Acronis

acronis.com

Acronis Cyber Protect 15

Update 6

ユーザー ガイド

リビジョン: 2023/06/21

目次

Acronis Cyber Protect 15エディション **17**
オペレーティングシステムでサポートされるCyber Protectの機能 17
ライセンス **21**
ライセンス種類 21
AcronisCyber Protect 15 Update 3以降のライセンス 21
管理サーバーの種類 22
Acronisアカウント、ローカルとクラウドコンソール 23
ライセンスの管理 25
AcronisCyber Protect 15 Update 2以前のライセンス 41
管理サーバーにライセンスキーを追加する 41
サブスクリプションライセンスの管理 41
永久ライセンスの管理 42
インストール **44**
インストール概要 44
オンプレミスデプロイ 44
クラウドデプロイ 45
コンポーネント 47
エージェント 47
その他のコンポーネント 50
Acronis Cyber Protectをユーザーの環境で他のセキュリティソリューションと併用する 51
制限事項 52
ソフトウェア要件 52
推奨 Web ブラウザ 52
サポートされるオペレーティング システムと環境 53
サポートされる Microsoft SQL Server のバージョン 61
サポートされるMicrosoft Exchange Serverのバージョン 61
サポートされる Microsoft SharePoint のバージョン 62
サポート対象の Oracle データベースのバージョン 62
サポート対象の SAP HANA バージョン 62
サポートされる仮想環境プラットフォーム 62
Linuxパッケージ 67
暗号化ソフトウェアとの互換性 71
Dell EMC Data Domainストレージの機能 73
システム要件 74
サポートされるファイル システム 75

Acronis Cyber Protectのネットワーク接続図 78
ネットワーク接続図 - Cyber Protectプロセス 79
オンプレミスデプロイ 82
Management Serverのインストール 82
サービスログオンアカウントに必要なユーザー権限 85
スキャンサービスのデータベース 89
Cyber Protect Webコンソールからマシンを追加する 93
エージェントをローカルでインストールする 102
無人インストールまたはインストール解除 106
共通パラメータ 108
管理サーバーインストールパラメータ 112
エージェントインストールパラメータ 113
Storage Node インストールパラメータ 114
カタログサービスのインストールパラメータ 114
マシンの手動登録 120
ソフトウェアのアップデートの確認 123
管理サーバーをマイグレーションする 124
クラウドデプロイ 129
アカウントのアクティブ化 129
インストールする前に 129
プロキシサーバー設定 132
エージェントのインストール 134
無人インストールまたはインストール解除 139
基本パラメータ 141
登録パラメータ 142
その他のパラメータ 143
基本パラメータ 146
登録パラメータ 147
その他のパラメータ 148
情報パラメータ 149
レガシー機能のパラメータ 150
マシンの手動登録 153
oVirt（仮想アプライアンス）エージェントをデプロイ中 156
Virtuozzo Hybrid Infrastructureエージェント（仮想アプライアンス）の配置 156
マシンの自動検出 156
前提条件 156
自動検出の仕組み 157

自動検出と手動検出 159
検出されたマシンの管理 163
トラブルシューティング 163
OVFテンプレートからエージェント for VMware（仮想アプライアンス）のデプロイ 165
開始する前に 165
OVFテンプレートの配置 166
仮想アプライアンスの設定 166
Scale Computing HC3 エージェント（仮想アプライアンス）の配置 168
開始する前に 168
仮想アプライアンスのデプロイ 169
仮想アプライアンスの設定 169
Scale Computing HC3 エージェント – 必要なロール 174
グループポリシーによるエージェントの配置 174
前提条件 174
手順1:登録トークンの生成 175
手順2:.mstトランスフォームファイルの作成とインストールパッケージの抽出 175
手順 3:グループ ポリシー オブジェクトの設定 175
既存の仮想アプライアンスをアップデートする 176
オンプレミスデプロイ 176
クラウドデプロイ 177
エージェントのアップデート 177
Acronis Cyber Protect 15にアップグレードする 178
製品のアンインストール 179
Windowsの場合 179
Linuxの場合 180
macOSの場合 180
エージェント for VMware（仮想アプライアンス）の削除 180
Cyber Protectウェブ コンソールからマシンを削除する 180
Cyber Protect ウェブ コンソールへのアクセス 182
オンプレミスデプロイ 182
Windowsの場合 182
Linuxの場合 183
クラウドデプロイ 183
言語の変更 183
統合Windows認証のためのWebブラウザの設定 183
Internet Explorer、Microsoft Edge、Opera、およびGoogle Chromeの設定 183
Mozilla Firefoxの設定 184

ローカルイントラネットサイトのリストへのコンソールの追加 184
信頼されたサイトのリストへのコンソールの追加 186
HTTPS接続によるWebコンソールへのログインのみを許可する 189
Webコンソールにカスタムメッセージを追加します 190
前提条件 190
SSL証明書の設定 193
自己署名証明書の使用 193
信頼できる認証局が発行した証明書の使用 194
Cyber Protectウェブコンソール表示 197
保護計画とモジュール 199
保護計画の作成 199
計画の競合の解決 201
複数の計画のデバイスへの適用 201
計画の競合の解決 201
保護計画を使用した操作 202
バックアップ 204
バックアップモジュールのチートシート 206
制限事項 208
バックアップ対象の選択 209
マシン全体を選択する 209
ディスクとボリュームの選択 210
ファイルとフォルダの選択 213
システム状態の選択 215
ESXi構成の選択 215
継続的データ保護（CDP） 216
バックアップ先の選択 223
サポートされるロケーション 223
詳細ストレージオプション 224
Secure Zoneのバージョン情報 226
Acronis Cyber Infrastructureについて 228
スケジュール 229
クラウドストレージにバックアップする場合 230
別のロケーションにバックアップする場合 230
追加のスケジュールオプション 231
イベント別のスケジュール 232
開始条件 235
保持ルール 241

その他の注意点 242
暗号化 243
保護計画での暗号化 243
マシンプロパティとして暗号化 243
暗号化の動作方法 245
ノータリゼーション 245
ノータリゼーションの使用方法 245
仕組み 245
仮想コンピュータへの変換 246
変換方法 246
変換に関する注意点 246
保護計画での仮想マシンへの変換 248
VM への定期的な変換の動作 249
レプリケーション 250
使用例 250
サポートされるロケーション 250
Advancedライセンスを持つユーザーのための考慮事項 251
手動でのバックアップの開始 252
バックアップ オプション 253
使用可能なバックアップ オプション 253
アラート 259
バックアップの統合 260
バックアップ ファイル名 261
バックアップ形式 264
バックアップのベリファイ 266
Changed Block Tracking（CBT） 267
クラスターバックアップモード 267
圧縮レベル 269
電子メールによる通知 269
エラー処理 270
高速の増分/差分バックアップ 271
ファイルフィルタ 271
ファイルレベルのバックアップのスナップショット 273
フォレンジックデータ 274
ログの切り詰め 282
LVMのスナップショット 282
マウントポイント 283

マルチボリュームスナップショット 284
ワンクリック復元 284
パフォーマンスとバックアップウィンドウ 285
物理データ配送 289
処理の前後のコマンド 290
データ取り込みの前後に実行するコマンド 291
SANハードウェアスナップショット 294
スケジューリング 294
セクタ単位のバックアップ 295
分割 295
テープ管理 295
タスク失敗時の処理 300
タスクの開始条件 300
ボリューム シャドウ コピー サービス（VSS） 301
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） 302
週単位のバックアップ 303
Windowsイベントログ 303
復元 **304**
復元のチートシート 304
安全な復元 305
仕組み 305
ブータブルメディアの作成 306
マシンの復元 307
物理マシンをリカバリする 307
物理マシンを仮想マシンにリカバリする 309
仮想コンピュータの復元 311
再起動を伴う復元 314
ブータブルメディアを使用したディスクとボリュームの復元 314
Universal Restoreの使用 316
ファイルの復元 319
Webインターフェイスを使用したファイルの復元 319
クラウドストレージからのファイルのダウンロード 320
Notaryサービスを使用したファイル真正性のベリファイ 321
ASignを使用したファイルの署名 322
ブータブルメディアを使用したファイルの復元 323
ローカルバックアップからファイルを抽出 324
システム状態の復元 324

ESXi構成の復元 325
復元オプション 325
使用可能な復元オプション 326
バックアップのベリファイ 327
起動モード 328
ファイルの日付と時刻 329
エラー処理 329
ファイルの除外 330
ファイルレベルのセキュリティ 330
Flashback 331
フルパスの復元 331
マウントポイント 331
パフォーマンス 332
処理の前後のコマンド 332
テープ管理 333
SIDの変更 334
VMの電源管理 334
Windowsイベントログ 334
復元後に電源オンにする 335
災害復旧 **336**
バックアップの操作 **337**
バックアップストレージタブ 337
バックアップからのボリュームのマウント 338
要件 338
使用例 338
バックアップのベリファイ 339
バックアップのエクスポート 340
バックアップの削除 341
[計画] タブ **343**
オフホストのデータ処理 343
バックアップスキャンの計画 344
バックアップのレプリケーション 344
ベリファイ 346
クリーンアップ 348
仮想コンピュータへの変換 349
ブータブル メディア **351**
ブータブル メディア 351

ブータブルメディアの作成か、既成のブータブルメディアのダウンロードか 351
Linuxベースのブータブルメディアか、WinPEベースのブータブルメディアか 353
Linux ベース 353
WinPEベース 353
ブータブルメディアビルダー 354
メディアビルダを使用する理由 354
32ビットまたは64ビット 354
Linux ベースのブータブル メディア 355
トップレベルオブジェクト 365
変数オブジェクト 365
コントロールの種類 366
WinPE ベースのブータブル メディア 372
メディアから起動したコンピュータへの接続 378
ネットワーク設定 378
ローカル接続 379
リモート接続 379
Management Serverでメディアを登録 379
メディアUIからのメディアの登録 379
ブータブルメディアのローカル処理 380
ディスプレイ モードの設定 381
オンプレミスでのブータブルメディアによるバックアップ 381
オンプレミスでのブータブルメディアによる復元 391
ブータブルメディアによるディスク管理 400
シンプル ボリューム 417
スパン ボリューム 417
ストライプ ボリューム 417
ミラー ボリューム 418
ミラー ストライプ ボリューム 418
RAID-5 418
ブータブルメディアのリモート操作 425
iSCSIデバイスの構成 427
Startup Recovery Manager 428
Startup Recovery Managerの有効化 429
Startup Recovery Managerの無効化 429
Acronis PXE Server 430
Acronis PXE Server のインストール 430
PXE から起動するコンピュータの設定 431

サブネットをまたがる操作 ... 431
モバイル デバイスの保護 ... 432
サポートされるモバイル デバイス ... 432
バックアップできる内容 ... 432
留意事項 ... 432
バックアップアプリの入手先 ... 433
データのバックアップを開始する方法 ... 433
モバイルデバイスにデータを復元する方法 ... 434
Cyber Protectウェブコンソールからデータをレビューする方法 ... 434
Microsoft アプリケーションの保護 ... 436
Microsoft SQL ServerとMicrosoft Exchange Serverの保護 ... 436
Microsoft SharePointの保護 ... 436
ドメインコントローラの保護 ... 437
アプリケーションの復元 ... 437
前提条件 ... 438
一般的な要件 ... 438
アプリケーション認識型バックアップのその他の要件 ... 438
データベースのバックアップ ... 440
SQLデータベースの選択 ... 440
Exchange Serverデータの選択 ... 441
Always On可用性グループ（AAG）の保護 ... 442
データベース可用性グループ（DAG）の保護 ... 443
アプリケーション認識型バックアップ ... 445
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。 ... 445
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。 ... 446
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 ... 446
メールボックスのバックアップ ... 447
Exchange Serverメールボックスの選択 ... 448
必要なユーザー権限 ... 449
SQL データベースの復元 ... 449
システムデータベースの復元 ... 451
SQL Server データベースの接続 ... 452
Exchangeデータベースの復元 ... 453
Exchange Server データベースのマウント ... 455
Exchange メールボックスとメールボックスのアイテムを復元 ... 455
Exchange Server に復元 ... 456
Microsoft 365への復元 ... 456

メールボックスの復元 ... 457
メールボックスのアイテムの復元 ... 459
Microsoft Exchange Server のライブラリのコピー ... 461
SQLサーバーまたはExchangeサーバーのアクセス認証の変更 ... 462
Microsoft 365メールボックスの保護 ... 463
Microsoft 365メールボックスをバックアップする理由 ... 463
復元 ... 463
制限事項 ... 464
Microsoft 365組織の追加 ... 464
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 ... 464
Microsoft 365アクセス認証の変更 ... 466
メールボックスの選択 ... 466
メールボックスおよびメールボックスアイテムの復元 ... 466
メールボックスの復元 ... 466
メールボックスのアイテムの復元 ... 467
Google Workspaceデータを保護 ... 469
Oracle データベースの保護 ... 470
仮想コンピュータの特別な操作 ... 471
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） ... 471
使用例 ... 471
前提条件 ... 471
コンピュータの実行 ... 472
コンピュータの削除 ... 473
コンピュータの確定 ... 473
VMware vSphere での作業 ... 474
仮想コンピュータのレプリケーション ... 474
LAN フリー バックアップ ... 480
SANハードウェアスナップショットの使用 ... 483
ローカルに接続されたストレージの使用 ... 488
仮想コンピュータのバインド ... 489
VM 移行のサポート ... 491
仮想環境の管理 ... 492
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 ... 493
VMware エージェント - 必要な権限 ... 493
クラスタ化された Hyper-V コンピュータのバックアップ ... 497
復元されたコンピュータの高可用性 ... 497
同時にバックアップされる仮想マシンの合計数の制限 ... 497

コンピュータの移行 499
Windows AzureおよびAmazon EC2仮想コンピュータ 500
ネットワーク要件 500
SAP HANA の保護 502
マルウェア対策とWeb保護 503
ウイルスおよびマルウェア対策保護 503
リアルタイム保護スキャン 503
オンデマンドマルウェアスキャン 504
ウイルスおよびマルウェア対策保護の設定 504
Active Protection 511
Windows Defender Antivirus 512
スケジュールスキャン 512
デフォルトのアクション 512
リアルタイム保護 513
詳細 513
除外 514
Microsoft Security Essentials 514
URLフィルタリング 515
仕組み 515
URLフィルタ処理の設定 517
検疫 522
ファイルが検疫フォルダに移される仕組み 523
検疫されたファイルの管理 523
マシンの検疫ロケーション 523
企業ホワイトリスト 523
ホワイトリストへの自動追加 524
ホワイトリストへの手動追加 524
隔離されたファイルをホワイトリストに追加する 524
ホワイトリスト設定 524
ホワイトリストに登録されている項目の詳細を表示 525
バックアップのマルウェア対策スキャン 525
制限事項 526
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 527
脆弱性診断とパッチ管理 528
脆弱性診断 528
サポート対象のMicrosoft製品とサードパーティ製品 528
サポートされているLinux製品 530

脆弱性診断の設定 530
Windowsマシンの脆弱性診断 532
Linuxマシンの脆弱性診断 532
検出された脆弱性の管理 532
パッチ管理 533
仕組み 534
パッチ管理の設定 535
パッチのリストの管理 537
自動パッチ承認 539
手動パッチ承認 542
オンデマンドのパッチインストール 542
リスト内のパッチのライフタイム 543
スマート保護 **544**
脅威フィード 544
仕組み 544
すべてのアラートの削除 546
データ保護マップ 546
仕組み 546
検出された保護されていないファイルの管理 547
データ保護マップの設定 547
リモートデスクトップアクセス **550**
リモートアクセス（RDPクライアントとHTML5クライアント） 550
仕組み 551
リモートのマシンに接続する方法 553
リモート接続を共有 553
リモートワイプ **555**
デバイスグループ **556**
ビルトイングループ 556
カスタム グループ 556
静的グループの作成 557
静的グループへのデバイスの追加 557
ダイナミックグループの作成 557
検索クエリ 558
演算子 567
グループへの保護計画の適用 568
監視とレポート **569**
概要ダッシュボード 569

Cyber Protection 571
保護ステータス 571
ディスク状態監視 571
データ保護マップ 576
脆弱性診断ウィジェット 577
パッチインストールウィジェット 577
バックアップスキャンの詳細 578
最近影響を受けたもの 578
最近のバックアップ取得なし 578
アクティビティタブ 580
レポート 581
アラートの重大度の設定 585
アラート設定ファイル 585
詳細ストレージオプション 587
テープ デバイス 587
テープ デバイスについて 587
テープ サポートの概要 587
テープ デバイスの操作 593
テープ管理 599
ストレージ ノード 608
Storage Nodeとカタログサービスのインストール 608
管理対象ロケーションの追加 610
重複除外 612
ロケーションの暗号化 615
カタログ作成 616
システム設定 619
電子メールによる通知 619
電子メールサーバー 620
セキュリティ 620
非アクティブのユーザーをログアウトさせる時間 621
現在のユーザーの前回ログインに関する通知を表示する 621
ローカルまたはドメインのパスワードの失効に関する警告を表示する 621
アップデート 621
デフォルトのバックアップ オプション 621
保護の設定 623
保護定義のアップデート 623
アップデータロールを持つエージェント 623

アップデートのスケジュール設定 624
ダウンロードロケーションの変更 625
キャッシュストレージオプション 626
最新の保護定義のソース 626
リモート接続 626
エアギャップ環境での保護定義のアップデート 627
オンライン管理サーバーへの定義のダウンロード 627
HTTPサーバーに定義ファイルを転送する 629
エアギャップ環境で動作する管理サーバーの定義ソースの構成 629
ユーザーアカウントと組織部署の管理 631
オンプレミスデプロイ 631
部署および管理アカウント 631
管理アカウントを追加 634
部署の作成 635
クラウドデプロイ 635
制限値（クォータ） 635
通知 637
レポート 638
コマンド ライン リファレンス 639
トラブルシューティング 640
用語集 641
索引 643

著作権情報

Acronis の特許取得済みの技術

この製品で使用されている技術は、以下の番号の 1 つ以上の米国特許によって保護されています。
7,047,380号、7,246,211号、7,275,139号、7,281,104号、7,318,135号、7,353,355号、7,366,859号、
7,383,327号、7,475,282号、7,603,533号、7,636,824号、7,650,473号、7,721,138号、7,779,221号、
7,831,789号、7,836,053号、7,886,120号、7,895,403号、7,934,064号、7,937,612号、7,941,510号、
7,949,635号、7,953,948号、7,979,690号、8,005,797号、8,051,044号、8,069,320号、8,073,815号、
8,074,035号、8,074,276号、8,145,607号、8,180,984号、8,225,133号、8,261,035号、8,296,264号、
8,312,259号、8,347,137号、8,484,427号、8,645,748号、8,732,121号、8,850,060号、8,856,927号、
8,996,830号、9,213,697号、9,400,886号、9,424,678号、9,436,558号、9,471,441号、9,501,234号、および出願中特許。

Acronis Cyber Protect 15エディション

Acronis Cyber Protect 15は次のエディションで利用可能です。

- Cyber Protect Essentials
- Cyber Protect Standard
- Cyber Protect Advanced
- Cyber Backup Standard
- Cyber Backup Advanced

各エディションに含まれる機能の詳細については、「Acronis Cyber Protect 15エディションのクラウド配置を含んだ比較」を参照してください。

Acronis Cyber Protect 15のすべてのエディションは、保護対象のワークロードの数とその種類（ワークステーション、サーバー、仮想ホスト）ごとにライセンスされています。Cyber Protect エディションで利用できるのは、サブスクリプションライセンスのみです。サイバーバックアップエディションは、サブスクリプションと永続ライセンスの両方が利用可能です。利用できるオプションの詳細については、"ライセンス"（21ページ）を参照してください。

バージョン 15 の永続ライセンスキーは、Acronis Cyber Backup 12.5 のバックアップエージェントでは使用できません。ただし、これらのエージェントは以前のライセンスキーで引き続き動作します。管理サーバーがバージョン15にアップグレードされた場合も動作します。

バックアップサブスクリプションライセンスは、エージェントがバージョン15にアップグレードされた場合も、バージョン12.5のエージェントで使用可能です。Cyber Protectサブスクリプションライセンスはバージョン15のエージェントでのみ使用できます。

バージョン15の管理サーバーに登録されているバージョン12.5のバックアップエージェントでは、バックアップのレプリケーション、バックアップの検証、クリーンアップ、仮想マシンへの変換など、オフホストデータ処理の操作を実行することはできません。

注意
エディションが異なると、機能も異なります。このドキュメントに記載されているいくつかの機能は、ご利用のライセンスでは使用できない場合があります。各エディションに含まれる機能の詳細については、「Acronis Cyber Protect 15エディションのクラウド配置を含んだ比較」を参照してください。

オペレーティングシステムでサポートされるCyber Protectの機能

Cyber Protectの機能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:Windows 7以降、Windows Server 2008 R2以降。
  Windows Defender Antivirusの管理はWindows 8.1以降でサポートされています。
- Linux:CentOS 7.x、CentOS 8.0、Virtuozzo 7.x、Acronis Cyber Infrastructure 3.x。
  他のLinuxディストリビューションとバージョンもCyber Protect機能をサポートしている場合があり

ますが、テストされていません。

- macOS:10.13.x以降（ウイルスおよびマルウェア対策保護のみがサポートされています）。

重要
Cyber Protectの機能は、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、またはScale Computingエージェントなどによる、エージェントレスモードで保護された仮想マシンについては、バックアップのみがサポートされます。

Cyber Protectの機能	Windows	Linux	macOS
フォレンジックバックアップ	はい	いいえ	いいえ
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
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
Acronis Anti-malware Protection			
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	いいえ	いいえ
クリプトマイニングプロセス検出	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	いいえ	はい
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	いいえ	いいえ
Acronisバックアップファイルの自己防御機能	はい	いいえ	いいえ
Acronisソフトウェアの自己防御機能	はい	いいえ	いいえ
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*
外付けドライブ保護（HDD、フラッシュドライブ、SD	はい	いいえ	いいえ

カード)			
ネットワークフォルダの保護	はい	いいえ	いいえ
サーバー側保護機能	はい	いいえ	いいえ
Zoom、Webex、Microsoft Teamsの保護、およびその他のリモートワーク保護機能	はい	いいえ	いいえ
オンデマンドマルウェア対策スキャン	はい	いいえ	はい
アーカイブファイルのスキャン	はい	いいえ	はい
ファイル/フォルダの除外	はい	いいえ	はい**
プロセスの除外	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
振る舞い検知	はい	いいえ	いいえ
検疫	はい	いいえ	はい
URLフィルタリング（http/https）	はい	いいえ	いいえ
Windows Defenderウイルス対策管理	はい	いいえ	いいえ
Microsoft Security Essentials管理	はい	いいえ	いいえ
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***	いいえ
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	いいえ
パッチ管理			
パッチの自動承認	はい	いいえ	いいえ
パッチの手動インストール	はい	いいえ	いいえ
自動パッチインストールのスケジューリング	はい	いいえ	いいえ
フェー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
データ保護マップ			

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
データ保護マップでの保護アクション	はい	いいえ	いいえ
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
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
バックアップスキャン			
暗号化されたバックアップのスキャン	はい	いいえ	いいえ
ローカルストレージ、ネットワーク共有、Acronis Cloud Storageでのディスクバックアップのスキャン	はい	いいえ	いいえ
安全な復元			
Acronisの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アンチマルウェアスキャン	はい	いいえ	いいえ
リモートデスクトップ			
HTML5ベースクライアント経由の接続	はい	いいえ	いいえ
ネイティブWindows RDPクライアント経由の接続	はい	いいえ	いいえ
リモートワイプ	はい****	いいえ	いいえ
Cyber Protectモニター	はい	いいえ	はい

* macOSでは、ポータブル実行可能ファイルの静的分析は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。

** macOSでは、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、除外を使用できます。

*** 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。

**** リモートワイプはWindows 10以降を実行するマシンでのみ使用できます。

ライセンス

Acronis Cyber Protectを使用してワークロードを保護するには、ライセンスが必要です。Acronis Cyber Protectのインストールにはライセンスは必要ありません。

ライセンス種類

Acronis Cyber Protectは、サブスクリプションライセンスで利用できます。購入日を起点とする有効期間内であれば、無制限のアップデートと無料のテクニカルサポートをご利用いただけます。有効期間が終了すると、既存の保護計画は機能しなくなり、新しい保護計画を作成できなくなります。

従来の永続ライセンスの更新が可能です。クラウド配置やクラウドツークラウドバックアップなどの一部の機能は、永続ライセンスでは利用できません。

試用版ライセンスもご利用いただけます。ライセンスのアクティベーションから30日間は、すべての製品機能をご利用いただけます。

各種ライセンスオプションの詳細については、ナレッジベースのAcronis Cyber Protect 15: ライセンスおよびアップグレード/ダウングレードに関するFAQを参照してください。Acronisのライセンスポリシーについては、https://www.acronis.com/company/licensing.htmlを参照してください。

重要
Acronis Cyber Protect 15 Update 3では、新しいライセンスモデルが導入されました。オンプレミス管理サーバーのライセンス登録とアクティベーションが必要です。

AcronisCyber Protect 15 Update 3以降のライセンス

Acronis Cyber Protect 15 Update 3以降の場合、ライセンスキーは管理サーバーのローカルコンソール（https://<**管理サーバーのIPアドレス**>:<**ポート**>）に追加されません。

代わりに、Acronisカスタマーポータル（https://account.acronis.com）で、アカウントにライセンスを追加し、Acronis Cyber Protectクラウドコンソール（https://cloud.acronis.com）でライセンスを管理します。

オフライン管理サーバーでライセンスを管理するには、ローカルコンソールとクラウドコンソールの両方での操作が必要です。

ローカルコンソールとクラウドコンソールの詳細については、"Acronisアカウント、ローカルとクラウドコンソール"（23ページ）を参照してください。

AcronisCyber Protect 15 Update 3以降で、管理サーバーの使用を開始するには

1. Acronisカスタマーポータル（https://account.acronis.com）で、アカウントに1つまたは複数のライセンスを追加します。
   オンラインで購入されたライセンスは、自動的にこのアカウントに追加されます。
2. （オンプレミス配置モードの場合）管理サーバーを有効化します。
3. 管理サーバーにライセンスを割り当てます。

管理サーバーの種類

配置モードに応じて、次の種類の管理サーバーを使用できます。

- クラウド管理サーバー
- オンプレミス管理サーバー
  - オンライン管理サーバー
  - オフライン管理サーバー

Acronisアカウントでは、複数の管理サーバーを利用することができます。また、クラウド管理サーバーとオンプレミス管理サーバーを混在させた配置モードも利用可能です。

複数の管理サーバーを使用する場合、ライセンスクォータを分割して使用することができます。その方法の詳細については、"ライセンスクォータを別の管理サーバーに転送する"（33ページ）を参照してください。

クラウド管理サーバー

クラウド配置では、ネットワークに管理サーバーをインストールして維持することはありません。必要な手順は、Acronisデータセンターにすでに配置されている管理サーバーを使用し、ワークロード用のプロテクションエージェントをインストールするだけです。

クラウド管理サーバーをアクティベーションする必要はありません。クラウド管理サーバーは常にオンラインであり、ライセンス情報はサーバーと現在のAcronisアカウントの間で自動的に同期されます。

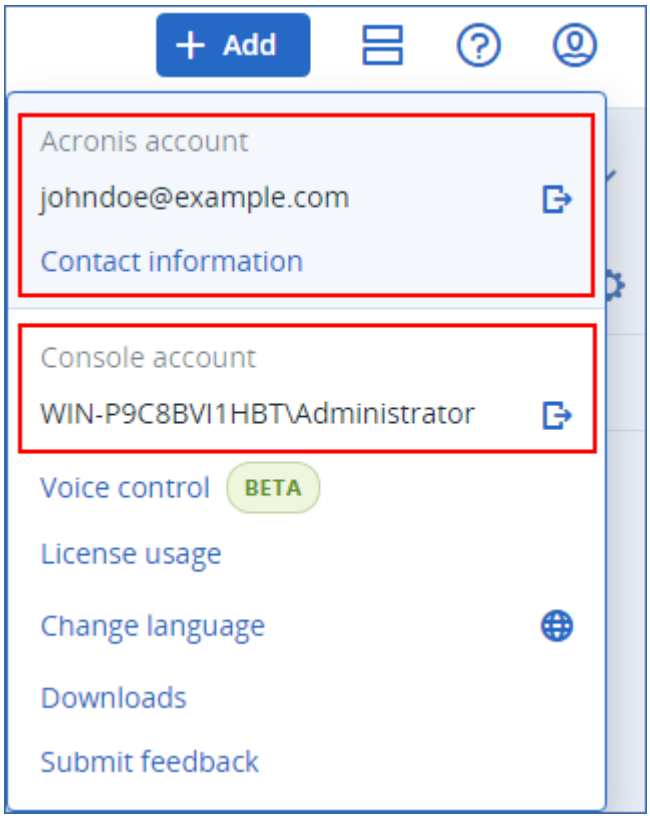
オンプレミス管理サーバー

オンプレミス配置では、現在のネットワークに管理サーバーとプロテクションエージェントの両方をインストールします。インターネット接続のないオフライン管理サーバー、またはインターネットに接続されたオンライン管理サーバーのいずれも利用可能です。

オンプレミス管理サーバーの場合は、アクティベーションする必要があります。アクティベーションの詳細情報については、"管理サーバーの有効化"（27ページ）を参照してください。

注意

有効化されたオンプレミス管理サーバーのローカルコンソールに、2種類のアカウントが表示されます。ライセンス情報の同期に使用されるAcronisアカウントと、ローカルコンソールへのアクセスに使用されるコンソールアカウントです。



オンラインのオンプレミス管理サーバー

ローカルコンソールへの初回アクセス時に、Acronisアカウントにサインインして、インターネット経由でオンライン管理サーバーを有効化します。

オフラインのオンプレミス管理サーバー

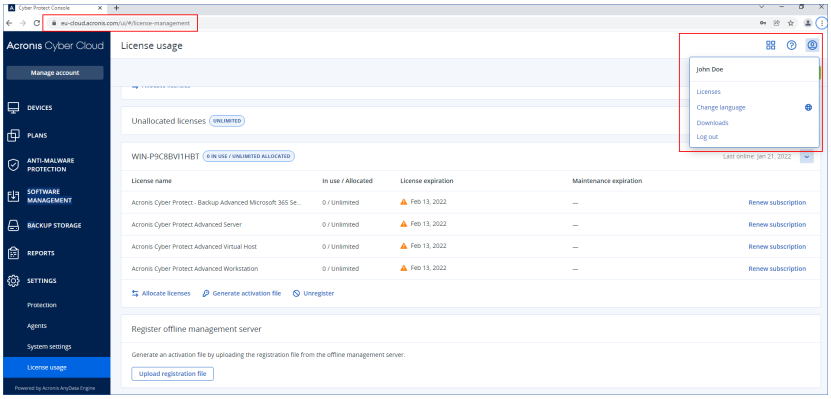
オフライン管理サーバーを有効化し、ファイル経由でライセンス情報を現在のAcronisアカウントと手動で同期します。

Acronisアカウント、ローカルとクラウドコンソール

Acronis Cyber Protectを使用し、現在のライセンスとその使用状況を管理するには、Acronisアカウントが必要です。すべてのライセンスと管理サーバーがそのアカウントに登録されます。

このアカウントで、次のコンソールにアクセスできます。

- クラウドコンソール（https://cloud.acronis.com）

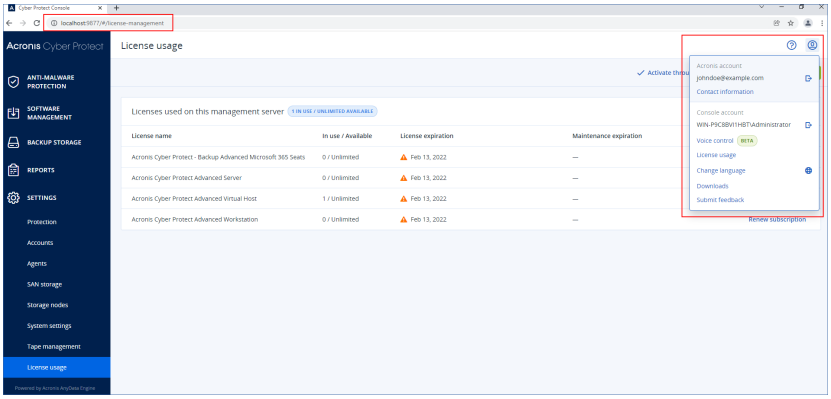


注意

クラウドコンソールにログインすると、そのURLが変更され、アカウントが実際に配置されているデータセンターが表示されます。これはたとえば、https://eu-cloud.acronis.comやhttps://jp-cloud.acronis.comとなります。

クラウドコンソールは、ライセンスを管理する主なロケーションです。サービスコンソールの **[設定]** > **[ライセンス使用状況]** タブで、使用可能なライセンスとライセンスクォータを特定の管理サーバーに割り当てたり、それらを別の管理サーバーに再割り当てしたりすることができます。また、オフライン管理サーバーの登録を最終化することもできます。

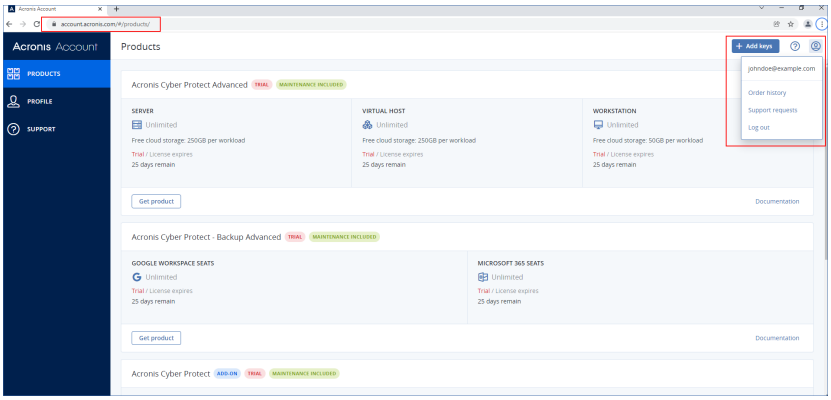
- オンプレミス管理サーバーのローカルコンソール（https://**<管理サーバーのIPアドレス>**:**<ポート>**）



ここでは、割り当てられたライセンス、ライセンスクォータと使用状況、有効期限を確認することができます。

オフラインの管理サーバーを有効化したり、ライセンスを割り当てたりする際には、クラウドコンソールとともに、ローカルコンソールを使用します。

- Acronisカスタマーポータル（https://account.acronis.com）



Acronisカスタマーポータルでは、購入した製品を管理できます。例えば、サブスクリプションの有効期限の確認、新しいライセンスキーの追加、ライセンス更新の登録、アップグレードのリクエストなどを実行できます。また、サポートチームに連絡して、製品のインストールファイルをダウンロードしたり、製品の文書にアクセスしたりすることもできます。

ライセンスの管理

下の表に、利用可能な操作の概要と、その操作を行う場所を示します。

操作	ロケーション
現在のアカウントにライセンスを追加する	Acronisカスタマーポータル（https://account.acronis.com）で、ライセンスを追加します。オンラインで購入されたライセンスは、自動的にここに追加されます。
管理サーバーを有効化する	管理サーバーは、現在のアカウントに登録することで、有効化できます。 アカウントにサインインして、ローカルコンソール（https://<**管理サーバーのIPアドレス**>:<**ポート**>）でオンライン管理サーバーを有効化します。 オフライン管理サーバーのアクティベーションには、ローカルコンソールとクラウドコンソールの両方での操作が必要です。
管理サーバーへライセンスを割り当てる 既存のライセンス割り当てを変更する	オンライン管理サーバーの場合、クラウドコンソール（https://cloud.acronis.com）を使用してライセンスを割り当てることができます。割り当てられたライセンスは、管理サーバーと自動的に同期されます。 オフライン管理サーバーの場合、ライセンスはアクティベーションファイル経由で割り当てられます。この手順では、管理サーバーのローカルコンソール（https://<**管理サーバーのIPアドレス**>:<**ポート**>）とクラウドコンソール（https://cloud.acronis.com）の両方を使用する必要があります。
ワークロードにライセンスを割り当てる	この操作は自動で実行されます。
アカウントから管理サーバーの登録を	クラウドコンソール（https://cloud.acronis.com）を使用してオンライン管理サーバーの登録を解除できます。

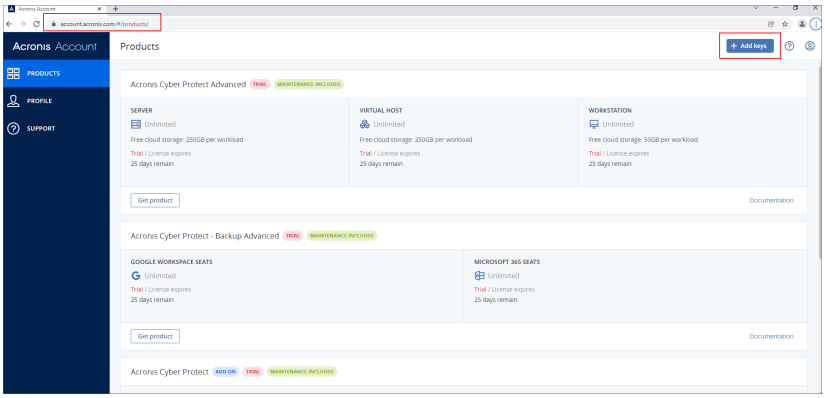
操作	ロケーション
解除する	オフライン管理サーバーの登録を解除するには、アクティベーション解除ファイルを使用します。この手順では、オフライン管理サーバーのローカルコンソール（https://<**管理サーバーのIPアドレス**>:<**ポート**>）とクラウドコンソール（https://cloud.acronis.com）の両方を使用する必要があります。 アクセス権のないオフライン管理サーバーの登録を解除するには、必ずクラウドコンソールを使用します。

現在のAcronisアカウントにライセンスを追加

ライセンスを使用するには、現在のAcronisアカウントに追加する必要があります。オンラインで購入されたライセンスは、自動的に現在のアカウントに追加されます。オフラインで購入したライセンスを手動で追加する必要があります。

現在のAcronisアカウントにライセンスを追加するには

1. アカウントの資格情報を使用して、Acronisカスタマーポータル（https://account.acronis.com）にログインします。
2. ナビゲーションメニューで、**[製品]** をクリックします。
3. **[キーの追加]** をクリックします。



4. 1つまたは複数のライセンスキーを入力（1行に1つずつ）し、**[追加]** をクリックします。

> **注意**
> ライセンスキーは一度に100個まで入力可能です。

現在のアカウントにライセンスが追加され、クラウドコンソール（https://cloud.acronis.com）でライセンスの使用状況を管理できるようになります。

重要
Acronis Cyber Protect 15 Update 3にアップグレードする前に、ローカルに保存されている永続ライセンスをファイルにエクスポートしてから、現在のAcronisアカウントに追加してください。

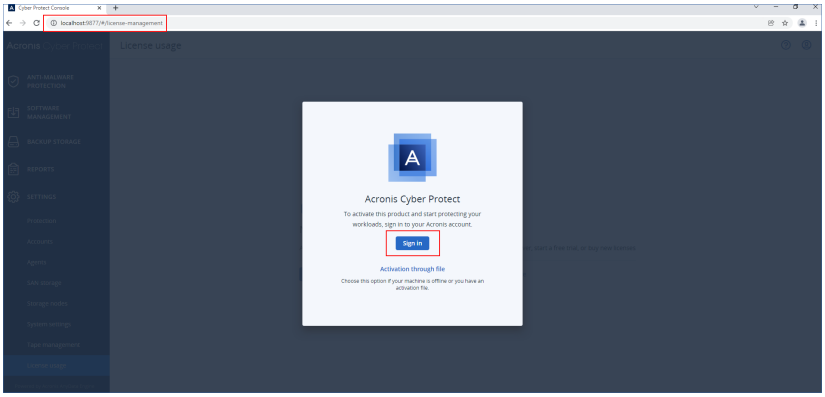
ローカルで入力したライセンスキーを管理サーバーで確認するには、https://<**管理サーバーのIPアドレス**>:<**ポート**>/api/account_server/v2/licensing/legacy/license_keysにアクセスしてください。

管理サーバーの有効化

これを現在のAcronisアカウントに登録することで、管理サーバーを有効化することができます。

オンライン管理サーバーを有効化するには

1. Acronis Cyber Protect管理サーバーをインストールしてから、ローカルコンソール（**https://<管理サーバーのIPアドレス>:<ポート>**）を開きます。
2. 開いたダイアログボックスで、**[サインイン]** をクリックします。



3. 現在のAcronisアカウントにサインインします。

これにより、管理サーバーが自動的に登録および有効化されます。

ワークロードの保護を開始するには、このサーバーに少なくとも1つのライセンスを割り当てます。ライセンスを割り当てる方法については、"管理サーバーへのライセンス割り当て"（30ページ）を参照してください。

注意
オンライン管理サーバーでは、Acronisアカウントにライセンス情報を同期させるために、インターネットへのアクセスが必要です。サーバーが30日以上オフラインになると、その保護計画は機能しなくなり、現在のワークロードは保護されなくなります。

ローカルコンソールでAcronisアカウントからサインアウトした場合、ライセンス情報を同期できません。30日以内に再度サインインしない場合、保護計画は機能しなくなり、現在のワークロードの保護は停止されます。

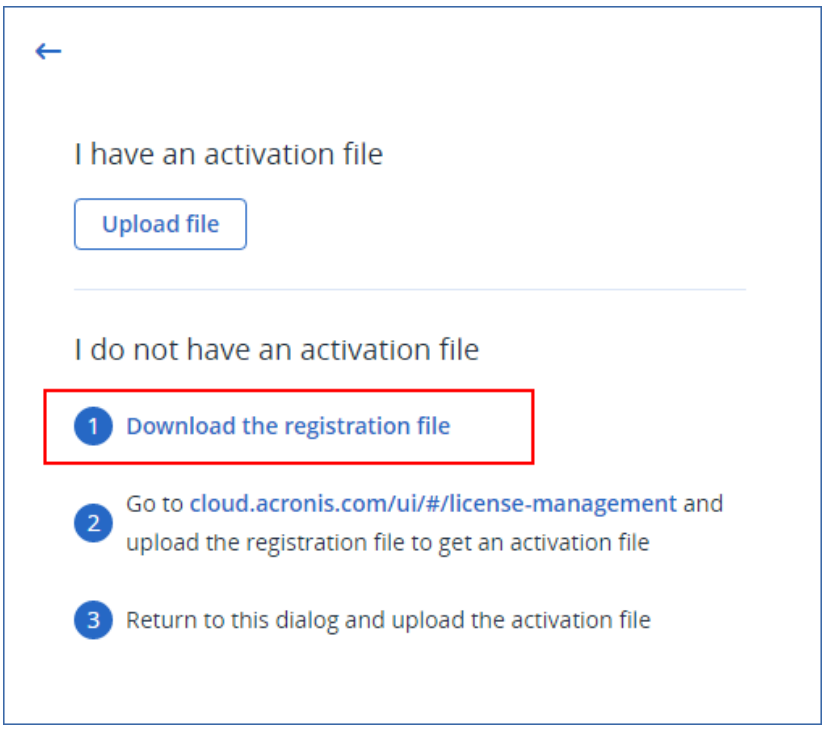
オフライン管理サーバーを有効化するには

オフライン管理サーバーのアクティベーションには、ローカルコンソールとクラウドコンソールの両方での操作が必要です。

クラウドコンソールにアクセスするには、インターネットに接続された2台目のマシンが必要です。

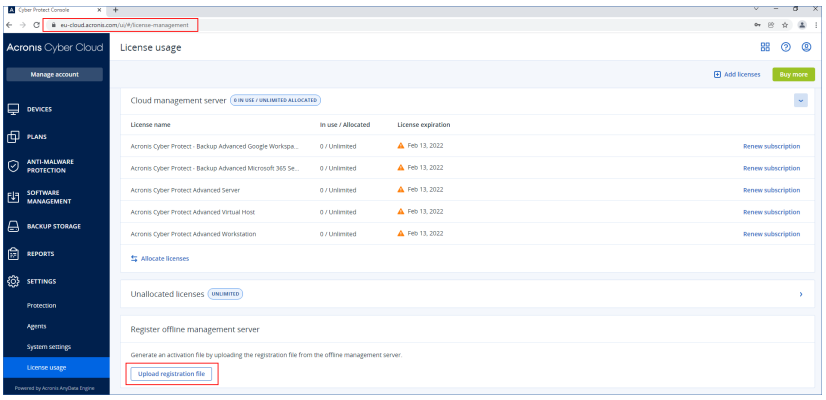
1. Acronis Cyber Protect管理サーバーをインストールしてから、ローカルコンソール（**https://<管理サーバーのIPアドレス>:<ポート>**）を開きます。
2. 開いたダイアログボックスで、**[ファイル経由でアクティベーション]** をクリックします。

