desktop`、`/Users/<`**ユーザー名**`>/Documents`、および`/Users/<`**ユーザー名**`>/Downloads`と指定します。
  - このマシンにアカウントを持つすべてのユーザーのホームフォルダをバックアップするには、`/Users`を指定します。
  - アプリケーションがインストールされたフォルダをバックアップするには、`/Applications`を指定します。
- 事前に定義されたルール
  - `[All Profiles Folder]`では、`/Users`が選択されます。デフォルトでは、すべてのユーザープロファイルはこのフォルダに保存されます。

システム状態の選択

注意
システム状態のバックアップは、Windowsエージェントがインストールされている Windows 7以降のマシンで利用できます。ハイパーバイザーレベルでバックアップされる仮想マシン（エージェントレスバックアップ）では、システム状態のバックアップは利用できません。

システム状態をバックアップするには、[**バックアップの対象**] で[**システム状態**] を選択します。

システム状態のバックアップは、次のファイルから構成されます。

- タスクスケジューラ構成
- VSS Metadata Store
- パフォーマンスカウンタ構成情報
- MS Search Service
- バックグラウンドインテリジェント転送サービス（BITS）
- レジストリ
- Windows Management Instrumentation（WMI）
- Component Services Class登録データベース

ESXi構成の選択

ESXiホスト構成のバックアップにより、ESXiホストをベアメタルに復元できます。この復元はブータブルメディアで実行されます。

ホストで実行中の仮想コンピュータは、バックアップ内に含まれません。バックアップと復元をそれぞれ個別に行えます。

ESXiホスト構成のバックアップには以下が含まれます。

- ホストのブートバンクパーティションとブートローダー
- ホストの状態（仮想ネットワークとストレージの構成、SSLキー、サーバーネットワーク設定、ローカルユーザー情報）
- ホストにインストールまたはステージングされた拡張機能やパッチ
- ログファイル

前提条件

- ESXiホスト構成の **[セキュリティプロファイル]** では、SSHが有効になっている必要があります。
- ESXiホストの「ルート」アカウントのパスワードを知っている必要があります。

制限事項

- VMware ESXi 7.0以降を実行するホストでは、ESXi設定のバックアップはサポートされていません。
- ESXi構成をクラウドストレージにバックアップできません。

ESXi構成を選択する手順

1. **[デバイス]** > **[すべてのデバイス]** をクリックし、バックアップするESXiホストのロケーションを参照します。
2. **[保護]** をクリックします。
3. **[バックアップの対象]** で **[ESXi構成]** を選択します。
4. **[ESXiの「ルート」パスワード]** で、選択した各ホストの「ルート」アカウントのパスワードを指定するか、すべてのホストに同じパスワードを適用します。

継続的データ保護（CDP）

継続的データ保護（CDP）は、Advanced Backupパックの一部です。継続的データ保護（CDP）では、このデータが変更された直後に重要なデータがバックアップされます。これにより、2回のスケジュール済みバックアップの間にシステム障害が発生した場合でも変更が失われないようにします。次のデータに対して継続的データ保護を構成できます。

- 特定のロケーションにあるファイルまたはフォルダ
- 特定のアプリケーションによって変更されたファイル

継続的データ保護は、NTFSファイルシステムと次のオペレーティングシステムでのみサポートされます。

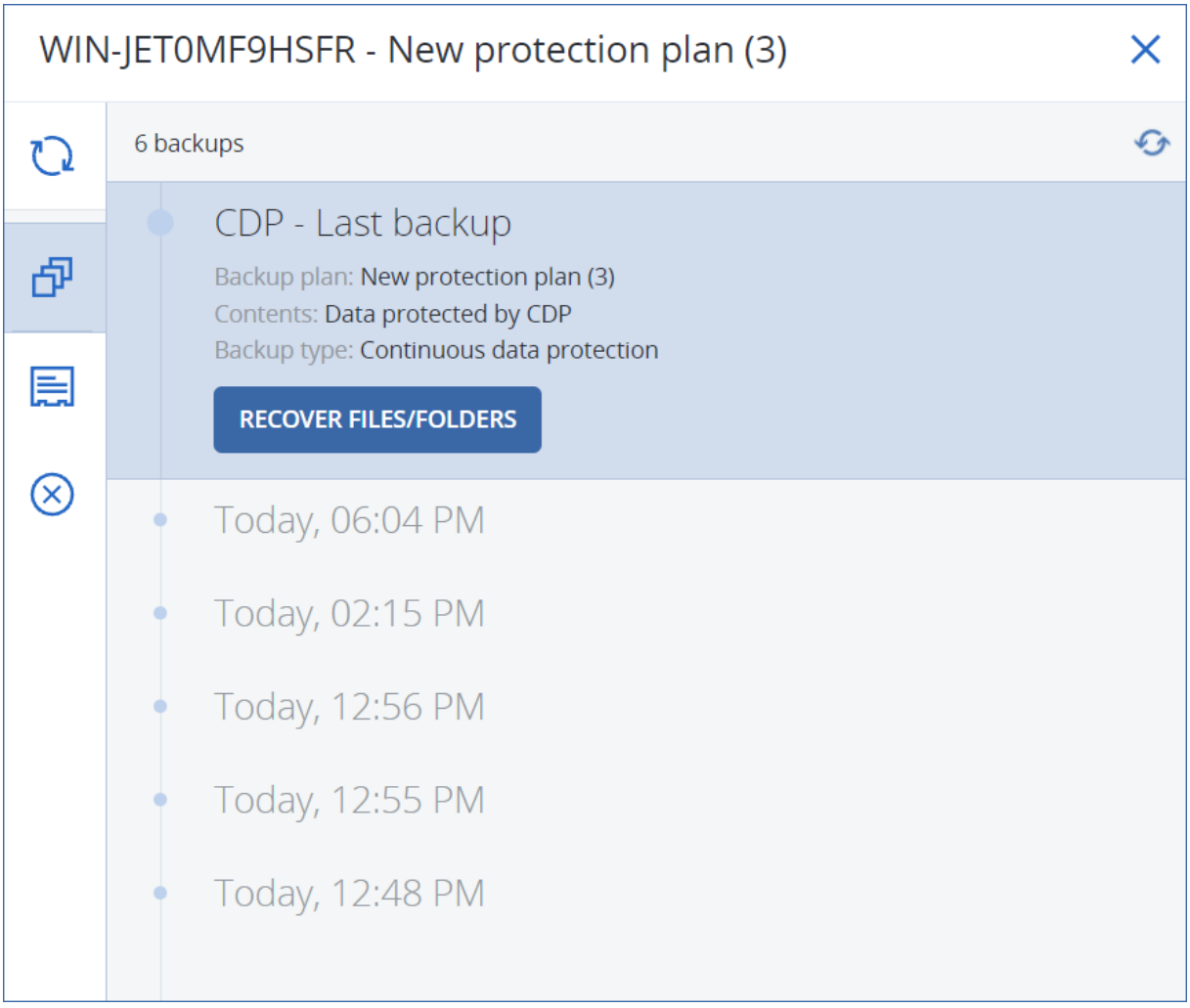
- デスクトップ:Windows 7以降
- サーバー:Windows Server 2008 R2以降

ローカルフォルダのみサポートされます。継続的データ保護のためにネットワークフォルダを選択することはできません。

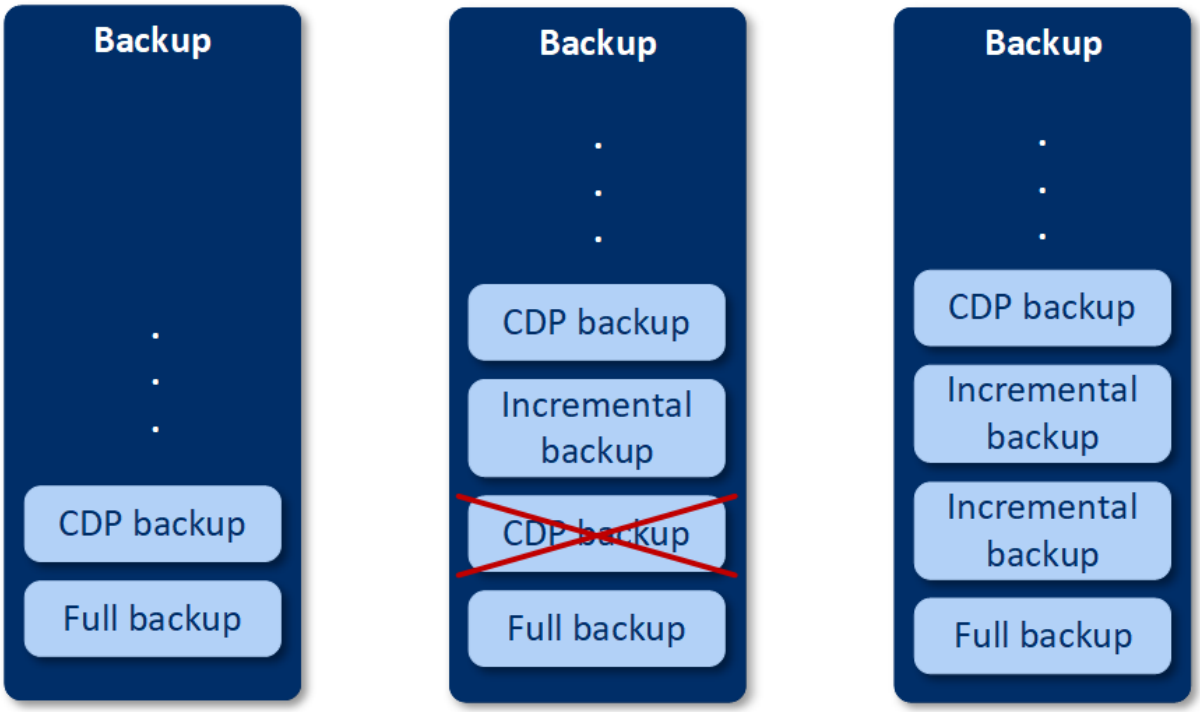
継続的データ保護は [**アプリケーションバックアップ**] オプションとの互換性がありません。

仕組み

継続的データ保護によってトラックされるファイルとフォルダの変更は、特別なCDPバックアップにすぐに保存されます。バックアップセットにはCDPバックアップが1つだけ存在します。これは常に最新のものです。



スケジュール済みの定期バックアップが開始されると、最新のデータがスケジュール済みバックアップに含められるため、継続的データ保護は保留になります。スケジュール済みバックアップが終了すると、継続的データ保護が再開され、古いCDPバックアップが削除されて、新しいCDPバックアップが作成されます。したがって、CDPバックアップは常にバックアップセット内の最新のバックアップを保持し、トラックされたファイルまたはフォルダの最新の状態のみを保存します。



定期的なバックアップ中にマシンがクラッシュした場合、マシンの再起動後に継続的データ保護が自動的に再開され、最後に成功したスケジュール済みバックアップ上にCDPバックアップが作成されます。

継続的データ保護では、CDPバックアップの前に少なくとも1つの定期的なバックアップを作成する必要があります。そのため、継続的データ保護を使用して保護計画を初めて実行すると、完全バックアップが作成され、そのバックアップ上にすぐにCDPバックアップが追加されます。既存の保護計画で **[継続的データ保護]** オプションを有効にすると、CDPバックアップが既存のバックアップセットに追加されます。

注意
Advanced Backup機能が有効になっていて、選択したマシンで他のAdvanced Backup機能が使用されていない場合、**[デバイス]** タブから作成した保護計画では、デフォルトで継続的データ保護が有効になります。選択したマシンに対して継続的データ保護を使用する計画が既に存在している場合、新しく作成された計画では、デフォルトでそのマシンに対する継続的データ保護が有効になりません。
デバイスグループ用に作成された計画では、継続的データ保護はデフォルトで有効になっていません。

サポートされるデータソース

次のデータソースに対して継続的データ保護を構成できます。

- コンピュータ全体
- ディスク/ボリューム
- ファイル/フォルダ

保護計画の **[バックアップ対象]** セクションでデータソースを選択した後、**[継続的な保護対象のアイテム]** セクションで、継続的データ保護のファイル、フォルダ、またはアプリケーションを選択します。

継続的データ保護を構成する方法については、「"CDPバックアップの構成"（400ページ）」を参照してください。

サポートされるバックアップ先

次のバックアップ先を使用して継続的データ保護を構成できます。

- ローカルフォルダ
- ネットワークフォルダ
- クラウドストレージ
- Acronis Cyber Infrastructure
- スクリプトで定義したロケーション

注意
上記のロケーションのみをスクリプトで定義できます。

CDPバックアップの構成

保護計画の **[バックアップ]** モジュールで継続的データ保護を構成できます。保護計画を作成する方法については、「"保護計画の作成"（209ページ）」を参照してください。

継続的データ保護の設定を構成するには

1. 保護計画の **[バックアップ]** モジュールで、**[継続的データ保護（CDP）]** スイッチを有効にします。
   このスイッチは、次のデータソースでのみ使用できます。
   - コンピュータ全体
   - ディスク/ボリューム
   - ファイル/フォルダ
2. **[継続的な保護対象のアイテム]** で、**アプリケーション**または**ファイル/フォルダ**、あるいはその両方の継続的データ保護を構成します。
   - **[アプリケーション]** をクリックして、特定のアプリケーションによって変更されたファイルのCDPバックアップを構成します。
     事前定義のカテゴリからアプリケーションを選択できます。その他のアプリケーションを追加する場合は、対象となるアプリケーションの実行可能ファイルのパスを指定してください。例:
     - `C:\Program Files\Microsoft Office\Office16\WINWORD.EXE`
     - `*:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE`
   - **[ファイル/フォルダ]** をクリックして、特定のロケーションにあるファイルのCDPバックアップを構成します。
     これらのロケーションは、選択ルールを使用するか、ファイルとフォルダを直接選択することで定義できます。
     - （すべてのマシン）選択ルールを作成するには、テキストボックスを使用します。
       ファイルへのフルパスまたはワイルドカード文字（*および?）を含むパスを使用できます。アスタリスクは0個以上の文字を意味します。疑問符は1文字を意味します。

重要

フォルダのCDPバックアップを作成するには、アスタリスクのワイルドカード文字を使用してその内容を指定する必要があります。

正しいパス: `D:\Data\*`

正しくないパス:`D:\Data\`

- （オンラインマシンの場合）ファイルやフォルダを直接選択するには:
  - [**参照元マシン**] で、ファイルまたはフォルダが存在するマシンを選択します。
  - [**ファイルとフォルダの選択**] をクリックして、選択したマシンを参照します。

    直接選択すると、選択ルールが作成されます。保護計画を複数のマシンに適用していて、選択ルールがマシンに対して有効でない場合、そのマシンではスキップされます。

3. 保護計画ペインで、[**作成**] をクリックします。

その結果、指定したデータは、スケジュールされたバックアップ間で継続的にバックアップされます。

バックアップ先の選択

[**バックアップ先**] をクリックして、次のいずれかを選択します。

- **クラウドストレージ**

  バックアップがクラウドデータセンターに保存されます。
- **ローカル フォルダ**

  単一のコンピュータを選択した場合は、選択したコンピュータのフォルダを参照するか、フォルダパスを入力します。

  複数のコンピュータを選択した場合は、フォルダパスを入力します。バックアップは、選択した物理コンピュータまたは仮想コンピュータのエージェントがインストールされたコンピュータのそれぞれで、このフォルダに保存されます。フォルダが存在しない場合、フォルダが作成されます。
- **ネットワークフォルダ**

  これは、SMB/CIFS/DFSを介して共有されるフォルダです。

  必要な共有フォルダを参照するか、次の形式でパスを入力します。
  - SMB/CIFS共有の場合：`\\<ホスト名>\<パス>\` または `smb://<ホスト名>/<パス>/`
  - DFS共有の場合：`\\<完全な DNS ドメイン名>\<DFS ルート>\<パス>`

    たとえば、`\\example.company.com\shared\files` のようになります。

  次に、矢印ボタンをクリックします。メッセージが表示されたら、共有フォルダのユーザー名とパスワードを指定します。フォルダ名の隣のキーアイコンをクリックすることで、これらの資格情報をいつでも変更できます。

  匿名アクセスでのフォルダへのバックアップはサポートされていません。
- **パブリッククラウド**

  このオプションは、Advanced Backupパックの一部として利用できます。

  追加のコンポーネント（Microsoft Azureやゲートウェイとしての他の仮想マシンなど）を配置することなく、パブリッククラウド対応のストレージへの直接バックアップを構成できます。必要に応じて、関連するパブリッククラウドを選択して接続します。

詳細については、"パブリッククラウドへのワークロードのバックアップ"（527ページ）を参照してください。

- **NFS フォルダ**（Linux または macOS を実行するマシンで使用可能）
  Linuxエージェントがインストールされ たLinuxサーバーにnfs-utilsパッケージがインストールされていることを確認します。
  必要なNFSフォルダを参照するか、次の形式でパスを入力します。
  `nfs://<ホスト名>/<エクスポート対象フォルダ>:/<サブフォルダ>`
  次に、矢印ボタンをクリックします。

  注意
  パスワードで保護されたNFSフォルダにバックアップすることはできません。

- **Secure Zone**（選択された各マシンに存在する場合に使用可能）
  Secure Zoneは、バックアップマシンのディスク上にあるセキュアパーティションです。このパーティションは、バックアップを構成する前に手動で作成する必要があります。Secure Zoneの作成方法、メリット、制限に関する詳細については、「"Secure Zoneのバージョン情報"（403ページ）」を参照してください。

詳細ストレージオプション

注意
この機能が利用できるのは、Cyber ProtectionサービスのAdvanced Editionのみです。

スクリプトで定義（Windows を実行するマシンに対して利用可能）

各マシンのバックアップを、スクリプトで定義したフォルダに保存できます。ソフトウェアでは、JScript、VBScript または Python 3.5 で記述されたスクリプトがサポートされます。保護計画を配置すると、ソフトウェアによって各マシンでスクリプトが実行されます。各マシンのスクリプトの出力先は、ローカルフォルダまたはネットワークフォルダのパスにする必要があります。フォルダが存在しない場合は、フォルダが作成されます（制限:Python で記述されたスクリプトでは、ネットワーク共有フォルダは作成できません）。[**バックアップストレージ**] タブに、各フォルダが個別のバックアップロケーションとして表示されます。

[**スクリプトの種類**] で、スクリプトの種類（**JScript**、**VBScript** または **Python**）を選択し、スクリプトのインポート、コピー、貼り付けを行います。ネットワークフォルダの場合は、読み込み/書き込み許可のアクセス認証を指定します。

例：

- 次のJScriptスクリプトでは、マシンのバックアップロケーションが、`\\bkpsrv\<マシン名>`の形式で出力されます:

  ```
  WScript.Echo("\\\\bkpsrv\\" + WScript.CreateObject("WScript.Network").ComputerName);
  ```

  この結果、各マシンのバックアップは、サーバー **bkpsrv** 上の同じ名前のフォルダに保存されます。

- 次のJScriptスクリプトは、スクリプトが実行されるマシン上のフォルダにバックアップロケーションを出力します。

```
WScript.Echo("C:\\Backup");
```

その結果、このマシンのバックアップは、同じマシンのC:\Backupフォルダに保存されます。

注意
これらのスクリプトのロケーションパスでは、大文字と小文字が区別されます。従って、C:\BackupとC:\backupは、Cyber Protectコンソールに異なるロケーションとして表示されます。また、ドライブ文字には大文字を使用してください。

Secure Zoneのバージョン情報

Secure Zoneは、バックアップマシンのディスク上にあるセキュアパーティションです。このコンピュータのディスク、ファイル、またはファイルのバックアップを格納できます。

ディスクの物理的な障害が発生すると、そのSecure Zoneに配置されたバックアップは失われるおそれがあります。このため、Secure Zone セキュア ゾーンを唯一のバックアップの保存場所にはしないでください。エンタープライズ環境では、通常の場所が一時的に利用できない場合や、接続チャネルが低速または混雑している状態のときに、バックアップに使用する中間ロケーションとしてSecure Zoneを使用できます。

Secure Zoneを使用する理由

Secure Zone:

- バックアップが置かれているディスク自体からディスクを復元することができます。
- ソフトウェアの誤動作、ウィルス攻撃、ヒューマンエラーからデータを保護するためのコスト効率のよい便利な方法です。
- データをバックアップまたは復元するための別のメディアやネットワーク接続が不要になります。このことは、ローミングユーザーにとって特に便利です。
- バックアップのレプリケーションの使用時に、プライマリの保存先として利用できます。

制限事項

- Macでは、Secure Zoneを構成できません。
- Secure Zoneは、ベーシックディスク上のパーティションです。ダイナミックディスク上に構成したり、論理ボリューム（LVMにより管理）として作成したりすることはできません。
- Secure ZoneはFAT32ファイルシステムでフォーマットされています。FAT32には4GBのファイルサイズ制限があるため、このサイズを上回るバックアップファイルはSecure Zoneに保存されるときに分割されます。これによって復元手順や速度に影響が出ることはありません。

Secure Zoneを作成する際にディスクがどのように変換されるか

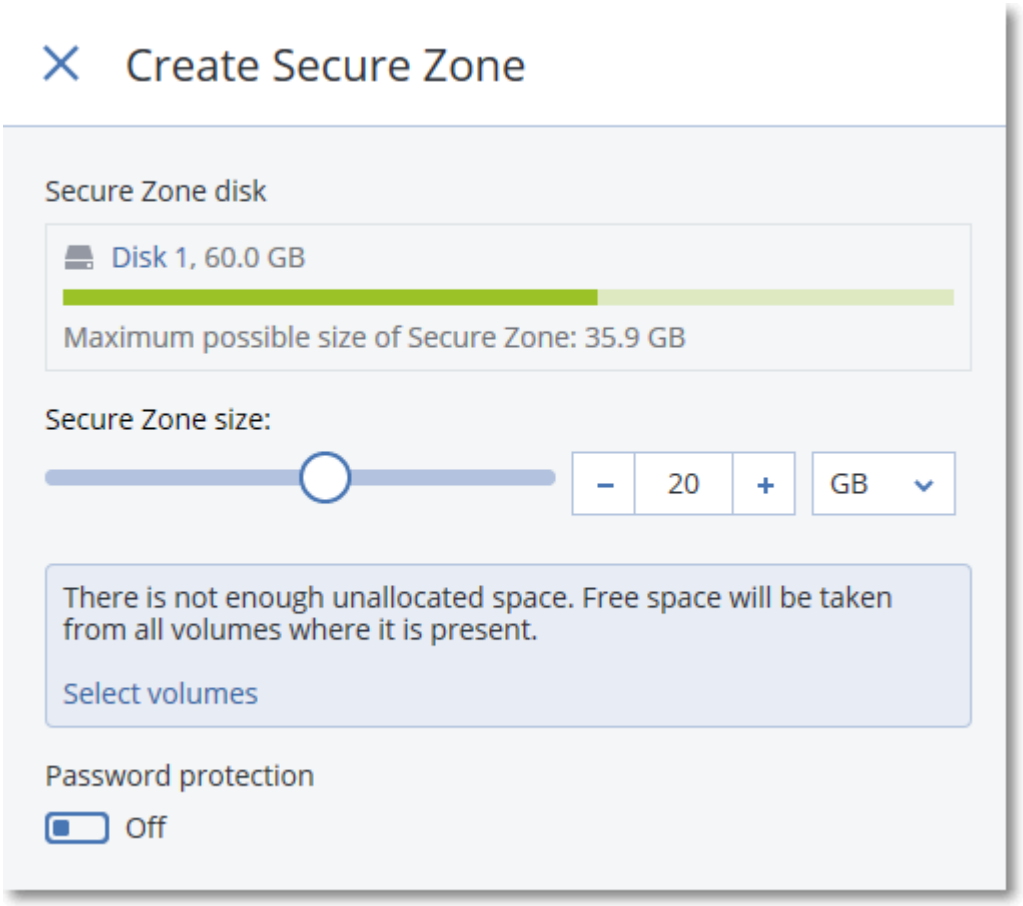
- Secure Zoneは、常にハードディスクの末尾に作成されます。
- ディスクの末尾に未割り当ての領域がない、または十分にないがボリュームの間に未割り当ての領域がある場合は、ディスクの末尾に未割り当ての領域を追加するためにボリュームが移動します。
- すべての未割り当ての領域を集めてもまだ十分ではない場合は、選択したボリュームから空き領域が取得され、それに合わせてボリュームのサイズが縮小されます。
- ただし、一時ファイルを作成する場合など、オペレーティング システムとアプリケーションが動作できるようにするにはボリュームに空き領域が必要です。空き領域がボリュームの合計サイズの25 %を下回っているか、下回ることになる場合、ボリュームのサイズは縮小されません。ディスク上のすべてのボリュームの空き領域が25 %以下の場合にのみ、比率に応じてボリュームのサイズが引き続き縮小されます。

これらのことから、Secure Zoneを利用できる最大サイズに設定することは推奨されません。ボリューム上に空き領域がなくなると、オペレーティングシステムやアプリケーションの動作が不安定になり、起動できなくなることがあります。

重要
システムの起動元のボリュームを移動またはサイズ変更するには、システムを再起動する必要があります。

Secure Zoneの作成方法

1. Secure Zoneを作成するマシンを選択します。
2. **[詳細]** > **[Secure Zone の作成]** をクリックします。
3. **[Secure Zone ディスク]**で**[選択]** をクリックしてから、ゾーンを作成するハードディスク（複数ある場合）を選択します。
   使用可能なSecure Zoneの最大サイズが算出されます。
4. Secure Zoneのサイズを入力するか、スライダをドラッグしてサイズを選択します。
   ハード ディスクにもよりますが、最小サイズは約 50 MB になります。最大サイズは、ハード ディスクの未割り当ての領域と、すべてのディスクボリュームの空き領域の合計に等しくなります。
5. すべての未割り当ての領域でも指定のサイズに十分ではない場合は、既存のボリュームから空き領域が取得されます。デフォルトでは、すべてのボリュームが選択されます。除外するボリュームがある場合は、**[ボリュームの選択]** をクリックします。それ以外の場合は、この手順をスキップします。



6. （オプション）**[パスワードによる保護]**スイッチを有効にしてパスワードを指定します。
   Secure Zoneにあるバックアップにアクセスするにはパスワードが必要になります。Secure Zoneへのバックアップでは、ブータブルメディアでバックアップを実行する場合を除き、パスワードは必要ありません。
7. **[作成]** をクリックします。
   除外パーティションレイアウトが表示されます。**[OK]** をクリックします。
8. Secure Zoneが作成されるのを待ちます。

これで、保護計画を作成するときに **[バックアップの保存先]** としてSecure Zoneを選択できるようになりました。

Secure Zoneの削除方法

1. Secure Zoneがあるマシンを選択します。
2. **[詳細]** をクリックします。
3. **Secure Zone**の横にあるギアアイコンをクリックして、**[削除]** をクリックします。
4. （オプション）ゾーンから解放される領域を追加するボリュームを指定します。デフォルトでは、すべてのボリュームが選択されます。
   領域は選択された各ボリュームに対して均等に分配されます。ボリュームを選択しない場合、空き領域は未割り当てになります。

システムの起動元のボリュームをサイズ変更するには、システムを再起動する必要があります。

5. **[削除]** をクリックします。

   Secure Zoneおよびそこに保存されているすべてのバックアップが削除されます。

バックアップスケジュール

バックアップは、特定の時間、特定の間隔、または特定のイベントで自動的に実行されるように構成できます。

非クラウドツークラウドリソースのスケジュールバックアップは、プロテクションエージェントがインストールされているワークロードのタイムゾーン設定に従って実行されます。例えば、異なるタイムゾーン設定のワークロードに同じ保護計画を適用する場合、バックアップは各ワークロードのローカルタイムゾーンに従って開始されます。

バックアップのスケジューリングには以下の操作が含まれます:

- バックアップスキームの選択
- バックアップのトリガーとなる時間の構成やイベントの選択
- オプション構成とスタート条件の設定

バックアップ スキーム

バックアップスキームは、どのタイプのバックアップ（完全、差分、増分）をいつ作成するかを定義する保護計画スケジュールの一部です。事前に定義されたバックアップスキームまたはカスタムスキームのいずれかを選択できます。

利用可能なバックアップスキームとタイプは、バックアップのロケーションとソースによって異なります。例えば、SQLデータ、Exchangeデータ、システム状態をバックアップする場合、差分バックアップは利用できません。**常に増分（単一ファイル）**スキームはテープデバイスではサポートされていません。

バックアップ スキーム	説明	構成可能な要素
常に増分（単一ファイル）	最初のバックアップは完全バックアップで、時間がかかるかもしれません。その後のバックアップは増分バックアップとなり、大幅に高速化されます。 このバックアップでは単一ファイルバックアップ形式1*が使用されます。 デフォルト設定では、バックアップは月曜日から金曜	• スケジュールのタイプ: 月単位、週単位、日単位、時間単位 • バックアップトリガー: 時間またはイベント • 開始時刻 • 開始条件

1バックアップ形式は、最初の完全バックアップアップとその後の増分バックアップが保存された単一の.tibxファイルです。この形式の場合、増分バックアップの速度が上がり、古くなったバックアップの削除が難しいという増分バックアップの欠点を補うことができます。古くなったバックアップで使用されているブロックは、ソフトウェアによって「空き領域」としてマークされ、新しいバックアップによって上書きされます。これにより、リソース消費を最小限に抑えながら、クリーンアップを飛躍的に高速化できます。 単一ファイルバックアップ形式は、ランダムアクセスの書き込みと読み込みをサポートしていないロケーションにバックアップする場合には使用できません。

バックアップ スキーム	説明	構成可能な要素
	日まで毎日実行されます。 増分バックアップは高速で、ネットワークトラフィックが少ないため、クラウドストレージにバックアップを保存する場合は、このスキームを使用することをお勧めします。	• その他のオプション
常に完全	バックアップセット内のすべてのバックアップは完全バックアップです。 デフォルト設定では、バックアップは月曜日から金曜日まで毎日実行されます。	• スケジュールのタイプ: 月単位、週単位、日単位、時間単位 • バックアップトリガー: 時間またはイベント • 開始時刻 • 開始条件 • その他のオプション
週単位で完全、日単位で増分	完全バックアップは週に1回作成され、その他のバックアップは増分になります。 最初のバックアップは完全バックアップで、その週の他のバックアップは増分バックアップです。 週単位の完全バックアップを作成する日を選択するには、保護計画でギアアイコンをクリックし、[**バックアップオプション**] > [**週単位のバックアップ**] に移動します。 デフォルト設定では、バックアップは月曜日から金曜日まで毎日実行されます。	• バックアップトリガー: 時間またはイベント • 開始時刻 • 開始条件 • その他のオプション

月単位で完全、週単位で差分、日単位で増分（GFS）	デフォルト設定では、増分バックアップは月曜日から金曜日まで毎日実行されます。差分バックアップは毎週土曜日に実行されます。完全バックアップは毎月1日に実行されます。
	
	注意
	これは定義済みのカスタムスキームです。このスキームは保護計画で、**カスタム**として表示されます。
		• バックアップタイプごとに既存のスケジュールを変更します。
		  ◦ スケジュールのタイプ: 月単位、週単位、日単位、時間単位
		  ◦ バックアップトリガー: 時間またはイベント
		  ◦ 開始時刻
		  ◦ 開始条件
		  ◦ その他のオプション
		• バックアップタイプごとに新しいスケジュールを追加

バックアップ スキーム	説明	構成可能な要素
カスタム	バックアップのタイプ（完全、差分、増分）を選択し、それぞれに個別のスケジュールを設定する必要があります*。	• バックアップタイプごとに既存のスケジュールを変更します。 ◦ スケジュールのタイプ: 月単位、週単位、日単位、時間単位 ◦ バックアップトリガー: 時間またはイベント ◦ 開始時刻 ◦ 開始条件 ◦ その他のオプション • バックアップタイプごとに新しいスケジュールを追加

*保護計画を作成した後は、**常に増分（単一ファイル）**と他のバックアップスキームを相互に切り替えることはできません。**常に増分（単一ファイル）**スキームは単一ファイル形式、それ以外のスキームはマルチファイル形式になります。形式を切り替えたい場合は、新しい保護計画を作成します。

バックアップタイプ

次のバックアップタイプを使用できます。

- 完全 - 完全バックアップには、すべてのソースデータが含まれます。完全バックアップは自己完結型です。データをリカバリするために、それ以外のバックアップにアクセスする必要はありません。

  注意
  保護計画によって作成される初回のバックアップは必ず完全バックアップになります。

- 増分 - 増分バックアップでは、最新のバックアップが完全バックアップ、差分バックアップ、増分バックアップのいずれであるかに関わりなく、最新バックアップ以降のデータ変更が保存されます。データをリカバリするには、増分バックアップが依存するバックアップチェーン全体（最初の完全バックアップまで遡る）が必要です。
- 差分 - 差分バックアップでは、最新の完全バックアップ以降のデータ変更が保存されます。データをリカバリするには、差分バックアップと、依存関係にある完全バックアップの両方が必要です。

スケジュールでバックアップを実行する

特定の時間または特定のイベント時に自動的にバックアップを実行するには、保護計画でスケジュールを有効にします。

スケジュールを有効にするには

1. 保護計画で、**バックアップ**モジュールを展開します。
2. **[スケジュール]** をクリックします。
3. スケジュールスイッチを有効にします。
4. バックアップスキームを選択します。
5. 必要に応じてスケジュールを構成し、**[完了]** をクリックします。
   利用可能なスケジューリングオプションの詳細については、"時刻でスケジュール"（409ページ）および"イベント別のスケジュール"（411ページ）を参照してください。
6. （オプション） 開始条件や追加のスケジューリングオプションを構成します。
7. 保護計画を保存します。

これにより、スケジュール条件が満たされるたびにバックアップ操作が開始されます。

スケジュールを無効にするには

1. 保護計画で、**バックアップ**モジュールを展開します。
2. **[スケジュール]** をクリックします。
3. スケジュールスイッチを無効にします。
4. 保護計画を保存します。

これにより、バックアップは手動で起動した場合のみ実行されるようになります。

注意
スケジュールが無効の場合、保持ルールは自動的に適用されません。これらを適用するには、手動でバックアップを実行してください。

時刻でスケジュール

以下の表では、時間に基づくスケジューリングオプションを示します。これらのオプションが利用できるかどうかは、バックアップスキームに依存します。詳細については、"バックアップ スキーム"（406ページ）を参照してください。

オプション	説明	例
月単位	月、日、曜日を選択し、バックアップ開始時刻を選択します。	1月1日と2月3日の午前12時にバックアップを実行します。 毎月1日の午前10時にバックアップを実行します。 3月1日、3月5日、4月1日、4月5日の午前9時にバックアップを実行します。 毎月第2、第3金曜日の午前11時にバックアップを実行します。 毎月最終水曜日の午後10時30分にバックアップを実行します。
週単位	曜日を選択し、バックアップ開始時刻を選択	月曜日から金曜日の午前10時にバックアッ

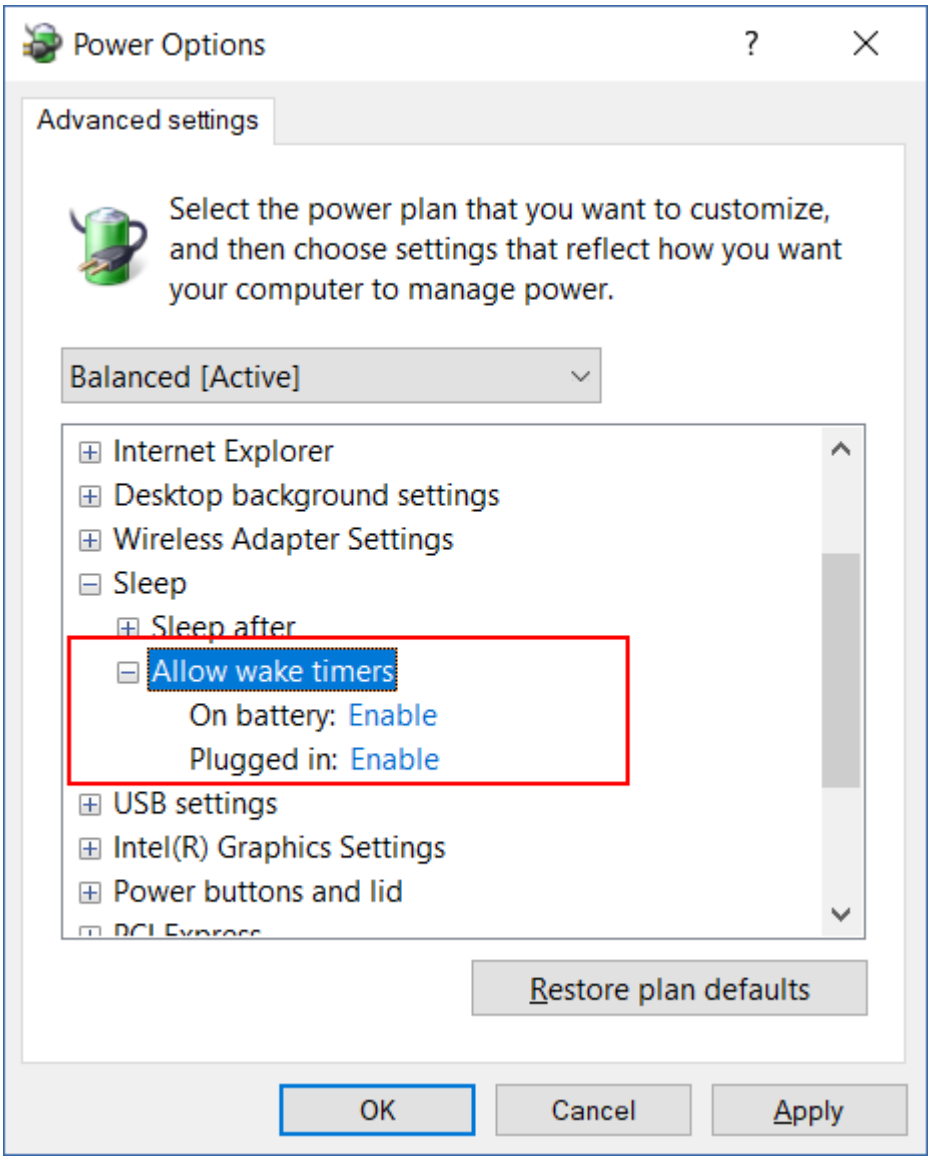
オプション	説明	例
	します。	プを実行します。 月曜日の午後11時にバックアップを実行します。 火曜日と土曜日の午前8時にバックアップを実行します。
日単位	日数（毎日または平日のみ）を選択し、バックアップ開始時間を選択します。	毎日、午前11時45分にバックアップを実行します。 月曜日から金曜日の午後9時30分にバックアップを実行します。
時間単位	曜日を選択し、連続する2件のバックアップの時間間隔とバックアップを実行する時間範囲を選択します。 分単位で間隔を設定する場合、10分から60分の間で推奨間隔を選択するか、45分や75分などのカスタム間隔を指定することができます。	月曜日から金曜日の午前8時から午後6時までの間、1時間ごとにバックアップを実行します。 土曜日と日曜日の午前1時から午後6時までの間、3時間ごとにバックアップを実行します。

その他のオプション

バックアップを時間でスケジュールする場合、以下の追加スケジューリングオプションが利用できます。

これらを使用するには、**スケジュール**ペインで、**[詳細を表示]** をクリックします。

- **マシンの電源が入っていないため実行されなかったタスクを起動時に実行する**
  既定の設定:無効。
- **バックアップ中にスリープモードや休止モードにしない**
  このオプションは、Windowsが実行されているマシンにのみ適用されます。
  既定の設定:有効。
- **スリープモードや休止モードから起動して、スケジュールされたバックアップを開始する**
  このオプションは、**[ウェイクタイマーを許可]** オプションが有効になっている電源計画で、Windowsを実行しているマシンにのみ適用されます。



このオプションはWake-on-LAN機能を使用するものではなく、電源がオフになっているマシンには適用されません。

既定の設定:無効。

イベント別のスケジュール

特定のイベント発生時に実行されるバックアップを構成するには、以下のオプションのいずれかを選択します。

オプション	説明	例
前回のバックアップからの経過時間	バックアップは、最後にバックアップが成功した後、指定された期間後に開始されます。	最後にバックアップが成功してから1日後にバックアップを実行します。 最後にバックアップが成功してから4時間後にバックアップを実行します。

オプション	説明	例
	注意 このオプションは、前回のバックアップがどのように完了したかによって異なります。バックアップが失敗した場合、次のバックアップは自動的に開始されません。この場合、スケジュールをリセットするために、手動でバックアップを実行し、正常に完了したことを確認する必要があります。	
ユーザーがシステムにログインするとき	バックアップは、ユーザーがマシンにログインしたときに開始されます。 このオプションは、すべてのログインまたは特定のユーザーのログインに対して構成できます。 **注意** 一時的なユーザープロファイルでログインしても、バックアップは開始されません。	ユーザー「John Doe」がログインしたときにバックアップを実行します。
ユーザーがシステムからログオフするとき	バックアップは、ユーザーがマシンにログオフしたときに開始されます。 このオプションは、すべてのログオフまたは特定のユーザーのログオフに対して構成できます。 **注意** 一時的なユーザープロファイルからログオフしても、バックアップは開始されません。 マシンをシャットダウンしてもバックアップは開始されません。	すべてのユーザーがログオフしたときにバックアップを実行します。
システムの起動時	バックアップは保護されているマシンの起動時に実行されます。	ユーザーがマシンを起動したときにバックアップを実行します。
システムのシャットダウン時	バックアップは保護されているマシンのシャットダウン時に実行されます。	ユーザーがマシンをシャットダウンしたときにバックアップを実行します。
Windowsイベントログ イベント発生時	バックアップは、指定したWindowsイベントに応じて実行されます。	タイプエラーおよびソースディスクで、イベント7がWindowsシステムログに記録されたらバックアップを実行します。

これらのオプションの可用性は、バックアップソースと保護ワークロードのオペレーティングシステムに依存します。以下の表に、Windows、Linux、macOSで利用可能なオプションを示します。

イベント	バックアップソース（バックアップ対象）					
	マシン全体、ディスク/ボリューム、ファイル/フォルダ（物理マシン）	マシン全体またはディスク/ボリューム（仮想マシン）	ESXi構成	Microsoft 365メールボックス	Exchangeデータベースおよびメールボックス	SQLデータベース
前回のバックアップからの経過時間	Windows, Linux, macOS	Windows, Linux	Windows, Linux	Windows	Windows	Windows
ユーザーがシステムにログインするとき	Windows	なし	なし	なし	なし	なし
ユーザーがシステムからログオフするとき	Windows	なし	なし	なし	なし	なし
システムの起動時	Windows, Linux, macOS	なし	なし	なし	なし	なし
システムのシャットダウン時	Windows	なし	なし	なし	なし	なし
Windowsイベントログ イベント発生時	Windows	なし	なし	Windows	Windows	Windows

Windowsイベントログ イベント発生時

特定のイベントがアプリケーションログ、セキュリティログ、システムログなどのWindowsイベントログに記録されると、自動的にバックアップが実行されます。

注意
Windowsの **[コンピューターの管理]** > **[イベントビューアー]** で、イベントを参照し、そのプロパティを表示できます。セキュリティログを開くには、管理者権限が必要です。

イベントのパラメータ

次の表に、**[Windowsイベントログ イベント発生時]** オプションを設定するときに指定する必要のあるパラメータを示します。

パラメータ	説明
[ログ名]	ログの名前です。 標準のログの名前（[アプリケーション]、[セキュリティ]、または[システム]）を選択するか、別のログ名を指定します。例: Microsoft Office セッション。
[イベントソース]	イベントソースには、イベントが発生する原因となったプログラムやシステムコンポーネントが示されます。例: ディスク。 指定された文字列を含むイベントソースすべてによって、スケジュール済みバックアップが開始されます。このオプションでは大文字と小文字は区別されません。例えば、serviceを指定した場合、Service Control ManagerとTime-Serviceの両方のイベントソースによってイベントが開始されます。
[イベントの種類]	イベントの種類:[エラー]、[警告]、[情報]、[成功の監査]、または[失敗の監査] を指定します。
[イベントID]	イベントIDにより、イベントソース内にある特定の種類のイベントを識別できます。 例えば、Windowsでディスクの不良ブロックが検出されたときは、イベントソースがディスクでイベントIDが7のエラーイベントが発生し、ディスクがまだアクセス可能になっていないときは、イベントソースがディスクでイベントIDが15のエラーイベントが発生します。

例:ハードディスクに不良ブロックが発生した場合の緊急バックアップ

ハードディスクドライブに1つまたは複数の不良ブロックがある場合、間もなく障害が発生する可能性があることを示しています。このため不良ブロックが検出されたときは、バックアップを作成するのが賢明です。

Windowsでディスク上の不良ブロックが検出されると、イベントソースディスクでイベント番号7のエラーイベントがシステムログに記録されます。保護計画で、以下のスケジュールを設定します:

- スケジュール:Windowsイベントログ イベント発生時
- ［ログ名］:システム
- [イベントソース]: ディスク

- ［イベントの種類］:エラー
- ［イベント ID］:7

重要
不良ブロックがあってもバックアップが完了するようにするには、**[バックアップオプション]** で **[エラーの処理]** に移動し、**[不良セクタを無視する]** チェックボックスをオンにします。

開始条件

特定の条件が満たされた場合にのみバックアップを実行するには、1つまたは複数の開始条件を設定します。複数の条件を設定した場合、バックアップを開始するには、すべての条件が同時に満たされる必要があります。条件が満たされているかどうかに関係なく、バックアップが実行される期間を指定できます。このバックアップオプションの詳細については、"タスクの開始条件"（480ページ）を参照してください。

手動でバックアップを開始する場合、開始条件は適用されません。

Windows、Linux、およびmacOSで各種データ向けに使用できる開始条件を次の表に示します。

開始条件	バックアップソース（バックアップ対象）					
	マシン全体、ディスク/ボリューム、ファイル/フォルダ（物理マシン）	マシン全体またはディスク/ボリューム（仮想マシン）	ESXi構成	Microsoft 365メールボックス	Exchangeデータベースおよびメールボックス	SQLデータベース
ユーザーがアイドル状態	Windows	なし	なし	なし	なし	なし
バックアップロケーションのホストが利用できる状態	Windows, Linux, macOS	Windows, Linux	Windows, Linux	Windows	Windows	Windows
ユーザーがログオフ	Windows	なし	なし	なし	なし	なし
以下の開始・	Windows, Linux,	Windows, Linux	なし	なし	なし	なし

開始条件	バックアップソース（バックアップ対象）					
	マシン全体、ディスク/ボリューム、ファイル/フォルダ（物理マシン）	マシン全体またはディスク/ボリューム（仮想マシン）	ESXi構成	Microsoft 365メールボックス	Exchangeデータベースおよびメールボックス	SQLデータベース
終了時刻に該当	macOS					
バッテリー電源を節約	Windows	なし	なし	なし	なし	なし
従量制課金の接続時には開始しない	Windows	なし	なし	なし	なし	なし
以下のWi-Fiネットワークに接続している場合は開始しない	Windows	なし	なし	なし	なし	なし
デバイスのIPアドレスをチェック	Windows	なし	なし	なし	なし	なし

ユーザーがアイドル状態

[ユーザーがアイドル状態] は、コンピュータでスクリーンセーバーが実行されているかコンピュータがロックされているという意味です。

例

毎日午後9時に、できればユーザーがアイドル状態のときにバックアップを実行します。午後11時になってもユーザーがアクティブなときは、バックアップを強制的に実行します。

- スケジュール:**日単位**、**毎日実行**。開始時刻:**午後9時**。
- 条件:**ユーザーがアイドル状態**。
- バックアップ開始条件:**条件が満たされるまで待機する**、**次の時間が経過するとタスクを実行する: 2** 時間。

作成が完了すると以下のようになります。

- ユーザーが午後9時より前にアイドル状態になった場合、バックアップは午後9時に開始されます。
- ユーザーが午後9時から午後11時の間にアイドル状態になった場合、バックアップは直ちに開始されます。
- 午後11時になってもユーザーがアクティブな場合は、バックアップは午後11時に開始されます。

バックアップロケーションのホストが利用できる状態

「バックアップロケーションのホストが利用できる状態」は、バックアップロケーションをホストしているマシンがネットワーク経由で使用可能であるという意味です。

この条件は、ネットワークフォルダとクラウドストレージ、およびStorage Nodeによって管理されるロケーションに適用されます。

この条件にロケーションそのものが利用できるかどうかは関連しません。対象となるのはホストが利用可能かどうかのみです。たとえば、ホストは利用できるが、このホスト状のネットワークフォルダが共有されていない場合、またはフォルダの資格情報が有効ではない場合でも、条件は満たされています。

例

毎営業日午後9時にネットワークフォルダへのバックアップを実行します。また、このフォルダをホストしているマシンが使用できない（メンテナンスなどのため）場合は、バックアップをスキップし、翌営業日にスケジュールされている開始時刻まで待機します。

- スケジュール:**日単位**、**月曜日から金曜日まで実行**。開始時刻:**午後9時**。
- 条件:**バックアップロケーションのホストが利用できる状態**。
- バックアップ開始条件:**スケジュールされたバックアップをスキップ**。

作成が完了すると以下のようになります。

- ホストが午後9時に利用可能な場合、バックアップは直ちに開始されます。
- ホストが午後9時に利用可能でない場合、バックアップは翌営業日に開始されます（この日の午後9時にホストが利用可能な場合）。
- 営業日の午後9時の時点でホストが使用可能にならない限り、バックアップが開始されることはありません。

ユーザーがログオフ

この開始条件を使用して、すべてのユーザーがWindowsマシンからログオフするまでバックアップを延期します。

例

毎週金曜日の午後8時、できればすべてのユーザーがログオフしている時間にバックアップを実行します。ただし、午後11時になってもログオンしているユーザーがいる場合は、バックアップは強制的に実行されます。

- スケジュール:**週単位**、毎金曜日。開始時刻:**午後8時**。
- 条件:**ユーザーがログオフした場合**。
- バックアップ開始条件:**条件が満たされるまで待機**し、**3時間が経過するとバックアップを実行**。

作成が完了すると以下のようになります。

- 午後8時にすべてのユーザーがログオフしていた場合は、バックアップが午後8時に開始されます。
- 最後のユーザーが午後8時から午後11時の間にログオフした場合、バックアップは直ちに開始されます。
- 午後11時の時点でまだログインしているユーザーがいる場合、バックアップは午後11時に開始されます。

以下の開始・終了時刻に該当

この開始条件を使用して、バックアップの開始を指定した間隔に制限します。

例

ある企業では、ユーザーデータとサーバーを、同じネットワーク接続ストレージ上の異なるロケーションにバックアップします。

営業日の業務時間は午前8時から午後5時までです。ユーザーのデータはユーザーがログオフしたらすぐにバックアップする必要がありますが、実行できる時間は午後4時30分以降です。

毎日午後11時に会社のサーバーをバックアップします。このため、サーバーバックアップでネットワークの帯域幅をすべて利用できるように、午後11時までにすべてのユーザーデータのバックアップが完了すると理想的です。

ユーザーデータのバックアップは1時間以内に完了するため、バックアップ開始時間は遅くても午後10時にする必要があります。指定された時間間隔内にユーザーがまだログインしている場合、またはそれ以外の時間にログオフした場合、ユーザーデータのバックアップはスキップされる必要があります。

- イベント:**ユーザーがシステムからログオフするとき**ユーザーアカウントを指定:**すべてのユーザー**
- 条件:**午後4時30分**から**午後10時**までの**以下の開始・終了時刻に該当**。
- バックアップ開始条件:**スケジュールされたバックアップをスキップ**。

作成が完了すると以下のようになります。

- ユーザーが午後4時30分から午後10時の間にログオフした場合、バックアップは直ちに開始されます。
- ユーザーがその期間以外の時刻にログオフすると、バックアップはスキップされます。

バッテリー電源を節約

この開始条件を使用して、マシン（ラップトップやタブレットなど）が電源に接続されていない場合にバックアップが実行されないようにします。オプションのバックアップ開始条件の値によって、マシンを電源に接続した後に、スキップされたバックアップが開始されるかどうかが異なります。

次から選択できます。

- **バッテリー駆動時は開始しない**
  マシンが電源に接続されている場合のみ、バックアップが開始されます。
- **バッテリーレベルが以下の値より高い場合に開始する**
  マシンが電源に接続されているか、バッテリーレベルが指定した値よりも高い場合にバックアップを開始します。

例

毎営業日午後9時にデータがバックアップされます。マシンが電源に接続されていない場合、バッテリーを節約するためにバックアップをスキップし、マシンが電源に接続するまで待機したい場合。

- スケジュール:**日単位、月曜日から金曜日まで実行。**開始時刻:**午後9時。**
- 条件:[**バッテリー電源を節約**]、[**バッテリー駆動時は開始しない**]。
- バックアップ開始条件:**条件が満たされるまで待機する。**

作成が完了すると以下のようになります。

- 午後9時の時点でマシンが電源に接続されている場合、バックアップは直ちに開始されます。
- 午後9時の時点でマシンがバッテリーで動作している場合、マシンを電源に接続するとバックアップが開始されます。

従量制課金の接続時には開始しない

起動条件を使用して、Windowsで従量制課金が設定された接続経由でマシンがインターネットに接続されている場合に、バックアップ（ローカルディスクへのバックアップを含む）が実行されないようにします。Windows での従量制課金接続の詳細については、https://support.microsoft.com/ja-jp/help/17452/windows-metered-internet-connections-faq を参照してください。

従量制課金の接続時には開始しないの追加条件を有効にすると、**次のWi-Fiネットワークへの接続時には開始しない**の条件が自動的に有効になります。これは、モバイルホットスポット経由でのバックアップを回避するための追加措置でです。android、phone、mobile、modemのネットワーク名はデフォルトで指定されています。

これらの名前をリストから削除するには、[X] をクリックします。新しい名前を追加するには、空のフィールドに入力します。

例

毎営業日午後9時にデータがバックアップされます。従量制課金接続を経由してマシンがインターネットに接続されている場合、ネットワークトラフィックを節約するためにバックアップをスキップし、次の営業日にスケジュールされた開始時刻まで待機します。

- スケジュール:**日単位、月曜日から金曜日まで実行。**開始時刻:**午後9時。**
- 条件:**従量制課金の接続時には開始しない。**
- バックアップ開始条件:**スケジュールされたバックアップをスキップ。**

作成が完了すると以下のようになります。

- 午後9時の時点でマシンが従量制接続でインターネットに接続されていない場合、バックアップは直ちに開始されます。
- 午後9時の時点でマシンが従量制接続でインターネットに接続されている場合、バックアップは翌営業日に開始されます。
- 営業日の午後9時の時点でマシンが常に従量制接続でインターネットに接続されている場合、バックアップが開始されることはありません。

以下のWi-Fiネットワークに接続している場合は開始しない

この開始条件を使用すると、マシンが指定したワイヤレスネットワークに接続されている場合、バックアップ（ローカルディスクへのバックアップを含む）が回避されます（例えば、携帯電話のホットスポット経由のバックアップを制限したい場合など）。

Wi-Fi のネットワーク名（SSID）を指定できます。この制限は、名前の文字列の中に指定した名前が含まれるすべてのネットワークに適用されます（大文字と小文字は区別されません）。たとえば、ネットワーク名にphoneと指定すると、マシンが次のいずれかのネットワークに接続されている場合、バックアップ開始されることはありません。`John's iPhone`、`phone_wifi`、または`my_PHONE_wifi`。

従量制課金の接続時には開始しないの条件を有効にすると、**次のWi-Fiネットワークへの接続時には開始しない**の条件が自動的に有効になります。android、`phone`、`mobile`、modemのネットワーク名はデフォルトで指定されています。

これらの名前をリストから削除するには、[X] をクリックします。新しい名前を追加するには、空のフィールドに入力します。

例

毎営業日午後9時にデータがバックアップされます。マシンがモバイルホットスポットを介してインターネットに接続されている場合、バックアップをスキップして、次の営業日にスケジュールされた時間まで待機するように設定します。

- スケジュール:**日単位、月曜日から金曜日まで実行。**開始時刻:**午後9時。**
- 条件:[**以下のWi-Fiネットワークに接続している場合は開始しない**]、[**ネットワーク名**] に **<ホットスポットのネットワークの** `SSID>` を指定。
- バックアップ開始条件:**スケジュールされたバックアップをスキップ。**

作成が完了すると以下のようになります。

- 午後9時の時点でマシンが指定されたネットワークに接続されていない場合、バックアップは直ちに開始されます。
- 午後9時の時点でマシンが指定されたネットワークに接続されていない場合、バックアップは翌営業日に開始されます。
- 午後9時の時点でマシンが常に指定したネットワークに接続されている場合、バックアップが開始されることはありません。

デバイスのIPアドレスをチェック

この起動条件を使用して、マシンのIPアドレスに指定したIPアドレスの範囲内または範囲外のものが含まれる場合に、バックアップ（ローカルディスクへのバックアップを含む）が実行されないようにします。例えば、海外に所在するユーザーのマシンをバックアップする際に、多額のデータ転送料金が発生するのを回避したり、VPN（Virtual Private Network）接続経由でのバックアップを拒否したりすることができます。

次から選択できます。

- **以下のIPレンジの範囲外の場合に開始する**
- **以下のIPレンジの範囲内の場合に開始する**

どちらのオプションでも、複数の範囲を指定できます。IPv4 アドレスのみがサポートされています。

例

毎営業日午後9時にデータがバックアップされます。マシンがVPNトンネルを使って企業ネットワークに接続している場合に、バックアップをスキップしたいと考えています。

- スケジュール:**日単位、月曜日から金曜日まで実行。**開始時刻: **午後9時。**
- 条件:**デバイスの IP アドレスを確認し、以下のIPレンジの範囲外の場合に開始する。開始**: `<VPN IP アドレス範囲の開始>`、**終了**: `<end of the VPN IP アドレス範囲の終了>`
- バックアップ開始条件:**条件が満たされるまで待機する。**

作成が完了すると以下のようになります。

- 午後9時の時点でマシンのIPアドレスが指定された範囲にない場合、バックアップは直ちに開始されます。
- 午後9時の時点でマシンのIPアドレスが指定された範囲にある場合、マシンがVPN以外のIPアドレスを取得した時点でバックアップが開始されます。
- 営業日の午後9時に、マシンのIPアドレスが常に指定した範囲内にある場合、バックアップが開始されることはありません。

追加のスケジュールオプション

特定の条件が満たされた場合のみバックアップを実行する、指定された期間のみバックアップを実行する、またはスケジュールよりも遅延してバックアップを実行するように構成できます。

開始条件を構成するには

1. 保護計画で、**バックアップ**モジュールを展開します。
2. **[スケジュール]** をクリックします。
3. **スケジュール**ペインで、**[詳細を表示]** をクリックします。
4. 含める開始条件の横にあるチェックボックスをオフにして、**[完了]** をクリックします。
   利用可能な開始条件とその設定方法の詳細については、"開始条件"（415ページ）を参照してください。
5. 保護計画を保存します。

時間範囲を構成するには

1. 保護計画で、**バックアップ**モジュールを展開します。
2. **[スケジュール]** をクリックします。
3. **[設定した期間内で計画を実行する]** チェックボックスをオンにします。
4. 必要に応じて期間を指定して **[完了]** をクリックします。
5. 保護計画を保存します。

その結果、バックアップは指定された期間のみ実行されます。

遅延を構成するには

複数のワークロードをネットワークロケーションにバックアップする際にネットワーク負荷が大きくなるのを避けるため、バックアップオプションとして小さなランダム遅延が構成されています。無効にしたり、設定を変更したりできます。

1. 保護計画で、**バックアップ**モジュールを展開します。
2. **[バックアップオプション]** をクリックし、**[スケジューリング]** を選択します。
   各ワークロードの遅延値は、ゼロから指定した最大値の間でランダムに選択されます。デフォルトでは、最大値は30分です。
   このバックアップオプションの詳細については、"スケジューリング"（478ページ）を参照してください
   各ワークロードの遅延値は、そのワークロードに保護計画を適用するときに算出され、最大遅延値が編集されるまで変更されることはありません。
3. 必要に応じて期間を指定して **[完了]** をクリックします。
4. 保護計画を保存します。

手動でのバックアップの実行

手動でスケジュールおよび非スケジュールバックアップを実行できます。

手動でバックアップを実行するには

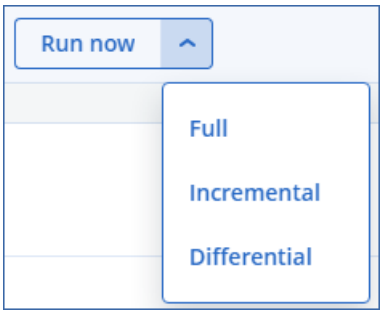
1. Cyber Protectコンソールで **[デバイス]** に進みます。
2. バックアップを実行するワークロードを選択し、**[保護]** をクリックします。
3. バックアップを作成する保護計画を選択します。
   ワークロードに保護計画が適用されていない場合は、既存の計画を適用するか、新しい計画を作成します。

保護計画を作成する方法の詳細については、"保護計画の作成"（209ページ）を参照してください。

4. （バックアップのデフォルトタイプを作成するには）保護計画で **[今すぐ実行]** アイコンをクリックします。

または、保護計画で**バックアップ**モジュールを展開し、**[今すぐ実行]** ボタンをクリックします。

5. （特定のタイプのバックアップを作成するには）保護計画で**バックアップ**モジュールを展開し、**[今すぐ実行]** ボタンの横の矢印をクリックして、バックアップのタイプを選択します。



注意
1つのバックアップ方法のみを使用するバックアップスキームでは、タイプを選択することはできません（例: **常に増分（単一ファイル）**または**常に完全**）。

その結果、バックアップ操作が開始できません。その進行状況と結果は、**[デバイス]** タブの **[ステータス]** 列で確認できます。

保持ルール

古いバックアップを自動的に削除するには、保護計画でバックアップ保持ルールを構成します。

保持ルールは、以下のバックアッププロパティのいずれかに基づいて設定できます:

- 番号
- 世代
- サイズ

利用可能な保持ルールとそのオプションは、バックアップスキームによって異なります。このルールは、エージェント、ワークロード、クラウドツークラウドバックアップにも関連します。詳細については、"バックアップスキームによる保持ルール"（424ページ）を参照してください。

保持ルールの設定中に、**[バックアップを無期限に保持する]** オプションを選択すると、古いバックアップの自動クリーンアップを無効にできます。その結果、ストレージの使用量が増え、不要な古いバックアップを手動で削除しなければならなくなる場合があります。

重要なヒント

- 保持ルールは保護計画の一部です。計画を取り消したり削除したりすると、その計画の保持ルールは適用されなくなります。不要になったバックアップを削除する方法については、"バックアップの削除"（520ページ）を参照してください。
- バックアップスキームおよびバックアップ形式に従って、各バックアップが個別のファイルとして保存される場合、他の増分バックアップまたは差分バックアップと依存関係のあるバックアップを削除することはできません。このバックアップは、依存関係のあるバックアップに適用される保持ルールに従って削除されます。この構成では、一部のバックアップについて削除のタイミングが延期されるため、ストレージ使用量が増加する可能性があります。また、バックアップの世代、数量、サイズが指定した値を超過する場合があります。 この動作を変更する方法については、"バックアップの統合"（439ページ）を参照してください。
- デフォルトでは、保護計画で作成された最新のバックアップが削除されることはありません。一方で、新しいバックアップ操作を開始する前に、バックアップクリーンアップの保持ルールを設定していて、保持するバックアップの数がゼロになっている場合は、最新のバックアップも削除されます。

警告
この保持ルールを単一のバックアップを含むバックアップセットに適用している場合、バックアップ操作が失敗すると、新しいバックアップが作成される前に既存のバックアップが削除されるため、データをリカバリすることができません。

バックアップスキームによる保持ルール

利用可能な保持ルールとその設定は、保護計画で使用するバックアップスキームによって異なります。そのバックアップスキームの詳細については、"バックアップ スキーム"（406ページ）を参照してください。

次の表に、利用可能な保持ルールとその設定を示します。

バックアップ スキーム	スケジュール	利用可能な保持ルールと設定
常に増分（単一ファイル）	月単位 週単位 日単位 時間単位 イベントトリガーによるバックアップ	バックアップの数 バックアップ世代（月単位、週単位、日単位、時間単位のバックアップ） バックアップを無期限に保存する
常に完全	月単位 週単位 日単位 時間単位	バックアップの数 バックアップ世代（月単位、週単位、日単位、時間単位のバックアップ） バックアップの合計サイズ別

バックアップ スキーム	スケジュール	利用可能な保持ルールと設定
	イベントトリガーによるバックアップ	バックアップを無期限に保存する
週単位で完全、日単位で増分	日単位 イベントトリガーによるバックアップ	バックアップの数 バックアップ世代（週単位、日単位のバックアップ） バックアップの合計サイズ別 バックアップを無期限に保存する
毎月完全、毎週差分、毎日増分	月単位 週単位 日単位 時間単位 イベントトリガーによるバックアップ	バックアップの数 バックアップ世代（完全バックアップ、差分バックアップ、および増分バックアップの個別設定） バックアップの合計サイズ別 バックアップを無期限に保存する
カスタム	月単位 週単位 日単位 時間単位 イベントトリガーによるバックアップ	バックアップの数 バックアップ世代（完全バックアップ、差分バックアップ、および増分バックアップの個別設定） バックアップの合計サイズ別 バックアップを無期限に保存する

なぜ時間単位のスキームで月単位のバックアップがあるのですか？

バックアップスキームに応じて、**[バックアップ世代]** オプションを次のいずれかのバックアップに構成できます:

- 月単位、週単位、日単位、時間単位のバックアップ。
  これらの設定は、非カスタムバックアップスキームで利用可能で、時間に基づいています。バックアップを時間単位で実行するように構成している場合でも、これらのバックアップ（月単位、週単位、日単位、時間単位）をすべて利用可能です。以下を参照してください。

バックアップ	説明
月単位	月単位のバックアップとは、毎月最初のバックアップのことです。
週単位	週単位のバックアップでは、[週単位のバックアップ] オプションで指定した曜日に最初のバックアップが実行されます。この日は、保持ルール上、週の初日とみなされます。 週単位のバックアップが月の最初のバックアップでもある場合、それは月単位のバックアップとみなされます。この場合、週単位のバックアップ

バックアップ	説明
	は、翌週の選択した曜日に作成されます。
日単位	日単位のバックアップは、1日の最初のバックアップになります。ただし、このバックアップが月単位または週単位のバックアップの定義に属する場合は例外となります。この場合、日単位のバックアップは翌日に作成されます。
時間単位	時間単位のバックアップは、1時間の始めに実行されるバックアップです。ただしこのバックアップが月単位、週単位、または日単位のバックアップの定義に属する場合を除きます。この場合、時間単位のバックアップは次の1時間に作成されます。

- 完全バックアップ、差分バックアップ、および増分バックアップ。
  これらの設定は**カスタム**カスタムバックアップスキームで使用可能で、バックアップ方式に基づいています。**毎月完全、毎週差分、毎日増分**は事前に設定されたカスタムスキームです。

例

時間単位のバックアップのデフォルト設定で、**常に増分（単一ファイル）**バックアップスキームを使用します。

- 時刻でスケジュール。
- 時間単位のバックアップ:月～金、午前8時～午後6時の1時間ごと。
- **[週単位のバックアップ]** オプションは月曜日に設定されています。

保護計画の **[保持する期間]** セクションでは、月単位、週単位、日単位、時間単位のバックアップに保持ルールを適用できます。

次の表に、8日間に作成されるバックアップの種類を示します。

日付	曜日	説明
7月1日	月曜日	毎月の最初のバックアップは月単位のバックアップなので、この日の最初のバックアップは月単位バックアップになります。この日の他のバックアップは時間単位のバックアップとなります。 この週の最初のバックアップが月単位のバックアップとみなされます。このため週単位のバックアップはありません。次週の最初のバックアップは、週単位のバックアップになります。
7月2日	火曜日	この日の最初のバックアップは日単位、その他のバックアップは時間単位のバックアップになります。
7月3日	水曜日	この日の最初のバックアップは日単位、その他のバックアップは時間単位のバックアップになります。
7月4日	木曜日	この日の最初のバックアップは日単位、その他のバックアップは時間単位のバックアップになります。

日付	曜日	説明
7月5日	金曜日	この日の最初のバックアップは日単位、その他のバックアップは時間単位のバックアップになります。
7月6日	土曜日	この日の最初のバックアップは日単位、その他のバックアップは時間単位のバックアップになります。
7月7日	日曜日	この日の最初のバックアップは日単位、その他のバックアップは時間単位のバックアップになります。
7月8日	月曜日	この日の最初のバックアップは週単位、その他のバックアップは時間単位のバックアップになります。

保持ルールの構成

保持ルールは保護計画の一部であり、その可用性とオプションはバックアップスキームに依存します。詳細については、"バックアップスキームによる保持ルール"（424ページ）を参照してください。

保持ルールを構成するには

1. 保護計画で、**バックアップ**モジュールを展開します。
2. **[保持する数]** をクリックします。
3. 次のオプションからひとつを選択します。
   - **バックアップの数**
   - **バックアップ世代**

     月次、週次、日次、毎時のバックアップを個別に設定できます。いずれのタイプでも最大値は9999です。

     また、すべてのバックアップに単一の設定を使用することもできます。
   - **バックアップの合計サイズ別**

     この設定は、**[常に増分（単一ファイル）]** バックアップスキームが指定されている場合は使用できません。
   - **バックアップを無期限に保存する**
4. （**[バックアップを無期限に保存する]** を選択していない場合）選択したオプションの値を構成します。
5. （**[バックアップを無期限に保存する]** を選択していない場合）保持ルールを適用するタイミングを選択します。
   - バックアップ後
   - バックアップ前

     このオプションは、Microsoft SQL ServerクラスターまたはMicrosoft Exchange Serverクラスターのバックアップでは使用できません。
6. **[完了]** をクリックします。
7. 保護計画を保存します。

レプリケーション

レプリケーションでは、新しいバックアップがレプリケーションロケーションに自動的にコピーされます。レプリケーションのロケーションにあるバックアップは、ソースのロケーションにあるバックアップに依存せず、その逆もまた同様です。

ソースロケーションの最新バックアップのみがレプリケートされます。ただし、それ以前のバックアップがレプリケートされない場合（ネットワーク接続の問題など）、レプリケーション処理には、最後に正常にレプリケートされた後に作成されたすべてのバックアップが含まれます。

レプリケーション処理が中断された場合、処理されたデータは次のレプリケーション処理で使用されます。

注意
このトピックでは、保護計画の一部としてのレプリケーションについて説明します。また、個別のバックアップレプリケーション計画を作成することもできます。 詳細については、"バックアップのレプリケーション"（194ページ）を参照してください。

使用例

- 確実で信頼性の高い復元
  バックアップをオンサイト（その場での復元向け）とオフサイトの両方に保存します。オフサイトのバックアップにより、プライマリロケーションに影響を及ぼすストレージ障害や自然災害が発生した場合でもバックアップが安全性を確保できます。
- クラウドストレージを使用した、自然災害からのデータの保護
  変更されたデータのみを転送することでクラウド ストレージにバックアップをレプリケートします。
- 最新のリカバリ ポイントのみを保存
  ストレージコストを節約するために、高速ストレージから古いバックアップを削除する保持ルールを設定します。

サポートされるロケーション

ロケーション	ソースロケーションとして	レプリケーションのロケーションとして
ローカルフォルダ	+	+
ネットワークフォルダ	+	+
クラウドストレージ	-	+
Secure Zone	+	–
パブリッククラウド	+	+

レプリケーションを有効化するには

1. 保護計画で、**[バックアップ]** モジュールを展開し、**[ロケーションを追加]** をクリックします。

   注意
   [バックアップ先] でクラウドストレージを選択した場合は、**[ロケーションを追加]** オプションは使用できません。

2. 利用可能なロケーションのリストから、レプリケーションのロケーションを選択します。
   このロケーションは、レプリケーション用に追加したロケーションの数に応じて、**2番目のロケーション**、**3番目のロケーション**、**4番目のロケーション**、または**5番目のロケーション**として保護計画に表示されます。
3. （オプション） ギアアイコンをクリックして、レプリケーションのロケーションのオプションを設定します。
   - **パフォーマンスとバックアップウィンドウ** - 選択したロケーションのバックアップウィンドウを設定します（"パフォーマンスとバックアップウィンドウ"（468ページ）を参照）。これらの設定により、レプリケーションパフォーマンスを定義します。
   - **ロケーションの削除** - 現在選択されているレプリケーションのロケーションを削除します。
   - （クラウドストレージのみ）**物理データ配送** - 当初のバックアップのレプリカをインターネット上で作成するのではなく、リムーバブルストレージデバイスに保存し、クラウドストレージへのアップロード向けに発送します。
     このオプションは、ネットワークの接続速度が遅いロケーションや、ネットワークでの大容量ファイル転送時の帯域幅消費を軽減したい場合に適しています。このオプションを有効にする際に、Advanced Cyber Protectのサービスクォータが必要となることはありません。ただし、配送オーダーを作成してトラックするには、物理データ配送のサービスクォータが必要になります。["物理データ配送"（472ページ）]をご覧ください。

     注意
     このオプションは、プロテクションエージェントのバージョンがC21.06以降の場合にサポートされます。

4. （オプション） レプリケーションのロケーション以下の **[保持期間]** で、該当のロケーションの保持ルールを構成します（"保持ルール"（423ページ）を参照）。
5. （オプション） 手順1～4を繰り返して、さらにレプリケーションのロケーションを追加します。
   最大で4つのレプリケーションのロケーション（**2番目のロケーション**、**3番目のロケーション**、**4番目のロケーション**、**5番目のロケーション**）を構成できます。**クラウドストレージ**を選択した場合、レプリケーションのロケーションを追加することはできません。

重要
同じ保護計画でバックアップとレプリケーションを有効にしている場合、次回のスケジュールバックアップの前にレプリケーションが完了するように設定されていることを確認してください。レプリケーションが進行中の場合、スケジュールバックアップは開始されません。例えば、レプリケーションの完了に26時間要する場合、24時間に1回実行されるスケジュールバックアップが開始されることはありません。

この依存関係を回避するには、バックアップのレプリケーションに別の計画を使用するようにします。この特定の計画の詳細については、「"バックアップのレプリケーション"（194ページ）」を参照してください。

暗号化

Advanced Encryption Standard（AES）暗号化アルゴリズムはGalois/Counterモード（GCM）で動作し、256ビットのランダムに生成されたキーを使用します。暗号化キーは、パスワードのSHA-2（256ビット）ハッシュをキーとしてAES-256アルゴリズムで暗号化されます。パスワードはディスク上やバックアップ内には保管されず、パスワードのハッシュは検証に使用されます。

この2段階のセキュリティにより、バックアップ データは不正なアクセスから保護されますが、失われたパスワードを復元することはできません。

注意
強力なパスワードを使用したAES-256アルゴリズムは、耐量子性の暗号化を提供します。これは量子コンピューターを利用した暗号解析攻撃に対して有効です。

特に、規制コンプライアンスが適用される企業の場合、クラウドストレージに格納されるすべてのバックアップを暗号化することをお勧めします。

次の方法で暗号化を構成できます。

- 保護計画で
- マシンのプロパティとして、Cyber Protectモニターまたはコマンドラインインターフェイスを使用して

保護計画で暗号化を構成する

保護計画では、暗号化はデフォルトで有効になっており、AES-256アルゴリズムが使用されてます。

強力なパスワードの使用によって、AES-256アルゴリズムは耐量子性の暗号化を提供します。

コンプライアンスモードのアカウントの場合、保護計画で暗号化を設定できません。保護対象デバイスで暗号化を設定する方法については、"マシンプロパティとして暗号化を構成する"（431ページ）を参照してください。

暗号化を構成するには

1. 保護計画で、**[バックアップ]** モジュールを展開します。
2. **[暗号化]** で、**[パスワードを指定]** をクリックしします。
3. 暗号化パスワードを指定して確認します。
4. **[OK]** をクリックします。

警告
パスワードを失くしたり忘れたりした場合に、暗号化されたバックアップをリカバリする方法はありません。

保護計画を適用した後に、暗号化の設定を変更することはできません。異なる暗号化の設定を使用するには、新しい計画を作成する必要があります。

マシンプロパティとして暗号化を構成する

マシンのプロパティとしてバックアップ暗号化を構成できます。この場合、バックアップ暗号化は保護計画ではなく、保護されたワークロード上で構成されます。マシンのプロパティとしての暗号化には、256ビットキー（AES-256）を使用したAESアルゴリズムが使用されます。

注意
強力なパスワードを使用したAES-256アルゴリズムは、耐量子性の暗号化を提供します。これは量子コンピューターを利用した暗号解析攻撃に対して有効です。

マシンのプロパティとして暗号化を構成すると、保護計画には次のような影響があります。

- **既にマシンに適用されている保護計画。**保護計画にある暗号化設定が異なっていると、バックアップが失敗します。
- **後でマシンに適用される保護計画。**マシンに保存された暗号化設定により、保護計画の暗号化設定が上書きされます。バックアップモジュールの設定で暗号化が無効になっている場合でも、バックアップは暗号化されます。

コンプライアンスモードのアカウントでは、マシンプロパティとしての暗号化のみが利用可能です。

同じvCenter Serverに接続されたVMwareのエージェントが複数あり、マシンのプロパティとして暗号化を構成する場合、エージェント間のロードバランシングのため、VMwareのエージェントがあるすべてのマシンで同じ暗号化パスワードを使用する必要があります。

次の方法で、マシンのプロパティとして暗号化を設定することができます。

- コマンドライン上で
- Cyber Protectモニター（WindowsおよびmacOSで利用可能）で

暗号化を構成するには

コマンドライン上で

1. 管理者（Windows）またはルートユーザー（Linux）でログインします。
2. コマンドラインで以下のコマンドを実行します。

- Windowsの場合:

```
<installation_path>\PyShell\bin\acropsh.exe -m manage_creds --set-password
<encryption_password>
```

  デフォルトのインストールパスは%ProgramFiles%\BackupClientです。
- Linuxの場合:

```
/usr/sbin/acropsh -m manage_creds --set-password <encryption_password>
```

- 仮想アプライアンスの場合:

```
 /./sbin/acropsh -m manage_creds --set-password <encryption_password>
```

警告
パスワードを失くしたり忘れたりした場合に、暗号化されたバックアップをリカバリする方法はありません。

Cyber Protectモニターで

1. 管理者としてログインします。
2. 通知領域（Windows）またはメニューバー（macOS）でCyber Protectモニターアイコンをクリックします。
3. ギアアイコンをクリックしてから、**[設定]** > **[暗号化]** をクリックします。
4. **[このマシンのパスワードを設定]** を選択します。暗号化パスワードを指定および確認します。
5. **[保存]** をクリックします。

警告
パスワードを失くしたり忘れたりした場合に、暗号化されたバックアップをリカバリする方法はありません。

暗号化設定をリセットするには

1. 管理者（Windows）またはルートユーザー（Linux）でログインします。
2. コマンドラインで以下のコマンドを実行します。
   - Windowsの場合:

```
<installation_path>\PyShell\bin\acropsh.exe -m manage_creds --reset
```

     デフォルトのインストールパスは%ProgramFiles%\BackupClientです。
   - Linuxの場合:

```
/usr/sbin/acropsh -m manage_creds --reset
```

   - 仮想アプライアンスの場合:

```
/./sbin/acropsh -m manage_creds --reset
```

重要
保護計画でバックアップが作成された後にマシンのプロパティとしての暗号化をリセットしたり、暗号化パスワードを変更したりすると、次回のバックアップ操作は失敗します。ワークロードのバックアップを続行するには、新しい保護計画を作成してください。

ノータリゼーション

注意
この機能は、Advanced Backupパックで利用可能です。

ノータリゼーションでは、ファイルが本物であり、バックアップ後に改変されていないことを証明できます。法律関係の文書のファイルやその他の非改ざん性の証明が必要なファイルをバックアップする際に、ノータリゼーションを有効にすることを推奨します。

ノータリゼーションは、ファイルレベルのバックアップのみで実行できます。デジタル署名のあるファイルは、ノータライズ（公証）の必要がないためスキップされます。

以下の場合はノータリゼーションを使用できません。

- バックアップ形式が **[バージョン 11]** に設定されている場合
- バックアップ先がSecure Zoneの場合

ノータリゼーションの使用方法

バックアップ対象として選択されたすべてのファイル（デジタル署名のあるファイルを除く）のノータリゼーションを有効にするには、保護計画作成時に **[ノータリゼーション]** スイッチをオンにします。

復元を設定する場合、ノータライズ（公証）されたファイルには特別なアイコンが付き、ファイルの非改ざん性をベリファイできます。

仕組み

バックアップ中に、エージェントはバックアップされるファイルのハッシュコードを計算します。ハッシュツリーを作成（フォルダ構造に基づく）して、バックアップに保存し、ハッシュツリーのルートをノータリー（公証）サービスに送信します。ノータリー（公証）サービスで、ハッシュツリーのルートが Ethereum ブロックチェーンデータベースに保存され、この値が変更されていないことが確認されます。

ファイルの非改ざん性をベリファイする場合、エージェントはファイルのハッシュを計算し、それをバックアップ内のハッシュツリーに保存されているハッシュと比較します。これらのハッシュが一致しない場合、ファイルは本物ではないと見なされます。一致する場合は、ハッシュツリーによってファイルの非改ざん性が保証されます。

ハッシュツリー自身が不正なものではないことをベリファイするために、エージェントはハッシュツリーのルートをノータリー（公証）サービスに送信します。ノータリー（公証）サービスはそれをブロックチェーンデータベースに保存されているものと比較します。ハッシュが一致すると、選択した

ファイルが本物であることが保証されます。一致しない場合は、ファイルが本物ではないというメッセージが表示されます。

デフォルトのバックアップ オプション

バックアップ オプションのデフォルト値は、企業、部署、およびユーザーレベルで存在します。部署またはユーザーアカウントが企業内または部署内で作成されると、企業または部署に設定されたデフォルト値を継承します。

企業管理者、部署管理者、および管理者権限を持たないすべてのユーザーは、あらかじめ定義された値を変更して、デフォルトのオプション値を設定できます。変更後にそれぞれのレベルに作成されるすべての保護計画で、新しい値がデフォルトで使用されます。

保護計画作成時に、ユーザーはその計画専用にカスタマイズした値でデフォルトの設定を上書きできます。

デフォルトのオプション値を変更するには

1. 次のいずれかを実行します。
   - 企業のためのデフォルト値を変更するには、企業管理者としてCyber Protectコンソールにサインインします。
   - 部署のためのデフォルト値を変更するには、部署の管理者としてCyber Protectコンソールにサインインします。
   - ユーザー自身のためのデフォルト値を変更するには、管理者権限のないアカウントを使用してCyber Protectコンソールにサインインします。
2. **[設定]** > **[システム設定]** をクリックします。
3. **[デフォルトのバックアップ オプション]** セクションを展開します。
4. オプションを選択し、必要な変更を実行します。
5. **[保存]** をクリックします。

バックアップ オプション

保護計画のバックアップオプションを変更するには、**バックアップ**モジュールの **[バックアップオプション]** フィールドで、**[変更]** をクリックします。

使用可能なバックアップ オプション

使用可能なバックアップ オプションのセットは次の条件によって異なります。

- エージェントが動作する環境（Windows、Linux、macOS）
- バックアップするデータの種類（ディスク、ファイル、仮想コンピュータ、アプリケーションデータ）。
- バックアップ先（クラウドストレージ、ローカル フォルダまたはネットワークフォルダ）。

次の表は、使用可能なバックアップ オプションを示しています。

	ディスクレベル バックアップ			ファイルレベルのバックアップ			仮想コンピュータ			SQLおよびExchange
	Windows	Linux	macOS	Windows	Linux	macOS	ESXi	Hyper-V	Virtuozzo	Windows
アラート	+	+	+	+	+	+	+	+	+	+
バックアップの統合	+	+	+	+	+	+	+	+	+	-
バックアップファイル名	+	+	+	+	+	+	+	+	+	+
バックアップ形式	+	+	+	+	+	+	+	+	+	+
バックアップのベリファイ	+	+	+	+	+	+	+	+	+	+
Changed Block Tracking（CBT）	+	-	-	-	-	-	+	+	-	-
クラスターバックアップモード	-	-	-	-	-	-	-	-	-	+
圧縮レベル	+	+	+	+	+	+	+	+	+	+
エラー処理										
エラーが発生した場合は再	+	+	+	+	+	+	+	+	+	+

試行する										
処理中にメッセージやダイアログを表示しない（サイレントモード）	+	+	+	+	+	+	+	+	+	+
不良セクタを無視する	+	-	+	+	-	+	+	+	+	-
VMスナップショットの作成中にエラーが発生した場合は再試行	-	-	-	-	-	-	+	+	+	-
高速の増分/差分バックアップ	+	+	+	-	-	-	-	-	-	-
ファイルレベルのバックアップのスナップショット	-	-	-	+	+	+	-	-	-	-
ファイルフィ	+	+	+	+	+	+	+	+	+	-

ルタ										
フォレンジックデータ	+	-	-	-	-	-	-	-	-	-
ログの切り詰め	-	-	-	-	-	-	+	+	-	SQLのみ
LVMのスナップショット	-	+	-	-	-	-	-	-	-	-
マウントポイント	-	-	-	+	-	-	-	-	-	-
マルチボリュームスナップショット	+	+	-	+	+	-	-	-	-	-
ワンクリック復元	+	+	-	-	-	-	-	-	-	-
パフォーマンスとバックアップウィンドウ	+	+	+	+	+	+	+	+	+	+
物理データ配送	+	+	+	+	+	+	+	+	+	-
処理の前後のコマンド	+	+	+	+	+	+	+	+	+	+

データ取り込みの前後に実行するコマンド	+	+	+	+	+	+	-	-	-	+
スケジューリング										
開始時間を時間枠内で割り振る	+	+	+	+	+	+	+	+	+	+
同時に実行するバックアップの数を制限	-	-	-	-	-	-	+	+	+	-
セクタ単位のバックアップ	+	+	-	-	-	-	+	+	+	-
分割	+	+	+	+	+	+	+	+	+	+
タスク失敗時の処理	+	+	+	+	+	+	+	+	+	+
タスクの開始条件	+	+	-	+	+	-	+	+	+	+
ボリューム シャドウ コピー サービス（VSS）	+	-	-	+	-	-	-	+	-	+
仮想マシンのボ	-	-	-	-	-	-	+	+	-	-

リュームシャドウコピーサービス（VSS）										
週単位のバックアップ	+	+	+	+	+	+	+	+	+	+
Windowsイベントログ	+	-	-	+	-	-	+	+	-	+

アラート

指定した日数にわたり、正常に完了したバックアップがありません

デフォルト設定:**無効**。

このオプションによって、保護計画で指定の期間に正常なバックアップがまったく実行されなかった場合にアラートを生成するかどうかが決まります。バックアップが失敗した場合に加え、スケジュールどおりにバックアップが実行されなかった場合もカウントします（バックアップの失敗）。

アラートはコンピュータ単位で生成され[**アラート**] タブに表示されます。

アラート生成するバックアップがない場合の連続日数を指定することができます。

バックアップの統合

このオプションは、クリーンアップ時にバックアップを統合するか、バックアップチェーン全体を削除するかを定義します。

デフォルト設定:**無効**。

統合とは以降の複数回のバックアップを1つのバックアップにまとめる処理です。

このオプションを有効にした場合、クリーンアップ中に削除される必要があるバックアップが、その次の依存関係のあるバックアップ（増分または差分）と統合されます。

あるいは、すべての依存関係のあるバックアップが削除の対象になるまで、バックアップが保持されます。これは長い時間がかかる可能性のある統合の回避に役立ちますが、削除を延期されたバックアップの保存領域の追加が必要になります。バックアップの経過時間または回数は、保持ルールで指定された値を上回ることがあります。

重要
統合は削除の方法の1つに過ぎず、削除に代わる手段ではないことに注意してください。統合した後のバックアップには、削除されたバックアップ内には存在していて、保持された増分バックアップや差分バックアップには存在していなかったデータは含まれません。

このオプションは、次のいずれかが当てはまる場合は効果がありません。

- バックアップ先がクラウドストレージである。
- バックアップスキームが **[常に増分（単一ファイル）]** に設定されている。
- バックアップ形式が **[バージョン12]** に設定されている。

クラウドストレージに保存されているバックアップと単一ファイルバックアップ（バージョン 11 と 12 の両方のフォーマット）は、高速で簡便な統合に適した内部構造であるため、常に統合されます。

ただし、バージョン 12 のフォーマットが使用され、複数のバックアップチェーンが存在する場合（各チェーンは別の .tibx ファイルに保存されます）、統合は最後のチェーン内でのみ機能します。他のチェーンは全体として削除されますが、最初のチェーンは削除されず、メタ情報を保持するために最小サイズに縮小されます（～12KB）。このメタ情報は、同時読み書き操作中にデータの一貫性を保証するために必要です。これらのチェーンに含まれるバックアップは、チェーン全体が削除されるまで物理的に存在しますが、保持ルールが適用されるとすぐに GUI から消えます。

それ以外の場合は、削除が延期されているバックアップにGUIのごみ箱アイコン（  ）が付けられます。このようなバックアップを X 記号をクリックして削除すると、統合が実行されます。

バックアップ ファイル名

このオプションでは、保護計画またはクラウドアプリケーションバックアップ計画によって作成されるバックアップファイルの名前を定義します。

保護計画によって作成されたバックアップファイルの場合、バックアップのロケーションを参照すると、ファイルマネージャーでこれらの名前を確認できます。

バックアップファイルについて

保護計画はそれぞれ、どのバックアップスキームとバックアップ形式が使用されているかに応じて、1つ以上のファイルをバックアップロケーションに作成します。次の表に、コンピュータごとまたはメールボックスごとに作成できるファイルの一覧を示します。

	常に増分（単一ファイル）	**その他のバックアップスキーム**
バックアップ形式が **[バージョン11]** である場合	1つのTIBファイルと1つのXMLメタデータファイル	複数のTIBファイルと1つのXMLメタデータファイル
バックアッ	バックアップチェーン（完全バックアップまたは差分バックアップ、およびそれに依存するす	

プ形式が **[バージョン12]** である場合	べての増分バックアップ）ごとに1つのTIBXファイル。ローカルまたはネットワーク（SMB）フォルダに保存されたファイルのサイズが200GBを超える場合、ファイルはデフォルトで200GBのファイルに分割されます。

ファイルの名前はすべて同じになります。タイムスタンプまたは連番が付く場合と付かない場合があります。この名前（バックアップファイル名となる）は、保護計画またはクラウドアプリケーションのバックアップ計画を作成または編集するときに定義できます。

注意
バージョン11のバックアップ形式の場合に限り、タイムスタンプがバックアップファイル名に追加されます。

保護計画またはクラウドアプリケーションのバックアップ計画でバックアップファイル名を変更すると、次のバックアップは完全バックアップになります。

同じマシンの既存バックアップのファイル名を指定すると、計画のスケジュールに従って完全バックアップ、増分バックアップ、または差分バックアップが作成されます。

注意
バックアップファイル（.tibx）を元のストレージから移動する場合は、ファイル名を変更しないでください。名前を変更したファイルは破損したものとして表示され、そこからデータをリカバリすることはできません。

ファイルマネージャーから参照できないロケーション（クラウドストレージなど）のバックアップファイル名を設定できます。この場合、**[バックアップストレージ]** タブにカスタム名が表示されます。

バックアップファイル名が表示される場所

保護計画の場合は、**[バックアップストレージ]** タブでロケーションを選択し、バックアップアーカイブを選択します。

- デフォルトのバックアップファイル名は **[詳細]** パネルに表示されます。
- デフォルト以外のバックアップファイル名を設定した場合は、**[バックアップストレージ]** タブの **[名前]** 列に直接表示されます。

クラウドアプリケーションのバックアップ計画の場合は、**[バックアップストレージ]** タブでロケーションを選択し、バックアップアーカイブを選択し、ギアアイコンをクリックします。

バックアップファイル名の制限

- バックアップファイル名の末尾を数字にすることはできません。
  デフォルトのバックアップファイル名では、名前の末尾が数字にならないように、文字「A」が追加されます。カスタム名を作成する場合は、末尾が数字でないことを確認してください。変数は数字で終わる可能性があるため、名前の末尾には変数を使用しないでください。
- バックアップファイル名に、**()&?*$<>":¥|/#**、改行記号（**¥n**）、およびタブ記号（**¥t**）を使用することはできません。

注意
使いやすいバックアップファイル名を選びます。ファイルマネージャーでバックアップロケーションを参照する際に、バックアップを簡単に区別することができます。

デフォルトのバックアップファイル名

物理マシンと仮想マシン全体、ディスク/ボリューム、ファイル/フォルダ、Microsoft SQL Serverデータベース、Microsoft Exchange Serverデータベース、およびESXi構成のバックアップのデフォルトのバックアップファイル名は、`[Machine Name]-[Plan ID]-[Unique ID]A`です。

ローカルのMicrosoft 365エージェントによって作成されたExchangeメールボックスバックアップおよびMicrosoft 365メールボックスバックアップのデフォルト名は、`[Mailbox ID]_mailbox_[Plan ID]A`です。

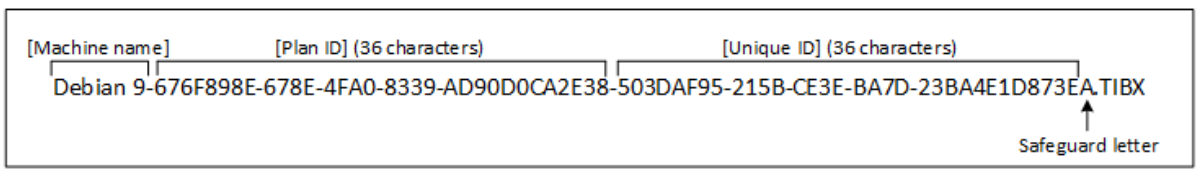
Microsoft Azureバックアップのデフォルト名には、`[Mailbox ID]_`の接頭辞が付きます。この接頭辞は削除できません。

クラウドエージェントによって作成されたクラウドアプリケーションバックアップのデフォルト名は、`[Resource Name]_[Resource Type]_[Resource Id]_[Plan Id]A`です。

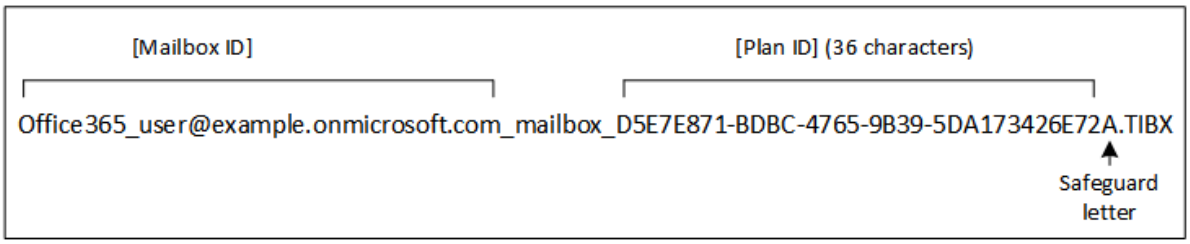
デフォルト名は次の変数で構成されます。

- `[Machine Name]` この変数は、マシン名（Cyber Protectコンソールに表示されるのと同じ名前）に置き換えられます。
- `[Plan ID]`, `[Plan Id]` これらの変数は保護計画の一意の識別子に置き換えられます。計画の名前が変更されても、この値は変更されません。
- `[Unique ID]` この変数は、選択したマシンの一意のIDに置き換えられます。マシンの名前が変更されても、この値は変更されません。
- `[Mailbox ID]` この変数は、メールボックスユーザーのプリンシパル名（UPN）に置き換えられます。
- `[Resource Name]` この変数は、ユーザーのプリンシパル名（UPN）、SharePointサイトのURL、共有ドライブ名などのクラウドデータソース名に置き換えられます。
- `[Resource Type]` この変数は、`mailbox`、`O365Mailbox`、`O365PublicFolder`、`OneDrive`、`SharePoint`、`GDrive`といったクラウドデータソースタイプに置き換えられます。
- `[Resource ID]` この変数は、クラウドデータソースの一意のIDに置き換えられます。クラウドデータソースの名前が変更されても、この値は変更されません。
- 「`A`」は、名前の末尾が数字になるのを防ぐために付加される文字です。

次の図は、デフォルトのバックアップファイル名を示しています。



次の図は、ローカルエージェントによって実行されるMicrosoft 365メールボックスのバックアップの、デフォルトのバックアップファイル名を示しています。



変数を含まない名前

バックアップファイル名を「MyBackup」に変更すると、バックアップファイルは次の例のようになります。どちらの例も、2016年9月13日から毎日14:40に実行するようにスケジュールされた増分バックアップを想定しています。

バックアップスキームを **[常に増分（単一ファイル）]** に設定したバージョン12形式の場合:

```
MyBackup.tibx
```

その他のバックアップスキームを設定したバージョン12形式の場合:

```
MyBackup.tibx
MyBackup-0001.tibx
MyBackup-0002.tibx
...
```

変数の使用

デフォルトで使用される変数のほかに、下記の変数を使用できます。

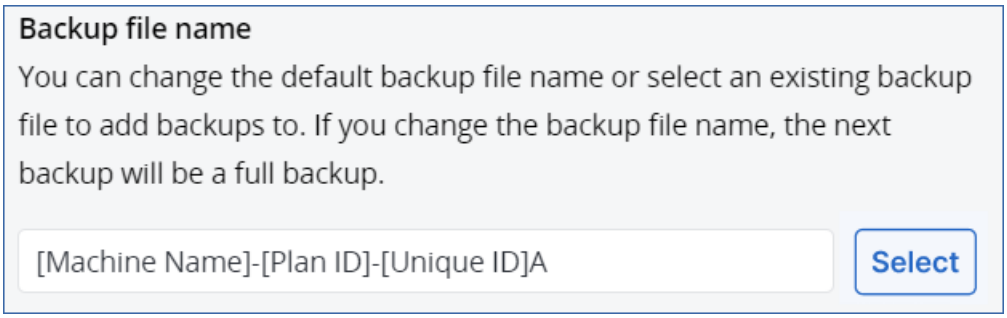
- 保護計画名に置き換えられる `[Plan name]` 変数。
- 仮想マシンがVMwareエージェントによってバックアップされている場合は「vmwesx」に、仮想マシンがHyper-Vエージェントによってバックアップされている場合は「mshyperv」に置き換えられる、`[Virtualization Server Type]` 変数。

バックアップ対象として複数のマシンまたはメールボックスを選択する場合は、バックアップファイル名に `[Machine Name]`、`[Unique ID]`、`[Mailbox ID]`、`[Resource Name]`、または `[Resource Id]` 変数を含める必要があります。

既存のバックアップアーカイブでのバックアップ作成

ワークロードのバックアップを既存のバックアップアーカイブに追加する設定ができます。

このオプションは、保護計画が1台のマシンに適用されていて、そのマシンをCyber Protectコンソールから削除するか、構成設定とともにエージェントをアンインストールする必要がある場合などに便利です。マシンを再度追加するか、エージェントを再インストールした後、強制的に保護計画を元のアーカイブにバックアップさせ続けることができます。



ワークロードのバックアップを既存のバックアップアーカイブに追加するように設定するには

非クラウドツークラウドワークロード

1. **[すべてのデバイス]** 画面で、ワークロードをクリックし、**[保護]** をクリックします。
2. 保護計画の設定で **[バックアップ]** モジュールを展開します。
3. **[バックアップオプション]** をクリックし、**[変更]** をクリックします。
4. **[バックアップ ファイル名]** タブで、**[選択]** をクリックします。
   [選択] ボタンをクリックすると、保護計画の **[バックアップ先]** セクションで選択したロケーションにあるバックアップが表示されます。

   注意
   単一のワークロードのために作成してそのデバイスに対して適用した保護計画の場合に限り、**[選択]** ボタンを利用できます。

5. アーカイブを選択して、**[完了]** をクリックします。
6. **[完了]**をクリックして、**[適用]** をクリックします。

クラウドツークラウドワークロード

1. **[管理]** > **[クラウドアプリケーションバックアップ]** タブで計画を選択します。
2. **[編集]**をクリックして、計画名の横のギアアイコンをクリックします。
3. **[ファイルバックアップ名]** タブで、**[選択]** をクリックします。

   注意
   単一のワークロードのために作成してそのデバイスに対して適用したバックアップ計画の場合に限り、**[選択]** ボタンを利用できます。

4. バックアップアーカイブを選択し、**[完了]** をクリックします。
5. **[完了]**をクリックして、**[変更を保存]** をクリックします。

バックアップ形式

バックアップ形式オプションは、保護計画によって作成されるバックアップの形式を定義します。このオプションは、バージョン11バックアップ形式を既に使用している保護計画でのみ使用できます。その場合、バックアップ形式をバージョン12へ変更できます。バックアップ形式のバージョン12への切り替え後、このオプションは利用できなくなります。

- **バージョン11**
  下位互換性のために残されたレガシー形式。

  注意
  バックアップ形式バージョン11を使用して、データベース可用性グループ（DAG）をバックアップすることはできません。DAGのバックアップをサポートしているのは、バージョン12形式のみです。

- **バージョン12**
  Acronis Backup 12で導入されたバックアップ形式では、バックアップと復元をより高速に実行できます。各バックアップチェーン（完全バックアップまたは差分バックアップ、およびそれに依存するすべての増分バックアップ）は、単一のTIBXファイルに保存されます。

バックアップ形式とバックアップファイル

バックアップロケーションがファイルマネージャで参照できるロケーション（ローカルフォルダ、ネットワークフォルダなど）である場合は、バックアップ形式に応じてファイル数とその拡張子が決まります。次の表に、コンピュータごとまたはメールボックスごとに作成できるファイルの一覧を示します。

	常に増分（単一ファイル）	**その他のバックアップスキーム**
バックアップ形式が **[バージョン11]** である場合	1つのTIBファイルと1つのXMLメタデータファイル	複数のTIBファイルと1つのXMLメタデータファイル
バックアップ形式が **[バージョン12]** である場合	バックアップチェーン（完全バックアップまたは差分バックアップ、およびそれに依存するすべての増分バックアップ）ごとに1つのTIBXファイル。ローカルまたはネットワーク（SMB）フォルダに保存されたファイルのサイズが200GBを超える場合、ファイルはデフォルトで200GBのファイルに分割されます。	

バックアップ形式のバージョン12（TIBX）への変更

バックアップ形式をバージョン11（TIB形式）からバージョン12（TIBX形式）へ変更する場合:

- 次回のバックアップは完全バックアップになります。
- ファイルマネージャーで参照できるバックアップロケーション（ローカルフォルダ、ネットワークフォルダなど）において、新しいTIBXファイルが作成されます。新しいファイルは元のファイルと同じ名前になり、**_v12A**サフィックスが追加されます。
- 保持ルールとレプリケーションは新しいバックアップにのみ適用されます。
- 古いバックアップは削除されず、**[バックアップストレージ]** タブから引き続き使用可能です。これらは、手動で削除できます。
- 古いクラウドバックアップは**クラウドストレージ**のクォータを消費しません。
- 手動で削除するまで、古いローカルバックアップは**ローカルバックアップ**のクォータを消費します。

アーカイブ内の重複除外

バージョン12のTIBXバックアップ形式では、アーカイブ内の重複除外がサポートされています。以下のようなメリットがあります。

- 組み込みのブロックレベル重複除外をどのようなタイプのデータにも使用することで、バックアップサイズが大幅に減少
- 重複ストレージが発生しない、ハードリンクの効率的な処理
- ハッシュベースのチャンク実行

注意
アーカイブ内での重複除外が、TIBX形式のすべてのバックアップを対象にデフォルトで有効になります。バックアップオプションで有効にする必要はありません。また、無効にすることもできません。

異なる製品バージョン間におけるバックアップ形式の互換性

異なる製品バージョン間におけるバックアップ形式の互換性については、「異なる製品バージョン間におけるバックアップアーカイブの互換性（1689）」を参照してください。

バックアップのベリファイ

検証は、バックアップからデータ復元ができるかどうかを確認する処理です。このオプションを有効にした場合、保護計画で作成された各バックアップは、作成後直ちにチェックサム検証メソッドによって検証されます。この処理は、プロテクションエージェントによって実行されます。

デフォルト設定:**無効**。

チェックサム検証経由の検証の詳細については、"チェックサムのベリファイ"（200ページ）を参照してください。

注意
サービスプロバイダーが選択する設定によっては、クラウドストレージにバックアップするときに検証を利用できない場合があります。また、パブリッククラウド上のバックアップロケーションでは、検証は利用できません。

Changed Block Tracking（CBT）

このオプションは以下のバックアップに対して有効です:

- 仮想マシンのディスクレベルバックアップ
- Windowsを実行する物理マシンのディスクレベルバックアップ
- Microsoft SQL Serverデータベースのバックアップ
- Microsoft Exchange Serverデータベースのバックアップ

デフォルト設定:**有効**。

このオプションによって、増分バックアップまたは差分バックアップの実行時にChanged Block Tracking（CBT）を使用するかどうかを決定します。

CBTテクノロジは、バックアッププロセスを高速にします。ディスクまたはデータベースの内容に対する変更は、ブロックレベルで継続的に追跡されます。バックアップが開始されると、変更は即座にバックアップに保存されます。

クラスターバックアップモード

注意
この機能は、Advanced Backupパックで利用可能です。

これらのオプションは、Microsoft SQL ServerおよびMicrosoft Exchange Serverのデータベースレベルのバックアップの場合に選択できます。

これらのオプションは、クラスター内の個々のノードやデータベースではなく、クラスター自体（Microsoft SQL Server Always On可用性グループ（AAG）またはMicrosoft Exchange Serverデータベース可用性グループ（DAG））がバックアップ対象として選択されている場合にのみ選択できます。クラスタ内の個々のアイテムを選択すると、バックアップはクラスタ対応にならず、選択されたアイテムのコピーのみがバックアップされます。

Microsoft SQL Server

このオプションでは、SQLサーバーAlways On可用性グループ（AAG）のバックアップモードを決定します。このオプションを有効にするには、SQLエージェントをすべてのAAGノードにインストールする必要があります。Always On可用性グループのバックアップの詳細については、「Always On可用性グループ（AAG）の保護」を参照してください。

デフォルト設定:**セカンダリレプリカ（可能な場合）**。

次の中からひとつ選択できます。

- **セカンダリレプリカ（可能な場合）**
  すべてのセカンダリレプリカがオフラインの場合は、プライマリレプリカがバックアップされます。プライマリレプリカをバックアップすると、SQLサーバーの動作が遅くなる可能性がありますが、データは最新の状態でバックアップされます。
- **セカンダリレプリカ**
  すべてのセカンダリレプリカがオフラインの場合、バックアップは失敗します。セカンダリレプリカをバックアップしても、SQLサーバーのパフォーマンスには影響せず、バックアップウィンドウを拡張できます。ただし、パッシブレプリカには、最新ではない情報が含まれていることがあります。これは、そのようなレプリカが多くの場合、非同期に（遅れて）アップデートされるように設定されているためです。
- **プライマリレプリカ**
  プライマリレプリカがオフラインの場合、バックアップは失敗します。プライマリレプリカをバックアップすると、SQLサーバーの動作が遅くなる可能性がありますが、データは最新の状態でバックアップされます。

このオプションの値に関係なく、データベースの一貫性を保つために、バックアップ開始時に **[同期]** 状態でも **[同期しています]** 状態でもないデータベースはスキップされます。すべてのデータベースがスキップされると、バックアップは失敗します。

Microsoft Exchange Server

このオプションは、Exchangeサーバーのデータベース可用性グループ（DAG）のバックアップモードを決定します。このオプションを有効にするには、Exchangeエージェントをすべての DAG ノードにインストールする必要があります。データベース可用性グループの詳細については、「データベース可用性グループ（DAG）の保護」を参照してください。

デフォルト設定:**パッシブコピー（可能な場合）**。

次の中からひとつ選択できます。

- **パッシブコピー（可能な場合）**
  すべてのパッシブコピーがオフラインの場合、アクティブコピーがバックアップされます。アクティブコピーをバックアップすると、Exchangeサーバーの動作が遅くなる可能性がありますが、データは最新の状態でバックアップされます。
- **パッシブコピー**
  すべてのパッシブコピーがオフラインの場合、バックアップは失敗します。パッシブコピーをバックアップしてもExchange Serverのパフォーマンスには影響はありません。また、これにより、バックアップウィンドウを拡張できるようになります。ただし、パッシブ コピーは非同期的に（遅れて）アップデートされるように設定されていることが多いため、このコピーには最新の情報が含まれていない可能性があります。
- **アクティブコピー**
  アクティブコピーがオフラインの場合、バックアップは失敗します。アクティブコピーをバックアップすると、Exchangeサーバーの動作が遅くなる可能性がありますが、データは最新の状態でバックアップされます。

このオプションの値に関係なく、データベースの一貫性を保つために、バックアップ開始時に **[正常]** 状態でも **[アクティブ]** 状態でもないデータベースはスキップされます。すべてのデータベースがスキップされると、バックアップは失敗します。

圧縮レベル

注意
このオプションはクラウドツークラウドバックアップでは使用できません。これらのバックアップの圧縮は、デフォルトで、**通常**レベル以下に対応する固定レベルで有効になっています。

このオプションは、バックアップ データに適用する圧縮レベルを定義します。選択可能なレベルは次のとおりです。**[なし]**、**[通常]**、**[高]**、**[最大]**。

デフォルト設定:**[通常]** です。

圧縮レベルが高くなるほど、バックアップに時間がかかりますが、その結果、必要となるスペースは小さくなります。現時点で、**高**レベルと**最大**レベルの動作は変わりません。

最適なデータ圧縮レベルは、バックアップするデータの種類によって異なります。たとえば、バックアップに含まれるファイルが基本的に.jpg、.pdf、.mp3などの圧縮ファイルの場合、圧縮レベルを最大にしてもバックアップサイズはそれほど縮小されません。ただし、.doc または .xls などのフォーマットであれば十分に圧縮されます。

エラー処理

これらのオプションによって、バックアップ中に発生する可能性があるエラーを処理する方法を指定できます。

エラーが発生した場合は再試行する

デフォルト設定:**有効。試行数:10回。試行間隔:30 秒。**

復元可能なエラーが発生した場合、失敗した処理が再試行されます。試行間隔および試行回数を設定できます。試行は、処理が成功するか、または指定した回数の試行が行われると停止します。

たとえば、バックアップの実行中にネットワーク上のバックアップ先が利用できないか、接続できない場合、30秒ごとに30回を超えない範囲でバックアップ先への接続が試行されます。試行は、接続が再開されるか、または指定された回数の試行が行われると停止します。

ただし、バックアップの開始時にバックアップ先が利用できない場合は、10回に限って試行されます。

処理中にメッセージやダイアログを表示しない（サイレントモード）

デフォルト設定:**有効。**

サイレントモードをオンにすると、ユーザーによる操作を必要とする場面で処理が自動的に行われます（不良セクタへの対応は別のオプションとして定義されているため、この設定では制御されません）。ユーザーによる操作なしに処理を続行できない場合、その処理は失敗します。処理の詳細（エラーがある場合は、それも含む）は、処理のログに記載されます。

不良セクタを無視する

デフォルト設定:**無効。**

このオプションを無効にした場合、プログラムが不良セクタを検出するたびに、バックアップアクティビティに **[ユーザーによる操作が必要]** ステータスが割り当てられます。障害が急速に深刻化しているディスクから有効な情報をバックアップするには、[不良セクタを無視する] をオンにします。残りのデータはバックアップされるため、作成されたディスクバックアップをマウントして有効なファイルを別のディスクに取り出すことができます。

注意
不良セクタのスキップは、Linuxではサポートされません。Cyber Protectのオンプレミスバージョンのブータブルメディアビルダーにより、オフラインモードを使用して、不良セクタのあるLinuxシステムをバックアップできます。オンプレミスのブータブルメディアビルダーを使用する場合は、別途ライセンスが必要です。アドバイスが必要な場合は、サポートにお問い合わせください。

VMスナップショットの作成中にエラーが発生した場合は再試行

デフォルト設定:**有効。試行回数:3。試行間隔:5 分間。**

仮想マシンのスナップショットの取得が失敗した場合、プログラムにより失敗した処理が再試行されます。試行間隔および試行回数を設定できます。試行は、処理が成功するか、または指定した回数の試行が行われると停止します。

高速の増分/差分バックアップ

このオプションは、ディスクレベルの増分/差分バックアップで有効です。

このオプションはJFS、ReiserFS3、ReiserFS4、ReFS、またはXFSファイルシステムでフォーマットされたボリュームには有効ではありません（常に無効）。

デフォルト設定:**有効。**

増分/差分バックアップは、変更されたデータのみ取り込みます。バックアップ処理を高速化するため、ファイルが変更されたかどうかの判定は、ファイルが最後に保存されたときの日付/時刻とファイル サイズに基づいて行われます。この機能を無効にすると、ファイル全体の内容がバックアップに保存されている内容と比較されます。

ファイルフィルタ（除外/包含）

ファイルフィルタを使用して、特定のファイルとフォルダだけをバックアップに含めたり、特定のファイルとフォルダをバックアップから除外したりします。

ファイルフィルタは、特に定められていない限り、マシン全体のバックアップ、ディスクレベルバックアップ、ファイルレベルのバックアップで使用できます。

ファイルフィルタは、XFS、JFS、exFAT、およびReiserFS4ファイルシステムでは利用できません。詳細については、"サポートされるファイル システム"（52ページ）を参照してください。

ファイルフィルタは、VMwareエージェント、Hyper-Vエージェント、またはScale Computingエージェントなど、エージェントレスモードでバックアップする仮想マシンのダイナミックディスク（LVMボリュームまたはLDMボリューム）には適用できません。

ファイルフィルタを有効にする手順

1. 保護計画で、**[バックアップ]** モジュールを展開します。
2. **[バックアップオプション]** で **[変更]** をクリックします。
3. **ファイルフィルタ（除外/包含）**を選択します。
4. 次に示すいずれかのオプションを使用します。

包含/除外フィルタ

フィルタには、包含フィルタと除外フィルタの2種類があります。

- **以下の条件に合致するファイルのみを含める**
  包含フィルタでC:\File.exeを指定すると、マシン全体のバックアップを選択しても、このファイルのみがバックアップされます。

  注意
  バックアップ形式が**バージョン11**で、バックアップ先がクラウドストレージではない場合、このフィルタはファイルレベルのバックアップをサポートしません。

- **以下の条件に合致するファイルを除外する**
  除外フィルタでC:\File.exeを指定すると、マシン全体のバックアップを選択しても、このファイルはバックアップ中にスキップされます。

両方のフィルタを同時に使用できます。除外フィルタは包含フィルタより優先されます。つまり、両方のフィールドでC:\File.exeを指定した場合、バックアップ時にこのファイルはスキップされます。

フィルタ条件

フィルタ条件として、ファイル名やフォルダ名、ファイルやフォルダのフルパス、ワイルドカード記号を使ったマスクが使用できます。

フィルタ条件では、大文字と小文字は区別されません。例えば、C:\Tempを指定した場合、C:\TEMPとC:\tempが選択されます。

- 名前
  Document.txt など、ファイルまたはフォルダの名前を指定してください。その名前のファイルとフォルダがすべて選択されます。
- フルパス
  ファイルまたはフォルダのフルパスは、ドライブ文字（Windowsをバックアップする場合）またはルートディレクトリ（LinuxまたはmacOSをバックアップする場合）を先頭にして指定します。Windows、Linux、macOSの場合、通常のスラッシュ記号を使用できます（例: C:/Temp/File.tmp）。Windowsでは、円記号（バックスラッシュ）も使用できます（例: C:\Temp\File.tmp）。

  重要
  ディスクレベルバックアップ中に、バックアップされたマシンのオペレーティングシステムが正しく検出されない場合、フルパスファイルフィルタは機能しません。除外フィルタに、警告が表示されます。インクルージョンフィルタがあると、バックアップは失敗します。
  例えばファイルのフルパスは、C:\Temp\File.tmpのようになります。ドライブ文字やルートディレクトリを含むフルパスフィルタ（C:\Temp\File.tmpやC:\Temp*など）は、警告や失敗の原因になります。
  ドライブ文字やルートディレクトリを使用しないフィルタ（例えば、Temp* や Temp\File.tmp）や、アスタリスクで始まるフィルタ（例えば、*C:\）では、警告や失敗が発生することはありません。ただし、バックアップされたマシンのオペレーティングシステムが正しく検出されない場合、これらのフィルタも機能しません。

- マスク

名前とフルパスには、アスタリスク（*）、ダブルアスタリスク（**）、クエスチョンマーク（?）のワイルドカード文字を使用できます。

アスタリスク（*）は0個以上の文字を表します。例えば、**Doc*.txt**というフィルタ条件は`Doc.txt`や`Document.txt`のファイルと一致します。

ダブルアスタリスク（**）は、0個以上の文字（スラッシュを含む）を表します。例えば、「****/Docs/**.txt**」とは、「`Docs`」という名前のフォルダ以下、およびそのすべてのサブフォルダ以下にある、すべてのテキストファイル（.txt）と一致します。ダブルアスタリスク（**）ワイルドカードは、バージョン12形式のバックアップにのみ使用できます。

クエスチョンマーク（?）は1文字のみを表します。例えば、**Doc?.txt**は、`Doc1.txt`や`Docs.txt`と一致しますが、`Doc.txt`または`Doc11.txt`などのファイルとは一致しません。

ファイルレベルのバックアップのスナップショット

このオプションは、ファイルレベルのバックアップでのみ有効です。

このオプションでは、ファイルを 1 つずつバックアップするか、またはデータのインスタント スナップショットを作成するかを定義します。

注意
ネットワーク共有に保存されているファイルは、常に1つずつバックアップされます。

デフォルト設定:

- バックアップの対象としてLinuxを実行しているマシンのみが選択されている場合:**スナップショットを作成しません。**
- それ以外の場合:**可能な場合はスナップショットを作成します。**

次のいずれかを選択できます。

- **可能な場合はスナップショットを作成します**
  スナップショットを作成できない場合は、直接ファイルをバックアップします。
- **常にスナップショットを作成します**
  スナップショットでは、排他アクセスで開かれているファイルを含む、すべてのファイルをバックアップできます。ファイルは特定の同じ時点でバックアップされます。この設定は、これらの要素が不可欠である場合のみ、つまりスナップショットなしでファイルをバックアップしても意味がない場合にのみ選択してください。スナップショットを作成できない場合、バックアップは失敗します。
- **スナップショットを作成しません**
  常に直接ファイルをバックアップします。排他アクセスで開かれているファイルをバックアップしようとすると、読み取りエラーになります。バックアップに含まれるファイルの時間的な整合性が失われることがあります。

フォレンジックデータ

ウイルス、マルウェア、ランサムウェアは、データを盗んだり改ざんしたりするなどの悪質なアクティビティを行います。これらのアクティビティの調査が必要になる場合がありますが、調査が可能なのはデジタル痕跡が残されている場合に限られます。しかし、ファイルやアクティビティのトレースなどデ

ジタル痕跡の一部が削除されていたり、悪意のあるアクティビティの影響を受けたマシンが利用できなくなったりしている場合があります。

フォレンジックデータを伴うバックアップでは、調査担当者が、通常のディスクバックアップには含まれてないディスク領域を分析できます。**[フォレンジックデータ]** というバックアップオプションを使用すれば、フォレンジック調査に使用できるデジタル痕跡として、未使用のディスク領域のスナップショット、メモリーダンプ、実行中のプロセスのスナップショットを収集することができます。

フォレンジックデータが含まれているバックアップでは、自動的に公証が行われます。

[フォレンジックデータ] オプションを使用できるのは、以下のオペレーティングシステムを搭載したWindowsマシンのマシン全体のバックアップのみです。

- Windows 8.1、Windows 10
- Windows Server 2012 R2～Windows Server 2019

以下のマシンでは、フォレンジックデータを伴うバックアップを利用できません。

- VPN経由でネットワークに接続していて、インターネットに直接アクセスすることができないマシン
- BitLockerで暗号化されたディスクを持つマシン

注意
バックアップモジュールを有効にした保護計画をマシンに適用した後は、フォレンジックデータの設定を変更することはできません。別のフォレンジックデータ設定を使用する場合は、新しい保護計画を作成してください。

フォレンジックデータを伴うバックアップは、以下のロケーションに保存することができます。

- クラウドストレージ
- ローカルフォルダ

  注意
  USBで接続した外付けハードディスクの場合のみ、ローカルフォルダのロケーションがサポートされます。
  ローカルダイナミックディスクは、フォレンジックデータのバックアップロケーションとしてはサポートされていません。

- ネットワークフォルダ

フォレンジックバックアップのプロセス

フォレンジックバックアップのプロセスでは、システムが以下の処理を実行します。

1. 未処理のメモリダンプを収集し、実行中のプロセスのリストを作成します。
2. ブータブルメディアで自動的にマシンを再起動します。
3. 占有済みの領域と未割り当ての領域の両方を組み込んだバックアップを作成します。
4. バックアップしたディスクの公証を行います。

5. ライブのオペレーティングシステムで再起動して、計画を引き続き実行します（レプリケーション、保持、ベリファイなど）。

フォレンジックデータの収集を構成するには

1. Cyber Protectコンソールで **[デバイス]** > **[すべてのデバイス]** に進みます。あるいは、**[管理]** タブで保護計画を作成することも可能です。
2. 対象のデバイスを選択して、**[保護]** をクリックします。
3. 保護計画で **[バックアップ]** モジュールを有効にします。
4. **[バックアップの対象]** で **[マシン全体]** を選択します。
5. **[バックアップオプション]** で **[変更]** をクリックします。
6. **[フォレンジックデータ]** オプションを見つけます。
7. **[フォレンジックデータの収集]** を有効にします。システムが自動的にメモリダンプを収集し、実行中のプロセスのスナップショットを作成します。

   注意
   フルメモリダンプには、パスワードなどの機密データも含まれている可能性があります。

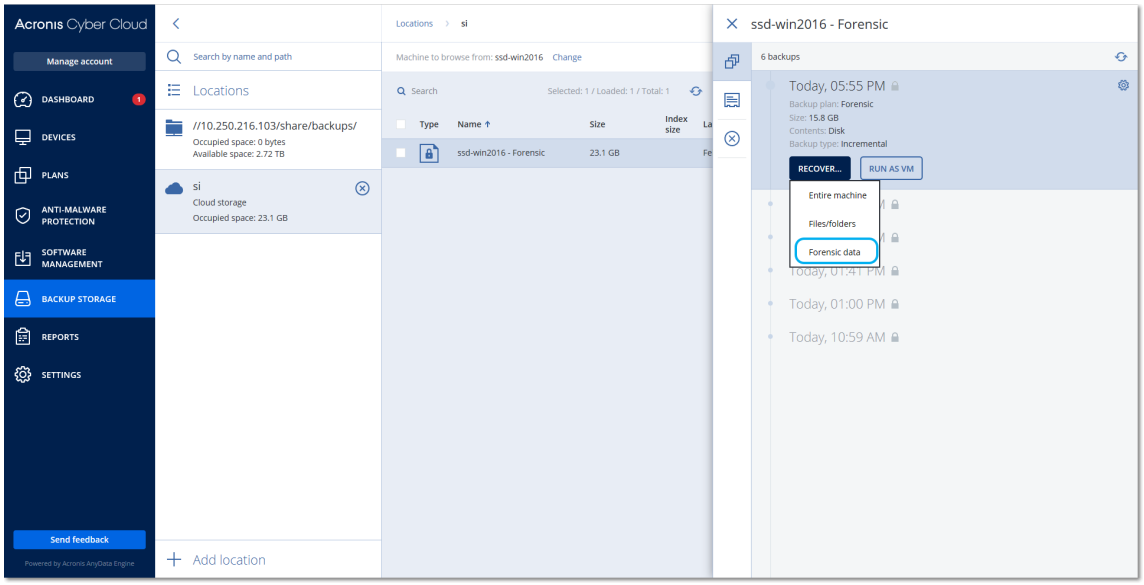
8. ロケーションを指定します。
9. **[今すぐ実行]** をクリックして、フォレンジックデータのバックアップをすぐに実行するか、スケジュールに沿ってバックアップが作成されるのを待ちます。
10. **[監視]** > **[アクティビティ]** に進み、フォレンジックデータのバックアップが正常に作成されていることを確認します。

バックアップにフォレンジックデータが組み込まれるので、そのデータを抽出して分析できるようになります。フォレンジックデータが含まれているバックアップには、そのことを示すマークが付くので、**[バックアップストレージ]** > **[ロケーション]** で、**[フォレンジックデータのみ]** オプションを使用すれば、フィルタリングによって他のバックアップと区別して表示できます。

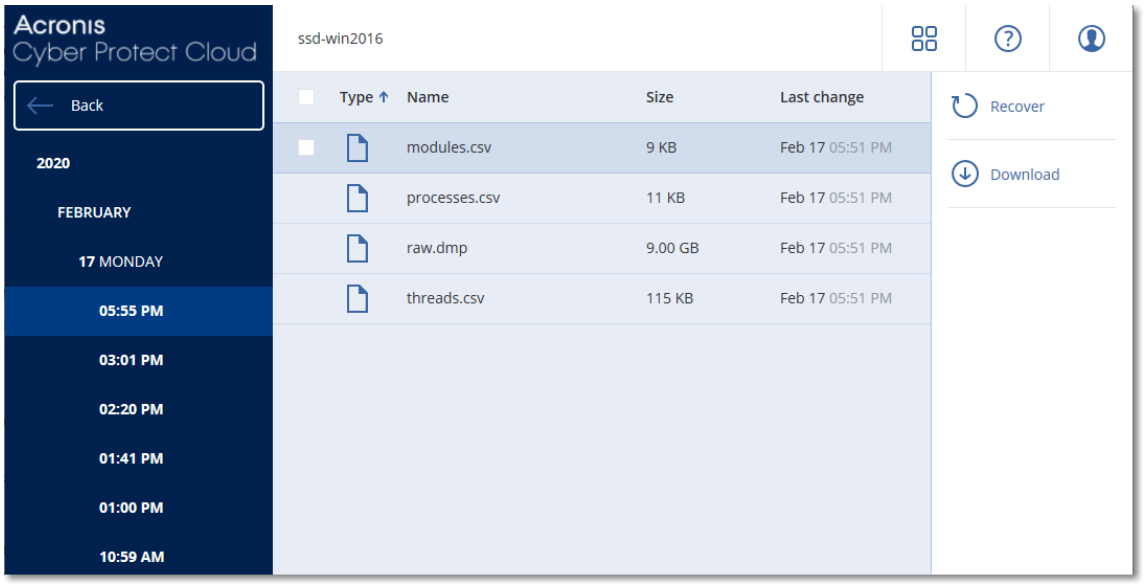
バックアップからフォレンジックデータを抽出する方法

1. Cyber Protectコンソールで **[バックアップストレージ]** に進み、フォレンジックデータが含まれているバックアップのロケーションを選択します。
2. フォレンジックデータのバックアップを選択し、**[バックアップの表示]** をクリックします。
3. フォレンジックデータのバックアップの **[復元]** をクリックします。

- フォレンジックデータだけを抽出する場合は、[**フォレンジックデータ**] をクリックします。



フォレンジックデータが含まれているフォルダが表示されます。メモリダンプファイルや他のフォレンジックファイルを選択してから、[**ダウンロード**] をクリックします。



- フォレンジックバックアップ全体を復元する場合は、[**マシン全体**] をクリックします。起動モードなしでバックアップが復元されます。その結果、ディスクが変更されていないことを確認できるようになります。

サードパーティ製のフォレンジックソフトウェアでメモリダンプを分析することも可能です。例えば、メモリを詳しく分析するためのVolatility Framework（https://www.volatilityfoundation.org/）などがあります。

フォレンジックデータが含まれているバックアップの公証

フォレンジックデータが含まれているバックアップが作成時のイメージのまま何も変更されていないということを確認するために、バックアップモジュールには、フォレンジックデータが含まれているバッ

クアップの公証の機能が用意されています。

仕組み

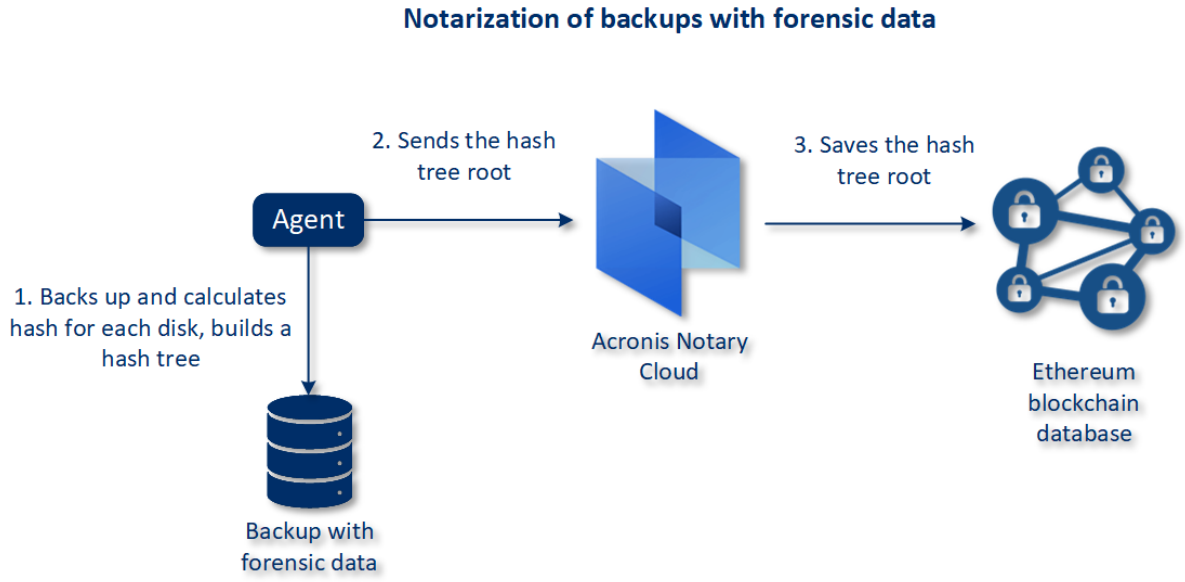
公証の機能を使用すれば、フォレンジックデータが含まれているディスクが本物で、バックアップ後に改変されていないことを証明できます。

エージェントはバックアップ時に、バックアップディスクのハッシュコードを計算し、ハッシュツリーを作成し、そのツリーをバックアップに保存し、ハッシュツリーのルートをノータリー（公証）サービスに送信します。ノータリー（公証）サービスで、ハッシュツリーのルートが Ethereum ブロックチェーンデータベースに保存され、この値が変更されていないことが確認されます。

エージェントは、フォレンジックデータが含まれているディスクが本物かどうかを確認するときにもディスクのハッシュを計算し、そのハッシュを、バックアップ内のハッシュツリーに保管されているハッシュと比較します。ハッシュが一致しないと、そのディスクは本物ではないと見なされます。一致すれば、ハッシュツリーによってそのディスクは本物だと証明されたことになります。

ハッシュツリー自身が不正なものではないことをベリファイするために、エージェントはハッシュツリーのルートをノータリー（公証）サービスに送信します。ノータリー（公証）サービスはそれをブロックチェーンデータベースに保存されているものと比較します。ハッシュが一致すると、選択したディスクが本物であることが証明されます。一致しない場合は、ディスクが本物ではないというメッセージが表示されます。

フォレンジックデータが含まれているバックアップの公証プロセスを以下に簡単にまとめます。



公証の対象になるディスクバックアップを手動で確認する場合は、そのバックアップの証明書を取得し、tibxreadツールを使用して、証明書に示されている検証手順を実行します。

フォレンジックデータが含まれているバックアップの証明書の取得

コンソールを使用して、フォレンジックデータが含まれているバックアップの証明書を取得するには、以下のようにします。

1. **[バックアップストレージ]** に進んで、フォレンジックデータが含まれているバックアップを選択します。
2. マシン全体を復元します。
3. **[ディスクマッピング]** ビューが表示されます。
4. ディスクの **[証明書の取得]** アイコンをクリックします。
5. 証明書が生成され、ブラウザの新しいウィンドウにその証明書が表示されます。証明書の下に、公証の対象になるディスクバックアップの手動確認の手順が表示されます。

バックアップデータを取得するための「tibxread」ツール

Cyber Protectionには、バックアップディスクが変更されていないことを手動で確認するために、`tibxread`というツールが用意されています。このツールを使用すると、バックアップからデータを抽出し、指定のディスクのハッシュを計算できます。このツールは、以下のコンポーネントと一緒に自動的にインストールされます。つまり、Windowsエージェント、Linuxエージェント、Macエージェントです。

インストールパスは、エージェントと同じフォルダです（`C:\Program Files\BackupClient\BackupAndRecovery`など）。

サポートされているロケーションは、以下のとおりです。

- ローカルディスク
- 資格情報なしでアクセスできるネットワークフォルダ（CIFS/SMB）です。
  パスワード保護のネットワークフォルダの場合は、OSツールを使用してローカルフォルダにネットワークフォルダをマウントしてから、そのローカルフォルダをこのツールのソースとして指定できます。
- クラウドストレージ
  URLとポートと証明書を指定する必要があります。URLとポートは、Windowsの場合はレジストリキーから、Linux/Macマシンの場合は構成ファイルから取得できます。
  Windowsの場合:

  ```
  HKEY_LOCAL_
  MACHINE\SOFTWARE\Acronis\BackupAndRecovery\Settings\OnlineBackup\FesAddressCache\Defa
  ult\<tenant_login>\FesUri
  ```

  Linuxの場合:

  ```
  /etc/Acronis/BackupAndRecovery.config
  ```

  macOSの場合:

  ```
  /Library/Application Support/Acronis/Registry/BackupAndRecovery.config
  ```

  証明書は以下のロケーションにあります。
  Windowsの場合:

  ```
  %allusersprofile%\Acronis\BackupAndRecovery\OnlineBackup\Default
  ```

Linuxの場合:

```
/var/lib/Acronis/BackupAndRecovery/OnlineBackup/Default
```

macOSの場合:

```
/Library/Application Support/Acronis/BackupAndRecovery/OnlineBackup/Default
```

このツールには以下のコマンドがあります。

- `list backups`
- `list content`
- `get content`
- `calculate hash`

list backups

バックアップの復元ポイントを表示します。

概要:

```
tibxread list backups --loc=URI --arc=BACKUP_NAME --raw
```

オプション

```
--loc=URI
--arc=BACKUP_NAME
--raw
--utc
--log=PATH
```

出力テンプレート:

```
GUID   Date   Date timestamp
----   ------ --------------
<guid> <date> <timestamp>
```

<guid> - バックアップのGUID。

<date> - バックアップの作成日。形式は「DD.MM.YYYY HH24:MM:SS」です。デフォルトではローカルタイムゾーンになります（--utcオプションを使用して変更することも可能です）。

出力例:

```
GUID   Date   Date timestamp
----   ------ --------------
516FCE73-5E5A-49EF-B673-A9EACB4093B8 18.12.2019 16:01:05 1576684865
516FCE73-5E5A-49EF-B673-A9EACB4093B9 18.12.2019 16:02:05 1576684925
```

list content

復元ポイントの内容を表示します。

概要:

```
tibxread list content --loc=URI --arc=BACKUP_NAME --password --backup=RECOVERY_POINT_ID
--raw --log=PATH
```

オプション

```
--loc=URI
--arc=BACKUP_NAME
--password
--backup=RECOVERY_POINT_ID
--raw
--log=PATH
```

出力テンプレート:

```
Disk     Size   Notarization status
-------- ------ --------------------
<number> <size> <notarization_status>
```

<number> - ディスクのID。

<size> - サイズ（バイト単位）。

<notarization_status> - 以下のステータスがあります。つまり、公証なし、公証済、次回のバックアップです。

出力例:

```
Disk     Size   Notary status
-------- ------ --------------
1        123123465798 Notarized
2        123123465798 Notarized
```

get content

復元ポイントの指定のディスクの内容を標準出力（stdout）に書き出します。

概要:

```
tibxread get content --loc=URI --arc=BACKUP_NAME --password --backup=RECOVERY_POINT_ID -
-disk=DISK_NUMBER --raw --log=PATH --progress
```

オプション

```
--loc=URI
--arc=BACKUP_NAME
--password
--backup=RECOVERY_POINT_ID
--disk=DISK_NUMBER
--raw
--log=PATH
--progress
```

calculate hash

SHA-2（256ビット）アルゴリズムを使用して復元ポイントの指定ディスクのハッシュを計算し、標準出力に書き出します。

概要:

```
tibxread calculate hash --loc=URI --arc=BACKUP_NAME --password --backup=RECOVERY_POINT_ID --disk=DISK_NUMBER --raw --log=PATH --progress
```

オプション

```
--loc=URI
--arc=BACKUP_NAME
--password
--backup=RECOVERY_POINT_ID
--disk=DISK_NUMBER
--raw
--log=PATH
```

オプションの説明

オプション	説明
--arc=BACKUP_NAME	Cyber Protectコンソールのバックアッププロパティから取得できるバックアップファイル名です。バックアップファイルは、拡張子.tibxを付けた形で指定する必要があります。
--backup=RECOVERY_POINT_ID	復元ポイントのID
--disk=DISK_NUMBER	ディスク番号（「get content」コマンドで出力される番号と同じ）
--loc=URI	バックアップロケーションのURI。「--loc」オプションの有効な形式は、以下のとおりです。 • ローカルパス名（Windows） `c:/upload/backups` • ローカルパス名（Linux）

	`/var/tmp`
	• SMB/CIFS
	`\\server\folder`
	• クラウドストレージ
	`--loc=<IP_address>:443 --cert=<path_to_certificate> [--storage_path=/1]`
	`<IP_address>` - Windowsでは、以下のレジストリキーにあります。HKEY_LOCAL_MACHINE¥SOFTWARE¥Acronis¥BackupAndRecovery¥Settings¥OnlineBackup¥FesAddressCache¥Default¥<tenant_login>¥FesUri
	`<path_to_certificate>` - Cyber Protect Cloudにアクセスするための証明書ファイルのパス。たとえばWindowsでは、この証明書は `C:\ProgramData\Acronis\BackupAndRecovery\OnlineBackup\Default\<ユーザー名>.crt` にあります。<ユーザー名> はCyber Protect Cloudにアクセスするアカウント名です。

--log=PATH	指定のPATH（ローカルパスのみ）へのログの書き込みを有効にします。形式は、`--loc=URI`パラメータと同じです。ログのレベルはDEBUGです。
--password=PASSWORD	バックアップの暗号化パスワードです。バックアップを暗号化しない場合は、値を空のままにしてください。

--raw	コマンド出力のヘッダー（最初の2行）を非表示にします。コマンド出力を解析するときに使用します。
	「`--raw`」なしの出力例:
	`GUID Date Date timestamp`
	`---- ------ --------------`
	`516FCE73-5E5A-49EF-B673-A9EACB4093B8 18.12.2019 16:01:05 1576684865`
	`516FCE73-5E5A-49EF-B673-A9EACB4093B9 18.12.2019 16:02:05 1576684925`
	「`--raw`」付きの出力:
	`516FCE73-5E5A-49EF-B673-A9EACB4093B8 18.12.2019 16:01:05 1576684865`
	`516FCE73-5E5A-49EF-B673-A9EACB4093B9 18.12.2019 16:02:05 1576684925`

--utc	日付をUTCで表示します。

--progress	操作の進行状況を表示します。
	例:
	`1%`
	`2%`
	`3%`
	`4%`
	`...`
	`100%`

ログの切り詰め

このオプションは、Microsoft SQL Serverのデータベースのバックアップや、Microsoft SQL Serverアプリケーションバックアップが有効なディスクレベルのバックアップに対して有効です。

このオプションでは、バックアップの成功後にSQL Serverのトランザクションログを切り捨てるかどうかを定義します。

デフォルト設定:**有効**。

このオプションを有効にした場合、このソフトウェアでバックアップが作成された時点にのみデータベースを復元できます。Microsoft SQL Serverのネイティブのバックアップエンジンを使用してトランザクションログをバックアップする場合は、このオプションを無効にします。復元後にはトランザクションログを適用し、任意の時点にデータベースを復元できます。

LVMのスナップショット

このオプションは、物理コンピュータに対してのみ有効です。

このオプションは、Linux論理ボリュームマネージャ（LVM）が管理しているボリュームのディスクレベルのバックアップに対して有効です。このようなボリュームは、論理ボリュームとも呼ばれます。

このオプションは、論理ボリュームのスナップショットを取得する方法を定義します。バックアップソフトウェアは、それ自体でスナップショットを取得することも、Linux論理ボリュームマネージャ（LVM）に取得させることも可能です。

デフォルト設定:**バックアップソフトウェア別**。

- **バックアップソフトウェア別**。スナップショットデータは、ほとんどの場合、RAMに格納されています。バックアップは高速に進み、ボリュームグループに未割り当ての領域は必要ありません。したがって、論理ボリュームのバックアップに問題が発生した場合にのみ事前設定を変更することをお勧めします。
- **LVM別**。スナップショットは、ボリュームグループの未割り当て領域に格納されます。未割り当て領域がない場合、スナップショットはバックアップソフトウェアが取得します。

スナップショットはバックアップ操作中のみ使用され、バックアップ操作が完了すると自動的に削除されます。一時ファイルは保存されません。

マウントポイント

このオプションは、マウントされたボリュームまたはクラスターの共有ボリュームを含むデータソースに対し、Windowsでファイルレベルのバックアップを行う場合にのみ有効です。

このオプションは、フォルダ階層内でマウント ポイントより上位にあるフォルダにバックアップする場合にのみ有効です。（マウントポイントとは、追加のボリュームが論理的に接続されるフォルダです）。

- このようなフォルダ（親フォルダ）をバックアップ対象として選択し、[**マウントポイント**] オプションをオンにすると、マウントされたボリューム上に存在するすべてのファイルが、バックアップに格

納されます。[**マウントポイント**] オプションをオフにすると、バックアップ内のマウントポイントは空になります。

親フォルダの復元中、マウントポイントの内容は、復元用の [**マウントポイント**] オプションがオンになっていれば復元され、オフになっていれば復元されません。

- マウント ポイントを直接選択するか、マウント ボリューム内の任意のフォルダを選択すると、選択したフォルダは通常のフォルダと認識されます。このフォルダは、[**マウントポイント**] オプションの状態にかかわりなくバックアップされ、復元用の [**マウントポイント**] オプションの状態にかかわりなく復元されます。

デフォルト設定:**無効**。

注意
ファイルレベルのバックアップを使用して、目的のファイルまたはボリューム全体をバックアップすることで、クラスターの共有ボリュームに存在するHyper-V仮想マシンをバックアップできます。仮想コンピュータを整合性のある状態でバックアップするため、仮想コンピュータの電源をオフにしてください。

例

C:¥Data1¥フォルダが、マウントされたボリュームのマウントポイントであると仮定します。ボリュームには、フォルダ**Folder1**と**Folder2**が格納されています。データに対してファイルレベルのバックアップを行う保護計画を作成します。

ボリュームCのチェックボックスを選択して、[**マウントポイント**] オプションを有効にすると、バックアップ内の**C:¥Data1¥**フォルダに**Folder1**と**Folder2**が格納されます。バックアップデータを復元する際には、復元用の [**マウントポイント**] オプションを正しく使用するように注意してください。

ボリュームCのチェックボックスをオンにして、[**マウントポイント**] オプションをオフにすると、バックアップ内の**C:¥Data1¥**フォルダは空になります。

Data1、**Folder1**、または**Folder2**フォルダのチェックボックスをオンにすると、オンにしたフォルダが、[**マウントポイント**] オプションの状態にかかわりなくバックアップ内に通常のフォルダとして格納されます。

マルチボリュームスナップショット

このオプションは、Windows または Linux が実行されている物理マシンのバックアップで有効です。

このオプションは、ディスクレベルのバックアップで使用できます。スナップショットを取得することでファイルレベルバックアップが実行された場合には、ファイルレベルバックアップでも使用できます。（[ファイルレベルバックアップのスナップショット] オプションによって、ファイルレベルのバックアップの最中にスナップショットが取得されるかどうかが決定します）。

このオプションでは、複数のボリュームのスナップショットを同時に取得するか、1つずつ取得するかを指定します。

デフォルト設定:

- Windows が実行されているマシンがバックアップ対象として少なくとも 1 つ選択されている場合:**有効**。
- それ以外の場合:**無効**。

このオプションを有効にした場合、バックアップされるすべてのボリュームのスナップショットが同時に取得されます。このオプションを使用すると、Oracleデータベースなどの複数のボリュームにまたがるデータについて、時間的に整合性がとれたバックアップを作成できます。

このオプションを無効にした場合、ボリュームのスナップショットが1つずつ取得されます。その結果、データが複数のボリュームにまたがる場合、作成されるバックアップの整合性が失われる可能性があります。

ワンクリック復元

注意
この機能は、Advanced Backupパックで利用可能です。

ワンクリック復元を使用すると、WindowsまたはLinuxマシンのディスクバックアップを自動的に復元することができます。このバックアップは、マシン全体のバックアップでも、マシン上の特定のディスクやボリュームのバックアップでもかまいません。

ワンクリック復元は、次の操作をサポートしています:

- 最新のバックアップからの自動復元
- バックアップアーカイブ内の特定のバックアップ（別名、復元ポイント）からの復元

ワンクリック復元は、次のバックアップストレージをサポートしています:

- Secure Zone
- ローカルフォルダ
- ネットワークフォルダ
- クラウドストレージ

重要
以下の操作を行った場合、マシンの次の再起動までBitlockerによる暗号化を一時的に停止します。

- Secure Zoneの作成、変更、削除。
- Startup Recovery Managerの有効化および無効化。
- （Startup Recovery Managerが有効になっていない場合のみ）保護計画でワンクリック復元を有効にした後、初回のバックアップを実行します。この操作により、Startup Recovery Managerが自動的に有効化されます。
- Startup Recovery Managerのアップデート（プロテクションのアップデートなど）。

これらの操作中にBitLocker暗号化が停止されなかった場合は、マシンを再起動した後にBitLockerピンを指定する必要があります。

ワンクリック復元の有効化

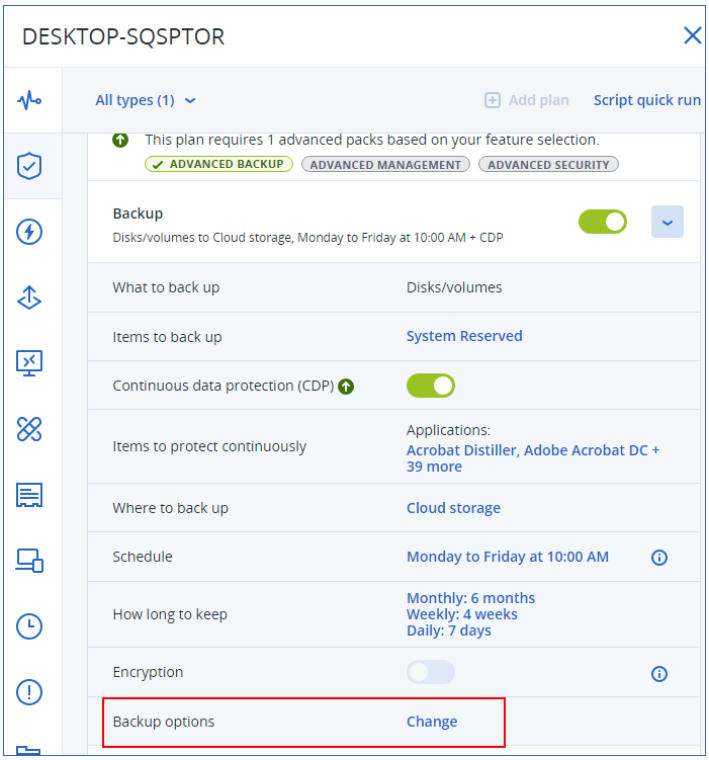
ワンクリック復元は保護計画のバックアップオプションです。計画の作成方法の詳細については、「"保護計画の作成"（209ページ）」を参照してください。

注意

ワンクリックバックアップを有効にすると、ターゲットマシンでStartup Recovery Managerも有効になります。Startup Recovery Managerを有効にできない場合、ワンクリック復元バックアップを作成するバックアップ操作は失敗します。Startup Recovery Managerの詳細については、「"Startup Recovery Manager"（711ページ）」を参照してください。

ワンクリック復元を有効にするには

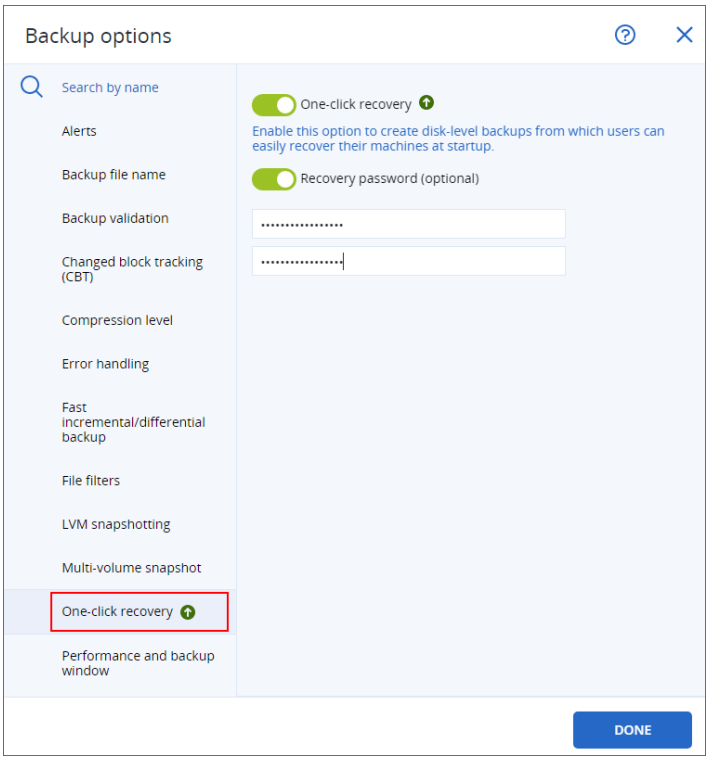
1. 保護計画で、**バックアップ**モジュールを展開します。
2. **[バックアップの対象]** で **[マシン全体]** または **[ディスク/ボリューム]** を選択します。
3. （**[ディスク/ボリューム]** を選択した場合）**[バックアップする項目]** で、バックアップの対象となるディスクまたはボリュームを選択します。
4. **[バックアップオプション]** で **[変更]** をクリックし、**[ワンクリック復元]** を選択します。



5. **[ワンクリック復元]** スイッチを有効にします。
6. （オプション）**[パスワードを復元]** スイッチを有効にしてパスワードを指定します。

重要

復元パスワードを指定することを強くお勧めします。ターゲットマシンでワンクリック復元を実行するユーザーがこのパスワードを知っているかどうかを確認します。



7. **[完了]** をクリックします。
8. 必要に応じて保護計画の他の要素を構成し、計画を保存します。

これで、保護計画が実行されバックアップが作成された後、保護されているマシンのユーザーがワンクリック復元を利用できるようになります。

重要
プロテクションエージェントをアップデートすると、ワンクリック復元が一時的に使用できなくなります。ワンクリック復元を再度有効にするには、バックアップを実行します。バックアップが完了すると、再びワンクリック復元は使用できるようになります。

ワンクリック復元の無効化

次の方法で特定の復元のワークロードのワンクリック復元を無効化できます。

- ワークロードに適用されている保護計画の **[ワンクリック復元]** オプションを無効にします。
- **[ワンクリック復元]**オプションが有効になっている保護計画を取り消します。
- **[ワンクリック復元]**オプションが有効になっている保護計画を削除します。

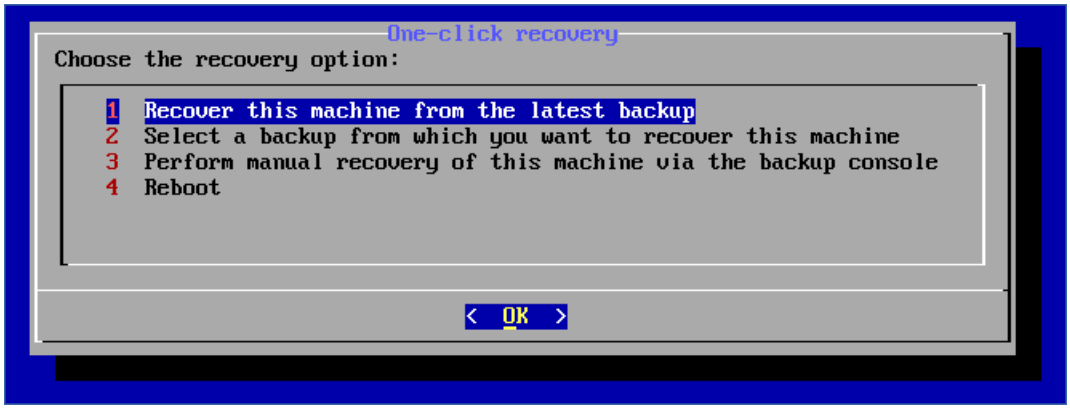
ワンクリック復元でマシンをリカバリする

前提条件

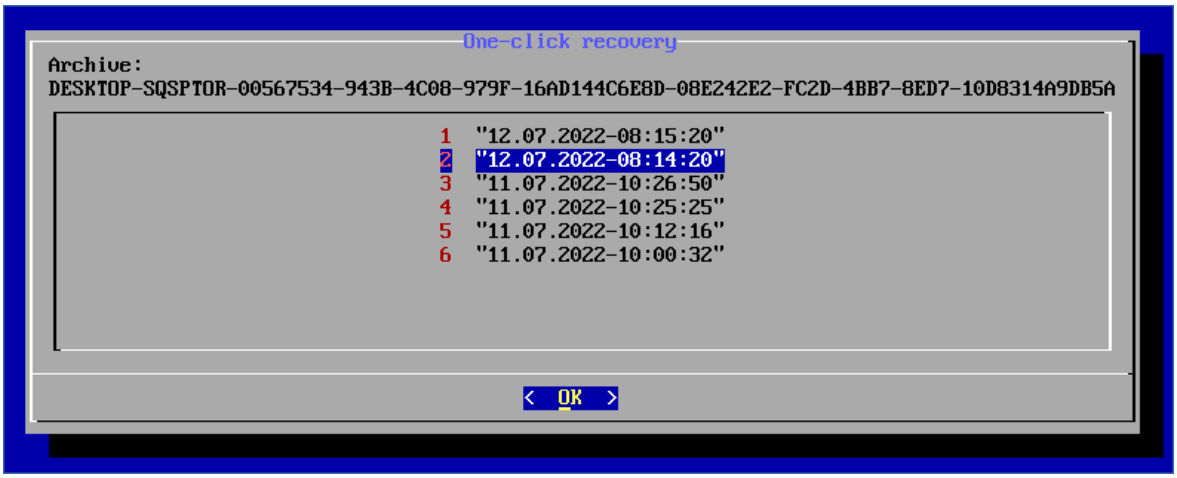
- **[ワンクリック復元]** バックアップオプションが有効化されている保護計画が、マシンに適用されます。
- このマシンについて、少なくとも1つのディスクバックアップが存在します。

マシンをリカバリするには

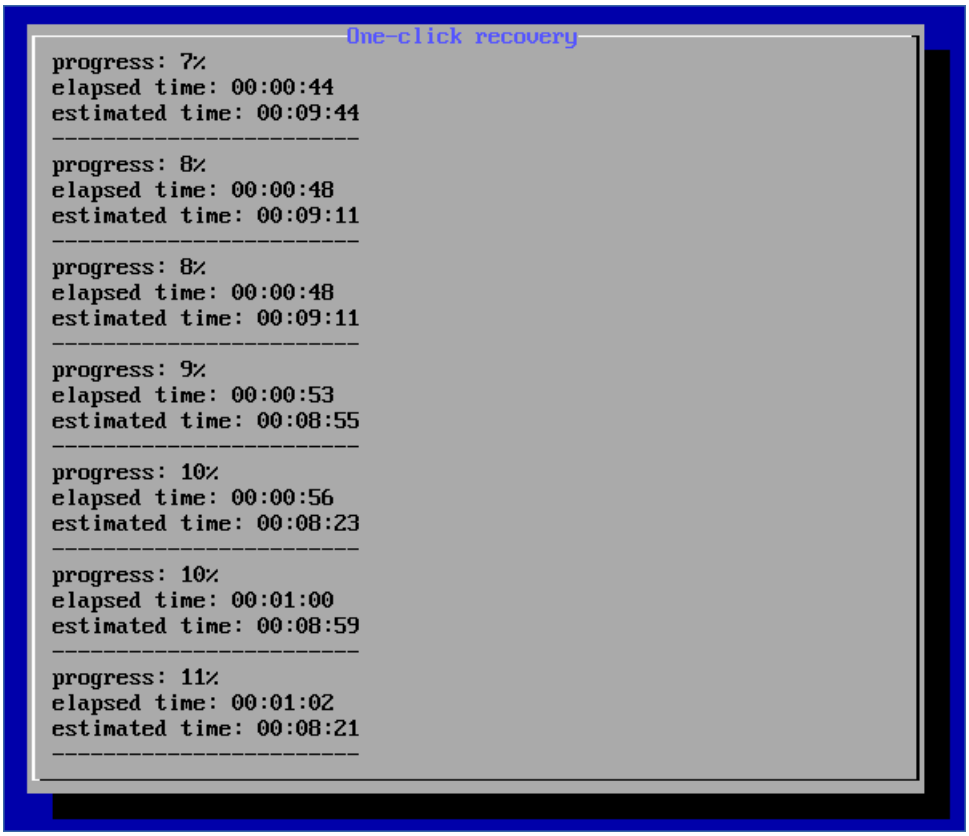
1. リカバリするマシンを再起動します。
2. 再起動中にF11キーを押して、Startup Recovery Managerを入力します。
   レスキューメディアウィンドウが開きます。
3. **Acronis Cyber Protect**を選択します。
4. （保護計画で復元パスワードが指定されている場合）復元パスワードを入力し、**[OK]** をクリックします。
5. ワンクリック復元オプションを選択します。
   - 最新のバックアップを自動的にリカバリするには、最初のオプションを選択してから、**[OK]** をクリックします。
   - バックアップアーカイブ内の別のバックアップをリカバリするには、2番目のオプションを選択してから、**[OK]** をクリックします。



6. **[はい]** をクリックしてこの選択内容を確認します。
   レスキューメディアウィンドウが開き、その後非表示になります。インターフェースは表示されませんが、復元処理は続行されます。
7. （指定したバックアップの復元を選択した場合）復元するバックアップを選択してから、**[OK]** をクリックします。



しばらくすると、復元が開始し、進捗状況が表示されます。復元が完了すると、マシンが再起動します。



パフォーマンスとバックアップウィンドウ

このオプションは、一週間における毎時のバックアップ作成速度（高、低、禁止）について3レベルのうちの1つの設定を有効にします。このようにして、バックアップの開始と実行を許可する時間ウィンドウを定義できます。プロセスの優先度と出力速度に関して高および低パフォーマンスレベルが設定できます。

このオプションは、Webサイトバックアップやクラウド復元サイトのサーバーバックアップなどの、クラウドエージェントが実行するバックアップの際には使用できません。

このオプションは、バックアップとバックアップのレプリケーション処理でのみ有効です。バックアップ後のコマンドと保護計画に含まれるその他の操作（ベリファイなど）は、このオプションに関係なく実行されます。

デフォルト設定:**無効**。

このオプションが無効の場合、事前設定値に対してパラメーターが変更されても、バックアップは以下のパラメーターでいつでも実行できます。

- CPUの優先度: **低** （Windowsでは **[通常以下]** に相当）
- 出力速度:**無制限**

このオプションが有効である場合、現在の時間に指定されたパフォーマンスパラメーターに応じてスケジュールバックアップが許可またはブロックされます。バックアップがブロックされる時間の最初の時点でバックアップ処理が自動的に停止し、アラートが生成されます。スケジュール済みバックアップが

ブロックされても、バックアップは手動で開始できます。最後にバックアップが許可された時間のパフォーマンスパラメーターが使用されます。

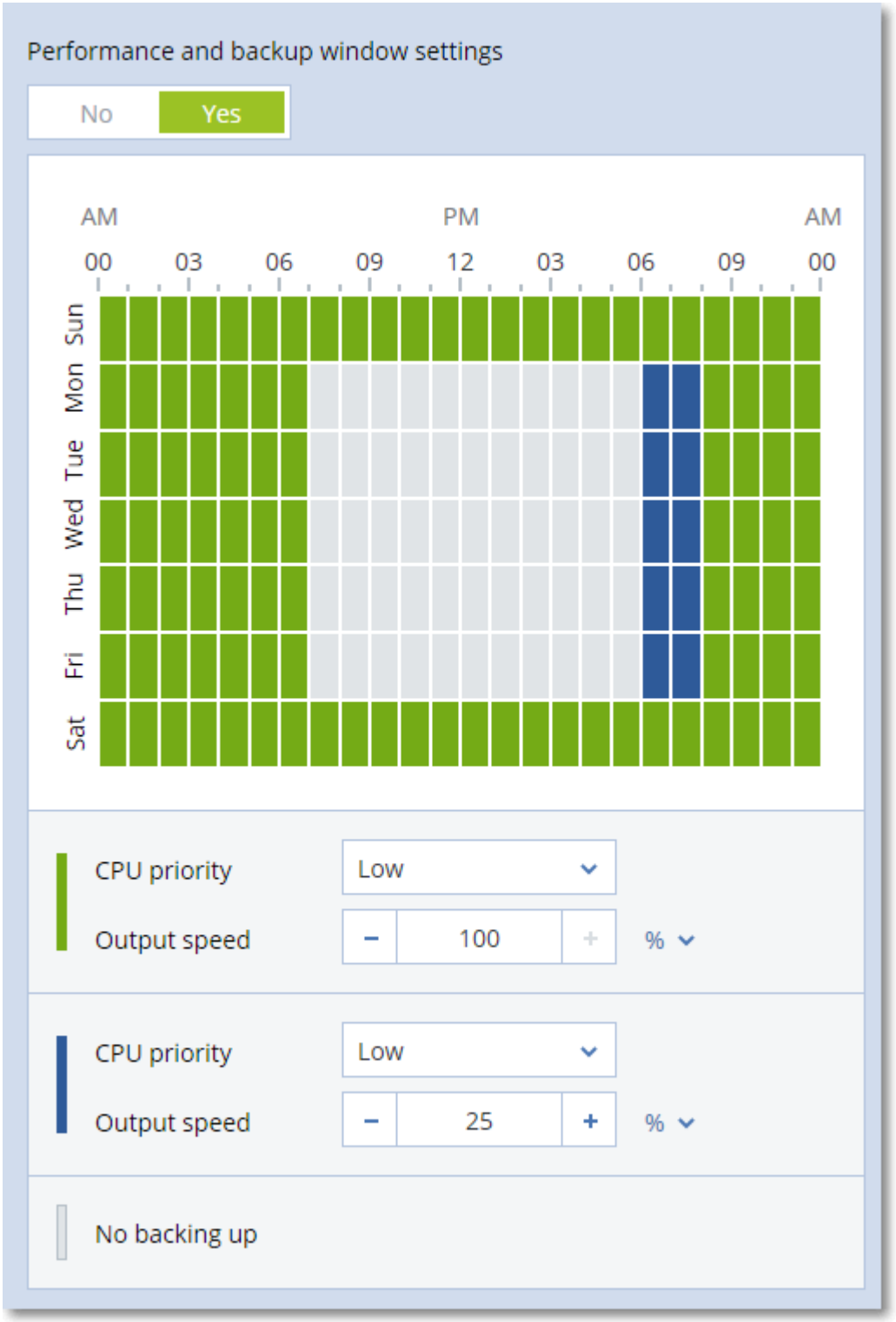
注意
レプリケーションロケーションごとに、パフォーマンスとバックアップの時間帯を個別に設定できます。レプリケーションロケーションの設定にアクセスするには、保護計画でロケーション名の横にあるギアアイコンをクリックし、[**パフォーマンスとバックアップウィンドウ**] をクリックします。

バックアップウィンドウ

各四角は平日における1時間を表しています。四角をクリックし、以下の状態を循環させます。

- **緑:** 以下の緑色セクションで指定したパラメーターに従ってバックアップを許可します。
- **青:** 以下の青色セクションで指定したパラメーターに従ってバックアップを許可します。
  バックアップ形式が [**バージョン11**] に設定されている場合、この状態は選択できません。
- **灰色:** バックアップはブロックされます。

クリックおよびドラッグにより複数の四角の状態を同時に変更できます。



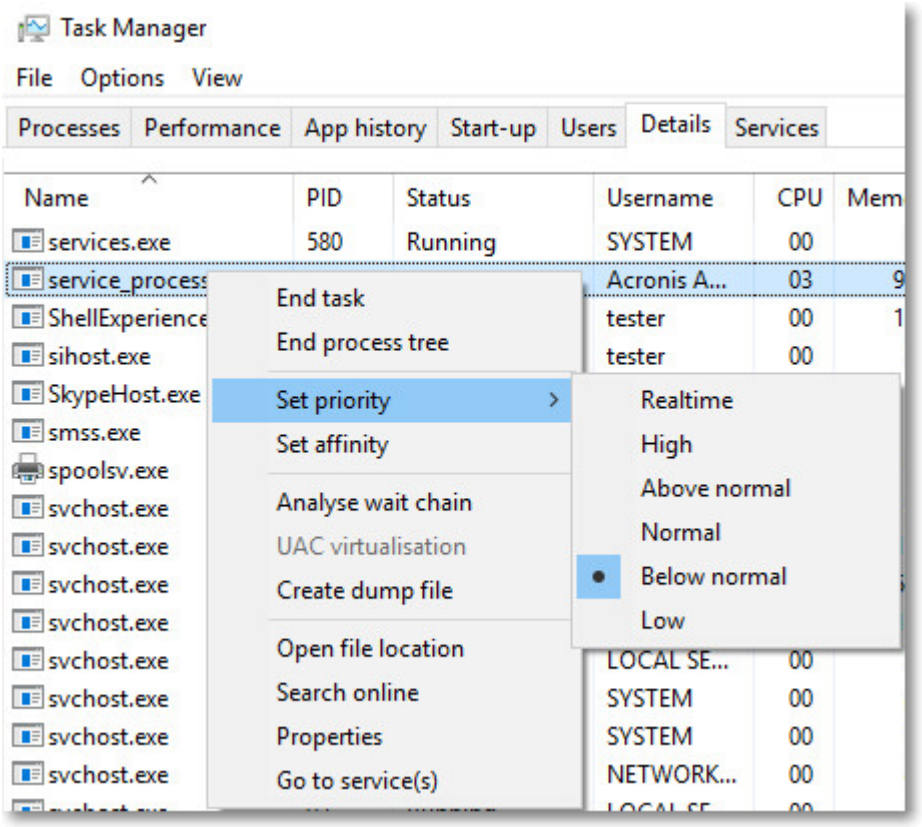
CPUの優先度

このパラメーターでは、オペレーティングシステム内のバックアッププロセスの優先度を定義します。

選択可能な設定は次のとおりです。**[低]**、**[通常]**、**[高]**。

システムで実行されるプロセスの優先度によって、そのプロセスに割り当てられるCPUやシステムのリソース量が決まります。バックアップの優先度を下げると、他のアプリケーションのためのリソースを増やすことができます。バックアップの優先度を上げると、バックアップ アプリケーションに割り当てる CPU などのリソースを増やすようにオペレーティング システムに要求することによって、バックアップの処理速度が上がる場合があります。ただし、その効果は、全体的な CPU の使用率およびディスク入出力速度、ネットワーク トラフィックなどのその他の要素に依存します。

このオプションを使用して、Windows ではバックアッププロセスの優先度（**service_process.exe**）、Linux や macOS ではバックアッププロセスの nice 値（**service_process**）を設定します。



Windows、Linux、macOSにおけるこの設定のマッピングを以下の表に示します。

Cyber Protection優先度	Windows の優先度	WindowsおよびmacOS のnice値
低	通常より下	10
通常	通常	0
高	高	-10

バックアップ中の出力速度

このパラメーターでは、ハードドライブの書き込み速度（ローカルフォルダにバックアップする場合）またはネットワークを介したバックアップデータの転送速度（ネットワーク共有またはクラウドスト

レージにバックアップする場合）を制限できます。

このオプションを有効にした場合、許容される最大出力速度を指定できます。

- 目的のハードディスクの推定書き込み速度（ローカルフォルダにバックアップする場合）、またはネットワーク接続を介した推定最高速度（ネットワーク共有またはクラウドストレージにバックアップする場合）の割合として指定します。
  この設定は、エージェントが Windows で実行されている場合のみ機能します。
- KB/秒単位（すべてのターゲットに対して）。

物理データ配送

このオプションは、バックアップ先またはレプリケーション先がクラウドストレージで、バックアップ形式が **[バージョン12]** に設定されている場合に利用できます。

このオプションは、Windowsエージェント、Linuxエージェント、Macエージェント、VMwareエージェント、Hyper-Vエージェント、およびVirtuozzoエージェントによって作成されるディスクレベルバックアップとファイルバックアップで有効です。

物理データ配送サービスを使用して、保護計画によって作成される最初の完全バックアップをハードディスクドライブ上のクラウドストレージに送信する場合は、このオプションを使用します。以降の増分バックアップは、ネットワーク経由で実行できます。

クラウドにレプリカが作成されるローカルバックアップの場合、最初のバックアップがクラウドストレージにアップロードされるまでの間、増分バックアップが継続的にローカルに保存されます。その後、クラウドにすべての増分変更のレプリカが作成され、バックアップスケジュールに従ってレプリケーションが継続されます。

デフォルト設定:**無効**です。

物理データ配送サービスについて

物理データ配送サービスのWebインターフェースは、管理者のみが使用できます。

物理データ配送サービスと注文作成ツールの使用方法の詳しい手順については、『物理データ配送管理者ガイド』を参照してください。物理データ配送サービスのWebインターフェースでこの文書にアクセスするには、[?]アイコンをクリックします。

物理データ配送プロセスの概要

1. （クラウドストレージをプライマリのバックアップロケーションにしているバックアップを配送するには）
   a. クラウドへのバックアップを伴う新しい保護計画を作成します。
   b. **[バックアップオプション]** 行で、**[変更]** をクリックします。
   c. 使用可能なオプションのリストで、**[物理データ配送]** をクリックします。
   リムーバブルドライブに直接バックアップするか、ローカルフォルダまたはネットワークフォルダにバックアップして、そのバックアップをドライブにコピー/移動することができます。

2. （クラウドにレプリカが作成されたローカルバックアップを配送するには）

   注意
   このオプションは、プロテクションエージェントのバージョンがC21.06以降の場合にサポートされます。

   a. ローカルまたはネットワークストレージへのバックアップを伴う新しい保護計画を作成します。
   b. **[ロケーションの追加]** をクリックして、**[クラウドストレージ]** を選択します。
   c. **[クラウドストレージ]** ロケーション行で、ギアアイコンをクリックして **[物理データ配送]** を選択します。
3. **[物理データ配送を使用]** 以下で、**[はい]** と **[完了]** をクリックします。
   配送されるバックアップはすべて暗号化が必須であるため、保護計画では暗号化オプションが自動的に有効になります。
4. **[暗号化]** 行で **[パスワードの指定]** をクリックし、暗号化のパスワードを入力します。
5. **[物理データ配送]** 行で、初期バックアップを保存するリムーバブルドライブを選択します。
6. **[作成]** をクリックして、保護計画を保存します。
7. 最初のバックアップが完了した後に、物理データ配送サービスのWebインターフェースを使用して注文作成ツールをダウンロードし、注文を作成します。
   このWebインターフェイスにアクセスするには、管理ポータルにログインし、**[概要]** > **[使用状況]**をクリックして、**[物理データ配送]** の **[サービスの管理]** をクリックします。

   重要
   最初の完全バックアップが完了したら、以降のバックアップは同じ保護計画で実行する必要があります。別の保護計画では、同じパラメータを使用して同じマシンに対して行うものであっても、別の物理データ配送サイクルが必要になります。

8. ドライブを梱包してデータセンターに配送します。

   重要
   『物理データ配送管理者ガイド』で説明するパッケージング手順に必ず従ってください。

9. 物理データ配送サービスのWebインターフェースを使用して注文ステータスを追跡します。以降のバックアップは、最初のバックアップがクラウドストレージにアップロードされるまでは失敗するため注意してください。

処理の前後のコマンド

このオプションによって、バックアップ処理の前後に自動的に実行されるコマンドを定義できます。

次の図に、バックアップ処理の前後に実行するコマンドが実行されるタイミングを示します。

バックアップ前に実行するコマンド	バックアップ	バックアップ後に実行するコマンド

バックアップ処理の前後に実行するコマンドを使用する方法の例:

- バックアップを開始する前に、ディスクから一時ファイルを削除する
- バックアップを開始する前に、毎回サードパーティのアンチウィルス製品を実行するように設定する。
- 別のロケーションにバックアップを選択的にコピーする。このオプションは便利です。保護計画で設定したレプリケーションによってすべてのバックアップが後続のロケーションにコピーされるからです。

エージェントは、バックアップ後のコマンドを実行した後にレプリケーションを実行します。

「pause」などのユーザーの入力を必要とするような対話型のコマンドはサポートされません。

バックアップ前に実行するコマンド

バックアップ処理を開始する前に実行するコマンド/バッチ ファイルを指定する手順は、次のとおりです。

1. **[バックアップ前にコマンドを実行]** スイッチを有効にします。
2. **[コマンド...]** フィールドにコマンドを入力するか、バッチファイルを参照します。「pause」などのユーザーの入力を必要とするような対話型のコマンドはサポートされません。
3. **[作業ディレクトリ]** フィールドで、コマンド/バッチファイルを実行するディレクトリのパスを指定します。
4. **[引数]** フィールドで、必要に応じて、コマンドを実行する際の引数を指定します。
5. 処理内容に応じて、次の表で説明するオプションから、適切なオプションを選択します。
6. **[完了]** をクリックします。

チェックボックス	**選択内容**			
[コマンドの実行に失敗した場合、バックアップを失敗させる]*	オン	オフ	オン	オフ
[コマンドの実行が完了するまでバックアップを行わない]	オン	オン	オフ	オフ
結果				
	[事前設定] コマンドが正常に実行された後にのみバックアップを実行します。コマンドの実行に失敗した場合、バックアップを失敗させます。	コマンドの実行の失敗または成功にかかわらず、コマンドの実行後にバックアップを実行します。	なし	コマンドの実行結果にかかわらず、コマンドの実行と並行してバックアップを実行します。

* 終了コードがゼロでない場合、コマンドは失敗したと認識されます。

注意

Linuxで必要なライブラリバージョンに関連する競合が原因でスクリプトが失敗した場合は、スクリプトに次の行を追加することにより、LD_LIBRARY_PATHおよびLD_PRELOAD環境変数を除外します。

```
#!/bin/sh
unset LD_LIBRARY_PATH
unset LD_PRELOAD
```

バックアップ後に実行するコマンド

バックアップの完了後に実行するコマンド/実行可能ファイルを指定する手順は、次のとおりです。

1. **[バックアップ後にコマンドを実行する]** スイッチを有効にします。
2. **[コマンド...]** フィールドにコマンドを入力するか、バッチファイルを参照します。
3. **[作業ディレクトリ]** フィールドで、コマンド/バッチファイルを実行するディレクトリのパスを指定します。
4. **[引数]** フィールドで、必要に応じて、コマンドを実行する際の引数を指定します。
5. コマンドが正常に実行されることが重要な場合、**[コマンドの実行に失敗した場合、バックアップを失敗させる]** チェックボックスをオンにします。終了コードがゼロでない場合、コマンドは失敗したと認識されます。コマンドの実行に失敗した場合、バックアップのステータスは **[エラー]** として設定されます。

   このチェックボックスがオフになっていると、コマンドの実行結果はバックアップの失敗または成功に影響しません。コマンドの実行結果は、**[アクティビティ]** タブを確認するとトラックできます。
6. **[完了]** をクリックします。

データ取り込みの前後に実行するコマンド

このオプションによって、データ取り込み（つまり、データのスナップショット作成）の前後に自動的に実行されるコマンドを定義できます。データ取り込みは、バックアップ手順の開始時に実行されます。

次の図に、データキャプチャ前後のコマンドが実行されるタイミングを示します。

	<---------- **バックアップ** ---------->				
バックアップ前に実行するコマンド	データ取り込みの前に実行するコマンド	データ取り込み	データ取り込みの後に実行するコマンド	バックアップセットにデータを書き込む	バックアップ後に実行するコマンド

他のバックアップオプションとのインタラクション

データキャプチャ前後のコマンドの実行は、他のバックアップオプションによって変更できます。

[マルチボリュームスナップショット] オプションが有効になっている場合、すべてのボリュームのスナップショットが同時に作成されるため、データキャプチャ前後のコマンドは1回だけ実行されます。

[マルチボリュームスナップショット] オプションが無効になっている場合、スナップショットはボリュームごとに順番に作成されるため、バックアップされるすべてのボリュームに対してデータキャプチャ前後のコマンドが実行されます。

[ボリュームシャドウコピーサービス（VSS）] オプションが有効になっている場合、データキャプチャ前後のコマンドとMicrosoft VSSアクションは次のように実行されます。

データキャプチャ前のコマンド > [VSSサスペンド] > [データキャプチャ] > [VSSレジューム] > データキャプチャ後のコマンド

データ取り込みの前後に実行するコマンドを使用すると、VSSと互換性のないデータベースまたはアプリケーションの停止と再開を行うことができます。データ取り込みは数秒で終わるため、データベースまたはアプリケーションのアイドル時間は最小となります。

データ取り込みの前に実行するコマンド

データ取り込みの前に実行するコマンド/バッチ ファイルを指定する手順は、次のとおりです。

1. **[データキャプチャ前にコマンドを実行]** スイッチを有効にします。
2. **[コマンド...]** フィールドにコマンドを入力するか、バッチファイルを参照します。「pause」などのユーザーの入力を必要とするような対話型のコマンドはサポートされません。
3. **[作業ディレクトリ]** フィールドで、コマンド/バッチファイルを実行するディレクトリのパスを指定します。
4. **[引数]** フィールドで、必要に応じて、コマンドを実行する際の引数を指定します。
5. 処理内容に応じて、次の表で説明するオプションから、適切なオプションを選択します。
6. **[完了]** をクリックします。

チェックボックス	**選択内容**			
[コマンドの実行に失敗した場合、バックアップを失敗させる]*	オン	オフ	オン	オフ
[コマンドの実行が完了するまでデータキャプチャを実行しない]	オン	オン	オフ	オフ
結果				
	[事前設定] コマンドが正常に実行された場合にのみデータ取り込みを実行します。コマンドの実行に失敗した場	コマンドの実行の失敗または成功にかかわらず、コマンドの実行後にデータ取り込みを実行します。	なし	コマンドの実行結果にかかわらず、コマンドの実行と並行してデータ取り込みを実行します。

	合、バックアップを失敗させます。			

* 終了コードがゼロでない場合、コマンドは失敗したと認識されます。

注意
Linuxで必要なライブラリバージョンに関連する競合が原因でスクリプトが失敗した場合は、スクリプトに次の行を追加することにより、LD_LIBRARY_PATHおよびLD_PRELOAD環境変数を除外します。

```
#!/bin/sh
unset LD_LIBRARY_PATH
unset LD_PRELOAD
```

データ取り込みの後に実行するコマンド

データ取り込みの後に実行するコマンド/バッチ ファイルを指定する手順は、次のとおりです。

1. **[データキャプチャ後にコマンドを実行]** スイッチを有効にします。
2. **[コマンド...]** フィールドにコマンドを入力するか、バッチファイルを参照します。「pause」などのユーザーの入力を必要とするような対話型のコマンドはサポートされません。
3. **[作業ディレクトリ]** フィールドで、コマンド/バッチファイルを実行するディレクトリのパスを指定します。
4. **[引数]** フィールドで、必要に応じて、コマンドを実行する際の引数を指定します。
5. 処理内容に応じて、次の表で説明するオプションから、適切なオプションを選択します。
6. **[完了]** をクリックします。

チェックボックス	**選択内容**			
[コマンドの実行に失敗した場合、バックアップを失敗させる]*	オン	オフ	オン	オフ
[コマンドの実行が完了するまでバックアップを行わない]	オン	オン	オフ	オフ
結果				
	[事前設定] コマンドが正常に実行された場合にのみバックアップを続行します。	コマンドの実行の失敗または成功にかかわらず、コマンドの実行後にバックアップを続行します。	なし	コマンドの実行結果にかかわらず、コマンドの実行と並行してバックアップを続行します。

* 終了コードがゼロでない場合、コマンドは失敗したと認識されます。

スケジューリング

このオプションでは、バックアップをスケジュールどおり開始するか、遅延させるか、同時にバックアップする仮想マシンは何台かを定義します。

バックアップスケジュールの構成方法については、"スケジュールでバックアップを実行する"（408ページ）を参照してください。

デフォルト設定:**設定した時間枠内でバックアップ開始時間を分散する。最大遅延時間:30分。**

次のいずれかを選択できます。

- **すべてのバックアップを正確にスケジュールどおりに開始する**
  物理コンピュータのバックアップがスケジュールどおりに開始されます。仮想コンピュータは順次バックアップされます。
- **開始時間を時間枠内で割り振る**
  物理コンピュータのバックアップがスケジュールされた時間から遅延させて開始されます。各コンピュータの遅延値はランダムに選択され、ゼロから指定した最大値の範囲になります。複数のコンピュータをネットワーク ロケーションにバックアップするときに、過剰なネットワーク負荷を避けるためにこの設定を使用できます。各マシンの遅延値は、保護計画がマシンに適用されるときに決定され、保護計画を編集して最大遅延値を変更するまで同じ値が維持されます。
  仮想コンピュータは順次バックアップされます。
- **同時に実行するバックアップの数を制限する基準**
  ハイパーバイザーレベルでバックアップされる仮想マシンの並列バックアップを管理するにはこのオプションを使用します（エージェントレスバックアップ）。
  このオプションが選択されている保護計画は、同じエージェントで処理される他の保護計画と同時に実行できます。このオプションを選択する場合は、計画ごとに並列バックアップの数を指定する必要があります。いずれの計画でも、同時にバックアップできるマシンの総数は、エージェントごとに10台までです。デフォルトの制限を変更する方法については、"同時にバックアップされる仮想マシンの合計数の制限"（684ページ）を参照してください。
  このオプションが選択されていない保護計画の場合、仮想マシンのバックアップ操作は、1台ごとに連続で実行されます。

セクタ単位のバックアップ

このオプションは、ディスクレベルのバックアップのみで有効です。

このオプションでは、ディスクまたはボリュームの物理レベルでの厳密なコピーを作成するかどうかを定義します。

デフォルト設定:**無効。**

このオプションを有効にした場合、未割り当て領域やデータのないセクタも含め、ディスクまたはボリュームのすべてのセクタがバックアップされます。生成されるバックアップのサイズはバックアップされるディスクと同じになります（[圧縮レベル] オプションが **[なし]** に設定されている場合）。認識さ

れないファイル システムやサポートされていないファイル システムでドライブをバックアップする際は、ソフトウェアが自動的にセクタ単位のモードに切り替えられます。

注意
セクタ単位モードで作成されたバックアップから、アプリケーションデータの復元を実行することはできません。

分割

このオプションで大きいバックアップファイルをより小さなファイルに分割する方法を選択できます。

注意
クラウドストレージをバックアップロケーションとして利用する保護計画では、スプリッティングは利用できません。

デフォルト設定:

- バックアップロケーションがローカルまたはネットワーク（SMB）フォルダであり、バックアップ形式がバージョン12である場合。**固定サイズ - 200GB**
  この設定により、ファイルのフラグメンテーションによる悪影響を受けることなく、バックアップソフトウェアがNTFSファイルシステム上の大きなボリュームのデータを扱うことができます。
- それ以外の場合:**自動**

次の設定を使用できます。

- **自動**
  ファイルシステムでサポートされたファイルの最大サイズを上回ると、バックアップファイルは分割されます。
- **固定サイズ**
  ファイル サイズを入力するか、ドロップダウン リストから選択します。

タスク失敗時の処理

このオプションでは、スケジュール管理された保護計画の実行が失敗した場合、またはバックアップの実行中にマシンが再起動した場合のプログラムの動作を指定します。保護計画を手動で開始すると、このオプションは無効になります。

このオプションを有効にすると、プログラムによって保護計画が再実行されます。試行回数および試行間隔を指定できます。プログラムの試行は、その試行が正常に終了するか、指定された回数の試行が行われたときのいずれか早い段階で終了します。

このオプションが有効になっていると、バックアップの実行中にマシンが再起動されても、バックアップ操作は失敗しません。再起動後から数分後にバックアップ操作が自動的に続行され、欠落していたデータを含むバックアップファイルが完成します。このユースケースでは、**[試行間隔]** オプションは関係ありません。

デフォルト設定:**有効**。

注意
このオプションは、フォレンジックバックアップでは効力を持ちません。

タスクの開始条件

このオプションは、Windows および Linux オペレーティング システムで有効です。

このオプションでは、タスクの開始時（スケジュールされた時刻になるか、またはスケジュールで設定したイベントが発生した場合）に1つ以上の条件が満たされていない場合の動作を指定します。条件の詳細については、"開始条件"（415ページ）を参照してください。

デフォルト設定:**スケジュール設定の条件が満たされるまで待機する**

スケジュール設定の条件が満たされるまで待機する

この設定では、スケジューラは条件の監視を開始し、条件が満たされると直ちにタスクを起動します。条件が満たされない場合、タスクは起動されません。

条件が長期間満たされず、タスクがさらに遅れる危険性が高まっている場合に、条件にかかわらずタスクを実行するまでの間隔を設定できます。［**次の時間が経過するとタスクを実行する**］チェックボックスをオンにし、間隔を指定します。条件が満たされるか、最大遅延時間が経過すると、タスクが起動されます。

タスクの実行をスキップする

指定した時間ちょうどにタスクを実行する必要がある場合など、タスクの遅延を容認できない場合もあります。特に、比較的頻繁にタスクが発生するような場合は、条件が満たされるのを待つのではなく、タスクをスキップする方が合理的です。

ボリューム シャドウ コピー サービス（VSS）

このオプションは、Windowsオペレーティングシステムにのみ適用されます。

このオプションでは、1つまたは複数のボリュームシャドウコピーサービス（VSS）ライターが正常に動作しない場合にバックアップを成功させることができるか、また、VSS対応アプリケーションに対し、どのプロバイダーからバックアップの開始が通知されるかを定義します。

ボリュームシャドウコピーサービス（VSS）により、バックアップソフトウェアがデータスナップショットを取得する時点において、特にすべてのデータベーストランザクションの完了など、アプリケーションが使用するすべてのデータについて一貫性のある状態を維持できます。データの整合性を維持することにより、アプリケーションは正しい状態に復元され、復元直後から動作可能になります。

スナップショットはバックアップ操作中のみ使用され、バックアップ操作が完了すると自動的に削除されます。一時ファイルは保存されません。

さらにデータキャプチャの前後に実行するコマンドを使用することで、一貫性のある状態でデータをバックアップできます。例えば、データキャプチャ前にデータベースを一時停止し、すべてのキャッシュをフラッシュしてすべてのトランザクションが完了することを確認するためのコマンドを指定し、

さらにスナップショットが作成された後にデータベース操作を再開するためのデータキャプチャ後のコマンドを指定することができます。

注意
HKEY_LOCAL_MACHINE¥SYSTEM¥CurrentControlSet¥Control¥BackupRestore¥FilesNotToSnapshotレジストリキーに指定されているファイルとフォルダは、バックアップされません。特に、オフラインのOutlookデータファイル（.ost）は、このキーの**OutlookOST**値で指定されているため、バックアップされません。

正常に動作しないVSSライターを無視する

次のいずれかを選択できます。

- **正常に動作しないVSSライターを無視する**
  このオプションにより、1つまたは複数のVSSライターが正常に動作しない場合でもバックアップを成功させることができるようになります。

  重要
  アプリケーション固有のライターが正常に動作しない場合、アプリケーション認識型バックアップも失敗します。例えば、SQL Serverのデータをアプリケーション認識型バックアップでバックアップしようとしている場合、**SqlServerWriter**で問題が発生すると、バックアップ操作も失敗します。

  このオプションが有効になっている場合、VSSスナップショットは最大3回まで試行されます。
  初回の試行では、すべてのVSSライターが必要です。もし最初の試みが失敗した場合、再試行が行われます。2回目も失敗した場合、失敗したVSSライターはバックアップ操作のスコープから除外され、3回目の試行が行われます。3回目の試行が成功した場合、バックアップは失敗したVSSライターに関する警告を伴って完了します。3回目の試行が失敗した場合、バックアップは失敗となります。

- **すべてのVSSライターの正常な処理を要求する**
  VSSライターのいずれかが正常に動作しない場合、バックアップ操作も失敗します。

スナップショットプロバイダーを選択する

次のいずれかを選択できます。

- **自動的にスナップショットプロバイダを選択**
  自動的にハードウェアスナップショットプロバイダ、ソフトウェアスナップショットプロバイダ、Microsoft Software Shadow Copy Providerの中から選択します。
- **Microsoft Software Shadow Copy Providerを使用**
  アプリケーションサーバー（Microsoft Exchange Server、Microsoft SQL Server、Microsoft SharePoint、またはActive Directory）をバックアップするときは、このオプションを選択することをお勧めします。

VSS完全バックアップの有効化

このオプションを有効にした場合、ディスクレベルの完全バックアップ、増分バックアップ、差分バックアップが正常に実行されると、Microsoft Exchange Serverやその他のVSS対応アプリケーション（Microsoft SQL Serverを除く）のログが切り捨てられます。

デフォルト設定:**無効**。

次の場合、このオプションは無効のままにしてください。

- Exchange Serverのデータをバックアップするために Exchangeエージェントまたはサードパーティ製のソフトウェアを使用する場合。これは、ログの切り捨てにより、生成されるトランザクションログのバックアップに影響が生じるためです。
- SQL Server のデータのバックアップのためにサード パーティ製のソフトウェアを使用する場合。サードパーティ製のソフトウェアは、生成されるディスクレベルのバックアップを、そのソフトウェアの完全バックアップに使用します。その結果、SQL Server のデータに対する次の差分バックアップが失敗します。このサードパーティ製のソフトウェアが「そのソフトウェアの」次の完全バックアップを作成するまで、バックアップの失敗が続きます。
- コンピュータ上で他のVSS対応アプリケーションが実行されていて、何らかの理由でこのアプリケーションのログを保持する必要がある場合。

重要
このオプションを有効にしても、Microsoft SQL Server ログの切り捨ては行われません。バックアップ後にSQL Serverログを切り捨てるには、[ログの切り詰め] バックアップオプションを有効にします。

仮想マシンのボリュームシャドウコピーサービス（VSS）

このオプションでは、仮想コンピュータの静止スナップショットを取得するかどうかを定義します。

デフォルト設定:**有効**。

このオプションを無効にした場合、停止スナップショットが取得されます。仮想コンピュータのバックアップがクラッシュコンシステント状態で作成されます。

このオプションを有効にした場合、仮想マシンで実行中のすべてのVSS対応アプリケーションに関するトランザクションが完了してから、停止スナップショットが取得されます。

[エラー処理] オプションで指定した回数だけ再試行が繰り返されても、停止スナップショットを取得できない場合、アプリケーションのバックアップが有効となり、バックアップが失敗します。

[エラー処理] オプションで指定した回数だけ再試行が繰り返されても、停止スナップショットを取得できない場合、アプリケーションのバックアップが無効となり、クラッシュ一貫性のあるバックアップが作成されます。クラッシュ一貫性のあるバックアップを作成する代わりにバックアップを失敗させるには、**[停止スナップショットの取得が不可能な場合にバックアップが失敗する]** チェックボックスを選択します。