3. [**アクティベーションファイルがありません**] 以下で、[**登録ファイルをダウンロード**] をクリックします。



登録ファイルが現在のマシンにダウンロードされます。

4. インターネットにアクセスできるマシンで、クラウドコンソール（https://cloud.acronis.com）にログインし、[**設定**] > [**ライセンスの使用状況**] に移動します。
5. [**オフライン管理サーバーの登録**] セクションで、[**登録ファイルをアップロード**] をクリックします。



6. 開いたダイアログボックスで、[**参照**] をクリックして、オフライン管理サーバーからダウンロードした登録ファイルを選択します。
7. 開いたダイアログボックスで、[**ファイルをダウンロード**] をクリックします。
アクティベーションファイルが現在のマシンにダウンロードされます。

重要

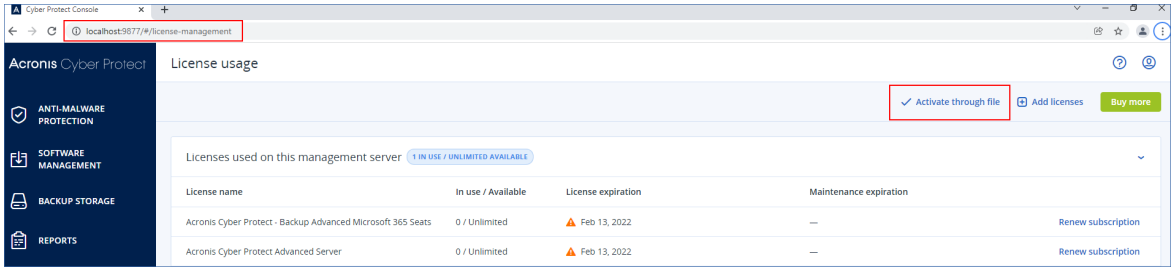
このオフライン管理サーバーが現在の環境内における唯一の管理サーバーである場合、Acronisアカウント内のライセンスは自動的に割り当てられます。アクティベーションファイルにはこの情報が含まれているため、追加の割り当ては必要ありません。

この管理サーバーが、現在の環境における唯一の管理サーバーでない場合は、アクティベーション後、"管理サーバーへのライセンス割り当て"（30ページ）の手順でライセンスを割り当てる必要があります。

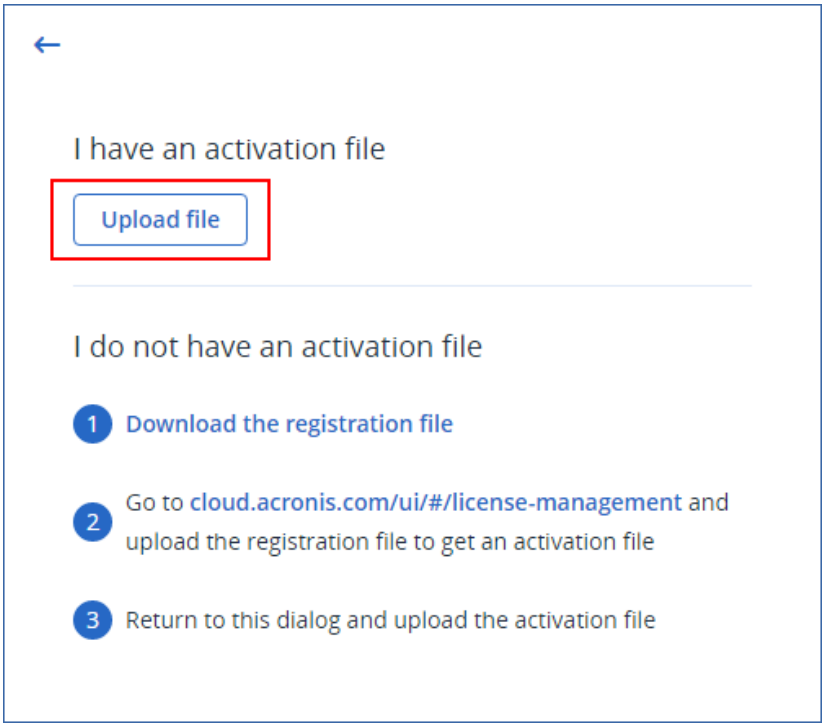
8. オフライン管理サーバーのローカルコンソール（https://**<管理サーバーのIPアドレス>**:**<ポート>**）で、**[ファイル経由でアクティベーション]** ダイアログボックスに移動します。

注意

[ファイル経由でアクティベーション] ダイアログボックスが開いていない場合は、**[設定]** > **[ライセンスの使用状況]** に移動し、**[ファイル経由でアクティベーション]** をクリックします。



9. **[アクティベーションファイルがあります]** 以下で、**[ファイルをアップロード]** をクリックし、クラウドコンソールからダウンロードしたアクティベーションファイルを選択します。



これにより、オフライン管理サーバーは現在のAcronisアカウントに登録されて、有効化されます。

注意
UUIDが一意でない仮想マシン上で動作する管理サーバーは、有効化できない場合があります。仮想マシンのクローンを作成したり、VMware vCenter Converterで変換したりする際に、UUIDが重複してしまうことがあります。このような問題が発生した場合は、サポートチームまでご連絡ください。

VMware仮想マシンでUUIDの重複を防ぐ方法については、「UUID.biosが重複している仮想マシンを編集する（1002403）」を参照してください。

管理サーバーへのライセンス割り当て

ライセンスを使用するには、そのクォータまたはクォータの一部を管理サーバーに割り当てる必要があります。管理サーバーに複数のライセンスを割り当てることができます。また、ライセンスクォータを分割し、管理サーバー別にクォータを分配して割り当てることができます。

注意
Acronisアカウントに管理サーバーが1台のみ存在する場合、このサーバーに対してすべてのライセンスが自動的に割り当てられます。別の管理サーバーにライセンスを再度割り当てる方法については、"ライセンスクォータを別の管理サーバーに転送する"（33ページ）を参照してください。

Acronisアカウントに複数の管理サーバーが存在する場合、新しいライセンスはクラウドコンソール（https://cloud.acronis.com）の**未割り当てライセンス**の下に表示されます。これらのライセンスは、手動で割り当てる必要があります。

ライセンスを使用したすべての操作は、オンライン管理サーバーと自動的に同期されます。オフラインの管理サーバーに割り当ての変更を同期させるには、新しいアクティベーションファイルを作成してから、割り当ての手順を繰り返してください。異なる管理サーバーの詳細については、"管理サーバーの種類"（22ページ）を参照してください。

オンライン管理サーバーにライセンスを割り当てるには

1. クラウドコンソール（https://cloud.acronis.com）で、**[設定]** > **[ライセンスの使用状況]** をクリックします。
2. ライセンスを割り当てたい管理サーバーに移動します。
3. **[ライセンスを割り当て]** をクリックします。
4. 開いたダイアログボックスで、このサーバーに割り当てるライセンスとライセンスクォータを指定します。
5. **[保存]** をクリックします。

その結果、ライセンス情報が管理サーバーと自動的に同期され、割り当てられたライセンスを使用してワークロードを保護できます。

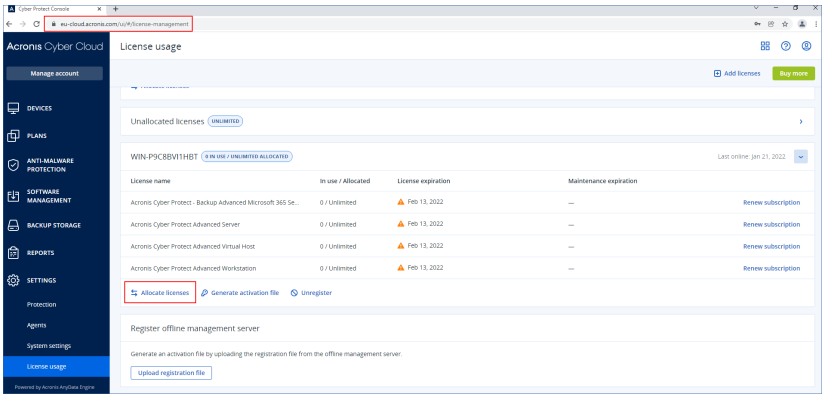
割り当てを変更する場合は、上記の手順を繰り返します。

重要
修正されたライセンスクォータの数が、プロテクションエージェントの数よりも少ない場合、最も負荷の少ないエージェントが動作を停止します。この選択は自動で実行されます。ニーズに合致しない場合は、使用可能なライセンスを手動で再割り当てしてください。

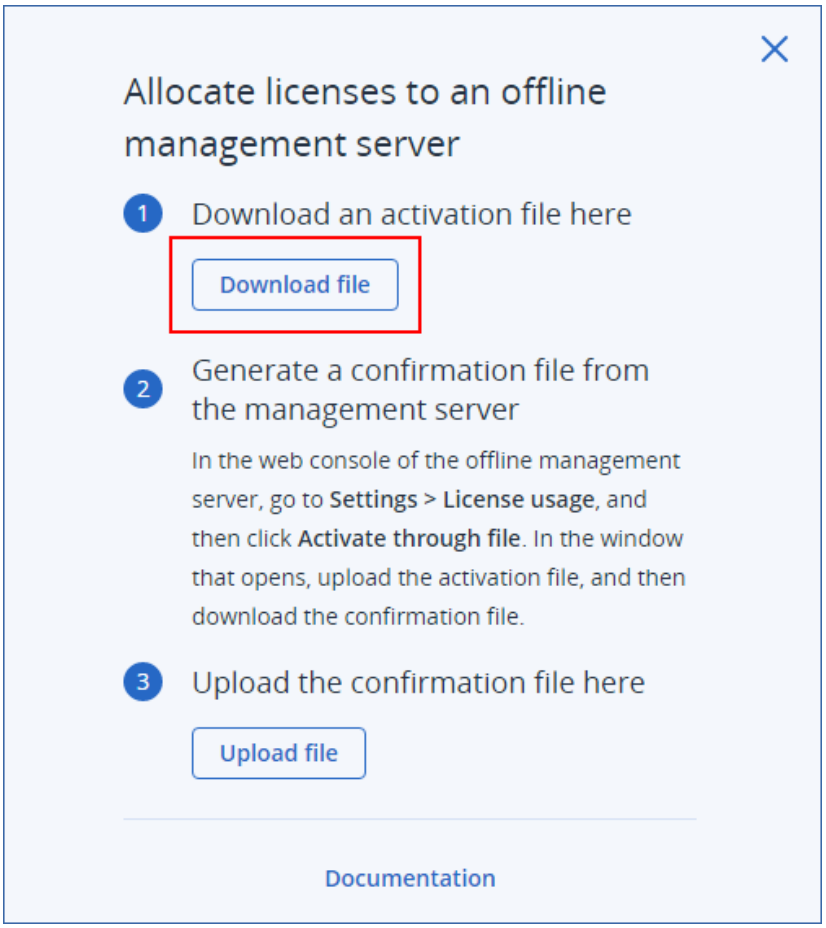
オフライン管理サーバーにライセンスを割り当てるには

オフラインの管理サーバーにライセンスを割り当てるには、クラウドとローカルの両方のコンソールを使用する必要があります。クラウドコンソールにアクセスするには、インターネットに接続された2台目のマシンが必要です。

1. インターネットにアクセスできるマシンで、クラウドコンソール（https://cloud.acronis.com）にログインし、**[設定]** > **[ライセンスの使用状況]** をクリックします。
2. ライセンスを割り当てたい管理サーバーに移動します。
3. **[ライセンスを割り当て]** をクリックします。

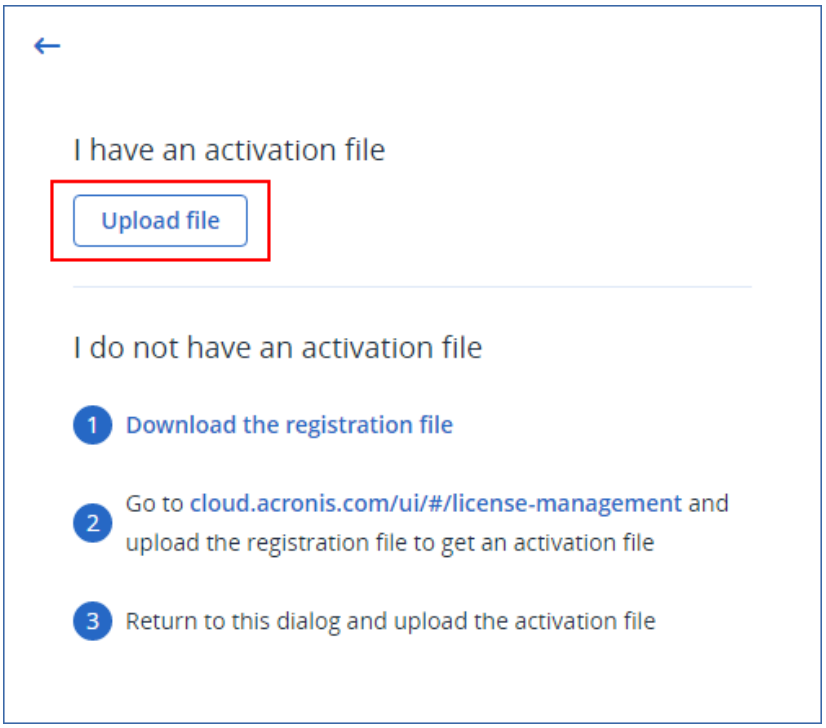


4. 開いたダイアログボックスで、このサーバーに割り当てるライセンスとライセンスクォータを指定します。
5. **[保存]** をクリックします。
6. **[オフライン管理サーバーにライセンスを割り当てる]** ダイアログボックスで、**[ファイルをダウンロード]** をクリックします。



アクティベーションファイルが現在のマシンにダウンロードされます。

7. オフライン管理サーバーのローカルコンソール（https://<管理サーバーのIPアドレス>:<ポート>）で、**[設定]**> **[ライセンスの使用状況]** に移動し、**[ファイル経由で有効化]** をクリックします。
8. 開いたダイアログボックスの **[アクティベーションファイルがあります]** 以下で、**[ファイルをアップロード]** をクリックし、クラウドコンソールからダウンロードしたアクティベーションファイルを選択します。



その結果、現在のAcronisアカウントとオフライン管理サーバーの間でライセンス情報が同期されます。

割り当てられたライセンスクォータを増やす場合は、上記の手順を繰り返します。

割り当てられたライセンスクォータを減らす場合は、"オフライン管理サーバーに割り当てるライセンスクォータを減らす"（34ページ）を参照してください。

ライセンスクォータを別の管理サーバーに転送する

ある管理サーバーから別の管理サーバーにライセンスクォータを転送できます。このオプションは、管理サーバーに割り当てられたライセンスがどのワークロードでも使用されていない場合、また別の管理サーバー用にさらにライセンスが必要な場合に有用です。

注意
Acronisアカウントに管理サーバーが1台のみ存在する場合、このサーバーに対して自動的にすべてのライセンスが割り当てられます。

Acronisアカウントに複数の管理サーバーが存在する場合、新しいライセンスはクラウドコンソール（https://cloud.acronis.com）の**未割り当てライセンス**の下に表示されます。これらのライセンスは、手動で割り当てる必要があります。

ライセンスクォータを別の管理サーバーに転送するには

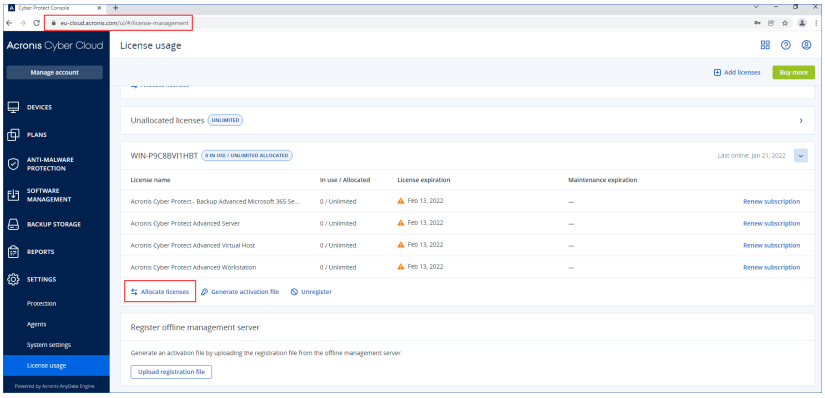
1. "管理サーバーへのライセンス割り当て"（30ページ）の手順を実行して、元の管理サーバーに割り当てられているライセンスクォータを減らします。
   リリースされたライセンスクォータは、クラウドコンソールの [**未割り当てライセンス**] セクションに表示されます。

2. "管理サーバーへのライセンス割り当て"（30ページ）の手順を実行して、2番目の管理サーバーにライセンスクォータを割り当てます。

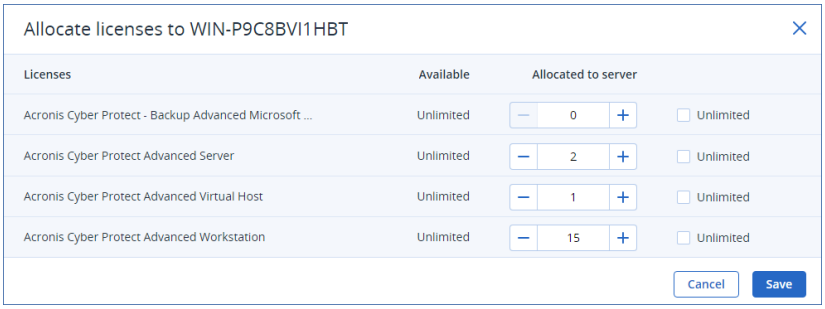
オフライン管理サーバーに割り当てるライセンスクォータを減らす

オフライン管理サーバーに割り当てられたライセンスクォータを減らすには、クラウドとローカルの両方のコンソールを使用する必要があります。クラウドコンソールにアクセスするには、インターネットに接続された2台目のマシンが必要です。

1. インターネットにアクセスできるマシンで、クラウドコンソール（https://cloud.acronis.com）にログインしてから、[**設定**] > [**ライセンスの使用状況**] をクリックします。
2. ライセンスを割り当てたい管理サーバーに移動して、[**ライセンスを割り当て**] をクリックします。

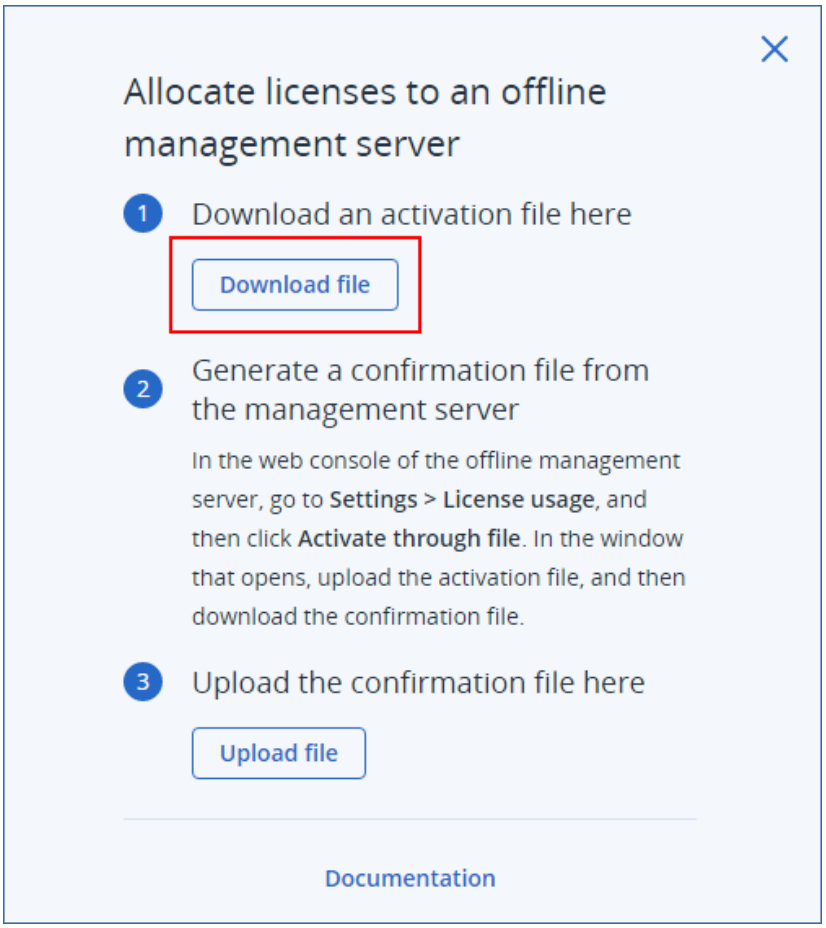


3. 開いたダイアログボックスで、このサーバーに割り当てるライセンスとライセンスクォータを変更してから、[**保存**] をクリックします。



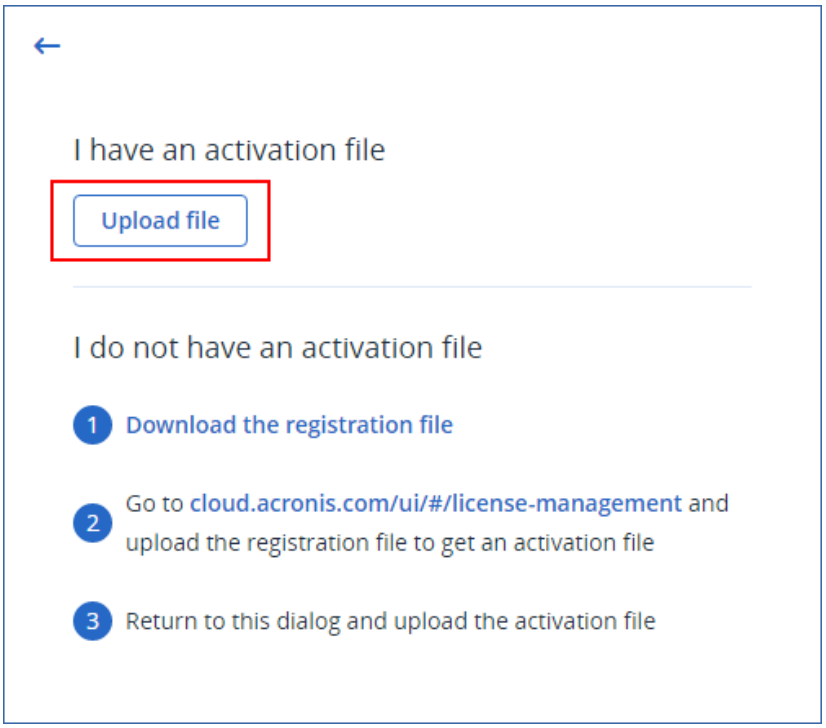
新しい割り当ては保留中です。キャンセルするには、[**この割り当てを削除**] をクリックします。

4. [**オフライン管理サーバーにライセンスを割り当てる**] ダイアログボックスで、[**ファイルをダウンロード**] をクリックします。

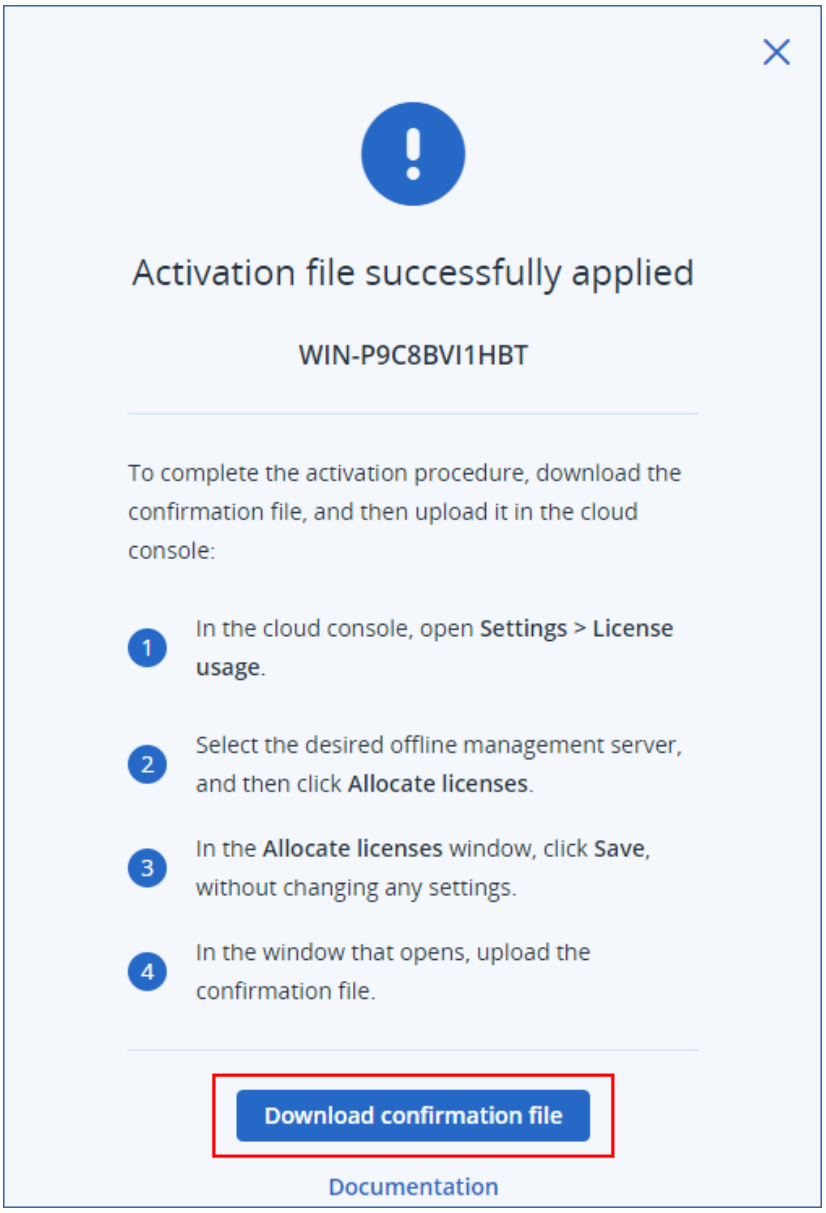


アクティベーションファイルが現在のマシンにダウンロードされます。

5. オフライン管理サーバーのローカルコンソール（https://<管理サーバーのIPアドレス>:<ポート>）で、**[設定]**> **[ライセンスの使用状況]** に移動し、**[ファイル経由で有効化]** をクリックします。
6. 開いたダイアログボックスの **[アクティベーションファイルがあります]** 以下で、**[ファイルをアップロード]** をクリックし、クラウドコンソールからダウンロードしたアクティベーションファイルを選択します。

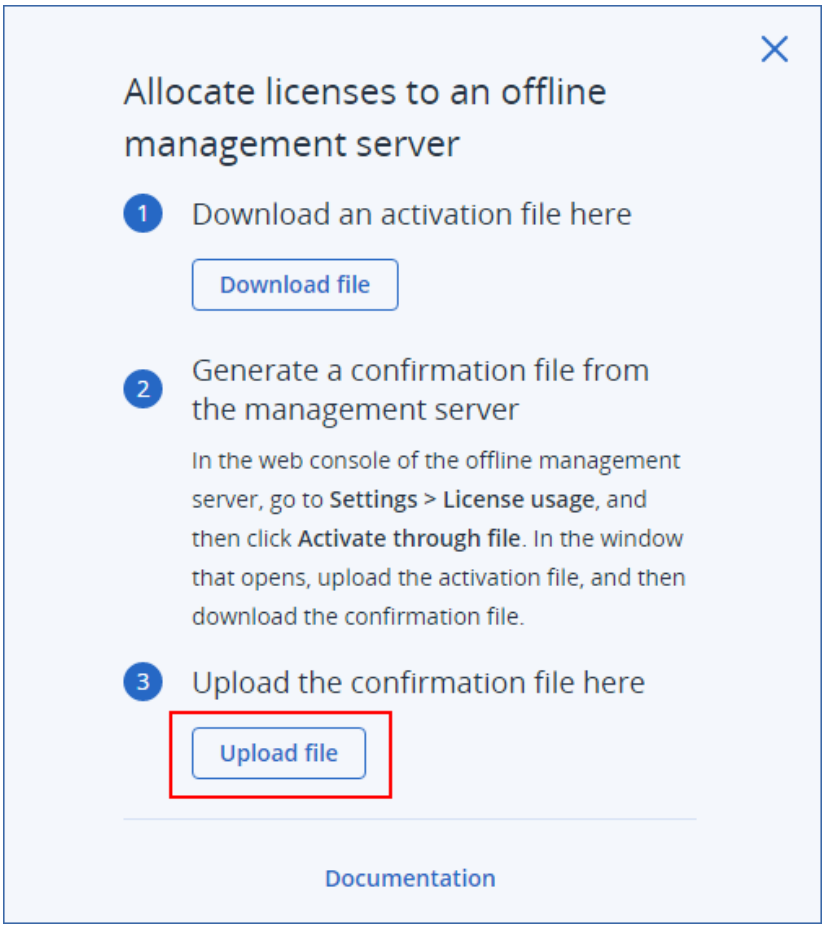


7. 開いたダイアログボックスで、**[確認ファイルをダウンロード]** をクリックします。



確認ファイルが現在のマシンにダウンロードされます。

8. クラウドコンソール（https://cloud.acronis.com）で、**[設定]** > **[ライセンスの使用状況]** をクリックします。
9. ライセンスを割り当てたい管理サーバーに移動して、**[ライセンスを割り当て]** をクリックします。
10. 開いたダイアログボックスで、設定を変更せずに **[保存]** をクリックします。
11. **[オフライン管理サーバーにライセンスを割り当てる]** ダイアログボックスで、**[ファイルをアップロード]** をクリックし、オフライン管理サーバーからダウンロードした確認ファイルを選択します。



その結果、現在のAcronisアカウントとオフライン管理サーバーの間でライセンス情報が同期されます。

重要
修正されたライセンスクォータの数が、プロテクションエージェントの数よりも少ない場合、最も負荷の少ないエージェントが動作を停止します。この選択は自動で実行されます。ニーズに合致しない場合は、使用可能なライセンスを手動で再割り当てしてください。

ワークロードへのライセンスの割り当て

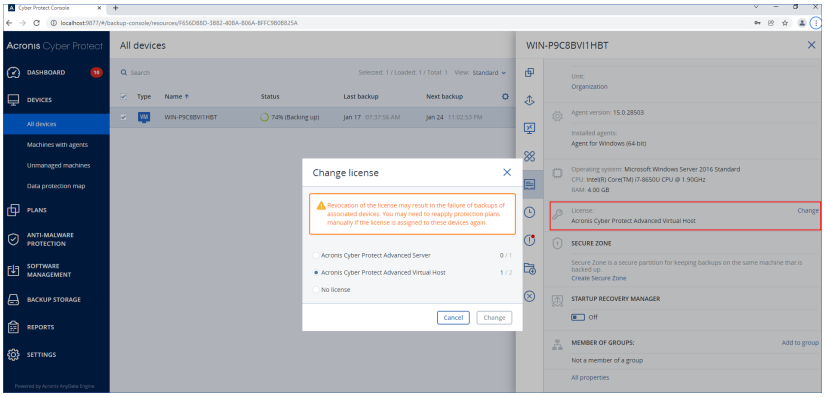
管理サーバーは、このサーバーに登録されているワークロード間で割り当てられたライセンスを分散します。

ワークロードに保護計画を初めて適用するときに、管理サーバーがこのワークロードに対してライセンスを割り当てます。管理サーバーに複数のライセンスが割り当てられている場合は、ワークロードの種類、オペレーティングシステム、および必要な保護レベルに応じて、ワークロードに最適なライセンスが割り当てられます。

割り当てられたライセンスを確認するには、管理サーバーのウェブコンソールで任意のワークロードを選択し、**[詳細]** をクリックします。

ライセンスをワークロードに手動で再割り当てするには

1. 管理サーバーのウェブコンソールコンソールで **[デバイス]** をクリックし、任意のワークロードを選択します。
2. **[詳細]** をクリックします。
3. （オンプレミスの管理サーバーの場合）**[ライセンス]** セクションに移動して、**[変更]** をクリックします。
4. （クラウドの管理サーバーの場合）**[サービスクォータ]** セクションに移動して、**[変更]** をクリックします。
5. 任意のライセンス（サービスクォータ）を選択して、**[変更]** をクリックします。



制限事項

オフラインの管理サーバーの場合、ライセンスクォータの現在の使用状況は、ローカルコンソールのみに表示されます。オフラインの管理サーバーでは、このデータがAcronisアカウントに同期されないため、クラウドコンソールから利用することはできません。

既知の問題

クラウドコンソールで、**仮想ホスト**ライセンスの使用または割り当てが正しく表示されないことがあります。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。

管理サーバーの登録解除

オンライン管理サーバーの登録を解除するには

1. クラウドコンソール（https://cloud.acronis.com）で、**[設定]** > **[ライセンスの使用状況]** をクリックします。
2. 任意の管理サーバーに移動し、**[登録解除]** をクリックします。
3. **[管理サーバーの登録を解除]** ウィンドウが表示されます。
4. アカウントに関連付けられたEメールアドレスを入力して、登録の解除を確認してください。
5. **[登録解除]** をクリックします。

これにより、未登録サーバーに割り当てられていたライセンスはすべてリリースされ、アカウント内の別の管理サーバーに割り当てることができます。未登録管理サーバーのローカルコンソールでは、ライセンスはゼロにリセットされます。

オフライン管理サーバーの登録を解除するには

2種類のエントリポイントから、オフライン管理サーバーの登録を解除できます。

ローカルコンソールを使用する場合:

1. ローカルコンソールで、アカウントが表示されている行の **[登録解除]** をクリックする。**[管理サーバーの登録を解除]** ウィンドウが表示されます。
2. **[ログイン]** フィールドに、ローカル管理者に関連するEメールアドレスを入力します。
3. **[登録解除]** をクリックします。
4. **[登録は正常に解除されました]** というポップアップ画面が表示されます。
5. **[登録解除ファイルをダウンロード]** をクリックします。
6. クラウドコンソールを開き、**[登録解除]** をクリックします。**[管理サーバーの登録を解除]** ウィンドウが表示されます。
7. **[オフライン管理サーバーの登録を解除]** をクリックします。**[オフライン管理サーバーの登録を解除]** ウィンドウが表示されます。
8. **[参照]** をクリックして、ローカルコンソールからダウンロードした登録解除ファイルを選択します。
9. **[登録解除]** をクリックします。

クラウドコンソールを使用する場合:

1. インターネットにアクセスできるマシンで、クラウドコンソール（https://cloud.acronis.com）にログインし、**[設定]** > **[ライセンスの使用状況]** をクリックします。
2. 任意の管理サーバーに移動し、**[登録解除]** をクリックします。**[管理サーバーの登録を解除]** ウィンドウが表示されます。
3. **[オフライン管理サーバーの登録を解除]** をクリックします。**[オフライン管理サーバーの登録を解除]** ウィンドウが表示されます。
4. 登録を解除したい管理サーバーのローカルコンソール（https://**<管理サーバーのIPアドレス>**:**<ポート>**）で、**[設定]**> **[ライセンスの使用状況]** に移動し、**[登録解除]** をクリックします。登録解除ファイルが現在のマシンにダウンロードされます。
5. クラウドコンソールで、**[オフライン管理サーバーの登録を解除]** ウィンドウに戻ります。
6. **[参照]** をクリックして、ローカルコンソールからダウンロードした登録解除ファイルを選択します。
7. **[登録解除]** をクリックします。
8. 一方、管理サーバーがインストールされているマシンにアクセスできない場合は、**[管理サーバーのマシンにアクセスできません]** をクリックします。

警告
このマシンは恒久的にブロックされ、現在のアカウントから削除されます。今後、このマシンに管理サーバーを登録することはできなくなります。

これにより、未登録サーバーに割り当てられていたライセンスはすべてリリースされ、アカウント内の別の管理サーバーに割り当てることができます。未登録管理サーバーのローカルコンソールでは、ライセンスはゼロにリセットされます。

AcronisCyber Protect 15 Update 2以前のライセンス

Acronis Cyber Protect 15 Update 2以前のバージョンを使用するには、1つまたは複数のライセンスキーを管理サーバーに追加する必要があります。保護計画が適用されるときに、ライセンスは自動的にマシンに割り当てられます。

ライセンスの割り当てや取り消しは手動で行うこともできます。ライセンスの手動操作は、組織管理者のみが行えます。管理者の詳細情報については、"部署および管理アカウント"（631ページ）を参照してください。

管理サーバーにライセンスキーを追加する

Acronis Cyber Protect 15 Update 2以前のバージョンでは、ライセンスキーを管理サーバーに追加します。

管理サーバーにライセンスキーを追加するには

1. Cyber Protectウェブコンソールで、**[設定]** > **[ライセンス]** に移動します。
2. **[キーの追加]** をクリックします。
3. 1つまたは複数のライセンスキーを各行に1つずつ入力します。
4. **[追加]** をクリックします。
5. （サブスクリプションライセンスキーを追加する場合）サブスクリプションライセンスを有効化するには、Acronisアカウントにサインインします。
   a. サインインフォームで、Acronisカスタマーポータル（https://account.acronis.com）で使用している資格情報を入力し、**[サインイン]** をクリックします。
   b. アカウントを確認してから、**[同期]** をクリックします。
   c. 処理が完了したら、**[完了]** をクリックします。
6. **[ライセンスキーを追加]** パネルで、**[完了]** をクリックします。

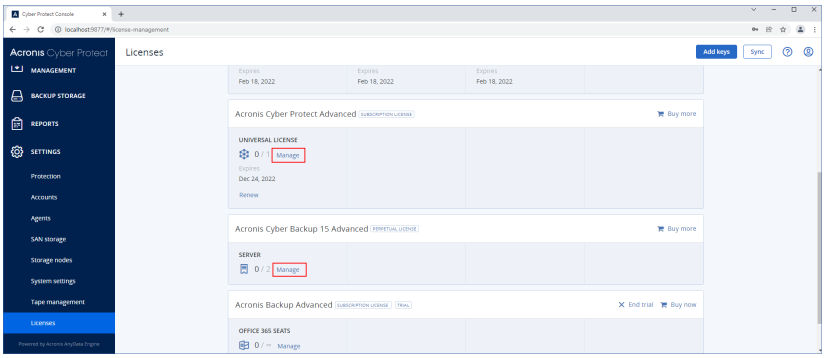
注意
Acronisアカウントに登録されているサブスクリプションライセンスキーを自動的にインポートできます。管理サーバーに再度追加する必要はありません。ライセンスキーをインポートするには、**[ライセンスキーを追加]** パネルで、**[アクロニスアカウントと同期]** をクリックし、Acronisアカウントにサインインします。

サブスクリプションライセンスの管理

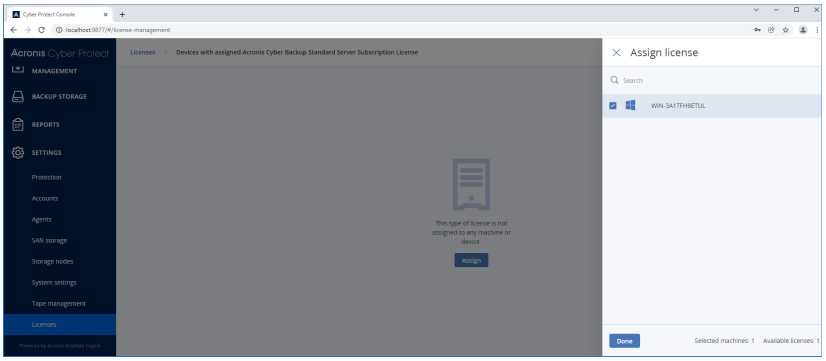
ワークロードにライセンスを割り当てる前に、ライセンスキーを管理サーバーに追加する必要があります。その方法については、"管理サーバーにライセンスキーを追加する"（41ページ）を参照してください。

サブスクリプションライセンスをワークロードに割り当てるには

1. Cyber Protectウェブコンソールで、**[設定]** > **[ライセンス]** に移動します。
2. 任意のライセンスに移動して、**[管理]** をクリックします。



3. **[割り当て]** をクリックします。
   このライセンスを割り当てることができるワークロードが表示されます。



4. ワークロードを選択して、**[完了]** をクリックします。

ワークロードからサブスクリプションライセンスを取り消すには

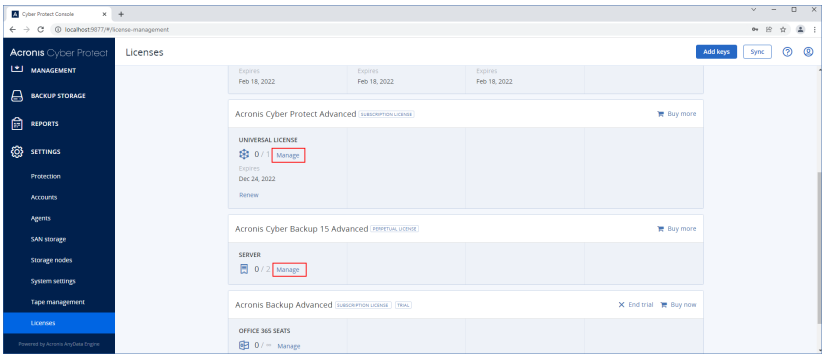
1. Cyber Protectウェブコンソールで、**[設定]** > **[ライセンス]** に移動します。
2. 任意のライセンスに移動して、**[管理]** をクリックします。
   このライセンスが割り当てられているすべてのワークロードが表示されます。
3. ライセンスを取り消すワークロードを選択します。
4. **[取り消し]** をクリックします。
5. 操作を確定します。
   取り消されたライセンスキーはリリースされ、別のワークロードに割り当てることができます。

永久ライセンスの管理

ワークロードにライセンスを割り当てる前に、ライセンスキーを管理サーバーに追加する必要があります。その方法については、"管理サーバーにライセンスキーを追加する"（41ページ）を参照してください。

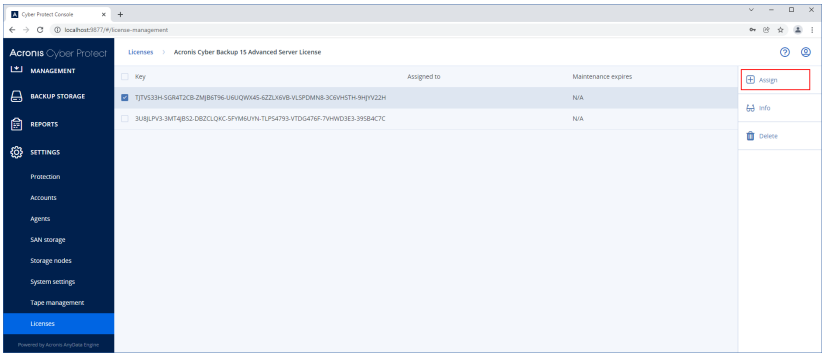
永続ライセンスをワークロードに割り当てるには

1. Cyber Protectウェブコンソールで、**[設定]** > **[ライセンス]** に移動します。
2. 任意のライセンスに移動して、**[管理]** をクリックします。



選択したライセンスに対応するライセンスキーが表示されます。

3. ワークロードに割り当てるライセンスキーを選択します。
4. **[割り当て]** をクリックします。



このライセンスキーを割り当てることができるワークロードが表示されます。

5. ワークロードを選択して、**[完了]** をクリックします。

ワークロードから永続ライセンスを取り消すには

1. Cyber Protectウェブコンソールで、**[設定]** > **[ライセンス]** に移動します。
2. 任意のライセンスを選択して、**[管理]** をクリックします。
   選択したライセンスに対応するライセンスキーが表示されます。このライセンスキーが割り当てられているワークロードを **[割り当て先]** 列で確認します。
3. 取り消すライセンスキーを選択します。
4. **[取り消し]** をクリックします。
5. 操作を確定します。
   取り消されたライセンスキーは、ライセンスリストに残り、別のワークロードに割り当てることができます。

インストール

インストール概要

Acronis Cyber Protect はオンプレミスとクラウドの 2 つの配置方法をサポートします。これらの主な違いはAcronis Cyber Protect管理サーバーのロケーションです。

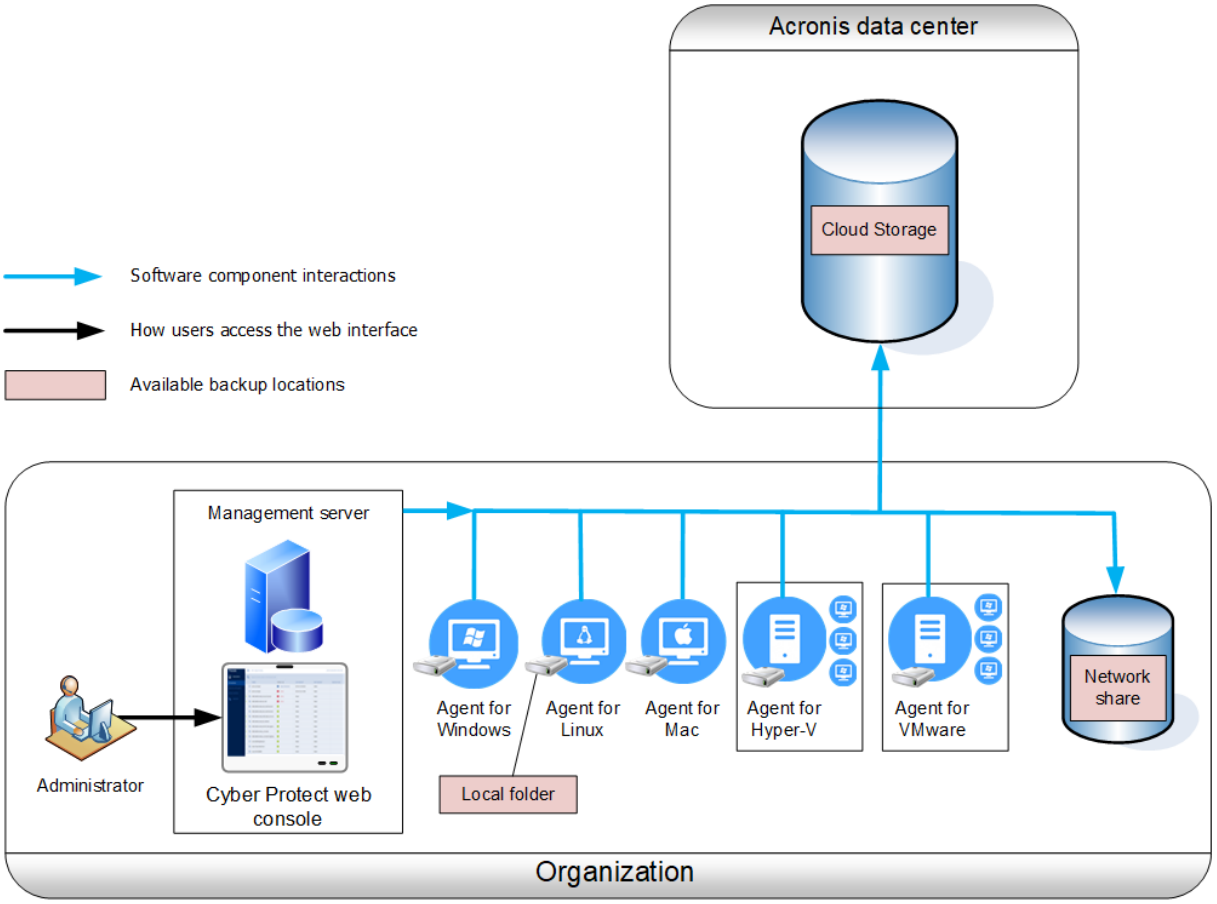
管理サーバーはすべてのバックアップを管理するための集中管理ポイントです。オンプレミス配置の場合は、ローカルネットワークにインストールされ、クラウド配置の場合は、Acronis データセンターのいずれかに配置されます。このサーバーへの Web インターフェースは、Cyber Protect ウェブ コンソールと呼ばれます。

管理サーバーはプロテクションエージェントとの通信を担い、計画管理機能全般を実行します。すべての保護アクティビティの前に、エージェントは管理サーバーを参照して前提条件を確認します。管理サーバーへの接続が失われることがあり、その場合新しい保護計画の配置は行われません。ただし、保護計画が既にマシンに配置されている場合、エージェントは管理サーバーとの接続が失われた後30日間保護操作を継続します。

いずれのタイプの配置も、バックアップする各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。サポートされているタイプのストレージも同じです。クラウド ストレージスペースは Acronis Cyber Protect ライセンスとは別売です。

オンプレミスデプロイ

オンプレミスデプロイメントは、すべての製品コンポーネントがローカルネットワークにインストールされることを意味します。これは、永久ライセンスで使用可能な唯一の方法です。また、コンピュータがインターネットに接続されていない場合は、この方法を使用する必要があります。



Management Serverロケーション

WindowsまたはLinuxコンピュータにManagement Serverをインストールできます。

Windowsでのインストールが推奨されます。Management Serverから他のコンピュータにエージェントをデプロイできるためです。Advancedライセンスでは、組織単位（OU）を作成し、それらに管理者を追加することができます。この方法によって、対応する部署に厳密に限定されたアクセス許可を持つ他のユーザーに、保護管理を委任できます。

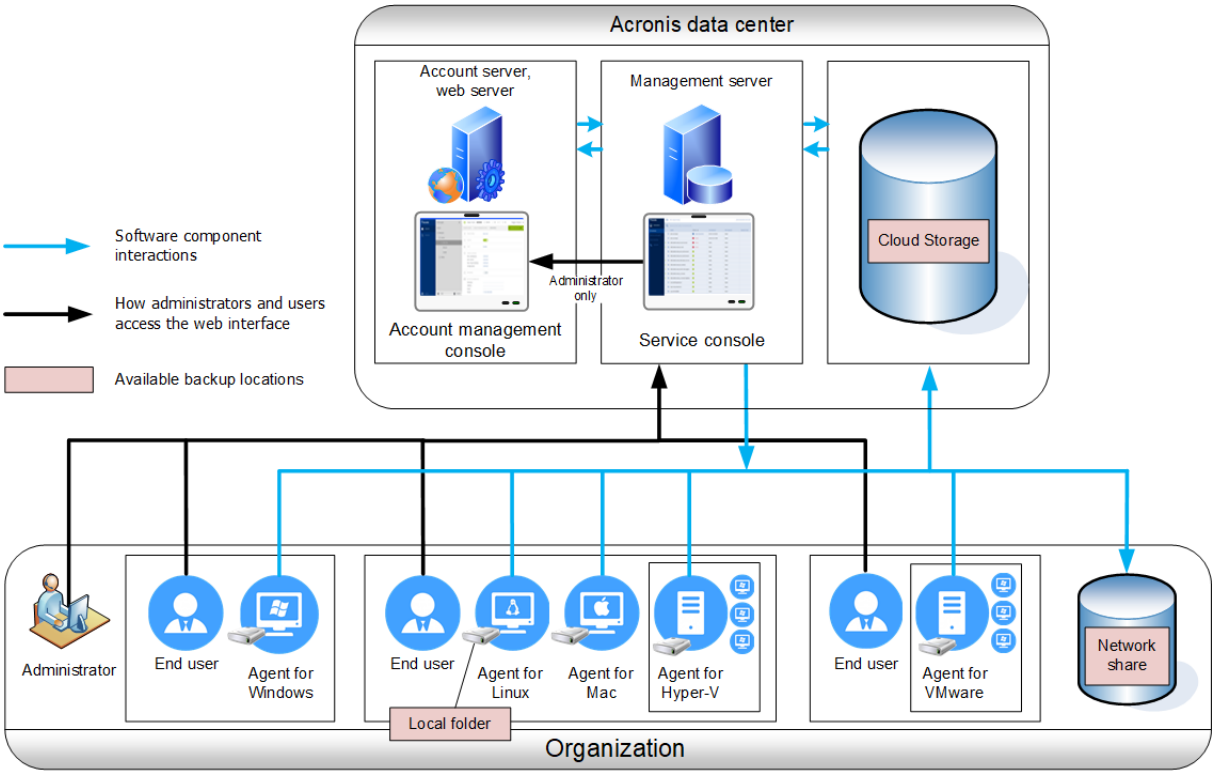
LinuxでのインストールはLinuxのみの環境で推奨されます。バックアップするコンピュータでローカルにエージェントをインストールする必要があります。

クラウドデプロイ

クラウド配置では Acronis データセンターのいずれかに管理サーバーがあります。この方法の利点は、ローカルネットワークでManagement Serverを管理する必要がないことです。Acronis Cyber Protect は Acronis から提供されるサイバープロテクションサービスと考えることができます。

アカウントサーバーにアクセスすると、ユーザーアカウントの作成、サービス使用クォータの設定、組織構造を反映するユーザーグループの作成（部署）ができます。すべてのユーザーは Cyber Protect ウェブ コンソールにアクセスして必要なエージェントをダウンロードし、数分でマシンにインストールできます。

管理者アカウントは組織または部署レベルで作成できます。各アカウントには制御領域に制限されたビューがあります。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。



次の表は、オンプレミスデプロイメントとクラウドデプロイメントの違いをまとめています。各列には、対応するデプロイの種類に限り利用可能な機能が列挙されています。

オンプレミスデプロイ	クラウドデプロイ
• 永続ライセンスを使用できます • エアギャップ環境で使用できるオンプレミスの管理サーバー* • バックアップロケーションとしてのSFTPサーバー • バックアップロケーションとしての Acronis Cyber Infrastructure • バックアップロケーションとしてのテープデバイスおよび Acronis Storage Node** • Backup for VMware を含む Acronis Cyber Protect の以前のバージョンからアップグレード	• グループ、パブリックフォルダ、OneDrive**およびSharePointオンラインデータの保護を含む、Microsoft 365データのクラウドツークラウドバックアップ • Google Workspaceデータのクラウドツークラウドバックアップ • Macエージェントは、x64およびAppleシリコンM1やM2などのARMベースのプロセッサをサポートしています。 • Virtuozzoエージェント（ハイパーバイザーレベルでのVirtuozzo仮想マシンのバックアップ） • oVirtエージェント（ハイパーバイザーレベルでのoVirt KVM仮想マシンのバックアップ） • Virtuozzo Hybrid Infrastructureエージェント（ハイパーバイザーレベルでのVirtuozzo Hybrid Infrastructure仮想マシンのバックアップ） • クラウドサービスとしてのディザスタリカバリ***

*エアギャップ環境における管理サーバーのアクティベーションの詳細については、"オフライン管理サーバーを有効化するには"（27ページ）を参照してください。

**この機能はStandard Editionでは使用できません。

***デフォルトでは、OneDriveのルートフォルダはバックアップ処理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、アーカイブ内に無効なコンテンツが含められます。

****この機能は、ディザスタリカバリアドオンでのみ利用可能です。

コンポーネント

エージェント

エージェントは、Acronis Cyber Protect によって管理されるマシン上でデータのバックアップ、復元、その他の処理を実行するアプリケーションです。

Windowsエージェントは、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インストールされます。また、エージェント for SQLをインストールした場合、エージェントがインストールされたコンピュータ全体をバックアップできるようになります。

特定のロールやアプリケーションを持つマシンにしかインストールできないエージェントもあります。例えば、Hyper-VエージェントはHyper-Vロールを実行しているマシンに、SQLエージェントはSQLデータベースを実行しているマシンに、ExchangeエージェントはMicrosoft Exchange Serverのメールボックスロールを実行しているマシンに、Active Directoryエージェントはドメインコントローラーにのみインストールできます。

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。次の表に、エージェントの選択に役立つ情報をまとめています。

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	エージェントの可用性	
			オンプレミス	クラウド
物理マシン				
Windowsを実行する物理コンピュータのディスク、ボリューム、ファイル	Windowsエージェント	バックアップ対象のコンピュータ	+	+
Linuxを実行する物理コンピュータのディスク、ボリューム、ファイル	エージェント for Linux		+	+
macOS を実行する物理マ	エージェント for		+	+

シンのディスク、ボリューム、ファイル	Mac			
アプリケーション				
SQLデータベース	エージェント for SQL	Microsoft SQL Serverを実行しているコンピュータ。	+	+
Exchangeのデータベースとメールボックス	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。* メールボックスのバックアップのみが必要な場合、Microsoft Exchange Serverのクライアント アクセスの役割を実行するコンピュータへのネットワークアクセスを持つ任意のWindowsコンピュータにエージェントをインストールできます。	+	+ メールボックスのバックアップなし
Microsoft 365メールボックス	エージェント for Office 365	インターネットに接続している Windows コンピュータ	+	+
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	+	+
Oracle データベースを実行しているマシン	Oracle エージェント	Oracleデータベースを実行しているマシン。	+	-
仮想マシン				
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	エージェント for Hyper-V	Hyper-Vホスト	+	+
Scale Computing HC3仮想マシン	Scale Computing HC3エージェント	Scale Computing HC3ホスト。	+	+

Windows Azure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コンピュータ	+	+
Amazon EC2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）仮想マシン				
Kernel-based Virtual Machine（KVM）				
Oracle 仮想コンピュータ				
Nutanix AHV仮想マシン				
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。詳細な手順については、「LANフリーバックアップ」を参照してください。

***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。それでも、クラウドの配置で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。

****Acronis Cyber Protect Advanced Virtual Host ラインセンスでは、これらの仮想マシンは仮想として見なされます（ホスト単位のライセンスが使用されます）。Acronis Cyber Protect Virtual Host ラインセンスでは、これらのマシンは物理として見なされます（マシン単位のライセンスが使用されます）。

その他のコンポーネント

コンポーネント	機能	インストール先	可用性	
			オンプレミス	クラウド
管理サーバー	管理サーバーはすべてのバックアップを管理するための集中管理ポイントです。オンプレミス配置の場合、管理サーバーはローカルネットワークにインストールされます。これにより エージェントを管理し、ユーザーにWebインターフェースを提供できます。	WindowsまたはLinuxを実行するコンピュータ。	+	-
リモート インストールのコンポーネント	エージェントのインストールパッケージをローカルフォルダに保存します。	管理サーバーを実行する Windows マシン。	+	-
スキャンサービス	オプションのコンポーネントにより、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のバックアップのマルウェア対策スキャンを実行できます。 スキャンサービスには Microsoft SQL ServerまたはPostgreSQLデータベースが必要です。管理サーバーが使用するデフォルトのSQLiteデータベースとの互換性はありません。	管理サーバーを実行するWindowsまたはLinuxマシン。	+	-
ブータブル メディアビルダー	ブータブル メディアを作成します。	WindowsまたはLinuxを実行するコンピュータ。	+	-
コマンドラインツール	**acrocmd**ユーティリティ向けのコマンドラインインターフェースがサポートされています。**acrocmd**本体にはコマンドを物理的に実行するツー	Windows、macOS、Linuxを実行するマシン。	+	+

	ルは含まれていません。Cyber Protectコンポーネント（エージェントと管理サーバー）へのコマンドラインインターフェースだけを提供するものです。			
Acronis Cyber Protect 15 モニタ	Windowsエージェントおよび Macエージェント向けのグラフィカルユーザーインターフェースを利用できます。モニタには、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。またユーザーはモニタを使用して、バックアップの暗号化構成とプロキシサーバの設定を実行できます。 WindowsでAcronis Cyber Protect 15モニタを使用する場合、同じマシンにWindowsエージェントをインストールしておく必要があります。	Windows または macOS を実行するマシン。	+	+
ストレージノード	バックアップを保存します。カタログと重複除外に必要です。 Storage Nodeでは、同じマシンにWindowsエージェントをインストールしておく必要があります。	Windowsを実行するコンピュータ。	+	-
カタログサービス	Storage Nodeでバックアップのカタログを実行します。	Windowsを実行するコンピュータ。	+	-
PXE Server	ネットワーク経由のブータブルメディアでのコンピュータの起動を有効にします。	Windowsを実行するコンピュータ。	+	-

Acronis Cyber Protectをユーザーの環境で他のセキュリティソリューションと併用する

スタンドアロンのウイルス対策ソフトウェアなどのセキュリティソリューションの有無にかかわらず、お使いの環境で Acronis Cyber Protect をご利用いただけます。

他のセキュリティソリューションがない場合、ライセンスと必要に応じて、Acronis Cyber Protect を包括的なサイバープロテクション用に、もしくは従来通り、バックアップと復元用にご利用いただけます。各ライセンスで利用できる機能の詳細については、「Acronis Cyber Protect 15 エディションのクラウド配置を含んだ比較」を参照してください。必要なモジュールだけを有効化することにより、保護計画のスコープを調整できます。

現在の環境ですでに他のセキュリティソリューションをお持ちでも、ウイルスやその他のマルウェアからの保護を含む完全なサイバープロテクションのためにAcronis Cyber Protectを選択いただけます。その場合、競合を避けるために別のセキュリティソリューションを無効にするか削除する必要があります。

あるいは、ご使用中のセキュリティソリューションを無効にしたり削除したりせずに、サイバープロテクションを強化したいと思うかもしれません。ウイルス対策とマルウェア対策モジュールを保護計画で使用しないようにするだけで、そうすることも可能です。これら以外のすべてのモジュールは自由にお使いいただけます。

制限事項

- バックアップのマルウェア対策スキャンを使用するには、Cyber Protect Management Server のインストール時にスキャンサービスをインストールする必要があります。
- HTML5 クライアントを介したリモートアクセスは、Cyber Protect Management Server が Linux が実行されているマシンにインストールされている場合にのみ使用できます。

ソフトウェア要件

推奨 Web ブラウザ

Webインターフェイスは、次のWebブラウザに対応しています。

- Google Chrome 29以降
- Mozilla Firefox 23以降
- Opera 16以降
- Windows Internet Explorer 10以降

注意
クラウド配置の場合、Internet Explorerはサポートされません。

- 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

エージェント

エージェント for Windows

- Windows XP Professional SP1（x64）、SP2（x64）、SP3（x86）
- Windows XP Professional SP2（x86）は、Windowsエージェントのスペシャル版をサポートします。このサポートの詳細と制限事項については、「Windows XP SP2のエージェント」をご参照ください。
- Windows XP Embedded SP3
- Windows Server 2003 SP1/2003 R2以降 – StandardおよびEnterpriseエディション (x86、x64)

注意
Acronis Cyber Protectでは、MicrosoftのKB940349アップデートが必要ですが、これは別途ダウンロードすることができなくなりました。KB940349の機能をご利用のマシンで確実に利用できるようにするために、現在利用可能なWindows Server 2003のアップデートプログラムをすべてインストールしてください。
KB940349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。

- Windows Small Business Server 2003/2003 R2
- 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（x86、x64）

注意
Windows 7でAcronis Cyber Protectを使用するには、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拡張セキュリティ更新プログラム（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

SQL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）、Active Directoryエージェント

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対象となるバージョンのアプリケーションを実行するマシンにインストールできます。

- SQLエージェントは、Microsoft Windows 7 StarterおよびHomeエディション（x86、x64）上のオンプレミス配置をサポートしていません

Exchangeエージェント（メールボックスバックアップ用）

このエージェントは、Microsoft Exchange Server を使用するマシンにも、使用しないマシンにもインストールできます。

- 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

エージェント for Office 365

- 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）

エージェント for Linux

注意
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。

Acronis Cyber Protect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, 8.0, 8.1, 8.2, 8.3, 8.4*, 8.5*, 8.6*, 8.7*
- 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
- Fedora 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31
- 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, 8.0, 8.1, 8.2, 8.3, 8.4*, 8.5*
- CentOS Stream 8
- Oracle Linux 5.x, 6.x, 7.x, 8.0, 8.1, 8.2, 8.3, 8.4*, 8.5*– Unbreakable Enterprise KernelとRed Hat Compatible Kernelの両方
- CloudLinux 5.x, 6.x, 7.x, 8.0, 8.1, 8.2, 8.3, 8.4*, 8.5*
- ClearOS 5.x, 6.x, 7.x, 8.0, 8.1, 8.2, 8.3, 8.4*, 8.5*
- AlmaLinux 8.4*、8.5*
- Rocky Linux 8.4*
- ALT Linux 7.0

RPM Package Manager を使用していないシステム（Ubuntu システムなど）に製品をインストールする場合は、インストールの前に、ルート ユーザーとして次のコマンドを実行するなどしてこのマネージャを手動でインストールする必要があります: `apt-get install rpm`

お使いのLinuxディストリビューションがD-Busメカニズムに対応していない場合（例えば、Red Hat Enterprise Linux 6.xやCentOS 6.x）Acronis Cyber Protectは、オペレーティングシステムがD-Busをサポートするロケーションを提供しないため、セキュアキーの保管場所としてデフォルトのロケーションが使用されます。

*4.18～5.19のカーネルのみサポート

エージェント for Mac

注意
ARMベースのプロセッサ（例: AppleシリコンM1およびM2）はサポートされていません。

- OS X Mavericks 10.9
- OS X Yosemite 10.10
- OS X El Capitan 10.11
- macOS Sierra 10.12
- macOS High Sierra 10.13
- macOS Mojave 10.14
- macOS Catalina 10.15
- macOS Big Sur 11
- macOS Monterey 12
- macOS Ventura 13

エージェント for VMware（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。

エージェント for Hyper-V

- 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以外の全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以外の全インストールオプション
- Microsoft Hyper-V Server 2019
- Windows Server 2022 with Hyper-V – すべてのインストールオプション（Nano Serverを除く）

Scale Computing HC3エージェント（仮想アプライアンス）

このエージェントは、Cyber Protect ウェブ コンソールを介して Scale Computing HC3 クラスターに配置される仮想アプライアンスとして提供されます。このエージェントのスタンドアロンインストーラがありません。

Scale Computing Hypercore 8.8、8.9、9.0

管理サーバー（オンプレミスデプロイメントのみ）

Windowsの場合

- Windows 7 – すべてのエディション（x86、x64）

> **注意**
> Windows 7でAcronis Cyber Protectを使用するには、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拡張セキュリティ更新プログラム（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 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 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

Linuxの場合

> **注意**
> 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。
>
> Acronis Cyber Protect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_64のディストリビューションを含む）。

x86ディストリビューションはサポートされていません。

- Red Hat Enterprise Linux 6.x, 7.x, 8.0, 8.1, 8.2, 8.3, 8.4*, 8.5*, 8.6*, 8.7*
- 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
- Fedora 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31
- 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, 8.0, 8.1, 8.2, 8.3, 8.4*, 8.5*
- CentOS Stream 8
- Oracle Linux 5.x, 6.x, 7.x, 8.0, 8.1, 8.2, 8.3, 8.4*, 8.5*– Unbreakable Enterprise KernelとRed Hat Compatible Kernelの両方
- CloudLinux 5.x, 6.x, 7.x, 8.0, 8.1, 8.2, 8.3, 8.4*, 8.5*
- ClearOS 5.x, 6.x, 7.x, 8.0, 8.1, 8.2, 8.3, 8.4*, 8.5*
- AlmaLinux 8.4*、8.5*
- Rocky Linux 8.4*
- ALT Linux 7.0

RPM Package Manager を使用していないシステム（Ubuntu システムなど）に製品をインストールする場合は、インストールの前に、ルート ユーザーとして次のコマンドを実行するなどしてこのマネージャを手動でインストールする必要があります: `apt-get install rpm`

お使いのLinuxディストリビューションがD-Busメカニズムに対応していない場合（例えば、Red Hat Enterprise Linux 6.xやCentOS 6.x）Acronis Cyber Protectは、オペレーティングシステムがD-Busをサポートするロケーションを提供しないため、セキュアキーの保管場所としてデフォルトのロケーションが使用されます。

*4.18～5.19のカーネルのみサポート

Storage Node（オンプレミスデプロイメントのみ）

- Windows Server 2008 - Standard、Enterprise、Datacenter、Foundationの各エディション（x64のみ）
- Windows Small Business Server 2008
- Windows 7 – すべてのエディション（x64のみ）
- Windows Server 2008 R2 – Standard、Enterprise、Datacenter、Foundation 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（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
- Windows 10 – （Home、Pro、Education、Enterprise、IoT Enterprise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 Server 2022 - Nano Server以外のすべてのインストールオプション

Windows XP SP2エージェント

Windows XP SP2エージェントは、Windows XP SP2の32ビットバージョンのみサポートします。

Windows XP SP1（x64）、Windows XP SP2（x64）、またはWindows XP SP3（x86）を実行中のマシンを保護するには標準のWindowsエージェントを使用します。

Windows XP SP2エージェントにはAcronis Cyber Backup 12.5ライセンスが必要です。Acronis Cyber Protect 15ライセンスキーはサポート対象外です。

インストール

Windows XP SP2エージェントには、550MB以上のディスク容量と150MB以上のRAMが必要となります。バックアップ中、一般的にエージェントは約350MBのメモリを消費します。処理するデータの量により、最大使用量は2GBに達する場合があります。

バックアップするマシンのローカルにのみWindows XP SP2エージェントをインストールできます。エージェント設定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]** > **[Windows XP SP2エージェント]** の順にクリックします。

Cyber Protect モニターとブータブルメディアビルダーはインストールできません。ブータブルメディアのISOファイル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 > **[ダウンロード]** > **[ブータブルメディア]** の順にクリックします。

アップデート

Windows XP SP2エージェントは、リモートアップデート機能をサポートしていません。エージェントをアップデートするには、セットアッププログラムの新しいバージョンをダウンロードし、インストールを繰り返します。

Windows XPをSP2からSP3へアップデートした場合、Windows XP SP2エージェントをアンインストールし、標準のWindowsエージェントをインストールします。

制限事項

- ディスクレベルのバックアップのみが使用可能です。ディスクまたはボリュームのバックアップから個別のファイルを復元します。
- イベント別のスケジュールはサポートされていません。
- 保護計画実行の条件はサポートされていません。
- 以下のバックアップ先だけがサポートされます。

    - 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
    - Secure Zone
- **バージョン12**バックアップ形式、および**バージョン12**バックアップ形式を必要とする機能はサポートされていません。特に、物理データ配送は使用できません。**パフォーマンスとバックアップウィンドウ**オプションは有効な場合、グリーンレベル設定にのみ適用されます。
- 復元のための個別のディスク/ボリュームの選択および復元中の手動ディスクマッピングは、Webインターフェースでサポートされていません。この機能は、ブータブルメディアで利用できます。
- オフホストのデータ処理はサポートされていません。
- Windows XP SP2エージェントは、バックアップへの次の操作を実行できません。
    - バックアップの仮想マシンへの変換
    - バックアップからのボリュームのマウント
    - バックアップからのファイル抽出
    - バックアップのエクスポートおよび手動ベリファイ。

  これらの操作は、別のエージェントを使用して実行できます。
- Windows XP SP2エージェントによって作成されたバックアップを仮想マシンとして実行することはできません。

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

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。

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

Acronis Cyber Protect 15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）

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。

注意
ゲストOSメソッド内のバックアップを介してサポートされる、次のハイパーバイザーベンダーとバージョンが明示的なテストの対象となっています。ただし、以下のリストに掲載されていないベンダーまたはバージョンのハイパーバイザーを実行している場合でも、**ゲストOSメソッド内のバックアップ**は、必要なすべてのシナリオで正しく動作する可能性があります。

AcronisCyber Protectの使用中に、特定のハイパーバイザーのベンダーと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。

プラットフォーム	ハイパーバイザレベルのバックアップ（エージェントレス バックアップ）	ゲスト OS の内部からバックアップ
VMware		
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	+	+
VMware vSphere Hypervisor（Free ESXi）**		+
VMware サーバー（VMware 仮想サーバー） VMware Workstation VMware ACE VMware Player		+
Microsoft* **		
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（Hyper-V 使用）– すべてのインストールオプション（Nano Serverを除く） Microsoft Hyper-V Server 2016 Windows Server 2019（Hyper-V 使用）– すべてのインストールオプション（Nano Serverを除く）	+	+

Microsoft Hyper-V Server 2019 Windows Server 2022（Hyper-V 使用） – すべてのインストールオプション（Nano Serverを除く）		
Microsoft Virtual PC 2004、2007 Windows Virtual PC		+
Microsoft Virtual Server 2005		+
Scale Computing		
Scale Computing Hypercore 8.8、8.9、9.0	+	+
Citrix		
Citrix XenServer 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、7.6		完全仮想化（HVM）ゲストのみ。準仮想化（PV）ゲストはサポート対象外です。
Red Hat および Linux		
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		+
Red Hat Virtualization（oVirtによる管理）4.2、4.3、4.4 （クラウド配置でのみ利用可能）	+	+
Kernel-based Virtual Machine（KVM）		+
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） （クラウド配置およびAdvancedライセンスでのみ利用可能）	+	+
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） （クラウド配置およびAdvancedライセンスでのみ利用可能）	+	+
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） （クラウド配置およびAdvancedライセンスでのみ利用可能）	+	+

Parallels		
Parallels Workstation		+
Parallels Server 4 Bare Metal		+
Oracle		
Oracle VM Server 3.0、3.3、3.4		完全仮想化（HVM）ゲストのみ。準仮想化（PV）ゲストはサポート対象外です。
Oracle VM VirtualBox 4.x		+
Nutanix		
NutanixAcropolisハイパーバイザー(AHV)20160925.xから20180425.x		+
Virtuozzo（クラウド配置でのみ利用可能）		
Virtuozzo 6.0.10、6.0.11、6.0.12	+	仮想マシンのみ。コンテナはサポート対象外です。
Virtuozzo 7.0.13、7.0.14	Ploopコンテナのみ。仮想マシンはサポート対象外です。	仮想マシンのみ。コンテナはサポート対象外です。
Virtuozzo Hybrid Server 7.5	+	仮想マシンのみ。コンテナはサポート対象外です。
Virtuozzo Hybrid Infrastructure（クラウド配置でのみ利用可能）		
Virtuozzo Hybrid Infrastructure、3.5、4.0、4.5	+	+
Amazon		
Amazon EC2インスタンス		+
Microsoft Azure		
Azure仮想コンピュータ		+

*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。

***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

- **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。
- **パス スルー ディスク**
  エージェント for Hyper-V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**
  VMwareエージェントと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。ESXiと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。
- **論理ボリューム（LVM）を含むLinuxマシン**

VMwareエージェントとHyper-Vエージェントでは、LVMを持つLinuxマシンに対して、
  - P2VおよびV2P移行。バックアップおよびリカバリ用ブータブルメディアの作成には、Linuxエージェントまたはブータブルメディアを使用します。
  - Linux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たバックアップから仮想マシンを実行します。
  - Linux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たバックアップを仮想マシンに変換します。
- **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。
- **セキュア起動**（VMware vSphere 6.5で導入）

  セキュア起動は仮想コンピュータが新しい仮想コンピュータ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。
- 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。

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。

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
- CheckPoint Harmony Endpoint
- 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ます。
2. プロテクションエージェントをインストールします。
3. Secure Zoneを作成します。
4. 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 バックアップを実行できます。ブータブル メディアを使用してバックアップしないでください。

ソフトウェア固有の復元手順

Microsoft BitLocker Drive EncryptionとCheckPoint Harmony Endpoint

再起動によるリカバリやブータブルメディアを使用することで、システムを復元できます。

再起動を伴う復元

暗号化されたシステムをリカバリするには、"物理マシンをリカバリする"（307ページ）の手順を実行します。

"再起動を伴う復元"（314ページ）の要件が満たされていることを確認します。

注意
BitLockerで暗号化されたボリュームの場合、再起動による復元はUEFIベースのマシンでのみ利用可能であり、Windows 7以降またはWindows Server 2008 R2以降が動作している必要があります。
CheckPointで暗号化されたボリュームの場合、再起動時の復元はUEFIベースのマシンでのみ利用可能であり、Windows 10およびWindows 11が動作している必要があります。

BIOSベースのマシンや、Linux/macOSで動作しているマシンでは、再起動による復元は実行できません。

ブータブルメディアによる復元

1. ブータブル メディアから起動します。
2. システムを復元します。

   重要
   バックアップ済みのデータは、暗号化されていない状態でリカバリされます。

3. 復元されたシステムを再起動します。
4. 暗号化ソフトウェアを有効にします。

パーティションが複数あるディスクで、1つのパーティションのみをリカバリする場合は、オペレーティングシステムで復元を実行します。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リカバリが可能なのは、ブータブルメディアを使用する場合のみです。

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

Acronis Cyber Protectにより、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できます。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。

Windowsに変数を追加するには

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に変数を追加するには

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に変数を追加するには

1. 仮想アプライアンスのマシン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。

システム要件

次の表には、一般的なインストールのためのディスク領域とメモリ要件をまとめます。インストールはデフォルト設定で実行されます。

インストールされるコンポーネント	インストールに必要なディスク領域	最低メモリ使用量
エージェント for Windows	850MB	150MB
エージェント for Windowsには、次のエージェントのいずれかが必要です。 • SQLエージェント • Exchangeエージェント	950MB	170MB
エージェント for Windowsには、次のエージェントのいずれかが必要です。 • VMwareエージェント（Windows） • エージェント for Hyper-V	1170MB	180MB
エージェント for Office 365	500 MB	170 MB
エージェント for Linux	2.0GB	130MB
エージェント for Mac	500MB	150MB
オンプレミスデプロイのみ		
WindowsのManagement Server	1.7GB	200MB
LinuxのManagement Server	1.5GB	200MB
Management Serverとエージェント for Windows	2.4GB	360MB
Management ServerとWindows、Microsoft SQL Server、Microsoft Exchange Serve、Active Directory Domain Servicesを実行するコンピュータのエージェント	3.35GB	400MB
Management Serverとエージェント for Linux	4.0GB	340MB
Storage Nodeとエージェント for Windows • 64ビットプラットフォームのみ。 • 重複除外を使用するには、最低8GBのRAMが必要です。詳細については、"重複除外のベスト プラクティス"（613ページ）を参照してください。	1.1GB	330MB

バックアップ中、一般的にエージェントは約350 MBのメモリを消費します（500 GBのボリュームバックアップ中に測定）。処理するデータの量や種類により、最大使用量は2GBに達する場合があります。

サイズの大きなバックアップセット（600GB以上）にバックアップするには、バックアップセットのサイズ1TBあたり約1GBのRAMが必要です。

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。

登録済みのワークロードが1件存在する管理サーバーでは、200MBのメモリが消費されます。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。さらにワークロードが1つ増えるごとに、追加で約2MBのメモリが消費されます。このため、100件のワークロードが登録されたサーバーでは、オペレーティングシステムと実行中のアプリケーションの他に約400MBのメモリが必要になります。

登録済みワークロードの最大数は900～1000です。この制限は管理サーバーの組み込みSQLiteデータベースによるものです。

この制限を回避するには、管理サーバーのインストールの際に、外部Microsoft SQL Serverインスタンスを指定します。外部SQLデータベースを利用することで、パフォーマンスを大きく低下させずに、最大8000件のワークロードを管理サーバーに登録できます。8000件のワークロードを登録した場合、SQLサーバーインスタンスは約8GBのRAMを消費することになります。

バックアップの作成速度が低下しないよう、最大500件のワークロードごとにグループを作成して、グループでワークロードを管理してください。

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。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	WinPE ブータブルメディア	Linux ベースのブータブル メディア	Macブータブル メディア	

FAT16/32	全エージェント	+	+	+	制限なし
NTFS		+	+	+	
ext2/ext3/ext4		+	+	-	
HFS+	エージェント for Mac	-	-	+	
APFS		-	-	+	• 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	エージェント for Linux	-	+	-	• ディスクバックアップからファイルを除外することはできません • 高速増分/差分バックアップを有効にできません
ReiserFS3		-	+	-	
ReiserFS4		-	+	-	• ディスクバックアップからファイルを除外することはできません • 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	+	+	+	
XFS		+	+	+	• ディスクバックアップからファイルを除外することはできません • 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 • テープに保存されているバックアップからのファイルの復元はサポートされていません
Linux Swap	エージェント for Linux	-	+	-	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、ブータブルメディアを復元に使用することはできません	+	• 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 • バックアップからファイルを除外することはできません • 個別のファイルはバックアップから復元できません

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。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復元はディスクレベルで制限なく行うことができます。Acronis VSS Provider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。

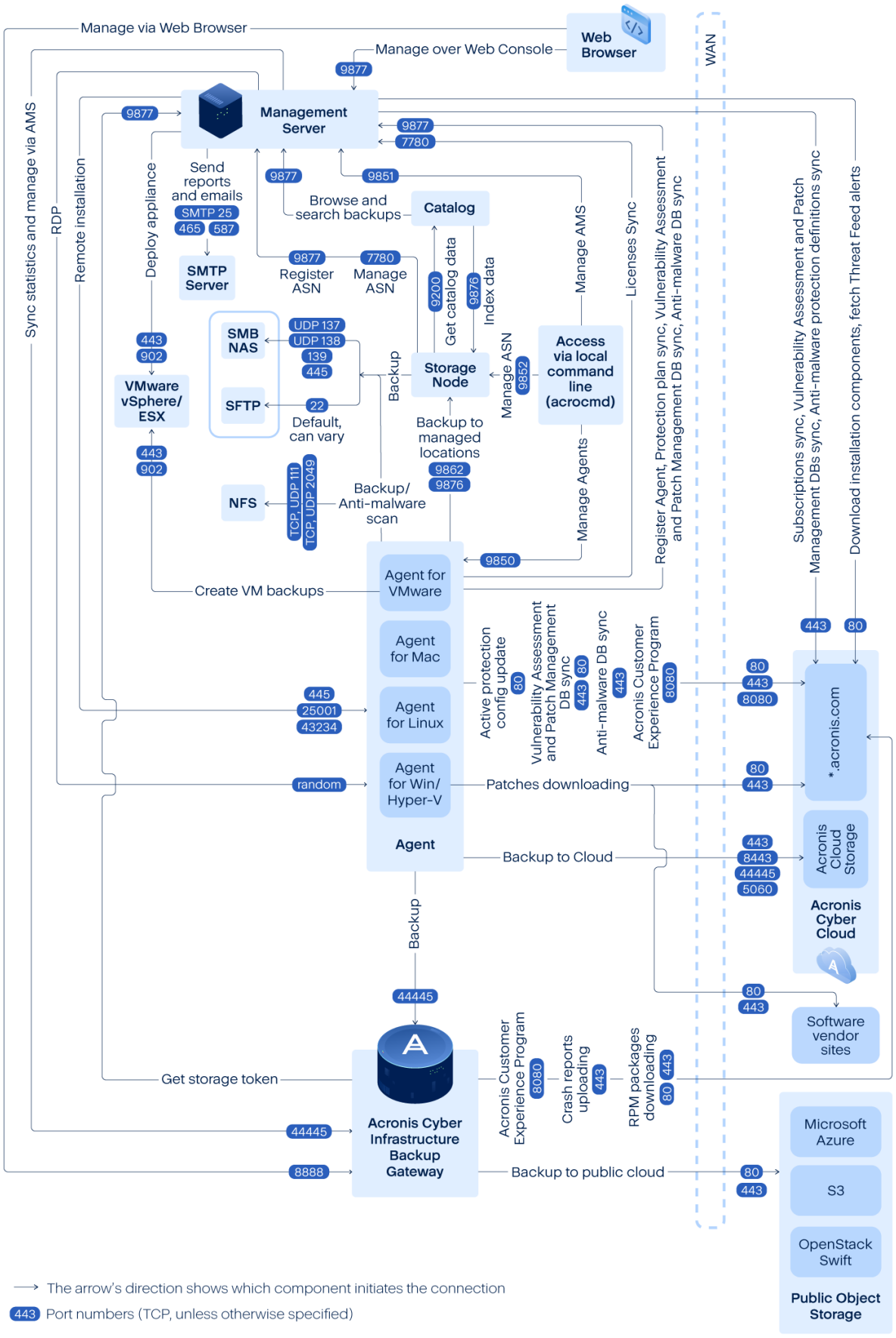
Acronis Cyber Protectのネットワーク接続図

このトピックには、Acronis Cyber Protectの接続図が含まれています。

Acronis Cyber Protectが利用するポート、サービス、プロセスのリストについては、アクロニスのナレッジベースをご覧ください。

- Windowsについては、「Windowsのサービスとプロセス（65663）」を参照してください。
- Linuxについては、「Linuxのコンポーネント、サービス、プロセス（67276）」を参照してください。

ネットワーク接続図 - Cyber Protectプロセス



重要
ネットワーク図の送信ポートは動的なものです。一部のサービスでは、受信接続に動的ポートも使用できます。ネットワークの問題をトラブルシュートする際には、動的ポートを介したトラフィックが許可されていることを確認してください。

動的ポートはオペレーティングシステムによって管理され、ランダムに割り当てられます。Windowsのデフォルトの動的ポート範囲は49152から65535です。この範囲は、オペレーティングシステムによって異なる場合があり、手動で変更することも可能です。

管理サーバーは、Acronis Cyber Protectの主要コンポーネントです。2つのTCPポートが公開されています。（7780および9877）。TLSで保護されたポート9877は、REST APIとウェブベースのユーザーインターフェースの両方を提供するために使用されます。REST APIのエンドポイントでは、JWTトークンを使用してリクエストが認証されます。JWTトークンは個別のHTTPヘッダーとして、またはHTTP Cookieとしてエンコードされます。ポート7780には、ZMTP CURVE認証と暗号化を備えたZeroMQプロトコルが実装されています。エージェントとStorage Nodeが管理サーバーと非同期的に管理メッセージを交換する場合は、ポート7780が使用されます。また、管理サーバーはクラウドサービスと通信し、標準的なHTTPおよびHTTPSポートを使ってアップデートをダウンロードします。

Storage Nodeは、Acronis Cyber Protectのストレージコンポーネントです。TCPポート9876が公開されています。このポートは、バックアップデータの送受信に使用されます。転送はTLSで保護され、認証には相互TLSが使用されます。アプリケーションレベルのプロトコルは、Acronis独自のものです。Storage Nodeとバックエンドストレージシステムの通信には、適切なプロトコルと認証メカニズムが使用されます。

カタログは、Acronis Cyber Protectの副次的なコンポーネントです。カタログにより、Storage Node上のデータがインデックス化されます。カタログへのアクセスにはポート9876、インデックスの公開にはポート9200が使用されます。

バックアップゲートウェイは、Acronis独自の次世代型のデータアクセス用プロトコルを実装しています。カスタマーがクラウドバックアップを選択する場合、同じコンポーネントがAcronis Cyber Cloudでも使用されます。TCPポート44445（IANA登録済み）がゲートウェイで使用されます。データ保護にはTLSが使用され、認証には相互TLSが使用されます。バックアップゲートウェイでは、HTTPSベースの管理サービス用にポート8888が使用されることもあります。