次の表に、使用可能な設定とその結果を示します。

設定	停止スナップショットが正常に取得されました		停止スナップショットが取得されませんでした	
	アプリケーションバックアップが有効	**アプリケーションバックアップ無効**	**アプリケーションバックアップが有効**	**アプリケーションバックアップ無効**
[仮想マシンのボリュームシャドウコピーサービス（VSS）] が有効 **[停止スナップショットの取得が不可能な場合にバックアップが失敗する]** が未選択	停止スナップショットが取得されます。アプリケーション一貫性のあるバックアップが作成されます。	停止スナップショットが取得されます。アプリケーション一貫性のあるバックアップが作成されます。	バックアップは失敗します。	非停止スナップショットが取得されます。クラッシュ一貫性のあるバックアップが作成されます。
[仮想マシンのボリュームシャドウコピーサービス（VSS）] が有効 **[停止スナップショットの取得が不可能な場合にバックアップが失敗する]** が選択済み	停止スナップショットが取得されます。アプリケーション一貫性のあるバックアップが作成されます。	停止スナップショットが取得されます。アプリケーション一貫性のあるバックアップが作成されます。	バックアップは失敗します。	バックアップは失敗します。
[仮想マシンのボリュームシャドウコピーサービス（VSS）] が無効	非停止スナップショットが取得されます。クラッシュ一貫性のあるバックアップが作成されます。	非停止スナップショットが取得されます。クラッシュ一貫性のあるバックアップが作成されます。	非停止スナップショットが取得されます。クラッシュ一貫性のあるバックアップが作成されます。	非停止スナップショットが取得されます。クラッシュ一貫性のあるバックアップが作成されます。

[仮想マシンのボリュームシャドウコピーサービス（VSS）] を有効にすると、仮想マシンのバックアップ時に使用された凍結前および凍結解除後スクリプトも自動実行されます。これらのスクリプトの詳細については、「"凍結前スクリプトと凍結解除後スクリプトを自動的に実行する"（677ページ）」を参照してください。

静止スナップショットを取得する場合は、バックアップソフトウェアがVMware Tools、Hyper-V Integration Service、Virtuozzoゲストツール、Red Hat Virtualizationゲストツール、QEMUゲストツールを使用し、仮想マシン内でVSSを適用します。

注意
Red Hat Virtualization（oVirt）仮想マシンでは、Red Hat Virtualizationゲストツールの代わりにQEMUゲストツールをインストールすることをお勧めします。Red Hat Virtualizationゲストツールの一部のバージョンは、アプリケーションについて一貫性のあるスナップショットをサポートしていません。

このオプションはScale Computing HC3仮想マシンには影響しません。それらのマシンにおける静止スナップショットの取得は、拡張ツールが仮想マシンにインストールされているかどうかによって異なります。

週単位のバックアップ

このオプションでは、バックアップの保持ルールとバックアップスキームで「週単位」と見なされるバックアップを決定します。「週単位」のバックアップでは、週の初めに最初のバックアップが作成されます。

デフォルト設定:**月曜日**。

Windowsイベントログ

このオプションは、Windows オペレーティング システムの場合にのみ有効です。

このオプションでは、エージェントがバックアップ操作のイベントをWindowsのアプリケーションイベントログに記録する必要があるかどうかを定義します（このログを表示するには、eventvwr.exeを実行するか、**[コントロールパネル]** > **[管理ツール]** > **[Event Viewer]** の順に選択します）。ログに記録するイベントにフィルタを設定することができます。

デフォルト設定:**無効**。

復元

復元のチートシート

次の表は、使用可能な復元方法を示しています。この表を使用して、要件に最も適した復元方法を選択してください。

注意
コンプライアンスモードのテナント対しCyber Protectコンソールではバックアップをリカバリできません。このようなバックアップをリカバリする方法の詳細については、"コンプライアンスモードでテナントのバックアップを復元する"（1050ページ）を参照してください。

復元元	復元方法
物理マシン （WindowsまたはLinux）	Cyber Protectコンソールを使用する ブータブルメディアを使用

物理マシン （Mac）	ブータブルメディアを使用
仮想マシン （VMware、Hyper-V、Red Hat Virtualization（oVirt）またはScale Computing HC3）	Cyber Protectコンソールを使用する ブータブルメディアを使用
仮想マシンまたはコンテナ （Virtuozzo、Virtuozzo Hybrid Server、Virtuozzo Hybrid Infrastructure）	Cyber Protectコンソールを使用する
ESXi構成	ブータブルメディアを使用
ファイル/フォルダ	Cyber Protectコンソールを使用する クラウドストレージからのファイルのダウンロード ブータブルメディアを使用 ローカルバックアップからファイルを抽出
システム状態	Cyber Protectコンソールを使用する
SQLデータベース	Cyber Protectコンソールを使用する
Exchangeデータベース	Cyber Protectコンソールを使用する
Exchangeメールボックス	Cyber Protectコンソールを使用する
Web サイト	Cyber Protectコンソールを使用する
Microsoft 365	
メールボックス （ローカルのMicrosoft 365エージェント）	Cyber Protectコンソールを使用する
メールボックス （Microsoft 365クラウドエージェント）	Cyber Protectコンソールを使用する
パブリック フォルダ	Cyber Protectコンソールを使用する
OneDriveファイル	Cyber Protectコンソールを使用する
SharePoint Onlineデータ	Cyber Protectコンソールを使用する
Google Workspace	
メールボックス	Cyber Protectコンソールを使用する
Google ドライブのファイル	Cyber Protectコンソールを使用する

共有ドライブファイル	Cyber Protectコンソールを使用する

クロスプラットフォーム復元

クロスプラットフォーム復元は、マシン全体のバックアップおよびオペレーティングシステムを含むディスクのバックアップで使用できます。

クロスプラットフォーム復元は、以下の場合に実行されます:

- あるタイプのエージェントによってバックアップが作成され、別のタイプのエージェントによってリカバリされる。
- エージェントベースのバックアップがハイパーバイザーレベルでリカバリされる（エージェントレス復元）、またはエージェントレスバックアップがエージェントによってリカバリされる（エージェントベース復元）。
- バックアップが、異なるハードウェア（仮想ハードウェアを含む）にリカバリされる。

注意
クロスプラットフォーム復元を実行すると、プリンタなどの一部の周辺デバイスが正しくリカバリされない場合があります。

クロスプラットフォーム復元の例を次の表に示します。

クロスプラットフォーム復元	
エージェントレスバックアップ	エージェントベースの復元
エージェントベースのバックアップ	エージェントレス復元
Windowsエージェントによるバックアップ	VMwareエージェントによる復元
VMwareエージェントによるバックアップ	Hyper-Vエージェントによる復元
VMware ESXi仮想マシンにインストールされたWindowsエージェントによるバックアップ（エージェントベース）	同じVMware ESXiホスト上のVMwareエージェントによる復元（エージェントレス）
Windowsエージェントによるバックアップ	異なるハードウェアを含むマシンにインストールされたWindowsエージェントによる復元
物理マシンのバックアップ	仮想マシンとしての復元

Macユーザー向けの注意事項

- 10.11 El Capitanから、特定のシステムファイル、フォルダ、プロセスに、拡張ファイル属性com.apple.rootlessを使用して保護フラグが付けられます。この機能は、System Integrity Protection（SIP）と呼ばれます。保護対象のファイルには、プレインストールされたアプリケーション、および/system、/bin、/sbin、/usrの各フォルダ内のほとんどが含まれます。

保護対象のファイルとフォルダは、オペレーティングシステムの下で復元する際に上書きできません。保護対象のファイルを上書きする必要がある場合は、ブータブル メディアの下で復元を実行します。

- macOS Sierra 10.12から、クラウド機能のStoreにより使用頻度の低いファイルをiCloudに移動させることができます。これらのファイルでフットプリントの少ないものはファイル システムに保持されます。これらのフットプリントは元のファイルの代わりにバックアップされます。

  フットプリントを元のロケーションに復元する際には、iCloudと同期し元のファイルが使用できるようになります。フットプリントを別のロケーションに復元する際には、同期できないので元のファイルは使用できません。

安全な復元

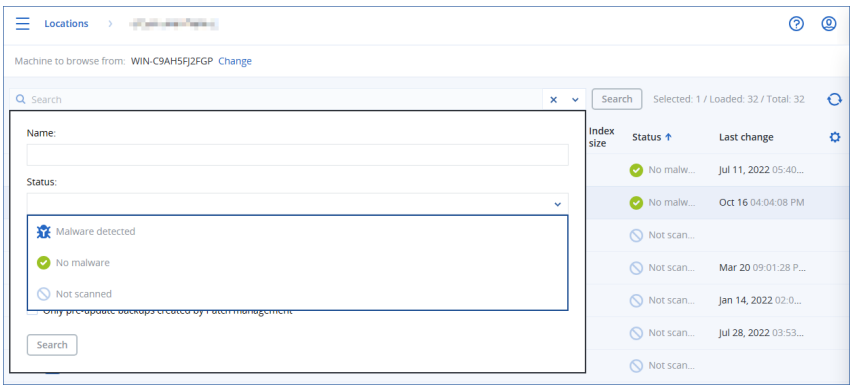
Windowsワークロードの**マシン全体**バックアップまたは**ディスク/ボリューム**バックアップで安全な復元を使用すると、バックアップに感染したファイルが含まれていても、マルウェアに感染していないデータのみをリカバリできます。

安全な復元操作時に、バックアップのマルウェアが自動的にスキャンされます。その後、プロテクションエージェントによりターゲットワークロード上のバックアップがリカバリされ、感染したファイルが削除されます。その結果、マルウェアに感染していないバックアップがリカバリされます。

また、バックアップに以下のいずれかのステータスが割り当てられます。

- マルウェアが検出されました
- マルウェアはありません
- スキャンされていません

ステータスを使用して、バックアップアーカイブをフィルタリングできます。



制限事項

- 安全な復元は、プロテクションエージェントがインストールされた物理/仮想Windowsマシンでサポートされます。
- 安全な復元は、**マシン全体**または**ディスク/ボリューム**バックアップでサポートされています。
- NTFSボリュームのみがマルウェアスキャンの対象となります。NTFS以外のボリュームは、マルウェア対策スキャンを経ずにリカバリされます。

- 安全な復元は、アーカイブの継続的データ保護（CDP）バックアップではサポートされていません。CDPバックアップからデータをリカバリする場合は、追加の**ファイル/フォルダ**の復元操作を実行します。CDPバックアップの追加の処理については、"継続的データ保護（CDP）"（397ページ）を参照してください。

マシンの復元

物理マシンのリカバリ

このセクションでは、Web インターフェイスを使用した物理コンピュータの復元について説明します。

復元する必要がある場合、Web インターフェイスではなくブータブルメディアを使用します。

- macOSを実行しているマシン
- コンプライアンスモードになっているテナントのマシン
- 任意のオペレーティング システムをベアメタルまたはオフラインコンピュータに復元する場合
- 論理ボリューム（LinuxにLVM（論理ボリュームマネージャ）で作成されたボリューム）の構成。メディアでは、論理ボリューム構成を自動的に再作成できます。

注意
Appleシリコンプロセッサを搭載するMacに、IntelベースMacのディスクレベルバックアップをリカバリすることはできません。ファイルおよびフォルダをリカバリできます。

再起動を伴う復元

オペレーティングシステムの復元、およびBitLockerで暗号化されたボリュームの復元には、再起動が必要です。コンピュータを自動的に再起動するか、**[ユーザーによる操作が必要]** ステータスに割り当てるかを選択できます。復元されたオペレーティングシステムは、自動的にオンラインになります。

重要
バックアップされた暗号化ボリュームは、非暗号化ボリュームとしてリカバリされます。

BitLockerで暗号化されたボリュームを復元する場合、同じマシン上に暗号化されていないボリュームがあり、そのボリュームに少なくとも1GBの空き領域がなければなりません。両方の条件が満たされない限り、復元は失敗します。

暗号化されたシステムボリュームをリカバリする場合、追加の操作は必要ありません。暗号化されている非システムボリュームをリカバリするには、まずこのボリュームをロックする必要があります。これは、ボリューム上に存在するファイルを開くことなどで実行できます。そうでない場合は、再起動を伴わずに復元が続行され、復元されたボリュームがWindowsから認識できなくなる可能性があります。

注意
復元に失敗し、**「パーティションからファイルを取得できません」**というエラーによりマシンが再起動する場合は、セキュアブートを無効にしてから試行してください。この方法については、Microsoftテクニカルドキュメントの「セキュア ブートの無効化」を参照してください。

物理コンピュータの復元手順

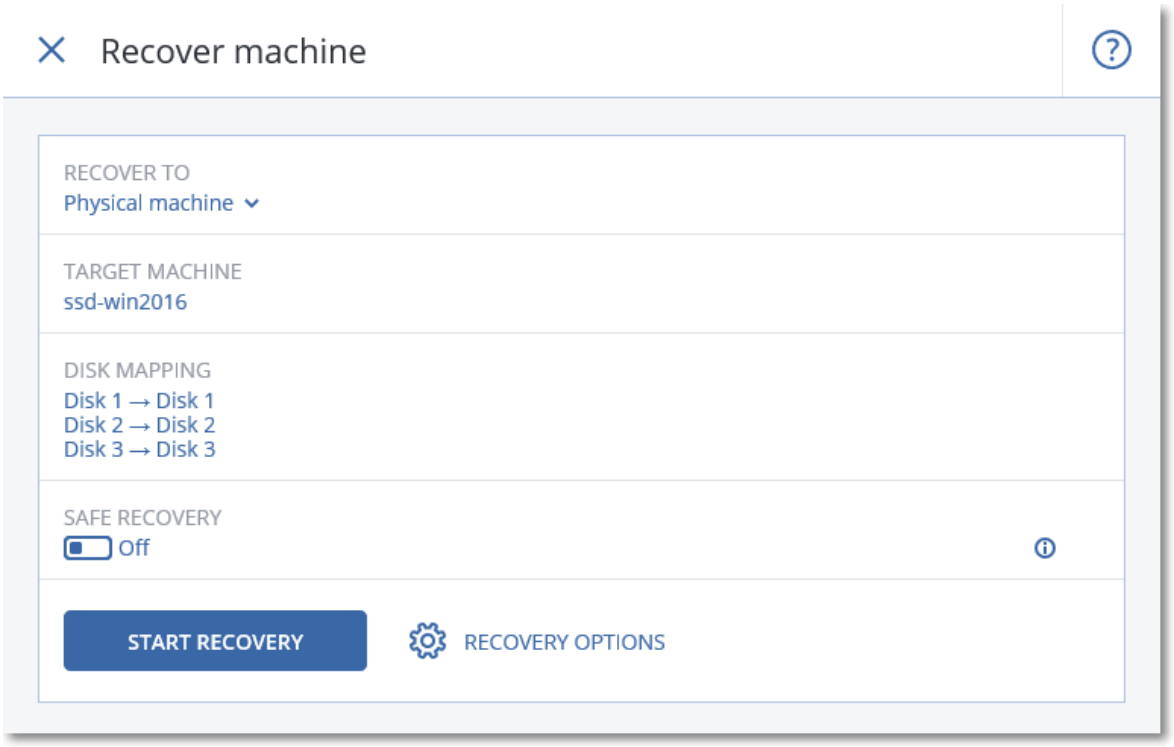
1. バックアップされたコンピュータを選択します。
2. **[復元]** をクリックします。
3. リカバリ ポイントを選択します。復元ポイントは、保存場所でフィルタされます。

   コンピュータがオフラインになっている場合、リカバリ ポイントは表示されません。次の手順のいずれかを実行します。

   - バックアップのロケーションがクラウドまたは共有ストレージの（他のエージェントがアクセスできる）場合は、**[コンピュータを選択]** をクリックして、オンラインになっているターゲット コンピュータを選択してから、リカバリ ポイントを選択します。
   - [バックアップストレージ] タブで復元ポイントを選択します。
   - 「ブータブル メディアを使用したディスクの復元」の説明に従って、コンピュータを復元します。
4. **[復元]** > **[コンピュータ全体]** をクリックします。

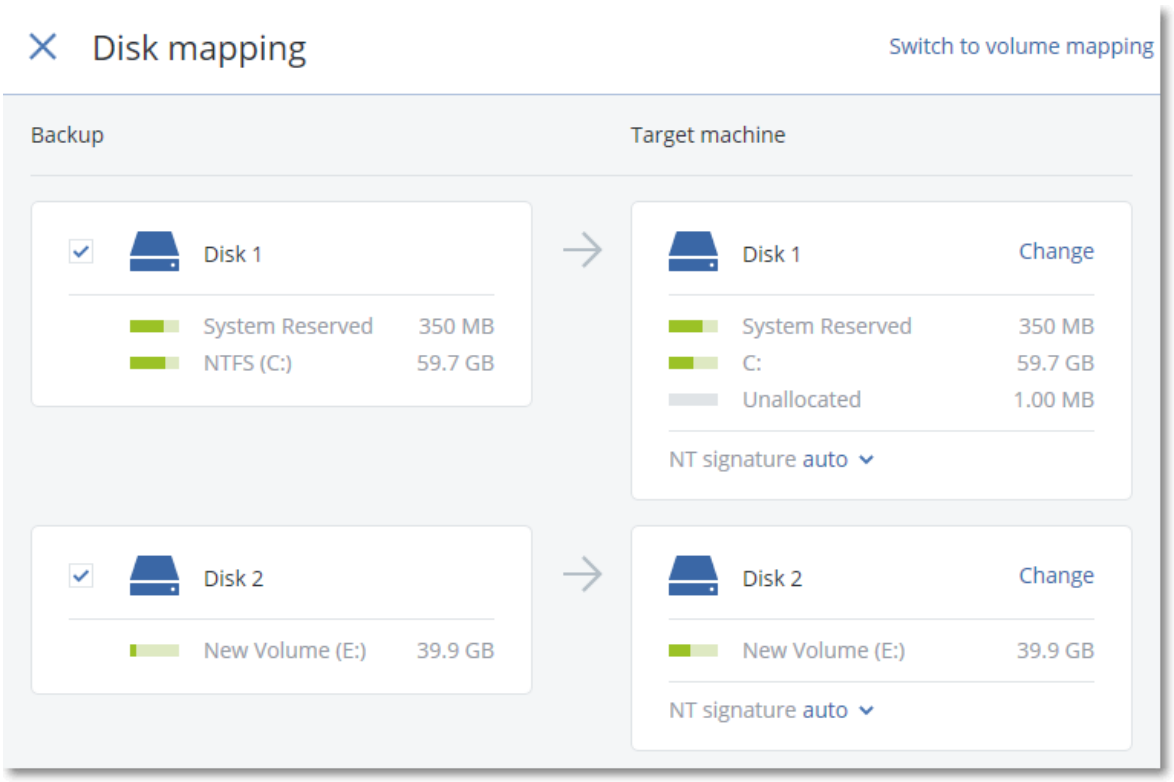
   バックアップされたディスクをターゲット コンピュータのディスクへ自動的にマップします。

   別の物理コンピュータに復元するには、**[復元先のコンピュータ]** をクリックして、オンラインの復元先のコンピュータを選択します。



5. マッピング結果に満足できない場合や、マッピングが正常に行われなかった場合は、**[ボリューム マッピング]** をクリックして、ディスクを手動で再度マッピングできます。

   マッピングセクションでは、復元対象の個別のディスクまたはボリュームを選択することもできます。右上の **[...に切り替え]** リンクを使用することによって、リカバリするディスクおよびボリュームを切り替えることができます。



6. （プロテクションエージェントがインストールされているWindowsマシンでのみ使用可能）**[安全な復元]** スイッチを有効にして、リカバリデータがマルウェアに感染していないことを確認します。安全な復元の仕組みについては、"安全な復元"（487ページ）を参照してください。
7. **[復元を開始]** をクリックします。
8. ディスクをバックアップされたバージョンで上書きすることを確認します。コンピュータを自動的に再起動するかどうかを選択します。

復元の進行状況は **[アクティビティ]** タブに表示されます。

物理コンピュータから仮想コンピュータへ

サポートされているいずれかのハイパーバイザーで、物理マシンを仮想マシンにリカバリできます。これは、物理マシンを仮想マシンに移行するメカニズムでもあります。サポートされるP2Vマイグレーションパスの詳細については、「マシンの移行」を参照してください。

このセクションでは、Webインターフェースを使用して、物理マシンを仮想マシンとして復元する方法を説明します。この操作は、関連するハイパーバイザーのエージェントが、Acronis管理サーバーに少なくとも1つインストールされ、登録されている場合に実行できます。たとえば、VMware ESXiへの復元には、その環境で少なくとも1つのVMwareエージェントがインストールおよび登録されている必要があり、Hyper-Vへの復元にはその環境で少なくとも1つのHyper-Vエージェントがインストールおよび登録されている必要があります。

コンプライアンスモードのテナントは、Webインターフェイスを介した復元を利用できません。

注意
Hyper-VはmacOSをサポートしていないため、macOS仮想マシンをHyper-Vホストにリカバリすることはできません。macOS仮想マシンは、Macハードウェアにインストールされ ているVMwareホストにリカバリできます。

また、macOS物理マシンのバックアップを仮想マシンとしてリカバリすることはできません。

物理コンピュータを仮想コンピュータとして復元するには

1. バックアップされたコンピュータを選択します。
2. **[復元]** をクリックします。
3. リカバリ ポイントを選択します。復元ポイントは、保存場所でフィルタされます。
   コンピュータがオフラインになっている場合、リカバリ ポイントは表示されません。次の手順のいずれかを実行します。
   - バックアップのロケーションがクラウドまたは共有ストレージの（他のエージェントがアクセスできる）場合は、**[コンピュータを選択]** をクリックして、オンラインになっているコンピュータを選択してから、リカバリ ポイントを選択します。
   - [バックアップストレージ] タブで復元ポイントを選択します。
   - 「ブータブル メディアを使用したディスクの復元」の説明に従って、コンピュータを復元します。
4. **[復元]** > **[コンピュータ全体]** をクリックします。
5. **[復元先]** で、**[仮想コンピュータ]** を選択します。
6. **[対象コンピュータ]** をクリックします。
   a. ハイパーバイザーを選択します。

      注意
      該当のハイパーバイザーのエージェントが、Acronis管理サーバーに少なくとも1つインストールおよび登録されている必要があります。

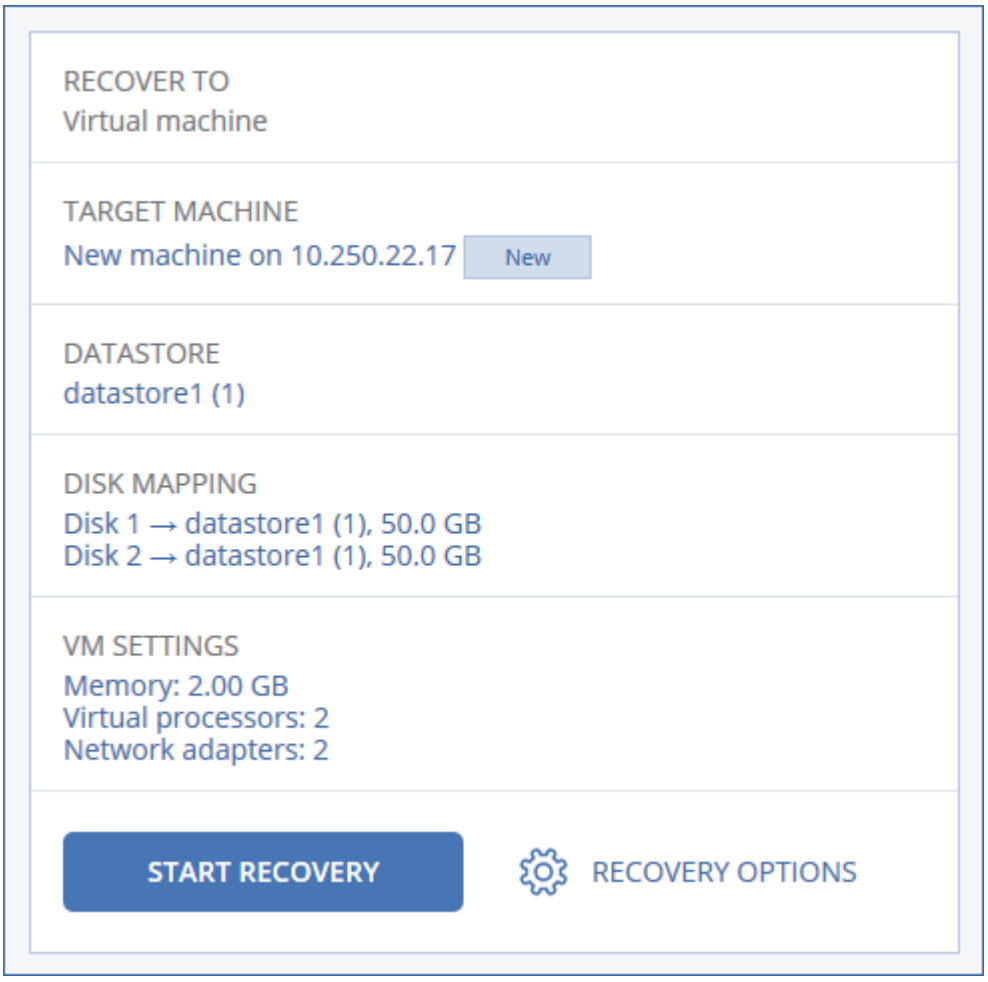
   b. 新規または既存のコンピュータに復元するかどうかを選択します。ターゲット コンピュータのディスク構成がバックアップのディスク構成に完全に一致する必要がないため、新規のコンピュータを選択することをおすすめします。
   c. ホストを選択し、新しいコンピュータ名を指定するか、既存のターゲット コンピュータを選択します。
   d. **[OK]** をクリックします。
7. （Virtuozzo Hybrid Infrastructureの場合）**[VM設定]** をクリックして、**[フレーバー]** を選択します。
   オプションで、仮想マシンのメモリサイズ、プロセッサー数、ネットワーク接続を変更できます。

   注意
   Virtuozzo Hybrid Infrastructureの場合、フレーバー選択の手順は必須です。

8. （オプション） 追加の復元オプションを構成します。

- （Virtuozzo Hybrid Infrastructure以外）**[データストア]**（ESXi）または **[パス]**（Hyper-V）をクリックしてから、仮想マシンのデータストア（ストレージ）を選択します。
- **[ディスクマッピング]** をクリックして、各仮想ディスクのデータストア（ストレージ）、インターフェース、プロビジョニングモードを選択します。マッピングセクションでは、復元対象の個別のディスクを選択することもできます。

  Virtuozzo Hybrid Infrastructureの場合、ターゲットディスクに対して選択できるのはストレージポリシーのみです。設定する場合、対象のターゲットディスクを選択し、[変更] をクリックします。ブレードが開いたら、ギアアイコンをクリックし、ストレージポリシーを選択して [完了] をクリックします。
- （VMware ESXi、Hyper-V、およびRed Hat Virtualization/oVirtの場合）**[VM設定]** をクリックして、仮想マシンのメモリサイズ、プロセッサー数、ネットワーク接続を変更します。



9. （プロテクションエージェントがインストールされているWindowsマシンでのみ使用可能）**[安全な復元]** スイッチを有効にして、リカバリデータがマルウェアに感染していないことを確認します。安全な復元の仕組みについては、"安全な復元"（487ページ）を参照してください。
10. **[復元を開始]** をクリックします。
11. 既存の仮想コンピュータに復元するときには、ディスクを上書きすることを確認します。

復元の進行状況は **[アクティビティ]** タブに表示されます。

仮想コンピュータの復元

バックアップから仮想マシンをリカバリできます。

注意
コンプライアンスモードのテナント対しCyber Protectコンソールではバックアップをリカバリできません。このようなバックアップをリカバリする方法の詳細については、"コンプライアンスモードでテナントのバックアップを復元する"（1050ページ）を参照してください。

前提条件

- このコンピュータへの復元中は、仮想コンピュータを停止する必要があります。デフォルトでは、確認メッセージを表示することなくマシンが停止します。復元が完了したら、コンピュータを手動で起動する必要があります。このデフォルトの動作はVM電源管理復元オプションを使用して変更できます（**[復元オプション]** > **[VM電源管理]**をクリック）。

手順

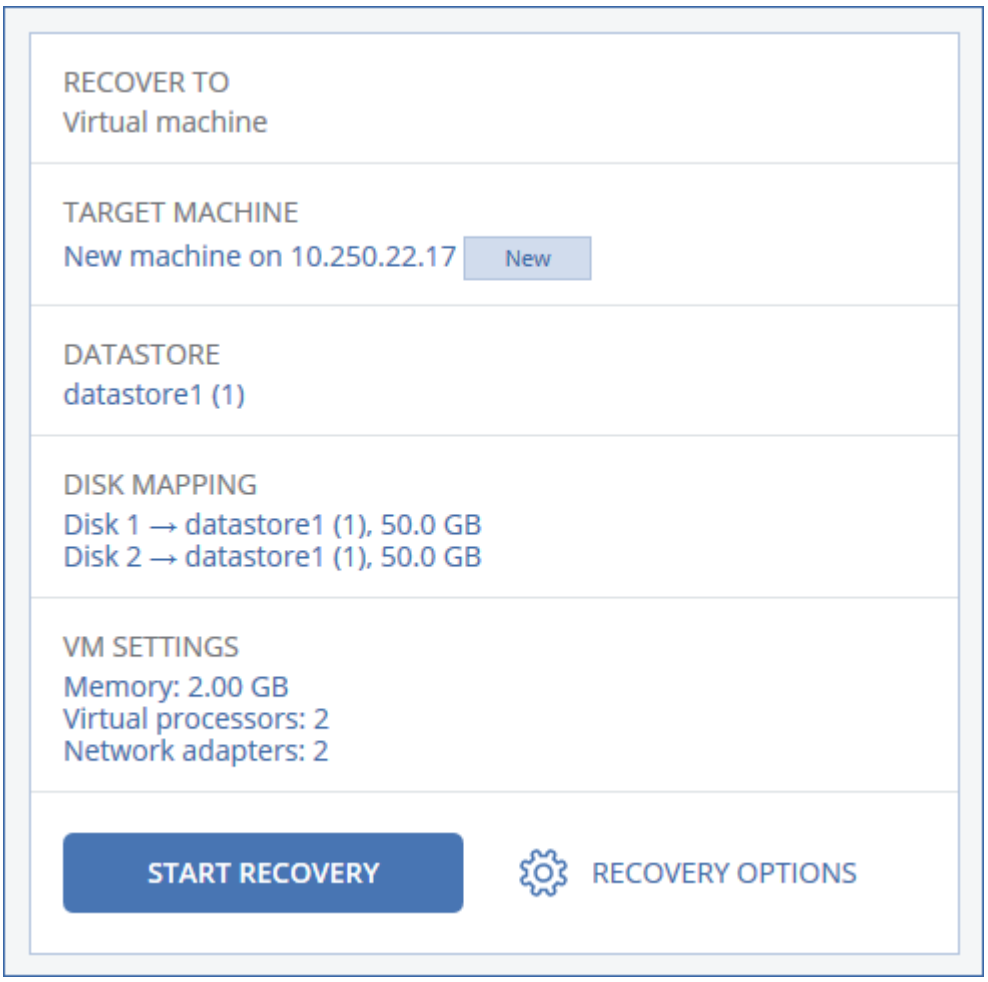
1. 次のいずれかを実行します。
   - バックアップされたコンピュータを選択し、**[復元]** をクリックしてから、リカバリポイントを選択します。
   - ［バックアップストレージ］タブで復元ポイントを選択します。
2. **[復元]** > **[コンピュータ全体]** をクリックします。
3. 物理コンピュータに復元する場合は、**[復元先]** で **[物理コンピュータ]** を選択します。それ以外の場合は、この手順をスキップします。
   対象コンピュータのディスク構成がバックアップのディスク構成と正確に一致する場合にのみ、物理コンピュータへの復元が可能です。
   この場合、「物理コンピュータ」の手順4に続きます。それ以外の場合は、ブータブルメディアを使用して、V2P移行を実行することをお勧めします。
4. （オプション）デフォルトでは、ターゲットマシンとして自動的に元のコンピュータが選択されます。別の仮想コンピュータに復元するには、**[ターゲットコンピュータ]** をクリックしてから次の手順を実行します。
   a. ハイパーバイザーを選択します（**VMware ESXi**、**Hyper-V**、**Virtuozzo**、**Virtuozzo Hybrid Infrastructure**、**Scale Computing HC3**、または**oVirt**）。
      Virtuozzoに復元できるのは、Virtuozzo仮想コンピュータのみです。V2V移行の詳細については、「マシンの移行」を参照してください。
   b. 新規または既存のコンピュータに復元するかどうかを選択します。
   c. ホストを選択し、新しいコンピュータ名を指定するか、既存のターゲット コンピュータを選択します。
   d. **[OK]** をクリックします。
5. 必要な追加の復元オプションを設定します。
   - （オプション）（Virtuozzo Hybrid InfrastructureおよびScale Computing HC3では利用不可）仮想マシンのデータストアを選択するには、**[データストア]**（ESXi）、**[パス]**（Hyper-Vおよび

Virtuozzo）、または **[ストレージドメイン]**（Red Hat Virtualization/oVirt）をクリックしてから、仮想マシンのデータストア（ストレージ）を選択します。

- （オプション） 各仮想ディスクのデータストア（ストレージ）、インターフェース、プロビジョニングモードを表示するには、**[ディスクマッピング]** をクリックします。Virtuozzoコンテナまたはは Virtuozzo Hybrid Infrastructure仮想マシンの復元中でなければ、これらの設定を変更できます。

  Virtuozzo Hybrid Infrastructureの場合、ターゲットディスクに対して選択できるのはストレージポリシーのみです。設定する場合、対象のターゲットディスクを選択し、**[変更]** をクリックします。ブレードが開いたら、ギアアイコンをクリックし、ストレージポリシーを選択して **[完了]** をクリックします。

  マッピングセクションでは、復元対象の個別のディスクを選択することもできます。
- （オプション） （VMware ESXi、Hyper-V、Virtuozzoで利用可能）仮想マシンのメモリサイズ、プロセッサー数、ネットワーク接続を変更するには、**[VM設定]** をクリックします。
- （Virtuozzo Hybrid Infrastructure向け）仮想マシンのメモリサイズ、プロセッサー数を変更するには、**[フレーバー]** をクリックします。



6. （プロテクションエージェントがインストールされているWindowsマシンでのみ使用可能）**[安全な復元]** スイッチを有効にして、リカバリデータがマルウェアに感染していないことを確認します。安全な復元の仕組みについては、"安全な復元"（487ページ）を参照してください。
7. **[復元を開始]** をクリックします。

8. 既存の仮想コンピュータに復元するときには、ディスクを上書きすることを確認します。
復元の進行状況は **[アクティビティ]** タブに表示されます。

ブータブルメディアを使用したディスクの復元

ブータブルメディアの作成方法については、「"物理的なブータブルメディアの作成"（691ページ）」を参照してください。

注意
Appleシリコンプロセッサを搭載するMacに、IntelベースMacのディスクレベルバックアップをリカバリすることはできません。ファイルおよびフォルダをリカバリできます。

ブータブル メディアを使用したディスクの復元手順

1. ブータブル メディアを使用して復元対象のコンピュータを起動します。
2. （Mac の復元時のみ）APFS でフォーマットされたディスクやボリュームを別のマシンやベアメタルに復元する場合は、オリジナルディスクの設定を手動で再作成します。
   a. **[ディスクユーティリティ]** をクリックします。
   b. ターゲットディスクを消去して、APFSにフォーマットします。手順については、https://support.apple.com/en-us/HT208496#erasediskを参照してください。
   c. オリジナルディスクの設定を再作成します。手順については、https://support.apple.com/guide/disk-utility/add-erase-or-delete-apfs-volumes-dskua9e6a110/19.0/mac/10.15を参照してください。
   d. **[ディスクユーティリティ]** > **[クイックディスクユーティリティ]** をクリックします。
3. 使用するメディアの種類によって **[このコンピュータをローカルで管理]** クリックするか、**[レスキュー ブータブル メディア]** を2回クリックします。
4. プロキシサーバーがネットワークで有効な場合、**[ツール]** > **[プロキシサーバー]** をクリックして、プロキシサーバーホスト名/IP アドレス、ポート、および資格情報を指定します。それ以外の場合は、この手順をスキップします。
5. （オプション）WindowsまたはLinuxをリカバリするときは、**[ツール]** > **[Cyber Protectionサービスでメディアを登録]** をクリックして、メディアをダウンロードしたときに取得した登録トークンを指定します。この場合、手順8に説明されているように、クラウドストレージにアクセスするために資格情報または登録コードを入力する必要はありません。
6. [ようこそ] 画面で、 **[復元]** をクリックします。
7. **[データの選択]** をクリック後、**[参照]** をクリックします。
8. バックアップのロケーションを指定します。
   - クラウドストレージから復元するには、**[クラウドストレージ]** を選択します。バックアップされたコンピュータに割り当てられているアカウントの資格情報を入力します。
     WindowsまたはLinuxを復元するときは、資格情報の代わりに登録コードのリクエストを選択できます。**[登録コードを使用]** > **[コードを要求]** をクリックします。ソフトウェアに登録リンクと登録コードが表示されます。リンクとコードをコピーして、ほかのマシンで登録手順を実行できます。登録コードの有効期限は 1 時間です。

- ローカル フォルダまたはネットワークフォルダから復元するには、**[ローカル フォルダ]** または **[ネットワークフォルダ]** のフォルダを参照します。
- Microsoft Azure、Amazon S3、Wasabi、S3 互換などのパブリッククラウドストレージ上のバックアップロケーションから復元するには、まず **[Cyber Protectionサービスでメディアを登録]** をクリックし、次にWebインターフェイスを使用して復元を設定します。Webンターフェイスを使用したリモートでのメディア管理の詳細については、"ブータブルメディアのリモート操作"（708 ページ）を参照してください。

[OK] をクリックし、選択を確定します。

9. 復元するバックアップデータを選択します。バックアップデータのパスワードを要求される場合は、設定したパスワードを入力します。
10. **[バックアップ内容]** で、復元対象のディスクを選択します。**[OK]** をクリックし、選択を確定します。
11. **[復元先]** で、選択されたディスクがターゲット ディスクに自動的に割り当てられます。
    ディスクの割り当てが正常に行われなかった場合、または割り当て結果が意図したものと異なる場合は、ディスクを手動で再度割り当てることができます。

    注意
    ディスクのレイアウトを変更すると、オペレーティングシステムのブータビリティに影響することがあります。正常に実行される確証がある場合を除き、元のコンピュータのディスクレイアウトを使用してください。

12. （Linuxの復元）バックアップされたコンピュータに論理ボリューム（LVM）があり、元のLVM構造を再現する場合：
    a. 復元先のコンピュータのディスクの数および各ディスクの容量が元のコンピュータの数量以上であることを確認し、**[RAID/LVM の適用]** をクリックします。
    b. ボリューム構成を確認し、**[RAID/LVM の適用]** をクリックし、作成します。
13. （オプション）その他の設定が必要な場合、**[復元オプション]** をクリックして、設定します。
14. **[OK]** をクリックして復元を開始します。

Universal Restoreの使用

最新のオペレーティングシステムは、VMwareやHyper-Vプラットフォームを含め、異なるハードウェアに復元される場合も、引き続きブータブルとなります。復元されたオペレーティングシステムが起動しない場合は、Universal Restoreツールを使用し、オペレーティングシステムの起動にとって重要なドライバとモジュールをアップデートします。

UniversalRestoreはWindowsとLinuxに適用できます。

Universal Restoreを適用する方法

1. ブータブル メディアからコンピュータを起動します。
2. **[Universal Restoreの適用]** をクリックします。
3. コンピュータ上に複数のオペレーティングシステムが存在する場合、Universal Restoreを適用するオペレーティングシステムを選択します。

4. （Windowsのみ）その他の設定を設定します。
5. **[OK]** をクリックします。

WindowsにおけるUniversal Restore

インストールする前に

ドライバの準備

Universal RestoreをWindowsオペレーティングシステムに適用する前に、新しいHDDコントローラとチップセット用のドライバがあることを確認します。これらのドライバは、オペレーティング システムの起動に不可欠です。ハードウェアベンダから提供されているCDまたはDVDを使用するか、ベンダのウェブサイトからドライバをダウンロードします。ドライバファイルの拡張子は、*.infです。*.exe、*.cab、または *.zip 形式でドライバをダウンロードする場合、サードパーティ製のアプリケーションを使用してそれらのドライバを取り出します。

ベストプラクティスは、組織で使用するすべてのハードウェアのドライバを、デバイスの種類やハードウェア構成ごとに単一のレポジトリに保存することです。レポジトリのコピーをDVDまたはフラッシュドライブに保存し、いくつかのドライバを選択してブータブルメディアに追加し、サーバーごとに必要なドライバ（およびネットワーク構成）を搭載したカスタムのブータブルメディアを作成できます。または、Universal Restore を使用するたびに、レポジトリのパスを指定することもできます。

起動用の環境におけるドライバへのアクセスを確認

ブータブルメディアを使用する場合は、ドライバが保存されているデバイスにアクセスする権限を持っていることを確認します。デバイスがWindowsで使用可能であってもLinuxベースのメディアによって検出されない場合は、WinPEベースのメディアを使用してください。

Universal Restoreの設定

自動ドライバ検索

プログラムがHAL（Hardware Abstraction Layer）、HDDコントローラのドライバ、およびネットワークアダプターのドライバを探す場所を指定します。

- ドライバがベンダのディスクまたはその他のリムーバブルメディアにある場合は、**[リムーバブルメディアの検索]** をオンにします。
- ドライバがネットワーク上のフォルダまたはブータブル メディアにある場合は、**[フォルダの追加]** をクリックして、フォルダのパスを指定します。

また、Universal Restoreでは、Windowsのデフォルトのドライバストレージフォルダが検索されます。このフォルダの場所は、レジストリ値**DevicePath**で指定されています。このレジストリ値は、レジストリキー**HKEY_LOCAL_MACHINE¥SOFTWARE¥Microsoft¥Windows¥CurrentVersion**にあります。通常、このストレージ フォルダは WINDOWS/inf です。

Universal Restoreでは、指定したフォルダ内のすべてのサブフォルダを再帰的に検索し、利用可能なすべてのHALおよびHDDコントローラーのドライバから最適なドライバを特定して、システムへのインス

トールが行われます。Universal Restore は、ネットワーク アダプタのドライバも検索し、見つかったドライバのパスがUniversal Restore によってオペレーティング システムに 伝達 されます。ハードウェアに複数のネットワーク インターフェイス カードがある場合、Universal Restore はすべてのカードのドライバの構成を試みます。

インストールする大容量記憶装置ドライバ

次の場合、この設定が必要です。

- ハードウェアに、RAID（特にNVIDIA RAID）やファイバチャネルアダプタなどの、固有の大容量記憶装置コントローラが存在する場合です。
- SCSIハードドライブコントローラを使用する仮想コンピュータにシステムを移行した場合です。仮想環境ソフトウェアに同梱されているSCSIドライバを使用するか、最新版のドライバをソフトウェアメーカーのウェブサイトからダウンロードしてください。
- 自動ドライバ検索によっても、システムを起動できない場合です。

[ドライバの追加] をクリックして、適切なドライバを指定します。さらに適切なドライバが見つかった場合でも、警告を表示してそのドライバがインストールされます。

Universal Restoreプロセス

必要な設定を行った後で、**[OK]** をクリックします。

Universal Restoreによって、指定したロケーションに互換性のあるドライバが検出されなかった場合、問題のデバイスを示すプロンプトが表示されます。次のいずれかを実行します。

- 過去に指定したロケーションのいずれかにドライバを追加して、**[再試行]** をクリックします。
- 指定したロケーションを思い出せない場合、**[無視]** をクリックしてプロセスを続行してください。求めていた結果と異なる場合は、Universal Restoreを再適用します。処理を設定する際に、必要なドライバを指定します。

Windows が起動すると、新しいハードウェアをインストールするための標準の手順が開始されます。ドライバにMicrosoft Windowsのシグネチャがある場合、ネットワークアダプターのドライバはダイアログが表示されることなくインストールされます。それ以外の場合、Windows は、署名されていないドライバをインストールするかどうかの確認を求めます。

その後で、ネットワーク接続を構成し、ビデオアダプタ、USB、およびその他のデバイスのドライバを指定できます。

Linux における Universal Restore

Universal Restore は、カーネルのバージョン 2.6.8 以降の Linux オペレーティング システムに適用できます。

Universal Restore を Linux オペレーティング システムに適用すると、イニシャル RAM ディスクという一時ファイル システム（initrd）がアップデートされます。これにより、オペレーティング システムを新しいハードウェアで起動できるようになります。

Universal Restore によって、新しいハードウェアのモジュール（デバイス ドライバを含む）が、イニシャル RAM ディスクに追加されます。通常、必要なモジュールは **/lib/modules** ディレクトリにあります。Universal Restore によって必要なモジュールが検索できない場合、そのモジュールのファイル名がログに記録されます。

Universal Restore によって、GRUB ブート ローダーの設定が変更される場合があります。たとえば、新しいコンピュータのボリューム レイアウトが元のコンピュータとは異なる場合、システムのブータビリティを確保するために、この変更が必要となる可能性があります。

Universal Restore によって Linux カーネルが変更されることはありません。

オリジナルのイニシャル RAM ディスクへの復元

必要に応じて、オリジナルのイニシャル RAM ディスクに復元できます。

イニシャル RAM ディスクは、コンピュータ上のファイル内に保存されています。初めてイニシャル RAM ディスクをアップデートする場合は、Universal Restore によって、ディスクのコピーが同じディレクトリに事前に保存されます。このコピーの名前は、ファイル名の後に **_acronis_backup.img** という接尾辞を付けたものになります。複数回 Universal Restore を実行（たとえば、不足していたドライバを追加した後など）しても、このコピーは上書きされません。

オリジナルのイニシャル RAM ディスクに復元するには、次の手順のいずれかを実行します。

- 適宜、コピーの名前を変更します。たとえば、次のようなコマンドを実行します。

  ```
  mv initrd-2.6.16.60-0.21-default_acronis_backup.img initrd-2.6.16.60-0.21-default
  ```

- GRUB ブート ローダー設定の **initrd** 行でコピーを指定します。

ファイルの復元

Cyber Protectコンソールでファイルをリカバリする

注意
コンプライアンスモードのテナント対しCyber Protectコンソールではバックアップをリカバリできません。このようなバックアップをリカバリする方法の詳細については、"コンプライアンスモードでテナントのバックアップを復元する"（1050ページ）を参照してください。

1. 復元するデータが存在していたコンピュータを選択します。
2. **[復元]** をクリックします。
3. リカバリ ポイントを選択します。復元ポイントは、保存場所でフィルタされます。

   選択したコンピュータが物理でオフラインの場合は、復元ポイントが表示されません。次の手順のいずれかを実行します。

   - [推奨] バックアップのロケーションがクラウドまたは共有ストレージ（つまり、他のエージェントがアクセスできる）の場合は、**[マシンを選択]** をクリックして、オンラインになっているターゲットマシンを選択してから、リカバリポイントを選択します。
   - [バックアップストレージ] タブで復元ポイントを選択します。

- クラウドストレージからファイルをダウンロードします。
- ブータブルメディアを使用します

4. **[復元]** > **[ファイル/フォルダ]** の順にクリックします。
5. 目的のフォルダを直接参照するか、検索バーを使用して目的のファイルおよびフォルダの一覧を取得します。

   検索は言語に依存しません。

   1つ以上のワイルドカード文字（*および?）を使用できます。ワイルドカードの使用に関する詳細については、"マスク"（451ページ）を参照してください。

   注意
   クラウドストレージに保存されたディスクレベルバックアップでは、検索は使用できません。

6. 復元するファイルを選択します。
7. ファイルを.zipファイルとして保存する場合は、**[ダウンロード]** をクリックし、データの保存先を選択して、**[保存]** をクリックします。それ以外の場合は、この手順をスキップします。

   フォルダが選択されている場合、または選択されたファイルの合計サイズが100MBを超えている場合は、ダウンロードできません。大量のデータをクラウドから取得するには、手順"クラウドストレージからのファイルのダウンロード"（501ページ）を使用します。
8. **[復元]** をクリックします。

   リカバリ先で、復元操作のターゲットをクリックして選択するか、デフォルトのターゲットのままにします。デフォルトのターゲットは、バックアップ元によって異なります。

   以下のターゲットを利用できます。

   - ソースマシン（プロテクションエージェントがインストールされている）。

     これは、リカバリするファイルが存在していたマシンです。
   - プロテクションエージェントがインストールされている他のマシン（物理マシン、仮想マシン、およびプロテクションエージェントがインストールされている仮想化ホスト、または仮想アプライアンスなど）。

     物理マシン、仮想マシン、およびプロテクションエージェントがインストールされている仮想化ホストにファイルをリカバリできます。プロテクションエージェントがインストールされていない仮想マシン（Virtuozzo仮想マシンを除く）に、ファイルをリカバリすることはできません。
   - Virtuozzoコンテナまたは仮想マシン。

     Virtuozzoコンテナや仮想マシンにファイルをリカバリすることができます（一部の制限あり）。これらの条件の詳細については、"Cyber Protectコンソールでファイルをリカバリする際の制限事項"（505ページ）を参照してください。
9. **[パス]** で、復元先を選択します。次のいずれかを選択できます。
   - （元のマシンにリカバリする場合）元のロケーション。
   - ターゲットマシンのローカルフォルダまたは接続ストレージ。

     注意
     シンボリックリンクはサポートされていません。

   - 復元先のコンピュータからアクセスできるネットワークフォルダ

10. **[復元を開始]** をクリックします。
11. 次のいずれかのファイル上書きオプションを選択します。
    - **[既存のファイルを上書きする]**
    - **[既存のファイルが古い場合は上書きする]**
    - **[既存のファイルを上書きしない]**

復元の進行状況は **[アクティビティ]** タブに表示されます。

クラウドストレージからのファイルのダウンロード

Web復元コンソールでは、クラウドストレージを参照したり、バックアップの内容を表示したり、バックアップされたファイルとフォルダをダウンロードしたりできます。

注意
Web Restoreコンソールにアクセスできるのは、顧客のCyber Protection管理者または顧客のテナントユーザーのみです。パートナーレベルのユーザーロールはアクセスできません。

制限事項

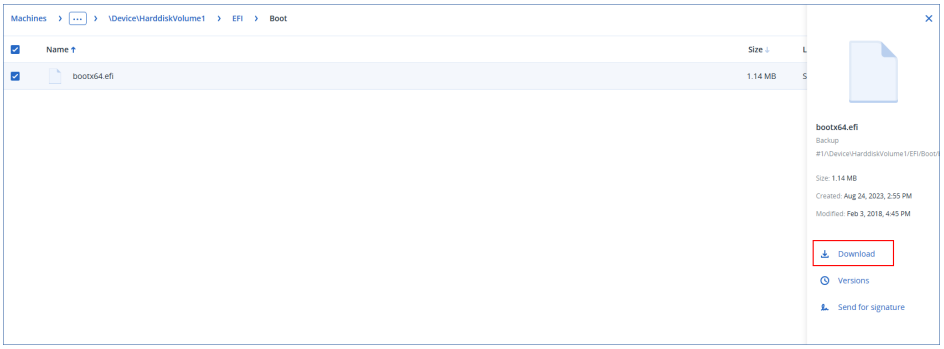
- バックアップされたディスク、ボリューム、または全体の復元ポイントをダウンロードすることはできません。
- ディスクレベルバックアップを参照する場合、論理ボリューム（LVMやLDMなど）は表示されません。
- システム状態、SQLデータベース、およびExchangeデータベースのバックアップを参照することはできません。

クラウドストレージからファイルとフォルダをダウンロードするには

1. Cyber Protectionコンソールで必要なワークロードを選択してから、**[復元]** をクリックします。
2. （複数のバックアップロケーションが利用可能な場合）バックアップロケーションを選択してから、**[その他の復元方法]** をクリックします。
3. **[ファイルのダウンロード]** をクリックしします。
4. **マシン**の下で、ワークロード名をクリックしてから、バックアップアーカイブをクリックします。
   バックアップアーカイブには、1つまたは複数のバックアップ（復元ポイント）が含まれています。
5. ダウンロードしたいファイルやフォルダが含まれているバックアップ番号（復元ポイント）をクリックし、必要な項目に移動します。
6. ダウンロードする項目のとなりにあるチェックボックスを選択します。

   注意
   複数の項目を選択すると、ZIPファイルとしてまとめてダウンロードされます。

7. **[ダウンロード]** をクリックします。



Notaryサービスを使用したファイル真正性のベリファイ

バックアップ中のノータリゼーションが有効になっている場合は、バックアップされたファイルの非改ざん性をベリファイできます。

ファイルの真正性をベリファイするには

1. 「Webインターフェースを使用したファイルの復元」セクションの手順1～6、または「クラウドストレージからのファイルのダウンロード」セクションの手順1～5の説明に従って、ファイルを選択します。
2. 選択したファイルに  アイコンが付いていることを確認します。これは、ファイルが認証済みであることを表しています。
3. 次のいずれかを実行します。
   - **[ベリファイ]** をクリックします。
     ファイルの非改ざん性がチェックされ、結果が表示されます。
   - **[証明書の取得]** をクリックします。
     Web ブラウザウィンドウで、ファイルのノータリゼーションを確認する証明書が開きます。ウィンドウには、ファイルの非改ざん性を手動でベリファイする手順も表示されます。

ASignを使用したファイルの署名

注意
この機能は、Advanced Backupパックで利用可能です。

ASignは、1つのバックアップファイルに複数のユーザーが電子署名できるようにするサービスです。この機能は、クラウドストレージに保存されているファイルレベルのバックアップに対してのみ使用できます。

1回に署名できるファイルのバージョンは1つだけです。ファイルが複数回バックアップされた場合は、署名するバージョンを選択する必要があり、そのバージョンだけが署名されます。

たとえば、次のファイルの電子署名にASignを使用できます。

- レンタルまたはリース契約
- 売買契約

- 資産購入契約
- ローン契約
- 許可書
- 財務書類
- 保険書類
- 免責同意書
- 医療書類
- 研究論文
- 製品の証明書
- 守秘義務契約書
- 合格通知
- 秘密保持契約書
- 独立請負人契約書

ファイルのいずれかのバージョンに署名するには

1. 「Webインターフェースを使用したファイルの復元」セクションの手順1～6、または「クラウドストレージからのファイルのダウンロード」セクションの手順1～5の説明に従って、ファイルを選択します。
2. 左側のパネルで正しい日付と時刻が選択されていることを確認します。
3. **[ファイルのこのバージョンに署名]** をクリックします。
4. バックアップが保存されているクラウドストレージアカウントのパスワードを指定します。プロンプトウィンドウにアカウントのログインIDが表示されます。
   ASignサービスインターフェースはWebブラウザウィンドウで開きます。
5. メールアドレスを指定して他の署名者を追加します。招待メールを送信した後に署名者を追加または削除することはできません。そのため、署名が必要な全員がリストに含まれていることを確認してください。
6. 署名者に招待メールを送るには **[署名に招待]** をクリックしてください。
   各署名者は、署名を求める電子メールメッセージを受信します。リクエストされたすべての署名者がファイルに署名すると、それはNotary（公証）サービスによって公証されて署名されます。
   各署名者がファイルに署名したとき、およびプロセス全体が完了したときに通知を受け取ります。受け取ったメールメッセージの **[詳細の表示]** をクリックすると、ASignのWebページにアクセスできます。
7. プロセスが完了したら、ASignのWebページにアクセスして、**[ドキュメントの取得]** をクリックして、以下を含む.pdfドキュメントをダウンロードします:
   - 収集した署名が記載された署名証明書ページ
   - アクティビティ履歴が掲載された監査証跡ページ: 署名者に招待状が送られた日時や、各署名者がファイルに署名した日時など

ブータブルメディアを使用したファイルの復元

ブータブル メディアの作成方法については、「ブータブル メディアの作成」を参照してください。

ブータブル メディアを使用してファイルを復元するには

1. ブータブル メディアを使用して復元先のコンピュータを起動します。
2. 使用するメディアの種類によって **[このコンピュータをローカルで管理]** クリックするか、**[レスキュー ブータブル メディア]** を2回クリックします。
3. プロキシサーバーがネットワークで有効な場合、**[ツール]** > **[プロキシサーバー]** をクリックして、プロキシサーバーホスト名/IP アドレス、ポート、および資格情報を指定します。それ以外の場合は、この手順をスキップします。
4. （オプション）WindowsまたはLinuxをリカバリするときは、**[ツール]** > **[Cyber Protectionサービスでメディアを登録]** をクリックして、メディアをダウンロードしたときに取得した登録トークンを指定します。この場合、手順7に説明されているように、クラウドストレージにアクセスするために資格情報または登録コードを入力する必要はありません。
5. [ようこそ] 画面で、 **[復元]** をクリックします。
6. **[データの選択]** をクリック後、**[参照]** をクリックします。
7. バックアップのロケーションを指定します。
   - クラウドストレージから復元するには、**[クラウドストレージ]** を選択します。バックアップされたコンピュータに割り当てられているアカウントの資格情報を入力します。

     WindowsまたはLinuxを復元するときは、資格情報の代わりに登録コードのリクエストを選択できます。**[登録コードを使用]** > **[コードを要求]** をクリックします。ソフトウェアに登録リンクと登録コードが表示されます。リンクとコードをコピーして、ほかのマシンで登録手順を実行できます。登録コードの有効期限は 1 時間です。
   - ローカル フォルダまたはネットワークフォルダから復元するには、**[ローカル フォルダ]** または **[ネットワークフォルダ]** のフォルダを参照します。
   - Microsoft Azure、Amazon S3、Wasabi、S3 互換などのパブリッククラウドストレージ上のバックアップロケーションから復元するには、まず **[Cyber Protectionサービスでメディアを登録]** をクリックし、次にWebインターフェイスを使用して復元を設定します。Webンターフェイスを使用したリモートでのメディア管理の詳細については、"ブータブルメディアのリモート操作"（708 ページ）を参照してください。

   [OK] をクリックし、選択を確定します。
8. 復元するバックアップデータを選択します。バックアップデータのパスワードを要求される場合は、設定したパスワードを入力します。
9. **[バックアップ内容]** で **[フォルダ/ファイル]** を選択します。
10. 復元するデータを選択します。**[OK]** をクリックし、選択を確定します。
11. **[復元先]** でフォルダを指定します。任意で、復元先のファイルが復元元よりも新しいバージョンであった場合に上書きを禁止したり、復元対象から一部のファイルを除外したりできます。
12. （オプション）その他の設定が必要な場合、**[復元オプション]** をクリックして、設定します。
13. **[OK]** をクリックして復元を開始します。

ローカルバックアップからファイルを抽出

バックアップの内容を参照し、必要なファイルを抽出できます。

要件

- この機能は、Windowsでエクスプローラを使用する場合のみ利用できます。
- バックアップのファイルシステムは、次のいずれかである必要があります:FAT16、FAT32、NTFS、ReFS、Ext2、Ext3、Ext4、XFS、HFS+。

前提条件

- バックアップの参照元のマシンに保護エージェントをインストールしておく必要があります。
- バックアップは、ローカルフォルダまたはネットワーク共有（SMB/CIFS）に格納する必要があります。

バックアップからファイルを抽出する手順は、次のとおりです。

1. エクスプローラで、バックアップロケーションを参照します。
2. バックアップファイルをダブルクリックします。ファイル名は次のテンプレートに基づいています。

   <マシン名> - **<保護計画GUID>**
3. バックアップが暗号化されている場合は、暗号化パスワードを入力します。それ以外の場合は、この手順をスキップします。

   エクスプローラに、復元ポイントが表示されます。
4. 復元ポイントをダブルクリックします。

   エクスプローラに、バックアップデータが表示されます。
5. 必要なフォルダを参照します。
6. 必要なファイルを、ファイルシステム上の任意のフォルダにコピーします。

Cyber Protectコンソールでファイルをリカバリする際の制限事項

コンプライアンスモードのテナント

コンプライアンスモードのテナント対しCyber Protectコンソールではバックアップをリカバリできません。このようなバックアップをリカバリする方法の詳細については、"コンプライアンスモードでテナントのバックアップを復元する"（1050ページ）を参照してください。

VirtuozzoコンテナまたはVirtuozzo仮想マシンへの復元

- QEMUゲストエージェントがターゲット仮想マシンにインストールされている必要があります。
- （コンテナへのリカバリの場合のみ）コンテナ内のマウントポイントは、リカバリのターゲットとして使用できません。例えば、コンテナにマウントされた2台目のハードディスクやNFS共有にファイルをリカバリすることはできません。
- Windows仮想マシンにファイルをリカバリする場合で、かつ"ファイルレベルのセキュリティ"（511ページ）リカバリオプションが有効になっている場合、復元されたファイルにはアーカイブビット属性が設定されます。
- リカバリがWindows Server 2012以前およびWindows 7以前のマシンで実行されていて、ファイル名に非ANSI文字が含まれる場合、これらのファイルは間違った名前でリカバリされます。

- Virtuozzo Hybrid Serverで実行されるCentOSやRed Hat Enterprise Linuxの仮想マシンにファイルをリカバリするには、次のようにqemu-gaファイルを編集する必要があります。
  - ターゲット仮想マシンで、/etc/sysconfig/に移動し、編集用にqemu-gaファイルを開きます。
  - 以下の行に移動し、等号（=）以下をすべて削除します。

    ```
    BLACKLIST_RPC=
    ```

  - 次のコマンドを実行して、QEMUゲストエージェントを再起動します:

    ```
    systemctl restart qemu-guest-agent
    ```

システム状態の復元

注意
コンプライアンスモードのテナント対しCyber Protectコンソールではバックアップをリカバリできません。このようなバックアップをリカバリする方法の詳細については、"コンプライアンスモードでテナントのバックアップを復元する"（1050ページ）を参照してください。

1. システム状態を復元するマシンを選択します。
2. **[復元]** をクリックします。
3. システム状態の復元ポイントを選択します。復元ポイントは、保存場所でフィルタされます。
4. **[システム状態を復元]** をクリックします。
5. システム状況をバックアップされたバージョンで上書きすることを確認します。

復元の進行状況は **[アクティビティ]** タブに表示されます。

ESXi構成の復元

ESXi構成を復元する場合は、Linuxベースのブータブルメディアが必要となります。ブータブルメディアの作成方法については、「"物理的なブータブルメディアの作成"（691ページ）」を参照してください。

ESXi構成を元のホスト以外に復元する場合で、元のホストが依然としてvCenter Serverに接続されている場合は、このホストのvCenter Serverとの接続を切断し、復元中に不測の事態が発生しないようにします。元のホストを復元されたホストと一緒に維持する場合、復元が完了した後で再度追加できます。

ホストで実行中の仮想コンピュータは、ESXi構成のバックアップ内に含まれません。バックアップと復元をそれぞれ個別に行えます。

ESXi構成を復元する手順

1. ブータブル メディアを使用して復元先のコンピュータを起動します。
2. **[このコンピュータをローカルで管理]** をクリックします。
3. [ようこそ] 画面で、 **[復元]** をクリックします。
4. **[データの選択]** をクリック後、**[参照]** をクリックします。
5. バックアップのロケーションを指定します。

- [**ローカル フォルダ**] または [**ネットワークフォルダ**] のフォルダを参照します。

  [**OK**] をクリックし、選択を確定します。
6. [**表示**] で [**ESXi構成**] を選択します。
7. 復元するバックアップデータを選択します。バックアップデータのパスワードを要求される場合は、設定したパスワードを入力します。
8. [**OK**] をクリックします。
9. [**新しいデータストアで使用するディスク**] で以下を実行します。
   - [**ESXiの復元先**] の下でホスト構成の復元先とするディスクを選択します。元のホストに構成を復元する場合、デフォルトでオリジナル ディスクが選択されます。
   - （オプション）[**新しいデータストアで使用**] の下で新しいデータストアを作成するディスクを選択します。選択されたディスクの上にあるデータがすべて失われるため、注意してください。既存のデータストアに仮想コンピュータを保存する場合は、ディスクを選択しません。
10. 新しいデータストアのディスクが選択されている場合、データストアの作成方法は [**新しいデータストアを作成する方法**] の[**ディスクごとに1つのデータストアを作成**] または [**選択されたすべてのHDDに1つのデータストアを作成**] を選択します。
11. （オプション）[**ネットワークマッピング**] で物理ネットワークアダプターに対するバックアップ内の仮想スイッチの自動マッピング結果を変更できます。
12. （オプション）その他の設定が必要な場合、[**復元オプション**] をクリックして、設定します。
13. [**OK**] をクリックして復元を開始します。

復元オプション

復元設定時に復元オプションを変更するには [**復元オプション**] をクリックします。

使用可能な復元オプション

使用可能な復元オプションのセットは次の条件によって異なります。

- 復元を実行するエージェントが動作する環境（Windows、Linux、macOS、またはブータブルメディア）。
- 復元するデータの種類（ディスク、ファイル、仮想コンピュータ、アプリケーションデータ）。

次の表は、使用可能な復元オプションを示しています。

	ディスク			ファイル				仮想コンピュータ	SQLおよびExchange
	Windows	Linux	ブータブル メディア	Windows	Linux	macOS	ブータブル メディア	ESXi、Hyper-V、Virtuozzo	Windows
バックアップのベリ	+	+	+	+	+	+	+	+	+

ファイ									
起動モード	+	-	-	-	-	-	-	+	-
ファイルの日付と時刻	-	-	-	+	+	+	+	-	-
エラー処理	+	+	+	+	+	+	+	+	+
ファイルの除外	-	-	-	+	+	+	+	-	-
ファイルレベルのセキュリティ	-	-	-	+	-	-	-	-	-
Flashback	+	+	+	-	-	-	-	+	-
フルパスの復元	-	-	-	+	+	+	+	-	-
マウントポイント	-	-	-	+	-	-	-	-	-
パフォーマンス	+	+	-	+	+	+	-	+	+
処理の前後のコマンド	+	+	-	+	+	+	-	+	+
SIDの変更	+	-	-	-	-	-	-	-	-
VMの電源管理	-	-	-	-	-	-	-	+	-
Windowsイベントログ	+	-	-	+	-	-	-	Hyper-Vのみ	+

バックアップのベリファイ

このオプションでは、データをバックアップからリカバリする前にバックアップが破損していないことを検証するかどうかを定義します。この処理は、プロテクションエージェントによって実行されます。

デフォルト設定:**無効**。

チェックサム検証経由の検証の詳細については、"チェックサムのベリファイ"（200ページ）を参照してください。

注意
サービスプロバイダーが選択する設定によっては、クラウドストレージにバックアップするときに検証を利用できない場合があります。

起動モード

このオプションは、Windows オペレーティングシステムが含まれるディスクレベルバックアップから物理マシンまたは仮想マシンを復元するときに有効です。

このオプションを使用すると、復元後に Windows で使用される起動モード（BIOS または UEFI） を選択できます。元のマシンの起動モードと選択した起動モードが異なる場合、このソフトウェアは次のように動作します。

- 選択した起動モード（BIOS の場合は MBR、UEFI の場合は GPT）に従って、システムボリュームの復元先となるディスクを初期化します。
- 選択した起動モードを使用して起動できるように Windows オペレーティングシステムを調整します。

デフォルト設定:**ターゲットマシン。**

次の中からひとつ選択できます。

- **ターゲットマシン**
  ターゲットマシン上で実行されているエージェントによって、現在 Windows で使用されている起動モードが検出され、この起動モードに従って調整が行われます。
  以下に示す制限が適用されない限り、自動的にブータブルシステムになるため、これが一番安全な値です。**[起動モード]** オプションはブータブルメディアに存在しないため、メディア上のエージェントは常にこの値が選択されているかのように動作します。
- **バックアップしたマシン**
  ターゲットマシンで実行されているエージェントによって、バックアップから起動モードが読み取られ、この起動モードに従って調整が行われます。これによって、このマシンで別の起動モードが使用されていても、別のマシン上でシステムを復元し、バックアップされたマシンのディスクを置き換えることができます。
- **BIOS**
  ターゲットマシンで実行されているエージェントによって、BIOS を使用するための調整が行われます。
- **UEFI**
  ターゲットマシンで実行されているエージェントによって、UEFI を使用するための調整が行われます。

設定が変更されたら、ディスクマッピング手順が繰り返されます。これには時間がかかります。

推奨事項

UEFI と BIOS の間で Windows を転送する必要がある場合:

- システムボリュームが存在するディスク全体を復元します。既存のボリューム上のシステムボリュームのみを復元する場合、エージェントはターゲットディスクを適切に初期化できなくなります。
- BIOS では 2 TB を超えるディスク領域を使用できないことに注意してください。

制限事項

- UEFI と BIOS の間での転送は次の環境でサポートされています。
  - Windows 7以降の64ビットのWindowsオペレーティングシステム
  - Windows Server 2008 SP1 以降の 64 ビットの Windows Server オペレーティングシステム
- バックアップがテープデバイスに保存されている場合、UEFI と BIOS の間での転送はサポートされません。

UEFI と BIOS の間での転送がサポートされていない場合、エージェントは、**[バックアップしたマシン]** 設定が選択されているかのように動作します。ターゲットマシンで UEFI と BIOS の両方がサポートされている場合、元のマシンに対応する起動モードを手動で有効にする必要があります。そうしないと、システムが起動しなくなります。

ファイルの日付と時刻

このオプションは、ファイルを復元する場合にのみ有効です。

このオプションでは、ファイルの日付と時刻をバックアップから復元するか、現在の日付と時刻を割り当てるかを定義します。

このオプションを有効にした場合、ファイルに現在の日付と時刻が割り当てられます。

デフォルト設定:**有効**。

エラー処理

これらのオプションによって、復元中に発生する可能性があるエラーを処理する方法を指定できます。

エラーが発生した場合は再試行する

デフォルト設定:**有効。試行回数:30。試行間隔:30 秒。**

復元可能なエラーが発生した場合、失敗した処理が再試行されます。試行間隔および試行回数を設定できます。試行は、処理が成功するか、または指定した回数の試行が行われると停止します。

処理中にメッセージやダイアログを表示しない（サイレントモード）

デフォルト設定:**無効**。

サイレントモードをオンにすると、ユーザーによる操作を必要とする状況が可能な限り自動的に処理されます。ユーザーによる操作なしに処理を続行できない場合、その処理は失敗します。処理の詳細（エラーがある場合は、それも含む）は、処理のログに記載されます。

再起動を伴う復元が失敗する場合、システム情報を保存する

このオプションは、WindowsまたはLinuxが実行されている物理マシンへのディスクまたはボリューム復元で有効です。

デフォルト設定:**無効**。

このオプションが有効な場合、ローカルディスク（ターゲットマシンのフラッシュまたはHDDドライブ）のフォルダまたは、ログ、システム情報、およびクラッシュダンプファイルが保存されるネットワーク共有の中のフォルダを指定できます。このファイルは、テクニカルサポートの担当者が問題を特定する助けとなります。

ファイルの除外

このオプションは、ファイルを復元する場合にのみ有効です。

このオプションでは、復元処理中にスキップして、復元する項目の一覧から除外するファイルとフォルダを定義します。

注意
除外は、復元するデータ項目の選択よりも優先されます。たとえば、MyFile.tmp というファイルの復元を選択し、すべての .tmp ファイルを除外する場合、MyFile.tmp というファイルは復元されません。

ファイルレベルのセキュリティ

このオプションは、NTFS 形式のボリュームのディスクレベルとファイルレベルのバックアップからファイルを復元する場合に有効です。

このオプションでは、ファイルに対するNTFSのアクセス許可をファイルと共に復元するかどうかを定義します。

デフォルト設定:**有効**。

アクセス許可を復元するか、ファイルの復元先のフォルダの NTFS アクセス許可をファイルに継承するかを選択できます。

Flashback

このオプションはMac向けを除き、物理マシンおよび仮想マシンのディスクとボリュームを復元する場合に有効です。

このオプションは、復元するディスクのボリュームレイアウトがターゲットディスクのボリュームレイアウトと完全に一致する場合にのみ機能します。

このオプションが有効な場合、バックアップのデータとターゲットディスクのデータの差分のみが復元されます。これにより、物理マシンおよび仮想マシンの復元が高速化されます。データはブロックレベルで比較されます。

物理マシンを復元するときの事前設定は次のとおりです:**無効**。

仮想マシンを復元するときの事前設定は次のとおりです:**有効**。

フルパスの復元

このオプションは、ファイルレベルのバックアップからデータを復元する場合にのみ有効です。

このオプションを有効にした場合、ファイルへのフルパスが復元先で再作成されます。

デフォルト設定:**無効**。

マウントポイント

このオプションは、Windowsでファイルレベルのバックアップからデータを復元する場合にのみ有効です。

マウントされたボリュームに保存され、[マウントポイント] オプションを有効にしてバックアップされたファイルとフォルダをリカバリする場合は、このオプションを有効にします。

デフォルト設定:**無効**。

このオプションは、フォルダ階層内でマウントポイントより上位にあるフォルダを復元対象に選択する場合にのみ有効です。マウントポイント内のフォルダ、またはマウントポイント自体を復元する場合、**[マウントポイント]** オプションの値にかかわりなく、選択したアイテムがリカバリされます。

注意
復元時にボリュームがマウントされていない場合、データはバックアップ時にマウント ポイントであったフォルダに直接復元されることに注意してください。

パフォーマンス

このオプションでは、オペレーティングシステム内の復元プロセスの優先度を定義します。

選択可能な設定は次のとおりです。**[低]**、**[通常]**、**[高]**。

デフォルト設定:**通常**。

システムで実行されるプロセスの優先度によって、そのプロセスに割り当てられるCPUやシステムのリソース量が決まります。復元の優先度を下げると、他のアプリケーションのためのリソースを増やすことができます。復元の優先度を上げると、復元を実行するアプリケーションに割り当てるリソースを増やすようにオペレーティング システムに要求することによって、復元の処理速度が上がる場合があります。ただし、全体的なCPUの使用率およびディスク入出力速度、ネットワークトラフィックなどその他の要素によってその効果は異なります。

処理の前後のコマンド

このオプションによって、データ復元の前後に自動的に実行されるコマンドを定義できます。

処理の前後に実行するコマンドを使用する方法の例:

- **Checkdisk**コマンドを起動し、復元の開始前または終了後に論理ファイルシステムのエラー、物理エラー、または不良セクタを見つけて修復します。

「pause」などのユーザーの入力を必要とするような対話型のコマンドはサポートされません。

再起動を伴う復元の場合、復元後に実行するコマンドは実行されません。

復元前に実行するコマンド

復元処理を開始する前に実行するコマンド/バッチ ファイルを指定する手順は、次のとおりです。

1. **[復元前にコマンドを実行]** スイッチを有効にします。
2. **[コマンド...]** フィールドにコマンドを入力するか、バッチファイルを参照します。「pause」などのユーザーの入力を必要とするような対話型のコマンドはサポートされません。
3. **[作業ディレクトリ]** フィールドで、コマンド/バッチファイルを実行するディレクトリのパスを指定します。
4. **[引数]** フィールドで、必要に応じて、コマンドを実行する際の引数を指定します。
5. 処理内容に応じて、次の表で説明するオプションから、適切なオプションを選択します。
6. **[完了]** をクリックします。

チェックボックス	**選択内容**			
[コマンドの実行に失敗した場合、復元を失敗させる]*	オン	オフ	オン	オフ
[コマンドの実行が完了するまで復元を行わない]	オン	オン	オフ	オフ
結果				
	[事前設定] コマンドが正常に実行された後にのみ復元を実行します。コマンドの実行に失敗した場合、復元を失敗させます。	コマンド実行の失敗または成功にかかわらず、コマンドの実行後に復元を実行します。	なし	コマンドの実行結果にかかわらず、コマンドの実行と並行して復元を実行します。

* 終了コードがゼロでない場合、コマンドは失敗したと認識されます。

復元後に実行するコマンド

復元の完了後に実行するコマンド/実行可能ファイルを指定する手順は、次のとおりです。

1. **[復元後にコマンドを実行する]** スイッチを有効にします。
2. **[コマンド...]** フィールドにコマンドを入力するか、バッチファイルを参照します。
3. **[作業ディレクトリ]** フィールドで、コマンド/バッチファイルを実行するディレクトリのパスを指定します。
4. **[引数]** フィールドで、必要に応じて、コマンドを実行する際の引数を指定します。
5. コマンドが正常に実行されることが重要な場合、**[コマンドの実行に失敗した場合、復元を失敗させる]** チェックボックスをオンにします。終了コードがゼロでない場合、コマンドは失敗したと認識されます。コマンドの実行に失敗した場合、復元のステータスは **[エラー]** として設定されます。
   このチェックボックスがオフになっていると、コマンドの実行結果は復元の失敗または成功に影響しません。コマンドの実行結果は、**[アクティビティ]** タブを確認するとトラックできます。
6. **[完了]** をクリックします。

注意
再起動を伴う復元の場合、復元後に実行するコマンドは実行されません。

SIDの変更

このオプションはWindows 8.1/Windows Server 2012 R2以前の復元で有効です。

このオプションは、仮想マシンへの復元をVMwareエージェント、Hyper-Vエージェント、Scale Computing HC3エージェント、またはoVirtエージェントで実行する場合は有効になりません。

デフォルト設定:**無効**。

このソフトウェアは、復元されたオペレーティングシステムの一意のセキュリティ識別子（コンピュータSID）を生成できます。このオプションは、コンピュータSIDに依存するサードパーティ製のソフトウェアの操作性を確認する場合のみ必要になります。

Microsoftは、展開または復元されたシステムでのSIDの変更は、公式にはサポートしていません。そのため、このオプションは自己責任で使用してください。

VMの電源管理

復元先の仮想マシンが、VMwareエージェント、Hyper-Vエージェント、Virtuozzoエージェント、Scale Computing HC3エージェント、またはoVirtエージェントによって実行されている場合は、これらのオプションが効果的です。

復元の開始時にターゲット仮想コンピュータの電源をオフにする

デフォルト設定:**有効**。

既存の仮想コンピュータがオンラインの場合は復元先として利用できないため、復元が開始されるとすぐに電源は自動的にオフになります。ユーザーはコンピュータから切断され、保存されていないデータは失われます。

復元前に手動で仮想コンピュータの電源をオフにする場合は、このオプションのチェックボックスをオフにしてください。

復元が完了したら、復元先の仮想コンピュータの電源をオンにします。

デフォルト設定:**無効**。

コンピュータがバックアップから別のコンピュータに復元された後に、既存のコンピュータのレプリカがネットワーク上に表示される場合があります。安全のために必要な予防措置を行った後で、復元された仮想コンピュータの電源を手動でオンにします。

Windowsイベントログ

このオプションは、Windows オペレーティング システムの場合にのみ有効です。

このオプションでは、エージェントが復元操作のイベントをWindowsのアプリケーションイベントログに記録する必要があるかどうかを定義します（このログを表示するには、eventvwr.exeを実行するか、

[コントロールパネル] > **[管理ツール]** > **[Event Viewer]** の順に選択します）。ログに記録するイベントにフィルタを設定することができます。

デフォルト設定:**無効**。

バックアップの操作

バックアップストレージタブ

[バックアップストレージ] タブでは、オフラインマシンのバックアップ、Cyber Protectionサービス未登録マシンのバックアップ、Microsoft Azureなどパブリッククラウドへのバックアップ、また孤立したバックアップ[1]を含め、すべてのバックアップにアクセスできます。

acrocmdを介して作成されたバックアップには、孤立状態のマークが付けられます。12.5バージョンの製品で作成されたバックアップも孤立状態であるとみなされます。

注意
なお、孤立状態のバックアップも課金対象となります。

共有のロケーション（SMBやNFS共有など）に保存されたバックアップはそのロケーションに閲覧権限のあるすべてのユーザーが表示できます。

Windowsでは、バックアップファイルは親フォルダからアクセス許可を継承します。従って、このフォルダの読み取り許可を制限することをお勧めします。

クラウドストレージではユーザーは独自のバックアップにのみアクセスできます。

管理者は、アカウント向けのクラウドストレージを選択することで、特定の部署または企業、およびその子グループに属する任意のアカウントの代理として、バックアップを表示できます。クラウドからデータを取得するために使用するデバイスを選択するには、**[参照元マシン]** 行で、**[変更]** をクリックします。**[バックアップストレージ]** タブには、選択済みアカウントに登録されたすべてのマシンのバックアップが表示されます。

クラウドMicrosoft 365エージェントで作成されたバックアップと、Google Workspaceデータのバックアップは、**クラウドストレージ**のロケーションではなく、**[クラウドアプリケーションバックアップ]** という別のセクションに表示されます。

保護計画で使用されるバックアップロケーションが、自動的に **[バックアップストレージ]** タブに追加されます。カスタムのフォルダ（取り外し可能なUSBデバイスなど）をバックアップロケーションのリストに追加するには、**[参照]** をクリックしてフォルダパスを指定します。

ファイルマネージャーを使用してバックアップを追加または削除した場合は、ロケーション名の横にあるギアアイコンをクリックして、**[更新]** をクリックします。

[1]孤立したバックアップは、いずれの保護計画とも関連付けられていないバックアップです。

警告
バックアップファイルを手動で編集しようとしないでください。ファイルが破損し、バックアップが利用できなくなる可能性があります。また、バックアップファイルを手動で移動するのではなく、バックアップのレプリケーションを使用することをお勧めします。

バックアップロケーションにバックアップされたことがあるマシンすべてがサービスから削除されると、そのロケーション（クラウド ストレージの場合を除く）が **[バックアップストレージ]** タブに表示されなくなります。そのロケーションに保存されたバックアップに対する支払いが不要になったことを確認できます。そのロケーションへのバックアップが発生すると、ロケーションとそこに保存されたバックアップすべてが再度追加されます。

[バックアップストレージ] タブでは、以下の条件を使用してバックアップのリストを絞り込むことができます。

- **[フォレンジックデータのみ]** - フォレンジックデータのあるバックアップのみが表示されます。
- **パッチ管理で作成されたアップデート前のバックアップのみ** - パッチインストール前のパッチ管理実行中に作成されたバックアップのみが表示されます。

バックアップストレージタブを使用して復元ポイントを選択するには

1. **[バックアップストレージ]** タブで、バックアップが保存されるロケーションを選択します。
   選択した場所でアカウントが表示できるすべてのバックアップが表示されます。バックアップはグループで統合されます。グループ名は次のテンプレートに基づいています。
   <マシン名> - <保護計画名>
2. データを復元するグループを選択します。
3. （オプション）**[参照元マシン]** の横の **[変更]** をクリックし、別のコンピュータを選択します。一部のバックアップは特定のエージェントによってのみ参照できます。たとえば、Microsoft SQL Server データベースのバックアップを参照するには、エージェントfor SQLを実行するコンピュータを選択する必要があります。

   重要
   [参照元マシン] は物理マシンのバックアップから復元するためのデフォルトの場所です。リカバリポイントを選択し、**[復元]** をクリックした後、**[復元先のコンピュータ]** 設定をオンにし、この特定のコンピュータに復元することを確認します。復元先を変更するには、**[参照元のコンピュータ]** で別のコンピュータを選択します。

4. **[バックアップの表示]** をクリックします。
5. リカバリ ポイントを選択します。

バックアップのロケーションを追加するには

注意
この処理は、オンラインエージェントを利用している場合にのみ実行できます。

[バックアップストレージ] タブで、**[ロケーションを追加]** をクリックします。

以下のロケーションのタイプからロケーションを選択し、**[完了]** をクリックします：

- ローカルフォルダ
- ネットワークフォルダ
- Secure Zone
- NFSフォルダ
- パブリッククラウド

バックアップからのボリュームのマウント

ディスクレベルのバックアップからボリュームをマウントすると、物理ディスクと同様にボリュームにアクセスできます。

読み込み/書き込みレベルでボリュームをマウントすると、バックアップコンテンツの変更（ファイルまたはフォルダの保存、移動、作成、削除）、および単一のファイルで構成されている実行可能ファイルを実行できます。このモードでは、バックアップコンテンツに加えた変更を含む増分バックアップが作成されます。その後のバックアップには、これらの変更が含まれないことに注意してください。

要件

- この機能は、Windowsでエクスプローラを使用する場合のみ利用できます。
- マウント操作を実行するコンピュータには、Windowsエージェントがインストールされている必要があります。
- バックアップのファイルシステムは、コンピュータが実行しているWindowsバージョンによりサポートされている必要があります。
- バックアップは、ローカルフォルダ、ネットワーク共有（SMB/CIFS）、またはSecure Zoneに格納されている必要があります。

使用例

- データの共有

  マウントされたボリュームは、ネットワーク経由で容易に共有できます。
- 「応急処置的な」データベース復元ソリューション

  最近障害が発生したマシンのSQLデータベースを含むボリュームをマウントします。これにより、障害が発生したコンピュータが復元されるまでの、データベースへのアクセスが可能になります。このアプローチは、SharePoint Explorerを使用したMicrosoft SharePointデータの粒度復元のためにも使用できます。
- オフラインのウイルス駆除

  コンピュータが感染した場合、そのバックアップをマウントし、ウイルス対策プログラムを使用して駆除し（または、感染していない最新のバックアップを探し）、そのバックアップからコンピュータを復元します。
- エラーチェック

  ボリュームのサイズ変更を伴う復元が失敗した場合、その理由は、バックアップされたファイルシステムのエラーである可能性があります。バックアップを読み取り/書き込みモードでマウントします。次に、`chkdsk /r`コマンドを使用して、マウントされたボリュームにエラーがないかどうかを

チェックします。エラーが修復され、新しい増分バックアップが作成されたら、このバックアップからシステムをリカバリします。

バックアップからボリュームをマウントする手順

1. エクスプローラで、バックアップロケーションを参照します。
2. バックアップファイルをダブルクリックします。ファイル名は次のテンプレートに基づいています。

   <マシン名> - **<保護計画GUID>**
3. バックアップが暗号化されている場合は、暗号化パスワードを入力します。それ以外の場合は、この手順をスキップします。

   エクスプローラに、復元ポイントが表示されます。
4. 復元ポイントをダブルクリックします。

   エクスプローラに、バックアップボリュームが表示されます。

   注意
   ボリュームをダブルクリックして、そのコンテンツを参照します。バックアップのファイルとフォルダを、ファイルシステム上の任意のフォルダにコピーできます。
5. マウントするボリュームを右クリックして、次のオプションのいずれかを選択します。
   a. **マウント**

      注意
      アーカイブ内の最後のバックアップ（バックアップチェーン）は、読み取り/書き込みモードでのみマウントできます。

   b. **読み取り専用モードでマウント**
6. バックアップがネットワーク共有に格納されている場合、ログイン情報を指定します。それ以外の場合は、この手順をスキップします。

   ソフトウェアにより、選択したボリュームがマウントされます。最初の未使用のドライブ文字がボリュームに割り当てられます。

ボリュームをアンマウントする手順

1. エクスプローラを使用して、**[コンピュータ]**（Windows 8.1以降では **[PC]**）を参照します。
2. マウントされたボリュームを右クリックします。
3. **[アンマウント]** をクリックします。
4. （オプション） ボリュームが読み込み/書き込みレベルでマウントされており、その内容が変更されている場合は、その変更を含めた増分バックアップを作成するかどうかを選択します。それ以外の場合は、この手順をスキップします。

ソフトウェアにより、選択したボリュームがアンマウントされます。

バックアップのベリファイ

バックアップを検証して、そのバックアップからデータをリカバリできることを検証します。この操作の詳細については、「"ベリファイ"（197ページ）」を参照してください。

注意
この機能は、Advanced Backupパックの一部として**Advanced Backup - Servers**または**Advanced Backup - NASの**クォータが有効になっているカスタマーテナントで使用できます。

バックアップを検証するには

1. バックアップされたワークロードを選択します。
2. **[復元]** をクリックします。
3. リカバリ ポイントを選択します。復元ポイントは、保存場所でフィルタされます。
   ワークロードがオフラインになっている場合、復元ポイントは表示されません。次の手順のいずれかを実行します。
   - バックアップのロケーションがクラウドまたは共有ストレージである（つまり他のエージェントからアクセスできる）場合は、**[マシンを選択]** をクリックして、オンラインになっているターゲットワークロードを選択してから、復元ポイントを選択します。
   - [バックアップストレージ] タブで復元ポイントを選択します。そのバックアップの詳細については、「"バックアップストレージタブ"（515ページ）」を参照してください。
4. ギアアイコンをクリックし、**[検証する]** をクリックします。
5. 検証を実行するエージェントを選択します。
6. 検証方法を選択します。
7. バックアップが暗号化されている場合は、暗号化パスワードを指定します。
8. **[開始]** をクリックします。

バックアップのエクスポート

エクスポート操作によって、バックアップの自己完結型のコピーを指定したロケーションに作成します。元のバックアップは変更されません。バックアップのエクスポートにより、特定のバックアップを増分および差分バックアップのチェーンと区別することができます。それにより、迅速な復元、リムーバブルメディアや取り外し可能なメディアへの書き込みなどの目的に使用できます。

注意
この機能は、Advanced Backupパックの一部として**Advanced Backup - Servers**または**Advanced Backup - NASの**クォータが有効になっているカスタマーテナントで使用できます。

エクスポート操作の結果は常に完全バックアップです。異なるロケーションへバックアップチェーン全体のレプリケーションを行い、複数の復元ポイントを保存したい場合、バックアップのレプリケーション計画を使用します。この計画の詳細については、「"バックアップのレプリケーション"（194ページ）」を参照してください。

エクスポートされたバックアップのバックアップファイル名は、シーケンス番号を除いて、元のバックアップのファイル名と同じになります。同じバックアップチェーンから複数のバックアップが同じロケーションへエクスポートされると、最初のものを除き、4桁のシーケンス番号がすべてのバックアップのファイル名に付加されます。

エクスポートされたバックアップは、元のバックアップから暗号化設定とパスワードを継承します。暗号化されたバックアップのエクスポートを行う際は、パスワードを指定する必要があります。

バックアップをエクスポートするには

1. バックアップされたワークロードを選択します。
2. **[復元]** をクリックします。
3. リカバリ ポイントを選択します。復元ポイントは、保存場所でフィルタされます。
   ワークロードがオフラインになっている場合、復元ポイントは表示されません。次の手順のいずれかを実行します。
   - バックアップのロケーションがクラウドまたは共有ストレージである（つまり他のエージェントからアクセスできる）場合は、**[マシンを選択]** をクリックして、オンラインになっているターゲットワークロードを選択してから、復元ポイントを選択します。
   - [バックアップストレージ] タブで復元ポイントを選択します。そのバックアップの詳細については、「"バックアップストレージタブ"（515ページ）」を参照してください。
4. ギアアイコンをクリックし、**[エクスポート]** をクリックします。
5. エクスポートを実行するエージェントを選択します。
6. バックアップが暗号化されている場合は、暗号化パスワードを指定します。それ以外の場合は、この手順をスキップします。
7. エクスポート先を指定します。
8. **[開始]** をクリックします。

バックアップの削除

バックアップアーカイブには、1つまたは複数のバックアップが含まれます。アーカイブ内の特定のバックアップ（復元ポイント）またはアーカイブ全体を削除できます。

バックアップアーカイブを削除すると、その中のすべてのバックアップが削除されます。ワークロードのすべてのバックアップを削除すると、これらのバックアップを含むバックアップアーカイブが削除されます。

バックアップの削除は、Cyber Protect コンソールの **[デバイス]** タブと **[バックアップストレージ]** タブを使用して行うことができます。また、Web Restoreコンソールを使用して、クラウドストレージからバックアップを削除することもできます。

警告
不変ストレージが無効になっている場合、バックアップデータは完全に削除され、リカバリできません。

バックアップまたはバックアップアーカイブを削除するには

[デバイス] タブでの操作

この手順は、オンラインのワークロードにのみ適用されます。

1. Cyber Protectコンソールで **[デバイス]** > **[すべてのデバイス]** に進みます。
2. 削除するワークロードバックアップを選択します。

3. **[復元]** をクリックします。
4. （複数のバックアップ先がある場合）バックアップロケーションを選択します。
5. （ワークロードのすべてのバックアップを削除するには）**[すべて削除]** をクリックします。
   すべてのバックアップを削除すると、これらのバックアップを含むバックアップアーカイブも削除されます。
6. （特定のバックアップを削除するには）削除するバックアップ（復元ポイント）を選択し、**[アクション]** > **[削除]** をクリックします。
7. （すべてのバックアップを削除する場合）チェックボックスを選択し、**[削除]**をクリックして決定を確定します。
8. （特定のバックアップを削除する場合）**[削除]** をクリックして決定を確定します。

[バックアップストレージ] タブでの操作

この手順は、オンラインおよびオフラインのワークロードに適用されます。

1. Cyber Protectコンソールで、**[バックアップストレージ]** に移動します。
2. バックアップを削除する場所を選択します。
3. バックアップを削除するバックアップアーカイブを選択します。
   アーカイブ名には以下のテンプレートが使用されます。
   - 非クラウドツークラウドバックアップのアーカイブ: <ワークロード名> - <保護計画名>
   - クラウドツークラウドバックアップのアーカイブ: <ユーザー名> または <ドライブ名> または <チーム名> - <クラウドサービス> - <保護計画名>
4. （バックアップアーカイブ全体を削除するには）**[削除]** をクリックします。
   バックアップアーカイブを削除すると、そのアーカイブ内のすべてのバックアップが削除されます。
5. （バックアップアーカイブ内の特定のバックアップを削除するには）**[バックアップの表示]** をクリックします。
   a. 削除するバックアップ（復元ポイント）を選択します。
   b. **[Actions]**>**[削除]** をクリックします。
6. （バックアップアーカイブを削除する場合）チェックボックスを選択し、**[削除]**をクリックして決定を確定します。
7. （特定のバックアップを削除する場合）**[削除]** をクリックして決定を確定します。

Web Restoreコンソール内

この手順は、クラウドストレージ内のバックアップアーカイブにのみ適用されます。

1. Cyber Protectionコンソールで **[デバイス]** > **[すべてのデバイス]** に進みます。
2. 削除するワークロードバックアップを選択し、**[復元]** をクリックします。
3. （複数のバックアップロケーションが利用可能な場合）バックアップロケーションを選択してから、**[その他の復元方法]** をクリックします。
4. **[ファイルのダウンロード]** をクリックしします。
   Web Restoreコンソールにリダイレクトされます。
5. Web Restoreコンソールの **[マシン]** でワークロード名をクリックします。
6. **[最終バージョン]** で日付をクリックし、**[削除]**をクリックします。

この動作はバックアップアーカイブレベルでのみ使用できます。アーカイブをドリルダウンして、そこから特定のバックアップを削除することはできません。

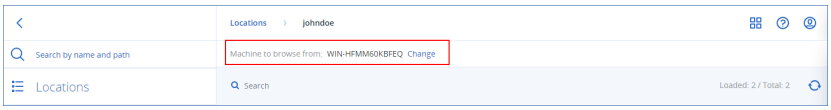
7. **[削除]** をクリックして、決定を確定します。

Cyber Protectコンソール外でバックアップを削除する

Cyber Protectコンソールを使用してバックアップを削除することをお勧めします。Web Restoreコンソールを使用してクラウドストレージからバックアップを削除する場合、またはファイルマネージャーを使用してローカルバックアップを削除する場合、Cyber Protectコンソールに変更を同期するためにバックアップロケーションをリフレッシュする必要があるからです。

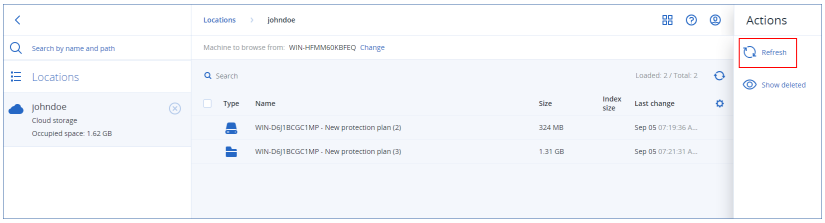
前提条件

- バックアップロケーションにアクセスできるオンラインエージェントは、コンソールで **[参照元マシン]** として選択されている必要があります。



バックアップロケーションをリフレッシュするには

1. Cyber Protectコンソールで、**[バックアップストレージ]** に移動します。
2. 削除されたバックアップが保管されていたバックアップロケーションを選択します。
3. **[操作]** ペインで、**[リフレッシュ]** をクリックします。



ボトルネックの検出について

ボトルネック検出機能により、バックアップや復元プロセスの最中に、システムのどのコンポーネントが最も遅かったかがハイライト表示されます。これは、パフォーマンスを改善できる領域を判断するのに役立ちます。

ボトルネックはどのような転送イベントでも必ず発生するため、必ずしも解決する必要があるとは限りません。バックアップが既に十分に高速で、バックアップウィンドウを完全に達成しており、SLAも満たしていている場合、解決すべき問題はないと考えられます。

[アクティビティの詳細] タブで、ボトルネックを簡単に表示およびトラックできます。これを実行するには、Cyber Protectコンソールで、**[監視]** > **[アクティビティ]** に進み、関連するアクティビティをクリックします。ボトルネックの表示の詳細については、"ボトルネックの詳細の表示"（524ページ）および"どのようなワークロード、エージェント、バックアップロケーションにボトルネックがありますか？"（526ページ）を参照してください。

ボトルネックについて

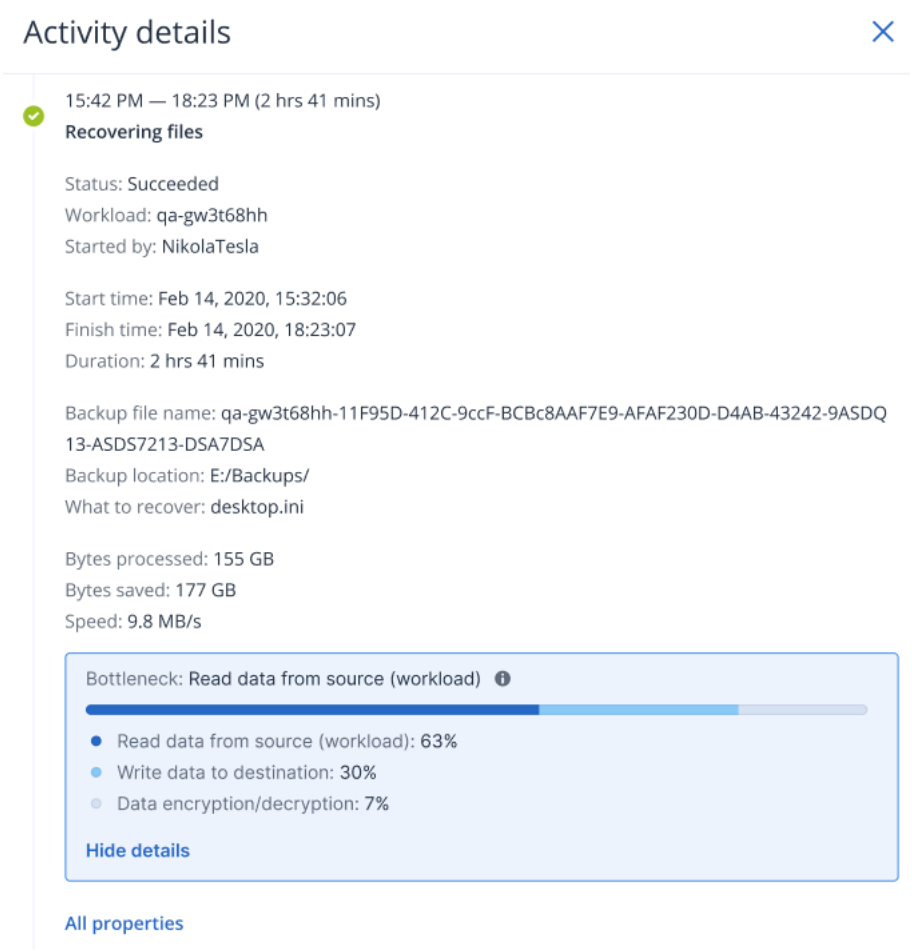
ボトルネックは通常、処理チェーンの中で遅いコンポーネント、言い換えれば、他のコンポーネントを待たせているコンポーネントが原因で発生します。

ボトルネック検出機能により、バックアップと復元のプロセス中に、これらの遅いコンポーネントをトラックすることができます。以下のコンポーネントタイプのうち、どれが最も遅いかを判断できます。

- **ソース**:バックアップ/復元ソースからの読み込み速度がボトルネックになっているかどうかをすばやく把握できます。
- **保存先**:バックアップ/復元先への書き込み速度がパフォーマンスに影響しているかどうかを把握できます。
- **エージェント**:エージェントが十分な速度でデータを処理しているかどうかを把握します。

ソース、保存先、エージェントのいずれがボトルネックタイプになっている場合でも、バックアップ/復元アクティビティ中の不特定のタイミングで変更される可能性があります。以下の **[アクティビティの詳細]** タブの **[ボトルネック]** セクションに表示される割合（例えば、**ソース（ワークロード）からデータを読み取る: 63%**）は、このタイプのボトルネックが発生している時間の割合を示しています。このケースでは、復元アクティビティ時間の63%において、ボトルネックのタイプはデータの読み込み、つまりエージェントによるバックアップアーカイブからのデータ読み込み速度の遅さにあった、ということになります。

同様に、復元先へのデータ書き込み速度の遅さがボトルネックになっている時間が30%ありました（**宛先にデータを書き込む: 30%**）。



注意
[アクティビティの詳細] タブにボトルネック統計が表示されるのは通常の動作です。これらの統計は、1分以上のタスクに対してのみ利用可能です。

ボトルネックを軽減する方法

上述したように、ボトルネック検出機能では、バックアップコンポーネント間の読み取りおよび書き込みデータフローがハイライト表示されます。読み込み統計はデータソースからバックアップ/復元操作を実行するエージェントへのデータフローを指し、書き込み統計はエージェントとバックアップアーカイブ（宛先）間のデータフローを指します。

ボトルネックを減らし、読み取り/書き込みデータフローのパフォーマンスを改善するために、エージェントとデータソース/バックアップアーカイブ間のチャネルを分析する必要があります。例えば、エージェントがローカルファイルをバックアップしている場合、ハードディスクのベンチマークを実行してみることができます。

ボトルネックの詳細の表示

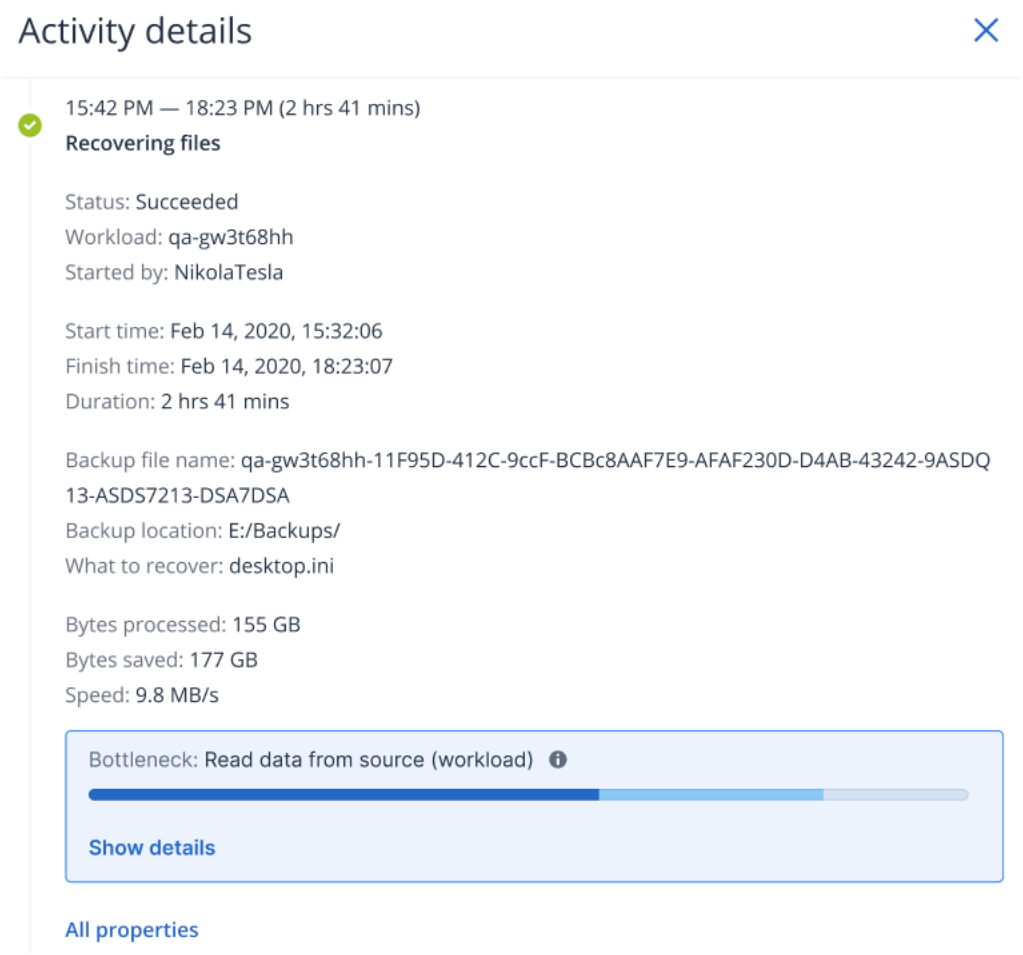
検出されたボトルネックは、仮想マシンのバックアップ、マシンのバックアップ、ファイル/フォルダのバックアップなど、あらゆるタイプのバックアップ、バックアップのレプリケーション、または復元プ

ロセス（あらゆるタイプの保存先フォルダまたはロケーション）で表示できます。仮想マシンのレプリケーションとフェールバックアクティビティのボトルネックも表示できます。

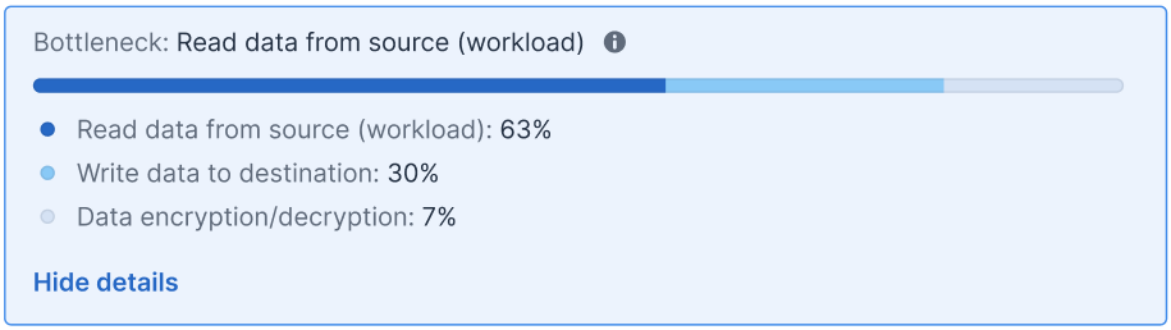
ボトルネックタイプの定義とコア概念の詳細については、"ボトルネックの検出について"（522ページ）を参照してください。

ボトルネックの詳細を表示するには

1. Cyber Protectコンソールで、**[監視]** > **[アクティビティ]** に進みます。
2. 該当するアクティビティをクリックしてください。
   [アクティビティの詳細] タブでは、**[ボトルネック]** セクションが青で表示されます。



3. バックアップ/復元操作中に最も頻繁に発生するボトルネックを表示するには、**[詳細の表示]** をクリックします。
   [ボトルネック] セクションが展開し、関連するボトルネックタイプの概要が表示されます。



上記の例では、処理時間全体の63%を占めるボトルネックは、（エージェントが実行する）読み取り処理に起因しています。

注意
ボトルネックの値は、対応するアクティビティが実行されている間、1分ごとに動的にアップデートされます。

どのようなワークロード、エージェント、バックアップロケーションにボトルネックがありますか？

ボトルネックの検出は、以下のタイプのワークロード、エージェント、およびバックアップロケーションで利用可能です。

- ディスク/イメージレベルのバックアップの実行元:
  - Azureエージェント
  - Windowsエージェント
  - Linuxエージェント
  - Macエージェント
  - VMwareエージェント（仮想アプライアンスとWindowsの両方、VMレプリケーションとレプリカからのフェールバック（レプリカからの復元）アクティビティを含む）
  - Hyper-Vエージェント
  - Scale Computingエージェント
  - oVirt（KVM）エージェント
  - Virtuozzo Infrastructure Platformエージェント
  - Virtuozzoエージェント
  - VMware Cloud Directorエージェント（vCD-BA）
- ファイルレベルのバックアップの場合
  - Windowsエージェント
  - Linuxエージェント
  - Macエージェント
- アプリケーションレベルのバックアップ
  - SQL エージェント
  - Exchangeエージェント
  - MySQL/MariaDBエージェント

    - Oracle エージェント
    - SAP HANAエージェント
- バックアップ保存先
    - Acronis Cloud Storage（パートナーホステッドストレージを含む）
    - パブリッククラウドストレージ
    - ネットワーク共有（SMB + NFS）
    - ローカル フォルダ
    - スクリプトで定義したロケーション
    - Acronis Secure Zone

パブリッククラウドへのワークロードのバックアップ

注意
この機能は、Advanced Backupパックの一部であり、さらにサイバープロテクションサービスにも含まれています。なお、保護計画にこの機能を追加する場合、追加料金が発生する場合があります。

Cyber Protectコンソールでは、Microsoft AzureやAmazon S3（Simple Storage Service）などのパブリッククラウドサービスをバックアップ先として選択できます。

パブリッククラウド上にバックアップロケーションを設定するには、企業管理者またはユニット管理者であるか、サイバー管理者、管理者、またはユーザーのうちいずれかのサイバープロテクションサービスで定義されたロールが必要です。

Microsoft Azureでバックアップロケーションを定義する

注意
Microsoft Azureにバックアップロケーションを設定するには、サイバープロテクションサービスに、企業管理者、ユーザー、サイバー管理者のいずれかのロールを定義する必要があります。

Microsoft Azureにワークロードをバックアップするには、Cyber ProtectコンソールでMicrosoft Azureのバックアップロケーションを定義し、関連するMicrosoft Azureサブスクリプションに接続する必要があります。これは、以下の方法で実行できます。

- 保護計画を作成または編集する際。
- バックアップストレージのロケーションを定義および管理する際。

重要
管理者と非管理者の両方のユーザーが、ワークロードをMicrosoft Azureにバックアップできます。

非管理者ユーザーは、Microsoft Azureサブスクリプションへのアクセスを追加できますが（"Microsoft Azureサブスクリプションへのアクセスを管理する"（538ページ）を参照）、バックアップロケーションが自分で追加したMicrosoft Azureサブスクリプションに接続されており、自分の名前でCyber Protectコンソールに登録されているワークロードに対してのみ、保護計画を適用できます。

管理者は、自分自身で追加したMicrosoft Azureサブスクリプション、または他の管理者によって追加されたサブスクリプションにバックアップロケーションが接続され、任意のユーザー名でCyber Protectコンソールに登録されたワークロードに対して、保護計画を適用できます。

Microsoft Azureでバックアップロケーションを定義するには

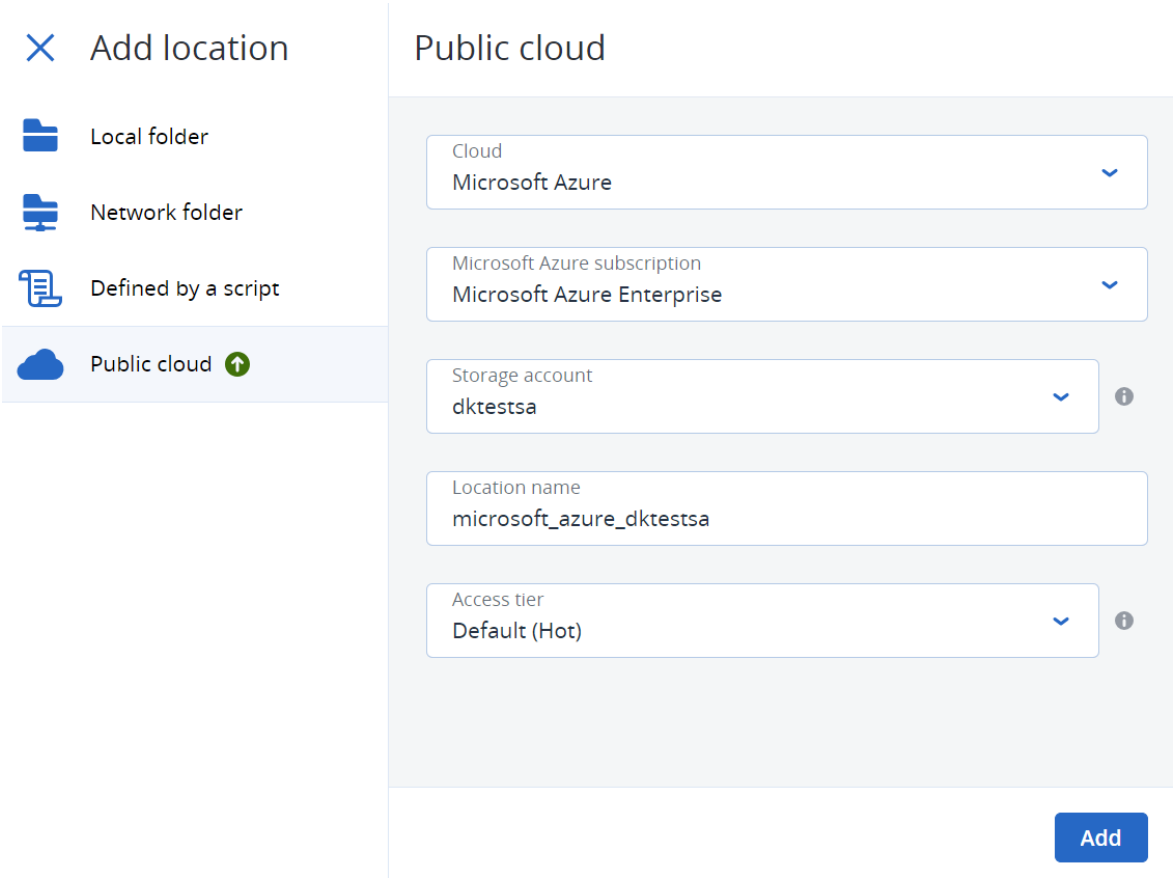
1. Cyber Protectコンソールで、次のいずれかを実行します。
   - 保護計画を作成または編集している場合は、**[デバイス]** に移動し、Microsoft Azureにバックアップするワークロードを選択します。選択したワークロードの保護計画の**バックアップ**セクションで、**バックアップの保存先**行のリンクをクリックします。
     保護計画との連携の詳細については、"保護計画とモジュール"（209ページ）を参照してください。
   - バックアップストレージのロケーションを管理しており、Microsoft Azureを新しいロケーションとして追加する場合は、**バックアップストレージ**に進みます。
     バックアップストレージのロケーション管理の詳細については、"バックアップストレージタブ"（515ページ）を参照してください。
2. **[ロケーションの追加]** をクリックします。
3. **[パブリッククラウド]** ドロップダウンリストから、**[Microsoft Azure]** を選択します。
4. 該当するMicrosoft Azureサブスクリプションがすでにに Cyber Protectコンソールに登録されている場合は、サブスクリプションのリストから選択します。
   該当するサブスクリプションがCyber Protectコンソールに登録されていない場合は、**[追加]** をクリックし、表示されたダイアログで **[サインイン]** をクリックします。Microsoftのログインページにリダイレクトされます。Microsoft Azureサブスクリプションへのアクセスの追加と定義の詳細については、"Microsoft Azureサブスクリプションへのアクセスの追加"（539ページ）を参照してください。
5. **ストレージアカウント**フィールドで、関連するアカウントを選択します。

   注意
   現在サポートされているのは、`core.windows.net`を含む通常のエンドポイントサフィックスを持つMicrosoft Azureストレージアカウントのみです。また、選択したストレージアカウントは、StorageV2アカウントタイプである必要があります。

   選択したストレージアカウントに応じて、デフォルトで**ロケーション名**フィールドと**アクセスティア**フィールドが自動的に入力されます。表示されるロケーション名は`microsoft_azure_[`**ストレージアカウ**

ント]で、選択されるアクセスティアは**デフォルト（ホット）**です。両フィールドは必要に応じて変更できます。

注意
ロケーション名を変更する場合は、一意のロケーション名を入力します（この名前はカスタマーテナントに固有である必要があります）。追加した名前がすでにストレージアカウントに存在する場合は、Acronisにより、名前に接尾辞番号が追加されます。例えば、**Microsoft Azure Storage**がすでに存在する場合、名前は自動的に**Microsoft Azure Storage_01**にアップデートされます。



6. **[追加]** をクリックします。
保護計画を作成または編集している場合、Microsoft Azureバックアップのロケーションは、**バックアップの保存先**行のロケーションとして設定されます。バックアップが実行されると（手動でまたはスケジュールにより）、バックアップは定義されたロケーションに保存されます。
バックアップストレージのロケーションを管理している場合は、必要に応じてロケーションの詳細を表示およびアップデートできます。Microsoft Azureのロケーションは、ワークロードのバックアップロケーションを定義する際にも利用できます。詳細については、"パブリッククラウドのバックアップロケーションの表示とアップデート"（534ページ）を参照してください。

Amazon S3でバックアップロケーションを定義する

注意
Amazon S3にバックアップロケーションを設定するには、サイバープロテクションサービスに、企業管理者、ユーザー、サイバー管理者のいずれかのロールを定義する必要があります。

Amazon S3にワークロードをバックアップするには、Cyber ProtectコンソールでAmazon S3のバックアップロケーションを定義し、該当するAmazon S3接続に接続する必要がありますが、次の方法で可能です。

- 保護計画を作成または編集する際。
- バックアップストレージのロケーションを定義および管理する際。

重要
管理者と非管理者の両方のユーザーが、ワークロードをAmazon S3にバックアップできます。

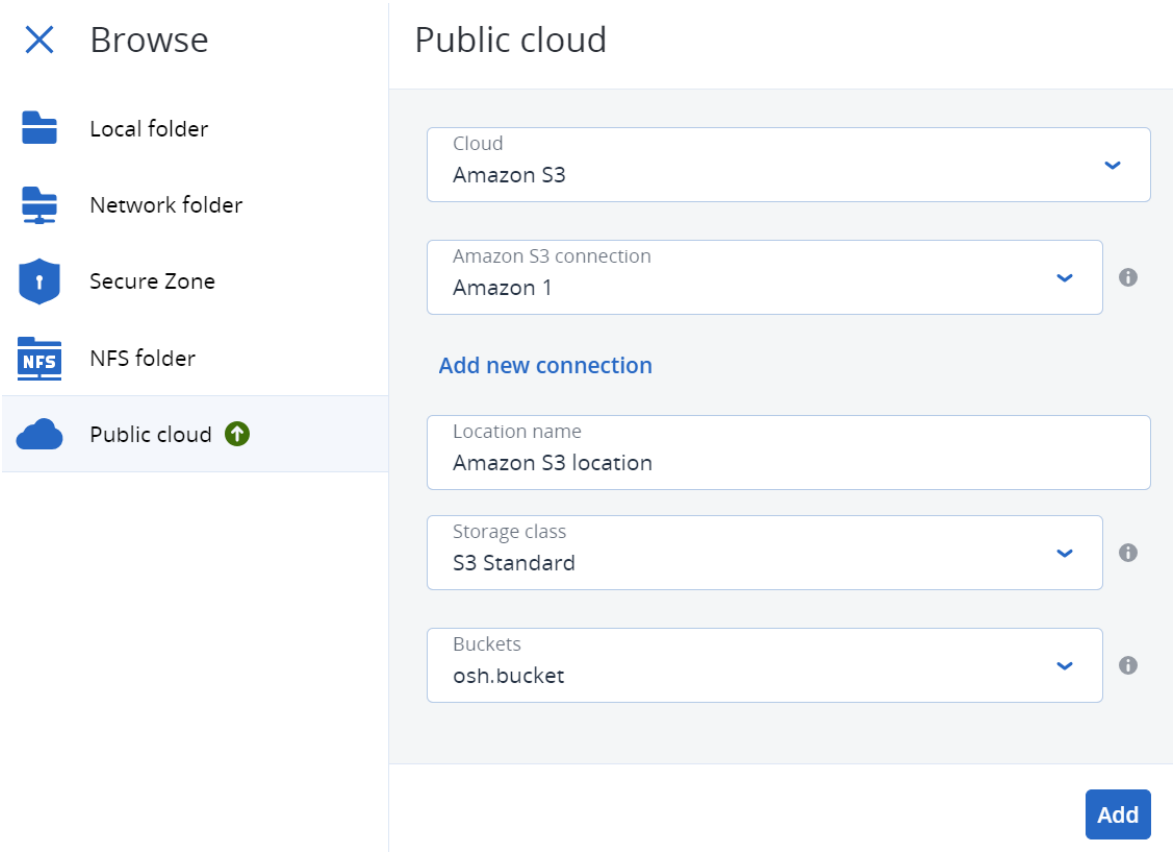
非管理者ユーザーは、Amazon S3接続へのアクセスを追加できますが（"他のパブリッククラウドストレージサービスへのアクセス管理"（541ページ）を参照）、バックアップロケーションが自分で追加したAmazon S3接続に接続されていて自分の名前でCyber Protectコンソールに登録されているワークロードに対してのみ、保護計画を適用できます。

管理者は、自分自身で追加したAmazon S3接続、または他の管理者によって追加されたサブスクリプションにバックアップロケーションが接続され、任意のユーザー名でCyber Protectコンソールに登録されたワークロードに対して、保護計画を適用できます。

Amazon S3でバックアップロケーションを定義するには

1. Cyber Protectコンソールで、次のいずれかを実行します。
   - 保護計画を作成または編集している場合は、**[デバイス]** に移動し、Amazon S3にバックアップするワークロードを選択します。選択したワークロードの保護計画の **[バックアップ]** セクションで、**[バックアップの保存先]** 行のリンクをクリックします。
     保護計画との連携の詳細については、"保護計画とモジュール"（209ページ）を参照してください。
   - バックアップストレージのロケーションを管理しており、Amazon S3を新しいロケーションとして追加する場合は、**[バックアップストレージ]**に移動します。
     バックアップストレージのロケーション管理の詳細については、"バックアップストレージタブ"（515ページ）を参照してください。
2. **[ロケーションの追加]** をクリックします。
3. **[パブリッククラウド]** ドロップダウンリストから、**[Amazon S3]** を選択します。
4. 該当するAmazon S3接続がすでにCyber Protectコンソールに登録されている場合は、そのリストから選択します。

該当する接続がCyber Protectコンソールに登録されていない場合は、**[新しい接続を追加]** をクリックします。Amazon S3接続の追加とアクセス定義の詳細については、"パブリッククラウド接続へのアクセス追加"（542ページ）を参照してください。接続が追加されたら、次の手順に進みます。



5. 以下を定義します。
   - **[ロケーション名]** フィールドに、バックアップのロケーション名を入力します。

     注意
     ロケーション名は、顧客テナントに固有である必要があります。追加した名前がすでにストレージアカウントに存在する場合は、Acronisにより、名前に接尾辞番号が追加されます。例えば、**Amazon S3ストレージ**がすでに存在する場合、名前は自動的に**Amazon S3ストレージ1**にアップデートされます。

   - **[ストレージクラス]** フィールドで、次のいずれかのサポートされているストレージクラスを選択します。
     - S3標準
     - 標準 - 低頻度アクセス（S3標準-IA）
     - 1ゾーン - 低頻度アクセス（S3 1ゾーン-IA）
     - S3 Intelligent Tiering
   - **[バケット]**フィールドで、該当するAmazon S3バケットを選択します。
6. **[追加]** をクリックします。

保護計画を作成または編集している場合は、Amazon S3のバックアップロケーションが[**バックアップの保存先**] 行のロケーションとして設定されます。バックアップが実行されると（手動でまたはスケジュールにより）、バックアップは定義されたロケーションに保存されます。

バックアップストレージのロケーションを管理している場合は、必要に応じてロケーションの詳細を表示およびアップデートできます。Amazon S3のロケーションは、ワークロードのバックアップロケーションを定義する際にも利用できます。詳細については、"パブリッククラウドのバックアップロケーションの表示とアップデート"（534ページ）を参照してください。

Wasabiでバックアップロケーションを定義する

注意
Wasabiにバックアップロケーションを設定するには、サイバープロテクションサービスに、企業管理者、ユーザー、サイバー管理者のいずれかのロールを定義する必要があります。

Wasabiにワークロードをバックアップするには、Cyber ProtectコンソールでWasabiのバックアップロケーションを定義し、該当するWasabi接続に接続する必要がありますが、次の方法で可能です。

- 保護計画を作成または編集する際。
- バックアップストレージのロケーションを定義および管理する際。

重要
管理者と非管理者の両方のユーザーが、ワークロードをWasabiにバックアップできます。

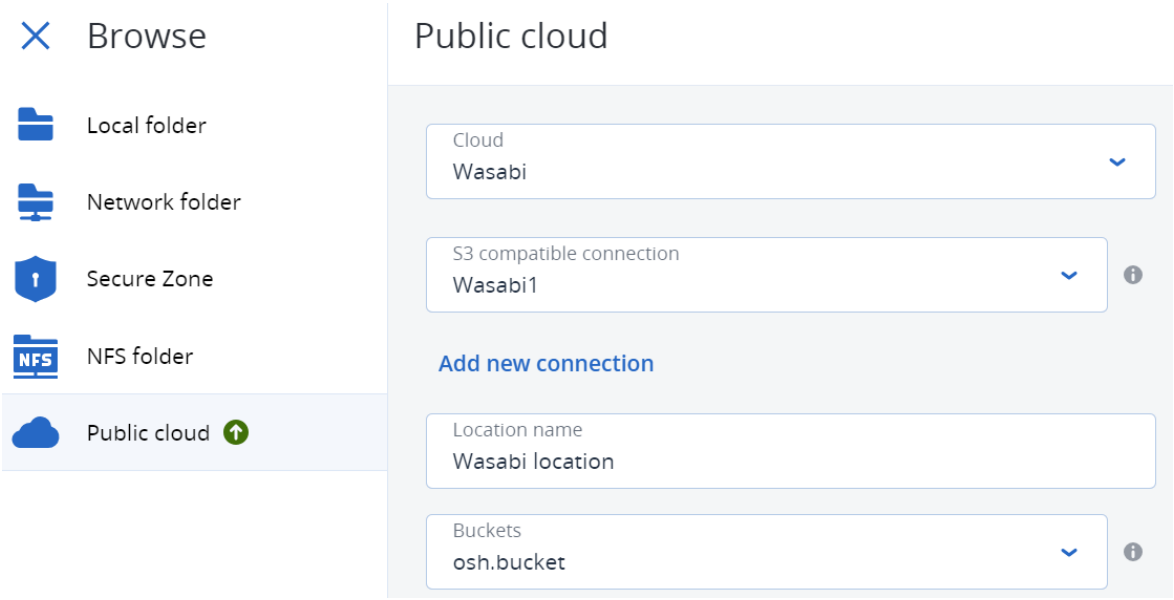
非管理者ユーザーは、Wasabi接続へのアクセスを追加できますが（"他のパブリッククラウドストレージサービスへのアクセス管理"（541ページ）を参照）、バックアップロケーションが自分で追加したWasabi接続に接続されていて自分の名前でCyber Protectコンソールに登録されているワークロードに対してのみ、保護計画を適用できます。

管理者は、自分自身で追加したWasabi接続、または他の管理者によって追加されたサブスクリプションにバックアップロケーションが接続され、任意のユーザー名でCyber Protectコンソールに登録されたワークロードに対して、保護計画を適用できます。

Wasabiでバックアップロケーションを定義するには

1. Cyber Protectコンソールで、次のいずれかを実行します。
   - 保護計画を作成または編集している場合は、[**デバイス**] に移動し、Wasabiにバックアップするワークロードを選択します。選択したワークロードの保護計画の [**バックアップ**] セクションで、[**バックアップの保存先**] 行のリンクをクリックします。
     保護計画との連携の詳細については、"保護計画とモジュール"（209ページ）を参照してください。
   - バックアップストレージのロケーションを管理しており、Wasabiを新しいロケーションとして追加する場合は、[**バックアップストレージ**]に移動します。
     バックアップストレージのロケーション管理の詳細については、"バックアップストレージタブ"（515ページ）を参照してください。

2. **[ロケーションの追加]** をクリックします。
3. **[パブリッククラウド]** ドロップダウンリストから、**[Wasabi]** を選択します。
4. 該当するWasabi接続がすでにCyber Protectコンソールに登録されている場合は、その接続リストから選択します。
   該当する接続がCyber Protectコンソールに登録されていない場合は、**[新しい接続を追加]** をクリックします。Wasabi接続の追加とアクセス定義の詳細については、"パブリッククラウド接続へのアクセス追加"（542ページ）を参照してください。接続が追加されたら、次の手順に進みます。



5. 以下を定義します。
   - **[ロケーション名]** フィールドに、バックアップのロケーション名を入力します。

     注意
     ロケーション名は、顧客テナントに固有である必要があります。追加した名前がすでにストレージアカウントに存在する場合は、Acronisにより、名前に接尾辞番号が追加されます。例えば、**Wasabiストレージ**がすでに存在する場合、名前は自動的に**Wasabiストレージ1**にアップデートされます。

   - **[バケット]**フィールドで、該当するWasabiバケットを選択します。
6. **[追加]** をクリックします。
   保護計画を作成または編集している場合は、Wasabiのバックアップロケーションが**[バックアップの保存先]** 行のロケーションとして設定されます。バックアップが実行されると（手動でまたはスケジュールにより）、バックアップは定義されたロケーションに保存されます。
   バックアップストレージのロケーションを管理している場合は、必要に応じてロケーションの詳細を表示およびアップデートできます。Wasabiのロケーションは、ワークロードのバックアップロケーションを定義する際にも利用できます。詳細については、"パブリッククラウドのバックアップロケーションの表示とアップデート"（534ページ）を参照してください。

パブリッククラウドのバックアップロケーションの表示とアップデート

バックアップストレージモジュールで、または保護計画を作成または編集するときに定義した、Microsoft Azure、Amazon S3、およびWasabiのバックアップロケーションを表示およびアップデートできます。

Cyber ProtectコンソールからMicrosoft Azureサブスクリプションへのアクセスを削除する方法については、"Microsoft Azureサブスクリプションへのアクセスの削除"（541ページ）を参照してください。その他のパブリッククラウド接続へのアクセスを削除する方法については、"他のパブリッククラウドストレージサービスへのアクセス管理"（541ページ） を参照してください。

注意
バックアップストレージモジュールでパブリッククラウドのバックアップロケーションを手動でリフレッシュまたは削除することはできません。バックアップロケーションの内容は、バックアップまたは復元操作のたびに自動的にアップデートされます。

パブリッククラウドのバックアップロケーションを表示するには

1. Cyber Protectコンソールで、**[バックアップストレージ]** に移動します。
   バックアップロケーションの一覧が、各ロケーションに割り当てられているストレージ容量とバックアップ数の詳細とともに表示されます。
   リストされたバックアップロケーションの動作の詳細については、"バックアップストレージタブ"（515ページ）を参照してください。
2. 関連するロケーションを選択します。
   選択したロケーションの現在のバックアップが一覧表示されます。
3. （オプション）バックアップをクリックして、バックアップの詳細を表示します。

保護計画内のパブリッククラウドのバックアップロケーションをアップデートするには

1. 関連する保護計画に移動し、**[編集]** を選択します。
2. **バックアップの保存先**行のリンクをクリックします。
3. 既存のバックアップロケーションのリストから選択するか、**[ロケーションの追加]** をクリックして新しいロケーションを追加します。
   該当するMicrosoft Azureサブスクリプションまたはパブリッククラウド接続がすでにCyber Protectコンソールに登録されている場合は、サブスクリプションの一覧から選択します。
   新しいMicrosoft Azureサブスクリプションを追加する場合は、Microsoftアカウントの詳細を認証するよう求められます（"Microsoft Azureサブスクリプションへのアクセスの追加"（539ページ）を参照）。Microsoft Azureへの接続に必要な許可の詳細については、Microsoft Azure接続のセキュリティと監査（72684）の記事を参照してください。

パブリッククラウドアカウントへのアクセス管理

パブリッククラウドプラットフォームで、Acronis Cyber Protectionサービスを有効にするには、関連するパブリッククラウドアカウントへのアクセスを構成する必要があります。

例えば、Microsoft Azureと連携する場合、Microsoft Azureサブスクリプションへのアクセスが必要です。Cyber Protectコンソールに追加されると、Microsoft Azureへの直接バックアップを構成するときにサブスクリプションを選択できます。同様に、Amazon S3やWasabiを使用する場合は、特定のバックアップ関連ポリシーに関連するアクセスキーが必要です。

パブリッククラウドへのアクセスは、コンソールの**インフラストラクチャ**メニューで管理します。

重要
パブリッククラウドストレージ上のバックアップの検証は、過度のトラフィックコストを避けるために無効化されています。また、パブリッククラウド上のバックアップロケーションが過去に削除された場合、そのロケーションは、対象の顧客テナントが同じでも異なっていても「再アタッチ」することはできません。詳細については、サポートチームまでお問い合わせください。

パブリッククラウドストレージへのバックアップに必要なアクセス要件

パブリッククラウドストレージサービスに直接バックアップする場合、次のプラットフォームごとに考慮する必要がある要件が数多くあります。

- Microsoft Azure
- Amazon S3
- Wasabi

Microsoft Azureへのバックアップ

Microsoft Azureサブスクリプションに接続するには、いくつかの権限が必要です。詳細については、「Microsoft Azure接続のセキュリティと監査（72684）」の記事を参照してください。

Amazon S3へのバックアップ

Amazon S3にバックアップする場合、Amazon S3のバックアップロケーションを定義する際に次に示すいくつかの要件があります。

- サポートされるストレージクラス
- ポリシーの許可
- アクセスキー
- バケット設定

サポートされるストレージクラス

現在、以下のAmazon S3ストレージクラスがサポートされています。

- S3標準
- 標準 - 低頻度アクセス（S3標準-IA）
- 1ゾーン - 低頻度アクセス（S3 1ゾーン-IA）
- S3 Intelligent Tiering

ポリシーの許可

Amazon S3にバックアップする場合、Acronisが該当するワークロードをAmazon S3にバックアップできるように、Amazonアカウントに最小限の権限が適用されている必要があります。つまり、該当するユーザーがAWS管理コンソールにアクセス権があり、割り当てられたグループに関連するポリシーが適用されている必要があるということです。

例

次のポリシー例では、広範なリソースに対する最小限の権限セットが示されています。*は、すべてのリソースを表しています。

```
{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Action":
"s3:ListAllMyBuckets", "Resource": "*" }, { "Effect": "Allow", "Action": [
"s3:GetBucketLocation", "s3:GetBucketObjectLockConfiguration" ], "Resource": "*" },
{ "Effect": "Allow", "Action": "sts:GetFederationToken", "Resource": "*" }, {
"Effect": "Allow", "Action": [ "s3:GetBucketLocation", "s3:PutObject",
"s3:GetObject", "s3:DeleteObject" ], "Resource": "*" }, { "Effect": "Allow",
"Action": [ "s3:ListBucket" ], "Resource": "*" } ] }
```

次のポリシー例は、特定のバケットに制限された最小の権限が示されています。[BUCKETNAME] はバケット名に置き換えます。

```
{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Action":
"s3:ListAllMyBuckets", "Resource": "*" }, { "Effect": "Allow", "Action": [
"s3:GetBucketLocation", "s3:GetBucketObjectLockConfiguration" ], "Resource":
"arn:aws:s3:::[BUCKETNAME]" }, { "Effect": "Allow", "Action":
"sts:GetFederationToken", "Resource": "*" }, { "Effect": "Allow", "Action": [
"s3:GetBucketLocation", "s3:PutObject", "s3:GetObject", "s3:DeleteObject" ],
"Resource": "arn:aws:s3:::[BUCKETNAME]/*" }, { "Effect": "Allow", "Action": [
"s3:ListBucket" ], "Resource": "arn:aws:s3:::[BUCKETNAME]" } ] }
```

アクセスキー

アクセスキーは、Amazon S3接続ごとにAcronisが必要とし、Amazon S3接続を定義する際に使用されます。アクセスキーとアクセスキーIDの生成の詳細については、Amazon S3のドキュメントを参照してください。

バケット設定

Amazon S3バケットをバックアップロケーションとして使用する場合は、すべてのパブリックアクセスのブロックなど、バケットを必ずデフォルト設定で設定します（デフォルト設定で **[オン]**）。バケット

の操作の詳細については、 Amazon S3 のドキュメントを参照してください。

注意
Acronisは現在、バケット上で有効になっている場合でも、Amazon S3のバケットバージョニングとオブジェクトロックをサポートしていません。

Wasabiへのバックアップ

Wasabiにバックアップする場合、次の項目において、バックアップロケーションを定義する際に考慮する必要がある多数の要件があります。

- ポリシーの許可
- アクセスキー
- バケット設定

ポリシーの許可

Wasabiでバックアップロケーションを定義する場合には、関連するポリシーがWasabiの該当するグループとユーザーに適用されていることを確認してください。

例

次のポリシー例では、広範なリソースで最小限の権限セットが示されています。*は、あらゆるリソースを表しています。

```
{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Action":
"s3:ListAllMyBuckets", "Resource": "*" }, { "Effect": "Allow", "Action":
"s3:GetBucketLocation", "Resource": "*" }, { "Effect": "Allow", "Action": [
"iam:CreateRole", "iam:AttachRolePolicy", "sts:GetCallerIdentity", "sts:AssumeRole"
], "Resource": "*" }, { "Effect": "Allow", "Action": [ "s3:PutObject",
"s3:GetObject", "s3:DeleteObject" ], "Resource": "*" }, { "Effect": "Allow",
"Action": "s3:ListBucket", "Resource": "*" } ] }
```

次のポリシー例は、制限された範囲のリソースでの限定的な権限が示されています。`[BUCKETNAME]` はバケット名に置き換え、`[ACCOUNTID]`はWasabiアカウントのIDに置き換えます。

```
{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Action":
"s3:ListAllMyBuckets", "Resource": "*" }, { "Effect": "Allow", "Action":
"s3:GetBucketLocation", "Resource": "arn:aws:s3:::[BUCKETNAME]" }, { "Effect":
"Allow", "Action": [ "iam:CreateRole", "iam:AttachRolePolicy",
"sts:GetCallerIdentity", "sts:AssumeRole" ], "Resource": "arn:aws:iam::
[ACCOUNTID]:*" }, { "Effect": "Allow", "Action": [ "s3:PutObject", "s3:GetObject",
"s3:DeleteObject" ], "Resource": "arn:aws:s3:::[BUCKETNAME]/*" }, { "Effect":
"Allow", "Action": "s3:ListBucket", "Resource": "arn:aws:s3:::[BUCKETNAME]" } ] }
```

アクセスキー

アクセスキーは、Wasabi接続ごとにAcronisが必要とし、Wasabiを定義する際に使用されます。アクセスキーとアクセスキーIDの生成の詳細については、Wasabiのドキュメントを参照してください。

バケット設定

Wasabiバケットをバックアップロケーションとして使用する場合は、バケットを必ずデフォルト設定で設定します。バケットの連携に関する詳細については、Wasabiのドキュメントを参照してください。

注意
Acronisは現在、バケット上で有効になっている場合でも、Wasabiのバケットバージョニングとオブジェクトロックをサポートしていません。

Microsoft Azureサブスクリプションへのアクセスを管理する

Cyber Protectコンソールで関連するMicrosoft Azureサブスクリプションに接続することで、関連するワークロードをMicrosoft Azureに直接バックアップできます。

サブスクリプションへの接続は、**デバイス**または**バックアップストレージ**メニューを使用してバックアップロケーションを作成するときに構成できます（"Microsoft Azureでバックアップロケーションを定義する"（527ページ）を参照）。

また、これらのMicrosoft Azureサブスクリプションは、パブリッククラウド画面で構成することもできます（**[インフラストラクチャ]** > **[パブリッククラウド]** に進む）。ここでは、サブスクリプションを管理することもできます。サブスクリプションへのアクセスの更新、サブスクリプションのプロパティとアクティビティの表示、サブスクリプションの削除などを実行できます。

割り当てられた管理者のロールによっては、組織内の他のユーザーが追加したMicrosoft Azureサブスクリプションを管理できる場合があります。例えば、企業管理者またはユニット管理者である場合、またはサイバープロテクションサービスでサイバー管理者または管理者ロールが割り当てられている場合、他の管理者によって追加されたMicrosoft Azureサブスクリプション、および管理者以外のユーザーによって追加されたサブスクリプションを表示および管理できます。非管理者ユーザーは、Cyber Protectコンソールに追加したMicrosoft Azureサブスクリプションのみを表示およびアクセスできます。

注意
パートナーは、自分のレベルより下位の階層に存在するカスタマーのMicrosoft Azureサブスクリプションを管理できます。ただし、パートナーが **[すべてのカスタマー]** を選択した場合、コンソールの **[インフラストラクチャ]** メニューは使用できません。

重要
Microsoft Azureサブスクリプションに接続する場合、Acronisでサブスクリプションに接続するための最小限の許可が必要になります。必要な許可の詳細については、「Microsoft Azure接続のセキュリティと監査（72684）」の記事を参照してください。

Microsoft Azureサブスクリプションへのアクセスの追加

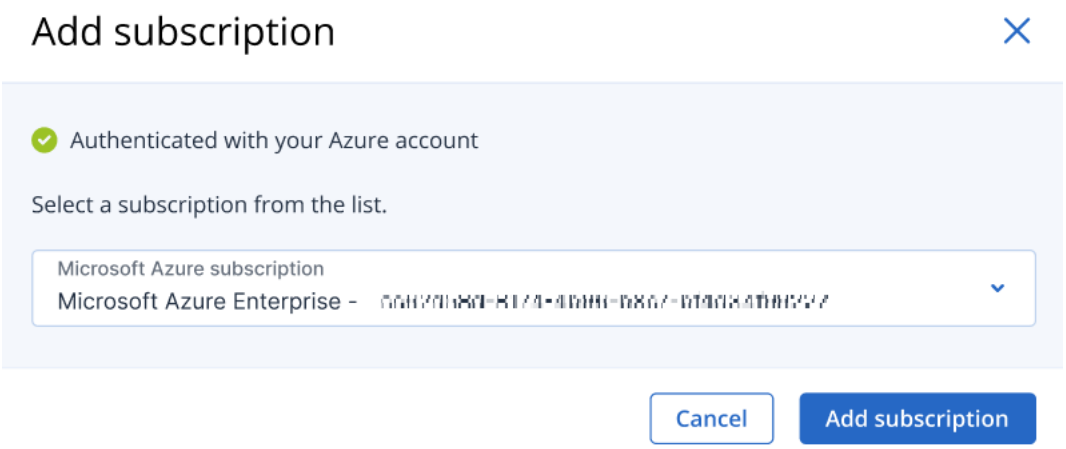
Cyber ProtectコンソールでMicrosoft Azureサブスクリプションを追加することで、Acronisはサブスクリプションに安全にアクセスし、関連するワークロードをMicrosoft Azureに直接バックアップできます。

Microsoft Azureサブスクリプションにアクセスを追加するには

1. Cyber Protectコンソールで **[インフラストラクチャ]** > **[パブリッククラウド]** に進みます。
2. **[追加]** をクリックし、表示されたオプション一覧で**[Microsoft Azure]** を選択します。
3. 表示されたダイアログで、**[サインイン]** をクリックします。Microsoftのログインページにリダイレクトされます。

注意
サブスクリプションへの接続を完了するには、Microsoft Azure ADで次に挙げるいずれかのロールの割り当てが必要です:クラウドアプリケーション管理者、アプリケーション管理者、またはグローバル管理者。また、選択した各サブスクリプションにOwnerロールが割り当てられている必要があります。

4. Microsoftのログイン画面で、ログイン資格情報を入力し、要求された許可を承認します。接続プロセスが開始されます。これには、数分かかる場合があります。
   Microsoft Azureおよびサブスクリプションへの安全なアクセスの詳細については、「Microsoft Azure接続のセキュリティと監査（72684）」の記事を参照してください。
5. 接続が完了したら、表示されたダイアログのドロップダウンリストから関連するサブスクリプションを選択し、**[サブスクリプションを追加]** をクリックします。



   サブスクリプションがパブリッククラウドのリストに追加されます。
   サブスクリプションの年間アクセス証明書を更新する場合は、"Microsoft Azureサブスクリプションへのアクセスの更新"（540ページ）を参照してください。
   サブスクリプションへのアクセスを削除する場合は、"Microsoft Azureサブスクリプションへのアクセスの削除"（541ページ）を参照してください。

注意
ログインしているMicrosoft Azureアカウントに、ゲストユーザーとして招待されたADを含む複数のMicrosoft Azure ADへのアクセスが含まれている場合、デフォルトのユーザーディレクトリのみが選択されます。ゲストユーザーとして割り当てられているディレクトリを使用したい場合は、その特定のMicrosoft Azure ADで新しいユーザーを作成する必要があります。その後、そのアカウントにログインし、関連するサブスクリプションに接続できます。

Microsoft Azureサブスクリプションへのアクセスの更新

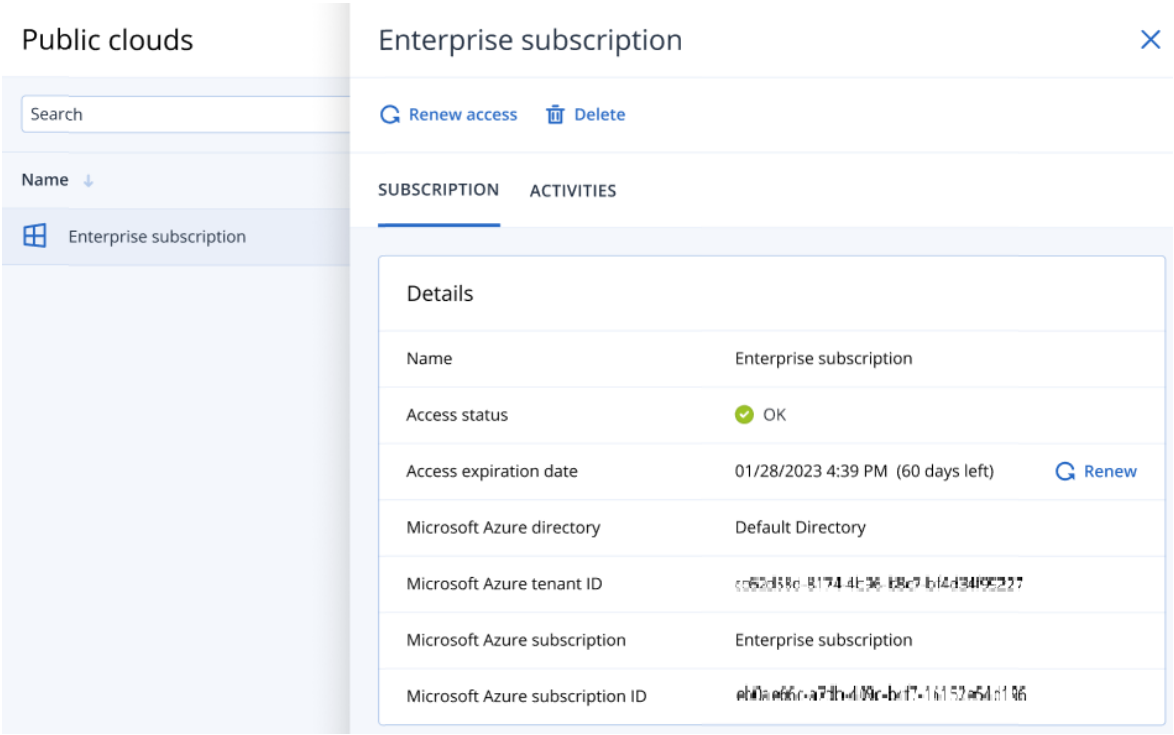
Cyber Protectコンソールに登録すると、無料で一意のアクセス証明書を使用するAcronisにより、1年間のMicrosoft Azureサブスクリプションへのアクセスが自動で設定されます。証明書の有効期限が近づいたら、すばやく簡単に更新できます。

Microsoft Azureサブスクリプションのアクセス証明書を更新するには

1. Cyber Protectコンソールで **[インフラストラクチャ]** > **[パブリッククラウド]** に進みます。
2. 表示されたリストから該当するサブスクリプションを選択します。

注意
アクセスステータス列は、各サブスクリプションのアクセス証明書に関する現在のステータスを示し、2つのステータスのいずれかが表示されます:**[OK]** または **[期限切れ]** です。

3. 右側のペインで、**[アクセスを更新]** をクリックします。
   または、**[サブスクリプション]** タブをクリックし、**アクセス有効期限**フィールドの **[更新]** をクリックします。



4. Microsoftのログイン画面で、ログイン資格情報を入力し、要求された許可を承認します。接続プロセスが開始されます。これには、数分かかる場合があります。

   認証が成功すると、アクセスは自動的に1年間更新されます。

   必要な許可の詳細については、「Microsoft Azure接続のセキュリティと監査（72684）」の記事を参照してください。

Microsoft Azureサブスクリプションへのアクセスの削除

Microsoft Azureにワークロードをバックアップしない場合は、Microsoft Azureサブスクリプションへのアクセスを削除する必要があります。

Microsoft Azureサブスクリプションへのアクセスを削除するには

重要
サブスクリプションが現在Microsoft Azureへのバックアップに使用されている場合は、サブスクリプションを削除できません。

1. Cyber Protectコンソールで **[インフラストラクチャ]** > **[パブリッククラウド]** に進みます。
2. 表示されたリストから該当するサブスクリプションを選択します。
3. 右側のペインで、**[削除]** をクリックします。

   注意
   削除できるのは、追加したサブスクリプションのみです。また、会社管理者またはユニット管理者であるか、サイバープロテクションサービスでCyber administratorまたはAdministratorのロールが割り当てられている場合も、サブスクリプションを削除できます。

4. 表示された確認メッセージで **[削除]** をクリックします。

他のパブリッククラウドストレージサービスへのアクセス管理

注意
このセクションでは、"Microsoft Azureサブスクリプションへのアクセスを管理する"（538ページ）で説明されている Microsoft Azure以外のすべてのパブリッククラウドストレージサービスのアクセス管理について説明します。

Cyber Protectコンソールで該当するパブリッククラウドアカウントに接続することで、該当するパブリッククラウドストレージにワークロードを直接バックアップできます。

[デバイス] または **[バックアップストレージ]** メニューからバックアップロケーションを作成する際に、パブリッククラウドストレージアカウントへの接続を構成できます。また、**[パブリッククラウド]**画面（**[インフラストラクチャ]** > **[パブリッククラウド]**へ移動）でパブリッククラウド接続を構成することもできます。ここでは、接続へのアクセスの更新、接続のプロパティとアクティビティの表示、接続の削除など、接続を管理することもできます。

割り当てられた管理者のロールによっては、組織内の他のユーザーが追加したパブリッククラウド接続を管理できる場合があります。例えば、企業管理者またはユニット管理者である場合、またはサイバー

プロテクションサービスでサイバー管理者または管理者ロールが割り当てられている場合、他の管理者によって追加されたパブリッククラウド接続、および非管理ユーザーによって追加された接続を表示および管理できます。非管理ユーザーは、Cyber Protectコンソールに追加したパブリッククラウド接続のみを表示およびアクセスできます。

注意
パートナーは、自分のレベルより下位の階層に存在するカスタマーのパブリッククラウド接続を管理できます。ただし、パートナーが **[すべてのカスタマー]** を選択した場合、コンソールの **[インフラストラクチャ]** メニューは使用できません。

重要
パブリッククラウド接続に接続する場合、Acronisには多くの権限が必要です。詳細については、"パブリッククラウドストレージへのバックアップに必要なアクセス要件"（535ページ）を参照してください。

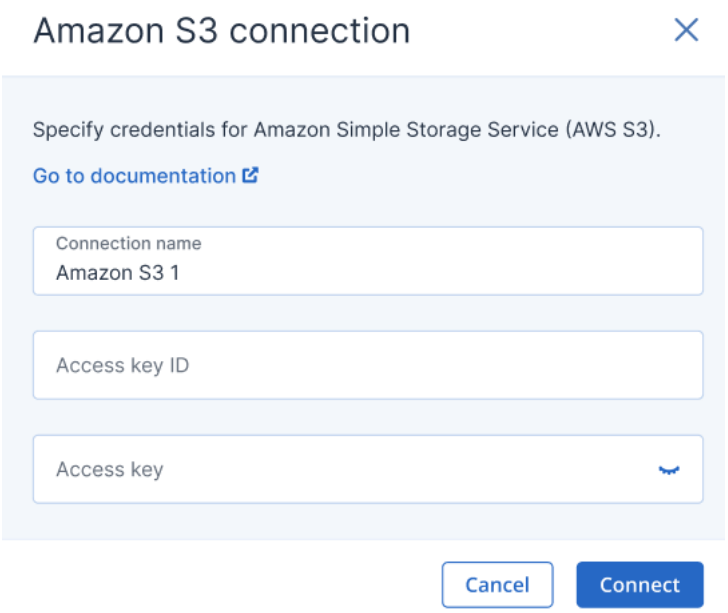
パブリッククラウド接続へのアクセス追加

Cyber Protectコンソールでパブリッククラウド接続（Amazon S3やWasabiなど）を追加すると、Acronisではクラウドリソースに安全にアクセスし、関連するパブリッククラウドストレージにワークロードを直接バックアップできます。

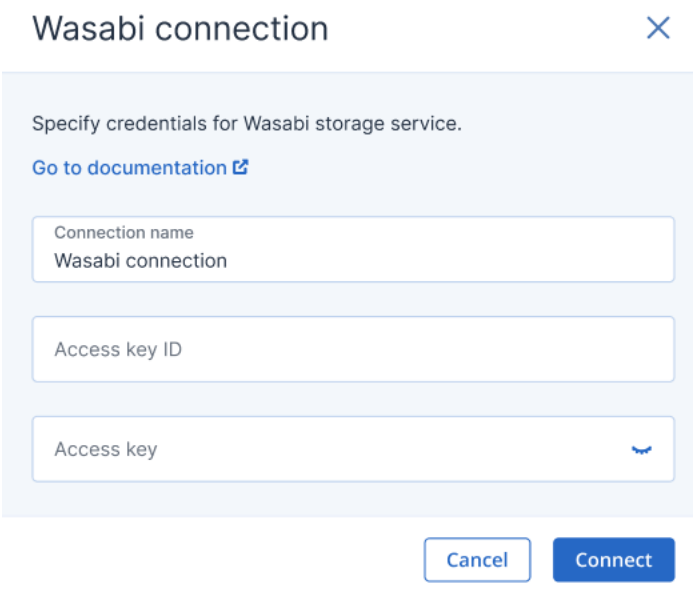
パブリッククラウド接続へのアクセスを追加するには

1. Cyber Protectコンソールで **[インフラストラクチャ]** > **[パブリッククラウド]** に進みます。
2. **[追加]** クリックして、次のオプションのいずれかを選択します。
   - **Amazon S3**
     表示されたダイアログで次の項目を定義します。
     - **接続名**: Amazon S3接続の名前。
     - **アクセスキーID**: Amazon S3サービスのユーザーアクセスキーのID。
     - **アクセスキー**: Amazon S3サービスのユーザーアクセスキー。
       アクセスキーとアクセスキーIDによって、Acronisが関連する接続のストレージクラスとバケットにアクセスできます。Acronisが必要とするアクセスキーとアクセス許可の詳細については、"パブリッククラウドストレージへのバックアップに必要なアクセス要件"（535ページ）を参照

してください。



- **Wasabi**
  表示されたダイアログで次の項目を定義します。
  - **接続名**: Wasabi接続の名前。
  - **アクセスキーID**: WasabiサービスのユーザーアクセスキーのID。
  - **アクセスキー**: Wasabiサービスのユーザーアクセスキー。
    アクセスキーとアクセスキーIDによって、Acronisが関連する接続のストレージクラスとバケットにアクセスできます。Acronisが必要とするアクセスキーとアクセス許可の詳細については、"パブリッククラウドストレージへのバックアップに必要なアクセス要件"（535ページ）を参照してください。



3. **[接続]** をクリックします。

接続プロセスが開始されます。これには、数分かかる場合があります。完了すると、接続がパブリッククラウドのリストに追加されます。

接続の年間アクセス証明書を更新する場合は、"パブリッククラウド接続の更新"（544ページ）を参照してください。

接続へのアクセスを削除する場合は、"パブリッククラウド接続の削除"（545ページ）を参照してください。

パブリッククラウド接続の更新

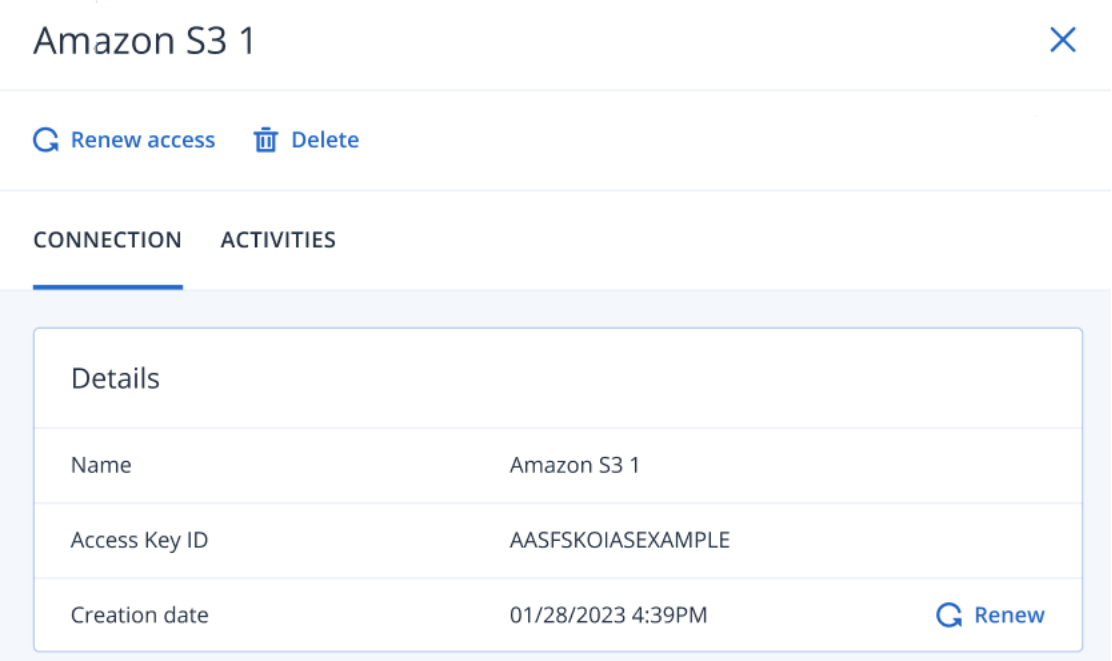
パブリッククラウド接続がCyber Protectコンソールに登録されると、Acronisによってパブリッククラウド接続へのアクセスを可能にする無料の一意のアクセス証明書が自動的に割り当てられます。証明書の有効期限は1年間です。証明書の有効期限が近づいたら、更新することができます。

パブリッククラウド接続のアクセス証明書を更新するには

1. Cyber Protectコンソールで **[インフラストラクチャ]** > **[パブリッククラウド]** に進みます。
2. 一覧から該当する接続を選択します。

注意
[アクセスステータス] 列は、各接続のアクセス証明書に関する現在のステータスを示し、**[OK]** または **[期限切れ]** の2つのステータスのいずれかが表示されます。

3. 右側のペインで、**[アクセスを更新]** をクリックします。
   または、**[接続]** タブをクリックし、**[作成日]** 列の **[更新]** をクリックします。



認証が成功すると、アクセスは自動的に1年間更新されます。

パブリッククラウド接続の削除

パブリッククラウドにワークロードをバックアップしない場合は、パブリッククラウド接続へのアクセスを削除する必要があります。

パブリッククラウド接続へのアクセスを削除するには

重要
パブリッククラウドへのバックアップに使用中の接続は削除できません。

1. Cyber Protectコンソールで **[インフラストラクチャ]** > **[パブリッククラウド]** に進みます。
2. 一覧から接続を選択します。
3. 右側のペインで、**[削除]** をクリックします。

   注意
   自身で追加した接続のみが削除できます。また、会社管理者またはユニット管理者であるか、サイバープロテクションサービスでサイバー管理者または管理者のロールが割り当てられている場合も、接続を削除できます。

4. 表示された確認メッセージで **[削除]** をクリックします。

Microsoft アプリケーションの保護

Microsoft SQL ServerとMicrosoft Exchange Serverの保護

注意
Microsoft SQLバックアップは、NFTS、REFS、およびFAT32ファイルシステム上で実行されているデータベースに対してのみサポートされています。ExFatはサポートされていません。

Microsoftのアプリケーションを保護する方法には、以下の2つがあります。

- **データベースのバックアップ**
  これはデータベースやデータベースと関連づけられたメタデータをファイルレベルでバックアップする方法です。データベースはライブアプリケーションまたはファイルに復元できます。
- **アプリケーション認識型バックアップ**
  これは、アプリケーションのメタデータも収集するディスクレベルのバックアップです。このメタデータを使用すると、ディスクやボリューム全体を復元しなくても、アプリケーションデータの参照と復元ができるようになります。ディスク全体またはボリューム全体を復元することもできます。これは、ディザスタリカバリとデータ保護の両方の目的に、同じソリューションと同じ保護計画を使用できることを意味します。

Microsoft Exchange Serverの場合は、**[メールボックスのバックアップ]** を選択できます。これは、Exchange Webサービスプロトコルを介した個別のメールボックスのバックアップです。メールボックスやメールボックスアイテムを稼働中のExchange ServerまたはMicrosoft 365にリカバリできます。

メールボックスのバックアップは、Microsoft Exchange Server 2010 Service Pack 1（SP1）以降でのみサポートされています。

Microsoft SharePointの保護

Microsoft SharePointファームは、SharePointサービスを実行するフロントエンドサーバー、Microsoft SQL Serverを実行するデータベースサーバーと、フロントエンドサーバーからSharePointサービスの一部をオフロードするオプションのアプリケーションサーバーで構成されています。一部のフロントエンドサーバーとアプリケーションサーバーは、同一の場合があります。

SharePointファーム全体を保護する手順

- すべてのデータベースサーバーをアプリケーション認識型バックアップでバックアップします。
- すべての一意のフロントエンドサーバーとアプリケーションサーバーを通常のディスクレベルのバックアップでバックアップします。

すべてのサーバーのバックアップは、同じスケジュールで実行する必要があります。

コンテンツのみを保護する場合、コンテンツデータベースを個別にバックアップできます。

ドメインコントローラの保護

Active Directoryドメインサービスを実行するコンピュータは、アプリケーション認識型バックアップで保護できます。ドメインに複数のドメインコントローラがあり、いずれかを復元する場合は、権限のない復元が実行され、USNロールバックが復元後に発生しません。

アプリケーションの復元

次の表は、使用可能なアプリケーション復元方法を示しています。

	データベースバックアップから	**アプリケーション認識型バックアップから**	**ディスクバックアップから**
Microsoft SQL Server	データベースをライブSQLサーバーインスタンスへ データベースをファイルとして	コンピュータ全体 データベースをライブSQLサーバーインスタンスへ データベースをファイルとして	コンピュータ全体
Microsoft Exchange Server	データベースをライブExchangeへ データベースをファイルとして 稼働中のExchangeまたはMicrosoft 365への粒度復元*	コンピュータ全体 データベースをライブExchangeへ データベースをファイルとして 稼働中のExchangeまたはMicrosoft 365への粒度復元*	コンピュータ全体

Microsoft SharePointデータベースサーバー	データベースをライブSQLサーバーインスタンスへ データベースをファイルとして SharePoint Explorerを使用した粒度復元	コンピュータ全体 データベースをライブSQLサーバーインスタンスへ データベースをファイルとして SharePoint Explorerを使用した粒度復元	コンピュータ全体
Microsoft SharePointフロントエンドウェブサーバー	-	-	コンピュータ全体
Active Directoryドメインサービス	-	コンピュータ全体	-

*粒度復元は、メールボックスのバックアップからも利用できます。Exchangeデータアイテムの Microsoft 365への復元およびその逆の操作は、Microsoft 365エージェントがローカルにインストール済みという条件下でのみサポートされます。

前提条件

アプリケーションバックアップを構成する前に、次の要件が満たされていることを確認します。

VSSライターの状態を確認するには、`vssadmin list writers`コマンドを使用します。

一般的な要件

Microsoft SQL Serverの場合、次の要件を満たす必要があります。

- 少なくとも1つのMicrosoft SQL Serverインスタンスが起動していること。
- SQLライターfor VSSがオンになっていること。

Microsoft Exchange Serverの場合、次の要件を満たす必要があります。

- Microsoft Exchangeインフォメーションストアサービスが起動していること。
- Windows PowerShellがインストールされていること。Exchange 2010以降の場合、Windows PowerShellのバージョンは2.0以上である必要があります。
- Microsoft .NET Frameworkがインストールされていること。
  Exchange 2007の場合、Microsoft .NET Frameworkのバージョンは2.0以上である必要があります。
  Exchange 2010以降の場合、Microsoft .NET Frameworkのバージョンは3.5以上である必要があります。
- Exchange ライター for VSS がオンになっていること。

注意
Exchangeエージェントを動作させるためには一時的なストレージが必要です。デフォルトでは、一時ファイルは%ProgramData%\Acronis\Tempに格納されています。%ProgramData% フォルダが存在するボリュームの空き領域が Exchange データベースのサイズの 15 パーセント以上であることを確認してください。Exchangeバックアップを作成する前に、一時ファイルのロケーションを変更することもできます。詳細については、「一時ファイルおよびフォルダのロケーションを変更する（40040）」を参照してください。

ドメインコントローラーを使用する場合、次の要件を満たす必要があります。

- Active Directoryライターfor VSSがオンになっていること。

保護計画を作成するときに、以下のことを確認してください。

- 物理マシンと、エージェントがインストールされているマシンでは、[ボリュームシャドウコピーサービス（VSS）] バックアップオプションが有効になっていること。
- 仮想マシンでは、[仮想マシンのボリュームシャドウコピーサービス（VSS）] バックアップオプションが有効であること。

アプリケーション認識型バックアップのその他の要件

保護計画を作成するときに、バックアップで **[マシン全体]** が選択されていることを確認します。保護計画で、**セクタ単位**のバックアップオプションを無効にする必要があります。無効にしないと、そのようなバックアップからアプリケーションデータを復元することはできません。自動的に**セクタ単位**モードに切り替わったことにより、計画がこのモードで実行された場合、アプリケーションデータの復元もできなくなります。

ESXi仮想マシンの要件

VMwareエージェントによりバックアップされている仮想マシンでアプリケーションを実行する場合は、次の要件を満たす必要があります。

- バックアップされている仮想マシンが、VMware文書の「Windows Backup Implementations」の記事（https://code.vmware.com/docs/1674/virtual-disk-programming-guide/doc/vddkBkupVadp.9.6.html）に記載されているアプリケーション一貫性のあるバックアップと復元の要件を満たしていること。
- マシンに最新のVMware Toolsがインストールされていること。
- マシンでユーザーアカウント制御（UAC）が無効であること。UACを無効にしない場合は、アプリケーションバックアップを有効にするときに、ビルトインのドメイン管理者（ドメイン¥管理者）の資格情報が必要になります。
  UACを無効にしない場合は、アプリケーションバックアップを有効にするときに、ビルトインのドメイン管理者（ドメイン¥管理者）の資格情報が必要になります。

  注意
  ドメイン作成時に構成された、ビルトインのドメイン管理者アカウントを使用します。後から作成されたアカウントはサポート対象外です。

Hyper-V仮想マシンの要件

Hyper-Vエージェントによりバックアップされている仮想マシンでアプリケーションを実行する場合は、次の要件を満たす必要があります。

- ゲストオペレーティングシステムはWindows Server 2008以降です。
- Hyper-V 2008 R2の場合: ゲストオペレーティングシステムはWindows Server 2008/2008 R2/2012です。
- 仮想マシンにダイナミックディスクがありません。
- Hyper-Vホストとゲストオペレーティングシステムの間にネットワーク接続が存在しています。これは、仮想マシン内でリモートWMIクエリを実行するために必要です。
- マシンでユーザーアカウント制御（UAC）が無効であること。UACを無効にしない場合は、アプリケーションバックアップを有効にするときに、ビルトインのドメイン管理者（ドメイン¥管理者）の資格情報が必要になります。
  UACを無効にしない場合は、アプリケーションバックアップを有効にするときに、ビルトインのドメイン管理者（ドメイン¥管理者）の資格情報が必要になります。

  注意
  ドメイン作成時に構成された、ビルトインのドメイン管理者アカウントを使用します。後から作成されたアカウントはサポート対象外です。

- 仮想マシン構成は次の条件を満たします。
  - 最新のHyper-V統合サービスがインストールされていること。重要なアップデートは、https://support.microsoft.com/en-us/help/3063109/hyper-v-integration-components-update-for-windows-virtual-machines
  - 仮想マシン設定で、**[管理]** > **[統合サービス]** > **[バックアップ（ボリュームチェックポイント）]** オプションが有効になっていること。
  - Hyper-V 2012以降の場合: 仮想マシンにチェックポイントがないこと。
  - Hyper-V 2012 R2以降の場合: 仮想マシンにSCSIコントローラがあること（**[設定]** > **[ハードウェア]** をチェック）。

データベースのバックアップ

データベースをバックアップする前に [前提条件] のリストに載っている要件が満たされていることを確認します。

下記のようにデータベースを選択し、保護計画のその他の設定を必要に応じて指定します。

SQLデータベースの選択

SQLデータベースのバックアップには、データベースファイル（.mdf、.ndf）、ログファイル（.ldf）、その他の関連ファイルが含まれます。ファイルはSQLライターサービスを使用してバックアップされます。ボリュームシャドウコピーサービス（VSS）がバックアップまたは復元を要求する時点で、サービスが実行されている必要があります。

バックアップが成功するたびに、SQLトランザクションログが切り捨てられます。SQLログの切り捨ては、保護計画のオプションで無効にできます。

SQLデータベースの選択手順

1. **[デバイス]** > **[Microsoft SQL]** をクリックします。
   SQLサーバーのAlways On可用性グループ（AAG）、Microsoft SQL Serverを実行するコンピュータ、SQLサーバーインスタンス、データベースのツリーが表示されます。
2. バックアップするデータを参照します。
   ツリーノードを展開するか、ツリーの右側にあるリストの項目をダブルクリックします。
3. バックアップするデータを選択します。AAG、SQLサーバーを実行するコンピュータ、SQLサーバーインスタンス、または個々のデータベースを選択できます。
   - AAGを選択すると、選択したAAGに含まれている全データベースがバックアップされます。AAGのバックアップまたは個別のAAGデータベースの詳細については、「Always On可用性グループ（AAG）の保護」を参照してください。
   - SQLサーバーを実行するマシンを選択すると、選択したマシンが実行している全SQLサーバーインスタンスに接続されている全データベースがバックアップされます。
   - SQLサーバーインスタンスを選択すると、選択したインスタンスに接続されているすべてのデータベースがバックアップされます。
   - データベースを直接選択する場合、選択したデータベースのみがバックアップされます。
4. **[保護]** をクリックします。ログイン情報を求められた場合は、SQL Serverデータにアクセスするためのログイン情報を入力します。
   Windows認証を使用する場合、アカウントは、マシンの**バックアップオペレーター**または**Administrators**グループのメンバー、およびバックアップ対象の各インスタンスで**sysadmin**ロールのメンバーである必要があります。
   SQLサーバー認証を使用する場合、アカウントは、バックアップ対象の各インスタンスで**sysadmin**ロールのメンバーである必要があります。

Exchange Serverデータの選択

以下の表は、バックアップ対象として選択できる Microsoft Exchange Server データと、データのバックアップに最低限必要なユーザー権限を示しています。

Exchangeのバージョン	データアイテム	ユーザー権限
2007	ストレージ グループ	**Exchange Organization Management** 役割グループのメンバーシップ
2010/2013/2016/2019	データベース、データベース可用性グループ（DAG）	**サーバー管理**役割グループのメンバーシップ

完全バックアップには、選択したすべてのExchange Server データが含まれます。

増分バックアップには、データベース ファイルの変更ブロック、チェックポイントファイル、対応するデータベース チェックポイントより新しい小さい番号のログ ファイルが含まれます。データベースファイルへの変更はバックアップに含まれているので、前回のバックアップ以降のトランザクション ログ レ

コードをすべてバックアップする必要はありません。チェックポイントより新しいログのみ、復元後に再生される必要があります。これにより、循環ログ方式が有効になっていても、復元にかかる時間が短縮され、正常なデータベースバックアップを確実に行えます。

バックアップが成功するたびにトランザクションログファイルが切り捨てられます。

Exchange Serverデータの選択手順

1. **[デバイス]** > **[Microsoft Exchange]** をクリックします。
   Exchange Serverのデータベース可用性グループ（DAG）、Microsoft Exchange Serverを実行するマシン、およびExchange Serverデータベースのツリーが表示されます。"メールボックスのバックアップ"（557ページ）の説明に従ってExchangeエージェントを設定すると、メールボックスもこのツリーに表示されます。
2. バックアップするデータを参照します。
   ツリーノードを展開するか、ツリーの右側にあるリストの項目をダブルクリックします。
3. バックアップするデータを選択します。
   - DAGを選択すると、クラスター化された各データベースのコピーがそれぞれバックアップされます。DAGのバックアップの詳細については、"データベース可用性グループ（DAG）の保護"（553ページ）を参照してください。
   - Microsoft Exchange Serverを実行するコンピュータを選択すると、選択したコンピュータで実行されているExchange Serverにマウントされている全データベースがバックアップされます。
   - データベースを直接選択する場合、選択したデータベースのみがバックアップされます。
   - "メールボックスのバックアップ"（557ページ）の説明に従ってExchangeエージェントを設定すると、バックアップするメールボックスを選択できます。

   複数のデータベースを選択した場合、2件ずつ処理されます。最初のグループのバックアップが終了すると、次のグループのバックアップが開始されます。
4. ログイン情報を求められた場合は、データにアクセスするためのログイン情報を入力します。
5. **[保護]** をクリックします。

Always On可用性グループ（AAG）の保護

注意
この機能は、Advanced Backupパックで利用可能です。

SQL Server高可用性ソリューションの概要

Windowsサーバーフェールオーバークラスタリング（WSFC）機能を使用すると、インスタンスレベル（Failover Cluster Instance（FCI））またはデータベースレベル（AlwaysOn可用性グループ（AAG））での冗長性を活用して、高可用性のSQLサーバーを構成できるようになります。両方のメソッドを組み合わせることもできます。

Failover Cluster Instance では、SQL データベースが共有ストレージ上に配置されます。このストレージは、アクティブなクラスタノードからのみアクセスできます。アクティブ ノードに障害が発生した場合、フェイルオーバーが発生し、別のノードがアクティブになります。

可用性グループでは、各データベースのレプリカは異なるノード上に存在します。プライマリ レプリカが使用できなくなった場合は、別のノード上に存在するセカンダリ レプリカにプライマリ ロールが割り当てられます。

つまり、クラスタは自体が既に障害復元ソリューションとしての役割を果たしています。ただし、データベースが論理破損した場合や、クラスタ全体がダウンしている場合など、クラスタがデータを保護できないこともあります。また、有害なコンテンツの変更は通常、すべてのクラスタ ノードに即座にレプリケートされるため、クラスタ ソリューションではこのような変更からは保護されません。

サポートされているクラスタ構成

このバックアップソフトウェアでは、SQL Server 2012以降のAlwaysOn可用性グループ（AAG）のみをサポートしています。フェールオーバークラスタインスタンス、データベースミラーリング、ログ配布など、その他のクラスタ構成はサポートされていません。

クラスタ データのバックアップおよび復元に必要なエージェントの数

クラスタのデータを正常にバックアップおよび復元するには、WSFCクラスタの各ノードにエージェントfor SQLをインストールする必要があります。

AAGに含まれるデータベースのバックアップ

1. エージェントfor SQLをWSFCクラスタの各ノードにインストールします。
2. 「SQLデータベースの選択」に従って、バックアップするAAGを選択します。
   AAGのすべてのデータベースをバックアップするには、AAG自体を選択する必要があります。データベースのセットをバックアップするには、AAGのすべてのノードのデータベースセットを定義します。

   警告
   データベースセットはすべてのノードで完全に同じである必要があります。1つでも異なるセットがあるか、すべてのノードで定義されていない場合、クラスターバックアップが正しく動作しません。

3. [クラスターバックアップモード]バックアップオプションを設定します。

AAGに含まれるデータベースの復元

1. 復元するデータベースを選択し、データベースを復元するリカバリポイントを選択します。
   [デバイス] > **[Microsoft SQL]** > **[データベース]** でクラスタ化済みデータベースを選択し、**[復元]** をクリックすると、選択されたデータベースのコピーがバックアップされた時点と一致するリカバリポイントのみが表示されます。
   クラスター化されたデータベースのすべての復元ポイントを表示する最も簡単な方法は、[バックアップストレージ] タブでAAG全体のバックアップを選択することです。AAGのバックアップ名は、**<AAG名>** - **<保護計画名>**テンプレートに基づいていて、特別なアイコンが付いています。
2. 復元を設定するには、「SQLデータベースの復元」の手順5以降に従います。

データの復元先となるクラスタノードが自動的に定義されます。ノードの名前が、[**復元先**] フィールドに表示されます。ターゲットノードは手動で変更できます。

重要
AlwaysOn可用性グループ（AAG）に含まれているデータベースを、復元時に上書きすることはできません。Microsoft SQL Serverによって禁止されているためです。復元前にAAGからターゲットデータベースを除外する必要があります。あるいは、新しい AAG 以外のデータベースとしてデータベースを復元します。復元が完了したら、元のAAGの設定を再構成できます。

データベース可用性グループ（DAG）の保護

注意
この機能は、Advanced Backupパックで利用可能です。

Exchange Serverクラスタの概要

Exchange クラスタには、データベースの高可用性、高速フェールオーバーを提供し、データ損失がないという大きな特徴があります。通常、このためには、クラスタ メンバ（クラスタ ノード）上にデータベースまたはストレージ グループを配置します。アクティブ データベース コピーをホストしているクラスタ ノード、またはアクティブ データベース コピー自体に不具合が発生した場合、パッシブ コピーをホストしているもう 1 つのノードが不具合を起こしたノードの操作を自動的に引き継ぎ、Exchange サービスへのアクセスを提供し、中断時間を最小限に抑えます。つまり、クラスタは自体が既に障害復元ソリューションとしての役割を果たしています。

ただし、データベースが論理破損した、クラスタに含まれる特定のデータベースのコピー（レプリカ）がない、クラスタ全体がダウンしている場合など、フェールオーバー クラスタ ソリューションがデータ保護できないこともあります。また、有害なコンテンツの変更は通常、すべてのクラスタ ノードに即座にレプリケートされるため、クラスタ ソリューションではこのような変更からは保護されません。

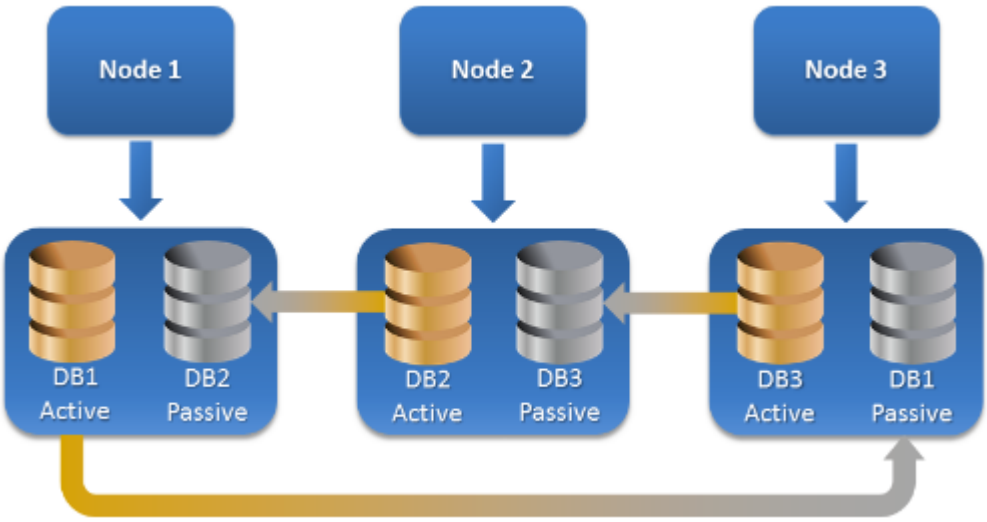
クラスター認識型バックアップ

クラスター認識型バックアップでは、クラスター化されたデータの単一のコピーのみをバックアップします。データのロケーションがクラスター内で変更されたとしても（たとえば、切り替え、またはフェールオーバーのため）、このデータの再配置はすべて追跡され、確実にバックアップされます。

サポートされているクラスタ構成

クラスター認識型バックアップは、Exchange Server 2010 以降のデータベース可用性グループ（DAG）に対してのみサポートされています。Exchange 2007 のシングルコピークラスター（SCC）やクラスター連続レプリケーション（CCR）などのその他のクラスター設定はサポートされていません。

DAG は、最大 16 の Exchange メールボックス サーバーからなるグループです。すべてのノードが他のノードのメールボックス データベース コピーをホスティングできます。それぞれのノードは、パッシブおよびアクティブのデータベース コピーをホスティングすることができます。各データベースのコピーは、最大 16 個まで作成することができます。



クラスター認識型バックアップおよび復元に必要なエージェントの数

クラスター化されたデータベースを正常にバックアップおよび復元するには、Exchange クラスターの各ノードに Exchangeエージェントをインストールする必要があります。

注意
ノードの1台にエージェントをインストールすると、Cyber Protectコンソールの **[デバイス]** > **[Microsoft Exchange]** > **[データベース]** に、DAGとDAGのノードが表示されます。残りのノードにエージェントfor Exchangeをインストールするには、DAGを選択し、**[詳細]** をクリックして、各ノードの横にある **[エージェントのインストール]** をクリックします。

Exchange クラスタ データのバックアップ

1. 保護計画を作成する場合は、DAGを選択します（"Exchange Serverデータの選択"（550ページ）を参照）。
2. "クラスターバックアップモード"（447ページ）バックアップオプションを構成します。
3. 必要に応じて、保護計画のその他の設定を指定します。

重要
クラスター認識型バックアップでは、必ずDAG自体を選択してください。DAG 内の個々のノードまたはデータベースを選択する場合は、選択されたアイテムのみがバックアップされ、**[クラスターバックアップモード]** オプションは無視されます。

Exchangeクラスタデータの復元

1. 復元するデータベースの復元ポイントを選択します。1 つのクラスター全体を復元の対象として選択することはできません。
   [デバイス] > **[Microsoft Exchange]** > **[データベース]** > **<クラスター名>** > **<ノード名>** でクラスター化されたデータベースのコピーを 1 つ選択し、**[復元]** をクリックすると、このコピーがバックアップされた時点と一致する復元ポイントのみが表示されます。

クラスター化されたデータベースのすべての復元ポイントを表示する最も簡単な方法は、[バックアップストレージ] タブでそのバックアップを選択することです。

2. "Exchangeデータベースの復元"（567ページ）の手順5以降に従います。
   データの復元先となるクラスタノードが自動的に定義されます。ノードの名前が、**[復元先]** フィールドに表示されます。ターゲットノードは手動で変更できます。

アプリケーション認識型バックアップ

ディスクレベルのアプリケーション認識型バックアップは、物理マシン、ESXi仮想マシン、およびHyper-V仮想マシンで使用できます。

Microsoft SQL Server、Microsoft Exchange Server、または Active Directory ドメインサービスを実行するマシンをバックアップするときには、これらのアプリケーションデータをさらに保護するために、**アプリケーションバックアップ**を有効にします。

なぜアプリケーション認識型バックアップを使用するのですか。

アプリケーション認識型バックアップを使用すると、次のことを保証できます。

- アプリケーションは一貫した状態でバックアップされるため、コンピュータが復元された直後に使用できます。
- コンピュータ全体を復元せずに、SQLおよびExchangeデータベース、メールボックス、メールボックスアイテムを復元できます。
- バックアップが成功するたびに、SQLトランザクションログが切り捨てられます。SQLログの切り捨ては、保護計画のオプションで無効にできます。Exchangeトランザクションログは、仮想コンピュータでのみ切り捨てられます。物理マシンで Exchange トランザクションログを切り捨てる場合は、VSS 完全バックアップオプションを有効にできます。
- ドメインに複数のドメインコントローラがあり、いずれかを復元する場合は、権限のない復元が実行され、USNロールバックが復元後に発生しません。

アプリケーション認識型バックアップを使用するために必要なものは何でしょうか。

物理コンピュータでは、Windowsエージェントに加えて、SQLエージェント、Exchangeエージェント、または両方をインストールする必要があります。

仮想マシンでは、エージェントをインストールする必要はありません。マシンは、VMware（Windows）エージェントまたはHyper-Vエージェントによりバックアップされることが前提になっています。

注意
Windows Server 2022が動作するHyper-VおよびVMware ESXi仮想マシンの場合、エージェントレスモード（Hyper-Vエージェントまたは VMwareエージェントいずれかによるバックアップの実行）を使用するアプリケーション認識型バックアップはサポートされていません。これらのマシン上でMicrosoftアプリケーションを保護するには、ゲストオペレーティングシステムにWindowsエージェントをインストールする必要があります。

VMwareエージェント（仮想アプライアンス）によってアプリケーション認識型バックアップを作成できますが、このバックアップからアプリケーションデータを復元することはできません。このエージェントによって作成されたバックアップからアプリケーションデータを復元するには、VMwareエージェント（Windows）、SQLエージェント、またはExchangeエージェントが、バックアップの保存されているロケーションにアクセスできるマシンに存在する必要があります。アプリケーションデータの復元を設定する場合、**[バックアップストレージ]** タブで復元ポイントを選択し、**[参照元マシン]** からこのマシンを選択します。

その他の要件は、「前提条件」と「必要なユーザー権限」のセクションに記載されています。

注意
Hyper-V仮想マシンのアプリケーション認識型バックアップは、「WMI『ExecQuery』がクエリを実行できませんでした」というエラーまたは「WMIを介して新しいプロセスを作成できませんでした」というエラーで失敗する場合があります。これは、バックアップが負荷の高いホストで実行されているため、Windows Management Instrumentationからの応答がないか遅延しているためです。これらのバックアップを再試行する場合は、ホストの負荷が低い時間帯を選択してください。

アプリケーション認識型バックアップに必要なユーザー権限

アプリケーション認識型バックアップには、ディスクにあるVSS認識型アプリケーションのメタデータが含まれます。このメタデータにアクセスするには、次に示す適切な権限のアカウントがエージェントに必要となります。アプリケーションバックアップを有効にするときには、このアカウントを指定する必要があります。

- SQL Server:
  アカウントは、マシンの**バックアップオペレーター** または **管理者**グループのメンバー、およびバックアップ対象の各インスタンスで**sysadmin**の役割のメンバーである必要があります。

  注意
  Windows認証のみがサポートされています。

- Exchange Server:
  Exchange 2007:アカウントは、マシンの**管理者**グループのメンバーであるとともに、**Exchange組織管理者**ロールグループのメンバーである必要があります。
  Exchange 2010以降:アカウントは、マシンの**管理者**グループのメンバーであるとともに、**組織管理**ロールグループのメンバーである必要があります。

- Active Directory:
  アカウントはドメイン管理者である必要があります。

ESXi仮想マシンの追加要件

VMwareエージェントまたはHyper-Vエージェントによりバックアップされている仮想マシンでアプリケーションを実行する場合は、ユーザーアカウント制御（UAC）がマシンで無効であることを確認します。

UACを無効にしない場合は、アプリケーションバックアップを有効にするときに、ビルトインのドメイン管理者（ドメイン¥管理者）の資格情報が必要になります。

注意
ドメイン作成時に構成された、ビルトインのドメイン管理者アカウントを使用します。後から作成されたアカウントはサポート対象外です。

Windowsを実行するマシンに関する追加の要件

Windows（すべてのバージョン）では、ユーザーアカウント制御（UAC）ポリシーを無効化して、アプリケーション認識型バックアップを許可する必要があります。

UACを無効にしない場合は、アプリケーションバックアップを有効にするときに、ビルトインのドメイン管理者（ドメイン¥管理者）の資格情報が必要になります。

注意
ドメイン作成時に構成された、ビルトインのドメイン管理者アカウントを使用します。後から作成されたアカウントはサポート対象外です。

WindowsでUACポリシーを無効化するには

1. レジストリエディタで、次のレジストリキーを見つけます。
   `HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System`
2. **EnableLUA**の値を**0**に変更します。
3. コンピュータを再起動します。

メールボックスのバックアップ

メールボックスのバックアップは、Microsoft Exchange Server 2010 Service Pack 1（SP1）以降でのみサポートされています。

1つ以上のエージェントfor ExchangeがManagement Serverに登録されている場合は、メールボックスバックアップが利用可能です。エージェントは、Microsoft Exchange Serverと同じActive Directoryフォレストに属しているマシンにインストールされている必要があります。

メールボックスをバックアップする前に、Exchangeエージェントを Microsoft Exchange Server の**クライアントアクセス**サーバーロール（CAS）を実行するマシンに接続する必要があります。Exchange 2016 以降では、別個のインストールオプションとして CAS ロールは使用できません。それはメール

ボックスサーバーの役割の一部として自動的にインストールされます。したがって、**メールボックスロール**を実行中の任意のサーバーにエージェントを接続できます。

注意
データベースバックアップおよびアプリケーション認識型バックアップからもメールボックス/メールボックス項目をリカバリできます。詳細については、"Exchange メールボックスとメールボックスのアイテムを復元"（570ページ）を参照してください。データベースバックアップとアプリケーション認識型バックアップでは、個別のメールボックスの保護計画を作成できません。

エージェントfor ExchangeをCASに接続するには

1. **[デバイス]** > **[追加]** をクリックします。
2. **[Microsoft Exchange Server]** をクリックします。
3. **[Exchange メールボックス]** をクリックします。
   管理サーバーに Exchangeエージェントが登録されていない場合は、エージェントをインストールすることを勧められます。インストール後、この操作を手順 1 から繰り返します。
4. （オプション）複数の Exchangeエージェントが管理サーバーに登録されている場合は、**[エージェント]** をクリックし、バックアップを実行するエージェントを変更します。
5. **[クライアントアクセスサーバー]** で、Microsoft Exchange Server の**クライアントアクセス**の役割が有効なマシンの完全修飾ドメイン名（FQDN）を指定します。
   Exchange 2016 以降では、クライアントアクセスサービスがメールボックスサーバーの役割の一部として自動的にインストールされます。したがって、**メールボックスロール**を実行中の任意のサーバーを指定できます。このセクションの後半では、このサーバーを CAS と呼びます。
6. **[認証タイプ]** で、CASによって使用される認証タイプを選択します。**[Kerberos]**（デフォルト）または **[ベーシック]** を選択できます。
7. （ベーシックな認証のみ）使用するプロトコルを選択します。**[HTTPS]**（デフォルト）または **[HTTP]** を選択できます。
8. （HTTPS プロトコルを使用したベーシックな認証のみ）CAS が認証機関から取得した SSL 証明書を使用していて、CAS への接続時に証明書を確認する場合は、**[SSL 証明書を確認]** チェックボックスをオンにします。それ以外の場合は、この手順をスキップします。
9. CAS にアクセスするために使用するアカウントの資格情報を入力します。このアカウントの要件は、「必要なユーザー権限」に記載されています。
10. **[追加]** をクリックします。

その結果、**[デバイス]** > **[Microsoft Exchange]** > **[メールボックス]** にメールボックスが表示されます。

Exchange Serverメールボックスの選択

下記のようにメールボックスを選択し、保護計画のその他の設定を必要に応じて指定します。

Exchangeのメールボックスを選択するには

1. **[デバイス]** > **[Microsoft Exchange]** をクリックします。
   Exchange データベースとメールボックスのツリーが表示されます。

2. [**メールボックス**] をクリックし、バックアップするメールボックスを選択します。
3. [**保護**] をクリックします。

必要なユーザー権限

メールボックスにアクセスするには、Exchange エージェントに適切な権限を持つアカウントが必要です。メールボックスでさまざまな操作を設定するときに、このアカウントを指定するよう求められます。

組織管理役割グループのアカウントメンバーシップは、将来作成されるメールボックスを含むすべてのメールボックスにアクセスすることを可能にします。

必要な最小限のユーザー権限は、次のとおりです。

- アカウントは、**サーバー管理**および**受取人管理**役割グループのメンバーである必要があります。
- アカウントに、エージェントがメールボックスにアクセスするすべてのユーザーまたはユーザーグループに対して有効な、[**ApplicationImpersonation**]管理役割が必要です。
  [**ApplicationImpersonation**] 管理役割の設定については、次のマイクロソフトサポート技術情報の記事を参照してください: https://msdn.microsoft.com/en-us/library/office/dn722376.aspx。

SQL データベースの復元

データベースバックアップおよびアプリケーション認識型バックアップからSQLデータベースをリカバリできます。2つのバックアップタイプの違いについては、"Microsoft SQL ServerとMicrosoft Exchange Serverの保護"（545ページ）を参照してください。

SQLデータベースは、元のインスタンス、元のマシンにある別のインスタンス、または元のマシンではないマシン上のインスタンスにリカバリできます。元のマシン以外に復元する場合、ターゲットマシンにSQLエージェントをインストールする必要があります。

また、データベースをファイルとして復元することもできます。

SQLインスタンスの認証を使用する場合、マシンの**バックアップオペレーター**または**Administrators**グループのメンバー、およびターゲットインスタンスの**sysadmin**ロールのメンバーとなっているアカウントの資格情報を入力する必要があります。SQL Server認証を使用する場合、ターゲットインスタンスの**sysadmin**ロールのメンバーとなっているアカウントの資格情報を入力する必要があります。

システムデータベースはユーザーデータベースと同様にリカバリできますが、いくつか異なる点があります。これらの違いの詳細については、"システムデータベースの復元"（566ページ）を参照してください。

復元中は、Cyber Protectコンソールの [**監視**] > [**アクティビティ**] タブで処理の進行状況を確認できます。

SQLデータベースを元のマシンにリカバリする

SQLデータベースは、元のインスタンス、元のマシンにある別のインスタンス、または元のマシンではないターゲットマシン上のインスタンスにリカバリできます。

SQLデータベースを元のマシンにリカバリするには

データベースバックアップから

1. Cyber Protectコンソールで、**[デバイス]** > **[Microsoft SQL]** に進みます。
2. SQL Serverインスタンスを選択するか、インスタンス名をクリックしてリカバリする特定のデータベースを選択してから、**[復元]** をクリックします。

   マシンがオフラインになっている場合、復元ポイントは表示されません。元のマシン以外にデータをリカバリする手順については、"SQLデータベースを元のマシン以外にリカバリする"（562ページ）を参照してください。
3. リカバリ ポイントを選択します。

   復元ポイントは、ロケーションでフィルタリングされます。
4. **[復元]** > **[データベースをインスタンスに]** の順にクリックします。

   デフォルトでは、インスタンスおよびデータベースは元のデータベースにリカバリされます。また、元のデータベースを新しいデータベースとしてリカバリすることもできます。
5. （同じマシンで元のインスタンス以外にリカバリする場合）**[ターゲットSQL Serverインスタンス]** をクリックして、ターゲットインスタンスを選択してから、**[完了]** をクリックします。
6. （新しいデータベースとして復元する場合）データベース名をクリックし、**[復元先]** で **[新しいデータベース]** を選択します。
   - 新しいデータベース名を指定します。
   - 新しいデータベースのパスを指定します。
   - ログのパスを指定します。
7. （オプション）（データベースを新規にリカバリする場合は利用できない）復元後にデータベースの状態を変更するには、データベース名をクリックして、以下のいずれかのステータスを選択してから **[完了]** をクリックします。
   - **使用可（復元モードで復元）**（デフォルト）

     復元が完了した後にデータベースが使用可能になります。ユーザーは復元されたデータベースに対してフルアクセス権を持ちます。トランザクションログに保存されている、復元されたデータベースのすべてのコミットされていないトランザクションはロールバックされます。Microsoft SQL ネイティブのバックアップから追加のトランザクション ログを復元することはできません。
   - **使用不可（復元なしモードで復元）**

     復元が完了した後、データベースは非稼動の状態になります。ユーザーはこのデータベースにアクセスできなくなります。復元されたデータベースのコミットされていないトランザクションはすべて保持されます。Microsoft SQL ネイティブのバックアップから追加のトランザクション ログを復元して必要なリカバリ ポイントにアクセスできます。
   - **読み取り専用（スタンバイ モードで復元）**

     復元が完了すると、ユーザーはデータベースに読み取り専用でアクセスできるようになります。コミットされていないトランザクションは取り消されます。ただし、元に戻す処理は一時スタンバイ ファイルに保存され、復元により何らかの影響が発生しても元に戻すことができるようになります。

     この値は主に、SQL Serverのエラーが発生した時点を検出するために使用されます。
8. **[復元を開始]** をクリックします。

アプリケーション認識型バックアップから

1. Cyber Protectコンソールで **[デバイス]** > **[すべてのデバイス]** に進みます。
2. リカバリするデータが存在していたマシンを選択してから、**[復元]** をクリックします。

   マシンがオフラインになっている場合、復元ポイントは表示されません。元のマシン以外にデータをリカバリする手順については、"SQLデータベースを元のマシン以外にリカバリする"（562ページ）を参照してください。
3. リカバリ ポイントを選択します。

   復元ポイントは、ロケーションでフィルタリングされます。
4. **[復元]** > **[SQLデータベース]** の順にクリックします。
5. SQL Serverインスタンスを選択するか、インスタンス名をクリックしてリカバリする特定のデータベースを選択してから、**[復元]** をクリックします。

   デフォルトでは、インスタンスおよびデータベースは元のデータベースにリカバリされます。また、元のデータベースを新しいデータベースとしてリカバリすることもできます。
6. （同じマシンで元のインスタンス以外にリカバリする場合）**[ターゲットSQL Serverインスタンス]** をクリックして、ターゲットインスタンスを選択してから、**[完了]** をクリックします。
7. （新しいデータベースとして復元する場合）データベース名をクリックし、**[復元先]** で **[新しいデータベース]** を選択します。
   - 新しいデータベース名を指定します。
   - 新しいデータベースのパスを指定します。
   - ログのパスを指定します。
8. （オプション）（データベースを新規にリカバリする場合は利用できない）復元後にデータベースの状態を変更するには、データベース名をクリックして、以下のいずれかのステータスを選択してから **[完了]** をクリックします。
   - **使用可（復元モードで復元）**（デフォルト）

     復元が完了した後にデータベースが使用可能になります。ユーザーは復元されたデータベースに対してフルアクセス権を持ちます。トランザクションログに保存されている、復元されたデータベースのすべてのコミットされていないトランザクションはロールバックされます。Microsoft SQL ネイティブのバックアップから追加のトランザクション ログを復元することはできません。
   - **使用不可（復元なしモードで復元）**

     復元が完了した後、データベースは非稼動の状態になります。ユーザーはこのデータベースにアクセスできなくなります。復元されたデータベースのコミットされていないトランザクションはすべて保持されます。Microsoft SQL ネイティブのバックアップから追加のトランザクション ログを復元して必要なリカバリ ポイントにアクセスできます。
   - **読み取り専用（スタンバイ モードで復元）**

     復元が完了すると、ユーザーはデータベースに読み取り専用でアクセスできるようになります。コミットされていないトランザクションは取り消されます。ただし、元に戻す処理は一時スタンバイ ファイルに保存され、復元により何らかの影響が発生しても元に戻すことができるようになります。

     この値は主に、SQL Serverのエラーが発生した時点を検出するために使用されます。
9. **[復元を開始]** をクリックします。

SQLデータベースを元のマシン以外にリカバリする

SQLエージェントがインストールされている、元のマシンではないターゲットマシン上のSQL Serverインスタンスに対して、アプリケーション認識型バックアップとデータベースバックアップの両方をリカバリできます。バックアップはクラウドストレージまたはターゲットマシンがアクセスできる共有ストレージに配置する必要があります。

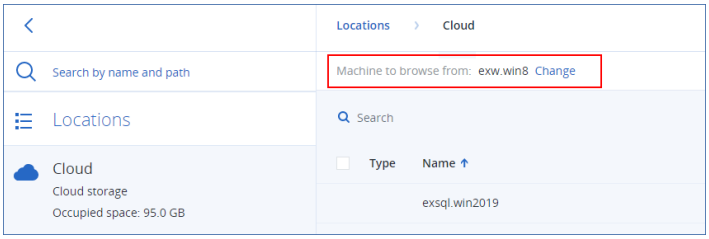
ターゲットマシンのSQL Serverバージョンは、ソースマシンのバージョン以降でなければなりません。

SQLデータベースを元のマシン以外にリカバリするには

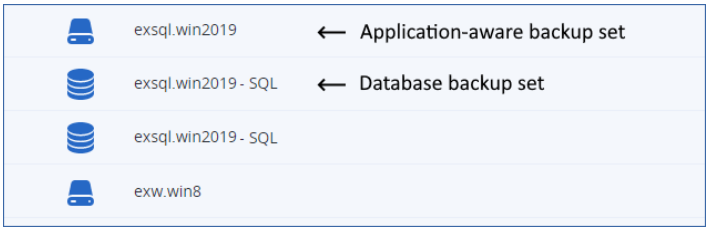
バックアップストレージから

この手順は、アプリケーション認識型バックアップとデータベースバックアップに適用されます。

1. Cyber Protectコンソールで、**[バックアップストレージ]** に移動します。
2. データをリカバリするバックアップセットのロケーションを選択します。
3. **[参照元マシン]** で、ターゲットマシンを選択します。
   これはデータをリカバリするマシンです。ターゲットマシンはオンライン状態でなければなりません。



4. バックアップセットを選択してから、**[操作]** ペインで **[バックアップを表示]** をクリックします。
   アプリケーション認識型バックアップセットとデータベースバックアップセットでは、アイコンが異なります。



5. データを復元する復元ポイントを選択します。
6. （データベースバックアップの場合）**[SQLデータベースをリカバリ]** をクリックします。
7. （アプリケーション認識型バックアップの場合）**[復元]** > **[SQLデータベース]** の順にクリックします。
8. SQL Serverインスタンスを選択するか、インスタンス名をクリックしてリカバリする特定のデータベースを選択してから、**[復元]** をクリックします。
9. （ターゲットマシンに複数のSQLインスタンスがある場合）**[ターゲットSQL Serverインスタンス]** をクリックして、ターゲットインスタンスを選択してから、**[完了]** をクリックします。

10. データベース名をクリックし、新しいデータベースパスとログパスを指定してから、**[完了]** をクリックします。
    以下のように両方のフィールドに同じパスを指定することができます。

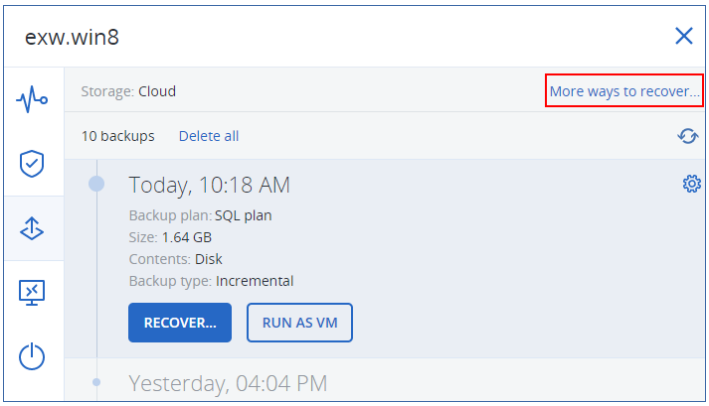
    ```
    C:\Program Files\Microsoft SQL Server\MSSQL16.MSSQLSERVER\MSSQL\DATA\
    ```

11. **[復元を開始]** をクリックします。

デバイスから

この手順は、アプリケーション認識型バックアップのみに適用されます。

1. Cyber Protectコンソールで **[デバイス]** > **[すべてのデバイス]** に進みます。
2. リカバリするデータが存在していたマシンを選択してから、**[復元]** をクリックします。
3. （ソースマシンがオンラインの場合）**[その他の復元方法]** をクリックします。



4. **[マシンを選択]** をクリックしてターゲットマシンを選択してから、**[OK]** をクリックします。
    これはデータをリカバリするマシンです。ターゲットマシンはオンライン状態でなければなりません。
5. リカバリ ポイントを選択します。
    復元ポイントは、ロケーションでフィルタリングされます。
6. **[復元]** > **[SQLデータベース]** の順にクリックします。
7. SQL Serverインスタンスを選択するか、インスタンス名をクリックしてリカバリする特定のデータベースを選択してから、**[復元]** をクリックします。
8. （ターゲットマシンに複数のSQLインスタンスがある場合）**[ターゲットSQL Serverインスタンス]** をクリックして、ターゲットインスタンスを選択してから、**[完了]** をクリックします。
9. データベース名をクリックし、新しいデータベースパスとログパスを指定してから、**[完了]** をクリックします。
    以下のように両方のフィールドに同じパスを指定することができます。

    ```
    C:\Program Files\Microsoft SQL Server\MSSQL16.MSSQLSERVER\MSSQL\DATA\
    ```

10. **[復元を開始]** をクリックします。

SQLデータベースをファイルとして復元する

データベースをファイルとして復元できます。このオプションは、サードパーティのツールでデータマイニング、監査またはさらなる処理を行うためにデータを抽出する場合に役立つかもしれません。SQL ServerインスタンスにSQLデータベースファイルを添付する方法については、"SQL Server データベースの接続"（566ページ）を参照してください。

SQLエージェントがインストールされている元のマシンまたは元のマシンではないターゲットマシンに、データベースをファイルとしてリカバリできます。元のマシン以外にデータをリカバリする場合、バックアップはクラウドストレージまたはターゲットマシンがアクセスできる共有ストレージに配置する必要があります。

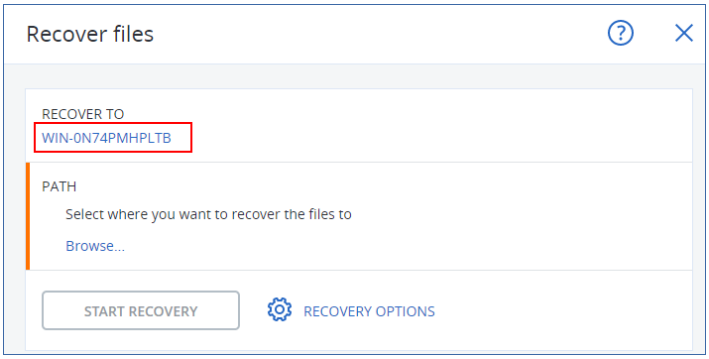
注意
VMwareエージェント（Windows）を使用する場合、データベースをファイルとして復元する方法のみを使用できます。VMwareエージェント（仮想アプライアンス）を使用してデータベースを復元することはできません。

SQLデータベースをファイルとして復元するには

データベースバックアップから

この手順は、オンラインソースマシンに適用されます。

1. Cyber Protectコンソールで、**[デバイス]** > **[Microsoft SQL]** に進みます。
2. リカバリするデータベースを選択してから、**[復元]** をクリックします。
3. リカバリ ポイントを選択します。
   復元ポイントは、ロケーションでフィルタリングされます。
4. **[復元]** > **[データベースをファイルとして]** をクリックします。
5. （元のマシン以外にリカバリする場合）**復元先**で、ターゲットマシンを選択します。
   これはデータをリカバリするマシンです。ターゲットマシンはオンライン状態でなければなりません。
   選択を変更するには、マシン名をクリックして別のマシンを選択してから、**[OK]** をクリックします。

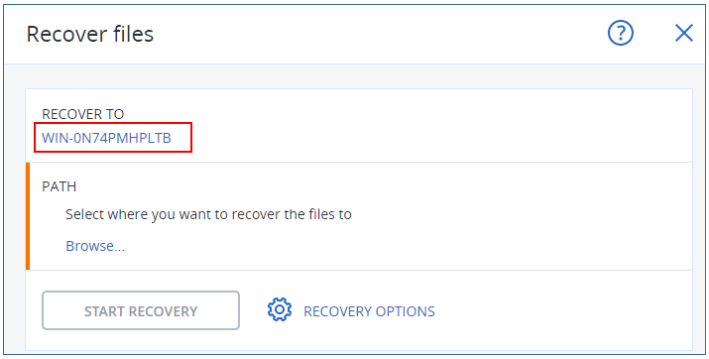


6. **パス**で、**[参照]** をクリックし、ファイルの保存先となるローカルフォルダまたはネットワークフォルダを選択してから、**[完了]** をクリックします。
7. **[復元を開始]** をクリックします。

アプリケーション認識型バックアップから

この手順は、オンラインソースマシンに適用されます。

1. Cyber Protectコンソールで **[デバイス]** > **[すべてのデバイス]** に進みます。
2. リカバリするデータが存在していたマシンを選択してから、**[復元]** をクリックします。
3. リカバリ ポイントを選択します。
   復元ポイントは、ロケーションでフィルタリングされます。
4. **[復元]** > **[SQLデータベース]** をクリックし、復元するデータベースを選択してから、**[ファイルとして復元]** をクリックします。
5. （元のマシン以外にリカバリする場合）**復元先**で、ターゲットマシンを選択します。
   これはデータをリカバリするマシンです。ターゲットマシンはオンライン状態でなければなりません。
   選択を変更するには、マシン名をクリックして別のマシンを選択してから、**[OK]** をクリックします。

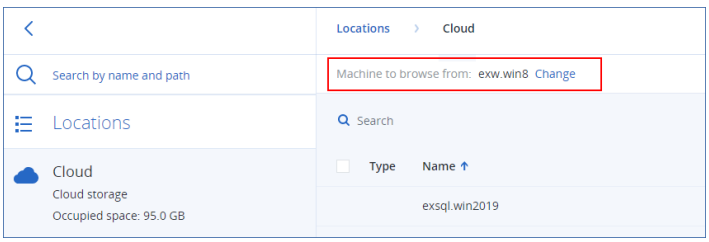


6. **パス**で、**[参照]** をクリックし、ファイルの保存先となるローカルフォルダまたはネットワークフォルダを選択してから、**[完了]** をクリックします。
7. **[復元を開始]** をクリックします。

オフラインのマシンのバックアップから

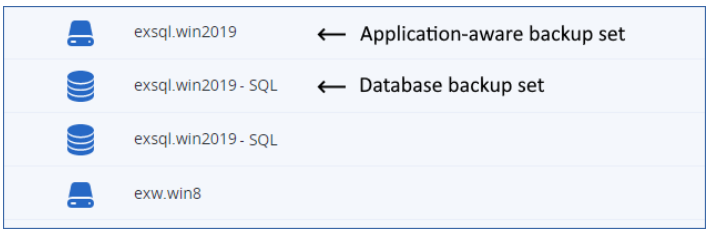
この手順は、オフラインになっているソースマシンのアプリケーション認識型バックアップとデータベースバックアップに適用されます。

1. Cyber Protectコンソールで、**[バックアップストレージ]** に移動します。
2. データをリカバリするバックアップセットのロケーションを選択します。
3. **[参照元マシン]** で、ターゲットマシンを選択します。
   これはデータをリカバリするマシンです。ターゲットマシンはオンライン状態でなければなりません。



4. バックアップセットを選択してから、**[操作]** ペインで **[バックアップを表示]** をクリックします。

アプリケーション認識型バックアップセットとデータベースバックアップセットでは、アイコンが異なります。



5. データを復元する復元ポイントを選択します。
6. （データベースバックアップの場合）[**SQLデータベースをリカバリ**] をクリックします。
7. （アプリケーション認識型バックアップの場合）[**復元**] > [**SQLデータベース**] の順にクリックします。
8. SQL Serverインスタンスを選択するか、インスタンス名をクリックしてリカバリする特定のデータベースを選択してから、[**ファイルとして復元**] をクリックします。
9. **パス**で、[**参照**] をクリックし、ファイルの保存先となるローカルフォルダまたはネットワークフォルダを選択してから、[**完了**] をクリックします。
10. [**復元を開始**] をクリックします。

システムデータベースの復元

インスタンスのすべてのデータベースは、一度に復元されます。システムデータベースを復元する場合、復元先インスタンスは自動的に単一ユーザー モードで再起動します。復元が完了すると、インスタンスが再起動し、他のデータベースが（あれば）復元されます。

システムデータベースを復元する場合、次の点にも注意する必要があります。

- システムデータベースは元のインスタンスと同じバージョンのインスタンスにしか復元できません。
- システムデータベースは必ず「使用可能」な状態で復元されます。

マスターデータベースの復元

システムデータベースには、**マスター**データベースが含まれています。**マスター**データベースには、インスタンスのすべてのデータベースに関する情報が記録されます。そのため、バックアップの**マスター**データベースには、バックアップの時点でインスタンスに存在していたデータベースの情報が格納されています。**マスター**データベースをリカバリした後、次の作業が必要になる場合があります。

- バックアップ後にインスタンスに表示されていたデータベースはインスタンスから認識できません。これらのデータベースを再度稼働させるには、SQL Server Management Studioを使用して、インスタンスに手動で添付します。
- バックアップの実行後に削除されたデータベースは、インスタンス内でオフラインとして表示されます。これらのデータベースはSQL Server Management Studioで削除します。

SQL Server データベースの接続

このセクションでは、SQL Server Management Studio を使用して、SQL Server 内でデータベースを接続する方法について説明します。一度に、1 つのデータベースのみを接続できます。

データベースを接続するには、以下のいずれかの許可が必要です。**CREATE DATABASE**、**CREATE ANY DATABASE**、または**ALTER ANY DATABASE**。通常、これらの許可はインスタンスの**sysadmin**ロールに付与されます。

データベースを接続するには、次の手順に従います。

1. Microsoft SQL Server Management Studio を実行します。
2. 必要な SQL Server インスタンスに接続して、このインスタンスを展開します。
3. **[データベース]** を右クリックして、**[接続]** をクリックします。
4. **[追加]** をクリックします。
5. **[データベースファイルの検索]** ダイアログボックスで、データベースの.mdfファイルを検索して選択します。
6. **[データベースの詳細]** セクションで、残りのデータベースファイル（.ndfおよび.ldfファイル）が見つかったことを確認します。

   詳細:次の場合、SQL Server データベース ファイルが自動的に検出されないことがあります。
   - ファイルがデフォルトのロケーションにない場合、またはファイルがプライマリ データベース ファイル（.mdf）と同じフォルダに入っていない場合。解決策:**[現在のファイルパス]** 列で、必要なファイルへのパスを手動で指定します。
   - データベースを構成するファイルを復元したが、一部のファイルが不足している場合。解決策:不足しているSQL Serverデータベースファイルをバックアップからリカバリします。
7. すべてのファイルが見つかったら、**[OK]** をクリックします。

Exchangeデータベースの復元

このセクションでは、データベースバックアップとアプリケーション認識型バックアップの両方からの復元について説明します。

Exchange Serverデータを、稼働中のExchange Serverに復元できます。この場合、元のExchange Server、または同じ完全修飾ドメイン名（FQDN）のコンピュータで稼働する同じバージョンのExchange Serverを使用できます。エージェント for Exchangeを復元先のコンピュータにインストールする必要があります。

以下の表は、復元対象として選択できる Exchange Serverデータとデータの復元に最低限必要なユーザー権限を示しています。

Exchangeのバージョン	データアイテム	ユーザー権限
2007	ストレージ グループ	**Exchange Organization Management** 役割グループのメンバーシップ
2010/2013/2016/2019	データベース	**サーバー管理**役割グループのメンバーシップ

代わりに、データベース（ストレージ グループ）をファイルとして復元できます。データベースファイルとトランザクション ログ ファイルは、バックアップから指定したフォルダに取り出されます。これは、監査や、サードパーティ（他社製）ツールによってさらに処理するためにデータを取り出す必要があったり、何らかの理由により復元が失敗し、データベースを手動でマウントするための回避策を探したりする場合に役立ちます。

VMwareエージェント（Windows）のみを使用している場合は、データベースをファイルとして復元する方法のみを使用できます。VMwareエージェント（仮想アプライアンス）を使用してデータベースを復元することはできません。

次の手順では、データベースとストレージグループの両方を「データベース」と呼びます。

ExchangeデータベースをライブExchange Serverに復元するには

1. 次のいずれかを実行します。
   - アプリケーション認識型バックアップから復元する場合は、**[デバイス]** で、復元するデータが存在していたコンピュータを選択します。
   - データベースバックアップから復元する場合は、**[デバイス]** > **[Microsoft Exchange]** > **[データベース]** をクリックし、復元するデータベースを選択します。
2. **[復元]** をクリックします。
3. リカバリ ポイントを選択します。復元ポイントは、保存場所でフィルタされます。
   コンピュータがオフラインになっている場合、リカバリ ポイントは表示されません。次のいずれかを実行します。
   - （アプリケーション認識型バックアップから復元する場合のみ）バックアップのロケーションが（他のエージェントがアクセスできる）クラウドまたは共有ストレージの場合は、**[コンピュータを選択]** をクリックして、エージェントfor Exchangeがあるオンラインのコンピュータを選択してから、リカバリポイントを選択します。
   - [バックアップストレージ] タブで復元ポイントを選択します。

   上記のアクションのいずれかで参照用に選択されたコンピュータは、Exchangeデータ復元のターゲット コンピュータになります。
4. 次のいずれかを実行します。
   - アプリケーション認識型バックアップから復元する場合は、**[復元]** > **[Exchangeデータベース]** をクリックし、復元するデータベースを選択してから、**[復元]** をクリックします。
   - データベースバックアップから復元する場合は、**[復元]** > **[データベースをExchangeサーバーに]** をクリックします。
5. デフォルトでは、データベースは元のデータベースに復元されます。元のデータベースが存在しない場合は、再作成されません。
   データベースを別のものとして復元する手順
   a. データベース名をクリックします。
   b. **[復元先]** で、**[新しいデータベース]** を選択します。
   c. 新しいデータベース名を指定します。
   d. 新しいデータベースのパスとログのパスを指定します。指定するフォルダには、元のデータベースおよびログファイルが含まれていないようにする必要があります。
6. **[復元を開始]** をクリックします。

復元の進行状況は [アクティビティ] タブに表示されます。

Exchangeデータベースをファイルとして復元するには

1. 次のいずれかを実行します。
   - アプリケーション認識型バックアップから復元する場合は、**[デバイス]** で、復元するデータが存在していたコンピュータを選択します。
   - データベースバックアップから復元する場合は、**[デバイス]** > **[Microsoft Exchange]** > **[データベース]** をクリックし、復元するデータベースを選択します。
2. **[復元]** をクリックします。
3. リカバリ ポイントを選択します。復元ポイントは、保存場所でフィルタされます。

   コンピュータがオフラインになっている場合、リカバリ ポイントは表示されません。次のいずれかを実行します。
   - （アプリケーション認識型バックアップから復元する場合のみ）バックアップのロケーションが（他のエージェントがアクセスできる）クラウドまたは共有ストレージの場合は、**[マシンを選択]** をクリックして、Exchangeエージェントまたは VMwareエージェントがあるオンラインのマシンを選択してから、復元ポイントを選択します。
   - [バックアップストレージ] タブで復元ポイントを選択します。

   上記のアクションのいずれかで参照用に選択されたコンピュータは、Exchangeデータ復元のターゲット コンピュータになります。
4. 次のいずれかを実行します。
   - アプリケーション認識型バックアップから復元する場合は、**[復元]** > **[Exchangeデータベース]** をクリックし、復元するデータベースを選択してから、**[ファイルとして復元]** をクリックします。
   - データベースバックアップから復元する場合は、**[復元]** > **[データベースをファイルとして]** をクリックします。
5. **[参照]** をクリックし、ファイルの保存先となるローカルフォルダまたはネットワークフォルダを選択します。
6. **[復元を開始]** をクリックします。

復元の進行状況は [アクティビティ] タブに表示されます。

Exchange Server データベースのマウント

データベース ファイルを復元した後で、データベースをマウントすることによってそれらをオンラインにすることができます。マウントを実行するには、Exchange 管理コンソール、Exchange システム マネージャ、または Exchange 管理シェルを使用します。

復元されたデータベースは、ダーティ シャットダウン状態にあります。ダーティ シャットダウン状態のデータベースは、元のロケーションに復元される（つまり、元のデータベースに関する情報が Active Directory 内に存在する）場合にシステムによってマウントできます。データベースを別のロケーションにリカバリする場合は（新しいデータベースまたはリカバリデータベースとしてリカバリするなど）、`Eseutil /r <Enn>`コマンドを使用してクリーンシャットダウン状態にするまでデータベースをマウントできません。`<Enn>`には、トランザクションログファイルを適用する必要があるデータベース（またはデータベースが含まれるストレージグループ）のログファイルのプレフィックスを指定します。

データベースを接続するために使用するアカウントは、Exchange Server 管理者の役割を委任され、ターゲット サーバーのローカル Administrators グループのメンバになっている必要があります。

データベースのマウント方法の詳細については、次の記事を参照してください。

- Exchange 2010以降: http://technet.microsoft.com/en-us/library/aa998871.aspx（英語）
- Exchange 2007: http://technet.microsoft.com/ja-jp/library/aa998871(v=EXCHG.80).aspx

Exchange メールボックスとメールボックスのアイテムを復元

次のバックアップからExchangeメールボックスとメールボックスの項目をリカバリできます。

- データベースのバックアップ
- アプリケーション認識型バックアップ
- メールボックスのバックアップ

次の項目をリカバリできます。

- メールボックス（アーカイブメールボックスを除く）
- パブリック フォルダ

> **注意**
> データベースバックアップでのみ利用可能です。"Exchange Serverデータの選択"（550ページ）をご覧ください。

- パブリック フォルダのアイテム
- 電子メールフォルダ
- メールメッセージ
- カレンダーのイベント
- タスク
- 連絡先
- 履歴項目
- メモ

アイテムの場所は検索で確認できます。

メールボックスやメールボックスアイテムを稼働中のExchange ServerまたはMicrosoft 365にリカバリできます。

Exchange Server に復元

詳細復元は、Microsoft Exchange Server 2010 Service Pack 1（SP1）以降でのみ実行可能です。ソースのバックアップには、サポートされるすべての Exchange バージョンのデータベースまたはメールボックスを含めることができます。

詳細復元は、エージェント for Exchangeまたはエージェント for VMware（Windows）より実行できます。ターゲットのExchange Serverとエージェントを実行するコンピュータは、同じActive Directoryフォレストに属している必要があります。

メールボックスが既存のメールボックスに復元されると、IDが一致する既存のアイテムは上書きされます。

メールボックスのアイテムの復元で上書きされるものはありません。その代わりに、メールボックスアイテムへのフルパスは、ターゲットフォルダで再作成されます。

ユーザーアカウントに関する要件

バックアップから復元されるメールボックスは、Active Directoryに関連付けられたユーザーアカウントを保有している必要があります。

ユーザーメールボックスとその内容は、関連付けられたユーザーアカウントが [有効] である場合のみ復元されます。共有、会議室、備品用の各メールボックスは、関連付けられたユーザー アカウントが無効である場合のみ復元されます。

上記の条件を満たさないメールボックスは、復元中にスキップされます。

一部のメールボックスがスキップされた場合、復元自体は正常終了しますが、警告が表示されます。すべてのメールボックスがスキップされた場合、復元は失敗します。

Microsoft 365への復元

ExchangeデータアイテムのMicrosoft 365への復元およびその逆の操作は、Microsoft 365エージェントがローカルにインストール済みという条件下でのみサポートされます。

復元は、Microsoft Exchange Server 2010 以降でのみ実行可能です。

メールボックスが既存のMicrosoft 365メールボックスにリカバリされると、既存のアイテムはそのまま保存され、リカバリされたアイテムはその横に配置されます。

単一のメールボックスを復元する場合は、ターゲットのMicrosoft 365メールボックスを選択する必要があります。1 回の復元操作で複数のメールボックスを復元する場合、各メールボックスは、同じ名前のユーザーのメールボックスに復元されます。該当するユーザーが見つからない場合、そのメールボックスはスキップされます。一部のメールボックスがスキップされた場合、復元自体は正常終了しますが、警告が表示されます。すべてのメールボックスがスキップされた場合、復元は失敗します。

Microsoft 365の復元の詳細については、"Microsoft 365データの保護"（584ページ）を参照してください。

メールボックスの復元

アプリケーション認識型バックアップまたはデータベースバックアップからメールボックスを復元するには

1. （データベースバックアップからMicrosoft 365にリカバリする場合のみ）Exchange Serverが実行されているバックアップ済みのマシンにMicrosoft 365エージェントがインストールされていない場合は、以下のいずれかの対応を行ってください。
   - 組織内にMicrosoft 365エージェントが存在しない場合は、バックアップされたマシン（または同じバージョンのMicrosoft Exchange Serverがインストールされている別のマシン）にMicrosoft 365エージェントをインストールします。
   - 組織でMicrosoft 365エージェントを既に使用している場合は、「Microsoft Exchangeライブラリのコピー」に記載されているように、バックアップされたマシン（または同じバージョンの

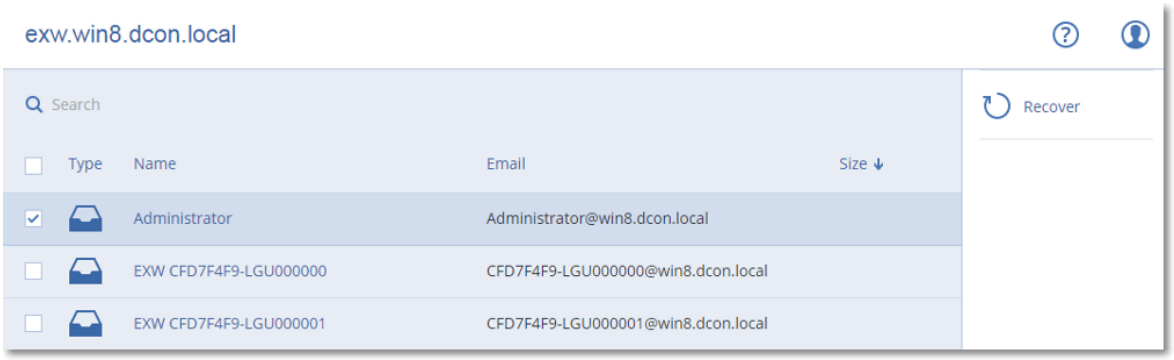
Microsoft Exchange Serverがインストールされている別のマシン）から、Microsoft 365エージェントがインストールされたマシンにライブラリをコピーします。

2. 次のいずれかを実行します。
   - アプリケーション認識型バックアップから復元する場合は、**[デバイス]** で、復元するデータが存在していたコンピュータを選択します。
   - データベースバックアップから復元する場合は、**[デバイス]** > **[Microsoft Exchange]** > **[データベース]** をクリックし、復元するデータが存在していたデータベースを選択します。
3. **[復元]** をクリックします。
4. リカバリ ポイントを選択します。復元ポイントは、保存場所でフィルタされます。

   コンピュータがオフラインになっている場合、リカバリ ポイントは表示されません。他の方法を使用して復元する手順は、次のようになります。
   - （アプリケーション認識型バックアップから復元する場合のみ）バックアップのロケーションが（他のエージェントがアクセスできる）クラウドまたは共有ストレージの場合は、**[マシンを選択]** をクリックして、Exchangeエージェントまたは VMwareエージェントがあるオンラインのマシンを選択してから、復元ポイントを選択します。
   - [バックアップストレージ] タブで復元ポイントを選択します。

   上記のアクションのいずれかで参照用に選択されたコンピュータが、オフラインである元のコンピュータの代わりに、復元を実行します。
5. **[復元]** > **[Exchangeメールボックス]** の順にクリックします。
6. 復元するメールボックスを選択します。

   メールボックスを名前で検索できます。ワイルドカードはサポートされていません。



7. **[復元]** をクリックします。
8. （Microsoft 365にリカバリする場合のみ）：
   a. **[復元先]** で、**[Microsoft 365]** を選択します。
   b. （手順 6 で単一のメールボックスを選択した場合）**[ターゲットメールボックス]** で、ターゲットメールボックスを指定します。
   c. **[復元を開始]** をクリックします。

   ここでは、その他の手順は不要です。
9. **[Microsoft Exchange Serverを搭載するターゲットコンピュータ]** をクリックして、復元先のコンピュータを選択または変更します。この手順により、エージェント for Exchangeを実行していないコンピュータへの復元が可能になります。

クライアントアクセス（Microsoft Exchange Server 2010/2013）の役割、または**メールボックスロール**（Microsoft Exchange Server 2016 以降）が有効なマシンの完全修飾ドメイン名（FQDN）を指定します。このコンピュータは、復元を実行するコンピュータと同じActive Directoryフォレストに属している必要があります。
プロンプトが表示されたら、マシンにアクセスするために使用するアカウントの資格情報を入力します。このアカウントの要件は、「必要なユーザー権限」に記載されています。

10. （オプション）選択済みデータベースを自動的に変更するには、**[見つからないメールボックスを再作成するためのデータベース]** をクリックします。
11. **[復元を開始]** をクリックします。

復元の進行状況は **[アクティビティ]** タブに表示されます。

メールボックスのバックアップからメールボックスを復元するには

1. **[デバイス]** > **[Microsoft Exchange]** > **[メールボックス]** をクリックします。
2. 復元するメールボックスを選択してから、**[復元]** をクリックします。
   メールボックスを名前で検索できます。ワイルドカードはサポートされていません。
   メールボックスが削除された場合は、そのメールボックスを [バックアップストレージ] タブで選択してから、**[バックアップの表示]** をクリックします。
3. リカバリ ポイントを選択します。復元ポイントは、保存場所でフィルタされます。
4. **[復元]** >**[メールボックス]** の順にクリックします。
5. 上記の手順 8～11 を実行します。

メールボックスのアイテムの復元

アプリケーション認識型バックアップまたはデータベースバックアップからメールボックスアイテムを復元するには

1. （データベースバックアップからMicrosoft 365にリカバリする場合のみ）Exchange Serverが実行されているバックアップ済みのマシンにMicrosoft 365エージェントがインストールされていない場合は、以下のいずれかの対応を行ってください。
   - 組織内にMicrosoft 365エージェントが存在しない場合は、バックアップされたマシン（または同じバージョンのMicrosoft Exchange Serverがインストールされている別のマシン）にMicrosoft 365エージェントをインストールします。
   - 組織でMicrosoft 365エージェントを既に使用している場合は、「Microsoft Exchangeライブラリのコピー」に記載されているように、バックアップされたマシン（または同じバージョンのMicrosoft Exchange Serverがインストールされている別のマシン）から、Microsoft 365エージェントがインストールされたマシンにライブラリをコピーします。
2. 次のいずれかを実行します。
   - アプリケーション認識型バックアップから復元する場合は、**[デバイス]** で、復元するデータが存在していたコンピュータを選択します。
   - データベースバックアップから復元する場合は、**[デバイス]** > **[Microsoft Exchange]** > **[データベース]** をクリックし、復元するデータが存在していたデータベースを選択します。
3. **[復元]** をクリックします。
4. リカバリ ポイントを選択します。復元ポイントは、保存場所でフィルタされます。

コンピュータがオフラインになっている場合、リカバリ ポイントは表示されません。他の方法を使用して復元する手順は、次のようになります。

- （アプリケーション認識型バックアップから復元する場合のみ）バックアップのロケーションが（他のエージェントがアクセスできる）クラウドまたは共有ストレージの場合は、**[マシンを選択]** をクリックして、Exchangeエージェントまたは VMwareエージェントがあるオンラインのマシンを選択してから、復元ポイントを選択します。
- [バックアップストレージ] タブで復元ポイントを選択します。

上記のアクションのいずれかで参照用に選択されたコンピュータが、オフラインである元のコンピュータの代わりに、復元を実行します。

5. **[復元]** > **[Exchangeメールボックス]** の順にクリックします。
6. 復元するアイテムが元々存在していたメールボックスをクリックします。
7. 復元するアイテムを選択します。

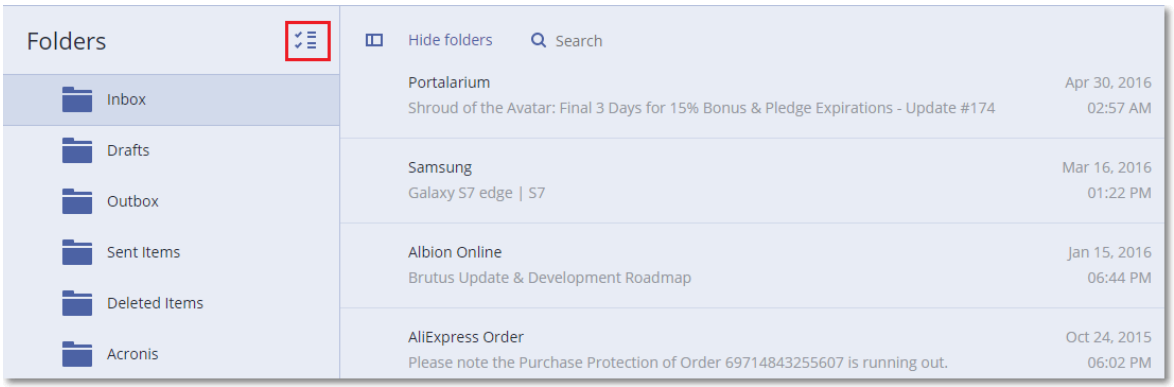
   以下の検索オプションを選択できます。ワイルドカードはサポートされていません。

   - 電子メールのメッセージの場合、件名、送信者、受信者、日付で検索します。
   - イベントの場合、タイトルと日付で検索します。
   - タスクの場合、件名と日付で検索します。
   - 連絡先の場合、名前、メールアドレス、電話番号で検索します。

   電子メールのメッセージを選択したら、**[内容を表示]** をクリックすると、添付ファイルを含む内容を表示できます。

   注意
   添付ファイルをダウンロードするには、そのファイルの名前をクリックします。

   フォルダを選択できるようにするには、フォルダ復元のアイコンをクリックします。



8. **[復元]** をクリックします。
9. Microsoft 365にリカバリするには、**[復元先]** で **[Microsoft 365]** を選択します。

   Exchange Server に復元するには、**[復元先]** の値をデフォルトの **[Microsoft Exchange]** のままにします。
10. （Exchange Server に復元する場合のみ）**[Microsoft Exchange Server を搭載するターゲットマシン]** をクリックして、復元先のマシンを選択または変更します。この手順により、エージェント for Exchangeを実行していないコンピュータへの復元が可能になります。

クライアントアクセス（Microsoft Exchange Server 2010/2013）の役割、または**メールボックスロール**（Microsoft Exchange Server 2016 以降）が有効なマシンの完全修飾ドメイン名（FQDN）を指定します。このコンピュータは、復元を実行するコンピュータと同じActive Directoryフォレストに属している必要があります。
プロンプトが表示されたら、マシンにアクセスするために使用するアカウントの資格情報を入力します。このアカウントの要件は、「必要なユーザー権限」に記載されています。

11. **[ターゲットメールボックス]** で、ターゲットメールボックスを表示、変更、または指定します。
    デフォルトでは、元のメールボックスが選択されます。このメールボックスが存在しない場合、または元は復元先のコンピュータではないコンピュータが選択されている場合は、ターゲットメールボックスの指定が必要です。
12. （電子メールメッセージを復元する場合のみ）**[ターゲットフォルダ]** で、ターゲットメールボックスのターゲットフォルダを表示または変更します。デフォルトでは、**[復元されたアイテム]** フォルダが選択されます。Microsoft Exchangeの場合は、**[ターゲットフォルダ]** の指定内容にかかわりなく、イベントやタスクやメモや連絡先が元のロケーションに復元される、という制限事項があります。
13. **[復元を開始]** をクリックします。

復元の進行状況は **[アクティビティ]** タブに表示されます。

メールボックスのバックアップからメールボックスアイテムを復元するには

1. **[デバイス]** > **[Microsoft Exchange]** > **[メールボックス]** をクリックします。
2. 復元するアイテムが元々存在していたメールボックスを選択し、**[復元]** をクリックします。
   メールボックスを名前で検索できます。ワイルドカードはサポートされていません。
   メールボックスが削除された場合は、そのメールボックスを [バックアップストレージ] タブで選択してから、**[バックアップの表示]** をクリックします。
3. リカバリ ポイントを選択します。復元ポイントは、保存場所でフィルタされます。
4. **[復元]** > **[メールメッセージ]** の順にクリックします。
5. 復元するアイテムを選択します。
   以下の検索オプションを選択できます。ワイルドカードはサポートされていません。
   - 電子メールのメッセージの場合、件名、送信者、受信者、日付で検索します。
   - イベントの場合、タイトルと日付で検索します。
   - タスクの場合、件名と日付で検索します。
   - 連絡先の場合、名前、メールアドレス、電話番号で検索します。

   電子メールのメッセージを選択したら、**[内容を表示]** をクリックすると、添付ファイルを含む内容を表示できます。

   注意
   添付ファイルをダウンロードするには、そのファイルの名前をクリックします。

   電子メールのメッセージを選択したら、**[電子メールで送信]** をクリックすると、メッセージをメールアドレスに送信できます。メッセージは管理者アカウントのメールアドレスから送信されます。

   フォルダを選択できるようにするには、フォルダ復元アイコン（  ）をクリックします。

6. **[復元]** をクリックします。
7. 上記の手順 9〜13 を実行します。

Microsoft Exchange Server のライブラリのコピー

Exchangeメールボックスまたはメールボックスアイテムをリカバリするとき、バックアップされたマシン（または同じバージョンのMicrosoft Exchange Serverがインストールされている別のマシン）から、Microsoft 365エージェントがインストールされているマシンに次のライブラリをコピーしなければならない場合があります。

バックアップされた Microsoft Exchange Server のバージョンに応じて、次のファイルをコピーします。

Microsoft Exchange Server のバージョン	ライブラリ	デフォルトのロケーション

Microsoft Exchange Server 2010	`ese.dll`
	`esebcli2.dll`
	`store.exe`
		`%ProgramFiles%\Microsoft\Exchange Server\V14\bin`

Microsoft Exchange Server 2013	`ese.dll`	`%ProgramFiles%\Microsoft\Exchange Server\V15\bin`
	`msvcr110.dll`	`%WINDIR%\system32`
Microsoft Exchange Server 2016、2019	`ese.dll`	`%ProgramFiles%\Microsoft\Exchange Server\V15\bin`
	`msvcr110.dll` `msvcp110.dll`	`%WINDIR%\system32`

このライブラリは、`%ProgramData%\Acronis\ese`フォルダに配置されている必要があります。このフォルダが存在しない場合、手動で作成します。

SQLサーバーまたはExchangeサーバーのアクセス認証の変更

エージェントをインストールし直すことなく、SQLサーバーまたはExchangeサーバーのアクセス認証を変更することができます。

SQLサーバーまたはExchangeサーバーのアクセス認証を変更するには

1. **[デバイス]** をクリックし、**[Microsoft SQL]** または **[Microsoft Exchange]** をクリックします。
2. アクセス認証を変更するAlways On可用性グループ、データベース可用性グループ、SQLサーバーインスタンス、またはExchange Serverを選択します。
3. **[資格情報の指定]** をクリックします。
4. 新しいアクセス認証を指定し、**[OK]** をクリックします。

Exchangeサーバーのメールボックスバックアップのアクセス認証を変更するには

1. **[デバイス]** > **[Microsoft Exchange]** をクリックしてから、**[メールボックス]** を展開します。
2. アクセス認証を変更するExchangeサーバーを選択します。
3. **[設定]** をクリックします。
4. **[Exchange管理者アカウント]** で新しいアクセス認証を指定し、**[保存]** をクリックします。

モバイル デバイスの保護

Cyber Protectアプリにより、モバイルデータをクラウドストレージにバックアップし、紛失または破損した場合にそれをリカバリできます。クラウド ストレージへのバックアップには、アカウントとクラウドサブスクリプションが必要であることに注意してください。

サポートされるモバイル デバイス

Cyber Protectアプリは、以下のいずれかのオペレーティングシステムを実行しているモバイルデバイスにインストールできます。

- iOS 14からiOS 16（iPhone、iPod、iPad）
- Android 9からAndroid 13

バックアップできる内容

- 連絡先（名前、電話番号、Eメール）
- 写真（写真の元のサイズと形式は保持されます）
- 動画
- カレンダー
- リマインダ（iOSデバイスのみ）

留意事項

- データは、クラウドストレージにのみバックアップできます。
- アプリを開くといつでも、データ変更のサマリを確認し、バックアップを手動で開始できます。
- **継続的バックアップ**機能は、デフォルトで有効になっています。この設定がオンになっている場合、Cyber Protectアプリはその場で新しいデータを自動的に検出し、それをクラウドにアップロードします。
- **[Wi-Fiのみを使用]** オプションは、アプリの設定によりデフォルトで有効になります。この設定がオンの場合、Cyber ProtectアプリはWi-Fi接続が利用可能なときにのみデータをバックアップします。Wi-Fi接続が失われると、バックアップ処理は開始しません。アプリを携帯電話接続でも使用するためには、このオプションをオフにします。
- デバイスのバッテリーを最適化すると、Cyber Protectアプリが適切に動作しなくなる可能性があります。時間どおりにバックアップを実行するには、アプリのバッテリー最適化を停止する必要があります。
- エネルギーを節約する2つの方法があります。
  - **[充電中にバックアップ]** 機能はデフォルトで無効になります。この設定がオンの場合、Cyber Protectアプリはデバイスが電源に接続されているときにのみデータをバックアップします。自動

バックアップ処理中にデバイスが電源から切断されると、バックアップは一時停止します。
    - **[節電モード]** はデフォルトで有効になります。この設定がオンの場合、Cyber Protectアプリはデバイスのバッテリー残量に余裕がある場合に限りデータをバックアップします。デバイスのバッテリー残量が少なくなると、自動バックアップは一時停止します。
- 自分のアカウントの下で登録されたモバイルデバイスから、バックアップデータにアクセスできます。この機能は、古いモバイル デバイスから新しいデバイスにデータを転送するために役立ちます。Androidデバイスの連絡先と写真は、iOSデバイスに復元できます（逆も可能）。Cyber Protectコンソールを使用して、写真、動画、連絡先をあらゆるデバイスにダウンロードすることもできます。
- お使いのアカウントで登録されたモバイル デバイスからバックアップされたデータは、そのアカウントでのみ使用できます。他のアカウントからはそのデータの表示も復元もできません。
- Cyber Portectアプリでは、最新のデータバージョンのみをリカバリできます。特定のバックアップのバージョンからリカバリする必要がある場合は、タブレットまたはコンピューターでCyber Protectコンソールを使用します。
- 保持ルールは、モバイル デバイスのバックアップには適用されません。
- [Androidデバイス限定] バックアップ中にSDカードが存在する場合、このカードに格納されているデータもバックアップされます。このデータは、復元中に存在する場合はSDカードの**バックアップによって復元**フォルダに復元されます。または、データをリカバリする別のロケーションをアプリが要求します。

Cyber Portectアプリの入手先

モバイルデバイスに応じて、App StoreまたはGoogle Playからアプリをインストールします。

データのバックアップを開始する方法

1. アプリを開きます。
2. 自分のアカウントを使用してサインインします。
3. **[セットアップ]** をタップしてバックアップを作成します。モバイルデバイスのバックアップが存在しない場合にのみこのボタンが表示されることに注意してください。
4. バックアップするデータのカテゴリを選択します。デフォルト設定では、すべてのカテゴリが選択されます。
5. [オプションステップ] **バックアップの暗号化**を有効にし、暗号化によってバックアップを保護します。この場合は、以下を行う必要もあります。
   a. 暗号化パスワードを2回入力します。

      注意
      忘れたパスワードは復元または変更できないので、パスワードを忘れないでください。

   b. **[暗号化]** をタップします。
6. **[バックアップ]** をタップします。
7. アプリの個人データへのアクセスを許可します。特定のデータカテゴリへのアクセスを拒否すると、そのカテゴリはバックアップされません。

バックアップが開始されます。

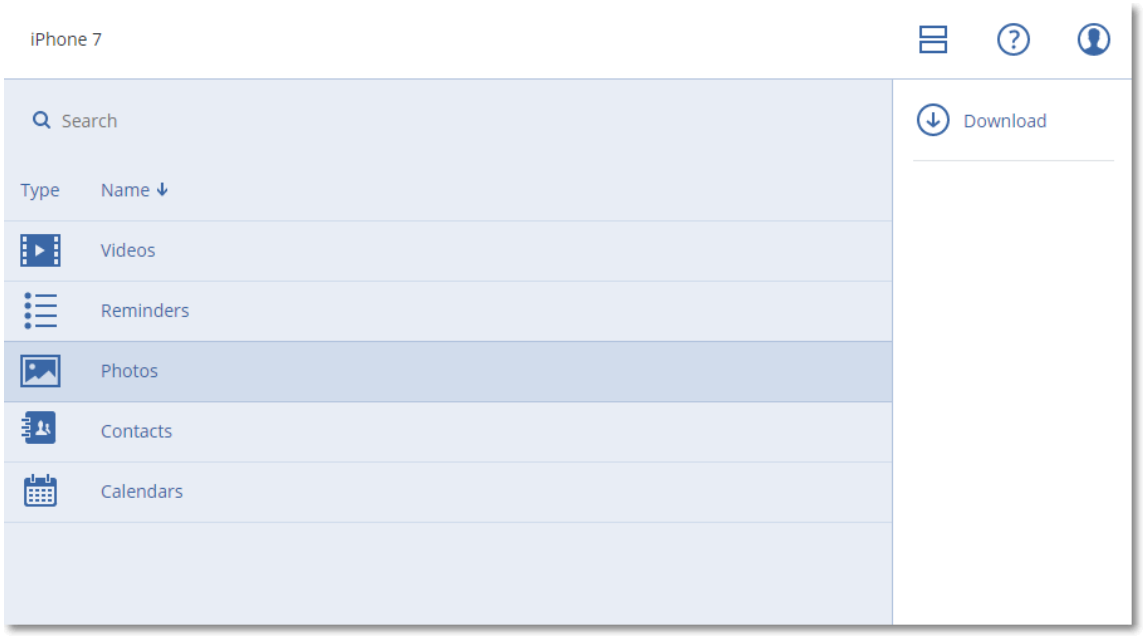
モバイルデバイスにデータを復元する方法

警告
モバイルデータを復元するには、エンドユーザーアカウントを使用する必要があります。

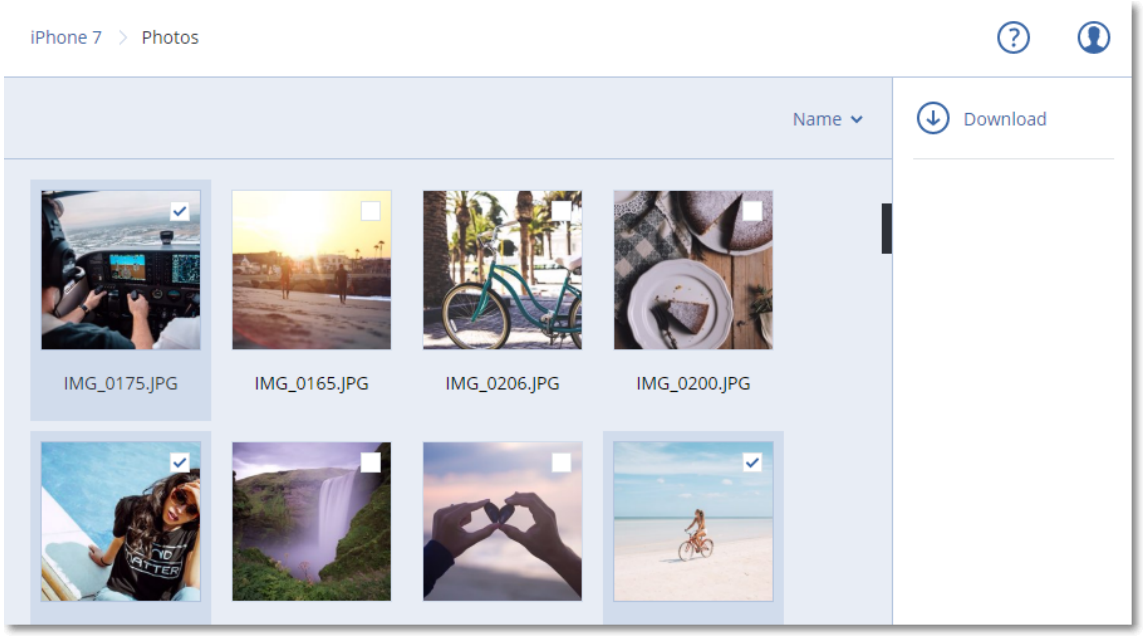
1. Cyber Protectアプリを開きます。
2. **[参照]** をタップします。
3. デバイス名をタップします。
4. 次のいずれかを実行します。
   - バックアップされたデータをすべて復元するには、**[すべて復元]** をタップします。これ以上の操作は不要です。
   - データ カテゴリを 1 つ以上復元するには、**[選択]** をタップしてから必要なデータ カテゴリのチェック ボックスをタップします。**[復元]** をタップします。これ以上の操作は不要です。
   - 同一のデータ カテゴリに属しているデータ アイテムを復元するには、そのデータ カテゴリをタップします。手順に従って進めます。
5. 次のいずれかを実行します。
   - 単一のデータ アイテムを復元するには、そのデータ アイテムをタップします。
   - 複数のデータ アイテムを復元するには、**[選択]** をタップしてから必要なデータ アイテムのチェック ボックスをタップします。
6. **[復元]** をタップします。

Cyber Protectコンソールからデータをレビューする方法

1. コンピューターでブラウザを開き、Cyber ProtectコンソールのURLを入力します。
2. 自分のアカウントを使用してサインインします。
3. **[すべてのデバイス]** で、モバイルデバイスの名前の下にある **[復元]** をクリックします。
4. 次の手順のいずれかを実行します。
   - 写真、動画、連絡先、予定表、またはリマインダーをすべてダウンロードするには、それぞれのデータカテゴリを選択します。**[ダウンロード]** をクリックします。



- 個々の写真、動画、連絡先、予定表、またはリマインダーをダウンロードするには、それぞれのデータカテゴリ名を選択してから、必要なデータアイテムのチェックボックスを選択します。**[ダウンロード]** をクリックします。



- 写真や連絡先をプレビューするには、それぞれのデータカテゴリ名をクリックしてから、必要なデータアイテムをクリックします。

Hosted Exchangeデータの保護

バックアップできるアイテム

ユーザーメールボックス、共有メールボックス、およびグループメールボックスをバックアップできます。オプションとして、選択したメールボックスのアーカイブメールボックス（**インプレースアーカイ**

ブ）のバックアップを選択できます。

復元できるアイテム

メールボックス バックアップから復元できるアイテムは次のとおりです。

- メールボックス
- 電子メールフォルダ
- メールメッセージ
- カレンダーのイベント
- タスク
- 連絡先
- 履歴項目
- メモ

アイテムの場所は検索で確認できます。

メールボックス、メールボックスのアイテム、パブリックフォルダ、およびパブリックフォルダのアイテムを復元するとき、ターゲットロケーションにあるアイテムを上書きするかどうかを選択できます。

メールボックスが既存のメールボックスに復元されると、IDが一致する既存のアイテムは上書きされます。

メールボックスのアイテムの復元で上書きされるものはありません。その代わりに、メールボックスアイテムへのフルパスは、ターゲットフォルダで再作成されます。

Exchange Onlineメールボックスを選択する

下記のようにメールボックスを選択し、保護計画のその他の設定を必要に応じて指定します。

Exchange Onlineのメールボックスを選択する方法

1. **[デバイス]** > **[Hosted Exchange]** をクリックします。
2. Cyber Protectionサービスに複数のHosted Exchange組織を追加している場合、バックアップするユーザーのデータがある組織を選択します。それ以外の場合は、この手順をスキップします。
3. 次のいずれかを実行します。
   - すべてのユーザーメールボックスとすべての共有メールボックス（将来作成されるメールボックスを含む）をバックアップするには、**[ユーザー]** ノードを展開し、**[すべてのユーザー]** を選択して、**[グループバックアップ]** をクリックします。
   - 個々のユーザーメールボックスや共有メールボックスをバックアップするには、**[ユーザー]** ノードを展開し、**[すべてのユーザー]** を選択し、バックアップするメールボックスのユーザーを選択し、**[バックアップ]** をクリックします。
   - すべてのグループメールボックス（将来作成されるグループのメールボックスを含む）をバックアップするには、**[グループ]** ノードを展開し、**[すべてのグループ]** を選択して、**[グループバックアップ]** をクリックします。

- 個々のグループメールボックスをバックアップするには、**[グループ]** ノードを展開し、**[すべてのグループ]** を選択し、バックアップするメールボックスのグループを選択し、**[バックアップ]** をクリックします。

メールボックスおよびメールボックスアイテムの復元

メールボックスの復元

1. **[デバイス]** > **[Hosted Exchange]** をクリックします。
2. Cyber Protectionサービスに複数のHosted Exchange組織が追加されている場合は、バックアップされたデータをリカバリする組織を選択します。それ以外の場合は、この手順をスキップします。
3. 次のいずれかを実行します。
   - ユーザーメールボックスを復元するには、**[ユーザー]** ノードを展開し、**[すべてのユーザー]** を選択し、復元するメールボックスのユーザーを選択し、**[復元]** をクリックします。
   - 共有メールボックスを復元するには、**[ユーザー]** ノードを展開し、**[すべてのユーザー]** を選択し、復元する共有メールボックスを選択し、**[復元]** をクリックします。
   - グループメールボックスを復元するには、**[グループ]** ノードを展開し、**[すべてのグループ]** を選択し、復元するメールボックスのグループを選択し、**[復元]** をクリックします。
   - ユーザー、グループ、または共有メールボックスが削除されている場合は、[バックアップストレージ] タブの **[クラウドアプリケーションバックアップ]** セクションでその項目を選択して、**[バックアップの表示]** をクリックします。

   ユーザーおよびグループを名前で検索できます。ワイルドカードはサポートされていません。
4. リカバリ ポイントを選択します。
5. **[復元]** > **[メールボックス全体]** の順にクリックします。
6. Cyber Protectionサービスに複数のHosted Exchange組織が追加されている場合は、**[Hosted Exchange組織]** をクリックして、ターゲット組織の表示、変更、または指定を行います。

   デフォルトでは、元の組織が選択されます。この組織がCyber Protectionサービスに現在登録されていない場合は、ターゲット組織を指定する必要があります。
7. **[メールボックスに復元]** で、ターゲットメールボックスを表示、変更、または指定します。

   デフォルトでは、元のメールボックスが選択されます。このメールボックスが存在しないか、元と異なる組織が選択されている場合は、ターゲットメールボックスを指定する必要があります。
8. **[復元を開始]** をクリックします。
9. 次のいずれかの上書きオプションを選択します。
   - **[既存のアイテムに上書きする]**
   - **[既存のアイテムを上書きしない]**
10. **[続行]** をクリックして、操作を確定します。

メールボックスのアイテムの復元

1. **[デバイス]** > **[Hosted Exchange]** をクリックします。
2. Cyber Protectionサービスに複数のHosted Exchange組織が追加されている場合は、バックアップされたデータをリカバリする組織を選択します。それ以外の場合は、この手順をスキップします。

3. 次のいずれかを実行します。
   - ユーザーメールボックスからアイテムを復元するには、**[ユーザー]** ノードを展開し、**[すべてのユーザー]** を選択し、復元するアイテムが最初にあったメールボックスのユーザーを選択し、**[復元]** をクリックします。
   - 共有メールボックスからアイテムを復元するには、**[ユーザー]** ノードを展開し、**[すべてのユーザー]** を選択し、復元するアイテムが最初にあった共有メールボックスを選択し、**[復元]** をクリックします。
   - グループメールボックスからアイテムを復元するには、**[グループ]** ノードを展開し、**[すべてのグループ]** を選択し、復元するアイテムが最初にあったメールボックスのグループを選択し、**[復元]** をクリックします。
   - ユーザー、グループ、または共有メールボックスが削除されている場合は、[バックアップストレージ] タブの **[クラウドアプリケーションバックアップ]** セクションでその項目を選択して、**[バックアップの表示]** をクリックします。

   ユーザーおよびグループを名前で検索できます。ワイルドカードはサポートされていません。
4. リカバリ ポイントを選択します。
5. **[復元]** > **[メールメッセージ]** の順にクリックします。
6. 目的のフォルダを参照するか、検索を使用して目的のアイテムの一覧を取得します。

   以下の検索オプションを選択できます。ワイルドカードはサポートされていません。
   - Eメールのメッセージの場合、件名、送信者、受信者、添付ファイル名、日付で検索します。
   - イベントの場合、タイトルと日付で検索します。
   - タスクの場合、件名と日付で検索します。
   - 連絡先の場合、名前、メールアドレス、電話番号で検索します。
7. 復元するアイテムを選択します。フォルダを選択できるようにするには、[フォルダ復元] のアイコン（  ）をクリックします。

   また、次のいずれかを実行できます。
   - アイテムを選択する際に、添付ファイルを含む内容を表示するには、**[内容の表示]** をクリックします。 添付ファイルをダウンロードするには、そのファイルの名前をクリックします。
   - メールメッセージまたはカレンダーアイテムを選択したら、**[メールで送信]** をクリックして、アイテムを指定したメールアドレスに送信します。送信者を選択し、転送するアイテムに追加するテキストを作成できます。
   - バックアップが暗号化されておらず、検索を使用して、検索結果で1つのアイテムを選択した場合のみ、**[バージョンを表示]** をクリックして、復元するアイテムのバージョンを選択します。選択した復元ポイントより前または後の、任意のバックアップバージョンを選択できます。
8. **[復元]** をクリックします。
9. Cyber Protectionサービスに複数のHosted Exchange組織が追加されている場合は、**[Hosted Exchange組織]** をクリックして、ターゲット組織の表示、変更、または指定を行います。

   デフォルトでは、元の組織が選択されます。この組織がCyber Protectionサービスに現在登録されていない場合は、ターゲット組織を指定する必要があります。
10. **[メールボックスに復元]** で、ターゲットメールボックスを表示、変更、または指定します。

デフォルトでは、元のメールボックスが選択されます。このメールボックスが存在しないか、元と異なる組織が選択されている場合は、ターゲットメールボックスを指定する必要があります。

11. （ユーザーメールボックスまたは共有メールボックスへ復元する場合のみ）**[パス]** で、ターゲットメールボックスのターゲットフォルダを表示または変更します。デフォルトでは、**[復元されたアイテム]** フォルダが選択されます。
    グループメールボックスのアイテムは、常に **[受信ボックス]** フォルダに復元されます。
12. **[復元を開始]** をクリックします。
13. 次のいずれかの上書きオプションを選択します。
    - **[既存のアイテムに上書きする]**
    - **[既存のアイテムを上書きしない]**
14. **[続行]** をクリックして、操作を確定します。

Microsoft 365データの保護

Microsoft 365データをバックアップする理由

Microsoft 365はクラウドサービスのセットですが、定期的にバックアップすることで、ユーザーの過失や悪意を持った意図的な行為からの保護レベルを高めます。Microsoft 365の保持期間が終了した後でもバックアップから削除したアイテムをリカバリできます。規制コンプライアンスに必要な場合、Exchange Onlineメールボックスのローカルコピーを保存できます。

バックアップされたデータは自動的に圧縮されるため、バックアップ先で使用されるスペースは元のロケーションよりも小さくなります。クラウドツークラウドバックアップの圧縮レベルは固定であり、非クラウドツークラウドバックアップの**通常**レベルに相当します。これらのレベルの詳細については、"圧縮レベル"（448ページ）を参照してください。

クラウドエージェントとローカルエージェント

Microsoft 365ワークロードでは、2種類のエージェントが利用可能です。

- クラウドエージェント
  クラウドエージェントでは拡張バックアップ機能が提供され、Cyber Protectコンソールから直接アクセスできます。インストールの必要はありません。詳細については、"Microsoft 365クラウドエージェントを使用する"（593ページ）を参照してください。
- ローカルエージェント
  ローカルエージェントでは、Exchange Onlineメールボックスのバックアップのみが提供されます。このエージェントは、必ずインターネットに接続しているWindowsマシンにインストールする必要があります。詳細については、"ローカルにインストールされたOffice 365エージェントの使用"（589ページ）を参照してください。

Azure Information Protection（AIP）は両方のエージェントでサポートされています。

注意
コンプライアンスモードのテナントでは、ローカルエージェントのみ利用可能です。これらのテナントでは、Microsoft 365メールボックスのみをバックアップできます。クラウドエージェントが提供する拡張機能を利用することはできません

エージェントの機能については、次の表に示します。

	ローカルエージェント	クラウドエージェント
バックアップできるデータアイテム	**Exchange Online:** ユーザーメールボックスと共有メールボックス（Kiosk計画上のユーザーのメールボックスおよび訴訟ホールドのメールボックスを含む）	• **Exchange Online**: ◦ ユーザーメールボックスと共有メールボックス（Kiosk計画上のユーザーのメールボックスおよび訴訟ホールドのメールボックスを含む） ◦ グループメールボックス ◦ パブリックフォルダ • **OneDrive**: ユーザーファイルとフォルダ • **SharePoint Online**: ◦ クラシックサイトコレクション ◦ グループ（チーム）サイト ◦ 通信サイト ◦ 個別データ項目 • **Microsoft 365 Teams**: ◦ チーム全体 ◦ チームチャネル ◦ チャネルのファイル ◦ チームのメールボックス ◦ チームのメールボックス内のファイルとEメールメッセージ ◦ 会議 ◦ チームサイト • **OneNoteノートブック**: OneDrive、SharePoint Online、Microsoft 365 Teamsのバックアップの一部として
アーカイブメールボックス（**インプレースアーカイブ**）のバックアップ	いいえ	はい
バックアップスケジュール	ユーザー定義	1日6回まで*

	ローカルエージェント	クラウドエージェント
バックアップ保存先	クラウドストレージ、ローカルフォルダ、ネットワークフォルダ	クラウドストレージのみ （パートナーホステッドストレージを含む）
新しいMicrosoft 365ユーザー、グループ、サイト、チームの自動保護	いいえ	はい（保護計画を **[すべてのユーザー]**、**[すべてのグループ]**、**[すべてのサイト]**、**[すべてのチーム]** グループに適用することで可能）
複数のMicrosoft 365組織を保護	いいえ	はい
詳細復元	はい	はい
1つの組織内の別のユーザーに復元	はい	はい
別の組織への復元	いいえ	はい
オンプレミスMicrosoft Exchange Serverに復元	いいえ	いいえ
パフォーマンスの低下を伴わずにバックアップできるアイテムの最大数	クラウドストレージにバックアップする場合:会社ごとに5000メールボックス 別の場所にバックアップする場合:保護計画ごとに2000個のメールボックス（会社ごとのメールボックス数は無制限）	会社ごとに10,000件の保護されたアイテム（メールボックス、OneDrive、またはサイト）**
手動バックアップ実行の最大数	いいえ	1時間に10回の手動実行
同時復元操作の最大数	いいえ	Google Workspaceの復元操作を含め、10回の操作

* デフォルトのオプションは、**1日に一度**です。Advanced Backupパックでは、最大1日に6回のバックアップをスケジュールできます。バックアップは、データセンター内で複数のカスタマーにサービスを提供しているクラウドエージェントの現在の負荷に応じて、おおよその間隔で開始されます。これにより、1日の負荷が均等になり、すべてのカスタマーのサービス品質が均等化されます。

注意

保護スケジュールは、サードパーティサービスの動作（Microsoft 365サーバーのアクセシビリティ、Microsoftサーバーの調整設定など）による影響を受けることがあります。
https://docs.microsoft.com/en-us/graph/throttlingも参照してください。

**保護された項目を、次の順序で徐々にバックアップすることをお勧めします。

1. メールボックス。
2. メールボックスがすべてバックアップされた後、OneDriveに進みます。
3. OneDriveのバックアップ完了後、SharePoint Onlineサイトに進みます。

保護対象アイテムの数とサイズによっては、初回の完全バックアップに数日かかります。

必要なユーザー権限

Cyber Protection内

ローカルエージェントは、企業管理者アカウントで登録され、カスタマーテナントレベルで使用されていなければなりません。ユニットレベルでの企業管理者、部署管理者、およびユーザーは、Microsoft 365データのバックアップやリカバリを実行できません。

クラウドエージェントは、カスタマーのテナントレベルとユニットレベルの両方で利用できます。これらのレベルとそれぞれの管理者の詳細については、"異なるレベルで追加されたMicrosoft 365組織の管理"（594ページ）を参照してください。

Microsoft 365の場合

アカウントにMicrosoft 365のグローバル管理者権限が割り当てられている必要があります。

Microsoft 365のパブリックフォルダを検出して、バックアップとリカバリを行うには、メールボックスを利用できる、少なくとも1つのMicrosoft 365管理者アカウントが存在していて、そのアカウントにバックアップ対象のパブリックフォルダに対する読み取り/書き込み権限が付与されていなければなりません。

- ローカルエージェントはこのアカウントを使用してMicrosoft 365にログインします。エージェントがメールボックスの内容すべてにアクセスできるようにするために、このアカウントには**ApplicationImpersonation**管理ロールが割り当てられます。このアカウントパスワードを変更する場合は、Cyber Protectコンソールでパスワードをアップデートします（"Microsoft 365アクセス認証の変更"（591ページ）を参照）。
- クラウドエージェントはMicrosoft 365にログインしません。クラウドエージェントの操作に必要な許可を付与するには、まずグローバル管理者としてMicrosoft 365にログインする必要があります。
  Microsoft 365で以下の許可が必要です。
  - ユーザープロファイルによるサインインと読み取り
  - すべてのサイトコレクションファイルの読み取りと書き込み
  - 全ユーザーのプロファイルの読み取りと書き込み（制限なし）
  - すべてのグループの読み取りと書き込み
  - ディレクトリデータの読み取り
  - すべてのチャネルメッセージの読み取り
  - 管理メタデータの読み取りと書き込み
  - すべてのサイトコレクションの項目およびリストの読み取りと書き込み
  - すべてのサイトコレクションに対する完全な制御

- すべてのサイトコレクション項目の読み取りと書き込み
- すべてのメールボックスに無制限でアクセスできるExchange Webサービスを使用

- クラウドエージェントは、アカウント資格情報を保存せず、バックアップと復元を実行するために使用しません。資格情報の変更、アカウントの無効化、またはアカウントの削除は、クラウドエージェントの動作に影響しません。

制限事項

- ローカルエージェントでは、最大5000ワークロードを保護できます。クラウドエージェントでは、最大50000ワークロードを保護できます。
- メールボックスまたはOneDriveを所有するすべてのユーザーが、Cyber Protectコンソールに表示されます。これにはMicrosoft 365ライセンスを持たないユーザーやMicrosoft 365サービスへのサインインをブロックされているユーザーも含まれます。
- メールボックスのバックアップには、ユーザーから可視状態のフォルダのみが含まれます。**復元可能なアイテム**のフォルダとそのサブフォルダ（**削除**、**バージョン**、**完全削除**、**監査**、**DiscoveryHold**、**カレンダーログ**）は、メールボックスのバックアップに含まれません。
- 復元中にユーザー、パブリックフォルダ、グループ、またはサイトの自動作成はできません。たとえば、削除したSharePoint Onlineサイトを復元する場合、最初に新しいサイトを手動で作成し、その後で復元中にターゲットサイトとして指定します。
- 検索結果からアイテムを選択できたとしても、異なるリカバリポイントからそれらのアイテムを同時にリカバリすることはできません。
- バックアップ時には、コンテンツに適用されている機密性ラベルが保持されます。そのため、機密性の高いコンテンツが元のロケーション以外にリカバリされ、関係するユーザーのアクセス権限が異なっている場合は、コンテンツが非表示になる可能性があります。
- 同じワークロードに複数の個別のバックアップ計画を適用することはできません。
- 個別のバックアップ計画とグループバックアップ計画が同じワークロードに適用される場合、個別計画の設定が優先されます。

Microsoft 365シートライセンスレポート

社内管理者は、保護済みのMicrosoft 365シートとそのライセンスに関するレポートをダウンロードできます。レポートは、CSV形式で提供され、シートのライセンスステータスや、ライセンスが使用される理由などの情報が記載されています。またレポートには、保護済みのシート名、関連付けられたEメール、グループ、Microsoft 365組織、保護済みのワークロードタイプと名前などの情報も含まれます。

このレポートは、Microsoft 365組織が登録されたテナントでのみ利用可能です。

Microsoft 365シートライセンスレポートをダウンロードするには

1. 企業管理者としてCyber Protectコンソールにログインします。
2. 右上にあるアカウントアイコンをクリックします。
3. [**Microsoft 365シートライセンスレポート**] をクリックします。

ログの記録

バックアップされたEメールの内容を見る、添付物やファイルをダウンロードする、元のメールボックスではない場所にEメールをリカバリする、また上述の対象をEメールとして送信するなどのクラウドツークラウドリソースを利用した操作は、ユーザーのプライバシーを侵害する可能性があり、ログに記録されます。これらの操作は、管理ポータルの **[監視]** > **[監査ログ]** に記録されます。

ローカルにインストールされたOffice 365エージェントの使用

Microsoft 365組織の追加

Microsoft 365組織を追加するには

1. 企業管理者としてCyber Protectコンソールにログインします。
2. 右上にあるアカウントアイコンをクリックし、その後 **[ダウンロード]** > **[Agent for Office 365]** の順にクリックします。
3. このエージェントをダウンロードし、インターネットに接続されたWindowsマシンにインストールします。
4. Cyber Protectコンソールで、**[デバイス]** > **[Microsoft Office 365（ローカルエージェント）]** に進みます。
5. 表示されたウィンドウで、アプリケーションID、アプリケーションシークレット、Microsoft 365テナントIDを入力します。これらを検索する方法の詳細については、"アプリケーション ID とアプリケーションシークレットの取得"（589ページ）を参照してください。
6. **[OK]** をクリックします。

これにより、組織のデータアイテムが **[Microsoft Office 365（ローカルエージェント）]** ページのCyber Protectコンソールに表示されます。

重要
1つの組織（企業グループ）に許可されるローカルにインストールされるAgent for Office 365は1つのみです。

アプリケーション ID とアプリケーションシークレットの取得

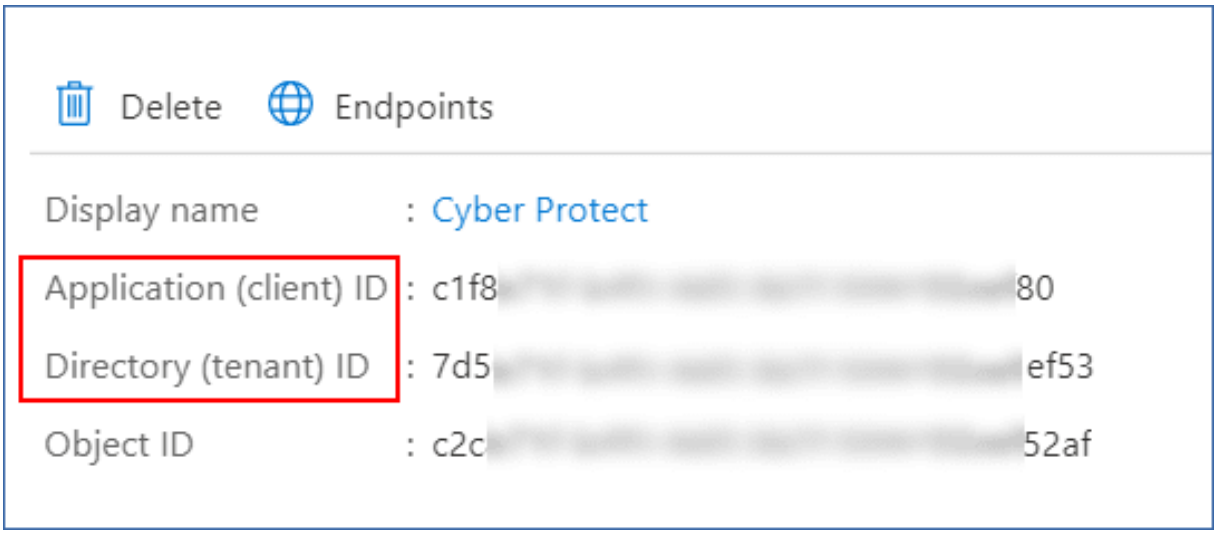
Office 365用のモダン認証を使用するには、Entra管理センターでカスタムアプリケーションを作成し、特定のAPI権限を付与する必要があります。この結果、 コンソールに入力する必要のある **アプリケーションID**、**アプリケーションシークレット**、**およびディレクトリ（テナント）ID**が取得できます。

注意
Agent for Office 365がインストールされているマシンで、ポート443を経由でのgraph.microsoft.comへのアクセスが許可されていることを確認します。

Entra管理センターでアプリケーションを作成するには

1. Entra管理センターに管理者としてログインします。
2. **[Azure Active Directory]** > **[アプリ登録]** に移動し、**[新規登録]** をクリックします。
3. Cyber Protectionなどのカスタムアプリケーションの名前を指定します。
4. **[サポートされているアカウントタイプ]** で、**[この組織ディレクトリのアカウントのみ]** を選択します。
5. **[登録]** をクリックします。

これでアプリケーションが作成されました。Entra管理センターで、アプリケーションの **[概要]** ページに移動し、アプリケーション（クライアント）IDとディレクトリ（テナントID）を確認します。



Entra管理センターでアプリケーションを作成する方法ついては、Microsoftの文書を参照してください。

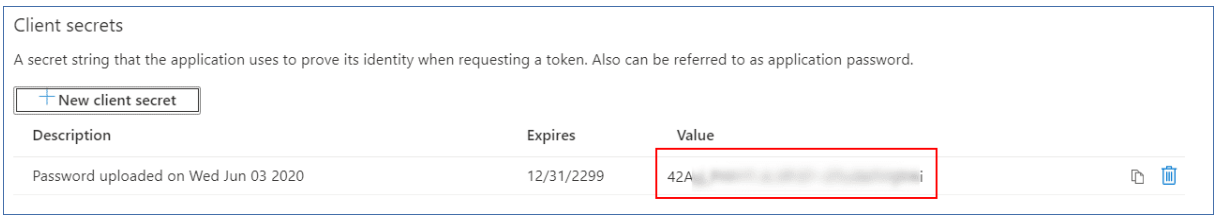
必要な API 許可をアプリケーションに付与する

1. Entra管理センターで、アプリケーションの **[API 許可]** に移動し、**[許可の追加]** をクリックします。
2. **[組織で使用する API]** タブを選択し、**[Office 365 Exchange Online]** を検索します。
3. **[Office 365 Exchange Online]** をクリックしてから、**[アプリケーション許可]** をクリックします。
4. **[full_access_as_app]** チェックボックスをオンにし、**[許可の追加]** をクリックします。
5. **[API 許可]** で **[許可の追加]** をクリックします。
6. **Microsoft Graph** を選択します。
7. **[アプリケーション許可]** を選択します。
8. **[ディレクトリ]** タブを展開して、**[Directory.Read.All]** チェックボックスをオンにします。**[許可の追加]** をクリックします。
9. すべての許可を確認し、**[<アプリケーション名> の管理者同意を付与]** をクリックします。
10. **[はい]** をクリックしてこの選択内容を確認します。

アプリケーションシークレットを作成する

1. Entra管理センターで、アプリケーションの**[証明書とシークレット]** > **[新しいクライアントシークレット]** に移動します。

2. 開いたダイアログボックスで、[有効期限:]**[なし]** を選択し、**[追加]** をクリックします。
3. **[値]** フィールドのアプリケーションシークレットを確認し、必ずそれを覚えていてください。



アプリケーションシークレットの詳細については、Microsoft 文書を参照してください。

Microsoft 365アクセス認証の変更

エージェントをインストールし直すことなく、Microsoft 365のアクセス認証を変更することができます。

Microsoft 365アクセス認証を変更するには

1. **[デバイス]** > **[Microsoft Office 365（ローカルエージェント）]** をクリックします。
2. Microsoft 365組織を選択します。
3. **[資格情報の指定]** をクリックします。
4. アプリケーションID、アプリケーションシークレット、Microsoft 365テナントIDを入力します。これらを検索する方法の詳細については、"アプリケーション ID とアプリケーションシークレットの取得"（589ページ）を参照してください。
5. **[OK]** をクリックします。

Exchange Onlineメールボックスの保護

バックアップできるアイテム

ユーザーメールボックスと共有メールボックスをバックアップできます。グループメールボックスとアーカイブメールボックス（**インプレースアーカイブ**）はバックアップできません。

復元できるアイテム

メールボックス バックアップから復元できるアイテムは次のとおりです。

- メールボックス
- 電子メールフォルダ
- メールメッセージ
- カレンダーのイベント
- タスク
- 連絡先
- 履歴項目
- メモ

アイテムの場所は検索で確認できます。

メールボックスが既存のメールボックスに復元されると、IDが一致する既存のアイテムは上書きされます。

メールボックスのアイテムの復元で上書きされるものはありません。その代わりに、メールボックスアイテムへのフルパスは、ターゲットフォルダで再作成されます。

Microsoft 365メールボックスを選択する

下記のようにメールボックスを選択し、保護計画のその他の設定を必要に応じて指定します。

メールボックスを選択する方法

1. [**Microsoft Office 365（ローカルエージェント）**] をクリックします。
2. バックアップするメールボックスを選択します。
3. [**バックアップ**] をクリックします。

メールボックスおよびメールボックスアイテムの復元

メールボックスの復元

1. [**Microsoft Office 365（ローカルエージェント）**] をクリックします。
2. 復元するメールボックスを選択してから、[**復元**] をクリックします。
   メールボックスを名前で検索できます。ワイルドカードはサポートされていません。
   メールボックスが削除された場合は、そのメールボックスを [バックアップストレージ] タブで選択してから、[**バックアップの表示**] をクリックします。
3. リカバリ ポイントを選択します。復元ポイントは、保存場所でフィルタされます。
4. [**復元**] >[**メールボックス**] の順にクリックします。
5. [**ターゲットメールボックス**] で、ターゲットメールボックスを表示、変更、または指定します。
   デフォルトでは、元のメールボックスが選択されます。このメールボックスが存在しない場合、ターゲットメールボックスの指定が必要です。
6. [**復元を開始**] をクリックします。

メールボックスのアイテムの復元

1. [**Microsoft Office 365（ローカルエージェント）**] をクリックします。
2. 復元するアイテムが元々存在していたメールボックスを選択し、[**復元**] をクリックします。
   メールボックスを名前で検索できます。ワイルドカードはサポートされていません。
   メールボックスが削除された場合は、そのメールボックスを [バックアップストレージ] タブで選択してから、[**バックアップの表示**] をクリックします。
3. リカバリ ポイントを選択します。復元ポイントは、保存場所でフィルタされます。
4. [**復元**] > [**メールメッセージ**] の順にクリックします。
5. 復元するアイテムを選択します。
   以下の検索オプションを選択できます。ワイルドカードはサポートされていません。
   - Eメールのメッセージの場合、件名、送信者、受信者、添付ファイル名、日付で検索します。
   - イベントの場合、タイトルと日付で検索します。

- タスクの場合、件名と日付で検索します。
- 連絡先の場合、名前、メールアドレス、電話番号で検索します。

電子メールのメッセージを選択したら、**[内容を表示]** をクリックすると、添付ファイルを含む内容を表示できます。

注意
添付ファイルをダウンロードするには、そのファイルの名前をクリックします。

電子メールのメッセージを選択したら、**[電子メールで送信]** をクリックすると、メッセージをメールアドレスに送信できます。メッセージは管理者アカウントのメールアドレスから送信されます。

フォルダを選択できるようにするには、[フォルダ復元] のアイコン（  ）をクリックします。

6. **[復元]** をクリックします。
7. **[ターゲットメールボックス]** で、ターゲットメールボックスを表示、変更、または指定します。
   デフォルトでは、元のメールボックスが選択されます。このメールボックスが存在しない場合、ターゲットメールボックスの指定が必要です。
8. **[復元を開始]** をクリックします。
9. 操作を確定します。

メールボックスのアイテムは、常にターゲットメールボックスの **[復元されたアイテム]** フォルダに復元されます。

Microsoft 365クラウドエージェントを使用する

Microsoft 365組織の追加

管理者は、単一または複数のMicrosoft 365組織をカスタマーのテナントまたはユニットに追加できます。

カスタマーテナントには、社内管理者が組織を追加します。ユニットには、ユニット管理者と、ユニットレベルで業務を行うカスタマー管理者が、組織を追加します。

Microsoft 365組織を追加するには

1. 組織を追加する必要がある場所に応じて、社内管理者またはユニット管理者としてCyber Protectコンソールにログインします。
2. （ユニットレベルで業務を行う社内管理者向け）管理ポータルから目的のユニットに移動します。
3. **[デバイス]** > **[追加]** > **[Microsoft 365ビジネス]** をクリックします。
   ソフトウェアによりMicrosoft 365のログインページにリダイレクトされます。
4. Microsoft 365のグローバル管理者の資格情報でサインインします。
   Microsoft 365に、組織のデータをバックアップおよびリカバリするために必要な権限の一覧が表示されます。
5. Cyber Protectionサービスにこれらの許可を与えることを確認します。

その結果、コンソールの **[デバイス]** タブの下に、Microsoft 365組織が表示されます。

役立つヒント

- 組織がCyber Protectionサービスに追加された時点から、クラウドエージェントは24時間ごとにMicrosoft 365と同期します。ユーザー、グループ、またはサイトの追加や削除を行った場合、変更がすぐにCyber Protectコンソールに表示されることはありません。変更をすぐに同期するには、**[Microsoft 365]** ページで組織を選択し、**[リフレッシュ]** をクリックします。
  Microsoft 365組織のリソースとCyber Protectコンソールの同期の詳細については、"Microsoft 365リソースの検出"（595ページ）を参照してください。
- 保護計画を **[すべてのユーザー]**、**[すべてのグループ]**、または **[すべてのサイト]** グループに適用した場合、新しく追加されたアイテムは同期後にのみバックアップに含まれます。
- Microsoftのポリシーにより、ユーザー、グループまたはサイトがMicrosoft 365のグラフィカルユーザーインターフェースから削除された場合でも、APIを介して数日間は利用可能な状態が維持されます。この間に削除されたアイテムは、Cyber Protectコンソールで非アクティブになって（グレーアウトされて）おり、バックアップされていません。削除されたアイテムがAPI経由で利用できなくなると、Cyber Protectコンソールに表示されなくなります。そのようなバックアップ（存在する場合）は **[バックアップストレージ]** > **[クラウドアプリケーションバックアップ]** で見つけることができます。

異なるレベルで追加されたMicrosoft 365組織の管理

カスタマーテナントレベルで追加されたMicrosoft 365組織に対しては、社内管理者は制限なくアクセスできます。

ユニットに追加された組織に対しては、社内管理者のアクセスは制限されています。これらの組織の場合は、ユニット名が括弧内に表示され、社内管理者は以下の操作を実行できます。

- バックアップからデータをリカバリする。
  社内管理者は、これらの組織が追加されたレベルに関わりなく、テナント内に存在するすべての組織のデータをリカバリすることができます。
- バックアップと、バックアップの復元ポイントを参照する。
- バックアップと、バックアップの復元ポイントを削除する。
- アラートおよびアクティビティを表示する。

社内管理者は、カスタマーテナントレベルで業務を行う場合、次の操作は実行できません。

- ユニットにMicrosoft 365組織を追加する。
- ユニットからMicrosoft 365組織を削除する。
- ユニットに追加されたMicrosoft 365組織を同期する。
- ユニットに追加されたMicrosoft 365組織内のデータ項目に関する保護計画の表示、作成、編集、削除、適用、実行、取り消しを行う。

ユニット管理者と、ユニットレベルで業務を行う社内管理者は、ユニットに追加された組織に制限なくアクセスすることができます。ただし、親カスタマーテナントからのリソース、例えばその内部で作成された保護計画などにアクセスすることはできません。

Microsoft 365組織の削除

Microsoft 365組織を削除しても、この組織のデータから取得された既存のバックアップには影響しません。これらのバックアップが不要になった場合は、まずバックアップを削除してから、Microsoft 365組織を削除してください。そうでない場合、引き続きバックアップは課金対象となる可能性のあるクラウドストレージスペースを使用します。

バックアップを削除する方法の詳細については、「"バックアップまたはバックアップアーカイブを削除するには"（520ページ）」を参照してください。

Microsoft 365組織を削除するには

1. 組織を追加する場所に応じて、社内管理者またはユニット管理者としてCyber Protectコンソールにサインインします。
2. （ユニットレベルで業務を行う社内管理者向け）管理ポータルから目的のユニットに移動します。
3. **[デバイス]** > **[Microsoft 365]** に進みます。
4. 組織を選択して、**[グループを削除]** をクリックします。

この操作により、このグループに適用されたバックアップ計画は取り消されます。

ただし、バックアップサービスアプリケーションのMicrosoft 365組織データへのアクセス権限は、手動で取り消す必要があります。

アクセス権を取り消す

1. グローバル管理者として、Microsoft 365にログインします。
2. **[管理センター]** > **[Azure Active Directory]** > **[エンタープライズアプリケーション]** > **[すべてのアプリケーション]** の順に進みます。
3. **[バックアップサービス]** アプリケーションを選択してドリルダウンします。
4. **[プロパティ]** タブに進み、アクションパネルで **[削除]** をクリックします。
5. 削除処理を確認します。

この操作により、バックアップサービスアプリケーションからMicrosoft 365組織データへのアクセス権が取り消されます。

Microsoft 365リソースの検出

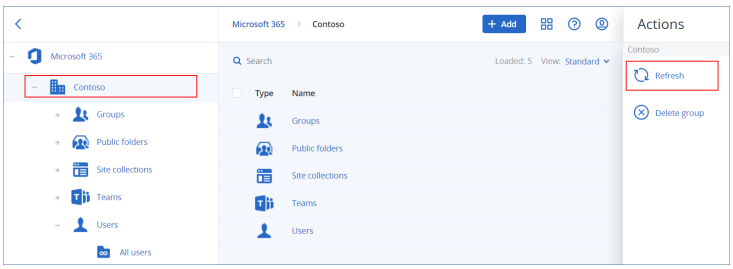
Microsoft 365組織をCyber Protectionサービスに追加すると、メールボックス、OneDriveストレージ、Microsoft Teams、SharePointサイトなど、この組織のリソースがCyber Protectコンソールに同期されます。この操作は検出と呼ばれ、**[監視]** > **[アクティビティ]** に記録されます。

検出処理が完了すると、コンソールの **[デバイス]** > **[Microsoft 365]** タブにMicrosoft 365組織のリソースが表示され、バックアップ計画を適用できるようになります。

自動検出処理は日次ベースで実行され、Cyber Protectコンソールのリソースのリストは常に最新の状態に維持されます。このリストは、手動で検出処理を再実行することにより、オンデマンドで同期させることもできます。

検出処理を手動で再実行するには

1. Cyber Protectコンソールで、[**デバイス**] > [**Microsoft 365**] に進みます。
2. Microsoft 365組織を選択し、[**操作**] ペインで [**リフレッシュ**] をクリックします。



注意
手動による検出処理は、1時間に最大10回まで実行できます。この回数に達すると、許可される実行回数は1時間に1回にリセットされます。その後は1時間に許可される実行回数が再び10回に達するまで、毎時1回の実行回数が追加されます。

Microsoft 365バックアップの頻度を設定する

デフォルトでは、Microsoft 365のバックアップは1日1回実行され、追加のスケジューリングオプションは利用できません。

テナントでAdvanced Backupパックが有効になっている場合、より頻度の高いバックアップを構成できます。1日のバックアップ回数は選択できますが、バックアップ開始時刻は構成できません。バックアップは、データセンター内で複数のカスタマーにサービスを提供しているクラウドエージェントの現在の負荷に応じて、おおよその間隔で自動的に開始されます。これにより、1日の負荷が均等になり、すべてのカスタマーのサービス品質が均等化されます。

次のオプションを使用できます。

スケジューリングオプション	各バックアップのおおよその間隔
1 日に一度	24 時間
1日に2回（デフォルト）	12 時間ごと
1日に3回	8 時間ごと
1日に6回	4 時間ごと

注意
クラウドエージェントの負荷やMicrosoft 365側で必要となる調整に応じて、バックアップの開始がスケジュールより遅れたり、完了までに時間がかかったりすることがあります。バックアップに平均間隔より長い時間がかかる場合、次回のバックアップが再スケジュールされるため、1日あたりのバックアップ回数が選択した回数より少なくなる可能性があります。例えば、1日6回のバックアップを選択したにもかかわらず、1日2回しか実行されない場合があります。

グループメールボックスのバックアップは、1日に一度だけ実行できます。

Exchange Onlineデータの保護

バックアップできるアイテム

ユーザーメールボックス、共有メールボックス、およびグループメールボックスをバックアップできます。オプションとして、選択したメールボックスのオンラインアーカイブメールボックス（**インプレースアーカイブ**）のバックアップを選択できます。

Cyber Protectionサービスのバージョン8.0以降では、パブリックフォルダをバックアップできます。組織がバージョン8.0のリリース以前にCyber Protectionサービスに追加された場合、この機能を取得するために組織を再度追加する必要があります。組織を削除せず、"Microsoft 365組織の追加"（593ページ）に説明されているステップを単純に繰り返してください。結果として、Cyber Protectionサービスは対応するAPIの使用許可を取得します。

復元できるアイテム

メールボックス バックアップから復元できるアイテムは次のとおりです。

- メールボックス
- 電子メールフォルダ
- メールメッセージ
- カレンダーのイベント
- タスク
- 連絡先
- 履歴項目
- メモ

以下のアイテムをパブリックフォルダバックアップから復元できます。

- サブフォルダ
- 投稿
- メールメッセージ

アイテムの場所は検索で確認できます。

メールボックス、メールボックスのアイテム、パブリックフォルダ、およびパブリックフォルダのアイテムを復元するとき、ターゲットロケーションにあるアイテムを上書きするかどうかを選択できます。

メールボックスの選択

下記のようにメールボックスを選択し、保護計画のその他の設定を必要に応じて指定します。

Exchange Onlineのメールボックスを選択する方法

1. **[Microsoft 365]** をクリックします。
2. Cyber Protectionサービスに複数のMicrosoft 365組織を追加している場合、バックアップするユーザーのデータがある組織を選択します。それ以外の場合は、この手順をスキップします。

3. 次のいずれかを実行します。
   - すべてのユーザーメールボックスとすべての共有メールボックス（将来作成されるメールボックスを含む）をバックアップするには、**[ユーザー]** ノードを展開し、**[すべてのユーザー]** を選択して、**[グループバックアップ]** をクリックします。
   - 個々のユーザーメールボックスや共有メールボックスをバックアップするには、**[ユーザー]** ノードを展開し、**[すべてのユーザー]** を選択し、バックアップするメールボックスのユーザーを選択し、**[バックアップ]** をクリックします。
   - すべてのグループメールボックス（将来作成されるグループのメールボックスを含む）をバックアップするには、**[グループ]** ノードを展開し、**[すべてのグループ]** を選択して、**[グループバックアップ]** をクリックします。
   - 個々のグループメールボックスをバックアップするには、**[グループ]** ノードを展開し、**[すべてのグループ]** を選択し、バックアップするメールボックスのグループを選択し、**[バックアップ]** をクリックします。

     注意
     クラウドのMicrosoft 365エージェントには、グループメールボックスにアクセスするための適切な権限を持つアカウントが必要です。このため、グループメールボックスをバックアップする場合、グループ所有者の少なくとも1人が、ライセンスされたMicrosoft 365ユーザーとしてメールボックスを使用している必要があります。そのグループがプライベートまたは非表示のメンバーシップである場合、所有者がそのグループのメンバーでなければなりません。

4. 保護計画パネルで、次の手順を実行します。
   - **[バックアップの対象]** で、**[Microsoft 365メールボックス]** アイテムが選択されていることを確認します。

     個別に選択した一部のユーザーがMicrosoft 365計画にExchangeサービスを含めていない場合、このオプションを選択することはできません。

     グループバックアップ向けに選択した一部のユーザーがMicrosoft 365計画にExchange サービスを含めていない場合、このオプションを選択することができますが、保護計画はそれらのユーザーには適用されません。
   - アーカイブメールボックスをバックアップしない場合は、**[アーカイブメールボックス]** スイッチを無効にします。

パブリックフォルダの選択

下記のようにパブリックフォルダを選択し、保護計画のその他の設定を必要に応じて指定します。

注意
パブリックフォルダではMicrosoft 365シートのライセンスをバックアップのクォータから使用します。

Exchange Onlineのパブリックフォルダを選択するには

1. **[Microsoft 365]** をクリックします。
2. Cyber Protectionサービスに複数のMicrosoft 365組織が追加されている場合は、データをバックアップする組織を展開します。それ以外の場合は、この手順をスキップします。

3. **パブリックフォルダ**ノードを拡張してから、**すべてのパブリックフォルダ**を選択します。
4. 次のいずれかを実行します。
   - すべてのパブリックフォルダ（将来作成されるパブリックフォルダを含む）をバックアップするには、[**グループバックアップ**] をクリックします。
   - 個々のパブリックフォルダをバックアップするには、バックアップするパブリックフォルダを選択し、[**バックアップ**] をクリックします。
5. 保護計画パネルの [**バックアップの対象**] で、[**Microsoft 365メールボックス**] アイテムが選択されていることを確認します。

メールボックスおよびメールボックスアイテムの復元

メールボックスの復元

1. [**Microsoft 365**] をクリックします。
2. Cyber Protectionサービスに複数のMicrosoft 365組織を追加している場合は、バックアップされたデータをリカバリする組織を選択します。それ以外の場合は、この手順をスキップします。
3. 次のいずれかを実行します。
   - ユーザーメールボックスを復元するには、[**ユーザー**] ノードを展開し、[**すべてのユーザー**] を選択し、復元するメールボックスのユーザーを選択し、[**復元**] をクリックします。
   - 共有メールボックスを復元するには、[**ユーザー**] ノードを展開し、[**すべてのユーザー**] を選択し、復元する共有メールボックスを選択し、[**復元**] をクリックします。
   - グループメールボックスを復元するには、[**グループ**] ノードを展開し、[**すべてのグループ**] を選択し、復元するメールボックスのグループを選択し、[**復元**] をクリックします。
   - ユーザー、グループ、または共有メールボックスが削除されている場合は、[バックアップストレージ] タブの [**クラウドアプリケーションバックアップ**] セクションでその項目を選択して、[**バックアップの表示**] をクリックします。

   ユーザーおよびグループを名前で検索できます。ワイルドカードはサポートされていません。
4. リカバリ ポイントを選択します。

   注意
   メールボックスを含む復元ポイントのみを表示するには、[**コンテンツでフィルタ**] で [**メールボックス**] を選択します。

5. [**復元**] > [**メールボックス全体**] の順にクリックします。
6. Cyber Protectionサービスに複数のMicrosoft 365組織が追加されている場合は、[**Microsoft 365組織**] をクリックして、ターゲット組織の表示、変更、または指定を行います。

   デフォルトでは、元の組織が選択されます。この組織がCyber Protectionサービスに現在登録されていない場合は、ターゲット組織を指定する必要があります。
7. [**メールボックスに復元**] で、ターゲットメールボックスを表示、変更、または指定します。

   デフォルトでは、元のメールボックスが選択されます。このメールボックスが存在しないか、元と異なる組織が選択されている場合は、ターゲットメールボックスを指定する必要があります。

   復元中に新しいターゲットのメールボックスを作成できません。メールボックスを新しいものにリカバリするには、まず、対象となるMicrosoft 365の組織でターゲットのメールボックスを作成し、そ

れから、クラウドエージェントに変更を同期させる必要があります。クラウド エージェントは、24時間ごとにMicrosoft 365と自動的に同期します。変更を即座に同期するには、Cyber Protectコンソールで、**Microsoft 365**ページの組織を選択し、**[リフレッシュ]** をクリックします。

8. **[復元を開始]** をクリックします。
9. 次のいずれかの上書きオプションを選択します。
   - **[既存のアイテムに上書きする]**
   - **[既存のアイテムを上書きしない]**
10. **[続行]** をクリックして、操作を確定します。

メールボックスのアイテムの復元

1. **[Microsoft 365]** をクリックします。
2. Cyber Protectionサービスに複数のMicrosoft 365組織を追加している場合は、バックアップされたデータをリカバリする組織を選択します。それ以外の場合は、この手順をスキップします。
3. 次のいずれかを実行します。
   - ユーザーメールボックスからアイテムを復元するには、**[ユーザー]** ノードを展開し、**[すべてのユーザー]** を選択し、復元するアイテムが最初にあったメールボックスのユーザーを選択し、**[復元]** をクリックします。
   - 共有メールボックスからアイテムを復元するには、**[ユーザー]** ノードを展開し、**[すべてのユーザー]** を選択し、復元するアイテムが最初にあった共有メールボックスを選択し、**[復元]** をクリックします。
   - グループメールボックスからアイテムを復元するには、**[グループ]** ノードを展開し、**[すべてのグループ]** を選択し、復元するアイテムが最初にあったメールボックスのグループを選択し、**[復元]** をクリックします。
   - ユーザー、グループ、または共有メールボックスが削除されている場合は、[バックアップストレージ] タブの **[クラウドアプリケーションバックアップ]** セクションでその項目を選択して、**[バックアップの表示]** をクリックします。

   ユーザーおよびグループを名前で検索できます。ワイルドカードはサポートされていません。
4. リカバリ ポイントを選択します。

   注意
   メールボックスを含む復元ポイントのみを表示するには、**[コンテンツでフィルタ]** で **[メールボックス]** を選択します。

5. **[復元]** > **[メールメッセージ]** の順にクリックします。
6. 目的のフォルダを参照するか、検索を使用して目的のアイテムの一覧を取得します。

   以下の検索オプションを選択できます。ワイルドカードはサポートされていません。
   - Eメールのメッセージの場合、件名、送信者、受信者、添付ファイル名、日付で検索します。開始日と終了日のいずれか、または両方の日付を選択して、時間範囲内で検索できます。
   - イベントの場合、タイトルと日付で検索します。
   - タスクの場合、件名と日付で検索します。
   - 連絡先の場合、名前、メールアドレス、電話番号で検索します。

7. 復元するアイテムを選択します。フォルダを選択できるようにするには、[フォルダ復元] のアイコン（  ）をクリックします。

   復元中に新しいターゲットのメールボックスを作成できません。新しいメールボックス項目を新しいメールボックスにリカバリするには、まず、Microsoft 365の組織でターゲットの新しいメールボックス項目を作成し、それから、クラウドエージェントに変更を同期させる必要があります。クラウドエージェントは、24時間ごとにMicrosoft 365と自動的に同期します。変更を即座に同期するには、Cyber Protectコンソールで、**Microsoft 365**ページの組織を選択し、**[リフレッシュ]** をクリックします。

   また、次のいずれかを実行できます。

   - アイテムを選択する際に、添付ファイルを含む内容を表示するには、**[内容を表示]** をクリックします。添付ファイルをダウンロードするには、そのファイルの名前をクリックします。
   - メールメッセージまたはカレンダーアイテムを選択したら、**[メールで送信]** をクリックして、アイテムを指定したメールアドレスに送信します。送信者を選択し、転送するアイテムに追加するテキストを作成できます。
   - バックアップが暗号化されておらず、検索を使用して、検索結果で1つのアイテムを選択した場合のみ、**[バージョンを表示]** をクリックして、復元するアイテムのバージョンを選択します。選択した復元ポイントより前または後の、任意のバックアップバージョンを選択できます。
8. **[復元]** をクリックします。
9. Cyber Protectionサービスに複数のMicrosoft 365組織が追加されている場合は、**[Microsoft 365組織]** をクリックして、ターゲット組織の表示、変更、または指定を行います。

   デフォルトでは、元の組織が選択されます。この組織がCyber Protectionサービスに現在登録されていない場合は、ターゲット組織を指定する必要があります。
10. **[メールボックスに復元]** で、ターゲットメールボックスを表示、変更、または指定します。

    デフォルトでは、元のメールボックスが選択されます。このメールボックスが存在しないか、元と異なる組織が選択されている場合は、ターゲットメールボックスを指定する必要があります。
11. （ユーザーメールボックスまたは共有メールボックスへ復元する場合のみ）**[パス]** で、ターゲットメールボックスのターゲットフォルダを表示または変更します。デフォルトでは、**[復元されたアイテム]** フォルダが選択されます。

    グループメールボックスのアイテムは、常に **[受信ボックス]** フォルダに復元されます。
12. **[復元を開始]** をクリックします。
13. 次のいずれかの上書きオプションを選択します。
    - **[既存のアイテムに上書きする]**
    - **[既存のアイテムを上書きしない]**
14. **[続行]** をクリックして、操作を確定します。

メールボックス全体のPSTデータファイルへのリカバリ

注意

インプレースアーカイブは、PSTファイルへの復元の一部としては復元できません。メールボックスとともにインプレースアーカイブを復元するには、"メールボックスの復元"（599ページ）を参照してください。

メールボックスをリカバリするには

1. **[Microsoft 365]** をクリックします。
2. Cyber Protectionサービスに複数のMicrosoft 365組織を追加している場合は、バックアップされたデータをリカバリする組織を選択します。それ以外の場合は、この手順をスキップします。
3. 次のいずれかを実行します。
   - ユーザーメールボックスをPSTデータファイルにリカバリするには、**[ユーザー]** ノードを展開し、**[すべてのユーザー]** を選択し、リカバリするメールボックスを選択してから、**[復元]** をクリックします。
   - 共有メールボックスをPSTデータファイルにリカバリするには、**[ユーザー]** ノードを展開し、**[すべてのユーザー]** を選択し、リカバリするメールボックスを選択してから、**[復元]** をクリックします。
   - グループメールボックスをPSTデータファイルにリカバリするには、**[グループ]** ノードを展開し、**[すべてのグループ]** を選択し、リカバリするメールボックスのグループを選択してから、**[復元]** をクリックします。

   ユーザーおよびグループを名前で検索できます。ワイルドカードはサポートされていません。

   ユーザー、グループ、または共有Outlookデータファイルが削除されている場合は、[バックアップストレージ] タブの **クラウドアプリケーションバックアップ**セクションでその項目を選択して、**[バックアップの表示]** をクリックします。
4. **[復元]** > **[PSTファイルとして]** をクリックします。
5. PSTファイルを含むアーカイブを暗号化するためのパスワードを設定します。

   パスワードには、最低でも1文字の記号を含める必要があります。
6. パスワードを確認し、**[完了]** をクリックします。
7. 選択されたメールボックス項目は、PSTデータファイルとしてリカバリされ、ZIP形式でアーカイブされます。1件のPSTファイルのサイズは最大で2GBに制限されているため、リカバリするデータが2GBを超える場合は複数のPSTファイルに分割されます。ZIPアーカイブは、設定したパスワードで保護されます。
8. 作成されたPSTファイルを含むZIPアーカイブへのリンクが記載されたEメールが届きます。
9. 管理者には、復元の手順が実行されたことを知らせるEメールが届きます。

注意
PSTファイルへのメールボックス復元は、データ転送の他に、複雑なアルゴリズムによるデータ変換が必要なため、時間がかかる場合があります。

PSTファイルを含むアーカイブをダウンロードして、復元を完了するには

1. 次のいずれかを実行します。
   - Eメールからアーカイブをダウンロードするには、**ファイルをダウンロード**のリンクをクリックしてください。

     アーカイブは24時間以内に限りダウンロード可能です。リンクの期限が切れた場合は、復元の手順を再度実行します。
   - Cyber Protectコンソールからアーカイブをダウンロードするには:

a. [**バックアップストレージ**] > [**PSTファイル**] に移動します。
b. ハイライトされた最新のアーカイブを選択します。
c. 右側のペインで、[**ダウンロード**] をクリックします。

アーカイブは、ご利用のコンピューターのデフォルトに設定されているダウンロードディレクトリにダウンロードされます。

2. アーカイブを暗号化するために設定したパスワードを使用して、アーカイブからPSTファイルを抽出します。
3. このPSTファイルはMicrosoft Outlookで開くことができます。

成果PSTファイルのサイズは、元のメールボックスよりもずっと小さくなる場合があり、通常このようになります。

重要
これらのファイルを**インポートおよびエクスポートウィザード**を使用して、Microsoft Outlookにインポートすることは避けてください。
ファイルをダブルクリックするか右クリックして、コンテキストメニューから [**このアプリケーションで開く**] > [**Microsoft Outlook**] を選択して開きます。

メールボックス項目のPSTファイルへのリカバリ

注意
インプレースアーカイブは、PSTファイルへの復元の一部としては復元できません。メールボックスとともにインプレースアーカイブを復元するには、"メールボックスの復元"（599ページ）を参照してください。

メールボックスの項目をリカバリするには

1. [**Microsoft 365**] をクリックします。
2. Cyber Protectionサービスに複数のMicrosoft 365組織を追加している場合は、バックアップされたデータをリカバリする組織を選択します。それ以外の場合は、この手順をスキップします。
3. 次のいずれかを実行します。
   - ユーザーメールボックスからアイテムを復元するには、[**ユーザー**] ノードを展開し、[**すべてのユーザー**] を選択し、復元するアイテムが最初にあったメールボックスのユーザーを選択し、[**復元**] をクリックします。
   - 共有メールボックスからアイテムを復元するには、[**ユーザー**] ノードを展開し、[**すべてのユーザー**] を選択し、復元するアイテムが最初にあった共有メールボックスを選択し、[**復元**] をクリックします。
   - グループメールボックスからアイテムを復元するには、[**グループ**] ノードを展開し、[**すべてのグループ**] を選択し、復元するアイテムが最初にあったメールボックスのグループを選択し、[**復元**] をクリックします。
   - ユーザー、グループ、または共有メールボックスが削除されている場合は、[バックアップストレージ] タブの [**クラウドアプリケーションバックアップ**] セクションでその項目を選択して、[**バックアップの表示**] をクリックします。

ユーザーおよびグループを名前で検索できます。ワイルドカードはサポートされていません。

4. **[復元]** > **[メールメッセージ]** の順にクリックします。
5. 目的のフォルダを参照するか、検索を使用して目的のアイテムの一覧を取得します。
   以下の検索オプションを選択できます。ワイルドカードはサポートされていません。
   - Eメールのメッセージの場合、件名、送信者、受信者、添付ファイル名、日付で検索します。
   - イベントの場合、タイトルと日付で検索します。
   - タスクの場合、件名と日付で検索します。
   - 連絡先の場合、名前、メールアドレス、電話番号で検索します。
6. 復元するアイテムを選択します。フォルダを選択できるようにするには、[フォルダ復元] のアイコン（  ）をクリックします。
   また、次のいずれかを実行できます。
   - アイテムを選択する際に、添付ファイルを含む内容を表示するには、**[内容の表示]** をクリックします。 添付ファイルをダウンロードするには、そのファイルの名前をクリックします。
   - メールメッセージまたはカレンダーアイテムを選択したら、**[メールで送信]** をクリックして、アイテムを指定したメールアドレスに送信します。送信者を選択し、転送するアイテムに追加するテキストを作成できます。
   - バックアップが暗号化されておらず、検索を使用して、検索結果で1つのアイテムを選択した場合のみ、**[バージョンを表示]** をクリックして、復元するアイテムのバージョンを選択します。選択した復元ポイントより前または後の、任意のバックアップバージョンを選択できます。
7. **[PSTファイルとしてリカバリ]** をクリックします。
8. PSTファイルを含むアーカイブを暗号化するためのパスワードを設定します。
   パスワードには、最低でも1文字の記号を含める必要があります。
9. パスワードを確認し、**[完了]** をクリックします。

選択されたメールボックス項目は、PSTデータファイルとしてリカバリされ、ZIP形式でアーカイブされます。1件のPSTファイルのサイズは最大で2GBに制限されているため、リカバリするデータが2GBを超える場合は複数のPSTファイルに分割されます。ZIPアーカイブは、設定したパスワードで保護されます。

作成されたPSTファイルを含むZIPアーカイブへのリンクが記載されたEメールが届きます。

管理者には、復元の手順が実行されたことを知らせるEメールが届きます。

PSTファイルを含むアーカイブをダウンロードして、復元を完了するには

1. 次のいずれかを実行します。
   - Eメールからアーカイブをダウンロードするには、**ファイルをダウンロード**のリンクをクリックしてください。
     アーカイブは24時間以内に限りダウンロード可能です。リンクの期限が切れた場合は、復元の手順を再度実行します。
   - Cyber Protectコンソールからアーカイブをダウンロードするには:
     a. **[バックアップストレージ]** > **[PSTファイル]** に移動します。
     b. ハイライトされた最新のアーカイブを選択します。
     c. 右側のペインで、**[ダウンロード]** をクリックします。

アーカイブは、ご利用のコンピューターのデフォルトに設定されているダウンロードディレクトリにダウンロードされます。

2. アーカイブを暗号化するために設定したパスワードを使用して、アーカイブからPSTファイルを抽出します。
3. このPSTファイルはMicrosoft Outlookで開くことができます。

   成果PSTファイルのサイズは、元のメールボックスよりもずっと小さくなる場合があり、通常このようになります。

重要

これらのファイルを**インポートおよびエクスポートウィザード**を使用して、Microsoft Outlookにインポートすることは避けてください。

ファイルをダブルクリックするか右クリックして、コンテキストメニューから **[このアプリケーションで開く]** > **[Microsoft Outlook]** を選択して開きます。

パブリックフォルダおよびフォルダアイテムの復元

パブリックフォルダまたはパブリックフォルダのアイテムをリカバリするには、ターゲットのMicrosoft 365組織の少なくとも1人の管理者に、ターゲットのパブリックフォルダに対する**所有者**の権限が必要です。アクセスが拒否されたというエラーで復元が失敗した場合は、ターゲットフォルダのプロパティでその権限を割り当て、Cyber Protectコンソールでターゲット組織を選択し、**[リフレッシュ]** をクリックしてから、復元を繰り返します。

パブリックフォルダまたはフォルダのアイテムを復元するには

1. **[Microsoft 365]** をクリックします。
2. Cyber Protectionサービスに複数のMicrosoft 365組織が追加されている場合は、バックアップデータをリカバリする組織を展開します。それ以外の場合は、この手順をスキップします。
3. 次のいずれかを実行します。
   - **[パブリックフォルダ]** ノードを展開し、**[すべてのパブリックフォルダ]** を選択し、復元するパブリックフォルダまたは復元するアイテムが元々含まれていたパブリックフォルダを選択し、**[復元]** をクリックします。
   - パブリックフォルダが削除されている場合は、[バックアップストレージ] タブの **[クラウドアプリケーションバックアップ]** セクションでそのチームドライブを選択して、**[バックアップの表示]** をクリックします。

   パブリックフォルダを名前で検索できます。ワイルドカードはサポートされていません。
4. リカバリ ポイントを選択します。
5. **[データの復元]** をクリックします。
6. 目的のフォルダを参照するか、検索を使用して目的のアイテムの一覧を取得します。

   電子メールのメッセージおよび投稿を、件名、送信者、受信者、日付で検索できます。ワイルドカードはサポートされていません。
7. 復元するアイテムを選択します。フォルダを選択できるようにするには、[フォルダ復元] のアイコン（  ）をクリックします。

   また、次のいずれかを実行できます。

- Eメールのメッセージまたは投稿を選択する際に、添付ファイルを含む内容を表示するには、**[内容を表示]** をクリックします。 添付ファイルをダウンロードするには、そのファイルの名前をクリックします。
- メールメッセージまたは投稿を選択したら、**[メールで送信]** をクリックして、アイテムを指定したメールアドレスに送信します。送信者を選択し、転送するアイテムに追加するテキストを作成できます。
- バックアップが暗号化されておらず、検索を使用して、検索結果で1つのアイテムを選択した場合のみ、**[バージョンを表示]** をクリックして、復元するアイテムのバージョンを選択します。選択した復元ポイントより前または後の、任意のバックアップバージョンを選択できます。

8. **[復元]** をクリックします。
9. Cyber Protectionサービスに複数のMicrosoft 365組織が追加されている場合は、**[Microsoft 365組織]** をクリックして、ターゲット組織の表示、変更、または指定を行います。

   デフォルトでは、元の組織が選択されます。この組織がCyber Protectionサービスに現在登録されていない場合は、ターゲット組織を指定する必要があります。
10. **[パブリックフォルダに復元]** で、ターゲットパブリックフォルダを表示、変更、または指定します。

    デフォルトでは、元のフォルダが選択されます。このフォルダが存在しない場合、または元と異なる組織が選択されている場合は、ターゲットフォルダを指定する必要があります。

    復元中に新しいパブリックフォルダを作成できません。パブリックフォルダを新しいものにリカバリするには、まず、対象となるMicrosoft 365の組織でターゲットのパブリックフォルダを作成し、それから、クラウドエージェントに変更を同期させる必要があります。クラウド エージェントは、24時間ごとにMicrosoft 365と自動的に同期します。変更を即座に同期するには、Cyber Protectコンソールで、**Microsoft 365**ページの組織を選択し、**[リフレッシュ]** をクリックします。
11. **[パス]** で、ターゲットパブリックフォルダにあるターゲットサブフォルダを表示または変更します。デフォルトでは、元のパスは再作成されます。
12. **[復元を開始]** をクリックします。
13. 次のいずれかの上書きオプションを選択します。

オプション	説明
[既存のアイテムに上書きする]	保存先のロケーションにある既存のファイルはすべて上書きされます。
[既存のアイテムを上書きしない]	保存先のロケーションに同名のファイルがある場合、そのファイルは上書きされず、ソースファイルは保存先に保存されません。

14. **[続行]** をクリックして、操作を確定します。

OneDriveファイルの保護

バックアップできるアイテム

OneDrive全体、または個別のファイルとフォルダをバックアップできます。

バックアップ計画の個別オプションでは、OneNoteノートブックのバックアップを利用できます。

ファイルは、共有権限とともにバックアップされます。高度な権限レベル（**[デザイン]**、**[フル]**、**[投稿]**）はバックアップされません。

一部のファイルには機密情報が含まれている場合があり、Microsoft 365のデータ損失防止（DLP）ルールによってアクセスがブロックされている可能性があります。これらのファイルのバックアップは実行されず、バックアップ操作の完了後に警告が表示されることもありません。

制限事項

共有メールボックスのOneDriveコンテンツのバックアップはサポートされていません。このコンテンツをバックアップするには、共有メールボックスを通常のユーザーアカウントに変換し、そのアカウントでOneDriveが有効になっていることを確認します。

復元できるアイテム

OneDrive全体またはバックアップされている任意のファイルまたはフォルダを復元できます。

アイテムの場所は検索で確認できます。

共有権限を復元するか、ファイルの復元先のフォルダのアクセス許可をファイルが継承するかを選択できます。

ファイルおよびフォルダの共有リンクは復元されません。

OneDriveファイルの選択

以下の記述のとおり、ファイルを選択し、保護計画のその他の設定を必要に応じて指定します。

OneDriveファイルを選択する方法

1. **[Microsoft 365]** をクリックします。
2. Cyber Protectionサービスに複数のMicrosoft 365組織を追加している場合、バックアップするユーザーのデータがある組織を選択します。それ以外の場合は、この手順をスキップします。
3. 次のいずれかを実行します。
   - すべてのユーザー（将来作成されるユーザーを含む）のファイルをバックアップするには、**[ユーザー]** ノードを展開し、**[すべてのユーザー]** を選択して、**[グループバックアップ]** をクリックします。
   - 個々のユーザーのファイルをバックアップするには、**[ユーザー]** ノードを展開し、**[すべてのユーザー]** を選択し、バックアップするファイルのユーザーを選択し、**[バックアップ]** をクリックします。
4. 保護計画パネルで、次の手順を実行します。
   - **[バックアップの対象]** で、**[OneDrive]** アイテムが選択されていることを確認します。
     個別に選択した一部のユーザーがMicrosoft 365計画にOneDrive サービスを含めていない場合、このオプションを選択することはできません。
     グループバックアップ向けに選択した一部のユーザーがMicrosoft 365計画にOneDriveサービスを含めていない場合、このオプションを選択することができますが、保護計画はそれらのユーザーには適用されません。

- **[バックアップの対象]** で、以下のいずれかを実行します。
  - デフォルト設定 **[すべて]**（すべてのファイル）を保持する。
  - 名前またはパスを追加して、バックアップするファイルとフォルダを指定する。
    ワイルドカード文字（*、**、?）を使用できます。パスの指定およびワイルドカードの使用に関する詳細については、「ファイルフィルタ」を参照してください。
  - 参照して、バックアップするファイルとフォルダを指定します。
    [参照] リンクは、単一のユーザーの保護計画を作成するときにのみ使用できます。
- （オプション）**[バックアップの対象]** で、**[除外の表示]** をクリックして、バックアップ中にスキップするファイルとフォルダを指定します。
  [ファイルの除外] では、ファイルの選択が上書きされます。つまり、両方のフィールドで同じファイルを指定した場合、バックアップ時にこのファイルはスキップされます。
- （オプション） OneNoteノートブックをバックアップするには、**[OneNoteを含める]** スイッチを有効にします。

OneDriveとOneDriveファイルの復元

OneDrive全体の復元

1. **[Microsoft 365]** をクリックします。
2. Cyber Protectionサービスに複数のMicrosoft 365組織を追加している場合は、バックアップされたデータをリカバリする組織を選択します。それ以外の場合は、この手順をスキップします。
3. **[ユーザー]** ノードを展開し、**[すべてのユーザー]** を選択し、復元するOneDriveのユーザーを選択し、**[復元]** をクリックします。
   ユーザーが削除されている場合は、[バックアップストレージ] タブの **[クラウドアプリケーションバックアップ]** セクションでそのユーザーを選択して、**[バックアップの表示]** をクリックします。
   ユーザーを名前で検索できます。ワイルドカードはサポートされていません。
4. リカバリ ポイントを選択します。

   注意
   OneDriveのファイルを含む復元ポイントのみを表示するには、**[コンテンツでフィルタ]** で **[OneDrive]** を選択します。

5. **[復元]** > **[OneDrive全体]** をクリックします。
6. Cyber Protectionサービスに複数のMicrosoft 365組織が追加されている場合は、**[Microsoft 365組織]** をクリックして、ターゲット組織の表示、変更、または指定を行います。
   デフォルトでは、元の組織が選択されます。この組織がCyber Protectionサービスに現在登録されていない場合は、ターゲット組織を指定する必要があります。
   復元中に新しいOneDriveターゲットを作成できません。OneDriveを新しいものにリカバリするには、まず、Microsoft 365の組織でターゲットのOneDriveを作成し、それから、クラウドエージェントに変更を同期させる必要があります。クラウド エージェントは、24時間ごとにMicrosoft 365と自動的に同期します。変更を即座に同期するには、Cyber Protectコンソールで、**Microsoft 365**ページの組織を選択し、**[リフレッシュ]** をクリックします。

7. **[ドライブに復元]** で、ターゲットユーザーを表示、変更、または指定します。
   デフォルトでは、元のユーザーが選択されます。このユーザーが存在しないか、元と異なる組織が選択されている場合は、ターゲットユーザーを指定する必要があります。
8. ファイルの共有権限を復元するかどうかを選択します。
9. **[復元を開始]** をクリックします。
10. 次のいずれかの上書きオプションを選択します。

オプション	説明
[既存のファイルが古い場合は上書きする]	保存先のロケーションに同じ名前のファイルがあり、それがソースファイルより古い場合、ソースファイルは以前のバージョンと置き換えられて保存先のロケーションに保存されます。
[既存のファイルを上書きする]	最終更新日に関係なく、保存先のロケーションにある既存のファイルはすべて上書きされます。
[既存のファイルを上書きしない]	保存先のロケーションに同じ名前のファイルがある場合、そのファイルには変更は適用されず、ソースファイルは保存先のロケーションに保存されません。

注意
OneNoteノートブックをリカバリする場合、**[既存のファイルが古い場合は上書きする]** および **[既存のファイルを上書きする]** のいずれでも、既存のOneNoteノートブックが上書きされます。

11. **[続行]** をクリックして、操作を確定します。

OneDriveファイルの復元

1. **[Microsoft 365]** をクリックします。
2. Cyber Protectionサービスに複数のMicrosoft 365組織を追加している場合は、バックアップされたデータをリカバリする組織を選択します。それ以外の場合は、この手順をスキップします。
3. **[ユーザー]** ノードを展開し、**[すべてのユーザー]** を選択し、復元するOneDriveファイルのユーザーを選択し、**[復元]** をクリックします。
   ユーザーが削除されている場合は、[バックアップストレージ] タブの **[クラウドアプリケーションバックアップ]** セクションでそのユーザーを選択して、**[バックアップの表示]** をクリックします。
   ユーザーを名前で検索できます。ワイルドカードはサポートされていません。
4. リカバリ ポイントを選択します。

注意
OneDriveのファイルを含む復元ポイントのみを表示するには、**[コンテンツでフィルタ]** で **[OneDrive]** を選択します。

5. **[復元]** > **[ファイル/フォルダ]** の順にクリックします。
6. 目的のフォルダを直接参照するか、検索を使用して目的のファイルとフォルダの一覧を取得します。
7. 復元するファイルを選択します。

バックアップが暗号化されておらず、1つのファイルを選択した場合、**[バージョンを表示]** をクリックして、復元するファイルのバージョンを選択できます。選択した復元ポイントより前または後の、任意のバックアップバージョンを選択できます。

8. ファイルをダウンロードする場合は、そのファイルを選択し、**[ダウンロード]** をクリックし、ファイルの保存先を選択して、**[保存]** をクリックします。それ以外の場合は、この手順をスキップします。
9. **[復元]** をクリックします。
10. Cyber Protectionサービスに複数のMicrosoft 365組織が追加されている場合は、**[Microsoft 365組織]** をクリックして、ターゲット組織の表示、変更、または指定を行います。

    デフォルトでは、元の組織が選択されます。この組織がCyber Protectionサービスに現在登録されていない場合は、ターゲット組織を指定する必要があります。

    復元中に新しいOneDriveを作成できません。ファイルを新しいOneDriveにリカバリするには、まず、対象となるMicrosoft 365の組織でターゲットのOneDriveを作成し、それから、クラウドエージェントに変更を同期させる必要があります。クラウド エージェントは、24時間ごとにMicrosoft 365と自動的に同期します。変更を即座に同期するには、Cyber Protectコンソールで、**Microsoft 365**ページの組織を選択し、**[リフレッシュ]** をクリックします。
11. **[ドライブに復元]** で、ターゲットユーザーを表示、変更、または指定します。

    デフォルトでは、元のユーザーが選択されます。このユーザーが存在しないか、元と異なる組織が選択されている場合は、ターゲットユーザーを指定する必要があります。
12. **[パス]** で、ターゲットユーザーのOneDriveにあるターゲットフォルダを表示または変更します。デフォルトでは、元のロケーションが選択されます。
13. ファイルの共有権限を復元するかどうかを選択します。
14. **[復元を開始]** をクリックします。
15. 次のいずれかのファイル上書きオプションを選択します。

オプション	説明
[既存のファイルが古い場合は上書きする]	保存先のロケーションに同じ名前のファイルがあり、それがソースファイルより古い場合、ソースファイルは以前のバージョンと置き換えられて保存先のロケーションに保存されます。
[既存のファイルを上書きする]	最終更新日に関係なく、保存先のロケーションにある既存のファイルはすべて上書きされます。
[既存のファイルを上書きしない]	保存先のロケーションに同じ名前のファイルがある場合、そのファイルには変更は適用されず、ソースファイルは保存先のロケーションに保存されません。

注意

OneNoteノートブックをリカバリする場合、**[既存のファイルが古い場合は上書きする]** および **[既存のファイルを上書きする]** のいずれでも、既存のOneNoteノートブックが上書きされます。

16. **[続行]** をクリックして、操作を確定します。

SharePoint Onlineサイトの保護

バックアップできるアイテム

SharePointクラシックサイトコレクション、グループ（現在はチーム）サイト、およびコミュニケーションサイトをバックアップできます。また、バックアップ対象に、個々のサブサイト、リスト、およびライブラリを選択することもできます。

バックアップ計画の個別オプションでは、OneNoteノートブックのバックアップを利用できます。

バックアップ中、次のアイテムはスキップされます。

- **[外観]** サイト設定（**タイトル、説明、およびロゴ**を除く）。
- サイトページコメントとページコメント設定（コメント**[オン]**/**[オフ]**）。
- **[サイトの機能]** サイト設定。
- WebパーツのページとWikiページに埋め込まれているWebパーツ（SharePoint Online APIの制限により）。
- チェックアウトされたファイル。編集するために手動でチェックアウトしたファイル、およびライブラリに作成またはアップロードされたすべてのファイルで、**[チェックアウト必須]** オプションがオンになっているファイル。これらのファイルをバックアップするには、最初にチェックインします。
- 列の外部データと管理対象メタデータタイプ。
- デフォルトのサイトコレクション"domain-my.sharepoint.com"。これは、すべての組織ユーザーのOneDriveファイルがコレクションです。
- ごみ箱の内容。

制限事項

- タイトル/説明のサイズが10000バイトを超える場合、サイト/サブサイト/リスト/列のタイトルと説明はバックアップ中に切り詰められます。
- SharePoint Onlineで作成された旧バージョンのファイルをバックアップすることはできません。最新バージョンのファイルのみ保護されます。
- 保持保留ライブラリをバックアップすることはできません。
- Microsoft 365の前身のサービスであるBusiness Productivity Online Suite（BPOS）で作成されたサイトはバックアップできません。
- 管理対象パス`/portals`を使用するサイトの設定はバックアップできません（例: `https://<テナント>.sharepoint.com/portals/...`）。
- リストまたはライブラリのIRM（Information Rights Management、情報権利管理）設定は、ターゲットのMicrosoft 365組織でIRMが有効になっている場合にのみリカバリできます。

復元できるアイテム

以下のアイテムをサイトバックアップから復元できます。

- サイト全体
- サブサイト

- 一覧
- リストアイテム
- ドキュメントライブラリ
- ［ドキュメント］
- リストアイテムの添付ファイル
- サイトページとWikiページ

アイテムの場所は検索で確認できます。

アイテムは、元のサイトまたは元以外のサイトに復元できます。復元されたアイテムへのパスは元のアイテムへのパスと同じです。パスが存在しない場合は、作成されます。

共有権限を復元するか、アイテムが復元後の親オブジェクトから権限を継承するかを選択できます。

復元できないアイテム

- **Visio Process Repository**テンプレートによるサブサイト。
- 次の種類のリスト。**調査リスト**、**タスクリスト**、**画像ライブラリ**、**リンク**、**カレンダー**、**掲示板**、**外部**、および**インポートスプレッドシート**。
- 複数のコンテンツタイプが有効にされるリスト。

SharePoint Onlineデータの選択

以下の記述のとおり、データを選択し、保護計画のその他の設定を必要に応じて指定します。

SharePoint Onlineデータを選択する方法

1. **[Microsoft 365]** をクリックします。
2. Cyber Protectionサービスに複数のMicrosoft 365組織を追加している場合、バックアップするユーザーのデータがある組織を選択します。それ以外の場合は、この手順をスキップします。
3. 次のいずれかを実行します。
   - 組織内のすべてのクラシックSharePointサイト（将来作成されるサイトを含む）をバックアップするには、**[サイトコレクション]** ノードを展開し、**[すべてのサイトコレクション]** を選択して、**[グループバックアップ]** をクリックします。
   - 個々のクラシックサイトをバックアップするには、**[サイトコレクション]** ノードを展開し、**[すべてのサイトコレクション]** を選択し、バックアップするサイトを選択し、**[バックアップ]** をクリックします。
   - 将来作成されるサイトを含むすべてのグループ（現在はチーム）サイトをバックアップするには、**[グループ]** ノードを展開し、**[すべてのグループ]** を選択して、**[グループバックアップ]** をクリックします。
   - 個別のグループ（現在はチーム）サイトをバックアップするには、**[グループ]** ノードを展開し、**[すべてのグループ]** を選択してから、バックアップするサイトのグループを選択して、**[バックアップ]** をクリックします。
4. 保護計画パネルで、次の手順を実行します。
   - **[バックアップの対象]** で、**[SharePointサイト]** アイテムが選択されていることを確認します。
   - **[バックアップの対象]** で、以下のいずれかを実行します。

- デフォルト設定 **[すべて]**（選択したサイトのすべてのアイテム）を保持する。
- 名前またはパスを追加して、バックアップするサブサイト、リスト、およびライブラリを指定する。

  サブサイトまたは最上位のサイトリスト/ライブラリをバックアップするには、次の形式で表示名を指定します。**/表示名/****

  サブサイトリスト/ライブラリをバックアップするには、次の形式で表示名を指定します。**/サブサイト表示名/リスト表示名/****

  サブサイト、リスト、およびライブラリの表示名が、SharePointサイトまたはサブサイトの **[サイト コンテンツ]** に表示されます。
- 参照して、バックアップするサブサイトを指定します。

  [参照] リンクは、単一のサイトの保護計画を作成するときにのみ使用できます。

- （オプション）**[バックアップの対象]** で、**[除外の表示]** をクリックして、バックアップ中にスキップするサブサイト、リスト、およびライブラリを指定します。

  項目の除外は、項目の選択を上書きします。つまり、両方のフィールドで同じサブサイトを指定した場合、バックアップ時にこのサブサイトはスキップされます。
- （オプション） OneNoteノートブックをバックアップするには、**[OneNoteを含める]** スイッチを有効にします。

SharePoint Onlineデータの復元

1. **[Microsoft 365]** をクリックします。
2. Cyber Protectionサービスに複数のMicrosoft 365組織を追加している場合は、バックアップされたデータをリカバリする組織を選択します。それ以外の場合は、この手順をスキップします。
3. 次のいずれかを実行します。
   - グループ（現在はチーム）サイトからデータを復元するには、**[グループ]** ノードを展開し、**[すべてのグループ]** を選択し、復元するアイテムが最初にあったサイトのグループを選択し、**[復元]** をクリックします。
   - クラシックサイトからデータを復元するには、**[サイトコレクション]** ノードを展開し、**[すべてのサイトコレクション]** を選択し、復元するアイテムが最初にあったサイトを選択し、**[復元]** をクリックします。
   - サイトが削除されている場合は、[バックアップストレージ] タブの **[クラウドアプリケーションバックアップ]** でそのサイトを選択して、**[バックアップの表示]** をクリックします。

   グループおよびサイトを名前で検索できます。ワイルドカードはサポートされていません。
4. リカバリ ポイントを選択します。

   注意

   SharePointサイトを含む復元ポイントのみを表示するには、**[コンテンツでフィルタ]** で **[SharePointサイト]** を選択します。
5. **[SharePointファイルの復元]** をクリックします。
6. 目的のフォルダを参照するか、検索を使用して目的のデータアイテムの一覧を取得します。
7. 復元するアイテムを選択します。

バックアップが暗号化されておらず、検索を使用して、検索結果で1つのアイテムを選択した場合、**[バージョンを表示]** をクリックして、復元するアイテムのバージョンを選択できます。選択した復元ポイントより前または後の、任意のバックアップバージョンを選択できます。

8. （オプション） アイテムをダウンロードする場合は、そのアイテムを選択し、**[ダウンロード]** をクリックしてから、アイテムの保存先のロケーションを選択して、**[保存]** をクリックします。
9. **[復元]** をクリックします。
10. Cyber Protectionサービスに複数のMicrosoft 365組織が追加されている場合は、**[Microsoft 365組織]** をクリックして、ターゲット組織の表示、変更、または指定を行います。

    デフォルトでは、元の組織が選択されます。この組織がCyber Protectionサービスに現在登録されていない場合は、ターゲット組織を指定する必要があります。
11. **[サイトに復元]** で、ターゲットサイトを表示、変更、または指定します。

    復元中に新しいSharePointサイトを作成できません。SharePointサイトを新しいものにリカバリするには、まず、対象となるMicrosoft 365の組織でターゲットのサイトを作成し、それから、クラウドエージェントに変更を同期させる必要があります。クラウド エージェントは、24時間ごとにMicrosoft 365と自動的に同期します。変更を即座に同期するには、Cyber Protectコンソールで、**Microsoft 365**ページの組織を選択し、**[リフレッシュ]** をクリックします。
12. 復元されたアイテムの共有権限を復元するかどうかを選択します。
13. **[復元を開始]** をクリックします。
14. 次のいずれかの上書きオプションを選択します。

オプション	説明
[既存のファイルが古い場合は上書きする]	保存先のロケーションに同じ名前のファイルがあり、それがソースファイルより古い場合、ソースファイルは以前のバージョンと置き換えられて保存先のロケーションに保存されます。
[既存のファイルを上書きする]	最終更新日に関係なく、保存先のロケーションにある既存のファイルはすべて上書きされます。
[既存のファイルを上書きしない]	保存先のロケーションに同じ名前のファイルがある場合、そのファイルには変更は適用されず、ソースファイルは保存先のロケーションに保存されません。

注意
OneNoteノートブックをリカバリする場合、**[既存のファイルが古い場合は上書きする]** および **[既存のファイルを上書きする]** のいずれでも、既存のOneNoteノートブックが上書きされます。

15. **[続行]** をクリックして、操作を確定します。

Microsoft 365 Teamsの保護

バックアップできるアイテム

チーム全体をバックアップできます。バックアップ対象には、チーム名、チームメンバーリスト、チームチャネルとその内容、チームのメールボックスと会議、チームサイトが含まれます。

バックアップ計画の個別オプションでは、OneNoteノートブックのバックアップを利用できます。

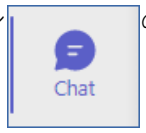
復元できるアイテム

- チーム全体
- チームチャネル
- チャネルのファイル
- チームのメールボックス
- チームのメールボックス内のメールフォルダ
- チームのメールボックス内のメールメッセージ
- 会議
- チームサイト

チームチャネルでの会話は復元できませんが、単一のhtmlファイルとしてダウンロードできます。

制限事項

以下の項目は、バックアップの対象外です。

- 一般チャネルの設定（モデレーション設定） - Microsoft Teams beta APIの制限によるものです。
- カスタムチャネルの設定（モデレーション設定） – Microsoft Teams beta APIの制限によるものです。
- ミーティングノート。
- チャットセクション 

のメッセージ。このセクションには、1対1のプライベートチャットとグループチャットがあります。
- ステッカーおよびいいね。

次のチャネルタブではバックアップと復元がサポートされます。

- Word
- Excel
- PowerPoint
- PDF
- ドキュメント ライブラリ

チームの選択

以下の記述のとおり、チームを選択し、保護計画のその他の設定を必要に応じて指定します。

チームの選択方法

1. **[Microsoft 365]** をクリックします。
2. Cyber Protectionサービスに複数のMicrosoft 365組織を追加している場合、バックアップするチームのデータがある組織を選択します。それ以外の場合は、この手順をスキップします。
3. 次のいずれかを実行します。

- 組織内のチームすべて（将来作成するチームを含む）をバックアップするには、**[チーム]** ノードを展開し、**[すべてのチーム]** を選択した上で、**[グループバックアップ]** をクリックします。
- 個々のチームをバックアップするには、**[チーム]** ノードを展開し、**[すべてのチーム]** を選択し、バックアップするチームを選択した上で、**[バックアップ]** をクリックします。

チームは名前で検索できます。ワイルドカードはサポートされていません。

4. 保護計画パネルで、次の手順を実行します。
   - **[バックアップの対象]** で、**[Microsoft Teams]** の項目が選択されていることを確認します。
   - （オプション）**[保存期間]** で、クリーンアップのオプションを設定します。
   - （オプション）バックアップを暗号化する場合は、**[暗号化]** スイッチをオンにした上で、パスワードを設定して暗号化アルゴリズムを選択します。
   - （オプション） OneNoteノートブックをバックアップするには、**[OneNoteを含める]** スイッチを有効にします。

チーム全体を復元

1. **[Microsoft 365]** をクリックします。
2. Cyber Protectionサービスに複数のMicrosoft 365組織を追加している場合は、バックアップされたチームをリカバリする組織を選択します。それ以外の場合は、この手順をスキップします。
3. **[チーム]** ノードを展開し、**[すべてのチーム]** を選択し、リカバリするチームを選択した上で、**[復元]** をクリックします。

   チームは名前で検索できます。ワイルドカードはサポートされていません。
4. リカバリ ポイントを選択します。
5. **[復元]** > **[チーム全体]** の順にクリックします。

   Cyber Protectionサービスに複数のMicrosoft 365組織が追加されている場合は、**[Microsoft 365組織]** をクリックして、ターゲット組織の表示、変更、または指定を行います。

   デフォルトでは、元の組織が選択されます。この組織がCyber Protectionサービスに現在登録されていない場合は、ターゲット組織を指定する必要があります。
6. **[チームに復元]** で、ターゲットチームを表示するか、別のターゲットチームを選択します。

   デフォルトでは、元のチームが選択されています。このチームが存在しない場合（たとえば、削除された場合）、または元のチームを含まない組織を選択した場合は、ドロップダウンリストからターゲットチームを選択する必要があります。

   チームは既存のチームにのみリカバリできます。復元操作中にチームを作成することはできません。
7. **[復元を開始]** をクリックします。
8. 次のいずれかの上書きオプションを選択します。
   - **既存のコンテンツが古い場合は上書きする**
   - **既存のコンテンツに上書きする**
   - **既存の内容を上書きしない**

注意
OneNoteノートブックをリカバリする場合、**[既存のコンテンツが古い場合は上書きする]** および **[既存のコンテンツに上書きする]** のいずれのオプションでも、既存のOneNoteノートブックが上書きされます。

9. **[実行]** をクリックして、操作を確定します。

Microsoft Teamsのグラフィックインターフェースでチャネルを削除すると、チャネルはシステムからすぐに削除されます。それで、チーム全体を復元すると、チャネル名は使用されずに接尾辞が追加されます。

会話は、チャネルの **[ファイル]** タブで、単一のhtmlファイルとして復元されます。このファイルは、**<チーム名>_<チャネル名>_conversations_backup_<復元日>T<復元時間>Z** という規則に準じて命名されたフォルダに格納されています。

注意
チームまたはチームチャネルをリカバリした後、Microsoft Teamsに移動し、リカバリされたチャネルを選択してから、**[ファイル]** タブをクリックします。そうでない場合、これらのチャネルのその後のバックアップには、このタブの内容が含められません。これはMicrosoft Teams beta APIの制限によります。

チームチャネルにおけるチームチャネルまたはファイルの復元

チームチャネルを復元するには

1. **[Microsoft 365]** をクリックします。
2. Cyber Protectionサービスに複数のMicrosoft 365組織を追加している場合は、バックアップされたチームをリカバリする組織を選択します。それ以外の場合は、この手順をスキップします。
3. **[チーム]** ノードを展開し、**[すべてのチーム]** を選択し、チャネルを復元するチームを選択した上で、**[復元]** をクリックします。
4. リカバリ ポイントを選択します。
5. **[復元]** >**[チャネル]** の順にクリックします。
6. 復元するチャネルを選択してから、**[復元]** をクリックします。メインペインでチャネルを選択して、名前の前にあるチェックボックスを選択します。
   以下の検索オプションを選択できます。
   - **会話**: 送信者、件名、内容、言語、添付名、日付または日付範囲。
   - **ファイル**: ファイル/フォルダ名、ファイルの種類、サイズ、直近の変更日付または日付範囲。

   注意
   また、ファイルをリカバリせずに、ローカルにダウンロードすることも可能です。
7. Cyber Protectionサービスに複数のMicrosoft 365組織が追加されている場合は、**[Microsoft 365組織]** をクリックして、ターゲット組織の表示、変更、または指定を行います。

デフォルトでは、元の組織が選択されます。この組織がCyber Protectionサービスに現在登録されていない場合は、ターゲット組織を指定する必要があります。

8. **[チームに復元]** で、ターゲットチームを表示、変更、または指定します。
   デフォルトでは、元のチームが選択されます。このチームが存在しない場合、または元と異なる組織が選択されている場合は、ターゲットチームを指定する必要があります。
9. **[チャネルに復元]** で、ターゲットチャネルを表示、変更、または指定します。
10. **[復元を開始]** をクリックします。
11. 次のいずれかの上書きオプションを選択します。
    - **既存のコンテンツが古い場合は上書きする**
    - **既存のコンテンツに上書きする**
    - **既存の内容を上書きしない**

    注意
    OneNoteノートブックをリカバリする場合、**[既存のコンテンツが古い場合は上書きする]** および **[既存のコンテンツに上書きする]** のいずれのオプションでも、既存のOneNoteノートブックが上書きされます。
12. **[続行]** をクリックして、操作を確定します。

会話は、チャネルの **[ファイル]** タブで、単一のhtmlファイルとして復元されます。このファイルは、**<チーム名>_<チャネル名>_conversations_backup_<復元日>T<復元時間>Z** という規則に準じて命名されたフォルダに格納されています。

注意
チームまたはチームチャネルをリカバリした後、Microsoft Teamsに移動し、リカバリされたチャネルを選択してから、**[ファイル]** タブをクリックします。そうでない場合、これらのチャネルのその後のバックアップには、このタブの内容が含められません。これはMicrosoft Teams beta APIの制限によります。

チームのチャネルでファイルを復元するには

1. **[Microsoft 365]** をクリックします。
2. Cyber Protectionサービスに複数のMicrosoft 365組織を追加している場合は、バックアップされたチームをリカバリする組織を選択します。それ以外の場合は、この手順をスキップします。
3. **[チーム]** ノードを展開し、**[すべてのチーム]** を選択し、チャネルを復元するチームを選択した上で、**[復元]** をクリックします。
4. リカバリ ポイントを選択します。
5. **[復元]** >**[チャネル]** の順にクリックします。
6. 希望のチャネルを選択して、**[ファイル]** フォルダを開きます。
   目的の項目を直接参照するか、検索を使用して目的の項目の一覧を取得します。次の検索オプションが利用可能です: ファイル/フォルダ名、ファイルの種類、サイズ、直近の変更日付または日付範囲。
7. （オプション） アイテムをダウンロードする場合は、そのアイテムを選択し、**[ダウンロード]** をクリックしてから、アイテムの保存先のロケーションを選択して、**[保存]** をクリックします。
8. 復元する項目を選択してから、**[復元]** をクリックします

9. Cyber Protectionサービスに複数のMicrosoft 365組織が追加されている場合は、[Microsoft 365組織] をクリックして、ターゲット組織の表示、変更、または指定を行います。
   デフォルトでは、元の組織が選択されます。この組織がCyber Protectionサービスに現在登録されていない場合は、ターゲット組織を指定する必要があります。
10. **[チームに復元]** で、ターゲットチームを表示、変更、または指定します。
    デフォルトでは、元のチームが選択されます。このチームが存在しない場合、または元と異なる組織が選択されている場合は、ターゲットチームを指定する必要があります。
11. **[チャネルに復元]** で、ターゲットチャネルを表示、変更、または指定します。
12. 復元されたアイテムの共有権限を復元するかどうかを選択します。
13. **[復元を開始]** をクリックします。
14. 次のいずれかの上書きオプションを選択します。
    - **既存のコンテンツが古い場合は上書きする**
    - **既存のコンテンツに上書きする**
    - **既存の内容を上書きしない**

    注意
    OneNoteノートブックをリカバリする場合、**[既存のコンテンツが古い場合は上書きする]** および **[既存のコンテンツに上書きする]** のいずれのオプションでも、既存のOneNoteノートブックが上書きされます。
15. **[続行]** をクリックして、操作を確定します。

個別の会話を復元することはできません。メインペインで **[会話]** フォルダを参照するか、その内容を単一のhtmlファイルとしてダウンロードするかのいずれかです。これを行うには、[フォルダを復元] のアイコン  をクリックしてから、希望する **[会話]** フォルダを選択して、**[ダウンロード]** をクリックします。

[会話] フォルダでは、次のオプションでメッセージを検索できます:

- 送信者
- ［コンテンツ］
- 添付ファイル名
- 日付

チームメールボックスの復元

1. **[Microsoft 365]** をクリックします。
2. Cyber Protectionサービスに複数のMicrosoft 365組織を追加している場合は、バックアップされたチームをリカバリする組織を選択します。それ以外の場合は、この手順をスキップします。
3. **[チーム]** ノードを展開し、**[すべてのチーム]** を選択し、メールボックスをリカバリするチームを選択してから、**[復元]** をクリックします。
   チームは名前で検索できます。ワイルドカードはサポートされていません。
4. リカバリ ポイントを選択します。
5. **[復元]** > **[メールメッセージ]** の順にクリックします。

6. [フォルダを復元] アイコン  をクリックし、ルートのメールボックスフォルダを選択して、**[復元]** をクリックします。

   注意
   選択したメールボックスから個別のフォルダをリカバリすることもできます。

7. **[復元]** をクリックします。
8. Cyber Protectionサービスに複数のMicrosoft 365組織が追加されている場合は、**[Microsoft 365組織]** をクリックして、ターゲット組織の表示、変更、または指定を行います。
   デフォルトでは、元の組織が選択されます。この組織がCyber Protectionサービスに現在登録されていない場合は、ターゲット組織を指定する必要があります。
9. **[メールボックスに復元]** で、ターゲットメールボックスを表示、変更、または指定します。
   デフォルトでは、元のメールボックスが選択されます。このメールボックスが存在しないか、元と異なる組織が選択されている場合は、ターゲットメールボックスを指定する必要があります。
10. **[復元を開始]** をクリックします。
11. 次のいずれかの上書きオプションを選択します。
    - **[既存のアイテムに上書きする]**
    - **[既存のアイテムを上書きしない]**
12. **[実行]** をクリックして、操作を確定します。

チームのメールボックス項目をPSTファイルにリカバリする

チームのメールボックス項目をリカバリするには

1. **[Microsoft 365]** をクリックします。
2. Cyber Protectionサービスに複数のMicrosoft 365組織を追加している場合は、バックアップされたデータをリカバリする組織を選択します。それ以外の場合は、この手順をスキップします。
3. ユーザーおよびグループを名前で検索できます。ワイルドカードはサポートされていません。
4. **[チーム]** ノードを展開し、**[すべてのチーム]** を選択し、リカバリする項目を含むメールボックスを所有するチームを選択してから、**[復元]** をクリックします。
5. **[復元]** > **[メールメッセージ]** の順にクリックします。
6. 目的のフォルダを参照するか、検索を使用して目的のアイテムの一覧を取得します。
   以下の検索オプションを選択できます。ワイルドカードはサポートされていません。
   - Eメールのメッセージの場合、件名、送信者、受信者、添付ファイル名、日付で検索します。
   - イベントの場合、タイトルと日付で検索します。
   - タスクの場合、件名と日付で検索します。
   - 連絡先の場合、名前、メールアドレス、電話番号で検索します。
7. 復元するアイテムを選択します。フォルダを選択できるようにするには、[フォルダ復元] のアイコン（  ）をクリックします。
   また、次のいずれかを実行できます。

- アイテムを選択する際に、添付ファイルを含む内容を表示するには、**[内容の表示]** をクリックします。 添付ファイルをダウンロードするには、そのファイルの名前をクリックします。
- メールメッセージまたはカレンダーアイテムを選択したら、**[メールで送信]** をクリックして、アイテムを指定したメールアドレスに送信します。送信者を選択し、転送するアイテムに追加するテキストを作成できます。
- バックアップが暗号化されていない場合、検索を使用して検索結果から1つの項目を選択し、**[バージョンを表示]** をクリックして、項目のバージョンを表示します。選択した復元ポイントの前または後であるかにかかわらず、任意のバックアップバージョンを選択できます。

8. **[PSTファイルとしてリカバリ]** をクリックします。
9. PSTファイルを含むアーカイブを暗号化するためのパスワードを設定します。
   パスワードには、最低でも1文字の記号を含める必要があります。
10. パスワードを確認し、**[完了]** をクリックします。

選択されたメールボックス項目は、PSTデータファイルとしてリカバリされ、ZIP形式でアーカイブされます。1件のPSTファイルのサイズは最大で2GBに制限されているため、リカバリするデータが2GBを超える場合は複数のPSTファイルに分割されます。ZIPアーカイブは、設定したパスワードで保護されます。

作成されたPSTファイルを含むZIPアーカイブへのリンクが記載されたEメールが届きます。

管理者には、復元の手順が実行されたことを知らせるEメールが届きます。

PSTファイルを含むアーカイブをダウンロードして、復元を完了するには

1. 次のいずれかを実行します。
   - Eメールからアーカイブをダウンロードするには、**ファイルをダウンロード**のリンクをクリックしてください。
     アーカイブは24時間以内に限りダウンロード可能です。リンクの期限が切れた場合は、復元の手順を再度実行します。
   - Cyber Protectコンソールからアーカイブをダウンロードするには:
     a. **[バックアップストレージ]** > **[PSTファイル]** に移動します。
     b. ハイライトされた最新のアーカイブを選択します。
     c. 右側のペインで、**[ダウンロード]** をクリックします。

   アーカイブは、ご利用のコンピューターのデフォルトに設定されているダウンロードディレクトリにダウンロードされます。
2. アーカイブを暗号化するために設定したパスワードを使用して、アーカイブからPSTファイルを抽出します。
3. Microsoft OutlookでPSTファイルを開くか、インポートします。この方法については、Microsoftの文書を参照してください。

Eメールメッセージおよび会議の復元

1. **[Microsoft 365]** をクリックします。
2. Cyber Protectionサービスに複数のMicrosoft 365組織を追加している場合は、バックアップされたチームをリカバリする組織を選択します。それ以外の場合は、この手順をスキップします。

3. **[チーム]** ノードを展開し、**[すべてのチーム]** を選択し、Eメールメッセージまたは会議をリカバリするチームを選択した上で、**[復元]** をクリックします。
   チームは名前で検索できます。ワイルドカードはサポートされていません。
4. リカバリ ポイントを選択します。
5. **[復元]** > **[メールメッセージ]** の順にクリックします。
6. 目的の項目を直接参照するか、検索を使用して目的の項目の一覧を取得します。
   以下の検索オプションを選択できます。
   - 電子メールのメッセージの場合、件名、送信者、受信者、日付で検索します。
   - 会議は、イベント名と日付で検索します。
7. 復元する項目を選択してから、**[復元]** をクリックします。

   注意
   会議は、**[カレンダー]** フォルダで見つけることができます。

   また、次のいずれかを実行できます。
   - アイテムを選択する際に、添付ファイルを含む内容を表示するには、**[内容の表示]** をクリックします。添付ファイルをダウンロードするには、そのファイルの名前をクリックします。
   - Eメールメッセージまたは会議を選択したら、**[Eメールで送信]** をクリックして、指定したEメールアドレスに項目を送信します。送信者を選択し、転送するアイテムに追加するテキストを作成できます。
8. Cyber Protectionサービスに複数のMicrosoft 365組織が追加されている場合は、**[Microsoft 365組織]** をクリックして、ターゲット組織の表示、変更、または指定を行います。
   デフォルトでは、元の組織が選択されます。この組織がCyber Protectionサービスに現在登録されていない場合は、ターゲット組織を指定する必要があります。
9. **[メールボックスに復元]** で、ターゲットメールボックスを表示、変更、または指定します。
   デフォルトでは、元のメールボックスが選択されます。このメールボックスが存在しないか、元と異なる組織が選択されている場合は、ターゲットメールボックスを指定する必要があります。
10. **[復元を開始]** をクリックします。
11. 次のいずれかの上書きオプションを選択します。
    - **[既存のアイテムに上書きする]**
    - **[既存のアイテムを上書きしない]**
12. **[実行]** をクリックして、操作を確定します。

チームサイトまたはサイトの特定の項目の復元

1. **[Microsoft 365]** をクリックします。
2. Cyber Protectionサービスに複数のMicrosoft 365組織を追加している場合は、バックアップされたチームをリカバリする組織を選択します。それ以外の場合は、この手順をスキップします。
3. **[チーム]** ノードを展開し、**[すべてのチーム]** を選択し、サイトを復元するチームを選択してから、**[復元]** をクリックします。
   チームは名前で検索できます。ワイルドカードはサポートされていません。
4. リカバリ ポイントを選択します。

5. **[復元]** >**[チームサイト]** の順にクリックします。
6. 目的の項目を直接参照するか、検索を使用して目的の項目の一覧を取得します。
7. （オプション） アイテムをダウンロードする場合は、そのアイテムを選択し、**[ダウンロード]** をクリックしてから、アイテムの保存先のロケーションを選択して、**[保存]** をクリックします。
8. 復元する項目を選択してから、**[復元]** をクリックします。
9. Cyber Protectionサービスに複数のMicrosoft 365組織が追加されている場合は、**[Microsoft 365組織]** をクリックして、ターゲット組織の表示、変更、または指定を行います。
   デフォルトでは、元の組織とチームが選択されます。この組織がCyber Protectionサービスに現在登録されていない場合は、ターゲット組織を指定する必要があります。
10. **[チームに復元]** で、ターゲットチームを表示、変更、または指定します。
    デフォルトでは、元のチームが選択されます。このチームが存在しない場合、または元と異なる組織が選択されている場合は、ターゲットサイトを指定する必要があります。
11. 復元されたアイテムの共有権限を復元するかどうかを選択します。
12. **[復元を開始]** をクリックします。
13. 次のいずれかの上書きオプションを選択します。
    - **既存のコンテンツが古い場合は上書きする**
    - **既存のコンテンツに上書きする**
    - **既存の内容を上書きしない**

    注意
    OneNoteノートブックをリカバリする場合、**[既存のコンテンツが古い場合は上書きする]** および **[既存のコンテンツに上書きする]** のいずれのオプションでも、既存のOneNoteノートブックが上書きされます。
14. **[実行]** をクリックして、操作を確定します。

OneNoteノートブックを保護する

デフォルトでは、OneNoteノートブックはOneDriveファイル、Microsoft Teams、およびSharePointサイトのバックアップに含まれています。

これらのバックアップからOneNoteノートブックを除外するには、該当するバックアップ計画で **[Onenoteを含める]** のスイッチを無効にします。

バックアップされたOneNoteノートブックのリカバリ

バックアップされたOneNoteノートブックをリカバリする方法については、それぞれのトピックを参照してください。

- OneDriveのバックアップについては、"OneDrive全体の復元"（608ページ）または"OneDriveファイルの復元"（609ページ）を参照してください。
- Teamsのバックアップについては、"チーム全体を復元"（616ページ）、"チームチャネルにおけるチームチャネルまたはファイルの復元"（617ページ）または"チームサイトまたはサイトの特定の項目の復元"（622ページ）を参照してください。

- SharePointサイトのバックアップについては、"SharePoint Onlineデータの復元"（613ページ）を参照してください。

サポートされるバージョン

- OneNote（OneNote 2016以降）
- Windows 10向けOneNote

制限事項および既知の問題点

- OneDriveやSharePointに保存するOneNoteノートブックの容量は2GBに制限されています。これより大きなOneNoteノートブックをOneDriveやSharePointのターゲットにリカバリすることはできません。
- セクショングループを含むOneNoteノートブックはサポートされていません。
- バックアップされたOneNoteノートブックにデフォルト以外の名前のセクションがある場合、最初のセクションはデフォルトの名前（**新しいセクション**、**無題セクション**など）で表示されます。このため、複数のセクションを含むノートブックでは、セクションの順番に影響が出る場合があります。
- OneNoteノートブックをリカバリする場合、**[既存のコンテンツが古い場合は上書きする]** および **[既存のコンテンツに上書きする]** のいずれのオプションでも、既存のOneNoteノートブックが上書きされます。
- チーム全体、チームサイト、またはチームサイトの**サイトアセット**フォルダをリカバリする場合、**[既存のコンテンツが古い場合は上書きする]**、または **[既存のコンテンツに上書きする]** を選択すると、そのチームのデフォルトOneNoteノートブックは上書きされません。ファイル「/sites/<チーム名>/SiteAssets/<OneNoteノート名>」のプロパティのアップデートに失敗しましたという警告とともに復元に成功します。

Microsoft 365コラボレーションアプリシートを保護する

Advanced Email Securityパックを使用して、Microsoft 365、Google Workspace、Open-Xchangeのメールボックスをリアルタイムに保護できます。

- マルウェア対策およびスパム対策
- Eメール内のURLスキャン
- DMARC分析
- フィッシング対策
- なりすまし防止
- 添付ファイルのスキャン
- コンテンツの対処と再構築
- 信頼性の可視化

また、Microsoft 365コラボレーションアプリシートを有効にすることで、コンテンツを介するセキュリティ脅威からMicrosoft 365クラウドコラボレーションアプリケーションを保護することができます。これらのアプリケーションには、OneDrive、SharePoint、Teamsが含まれる。

Advanced Email Securityは、ワークロード単位またはギガバイト単位で有効にすることができ、ライセンスモデルに影響します。

Cyber Protect CloudコンソールからAdvanced Email Securityのオンボーディングを行うには

1. **[デバイス]** > **[Microsoft 365]** をクリックします。
2. **[ユーザー]** ノードをクリックし、右上の **[Email Securityに移動]** リンクをクリックします。

Advanced Email Securityの詳細については、「Advanced Email Securityデータシート」を参照してください。

構成方法については、「Advanced Email SecurityとPerception Point」を参照してください。

Google Workspaceデータの保護

注意
この機能は、コンプライアンスモードのテナントでは利用できません。詳細については、"コンプライアンスモード"（1048ページ）を参照してください。

Google Workspaceの保護とは

- Google Workspaceユーザーデータ（Gmailメールボックス、カレンダー、連絡先、Googleドライブ）およびGoogle Workspace共有ドライブの、クラウドからクラウドへのバックアップおよび復元。
- メール、ファイル、連絡先、およびその他のアイテム単位の復元。
- 複数のGoogle Workspace組織および組織間の復元のサポート。
- Ethereumブロックチェーンデータベースによるオプション機能のバックアップファイルノータリゼーション。有効にすると、ファイルが本物でありバックアップ後に改変されていないことを証明できます。
- オプションの全文検索。有効にすると、メールをその内容で検索できます。
- パフォーマンスの低下を伴わずに、会社ごとに最大5000のアイテム（メールボックス、Googleドライブ、共有ドライブ）を保護できます。
- バックアップされたデータは自動的に圧縮されるため、バックアップ先で使用されるスペースは元のロケーションよりも小さくなります。クラウドツークラウドバックアップの圧縮レベルは固定であり、非クラウドツークラウドバックアップの**通常**レベルに相当します。これらのレベルの詳細については、"圧縮レベル"（448ページ）を参照してください。

必要なユーザー権限

Cyber Protection内

Cyber Protectionで、カスタマーテナントレベルの企業管理者でなければなりません。部署レベルでの企業管理者、部署管理者、およびユーザーは、Google Workspaceデータのバックアップや復元を実行できません。

Google Workspace において

Google Workspace組織をCyber Protectionサービスに追加するには、APIアクセスの有効な特権管理者としてサインインする必要があります（Google Adminコンソールで **[セキュリティ]** > **[API参照]** > **[APIアクセス有効化]**）。

特権管理者のパスワードはどこにも保管されず、バックアップと復元の実行には使用されません。このパスワードをGoogle Workspaceで変更しても、Cyber Protectionサービスの操作には影響しません。

Google Workspace組織を追加した特権管理者が、Google Workspaceから削除されるか、より権限が小さなロールに割り当てられると、「アクセスが拒否されました」といったエラーとともにバックアップが失敗します。この場合は、"Google Workspace組織を追加"（627ページ）で説明した手順を繰り返し、有効な特権管理者の資格情報を指定します。この状況を避けるため、バックアップ・復元専用の特権管理者ユーザーを作成することを推奨します。

バックアップスケジュールについて

クラウドエージェントは複数のカスタマーにサービスを提供しているため、1日の中での負荷を均等化し、すべてのカスタマーに均一なサービス品質を確保できるよう、各保護計画の開始時刻をエージェントが決定します。

各保護計画は、毎日同じ時刻に実行されます。

デフォルトのオプションは、**1日に一度**です。Advanced Backupパックでは、最大1日に6回のバックアップをスケジュールできます。バックアップは、データセンター内で複数のカスタマーにサービスを提供しているクラウドエージェントの現在の負荷に応じて、おおよその間隔で開始されます。これにより、1日の負荷が均等になり、すべてのカスタマーのサービス品質が均等化されます。

制限事項

- コンソールには、Google Workspaceのライセンスが割り当てられていて、メールボックスまたはGoogle Driveを使用しているユーザーのみが表示されます。
- Googleのネイティブ形式の文書は、一般的なオフィス文書としてバックアップされ、Cyber Protectコンソールでは、.docxや.pptxなどの異なる拡張子で表示されます。復元時には、文書は元の形式に変換されます。
- 1時間に実行できる手動バックアップは10回以下です。
- 同時に行える復元操作は10件まで（Microsoft 365およびGoogle Workspaceの復元を両方とも含む）です。
- 検索結果からアイテムを選択できたとしても、異なるリカバリポイントからそれらのアイテムを同時にリカバリすることはできません。
- 削除されたGoogle Workspaceユーザーアカウントのバックアップは、クラウドストレージから自動的に削除されません。これらのバックアップは、使用したストレージスペースに応じて課金されます。
- 同じワークロードに複数の個別のバックアップ計画を適用することはできません。

- 個別のバックアップ計画とグループバックアップ計画が同じワークロードに適用される場合、個別計画の設定が優先されます。

ログの記録

バックアップされたEメールの内容を見る、添付物やファイルをダウンロードする、元のメールボックスではない場所にEメールをリカバリする、また上述の対象をEメールとして送信するなどのクラウドツークラウドリソースを利用した操作は、ユーザーのプライバシーを侵害する可能性があり、ログに記録されます。これらの操作は、管理ポータルの **[監視]** > **[監査ログ]** に記録されます。

Google Workspace組織を追加

Google Workspace組織をCyber Protectionサービスに追加するには、専用のパーソナルGoogle Cloudプロジェクトが必要です。このようなプロジェクトを作成して設定する方法の詳細については、「"個人向けGoogle Cloudプロジェクトの作成"（628ページ）」を参照してください。

専用の個人向けGoogle Cloudプロジェクトを使用してGoogle Workspace組織を追加するには

1. 企業管理者としてCyber Protectコンソールにログインします。
2. **[デバイス]** > **[追加]** > **[Google Workspace]** の順にクリックします。
3. Google Workspaceアカウントの特権管理者のEメールアドレスを入力します。
   この手順は、特権管理者のEメールアカウントで2段階認証が有効になっているかどうかにかかわらず実行します。
4. Google Cloudプロジェクトで作成したサービスアカウントの秘密キーを含むJSONファイルを参照します。
   ファイルの内容をテキストとして貼り付けることもできます。
5. **[確認]** をクリックします。

その結果、コンソールの **[デバイス]** タブの下に、Google Workspace組織が表示されます。

役立つヒント

- Google Workspace組織を追加した後には、プライマリドメインとすべてのセカンダリドメイン（存在する場合）の両方にあるユーザーデータと共有ドライブがバックアップされます。バックアップされたリソースは1つのリストに表示され、ドメイン別のグループ分けは行われません。
- 組織がCyber Protectionサービスに追加された時点から、クラウドエージェントは24時間ごとにGoogle Workspaceと同期します。ユーザーまたは共有ドライブを追加/削除する場合、この変更はCyber Protectコンソールに直ちには表示されません。変更をすぐに同期するには、**Google Workspace**ページで組織を選択し、**[リフレッシュ]** をクリックします。
  Google Workspace組織のリソースとCyber Protectコンソールの同期の詳細については、"Google Workspaceリソースの検出"（631ページ）を参照してください。
- 保護計画を **[すべてのユーザー]** または **[すべての共有ドライブ]** グループに適用した場合、新しく追加されたアイテムは同期後にのみバックアップに含まれます。
- Googleのポリシーにより、ユーザーまたは共有ドライブがGoogle Workspaceのグラフィカルユーザーインターフェイスから削除された場合でも、APIを介して数日間は利用可能な状態が維持されま

す。この間に削除されたアイテムは、Cyber Protectコンソールで非アクティブになって（グレーアウトされて）おり、バックアップされていません。削除されたアイテムがAPI経由で利用できなくなると、Cyber Protectコンソールに表示されなくなります。そのようなバックアップ（存在する場合）は **[バックアップストレージ]** > **[クラウドアプリケーションバックアップ]** で見つけることができます。

個人向けGoogle Cloudプロジェクトの作成

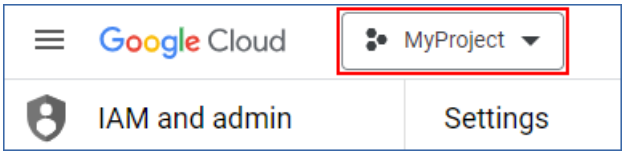
専用のGoogle Cloudプロジェクトを利用して、Google Workspace組織をCyber Protectionサービスに追加するには、次の手順を実行する必要があります。

1. 新しいGoogle Cloudプロジェクトを作成します。
2. このプロジェクトに必要なAPIを有効にします。
3. このプロジェクトの資格情報を設定します。
   a. OAuth同意画面を設定します。
   b. Cyber Protectionサービスのサービスアカウントを作成し、構成します。
4. 新しいプロジェクトにGoogle Workspaceアカウントへのアクセスを許可します。

注意
このトピックには、予告なく変更される可能性のあるサードパーティ製のユーザーインターフェースに関する説明が含まれています。

新しいGoogle Cloudプロジェクトを作成するには

1. Google Cloud Platform（console.cloud.google.com）に特権管理者としてログインします。
2. Googleクラウドプラットフォームのコンソールで、左上のプロジェクトピッカーをクリックします。



3. 開いた画面で組織を選択し、**[新規プロジェクト]** をクリックします。

4. 新しいプロジェクトの名前を指定します。
5. **[作成]** をクリックします。

これにより、新しいGoogle Cloudプロジェクトが作成されます。

このプロジェクトに必要なAPIを有効にするには

1. Google Cloud Platformコンソールで、新しいプロジェクトを選択します。
2. ナビゲーションメニューから、**[APIとサービス]** > **[有効なAPIとサービス]** を選択します。
3. このプロジェクトにおいてデフォルトで有効になっているすべてのAPIを1つずつ無効にします。
   a. **[有効なAPIとサービス]** ページを下にスクロールして、有効になっているAPIの名前をクリックします。
   選択したAPIの **[API/サービス詳細]** ページが開きます。

b. **[APIの無効化]** をクリックし、**[無効化]** をクリックして選択を確認します。

c. （プロンプトが表示されたら）**[確認]** をクリックして選択を確定します。

d. **[APIとサービス]** > **[有効なAPIとサービス]** に戻り、次のAPIを無効にします。

4. ナビゲーションメニューから、**[APIとサービス]** > **[ライブラリ]** を選択します。
5. APIライブラリでは、以下のAPIを1つずつ有効にします。
   - Admin SDK API
   - Gmail API
   - Google Calendar API
   - Google Drive API
   - Google People API

   検索バーを使用して、必要なAPIを検索します。APIを有効にするには、APIの名前をクリックしてから、**[有効化]** をクリックします。次のAPIを検索するには、ナビゲーションメニューから **[APIとサービス]** > **[ライブラリ]** を選択して、APIライブラリに戻ります。

OAuth同意画面を構成するには

1. Google Cloud Platformのナビゲーションメニューから、**[APIとサービス]** > **[OAuth同意画面]** を選択します。
2. 表示されたウィンドウで、ユーザータイプとして **[内部]** を選択してから、**[作成]** をクリックします。
3. **[アプリケーション名]** フィールドで、アプリケーションの名前を指定します。
4. **[ユーザーサポートEメール]** フィールドで、特権管理者のEメールアドレスを入力します。
5. **[開発者連絡先情報]** フィールドで、特権管理者のEメールアドレスを入力します。
6. 他のフィールドはすべて空白のままにして、**[保存して続行]** をクリックします。
7. **[スコープ]** のページで、変更を加えずに **[保存して続行]** をクリックします。
8. **[サマリ]** ページで設定を確認し、**[ダッシュボードに戻る]** をクリックします。

Cyber Protectionサービスのサービスアカウントを作成して構成するには

1. Google Cloud Platformのナビゲーションメニューから、**[IAMと管理]** > **[サービスアカウント]** を選択します。
2. **[サービスアカウントの作成]** をクリックします。
3. サービスアカウント名を指定します。
4. （オプション） サービスアカウントの説明を指定します。
5. **[作成して続行]** をクリックします。
6. **このサービスアカウントへのアクセス権をプロジェクトに付与**、および**このサービスアカウントへのアクセス権をユーザーに付与**の手順では何も変更しないでください。
7. **[完了]** をクリックします。

   [サービスアカウント] ページが開きます。
8. **[サービスアカウント]** ページで、新しいサービスアカウントを選択し、**[アクション]** の下の **[キーの管理]** をクリックします。
9. **[キー]** の下で、**[キーを追加]** > **[新しいキーを作成]** をクリックして、**[JSON]** キータイプを選択します。

10. **[作成]** をクリックします。
    その結果、サービスアカウントの秘密キーを持つJSONファイルが自動的に現在のマシンにダウンロードされます。このファイルは、Google Workspace組織をCyber Protectionサービスに追加するために必要なので、安全に保管してください。

新しいプロジェクトにGoogle Workspaceアカウントへのアクセスを許可するには

1. Google Cloud Platformのナビゲーションメニューから、**[IAMと管理]** > **[サービスアカウント]** を選択します。
2. リストで、作成したサービスアカウントを見つけて、**OAuth 2.0 Client ID**列に表示されているクライアントIDをコピーします。
3. Google管理者コンソール（console.cloud.google.com）に、特権管理者としてログインします。
4. ナビゲーションメニューから、**[セキュリティ]** > **[アクセスとデータ管理]** > **[APIコントロール]** を選択します。
5. **[APIコントロール]** ページを下にスクロールし、**[ドメイン全体の委任]** の下の **[ドメイン全体の委任の管理]** をクリックします。
   [ドメイン全体の委任] ページが開きます。
6. **[ドメイン全体の委任]** ページで、**[新規追加]** をクリックします。
   [新規クライアントIDの追加] ウィンドウが開きます。
7. **[クライアントID]** フィールドには、サービスアカウントクライアントのクライアントIDを入力します。
8. **OAuthスコープ**フィールドに、以下のスコープのカンマ区切りリストをコピーして貼り付けます:

   ```
   https://mail.google.com,https://www.googleapis.com/auth/contacts,https://www.googleapis.com/auth/calendar,https://www.googleapis.com/auth/admin.directory.user.readonly,https://www.googleapis.com/auth/admin.directory.domain.readonly,https://www.googleapis.com/auth/drive,https://www.googleapis.com/auth/gmail.modify
   ```

   または、1行に1つずつスコープを追加することもできます：
   - https://mail.google.com
   - https://www.googleapis.com/auth/contacts
   - https://www.googleapis.com/auth/calendar
   - https://www.googleapis.com/auth/admin.directory.user.readonly
   - https://www.googleapis.com/auth/admin.directory.domain.readonly
   - https://www.googleapis.com/auth/drive
   - https://www.googleapis.com/auth/gmail.modify
9. **[承認]** をクリックしてください。

これにより、新しいGoogle Cloudプロジェクトから、現在のGoogle Workspaceアカウントのデータにアクセスできるようになります。データをバックアップするには、このプロジェクトをCyber Protectionサービスにリンクする必要があります。その方法については、「"専用の個人向けGoogle Cloudプロジェクトを使用してGoogle Workspace組織を追加するには"（627ページ）」を参照してください

Google Cloudプロジェクトから現在のGoogle Workspaceアカウントへのアクセス、およびCyber Protectionサービスへのアクセスをそれぞれ取り消す必要がある場合は、プロジェクトが使用しているAPIクライアントを削除してください。

Google Workspaceアカウントへのアクセスを取り消すには

1. Google管理者コンソール（console.cloud.google.com）で、特権管理者としてサインインします。
2. ナビゲーションメニューから、**[セキュリティ]** > **[アクセスとデータ管理]** > **[APIコントロール]** を選択します。
3. **[APIコントロール]** ページを下にスクロールし、**[ドメイン全体の委任]** の下の **[ドメイン全体の委任の管理]** をクリックします。
   [ドメイン全体の委任] ページが開きます。
4. **[ドメイン全体の委任]** ページで、プロジェクトが使用しているAPIクライアントを選択し、**[削除]** をクリックします。
   これにより、Google CloudプロジェクトとCyber Protectionサービスは、Google Workspaceアカウントにアクセスしたり、その中のデータをバックアップしたりすることができなくなります。

Google Workspaceリソースの検出

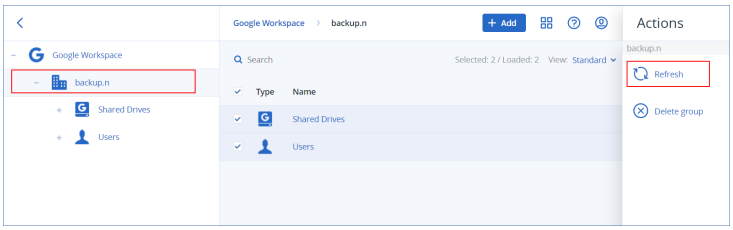
Google Workspace組織をCyber Protectionサービスに追加すると、メールボックスやGoogle Drivesなど、この組織のリソースがCyber Protectコンソールに同期されます。この操作は検出と呼ばれ、**[監視]** > **[アクティビティ]** に記録されます。

検出処理が完了すると、コンソールの **[デバイス]** > **[Google Workspace]** タブにGoogle Workspace組織のリソースが表示され、バックアップ計画を適用できるようになります。

自動検出処理は日次ベースで実行され、Cyber Protectコンソールのリソースのリストは常に最新の状態に維持されます。このリストは、手動で検出処理を再実行することにより、オンデマンドで同期させることもできます。

検出処理を手動で再実行するには

1. Cyber Protectコンソールで **[デバイス]** > **[Google Workspace]** に進みます。
2. Google Workspace組織を選択し、**[操作]** ペインで **[リフレッシュ]** をクリックします。



注意
手動による検出処理は、1時間に最大10回まで実行できます。この回数に達すると、許可される実行回数は1時間に1回にリセットされます。その後は1時間に許可される実行回数が再び10回に達するまで、毎時1回の実行回数が追加されます。

Google Workspaceバックアップの頻度を設定する

デフォルトでは、Google Workspaceのバックアップは1日1回実行され、追加のスケジューリングオプションは利用できません。

テナントでAdvanced Backupパックが有効になっている場合、より頻度の高いバックアップを構成できます。1日のバックアップ回数は選択できますが、バックアップ開始時刻は構成できません。バックアップは、データセンター内で複数のカスタマーにサービスを提供しているクラウドエージェントの現在の負荷に応じて、おおよその間隔で自動的に開始されます。これにより、1日の負荷が均等になり、すべてのカスタマーのサービス品質が均等化されます。

次のオプションを使用できます。

スケジューリングオプション	各バックアップのおおよその間隔
1 日に一度	24 時間
1日に2回（デフォルト）	12 時間ごと
1日に3回	8 時間ごと
1日に6回	4 時間ごと

注意
クラウドエージェントの負荷やGoogle Workspace側で必要となる調整に応じて、バックアップの開始がスケジュールより遅れたり、完了までに時間がかかったりすることがあります。バックアップに平均間隔より長い時間がかかる場合、次回のバックアップが再スケジュールされるため、1日あたりのバックアップ回数が選択した回数より少なくなる可能性があります。例えば、1日6回のバックアップを選択したにもかかわらず、1日2回しか実行されない場合があります。

Gmailデータを保護

バックアップできるアイテム

Gmailユーザーのメールボックスをバックアップできます。メールボックスのバックアップには、カレンダーと連絡先のデータも含まれます。オプションとして、共有カレンダーのバックアップを選択できます。

バックアップ中、次のアイテムはスキップされます。

- **誕生日**、**リマインダー**、**タスク**カレンダー
- カレンダーのイベントに添付されたフォルダ
- 連絡先の**ディレクトリ**フォルダ

Google Calendar APIの制限により、以下のカレンダーアイテムはスキップされます。

- 予約
- 予定の会議フィールド

- カレンダーの設定、**全日の予定通知**
- カレンダーの設定、**招待状の自動承認**（部屋または共有スペースのカレンダー）

Google People APIの制限により、以下の連絡先のアイテムはスキップされます。

- **その他連絡先**フォルダ
- 連絡先の外部プロファイル（**ディレクトリプロファイル**、**Googleプロファイル**）
- 連絡先フィールド、**ファイル形式**

復元できるアイテム

メールボックス バックアップから復元できるアイテムは次のとおりです。

- メールボックス
- メールフォルダ（Google用語では、「ラベル」。**ラベル**は、他のデータ表示との一貫性のために、バックアップソフトウェア内にフォルダとして表示されます）
- メールメッセージ
- カレンダーのイベント
- 連絡先

バックアップ内の項目の位置を特定するために、検索を使用できます。

メールボックスとメールボックスのアイテムを復元するとき、ターゲットロケーションにあるアイテムを上書きするかどうかを選択できます。

制限事項

- 連絡先の写真は復元できません
- Google Calendar API制限のため、**不在**カレンダーアイテムは標準カレンダーの予定として復元されます

Gmailメールボックスを選択する

下記のようにメールボックスを選択し、保護計画のその他の設定を必要に応じて指定します。

Gmailメールボックスを選択するには、以下の手順を実行してください

1. **Google Workspace**をクリックします。
2. Cyber Protectionサービスに複数のGoogle Workspace組織を追加している場合、バックアップするユーザーのデータがある組織を選択します。それ以外の場合は、この手順をスキップします。
3. 次のいずれかを実行します。
   - すべてのユーザー（将来作成されるメールボックスを含む）のメールボックスをバックアップするには、**[ユーザー]** ノードを展開し、**[すべてのユーザー]** を選択して、**[グループバックアップ]** をクリックします。
   - 個々のユーザーメールボックスをバックアップするには、**[ユーザー]** ノードを展開し、**[すべてのユーザー]** を選択し、バックアップするメールボックスのユーザーを選択し、**[バックアップ]** をクリックします。
4. 保護計画パネルで、次の手順を実行します。

- **[バックアップの対象]** で、**[Gmail]** アイテムが選択されていることを確認します。
- 選択したユーザーと共有しているカレンダーをバックアップするには、**[共有カレンダーを含める]** スイッチをオンにします。
- バックアップしたメールメッセージにおいて、全文検索が必要かどうかを決定します。このオプションにアクセスするには、歯車アイコンをクリックし、**[バックアップオプション]** > **[全文検索]** をクリックします。

メールボックスおよびメールボックスアイテムの復元

メールボックスの復元

1. **Google Workspace**をクリックします。
2. Cyber Protectionサービスに複数のGoogle Workspace組織を追加している場合は、バックアップされたデータをリカバリする組織を選択します。それ以外の場合は、この手順をスキップします。
3. **[ユーザー]** ノードを展開し、**[すべてのユーザー]** を選択し、メールボックスを復元するユーザーを選択し、**[復元]** をクリックします。
   ユーザーが削除されている場合は、[バックアップストレージ] タブの **[クラウドアプリケーションバックアップ]** セクションでそのユーザーを選択して、**[バックアップの表示]** をクリックします。
   ユーザーおよびグループを名前で検索できます。ワイルドカードはサポートされていません。
4. リカバリ ポイントを選択します。

   注意
   メールボックスを含む復元ポイントのみを表示するには、**[コンテンツでフィルタ]** で **[Gmail]** を選択します。

5. **[復元]** > **[メールボックス全体]** の順にクリックします。
6. Cyber Protectionサービスに複数のGoogle Workspace組織が追加されている場合は、**[Google Workspace組織]** をクリックして、ターゲット組織の表示、変更、または指定を行います。
   デフォルトでは、元の組織が選択されます。この組織がCyber Protectionサービスに現在登録されていない場合は、利用可能な登録済みの組織の中から、新しいターゲット組織を選択する必要があります。
7. **[メールボックスに復元]** で、ターゲットメールボックスを表示、変更、または指定します。
   デフォルトでは、元のメールボックスが選択されます。このメールボックスが存在しないか、元と異なる組織が選択されている場合は、ターゲットメールボックスを指定する必要があります。
   復元中に新しいターゲットメールボックスを作成することはできません。メールボックスを新しいメールボックスにリカバリするには、最初に任意のGoogle Workspace組織でターゲットとなるメールボックスを作成してから、クラウドエージェントで変更の同期を行う必要があります。クラウドエージェントは24時間ごとに自動でGoogle Workspaceと同期します。変更をすぐに同期するには、Cyber Protectコンソールの**Google Workspace**ページで組織を選択し、**[リフレッシュ]** をクリックします。
8. **[復元を開始]** をクリックします。
9. 次のいずれかの上書きオプションを選択します。

- **[既存のアイテムに上書きする]**
- **[既存のアイテムを上書きしない]**

10. **[続行]** をクリックして、操作を確定します。

メールボックスのアイテムの復元

1. **Google Workspace**をクリックします。
2. Cyber Protectionサービスに複数のGoogle Workspace組織を追加している場合は、バックアップされたデータをリカバリする組織を選択します。それ以外の場合は、この手順をスキップします。
3. **[ユーザー]** ノードを展開し、**[すべてのユーザー]** を選択し、復元するアイテムがメールボックスに元々含まれていたユーザーを選択し、**[復元]** をクリックします。
   ユーザーが削除されている場合は、[バックアップストレージ] タブの **[クラウドアプリケーションバックアップ]** セクションでそのユーザーを選択して、**[バックアップの表示]** をクリックします。
   ユーザーおよびグループを名前で検索できます。ワイルドカードはサポートされていません。
4. リカバリ ポイントを選択します。

   注意
   メールボックスを含む復元ポイントのみを表示するには、**[コンテンツでフィルタ]** で **[Gmail]** を選択します。

5. **[復元]** > **[メールメッセージ]** の順にクリックします。
6. 必要なフォルダを参照します。バックアップが暗号化されていない場合は、検索を使用して目的のアイテムの一覧を取得できます。
   以下の検索オプションを選択できます。ワイルドカードはサポートされていません。
   - メールメッセージの場合は、件名、送信者、受信者、日付、添付ファイル名、メッセージ内容で検索します。
     日付で検索する場合は、開始日と終了日美のいずれか、または両方の日付を選択して、時間範囲内で検索できます。
     添付ファイル名またはメッセージの内容で検索する場合は、バックアップ時に **[フルテキストの検索]** オプションが有効化されていた場合にのみ結果が出力されます。付加的なパラメータとして、検索されるメッセージフラグメントの言語を指定できます。
   - イベントの場合、タイトルと日付で検索します。
   - 連絡先の場合、名前、メールアドレス、電話番号で検索します。
7. 復元するアイテムを選択します。フォルダを選択できるようにするには、[フォルダ復元] のアイコン（  ）をクリックします。
   また、次のいずれかを実行できます。
   - アイテムを選択する際に、添付ファイルを含む内容を表示するには、**[内容の表示]** をクリックします。 添付ファイルをダウンロードするには、そのファイルの名前をクリックします。
   - バックアップが暗号化されておらず、検索を使用して、検索結果で1つのアイテムを選択した場合のみ、**[バージョンを表示]** をクリックして、復元するアイテムのバージョンを選択します。選択した復元ポイントより前または後の、任意のバックアップバージョンを選択できます。
8. **[復元]** をクリックします。

9. Cyber Protectionサービスに複数のGoogle Workspace組織が追加されている場合は、**[Google Workspace組織]** をクリックして、ターゲット組織の表示、変更、または指定を行います。
   デフォルトでは、元の組織が選択されます。この組織がCyber Protectionサービスに現在登録されていない場合は、利用可能な登録済みの組織の中から、新しいターゲット組織を選択する必要があります。
10. **[メールボックスに復元]** で、ターゲットメールボックスを表示、変更、または指定します。
    デフォルトでは、元のメールボックスが選択されます。このメールボックスが存在しないか、元と異なる組織が選択されている場合は、ターゲットメールボックスを指定する必要があります。
11. **[パス]** で、ターゲットメールボックスにあるターゲットフォルダを表示または変更します。デフォルトでは、元のフォルダが選択されます。
12. **[復元を開始]** をクリックします。
13. 次のいずれかの上書きオプションを選択します。
    - **[既存のアイテムに上書きする]**
    - **[既存のアイテムを上書きしない]**
14. **[続行]** をクリックして、操作を確定します。

Google ドライブのファイルを保護

バックアップできるアイテム

Googleドライブ全体、または個別のファイルとフォルダをバックアップできます。ファイルは、共有権限とともにバックアップされます。

重要
以下の項目は、バックアップの対象外です。

- **他のユーザーからの共有**フォルダ
- **コンピューター**フォルダ（バックアップおよび同期クライアントにより作成）

制限事項

Google固有のファイル形式のうち、Googleドキュメント、Googleシート、Googleスライドは、バックアップおよび復元の対象として完全にサポートされています。その他のGoogle固有のファイル形式については、完全にはサポートされていないか、まったくサポートされていない可能性があります。例えば、Google Drawingsファイルは`.svg`としてリカバリされます。また、Google Sitesファイルは`.txt`としてリカバリされ、Google Jamboardファイルは`.pdf`としてリカバリされます。さらにGoogle My Mapsファイルについてはバックアップ中にスキップされます。

注意
Google固有のファイル形式でないもの、例えば、`.txt`、`.docx`、`.pptx`、`.pdf`、`.jpg`、`.png`、`.zip`などは、バックアップおよび復元の対象として完全にサポートされています。

復元できるアイテム

Google ドライブ全体またはバックアップされている任意のファイルまたはフォルダを復元できます。

共有権限を復元するか、ファイルの復元先のフォルダのアクセス許可をファイルに継承させるかを選択できます。

制限事項

- ファイル内のコメントは復元されません。
- ファイルおよびフォルダの共有リンクは復元されません。
- 共有ファイルの読み取り専用の**所有者設定**（**エディタによりアクセスが変更され新たな人が追加されるのを防止し、コメント者と閲覧者に対してダウンロード、印刷、コピーするオプションを無効化する**）は、復元の最中に変更できません。
- 共有フォルダの所有権は、**エディタによりアクセスが変更され新たな人が追加されるのを防止する**オプションがこのフォルダで有効になっている場合、復元の最中に変更できません。この設定により、Google ドライブAPIでフォルダ権限がリストされるのが防止されます。フォルダ内のファイルの所有権は正しく復元されます。