エージェントと、管理サーバー、Storage Node、バックアップゲートウェイとの通信には、上述のポートが使用されます。エージェントのバックアップ先として、標準ベースのファイルサービス（SMB、NFS）が使用されている場合、それらとの通信にも使用されます。この場合は、標準的なポートと適切な認証プロトコルとなります。こういった機能がVMwareエージェントで構成されている場合、VMware vSphere APIでは、VMware vSphereで定義されたポートが使用されます。

Linuxの脆弱性診断は、Acronis Cyber Cloudに配置されたCVSSサービス経由で実装されます。プロテクションエージェントは、https://cloud.acronis.com/services.jsonの一覧から、pingによる最も近いデータセンターを動的に選択します。

オンプレミスデプロイ

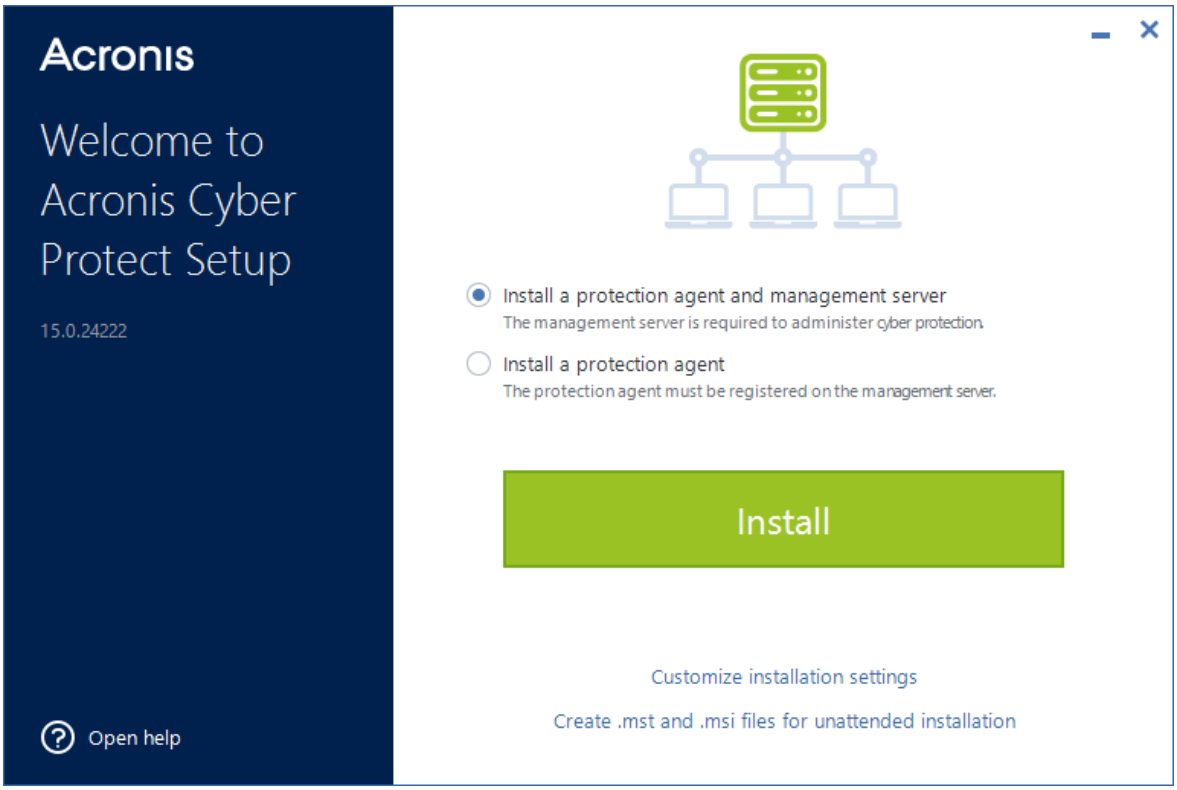
オンプレミス配置には、"コンポーネント"（47ページ）セクションに記載されている複数のソフトウェアコンポーネントが含まれます。これらのコンポーネントと必要なポート間のインタラクションの詳細については、"Acronis Cyber Protectのネットワーク接続図"（78ページ）を参照してください。

Management Serverのインストール

Windows でのインストール

Management Serverのインストール手順

1. 管理者としてログオンし、Acronis Cyber Protect プログラムの設定を起動します。
2. （オプション）プログラムの設定の言語を変更するには、**[言語の設定]** をクリックします。
3. ライセンス契約とプライバシーステートメントに同意して、**[次へ]** をクリックします。
4. **[プロテクション エージェントおよび管理サーバーのインストール]** のデフォルト設定を使用します。



5. 次の手順のいずれかを実行します。
   - **[インストール]** をクリックします。
     これは、製品をインストールする最も簡単な方法です。インストール パラメータの多くは、デフォルト値に設定されます。
     次のコンポーネントがインストールされます。

- 管理サーバー
- リモート インストールのコンポーネント
- エージェント for Windows
- 該当するハイパーバイザまたはアプリケーションがコンピュータで検出される場合は、その他のエージェント（エージェント for Hyper-V、エージェント for Exchange、エージェント for SQL、エージェント for Active Directory）
- ブータブルメディアビルダー
- コマンドラインツール
- Cyber Protectモニター

- **[インストール設定のカスタマイズ]** をクリックしてセットアップを構成します。
  インストールするコンポーネントを選択したり、その他のパラメータを指定したりできます。詳細については、"インストール設定のカスタマイズ"（83ページ）を参照してください。
- **[無人インストールの .mst および .msi を作成]** をクリックして、インストールパッケージを抽出します。.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、**[生成]** をクリックします。ここでは、その他の手順は不要です。
  グループポリシーを使用してエージェントを配置する場合は、"グループポリシーによるエージェントの配置"（174ページ）を参照してください。

6. インストールを続けます。
7. インストールが完了した後、［**閉じる**］をクリックします。

管理サーバーの使用を開始するには、現在のAcronisアカウントにサインインするか、アクティベーションファイルを使用してサーバーを有効化します。

インストール設定のカスタマイズ

このセクションでは、インストール中に変更できる設定について説明します。

インストールするコンポーネント

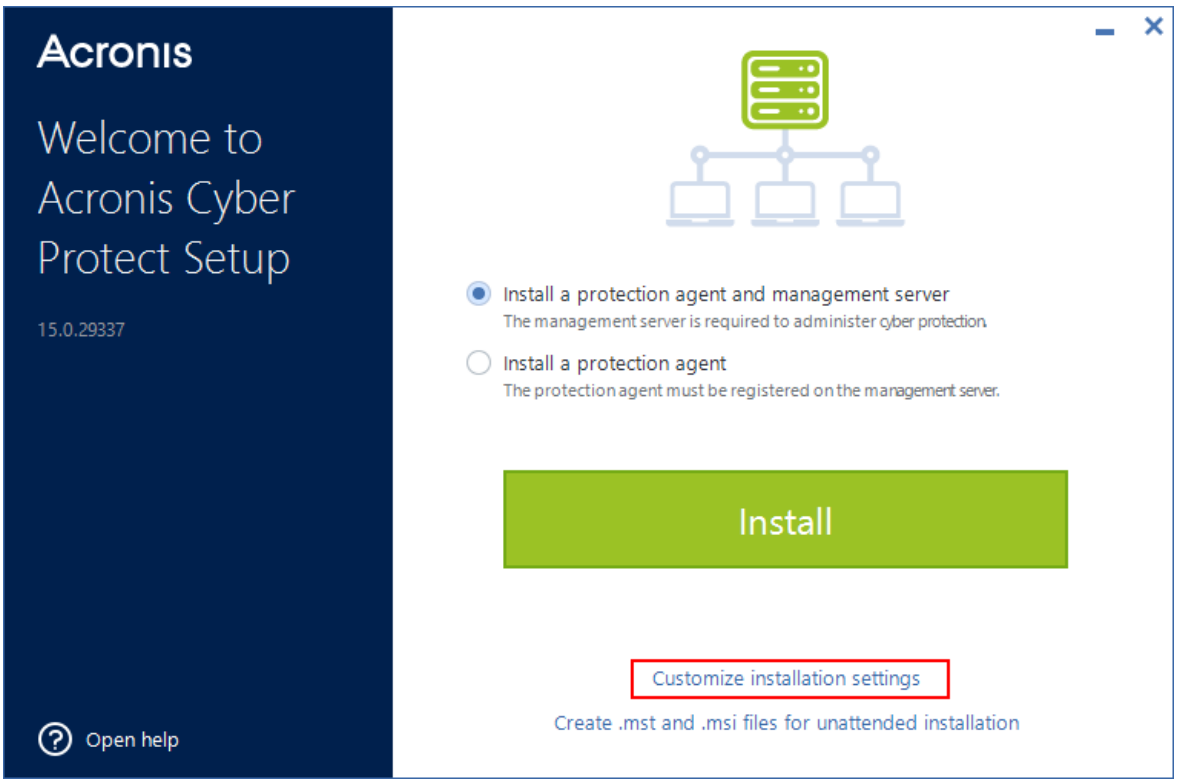
管理サーバーとプロテクションエージェントからなるインストール構成か、プロテクションエージェントのみのインストール構成かに応じて、デフォルトで次のコンポーネントが選択されます。

管理サーバーとプロテクションエージェント	プロテクションエージェントのみ
管理サーバー	Windowsエージェント
リモート インストールのコンポーネント	ブータブルメディアビルダー
Windowsエージェント	コマンドラインツール
ブータブルメディアビルダー	Cyber Protectモニタ
コマンドラインツール	
Cyber Protectモニタ	

利用できるコンポーネントの完全なリストについては、"コンポーネント"（47ページ）を参照してください。

オプションコンポーネントをインストールするには

1. インストールウィザードで、[**インストール設定のカスタマイズ**] をクリックします。



2. [**インストールする項目**] の [**変更**] をクリックします。
3. 任意のコンポーネントを選択して、[**完了**] をクリックします。
4. プロンプトが表示されたら、選択したコンポーネントの設定を構成します。
5. [**インストール**] をクリックします。

サービスのログオン アカウント

エージェントまたは管理サービスを実行するアカウントを変更するには、それぞれ [**エージェントサービスのログオンアカウント**] オプション、または [**管理サーバーサービスのログオンアカウント**] オプションを使用します。

以下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。このオプションの利点は、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**（管理サーバーサービスと Storage Node サービスのデフォルト）
  エージェント、管理サーバー、Storage Nodeサービスのアカウント名は、それぞれ **Acronis Agent User**、**AMS ユーザー**、**ASN 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製品をインストールする場合は、プログラムの設定で、各サービスに既存のアカウント（または同じアカウント）を指定するよう求められます。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。

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。

また管理サーバーをSQLデータベースで構成する場合、**[次のアカウントを使用する]** を選択すれば、Microsoft SQL ServerのWindows認証を使用できるようになります。

[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、アカウントに割り当てられたユーザー権限が失われる場合、関連するコンポーネントで正しくない挙動が発生したり、まったく動作しなくなったりする可能性があります。

サービスログオンアカウントに必要なユーザー権限

プロテクションエージェントは、Windowsマシンの**Managed Machine Service**（MMS）として稼働します。エージェントを正しく動作させるために、エージェントを実行するアカウントで次の権限が必要になります:

1. **Backup Operators**グループと**Administrators**グループにMMSユーザーを追加する必要があります。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. MMSユーザーに、`%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に対する**フルコントロール**を許可する必要があります。
3. MMSユーザーに、次のレジストリキーに属する特定のキーに対する**フルコントロール**を許可する必要があります。`HKEY_LOCAL_MACHINE\SOFTWARE\Acronis`。
4. MMSユーザーに対し、Windowsの以下のユーザー権限を割り当てる必要があります:
   - **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**

ASN（Acronis Storage Node）ユーザーには、Acronis Storage Nodeがインストールされているマシンのローカル管理者権限が必要です。

Windowsでユーザー権限を割り当てるには

注意
この手順では、例として**サービスとしてログオン**のユーザー権限を使用します。他のユーザー権限に関する手順も同様です。

1. 管理者としてコンピューターにログインします。
2. **コントロールパネル**で、**管理ツール**を開きます。または、キーボードのWin+Rキーを押して、**control admintools**と入力し、Enterキーを押します。
3. **ローカルセキュリティポリシー**を開きます。
4. [**ローカルポリシー**] を展開してから、[**ユーザー権限の割り当て**] をクリックします。
5. 右側のペインで [**サービスとしてログオン**] を右クリックしてから、[**プロパティ**] を選択します。
6. [**ユーザーまたはグループの追加**] をクリックして、新しいユーザーを追加します。
7. [**ユーザー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追加し、[**OK**] をクリックします。
8. [**サービスとしてログオンのプロパティ**] ウィンドウで [**OK**] をクリックし、変更内容を保存します。

注意
[**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を [**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**] のリストに含めることはできません。

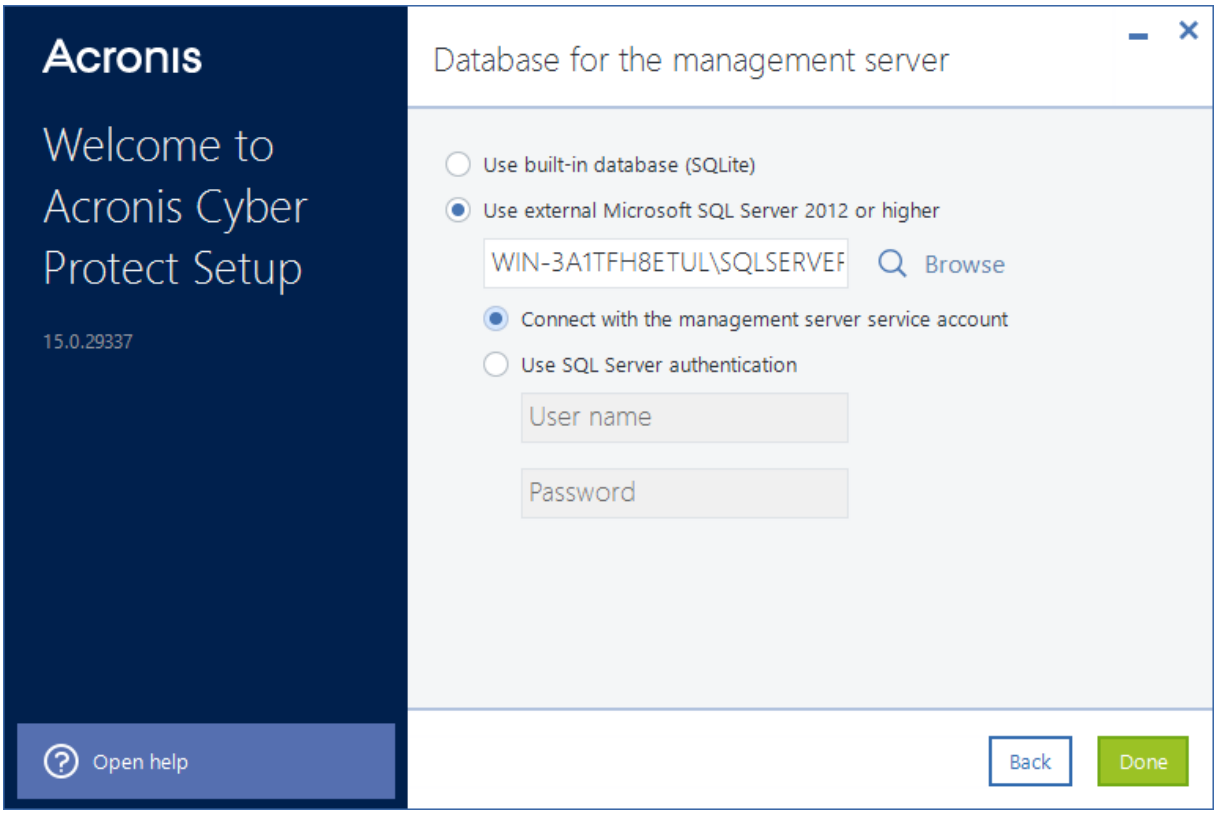
重要
インストール完了後、ログオンアカウントを手動で変更することは推奨されません。

Management Serverのデータベース

管理サーバーには、以下のデータベースを構成できます:

- SQLite
  管理サーバーはデフォルトで、ビルトインのSQLiteデータベースを使用します。管理サーバーには、約900～1000個のワークロードを登録できます。SQLiteとスキャンサービスには互換性がありません。
- Microsoft SQL
  Microsoft SQLを利用すれば、パフォーマンスを大きく低下させずに、最大8000件のワークロードを管理サーバーに登録できます。管理サーバー、スキャンサービス、その他のプログラムで、同一のMicrosoft SQLインスタンスを使用できます。
  以下のMS SQL Serverのバージョンがサポートされています:
  - Microsoft SQL Server 2019（Windows で実行）
  - Microsoft SQL Server 2017（Windows で実行）
  - Microsoft SQL Server 2016
  - Microsoft SQL Server 2014
  - Microsoft SQL Server 2012

Microsoft SQLのインスタンスが、デフォルト名である**MSSQLSERVER**の場合、必ずこのインスタンスが実行されているマシンの名前を指定します。インスタンスにカスタム名がある場合は、**<マシン名>\<インスタンス名>**の形式で指定する必要があります。



注意
Microsoft SQLインスタンスを実行しているマシンで、SQLサーバーのブラウザサービスとTCP/IPプロトコルが有効になっていることを確認してください。SQL Server Browser Serviceを起動する方法の詳細については、http://msdn.microsoft.com/en-us/library/ms189093.aspxを参照してください。同様の手順を使用して、TCP/IP プロトコルを有効にすることができます。

指定したMicrosoft SQLインスタンスに接続するには、以下の認証方法を使用します:

- Windows認証（**管理サーバーのサービスアカウントで接続**）
  管理サーバーサービスのログオンアカウントを **[次のアカウントを使用する]** オプションで構成（例えば、**<マシン名>**\Administratorを指定）した場合、このメソッドを使用できます。指定したアカウントには、Microsoft SQL Serverの**dbcreator**または**sysadmin**ロールが必要です。
  ログオンアカウントの詳細情報については、"サービスログオンアカウントに必要なユーザー権限"（85ページ）を参照してください。
- SQL サーバー認証
  このメソッドは常に使用できます。指定したアカウントには、Microsoft SQL Serverの**dbcreator**または**sysadmin**ロールが必要です。

スキャンサービス

スキャンサービスはオプションのコンポーネントであり、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のバックアップに対するマルウェア対策スキャンを実行できます。スキャンサービスと管理サーバーは、同じマシンにインストールしておく必要があります。

スキャンサービスをインストールすると、以下の機能を利用できるようになります:

- バックアップスキャンの計画
- バックアップスキャンの詳細ウィジェット
- 企業ホワイトリスト
- 安全な復元
- バックアップの一覧の [**ステータス**] 列

管理サーバーのインストール時にスキャンサービスをインストールできます。または既存のバージョンに後からスキャンサービスを追加することもできます。スキャンサービスとしてオプションコンポーネントをインストールする方法については、"オプションコンポーネントをインストールするには"（84ページ）を参照してください。

重要

スキャンサービスと管理サーバーが使用するデフォルトのSQLiteデータベースの間に互換性はありません。

スキャンサービスは、Microsoft SQLまたはPostgerSQLデータベースを使用して構成できます。いずれかを選択する方法については、"スキャンサービスのデータベース"（89ページ）を参照してください。

スキャンサービスのデータベース

スキャンサービスと管理サーバーのデフォルトデータベースであるSQLiteの間には、互換性がありません。

管理サーバーでSQLiteが使用されている場合、スキャンサービスは必ずPostgreSQLデータベースを使用して構成します。PostgreSQL 9.6以降がサポートされています。

管理サーバーでMicrosoft SQL Serverが使用されている場合、追加の設定なしに、同じデータベースでスキャンサービスを構成できます。スキャンサービスは、PostgreSQLデータベースによって構成することもできます。

PostgreSQLデータベースでスキャンサービスを構成するには

1. インストールウィザードの **[スキャンサービスのデータベース]** 以下で、**[変更]** をクリックします。
2. **[PostgreSQLサーバーデータベース]** を選択します。
3. PostgreSQLインスタンスのホスト名、またはIPアドレスとポートを指定します。
4. **CREATEDB**権限を持つユーザー、またはスーパーユーザーの資格情報を指定します。

   注意
   PostgreSQL 10以降では、SCRAM-SHA-256認証方式はサポートされていません。

5. **[完了]** をクリックします。

ポート

管理サーバーにアクセスするためにWebブラウザで使用されるポート（デフォルトでは9877）、および製品コンポーネント間の通信に使用されるポート（デフォルトでは7780）は、カスタマイズできます。インストールの完了後に後者のポートを変更する場合は、すべてのコンポーネントを再登録する必要があります。

Windows ファイアウォールは、インストール中に自動的に設定されます。別のファイアウォールを使用している場合は、そのファイアウォールを経由する受信要求と送信要求の両方に対して必ずこのポートを開いてください。

プロキシサーバー

クラウドストレージにバックアップする場合、またクラウドストレージから復元する場合は、プロテクションエージェントがHTTPプロキシサーバーを使用するかどうかを選択できます。

また、異なるAcronis Cyber Protectコンポーネント間の通信には、同一のプロキシサーバを使用します。

プロキシサーバを使用するには、ホスト名またはIPアドレスとポート番号を指定します。プロキシサーバで認証が必要な場合は、アクセス認証情報を指定します。

注意
プロキシサーバを使用している場合、各保護機能の定義（ウイルス対策およびマルウェア対策の定義、高度な検索の定義、脆弱性診断とパッチ管理の定義）をアップデートすることはできません。

Linux でのインストール

インストールする前に

1. エージェント for LinuxとManagement Serverをインストールする場合は、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。
2. 管理サーバーによって使用されるデータベースを選択します。

制限事項

Linuxマシン上で動作する管理サーバーは、自動検出の手順などで使用されるプロテクションエージェントのリモートインストールをサポートしていません。可能な回避策については、ナレッジベース（https://kb.acronis.com/content/69553）を参照してください。

インストール

管理サーバーをインストールするには、少なくとも4GBの空きディスク領域が必要です。

Management Serverのインストール手順

1. 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>
   ```

2. 使用許諾契約の内容に同意します。
3. [任意] インストールするコンポーネントを選択します。
   デフォルトでは、次のコンポーネントがインストールされます。
   - 管理サーバー
   - Linuxエージェント
   - ブータブルメディアビルダー
4. Management ServerにアクセスするためにWebブラウザで使用されるポートを指定します。デフォルト値は9877です。
5. 製品コンポーネント間の通信用のポートを指定しますデフォルト値は7780です。
6. **[次へ]** をクリックして、インストールを続行します。
7. インストール完了後、**[Webコンソールを開く]** を選択してから **[終了]** をクリックします。Cyber Protect ウェブ コンソールがデフォルト Web ブラウザで開きます。

管理サーバーの使用を開始するには、現在のAcronisアカウントにサインインするか、アクティベーションファイルを使用してサーバーを有効化します。

Acronis Cyber Protect アプライアンス

Acronis Cyber Protect アプライアンスを使用すると、次のソフトウェアを使用している仮想マシンを簡単に取得できます。

- CentOS
- Acronis Cyber Protect コンポーネント:
  - 管理サーバー
  - エージェント for Linux
  - VMwareエージェント（Linux）

アプライアンスは .zip アーカイブとして提供されます。アーカイブには .ovf ファイルと .iso ファイルが含まれます。.ovf ファイルを ESXi ホストにデプロイするか、.iso ファイルを使用して既存の仮想マシンを起動できます。アーカイブには、.ovf と同じディレクトリに配置する必要がある .vmdk ファイルも含まれます。

注意
VMware Host Client（スタンドアロン ESXi 6.0 以降の管理に使用する Web クライアント）では、ISO イメージを内部に含む OVF テンプレートを配置することはできません。そのような場合は、下記の要件を満たす仮想マシンを作成し、.iso ファイルを使用してソフトウェアをインストールします。

仮想アプライアンスの要件は以下のとおりです。

- 最小システム要件:
  - 2 つの CPU
  - 6 GB の RAM
  - 10 GB の仮想ディスク 1 つ（40 GB を推奨）
- VMware の仮想マシンの設定で、**[オプション]** タブ > **[全般]** > **[構成パラメータ]** の順にクリックし、`disk.EnableUUID` パラメータ値が `true` になっていることを確認します。

制限事項

Acronis Cyber Protectアプライアンスを含むLinuxマシン上で動作する管理サーバーは、自動検出の手順などで使用されるプロテクションエージェントのリモートインストールをサポートしていません。可能な回避策については、ナレッジベース（https://kb.acronis.com/content/69553）を参照してください。

ソフトウェアのインストール

1. 次のいずれかを実行します。
   - .ovf からアプライアンスをデプロイします。配置の完了後、生成されたマシンの電源を入れます。
   - .iso から既存の仮想マシンを起動します。

2. **[Acronis Cyber Protect のインストールまたはアップデート]** を選択し、**Enter** キーを押します。最初のセットアップウィンドウが表示されるのを待ちます。
3. （オプション）インストール設定を変更するには、**[設定の変更]** を選択し、**Enter** キーを押します。次の設定を指定できます。
   - アプライアンスのホスト名（デフォルトでは `AcronisAppliance- <ランダムな部分>`）。
   - Cyber Protect ウェブ コンソールへのログインに使用される「root」アカウントのパスワード（デフォルトでは**指定されていません**）。

     デフォルト値のままにする場合、Acronis Cyber Protect のインストール後に、パスワードを指定するよう求められます。このパスワードを設定しないと、Cyber Protect ウェブ コンソールと Cockpit ウェブ コンソールにログインできません。
   - ネットワークインターフェースカードのネットワーク設定:
     - **DHCP を使用**（デフォルト）
     - **静的 IP アドレスを設定**

     マシンに複数のネットワークインターフェースカードがある場合は、ランダムに 1 つが選択され、これらの設定が適用されます。
4. **[現在の設定でインストール]** を選択します。

その場合は、CentOS と Acronis Cyber Protect がマシンにインストールされます。

その他の操作

インストールの完了後、Cyber Protect ウェブ コンソールと Cockpit ウェブ コンソールへのリンクが表示されます。Cyber Protect ウェブ コンソールに接続し、Acronis Cyber Protect の使用を開始します（デバイスの追加、バックアップ計画の作成など）。

ESXi 仮想マシンを追加するには、**[追加]** > **[VMware ESXi]** をクリックし、vCenter Server またはスタンドアロン ESXi ホストのアドレスと資格情報を指定します。

Cockpit ウェブ コンソールで設定する Acronis Cyber Protect の設定はありません。コンソールで、さまざま操作やトラブルシューティングを行うことができます。

ソフトウェアのアップデート

1. アプライアンスの新バージョンの .zip アーカイブをダウンロードして展開します。
2. 前の手順で展開した .iso からマシンを起動します。
   a. .isoファイルをvSphereデータストアに保存します。
   b. .isoファイルをマシンのCD/DVDドライブに接続します。
   c. コンピュータを再起動します。
   d. [最初のアップデートの時のみ] **[F2]** を押してから、CD/DVDドライブが先頭に来るようにブート順を変更します。
3. **[Acronis Cyber Protect のインストールまたはアップデート]** を選択し、**Enter** キーを押します。
4. **[アップデート]** を選択し、**Enter** キーを押します。
5. アップデートの完了後、マシンのCD/DVDドライブから.isoファイルを取り出してください。

それにより、Acronis Cyber Protect がアップデートされます。.iso ファイル内の CentOS のバージョンもディスク上のバージョンより新しい場合は、Acronis Cyber Protect のアップデートの前に、オペレーティングシステムがアップデートされます。

Cyber Protect Webコンソールからマシンを追加する

以下のいずれかの方法でマシンを追加できます:

- セットアッププログラムをダウンロードし、ターゲットマシンのローカルで実行する。
- リモートでターゲット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。

制限事項

- リモートインストールは、Acronis管理サーバーがWindowsマシン上で実行されている場合にのみ利用可能です。ターゲットマシンでもWindowsが実行されている必要があります。
- Windows XPが動作しているマシンでのリモートインストールはサポートされていません。
- ドメインコントローラでリモートインストールはサポートされていません。ドメインコントローラに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、"Windows でのインストール"（102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**で、**[次のアカウントを使用する]** を選択して、インストール設定がカスタマイズされていることを確認してください。このオプションの詳細については、"サービスログオンアカウントに必要なユーザー権限"（85ページ）を参照してください。

Windowsを実行するコンピュータの追加

リモートのCyber Protect Webコンソールでプロテクションエージェントをインストールするか、またはローカルでセットアッププログラムをダウンロードして実行することで、Windowsマシンを追加できます。

エージェントをリモートでインストールするには

重要
インストールを開始する前に、リモートインストールの前提条件が満たされていることを確認し、配置エージェントとして使用される環境内に少なくとも1つのエージェントが存在することを確認してください。詳細については、"リモートインストールの前提条件"（94ページ）および"配置エージェント"（96ページ）を参照してください。

1. Cyber Protect Web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. （Windowsエージェントをインストールするには）**[Windows]** をクリックします。
4. （他のサポートされるエージェントをインストールするには）保護対象のアプリケーションに対応するボタンをクリックします。
   次のエージェントを使用できます。
   - Hyper-Vエージェント
   - エージェント for SQL + エージェント for Windows

- エージェント for Exchange + エージェント for Windows

  [Microsoft Exchange Server] > **[Exchangeメールボックス]** の順にクリックし、Exchangeエージェントが既に1つ以上登録されている場合は、手順9に進みます。
- エージェント for Active Directory + エージェント for Windows
- エージェント for Office 365

5. 表示されたペインで配置エージェントを実行します。
6. ターゲットマシンのホスト名またはIPアドレス、そのマシンで管理者権限があるアカウントの資格情報を指定します。

   ビルトインの管理者アカウントを使用することをお勧めします。別のアカウントを使用する場合は、そのアカウントをAdministratorsグループに追加し、ターゲットマシンのレジストリを以下の記事に記載されている方法で変更してください: https://support.microsoft.com/en-us/help/951016/description-of-user-account-control-and-remote-restrictions-in-windows。
7. エージェントが管理サーバーへのアクセスに使用するサーバー名またはIPアドレスを選択します。

   デフォルトでは、サーバー名が選択されています。もし管理サーバーに複数のネットワークインターフェースが存在する場合や、エージェントの登録失敗の原因となり得るDNSの問題がある場合は、IPアドレスを選択する必要があります。
8. **[インストール]** をクリックします。
9. （手順4で **[Microsoft Exchange Server]** > **[Exchange メールボックス]** の順にクリックした場合）Microsoft Exchange Serverの**クライアントアクセス**サーバーロール（CAS）が有効になっているマシンを指定します。詳細については、"メールボックスのバックアップ"（447ページ）を参照してください。

エージェントをローカルでダウンロードおよびインストールするには

1. Cyber Protect Webコンソールで、右上隅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。
2. 必要なWindowsインストーラの名前をクリックします。

   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。
3. 保護するマシンで、セットアッププログラムを実行します。詳細については、"Windows でのインストール"（102ページ）を参照してください。

リモートインストールの前提条件

- 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。これを無効化する方法については、"UACを無効にするには"（95ページ）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。これらを無効

化する方法については、"UACのリモート制限を無効にする手順は、次のとおりです"（96ページ）を参照してください。

- [ファイルとプリンタの共有] が、リモートのマシンで [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。
- Acronis Cyber Protect 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**が自動的に開きます。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。

注意
Windows XPが動作しているマシンでのリモートインストールはサポートされていません。

注意
ドメインコントローラでリモートインストールはサポートされていません。ドメインコントローラに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、"Windows でのインストール"（102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**で、**[次のアカウントを使用する]** を選択して、インストール設定がカスタマイズされていることを確認してください。このオプションの詳細については、"サービスログオンアカウントに必要なユーザー権限"（85ページ）を参照してください。

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を無効にするには

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、リモートインストールなどの管理操作の完了後には、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**。

配置エージェント

Cyber Protect Webコンソールからリモート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するには、現在の環境に少なくとも1個のエージェントが既にインストールされている必要があります。このエージェントは、リモートインストール用の配置エージェントとして機能し、管理サーバーとターゲットのリモートのマシンに接続されます。

通常、環境内の最初のプロテクションエージェントは、管理サーバーと同時にインストールされるエージェントになります。ただし、環境内の各Windowsエージェントを配置エージェントとして選択することもできます。

注意
プロテクションエージェントを自動検出して複数のマシンにインストールする場合、配置エージェントは検出エージェントと呼ばれます。

配置エージェントの動作について

1. 配置エージェントは管理サーバーに接続し、`web_installer.exe`ファイルをダウンロードします。

2. 配置エージェントは、指定したリモートのマシンのホスト名またはIPアドレス、および管理者の資格情報を使用してリモートマシンに接続し、その後、web_installer.exeファイルをアップロードします。
3. web_installer.exeファイルは、リモートのマシンにおいて無人モードで実行されます。
4. ウェブインストーラーは必要なインストールのスコープに応じて、管理サーバーのinstallation_filesフォルダ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。

   Installation_filesフォルダは次の場所にあります。

   - Windows: \Program Files\Acronis\RemoteInstallationFiles\
   - Linux: /usr/lib/Acronis/RemoteInstallationFiles/
5. インストールが完了すると、エージェントは管理サーバーに登録されます。

リモート インストールのコンポーネント

リモートインストール用のコンポーネントは、管理サーバーのインストール時にデフォルトでインストールされます。

これらのコンポーネントが配置されるロケーションは、管理サーバーが実行されているマシンのオペレーティングシステムによって異なります。以下の通りです。

- Windows: %Program Files%\Acronis\RemoteInstallationFiles\installation_files
- Linux: /usr/lib/Acronis/RemoteInstallationFiles/installation_files

Acronis Cyber Protectの以前のバージョンからアップグレードした場合や、管理サーバーのインストール時に明示的に**リモートインストールのコンポーネント**を除外した場合、これらのロケーションは有効でない可能性があります。この場合、リモートインストール用のコンポーネントは、既存のAcronis Cyber Protectをアップデート/修正して、手動で追加する必要があります。

既存のインストールファイルにリモートインストール用のコンポーネントを追加するには

1. 最新のAcronis Cyber Protect向けインストールファイルをAcronis Webサイトからダウンロードします。

   利用しているオペレーティングシステムのビット数に対応したインストールファイルを選択してください。ほとんどの場合、**Windows 64ビット**のインストールファイルが必要になります。32ビットマシンにリモートで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る場合、**Windows 32/64ビット**のインストールファイルをダウンロードしてください。
2. 管理サーバーが実行されているマシンでインストールファイルを起動してから、[**アップデート**] を選択します。
3. アップデートが完了したら、再度インストールファイルを起動し、[**現在のインストールの変更**] を選択してください。
4. [**リモートインストールのコンポーネント**] を選択してから、[**完了**] をクリックします。

インストールが完了すると、Cyber Protect Webコンソールからリモート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することができます。

Linuxを実行するコンピュータの追加

Linuxマシンを追加するには、プロテクションエージェントをローカルにインストールする必要があります。リモートインストールはサポートされていません。

Linuxを実行中のマシンを追加するには

1. Cyber Protect Webコンソールで、**[すべてのデバイス]** > **[追加]** の順にクリックします。
2. **[Linux]** 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。
3. 保護するマシンで、セットアッププログラムを実行します。詳細については、"Linux でのインストール"（104ページ）を参照してください。

macOS を実行するマシンの追加

macOSマシンを追加するには、プロテクションエージェントをローカルにインストールする必要があります。リモートインストールはサポートされていません。

macOSを実行中のマシンを追加するには

1. Cyber Protect Webコンソールで、**[すべてのデバイス]** > **[追加]** の順にクリックします。
2. **[Mac]** 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。
3. 保護するマシンで、セットアッププログラムを実行します。詳細については、"macOS でのインストール"（105ページ）を参照してください。

vCenterまたはESXiホストの追加

vCenter またはスタンドアロン ESXi ホストを管理サーバーに追加する方法は 4 つあります。

- エージェント for VMware（仮想アプライアンス）の配置
  ほとんどの場合、この方法をお勧めします。仮想アプライアンスは指定するvCenterによって管理されるすべてのホストに自動的にデプロイされます。ホストを選択し、仮想アプライアンス設定をカスタマイズできます。
- エージェント for VMware（Windows）のインストール
  負荷削減またはLAN フリー バックアップのために、エージェント for VMwareをWindows物理コンピュータにインストールできます。
  - **負荷削減バックアップ**
    本番ESXiホストの負荷がきわめて高く、仮想アプライアンスに適していない場合に使用します。
  - **LAN フリー バックアップ**
    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。詳細な手順については、「LANフリーバックアップ」を参照してください。

管理サーバーが Windows で実行されている場合、エージェントは指定するマシンに自動的にデプロイされます。管理サーバーが Windows 以外で実行されている場合は、エージェントを手動でインストールする必要があります。

- 既にインストールされているエージェント for VMwareの登録
  管理サーバーを再インストールした後に必要な手順です。OVF テンプレートからデプロイされる VMware エージェント（仮想アプライアンス）を登録および設定することもできます。
- 登録済みの VMwareエージェントの設定
  VMware エージェント（Windows）を手動でインストールした後または Acronis Cyber Protect アプライアンスを配置した後に必要な手順です。設定済みの VMware エージェントを別の vCenter Server またはスタンドアロン ESXi ホストに関連付けることもできます。

Webインターフェイスを使用したVMwareエージェント（仮想アプライアンス）のデプロイ

1. **[すべてのデバイス]** > **[追加]**をクリックします。
2. **[VMware ESXi]** をクリックします。
3. **[vCenter の各ホストに仮想アプライアンスとしてデプロイする]** を選択します。
4. vCenter Server またはスタンドアロン ESXi ホストのアドレスおよびアクセス認証を指定します。**管理者**の役割が割り当てられたアカウントを使用することをお勧めします。そうしない場合は、vCenter ServerまたはESXi上で必要な権限を持つアカウントを指定します。
5. エージェントが管理サーバーへのアクセスに使用するサーバー名またはIPアドレスを選択します。
   デフォルトでは、サーバー名が選択されています。もし管理サーバーに複数のネットワークインターフェースが存在する場合や、エージェントの登録失敗の原因となり得るDNSの問題がある場合は、IPアドレスを選択する必要があります。
6. （オプション）**[設定]** をクリックしてデプロイ設定をカスタマイズします。
   - エージェントをデプロイするESXiホスト（vCenter Serverが前の手順で指定された場合にのみ）。
   - 仮想アプライアンス名。
   - アプライアンスがあるデータストア。
   - アプライアンスを含むリソースプールまたはvApp。
   - 仮想アプライアンスのネットワークアダプターが接続されるネットワーク。
   - 仮想アプライアンスのネットワーク設定。DHCP自動構成を選択するか、静的IPアドレスを含む値を手動で指定します。
7. **[デプロイ]** をクリックします。

エージェント for VMware（Windows）のインストール

インストールする前に

「Windows を実行するマシンの追加」セクションの準備手順に従います。

インストール

1. **[すべてのデバイス]** > **[追加]**をクリックします。
2. **[VMware ESXi]** をクリックします。
3. **[Windows を実行するマシンでリモートインストール]** を選択します。
4. デプロイエージェントを選択します。
5. ターゲットマシンのホスト名またはIPアドレス、そのマシンで管理者権限があるアカウントの資格情報を指定します。
6. エージェントが管理サーバーへのアクセスに使用するサーバー名またはIPアドレスを選択します。
   デフォルトでは、サーバー名が選択されています。もし管理サーバーに複数のネットワークインターフェースが存在する場合や、エージェントの登録失敗の原因となり得るDNSの問題がある場合は、IPアドレスを選択する必要があります。
7. **[接続]** をクリックします。
8. vCenter Server またはスタンドアロン ESXi ホストのアドレスおよび資格情報を指定し、**[接続]** をクリックします。**管理者**の役割が割り当てられたアカウントを使用することをお勧めします。そうしない場合は、vCenter ServerまたはESXi上で必要な権限を持つアカウントを指定します。
9. **[インストール]** をクリックして、エージェントをインストールします。

既にインストールされているエージェント for VMwareの登録

このセクションでは、Webインターフェイスを使用して、VMwareエージェントの登録について説明します。

別の登録方法:

- VMwareエージェント（仮想アプライアンス）を登録するには、仮想アプライアンスUIでManagement Serverを指定します。「OVFテンプレートからVMwareエージェント（仮想アプライアンス）のデプロイ」セクションの「仮想アプライアンスの構成」の下の手順3を参照してください。
- VMware エージェント（Windows）はローカルインストール中に登録されます。

VMwareエージェントを登録するには

1. **[すべてのデバイス]** > **[追加]**をクリックします。
2. **[VMware ESXi]** をクリックします。
3. **[既にインストールされているエージェントを登録する]** を選択します。
4. デプロイエージェントを選択します。
5. VMware エージェント（Windows）を登録する場合は、エージェントがインストールされているマシンのホスト名または IP アドレス、およびそのマシンで管理者権限があるアカウントの資格情報を指定します。
   VMwareエージェント（仮想アプライアンス）を登録する場合は、仮想アプライアンスのホスト名または IP アドレス、およびアプライアンスが実行されている vCenter Server またはスタンドアロン ESXi ホストの資格情報を指定します。

6. エージェントが管理サーバーへのアクセスに使用するサーバー名またはIPアドレスを選択します。
   デフォルトでは、サーバー名が選択されています。もし管理サーバーに複数のネットワークインターフェースが存在する場合や、エージェントの登録失敗の原因となり得るDNSの問題がある場合は、IPアドレスを選択する必要があります。
7. **[接続]** をクリックします。
8. vCenter ServerまたはESXiホストのホスト名とIPアドレス、およびアクセスするための資格情報を指定し、**[接続]** をクリックします。**管理者**の役割が割り当てられたアカウントを使用することをお勧めします。そうしない場合は、vCenter ServerまたはESXi上で必要な権限を持つアカウントを指定します。
9. **[登録]** をクリックして、エージェントを登録します。

登録済みの VMwareエージェントの設定

このセクションでは、Web インターフェースで vCenter Server または ESXi を使用して VMware エージェントを関連付ける方法について説明します。別の方法として、VMware エージェント（仮想アプライアンス）コンソールでこの操作を行うこともできます。

この手順を使用して、VMware エージェントと vCenter Server または ESXi との既存の関連付けを変更することもできます。別の方法として、**[設定]** > **[エージェント]** > 目的のエージェント > **[詳細]** > **[vCenter/ESXi]** をクリックして VMware エージェント（仮想アプライアンス）コンソールでこの操作を行うこともできます。

VMwareエージェントを設定する手順

1. **[すべてのデバイス]** > **[追加]**をクリックします。
2. **[VMware ESXi]** をクリックします。
3. このソフトウェアでは、未設定の VMware エージェントが最初にアルファベット順で表示されます。
   管理サーバーに登録されているすべてのエージェントが設定済みの場合、**[登録済みのエージェントを設定]** をクリックすると、エージェントが最初にアルファベット順で表示されます。
4. 必要に応じて、**[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、設定するエージェントを選択します。
5. vCenter Server または ESXi ホストのホスト名または IP アドレスと、アクセスするための資格情報を指定または変更します。**管理者**の役割が割り当てられたアカウントを使用することをお勧めします。そうしない場合は、vCenter ServerまたはESXi上で必要な権限を持つアカウントを指定します。
6. **[設定]** をクリックして変更を保存します。

Scale Computing HC3 クラスターの追加

Scale Computing HC3 クラスターを Cyber Protect 管理サーバーに追加する

1. クラスターに Scale Computing HC3 エージェント（仮想アプライアンス）をデプロイします。
2. このクラスターと 管理サーバーの両方への接続を構成します。

エージェントをローカルでインストールする

Windows でのインストール

エージェント for Windows、エージェント for Hyper-V、エージェント for Exchange、エージェント for SQL、およびエージェント for Active Directoryのインストール手順

1. 管理者としてログオンし、Acronis Cyber Protect プログラムの設定を起動します。
2. （オプション）プログラムの設定の言語を変更するには、**[言語の設定]** をクリックします。
3. ライセンス契約とプライバシーステートメントに同意して、**[次へ]** をクリックします。
4. **[プロテクション エージェントのインストール]**を選択します。
5. 次の手順のいずれかを実行します。
   - **[インストール]** をクリックします。
     これは、製品をインストールする最も簡単な方法です。インストール パラメータの多くは、デフォルト値に設定されます。
     次のコンポーネントがインストールされます。
     - エージェント for Windows
     - 該当するハイパーバイザまたはアプリケーションがコンピュータで検出される場合は、その他のエージェント（エージェント for Hyper-V、エージェント for Exchange、エージェント for SQL、エージェント for Active Directory）
     - ブータブルメディアビルダー
     - コマンドラインツール
     - Cyber Protectモニタ
   - **[インストール設定のカスタマイズ]** をクリックしてセットアップを構成します。
     インストールするコンポーネントを選択したり、その他のパラメータを指定したりできます。詳細については、"インストール設定のカスタマイズ"（83ページ）を参照してください。
   - **[無人インストールの .mst および .msi を作成]** をクリックして、インストールパッケージを抽出します。.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、**[生成]** をクリックします。ここでは、その他の手順は不要です。
     グループポリシーを使用してエージェントを配置する場合は、"グループポリシーによるエージェントの配置"（174ページ）に記載されている手順に従います。
6. エージェントがインストールされているマシンを登録する管理サーバーを指定します。
   a. Management Serverがインストールされているコンピュータのホスト名または IPアドレスを指定します。
   b. 管理サーバーの管理者の資格情報または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、"手順1:登録トークンの生成"（175ページ）を参照してください。
   c. **[完了]** をクリックします。
7. 指定するよう求められたら、エージェントがインストールされているマシンを、組織に追加するか部署の 1 つに追加するかを選択します。

このプロンプトは、複数の部署を管理する場合、または最低1つの部署がある組織を管理する場合に表示されます。それ以外の場合は、通知されることなく、マシンは管理対象の部署または組織に追加されます。詳細については、"部署および管理アカウント"（631ページ）を参照してください。

8. インストールを続けます。
9. インストールが完了した後、［**閉じる**］をクリックします。
10. Exchangeエージェントをインストールした場合は、Exchangeデータベースをバックアップできるようになります。Exchange メールボックスをバックアップする場合は、Cyber Protect ウェブ コンソールを開き、**[追加]** > **[Microsoft Exchange Server]** > **[Exchange メールボックス]** をクリックし、Microsoft Exchange Server の**クライアントアクセス**サーバーの役割（CAS）が有効になっているマシンを指定します。詳細については、"メールボックスのバックアップ"（447ページ）を参照してください。

VMwareエージェント（Windows）、Office 365エージェント、Oracleエージェント、または Exchangeエージェントを、Microsoft Exchange Server を使用しないマシンにインストールするには

1. 管理者としてログオンし、Acronis Cyber Protect プログラムの設定を起動します。
2. （オプション）プログラムの設定の言語を変更するには、**[言語の設定]** をクリックします。
3. ライセンス契約とプライバシーステートメントに同意して、**[次へ]** をクリックします。
4. **[プロテクション エージェントのインストール]** を選択し、**[インストール設定のカスタマイズ]** をクリックします。
5. **[インストールする項目]** の横にある **[変更]** をクリックします。
6. 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。インストールしないコンポーネントのチェックボックスの選択を解除します。［**完了**］をクリックして先に進んでください。
7. エージェントがインストールされているマシンを登録する管理サーバーを指定します。
   a. **[Acronis Cyber Protect Management Server]** の横で **[指定]** をクリックします。
   b. Management Serverがインストールされているコンピュータのホスト名または IPアドレスを指定します。
   c. 管理サーバーの管理者の資格情報または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、"手順1:登録トークンの生成"（175ページ）を参照してください。
   d. **[完了]** をクリックします。
8. 指定するよう求められたら、エージェントがインストールされているマシンを、組織に追加するか部署の 1 つに追加するかを選択します。
   このプロンプトは、複数の部署を管理する場合、または最低1つの部署がある組織を管理する場合に表示されます。それ以外の場合は、通知されることなく、マシンは管理対象の部署または組織に追加されます。詳細については、"部署および管理アカウント"（631ページ）を参照してください。
9. （オプション）"インストール設定のカスタマイズ"（83ページ）の説明に従って他のインストール設定を変更します。
10. **[インストール]** をクリックして、インストールを続行します。
11. インストールが完了した後、［**閉じる**］をクリックします。

12. （VMwareエージェント（Windows）をインストールする場合のみ）"登録済みの VMwareエージェントの設定"（101ページ）で説明されている手順を実行します。
13. （Exchange エージェントをインストールする場合のみ）Cyber Protect ウェブ コンソールを開き、**[追加]** > **[Microsoft Exchange Server]** > **[Exchange メールボックス]** をクリックし、Microsoft Exchange Server の**クライアントアクセス**サーバーの役割（CAS）が有効になっているマシンを指定します。詳細については、"メールボックスのバックアップ"（447ページ）を参照してください。

Linux でのインストール

インストールする前に

1. 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。
2. 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 Web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。

エージェント for Linuxをインストールする

1. ルートユーザーとして、インストールファイル（.i686または.x86_64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>
   ```

2. 使用許諾契約の内容に同意します。
3. インストールするコンポーネントを指定します。
   a. **[Acronis Cyber Protect Management Server]** チェックボックスをクリアします。
   b. 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。
      - **エージェント for Linux**
      - **Oracle エージェント**

      Oracle 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。
   c. **[次へ]** をクリックします。
4. エージェントがインストールされているマシンを登録する管理サーバーを指定します。
   a. Management Serverがインストールされているコンピュータのホスト名または IPアドレスを指定します。

b. 管理サーバーの管理者のユーザー名とパスワードを指定します。

c. **[次へ]** をクリックします。

5. 指定するよう求められたら、エージェントがインストールされているマシンを、組織に追加するか部署の 1 つに追加するかを選択して **Enter** キーを押します。

   このプロンプトは、前の手順で指定したアカウントが、複数の部署を管理する場合、または部署が 1 つ以上ある組織を管理する場合に表示されます。

6. 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。

7. 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 でのインストール

Macエージェントをインストールする

1. インストールファイル（.dmg）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ションシステムにマウントされるのを待ちます。
3. **[インストール]** をダブルクリックし、**[続行]** をクリックします。
4. （オプション）**[インストールロケーションの変更]** をクリックしてソフトウェアをインストールするディスクを変更します。デフォルトでは、システム起動時のディスクが選択されます。
5. **[インストール]** をクリックします。入力を求められたら、管理者のユーザー名とパスワードを入力します。
6. エージェントがインストールされているマシンが登録される管理サーバーを指定します。
   a. Management Serverがインストールされているコンピュータのホスト名または IPアドレスを指定します。
   b. 管理サーバーの管理者のユーザー名とパスワードを指定します。
   c. **[登録]** をクリックします。
7. 指定するよう求められたら、エージェントがインストールされているマシンを、組織に追加するか部署の 1 つに追加するかを選択して **[完了]** をクリックします。

このプロンプトは、前の手順で指定したアカウントが、複数の部署を管理する場合、または部署が 1 つ以上ある組織を管理する場合に表示されます。

8. インストールが完了した後、［**閉じる**］をクリックします。

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

このセクションでは、Windowsを実行しているマシンで、Windows Installer（`msiexec`プログラム）によってAcronis Cyber Protectのインストールとアンインストールを無人モードで実行する方法を説明します。Active Directoryドメインでは、グループポリシーを使用して無人インストールを行う方法があります。これについては、"グループポリシーによるエージェントの配置"（174ページ）を参照してください。

インストール中に、**トランスフォーム**と呼ばれるファイル（.mst ファイル）を使用できます。トランスフォームは、インストールパラメータが指定されたファイルです。別の方法として、コマンドラインで直接インストールパラメータを指定することができます。

.mst トランスフォームファイルの作成とインストールパッケージの抽出

1. Windowsに管理者権限でログオンし、プログラムの設定を開始します。
2. **[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。
3. （一部のセットアッププログラムでは利用不可）**コンポーネントのビット数**には、**32ビット**または**64ビット**を選択します。
4. **[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、セットアッププログラムから取り出します。
5. **Acronis Cyber Protect管理サーバー** 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、"手順1:登録トークンの生成"（175ページ）を参照してください。
6. （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。
7. .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。

8. .mstトランスフォームファイルを生成して.msiと.cabのインストールパッケージを抽出する、フォルダを選択します。それから **[生成]** をクリックします。

これにより、.mst トランスフォームファイルが生成され、.mst および .cab インストールパッケージが、指定したフォルダに抽出されます。

.mst トランスフォームを使用した製品のインストール

コマンドラインで以下のコマンドを実行します。

```
msiexec /i <package name> TRANSFORMS=<transform name>
```

ここで、

- **<パッケージ名>** は、.msi ファイルの名前です。この名前は、オペレーティングシステムのビット数に応じて **AB.msi** または **AB64.msi** となります。
- **<変換名>** は、トランスフォームの名前です。この名前は、オペレーティングシステムのビット数に応じて **AB.msi.mst** または **AB64.msi.mst** となります。

たとえば、`msiexec /i AB64.msi TRANSFORMS=AB64.msi.mst`のように指定します。

手動でのパラメータ指定による製品のインストールやインストール解除

コマンドラインで以下のコマンドを実行します。

```
msiexec /i <package name><PARAMETER 1>=<value 1> ... <PARAMETER N>=<value n>
```

ここでは、**<パッケージ名>** は、.msi ファイルの名前です。この名前は、オペレーティングシステムのビット数に応じて **AB.msi** または **AB64.msi** となります。

有効なパラメータと値の説明については、"共通パラメータ"（108ページ）を参照してください。

例

- 管理サーバーとリモートインストールのコンポーネントのインストール。

  ```
  msiexec.exe /i ab64.msi /l*v my_log.txt /qn
  ADDLOCAL=AcronisCentralizedManagementServer,WebConsole,ComponentRegisterFeature
  TARGETDIR="C:\Program Files\Acronis" REBOOT=ReallySuppress CURRENT_LANGUAGE=en ACEP_
  AGREEMENT=1 AMS_USE_SYSTEM_ACCOUNT=1
  ```

- 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。以前インストールした管理サーバー上のエージェントへのマシンの登録。

  ```
  msiexec.exe /i ab64.msi /l*v my_log.txt /qn
  ADDLOCAL=AgentsCoreComponents,BackupAndRecoveryAgent,CommandLineTool,TrayMonitor
  TARGETDIR="C:\Program Files\Acronis" REBOOT=ReallySuppress CURRENT_LANGUAGE=en ACEP_
  AGREEMENT=1 MMS_CREATE_NEW_ACCOUNT=1 REGISTRATION_ADDRESS=10.10.1.1
  ```

- 管理サーバー、Storage Node、カタログサービス、プロテクションエージェントをアップデートします。

```
msiexec.exe /i ab64.msi /l*v my_log.txt /qn
ADDLOCAL=AcronisCentralizedManagementServer,BackupAndRecoveryAgent,AgentsCoreComponen
ts,StorageServer,CatalogBrowser CATALOG_DATA_MIGRATION_PATH="C:\MyFolder\tmp"
```

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、Windows での無人インストールまたはインストール解除中に使用されるパラメータについて説明します。

これらのパラメータに加え、https://msdn.microsoft.com/en-us/library/windows/desktop/aa367988(v=vs.85).aspxに記載されている`msiexec`のパラメータを使用できます。

インストールパラメータ

共通パラメータ

`ADDLOCAL=<list of components>`

インストールするコンポーネントは、スペース文字なしのカンマ区切りで指定します。インストールの前に、指定したすべてのコンポーネントをセットアッププログラムから取り出す必要があります。

コンポーネントの完全なリストは、次のとおりです。

コンポーネント	一緒にインストールする必要があるもの	ビット数	コンポーネント名/説明
AcronisCentralizedManagementServer	WebConsole	32ビット/64ビット	管理サーバー
WebConsole	AcronisCentralizedManagementServer	32ビット/64ビット	Webコンソール
ComponentRegisterFeature	AcronisCentralizedManagementServer	32ビット/64ビット	リモート インストールのコンポーネント
AtpScanService	AcronisCentralizedManagementServer	32ビット/64	スキャンサービス

		ビット	
AgentsCoreComponents		32ビット/64ビット	エージェントのコアコンポーネント
BackupAndRecoveryAgent	AgentsCoreComponents	32ビット/64ビット	エージェント for Windows
ArxAgentFeature	BackupAndRecoveryAgent	32ビット/64ビット	Exchange エージェント
ArsAgentFeature	BackupAndRecoveryAgent	32ビット/64ビット	エージェント for SQL
ARADAgentFeature	BackupAndRecoveryAgent	32ビット/64ビット	エージェント for Active Directory
OracleAgentFeature	BackupAndRecoveryAgent	32ビット/64ビット	Oracle エージェント
ArxOnlineAgentFeature	AgentsCoreComponents	32ビット/64ビット	エージェント for Office 365
AcronisESXSupport	AgentsCoreComponents	32ビット/64	エージェント for VMware（Windows）

		ビット	
HyperVAgent	AgentsCoreComponents	32ビット/64ビット	エージェント for Hyper-V
ESXVirtualAppliance		32ビット/64ビット	エージェント for VMware（仮想アプライアンス）
ScaleVirtualAppliance		32ビット/64ビット	Scale Computing HC3エージェント（仮想アプライアンス）
CommandLineTool		32ビット/64ビット	コマンドラインツール
TrayMonitor	BackupAndRecoveryAgent	32ビット/64ビット	Cyber Protect モニタ
BackupAndRecoveryBootableComponents		32ビット/64ビット	ブータブルメディアビルダー
PXEServer		32ビット/64ビット	PXE Server
StorageServer	BackupAndRecoveryAgent	64ビッ	ストレージノード

		ト	
CatalogBrowser	JRE 8 Update 111 以降	64 ビット	カタログ サービス

TARGETDIR=<path>

製品のインストール先フォルダ。

REBOOT=ReallySuppress

このパラメータが指定されていると、マシンの再起動が禁止されます。

CURRENT_LANGUAGE=<language ID>

製品の言語。使用できる値: en、en_GB、cs、da、de、es_ES、fr、ko、it、hu、nl、ja、pl、pt、pt_BR、ru、tr、zh、zh_TW。

ACEP_AGREEMENT={0,1}

値が1の場合、マシンはAcronisカスタマーエクスペリエンスプログラム（ACEP）に参加します。

REGISTRATION_ADDRESS=<host name or IP address>:<port>

管理サーバーがインストールされるマシンのホスト名または IP アドレス。ADDLOCALパラメーターで指定されるエージェント、Storage Node、カタログサービスが、この管理サーバーに登録されます。デフォルト値（9877）と異なる場合、ポート番号が必須です。

このパラメータでは、REGISTRATION_TOKENパラメータ、またはREGISTRATION_LOGINとREGISTRATION_PASSWORDパラメータを指定する必要があります。

REGISTRATION_TOKEN=<token>

「グループポリシーによるエージェントの配置」に記載されている、Cyber Protect ウェブコンソールに生成された登録トークンです。

REGISTRATION_LOGIN=<user name>, REGISTRATION_PASSWORD=<password>

管理サーバーの管理者のユーザー名とパスワード。

REGISTRATION_TENANT=<unit ID>

組織内の部署。ADDLOCALパラメーターで指定されるエージェント、Storage Node、カタログサービスが、この部署に追加されます。

部署IDを確認するには、Cyber Protectのウェブコンソールで、**[設定]** > **[アカウント]** をクリックし、部署を選択して **[詳細]** をクリックします。

このパラメーターはREGISTRATION_TOKEN、またはREGISTRATION_LOGINとREGISTRATION_PASSWORDがないと機能しません。この場合、コンポーネントは組織に追加されます。

このパラメータを指定しない場合は、コンポーネントは組織に追加されます。

`REGISTRATION_REQUIRED={0,1}`

登録失敗時のインストール結果。値が1の場合、インストールは失敗します。値が0である場合、コンポーネントは未登録ですがインストールは無事に完了します。

`REGISTRATION_CA_SYSTEM={0,1}|REGISTRATION_CA_BUNDLE={0,1}|REGISTRATION_PINNED_PUBLIC_KEY=<public key value>`

これらの相互排他的なパラメーターは、登録中の管理サーバー証明書のチェック方法を定義します。MITM攻撃を防ぐために管理サーバーの信頼性をベリファイしたい場合、証明書をチェックします。

値が1である場合、システムCA、または製品と共に配布されたCAバンドルがベリファイに適宜使用されます。ピン公開鍵が指定されている場合、このキーがベリファイに使用されます。値が0である場合、またはパラメーターを指定しない場合、証明書のベリファイは実行されず、登録トラフィックは暗号化されたままになります。

`/l*v <log file>`

このパラメータを指定すると、verbose モードのインストールログが、指定したファイルに保存されます。このログファイルはインストールに関する問題の分析に使用できます。

管理サーバーインストールパラメータ

`WEB_SERVER_PORT=<port number>`

Web ブラウザが管理サーバーにアクセスするために使用するポート。デフォルトでは 9877。

`AMS_ZMQ_PORT=<port number>`

製品コンポーネント間の通信に使用するポート。デフォルトでは 7780。

`SQL_INSTANCE=<instance>`

Management Serverによって使用されるデータベース。Microsoft SQL Server 2012、Microsoft SQL Server 2014、またはMicrosoft SQL Server 2016のどのエディションでも選択できます。選択したインスタンスは、他のプログラムでも使用できます。

このパラメータを指定しない場合は、ビルトインの SQLite データベースが使用されます。

`SQL_USER_NAME=<user name>` および `SQL_PASSWORD=<password>`

Microsoft SQL Server ログインアカウントの資格情報。これらの資格情報が管理サーバーによって、選択された SQL サーバーインスタンスへの接続に使用されます。これらのパラメータを指定していない場合、管理サーバーで、管理サーバーのサービスアカウント（**AMS ユーザー**）の資格情報が使用されます。

管理サーバーのサービスを実行するアカウント

次のいずれかのパラメータを指定します。

- `AMS_USE_SYSTEM_ACCOUNT={0,1}`
  値が1の場合はシステムアカウントが使用されます。

- AMS_CREATE_NEW_ACCOUNT={0,1}
  値が1の場合は新しいアカウントが作成されます。
- AMS_SERVICE_USERNAME=<user name> および AMS_SERVICE_PASSWORD=<password>
  指定したアカウントが使用されます。

エージェントインストールパラメータ

HTTP_PROXY_ADDRESS=<IP address> および HTTP_PROXY_PORT=<port>

エージェントが使用するHTTPプロキシサーバー。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=<login> および HTTP_PROXY_PASSWORD=<password>

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。

HTTP_PROXY_ONLINE_BACKUP={0,1}

値が0の場合、またはパラメータが指定されていない場合、エージェントはクラウドからのバックアップと復元にのみプロキシサーバーを使用します。値が1である場合、エージェントはさらにプロキシサーバー経由で管理サーバーに接続します。

SET_ESX_SERVER={0,1}

値が0の場合、インストールされるVMwareエージェントは、vCenter ServerやESXiホストに接続されません。インストール後、「登録済みの VMware エージェントの設定」に記載されている手順に従います。

値が1の場合、次のパラメータを指定します。

ESX_HOST=<host name or IP address>

vCenter Server または ESXi ホストのホスト名または IP アドレス。

ESX_USER=<user name> および ESX_PASSWORD=<password>

vCenter Server または ESXi ホストにアクセスするための資格情報。

エージェントサービスを実行するアカウント

次のいずれかのパラメータを指定します。

- MMS_USE_SYSTEM_ACCOUNT={0,1}
  値が1の場合はシステムアカウントが使用されます。
- MMS_CREATE_NEW_ACCOUNT={0,1}
  値が1の場合は新しいアカウントが作成されます。
- MMS_SERVICE_USERNAME=<user name> および MMS_SERVICE_PASSWORD=<password>
  指定したアカウントが使用されます。

Storage Node インストールパラメータ

Storage Node サービスを実行するアカウント

次のいずれかのパラメータを指定します。

- `ASN_USE_SYSTEM_ACCOUNT={0,1}`
  値が1の場合はシステムアカウントが使用されます。
- `ASN_CREATE_NEW_ACCOUNT={0,1}`
  値が1の場合は新しいアカウントが作成されます。
- `ASN_SERVICE_USERNAME=<user name>` および `ASN_SERVICE_PASSWORD=<password>`
  指定したアカウントが使用されます。

カタログサービスのインストールパラメータ

`CATALOG_DATA_MIGRATION_PATH=<path>`

このパラメータを使用して、カタログデータをAcronis Cyber Protect 15 Update 4の新しいバージョンのカタログサービスにマイグレーションできます。カタログデータをエクスポートする一時フォルダのパスを指定します。

`SKIP_CATALOG_DATA_MIGRATION=1`

カタログデータのマイグレーションをスキップする場合は、このパラメータを使用します。

パラメータ`SKIP_CATALOG_DATA_MIGRATION`と`CATALOG_DATA_MIGRATION_PATH`は、いずれか一方のみ使用可能です。

インストール解除パラメータ

`REMOVE={<list of components>|ALL}`

削除するコンポーネントは、スペース文字なしのカンマ区切りで指定します。

使用できるコンポーネントは、このセクションの前の方に記載されています。

値が`ALL`の場合、すべての製品コンポーネントがアンインストールされます。また、次のパラメータを指定できます。

`DELETE_ALL_SETTINGS={0, 1}`

値が1の場合、製品のログ、タスク、構成の設定が削除されます。

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Acronis Cyber Protect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。

製品をインストールまたはインストール解除する手順

1. ターミナルを開きます。
2. 次のコマンドを実行します。

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

   ここで、**<パッケージ名>** 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）。
3. （Linuxエージェントがインストールされている場合のみ）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。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、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。

インストールパラメータ

共通パラメータ

`{-i |--id=}<list of components>`

インストールするコンポーネントは、スペース文字なしのカンマ区切りで指定します。

以下のコンポーネントをインストールに利用できます。

コンポーネント	コンポーネントの説明
AcronisCentralizedManagementServer	管理サーバー
BackupAndRecoveryAgent	エージェント for Linux
BackupAndRecoveryBootableComponents	ブータブルメディアビルダー

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。

`--language=<language ID>`

製品の言語。使用できる値: en、en_GB、cs、da、de、es_ES、fr、ko、it、hu、nl、ja、pl、pt、pt_BR、ru、tr、zh、zh_TW。

`{-d|--debug}`

このパラメータを指定すると、verbose モードでインストールログが記述されます。このログは、ファイル **/var/log/trueimage-setup.log** 内にあります。

`{-t|--strict}`

このパラメータを指定すると、インストール中に警告が発生した場合に、すべてインストールエラーとなります。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}`

このパラメータを指定すると、インストール中に必要な Linux パッケージがなくても無視されます。

管理サーバーインストールパラメータ

`{-W |--web-server-port=}<port number>`

Web ブラウザが管理サーバーにアクセスするために使用するポート。デフォルトでは 9877。

`--ams-tcp-port=<port number>`

製品コンポーネント間の通信に使用するポート。デフォルトでは 7780。

エージェントインストールパラメータ

次のいずれかのパラメータを指定します。

- `--skip-registration`
  - 管理サーバーにエージェントを登録しません。
- `{-C |--ams=}<host name or IP address>`
  - 管理サーバーがインストールされるマシンのホスト名または IP アドレス。エージェントはこの管理サーバーに登録されます。

エージェントと管理サーバーを1つのコマンドでインストールすると、`-C`パラメーターに関係なく、エージェントはこの管理サーバーに登録されます。

このパラメータでは、`token`パラメータ、または`login`と`password`パラメータを指定する必要があります。

`--token=<token>`

「グループポリシーによるエージェントの配置」に記載されている、Cyber Protectウェブコンソールに生成された登録トークンです。

`{-g |--login=}<user name>` および `{-w |--password=}<password>`

管理サーバーの管理者の資格情報。

`--unit=<unit ID>`

組織内の部署。エージェントはこの部署に追加されます。

部署IDを確認するには、Cyber Protectのウェブコンソールで、**[設定]** > **[アカウント]** をクリックし、部署を選択して **[詳細]** をクリックします。

このパラメータを指定しない場合、エージェントは組織に追加されます。

`--reg-transport={https|https-ca-system|https-ca-bundle|https-pinned-public-key}`

登録中の管理サーバー証明書のチェック方法。MITM攻撃を防ぐために管理サーバーの信頼性をベリファイしたい場合、証明書をチェックします。

値がhttpsである場合、またはパラメーターを指定しない場合、証明書のチェックは実行されず、登録トラフィックは暗号化されたままになります。値がhttpsではない場合、システムCA、または製品と共に配布されたCAバンドルまたはピン公開鍵がチェックに適宜使用されます。

`--reg-transport-pinned-public-key=<public key value>`

ピン公開鍵の値。このパラメーターは`--reg-transport=https-pinned-public-key`パラメーターと共に、またはその代わりに指定します。

- `--http-proxy-host=<IP address>` および `--http-proxy-port=<port>`
  - 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=<login>` および `--http-proxy-password=<password>`
  - 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。
- `--no-proxy-to-ams`
  - プロテクションエージェントは、`--http-proxy-host`および`--http-proxy-port`パラメーターで指定されたプロキシサーバーを使用せずに管理サーバーに接続します。

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`

製品のログ、タスク、構成の設定を削除します。

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。

例

- Management Server のインストール。

```
./AcronisCyberProtect_15_64-bit.x86_64 -a -i AcronisCentralizedManagementServer
```

- 管理サーバーのインストール、カスタムポートの指定。

```
./AcronisCyberProtect_15_64-bit.x86_64 -a -i AcronisCentralizedManagementServer --
web-server-port 6543 --ams-tcp-port 8123
```

- Linuxエージェントのインストールと指定した管理サーバーへの登録。

```
./AcronisCyberProtect_15_64-bit.x86_64 -a -i BackupAndRecoveryAgent --ams 10.10.1.1 -
-login root --password 123456
```

- 指定した部署における、Linuxエージェントのインストールと指定した管理サーバーへの登録。

```
./AcronisCyberProtect_15_64-bit.x86_64 -a -i BackupAndRecoveryAgent --ams 10.10.1.1 -
-login root --password 123456 -unit 01234567-89AB-CDEF-0123-456789ABCDEF
```

macOS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、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。インストールファイル（.dmg）をダウンロードする方法の詳細については、「macOSを実行しているマシンの追加」を参照してください。

Macエージェントをインストールする

1. 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>
   ```

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

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

   <dmg_file> はインストールファイルの名前です。たとえば、**AcronisCyberProtect_15_MAC.dmg** と指定します。
3. インストーラを実行します。

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

4. 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/AcronisCyberProtect_15_MAC.dmg -mountpoint mydirectory
  ```

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

  ```
  hdiutil detach mydirectory
  ```

Macエージェントを登録するには

次のいずれかを実行します。

- 特定の管理者アカウントでエージェントを登録します。

  ```
  sudo /Library/Application\
  Support/BackupClient/Acronis/RegisterAgentTool/RegisterAgent -o register -a
  <management server address:port> -u <user name> -p <password>
  ```

  <管理サーバーアドレス:ポート>は、AcronisCyber Protect管理サーバーがインストールされるマシンのホスト名またはIPアドレスです。デフォルト値（9877）と異なる場合、ポート番号が必須です。

  <ユーザー名>および**<パスワード>**は、エージェントが登録される管理者アカウントの資格情報です。
- 特定の部署でエージェントを登録します。

  ```
  sudo /Library/Application\
  Support/BackupClient/Acronis/RegisterAgentTool/RegisterAgent  -o register -a
  <management server address:port> -u <user name> -p <password> --tenant <unit ID>
  ```

  部署IDを確認するには、Cyber Protectのウェブコンソールで、**[設定]** > **[アカウント]** をクリックし、目的の部署を選択して **[詳細]** をクリックします。

  重要
  管理者は、組織レベルの階層でのみ、部署IDを指定してエージェントを登録できます。部署管理者は、自身の部署とその配下の部署でマシンを登録できます。組織管理者は、すべての部署でマシンを登録できます。それぞれの管理者アカウントの詳細については、「ユーザーアカウントと組織部署の管理」を参照してください。
- 登録トークンを使用してエージェントを登録します。

  ```
  sudo /Library/Application\
  Support/BackupClient/Acronis/RegisterAgentTool/RegisterAgent -o register -a
  <management server address:port> --token <token>
  ```
  ```

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ウェブ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）。

重要
macOS 10.14以降では、プロテクションエージェントにフルディスクアクセスを付与する必要があります。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。

例

ユーザー名とパスワードで登録します。

- ```
  sudo /Library/Application\
  Support/BackupClient/Acronis/RegisterAgentTool/RegisterAgent -o register -a
  https://10.250.144.179:9877 -u johndoe -p johnspassword
  ```

部署IDと管理者の資格情報で登録します。

- ```
  sudo /Library/Application\
  Support/BackupClient/Acronis/RegisterAgentTool/RegisterAgent -o register -a
  https://10.250.144.179:9877 -u johndoe -p johnspassword --tenant 4dd941c1-c03f-11ea-
  86d8-005056bdd3a0
  ```

トークンで登録します。

- ```
  sudo /Library/Application\
  Support/BackupClient/Acronis/RegisterAgentTool/RegisterAgent -o register -a
  https://10.250.144.179:9877 --token D91D-DC46-4F0B
  ```

Macエージェントをインストール解除する

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
  ```

Macエージェントをインストール解除して、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
  ```

マシンの手動登録

エージェントのインストール時にCyber Protect管理サーバーにマシンを登録できますが、それ以外に、コマンドラインインターフェースを使用して登録することも可能です。エージェントのインストール時
  ```

に自動登録が失敗した場合や、既存のマシンを新しいアカウントで登録する場合などに、この操作が必要になります。

マシンを登録するには

エージェントがインストールされているマシンのコマンドプロンプトで、次のコマンドのいずれかを実行します。

- 特定の管理者アカウントでマシンを登録します。

  ```
  <path to the registration tool> -o register -a <management server address:port> -u
  <user name> -p <password>
  ```

  <登録ツールへのパス>:
  - Windowsの場合: `%ProgramFiles%\Acronis\RegisterAgentTool\register_agent.exe`
  - Linuxの場合: `/usr/lib/Acronis/RegisterAgentTool/RegisterAgent`
  - macOSの場合: `/Library/Application Support/BackupClient/Acronis/RegisterAgentTool/RegisterAgent`

  <管理サーバーアドレス:ポート>は、AcronisCyber Protect管理サーバーがインストールされるマシンのホスト名またはIPアドレスです。デフォルトのポート9877を使用する場合、明示的に指定する必要はありません。

  <ユーザー名>および**<パスワード>**は、エージェントが登録される管理者アカウントの資格情報です。
- 特定の部署でマシンを登録するには、部署IDを指定します。

  ```
  <path to the registration tool> -o register -a <management server address:port> u
  <user name> -p <password> --tenant <unit ID>
  ```

  部署IDを確認するには、Cyber Protectのウェブコンソールで、**[設定]** > **[アカウント]** をクリックし、目的の部署を選択して **[詳細]** をクリックします。

  重要
  管理者は、組織レベルの階層で、エージェントの登録のみを行えます。部署管理者は、自身の部署とその配下の部署でエージェントを登録できます。組織管理者は、すべての部署でエージェントを登録できます。それぞれの管理者アカウントの詳細については、「ユーザーアカウントと組織部署の管理」を参照してください。
- 登録トークンを使用してマシンを登録します。

  ```
  <path to the registration tool> -o register -a <management server address:port> --
  token <token>
  ```

  - 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、「グループポリシーによるエージェントの配置」を参照してください。

マシンを登録解除するには

エージェントがインストールされているマシンのコマンドプロンプトで、次のコマンドを実行します。

```
<path to the registration tool> -o unregister
```

例

Windows

```
"%ProgramFiles%\Acronis\RegisterAgentTool\register_agent.exe" -o register -a
https://10.250.144.179:9877 -u johndoe -p johnspassword
```

```
"%ProgramFiles%\Acronis\RegisterAgentTool\register_agent.exe" -o register -a
https://10.250.144.179:9877 --tenant 590b1dd7-8adb-11ea-bf44-0050569deecf
```

```
"%ProgramFiles%\Acronis\RegisterAgentTool\register_agent.exe" -o register -a
https://10.250.144.179:9877 -u johndoe -p johnspassword --tenant 590b1dd7-8adb-11ea-
bf44-0050569deecf
```

```
"%ProgramFiles%\Acronis\RegisterAgentTool\register_agent.exe" -o register -a
https://10.250.144.179:9877 --token 3B4C-E967-4FBD
```

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

Linux

```
sudo "/usr/lib/Acronis/RegisterAgentTool/RegisterAgent" -o register -a
https://10.250.144.179:9877 -u johndoe -p johnspassword
```

```
sudo "/usr/lib/Acronis/RegisterAgentTool/RegisterAgent" -o register -a
https://10.250.144.179:9877 --tenant 590b1dd7-8adb-11ea-bf44-0050569deecf
```

```
sudo "/usr/lib/Acronis/RegisterAgentTool/RegisterAgent" -o register -a
https://10.250.144.179:9877 -u johndoe -p johnspassword --tenant 590b1dd7-8adb-11ea-
bf44-0050569deecf
```

```
sudo "/usr/lib/Acronis/RegisterAgentTool/RegisterAgent" -o register -a
https://10.250.144.179:9877 --token 34F6-8C39-4A5C
```

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

macOS

```
sudo "/Library/Application Support/BackupClient/Acronis/RegisterAgentTool/RegisterAgent"
-o register -a https://10.250.144.179:9877 -u johndoe -p johnspassword
```

```
sudo "/usr/lib/Acronis/RegisterAgentTool/RegisterAgent" -o register -a
https://10.250.144.179:9877 --tenant 590b1dd7-8adb-11ea-bf44-0050569deecf
```

```
sudo "/usr/lib/Acronis/RegisterAgentTool/RegisterAgent" -o register -a
https://10.250.144.179:9877 -u johndoe -p johnspassword --tenant 590b1dd7-8adb-11ea-
bf44-0050569deecf
```

```
sudo "/Library/Application Support/BackupClient/Acronis/RegisterAgentTool/RegisterAgent"
-o register -a https://10.250.144.179:9877 --token 9DBF-3DA9-4DAB
```

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

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。

```
<path to the registration tool> -o register -a <management server address:port> -u <user
name> -p <"password">
```

例（Windows）：

```
"%ProgramFiles%\BackupClient\RegisterAgentTool\register_agent.exe" -o register -a
https://10.250.144.179:9877 -u johndoe -p "johns password"
```

それでもエラーになる場合は、以下の手順を実行します。

1. 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）。
2. 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（Windows）：

```
"%ProgramFiles%\BackupClient\RegisterAgentTool\register_agent.exe" -o register -a
https://10.250.144.179:9877 -u johndoe -b -p am9obnNwYXNzd29yZA==
```

ソフトウェアのアップデートの確認

この機能は、組織管理者のみが利用できます。

Cyber Protect ウェブ コンソールにサインインするたびに、Acronis Cyber Protect が Acronis の Web サイトで新バージョンが公開されているかどうかを確認します。新バージョンが利用できる場合は、Cyber Protect ウェブ コンソールに、**[デバイス]**、**[計画]**、**[バックアップストレージ]** タブの各ページの下部に新バージョンのダウンロードリンクが表示されます。**[設定]** > **[エージェント]** ページでもリンクを利用できます。

アップデートの自動確認を有効または無効にするには、**アップデート**のシステム設定を変更します。

手動でアップデートを確認するには、右上にある「?」アイコン > **[バージョン情報]** > **[更新の確認]** をクリックするか、「?」アイコン > **[更新の確認]** をクリックします。

管理サーバーをマイグレーションする

同じ環境内の別のWindowsマシンで実行されている管理サーバーをマイグレーションできます。

マイグレーションのプロセスは以下のフェーズで構成されます:

1. "ソースマシンの処理"（124ページ）
   このフェーズでは、マイグレーション用に元の管理サーバーのデータを準備します。
2. "ターゲットマシン上での処理"（126ページ）
   このフェーズでは、新しい管理サーバーをインストールおよび構成し、元の管理サーバーから新しい管理サーバーにデータをコピーします。

前提条件

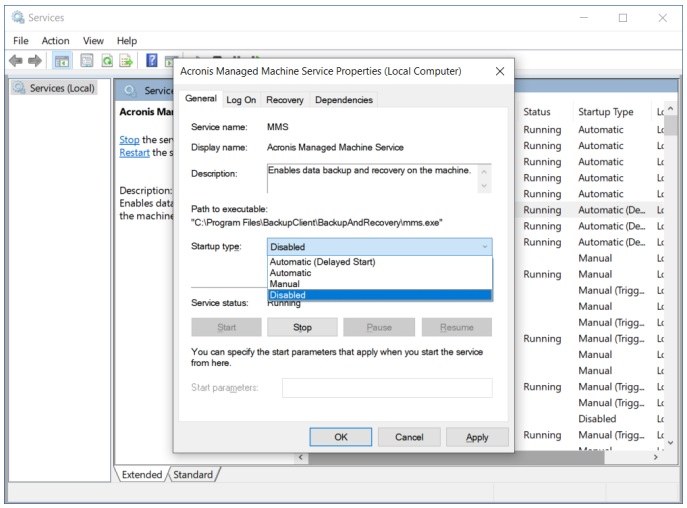
- 管理サーバーでは、外部のMicrosoft SQL Serverデータベースが使用されます。Microsoft SQL Serverインスタンスは、専用マシンで稼働しています。
- プロテクションエージェントは、管理サーバーのホスト名を使用して登録されます（IPアドレスではなく）。
- 管理サーバーのバージョンは、Acronis Cyber Protect Update 4（ビルド29486）以降です。
- ソースおよびターゲットマシンの両方に、同じバージョンの管理サーバーがインストールされています。

ソースマシンの処理

このフェーズでは、マイグレーション用に元の管理サーバーのデータを準備します。

マイグレーション用のデータを準備するには

1. 元の管理サーバーマシンで、すべてのAcronisサービスを停止します。
   a. **[サービス]** を開き、**Acronis Active Protection Service**と**Acronis Cyber Protection Service**以外のAcronisサービスの起動を無効化します。



b. **[Regedit]** を開き、**Acronis Active Protection Service**と**Acronis Cyber Protection Service**のキーを編集して無効化します。

- `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\AcronisCyberProtectionService` キーで、**Start**の値を開き、値データを4に設定します。
- `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\AcronisActiveProtectionService` キーで、**Start**の値を開き、値データを4に設定します。

2. 管理サーバーマシンを再起動し、無効化されたAcronisサービスが稼働していないことを確認します。

注意
Acronis Scheduler Service Helperと**Acronis TIB Mounter Monitor**の2種類のサービスが依然として実行されている可能性があります。これらは無視しても問題ありません。

3. （管理サーバーマシンにCyber Protectモニタコンポーネントがインストールされている場合）Acronis Cyber Protectモニタを終了します。
4. Windowsのコマンドプロンプトで以下のコマンドを実行し、`%ProgramData%\Acronis`および`%ProgramFiles%\Acronis`フォルダの所有者を変更します:

```
takeown /f "%ProgramData%\Acronis" /r /d y
```

```
takeown /f "%ProgramFiles%\Acronis" /r /d y
```

5. 以下のコマンドを実行して、これらのフォルダおよびそのサブフォルダのアクセス許可を編集します:

```
icacls "%ProgramData%\Acronis" /grant everyone:F /t
```

```
icacls "%ProgramFiles%\Acronis" /grant everyone:F /t
```

6. 新しい管理サーバーマシンがアクセスできるネットワーク共有に、`%ProgramData%\Acronis`および`%ProgramFiles%\Acronis`フォルダをコピーします。

7. 元の管理サーバーマシンをシャットダウンします。

次に、"ターゲットマシン上での処理"（126ページ）の手順を実行します。

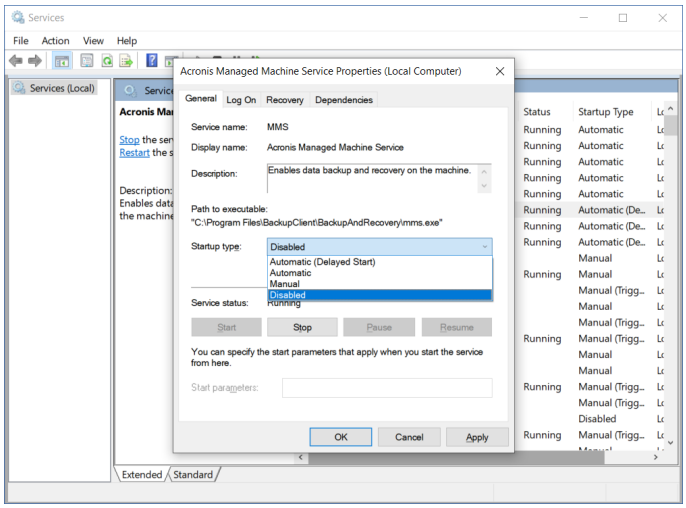
ターゲットマシン上での処理

このフェーズでは、新しい管理サーバーをインストールおよび構成し、そのサーバーにデータをマイグレーションします。

ターゲットマシン上での処理を実行する前に、"ソースマシンの処理"（124ページ）の手順が完了していることを確認します。

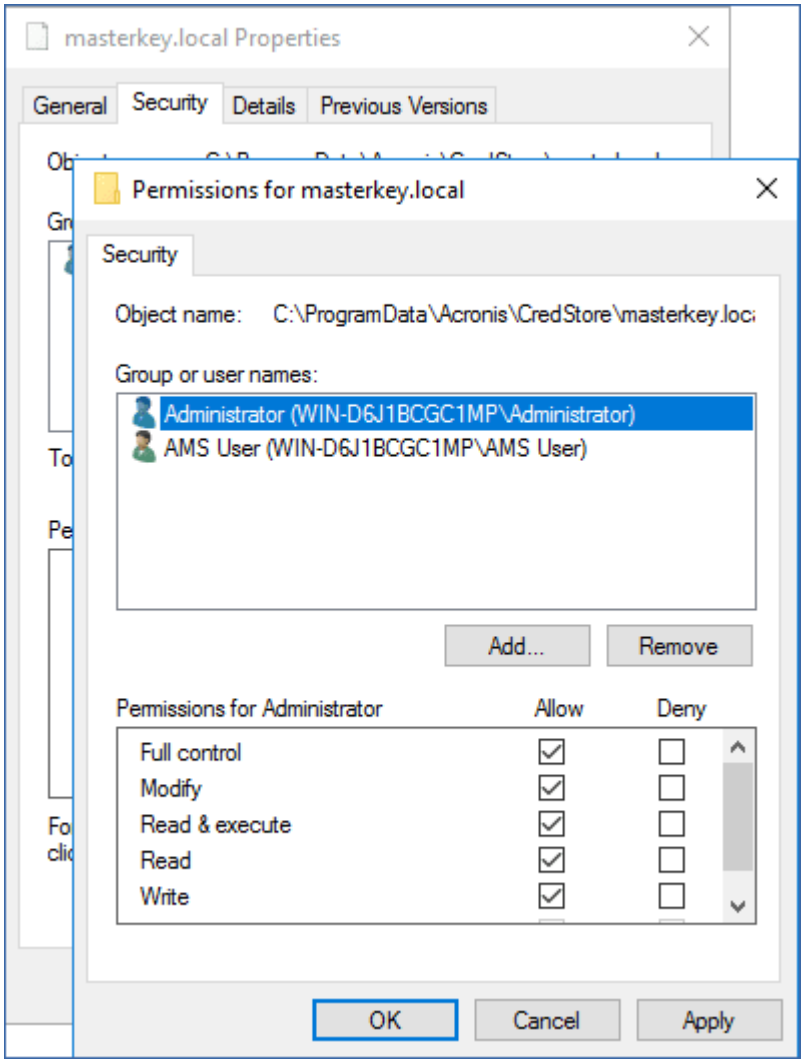
新しい管理サーバーにデータをマイグレーションするには

1. 新しい管理サーバーをインストールするマシンのホスト名を設定します。この名前は、元の管理サーバーのマシン名と同一でなければなりません。
2. TCPポート9877のトラフィックをすべてブロックするファイアウォールルールを作成します。
3. Acronis Cyber Protectセットアッププログラムを実行します。
   a. ライセンス契約とプライバシーステートメントに同意して、**[次へ]** をクリックします。
   b. **[インストール設定のカスタマイズ]** をクリックします。
   c. **[インストールする項目]** で、以下のコンポーネントのみを選択してから、**[完了]** をクリックします。
      - 管理サーバー
      - リモート インストールのコンポーネント
      - ブータブルメディアビルダー
      - コマンドラインツール
   d. **管理サーバーのデータベース**で、デフォルトのオプションである **[ビルトインSQLite]** をそのまま使用します。
   e. **管理サーバーサービスのログオンアカウント**では、元の管理サーバーと同じオプションを使用します。
4. すべてのAcronisサービスを停止します。
   a. **[サービス]** を開き、すべてのAcronisサービスの起動を無効化します。



b. マシンを再起動し、無効化されたAcronisサービスが稼働していないことを確認します。

5. `%ProgramData%\Acronis\CredStore`に移動し、`masterkey.local`ファイルの許可を以下のように調整します。
   a. ファイルの所有権を**管理者**ユーザーアカウントに付与します。
   b. **管理者**ユーザーアカウントの**フルコントロール**許可を付与します。