Google ドライブのファイルを選択

以下の記述のとおり、ファイルを選択し、保護計画のその他の設定を必要に応じて指定します。

Google ドライブのファイルを選択するには、以下の手順を実行してください

1. **Google Workspace**をクリックします。
2. Cyber Protectionサービスに複数のGoogle Workspace組織を追加している場合、バックアップするユーザーのデータがある組織を選択します。それ以外の場合は、この手順をスキップします。
3. 次のいずれかを実行します。
   - すべてのユーザー（将来作成されるユーザーを含む）のファイルをバックアップするには、**[ユーザー]** ノードを展開し、**[すべてのユーザー]** を選択して、**[グループバックアップ]** をクリックします。
   - 個々のユーザーのファイルをバックアップするには、**[ユーザー]** ノードを展開し、**[すべてのユーザー]** を選択し、バックアップするファイルのユーザーを選択し、**[バックアップ]** をクリックします。
4. 保護計画パネルで、次の手順を実行します。
   - **[バックアップの対象]** で、**[Google ドライブ]** アイテムが選択されていることを確認します。
   - **[バックアップの対象]** で、以下のいずれかを実行します。
     - デフォルト設定 **[すべて]**（すべてのファイル）を保持する。
     - 名前またはパスを追加して、バックアップするファイルとフォルダを指定する。
       ワイルドカード文字（*、**、?）を使用できます。パスの指定およびワイルドカードの使用に関する詳細については、「ファイルフィルタ」を参照してください。
     - 参照して、バックアップするファイルとフォルダを指定します。
       [参照] リンクは、単一のユーザーの保護計画を作成するときにのみ使用できます。
   - （オプション）**[バックアップの対象]** で、**[除外の表示]** をクリックして、バックアップ中にスキップするファイルとフォルダを指定します。
     [ファイルの除外] では、ファイルの選択が上書きされます。つまり、両方のフィールドで同じファイルを指定した場合、バックアップ時にこのファイルはスキップされます。

- バックアップに選択されたすべてのファイルのノータリゼーションを有効にするには、**[ノータリゼーション]** スイッチをオンにします。ノータリゼーションの詳細については、「ノータリゼーション」を参照してください。

Google ドライブおよびGoogle ドライブのファイルを復元

Google ドライブ全体を復元

1. **Google Workspace**をクリックします。
2. Cyber Protectionサービスに複数のGoogle Workspace組織を追加している場合は、バックアップされたデータをリカバリする組織を選択します。それ以外の場合は、この手順をスキップします。
3. **[ユーザー]** ノードを展開し、**[すべてのユーザー]** を選択し、Google ドライブを復元するユーザーを選択し、**[復元]** をクリックします。
   ユーザーが削除されている場合は、[バックアップストレージ] タブの **[クラウドアプリケーションバックアップ]** セクションでそのユーザーを選択して、**[バックアップの表示]** をクリックします。
   ユーザーを名前で検索できます。ワイルドカードはサポートされていません。
4. リカバリ ポイントを選択します。

   注意
   Google ドライブのファイルを含む復元ポイントのみを表示するには、**[コンテンツでフィルタ]** で **[Google ドライブ]** を選択します。

5. **[復元]** > **[ドライブ全体]** の順にクリックします。
6. Cyber Protectionサービスに複数のGoogle Workspace組織が追加されている場合は、**[Google Workspace組織]** をクリックして、ターゲット組織の表示、変更、または指定を行います。
   デフォルトでは、元の組織が選択されます。この組織がCyber Protectionサービスに現在登録されていない場合は、利用可能な登録済みの組織の中から、新しいターゲット組織を選択する必要があります。
7. **[ドライブに復元]** で、ターゲットユーザーまたはターゲット共有ドライブを表示、変更、または指定します。
   デフォルトでは、元のユーザーが選択されます。このユーザーが存在しないか、元と異なる組織が選択されている場合は、ターゲットユーザーまたはターゲット共有ドライブを指定する必要があります。
   バックアップに共有ファイルが含まれる場合、ファイルはターゲットドライブのルートフォルダへ復元されます。
8. ファイルの共有権限を復元するかどうかを選択します。
9. **[復元を開始]** をクリックします。

10. 次のいずれかの上書きオプションを選択します。

オプション	説明
[既存のファイルが古い場合は上書きする]	保存先のロケーションに同じ名前のファイルがあり、それがソースファイルより古い場合、ソースファイルは以前のバージョンと置き換えられて保存先のロケーションに保存されます。
[既存のファイルを上書きする]	最終更新日に関係なく、保存先のロケーションにある既存のファイルはすべて上書きされます。
[既存のファイルを上書きしない]	保存先のロケーションに同じ名前のファイルがある場合、そのファイルには変更は適用されず、ソースファイルは保存先のロケーションに保存されません。

11. **[続行]** をクリックして、操作を確定します。

Google ドライブのファイルを復元

1. **Google Workspace**をクリックします。
2. Cyber Protectionサービスに複数のGoogle Workspace組織を追加している場合は、バックアップされたデータをリカバリする組織を選択します。それ以外の場合は、この手順をスキップします。
3. **[ユーザー]** ノードを展開し、**[すべてのユーザー]** を選択し、Google ドライブのファイルを復元するユーザーを選択し、**[復元]** をクリックします。
   ユーザーが削除されている場合は、[バックアップストレージ] タブの **[クラウドアプリケーションバックアップ]** セクションでそのユーザーを選択して、**[バックアップの表示]** をクリックします。
   ユーザーを名前で検索できます。ワイルドカードはサポートされていません。
4. リカバリ ポイントを選択します。

   注意
   Google ドライブのファイルを含む復元ポイントのみを表示するには、**[コンテンツでフィルタ]** で **[Google ドライブ]** を選択します。

5. **[復元]** > **[ファイル/フォルダ]** の順にクリックします。
6. 目的のフォルダを直接参照するか、検索を使用して目的のファイルとフォルダの一覧を取得します。
7. 復元するファイルを選択します。
   バックアップが暗号化されておらず、1つのファイルを選択した場合、**[バージョンを表示]** をクリックして、復元するファイルのバージョンを選択できます。選択した復元ポイントより前または後の、任意のバックアップバージョンを選択できます。
8. ファイルをダウンロードする場合は、そのファイルを選択し、**[ダウンロード]** をクリックし、ファイルの保存先を選択して、**[保存]** をクリックします。それ以外の場合は、この手順をスキップします。
9. **[復元]** をクリックします。
10. Cyber Protectionサービスに複数のGoogle Workspace組織が追加されている場合は、**[Google Workspace組織]** をクリックして、ターゲット組織の表示、変更、または指定を行います。

デフォルトでは、元の組織が選択されます。この組織がCyber Protectionサービスに現在登録されていない場合は、利用可能な登録済みの組織の中から、新しいターゲット組織を選択する必要があります。

11. **[ドライブに復元]** で、ターゲットユーザーまたはターゲット共有ドライブを表示、変更、または指定します。
    デフォルトでは、元のユーザーが選択されます。このユーザーが存在しないか、元と異なる組織が選択されている場合は、ターゲットユーザーまたはターゲット共有ドライブを指定する必要があります。
12. **[パス]** で、ターゲットユーザーのGoogleドライブまたはターゲット共有ドライブにあるターゲットフォルダを表示または変更します。デフォルトでは、元のロケーションが選択されます。
13. ファイルの共有権限を復元するかどうかを選択します。
14. **[復元を開始]** をクリックします。
15. 次のいずれかのファイル上書きオプションを選択します。

オプション	説明
[既存のファイルが古い場合は上書きする]	保存先のロケーションに同じ名前のファイルがあり、それがソースファイルより古い場合、ソースファイルは以前のバージョンと置き換えられて保存先のロケーションに保存されます。
[既存のファイルを上書きする]	最終更新日に関係なく、保存先のロケーションにある既存のファイルはすべて上書きされます。
[既存のファイルを上書きしない]	保存先のロケーションに同じ名前のファイルがある場合、そのファイルには変更は適用されず、ソースファイルは保存先のロケーションに保存されません。

16. **[続行]** をクリックして、操作を確定します。

共有ドライブファイルを保護

バックアップできるアイテム

共有ドライブ全体、または個別のファイルとフォルダをバックアップできます。ファイルは、共有権限とともにバックアップされます。

重要
他のユーザーからの共有フォルダはバックアップされません。

制限事項

- GoogleドライブAPIの制限により、メンバーのいない共有ドライブをバックアップすることはできません。
- Google固有のファイル形式のうち、Googleドキュメント、Googleシート、Googleスライドは、バックアップおよび復元の対象として完全にサポートされています。その他のGoogle固有のファイル形式については、完全にはサポートされていないか、まったくサポートされていない可能性があります。例えば、Google Drawingsファイルは.svgとしてリカバリされます。また、Google Sitesファイル

は.txtとしてリカバリされ、Google Jamboardファイルは.pdfとしてリカバリされます。さらにGoogle My Mapsファイルについてはバックアップ中にスキップされます。

注意
Google固有のファイル形式でないもの、例えば、.txt、.docx、.pptx、.pdf、.jpg、.png、.zipなどは、バックアップおよび復元の対象として完全にサポートされています。

復元できるアイテム

共有ドライブ全体またはバックアップされている任意のファイルまたはフォルダを復元できます。

共有権限を復元するか、ファイルの復元先のフォルダのアクセス許可をファイルに継承させるかを選択できます。

以下のアイテムは復元されません。

- ターゲット共有ドライブで組織外との共有が無効になっている場合、組織外のユーザーとのファイル共有許可は復元されません。
- ターゲット共有ドライブで**メンバー以外との共有**が無効になっている場合、ターゲット共有ドライブのメンバーではないユーザーとのファイル共有許可は復元されません。

制限事項

- ファイル内のコメントは復元されません。
- ファイルおよびフォルダの共有リンクは復元されません。

共有ドライブファイルを選択

以下の記述のとおり、ファイルを選択し、保護計画のその他の設定を必要に応じて指定します。

共有ドライブファイルを選択するには

1. **Google Workspace**をクリックします。
2. Cyber Protectionサービスに複数のGoogle Workspace組織を追加している場合、バックアップするユーザーのデータがある組織を選択します。それ以外の場合は、この手順をスキップします。
3. 次のいずれかを実行します。
   - すべての共有ドライブ（将来作成される共有ドライブを含む）のファイルをバックアップするには、[**共有ドライブ**] ノードを展開し、[**すべての共有ドライブ**] を選択して、[**グループバックアップ**] をクリックします。
   - 個々の共有ドライブのファイルをバックアップするには、[**共有ドライブ**] ノードを展開し、[**すべての共有ドライブ**] を選択し、バックアップする共有ドライブを選択し、[**バックアップ**] をクリックします。
4. 保護計画パネルで、次の手順を実行します。
   - [**バックアップの対象**] で、以下のいずれかを実行します。
     - デフォルト設定 [**すべて**]（すべてのファイル）を保持する。
     - 名前またはパスを追加して、バックアップするファイルとフォルダを指定する。

ワイルドカード文字（*、**、?）を使用できます。パスの指定およびワイルドカードの使用に関する詳細については、「ファイルフィルタ」を参照してください。

- 参照して、バックアップするファイルとフォルダを指定します。

  [参照] リンクは、単一の共有ドライブの保護計画を作成するときにのみ使用できます。

- （オプション）**[バックアップの対象]** で、**[除外の表示]** をクリックして、バックアップ中にスキップするファイルとフォルダを指定します。

  [ファイルの除外] では、ファイルの選択が上書きされます。つまり、両方のフィールドで同じファイルを指定した場合、バックアップ時にこのファイルはスキップされます。
- バックアップに選択されたすべてのファイルのノータリゼーションを有効にするには、**[ノータリゼーション]** スイッチをオンにします。ノータリゼーションの詳細については、「ノータリゼーション」を参照してください。

共有ドライブおよび共有ドライブファイルを復元

共有ドライブ全体を復元

1. **Google Workspace**をクリックします。
2. Cyber Protectionサービスに複数のGoogle Workspace組織を追加している場合は、バックアップされたデータをリカバリする組織を選択します。それ以外の場合は、この手順をスキップします。
3. **[共有ドライブ]** ノードを展開し、**[すべての共有ドライブ]** を選択し、復元する共有ドライブを選択し、**[復元]** をクリックします。

   共有ドライブが削除されている場合は、[バックアップストレージ] タブの **[クラウドアプリケーションバックアップ]** セクションでそのドライブを選択して、**[バックアップの表示]** をクリックします。

   共有ドライブを名前で検索できます。ワイルドカードはサポートされていません。
4. リカバリ ポイントを選択します。
5. **[復元]** > **[共有ドライブ全体]** の順にクリックします。
6. Cyber Protectionサービスに複数のGoogle Workspace組織が追加されている場合は、**[Google Workspace組織]** をクリックして、ターゲット組織の表示、変更、または指定を行います。

   デフォルトでは、元の組織が選択されます。この組織がCyber Protectionサービスに現在登録されていない場合は、利用可能な登録済みの組織の中から、新しいターゲット組織を選択する必要があります。
7. **[ドライブに復元]** で、ターゲット共有ドライブまたはターゲットユーザーを表示、変更、または指定します。ユーザーを指定すると、データはそのユーザーのGoogle ドライブへ復元されます。

   デフォルトでは、元の共有ドライブが選択されます。この共有ドライブが存在しないか、元と異なる組織が選択されている場合は、ターゲット共有ドライブまたはターゲットユーザーを指定する必要があります。
8. ファイルの共有権限を復元するかどうかを選択します。
9. **[復元を開始]** をクリックします。

10. 次のいずれかの上書きオプションを選択します。

オプション	説明
[既存のファイルが古い場合は上書きする]	保存先のロケーションに同じ名前のファイルがあり、それがソースファイルより古い場合、ソースファイルは以前のバージョンと置き換えられて保存先のロケーションに保存されます。
[既存のファイルを上書きする]	最終更新日に関係なく、保存先のロケーションにある既存のファイルはすべて上書きされます。
[既存のファイルを上書きしない]	保存先のロケーションに同じ名前のファイルがある場合、そのファイルには変更は適用されず、ソースファイルは保存先のロケーションに保存されません。

11. **[続行]** をクリックして、操作を確定します。

共有ドライブファイルを復元

1. **Google Workspace**をクリックします。
2. Cyber Protectionサービスに複数のGoogle Workspace組織を追加している場合は、バックアップされたデータをリカバリする組織を選択します。それ以外の場合は、この手順をスキップします。
3. **[共有ドライブ]** ノードを展開し、**[すべての共有ドライブ]** を選択し、復元するファイルが元々存在していた共有ドライブを選択し、**[復元]** をクリックします。
   共有ドライブが削除されている場合は、[バックアップストレージ] タブの **[クラウドアプリケーションバックアップ]** セクションでそのドライブを選択して、**[バックアップの表示]** をクリックします。
   共有ドライブを名前で検索できます。ワイルドカードはサポートされていません。
4. リカバリ ポイントを選択します。
5. **[復元]** > **[ファイル/フォルダ]** の順にクリックします。
6. 目的のフォルダを直接参照するか、検索を使用して目的のファイルとフォルダの一覧を取得します。
7. 復元するファイルを選択します。
   バックアップが暗号化されておらず、1つのファイルを選択した場合、**[バージョンを表示]** をクリックして、復元するファイルのバージョンを選択できます。選択した復元ポイントより前または後の、任意のバックアップバージョンを選択できます。
8. ファイルをダウンロードする場合は、そのファイルを選択し、**[ダウンロード]** をクリックし、ファイルの保存先を選択して、**[保存]** をクリックします。それ以外の場合は、この手順をスキップします。
9. **[復元]** をクリックします。
10. Cyber Protectionサービスに複数のGoogle Workspace組織が追加されている場合は、**[Google Workspace組織]** をクリックして、ターゲット組織の表示、変更、または指定を行います。
    デフォルトでは、元の組織が選択されます。この組織がCyber Protectionサービスに現在登録されていない場合は、利用可能な登録済みの組織の中から、新しいターゲット組織を選択する必要があります。
11. **[ドライブに復元]** で、ターゲット共有ドライブまたはターゲットユーザーを表示、変更、または指定します。ユーザーを指定すると、データはそのユーザーのGoogle ドライブへ復元されます。

デフォルトでは、元の共有ドライブが選択されます。この共有ドライブが存在しないか、元と異なる組織が選択されている場合は、ターゲット共有ドライブまたはターゲットユーザーを指定する必要があります。

12. **[パス]** で、ターゲット共有ドライブドライブまたはターゲットユーザーのGoogleドライブにあるターゲットフォルダを表示または変更します。デフォルトでは、元のロケーションが選択されます。
13. ファイルの共有権限を復元するかどうかを選択します。
14. **[復元を開始]** をクリックします。
15. 次のいずれかのファイル上書きオプションを選択します。

オプション	説明
[既存のファイルが古い場合は上書きする]	保存先のロケーションに同じ名前のファイルがあり、それがソースファイルより古い場合、ソースファイルは以前のバージョンと置き換えられて保存先のロケーションに保存されます。
[既存のファイルを上書きする]	最終更新日に関係なく、保存先のロケーションにある既存のファイルはすべて上書きされます。
[既存のファイルを上書きしない]	保存先のロケーションに同じ名前のファイルがある場合、そのファイルには変更は適用されず、ソースファイルは保存先のロケーションに保存されません。

16. **[続行]** をクリックして、操作を確定します。

ノータリゼーション

ノータリゼーションでは、ファイルが本物であり、バックアップ後に改変されていないことを証明できます。法律関係の文書のファイルやその他の非改ざん性の証明が必要なファイルをバックアップする際に、ノータリゼーションを有効にすることを推奨します。

ノータリゼーションは、GoogleドライブのファイルおよびGoogle Workspace共有ドライブのファイルのバックアップに対してのみ利用可能です。

ノータリゼーションの使用方法

バックアップに選択されたすべてのファイルのノータリゼーションを有効にするには、保護計画作成時に **[ノータリゼーション]** スイッチをオンにします。

復元を設定する場合、ノータライズ（公証）されたファイルには特別なアイコンが付き、ファイルの非改ざん性をベリファイできます。

仕組み

バックアップ中に、エージェントはバックアップされるファイルのハッシュコードを計算します。ハッシュツリーを作成（フォルダ構造に基づく）して、バックアップに保存し、ハッシュツリーのルートをノータリー（公証）サービスに送信します。ノータリー（公証）サービスで、ハッシュツリーのルートが Ethereum ブロックチェーンデータベースに保存され、この値が変更されていないことが確認されます。

ファイルの非改ざん性をベリファイする場合、エージェントはファイルのハッシュを計算し、それをバックアップ内のハッシュツリーに保存されているハッシュと比較します。これらのハッシュが一致しない場合、ファイルは本物ではないと見なされます。一致する場合は、ハッシュツリーによってファイルの非改ざん性が保証されます。

ハッシュツリー自身が不正なものではないことをベリファイするために、エージェントはハッシュツリーのルートをノータリー（公証）サービスに送信します。ノータリー（公証）サービスはそれをブロックチェーンデータベースに保存されているものと比較します。ハッシュが一致すると、選択したファイルが本物であることが保証されます。一致しない場合は、ファイルが本物ではないというメッセージが表示されます。

Notaryサービスを使用したファイル真正性のベリファイ

バックアップ中のノータリゼーションが有効になっている場合は、バックアップされたファイルの非改ざん性をベリファイできます。

ファイルの真正性をベリファイするには

1. 次のいずれかを実行します。
   - Google ドライブのファイルの真正性をベリファイするには、「Google ドライブのファイルを復元」セクションの手順1〜7の説明に従って、ファイルを選択します。
   - Google Workspace共有ドライブのファイルの真正性をベリファイするには、「共有ドライブのファイルを復元」セクションの手順1〜7の説明に従って、ファイルを選択します。
2. 選択したファイルに  アイコンが付いていることを確認します。これは、ファイルが認証済みであることを表しています。
3. 次のいずれかを実行します。
   - **[ベリファイ]** をクリックします。
     ファイルの非改ざん性がチェックされ、結果が表示されます。
   - **[証明書の取得]** をクリックします。
     Web ブラウザウィンドウで、ファイルのノータリゼーションを確認する証明書が開きます。ウィンドウには、ファイルの非改ざん性を手動でベリファイする手順も表示されます。

クラウドツークラウドバックアップで検索

データをリカバリする際、バックアップアーカイブを参照する代わりに、特定のバックアップ済みアイテムを検索することができます。

暗号化されていないバックアップの場合、常に検索を利用できます。強力な（インデックスベースの）検索機能のみがサポートされています。

インデックスベースの検索はより高速で、バックアップされた項目のバージョンの表示、添付ファイル名の検索、Gmailバックアップのフルテキストの検索など、追加のオプションが提供されます。

暗号化されたバックアップでは、強力な（インデックスベースの）検索機能も有効にすることができます。強化検索を有効にしない場合でも、Microsoft 365メールボックスのバックアップに対する基本的な検索は利用可能です。その他のすべてのワークロードに対する検索は、利用できません。

以下の表は、暗号化されたバックアップで利用可能なオプションをまとめたものです。

ワークロードの種類	復元元	強力な検索機能は無効化されています	強力な検索機能は有効化されています
Microsoft 365ワークロード			
メールボックス	メールメッセージ	基本的な（インデックスベースでない）検索が利用可能です	強力な（インデックスベースの）検索機能が利用可能です
OneDrive	ファイル/フォルダ	検索は利用できません	強力な（インデックスベースの）検索機能が利用可能です
SharePointサイト	SharePointのファイル	検索は利用できません	強力な（インデックスベースの）検索機能が利用可能です
Teams	チャネル	検索は利用できません	強力な（インデックスベースの）検索機能が利用可能です
	メールメッセージ	基本的な（インデックスベースでない）検索が利用可能です	強力な（インデックスベースの）検索機能が利用可能です
	チームサイト	検索は利用できません	強力な（インデックスベースの）検索機能が利用可能です
Google Workspaceワークロード			
メールボックス	メールメッセージ	検索は利用できません	強力な（インデックスベースの）検索機能が利用可能です
Google Drive	ファイル/フォルダ	検索は利用できません	強力な（インデックスベースの）検索機能が利用可能です
共有ドライブ	ファイル/フォルダ	検索は利用できません	強力な（インデックスベースの）検索機能が利用可能です

全文検索

全文テキストの検索は、Gmailのバックアップにのみ利用可能で、デフォルトで有効になっています。これにより、バックアップされたEメールの本文内を検索することができます。このオプションが無効になっている場合、件名、送信者、受信者、日付でのみ検索可能です。

全文テキストの検索インデックスが占有するストレージスペースは、Gmailのバックアップで使用されるストレージスペースの10～30%に及びます。全文テキスト検索データを含まないインデックスのサイズは、大幅に小さくなります。ストレージスペースを節約するために、全文テキストの検索を無効にし、インデックスの全文テキスト検索データが含まれる部分を消去できます。

検索インデックス

検索インデックスにより、クラウドツークラウドバックアップアーカイブにおける強力な検索機能が利用できます。

各バックアップ操作の後に、アーカイブに対して自動的にインデックス付けが実行されます。インデックス付けとバックアップは異なるソフトウェアコンポーネントによって実行されるため、インデックス付けの処理が、バックアップの作成速度に影響を与えることはありません。

インデックス付けの処理が完了した後、検索結果を表示できるようになります。これには最大24時間かかる場合があります。通常、 最初のバックアップ（フルバックアップ）のインデックス付けには、後続の増分バックアップのインデックス付けよりも時間がかかります。

すべてのインデックスには、件名、送信者、受信者、または日付による検索など、主要な検索機能をサポートするメタデータが含まれています。フルテキストの検索が有効になっている場合、Gmailバックアップ向けのインデックスには追加のデータが含められます。

検索インデックスのサイズを確認する

検索インデックスのサイズは時間の計画とともに大きくなります。フルテキストの検索が有効になっているバックアップアーカイブのインデックスは、最大でアーカイブサイズの30パーセントを占める可能性があります。

検索インデックスのサイズを確認するには

1. 管理者としてCyber Protectコンソールにログインします。
2. [**バックアップストレージ**] タブで、[**クラウドアプリケーションのバックアップ**] をクリックします。
3. **インデックスサイズ**列の値を確認します。

インデックスのアップデート、再構築、または削除

クラウドツークラウドバックアップの検索関連の問題をトラブルシュートするために、検索インデックスをアップデート、再構築、または削除できます。

注意
インデックスをアップデート、再構築、または削除する前に、サポートチームに連絡することをお勧めします。

インデックスをアップデート、再構築、または削除するには

1. Cyber Protectコンソールに管理者としてログインします。
2. [**バックアップストレージ**] タブで、[**クラウドアプリケーションのバックアップ**] をクリックします。
   アップデート、再構築、または削除するインデックスのアーカイブを選択します。
   これらの操作が利用できるかどうかは、以下のように管理者レベルとロールに依存します。

アカウントレベル	ロール	インデックスのアップデートが可能	インデックスの再構築が可能	インデックスの削除が可能
パートナーテナント	企業管理者	+	+	+
	サイバー管理者の保護	+	-	-
	管理者の保護	+	-	-
	読み取り専用管理者の保護	-	-	-
カスタマーテナント	企業管理者	+	-	-
	管理者の保護	+	-	-
	読み取り専用管理者の保護	-	-	-
ユニット	部署管理者	+	-	-
	管理者の保護	+	-	-
	読み取り専用管理者の保護	-	-	-

3. **[操作]** ペインで、実行する操作を選択します。
   - **インデックスのアップデート** - アーカイブ内の復元ポイントが確認され、不足しているインデックスが追加されます。
   - **インデックスの再構築** - アーカイブ内のすべての復元ポイントのインデックスが削除され、その後、インデックスが再度作成されます。
   - **インデックスの削除** - アーカイブ内のすべての復元ポイントのインデックスが削除されます。
4. （暗号化されたアーカイブの場合）暗号化パスワードを指定してから、**[OK]** をクリックしてください。
5. 操作のスコープを選択してから、**[OK]** をクリックします。
   アーカイブと選択された操作に応じて、以下のオプション（複数可）が利用可能です。
   - **メタデータのみ**
   - **コンテンツのみ**
   - **メタデータとコンテンツ検索**

暗号化済みバックアップで、強力な検索機能を許可する

暗号化されたクラウドツークラウドバックアップのバックアップ計画を作成する際には、強力な（インデックスベースの）検索機能を有効にできます。

強力な検索機能を有効にしない場合、Microsoft 365のメールボックスのバックアップに対して、基本検索機能を利用できます。他のすべてのワークロードでは、検索を利用できません。利用可能なオプションの詳細については、"クラウドツークラウドバックアップで検索"（645ページ）を参照してください。

注意
この機能は選択されたデータセンターで利用可能であり、すべてのカスタマーが利用できるわけではありません。

暗号化されたバックアップでの検索を有効にするには

1. バックアップ計画を作成する際に、**[暗号化]** スイッチを有効にします。
2. 暗号化パスワードを指定して確認します。
3. **[暗号化済みバックアップで、強力な検索を許可]** チェックボックスを選択します。
4. **[完了]** をクリックします。

注意
後から暗号化を無効にしたり、暗号化パスワードを変更したりすることはできません。暗号化されていないバックアップを作成したり、暗号化パスワードを変更したりするには、新しいバックアップ計画を作成します。

既存の計画で強力な検索機能を有効または無効にする

既存の暗号化バックアップの計画を編集して、強力な（インデックスベースの）検索機能を有効または無効にできます。

強力な検索機能を有効にしない場合、Microsoft 365のメールボックスのバックアップに対して、基本検索機能を利用できます。他のすべてのワークロードでは、検索を利用できません。利用可能なオプションの詳細については、"クラウドツークラウドバックアップで検索"（645ページ）を参照してください。

暗号化されていないバックアップでは、強力な検索機能を常に利用できます。このオプションを無効にすることはできません。

暗号化されたバックアップで強力な検索機能を有効または無効にするには

1. 暗号化が有効になっているバックアップ計画を編集するには、右上隅のギアアイコンをクリックします。
2. **[検索オプション]** タブで、必要に応じてスイッチを切り替えます。
3. **[完了]** をクリックします。
4. **[設定を保存]** をクリックします。

注意
強力な検索機能を再度有効にすると、このバックアップ計画で作成されたすべてのアーカイブが再度インデックス付けされます。この処理には時間がかかります。

Gmailバックアップのフルテキスト検索を無効にする

全文テキストの検索は、Gmailのバックアップにのみ利用可能で、デフォルトで有効になっています。これにより、バックアップされたEメールの本文内を検索することができます。このオプションが無効になっている場合、件名、送信者、受信者、日付でのみ検索可能です。

検索インデックスのサイズを最小限に抑える必要がある場合、フルテキストの検索を無効にすることをお勧めします。

フルテキストの検索を無効にするには

1. バックアップ計画を作成または編集するときは、右上隅のギアアイコンをクリックします。
2. **[フルテキストの検索]** タブで、スイッチを無効にします。
3. **[完了]** をクリックします。
4. （計画を作成する場合）**[適用]** をクリックします。
5. （計画を編集する場合）**[設定を保存]** をクリックします。

注意
フルテキストの検索を再度有効にすると、このバックアップ計画で作成されたすべてのアーカイブが再度インデックス付けされます。この処理には時間がかかります。

Oracle データベースの保護

注意
この機能は、Advanced Backupパックで利用可能です。

Oracleデータベースの保護については、https://dl.managed-protection.com/u/pdf/OracleBackup_whitepaper_en-US.pdfで入手できる個別の文書に記載されています

SAP HANA の保護

注意
この機能は、Advanced Backupパックで利用可能です。

SAP HANAの保護については、https://dl.managed-protection.com/u/pdf/SAP_HANA_backup_whitepaper_en-US.pdfで入手できる個別の文書に記載されています

MySQLおよびMariaDBデータを保護する

アプリケーション認識型バックアップで、MySQLやMariaDBのデータを保護できます。アプリケーションのメタデータを収集し、インスタンス、データベース、テーブルの各レベルで粒度復元を可能にします。

注意
MySQLまたはMariaDBデータのアプリケーション認識型バックアップは、Advanced Backup Packで利用可能です。

MySQLまたはMariaDBインスタンスが動作する物理マシンまたは仮想マシンをアプリケーション認識型バックアップで保護するには、これらのマシンにMySQL/MariaDBエージェントをインストールする必要があります。MySQL/MariaDBエージェントはLinuxエージェント（64ビット）にバンドルされている

ため、64-bitのLinuxベースのオペレーティングシステムにのみインストールできます。["サポートされるオペレーティング システムと環境"（23ページ）]をご覧ください。

Linuxエージェント（64ビット）のインストールファイルをダウンロードするには

1. Cyber Protectコンソールにログインします。
2. 右上にあるアカウントアイコンをクリックしてから、**[ダウンロード]** を選択します。
3. **[Linuxエージェント（64ビット）]** をクリックします。

インストールファイルが現在のマシンにダウンロードされます。エージェントをインストールするには、「"Linuxでプロテクションエージェントをインストールする"（79ページ）」または「"Linux での無人インストールまたはインストール解除"（103ページ）」で説明されている手順を実行します。オプションコンポーネントである [MySQL/MariaDBエージェント] が選択されていることを確認してください。

データベースとテーブルを稼働中のインスタンスにリカバリするには、MySQL/MariaDBエージェントを動作させるための一時ストレージが必要です。デフォルトでは、`/tmp`ディレクトリが使用されます。このディレクトリは、`ACRONIS_MYSQL_RESTORE_DIR`環境変数の設定で変更できます。

制限事項

- MySQL/MariaDBクラスターはサポート対象外です。
- Dockerコンテナで実行中のMySQL/MariaDBインスタンスは、サポート対象外です。
- BTRFSファイルシステムを使用するオペレーティングシステム上で実行中のMySQL/MariaDBインスタンスは、サポート対象外です。
- システムデータベース（`sys`、`mysql`、`information-schema`、`performance_schema`）とテーブルを含まないデータベースは、稼働中のインスタンスにリカバリできません。ただしこれらのデータベースは、インスタンス全体を復元する際にファイルとして復元できます。
- バックアップしたインスタンスと同一またはそれ以降のバージョンのターゲットインスタンスに対する復元のみが、サポートされます。ただし、以下の制約があります。
  - MySQL 5.xインスタンスからMySQL 8.xインスタンスへの復元はサポートされていません。
  - MySQL 5.x（マイナーバージョンを含む）以降のバージョンへの復元は、インスタンス全体をファイルとして復元する場合のみサポートされます。復元を実行する前に、ターゲットバージョンの公式MySQLアップグレードガイド（『MySQL 5.7アップグレードガイド』など）を参照してください。
- Secure Zoneに保存されたバックアップからの復元はサポートされていません。
- AppArmorがインストールされているマシン上で動作するMySQL/MariaDBエージェントでは、データベースおよびテーブルを復元することはできません。インスタンスをファイルとして復元すること、またはマシン全体を復元することは可能です。
- シンボリックリンクで構成されたターゲットデータベースへの復元はサポートされていません。バックアップされたデータベースは、名前を変えて新しいデータベースとしてリカバリすることができます。

既知の問題

パスワードで保護されたSamba共有からデータをリカバリする際に問題が発生する場合、Cyber Protectコンソールからログアウトし、ログインし直してください。復元ポイントを選択して、**[MySQL/MariaDBデータベース]** をクリックします。**[マシン全体]** または **[ファイル/フォルダ]** をクリックしないでください。

アプリケーション認識型バックアップを構成する

前提条件

- 選択したマシン上で、少なくとも1つのMySQLインスタンスまたはMariaDBインスタンスが動作していなければなりません。
- MySQLまたはMariaDBインスタンスが動作しているマシン上で、rootユーザーとしてプロテクションエージェントを起動する必要があります。
- アプリケーション認識型バックアップは、保護計画のバックアップ元に **[マシン全体]** が選択されている場合にのみ利用可能です。
- **[セクタ単位]** バックアップオプションは、保護計画で無効にする必要があります。そうでない場合、アプリケーションのデータをリカバリできません。

アプリケーション認識型バックアップを構成するには

1. Cyber Protectコンソールで、MySQLまたはMariaDBインスタンスが動作している1台または複数のマシンを選択します。
   各マシンで、1つまたは複数のインスタンスを動作させることができます。
2. バックアップモジュールを有効にした保護計画を作成します。
3. **[バックアップの対象]** で **[マシン全体]** を選択します。
4. **[アプリケーションバックアップ]** をクリックし、**[MySQL/MariaDB Server]** の横にあるスイッチを有効にします。
5. MySQLまたはMariaDBインスタンスを指定する方法を選択します。
   - **すべてのワークロードを許可**
     このオプションは、複数のサーバーで同一構成のインスタンスを実行する場合に使用します。すべてのインスタンスで同じ接続パラメータとアクセス認証が使用されます。
   - **特定のワークロード向け**
     このオプションを使用して、各インスタンスの接続パラメータとアクセス認証を指定します。
6. **[インスタンスを追加]** をクリックして、接続パラメータとアクセス認証を指定します。
   a. 接続タイプを選択し、以下を指定します。
      - （TCPソケットの場合）IPアドレスとポート。
      - （Unixソケットの場合）ソケットパス。
   b. インスタンスに対して以下の権限を持つユーザーアカウントの資格情報を指定します。
      - すべてのデータベースおよびテーブル（*.*）に対応するFLUSH_TABLESまたはRELOAD

- `information_schema.tables`の`SELECT`

c. **[OK]** をクリックします。

7. **[完了]** をクリックします。

アプリケーション認識型バックアップからデータを復元する

アプリケーション認識型バックアップから、MySQL/MariaDBのインスタンス、データベース、およびテーブルをリカバリすることができます。また、インスタンスが動作しているサーバー全体や、このサーバーのファイル/フォルダをリカバリすることもできます。

すべての復元オプションを以下の表にまとめて掲載します。

復元元	復元:	復元先
MySQLサーバー MariaDBサーバー	コンピュータ全体	Linuxエージェントがインストールされているマシン*
MySQLサーバー MariaDBサーバー	ファイルとフォルダ	Linuxエージェントがインストールされているマシン*
インスタンス	ファイル	MySQL/MariaDBエージェントがインストールされているマシン*
データベース	同じデータベース 新しいデータベース	MySQL/MariaDBエージェントがインストールされているマシン* • 元のインスタンス • 別のインスタンス • 元のデータベース • 新しいデータベース
テーブル	同じテーブル 新しいテーブル	MySQL/MariaDBエージェントがインストールされているマシン* • 元のインスタンス • 別のインスタンス • 元のデータベース • 元のテーブル • 新しいテーブル

*エージェントがインストールされている仮想マシンは、バックアップの観点から物理マシンとして扱われます。

サーバー全体を復元する

MySQL/MariaDBインスタンスが動作しているサーバー全体をリカバリする方法については、「"マシンの復元"（488ページ）」を参照してください。

インスタンスを復元する

アプリケーション認識型バックアップから、MySQL/MariaDBのインスタンスをファイルとしてリカバリすることができます。

インスタンスをリカバリするには

1. Cyber Protectコンソールで、リカバリ対象のデータが存在していた元のマシンを選択します。
2. **[復元]** をクリックします。
3. リカバリ ポイントを選択します。復元ポイントは、保存場所でフィルタされます。

   コンピュータがオフラインになっている場合、リカバリ ポイントは表示されません。次のいずれかを実行します。

   - バックアップのロケーションがクラウドまたは共有ストレージである（つまり、他のエージェントからアクセスできる）場合は、**[マシンを選択]** をクリックして、MySQL/MariaDBエージェントを含むオンラインのマシンを選択してから、復元ポイントを選択します。
   - **[バックアップストレージ]** タブで復元ポイントを選択します。

   上記のアクションのいずれかで参照用に選択されたマシンは、復元のターゲットマシンになります。
4. **[復元]** >**[MySQL/MariaDBデータベース]** の順にクリックします。
5. 復元するインスタンスを選択してから、**[ファイルとして復元]** をクリックします。
6. **[パス]** で、ファイルの復元先となるディレクトリを選択します。
7. **[復元を開始]** をクリックします。

データベースを復元する

アプリケーション認識型バックアップから、稼働中のMySQL/MariaDBインスタンスにデータベースをリカバリすることができます。

1. Cyber Protectコンソールで、リカバリ対象のデータが存在していた元のマシンを選択します。
2. **[復元]** をクリックします。
3. リカバリ ポイントを選択します。復元ポイントは、保存場所でフィルタされます。

   コンピュータがオフラインになっている場合、リカバリ ポイントは表示されません。次のいずれかを実行します。

   - バックアップのロケーションがクラウドまたは共有ストレージである（つまり、他のエージェントからアクセスできる）場合は、**[マシンを選択]** をクリックして、MySQL/MariaDBエージェントを含むオンラインのマシンを選択してから、復元ポイントを選択します。
   - **[バックアップストレージ]** タブで復元ポイントを選択します。

   上記のアクションのいずれかで参照用に選択されたマシンは、復元のターゲットマシンになります。
4. **[復元]** >**[MySQL/MariaDBデータベース]** の順にクリックします。
5. 任意のインスタンスの名前をクリックすると、そのデータベースの詳細を参照できます。
6. リカバリ対象である、1つまたは複数のデータベースを選択します。
7. **[復元]** をクリックします。
8. **[ターゲットMySQL/MariaDBインスタンス]** をクリックし、ターゲットインスタンスの接続パラメータとアクセス認証を指定します。

- データのリカバリ先のインスタンスを確認します。デフォルトでは、元のインスタンスが選択されます。
- ターゲットインスタンスにアクセスできるユーザーアカウントの資格情報を指定します。このユーザーアカウントには、すべてのデータベースおよびテーブル（*.*）に対応する、以下の権限を割り当てる必要があります。
  - INSERT
  - CREATE
  - DROP
  - LOCK_TABLES
  - ALTER
  - SELECT
- **[OK]** をクリックします。

9. ターゲットデータベースを確認します。

   デフォルトでは、元のデータベースが選択されています。

   新しいデータベースとしてリカバリする場合は、ターゲットデータベースの名前をクリックして、変更します。この操作は、単一のデータベースをリカバリする場合にのみ有効です。
10. **[既存のデータベースを上書き]** 以下の、上書きモードを選択します。

    デフォルトでは、上書きが有効になっており、バックアップされたデータベースが、同じ名前のターゲットデータベースと置き換えられます。

    上書きが無効になっている場合、バックアップされたデータベースは復元操作中にスキップされ、同じ名前のターゲットデータベースと置き換えられることはありません。
11. **[復元を開始]** をクリックします。

ファイルを復元する

アプリケーション認識型バックアップから、稼働中のMySQL/MariaDBインスタンスにテーブルをリカバリすることができます。

1. Cyber Protectコンソールで、リカバリ対象のデータが存在していた元のマシンを選択します。
2. **[復元]** をクリックします。
3. リカバリ ポイントを選択します。復元ポイントは、保存場所でフィルタされます。

   コンピュータがオフラインになっている場合、リカバリ ポイントは表示されません。次のいずれかを実行します。
   - バックアップのロケーションがクラウドまたは共有ストレージである（つまり、他のエージェントからアクセスできる）場合は、**[マシンを選択]** をクリックして、MySQL/MariaDBエージェントを含むオンラインのマシンを選択してから、復元ポイントを選択します。
   - **[バックアップストレージ]** タブで復元ポイントを選択します。

   上記のアクションのいずれかで参照用に選択されたマシンは、復元のターゲットマシンになります。
4. **[復元]** >**[MySQL/MariaDBデータベース]** の順にクリックします。
5. 任意のインスタンスの名前をクリックすると、そのデータベースの詳細を参照できます。
6. 任意のテーブルの名前をクリックすると、そのテーブルの詳細を参照できます。
7. リカバリ対象である、1つまたは複数のテーブルを選択します。

8. **[復元]** をクリックします。
9. **[ターゲットMySQL/MariaDBインスタンス]** をクリックし、ターゲットインスタンスの接続パラメータとアクセス認証を指定します。
   - データのリカバリ先のインスタンスを確認します。デフォルトでは、元のインスタンスが選択されます。
   - ターゲットインスタンスにアクセスできるユーザーアカウントの資格情報を指定します。このユーザーアカウントには、すべてのデータベースおよびテーブル（*.*）に対応する、以下の権限を割り当てる必要があります。
     - INSERT
     - CREATE
     - DROP
     - LOCK_TABLES
     - ALTER
     - SELECT
   - **[OK]** をクリックします。
10. ターゲットテーブルを確認します。

    デフォルトでは、元のテーブルが選択されています。

    新しいテーブルとしてリカバリする場合は、ターゲットのテーブルの名前をクリックして、変更します。この操作は、単一のテーブルをリカバリする場合にのみ有効です。
11. **[既存のテーブルを上書き]** 以下の、上書きモードを選択します。

    デフォルトでは、上書きが有効になっており、バックアップされたテーブルが、同じ名前のターゲットテーブルと置き換えられます。

    上書きが無効になっている場合、バックアップされたテーブルは復元操作中にスキップされ、同じ名前のターゲットテーブルと置き換えられることはありません。
12. **[復元を開始]** をクリックします。

保管済みルーチンのリカバリ

MySQLインスタンス全体をリカバリする場合、保管済みルーチンは自動的にリカバリされます。

個別のデータベースをオリジナルでないインスタンスにリカバリする場合、または新しいデータベースとしてリカバリする場合、保管済みルーチンは自動的にリカバリされません。保管済みルーチンをSQLファイルにエクスポートし、リカバリしたデータベースに追加することで、保管済みルーチンを手動でリカバリできます。

保管済みルーチンをエクスポートし、リカバリしたデータベースに追加するには

1. 元のMySQLインスタンスが存在するマシンで、ターミナルを開きます。
2. 以下のコマンドを実行して保管済みルーチンをエクスポートします。
3. ```
   mysqldump -p [source_database_name] --routines --no-create-info --no-data >
   [exported_db_routines.sql]
   ```
4. データベースをリカバリしたマシンで、MySQLコマンドラインクライアントを開きます。
   ```

5. 以下のコマンドを実行して、リカバリしたデータベースにルーチンを追加します。

```
mysql>  use [recovered_database_name];
```

```
mysql>  source [path_to_exported_db_routines.sql];
```

Webサイトとホスティングサーバーの保護

Web サイトの保護

不正なアクセスやマルウェア攻撃の結果、Webサイトが破損する可能性があります。破損した際に簡単に元の状態に戻したい場合、Webサイトをバックアップします。

Webサイトをバックアップするために必要なものは何でしょうか。

Webサイトは、SFTPまたはSSHプロトコルを介してアクセス可能でなければなりません。エージェントをインストールする必要はありません。このセクションで後述するように、Webサイトを追加するだけです。

どのアイテムをバックアップできますか。

次のアイテムをバックアップできます:

- **Webサイトコンテンツファイル**
  SFTPまたはSSH接続用に指定したアカウントからアクセスできるすべてのファイル。
- **MySQLサーバーでホストされているリンク済データベース（存在する場合）。**
  指定したMySQLアカウントにアクセスできるすべてのデータベース。

Webサイトでデータベースを使用している場合、ファイルとデータベースの両方をバックアップして、一貫性のある状態に復元することをおすすめします。

制限事項

- Webサイトのバックアップに使用できる唯一のバックアップロケーションはクラウドストレージです。
- 1つのWebサイトに複数の保護計画を適用することは可能ですが、スケジュール実行できるのはそのうち1つだけです。その他の計画は手動で開始する必要があります。
- 唯一利用可能なバックアップオプションは、「バックアップファイル名」です。
- Webサイト保護計画は、**[管理]** > **[保護計画]** タブに表示されません。

Webサイトのバックアップ

Web サイトを追加する

1. **[デバイス]** > **[追加]** をクリックします。
2. **[Webサイト]** をクリックします。

3. Webサイトの次のアクセス設定を設定します:
   - **[Webサイト名]** で、Webサイトの名前を作成して入力します。この名前はCyber Protectコンソールに表示されます。
   - **[ホスト]** で、SFTPまたはSSH経由でWebサイトにアクセスするために使用するホスト名またはIPアドレスを指定します。たとえば、`my.server.com`または`10.250.100.100`。
   - **[ポート]** で、ポート番号を指定します。
   - **[ユーザー名]** および **[パスワード]** で、SFTPまたはSSH経由でWebサイトにアクセスするために使用できるアカウントの資格情報を指定します。

     重要
     指定されたアカウントからアクセス可能なファイルのみがバックアップされます。

     パスワードの代わりに、SSH秘密鍵を指定することができます。これを行うには、**[パスワードの代わりにSSH秘密鍵を使用する]** チェックボックスをオンにして、鍵を指定します。
4. **[次へ]** をクリックします。
5. WebサイトがMySQLデータベースを使用している場合は、データベースのアクセス設定を設定します。それ以外の場合は **[スキップ]** をクリックします。
   a. **[接続タイプ]** で、クラウドからデータベースにアクセスする方法を選択します:
      - **ホストからSSH経由**: 手順3で指定したホスト経由でデータベースにアクセスします。
      - **直接接続**:データベースに直接アクセスします。この設定は、データベースがインターネットからアクセスできる場合にのみ選択します。
   b. **[ホスト]** で、MySQLサーバーが動作しているホストの名前またはIPアドレスを指定します。
   c. **[ポート]** で、サーバーへのTCP/IP接続ポート番号を指定します。デフォルトのポート番号は3306です。
   d. **[ユーザー名]** および **[パスワード]** で、MySQLアカウントの資格情報を指定します。

      重要
      指定されたアカウントからアクセス可能なデータベースのみがバックアップされます。

   e. **[作成]** をクリックします。

   Webサイトは、Cyber Protectコンソールの **[デバイス]** > **[Webサイト]** に表示されます。

接続の設定を変更するには

1. **[デバイス]** > **[Webサイト]** でWebサイトを選択します。
2. **[詳細]** をクリックします。
3. Webサイトまたはデータベース接続設定の横にある鉛筆アイコンをクリックします。
4. 必要な変更を実行し、**[保存]** をクリックします。

Webサイトの保護計画を作成する手順

1. **[デバイス]** > **[Web サイト]** で 1 つまたは複数の Web サイトを選択します。
2. **[保護]** をクリックします。
3. （オプション）データベースのバックアップを有効にします。

複数の Web サイトを選択した場合、データベースのバックアップはデフォルトで無効になります。

4. （オプション）保持ルールを変更します。
5. （オプション）バックアップの暗号化を有効にします。
6. （オプション）ギアアイコンをクリックして、**バックアップファイル名**オプションを編集します。これは、次の 2 つの場合に役立ちます。
   - この Web サイトを以前にバックアップしており、既存のバックアップシーケンスを継続する場合
   - **[バックアップストレージ]** タブにカスタム名を表示させる場合
7. **[適用]** をクリックします。

マシンに対するのと同じ方法で、Webサイトの保護計画の編集、取り消し、および削除を行えます。これらの操作については、「保護計画を使用した操作」で説明します。

Web サイトの復元

Webサイトを復元するには

1. 次のいずれかを実行します。
   - **[デバイス]** > **[Web サイト]** で、復元する Web サイトを選択してから、**[復元]** をクリックします。

     Webサイトを名前で検索できます。ワイルドカードはサポートされていません。
   - Webサイトが削除されている場合は、[バックアップストレージ] タブの **[クラウドアプリケーションバックアップ]** セクションでそのチームドライブを選択して、**[バックアップの表示]** をクリックします。

     削除済みの Web サイトを復元するには、ターゲットサイトをデバイスとして追加する必要があります。
2. リカバリ ポイントを選択します。
3. **[復元]** をクリックして、復元する対象を選択します:**Web サイト全体**、**データベース**（該当する場合）、または**ファイル/フォルダ**。

   Webサイトが一貫性のある状態になるように、ファイルとデータベースの両方を任意の順序でリカバリすることをお勧めします。
4. 選択に応じて、下記のいずれかの手順に従ってください。

Web サイト全体を復元するには

1. **[Web サイトに復元]** で、ターゲット Web サイトを表示または変更します。

   デフォルトでは、元の Web サイトが選択されます。元の Web サイトが存在しない場合、ターゲットの Web サイトを選択する必要があります。
2. 復元されたアイテムの共有権限を復元するかどうかを選択します。
3. **[復元を開始]** をクリックして操作を確定します。

データベースを復元するには

1. 復元するデータベースを選択します。
2. データベースをファイルとしてダウンロードする場合は、**[ダウンロード]** をクリックし、ファイルの保存先を選択して、**[保存]** をクリックします。それ以外の場合は、この手順をスキップします。

3. **[復元]** をクリックします。
4. **[Web サイトに復元]** で、ターゲット Web サイトを表示または変更します。
   デフォルトでは、元の Web サイトが選択されます。元の Web サイトが存在しない場合、ターゲットの Web サイトを選択する必要があります。
5. **[復元を開始]** をクリックして操作を確定します。

Webサイトのファイル/フォルダを復元するには

1. 復元するファイル/フォルダを選択します。
2. ファイルを保存する場合は、**[ダウンロード]** をクリックし、ファイルの保存先を選択して、**[保存]** をクリックします。それ以外の場合は、この手順をスキップします。
3. **[復元]** をクリックします。
4. **[Web サイトに復元]** で、ターゲット Web サイトを表示または変更します。
   デフォルトでは、元の Web サイトが選択されます。元の Web サイトが存在しない場合、ターゲットの Web サイトを選択する必要があります。
5. 復元されたアイテムの共有権限を復元するかどうかを選択します。
6. **[復元を開始]** をクリックして操作を確定します。

Webホスティングサーバーの保護

Plesk、cPanel、DirectAdmin、VirtualMin、またはISPManagerコントロールパネルを実行しているLinuxベースのWebホスティングサーバーを保護することができます。他ベンダーのWebホスティングコントロールパネルを実行するサーバーは、通常のワークロードとして保護されます。

制限値（クォータ）

Plesk、cPanel、DirectAdmin、VirtualMin、またはISPManagerコントロールパネルを実行しているサーバーは、Webホスティングサーバーと見なされます。バックアップされたWebホスティングサーバーは、それぞれ**Webホスティングサーバー**のクォータを消費します。このクォータが無効の場合やクォータの追加容量を超過した場合は、以下のようにクォータが割り当てられるか、バックアップが失敗することになります。

- 物理サーバーの場合、**サーバー**クォータが使用されます。このクォータが無効の場合、またはクォータの追加容量を超過した場合、バックアップは失敗します。
- 仮想サーバーの場合、**仮想マシン**クォータが使用されます。このクォータが無効の場合、またはクォータの追加容量を超過した場合、バックアップは失敗します。

DirectAdmin、cPanel、Pleskの統合

DirectAdmin、Plesk、cPanelを使用しているWebホスティング管理者は、これらのコントロールパネルをCyber Protectionサービスと統合することにより、以下に挙げるような強力な機能を利用できるようになります。

- ディスクレベルバックアップでWebホスティングサーバー全体をクラウドストレージにバックアップします。
- すべてのWebサイトやアカウントを含む、サーバー全体をリカバリする

- アカウント、Webサイト、個別のファイル、メールボックス、またはデータベースの粒度復元とダウンロードを実行する
- リセラーやカスタマーが自分のデータをセルフサービスで復元できるようにする

統合を実行するには、Cyber Protectionサービス拡張子を使用する必要があります。詳細については、対応する機能統合のガイドを参照してください。

- DirectAdmin統合ガイド
- WHMおよびcPanel統合ガイド
- Plesk統合ガイド

仮想コンピュータの特別な操作

バックアップからの仮想コンピュータの実行（インスタント復元）

オペレーティングシステムを含むディスクレベル バックアップから仮想コンピュータを実行できます。この処理はインスタント復元ともいい、数秒で仮想サーバーを実行できます。仮想ディスクはバックアップから直接エミュレートされるため、データストア（ストレージ）の領域を消費しません。記憶域スペースは、仮想ディスクに変更を保持する目的でのみ必要です。

この一時的な仮想マシンは、最大3日間稼動させておくことをお勧めします。その後、完全に削除するか、ダウンタイムなしで標準の仮想コンピュータ（確定）に変換できます。

一時仮想コンピュータが存在するかぎり、保持ルールをそのコンピュータで使用されるバックアップに適用できません。元のコンピュータのバックアップは実行し続けることができます。

使用例

- **災害復旧**
  障害があるコンピュータのコピーを即時にオンラインにします。
- **バックアップのテスト**
  バックアップからコンピュータを実行し、ゲストOSおよびアプリケーションが正しく機能していることを確認します。
- **アプリケーションデータへのアクセス**
  コンピュータの実行中に、アプリケーションのネイティブ管理ツールを使用して、必要なデータにアクセスして抽出します。

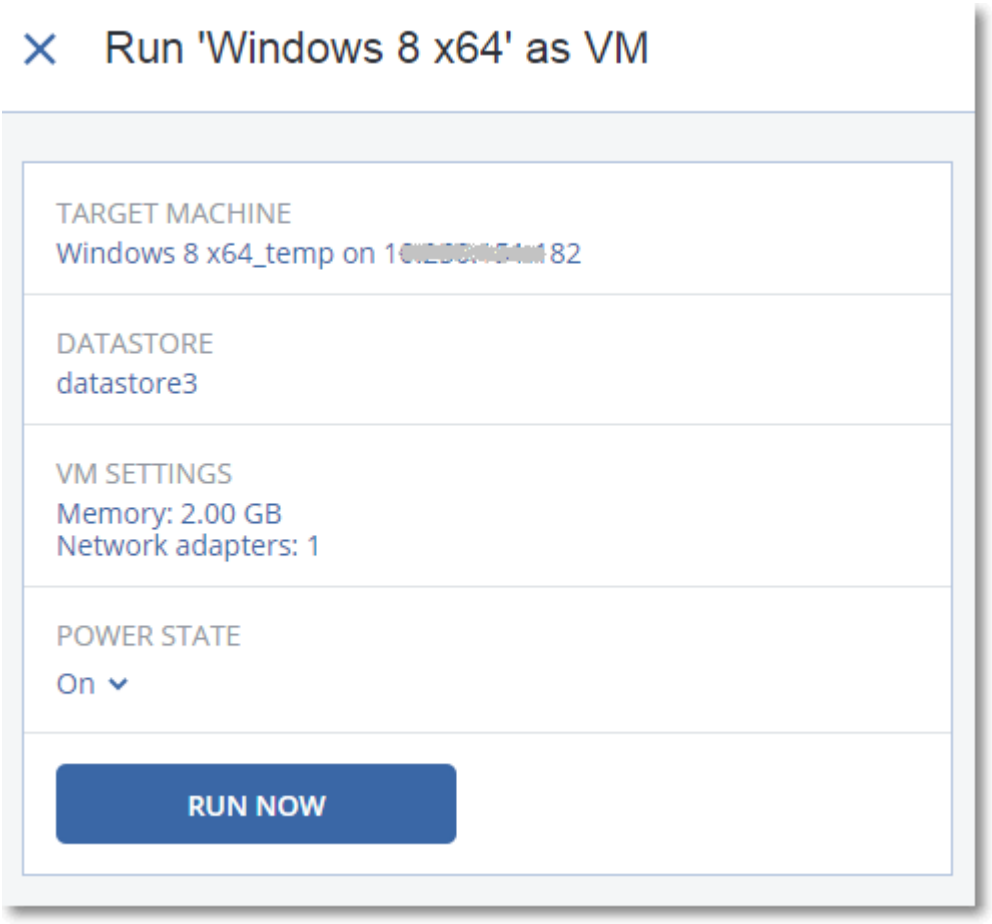
前提条件

- 1つまたは複数のVMwareエージェントまたはHyper-Vエージェントを Cyber Protectionサービスに登録する必要があります。
- バックアップは、ネットワークフォルダ、またはVMwareエージェントまたはHyper-Vエージェントがインストールされているコンピュータのローカル フォルダに保存することができます。ネットワークフォルダを選択する場合は、コンピュータからアクセスできる必要があります。仮想コンピュータは、クラウドストレージに格納されたバックアップから実行できますが、この操作では、バックアップから大量のランダムアクセス読み取りを行う必要があるため動作が遅くなります。

- バックアップにはコンピュータ全体またはオペレーティングシステムを起動するのに必要なすべてのボリュームを含める必要があります。
- 物理コンピュータと仮想コンピュータの両方のバックアップを使用できます。 Virtuozzo コンテナのバックアップは使用できません。
- Linux論理ボリューム（LVM）を含むバックアップは、VMwareエージェントまたはHyper-Vエージェントによって作成されたものであることが必要です。仮想マシンは元のマシンと同じタイプであることが必要です（ESXiまたはHyper-V）。

コンピュータの実行

1. 次のいずれかを実行します。
   - バックアップされたコンピュータを選択し、**[復元]** をクリックしてから、リカバリポイントを選択します。
   - [バックアップストレージ] タブで復元ポイントを選択します。
2. **[VMとして実行]**をクリックします。
   ホストと他の必要なパラメータが自動的に選択されます。



3. （オプション）**[ターゲットマシン]** をクリックし、仮想マシンタイプ（ESXiまたはHyper-V）、ホスト、仮想マシン名を変更します。
4. （オプション）**[データストア]**（ESXi）または **[パス]**（Hyper-V）をクリックしてから、仮想マシンのデータストアを選択します。

仮想ディスクの変更はコンピュータの実行中に累積されます。選択したデータストアに十分な空き領域があることを確認してください。これらの変更点を仮想マシンの常設化により保存することを計画している場合、本番でマシンを実行するのに適したデータストアを選択してください。

5. （オプション）**[VM設定]** をクリックして、仮想マシンのメモリサイズとネットワーク接続を変更します。
6. （オプション）VM電源状態（**オン**/**オフ**）を選択します。
7. **[今すぐ実行]** をクリックします。

結果として、マシンが  または 

アイコンと一緒にWebインターフェースに表示されます。このような仮想コンピュータはバックアップ用に選択できません。

注意
Microsoft Azureのバックアップで、「仮想マシンとして実行（インスタント復元）」処理を実行できます。ただし、この処理では大量の送信トラフィックが発生し、Microsoft Azureサブスクリプションの請求に追加されます。Microsoft AzureバックアップからWindowsマシンを実行する場合、仮想マシンの起動からログインまでに発生する一般的な送信トラフィックは、約5GBになります。

コンピュータの削除

vSphere/Hyper-Vで直接一時仮想マシンを削除しないことをお勧めします。これはWebインターフェイスのアーチファクトになる場合があります。また、コンピュータが実行されているバックアップがしばらくロックされた状態になる場合があります（保持ルールでは削除できません）。

バックアップから実行されている仮想コンピュータを削除するには

1. **[すべてのデバイス]** タブで、バックアップから実行するマシンを選択します。
2. **[削除]** をクリックします。

コンピュータはWebインターフェイスから削除されます。vSphereまたはHyper-Vインベントリおよびデータベース（ストレージ）からも削除されます。コンピュータの実行中にデータで行われたすべての変更は失われます。

コンピュータの確定

仮想コンピュータをバックアップから実行しているときには、仮想ディスクの内容がバックアップから直接取得されます。このため、バックアップロケーションまたは保護エージェントへの接続が失われると、マシンにアクセスできなくなったり、マシンが破損したりする場合があります。

このマシンを永久にすることができます。つまり、仮想ディスクのすべてとマシンの実行中に発生した変更をこれらの変更が保存されるデータストアに復元します。この処理は確定といいます。

確定はダウンタイムなしで実行されます。確定中は、仮想マシンの電源がオフになることはありません。

確定仮想ディスクのロケーションは、**[VMとして実行]** 操作（ESXiでは **[データストア]**、Hyper-Vでは **[パス]**）のパラメータで定義されます。確定を開始する前に、このデータストアの空き領域、共有機能、およびパフォーマンスが、本番環境でのマシンの実行に適していることを確認してください。

注意
Windows Server 2008/2008 R2およびMicrosoft Hyper-V Server 2008/2008 R2で実行されているHyper-Vについては、これらのバージョンのHyper-Vに必要なAPIがないため、確定はサポートされていません。

バックアップから実行されている仮想コンピュータを確定するには

1. **[すべてのデバイス]** タブで、バックアップから実行するマシンを選択します。
2. **[確定]** をクリックします。
3. （オプション）コンピュータの新しい名前を指定します。
4. （オプション）ディスクプロビジョニングモードを変更します。デフォルトの設定は **[Thin（シン）]** です。
5. **[確定]** をクリックします。

コンピュータ名はすぐに変更されます。復元の進行状況は **[アクティビティ]** タブに表示されます。復元が完了したら、コンピュータアイコンが標準仮想コンピュータのアイコンに変わります。

確定に関する注意点

確定と標準復元

確定プロセスは、以下の理由で標準復元より時間がかかります。

- 確定中、エージェントはバックアップのさまざまな部分へのランダムアクセスを実行します。マシン全体を復元するとき、エージェントはバックアップから順にデータを読み取ります。
- 確定中に仮想マシンが動作している場合、両方の処理を同時に維持するために、エージェントはより頻繁にバックアップからデータを読み取ります。標準復元中、仮想マシンは停止されます。

バックアップから実行しているマシンの確定

バックアップデータへの集中的なアクセスにより、終了処理の速度はバックアップロケーションとエージェントの間の接続帯域幅に大きく依存します。ローカルバックアップと比較して、クラウドに配置されたバックアップの確定には時間がかかります。インターネット接続が非常に遅いかまたは不安定な場合、クラウドバックアップから動作しているマシンの確定は失敗する場合があります。終了処理を実行する計画があり、選択できる場合は、仮想マシンをローカルバックアップから実行することをお勧めします。

注意
終了処理の速度は、エージェントがVMware ESXiホストまたはvCenterのどちらに接続されているかによって異なります（"仮想アプライアンスの設定"（133ページ）の手順3を参照）。VMware vCenterに接続すると、VMware APIの仕様により、終了処理が遅延する可能性があります。終了処理を高速化するには、**VMとして実行**処理に続いて、終了処理を実行するための別のVMwareエージェントを使用します。このエージェントは、vCenterではなくESXiホストに接続されます。

VMware vSphere での作業

このセクションでは、VMware vSphere環境特有の操作について説明します。

仮想コンピュータのレプリケーション

レプリケーションは、VMware ESXi仮想コンピュータでのみ可能です。

レプリケーションは、仮想コンピュータの厳密なコピー（レプリカ）を作成し、そのレプリカと元のコンピュータの同期を維持するプロセスです。重要な仮想コンピュータのレプリケーションにより、このコンピュータのコピーをいつでも開始できる状態で維持できます。

レプリケーションは、手動でまたは指定したスケジュールに従って開始できます。最初のレプリケーションはフル（コンピュータ全体をコピー）で実行されます。以後のレプリケーションは、このオプションが無効にされていない限り、すべて増分に対して [Changed Block Tracking] を使用して実行されます。

レプリケーションとバックアップ

スケジュール設定によるバックアップと異なり、レプリカは仮想コンピュータの最新状態のみを維持します。バックアップは比較的安価なストレージで維持できるのに対し、レプリカはデータストアのスペースを消費します。

ただし、レプリカの電源をオンにするための所要時間は、復元するよりもはるかに短く、仮想コンピュータをバックアップから実行するための所要時間と比べても短くなります。電源がオンになると、レプリカはバックアップから実行するVMよりも高速で機能し、VMwareエージェントをロードしません。

使用例

- **リモートサイトへの仮想マシンのレプリケーション。**
  プライマリサイトからセカンダリサイトに仮想コンピュータのクローンを作成することにより、レプリケーションを作成します。データセンターの一部または全部に障害が発生しても、このレプリケーションを使用して作業を継続できます。セカンダリサイトの設置施設は、通常、環境、インフラストラクチャなど、プライマリサイトの障害発生原因の影響を受けにくい、地理的に離れた場所に設置されます。
- **同じサイト内での仮想マシンのレプリケーション（ホスト間やデータストア間）。**
  オンサイトレプリケーションは可用性を高め、災害復旧のシナリオを成立させるために使用されます。

レプリカの用途

- **レプリカのテスト**

  テストのためにレプリカの電源をオンにします。vSphereクライアントなどのツールを使用して、レプリカが正しく機能することを確認します。テストの進行中は、レプリケーションは一時停止されます。
- **レプリカへのフェールオーバー**

  フェールオーバーは元の仮想コンピュータからレプリカへのシステムの移行です。フェールオーバーの進行中は、レプリケーションは一時停止されます。
- **レプリカのバックアップ**

  バックアップとレプリケーションの両方で仮想ディスクへのアクセスが必要となり、仮想コンピュータが実行しているホストのパフォーマンスに影響します。仮想コンピュータのレプリカとバックアップの両方が必要でも、本番ホストに余計な負荷をかけないようにするには、コンピュータのレプリケーション先を別のホストにし、レプリカのバックアップを設定します。

制限事項

- 以下のタイプの仮想コンピュータはレプリケーションができません。
  - ESXi 5.5以前で実行しているFault Toleranceが設定されたコンピュータ
  - バックアップから実行しているコンピュータ
  - 仮想コンピュータのレプリカ
- ESXiホストにネットワークインターフェイスカード（NIC）を追加したり、NICを取り外したりするなどのハードウェアの変更により、ホストの内部IDが変更されます。この変更は、VMのレプリケーション計画に影響します。このような変更後は、ESXiホストがレプリケーション元またはレプリケーション先として選択されている VMレプリケーション計画を再作成する必要があります。再作成しなかった場合、そのVMレプリケーション計画は失敗します。

レプリケーション計画の作成

レプリケーション計画は、コンピュータごとにそれぞれ作成する必要があります。既存の計画を他のコンピュータに適用することはできません。

レプリケーション計画の作成手順

1. レプリケーション対象の仮想コンピュータを選択します。
2. **[レプリケーション]** をクリックします。

   ソフトウェアには新しいレプリケーション計画テンプレートが表示されます。
3. （オプション）レプリケーション計画名を変更するには、デフォルト名をクリックします。
4. **[ターゲットマシン]** をクリックして、次の操作を行います。
   a. 新しいレプリカを作成するか、元のコンピュータの既存のレプリカを使用するかを選択します。
   b. ESXiホストを選択し、新しいレプリカ名を指定するか、既存のレプリカを選択します。

      新しいレプリカのデフォルトの名前は、**（元のマシン名）_replica**になります。
   c. **[OK]** をクリックします。

5. （新しいマシンにレプリケーションする場合のみ）[**データストア**] をクリックし、仮想マシンのデータストアを選択します。
6. （オプション）[**スケジュール**] をクリックして、レプリケーションスケジュールを変更します。
   デフォルトでは、レプリケーションは月曜日から金曜日まで毎日実行されます。レプリケーションを実行する時刻を選択できます。
   レプリケーションを頻繁に実行する場合、スライダを移動して、レプリケーションのスケジュールを指定できます。
   また、次の操作を実行することもできます。
   - スケジュールが有効となる日付範囲を設定できます。[**設定した期間内で実行する**] チェック ボックスをオンにして、日付範囲を指定します。
   - スケジュールを無効にします。この場合、レプリケーションを手動で起動できます。
7. （オプション）ギアアイコンをクリックして、レプリケーションオプションを変更します。
8. [**適用**] をクリックします。
9. （オプション）計画を手動で実行するには、計画パネルで [**今すぐ実行**] をクリックします。

レプリケーション計画を実行した結果として、[**すべてのデバイス**] リストに、仮想マシンのレプリカが次のアイコン付きで表示されます。 

レプリカのテスト

レプリカのテストの準備手順

1. テストするレプリカを選択します。
2. [**レプリカのテスト**] をクリックします。
3. [**テストの開始**] をクリックします。
4. 電源の投入されたレプリカをネットワークに接続するかどうかを選択します。デフォルトでは、レプリカはネットワークに接続されません。
5. （オプション）レプリカをネットワークに接続する選択をした場合は、レプリカの電源を投入する前に元のマシンを停止するために、[**元の仮想マシンを停止**] チェックボックスをオンにします。
6. [**開始**] をクリックします。

レプリカのテストを停止する手順

1. テストが進行中のレプリカを選択します。
2. [**レプリカのテスト**] をクリックします。
3. [**テストの停止**] をクリックします。
4. 操作を確定します。

レプリカへのフェールオーバー

コンピュータをレプリカにフェールオーバーする手順

1. フェールオーバー先となるレプリカを選択します。
2. [**レプリカの操作**] をクリックします。

3. **[フェールオーバー]** をクリックします。
4. 電源の投入されたレプリカをネットワークに接続するかどうかを選択します。デフォルトでは、レプリカは、元のコンピュータと同じネットワークに接続されます。
5. （オプション）レプリカをネットワークに接続するよう選択した場合は、元のマシンのオンライン接続を維持するために、**[元の仮想マシンの停止]** チェックボックスをオフにします。
6. **[開始]** をクリックします。

レプリカがフェールオーバー状態の間は、次のアクションのいずれかを選択できます。

- **フェールオーバーの停止**
  元のコンピュータが修復された場合、フェールオーバーを停止します。レプリカの電源がオフになります。レプリケーションが再開されます。
- **レプリカに対して永続的フェールオーバーを実行**
  このインスタント操作により、仮想コンピュータに対するレプリケーションができなくなるように、仮想コンピュータから「レプリカ」フラグが削除されます。レプリケーションを再開する場合は、レプリケーション計画を編集し、このコンピュータをソースとして選択します。
- **フェールバック**
  継続的に運用する予定のないサイトにフェールオーバーした場合、フェールバックを実行します。レプリカは、元の仮想コンピュータまたは新しい仮想コンピュータに復元されます。元のコンピュータに復元が完了すると、電源が投入され、レプリケーションが再開されます。新しいコンピュータへの復元を選択した場合は、レプリケーション計画を編集し、このコンピュータをソースとして選択します。

フェールオーバーの停止

フェールオーバーを停止する手順

1. フェールオーバー状態のレプリカを選択します。
2. **[レプリカの操作]** をクリックします。
3. **[フェールオーバーの停止]** をクリックします。
4. 操作を確定します。

永続的フェールオーバーの実行

永続的フェールオーバーの実行手順

1. フェールオーバー状態のレプリカを選択します。
2. **[レプリカの操作]** をクリックします。
3. **[永続的フェールオーバー]** をクリックします。
4. （オプション）仮想コンピュータの名前を変更します。
5. （オプション）**[元の仮想マシンの停止]** チェックボックスをオンにします。
6. **[開始]** をクリックします。

フェールバック

レプリカからフェールバックする手順

1. フェールオーバー状態のレプリカを選択します。
2. **[レプリカの操作]** をクリックします。
3. **[レプリカからのフェールバック]** をクリックします。
   このソフトウェアは自動的に対象コンピュータとして元のコンピュータを選択します。
4. （オプション）**[ターゲットマシン]** をクリックして、次の操作を行います。
   a. 新規または既存のコンピュータにフェールバックするかどうかを選択します。
   b. ESXiホストを選択し、新しいコンピュータ名を指定するか、既存のコンピュータを選択します。
   c. **[OK]** をクリックします。
5. （オプション）新しいコンピュータにフェールバックするときには、次を実行することもできます。
   - **[データストア]** をクリックして、仮想マシンのデータストアを選択します。
   - **[VM設定]** をクリックして、仮想マシンのメモリサイズ、プロセッサ数、ネットワーク接続を変更します。
6. （オプション）**[復元オプション]** をクリックしてフェールバックオプションを変更します。
7. **[復元を開始]** をクリックします。
8. 操作を確定します。

レプリケーションオプション

レプリケーションオプションを変更するには、レプリケーション計画名の横にあるギア アイコンをクリックし、**[レプリケーションオプション]** をクリックします。

Changed Block Tracking（CBT）

このオプションは、バックアップ オプション [Changed Block Tracking (CBT)] と同じ内容です。

ディスクプロビジョニング

このオプションでは、レプリカのディスクプロビジョニング設定を定義します。

デフォルト設定:**シンプロビジョニング**です。

次の値を使用できます。**[シンプロビジョニング]**、**[シックプロビジョニング]**、**[元の設定を維持]**。

エラー処理

このオプションは、バックアップ オプション [エラー処理] と同じ内容です。

処理の前後のコマンド

このオプションは、バックアップ オプション [処理の前後のコマンド] と同じ内容です。

仮想コンピュータのボリューム シャドウ コピー サービス（VSS）

このオプションは、バックアップ オプション [仮想コンピュータのボリューム シャドウ コピー サービス（VSS）] と同じ内容です。

フェールバック オプション

フェールバックオプションを変更するには、フェールバック設定時に **[復元オプション]** をクリックしてください。

エラー処理

このオプションは、復元オプション [エラー処理] と同じ内容です。

パフォーマンス

このオプションは、復元オプション [パフォーマンス] と同じ内容です。

処理の前後のコマンド

このオプションは、復元オプション [処理の前後のコマンド] と同じ内容です。

VMの電源管理

このオプションは、復元オプション [VM電源管理] と同じ内容です。

初期レプリカのシード

遠隔地へのレプリケーション速度を上げてネットワークの帯域幅を節約するために、レプリカのシーディングを実行できます。

重要
レプリカシードを実行するには、ターゲットESXiでVMwareエージェント（仮想アプライアンス）が実行されている必要があります。

初期レプリカのシード

1. 次のいずれかを実行します。
   - 元の仮想コンピュータをオフにできる場合は、オフにしてから、手順4に進みます。
   - 元の仮想コンピュータをオフにできない場合は、次の手順に進みます。
2. レプリケーション計画を作成します。
   計画を作成するときには、**[ターゲットマシン]** で **[新しいレプリカ]** および元のマシンをホストするESXiを選択します。
3. 計画を1回実行します。
   レプリカが元のESXiで作成されます。
4. 仮想コンピュータ（またはレプリカ）ファイルを外部ハードドライブにエクスポートします。
   a. vSphereクライアントが実行されているコンピュータに外部ハードドライブを接続します。
   b. vSphereクライアントを元のvCenter¥ESXiに接続します。
   c. インベントリで新しく作成されたレプリカを選択します。
   d. **[ファイル]** > **[エクスポート]** > **[OVFテンプレートのエクスポート]** をクリックします。

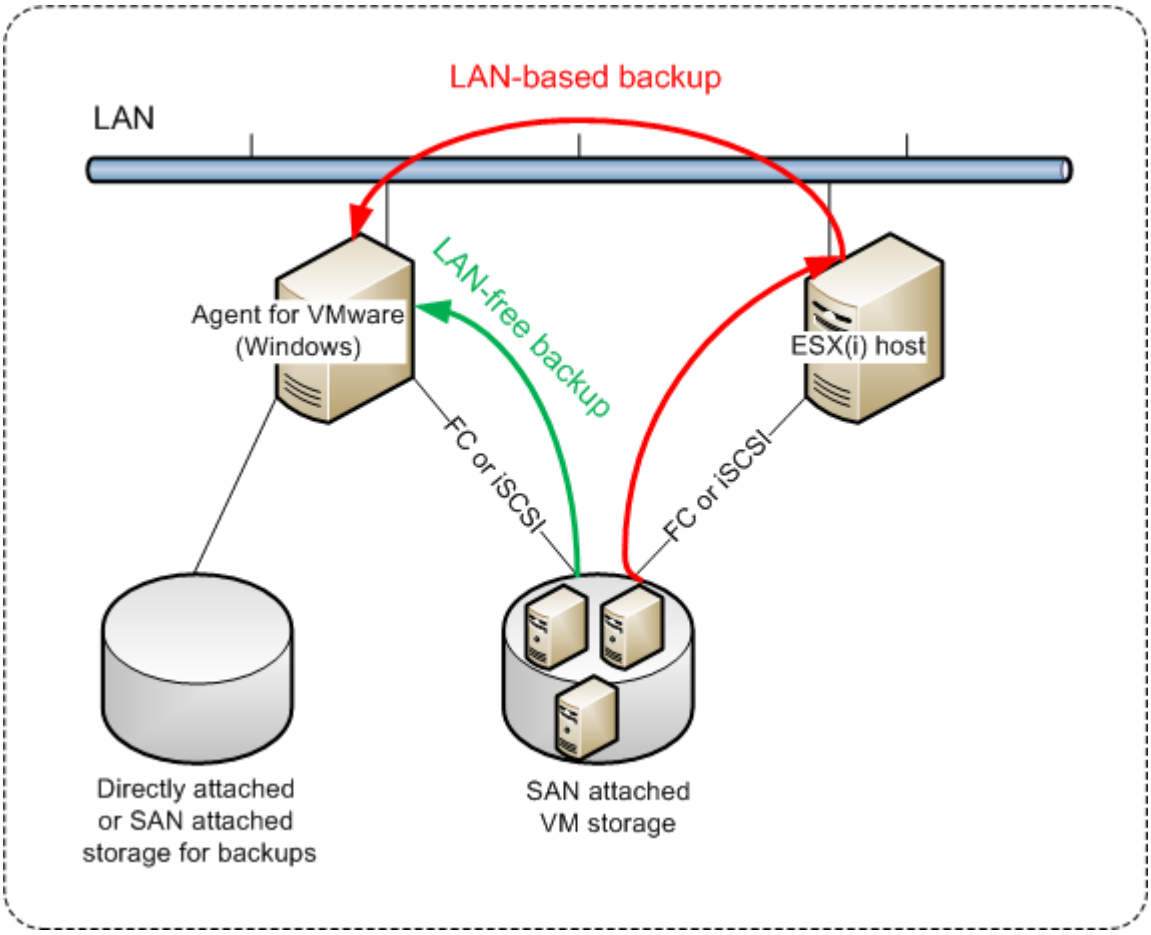
e. **[ディレクトリ]** で外部ハードドライブのフォルダを指定します。
f. **[OK]** をクリックします。
5. ハードドライブをリモートロケーションに転送します。
6. レプリカをターゲットESXiにインポートします。
   a. vSphereクライアントが実行されているコンピュータに外部ハードドライブを接続します。
   b. vSphereクライアントをターゲットvCenter¥ESXiに接続します。
   c. **[ファイル]** > **[OVFテンプレートのデプロイ]** をクリックします。
   d. **[ファイルまたはURLからのデプロイ]** で、手順4でエクスポートしたテンプレートを指定します。
   e. インポート手順を完了します。
7. 手順2で作成したレプリケーション計画を編集します。**[ターゲットマシン]** で **[既存のレプリカ]** を選択し、インポートされたレプリカを選択します。

結果として、レプリカのアップデートが続きます。すべてのレプリケーションは増分です。

エージェント for VMware - LAN フリー バックアップ

使用しているESXiでSAN接続ストレージが使用されている場合は、このエージェントを同じSAN接続コンピュータにインストールします。エージェントは、ESXiホストやLANを経由せずにストレージから仮想コンピュータを直接バックアップします。この機能は、LAN フリー バックアップと呼ばれます。

下の図は、LAN ベースのバックアップと LAN フリー バックアップを示しています。ファイバ チャネル（FC）または iSCSI ストレージ エリア ネットワークがある場合は、仮想コンピュータに LAN フリー アクセスすることができます。バックアップされたデータを LAN 経由で一切転送しないようにするには、バックアップをエージェントのコンピュータのローカル ディスク、または SAN に接続されたストレージに保存します。



エージェントのデータ ストアへの直接アクセスを有効化する手順

1. vCenter Serverに接続できるWindowsコンピュータにエージェント for VMwareをインストールします。
2. データ ストアをホストする論理装置番号（LUN）をコンピュータに接続します。以下について考慮してください。
   - ESXiへのデータ ストア接続に使用されているプロトコル（iSCSIまたはFC）と同じプロトコルを使用します。
   - **ディスク管理**で、LUNは初期化されず、「オフライン」ディスクとして表示される必要があります。WindowsによってLUNが初期化されると、破損してVMware vSphereで読み取れなくなる場合があります。

その結果、エージェントは仮想ディスクへの接続にSAN転送モードを使用するようになります。つまり、VMFSファイル システムを識別しないでiSCSI/FCからRaw LUNセクターを読み込みます（これはWindowsには認識されません）。

制限

- vSphere 6.0以降では、VMディスクがVMware Virtual Volume（VVol）にあるものとそうでないものがある場合、エージェントはSAN転送モードを使用できません。そのような仮想コンピュータのバックアップはできません。

- VMware vSphere 6.5で導入された暗号化仮想コンピュータは、エージェントにSAN転送モードを設定してもLAN経由でバックアップされます。VMwareが暗号化仮想ディスクのバックアップにSAN転送をサポートしないため、エージェントはNBD転送にフォールバックします。

例

iSCSI SANを使用している場合、エージェント for VMwareがインストールされているWindowsを実行しているiSCSI イニシエーターを設定します。

SAN ポリシーの設定手順

1. 管理者としてログインし、コマンドプロンプトを開き、`diskpart`と入力してから、**Enter**キーを押します。
2. `san`と入力し、**Enter**キーを押します。[**SAN ポリシー:すべてオフライン**] と表示されることを確認してください。
3. SANポリシーに別の値が設定されている場合は、次のようにします。
   a. `san policy=offlineall`と入力します。
   b. **Enter**キーを押します。
   c. この設定が正しく適用されたことを確認するには、手順2を実行します。
   d. コンピュータを再起動します。

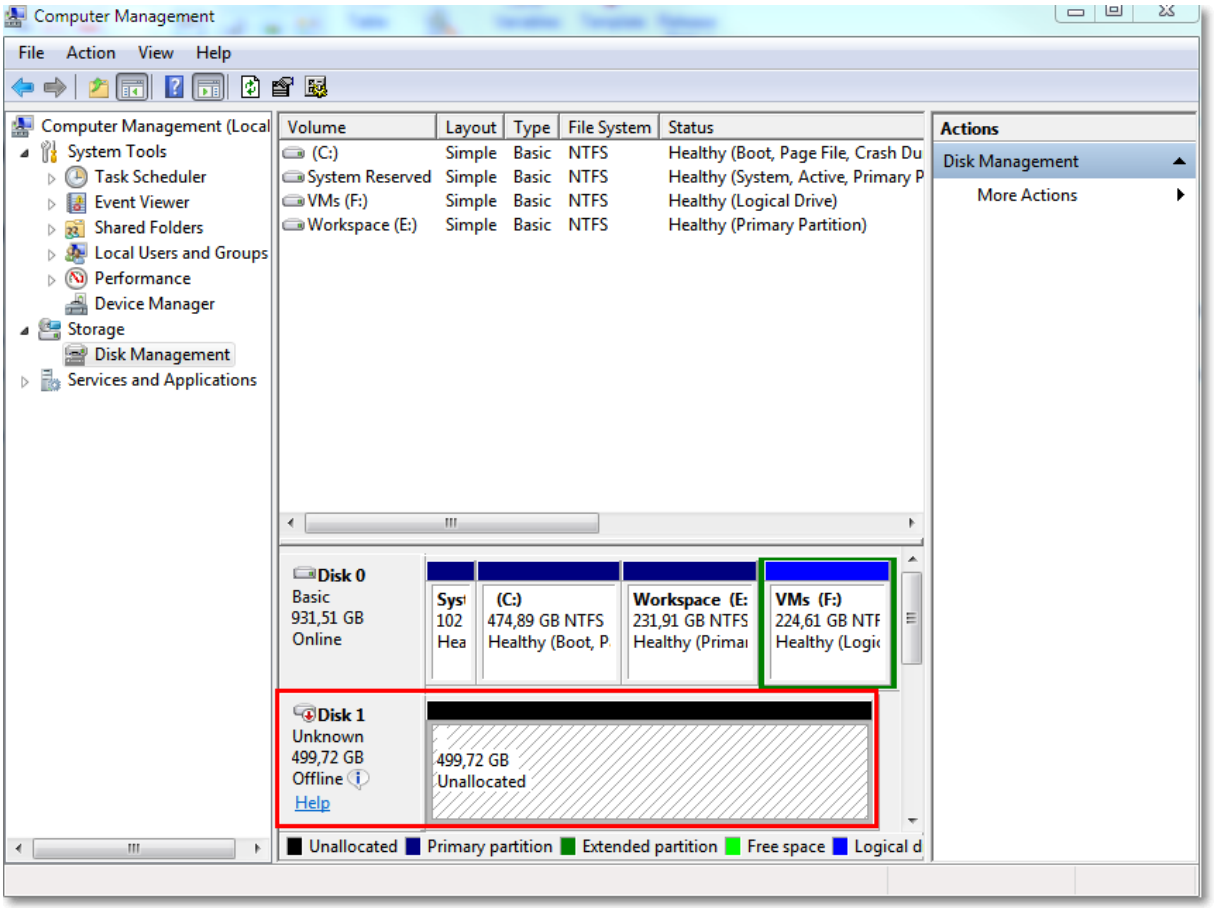
iSCSI イニシエーターの設定手順

1. [**コントロール パネル**] > [**管理ツール**] > [**iSCSI イニシエーター**] に移動します。

   注意
   管理ツールアプレットを見つけるに**コントロール パネル**表示を[**ホーム**] または [**カテゴリ**] 以外に変更するか、検索してください。

2. Microsoft iSCSI イニシエーターを初めて起動する場合は、Microsoft iSCSI イニシエーターサービスが開始されることをご承知ください。
3. [**ターゲット**] タブで、SANデバイスの完全修飾ドメイン名（FQDN）またはIPアドレスを入力して、[**クイック接続**] をクリックします。
4. データ ストアをホストするLUNを選択し、[**接続**] をクリックします。
   LUNが表示されない場合は、iSCSI ターゲットのゾーニングがLUNにアクセスするエージェントを実行しているコンピュータで有効になっているか確認してください。対象のコンピュータはこのターゲットで許可されたiSCSI イニシエーターのリストに登録されている必要があります。
5. [**OK**] をクリックします。

次のスクリーンショットに示すように準備ができたSAN LUNが[**ディスク管理**] に表示されます。



ローカルに接続されたストレージの使用

追加のディスクをエージェント for VMware（仮想アプライアンス）に接続して、エージェントによるバックアップ先を、ローカルに接続されたこのストレージに設定できます。このアプローチでは、エージェントとバックアップロケーションとの間のネットワークトラフィックが排除されます。

バックアップされた仮想マシンと同じホストまたはクラスター上で実行されている仮想アプライアンスは、マシンが存在するデータストアに直接アクセスできます。これは、アプライアンスがバックアップされたディスクを HotAdd トランスポートを使用して接続でき、そのためバックアップトラフィックがあるローカルディスクから別のローカルディスクに向けられることを意味します。データストアが **NFS** ではなく**ディスク/LUN** として接続されている場合は、完全な LAN フリーのバックアップになります。NFS データストアの場合は、データストアとホストとの間にネットワークトラフィックが発生します。

ローカルに接続されたストレージを使用する場合、エージェントが常に同じコンピュータをバックアップすることを前提としています。複数のエージェントがvSphere内で動作しており、その中にローカルに接続されたストレージを使用しているエージェントがある場合は、バックアップする必要があるすべてのコンピュータと各エージェントを手動でバインドする必要があります。バインドしない場合、Management Serverによって各コンピュータが各エージェントに再分配されると、1 つのコンピュータのバックアップが、複数のストレージに分散される場合があります。

既に実行中のエージェントに、または OVF テンプレートからエージェントをデプロイする際に、ストレージを追加できます。

既に実行中のエージェントにストレージを接続するには

1. VMware vSphere のインベントリで、エージェント for VMware（Virtual Appliance）を右クリックします。
2. 仮想コンピュータの設定を編集してディスクを追加します。ディスク サイズは 10 GB 以上必要です。

警告
既存のディスクを追加するタイミングには注意してください。ストレージを作成すると、既存のディスクに存在していたデータはすべて失われます。

3. 仮想アプライアンス コンソールに移動します。**[ストレージの作成]** リンクが、画面の下部に表示されています。表示されていない場合は、**[更新]** をクリックします。
4. **[ストレージの作成]** リンクをクリックし、ディスクを選択し、そのディスクのラベルを指定します。ファイルシステムの制限により、ラベル長は 16 文字に制限されています。

ローカルに接続されたストレージをバックアップ先として選択するには

- 保護計画を作成している場合は、**[バックアップ先]** で **[ローカルフォルダ]** を選択し、ローカル接続のストレージに対応する文字を入力します（例: **D:¥**）。

注意
ローカル接続ストレージ（LAS）は、単一のエージェント（仮想アプライアンス）を使用する比較的小規模な環境向けに設計されています。Acronisでは、最大5TBまでのLASユニットについてテストを実行済みです。この容量を上回るディスクを自己責任で接続することはできますが、そのような構成はサポートされていません。それで5TBを超えるバックアップデータについては、他のタイプのストレージを使用することをお勧めします。例えば、任意の仮想マシンにVMware仮想ディスクを作成して接続し、そのディスク上にネットワーク共有を作成すると、LASの代わりにバックアップ先として使用できます。

仮想コンピュータのバインド

このセクションでは、Cyber ProtectionサービスがVMware vCenter内で複数のエージェントの処理を整理する方法の概要について説明します。

配分アルゴリズム（以下参照）は、Windows にインストールされた仮想アプライアンスとエージェントの両方で機能します。

配分アルゴリズム

仮想コンピュータは、自動的にVMwareエージェントの間で均等に配分されます。均等とは、各エージェントで同じ台数のコンピュータを管理することを意味します。仮想コンピュータが占有するストレージ領域の容量はカウントされません。

ただし、コンピュータのエージェントを選択すると、全体的なシステムパフォーマンスの最適化が図られます。特に、エージェントと仮想コンピュータのロケーションが考慮されます。同じホストでホストされているエージェントが好ましいとされます。同じホストにエージェントがない場合は、同じクラスタのエージェントが好ましいとされます。

仮想コンピュータがひとたびエージェントに割り当てられると、そのコンピュータの全バックアップはそのエージェントが担います。

再配分

再配分は、確立されたバランスが崩れるたび、具体的にはエージェント間で負荷の不均衡が 20% に達すると実行されます。これは、コンピュータまたはエージェントが追加または削除された場合、コンピュータが別のホストまたはクラスタに移行された場合、または手動でコンピュータをエージェントにバインドした場合に発生する可能性があります。不均衡が発生すると、Cyber Protectionサービスは同じアルゴリズムを使用してマシンを再配分します。

たとえば、スループットを向上させるためにより多くのエージェントが必要で、追加の仮想アプライアンスをクラスタに配置する必要があるとします。Cyber Protectionサービスは、最も適したマシンを新しいエージェントに割り当てます。これにより、古いエージェントの負荷は軽減されます。

エージェントをCyber Protectionサービスから削除すると、エージェントに割り当てられたマシンが残りのエージェントの間で再配分されます。ただし、エージェントが破損した場合、またはvSphereから手動で削除された場合は、実行されません。再配分は、このようなエージェントをWebインターフェイスから削除してはじめて開始されます。

配分結果の表示

自動配分の結果は以下に表示されます。

- **[すべてのデバイス]** セクションの各仮想マシンの **[エージェント]** 列
- エージェントが **[設定]** > **[エージェント]** セクションで選択された場合は、**[詳細]** パネルの **[割り当てられた仮想コンピュータ]** セクション

手動バインド

[VMwareエージェントバインド] では、この仮想コンピュータを常にバックアップするエージェントを指定して、その仮想コンピュータを配分処理から除外できます。全体的なバランスは維持されますが、元のエージェントが削除された場合にかぎり、この該当するコンピュータを別のエージェントに渡すことができます。

コンピュータをエージェントにバインドするには

1. コンピュータを選択します。
2. **[詳細]** をクリックします。
   [割り当てられたエージェント] セクションに、選択したコンピュータを現在管理しているエージェントが表示されます。
3. **[変更]** をクリックします。
4. ［**手動**］ をクリックします。
5. コンピュータにバインドするエージェントを選択します。
6. **[保存]** をクリックします。

コンピュータをエージェントとのバインドから解除するには

1. コンピュータを選択します。
2. **[詳細]** をクリックします。
   [割り当てられたエージェント] セクションに、選択したコンピュータを現在管理しているエージェントが表示されます。
3. **[変更]** をクリックします。
4. **[自動]** を選択します。
5. **[保存]** をクリックします。

エージェントの自動割り当ての無効化

VMwareエージェントバインドがバックアップするコンピュータのリストを指定すると、自動割り当てを無効にして、このエージェントを配分処理から除外できます。全体的なバランスは他のエージェント間で維持されます。

登録済みエージェントが他にない場合、または自動割り当てが他のすべてのエージェントで無効になっている場合は、自動割り当てを無効にできません。

エージェントの自動割り当てを無効にするには

1. **[設定]** > **[エージェント]** の順にクリックします。
2. 自動割り当てを無効にするVMwareエージェントバインドを選択します
3. **[詳細]** をクリックします。
4. **[自動割り当て]** スイッチをオフにします。

使用例

- 手動バインドは、特定の（非常に大きな）コンピュータはVMwareエージェントバインド（Windows）を使用してファイバチャネル経由でバックアップし、他のコンピュータは仮想アプライアンスを使用してバックアップする場合に便利です。
- エージェントにローカル接続されたストレージがある場合は、仮想コンピュータをエージェントにバインドする必要があります。
- 自動割り当てを無効にすると、特定のコンピュータを指定したスケジュールに基づいてバックアップできます。単一の仮想コンピュータしかバックアップしないエージェントが、スケジュールされた時刻になって他の仮想コンピュータのバックアップに追われているということはありえません。
- 自動割り当てを無効にすることは、地理的に離れているESXiホストが複数ある場合に便利です。自動割り当てを無効にし、各ホストの仮想コンピュータを同じホストで実行されているエージェントにバインドすると、そのエージェントはリモートESXiホストで実行されているコンピュータのバックアップを決して実行しないため、ネットワークトラフィックを削減できます。

凍結前スクリプトと凍結解除後スクリプトを自動的に実行する

VMware Toolsでは、エージェントレスモードでバックアップした仮想マシンで、カスタマイズされた凍結前スクリプトと凍結解除後スクリプトを自動的に実行できます。これにより、たとえば、VSS対応ではないアプリケーションを実行している仮想マシンで、カスタムの静止スクリプトを実行したり、アプリケーションについて一貫性のあるバックアップを作成したりできます。

前提条件

pre-freezeおよびpost-thawスクリプトは、仮想マシン上の特定のフォルダに配置する必要があります。

- Windows仮想マシンの場合、このフォルダのロケーションはホストのESXiバージョンによって異なります。

  たとえば、ESXi 6.5ホスト上で動作する仮想マシンの場合、このフォルダは、`C:\Program Files\VMware\VMware Tools\backupScripts.d\`になります。`backupScritps.d`フォルダを手動で作成する必要があります。このフォルダに他の種類のファイルを保存しないでください。VMware Toolsの動作が不安定になる場合があります。

  他のバージョンのESXiにおけるpre-freezeおよびpost-thawスクリプトのロケーションについては、VMwareの文書を参照してください。
- Linux仮想マシンの場合、`/usr/sbin/pre-freeze-script`ディレクトリと`/usr/sbin/post-thaw-script`ディレクトリにそれぞれスクリプトをコピーします。`/usr/sbin/pre-freeze-script`にあるスクリプトは、スナップショットを作成したときに実行され、`/usr/sbin/post-thaw-script`にあるスクリプトは、スナップショットが最終化されたときに実行されます。スクリプトは、VMware Toolsユーザーが実行できるものでなければなりません。

凍結前スクリプトと凍結解除後スクリプトを自動的に実行するには

1. 仮想マシンにVMware Toolsがインストールされていることを確認します。
2. 仮想マシン上で、必要なフォルダにカスタムスクリプトを配置します。
3. 対象となるマシンの保護計画で、**[仮想マシンのボリュームシャドウコピーサービス（VSS）]** オプションを有効にします。

   これにより、**[静止ゲストファイルシステム]** オプションを有効にしたVMwareスナップショットが作成され、仮想マシン内の凍結前および凍結解除後スクリプトが自動的に実行されます。

Microsoft SQL ServerやMicrosoft Exchangeなど、VSS対応アプリケーションを実行している仮想マシンでは、カスタムの停止スクリプトを実行する必要はありません。このようなマシンに対し、アプリケーションについて一貫性のあるバックアップを作成するには、保護計画で **[仮想マシンのボリュームシャドウコピーサービス（VSS）]** オプションを有効にします。

仮想マシンのマイグレーションをサポート

このセクションでは、vSphereクラスターの一部であるESXiホスト間のマイグレーションを含む、vSphere環境内での仮想マシンのマイグレーションについて説明します。

vMotionは、仮想マシンのディスクを共有ストレージの同じロケーションに残したまま、仮想マシンの状態や構成を別のホストに移動させることができます。Storage vMotionでは、仮想マシンのディスクをデータストア間で移動させることができます。

- Storage vMotionを含むvMotionによるマイグレーションは、VMwareエージェント（仮想アプライアンス）が動作する仮想マシンではサポートされておらず、自動的に無効になります。この仮想マシンは、vSphereクラスター構成の**VMオーバーライド**リストに追加されます。
- 仮想マシンのバックアップを開始すると、Storage vMotionを含むvMotionによるマイグレーションが自動的に無効になります。この仮想マシンは、vSphereクラスター構成の**VMオーバーライド**リスト

に一時的に追加されます。バックアップが終了すると、**VMオーバーライド**の設定は自動的に以前の状態に戻されます。

- Storage vMotionを含むvMotionによるマイグレーションが進行中の仮想マシンでは、バックアップを開始できません。このマシンのバックアップは、関連するマイグレーションが終了した時点で開始されます。

仮想環境の管理

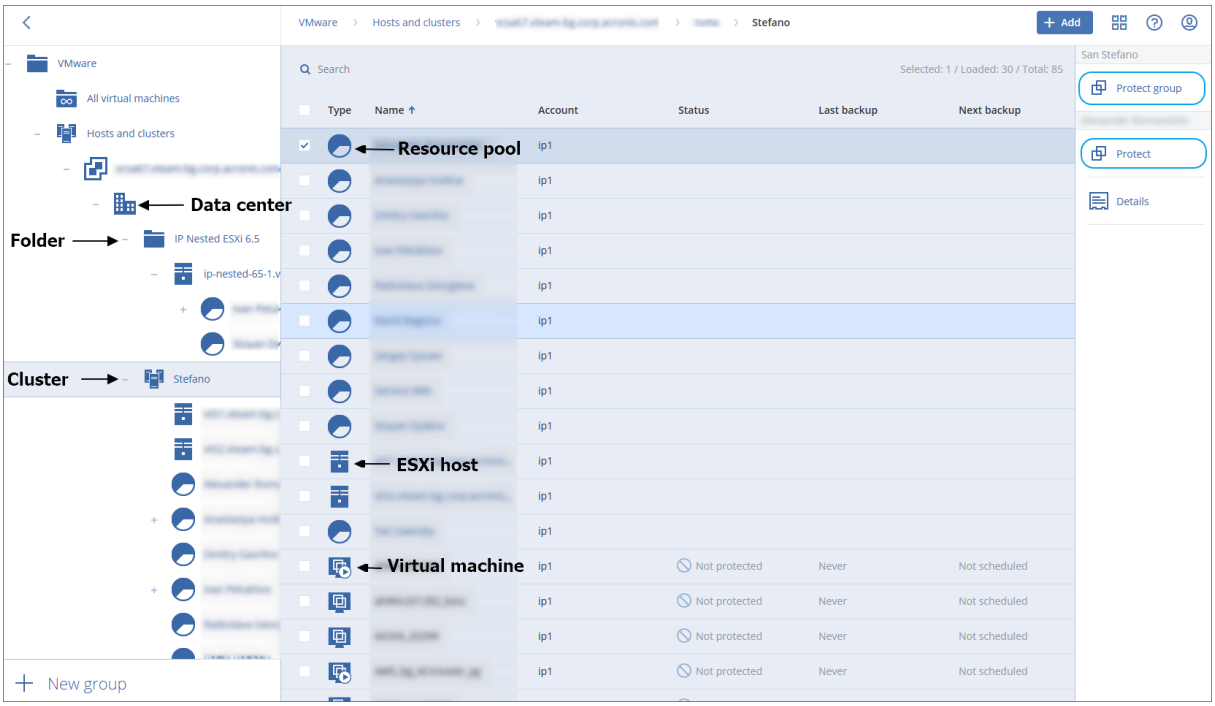
ネイティブ表示でvSphere、Hyper-V、Virtuozzo環境を表示できます。対応するエージェントがインストールおよび登録されると、[**デバイス**] の下に [**VMware**]、[**Hyper-V**]、または [**Virtuozzo**] の各タブが表示されます。

[**VMware**] タブで、以下のvSphereインフラストラクチャオブジェクトをバックアップします。

- データセンター
- フォルダ
- クラスタ
- ESXiホスト
- リソースプール

各インフラストラクチャオブジェクトは、仮想マシンのグループオブジェクトとしての役割を果たします。いずれかのグループオブジェクトに保護計画を適用すると、そのグループオブジェクトに含まれているすべての仮想マシンがバックアップされます。選択したグループマシンをバックアップする場合は、[**保護**] をクリックします。選択したグループが含まれている親グループマシンをバックアップする場合は、[**グループの保護**] をクリックします。

たとえば、Stefanoクラスターを選択してから、その中に入っているリソースプールを選択したとします。[**保護**] をクリックすると、選択したリソースプールに含まれているすべての仮想マシンがバックアップされます。[**グループの保護**] をクリックすると、Stefanoクラスターに含まれているすべての仮想マシンがバックアップされます。



[VMware] タブでは、エージェントを再インストールせずに、vCenter ServerまたはスタンドアロンESXiホストのアクセス認証情報を変更できます。

vCenter ServerまたはESXiホストアクセス資格情報を変更するには

1. **[デバイス]** で、**[VMware]** をクリックします。
2. **[ホストとクラスタ]** をクリックします。
3. **[ホストとクラスタ]** リスト（**[ホストとクラスタ]** ツリーの右）で、VMwareエージェントのインストール時に指定されたvCenter ServerまたはスタンドアロンESXiホストを選択します。
4. **[詳細]** をクリックします。
5. **[資格情報]** の下でユーザー名をクリックします。
6. 新しいアクセス認証を指定し、**[OK]** をクリックします。

vSphere クライアントにおけるバックアップステータスの表示

vSphere クライアントで仮想マシンのバックアップステータスと最終バックアップ時刻を表示できます。

この情報は、仮想マシンの概要（クライアントタイプおよび vSphere のバージョンに応じて、**[概要]** > **[カスタム属性]** / **[注釈]** / **[メモ]**）に表示されます。ホスト、データセンター、フォルダ、リソースプール、または vCenter Server 全体について、**[仮想マシン]** タブの **[最終バックアップ]** 列と **[バックアップステータス]** 列を有効にすることもできます。

これらの属性を提供するには、「VMware エージェント - 必要な権限」で説明されている権限に加えて、VMware エージェントに対する次の権限が必要です。

- **[グローバル]** > **[カスタム属性の管理]**
- **[グローバル]** > **[カスタム属性の設定]**

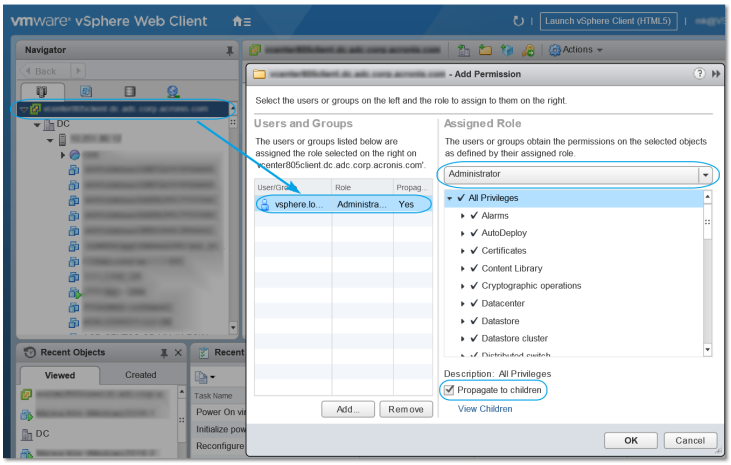
VMware エージェント - 必要な権限

vCenterオブジェクト（仮想マシン、ESXiホスト、クラスター、vCenterなど）で操作を実行する場合は、VMwareエージェントが、ユーザーが指定したvSphere資格情報に基づいてvCenterやESXiホストで認証を行います。VMwareエージェントからvSphereへの接続で使用するvSphereアカウントは、vSphereインフラストラクチャのvCenterレベルから始まるあらゆるレベルで必要な権限を持っていなければなりません。

VMwareエージェントのインストール時または構成時に、必要な権限を持つvSphereアカウントを指定してください。後からアカウントの変更が必要になる場合は、「"仮想環境の管理"（679ページ）」を参照してください。

vCenterレベルでvSphereユーザーに許可を割り当てるには

1. vSphere Webクライアントにログインします。
2. vCenterを右クリックして、**[許可の追加]** をクリックします。
3. 必要なロールを持つ新しいユーザーを選択するか、追加します。そのロールには、必要な許可がすべて含まれていなければなりません（下の表を参照）。
4. **[子への継承]** オプションを選択します。



目的	権限	操作			
		VM のバックアップ	新しい VM への復元	既存の VM へのリカバリ	バックアップから VM を実行
暗号化操作 （vSphere 6.5から）	**ディスクの追加**	+*			
	直接アクセス	+*			
データストア	**領域の割り当て**		+	+	+
	データストアの参照				+

	データストアの構成	+	+	+	+
	下位レベルのファイルの操作				+
グローバル	ライセンス	+	+	+	+
	メソッドの無効化	+	+	+	
	メソッドの有効化	+	+	+	
	カスタム属性の管理	+	+	+	
	カスタム属性の設定	+	+	+	
ホスト > 構成	ストレージパーティションの構成				+
ホスト >ローカル操作	VM の作成				+
	VM の削除				+
	VM の再構成				+
ネットワーク	ネットワークの割り当て		+	+	+
リソース	リソース プールへの VM の割り当て		+	+	+
仮想コンピュータ > 構成	既存のディスクの追加	+	+		+
	新しいディスクの追加		+	+	+
	デバイスの追加または削除		+		+
	詳細	+	+	+	
	CPU 数の変更		+		
	ディスク変更の追跡	+		+	
	ディスク リース	+		+	
	RAM		+		
	ディスクの削除	+	+	+	+
	名前の変更		+		
	注釈の設定				+
	設定		+	+	+
仮想コンピュータ > ゲスト操作	ゲスト操作のプログラム実行	+**			

	ゲスト操作のクエリ	+**			
	ゲスト操作の変更	+**			
仮想コンピュータ > **操作**	**ゲスト制御チケットの取得** （vSphere4.1と5.0）				+
	CD メディアの設定		+	+	
	VIX API によるゲスト OS 管理（vSphere5.1 以降）				+
	電源オフ			+	+
	電源オン		+	+	+
仮想コンピュータ > **インベントリ**	**既存から作成**		+	+	+
	新規作成		+	+	+
	登録				+
	削除		+	+	+
	登録解除				+
仮想コンピュータ > **プロビジョニング**	**ディスク アクセスの許可**		+	+	+
	読み取り専用ディスクアクセスの許可	+		+	
	仮想マシンのダウンロードを許可	+	+	+	+
仮想コンピュータ > **状態** **[仮想マシン]** > **[スナップショット管理]**（vSphere 6.5 以降）	**スナップショットの作成**	+		+	+
	スナップショットの削除	+		+	+
vApp	**仮想マシンの追加**				+

* 暗号化コンピュータのバックアップの場合のみ必須です。

** アプリケーションアウェアバックアップの場合のみ必須です。

クラスタ化された Hyper-V コンピュータのバックアップ

Hyper-V クラスタでは、仮想コンピュータをクラスタ ノード間で移行することができます。クラスタ化された Hyper-V コンピュータのバックアップを正しく設定するには、次の推奨事項に従ってください。

1. 移行先のノードに関係なく、コンピュータをバックアップに使用できるようにしておく必要があります。Hyper-V エージェントでどのノードのマシンにもアクセスできるようにするには、各クラスターノードに対して管理者権限のあるドメインユーザーアカウントでエージェントサービスを実行します。

   Hyper-Vエージェント のインストール時に、このようなアカウントをエージェント サービスに指定しておくことをお勧めします。
2. Hyper-Vエージェント をクラスタの各ノードにインストールします。
3. すべてのエージェントをCyber Protectionサービスに登録します。

復元されたコンピュータの高可用性

バックアップしたディスクを既存の Hyper-V 仮想マシンに復元するとき、マシンの高可用性プロパティはそのままの状態で残ります。

バックアップしたディスクを新しい Hyper-V 仮想マシンに復元するとき、作成されるマシンは高可用性にはなりません。予備のコンピュータとみなされ、通常、電源がオフになります。運用環境でマシンを使用する必要がある場合、**フェールオーバークラスター管理**スナップインから高可用性に設定できます。

同時にバックアップされる仮想マシンの合計数の制限

[スケジューリング] バックアップオプションでは、同時にバックアップ可能な仮想マシンの数を保護計画ごとに制限できます。

エージェントで複数の計画を同時に実行すると、同時にバックアップされるマシンの数が増加します。これはバックアップの作成速度に影響し、ホストと仮想マシンのストレージに過度の負荷がかかる可能性があります。エージェントレベルで制限を構成することで、このような問題を避けることができます。

エージェントレベルで同時バックアップ数を制限するには

エージェント for VMware（Windows）

1. エージェントを実行しているマシンで、新しいテキスト文書を作成し、テキストエディタで開きます。
2. 次の行をコピーしてファイルに貼り付けます。

```
Windows Registry Editor Version 5.00

[HKEY_LOCAL_
MACHINE\SOFTWARE\Acronis\MMS\Configuration\ManagedMachine\SimultaneousBackupsLimits]
"MaxNumberOfSimultaneousBackups"=dword:00000001
```

3. `00000001`は設定する制限の16進値で置換します。
   たとえば、`00000001`は1で、`0000000A`は10です。
4. **limit.reg**として文書を保存します。
5. ファイルを管理者として実行します。
6. Windowsレジストリを編集することを確認します。
7. エージェントを再起動します。
   a. **[スタート]** メニューで、**[実行]** をクリックします。
   b. 「**cmd**」と入力してから **[OK]** をクリックします。
   c. コマンドラインで以下のコマンドを実行します。

```
net stop mms
net start mms
```

Hyper-Vエージェント

1. エージェントを実行しているマシンで、新しいテキスト文書を作成し、テキストエディタで開きます。
2. 次の行をコピーしてファイルに貼り付けます。

```
Windows Registry Editor Version 5.00

[HKEY_LOCAL_
MACHINE\SOFTWARE\Acronis\MMS\Configuration\ManagedMachine\SimultaneousBackupsLimits]
"MaxNumberOfSimultaneousBackups"=dword:00000001
```

3. `00000001`は設定する制限の16進値で置換します。
   たとえば、`00000001`は1で、`0000000A`は10です。
4. **limit.reg**として文書を保存します。
5. ファイルを管理者として実行します。
6. Windowsレジストリを編集することを確認します。
7. エージェントを再起動します。
   a. **[スタート]** メニューで、**[実行]** をクリックします。
   b. 「**cmd**」と入力してから **[OK]** をクリックします。
   c. コマンドラインで以下のコマンドを実行します。

```
net stop mms
net start mms
```

仮想アプライアンス

この手順は、VMwareエージェント（仮想アプライアンス）、Scale Computingエージェント、Virtuozzo Hybrid Infrastructureエージェント、およびoVirtエージェントに適用されます。

1. 仮想アプライアンスのコンソールで、CTRL+SHIFT+F2キーでコマンドラインインターフェイスが開きます。
2. テキストエディタで`/etc/Acronis/MMS.config`ファイルを開きます。

3. 次のセクションを見つけます。

```
<key name="SimultaneousBackupsLimits">
    <value name="MaxNumberOfSimultaneousBackups" type="Tdword">"10"</value>
</key>
```

4. 10を設定したい最大同時バックアップ数に置き換えます。
5. ファイルを保存します。
6. rebootコマンドを実行してエージェントを再起動します。

コンピュータの移行

コンピュータの移行を実行するには、別のコンピュータにバックアップを復元します。

次の表に、使用可能な移行オプションを示します。

バックアップされるコンピュータのタイプ	使用可能な復元先							
	物理コンピュータ	ESXi仮想コンピュータ	Hyper-V仮想コンピュータ	Virtuozzo		Virtuozzo Hybrid Infrastructure 仮想マシン	Scale Computing HC3 仮想マシン	RHV/oVirt仮想マシン
				仮想コンピュータ	コンテナ			
物理コンピュータ	+	+	+	-	-	+	+*	+
VMware ESXi 仮想コンピュータ	+	+	+	-	-	+	+*	+
Hyper-V仮想コンピュータ	+	+	+	-	-	+	+*	+
Virtuozzo仮想コンピュータ	+	+	+	+	-	+	+*	+
Virtuozzoコンテナ	-	-	-	-	+	-	-	-
Virtuozzo Hybrid Infrastructure 仮想マシン	+	+	+	-	-	+	+*	+
Scale Computing HC3仮想マシン	+	+	+	-	-	+	+	+

Red Hat Virtualization /oVirt仮想マシン	+	+	+	-	-	+	+*	+

*ソースマシンでセキュアブートが有効になっている場合、復元後のVMはセキュアブートを無効にしない限り起動できません。復元後に仮想マシンのコンソールでセキュアブートを無効にする必要があります。

注意
Hyper-VはmacOSをサポートしていないため、macOS仮想マシンをHyper-Vホストにリカバリすることはできません。macOS仮想マシンは、Macハードウェアにインストールされ ているVMwareホストにリカバリできます。

マイグレーション処理の実行方法の詳細については、次のトピックを参照してください:

- 物理から仮想（P2V）へのマイグレーションについては、"物理コンピュータから仮想コンピュータへ"（490ページ）を参照してください。
- 仮想から仮想（V2V）へのマイグレーションについては、"仮想コンピュータの復元バックアップから仮想マシンをリカバリできます。コンプライアンスモードのテナント対しCyber Protectコンソールではバックアップをリカバリできません。このようなバックアップをリカバリする方法の詳細については、"コンプライアンスモードでテナントのバックアップを復元する"（1ページ）を参照してください。前提条件このコンピュータへの復元中は、仮想コンピュータを停止する必要があります。デフォルトでは、確認メッセージを表示することなくマシンが停止します。復元が完了したら、コンピュータを手動で起動する必要があります。このデフォルトの動作はVM電源管理復元オプションを使用して変更できます（[復元オプション] > [VM電源管理]をクリック）。手順次のいずれかを実行します。バックアップされたコンピュータを選択し、[復元] をクリックしてから、リカバリポイントを選択します。[バックアップストレージ] タブで復元ポイントを選択します。[復元] > [コンピュータ全体] をクリックします。物理コンピュータに復元する場合は、[復元先] で [物理コンピュータ] を選択します。それ以外の場合は、この手順をスキップします。対象コンピュータのディスク構成がバックアップのディスク構成と正確に一致する場合にのみ、物理コンピュータへの復元が可能です。この場合、「物理コンピュータ」の手順4に続きます。それ以外の場合は、ブータブルメディアを使用して、V2P移行を実行することをお勧めします。（オプション）デフォルトでは、ターゲットマシンとして自動的に元のコンピュータが選択されます。別の仮想コンピュータに復元するには、[ターゲットコンピュータ] をクリックしてから次の手順を実行します。ハイパーバイザーを選択します（VMware ESXi、Hyper-V、Virtuozzo、Virtuozzo Hybrid Infrastructure、Scale Computing HC3、またはoVirt）。Virtuozzoに復元できるのは、Virtuozzo仮想コンピュータのみです。V2V移行の詳細については、「マシンの移行」を参照してください。新規または既存のコンピュータに復元するかどうかを選択します。ホストを選択し、新しいコンピュータ名を指定するか、既存のターゲット コンピュータを選択します。[OK] をクリックします。必要な追加の復元オプションを設定します。（Virtuozzo Hybrid InfrastructureおよびScale Computing HC3では利用不可）仮想マシンのデータストアを選択するには、[データストア]（ESXi）、[パス]（Hyper-VおよびVirtuozzo）、または [ストレージドメイン]（Red Hat Virtualization/oVirt）をクリックしてから、仮想マシンのデータストア（ストレージ）を選択します。各仮想ディスクのデータストア（ストレージ）、インターフェース、

プロビジョニングモードを表示するには、[ディスクマッピング] をクリックします。VirtuozzoコンテナまたはVirtuozzo Hybrid Infrastructure仮想マシンの復元中でなければ、これらの設定を変更できます。Virtuozzo Hybrid Infrastructureの場合、ターゲットディスクに対して選択できるのはストレージポリシーのみです。設定する場合、対象のターゲットディスクを選択し、[変更] をクリックします。ブレードが開いたら、ギアアイコンをクリックし、ストレージポリシーを選択して [完了] をクリックします。マッピングセクションでは、復元対象の個別のディスクを選択することもできます。
（VMware ESXi、Hyper-V、Virtuozzoで利用可能）仮想マシンのメモリサイズ、プロセッサー数、ネットワーク接続を変更するには、[VM設定] をクリックします。（Virtuozzo Hybrid Infrastructure向け）仮想マシンのメモリサイズ、プロセッサー数を変更するには、[フレーバー] をクリックします。（プロテクションエージェントがインストールされているWindowsマシンでのみ使用可能）[安全な復元] スイッチを有効にして、リカバリデータがマルウェアに感染していないことを確認します。安全な復元の仕組みについては、"安全な復元"（1ページ）を参照してください。[復元を開始] をクリックします。既存の仮想コンピュータに復元するときには、ディスクを上書きすることを確認します。復元の進行状況は [アクティビティ] タブに表示されます。"（1ページ）を参照してください。

- 仮想から物理へのマイグレーション（V2P）については、"仮想コンピュータの復元バックアップから仮想マシンをリカバリできます。コンプライアンスモードのテナント対しCyber Protectコンソールではバックアップをリカバリできません。このようなバックアップをリカバリする方法の詳細については、"コンプライアンスモードでテナントのバックアップを復元する"（1ページ）を参照してください。前提条件このコンピュータへの復元中は、仮想コンピュータを停止する必要があります。デフォルトでは、確認メッセージを表示することなくマシンが停止します。復元が完了したら、コンピュータを手動で起動する必要があります。このデフォルトの動作はVM電源管理復元オプションを使用して変更できます（[復元オプション] > [VM電源管理]をクリック）。手順次のいずれかを実行します。バックアップされたコンピュータを選択し、[復元] をクリックしてから、リカバリポイントを選択します。[バックアップストレージ] タブで復元ポイントを選択します。[復元] > [コンピュータ全体] をクリックします。物理コンピュータに復元する場合は、[復元先] で [物理コンピュータ] を選択します。それ以外の場合は、この手順をスキップします。対象コンピュータのディスク構成がバックアップのディスク構成と正確に一致する場合にのみ、物理コンピュータへの復元が可能です。この場合、「物理コンピュータ」の手順4に続きます。それ以外の場合は、ブータブルメディアを使用して、V2P移行を実行することをお勧めします。（オプション）デフォルトでは、ターゲットマシンとして自動的に元のコンピュータが選択されます。別の仮想コンピュータに復元するには、[ターゲットコンピュータ] をクリックしてから次の手順を実行します。ハイパーバイザーを選択します（VMware ESXi、Hyper-V、Virtuozzo、Virtuozzo Hybrid Infrastructure、Scale Computing HC3、またはoVirt）。Virtuozzoに復元できるのは、Virtuozzo仮想コンピュータのみです。V2V移行の詳細については、「マシンの移行」を参照してください。新規または既存のコンピュータに復元するかどうかを選択します。ホストを選択し、新しいコンピュータ名を指定するか、既存のターゲット コンピュータを選択します。[OK] をクリックします。必要な追加の復元オプションを設定します。
（Virtuozzo Hybrid InfrastructureおよびScale Computing HC3では利用不可）仮想マシンのデータストアを選択するには、[データストア]（ESXi）、[パス]（Hyper-VおよびVirtuozzo）、または [ストレージドメイン]（Red Hat Virtualization/oVirt）をクリックしてから、仮想マシンのデータストア（ストレージ）を選択します。各仮想ディスクのデータストア（ストレージ）、インターフェース、プロビジョニングモードを表示するには、[ディスクマッピング] をクリックします。VirtuozzoコンテナまたはVirtuozzo Hybrid Infrastructure仮想マシンの復元中でなければ、これらの設定を変更できま

す。Virtuozzo Hybrid Infrastructureの場合、ターゲットディスクに対して選択できるのはストレージポリシーのみです。設定する場合、対象のターゲットディスクを選択し、[変更] をクリックします。ブレードが開いたら、ギアアイコンをクリックし、ストレージポリシーを選択して [完了] をクリックします。マッピングセクションでは、復元対象の個別のディスクを選択することもできます。

（VMware ESXi、Hyper-V、Virtuozzoで利用可能）仮想マシンのメモリサイズ、プロセッサー数、ネットワーク接続を変更するには、[VM設定] をクリックします。（Virtuozzo Hybrid Infrastructure向け）仮想マシンのメモリサイズ、プロセッサー数を変更するには、[フレーバー] をクリックします。（プロテクションエージェントがインストールされているWindowsマシンでのみ使用可能）[安全な復元] スイッチを有効にして、リカバリデータがマルウェアに感染していないことを確認します。安全な復元の仕組みについては、"安全な復元"（1ページ）を参照してください。[復元を開始] をクリックします。既存の仮想コンピュータに復元するときには、ディスクを上書きすることを確認します。復元の進行状況は [アクティビティ] タブに表示されます。"（1ページ）および"ブータブルメディアを使用したディスクの復元"（495ページ）を参照してください。

ブータブルメディアによるマイグレーション

Cyber Protectコンソールで実行するマシンマイグレーションの代わりに、ブータブルメディアを使用してマシンをリカバリできます。

以下の場合は、ブータブルメディアを使用することをお勧めします:

- ネイティブサポートされていないマイグレーションを実行する。
  例えば、ブータブルメディアを使用して、物理マシンまたは非Virtuozzo仮想マシンをVirtuozzoホスト上のVirtuozzo仮想マシンとしてリカバリします。
- 論理ボリューム（LVM）を含むLinuxマシンのマイグレーションを実行する。
  Linuxエージェントまたはブータブルメディアを使用してバックアップを作成し、ブータブルメディアを使用してバックアップをリカバリします。
- システムのブータビリティに重要な特定のハードウェアのドライバを提供する。
  必要なドライバを使用できるブータブルメディアを構築します。詳細については、"ブータブルメディアビルダー"（692ページ）を参照してください。

Microsoft AzureおよびAmazon EC2仮想マシン

Microsoft AzureまたはAmazon EC2仮想マシンをバックアップするには、マシンにプロテクションエージェントをインストールします。バックアップおよび復元操作は、物理マシンの場合と同じです。それでも、コンピュータ数の制限値を設定すると、仮想コンピュータとしてカウントされます。

物理マシンとの違いは、Microsoft AzureおよびAmazon EC2仮想マシンは、ブータブルメディアから起動できないことです。新しいMicrosoft AzureまたはAmazon EC2仮想マシンにリカバリする必要がある場合は、次の手順に従います。

注意
以下の復元手順は、Microsoft Azureでのネイティブ実行に必要なドライバをすべて含んでいるマシンのバックアップにのみ適用されます（Azure VM、ローカルHyper-Vマシン、またはWindows Server 2016以降のソースマシンの場合）。クロスプラットフォームでの復元については、こちらのナレッジベース記事を参照してください。

Microsoft AzureまたはAmazon EC2仮想マシンとしてマシンをリカバリする手順

1. Microsoft AzureまたはAmazon EC2のイメージ/テンプレートから、新しい仮想マシンを作成します。新しいコンピュータは、復元するコンピュータと同じディスク構成である必要があります。
2. 新しいコンピュータに、Windowsエージェントまたは Linuxエージェントをインストールします。
3. 「物理マシン」の説明に従って、バックアップされたマシンを復元します。復元を構成する際に、新しいコンピュータをターゲットコンピュータとして選択します。

ブータブルメディアを作成して、オペレーティングシステムをリカバリする

ブータブルメディアとは、CD、DVD、USBフラッシュドライブ、またはその他のリムーバブルメディアであり、Linuxベースの環境、またはWindowsプレインストール環境/Windowsリカバリ環境（WinPE/WinRE）のいずれかで、オペレーティングシステムに依存せずにプロテクションエージェントを実行することができます。ブータブルメディアは主に、起動できないオペレーティングシステムのリカバリを目的としています。

注意
ブータブルメディアはハイブリッドドライブをサポートしません。

カスタムのブータブルメディアか既製のブータブルメディアか

ブータブルメディアビルダーを使用して、Windows、Linux、またはmacOSコンピューター用にカスタムのブータブルメディア（LinuxベースまたはWinPEベース）を作成することができます。LinuxベースとWinPE/WinREベースのカスタムブータブルメディアでは、自動登録、ネットワーク設定、プロキシサーバー設定などの追加設定を行うことができます。WinPE/WinREベースのカスタムブータブルメディアでは、他のドライバを追加することも可能です。

あるいは、既製のブータブルメディアをダウンロードすることもできます（Linuxベースのみ）。既製のブータブルメディアは、復元操作とUniversal Restoreへのアクセスにのみ使用できます。

Linuxベースのブータブルメディアか、WinPE/WinREベースのブータブルメディアか

Linux ベース

Linuxベースのブータブルメディアには、Linuxカーネルを基盤とする、プロテクションエージェントが含まれています。このエージェントは、任意のPC/AT互換機から起動して操作を実行することができます。ベアメタル状態のディスク、破損状態のファイルシステムやサポート対象でないファイルシステムを使用しているマシンなどからも起動することができます。

WinPE/WinREベース

WinPEベースのブータブルメディアには、Windowsプレインストール環境（WinPE）と呼ばれる最小限のWindowsシステム、およびプロテクションエージェントをプレインストール環境で実行できるように変更された、WinPE用のCyber Protectionプラグインが含まれています。WinREベースのブータブルメディアは、Windowsリカバリ環境を使用し、Windowsパッケージの追加インストールを必要としません。

WinPE は、異種のハードウェアが混在する大規模な環境では、最も便利なブータブル ソリューションであることが証明されています。

利点:

- Windowsプレインストール環境でCyber Protectionを使用すると、Linuxベースのブータブルメディアを使用するときに比べ、より多くの機能を利用できます。PC/AT互換機をWinPEで起動すると、プロテクションエージェントだけでなく、PEコマンドとPEスクリプトおよびPEに追加したその他のプラグインも使用できます。
- PEベースのブータブルメディアを使用すると、特定のRAIDコントローラーのサポートやRAIDアレーの特定レベルのみのサポートなど、Linuxに関連するブータブルメディアの複数の問題を解決できます。WinPE 2.x以降をベースとしたメディアを使用すると、必要なデバイスドライバを動的に読み込むことができます。

制限事項:

- バージョン 4.0 より前の WinPE ベースのブータブル メディアは、Unified Extensible Firmware Interface（UEFI）を使用するコンピュータでは起動しません。

物理的なブータブルメディアの作成

ディスクレベルバックアップの利用を開始するタイミングでブータブルメディアを作成し、テストすることを強く推奨します。また、保護エージェントのメジャーアップデートを行うたびにメディアを再作成することもお勧めします。

同じメディアを使用して、WindowsまたはLinuxのどちらかを復元できます。macOS を復元するには、macOS を実行しているマシンで別のメディアを作成します。

WindowsまたはLinuxの物理的なブータブルメディアの作成手順

1. カスタムブータブルメディアのISOファイルを作成するか、既製のISOファイルをダウンロードします。

   カスタムISOファイルを作成するには、"ブータブルメディアビルダー"（692ページ）を使用します。

   事前構成済みのISOファイルをダウンロードするには、Cyber Protectコンソールでマシンを選択して、[**リカバリ**] > [**その他のリカバリ方法...**] > [**ISOイメージのダウンロード**] の順にクリックします。
2. （オプション）Cyber Protectコンソールで、登録トークンを生成します。既製のISOファイルをダウンロードすると、登録トークンが自動的に表示されます。

   このトークンを使用すると、ログイン名とパスワードの入力を求められることなく、ブータブルメディアからクラウドストレージにアクセスできます。
3. 次のいずれかの方法で、物理的なブータブルメディアを作成します。
   - CD/DVDにISOファイルを書き込みます。
   - オンラインで入手可能なフリーツール

     UEFIマシンを起動する必要がある場合は`ISO to USB`または`RUFUS`を使用し、BIOSマシンには`Win32DiskImager`を使用します。Linux では、`dd` ユーティリティを使用するのが適切です。

   仮想マシンの場合、ISOファイルをCD/DVDドライブとして、リカバリする仮想マシンに接続します。

macOSの物理的なブータブルメディアの作成手順

1. Macエージェントがインストールされたマシンで、[**アプリケーション**] >[**レスキューメディアビルダー**] の順にクリックします。
2. 接続されたリムーバブルメディアが、ソフトウェアに表示されます。ブータブルにするメディアを選択します。

   警告
   ディスク上のすべてのデータが消去されます。
3. [**作成**] をクリックします。
4. ブータブルメディアが作成されるのを待ちます。

ブータブルメディアビルダー

ブータブルメディアビルダーは、ブータブルメディアを作成するための専用ツールです。プロテクションエージェントがインストールされているマシンに、オプションのコンポーネントとしてインストールされます。

ブータブルメディアビルダーを使用する理由

Cyber Protectコンソールでダウンロードできる事前構成済みのブータブルメディアは、Linuxカーネルを基盤としています。Windows PEとは異なり、そのままカスタムドライバを挿入できません。

ブータブルメディアビルダーでは、カスタマイズされたLinuxベースおよびWinPEベースのブータブルメディアイメージを作成することができます。

32ビットか64ビットか

ブータブルメディアビルダーは、32ビットと64ビットの両方のコンポーネントで、ブータブルメディアを作成します。UEFI（Unified Extensible Firmware Interface）を使用するマシンを起動するには、通常は64ビットメディアが必要です。

Linux ベースのブータブル メディア

Linux ベースのブータブル メディアを作成するには

1. **ブータブルメディアビルダー**を起動します。
2. **[ブータブルメディアの種類]** で **[デフォルト（Linuxベースメディア）]** を選択します。
3. ボリュームおよびネットワークリソースの表記方法を選択します。
   - Linux形式でボリューム表記を行うブータブルメディアでは、ボリュームがhda1、sdb2のように表示されます。復元の開始前に、MDデバイスおよび論理ボリューム（LVM）を再構築しようとします。
   - Windows形式でボリューム表記を行うブータブルメディアでは、ボリュームがC:、D:のように表示されます。これにより、ダイナミックボリューム（LDM）にアクセスできます。
4. （オプション）Linux カーネルのパラメータを指定します。複数のパラメータは、スペースで区切って入力します。

   例えば、メディアを起動するたびにブータブルエージェントのディスプレイモードを選択できるようにするには、「**vga=ask**」と入力します。利用可能なパラメータの詳細情報については、「"カーネル パラメータ"（694ページ）」を参照してください。
5. （オプション） ブータブルメディアの言語を選択します。
6. （オプション） 復元後にWindowsで使用される起動モード（BIOSまたはUEFI）を選択します。
7. メディアに配置するコンポーネントを選択します - Cyber Protectionブータブルエージェント。
8. （オプション） ブートメニューのタイムアウト間隔を指定します。この設定が行われていない場合は、オペレーティングシステム（存在する場合）またはコンポーネントを起動するかどうかを選択するまで、 ローダーは待機します。
9. （オプション） ブータブルエージェントの操作を自動化する場合、**[次のスクリプトを使用する]** チェックボックスをオンにします。いずれかのスクリプトを選択し、スクリプトパラメータを指定します。スクリプトの詳細情報については、「"ブータブルメディアのスクリプト"（696ページ）」を参照してください。
10. （オプション） 起動時にブータブルメディアをCyber Protectionサービスに登録する方法を選択します。登録設定の詳細については、「"ブータブルメディアの登録"（704ページ）」を参照してください。
11. 起動したマシンで使用するネットワークアダプタのネットワーク設定を指定するか、自動DHCP構成を維持します。
12. （オプション） プロキシサーバーがネットワークで有効な場合、ホスト名/IPアドレスとポートを指定します。
13. 作成したブータブルメディアのファイルタイプを選択します。

- ISO イメージ
- ZIPファイル

14. ブータブルメディアファイルのファイル名を指定します。
15. サマリー画面で設定を確認し、**[実行]** をクリックします。

カーネル パラメータ

Linuxカーネルのパラメータを1つまたは複数指定できます。パラメータは、ブータブルメディアの起動時に自動的に適用されます。これらのパラメータは、通常、ブータブルメディアの操作中に問題が発生する場合に使用されます。通常は、このフィールドは空のままにできます。

ブートメニューでF11キーを押し、これらのパラメータのいずれかを指定することも可能です。

パラメータ

複数のパラメータを指定する場合、パラメータをスペースで区切ります。

- **acpi=off**
  Advanced Configuration and Power Interface（ACPI）を無効にします。特定のハードウェア構成で問題が発生した場合、このパラメータを使用します。
- **noapic**
  Advanced Programmable Interrupt Controller（APIC）を無効にします。特定のハードウェア構成で問題が発生した場合、このパラメータを使用します。
- **vga=ask**
  ブータブル メディアのグラフィカル ユーザー インターフェイスによって使用されるビデオ モードを要求するメッセージが表示されます。**vga** パラメータを指定しない場合、ビデオモードは自動的に検出されます。
- **vga**= mode_number
  ブータブル メディアのグラフィカル ユーザー インターフェイスによって使用されるビデオ モードを指定します。モード番号は、mode_number に 16 進数で指定します。たとえば、**vga=0x318** のように指定します。
  モード番号に対応する画面の解像度と色数は、マシンによって異なる場合があります。最初に **vga=ask**パラメータを使用して、mode_numberの値を選択することをお勧めします。
- **quiet**
  Linux カーネルが読み込まれる際のスタートアップ メッセージの表示を無効にして、カーネルが読み込まれた後に管理コンソールを開始します。
  このパラメータは、ブータブルメディアの作成時に自動的に指定されますが、ブートメニューで削除することができます。
  このパラメータを削除すると、コマンドプロンプトが表示される前にすべての起動メッセージが表示されます。コマンドプロンプトから管理コンソールを開始するには、**/bin/product** コマンドを実行します。
- **nousb**
  USB（Universal Serial Bus）サブシステムの読み込みを無効にします。
- **nousb2**

USB 2.0 のサポートを無効にします。このパラメータを指定しても、USB 1.1 デバイスは動作します。このパラメータを指定すると、USB 2.0 モードでは動作しない一部の USB ドライブを USB 1.1 モードで使用できます。

- **nodma**
  すべての IDE ハード ディスク ドライブの Direct Memory Access（DMA）を無効にします。一部のハードウェアでカーネルがフリーズするのを防ぎます。
- **nofw**
  FireWire（IEEE1394）インターフェイスのサポートを無効にします。
- **nopcmcia**
  PCMCIAハードウェアの検出を無効にします。
- **nomouse**
  マウスのサポートを無効にします。
- module_name =**off**
  module_name に指定した名前のモジュールを無効にします。たとえば、SATA モジュールの使用を無効にするには、**sata_sis=off** と指定します。
- **pci=bios**
  ハードウェア デバイスに直接アクセスせず、PCI BIOS を強制的に使用します。コンピュータに非標準の PCI ホスト ブリッジが存在している場合は、このパラメータを使用します。
- **pci=nobios**
  PCI BIOS の使用を無効にします。ハードウェアへの直接アクセスのみを許可します。BIOS が原因でブータブル メディアを起動できない場合など、このパラメータを使用します。
- **pci=biosirq**
  PCI BIOS の呼び出しを使用して、割り込みルーティング テーブルを取得します。カーネルが、割り込み要求（IRQ）を割り当てられなかったり、マザーボード上のセカンダリ PCI バスを検出できなかったりする場合、このパラメータを使用します。
  これらの呼び出しは、一部のコンピュータで正しく動作しない可能性があります。しかし、この呼び出し以外に割り込みルーティング テーブルを取得する方法はありません。
- **LAYOUTS=en-US, de-DE, fr-FR, ...**
  ブータブルメディアのグラフィカルユーザーインターフェースで使用できるキーボードレイアウトを指定します。
  このパラメータを指定していない場合、使用できるレイアウトは 2 つのみです。英語（USA）とメディアのブートメニューで選択した言語に対応するレイアウトを使用できます。
  次の任意のレイアウトを選択できます。
  ベルギー語: **be-BE**
  チェコ語: **cz-CZ**
  英語: **en-GB**
  英語（米国）: **en-US**
  フランス語: **fr-FR**
  フランス語（スイス）: **fr-CH**
  ドイツ語: **de-DE**

ドイツ語（スイス）: **de-CH**

イタリア語: **it-IT**

ポーランド語: **pl-PL**

ポルトガル語: **pt-PT**

ポルトガル語（ブラジル）: **pt-BR**

ロシア語: **ru-RU**

セルビア語（キリル）: **sr-CR**

セルビア語（ラテン）: **sr-LT**

スペイン語: **es-ES**

ブータブルメディアの環境下で作業するときは、CTRLキーとSHIFTキーを同時に使用して、使用可能なレイアウトをローテーションして表示させます。

ブータブルメディアのスクリプト

ブータブルメディアにより事前定義された一連の操作を実行したい場合は、ブータブルメディアビルダーでメディアを作成する際にスクリプトを指定できます。これにより、メディアからマシンが起動されるたびに指定されたスクリプトが実行されるようになり、ユーザーインターフェースが表示されることはありません。

定義済みスクリプトのいずれかを選択することも、スクリプト規則に従ってカスタムスクリプトを作成することもできます。

定義済みスクリプト

ブータブルメディアビルダは、次の定義済みスクリプトを提供しています。

- クラウドストレージからの復元（**entire_pc_cloud**）
- ネットワーク共有からの復元（**entire_pc_share**）

スクリプトは、ブータブルメディアビルダーがインストールされたマシン上の次のフォルダに配置されます。

- Windowsの場合: %**ProgramData%¥Acronis¥MediaBuilder¥scripts¥**
- Linuxの場合: **/var/lib/Acronis/MediaBuilder/scripts/**

クラウド ストレージからのバックアップ

ブータブルメディアビルダで、次のスクリプトパラメータを指定します。

1. バックアップファイル名。
2. （オプション） スクリプトが暗号化されたバックアップにアクセスする際に使用するパスワードです。

ネットワーク共有からの復元

ブータブルメディアビルダで、次のスクリプトパラメータを指定します。

- バックアップのネットワーク共有のパスです。
- ネットワーク共有のユーザー名とパスワード。
- バックアップファイル名。バックアップファイル名を確認するには:
  a. Cyber Protectコンソールで、**[バックアップストレージ]** > **[ロケーション]** に移動します。
  b. ネットワーク共有を選択します（共有が表示されていない場合は、**[ロケーションの追加]** をクリックします）。
  c. バックアップを選択します。
  d. **[詳細]** をクリックします。**[バックアップファイル名]** にファイル名が表示されます。
- （オプション） スクリプトが暗号化されたバックアップにアクセスする際に使用するパスワードです。

カスタムスクリプト

重要
カスタムスクリプトの作成には、Bashコマンド言語およびJavaScriptオブジェクト表記法（JSON）の知識が必要です。Bashを使い慣れていない場合は、http://www.tldp.org/LDP/abs/htmlなどで学ぶことができます。JSON の仕様については、http://www.json.org を参照してください。

スクリプトのファイル

スクリプトは、ブータブルメディアビルダーがインストールされたマシン上の次のディレクトリに置かれている必要があります。

- Windows の場合: %**ProgramData%¥Acronis¥MediaBuilder¥scripts¥**
- Linux の場合: **/var/lib/Acronis/MediaBuilder/scripts/**

スクリプトは3つ以上のファイルで構成されている必要があります。

- **<script_file>.sh**:Bashスクリプトを含むファイルスクリプト作成時には、https://busybox.net/downloads/BusyBox.html に記載されている限られたシェルコマンドのみを使用します。また、次のコマンドを使用できます。
  - `acrocmd`: バックアップと復元のコマンドラインユーティリティ
  - `product`: ブータブルメディアのユーザーインターフェースを開始するコマンド

  このファイルおよび（たとえば、dot コマンドを使用することによって）スクリプトに含まれるその他のファイルは、**bin** サブフォルダに置かれている必要があります。スクリプトでは、**/ConfigurationFiles/bin/<some_file>** としてその他のファイルパスを指定します。
- **autostart**:**<script_file>.sh**を開始するためのファイル。ファイルには以下が含まれている必要があります。

```
#!/bin/sh
. /ConfigurationFiles/bin/variables.sh
. /ConfigurationFiles/bin/<script_file>.sh
. /ConfigurationFiles/bin/post_actions.sh
```

- **autostart.json**: 以下を含むJSONファイル

- ブータブルメディアビルダーに表示されるスクリプト名と説明。
- ブータブルメディアビルダーを使用して設定するスクリプトの変数名。
- 各変数に関してブータブルメディアビルダに表示されるコントロールのパラメータ

autostart.jsonの構造

トップレベルオブジェクト

ペア		必須	説明
名前	値の種類		
displayName	文字列	はい	ブータブルメディアビルダに表示されるスクリプト名
description	文字列	いいえ	ブータブルメディアビルダに表示されるスクリプトの説明
timeout	数字	いいえ	スクリプト開始前のブートメニューのタイムアウト（秒）ペアが指定されていない場合、タイムアウトは 10 秒です。
variables	オブジェクト	いいえ	ブータブルメディアビルダを使用して設定する**<script_file>.sh**の任意の変数 値は、変数の文字列IDおよび変数のオブジェクトの一連のペアである必要があります（次の表を参照）。

変数オブジェクト

ペア		必須	説明
名前	値の種類		
displayName	文字列	はい	**<script_file>.sh**で使用される変数名
type	文字列	はい	ブータブルメディアビルダに表示されるコントロールの種類このコントロールは、変数の値を設定するために使用されます。 サポートされている種類については、次の表を参照してください。
description	文字列	はい	ブータブルメディアビルダでコントロールの上に表示されるコントロールラベル
default	typeが string、multiString、password、または enum なら文字列	いいえ	コントロールのデフォルト値ペアが指定されていない場合、デフォルト値はコントロールの種類に基づき空の文字列またはゼロになります。 チェックボックスのデフォルト値には 0（選択されていない状態）または 1（選択された状態）を指定できます。

	種類が number、spinner、または checkbox なら数字		
order	数字 （自然数）	はい	ブータブルメディアビルダ内でのコントロールの順番値が高いほど、コントロールは、**autostart.json**に定義された他のコントロールに対して低く配置されます。初期値は 0 である必要があります。
min （spinner のみ）	数字	いいえ	スピンボックス内のスピンコントロールの最小値ペアが指定されていない場合、値は 0 となります。
max （spinner のみ）	数字	いいえ	スピンボックス内のスピンコントロールの最大値ペアが指定されていない場合、値は 100 となります。
step （spinner のみ）	数字	いいえ	スピンボックス内のスピンコントロールの段階値ペアが指定されていない場合、値は 1 となります。
items （enum のみ）	文字列一覧	はい	ドロップダウンリストの値。
required （string、multiString、password、および enum）	数字	いいえ	コントロール値として、空（0）または拒否（1）を許可するかどうかを指定します。ペアが指定されていない場合、コントロール値は空にできます。

コントロールの種類

名前	説明
string	短い文字列の入力または編集に使用する1行の制約なしのテキストボックス
multiString	長い文字列の入力または編集に使用する複数行の制約なしのテキストボックス
password	パスワードを安全に入力するために使用する1行の制約なしのテキストボックス
number	数字の入力または編集に使用する1行の数字のみのテキストボックス
spinner	数字の入力または編集に使用する1行の数字のみのスピンコントロール付きテキストボックススピンボックスとも呼ばれています。
enum	固定された一連の事前定義済みの値を含む標準ドロップダウンリスト

checkbox	2つの状態（選択されていない状態または選択された状態）があるチェックボックス。

次の**autostart.json**の例には、**<script_file>.sh**の変数設定に使用できるすべての種類のコントロールが含まれています。

```
{
        "displayName":"自動スタートスクリプト名"、
        "description":"これは自動スタートスクリプトの説明です。"、
        "variables": {
                "var_string": {
                        "displayName": "VAR_STRING",
                        "type":"string", "order": 1,
                        "description":"これは'文字列'の制御です:", "デフォルト":"Hello, world!"
                },
                "var_multistring": {
                        "displayName": "VAR_MULTISTRING",
                        "type": "multiString", "order":2,
                        "description":"これは'multiString'の制御です:",
                        "default":"Lorem ipsum dolor sit amet,\nconsectetur adipiscing elit."
                },
                "var_number": {
                        "displayName":"VAR_NUMBER",
                        "type":"number", "order":3,
                        "description":"これは'数字'の制御です:", "デフォルト":10
                },
                "var_spinner": {
                        "displayName":"VAR_SPINNER",
                        "type":"spinner", "order":4,
                        "description":"これは'スピナー'の制御です:",
                        "min":1, "max":10, "step":1, "default":5
                },
                "var_enum": {
```

```
                "displayName":"VAR_ENUM",
                "type":"enum", "order":5,
                "description":"これは'enum'の制御です:",
                "items": ["1 番目", "2 番目", "3 番目"], "デフォルト": "2 番目"
        },
        "var_password": {
                "displayName":"VAR_PASSWORD",
                "type":"password", "order":6,
                "description":"これは'パスワード'制御です:", "デフォルト": "qwe"
        },
        "var_checkbox": {
                "displayName":"VAR_CHECKBOX",
                "type":"checkbox", "order":7,
                "description":"これは'checkbox'制御です", "デフォルト":1
        }
    }
}
```

WinPEベースおよびWinREベースのブータブルメディア

準備作業を追加することなくWinREイメージを作成できます。もしくは、Windows自動インストールキット（AIK）かWindowsアセスメント&デプロイメントキット（ADK）をインストールしてからWinPEイメージを作成することもできます。

WinREイメージ

WinREイメージの作成は、以下のオペレーティングシステムでサポートされています。

- Windows 7（64ビット）
- Windows 8（32ビットおよび64ビット）
- Windows 8.1（32ビットおよび64ビット）
- Windows 10（32ビットおよび64ビット）
- Windows 11（64ビット）
- Windows Server 2012（64ビット）
- Windows Server 2016（64ビット）
- Windows Server 2019（64ビット）
- Windows Server 2022（64ビット）

WinPEイメージ

Windows自動インストールキット（AIK）またはWindowsアセスメント&デプロイメントキット（ADK）のインストール後、ブータブルメディアビルダーは、次のカーネルを基にしたWinPEディストリビューションをサポートします。

- Windows Vista (PE 2.0)
- Windows Vista SP1 および Windows Server 2008（PE 2.1）
- Windows 7（PE 3.0）（Windows 7 SP1（PE 3.1）が適用されている、またはされていない）
- Windows 8 (PE 4.0)
- Windows 8.1 (PE 5.0)
- Windows 10 (PE 10.0.1xxx)
- Windows 11 (PE 10.0.2xxx)

ブータブル メディア ビルダは 32 ビットと 64 ビットの両方の WinPE ディストリビューションをサポートします。32 ビット WinPE ディストリビューションは、64 ビット ハードウェアでも機能します。しかし、UEFI（Unified Extensible Firmware Interface）を使用するコンピュータを起動するには、64 ビットディストリビューションが必要です。

注意
WinPE 4 以降がベースの PE イメージが機能するには、約 1 GB の RAM が必要です。

WinPEまたはWinREブータブルメディアの作成

ブータブルメディアビルダーは、Cyber ProtectionとWinPEおよびWinREを統合するための2つの方法を提供します。

- Cyber Protectionプラグインを使って、初期状態からISOファイルを作成します。
- 今後考えられる任意の目的（手動によるISOのビルド、イメージへの他のツールの追加など）のために、Cyber ProtectionプラグインをWIMファイルに追加します。

WinPEまたはWinREブータブルメディアを作成するには

1. プロテクションエージェントがインストールされているマシン上で、ブータブルメディアビルダーを実行します。
2. **[ブータブルメディアタイプ]**で、**[Windows PE]** または **[Windows PE（64ビット）]** を選択します。UEFI（Unified Extensible Firmware Interface）を使用するコンピュータを起動するには、64 ビット メディアが必要です。
3. ブータブルメディアのサブタイプを選択します。**[WinRE]** または **[WinPE]** です。
   WinREブータブルメディアの作成には、追加パッケージのインストールは必要ありません。
   64ビットのWinPEメディアを作成するには、Windows自動インストールキット（AIK）かWindowsアセスメント&デプロイメントキット（ADK）をダウンロードする必要があります。32ビットのWinPEメディアを作成するには、AIKまたはADKのダウンロードに加えて、次の操作が必要になります。

a. **[プラグインfor WinPE（32ビット）をダウンロード]** をクリックします。
b. プラグインを**%PROGRAM_FILES%¥BackupClient¥BootableComponents¥WinPE32**に保存します。

4. （オプション） ブータブルメディアの言語を選択します。
5. （オプション） 復元後にWindowsで使用される起動モード（BIOSまたはUEFI）を選択します。
6. 起動したマシンで使用するネットワークアダプタのネットワーク設定を指定するか、自動DHCP構成を維持します。
7. （オプション） 起動時にブータブルメディアをCyber Protectionサービスに登録する方法を選択します。登録設定の詳細については、「"ブータブルメディアの登録"（704ページ）」を参照してください。
8. （オプション）ブータブルメディアに追加するWindowsドライバを指定します。
   Windows PEまたはWindows REでマシンを起動すると、ドライバにより、バックアップが保存されているデバイスにアクセスすることができます。32ビットのWinPEまたはWinREディストリビューションを使用する場合は、32ビットドライバを追加します。64ビットのWinPEまたはWinREディストリビューションを使用する場合は、64ビットドライバを追加します。
   ドライバを追加する手順は、次のとおりです。
   - **[追加]** をクリックし、対応するSCSI、RAID、SATAコントローラー、ネットワークアダプタ、テープドライブ、その他のデバイスに必要な.infファイルのパスを指定します。
   - 生成されるWinPEまたはWinREメディアに追加するドライバごとに、この手順を繰り返します。
9. 作成したブータブルメディアのファイルタイプを選択します。
   - ISO イメージ
   - WIM イメージ
10. 作成するイメージファイルのフルパスを、ファイル名を含めて指定します。
11. サマリー画面で設定を確認し、**[実行]** をクリックします。

生成されるWIMファイルからPEイメージ（ISOファイル）を作成するには

- Windows PE フォルダ内のデフォルトの boot.wim ファイルを、新しく作成した WIM ファイルに置き換えます。上の例では、次のように入力します。

```
c:\RecoveryWIMMedia.wim c:\winpe_x86\ISO\sources\boot.wimをコピーします
```

- **Oscdimg**ツールを使用します。上の例では、次のように入力します。

```
oscdimg -n -bc:\winpe_x86\etfsboot.com c:\winpe_x86\ISO c:\winpe_x86\winpe_x86.iso
```

警告
この例をコピーして貼り付けないでください。コマンドを手動で入力しないと、処理に失敗します。

準備:WinPE 2.x および 3.x

PE 2.xまたは3.xイメージを作成または変更できるようにするには、ブータブルメディアビルダーとWindows自動インストールキット（AIK）を同じマシンにインストールします。

マシンの準備

1. MicrosoftのWebサイトから、以下の手順でAIKイメージファイルをダウンロードします。
   - Windows Vista (PE 2.0) の場合: https://www.microsoft.com/ja-jp/download/details.aspx?id=10333
   - Windows Vista SP1 および Windows Server 2008 (PE 2.1) の場合: https://www.microsoft.com/ja-jp/download/details.aspx?id=9085
   - Windows 7 (PE 3.0) の場合: https://www.microsoft.com/ja-jp/download/details.aspx?id=5753
     Windows 7 SP1 (PE 3.1) には、https://www.microsoft.com/ja-jp/download/details.aspx?id=5188にあるAIK補足プログラムも必要です。
2. イメージファイルをDVDディスクまたはUSBフラッシュドライブに書き込みます。
3. イメージファイルから以下をインストールします。
   - Microsoft .NET Framework（ハードウェアによりNETFXx86かNETFXx64のどちらか）
   - MSXML（マイクロソフトXMLパーサー）
   - Windows AIK
4. 同じコンピュータにブータブル メディア ビルダをインストールします。

準備:WinPE 4.0 以降

PE 4以降のイメージを作成または変更するには、ブータブルメディアビルダーとWindows アセスメント & デプロイメントキット（ADK）を同じマシンにインストールします。

マシンの準備

1. MicrosoftのWebサイトからADKセットアップ プログラムをダウンロードします。
   以下のWindowsバージョンに対応しています。
   - Windows 11 (PE 10.0.2xxx)
   - Windows 10 (PE 10.0.1xxx)
   - Windows 8.1（PE 5.0）
   - Windows 8（PE 4.0）
2. セスメント&デプロイメントキットをインストールします。
3. ブータブルメディアビルダーをインストールします。

ブータブルメディアの登録

ブータブルメディアをCyber Protectionサービスに登録することで、バックアップ用のクラウドストレージにアクセスできるようになります。ブータブルメディアを作成している間に、登録の事前構成を実行できます。登録の事前構成が行われていない場合は、該当メディアでマシンを起動した後に登録することができます。

Cyber Protectionサービスで、登録の事前構成を行うには

1. ブータブルメディアビルダーで、**[ブータブルメディアの登録]** に移動します。
2. **[サービスURL]** で、Cyber Protectionサービスのアドレスを指定します。
3. （オプション）**[表示名]** で、起動するマシンの名前を指定します。
4. Cyber Protectionサービスで自動登録を設定するには、**[自動的にブータブルメディアを登録]** チェックボックスを選択してから、自動登録のレベルを選択します。

- **起動時に登録トークンを確認**
  このトークンは、ブータブルメディアからマシンを起動するたびに指定する必要があります。
- **次のトークンを使用する**
  ブータブルメディアから起動すると、マシンが自動的に登録されます。

ブータブルメディアからマシンを起動した後に、ブータブルメディアを登録するには

1. ブータブル メディアからコンピュータを起動します。
2. 起動ウィンドウで、**[メディアの登録]** をクリックします。
3. **[サーバー]** で、Cyber Protectionサービスのアドレスを指定します。
4. **[登録トークン]** で、登録トークンを入力します。
5. **[登録]** をクリックします。

ネットワーク設定

ブータブルメディアを作成している間に、ブータブルエージェントが使用するネットワーク接続を事前構成できます。次のパラメータを事前構成できます。

- IPアドレス
- サブネット マスク
- ゲートウェイ
- DNS サーバー
- WINSサーバー

マシンでブータブルエージェントが起動すると、マシンのネットワークインターフェースカードカード（NIC）に設定が適用されます。設定が事前構成されていない場合、エージェントでDHCP自動設定が使用されます。

マシンでブータブルエージェントを実行しているときに、手動でネットワーク設定を構成することもできます。

複数のネットワーク接続の事前構成

最大で10個のネットワークインターフェースカード（NIC）のTCP/IP設定を事前構成できます。それぞれの NIC に適切な設定が割り当てられるようにするには、メディアをカスタマイズするサーバー上でメディアを作成します。ウィザードのウィンドウで既存のNICを選択すると、メディアに保存するNICの設定が選択されます。既存の NIC それぞれの MAC アドレスもメディアに保存されます。

MACアドレス以外の設定を変更したり、存在しないNICの設定を構成したりすることもできます。

サーバーでブータブルエージェントが起動すると、エージェントは使用可能なNICの一覧を取得します。この一覧は、NICが使用するスロットを基準として（プロセッサーに最も近いものから順番に）並べ替えられます。

ブータブルエージェントは、既知のNICそれぞれに適切な設定を割り当て、MACアドレスによってNICを識別します。既知のMACアドレスでNICを設定した後、残りのNICには、上位の未割り当てNICから順に、存在しないNICに対して作成した設定が割り当てられます。

メディアを作成したマシンだけでなく、任意のマシンのブータブルメディアをカスタマイズできます。そのために、そのマシンのスロットの順序に従ってNICを設定します。つまりNIC1がプロセッサーに最も近いスロットを使用し、NIC2が次のスロットを使用するようにします。以下同様に構成します。該当のマシンでブータブルエージェントが起動した際に、既知のMACアドレスを持つNICが見つからない場合は、カスタマイズしたときと同じ順序でNICが設定されます。

例

ブータブルエージェントは、稼働中のネットワークを経由して管理コンソールと通信するため、いずれかのネットワークアダプタを使用できます。自動設定でこの接続の設定を行うことができます。復元用の大きなデータは、静的なTCP/IP設定でバックアップ専用のネットワークに接続された、2番目のNICを経由して転送できます。

ブータブルメディアから起動したマシンへの接続

ローカル接続

ブータブルメディアから起動したマシンで直接操作するには、スタートアップウィンドウで **[このコンピュータをローカルで管理]** をクリックします。

ブータブルメディアからマシンを起動すると、マシン端末にスタートアップウィンドウが表示され、DHCPから取得したIPアドレスか、あらかじめ構成された値に設定されたIPアドレスが表示されます。

ネットワーク設定

現行セッションのネットワーク設定を変更するには、スタートアップウィンドウで **[ネットワークの設定]** をクリックします。**[ネットワークの設定]** ウィンドウが表示されます。このウィンドウでは、マシンの各ネットワークインターフェースカード（NIC）についてネットワーク設定を行うことができます。

セッション中に行った変更は、マシンを再起動すると失われます。

VLAN の追加

[ネットワークの設定] ウィンドウでは、仮想ローカルエリアネットワーク（VLAN）を追加できます。特定の VLAN に存在するバックアップ ロケーションにアクセスする必要がある場合は、この機能を使用してください。

VLAN は、通常、ローカル エリア ネットワークをセグメントに分割するために使用されます。スイッチのaccessポートに接続されているNICは、ポート設定で指定されたVLANに必ずアクセスできます。スイッチのtrunkポートに接続されているNICは、ネットワーク設定でVLANを指定した場合に限り、ポート設定で許可されたVLANにアクセスできます。

トランク ポート経由で VLAN にアクセスできるようにするには

1. **[VLANの追加]** をクリックします。
2. 必要な VLAN を含むローカル エリア ネットワークへのアクセスを提供する NIC を選択します。
3. VLAN ID を指定します。

[OK] をクリックすると、ネットワークアダプターのリストに新しいエントリが表示されます。

VLANを削除する必要がある場合は、目的のVLANエントリをクリックし、**[VLANを削除]** をクリックします。

ブータブルメディアのローカル処理

ブータブルメディアの操作は、実行中のオペレーティングシステムで実行される復元操作に似ています。違いは次のとおりです。

1. Windows形式のブータブルメディアのボリューム表示は、Windowsボリュームのドライブ文字の表示と同じになります。Windowsのドライブ文字がないボリューム（システム予約済みボリュームなど）には、ディスク上の順序に従って空きドライブ文字が割り当てられます。
   ブータブルメディアがマシン上の Windows を検出できない場合や複数の Windows を検出した場合は、すべてのボリューム（ドライブ文字が割り当てられていないドライブも含む）に、ディスク上の順序に従って文字が割り当てられます。このように、ボリュームのドライブ文字が Windows の文字とは異なることがあります。たとえば、ブータブル メディアでは D: ドライブが Windows の E: ドライブに対応することがあります。

   注意
   各ボリュームに一意の名前を割り当てておくことをお勧めします。

2. Linux形式のボリュームのブータブルメディアでは、ローカルディスクとボリュームがアンマウント（sda1、sda2...）として表示されます。
3. タスクをスケジュールできません。操作を繰り返す必要がある場合は、操作手順を最初から設定します。
4. ログは、現在のセッションの期間内だけ有効です。ログ全体またはフィルタ処理されたログ エントリをファイルに保存できます。

ディスプレイ モードの設定

Linux ベースのブータブルメディアでマシンを起動すると、ディスプレイ ビデオ モードがハードウェア構成（モニターおよびグラフィック カードの仕様）に基づいて自動的に検出されます。正しくないビデオ モードが検出された場合は、次の操作を行います。

1. ブート メニューで [F11] を押します。
2. コマンドラインで**vga=ask**と入力し、起動を続行します。
3. サポートされているビデオモードの一覧から、該当する数字（**318** など）を入力して適切なモードを1つ選択し、**Enter**を押します。

特定のハードウェア構成を起動するたびに、この手順を繰り返したくない場合は、**[カーネルパラメータ]** フィールドで適切なモード番号（**vga=0x318**など）を指定して、ブータブルメディアを再作成します。

オンプレミスでのブータブルメディアによる復元

1. ブータブルメディアからマシンを起動します。
2. **[このコンピュータをローカルで管理]** をクリックします。
3. **[復元]** をクリックします。
4. **[復元元]** で **[データの選択]** をクリックします。
5. リカバリするバックアップファイルを選択します。
6. 左下のペインで、リカバリするドライブ/ボリューム（またはファイル/フォルダ）を選択し、**[OK]** をクリックします。
7. 上書きルールを構成します。
8. 復元除外を構成します。
9. 復元オプションを構成します。
10. 設定が正しいことを確認し、**[OK]**をクリックします。

ブータブルメディアのリモート操作

注意
この機能は、Advanced Backupパックで利用可能です。

ブータブルメディアをCyber Protectコンソールで確認には、まず登録する必要があります（"ブータブルメディアの登録"（704ページ）を参照）。

メディアをCyber Protectコンソールで登録すると **[デバイス]** > **[ブータブルメディア]** タブに表示されるようになります。30日を越えてオフラインとなっているブータブルメディアは、このタブに表示されません。

ブータブルメディアはCyber Protectコンソールでリモート管理できます。例えば、データのリカバリ、メディアで起動したマシンの再起動やシャットダウン、メディアに関する情報、アクティビティ、アラートの表示などが可能です。

重要
ブータブルメディアをリモートでアップデートすることはできません。ブータブルメディアのアップデートは、コンソールの **[設定]** > **[エージェント]** タブから実行します。

ブータブルメディアをアップデートするには、新しく作成してください（"ブータブルメディアビルダー"（692ページ）セクションを参照）。または、アカウントアイコンをクリックして、コンソールの **[ダウンロード]** > **[ブータブルメディア]** で、事前構成済みのメディアをダウンロードすることもできます。

ブータブルメディアのファイル/フォルダをリモートでリカバリするには

1. Cyber Protectコンソールで、**[デバイス]** > **[ブータブルメディア]** に進みます。
1. データ復元に使用するメディアを選択します。
2. **[復元]** をクリックします。

3. ロケーションを選択し、必要なバックアップを選択します。バックアップは、ロケーションでフィルタされます。
4. 復元ポイントを選択して、**[ファイル/フォルダをリカバリ]** をクリックします。
5. 目的のフォルダを直接参照するか、検索バーを使用して目的のファイルおよびフォルダの一覧を取得します。

   検索は言語に依存しません。

   1つ以上のワイルドカード文字（*および?）を使用できます。ワイルドカードの使用に関する詳細については、"ファイルフィルタ（除外/包含）"（450ページ）を参照してください。
6. リカバリするファイルを選択してから、**[復元]** をクリックします。
7. **[パス]** で、復元先を選択します。
8. （オプション） 高度な復元構成を実行するには、**[復元オプション]** をクリックします。詳細については、"復元オプション"（507ページ）を参照してください。
9. **[復元を開始]** をクリックします。
10. 次のいずれかのファイル上書きオプションを選択します。
    - **[既存のファイルを上書きする]**
    - **[既存のファイルが古い場合は上書きする]**
    - **[既存のファイルを上書きしない]**

    コンピュータを自動的に再起動するかどうかを選択します。
11. **[実行]** をクリックすると、復元が開始します。復元の進行状況は **[アクティビティ]** タブに表示されます。

ブータブルメディアを使用してディスク、ボリューム、またはマシン全体をリモートでリカバリするには

1. **[デバイス]** タブで、**[ブータブルメディア]** グループに移動し、データ復元に使用するメディアを選択します。
2. **[復元]** をクリックします。
3. ロケーションを選択し、必要なバックアップを選択します。バックアップは、ロケーションでフィルタされます。
4. 復元ポイントを選択して、**[復元]** > **[マシン全体]** をクリックします。

   必要に応じて、ターゲットマシンとボリュームのマッピングを構成します（"物理マシンのリカバリ
   このセクションでは、Web インターフェイスを使用した物理コンピュータの復元について説明します。復元する必要がある場合、Web インターフェイスではなくブータブルメディアを使用します。
   macOSを実行しているマシンコンプライアンスモードになっているテナントのマシン任意のオペレーティング システムをベアメタルまたはオフラインコンピュータに復元する場合論理ボリューム（LinuxにLVM（論理ボリュームマネージャ）で作成されたボリューム）の構成。メディアでは、論理ボリューム構成を自動的に再作成できます。Appleシリコンプロセッサを搭載するMacに、IntelベースMacのディスクレベルバックアップをリカバリすることはできません。ファイルおよびフォルダをリカバリできます。再起動を伴う復元オペレーティングシステムの復元、およびBitLockerで暗号化されたボリュームの復元には、再起動が必要です。コンピュータを自動的に再起動するか、[ユーザーによる操作が必要] ステータスに割り当てるかを選択できます。復元されたオペレーティングシステムは、自動的にオンラインになります。バックアップされた暗号化ボリュームは、非暗号化

ボリュームとしてリカバリされます。BitLockerで暗号化されたボリュームを復元する場合、同じマシン上に暗号化されていないボリュームがあり、そのボリュームに少なくとも1GBの空き領域がなければなりません。両方の条件が満たされない限り、復元は失敗します。暗号化されたシステムボリュームをリカバリする場合、追加の操作は必要ありません。暗号化されている非システムボリュームをリカバリするには、まずこのボリュームをロックする必要があります。これは、ボリューム上に存在するファイルを開くことなどで実行できます。そうでない場合は、再起動を伴わずに復元が続行され、復元されたボリュームがWindowsから認識できなくなる可能性があります。復元に失敗し、「パーティションからファイルを取得できません」というエラーによりマシンが再起動する場合は、セキュアブートを無効にしてから試行してください。この方法については、Microsoftテクニカルドキュメントの「セキュア ブートの無効化」を参照してください。物理コンピュータの復元手順バックアップされたコンピュータを選択します。[復元] をクリックします。リカバリ ポイントを選択します。復元ポイントは、保存場所でフィルタされます。コンピュータがオフラインになっている場合、リカバリ ポイントは表示されません。次の手順のいずれかを実行します。バックアップのロケーションがクラウドまたは共有ストレージの（他のエージェントがアクセスできる）場合は、[コンピュータを選択] をクリックして、オンラインになっているターゲット コンピュータを選択してから、リカバリ ポイントを選択します。[バックアップストレージ] タブで復元ポイントを選択します。「ブータブル メディアを使用したディスクの復元」の説明に従って、コンピュータを復元します。[復元] > [コンピュータ全体] をクリックします。バックアップされたディスクをターゲット コンピュータのディスクへ自動的にマップします。別の物理コンピュータに復元するには、[復元先のコンピュータ] をクリックして、オンラインの復元先のコンピュータを選択します。マッピング結果に満足できない場合や、マッピングが正常に行われなかった場合は、[ボリュームマッピング] をクリックして、ディスクを手動で再度マッピングできます。マッピングセクションでは、復元対象の個別のディスクまたはボリュームを選択することもできます。右上の [...に切り替え] リンクを使用することによって、リカバリするディスクおよびボリュームを切り替えることができます。（プロテクションエージェントがインストールされているWindowsマシンでのみ使用可能）[安全な復元] スイッチを有効にして、リカバリデータがマルウェアに感染していないことを確認します。安全な復元の仕組みについては、"安全な復元"（1ページ）を参照してください。[復元を開始] をクリックします。ディスクをバックアップされたバージョンで上書きすることを確認します。コンピュータを自動的に再起動するかどうかを選択します。復元の進行状況は [アクティビティ] タブに表示されます。"（1ページ）を参照）。

5. 高度な復元構成を実行するには、**[復元オプション]** をクリックします。詳細については、"復元オプション"（507ページ）を参照してください。
6. **[復元を開始]** をクリックします。
7. ディスクをバックアップされたバージョンで上書きすることを確認します。コンピュータを自動的に再起動するかどうかを選択します。
8. 復元の進行状況は **[アクティビティ]** タブに表示されます。

リモートで起動されたマシンを再起動するには

1. **[デバイス]** タブで、**[ブータブルメディア]** グループに移動し、データ復元に使用するメディアを選択します。
2. **[再起動]** をクリックします。
3. メディアで起動したマシンを再起動することを確認します。

リモートで起動されたマシンをシャットダウンするには

1. **[デバイス]** タブで、**[ブータブルメディア]** グループに移動し、データ復元に使用するメディアを選択します。
2. **[シャットダウン]** をクリックします。
3. メディアで起動したマシンをシャッドダウンすることを確認します。

ブータブルメディアの情報を表示するには

1. **[デバイス]** タブで、**[ブータブルメディア]** グループに移動し、データ復元に使用するメディアを選択します。
2. **[詳細]**、**[アクティビティ]**、**[アラート]** をクリックすると、対応する情報が表示されます。

ブータブルメディアをリモートで削除するには

1. **[デバイス]** タブで、**[ブータブルメディア]** グループに移動し、データ復元に使用するメディアを選択します。
2. **[削除]** をクリックして、Cyber Protectコンソールからブータブルメディアを削除します。
3. ブータブルメディアを削除することを確認します。

Startup Recovery Manager

Startup Recovery Managerは、ハードドライブに存在するブータブルコンポーネントです。Startup Recovery Managerを使用することで、別のブータブルメディアを使わずに、ブータブルレスキューユーティリティを起動することができます。

障害が発生した場合は、マシンを再起動し、「**Press F11 for Acronis Startup Recovery Manager**」という起動時のメッセージが表示されたら、F11を押すか、（GRUBブートローダーを使用している場合）ブートメニューからStartup Recovery Managerを選択します。Startup Recovery Managerが起動し、復元を実行できます。

制限事項

- （マスターブートレコードにインストールされているGRUBには使用不可）Startup Recovery Managerをアクティブ化すると、マスタ ブート レコード（MBR）がリカバリ マネージャのブートコードで上書きされます。その結果、アクティベーション後にサードパーティのブートローダーのアクティブ化が再度必要になる場合があります。
- （GRUBには使用不可）LinuxでStartup Recovery Managerをアクティブ化する前に、ブートローダーをマスターブートレコードにインストールするのではなく、ルートパーティションのブートレコードまたは /bootパーティションのブートレコードにインストールすることをお勧めします。それ以外の場合は、アクティベーション後に手動でブートローダーを再設定してください。

Startup Recovery Managerの有効化

「**Press F11 for Acronis Startup Recovery Manager**」という起動時のメッセージを有効にする（または、**Startup Recovery Manager**項目をGRUBメニューに追加する）には、Startup Recovery Managerを有効化します。

注意
暗号化されていないシステムボリュームのあるマシンでStartup Recovery Managerを有効化するには、そのマシンに100 MB以上の空き容量が必要です。再起動による復元には、さらに100 MBの空き容量が必要です。

BitLockerで暗号化されたボリュームのあるマシンでStartup Recovery Managerを有効化するには、このマシンに1つ以上の暗号化されていないボリュームがあり、そのボリュームに500 MB以上の空き領域が必要です。再起動による復元には、さらに500 MBの空き容量が必要です。

Startup Recovery Managerが有効になっていない場合、ワンクリック復元バックアップを作成するバックアップ操作は失敗します。

Startup Recovery Managerを有効化するには

エージェントのあるWindowsまたはLinuxマシン上

1. Cyber Protectコンソールで、Startup Recovery Managerを有効化するマシンを選択します。
2. **[詳細]** をクリックします。
3. **Startup Recovery Manager** スイッチを有効にします。

エージェントがないマシン上

1. ブータブルメディアを使用してマシンを起動します。
2. ブータブルメディアのグラフィカル ユーザー インターフェイスで **[ツール]** > **[Startup Recovery Managerの有効化]** をクリックします。
3. **[有効化]** を選択します。
4. **[OK]** をクリックします。
5. **[詳細]**タブで **[結果]**行をチェックしてアクティベーションが成功したことを確認し、**[閉じる]** をクリックします。

Startup Recovery Managerの無効化

無効にすると、「**Press F11 for Acronis Startup Recovery Manager**」というという起動時のメッセージが表示されなくなります（または、**Startup Recovery Manager**項目がGRUBのメニューから削除されます）。

Startup Recovery Managerが有効化されていない場合でも、別のブータブルメディアを使用することで、起動に失敗したマシンをリカバリすることができます。

注意
Startup Recovery Managerが有効になっていない場合、ワンクリック復元バックアップを作成するバックアップ操作は失敗します。

Startup Recovery Managerを無効化するには

エージェントのあるWindowsまたはLinuxマシン上

1. Cyber Protectコンソールで、Startup Recovery Managerを無効化するマシンを選択します。
2. **[詳細]** をクリックします。
3. **Startup Recovery Manager**スイッチを無効にします。

エージェントがないマシン上

1. ブータブルメディアを使用してマシンを起動します。
2. ブータブルメディアのグラフィカル ユーザー インターフェイスで **[ツール]** > **[Startup Recovery Managerの無効化]** をクリックします。
3. **[無効化]** を選択します。
4. **[OK]** をクリックします。
5. **[詳細]**タブで **[結果]**行をチェックして無効化が成功したことを確認し、**[閉じる]** をクリックします。

ディザスタリカバリを実装する

注意
- この機能では、Microsoft Azureバックアップロケーションがサポートされていません。

Cyber Disaster Recovery Cloudのバージョン情報

Cyber Disaster Recovery Cloud（DR）: Cyber Protectionの一部で、ディザスタリカバリをサービスとして提供します（DRaaS）。Cyber Disaster Recovery Cloudは、人為的災害や自然災害が発生した場合に、マシンをそのままコピーしたものをクラウドサイトに立ち上げ、元の破損したマシンからワークロードをリカバリサーバーに切り替える、高速で安定したソリューションを実現します。

次の方法で、ディザスタリカバリをセットアップして設定できます。

- ディザスタリカバリモジュールを含めた保護計画を作成し、デバイスに適用します。これによって、デフォルトのディザスタリカバリインフラが自動的にセットアップされます。「ディザスタリカバリ保護計画の作成」を参照してください。
- ディザスタリカバリクラウドインフラを手動でセットアップし、それぞれの手順を制御します。"復元サーバー設定"（759ページ）をご覧ください。

重要な機能

注意
適用されるライセンスモデルによっては、一部の機能で追加のライセンスが必要になる場合があります。

- Cyber Disaster Recovery Cloudサービスを単一のコンソールから管理
- セキュアなVPNトンネルを使用して最大23個のローカルネットワークをクラウドに拡張
- VPNアプライアンス[1]を配置せずに（クラウド限定モードで）クラウドサイトへの接続を確立
- ローカルおよびクラウドサイトへのポイントツーサイト接続を確立
- クラウドの復元サーバーを使用してマシンを保護
- クラウドのプライマリサーバーを使用してアプリケーションとアプライアンスを保護
- 暗号化済みバックアップへの自動ディザスタリカバリ操作を実行
- 隔離されたネットワークでテストフェールオーバーを実行
- ランブックを使用して、クラウドの本番環境をスピンアップ

[1][Disaster Recovery] 安全なVPNトンネルを介してローカルネットワークとクラウドサイト間の接続を可能にする特別な仮想マシン。VPNアプライアンスはローカルサイトに配置されています。

ソフトウェア要件

サポートされるオペレーティング システム

リカバリサーバーによる保護は、次のオペレーティングシステムで確認されています。

- CentOS 6.6, 7.x, 8.x
- Debian 9.x, 10.x, 11.x
- Red Hat Enterprise Linux 6.6, 7.x, 8.x
- Ubuntu 16.04, 18.04, 20.x, 21.x
- Oracle Linux 7.3 and 7.9 with Unbreakable Enterprise Kernel
- Windows Server 2008 R2
- Windows Server 2012/2012 R2
- Windows Server 2016: Nano Server以外のすべてのインストールオプション
- Windows Server 2019: Nano Server以外のすべてのインストールオプション
- Windows Server 2022: Nano Server以外のすべてのインストールオプション

このソフトウェアは他の Windows オペレーティングシステムや Linux ディストリビューションでも動作しますが、これは保証されていません。

注意
復元サーバーによる保護は、以下のオペレーティングシステムを搭載したMicrosoft Azure VMでテスト済みです。

- Windows Server 2008 R2
- Windows Server 2012/2012 R2
- Windows Server 2016: Nano Server以外のすべてのインストールオプション
- Windows Server 2019: Nano Server以外のすべてのインストールオプション
- Windows Server 2022: Nano Server以外のすべてのインストールオプション
- Ubuntu Server 20.04 LTS - Gen2（Canonical）。復元サーバーコンソールへのアクセスの詳細については、https://kb.acronis.com/content/71616を参照してください。

サポートされる仮想環境プラットフォーム

リカバリサーバーによる仮想マシンの保護は、次の仮想環境プラットフォームで確認されています。

- VMware ESXi 5.1, 5.5, 6.0, 6.5, 6.7, 7.0
- Windows Server 2008 R2（Hyper-V 使用）
- Windows Server 2012/2012 R2（Hyper-V 使用）
- Windows Server 2016 with Hyper-V: Nano Server以外のすべてのインストールオプション
- Windows Server 2019 with Hyper-V: Nano Server以外のすべてのインストールオプション
- Windows Server 2022 with Hyper-V: Nano Server以外のすべてのインストールオプション
- Microsoft Hyper-V Server 2012/2012 R2

- Microsoft Hyper-V Server 2016
- カーネルベース仮想マシン（KVM） - 完全仮想化ゲスト（HVM）のみ。準仮想化ゲスト（PV）はサポート対象外です。
- Red Hat Enterprise Virtualization (RHEV) 3.6
- Red Hat Virtualization (RHV) 4.0
- Citrix XenServer: 6.5, 7.0, 7.1, 7.2

VPN アプライアンスは、次の仮想環境プラットフォームで確認されています。

- VMware ESXi 5.1, 5.5, 6.0, 6.5, 6.7
- Windows Server 2008 R2（Hyper-V 使用）
- Windows Server 2012/2012 R2（Hyper-V 使用）
- Windows Server 2016 with Hyper-V: Nano Server以外のすべてのインストールオプション
- Windows Server 2019 with Hyper-V: Nano Server以外のすべてのインストールオプション
- Windows Server 2022 with Hyper-V: Nano Server以外のすべてのインストールオプション
- Microsoft Hyper-V Server 2012/2012 R2
- Microsoft Hyper-V Server 2016

このソフトウェアは他の仮想環境プラットフォームやバージョンでも動作しますが、これは保証されていません。

制限事項

以下のプラットフォームと構成はCyber Disaster Recovery Cloudではサポート対象外です。

1. サポート外プラットフォーム:
   - Virtuozzoエージェント
   - macOS
   - Windowsデスクトップオペレーティングシステムは、Microsoftの製品利用規約により、サポートされません。
   - Windows Server Azure Edition

     Azure Editionは、Azure IaaS仮想マシン（VM）としてAzureで実行するか、Azure Stack HCIクラスター上のVMとして実行することに特化して構築されたWindows Serverの特別バージョンです。Standard Editionやデータセンターエディションとは異なり、Azure Editionは、ベアメタルハードウェア、WindowsクライアントHyper-V、Windows Server Hyper-V、サードパーティ製ハイパーバイザー、サードパーティ製クラウドでの実行はライセンスされていません。
2. サポート外構成:

   Microsoft Windows
   - ダイナミックディスクはサポート対象外です
   - Windowsデスクトップオペレーティングシステムは、（Microsoftの製品利用規約により）サポートされません
   - Active Directory service with FRSレプリケーションはサポート対象外です

- GPTまたはMBRフォーマットなしのリムーバブルメディア（いわゆる「スーパーフロッピー」）はサポート対象外です

Linux

- パーティションテーブルのないファイルシステム
- エージェントを使用してゲストOSからバックアップされた、以下の高度なLVM（論理ボリュームマネージャー）構成のボリュームを持つLinuxワークロード:ストライプボリューム、ミラーボリューム、RAID 0、RAID 4、RAID 5、RAID 6、RAID 10ボリューム。

注意
複数のオペレーティングシステムがインストールされたワークロードはサポートされていません。

3. サポートされていないバックアップの種類:
   - 継続的データ保護（CDP）復元ポイントに互換性がありません。

     重要
     CDP復元ポイントを有するバックアップからリカバリサーバーを作成する場合、フェールバックまたはリカバリサーバーの作成中に、CDP復元ポイントを含むデータが失われます。

   - フォレンジックバックアップは、リカバリサーバーの作成に利用できません。

リカバリサーバーには 1 つのネットワークインターフェースがあります。元のマシンに複数のネットワークインターフェースがある場合は、1 つだけがエミュレートされます。

クラウドサーバーは暗号化されていません。

Cyber Disaster Recovery Cloud試用版

Acronis Cyber Disaster Recovery Cloudの30日間の試用版をご利用いただけます。この場合パートナーテナントでは、ディザスタリカバリに次の制限があります。

- 復元サーバーおよびプライマリーサーバーはパブリックインターネットにアクセスできません。サーバーにパブリックIPアドレスを割り当てることはできません。
- IPsecマルチサイトVPNを利用できません。

地理的冗長性クラウドストレージ使用時の制限事項

地理的冗長性クラウドストレージは、バックアップデータのセカンダリロケーションを提供します。セカンダリロケーションは、プライマリのストレージロケーションとは地理的に異なる地域に存在します。地域を地理的に分離することで、万が一いずれかの地域に災害が発生し、バックアップデータが復旧不可能になっても、もう一方の地域は影響を受けず、処理を継続することができます。

重要
バックアップストレージのロケーションがプライマリロケーションから地理的に冗長化されたセカンダリロケーションに変更された場合、ディザスタリカバリサービスはサポートされません。

ディザスタリカバリと暗号化ソフトウェアの互換性

ディザスタリカバリには、以下のディスクレベルの暗号化ソフトウェアとの互換性があります。

- Microsoft BitLocker Drive Encryption
- McAfee Endpoint Encryption
- PGP Whole Disk Encryption

注意

- ディスクレベルの暗号化を利用するワークロードの場合、ワークロードのゲストオペレーティングシステムにプロテクションエージェントをインストールし、エージェントベースのバックアップを実行することをお勧めします。
- 暗号化されたワークロードのエージェントレスバックアップでは、フェールオーバーとフェールバックはサポートされていません。

Cyber Protectionと暗号化ソフトウェアの互換性の詳細については、"暗号化ソフトウェアとの互換性"（41ページ）を参照してください。

コンピュートポイント

Disaster Recoveryでは、テストフェールオーバー時や本番フェールオーバー時のプライマリサーバーや復元サーバーに計算ポイントが使用されます。計算ポイントは、クラウド上のサーバー（仮想マシン）の実行に使用される計算リソースを反映します。

ディザスタリカバリ中の計算ポイントの消費は、サーバーのパラメータ、およびサーバーがフェールオーバー状態にある時間によって異なります。サーバーの処理能力が大きく、負荷がかかる時間が長いほど、より多くの計算ポイントが消費されます。より多くの計算ポイントが消費されるほど、請求金額が大きくなります。

Acronis Cloudで稼動しているすべてのサーバーは、状態（電源オンまたは電源オフ）に関係なく、設定されたフレーバーに応じて、計算ポイントに対して請求されます。

スタンバイ状態の復元サーバーは、計算ポイントを消費しないため、計算ポイントが請求されることはありません。

次の表では、異なるフレーバーを持つクラウド上の8台のサーバーと、それらが1時間あたりに消費する計算ポイントの例を示しています。サーバーのフレーバーは、**[詳細]** タブで変更できます。

種類	CPU	RAM	コンピュートポイント
F1	1 vCPU	2GB	1
F2	1 vCPU	4GB	2
F3	2 vCPU	8GB	4
F4	4 vCPU	16GB	8

種類	CPU	RAM	コンピュートポイント
F5	8 vCPU	32GB	16
F6	16 vCPU	64GB	32
F7	16 vCPU	128GB	64
F8	16 vCPU	256GB	128

表の情報を使用して、サーバー（仮想マシン）で消費される計算ポイント数を簡単に予測できます。

例えば、16GB RAMとvCPU*4基を備えた1台の仮想マシンと、8GBのRAMとvCPU 2基を備えた1台の仮想マシンをディザスタリカバリで保護する場合、最初の仮想マシンでは1時間あたり8個の計算ポイントが消費され、2番目の仮想マシンでは、1時間あたり4個の計算ポイントが消費されます。両方の仮想マシンがフェールオーバーされている状態では、合計消費量は1時間あたり12計算ポイント、つまり1日で288計算ポイントになります（12計算ポイントx24時間=288計算ポイント）。

*vCPUとは、仮想マシンに割り当てられる物理的な中央演算処理装置（CPU）のことであり、時間依存で存在します。

注意
計算ポイントクォータが制限値に達した場合、プライマリサーバーおよび復元サーバーはすべてシャットダウンされます。次の請求期間の開始まで、またはクォータを増やすまで、これらのサーバーを使用することはできません。デフォルトの請求期間は暦月です。

ディザスタリカバリ機能を設定

注意
適用されるライセンスモデルによっては、一部の機能で追加のライセンスが必要になる場合があります。

ディザスタリカバリ機能を設定するには

1. クラウドサイトへの接続タイプを設定します:
   - ポイントツーサイト接続
   - サイト間OpenVPN接続
   - マルチサイトIPsec VPN接続
   - クラウド限定モード
2. バックアップモジュールを有効にした保護計画を作成して、バックアップするマシン全体またはシステム、およびブートボリュームを選択します。リカバリサーバーを作成するには、少なくとも1つの保護計画が必要です。
3. 保護計画を保護するローカルサーバーへ適用します。
4. 保護するローカルサーバー毎に復元サーバーの作成を行ないます。
5. どのように機能しているかをチェックするためにフェールオーバーのテストを実行します。
6. （オプション）アプリケーションのレプリケーションのためにプライマリサーバーを作成します。

その結果、ローカルサーバーを災害から保護するためのディザスタリカバリ機能が設定されました。

災害が発生した場合、クラウドの復元サーバーに対しワークロードのフェールオーバーを行うことができます。リカバリサーバーにフェールオーバーする前に、少なくとも1つの復元ポイントを作成する必要があります。ローカルサイトが災害からリカバリされたら、フェールバックを実行してワークロードをローカルサイトへ切り替えることができます。フェールバックプロセスの詳細については、「"前提条件"（773ページ）」および「"前提条件"（777ページ）」を参照してください。

ディザスタリカバリ保護計画の作成

ディザスタリカバリモジュールを含めた保護計画を作成し、デバイスに適用します。

デフォルトでは、新しい保護計画の作成時にディザスタリカバリモジュールが無効になっています。ディザスタリカバリ機能を有効にしてサービスに計画を適用すると、クラウドネットワークインフラが作成されます。ここで作成されるインフラには、個別の保護対象のサービスに対応する復元サーバーが含まれています。復元サーバーは、選択されたデバイスをコピーしたクラウド内の仮想マシンです。選択されたそれぞれのデバイスに対して、デフォルト設定の復元サーバーがスタンバイ状態（仮想マシンが実行されていない）で作成されます。復元サーバーのサイズは、保護されているデバイスのCPUとRAMに応じて自動的に設定されます。次のようなデフォルトのクラウドネットワークインフラも自動的に作成されます。クラウドサイトのVPNゲートウェイとネットワーク。リカバリサーバーの接続先になります。

保護計画のディザスタリカバリモジュールを取り消したり、削除または無効化したりする場合でも、復元サーバーとクラウドネットワークが自動的に削除されることはありません。必要な場合は、ディザスタリカバリインフラを手動で削除できます。

注意

- ディザスタリカバリを構成すると、デバイスの復元サーバー作成後に生成された任意の復元ポイントから、テストまたは本番のフェールオーバーを実行できるようになります。デバイスがディザスタリカバリで保護される前（復元サーバーが作成される前）に生成された復元ポイントを使用してフェールオーバーを実行することはできません。
- デバイスのIPアドレスを検出できない場合、ディザスタリカバリ保護計画を有効にすることはできません。仮想マシンがエージェントレスでバックアップされ、IPアドレスが割り当てられていない場合などがこれに当たります。
- 保護計画を適用する際には、同じネットワークとIPアドレスがクラウドサイトで割り当てられます。IPsec VPN接続では、クラウドのネットワークセグメントとローカルサイトが重複しないことが求められます。マルチサイトIPsec VPN接続が構成され、1台または複数のデバイスに保護計画が後で適用される場合、追加でクラウドネットワークをアップデートしてクラウドサーバーのIPアドレスを再割り当てする必要があります。詳細については、"IPアドレスの再割り当て"（749ページ）を参照してください。

ディザスタリカバリ保護計画を作成するには

1. Cyber Protectコンソールで **[デバイス]** > **[すべてのデバイス]** に進みます。
2. 保護するマシンを選択します。

3. **[保護]** をクリックしてから、**[計画の作成]** をクリックします。
   保護計画のデフォルト設定が開きます。
4. バックアップオプションを設定します。
   ディザスタリカバリの機能を使用する場合、この計画では、マシン全体、または起動と必須のサービスの提供に必要なディスクのみをクラウド ストレージにバックアップする必要があります。
5. モジュール名の横にあるスイッチをクリックして、ディザスタリカバリモジュールを有効にします。
6. **[作成]** をクリックします。
   計画が作成され、選択されたマシンに適用されます。

次に行うこと

- 復元サーバーのデフォルト設定は編集できます。詳細については、"復元サーバー設定"（759ページ）を参照してください。
- デフォルトのネットワーク設定は編集できます。詳細については、"接続設定"（723ページ）を参照してください。
- 復元サーバーのデフォルトパラメータとクラウドネットワークインフラについて、詳細が確認できます。詳細については、「"復元サーバーのデフォルトパラメータの編集"（721ページ）」と「"クラウドネットワークインフラストラクチャ"（722ページ）」を参照してください。

復元サーバーのデフォルトパラメータの編集

ディザスタリカバリ保護計画を作成して適用すると、デフォルトパラメータで復元サーバーが作成されます。これらのデフォルトパラメータは後で編集できます。

注意
リカバリサーバーは、存在していなかった場合のみ作成されます。既存の復元サーバーに変更や再作成は発生しません。

復元サーバーのデフォルトパラメータを編集するには

1. **[デバイス]** > **[すべてのデバイス]** に進みます。
2. デバイスを選択し、**[ディザスタリカバリ]** をクリックします。
3. 復元サーバーのデフォルトパラメータを編集します。
   復元サーバーのパラメータについては、次のテーブルで説明されています。

復元サーバーパラメータ	デフォルト数	説明
CPUとRAM	自動	リカバリサーバーの仮想CPUの数とRAMの容量。デフォルト設定は元のデバイスのCPUとRAMの設定に基づいて自動的に決定されます。
クラウドネットワーク	自動	サーバーが接続されるクラウドネットワーク。クラウドネットワークの設定内容の詳細については、「クラウドネットワークインフラストラクチャ」を

		参照してください。
本番ネットワークのIPアドレス	自動	稼働中のネットワークでサーバーに与えられるIPアドレス。デフォルトでは、元のマシンの IP アドレスが設定されています。
テストIPアドレス	無効化	テスト用のIPアドレスを使用することで、隔離されたテストネットワーク内でフェールオーバーをテストし、テストフェールオーバー中にRDPまたはSSH経由でリカバリサーバーに接続することが可能になります。テストフェールオーバーモードでは、VPNゲートウェイが、NATプロトコルを使用してテストIPアドレスを本番IPアドレスに置き換えます。テスト用のIPアドレスを指定しない場合、テストフェールオーバー中はコンソール以外でサーバーにアクセスできなくなります。
インターネットアクセス	有効化	リカバリサーバーが、実際のフェールオーバーまたはテストフェールオーバー中にインターネットにアクセスできるようにします。デフォルトでは、TCPポート25番の送信接続は拒否されます。
パブリックアドレスの使用	無効化	パブリック IP アドレスを使用すると、フェールオーバーまたはテストフェールオーバー中にインターネットからリカバリサーバーを使用できるようになります。パブリックIPアドレスを使用しない場合、サーバーは稼働中のネットワーク内部でのみ使用可能になります。パブリックIPアドレスを使用するには、インターネットアクセスを有効にする必要があります。パブリック IP アドレスは、設定が完了した後に表示されます。デフォルトでは、TCPポート443番は受信接続用に開いています。
RPO しきい値を設定	無効化	RPO しきい値は、最後の復元ポイントと現在時刻との間の最大許容時間間隔を定義します。数値は15～60分、1～24時間、1～14日間の範囲で設定できます。

クラウドネットワークインフラストラクチャ

クラウドネットワークインフラストラクチャは、クラウドサイトのVPNゲートウェイと復元サーバーが接続されるクラウドネットワークから構成されます。

注意
ディザスタリカバリ保護計画を適用すると、存在していない場合には復元クラウドネットワークインフラが作成されます。既存のクラウドネットワークの変更や再作成は発生しません。

システムによってデバイスのIPアドレスがチェックされ、IPアドレスに適した既存のクラウドネットワークが存在しない場合は、適切なクラウドネットワークが自動的に作成されます。リカバリサーバーのIPアドレスに適したクラウドネットワークが既に存在していれば、既存のクラウドネットワークの変更や作作成は発生しません。

- クラウドネットワークが存在しない場合や、初めてディザスタリカバリ設定を実施する場合、そのようなクラウドネットワークにはデバイスのIPアドレス範囲に基づいて、IANAがプライベートでの使用に推奨している最大範囲（10.0.0.0/8、172.16.0.0/12、192.168.0.0/16）が設定されます。ネットワークマスクを編集すれば、ネットワーク範囲を狭くすることができます。
- 選択されたデバイスが複数のローカルネットワークに属している場合、クラウドサイトのネットワークはそれらのローカルネットワークのスーパーセットになる場合があります。ネットワークは **[接続]** セクションで再設定できます。"ネットワークの管理"（743ページ）をご覧ください。
- サイト間Open VPN接続をセットアップする必要がある場合は、VPNアプライアンスをダウンロードしてセットアップしてください。"サイト間Open VPNの構成"（734ページ）をご覧ください。クラウドネットワークの範囲が、VPNアプライアンスに接続されたローカルネットワークの範囲と一致しているのを確認します。
- デフォルトのネットワーク設定を変更するには、保護計画のディザスタリカバリモジュールにある **[接続に移動]** リンクをクリックするか、**[ディザスタリカバリ]** > **[接続]** へ移動します。

接続設定

このセクションでは、Cyber Disaster Recovery Cloudですべての機能がどのように動作するのかを理解するために必要なネットワークの概念について説明します。必要に応じてクラウドサイトへの異なる種類の接続をどのように設定するのかについて知ることができます。最終的には、クラウドでのネットワーク管理方法およびVPNアプライアンスとVPNゲートウェイの設定管理について知ることができます。

ネットワーク概念

注意
適用されるライセンスモデルによっては、一部の機能で追加のライセンスが必要になる場合があります。

Cyber Disaster Recovery Cloudでは、クラウドサイトへの次の接続タイプを定義できます。

- **クラウド限定モード**

  この種類の接続にはローカルサイトへのVPNアプライアンス配置が必要ありません。

  ローカルネットワークとクラウドネットワークは、独立したネットワークです。この種類の接続は、すべてのローカルサイトの保護されたサーバーのフェールオーバー、またはローカルサイトと通信する必要のない独立したサーバーの部分的なフェールオーバーのどちらか一方を意味します。

  クラウドサイト上のクラウドサーバーは、ポイントツーサイトVPN、およびパブリックIPアドレス（割り当てられている場合）を介してアクセスできます。
- **サイト間Open VPN接続**

  この種類の接続にはローカルサイトへのVPNアプライアンス配置が必要です。

サイト間Open VPN接続により、IPアドレスを保持しながら、ネットワークをクラウドに拡張できます。

セキュアなVPNトンネルによりローカルサイトがクラウドに接続されました。この種類の接続は、ローカルサイトにWebサーバーやデータベースサーバーなどの高依存度のサーバーがある場合に適しています。部分的なフェールオーバーの場合、これらのサーバーの多数がローカルサイトにとどまっている間に1つのサーバーがクラウドサイトで再作成されても、VPNトンネルを介して互いに通信できます。

クラウドサイト上のクラウドサーバーは、ローカルネットワーク、ポイントツーサイトVPN、およびパブリックIPアドレス（割り当てられている場合）を介してアクセスできます。

- **マルチサイトIPsec VPN接続**

  このタイプの接続では、IPsec IKE v2をサポートするローカルVPNデバイスが必要となります。

  マルチサイトIPsec VPN接続の構成を開始すると、Cyber Disaster Recovery Cloudが自動的にパブリックIPアドレスによるクラウドVPNゲートウェイを作成します。

  マルチサイトIPsec VPNを使用すると、セキュアなIPsec VPNトンネルによりローカルサイトがクラウドに接続されます。

  このタイプの接続は、1つまたは複数のローカルサイトで重要なワークロードをホストしているか、サービスに緊密に依存している場合のディザスタリカバリシナリオに適しています。

  サーバー群の1つが部分的にフェールオーバーする場合、そのサーバーがクラウドサイトで再作成される間も、他のサーバーはローカルサイトにとどまってIPsec VPNトンネルを介して引き続き互いに通信することが可能です。

  ローカルサイトの1つが部分的にフェールオーバーする場合は、それ以外のローカルサイトは運用可能なままで、IPsec VPNトンネルを介して引き続き互いに通信できます。

- **ポイントツーサイトリモートVPNアクセス**

  エンドポイントデバイスを使用する外部からのクラウドおよびローカルワークロードに対するセキュアなポイントツーサイトリモートVPNアクセス。

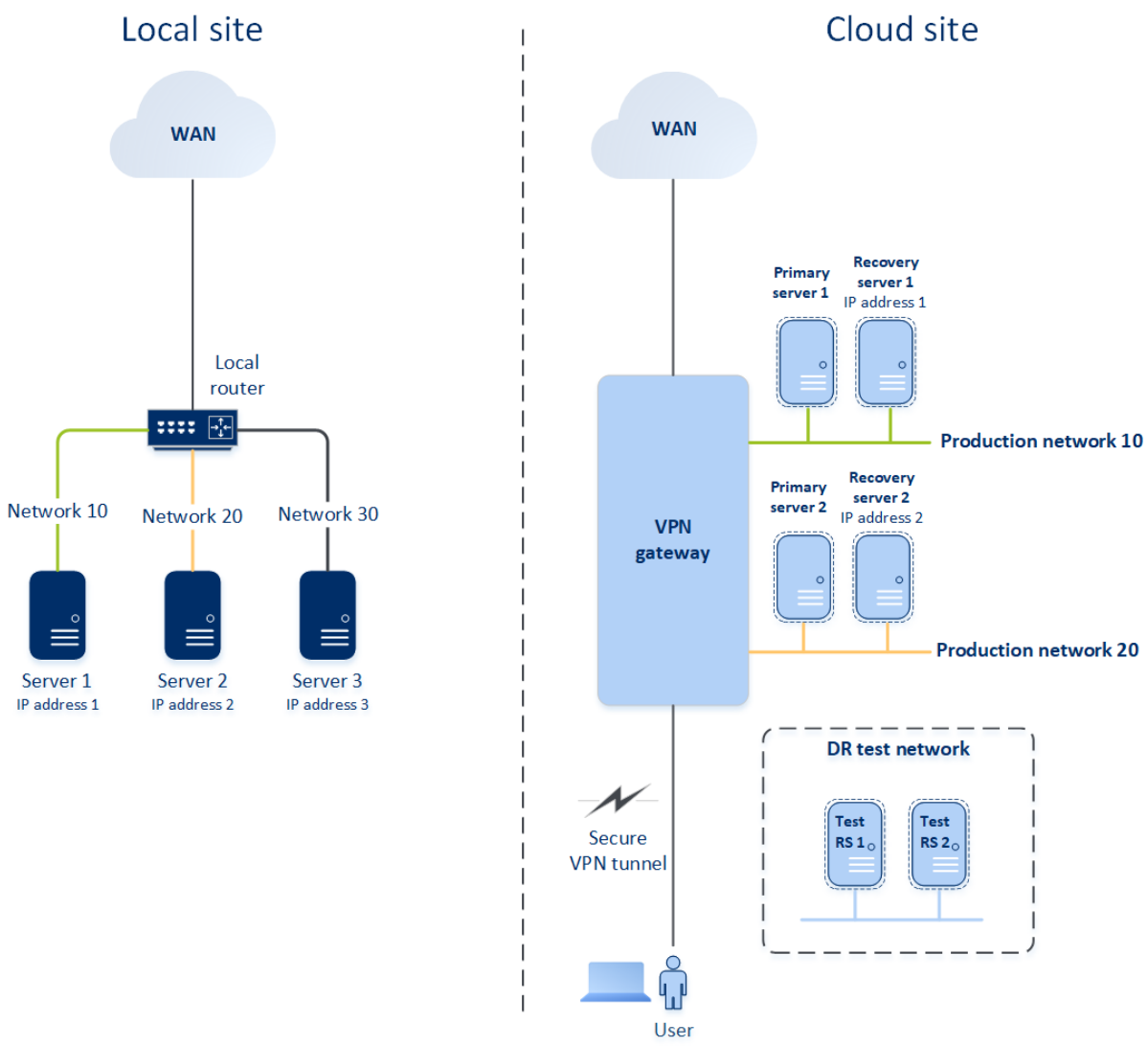
  ローカルサイトにアクセスする場合、この種類の接続にはローカルサイトへのVPNアプライアンス配置が必要です。

クラウド限定モード

クラウド限定モードでは、ローカルサイトへのVPNアプライアンス配置は必要ありません。これは、1つはローカルサイトに、もう1つはクラウドサイトにある、2つの独立したネットワークがあることを意味します。クラウドサイトのルータでルーティングが実行されます。

ルーティングが動作する仕組み

クラウドオンリーモードが確立している場合、クラウドサイトのルーターによってルーティングが実行され、異なるクラウドネットワークに属するサーバー同士で通信できます。



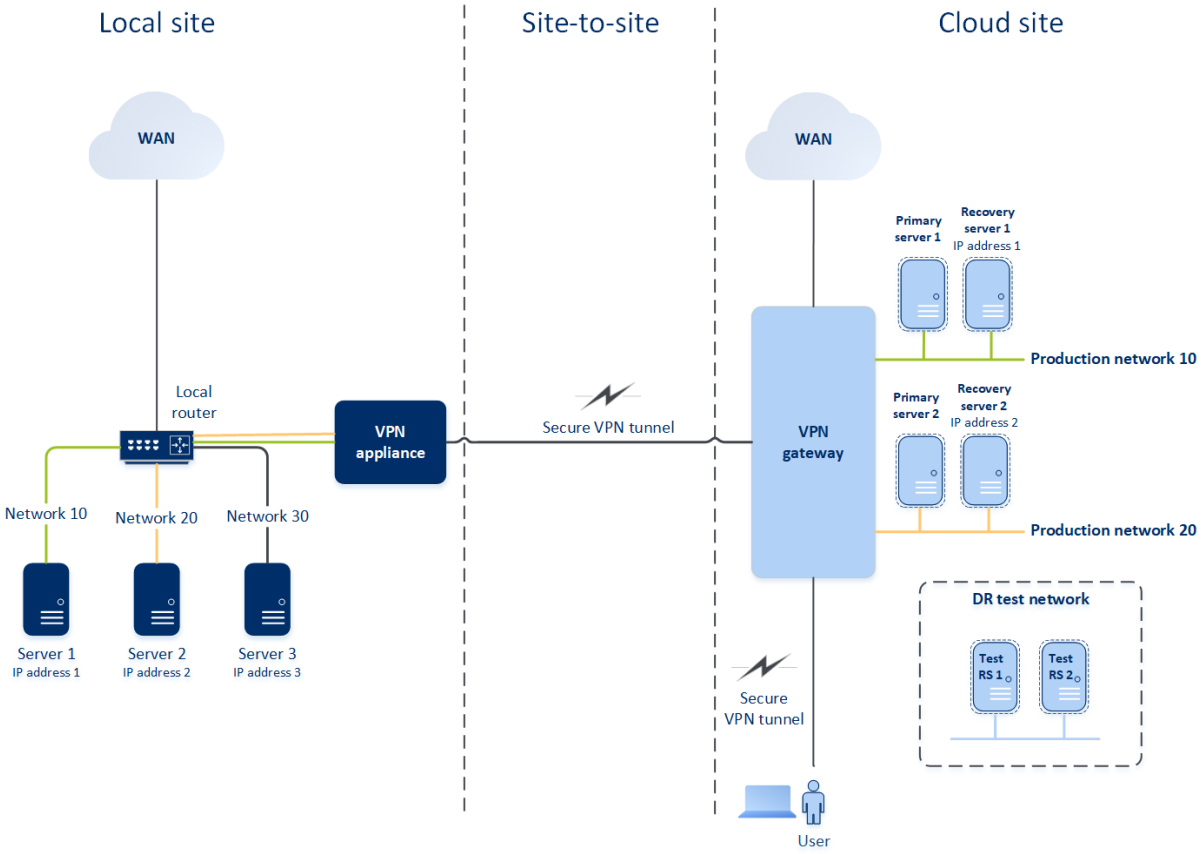
サイト間Open VPN接続

注意
この機能を利用できるかどうかは、現在のアカウントで有効になっているサービスクォータによって異なります。

Cyber Disaster Recovery Cloudサービスでネットワークがどのように機能するかを理解するため、ローカルサイトの3つのネットワークに各々1つのマシンがある事例を検討します。ネットワーク10とネットワーク20の2つのネットワークについて、災害からの保護を設定します。

下の図では、マシンがホストされているローカルサイトと、災害発生時のためにクラウドサーバーが実行されているクラウドサイトが表示されています。

Cyber Disaster Recovery Cloudソリューションでは、ローカルサイトの破損したマシンからクラウド上のクラウドサーバーに対して、すべてのワークロードのフェールオーバーを行うことができます。
Cyber Disaster Recovery Cloudを使用して最大で23個のネットワークを保護できます。



ローカルサイトとクラウドサイト間のサイトツーサイトOpen VPN通信を確立するには、**VPNアプライアンス**と**VPNゲートウェイ**を使用します。Cyber Protectコンソールでサイトツーサイトopen VPN接続の設定を始める際、VPNゲートウェイは自動的にクラウドサイトに配置されます。それから、ローカルサイトへVPNアプライアンスを配置し、保護するネットワークを追加し、クラウドでアプライアンスを登録する必要があります。Cyber Disaster Recovery Cloudは、クラウドにローカルネットワークのレプリカを作成します。安全なVPNトンネルがVPNアプライアンスとVPNゲートウェイ間に確立されます。これにより、ローカルネットワーク拡張がクラウドに提供されます。クラウドの本番ネットワークがローカルネットワークにブリッジされます。ローカルサーバーとクラウドサーバーはこのVPNトンネルを介してあたかもそれらすべてが同じイーサネットセグメント内にあるかのように通信できます。ローカルのルーターによりルーティングが実行されます。

各ソースマシンを保護するために、クラウドサイトにリカバリサーバーを作成する必要があります。フェールオーバーイベントが生じるまで**スタンバイ**状態を保ちます。（**本番モード**で）災害が発生しフェールオーバープロセスを開始すると、保護されたマシンの厳密なコピーであるリカバリサーバーがクラウドで起動します。ソースマシンと同じIPアドレスを割り当て、同じイーサネットセグメントで起動することができます。顧客は、バックグラウンドでの変更に気付くことなくサーバーでの作業を続けることができます。

フェールオーバープロセスを**テストモード**で開始することもできます。これは、ソースマシンがまだ機能している時に、同時に同じIPアドレスを持つそれぞれの復元サーバーがクラウドで起動することを意味します。IPアドレスの競合を防ぐため、**テストネットワーク**という特別な仮想ネットワークがクラウドに作成されます。テストネットワークは、1つのイーサネットセグメント内でのソースマシンのIPアドレスの重複を防ぐために隔離されています。フェールオーバーのテストモードで復元サーバーにアクセ

スするには、復元サーバーの作成時に、**テストIPアドレス**を復元サーバーに割り当てる必要があります。指定できる復元サーバのパラメータは他にもあり、それらについては以下の各セクションで説明します。

ルーティングが動作する仕組み

サイト間接続が確立されている場合、ローカルのルーターによりクラウドネットワーク間のルーティングが実行されます。VPNサーバーは、異なるクラウドネットワークに配置されたクラウドサーバー間のルーティングを実行しません。いずれかのネットワークにあるクラウドサーバーと、別のクラウドネットワークにあるサーバーで通信が必要な場合、トラフィックはVPNトンネルを通じてローカルサイトのローカルルーターへ送られ、その後、ローカルルーターが、別のネットワークへのルーティングを実行します。そして、トラフィックはトンネル経由でクラウドサイトの目的のサーバーに戻ります。

VPN ゲートウェイ

ローカルサイトとクラウドサイト間の通信を可能にする主要なコンポーネントは**VPNゲートウェイ**です。これは、特別なソフトウェアがインストールされ、ネットワークが特異的に構成されているクラウド内の仮想マシンです。VPNゲートウェイには以下の機能があります。

- ローカルネットワークのイーサネットセグメントとクラウド内の稼働中のネットワークをL2モードで接続。
- iptablesとebtablesのルールを入力。
- テストネットワークと稼働しているネットワークのマシンのデフォルトルーターおよびNATとして動作。
- DHCPサーバーとして動作。本番ネットワークとテストネットワークのすべてのマシンはDHCPを介してネットワークの構成（IPアドレス、DNS設定）を取得します。クラウドサーバーは毎回、DHCPサーバーから同一のIPアドレスを取得します。カスタムDNS設定をセットアップする必要がある場合は、サポートチームに連絡する必要があります。
- キャッシングDNSとして動作。

VPNゲートウェイネットワークの構成

VPNゲートウェイには幾つかのネットワークインターフェースがあります。

- インターネットに接続されている外部インターフェース
- 本番ネットワークに接続されている本番インターフェース
- テストネットワークに接続されているテストインターフェース

加えて、2つの仮想インターフェースがポイントツーサイトおよびサイト間接続用に追加されています。

VPNゲートウェイが配置され初期化されると、ブリッジが作成されます。1つは外部インターフェース用、もう1つは顧客および本番インターフェース用です。クライアント本番環境のブリッジとテストインターフェースは同じIPアドレスを使用しますが、VPNゲートウェイは特定の技術を使用してパッケージを正しくルーティングできます。

VPNアプライアンス

VPNアプライアンスは、Linuxと特別なソフトウェアがインストールされ、ネットワークが特異的に構成されている、ローカルサイト上の仮想マシンです。ローカルサイトとクラウドサイト間の通信を可能にします。

リカバリサーバー

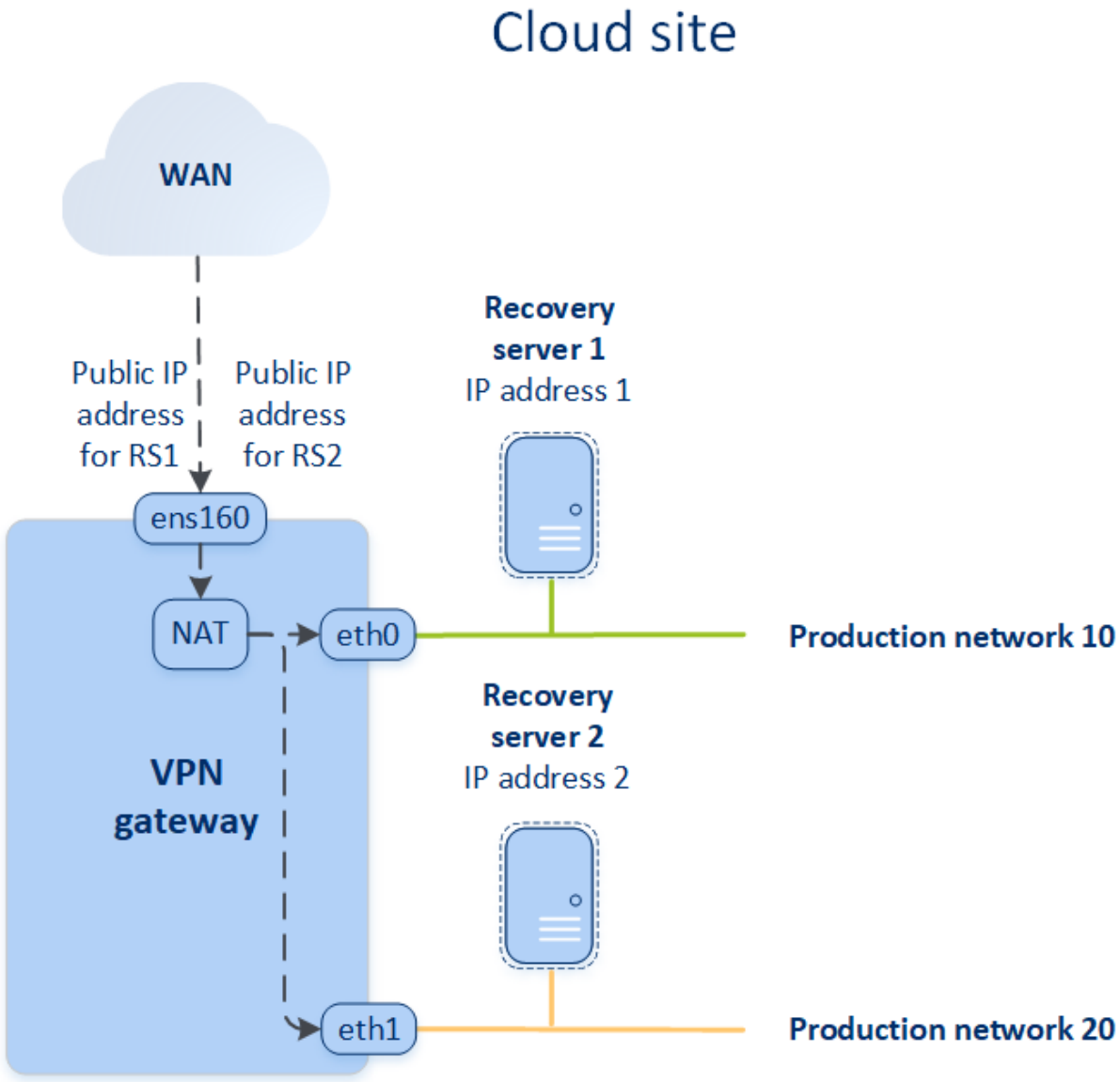
復元サーバーは、クラウドに保存されている保護されたサーバーのバックアップに基づく元のマシンのレプリカです。復元サーバーは、災害発生時にワークロードを元のサーバーから切り替えるのに使用されます。

復元サーバーを作成する際、以下のネットワークパラメータを指定する必要があります。

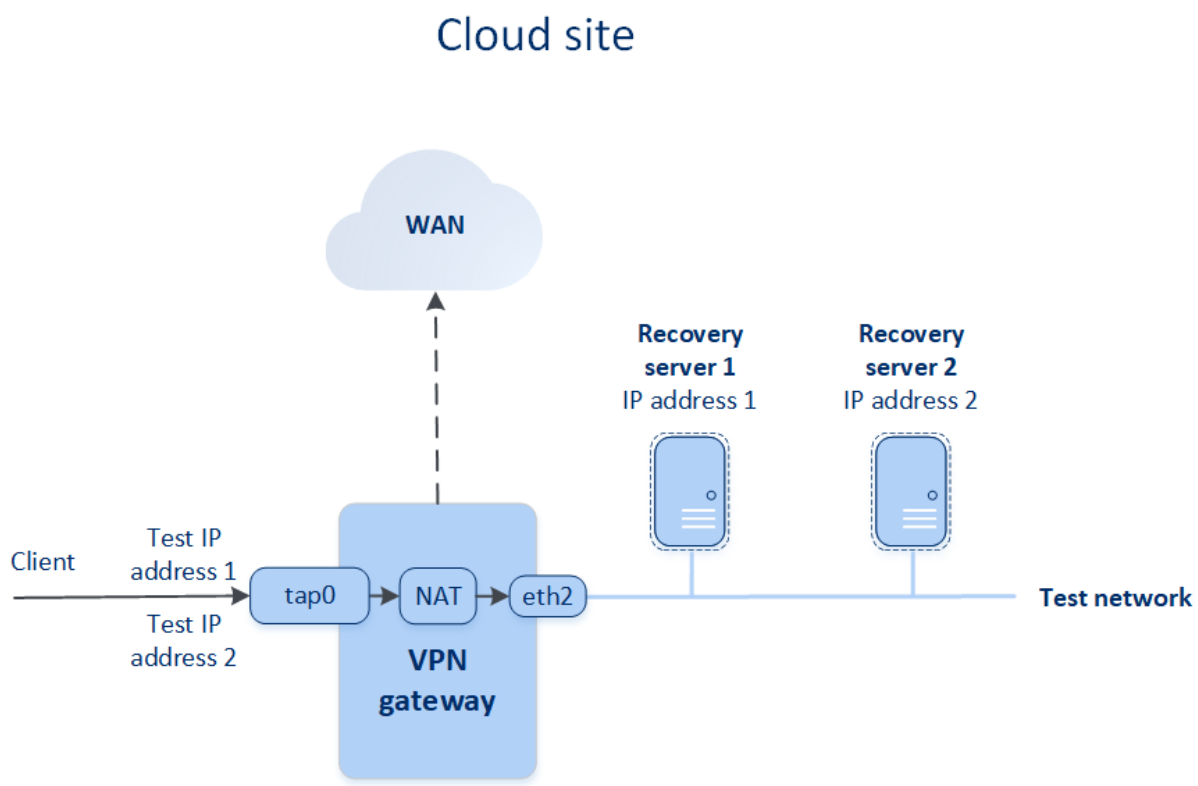
- **クラウドネットワーク**（必須）: 復元サーバーが接続されるクラウドネットワークです。
- **本番ネットワークにおける IP アドレス**（必須）:復元サーバー用の仮想マシンが起動する IP アドレス。このアドレスは本番ネットワークおよびテストネットワークの両方で使用されます。起動する前に、DHCPを介してIPアドレスを取得するよう仮想マシンを設定します。
- **テストIPアドレス**（オプション）:テストフェールオーバー中に顧客の稼働中ネットワークから復元サーバーにアクセスして、稼働中のIPアドレスが同じネットワーク内で重複しないようにするためのIPアドレス。このIPアドレスは本番ネットワークのIPアドレスとは異なります。ローカルサイトのサーバーは、テストIPアドレスを介してフェールオーバーのテスト中に復元サーバーに到達できますが、逆方向のアクセスは利用できません。復元サーバーの作成中に**インターネットアクセス**オプションが選択される場合、テストネットワークにおける復元サーバーからのインターネットアクセスが利用できます。
- **パブリックIPアドレス**（オプション）:インターネットから復元サーバーにアクセスするためのIPアドレス。サーバーにパブリックIPアドレスがない場合、ローカルネットワークからのみアクセスできます。
- **インターネットアクセス**（オプション）: 復元サーバがインターネットにアクセスすることを可能にします（本番およびテストのフェイルオーバーの両方）。

パブリックおよびテストIPアドレス

復元サーバー作成時にパブリックIPアドレスを割り当てた場合、復元サーバーはこのIPアドレスを介してインターネットから利用可能になります。ターゲットパブリックIPアドレスを持つパケットがインターネットから届くと、VPNゲートウェイはNATを使用してそれを適切な本番IPアドレスに再マッピングし、対応するリカバリサーバーに送信します。



復元サーバー作成時にテストIPアドレスを割り当てた場合、復元サーバーはこのIPアドレスを介してテストネットワークで利用可能になります。テストフェールオーバーを実行すると、元のマシンは実行されたままになり、同じIPアドレスを持つ復元サーバーがクラウドのテストネットワークで起動されます。テストネットワークが隔離されているので、IPアドレスの競合はありません。テストネットワーク内の復元サーバーは、NATを介して本番IPアドレスに再マッピングされる、それらのテストIPアドレスにより到達可能です。



サイト間Open VPNの詳細については、"サイトツーサイトOpen VPN - 追加情報"（182ページ）を参照してください。

プライマリサーバー

プライマリサーバーは、復元サーバーと比較すると、ローカルサイト上にリンクされたマシンがない仮想マシンです。プライマリサーバーは、レプリケーションによるアプリケーションの保護や、さまざまな補助サービスの実行などに使用されます（Webサーバーなど）。

通常、プライマリサーバーは、重要なアプリケーションを実行するサーバー間でのリアルタイムデータレプリケーションに使用されます。アプリケーションのネイティブツールを使用して、自分でレプリケーションをセットアップします。例えば、ローカルサーバーとプライマリサーバーの間でActive Directoryレプリケーションまたは SQLレプリケーションを構成できます。

または、プライマリサーバーを AlwaysOn 可用性グループ（AAG）またはデータベース可用性グループ（DAG）に含めることもできます。

どちらの方法でも、アプリケーションと管理者権限についての深い知識が必要です。プライマリサーバーは、コンピューティングリソースと高速ディザスタリカバリストレージの領域を絶えず消費します。それらはお客様側でメンテナンスが必要です。レプリケーションの監視、ソフトウェアアップデートのインストール、バックアップです。メリットは、サーバー全体をクラウドにバックアップする場合と比較して、本番環境への負荷を最小限に抑えた最小限の RPO と RTO です。

プライマリサーバーは本番ネットワーク上でのみ常に起動されており、以下のネットワークパラメータがあります。

- **クラウドネットワーク**（必須）: プライマリサーバーが接続されるクラウドネットワークです。
- **本番ネットワークにおける IP アドレス**（必須）:プライマリサーバーが本番ネットワークで持つ IP アドレス。デフォルトでは、本番ネットワークの最初の空き IP アドレスが設定されています。
- **パブリックIPアドレス**（オプション）:インターネットからプライマリサーバーにアクセスするためのIPアドレス。サーバーにパブリックIPアドレスがない場合、インターネット経由ではなくローカルネットワークからのみアクセスできます。
- **インターネットアクセス**（オプション）: プライマリサーバーがインターネットにアクセスすることを可能にします。

マルチサイトIPsec VPN接続

注意
この機能を利用できるかどうかは、現在のアカウントで有効になっているサービスクォータによって異なります。

マルチサイトIPsec VPN接続を使用して、セキュアなL3 IPsec VPN接続を介した単一ローカルサイトの接続、または複数ローカルサイトのCyber Disaster Recovery Cloudへの接続が行えます。

この接続タイプは、ディザスタリカバリシナリオが次のユースケースに該当する場合に便利です。

- 重要なワークロードをホストする単一のローカルサイトがある。
- 重要なワークロードをホストする複数のローカルサイトがある（異なるロケーションにオフィスがあるなど）。
- サードパーティ製ソフトウェアのサイト、もしくはマネージドサービスプロバイダのサイトを使用しており、 それらがIPsec VPNトンネルを介して接続されている。

ローカルサイトとクラウドサイト間のマルチサイトIPsec VPN通信を確立するには、**VPNゲートウェイ**が使用されます。Cyber Protectコンソールでマルチサイトipsec VPN通信の設定を開始する場合には、VPNゲートウェイが自動的にクラウドサイトに配置されます。クラウドネットワークセグメントを設定し、ローカルネットワークセグメントと重複しないようにする必要があります。セキュアなVPNトンネルがローカルサイトとクラウドサイト間に確立されます。ローカルサーバーとクラウドサーバーはこのVPNトンネルを介してあたかもそれらすべてが同じイーサネットセグメント内にあるかのように通信できます。

各ソースマシンを保護するために、クラウドサイトにリカバリサーバーを作成する必要があります。フェールオーバーイベントが生じるまで**スタンバイ**状態を保ちます。（**本番モード**で）災害が発生しフェールオーバープロセスを開始すると、保護されたマシンの厳密なコピーであるリカバリサーバーがクラウドで起動します。顧客は、バックグラウンドでの変更に気付くことなくサーバーでの作業を続けることができます。

フェールオーバープロセスを**テストモード**で起動することもできます。これは、ソースマシンがまだ機能しているときに、同時にそれぞれの復元サーバーがクラウドで作成された特別な仮想ネットワーク（**テストネットワーク**）で起動することを意味します。テストネットワークは、他のクラウドネットワークセグメント内でのIPアドレスの重複を防ぐために隔離されています。

VPN ゲートウェイ

ローカルサイトとクラウドサイト間の通信を可能にする主要なコンポーネントは**VPNゲートウェイ**です。これは、特別なソフトウェアがインストールされ、ネットワークが特異的に構成されているクラウド内の仮想マシンです。VPNゲートウェイは以下の機能を提供します。

- ローカルネットワークのイーサネットセグメントとクラウド内の稼働中のネットワークをL3 IPsecモードで接続。
- テストネットワークと稼働しているネットワークのマシンのデフォルトルーターおよびNATとして動作。
- DHCPサーバーとして動作。本番ネットワークとテストネットワークのすべてのマシンはDHCPを介してネットワークの構成（IPアドレス、DNS設定）を取得します。クラウドサーバーは毎回、DHCPサーバーから同一のIPアドレスを取得します。

  必要に応じて、カスタムDNS構成を設定できます。詳細については、"カスタムDNSサーバーの構成"（750ページ）を参照してください。
- キャッシングDNSとして動作。

ルーティングが動作する仕組み

クラウドネットワーク間のルーティングはクラウドサイトのルーターで実行され、異なるクラウドネットワークに属するサーバー同士で通信できます。

ポイントツーサイトリモートVPNアクセス

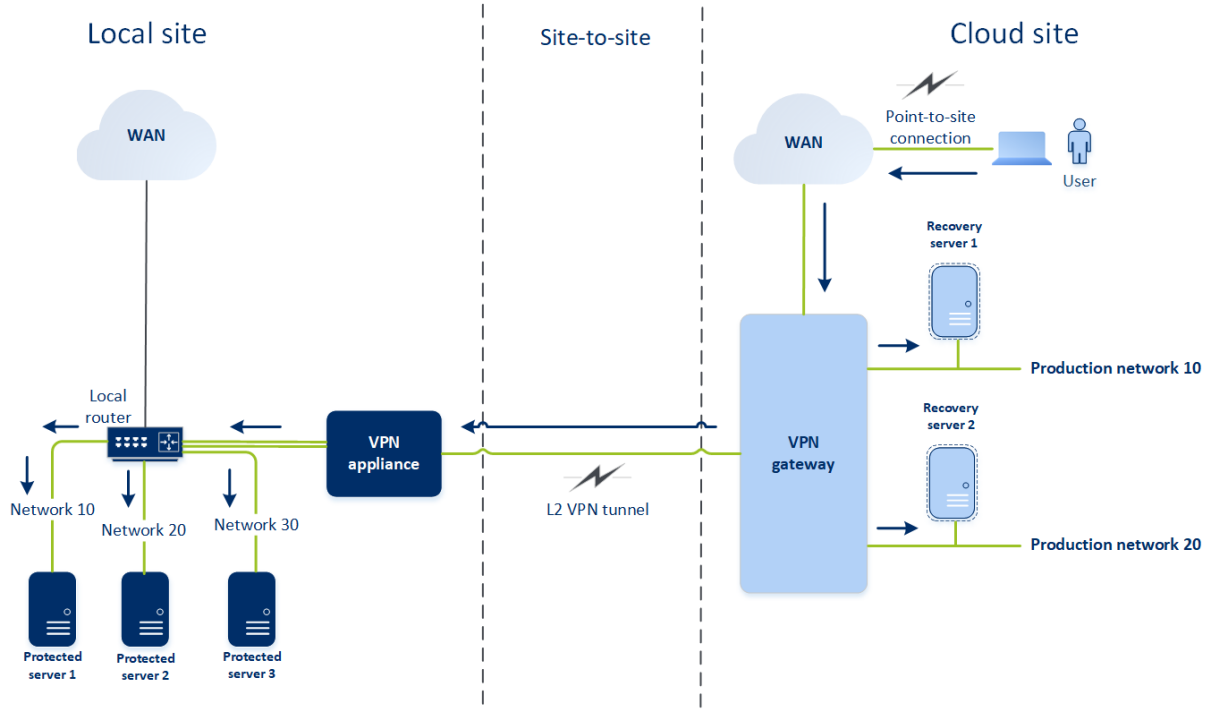
注意
この機能を利用できるかどうかは、現在のアカウントで有効になっているサービスクォータによって異なります。

ポイントツーサイト接続は、エンドポイントデバイス（コンピューターまたはノートPCなど）を使用して外部からクラウドサイトおよびローカルサイトにVPN経由で接続する安全な接続方法です。Cyber Disaster Recovery Cloudサイトへのサイト間Open VPN接続を確立した後に利用できます。このタイプの接続は次の場合に便利です。

- 多くの企業では、自社のサービスとWebリソースは、社内ネットワークに存在する場合のみ利用可能です。ポイントツーサイト接続を使用すると、ローカルサイトにセキュアに接続できます。
- 災害が発生し、ワークロードがクラウドサイトに切り替えられ、ローカルネットワークが停止した場合、クラウドサーバーに直接アクセスする必要があります。これは、クラウドサイトへのポイントツーサイト接続により可能となります。

ローカルサイトへのポイントツーサイト接続には、ローカルサイトにVPNアプライアンスをインストールしてからサイト間接続を設定し、その後ローカルサイトへのポイントツーサイト接続を設定する必要があります。これにより、リモートの従業員は、L2 VPNを介して社内ネットワークにアクセスできるようになります。

以下の図では、ローカルサイト、クラウドサイト、サーバー間通信が緑色で示されています。L2 VPNトンネルにより、ローカルサイトとクラウドサイトが接続されています。ユーザーがポイントツーサイト接続を確立すると、ローカルサイトへの通信がクラウドサイト経由で実行されます。



ポイントツーサイト構成では、証明書を使用してVPNクライアントを認証します。加えて、認証にはユーザー資格情報が使用されます。ローカルサイトへのポイントツーサイト接続については、次の点に注意してください。

- ユーザーはVPNクライアントでの認証にCyber Protect Cloudの資格情報を使用する必要があります。ユーザーには、「企業管理者」または「サイバープロテクション」ユーザーロールが必要です。
- OpenVPN設定を再生成した場合、クラウドサイトへのポイントツーサイト接続を使用しているすべてのユーザーにアップデートされた設定を提供する必要があります。

クラウドサイトで使用されていないカスタマー環境の自動削除

ディザスタリカバリサービスは、ディザスタリカバリ目的で作成されたカスタマー環境の使用状況をトラックします。カスタマー環境が使用されていない場合は、自動的に削除されます。

カスタマーテナントがアクティブかどうかを定義するために、次の条件が使用されます。

- 現在少なくとも1つのクラウドサーバーが存在するか、過去7日以内にクラウドサーバーが存在していた。
  または
- **[ローカルサイトへのVPNアクセス]** オプションが有効化されて、サイト間Open VPNトンネルが確立されるか、VPNアプライアンスから提供された過去7日のレポートデータが存在する。

残りのすべてのテナントは、非アクティブのテナントと見なされます。このようなテナントについてはシステムで次の処理が実行されます。

- VPNゲートウェイとテナントに関連するすべてのクラウドリソースを削除。
- VPNアプライアンスの登録を解除。

非アクティブなテナントは、接続が設定される前の状態にロールバックされます。

初期接続設定

このセクションでは、接続設定シナリオについて説明します。

クラウド限定モードの構成

クラウド限定モードでの接続を構成するには

1. Cyber Protectコンソールで、**[ディザスタリカバリ]** > **[接続]** の順に移動します。
2. **[クラウド限定]** を選択し、**[設定]** をクリックします。
   その結果、VPNゲートウェイと、定義済みのアドレスおよびマスクを持つクラウドネットワークがクラウドサイトに配置されます。

クラウドでのネットワーク管理方法およびVPNゲートウェイの設定方法については、「クラウドネットワークの管理」を参照してください。

サイト間Open VPNの構成

注意
この機能を利用できるかどうかは、現在のアカウントで有効になっているサービスクォータによって異なります。

VPNアプライアンスの要件

システム要件

- 1個のCPU
- 1GBのRAM
- 8GBのディスク容量

ポート

- TCP 443（送信）- VPN接続用
- TCP 80（送信）- アプライアンスの自動アップデート用

ファイアウォールおよびネットワークセキュリティのその他のコンポーネントで、これらのポートを通じて任意のIPアドレスに接続できることを確認します。

サイト間Open VPN接続の構成

VPNアプライアンスは、安全なVPNトンネルを経由してローカルネットワークをクラウドに拡張します。この種の接続は、しばしば「サイトツーサイト」（S2S）接続と呼ばれます。以下の手順を実行するか、ビデオチュートリアルを視聴できます。

VPNアプライアンスを介した接続を構成するには

1. Cyber Protectコンソールで、**[ディザスタリカバリ]** > **[接続]** の順に移動します。
2. **[サイト間Open VPN接続]** を選択し、**[構成]** をクリックします。
   システムはクラウドにVPNゲートウェイを展開し始めます。これには時間がかかります。一方、次のステップに進むことができます。

   注意
   VPNゲートウェイは追加料金なしで提供されます。ディザスタリカバリ機能が使用されていない場合、つまりプライマリサーバーまたは復元サーバーがクラウドに7日間存在しない場合、このファイルは削除されます。

3. **[VPNアプライアンス]** ブロックで、**[ダウンロードとデプロイ]** をクリックします。使用している仮想化プラットフォームに応じて、VMware vSphere または Microsoft Hyper-V 用の VPN アプライアンスをダウンロードします。
4. アプライアンスをデプロイし、本番ネットワークに接続します。
   vSphere では、**無差別モード**および**偽装転送**が有効になっており、VPN アプライアンスを本番ネットワークに接続するすべての仮想スイッチに対して**受け入れる**に設定されていることを確認します。これらの設定にアクセスするには、vSphere クライアントで [ホスト] > **[概要]** > **[ネットワーク]** > [スイッチを選択] > **[編集設定...]** > **[セキュリティ]** を選択します。
   Hyper-Vで、1024MBのメモリを搭載した**第1世代**の仮想マシンを作成します。マシンの**ダイナミックメモリ**を有効にすることを推奨します。マシンが作成されたら、**[設定]** > **[ハードウェア]** > **[ネットワークアダプタ]** > **[高度な機能]** に移動し、**[MACアドレスなりすまし有効]** チェックボックスをオンにします。
5. アプライアンスの電源を投入します。
6. アプライアンスコンソールを開き、「admin」/「admin」ユーザー名とパスワードでログインします。
7. （オプション）パスワードを変更します。
8. （オプション）必要であれば、ネットワーク設定を変更します。どのインターフェースが、インターネット接続のWANとして使用されるかを定義します。
9. 企業管理者の資格情報を使用して、Cyber Protectionサービスにアプライアンスを登録します。
   これらの資格情報は、証明書を取得するときに一度だけ使用されます。データセンターのURLは定義済みです。

   注意
   アカウントに二要素認証が設定されている場合、TOTPコードの入力も求められます。二要素認証が有効になっているもののアカウントに設定されていない場合、VPNアプライアンスを登録することはできません。まず、Cyber Protectコンソールのログインページへ移動し、アカウントのための二要素認証設定を完了する必要があります。二要素認証の詳細については、管理ポータル管理者ガイドをご覧ください。

設定が完了すると、アプライアンスは**オンライン**ステータスになります。アプライアンスはVPNゲートウェイに接続し、すべてのアクティブなインターフェースからCyber Disaster Recovery Cloudサービス

へのネットワークについての情報のレポートを開始します。Cyber Protectコンソールは、VPNアプライアンスからの情報に基づいてインターフェイスを表示します。

マルチサイトIPsec VPNの構成

注意
この機能を利用できるかどうかは、現在のアカウントで有効になっているサービスクォータによって異なります。

次の2つの方法で、マルチサイトIPsec VPN接続を構成できます。

- **[ディザスタリカバリ]** > **[接続]** タブから。
- 1台または複数のデバイスで保護計画を適用します。次に自動で作成されたサイト間Open VPN接続を手動でマルチサイトIPsec VPN接続に切り替え、マルチサイトIPsec VPN設定を構成してIPアドレスを再割り当てします。

[接続] タブからマルチサイトIPsec VPN接続を構成するには

1. Cyber Protectコンソールで、**[ディザスタリカバリ]** > **[接続]** の順に移動します。
2. **[マルチサイトVPN接続]** セクションで、**[設定]** をクリックします。
   VPNゲートウェイがクラウドサイトに配置されます。
3. マルチサイトIPsec VPN設定を構成する。

保護計画からマルチサイトIPsec VPN接続を構成するには

1. Cyber Protectコンソールで **[デバイス]** に進みます。
2. 一覧から1台または複数のデバイスに保護計画を適用します。
   復元サーバーとクラウドインフラ設定が自動的にサイト間Open VPN接続に設定されます。
3. **[Disaster Recovery]** > **[接続]** の順に移動します。
4. **[プロパティを表示]** をクリックします。
5. **[マルチサイトIPsec VPNへの切り替え]** をクリックします。
6. マルチサイトIPsec VPN設定を構成する。
7. クラウドネットワークとクラウドサーバーのIPアドレスを再割り当てする。

マルチサイトIPsec VPN設定の構成

注意
この機能を利用できるかどうかは、現在のアカウントで有効になっているサービスクォータによって異なります。

マルチサイトIPsec VPNを構成後、**[ディザスタリカバリ]** > **[接続]** タブでクラウドサイトとローカルサイトの設定を行う必要があります。

前提条件

- マルチサイトIPsec VPN接続が設定されている。マルチサイトIPsec VPN接続の設定の詳細については、"マルチサイトIPsec VPNの構成"（736ページ）を参照してください。
- 各ローカルIPsec VPNゲートウェイにはパブリックIPアドレスがあります。
- （稼働中のネットワークの）保護されているマシンのコピーであるクラウドサーバー用のIPアドレスと、復元サーバー用のIPアドレス（必要に応じて、1つまたは2つのIPアドレス）が、クラウドネットワークで確保されます。
- （ローカルサイトとクラウドサイト間でファイアウォールを使用する場合）ローカルサイトで次のIPプロトコルとUDPポートに許可を付与します。IPプロトコルID 50（ESP）、UDPポート500（IKE）、UDPポート4500。
- ローカルサイトのNAT-T構成が無効になっています。

マルチサイトIPsec VPN接続を構成するには

1. クラウドサイトに1つ以上のネットワークを追加します。
   a. **[ネットワークを追加]** をクリックします。

   注意
   クラウドネットワークを追加すると、テストフェールオーバーを実行するために、対応するテストネットワークが、同じネットワークアドレスとマスクを使用して自動的に追加されます。テストネットワーク内のクラウドサーバーには、クラウドで稼働中のネットワークと同じIPアドレスが与えられます。テストフェールオーバー中に稼働中のネットワークからクラウドサーバーにアクセスする必要がある場合は、復元サーバーを作成する際に、2番目のテストIPアドレスを割り当てます。

   b. **[ネットワークアドレス]** フィールドで、ネットワークのIPアドレスを入力します。
   c. **[ネットワークマスク]** フィールドで、ネットワークのマスクを入力します。
   d. **[追加]** をクリックします。
2. ローカルサイトの推奨事項に沿って、クラウドサイトに接続する各ローカルサイトの設定を行います。これらの推奨事項の詳細については、「"ローカルサイト向けの一般的な推奨事項"（738ページ）」を参照してください。
   a. **[接続を追加]** をクリックします。
   b. ローカルVPNゲートウェイの名前を入力します。
   c. ローカルVPNゲートウェイの公開IPアドレスを入力します。
   d. （オプション） ローカルVPNゲートウェイの説明を入力します。
   e. **[次へ]** をクリックします。
   f. **[事前共有鍵]** フィールドで、事前共有鍵を入力するか、**[新しい事前共有鍵を生成]** をクリックして自動生成される値を使用します。

   注意
   ローカルおよびクラウドのVPNゲートウェイに同じ事前共有鍵を使用する必要があります。

g. **[IPsec/IKEセキュリティ設定]** をクリックして、設定を行います。構成可能な設定の詳細については、「"IPsec/IKEセキュリティ設定"（739ページ）」を参照してください。

注意
自動入力されるデフォルトの設定か、カスタム値を使用できます。IKEv2プロトコル接続のみがサポートされています。VPN確立時のデフォルトの **[起動アクション]** は **[追加]**（ローカルVPNゲートウェイから接続が開始される）ですが、**[開始]**（クラウドVPNゲートウェイから接続が開始される）か **[ルート]**（ルートオプションをサポートするファイアウォールに適しています）に変更できます。

h. **[ネットワークポリシー]** を構成します。
ネットワークポリシーでは、ネットワークが接続するIPsec VPNを指定します。CIDR形式を使用して、ネットワークのIPアドレスとマスクを入力します。ローカルネットワークとクラウドネットワークワークは、重複してはいけません。

i. **[保存]** をクリックします。

ローカルサイト向けの一般的な推奨事項

注意
この機能を利用できるかどうかは、現在のアカウントで有効になっているサービスクォータによって異なります。

ローカルサイトにマルチサイトIPsec VPN接続を設定する場合、次の推奨事項を考慮してください。

- IKEフェーズごとに、クラウドサイトで次のパラメータの値を少なくとも1つ設定します。暗号化アルゴリズム、ハッシュアルゴリズム、ディフィーヘルマン群数。
- IKEフェーズ2については、クラウドサイトで設定されるディフィーヘルマン群数の値の少なくとも1つでPerfect Forward Secrecyを有効にします。
- IKEフェーズ1とIKEフェーズ2の **[ライフタイム]** をクラウドサイトと同様に設定します。
- NATトラバーサル（NAT-T）を使用した構成はサポートされていません。ローカルサイトでNAT-T構成を無効にしてください。それ以外の場合、追加のUDPカプセルとのネゴシエイトを実行できなくなる可能性があります。
- どちらの側から接続を開始するかは、**[起動アクション]** 設定で定義します。デフォルト値の **[追加]** を選択すると、ローカルサイトから接続が開始され、クラウドサイトは接続の開始を待機します。クラウドサイトから接続を開始する場合は、値を **[開始]** に変更します。また、両方の側から接続を開始できるようにする場合（ルートオプションをサポートするファイアウォールに適しています）は、値を **[ルート]** に変更します。

別のソリューションの詳細と設定例については、次を参照してください。

- この一連のナレッジベースの記事
- このビデオの例

IPsec/IKEセキュリティ設定

注意
この機能を利用できるかどうかは、現在のアカウントで有効になっているサービスクォータによって異なります。

Psec/IKEセキュリティパラメータの詳細を次の表に示します。

パラメータ	説明
暗号化アルゴリズム	転送中のデータが見えないようにするために使用される暗号化アルゴリズムです。デフォルト設定では、すべてのアルゴリズムが選択されています。各IKEフェーズを対象とするローカルゲートウェイデバイスで、選択されたアルゴリズムのうち少なくとも1つを構成する必要があります。
ハッシュアルゴリズム	データのインテグリティと真正性を検証するために使用されるハッシュアルゴリズムです。デフォルト設定では、すべてのアルゴリズムが選択されています。各IKEフェーズを対象とするローカルゲートウェイデバイスで、選択されたアルゴリズムのうち少なくとも1つを構成する必要があります。
ディフィーヘルマン群数	ディフィーヘルマン群数により、インターネット鍵交換（IKE）プロセスで使用される鍵の強度を定義します。 群位数が高いほど安全ですが、鍵の算出に要する時間は長くなります。 デフォルト設定では、すべての群が選択されています。各IKEフェーズを対象とするローカルゲートウェイデバイスで、選択された群のうち少なくとも1つを構成する必要があります。
ライフタイム（秒）	ライフタイム値により、ネゴシエーションが成功してから有効期限が切れるまでの、ユーザーパケットの暗号化/認証鍵のセットを持つ接続インスタンスの持続時間を決定します。 フェーズ1の範囲:900-28800秒（デフォルトでは28800秒）。 フェーズ2の範囲:900-3600秒（デフォルトでは3600秒）。 フェーズ2のライフタイムは、フェーズ1のライフタイムより短くする必要があります。

パラメータ	説明
	接続は、期限が切れるまでにキー設定チャネルを通じて再ネゴシエートされます。「**キー再設定のマージン時間**」を参照してください。ローカルサイドとリモートサイドでライフタイムが一致しない場合、ライフタイムが長い方のサイドで優先されたコネクションのクラッタが発生します。「**キー再設定のマージン時間**」と「**キー再設定ファズ**」も参照してください。
キー再設定のマージン時間（秒）	VPN接続のローカル側で交換のネゴシエートを試行する際に、接続の有効期限またはキー設定チャネルの有効期限に設けられるマージン時間。キー再設定の正確な時間は、**キー再設定ファズ**の値に基づいてランダムに選択されます。これはローカルにのみ関係します。リモート側でこれに同意する必要はありません。範囲:900-3600秒。デフォルト値は3600です。
リプレイウィンドウサイズ（パケット）	この接続に対応するIPsecのリプレイウィンドウサイズです。 デフォルトの-1にすると、strongswan.confファイルのcharon.replay_windowで設定される値を使用します。 32より大きな値は、Netlinkバックエンドを使用する際にのみサポートされます。 値を0にすると、IPsecリプレイ保護が無効になります。
キー再設定ファズ（%）	マージンバイト、マージンパケット、マージン時間をランダムに増加させて、キー再設定の間隔をランダムにする最大パーセンテージです（接続数の多いホストでは重要）。 キー再設定ファズ値は、100%を超過する場合があります。ランダムで増加させた後に、marginTYPEの値がlifeTYPEの値を超えてはいけません。TYPEには、bytes、packets、timeのいずれかが入ります。 値を0%にすると、ランダム化が無効になります。これはローカルにのみ関係します。リモート側でこれに同意する必要はありません。
DPDタイムアウト（秒）	デッドピア検出（DPD）タイムアウトが発生した後の時間です。値は30より上で指定できます。デフォルト値は30です。
デッドピア検出（DPD）タイムアウトアク	デッドピア検出（DPD）タイムアウトが発生した後

パラメータ	説明
ション	に実行するアクションです。 **再起動**: DPDタイムアウトが発生したときに、セッションを再起動します。 **クリア**: DPDタイムアウトが発生したときに、セッションを終了します。 **指定しない**: DPDタイムアウトが発生したときのアクションを指定しません。
起動アクション	どちらの側から接続を開始してVPN接続のトンネルを確立するかを決定します。 **追加**: ローカルVPNゲートウェイから接続を開始します。 **開始**: クラウドVPNゲートウェイから接続を開始します。 **ルート**:ルートオプションをサポートするVPNゲートウェイに適しています。トンネルは、ローカルのVPNゲートウェイまたはクラウドのVPNゲートウェイのいずれかから開始されたトラフィックが存在する場合にのみ起動します。

Active Directoryドメインサービスのアベイラビリティーに関する推奨事項

保護済みワークロードがドメインコントローラーでの認証を必要する場合は、ディザスタリカバリサイトにActive Directoryドメインコントローラー（AD DC）インスタンスを用意することを推奨します。

L2 Open VPN接続用Active Directoryドメインコントローラー

L2 Open VPN接続を使用する場合、テストフェールオーバーまたは本番フェールオーバーの間、保護済みワークロードのIPアドレスはクラウドサイトで保持されます。そのため、テストフェールオーバーまたは本番フェールオーバーの間のAC DCのIPアドレスは、ローカルサイトのものと同じになります。

カスタムDNSを使用する場合は、すべてのクラウドサーバーに対して独自のカスタムDNSサーバーを設置できます。詳細については、"カスタムDNSサーバーの構成"（750ページ）を参照してください。

L3 IPsec VPN接続用Active Directoryドメインコントローラー

L3 IPsec VPN接続を使用する場合、保護済みワークロードのIPアドレスはクラウドサイトで保持されません。そのため、本番フェールオーバーを実行する前に、他の専用AD DCインスタンスをプライマリサーバーとしてクラウドサイトに用意することを推奨します。

専用AD DCインスタンスをプライマリサーバーとしてクラウドサイトで設定する場合の推奨事項は次の通りです。

- Windowsファイアウォールをオフにする。
- プライマリサーバーをActive Directoryサービスに接続する。
- プライマリサーバーがインターネットに接続できることを確認する。
- Active Directory機能を追加する。

カスタムDNSを使用する場合は、すべてのクラウドサーバーに対して独自のカスタムDNSサーバーを設置できます。詳細については、"カスタムDNSサーバーの構成"（750ページ）を参照してください。

ポイントツーサイトリモートVPNアクセスの構成

注意
この機能を利用できるかどうかは、現在のアカウントで有効になっているサービスクォータによって異なります。

ローカルサイトにリモート接続する必要がある場合は、ローカルサイトへのポイントツーサイト接続を構成できます。以下の手順を実行するか、ビデオチュートリアルを視聴できます。

前提条件

- サイト間Open VPN接続が設定されている。
- VPNアプライアンスがローカルサイトにインストールされている。

ローカルサイトへのポイントツーサイト接続を構成するには

1. Cyber Protectコンソールで、**[ディザスタリカバリ]** > **[接続]** の順に移動します。
2. **[プロパティを表示]** をクリックします。
3. **[ローカルサイトへのVPNアクセス]** オプションを有効にします。
4. ローカルサイトへのポイントツーサイト接続を確立する必要があるユーザーが、
   - Cyber Protect Cloudにユーザーアカウントを所有していることを確認する。これらの資格情報は、VPNクライアントでの認証に使用されます。所有していない場合は、Cyber Protect Cloudにユーザーアカウントを作成します。
   - 「企業管理者」または「サイバープロテクション」ユーザーロール。
5. OpenVPNクライアントの構成
   a. OpenVPNクライアントバージョン2.4.0以降を、https://openvpn.net/community-downloads/からダウンロードします。
   b. ローカルサイトに接続するマシンにOpenVPNクライアントをインストールします。
   c. **[OpenVPN の設定のダウンロード]** をクリックします。構成ファイルは、組織の「企業管理者」または「サイバープロテクション」ユーザーロールを持つユーザーに対して有効です。
   d. OpenVPNにダウンロード済みの設定をインポートします。
   e. Cyber Protect Cloudユーザーの資格情報でOpenVPNクライアントにログインします（上記の手順4を参照）。
   f. （オプション）組織で二要素認証が有効になっている場合は、1回限りのTOTPコードを入力する必要があります。

重要
アカウントで二要素認証を有効化した場合は、構成ファイルを再生成して、既存のOpenVPNで構成ファイルを更新する必要があります。アカウントに二要素認証を設定するには、Cyber Protect Cloudに再度ログインする必要があります。

これによりユーザーはローカルサイト上のマシンに接続できるようになります。

ネットワーク管理

このセクションでは、ネットワーク管理シナリオについて説明します。

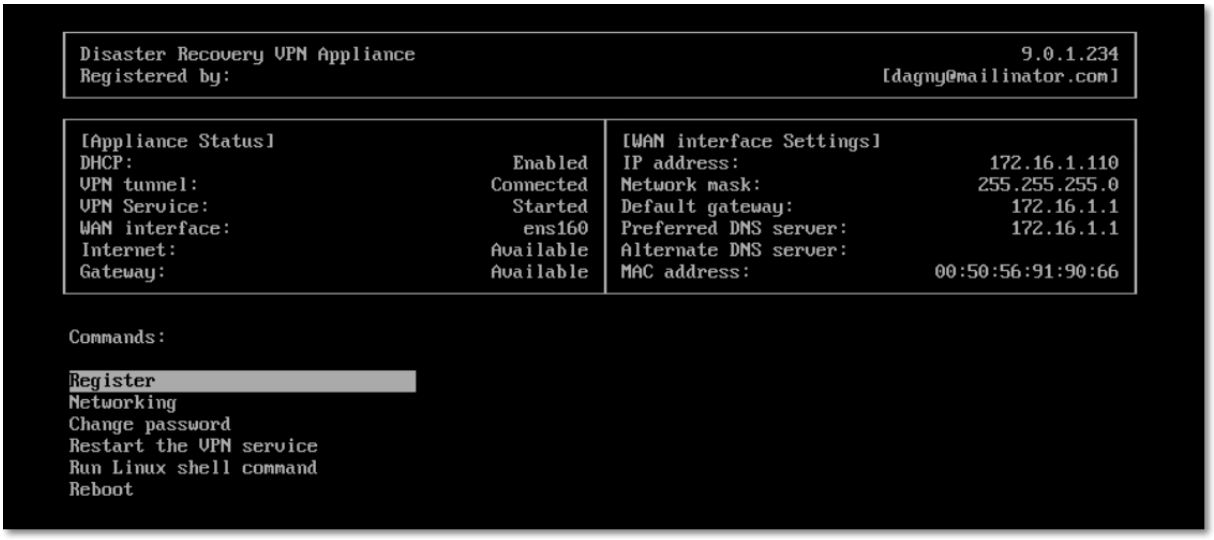
ネットワークの管理

注意
適用されるライセンスモデルによっては、一部の機能で追加のライセンスが必要になる場合があります。

サイト間Open VPN接続

ローカルサイトにネットワークを追加してクラウドに拡張するには

1. VPNアプライアンスで、クラウド内に拡張するローカルネットワークとの新しいネットワークインターフェースを設定します。
2. VPNアプライアンスコンソールにログインします。
3. **ネットワーク**セクションで、新しいインターフェースのためのネットワーク設定を行ないます。



VPNアプライアンスは、すべてのアクティブなインターフェイスからCyber Disaster Recovery Cloudへのネットワークについての情報のレポートを開始します。Cyber Protectコンソールは、VPNアプライアンスからの情報に基づいてインターフェイスを表示します。

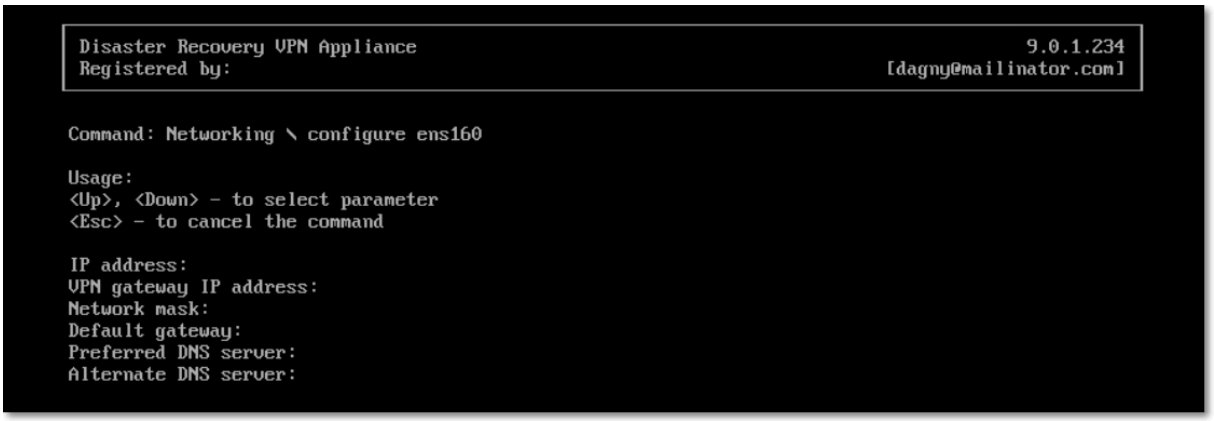
クラウドに拡張したネットワークを削除するには

1. VPNアプライアンスコンソールにログインします。
2. **ネットワーク**セクションで、削除するインターフェースを選択してから、**[ネットワーク設定の消去]** をクリックします。
3. 処理を確認します。

その結果、セキュアなVPNトンネル経由でのクラウドへのローカルネットワーク拡張が停止します。このネットワークは独立したクラウドセグメントとして稼働します。このインターフェースを使用してクラウドサイトから（へ）トラフィックを渡すと、クラウドサイトから（へ）のすべてのネットワーク接続が切断されます。

ネットワークパラメータを変更するには

1. VPNアプライアンスコンソールにログインします。
2. **ネットワーク**セクションで、編集するインターフェースを選択します。
3. **[ネットワーク設定の編集]** をクリックします。
4. 2つの可能なオプションのうちの1つを選択します。
   - DHCPを介した自動ネットワーク構成については、**[DHCPを使用]** をクリックします。処理を確認します。
   - 手動ネットワーク構成については、**[静的IPアドレスを設定]** をクリックします。次の設定を編集に使用できます。
     - **[IP アドレス]**: ローカルネットワークにおけるインターフェースの IP アドレスです。
     - **[VPNゲートウェイのIPアドレス]**: 適切なCyber Disaster Recovery Cloudサービス作業のためにネットワークのクラウドセグメント用に予約されている特別なIPアドレスです。
     - **[ネットワークマスク]**: ローカルネットワークのネットワークマスクです。
     - **[デフォルトゲートウェイ]**: ローカルサイト上のデフォルトゲートウェイです。
     - **[優先 DNS サーバー]**: ローカルサイト上のプライマリ DNS サーバーです。
     - **[代替 DNS サーバー]**: ローカルサイト上のセカンダリ DNS サーバーです。



- 必要な変更を実行し、[実行] をクリックして確認します。

クラウド限定モード

クラウドには最大で23個のネットワークを設定できます。

新しいクラウドネットワークを追加するには

1. **[Disaster Recovery]** > **[接続]** の順に移動します。
2. **[クラウドサイト]** で、**[クラウドネットワークを追加]** をクリックします。
3. ネットワークアドレスとマスクを含む、クラウドネットワークパラメータを定義します。準備ができたら、**[完了]** をクリックします。

その結果、定義済みのアドレスおよびマスクを持つ追加のクラウドネットワークがクラウドサイトに作成されます。

クラウドネットワークを削除するには

注意
1つ以上のクラウドサーバーが含まれているクラウドネットワークは、削除できません。まずクラウドサーバーを削除し、それからネットワークを削除します。

1. **[Disaster Recovery]** > **[接続]** の順に移動します。
2. **クラウドサイト**で、削除するネットワークアドレスをクリックします。
3. **[削除]** をクリックして、操作を確定します。

クラウドネットワークパラメータを変更するには

1. **[Disaster Recovery]** > **[接続]** の順に移動します。
2. **クラウドサイト**で、編集するネットワークアドレスをクリックします。
3. **[編集]** をクリックします。
4. ネットワークアドレスとマスクを定義し、**[完了]** をクリックします。

IPアドレスの再構成

適切なディザスタリカバリパフォーマンスのために、ローカルサーバとクラウドサーバに割り当てられているIPアドレスは一致している必要があります。IPアドレスに矛盾や不一致がある場合は、**[Disaster Recovery]** > **[接続]** の対応するネットワークの横に感嘆符が表示されます。

IPアドレスの不一致の、一般的に知られている理由の幾つかを以下に示します。

1. 復元サーバーが、あるネットワークから別のネットワークに移行された、またはクラウドネットワークのネットワークマスクが変更されました。その結果、クラウドサーバーに、接続されていないネットワークからのIPアドレスがあります。
2. 接続タイプが、サイト間接続なしからサイト間接続へと切り替えられました。その結果、ローカルサーバーは、クラウドサイト上の復元サーバーのために作成されたものとは異なるネットワークに配置されます。
3. 接続タイプが、サイト間Open VPNからマルチサイトIPsec VPN、またはマルチサイトIPsec VPNからサイト間Open VPNに切り替えられました。このシナリオの詳細については、「接続の切り替え」と「IPアドレスの再割り当て」を参照してください。
4. VPNアプライアンスサイトで以下のネットワークパラメータを編集します。
   - ネットワーク設定を介してインターフェースを追加
   - インターフェース設定を介してネットワークマスクを手動で編集
   - DHCPを介してネットワークマスクを編集

- インターフェース設定を介してネットワークアドレスおよびマスクを手動で編集
- DHCPを介してネットワークマスクおよびアドレスを編集

上記のアクションの結果、クラウドサイト上のネットワークがローカルネットワークのサブセットまたはスーパーセットになるか、またはVPNアプライアンスインターフェースが、異なるインターフェイスに対して同じネットワーク設定をレポートすることがあります。

ネットワーク設定上の問題を解決するには

1. IPアドレスの再構成が必要なネットワークをクリックします。
   選択したネットワーク内のサーバーのリスト、それらのステータス、およびIPアドレスが表示されます。ネットワーク設定に矛盾があるサーバーは、感嘆符でマークされます。
2. サーバー用のネットワーク設定を変更するには、**[サーバーへ移動]** をクリックします。すべてのサーバー用のネットワーク設定を一括で変更するには、通知ブロックで、**[変更]** をクリックします。
3. **[新規IP]** および **[新規テストIP]** フィールドで定義することにより、必要に応じてIPアドレスを変更します。
4. 準備ができたら、**[確認]** をクリックします。

サーバーを適切なネットワークに移動する

ディザスタリカバリ保護計画を作成し、選択したデバイスに適用するとき、システムによってデバイスのIPアドレスがチェックされ、IPアドレスに適したクラウドネットワークが存在しない場合はクラウドネットワークが自動的に作成されます。デフォルトでは、そのようなクラウドネットワークにはIANAがプライベートでの使用に推奨している最大範囲（10.0.0.0/8、172.16.0.0/12、192.168.0.0/16）が設定されます。ネットワークマスクを編集すれば、ネットワーク範囲を狭くすることができます。

選択されたデバイスが複数のローカルネットワークに属している場合、クラウドサイトのネットワークはそれらのローカルネットワークのスーパーセットになります。この場合、クラウドネットワークを再設定するには次のようにします。

1. ネットワークサイズの再設定が必要なクラウドネットワークをクリックしてから、**[編集]** をクリックします。
2. ネットワークサイズを正しい値に再設定します。
3. その他の必要なネットワークを作成します。
4. ネットワークに接続されたデバイス数の横にある通知アイコンをクリックします。
5. **[適切なネットワークに移動する]** をクリックします。
6. 適切なネットワークに移動するサーバーを選択してから、**[移動]** をクリックします。

VPNアプライアンス設定の管理

注意
この機能を利用できるかどうかは、現在のアカウントで有効になっているサービスクォータによって異なります。

Cyber Protectコンソール（**[ディザスタリカバリ]** > **[接続]**）では、次の操作を実行できます。

- ログファイルをダウンロードする。
- アプライアンスの登録を解除する（VPNアプライアンスの設定をリセットするか、クラウド限定モードに切り替える必要がある場合）。

これらの設定にアクセスするには、**[VPNアプライアンス]** ブロックの **[i]** アイコンをクリックします。

VPNアプライアンスコンソールでは、次の操作を実行できます。

- アプライアンスのパスワードを変更する。
- ネットワーク設定を表示/変更する。インターネット接続用のWANとして使用するインターフェースを定義する。
- （登録を繰り返すことにより）登録アカウントを登録/変更する。
- VPNサービスを再起動する。
- VPNアプライアンスを再起動する。
- Linux Shellコマンドを実行する（高度なトラブルシューティングの場合のみ）。

VPNゲートウェイの再インストール

VPNゲートウェイに解決できない問題が発生した場合は、VPNゲートウェイを再インストールすることをお勧めします。次のような問題が発生する可能性があります。

- VPNゲートウェイが、**エラー**ステータスである。
- VPNゲートウェイが、長時間**保留中**ステータスになる。
- VPNゲートウェイのステータスが、長時間確定されない。

VPNゲートウェイの再インストールでは、既存のVPNゲートウェイ仮想マシンを完全に削除し、テンプレートから新しい仮想マシンをインストールし、新しい仮想マシンに以前のVPNゲートウェイの設定を適用するという自動的な操作が実行されます。

前提条件:

クラウドサイトへの接続タイプの1つを設定する必要があります。

VPNゲートウェイを再インストールするには

1. Cyber Protectコンソールで、**[ディザスタリカバリ]** > **[接続]** の順に移動します。
2. VPNゲートウェイのギアアイコンをクリックし、**[VPNゲートウェイを再インストール]** を選択します。
3. **[VPNゲートウェイを再インストール]** ダイアログで、ログイン情報を入力します。
4. **[再インストール]** をクリックします。

サイト間接続の有効化または無効化

注意
この機能を利用できるかどうかは、現在のアカウントで有効になっているサービスクォータによって異なります。

次のような場合にサイト間接続を有効にできます。

- ローカルサイトのサーバーと通信するためにクラウドサイトのクラウドサーバーが必要である場合。
- クラウドへのフェールオーバーの後、ローカルインフラストラクチャはリカバリされ、サーバーをローカルサイトにフェールバックできます。

サイト間接続を有効にするには

1. **[Disaster Recovery]** > **[接続]** の順に移動します。
2. **[プロパティを表示]** をクリックしてから、**[サイト間接続]** オプションを有効にします。

その結果、ローカルサイトとクラウドサイト間のサイト間VPN接続が有効になります。Cyber Disaster Recovery Cloudサービスは、VPNアプライアンスからネットワーク設定を取得し、ローカルネットワークをクラウドサイトに拡張します。

ローカルサイトのサーバーと通信するためにクラウドサイトのクラウドサーバーが必要ない場合は、サイト間接続を無効にできます。

サイト間接続を無効にするには

1. **[Disaster Recovery]** > **[接続]** の順に移動します。
2. **[プロパティを表示]** をクリックしてから、**[サイト間接続]** オプションを無効にします。

その結果、ローカルサイトがクラウドサイトから切断されます。

サイト間接続タイプの切り替え

注意
この機能を利用できるかどうかは、現在のアカウントで有効になっているサービスクォータによって異なります。

サイト間Open VPN接続からマルチサイトIPsec VPN接続、およびマルチサイトIPsec VPN接続からサイト間Open VPN接続への切り替えを簡単に行うことができます。

接続タイプを切り替える際には、アクティブなVPN接続が削除されますが、クラウドサーバーとネットワーク構成は保持されます。ただし、引き続きクラウドネットワークとクラウドサーバーのIPアドレスを再割り当てする必要があります。

次の表では、サイト間Open VPN接続とマルチサイトIPsec VPN接続の基本的な特徴を比べています。

	サイト間Open VPN	マルチサイトIPsec VPN
ローカルサイトサポート	単一	単一、複数
VPNゲートウェイモード	L2 Open VPN	L3 IPsec VPN
ネットワークセグメント	ローカルネットワークをクラウドネットワークへ拡張	ローカルネットワークとクラウドネットワークワークのセグメントは、重複できない
ローカルサイトへのポイントツーサイトアクセスをサポート	はい	いいえ

	サイト間Open VPN	マルチサイトIPsec VPN
クラウドサイトへのポイントツーサイトアクセスをサポート	はい	はい
パブリックIPの提供項目が必要	いいえ	はい

サイト間Open VPN接続からマルチサイトIPsec VPN接続へ切り替えるには

1. Cyber Protectコンソールで、**[ディザスタリカバリ]** > **[接続]** の順に移動します。
2. **[プロパティを表示]** をクリックします。
3. **[マルチサイトIPsec VPNへの切り替え]** をクリックします。
4. **[再構成]** をクリックします。
5. クラウドネットワークとクラウドサーバーのIPアドレスを再割り当てする。
6. マルチサイトIPsec接続設定を構成する。

マルチサイトIPsec VPN接続からサイト間Open VPN接続へ切り替えるには

1. Cyber Protectコンソールで、**[ディザスタリカバリ]** > **[接続]** の順に移動します。
2. **[プロパティを表示]** をクリックします。
3. **[サイト間Open VPNへの切り替え]** をクリックします。
4. **[再構成]** をクリックします。
5. クラウドネットワークとクラウドサーバーのIPアドレスを再割り当てする。
6. サイト間接続設定を行う。

IPアドレスの再割り当て

注意
この機能を利用できるかどうかは、現在のアカウントで有効になっているサービスクォータによって異なります。

次の場合に設定を完了するには、クラウドネットワークとクラウドサーバーのIPアドレスを再割り当てする必要があります。

- サイト間Open VPNからマルチサイトIPsec VPNに切り替えた後、もしくはその逆。
- 保護計画を適用した後（マルチサイトIPsec VPN接続が構成される場合）。

クラウドネットワークのIPアドレスを再割り当てするには

1. **[接続]** タブで、クラウドネットワークのIPアドレスをクリックします。
2. **[ネットワーク]** ポップアップで、**[編集]** をクリックします。
3. 新しいネットワークアドレスとネットワークマスクを入力します。
4. **[完了]** をクリックします。

クラウドネットワークのIPアドレスを再割り当てしたら、再割り当てされたクラウドネットワークに属するクラウドサーバーの再割り当てを行う必要があります。

サーバーのIPアドレスを再割り当てするには

1. **[接続]** タブで、クラウドネットワークのサーバーのIPアドレスをクリックします。
2. **[サーバー]** ポップアップで、**[IPアドレスを変更する]** をクリックします。
3. **[IPアドレスを変更する]** ポップアップで、サーバーの新しいIPアドレスを入力するか、再割り当てされたクラウドネットワークに含まれる自動生成されたIPアドレスを使用します。

   注意
   Cyber Disaster Recovery Cloudにより、ネットワークIPアドレスの再割り当て前にクラウドネットワークに含まれていたすべてのクラウドサーバーに、クラウドネットワークのIPアドレスが割り当てられます。推奨されたIPアドレスをすべてのクラウドサーバーに対するIPアドレスの再割り当てにすぐに使用できます。

4. **[確認]** をクリックします。

カスタムDNSサーバーの構成

注意
この機能を利用できるかどうかは、現在のアカウントで有効になっているサービスクォータによって異なります。

接続を構成するときには、Cyber Disaster Recovery Cloudがクラウドネットワークインフラストラクチャを作成します。クラウドDHCPサーバーにより、復元サーバーとプライマリサーバーに自動的にデフォルトのDNSサーバーが割り当てられます。ただし、デフォルト設定を変更してカスタムDNSサーバーを構成することが可能です。新しいDNS設定は、DHCPサーバーに対する次回のリクエスト時に適用されます。

前提条件:

クラウドサイトへの接続タイプの1つを設定する必要があります。

カスタムDNSサーバーを構成するには

1. Cyber Protectコンソールで、**[ディザスタリカバリ]** > **[接続]** の順に移動します。
2. **[プロパティを表示]** をクリックします。
3. **[デフォルト（クラウドサイトにより提供）]** をクリックします。
4. **[カスタムサーバー]** を選択します。
5. DNSサーバーのIPアドレスを入力します。
6. [オプション]別のDNSサーバーを追加する場合は、**[追加]** をクリックし、DNSサーバーのIPアドレスを入力します。

   注意
   カスタムDNSサーバーの追加後、デフォルトのDNSサーバーを追加することもできます。そのようにすることで、カスタムDNSサーバーが利用不能な場合に、Cyber Disaster Recovery Cloudがデフォルトの DNSサーバーを使用します。

7. **[完了]** をクリックします。

カスタムDNSサーバーの削除

注意
この機能を利用できるかどうかは、現在のアカウントで有効になっているサービスクォータによって異なります。

カスタムDNSの一覧からDNSサーバーを削除できます。

前提条件:

カスタムDNSサーバーが構成されている。

カスタムDNSサーバーを削除するには

1. Cyber Protectコンソールで、**[ディザスタリカバリ]** > **[接続]** の順に移動します。
2. **[プロパティを表示]** をクリックします。
3. **[カスタムサーバー]** をクリックします。
4. DNSサーバーの横にある削除アイコンをクリックします。

   注意
   利用できるカスタムDNSサーバーが1台だけの場合、削除操作は無効です。カスタムDNSサーバーをすべて削除する場合は、**[デフォルト（クラウドサイトにより提供）]** を選択します。

5. **[完了]** をクリックします。

ローカルルーティングの設定

VPNアプライアンスを介してクラウドに拡張されているローカルネットワークに加えて、VPNアプライアンスに登録されていないもののその中のサーバーがクラウドサーバーと通信する必要がある他のローカルネットワークがあるかもしれません。そのようなローカルサーバーとクラウドサーバー間の接続を確立するため、ローカルルーティングを設定する必要があります。

ローカルルーティングを設定するには

1. **[ディザスタリカバリ]** > **[接続]** の順に移動します。
2. **[プロパティを表示]** をクリックして、**[ローカルルーティング]** をクリックします。
3. CIDR表記でローカルネットワークを指定します。
4. **[保存]** をクリックします。

その結果、指定されたローカルネットワーク経由のサーバーがクラウドサーバーと通信できるようになります。

L2 VPNを介したDHCPトラフィックを許可

ローカルサイトのデバイスがDHCPサーバーからIPアドレスを取得する構成の場合、ディザスタリカバリによるDHCPサーバー保護を利用できます。つまり、DHCPサーバーをクラウドにフェールオーバーしている状態で、DHCPトラフィックをL2 VPN上で処理することが可能です。こうすれば、クラウド上で動作するDHCPサーバーから、ローカルデバイスへのIPアドレス割り当てを続行できます。

前提条件:

クラウドサイトへの接続タイプに、サイト間L2 VPN接続を設定する必要があります。

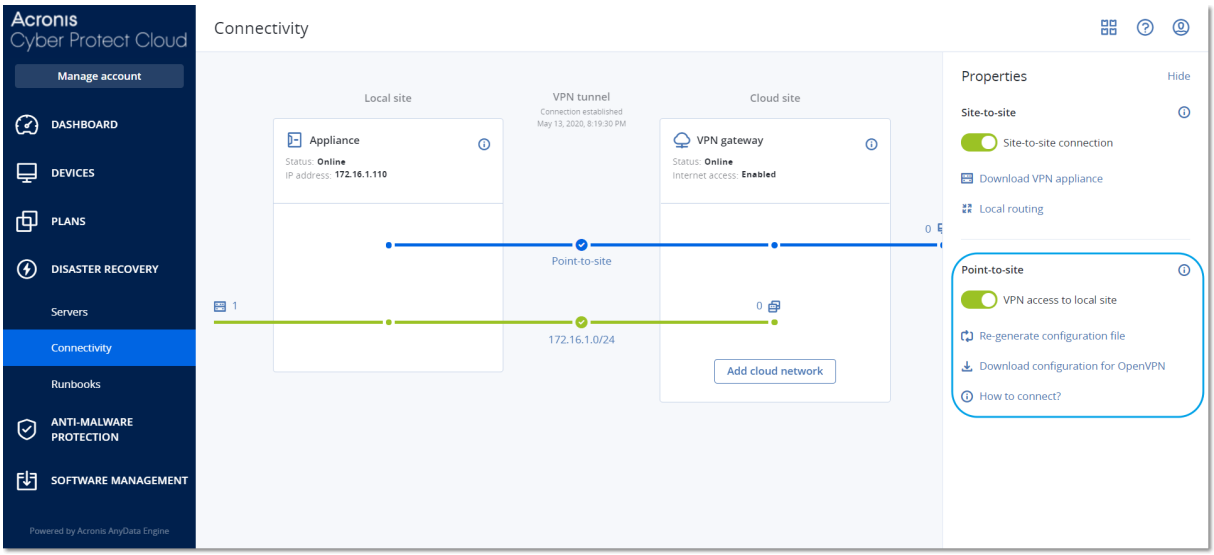
L2 VPN接続によるDHCPトラフィックを許可するには

1. **[ディザスタリカバリ]** > **[接続]** タブに移動します。
2. **[プロパティを表示]** をクリックします。
3. **[L2 VPNを介したDHCPトラフィックを許可]** スイッチを有効化します。

ポイントツーサイト接続設定の管理

注意
この機能を利用できるかどうかは、現在のアカウントで有効になっているサービスクォータによって異なります。

Cyber Protectコンソールで、**[ディザスタリカバリ]** > **[接続]** の順に移動し、右上隅の**[プロパティを表示]** をクリックします。



ローカルサイトへの VPN アクセス

このオプションは、ローカルサイトへのVPNアクセスの管理に使用します。デフォルト設定では、有効になっています。このオプションを無効にすると、ローカルサイトへのポイントツーサイトアクセスが許可されなくなります。

OpenVPNの設定をダウンロード

これは OpenVPN クライアントの設定ファイルをダウンロードします。このファイルは、クラウドサイトへのポイントツーサイト接続を確立するために必要です。

設定を再生成

OpenVPN クライアントの設定ファイルを再生成することができます。

これは、次の場合に必要です。

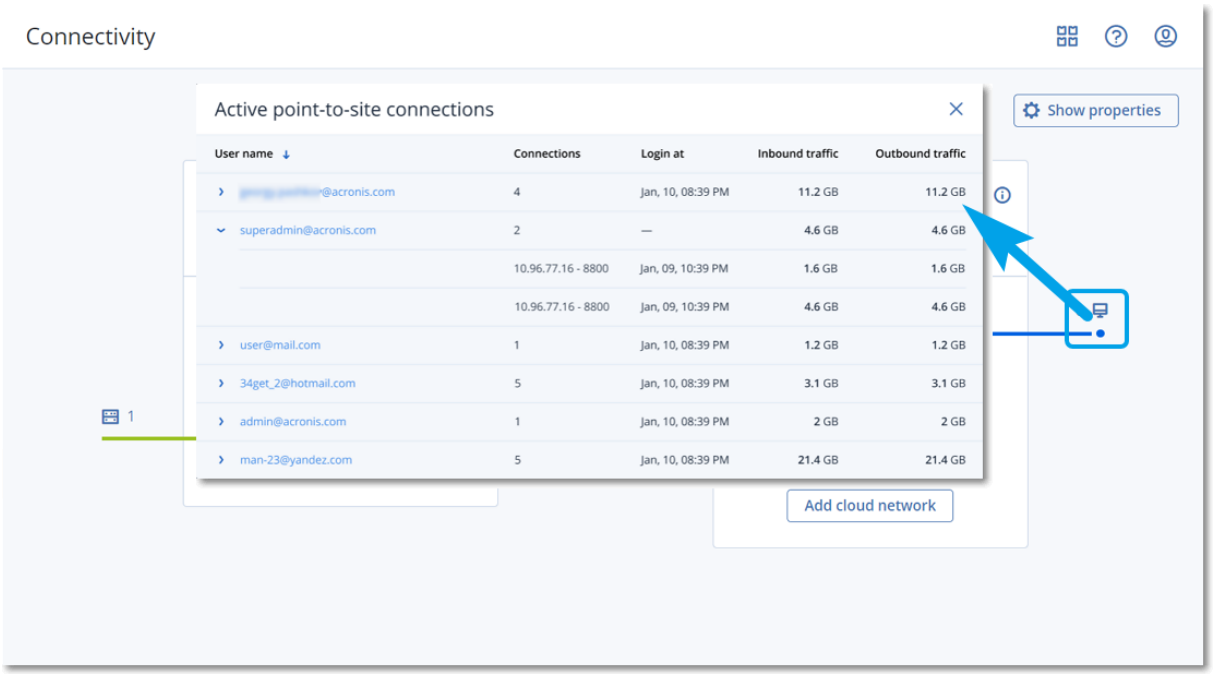
- 設定ファイルが侵害されていると思われる場合。
- 二要素認証がアカウントで有効になっていた場合。

設定ファイルが更新されるとすぐに、古い設定ファイルによる接続は不可能になります。ポイントツーサイト接続の使用を許可されているユーザーに新しいファイルを配布するようにしてください。

有効なポイントツーサイト接続

注意
この機能を利用できるかどうかは、現在のアカウントで有効になっているサービスクォータによって異なります。

アクティブなポイントツーサイト接続は、**[ディザスタリカバリ]** > **[接続]** で確認できます。青の**ポイントツーサイト**ライン上のマシンアイコンをクリックすると、アクティブなポイントツーサイト接続に関する詳細な情報がユーザー名グループ別に表示されます。



ログを利用する

ディザスタリカバリでは、VPNアプライアンスとVPNゲートウェイのログが収集されます。ログは.txtファイルとして保存され、ZIPアーカイブに圧縮されます。アーカイブをダウンロードしてから展開し、トラブルシューティングや監視に利用できます。

次のリストでは、ZIPアーカイブの一部であるログファイルと、そこに含まれる情報について示します。

`dnsmasq.config.txt` - DNSとDHCPアドレスを提供するサービスの構成に関する情報が含まれているファイルです。

`dnsmasq.config.txt` - 現在のDHCPアドレスリースの情報が含まれているファイルです。

`dnsmasq_log.txt` - dnsmasqサービスのログが含まれているファイルです。

`ebtables.txt` - ファイアウォールテーブルに関する情報が含まれているファイルです。

`free.txt` - 空きメモリに関する情報が含まれているファイルです。

`ip.txt` - このファイルには、**ネットワークパケットのキャプチャ**の設定に使用できる名前を含む、ネットワークインターフェースの構成から得られたログが含まれています。

`NetworkManager_log.txt` - NetworkManagerサービスのログが含まれているファイルです。

`NetworkManager_status.txt` - NetworkManagerサービスのステータスに関する情報が含まれているファイルです。

`openvpn@p2s_log.txt` - OpenVPNサービスのログが含まれているファイルです。

`openvpn@p2s_status.txt` - VPNトンネルのステータスに関する情報が含まれているファイルです。

`ps.txt` - VPNゲートウェイまたはVPNアプライアンスで現在実行中のプロセスに関する情報が含まれているファイルです。

`resolf.conf.txt` - DNSサーバーの構成に関する情報が含まれているファイルです。

`routes.txt` - ネットワーキングのルートに関する情報が含まれているファイルです。

`uname.txt` - 現在稼働中のオペレーティングシステムのカーネルバージョンに関する情報が含まれているファイルです。

`uptime.txt` - オペレーティングシステムが再起動されなかった期間に関する情報が含まれているファイルです。

`vpnserver_log.txt` - VPNサービスのログが含まれているファイルです。

`vpnserver_status.txt` - VPNサーバーのステータスに関する情報が含まれているファイルです。

IPsec VPN接続に特化したログファイルについては、"マルチサイトIPsec VPNログファイル"（759ページ）を参照してください。

VPNアプライアンスログのダウンロード

VPNアプライアンスログを含むアーカイブをダウンロードしてから展開し、トラブルシューティングや監視に利用できます。

VPNアプライアンスログをダウンロードするには

1. **接続**ページで、VPNアプライアンスの横にあるギアアイコンをクリックします。
2. **[ログをダウンロード]** をクリックします。
3. （オプション）**[ネットワークパケットをキャプチャ]** を選択し、設定を構成します。詳細については、"ネットワークパケットのキャプチャ"（755ページ）を参照してください。
4. **[完了]** をクリックします。
5. ZIPアーカイブをダウンロードする準備が完了したら、**[ログをダウンロード]** をクリックして、ローカルに保存します。

VPNゲートウェイログのダウンロード

VPNゲートウェイログを含むアーカイブをダウンロードしてから展開し、トラブルシューティングや監視に利用できます。

VPNゲートウェイログをダウンロードするには

1. **接続**ページで、VPNゲートウェイの横にあるギアアイコンをクリックします。
2. **[ログをダウンロード]** をクリックします。
3. （オプション）**[ネットワークパケットをキャプチャ]** を選択してから、設定を構成します。詳細については、"ネットワークパケットのキャプチャ"（755ページ）を参照してください。
4. **[完了]** をクリックします。
5. ZIPアーカイブをダウンロードする準備が完了したら、**[ログをダウンロード]** をクリックして、ローカルに保存します。

ネットワークパケットのキャプチャ

ローカルの本番サイトとプライマリサーバーまたは復元サーバー間の通信をトラブルシュートおよび分析するには、VPNゲートウェイまたはVPNアプライアンスのネットワークパケットを収集します。

32000個のネットワークパケットが収集されるか、制限時間に到達すると、ネットワークパケットのキャプチャが停止し、結果が.libpcapファイルに書き込まれ、「logs」という名前のZIPアーカイブに追加されます。

構成可能な**ネットワークパケットのキャプチャ**設定の詳細を次の表に示します。

設定	説明
ネットワークインターフェース名	ネットワークパケットをキャプチャするネットワークインターフェース。すべてのネットワークインターフェースでネットワークパケットをキャプチャするには、**[すべて]** を選択します。

設定	説明
時間制限（秒）	ネットワークパケットキャプチャの時間制限。設定可能な最大値は1800です。
フィルタ処理	キャプチャ済みのネットワークパケットに適用される追加フィルタ。 プロトコル、ポート、方向、およびそれらの組み合わせを含む文字列を、スペースで区切って入力できます。例えば、「and」、「or」、「not」、「(」、「)」、「src」、「dst」、「net」、「host」、「port」、「ip」、「tcp」、「udp」、「icmp」、「arp」、「esp」などの文字列を使用できます。 括弧を使用する場合は、前後にスペースを挿入してください。また、IPアドレスやネットワークアドレスを入力することもできます（例:「icmp or arp」、「port 67 or 68」。）。 入力できる値の詳細については、Linuxのtcpdumpコマンドのヘルプを参照してください。

IPsec VPN設定のトラブルシューティング

注意
この機能を利用できるかどうかは、現在のアカウントで有効になっているサービスクォータによって異なります。

IPsec VPN接続の設定時または使用時に、問題が発生することがあります。

発生した問題についてはIPsecログファイルで詳細を確認できます。また、IPsec VPN設定の問題箇所のトラブルシューティングを行い、発生する可能性がある一般的な問題に対するソリューションをチェックすることが可能です。

IPsec VPN設定の問題のトラブルシューティング

注意
この機能を利用できるかどうかは、現在のアカウントで有効になっているサービスクォータによって異なります。

次の表では、 IPsec VPN設定について比較的よく起こる問題と、そのトラブルシュートの方法について説明します。

問題	考えられるソリューション
表示されるエラー:**IKEフェーズ1のネゴシエーションエラー。クラウド側とローカル側のIPsec IKEの設定を確認してください。**	**[再試行]** をクリックし、より具体的なエラーメッセージが表示されないか確認します。例えば、より具体的なエラーメッセージとしては、アルゴリズムの不一致や不正な事前共有鍵に関するエラーメッセージが挙げられます。

問題	考えられるソリューション
	注意 セキュリティ上の理由から、IPsec VPN接続には次のような制限事項が適用されます。 • IKEv1はRFC8247で非推奨とされています。これはセキュリティ上のリスクのためサポートされていません。IKEv2プロトコル接続のみがサポートされています。 • 次の暗号化アルゴリズムは安全ではないとみなされており、サポートされていません。DESおよび3DES。 • 次のハッシュアルゴリズムは安全ではないとみなされており、サポートされていません。SHA1およびMD5。 • ディフィーヘルマン群数2は安全ではないとみなされており、サポートされていません。
ローカルサイトとクラウドサイト間の接続ステータスが **[接続しています]** のままになる。	次の項目を確認します。 • UDPポート500が開いているか（ファイアウォールを使用する場合）。 • ローカルサイトとクラウドサイト間の接続。 • ローカルサイトのIPアドレスが正しいか。
ローカルサイトとクラウドサイト間の接続ステータスが **[接続を待機中]** のままになる。	クラウドサイトの **[起動アクション]** が **[追加]** に設定されている場合にこのステータスが表示されます。これは、クラウドサイトがローカルサイトからの接続が開始されるまで待機していることを意味します。 ローカルサイトから接続を開始します。
ローカルサイトとクラウドサイト間の接続ステータスが **[トラフィックを待機中]** のままになる。	クラウドサイトの **[起動アクション]** が **[ルート]** に設定されている場合にこのステータスが表示されます。 ローカルサイトからの接続が見込まれる場合は、次の内容を実施します。 • ローカルサイトからクラウドサイトの仮想マシンに対してpingを試行します。これは、Cisco ASAなどのデバイスでトンネルを確立するために必要な標準動作です。（ルートモード） • ローカルサイトの **[起動アクション]** を **[開始]** に設定して、ローカルサイトでトンネルが確立されたか確認します。
ローカルサイトとクラウドサイト間の接続	この問題は、以下が原因である可能性があります。

問題	考えられるソリューション
が確立されたが、1つ以上のネットワークポリシーのダウンが表示される。	• クラウドIPsecサイトのネットワークマッピングがローカルサイトのネットワーキングと異なっている。 ローカルサイトとクラウドサイトのネットワークマッピングとネットワークポリシーの順序が正確に一致しているか確認します。 • ローカルサイトとクラウドサイト、またはそれらのいずれかの **[起動アクション]** が **[ルート]** に設定されている場合（例えばCisco ASAデバイス上）、このステータスに問題はなく、その時点ではトラフィックが発生していません。pingを試行して、トンネルが確立されていることを確認できます。pingが動作しない場合は、ローカルサイトとクラウドサイトのネットワークマッピングをチェックします。
特定のIPsec接続を再起動する。	特定のIPsec接続を再起動するには: 1. **[ディザスタリカバリ]** > **[接続]** 画面で、IPsec接続をクリックします。 2. **[接続を無効化]** をクリックします。 3. IPsec接続を再度クリックします。 4. **[接続を有効化]** をクリックします。

IPsec VPNログファイルのダウンロード

注意
この機能を利用できるかどうかは、現在のアカウントで有効になっているサービスクォータによって異なります。

IPsec接続に関するその他の情報は、VPNサーバーのログファイルで確認できます。ログファイルは.ZIPアーカイブで圧縮されており、ダウンロードして展開可能です。

前提条件

マルチサイトIPsec VPN接続が設定されている。

ログファイルの.ZIPアーカイブをダウンロードするには

1. Cyber Protectコンソールで、**[ディザスタリカバリ]** > **[接続]** の順に移動します。
2. クラウドサイトのVPNゲートウェイの横にあるギアアイコンをクリックします。
3. **[ログをダウンロードする]** をクリックします。
4. **[完了]** をクリックします。
5. ZIPアーカイブをダウンロードする準備が完了したら、**[ログをダウンロード]** をクリックして、ローカルに保存します。

マルチサイトIPsec VPNログファイル

注意
この機能を利用できるかどうかは、現在のアカウントで有効になっているサービスクォータによって異なります。

ZIPアーカイブの一部であるIPsec VPNログファイルと、そこに含まれる情報を次のリストに示します。

- `ip.txt`:このファイルにはネットワークインターフェースの構成ログが含まれます。パブリックIPアドレスとローカルIPアドレスの2つのIPアドレスが確認できるはずです。このログにこれらのIPアドレスが記載されていない場合は、何らかの問題があります。サポートチームにお問い合わせください。

  注意
  パブリックIPアドレスのマスクは32である必要があります。

- `swanctl-list-loaded-config.txt`: このファイルにはすべてのIPsecサイトに関する情報が含まれます。
  ファイルにサイトの情報がない場合は、IPsec構成が適用されていません。構成のアップデートを試して保存するか、サポートチームに問い合わせてください。
- `swanctl-list-active-sas.txt`: このファイルには、ステータスがアクティブか接続中の接続とポリシーが含まれます。

復元サーバー設定

このセクションでは、フェールオーバーとフェールバックの概念、復元サーバーの作成、およびディザスタリカバリ操作について説明します。

復元サーバーの作成

ワークロードのコピーとなる復元サーバーを作成するには、以下の手順を実行します。また、その手順を扱ったビデオチュートリアルを参照することもできます。

重要
フェールオーバーを実行する際は、復元サーバーの作成後に作成された復元ポイントのみを選択できます。

前提条件

- 保護する元のマシンに保護計画を適用する必要があります。この計画では、マシン全体、または起動と必須のサービスの提供に必要なディスクのみをクラウドストレージにバックアップする必要があります。
- クラウドサイトへの接続タイプの1つを設定する必要があります。

リカバリサーバーの作成

1. **[すべてのデバイス]** タブで、保護するマシンを選択します。
2. **[ディザスタリカバリ]** をクリックし、**[リカバリサーバーを作成]** をクリックします。
3. 仮想コアの数と RAM のサイズを選択します。

注意
すべてのオプションの計算ポイントを確認できます。コンピュートポイントの数は、リカバリサーバーを 1 時間当たり実行するコストを反映しています。詳細については、"コンピュートポイント"（718ページ）を参照してください。

4. サーバーが接続されるクラウドネットワークを指定します。
5. **[DHCP]** オプションを選択します。

DHCPオプション	説明
クラウドサイトにより提供	デフォルトの設定。サーバーのIPアドレスは、クラウド上に自動設定されたDHCPサーバーにより提供されます。
カスタム	サーバーのIPアドレスは、クラウド上で現在動作しているDHCPサーバーにより提供されます。

6. （オプション） **MACアドレス**を指定します。
MACアドレスは、サーバーのネットワークアダプタに割り当てられる一意の識別子です。カスタムのDHCPを使用する場合、特定のMACアドレスに対して、常に特定のIPアドレスが割り当てられるように設定できます。これにより、復元サーバーが常に同じIPアドレスを取得できるようになります。MACアドレスで登録されたライセンスを有するアプリケーションを実行することができます。
7. 本番ネットワークでサーバーが持つ IP アドレスを指定します。デフォルトでは、元のマシンの IP アドレスが設定されています。

注意
DHCPサーバーを使用する場合は、IPアドレスの競合を回避するために、このIPアドレスをサーバーの除外一覧に追加します。
カスタムのDHCPサーバーを使用する場合、**稼働中のネットワークのIPアドレス**には、DHCPサーバーの設定と同一のIPアドレスを指定する必要があります。そうしない場合、テストフェールオーバーが正しく動作せず、パブリックIPアドレス経由でサーバーに到達できなくなります。

8. （オプション）**[テストIPアドレス]** チェックボックスをオンにして、IP アドレスを指定します。
これにより、隔離されたテストネットワーク内でフェールオーバーをテストする機能、およびテストフェールオーバー中にRDPまたはSSH経由で復元サーバーに接続する機能が提供されます。テストフェールオーバーモードでは、VPNゲートウェイが、NATプロトコルを使用してテストIPアドレスを本番IPアドレスに置き換えます。
チェックボックスをオフのままにすると、コンソールがテストフェールオーバー中にサーバーにアクセスする唯一の方法になります。

注意
DHCPサーバーを使用する場合は、IPアドレスの競合を回避するために、このIPアドレスをサーバーの除外一覧に追加します。

提案された IP アドレスのいずれかを選択するか、別の IP アドレスを入力することができます。

9. （オプション）[**インターネットアクセスの許可**] チェックボックスをオンにします。
これにより、リカバリサーバーは、実際のフェールオーバーまたはテストフェールオーバー中にインターネットにアクセスできます。デフォルトでは、TCPポート25番はパブリックIPアドレスへの送信接続用に開いています。
10. （オプション）**RPOしきい値**を設定します。
RPOしきい値は、フェールオーバーのための最後の適切な復元ポイントと現在時刻との間の許容される最大時間間隔を定義します。数値は15～60分、1～24時間、1～14日間の範囲で設定できます。
11. （オプション）[**パブリックIPアドレスを使用する**] チェックボックスをオンにします。
パブリック IP アドレスを使用すると、フェールオーバーまたはテストフェールオーバー中にインターネットからリカバリサーバーを使用できるようになります。チェックボックスをオフのままにすると、サーバーは本番ネットワークでのみ使用可能になります。
パブリックIPアドレスを使用するオプションでは、**インターネットアクセス**オプションを有効にする必要があります。
パブリック IP アドレスは、設定が完了した後に表示されます。デフォルトでは、TCPポート443番はパブリックIPアドレスへの受信接続用に開いています。

注意
[**パブリックIPアドレスを使用する**] チェックボックスをオフにするか、復元サーバーを削除すると、そのパブリックIPアドレスは予約されません。

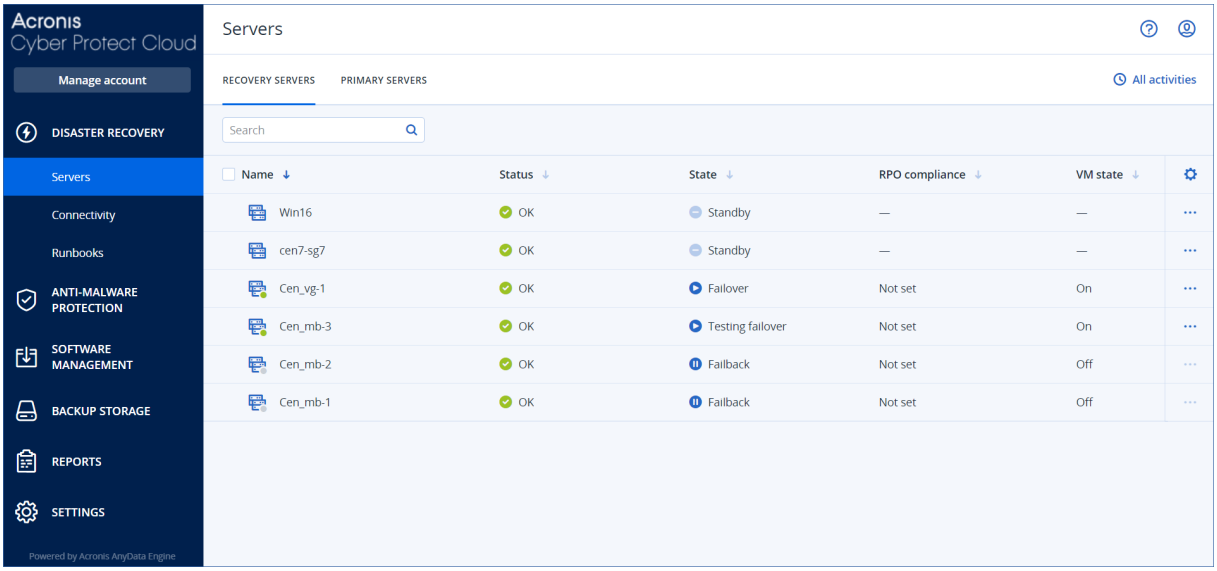
12. （オプション）（選択したマシンのバックアップがマシンプロパティとしての暗号化を使用して暗号化されている場合）暗号化されたバックアップから復元サーバー用の仮想マシンを作成する際に自動的に使用されるパスワードを指定します。
    a. [**指定**] をクリックし、暗号化バックアップのパスワードを入力し、資格情報の名前を定義します。
    デフォルトでは、リスト内の最新のバックアップが表示されます。
    b. （オプション） すべてのバックアップを表示するには、**すべてのバックアップを表示**を選択します。
    c. [**完了**] をクリックします。

注意
指定したパスワードは安全な資格情報ストアに保存されますが、パスワードを保管する行為がコンプライアンス規定に抵触する場合があります。

13. （オプション）リカバリサーバー名を変更します。
14. （オプション）リカバリサーバーの説明を入力します。

15. （オプション）**[クラウドファイアウォールのルール]** タブをクリックして、デフォルトのファイアウォールルールを編集します。詳細については、"クラウドサーバーのファイアウォールルール設定"（786ページ）を参照してください。
16. **[作成]** をクリックします。

復元サーバーは、Cyber Protectコンソールの **[ディザスタリカバリ]** > **[サーバー]** > **[復元サーバー]** タブに表示されます。元のマシンを選択して **[ディザスタリカバリ]** をクリックしてその設定を表示することができます。



フェールオーバーが動作する仕組み

本番フェールオーバー

注意
この機能を利用できるかどうかは、現在のアカウントで有効になっているサービスクォータによって異なります。

復元サーバーが作成されると、**スタンバイ**状態が維持されます。フェールオーバーが開始するまで、対応する仮想マシンは存在しない状態になります。フェールオーバープロセスを開始する前に、元のマシンの少なくとも1つのディスクイメージバックアップ（ブータブルボリュームを含む）を作成する必要があります。

フェールオーバープロセスを開始した際、定義済みパラメータを有する仮想マシンの作成元である元のマシンの復元ポイント（バックアップ）を選択します。フェールオーバー操作では、「バックアップからVMを実行する」機能を使用します。復元サーバーはトランジション状態の**確定**を取得します。このプロセスは、サーバーの仮想ディスクをバックアップストレージ（「コールド」ストレージ）からディザスタリカバリストレージ（「ホット」ストレージ）に転送することを意味します。

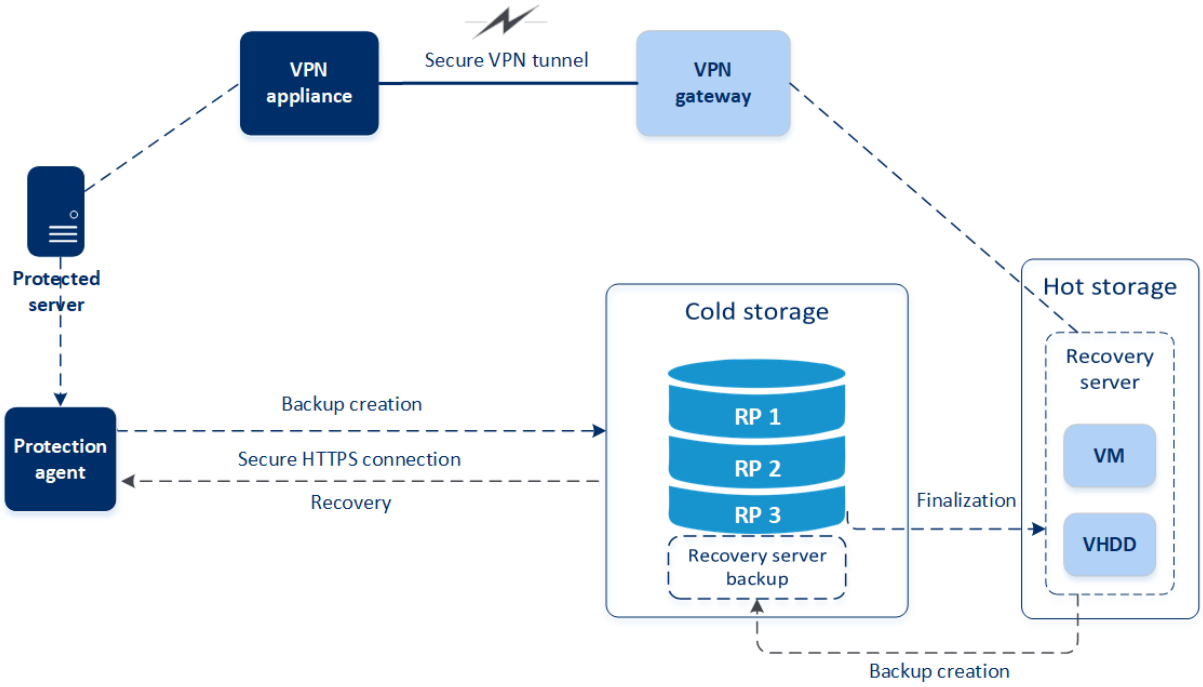
注意

確定処理中は、パフォーマンスが通常より低くなりますが、サーバーはアクセスおよび操作可能です。サーバーコンソールを開くには、**コンソールの準備ができました**のリンクをクリックします。このリンクは、[**ディザスタリカバリ**] > [**サーバー**] 画面の [**VMステータス**] 列、およびサーバーの**詳細**ビューから利用可能です。

確定が完了すると、サーバーのパフォーマンスは通常の値に到達し、サーバーのステータスが、**フェールオーバー**に変わります。これで、ワークロードが元のマシンからクラウドサイトの復元サーバーに切り替わりました。

リカバリサーバーの内部に保護エージェントがある場合は、干渉（バックアップを開始したり古い状態をバックアップコンポーネントに報告したりする処理）を回避するために、エージェントサービスが停止します。

下の図では、フェールオーバーおよびフェールバック処理の両方について見ることができます。



テストフェールオーバー

テストフェールオーバー中、仮想マシンは最終化されません。これは、エージェントがバックアップから直接仮想ディスクのコンテンツを読み取る、つまり、バックアップのさまざまな部分へのランダムアクセスを実行するという意味です。これにより、パフォーマンスが通常の場合より低下する可能性があります。テストフェールオーバープロセスの詳細については、"テストフェールオーバーの実行"（764 ページ）を参照してください。

自動テストフェールオーバー

自動テストフェールオーバーを構成すると、手動によるインタラクションなしにフェールオーバーが毎月実行されるようになります。詳細については、「"自動テストフェールオーバー"（766ページ）」と「"自動テストフェールオーバーの構成"（766ページ）」を参照してください。

テストフェールオーバーの実行

フェールオーバーのテストを実行することは、稼働中のネットワークから隔離されたテスト用VLAN内の復元サーバーを起動することを意味します。複数の復元サーバーを一度にテストして、インタラクションを確認できます。テストネットワークでは、サーバーは本番IPアドレスを使用して通信しますが、ローカルネットワーク内のワークロードへのTCPまたはUDP接続は開始できません。

テストフェールオーバー中、仮想マシン（復元サーバー）は最終化されません。エージェントでは、仮想ディスクの内容がバックアップから直接読み込まれ、バックアップの個別のパートにランダムアクセスされます。このため、ステータスがテストフェールオーバーになっている復元サーバーのパフォーマンスは、通常時のパフォーマンスと比べて低速になる場合があります。

フェールオーバーのテストの実行はオプションですが、コストと安全性の面で適切な頻度で定期的に実行することをお勧めします。クラウドの本番環境をスピンアップする方法を説明する一連の手順であるランブックを作成することをお勧めします。

重要

デバイスを災害から保護するために、事前に復元サーバーを作成する必要があります。

デバイスの復元サーバーが作成された後に作成された復元ポイントからのみ、フェールオーバーを実行できます。

復元サーバーへのフェールオーバーを実行する前に、少なくとも1つの復元ポイントを作成する必要があります。サポートされる復元ポイントの最大数は100件です。

テストフェールオーバーの実行

1. 元のマシンを選択するか、テストするリカバリサーバーを選択します。
2. [**ディザスタリカバリ**] をクリックします。
   リカバリサーバーの説明が開きます。
3. [**フェールオーバー**] をクリックします。
4. フェールオーバーの種類、[**テストフェールオーバー**] を選択します。
5. 復元ポイント（バックアップ）を選択して、[**開始**] をクリックします。
6. 選択したバックアップがマシンのプロパティとしての暗号化により暗号化されている場合:

a. バックアップセットの暗号化パスワードを入力します。

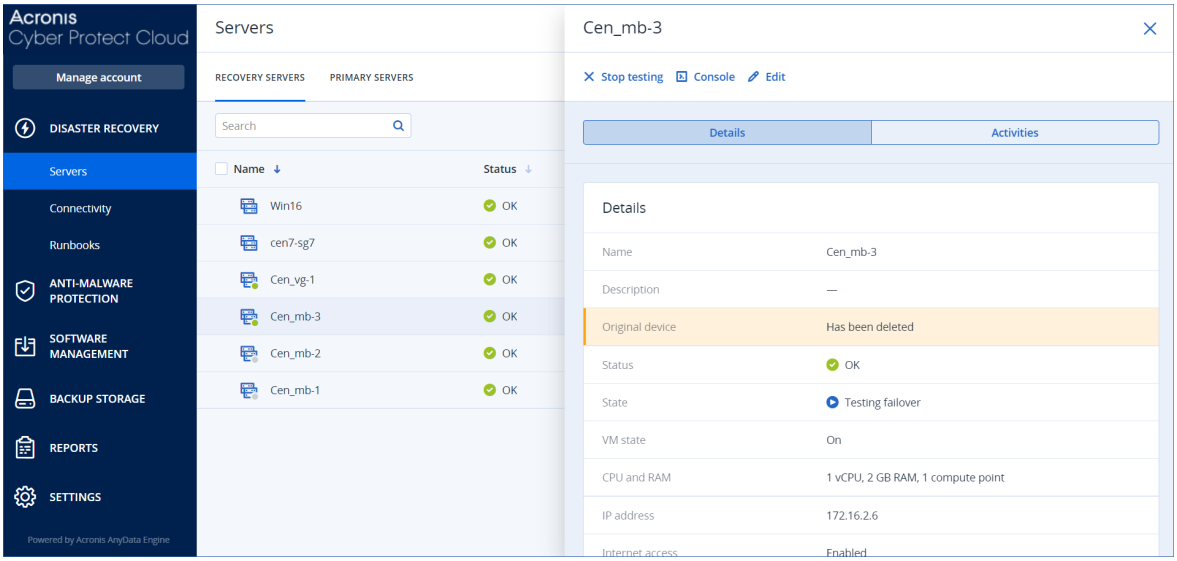
> **注意**
> パスワードは一時的に保存され、現在のテストフェールオーバー処理にのみ使用されます。パスワードは、テストフェールオーバーが停止または完了すると、資格情報ストアから自動的に削除されます。

b. （オプション） バックアップセットのパスワードを保存し、以降のフェールオーバー処理で使用するには、**[セキュアな資格情報ストアにパスワードを保存...]** チェックボックスを選択し、**資格情報名**フィールドに資格情報の名前を入力します。

> **重要**
> パスワードはセキュアな資格情報ストアに保存され、以降のフェールオーバー処理で自動的に適用されます。ただしパスワードを保管する行為が、コンプライアンス規定に抵触する場合があります。ご注意ください。

c. **[完了]** をクリックします。

リカバリサーバーが起動すると、状態は **[フェールオーバーテスト中]** に変わります。



7. 次のいずれかの方法を使用して、リカバリサーバーをテストします。
   - **[ディザスタリカバリ]** > **[サーバー]** でリカバリサーバーを選択して、**[コンソール]** をクリックします。
   - RD PまたはSSH、およびリカバリサーバーの作成時に指定したテストIPアドレスを使用して、リカバリサーバーに接続します。本番ネットワークの内部と外部の両方から接続を試してください（「ポイントツーサイト接続」に記載されています）。
   - リカバリサーバー内でスクリプトを実行します。
     スクリプトは、ログイン画面、アプリケーションの起動の有無、インターネット接続、および復元サーバーに接続する他のマシンの機能を確認できます。
   - 復元サーバーがインターネットとパブリックIPアドレスにアクセスできる場合は、TeamViewerを使用することができます。

8. テストが完了したら、[**テストの停止**] をクリックします。
   リカバリサーバーが停止します。テストフェールオーバー中に復元サーバーに加えられたすべての変更点は保存されません。

注意
ランブックの場合でも、手動でテストフェールオーバーを開始する場合でも、**サーバーを起動**および**サーバーを停止**アクションが、テストフェールオーバーの操作に適用されることはありません。これらのアクションを実行しようとすると、次のエラーメッセージが表示されて失敗します。
失敗:この操作は、現在のサーバーの状態には適用できません。

自動テストフェールオーバー

自動テストフェールオーバーでは、月に一度、自動的に復元サーバーのテストが行われます。手動のインタラクションは必要ありません。

自動テストフェールオーバーの処理は、以下のパートで構成されています。

1. 最新の復元ポイントから仮想マシンを作成する
2. 仮想マシンのスクリーンショットを取得する
3. 仮想マシンのオペレーティングシステムが正常に起動されたかどうかを分析する
4. テストフェールオーバーステータスに関して通知する

注意
自動テストフェールオーバーにより、コンピュートポイントが消費されます。

復元サーバーの設定で、自動テストフェールオーバーを設定できます。詳細については、"自動テストフェールオーバーの構成"（766ページ）を参照してください。

ごくまれに、自動テストのフェールオーバーがスキップされたり、スケジュールされた時刻に実行できなかったりする場合があります。ご注意ください。これは、本番環境でのフェールオーバーの優先度が自動テストでのフェールオーバーよりも高いため、自動テストでのフェールオーバーに割り当てられたハードウェアリソース（CPUとRAM）が一時的に制限されて、本番環境でのフェールオーバーを同時に行うためのリソースの確保が優先される可能性があるためです。

何らかの理由で自動テストのフェールオーバーがスキップされた場合、アラートが生成されます。

注意
オリジナルのマシンのバックアップがマシンプロパティとしての暗号化を使用して暗号化され、復元サーバーを作成する際に暗号化パスワードが指定されていない場合、自動テストフェールオーバーは失敗します。暗号化パスワードの指定の詳細については、"復元サーバーの作成"（759ページ）を参照してください。

自動テストフェールオーバーの構成

自動テストフェールオーバーを構成することで、手動で操作を行うことなく、毎月復元サーバーのテストを実行できます。

自動テストフェールオーバーを構成するには

1. コンソールで **[ディザスタリカバリ]** > **[サーバー]** > **[復元サーバー]** に移動し、復元サーバーを選択します。
2. **[編集]** をクリックします。
3. **[自動テストフェールオーバー]** セクションの **[スケジュール]** フィールドで、**[月単位]** を選択します。
4. （オプション）**[スクリーンショットのタイムアウト]** で、自動テストフェールオーバーの実行をシステムが試行する最大時間（分単位）のデフォルト値を変更します。
5. （オプション）**[スクリーンショットのタイムアウト]**の値をデフォルト値として保存し、他の復元サーバーの自動テストフェールオーバーを有効にするときの自動入力の値として使用するには、**[デフォルトタイムアウトとして設定]** を選択します。
6. **[保存]** をクリックします。

自動テストフェールオーバーのステータスを表示

自動テストフェールオーバーが完了すると、ステータス、開始時間、終了時間、期間、仮想マシンのスクリーンショットなどの詳細を表示できます。

復元サーバーの自動テストフェールオーバーステータスを表示するには

1. コンソールで **[ディザスタリカバリ]** > **[サーバー]** > **[復元サーバー]** に移動し、復元サーバーを選択します。
2. **[自動テストフェールオーバー]** セクションで、前回の自動テストフェールオーバーの詳細を確認します。
3. （オプション）**[スクリーンショットを表示]** をクリックすると、仮想マシンのスクリーンショットが表示されます。

自動テストフェールオーバーの無効化

リソースを節約したい場合や、特定の復元サーバーに対して自動テストフェールオーバーを実行する必要がない場合は、自動テストフェールオーバーを無効にすることができます。

自動テストフェールオーバーを無効化するには

1. コンソールで **[ディザスタリカバリ]** > **[サーバー]** > **[復元サーバー]** に移動し、復元サーバーを選択します。
2. **[編集]** をクリックします。
3. **[自動テストフェールオーバー]** セクションで、**[スケジュール]** フィールドで、**[なし]** を選択します。
4. **[保存]** をクリックします。

フェールオーバーの実行

注意
この機能を利用できるかどうかは、現在のアカウントで有効になっているサービスクォータによって異なります。

フェールオーバーとは、構内からクラウドへワークロードを移動するプロセスおよびワークロードがクラウドに残っているときの状態です。

フェールオーバーを開始すると、復元サーバーが稼働中のネットワークで起動します。干渉や不要な問題が発生するのを回避するため、元のワークロードがオンラインでないこと、またVPN経由でアクセスできないことを確認してください。

同じクラウドアーカイブへのバックアップの干渉を避けるには、現在**フェールオーバー**ステータスになっているワークロードから保護計画を手動で取り消します。計画の取り消しの詳細については、「保護計画の取り消し」を参照してください。

重要
デバイスを災害から保護するために、事前に復元サーバーを作成する必要があります。

デバイスの復元サーバーが作成された後に作成された復元ポイントからのみ、フェールオーバーを実行できます。

復元サーバーへのフェールオーバーを実行する前に、少なくとも1つの復元ポイントを作成する必要があります。サポートされる復元ポイントの最大数は100件です。

以下の操作を実行するか、ビデオチュートリアルを視聴できます。

フェールオーバーの実行

1. 元のマシンがネットワーク上で使用できないことを確認します。
2. Cyber Protectコンソールで **[ディザスタリカバリ]** > **[サーバー]** > **[復元サーバー]** に移動し、復元サーバーを選択します。
3. **[フェールオーバー]** をクリックします。
4. フェールオーバーの種類、**本番フェールオーバー**を選択します。
5. 復元ポイント（バックアップ）を選択して、**[開始]** をクリックします。
6. （選択したバックアップがマシンのプロパティとしての暗号化により暗号化されている場合）
   a. バックアップセットの暗号化パスワードを入力します。

      注意
      パスワードは一時的に保存され、現在のフェールオーバー処理にのみ使用されます。フェールオーバー処理が完了し、サーバーが**スタンバイ**状態に戻ると、パスワードは資格情報ストアから自動的に削除されます。

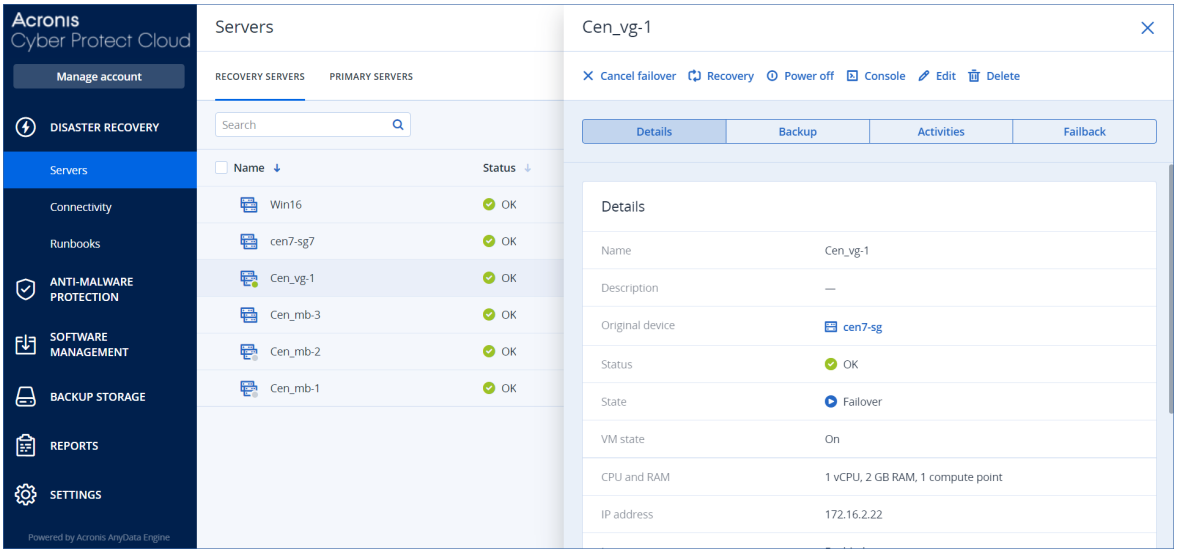
   b. （オプション） バックアップセットのパスワードを保存し、以降のフェールオーバー処理で使用するには、**[セキュアな資格情報ストアにパスワードを保存...]** チェックボックスを選択し、**資格情報名**フィールドに資格情報の名前を入力します。

      重要
      パスワードはセキュアな資格情報ストアに保存され、以降のフェールオーバー処理で自動的に適用されます。ただしパスワードを保管する行為が、コンプライアンス規定に抵触する場合があり

ます。ご注意ください。

c. **[完了]** をクリックします。
リカバリサーバーが起動すると、状態は **[確定]** に変わり、しばらくしてから **[フェールオーバー]** になります。

重要
サーバーは、**確定**および**フェールオーバー**のいずれのステータスでも利用できることを理解しておく必要があります。**確定**ステータスの間に、サーバーコンソールを開くには、**コンソールの準備ができました**のリンクをクリックします。このリンクは、**[ディザスタリカバリ]** > **[サーバー]** 画面の **[VMステータス]** 列、およびサーバーの**詳細**ビューから利用可能です。詳細については、"フェールオーバーが動作する仕組み"（762ページ）を参照してください。



7. コンソールを表示して、リカバリサーバーが起動していることを確認します。**[ディザスタリカバリ]** > **[サーバー]** をクリックし、リカバリサーバーを選択して、**[コンソール]** をクリックします。
8. 復元サーバーの作成時に指定した本番IPアドレスを使用して、復元サーバーにアクセスできることを確認します。

リカバリサーバーが確定されると、新しい保護計画が自動的に作成され、適用されます。この保護計画は、リカバリサーバーの作成に使用された保護計画に基づいており、一定の制限があります。この計画では、スケジュールと保存ルールのみを変更できます。詳細については、「クラウドサーバーのバックアップ」を参照してください。

フェールオーバーをキャンセルする場合は復元サーバーを選択して **[フェールオーバーをキャンセル]** をクリックします。復元サーバーのバックアップを除き、フェールオーバー時点以降のすべての変更は失われます。リカバリサーバーは、**スタンバイ**状態に戻ります。

フェールバックを実行する場合、復元サーバーを選択して、**[フェールバック]** をクリックします。

ローカルDNSを使用してサーバーのフェールオーバーを実行する方法

ローカルサイトでDNSサーバーを使用してマシン名を解決する場合、フェールオーバー後、DNSに依存しているマシンに対応する復元サーバーは、クラウドで使用されているDNSサーバーが異なるため、通信に失敗します。デフォルトでは、クラウドサイトのDNSサーバーが、新しく作成されたクラウドサーバーに使用されます。カスタムDNS設定を適用する必要がある場合は、サポートチームに連絡してください。

DHCPサーバーのフェールオーバーを実行する方法

ローカルインフラストラクチャでは、WindowsまたはLinuxホストにDHCPサーバーが配置されている場合があります。そのようなホストがクラウドサイトにフェールオーバーされると、DHCPサーバーの複製の問題が生じます。これはクラウド内のVPNゲートウェイもDHCPの役割を果たしているためです。この問題を解決するには、次のいずれかを実行します。

- 残りのローカルサーバーがまだローカルサイトにある間にDHCPホストだけがクラウドにフェールオーバーされた場合、クラウド内のDHCPホストにログインして、その上にあるDHCPサーバーをオフにする必要があります。したがって、競合は発生せずに、VPNゲートウェイのみがDHCPサーバーとして機能します。
- クラウドサーバーがDHCPホストからすでにIPアドレスを取得している場合、クラウド内のDHCPホストにログインして、その上にあるDHCPサーバーをオフにする必要があります。さらに、正しいDHCPサーバー（VPNゲートウェイでホストされている）から割り当てられた新しいIPアドレスを割り当てるため、クラウドサーバーにログインし、DHCPリースを更新する必要があります。

注意
クラウドDHCPサーバーが **[カスタムDHCP]** オプションで構成されており、復元サーバーまたはプライマリサーバーのいずれかが、このDHCPサーバーからIPアドレスを取得している場合、この手順を使用することはできません。

フェールバックの動作について

注意
この機能を利用できるかどうかは、現在のアカウントで有効になっているサービスクォータによって異なります。

フェールバックは、クラウドからローカルサイトの物理マシンまたは仮想マシンにワークロードを戻すプロセスです。**フェールオーバー**状態の復元サーバーでフェールバックを実行できます。またローカルサイトのサーバーを引き続き使用できます。

ローカルサイトの仮想または物理ターゲットマシンに対する自動フェールオーバーを実行できます。フェールバック中に、クラウド内の仮想マシンを引き続き実行しながら、バックアップデータをローカルサイトに転送できます。このテクノロジーにより、ダウンタイムを大幅に短縮できます。また予測される概算のダウンタイムがCyber Protectコンソールに表示されます。この情報を確認および使用してアクティビティを計画し、今後のダウンタイムに関して、必要に応じてクライアントに注意を喚起できます。

ターゲット仮想マシンとターゲット物理マシンに対するフェールバックプロセスは若干異なります。フェールバックプロセスのフェーズの詳細については、「"ターゲット仮想マシンへのフェールバック"（771ページ）」および「"ターゲット物理マシンへのフェールバック"（776ページ）」を参照してください。

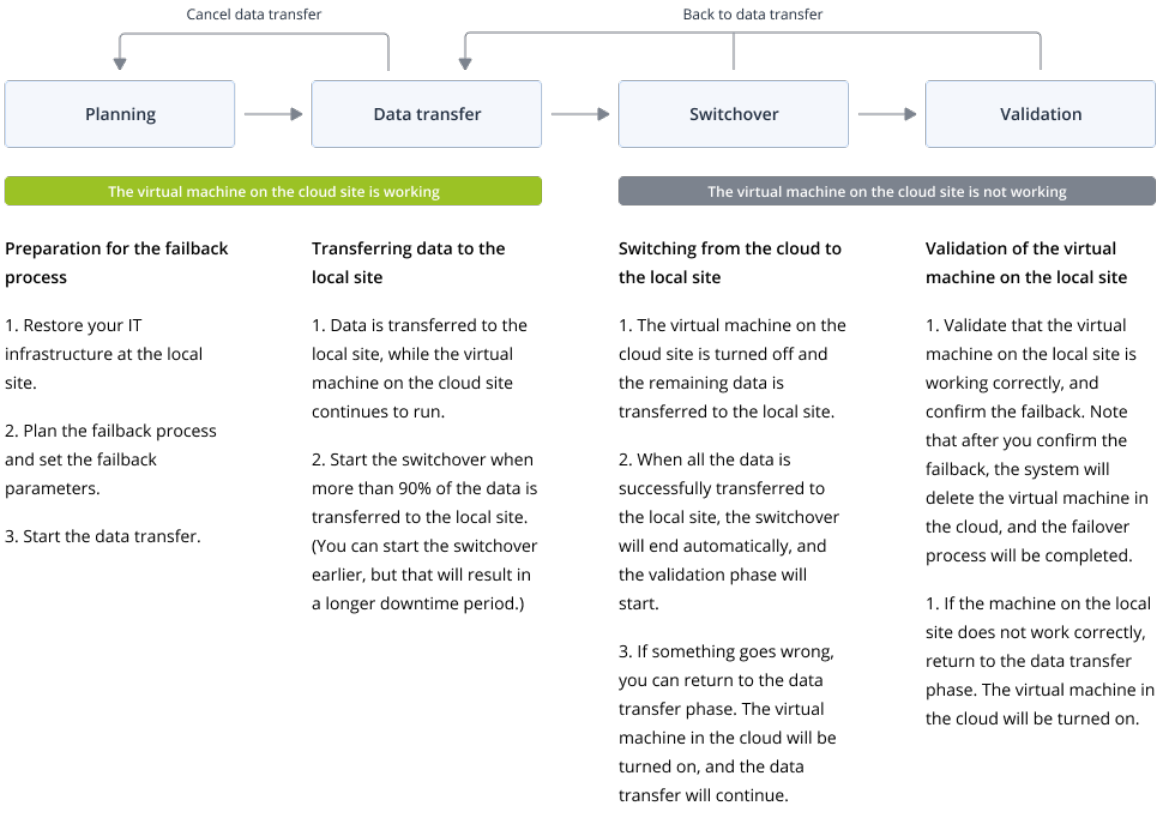
自動化されたフェールバック手順を使用できない特定のケースでは、手動でフェールバックを実行できます。詳細については、"手動フェールバック"（779ページ）を参照してください。

注意
ランブックの処理では、手動モードのフェールバックのみがサポートされます。これは、**フェールバックサーバー**手順を含むランブックを実行してフェールバックプロセスを開始した場合、その手順で手動によるインタラクションが必要となることを意味しています。つまり、マシンを手動でリカバリし、**[ディザスタリカバリ]** > **[サーバー]** タブからフェールバックプロセスを確認またはキャンセルする必要があります。

ターゲット仮想マシンへのフェールバック

注意
この機能を利用できるかどうかは、現在のアカウントで有効になっているサービスクォータによって異なります。

ターゲット仮想マシンのフェールバックプロセスは次の4つのフェーズで構成されます。



1. **計画**:このフェーズでは、ホストやネットワーク構成などのローカルサイトのITインフラストラクチャを復元し、フェールバックパラメータを構成します。また、データ転送を開始するタイミングの計画を策定します。

   注意
   フェールバックプロセスの合計時間を最小限に抑えるために、ローカルサーバーをセットアップした直後にデータ転送フェーズを実行し、データ転送の間に、ネットワークと残りのローカルインフラストラクチャの構成を続行します。

2. **データ転送**:このフェーズでは、クラウド内の仮想マシンが引き続き実行されている間に、クラウドサイトからローカルサイトにデータが転送されます。データ転送の間は、任意のタイミングで次のフェーズであるスイッチオーバーを開始できます。ただし、次の関連要素を考慮する必要があります。

   データ転送フェーズの所要時間が長くなる
   - クラウドにおける仮想マシンの実行時間が長くなる。
   - 比較的多くのデータがローカルサイトに転送される
   - コストが高くなる（より多くのコンピュートポイントを消費する）
   - スイッチオーバーフェーズの間に発生するダウンタイムが短くなる。

   ダウンタイムを最小限に抑えたい場合は、データの90%以上がローカルサイトに転送された後にスイッチオーバーフェーズを開始します。

   より長いダウンタイムを許容する余裕があり、クラウドで仮想マシンを実行するために余分な計算ポイントを消費したくない場合は、より早いタイミングでスイッチオーバーフェーズを開始できます。

   データ転送フェーズ中にフェールバックプロセスをキャンセルした場合、転送されたデータはローカルサイトから削除されません。問題の発生をできるだけ回避するには、新しいフェールバックプロセスを開始する前に、転送されたデータを手動で削除します。以下のデータ転送プロセスは最初から開始されます。

3. **スイッチオーバー**:このフェーズでは、クラウド内の仮想マシンがオフになり、最新のバックアップ増分を含む残りのデータがローカルサイトに転送されます。復元サーバーにバックアップ計画が適用されていない場合、スイッチオーバーフェーズで自動的にバックアップが実行されるため、処理速度が遅くなります。

   このフェーズが終了するまでの推定時間（ダウンタイム期間）は、Cyber Protectコンソールで確認できます。すべてのデータがローカルサイトに転送された時点（データ損失がなく、ローカルサイトの仮想マシンがクラウド内の仮想マシンの正確なコピーになる）で、スイッチオーバーフェーズが完了します。ローカルサイトの仮想マシンがリカバリされ、検証フェーズが自動的に開始されます。

4. **検証**。このフェーズで、ローカルサイトの仮想マシンの準備が整い、自動的に起動しています。仮想マシンが正しく動作しているかどうかを確認できます。
   - すべてが意図したとおりに動作している場合は、フェールバックを確認します。フェールバック後、クラウドの仮想マシンが削除され、復元サーバーが**スタンバイ**状態に戻ります。これでフェールバックプロセスは終了です。
   - 何か問題がある場合は、スイッチオーバーをキャンセルしてデータ転送フェーズに戻ることができます。

仮想マシンへのフェールバックの実行

注意
この機能を利用できるかどうかは、現在のアカウントで有効になっているサービスクォータによって異なります。

現在のローカルサイトのターゲット仮想マシンに対するフェールバックを実行できます。

前提条件

- フェールバックの実行に使用するエージェントはオンラインであり、現在、別のフェールバック操作には使用されていません。
- インターネット接続は安定しています。
- クラウド上に少なくとも1件の仮想マシンの完全バックアップが存在する。

仮想マシンのフェールバックを実行するには

1. Cyber Protectコンソールで、**[ディザスタリカバリ]** > **[サーバー]** の順に移動します。
2. **[フェールオーバー]** 状態のリカバリサーバーを選択します。
3. **[フェールバック]** タブをクリックします。
4. **[フェールバックパラメータ]** セクションで、**ターゲット**として **[仮想マシン]** を選択し、他のパラメータを構成します。
   デフォルトでは、一部の**フェールバックパラメータ**に対して推奨値が自動入力されますが、変更することができます。
   次の表に、**フェールバックパラメータ**の詳細を示します。

パラメータ	説明
バックアップ容量	フェールバック処理中にローカルサイトに転送されるデータの量です。 ターゲット仮想マシンへのフェールバック処理を開始すると、クラウド上の仮想マシンが継続して実行され、新しいデータが生成されるため、データ転送フェーズにおける**バックアップ容量**が大きくなります。 ターゲット仮想マシンへのフェールバック処理に伴うダウンタイムの目安を計算するには、**バックアップ容量**の10%に相当する値を算出（データの90%がローカルサイトに転送された後にスイッチオーバーフェーズを開始することを推奨しているため）して、その値をインターネットの転送速度で除算します。 **注意** 複数のフェールバック処理を同時に行うと、インターネット速度の値が低下します。
ターゲット	クラウドサーバーをリカバリするローカルサイトのワークロードのタイプ:**仮想マシン**または**物理マシン**。
ター	フェールバックロケーション: VMware ESXiホストまたはMicrosoft Hyper-Vホスト。

パラメータ	説明
ゲストマシンロケーション	サイバープロテクションサービスに登録されているエージェントが存在するすべてのホストから選択できます。
エージェント	フェールバック操作を実行するエージェント。 1つのエージェントを使用して、同時に1件のフェールバック操作を実行できます。 オンラインで、現在別のフェールバックプロセスに使用されておらず、フェールバック機能をサポートするバージョンがあり、バックアップにアクセスする権限が付与されているエージェントを選択できます。 VMware ESXiホストに複数のエージェントをインストールし、それぞれを使用して個別のフェールバックプロセスを開始できることに注意してください。これらのフェールバックプロセスは同時に実行できます。
ターゲットマシン設定	仮想マシンの設定: • **仮想プロセッサー**:仮想プロセッサーの数を選択します。 • **メモリ**:仮想マシンに搭載するメモリ容量を選択します。 • **単位**:メモリの単位を選択します。 • （オプション） **ネットワークアダプタ**:ネットワークアダプタを追加するには、**[追加]** をクリックして、**[ネットワーク]** フィールドでネットワークを選択します。 変更の準備ができたら、**[完了]** をクリックします。
パス	（Microsoft Hyper-Vホストの場合）マシンが保存されるホスト上のフォルダ。 ホストにマシン用の十分な空きメモリ容量があることを確認してください。
データストア	（VMware ESXiホストの場合）マシンが保存されるホスト上のデータストア。 ホストにマシン用の十分な空きメモリ容量があることを確認してください。
プロビジョニングモード	仮想ディスクの割り当て方法。 Microsoft Hyper-Vホストの場合: • **容量可変**（デフォルト値） • **固定サイズ** Microsoft Hyper-Vホストの場合: • **シン**（デフォルト値） • **シック**
ターゲットマシン名	ターゲットマシンの名前。デフォルトでは、ターゲットマシンの名前は復元サーバーの名前と同じです。 ターゲットマシン名は、選択した**ターゲットマシンロケーション**において一意である必要があります。

5. **[データ転送を開始]** をクリックして、確認ウィンドウでもう一度 **[開始]** をクリックします。

注意
クラウド上に仮想マシンのバックアップがない場合、システムはデータ転送フェーズの前に自動的にバックアップを実行します。

データ転送フェーズが開始します。コンソールには、次の情報が表示されます。

フィールド	説明
進行状況	このパラメータは、ローカルサイトにすでに転送されているデータの量と、転送する必要のあるデータの合計量を示します。 データの合計量には、データ転送フェーズが開始される前の最後のバックアップからのデータと、データ転送フェーズ中に仮想マシンが引き続き実行されることによって新しく生成される、データのバックアップ（バックアップの増分）が含まれます。このため、**進行状況**パラメータの2種類の値は時間とともに増加します。
ダウンタイムの推定	このパラメータは、スイッチオーバーフェーズを開始する場合、クラウドの仮想マシンが使用できなくなる期間を示します。この値は、**進行状況**パラメータの値に基づいて計算され、時間とともに減少します。

6. [**スイッチオーバー**] をクリックして、確認ウィンドウでもう一度 [**スイッチオーバー**] をクリックします。
   スイッチオーバーフェーズが開始します。コンソールには、次の情報が表示されます。

フィールド	説明
進行状況	このパラメータは、マシンのローカルサイトに対する復元の進行状況を示します。
完了までの推定所要時間	このパラメータは、スイッチオーバーフェーズが完了し、ローカルサイトでマシンを起動できるようになるまでの、おおよその時間を示します。

注意
クラウド上の仮想マシンにバックアップ計画が適用されていない場合、スイッチオーバーフェーズで自動的にバックアップが実行されるため、ダウンタイムが長くなります。

7. **スイッチオーバー**フェーズが完了し、ローカルサイトの仮想マシンが自動的に起動したら、正しく動作していることを検証します。
8. [**フェールバックの確認**] をクリックし、確認ウィンドウでもう一度 [**確認**] をクリックして、プロセスを最終化します。
   クラウドの仮想マシンが削除され、復元サーバーが**スタンバイ**状態に戻ります。

注意

フェールバック処理で、リカバリされたサーバーに保護計画が適用されることはありません。フェールバック処理が完了したら、リカバリされたサーバーに保護計画を適用して、保護が再開されるようにします。元のサーバーに適用されていたものと同じ保護計画、または**ディザスタリカバリ**モジュールが有効になっている新しい保護計画を適用できます。

ターゲット物理マシンへのフェールバック

注意

この機能を利用できるかどうかは、現在のアカウントで有効になっているサービスクォータによって異なります。

ターゲット物理マシンへの自動フェールバックプロセスは、次のフェーズで構成されます。

1. **計画**:このフェーズでは、ホストやネットワーク構成などのローカルサイトのITインフラストラクチャを復元し、フェールバックパラメータを構成します。また、データ転送を開始するタイミングの計画を策定します。
2. **データ転送**:このフェーズでは、クラウド内の仮想マシンが引き続き実行されている間に、クラウドサイトからローカルサイトにデータが転送されます。データ転送の間は、任意のタイミングで次のフェーズであるスイッチオーバーを開始できます。ただし、次の関連要素を考慮する必要があります。

   データ転送フェーズの所要時間が長くなる

   - クラウドにおける仮想マシンの実行時間が長くなる。
   - 比較的多くのデータがローカルサイトに転送される
   - コストが高くなる（より多くのコンピュートポイントを消費する）
   - スイッチオーバーフェーズの間に発生するダウンタイムが短くなる。

   ダウンタイムを最小限に抑えたい場合は、データの90%以上がローカルサイトに転送された後にスイッチオーバーフェーズを開始します。

   より長いダウンタイムを許容する余裕があり、クラウドで仮想マシンを実行するために余分な計算ポイントを消費したくない場合は、より早いタイミングでスイッチオーバーフェーズを開始できます。

   注意

   データ転送プロセスでは、フラッシュバック技術が使用されます。このテクノロジーでは、ターゲットマシンで利用可能なデータとクラウド上の仮想マシンのデータが比較されます。データの一部がすでにターゲットマシンで利用可能な場合、そのデータは再度転送されません。このテクノロジーにより、データ転送フェーズが高速化されます。

   このため、サーバーをローカルサイトの元のマシンに復元することをお勧めします。

3. **スイッチオーバー**:このフェーズでは、クラウド内の仮想マシンがオフになり、最新のバックアップ増分を含む残りのデータがローカルサイトに転送されます。復元サーバーにバックアップ計画が適用されていない場合、スイッチオーバーフェーズで自動的にバックアップが実行されるため、処理速度が遅くなります。

4. **検証**:このフェーズで、ローカルサイトの物理マシンの準備が整い、Linuxベースのブータブルメディアを使って再起動できるようになります。仮想マシンが正しく動作しているかどうかを確認できます。
   - すべてが意図したとおりに動作している場合は、フェールバックを確認します。フェールバック後、クラウドの仮想マシンが削除され、復元サーバーが**スタンバイ**状態に戻ります。これでフェールバックプロセスは終了です。
   - 何か問題がある場合は、フェールオーバーをキャンセルして計画フェーズに戻ることができます。

   注意
   ブータブルメディアが再起動された後は、そのメディアを再度使用することはできません。検証フェーズで何らかの問題が見つかった場合は、新しいブータブルメディアを登録し、フェールバックプロセスを再度開始する必要があります。
   ただし、フラッシュバックテクノロジーが使用されるため、ローカルサイトにあるデータは再度転送されず、フェールバックプロセスはより高速になります。

物理マシンへのフェールバックの実行

注意
この機能を利用できるかどうかは、現在のアカウントで有効になっているサービスクォータによって異なります。

現在のローカルサイトのターゲット物理マシンに対する自動フェールバックを実行できます。

注意
データ転送プロセスでは、フラッシュバック技術が使用されます。このテクノロジーでは、ターゲットマシンで利用可能なデータとクラウド上の仮想マシンのデータが比較されます。データの一部がすでにターゲットマシンで利用可能な場合、そのデータは再度転送されません。このテクノロジーにより、データ転送フェーズが高速化されます。

このため、サーバーをローカルサイトの元のマシンに復元することをお勧めします。

前提条件

- フェールバックの実行に使用するエージェントはオンラインであり、現在、別のフェールバック操作には使用されていません。
- インターネット接続は安定しています。
- 登録済みのブータブルメディアが利用可能である。詳細については、『Cyber Protectionユーザーガイド』の「ブータブルメディアを作成して、オペレーティングシステムをリカバリする」を参照してください。
- ターゲットの物理マシンがローカルサイトの元のマシンであるか、元のマシンと同じファームウェアを使用している。
- クラウド上に少なくとも1件の仮想マシンの完全バックアップが存在する。

物理マシンのフェールバックを実行するには

1. Cyber Protectコンソールで、**[ディザスタリカバリ]** > **[サーバー]** の順に移動します。
2. **[フェールオーバー]** 状態のリカバリサーバーを選択します。
3. **[フェールバック]** タブをクリックします。
4. **ターゲット**フィールドで、**[物理マシン]** を選択します。
5. **ターゲットブータブルメディア**フィールドで、**[指定]** をクリックし、ブータブルメディアを選択して **[完了]** をクリックします。

   注意
   ブータブルメディアはすでに構成されているため、事前構成済みのブータブルメディアを使用することをお勧めします。詳細については、『Cyber Protectionユーザーガイド』の「ブータブルメディアを作成して、オペレーティングシステムをリカバリする」を参照してください。

6. （オプション） デフォルトのディスクマッピングを変更するには、**ディスクマッピング**フィールドで **[指定]** をクリックし、バックアップのディスクをターゲットマシンのディスクにマッピングして、**[完了]** をクリックします。
7. **[データ転送を開始]** をクリックして、確認ウィンドウでもう一度 **[開始]** をクリックします。

   注意
   クラウド上に仮想マシンのバックアップがない場合、システムはデータ転送フェーズの前に自動的にバックアップを実行します。

   データ転送フェーズが開始します。コンソールには、次の情報が表示されます。

フィールド	説明
進行状況	このパラメータは、ローカルサイトにすでに転送されているデータの量と、転送する必要のあるデータの合計量を示します。 データの合計量には、データ転送フェーズが開始される前の最後のバックアップからのデータと、データ転送フェーズ中に仮想マシンが引き続き実行されることによって新しく生成される、データのバックアップ（バックアップの増分）が含まれます。このため、**進行状況**の値は時間とともに増加します。 システムによるデータ転送中はフラッシュバック技術が使用され、ターゲットマシン上ですでに利用可能なデータが転送されることはありません。それで、進行状況はコンソールで最初に計算された値よりも速く進む可能性があります。
ダウンタイムの推定	このパラメータは、スイッチオーバーフェーズを開始する場合、クラウドの仮想マシンが使用できなくなる期間を示します。この値は、**進行状況**パラメータの値に基づいて計算され、時間とともに減少します。 システムによるデータ転送中には、フラッシュバック技術が使用され、ターゲットマシン上ですでに利用可能なデータが転送されることはありません。それでダウンタイムはコンソールに最初に表示される値よりもはるかに短くなる可能性があります。

8. **[スイッチオーバー]** をクリックして、確認ウィンドウでもう一度 **[スイッチオーバー]** をクリックします。

スイッチオーバーフェーズが開始します。コンソールには、次の情報が表示されます。

フィールド	説明
進行状況	このパラメータは、マシンのローカルサイトに対する復元の進行状況を示します。
完了までの推定所要時間	このパラメータは、スイッチオーバーフェーズが完了し、ローカルサイトでマシンを起動できるようになるまでの、おおよその時間を示します。

注意
クラウド上の仮想マシンにバックアップ計画が適用されていない場合、スイッチオーバーフェーズで自動的にバックアップが実行されるため、ダウンタイムが長くなります。

9. **スイッチオーバー**フェーズが完了したら、ブータブルメディアを再起動し、ローカルサイトの物理マシンが想定した通りに動作していることを確認します。
   詳細については、『Cyber Protectionユーザーガイド』の「ブータブルメディアを使用したディスクのリカバリ」を参照してください。
10. **[フェールバックの確認]** をクリックし、確認ウィンドウでもう一度 **[確認]** をクリックして、プロセスを最終化します。
    クラウドの仮想マシンが削除され、復元サーバーが**スタンバイ**状態に戻ります。

注意
フェールバック処理で、リカバリされたサーバーに保護計画が適用されることはありません。
フェールバック処理が完了したら、リカバリされたサーバーに保護計画を適用して、保護が再開されるようにします。元のサーバーに適用されていたものと同じ保護計画、または**ディザスタリカバリ**モジュールが有効になっている新しい保護計画を適用できます。

手動フェールバック

注意
サポートチームからアドバイスを受けた場合に限り、手動モードの使用によるフェールバックプロセスの実行をお勧めします。

手動モードでフェールバックプロセスを開始することもできます。この場合、クラウド上のバックアップからローカルサイトへのデータ転送は自動的には行われません。クラウド上の仮想マシンの電源が遮断された後に手動で行う必要があります。このため、手動モードでのフェールバック処理は非常に遅くなり、ダウンタイムの期間が長くなることが想定されます。

手動モードでのフェールバックプロセスは、以下のフェーズで構成されます:

1. **計画**:このフェーズでは、ホストやネットワーク構成などのローカルサイトのITインフラストラクチャを復元し、フェールバックパラメータを構成します。また、データ転送を開始するタイミングの計画を策定します。

2. **スイッチオーバー**:このフェーズでは、クラウド内の仮想マシンがオフになり、新しく生成されたデータがバックアップされます。復元サーバーにバックアップ計画が適用されていない場合、スイッチオーバーフェーズで自動的にバックアップが実行されるため、処理速度が遅くなります。バックアップが完了したら、ローカルサイトにマシンを手動でリカバリします。ブータブルメディアを使用してディスクをリカバリするか、クラウドバックアップストレージからマシン全体をリカバリすることができます。
3. **検証**:このフェーズでは、ローカルサイトの物理マシンまたは仮想マシンが正しく動作していることを検証し、フェールバックを確認します。確認後、クラウドサイトの仮想マシンが削除され、復元サーバーが**スタンバイ**状態に戻ります。

手動フェールバックを実行する

注意
この機能を利用できるかどうかは、現在のアカウントで有効になっているサービスクォータによって異なります。

現在のローカルサイトのターゲット物理マシンまたは仮想マシンに対する手動フェールバックを実行できます。

手動フェールバックを実行するには

1. Cyber Protectコンソールで、**[ディザスタリカバリ]** > **[サーバー]** の順に移動します。
2. **[フェールオーバー]** 状態のリカバリサーバーを選択します。
3. **[フェールバック]** タブをクリックします。
4. **ターゲット**フィールドで、**[物理マシン]** を選択します。
5. ギアアイコンをクリックし、**[マニュアルモードを使用する]** スイッチを有効にします。
6. （オプション）**バックアップサイズ**の値をインターネットの転送速度で除算することで、ターゲット物理マシンへのフェールバック処理に伴うダウンタイムの目安を計算できます。

   注意
   複数のフェールバック処理を同時に行うと、インターネット速度の値が低下します。

7. **[スイッチオーバー]** をクリックして、確認ウィンドウでもう一度 **[スイッチオーバー]** をクリックします。
   クラウドサイトの仮想マシンがオフになっています。

   注意
   クラウド上の仮想マシンにバックアップ計画が適用されていない場合、スイッチオーバーフェーズで自動的にバックアップが実行されるため、ダウンタイムが長くなります。

8. 現在のローカルサイトの物理マシンまたは仮想マシンに対して、クラウドバックアップからサーバーをリカバリします。詳細については、『Cyber Protectionユーザーガイド』の「マシンをリカバリする」を参照してください。
9. リカバリが完了し、リカバリしたマシンが正常に動作することを確認してから、**[マシンが復元されました]** をクリックします。

10. 意図したとおりに動作が完了している場合、**[フェールバックの確認]** をクリックして、確認ウィンドウでもう一度 **[確認]** をクリックします。
    復元サーバーと復元ポイントは、次のフェールオーバーのために準備完了となります。新しい復元ポイントを作成するには、新しいローカルサーバーに保護計画を適用します。

    注意
    フェールバック処理で、リカバリされたサーバーに保護計画が適用されることはありません。
    フェールバック処理が完了したら、リカバリされたサーバーに保護計画を適用して、保護が再開されるようにします。元のサーバーに適用されていたものと同じ保護計画、または**ディザスタリカバリ**モジュールが有効になっている新しい保護計画を適用できます。

暗号化されたバックアップでの作業

暗号化されたバックアップから復元サーバーを作成できます。便宜を図るため、復元サーバーへのフェールオーバー中に、暗号化されたバックアップに対して自動パスワードアプリケーションを設定できます。

復元サーバーを作成する際、自動ディザスタリカバリ操作に使用するパスワードを指定できます。これは、資格情報の安全な保管場所である資格情報ストアに保存されます。資格情報ストアは、**[設定]** > **[資格情報]** セクションにあります。

1つの資格情報を幾つかのバックアップにリンクさせることができます。

資格情報ストアで保存したパスワードを管理するには

1. **[設定]** > **[資格情報]** へ進みます。
2. 特定の資格情報を管理するには、最後の列のアイコンをクリックします。この資格情報にリンクされたアイテムを確認できます。
   - 選択した資格情報からバックアップをリンク解除するには、バックアップの近くにあるゴミ箱アイコンをクリックします。その結果、復元サーバーへのフェールオーバー中、パスワードを手動で指定する必要が生じます。
   - 資格情報を編集するには、**[編集]** をクリックし、名前またはパスワードを指定します。
   - 資格情報を削除するには、**[削除]** をクリックします。復元サーバーへのフェールオーバー中、パスワードを手動で指定する必要があることに留意してください。

Microsoft Azure仮想マシンを使った処理

注意
適用されるライセンスモデルによっては、一部の機能で追加のライセンスが必要になる場合があります。

Microsoft Azure仮想マシンのフェールオーバーをAcronis Cyber Protect Cloudで実行できます。詳細については、"フェールオーバーの実行"（767ページ）を参照してください。

その後、Acronis Cyber Protect CloudからAzure仮想マシンへのフェールバックを実行できます。このフェールバックプロセスは、物理マシンへのフェールバックプロセスと同様です。詳細については、"前提条件"（777ページ）を参照してください。

注意
フェールバック用のAzure仮想マシンを新規に登録するには、Azureで利用可能なAcronis Backup VM拡張機能を使用できます。

Acronis Cyber Protect CloudとAzure VPNゲートウェイ間のマルチサイトIPsec VPN接続を構成できます。詳細については、"マルチサイトIPsec VPNの構成"（736ページ）を参照してください。

プライマリサーバー設定

このセクションでは、プライマリサーバーの作成および管理の方法について説明します。

プライマリサーバーの作成

前提条件

- クラウドサイトへの接続タイプの1つを設定する必要があります。

プライマリサーバーを作成します

1. **[ディザスタリカバリ]** > **[サーバー]** > **[プライマリサーバー]** タブの順に移動します。
2. **[作成]** をクリックします。
3. 新しい仮想マシンのテンプレートを選択します。
4. 構成のフレーバー（仮想コアの数とRAMのサイズ）を選択します。次の表は、各フレーバーのディスク容量合計の最大値（GB）を示しています。

種類	vCPU	RAM（GB）	ディスク容量合計の最大値（GB）
F1	1	2	500
F2	1	4	1000
F3	2	8	2000
F4	4	16	4000
F5	8	32	8000
F6	16	64	16000
F7	16	128	32000
F8	16	256	64000

注意
すべてのオプションの計算ポイントを確認できます。コンピュートポイントの数は、プライマリサーバーを 1 時間当たり実行するコストを反映しています。詳細については、"コンピュートポイント"（718ページ）を参照してください。

5. （オプション）仮想ディスクサイズの変更複数のハードディスクが必要な場合は、**[ディスクを追加]** をクリックし、新しいディスクサイズを指定します。現在、プライマリサーバーにはディスクを9台まで追加できます。
6. プライマリサーバーが含まれるクラウドネットワークを指定します。
7. **[DHCP]** オプションを選択します。

DHCPオプション	説明
クラウドサイトにより提供	デフォルトの設定。サーバーのIPアドレスは、クラウド上に自動設定されたDHCPサーバーにより提供されます。
カスタム	サーバーのIPアドレスは、クラウド上で現在動作しているDHCPサーバーにより提供されます。

8. （オプション） **MACアドレス**を指定します。
   MACアドレスは、サーバーのネットワークアダプタに割り当てられる一意の識別子です。カスタムのDHCPを使用する場合、特定のMACアドレスに対して、常に特定のIPアドレスが割り当てられるように設定できます。これにより、プライマリサーバーが常に同じIPアドレスを取得できるようになります。MACアドレスで登録されたライセンスを有するアプリケーションを実行することができます。
9. 本番ネットワークでサーバーが持つ IP アドレスを指定します。デフォルトでは、本番ネットワークの最初の空き IP アドレスが設定されています。

注意
DHCPサーバーを使用する場合は、IPアドレスの競合を回避するために、このIPアドレスをサーバーの除外一覧に追加します。
カスタムのDHCPサーバーを使用する場合、**稼働中のネットワークのIPアドレス**には、DHCPサーバーの設定と同一のIPアドレスを指定する必要があります。そうしない場合、テストフェールオーバーが正しく動作せず、パブリックIPアドレス経由でサーバーに到達できなくなります。

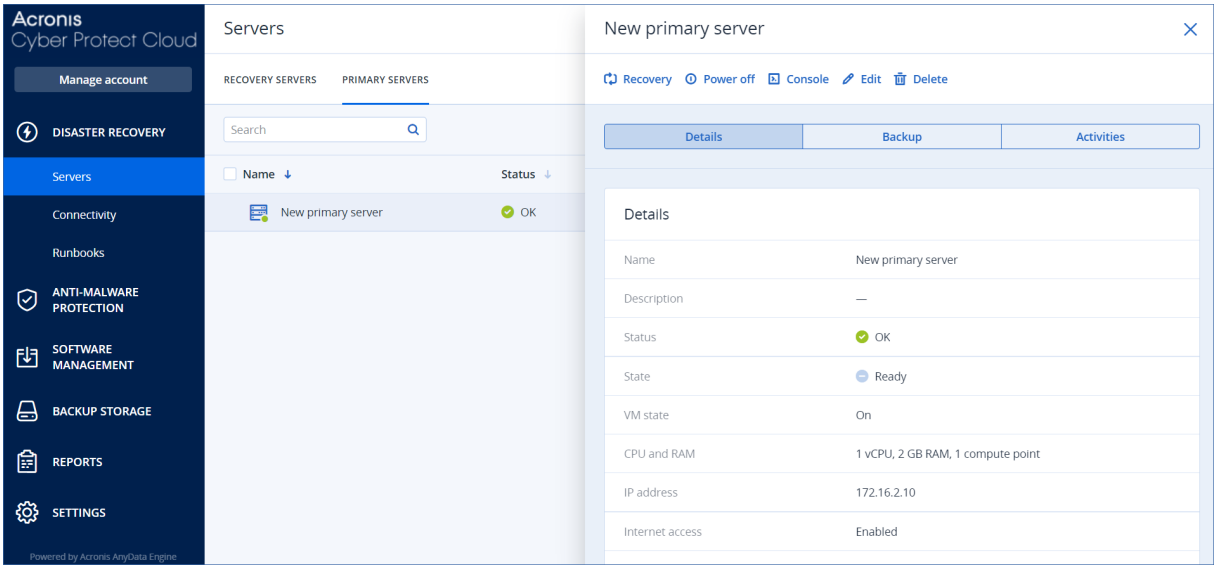
10. （オプション）**[インターネットアクセスの許可]** チェックボックスをオンにします。
    これにより、プライマリサーバーはインターネットにアクセスできます。デフォルトでは、TCPポート25番はパブリックIPアドレスへの送信接続用に開いています。
11. （オプション）**[パブリックIPアドレスを使用する]** チェックボックスをオンにします。
    パブリック IP アドレスを持つことで、プライマリサーバーがインターネットから利用可能になります。チェックボックスをオフのままにすると、サーバーは本番ネットワークでのみ使用可能になります。

パブリック IP アドレスは、設定が完了した後に表示されます。デフォルトでは、TCPポート443番はパブリックIPアドレスへの受信接続用に開いています。

注意
[パブリックIPアドレスを使用する] チェックボックスをオフにするか、復元サーバーを削除すると、そのパブリックIPアドレスは予約されません。

12. （オプション）**RPO しきい値を設定**を選択します。
    RPO しきい値は、最後の復元ポイントと現在時刻との間の最大許容時間間隔を定義します。数値は15～60分、1～24時間、1～14日間の範囲で設定できます。
13. プライマリサーバー名を定義します。
14. （オプション）プライマリサーバーの説明を指定します。
15. （オプション）**[クラウドファイアウォールのルール]** タブをクリックして、デフォルトのファイアウォールルールを編集します。詳細については、"クラウドサーバーのファイアウォールルール設定"（786ページ）を参照してください。
16. **[作成]** をクリックします。

プライマリサーバーが本番ネットワークで使用できるようになります。コンソール、RDP、SSH、または TeamViewer を使用してサーバーを管理できます。



プライマリサーバーでの操作

プライマリサーバーは、コンソールの **[ディザスタリカバリ]** > **[サーバー]** > **[プライマリサーバー]** タブに表示されます。

サーバーを起動または停止するには、プライマリサーバーパネルの **[電源オン]** または **[電源オフ]** をクリックします。

プライマリサーバーの設定を編集するには、サーバーを停止し、**[編集]** をクリックします。

プライマリサーバーに保護計画を適用するには、該当の保護計画を選択し、**[計画]** タブで **[作成]** をクリックします。スケジュールと保持ルールのみを変更できる事前定義済みの保護計画が表示されます。詳細については、「クラウドサーバーのバックアップ」を参照してください。

クラウドサーバーの管理

クラウドサーバーを管理するには、**[Disaster Recovery]** > **[サーバー]** の順に移動します。2種類のタブがあります。**[リカバリサーバー]** と **[プライマリサーバー]** です。表内のすべてのオプション列を表示するには、ギアアイコンをクリックします。

タブをクリックすると、各クラウドサーバーについて以下の情報を見つけることができます。

列名	説明
名前	定義したクラウドサーバー名
ステータス	クラウドサーバーに関係する最も深刻な問題を反映しているステータス（アクティブアラートに基づく）
状態	クラウドサーバーの状態
VMの状態	クラウドサーバーに関連付けられた仮想マシンの電源の状態
アクティブなロケーション	サーバーがホストされるロケーションです。たとえば、**クラウド**のようになります。
RPOしきい値	フェールオーバーのための最後の適切な復元ポイントと現在時刻との間の許容される最大時間間隔。数値は15～60分、1～24時間、1～14日間の範囲で設定できます。
RPOコンプライアンス	RPOコンプライアンスは、実際のRPOとRPOしきい値との比率です。RPOしきい値が定義されるとRPOコンプライアンスが表示されます。 それは以下のように計算されます。 **RPOコンプライアンス=実際のRPO/RPOしきい値** ここで、 **実際のRPO=現在時刻–直近の復元ポイント** **RPOコンプライアンス状態** 実際のRPOとRPOしきい値との比率の値に応じて、以下の状態が使用されます。 • **準拠**。RPOコンプライアンス<1x。サーバーがRPOしきい値を満たしています。 • **超過**。RPOコンプライアンス<=2x。サーバーがRPOしきい値に違反しています。 • **大幅に超過**。RPOコンプライアンス<=4x。サーバーがRPOしきい値に2倍以上違反しています。 • **危機的な超過**。RPOコンプライアンス>4x。サーバーがRPOしきい値に4倍以上違反しています。 • **保留中（バックアップなし）**。サーバーは保護計画により保護されていますが、バックアップは作成中で、まだ完了していません。

実際のRPO	最後の復元ポイント作成から経過した時間
前回の復元ポイント	前回復元ポイントが作成された日時

クラウドサーバーのファイアウォールルール

ファイアウォールルールを構成して、クラウドサイトのプライマリサーバーと復元サーバーの受信トラフィックと送信トラフィックを制御できます。

クラウドサーバーのパブリックIPアドレスをプロビジョニングした後、受信ルールを構成できます。デフォルトでは、TCPポート443番が許可され、他のすべての受信接続は拒否されます。デフォルトのファイアウォールルールを変更したり、受信例外を追加または削除したりできます。パブリックIPがプロビジョニングされていない場合、受信ルールは表示のみが可能であり、構成することはできません。

クラウドサーバーにインターネットアクセスをプロビジョニングした後、送信ルールを構成できます。デフォルトでは、TCPポート25番は拒否され、他のすべての送信接続は許可されます。デフォルトのファイアウォールルールを変更したり、送信例外を追加または削除したりできます。インターネットアクセスがプロビジョニングされていない場合、送信ルールは表示のみが可能であり、構成することはできません。

注意
セキュリティ上の理由から変更できない、事前定義のファイアウォールルールがあります。

受信および送信接続の場合:

- pingを許可する:ICMPエコー要求（タイプ8、コード0）およびICMPエコー応答（タイプ0、コード0）
- ICMP need-to-fragを許可（タイプ3、コード4）
- TTL超過を許可（タイプ11、コード0）

受信接続のみの場合:

- 構成できない部分:すべて拒否

送信接続のみの場合:

- 構成できない部分:すべて拒否

クラウドサーバーのファイアウォールルール設定

クラウド内のプライマリサーバーと復元サーバーにおけるデフォルトのファイアウォールルールを編集できます。

クラウドサイト上のサーバーのファイアウォールルールを編集するには

1. Cyber Protectコンソールで、**[ディザスタリカバリ]** > **[サーバー]** の順に移動します。
2. 復元サーバーのファイアウォールルールを編集する場合は、**[復元サーバー]** タブをクリックします。また、プライマリサーバーのファイアウォールルールを編集する場合は、**[プライマリサーバー]**

タブをクリックします。

3. サーバーをクリックしてから、［**編集**］ をクリックします。
4. [**クラウドファイアウォールのルール**] タブをクリックします。
5. 受信接続のデフォルトアクションを変更する場合:
   a. [**受信**] ドロップダウンフィールドで、デフォルトのアクションを選択します。

アクション	説明
すべて拒否	すべての受信トラフィックを拒否 例外を追加して、特定のIPアドレス、プロトコル、およびポートからのトラフィックを許可できます。
すべて許可	すべての受信TCPおよびUDPトラフィックを許可します。 例外を追加して、特定のIPアドレス、プロトコル、およびポートからのトラフィックを拒否できます。

注意
デフォルトのアクションを変更すると、既存の受信ルールの構成が無効になり、削除されます。

   b. （オプション） 既存の例外を保存する場合は、確認ウィンドウで [**記述済みの例外を保存する**] を選択します。
   c. [**確認**] をクリックします。
6. 例外を追加する場合:
   a. [**例外の追加**] をクリックします。
   b. ファイアウォールのパラメータを指定します。

ファイアウォールパラメータ	説明
プロトコル	接続のプロトコルを選択します。次のオプションがサポートされています。 • **TCP** • **UDP** • **TCP+UDP**
サーバーポート	ルールを適用するポートを選択します。次の項目を指定できます。 • 特定のポート番号（`2298`など） • ポート番号の範囲（`6000-6700`など） • 任意のポート番号。ルールを任意のポート番号に適用する場合、`*`を使用します。
クライアントIPアドレス	ルールを適用するIPアドレスを選択します。次の項目を指定できます。 • 特定のIPアドレス（`192.168.0.0`など）

ファイアウォールパラメータ	説明
	• CIDR表記を使用したIPアドレスの範囲（`192.168.0.0/24`など）。 • 任意のIPアドレス。ルールを任意のIPアドレスに適用する場合、`*`を使用します。

7. 既存の受信例外を削除する場合は、その横にあるごみ箱アイコンをクリックします。
8. 送信接続のデフォルトアクションを変更する場合:
   a. **[送信]** ドロップダウンフィールドで、デフォルトのアクションを選択します。

アクション	説明
すべて拒否	すべての送信トラフィックを拒否します。 例外を追加して、特定のIPアドレス、プロトコル、およびポートへのトラフィックを許可できます。
すべて許可	すべての送信トラフィックを許可します。 例外を追加して、特定のIPアドレス、プロトコル、およびポートからのトラフィックを拒否できます。

注意
デフォルトのアクションを変更すると、既存の送信ルールの構成が無効になり、削除されます。

   b. （オプション） 既存の例外を保存する場合は、確認ウィンドウで **[記述済みの例外を保存する]** を選択します。
   c. **[確認]** をクリックします。
9. 例外を追加する場合:
   a. **[例外の追加]** をクリックします。
   b. ファイアウォールのパラメータを指定します。

ファイアウォールパラメータ	説明
プロトコル	接続のプロトコルを選択します。次のオプションがサポートされています。 • **TCP** • **UDP** • **TCP+UDP**
サーバーポート	ルールを適用するポートを選択します。次の項目を指定できます。 • 特定のポート番号（`2298`など） • ポート番号の範囲（`6000-6700`など）

ファイアウォールパラメータ	説明
	• 任意のポート番号。ルールを任意のポート番号に適用する場合、*を使用します。
クライアントIPアドレス	ルールを適用するIPアドレスを選択します。次の項目を指定できます。 • 特定のIPアドレス（192.168.0.0など） • CIDR表記を使用したIPアドレスの範囲（192.168.0.0/24など）。 • 任意のIPアドレス。ルールを任意のIPアドレスに適用する場合、*を使用します。

10. 既存の送信例外を削除する場合は、その横にあるごみ箱アイコンをクリックします。
11. **[保存]** をクリックします。

クラウドファイアウォールのアクティビティを確認する

クラウドサーバーのファイアウォールルールの構成をアップデートすると、アップデートアクティビティのログがCyber Protectコンソールで利用できるようになります。ログを表示して、次の情報を確認できます。

- 構成をアップデートしたユーザーのユーザー名
- アップデートの日時
- 受信および送信接続のファイアウォール設定
- 受信および送信接続のデフォルトアクション
- 受信接続と送信接続の例外のプロトコル、ポート、およびIPアドレス

クラウドファイアウォールルールの構成変更に関する詳細を表示するには

1. Cyber Protectコンソールで、**[監視]** > **[アクティビティ]** をクリックします。
2. 対応するアクティビティをクリックしてから、**[すべてのプロパティ]** をクリックします。
   アクティビティの説明を、**クラウドサーバー構成の更新**にする必要があります。
3. **[コンテキスト]** フィールドで、興味のある情報を調べます。

クラウドサーバーのバックアップ

プライマリサーバーと復元サーバーは、クラウドサイトにてエージェントレスでバックアップされます。これらのバックアップには以下の制限があります。

- 唯一可能なバックアップロケーションはクラウドストレージです。プライマリサーバーのバックアップ先は、**プライマリサーバーのバックアップ**ストレージです。

注意
Microsoft Azureのバックアップロケーションはサポートされていません。

- 複数のサーバーにバックアップ計画を適用することはできません。すべてのバックアップ計画に同じ設定が適用されていても、各サーバーには独自のバックアップ計画が必要です。
- サーバーに適用できるバックアップ計画は 1 つのみです。
- アプリケーションアウェアバックアップはサポートされていません。
- 暗号化は使用できません。
- バックアップオプションを使用できません

プライマリサーバーを削除すると、そのバックアップも削除されます。

リカバリサーバーは、フェールオーバー状態でのみバックアップされます。そのバックアップは、元のサーバーのバックアップシーケンスを続行します。フェールバックが実行されると、元のサーバーはこのバックアップシーケンスを続行できます。したがって、リカバリサーバーのバックアップは、手動で、または保持ルールを適用した結果としてのみ削除できます。リカバリサーバーが削除されると、そのバックアップは常に保持されます。

注意
クラウドサーバーのバックアップ計画はUTC時間に従って実行されます。

オーケストレーション（ランブック）

注意
適用されるライセンスモデルによっては、一部の機能で追加のライセンスが必要になる場合があります。

ランブックは、クラウドで製品環境を立ち上げる方法を説明する指示のセットです。ランブックは、Cyber Protectコンソールから作成できます。**[ランブック]** 画面にアクセスするには、**[ディザスタリカバリ]** > **[ランブック]** を選択します。

ランブックを使用する理由

ランブックを使用して以下の操作を実行できます。

- 1台以上のサーバーのフェールオーバーを自動化する
- サーバーIPアドレスにpingを実行し、指定するポートとの接続を確認して、フェールオーバーの結果を自動的に確認する
- 分散アプリケーションを実行しているサーバーの操作の順序を設定する
- ワークフローに手動操作を含める
- ランブックをテストモードで実行して、ディザスタリカバリソリューションのインテグリティを検証します。

ランブックの作成

ランブックは、連続して実行される手順で構成されています。手順は、同時に開始される操作で構成されています。

以下の操作を実行するか、ビデオチュートリアルを視聴できます。

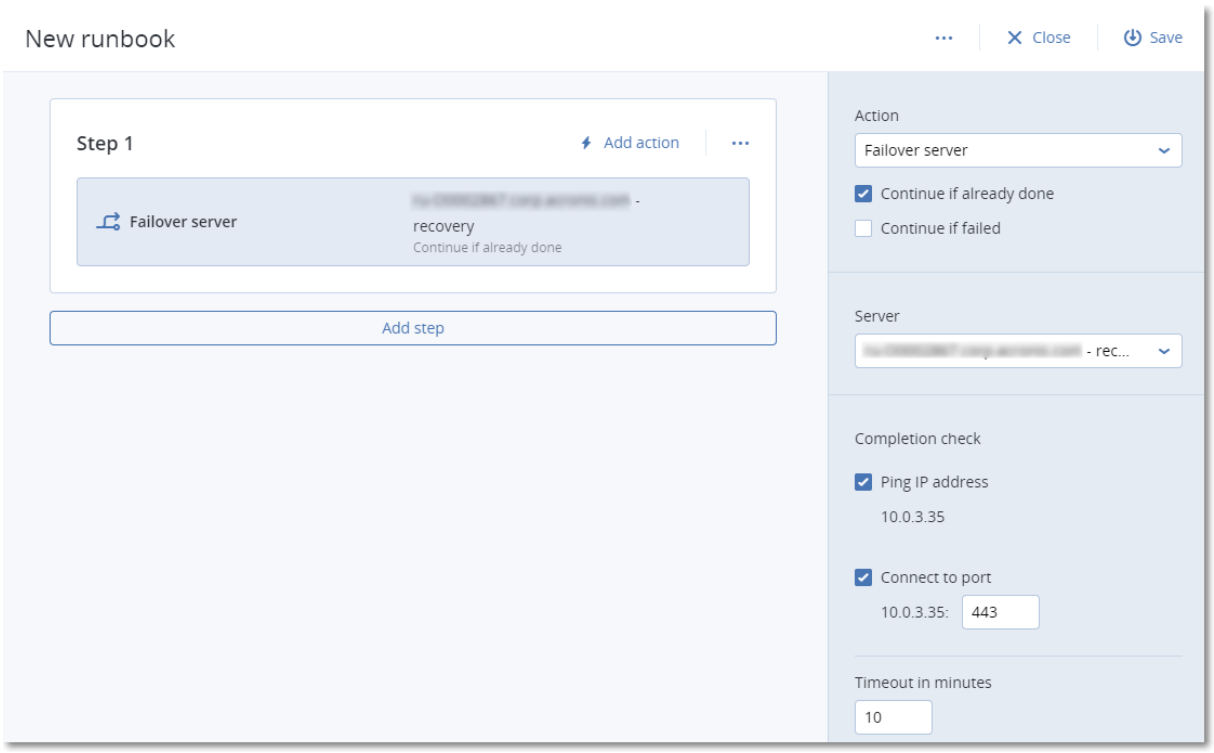
ランブックを作成するには

1. Cyber Protectionコンソールで、**[ディザスタリカバリ]** > **[ランブック]** に移動します。
2. **[ランブックを作成]** をクリックします。
3. **[手順を追加]** をクリックします。
4. **[操作を追加]** をクリックし、手順に追加したい操作を選択します。

アクション	説明
サーバーをフェールオーバー	クラウドサーバーのフェールオーバーを実行します。この操作を定義するには、クラウドサーバーを選択し、この操作で利用可能なランブックのパラメータを設定する必要があります。これらのパラメータについての詳細は、"ランブックパラメータ"（793ページ）を参照してください。 **注意** 選択したサーバーのバックアップがマシンプロパティとしての暗号化を使用して暗号化されている場合、**サーバーをフェールオーバー**の操作は一時停止され、自動的に**インタラクションが必要**に変更されます。ランブックの実行を続けるためには、暗号化されたバックアップのパスワードを指定する必要があります。
サーバーをフェールバック	クラウドサーバーのフェールバックを実行します。この操作を定義するには、クラウドサーバーを選択し、この操作に利用可能なランブックのパラメータを設定する必要があります。これらの設定の詳細については、"ランブックパラメータ"（793ページ）を参照してください。 **注意** ランブックの処理では、手動モードのフェールバックのみがサポートされます。これは、**サーバーをフェールバック**手順を含むランブックを実行してフェールバックプロセスを開始した場合、その手順で手動によるインタラクションが必要となることを意味しています。つまり、マシンを手動でリカバリし、**[ディザスタリカバリ]** > **[サーバー]** タブからフェールバックプロセスを確認またはキャンセルする必要があります。
サーバーを起動	クラウドサーバーを起動します。この操作を定義するには、クラウドサーバーを選択し、この操作で利用可能なランブックのパラメータを設定する必要があります。これらの設定の詳細については、"ランブックパラメータ"（793ページ）を参照してください。

アクション	説明
	注意 **サーバーを起動**操作は、ランブック内のテストフェールオーバー操作には適用できません。この操作を実行しようとすると、次のエラーメッセージにより失敗します。 失敗: この操作は現在のサーバーステータスには適用できません。
サーバーを停止	クラウドサーバーを停止します。この操作を定義するには、クラウドサーバーを選択し、この操作で利用可能なランブックのパラメータを設定する必要があります。これらの設定の詳細については、"ランブックパラメータ"（793ページ）を参照してください。 **注意** **サーバーを停止**操作は、ランブック内のテストフェールオーバー操作には適用できません。この操作を実行しようとすると、次のエラーメッセージにより失敗します。 失敗: この操作は現在のサーバーステータスには適用できません。
手動処理	手動処理はユーザーからのインタラクションを必要とします。この操作を定義するには、説明を入力する必要があります。 ランブックのシーケンスが手動処理に到達すると、ランブックは一時停止し、ユーザーが確認ボタンをクリックするなどの必要な手動処理が実行されるまで、続行されません。
ランブックを実行する	別のランブックを実行します。この操作を定義するには、ランブックを選択する必要があります。 ランブックは、任意のランブックの1つの実行のみを含めることができます。たとえば、アクション"ランブックAを実行"を追加した場合、アクション"ランブックBを実行"は追加できますが、別のアクション"ランブックAを実行"を含めることはできません。

5. 操作のランブックパラメータを定義します。これらのパラメータの詳細については、"ランブックパラメータ"（793ページ）を参照してください。
6. （オプション） 手順の説明を追加するには:
   a. アイコンの省略記号をクリックしてから、**[説明]** をクリックします。
   b. 手順の説明を入力します。
   c. **[完了]** をクリックします。
7. 必要な手順と操作のシーケンスが作成できるまで、手順3から6を繰り返します。
8. （オプション） ランブックのデフォルト名を変更するには:
   a. 省略記号アイコンをクリックします。
   b. ランブックの名前を入力します。
   c. ランブックの説明を入力します。
   d. **[完了]** をクリックします。
9. **[保存]** をクリックします。
10. **[閉じる]** をクリックします。



ランブックパラメータ

ランブックのパラメータは、ランブックの操作を定義するために構成しなければならない特定の設定です。ランブックのパラメータには、操作パラメータと完全性チェックパラメータの2種類のカテゴリがあります。

操作パラメータは、操作の初期化状態または結果によってランブックの動作を定義します。

完全性チェックパラメータは、サーバーが利用可能で必要なサービスが提供されていることを確認します。完全性チェックが失敗すると、その操作は失敗とみなされます。

各操作に対して構成可能なランブックのパラメータを次の表に示します。

ランブックパラメータ	カテゴリ	操作に対して利用可能	説明
実行済みの場合は続行	操作パラメータ	• **サーバーをフェールオーバー** • **サーバーを起動** • **サーバーを停止** • **サーバーをフェールバック**	このパラメータでは、必要な操作がすでに完了している場合（例えば、フェールオーバーがすでに実行されているか、サーバーがすでに稼働している場合など）のランブックの動作を定義します。有効にすると、ランブックで警告が発生したあとも、処理が続行されます。無効にした場合、操作が失敗したあとは、ランブックは実行されません。 デフォルトでは、このパラメータは有効化されています。

ランブックパラメータ	カテゴリ	操作に対して利用可能	説明
失敗の場合は続行	操作パラメータ	• **サーバーをフェールオーバー** • **サーバーを起動** • **サーバーを停止** • **サーバーをフェールバック**	このパラメータでは、必要な操作が失敗したときのランブックの動作を定義します。有効にすると、ランブックで警告が発生したあとも、処理が続行されます。無効にした場合、操作が失敗したあとは、ランブックは実行されません。 デフォルトでは、このパラメータは無効化されています。
IPアドレスにpingを実行	完了の確認	• **サーバーを起動**	ソフトウェアは、サーバーが応答するかタイムアウトするか、いずれか早い方まで、クラウドサーバーの本番IPアドレスにpingを実行します。
[ポートに接続]（デフォルトでは443）	完了の確認	• **サーバーをフェールオーバー** • **サーバーを起動**	ソフトウェアは、接続が確立するかタイムアウトするか、いずれか早い方まで、クラウドサーバーの本番IPアドレスと指定するポートを使用して、クラウドサーバーに接続しようとします。この方法で、指定したポートで待機するアプリケーションが動作しているかどうかを確認できます。
タイムアウト（分）	完了の確認	• **サーバーをフェールオーバー** • **サーバーを起動**	デフォルトのタイムアウトは10分間です。

ランブックの操作

注意
この機能を利用できるかどうかは、現在のアカウントで有効になっているサービスクォータによって異なります。

操作の一覧にアクセスするには、ランブックにマウスポインタを重ね、省略記号アイコンをクリックします。ランブックが実行中ではない場合は、以下の操作が利用できます。

- **実行**
- **編集**
- **クローンを作成**
- **削除**

ランブックの実行

[実行] をクリックするたびに、実行パラメータを求められます。これらのパラメータは、ランブックに含まれるすべてのフェールオーバーとフェールバックに適用されます。**[ランブックを実行]** 操作で指定されるランブックは、メインのランブックからこれらのパラメータを継承します。

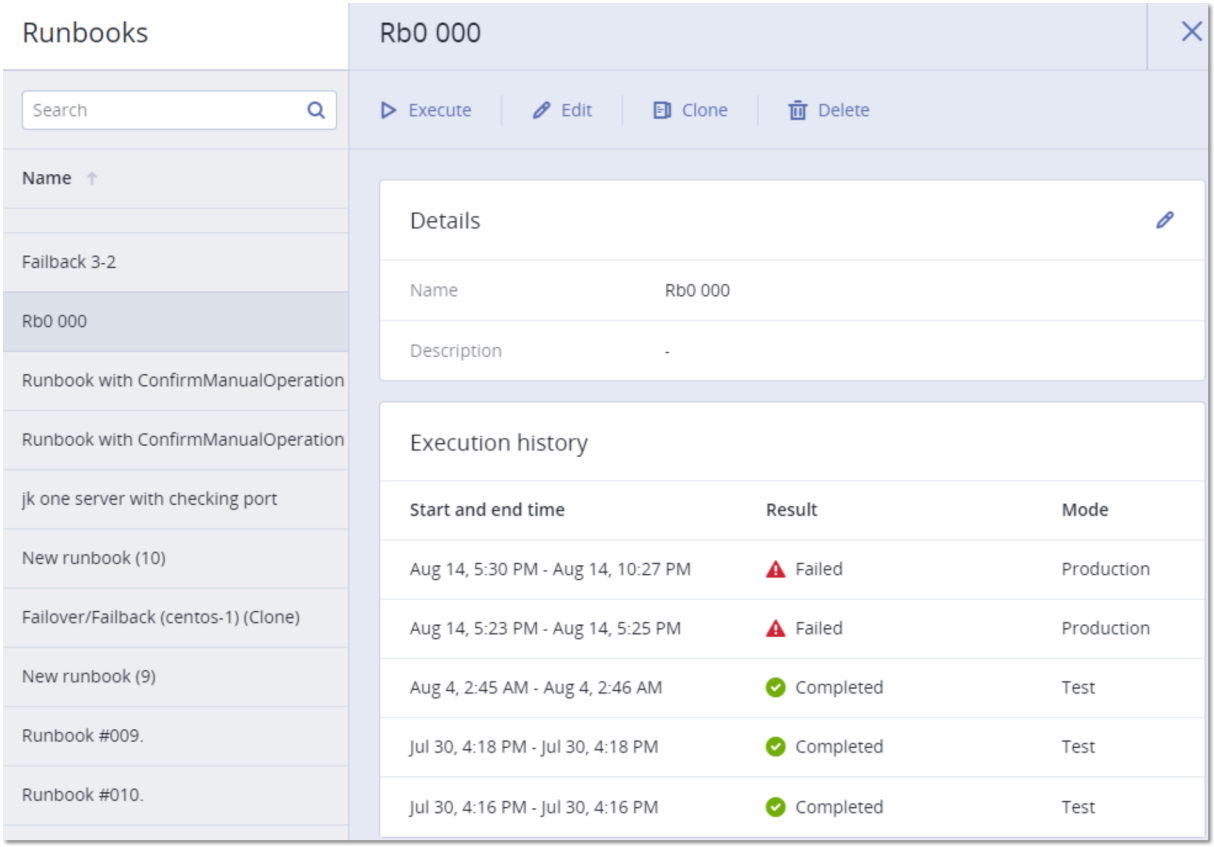
- **フェールオーバーおよびフェールバックモード**
  テストフェールオーバー（デフォルト）を実行するか本番フェールオーバーを実行するかを選択します。フェールバックモードは、選択されたフェールオーバーモードに対応します。
- **フェールオーバー復元ポイント**
  最新の復元ポイントを選択する（デフォルト）か、過去の時点を選択します。後者の場合、各サーバーについて、指定した日時の前で最も近い復元ポイントが選択されます。

ランブックの実行の停止

ランブックの実行中、操作の一覧で **[停止]** を選択できます。ユーザーの干渉を必要とするものを除き、ソフトウェアは、開始済みのすべてのアクションを完了します。

実行履歴の表示

[ランブック] タブでランブックを選択したとき、ソフトウェアによりランブックの詳細と実行履歴が表示されます。実行ログを表示するには、特定の実行に対応する行をクリックします。



ウイルスおよびマルウェア対策保護を構成する

注意
Windowsマシンで、マルウェア対策保護機能を利用するには、マルウェア対策保護エージェントのインストールが必要であり、URLフィルタリング機能を利用するには、URLフィルタリングエージェントのインストールが必要です。これらのエージェントは、保護計画で**ウイルスおよびマルウェア対策保護**や**URLフィルタリング**のモジュールが有効になっている場合、保護対象のワークロードに自動的にインストールされます。

Cyber Protectionのマルウェア対策機能には以下のメリットがあります。

- 事前、実行時、事後のどのステージでも最高度の保護が可能です。
- 4種類のマルウェア対策テクノロジーが組み込まれていて、最先端の多層保護を実現できます。
- Microsoft Security EssentialsとMicrosoft Defender Antivirusを管理できます。

> **注意**
> この機能を利用できるかどうかは、現在のアカウントで有効になっているサービスクォータによって異なります。

重要
EICARテストファイルは、保護計画で **[高度なマルウェア対策機能]** オプションが有効になっている場合にのみ検出されます。ただし、EICARファイルが検出されなくても、Cyber Protectionのマルウェア対策機能には影響しません。

サポートされるプラットフォーム

Active Protection、ウイルスおよびマルウェア対策機能は、以下のプラットフォームでサポートされています。

オペレーティングシステム	バージョン/ディストリビューション
Windows	Windows 7 Service Pack 1以降 Windows Server 2008 R2 Service Pack 1以降 **注意** Windows 7の場合、プロテクションエージェントをインストールする前に、Microsoftが提供する次のアップデートプログラムをインストールする必要があります。 • Windows 7拡張セキュリティアップデートプログラム（ESU） • KB4474419 • KB4490628 必要なアップデートの詳細については、このナレッジベースの記事を参照してください。

オペレーティングシステム	バージョン/ディストリビューション
Linux	Red Hat Linux 7.x, 8.x, 9.x CloudLinux 6.10, 7.x, 8.x CentOS 6.5および6.x以降のバージョン、7.x、8.x Ubuntu 16.04, 18.04, 20.04, 22.04, 22.10 Debian 8.x, 9.x, 10,x, 11.x Oracle Linux 7.x, 8.x, 9.x SUSE Enterprise Linux 15.x openSUSE Leap 15.x
macOS	macOS 10.13.x以降