6. `%ProgramData%\Acronis\AMS\AccessVault\config`に移動してから、以下のファイルに対する**管理者**ユーザーアカウントの**フルコントロール**許可を付与します。
   - `%ProgramData%\Acronis\AMS\AccessVault\config\preferred`
   - `%ProgramData%\Acronis\AMS\AccessVault\config\preferred.json`
7. 以下のフォルダを、元の管理サーバーマシンからネットワーク共有にコピーしたフォルダと置き換えます。
   - `%ProgramData%\Acronis`
   - `%ProgramFiles%\Acronis`

重要
既存のフォルダを削除せずに上書きします。

注意
メッセージが表示され、%ProgramFiles%\Acronis\ShellExtentionsフォルダを置き換えることができない場合、このフォルダはスキップしてください。

8. 以下のファイルの許可を復元します。
   - %ProgramData%\Acronis\CredStore\masterkey.local - 許可を付与されたユーザーのリストから**管理者**ユーザーアカウントを削除します。
   - %ProgramData%\Acronis\AMS\AccessVault\config\preferred - **管理者**ユーザーアカウントに**読み取り**許可のみを付与します。
   - %ProgramData%\Acronis\AMS\AccessVault\config\preferred.json - **管理者**ユーザーアカウントに**読み取り**許可のみを付与します。
9. NGMP\latestフォルダのディレクトリショートカットを作成します。
   - Windowsのコマンドプロンプトで、%ProgramData%\Acronis\NGMPに移動し、latestフォルダを削除します。

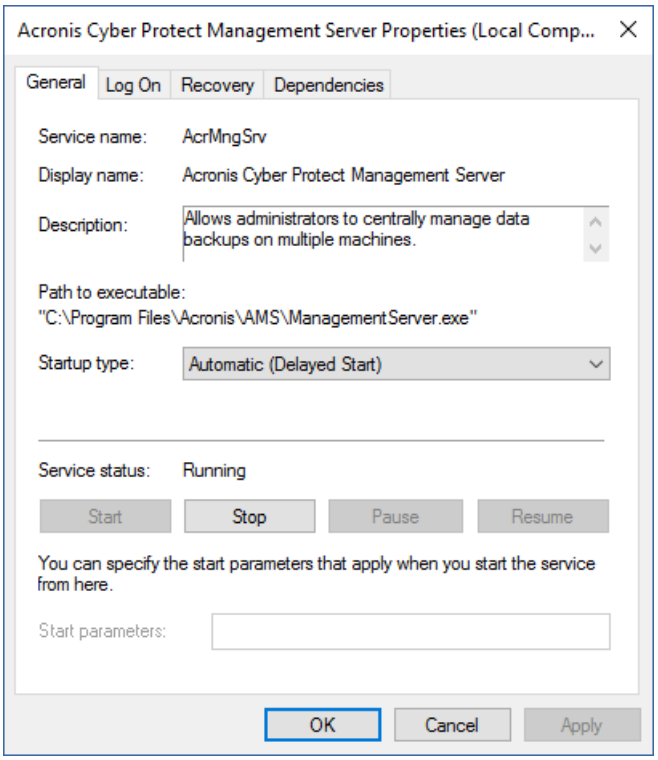
     ```
     cd %ProgramData%\Acronis\NGMP
     ```

     ```
     rmdir latest
     ```

   - ディレクトリショートカットlatestを作成し、現在のNGMPバージョンを示すフォルダと関連付けます。例:

     ```
     mklink /j latest C:\ProgramData\Acronis\NGMP\1.0.2653.0
     ```

10. 新しい管理サーバーを元の管理サーバーが使用していたMicrosoft SQL Serverデータベースと関連付けます。
    a. **Regedit**を開きます。
    b. HKEY_LOCAL_MACHINE\SOFTWARE\Acronis\AMS\Settingsキーで、AmsDmlDbProtocolの値のデータをconfig://C:\ProgramData\Acronis\AMS\mssql\dml_mssql.configに変更します。
11. **サービス**を開き、無効化されているAcronisサービスをすべて有効化します。
    Acronis Cyber Protect管理サーバーの起動タイプを **[自動（遅延起動）]**、その他のAcronisサービスの起動タイプを **[自動]** に設定します。



12. ファイアウォールで、TCPポート9877のすべてのトラフィックを許可します。
13. マシンを再起動し、すべてのAcronisサービスが稼働していることを確認します。
14. Acronis Cyber Protectセットアッププログラムを実行し、以下の項目をインストールします。
    - Windowsエージェント
    - （オプション） Cyber Protectモニタ
15. コンピュータを再起動します。

クラウドデプロイ

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。

- **アカウント有効化リンク。**リンクをクリックして、アカウントのパスワードを設定します。アカウント承認ページに表示されているログイン情報を覚えておいてください。
- **Cyber Protect ウェブ コンソールのログインページへのリンク。**このリンクは今後コンソールにアクセスするために使用します。ログインIDとパスワードは、前の手順と同じです。

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。エージェントの詳細については、"コンポーネント"（47ページ）を参照してください。

手順2

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"（174ページ）で詳しく説明しています。

Agent for Office 365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]** > **[Agent for Office 365]** 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。

サイバープロテクション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3

インストールする前に、ファイアウォールおよびネットワークセキュリティシステム（プロキシサーバーなど）で次のTCPポートを使用した受信と送信の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 ProtectWeb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"（132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。

手順4

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。

Active ProtectionサービスはTCPポート**6109**でリッスンします。他のプロセスによって使用されていないことを確認してください。

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`

プロキシサーバー設定

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、インストール中またはあらかじめプロキシサーバー設定を指定する必要があります。

Windowsの場合

Windowsでプロキシサーバーが構成されている場合（**[コントロールパネル]** > **[インターネットオプション]** > **[接続]**）、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。または、インストール中にプロキシ設定を入力することや、以下に説明する手順に従ってあらかじめ指定することもできます。インストール後にプロキシ設定を変更するには、同じ手順を実行します。

Windowsでプロキシ設定を指定するには

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. プロテクション エージェントがまだインストールされていない場合は、ここでインストールできます。または、次の手順でエージェントを再起動します。
   a. **[スタート]** メニューで、**[ファイル名を指定して実行]** をクリックし、「**cmd**」と入力します。
   b. **[OK]** をクリックします。

c. 次のコマンドを実行します。

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

Linuxの場合

パラメータ--http-proxy-host=ADDRESS --http-proxy-port=PORT --http-proxy-login=LOGIN--http-proxy-password=PASSWORDを使用してインストールファイルを実行します。インストール後にプロキシ設定を変更するには、次に説明する手順を実行します。

Linuxでプロキシ設定を変更するには

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

   - 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。
3. **アドレス**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、**ポート**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、**ログイン**と**パスワード**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. 任意のディレクトリで次の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
   ```

macOSの場合

インストール中にプロキシ設定を入力することや、以下に説明する手順に従ってあらかじめ指定することもできます。インストール後にプロキシ設定を変更するには、同じ手順を実行します。

macOSでプロキシ設定を指定するには

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. プロテクション エージェントがまだインストールされていない場合は、ここでインストールできます。または、次の手順でエージェントを再起動します。
   a. **[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。
   b. 次のコマンドを実行します。

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

ブータブルメディアにおいて

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指定するには、**[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、および資格情報を指定します。

エージェントのインストール

Windowsの場合

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. Windowsに管理者権限でログオンし、プログラムの設定を開始します。
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（特に、Cyber Protect Monitor とコマンドラインツールのインストールを無効にするには）。
   - サイバープロテクションサービスにマシンを登録する方法を変更する場合。**[Cyber Protect コンソールを使用]**（デフォルト）から **[資格情報を使用]** または **[登録トークンを使用]** へ切り替えることができます。
   - 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のアカウントを変更する場合。
   - 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. （エージェント for VMware をインストールする場合のみ）仮想マシンがバックアップ対象の 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**の役割が割り当てられたアカウントを使用することをお勧めします。そうしない場合は、vCenter ServerまたはESXi上で必要な権限を持つアカウントを指定します。
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 **[Cyber Protect コンソールを使用]** 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。
   - **[マシンの登録]** をクリックします。開いたブラウザウィンドウで、Cyber Protect ウェブ コンソールにサインインしてから、登録の詳細を確認して **[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。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。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。
9. **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から、**[マシンを登録する]** をクリックする必要があります。

   その結果、マシンは Cyber Protect ウェブ 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。

Linuxの場合

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. rootユーザーとしてインストール ファイルを実行します。
   ネットワーク内でプロキシサーバが有効な場合、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`。

サイバープロテクション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。
   - **エージェント for Linux**
   - **エージェント for Virtuozzo**

   エージェント for Virtuozzo は Linux エージェントがないとインストールできません。
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、サイバープロテクション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。
   - **[マシンの登録]** をクリックします。開いたブラウザウィンドウで、Cyber Protect ウェブ コンソールにサインインしてから、登録の詳細を確認して **[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。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。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。
6. **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、マシンは Cyber Protect ウェブ 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。
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

   インストール中に新しいキーが生成され、このキーが`snapapi`モジュールに署名するために使用され、マシン所有者キー（MOK）として登録されます。このキーを登録するために、再起動が必須です。キーの登録をしないと、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、手順 6 を含むインストールを繰り返します。
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の場合

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 **[プロテクション 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。
   - **[マシンの登録]** をクリックします。開いたブラウザウィンドウで、Cyber Protect ウェブ コンソールにサインインしてから、登録の詳細を確認して **[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。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。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。
10. **ヒント**登録を確認するまで、セットアッププログラム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、マシンは Cyber Protect ウェブ 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。

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。

インストールの完了後にログオンアカウントを手動で変更することはお勧めできません。

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

このセクションでは、Windowsを実行しているマシンで、Windows Installer（`msiexec`プログラム）によってプロテクションエージェントのインストールとアンインストールを無人モードで実行する方法を説明します。Active Directoryドメインでは、グループポリシーを使用して無人インストールを行う方法があります。これについては、"グループポリシーによるエージェントの配置"（174ページ）を参照してください。

インストール中に、**トランスフォーム**と呼ばれるファイル（.mst ファイル）を使用できます。トランスフォームは、インストールパラメータが指定されたファイルです。別の方法として、インストールパラメータをコマンドラインで直接指定することも可能です。

.mst トランスフォームファイルの作成とインストールパッケージの抽出

1. Windowsに管理者権限でログオンし、プログラムの設定を開始します。
2. [**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。
3. [**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、セットアッププログラムから取り出します。
4. [**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。登録トークンを生成する詳細な方法については、"手順1:登録トークンの生成"（175ページ）を参照してください。
5. （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。

6. .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。
7. .mstトランスフォームファイルを生成して.msiと.cabのインストールパッケージを抽出する、フォルダを選択します。それから **[生成]** をクリックします。

.mst トランスフォームを使用した製品のインストール

コマンドラインで以下のコマンドを実行します。

コマンドテンプレート:

```
msiexec /i <package name> TRANSFORMS=<transform name>
```

ここで、

- **<パッケージ名>** は、.msi ファイルの名前です。
- **<変換名>** は、トランスフォームの名前です。

コマンド例:

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

手動でのパラメータ指定による製品のインストールやインストール解除

コマンドラインで以下のコマンドを実行します。

コマンドテンプレート（インストール）:

```
msiexec /i <package name><PARAMETER 1>=<value 1> ... <PARAMETER N>=<value n>
```

ここでの**<パッケージ名>**は、.msiファイルの名前です。すべての有効なパラメータと値の説明については、"基本パラメータ"（141ページ）を参照してください。

コマンドテンプレート（アンインストール）:

```
msiexec /x <package name> <PARAMETER 1>=<value 1> ... <PARAMETER N>=<value n>
```

.msiパッケージは、アンインストールする製品と同じバージョンでなければなりません。

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、Windows での無人インストールまたはインストール解除中に使用されるパラメータについて説明します。これらのパラメータに加え、https://msdn.microsoft.com/en-us/library/windows/desktop/aa367988(v=vs.85).aspxに記載されているmsiexecのパラメータを使用できます。

インストールパラメータ

基本パラメータ

ADDLOCAL=<list of components>

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。インストールの前に、指定したすべてのコンポーネントをセットアッププログラムから取り出す必要があります。

コンポーネントの完全なリストは、次のとおりです。

コンポーネント	一緒にインストールする必要があるもの	ビット数	コンポーネント名/説明
MmsMspComponents		32 ビット/64 ビット	エージェントのコアコンポーネント
BackupAndRecoveryAgent	MmsMspComponents	32 ビット/64 ビット	エージェント for Windows
ArxAgentFeature	BackupAndRecoveryAgent	32 ビット/64 ビット	Exchangeエージェント
ArsAgentFeature	BackupAndRecoveryAgent	32 ビット/64 ビット	エージェント for SQL
ARADAgentFeature	BackupAndRecoveryAgent	32 ビット/64 ビット	エージェント for Active Directory
ArxOnlineAgentFeature	MmsMspComponents	32 ビット/64 ビット	エージェント for Office 365
OracleAgentFeature	BackupAndRecoveryAgent	32 ビット/64 ビット	Oracle エージェント
AcronisESXSupport	MmsMspComponents	64 ビット	VMware ESX(i) エージェント（Windows）
HyperVAgent	MmsMspComponents	32 ビット/64	エージェント for

		ビット	Hyper-V
CommandLineTool		32 ビット/64 ビット	コマンドライン ツール
TrayMonitor	BackupAndRecoveryAgent	32 ビット/64 ビット	Cyber Protectモニター

TARGETDIR= <path>

製品のインストール先フォルダ。以下のフォルダがデフォルトです。C:\Program Files\BackupClient。

REBOOT=ReallySuppress

このパラメータが指定されていると、マシンの再起動が禁止されます。

/l*v <log file>

このパラメータを指定すると、verbose モードのインストールログが、指定したファイルに保存されます。このログファイルはインストールに関する問題の分析に使用できます。

CURRENT_LANGUAGE= <language 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、システム言語が上記のリストに含まれていれば、それに基づいて製品の言語が定義されます。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

REGISTRATION_ADDRESS

これはCyber Protectサービスの URLです。このパラメータは、REGISTRATION_LOGINおよびREGISTRATION_PASSWORDの両パラメータと一緒に使用することも、REGISTRATION_TOKENと一緒に使用することもできます。

- REGISTRATION_ADDRESSをREGISTRATION_LOGINおよび REGISTRATION_PASSWORDの両パラメータと一緒に使用する場合、Cyber Protect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。

- REGISTRATION_ADDRESSをREGISTRATION_TOKENパラメータと一緒に使用する場合は、データセンターのアドレスをそのまま指定します。これは、Cyber Protectサービスに**ログインすると**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。

`REGISTRATION_LOGIN`および`REGISTRATION_PASSWORD`

エージェントをCyber Protect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。

`REGISTRATION_PASSWORD_ENCODED`

base64でエンコードされた、エージェントをCyber Protect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、「マシンの手動登録」を参照してください。

`REGISTRATION_TOKEN`

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。ウェブ 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）。

`REGISTRATION_REQUIRED={0,1}`

登録が失敗した場合のインストールの終了方法を定義します。値が1の場合、インストールも失敗します。デフォルト値は`0`です。このパラメータを指定しない場合は、エージェントが登録されなくてもインストールは正常に完了します。

その他のパラメータ

Windowsでエージェントサービスのログオンアカウントを定義する場合は、以下のいずれかのパラメータを使用します。

- `MMS_USE_SYSTEM_ACCOUNT={0,1}`
  値が1の場合、**ローカルシステム**のアカウントでエージェントが実行されます。
- `MMS_CREATE_NEW_ACCOUNT={0,1}`
  値が1の場合、**Acronis Agent User**という名前で新規作成されたアカウントでエージェントが実行されます。
- `MMS_SERVICE_USERNAME= <user name>` および `MMS_SERVICE_PASSWORD=<password>`
  これらのパラメータを使用して、エージェントを実行する既存の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」を参照してください。

`SET_ESX_SERVER={0,1}`

- 値が`0`の場合、インストールされるVMwareエージェントは、vCenter ServerやESXiホストに接続されません。値が1の場合、次のパラメータを指定します。

- ESX_HOST=<host name>

  vCenter Server または ESXi ホストのホスト名または IP アドレス。
- ESX_USER=<user name> および ESX_PASSWORD=<password>

  vCenter Server または ESXi ホストにアクセスするための資格情報。

HTTP_PROXY_ADDRESS=<IP address> および HTTP_PROXY_PORT=<port>

エージェントが使用するHTTPプロキシサーバー。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=<login> および HTTP_PROXY_PASSWORD=<password>

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。

HTTP_PROXY_ONLINE_BACKUP={0,1}

値が0の場合、またはパラメータが指定されていない場合、エージェントはクラウドからのバックアップと復元にのみプロキシサーバーを使用します。値が1である場合、エージェントはさらにプロキシサーバー経由で管理サーバーに接続します。

インストール解除パラメータ

REMOVE={<list of components>|ALL}

削除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。値がALLの場合、すべての製品コンポーネントがアンインストールされます。

また、次のパラメータを指定できます。

DELETE_ALL_SETTINGS={0, 1}

値が1の場合、製品のログ、タスク、構成の設定が削除されます。

例

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

```
msiexec.exe /i BackupClient64.msi /l*v my_log.txt /qn
ADDLOCAL=MmsMspComponents,BackupAndRecoveryAgent,CommandLineTool,TrayMonitor
TARGETDIR="C:\Program Files\BackupClient" REBOOT=ReallySuppress MMS_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 Protection Monitorをインストールする操作。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 Protectサービスにマシンを登録する操作。

```
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 Protection Monitorをインストールする操作。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 Protectサービスにマシンを登録する操作。

```
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 Protection Monitorをインストールする操作。トークンを使用してCyber Protect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
```

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

```
msiexec.exe /x BackupClient64.msi /l*v uninstall_log.txt REMOVE=ALL DELETE_ALL_
SETTINGS=1 REBOOT=ReallySuppress
```

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。

保護エージェントをインストール/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。

- 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、**<パッケージ名>** 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」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。

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=}<list of components>`

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	エージェント for Linux
AgentForPCS	エージェント for Virtuozzo
OracleAgentFeature	Oracle 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エージェントとOracleエージェントの場合は、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 Protect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=<location>`

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=<language 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=}` `<user name>` および `{-w|--password=}<password>`

  エージェントをCyber Protect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=` `<token>`

  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。ウェブ 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=}` `<service address>`

    Cyber Protect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 Protect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 Protect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 Protect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 Protect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 address>` および `--http-proxy-port=<port>`

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=` `<login>` および `--http-proxy-password=<password>`

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=<location>`

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）。このオプションを使用することはお勧めできません。

`--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=}` `<path>`

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=}` `<port>`

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エージェントとVirtuozzoエージェントと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。インストールファイル（.dmg）をダウンロードする方法の詳細については、「macOSを実行しているマシンの追加」を参照してください。

Macエージェントをインストールする

1. 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>
   ```

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

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

   <dmg_file> はインストールファイルの名前です。たとえば、**AcronisAgentMspMacOSX64.dmg**のようになります。
3. インストーラを実行します。

   ```
   sudo installer -pkg <dmg_root>/Install.pkg -target LocalSystem
   ```
4. 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/AcronisAgentMspMacOSX64.dmg -mountpoint mydirectory
  ```

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

  ```
  hdiutil detach mydirectory
  ```

Macエージェントを登録するには

次のいずれかを実行します。
  ```

- ユーザー名とパスワードを使用して、指定したアカウントでエージェントを登録します。

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

この場合:

<Cyber Protectの**サービスアドレス**>は、Cyber Protectサービスへの**ログイン**に使用するアドレスです。
例:

<**ユーザー名**>および <**パスワード**> は、エージェントが登録され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。

- 登録トークンを使用してエージェントを登録します。

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

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ウェブ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）。

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サービスに**ログインすると**表示されるURLです。例:

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。

例

ユーザー名とパスワードで登録します。

-

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

トークンで登録します。

- ```
  sudo /Library/Application\
  Support/BackupClient/Acronis/RegisterAgentTool/RegisterAgent -o register -t cloud -a
  https://eu2-cloud company.com --token D91D-DC46-4F0B
  ```

Macエージェントをインストール解除する

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
  ```

インストール解除中にすべてのログ、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
  ```

マシンの手動登録

エージェントのインストール時にCyber Protectサービスにマシンを登録できますが、それ以外に、コマンドラインインターフェースを使用して登録することも可能です。エージェントのインストール時に自動登録が失敗した場合や、既存のマシンを新しいアカウントで登録する場合などに、この操作が必要になります。

マシンを登録するには

エージェントがインストールされているマシンのコマンドプロンプトで、次のコマンドのいずれかを実行します。

- 現在のアカウントでマシンを登録する:

  ```
  <path to the registration tool> -o register -s mms -t cloud --update
  ```

  - **<登録ツールへのパス>**:
    - Windowsの場合: `%ProgramFiles%\BackupClient\RegisterAgentTool\register_agent.exe`
    - Linuxの場合: `/usr/lib/Acronis/RegisterAgentTool/RegisterAgent`
    - macOSの場合: `/Library/Application Support/BackupClient/Acronis/RegisterAgentTool/RegisterAgent`
- 別のアカウントでマシンを登録する:

  ```
  <path to the registration tool> -o register -t cloud -a <service address> -u <user
  name> -p <password>
  ```

  - ここでは、**<ユーザー名>** および **<パスワード>** は、エージェントが登録される特定の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。
  ```

<サービスアドレス> は、Cyber Protect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。

- 登録トークンでマシンを登録する:

```
<path to the registration tool> -o register -t cloud -a <service address> --token
<token>
```

  - 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、「グループポリシーによるエージェントの配置」を参照してください。

    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 **<サービスアドレス>** として指定しなければなりません。これは、Cyber Protectサービスに**ログインすると**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。

マシンを登録解除するには

エージェントがインストールされているマシンのコマンドプロンプトで、次のコマンドを実行します。

```
<path to the registration tool> -o unregister
```

例

Windows

```
"%ProgramFiles%\BackupClient\RegisterAgentTool\register_agent.exe" -o register -s mms -t
cloud --update
```

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

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

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

Linux

```
sudo "/usr/lib/Acronis/RegisterAgentTool/RegisterAgent" -o register -s mms -t cloud --
update
```

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

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

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

macOS

```
sudo "/Library/Application Support/BackupClient/Acronis/RegisterAgentTool/RegisterAgent"
-o register -s mms -t cloud --update
```

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

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

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

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。

```
<path to the registration tool> -o register -t cloud -a <service address> -u <user name>
-p <"password">
```

例（Windows）：

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

それでもエラーになる場合は、以下の手順を実行します。

- 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）。
- 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。

```
<path to the registration tool> -o register -t cloud -a <service address> -u <user name>
-b -p <encoded password>
```

例（Windows）：

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

oVirt（仮想アプライアンス）エージェントをデプロイ中

oVirtエージェント（仮想アプライアンス）を配置および構成する方法については、Cyber Protection Cloudの文書を参照してください。

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

Virtuozzo Hybrid Infrastructureエージェント（仮想アプライアンス）を配置および構成する方法については、Cyber Protection Cloudの文書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管理サーバーへの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。

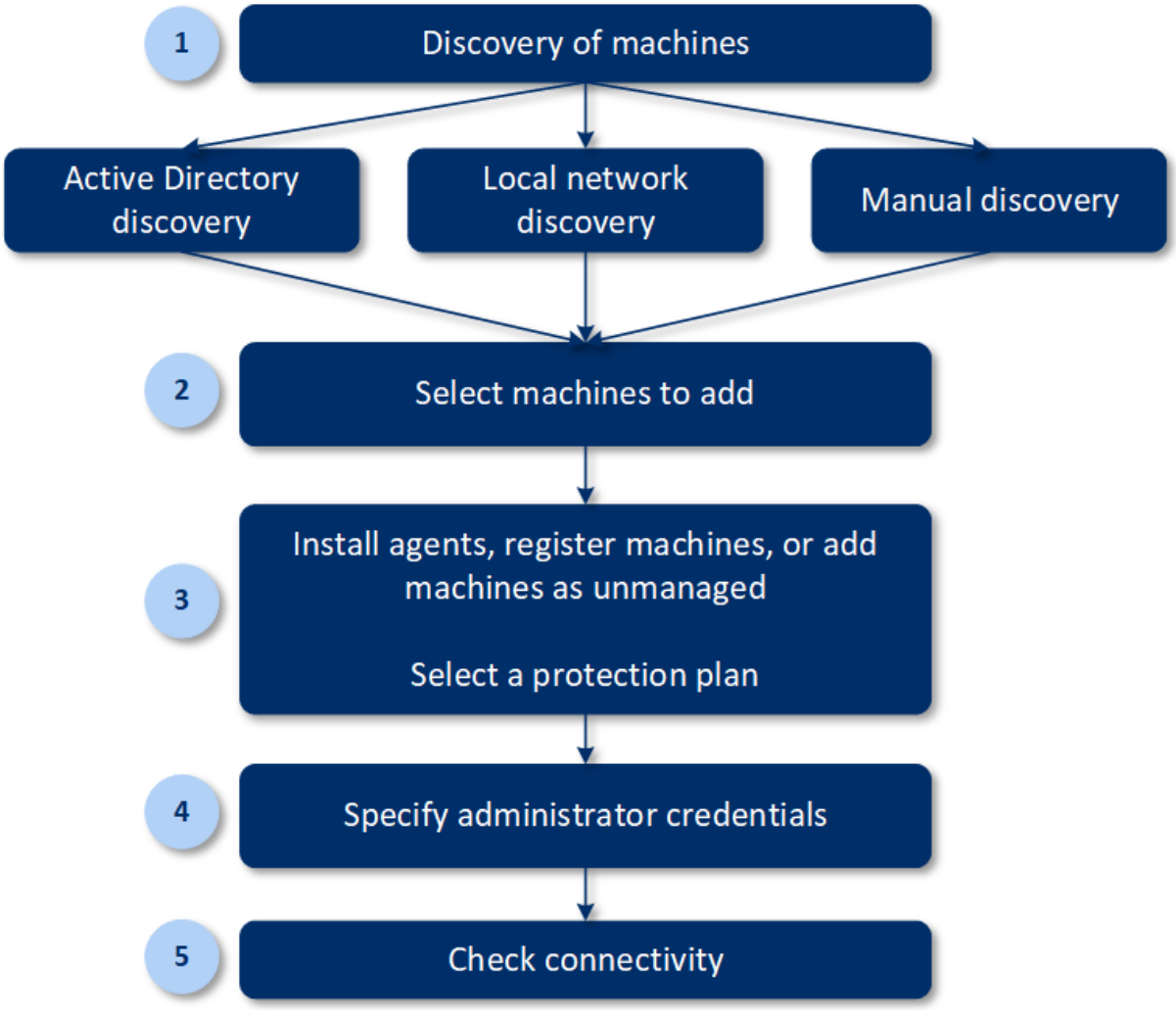
自動検出の仕組み

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（短い/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、それらをウェブコンソールに登録する。

- ウェブ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すで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**としてウェブ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、またはウェブ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. エージェントが管理サーバーへのアクセスに使用するサーバー名またはIPアドレスを選択します。

   デフォルトでは、サーバー名が選択されています。もし管理サーバーに複数のネットワークインターフェースが存在する場合や、エージェントの登録失敗の原因となり得るDNSの問題がある場合は、IPアドレスを選択する必要があります。
6. 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ウェブ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。

自動検出と手動検出

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。

マシンの検出手順

1. ウェブコンソールコンソールで **[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い場合は、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. （検出方法にActive Directoryまたはローカルネットワークが選択されている場合）リストを使用して、追加するマシンを選択します。

   （検出方法に手動検出が選択されている場合）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。ファイルのサンプル:

   ```
   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、ファイルからアドレスをインポートした後、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. 検出後に行う処理を選択します。

   - **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」を参照してください。最大で同時に100個のエージェントをインストールできます。

     [**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。

     [**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 Protectでの登録のみ必要な場合、このオプションが使用されます。マシン内に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**。エージェントはマシンにインストールされません。ウェブ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。

（検出後のアクションで **[エージェントのインストールとマシンの登録]** が選択された場合）**[必要に応じてマシンを再起動]** - このオプションが有効化された場合、インストール完了に必要な回数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。

（**[必要に応じてマシンを再起動]** が選択された場合）**[ユーザーのログイン中は再起動しない]** - このオプションが有効化された場合、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。たとえば、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た後、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、再起動が実行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。

（組織が部署に分かれている場合）**[マシンを登録する部署]** - マシンが登録される部署を選択します。

検出後のアクションのうち最初の2つのいずれかを選択した場合は、保護計画をマシンに登録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、「Windowsで実行するマシンの追加」 > 「準備」に記載された追加の準備手順を手動で実行する必要があります。

11. エージェントが管理サーバーへのアクセスに使用するサーバー名またはIPアドレスを選択します。

    デフォルトでは、サーバー名が選択されています。もし管理サーバーに複数のネットワークインターフェースが存在する場合や、エージェントの登録失敗の原因となり得るDNSの問題がある場合は、IPアドレスを選択する必要があります。

12. 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**ダッシュボード** > **[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。

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	
エージェント for Windows	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	
エージェント for Hyper-V	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。
エージェント for SQL	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。
エージェント for Office 365	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 Protect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。
コマンドラインツール	Cyber Protectには、acrocmdユーティリティに対するコマンドラインインターフェースが用意されています。acrocmdにはコマンドを物理的に実行するツールは含まれていません。Cyber Protectコンポーネント（エージェントと管理サーバー）へのコマンドラインインターフェースだけを提供するものです。選択された場合にインストールされます。

ブータブルメディアビルダー	このコンポーネントによって、ユーザーはブータブルメディアの作成を行えます。選択した場合は、Windows マシンにインストールされます。

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 Protect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。

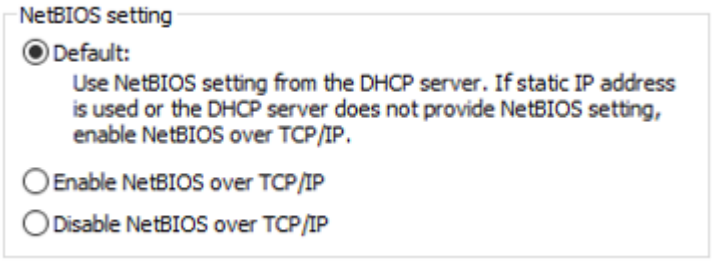
保護エージェントがマシンにインストールされると、それらのマシンが **[デバイス]** > **[エージェントがインストールされているマシン]** セクションに表示されます。

保護ステータスを確認するには、**[ダッシュボード]** > **[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。

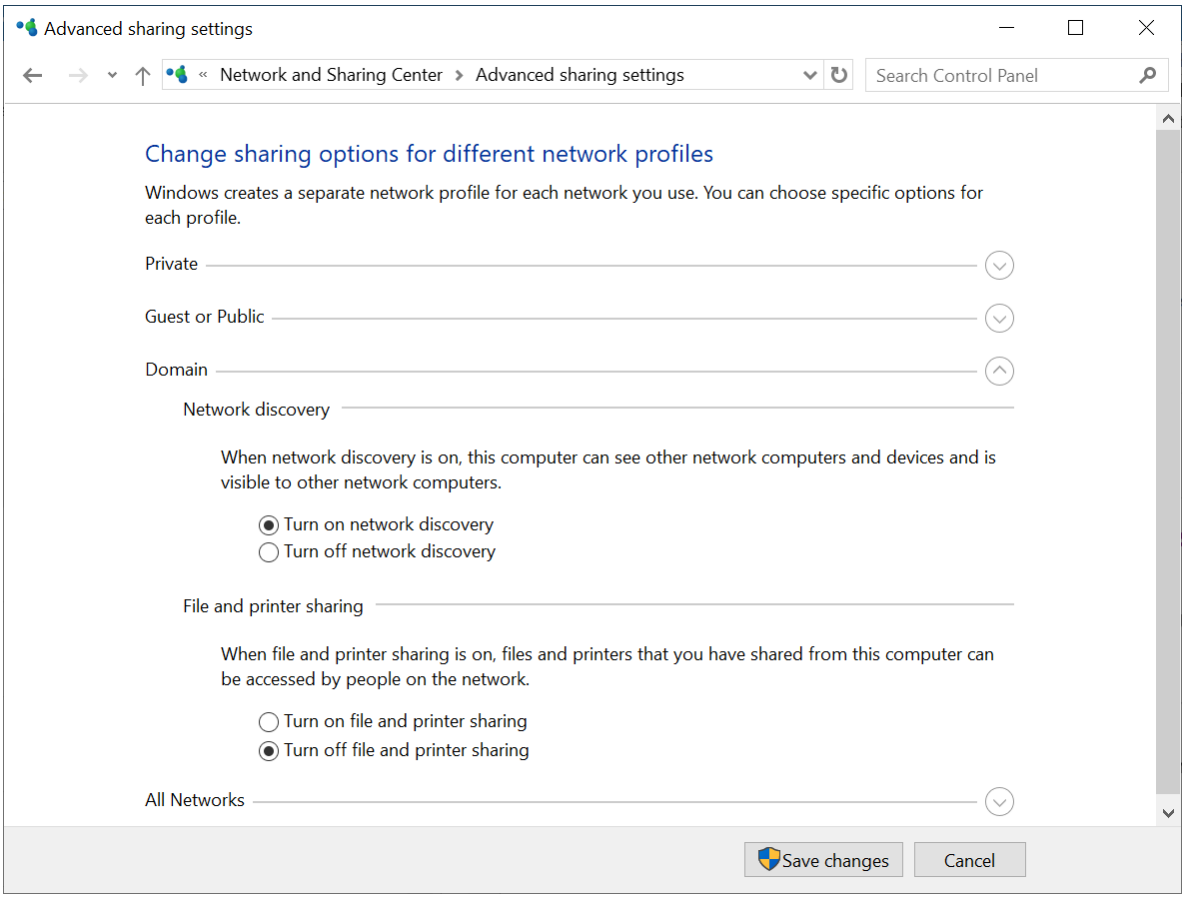
トラブルシューティング

自動検出機能に問題が発生した場合、次の点を試してください。

- 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]** に移動し、ネットワーク検出を有効にします。



- 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。

OVFテンプレートからエージェント for VMware（仮想アプライアンス）のデプロイ

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。バックアップトラフィック帯域幅が100MB/秒を超える（10GBitネットワークなど）場合、バックアップの作成速度を向上するために、これらのリソースを8GBのRAMと4個のvCPUに増設することをお勧めします。

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。

注意
仮想マシンのバックアップを有効にするには、vStorage APIをESXiホストにインストールする必要があります。https://kb.acronis.com/content/14931を参照してください。

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。詳細については、「ローカルに接続されたストレージの使用」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

OVFテンプレートのロケーション

OVF テンプレートは 1 つの .ovf ファイルと 2 つの .vmdk ファイルで構成されます。

オンプレミスデプロイ

管理サーバーのインストールが完了すると、仮想アプライアンスの OVF パッケージはフォルダ **%ProgramFiles%¥Acronis¥ESXAppliance**（Windows）または**/usr/lib/Acronis/ESXAppliance**（Linux）に置かれます。

クラウドデプロイの場合

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。

OVFテンプレートの配置

1. OVFテンプレートファイルがvSphereクライアントを実行するマシンからアクセスできることを確認してください。
2. vSphere クライアントを起動し、vCenter Serverにログインします。
3. 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クラウドデプロイで構成する場合は、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。ネットワーク接続をオンプレミスデプロイで構成する場合は、管理サーバーを含むネットワークを選択します。

仮想アプライアンスの設定

1. **仮想アプライアンスの起動**

   vSphere クライアントで、**[インベントリ]** を表示し、仮想アプライアンスの名前を右クリックしてから、**[パワー]** > **[パワー オン]** をクリックします。**[コンソール]**タブをクリックします。
2. **プロキシサーバー**

   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:

   a. コマンドシェルを起動するには、仮想アプライアンスUIで、CTRL+SHIFT+F2キーを押します。

   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. **アドレス**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、**ポート**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、**ログイン**と**パスワード**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。

それ以外の場合は、この手順をスキップします。

3. **ネットワーク設定**

   エージェントのネットワーク接続は DHCP（Dynamic Host Configuration Protocol）を使用して自動的に設定されます。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]**の下の **[eth0]** で **[変更]** をクリックして、必要なネットワーク設定を指定します。

4. **vCenter/ESX(i)**

   [エージェント オプション] の下の **[vCenter/ESX(i)]** で、**[変更]** をクリックして、vCenter Server名または IP アドレスを指定します。エージェントが、vCenter Serverによって管理されるすべての仮想コンピュータをバックアップおよび復元できるようになります。

   vCenter Serverを使用していない場合、仮想コンピュータをバックアップして復元する ESXiホストの名前または IP アドレスを指定します。通常、エージェントでホストしている仮想マシンをバックアップする場合、エージェントでホストされていないマシンと比較して、バックアップをより速く行えます。

   エージェントがvCenter Serverまたは ESXiへの接続に使用する資格情報を指定します。**管理者**の役割が割り当てられたアカウントを使用することをお勧めします。そうしない場合は、vCenter ServerまたはESXi上で必要な権限を持つアカウントを指定します。

   [接続の確認] をクリックすると、このアクセス認証情報が正しいかどうかを確認できます。

5. **管理サーバー**

a. **[エージェントオプション]** の下、**[管理サーバー]** で、**[変更]** をクリックします。
b. **サーバー名/IP**において、次のいずれかを実行します。
   - オンプレミスデプロイでは、**[ローカル]** を選択します。Management Serverがインストールされているコンピュータのホスト名または IPアドレスを指定します。
   - クラウドデプロイについては、**クラウド**を選択します。ソフトウェアにより、サイバープロテクション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]** と **[パスワード]** では、次のいずれかを実行します。
   - オンプレミスデプロイの場合、管理サーバーの管理者のユーザー名とパスワードを指定します。
   - クラウドデプロイメントの場合、サイバープロテクションサービスのユーザー名とパスワードを指定します。エージェントとエージェント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。

6. **タイム ゾーン**

   仮想コンピュータの**タイムゾーン**で**[変更]**をクリックします。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。

7. **（オプション）ローカルストレージ**

   追加のディスクを仮想アプライアンスに接続して、VMwareエージェントによるバックアップ先を、このローカルに接続されたストレージにすることが可能です。

   仮想コンピュータの設定を編集してディスクを追加し、**[アップデート]** をクリックします。**[ストレージの作成]** リンクが使用できるようになります。このリンクをクリックし、ディスクを選択して、そのディスクのラベルを指定します。

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

仮想アプライアンスを配置する際には、vCPU と RAM の組み合わせの中から選択できます。2 個の vCPU と 4GiB の RAM が十分かつ最適です。バックアップトラフィック帯域幅が 100MB/ 秒を超える（10GBit ネットワークなど）場合、バックアップの作成速度を向上するために、これらのリソースを 4 個の vCPU と8 GiB の RAM に増設することをお勧めします。

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。

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、各エージェントで同じ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。たとえば、マシンやエージェントの追加や削除を行ったときに、自動再配分が行われる場合があります。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Management Serverから削除すると、エージェントに割り当てられたコンピュータ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。

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
- **[設定]** > **[エージェント]** でエージェントを選択した場合は、**[詳細]** ペインの **[割り当てられた仮想マシン]** セクション

仮想アプライアンスのデプロイ

1. Cyber Protect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。
3. デプロイする仮想アプライアンスの数を選択します。
4. Scale Computing HC3 クラスターの IP アドレスまたはホスト名を指定します。
5. このクラスターで **VM 作成/編集**ロールが割り当てられたアカウントの資格情報を指定します。
6. 仮想アプライアンスのイメージファイルの一時ストレージ向けに使用されるネットワーク共有を指定します。2 GB 以上の空き領域が必要です。
7. このネットワーク共有への読み書きアクセスが付与されたアカウントの資格情報を指定します。
8. **[デプロイ]** をクリックします。

デプロイが完了した後、仮想アプライアンスを構成します。

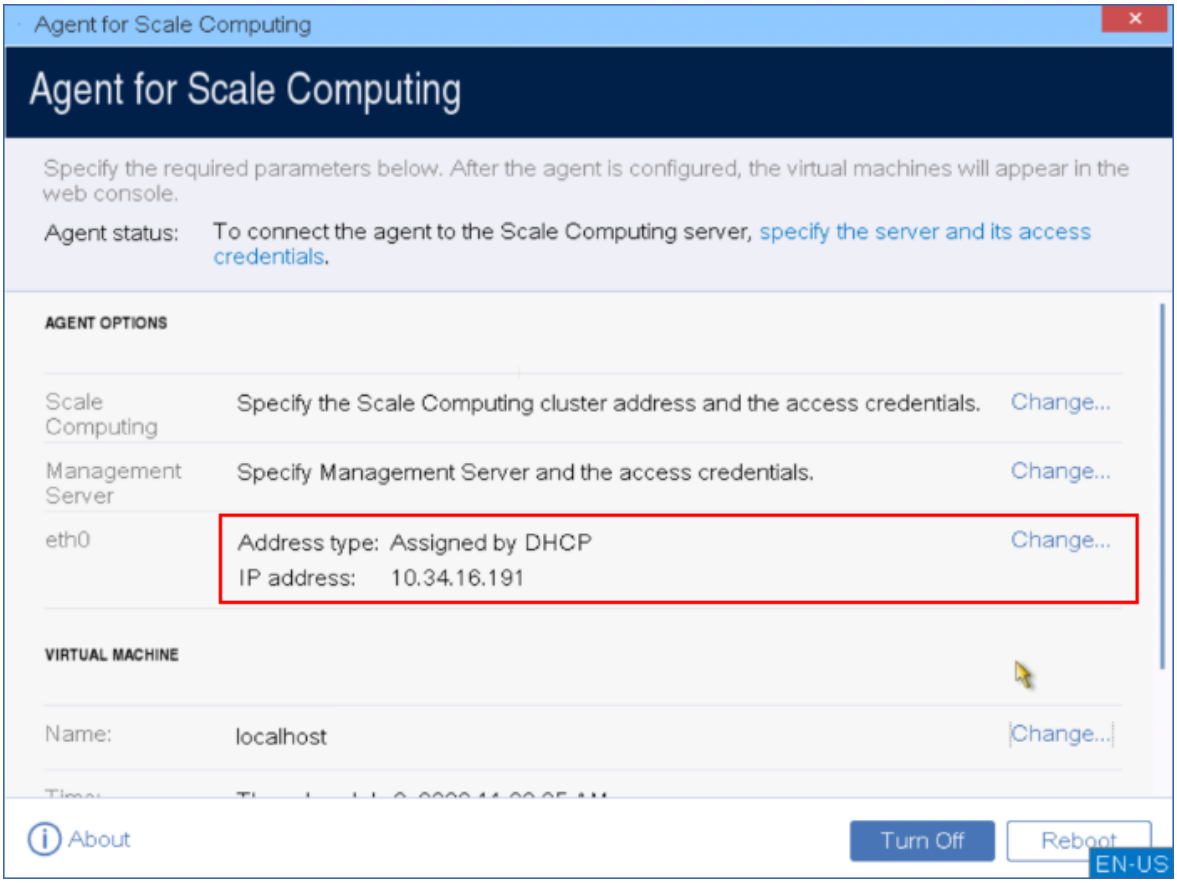
仮想アプライアンスの設定

仮想アプライアンスを配置した後、保護する Scale Computing HC3 クラスターと Cyber Protect 管理サーバー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。