プラットフォームごとにサポートされる機能

注意
LinuxとmacOS用のマルウェア対策保護は、高度なマルウェア対策機能パックで利用できます。

機能セット	Windows	Linux	macOS
ウイルスおよびマルウェア対策保護			
完全統合型のActive Protection機能	はい	いいえ	いいえ
リアルタイムのマルウェア対策保護	はい	はい（高度なマルウェア対策機能パック付属）	はい（Advancedマルウェア対策パック付属）
ローカル署名ベースの検出によるAdvancedリアルタイムマルウェア対策保護	はい	はい	はい
ポータブル実行可能ファイルの静的分析	はい	いいえ	はい*
オンデマンドマルウェア対策スキャン	はい	はい**	はい
ネットワークフォルダの保護	はい	はい	いいえ
サーバー側保護機能	はい	いいえ	いいえ
アーカイブファイルのスキャン	はい	いいえ	はい
リムーバブルドライブのスキャン	はい	いいえ	はい

機能セット	Windows	Linux	macOS
ウイルスおよびマルウェア対策保護			
新規ファイルと変更ファイルのみスキャン	はい	いいえ	はい
ファイル/フォルダの除外	はい	はい	はい***
プロセスの除外	はい	いいえ	はい
挙動分析エンジン	はい	いいえ	はい
エクスプロイト防御	はい	いいえ	いいえ
検疫	はい	はい	はい
検疫自動クリーンアップ	はい	はい	はい
URLフィルタ処理（http/https）	はい	いいえ	いいえ
全社レベルのホワイトリスト	はい	いいえ	はい
ファイアウォール管理****	はい	いいえ	いいえ
Microsoft Defender Antivirus管理*****	はい	いいえ	いいえ
Microsoft Security Essentials管理	はい	いいえ	いいえ
Windows Security Centerでのウイルスおよびマルウェア対策保護の登録と管理	はい	いいえ	いいえ
サポート対象のオペレーティングシステムとバージョンの詳細については、"サポートされるプラットフォーム"（796ページ）を参照してください。			

* ポータブル実行可能ファイルの静的分析は、macOSでのスケジュールされたスキャンでのみサポートされています。

** 開始条件は、Linuxのオンデマンドスキャンではサポートされていません。

*** ファイル/フォルダ除外は、macOSでのリアルタイム保護またはスケジュールスキャンによるスキャンを行わないファイルとフォルダを指定する場合にのみサポートされます。

****Windows 8以降でファイアウォールの管理がサポートされています。Windows Serverはサポート対象ではありません。

*****Microsoft Defender Antivirusの管理はWindows 8.1以降でサポートされています。

機能セット	Windows	Linux	macOS
Active Protection			
プロセスインジェクト検出	はい	いいえ	いいえ
影響を受けたファイルのローカルキャッシュからの自動復元	はい	はい	はい
Acronisバックアップファイルの自己防御	はい	いいえ	いいえ
Acronisソフトウェアの自己防御	はい	いいえ	はい (Active Protectionおよびマルウェア対策コンポーネントのみ)
信頼できる/ブロックされているプロセスの管理	はい	いいえ	はい
プロセス/フォルダの除外	はい	はい	はい
プロセスの動作に基づくランサムウェア検出（AIベース）	はい	はい	はい
プロセスの動作に基づくクリプトマイニングプロセス検出	はい	いいえ	いいえ
外付けドライブ保護（HDD、フラッシュドライブ、SDカード）	はい	いいえ	はい
ネットワークフォルダの保護	はい	はい	はい
サーバー側保護機能	はい	いいえ	いいえ
Zoom、Cisco WebEx、Citrix Workspace、Microsoft Teamsの保護	はい	いいえ	いいえ
サポート対象のオペレーティングシステムとバージョンの詳細については、"サポートされるプラットフォーム"（796ページ）を参照してください。			

ウイルスおよびマルウェア対策保護

注意
適用されるライセンスモデルによっては、一部の機能で追加のライセンスが必要になる場合があります。

ウイルスおよびマルウェア対策モジュールは、あらゆる最新のマルウェアの脅威からWindows、Linux、およびmacOSマシンを保護します。 サポート対象のマルウェア対策機能の一覧（"サポートされるプラットフォーム"（796ページ））を参照してください。

ウイルスおよびマルウェア対策保護は、Windows Security Centerでサポートされており、そこに登録されます。

マルウェア対策機能

- リアルタイム保護モードとオンデマンドモードでファイルのマルウェアを検出
- プロセスで有害な動作を検出する機能（Windows）
- 有害なURLへのアクセスをブロックする機能（Windows）
- 危険なファイルを検疫する機能
- 社内の信頼できるアプリケーションを許可リストに追加する機能

スキャンの種類

ウイルス対策およびマルウェア対策保護を構成して、バックグラウンドまたはオンデマンドで常に実行することができます。

リアルタイム保護

注意
この機能を利用できるかどうかは、現在のアカウントで有効になっているサービスクォータによって異なります。

リアルタイム保護では、マルウェアの脅威を防止するために、マシンで実行されるファイルや開かれるファイルをすべてチェックします。

互換性およびパフォーマンスの問題が生じるのを回避するため、リアルタイム保護を他のリアルタイム保護を使用するウイルス対策ソリューションと同時に運用することはできません。インストール済みの他のウイルス対策ソリューションのステータスは、Windows Security Centerにより判定されます。Windowsマシンがすでに別のウイルス対策ソリューションで保護されている場合、リアルタイム保護は自動的にオフにされます。

リアルタイム保護を有効化するには、他のウイルス対策ソリューションを無効化するかアンインストールしてください。リアルタイム保護とMicrosoft Defenderリアルタイム保護を自動的に置き換えることができます。

注意
Windows Serverオペレーティングシステムを実行しているマシンの場合、リアルタイム保護が有効になっていると、Microsoft Defenderが自動的にオフになることはありません。管理者は、潜在的な互換性の問題を回避するために、Microsoft Defenderを手動でオフにする必要があります。

次のスキャンモードのいずれかを選択できます。

- **スマートオンアクセス**検出では、マルウェアからの保護のプログラムをバックグラウンドで実行し、マシンシステムの電源がオンになっている間、システムにウイルスや他の有害な脅威がないかどうかを常時アクティブな状態でチェックします。ファイルが実行されているときと、ファイルを開く、読み取る、編集するといったさまざまなファイル操作を行っているときの両方で、マルウェアが検出されます。
- **実行時**検出では、実行時にのみ実行ファイルがスキャンされ、ファイルが感染しておらず、マシンやデータに被害を及ぼさないことを保証します。感染したファイルのコピーは検出されません。

スケジュールスキャン

マルウェア対策スキャンは、スケジュールに基づいて実行されます。

次のスキャンモードのいずれかを選択できます。

- **クイックスキャン** - ワークロードのシステムファイルのみを確認します。
- **フルスキャン** - ワークロード上のすべてのファイルを確認します。
- **カスタムスキャン** - 管理者が保護計画に追加したファイル/フォルダを確認します。

マルウェア対策スキャンが完了すると、**[監視]** > **[概要]** > [最近影響を受けたもの] ウィジェットで、脅威の影響を受けたワークロードの詳細を確認できます。

ウイルスおよびマルウェア対策保護の設定

このセクションでは、保護計画の**ウイルスおよびマルウェア対策保護**モジュールで構成できる機能について説明します。保護計画を作成する方法については、"保護計画の作成"（209ページ）を参照してください。

保護計画のウイルスおよびマルウェア対策保護モジュールでは、以下の機能を構成できます。

- "Active Protection"（802ページ）
- "高度なマルウェア対策機能"（802ページ）
- "ネットワークフォルダの保護"（803ページ）
- "サーバー側保護機能"（803ページ）
- "自己防御"（804ページ）
- "クリプトマイニングプロセス検出"（805ページ）
- "検疫"（806ページ）
- "振る舞い検知エンジン"（806ページ）
- "エクスプロイト防御"（807ページ）
- "リアルタイム保護"（809ページ）
- "スケジュールスキャン"（810ページ）
- "保護除外"（813ページ）

注意
すべてのオペレーティングシステムがウイルスおよびマルウェア対策保護の機能をサポートしているわけではありません。サポートされるオペレーティング システムと機能の詳細については、"サポートされるプラットフォーム"（796ページ） を参照してください。一部の機能は、保護計画で使用するために特定のライセンスが必要です。

Active Protection

Active Protectionはランサムウェアという悪意あるソフトウェアからシステムを守ります。ランサムウェアはファイルを暗号化し、暗号化キーに対する身の代金を要求します。

既定の設定:**有効**。

注意
保護されているマシンには、プロテクションエージェントがインストールされている必要があります。サポート対象のオペレーティングシステムと機能の詳細については、"サポートされるプラットフォーム"（796ページ）を参照してください。

Active Protectionを構成するには

1. **保護計画の作成**ウィンドウで、**ウイルス対策とマルウェア対策保護**モジュールを展開します。
2. **[Active Protection]** をクリックします。
3. **[検出時のアクション]** セクションで、利用可能なオプションのいずれかを選択します:
   既定の設定:**[キャッシュを使用して元に戻す]**
   - **通知のみ** - ソフトウェアによりランサムウェアによるアクティビティの疑いがあるプロセスに関するアラートが生成されます。
   - **プロセスを停止** - ソフトウェアによりアラートが生成され、ランサムウェアによるアクティビティの疑いがあるプロセスが停止されます。
   - **キャッシュを使用して元に戻す** - ソフトウェアによりアラートが生成され、プロセスが停止し、サービスキャッシュを使用してファイルの変更を元に戻します。
4. 選択したオプションを保護計画に適用するには、**[完了]** をクリックします。

高度なマルウェア対策機能

このエンジンは、ウイルスシグネチャの拡張データベースを使用して、クイックスキャンとフルスキャンの両方でマルウェア対策検出の効率を向上させます。

重要
この機能は、Advanced Security保護パックが有効になっている場合にのみ使用できます。詳細については、https://www.acronis.com/en-us/products/cloud/cyber-protect/security/を参照してください

注意
この機能を利用できるかどうかは、現在のアカウントで有効になっているサービスクォータによって異なります。

高度なマルウェア対策機能を構成するには

1. **保護計画の作成**ウィンドウで、**ウイルス対策とマルウェア対策保護**モジュールを展開します。
2. **[高度なマルウェア対策機能]** セクションで、トグルを使用してローカルシグネチャベースのエンジンを有効にします。

注意
macOSおよびLinuxのウイルスおよびマルウェア対策保護には、ローカル署名ベースのエンジンも必要になります。Windowsのウイルスおよびマルウェア対策保護は、このエンジンの有無にかかわらず利用できます。

ネットワークフォルダの保護

ネットワークフォルダの保護機能は、ウイルス対策およびマルウェア対策保護が、ローカルドライブとしてマッピングされているネットワークフォルダを保護するかどうかを定義します。この保護は、SMBまたはNFSプロトコルを使用して共有されているフォルダに適用されます。

ネットワークフォルダの保護を構成するには

1. **保護計画の作成**ウィンドウで、**ウイルス対策とマルウェア対策保護**モジュールを展開します。
2. **[ネットワークフォルダの保護]** をクリックします。
3. ネットワークフォルダをバックアップする場所のファイルを追加します:
   - 例えば、ワークロードがWindowsの場合、**Windows**フィールドに、ネットワークフォルダをバックアップする場所のWindowsファイルのパスを入力します。デフォルト値: C:¥ProgramData¥Acronis¥Restored Network Files。
   - 例えば、ワークロードがmacOSの場合、**macOS**フィールドに、ネットワークフォルダをバックアップする場所のmacOSファイルのパスを入力します。デフォルト値: /Library/Application Support/Acronis/Restored Network Files/。

   注意
   ローカルフォルダのパスを入力します。マッピングされているドライブを含むネットワークフォルダは、バックアップ先としてサポートされていません。
4. 選択したオプションを保護計画に適用するには、**[完了]** をクリックします。

サーバー側保護機能

この機能では、Active Protectionが、脅威を持ち込む可能性のあるネットワーク内の他のサーバーの外部受信接続から、ユーザーが共有しているネットワークフォルダを保護するかどうかを定義します。

既定の設定:**オフ**。

注意
サーバーサイド防御機能はLinuxではサポートされていません。

信頼済み接続を設定するには

1. **保護計画の作成**ウィンドウで、**ウイルス対策とマルウェア対策保護**モジュールを展開します。
2. **[サーバー側の保護]** をクリックします。
3. **[サーバー側の保護]** のトグルを使用して有効にします。
4. **[信頼できる]** タブを選択します。
5. **[信頼済み接続]** フィールドで、**[追加]** をクリックして、データの変更を許可する接続を定義します。
6. **コンピューター名/アカウント**フィールドに、プロテクションエージェントがインストールされているマシンのコンピューター名とアカウントを入力します。たとえば、`MyComputer\TestUser`のように指定します。
7. **[ホスト名]** フィールドに、プロテクションエージェントを使用してマシンへの接続を許可するマシンのホスト名を入力します。
8. 右側のチェックマークをクリックすると、接続定義が保存されます。
9. **[完了]** をクリックします。

ブロックされた接続を設定するには

1. **保護計画の作成**ウィンドウで、**ウイルス対策とマルウェア対策保護**モジュールを展開します。
2. **[サーバー側の保護]** をクリックします。
3. **[サーバー側の保護]** のトグルを使用して有効にします。
4. **[ブロックされています]** タブを選択します。
5. **ブロックする接続**フィールドで、**[追加]** をクリックして、データの変更を許可しない接続を定義します。
6. **コンピューター名/アカウント**フィールドに、プロテクションエージェントがインストールされているマシンのコンピューター名とアカウントを入力します。たとえば、`MyComputer\TestUser`のように指定します。
7. **[ホスト名]** フィールドに、プロテクションエージェントを使用してマシンへの接続を許可するマシンのホスト名を入力します。
8. 右側のチェックボックスを選択して、接続定義を保存します。
9. **[完了]** をクリックします。

自己防御

自己防御機能は、ソフトウェア自身のプロセス、レジストリ記録、実行ファイル、設定ファイル、およびローカルフォルダにあるバックアップへの不正な変更を防止します。

管理者は、**Active Protection**を有効化することなく、**自己防御機能**を有効化できます。

既定の設定:**オン**。

注意
自己防御機能はLinuxではサポートされていません。

自己防御機能を有効にするには

1. **保護計画の作成**ウィンドウで、**ウイルス対策とマルウェア対策保護**モジュールを展開します。
2. **[自己防御機能]** をクリックします。
3. **[自己防御機能]** トグルを使用して有効にします。

パスワードによる保護を有効にする手順

1. **自己防御機能**を有効にすると、トグルを使用して**パスワードによる保護**機能を有効にできます。
2. ローカルエージェントを変更または削除するためのパスワードを生成するには、**[新しいパスワードを生成]** をクリックします。
3. ローカルでコンポーネントリストを変更する際にパスワードが要求されるため、**[コピー]** をクリックし、安全なロケーションに貼り付けます。

   重要
   このパスワードは、ウィンドウを閉じた後は使用できません。デバイスにこのパスワードを適用するには、保護計画の設定が保存されている必要があります。

4. **[閉じる]** をクリックします。

パスワードによる保護では、権限のないユーザーまたはソフトウェアによるWindowsエージェントのアンインストールまたはコンポーネントの変更が防止されます。これらのアクションは、管理者が提供するパスワードによってのみ実行可能です。

次のアクションでは、パスワードは必要ありません。

- プログラムの設定をローカルで実行してインストールを更新する
- Cyber Protectコンソールを使用してインストールをアップデートする
- インストールを修復する

既定の設定:**無効**

パスワードによる保護を有効にする方法の詳細については、「エージェントの不正なインストール解除または変更の防止」を参照してください。

クリプトマイニングプロセス検出

クリプトマイニングマルウェアは、有用なアプリケーションのパフォーマンスを低下させ、電気代を増加させ、システムクラッシュの要因となる可能性があり、酷使によるハードウェアダメージをも引き起こしかねません。**クリプトマイニングプロセス検出**機能により、クリプトマイニングマルウェアからデバイスを保護して、コンピューターリソースの不正使用を防ぎます。

管理者は、**Active Protection**を有効化することなく、**クリプトマイニングプロセス検出**を有効化できます。デフォルトの設定:**有効**。

注意
クリプトマイニングプロセス検知はLinuxではサポートされていません。

ネットワークフォルダの保護を構成するには

1. **保護計画の作成**ウィンドウで、**ウイルス対策とマルウェア対策保護**モジュールを展開します。
2. **[クリプトマイニングプロセスを検出]** をクリックします。
3. **[クリプトマイニングプロセスを検出]** のトグルを使用して、この機能を有効または無効にします。
4. クリプトマイニングの疑いがあるプロセスに対して実行する処理を選択します:
   既定の設定:**[プロセスの停止]**
   - **通知のみ** - ソフトウェアによりアラートが生成されます。
   - **プロセスを停止する** - ソフトウェアによりアラートが生成され、プロセスが停止されます。
5. 選択したオプションを保護計画に適用するには、**[完了]** をクリックします。

検疫

検疫フォルダは、疑わしい（感染の可能性がある）ファイルや危険が潜んでいるファイルを隔離するためのフォルダです。

検疫を構成するには

1. **保護計画の作成**ウィンドウで、**ウイルス対策とマルウェア対策保護**モジュールを展開します。
2. **[検疫]** をクリックします。
3. **検疫されたファイルを削除するまでの時間**フィールドで、検疫されたファイルを削除するまでの日数を定義します。
   既定の設定:**30日**
4. **[完了]** をクリックします。

この機能の詳細については、「検疫」を参照してください。

振る舞い検知エンジン

振る舞い検知エンジン機能は、振る舞いの分析にヒューリスティックを使用することで悪意のあるプロセスを特定し、システムをマルウェアから保護します。

既定の設定:**有効**。

注意
振る舞い検知エンジンは、Linuxをサポートしていません。

ネットワークフォルダの保護を構成するには

1. **保護計画の作成**ウィンドウで、**ウイルス対策とマルウェア対策保護**モジュールを展開します。
2. **[振る舞い検知エンジン]** をクリックします。
3. **[振る舞い検知エンジン]** のトグルを使用して、機能を有効または無効にします。
4. **[検出時のアクション]** セクションで、ソフトウェアがマルウェアのアクティビティを検出したときに実行する操作を選択します。
   既定の設定:**検疫**
   - **通知のみ** - ソフトウェアによりマルウェアによるアクティビティの疑いがあるプロセスに関するアラートが生成されます。

- **プロセスを停止** - ソフトウェアによりアラートが生成され、マルウェアによるアクティビティの疑いがあるプロセスが停止されます。
- **検疫** - ソフトウェアによりアラートが生成され、プロセスが停止し、実行ファイルが検疫フォルダに移されます。

5. 選択したオプションを保護計画に適用するには、**[完了]** をクリックします。

エクスプロイト防御

重要
この機能は、Advanced Security保護パックが有効になっている場合にのみ使用できます。詳細については、https://www.acronis.com/en-us/products/cloud/cyber-protect/security/を参照してください

注意
この機能を利用できるかどうかは、現在のアカウントで有効になっているサービスクォータによって異なります。

エクスプロイト防御は、感染したプロセスの拡散およびシステム上のソフトウェアの脆弱性が悪用されることを検出および防止します。エクスプロイトが検出されると、エクスプロイトによるアクティビティが疑われるプロセスについてのアラートが生成され、プロセスが停止する場合があります。

エクスプロイト保護は、エージェントバージョン12.5.23130（21.08、2020年8月リリース）以降でのみ利用可能です。

既定の設定:新しく作成された保護計画については**有効**になっています。以前のバージョンのエージェントで作成された既存の保護計画については**無効**になっています。

注意
エクスプロイト防御はLinuxではサポートされていません。

エクスプロイトが検出されたときのプログラムによる処置、およびプログラムによって適用されるエクスプロイト防御措置を選択できます。

エクスプロイト防御を構成するには

1. **保護計画の作成**ウィンドウで、**ウイルス対策とマルウェア対策保護**モジュールを展開します。
2. **[エクスプロイト防御]** をクリックします。
3. **[検出時のアクション]** セクションで、利用可能なオプションのいずれかを選択します:
   既定の設定:**[プロセスの停止]**

   - **通知のみ**
     ソフトウェアにより、エクスプロイトによるアクティビティの疑いがあるプロセスに関するアラートが生成されます。
   - **[プロセスの停止]**
     ソフトウェアにより、エクスプロイトによるアクティビティが疑われるプロセスについてアラートが生成され、プロセスが停止されます。

4. **[有効なエクスプロイト防御技術]** セクションで、利用可能なオプションから適用する技術を選択します：

   既定の設定:**すべてのメソッドが有効**

   - **メモリ保護**

     メモリページの実行権限に対する疑わしい変更を検出して防ぎます。疑わしいプロセスにより、ページプロパティに対してそのような変更が適用されると、スタックやヒープなどの通常は実行可能でないメモリ領域からShellコードを実行することが可能になります。
   - **リターン指向プログラミング（ROP）保護**

     ROP（Return-Oriented Programming）エクスプロイト技術を使用する試みを検出および防止します。
   - **権限昇格保護**

     認証されていないコードやアプリケーションによる権限昇格を検出して防ぎます。権限昇格は、悪意のあるコードで攻撃対象マシンのフルアクセス権限を取得し、重要事項や機密情報に関するタスクを実行するために使用されます。認証を受けていないコードに対しては、重要なシステムリソースへのアクセスやシステム設定の変更は許可されません。
   - **コードインジェクション保護**

     リモートプロセスへの悪意のあるコードインジェクションを検出して防ぎます。コードインジェクションは、アプリケーションの悪意のある動作を正常なプロセスや安全とされるプロセスに隠蔽し、アンチマルウェア製品による検出を回避するために使用されます。
5. 選択したオプションを保護計画に適用するには、**[完了]** をクリックします。

注意
除外リストで信頼済みプロセスとして列挙されているプロセスについては、エクスプロイトのスキャンは実行されません。

プロセスがバックアップを変更することを許可する

[特定のプロセスにバックアップの変更を許可] 設定は、**自己防御機能**の設定が有効になっている場合に限り利用可能です。

拡張子が.tibx、.tib、.tiaで、ローカルフォルダにあるファイルに適用されます。

この設定では、バックアップファイルが自己防御機能で保護されていても変更できるプロセスを指定できます。この機能は、スクリプトを使用してバックアップファイルを削除する場合や、バックアップを別のロケーションに移動する場合に便利です。

この設定が無効になっている場合、バックアップファイルは、バックアップソフトウェアベンダーが署名したプロセスによってのみ変更できます。その結果、Webインターフェースからユーザーがリクエストしたときに、保持ルールが適用され、バックアップが削除されます。他のプロセスは、不審かどうかにかかわらず、バックアップを変更できません。

この設定が有効になっている場合、他のプロセスでバックアップを変更できます。実行可能なプロセスのフルパスを、ドライブ文字を先頭にして指定します。

既定の設定:**無効**。

リアルタイム保護

注意
この機能を利用できるかどうかは、現在のアカウントで有効になっているサービスクォータによって異なります。

リアルタイム保護は、コンピューターシステムの電源がオンになっている間、コンピューターのユーザーが一時停止させた場合を除き、常時システムにウイルスや他の悪意ある脅威がないかどうかをチェックします。

既定の設定:**有効**。

重要
この機能は、Advanced Security保護パックが有効になっている場合にのみ使用できます。詳細については、https://www.acronis.com/en-us/products/cloud/cyber-protect/security/を参照してください

リアルタイム保護を構成するには

1. **保護計画の作成**ウィンドウで、**ウイルス対策とマルウェア対策保護**モジュールを展開します。
2. **[リアルタイム保護]** をクリックします。
3. **[検出時のアクション]** ドロップダウンで、使用可能なオプションのいずれかを選択します:
   既定の設定:**検疫**
   - **通知のみ**
     ソフトウェアにより、ランサムウェアによるアクティビティの疑いがあるプロセスに関するアラートが生成されます。
   - **ブロックと通知**
     マルウェアのアクティビティが疑われるプロセスがブロックされ、そのプロセスについてのアラートが生成されます。
   - **検疫**
4. アラートが生成され、プロセスが停止し、実行可能ファイルが検疫フォルダに移されます。
5. **[スキャンモード]** セクションで、ウイルスまたは他の悪意のある脅威を検出したときに実行されるアクションを選択します。
   既定の設定:**スマートオンアクセス**
   - **スマートオンアクセス** - すべてのシステムアクティビティを監視し、ファイルへの読み取りまたは書き込みアクセスがあったときや、プログラムが起動したときに、自動的にファイルをスキャンします。
   - **実行時** - 実行可能ファイルの起動時に自動的に実行ファイルだけをスキャンし、そのファイルがクリーンな状態で、コンピューターやデータに損傷を与えないことを確認します。
6. **[完了]** をクリックします。

スケジュールスキャン

オンデマンドスキャンでは、指定したスケジュールに従って、コンピューターシステムのウイルスが確認されます。完全スキャンではマシン上のすべてのファイルを確認し、クイックスキャンではマシンのシステムファイルだけを確認します。

スケジュールスキャンを構成するには

デフォルトの設定:

- **カスタムスキャン**は無効化されています。
- **クイック**スキャンと**フル**スキャンのスケジュールが設定されています。

1. **保護計画の作成**ウィンドウで、**ウイルス対策とマルウェア対策保護**モジュールを展開します。
2. [**スキャンをスケジュール**] をクリックします。
3. トグルを使用して、マシンに適用するスキャンのタイプを有効にします。

利用可能なスキャンのタイプ:

- **フル** - すべてのファイルをチェックするのでクイックスキャンよりもかなり時間がかかります。
- **クイック** - 通常マルウェアが存在する、マシンの一般的な領域のみをスキャンします。
- **カスタム** - 保護計画の管理者が選択したファイル/フォルダをチェックします。

> **注意**
> 1つの保護計画で、3種類のスキャン処理（**クイック**、**フル**、**カスタム**）のスケジュールを設定できます。

カスタムスキャンを構成するには

- [**カスタムスキャン**] **トグル**を使用して、このタイプのスキャンを有効または無効にします。
- [**検出時のアクション**] ドロップダウンリストで、利用可能なオプションのいずれかを選択します:

既定の設定:**検疫**

検疫

アラートが生成され、実行可能ファイルが検疫フォルダに移されます。

通知のみ

マルウェアの疑いがあるプロセスについてのアラートが生成されます。

フィールド	説明
次のイベントを使ってタスクの実行スケジュールを設定します	この設定は、タスクがいつ実行されるかを定義します。 次の値を使用できます。 • **時刻でスケジュール** - これはデフォルト設定です。タスクは指定した時間に実行されます。 • **システムへのユーザーログイン時** - デフォルトでは、いずれかのユー

フィールド	説明
	ザーがログインするとタスクが開始されます。特定のユーザーアカウントのみがタスクをトリガーできるように、この設定を変更できます。 • **システムへのユーザーログオフ時** - デフォルトでは、いずれかのユーザーがログオフするとタスクが開始されます。特定のユーザーアカウントのみがタスクをトリガーできるように、この設定を変更できます。 **注意** このタスクは、システムのシャットダウン時には実行されません。シャットダウンとログオフは、スケジューリング構成における別個のイベントです。 • **システムの起動時** - オペレーティングシステムが起動するときにタスクが実行されます。 • **システムのシャットダウン時** - オペレーティングシステムがシャットダウンするときにタスクが実行されます。
スケジュールの種類	このフィールドは、**[次のイベントを使ってタスクの実行スケジュールを設定]** で **[時刻でスケジュール]** を選択した場合に表示されます。 次の値を使用できます。 • **月単位** - タスクを実行する該当月と、その月内の週または日を選択します。 • **日単位** - これはデフォルト設定です。タスクを実行する週中の日を選択しします。 • **時間単位** - タスクを実行する週中の日、繰り返しの回数、時間間隔を選択しします。
開始時刻	このフィールドは、**[次のイベントを使ってタスクの実行スケジュールを設定]** で **[時刻でスケジュール]** を選択した場合に表示されます。 タスクを実行する正確な時間を選択します。
日付範囲内に実行	このフィールドは、**[次のイベントを使ってタスクの実行スケジュールを設定]** で **[時刻でスケジュール]** を選択した場合に表示されます。 設定したスケジュールが有効な日付範囲を指定します。
ユーザーアカウントを指定し、そのアカウントがオペレーティングシステムにログインしたときにタスクを開始	このフィールドは、**[次のイベントを使ってタスクの実行スケジュールを設定]** で **[システムへのユーザーログイン時]** を選択した場合に表示されます。 次の値を使用できます。 • **任意のユーザー** - いずれかのユーザーがログインしたときにタスクを開始させたい場合は、このオプションを使用します。 • **次のユーザー** - 指定したユーザーアカウントのログインでタスクを開始させたい場合は、このオプションを使用します。

フィールド	説明
ユーザーアカウントを指定し、そのアカウントがオペレーティングシステムからログアウトしたときにタスクを開始	このフィールドは、[**次のイベントを使ってタスクの実行スケジュールを設定**] で [**システムへのユーザーログオフ時**] を選択した場合に表示されます。 次の値を使用できます。 • **任意のユーザー** - いずれかのユーザーがログアウトしたときにタスクを開始させたい場合は、このオプションを使用します。 • **次のユーザー** - 指定したユーザーアカウントのログアウトでタスクを開始させたい場合は、このオプションを使用します。
開始条件	すべての条件を定義して、同時に満たされたときにタスクを実行する条件を指定します。 マルウェア対策スキャンの開始条件は、**バックアップモジュール**の開始条件に類似しています。「開始条件」を参照してください。 以下のような追加の開始条件を定義できます。 • **時間枠内でタスク開始時間を分散する** - このオプションを使用すると、タスクを実行する時間枠を設定して、ネットワークのボトルネックを回避できます。遅延時間を、時間または分単位で指定できます。たとえばデフォルトの開始時間が10:00 AMで、遅延を60分とした場合、タスクは10:00 AMから11:00 AMの間に開始されます。 • **マシンの電源が入っていないため実行されなかったタスクを起動時に実行する** • **タスク実行中はスリープモードや休止モードに入らない** - このオプションは、Windowsを実行しているマシンに対してのみ有効です。 • **開始条件を満たさない場合でも、次の時間の経過後にタスクを実行** - 他の開始条件にかかわらずタスクが実行されるまでの時間を指定します。 **注意** 開始条件は、Linuxではサポートされていません。

- 新規作成および変更されたファイルのみをスキャンする場合は、[**新規ファイルと変更されたファイルのみスキャン**] チェックボックスをオンにします。

既定の設定:**有効**

- **完全スキャン**の**カスタムスキャン**に表示される2つの追加オプション:

1. **アーカイブファイルのスキャン**

   既定の設定:**有効**。

   再帰動作の最大深

   既定の設定:**16**

どのレベルまで埋め込みアーカイブをスキャンできますか。たとえば、MIME文書 > ZIPアーカイブ > Officeアーカイブ > 文書コンテンツのようになります。

最大サイズ

既定の設定:**100**

スキャンするアーカイブファイルの最大サイズ。

2. **リムーバブルドライブのスキャン**

既定の設定:**無効**

- **マッピングされた（遠隔）ネットワークドライブ**
- **USBストレージデバイス**（ペンドライブや外部ハードドライブなど）
- **CD/DVD**

注意
リムーバブルドライブのスキャンはLinuxではサポートされていません。

保護除外

保護除外により、信頼できるプログラムがランサムウェアやマルウェアとみなされた場合の誤検出を排除できます。保護除外リストに追加することで、信頼できる項目やブロックされたアイテムを定義できます。

信頼済み項目リストにファイル、プロセス、フォルダを追加して、システム内での安全性を示し、以後これらの項目が検出されるのを防ぐことができます。

ブロック項目リストでは、プロセスとハッシュを追加できます。このオプションにより、これらのプロセスがブロックされ、ワークロードが安全になることを保証します。

保護除外項目	ブロックされています	信頼できる
ハッシュ	ハッシュがブロックリストに追加されると、システムは提供されたハッシュに基づいてプロセスを停止します。 例えば、MD5ハッシュ 938c2cc0dcc05f2b68c4287040cfcf71を追加すると、このハッシュに関連するプロセスはブロックされます。	ハッシュが信頼済みリストに追加されると、システムは提供されたハッシュに基づいて、監視から除外しなければならないプロセスを識別します。 例えば、MD5ハッシュ 938c2cc0dcc05f2b68c4287040cfcf71を追加すると、このハッシュに関連するプロセスは信頼済みとなり、監視対象から除外されます。
プロセス	プロセスがブロックリストに追加されると、システムによりそれらのプロセスは監視対象として認識され、プロセスは常にブロックされます。	プロセスが信頼済みリストに追加されると、それらのプロセスはシステムによる監視から除外されます。

保護除外項目	ブロックされています	信頼できる
	例えば、パス C:¥Users¥user1¥application¥nppInstaller.exeをブロックリストに追加すると、この特定のプロセスがブロックされ、開こうとしても起動できなくなります。	**注意** Microsoftが署名したプロセスは常に信頼されます。 例えば、C:¥Users¥user1¥application¥nppInstaller.exeというパスを追加すると、この特定のプロセスは監視から除外され、ウイルス対策ソリューションはこのプロセスに干渉しなくなります。
ファイル/フォルダ		ファイルやフォルダが信頼済みリストに追加されると、それらのファイルやフォルダはシステムにより常に安全であるとみなされ、スキャン/監視の対象から除外されます。

常に信頼する項目を指定するには

1. 保護計画を開きます。
2. **ウイルスおよびマルウェア対策保護**モジュールを展開します。
3. **[除外]** オプションを選択します。
   保護除外ウィンドウが開きます。
4. **[信頼済みの項目]** セクションで、**[追加]** をクリックして、利用可能なオプションから選択します:
   - ファイル、フォルダ、またはプロセスを信頼するには、**[ファイル/フォルダ/プロセス]** オプションを選択します。**ファイル/フォルダ/プロセスを追加**ウィンドウが開きます。
     - **[ファイル/フォルダ/プロセス]** フィールドに、各プロセス、フォルダ、ファイルのパスを新しい行に入力します。**[説明]** セクションでは、信頼済み項目のリストで変更を認識できるように、短い説明を入力します。
     - **[ファイル/フォルダとして追加]** チェックボックスを選択してファイル/フォルダを信頼済みにします。
       フォルダ記述の例:D:¥folder¥、/home/Folder/folder2、F:¥
     - **[プロセスとして追加]** チェックボックスを選択してプロセスを信頼済みにします。選択されたプロセスは、監視対象から除外されます。

       注意
       実行可能なプロセスのフルパスを、ドライブ文字を先頭にして指定します。例:
       `C:\Windows\Temp\er76s7sdkh.exe`。

       注意
       ローカルネットワークのパスもサポートされています（例:
       ¥¥localhost¥folderpath¥file.exe）。

- **[ハッシュ]** オプションを選択して、MD5ハッシュを信頼済み項目のリストに追加します。**ハッシュを追加**ウィンドウが開きます。
  - ここで、MD5ハッシュを別の行に挿入して、信頼済みとして [保護除外] リストに含めることができます。Cyber Protectionは、これらのハッシュに基づき、MD5ハッシュで記述されたプロセスを監視対象から除外します。

既定の設定:デフォルトでは除外は定義されていません。

常にブロックする項目を指定するには

1. 保護計画を開きます。
2. **ウイルスおよびマルウェア対策保護**モジュールを展開します。
3. **[保護除外]** オプションを選択します。**保護除外**ウィンドウが開きます。

   [ブロック済みの項目] セクションで、**[追加]** をクリックして、利用可能なオプションから選択します。
   - プロセスをブロックするには、**[プロセス]** オプションを選択します。**プロセスを追加**ウィンドウが開きます。
     - 各プロセスのパスを**[プロセス]** フィールドの新しい行に入力します。**[説明]** フィールドでは、ブロック済み項目のリストで変更を認識できるように、短い説明を入力します。

     注意
     Active Protectionがマシン上で有効になっていると、これらのプロセスを開始できません。
   - ハッシュをブロックするには、**[ハッシュ]** オプションを選択します。**ハッシュを追加**ウィンドウが表示されます。
     - 各ハッシュのパスを**[ハッシュ]** フィールドの新しい行に入力します。**[説明]** フィールドでは、ブロック済み項目のリストで変更を認識できるように、短い説明を入力します。

既定の設定:デフォルトでは除外は定義されていません。

ワイルドカード

フォルダを指定する際は、ワイルドカード文字（*および?）を使用できます。アスタリスク（*）は、文字なし、または1文字以上の文字として解釈されます。クエスチョンマーク（?）は、厳密に1文字として解釈されます。環境変数（%AppData%など）は使用できません。

ワイルドカード（*）を使用して、除外リストにアイテムを追加できます。

- ワイルドカードは、記述の途中や最後の部分に使用できます。

記述に使用できるワイルドカードの例:

C:¥*.pdf

D:¥folders¥file.*

C:¥Users¥*¥AppData¥Roaming

- ワイルドカードを記述の先頭に使用することはできません。

記述に使用できないワイルドカードの例:

*.docx

*:¥folder¥

変数

変数を使用して、除外リストに項目を追加することもできます。ただし次のような制限があります。

- Windowsでは、システム変数のみがサポートされます。%USERNAME%、%APPDATA%などのユーザー固有の変数はサポートされていません。{username}を伴う変数はサポート対象外です。詳細については、https://ss64.com/nt/syntax-variables.htmlを参照してください。
- macOSでは、環境変数はサポートされていません。
- Linuxでは、環境変数はサポートされていません。

サポートされる形式の例:

- %WINDIR%¥Media
- %public%
- %CommonProgramFiles%¥Acronis¥

説明

[説明] フィールドを使用して、保護除外リストで追加した除外項目に関するメモを作成できます。メモを作成する際に推奨される内容をいくつか紹介します。

- 除外の理由と目的。
- ハッシュ除外の実際のファイル名。
- タイムスタンプ。

1つのエントリに複数の項目が追加されている場合、複数の項目に対して有効に動作するコメントは1つのみとなります。

Cyber Backup Standard EditionのActive Protection

Cyber Backup Standard Editionの場合、Active Protectionは保護計画の個別のモジュールです。そのため、デバイス別やデバイスグループ別に異なる内容を設定し、適用できます。

サイバープロテクションサービスの他のエディションの場合、Active Protectionは、保護計画の**ウイルスおよびマルウェア対策**モジュールの一部となります。

既定の設定:**有効**。

注意
保護されているマシンには、プロテクションエージェントがインストールされている必要があります。サポート対象のオペレーティングシステムと機能の詳細については、"サポートされるプラットフォーム"（796ページ）を参照してください。

仕組み

Active Protectionは、保護されているマシンで実行されているプロセスを監視します。サードパーティのプロセスがファイルの暗号化や暗号通貨の採掘をしようとすると、Active Protectionは、アラートを生成し、保護計画で指定されている追加のアクションを実行します。

加えて、Active Protectionは、バックアップソフトウェア自体のプロセス、レジストリレコード、実行可能ファイルと構成ファイル、およびローカルフォルダにあるバックアップへの不正な変更を防止します。

悪意のあるプロセスを特定するために、Active Protectionではビヘイビアヒューリスティック法を使用します。Active Protectionでは、プロセスによって実行された一連のアクションと、悪意のある振る舞いパターンのデータベースに記録された一連のイベントを比較します。この方法により、新たなマルウェアを典型的な振る舞いによって検知できます。

Cyber Backup StandardのActive Protection設定

Cyber Backup Standard Editionでは、次のActive Protection機能を構成できます。

- 検出時のアクション
- 自己防御機能
- ネットワークフォルダの保護
- サーバー側保護機能
- クリプトマイニングプロセス検出
- 除外

注意
Linux向けのActive Protectionでは、以下の設定をサポートしています。検出時のアクション、ネットワークフォルダの保護、除外。ネットワークフォルダ保護は常に有効な状態であり、構成することはできません。

検出時のアクション

[検出時のアクション] セクションで、利用可能なオプションのいずれかを選択します:

- **通知のみ**
  ソフトウェアにより、ランサムウェアによるアクティビティの疑いがあるプロセスに関するアラートが生成されます。
- **[プロセスの停止]**
  ソフトウェアにより、ランサムウェアのアクティビティの疑いがあるプロセスに関するアラートが生成され、プロセスが停止されます。
- **[キャッシュを使用して元に戻す]**
  アラートを生成し、プロセスを停止して、サービスキャッシュを使用してファイルの変更を元に戻します。

既定の設定:**キャッシュを使用して元に戻す**。

自己防御機能は、ソフトウェア自身のプロセス、レジストリ記録、実行ファイル、設定ファイル、およびローカルフォルダにあるバックアップへの不正な変更を防止します。

管理者は、**Active Protection**を有効化することなく、**自己防御機能**を有効化できます。

既定の設定:**オン**。

注意
自己防御機能はLinuxではサポートされていません。

自己防御機能を有効にするには

1. **保護計画の作成**ウィンドウで、**ウイルス対策とマルウェア対策保護**モジュールを展開します。
2. **[自己防御機能]** をクリックします。
3. **[自己防御機能]** トグルを使用して有効にします。

パスワードによる保護を有効にする手順

1. **自己防御機能**を有効にすると、トグルを使用して**パスワードによる保護**機能を有効にできます。
2. ローカルエージェントを変更または削除するためのパスワードを生成するには、**[新しいパスワードを生成]** をクリックします。
3. ローカルでコンポーネントリストを変更する際にパスワードが要求されるため、**[コピー]** をクリックし、安全なロケーションに貼り付けます。

   重要
   このパスワードは、ウィンドウを閉じた後は使用できません。デバイスにこのパスワードを適用するには、保護計画の設定が保存されている必要があります。

4. **[閉じる]** をクリックします。

パスワードによる保護では、権限のないユーザーまたはソフトウェアによるWindowsエージェントのアンインストールまたはコンポーネントの変更が防止されます。これらのアクションは、管理者が提供するパスワードによってのみ実行可能です。

次のアクションでは、パスワードは必要ありません。

- プログラムの設定をローカルで実行してインストールを更新する
- Cyber Protectコンソールを使用してインストールをアップデートする
- インストールを修復する

既定の設定:**無効**

パスワードによる保護を有効にする方法の詳細については、「エージェントの不正なインストール解除または変更の防止」を参照してください。

ネットワークフォルダの保護

[ローカルドライブとしてマッピングされているネットワークフォルダの保護] 設定では、Active Protectionによって、ローカルドライブとしてマッピングされているネットワークフォルダを有害なプ

ロセスから保護するかどうかを定義します。

この設定は、SMBまたはNFSプロトコル経由で共有されているフォルダに適用されます。

ファイルが当初、マップされたドライブにあった場合、**[キャッシュを使用して元に戻す]** アクションによりキャッシュから抽出されたときには、元のロケーションに保存することはできません。その代わりに、この設定で指定するフォルダに保存されます。 デフォルトのフォルダは、Windowsの場合は`C:\ProgramData\Acronis\Restored Network Files`、macOSの場合は`Library/Application Support/Acronis/Restored Network Files/`です。 このフォルダが存在しない場合は、作成されます。このパスを変更する場合は、ローカルフォルダを指定してください。マッピングされているドライブを含むネットワークフォルダは、サポートされていません。

既定の設定:**オン**。

この機能では、Active Protectionが、脅威を持ち込む可能性のあるネットワーク内の他のサーバーの外部受信接続から、ユーザーが共有しているネットワークフォルダを保護するかどうかを定義します。

既定の設定:**オフ**。

注意
サーバーサイド防御機能はLinuxではサポートされていません。

信頼済み接続を設定するには

1. **保護計画の作成**ウィンドウで、**ウイルス対策とマルウェア対策保護**モジュールを展開します。
2. **[サーバー側の保護]** をクリックします。
3. **[サーバー側の保護]** のトグルを使用して有効にします。
4. **[信頼できる]** タブを選択します。
5. **[信頼済み接続]** フィールドで、**[追加]** をクリックして、データの変更を許可する接続を定義します。
6. **コンピューター名/アカウント**フィールドに、プロテクションエージェントがインストールされているマシンのコンピューター名とアカウントを入力します。たとえば、`MyComputer\TestUser`のように指定します。
7. **[ホスト名]** フィールドに、プロテクションエージェントを使用してマシンへの接続を許可するマシンのホスト名を入力します。
8. 右側のチェックマークをクリックすると、接続定義が保存されます。
9. **[完了]** をクリックします。

ブロックされた接続を設定するには

1. **保護計画の作成**ウィンドウで、**ウイルス対策とマルウェア対策保護**モジュールを展開します。
2. **[サーバー側の保護]** をクリックします。
3. **[サーバー側の保護]** のトグルを使用して有効にします。
4. **[ブロックされています]** タブを選択します。
5. **ブロックする接続**フィールドで、**[追加]** をクリックして、データの変更を許可しない接続を定義します。

6. **コンピューター名/アカウント**フィールドに、プロテクションエージェントがインストールされているマシンのコンピューター名とアカウントを入力します。たとえば、`MyComputer\TestUser`のように指定します。
7. **[ホスト名]** フィールドに、プロテクションエージェントを使用してマシンへの接続を許可するマシンのホスト名を入力します。
8. 右側のチェックボックスを選択して、接続定義を保存します。
9. **[完了]** をクリックします。

クリプトマイニングマルウェアは、有用なアプリケーションのパフォーマンスを低下させ、電気代を増加させ、システムクラッシュの要因となる可能性があり、酷使によるハードウェアダメージをも引き起こしかねません。**クリプトマイニングプロセス検出**機能により、クリプトマイニングマルウェアからデバイスを保護して、コンピューターリソースの不正使用を防ぎます。

管理者は、**Active Protection**を有効化することなく、**クリプトマイニングプロセス検出**を有効化できます。デフォルトの設定:**有効**。

注意
クリプトマイニングプロセス検知はLinuxではサポートされていません。

ネットワークフォルダの保護を構成するには

1. **保護計画の作成**ウィンドウで、**ウイルス対策とマルウェア対策保護**モジュールを展開します。
2. **[クリプトマイニングプロセスを検出]** をクリックします。
3. **[クリプトマイニングプロセスを検出]** のトグルを使用して、この機能を有効または無効にします。
4. クリプトマイニングの疑いがあるプロセスに対して実行する処理を選択します:
   既定の設定:**[プロセスの停止]**
   - **通知のみ** - ソフトウェアによりアラートが生成されます。
   - **プロセスを停止する** - ソフトウェアによりアラートが生成され、プロセスが停止されます。
5. 選択したオプションを保護計画に適用するには、**[完了]** をクリックします。

保護除外により、信頼できるプログラムがランサムウェアやマルウェアとみなされた場合の誤検出を排除できます。保護除外リストに追加することで、信頼できる項目やブロックされたアイテムを定義できます。

信頼済み項目リストにファイル、プロセス、フォルダを追加して、システム内での安全性を示し、以後これらの項目が検出されるのを防ぐことができます。

ブロック項目リストでは、プロセスとハッシュを追加できます。このオプションにより、これらのプロセスがブロックされ、ワークロードが安全になることを保証します。

保護除外項目	ブロックされています	信頼できる
ハッシュ	ハッシュがブロックリストに追加されると、システムは提供されたハッシュに基づいてプロセスを停止します。 例えば、MD5ハッシュ938c2cc0dcc05f2b68c4287040cfcf71を追加すると、このハッシュに関連するプロセスはブロックされます。	ハッシュが信頼済みリストに追加されると、システムは提供されたハッシュに基づいて、監視から除外しなければならないプロセスを識別します。 例えば、MD5ハッシュ938c2cc0dcc05f2b68c4287040cfcf71を追加すると、このハッシュに関連するプロセスは信頼済みとなり、監視対象から除外されます。
プロセス	プロセスがブロックリストに追加されると、システムによりそれらのプロセスは監視対象として認識され、プロセスは常にブロックされます。 例えば、パスC:¥Users¥user1¥application¥nppInstaller.exeをブロックリストに追加すると、この特定のプロセスがブロックされ、開こうとしても起動できなくなります。	プロセスが信頼済みリストに追加されると、それらのプロセスはシステムによる監視から除外されます。 **注意** Microsoftが署名したプロセスは常に信頼されます。 例えば、C:¥Users¥user1¥application¥nppInstaller.exeというパスを追加すると、この特定のプロセスは監視から除外され、ウイルス対策ソリューションはこのプロセスに干渉しなくなります。
ファイル/フォルダ		ファイルやフォルダが信頼済みリストに追加されると、それらのファイルやフォルダはシステムにより常に安全であるとみなされ、スキャン/監視の対象から除外されます。

常に信頼する項目を指定するには

1. 保護計画を開きます。
2. **ウイルスおよびマルウェア対策保護**モジュールを展開します。
3. **[除外]** オプションを選択します。
   保護除外ウィンドウが開きます。
4. **[信頼済みの項目]** セクションで、**[追加]** をクリックして、利用可能なオプションから選択します:
   - ファイル、フォルダ、またはプロセスを信頼するには、**[ファイル/フォルダ/プロセス]** オプションを選択します。**ファイル/フォルダ/プロセスを追加**ウィンドウが開きます。
     - **[ファイル/フォルダ/プロセス]** フィールドに、各プロセス、フォルダ、ファイルのパスを新しい行に入力します。**[説明]** セクションでは、信頼済み項目のリストで変更を認識できるように、短い説明を入力します。

- **[ファイル/フォルダとして追加]** チェックボックスを選択してファイル/フォルダを信頼済みにします。
  フォルダ記述の例:D:¥folder¥、/home/Folder/folder2、F:¥
- **[プロセスとして追加]** チェックボックスを選択してプロセスを信頼済みにします。選択されたプロセスは、監視対象から除外されます。

  注意
  実行可能なプロセスのフルパスを、ドライブ文字を先頭にして指定します。例:
  `C:\Windows\Temp\er76s7sdkh.exe`。

  注意
  ローカルネットワークのパスもサポートされています（例:
  ¥¥localhost¥folderpath¥file.exe）。

- **[ハッシュ]** オプションを選択して、MD5ハッシュを信頼済み項目のリストに追加します。**ハッシュを追加**ウィンドウが開きます。
  - ここで、MD5ハッシュを別の行に挿入して、信頼済みとして [保護除外] リストに含めることができます。Cyber Protectionは、これらのハッシュに基づき、MD5ハッシュで記述されたプロセスを監視対象から除外します。

既定の設定:デフォルトでは除外は定義されていません。

常にブロックする項目を指定するには

1. 保護計画を開きます。
2. **ウイルスおよびマルウェア対策保護**モジュールを展開します。
3. **[保護除外]** オプションを選択します。**保護除外**ウィンドウが開きます。
   [ブロック済みの項目] セクションで、**[追加]** をクリックして、利用可能なオプションから選択します。
   - プロセスをブロックするには、**[プロセス]** オプションを選択します。**プロセスを追加**ウィンドウが開きます。
     - 各プロセスのパスを**[プロセス]** フィールドの新しい行に入力します。**[説明]** フィールドでは、ブロック済み項目のリストで変更を認識できるように、短い説明を入力します。

     注意
     Active Protectionがマシン上で有効になっていると、これらのプロセスを開始できません。

   - ハッシュをブロックするには、**[ハッシュ]** オプションを選択します。**ハッシュを追加**ウィンドウが表示されます。
     - 各ハッシュのパスを**[ハッシュ]** フィールドの新しい行に入力します。**[説明]** フィールドでは、ブロック済み項目のリストで変更を認識できるように、短い説明を入力します。

既定の設定:デフォルトでは除外は定義されていません。

ワイルドカード

フォルダを指定する際は、ワイルドカード文字（*および?）を使用できます。アスタリスク（*）は、文字なし、または1文字以上の文字として解釈されます。クエスチョンマーク（?）は、厳密に1文字として解釈されます。環境変数（%AppData%など）は使用できません。

ワイルドカード（*）を使用して、除外リストにアイテムを追加できます。

- ワイルドカードは、記述の途中や最後の部分に使用できます。

記述に使用できるワイルドカードの例:

C:¥*.pdf

D:¥folders¥file.*

C:¥Users¥*¥AppData¥Roaming

- ワイルドカードを記述の先頭に使用することはできません。

記述に使用できないワイルドカードの例:

*.docx

*:¥folder¥

変数

変数を使用して、除外リストに項目を追加することもできます。ただし次のような制限があります。

- Windowsでは、システム変数のみがサポートされます。%USERNAME%、%APPDATA%などのユーザー固有の変数はサポートされていません。{username}を伴う変数はサポート対象外です。詳細については、https://ss64.com/nt/syntax-variables.htmlを参照してください。
- macOSでは、環境変数はサポートされていません。
- Linuxでは、環境変数はサポートされていません。

サポートされる形式の例:

- %WINDIR%¥Media
- %public%
- %CommonProgramFiles%¥Acronis¥

説明

[説明] フィールドを使用して、保護除外リストで追加した除外項目に関するメモを作成できます。メモを作成する際に推奨される内容をいくつか紹介します。

- 除外の理由と目的。
- ハッシュ除外の実際のファイル名。
- タイムスタンプ。

1つのエントリに複数の項目が追加されている場合、複数の項目に対して有効に動作するコメントは1つのみとなります。

URLフィルタ処理

注意
この機能を利用できるかどうかは、現在のアカウントで有効になっているサービスクォータによって異なります。

マルウェアは、いわゆるドライブバイダウンロードという感染方法で有害なサイトや感染したサイトから送り込まれることが多くなっています。

URLフィルタ処理機能を使用すれば、インターネットからやってくるマルウェアやフィッシングなどの脅威からマシンを保護できます。有害なコンテンツが含まれている可能性のあるWebサイトへのユーザーアクセスをブロックすることで、組織を保護できます。

URLフィルタリングにより、外部の法令や社内のポリシーに準拠するようにWebの使用法を制御できます。関連するカテゴリに応じて、Webサイトへのアクセスを設定できます。URLフィルタリングは、現在44種類のWebサイトのカテゴリをサポートしており、それらに対するアクセスを管理できます。

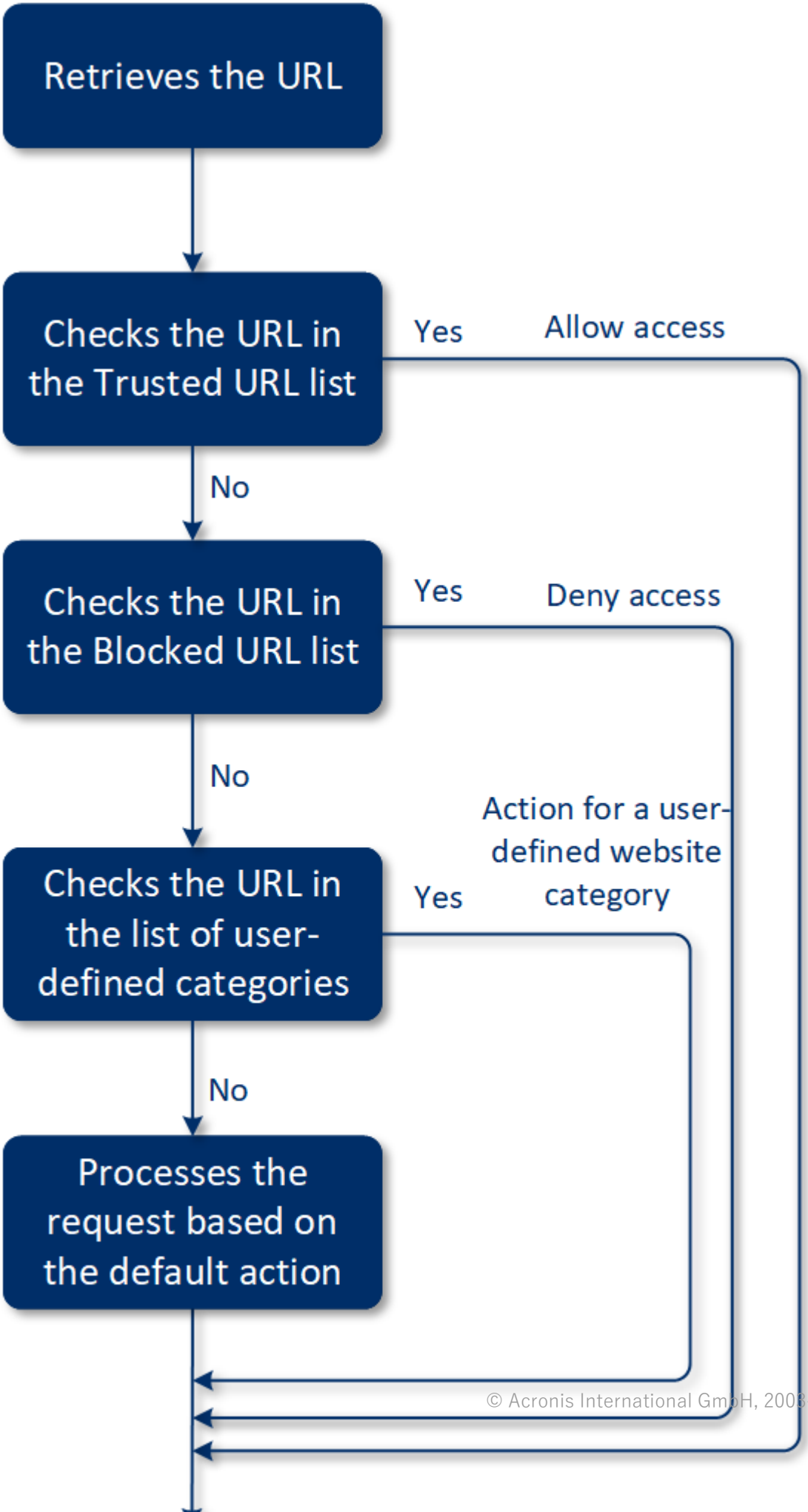
現時点では、WindowsマシンのHTTP/HTTPS接続が保護エージェントによってチェックされます。

URLフィルタリング機能を利用するには、インターネット接続が必要です。

注意
プロテクションエージェントビルド15.0.26692（リリースC21.03 HF1）以前との間で互換性の問題が発生するのを防止するため、別のウイルス対策ソリューションが検出された場合、またWindowsセキュリティセンターサービスがシステムに存在しない場合に、URLフィルタリング機能が自動的に無効になります。
それ以降のプロテクションエージェントでは、互換性の問題が解消されているため、ポリシーに従いURLフィルタリングが常に有効になります。

仕組み

ユーザーがブラウザにURLのリンクを入力します。インターセプターがリンクを取得して保護エージェントに送信します。エージェントがURLを取得し、解析して、判定をチェックします。ユーザーがリクエスト先のページに進むために手動で実行できるアクションについてのメッセージが記されたページに、インターセプターがユーザーをリダイレクトします。

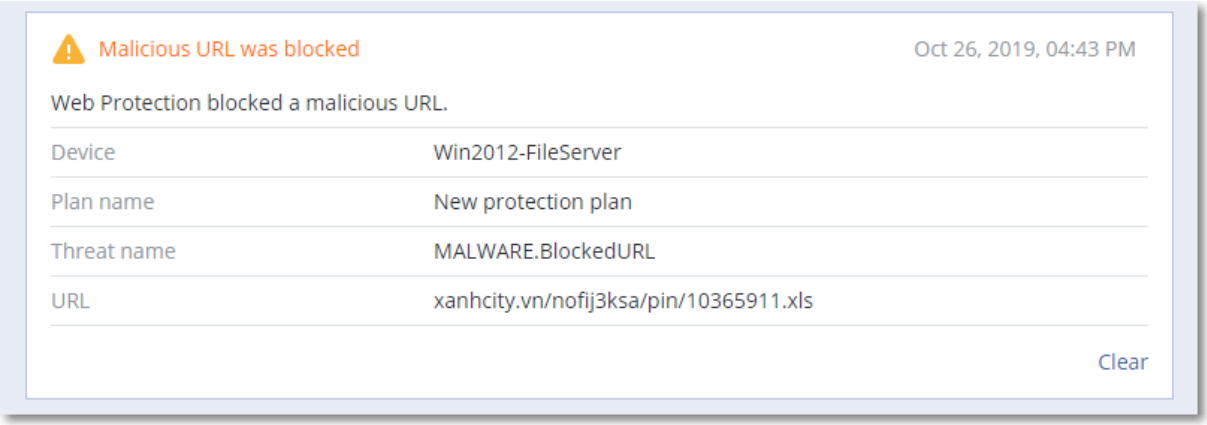


URLフィルタ処理の設定のワークフロー

通常、URLフィルタ処理の設定は、以下の流れで進んでいきます。

1. **URLフィルタ処理**モジュールを有効にした保護計画を作成します。
2. URLフィルタ処理の設定を指定します（以下を参照）。
3. 保護計画をマシンに割り当てます。

ブロックされたURLを確認するために、**[監視]** > **[アラート]** に進みます。



URLフィルタ処理の設定

URLフィルタ処理のモジュールでは、以下の設定を指定できます。

悪意あるWebサイトへのアクセス

ユーザーが有害なWebサイトを開いたときのアクションを指定します。

- **通知のみ**- ソフトウェアにより、ランサムウェアアクティビティの疑いのあるプロセスに関するアラートが生成されます。
- **ブロック** - 悪意のあるWebサイトへのアクセスをブロックします。ユーザーはWebサイトにアクセスできず、警告アラートが生成されます。
- **常にユーザーに確認** - そのWebサイトにアクセスするか、戻るかをユーザーに確認します。

フィルタリングするカテゴリ

44種類のWebサイトのカテゴリへのアクセスを次のように設定できます。

- **許可** - 選択したカテゴリに関連するWebサイトへのアクセスを許可します。
- **拒否** - 選択したカテゴリに関連するWebサイトへのアクセスを拒否します。

デフォルトでは、すべてのカテゴリが許可されています。

カテゴリでブロックされたURLに関するすべての通知を表示 - このオプションを有効にすると、カテゴリでブロックされたURLに関するすべての通知が表示されます。Webサイトに複数のサブドメインが存

在する場合、システムはそれらに対する通知も生成するので、通知が膨大な量になる可能性があります。

以下の表では、カテゴリについて説明します。

	Webサイトカテゴリ	説明
1	**広告**	このカテゴリには、広告の提供が主な目的である領域が該当します。
2	**メッセージボード**	このカテゴリには、フォーラム、ディスカッションボード、質疑応答形式の Web サイトが該当します。カスタマーが質問をする企業のWebサイトの特定のセクションは、このカテゴリに該当しません。
3	**個人のWebサイト**	このカテゴリには、個人の Web サイトのほかに、あらゆる種類のブログ（個人、グループ、会社のブログ）が該当します。ブログは、World Wide Webに公開されているジャーナル記事です。ブログはエントリ（「投稿」）から構成されており、一般的には、最新の投稿が最初に表示されるように新着順に表示されます。
4	**法人/企業のWebサイト**	これは、一般的に他のカテゴリに属さない企業 Web サイトが該当する幅広いカテゴリです。
5	**コンピューターソフトウェア**	このカテゴリには、一般的にオープンソース、フリーウェア、またはシェアウェアであるコンピューターソフトウェアを提供する Web サイトが該当します。このカテゴリには、一部のオンラインソフトウェアストアが該当する場合もあります。
6	**医薬品**	このカテゴリには、（合法的な）医薬品または麻薬器具、アルコール、タバコ製品の使用または販売に関するディスカッションを行う、医薬品/アルコール/タバコに関連する Web サイトが該当します。 非合法のドラッグは、薬物カテゴリに該当することにご注意ください。
7	**教育**	このカテゴリには、正式な教育機関（.edu ドメイン外の教育機関も含む）に属する Web サイトが該当します。このカテゴリには、百科事典などの教育系Webサイトも含まれます。
8	**エンターテイメント**	このカテゴリには、芸術活動や美術館に関連する情報を提供する Web サイト、および映画、音楽、芸術などのコンテンツをレビューまたは評価する Web サイトが該当します。
9	**ファイル共有**	このカテゴリには、ユーザーがファイルをアップロードして、他のユーザーと共有できる、ファイル共有Webサイトが該当します。また、このカテゴリには、torrent共有Webサイトや、torrentトラッカーも含まれます。
10	**ファイナンス**	このカテゴリには、オンラインアクセスを提供する世界中のすべての銀行に属するWebサイトが該当します。また、一部の信用組合やその他の金融機関も含まれます。ただし、一部の地方銀行は含まれない場合があります。
11	**ギャンブ**	このカテゴリには、ギャンブル関連のWebサイトが該当します。これらは、「オンライン

	ル	カジノ」または「オンライン宝くじ」タイプのWebサイトで、通常は、ユーザーが事前に支払いを行い、オンラインルーレット、ポーカー、ブラックジャック、または類似したゲームに金銭を賭けることができます。その中には、当選の可能性があるという意味で正当性のあるものもあれば、当選の可能性がないという意味で詐欺的なものもあります。また、ギャンブルやオンライン宝くじのWebサイトでお金を稼ぐ方法を説明する、「賭け方のコツと裏技」関連のWebサイトも検出します。
12	**ゲーム**	このカテゴリには、一般的にAdobe FlashまたはJavaアプレットに基づく、オンラインゲームを提供するWebサイトが該当します。無料であったり、サブスクリプション制であったりすることが検出に影響を及ぼすことはなく、カジノ形式のWebサイトはギャンブルカテゴリで検出されます。 以下のサイトはこのカテゴリに該当しません: • ビデオゲームを開発する（オンラインゲームを運営していない）企業のWebサイト • ゲームについて話し合われているディスカッション型Webサイト • オフラインゲームがダウンロードできるWebサイト（一部は非合法カテゴリに該当） • ユーザーが実行可能ファイルをダウンロードして実行しなければならないゲーム（World of Warcraftなど）。これらはファイアウォールによって別途に規制される可能性があります
13	**政府機関**	このカテゴリには、政府機関、大使館、政府事務所の Web サイトを含む政府機関の Web サイトが該当します。
14	**ハッキング**	このカテゴリには、ハッカー向けのハッキングツール、記事、ディスカッションプラットフォームを提供する Web サイトが該当します。また、FacebookやGmailアカウントのハッキングを促すといった、一般的なプラットフォームを不正利用する方法を扱うWebサイトも該当します。
15	**非合法な活動**	このカテゴリは、ヘイト、暴力、人種差別に関連する幅広いカテゴリで、次のようなカテゴリのWebサイトのブロックを前提としています。 • テロ組織に属するWebサイト • レイシストや外国人排斥に関連する内容のWebサイト • 攻撃的なスポーツについてディスカッションが行われたり、暴力を促進したりするWebサイト
16	**ヘルスケアおよびフィットネス**	このカテゴリには、医療機関に関連付けられたWebサイト、疾病予防および治療に関連するWebサイト、減量、食事、ステロイド、アナボリック、HGH製品に関連する情報や製品を提供するWebサイトが該当します。また美容整形の情報を提供するWebサイトも該当します。
17	**趣味**	このカテゴリには、収集、アートや工芸、サイクリングなど、一般的に個人の余暇に行われる活動に関連するリソースを提供する Web サイトが該当します。
18	**Webホスティング**	このカテゴリには、個人のユーザーや組織が Web ページを作成して公開できる、無料および商業用 Web サイトホスティングサービスが該当します。
19	**違法なダウンロー**	このカテゴリには、ソフトウェアの著作権侵害に関連するWebサイトが該当し、以下の種類のサイトを含みます。

	ド	• 著作権所有者の同意なく、著作権で保護されたコンテンツの頒布を促進すると認識されている、P2P（BitTorrent、emule、DC++）トラッカーWebサイト • Warez（不正な商用ソフトウェア）Webサイトおよび掲示板 • クラック、キージェネレーター、シリアルナンバーをユーザーに提供し、ソフトウェアの違法な使用を促進するWebサイト これらのWebサイトの一部は、収益のためにポルノやアルコールの広告を掲載していることが多いため、ポルノやアルコール/タバコのカテゴリとして検出されることもあります。
20	**インスタントメッセージ**	このカテゴリには、ユーザーがリアルタイムでチャットできるインスタントメッセージングとチャット Web サイトが該当します。また、コンテンツとしてインスタントメッセンジャーサービスが埋め込まれている、yahoo.comやgmail.comも検出対象となります。
21	**仕事/求人**	このカテゴリには、求人掲示板、求人広告、採用情報を提供する Web サイト、およびこのようなサービスのアグリゲーターが該当します。求人エージェントや通常の企業Webサイトの「求人」ページはこのカテゴリには該当しません。
22	**成人向けコンテンツ**	このカテゴリには、Webサイト作成者によって成人向けに制限されたコンテンツが該当します。このカテゴリには、カーマストラの書籍や性教育関連のWebサイトから、ハードコアポルノのWebサイトまで、広範なサイトが該当します。
23	**薬物**	このカテゴリには、快楽を得るための薬物や違法薬物に関する情報を共有する Web サイトが該当します。このカテゴリには、ドラッグの生成や栽培方法を扱うWebサイトも該当します。
24	**ニュース**	このカテゴリには、テキストおよび動画ニュースを提供するニュース Web サイトが該当します。このカテゴリでは、世界規模のニュースのWebサイトとローカルニュースのWebサイトの両方を網羅するように努めていますが、一部の小規模なローカルニュースのWebサイトは網羅されていない場合があります。
25	**出会い系**	このカテゴリには、ユーザーが何らかの条件を使用して他のユーザーを検索できるオンライン出会い系Webサイト（有料版および無料版）が該当します。利用者はプロフィールを投稿して、他の人から検索可能な状態にできます。このカテゴリには、無料版および有料版の出会い系Webサイトが含まれます。 広く利用されているソーシャルネットワークのほとんどは、オンラインの出会い系Webサイトとして利用可能なため、Facebookのような有名なWebサイトもこのカテゴリで検出されます。このカテゴリはソーシャルネットワークカテゴリとして使用することを推奨します。
26	**オンライン決済**	このカテゴリには、オンライン決済または送金を提供するWebサイトが該当します。PayPalやMoneybookersなど、広く利用されている決済向けのWebサイトが検出されます。また、クレジットカード情報を要求する通常のWebサイトのWebページをヒューリスティックに検出するため、見つけにくいオンラインストアや未知のオンラインストア、また違法なオンラインストアを検出することが可能です。
27	**画像共有**	このカテゴリには、ユーザーが画像をアップロードして共有できるようにすることが主な目的である画像共有 Web サイトが該当します。
28	**オンラインストア**	このカテゴリには、オンラインストアが該当します。商品やサービスをオンラインで販売しているWebサイトは、オンラインストアと見なされます。

29	**ポルノ**	このカテゴリには、性的なコンテンツおよびポルノを含む Web サイトが該当します。有料および無料のWebサイトをともに含みます。写真、ストーリー、ビデオを提供するWebサイトがこれに該当し、さらにコンテンツが混在するWebサイトのポルノコンテンツも検出されます。
30	**ポータル**	このカテゴリには、複数のソースやさまざまな分野からの情報を集約し、通常は検索エンジン、電子メール、ニュース、エンターテイメント情報などの機能を提供する Web サイトが該当します。
31	**ラジオ**	このカテゴリには、オンラインラジオステーションからオンデマンドオーディオコンテンツ（有料および無料）まで、インターネット音楽配信サービスを提供する Web サイトが該当します。
32	**宗教**	このカテゴリには、宗教または宗派を宣伝する Web サイトが該当します。さらに、単一の宗教または複数の宗教に関連したディスカッションフォーラムも該当します。
33	**検索エンジン**	このカテゴリには、Google、Yahoo、Bing などの検索エンジン Web サイトが該当します。
34	**ソーシャルネットワーク**	このカテゴリには、ソーシャルネットワークWebサイトが該当します。これには、MySpace.com、Facebook.com、Bebo.comなどが含まれます。ただし、YouTube.comのような特殊なソーシャルネットワークは、ビデオ/写真カテゴリに含められます。
35	**スポーツ**	このカテゴリには、スポーツ情報、ニュース、チュートリアルを提供する Web サイトが該当します。
36	**自殺**	このカテゴリには、自殺を推進、提供、主唱する Web サイトが該当します。自殺防止クリニックは、これに該当しません。
37	**タブロイド**	このカテゴリには、ソフトポルノや芸能人のゴシップ Web サイトが主に該当します。多くのタブロイド形式のニュースWebサイトは、ここに列挙したサブカテゴリを扱っている場合があります。このカテゴリの検出も、ヒューリスティックに行われます。
38	**時間の無駄**	このカテゴリには、個人がかなりの時間を費やす傾向があるWebサイトが該当します。これには、ソーシャルネットワークやエンターテイメントなど、他のカテゴリに該当するWebサイトも含まれます。
39	**旅行**	このカテゴリには、旅行サービス、旅行用品、旅行先のレビューや評価を提供する Web サイトが該当します。
40	**ビデオ**	このカテゴリには、ユーザーによるアップロードや、さまざまなコンテンツプロバイダーの提供により、さまざまな動画や写真がホストされるWebサイトが該当します。これには、YouTube、Metacafe、Google VideoなどのWebサイトや、PicasaやFlickrなどの写真関連のWebサイトが含まれます。これらは、ビデオが埋め込まれた他のWebサイトやブログとしても検出されます。
41	**暴力の描写があるアニメーション**	このカテゴリには、暴力、性的な言語、性的なコンテンツのため、未成年には不適切な場合がある暴力の描写がある漫画をディスカッション、共有、提供する Web サイトが該当します。 「トムとジェリー」といった主流のアニメーションを提供するWebサイトは、このカテゴリには該当しません。

42	**兵器**	このカテゴリには、販売、交換、製造、使用目的で兵器を提供する Web サイトが該当します。このカテゴリには、狩猟に関連する内容や、エアガン/BBガン、また凶器の使用に関連する内容も該当します。
43	**Eメール**	このカテゴリには、Eメール機能を Web アプリケーションとして提供する Web サイトが該当します。
44	**Webプロキシ**	このカテゴリには、Web プロキシを提供する Web サイトが該当します。これは、「ブラウザインブラウザ」形式のWebサイトで、ユーザーがWebページを開き、リクエストするURLをフォームに入力し、「送信」をクリックして利用するものです。Webプロキシサイトは、実際のページをダウンロードし、ユーザーのブラウザ内でそのページを表示します。 このタイプのサイトが検出される（場合によってはブロックが必要な）理由は以下のとおりです: • 匿名でブラウジングするため。宛先のWebサーバーへのリクエストはプロキシWebサーバーから行われるため、プロキシサーバーのIPアドレスについてのみ可視性があり、サーバー管理者がユーザーを追跡しても、Webプロキシまでしか追跡できません。また、プロキシサーバーが元のユーザーを特定するために必要なログを保持しているかどうかも断定できません。 • ロケーションを偽装するため。ユーザーのIPアドレスは、ソースのロケーションに応じてサービスをプロファイリングするためにしばしば利用されます（政府機関のWebサイトの中には、ローカルIPアドレスからしか利用できないものもあります）。プロキシサービスを利用することで、ユーザーが実際のロケーションを偽装できる場合があります。 • 制限されたコンテンツにアクセスするため。単純なURLフィルターを使用している場合、フィルターはWebプロキシのURLのみを確認し、ユーザーが実際に利用するサーバーを確認することがありません。 • 企業による監視を避けるため。企業ポリシーにより、従業員のインターネット利用状況の監視が求められている場合があります。すべてのアクセスにWebプロキシを介することで、ユーザーは正しい情報を提供せずに、監視から逃れることができる場合があります。 SDKはURLのみでなく、HTMLページ（提供されている場合）を分析します。このため一部のカテゴリでは、SDKによって内容を検出することができます。ただし、それ以外の理由がある場合、SDKの利用のみで回避することはできません。

URL除外

安全だと分かっているURLは、信頼できるドメインのリストに追加できます。脅威になるURLは、ブロックするドメインのリストに追加できます。

常に信頼するまたはブロックするURLを指定するには

1. 保護計画のURLフィルタリングモジュールで、**[URL除外]** をクリックします。
   URL除外ウィンドウが開きます。
   次のオプションが表示されます。

信頼済みの項目 - **[追加]** をクリックして、利用可能なオプションから選択します。

- **ドメイン** - このオプションを選択すると、[**ドメインを追加**] ウィンドウが開きます。
  - [**ドメイン**] フィールドの新しい行に各ドメインを入力します。[**説明**] フィールドでは、信頼済み項目のリストで変更を認識できるように、短い説明を入力します。
- **プロセス** - このオプションを選択すると、[**プロセスを追加**] ウィンドウが表示されます。
  - 各プロセスのパスを[**プロセス**] フィールドの新しい行に入力します。[**説明**] セクションでは、信頼済み項目のリストで変更を認識できるように、短い説明を入力します。

ブロック済み項目 - [**追加**] をクリックします。**ドメインを追加**ウィンドウが表示されます。

[**ドメイン**] フィールドの新しい行に各ドメインを入力します。[**説明**] フィールドでは、ブロック済み項目のリストで変更を認識できるように、短い説明を入力します。

注意
ローカルネットワークのパスもサポートされています。例: ¥¥localhost¥folderpath¥file.exe。

説明

[**説明**] フィールドを使用して、URL除外リストで追加した除外項目に関するメモを作成できます。メモを作成する際に推奨される情報をいくつか紹介します。

- 除外の理由と目的。
- タイムスタンプ。

1つのエントリに複数の項目が追加されている場合、複数の項目に対して有効に動作するコメントは1つのみとなります。

Microsoft Defender AntivirusおよびMicrosoft Security Essentials

注意
この機能を利用できるかどうかは、現在のアカウントで有効になっているサービスクォータによって異なります。

Windows Defender Antivirus

Microsoft Defender Antivirusは、Windows 8以降で提供されている、Microsoft Windowsの組み込みマルウェア対策コンポーネントです。

Microsoft Defender Antivirus（WDA）モジュールを使用すれば、Microsoft Defender Antivirusのセキュリティポリシーを設定して、Cyber Protectコンソールからステータスをトラックできます。

このモジュールを使用できるのは、Microsoft Defender Antivirusがインストールされているワークロードです。

Microsoft Security Essentials

Microsoft Security Essentialsは、Microsoft Windowsの組み込みマルウェア対策コンポーネントで、Windows 8より前のバージョンに用意されていました。

Microsoft Security Essentialsモジュールを使用すれば、Microsoft Security Essentialsのセキュリティポリシーを設定して、Cyber Protectコンソールからステータスをトラックできます。

このモジュールを使用できるのは、Microsoft Security Essentialsがインストールされているワークロードです。

Microsoft Security Essentialsの設定はMicrosoft Defender Antivirusの設定と類似していますが、リアルタイム保護を構成したり、Cyber Protectコンソールを介して除外を定義したりすることはできません。

スケジュールスキャン

スケジュールスキャンのスケジュールを指定します。

スキャンモード:

- **完全** - クイックスキャンの対象項目だけでなく、すべてのファイルとフォルダを完全にチェックします。実行に必要なマシンリソースがクイックスキャンの場合よりも多くなります。
- **クイック** - マルウェアが見つかりそうなインメモリプロセスとフォルダだけをチェックします。実行に必要なマシンリソースが少なくて済みます。

スキャンを実行する曜日と時刻を定義します。

毎日のクイックスキャン - 毎日のクイックスキャンの時刻を定義します。

必要に応じて以下のオプションも設定できます。

マシンがオンになっているが使用されていないときにスケジュール済みスキャンを開始

スケジュール済みスキャンの実行前にウイルスとスパイウェアの最新の定義を確認

スキャン中のCPU使用率を制限

Microsoft Defender Antivirusの設定の詳細については、https://docs.microsoft.com/en-us/sccm/protect/deploy-use/endpoint-antimalware-policies#scheduled-scans-settingsを参照してください

デフォルトのアクション

検出された脅威の重大度のレベルに応じてデフォルトのアクションを定義します。

- **クリーン** - ワークロードで検出されたマルウェアをクリーンアップします。
- **検疫** - 検出されたマルウェアを検疫フォルダに移しますが、削除はしません。
- **削除** - 検出されたマルウェアをワークロードから削除します。
- **許可** - 検出されたマルウェアを削除しないで、検疫にも移しません。

- **ユーザー定義** - 検出されたマルウェアに対して実行するアクションをユーザーが指定するための画面が表示されます。
- **アクションなし** - アクションを実行しません。
- **ブロック** - 検出されたマルウェアをブロックします。

Microsoft Defender Antivirusのデフォルトアクション設定の詳細については、https://docs.microsoft.com/en-us/sccm/protect/deploy-use/endpoint-antimalware-policies#default-actions-settingsを参照してください

リアルタイム保護

[リアルタイム保護] を有効にすると、マルウェアを検出して、マルウェアがワークロードでインストールされたり実行されたりするのを防止できます。

すべてのダウンロードのスキャン - 選択すると、ダウンロードしたすべてのファイルや添付ファイルがスキャンされます。

挙動監視の有効化 - 選択すると、挙動監視が有効になります。

ネットワークファイルのスキャン - 選択すると、ネットワークファイルがスキャンされます。

マッピング済みネットワークドライブの完全スキャンを許可 - 選択すると、マッピング済みのネットワークドライブの完全スキャンが実行されます。

電子メールのスキャンを許可 - 有効にすると、Eメールの形式に基づいてメールボックスとメールファイルが解析され、メールの本文と添付ファイルが分析されます。

Microsoft Defender Antivirusのリアルタイム保護設定の詳細については、https://docs.microsoft.com/en-us/sccm/protect/deploy-use/endpoint-antimalware-policies#real-time-protection-settingsを参照してください

詳細

スキャンの詳細設定を指定します。

- **アーカイブファイルのスキャン** - スキャンの対象としてアーカイブファイル（.zipや.rarなど）を含めます。
- **リムーバブルドライブのスキャン** - 完全スキャンの実行時にリムーバブルドライブをスキャンします。
- **システムのリストアポイントの作成** - 偽陽性の判定に基づいて重要なファイルやレジストリ項目が削除された場合に、リストアポイントからのリカバリが可能になります。
- **検疫されたファイルを削除するまでの時間** - 検疫されたファイルを削除するまでの期間を定義します。
- **詳細な分析が必要な場合、すべてのファイルサンプルを自動送信:**
  - **常に確認** - ファイル送信の前に常に確認が求められます。
  - **安全なサンプルを自動送信** - 個人情報が含まれている可能性のあるファイル以外のほとんどのサン

プルが自動的に送信されます。そのようなファイルについては、追加の確認操作が必要です。
  - **すべてのサンプルを自動送信** - すべてのサンプルが自動的に送信されます。
- **Windows Defender Antivirus GUIの無効化** - 選択すると、ユーザーがWDAユーザーインターフェイスを利用できなくなります。Cyber ProtectコンソールでWDAのポリシーを管理できます。
- **MAPS（Microsoft Active Protection Service）** - 潜在的な脅威に対応する方法を選択するのに役立つオンラインコミュニティ。
  - **MAPSに加入しない** - 検出されたソフトウェアについての情報がMicrosoftに送信されることはありません。
  - **Basicメンバーシップ** - 検出されたソフトウェアについての基本的な情報がMicrosoftに送信されます。
  - **Advancedメンバーシップ** - 検出されたソフトウェアについての詳細な情報がMicrosoftに送信されます。

  詳細については、https://www.microsoft.com/security/blog/2015/01/14/maps-in-the-cloud-how-can-it-help-your-enterprise/を参照してください

Microsoft Defender Antivirusの高度な設定の詳細については、https://docs.microsoft.com/en-us/sccm/protect/deploy-use/endpoint-antimalware-policies#advanced-settingsを参照してください

除外

スキャンから除外する以下のファイルやフォルダを定義できます。

- **プロセス** - 定義したプロセスの読み取り先/書き込み先のファイルがスキャンから除外されます。プロセスの実行可能ファイルのフルパスを定義する必要があります。
- **ファイルとフォルダ** - 指定したファイルとフォルダがスキャンから除外されます。フォルダやファイルのフルパスを定義するか、ファイル拡張子を定義する必要があります。

Microsoft Defender Antivirusの除外設定の詳細については、https://docs.microsoft.com/en-us/sccm/protect/deploy-use/endpoint-antimalware-policies#exclusion-settingsを参照してください

ファイアウォール管理

注意
この機能を利用できるかどうかは、現在のアカウントで有効になっているサービスクォータによって異なります。

ファイアウォール管理により、保護されたワークロードのファイアウォール設定を容易に行うことができます。

このCyber Protectの機能は、Microsoft Windowsに内蔵されているMicrosoft Defenderファイアウォールコンポーネントによって提供されています。Microsoft Defenderファイアウォールは、ワークロードとの間で送受信される不正なネットワークトラフィックをブロックします。

ファイアウォール管理は、Microsoft Defenderファイアウォールがインストールされているワークロードに適用されます。

サポートされるWindowsオペレーティングシステム

ファイアウォール管理では、以下のWindowsオペレーティングシステムがサポートされています。

Windows

- Windows 8
- Windows 8.1
- Windows 10
- Windows 11

Windows Serverはサポート対象ではありません。

ファイアウォール管理の有効化および無効化

保護計画を作成する際に、ファイアウォール管理を有効化できます。既存の保護計画を変更して、ファイアウォール管理を有効または無効にすることができます。

ファイアウォール管理を有効または無効にするには

1. Cyber Protectコンソールで **[デバイス]** > **[すべてのデバイス]** に進みます。
2. 以下のいずれかの手順を実行して、保護計画パネルを開きます。
   - 新しい保護計画を作成する場合は、保護されているマシンを選択して、**[保護]** をクリックしてから、**[計画の作成]** をクリックします。
   - 既存の保護計画を変更する場合は、保護されているマシンを選択して、**[保護]** をクリックしてから、保護計画の名前の横にある省略記号（...）をクリックします。その後、**[編集]** をクリックします。
3. 保護計画パネルで、**[ファイアウォール管理]** 領域に移動し、**[ファイアウォール管理]** を有効化または無効化します。
4. 次のいずれかの手順を実行します。
   - 保護計画を作成する場合は、**[作成]** をクリックします。
   - 保護計画を編集する場合は、**[保存]** をクリックします。

保護計画パネルの**ファイアウォール管理**領域における**Microsoft Defenderファイアウォール**のステータスは、ファイアウォール管理の有効/無効のステータスに応じて、**オン**または**オフ**と表示されます。

または、[管理] タブから保護計画パネルにアクセスすることもできます。ただし、この機能はCyber Protectionサービスのすべてのエディションで利用できるわけではありません。

検疫

検疫フォルダとは、マシンのハードディスクにある特殊な隔離フォルダのことで、ウイルスおよびマルウェア対策保護で検出された疑わしいファイルは、脅威の拡散を防ぐためこのフォルダに移されます。

検疫を実施すると、すべてのマシンで疑わしいファイルや危険がありそうなファイルを調べて、削除するか復元するかを決定できます。マシンをシステムから削除すると、検疫されたファイルも自動的に削除されます。

ファイルが検疫フォルダに移される仕組み

1. 保護計画を設定し、感染ファイルに対するデフォルトのアクションとして検疫を指定します。
2. スケジュールスキャンまたはオンアクセススキャンの実行時に有害なファイルが検出されると、そのファイルが安全なフォルダ（検疫フォルダ）に移されます。
3. システムでマシンの検疫リストが更新されます。
4. 保護計画の **[検疫されたファイルを削除するまでの時間]** 設定で定義されている期間が過ぎると、検疫フォルダからファイルが自動的にクリーンアップされます。

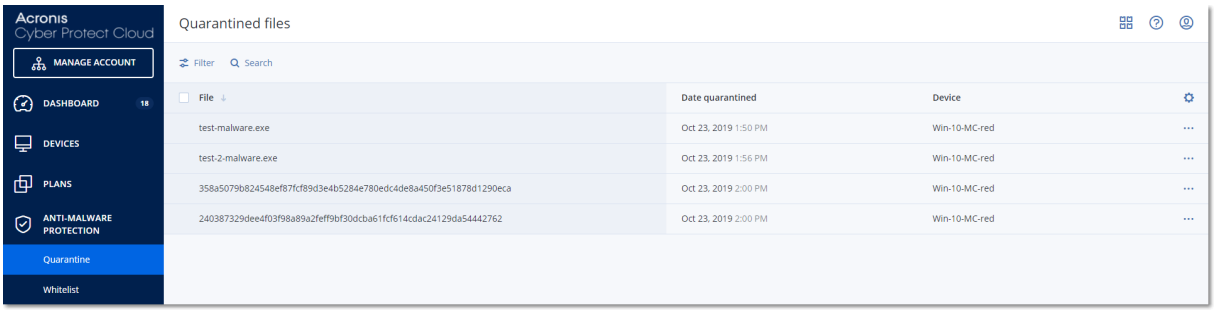
検疫されたファイルの管理

検疫されたファイルを管理するには、**[マルウェア対策保護]** > **[検疫]** に進みます。すべてのマシンの検疫されたファイルのリストが表示されます。

名前	説明
ファイル	ファイル名。
検疫日	ファイルが検疫に移された日時
デバイス	感染ファイルが見つかったデバイス。
脅威名	脅威名。
保護計画	検疫に移された疑わしいファイルの保護計画。

検疫されたファイルについては、2つのアクションが考えられます。

- **削除** - 隔離されたファイルをすべてのマシンから完全に削除します。同じファイルハッシュを持つすべてのファイルを削除できます。同じファイルハッシュを持つすべてのファイルを復元できます。ファイルをハッシュでグループ化し、必要なファイルを選択してから削除します。
- **復元** - 隔離されたファイルを変更せずに元の場所に復元します。現在、元の場所に同じ名前のファイルがある場合、そのファイルは復元さ れたファイルで上書きされます。復元されたファイルは許可リストに追加され、それ以降のマルウェア対策 スキャンではスキップされますのでご注意ください。



マシンの検疫ロケーション

検疫されたファイルのデフォルトのロケーションは、以下のとおりです。

- Windowsマシンの場合: `%programdata%Acronis</NGMP</quarantine`
- Macマシンの場合: `/Library/Application Support/Acronis/NGMP/quarantine`
- Linuxマシンの場合: `/var/lib/Acronis/NGMP/quarantine`

検疫ストレージは、サービスプロバイダーの自己防衛機能で保護されています。

オンデマンドのセルフサービスカスタムフォルダ

ワークロード上のカスタムフォルダを選択し、コンテキストメニューから直接スキャンを実行できます。

コンテキストメニューのCyber Protectオプションでスキャンにアクセスするには

保護計画でウイルス対策とマルウェア対策が有効になっているワークロードの場合、スキャンするファイル/フォルダを右クリックします。

注意
このオプションは、ワークロードの管理者のみが利用できます。

企業ホワイトリスト

正規に導入されている企業独自のアプリケーションが、ウイルス対策ソリューションにより不正なものとして識別される場合があります。こういった偽陽性による誤検知を防ぐために、信頼済みアプリケーションを手動でホワイトリストに追加できますが、これには時間がかかります。

注意
企業のホワイトリストは、バックアップのマルウェア対策スキャンには影響しません。

Cyber Protectionにより、このプロセスを自動化することができます。バックアップはウイルスおよびマルウェア対策保護モジュールによってスキャンされ、スキャンされたデータの解析により、該当するアプリケーションがホワイトリストに移動されます。このようにして偽陽性による誤検知が防ぐことができます。また、企業全体を対象とするホワイトリストを活用すれば、マルウェア対策スキャンのパフォーマンスがさらに向上します。

ホワイトリストはカスタマーごとに作成され、該当するカスタマーのデータのみに基づいています。

ホワイトリストは有効または無効にできます。無効にすると、追加されたファイルは一時的に非表示になります。

注意
管理者のロールを持つアカウントのみ（たとえば、Cyber Protection管理者、社内管理者、社内管理者の代理として業務にあたるパートナー管理者、部署管理者）が、ホワイトリストを構成および管理できます。この機能は、読み取り専用の管理者アカウントまたはユーザーアカウントでは使用できません。

ホワイトリストへの自動追加

1. 少なくとも2つのマシンでバックアップのクラウドスキャンを実行します。この操作を行うには、バックアップスキャン計画を使用します。
2. ホワイトリスト設定で **[ホワイトリストの自動生成]** のスイッチを有効にします。

ホワイトリストへの手動追加

[ホワイトリストの自動生成] のスイッチが無効になっている場合でも、手動でホワイトリストにファイルを追加することができます。

1. Cyber Protectコンソールで、**[マルウェア対策保護]** > **[ホワイトリスト]** に進みます。
2. **[ファイルの追加]** をクリックします。
3. ファイルのパスを指定して、**[追加]** をクリックします。

隔離されたファイルをホワイトリストに追加する

隔離されたファイルをホワイトリストに追加できます。

1. Cyber Protectコンソールで、**[マルウェア対策保護]** > **[検疫]** に進みます。
2. 隔離されたファイルを選択して、**[ホワイトリストに追加]** をクリックします。

ホワイトリスト設定

[ホワイトリストの自動生成] スイッチを有効にすると、ヒューリスティック保護のレベルを次のいずれかに指定するよう求められます。

- **低**
  - 相当長い時間が経過し、チェックが完了するまで、企業アプリケーションがホワイトリストに追加されることはありません。このようなアプリケーションは信頼性の高いものです。ただし、このアプローチでは偽陽性の検出確率が上がります。ファイルをクリーンで信頼できる状態だと見なす基準を高く設定するオプションです。
- **デフォルト**
  - 推奨保護レベルに基づいて企業アプリケーションがホワイトリストに追加されます。偽陽性の判定による検出は少なくなります。ファイルをクリーンで信頼できる状態だと見なす基準を中間レベルに設定するオプションです。
- **高**
  - 早い時点で企業アプリケーションがホワイトリストに追加され、偽陽性の判定による検出が少なくなります。ただし、ソフトウェアがクリーンであることが保証されるわけではないので、後になって疑わしいソフトウェアやマルウェアと見なされる場合もあります。ファイルをクリーンで信頼できる状態だと見なす基準を低く設定するオプションです。

ホワイトリストに登録されている項目の詳細を表示

ホワイトリストの項目をクリックすると、その項目の詳細情報が表示され、オンラインで分析できます。

追加した項目に確証が持てない場合は、VirtusTotalアナライザーで確認できます。**[VirusTotalを確認]**をクリックすると、サイトで不審なファイルやURLの分析が行われ、追加した項目のファイルハッシュによってマルウェアの種類を検出できます。ハッシュは**ファイルハッシュ（MD5）**の文字列で確認できます。

マシンの値は、バックアップスキャン中に該当のハッシュが見つかったマシンの数を表します。この値は、項目がバックアップスキャンまたは隔離から取り込まれた場合にのみ入力されます。ファイルが手動でホワイトリストに追加されている場合、このフィールドは空のままになります。

バックアップのマルウェア対策スキャン

バックアップのマルウェア対策スキャンによりバックアップでのマルウェアの有無を確認することで、感染ファイルの復元を防止できます。マルウェア対策のスキャンは、Cyber Protectionデータセンターに常駐するクラウドエージェントによって実行され、ローカルのコンピューティングリソースは使用されません。

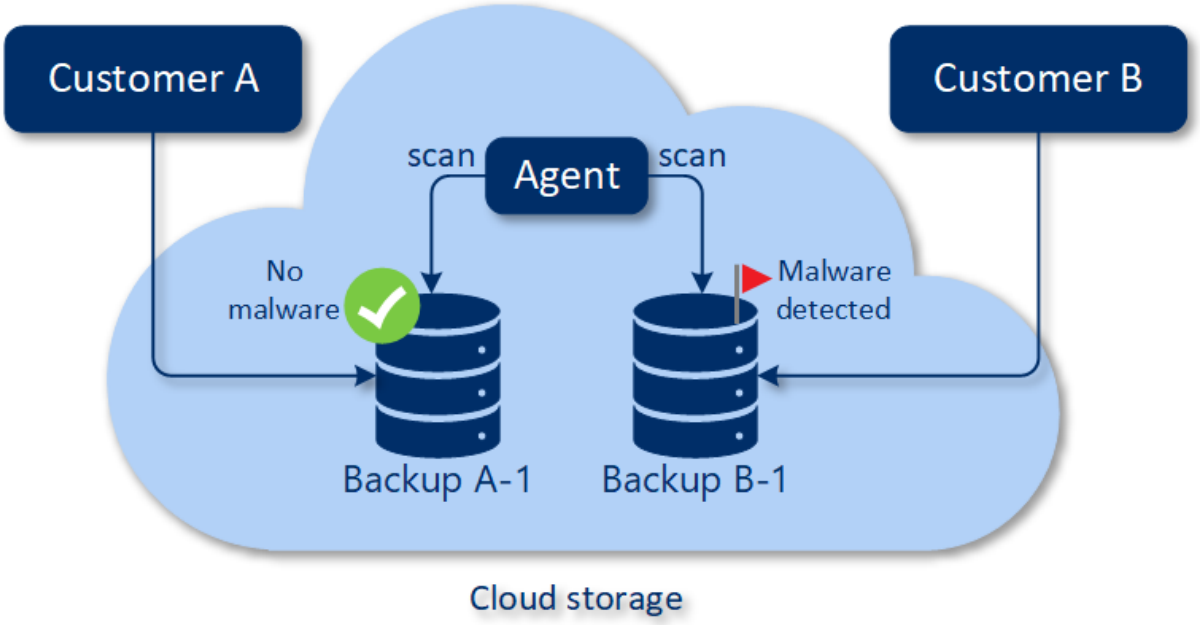
注意
この機能を利用できるかどうかは、現在のアカウントで有効になっているサービスクォータによって異なります。

マルウェア対策スキャンを実行するには、バックアップスキャン計画を構成する必要があります。その方法については、"バックアップスキャンの計画"（192ページ）を参照してください。

それぞれバックアップスキャン計画でクラウドエージェントのスキャンタスクが作成され、このタスクが各データセンターに1つずつあるキューに追加されます。スキャンタスクは、キュー内の順序に従って処理されます。また、スキャンの時間はバックアップサイズに応じて異なります。このため、バックアップスキャン計画を作成してからスキャンが完了するまでに時間がかかります。

スキャンを選択したバックアップは、次のいずれかのステータスになります。

- スキャンされていません
- マルウェアはありません
- マルウェアが検出されました



バックアップスキャンの結果は、**バックアップスキャンの詳細（脅威）**ウィジェットで確認できます。これは、Cyber Protectコンソールの **[監視]** > **[概要]** タブで確認できます。

制限事項

- マルウェア対策スキャンは、以下のワークロードの**マシン全体**または**ディスク/ボリューム**バックアップでサポートされています。
  - プロテクションエージェントがインストールされたWindowsマシン。
  - Hyper-VエージェントおよびVMwareエージェント（Windows）によって、ハイパーバイザーレベルでバックアップされるWindows仮想マシン（エージェントレスバックアップ）。

  マルウェア対策スキャンでは、VMwareエージェント（仮想アプライアンス）、Virtuozzoエージェント、Scale Computing HC3エージェントなどの仮想アプライアンスで作成されたバックアップはサポートされていません。
- GPTまたはMBRでパーティショニングされている、NTFSファイルシステムのボリュームのみがスキャンの対象になります。
- バックアップロケーションとしてサポートされているのは、デフォルトのクラウドストレージのみです。ローカルストレージ、パートナー所有のクラウドストレージはサポートされていません。
- スキャン対象のバックアップを選択するときは、継続的データ保護（CDP）バックアップが含まれているバックアップセットを選択できます。ただし、スキャンの対象となるのは、これらのバックアップセット内にあるCDP以外のバックアップのみです。CDPバックアップの詳細については、"継続的データ保護（CDP）"（397ページ）を参照してください。
- マシン全体の安全な復元を実行する場合は、CDPバックアップが含まれているバックアップセットを選択できます。ただし、この復元操作では、CDPバックアップのデータは使用されません。CDPデータをリカバリする場合は、追加の**ファイル/フォルダ**の復元操作を実行します。

Advanced保護機能の動作

Cyber Protectにはデフォルトで、サイバーセキュリティの脅威のほとんどをカバーする機能が含まれています。これらの機能は追加料金なしで使用できます。さらに、高度な機能を有効にして、ワークロードの保護を強化できます。

- 保護計画でAdvanced Protection機能を利用できる場合は、Advanced機能アイコン  のマークが付けられます。
- 高度な保護機能が利用できない場合は、必要なAdvanced保護パックを有効にするように管理者に連絡してください。
- 管理者が追加のセキュリティパックを購入できるようにした場合、Advanced機能を有効にできるようになります。追加の請求書発行が適用されることを通知するメッセージが表示されます。

注意
いずれか1つの機能でも有効になっている場合は、対応するAdvanced Protectionパックを購入する必要があります。

注意
保護計画ですべてのAdvanced機能が無効になっている場合、対応するAdvanced保護パックは無効になります。

Advanced保護パック	Advanced Protection機能
Advanced Backup	ワークロードを継続的に保護し、直前の作業変更も失われないようにする以下のような機能を提供しています。 • ワンクリック復元 • 継続的データ保護 • Microsoft SQL ServerクラスターおよびMicrosoft Exchangeクラスターのバックアップをサポート - Always On Availability Groups（AAG）およびデータベース可用性グループ（DAG） • MariaDB、MySQL、Oracle DB、SAP HANAのバックアップをサポート • データ保護マップおよびコンプライアンスレポート • オフホストのデータ処理 • Microsoft 365およびGoogle Workspaceワークロードのバックアップ間隔 • ブータブルメディアのリモート操作 • Microsoft Azureパブリッククラウドストレージへの直接バックアップ
Advanced SecurityとEDR	すべてのマルウェアの脅威からワークロードを継続的に保護する以下のような機能を提供しています。 • 集中管理されたインシデントページでインシデントを管理 • インシデントのスコープと影響を可視化 • 推奨事項と修復手順 • 脅威フィードを使用して、一般に公開されている、ワークロードに対する攻撃を確認。

	• セキュリティイベントを180日間保存 • ローカル署名ベースの検出によるウイルス対策およびマルウェア対策保護（リアルタイム保護） • エクスプロイト防御 • URLフィルタ処理 • エンドポイントファイアウォールの管理 • フォレンジックバックアップ、マルウェアに対応するバックアップスキャン、安全な復元、社内許可リスト • スマート保護計画（CPOCアラートとの統合） • マルウェアに対応する集中管理バックアップスキャン • リモートワイプ • Windows Defender Antivirus • Microsoft Security Essentials
Advanced管理	保護されたワークロードの脆弱性にパッチを当てる以下のような機能を提供しています。 • パッチ管理 • ディスク状態 • ソフトウェアインベントリ • フェールセーフパッチ • サイバースクリプト処理 • リモートアシスタンス • ファイル転送と共有 • 接続するセッションを選択 • マルチビューでワークロードを観察 • 接続モード: 制御、表示のみ、カーテン • クイックアシストアプリケーションによる接続 • リモート接続プロトコル:NEARとApple画面共有 • NEAR接続のセッション記録 • スクリーンショット送信 • セッション履歴リモート • 24個のモニタ • しきい値ベースの監視 • アノマリベースの監視
Advanced Data Loss Prevention	保護されたワークロードから機密情報の漏洩を防ぐ以下のような機能を提供しています • 周辺デバイスやネットワーク通信を介したワークロードのデータ漏洩をコンテンツ認識方式で防止 • 個人を特定できる情報（PII）、保護された医療情報（PHI）、PCI DSS（Payment Card Industry Data Security Standard、決済カード業界データセキュリティ基準）データ、および「機密扱い」カテゴリの文書を事前に自動検出 • データ漏洩防止ポリシーの自動作成（オプションでエンドユーザーアシスタンス付き） • 自動学習ベースのポリシー調整による適応型のデータ漏洩防止措置 • クラウドベースの集中管理監査ログ、アラート、エンドユーザー通知

Advanced Data Loss Prevention

Advanced Data Loss Preventionモジュールは、保護されたワークロードにおけるデータ転送の内容とコンテキストを分析し、データフローポリシーに基づいて、企業ネットワーク内部または外部の周辺デバイスやネットワーク転送による機密データ漏洩を防止します。

保護サービスとAdvanced Data Loss Preventionパックがカスタマーに対して有効になっている場合、カスタマーのテナントの保護計画にAdvanced Data Loss Preventionの機能を含めることができます。

Advanced Data Loss Preventionモジュールの使用を開始する前に、『基本ガイド』に記載されているAdvanced DLP管理の基本概念と論理構造を読み、理解していることを確認します。

また、『技術仕様』文書も参照してください。

データフローポリシーとポリシールールの作成

データ漏洩防止の主要な原則は、社内ITシステムのユーザーが、業務を遂行するために必要な範囲でのみ機密データを処理できるようにすることです。業務プロセスと関係がない、その他の機密データ転送はすべてブロックする必要があります。従って、ビジネス関連のデータ転送と不正なデータ転送またはフローを区別することが重要です。

データフローポリシーには、許可されるデータフローと禁止されるデータフローを指定するルールが含まれています。それで、データ漏洩防止モジュールが保護計画で有効になっていて、実行モードで稼働している場合、機密情報の不正な転送を防ぐことができます。

ポリシーの各機密カテゴリには、アスタリスク（*）でマークされた1件の既定ルールと、特定のユーザーまたはグループのデータフローを定義する1件または複数の明示的な（既定以外の）ルールが含まれます。ポリシールールの種類の詳細については、『基本ガイド』を参照してください。

データフローポリシーは通常、Advanced Data Loss Preventionが監視モードで実行されているときに自動的に作成されます。一般的なデータフローポリシーのビルドに必要な時間は約1ヶ月ですが、組織の業務プロセスによって異なる場合があります。データフローポリシーは、会社または部署の管理者が手動で作成、構成、または編集することもできます。

データフローポリシーの自動作成を開始するには

1. Cyber Protectコンソールに管理者としてログインします。
2. **[管理]** > **[保護計画]** に移動します。
3. **[計画の作成]** をクリックします。
4. **[データ漏洩防止]** セクションを展開し、**[モード]** 行をクリックします。

5. モードダイアログで、**[監視モード]** を選択し、データ転送の処理方法を選択します。

オプション	説明
すべて許可	ユーザーのワークロードから転送されるすべての機密データは、業務プロセスに必要であり、安全なものとして扱われます。ポリシーで既に定義されているルールと一致しない、検出されたデータフローごとに、新しいルールが作成されます。
すべて正当化	ユーザーのワークロードから転送されるすべての機密データは、業務プロセスに必要であるものの、リスクがあると見なされます。従って、以前に作成されたデータフロールールに一致しない、組織内外の受信者または宛先に対する機密データの転送（傍受対象）が発生するたび、ユーザーは業務上の正当性を明示する必要があります。正当化が提示されると、データフローポリシーに新しいデータフロールールが作成されます。
混合	「すべて許可」ロジックはすべての内部機密データフローに適用され、「すべて正当化」ロジックはすべての外部データフローに適用されます。 **注意** 内部/外部データについては、「宛先の自動検出」を参照してください

6. 保護計画を保存し、ポリシーをビルドするためのデータを収集するワークロードに適用します。

注意
観察モードの場合、データ漏洩は防止されません。

データフローポリシーを手動で構成するには

1. Cyber Protectコンソールで、**[保護]** > **[データフローポリシー]** に移動します。
2. **[新規データフロールール]** をクリックします。
   新規データフロールールペインが右側に展開されます。
3. 機密性カテゴリを選択し、送信者と受信者を追加します。さらに、選択したカテゴリ、送信者、および受信者のデータ転送の許可を定義します。

オプション	説明
許可	この送信者が該当する機密カテゴリのデータをこの受信者に転送できるようにします。
例外	この送信者が該当する機密カテゴリのデータをこの受信者に転送することを許可しません。ただし、送信者は個別の転送を可能にするためルールに例外をリクエストできます。 この送信者が該当の機密カテゴリのデータをこの受信者に転送しようとすると、転送がブロックされ、送信者は、この転送を許可するのに必要な例外をリクエストするよう求められます。例外がリクエストされると、データ転送を続行できます。 **重要** 該当の機密カテゴリに属する、この送信者と受信者の間に発生する後続のすべてのデータ転送は、例外がリクエストされてから5分間許可されます。

オプション	説明
拒否	この送信者が該当の機密カテゴリのデータをこの受信者に転送することを許可しません。また、送信者がルールの例外をリクエストすることも許可しません。

4. （オプション）ルールがトリガーされたときに実行する操作を選択します。

アクション	説明
ログに書き込み	ルールがトリガーされたときに、イベントレコードを監査ログに保存します。**例外**許可が付与されたルールに対しては、この操作を選択することをお勧めします。
アラートを生成	ルールがトリガーされたときに、Cyber Protect [**アラート**] タブでアラートを生成します。管理者に対する通知が有効になっている場合は、Eメール通知も送信されます。
データ転送が拒否された場合、エンドユーザーに通知	ユーザーによってルールがトリガーされると、画面上の警告により、リアルタイムでユーザーに通知されます。

5. [**保存**] をクリックします。
6. ステップ2～5を繰り返して、機密カテゴリとオプションが異なる複数のルールを作成し、作成したルールが選択したオプションに対応していることを確認します。

データフローポリシーの構造

ポリシールールは、**データフローポリシー**ビューで、制御する機密データのカテゴリに従ってグループ化されています。機密カテゴリの識別子は、ポリシールールのグループのすぐ上に表示されます。

- 機密
  - 保護済みヘルス情報（PHI）
  - 個人識別情報（PII）
  - 決済カード業界データセキュリティ標準（PCI DSS）、
  - 機密事項としてマーク済み
- 非機密

データフローポリシーの概念や機能については、『基本ガイド』を参照してください。

ルール構造

各ポリシールールは、次の要素で構成されています。

- **機密カテゴリ**
  - **保護済みヘルス情報（PHI）**
  - **個人識別情報（PII）**
  - **決済カード業界データセキュリティ標準（PCI DSS）**

- **機密事項としてマーク済み**
  "機密データの定義"（856ページ）をご覧ください
- **送信者** - このルールによって制御されるデータ転送の送信元ユーザーを指定します。単一のユーザー、ユーザーのリスト、またはユーザーグループなどを指定できます。
  - **すべての内部ユーザー** - 組織のすべての内部ユーザーを含むユーザーグループ。
  - **連絡先/組織から** - Advanced Data Loss Preventionによって認識される組織内のWindowsアカウント、および特定のWindowsアカウントで以前に使用されたことのある他のすべてのアカウント（サードパーティの通信アプリケーションで使用されるものを含む）。
  - **連絡先/カスタムID** - 次のいずれかの形式で指定された内部ユーザーの識別子: Eメールアドレス、Skype ID、ICQ識別子、IRC識別子、Jabber Eメールアドレス、Mail.ruエージェントEメールアドレス、Viber電話番号、ズームEメールアドレス。
    連絡先のグループを指定するため、次のワイルドカードを使用できます。
    - ***** - 任意の数の文字
    - **?** - 任意の文字（単一）
- **受信者** - このルールによって制御されるデータ転送の宛先ユーザーを指定します。単一のユーザー、ユーザーのリスト、ユーザーグループ、および以下に指定されている他のタイプの宛先などを指定できます。
  - **任意** - Advanced DLPでサポートされる任意の受信者タイプ。
  - **連絡先/任意の連絡先** - 任意の内部または外部の連絡先。
  - **連絡先/任意の内部連絡先** - 内部ユーザーの任意の連絡先（"宛先の自動検出"（856ページ）を参照）。
  - **連絡先/任意の外部連絡先** - 外部の個人または団体の連絡先。
  - **連絡先/組織から** - 送信者フィールドの説明と同じ原則。
  - **連絡先/カスタムID** - 送信者フィールドの説明と同じ原則。
  - **ファイル共有サービス** - 制御されたファイル共有サービスの識別子。
  - **ソーシャルネットワーク** - 制御されたソーシャルネットワークの識別子。
  - **ホスト/任意のホスト** - Advanced DLPによって内部または外部として認識される任意のコンピューター。
  - **ホスト/任意の内部ホスト** - Advanced DLPによって内部として認識される任意のコンピューター。
  - **ホスト/任意の外ホスト** - Advanced DLPによって外部として認識される任意のコンピューター。
  - **ホスト/特定のホスト** - ホスト名（例:FQDN）またはIPアドレス（IPv4またはIPv6）として指定されるコンピューターの識別子。
  - **デバイス/任意のデバイス** - ワークロードに接続されている任意の周辺デバイス。
  - **デバイス/外部ストレージ** - ワークロードに接続されたリムーバブルストレージまたはリダイレクトされたマップ済みドライブ。
  - **デバイス/暗号化済みリムーバブル** - BitLocker To Goで暗号化されたリムーバブルストレージデバイス。
  - **デバイス/リダイレクトされたクリップボード** - ワークロードに接続されたリダイレクトされたクリップボード。
  - **プリンター** - ワークロードに接続されているローカルプリンターまたはネットワークプリンター。

- **許可** - このルールによって制御されるデータ転送に適用される予防制御。詳細については、「データフローポリシールールの許可」のトピックを参照してください。
- **操作** - このルールがトリガーされたときに実行される非予防的操作。デフォルトでは、このフィールドは「アクションなし」に設定されています。次のオプションがあります:
  - **ログに書き込む** - ルールがトリガーされたときに、イベントレコードを監査ログに保存します。
  - **データ転送が拒否された場合エンドユーザーに通知** - ルールがトリガーされたときに、画面上の警告でリアルタイムにユーザーに通知します。
  - **アラートを生成** - ルールがトリガーされたときに管理者にアラートを送信します。

警告
アクションなしが選択されている場合、次のルールがトリガーされます。
- 監査ログにイベントの記録を追加しない。
- 管理者にアラートを送信しない。
- エンドユーザーに画面通知を表示しない。

どのような場合にポリシールールがトリガーされますか？

次のすべての条件が当てはまる場合、データ転送はデータフローポリシールールに一致すると見なされます:

- 該当のデータ転送におけるすべての送信者がリストに掲載されているか、ルールの **[送信者]** フィールドで指定されたユーザーグループに属している。
- 該当のデータ転送におけるすべての受信者がリストに掲載されているか、ルールの **[受信者]** フィールドで指定されたユーザーグループに属している。
- 転送されるデータが、ルールの**機密カテゴリ**と一致する。

データフローポリシールールの許可の調整

Advanced Data Loss Preventionは、データフローポリシールールにおいて3種類の許可をサポートしています。許可は、ポリシーの各ルールで個別に構成されます。

許可（許容）
ルールで定義された機密カテゴリ、送信者、受信者の組み合わせに一致するデータ転送が許可されます。

例外（禁止）
ルールで定義された機密カテゴリ、送信者、および受信者の組み合わせに一致するデータ転送は許可されません。ただし、送信者は個別の転送を可能にするためルールに例外をリクエストできます。

重要
該当の機密カテゴリに属する、この送信者と受信者の間に発生する後続のすべてのデータ転送は、例外がリクエストされてから5分間許可されます。

拒否（禁止）
ルールで定義された機密カテゴリ、送信者、および受信者の組み合わせに一致するデータ転送は許可されておらず、送信者には例外をリクエストするオプションがありません。

さらに、ポリシー管理の柔軟性を高めるために、**許可**および**例外**許可に優先度のフラグを割り当てることができます。この設定により、ポリシー内の他のデータフロールールで特定のグループに設定されたアクセス許可を上書きできます。これを使用して、一部のメンバーにのみグループデータフロールールを適用できます。これを実現するには、グループルールから除外する特定のユーザーのデータフロールールを作成し、それらのユーザーが属するグループのルールで構成されているデータフロー制限よりも、ユーザーに付与されたアクセス許可を優先させる必要があります。ルールを組み合わせる際の許可の優先順位については、"データフローポリシールールの組み合わせ"（849ページ）を参照してください。

重要
社内または部署のポリシーを観察モードから実行モードに切り替える前に、各機密データカテゴリのデフォルトルールを許容状態から禁止状態に調整する必要があります。デフォルトのルールには、**データフローポリシー**ビューでアスタリスク（*）が付けられています。ポリシールールの種類の詳細については、『基本ガイド』を参照してください。

ポリシールールの許可を編集するには

1. Cyber Protectコンソールに管理者としてログインします。
2. **[保護]** > **[データフローポリシー]** に移動します。
3. 編集するポリシールールを選択し、ルールリストの上にある **[編集]** をクリックします。
   [データフロールールの編集] ウィンドウが開きます。
4. **許可**セクションで、**[許可]**、**[例外]**、または **[拒否]** を選択します。
5. （オプション）このルールの **[許可]** または **[例外]** 許可を他のルールの許可よりも優先するには、**[優先]** チェックボックスをオンにします。
   このチェックボックスを使用して、デフォルトの [任意] > [その他] ルールよりもデータフロールールを優先させる必要はありません。これらのルールでは、デフォルトでポリシーの優先度が最も低く設定されているためです。
   ルールを組み合わせる際の許可の優先順位については、"データフローポリシールールの組み合わせ"（849ページ）を参照してください。
6. （オプション）ルールがトリガーされたときに実行する操作を選択します。
7. ポリシールールへの変更を保存します。

データフローポリシールールの組み合わせ

データ転送が複数のルールに一致する場合、すべてのルールで構成されている許可と操作が組み合わされ、次のように適用されます。

権限

データ転送が複数のルールに一致し、これらのルールにより同じデータカテゴリに対して異なる許可が付与されている場合、次の許可優先度リスト（降順）に従って、優先度の高い許可を付与されたルールが優先されます。

1. **優先**フラグによる例外
2. **優先**フラグによる許可

3. 拒否
4. 例外
5. 許可

データ転送が複数のルールに一致し、これらのルールが異なるデータカテゴリに対して別個の許可を付与されている場合、次のロジックが上書きで適用されます。

1. データ転送が一致する機密カテゴリごとに、最も制限の厳しいルールの許可が定義されます。
2. ポイント1で定義された最も制限の厳しいルール許可が適用されます。

例

ファイル転送は、次のように、異なる機密カテゴリの3つのルールに一致します。

機密カテゴリ	許可
PII	許可 - 優先
PHI	例外 - 優先
PCI	拒否

適用される許可は拒否です。

アクション

データ転送が複数のルールに一致し、これらのルールの **[操作]** フィールドに異なるオプションが構成されている場合、トリガーされたすべてのルールで構成されたすべての操作が実行されます。

ポリシーの確認と管理

自動的に作成されたベースラインデータフローポリシーを適用する前に、クライアントによる確認、検証、承認が必要です。業務プロセスの詳細を熟知しているのはクライアントであり、業務プロセスがベースラインポリシーの中で一貫性のある形で解釈されているかどうかの評価をクライアントが行うのが適切だからです。また、クライアントが不正確な部分を特定して、パートナー管理者が修正できます。

ポリシーの確認中に、パートナー管理者はベースラインデータフローポリシーをクライアントに提示します。クライアントは、ポリシー内の各データフローを確認し、業務プロセスとの整合性を検証します。Cyber Protectコンソールにおけるポリシールールの表現は直感的かつ明快であるため、検証に技術的スキルは必要ありません。各ルールは、機密データフローの送信者と受信者を記述します。

パートナー管理者は、クライアントの指示に基づいて、データフローポリシールールを編集、削除、および作成することにより、ベースラインポリシーを手動で調整します。クライアントによる承認後、保護対象のワークロードに適用される保護計画を実行モードに切り替えることで、確認済みのポリシーを保護対象のワークロードに適用します。

確認済みポリシーを適用する前に、機密データカテゴリに対して自動的に作成されたすべてのデフォルトポリシールールで、**許可**権限を**拒否**または**例外**に変更しておきます。ユーザーは**拒否**権限を上書きで

きません。一方、**例外**権限では、ルールに該当する転送がブロックされますが、緊急時に業務関連の例外をリクエストすることでブロックを上書きできます。

データフローポリシーの更新

社内または社内部署の業務プロセスが大幅に変更された場合、アップデートされたビジネスプロセスの機密データフローにおける変更点と一貫性を保つために、DLPポリシーを更新する必要があります。従業員の役職が変更された場合も、ポリシーの更新が必要です。この場合、従業員のワークロードを保護するために使用される部署ポリシーの一部も更新する必要があります。

高度なDLPポリシー管理ワークフローにより、管理者は、社内全体、部署、ユーザー、または部署内の一部ユーザーのポリシー更新を自動化できます。

社内または部署のポリシーを更新する

観察モードのすべてのオプションを使用して、社内または部署全体のポリシー、および部署内のユーザー（1人または複数）の部署ポリシーの一部を更新できます。

社内または部署のポリシーを更新するには

更新プロセスは、次の手順で構成されます。これらの手順は、社内管理者または社内のワークロードを管理するパートナーが実行する必要があります。

1. 適用されたポリシーのデフォルト以外のルールをすべて削除します。
2. 更新を開始するには、社内または部署に適用されたAdvanced DLPを使用する保護計画を、この特定の企業または部署に最適な観察モードオプションのいずれかに切り替え、社内または部署のすべてのワークロードに計画を適用します。
3. 更新期間が終了したら、クライアントを交えて新しい社内または部署ポリシーを確認し、必要に応じて調整して、クライアントの承認を得るようにします。
4. 社内または部署のワークロードに適用される保護計画を適切な実行モードオプション（部署のワークロードからのデータ漏洩を防ぐ上で、クライアントが最適であると考えるオプション）に切り替えます。

社内または部署のユーザー（1人または複数）のポリシーを更新する

ユーザーレベルのポリシーは、監視モードの任意のオプションと「適応して実行」モードを使用して更新できます。

ユーザーポリシーを更新するための監視モードの使用

社内（または部署）のユーザー（1人または複数）のポリシーを更新するために観察モードを使用する場合、更新処理中に発生するユーザーのデータ転送に対しては、社内全体（または部署全体）に適用されるデータフローポリシーが適用されません。その結果、更新中にユーザーによって新しい個別ルールが作成される可能性があります。ここで作成されたルールと、社内（または部署）に適用されるポリシーの既存のグループルールは、矛盾する場合または一致する場合があります。更新が完了し、ユーザーのデータ転送に対してポリシーが再適用された後、ユーザー用に作成されたこれらの新しい個別のルールが、実際にユーザーのデータ転送に適用されるかどうかは、該当のデータ転送に適用されるポリシー内の他のルールと新しい個別ルールの優先順位に依存します。

観察モードでユーザーのポリシーを更新するには

更新プロセスは、次の手順で構成されます。これらの手順は、社内管理者または社内のワークロードを管理するパートナーが実行する必要があります。

1. 単一の送信者であるユーザーが所属する企業（または部署）に適用されるポリシーについて、デフォルト以外のすべてのルールを削除します。
2. 適用されたポリシー内にあるすべての非デフォルトデータフロールールの送信者リストから、ユーザーを削除します。
3. 観察モードのAdvanced DLPを使用して新しい保護計画を作成し、それをユーザーのワークロードに適用して、更新（観察）期間を開始します。
   更新期間は、ユーザーによるワークロードからの機密データ転送に関わる、通常の全業務アクティビティ（またはアクティビティの90～95%）に必要な時間によって変化します。
4. 更新期間が終了したら、実行されたポリシーに追加された該当ユーザーに関連する新しいルールを確認し、必要に応じて調整して、クライアントの承認を受けます。
5. ユーザーのワークロードからのデータ漏洩を防ぐ上で、クライアントが最適であると考えるオプションに応じ、ユーザーのワークロードに適用される保護計画を**厳格に実行**モードまたは**適応して実行**モードに切り替えます。
   また、社内（または部署）に適用された保護計画をユーザーのワークロードに再適用することもできます。

ユーザーポリシー更新における「適応して実行」モードの使用

単一ユーザーのポリシー更新、また社内（または部署）全ユーザーの一部に対するポリシー更新は、ユーザーのワークロードにAdvanced DLPを適用した保護計画の「適応して実行」モードを使用して実行できます。

注意
このポリシー更新方法では、更新中に該当ユーザーからのデータ転送が発生する場合、このユーザーがメンバーとして属する送信者グループ（例: Any internal）に対して適用される社内（部署）ポリシールールが、更新中のデータ転送にも適用されます。つまり、更新処理中に、送信者グループの既存のポリシールールと矛盾または一致する、新しいユーザールールが個別に作成されることはありません。特定クライアントのユーザーポリシーの更新にこれら2つの方法のどちらがより効果的かは、個別のITセキュリティ要件によって異なります

「適応して実行」モードを使用してユーザーのポリシーを更新するには

更新プロセスは、次の手順で構成されます。これらの手順は、社内管理者または社内のワークロードを管理するパートナーが実行する必要があります。

1. 単一の送信者であるユーザーが所属する企業（部署）に適用されるポリシーについて、デフォルト以外のすべてのルールを削除します。
2. 適用されたポリシー内にあるすべての非デフォルトデータフロールールの送信者リストから、ユーザーを削除します。
3. 社内（または部署）に適用されるポリシーのすべてのデフォルトルールについて、それらのアクセス許可を **[例外]** に設定し、**[操作]** フィールドで **[ログに書き込む]** 操作を選択します。

4. ユーザーのワークロードに現在適用されている保護計画が**厳格に実行**モードに設定されている場合は、Advanced DLPを使用して新しい保護計画を作成し、それを**適応して実行**モードでユーザーのワークロードに適用して更新期間を開始します。
   更新期間は、ユーザーによるワークロードからの機密データ転送に関わる、通常の全業務アクティビティ（またはアクティビティの90～95%）に必要な時間によって変化します。
5. 更新期間が終了したら、実行されたポリシーに追加された該当ユーザーに関連する新しいルールを確認し、必要に応じて調整して、クライアントの承認を受けます。
6. ユーザーのワークロードからのデータ漏洩を防ぐ上で、クライアントが最適であると考えるオプションに応じて、ユーザーのワークロードに適用される保護計画を**厳格に実行**モードに切り替えるか、または**適応して実行**モードのままにします。
   また、社内（または部署）に適用された保護計画をユーザーのワークロードに再適用することもできます。

保護計画でのAdvanced Data Loss Preventionの有効化

保護サービスとAdvanced Data Loss Preventionパックがカスタマーに対して有効になっている場合、カスタマーのテナントの保護計画にAdvanced Data Loss Preventionの機能を含めることができます。

Advanced DLPは、データ損失防止機能グループの高度なモジュールです。Advanced DLPの機能とデバイス制御は、単独で使用することも、単一の保護計画内で、あるいは同じワークロードを保護する2件の計画内で同時に使用することもできます。同時に使用する場合、その機能は次のように調整されます。

- デバイス制御により、（Advanced DLPが転送データの内容を検査する）ローカルチャネルへのユーザーアクセス制御が停止されます。ただし、デバイス制御の設定が読み取り専用またはアクセス拒否の場合、次のデバイスタイプの制御が維持されます。
  - リムーバブル
  - 暗号化リムーバブル
  - マッピングされたドライブ

  例えば、デバイス制御とAdvanced DLPの両方が単一の保護計画、または同じワークロードを保護する2件の計画で有効になっていて、デバイス制御でUSBデバイスに対するアクセスが読み取り専用に設定されている場合、すべてのUSBデバイスに対するアクセスは読み取り専用になります（ただし、許可リストに記載されている場合は例外）。これは、Advanced DLPモジュールのアクセス設定に関わりなく適用されます。デバイス制御のデフォルトで、アクセスを有効にするように設定されている場合、Advanced DLPのアクセス設定が適用されます。
- 許可リスト内の次のローカルチャネルおよび周辺デバイスへのユーザーアクセスは、デバイス制御によって強制的に実行されます:
  - 光学ドライブ
  - フロッピードライブ
  - MTP接続のモバイルデバイス
  - Bluetoothアダプタ
  - Windowsクリップボード
  - スクリーンショットのキャプチャ
  - USBデバイスとデバイスタイプ（リムーバブルストレージおよび暗号化されたものを除く）

Advanced DLPで保護計画を作成するには

1. **[管理]** > **[保護計画]** に移動します。
2. **[計画の作成]** をクリックします。
3. **[データ漏洩防止]** セクションを展開し、**[モード]** 行をクリックします。
   [モード] ダイアログが開きます。
   - データフローポリシーの作成または更新を開始するには、**観察モード**を選択し、データ転送をどのように処理するかを選択します。

オプション	説明
すべて許可	ユーザーのワークロードから転送されるすべての機密データは、業務プロセスに必要であり、安全なものとして扱われます。ポリシーで既に定義されているルールと一致しない、検出されたデータフローごとに、新しいルールが作成されます。
すべて正当化	ユーザーのワークロードから転送されるすべての機密データは、業務プロセスに必要であるものの、リスクがあると見なされます。従って、以前に作成されたデータフロールールに一致しない、組織内外の受信者または宛先に対する機密データの転送（傍受対象）が発生するたび、ユーザーは業務上の正当性を明示する必要があります。正当化が提示されると、データフローポリシーに新しいデータフロールールが作成されます。
混合	すべての許可ロジックは、機密データのすべての内部転送に適用され、すべての正当化ロジックは機密データのすべての外部転送に適用されます。 内部の宛先の定義については、"宛先の自動検出"（856ページ）を参照してください

警告

- 以前にデータフローポリシーを作成していない場合、またはポリシーを更新する場合にのみ、**観察モード**を選択します。ポリシーの更新を開始する前に、"データフローポリシーの更新"（851ページ）を参照してください。
- 観察モードでは、データ漏洩は防止できません。『基本ガイド』の「観察モード」を参照してください。

   - 既存のデータフローポリシーを適用するには、**実行モード**を選択してから、データフローポリシールールを適用する厳密性を選択します。

オプション	説明
厳格に実行	データフローポリシーはそのまま適用され、従来の監視対象ではなかった機密データフローが検出された場合でも、新しい許容ポリシールールとして拡張されることはありません。 『基本ガイド』の「厳格に実行」を参照してください。
適応して実行（学習して実行）	実行されたポリシーは、観察期間中に実行されなかった業務オペレーション、または業務プロセスの変更に対して、自動的に適応します。このモードにより、ワークロード上で検出された新規学習データフローに基づいて、強制されたデータフローポリシーを拡張できます。 『基本ガイド』の「適応して実行」を参照してください。

重要
社内または部署のポリシーを観察モードから実行モードに切り替える前に、各機密データカテゴリのデフォルトルールを許容状態から禁止状態に調整する必要があります。デフォルトのルールには、**データフローポリシー**ビューでアスタリスク（*）が付けられています。ポリシールールの種類の詳細については、『基本ガイド』を参照してください。

4. **[完了]** をクリックして、[モード] ダイアログを閉じます。
5. （オプション）光学式文字認識、許可リスト、およびその他の保護オプションを構成するには、**[詳細設定]** をクリックします。
   使用可能なオプションについては、"詳細設定"（855ページ）を参照してください。
6. 保護計画を保存して、保護対象のワークロードに適用します。

詳細設定

Advanced Data Loss Preventionを含む保護計画の詳細設定を使用して、Advanced Data Loss Preventionによって制御されるチャネルのデータコンテンツ検査の品質を向上させることができます。また任意の予防制御から、許可リストにある周辺デバイスの種類、ネットワーク通信のカテゴリ、宛先ホストへのデータ転送、および許可リストにあるアプリケーションが開始したデータ転送を除外できます。以下の詳細設定を構成できます。

- **光学文字認識（OCR）**
  この設定により、光学式文字認識（OCR）をオンまたはオフにして、文書、メッセージ、スキャンデータ、スクリーンショットなどのグラフィックファイルやイメージから、31種類の言語のテキスト部分を抽出し、詳細な内容を確認できるようになります。
- **パスワードで保護されたデータの転送**
  パスワードで保護されたアーカイブや文書の内容を参照することはできません。この設定によってAdvanced DLPを使用すると、管理者はパスワードで保護されたデータの送信転送を許可するか、またはブロックするかを選択できるようになります。
- **エラー時のデータ転送防止**
  送信コンテンツの解析に失敗したり、DLPエージェントの処理時に別の制御エラーが発生したりすることもあります。このオプションを有効にすると、転送はブロックされます。このオプションを無効にすると、エラーが発生しても転送が許可されます。
- **デバイスの種類とネットワーク通信の許可リスト**
  このリストでチェックした周辺デバイスやネットワーク通信でのデータ転送は、データの機密性や適用されているデータフローポリシーに関係なく許可されます。

警告
このオプションは、特定のデバイスタイプまたはプロトコルで問題が発生した場合に使用されます。サポート担当者からのアドバイスがない限り、有効にしないでください。

- **リモートホストの許可リスト**
  このリストに記載されている宛先ホストへのデータ転送は、データの機密性や適用されているデータフローポリシーに関係なく許可されます。

- **アプリケーションの許可リスト**
  このリストに記載されているアプリケーションによるデータ転送は、データの機密性や適用されているデータフローポリシーに関係なく許可されます。

[保護計画の作成] ビューおよび保護計画の [詳細] ビューに表示される詳細設定の**セキュリティレベル**インジケータには、次のようなロジックでレベルが表示されます。

- **基本**は、詳細設定がオンになっていないことを示します。
- **中程度**は、1つまたは複数の設定がオンになっているものの、**OCR**、**パスワードで保護されたデータの転送**、また**エラー時のデータ転送防止**の組み合わせが有効化されていないことを示します。
- **厳格**は、少なくとも**OCR**、**パスワードで保護されたデータの転送**、また**エラー時のデータ転送防止**の組み合わせが有効化されていることを示します。

宛先の自動検出

混合観察モードの場合、Advanced Data Loss Preventionでは、検出されたデータ転送の宛先（内部または外部）に応じて異なるルールが適用されます。宛先を内部として判定するロジックを以下に説明します。他のすべての宛先は外部と見なされます。

Advanced Data Loss Preventionでは、傍受されたデータ転送ごとに、DNSリクエストが実行され、Data Loss Preventionエージェントが実行されているマシンとリモートサーバーのFQDN名を比較することにより、宛先HTTP、FTP、またはSMBサーバーが内部サーバーであるかどうかが自動的に検出されます。DNSリクエストが失敗すると、保護されたワークロードとリモートサーバーが同じネットワーク内にあるかどうかについても確認されます。Data Loss Preventionエージェントが実行されているマシンと同じドメイン名を持つ（または同じサブネットワーク内にある）サーバーは、内部と見なされます。

Eメールの通信において、Advanced Data Loss Preventionは、受信者のEメールアドレスが送信者のEメールアドレスと同じドメインにあり、受信者のメールサーバー名が同じである場合、社内Eメールサーバー経由で社内Eメールアドレスから送信されたすべてのEメールを内部転送として扱います。

社外のEメールは、受信者アカウントが既知のものでない限り、外部との通信として扱われます。Data Loss Preventionはネットワーク上のユーザーアクティビティを監視しており、ユーザーに関連付けられたEメールアドレスのデータでバックエンドのデータベースがアップデートされると、既存のEメールアドレスに関するデータもアップデートされます。

メッセンジャー経由の通信は、受信者のアカウントが既知のものでない限り、外部との通信として扱われます。Data Loss Preventionはネットワーク上のユーザーアクティビティを監視しており、ユーザーに関連付けられたアカウントのデータでバックエンドのデータベースがアップデートされると、既知のアカウントに関するデータもアップデートされます。

機密データの定義

このトピックでは、コンテンツ分析中に機密データが識別されるロジックについて説明します。

誤検知を減少させるため、記述された論理式のすべてのグループに同種の一致が存在する場合、それぞれが1件の一致としてカウントされます。

重要
コンテンツの識別に使用される論理式は、情報提供のみを目的としており、ソリューションの詳細を説明するものではありません。

保護済みヘルス情報（PHI）

サポート言語

- 米国、英国（英語） - 国際
- フィンランド語
- イタリア語
- フランス語
- ポーランド語
- ロシア語
- ハンガリー語
- ノルウェー語
- スペイン語

保護されたヘルス情報と見なされるデータ

次のデータは、保護されたヘルス情報と見なされます。

- 氏名
- 住所（町名と番地、市区町村、都道府県、郵便番号、およびそれらに相当する地理コード）
- 電話番号
- Eメールアドレス
- 社会保障番号
- 健康保険番号
- 銀行口座番号
- URL
- IPアドレスの番号
- ICD-10-CMコード
- ICD-10-PCS-and-GEMs
- HIPAA
- その他のヘルスケア関連
- クレジットカードの番号

コンテンツ検出に使用される論理式

論理式は、論理演算子ORで結合された次の文字列で構成されます。AND論理演算子が明示的に指定されていない限り、上記のリストのさまざまなデータグループの結合にOR演算子が使用されます。括弧内の数字は、陽性の検出結果を返す、検出されたインスタンスの数を表します。

- **社会保障番号**（5）
- （氏名（3） OR 住所（3） OR 電話番号（3） OR Eメールアドレス（3）） OR （銀行口座番号（3） OR クレジットカード番号（3）） AND （社会保障番号（3） OR 健康保険番号（3）* OR ICD-10-CMコード（3） OR ICD-10-PCS-and-GEMs（3） OR HIPAA（3） OR その他のヘルスケア関連（3））

個人識別情報（PII）

サポート言語

- 米国、英国（英語） - 国際
- ブルガリア語
- 中国語
- チェコ語
- デンマーク語
- オランダ語
- フィンランド語
- フランス語
- ドイツ語
- ハンガリー語
- インドネシア語
- イタリア語
- 韓国語
- マレー語
- ノルウェー語
- ポーランド語
- ポルトガル語（ブラジル）
- ポルトガル語（ポルトガル）
- ルーマニア語
- ロシア語
- セルビア語
- シンガポール
- スペイン語
- スウェーデン語
- 台湾
- トルコ語
- タイ語
- 日本語

個人識別情報（PII）と見なされるデータ

- 氏名
- 住所（町名と番地、市区町村、都道府県、郵便番号）
- 銀行口座番号
- 個人ID番号と財務ID番号
- パスポート番号
- 社会保障番号
- 電話番号
- 自動車ナンバープレート
- 運転免許番号
- IDおよびシリアルナンバー
- IPアドレス
- Eメールアドレス
- クレジットカードの番号

コンテンツ検出に使用される論理式

日本語を除くサポートされているすべての言語の論理式

論理式は、論理演算子ORまたはANDで結合された次の文字列で構成されます。括弧内の数字は、陽性の検出結果を返す、検出されたインスタンスの数を表します。

- 個人ID番号と財務ID番号（5）
- 氏名（3）AND（クレジットカード番号（3）OR社会保障番号（3）OR銀行口座番号（3）OR個人および財務ID番号（3）OR運転免許番号（3）ORパスポート番号（ 3）OR社会保障番号（3）OR IPアドレス（3）OR自動車ナンバープレート（3）OR IDおよびシリアルナンバー）
- 電話番号（3）AND（クレジットカード番号（3）OR社会保障番号（3）OR銀行口座番号（3）OR住所（3）OR個人および財務ID番号（3）OR運転免許番号（3）ORパスポート番号（3）OR社会保障番号（3）OR自動車ナンバープレート（3）OR IDおよびシリアルナンバー（3））
- （氏名（30）OR住所（30））AND（Eメールアドレス（30）OR電話番号（30）OR IPアドレス（30））
- Eメールアドレス（3）AND（クレジットカード番号（3）OR社会保障番号（3）OR銀行口座番号（3）OR個人および財務ID番号（3）OR運転免許番号（3）ORパスポート番号（3）OR社会保障番号（3）OR自動車ナンバープレート（3）OR IDおよびシリアルナンバー（3））
- Eメールアドレス（30）AND（住所（30）OR電話番号（30））
- 氏名（30）AND住所（30）
- 電話番号（30）および住所（30）
- 氏名（3）および銀行口座番号（3）
- 電話番号（3）AND（クレジットカード番号（3）OR銀行口座番号（3）OR社会保障番号（3）OR個人および財務ID番号（3）OR運転免許番号（3）ORパスポート番号（3））

日本語の論理式

注意
コンテンツ検出では、ユニークな一致のみがカウントされます。

論理式は、論理演算子ORで結合された次の文字列で構成されます。論理演算子ANDが明示的に指定されていない場合、異なるグループを結合するために演算子ORが使用されます。

- 社会保障番号（5）
- 氏名（3）AND（クレジットカード番号（3）OR銀行口座番号（3）OR運転免許番号（3）ORパスポート番号（3）OR社会保障番号（3））
- 氏名（30）AND（Eメールアドレス（30）OR電話番号（30）OR IPアドレス（30）OR住所（30））
- 住所（3）AND（クレジットカード番号（3）OR銀行口座番号（3）OR運転免許番号（3）ORパスポート番号（3）OR社会保障番号（3））
- Eメールアドレス（3）AND（クレジットカード番号（3）OR銀行口座番号（3）OR社会保障番号（3）OR運転免許番号（3））
- アドレス（5）AND（Eメールアドレス（5）OR氏名（5）OR電話番号（5）OR IPアドレス（5））
- 氏名（3）および銀行口座番号（3）
- 電話番号（3）AND（クレジットカード番号（3）OR銀行口座番号（3）OR住所（3）OR社会保障番号（3）OR運転免許番号（3））

決済カード業界データセキュリティ標準（PCI DSS）

サポート言語

この機密グループは言語に依存しません。PCIDSSデータは、国を問わず英語になります。

PCIDSSと見なされるデータ

- カード所有者データ
  - プライマリアカウント番号（PAN）
  - カード所有者名
  - 有効期限
  - サービスコード
- 機密性の高い認証データ
  - フルトラックデータ（磁気ストライプデータまたは同等のチップ）
  - CAV2/CVC2/CVV2/CID
  - PIN/PINブロック

コンテンツ検出に使用される論理式

論理式は、論理演算子ORで結合された次の文字列で構成されます。括弧内の数字は、陽性の検出結果を返す、検出されたインスタンスの数を表します。

- クレジットカード番号（5）
- クレジットカード番号（3）AND（米国名（例）（3）OR米国名（3）OR PCI DSSキーワード（3）OR日付（月/年）（3））
- クレジットカードダンプ（5）

機密事項としてマーク済み

機密としてマークされたデータは、キーワードグループを通じて検出されます。

一致条件は加重ベースになり、すべての単語の加重は1です。3より大きい加重で一致が発生すると、コンテンツ検出は陽性と見なされます。

サポート言語

- 英語
- ブルガリア語
- 中国語（簡体字）
- 中国語（繁体字）
- チェコ語
- デンマーク語
- オランダ語
- フィンランド語
- フランス語
- ドイツ語
- ハンガリー語
- インドネシア語
- イタリア語
- 日本語
- 韓国語
- マレー語
- ノルウェー語
- ポーランド語
- ポルトガル語 - ブラジル
- ポルトガル語 - ポルトガル
- ロシア語
- セルビア語
- スペイン語
- スウェーデン語
- トルコ語

キーワードグループ

各言語のキーワードグループには、英語の次のキーワードに相当する、各言語固有のキーワードが含まれています（大文字と小文字は区別されません）。

- confidential
- internal distribution
- not for distribution
- do not distribute
- not for public
- not for external distribution
- for internal use only
- highly qualified documentation
- private
- privileged information
- for internal use only
- for official use only

データ漏洩防止イベント

Advanced Data Loss Preventionにより、DLPイベントビューに次のようなイベントが生成されます。

- 監視モードでは、正当化されたすべてのデータ転送に対してイベントが生成されます。
- 実行モードでは、トリガーされたポリシールールごとに構成される**ログに書き込む**操作に基づいて、イベントが生成されます。

データフローポリシーで、ルールのイベントを表示するには

1. Cyber Protectコンソールに管理者としてログインします。
2. **[保護]** > **[データフローポリシー]** に移動します。
3. イベントを表示したいルールに移動して、ルールの行の末尾にある省略記号をクリックします。
4. **[イベントを表示]** を選択します。

DLPイベントビューでイベントの詳細を表示するには

1. Cyber Protectコンソールに管理者としてログインします。
2. **[保護]** > **[DLPイベント]** に移動します。
3. リスト内のイベントをクリックすると、そのイベントの詳細が表示されます。
   イベントの詳細ペインが右側に展開されます。
4. イベントの詳細ペインを上下にスクロールして、利用可能な情報を表示します。
   ペインに表示される詳細情報は、イベントをトリガーしたルールのタイプとルール設定によって異なります。

DLPイベントリストでイベントをフィルタリングするには

1. Cyber Protectコンソールに管理者としてログインします。
2. **[保護]** > **[DLPイベント]** に移動します。
3. 左上の **[フィルタ]** をクリックします。
4. ドロップダウンメニューから、機密カテゴリ、ワークロード、操作タイプ、ユーザー、およびチャネルを選択します。
   ドロップダウンメニューで複数の項目を選択できます。フィルタリング処理では、同じメニューの項目間に論理演算子ORが適用されますが、異なるメニューの項目間では論理演算子ANDが使用されます。
   たとえば、**PHI**と**PII**の機密カテゴリを選択すると、結果には、PHIまたはPII、あるいはその両方を含むすべてのイベントが返されます。機密カテゴリ**PHI**と**書き込みアクセス**操作を選択すると、両方のカテゴリに一致するイベントのみがフィルタリングされ、結果に表示されます。
5. **[適用]** をクリックします。
6. すべてのイベントを再度表示するには、**[フィルタ]**、**[デフォルトにリセット]**、**[適用]** の順にクリックします。

DLPイベントリストでイベントを検索するには

1. 上記の手順のステップ1〜2を繰り返します。
2. フィルタの右側にあるドロップダウンリストから、検索するカテゴリ（**送信者**、**宛先**、**プロセス**、**メッセージの件名**、**理由**）を選択します。
3. テキストボックスに、興味のあるフレーズを入力し、キーボードのEnterキーを押して確認します。
   入力したフレーズに一致するイベントのみがリストに表示されます。
4. イベントのリストをリセットするには、検索テキストボックスの **[X]** マークをクリックして、Enterキーを押します。

データフローポリシーの特定のルールに関連するイベントのリストを表示するには

1. Cyber Protectコンソールに管理者としてログインします。
2. **[保護]** > **[データフローポリシー]** に移動します。
3. 関心のあるポリシールールの名前の前にあるチェックボックスを選択します。
   必要に応じて、複数のポリシールールを選択できます。
4. **[イベントを表示]** をクリックします。
   ビューが **[保護]** > **[DLPイベント]** に切り替わり、選択したポリシールールに関連するイベントがリストに表示されます。

概要ダッシュボードのAdvanced Data Loss Preventionウィジェット

[概要] ダッシュボードには、データ漏洩防止など、Cyber Protectionサービスに関連する操作の概要を示すカスタマイズ可能なウィジェットが多数用意されています。**監視**以下の **[概要]**ダッシュボードに、次のAdvanced Data Loss Preventionウィジェットがあります。

- **機密データ転送** - 内部および外部受信者に対する機密データ転送処理の総数を示します。チャートは、許可のタイプ（許可、正当化、またはブロック）によって分類されます。このウィジェットでは、任意の時間範囲（1日、7日、30日、または当月）を選択してカスタマイズできます。

- **送信機密データカテゴリ** - 外部受信者に対する機密データ転送の総数を示します。チャートは、保護されたヘルス情報（PHI）、個人を特定できる情報（PII）、PCI DSS、機密扱い（Confidential）としてマーク、の各機密カテゴリに分類されます。
- **送信機密データの上位送信者** - 組織内から外部受信者への機密データ転送の総数と、転送数が最も多い上位5人のユーザー（転送数とともに）のリストが示されます。この統計には、許可された転送と正当化された転送の両方が含まれます。このウィジェットでは、任意の時間範囲（1日、7日、30日、または当月）を選択してカスタマイズできます。
- **ブロックされた機密データ転送の上位送信者** - ブロックされた機密データ転送の総数と、転送の試行回数が最も多い上位5人のユーザー（転送数とともに）のリストが示されます。このウィジェットでは、任意の時間範囲（1日、7日、30日、または当月）を選択してカスタマイズできます。
- **最近のDLPイベント** - 選択した時間範囲における最近のデータ漏洩防止イベントの詳細を示します。次のオプションを使用して、このウィジェットをカスタマイズできます。
  - **範囲（送信日）**（1日、7日、30日、または当月）。
  - **ワークロード**の名前
  - **処理のステータス**（許可、正当化、またはブロック）
  - **機密**（PHI、PII、機密、PCI DSS）
  - **宛先タイプ**（外部、内部）
  - **グループ化**（ワークロード、ユーザー、チャネル、宛先タイプ）

ウィジェットは、5分間隔でアップデートされます。ウィジェットには、クリックすることによって、問題を調査し、トラブルシューティングを実行できる要素が含まれています。ダッシュボードの現在の状態は、.pdf または/および .xlsx 形式でダウンロードできる他、電子メールで送信するようにも設定できます。

カスタム機密カテゴリ

カスタム機密データカテゴリにより、Advanced DLPに組み込まれたコンプライアンス規制関連のコンテンツ定義のカタログを拡張することができます。これは、組織固有の知的財産や機密データを保護するのに役立つ場合があります。

カスタム機密カテゴリを作成するには

1. Cyber Protectコンソールに管理者としてログインします。
2. **[保護]** > **[データ損失防止]** > **[データ分類]** に移動します。
3. **[機密カテゴリ]** を選択します。
4. ビルトインの情報（保護されたヘルス状態や個人を特定できる情報など）とカスタムの情報の両方について、機密カテゴリのリストが表示されます。
5. ウィンドウの右上にある **[機密カテゴリを作成]** をクリックします。
6. 次のウィンドウで、名前を入力します。
7. 新しいカスタム機密カテゴリは、デフォルトで常に無効になっています。すべてのパラメータを構成した後に、それらを有効にできます。
8. 新しい機密カテゴリを作成した後、そのコンテンツ検出ツールを設定する必要があります。矢印をクリックして新しい機密カテゴリのコンテンツを展開し、**[コンテンツ検出ツールを追加]** を選択します。

9. 次のウィンドウでは、既存のコンテンツ検出ツールを使用するか（名前の横のチェックマークをクリックし、右下の **[追加]** をクリック）、新しいツールを定義できます。
10. 新しい機密カテゴリを最初から作成する代わりに、既存の機密カテゴリのクローンを作成してそのパラメータを調整することで、ビルトインまたは既存のカスタム機密カテゴリを再利用することもできます。
    - 既存の機密カテゴリのクローンを作成するには、機密カテゴリの名前の横にあるチェックマークをクリックし、左上にある操作ドロップダウンメニュー（省略記号で表示）から **[クローン]** を選択します。一度に複数の項目を選択することで、複数の機密カテゴリのクローンを作成できます。
    - 次のウィンドウでは、各パラメータの横にあるチェックマークをクリックして、既存の機密カテゴリのどのパラメータを保持するかを選択できます。

注意
いずれかのテナント内でビルトインの機密カテゴリをコピーすると、同じ検出ツールで構成される新しい機密カテゴリが作成されます（コピーすると「カスタム」になります）。

新しいコンテンツ検出ツールを作成するには

1. Cyber Protectコンソールに管理者としてログインします。
2. **[保護]** > **[データ損失防止]** > **[データ分類]** に移動します。
3. **[コンテンツ検出ツール]** を選択します。
4. ビルトインとカスタム両方のコンテンツ検出ツールのリストが表示されます。
5. ウィンドウの右上にある **[コンテンツ検出ツールを作成]** をクリックします。
6. ドロップダウンメニューが表示され、作成する検出ツールの種類を選択できます。現時点では、**ファイルタイプ**のコンテンツ検出ツールのみが利用可能で、今後のアップデートでさらに多くのタイプが利用可能になります。
7. 次のウィンドウでは、コンテンツ検出ツールの構成を行います。

コンテンツ検出ツールのタイプ	説明
ファイルタイプのコンテンツ検出ツール	a. 2種類のリストがあります:**サポート対象のファイルタイプ**と**選択済みファイルタイプ**です。サポート対象のファイルタイプの右側にある「プラス」アイコンをクリックすると、選択済みのファイルタイプリストに移動します。また、ファイル名の横にあるチェックマークをクリックし、右上の **[選択済みを追加]** ボタンで複数のサポート対象のファイルタイプを選択できます。 b. 選択済みファイルタイプのリストからファイルのタイプを削除するには、そのファイル名の右にあるごみ箱アイコンをクリックします。また、チェックマークと **[選択済みを削除]** ボタンを使って、複数のファイルタイプを一括で削除できます。
キーワード	a. キーワードコンテンツ検出ツールを新規に作成する場合、ファイルからキーワードをインポートする必要があります。正常にインポートされた後は、新しいキーワードを既存のキー

コンテンツ検出ツールのタイプ	説明
コンテンツ検出ツール	ワードのリストに結合するか、既存のキーワードをインポートしたキーワードに置き換えることができます。 b. また、コンテンツ検出ツールで使用するキーワード一致の方式（リストのすべてのキーワードに一致、任意のキーワードに一致、または任意の数のキーワードに一致）を決定する必要があります。

8. 新しいコンテンツ検出ツールを最初から作成する代わりに、既存のコンテンツ検出ツール（ビルトインまたは既存のカスタム機密カテゴリ）のクローンを作成してそのパラメータを調整することで、コンテンツ検出ツールを再利用することもできます。
   - 既存のコンテンツ検出ツールのクローンを作成するには、コンテンツ検出ツールの名前の横にあるチェックマークをクリックし、左上にある操作ドロップダウンメニュー（省略記号で表示）から **[クローン]** を選択します。一度に複数の項目を選択することで、複数のコンテンツ検出ツールのクローンを作成できます。

注意
ビルトインのコンテンツ検出ツールをコピーすると、検出ツールがカスタム化されます。

組織マップ

注意
この機能には、企業管理者ユーザーのみがアクセスできます。

組織マップは、Advanced DLPによって傍受された、インスタントメッセージ、Eメール、またはその他の手段を通じてデータを転送するために使用されるユーザーとそのすべてのアカウントのデータを含むデータベースです。

組織マップは、Advanced DLPでユーザーグループを作成および管理し、Advanced DLPでユーザーおよびユーザーに関連付けられたアカウントを管理するための手段を提供します。ユーザーグループは、グループベースのDLPポリシー管理に使用できます。

組織マップを見つけるには

- Cyber Protect Cloudコンソールで、**[保護]**>**[DLP（データ損失防止）]** > **[組織マップ]** の順に移動します。

使用方法

注意
組織マップは、Advanced DLPモジュールが観察モードで動作している場合に入力されます。

DLPエージェントによって傍受されたデータ転送ごとに、以下の属性がバックエンドで収集されます。

属性	説明	UIのラベル
組織単位	手動で作成されたグループ。組織単位には、1つ以上ののネストされた組織単位を含めることができます。	グループ名（定義どおり）
セキュリティID	一意のセキュリティ識別子。	ユーザー詳細ページ > **[SID]**
	ユーザーのアカウント名に由来する、利用しやすい表示名。この名前は、組織マップで常に使用できるわけではありません。	**名前**
PC¥UserName	エンドポイント（ワークロード）のユーザー名。 ユーザー名は1つの組織単位にのみ割り当てることができます。	**ユーザー名**
デバイス（ワークロード）	エンドポイント（ワークロード）の名前。	**ワークロード**
アカウント	ユーザーのインスタントメッセージとEメールによる通信に使用され、DLPエージェントによって傍受されたアカウント。例えば、ユーザー名「PC¥John」がEメールを送信するためにjohn@gmail.comを使用することをエージェントが検出した場合、 このアカウントはPC¥Johnのユーザー名にリンクされます。	**アカウント**

組織マップでは、アカウント、ユーザー、グループの表示と検索、グループの作成、編集、削除ができます。

特定のアカウントを検索するには

インシデント調査の一環として、管理者ユーザーは、潜在的なデータ侵害に関与した特定のア カウントの所有者を見つける必要が生じる場合があります。

1. Cyber Protect Cloudコンソールで、**[保護]**>**[DLP（データ損失防止）]** > **[組織マップ]** の順に移動します。
2. ユーザーリストの上にある **[検索]** テキストボックスに、アカウントを入力するか貼り付けます。
   リストは、入力にしたがって絞り込まれます。

特定のユーザー名を検索するには

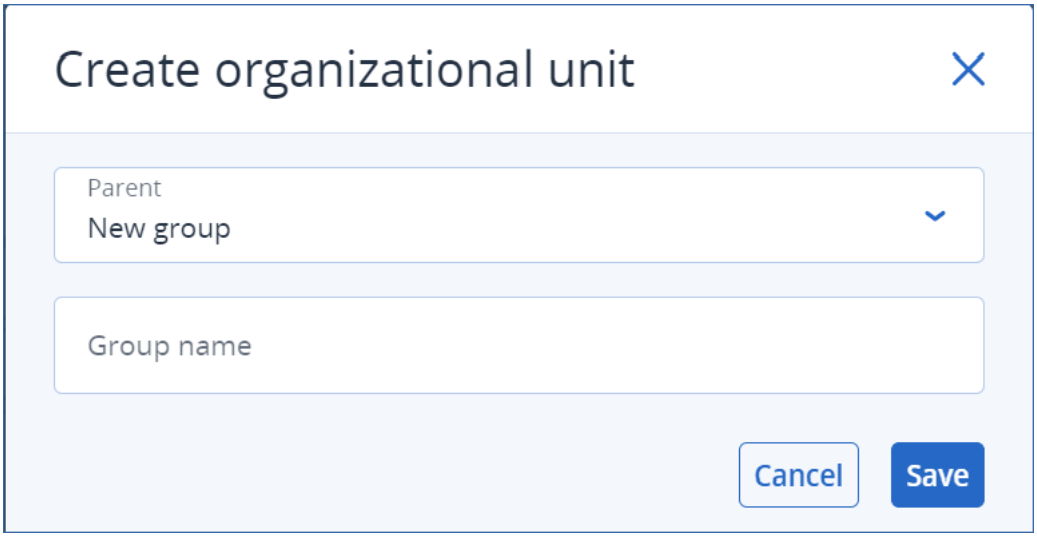
1. Cyber Protect Cloudコンソールで、**[保護]**>**[DLP（データ損失防止）]** > **[組織マップ]** の順に移動します。
2. 特定のグループで検索するには、リストのグループ名をクリックします。
3. ユーザーリストの上にある **[検索]** テキストボックスに、ユーザー名を入力するか貼り付けます。
   リストは、入力にしたがって絞り込まれます。

特定のユーザー名が使用しているアカウントを表示するには

1. ユーザーリストでユーザーを探します。
2. ユーザー行の末尾にある3つの点をクリックし、**[表示]** を選択する。
3. ユーザー詳細ダイアログで、**[関連アカウント]** セクションを探します。
4. [説明] テキストボックスにコメントを追加できます。

ユーザーグループを作成するには

1. Cyber Protect Cloudコンソールで、**[保護]**>**[DLP（データ損失防止）]** > **[組織マップ]** の順に移動します。
2. グループリストの左下のセクションで、**[グループの作成]** をクリックします。
   [組織単位（OU）を作成する] ダイアログが開きます。



3. [親] ドロップダウンメニューで新しいグループのコンテキストを選択します。

注意
後で親を変更することはできません。グループはこのコンテキストにネストされたままになります。

4. グループ名を入力し、**[保存]** をクリックします。

ユーザーをグループに追加するには

1. Cyber Protect Cloudコンソールで、**[保護]**>**[DLP（データ損失防止）]** > **[組織マップ]** の順に移動します。
2. ユーザーリストで追加したいユーザーを探し、ユーザー行の先頭にあるチェックボックスを選択します。
   ユーザーリストの上に **[選択したものを移動する]** ボタンと **[選択項目を削除]** ボタンが表示されます。
3. **[選択したものを移動する]** をクリックします。
   [ユーザーを移動する] ダイアログが開きます。
4. 選択したユーザーの新しい親を選択し、**[保存]** をクリックします。

注意
ユーザーは1つのグループにのみ属すことができます。

ユーザーに関連付けられているアカウントを削除するには

1. ユーザーリストでユーザーを探します。
2. ユーザー行の末尾にある3つの点をクリックし、**[表示]** を選択する。
3. ユーザー詳細ダイアログで、**[関連アカウント]** セクションを探します。
4. 削除したいアカウントを探し、その横にある3つの点をクリックします。
5. ドロップダウンリストで **[削除]** を選択します。

ユーザーグループの名前を変更するには

1. Cyber Protect Cloudコンソールで、**[保護]**>**[DLP（データ損失防止）]** > **[組織マップ]** の順に移動します。
2. グループ名の横にある3つの点をクリックし、**[名前の変更]** をクリックします。

ユーザーグループを削除するには

1. Cyber Protect Cloudコンソールで、**[保護]**>**[DLP（データ損失防止）]** > **[組織マップ]** の順に移動します。
2. グループ名の横にある3つの点をクリックし、**[削除]** をクリックします。
   グループのすべてのユーザーが親エンティティに移動します。

既知の問題と制限事項

- [DEVLOCK-4028] Zoomデスクトップエージェントのグループチャットが制御できない。
- [DEVLOCK-4016] GMX Web MailとWeb.de Mailで、ドラフト作成時にフレンドリ名と送信者IDがキャプチャされない。
- [DEVLOCK-4447] naver.com WebMailでドラフトを作成する場合、正当化ダイアログが表示されない。
- [DEVLOCK-1033] DeviceLockDriver: IRP_MN_QUERY_DEVICE_RELATIONSの処理中にデッドロックが発生し、DRIVER_POWER_STATE_FAILUREのバグが確認される場合がある。

エンドポイント検知と応答（EDR）

注意
この機能は、Advanced Security + EDR保護パックの一部であり、さらにサイバープロテクションサービスにも含まれています。なお、保護計画にEDR機能を追加する場合、追加料金が発生する場合があります。

EDR機能では、気づかれなかった攻撃を含め、ワークロード上の不審なアクティビティが検知されます。EDR機能により生成されたインシデントでは、各攻撃の概要がステップバイステップで説明されており、攻撃がどのように発生したか、またどのように再発を防止するかを理解するのに役立ちます。攻

撃の各ステージに関する分かりやすい説明を提供することで、攻撃の調査に費やす時間を数分に短縮することができます。

エンドポイント検知と応答（EDR）が必要な理由

サイバー脅威と悪意ある攻撃が拡大し続ける今日、予防措置はもはや100%の保護を保証するものではありません。一部の攻撃は予防レイヤを完全に突破し、ネットワークへの侵入に成功します。従来のソリューションでこのような事態が発生した場合、攻撃者は何日も、何週間も、あるいは何ヵ月も、現在の環境に自由に入り込むことができます。

既存のEDRソリューションは、攻撃者を迅速に発見し排除することで、こうした「サイレント障害」の防止に役立っています。しかし、通常はセキュリティに関する高度な専門知識や高価なSecurity Operation Center（SOC）アナリストが必要とされるため、インシデントの分析に非常に時間がかかる場合があります。

Acronis Advanced Security + EDR機能では、このような限界を克服するとともに、気づかなかった攻撃を検知し、攻撃が発生した原因や再発防止策を理解できるようサポートを提供します。その結果、攻撃の調査に費やす時間を短縮することができます。

EDRが必要な理由:

- **完全な可視性**:気づかれなかった攻撃についても、何がどのように生じたかを把握できます。また、各攻撃の進展状況は、ステップバイステップで視覚的にマッピングされ（最初の侵入ポイントから、ターゲットデータや流出したデータの参照まで）、インシデントのスコープと影響を迅速に把握することができます。詳細については、"サイバーキルチェーンでインシデントを調査する方法"（882ページ）を参照してください。
- **調査時間を最小化**:インシデントの調査時間を数時間からわずか数分に短縮できます。EDRにより、攻撃の各ステップの説明が分かりやすい言葉で提供されるため、コストのかかる専門家や追加人員の必要性を削減することができます。詳細については、"インシデントを調査する"（882ページ）を参照してください
- **ワークロードの既知の脅威を確認する**:マルウェアによる脅威、脆弱性、データ保護に影響を及ぼす可能性のあるその他の種類のグローバルイベントをワークロードから自動的に検索できます。これらの脅威はIOC（Incident of Compromise）と呼ばれ、Cyber Protection Operations Center（CPOC）から受信した脅威データに基づきます。詳細については、"ワークロード上の既知の攻撃によるIOC（Indicators of Compromise）を確認する"（892ページ）を参照してください。
- **インシデントへの対応を迅速化**:侵入後のすべてのアクティビティやキルチェーンの各ステップの詳細にアクセスすることで、各攻撃ポイントを修復するためのさまざまな操作を実行することができます。一例として、リモート制御やフォレンジックバックアップ（この機能は、早期利用版では使用できません）を使った調査、ワークロードの隔離、マルウェアプロセスの強制終了などが可能です。また、Cyber Disaster Recovery Cloudを使用して処理をリカバリできます。詳細については、"インシデントを修復"（895ページ）を参照してください。
- **セキュリティ状態に関する信頼性の高いレポートを作成する**:EDRを有効にすることで、サイバー攻撃が業務に与える不安や恐怖の多くを取り除くことができます。また、インシデント関連の情報は180日間保存され、監査に利用することができます。

機能

エンドポイント検知と応答（EDR）には、以下のような機能が含まれています。

- 情報漏洩時にアラート通知を受け取る
- インシデントページでインシデントを管理
- 攻撃手法を分かりやすく可視化
- 推奨事項と修復手順
- 脅威フィードを使用して、一般に公開されている、ワークロードに対する攻撃を確認
- 視認性に優れたダッシュボード概要
- セキュリティイベントを180日間保存

情報漏洩時にアラート通知を受け取る

EDRは、インシデントが発生するとアラートで通知します。これらのアラートは、Cyber Protectコンソールのメインメニューでハイライト表示されます。**[インシデントを調査]** ボタンをクリックすると、インシデント調査画面（別名: サイバーキルチェーン）にリダイレクトされ、アラートを調査することができます。

詳細については、"インシデントを確認する"（874ページ）を参照してください。

インシデントページでインシデントを管理

EDRでは、インシデントページ（Cyber Protectコンソールの保護メニューからアクセス可能）ですべてのインシデントを管理できます。インシデントページでは、要件に応じてフィルタリングを実行できます。インシデントの重大度、影響を受けるワークロード、陽性レベルなど、現在の状況をすばやく簡単に把握できます。また、サイバーキルチェーンに直接移動して、ノードごとに攻撃の手法を表示することもできます。

インシデントの詳細については、"インシデントを確認する"（874ページ）を参照してください。

攻撃手法を分かりやすく可視化

EDRは、攻撃の実態を分かりやすい視覚的な形式で表現したものです。これにより、セキュリティ担当者でなくても、攻撃の目的と重大度を把握することができます。EDRにより、攻撃がどのように発生したかを詳細に把握できます。Security Operation Center（SOC）サービスやセキュリティに特化した人員を配置する必要はありません。以下の情報が提供されます。

- 攻撃者の侵入経路
- 攻撃者が痕跡を隠蔽した方法
- 発生した損害
- 攻撃の拡散方法

詳細については、"サイバーキルチェーンでインシデントを調査する方法"（882ページ）を参照してください。

推奨事項と修復手順

EDRにより、ワークロードに対する攻撃に対処するための推奨操作を明確かつ簡単に実行できるようになります。攻撃を迅速に解決するには、**[インシデント全体を修復]** ボタンをクリックします。インシデントに及ぶ影響を軽減するための推奨手順が表示され、それに従うことができます。これらの推奨手順により、攻撃の影響を受けた処理を迅速に再開できます。一方、よりきめ細かい改善策を講じたい場合は、各ノードに移動して、関連する操作を実行して修復することができます。

詳細については、"インシデントを修復"（895ページ）を参照してください。

脅威フィードを使用して、一般に公開されている、ワークロードに対する攻撃を確認

EDRには、ワークロードに対する脅威フィードに含まれる既存かつ既知の攻撃を確認する機能があります。これらの脅威フィードは、Cyber Protection Operations Center（CPOC）から受け取った脅威データに基づいて自動的に生成されます。EDRにより、脅威がワークロードに影響を与えているかどうかを確認して、脅威を無効化するために必要な操作を適用できます。

詳細については、"ワークロード上の既知の攻撃によるIOC（Indicators of Compromise）を確認する"（892ページ）を参照してください。

視認性に優れたダッシュボード概要

EDRにより、Cyber Protectコンソールのダッシュボードでさまざまな統計情報が提供されます。次の情報が表示されます:

- 調査が必要なインシデントの数など、現在の脅威の状況。
- 考えられる攻撃手法（攻撃の重大度別）。
- クローズ済みインシデントの効率性。
- カスタマーの攻撃に使用される、もっとも効率的なタクティクス。
- ワークロードのネットワーク状態、つまり、孤立しているか、接続されているか。

セキュリティイベントを180日間保存

EDRは、ワークロードとアプリケーションのイベントを収集し、180日間保存します。180日以前のイベントは削除されます（イベントの削除は、ストレージスペースではなく、期間に基づいて行われます）。EDRをオフにした場合でも、ワークロードで過去に収集されたイベントはすべて保持され、インシデントの調査に利用できます。

ソフトウェア要件

エンドポイント検知と応答（EDR）は、以下のオペレーティングシステムをサポートしています。

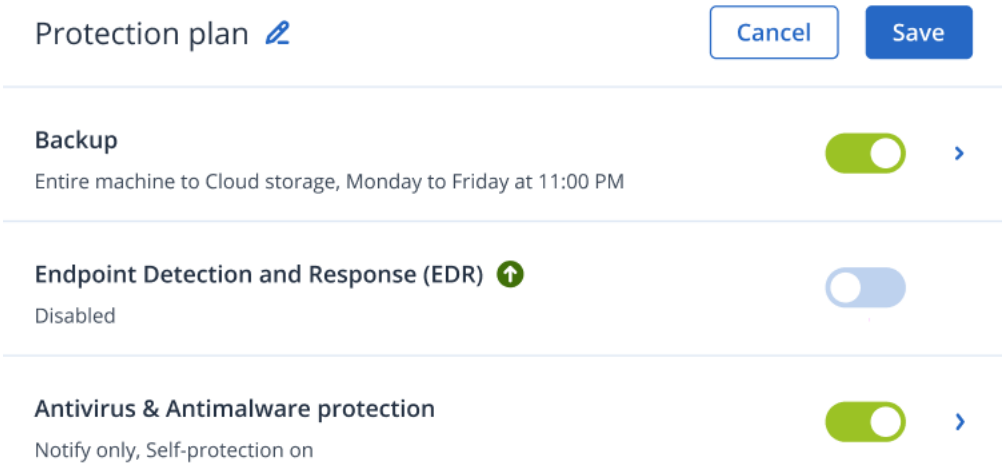
- Microsoft Windows 7 Service Pack 1以降
- Windows Server 2008 R2以降

エンドポイント検知と応答（EDR）機能を有効にする

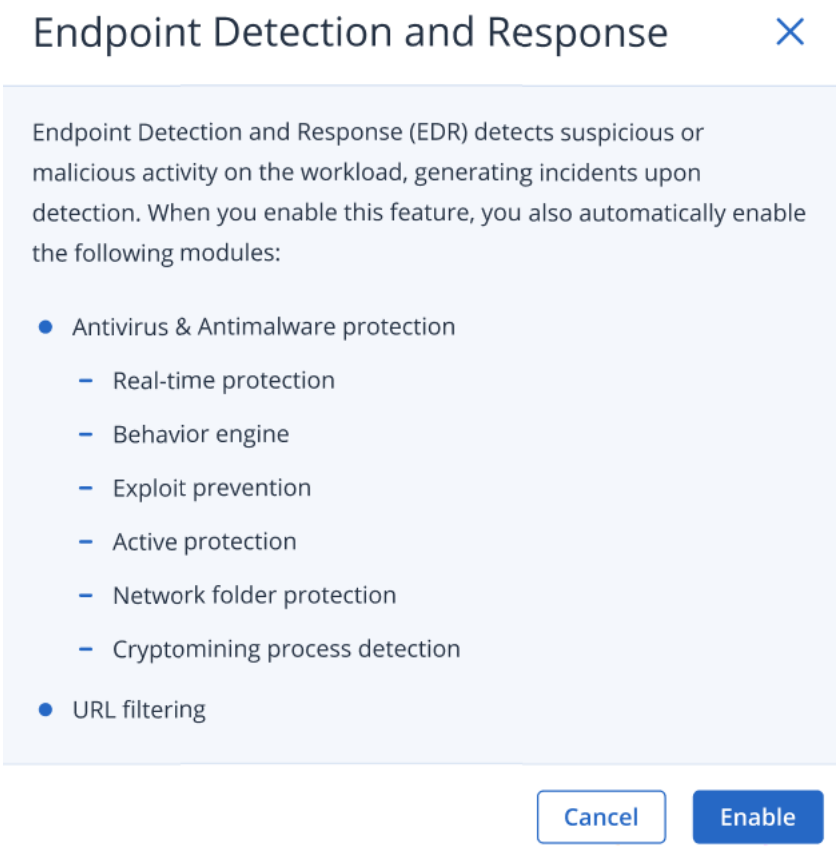
いずれの保護計画でもEDRを有効にすることができます。

EDRを有効化するには

1. Cyber Protectコンソールで、**[管理]** > **[保護計画]** に移動します。
2. 表示されたリストから該当する保護計画を選択し、右サイドバーで **[編集]** をクリックします。
   または、新しい保護計画を作成し、次の手順に進むこともできます。保護計画との連携の詳細については、"保護計画とモジュール"（209ページ）を参照してください。
3. 保護計画のサイドバーで、モジュール名の横にあるスイッチをクリックして、**エンドポイント検知と応答（EDR）**モジュールを有効にします。



4. 表示されたダイアログで、**[有効化]** をクリックします。なおEDRを有効にすると、表示されるダイアログに示されている通り、他の保護モジュールも有効になります。



注意
Active Protection、**振る舞い検知エンジン**、**エクスプロイト防止**、**URLフィルタ処理**のいずれかが**オフ**になっている場合、**エンドポイント検知と応答（EDR）**も**オフ**に切り替わります。

5. 選択した追加パックに応じて、保護計画の実行に必要な保護パックのリストに、下図のような**Advanced Security + EDR**パックアイコンが追加されます。

エンドポイント検知と応答（EDR）の使用方法

EDRにより、気づかれなかった攻撃を検知し、攻撃がどのように発生したか、またどのように再発を防止するかを理解できるようになります。攻撃の各ステージに関する分かりやすい説明を提供することで、攻撃の調査に費やす時間を数分に短縮することができます。

下の表は、EDRを使用する際の一般的なワークフローを説明したものです。最初に新しいインシデントの確認と優先順位付けを行い、サイバーキルチェーンにおいて追加の調査を行って、関連する修復操作を適用します。

手順	EDRの使用方法
手順1:インシデントを確認	EDRのインシデントリストで: • 組織のセキュリティ状況を把握する: どの程度のインシデントを調査する必要があるのか？ • もっとも重大なインシデントを把握し、その重大度に応じて調査の優先順位を決定します。 • どのインシデントが新規であるか、または進行中であるかを把握します。
手順2:インシデントを調査	EDRサイバーキルチェーンで: • 攻撃者の目的を把握し、使用される攻撃手法を確認します。 • インシデントが実際に悪意に基づく攻撃であかどうかを検証します。 • 脅威フィードがワークロードに影響を及ぼしているかどうかを検証します。 • インシデントに既に適用されている対応操作を確認できます。
手順3:インシデント全体を修復	該当するEDRの修復セクションにおいて: • グローバルな対応操作を適用することで、インシデント全体を迅速かつ容易に修復できます。 • インシデント内の個別の攻撃ポイントを修復します。 • 攻撃（または将来の攻撃）の拡散や、まだ攻撃者のターゲットになっていないワークロードへの影響を防ぐための操作を適用します。

インシデントを確認する

エンドポイント検知と応答（EDR）により、ワークロード上の予防操作（またはマルウェア）と疑わしい検出の両方を含むインシデントリストが提供されます。インシデントリストでは、ワークロードに影

響を及ぼしている攻撃や脅威（まだ軽減されていない脅威も含む）の概要をすばやく確認できます。

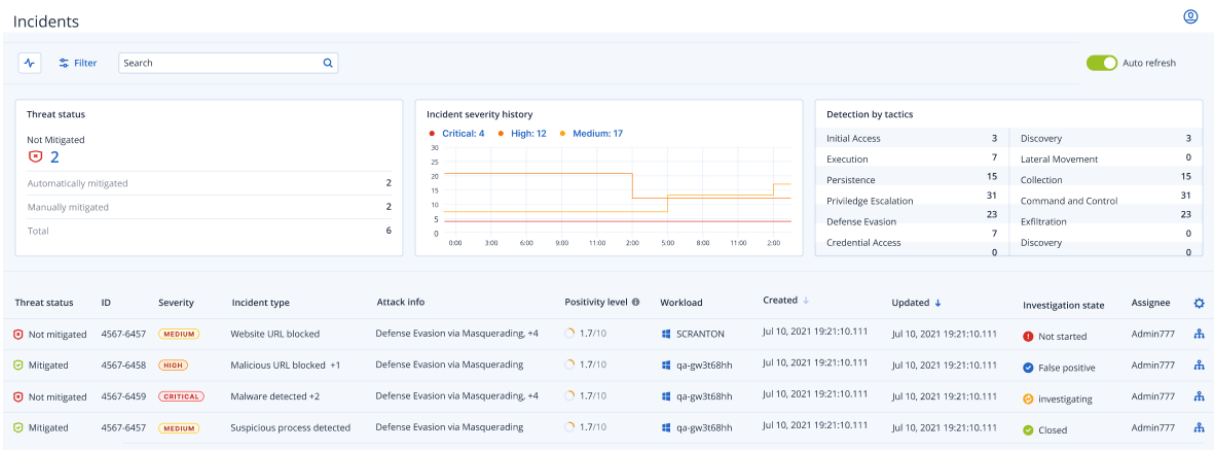
インシデントリストから、以下を簡単に判断できます。

- 組織のセキュリティ状況: どの程度のインシデントを調査する必要があるのか？
- もっとも重大なインシデントを把握し、その重大度に応じて調査の優先順位を決定する。
- どのインシデントが新規であるか、または進行中であるか。

注意
パートナー管理者としてログインすると、各カスタマーの個別のインシデントビューにアクセスしなくても、すべてのカスタマーからのインシデントを統合した単一の画面ですべてのEDRインシデントを表示できます。追加の **[カスタマー]** 列が表示され、各インシデントが属するカスタマー名が含まれます。さらに、**[概要]** ダッシュボードに表示されるウィジェットには、すべての顧客にわたって集約されたメトリクスデータが表示されます。

インシデントリスト（下図を参照）には、Cyber Protectコンソールの **[保護]** メニューからアクセスできます。インシデントリストのインシデントを確認する方法については、"現在軽減操作が適用されていないインシデントを表示"（878ページ）を参照してください。インシデントが作成されるタイミングについては、「インシデントとは具体的にはどのようなものなのか？」を参照してください。

注意
ワークロードでMDR（Managed Detection and Response）が有効になっている場合、追加の**MDRチケット**列が表示されます。この列には、MDRベンダーから提供されたチケット番号が表示されます。



注意
インシデント通知を受け取るには、Cyber Protectコンソールが開いている必要があります。

インシデントとは具体的にはどのようなものなのか？

インシデント（またはセキュリティインシデント）は、少なくとも1つの予防ポイントまたは不審な検出ポイント（またはその組み合わせ）のコンテナと考えることができます。インシデントには、単一の攻撃に関するすべての関連イベントと検出内容が含まれています。セキュリティインシデントには、発生した事象をより深く理解するために、良性の事象が含まれている場合もあります。

これにより、攻撃イベントを1つのインシデントとしてまとめて表示し、攻撃者が行った論理的な手順を把握できます。また、攻撃の際の調査時間の短縮にもつながります。

EDRが保護計画で有効になっていれば、セキュリティインシデントは以下の場合に作成されます。

- **予防レイヤで何らかの処理が停止される:**これらのインシデントは、保護計画の設定に従って、システムによって自動的にクローズされます。ただし、マルウェアが停止する前に、具体的に何が発生したかを調査することができます。例えば、ランサムウェアはファイルの暗号化を開始した時点で停止されますが、それ以前に資格情報を窃取したり、サービスをインストールしていたりする可能性があります。
- **EDRにより不審なアクティビティが検出される**:これらは、調査して修正すべき検出事項です。視認性が強化されたサイバーキルチェーン（詳細については"サイバーキルチェーンでインシデントを調査する方法"（882ページ）を参照）を確認することで、関連する修正操作を簡単に適用できます。

緊急に対応する必要があるインシデントの優先順位付け

Cyber Protectコンソールのインシデントリストは、コンソールの **[保護]** メニューからいつでもアクセスできます。インシデントリストでは、攻撃や脅威の概要を一目で確認できます。これにより注意が必要なインシデントの優先順位を判断できます。

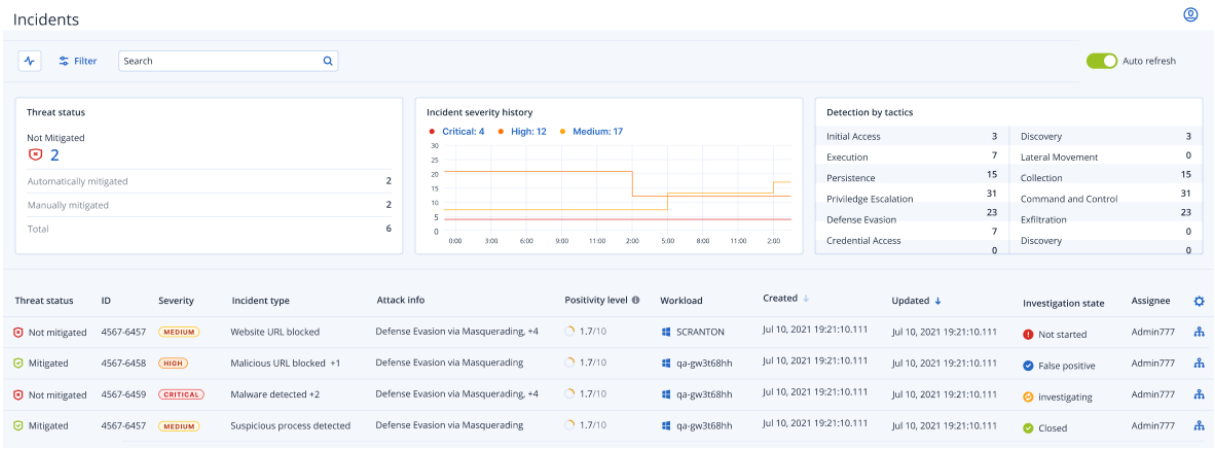
重要
ワークロードの安全性を確保するために、常に、進行中のインシデントや軽減操作が適用されていないインシデントを分析し、優先順位を付けます。

緊急の対応が必要なセキュリティインシデントを判別する方法

インシデントリストでは、リストアップされたインシデントを分析し、注意が必要なものに優先順位を付けることができます。次の操作を実行できます。

- 現在軽減操作が適用されていないインシデントを表示:インシデントリストから、現在進行中の攻撃があるかどうかをすばやく把握できます。**[脅威のステータス]** 列で示されるように、軽減操作が適用されていないインシデントは、すぐに調査する必要があります（デフォルトでは、インシデントリストにはこれらのインシデントが表示されるようにフィルタがかけられています）。
- インシデントのスコープと影響を把握する:新たに発生した攻撃や進行中の攻撃のフィルタリングを実行して、フィルタリング済みインシデントの重大度や業務への影響を把握します。

もっとも重要なインシデントの細分化リストを作成することで、インシデントを詳細に分析し、特定のインシデントや、攻撃者が目的を達成するために使用した技術をより深く理解することが可能になります。詳細については、"インシデントの詳細を分析する"（880ページ）を参照してください。

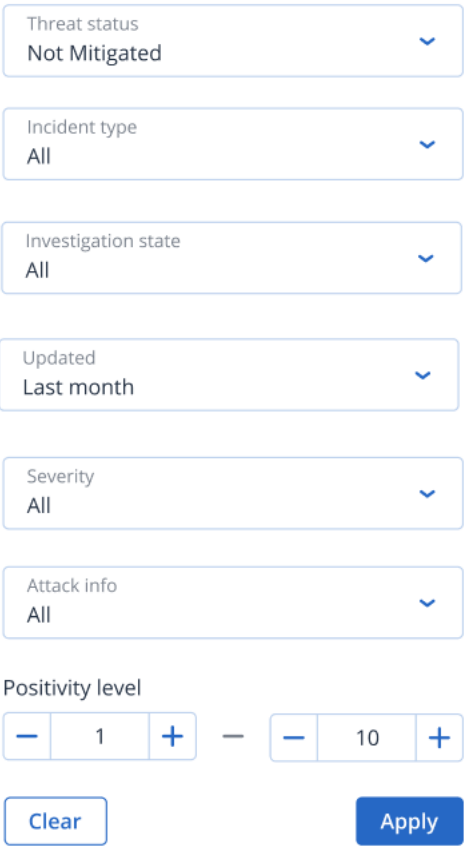


注意

インシデントリストはデフォルトでは、[**アップデート**] 列に応じてソートされます。この列には、インシデント内で記録された新しい検出により、インシデントが最後にアップデートされた日付と時刻の詳細が記載されています。既存のインシデントの場合、以前にインシデントがクローズされていたとしても、いつでもアップデート可能です。要件に応じて、新たな攻撃や進行中の攻撃を表示するよう、リストにフィルタを適用することもできます（以下の手順を参照）。

インシデントにフィルタを適用するには

1. インシデントリストの上部で、[**フィルタ**] をクリックして、表示されたインシデントのリストにフィルタを適用します。例えば、[**作成済み**] フィールドで開始日と終了日を選択すると、インシデントリストとウィジェットには、定義された期間中に作成された関連するインシデントが表示されます。



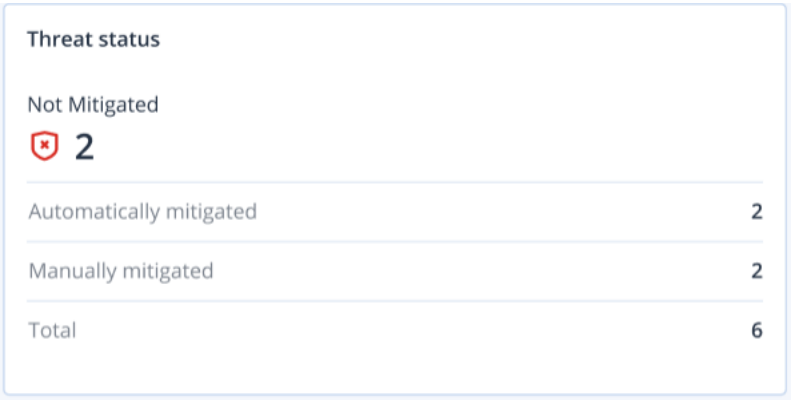
2. 完了したら、**[適用]** をクリックします。

現在軽減操作が適用されていないインシデントを表示

[脅威のステータス] 列には、インシデントの現在の脅威ステータスが表示され、インシデントが**軽減済み** または**未軽減**のいずれであるかを確認できます。脅威ステータスはEDRによって自動的に定義されます。軽減操作が適用されていないインシデントは、できるだけ早く調査する必要があります。

表示されたインシデントリストは、フィルタを適用することでさらに絞り込むことができます。例えば、脅威のステータスと特定の重大度レベルに従ってリストにフィルタを適用する場合は、関連するフィルタオプションを選択します。確認したいインシデントにフィルタを適用した後、インシデントの調査を実行できます（"インシデントを調査する"（882ページ）を参照）。

また、下図のような **[脅威のステータス]** ウィジェットで、現在の脅威ステータスを一目で把握できます。このウィジェットに表示されるデータは、適用済みのフィルタで絞り込まれていることに注意してください（"インシデントにフィルタを適用するには"（877ページ）を参照）。



インシデントのスコープと影響を把握する

重大度、**攻撃情報**、**陽性レベル**の列を確認することで、インシデントのスコープと影響をすばやく理解することができます。前述のように、現在進行中のインシデントを判別した後、これらの追加列をフィルタリングして以下の操作を実行できます。

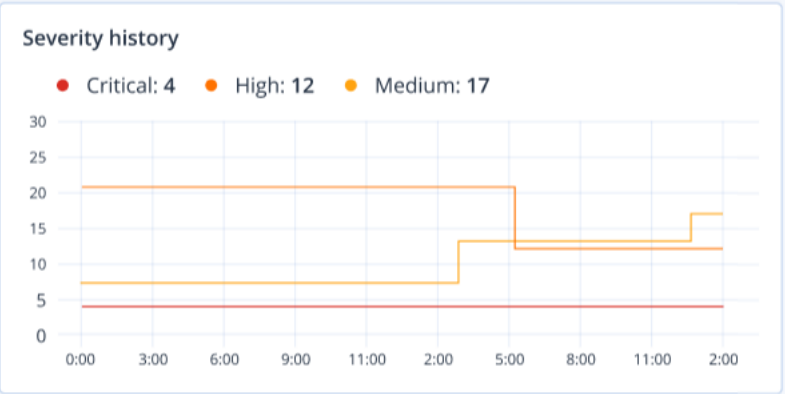
- **[重大度]** 列で、どのインシデントがより重要であるかを確認します。インシデントの重大度は、**重大**、**高**、**中**のいずれかになります。
  - **重大**:現在の環境では、重要なホストが危険にさらされる危険性があり、悪意のあるサイバーアクティビティが実行される深刻なリスクが存在します。
  - **高**:現在の環境に甚大な被害を及ぼす危険性のある、悪意あるサイバーアクティビティが実行される深刻なリスクが存在します。
  - **中**:悪意あるサイバーアクティビティのリスクが高まっています。

  注意
  EDRアルゴリズムが重大度を判定する際には、ワークロードの種類だけでなく、攻撃の各ステップのスコープも考慮されます。例えば、資格情報の窃取に関連するステップを含むインシデントは、**重大**に設定されます。

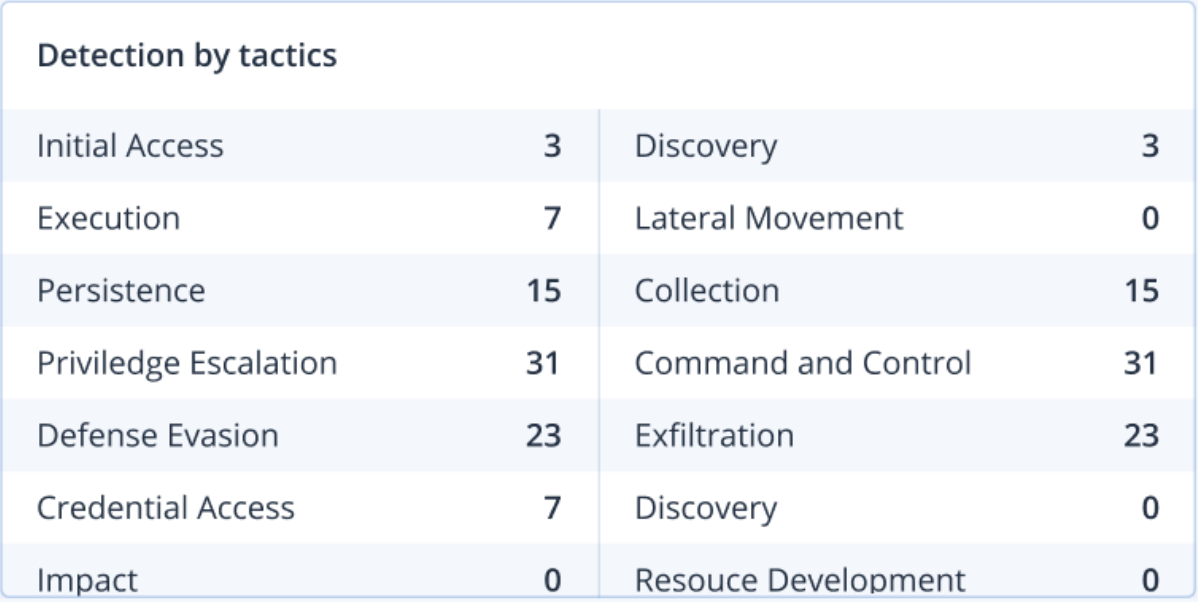
- **[インシデントタイプ]** 列でインシデントが作成された理由がわかります。インシデントタイプには、以下のいずれか1つ以上を含めることができます。
  - **ランサムウェアが検出されました**
  - **マルウェアが検出されました**
  - **不審なプロセスが検出されました**
  - **悪意のあるプロセスが検出されました**
  - **不審なURLがブロックされました**
  - **悪意のあるURLがブロックされました**
- **[攻撃情報]** 列でどの攻撃手法が使われているかを判断し、攻撃に共通のテーマやパターンがあるかどうかを把握します。
- インシデントが実際の悪意ある攻撃である可能性を確認します。**[陽性レベル]** の列には1～10のスコアが示されます（スコアが高いほど、実際の悪意ある攻撃の可能性が高くなります）。

早急な対応が必要なインシデントが見つかった場合、そのインシデントを調査できます（"インシデントを調査する"（882ページ）を参照）。

また、**[重大度の履歴]** と **[タクティクス別の検出]** ウィジェットを使用して、重大度と攻撃手法の概要をすばやく確認することもできます。



[タクティクス別の検出] ウィジェットには、使用されたさまざまな攻撃手法が表示されます。前回指定した時間範囲に増加している場合は緑色の数値で、減少している場合は赤色の数値で表示されます。このウィジェットでは、フィルタリングされたインシデントのすべての目的を集約して表示できるため、カスタマーへの影響をすばやく把握できます。