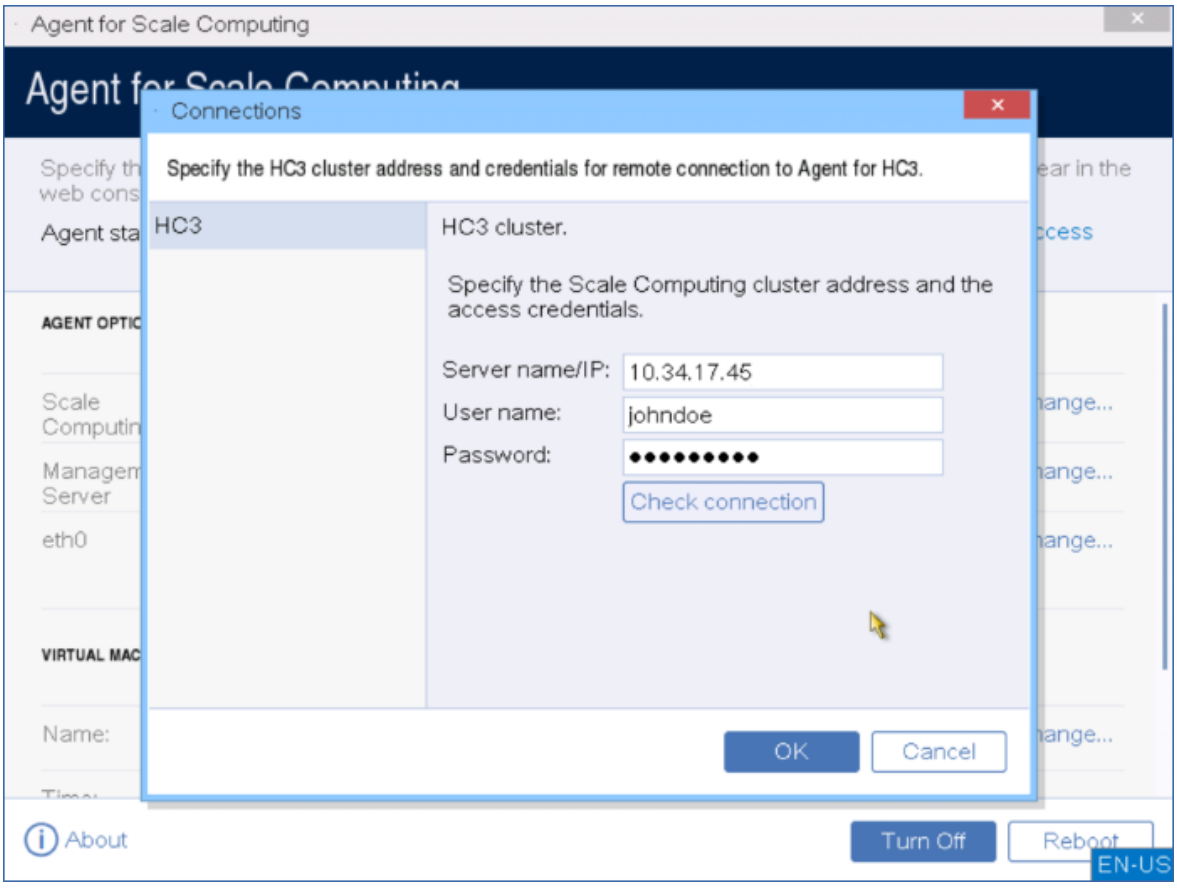
1. Scale Computing HC3 アカウントにログインします。
2. 構成する必要があるエージェントの仮想マシンを選択し、**コンソール**をクリックします。

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。

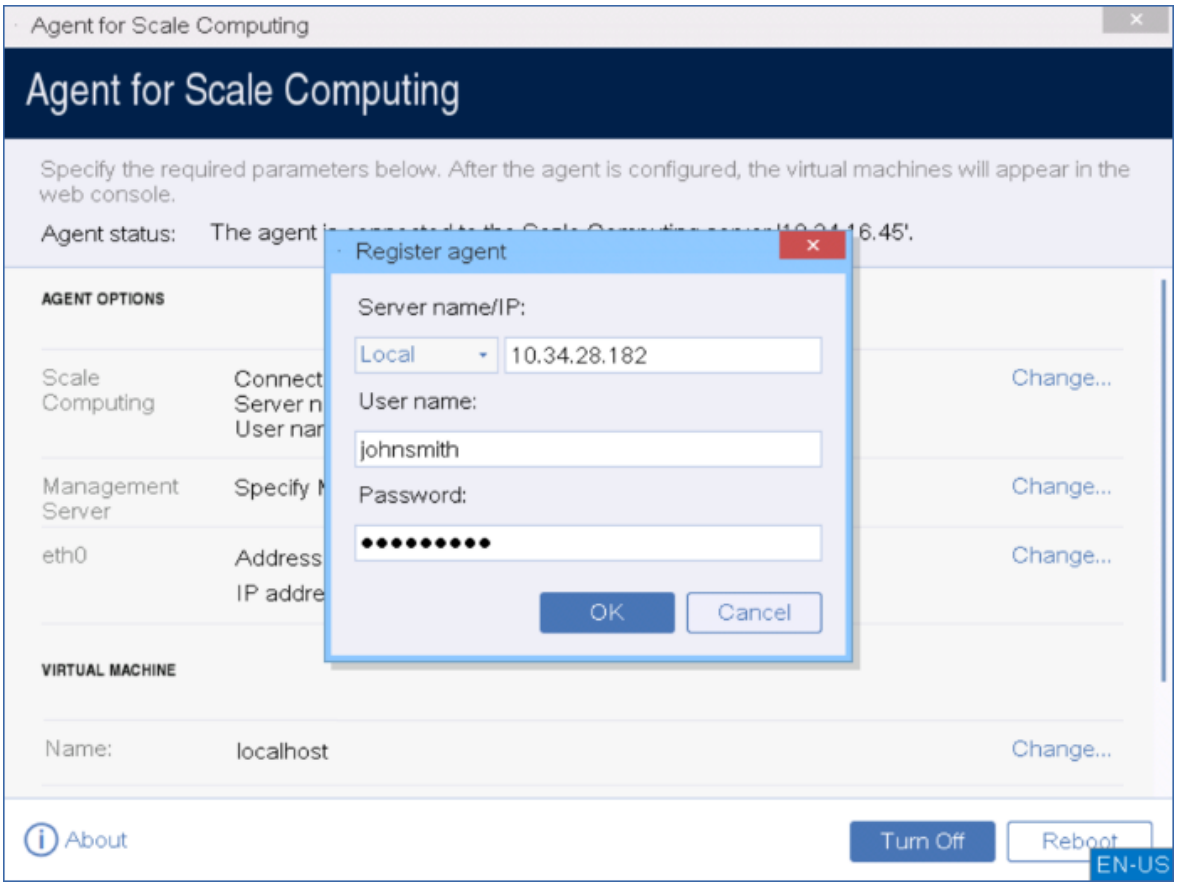


4. Scale Computing HC3 クラスターのアドレスと資格情報を指定します。
   - クラスターの DNS 名または IP アドレス。
   - **[ユーザー名]** と **[パスワード]** のフィールドに、適切なロールが割り当てられた Scale Computing HC3 アカウントの資格情報を入力します。

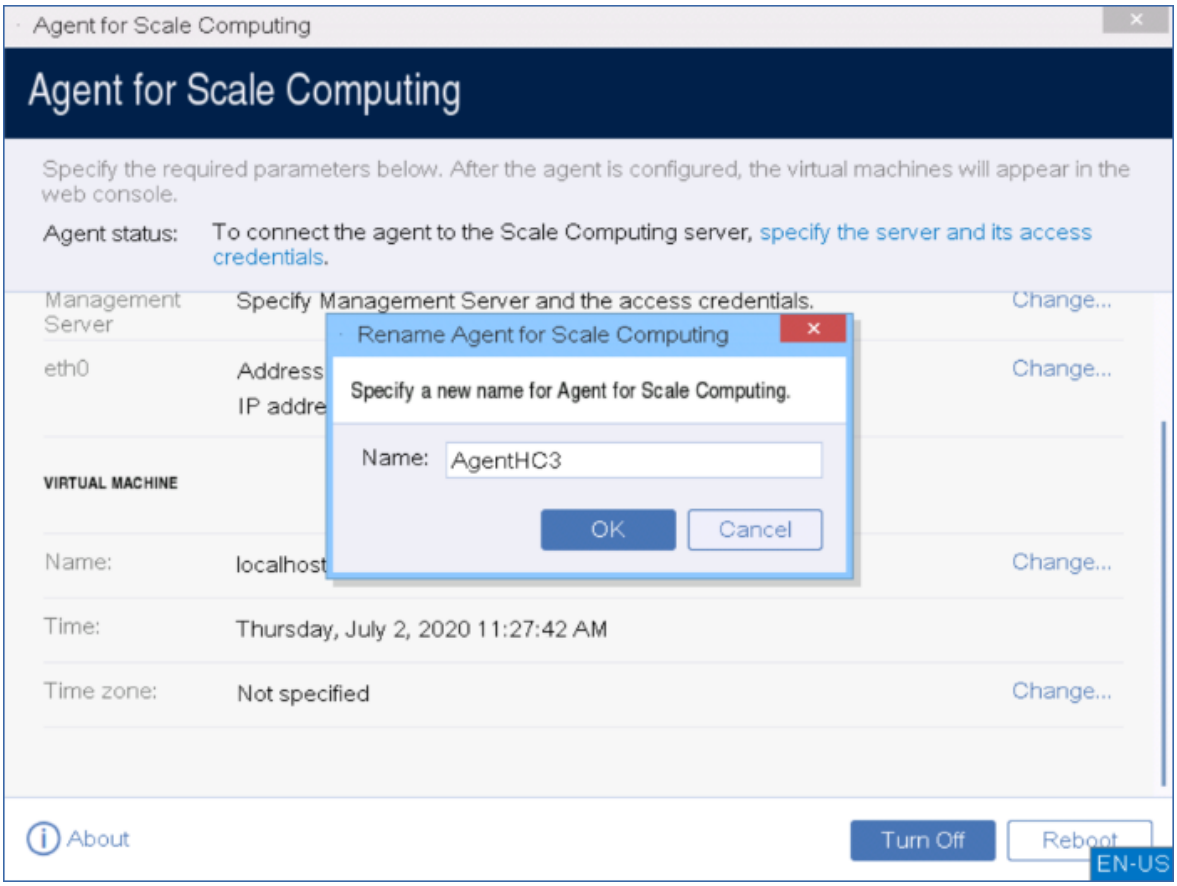
   [接続の確認] をクリックすると、このアクセス認証情報が正しいかどうかを確認できます。



5. Cyber Protect管理サーバーのアドレスとアクセス用の資格情報を指定します。



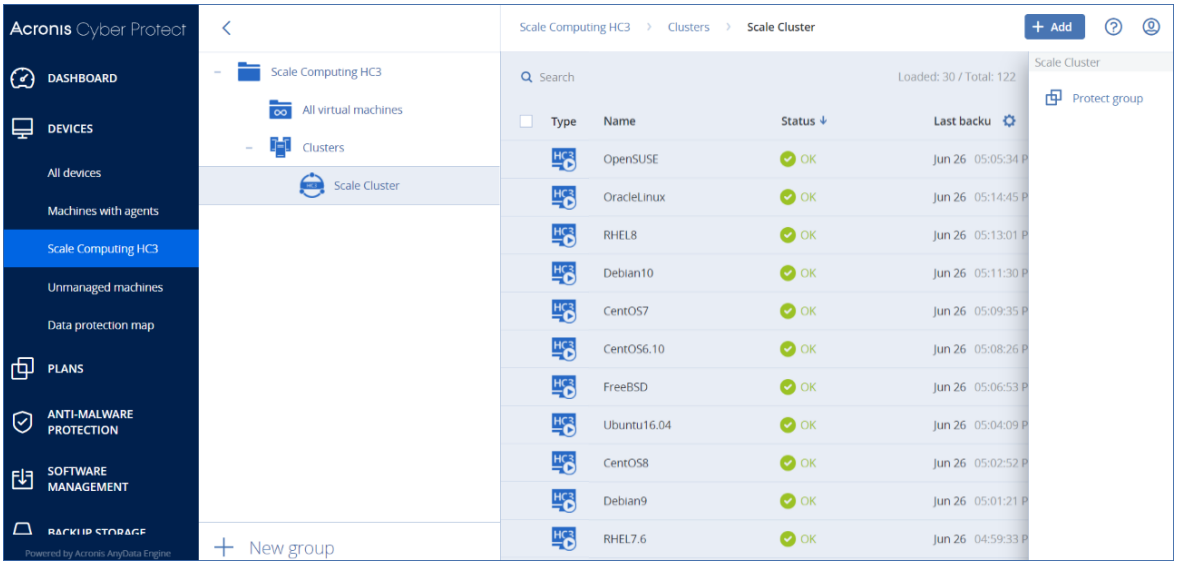
6. （オプション）エージェントの名前を指定します。この名前は Cyber Protect ウェブ コンソールに表示されます。



7. （オプション）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。

Scale Computing HC3 クラスター内の仮想マシンを保護する

1. Cyber Protect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. 任意のマシンを選択し、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 仮想マシンでの処理と仮想アプライアンスの配置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
仮想アプライアンスデプロイ	VM 作成/編集

グループポリシーによるエージェントの配置

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コンピュータ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

エージェントの配置を設定する前に、次の項目を確認します。

- 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 **Domain Admins** グループのメンバーである。

- **Windows のセットアッププログラムにインストールするすべてのエージェント**がダウンロードされている。ダウンロードリンクは ウェブ コンソールの**デバイスの追加**ページにあります。

手順1:登録トークンの生成

登録トークンは、Cyber Protect ウェブ コンソールにログインやパスワードを保存せずに、ユーザーの個人情報をプログラムの設定に渡します。これにより、自分のアカウントの下でマシンを何台でも登録できます。トークンの有効期間はセキュリティを強化するために制限されています。

登録トークンを生成するには

1. マシンが割り当てられるアカウントの資格情報を使用して Cyber Protect ウェブ コンソールにサインインします。
2. **[すべてのデバイス]** > **[追加]**をクリックします。
3. 下にスクロールして **[登録トークン]** を表示し、**[生成]** をクリックします。
4. トークンの有効期間を指定し、**[トークンを生成]** をクリックします。
5. トークンをコピーするか、書き留めます。その他の用途のために必要であれば、トークンを確実に保存してください。
   [アクティブなトークンを管理] をクリックして、生成済みのトークンを表示および管理できます。セキュリティの観点から、この表では完全なトークン値が表示されないことにご注意ください。

手順2:.mstトランスフォームファイルの作成とインストールパッケージの抽出

1. ドメインの任意のコンピュータで、管理者としてログオンします。
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. セットアッププログラムを開始します。
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. .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ます。管理サーバーへの接続方法を指定する際、**[登録トークンを使用する]** を選択してから、生成したトークンを入力します。
6. **[続行]** をクリックします。
7. **ファイルを保存する**には、作成したフォルダへのパスを指定します。
8. **[生成]** をクリックします。

これにより、.mst トランスフォームファイルが生成され、.mst および.cabインストールパッケージが作成したフォルダに抽出されます。

手順 3:グループ ポリシー オブジェクトの設定

1. ドメイン管理者としてドメインコントローラにログオンします。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）へのエージェントの配置を計画している場合は、その組織単位（OU）がドメイン内に存在していることを確認します。それ以外の場合は、この手順をスキップします。

3. **[スタート]** メニューで、**[管理ツール]** をポイントしてから、**[Active Directory ユーザーとコンピュータ]**（Windows Server 2003）または **[グループポリシーの管理]**（Windows Server 2008以降）をクリックします。
4. 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。

   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. 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。
6. **[Window エージェント]** グループポリシーオブジェクトを編集するために、次の手順に従って開きます。
   - Windows Server 2003 では、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。
   - Windows Server 2008 以降では、**[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。
7. 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。
8. 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。

   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。
9. **[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。
10. 前に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。
11. **[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。
12. **[変更]** タブで、**[追加]** をクリックして、前に作成した .mst トランスフォームを選択します。
13. **[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。

既存の仮想アプライアンスをアップデートする

オンプレミスデプロイ

15.24426（2020年9月リリース）より前のバージョンの仮想アプライアンス（エージェント for VMwareまたはScale Computing HC3エージェント）をアップデートするには、「"エージェントのアップデート"（177ページ）」に記載されている手順に従います。

バージョン15.24426以降の仮想アプライアンスをアップデートするには

1. http://kb.acronis.com/latestに記載されているアップデートパッケージをダウンロードします。
2. 以下に示す管理サーバーのマシンのディレクトリに`tar.bz`ファイルを保存します。

- Windows:`C:\Program Files\Acronis\VirtualAppliances\va-updates`
- Linux: `/usr/lib/Acronis/VirtualAppliances/va-updates`

3. Cyber Protectウェブコンソールで、**[設定]** > **[エージェント]** をクリックします。
   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。古い仮想アプライアンスがインストールされているマシンには、オレンジ色の感嘆符が表示されます。
4. アップデートする仮想アプライアンスがあるマシンを選択します。マシンはオンラインである必要があります。
5. **[エージェントのアップデート]** をクリックします。
6. デプロイエージェントを選択します。
7. ターゲットマシンの管理者権限を持つアカウントの資格情報を指定します。
8. エージェントが管理サーバーへのアクセスに使用する名前または IP アドレスを選択します。
   デフォルトでは、サーバー名が選択されています。DNSサーバーが名前からIPアドレスを解決できない場合（仮想アプライアンスの登録中にエラーが発生します）、この設定の変更が必要な場合があります。

[アクティビティ] タブにアップデートの進行状況が表示されます。

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。

クラウドデプロイ

クラウド配置で仮想アプライアンスをアップデートする方法の詳細については、クラウドドキュメントのエージェントのアップデートを参照してください。

エージェントのアップデート

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、https://support.microsoft.com/help/2999226/update-for-universal-c-runtime-in-windowsから入手できます。

エージェントのバージョンを確認するには、コンピュータを選択して、**[詳細]** をクリックします。

Cyber Protectウェブコンソールを使用するか、実行可能な任意の方法で再度インストールすることで、エージェントをアップデートできます。複数のエージェントを同時にアップデートするには、次の手順を使用します。

Cyber Protectウェブ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. （オンプレミスデプロイの場合のみ）管理サーバーをアップデートします。
2. （オンプレミスデプロイの場合のみ）管理サーバーがインストールされているマシンにインストールパッケージがあることを確認してください。正確な手順については、「Windows を実行するマシンの追加」の「インストールパッケージ」を参照してください。
3. Cyber Protectウェブコンソールで、**[設定]** > **[エージェント]** をクリックします。
   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。
4. 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。
5. **[エージェントのアップデート]** をクリックします。
6. デプロイエージェントを選択します。
7. ターゲットマシンの管理者権限を持つアカウントの資格情報を指定します。
8. エージェントが管理サーバーへのアクセスに使用するサーバー名またはIPアドレスを選択します。
   デフォルトでは、サーバー名が選択されています。もし管理サーバーに複数のネットワークインターフェースが存在する場合や、エージェントの登録失敗の原因となり得るDNSの問題がある場合は、IPアドレスを選択する必要があります。
9. （オンプレミスデプロイの場合のみ）**[アクティビティ]** タブにアップデートの進行状況が表示されます。

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。

マシンでCyber Protect定義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。
2. Cyber Protect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、**[Cyber Protectの定義]** 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。

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。

Acronis Cyber Protect 15にアップグレードする

次の方法で、以前の製品をAcronis Cyber Protect 15にアップグレードできます。

- 以前の製品をアンインストールすることなく、直接実行する。
  このオプションは、Acronis Backup 12.5 Update 5（ビルド16180）以降でのみ利用可能です。
- 以前の製品をアンインストールして、新たにAcronis Cyber Protect 15をインストールする。
  このオプションは、すべての対象製品で利用可能です。これらの製品の詳細については、こちらのナレッジベースの記事を参照してください。

注意
アップグレードの前にシステムをバックアップすることをお勧めします。バックアップしておくことで、アップグレードが失敗した場合に、元の構成にロールバックできます。

アップグレードを開始するには、インストーラを起動して、画面の指示に従います。

Acronis Cyber Protect 15 の管理サーバーは下位互換性があり、バージョン 12.5 のエージェントをサポートしています。ただし、このエージェントは Cyber Protect 機能はサポートしません。

エージェントをアップグレードしても、既存のバックアップセットとその設定に影響はありません。

製品のアンインストール

コンピュータから個別の製品コンポーネントを削除する場合は、セットアッププログラムを実行し、製品の修正を選択して、削除するコンポーネントの選択をオフにします。セットアッププログラムへのリンクは、**[ダウンロード]** ページにあります（右上の **[ダウンロード]** でアカウントアイコンをクリック）。

すべての製品コンポーネントをコンピュータから削除する場合は、以下の手順に従います。

警告
オンプレミスデプロイではコンポーネントをアンインストールする際には十分に注意してください。

管理サーバーを間違ってアンインストールすると、Cyber Protectウェブ コンソールを使用できなくなり、アンインストールされた管理サーバーで登録されていたすべてのマシンのバックアップも復元もできなくなります。

Windowsの場合

1. 管理者としてログインします。
2. **[コントロールパネル]** に移動し、**[プログラムと機能]**（Windows XPでは **[プログラムの追加と削除]**）＞ **[Acronis Cyber Protect]** ＞ **[アンインストール]** の順に選択します。
3. （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。
   エージェントをアンインストールし、再インストールする予定の場合は、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オンにする場合、マシンはCyber Protectウェブコンソールで複製され、古いマシンのバックアップは新しいマシンに関連付けられないことがあります。
4. 操作を確定します。

Linuxの場合

1. 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。
   エージェントをアンインストールし、再インストールする予定の場合は、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オンにする場合、マシンはCyber Protectウェブコンソールで複製され、古いマシンのバックアップは新しいマシンに関連付けられないことがあります。
3. 操作を確定します。

macOSの場合

1. インストールファイル（.dmg）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ション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。

エージェント for VMware（仮想アプライアンス）の削除

1. vSphere クライアントを起動し、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は、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、次の手順を実行します。
   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。**[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。
   c. **[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。

Cyber Protectウェブ コンソールからマシンを削除する

エージェントをアンインストールすると、管理サーバーから登録が解除されます。またエージェントがインストールされたマシンは、Cyber Protectウェブ コンソールから自動的に削除されます。

ただし、この操作中に管理サーバーへの接続が失われた場合（たとえばネットワークの問題など）、エージェントがアンインストールされていても、そのマシンがウェブ コンソールに表示される場合があります。この場合、ウェブ コンソールからマシンを手動で削除する必要があります。

ウェブ コンソールからマシンを手動で削除するには

1. Cyber Protectウェブコンソールで、**[設定]** > **[エージェント]** に移動します。
2. 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. **[削除]** をクリックします。

Cyber Protect ウェブ コンソールへのアクセス

Cyber Protect ウェブ コンソールにアクセスするには、ログインページのアドレスを Web ブラウザのアドレスバーに入力し、以下のようにしてサインインします。

オンプレミスデプロイ

ログインページのアドレスは、Management Serverがインストールされているコンピュータのアドレスまたは名前です。

HTTP と HTTPS の両方のプロトコルが同じ TCP ポートでサポートされています。これは、管理サーバーのインストールの際に設定できます。デフォルトのポートは 9877 です。

管理サーバーを設定して、HTTP 経由での Cyber Protect ウェブ コンソールへのアクセスを禁止し、サードパーティ SSL 証明書を使用することができます。

Windowsの場合

管理サーバーが Windows にインストールされている場合、Cyber Protect ウェブ コンソールにサインインするには 2 つの方法があります。

- 現在のWindowsユーザーとしてサインインするには **[サインイン]** をクリックします。
  これは、Management Serverがインストールされているのと同じコンピュータからサインインする最も簡単な方法です。
  Management Serverが別のコンピュータにインストールされている場合、以下の条件を満たすときにこの方法が機能します。
  - サインインするコンピュータが、Management Serverと同じActive Directoryドメインにある。
  - ドメインユーザーとしてログオンしている。

  統合Windows認証を実行するようにWebブラウザを設定することをお勧めします。この設定を行っていない場合は、ブラウザでユーザー名とパスワードの入力を求められます。ただし、このオプションは無効にできます。
- **[ユーザー名とパスワードを入力]** をクリックして、ユーザー名とパスワードを指定します。

いずれの場合も、アカウントがManagement Serverの管理者の一覧に含まれている必要があります。デフォルトでは、このリストには、Management Serverを実行するコンピュータの**アドミニストレータ**グループが含まれています。詳細については、「管理者と部署」を参照してください。

現在のWindowsユーザーオプションとしてのサインインを無効にする場合

1. 管理サーバーがインストールされているマシンで、`C:\Program Files\Acronis\AccountServer` に移動します。
2. 編集用にファイル**account_server.json**を開きます。
3. 「connectiors」セクションに移動し、次の行を削除します:

```
{
"type":"sspi",
"name": "1 Windows Integrated Logon",
```

```
"id": "sspi",
"config": {}
},
```

4. 「checksum」セクションに移動し、「sum」値を次のように変更します。

```
"sum":"FWY/8e8C6c0AgNl0BfCrjgT4v2uj7RQNmaIYbwbjpzU="
```

5. 「信頼できる認証局が発行した証明書の使用」の説明にあるように、AcronisService Manager サービスを再起動します。

Linuxの場合

管理サーバーが Linux にインストールされている場合は、管理サーバーの管理者のリストに含まれるアカウントのユーザー名とパスワードを指定します。デフォルトでは、このリストには管理サーバーを実行しているマシンの **root** ユーザーのみが含まれます。詳細については、「管理者と部署」を参照してください。

クラウドデプロイ

ログインページのアドレスはhttps://backup.acronis.com/です。ユーザー名とパスワードは Acronis アカウントと同じです。

アカウントがバックアップ管理者によって作成された場合は、アクティブ化メールのリンクをクリックして、アカウントをアクティブ化し、パスワードを設定する必要があります。

言語の変更

ログインして右上隅のアカウントアイコンをクリックすると、Web インターフェースの言語を変更できます。

統合Windows認証のためのWebブラウザの設定

統合 Windows 認証は、Windows を実行しているマシンまたはサポートされているブラウザから Cyber Protect ウェブ コンソールにアクセスする場合に使用することができます。

統合Windows認証を実行するようにWebブラウザを設定することをお勧めします。この設定を行っていない場合は、ブラウザでユーザー名とパスワードの入力を求められます。

Internet Explorer、Microsoft Edge、Opera、およびGoogle Chromeの設定

ブラウザを実行しているマシンがManagement Serverを実行しているマシンと同じActive Directoryドメイン内にある場合は、コンソールのログインページを**ローカルイントラネット**サイトのリストに追加します。

それ以外の場合は、コンソールのログインページを **[信頼済みサイト]** リストに追加し、**[現在のユーザー名とパスワードで自動的にログオンする]** 設定を有効にします。

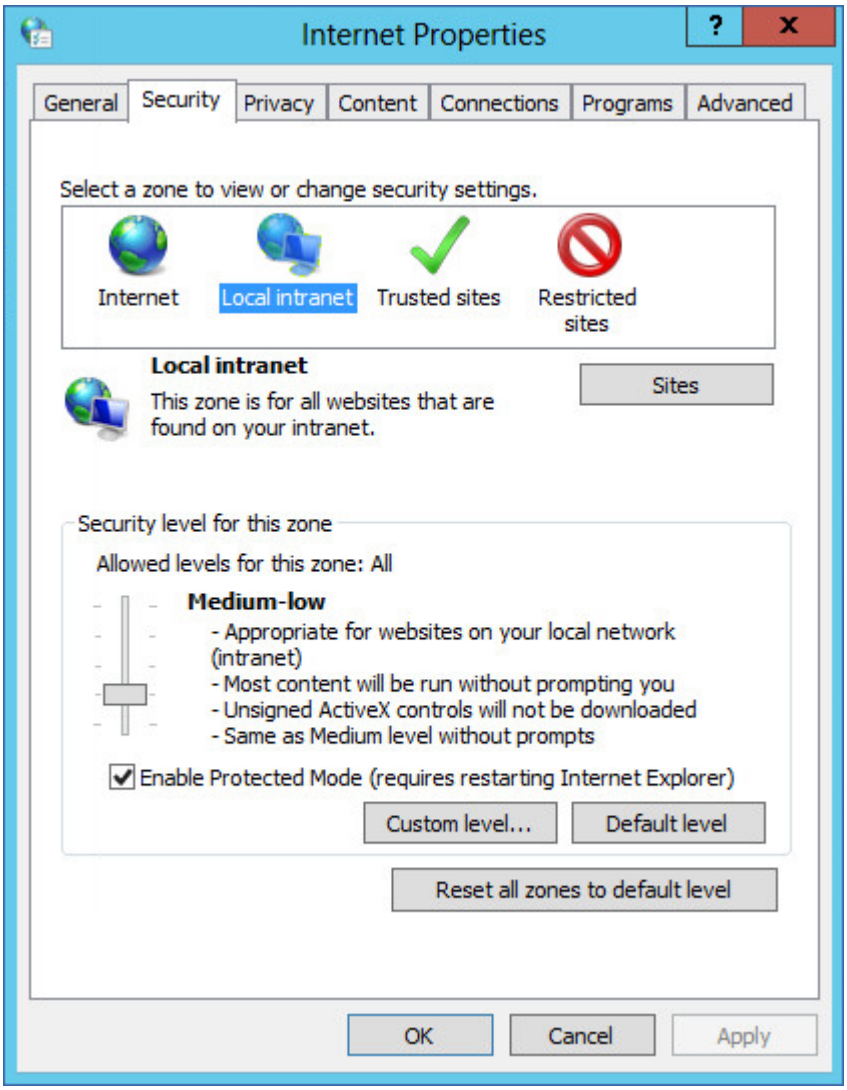
詳細な手順については、このセクションの後半で説明します。これらのブラウザはWindowsの設定を使用するため、Active Directoryドメイン内のグループポリシーを使用してこれらのブラウザを設定することもできます。

Mozilla Firefoxの設定

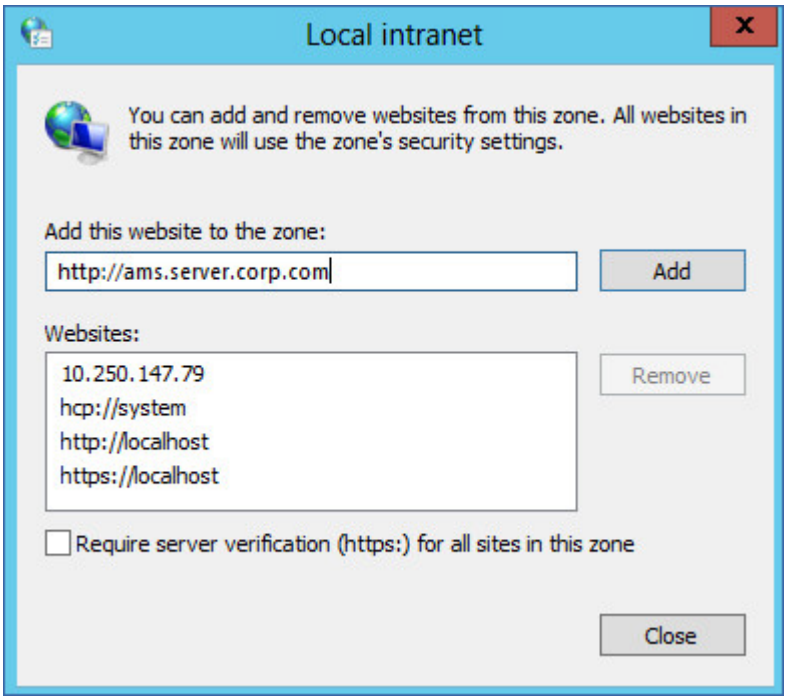
1. FirefoxでURL `about:config`に移動し、**[危険性を承知の上で使用する]** ボタンをクリックします。
2. **[検索]** フィールドで `network.negotiate-auth.trusted-uris` 設定を検索します。
3. この設定をダブルクリックし、Cyber Protect ウェブ コンソールのログインページのアドレスを入力します。
4. `network.automatic-ntlm-auth.trusted-uris`設定について手順2～3を繰り返します。
5. `about:config`ウィンドウを閉じます。

ローカルイントラネットサイトのリストへのコンソールの追加

1. **[コントロールパネル]** > **[インターネットオプション]** に移動します。
2. **[セキュリティ]** タブで、**[ローカルイントラネット]** を選択します。



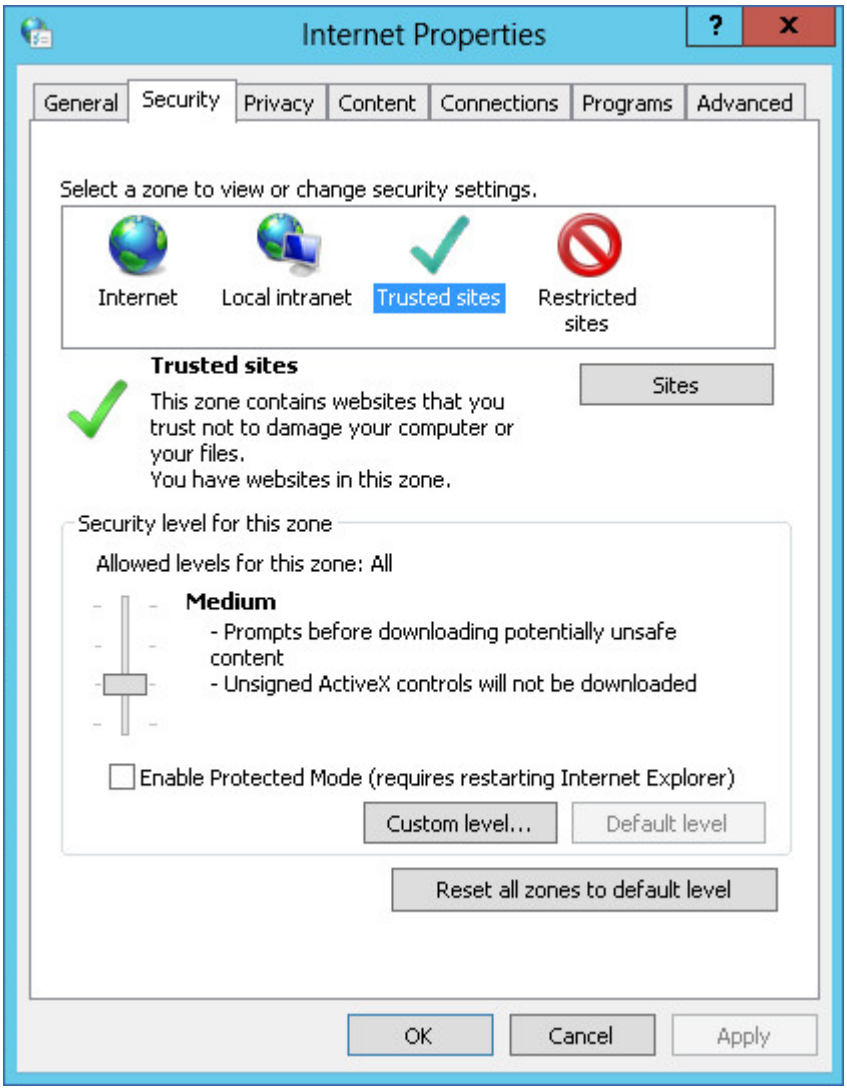
3. [**サイト**] をクリックします。
4. [**この Web サイトをゾーンに追加する**] で、Cyber Protect ウェブ コンソールのログインページのアドレスを入力して、[**追加**] をクリックします。



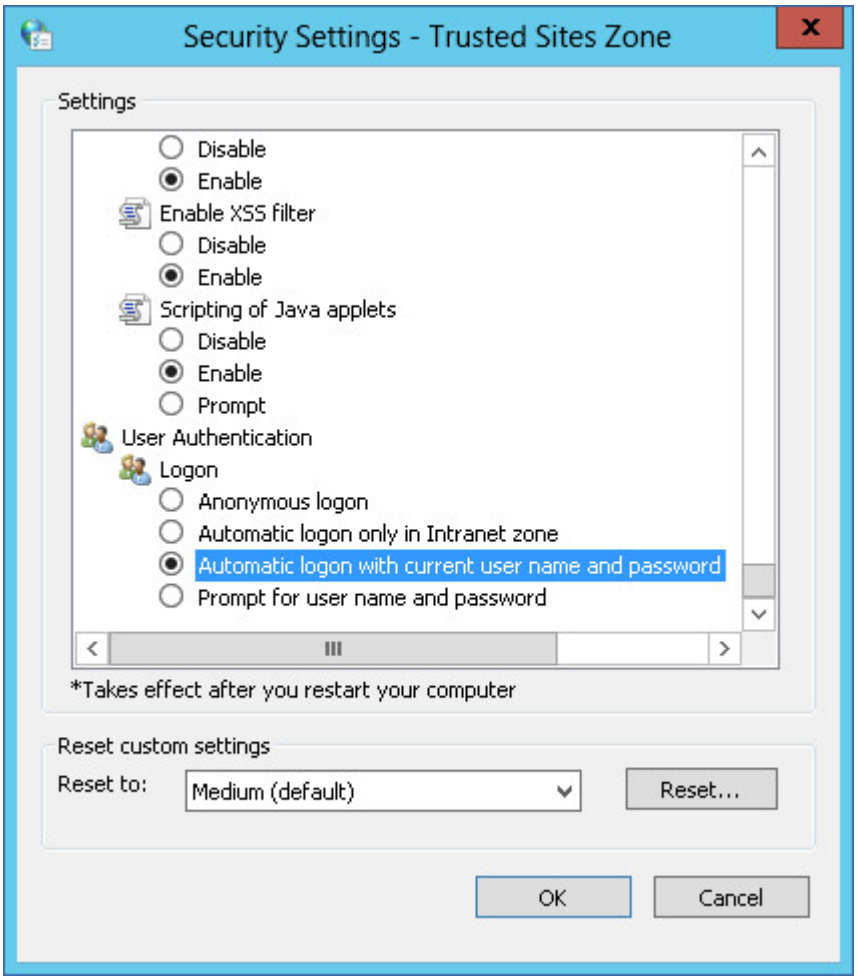
5. [**閉じる**] をクリックします。
6. [**OK**] をクリックします。

信頼されたサイトのリストへのコンソールの追加

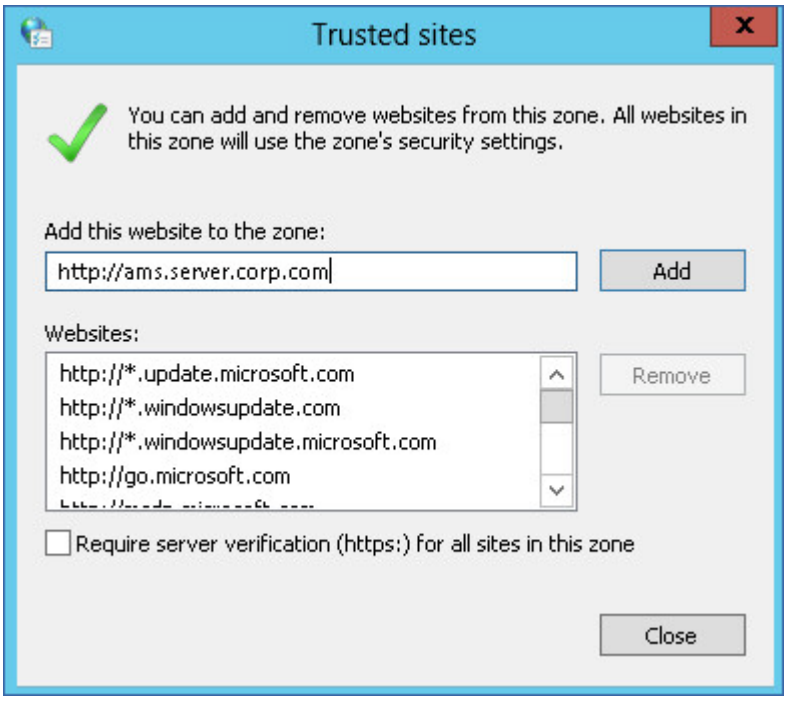
1. [**コントロールパネル**] > [**インターネットオプション**] に移動します。
2. [**セキュリティ**] タブで、[**信頼済みサイト**] を選択して、[**レベルのカスタマイズ**] をクリックします。



3. [**ログオン**] の下の [**現在のユーザー名とパスワードで自動的にログオンする**] を選択して、[**OK**] をクリックします。



4. [**セキュリティ**] タブで、[**信頼済みサイト**] を選択したまま、[**サイト**] をクリックします。
5. [**この Web サイトをゾーンに追加する**] で、Cyber Protect ウェブ コンソールのログインページのアドレスを入力して、[**追加**] をクリックします。



6. **[閉じる]** をクリックします。
7. **[OK]** をクリックします。

HTTPS接続によるWebコンソールへのログインのみを許可する

HTTPS接続のみを許可してします。セキュリティ上の理由で、ユーザーがHTTPプロトコル経由でCyber ProtectWebコンソールにアクセスできないようにします。

HTTPS接続によるWebコンソールへのログインのみを許可するには

1. 管理サーバーを実行しているマシンのテキストエディタで、以下の設定ファイルを開きます。
   - Windowsの場合: `%ProgramData%\Acronis\ApiGateway\api_gateway.json`
   - Linuxの場合: `/var/lib/Acronis/ApiGateway/api_gateway.json`
2. 次のセクションを見つけます。

```
"tls": {
  "auto_redirect" : false,
  "cert_file": "cert.pem",
```

3. `"auto_redirect"`の値を`false`から`true`に変更します。

   `"auto_redirect"`の行がない場合は、手動で追加してください。

```
"auto_redirect": true,
```

4. `api_gateway.json` ファイルを保存します。

重要
設定ファイル内のカンマ、括弧、引用符を誤って削除しないように注意してください。

5. 以下の説明にあるように、Acronis Service Manager Serviceを再起動します。

WindowsでAcronis Service Manager Serviceを再起動するには

Windowsの場合

1. **[スタート]** メニューで、**[ファイル名を指定して実行]** をクリックし、「**cmd**」と入力します。
2. **[OK]** をクリックします。
3. 次のコマンドを実行します。

```
net stop asm
net start asm
```