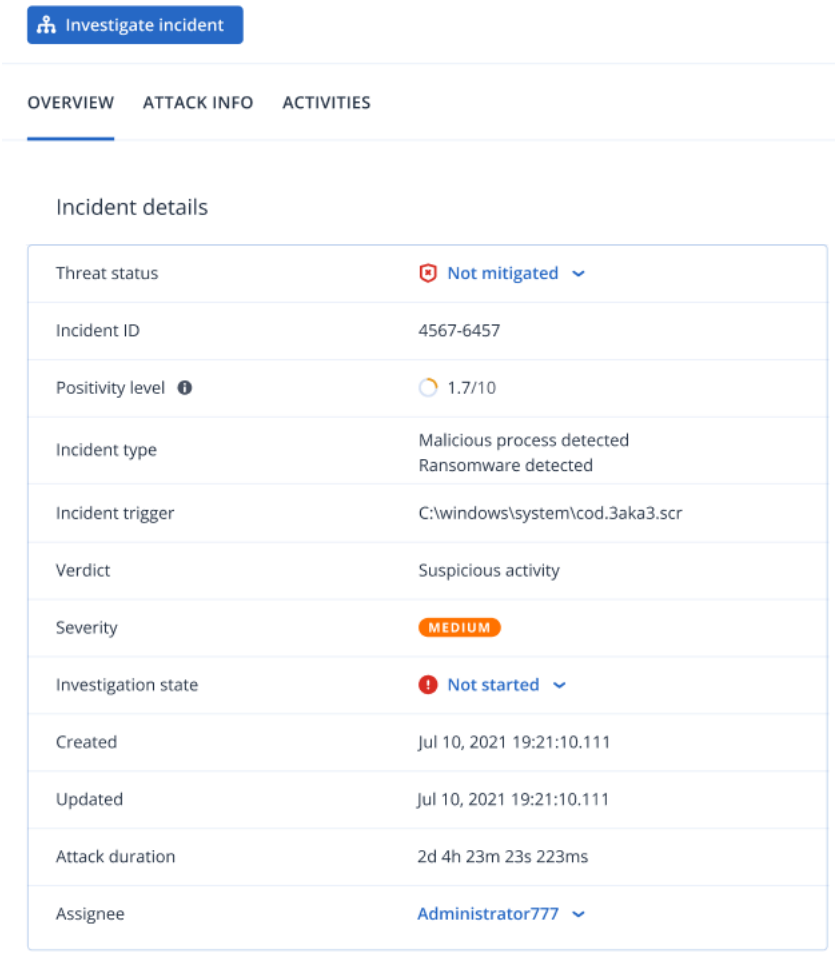


インシデントの詳細を分析する

インシデントのレビューステージでは、エンドポイント検知と応答（EDR）のインシデントリストから各インシデントの詳細を分析することも可能です。これらの詳細により、インシデント全体を掘り下げ、発生した時間や状況を把握できます。さらに、インシデントを特定のユーザーに割り当てて調査を依頼したり、調査ステータスを設定したりすることもできます。

インシデントの詳細を分析するには

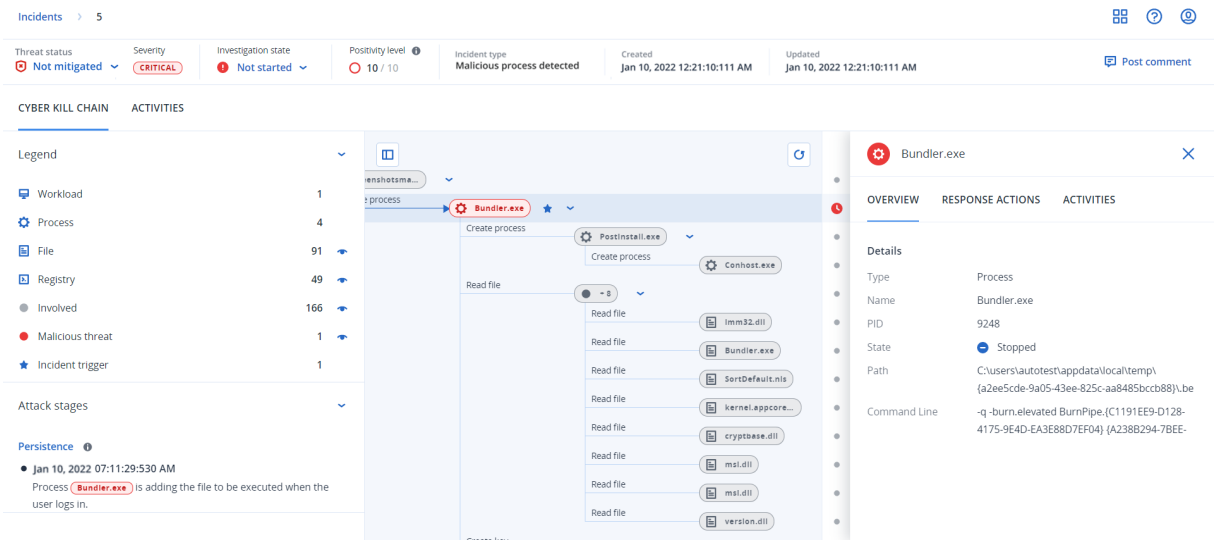
1. Cyber Protectコンソールで、**[保護]** > **[インシデント]** に進みます。インシデントのリストが表示されます。
2. 確認したいインシデントをクリックします。選択したインシデントの詳細が表示されます。
3. 表示された **[概要]** タブで、現在の脅威のステータスや重大度など、インシデントとワークロードの詳細を確認できます。また、**調査ステータス**（**調査中**、**未開始**（デフォルト）、**偽陽性**、**閉鎖済み**のいずれかを選択）、およびインシデントを割り当てるユーザー（**[割り当て先]** ドロップダウンリストで、関連ユーザーを選択）を定義することもできます。



4. **[攻撃情報]** タブをクリックして、攻撃の詳細と攻撃に使用された技術を確認します。各攻撃方法の横にあるリンクをクリックすると、MITRE.orgでその技術に関する詳細情報を確認できます。
5. **[アクティビティ]** タブをクリックして、インシデントを軽減するためサイバーキルチェーンで実行された操作を確認します。詳細については、"サイバーキルチェーンでインシデントを調査する方法"（882ページ）を参照してください。
   例えば、ワークロードにパッチが適用された場合、どのユーザーがパッチを起動し、どれくらいの時間がかかったか、パッチの実装中に発生したエラーは何かなどを確認できます。
6. **[インシデントを調査]** をクリックすることで、サイバーキルチェーンにアクセスし、インシデントをノードごとに調査できます。詳細については、"サイバーキルチェーンでインシデントを調査する方法"（882ページ）を参照してください。

インシデントを調査する

エンドポイント検知と応答（EDR）では、攻撃のステージや攻撃によって影響を受けるオブジェクト（プロセス、レジストリ、スケジュールされたタスク、ドメイン）すべてを含め、インシデント全体を調査できます。これらの対象は、分かりやすいサイバーキルチェーンのノードで表現されます（下図を参照）。サイバーキルチェーンにより、いつ、何が起こったかを迅速に把握することができます。



攻撃の各ステップをサイバーキルチェーンで確認し、インシデントがどのように、そしてなぜ発生したかを詳細に把握できます。サイバーキルチェーンでは、攻撃の各ステップが分かりやすい文章とグラフで説明されており、調査時間を短縮できます。

インシデントの範囲と影響を迅速に理解し、攻撃の進展をMITREフレームワークにマッピングできます。攻撃の各ステップで何が起こったかを分析できます。例えば以下の情報が得られます。

- エントリの開始点
- 攻撃の実行方法
- 発生した権限エスカレーション
- 検出回避技術
- 他のワークロードへのラテラルムーブメント
- 資格情報の窃取
- 流出の試行

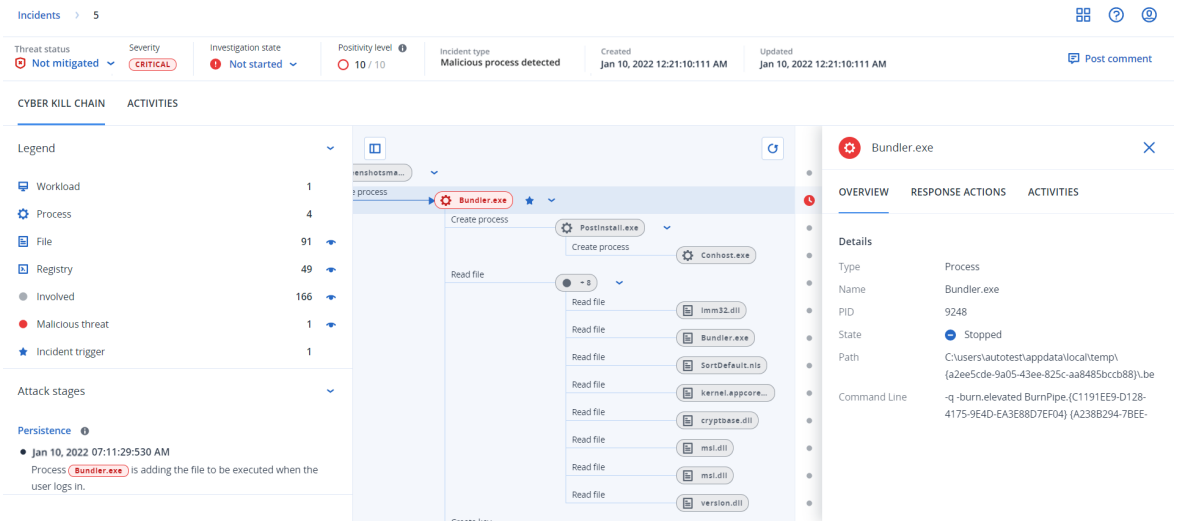
注意
プロセス、レジストリ、スケジュールされたタスク、ドメインなど、攻撃で影響を受けた各オブジェクトは、サイバーキルチェーンのノードで表示されます。

サイバーキルチェーンでインシデントを調査する方法

サイバーキルチェーンにおける攻撃の個別のステップを調査できます。サイバーキルチェーンの分かりやすい文章とグラフを活用して、攻撃の各ステップを把握し、調査時間を短縮できます。

サイバーキルチェーンで調査を開始するには

1. Cyber Protectコンソールで、**[保護]** > **[インシデント]** に進みます。
2. 表示されたインシデントのリストで、調査するインシデントの最右列の  をクリックします。選択したインシデントのサイバーキルチェーンが表示されます。



3. ページ上部の脅威ステータスバーで、インシデントの概要を確認できます。脅威ステータスバーには、以下の情報が表示されます。
   - 現在の脅威ステータス:脅威ステータスは、システムによって自動的に定義されます。**軽減操作が適用されていない**インシデントは、できるだけ早く調査する必要があります。

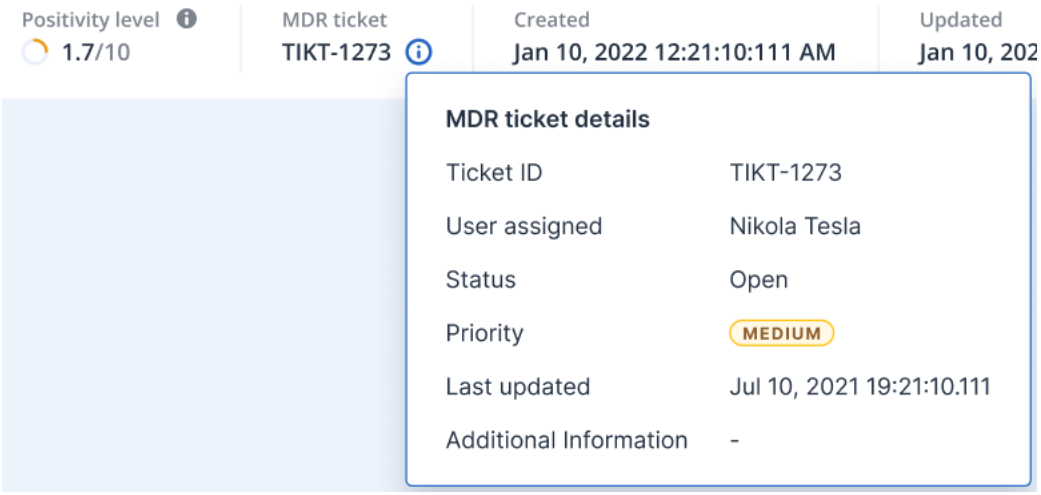
     重要
     バックアップからの復元が正常に完了した場合、またはすべての検出項目がプロセスの停止、隔離、またはロールバック操作によって正常に修復された場合、インシデントは**軽減済み**に設定されます。

     バックアップからの復元が正常に完了しなかった場合、または少なくとも1件の検出項目でプロセスの停止、隔離、またはロールバック操作による正常な修復が実行できなかった場合、インシデントは**軽減されていない**に設定されます。

     また、脅威ステータスを手動で**軽減済み**または**軽減されていない**に設定することもできます。いずれかのステータスを選択すると、コメントを入力するよう促されます。このコメントは調査アクティビティの一部として保存され、**[アクティビティ]** タブで見ることができます。インシデントで新たに何かが検出された場合、または対応操作が実行され正常に完了した場合、EDRにより脅威ステータスが、**軽減済み**または**軽減されていない**に戻されます。

   - インシデントの重大度:**重大**、**高**、**中**。詳細については、"インシデントを確認する"（874ページ）を参照してください。
   - 現在の調査ステータス:**調査中**、**未開始**（デフォルト）、**偽陽性**、**閉鎖済み**のいずれか。インシデントの調査を開始した時点でステータスを変更し、他のユーザーがインシデントの変更を認識できるようにする必要があります。
   - 陽性レベル:インシデントが実際の悪意ある攻撃である可能性を1～10の範囲で示します。詳細については、"インシデントを確認する"（874ページ）を参照してください。

- インシデントタイプ: **[検ランサムウェアが検出されました]**、**[マルウェアが検出されました]**、**[不審なプロセスが検出されました]**、**[悪意のあるプロセスが検出されました]**、**[不審なURLがブロックされました]**、**[悪意のあるURLがブロックされました]** の1つ以上。
- ワークロードでMDR（Managed Detection and Response）が有効になっている場合、**MDRチケット**フィールドが表示されます。インシデントに対して作成されたMDRチケットの詳細と、インシデントに割り当てられたMDRセキュリティアナリストを表示できます。



- インシデントが作成およびアップデートされた時期:インシデントが検出された日時、またはインシデント内に記録された新しい検出によりインシデントが最後にアップデートされた日時です。

4. キルチェーングラフを構成するさまざまなノードを表示するには、**[凡例]** タブをクリックし、表示するノードを定義します。詳細については、"サイバーキルチェーンビューの理解とカスタマイズ"（884ページ）を参照してください。
5. 以下の手順を実行して、インシデントを調査し、修正します。これは、インシデントの調査および修復の典型的なワークフローですが、各インシデントや各環境の独自要件によって異なる場合があります。ご注意ください。
   a. **[攻撃ステージ]** タブで各ステージを調査します。詳細については、"攻撃ステージのナビゲーションについて"（887ページ）を参照してください。
   b. **[インシデント全体を修復]** して、修正処理を適用します。詳細については、"インシデント全体を修復する"（895ページ）を参照してください。

      また、サイバーキルチェーン内の個別ノードを修復することもできます（"個別のサイバーキルチェーンノードに対する対応操作"（900ページ）を参照）。
   c. **[アクティビティ]** タブでインシデントを軽減するために行った操作を確認します。詳細については、"インシデントを軽減するために実行される操作を理解する"（890ページ）を参照してください。

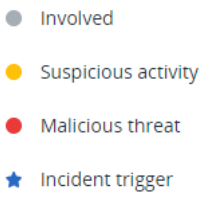
サイバーキルチェーンビューの理解とカスタマイズ

サイバーキルチェーンで影響が及ぶノードを把握するには、凡例にアクセスします。凡例には、インシデントに関連するすべてのノードが表示され、各ノードが攻撃者からどのような影響を受けたかを把握できます。またサイバーキルチェーンで、非表示にしたいノードと表示したいノードを定義できます。

凡例にアクセスするには

1. 凡例セクションの右側にある矢印アイコンをクリックします。
   下図のように [凡例] セクションが展開されます。

2. 凡例では主に4つの色が使われており、以下のようにサイバーキルチェーンの各ノードで発生した事象をすばやく把握できます。これらの色分けされたノードは、攻撃ステージにも含まれます（"攻撃ステージのナビゲーションについて"（887ページ）を参照）。



サイバーキルチェーンでノードを非表示/表示にするには

1. 拡張された凡例セクションで、サイバーキルチェーンに表示したいノードの横に が表示されていることを確認します。表示されているアイコンが の場合、アイコンをクリックして に変更します。
2. サイバーキルチェーンでノードを非表示にするには、 をクリックします。アイコンが に変わり、サイバーキルチェーンにノードが表示されなくなります。

インシデントの攻撃ステージを調査する

インシデントの攻撃ステージでは、すべてのインシデントが分かりやすく解説されています。

各攻撃ステージでは、具体的に何が起こったのか、ターゲットとなったオブジェクト（サイバーキルチェーンではノードと呼ばれる）は何だったのかが要約されています。例えば、ダウンロードしたファイルが他の何かに偽装されていた場合、攻撃ステージではそのことが示され、調査可能なサイバーキルチェーンの関連ノードと、関連するMITRE ATT&CK技術へのリンクが含められます。

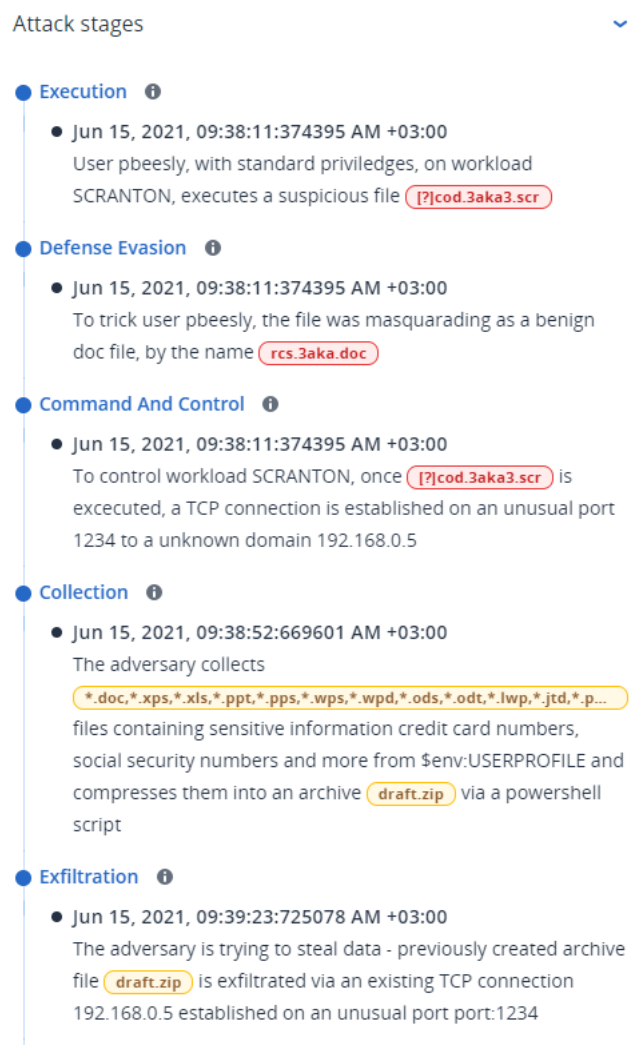
各ステージでは、以下の3つの重要な質問の答えに関する情報が提供されます。

- 攻撃者の目的は何か？
- 攻撃者はどのようにこの目的を達成したのか？
- どのノードがターゲットになったのか？

さらに重要なことは、タイムラインやグラフのノードから各セキュリティイベントを確認し、攻撃の解釈を作成する必要がないという点です。このため、インシデント調査に費やす時間は大幅に短縮されます。

また、攻撃ステージには、クレジットカード番号や社会保障番号などの機密情報を含む漏洩ファイルに関する情報も含まれています（例として以下に示す**収集**ステージを参照）。

詳細については、"攻撃ステージにはどのような情報が含まれるのでしょうか？"（887ページ）を参照してください。



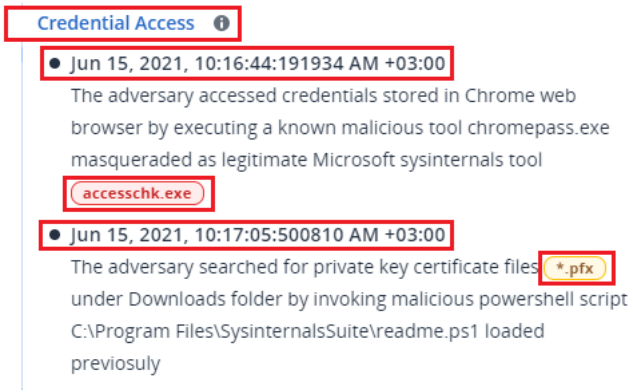
攻撃ステージのナビゲーションについて

攻撃ステージは時系列で表示されます。インシデントの攻撃ステージのリストをスクロールすると、全体を確認できます。

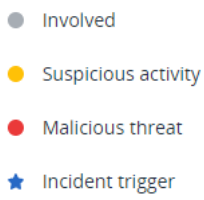
特定の攻撃ステージをさらに詳しく調査するには、攻撃ステージのいずれかの箇所をクリックして、サイバーキルチェーングラフの関連ノードに移動します。サイバーキルチェーングラフおよび特定ノードのナビゲーションについては、"サイバーキルチェーンで個別のノードを調査する"（888ページ）を参照してください。

攻撃ステージにはどのような情報が含まれるのでしょうか？

各攻撃ステージでは、読みやすい一般的な言葉で分かりやすい解説が提供されています。この解説は、以下に示すように、いくつかの要素で構成されています。以下の表で説明します。



攻撃ステージの要素	説明
ヘッダー	攻撃者が実行しようとした攻撃、その目的（上記の例では、**資格情報アクセス**）、および既知のMITRE ATT&CK技術へのリンクが記載されます。詳細については、MITRE ATT&CK Webサイトのリンクをクリックしてください。 **注意** 攻撃ステージが既知のMITRE ATT&CK技術でない場合、ヘッダーテキストはリンクされません。これは、ランダムフォルダで検出されたファイルなどの汎用的な技術に関連します。
タイムスタンプ	攻撃ステージが発生した時間です。
技術	攻撃者が技術的にどのような目的を達成したか、どのようなオブジェクト（レジストリエントリ、ファイル、スケジュールされたタスク）が影響を受けたかを示します。

攻撃ステージの要素	説明
	攻撃手法の説明文には、上記の例に示すように、サイバーキルチェーンにおける影響を受ける各ノードへの色分けされたリンクが含まれています。これらの色分けされたリンクにより、影響を受けたノードにすばやく移動し、発生した事象に関する詳細な調査を実行できます。攻撃ステージで使用される色分けは以下の通りです。  上記の凡例を見ると、例として取り上げた資格情報アクセスの攻撃ステージには、マルウェアノード accesschk.exe と不審なファイルノード *.pfx へのリンクがあることがわかります（リンクをクリックするとサイバーキルチェーンの該当ノードにジャンプします）。これらのノードのナビゲーションと実行可能な操作の詳細については、"サイバーキルチェーンで個別のノードを調査する"（888ページ）を参照してください。 なお攻撃ステージには、漏洩したファイルに関する情報（保護された健康情報（PHI）、クレジットカード番号、社会保障番号などの機密情報）を含むファイルノードへのリンクも含まれています。

注意
各攻撃ステージは単一の検出イベントでです。各ステージに記載された内容（ヘッダー、タイムスタンプ、テクニック）は、エンドポイント検知と応答（EDR）で保存されている攻撃ステージテンプレートに基づき、検知イベント内の特定パラメータに従って生成されます。

サイバーキルチェーンで個別のノードを調査する

攻撃ステージの確認に加え、サイバーキルチェーンの各攻撃ノード間を移動することができます。これにより、サイバーキルチェーンの特定ノードを掘り下げ、必要に応じて各ノードの調査や修復を行うことができます。

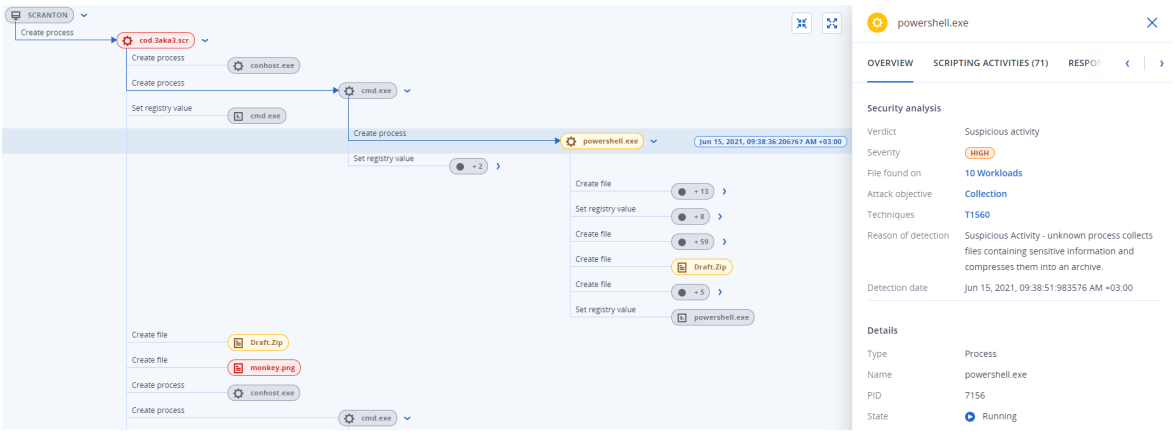
例えば、あるインシデントが実際の悪意ある攻撃である可能性を判断できます。また、調査に基づいて、ワークロードや不審なファイルの隔離など、さまざまな対応操作をノードに適用することができます。

サイバーキルチェーンにおける個別ノードを調査するには

1. Cyber Protectコンソールで、**[保護]** > **[インシデント]** に進みます。
2. 表示されたインシデントのリストで、調査するインシデントの最右列の  をクリックします。選択したインシデントのサイバーキルチェーンが表示されます。
3. 該当するノードに移動し、クリックすると、そのノードのサイドバーが表示されます。

> **注意**
> ノードをクリックすると、ノードが展開され、関連するノードが表示されます。

例えば、以下の例で**powershell.exe**ノードをクリックすると、そのノードのサイドバーが開きます。また、ノードの横にある矢印アイコンをクリックすると、**powershell.exe**ノードによって影響を受ける可能性のあるファイルやレジストリ値など、関連するノードを表示することができます。これらの関連するノードをクリックすると、さらに詳しく調査できます。



4. サイドバーのタブに含まれる情報を調査します。
   - **概要**:攻撃されたノードのセキュリティ概要を示す2つの主要なセクションが含まれています。
     - **セキュリティ分析**:攻撃されたノードの分析を提供します。脅威に関するEDRの判定（疑わしいアクティビティなど）、MITRE攻撃技術に従った攻撃の目的（リンクをクリックしてMITRE Webサイトへ移動）、検出理由、攻撃の影響を受ける可能性のあるワークロード数（**nワークロード**リンクをクリックして影響を受けるワークロードを表示）などを確認できます。

       > **注意**
       > **nワークロード**リンクは、特定の悪意あるまたは不審なオブジェクトが他のワークロードで発見されたことを意味します。これは、他のワークロードで攻撃が生じていることを意味するのではなく、他のワークロードにIOCがあることを意味します。攻撃は既に発生しているか（そして別のインシデントが作成されているか）、または攻撃者が攻撃「ツールキット」を使って他のワークロードの攻撃を準備している可能性があります。

- **詳細**:ノードのタイプ、名前、現在のステータス、ノードへのパス、ファイルのハッシュやデジタルシグネチャ（MD5や証明書のシリアルナンバーなど）など、ノードに関する詳細が含まれています。

- **スクリプト処理アクティビティ**:攻撃で呼び出された、または読み込まれたスクリプトの詳細が含まれます。詳しく調査するには、 をクリックしてスクリプトをクリップボードにコピーします。

  注意
  [スクリプト処理アクティビティ] タブは、コマンドやスクリプト（cmdやPowerShellコマンドなど）を実行するプロセスノードにのみ表示されます。

- **対応操作**:ノードの種類に応じて、追加の調査、修復、予防操作を提供する多くのセクションが含まれています。
  例えば、ワークロードノードの場合、フォレンジックバックアップとバックアップからの復元を含むいくつかの対応を定義できます。また、悪意のあるノードや不審なノードに対しては、ノードの停止や隔離、攻撃による変更のロールバック、保護計画の許可リストやブロックリストへの追加を実行できます。
  特定のノードに対応操作を適用する方法の詳細については、"個別のサイバーキルチェーンノードに対する対応操作"（900ページ）を参照してください。

- **アクティビティ**:インシデントに適用された操作を時系列で表示します。詳細については、"インシデントを軽減するために実行される操作を理解する"（890ページ）を参照してください。

インシデントを軽減するために実行される操作を理解する

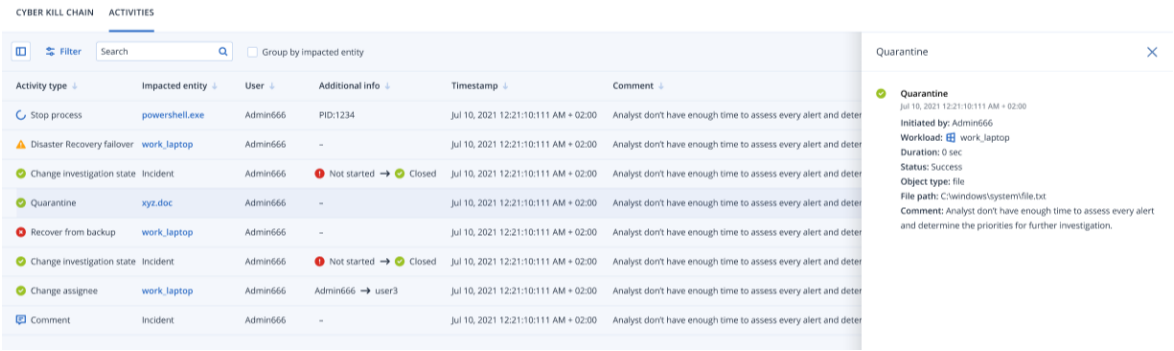
インシデントを確認し、攻撃がどのように発生したかを調査した後、通常は、対応操作を適用します。対応操作を適用すると、これらの操作は多くの箇所で表示されるようになり、インシデントを軽減するためにどのような手順が実行されたかをより正しく理解することができます。

注意
予防レイヤで作成されたインシデントには、保護計画で設定された操作が自動的に適用されます。検出ポイントについては、各攻撃シナリオを軽減するための関連する対応操作を定義する必要があります。

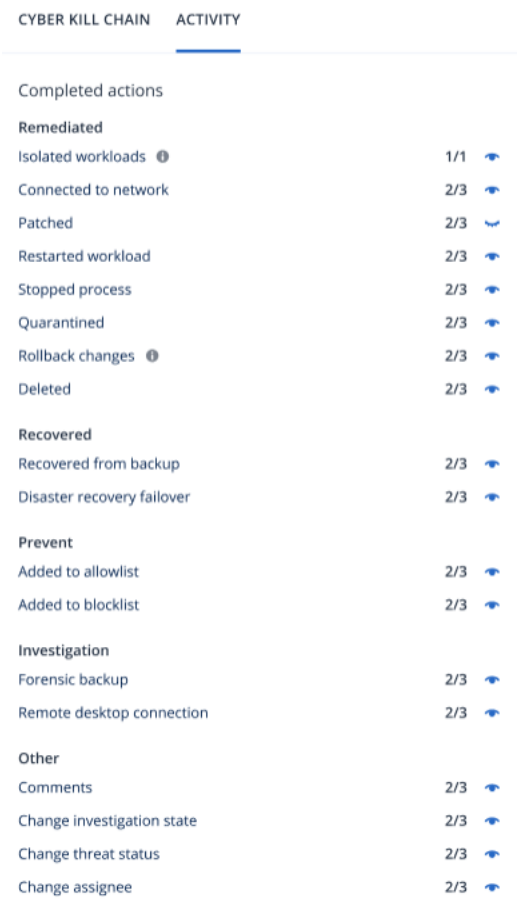
実行された対応操作を理解するために、インシデント全体に適用されたすべての対応操作を表示したり、インシデントのサイバーキルチェーンで特定のノードに適用された操作を表示したりできます。

インシデントに適用されるすべての対応操作を表示するには

1. Cyber Protectコンソールで、**[保護]** > **[インシデント]** に進みます。
2. 表示されたインシデントのリストで、調査するインシデントの最右列の をクリックします。選択したインシデントのサイバーキルチェーンが表示されます。
3. **[アクティビティ]** タブをクリックします。
   インシデントに既に適用されている対応操作のリストが表示されます。

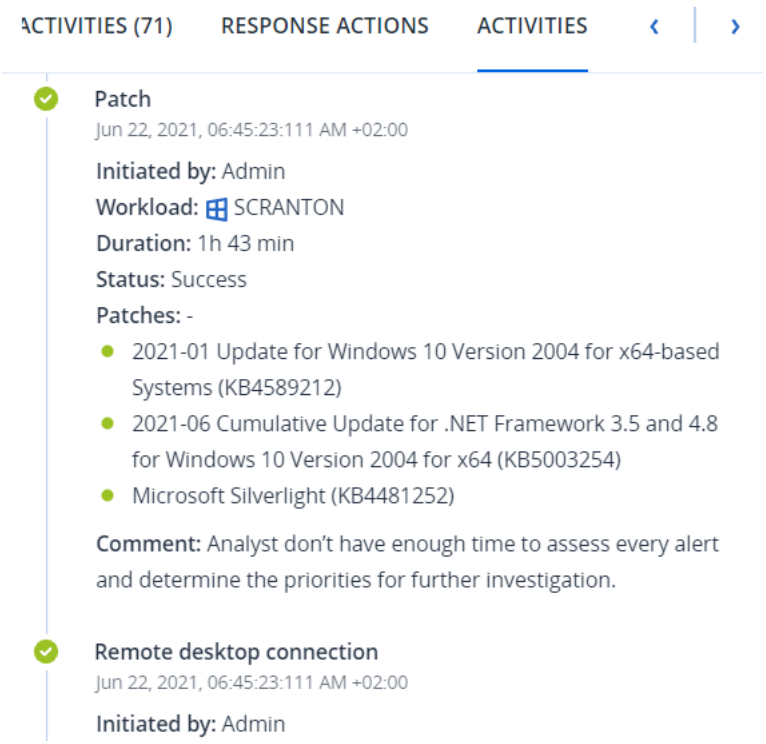


4. 表示されたリストで、さまざまな操作を実行できます。
   - アクティビティタイプの行をクリックすると、選択したアクティビティに関する詳細情報が表示されます。手順3のようにサイドバーに表示される情報には、操作を開始した人、ステータス、ファイルパス、開始者が追加したコメントなどの詳細が含まれます。
   - 特定の操作を検索するには、**[検索]** ボックスを使用します。
   - リストにフィルタを適用するには、**[フィルタ]** をクリックします。
   - **[影響を受けるエンティティごとにグループ化]** チェックボックスを選択して、エンティティごとに関連する操作をグループ化します。
   - 完了した操作のリストを表示/非表示にするには、  をクリックします。
     表示させたい操作の横に が表示されていることを確認します。表示されているリストで操作を非表示にする場合は、もう一度クリックすると に切り変わります。



特定のノードに適用された対応操作を表示するには

1. サイバーキルチェーンでは、ノードをクリックすると、そのノードのサイドバーが表示されます。
2. **[アクティビティ]** タブをクリックします。



3. 適用された操作とその理由を完全に把握するには、場合によってそのノードに適用された対応操作をスクロールする必要があります。例えば、リモートデスクトップ接続操作の場合、誰がいつ操作を開始したか、操作の継続時間、全体のステータス（成功したか、失敗したか、エラーを伴い成功したか）を表示することができます。

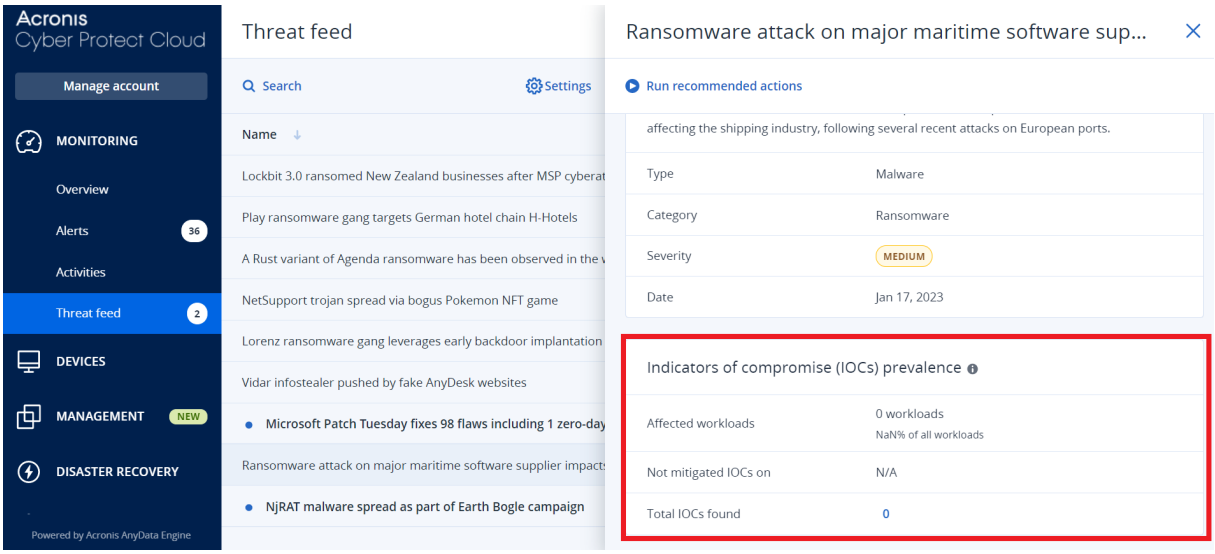
ワークロード上の既知の攻撃によるIOC（Indicators of Compromise）を確認する

エンドポイント検知と応答（EDR）には、ワークロードに対する脅威フィードに含まれる既存かつ既知の攻撃を確認する機能があります。これらの脅威フィードは、Cyber Protection Operations Center（CPOC）から受け取った脅威データに基づいて自動的に生成されます。EDRにより、脅威がワークロードに影響を与えているかどうかを確認して、脅威を無効化するために必要な操作を適用できます。

脅威フィードは、Cyber Protectコンソールの **[監視]** メニューからアクセスできます。詳細については、"脅威フィード"（293ページ）を参照してください。

具体的な脅威の詳細を確認し、ワークロードに影響があるかどうかを確認するには、脅威フィードをクリックします。検出されたIOCの数と影響を受けたワークロードを表示して、軽減されていないIOCを含むワークロードを掘り下げることができます。

注意
保護計画でEDRが有効になっていない場合、追加の脅威フィード機能は表示されません（下記参照）。



脅威フィードの設定を定義する

既知の脅威を自動的に検出し軽減するために、各種の脅威フィード設定を定義することができます。

脅威フィードの設定を定義するには

1. Cyber Protectコンソールで、**[監視]** > **[脅威フィード]** に進みます。
2. 表示された脅威フィードページで、**[設定]** をクリックします。
3. 表示されたダイアログで、以下のいずれかを選択します。

オプション	説明
IOC（Indicators of Compromise）の検索	ワークロードのIOC自動検索を有効にするには、このスイッチをクリックします。 このオプションを有効にすると、**[検出時の操作]** および **[アラートを生成]** オプションも表示されます。
検出時のアクション	ドロップダウンリストから、ワークロードで脅威が発見されたときに関連するファイルに対して実行する操作を選択します。 • **アクションなし** • **検疫** • **削除** • **分離されたワークロード**
アラートを生成	ワークロードでIOCが検出された場合にアラートを生成するためのチェックボックスを選択します。アラートはアラートページに表示されます。

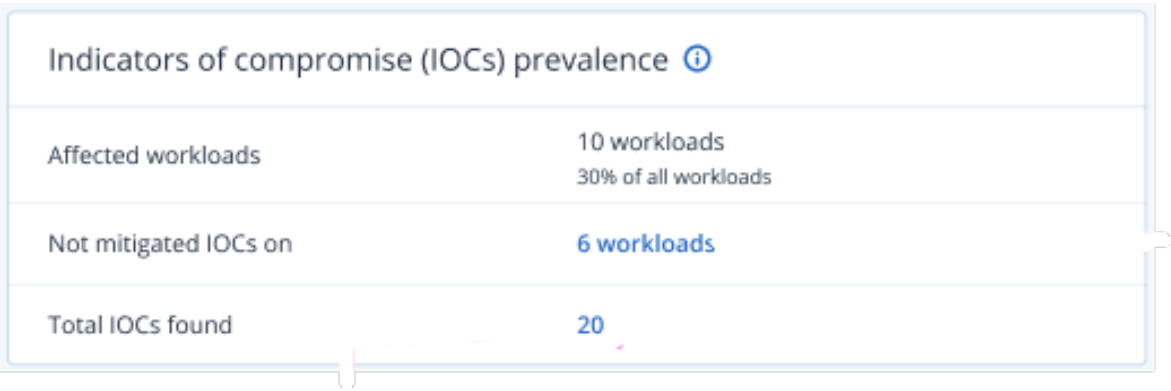
4. **[適用]** をクリックします。

影響を受けるワークロードのIOCを確認し、軽減操作を実行する

保護計画でエンドポイント検知と応答（EDR）を有効にすると、保護計画内のワークロードに影響を与えている既知の脅威を表示できます。また、自動的に軽減されなかった残りのIOC（Indicators of Compromise）の軽減操作を実行できます。IOCで自動的に軽減操作を実行する方法については、"脅威フィードの設定を定義する"（893ページ）を参照してください。

影響を受けるワークロードを確認し、軽減操作を実行するには

1. Cyber Protectコンソールで、**[監視]** > **[脅威フィード]** に進みます。
2. スレッドをクリックすると、その脅威の詳細が表示されます。
3. **[IOC（Indicators of Compromise）罹患率]** セクションで、**nワークロード**リンクをクリックして、未解決のIOCがあるワークロードを表示します。



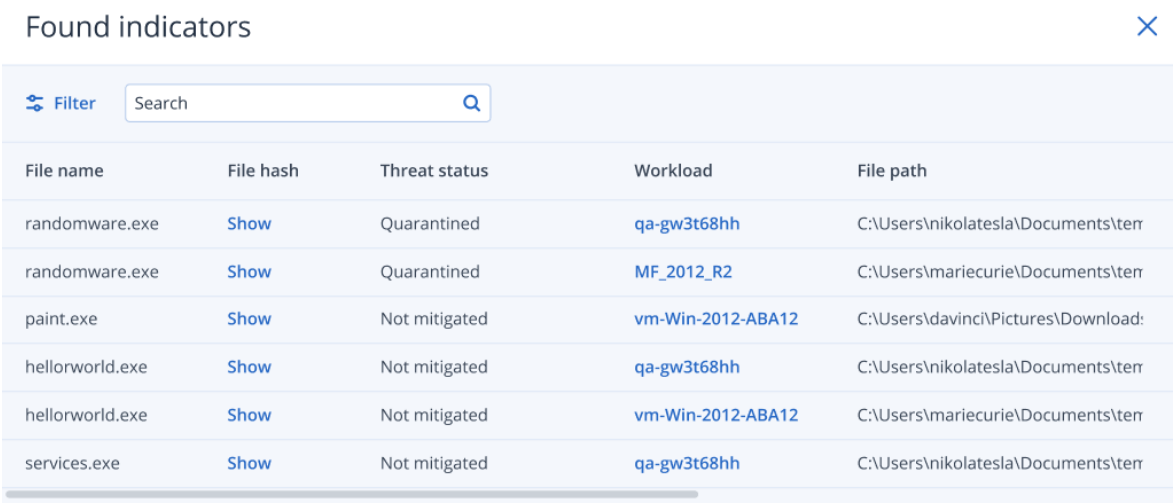
4. 表示されたワークロードのページで、該当するワークロードをクリックし、その詳細を確認します。ワークロードに対して特定の機能を実行することができます。例えば、フィルタリングする追加のURLを定義したり（"URLフィルタ処理"（824ページ）を参照）、悪意あるプロセスをブロックしたり（"ウイルスおよびマルウェア対策保護の設定"（801ページ）の除外セクションを参照）できます。
   例えば脅威フィードで、ワークロードがIOCの影響を受けていることが示されている場合、まずIOCのロケーションを特定し分析します（"検出されたIOCの確認と分析"（894ページ）を参照）。次に、ワークロードの保護計画に進み、悪意あるファイルハッシュやプロセスのブロックなど、追加の保護を定義します。

検出されたIOCの確認と分析

既知の脅威の影響を受けたワークロードの確認に加えて、特定のIOC（Indicators of Compromise）を確認および分析できます。これにより、IOCの影響を受けている個別のワークロードを確認し、IOCを軽減できます。

IOCを確認および分析するには

1. Cyber Protectコンソールで、**[監視]** > **[脅威フィード]** に進みます。
2. スレッドをクリックすると、その脅威の詳細が表示されます。
3. **[IOC（indicators of Compromise）罹患率]** セクションで、**検出された合計IOC**のリンクをクリックします。
   検出インジケータページが表示されます。



4. （オプション）IOCのリストをステータスに従ってフィルタリングするには、**[フィルタ]** オプションを使用します。また、**[検索]** オプションで特定のIOCを検索することもできます。
5. IOCによって影響を受けるワークロードを表示するには、**[ワークロード]** 列のリンクをクリックします。その後、パッチ管理の実行や保護計画の変更など、ワークロードに対してさまざまな操作を実行できます。
6. （オプション）特定のIOCで見つかったファイルハッシュを表示するには、**[ファイルハッシュ]** 列で、**[表示]** をクリックします。表示されたダイアログで をクリックし、IOCのファイルハッシュをテキストエディタにコピーします。

インシデントを修復

エンドポイント検知と応答（EDR）により、インシデント全体、またはインシデントの個別の攻撃ポイントを修復することが可能になります。

インシデント全体を修復することで、インシデントに対してグローバルに実行する修復（複数可）を選択できます。インシデントをよりきめ細かく管理したい場合は、必要に応じて、個別の攻撃ポイントを修復できます。例えば、ラテラルムーブメントやコマンドと制御（C&C）アクティビティを阻止するために、ワークロードのネットワークを分離したい場合があります。このオプションを使用すれば、ワークロードが分離されても、すべてのAcronis Cyber Protect技術の動作は継続し、調査を開始することができます。

EDRは、次のような方法で効果的な修復を実現します。

- 軽減操作 - 脅威を確実に停止する。
- リカバリ - すぐにサービスを再開できるようにする。
- 予防 - 攻撃で使用された技術を今後の攻撃で確実に阻止する。

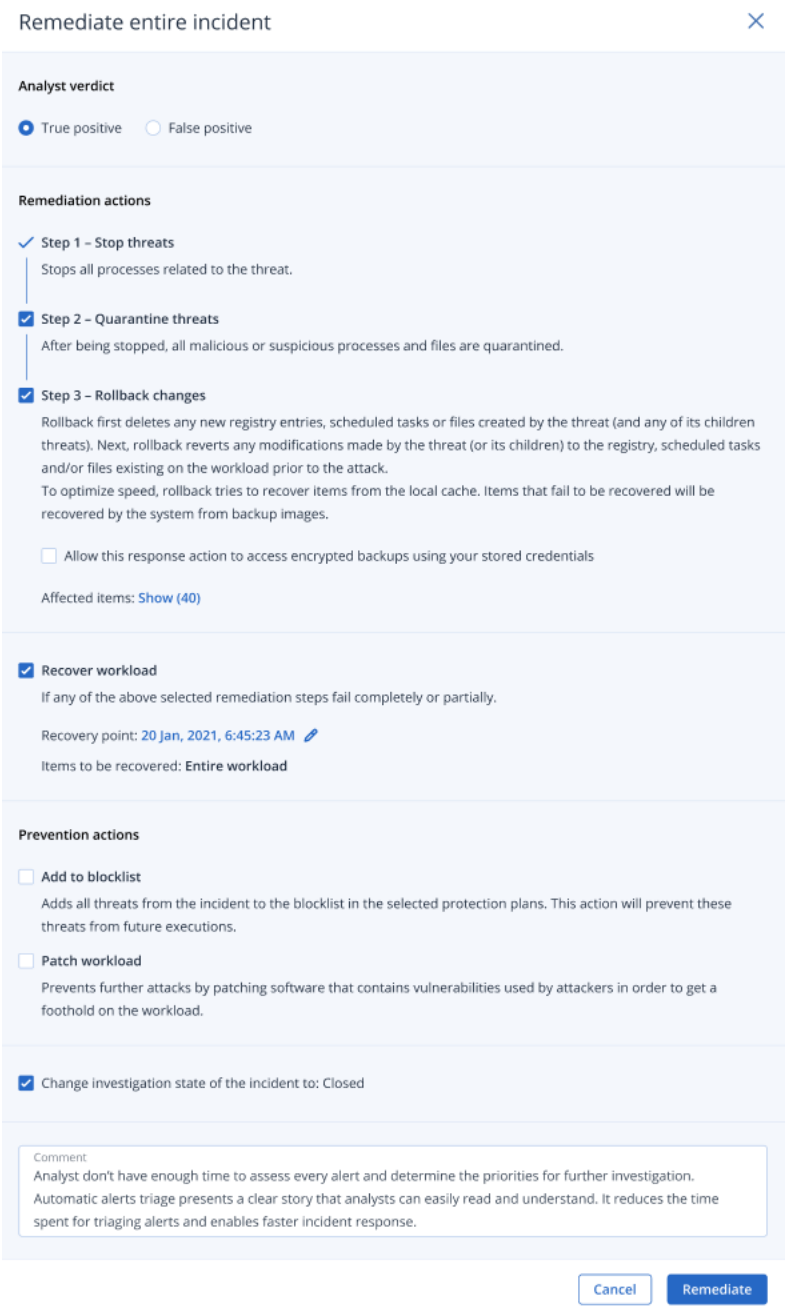
インシデント全体を修復する

インシデント全体を修復することで、インシデントに対してグローバルに実行する修復（複数可）を迅速かつ簡単に選択できます。エンドポイント検知と応答（EDR）では、修復プロセスのステップバイステップガイドが提供されています。

ネットワークとインシデントをさらに細かく管理する必要がある場合は、"個別のサイバーキルチェーンノードに対する対応操作"（900ページ）を参照してください。

インシデント全体を修復するには

1. Cyber Protectコンソールで、**[保護]** > **[インシデント]** に進みます。
2. 表示されたインシデントのリストで、調査するインシデントの最右列の をクリックします。選択したインシデントのサイバーキルチェーンが表示されます。
3. **[インシデント全体を修復]** をクリックします。[インシデント全体を修復] ダイアログが表示されます。



4. インシデントの調査に基づき、**[アナリスト評価]** セクションで次のいずれかを選択します。
   - **真陽性**:実際の攻撃であることが確認された場合に選択します。選択した後、修復および予防操作を追加します（次の手順を参照）。
   - **偽陽性**:実際の攻撃ではないことが確認された場合に選択します。このモードでは、インシデントを保護計画の許可リストに追加するなど、再発防止策を定義できます。

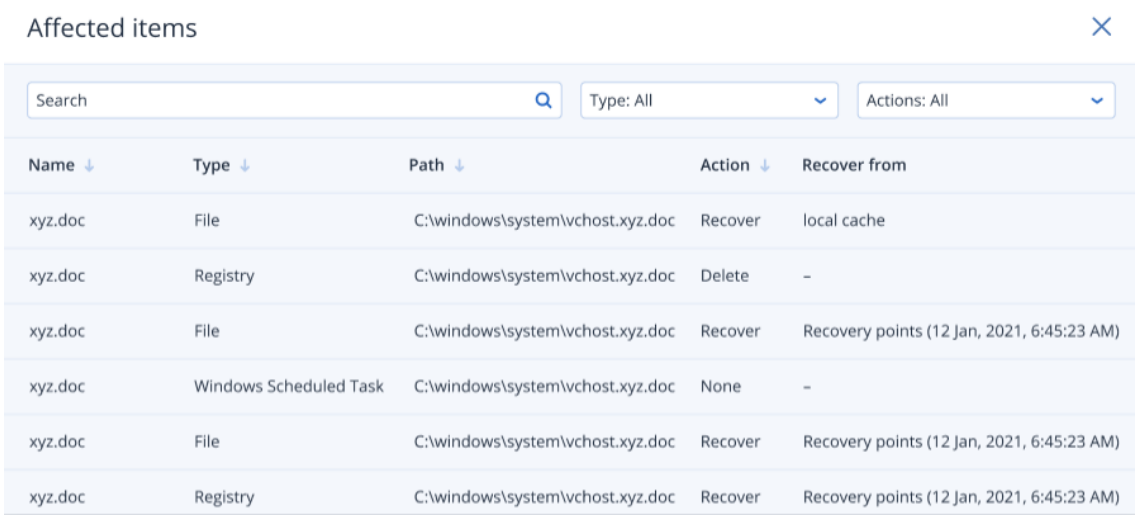
     注意
     [偽陽性] を選択すると、予防操作のみを定義できます。詳細については、"偽陽性インシデントを修復する"（899ページ）を参照してください。

5. **[修復操作]** セクションで、次の修復手順を実行します。例えば、手順1が完了する前に手順2を選択することはできませんのでご注意ください。
   a. **手順1 - 脅威を停止**:このチェックボックスを選択して、脅威に関連するすべてのプロセスを停止します。
   b. **手順2 - 脅威を隔離**:脅威が停止したら、このチェックボックスを選択して、悪意ある不審なプロセスやファイルをすべて隔離します。
   c. **手順3 - ロールバックの変更**:脅威が隔離された後、このチェックボックスを選択して、脅威（およびそのすべての子脅威）によって作成された新しいレジストリエントリ、スケジュールされたタスク、ファイルをすべて削除します。ロールバックプロセスが実行されると、攻撃前にワークロード上に存在したレジストリ、スケジュールされたタスク、ファイルに対して脅威（またはその子脅威）が加えた変更が元に戻されます。ロールバックプロセスでは、速度を最適化するために、ローカルキャッシュを利用した項目のリカバリが試行されます。リカバリに失敗した項目については、システムによりバックアップイメージからのリカバリが実行されます。

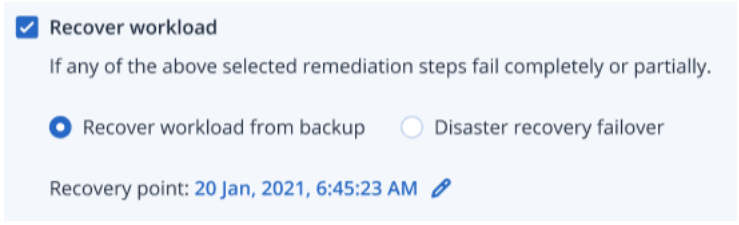
      注意
      ロールバック処理では、必ずローカルキャッシュ内の項目からリカバリが実行されます。バックアップアーカイブからのロールバックは今後のリリースで利用可能になる予定です。

      関連するバックアップへのアクセスが暗号化されている場合は、**[この対応操作により、保存済み資格情報を使用して暗号化されたバックアップにアクセスできるようにする]** チェックボックスを選択します。暗号化されたアーカイブを復号化し、関連ファイルを検索するために、EDRから保存されているユーザーの資格情報へのアクセスが発生します。

      [影響を受ける項目] をクリックして、ロールバックによって影響を受けるすべての項目（ファイル、レジストリ、スケジュールされたタスク）、適用された操作（**削除**、**復元**、**なし**）、ローカルキャッシュまたはバックアップイメージから項目を復元するかどうかのオプションを表示することもできます。



d. **ワークロードをリカバリ**:上記の修復手順のいずれかが完全に、または部分的に失敗した場合にワークロードをリカバリするには、このチェックボックスを選択します。



次の復元オプションのいずれかを選択します。

- **バックアップからワークロードをリカバリ**:特定の復元ポイントからワークロードをリカバリできるようにします。復元ポイントの編集アイコンをクリックして、復元用バックアップの一覧から選択します。
- **ディザスタリカバリフェールオーバー**:保護計画でこの機能を有効にしている場合に、ディザスタリカバリを実行できるようにします。ADサーバーやデータベースサーバーなどの重要なワークロードでは、このオプションの使用を推奨します。詳細については、"ディザスタリカバリを実装する"（714ページ）を参照してください。

6. [**予防操作**] セクションで、関連する修復手順を選択します。
   - **ブロックリストに追加**:このチェックボックスを選択し、表示された保護計画のリストから、該当する保護計画を選択します。この予防操作により、選択された保護計画について、インシデントのすべての検出が実行されないようにブロックできます。
   - **ワークロードにパッチを適用**:このチェックボックスを選択すると、脆弱性のあるソフトウェアにパッチが適用され、攻撃者がワークロードにアクセスするのを防止できます。次に、ユーザーがログインしているかどうかに応じて、パッチ完了後に実行する関連処理（**再起動しない**、**再起動**、**必要な場合に限り再起動**）を選択できます。
     [**バックアップ中は再起動しない**] チェックボックスを選択して、バックアップ中にワークロードが再起動されないようにすることもできます。

7. [**インシデントの調査ステータスを変更:クローズ済み**] チェックボックスを選択します。選択しない場合、調査ステータスは以前のステータスのままです。
8. [**修復**] をクリックします。選択した修復操作が段階的に実行され、各修復ステップの進行状況が [インシデント全体を修復] ダイアログに表示されます。
   クリックすると、[**アクティビティに移動**] ボタンが表示されます。[**アクティビティに移動**] をクリックして、インシデントに適用されたすべての対応操作を確認します。詳細については、"インシデントを軽減するために実行される操作を理解する"（890ページ）を参照してください。

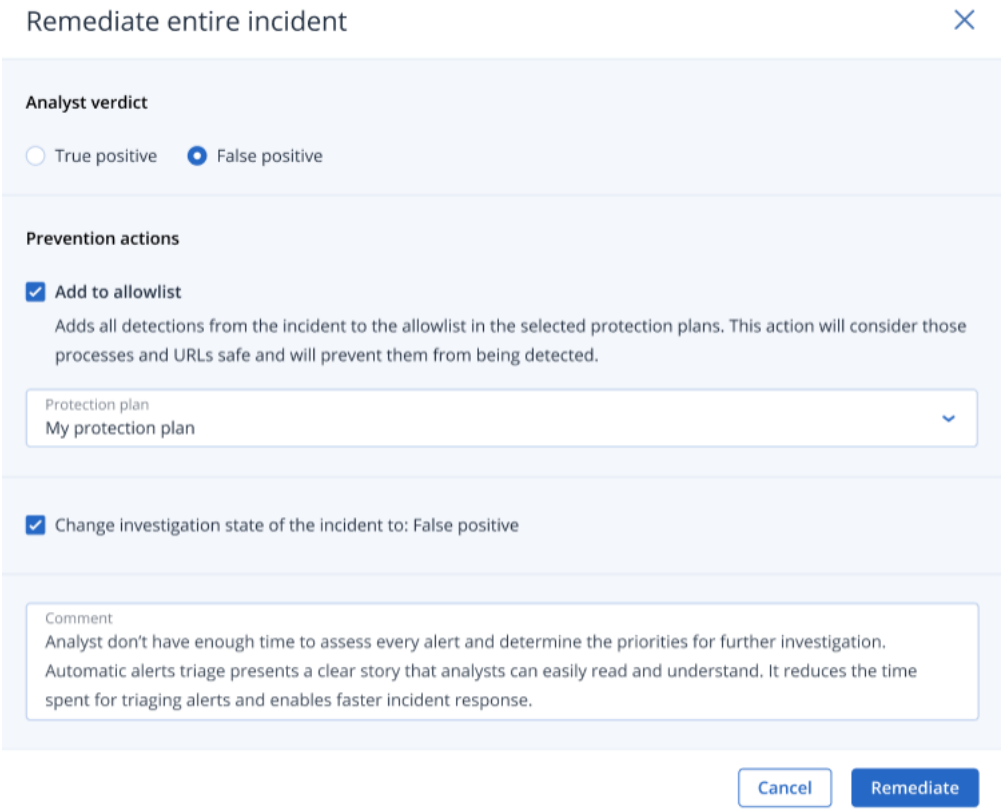
偽陽性インシデントを修復する

もし、ある攻撃が実際の攻撃でない、つまり偽陽性であることが確認できれば、そのインシデントが再び生成されないようにするための定義を作成できます。例えば、インシデントを保護計画の許可リストに追加できます。

偽陽性インシデントを修復するには

1. 選択したインシデントのサイバーキルチェーンで、[**インシデント全体を修復**] をクリックします。
   [インシデント全体を修復] ダイアログが表示されます。

2. [**アナリスト評価**] セクションで、[**偽陽性**] を選択します。



3. [**予防操作**] セクションで、[**許可リストに追加**] チェックボックスを選択します。表示された保護計画のリストから、該当する保護計画を選択します。
   この予防操作により、選択された保護計画について、インシデントの検出をすべて確実に予防できます。
4. [**インシデントの調査ステータスを変更: 偽陽性**] チェックボックスを選択します。
5. [**修復**] をクリックします。
   クリックすると、[**アクティビティに移動**] ボタンが表示されます。[**アクティビティに移動**] をクリックして、インシデントに適用された対応操作を確認します。詳細については、"インシデントを軽減するために実行される操作を理解する"（890ページ）を参照してください。

個別のサイバーキルチェーンノードに対する対応操作

インシデントをより細かく管理したい場合、個別のサイバーキルチェーンノードにさまざまな対応操作を適用することができます。これらの対応操作により、あらゆるノードを迅速かつ容易に修復することができます。

注意
インシデント全体にグローバルな対応操作を適用する場合は、"インシデント全体を修復する"（895ページ）を参照してください。

対応操作は以下のカテゴリに分類されますが、すべてのノードにカテゴリすべてが含まれているわけではありません。

- **修復**:このカテゴリの操作では、攻撃に対する即時対応を実行できます。この操作には、ワークロードのネットワーク分離の管理、ファイル、プロセス、レジストリ値の削除と隔離が含まれます。
- **調査**:このカテゴリの操作（ワークロードにのみ適用）では、フォレンジックバックアップの実行や、より詳細な調査のためのリモートデスクトップ接続を実行できます。
- **調査**:このカテゴリの操作（ワークロードにのみ適用）では、より詳細な調査のためのリモートデスクトップ接続を実行できます。
- **復元**:このカテゴリの操作（ワークロードにのみ適用）では、バックアップからの復元、またはディザスタリカバリフェールオーバーを実行して、集中的な攻撃に対応できます。
- **防止**:このカテゴリの操作で、脅威を保護計画の許可リストまたはブロックリストに追加して、将来の脅威に対抗するとともに、偽陽性による検出を防止できます。

注意

インシデントが完了すると、ノードに対応操作を適用できなくなります。ただし、該当の調査ステータスを変更して**調査中**にすることで、完了したインシデントを再度開くことができます。再度開くと、対応操作を適用できるようになります。

以下の表は、サイバーキルチェーンの各ノードタイプ、各ノードに適用されるカテゴリ、および利用可能な対応操作をまとめたものです。

ノード	カテゴリ	対応操作
ワークロード	修復	• ネットワーク分離を管理 • ワークロードを再起動
	調査	• フォレンジックバックアップ • リモートデスクトップ接続
	調査	• リモートデスクトップ接続
	復元	• バックアップから復元 • ディザスタリカバ

ノード	カテゴリ	対応操作
		リフェールオーバー
	防止	• [パッチ]
プロセス	修復	• プロセスを停止 • 検疫
	防止	• 許可リストに追加 • ブロックリストに追加
ファイル	修復	• 削除 • 検疫
	防止	• 許可リストに追加 • ブロックリストに追加
レジストリ	修復	• 削除
ネットワーク	防止	• 許可リストに追加 • ブロックリストに追加

影響を受けたワークロードに対する対応操作を定義する

攻撃への対応の一環として、影響を受けるワークロードに次の操作を適用できます。

- **ネットワーク分離を管理**:ワークロードのネットワーク分離を管理し、ラテラルムーブメントやコマンドと制御（C&C）アクティビティを阻止できます。詳細については、"ワークロードのネットワーク分離を管理する"（903ページ）を参照してください。
- **パッチ**:将来潜在的に考えられる攻撃において脆弱性のエクスプロイトが発生するのを防止するために、ワークロードにパッチを適用できます。詳細については、"ワークロードにパッチを適用"（907ページ）を参照してください。
- **ワークロードを再起動**:ワークロードを直ちに、または事前に定義されたタイムアウト期間に従って再起動できます。詳細については、"ワークロードを再起動"（908ページ）を参照してください。

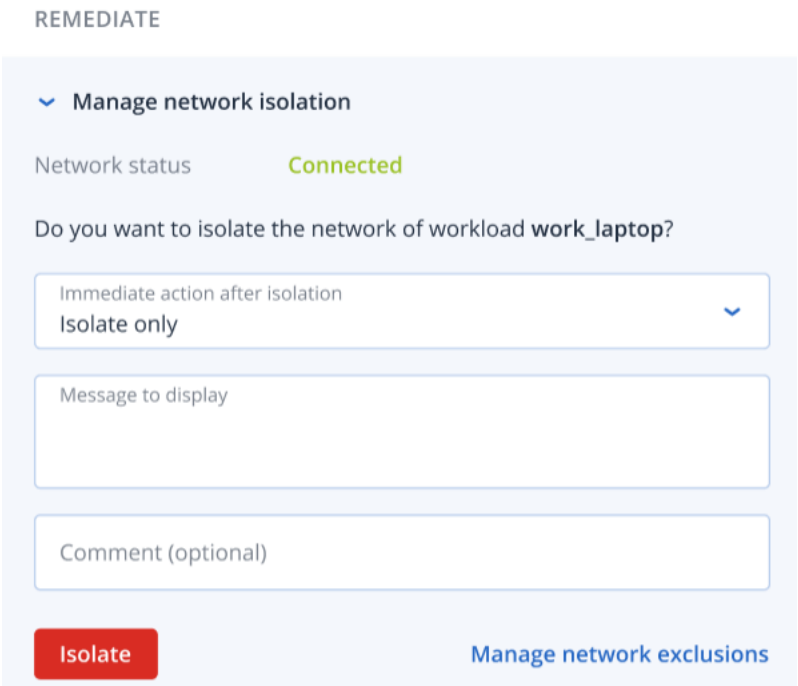
- **フォレンジックバックアップ**: 監査または詳細な調査の目的で、オンデマンドのフォレンジックバックアップを実行できます。詳細については、"オンデマンドでワークロードのフォレンジックバックアップを実行"（909ページ）を参照してください。
- **リモートデスクトップ接続**: 調査対象のワークロードにリモートでアクセスできます。詳細については、"ワークロードへのリモート接続"（910ページ）を参照してください。
- **バックアップから復元**:バックアップからのマシン全体、または特定のファイルやフォルダのリカバリが可能になります。詳細については、"バックアップから復元"（911ページ）を参照してください。
- **ディザスタリカバリフェールオーバー**:"ディザスタリカバリを実装する"（714ページ）を実行できます。なお、ワークロードでAdvanced Disaster Recoveryのサブスクリプションが取得されている必要があります。詳細については、"ディザスタリカバリフェールオーバー"（912ページ）を参照してください。

ワークロードのネットワーク分離を管理する

EDRにより、ワークロードのネットワーク分離を管理し、ラテラルムーブメントやコマンドと制御（C&C）アクティビティを阻止できます。要件に応じて、さまざまな分離オプションを選択できます。なお、ワークロードが分離された場合でも、すべてのAcronis Cyber Protect技術は機能しており、十分な調査が可能です。

ネットワークからワークロードを分離するには

1. サイバーキルチェーンで、修復したいワークロードのノードをクリックします。
2. 表示されたサイドバーで、**[対応操作]** タブをクリックします。
3. **[修復]** セクションで、**[ネットワーク分離を管理]** をクリックします。



注意
ネットワークステータスの値は、ワークロードの現在のネットワーク接続状態を示しています。値に**分離済み**と表示された場合、分離されたワークロードをネットワークに再接続できます（以下の手順を参照）。ワークロードがオフラインの場合でも、ワークロードを分離できます。ワークロードがオンラインに戻ると、自動的に**分離**状態になります。

4. **[分離後にすぐ実行する操作]** ドロップダウンリストで、以下のいずれかを選択します。
   - **分離のみ**
   - **ワークロードを分離してバックアップ**
   - **フォレンジックデータを伴うワークロードを分離してバックアップ**
   - **ワークロードを分離してパワーオフ**

   ワークロードのバックアップ先と暗号化オプションの定義の詳細については、"ワークロード/ファイルのバックアップを復元および管理する"（385ページ）を参照してください。
5. （オプション）**[表示するメッセージ]** フィールドで、エンドユーザーが分離されたワークロードにアクセスするときに表示するメッセージを追加します。例えば、ワークロードが分離されており、ワークロードに対する送受信のネットワークアクセスが現在利用できないことをユーザーに知らせることができます。なお、このメッセージはトレイモニターの通知としても表示され、ユーザーがメッセージを削除するまで表示されます。
6. （オプション）**[コメント]** フィールドに、コメントを追加します。このコメントは **[アクティビティ]** タブ（単一のノードまたはインシデント全体）に表示され、自分（または他の人）がインシデントを再度利用する際に、操作を実行した原因を思い出すヒントになります。
7. **[ネットワーク除外の管理]** をクリックして、分離中のワークロードにアクセスできるポート、URL、ホスト名、およびIPアドレスを追加します。詳細については、「ネットワーク除外を管理」を参照してください。
8. **[分離]** をクリックします。
   このワークロードは分離されています。この操作は、個別のノードとインシデント全体の **[アクティビティ]** タブで確認することもできます。詳細については、"インシデントを軽減するために実行される操作を理解する"（890ページ）を参照してください。

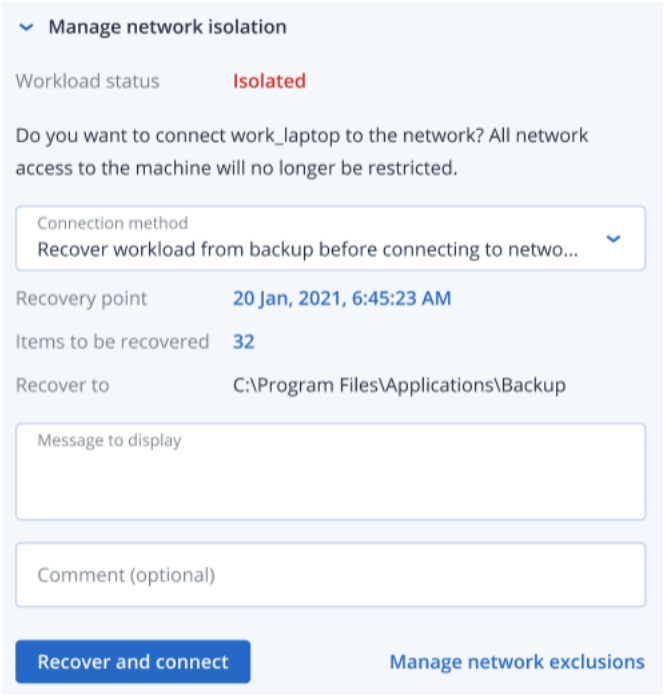
注意
ワークロードは、Cyber Protectコンソールの **[ワークロード]** メニューに**分離済み**として表示されます。1つまたは複数のワークロードを分離するには、**[ワークロード]** > **[エージェントを含むワークロード]** メニューから、関連するワークロードを選択し、右サイドバーで **[ネットワーク分離を管理]** を選択します。表示されたダイアログで、ネットワークの除外を管理し、**[分離]** または **[すべて分離]** をクリックして、選択したワークロードを分離できます。

分離されたワークロードをネットワークに戻すには

1. サイバーキルチェーンで、再接続したいワークロードのノードをクリックします。

注意
分離済みのワークロードが現在オフラインの場合でも、ワークロードをネットワークに再接続できます。ワークロードがオンラインに戻ると、自動的に**接続済み**のステータスに切り替わります。

2. 表示されたサイドバーで、**[対応操作]** タブをクリックします。
3. **[修復]** セクションで、**[ネットワーク分離を管理]** をクリックします。
4. 以下のいずれかを選択します。
   - **直ちにネットワークに接続する**:ワークロードはネットワークに再接続されます。
   - **ネットワークに接続する前に、バックアップからワークロードをリカバリする**:ワークロードをリカバリする復元ポイントを選択します。
     a. **[復元ポイント]** フィールドで、**[選択]** をクリックします。
     b. 表示されたサイドバーで、該当する復元ポイントを選択します。
     c. ワークロード上のすべてのファイルとフォルダを復元するには、**[リカバリ]** > **[ワークロード全体]** をクリックします。
     または
     ワークロード上の特定のファイルとフォルダを復元するには、**[リカバリ]** > **[ファイル/フォルダ]** をクリックします。その後、関連するファイルやフォルダを選択する画面が表示されます。選択した後、**[リカバリする項目]** フィールドの該当する値をクリックすると、項目のリストを表示することができます。



注意
選択した復元ポイントが暗号化されている場合は、パスワードの入力が求められます。

5. （オプション）**[ワークロードの自動的な再起動（必要な場合）]** チェックボックスを選択します。このオプションは、手順4で **[リカバリ]** > **[ワークロード全体]** を選択した場合にのみ関連します。
6. （オプション）**[表示するメッセージ]** フィールドで、エンドユーザーが接続済みワークロードにアクセスするときに表示するメッセージを追加します。例えば、ワークロードにバックアップが復元されたこと、ワークロードとの送受信ネットワークアクセスが再開されたことをユーザーに知らせることができます。
7. （オプション）**[コメント]** フィールドに、コメントを追加します。このコメントは **[アクティビティ]** タブ（単一のノードまたはインシデント全体）に表示され、自分（または他の人）がインシデントを再度利用する際に、操作を実行した原因を思い出すヒントになります。
8. 手順4で **[直ちにネットワークに接続する]** を選択している場合、**[接続]** をクリックします。
   または
   手順4で **[ネットワークに接続する前に、バックアップからワークロードをリカバリする]** を選択している場合、**[リカバリと接続]** をクリックします。
   ワークロードはネットワークに再接続され、ワークロードに対するすべてのネットワークアクセスの制限は解除されます。

注意
また、1つまたは複数の分離済みワークロードに接続するには、Cyber Protectコンソールの **[ワークロード]** > **[エージェントを含むワークロード]** メニューから、関連するワークロードを選択し、右サイドバーで **[ネットワーク分離を管理]** を選択します。表示されたダイアログで、**[接続]** または **[すべて接続]** をクリックして、選択したワークロードをネットワークに再接続します。

ネットワーク除外を管理するには

注意
ワークロードが分離されており、すべてのAcronis Cyber Protect技術が動作している場合でも、追加のネットワーク接続の確立が必要となるシナリオも考えられます（例えば、ワークロードから共有ディレクトリにファイルをアップロードする必要がある場合など）。このようなシナリオでは、ネットワーク除外を追加することができますが、除外を追加する前に、脅威が除去されていることを確認する必要があります。

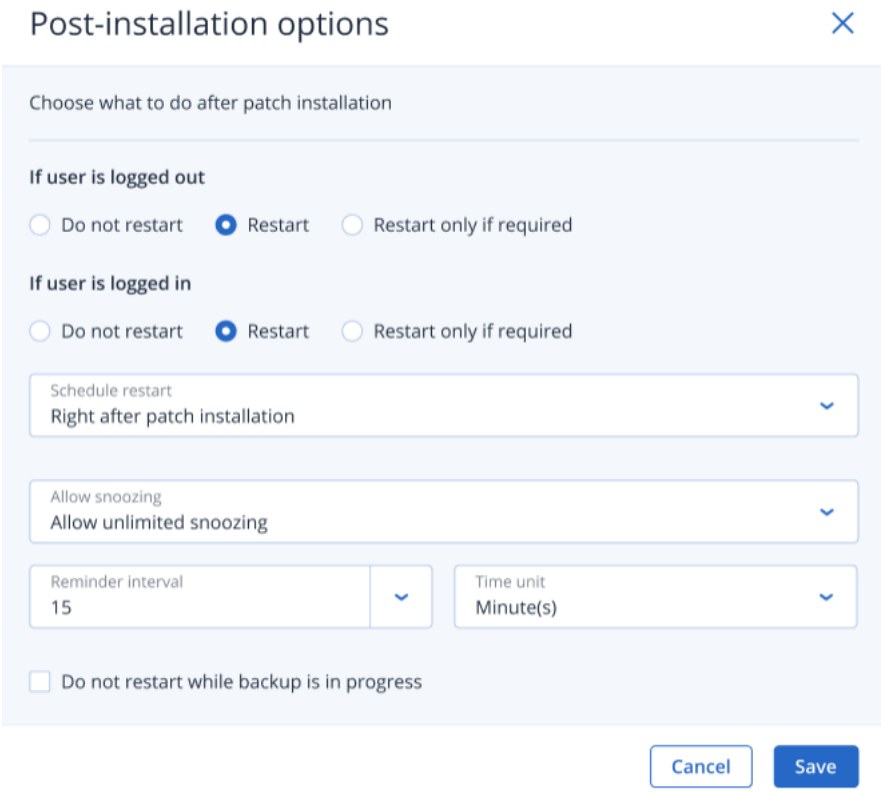
1. **[対応操作]** タブの **[修復]** セクションで、**[ネットワーク除外を管理]** をクリックします。
2. ネットワーク除外のサイドバーで、関連する除外を追加します。利用可能な各オプション（ポート、URLアドレス、ホスト名/IPアドレス）について、以下の操作を実行します。
   a. **[追加]** をクリックし、関連するポート、URLアドレス、またはホスト名/IPアドレスを入力します。
   b. **[トラフィックの方向]** ドロップダウンリストで、**[受信および送信接続]**、**[受信接続のみ]**、**[送信接続のみ]** のいずれかを選択します。
   c. **[追加]** をクリックします。
3. **[保存]** をクリックします。

ワークロードにパッチを適用

EDRでは、自動的にワークロードのパッチの必要性を検出し、パッチを適用することで、将来起こりうる攻撃における脆弱性のエクスプロイトを防止できます。この機能は、パートナーのワークロードでAdvanced Managementのサブスクリプションが有効な場合にのみ利用可能であることに注意してください。

ワークロードにパッチを適用するには

1. サイバーキルチェーンで、パッチを適用したいワークロードのノードをクリックします。
2. 表示されたサイドバーで、**[対応操作]** タブをクリックします。
3. **[修復]** セクションで、**[パッチ]** をクリックします。
4. **[パッチをインストール]** フィールドで、**[選択]** をクリックします。表示されたダイアログで、該当するパッチを選択し、**[選択]** をクリックします。
5. **[インストール後のオプション]** フィールドで、表示されたリンクをクリックします。[インストール後のオプション] ダイアログが表示されます。



6. パッチインストール後に実行する操作を選択します。
   - **ユーザーがログオフしたら:再起動しない**、**再起動**、**必要な場合に限り再起動**のいずれかを選択します。
   - **ユーザーがログインしたら:再起動しない**、**再起動**、**必要な場合に限り再起動**のいずれかを選択します。

     [再起動] を選択した場合、以下の定義も可能です。

- 再起動のスケジュールを設定する。
- スヌーズを許可する（スヌーズ間隔の定義を含む）。

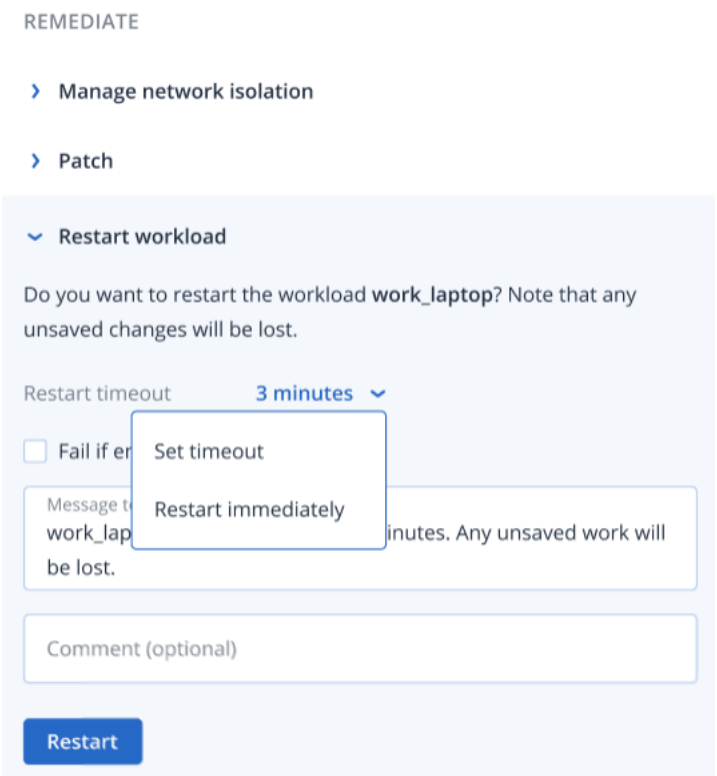
7. （オプション）[**バックアップ中は再起動しない**] チェックボックスを選択して、現在バックアップが進行中の場合にワークロードが再起動されないようにします。
8. [**保存**] をクリックします。
9. [**対応操作**] タブで、[**パッチ**] をクリックします。
   選択済みのパッチが実行されます。この操作は、個別のノードとインシデント全体の [**アクティビティ**] タブで確認することもできます。詳細については、"インシデントを軽減するために実行される操作を理解する"（890ページ）を参照してください。

ワークロードを再起動

EDRでは、攻撃への対処の一環として、ワークロードを直ちに、または事前に定義されたタイムアウト期間に従って再起動できます。

ワークロードを再起動するには

1. サイバーキルチェーンで、再起動のスケジュールを設定したいワークロードのノードをクリックします。
2. 表示されたサイドバーで、[**対応操作**] タブをクリックします。
3. [**修復**] セクションで、[**ワークロードを再起動**] をクリックします。



4. [**再起動のタイムアウト**] フィールドで、表示されたリンクをクリックし、次のいずれかを選択します。
   - **タイムアウトを設定**:[再起動のタイムアウト] ダイアログで、ワークロードの再起動時間を設定し、[**保存**] をクリックします。

- **直ちに再起動**:ワークロードを直ちに再起動する場合に選択します。

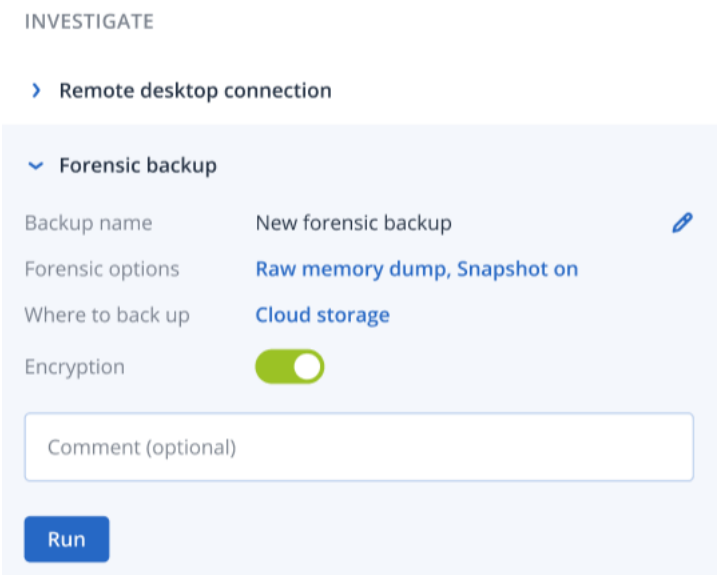
5. （オプション）[**エンドユーザーがログインしている場合、失敗する**] チェックボックスを選択して、ユーザーがログインしている場合にワークロードが再起動されないようにします。
6. [**表示するメッセージ**] フィールドで、分離されたワークロードにユーザーがアクセスするときに表示するメッセージを追加します。
7. （オプション）[**コメント**] フィールドに、コメントを追加します。このコメントは [**アクティビティ**] タブ（単一のノードまたはインシデント全体）に表示され、自分（または他の人）がインシデントを再度利用する際に、操作を実行した原因を思い出すヒントになります。
8. [**再起動**] をクリックします。
   ワークロードは、定義されたスケジュールに従って再起動するように設定されます。この操作は、個別のノードとインシデント全体の [**アクティビティ**] タブで確認することもできます。詳細については、"インシデントを軽減するために実行される操作を理解する"（890ページ）を参照してください。

オンデマンドでワークロードのフォレンジックバックアップを実行

EDRでは、攻撃に関する調査の一環として、監査やさらなる調査のためにオンデマンドでフォレンジックバックアップを実行できます。なおこの機能が利用できるのは、パートナーのワークロードでAdvanced Backupのサブスクリプションが有効な場合のみです。

フォレンジックバックアップを実行するには

1. サイバーキルチェーンで、フォレンジックバックアップを実行したいワークロードのノードをクリックします。
2. 表示されたサイドバーで、[**対応操作**] タブをクリックします。
3. [**調査**] セクションで、[**フォレンジックバックアップ**] をクリックします。



4. （オプション）[**バックアップ名**] フィールドで、編集アイコンをクリックしてバックアップ名を編集します。
5. [**フォレンジックオプション**] フィールドで、表示されたリンクをクリックします。表示されたフォレンジックオプションダイアログで、以下のいずれかを選択します:

- **Rawメモリダンプを収集**
- **カーネルメモリダンプを収集**

また、**[動作中のプロセスのスナップショット]** チェックボックスを選択すると、バックアップを開始した瞬間に実行中のプロセスの情報を追加できます。この情報は、バックアップイメージに保存されます。

[保存] をクリックして、フォレンジックオプションダイアログを閉じます。

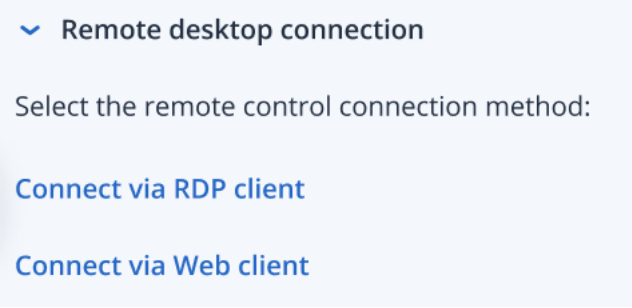
6. **[バックアップ先]** フィールドで、表示されたリンクをクリックし、バックアップのロケーションを定義します。
7. （オプション）暗号化を有効にするには **[暗号化]** オプションをクリックしてください。表示されたダイアログで、暗号化バックアップのパスワードを入力し、関連する暗号化アルゴリズムを選択します。
8. （オプション）**[コメント]** フィールドに、コメントを追加します。このコメントは **［アクティビティ］** タブ（単一のノードまたはインシデント全体）に表示され、自分（または他の人）がインシデントを再度利用する際に、操作を実行した原因を思い出すヒントになります。
9. **[実行]** をクリックします。
   フォレンジックバックアップが開始します。この操作は、個別のノードとインシデント全体の **[アクティビティ]** タブで確認することもできます。詳細については、"インシデントを軽減するために実行される操作を理解する"（890ページ）を参照してください。

ワークロードへのリモート接続

EDRでは、攻撃に関する調査の一環として、調査対象のワークロードにリモートでアクセスできるようになります。

ワークロードにリモート接続するには

1. サイバーキルチェーンで、リモート接続したいワークロードのノードをクリックします。
2. 表示されたサイドバーで、**[対応操作]** タブをクリックします。
3. **[調査]** セクションで、**[リモートデスクトップ接続]** をクリックします。



4. 以下のリモート接続方式のいずれかを選択します。
   - **RDPクライアント経由で接続**:この方法では、リモートデスクトップ接続クライアントのダウンロードとインストールを求めるメッセージが表示されます。その後、コンソールからワークロードにリモート接続できます。
   - **Webクライアント経由で接続**:この方法では、ワークロードにRDPクライアントをインストールする必要がありません。ログイン画面が表示され、そこでリモートのマシンの資格情報を入力する必要があります。

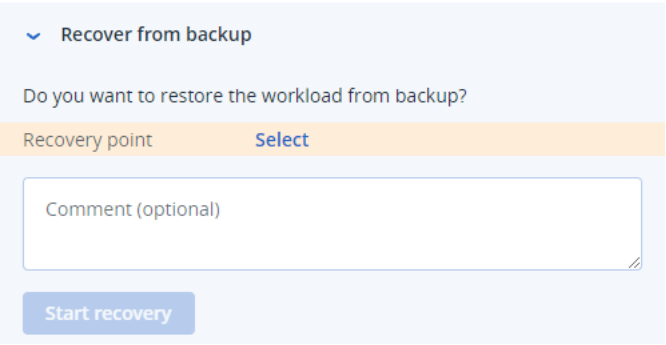
リモート接続が開始された後は、操作を個別のノードとインシデント全体の **[アクティビティ]** タブで確認できます。詳細については、"インシデントを軽減するために実行される操作を理解する"（890ページ）を参照してください。

バックアップから復元

EDRにより、攻撃に対する復元対応の一環として、バックアップからマシン全体、または特定のファイルやフォルダをリカバリできます。

バックアップからワークロードをリカバリするには

1. サイバーキルチェーンで、リカバリしたいワークロードのノードをクリックします。
2. 表示されたサイドバーで、**[対応操作]** タブをクリックします。
3. **[復元]** セクションで、**[バックアップから復元]** をクリックします。



4. **[復元ポイント]** フィールドで **[選択]** をクリックして、以下の手順を実行します。
   a. 表示されたサイドバーで、該当する復元ポイントを選択します。
   b. ワークロード上のすべてのファイルとフォルダを復元するには、**[リカバリ]** > **[ワークロード全体]** をクリックします。
   または
   ワークロード上の特定のファイルとフォルダを復元するには、**[リカバリ]** > **[ファイル/フォルダ]** をクリックします。その後、関連するファイルやフォルダを選択する画面が表示されます。選択した後、**[リカバリする項目]** フィールドの該当する値をクリックすると、復元用に選択した項目を表示することができます。

   注意
   選択した復元ポイントが暗号化されている場合は、パスワードの入力が求められます。

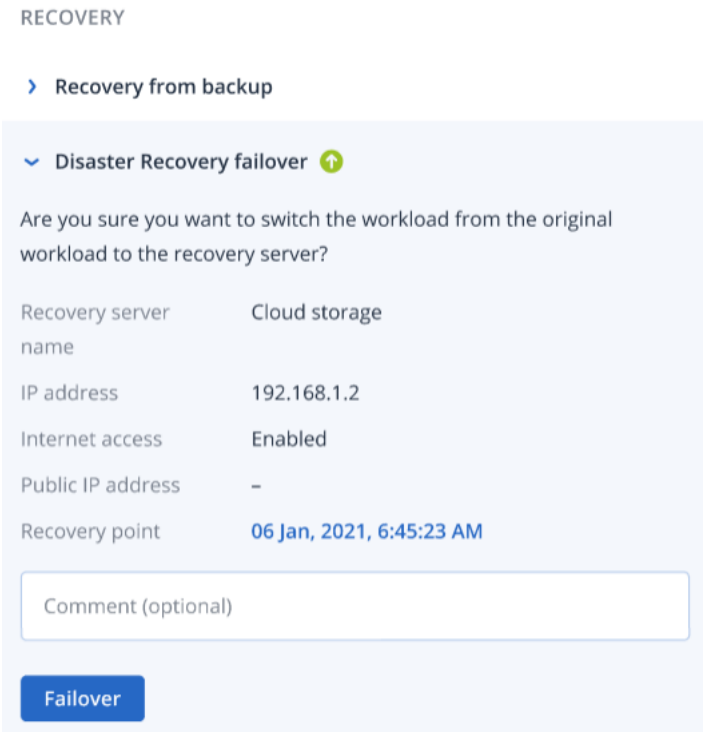
5. （オプション）**[ワークロードの自動的な再起動]** チェックボックスを選択します。このオプションは、手順4で **[リカバリ]** > **[ワークロード全体]** を選択した場合にのみ関連します。
6. （オプション）**[コメント]** フィールドに、コメントを追加します。このコメントは **[アクティビティ]** タブ（単一のノードまたはインシデント全体）に表示され、自分（または他の人）がインシデントを再度利用する際に、操作を実行した原因を思い出すヒントになります。
7. **[復元を開始]** をクリックします。
   ワークロードをリカバリするプロセスが開始されます。この操作の進行状況は、個別のノードとインシデント全体の **[アクティビティ]** タブで確認することができます。詳細については、"インシデントを軽減するために実行される操作を理解する"（890ページ）を参照してください。

ディザスタリカバリフェールオーバー

攻撃に対する復元対応の一環として、EDRでは"ディザスタリカバリを実装する"（714ページ）を実行することで、ワークロードを復元サーバーに切り替えることができます。なお、ワークロードでAdvanced Disaster Recoveryのサブスクリプションが取得されている必要があります。

ディザスタリカバリフェールオーバーを実行するには

1. サイバーキルチェーンで、リカバリしたいワークロードのノードをクリックします。
2. 表示されたサイドバーで、**[対応操作]** タブをクリックします。
3. **[復元]** セクションで、**[ディザスタリカバリフェールオーバー]** をクリックします。



4. **[復元ポイント]** フィールドで、以下の手順を実行します。
   a. 現在の復元ポイントの日付をクリックして、復元ポイントを選択します。
   b. 表示されたサイドバーで、該当する復元ポイントを選択します。

   注意
   Advanced Disaster Recoveryサブスクリプションをお持ちの場合、ディザスタリカバリで作成した該当の復元サーバー（オフラインVM）を選択できます。サブスクリプションをお持ちでない場合は、ディザスタリカバリを構成するよう促されます。

5. （オプション）**[コメント]** フィールドに、コメントを追加します。このコメントは **[アクティビティ]** タブ（単一のノードまたはインシデント全体）に表示され、自分（または他の人）がインシデントを再度利用する際に、操作を実行した原因を思い出すヒントになります。
6. **[フェールオーバー]** をクリックします。

ワークロードは復元サーバーに切り替わります。この操作は、個別のノードとインシデント全体の **[アクティビティ]** タブで確認することができます。詳細については、"インシデントを軽減するために実行される操作を理解する"（890ページ）を参照してください。

不審なプロセスに対する対応操作を定義する

攻撃に対する修復対応の一環として、不審なプロセスに次の操作を適用できます。

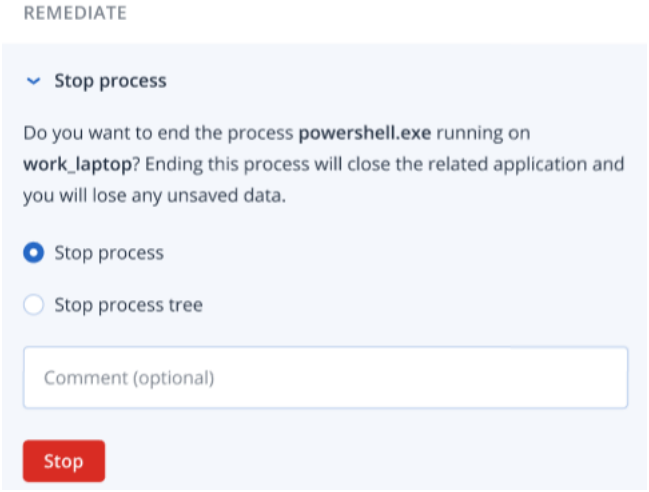
- プロセスを停止する（以下を参照）
- プロセスを隔離する（以下を参照）
- プロセスによる変更をロールバックする（以下を参照）
- 保護計画の許可リストまたはブロックリストにプロセスを追加する（"プロセス、ファイル、ネットワークを保護計画のブロックリストまたは許可リストで追加または削除する"（918ページ）を参照）

不審なプロセスを停止する

1. サイバーキルチェーンで、修復したいプロセスノードをクリックします。

   注意
   Windowsの重要なプロセスや実行されていないプロセスは停止できず、サイバーキルチェーンで無効化されます。

2. 表示されたサイドバーで、**[対応操作]** タブをクリックします。
3. **[修復]** セクションで、**[プロセスを停止]** をクリックします。



4. 次のいずれかを選択します。
   - **プロセスを停止**（特定のプロセスを停止）
   - **プロセスツリーを停止**（特定のプロセスとその子プロセスを停止）
5. （オプション）コメントを追加します。このコメントは **[アクティビティ]** タブ（単一のノードまたはインシデント全体）に表示され、自分（または他のユーザー）がインシデントを再度利用する際に、操作を実行した原因を思い出すヒントになります。

6. **[停止]** をクリックすると、プロセスが停止します。

注意
関連するアプリケーションは終了し、保存されていないデータは失われます。

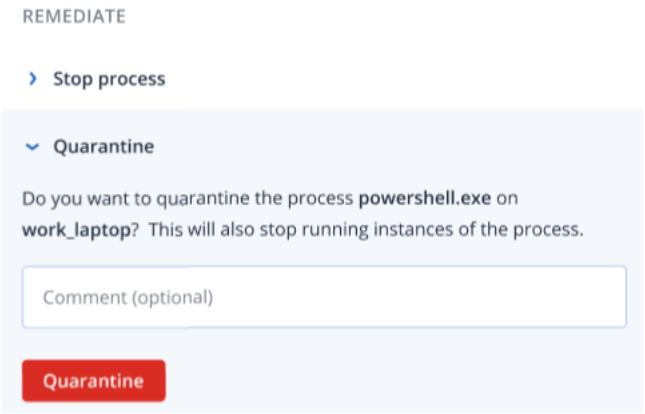
この操作は、個別のノードとインシデント全体の **[アクティビティ]** タブで確認することもできます。詳細については、"インシデントを軽減するために実行される操作を理解する"（890ページ）を参照してください。

不審なプロセスを隔離するには

1. サイバーキルチェーンで、隔離したいプロセスノードをクリックします。

注意
Windowsの重要なプロセスは隔離できず、サイバーキルチェーンで無効化されます。

2. 表示されたサイドバーで、**[対応操作]** タブをクリックします。
3. **[修復]** セクションで、**[検疫]** をクリックします。



4. （オプション）コメントを追加します。このコメントは ［**アクティビティ**］ タブ（単一のノードまたはインシデント全体）に表示され、自分（または他のユーザー）がインシデントを再度利用する際に、操作を実行した原因を思い出すヒントになります。
5. **[検疫]** をクリックします。プロセスが停止され、隔離されます。

注意
このプロセスは、マルウェア対策保護で利用可能な隔離セクションに追加され、管理されます。

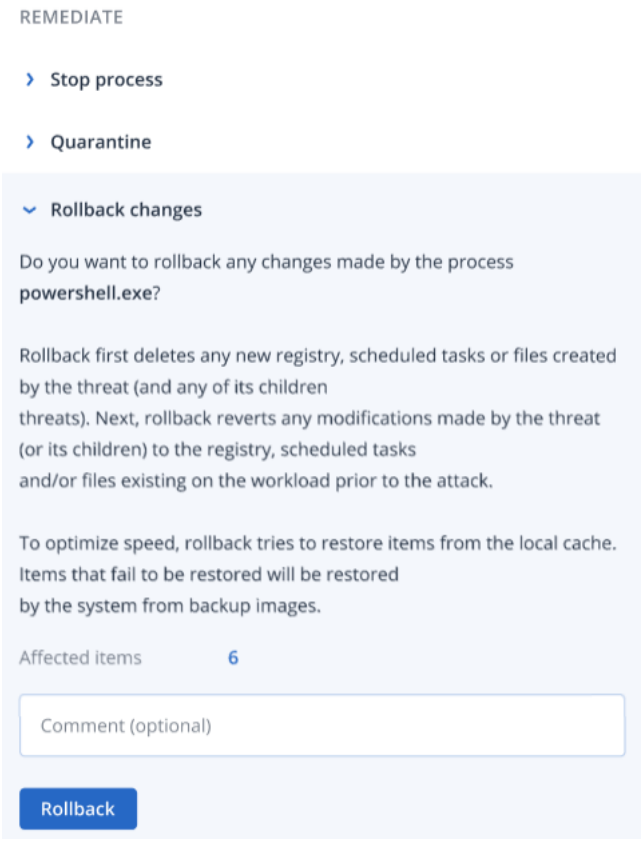
この操作は、個別のノードとインシデント全体の **[アクティビティ]** タブで確認することもできます。詳細については、"インシデントを軽減するために実行される操作を理解する"（890ページ）を参照してください。

ロールバックを変更するには

1. サイバーキルチェーンで、変更をロールバックしたいプロセスノードをクリックします。

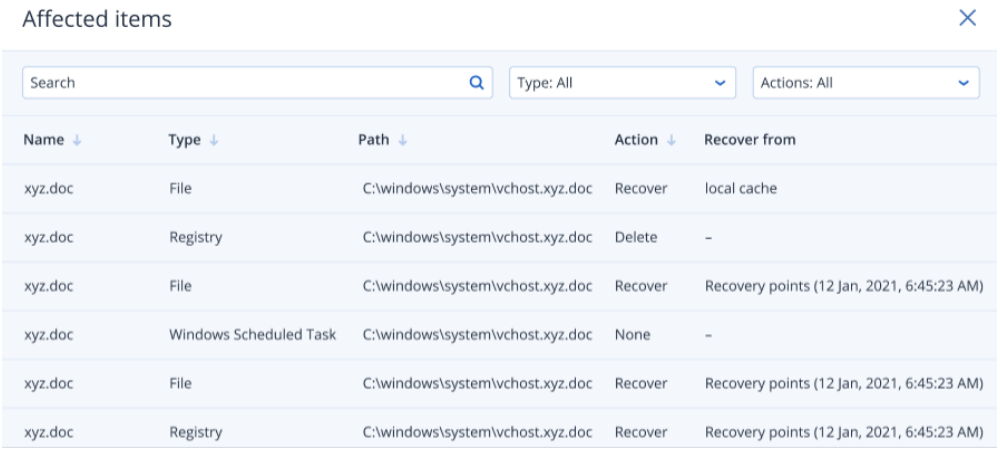
注意
この操作は、検出ノード（赤または黄色で表示されるノード）のみで利用可能です。

2. 表示されたサイドバーで、**[対応操作]** タブをクリックします。
3. **[修復]** セクションで、**[変更をロールバック]** をクリックします。



注意
ロールバック処理では、必ずローカルキャッシュ内の項目からリカバリが実行されます。バックアップアーカイブからのロールバックは今後のリリースで利用可能になる予定です。

4. ロールバックによる変更の影響を受ける項目を表示するには、**影響を受ける項目**リンクをクリックします。表示されるダイアログには、ロールバックによって戻されるすべての項目（ファイル、レジストリ、スケジュールされたタスク）と操作（**削除**、**復元**、**なし**）が表示されます。さらに、復元された項目がローカルキャッシュまたはバックアップの復元ポイントのいずれから復元されるかを確認できます。



5. （オプション）コメントを追加します。このコメントは［**アクティビティ**］タブ（単一のノードまたはインシデント全体）に表示され、自分（または他のユーザー）がインシデントを再度利用する際に、操作を実行した原因を思い出すヒントになります。
6. **[ロールバック]** をクリックします。ロールバック機能は、プロセスによって行われたレジストリ、ファイル、スケジュールされたタスクの変更を元に戻すものです。以下の手順によって実行できます。
   a. 脅威（およびその子脅威）によって作成された新しいエントリ（レジストリ、スケジュールされたタスク、ファイル）はすべて削除されます。
   b. 脅威（およびその子脅威）が、攻撃前にワークロード上に存在したレジストリ、スケジュールされたタスク/ファイルに加えた変更は、すべて元に戻されます。
   c. ロールバックでは、ローカルキャッシュを利用した項目のリカバリが試行されます。リカバリできない項目については、EDRがクリーンなバックアップイメージから自動的にリカバリします。

   このロールバック操作は、個別のノードとインシデント全体の **[アクティビティ]** タブで確認することもできます。詳細については、"インシデントを軽減するために実行される操作を理解する"（890ページ）を参照してください。

不審なファイルに対する対応操作を定義する

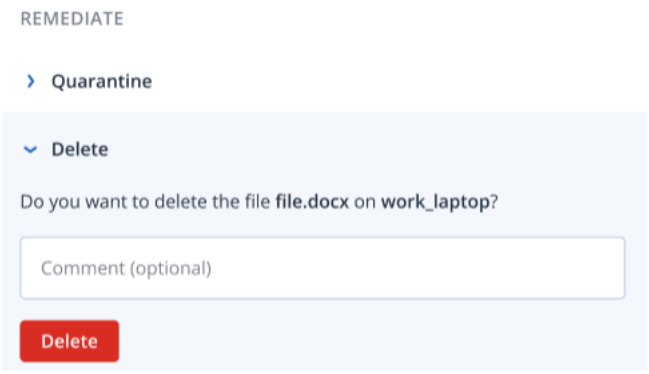
攻撃に対する修復対応の一環として、不審なファイルに次の操作を適用できます。

- ファイルを削除（下記参照）
- ファイルを隔離（下記参照）
- 保護計画の許可リストまたはブロックリストにファイルを追加する（"プロセス、ファイル、ネットワークを保護計画のブロックリストまたは許可リストで追加または削除する"（918ページ）を参照）

不審なファイルを削除するには

1. サイバーキルチェーンで、修復したいファイルノードをクリックします。
2. 表示されたサイドバーで、**[対応操作]** タブをクリックします。

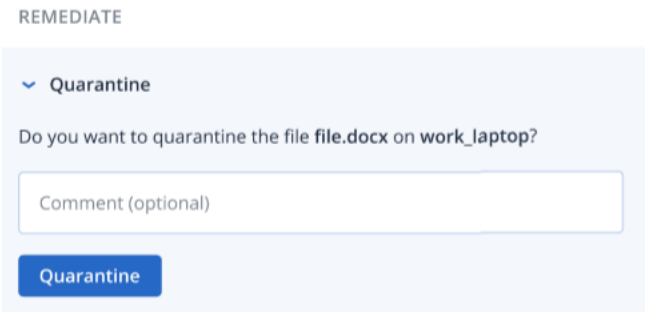
3. **[修復]** セクションで、**[削除]** をクリックします。



4. （オプション）コメントを追加します。このコメントは **［アクティビティ］** タブ（単一のノードまたはインシデント全体）に表示され、自分（または他のユーザー）がインシデントを再度利用する際に、操作を実行した原因を思い出すヒントになります。
5. **[削除]** をクリックします。
   ファイルが削除されます。この操作は、個別のノードとインシデント全体の **[アクティビティ]** タブで確認することもできます。詳細については、"インシデントを軽減するために実行される操作を理解する"（890ページ）を参照してください。

不審なファイルを隔離するには

1. サイバーキルチェーンで、修復したいファイルノードをクリックします。
2. 表示されたサイドバーで、**[対応操作]** に移動します。
3. **[修復]** セクションで、**[検疫]** をクリックします。



4. （オプション）コメントを追加します。このコメントは **［アクティビティ］** タブ（単一のノードまたはインシデント全体）に表示され、自分（または他のユーザー）がインシデントを再度利用する際に、操作を実行した原因を思い出すヒントになります。
5. **[検疫]** をクリックします。
   ファイルは隔離されます。この操作は、個別のノードとインシデント全体の **[アクティビティ]** タブで確認することもできます。詳細については、"インシデントを軽減するために実行される操作を理解する"（890ページ）を参照してください。

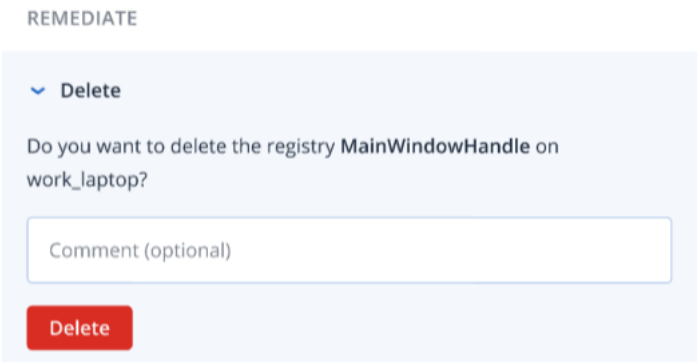
不審なレジストリエントリに対する対応操作を定義する

攻撃に対する修復対応の一環として、不審なレジストリエントリを削除できます。

このオプションはレジストリのサイバーキルチェーンノードで利用できます。

不審なレジストリエントリを削除するには

1. サイバーキルチェーンで、修復したいノードをクリックします。
2. 表示されたサイドバーで、**[対応操作]** タブをクリックします。
3. **[修復]** セクションで、**[削除]** をクリックします。



4. （オプション）コメントを追加します。このコメントは **［アクティビティ］** タブ（単一のノードまたはインシデント全体）に表示され、自分（または他のユーザー）がインシデントを再度利用する際に、操作を実行した原因を思い出すヒントになります。
5. **[削除]** をクリックします。
   レジストリエントリが削除されます。この操作は、個別のノードとインシデント全体の **[アクティビティ]** タブで確認することもできます。詳細については、"インシデントを軽減するために実行される操作を理解する"（890ページ）を参照してください。

プロセス、ファイル、ネットワークを保護計画のブロックリストまたは許可リストで追加または削除する

攻撃に対する予防的対応の一環として、保護計画の許可リストまたはブロックリストにノードを追加できます。

ノードの安全性が確認済みで、今後検出されないようにしたい場合、ノードを許可リストに追加できます。ノードをブロックリストに追加し、今後そのノードが実行されないようにします。

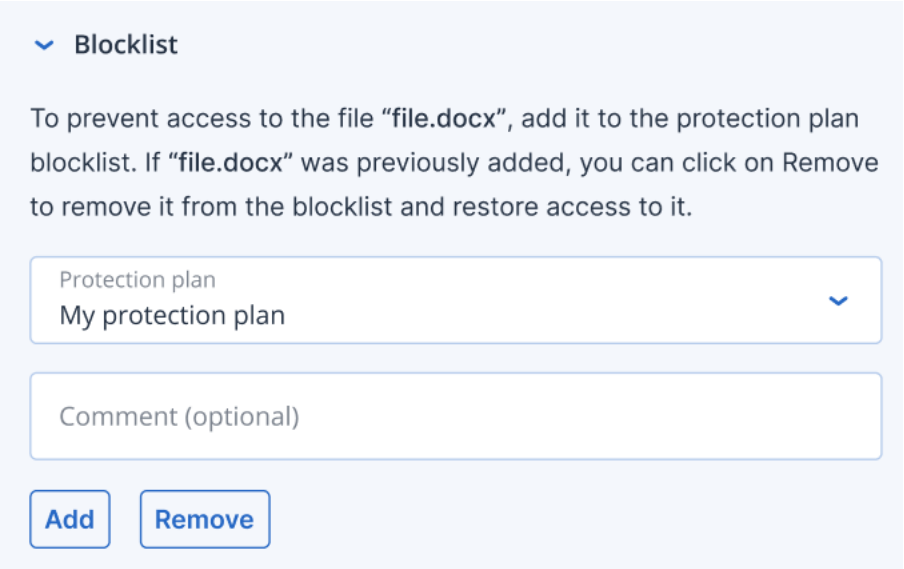
また、許可リストまたはブロックリストからノードを削除して、そのノードへの今後のアクセスを許可または防止することもできます。

このオプションは以下のサイバーキルチェーンノードで利用できます。

- プロセス
- ファイル
- ネットワーク

プロセス、ファイル、ネットワークを保護計画のブロックリストで追加または削除するには

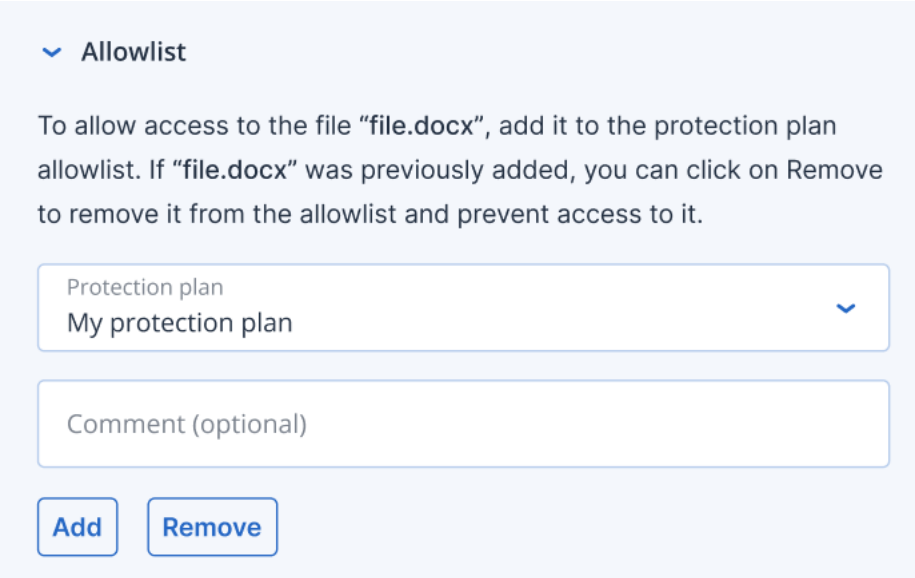
1. サイバーキルチェーンで、修復したいプロセス、ファイル、またはネットワークノードをクリックします。
2. 表示されたサイドバーで、**[対応操作]** タブをクリックします。
3. **[防止]** セクションで、**[ブロックリスト]** の横の矢印アイコンをクリックします。



4. この操作を適用したい関連する保護計画を選択します。
5. （オプション）コメントを追加します。このコメントは［**アクティビティ**］タブ（単一のノードまたはインシデント全体）に表示され、自分（または他のユーザー）がインシデントを再度利用する際に、操作を実行した原因を思い出すヒントになります。
6. **[追加]** をクリックします。
   操作が実行され、プロセス、ファイル、またはネットワークは今後起動されないようになります。
   また、プロセス、ファイル、またはネットワークが以前にブロックリストに追加されているけれど、現在はブロックリストから削除したい場合は、**[削除]** をクリックします。これにより、今後そのノードにアクセスできるようになります。
   この追加または削除の操作は、個別のノードとインシデント全体の **[アクティビティ]** タブで確認することもできます。詳細については、「"インシデントを軽減するために実行される操作を理解する"（890ページ）」を参照してください。

プロセス、ファイル、ネットワークを保護計画の許可リストで追加または削除するには

1. サイバーキルチェーンで、修復したいプロセス、ファイル、またはネットワークノードをクリックします。
2. 表示されたサイドバーで、**[対応操作]** タブをクリックします。
3. **[防止]** セクションで、**[許可リスト]** の横の矢印アイコンをクリックします。



4. この操作を適用したい関連する保護計画を選択します。
5. （オプション）コメントを追加します。このコメントは［**アクティビティ**］タブ（単一のノードまたはインシデント全体）に表示され、自分（または他のユーザー）がインシデントを再度利用する際に、操作を実行した原因を思い出すヒントになります。
6. **[追加]** をクリックします。
   操作が実行され、プロセス、ファイル、またはネットワークは今後検出されないようになります。
   また、プロセス、ファイル、またはネットワークが以前に許可リストに追加されているけれど、現在は許可リストから削除したい場合は、**[削除]** をクリックします。これにより、今後そのノードにアクセスできないようになります。
   この追加または削除の操作は、個別のノードとインシデント全体の **[アクティビティ]** タブで確認することもできます。詳細については、「"インシデントを軽減するために実行される操作を理解する"（890ページ）」を参照してください。

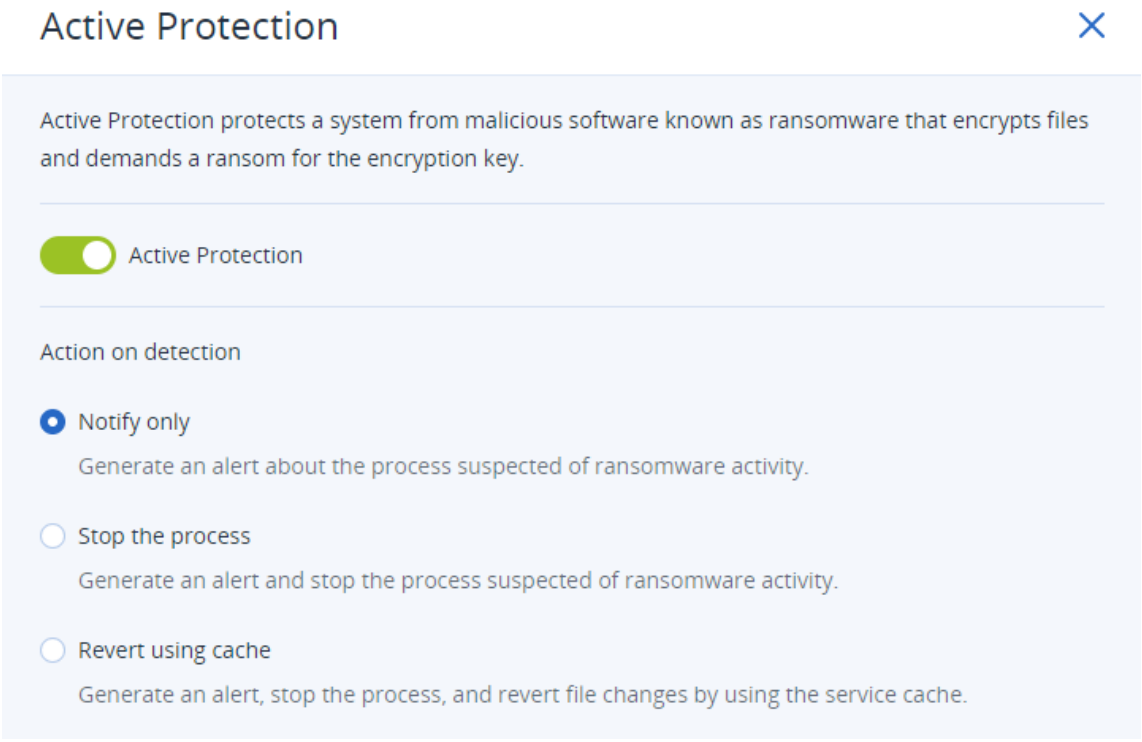
エンドポイント検知と応答（EDR）の監視モードを有効にする

Cyber Protectionの監視モードでは、製品環境でEDRを使用できます。これにより、偽陽性をチェックして、EDRの配置が完了する前に不必要な項目を除外できます。

監視モードでは、項目がブロックされたり、停止させられたりすることはなく、インシデントが作成されます。ただし、応答が初期化されることはありません。

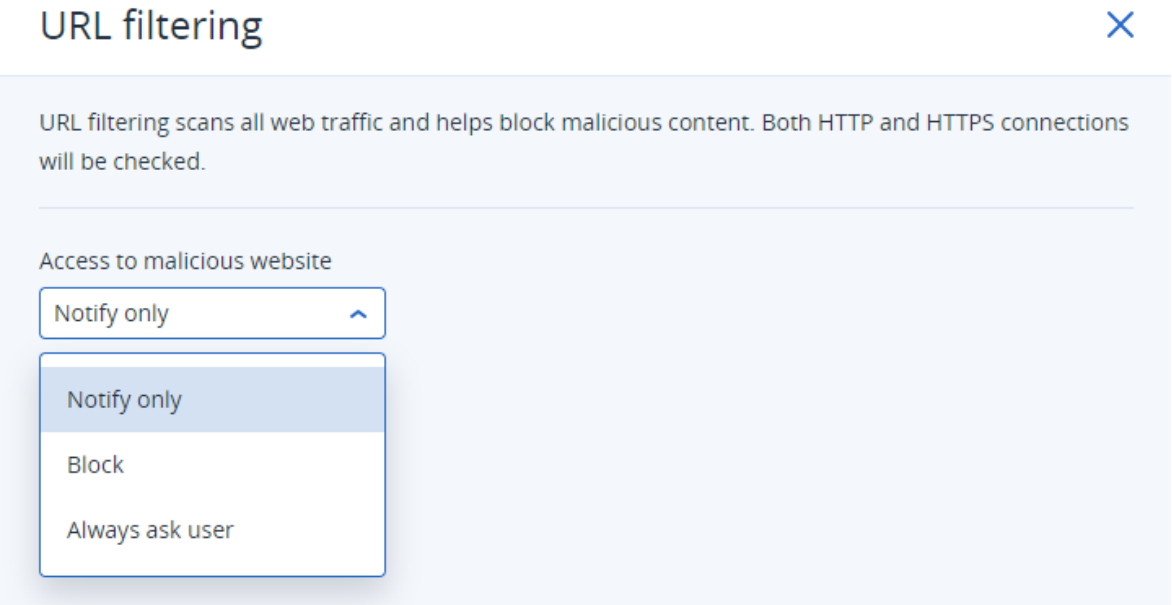
EDRの監視モードを有効にするには

1. 関連する保護計画で、EDRが有効になっていることを確認してください。詳細については、"エンドポイント検知と応答（EDR）機能を有効にする"（872ページ）を参照してください。
2. **ウイルスおよびマルウェア対策保護**モジュールを展開し、次の項目を定義します。
   - **[Active Protection]** をクリックし、**[検出時の操作]** セクションで、**[通知のみ]** を選択します。その後、**[完了]** をクリックします。詳細については、"Active Protection"（802ページ）を参照してください。



- **[振る舞い検知エンジン]** をクリックし、**[検出時の操作]** セクションで、**[通知のみ]** を選択します。その後、**[完了]** をクリックします。詳細については、"振る舞い検知エンジン"（806ページ）を参照してください。
- **[エクスプロイト防止]** をクリックし、**[検出時の操作]** セクションで、**[通知のみ]** を選択します。その後、**[完了]** をクリックします。詳細については、"エクスプロイト防御"（807ページ）を参照してください。
- **[リアルタイム保護]** をクリックし、**[検出時の操作]** セクションで、**[通知のみ]** を選択します。その後、**[完了]** をクリックします。詳細については、"リアルタイム保護"（809ページ）を参照してください。
- **[スケジュールスキャン]** をクリックし、**[検出時の操作]** セクションで、**[通知のみ]** を選択します。その後、**[完了]** をクリックします。詳細については、"スケジュールスキャン"（810ページ）を参照してください。

3. **URLフィルタリング**モジュールを展開し、**[悪意のあるWebサイトへのアクセス]** ドロップダウンリストで、**[通知のみ]** を選択します。その後、**[完了]** をクリックします。詳細については、"URLフィルタ処理"（824ページ）を参照してください。



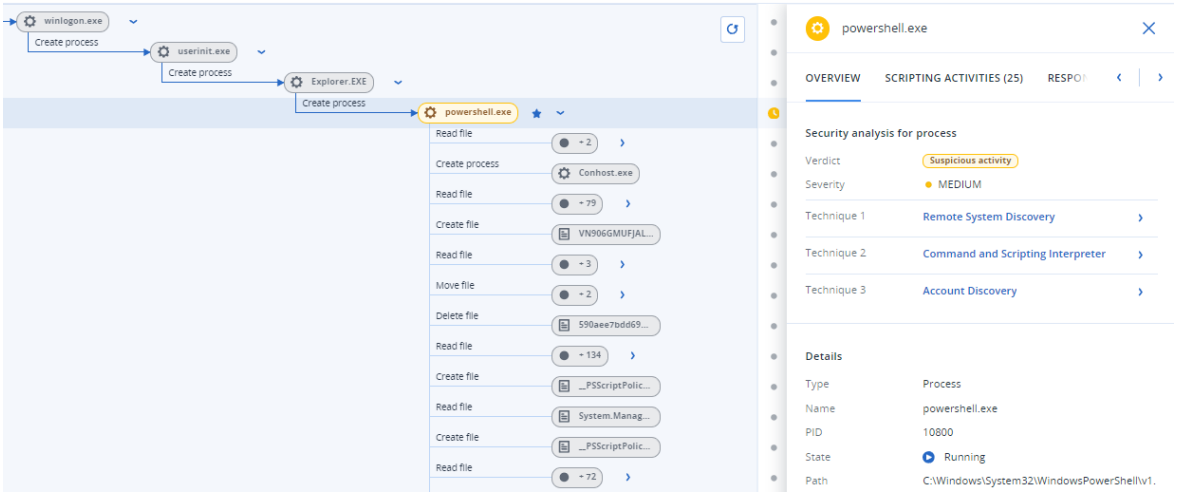
エンドポイント検知と応答（EDR）が正しく機能しているかどうかをテストする方法

EDRが配置されていて、正常に動作していることを確認するために、EDR検出のトリガーとなるコマンドをいくつか実行することができます。

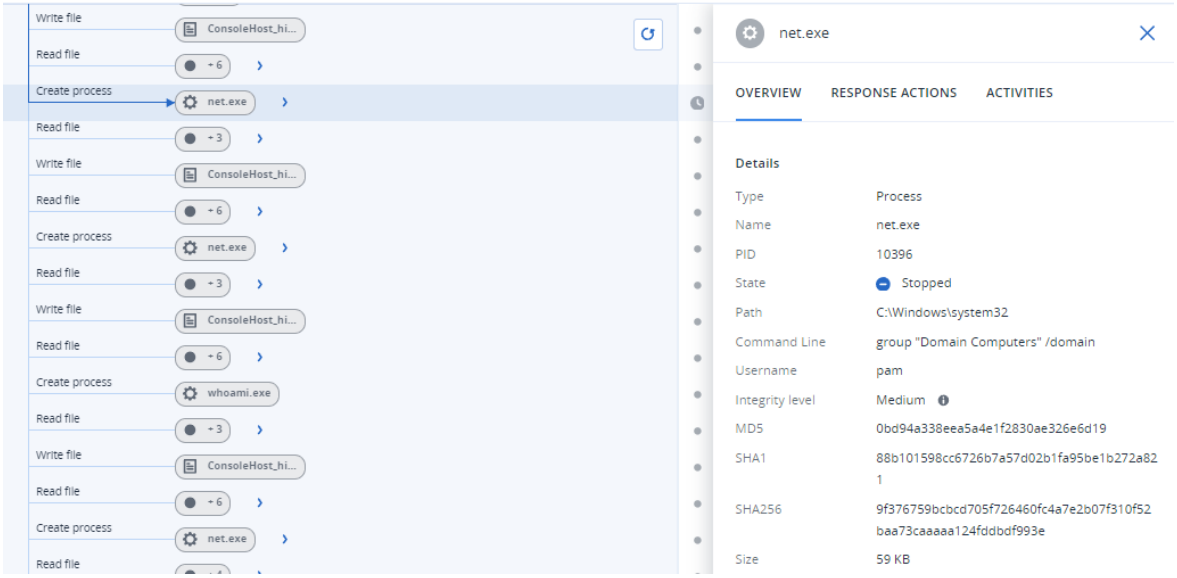
注意
EDRが配置されていれば、不正なアクティビティがあった場合にすぐにインシデントを確認できます。数日間新しいインシデントが発生していない場合、以下の手順により、EDRが機能しているかどうかを確認できます。

EDRが配置されていて、正常に動作しているかどうかをテストするには

1. ドメインに参加しているActive Directoryのユーザーアカウントにログインします。
2. Windows PowerShellで、次の2つのコマンドを実行します。
   - `net group "Domain Computers" /domain`
   - `net user administrator /domain`
3. Cyber Protectコンソールで、**[保護]** > **[インシデント]** に進み、生成されたインシデントを確認します。
   また、以下の例のように、発生した重大度が**中**のインシデントをクリックして、EDRサイバーキルチェーンに表示し、前の手順で実行したPowerShellコマンドを確認することもできます。



4. Windows PowerShellで、次のコマンドを実行します。
   - `c:\>whoami`
   - `c:\>net localgroup`
   - `c:\>net localgroup administrators`
   - `c:\>powershell -command start-process cmd -verb runas`
   - `c:\WINDOWS\system32>net user administrator /active:yes`
   - `c:\>powershell -command Get-Hotfix`
5. EDRサイバーキルチェーンで、実行可能ノード（**net.exe**または**whoami.exe**など）をクリックすると、コマンドラインで実行されたPowerShellコマンドがそのまま表示されます。これらのコマンドは、下の例の **[概要]** タブの**詳細**セクションに表示されています。



6. EDRインシデントが生成されたことを確認したら、手動でインシデントの**脅威ステータス**を**軽減済み**に、**調査ステータス**を**終了**に設定します。詳細については、"サイバーキルチェーンでインシデントを調査する方法"（882ページ）を参照してください。インシデントにコメントを入力して、これがテストインシデントであることを明示することもできます。

脆弱性評価とパッチ管理を実施する

脆弱性診断（VA）は、システムで見つかった脆弱性を特定、定量化、優先順位付けするプロセスです。脆弱性診断モジュールでは、マシンをスキャンして脆弱性を確認し、オペレーティングシステムとインストールされているアプリケーションが最新で正しく動作しているかどうかを確認できます。

脆弱性診断スキャンは、次のオペレーティングシステムを搭載したマシンでサポートされています。

- Windows。詳細については、"サポート対象のMicrosoft製品とサードパーティ製品"（924ページ）を参照してください。
- macOS。詳細については、"サポート対象のApple製品とサードパーティ製品"（926ページ）を参照してください。
- Linux（CentOS 7/Virtuozzo/Acronis Cyber Infrastructure）マシン。 詳細については、"サポートされているLinux製品"（927ページ）を参照してください。

パッチ管理（PM）を使用して、マシンにインストールされているアプリケーションやオペレーティングシステムのパッチ（アップデート）を管理し、システムを常に最新の状態に保ちます。パッチ管理のモジュールでは、マシンにアップデートをインストールする処理を自動または手動で承認できます。

パッチ管理は、Windowsオペレーティングシステムを搭載したマシンでサポートされています。詳細については、"サポート対象のMicrosoft製品とサードパーティ製品"（924ページ）を参照してください。

脆弱性診断

脆弱性診断プロセスは、次の手順で構成されています。

1. 脆弱性診断のモジュールを有効にして保護計画を作成し、脆弱性診断の設定を指定し、計画をマシンに割り当てます。
2. スケジュールモードでもオンデマンドモードでも、脆弱性診断スキャンを実行するコマンドが、マシンにインストールされているプロテクションエージェントに送信されます。
3. コマンドを受け取ったエージェントは、マシンに脆弱性があるかどうかを調べるためのスキャンを開始し、スキャンアクティビティを生成します。
4. 脆弱性診断スキャンが完了すると、エージェントが結果を生成して監視サービスに送信します。
5. 監視サービスは、エージェントから送られてきたデータを処理し、検出された脆弱性のリストを脆弱性評価ウィジェットに表示します。
6. 検出された脆弱性のリストが表示されたら、そのリストを処理して、どの脆弱性を解決する必要があるかを決定できます。

[監視] > **[概要]** > **脆弱性/既存の脆弱性**のウィジェットで、脆弱性診断の結果を監視できます。

サポート対象のMicrosoft製品とサードパーティ製品

以下のMicrosoft製品およびWindowsオペレーティングシステム用のサードパーティ製品が脆弱性診断およびパッチ管理でサポートされています。

サポート対象のMicrosoft製品

Windows OS

- Windows 7（Enterprise、Professional、Ultimate）
- Windows 8
- Windows 8.1
- Windows 10
- Windows 11

Windows Server OS

- Windows Server 2022
- Windows Server 2019
- Windows Server 2016
- Windows Server 2012 R2
- Windows Server 2012
- Windows Server 2008 R2

Microsoft Officeと関連コンポーネント

- Microsoft Office 2019 (x64, x86)
- Microsoft Office 2016 (x64, x86)
- Microsoft Office 2013 (x64, x86)
- Microsoft Office 2010 (x64, x86)

Windows OSの関連コンポーネント

- Internet Explorer
- Microsoft EDGE
- Windows Media Player
- .NET Framework
- Visual Studioとアプリケーション
- オペレーティングシステムのコンポーネント

サーバーアプリケーション

- Microsoft SQL Server 2008 R2
- Microsoft SQL Server 2012
- Microsoft SQL Server 2014
- Microsoft SQL Server 2016
- Microsoft SQL Server 2017
- Microsoft SQL Server 2019
- Microsoft Exchange Server 2013
- Microsoft Exchange Server 2016

- Microsoft Exchange Server 2019
- Microsoft SharePoint Server 2016
- Microsoft SharePoint Server 2019

Windows OSでサポートされているサードパーティ製品

リモートワークは世界中でますます広がっているため、コラボレーションとコミュニケーションツール、VPNクライアントが、常に最新の状態を保ち、考えられる脆弱性が検査されることが重要となっています。Cyber Protectionサービスは、このようなアプリケーションの脆弱性評価とパッチ管理をサポートします。

コラボレーションおよびコミュニケーションツール、VPNクライアント

- Microsoft Teams
- Zoom
- Skype
- Slack
- Webex
- NordVPN
- TeamViewer

Windows OSでサポートされる、サードパーティ製品の詳細については、「パッチ管理がサポートするサードパーティ製品のリスト（62853）」を参照してください。

サポート対象のApple製品とサードパーティ製品

以下のApple製品およびmacOS用のサードパーティ製品が脆弱性診断でサポートされています。

サポートされているApple製品

macOS

- macOS 10.13.x以降

macOSの組み込みアプリケーション

- Safari、iTunes、その他。

macOSでサポートされているサードパーティ製品

- Microsoft Office（Word、Excel、PowerPoint、Outlook、OneNote）
- Adobe Acrobat Reader
- Google Chrome
- Firefox
- Opera
- Zoom
- Skype

- Thunderbird
- VLCメディアプレイヤー

サポートされているLinux製品

VAでサポート対象になっているLinuxディストリビューションとバージョンを以下にまとめます。

- Virtuozzo 7.x
- CentOS 7.x
- CentOS 8.x

脆弱性診断の設定

脆弱性診断のモジュールを組み込んだ保護計画を作成する方法については、「保護計画の作成」を参照してください。VAスキャンは、スケジュールに基づいて実行することも、オンデマンドで実行することも可能です（オンデマンドで実行する場合は、保護計画の **[今すぐ実行]** アクションを使用します）。

脆弱性診断モジュールでは、次の設定を指定できます。

スキャン対象

脆弱性に関するスキャンを実行するソフトウェア製品を定義します。

- Windowsマシン:
  - **Microsoft製品**
  - **Windowsサードパーティ製品**（Windows OSでサポートされる、サードパーティ製品の詳細については、「パッチ管理がサポートするサードパーティ製品のリスト（62853）」を参照してください）
- macOSマシン:
  - **Apple製品**
  - **macOSのサードパーティ製品**
- Linuxマシン:
  - **Linuxパッケージのスキャン**

スケジュール

選択したマシンで脆弱性診断スキャンを実行するスケジュールを定義します。

フィールド	説明
次のイベントを使ってタスクの実行スケジュールを設定します	この設定は、タスクがいつ実行されるかを定義します。 次の値を使用できます。 • **時刻でスケジュール** - これはデフォルト設定です。タスクは指定した時間に実行されます。 • **システムへのユーザーログイン時** - デフォルトでは、いずれかのユーザーがログインするとタスクが開始されます。特定のユーザーアカウ

フィールド	説明
	ントのみがタスクをトリガーできるように、この設定を変更できます。 • **システムへのユーザーログオフ時** - デフォルトでは、いずれかのユーザーがログオフするとタスクが開始されます。特定のユーザーアカウントのみがタスクをトリガーできるように、この設定を変更できます。 **注意** このタスクは、システムのシャットダウン時には実行されません。シャットダウンとログオフは、スケジューリング構成における別個のイベントです。 • **システムの起動時** - オペレーティングシステムが起動するときにタスクが実行されます。 • **システムのシャットダウン時** - オペレーティングシステムがシャットダウンするときにタスクが実行されます。
スケジュールの種類	このフィールドは、**[次のイベントを使ってタスクの実行スケジュールを設定]** で **[時刻でスケジュール]** を選択した場合に表示されます。 次の値を使用できます。 • **月単位** - タスクを実行する該当月と、その月内の週または日を選択します。 • **日単位** - これはデフォルト設定です。タスクを実行する週中の日を選択しします。 • **時間単位** - タスクを実行する週中の日、繰り返しの回数、時間間隔を選択しします。
開始時刻	このフィールドは、**[次のイベントを使ってタスクの実行スケジュールを設定]** で **[時刻でスケジュール]** を選択した場合に表示されます。 タスクを実行する正確な時間を選択します。
日付範囲内に実行	このフィールドは、**[次のイベントを使ってタスクの実行スケジュールを設定]** で **[時刻でスケジュール]** を選択した場合に表示されます。 設定したスケジュールが有効な日付範囲を指定します。
ユーザーアカウントを指定し、そのアカウントがオペレーティングシステムにログインしたときにタスクを開始	このフィールドは、**[次のイベントを使ってタスクの実行スケジュールを設定]** で **[システムへのユーザーログイン時]** を選択した場合に表示されます。 次の値を使用できます。 • **任意のユーザー** - いずれかのユーザーがログインしたときにタスクを開始させたい場合は、このオプションを使用します。 • **次のユーザー** - 指定したユーザーアカウントのログインでタスクを開始させたい場合は、このオプションを使用します。

フィールド	説明
ユーザーアカウントを指定し、そのアカウントがオペレーティングシステムからログアウトしたときにタスクを開始	このフィールドは、**[次のイベントを使ってタスクの実行スケジュールを設定]** で **[システムへのユーザーログオフ時]** を選択した場合に表示されます。 次の値を使用できます。 • **任意のユーザー** - いずれかのユーザーがログアウトしたときにタスクを開始させたい場合は、このオプションを使用します。 • **次のユーザー** - 指定したユーザーアカウントのログアウトでタスクを開始させたい場合は、このオプションを使用します。
開始条件	すべての条件を定義して、同時に満たされたときにタスクを実行する条件を指定します。 マルウェア対策スキャンの開始条件は、**バックアップモジュール**の開始条件に類似しています。「開始条件」を参照してください。 以下のような追加の開始条件を定義できます。 • **時間枠内でタスク開始時間を分散する** - このオプションを使用すると、タスクを実行する時間枠を設定して、ネットワークのボトルネックを回避できます。遅延時間を、時間または分単位で指定できます。たとえばデフォルトの開始時間が10:00 AMで、遅延を60分とした場合、タスクは10:00 AMから11:00 AMの間に開始されます。 • **マシンの電源が入っていないため実行されなかったタスクを起動時に実行する** • **タスク実行中はスリープモードや休止モードに入らない** - このオプションは、Windowsを実行しているマシンに対してのみ有効です。 • **開始条件を満たさない場合でも、次の時間の経過後にタスクを実行** - 他の開始条件にかかわらずタスクが実行されるまでの時間を指定します。 **注意** 開始条件は、Linuxではサポートされていません。

Windowsマシンの脆弱性診断

WindowsマシンおよびWindows向けサードパーティ製品の脆弱性をスキャンできます。

Windowsマシンの脆弱性診断を構成するには

1. Cyber Protectコンソールで、保護計画を作成し、**脆弱性診断**モジュールを有効にします。
2. 脆弱性診断の設定を指定する
   - **スキャンの対象** - **Microsoft製品**、**Windowsのサードパーティ製品**、またはその両方を選択します。
   - **スケジュール** - 脆弱性診断の実行スケジュールを指定します。

   [スケジュール] オプションの詳細については、「"脆弱性診断の設定"（927ページ）」を参照してく

ださい。

3. 保護計画をWindowsマシンに割り当てます。

脆弱性診断スキャンの後、見つかった脆弱性のリストを参照できます。その情報を処理して、どの脆弱性を解決する必要があるかを決定できます。

脆弱性診断の結果を監視するには、**[監視]** > **[概要]** > **[脆弱性/既存の脆弱性]** ウィジェットを確認します。

Linuxマシンの脆弱性診断

Linuxマシンをスキャンして、アプリケーションレベルおよびカーネルレベルの脆弱性を確認できます。

Linuxマシンの脆弱性診断を構成するには

1. Cyber Protectコンソールで、保護計画を作成し、**脆弱性診断**モジュールを有効にします。
2. 脆弱性診断の設定を指定する
   - **スキャン対象** - **Linuxパッケージのスキャン**を選択します。
   - **スケジュール** - 脆弱性診断の実行スケジュールを指定します。

   [スケジュール] オプションの詳細については、「"脆弱性診断の設定"（927ページ）」を参照してください。
3. 保護計画をLinuxマシンに割り当てます。

脆弱性診断スキャンの後、見つかった脆弱性のリストを参照できます。その情報を処理して、どの脆弱性を解決する必要があるかを決定できます。

脆弱性診断の結果を監視するには、**[監視]** > **[概要]** > **[脆弱性/既存の脆弱性]** ウィジェットを確認します。

macOSデバイスの脆弱性診断

macOSデバイスをスキャンして、オペレーティングシステムレベルおよびアプリケーションレベルの脆弱性を見つけることができます。

macOSデバイスの脆弱性診断を構成するには

1. Cyber Protectコンソールで、保護計画を作成し、**脆弱性診断**モジュールを有効にします。
2. 脆弱性診断の設定を指定する
   - **スキャンの対象** - **Apple製品**、**macOSのサードパーティ製品**、またはその両方を選択します。
   - **スケジュール** - 脆弱性診断の実行スケジュールを指定します。

   [スケジュール] オプションの詳細については、「"脆弱性診断の設定"（927ページ）」を参照してください。
3. 計画をmacOSデバイスに割り当てます。

脆弱性診断スキャンの後、見つかった脆弱性のリストを参照できます。その情報を処理して、どの脆弱性を解決する必要があるかを決定できます。

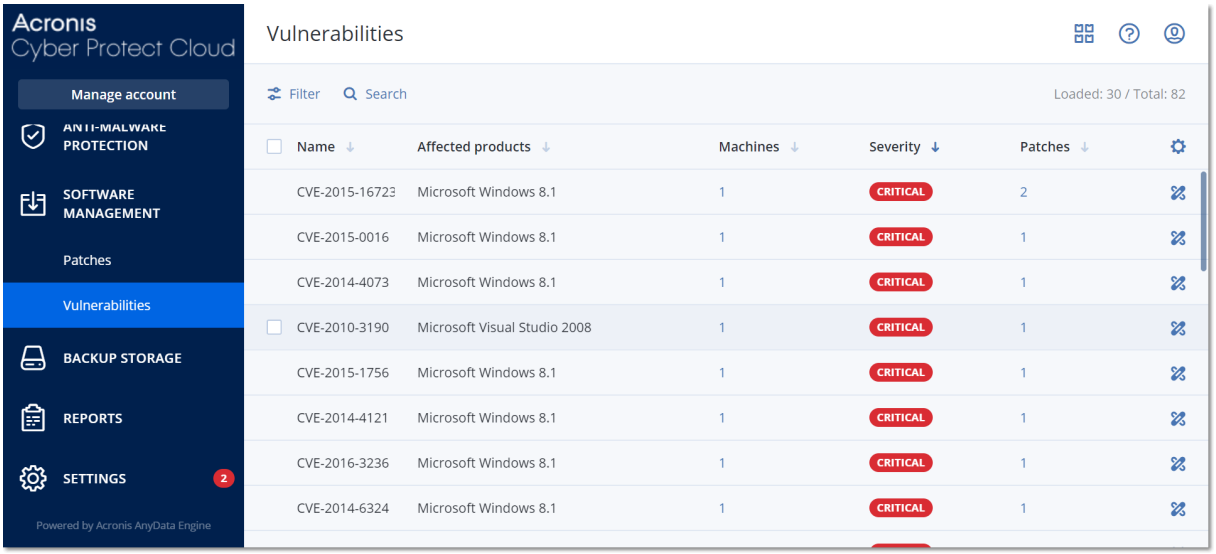
脆弱性診断の結果を監視するには、**[監視]** > **[概要]** > **[脆弱性/既存の脆弱性]** ウィジェットを確認します。

検出された脆弱性の管理

脆弱性診断を少なくとも一度実行した上で、脆弱性が検出されている場合は、**[ソフトウェア管理]** > **[脆弱性]** にその脆弱性が表示されます。脆弱性のリストには、インストールできるパッチがある脆弱性と、推奨パッチがない脆弱性の両方が表示されます。フィルタを使用して、パッチのある脆弱性だけを表示することもできます。

名前	説明
名前	脆弱性の名前。
影響を受けた製品	脆弱性が検出されたソフトウェア製品。
マシン	影響を受けたマシンの数。
重大度	検出された脆弱性の重大度。共通脆弱性評価システム（CVSS）に従って、次のレベルのいずれかで示されます。 • **重大**:9～10 CVSS • **高**:7～9 CVSS • **中**:3～7 CVSS • **低**:0～3 CVSS • **なし**
パッチ	該当するパッチの数。
公開	脆弱性がCommon Vulnerabilities and Exposures（CVE）に公開された日時。
検出	マシンで既存の脆弱性が最初に検出された日付。

検出された脆弱性の説明を確認するには、リストで脆弱性の名前をクリックします。



脆弱性の修復プロセスを開始するには

1. Cyber Protectコンソールで **[ソフトウェア管理]** > **[脆弱性]** に進みます。
2. リストで脆弱性を選択し、**[パッチをインストール]** をクリックします。脆弱性修復ウィザードが開きます。
3. 選択したマシンにインストールするパッチを選択して、**[次へ]** をクリックします。
4. パッチをインストールするマシンを選択します。
5. 再起動オプションを選択します。
   a. パッチのインストール後にマシンを再起動するかどうかを選択します。

オプション	説明
しない	パッチのインストール後、マシンは自動的に再起動されません。
必要な場合	パッチの適用に必要な場合のみ、マシンを再起動します。
はい。	パッチのインストール後、マシンは自動的に再起動されます。再起動の遅延時間を指定することもできます。

   b. （オプション） マシンのバックアップが進行している間、マシンの再起動を遅らせたい場合は、**[バックアップが完了するまで再起動しないでください]** を選択します。
6. **[パッチのインストール]** をクリックします。

選択したマシンに、選択したパッチがインストールされます。

パッチ管理

注意
この機能を利用できるかどうかは、現在のアカウントで有効になっているサービスクォータによって異なります。

Windows OSでサポートされる、サードパーティ製品の詳細については、「パッチ管理がサポートするサードパーティ製品のリスト（62853）」を参照してください。

パッチ管理機能を使用して、以下の操作を実行できます。

- OSレベルとアプリケーションレベルのアップデートをインストールする
- パッチを手動または自動で承認する
- オンデマンドモードまたはスケジュールモードでパッチをインストールする
- さまざまな基準（重大度、カテゴリ、承認ステータス）に基づいて、インストールするパッチを細かく定義する
- アップデートの失敗に備えてアップデート前のバックアップを実行する
- パッチのインストール後の再起動アクションを定義する

注意
パッチ管理機能をWindowsアップデートと連携させるには、ワークロード上でWindowsアップデートが有効になっている必要があります。

Cyber Protectionではピアツーピアテクノロジーが導入され、ネットワークの帯域幅のトラフィックが最小化されています。インターネットからアップデートをダウンロードしてネットワーク内の他のエージェントに分配するための専用エージェントを1つ以上選択することもできます。そうすれば、すべてのエージェントがピアツーピアエージェントとしてアップデートを共有することにもなります。

パッチ管理ワークフロー

パッチ管理ワークフローには、保護計画の構成と適用、脆弱性診断スキャンの実行、パッチ設定の構成、パッチの承認、そして承認されたパッチのインストールの各ステップが含まれます。ワークフローの具体的な手順は以下の通りです。

1. **脆弱性診断**および**パッチ管理**モジュールを有効にした保護計画を構成する。
2. 脆弱性診断の設定を構成する。これらの設定の詳細については、"脆弱性診断の設定"（927ページ）を参照してください。
3. パッチ管理設定を構成する。これらの設定の詳細については、"保護計画のパッチ管理設定"（933ページ）を参照してください。
4. 保護計画を1台または複数のマシンに適用する。
5. 脆弱性診断のスキャンが完了するまで待機する。スキャンは、保護計画で設定されたスケジュールに従って自動的に開始されます。または、保護計画の**脆弱性診断**モジュールで **[今すぐ実行]** アイコンをクリックして、必要に応じて手動でスキャンを開始することもできます。
6. パッチを承認する。テストマシンへのパッチの自動インストールを含む、自動パッチ承認の設定を定義できます。詳細については、"自動パッチ承認"（940ページ）を参照してください。また、承認ステータスを**承認済み**に設定して、パッチを手動で承認することもできます。詳細については、"パッチを手動で承認する"（945ページ）を参照してください。
7. パッチをインストールする。承認されたパッチは、保護計画で設定されたスケジュールに従って自動的にインストールされます。また、必要に応じて手動でパッチをインストールすることもできます。詳細については、"オンデマンドでのパッチのインストール"（945ページ）を参照してください。

[監視] > **[概要]** > **[パッチインストール履歴]** ウィジェットで、パッチインストールの結果を監視できます。

保護計画のパッチ管理設定

保護計画の**パッチ管理**モジュールでは、次のパッチ管理設定を構成できます。

- Windows OS向けのMicrosoft製品およびサードパーティ製品について、どのアップデートプログラムをインストールするか。
- 自動パッチインストールを実行するタイミング。
- アップデート前のバックアップを実行するかどうか。

保護計画の作成および**パッチ管理**モジュールの有効化の詳細については、"保護計画の作成"（209ページ）を参照してください。

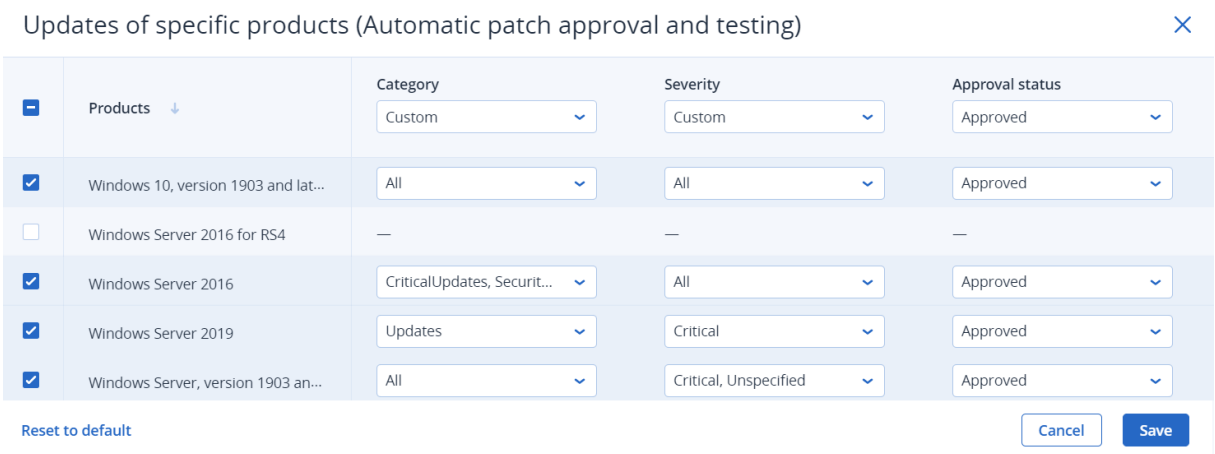
注意
この機能を利用できるかどうかは、現在のアカウントで有効になっているサービスクォータによって異なります。

Microsoft製品

選択したマシンにMicrosoftアップデートをインストールするには、**[Microsoft製品のアップデート]** オプションを有効にします。

インストールの種類を選択します。

オプション	説明
すべてのアップデート	承認済みのアップデートをすべてインストールする場合は、このオプションを使用します。
セキュリティアップデートと重要なアップデートのみ	承認済みのセキュリティアップデートおよび重要なアップデートをすべてインストールする場合は、このオプションを使用します。
特定製品のアップデート（自動パッチ承認およびテスト）	製品ごとにカスタム設定を定義する場合は、このオプションを使用します。 特定の製品をアップデートする場合は、カテゴリ、重大度、承認ステータスに基づいて、インストールするアップデートを製品ごとに定義できます。 パッチの自動テスト承認とテストを構成する場合は、このオプションを選択します。



Microsoft製品の場合、パッチ配信ではWindows APIサービスを使用します。パッチやアップデートプログラムが、内部または配信エージェント上にダウンロード/保存されることはありません。代わりに、Microsoft CDNからダウンロードされます。従って、アップデートロールが割り当てられていても、エージェントでパッチのダウンロードや配信が実行されることはありません。

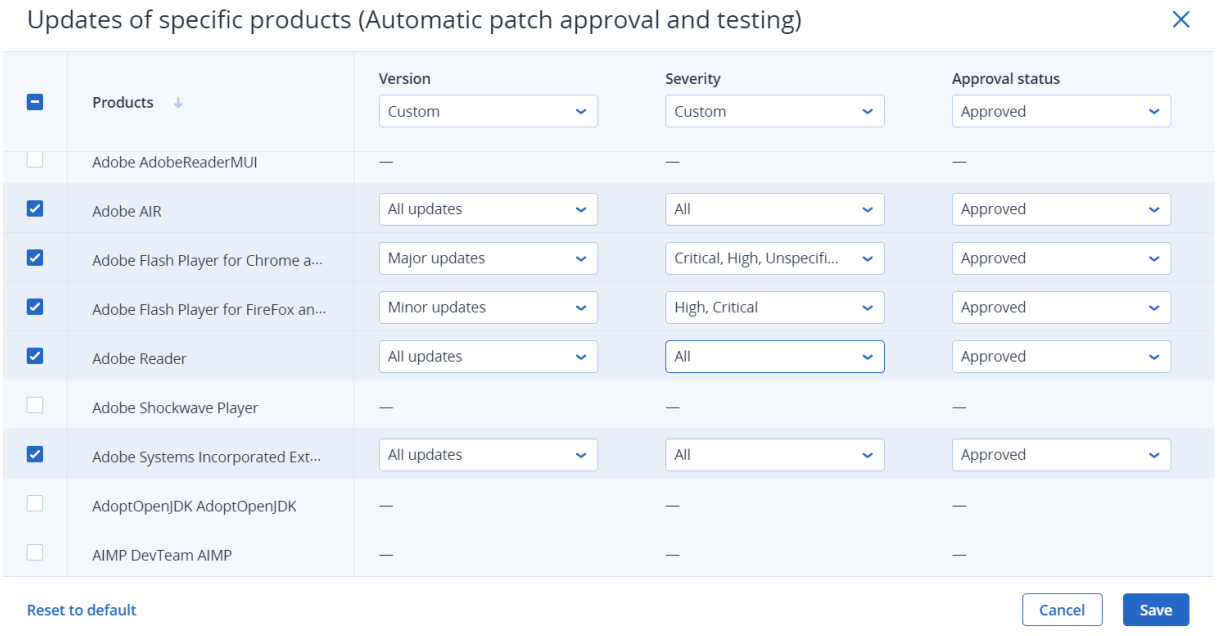
Windowsサードパーティ製品

選択したマシンにWindows OS向けサードパーティアップデートをインストールするには、[**Windows サードパーティ製品**] オプションを有効にします。

インストールオプションを選択します。

オプション	説明
すべてのアップデート	承認済みのアップデートをすべてインストールする場合は、このオプションを使用します。*
メジャーアップデートのみ	承認済みのメジャーアップデートをすべてインストールする場合は、このオプションを使用します。
マイナーアップデートのみ	承認済みのマイナーアップデートをインストールする場合は、このオプションを使用します。
特定製品のアップデート（自動パッチ承認およびテスト）	製品ごとにカスタム設定を定義する場合は、このオプションを使用します。 特定の製品をアップデートする場合は、カテゴリ、重大度、承認ステータスに基づいて、インストールするアップデートを製品ごとに定義できます。 パッチの自動テスト承認とテストを構成する場合は、このオプションを選択します。
脆弱性が検出されたアプリケーションにのみ、最新のバージョンをインストールする	脆弱性が検出されたアプリケーションに対してのみ最新のアップデートプログラムをインストールする場合は、このチェックボックスをオンにします。*

* このオプションでは、Cyber Protect エージェントバージョン23.11.36772以降が必要です。



Windowsのサードパーティ製品の場合、パッチは内部のAcronisデータベースから直接管理されているワークロードに配信されます。エージェントにアップデータロールが割り当てられている場合、そのエージェントはパッチをダウンロードおよび配信するために使用されます。

スケジュール

選択したマシンにアップデートをインストールするスケジュールおよび条件を定義します。

フィールド	説明
次のイベントを使ってタスクの実行スケジュールを設定します	この設定は、タスクがいつ実行されるかを定義します。 次の値を使用できます。 • **時刻でスケジュール** - これはデフォルト設定です。タスクは指定した時間に実行されます。 • **システムへのユーザーログイン時** - デフォルトでは、いずれかのユーザーがログインするとタスクが開始されます。特定のユーザーアカウントのみがタスクをトリガーできるように、この設定を変更できます。 • **システムへのユーザーログオフ時** - デフォルトでは、いずれかのユーザーがログオフするとタスクが開始されます。特定のユーザーアカウントのみがタスクをトリガーできるように、この設定を変更できます。 **注意** このタスクは、システムのシャットダウン時には実行されません。シャットダウンとログオフは、スケジューリング構成における別個のイベントです。 • **システムの起動時** - オペレーティングシステムが起動するときにタスクが実行されます。 • **システムのシャットダウン時** - オペレーティングシステムがシャットダウンするときにタスクが実行されます。
スケジュールの種類	このフィールドは、**[次のイベントを使ってタスクの実行スケジュールを設定]** で **[時刻でスケジュール]** を選択した場合に表示されます。 次の値を使用できます。 • **月単位** - タスクを実行する該当月と、その月内の週または日を選択します。 • **日単位** - これはデフォルト設定です。タスクを実行する週中の日を選択しします。 • **時間単位** - タスクを実行する週中の日、繰り返しの回数、時間間隔を選択しします。
開始時刻	このフィールドは、**[次のイベントを使ってタスクの実行スケジュールを設定]** で **[時刻でスケジュール]** を選択した場合に表示されます。 タスクを実行する正確な時間を選択します。

フィールド	説明
パッチのメンテナンス期間を構成する	このフィールドは、**[次のイベントを使ってタスクの実行スケジュールを設定]** で **[時刻でスケジュール]** を選択した場合に表示されます。 指定した時間間隔でのみパッチのインストールを実行したい場合は、この設定を選択します。パッチのメンテナンス期間で定義された終了時間までにパッチのインストールプロセスが完了しなかった場合、プロセスは自動的に停止します。
日付範囲内に実行	このフィールドは、**[次のイベントを使ってタスクの実行スケジュールを設定]** で **[時刻でスケジュール]** を選択した場合に表示されます。 設定したスケジュールが有効な日付範囲を指定します。
ユーザーアカウントを指定し、そのアカウントがオペレーティングシステムにログインしたときにタスクを開始	このフィールドは、**[次のイベントを使ってタスクの実行スケジュールを設定]** で **[システムへのユーザーログイン時]** を選択した場合に表示されます。 次の値を使用できます。 • **任意のユーザー** - いずれかのユーザーがログインしたときにタスクを開始させたい場合は、このオプションを使用します。 • **次のユーザー** - 指定したユーザーアカウントのログインでタスクを開始させたい場合は、このオプションを使用します。
ユーザーアカウントを指定し、そのアカウントがオペレーティングシステムからログアウトしたときにタスクを開始	このフィールドは、**[次のイベントを使ってタスクの実行スケジュールを設定]** で **[システムへのユーザーログオフ時]** を選択した場合に表示されます。 次の値を使用できます。 • **任意のユーザー** - いずれかのユーザーがログアウトしたときにタスクを開始させたい場合は、このオプションを使用します。 • **次のユーザー** - 指定したユーザーアカウントのログアウトでタスクを開始させたい場合は、このオプションを使用します。
開始条件	すべての条件を定義して、同時に満たされたときにタスクを実行する条件を指定します。 マルウェア対策スキャンの開始条件は、**バックアップモジュール**の開始条件に類似しています。「開始条件」を参照してください。 以下のような追加の開始条件を定義できます。 • **時間枠内でタスク開始時間を分散する** - このオプションを使用すると、タスクを実行する時間枠を設定して、ネットワークのボトルネックを回避できます。遅延時間を、時間または分単位で指定できます。たとえばデフォルトの開始時間が10:00 AMで、遅延を60分とした場合、タスクは10:00 AMから11:00 AMの間に開始されます。 • **マシンの電源が入っていないため実行されなかったタスクを起動時に実行する** • **タスク実行中はスリープモードや休止モードに入らない** - このオプ

フィールド	説明
	ションは、Windowsを実行しているマシンに対してのみ有効です。 • **開始条件を満たさない場合でも、次の時間の経過後にタスクを実行** - 他の開始条件にかかわらずタスクが実行されるまでの時間を指定します。 **注意** 開始条件は、Linuxではサポートされていません。
アップデート後に再起動	アップデートのインストール完了後にマシンを自動的に再起動するかどうかを定義します。 次の値を使用できます。 • **いいえ** - アップデートのインストール後に再起動を開始しません。 • **必要な場合** - アップデートを適用するために必要な場合に限って再起動を開始します。 • **常に開始** - アップデート後に常に再起動を開始します。再起動の遅延時間を指定できます。
バックアップが終了するまで再起動しない	このオプションを選択すると、バックアッププロセスが実行中の場合、バックアップが完了するまでマシンの再起動が延期されます。

アップデート前のバックアップ

[ソフトウェアアップデートのインストール前にバックアップを実行] - アップデートのインストール前にマシンの増分バックアップを作成します。前にバックアップを作成していない場合は、マシンの完全バックアップが作成されます。そうすれば、アップデートのインストールが失敗しても、直前の状態に復帰できます。**[アップデート前のバックアップ]** オプションを使用するには、対応するマシンの保護計画でパッチ管理とバックアップの両方のモジュールが有効になっている必要があります。また、バックアップする項目（マシン全体またはブートボリュームとシステムボリューム）を選択してください。選択したバックアップ対象が正しくない場合、**[アップデート前のバックアップ]** オプションを有効にできません。

利用可能なパッチのリストを表示する

脆弱性診断スキャンが完了すると、**[ソフトウェア管理]** > **[パッチ]** で利用可能なパッチに関する情報を表示できます。

特定のパッチの詳細を表示するには、パッチのリストで対応するパッチをクリックします。

次の表に、この画面で表示できるパッチの情報を示します。

フィールド	説明
承認ステータス	承認ステータスが必要になるのは主に自動承認の場合です。 パッチのステータスとして以下のいずれかを定義できます。

	• **承認済み** - 少なくとも1台のマシンにパッチがインストールされていて、問題のないことが確認されています • **拒否済み** - このパッチは安全ではなく、マシンシステムが破損する危険があります • **承認待ち** - パッチのステータスが不明なので、検証が必要です
ライセンス契約	• 同意済み • 同意しない。ライセンス契約に同意しない場合は、パッチのステータスが **[拒否済み]** になり、そのパッチはインストールされません
重大度	パッチの重大度: • **重大** • **高** • **中** • **低** • **なし**
ベンダー	パッチのベンダー
影響を受ける製品	パッチを適用する製品
インストール済みバージョン	既にインストールされている製品バージョン
バージョン	パッチのバージョン
カテゴリ	パッチのカテゴリ: • **重要なアップデート** - 特定の問題について広くリリースされているフィックス。重要なバグやセキュリティ関連以外のバグに対応しています。 • **セキュリティアップデート** - 特定の製品について広くリリースされているフィックス。セキュリティの問題に対応しています。 • **定義アップデート** - ウイルスなどの定義ファイルのアップデート。 • **アップデートロールアップ** - Hotfix、セキュリティアップデート、重要なアップデートの累積セット。各種のアップデートをパッケージ化して配置しやすくしたものです。ロールアップは通常、セキュリティなどの特定の分野やInternet Information Services（IIS）などの特定のコンポーネントをターゲットにしています。 • **サービスパック** - 製品のリリース以降に作成されたすべてのHotfix、セキュリティアップデート、重要なアップデートの累積セット。サービスパックには、カスタマーからのリクエストがあった設計変更や機能が限定的に盛り込まれている場合もあります。 • **ツール** - タスクの実行に役立つユーティリティや機能。 • **機能パック** - 新機能のリリース。通常は、次回のリリース時に製品に組み込まれます。 • **アップデート** - 特定の問題について広くリリースされているフィックス。重要でないバグやセキュリティ関連以外のバグに対応しています。 • **アプリケーション** – アプリケーションのパッチ。
リリース日	パッチがリリースされた日付

前回レポート済み	パッチが最後に報告された日付
最初にインストール済み	マシンにパッチが初めてインストールされた日付
Microsoft KB	Microsoft製品のパッチの場合は、フィールドにKBの記事のIDが表示されます
マシン	影響を受けたマシンの数
脆弱性	脆弱性の数。クリックすると、脆弱性のリストにリダイレクトされます。
サイズ	パッチの平均サイズ
言語	パッチでサポートされている言語
ベンダーサイト	ベンダーの公式サイト

リスト内のパッチのライフタイムを構成する

[パッチ] 画面のリストでパッチのライフタイムを設定することで、パッチのリストを最新の状態に保つことができます。この設定では、検出された有効なパッチをパッチリスト表示する期間を定義します。パッチは、（パッチが見つからない）すべてのマシンに正常にインストールされるか、リストの有効期間が過ぎると、リストから削除されます。

リスト内のパッチのライフタイムを構成するには

1. Cyber Protectコンソールで **[ソフトウェア管理]** > **[パッチ]** に進みます。
2. **[設定]** をクリックします。
3. **リスト内のライフタイム**で、適切なオプションを選択します。

オプション	説明
無期限	パッチは常にリストに表示されます。
7日間	パッチは最初のインストールから7日後にリストから削除されます。 例えば、パッチをインストールしなければならないマシンが2台あるとします。1台はオンライン、もう1台はオフラインです。パッチを最初のマシンにインストールします。7日が経過した時点で、そのパッチは2番目のマシンにインストールされていなくても、パッチリストから削除されます。2番目のマシンはオフラインだからです。
30日	パッチは最初のインストールから30日後にリストから削除されます。

自動パッチ承認

自動パッチ承認を利用すると、マシンにアップデートをインストールするプロセスを簡略化できます。自動パッチ承認では、手動パッチ承認プロセスによってパッチのインストールが遅延することはありま

せん。重要なアップデートや修正プログラムがより迅速にインストールされるため、システムの信頼性が向上します。

自動パッチ承認は、パッチの自動インストールのテストシナリオで使用できます。テストマシンにパッチが正常にインストールされると、本番マシンにもパッチが自動的にインストールされます。このシナリオの詳細については、"自動パッチ承認とテストのユースケース"（941ページ）を参照してください。

また、テストフェーズを省略して、本番環境にパッチを自動的にインストールするシナリオで自動パッチ承認を使用することもできます。このシナリオの詳細については、"テストを実行しない自動パッチ承認のユースケース"（944ページ）を参照してください。

自動パッチ承認の設定

自動パッチ承認を構成して、手動パッチ承認プロセスによってパッチのインストールが遅延しないようにすることができます。

自動パッチ承認を設定する手順

1. Cyber Protectコンソールで **[ソフトウェア管理]** > **[パッチ]** に進みます。
2. **[設定]** をクリックします。
3. **[自動パッチ承認]** を有効化します。
4. 自動パッチ承認の設定を構成します。
   a. 自動パッチ承認オプションを選択します。

オプション	説明
パッチの自動承認とテスト	パッチが正常にインストールされてから指定した日数が経過すると、パッチの承認ステータスが**承認済み**に変更されます。本番環境にパッチをインストールする場合は、まずテストマシンにパッチをインストールしてテストし、すべてが予想通りに動作することを確認してから、この設定を使用することをお勧めします。
自動パッチ承認（テストなし）	パッチが見つかってから指定した日数が経過すると、パッチの承認ステータスが**承認済み**に変更されます。

   b. 自動パッチ承認オプションの条件を満たしてから、経過する必要のある日数を選択します。この日数が経過すると、パッチの承認ステータスは自動的に**承認待ち**から**承認済み**に変更されます。
5. **[ライセンス契約の自動承認]** を選択します。
6. **[適用]** をクリックします。

自動パッチ承認とテストのユースケース

新しいパッチを本番マシンにインストールする前にテストマシンでテストしたい場合、テスト目的のパッチのインストール計画と、本番マシンへのテスト済みパッチのインストール計画の2つの保護計画を

設定できます。このようにして、本番環境にインストールするパッチが安全で、パッチインストール後に本番マシンが正しく動作することを確認します。。

ユースケースは、以下のステージで構成されます:

1. 自動パッチ承認の設定を構成する。**[パッチの自動承認とテスト]** オプションを選択する。詳細については、"自動パッチ承認の設定"（941ページ）を参照してください。
2. 有効化された**パッチ管理**モジュールでテスト目的の保護計画（例えば「テストパッチ」）を構成し、テスト環境のマシンに適用する。パッチの承認ステータスが **[承認待ち]** でなければならないというパッチインストール条件を指定します。このステップは、パッチを確認してパッチインストール後のマシンの状態を確かめるために必要です。詳細については、"テストパッチの保護計画を構成する"（942ページ）を参照してください。
3. **パッチ管理**のモジュールを有効にした本番環境の保護計画を構成し（「本番パッチ」など）、本番環境のマシンに適用します。パッチのステータスが **[承認済み]** でなければならないというパッチインストール条件を指定します。詳細については、"本番環境のパッチ保護計画を構成する"（943ページ）を参照してください。
4. テストパッチの計画を実行して、結果を確認します。問題のないマシンの承認ステータスは**承認待ち**のままにしておき、正しく動作していないマシンの承認ステータスを**拒否**に変更することができます。**パッチの自動承認**設定で設定した日数に応じて、パッチのステータスが自動的に**承認待ち**から**承認済み**に変わります。本番環境のパッチ計画を実行すると、**承認済み**のパッチのみが本番マシンにインストールされます。詳細については、"テストパッチ保護計画の実行と安全でないパッチの拒否"（944ページ）を参照してください。
5. 本番環境のパッチ計画を実行します。

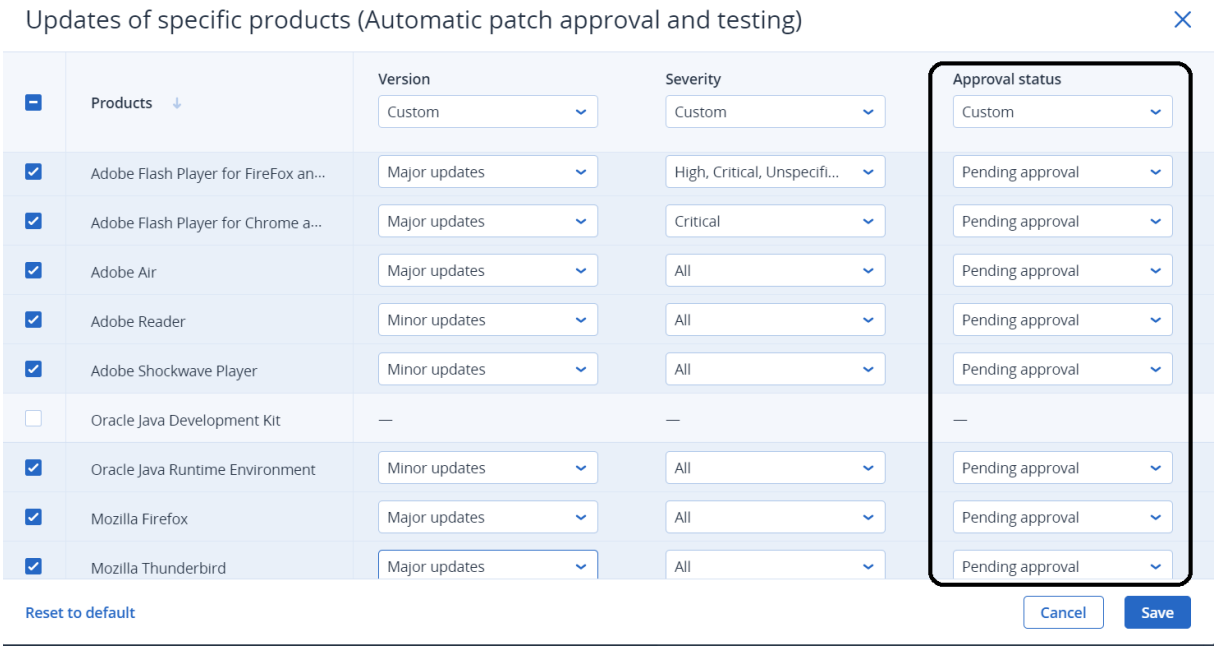
テストパッチの保護計画を構成する

テスト環境のマシンに対して、パッチインストール設定を含む保護計画を構成できます。

テストパッチ保護計画を構成するには

1. Cyber Protectコンソールで、**[管理]** > **[保護計画]** に移動します。
2. **[計画の作成]** をクリックします。
3. **[パッチ管理]** モジュールを有効にします。
4. インストールするMicrosoftおよびサードパーティ製品のアップデート、スケジュール、およびアップデート前のバックアップを定義します。これらの設定の詳細については、"保護計画のパッチ管理設定"（933ページ）を参照してください。

重要
アップデートするすべての製品について、承認ステータスを**承認待ち**にします。従って、エージェントでは、**承認待ち**のパッチのみがテスト環境で選択したマシンにインストールされます。



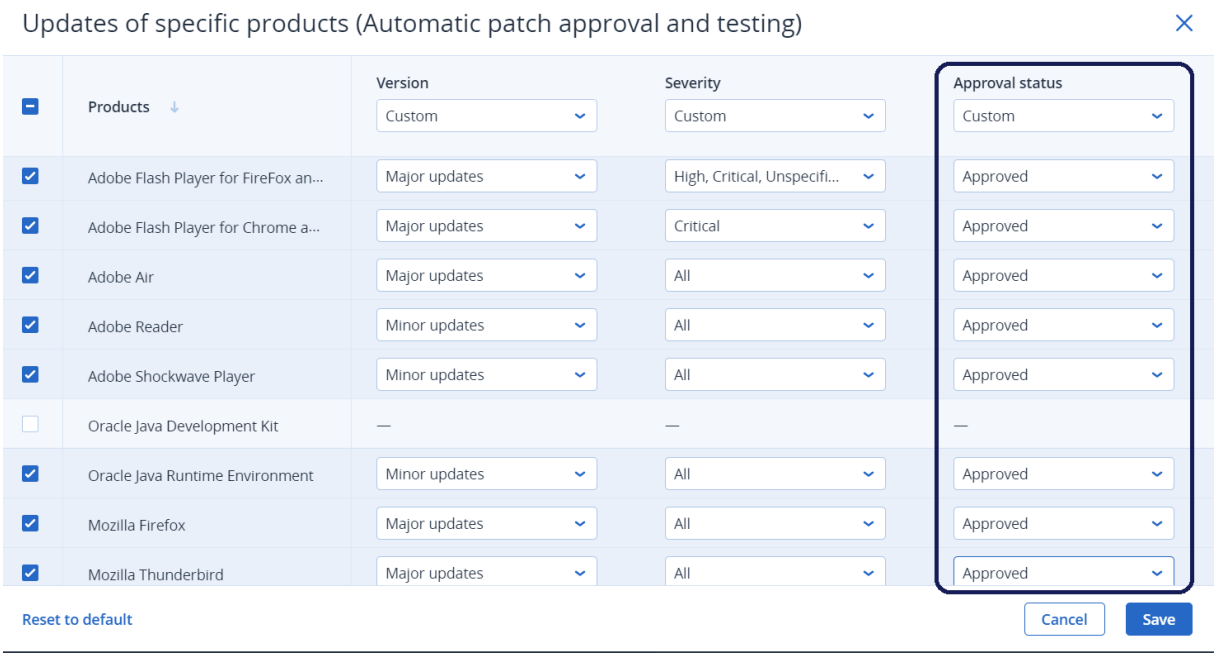
本番環境のパッチ保護計画を構成する

本番環境のマシンに対して、パッチインストール設定を含む保護計画を構成できます。

本番環境のパッチ保護計画を構成するには

1. Cyber Protectコンソールで、**[管理]** > **[保護計画]** に移動します。
2. **[計画の作成]** をクリックします。
3. **[パッチ管理]** モジュールを有効にします。
4. インストールするMicrosoftおよびサードパーティ製品のアップデート、スケジュール、およびアップデート前のバックアップを定義します。これらの設定の詳細については、"保護計画のパッチ管理設定"（933ページ）を参照してください。

重要
アップデートするすべての製品について、**承認ステータス**を**承認済み**に設定します。エージェントにより、本番環境で選択したマシンに**承認済み**のパッチだけがインストールされます。



テストパッチ保護計画の実行と安全でないパッチの拒否

テスト環境のマシンにパッチがインストールされてから、すべてが想定通りに動作しているかどうかを確認できます。問題のないマシンの承認ステータスは**承認待ち**のままにしておき、正しく動作していないマシンの承認ステータスを**拒否済み**に変更できます。

パッチ保護計画のテストを実行し、安全でないパッチを拒否するには

1. パッチ保護計画のテストを（スケジュールまたは手動で）実行します。
2. その結果に応じて、インストールされている各パッチの安全性を確認します。
3. **[ソフトウェア管理]** > **[パッチ]** に進み、安全でないパッチの **[承認ステータス]** を **[拒否済み]** に設定します。

テストを実行しない自動パッチ承認のユースケース

新しいパッチを最初にテストマシンにインストールせずに、できるだけ早く本番環境のマシンに自動インストールしたい場合は、単一の保護計画のみを構成します。

ユースケースは、以下のステージで構成されます:

1. 自動パッチ承認の設定を構成する。**[自動パッチ承認（テストなし）]** オプションを選択する詳細については、"自動パッチ承認の設定"（941ページ）を参照してください。
2. **パッチ管理**のモジュールを有効にした本番環境の保護計画を構成し（「本番パッチ」など）、本番環境のマシンに適用します。パッチのステータスが **[承認済み]** でなければならないというパッチインストール条件を指定します。詳細については、"本番環境のパッチ保護計画を構成する"（943ページ）を参照してください。
3. 本番環境のパッチ計画を実行します。

パッチを手動で承認する

パッチを手動で承認し、テストフェーズをスキップしてインストールを高速化できます。

前提条件

- **パッチ管理**モジュールを有効にした保護計画が、少なくとも1台のWindowsマシンに適用されている。
- 保護計画が適用されているマシン（単体または複数）、まだインストールされていないパッチがある。

手動でパッチを承認するには

1. Cyber Protectコンソールで [**ソフトウェア管理**] > [**パッチ**] に進みます。
2. インストールするパッチを選択し、ライセンス契約に同意します。
3. パッチの**承認ステータス**を**承認済み**に設定します。
   パッチの承認ステータスが**承認済み**に設定されます。パッチは、保護計画で定義されたスケジュールに基づいてマシンに自動的にインストールされます。パッチをすぐにインストールしたい場合は、"オンデマンドでのパッチのインストール"（945ページ）記載されている手順に従ってください。

オンデマンドでのパッチのインストール

スケジュールされたインストール時間まで待機できない場合は、オンデマンドでパッチの手動インストールを実行できます。

手動によるパッチのインストールは、次の3つの画面から開始できます:**パッチ**、**脆弱性**、**すべてのデバイス**です。

パッチを手動でインストールするには

パッチから

1. Cyber Protectコンソールで [**ソフトウェア管理**] > [**パッチ**] に進みます。
2. インストールするパッチのライセンス契約に同意します。
3. **パッチのインストール**ウィザードで、インストールするパッチを選択して、[**インストール**] をクリックします。
4. パッチをインストールするマシンを選択します。
5. 再起動オプションを選択します。

a. パッチのインストール後にマシンを再起動するかどうかを選択します。

オプション	説明
しない	パッチのインストール後、マシンは自動的に再起動されません。
必要な場合	パッチの適用に必要な場合のみ、マシンを再起動します。
はい。	パッチのインストール後、マシンは自動的に再起動されます。再起動の遅延時間を指定することもできます。

b. （オプション） マシンのバックアップが進行している間、マシンの再起動を遅らせたい場合は、[**バックアップが完了するまで再起動しないでください**] を選択します。

6. [**パッチのインストール**] をクリックします。

脆弱性から

1. Cyber Protectコンソールで [**ソフトウェア管理**] > [**脆弱性**] に進みます。
2. 修復プロセスを実行します（"検出された脆弱性の管理"（931ページ）を参照）。

すべてのデバイスから

1. Cyber Protectコンソールで [**デバイス**] > [**すべてのデバイス**] に進みます。
2. パッチをインストールするマシンを選択します。
3. [**パッチ**] をクリックします。
4. インストールするパッチを選択し、[**次へ**] をクリックします。
5. 再起動オプションを選択します。
   a. パッチのインストール後にマシンを再起動するかどうかを選択します。

オプション	説明
しない	パッチのインストール後、マシンは自動的に再起動されません。
必要な場合	パッチの適用に必要な場合のみ、マシンを再起動します。
はい。	パッチのインストール後、マシンは自動的に再起動されます。再起動の遅延時間を指定することもできます。

   b. （オプション） マシンのバックアップが進行している間、マシンの再起動を遅らせたい場合は、[**バックアップが完了するまで再起動しないでください**] を選択します。

6. [**パッチのインストール**] をクリックします。

ソフトウェアとハードウェアのインベントリを管理する

ソフトウェアインベントリ

ソフトウェアインベントリ機能は、アドバンスドパックが有効なデバイス、または（以前の）Cyber Protectライセンスが付与されているデバイスで利用可能です。ソフトウェアインベントリ機能を使用すると、すべてのWindowsおよびmacOSデバイスにインストールされている、すべてのソフトウェアアプリケーションを表示できます。

ソフトウェアインベントリデータを取得するには、デバイスで自動スキャンまたは手動スキャンを実行します。

ソフトウェアインベントリデータを使用して、次のことができます。

- 社内のデバイスにインストールされているすべてのアプリケーションに関する情報を参照して比較する
- アプリケーションをアップデートする必要があるかどうかを判断する
- 未使用のアプリケーションを削除する必要があるかどうかを判断する
- 複数の社内デバイスのソフトウェアバージョンが同一であることを確認する
- スキャンとスキャンの間のソフトウェアステータスの変化を監視する。

ソフトウェアインベントリスキャンを有効化

デバイスで、ソフトウェアインベントリスキャンが有効になっている場合、システムは12時間ごとに自動的にソフトウェアデータを収集します。

ソフトウェアインベントリスキャン機能は、必要なライセンスを有するすべてのデバイスに対してデフォルトで有効になっていますが、必要に応じて設定を変更できます。

注意
カスタマーのテナントで、ソフトウェアインベントリスキャンを有効化または無効化できます。ユニットテナントでは、ソフトウェアインベントリスキャンの設定を表示することのみ可能です。設定を変更することはできません。

ソフトウェアインベントリスキャンを有効化するには

1. Cyber Protectコンソールで **[設定]** に進みます。
2. **[保護]** をクリックします。
3. **[インベントリのスキャン]** をクリックします。
4. モジュール名の横にあるスイッチをクリックして、**ソフトウェアインベントリスキャン**モジュールを有効にします。

ソフトウェアインベントリスキャンを無効化するには

1. Cyber Protectコンソールで **[設定]** に進みます。
2. **[保護]** をクリックします。
3. **[インベントリのスキャン]** をクリックします。
4. モジュール名の横にあるスイッチをクリックして、**ソフトウェアインベントリスキャン**モジュールを無効にします。

ソフトウェアインベントリスキャンを手動で実行する

[ソフトウェアインベントリ] 画面、または **[インベントリ]** 画面の ［**ソフトウェア**］ タブから、ソフトウェアインベントリスキャンを手動で実行できます。

前提条件

- デバイスはWindowsまたはmacOSオペレーティングシステムを使用します。
- デバイスに必要な（以前の）Cyber Protectライセンスが存在するか、Advanced Managementパックが有効になっています。

[ソフトウェアインベントリ] 画面からソフトウェアインベントリスキャンを実行するには

1. Cyber Protectコンソールで **[ソフトウェア管理]** に進みます。
2. **[ソフトウェアインベントリ]** をクリックします。
3. **[グループ別:]** ドロップダウンフィールドで、**[デバイス]** を選択します。
4. スキャンするデバイスを見つけ、**[今すぐスキャン]** をクリックします。

[インベントリ] 画面の [ソフトウェア] タブからソフトウェアインベントリスキャンを実行するには

1. Cyber Protectコンソールで **[デバイス]** に進みます。
2. スキャンするデバイスをクリックし、**[インベントリ]** をクリックします。
3. **[ソフトウェア]** タブで **[今すぐスキャン]** をクリックします。

ソフトウェアインベントリを参照

社内のすべてのデバイスで使用可能な、すべてのソフトウェアアプリケーションのデータを表示および参照できます。

前提条件

- デバイスはWindowsまたはmacOSオペレーティングシステムを使用します。
- デバイスに必要な（以前の）Cyber Protectライセンスが存在するか、Advanced Managementパックが有効になっています。
- デバイスでのソフトウェアインベントリスキャンが正常に終了しました。

WindowsおよびmacOSで稼働するすべての社内デバイスで利用可能な、すべてのソフトウェアアプリケーションを表示する方法

1. Cyber Protectコンソールで **[ソフトウェア管理]** に進みます。
2. **[ソフトウェアインベントリ]** をクリックします。

デフォルトでは、データはデバイスごとにグループ化されています。次の表は、[**ソフトウェアインベントリ**] 画面に表示されるデータについて説明しています。

項目	説明
名前	アプリケーションの名前。
バージョン	アプリケーションのバージョン。
ステータス	アプリケーションのステータス。 • **新規**。 • **アップデート済み**。 • **削除済み**。 • **変更なし**。
ベンダー	アプリケーションのベンダー。
インストールされた日付	アプリケーションがインストールされた日時。
前回の実行	macOSデバイスの場合のみ。アプリケーションが最後にアクティブになった日時。
ロケーション	アプリケーションがインストールされているディレクトリ。
ユーザー	アプリケーションをインストールしたユーザー。
システムのタイプ	Windowsデバイスの場合のみ。アプリケーションのビットタイプ。 • **X86**: 32-bitアプリケーション。 • **X64**: 64-bitアプリケーション。

3. アプリケーション別にデータをグループ化するには、[**グループ別:**] ドロップダウンフィールドで、[**アプリケーション**] をクリックします。
4. 画面に表示される情報を絞り込むには、1つまたは組み合わせた複数のフィルターを使用します。
   a. [**フィルター**] をクリックします。
   b. 1つまたは組み合わせた複数のフィルターを選択します。
   次の表は、[**ソフトウェアインベントリ**] 画面のフィルターについて説明しています。

フィルタ	説明
デバイス名	デバイス名。複数選択が可能です。特定のデバイス上のソフトウェアを比較する場合は、このフィルターを使用します。
アプリケーション	アプリケーションの名前。複数選択が可能です。特定のデバイスまたはすべてのデバイス上で、特定のアプリケーションデータを比較する場合は、このフィルターを使用します。
ベンダー	アプリケーションのベンダー。複数選択が可能です。特定

フィルタ	説明
	のデバイスまたはすべてのデバイス上で、特定ベンダーのすべてのアプリケーションを表示する場合は、このフィルターを使用します。
ステータス	アプリケーションのステータス。複数選択が可能です。特定のデバイスまたはすべてのデバイス上で、選択したステータスのすべてのアプリケーションを表示する場合は、このフィルターを使用します。
インストールされた日付	アプリケーションがインストールされた日付。特定のデバイスまたはすべてのデバイス上で、特定の日付にインストールされたすべてのアプリケーションを表示する場合は、このフィルターを使用します。
スキャン日	ソフトウェアインベントリスキャンの日付。該当の日付にスキャンされた特定のデバイス、またはすべてのデバイスのソフトウェアに関する情報を表示する場合は、このフィルターを使用します。

c. **[適用]** をクリックします。

5. ソフトウェアインベントリリスト全体を参照するには、画面の左下部分にあるページ番号を使用します。

- 開きたいページの番号をクリックします。
- ドロップダウンフィールドで、開きたいページのページ番号を選択します。

単一デバイスのソフトウェアインベントリの表示

単一のデバイスにインストールされているすべてのソフトウェアアプリケーションのリストと、ステータス、バージョン、ベンダー、インストール日、最終実行、ロケーションなどのアプリケーションに関する詳細情報を表示できます。

前提条件

- デバイスはWindowsまたはmacOSオペレーティングシステムを使用します。
- デバイスに必要な（以前の）Cyber Protectライセンスが存在するか、Advanced Managementパックが有効になっています。
- デバイスでのソフトウェアインベントリスキャンが正常に終了しました。

[ソフトウェアインベントリ] 画面から単一デバイスのソフトウェアインベントリを表示するには

1. Cyber Protectコンソールで **[ソフトウェア管理]** に進みます。
2. **[ソフトウェアインベントリ]** をクリックします。
3. **[グループ別:]** ドロップダウンフィールドで、**[デバイス]** を選択します。
4. 以下のオプションのいずれかを使用して、検査するデバイスを見つけます。

- **[フィルター]** を使用してデバイスを見つけます:
  a. **[フィルター]** をクリックします。
  b. **[デバイス名]** フィールドで、表示するデバイスの名前を選択します。
  c. **[適用]** をクリックします。
- ダイナミック**検索**を使用してデバイスを見つけます:
  a. **[検索]** をクリックします。
  b. 完全なデバイス名またはデバイス名の一部を入力します。

[デバイス] 画面から単一デバイスのソフトウェアインベントリを表示するには

1. Cyber Protectコンソールで **[デバイス]** に進みます。
2. 表示するデバイスをクリックし、**[インベントリ]** をクリックします。
3. **[ソフトウェア]** タブをクリックします。

ハードウェアインベントリ

ハードウェアインベントリ機能を使用すると、次のデバイス上で利用可能なすべてのハードウェアコンポーネントを表示できます。

- ハードウェアインベントリ機能をサポートするライセンスが付帯する物理的なWindowsおよびmacOSデバイス。
- 次の仮想環境プラットフォームで実行されている仮想WindowsおよびmacOSマシン: VMware、Hyper-V、Citrix、Parallels、Oracle、Nutanix、Virtuozzo、Virtuozzo Hybrid Infrastructure。 サポート対象の仮想環境プラットフォームの詳細については、「"サポートされる仮想環境プラットフォーム"（31ページ）」を参照してください。

注意
仮想マシンのハードウェアインベントリ機能は、Cyber Protectの以前のエディションではサポートされていません。

ハードウェアインベントリ機能は、プロテクション エージェントがインストールされているデバイスでのみサポートされます。

ハードウェアインベントリデータを取得するには、デバイスで自動スキャンまたは手動スキャンを実行します。

ハードウェアインベントリデータを使用して、次のことができます。

- 組織のすべてのハードウェア資産を発見する
- 組織内に存在するすべてのデバイスのハードウェアインベントリを参照する
- 複数の企業に存在するデバイスのハードウェアコンポーネントを比較する
- ハードウェアコンポーネントに関する詳細情報を表示する。

ハードウェアインベントリスキャンを有効化

物理デバイスと仮想マシンでハードウェアインベントリスキャンが有効になっている場合、システムは12時間ごとに自動的にハードウェアデータを収集します。

ハードウェアインベントリスキャン機能はデフォルトで有効になっていますが、必要に応じて設定を変更できます。

注意
カスタマーのテナントで、ハードウェアインベントリスキャンを有効化または無効化できます。ユニットテナントでは、ハードウェアインベントリスキャンの設定を表示することのみ可能です。設定を変更することはできません。

ハードウェアインベントリスキャンを有効化するには

1. Cyber Protectコンソールで **[設定]** に進みます。
2. **[保護]** をクリックします。
3. **[インベントリのスキャン]** をクリックします。
4. モジュール名の横にあるスイッチをクリックして、**ハードウェアインベントリスキャン**モジュールを有効にします。

ハードウェアインベントリスキャンを無効化するには

1. Cyber Protectコンソールで **[設定]** に進みます。
2. **[保護]** をクリックします。
3. **[インベントリのスキャン]** をクリックします。
4. モジュール名の横にあるスイッチをクリックして、**ハードウェアインベントリスキャン**モジュールを無効にします。

ハードウェアインベントリスキャンを手動で実行する

単一のデバイスのハードウェアインベントリスキャンを手動で実行し、デバイスのハードウェアコンポーネントに関する現在のデータを表示できます。

注意
仮想マシンのハードウェアインベントリスキャンは、仮想マシンの現在の日付と時刻がUTCの現在の日付と時刻に対応している場合にのみサポートされます。仮想マシンで正しい時間設定が使用されるようにするには、仮想マシンで、**[時間同期]** オプションを無効にして、現在の日付、時刻、タイムゾーンを設定してから、**Acronis Agent Core Service**と**AcronisManaged Machine Service**を再起動します。

前提条件

- （すべてのデバイス向け）デバイスはWindowsまたはmacOSオペレーティングシステムを使用します。
- （すべてのデバイス向け）デバイスには、ハードウェアインベントリ機能をサポートするライセンスが付帯しています。仮想マシンのハードウェアインベントリ機能は、（以前の）Cyber Protectエディ

ションではサポートされていないことにご注意ください。
- （すべてのデバイス向け）プロテクションエージェントがデバイスにインストールされています。
- （仮想マシンの場合）マシンは、サポートされている仮想環境プラットフォームのいずれかで実行されます。詳細については、"ハードウェアインベントリ"（951ページ）を参照してください。

単一のデバイスでハードウェアインベントリスキャンを実行するには

1. Cyber Protectコンソールで **[デバイス]** に進みます。
2. スキャンするデバイスをクリックし、**[インベントリ]** をクリックします。
3. **[ハードウェア]** タブで **[今すぐスキャン]** をクリックします。

ハードウェアインベントリの参照

社内のすべてのデバイスで使用可能な、すべてのハードウェアコンポーネントのデータを表示および参照できます。

前提条件

- （すべてのデバイス向け）デバイスはWindowsまたはmacOSオペレーティングシステムを使用します。
- （すべてのデバイス向け）デバイスには、ハードウェアインベントリ機能をサポートするライセンスが付帯しています。仮想マシンのハードウェアインベントリ機能は、Cyber Protectの以前のエディションではサポートされていないことにご注意ください。
- （すべてのデバイス向け）プロテクションエージェントがデバイスにインストールされています。
- （すべてのデバイス向け）デバイスのハードウェアインベントリスキャンが正常に終了しました。
- （仮想マシンの場合）マシンは、サポートされている仮想環境プラットフォームのいずれかで実行されます。詳細については、"ハードウェアインベントリ"（951ページ）を参照してください。

WindowsおよびmacOSで稼働する社内のデバイスで、利用可能なすべてのハードウェアコンポーネントを表示する方法

1. Cyber Protectコンソールで **[デバイス]** に進みます。
2. **[ビュー:]** ドロップダウンフィールドで、**[ハードウェア]** を選択します。

注意
ビューとは、画面に表示されるデータを決定する列のセットです。事前定義されているビューとして、**[標準]** および **[ハードウェア]** があります。さまざまな列のセットを含むカスタムビューを作成して保存できるので、ニーズに応じて柔軟に利用できます。

次の表は、**[ハードウェア]** ビューに表示されるデータについて説明しています。

項目	説明
名前	デバイス名。
ハードウェアスキャンのステータス	ハードウェアスキャンのステータスです。 • **完了**。

項目	説明
	• **開始されていません**。 • **サポートされていません**。ハードウェアインベントリ機能がサポートされていないワークロード（仮想マシン、モバイルデバイス、Linuxデバイスなど）のステータスが表示されます。 • **エージェントをアップデート**。古いバージョンのエージェントがデバイスにインストールされている場合に表示されます。この操作をクリックすると、[設定] > [エージェント] ページにリダイレクトされ、管理者はエージェントのアップデートを実行できます。 • **クォータをアップグレード**。これをクリックすると、管理者が現在のライセンスをテナントライセンスで利用可能な他のライセンスのいずれかに切り替えるためのダイアログが開きます
プロセッサー	デバイスのすべてのプロセッサーモデル。
プロセッサーのコア	デバイスのすべてのプロセッサーコア数。
ディスクストレージ	使用済みストレージ、およびデバイスのすべてのディスク合計ストレージ。
RAM	デバイスの合計RAM容量。
スキャン日	最後にハードウェアインベントリスキャンが実行された日時。
マザーボード	デバイスのマザーボード。
マザーボードのシリアルナンバー	マザーボードのシリアルナンバー
BIOSのバージョン	システムのBIOSバージョン。
組織	デバイスが属している組織。
所有者	デバイスの所有者。
ドメイン	デバイスのドメイン。
オペレーティングシステム	デバイスのオペレーティングシステム。
オペレーティングシステムのビルド	デバイスのオペレーティングシステムのビルド。

3. テーブルに列を追加するには、列オプションアイコンをクリックして、テーブルに表示する列を選択します。
4. 画面に表示される情報を絞り込むには、1つまたは複数のフィルターを使用します。
   a. **[検索]** をクリックします。
   b. 矢印をクリックして、**[ハードウェア]** をクリックします。

c. 1つまたは組み合わせた複数のフィルターを選択します。

次の表は、**[ハードウェア]** フィルターについて説明しています。

フィルタ	説明
プロセッサーのモデル	複数選択が可能です。指定されたモデルのプロセッサーを搭載するデバイスのハードウェアデータを表示するには、このフィルターを使用します。
プロセッサーのコア	指定されたプロセッサーのコア数を備えるデバイスのハードウェアデータを表示するには、このフィルターを使用します。
ディスクの合計サイズ	指定された合計ストレージサイズを備えるデバイスのハードウェアデータを表示するには、このフィルターを使用します。
メモリ容量	指定されたRAM容量を備えるデバイスのハードウェアデータを表示するには、このフィルターを使用します。

d. **[適用]** をクリックします。

5. データを昇順で並べ替えるには、列名をクリックします。

単一デバイスのハードウェアを表示する

特定のデバイスのマザーボード、プロセッサー、メモリ、グラフィック、ストレージドライブ、ネットワーク、およびシステムに関する詳細情報を表示できます。

前提条件

- （すべてのデバイス向け）デバイスはWindowsまたはmacOSオペレーティングシステムを使用します。
- （すべてのデバイス向け）デバイスには、ハードウェアインベントリ機能をサポートするライセンスが付帯しています。仮想マシンのハードウェアインベントリ機能は、Cyber Protectの以前のエディションではサポートされていないことにご注意ください。
- （すべてのデバイス向け）プロテクションエージェントがデバイスにインストールされています。
- （すべてのデバイス向け）デバイスのハードウェアインベントリスキャンが正常に終了しました。
- （仮想マシンの場合）マシンは、サポートされている仮想環境プラットフォームのいずれかで実行されます。詳細については、"ハードウェアインベントリ"（951ページ）を参照してください。

特定のデバイスのハードウェアに関する詳細情報を表示するには

1. Cyber Protectコンソールで **[デバイス]** > **[すべてのデバイス]** に進みます。
2. **[ビュー:]** ドロップダウンフィールドで、**[ハードウェア]** を選択します。
3. 以下に説明する方法のいずれかを使用して、検査するデバイスを見つけます。

- [**フィルター**] を使用してデバイスを見つけます:
  a. [**フィルター**] をクリックします。
  b. デバイスを見つけるには、1つまたは組み合わせた複数のフィルターパラメータを選択します。
  c. [**適用**] をクリックします。
- **検索**を使用してデバイスを見つけます:
  a. [**検索**] をクリックします。
  b. 完全なデバイス名またはデバイス名の一部を入力し、[**入力**] をクリックします。

4. デバイスのリストが掲載されている行をクリックして、[**インベントリ**] をクリックします。
5. [**ハードウェア**] タブをクリックします。
   次のハードウェアデータを利用できます。

ハードウェアコンポーネント	表示される情報
マザーボード	デバイスのマザーボードの名前、製造元、モデル、およびシリアルナンバー。
プロセッサー	デバイスの各プロセッサーの製造元、モデル、最大クロック速度、およびコア数。
RAM	デバイスのメモリの容量、製造元、およびシリアルナンバー。
グラフィック	デバイスのGPUの製造元とモデル。
ストレージドライブ	デバイスのストレージドライブのモデル、メディアタイプ、使用可能な領域、およびサイズ。
ネットワーク	デバイスのMacアドレス、IPアドレス、およびネットワークアダプターのタイプ。
システム	製品ID、元のインストール日、システムの起動時間、システムの製造元、システムモデル、BIOSバージョン、起動デバイス、システムロケール、およびシステムのタイムゾーン。

リモートデスクトップまたはリモートアシスタンス向けのワークロードへの接続

リモートデスクトップとアシスタンスは、組織内のワークロードに接続して、リモート制御やリモートアシスタンスを実行する便利な機能です。2022年12月より、NEAR、RDP、Apple画面共有の各プロトコルの機能がサポートされています。詳細については、"リモート接続プロトコル"（962ページ）を参照してください。

リモートデスクトップ機能を利用して、以下のタスクを実行できます。

- 表示のみモードでNEARを使用して、Windows、macOS、Linuxのワークロードにリモートで接続する。
- RDPを使用して、Windowsのワークロードにリモートで接続する。
- 表示のみモードまたはカーテンモードでApple画面共有を使用して、macOSのワークロードにリモートで接続する。
- クラウドのリモート接続を使用して、管理対象ワークロードに接続し、リモートで制御する。
- ダイレクトリモート接続を使用して、非管理対象ワークロードに接続し、リモートで制御する。
- Acronis クイックアシストを使用して、非管理対象のリモートワークロードに接続する。
- リモートワークロードの資格情報、監視または制御の許可要求、アクセスコード（クイックアシスト向け）など、さまざまな認証方式を使用してリモートワークロードに接続する。
- マルチビューで複数のモニターを同時に観察する。
- リモートセッションを記録する（NEAR経由の接続時）。
- セッション履歴レポートを表示する。

StandardおよびAdvanced Managementパックに含まれる機能の詳細については、"サポートされるリモートデスクトップおよびアシスタンス機能"（958ページ）を参照してください。

リモートアシスタンス機能を利用して、以下のタスクを実行できます。

- 制御モードでNEARを使用して、Windows、macOS、Linuxのワークロードにリモートで接続する。
- 制御モードでApple画面共有を使用して、macOSのワークロードにリモートで接続する。
- クラウドリモート接続を使用して、ワークロードにリモートアシスタンスを提供する。
- ローカルとリモートのワークロード間でファイルを転送する。
- リモートワークロードに対し、再起動、シャットダウン、スリープ、ごみ箱を空にする、リモートユーザーのログアウトなどの基本管理操作を実行する。
- リモートワークロードのデスクトップのスクリーンショットを定期的に取得し、リモートワークロードを監視する。

Standard ProtectionおよびAdvanced Managementに含まれる機能の詳細については、"サポートされるリモートデスクトップおよびアシスタンス機能"（958ページ）を参照してください。

重要
管理対象ワークロードのリモートデスクトップおよびアシスタンス機能をすべて有効にするには、ワークロードにリモート管理計画を設定し、適用する必要があります。1件のワークロードに適用できるリモート管理計画は1つだけですが、ニーズに応じて、異なるリモート管理計画を構成し、別のワークロードに適用することができます。

例えば、RDPプロトコルのみを有効にしたリモート管理計画を作成し、いくつかのワークロードに適用することができます。これにより、ワークロードごとにAdvanced Managementライセンスを有効にすることなく、これらのワークロードにリモートで接続できるようになります。追加の費用は発生しません。

一方、NEARとApple画面共有プロトコルを有効にした別のリモート管理計画を作成することもできます。この場合、Advanced Managementライセンスはワークロードごとに有効化され、このリモート管理計画が適用される各ワークロードについて費用が発生します。

リモート管理計画の詳細とその動作については、"リモート管理計画"（965ページ）を参照してください。

注意
リモートデスクトップとアシスタンス機能が必要です。

- 管理側（ホスト）のワークロードで、接続クライアントのワンタイムインストールを実行します。ターゲットワークロードに対して初めてリモート操作（リモート制御またはリモートアシスタンス）を実行しようとすると、システムからクライアントをダウンロードするよう促されます。または、保護コンソールの **[ダウンロード]** ウィンドウから接続クライアントをダウンロードすることもできます。構成可能な設定の詳細については、「"接続クライアント設定を構成する"（994ページ）」を参照してください。
- 管理対象ワークロードに接続エージェントをインストールします。接続エージェントは、バージョン15.0.31266以降の保護エージェントに含まれているモジュールです。
- macOSのリモートワークロードの場合、必要なシステム許可を接続エージェントに付与する必要があります。詳細については、"macOSでプロテクションエージェントをインストールする"（81ページ）を参照してください。
- 非管理ワークロードでAcronis クイックアシストアプリケーションを実行します。Acronis クイックアシストは、Webサイトからダウンロードできます。

各リモートデスクトップおよびアシスタンスコンポーネントでサポートされるプラットフォームについては、"サポートされるプラットフォーム"（961ページ）を参照してください。

サポートされるリモートデスクトップおよびアシスタンス機能

2022年12月に導入されたリモートデスクトップおよびアシスタンスでサポートされる機能の変更について、以下の表で詳しく説明します。

機能	Standard Protection 2022年12月より前	Advanced管理 2022年12月より前	Standard Protection 2022年12月以降	Advanced管理 2022年12月以降
Windows版RDPによるリモートアシスタンス	はい	いいえ	いいえ	いいえ
リモート接続をユーザーと共有する	いいえ	はい	いいえ	いいえ
リモート接続				
リモート操作	いいえ	いいえ	はい	はい
接続するWindows/macOS/Linuxのセッションを選択	いいえ	いいえ	いいえ	はい
RDPおよびApple画面共有経由での直接接続	いいえ	いいえ	いいえ	はい
マルチウィンドウ制御	いいえ	いいえ	いいえ	はい
接続モード:制御/表示のみ/カーテン	いいえ	いいえ	いいえ	はい
リモート接続のための共通資格情報サポート	いいえ	いいえ	はい	はい
技術者1人あたりの同時接続数				
RDP経由	はい	はい	はい	はい
NEAR経由	いいえ	いいえ	いいえ	はい
ファイル転送と共有				
WindowsからWindows/MacOS/Linuxへ	いいえ	いいえ	いいえ	はい
macOSからWindows/macOS/Linuxへ	いいえ	いいえ	いいえ	はい
LinuxからWindows/MacOS/Linuxへ	いいえ	いいえ	いいえ	はい
クイックアシストアプリケーション経由での接続				
WindowsからWindows/MacOS/Linuxへ	いいえ	いいえ	いいえ	はい
macOSからWindows/macOS/Linuxへ	いいえ	いいえ	いいえ	はい

機能	Standard Protection 2022年12月より前	Advanced管理 2022年12月より前	Standard Protection 2022年12月以降	Advanced管理 2022年12月以降
LinuxからWindows/MacOS/Linuxへ	いいえ	いいえ	いいえ	はい
プロトコル経由でのリモート接続				
NEAR経由でのリモート接続				
WindowsからWindows/MacOS/Linuxへ	いいえ	いいえ	いいえ	はい
macOSからWindows/macOS/Linuxへ	いいえ	いいえ	いいえ	はい
LinuxからWindows/MacOS/Linuxへ	いいえ	いいえ	いいえ	はい
RDP経由でのリモート接続（デスクトップクライアント）				
WindowsからWindowsへ	はい	はい	はい	はい
macOSからWindowsへ	はい	はい	はい	はい
LinuxからWindowsへ	いいえ	いいえ	はい	はい
RDP経由でのリモート接続（Webクライアント）				
WindowsからWindowsへ	はい	はい	はい	はい
macOSからWindowsへ	はい	はい	はい	はい
LinuxからWindowsへ	いいえ	いいえ	はい	はい
Apple画面共有経由でのリモート接続				
Windows/MacOS/LinuxからmacOSへ	いいえ	いいえ	いいえ	はい
セッション管理				
セッションの記録	いいえ	いいえ	いいえ	はい
レポートおよび監視				
セッション履歴と検索	いいえ	いいえ	いいえ	はい
スクリーンショット送信	いいえ	いいえ	いいえ	はい

サポートされるプラットフォーム

リモートデスクトップおよびアシスタンス機能の各コンポーネントでサポートされているオペレーティングシステムを次の表に示します。

リモートデスクトップコンポーネント	サポートされるプラットフォーム
接続クライアント	• Windows 7以降 • macOS 10.13以降 • Linux: openSUSE 8 Debian 9, 10 Ubuntu 18.0-20.10 Red Hat Enterprise Linux 8 CentOS 8 Fedora 31-33 SUSE Linux Enterprise Server 15 SP2 Linux Mint 20 Manjaro 20
接続エージェント	• Windows 7以降 • Windows Server 2008 R2以降 • macOS 10.13以降 • Linux: Red Hat Enterprise Linux 8、8.1 Fedora 30 Ubuntu 18.4 LTS（Bionic Beaver）～19.04（Disco Dingo） Debian 9, 10 CentOS 8 openSUSE 15.1
Acronis クイックアシスト	• Windows 7以降 • Windows Server 2008 R2以降 • macOS 10.13以降 • Linux: Red Hat Enterprise Linux 8、8.1 Fedora 30 Ubuntu 18.4 LTS（Bionic Beaver）～19.04（Disco Dingo） Debian 9, 10 CentOS 8 openSUSE 15.1

リモート接続プロトコル

リモートデスクトップ機能では、リモート接続に以下のプロトコルを使用します。

NEAR

NEARは、Acronisが開発した高度にセキュアなプロトコルであり、次のような特徴があります。

- ### H.264

  NEARには以下の3種類の品質モードが実装されています:**スムーズ**、**バランス**、**シャープ**です。**スムーズ**モードの場合、NEARはmacOSとWindowsのハードウェアH.264エンコードを使用してデスクトップ画像をエンコードします。ハードウェアエンコーダが使用できない場合はソフトウェアエンコードにフォールバックします。画像サイズは現在、フルHD解像度（1920x1080）に制限されています。

- ### アダプティブコーデック

  バランスおよび**シャープ**画質モードの場合、NEARでは、H.264が使用するビデオモードとは異なり、32ビットでフル画質を実現するアダプティブコーデックが使用されます。

  バランスモードでは、ネットワーク状況に応じて画質が自動的に調整され、現在のフレームレートが保持されます。

  シャープモードでは、画像はフル画質ですが、ネットワーク、プロセッサ、ビデオカードに負荷がかかっている場合、フレームレートが低下することがあります。

  WindowsとmacOSのグラフィックドライバで利用可能な場合、アダプティブコーデックにより、OpenCLが使用されます。

- ### サウンド転送

  NEARでは、リモートコンピューターの音声をキャプチャし、それをホストに転送することができます。Windows、macOS、Linuxでリモートサウンドリダイレクトを有効にする方法については、"リモート音声のリダイレクト"（963ページ）を参照してください。

- ### さまざまなログインオプション

  リモートワークロードにログインするために、次の手順を使用できます。

  アクセスコード:リモートワークロードにログインしているユーザーがクイックアシストを実行し、アクセスコードを伝えます。この方法では、常に現在ログインしているユーザーのセッションに接続します。

  ワークロード資格情報: ワークロードに登録されている管理者資格情報を使用して、リモートワークロードにログインします。

  観察または制御の許可を求める: リモートワークロードにログインしているユーザーに、接続の許可/拒否について尋ねます。

- セキュリティ

  データは、NEARのAES暗号化により必ず双方向で暗号化されます。

RDP

Remote Desktop Protocol（RDP）とは、Microsoftが開発した、ネットワーク経由でリモートのWindowsコンピューターに接続するための独自プロトコルです。

Apple画面共有

Apple画面共有は、macOSバージョン10.5以降に搭載されている、Appleが提供するVNCクライアントです。

リモート音声のリダイレクト

接続クライアントは、NEAR接続プロトコルによる音声ストリーミングをサポートしています。NEARの詳細については、"リモート接続プロトコル"（962ページ）を参照してください。

リモートのWindowsワークロードからの音声をリダイレクトする

Windowsワークロードの場合、リモートの音声は自動で送信されます。リモートワークロードに音声出力デバイス（スピーカーまたはヘッドホン）が接続されていることを確認してください。

リモートのmacOSワークロードからの音声をリダイレクトする

macOSワークロードからの音声リダイレクトを有効にするには、以下を確認します。

- ワークロードに保護エージェントがインストールされている。
- ワークロードにサウンドキャプチャドライバがインストールされている。
- ワークロードのリモート接続でNEARプロトコルが使用されている。

注意
macOS 10.15 Catalinaの場合、接続エージェントにマイクの使用許可が付与されている必要がある。接続エージェントにマイクの使用許可を付与する方法については、"接続エージェントに必要なシステム許可を付与する"（82ページ）を参照してください。

このエージェントは、以下のサウンドキャプチャドライバで動作します:SoundflowerまたはBlackhole。

最新バージョンのインストール方法については、Blackholeのwikiページ（https://github.com/ExistentialAudio/BlackHole/wiki/Installation）を参照してください。

注意
接続クライアントは現在、Blackholeの2チャンネル版のみをサポートしています。

また、ワークロードにHomebrewがインストールされている場合、以下のコマンドを実行して、Blackholeをインストールできます。

```
brew install --cask blackhole-2ch
```

注意
リモートのmacOSワークロードの音声がリダイレクトされている場合、リモートワークロードにログインしているユーザーには音声が聞こえません。

リモートのLinuxワークロードからの音声をリダイレクトする

リモートサウンドリダイレクトは、ほとんどのLinuxディストリビューションで自動的に動作します。デフォルトでリモートのサウンドリダイレクトが機能しない場合は、以下のコマンドを実行して、PulseAudioドライバをインストールしてください。

```
sudo apt-get install pulseaudio
```

リモートデスクトップまたはリモートアシスタンスのリモートワークロードへの接続

リモートデスクトップおよびリモートアシスタンス機能では、ワークロードに対するリモートダイレクト接続またはクラウド接続を確立するための、複数の方法が提供されています。

直接接続は、エージェントがインストールされていない接続クライアントとリモートワークロードの間で、ローカルエリアネットワーク（LAN）のTCP/IPを介して確立されます。インターネットアクセスは必要ありません。

クラウド接続は、接続クライアントとワークロード上のエージェントまたはクイックアシストとの間で、Acronisクラウドを介して確立されます。

クラウド接続のオプションの詳細については、次の表を参照してください。

クラウド接続	クラウド接続オプション	表示モード	サポートされるリモート操作	使用可能:
NEAR経由	接続クライアントから接続エージェント 接続クライアントからクイックアシスト	制御 表示のみ	リモートデスクトップ リモートアシスタンス	管理対象ワークロード
RDP経由	接続クライアントから接続エージェント Webクライアントから接続エージェント	制御	リモートデスクトップ	管理対象ワークロード
Apple画面共有経由	接続クライアントから接続エージェント	制御 表示の	リモートデスクトップ	管理対象ワークロード

クラウド接続	クラウド接続オプション	表示モード	サポートされるリモート操作	使用可能:
		み カーテン	リモートアシスタンス	

直接接続のオプションの詳細については、次の表を参照してください。

直接接続	直接接続オプション	サポートされるリモート操作	使用可能:
RDP経由	接続クライアントからRDPサーバー	リモートデスクトップ	非管理対象ワークロード
Apple画面共有経由	接続クライアントからApple画面共有サーバー	リモートデスクトップ リモートアシスタンス	非管理対象ワークロード

リモート管理計画

リモート管理計画とは、管理対象ワークロードのリモートデスクトップ機能とアシスタンス機能を有効化および構成するために、保護エージェント上で適用する計画のことです。

ワークロードにリモート管理計画が適用されていない場合、リモートデスクトップとアシスタンスの機能は、リモート操作（再起動、シャットダウン、スリープ、ごみ箱を空にする、リモートユーザーのログアウト）に制限されます。

注意
リモート管理計画で構成できる内容は、テナントに適用されているサービスパックに依存します。すべての設定にアクセスするには、Advanced Managementパックを有効化します。StandardおよびAdvanced Managementパックに含まれる機能の詳細については、"サポートされるリモートデスクトップおよびアシスタンス機能"（958ページ）を参照してください。

リモート管理計画を作成する

リモート管理計画を作成し、ワークロードに割り当てることで、管理対象ワークロードのリモートデスクトップおよびリモートアシスタンス機能を構成できます。

注意
リモート管理計画の設定が利用できるかどうかは、テナントに割り当てられているサービスクォータによって異なります。標準機能を使用する場合は、RDP経由の接続に限り構成できます。

前提条件

ユーザーアカウントの二要素認証が有効になっています。

リモート管理計画を作成するには

リモート管理計画から

1. Cyber Protectコンソールで **[管理]** > **[リモート管理計画]** に進みます。
2. 2種類のオプションのいずれかを使用して、リモート管理計画を作成します。
   - リストにリモート管理計画がない場合は、**[作成]** をクリックします。
   - リストにリモート管理計画が存在する場合は、**[計画を作成]** をクリックします。
3. （オプション） 計画のデフォルト名を変更するには、鉛筆のアイコンをクリックし、計画名を入力してから、**[続行]** をクリックします。
4. **[接続プロトコル]** をクリックし、このリモート管理計画でリモート接続に使用するプロトコル（NEAR、RDP、またはApple画面共有）を有効にします。
5. （オプション）NEARプロトコルの場合、**[セキュリティ設定]** セクションで、対応する設定を有効または無効にするチェックボックスを選択/クリアして、**[完了]** をクリックします。

設定	説明	使用可能:
ユーザーがコンソールセッションから切断したときにワークロードをロックします	この設定を選択すると、コンソールセッションを切断したときに、リモートワークロードがロックされます。	Windows、macOS
NEARによる同時接続またはファイル転送を単一のユーザーに限定	この設定を選択した場合、ワークロードへのリモート接続がアクティブな間は、NEARを使用した接続およびファイル転送が実行できなくなります。	Windows、macOS、Linux
ワークロードの管理者に、管理者以外のユーザーセッションへの接続を許可	この設定を選択すると、管理者がワークロード上の任意の標準ユーザーセッションに接続する許可を付与します。**[ワークロードの管理者に、管理者以外のユーザーセッションへの接続を許可]** および **[システムセッションの作成を許可]** のチェックが外されている場合は、リモートmacOSワークロードのアクティブな管理者セッションにのみ接続できます。	Windows、macOS
システムセッションの作成を許可	この設定を選択すると、管理者がリモート接続を確立する場合に、既存のアクティブセッションではなく、新しいセッションで接続するようになります。	macOS

設定	説明	使用可能:
クリップボードの同期を許可	この設定を選択すると、利用中のクリップボードとリモートワークロードのクリップボード間でデータを転送できるようになります。例えば、リモートワークロード上のファイルから任意のテキストをコピーして、利用中のワークロード上のファイルに貼り付けることができます。その反対も可能です。	Windows、macOS、Linux

6. **[セキュリティ設定]** をクリックしてから、対応する設定を有効または無効にするチェックボックスを選択/クリアして、**[完了]** をクリックします。

設定	説明
ワークロードがリモート制御の場合に表示	この設定を選択している場合、ワークロードに対するアクティブなリモートデスクトップ接続が存在しているときに、リモートワークロードのデスクトップに通知が表示されます。
ワークロードのスクリーンショットを取得する許可をユーザーに求める	この設定を選択にすると、管理者からリモートワークロードに対しスクリーンショット送信が要求された場合に、リモートワークロードのユーザーに通知が表示されます。

7. **[ワークロード管理]** をクリックし、リモートワークロードで利用する機能を選択してから、**[完了]** をクリックします。

設定	説明	以下で利用可能:
ファイル転送	ローカルとリモートのワークロード間のファイル転送を可能にします。	Windows、macOS、Linux
スクリーンショット送信	リモートワークロードのデスクトップのスクリーンショットをCyber Protectコンソールに送信できるようにします。	Windows、macOS、Linux

8. **[ディスプレイ設定]** をクリックしてから、対応する設定を有効または無効にするチェックボックスを選択/クリアして、**[完了]** をクリックします。

注意
[ディスプレイ設定] は、NEAR経由の接続でのみ利用可能です。

設定	説明	以下で利用可能:
デスクトップのキャプチャにデスクトップ重複除外を使用する	デスクトップの複製は、Windowsにおける画面キャプチャのメソッドの1つです。環境によっては、不安定になる場合もあります。デスクトップの重複除外を使用しない場合、代わりに基本メソッド（BitBlt）が使用されるようになります。	Windows
OpenCLアクセラレーションを使用する	OpenCLアクセラレーションは、グラフィック処理ユニット（GPU）で複数の計算を実行することにより、**バランス**品質モードで使用されるアダプティブコーデックを高速化することができます。このため、リモートLinuxにOpenCLドライバをインストールする必要があります。 グラフィックドライバで利用可能な場合は、macOSとWindowsで、アダプティブコーデックによりOpenCLが使用されます。	Linux
ハードウェアH.264エンコードを使用する	NEARで以下の3種類の品質モードがサポートされています。**スムーズ**、**バランス**、**シャープ**です。 **スムーズ**モードでは、デスクトップ画像のエンコードにハードウェアH.264エンコードが使用されます。 **バランス**モードの場合、NEARでは、H.264によって使用される「ビデオ」モードとは異なり32ビットでフル画質を実現するアダプティブコーデックが使用されます。画質はネットワーク状況に応じて自動的に調整され、現行のフレームレートが保持されます。 **シャープ**モードの場合、NEAR	Windows、macOS

設定	説明	以下で利用可能:
	では、H.264によって使用される「ビデオ」モードとは異なり32ビットでフル画質を実現するアダプティブコーデックが使用されます。画質は常に最高品質が維持されますが、ネットワークやプロセッサ/ビデオカードに負荷がかかると、fpsが低下する場合があります。	

9. ワークロードの詳細に、ワークロードに対するユーザーの最終ログイン情報を表示したい場合は、**ツールボックス**をクリックし、**[最終ログインユーザーを表示]** を選択してから、**[完了]** をクリックします。
   最後にログインしたユーザーの詳細については、"最終ログインユーザーを検索"（383ページ）を参照してください。
10. （オプション）計画にワークロードを追加するには:
    a. **[ワークロードを追加]** をクリックします。
    b. ワークロードを選択してから、**[追加]** をクリックします。
    c. 解決したい互換性の問題がある場合は、"リモート管理計画との互換性の問題を解決する"（976ページ）で説明されている手順を実行します。
11. **[作成]** をクリックします。

すべてのデバイスから

1. Cyber Protectコンソールで **[デバイス]** > **[すべてのデバイス]** に進みます。
2. リモート管理計画を適用したいワークロードをクリックします。
3. **[保護]** をクリックしてから、**[計画を追加]** をクリックします。
4. **[計画の作成]** をクリックして、**[リモート管理]** を選択します。
5. （オプション） 計画のデフォルト名を変更するには、鉛筆のアイコンをクリックし、計画名を入力してから、**[続行]** をクリックします。
6. **[接続プロトコル]** をクリックし、このリモート管理計画でリモート接続に使用するプロトコル（NEAR、RDP、またはApple画面共有）を有効にします。
7. （オプション）NEARプロトコルの場合、**[セキュリティ設定]** セクションで、対応する設定を有効または無効にするチェックボックスを選択/クリアして、**[完了]** をクリックします。

設定	説明	使用可能:
ユーザーがコンソールセッションから切断したときにワークロードをロックします	この設定を選択すると、コンソールセッションを切断したときに、リモートワークロードがロックされます。	Windows、macOS

設定	説明	使用可能:
NEARによる同時接続またはファイル転送を単一のユーザーに限定	この設定を選択した場合、ワークロードへのリモート接続がアクティブな間は、NEARを使用した接続およびファイル転送が実行できなくなります。	Windows、macOS、Linux
ワークロードの管理者に、管理者以外のユーザーセッションへの接続を許可	この設定を選択すると、管理者がワークロード上の任意の標準ユーザーセッションに接続する許可を付与します。**[ワークロードの管理者に、管理者以外のユーザーセッションへの接続を許可]** および **[システムセッションの作成を許可]** のチェックが外されている場合は、リモートmacOSワークロードのアクティブな管理者セッションにのみ接続できます。	Windows、macOS
システムセッションの作成を許可	この設定を選択すると、管理者がリモート接続を確立する場合に、既存のアクティブセッションではなく、新しいセッションで接続するようになります。	macOS
クリップボードの同期を許可	この設定を選択すると、利用中のクリップボードとリモートワークロードのクリップボード間でデータを転送できるようになります。例えば、リモートワークロード上のファイルから任意のテキストをコピーして、利用中のワークロード上のファイルに貼り付けることができます。その反対も可能です。	Windows、macOS、Linux

8. **[セキュリティ設定]** をクリックしてから、対応する設定を有効または無効にするチェックボックスを選択/クリアして、**[完了]** をクリックします。

設定	説明
ワークロードがリモート制御の場合に表示	この設定を選択している場合、ワークロード

設定	説明
	に対するアクティブなリモートデスクトップ接続が存在しているときに、リモートワークロードのデスクトップに通知が表示されます。
ワークロードのスクリーンショットを取得する許可をユーザーに求める	この設定を選択にすると、管理者からリモートワークロードに対しスクリーンショット送信が要求された場合に、リモートワークロードのユーザーに通知が表示されます。

9. **[ワークロード管理]** をクリックし、リモートワークロードで利用する機能を選択してから、**[完了]** をクリックします。

設定	説明	以下で利用可能:
ファイル転送	ローカルとリモートのワークロード間のファイル転送を可能にします。	Windows、macOS、Linux
スクリーンショット送信	リモートワークロードのデスクトップのスクリーンショットをCyber Protectコンソールに送信できるようにします。	Windows、macOS、Linux

10. **[ディスプレイ設定]** をクリックしてから、対応する設定を有効または無効にするチェックボックスを選択/クリアして、**[完了]** をクリックします。

注意
[ディスプレイ設定] は、NEAR経由の接続でのみ利用可能です。

設定	説明	以下で利用可能:
デスクトップのキャプチャにデスクトップ重複除外を使用する	デスクトップの複製は、Windowsにおける画面キャプチャのメソッドの1つです。環境によっては、不安定になる場合もあります。デスクトップの重複除外を使用しない場合、代わりに基本メソッド（BitBlt）が使用されるようになります。	Windows
OpenCLアクセラレーションを使用する	OpenCLアクセラレーションは、グラフィック処理ユニット（GPU）で複数の計算を実行することにより、**バランス**	Linux

設定	説明	以下で利用可能:
	品質モードで使用されるアダプティブコーデックを高速化することができます。このため、リモートLinuxにOpenCLドライバをインストールする必要があります。 グラフィックドライバで利用可能な場合は、macOSとWindowsで、アダプティブコーデックによりOpenCLが使用されます。	
ハードウェアH.264エンコードを使用する	NEARでは3つの品質モードがサポートされています。**スムーズ**、**バランス**、**シャープ**です。 **スムーズ**モードでは、デスクトップ画像のエンコードにハードウェアH.264エンコードが使用されます。 **バランス**モードの場合、NEARでは、H.264によって使用される「ビデオ」モードとは異なり32ビットでフル画質を実現するアダプティブコーデックが使用されます。画質はネットワーク状況に応じて自動的に調整され、現行のフレームレートが保持されます。 **シャープ**モードの場合、NEARでは、H.264によって使用される「ビデオ」モードとは異なり32ビットでフル画質を実現するアダプティブコーデックが使用されます。画質は常に最高品質が維持されますが、ネットワークやプロセッサ/ビデオカードに負荷がかかると、fpsが低下する場合があります。	Windows、macOS

11. ワークロードの詳細に、ワークロードに対するユーザーの最終ログイン情報を表示したい場合は、**ツールボックス**をクリックし、**[最終ログインユーザーを表示]** を選択してから、**[完了]** をクリックします。

最後にログインしたユーザーの詳細については、"最終ログインユーザーを検索"（383ページ）を参照してください。

12. **[作成]** をクリックします。

リモート管理計画にワークロードを追加する

必要に応じて、計画を作成してから、リモート管理計画にワークロードを追加できます。

前提条件

ユーザーアカウントの二要素認証が有効になっています。

リモート管理計画にワークロードを追加するには

リモート管理計画から

1. Cyber Protectコンソールで **[管理]** > **[リモート管理計画]** に進みます。
2. リモート管理計画をクリックします。
3. 既に計画が適用されているワークロードの有無に応じて、次の操作を実行します。
   - 計画がまだいずれのワークロードにも適用されていない場合は、**[ワークロードを追加]** をクリックします。
   - 計画がいずれかのワークロードに適用されている場合は、**[ワークロードを管理]** をクリックします。
4. リストでワークロードを選択してから、**[追加]** をクリックします。
5. **[保存]** をクリックします。
6. **[確認]** をクリックすると、必要なサービスクォータがワークロードに適用されます。

すべてのデバイスから

1. Cyber Protectコンソールで **[デバイス]** > **[すべてのデバイス]** に進みます。
2. リモート管理計画を適用したいワークロードをクリックします。
3. **[保護]** をクリックしてから、**[計画を追加]** をクリックします。
4. **[以下のリストから計画を選択]** で、**[リモート管理]** を選択して、該当のリモート管理計画のみを表示します。
5. **[適用]** をクリックします。
6. **[確認]** をクリックすると、必要なサービスクォータがワークロードに適用されます。

リモート管理計画からワークロードを削除する

必要に応じて、リモート管理計画からワークロードを削除できます。

前提条件

ユーザーアカウントの二要素認証が有効になっています。

リモート管理計画からワークロードを削除するには

1. Cyber Protectコンソールで **[管理]** > **[リモート管理計画]** に進みます。
2. リモート管理計画をクリックします。
3. **[ワークロードを管理]** をクリックします。
4. リモート管理計画から削除する1つまたは複数のワークロードを選択し、**[削除]** をクリックします。
5. **[完了]** をクリックします。
6. **[保存]** をクリックします。

既存リモート管理計画での追加処理

[リモート管理計画] 画面で、リモート管理計画に関する次の追加処理を実行できます: 詳細の表示、編集、アクティビティの表示、アラートの表示、名前の変更、有効化、無効化、クローン作成、エクスポート、削除。

詳細の表示

前提条件

ユーザーアカウントの二要素認証が有効になっています。

リモート管理計画の詳細を表示するには

1. **[リモート管理計画]** 画面で、リモート管理計画の **[その他の操作]** アイコンをクリックします。
2. **[詳細の表示]** をクリックします。

編集

前提条件

ユーザーアカウントの二要素認証が有効になっています。

計画を編集するには

1. **[リモート管理計画]** 画面で、リモート管理計画の **[その他の操作]** アイコンをクリックします。
2. **[編集]** をクリックします。

アクティビティ

リモート管理計画に関連するアクティビティを表示するには

1. **[リモート管理計画]** 画面で、リモート管理計画の **[その他の操作]** アイコンをクリックします。
2. **[アクティビティ]** をクリックします。
3. アクティビティをクリックすると、その詳細が表示されます。

アラート

アラートを表示するには

1. **[リモート管理計画]** 画面で、リモート管理計画の **[その他の操作]** アイコンをクリックします。
2. **[アラート]** をクリックします。

名前の変更

前提条件

ユーザーアカウントの二要素認証が有効になっています。

リモート管理計画の名前を変更するには

1. **[リモート管理計画]** 画面で、リモート管理計画の **[その他の操作]** アイコンをクリックします。
2. **[名前の変更]** をクリックします。
3. 計画の新しい名前を入力し、**[続行]** をクリックします。

有効にする

前提条件

ユーザーアカウントの二要素認証が有効になっています。

リモート管理計画を有効化するには

1. **[リモート管理計画]** 画面で、リモート管理計画の **[その他の操作]** アイコンをクリックします。
2. **[有効にする]** をクリックします。

無効にする

前提条件

ユーザーアカウントの二要素認証が有効になっています。

リモート管理計画を無効化するには

1. **[リモート管理計画]** 画面で、リモート管理計画の **[その他の操作]** アイコンをクリックします。
2. **[無効にする]** をクリックします。

クローンを作成

前提条件

ユーザーアカウントの二要素認証が有効になっています。

リモート管理計画のクローンを作成するには

1. **[リモート管理計画]** 画面で、リモート管理計画の **[その他の操作]** アイコンをクリックします。
2. **[クローン]** をクリックします。
3. **[作成]** をクリックします。

エクスポート

前提条件

ユーザーアカウントの二要素認証が有効になっています。

リモート管理計画をエクスポートするには

1. **[リモート管理計画]** 画面で、リモート管理計画の **[その他の操作]** アイコンをクリックします。
2. **[エクスポート]** をクリックします。
   計画の構成はJSON形式でローカルのマシンにエクスポートされます。

削除

前提条件

ユーザーアカウントの二要素認証が有効になっています。

リモート管理計画を削除するには

1. **[リモート管理計画]** 画面で、リモート管理計画の **[その他の操作]** アイコンをクリックします。
2. **[削除]** をクリックします。
3. **[確認しました]** を選択して、**[削除]** をクリックします。

リモート管理計画との互換性の問題

ワークロードにリモート管理計画を適用すると、互換性の問題が発生する場合があります。以下のような互換性の問題が考えられます:

- 計画の競合 - ワークロードには1つのリモート管理計画しか適用できないため、別のリモート管理計画が既にワークロードに適用されている場合、この問題が発生します。
- 互換性のないオペレーティングシステム - この問題は、ワークロードのオペレーティングシステムがサポートされていない場合に発生します。
- サポートされていないエージェント - この問題は、ワークロード上のプロテクションエージェントのバージョンが古く、リモートデスクトップ機能がサポートされていない場合に発生します。
- クォータの不足 - この問題は、選択したワークロードに割り当てる十分なサービスクォータがテナントに存在しない場合に発生します。

150件以下のワークロードを個別に選択して、リモート管理計画を適用する場合、計画を保存する前に、既存の競合を解決するよう通知が表示されます。競合を解決するには、競合の根本原因を取り除くか、影響を受けるワークロードを計画から削除します。詳細については、"リモート管理計画との互換性の問題を解決する"（976ページ）を参照してください。競合を解決せずに計画を保存すると、互換性のないワークロードに対して計画が自動的に無効にされ、アラートが表示されます。

150件を超えるワークロードまたはデバイスグループに、リモート管理計画を適用する場合、保存が完了した後で互換性が確認されます。互換性のないワークロードについては、計画が自動的に無効化され、アラートが表示されます。

リモート管理計画との互換性の問題を解決する

互換性の問題の原因に応じ、新しいリモート管理計画を作成するプロセスの一環として、互換性の問題を解決するための各操作を実行できます。

注意
互換性の問題を解決するために計画からワークロードを削除する場合、デバイスグループの一部となっているワークロードを削除することはできません。

互換性の問題を解決するには

1. **[問題をレビュー]** をクリックします。
2. （新しい計画からワークロードを削除して、既存のリモート管理計画との間にある互換性の問題を解決するには）
   a. **[競合する計画]** タブで、削除するワークロードを選択します。
   b. **[計画からワークロードを削除]** をクリックします。
   c. **[削除]** をクリックしてから、**[閉じる]** をクリックします。
3. （ワークロードに既に適用されている計画を無効にして、リモート管理計画との互換性の問題を解決するには）
   a. **[適用された計画を無効化]** をクリックします。
   b. **[無効化]** をクリックしてから、**[閉じる]** をクリックします。
4. （互換性がないオペレーティングシステムの互換性の問題を解決するには）
   a. **[互換性がないオペレーティングシステム]** タブで、削除するワークロードを選択します。
   b. **[計画からワークロードを削除]** をクリックします。
   c. **[削除]** をクリックしてから、**[閉じる]** をクリックします。
5. （計画からワークロードを削除して、サポートされていないエージェントの互換性の問題を解決するには）
   a. **[サポートされていないエージェント]** タブで、削除するワークロードを選択します。
   b. **[計画からワークロードを削除]** をクリックします。
   c. **[削除]** をクリックしてから、**[閉じる]** をクリックします。
6. （エージェントのバージョンをアップデートして、サポートされていないエージェントとの互換性の問題を解決するには）**[エージェントリストに移動]** をクリックします。

   注意
   このオプションを使用できるのは、カスタマー管理者のみです。

7. （計画からワークロードを削除して、クォータの不足を伴う互換性の問題を解決するには）
   a. **[クォータの不足]** タブで、削除するワークロードを選択します。
   b. **[計画からワークロードを削除]** をクリックします。
   c. **[削除]** をクリックしてから、**[閉じる]** をクリックします。
8. （テナントのクォータを増やして、クォータの不足による互換性の問題を解決するには）

   注意
   このオプションを使用できるのは、パートナー管理者のみです。

   a. **[クォータの不足]** タブで、**[管理ポータルに移動]** をクリックします。
   b. カスタマーのサービスクォータを増やします。

ワークロードの資格情報

リモートワークロードの管理者および非管理者の資格情報（ユーザー名とパスワード、またはVNCパスワード）を追加してクラウド資格情報ストアに保存し、管理対象のワークロードに接続する際の自動認証に使用することができます。この方法では、接続の認証段階で毎回資格情報を手動で入力するのではなく、資格情報ストアにこれらの資格情報を保存しておき、複数のワークロードに割り当てます。こうして、接続クライアントがワークロードにリモートで接続するたびに、これらの資格情報を使用できるようになります。

注意

資格情報ストアに保存される資格情報は、異なるテナントレベルの間で共有されることはありません。資格情報は、同一のカスタマーテナントまたはパートナーテナントの同じテナントレベルでのみ共有されます。

つまり、カスタマーテナントに複数の管理者が存在する場合、それらの管理者は資格情報ストアにある資格情報を参照および共有できますが、他のパートナー管理者や他のテナントのカスタマー管理者は、これらの資格情報を参照または使用することができません。

資格情報の追加

資格情報を追加して、複数のワークロードに対するリモート接続に使用できます。

ワークロードに資格情報を追加して、資格情報ストアに保存するには

1. Cyber Protectコンソールで **[デバイス]** > **[すべてのデバイス]** に進みます。
2. 資格情報を追加したいワークロードをクリックします。
3. 次のいずれかの方法で **[設定]** メニューにアクセスできます。
   - **[リモートデスクトップ]**、**[設定]** の順にクリックします。
   - **[管理]** をクリックしてから、**[設定]** をクリックします。
4. **[資格情報を追加]** をクリックします。
5. **[資格情報ストア]** で、**[資格情報を追加]** をクリックします。
6. 資格情報を入力します。

フィールド	説明
資格情報名	資格情報ストアで表示される資格情報の識別子。
ユーザー名	ターゲットワークロードへのリモート接続に使用されるユーザー名。
パスワード	ターゲットワークロードへのリモート接続に使用されたパスワード。
VNCパスワード	このフィールドは、Apple画面共有の場合のみ利用可能です。

7. **[保存]** をクリックします。

ワークロードに資格情報を割り当てる

資格情報を追加すると、管理対象のワークロードに接続する際に、その資格情報を使用して自動的に認証されるようになります。

自動認証のために保存された資格情報をワークロードに割り当てるには

1. Cyber Protectコンソールで **[デバイス]** > **[すべてのデバイス]** に進みます。
2. 次のいずれかの方法で **[設定]** メニューにアクセスできます。
   - **[リモートデスクトップ]**、**[設定]** の順にクリックします。
   - **[管理]** をクリックしてから、**[設定]** をクリックします。
3. サポートされているプロトコル（NEAR、RDP、またはApple画面共有）のタブで、**[資格情報を追加]** をクリックします。
4. **資格情報ストア**で、リストから資格情報を選択し、**[資格情報を選択]** をクリックします。

資格情報の削除

不要になった資格情報を削除できます。

資格情報ストアから資格情報を削除するには

1. Cyber Protectコンソールで **[デバイス]** > **[すべてのデバイス]** に進みます。
2. 次のいずれかの方法で **[設定]** メニューにアクセスできます。
   - **[リモートデスクトップ]**、**[設定]** の順にクリックします。
   - **[管理]** をクリックしてから、**[設定]** をクリックします。
3. サポートされているプロトコル（NEAR、RDP、またはApple画面共有）のタブで、**[削除]** をクリックします。
4. 確認ウィンドウで **[削除]** をクリックします。

ワークロードから資格情報の割り当てを解除する

ワークロードから資格情報の割り当てを解除しても、資格情報ストアに資格情報を保持することができます。

1. Cyber Protectコンソールで **[デバイス]** > **[すべてのデバイス]** に進みます。
2. 次のいずれかの方法で **[設定]** メニューにアクセスできます。
   - **[リモートデスクトップ]**、**[設定]** の順にクリックします。
   - **[管理]** をクリックしてから、**[設定]** をクリックします。
3. サポートされているプロトコル（NEAR、RDP、またはApple画面共有）のタブで、**[割り当て解除する]** をクリックします。
4. 確認ウィンドウで **[割り当て解除]** をクリックします。

管理対象のワークロードの動作

管理対象ワークロードとは、保護エージェントがインストールされたワークロードを指します。

リモートの管理対象ワークロード上で次の操作を実行できます。

- 制御モードまたは表示のみモードでNEARを使用して、リモートアシスタンスやリモートデスクトップに接続
- 制御モードでRDPを使用して、リモートデスクトップに接続
- 制御モード、表示のみモード、カーテンモードでApple画面共有を使用して、リモートアシスタンスまたはリモートデスクトップに接続
- Webクライアント経由で、リモートデスクトップに接続
- リモートワークロードに対し、再起動、シャットダウン、スリープ、ごみ箱を空にする、リモートユーザーのログアウトを実行する
- 自分のワークロードとリモートのワークロードの間でファイルを転送する
- 管理対象ワークロードのスクリーンショットを取得して監視する

注意
管理対象ワークロードへのリモートデスクトップ接続で、保護エージェントのインストールとワークロードへのリモート管理計画の適用が必要になります。

RDP設定を構成する

管理対象ワークロードのリモート制御RDP接続に自動で適用される設定を構成できます。

ワークロードのRDP設定を構成するには

1. Cyber Protectコンソールで **[デバイス]** > **[エージェントがインストールされているマシン]** に進みます。
2. 次のいずれかの方法で **[設定]** メニューにアクセスできます。
   - **[リモートデスクトップ]**、**[設定]** の順にクリックします。
   - **[管理]** をクリックしてから、**[設定]** をクリックします。

3. [**RDP**] タブで設定を構成します。

設定	説明
オーディオの再生	この設定により、ローカルワークロード上でのリモートワークロード音声のリダイレクトを有効化または無効化します。
オーディオの記録	音声録音（マイク入力）をリモートワークロードに転送するかどうかを設定します。
プリンタをリダイレクト	この設定を選択すると、ワークロードのプリンタがリモートワークロードで利用できるようになります。
ファイルをリダイレクト	この設定により、ローカルワークロードのファイルをリモートワークロードに共有するかどうかを定義します。
色深度	この設定で、RDPが転送する画像の色数を決定します。値が大きい程、帯域幅が大きくなります。 **Highカラー**:16ビット **Trueカラー**: • Webクライアントによる RDP接続の場合は24ビット • 接続クライアントによるRDP接続の場合は32ビット

4. 閉じるボタンをクリックします。

リモートデスクトップまたはリモートアシスタンス向けの管理対象ワークロードへの接続

注意
リモート接続に使用できる接続プロトコルは、リモート管理計画の構成とリモートワークロードのオペレーティングシステムによって異なります。

前提条件

- 対応する接続プロトコルを有効にしたリモート管理計画が、管理対象のワークロードに適用されます。
- ワークロードに必要なサービスクォータが割り当てられます。（ワークロードにリモート管理計画を適用すると、サービスクォータが自動的に取得されます）。
- （Apple画面共有接続の場合）macOSのワークロードでApple画面共有が有効になっています。
- Acronis Cyber Protect Cloudで、ユーザーアカウントの二要素認証が有効化されます。

リモートデスクトップまたはリモートアシスタンス向けの管理対象ワークロードにリモートで接続するには

1. Cyber Protectコンソールで [**デバイス**] > [**エージェントがインストールされているマシン**] に進みます。
2. 接続したいワークロードをクリックします。
3. [**リモートデスクトップ**] をクリックします。

デフォルトでは、接続プロトコルとしてNEARが選択されています。

4. （オプション）**[接続プロトコル]** ドロップダウンリストで、使用する接続プロトコルを選択します。
5. 使用するビューモードをクリックします。

プロトコル	リモート接続先	表示モード	サポートされるリモート操作
NEAR	Windows Linux macOS	**制御** - このモードでは、リモートワークロードを観察し、処理を実行できます。 **表示のみ** - このモードでは、リモートワークロードの観察のみが可能です。	リモートデスクトップ リモートアシスタンス
RDP	Windows	**制御** - このモードでは、リモートワークロードを表示し、処理を実行できます。 **注意** ワークロードのOS設定でRDPが無効になっている場合、ポップアップウィンドウが表示されます。このウィンドウを使用して、現在のセッションの、または全般的なワークロードのRDPを有効にします。 • 現在のセッションでのみワークロードのRDPを有効にする場合は、**[セッション終了後に無効化してください]** を選択し、**[許可]** をクリックします。 • このワークロードでRDPを有効にする場合は、**[許可]** をクリックします。	リモートデスクトップ
Apple画面共有	macOS	**制御** - このモードでは、リモートワークロードを観察し、処理を実行できます。 **表示のみ** - このモードでは、リモートワークロードの観察のみが可能です。 **カーテン** - macOSのワークロードでのみ利用可能です。カーテンモードでリモートワークロードに接続すると、リモートワークロードのディスプレイが暗転し、リモートユーザーにワークロード上での操作が表示されなくなります。	リモートデスクトップ リモートアシスタンス

6. ワークロードでの接続クライアントインストールの有無に応じて、次のいずれかを実行します。
   - 接続クライアントがインストールされていない場合は、ダウンロードしてインストールし、表示される確認のポップアップで **[許可]** を選択します。

- 接続クライアントが既にインストールされている場合は、表示される確認のポップアップで **[接続クライアントを開く]** をクリックします。

7. **[認証]** ウィンドウで、認証オプションを選択し、必要な資格情報を入力します。

注意
ワークロードに資格情報を割り当てている場合、認証は自動的に行われ、この手順はスキップされます。詳細については、"ワークロードに資格情報を割り当てる"（979ページ）を参照してください。

認証オプション	説明
リモートワークロードの資格情報	リモートワークロードの管理者ユーザーのユーザー名とパスワードを指定すると、リモート接続の確立が許可されます。 このオプションは、NEAR、RDP、Apple画面共有で利用可能です。 このオプションは、リモートデスクトップおよびリモートアシスタンス向けの認証に使用できます。
観察の許可を求める	リモートワークロードでログインしているユーザーが許可した後に、観察モードでのリモート接続の確立が許可されます。 このオプションは、NEARおよびApple画面共有で利用可能です。 このオプションは、リモートアシスタンス向けの認証に使用できます。
制御の許可を求める	リモートワークロードでログインしているユーザーが許可した後に、制御モードでのリモート接続の確立が許可されます。 このオプションは、NEARおよびApple画面共有で利用可能です。 このオプションは、リモートアシスタンス向けの認証に使用できます。

8. **[接続]** をクリックしてから、表示するセッションをクリックします（ワークロードで複数のユーザーセッションが利用可能な場合）。
   接続クライアントで、リモートワークロードのデスクトップを表示できる新しいビューアウィンドウが開きます。ビューアには、リモート接続が確立された後にリモートワークロード上で実行できる、追加操作のためのツールバーがあります。詳細については、"ビューアウィンドウのツールバーを使用する"（991ページ）を参照してください。

Webクライアントによる管理対象ワークロードへの接続

Webクライアント経由で、管理対象ワークロードへのリモートデスクトップ接続を確立することができます。

前提条件

- ワークロードに標準サービスクォータが割り当てられます。
- RDPを有効にしたリモート管理計画が管理対象ワークロードに適用されます。
- 管理対象ワークロードでRDPが有効化されます。
- ブラウザがHTML5をサポートしています。
- Acronis Cyber Protect Cloudで、ユーザーアカウントの二要素認証が有効化されます。

Webクライアント経由でワークロードにリモート接続するには

1. Cyber Protectコンソールで **[デバイス]** > **[すべてのデバイス]** に進みます。
2. リモート接続の対象となるワークロードをクリックし、**[リモートデスクトップ]** > **[Webクライアント経由で接続]** をクリックします。
3. ワークロードにアクセスするためのログイン情報とパスワードを入力して、**[接続]** をクリックします。

> **注意**
> ワークロードに資格情報を割り当てている場合、認証は自動的に行われ、この手順はスキップされます。詳細については、"ワークロードに資格情報を割り当てる"（979ページ）を参照してください。

ファイルの転送

ローカルワークロードと管理対象ワークロードの間で、簡単にファイルを転送できます。

前提条件

- NEARプロトコルとファイル転送を有効にしたリモート管理計画がワークロードに適用されます。
- Advanced Managementのクォータがワークロードで適用されています。
- Acronis Cyber Protect Cloudで、ユーザーアカウントの二要素認証が有効化されます。

自分のワークロードと管理対象のワークロード間でファイルをリモート転送するには

1. Cyber Protectコンソールで **[デバイス]** > **[エージェントがインストールされているマシン]** に進みます。
2. 転送したいファイルを含むワークロードをクリックします。
3. **[管理]** をクリックしてから、**[ファイルを転送]** を選択します。
4. ワークロードでの接続クライアントインストールの有無に応じて、次のいずれかを実行します。
   - 接続クライアントがインストールされていない場合は、ダウンロードしてインストールし、表示される確認のポップアップで **[許可]** をクリックします。
   - 接続クライアントが既にインストールされている場合は、表示される確認のポップアップで **[接続クライアントを開く]** をクリックします。
5. **[認証]** ウィンドウで、認証オプションを選択し、必要な資格情報を入力します。

認証オプション	説明
リモートワークロードの資格情報	リモートワークロードの管理者ユーザーのユーザー名とパスワードを指定すると、リモート接続の確立が許可されます。
ファイル転送の許可を求める	リモートワークロードでログインしているユーザーが許可した後に、ファイルの転送が許可されます。

6. **[ファイル転送]** ウィンドウでファイルを参照し、任意の転送先にドラッグアンドドロップします。

注意
ローカルワークロードのファイルは左ペインに、リモートワークロードのファイルは右ペインに表示されます。
ファイル転送が開始されると、**[タスク]**ペインに表示されます。

7. （オプション） 完了したタスクを**[タスク]**ペインから削除するには、**[完了をクリア]** をクリックします。
8. すべての転送が完了したら、ウィンドウを閉じます。

管理対象ワークロードで制御操作を実行する

リモートワークロードに対して、ごみ箱を空にする、スリープ、再起動、シャットダウン、リモートユーザーのログアウトなどの基本的な制御操作を実行して、リモートワークロードを管理できます。

前提条件

- ワークロードに標準サービスクォータが適用されます。
- Acronis Cyber Protect Cloudで、ユーザーアカウントの二要素認証が有効化されます。

ごみ箱を空にする

リモートワークロードでごみ箱を空にするには

1. Cyber Protectコンソールで **[デバイス]** > **[エージェントがインストールされているマシン]** に進みます。
2. この操作を実行したいワークロードをクリックします。
3. **[管理]** をクリックしてから、**[ごみ箱を空にする]** をクリックします。
4. この操作を行いたいユーザーセッションを選択し、**[ごみ箱を空にする]** をクリックします。

スリープ

リモートワークロードをスリープさせるには

1. Cyber Protectコンソールで **[デバイス]** > **[エージェントがインストールされているマシン]** に進みます。
2. この操作を実行したいワークロードをクリックします。
3. **[管理]** をクリックしてから、**[スリープ]** をクリックします。

再起動

リモートワークロードを再起動するには

1. Cyber Protectコンソールで **[デバイス]** > **[エージェントがインストールされているマシン]** に進みます。
2. この操作を実行したいワークロードをクリックします。
3. **[管理]** をクリックしてから、**[再起動]** をクリックします。
   - Windowsワークロードの場合、ワークロードを再起動する前に、ワークロードにローカルで現在ログインしているユーザーが変更を保存できるようにするかどうかを選択し、ユーザーを選択し

てから、再度 **[再起動]** をクリックします。

- macOSワークロードの場合、ワークロードを再起動する前に、ワークロードにローカルで現在ログインしているユーザーが変更を保存できるようにするかどうかを選択してから、再度 **[再起動]** をクリックします。
- Linuxワークロードの場合、**[再起動]** をクリックします。

シャットダウン

リモートワークロードをシャットダウンするには

1. Cyber Protectコンソールで **[デバイス]** > **[エージェントがインストールされているマシン]** に進みます。
2. この操作を実行したいワークロードをクリックします。
3. **[管理]** をクリックしてから、**[シャットダウン]** をクリックします。
   - Windowsワークロードの場合、ワークロードをシャットダウンする前に、ワークロードにローカルで現在ログインしているユーザーが変更を保存できるようにするかどうかを選択し、ユーザーを選択してから、再度 **[シャットダウン]** をクリックします。
   - macOSワークロードの場合、ワークロードをシャットダウンする前に、ワークロードにローカルで現在ログインしているユーザーが変更を保存できるようにするかどうかを選択してから、再度 **[シャットダウン]** をクリックします。
   - Linuxワークロードの場合、**[シャットダウン]** をクリックします。

リモートユーザーをログアウト

リモートワークロードのユーザーをログアウトするには

1. Cyber Protectコンソールで **[デバイス]** > **[エージェントがインストールされているマシン]** に進みます。
2. この操作を実行したいワークロードをクリックします。
3. **[管理]** をクリックしてから、**[リモートユーザーをログアウト]** をクリックします。
4. ログアウトするユーザーを選択してから、**[ログアウト]** をクリックします。

スクリーンショット送信によるワークロードの監視

スクリーンショット送信機能により、ワークロードの状態を監視できます。

前提条件

- スクリーンショット送信機能を有効にしたリモート管理計画がワークロードに適用されます。
- プロテクションエージェントのバージョンは最新で、スクリーンショット送信機能をサポートしています。
- Advanced Managementのサービスクォータがワークロードで適用されています。
- このワークロードはオンラインです。
- Acronis Cyber Protect Cloudで、ユーザーアカウントの二要素認証が有効化されます。

スクリーンショット送信によるワークロードの監視

スクリーンショット送信によりワークロードを監視するには

1. Cyber Protectコンソールで **[デバイス]** > **[スクリーンショット送信]** に進みます。
2. 監視するワークロードをクリックします。
3. ユーザーセッションを選択します。
4. ディスプレイを選択します。
5. デスクトップの新しいスクリーンショットを取得するリフレッシュレートを選択します。
6. イメージの品質を選択します。
7. スクリーンショットをダウンロードするには、ダウンロードアイコンをクリックします。

ワークロードのスクリーンショットを取得する

管理対象のワークロードのスクリーンショットを取得するには

1. Cyber Protectコンソールで **[デバイス]** > **[エージェントがインストールされているマシン]** に進みます。
2. スクリーンショットを取得するワークロードをクリックします。
3. **[管理]** をクリックしてから、**[デスクトップのスクリーンショットを取得]** をクリックします。
   ワークロードが選択された状態で、**[スクリーンショット送信]** 画面が開きます。ワークロードに適用されているリモート管理計画の設定に応じて、スクリーンショットが直接表示される場合と、リモートワークロードのユーザーによるリクエスト承認後に表示される場合があります。

複数の管理対象ワークロードを同時に観察する

複数のリモートワークロードのデスクトップを単一のウィンドウで同時に観察できます。

注意
ウィンドウ内に同時に表示できるデスクトップの数は、モニターのサイズに応じて異なります。

前提条件

- ワークロードに適用されるリモート管理計画で、NEARまたはApple画面共有を有効にします。
- Advanced Managementのサービスクォータがワークロードで適用されています。
- Acronis Cyber Protect Cloudで、ユーザーアカウントの二要素認証が有効化されます。

複数のワークロードを同時に観察するには

1. Cyber Protectコンソールで **[デバイス]** > **[すべてのデバイス]** に進みます。
2. 観察するワークロードを選択します。
3. **[マルチビュー]** をクリックします。
4. ワークロードでの接続クライアントインストールの有無に応じて、次のいずれかを実行します。
   - 接続クライアントがインストールされていない場合は、ダウンロードしてインストールし、表示される確認のポップアップで **[許可]** を選択します。
   - 接続クライアントが既にインストールされている場合は、表示される確認のポップアップで **[接続クライアントを開く]** をクリックします。
5. **[認証]** ウィンドウで、認証オプションを選択し、必要な資格情報を入力します。

認証オプション	説明
リモートワークロードの資格情報	リモートワークロードの管理者ユーザーのユーザー名とパスワードを指定すると、リモート接続の確立が許可されます。
観察の許可を求める	リモートワークロードでログインしているユーザーが許可した後に、観察モードでのリモート接続の確立が許可されます。

6. 手順2で選択したすべてのリモートワークロードに接続する際に、同じ認証方式と資格情報を使用する場合は、[**他のコンピューターで使用する**] を選択します。
7. [**接続**] をクリックします。
   マルチビューウィンドウのツールバーで、ワークロードに接続するビューモードを選択できます。この操作により、該当のワークロード向けに別のビューアウィンドウが開きます。

注意
選択したワークロードのいずれかがオフラインである場合、またエージェントの古いバージョンがインストールされている場合は、マルチビューウィンドウに表示されません。
リモートワークロードに対するすべてのマルチビュー接続は、**表示のみ**モードになります。

非管理ワークロードの動作

非管理ワークロードとは、保護エージェントがインストールされていないワークロードを指します。

リモートの非管理ワークロード上で次の操作を実行できます。

- Acronisクイックアシストを使用してリモートアシスタンスに接続
- IPアドレスを使用してリモートデスクトップまたはリモートアシスタンスに接続
- クイックアシストを使用して、自分のワークロードとリモートのワークロードの間でファイルを転送する

注意
クイックアシストを使用して非管理対象のワークロードにリモート接続します。以下を確認してください。

- Advanced Managementパックが、カスタマーテナントに対して有効化されている。
- 接続先のリモートワークロードでクイックアシストアプリケーションが動作している。

Acronis クイックアシスト経由で非管理対象をワークロードに接続する

クイックアシスト機能を使用すると、オンデマンドで非管理下のワークロードにリモート接続し、1回限りのアシストを提供できます。

前提条件

- Advanced Managementパックは、カスタマーテナントに割り当てられます。
- Acronis Cyber Protect Cloudで、ユーザーアカウントの二要素認証が有効化されます。
- リモートユーザーは、クイックアシストからワークロードIDおよびアクセスコードを提供されています。
- リモートユーザーがAcronis クイックアシストをダウンロードおよび実行しました。

クイックアシストを使用してリモートアシスタンス向けのワークロードに接続するには

1. Cyber Protectコンソールで **[デバイス]** > **[すべてのデバイス]** に進みます。
2. **[クイックアシスト]** をクリックします。
3. **[クイックアシスト]** ウィンドウで、エンドユーザーから受け取ったワークロードIDを入力し、**[接続]** を選択します。
4. **[接続]** をクリックします。
5. ワークロードでの接続クライアントインストールの有無に応じて、次のいずれかを実行します。
   - 接続クライアントがインストールされていない場合は、ダウンロードしてインストールし、表示される確認のポップアップで **[許可]** を選択します。
   - 接続クライアントが既にインストールされている場合は、表示される確認のポップアップで **[接続クライアントを開く]** をクリックします。
6. **[認証]** ウィンドウで、アクセスコードを入力します。
7. 接続クライアントで、リモートワークロードのデスクトップを表示できる新しいビューアウィンドウが開きます。ビューアには、リモート接続が確立された後にリモートワークロード上で実行できる、追加操作のためのツールバーがあります。詳細については、"ビューアウィンドウのツールバーを使用する"（991ページ）を参照してください。

IPアドレス経由で非管理対象のワークロードに接続する

非管理対象のワークロードがLAN内部に存在する場合、ワークロードのIPアドレスを使用してリモート制御またはリモートアシスタンスに接続できます。この接続には、インターネットアクセスは必要ありません。

前提条件

- Advanced Managementパックは、カスタマーテナントに割り当てられます。
- Acronis Cyber Protect Cloudで、ユーザーアカウントの二要素認証が有効化されます。

IPアドレスを使用してリモートデスクトップまたはリモートアシスタンスのワークロードに接続するには

1. Cyber Protectコンソールで **[すべてのデバイス]** に進みます。
2. **[クイックアシスト]** をクリックします。
3. **[IPアドレス経由]** タブをクリックします。
4. ワークロードのIPアドレスとポートを入力します。

5. リモートワークロードのオペレーティングシステムに応じて、RDP（Windowsワークロード）またはApple画面共有（macOSワークロード）の接続プロトコルを選択します。

   注意
   RDP経由の接続は、リモートデスクトップ動作をサポートしており、Apple画面共有経由での接続は、リモートデスクトップ動作とリモートアシスタンス動作の両方をサポートしています。

6. **[接続]** をクリックします。
7. **[認証]** ウィンドウで、必要な資格情報を入力します。

Apple画面共有接続の場合、接続クライアントで、リモートワークロードのデスクトップを表示できる新しいビューアウィンドウが開きます。ビューアには、リモート接続が確立された後にリモートワークロード上で実行できる、追加操作のためのツールバーがあります。詳細については、"ビューアウィンドウのツールバーを使用する"（991ページ）を参照してください。

Acronis クイックアシスト経由のファイル転送

クイックアシスト機能を使用して、ワークロードと非管理ワークロードの間でファイルを転送できます。

前提条件

- Advanced Managementパックは、カスタマーテナントに割り当てられます。
- Acronis Cyber Protect Cloudで、ユーザーアカウントの二要素認証が有効化されます。
- リモートユーザーがAcronis クイックアシストをダウンロードおよび実行しました。
- リモートユーザーは、クイックアシストからコンピューターIDおよびアクセスコードを提供されています。

クイックアシストを使用してワークロードにファイルを転送するには

1. Cyber Protectコンソールで **[デバイス]** > **[すべてのデバイス]** に進みます。
2. **[クイックアシスト]** をクリックします。
3. **[クイックアシスト]** ウィンドウで、エンドユーザーから受け取ったワークロードIDを入力し、**[ファイル転送]** を選択します。
4. **[接続]** をクリックします。
5. ワークロードでの接続クライアントインストールの有無に応じて、次のいずれかを実行します。
   - 接続クライアントがインストールされていない場合は、ダウンロードしてインストールし、表示される確認のポップアップで **[許可]** を選択します。
   - 接続クライアントが既にインストールされている場合は、表示される確認のポップアップで **[接続クライアントを開く]** をクリックします。
6. **[認証]** ウィンドウで、アクセスコードを入力します。
7. **[ファイル転送]** ウィンドウでファイルを参照し、任意の転送先にドラッグアンドドロップします。

注意

ローカルワークロードのファイルは左ペインに、リモートワークロードのファイルは右ペインに表示されます。

ファイル転送が開始されると、[**タスク**]ペインに表示されます。

8. （オプション） 完了したタスクを[**タスク**]ペインから削除するには、[**完了をクリア**] をクリックします。
9. すべての転送が完了したら、ウィンドウを閉じます。

ビューアウィンドウのツールバーを使用する

リモートワークロードに接続した後、ビューアウィンドウのツールバーを使用して、さまざまな操作を簡単に実行できます。

アイコン	説明
	**実際のサイズ** リモートワークロードのデスクトップの1ピクセルがビューアウィンドウの1ピクセルに対応するように、リモートワークロードのデスクトップをスケーリングします。
	**ズームしてフィット** リモートワークロードのデスクトップをビューアのウィンドウに合わせてスケーリングします。
	**ロック**および**画面のロックを解除** リモートワークロードのディスプレイにプレースホルダーを表示し、リモートユーザーから操作が見えないようにします。
	**スクリーンショットを取得** リモートサーバーのデスクトップイメージをローカルファイルに保存します。
	**ディスプレイを選択** 表示したいリモートワークロードのディスプレイと任意の解像度を選択します。 macOSへのApple画面共有接続、およびすべてのオペレーティングシステムへのNEAR接続で利用可能です。
	**イメージ品質** Apple画面共有接続時に、リモート画面のイメージ品質を白黒から最高画質まで調整します。
	**NEARイメージ品質**

アイコン	説明
	NEAR接続時の品質/性能比を調整します。スライダーを左側（スムーズ）にすると、リモートデスクトップ画面で画質よりもパフォーマンスが優先されます。右側（シャープ）にすると、画質は上がりますが、おそらくパフォーマンスが低下します。
	**Ctrl+Alt+Delを送信** Ctrl+Alt+Deleteのシーケンスをリモートワークロードに送信します。 WindowsおよびLinuxのワークロードで利用可能です。
	**ファイル転送** リモートとローカルのワークロード間でファイルを交換するための [ファイルマネージャー] ウィンドウを開きます。NEAR接続で利用可能です。
	**ピンツールバー** ビューアのツールバーが自動的に隠される設定をオフにします。 Windowsのワークロードで利用可能です。
	**全画面** 全画面モードに切り替わり、リモートのワークロードをローカル画面全体に拡張します。 Windowsのワークロードで利用可能です。
	**閉じる** ビューアウィンドウを閉じ、リモートコントロールセッションを終了します。 Windowsのワークロードで利用可能です。

接続のタイプによっては、**その他**アイコンをクリックすると、追加のオプションが利用できる場合があります。

オプション	説明
記録を開始/記録を停止	現在のリモートデスクトップセッションを記録します。 セッションの記録は.crecファイルとしてローカルワークロードに保存されます。.crecファイルはAcronis 接続クライアントで開くことができます。 NEAR接続で利用可能です
クリップボードの自動同期	このオプションをオンにすると、クライアントでローカルのクリップボードとリモートコンピューターのクリップボードが自動的に同期されます。

オプション	説明
	NEAR、Apple画面共有接続で利用可能です。
クリップボードを送信 **クリップボードを取得**	**クリップボードの送信**により、リモートコンピューターのクリップボードの内容をローカルのクリップボードの内容と置き換えます。 **クリップボードの取得**により、リモートコンピューターのクリップボードの内容をローカルのクリップボードに転送します。
スマートキーボード/物理キー/物理キー（すべてのショートカット付き）	現在の接続されているキーボードの入力モードを変更します。 **スマートキーボード** - クライアントにより、ローカルで入力した記号のUnicodeコードがリモートコンピューターに送信されます **物理キー** - クライアントで、押下されたキーボードのボタンのコードがそのまま使用されます。 **物理キー（すべてのショートカット付き）** - クライアントがローカルシステムのショートカットを無効にし、リモートオペレーティングシステムに送信されるようにします。
マウスホバーのキーボードフォーカス	この機能を有効にすると、ローカルマウスカーソルがビューアウィンドウ上に配置されている間、クライアントはキーボード入力のみをキャプチャするようになります。 無効の場合、クライアントでウィンドウがアクティブになると、キーボードがキャプチャされます。
接続情報を表示/接続情報を非表示	**[接続情報を表示]** を選択すると、リモートデスクトップ画面上に小さな情報パネルが表示され、現在の接続に関する最も重要な情報が表示されます。
リモート音声	クライアントがリモートコンピューターからローカルコンピューターに音声をリダイレクトできるようにします。 NEAR接続で利用可能です
システム環境設定	接続クライアントの設定を構成します。詳細については、"接続クライアント設定を構成する"（994ページ）を参照してください。

リモートセッションの記録と再生

Acronis 接続クライアントでNEAR経由のリモートセッションを記録できます。

リモートセッションを記録するには

1. 接続クライアントのビューアツールバーで **[その他]** をクリックし、**[記録を開始]** を選択します。
2. 記録の名前とロケーションを選択します。
   デフォルトでは、ファイル名は現在の日付と時刻になり、現在のユーザーのホームディレクトリにある **[文書]** フォルダに保存されます。記録が有効な場合、**[ビューア]** ツールバーでリモート画面の右上に点滅する赤い円と記録タイマーが表示されます。

3. 記録を停止するには、[**その他**] をクリックして [**記録を停止**] をクリックします。Macの場合は、ツールバーの [**停止**] をクリックすることもできます。

   Acronis 接続クライアントで作成されたすべての.crecファイルは、デフォルトでAcronis 接続クライアントにより開かれます。

記録を再生するには

1. 記録ファイルを探します。
2. そのファイルを開きます。

   Acronis 接続クライアントプレイヤーが開きます。記録内で移動できませんのでご注意ください。記録の特定の時点を見つけるには、プレーヤーがその時点に到達するまで待ちます。
3. （オプション） 再生速度は、再生コントロールセクションの[<<] アイコンと [>>] アイコンで調整します。

   記録は、接続中にリモートサーバーとの間で送受信されたイベントのシーケンスとして保管されます。このため、最小のファイルサイズで最高の記録品質を確保します。けれども、それと同時に記録内で移動することができないことになります。現時点では、記録をビデオ形式に変換することもできません。

接続クライアント設定を構成する

ワークロードに接続クライアントをインストールした後、任意の設定を構成できます。

接続クライアントの設定を構成するには

1. スタートメニューで、**接続クライアント**を見つけて起動します。
2. [**全般**] タブで設定を構成します。

オプション	説明
詳細ログを書き込み	接続クライアントで冗長なログの書き込みを許可する場合は、このオプションを選択します。無効にされている場合、クライアントは一般的な情報のみをログファイルに書き込みます。
プロキシ設定	デフォルトのシステムプロキシを使用するか、カスタムSOCKSSプロキシを構成するかを選択します。

3. [**ビューア**] タブで設定を構成します。

オプション	説明
ビューアを閉じる際の確認を求める	ビューアウィンドウが誤って閉じられてしまうことを防止するため、ビューアウィンドウを閉じようとしたときに接続クライアントに確認メッセージを表示させるには、このオプションを選択します。
最小化使用時	CPUの負荷を軽減するために、最小化時にビューアのアクティビティを停止させるかどうかを選択します。

オプション	説明
最大化使用時	最大化時にフルスクリーンモードを有効にするかどうかを選択します。
クリップボードを転送	テキストやイメージをコピーしたり貼り付けたりしたときに、ビューアウィンドウにクリップボード転送インジケータを表示するようにします。
キーボードモード	マウスとキーボードのイベントがリモートのマシンに送信されるたびに、ビューアウィンドウのタイトルに入力モードインジケータを表示するようにします。
クリップボード	利用できる場合にクリップボードの自動同期を有効化するには、[**クリップボードの自動同期を有効化**] を選択します。
キーボードイベントを送信	接続クライアントウィンドウがアクティブなときに常にローカルのキーボード入力を取得するか、またはローカルのマウスポインタがウィンドウ上にあるときのみそうするかを選択します。
ビューアのバックグラウンドカラー	ビューアウィンドウのバックグラウンドカラーを変更します。
自動的に再接続	接続が中断された場合に、の接続を自動的に再確立する場合は、[**自動再接続を有効化**] を選択します。
H.264	ハードウェアデコーダを無効化できます。
アイドル時に閉じる	ビューアのウィンドウを閉じるまでのアイドル状態の時間間隔を選択します。

4. [**キーボード**] タブで設定を構成します。

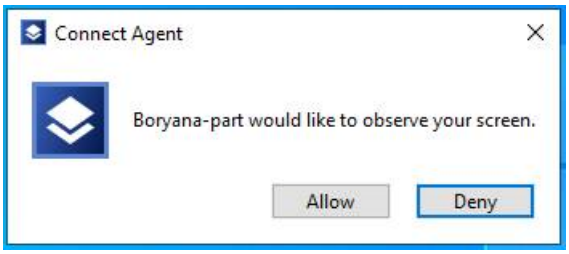
オプション	説明
修飾キーのマッピング	ポップアップメニューでの修飾キーの動作を変更します。これらの設定は、NEAR、Apple画面共有、RDP接続で別個に保存されます。
入力モード	接続の種類（ペインのヘッダーで選択済み）ごとに、デフォルトのキーボード入力モードを選択します。

5. [**OK**] をクリックします。

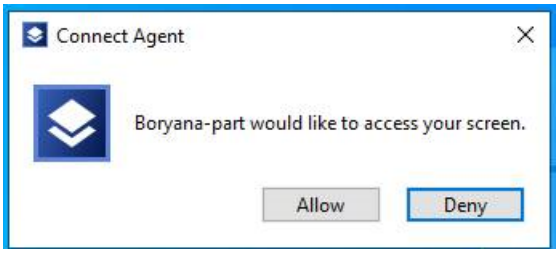
リモートデスクトップ通知

接続エージェントは、以下の場合にリモートワークロードのデスクトップに操作ダイアログ（通知）を表示します。

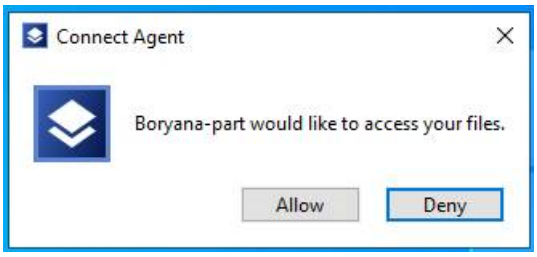
- リモートでワークロードに接続するため、観察の許可を求める場合。ローカルでリモートワークロードにログインしているユーザーは、リクエストを許可または拒否できます。



- リモートでワークロードに接続するため、制御の許可を求める場合。ローカルでリモートワークロードにログインしているユーザーは、リクエストを許可または拒否できます。



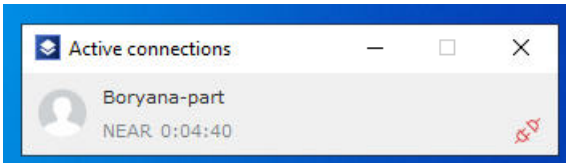
- 自分のワークロードとリモートのワークロードの間でファイルを交換するため、ファイル転送の許可を求める場合。ローカルでリモートワークロードにログインしているユーザーは、リクエストを許可または拒否できます。



ワークロードへのリモートデスクトップ接続が確立されると、ワークロードにログインしているユーザーに、次の情報を含む別の接続通知が表示されます。

- リモートで接続しているユーザー名
- リモート接続を確立するために使用される接続プロトコル
- リモート接続の期間

リモートワークロードにローカルでログインしているユーザーは、**切断**アイコンまたは**閉じる**アイコンをクリックして、いつでも接続を終了できます。



ワークロードのヘルス状態とパフォーマンスを監視する

組織内のシステムパラメータやワークロードのヘルス状態を監視できます。パラメータが基準値から外れている場合、すぐに通知され、問題を迅速に解決できます。また、カスタムアラートと自動対応操作を構成できます。これらは、ワークロードの異常な動作を解決するために自動的に実行される操作です。

注意
監視機能を利用するには、ワークロードに保護エージェントの15.0.35324以降のバージョンをインストールする必要があります。

計画の監視

管理対象のワークロードで、パフォーマンス、ハードウェア、ソフトウェア、システム、セキュリティパラメータの監視を開始するには、監視計画をワークロードに適用します。監視計画には、有効化および構成可能な各種のモニタが含まれています。一部のモニタでは、アノマリーベースの監視タイプがサポートされています。監視計画の詳細については、"計画の監視"（1027ページ）を参照してください。監視計画で構成できる利用可能なモニタの詳細については、"構成可能なモニタ"（998ページ）を参照してください。

エージェントが何らかの理由でワークロードからデータを収集できない場合、システムによりアラートが生成されます。

監視タイプ

計画で有効にする各モニタについて監視タイプを構成する必要があります。監視タイプは、モニタがワークロードの動作の正常性を判定するために使用するアルゴリズムを決定します。監視タイプには、しきい値ベースとアノマリベースの2種類があります。一部のモニタでは、しきい値ベースの監視タイプのみがサポートされています。

しきい値ベースの監視は、パラメータの値が、設定したしきい値を上回ったり、下回ったりする変化を追跡します。この監視タイプでは、ワークロードに対して正しいしきい値を定義する必要があります。システムは、これらの静的なしきい値に基づいて正常な動作を判断しますが、他の特定の条件がその動作を引き起こす可能性は考慮しません。そのため、しきい値ベースの監視は、アノマリベースの監視と比較して精度が劣る場合があります。

アノマリベース監視では、機械学習を利用して、ワークロードの正常な動作パターンを作成し、ワークロードの動作における異常を検出します。詳細については、"アノマリベースの監視"（997ページ）を参照してください。

アノマリベースの監視

アノマリベース監視では、機械学習技術を利用して、ワークロードの正常な動作パターンを作成し、ワークロードの動作における異常（時系列データにおける予期せぬスパイク）を検出します。この監視

タイプを有効化すると、システムにより基本モデルが作成され、ワークロードから収集されたデータに基づいて、トレーニングと特定のワークロードに対するモデルの調整が開始されます。そのためトレーニングが開始された当初は、データの精度が低い場合があります。信頼性の高いモデルを作成するには、最低でも3週間のモデルトレーニング期間が必要です。十分な量のデータが収集され過去のデータセットの分析が進むと、システムによるモデルの改良が行われます。その後ワークロードの各メトリクスに関する動的な上限および下限のしきい値が作成されます。この監視タイプでは、パラメータの値とその前後の状況が監視されます。それでしきい値ベースの監視に比べ、柔軟性に優れています。例えば、あるワークロードでは1日のうち特定の時間帯に負荷が大きくなる傾向にあり、これは正常な動作の範ちゅうかもしれません。しきい値ベースの監視タイプでは、これが異常な動作と誤認され、アラートが生成される可能性があります。

ワークロードの機械学習モデルは、リセットすることができます。この場合、ワークロードに適用されているモニタのデータおよびモデルはすべて削除されます。詳細については、"機械学習モデルをリセットする"（1036ページ）を参照してください。

監視でサポートされるプラットフォーム

監視機能は、以下のオペレーティングシステムをサポートしています。

サポートされるWindowsのバージョン	サポートされるmacOSのバージョン
• Windows 7 SP1 • Windows 8, 8.1 • Windows 10 • Windows 11 • Windows Server 2008 R2 • Windows Server 2012 • Windows Server 2012 R2 • Windows Server 2016 • Windows Server 2019 • Windows Server 2022	• macOS 10.14 (Mojave) • macOS 10.15 (Catalina) • macOS 11.x（Big Sur） • macOS 12.x（Monterey） • macOS 13.x（Ventura）

構成可能なモニタ

監視機能は、以下のモニタ（6種類のカテゴリ）をサポートしています:ハードウェア、パフォーマンス、ソフトウェア、システム、セキュリティ、カスタム。

モニタ	説明	サポートされるオペレーティング システム	データ収集の間隔	アノマリベース監視のサポート	Standard保護またはAdvanced Managementにおける可用性
ハードウェア					
ディスク容	ワークロード上で特定のドライ	Windows	1分	はい	Standard

モニタ	説明	サポートされるオペレーティング システム	データ収集の間隔	アノマリベース監視のサポート	Standard保護またはAdvanced Managementにおける可用性
量	ブの空き容量を監視します。	macOS			Protection
CPU温度	CPU温度を監視します。	Windows macOS	30秒	はい	Advanced管理
GPU温度	GPU温度を監視します。	Windows macOS	30秒	はい	Advanced管理
ハードウェアの変更	ワークロードのハードウェアの追加、削除、交換など、ハードウェアの変更を監視します。	Windows macOS	24時間	いいえ	Standard Protection
パフォーマンス					
CPU使用状況	全体のCPU使用状況（ワークロード上のすべてのCPUごと）を監視します。	Windows macOS	30秒	はい	Advanced管理
メモリ使用状況	全体のメモリ使用状況（ワークロード上のすべてのメモリスロットごと）を監視します。	Windows macOS	30秒	はい	Advanced管理
ディスク転送速度	ワークロード上の各物理ディスクの読み取り/書き込み速度を監視します。	Windows macOS	30秒	はい	Advanced管理
ネットワーク使用率	ワークロード上の各ネットワークアダプタの送受信トラフィックを監視します。	Windows macOS	30秒	はい	Advanced管理
プロセス別のCPU使用状況	特定のプロセスによるCPU使用状況を監視します。	Windows macOS	30秒	いいえ	Advanced管理
プロセス別のメモリ使用状況	選択されたプロセスのメモリ使用状況を監視します。	Windows macOS	30秒	いいえ	Advanced管理
プロセス別のディスク転送速度	選択したプロセスの読み取り/書き込み速度を監視します。	Windows macOS	30秒	いいえ	Advanced管理
プロセス別のネットワーク使用	選択したプロセスの送受信トラフィックを監視します。	Windows macOS	30秒	いいえ	Advanced管理

モニタ	説明	サポートされるオペレーティング システム	データ収集の間隔	アノマリベース監視のサポート	Standard保護またはAdvanced Managementにおける可用性
状況					
ソフトウェア					
Windows サービスのステータス	選択したWindowsサービスのステータス（実行中/停止済み）を監視します。	Windows	30秒	いいえ	Advanced管理
プロセスのステータス	選択しプロセスのステータス（実行中/停止済み）を監視します。	Windows macOS	30秒	いいえ	Advanced管理
インストール済みソフトウェア	ソフトウェアアプリケーションのインストール、アップデート、削除を監視します。	Windows macOS	24時間	いいえ	Advanced管理
システム					
前回のシステム再起動	ワークロードの再起動のタイミングを監視します。	Windows macOS	1時間	いいえ	Standard Protection
Windowsイベントログ	Windowsのイベントログに含まれる特定のビジネスクリティカルなイベントを監視します。	Windows	10分	いいえ	Advanced管理
ファイルとフォルダのサイズ	選択したファイルやフォルダの合計サイズを監視します。	Windows macOS	10分	いいえ	Standard Protection
セキュリティ					
Windows アップデートのステータス	ワークロードのWindows Updateのステータスを監視し、最新のアップデートプログラムがインストールされているかどうかを監視します。	Windows	15分	いいえ	Advanced管理
ファイアウォールのステータス	ワークロードにインストールされている組み込みまたはサードパーティのファイアウォールのステータスを監視します。	Windows macOS	5分	いいえ	Advanced管理
マルウェア対策ソフトウェアのス	ワークロードにインストールされている組み込みまたはサードパーティのマルウェア対策ソフ	Windows macOS	5分	いいえ	Advanced管理

モニタ	説明	サポートされるオペレーティング システム	データ収集の間隔	アノマリベース監視のサポート	Standard保護またはAdvanced Managementにおける可用性
テータス	トウェアのステータスを監視します。				
ログイン失敗	ワークロードのログイン試行失敗を監視します。	Windows	1時間	いいえ	Advanced管理
AutoRunのステータス	リムーバブルストレージメディアのAutoRun機能が有効かどうかを監視します。	Windows	1時間	いいえ	Advanced管理
カスタム					
カスタム	スクリプトの実行により、カスタムオブジェクトを監視します。	Windows macOS	カスタム	いいえ	Advanced管理

ディスク容量モニタを設定する

ディスク容量により、ワークロード上で特定のドライブの空き容量を監視します。

注意
この領域を計算する場合、モニタではWindowsおよびmacOSワークロードでは、バイナリバイト（1024バイト=1KB、1024KB=1MB、1024MB=1GB）が使用されます。

モニタに、次の設定を構成できます。

設定	説明
しきい値ベースの監視	
ドライブ	監視するドライブです。 次の値を使用できます。 • **システムドライブ** -これはデフォルト値です。 • **いずれかのドライブ**
演算子	演算子は、メトリクスのパフォーマンスをどのように測定するかを定義する条件付きの関数です。 次の値を使用できます。 • **未満** - これはデフォルト値です。 • **以下**
ディスク	しきい値と**演算子**により、監視対象のメトリクスの正常なパフォーマンスが判定され

設定	説明
空き容量しきい値	ます。監視対象のメトリクスの値が基準値から逸脱した場合、システムによりアラートが生成されます。 1～100（%）の範囲で整数値を入力します。デフォルト値は20です。
リムーバブルドライブを含める	この設定は、**ドライブ**の値が**いずれかのドライブ**の場合に有効です。 USBフラッシュドライブなどのリムーバブルドライブを監視対象として追加する場合は、この設定を選択します。デフォルトでは、設定は無効化されています。
期間	指定された期間中にメトリクスの値が通常範囲外の場合にのみ、検出された問題に対してシステムによりアラートが生成されます。 1～60（分）の範囲で整数値を入力します。デフォルト値は30です。
アノマリベースの監視	
ドライブ	監視するドライブです。 次の値を使用できます。 • **システムドライブ** -これはデフォルト値です。 • **いずれかのドライブ**
モデルトレーニング期間	エージェントから収集されたデータを基にシステムが機械学習モデルを学習し、ワークロードの正常な動作パターンを作成する期間です。モデルのトレーニング期間が長ければ長いほど、システムが作成する長期的な動作パターンはより正確になります。モデルのトレーニング期間として最低21日間を推奨します。 整数値（日）を入力します。デフォルト値は21です。
トレーニング期間中に異常アラートを受信	この設定を選択すると、モデルのトレーニング期間中に異常が検出された場合にアラートが送信されます。モデルのトレーニングがまだ進行中であり、十分に正確ではない可能性があるため、これらのアラートは偽陽性の場合があります。 デフォルトで、設定は選択されています。
感度レベル	感度レベルは、異常値が特定の範囲内にある場合に、事前フィルタとして機能します。このフィルタは、異常検出アルゴリズムとは独立して動作します。この目的は、指定された範囲内にある異常が、異常検出アルゴリズムによって処理されないようにすることです。 トレーニング期間中: 1. トレーニング中に収集されたデータを使用して、アルゴリズムのトレーニングが実行されます。 2. アルゴリズムにより、トレーニングデータに対する異常検出が実行されます。 3. 平均値と標準偏差に基づくフィルタリング処理が適用されます。 4. 指定された範囲内にあるすべての異常はフィルタリングされます。 5. 残った異常データポイントから、レベルが最も低い異常が選択されます。このレベル（0から1の浮動小数点数）はモデルに記録されます。

設定	説明
	予測の実行中: 1. アルゴリズムにより、推定データ上で異常が予測されます。 2. 予測された異常は、感度レベルに基づいて平均値と標準偏差でフィルタリングされます。 3. 残りの異常は、しきい値を超える値は異常と見なし、しきい値以下の値は正常な動作と見なすという原則に基づいてさらにフィルタリングされます 次の値を使用できます。 • **低** - 低レベルは、平均値および標準偏差の値に相当します。 • **通常** - これはデフォルト値です。通常レベルは、平均値と標準偏差の2倍の値に相当します。 • **高** - 高レベルは、平均値と標準偏差の値の3倍に相当します。
異常が発生している期間	指定された期間異常動作が継続した場合のみ、検出された異常に対してアラートを生成します。 デフォルト値は30分です。

CPU温度モニタの設定

CPU温度は、ワークロードのCPU温度を監視します。

モニタに、次の設定を構成できます。

設定	説明
しきい値ベースの監視	
CPU温度が超過しました（C°）	監視対象のメトリクスの上限値です。この値を超えた場合、アラートが生成されます。 整数値（°C）を入力します。デフォルト値は80です。
期間	指定された期間中にメトリクスの値が通常範囲外の場合にのみ、検出された問題に対してシステムによりアラートが生成されます。 1～60（分）の範囲で整数値を入力します。デフォルト値は5です。
アノマリベースの監視	
モデルトレーニング期間	エージェントから収集されたデータを基にシステムが機械学習モデルを学習し、ワークロードの正常な動作パターンを作成する期間です。モデルのトレーニング期間が長ければ長いほど、システムが作成する長期的な動作パターンはより正確になります。モデルのトレーニング期間として最低21日間を推奨します。 整数値（日）を入力します。デフォルト値は21です。

設定	説明
感度レベル	感度レベルは、異常値が特定の範囲内にある場合に、事前フィルタとして機能します。このフィルタは、異常検出アルゴリズムとは独立して動作します。この目的は、指定された範囲内にある異常が、異常検出アルゴリズムによって処理されないようにすることです。 トレーニング期間中: 1. トレーニング中に収集されたデータを使用して、アルゴリズムのトレーニングが実行されます。 2. アルゴリズムにより、トレーニングデータに対する異常検出が実行されます。 3. 平均値と標準偏差に基づくフィルタリング処理が適用されます。 4. 指定された範囲内にあるすべての異常はフィルタリングされます。 5. 残った異常データポイントから、レベルが最も低い異常が選択されます。このレベル（0から1の浮動小数点数）はモデルに記録されます。 予測の実行中: 1. アルゴリズムにより、推定データ上で異常が予測されます。 2. 予測された異常は、感度レベルに基づいて平均値と標準偏差でフィルタリングされます。 3. 残りの異常は、しきい値を超える値は異常と見なし、しきい値以下の値は正常な動作と見なすという原則に基づいてさらにフィルタリングされます 次の値を使用できます。 • **低** - 低レベルは、平均値および標準偏差の値に相当します。 • **通常** - これはデフォルト値です。通常レベルは、平均値と標準偏差の2倍の値に相当します。 • **高** - 高レベルは、平均値と標準偏差の値の3倍に相当します。
異常が発生している期間	指定された期間異常動作が継続した場合のみ、検出された異常に対してアラートを生成します。 1～60（分）の範囲で整数値を入力します。デフォルト値は15です。

GPU温度モニタを設定する

GPU温度により、ワークロードのGPU温度を監視します。

モニタに、次の設定を構成できます。

設定	説明
しきい値ベースの監視	
GPU温度が超過しました	監視対象のメトリクスの上限値です。この値を超えた場合、システムにより異常が検知されます。 整数値（°C）を入力します。デフォルト値は80です。
期間	指定された期間中にメトリクスの値が通常範囲外の場合にのみ、検出された問題に対してシステムによりアラートが生成されます。 1～60（分）の範囲で整数値を入力します。デフォルト値は5です。
アノマリベースの監視	
モデルトレーニング期間	エージェントから収集されたデータを基にシステムが機械学習モデルを学習し、ワークロードの正常な動作パターンを作成する期間です。モデルのトレーニング期間が長ければ長いほど、システムが作成する長期的な動作パターンはより正確になります。モデルのトレーニング期間として最低21日間を推奨します。 整数値（日）を入力します。デフォルト値は21です。
感度レベル	感度レベルは、異常値が特定の範囲内にある場合に、事前フィルタとして機能します。このフィルタは、異常検出アルゴリズムとは独立して動作します。この目的は、指定された範囲内にある異常が、異常検出アルゴリズムによって処理されないようにすることです。 トレーニング期間中: 1. トレーニング中に収集されたデータを使用して、アルゴリズムのトレーニングが実行されます。 2. アルゴリズムにより、トレーニングデータに対する異常検出が実行されます。 3. 平均値と標準偏差に基づくフィルタリング処理が適用されます。 4. 指定された範囲内にあるすべての異常はフィルタリングされます。 5. 残った異常データポイントから、レベルが最も低い異常が選択されます。このレベル（0から1の浮動小数点数）はモデルに記録されます。 予測の実行中: 1. アルゴリズムにより、推定データ上で異常が予測されます。 2. 予測された異常は、感度レベルに基づいて平均値と標準偏差でフィルタリングされます。 3. 残りの異常は、しきい値を超える値は異常と見なし、しきい値以下の値は正常な動作と見なすという原則に基づいてさらにフィルタリングされます 次の値を使用できます。 • **低** - 低レベルは、平均値および標準偏差の値に相当します。 • **通常** - これはデフォルト値です。通常レベルは、平均値と標準偏差の2倍の値に相当します。 • **高** - 高レベルは、平均値と標準偏差の値の3倍に相当します。

設定	説明
異常が発生している期間	指定された期間異常動作が継続した場合のみ、検出された異常に対してアラートを生成します。 1～60（分）の範囲で整数値を入力します。デフォルト値は15です。

ハードウェアの変更モニタを設定する

ハードウェアの変更により、ワークロードのハードウェアの追加、削除、交換など、ハードウェアの変更を監視します。

モニタに、次の設定を構成できます。

設定	説明
ハードウェアコンポーネント	変更を監視したいハードウェアコンポーネントを1つまたは複数選択します。 次の値を使用できます。 • **すべて** - これはデフォルト値です。 • **マザーボード** • **CPU** • **RAM** • **ディスク** • **GPU** • **ネットワークアダプタ**
監視の対象	選択したハードウェアコンポーネントの監視したい変更内容を指定します。リストから複数の項目を選択できます。 次の値を使用できます。 • **すべての変更** -これはデフォルト値です。 • **新しく追加済みのコンポーネント** • **交換済みコンポーネント** • **削除済みコンポーネント**

CPU使用状況モニタの設定

CPU使用状況モニタは、ワークロードの合計CPU使用率（プロセッサ使用率）を監視します。もしワークロードに複数のCPUがある場合、合計CPU使用率は各CPU使用率の合計になります。

モニタに、次の設定を構成できます。

設定	説明
しきい値ベースの監視	
演算子	演算子は、メトリクスのパフォーマンスをどのように測定するかを定義する条件付き

設定	説明
	の関数です。 次の値を使用できます。 • **を上回る** -これはデフォルト値です。 • **以上** • **未満** • **以下**
CPU使用状況のしきい値	しきい値と**演算子**により、監視対象のメトリクスの正常なパフォーマンスが判定されます。監視対象のメトリクスの値が基準値から逸脱した場合、システムによりアラートが生成されます。 1～100（%）の範囲で整数値を入力します。デフォルト値は90です。
期間	指定された期間中にメトリクスの値が通常範囲外の場合にのみ、検出された問題に対してシステムによりアラートが生成されます。 1～60（分）の範囲で整数値を入力します。デフォルト値は5です。
アノマリベースの監視	
モデルトレーニング期間	エージェントから収集されたデータを基にシステムが機械学習モデルを学習し、ワークロードの正常な動作パターンを作成する期間です。モデルのトレーニング期間が長ければ長いほど、システムが作成する長期的な動作パターンはより正確になります。モデルのトレーニング期間として最低21日間を推奨します。 整数値（日）を入力します。デフォルト値は21です。
トレーニング期間中に異常アラートを受信	この設定を選択すると、モデルのトレーニング期間中に異常が検出された場合にアラートが送信されます。モデルのトレーニングがまだ進行中であり、十分に正確ではない可能性があるため、これらのアラートは偽陽性の場合があります。 デフォルトで、設定は選択されています。
感度レベル	感度レベルは、異常値が特定の範囲内にある場合に、事前フィルタとして機能します。このフィルタは、異常検出アルゴリズムとは独立して動作します。この目的は、指定された範囲内にある異常が、異常検出アルゴリズムによって処理されないようにすることです。 トレーニング期間中: 1. トレーニング中に収集されたデータを使用して、アルゴリズムのトレーニングが実行されます。 2. アルゴリズムにより、トレーニングデータに対する異常検出が実行されます。 3. 平均値と標準偏差に基づくフィルタリング処理が適用されます。 4. 指定された範囲内にあるすべての異常はフィルタリングされます。 5. 残った異常データポイントから、レベルが最も低い異常が選択されます。このレベル（0から1の浮動小数点数）はモデルに記録されます。 予測の実行中:

設定	説明
	1. アルゴリズムにより、推定データ上で異常が予測されます。 2. 予測された異常は、感度レベルに基づいて平均値と標準偏差でフィルタリングされます。 3. 残りの異常は、しきい値を超える値は異常と見なし、しきい値以下の値は正常な動作と見なすという原則に基づいてさらにフィルタリングされます 次の値を使用できます。 • **低** - 低レベルは、平均値および標準偏差の値に相当します。 • **通常** - これはデフォルト値です。通常レベルは、平均値と標準偏差の2倍の値に相当します。 • **高** - 高レベルは、平均値と標準偏差の値の3倍に相当します。
異常が発生している期間	指定された期間異常動作が継続した場合のみ、検出された異常に対してアラートを生成します。 1～60（分）の範囲で整数値を入力します。デフォルト値は15です。

メモリ使用状況モニタを設定する

メモリ使用状況により、ワークロードのすべてのメモリモジュールによる合計メモリ使用量を監視します。

モニタに、次の設定を構成できます。

設定	説明
しきい値ベースの監視	
演算子	演算子は、メトリクスのパフォーマンスをどのように測定するかを定義する条件付きの関数です。 次の値を使用できます。 • **を上回る** -これはデフォルト値です。 • **以上** • **未満** • **以下**
メモリ使用状況のしきい値	しきい値と**演算子**により、監視対象のメトリクスの正常なパフォーマンスが判定されます。監視対象のメトリクスの値が基準値から逸脱した場合、システムによりアラートが生成されます。 1～100（%）の範囲で整数値を入力します。デフォルト値は90です。
期間	指定された期間中にメトリクスの値が通常範囲外の場合にのみ、検出された問題に対してシステムによりアラートが生成されます。 1～60（分）の範囲で整数値を入力します。デフォルト値は5です。

設定	説明
アノマリベースの監視	
モデルトレーニング期間	エージェントから収集されたデータを基にシステムが機械学習モデルを学習し、ワークロードの正常な動作パターンを作成する期間です。モデルのトレーニング期間が長ければ長いほど、システムが作成する長期的な動作パターンはより正確になります。モデルのトレーニング期間として最低21日間を推奨します。 整数値（日）を入力します。デフォルト値は21です。
トレーニング期間中に異常アラートを受信	この設定を選択すると、モデルのトレーニング期間中に異常が検出された場合にアラートが送信されます。モデルのトレーニングがまだ進行中であり、十分に正確ではない可能性があるため、これらのアラートは偽陽性の場合があります。 デフォルトで、設定は選択されています。
感度レベル	感度レベルは、異常値が特定の範囲内にある場合に、事前フィルタとして機能します。このフィルタは、異常検出アルゴリズムとは独立して動作します。この目的は、指定された範囲内にある異常が、異常検出アルゴリズムによって処理されないようにすることです。 トレーニング期間中: 1. トレーニング中に収集されたデータを使用して、アルゴリズムのトレーニングが実行されます。 2. アルゴリズムにより、トレーニングデータに対する異常検出が実行されます。 3. 平均値と標準偏差に基づくフィルタリング処理が適用されます。 4. 指定された範囲内にあるすべての異常はフィルタリングされます。 5. 残った異常データポイントから、レベルが最も低い異常が選択されます。このレベル（0から1の浮動小数点数）はモデルに記録されます。 予測の実行中: 1. アルゴリズムにより、推定データ上で異常が予測されます。 2. 予測された異常は、感度レベルに基づいて平均値と標準偏差でフィルタリングされます。 3. 残りの異常は、しきい値を超える値は異常と見なし、しきい値以下の値は正常な動作と見なすという原則に基づいてさらにフィルタリングされます 次の値を使用できます。 • **低** - 低レベルは、平均値および標準偏差の値に相当します。 • **通常** - これはデフォルト値です。通常レベルは、平均値と標準偏差の2倍の値に相当します。 • **高** - 高レベルは、平均値と標準偏差の値の3倍に相当します。
異常が発生している期間	指定された期間異常動作が継続した場合のみ、検出された異常に対してアラートを生成します。 1～60（分）の範囲で整数値を入力します。デフォルト値は30分です。

ディスク転送速度を設定する

ディスク転送速度により、ワークロード上の各物理ディスクの読み取り/書き込み速度を監視します。

モニタに、次の設定を構成できます。

設定	説明
しきい値ベースの監視	
監視の対象	監視する速度を選択します。 次の値を使用できます。 • **読み込み速度、書き込み速度**。これはデフォルト値です。 • **読み込み速度** • **書き込み速度**
読み込み速度の演算子	演算子は、メトリクスのパフォーマンスをどのように測定するかを定義する条件付きの関数です。 次の値を使用できます。 • **を上回る**。これはデフォルト値です。 • **以上** • **未満** • **以下**
読み込み速度のしきい値	しきい値と**演算子**により、監視対象のメトリクスの正常なパフォーマンスが判定されます。監視対象のメトリクスの値が基準値から逸脱した場合、システムによりアラートが生成されます。 整数値（kb/s）を入力します。デフォルト値は0kb/sです。
読み込み速度の期間	指定された期間中にメトリクスの値が通常範囲外の場合にのみ、検出された問題に対してシステムによりアラートが生成されます。 1～60（分）の範囲で整数値を入力します。デフォルト値は5です。
書き込み速度の演算子	演算子は、メトリクスのパフォーマンスをどのように測定するかを定義する条件付きの関数です。 次の値を使用できます。 • **を上回る** -これはデフォルト値です。 • **以上** • **未満** • **以下**
書き込み速度のしきい値	しきい値と**演算子**により、監視対象のメトリクスの正常なパフォーマンスが判定されます。監視対象のメトリクスの値が基準値から逸脱した場合、システムによりアラートが生成されます。

設定	説明
	整数値（kb/s）を入力します。デフォルト値は0kb/sです。
書き込み速度の期間	指定された期間中にメトリクスの値が通常範囲外の場合にのみ、検出された問題に対してシステムによりアラートが生成されます。 1～60（分）の範囲で整数値を入力します。デフォルト値は5です。
アノマリベースの監視	
モデルトレーニング期間	エージェントから収集されたデータを基にシステムが機械学習モデルを学習し、ワークロードの正常な動作パターンを作成する期間です。モデルのトレーニング期間が長ければ長いほど、システムが作成する長期的な動作パターンはより正確になります。モデルのトレーニング期間として最低21日間を推奨します。 整数値（日）を入力します。デフォルト値は21です。
トレーニング期間中に異常アラートを受信	この設定を選択すると、モデルのトレーニング期間中に異常が検出された場合にアラートが送信されます。モデルのトレーニングがまだ進行中であり、十分に正確ではない可能性があるため、これらのアラートは偽陽性の場合があります。 デフォルトで、設定は選択されています。
監視の対象	監視する速度を選択します。 次の値を使用できます。 • **読み込み速度、書き込み速度**。これはデフォルト値です。 • **読み込み速度** • **書き込み速度**
感度レベル	感度レベルは、異常値が特定の範囲内にある場合に、事前フィルタとして機能します。このフィルタは、異常検出アルゴリズムとは独立して動作します。この目的は、指定された範囲内にある異常が、異常検出アルゴリズムによって処理されないようにすることです。 トレーニング期間中: 1. トレーニング中に収集されたデータを使用して、アルゴリズムのトレーニングが実行されます。 2. アルゴリズムにより、トレーニングデータに対する異常検出が実行されます。 3. 平均値と標準偏差に基づくフィルタリング処理が適用されます。 4. 指定された範囲内にあるすべての異常はフィルタリングされます。 5. 残った異常データポイントから、レベルが最も低い異常が選択されます。このレベル（0から1の浮動小数点数）はモデルに記録されます。 予測の実行中: 1. アルゴリズムにより、推定データ上で異常が予測されます。 2. 予測された異常は、感度レベルに基づいて平均値と標準偏差でフィルタリングされます。 3. 残りの異常は、しきい値を超える値は異常と見なし、しきい値以下の値は正常な

設定	説明
	動作と見なすという原則に基づいてさらにフィルタリングされます 次の値を使用できます。 • **低** - 低レベルは、平均値および標準偏差の値に相当します。 • **通常** - これはデフォルト値です。通常レベルは、平均値と標準偏差の2倍の値に相当します。 • **高** - 高レベルは、平均値と標準偏差の値の3倍に相当します。
異常が発生している期間（読み込み速度）	指定された期間異常動作が継続した場合のみ、検出された異常に対してアラートを生成します。 1～60（分）の範囲で整数値を入力します。 デフォルト値は25です。
異常が発生している期間（書き込み速度）	指定された期間異常動作が継続した場合のみ、検出された異常に対してアラートを生成します。 1～60（分）の範囲で整数値を入力します。 デフォルト値は25です。

ネットワーク使用状況モニタを設定する

ネットワーク使用率により、ワークロード上の各ネットワークアダプタの送受信トラフィックを監視します。

モニタに、次の設定を構成できます。

設定	説明
しきい値ベースの監視	
トラフィックの方向	監視するトラフィックの方向です。 次の値を使用できます。 • **受信トラフィックと送信トラフィック**。これはデフォルト値です。 • **受信トラフィック** • **送信トラフィック**
受信トラフィックの演算子	演算子は、メトリクスのパフォーマンスをどのように測定するかを定義する条件付きの関数です。 次の値を使用できます。 • **を上回る** -これはデフォルト値です。 • **以上** • **未満** • **以下**

設定	説明
受信トラフィックのしきい値	しきい値と**演算子**により、監視対象のメトリクスの正常なパフォーマンスが判定されます。監視対象のメトリクスの値が基準値から逸脱した場合、システムによりアラートが生成されます。 整数値（kb/s）を入力します。デフォルト値は0kb/sです。
受信トラフィックの期間	指定された期間中にメトリクスの値が通常範囲外の場合にのみ、検出された問題に対してシステムによりアラートが生成されます。 1～60（分）の範囲で整数値を入力します。デフォルト値は5です。
送信トラフィックの演算子	演算子は、メトリクスのパフォーマンスをどのように測定するかを定義する条件付きの関数です。 次の値を使用できます。 • **を上回る** -これはデフォルト値です。 • **以上** • **未満** • **以下**
送信トラフィックのしきい値	しきい値と**演算子**により、監視対象のメトリクスの正常なパフォーマンスが判定されます。監視対象のメトリクスの値が基準値から逸脱した場合、システムによりアラートが生成されます。 整数値（kb/s）を入力します。デフォルト値は0kb/sです。
送信トラフィックの期間	しきい値と**演算子**により、監視対象のメトリクスの正常なパフォーマンスが判定されます。監視対象のメトリクスの値が基準値から逸脱した場合、システムによりアラートが生成されます。 1～60（分）の範囲で整数値を入力します。デフォルト値は5です。
アノマリベースの監視	
モデルトレーニング期間	エージェントから収集されたデータを基にシステムが機械学習モデルを学習し、ワークロードの正常な動作パターンを作成する期間です。モデルのトレーニング期間が長ければ長いほど、システムが作成する長期的な動作パターンはより正確になります。モデルのトレーニング期間として最低21日間を推奨します。 整数値（日）を入力します。デフォルト値は21です。
トレーニング期間中に異常アラートを受信	この設定を選択すると、モデルのトレーニング期間中に異常が検出された場合にアラートが送信されます。モデルのトレーニングがまだ進行中であり、十分に正確ではない可能性があるため、これらのアラートは偽陽性の場合があります。 デフォルトで、設定は選択されています。
トラフィックの方向	• **受信トラフィックと送信トラフィック**。これはデフォルト値です。 • **受信トラフィック** • **送信トラフィック**

設定	説明
感度レベル	感度レベルは、異常値が特定の範囲内にある場合に、事前フィルタとして機能します。このフィルタは、異常検出アルゴリズムとは独立して動作します。この目的は、指定された範囲内にある異常が、異常検出アルゴリズムによって処理されないようにすることです。 トレーニング期間中: 1. トレーニング中に収集されたデータを使用して、アルゴリズムのトレーニングが実行されます。 2. アルゴリズムにより、トレーニングデータに対する異常検出が実行されます。 3. 平均値と標準偏差に基づくフィルタリング処理が適用されます。 4. 指定された範囲内にあるすべての異常はフィルタリングされます。 5. 残った異常データポイントから、レベルが最も低い異常が選択されます。このレベル（0から1の浮動小数点数）はモデルに記録されます。 予測の実行中: 1. アルゴリズムにより、推定データ上で異常が予測されます。 2. 予測された異常は、感度レベルに基づいて平均値と標準偏差でフィルタリングされます。 3. 残りの異常は、しきい値を超える値は異常と見なし、しきい値以下の値は正常な動作と見なすという原則に基づいてさらにフィルタリングされます 次の値を使用できます。 • **低** - 低レベルは、平均値および標準偏差の値に相当します。 • **通常** - これはデフォルト値です。通常レベルは、平均値と標準偏差の2倍の値に相当します。 • **高** - 高レベルは、平均値と標準偏差の値の3倍に相当します。
異常が発生している期間（受信）	指定された期間異常動作が継続した場合のみ、検出された異常に対してアラートを生成します。 1～60（分）の範囲で整数値を入力します。 デフォルト値は25です。
異常が発生している期間（送信）	指定された期間異常動作が継続した場合のみ、検出された異常に対してアラートを生成します。 1～60（分）の範囲で整数値を入力します。 デフォルト値は25です。

プロセス別のCPU使用状況モニタの設定

プロセス別のCPU使用状況は、選択されたプロセスのCPU使用状況を監視します。もし同じプロセスの複数のインスタンスがある場合、システムはすべてのプロセスインスタンスの合計使用量を監視し、条件が満たされた場合にアラートを生成します。

モニタに、次の設定を構成できます。

設定	説明
プロセス名	監視するプロセスの名前です。拡張子を除いたプロセス名を入力します。
演算子	演算子は、メトリクスのパフォーマンスをどのように測定するかを定義する条件付きの関数です。 次の値を使用できます。 • **を上回る** -これはデフォルト値です。 • **以上** • **未満** • **以下**
しきい値	しきい値と**演算子**により、監視対象のメトリクスの正常なパフォーマンスが判定されます。監視対象のメトリクスの値が基準値から逸脱した場合、システムによりアラートが生成されます。 1～100（%）の範囲で整数値を入力します。デフォルト値は90です。
期間	指定された期間中にメトリクスの値が通常範囲外の場合にのみ、検出された問題に対してシステムによりアラートが生成されます。 1～60（分）の範囲で整数値を入力します。デフォルト値は5です。

プロセスモニタでメモリ使用状況を設定する

プロセス別のメモリ使用状況により、選択されたプロセスのメモリ使用状況を監視します。もし同じプロセスの複数のインスタンスがある場合、システムはすべてのプロセスインスタンスの合計使用量を監視し、条件が満たされた場合にアラートを生成します。

注意
エージェントは、プロセスのワーキングセット（プライベートおよび共有）の合計から、プロセスごとのメモリ使用量の大きさを推定します。そのため、ウィジェットで表示するサイズと、Windowsタスクマネージャ（プライベートワーキングセット）で表示されるメモリ使用量のサイズが異なる場合があります。

モニタに、次の設定を構成できます。

設定	説明
プロセス名	監視するプロセスの名前です。拡張子を除いたプロセス名を入力します。
演算子	演算子は、メトリクスのパフォーマンスをどのように測定するかを定義する条件付きの関数です。 次の値を使用できます。

設定	説明
	• **を上回る** -これはデフォルト値です。 • **以上** • **未満** • **以下**
しきい値	しきい値と**演算子**により、監視対象のメトリクスの正常なパフォーマンスが判定されます。監視対象のメトリクスの値が基準値から逸脱した場合、システムによりアラートが生成されます。 整数値（kb）を入力します。デフォルト値は1です。
期間	指定された期間中にメトリクスの値が通常範囲外の場合にのみ、検出された問題に対してシステムによりアラートが生成されます。 1～60（分）の範囲で整数値を入力します。デフォルト値は5です。

プロセスモニタ別にディスク転送速度を設定する

プロセスモニタ別のディスク転送速度により、選択したプロセスの読み取り/書き込み速度を監視します。もし同じプロセスの複数のインスタンスがある場合、システムはすべてのプロセスインスタンスの合計使用量を監視し、条件が満たされた場合にアラートを生成します。

モニタに、次の設定を構成できます。

設定	説明
プロセス名	監視するプロセスの名前です。拡張子を除いたプロセス名を入力します。
監視の対象	監視する速度です。 次の値を使用できます。 • **読み込み速度、書き込み速度**。これはデフォルト値です。 • **読み込み速度** • **書き込み速度**
読み込み速度の演算子	演算子は、メトリクスのパフォーマンスをどのように測定するかを定義する条件付きの関数です。 次の値を使用できます。 • **を上回る** -これはデフォルト値です。 • **以上** • **未満** • **以下**
読み込み速度のしきい値	しきい値と**演算子**により、監視対象のメトリクスの正常なパフォーマンスが判定されます。監視対象のメトリクスの値が基準値から逸脱した場合、システムによりアラートが生成されます。

設定	説明
	整数値（kb/s）を入力します。デフォルト値は0kb/sです。
読み込み速度の期間	指定された期間中にメトリクスの値が通常範囲外の場合にのみ、検出された問題に対してシステムによりアラートが生成されます。 1～60（分）の範囲で整数値を入力します。デフォルト値は5です。
書き込み速度の演算子	演算子は、メトリクスのパフォーマンスをどのように測定するかを定義する条件付きの関数です。 次の値を使用できます。 • **を上回る** -これはデフォルト値です。 • **以上** • **未満** • **以下**
書き込み速度のしきい値	しきい値と**演算子**により、監視対象のメトリクスの正常なパフォーマンスが判定されます。監視対象のメトリクスの値が基準値から逸脱した場合、システムによりアラートが生成されます。 整数値（kb/s）を入力します。デフォルト値は0kb/sです。
書き込み速度の期間	指定された期間中にメトリクスの値が通常範囲外の場合にのみ、検出された問題に対してシステムによりアラートが生成されます。 1～60（分）の範囲で整数値を入力します。デフォルト値は5です。

プロセスごとのネットワーク使用状況モニタを設定する

プロセスごとのネットワーク使用状況により、選択したプロセスの送受信トラフィックを監視します。もし同じプロセスの複数のインスタンスがある場合、システムはすべてのプロセスインスタンスの合計使用量を監視し、すべてのインスタンスの条件が満たされた場合にアラートを生成します。

モニタに、次の設定を構成できます。

設定	説明
プロセス名	監視するプロセスの名前です。拡張子を除いたプロセス名を入力します。
トラフィックの方向	監視するトラフィックの方向です。 次の値を使用できます。 • **受信トラフィックと送信トラフィック**。これはデフォルト値です。 • **受信トラフィック** • **送信トラフィック**
受信トラフィックの演算子	演算子は、メトリクスのパフォーマンスをどのように測定するかを定義する条件付きの関数です。 次の値を使用できます。

設定	説明
	• **を上回る** -これはデフォルト値です。 • **以上** • **未満** • **以下**
受信トラフィックのしきい値	しきい値と**演算子**により、監視対象のメトリクスの正常なパフォーマンスが判定されます。監視対象のメトリクスの値が基準値から逸脱した場合、システムによりアラートが生成されます。 整数値（kb/s）を入力します。デフォルト値は0kb/sです。
受信トラフィックの期間	指定された期間中にメトリクスの値が通常範囲外の場合にのみ、検出された問題に対してシステムによりアラートが生成されます。 1～60（分）の範囲で整数値を入力します。デフォルト値は5です。
送信トラフィックの演算子	演算子は、メトリクスのパフォーマンスをどのように測定するかを定義する条件付きの関数です。 次の値を使用できます。 • **を上回る** -これはデフォルト値です。 • **以上** • **未満** • **以下**
送信トラフィックのしきい値	しきい値と**演算子**により、監視対象のメトリクスの正常なパフォーマンスが判定されます。監視対象のメトリクスの値が基準値から逸脱した場合、システムによりアラートが生成されます。 整数値（kb/s）を入力します。デフォルト値は0kb/sです。
送信トラフィックの期間	指定された期間中にメトリクスの値が通常範囲外の場合にのみ、検出された問題に対してシステムによりアラートが生成されます。 1～60（分）の範囲で整数値を入力します。デフォルト値は5です。

Windowsサービスステータスモニタを設定する

Windowsサービスステータスにより、選択したWindowsサービスが実行中か停止中かを監視します。

モニタに、次の設定を構成できます。

設定	説明
サービス名	監視するWindowsサービスの名前です。 Windowsサービスのリストからサービスの名前を選択できます。ワークロードのソフトウェアインベントリスキャンが正常に完了すると、リストにテナントのすべてのエージェントが表示されます。また、リストにないサービス名を追加することもできます。これは、ソフトウェアインベントリスキャンがワークロードで実行されなかった場合にのみ利

設定	説明
	用できるオプションです。
サービスステータス	サービスが選択されたステータスの場合、システムによりイベントが生成されます。 次の値を使用できます。 • **実行中** • **停止**-これはデフォルト値です。
期間	指定された期間中にメトリクスの値が通常範囲外の場合にのみ、検出された問題に対してシステムによりアラートが生成されます。 1～60（分）の範囲で整数値を入力します。デフォルト値は1です。

プロセスステータスモニタを設定する

プロセスステータスにより、選択したプロセスが実行中か停止中かを監視します。もし同じプロセスの複数のインスタンスがある場合、システムは各プロセスのインスタンスを監視し、すべてのプロセスでインスタンスの条件が満たされた場合にアラートを生成します。

モニタに、次の設定を構成できます。

設定	説明
プロセス名	監視するプロセスの名前です。実行ファイルの名前を拡張子なしで入力します。
プロセスのステータス	プロセスが選択されたステータスの場合、システムによりイベントが生成されます。 次の値を使用できます。 • **実行中** • **停止**-これはデフォルト値です。
期間	指定された期間中にメトリクスの値が通常範囲外の場合にのみ、検出された問題に対してシステムによりアラートが生成されます。 1～60（分）の範囲で整数値を入力します。デフォルト値は1です。

インストール済みソフトウェアモニタを設定する

インストール済みソフトウェアにより、ワークロード上におけるソフトウェアアプリケーションのインストール、アップデート、削除を監視します。

モニタに、次の設定を構成できます。

設定	説明
監視対象のソフト	監視するソフトウェアを指定します。 次の値を使用できます。

設定	説明
ウェア	• **すべてのソフトウェア** -これはデフォルト値です。 • **特定のソフトウェア**
ソフトウェア名	この設定は、**監視対象のソフトウェア**で、**特定のソフトウェア**の値を選択した場合に有効になります。 1つまたは複数のソフトウェアアプリケーションの名前を入力します。 Windowsサービスのリストからソフトウェアアプリケーションの名前を選択できます。ワークロードのソフトウェアインベントリスキャンが正常に完了すると、リストにテナントのすべてのエージェントが表示されます。また、リストにないソフトウェアアプリケーション名を追加することもできます。これは、ソフトウェアインベントリスキャンがワークロードで実行されなかった場合にのみ利用できるオプションです。
インストールステータス	監視対象として、インストール済みソフトウェア、未インストールのソフトウェア、またはアップデート済みソフトウェアのいずれかを指定してください。 次の値を使用できます。 • **インストール済み** - これはデフォルト値です。この値を選択すると、新しいソフトウェアアプリケーションがワークロードにインストールされたときに、モニターによりアラートが生成されます。 • **アップデート済み** - この値を選択すると、ソフトウェアアプリケーションがアップデートされたときに、モニターによりアラートが生成されます。 • **未インストール** - この値を選択すると、ソフトウェアアプリケーションがインストール解除されたとき、またはワークロードで利用できないときに、モニターによりアラートが生成されます。

前回のシステム再起動モニタを設定する

前回のシステム再起動は、ワークロードの前回の再起動です。

モニタに、次の構成を設定できます。

設定	説明
以下の期間、ワークロードは再起動されていない	ワークロードの前回の再起動から経過した期間（日数）です。指定した期間を越えてワークロードが再起動されていない場合、システムによりアラートが生成されます。 1～180（日）の範囲で整数値を入力します。デフォルト値は30です。

Windowsイベントログモニタを設定する

Windowsイベントログにより、Windowsのイベントログに含まれる特定の業務に重要なイベントを監視します。

モニタに、次の設定を構成できます。

設定	説明
イベントログ名	Windows Event Viewerで利用可能なWindowsイベントログのリストから、特定のイベントログを選択します。 次の値を使用できます。 • **Any** -これはデフォルト値です。 • **アプリケーション** • **セキュリティ** • **システム**
[イベントソース]	イベントソース名 テナントのすべてのエージェントに基づき収集されたイベントソースのリストから値を選択します。また新しいソース名を手動で入力することもできます。 テナントでソフトウェアインベントリスキャンが無効になっている場合、イベントソースのリストは空になります。
マッチングモード	このフィールドでは、**イベントID**、**イベントの種類**、および**イベントの説明**の設定を**Any**（いずれか）または**All**（すべて）の演算子を使用して接続するかどうかを指定できます。 次の値を使用できます。 • **Any** -これはデフォルト値です。選択した条件のいずれかに合致した場合のみ、アラートが生成されます。 • **All** - 選択されたすべての条件に一致した場合に、アラートが生成されます。
イベントID	1つまたは複数のイベントIDをカンマで区切って入力します。このフィールドに入力したイベントコードがイベントログで見つかった場合、システムによりアラートが生成されます。
イベントの種類	監視したいイベントの種類を1つまたは複数選択します。 次の値を使用できます。 • **Any** -これはデフォルト値です。 • **エラー** • **警告** • **情報** • **成功監査** • **失敗監査**
イベントの説明	検索したいイベント説明文の具体的なキーワードやフレーズです。入力するキーワードやフレーズは、引用符で括り、カンマで区切る必要があります。システムにより入力したキーワードやフレーズのいずれかが検出された場合、アラートが生成されます。
発生回数	システムでアラートが生成されるために、ログ内で必要なイベントの最小発生回数です。 1～1000の範囲で整数値を入力します。
期間	指定された期間中にメトリクスの値が通常範囲外の場合にのみ、検出された問題に対して

設定	説明
	システムによりアラートが生成されます。 整数値を入力し、次に単位（分または時間）を選択します。デフォルト値は60分です。

ファイルとフォルダのサイズモニタを設定する

ファイルとフォルダのサイズにより、選択したファイルやフォルダの合計サイズを監視します。

モニタに、次の設定を構成できます。

設定	説明
監視するファイル/フォルダ	監視したいファイルやフォルダのパスです。また、監視対象から外したいファイルやフォルダを指定することもできます。 例えば次のようなワイルドカード文字を使用できます。 • * - ファイルまたはフォルダ名の0個以上の文字 • ? - ファイルまたはフォルダ名の1文字のみ Windowsワークロードの場合: • フルパスは、ドライブ文字から始まり、:\のセパレータが続きます。 • パスの区切り文字として、スラッシュまたはバックスラッシュを使用できます。 • ファイル名やフォルダ名の末尾にスペースやピリオドを使用することはできません。 macOSワークロードの場合: • フルパスは、ルートディレクトリから始まります。 • パスの区切り文字として、スラッシュを使用できます。 • ファイル名やフォルダ名の末尾にスペースやピリオドを使用することはできません。 除外フィルタの場合、特定のロケーションの指定は必須ではありません。ロケーションを指定せずに入力されたファイルは、監視対象フォルダから除外されます。
演算子	演算子は、メトリクスのパフォーマンスをどのように測定するかを定義する条件付きの関数です。 次の値を使用できます。 • **を上回る** -これはデフォルト値です。 • **未満**
しきい値	しきい値と**演算子**により、監視対象のメトリクスの正常なパフォーマンスが判定されます。監視対象のメトリクスの値が基準値から逸脱した場合、システムによりアラートが生成されます。 整数値（MB）を入力します。
期間	指定された期間中にメトリクスの値が通常範囲外の場合にのみ、検出された問題に対

設定	説明
	してシステムによりアラートが生成されます。 10～60（分）の範囲で整数値を入力します。デフォルト値は10です。

Windows Updateステータスモニタを設定する

Windows Updateステータスにより、ワークロードのWindows Updateのステータスを監視し、最新のアップデートプログラムがインストールされているかどうかを監視します。

このモニタを有効にすると、次のいずれかの状況でアラートが生成されます。

- ワークロードでWindows Updateが無効化されています。
- ワークロードでWindows Updateは有効化されていますが、最新のアップデートがインストールされませんでした。

ファイアウォールステータスモニタを設定する

ファイアウォールステータスにより、ワークロードにインストールされている組み込みの、またはサードパーティのファイアウォールのステータスを監視します。

このモニタを有効にすると、次のいずれかの状況でアラートが生成されます。

- OSビルトインのファイアウォール（Windows DefenderファイアウォールまたはmacOSファイアウォール）が無効になっており、サードパーティのファイアウォールが動作していない。
- パブリックネットワークに対しWindows Defenderファイアウォールが無効化されている。
- プライベートネットワークに対しWindows Defenderファイアウォールが無効化されている。
- ドメインネットワークに対しWindows Defenderファイアウォールが無効化されている。

ログイン失敗モニタを設定する

ログイン失敗により、ワークロードのログイン試行失敗を監視します。

モニタに、次の設定を構成できます。

設定	説明
ログイン試行失敗回数のしきい値	しきい値により、監視対象のメトリクスの正常なパフォーマンスの範囲を指定します。しきい値を超えると、正常値から外れた状態になります。 整数値を入力します。デフォルト値は60です。
期間	指定された期間中にメトリクスの値が通常範囲外の場合にのみ、検出された問題に対してシステムによりアラートが生成されます。 1～24の範囲で整数値を入力し、単位を「時間」または「日」から選択します。デフォルト値は12です。

マルウェア対策ソフトウェアのステータスモニタの設定

マルウェア対策ソフトウェアのステータスで、ワークロードにインストールされている組み込みまたはサードパーティのマルウェア対策ソフトウェアのステータスを監視できます。

このモニタを有効にすると、次のいずれかの状況が確認された場合にアラートが発生します。

- ワークロードにマルウェア対策ソフトウェアがインストールされていない。
- マルウェア対策ソフトウェアがインストールされているが、動作していない。
- マルウェア対策ソフトウェアはインストール済みで動作しているが、マルウェア対策の定義が最新ではない。

注意
この条件は、WindowsおよびWindows Serverオペレーティングシステムでチェックされます。

オペレーティングシステム	サポート対象のマルウェア対策ソフトウェア
Windows	• Acronis Cyber Protect • Windows Defender • Symantec Endpoint Security • Norton 360 • Norton antivirus • SentinelOne • Trend Micro Endpoint Security with Apex One • Trend Micro Worry-Free Business • McAfee Endpoint Security • McAfee Endpoint Protection for SMB • FireEye Endpoint Security • F-Secure SAFE • F-Secure Client Security • CrowdStrike Falcon • Kaspersky Endpoint Security Cloud • BitDefender Antivirus • Sophos Intercept X Endpoint • Avast Business Antivirus • AVG Antivirus Business Edition • AVG Internet Security Business Edition • Panda Endpoint Protection • Tencent PC Manager • Webroot Business Endpoint Protection • ESET Endpoint Security • Avira Antivirus • Comodo Internet Security

オペレーティングシステム	サポート対象のマルウェア対策ソフトウェア
	• Comodo Business Antivirus • K7 Business Security • K7 Total Security • Vipre Endpoint Protection • Total AV
Windows Server	• Acronis Cyber Protect • Windows Defender • ESET Endpoint Security **注意** このモニタは、他のマルウェア対策アプリケーションでも動作する可能性がありますが、保証対象外です。
macOS	• Acronis Cyber Protect • F-Secure Safe • BitDefender Anti-virus for Mac • Sophos Home • Sophos Endpoint Protection • Avast Security for Mac • AVG AntiVirus for Mac • Webroot SecureAnywhere • ESET Cybersecurity • Avira Antivirus for Mac • Comodo Antivirus for Mac • K7 Antivirus for Mac • Vipre Advanced Security • Total AV for Mac **注意** このモニタは、他のマルウェア対策アプリケーションでも動作する可能性がありますが、保証対象外です。

AutoRun機能のステータスモニタに関する設定

AutoRun機能のステータスで、リムーバブルメディアのAutoRun機能が有効かどうかを監視できます。

セキュリティ上の観点から、リムーバブルメディアのAutoRun機能は、ワークロードでは無効化することを推奨します。この機能が有効な場合、アラートが生成されます。

カスタムモニタを設定する

カスタムにより、スクリプトの実行を介してカスタムオブジェクトを監視します。

モニタに、次の設定を構成できます。

設定	説明
実行するスクリプト	スクリプトリポジトリから定義済みのスクリプトをリストアップします。
スケジュール	スクリプトを実行する時刻と、オプションで、スクリプトを実行するために満たすべき追加の条件を指定します。 次の値を使用できます。 • **時刻でスケジュール** - 明示した時間、日、週、月にスクリプトが実行されます。これはデフォルト値です。 **スケジュールの種類** - **時間単位**、**日単位**、**月単位** **日付範囲内に実行** - スクリプトを実行する時間帯を指定します。 • **システムへのユーザーログイン時** - ユーザーがワークロードにログインするときに、スクリプトが実行されます。 • **システムへのユーザーログオフ時** - ユーザーがワークロードからログアウトするときに、スクリプトが実行されます。 • **システムの起動時** - ワークロードのオペレーティングシステムが起動するときに、スクリプトが実行されます。 • **システムのシャットダウン時** - ワークロードがシャットダウンされるときに、スクリプトが実行されます。 • **システムがオンラインになったとき** - ワークロードがオンラインで利用可能になったときに、スクリプトが実行されます。 **条件で開始** - 条件に適合する場合のみ、指定した時間/イベント時にタスクが実行されます。複数条件を選択した場合、タスクを開始するにはすべての条件が同時に満たされる必要があります。 デフォルトでは、**スリープモードや休止モードに入らないようにして、スケジュールされたタスクを開始する**という条件が選択されています。 **開始条件を満たさない場合でも、次の時間の経過後にタスクを実行** - デフォルトではこの条件が有効化されています。デフォルト値は1時間です。
スクリプトを実行するアカウント	スクリプトを実行するアカウントです。 次の値を使用できます。 • **システムアカウント** - これはデフォルト値です。 • **現在ログインしているアカウント**
最大時間	ワークロード上でスクリプトを実行できる最大期間です。 この期間内にスクリプトが完了しない場合、処理は失敗します。 1～1440（分）の範囲で整数値を入力します。デフォルト値は3分です。
PowerShell実行ポリシー	PowerShell実行ポリシーです。 次の値を使用できます。

設定	説明
	• **Undefined** • **AllSigned** • **Bypass** - これはデフォルト値です。 • **RemoteSigned** • **Restricted** • **Unrestricted** これらの値の詳細については、Microsoftの文書を参照してください。

計画の監視

監視計画とは、監視機能を有効にし構成するために、管理対象のワークロードに適用する計画のことです。

ワークロードに監視計画が適用されていない場合、そのワークロードでは監視機能が利用できません。

注意
監視計画で構成できる内容は、テナントに適用されているサービスパックに依存します。すべての設定にアクセスするには、Advanced Managementパックを有効化します。

監視計画を作成する

監視計画を作成し、それにワークロードを追加することで、管理されたワークロード上の監視機能を設定できます。

前提条件

ワークロードにインストールされているエージェントのバージョンが、監視機能をサポートしている。

監視計画を作成するには

監視計画から

1. 保護コンソールで **[管理]** > **[監視計画]** に進みます。
2. 2種類のオプションのいずれかを使用して、監視計画を作成します。
   - リストに監視計画がない場合は、**[作成]** をクリックします。
   - リストに監視計画が存在する場合は、**[計画を作成]** をクリックします。
3. **[監視計画を作成]** ウィンドウでは、テナントでAdvanced Managementパックが有効化されているかどうかに応じて、以下の手順を実行します:
   - テナントがStandard保護を使用している場合、以下の4つのモニタが自動的に監視計画に追加されます。ディスク容量、ハードウェアの変更、前回のシステム再起動、ファイルおよびフォルダのサイズの4種類です。
   - テナントでAdvanced Managementパックが有効になっている場合は、テンプレートオプションを選択し、**[次へ]** をクリックして次へ進みます。

オプション	説明
推奨	このオプションを選択すると、デフォルトの監視構成で監視計画を作成します。
カスタム	このオプションを選択すると、監視計画はゼロから作成されます。

4. （オプション） 計画のデフォルト名を変更するには、鉛筆のアイコンをクリックし、計画名を入力してから、**[OK]** をクリックします。
5. （オプション） 計画にモニタを追加するには、**[モニタを追加]** をクリックし、リストでモニタを選択してから **[追加]** をクリックします。

   注意
   モニタの設定は、デフォルト値で自動的に入力されます。
   監視計画では、同じ種類のモニタを最大3つまで追加することができます。また、合計で最大30個のモニタを追加できます。

6. （オプション） モニタのパラメータ画面で、モニタとアラートのデフォルト設定を変更し、**[完了]** をクリックします。

   注意
   各モニタで異なる設定を構成できます。詳細については、「"構成可能なモニタ"（998ページ）」と「"アラートの監視を構成する"（1037ページ）」を参照してください。

7. （オプション） モニタを削除するには、ごみ箱アイコンをクリックし、**[削除]** をクリックします。
8. （オプション）計画にワークロードを追加するには:
   a. **[ワークロードを追加]** をクリックします。
   b. ワークロードを選択してから、**[追加]** をクリックします。
   c. 解決したい互換性の問題がある場合は、"監視計画との互換性の問題を解決する"（1035ページ）で説明されている手順を実行します。
9. **[作成]** をクリックします。

すべてのデバイスから

1. 保護コンソールで **[デバイス]** > **[すべてのデバイス]** に進みます。
2. 監視計画を適用したいワークロードをクリックします。
3. **[保護]** をクリックします。
4. ワークロードに監視計画が適用されているかどうかに応じて、以下の手順を実行します。
   - ワークロードに監視計画が既に適用されている場合は、**[計画を作成]** をクリックし、**[監視]** を選択します。
   - ワークロードに監視計画が適用されていない場合は、**[計画を追加]** をクリックし、**[計画を作成]** をクリックしてから **[監視]** を選択します。
5. **[監視計画を作成]** ウィンドウで、テンプレートオプションのいずれかを選択してから、**[次へ]** をクリックします。

オプション	説明
推奨	このオプションを選択すると、デフォルトの監視構成で監視計画を作成します。
カスタム	このオプションを選択すると、監視計画はゼロから作成されます。

6. （オプション） 計画のデフォルト名を変更するには、鉛筆のアイコンをクリックし、計画名を入力してから、**[OK]** をクリックします。
7. （オプション） 必要に応じてモニタとアラートのデフォルト設定を変更し、新しい値を構成してから **[完了]** をクリックします。

注意
監視計画では、同じ種類のモニタを最大3つまで追加することができます。また、合計で最大30個のモニタを追加できます。

8. （オプション） モニタのパラメータ画面で、モニタとアラートのデフォルト設定を変更し、**[完了]** をクリックします。

注意
各モニタで異なる設定を構成できます。詳細については、「"構成可能なモニタ"（998ページ）」と「"アラートの監視を構成する"（1037ページ）」を参照してください。

9. （オプション） モニタを削除するには、ごみ箱アイコンをクリックし、**[削除]** をクリックします。
10. **[作成]** をクリックします。

ワークロードを監視計画に追加する

ニーズに応じて、計画を作成してから、監視計画にワークロードを追加できます。

前提条件

- ユーザーアカウントの二要素認証が有効になっています。
- ワークロードにインストールされているエージェントのバージョンが、監視機能をサポートしている。
- 少なくとも1つの監視計画が存在する。

監視計画にワークロードを追加するには

監視計画から

1. 保護コンソールで **[管理]** > **[監視計画]** に進みます。
2. 監視計画をクリックします。
3. 既に計画が適用されているワークロードの有無に応じて、次の操作を実行します。
   - 計画がまだいずれのワークロードにも適用されていない場合は、**[ワークロードを追加]** をクリックします。

- 計画がいずれかのワークロードに適用されている場合は、[**ワークロードを管理**] をクリックします。

4. リストでワークロードを選択してから、[**追加**] をクリックします。
5. [**保存**] をクリックします。
6. 必要な場合、[**確認**] をクリックすると、サービスクォータがワークロードに適用されます。

すべてのデバイスから

1. 保護コンソールで [**デバイス**] > [**すべてのデバイス**] に進みます。
2. 監視計画を適用したいワークロードをクリックします。
3. [**保護**] をクリックします。
4. 監視計画を適用したいワークロードを見つけて、[**適用**] をクリックします。
5. 必要な場合、[**確認**] をクリックすると、サービスクォータがワークロードに適用されます。

監視計画を取り消す

計画が適用されたワークロードから、監視計画を取り消すことができます。

前提条件

少なくとも1つの監視計画が、ワークロードに適用されます。

監視計画を取り消すには

1. 保護コンソールで [**デバイス**] > [**すべてのデバイス**] に進みます。
2. ワークロードをクリックしてから、[**保護**] をクリックします。
3. 取り消したい監視計画の**その他の操作**アイコンをクリックし、[**取り消し**] をクリックします。

自動応答操作を構成する

アラートされたイベントに対する自動対応操作とは、検出されたイベントやインシデントに自動的に対応するために事前に定義された操作や措置のことです。これらの操作は、潜在的な脅威を軽減し、ダメージを最小限に抑えることを目的としています。

アラートイベントに対して1つまたは複数の自動対応操作を設定することができます。モニタごとの自動対応操作の最大数は20です。

自動対応操作を構成するには

1. 保護コンソールで [**管理**] > [**監視計画**] に進みます。
2. 自動対応操作を構成する監視計画を選択します。
3. 自動対応操作を構成したいモニタを選択します。まだモニタを追加していない場合は、[**モニタを追加**] をクリックして、リストでモニタを選択してから、[**追加**] をクリックします。
4. [**自動応答操作**] の横にあるリンクをクリックします。
5. [**自動応答操作**] ウィンドウで、アラートがトリガーされた際に自動的に実行される1つまたは複数の対応操作を追加します。

6. 各対応操作を構成します。例えば、対応操作として「**Windowsサービスを開始**」を追加した場合は、以下の手順を実行します。
   a. **Windowsサービス**の横にある、**[指定]** をクリックします。
   b. **サービス**フィールドで、対応操作として開始するサービスを選択します。
   c. **[完了]** をクリックします。
7. 追加されたすべての対応操作のリストで、上向き矢印や下向き矢印を使用するか、ドラッグアンドドロップで対応操作の順序を設定します。
8. 前の対応操作が失敗した場合に、連続した対応操作を処理する方法を構成します。次のいずれかを選択します。
   a. **次の対応操作を続行します。**
   b. **次の対応操作を続行しません。**
9. **[完了]** をクリックします。
   監視計画の**自動応答操作**設定の横に、構成された操作の数が表示されます。後からこれらの操作を編集/削除したり、新しいアクションを追加したりできます。

モニタ設定で利用可能なすべての自動対応操作とその説明を以下の表に示します。

自動応答操作	説明	サポート対象のOS
スクリプトを実行	この操作を追加することで、次の項目を実行できます。 1. ワークロードで実行する特定のスクリプトを選択する。 2. スクリプトを実行するアカウントを指定する。 3. 処理の最大継続時間を指定する。 4. PowerShell実行ポリシーを指定する。 5. スクリプトを実行する。 この操作を実行するには、対象のワークロードでAdvanced Managementパックライセンスが必要になります（まだ割り当てられていない場合）。 条件が満たされた場合、システムにより指定されたパラメータで選択したリモートスクリプトが実行されます。	Windows、macOS
ワークロードを再起動	この操作を追加すると、条件が満たされた場合、システムによりリモートでワークロードが再起動されます。	Windows、macOS
[プロセスの停止]	この操作を追加すると、手動でプロセス名を入力して停止するプロセスを指定できます。 条件が満たされた場合、システムによりプロセ	Windows、macOS

自動応答操作	説明	サポート対象のOS
	スが停止されます。	
Windowsサービスを開始	この操作を追加すると、エージェントから取得されたサービスの動的リストから、開始するWindowsサービスを選択できます。 条件が満たされた場合、システムによりサービスが開始されます。	Windows
Windowsサービスを停止	この操作を追加すると、エージェントから取得されたサービスの動的リストから、停止するWindowsサービスを選択できます。 条件が満たされた場合、システムによりサービスが停止されます。	Windows
Windowsアップデートを有効化	この操作を追加すると、条件が満たされた場合、Windows Updateが有効になります。 この操作は、Windows Updateのステータスモニタでのみ利用可能です。	Windows
リムーバブルドライブでAutoRunを無効化	この操作を追加すると、条件が満たされた場合、システムによりワークロードのリムーバブルストレージメディア上のAutoRun機能が無効化されます。 この操作は、AutoRun機能のステータスモニタでのみ利用可能です。	Windows

監視計画を含む追加処理

[監視計画] 画面から、監視計画に対して追加操作（詳細を表示、編集、アクティビティを表示、アラートを表示、名前を変更、有効化、無効化、クローン、エクスポート、削除）を実行できます。

詳細の表示

監視計画の詳細を表示するには

1. **[監視計画]** 画面で、監視計画の **[その他の操作]** アイコンをクリックします。
2. **[詳細の表示]** をクリックします。
3. （オプション） 計画で有効になっているモニタの詳細を表示するには、モニタの名前をクリックします。

編集

前提条件

ユーザーアカウントの二要素認証が有効になっています。

計画を編集するには

1. **[監視計画]** 画面で、監視計画の **[その他の操作]** アイコンをクリックします。
2. **[編集]** をクリックします。
3. （オプション） 計画からモニタを削除するには、モニタ名の右側にあるごみ箱のアイコンをクリックします。
4. （オプション） 計画内のモニタを有効化または無効化するには、モニタ名の横にあるスイッチを使用します。
5. （オプション） モニタのパラメータを編集するには、次の手順を実行します。
   a. モニタの名前をクリックします。
   b. モニタのパラメータの概要をクリックします。
   c. **モニタのパラメータ**画面で、パラメータを構成し、**[完了]** をクリックします。

      注意
      各モニタで異なる設定を構成できます。詳細については、「"構成可能なモニタ"（998ページ）」と「"アラートの監視を構成する"（1037ページ）」を参照してください。

   d. 画面を閉じて、変更を確認します。
6. （オプション） モニタを追加するには、**[モニタを追加]** をクリックし、必要に応じて前の手順で説明されたようにパラメータを編集します。
7. **[保存]** をクリックします。

アクティビティ

監視計画に関連するアクティビティを表示するには

1. **[監視計画]** 画面で、監視計画の **[その他の操作]** アイコンをクリックします。
2. **[アクティビティ]** をクリックします。
3. アクティビティをクリックすると、その詳細が表示されます。

アラート

アラートを表示するには

1. **[監視計画]** 画面で、監視計画の **[その他の操作]** アイコンをクリックします。
2. **[アラート]** をクリックします。

名前の変更

前提条件

ユーザーアカウントの二要素認証が有効になっています。

監視計画の名前を変更するには

1. **[監視計画]** 画面で、監視計画の **[その他の操作]** アイコンをクリックします。
2. **[名前の変更]** をクリックします。
3. 計画の新しい名前を入力し、**[OK]** をクリックします。

有効にする

前提条件

- ユーザーアカウントの二要素認証が有効になっています。
- 監視計画は、少なくとも1つのワークロードに適用されます。

監視計画を有効化するには

1. **[監視計画]** 画面で、監視計画の **[その他の操作]** アイコンをクリックします。
2. **[有効にする]** をクリックします。

無効にする

前提条件

ユーザーアカウントの二要素認証が有効になっています。

監視計画を無効化するには

1. **[監視計画]** 画面で、監視計画の **[その他の操作]** アイコンをクリックします。
2. **[無効にする]** をクリックします。

クローンを作成

前提条件

ユーザーアカウントの二要素認証が有効になっています。

監視計画のクローンを作成するには

1. **[監視計画]** 画面で、監視計画の **[その他の操作]** アイコンをクリックします。
2. **[クローン]** をクリックします。
3. **[作成]** をクリックします。

エクスポート

前提条件

ユーザーアカウントの二要素認証が有効になっています。

監視計画をエクスポートするには

1. **[監視計画]** 画面で、監視計画の **[その他の操作]** アイコンをクリックします。
2. **[エクスポート]** をクリックします。
   計画の構成はJSON形式でローカルのマシンにエクスポートされます。

削除

前提条件

ユーザーアカウントの二要素認証が有効になっています。

監視計画を削除するには

1. **[監視計画]** 画面で、監視計画の **[その他の操作]** アイコンをクリックします。
2. **[削除]** をクリックします。
3. **[確認しました]** を選択して、**[削除]** をクリックします。

監視計画の互換性の問題

ワークロードに監視計画を適用すると、互換性の問題が発生する場合があります。以下のような互換性の問題が考えられます:

- 互換性のないオペレーティングシステム - この問題は、ワークロードのオペレーティングシステムがサポートされていない場合に発生します。
- サポートされていないエージェント - この問題は、ワークロード上のプロテクションエージェントのバージョンが古く、監視機能がサポートされていない場合に発生します。
- クォータの不足 - この問題は、選択したワークロードに割り当てる十分なサービスクォータがテナントに存在しない場合に発生します。

150件以下のワークロードを個別に選択して、監視計画を適用する場合、計画を保存する前に、既存の競合を解決するよう通知が表示されます。競合を解決するには、競合の根本原因を取り除くか、影響を受けるワークロードを計画から削除します。詳細については、"監視計画との互換性の問題を解決する"（1035ページ）を参照してください。競合を解決せずに計画を保存すると、互換性のないワークロードに対して計画が自動的に無効にされ、アラートが表示されます。

150件を超えるワークロードまたはデバイスグループに、監視計画を適用する場合、保存が完了した後で互換性が確認されます。互換性のないワークロードについては、計画が自動的に無効化され、アラートが表示されます。

監視計画との互換性の問題を解決する

互換性の問題の原因に応じ、新しい監視計画を作成するプロセスの一環として、互換性の問題を解決するための各操作を実行できます。

互換性の問題を解決するには

1. **[問題をレビュー]** をクリックします。
2. （オプション） ワークロードを計画から削除することで、互換性のないオペレーティングシステムとの互換性の問題を解決するには:
   a. **[互換性がないオペレーティングシステム]** タブで、削除するワークロードを選択します。
   b. **[計画からワークロードを削除]** をクリックします。
   c. **[削除]** をクリックしてから、**[閉じる]** をクリックします。
3. （オプション） 計画でモニタを無効化することで、互換性のないオペレーティングシステムとの互換性の問題を解決するには:
   a. **[互換性がないオペレーティングシステム]** タブで、削除するモニタを選択します。
   b. **[モニタを無効化]** をクリックします。
   c. **[無効化]** をクリックしてから、**[閉じる]** をクリックします。

4. （オプション） 計画からワークロードを削除して、サポートされていないエージェントの互換性の問題を解決するには
   a. **[サポートされていないエージェント]** タブで、削除するワークロードを選択します。
   b. **[計画からワークロードを削除]** をクリックします。
   c. **[削除]** をクリックしてから、**[閉じる]** をクリックします。
5. （オプション） エージェントのバージョンをアップデートして、サポートされていないエージェントとの互換性の問題を解決するには、**[エージェントリストに移動]** をクリックします。

   注意
   このオプションを使用できるのは、カスタマー管理者のみです。

6. （オプション） 計画からワークロードを削除して、クォータの不足を伴う互換性の問題を解決するには:
   a. **[クォータの不足]** タブで、削除するワークロードを選択します。
   b. **[計画からワークロードを削除]** をクリックします。
   c. **[削除]** をクリックしてから、**[閉じる]** をクリックします。
7. （オプション） テナントのクォータを増やして、クォータの不足による互換性の問題を解決するには:
   a. **[クォータの不足]** タブで、**[管理ポータルに移動]** をクリックします。
   b. カスタマーのサービスクォータを増やします。

      注意
      このオプションを使用できるのは、パートナー管理者のみです。

機械学習モデルをリセットする

ワークロードのモデルが古くなったり、何らかの理由で無効となったりした場合に、リセットできます。この操作では、作成済みのモデルとアノマリベース監視タイプのモニタによりワークロードから収集されたデータが削除され、ワークロードの機械学習モデルのトレーニングが初期状態から開始されます。

ワークロードの機械学習モデルをリセットするには

1. 保護コンソールで **[デバイス]** > **[すべてのデバイス]** に進みます。
2. リストでワークロードをクリックしてから、**[詳細]** タブをクリックします。
3. **[機械学習モデルをリセット]** セクションで、**[リセット]** をクリックします。
4. 確認ウィンドウでもう一度 **[リセット]** をクリックします。

監視アラート

監視アラートは、保護コンソールに表示されます。また監視対象となっているワークロードで、通常とは異なる挙動が見られたときには、Eメールが送信されます。これらのアラートは、組織のIT環境に問題が発生した場合に、関係者ができるだけ早く情報を得られるようにするためのものです。

注意
監視アラートをEメールで受け取るには、対応するアラートの種類向けに少なくとも1件のEメール通知ポリシーを構成する必要があります。詳細については、"Eメール通知ポリシーを構成する"（1044ページ）を参照してください。

アラートの監視を構成する

モニタを監視計画に追加する際、または既存の監視計画に既に存在するモニタを編集する際に、モニタのアラート設定を構成できます。

監視アラートを構成するには

1. **[パラメータを監視]** ウィンドウで、**[アラートを生成]** セクションに移動します。
2. **アラートの重大度**で、アラートの優先度に対応する重大度を選択します。

オプション	説明
重大	これらのアラートは優先度が最も高く、ワークロードの運用の重要な問題に関連するものです。これらの問題は、できるだけ早く解決してください。
エラー	エラーアラートはより軽微であり、いずれかの箇所で問題があるか、正常に動作していないことを示しています。問題を適切なタイミングで解決して、より深刻な問題が発生するのを防ぐことができます。
警告	警告アラートは、まだ問題に至っていないものの、注意が必要な状態を示しています。重大アラートやエラーアラートの原因となっている問題を修正した後に、警告アラートの問題も解決してください。 これはデフォルト値です。
情報	優先順位の最も低いアラートです。重大度が「情報」の場合、問題を示すものではありません。この種類のアラートは、監視対象のオブジェクトに関連する操作についての情報を提供します。

3. **アラート頻度**で、条件が満たされたときにシステムがアラートを生成する頻度を選択します。

オプション	説明
確認が成功するまで1回	システムは、チェックが正常に完了するまで、1回だけアラートを生成します。 これはデフォルト値です。
X回連続で失敗した場合	X回連続でチェックに失敗するとアラートが生成されます（Xは整数値）。

4. **アラートメッセージ**で、鉛筆アイコンをクリックして、システムがアラートを生成する際に使用されるデフォルトのアラートメッセージを編集します。変数を含むカスタムアラートメッセージを指定できます。使用可能な変数の詳細については、"監視アラートの変数"（1038ページ）を参照してください。

注意
一部のモニタには、複数のアラートメッセージを設定できます。

5. **[アラート自動解決]** を有効にすると、監視されているメトリクスが正常な状態に戻り、動作が正常化した場合に、システムがアラートを自動的に解決するようになります。デフォルトでは、この設定は有効になっています。

監視アラートの変数

異なるモニタに対して異なるアラート変数を構成できます。変数を使用するには、{{}}で括る必要があります。

次の表に、利用可能な変数の詳細を示します。

変数	説明	モニタで利用可能
plan_name	ポリシーの名前	すべてのモニタ
monitor_name	監視計画のサブポリシーの名前	すべてのモニタ
workload_name	ワークロードの名前	すべてのモニタ
threshold_value	アラートを発生させるための特定の監視条件またはしきい値	しきい値ベースの監視をサポートするすべてのモニタ。
threshold_unit	しきい値に関連する単位です。例えば、%、MB、またはmb/sなどです。	しきい値ベースの監視をサポートするすべてのモニタ。
time_period	指定された期間中にメトリクスの値が通常範囲外の場合にのみ、検出された問題に対してシステムによりアラートが生成されます。	しきい値ベースの監視をサポートするすべてのモニタ。
time_unit	時間間隔に関連付ける単位（sec/mini/hours/day）です。	しきい値ベースの監視をサポートするすべてのモニタ。
anomaly_value	異常値	アノマリベースの監視をサポートするすべてのモニタ。
anomaly_unit	異常値に関連する単位	アノマリベースの監視をサポートするすべてのモニタ。
deviation_value	偏差値	アノマリベースの監視をサポートするすべてのモニタ。

変数	説明	モニタで利用可能
deviation_unit	偏差値に関連する単位	アノマリベースの監視をサポートするすべてのモニタ。
drive_name	Windowsの場合はドライブ、macOSの場合はパーティション	ディスク容量、
CPU_model	監視対象CPUのモデル	CPU温度
GPU_model	監視対象GPUのモデル	GPU温度
hardware_model	監視対象のコンポーネントのモデル	ハードウェアの変更
hardware_component	監視対象のハードウェアの種類	ハードウェアの変更
hardware_model_old	交換された監視対象コンポーネントのモデル	ハードウェアの変更
hardware_model_new	追加された新しい監視対象コンポーネントのモデル	ハードウェアの変更
disk_model	ディスクのモデル	ディスク転送速度
network_adapter_model	ネットワークアダプタのモデル	ネットワーク使用率
process_name	プロセスの名前	プロセス別のCPU使用状況 プロセス別のメモリ使用状況 プロセス別のディスク転送速度 プロセス別のネットワーク使用状況 プロセスのステータス
service_name	サービスの名前	Windowsサービスのステータス
software_name	ソフトウェアアプリケーションの名前	インストール済みソフトウェア
software_version	ソフトウェアアプリケーションのバージョン	インストール済みソフトウェア

変数	説明	モニタで利用可能
software_version_old	アップデート前のソフトウェアアプリケーションのバージョン	インストール済みソフトウェア
software_version_new	新しいまたはアップデート済みのソフトウェアアプリケーションのバージョン	インストール済みソフトウェア
number_of_occurrences	イベントがログに表示される回数	Windowsイベントログ
event_types	イベントの種類	Windowsイベントログ
event_source	イベントのソース	Windowsイベントログ
event_log_name	イベントの名前	Windowsイベントログ
firewall_software_name	ファイアウォールソフトウェアの名前	ファイアウォールのステータス
antimalware_software_name	マルウェア対策ソフトウェアの名前	マルウェア対策ソフトウェアのステータス
user_name	ユーザーの名前	自動実行機能のステータス
script_name	スクリプトの名前	カスタム

手動対応操作

アラートが表示された場合に、アラートの原因となったイベントに対して実行する対応操作を選択できます。

手動対応操作を実行するには

1. 保護コンソールで **[アラート]** に進みます。
2. 表示したいアラートを開きます。
3. **[対応操作]** をクリックし、ドロップダウンリストから対応操作を選択します。

特定のアラートに利用可能な対応操作のリストは、アラートのタイプ、テナントにおける特定の機能の利用可能性、およびワークロードのオペレーティングシステムによって異なります。

以下の表はすべての手動対応操作のリストと説明です。参考にしてください。

手動対応操作	説明	サポート対象のOS
ディスク領域の使用状況の傾向を参照	**ディスク使用状況**グラフのあるウィンドウでは、次の手順を実行できます。	Windows、macOS

手動対応操作	説明	サポート対象のOS
	• ディスク使用状況の変化を時系列（直近1日/7日/1ヵ月）で参照する。 • 選択した期間について、ディスク使用状況のデルタ値を相対値（%）で参照する。	
ファイルサイズ増大の傾向を参照	**ファイルサイズ増大**グラフのあるウィンドウでは、次の手順を実行できます。 • 監視対象ファイル/フォルダの合計サイズの変化を時系列（1日/7日/1ヵ月）で参照する。 • 選択した期間について、ファイルの合計サイズのデルタ値を相対値（%）で参照する。	Windows、macOS
スクリプトを実行	ウィンドウで、次の手順を実行できます。 1. ワークロードで実行する特定のスクリプトを選択する。 2. スクリプトを実行するアカウントを指定する。 3. 処理の最大継続時間を指定する。 4. PowerShell実行ポリシーを指定する。 5. スクリプトを実行する。 この操作を実行するには、対象のワークロードでAdvanced Managementパックライセンスが必要になります（まだ割り当てられていない場合）。	Windows、macOS
NEAR経由での接続	Acronis 接続クライアントでリモート接続を確立します。	Windows、macOS
RDP経由での接続	Acronis 接続クライアントでリモート接続を確立します。	Windows
ハードウェアインベントリを開く	現在のワークロードの **[ハードウェアインベントリ]** タブにリダイレクトされます。	Windows、macOS
CPU読み込み上位10件のプロセスを参照	アラート生成時にCPUに負荷をかけ、オーバーヒートの原因となった可能性のある上位10件のプロセスを表示するウィンドウが開きます（アラート生成時のシステムスナップショット）。	Windows、macOS
GPU読み込み上位10件のプロセスを参照	アラート生成時にGPUに負荷をかけ、オーバーヒートの原因となった可能性のある上位10件のプロセスを表示するウィンドウが開きます（アラート生成時のシステムスナップショット）。	Windows、macOS
メモリ読み込み上位10件のプ	アラート生成時にメモリに負荷をかけた可能性	Windows、

手動対応操作	説明	サポート対象のOS
ロセスを参照	のある上位10件のプロセスを表示するウィンドウが開きます（アラート生成時のシステムスナップショット）。	macOS
ディスク読み込み上位10件のプロセスを参照	アラート生成時にディスクに負荷をかけた可能性のある上位10件のプロセスを表示するウィンドウが開きます（アラート生成時のシステムスナップショット）。	Windows、macOS
ネットワーク読み込み上位10件のプロセスを参照	アラート生成時にネットワークインターフェースアダプタに負荷をかけた可能性のある上位10件のプロセスを表示するウィンドウが開きます（アラート生成時のシステムスナップショット）。	Windows、macOS
プロセス別のリソース使用状況を参照	関連するプロセスによるハードウェアリソースの使用状況に関する詳細情報を表示するウィンドウが開きます。CPU使用状況、メモリ使用状況、ディスクI/O、ネットワーク使用状況。	Windows、macOS
ワークロードを再起動	確認ウィンドウが開きます。確認後、ワークロードが再起動します。	Windows、macOS
Windowsサービスを開始	確認ウィンドウが開きます。確認後、Windowsサービスが開始します。	Windows
Windowsサービスを停止	確認ウィンドウが開きます。確認後、Windowsサービスが停止します。	Windows
プロセスを停止	確認ウィンドウが開きます。確認後、アラートが参照する処理を停止します。	Windows、macOS
Windowsアップデートを有効化	確認ウィンドウが開きます。確認後、Windowsアップデートが有効化されます。	Windows
リムーバブルドライブでAutoRun機能を無効化	確認ウィンドウが開きます。確認後、ワークロードのシステムレベルでAutoRun機能が無効化されます。	Windows

重要
次の手動対応操作を実行する場合、セキュリティ上の理由から、二要素認証を使用する必要があります。

- スクリプトを実行
- NEAR経由での接続
- RDP経由での接続
- ワークロードを再起動
- Windowsサービスを開始
- Windowsサービスを停止
- プロセスを停止
- Windowsアップデートを有効化
- リムーバブルドライブでAutoRun機能を無効化

ワークロードの監視アラートを表示する

[アラート] タブでは、特定のワークロードの監視アラートを表示したり、さまざまなアラート操作を実行したりできます。

ワークロードの監視アラートを表示するには

1. 保護コンソールで **[すべてのデバイス]** に進みます。
2. ワークロードをクリックし、**[監視]** タブを選択します。
3. （オプション） 監視アラートペインで、以下の操作のいずれかを実行します。
   - アラートを消去するには、**[消去]** をクリックします。
   - 対応操作を実行するには、**[対応操作]** をクリックしてから、操作をクリックします。
   - サポートチームに連絡するには、**[サポートの利用]** をクリックします。
4. （オプション） ワークロードのすべての監視アラートを消去するには、**[すべて消去]** をクリックします。

監視アラートのアラートログを表示する

監視アラートに関連するすべてのイベントを時系列順に表示できます。イベントには実行された対応操作（自動または手動）や送信されたEメール通知などが含まれます。

監視アラートの監査ログを表示するには

1. 保護コンソールで **[アラート]** に進みます。
2. **[テーブルビュー]** を開きます。
3. アラートのリストで、表示したい監視アラートをクリックします。
4. **[詳細]** をクリックしてから、**[アラートログ]** をクリックします。

Eメール通知ポリシーを構成する

Eメール通知ポリシーでは、どのユーザーが各種のモニターからEメール通知を受け取るかを指定します。

[Eメール通知] 画面から、Eメール通知ポリシーに対して、追加、編集、有効化、無効化、削除の各操作を実行できます。

追加

新しいEメール通知ポリシーを追加するには

1. 保護コンソールで、**[設定]** > **[Eメール通知]** に移動します。
2. **[ポリシーを追加]** をクリックします。
3. **[受信者を選択]** をクリックします。
4. **[受信者を選択]** 画面で、Eメールアラートを受け取りたいユーザーを選択してから、**[選択]** をクリックします。
5. **[アラートの種類]**で、システムにEメールアラートを送信するモニターを選択します。
6. **[追加]** をクリックします。

編集

Eメール通知ポリシーを編集するには

1. 保護コンソールで、**[設定]** > **[Eメール通知]** に移動します。
2. 通知ポリシーの省略記号アイコンをクリックしてから、**[編集]** をクリックします。
3. （オプション） 受信者を変更するには、**[受信者を編集]** をクリックし、リストからユーザーを追加または削除してから、**[選択]** をクリックします。
4. （オプション） **[アラートの種類]** で、選択した受信者に送信する監視アラートの種類を選択します。
5. **[保存]** をクリックします。

有効にする

Eメール通知ポリシーを有効にするには

1. 保護コンソールで、**[設定]** > **[Eメール通知]** に移動します。
2. **[Eメール通知]** 画面で、Eメール通知ポリシーの **[...]** アイコンをクリックします。
3. **[有効にする]** をクリックします。

無効にする

Eメール通知ポリシーを無効にするには

1. 保護コンソールで、**[設定]** > **[Eメール通知]** に移動します。
2. **[Eメール通知]** 画面で、Eメール通知ポリシーの **[...]** アイコンをクリックします。
3. **[無効にする]** をクリックします。

削除

Eメール通知ポリシーを削除するには

1. 保護コンソールで、**[設定]** > **[Eメール通知]** に移動します。
2. **[Eメール通知]** 画面で、Eメール通知ポリシーの **[...]** アイコンをクリックします。
3. **[削除]** をクリックしてから、**[確認]** をクリックします。

監視データを表示する

各ワークロードについて、グラフィカルビューによる適用されたモニターのリスト、モニターの現在の状態、およびパフォーマンス履歴詳細を表示できます。この情報を使用して、ワークロードのステータスと時間経過に伴うステータスの変化を分析できます。

前提条件

- ワークロードに監視計画が適用されている。
- ワークロードはオンラインであり、対応するモニタのデータが含まれている。
- ワークロードにインストールされているエージェントのバージョンが、監視計画をサポートしている。

ワークロードに適用されているモニタとモニタデータを表示するには

1. 保護コンソールで **[デバイス]** > **[すべてのデバイス]** に進みます。
2. ワークロードをクリックし、**[監視]** タブをクリックします。
   [監視] タブには、ワークロードで有効になっている各モニタのウィジェットが表示されます。各ウィジェットには、次の情報が表示されます。

表示される情報	説明
モニタ名	モニタの名前です
前回の結果	監視対象のメトリクスの最終値、またはイベントの最終ステータスです
前回の確認	モニタで最後にデータが収集された日付と時刻です
アラート	モニターによって生成された、未解決のアラートの数です。 該当のモニターによって生成された未解決のアラートが1つまたは複数ある場合、その番号をクリックすると **[アラート]** タブが開きます。アラートはフィルタリングされ、このモニターのアラートのみがリストアップされます。

注意
ウィジェットは、監視計画をワークロードに適用してから15分後（またはモニタに設定された最小の監視頻度）にタブに表示されるようになります。

3. （オプション） モニタの詳細、および該当する場合、監視対象のメトリクスについて収集された履歴データを表示するには、モニタのウィジェットで省略記号アイコンをクリックし、**[詳細]** をクリックします。
   ウィジェットで確認できるモニタの詳細については、"ウィジェットを監視"（1046ページ）を参照してください。

ウィジェットを監視

モニタウィジェットでは、モニタに関する以下の詳細情報を確認できます。

詳細	説明
監視計画	モニタを含む監視計画の名前です。監視計画の名前は、表示モードで監視計画を開くリンクになります。
モニタの間隔	モニタがワークロードからデータを収集する時間間隔
前回の結果	監視対象のメトリクスの最終値、またはイベントの最終ステータスです
前回の確認	モニタで最後にデータが収集された日付と時刻です
前回のアラート	最後にアラートが生成された日時です。このフィールドは、モニタで少なくとも1件のアラートが生成されている場合にのみ表示されます。
時系列のグラフ	時系列のデータを収集するモニターでは、ウィジェットにより選択した期間（1時間、6時間、12時間、1日、1週間、または1ヵ月）の過去のデータをグラフで表示できます。 グラフには、選択した期間中のメトリクスの実際の値が表示されます。何らかの理由によりエージェントで収集されたデータがクラウドに送信されなかった場合、欠落している値は、その値の前後の実際の値をつなぐ点線として表示されます。 **アノマリベース**の監視を使用しているモニターの場合、グラフには基準範囲、メトリクスの実際の値を示す線、および異常が表示されます。異常とは、基準から外れたスパイクまたは値のことで、グラフ上では赤い点として表示されます。 グラフにマウスをホバーすると、特定の時間における実際の値やしきい値を確認できます。

詳細	説明
	 **注意** グラフ上のデータは、ローカルシステムのタイムゾーンで表示されます。これは、保護コンソールにアクセスするワークロードのブラウザのタイムゾーンです。

追加のCyber Protectionツール

コンプライアンスモード

コンプライアンスモードは、より高いセキュリティが要求されるクライアント向けに設計されています。このモードでは、すべてのバックアップに暗号化を必須とし、ローカルで設定された暗号化パスワードのみを許可します。

コンプライアンスモードでは、顧客テナントとそのユニットで作成されたすべてのバックアップは、AESアルゴリズムと256ビットのキーで自動的に暗号化されます。ユーザーが暗号化パスワードを設定できるのは、保護対象デバイスのみであり、保護計画には設定できません。

重要
コンプライアンスモードは無効にできません。

制限事項

- コンプライアンスモードは、バージョンが15.0.26390以上のエージェントとのみ互換性があります。
- コンプライアンスモードは、Red Hat Enterprise Linux 4.x、5.x、およびそれらの派生OSを実行しているデバイスでは利用できません。
- クラウドサービスでは暗号化パスワードにアクセスできません。この制限のため、コンプライアンスモードのテナントでは、一部の機能を利用できません。

サポートされない機能

コンプライアンスモードのテナントでは、以下の機能を利用できません。

- Cyber Protectコンソールを介した復元
- Cyber Protectコンソールを介したバックアップのファイルレベルの参照
- クラウドからクラウドへのバックアップ
- Webサイトバックアップ
- アプリケーションのバックアップ
- モバイルデバイスのバックアップ
- バックアップのマルウェア対策スキャン
- 安全な復元
- 社内ホワイトリストの自動作成
- データ保護マップ
- 災害復旧
- 利用できない機能に関連するレポートとダッシュボード

暗号化パスワードの設定

保護対象のデバイスに、ローカルでこの暗号化パスワードを設定する必要があります。保護計画で暗号化パスワードを設定することはできません。パスワードがないとバックアップの作成に失敗します。

警告
パスワードを失くしたり忘れたりした場合に、暗号化されたバックアップをリカバリする方法はありません。

暗号化パスワードは、以下の方法で設定できます。

1. プロテクションエージェントのインストール中（Windows、macOS、Linux向け）。
2. コマンドラインを使用する（WindowsおよびLinux向け）。
   仮想アプライアンスに暗号化パスワードを設定する場合、この方法を利用する必要があります。
   Acropshツールで暗号化パスワードを設定する方法の詳細については、「"暗号化"（430ページ）」を参照してください。
3. Cyber Protectモニターを使用する（WindowsおよびmacOS向け）。

Cyber Protectモニターで暗号化パスワードを設定するには

1. 保護されたデバイスで、管理者としてログオンします。
2. 通知領域（Windows）またはメニューバー（macOS）でCyber Protect Monitorのアイコンをクリックします。
3. ギアアイコンをクリックします。
4. **[暗号化]** をクリックします。
5. 暗号化パスワードを設定します。
6. **[OK]** をクリックします。

暗号化パスワードの変更

保護計画がバックアップを作成する前に、暗号化パスワードを変更することができます。

バックアップ作成後に暗号化パスワードを変更すると、その後のバックアップが失敗するため、変更しないことを推奨します。同じマシンを保護し続けるには、該当のマシンに対応する新しい保護計画を作成する必要があります。暗号化パスワードと保護計画の両方を変更すると、変更したパスワードで暗号化された新しいバックアップが作成されます。これらを変更する前に作成されたバックアップは影響を受けません。

または、適用された保護計画を維持し、その中のバックアップファイルの名前のみを変更することもできます。これにより、変更したパスワードで暗号化された新しいバックアップも作成されます。バックアップファイルの名前の詳細については、「"バックアップ ファイル名"（440ページ）」を参照してください。

暗号化パスワードは、以下の方法で変更できます。

1. Cyber Protectモニターを使用する（WindowsおよびmacOS向け）。
2. コマンドラインを使用する（WindowsおよびLinux向け）。
   Acropshツールで暗号化パスワードを設定する方法の詳細については、「"暗号化"（430ページ）」を参照してください。

コンプライアンスモードでテナントのバックアップを復元する

コンプライアンスモードでは、Cyber Protectコンソールからバックアップをリカバリすることはできません。

次から選択できます。

- ブータブルメディアを使用して、マシン全体、ディスク、ファイルをリカバリすることができます。
- Windowsファイルエクスプローラーを使用して、インストール済みエージェントでWindowsマシンのローカルバックアップからファイルを抽出します。

不変ストレージ

不変ストレージを使用すると、指定した保持期間中に削除されたバックアップにアクセスできます。これらのバックアップからコンテンツをリカバリすることはできますが、それらを変更、移動、または削除することはできません。保持期間が終了すると、削除済みバックアップは恒久的に削除されます。

不変ストレージには以下のバックアップが含まれています。

- 手動で削除されたバックアップ。
- 保護計画の **[保持する期間]** セクションまたはクリーンアップ計画の **[保持ルール]** セクションの設定に従って自動的に削除されるバックアップ。

削除されたバックアップは不変ストレージに保存され、ストレージスペースを消費します。また消費量に応じて課金が発生します。

削除されたテナントは、不変ストレージを含め、ストレージの利用料はかかりません。

不変ストレージモード

カスタマーテナントの場合、不変ストレージは以下のモードで利用できます。

不変ストレージは以下のモードで利用できます。

- **ガバナンスモード**
  不変ストレージを無効にしたり、再度有効にしたりできます。保持期間の変更や、コンプライアンスモードへの切り替えもできます。
- **コンプライアンスモード**

  警告
  一度コンプライアンスモードを選択すると、元に戻せなくなります。

  不変ストレージを無効にすることはできません。保持期間を変更したり、ガバナンスモードに戻したりすることはできません。

サポートされるストレージとエージェント

- 不変ストレージはクラウドストレージのみでサポートされます。

  不変ストレージは、Acronis Cyber Infrastructureバージョン4.7.1以降を利用する、Acronisまたはパートナーがホストするクラウドストレージストレージで使用できます。

  Acronis Cyber Infrastructure ストレージ、Amazon S3 および EC2 ストレージ、Microsoft Azure ストレージなど、Acronis Cyber Infrastructure Backup Gatewayで使用できるすべてのストレージがサポートされています。

  不変ストレージでは、Acronis Cyber Infrastructure のバックアップゲートウェイサービス用にTCPポート40440が開放されている必要があります。バージョン4.7.1以降では、TCPポート40440は、**[バックアップ（ABGW）パブリック]** トラフィックタイプで自動的に開放されます。トラフィックタイプの詳細については、Acronis Cyber Infrastructureの文書を参照してください。
- 不変ストレージには、プロテクションエージェントバージョン21.12（ビルド15.0.28532）以降が必要です。
- TIBX（バージョン12）バックアップのみがサポートされています。

不変ストレージの有効化

不変ストレージの設定は、Cyber Protectコンソールまたは管理ポータルで実行できます。どちらを経由しても同じ設定にアクセスできます。以下の手順では、Cyber Protectコンソールを使用します。管理ポータルで不変ストレージを設定する方法については、管理者ガイドの「不変ストレージの構成」を参照してください。

不変ストレージを構成すると、管理者アカウントが属するテナントで二要素認証が必須となります。

不変のストレージを有効化するには

1. Cyber Protectコンソールに管理者としてログインします。
2. **[設定]** > **[システム設定]** に移動します。
3. デフォルトのバックアップオプションのリストをスクロールし、**[不変ストレージ]** をクリックします。
4. **[不変ストレージ]** スイッチを有効にします。
5. 保持期間を14日から3650日の間で指定します。

   デフォルトの保持期間は14日間です。保持期間が長くなると、ストレージの使用量が増える可能性があります。
6. 不変ストレージモードを選択し、プロンプトが表示されたら選択を確定します。

   管理モードでは、不変ストレージを有効または無効にし、保持期間を変更することができます。ガバナンスモードからコンプライアンスモードに切り替えられます。

   警告

   コンプライアンスモードへの切り替えは元に戻すことができません。コンプライアンスモードを選択した後は、不変ストレージを無効にしたり、モードや保持期間を変更したりすることはできません。

7. **[保存]** をクリックします。
8. 既存のアーカイブで不変ストレージをサポートするには、該当のアーカイブに新しいバックアップを作成します。
   新しいバックアップを作成するには、手動またはスケジュールで保護計画を実行します。

警告
アーカイブで不変ストレージがサポートされていない状態でバックアップを削除すると、バックアップは永久に削除されます。

不変ストレージの無効化

注意
ガバナンスモードでのみ、不変ストレージを無効にできます。

不変ストレージを無効化するには

1. Cyber Protectコンソールに管理者としてログインします。
2. ナビゲーションメニューで、**[設定]** > **[システム設定]** をクリックします。
3. デフォルトのバックアップオプションのリストをスクロールし、**[不変ストレージ]** をクリックします。
4. **[不変ストレージ]** スイッチを無効にします。
5. **[無効化]** をクリックしてこの選択内容を確認します。

警告
不変ストレージを無効にしても、すぐに変更が適用されるわけではありません。14日間の猶予期間中、不変ストレージは引き続き有効であり、元の保持期間に従って削除済みバックアップにアクセスできます。猶予期間が終了すると、不変ストレージ内のすべてのバックアップは恒久的に削除されます。

不変ストレージ内の削除されたバックアップへのアクセス

保持期間中は、削除されたバックアップにアクセスし、そこからデータをリカバリできます。

注意
削除されたバックアップへのアクセスを許可するには、受信接続用にバックアップストレージのポート40440を開く必要があります。

削除されたバックアップにアクセスするには

1. **[バックアップストレージ]** タブで、削除されたバックアップを含むクラウドストレージを選択します。
2. （削除されたアーカイブの場合のみ）削除されたアーカイブを表示するには、**[削除済みを表示]** をクリックします。
3. 復元するバックアップが含まれているアーカイブを選択してください。
4. **[バックアップを表示]** をクリックししてから、**[削除済みを表示]** をクリックします。

5. リカバリするバックアップの選択
6. 「"復元"（484ページ）」で説明されているように、復元操作を続行します。

地理的冗長性ストレージ

地理的冗長性ストレージは、プライマリロケーションから地理的に離れたセカンダリロケーションに対し非同期的にコピーを作成することで、データの耐久性を確保します。地理的冗長性により、プライマリロケーションが利用できない場合でもデータにアクセスできます。

重要
レプリケートされたデータは、元のデータと同じストレージスペースを使用します。

地理的冗長性ストレージの有効化と無効化

前提条件

- 地理的冗長性ストレージは、パートナー管理者が管理ポータルまたはAPI経由で有効にした後にのみ、Cyber Protectコンソールで使用できるようになります。
- Cyber Protectコンソールで地理的冗長性ストレージを有効または無効にできるのは管理者のみです。管理者権限が付与されていることを確認してください。

地理的冗長性ストレージを有効にするには

1. （API経由で地理的冗長性ストレージを有効にした場合のみ）上部に表示される「クラウド上のすべてのデータで地理的冗長性が利用可能です」というアラートで、**[地理的冗長性ストレージを有効にする]** をクリックします。
2. Cyber Protectコンソールで **[設定]** > **[システム設定]** に進みます。
3. デフォルトのバックアップオプションのリストをスクロールし、**[地理的冗長性クラウドストレージ]** をクリックします。
4. **[地理的冗長性クラウドストレージ]** スイッチを有効にします。
5. **[保存]** をクリックします。
   これで、セカンダリロケーションにデータのレプリカが作成にされ、プライマリロケーションに障害が発生した場合に利用可能になります。

地理的冗長性ストレージを無効にするには

警告
レプリケーションされたデータは、地理的冗長性を無効にしてから1日以内に削除されます。

1. Cyber Protectコンソールで **[設定]** > **[システム設定]** に進みます。
2. バックアップオプションのリストをスクロールし、**[地理的冗長性クラウドストレージ]** をクリックします。
3. **[地理的冗長性クラウドストレージ]** スイッチを無効にします。
4. 「**無効化**」と入力して選択を確認してから、**[無効化]** をクリックします。

ジオレプリケーションのステータス

地理的冗長性とは、データがセカンダリロケーションにレプリケートされることを意味します。ジオレプリケーションのステータスはこのプロセスの各ステージを示します。以下のステータスがあります:

- **同期中** - データがセカンダリロケーションにレプリケートされた。
- **同期実行中** - データをセカンダリロケーションにレプリケートしている。この操作にかかる時間は、データのサイズによって異なります。
- **保留中** - データをセカンダリロケーションにレプリケートしている。
- **無効** - データのレプリケーションが無効になっている。

Cyber Protectコンソールでレプリケーションのステータスを確認するには

1. Cyber Protectコンソールで、**[バックアップストレージ]** に移動します。
2. ロケーションとバックアップセットを選択します。
3. **[詳細]** をクリックし、**ジオレプリケーションのステータス**でステータスを確認します。

制限事項

- 現在、レプリケートデータのセカンダリロケーションは、米国とカナダでのみご利用いただけます。
- 地理的冗長性を使用する場合のディザスタリカバリサービスの制限については、ディザスタリカバリに関する文書を参照してください。

用語集

U

USBデバイスのデータベース

（デバイス制御）デバイス制御モジュールは、USBデバイスのデータベースを保持し、デバイスアクセス制御の除外リストにこれらを追加することができます。データベースにはUSBデバイスがデバイスIDで登録されており、手動で入力したり、Cyber Protectコンソール経由で既知のデバイスから選択したりすることができます。

V

VPNアプライアンス

[Disaster Recovery] 安全なVPNトンネルを介してローカルネットワークとクラウドサイト間の接続を可能にする特別な仮想マシン。VPNアプライアンスはローカルサイトに配置されています。

VPNゲートウェイ（旧称VPNサーバーまたは接続ゲートウェイ）

[Disaster Recovery] 安全なVPNトンネルを介してローカルサイトとクラウドサイトのネットワーク間の接続を提供する特別な仮想マシン。VPNゲートウェイはクラウドサイトに配置されます。

く

クラウドサーバー

[Disaster Recovery] 復元またはプライマリサーバーへの一般的な参照。

クラウドサイト（またはDRサイト）

[Disaster Recovery] リモートサイトはクラウドでホストされ、災害時に復元インフラストラクチャを実行するために使用されます。

さ

サイト間（S2S）接続

[Disaster Recovery] セキュアなVPNトンネル経由でローカルネットワークをクラウドに拡張する接続。

て

データ漏洩防止（旧: データ漏出防止）

組織内外の正当な権限を持たない使用者による、秘匿データ、保護データ、および機密データへの偶発的ならびに意図的な開示やアクセス、または信頼済みでない環境への移転を検知し、それらを防止することを目的とした、統合技術と組織的な対策を導入したシステムです。

データ漏洩防止エージェント

データ漏洩防止システムのクライアントコンポーネントで、コンテキストとコンテンツ分析技術を組み合わせて適用し、集中管理されたデータ漏洩防止ポリシーを実施することで、秘匿データ、保護データ、または機密データに対する、不正使用、送信、および保存からホストコンピューターを保護します。サイバープロテクションは、フル機能のデータ漏洩防止エージェントを提供しています。ただし、保護されたコンピューター上のエージェントの機能は、サイバープロテクションのライセンスで利用可能なデータ漏洩防止機能のセットに制限されており、そのコンピューターに適用されている保護計画に依存しています。

テストIPアドレス

[Disaster Recovery] 本番用IPアドレスの重複を防ぐために、フェールオーバーのテストの際に必要なIPアドレス。

テストネットワーク

[Disaster Recovery] フェールオーバープロセスをテストするために使用される、隔離された仮想ネットワーク。

デバイス制御モジュール

デバイス制御モジュールは保護計画の一環として、保護された各コンピューター上のデータ漏洩防止エージェントの機能的サブセットを活用して、ローカルコンピューターのチャネルを介したデータの不正アクセスおよび送信を検出し、防止します。制御の対象となるのは、周辺デバイスやポートへのユーザーアクセス、文書の印刷、クリップボードのコピー/貼り付け操作、メディアのフォーマットや取り出し操作、ローカルに接続されたモバイルデバイスとの同期などです。デバイス制御モジュールは、保護されたコンピューター上でユーザーに対してアクセスが許可されるデバイスやポートの種類、そしてユーザーがそれらのデバイスに対して実行できる操作をコンテキストに基づききめ細かく制御します。

は

バックアップセット

個別の保持ルールが提供されるバックアップのグループ。カスタムバックアップスキームの場合、バックアップセットはバックアップメソッド（完全、差分、増分）に対応します。その他の場合、バックアップセットは、月単位、日単位、週単位、および時間単位になります。月単位のバックアップでは、月の始めに最初のバックアップが作成されます。週単位のバックアップでは、[週単位のバックアップ] オプション（ギアアイコンをクリックし、次に [バックアップオプション] > [週単位のバックアップ] の順にクリック）で選択した曜日に最初のバックアップが作成されます。週単位のバックアップで月の始めに最初のバックアップが作成される場合、このバックアップは月単位とみなされます。この場合、週単位のバックアップは、翌週の選択した曜日に作成されます。日単位のバックアップでは、このバックアップが月単位または週単位のバックアップの定義に属する場合を除き、日の始めに最初のバックアップが作成されます。時間単位のバックアップでは、このバックアップが月単位、週単位、または日単位のバックアップの定義に属する場合を除き、時間の始めに最初のバックアップが作成されます。

パブリックIPアドレス

[Disaster Recovery] インターネットからクラウドサーバーを利用可能にするために必要なIPアドレス。

ふ

フェールオーバー

ワークロードを本番サーバーから予備サーバー（仮想マシンのレプリカやクラウドで実行されている復元サーバーなど）に切り替えます。

フェールバック

ワークロードを予備サーバー（仮想マシンのレプリカやクラウドで実行されている復元サーバーなど）から本番サーバーに切り替えます。

プライマリサーバー

[Disaster Recovery] ローカルサイト上にリンクされたマシンがない仮想マシン（リカバリサーバーなど）。プライマリサーバーは、アプリケーションの保護や、さまざまな補助サービスの実行などに使用されます（Webサーバーなど）。

へ

ベリファイ

バックアップからのデータ復元の可能性をチェックする操作。 ファイルバックアップの検証では、バックアップからダミーの復元先に対してすべてのファイルの復元を疑似的に実行します。ディスク バックアップのベリファイでは、バッ

クアップに保存されているすべてのデータ ブロックのチェックサムを計算します。どちらの手順もリソースを大量に消費します。 検証の成功は、復元できる可能性が高いことを示していますが、復元処理に影響するすべての要因を確認するわけではありません。

ほ

ポイントツーサイト（P2S）接続

[Disaster Recovery] エンドポイントデバイス（コンピュータまたはラップトップなど）を使用して、外部からクラウドおよびローカルサイトに接続する安全なVPN接続です。

も

モジュール

モジュールとは、特定のデータ保護機能を提供する保護計画内のパーツのことです。バックアップ、ウイルスおよびマルウェア対策保護などのモジュールがあります。

ら

ランブック

[Disaster Recovery] ディザスタリカバリアクションを自動化する設定可能なステップからなる計画シナリオ。

ろ

ローカルサイト

[Disaster Recovery] 会社の構内に配置されたローカルインフラストラクチャ。

漢字

仮想コンピュータ

VMwareエージェントやHyper-Vエージェントなどの外部エージェントによってハイパーバイザーレベルでバックアップされる仮想マシン。 エージェントがインストールされている仮想マシンは、バックアップの観点から物理マシンとして扱われます。

確定

バックアップから実行されている一時的な仮想マシンを恒久的な仮想マシンにする操作。物理的には、マシンの実行中に生じた変更とともに、すべての仮想マシンディスクを、これらの変更を保存するデータストアに復元することを意味します。

完全バックアップ

バックアップ用に選択した全データが含まれた自己完結型の バックアップ 。完全バックアップからデータを復元する場合、他の差分や増分のバックアップデータは必要ありません。

孤立したバックアップ

孤立したバックアップは、いずれの保護計画とも関連付けられていないバックアップです。

差分バックアップ

差分バックアップ：最新の完全バックアップからの変更分がバックアップデータとして保存されます。データを復元する場合、完全バックアップと差分バックアップの両方が必要になります。

増分バックアップ

最新のバックアップに対するデータの変更が保存されるバックアップ。増分バックアップからデータを復元するには、完全バックアップと完全バックアップ以降の増分バックアップデータが必要です。

単一ファイル バックアップ形式

バックアップ形式は、最初の完全バックアップアップとその後の増分バックアップが保存された単一の.tibxファイルです。この形式の場合、増分

バックアップの速度が上がり、古くなったバックアップの削除が難しいという増分バックアップの欠点を補うことができます。古くなったバックアップで使用されているブロックは、ソフトウェアによって「空き領域」としてマークされ、新しいバックアップによって上書きされます。これにより、リソース消費を最小限に抑えながら、クリーンアップを飛躍的に高速化できます。 単一ファイルバックアップ形式は、ランダムアクセスの書き込みと読み込みをサポートしていないロケーションにバックアップする場合には使用できません。

復元サーバー

[Disaster Recovery] クラウドに保存されている保護されたサーバーバックアップによる、元のマシンのVMレプリカ。災害発生時に、復元サーバーを使用して元のサーバーからワークロードを切り替えます。

復元ポイント目標（RPO）

（ディザスタリカバリ）停止によって失われたデータの量であり、計画された停止または災害イベントからの時間として測定されます。 RPOしきい値は、フェールオーバーのための最後の適切な復元ポイントと現在時刻との間の許容される最大時間間隔を定義します。

物理コンピュータ

オペレーティングシステムにインストールされたエージェントによってバックアップされるマシン。

保護エージェント

保護エージェントとは、データ保護のためにマシンにインストールするエージェントのことです。

保護計画

保護計画とは、バックアップ、ウイルスとマルウェア対策、URLフィルタリング、Windows Defenderウイルス対策、Microsoft Security Essentials、脆弱性評価、パッチ管理、データ保護マップ、デバイス制御など、いくつかのデータ保護モジュールを組み合わせた計画のことです。

本番ネットワーク

[Disaster Recovery] VPNトンネルによって拡張され、ローカルおよびクラウドサイトの両方をカバーする内部ネットワーク。ローカルサーバーとクラウドサーバーは本番ネットワーク上で互いに通信できます。

索引

H

I

L

M

N

U

V

W

あ

い

う

え

お

か

き

く

こ

さ

し

す

せ

そ

た

ち

て

は

ひ

ふ

ま

め

も

ゆ

ら

り

る

れ

ろ

わ

漢字