Linuxの場合

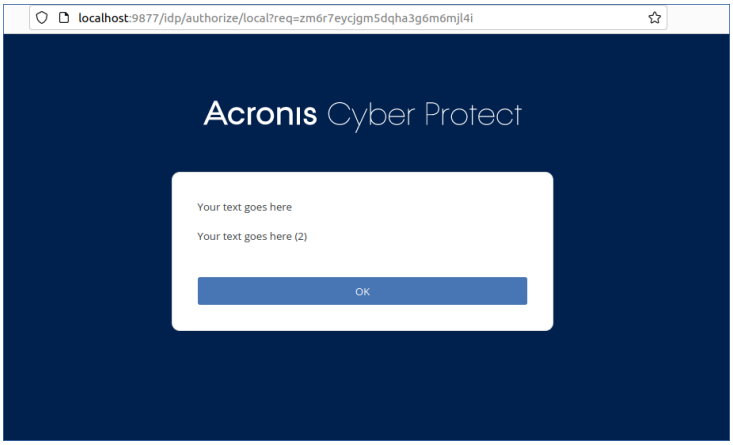
1. **ターミナル**を開きます。
2. 任意のディレクトリで次のコマンドを実行します。

```
sudo service acronis_asm restart
```

Webコンソールにカスタムメッセージを追加します

Cyber Protect Webコンソールにカスタムメッセージを追加できます。

このメッセージは、毎回ログインを試行する前に表示されます。



前提条件

管理サーバーが実行されているマシンに保護計画が適用されている場合、自己防御機能が無効になっていることを確認してください。また構成ファイルを後から編集することはできません。

自己防御機能を有効化/無効化する方法については、"自己防御機能"（506ページ）を参照してください。

Webコンソールにカスタムメッセージを追加するには

Windowsの場合

1. 管理サーバーがインストールされたマシンにログインします。アカウントに管理者権限が必要です。
2. %Program Files%\Acronis\AccountServerに移動します。
3. （オプション） AccountServer.zipファイルのバックアップコピーを作成します。
4. %Program Files%\Acronis\AccountServer\AccountServer.zip\static\localeに移動します。
5. Cyber Protect Webコンソールで使用している言語に対応するJSONファイルを展開してください。例えば、英語を使う場合は、en.jsonファイルを展開します。

   注意
   ファイルを編集するには、単にダブルクリックでファイルを開くのではなく、ファイルを展開する必要があります。

6. 展開されたファイルを編集用に開きます。メモ帳やNotepad++などのテキストエディタを使用します。
7. 次の行に移動し、最後にカンマを追加します:

   ```
   "APP_LOGINFORM_LOGIN_BUTTON":"Log in",
   ```

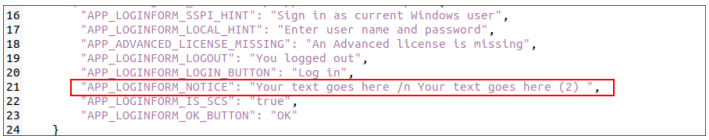
8. 「APP_LOGINFORM_LOGIN_BUTTON」:「**ログイン**」行の下に、以下の行を追加します。

   ```
   "APP_LOGINFORM_NOTICE": "<Type your custom message here>",
   ```

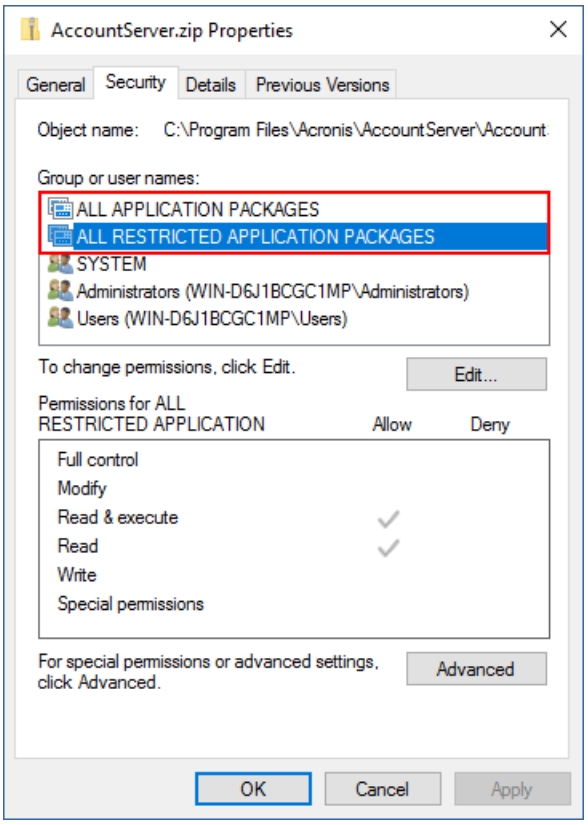
   ```
   "APP_LOGINFORM_IS_SCS": "true",
   ```

   ```
   "APP_LOGINFORM_OK_BUTTON":"OK"
   ```

   例:

9. 変更を保存したら、編集したJSONファイルを%Program Files%\Acronis\AccountServer\AccountServer.zip\static\localeディレクトリに配置します。
10. AccountServer.zipファイルを右クリックして、[**プロパティ**] > [**セキュリティ**] に移動して、**すべてのアプリケーションパッケージ**と**すべての制限付きアプリケーションパッケージ**が、**読み取り**と**読み取りと実行**の権限を付与された**グループまたはユーザー名**で追加されているか確認します。



注意

すべての制限付きアプリケーションパッケージが存在しない場合は、そのリストから**すべてのアプリケーションパッケージ**を削除し、再度追加します。**すべてのアプリケーションパッケージ**を追加すると、自動的に**すべての制限付きアプリケーションパッケージ**が表示されます。

11. **Acronis Service Manager Service**を再起動します（"Acronis Service Manager Serviceを再起動するには"（196ページ）を参照）。

Linuxの場合

1. 管理サーバーがインストールされたマシンにログインします。
2. `/usr/lib/Acronis/AccountServer`に移動します。
3. `AccountServer.zip`ファイルに対する書き込み許可があることを確認します。
4. （オプション） `AccountServer.zip`ファイルのバックアップコピーを作成します。
5. `/usr/lib/Acronis/AccountServer/static/locale`に移動します。
6. Cyber Protect Webコンソールで使用している言語に対応するJSONファイルを展開してください。例えば、英語を使う場合は、`en.json`ファイルを展開します。
7. 展開されたファイルを編集用に開きます。
8. 次の行に移動し、最後にカンマを追加します:

```
"APP_LOGINFORM_LOGIN_BUTTON":"Log in",
```

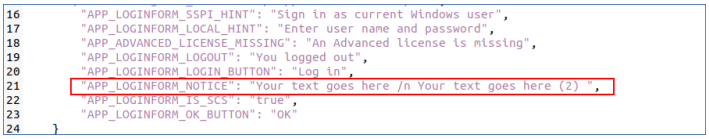
9. 「`APP_LOGINFORM_LOGIN_BUTTON`」:「**ログイン**」行の下に、以下の行を追加します。

```
"APP_LOGINFORM_NOTICE": "<Type your custom message here>",
```

```
"APP_LOGINFORM_IS_SCS": "true",
```

```
"APP_LOGINFORM_OK_BUTTON":"OK"
```

たとえば、次のようになります。



10. 変更を保存したら、編集したJSONファイルを`/usr/lib/Acronis/AccountServer/static/locale`に配置します。
11. **Acronis Service Manager Service**を再起動します（"Acronis Service Manager Serviceを再起動するには"（196ページ）を参照）。

SSL証明書の設定

このセクションでは、以下の方法について説明します。

- 管理サーバーによって生成された自己署名SSL（Secure Socket Layer）証明書を使用するプロテクションエージェントを構成する方法。
- 管理サーバーによって生成された自己署名SSL証明書を、信頼できる認証局（GoDaddy、Comodo、GlobalSignなど）によって発行された証明書に変更する方法。これを行うと、管理サーバーが使用する証明書は、任意のマシン上で信頼できるようになります。ブラウザのセキュリティアラートは、HTTPSプロトコルでCyber Protectウェブコンソールにログインしている場合は表示されません。

オプションで、すべてのユーザーをHTTPSにリダイレクトすることで、HTTP経由でのCyber Protectウェブコンソールへのアクセスを禁止するよう管理サーバーを設定できます。

自己署名証明書の使用

Windowsでのプロテクションエージェントの設定

1. エージェントがインストールされているマシンで、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¥Acronis¥BackupAndRecovery¥Settings¥CurlOptions**
3. **VerifyPeer**の値を**0**に設定します。
4. **VerifyHost**の値が**0**に設定されていることを確認します。
5. Managed Machine Service（MMS）を再起動します。
   a. **[スタート]** メニューで、**[ファイル名を指定して実行]** をクリックし、「**cmd**」と入力します。
   b. **[OK]** をクリックします。
   c. 次のコマンドを実行します。

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

Linuxでのプロテクションエージェントの設定

1. エージェントがインストールされているマシンで、編集用にファイル**/etc/Acronis/BackupAndRecovery.config**を開きます。
2. **CurlOptions**キーに移動し、**VerifyPeer**の値を**0**に設定します。**VerifyHost**の値も**0**に設定されていることを確認します。
3. 編集内容を保存します。
4. 任意のディレクトリで次のコマンドを実行してManaged Machine Service（MMS）を再起動します。

   ```
   sudo service acronis_mms restart
   ```

macOSでのプロテクションエージェントの設定

1. エージェントがインストールされているマシンで、Managed Machine Service（MMS）を停止します。
   a. **[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。
   b. 次のコマンドを実行します。

      ```
      sudo launchctl stop acronis_mms
      ```
2. 編集用にファイル**/Library/Application Support/Acronis/Registry/BackupAndRecovery.config**を開きます。
3. **CurlOptions**キーに移動し、**VerifyPeer**の値を**0**に設定します。**VerifyHost**の値も**0**に設定されていることを確認します。
4. 編集内容を保存します。
5. ターミナルで次のコマンドを実行してManaged Machine Service（MMS）を再起動します。

   ```
   sudo launchctl starts acronis_mms
   ```

信頼できる認証局が発行した証明書の使用

SSL証明書設定を構成するには

1. 次のすべてが用意されていることを確認します。

証明書と鍵ファイルを使用する場合	PFXファイルを使用する場合
証明書ファイル （.pem形式）	PFXファイル
証明書 の秘密鍵を含むファイル（通常は.key形式）	
秘密鍵のパスワード （キーがパスワードで保護されている場合）	PFXファイルのパスワード（ファイルがパスワードで保護されている場合）

2. 管理サーバーを実行するマシンにファイルをコピーします。
3. このマシンで、次の設定ファイルをテキストエディタで開きます。
   - Windowsの場合: `%ProgramData%\Acronis\ApiGateway\api_gateway.json`
   - Linuxの場合: `/var/lib/Acronis/ApiGateway/api_gateway.json`
4. 次のセクションを見つけます。

```
"tls": {
    "cert_file": "cert.pem",
    "key_file": "key.pem",
    "passphrase": "",
```

5. `"cert_file"`行の引用符内に、証明書ファイルまたはPFXファイルへのフルパスを指定します。
   たとえば、次のようになります。

オペレーティングシステム	証明書と鍵の組み合わせを使用する場合	.pfxファイルを使用する場合
Windows （前方のスラッシュに注意）	`"cert_file":"C:/certificate/local-domain.ams.pem"`	`"cert_file":"C:/certificate/local-domain.ams.pfx"`
Linux	`"cert_file": "/home/user/local-domain.ams.pem"`	`"cert_file": "/home/user/local-domain.ams.pfx"`

6. `"key_file"`行の引用符内に、証明書の鍵を含む秘密鍵ファイルまたはPFXファイルへのフルパスを指定します。
   通常、PFXファイルには、証明書とその鍵の両方が含まれています。この場合、`"key_file"`行で、前の手順と同じパスを指定します。
   たとえば、次のようになります。

オペレーティングシステム	証明書と鍵の組み合わせを使用する場合	.pfxファイルを使用する場合
Windows （前方のスラッ	`"key_file":"C:/certificate/private.key"`	`"cert_file":"C:/certificate/local-domain.ams.pfx"`

オペレーティングシステム	証明書と鍵の組み合わせを使用する場合	.pfxファイルを使用する場合
シュに注意）		
Linux	`"key_file": "/home/user/private.key"`	`"cert_file": "/home/user/local-domain.ams.pfx"`

7. （オプション） 秘密鍵またはPFXファイルがパスワードで保護されている場合は、`"passphrase"`行の引用符内にパスワードを指定します。

   例: `"passphrase": "my password"`

   注意

   `api_gateway.json`構成ファイルに、`"passphrase": ""`の行が見つからない場合は、手動で追加してください。

   例:

   ```
   "tls": {
       "cert_file": "cert.pem",
       "key_file": "key.pem",
       "passphrase": "my password",
   }
   ```

8. `api_gateway.json` ファイルを保存します。

   重要

   設定ファイル内のカンマ、括弧、引用符を誤って削除しないように注意してください。

9. 以下の説明にあるように、Acronis Service Manager Serviceを再起動します。

Acronis Service Manager Serviceを再起動するには

Windowsの場合

1. **[スタート]** メニューで、**[ファイル名を指定して実行]** をクリックし、「**cmd**」と入力します。
2. **[OK]** をクリックします。
3. 次のコマンドを実行します。

   ```
   net stop asm
   net start asm
   ```

Linuxの場合

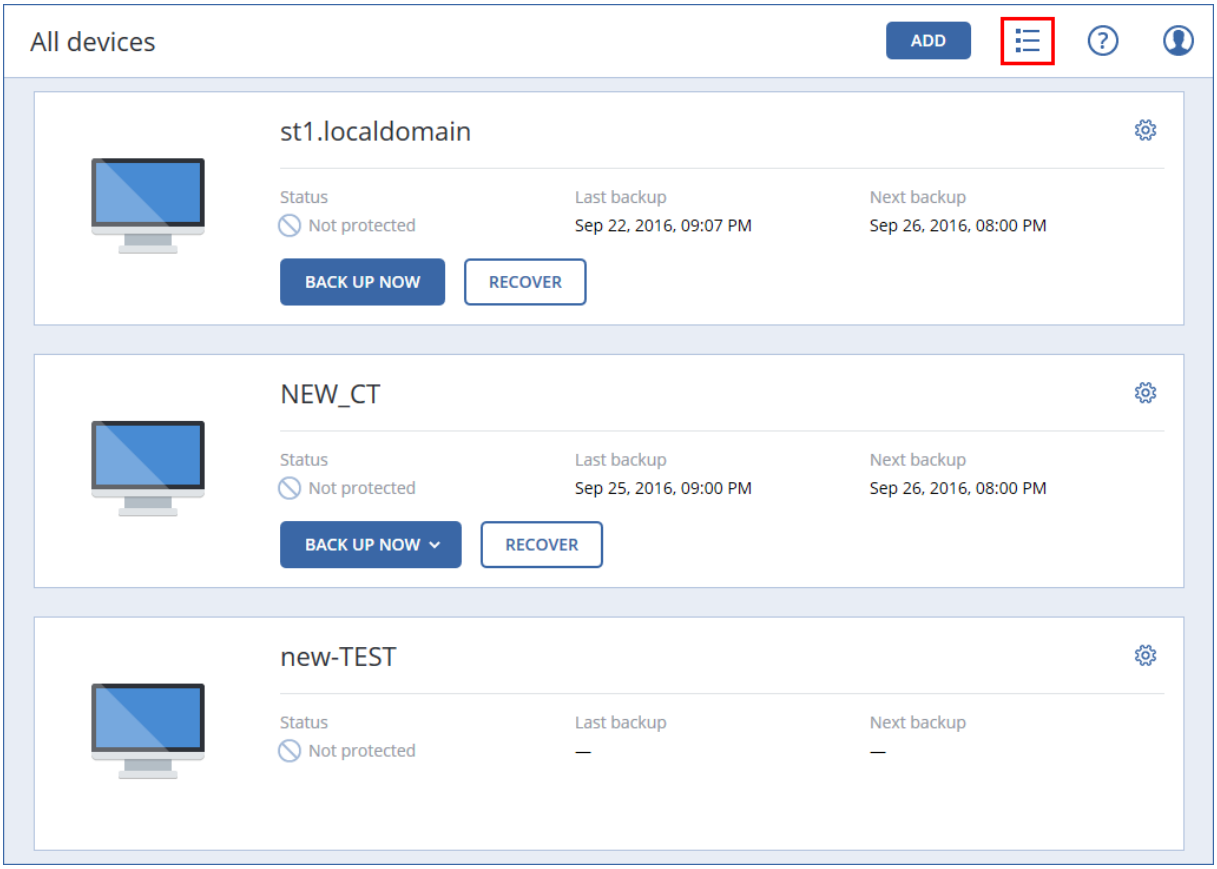
1. **ターミナル**を開きます。
2. 任意のディレクトリで次のコマンドを実行します。

   ```
   sudo service acronis_asm restart
   ```

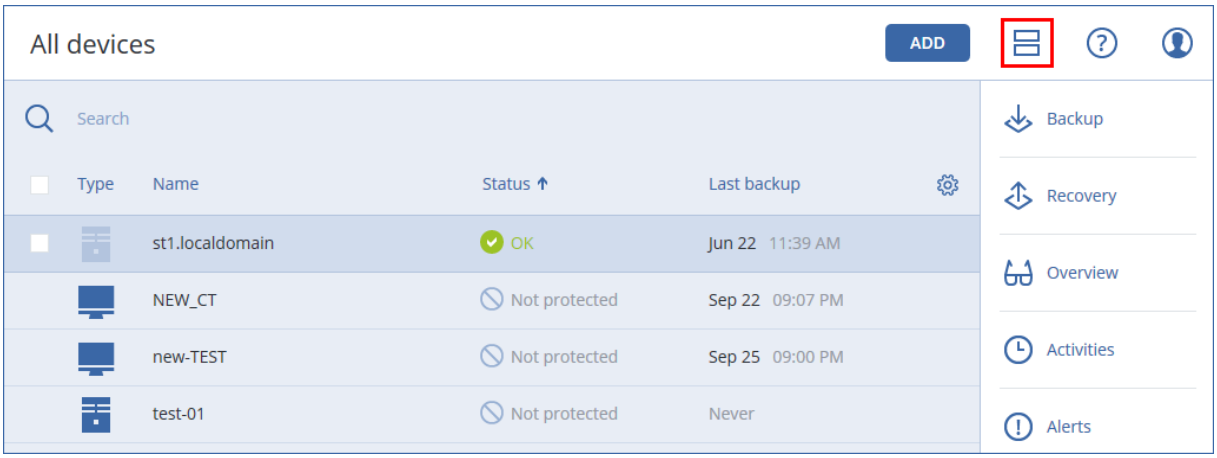
Cyber Protectウェブコンソール表示

Cyber Protectウェブコンソールには、簡易表示と一覧表示の2つの表示形式があります。表示形式を切り替えるには、右上隅にある該当するアイコンをクリックします。

簡易ビューは少数のコンピュータをサポートします。



テーブルビューは、コンピュータ数が多くなると自動的に有効になります。



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。

マシンがオンラインまたはオフラインに切り替わる場合、Cyber Protectウェブ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。

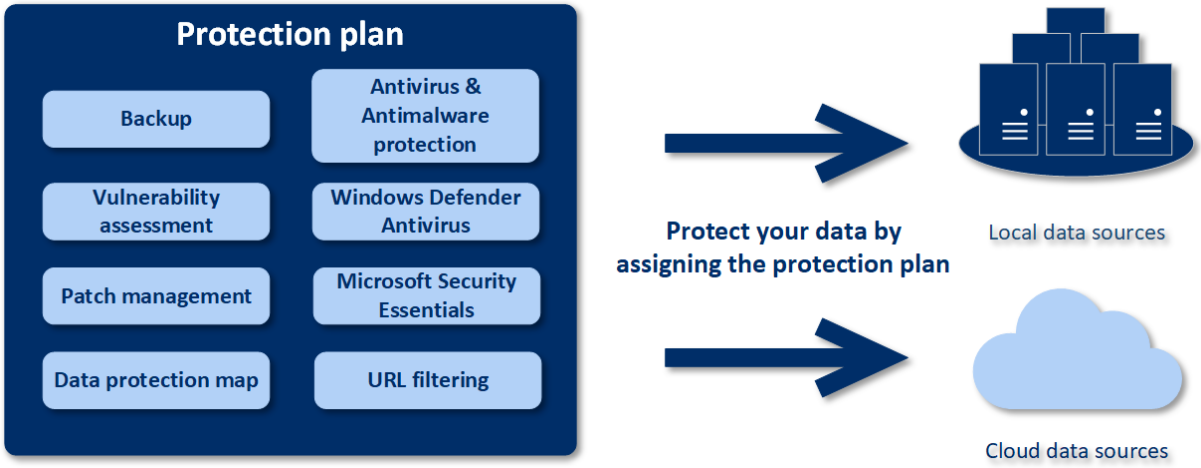
マシンのステータスは1分ごとに確認されます。このマシンにインストールされているエージェントでデータ転送が発生せず、確認に対する応答が5回連続で返ってこない場合、マシンはオフラインとして表示されます。ステータスの確認に対してマシンからの応答があるか、データ転送が開始すると、オンラインステータスに復帰したと表示されます。

保護計画とモジュール

保護計画は、次のようないくつかのデータ保護モジュールを組み合わせたプランです。

- 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。
- ウイルスおよびマルウェア対策保護 - 組み込みのマルウェア対策ソリューションを使用してマシンをチェックできます。
- URLフィルタリング - 悪意あるURLへのアクセスやコンテンツのダウンロード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できます。
- Microsoft Security Essentials - Microsoft Security Essentialsの設定を管理して環境を保護できます。
- 脆弱性診断 - マシンにインストールされたMicrosoft製品と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Microsoft製品と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、検出された脆弱性に対処します。
- 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。

保護計画によって、外部と内部の脅威からデータソースを完全に保護することができます。さまざまなモジュールを有効にするかどうかの切り替えとモジュール設定のセットアップによって、ビジネスの多様な需要を満たす柔軟な計画を作成できます。



保護計画の作成

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。計画を作成するときには、オペレーティングシステムとデバイスの種類（ワークステーション、仮想マシンなど）が確認され、デバイスに適用される計画モジュールのみが表示されます。

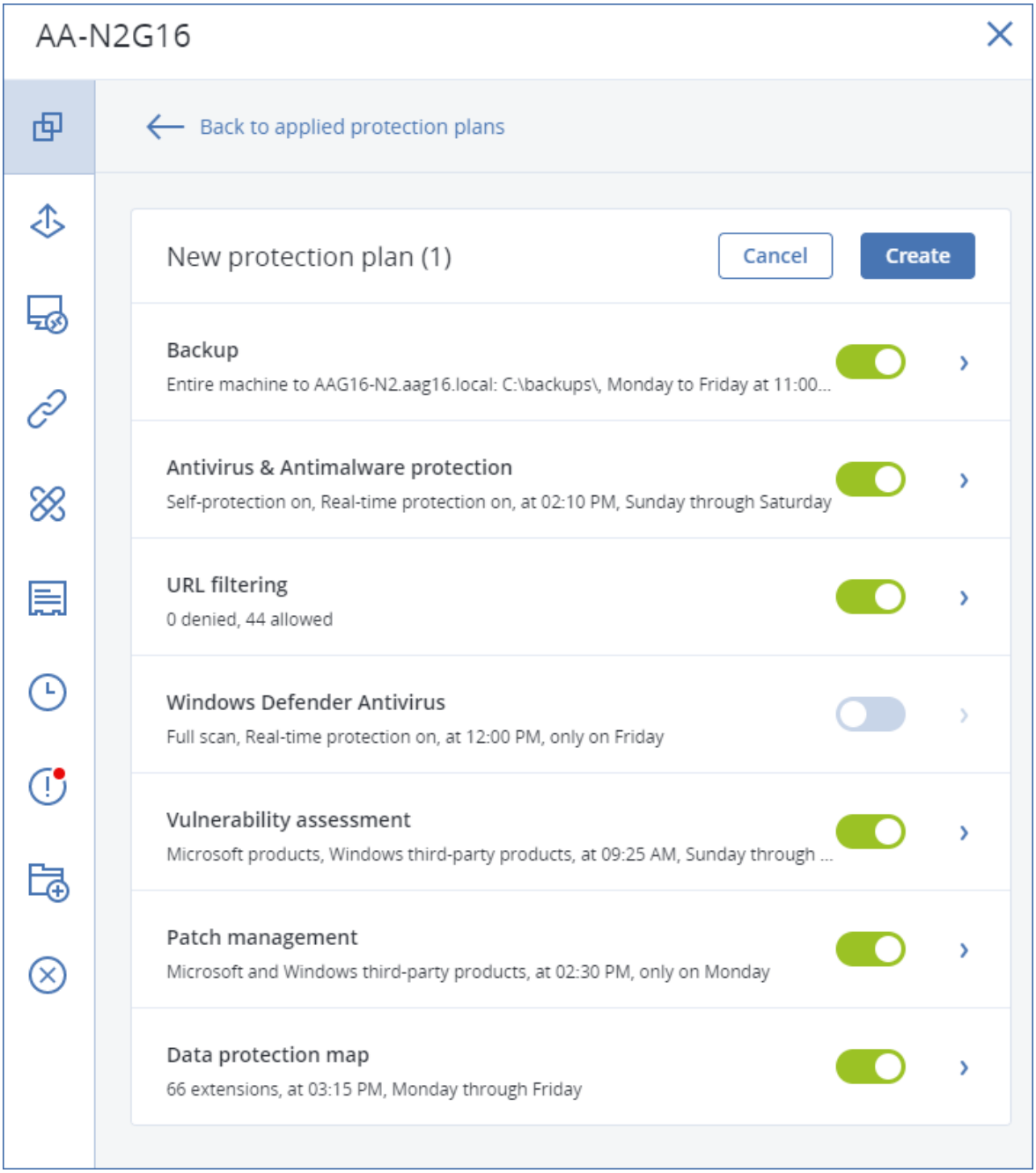
保護計画は2つの方法で作成できます。

- **[デバイス]** セクションから - 保護対象のデバイス（複数可）を選択してから、計画を作成します。
- **[計画]** セクションから - プランを作成してから、適用先のマシンを選択します。

最初の方法を考えてみましょう。

最初の保護計画を作成する手順

1. Cyber Protect ウェブ 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。既定の設定の保護計画が表示されます。



4. （オプション）保護計画名を変更するには、名前の横にある鉛筆アイコンをクリックします。
5. （オプション）保護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クリックします。

6. （オプション）モジュールのパラメータを設定するには、保護計画の対応するセクションをクリックします。
7. 準備ができたら、**[作成]** をクリックします。

バックアップ、ウイルスおよびマルウェア対策保護、脆弱性診断、パッチ管理、およびデータ保護マップの各モジュールは、**[今すぐ実行]** をクリックしてオンデマンドで実行できます。

計画の競合の解決

保護計画は次のいずれかのステータスになります。

- **[アクティブ]** - デバイスに割り当てられ、実行されている計画。
- **[非アクティブ]** - デバイスに割り当てられているが、無効化され、実行されていない計画。

複数の計画のデバイスへの適用

同じデバイスに複数の保護計画を適用できます。そうすることで、同じデバイスに割り当てた異なる保護計画を組み合わせた結果が得られます。たとえば、ウイルス対策およびマルウェア対策保護モジュールだけが有効化された 1 つの計画を適用し、さらにバックアップモジュールだけが含まれる別の計画を適用することができます。保護計画を組み合わせられるのは、モジュールが交錯しない場合のみです。同じモジュールが複数の保護計画で有効な場合は、競合を解決する必要があります。

計画の競合の解決

適用済みの計画と競合する計画

既に計画が適用されている1つ以上のデバイスに新しい計画を作成し、両者に競合が発生している場合、次のいずれかの方法で競合を解決できます。

- 新しい計画を作成して適用し、競合する適用済みの計画をすべて無効化する。
- 新しい計画を作成し、無効化する。

既に計画が適用されている1つ以上のデバイスの計画を編集し、その変更によって競合が発生する場合、次のいずれかの方法で競合を解決できます。

- そのプランの変更を保存し、競合する適用済みの計画をすべて無効化する。
- その計画の変更を保存し、無効化する。

デバイスの計画とグループの計画の競合

あるデバイスがグループ計画割り当て済みのデバイスグループに含まれている状態で、新しい計画をデバイスに割り当てようとすると、システムは次のいずれかの方法で競合を解決するよう求めます。

- そのデバイスをグループから削除してから、新しい計画をデバイスに適用する。
- 新しいプランをグループ全体に適用するか、現在のグループ計画を編集する。

ライセンスの問題

デバイスに割り当てられるクォータは、保護計画の実行、アップデート、または適用に適したものでなければなりません。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。

- 割り当て量に対応していないモジュールを無効にして、保護計画を使用し続けます。
- 手動で割り当て量を変更します。[**デバイス**] > [<**particular_device**>] > [**詳細**] > [**サービスクォータ**] に移動します。次に、既存の量を取り消し、新しく割り当てます。

保護計画を使用した操作

保護計画の作成方法については、「保護計画の作成」を参照してください。

保護計画で実行できるアクション

保護計画で以下のアクションを実行できます。

- 計画名の変更
- モジュールの有効化/無効化、各モジュールの設定の編集
- 計画の有効化/無効化

  無効化された計画は、該当の計画が適用されているデバイスでは実行されません。

  このアクションは、後から同じデバイス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。計画はデバイスから取り消されないため、管理者はプランを再度有効にするだけで保護を回復できます。
- デバイスまたはデバイスグループへの計画の適用
- デバイスで計画を取り消します

  取り消された計画は、デバイスに適用されなくなります。

  このアクションは、同じデバイスを同じ計画で再度すばやく保護する必要のない管理者にとって利便性があります。取り消された計画の保護を回復するには、管理者が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、目的のデバイスに計画を再度適用します。
- 計画のインポート/エクスポート

  注意

  インポートできるのは、AcronisCyber Protect 15で作成した保護計画だけに限られます。それより前のバージョンの製品で作成した保護計画には、AcronisCyber Protect 15との互換性がありません。
- 計画の削除

既存の保護計画を適用するには

1. 保護するマシンを選択します。
2. [**保護**] をクリックします。選択したマシンに保護計画が既にに適用されている場合は、[**計画の追加**] をクリックします。

3. 以前に作成された保護計画が表示されます。
4. 必要な保護を選択し、**[適用]** をクリックします。

保護計画を編集する手順

1. 適用先のすべてのマシンの保護計画を編集する場合は、そのマシンの1つを選択します。それ以外の場合は、保護計画を編集するマシンを選択します。
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. 保護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. 計画の設定内容を変更するには、保護計画パネルの該当するセクションをクリックします。
6. **[変更を保存]** をクリックします。
7. 適用先のすべてのマシンの保護計画を変更する場合は、**[変更をこの保護計画に適用]** をクリックします。それ以外の場合は、**[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。

保護計画をマシンから取り消す手順

1. 保護計画を取り消すマシンを選択します。
2. **[保護]** をクリックします。
3. 複数の保護計画がマシンに適用されている場合は、取り消し対象の保護計画を選択します。
4. 保護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。

保護計画を削除する手順

1. 削除する保護計画が適用されたいずれかのマシンを選択します。
2. **[保護]** をクリックします。
3. 複数の保護計画がマシンに適用されている場合は、削除対象の保護計画を選択します。
4. 保護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。
   すべてのマシンから保護計画が取り消され、Webインターフェースから完全に削除されます。

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。

注意
オンプレミスデプロイで、管理サーバーに存在するのが Standard ライセンスのみの場合、保護計画を複数の物理マシンに適用することはできません。物理マシンごとに独自の保護計画が必要です。

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

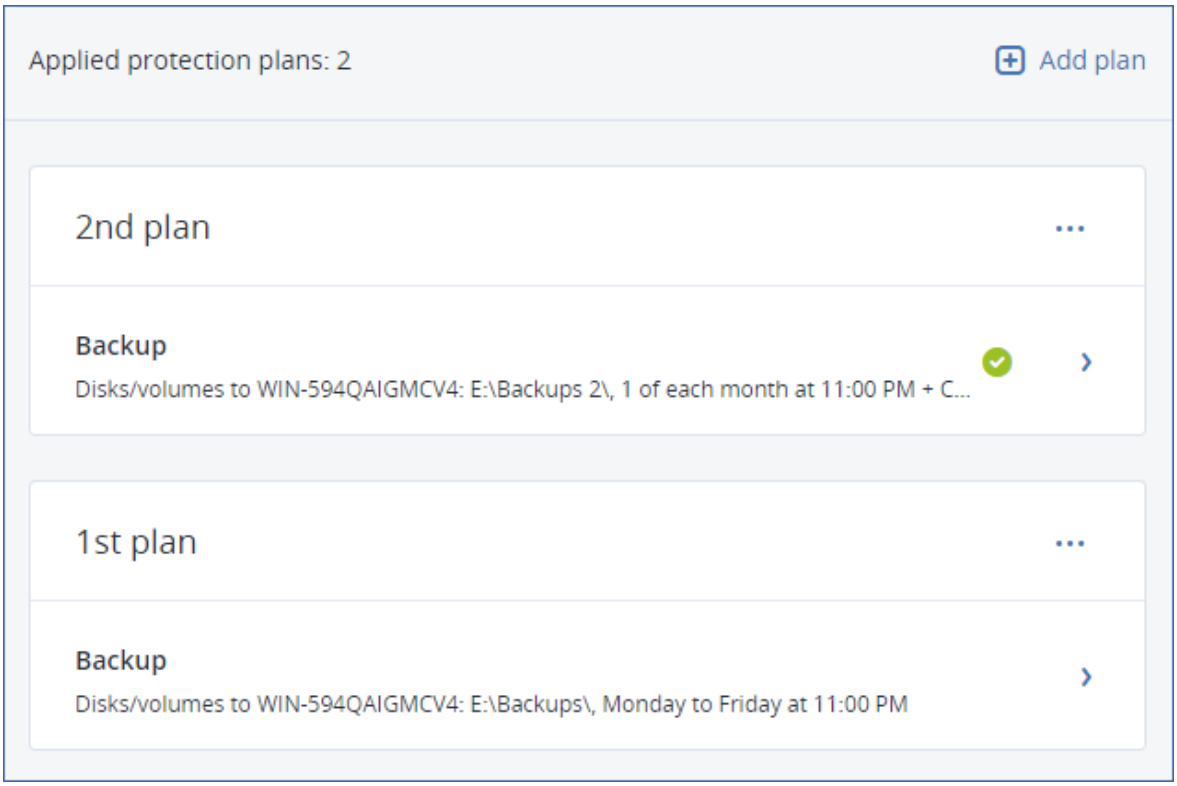
1. バックアップ対象のコンピュータを選択します。
2. **[保護]** をクリックします。
   ソフトウェアには、マシンに適用されている保護計画が表示されます。どの計画もまだ適用されていないマシンの場合、適用可能なデフォルトの保護計画が表示されます。必要に応じてこの計画の設定

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、保護計画ペインの該当するセクションをクリックします。
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には

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。

バックアップモジュールのチートシート

重要
このセクション内に記載されているいくつかの機能は、オンプレミスデプロイメントでのみ使用できます。

次の表は、使用可能なバックアップモジュール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 （クラウドでは使用不可）	保存期間

ディスク/ボリューム（物理マシン）	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 SFTPサーバー NFS* Secure Zone* 管理対象ロケーション* テープデバイス*	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）	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） 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）	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 SFTPサーバー NFS* 管理対象ロケーション* テープデバイス*		
ファイル（物理マシンのみ）	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 SFTPサーバー NFS* Secure Zone* 管理対象ロケーション* テープデバイス	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） 常に増分（単一ファイル）* 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 SFTPサーバー NFS*		

<table>
<tr><td>システム状態（クラウド配置のみ）</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 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><td rowspan="4"></td></tr>
<tr><td>SQLデータベース</td><td>直接選択</td><td rowspan="2">クラウド
ローカルフォルダ
ネットワークフォルダ
管理対象ロケーション*
テープデバイス</td></tr>
<tr><td>Exchangeデータベース</td><td>直接選択</td></tr>
<tr><td>Exchangeメールボックス</td><td>直接選択</td><td rowspan="2">クラウド
ローカルフォルダ
ネットワークフォルダ
管理対象ロケーション*</td><td rowspan="2">常に増分（1つのファイル）</td></tr>
<tr><td>Microsoft 365メールボックス</td><td>直接選択</td><td>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）
バックアップの数
無期限に保存</td></tr>
</table>

*以下の制限事項を参照してください。

制限事項

SFTPサーバーとテープデバイス

- これらのロケーションは、macOSを実行するコンピュータのバックアップ先には指定できません。
- これらのロケーションは、アプリケーション認識型バックアップのバックアップ先には指定できません。
- **[常に増分（単一ファイル）]** バックアップスキームは、これらの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。
- **[バックアップの合計サイズ別]** 保持ルールは、これらのロケーションには使用できません。

NFS

- Windowsでは、NFS共有へのバックアップは使用できません。
- ファイルの **[常に増分（単一ファイル）]** バックアップスキーム（物理マシン）は、NFS共有にバックアップする場合には使用できません。

Secure Zone

- Macでは、Secure Zoneを作成できません。

管理対象ロケーション

- 以下の場合、重複除外または暗号化が有効にされた管理対象ロケーションは、バックアップ先として選択できません。
  - バックアップスキームが **[常に増分（単一ファイル）]** に設定されている場合
  - 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
  - macOS を実行するマシンのディスクレベルバックアップ
  - ExchangeメールボックスおよびMicrosoft 365メールボックスのバックアップ。
- **[バックアップの合計サイズ別]** 保持ルールは、重複除外が有効にされた管理対象ロケーションには使用できません。

常に増分（単一ファイル）

- **[常に増分（単一ファイル）]** バックアップスキームは、SFTPサーバーまたはテープデバイスにバックアップする場合には使用できません。
- ファイルの **[常に増分（単一ファイル）]** バックアップスキーム（物理マシン）を使用できるのは、プライマリバックアップロケーションが Acronis クラウドの場合だけです。

バックアップの合計サイズ別

- 以下の場合、**[バックアップの合計サイズ別]** 保持ルールは使用できません。
  - バックアップスキームが **[常に増分（単一ファイル）]** に設定されている場合
  - SFTPサーバー、テープデバイス、または重複除外が有効にされた管理対象ロケーションにバックアップする場合

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以外のすべてのディスクのバックアップのことです。

このようなバックアップを構成するには、**[バックアップの対象]** で **[マシン全体]** を選択します。

重要
USBフラッシュドライブやUSBハードドライブなどの外付けドライブは、**マシン全体**のバックアップに含まれません。これらのドライブをバックアップするには、**Disks/volumes**バックアップを構成します。ディスクバックアップの詳細については、"ディスクとボリュームの選択"（210ページ）を参照してください。

ディスクとボリュームの選択

ディスクレベルのバックアップには、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。ディスクレベルのバックアップから個別のディスク、ボリューム、またはファイルを復元できます。マシン全体のバックアップとは、リムーバブルディスク以外のすべてのディスクのバックアップのことです。

注意
デフォルトでは、OneDriveのルートフォルダはバックアップ処理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、アーカイブ内に無効なコンテンツが含められます。

ディスク/ボリュームの選択には2 つの方法があります。各マシンで直接選択する方法とポリシールールを適用する方法です。ファイルフィルタを設定して、ディスクバックアップからファイルを除外できます。

直接選択

直接選択は、物理マシンのみで使用できます。仮想マシンのディスクとボリュームの直接選択を有効にするには、プロテクションエージェントをゲストオペレーティングシステムにインストールする必要があります。

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マシンで、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

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。
   保護計画に含まれているすべてのマシンにポリシールールが適用されます。バックアップ開始時にルールに準拠するデータがコンピュータになかった場合、そのコンピュータでバックアップは実行さ

れません。

5. **[完了]** をクリックします。

Windows、Linux、macOS のルール

- **[すべてのボリューム]** は、Windows を実行しているマシン上のすべてのボリュームと、Linux または macOS を実行しているマシン上のマウントされたすべてのボリュームを選択します。

Windowsのルール

- 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。
- **[固定ボリューム(物理マシン)]** は、リムーバブルメディア以外の物理マシンのすべてのボリュームを選択します。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。
- **[ブート+システム]** は、ブートボリュームとシステムボリュームを選択します。この組み合わせは、バックアップからのオペレーティングシステムの復元を確実にする最小設定です。
- **[起動+システムディスク(物理マシン)]** は起動ボリュームとシステムボリュームがあるディスクのすべてのボリュームを選択します。起動ボリュームとシステムボリュームが同じディスクにない場合、何も選択されません。このルールは物理マシンに対してのみ適用されます。
- **[ディスク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のルール

- `/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、次を入力します。

```
/dev/mapper/vg_1-lv1
/dev/mapper/vg-l-lv2
```

MacOS のルール

- [**ディスク**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。

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 7以降のオペレーティングシステムでは、Windowsのリストア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。

ファイルとフォルダの選択

ファイルレベルのバックアップは、ゲスト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た物理マシンと仮想マシンで使用できます。

オペレーティングシステムの復元が必要な場合は、ディスクとボリュームのバックアップを実行します。特定のデータのみを保護する場合、ファイル バックアップが適しています。これによりバックアップサイズが減少し、記憶域スペースを節約できます。

注意
デフォルトでは、OneDriveのルートフォルダはバックアップ処理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、アーカイブ内に無効なコンテンツが含められます。

ファイルの選択には2 つの方法があります。各コンピュータで直接選択する方法とポリシールールを適用する方法です。どちらの方法でも、ファイルフィルタによってバックアップ対象をさらに絞り込むことができます。

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]** 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. 保護計画に含まれているマシンごとに、以下の手順を実行します。

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。
選択したコンピュータから共有にアクセスできる必要があります。
c. 必要なファイル/フォルダを参照するか、パスを入力して、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。
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。
d. 必要なファイル/フォルダを選択します。
e. **[完了]** をクリックします。

ポリシールールを使用

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]** 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。
保護計画に含まれているすべてのマシンにポリシールールが適用されます。バックアップ開始時にルールに準拠するデータがコンピュータになかった場合、そのコンピュータでバックアップは実行されません。
5. **[完了]** をクリックします。

Windowsの選択ルール

- ファイルまたはフォルダへのフルパス、たとえば **D:¥Work¥Text.doc** または **C:¥Windows** など。
- テンプレート：
  - **[すべてのファイル]** 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。
  - **[全プロファイルフォルダ]** は、すべてのユーザープロファイルが存在するフォルダを選択します（通常、**C:¥Users**または**C:¥Documents and Settings**）。
- 環境変数：
  - `%ALLUSERSPROFILE%`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を選択します（通常、**C:¥ProgramData**または**C:¥Documents and Settings¥All Users**）。
  - `%PROGRAMFILES%`は、Program Filesフォルダを選択します（**C:¥Program Files**など）。
  - `%WINDIR%`は、Windowsがインストールされているフォルダを選択します（**C:¥Windows**など）。

  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。たとえば、マシン上のProgram Filesフォルダ内のJavaフォルダを選択するには、**%PROGRAMFILES%¥Java** と入力します。

Linuxの選択ルール

- ファイルまたはディレクトリへのフルパス。たとえば、 **home/usr/docs**にマウントされたボリューム**/dev/hda3**にある**file.txt**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。
  - `/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。
- テンプレート：
    - [**全プロファイルフォルダ**] は、**/home**を選択します。これは、デフォルト設定ではすべてのユーザープロファイルが格納されているフォルダです。

macOS の選択ルール

- ファイルまたはディレクトリへのフルパス。
- テンプレート：
    - [**全プロファイルフォルダ**] は、**/Users**を選択します。これは、デフォルト設定ではすべてのユーザープロファイルが格納されているフォルダです。

例：

- デスクトップにある **file.txt** をバックアップするには、**/Users/<username>/Desktop/file.txt**を指定します。 <username>には、ユーザー名を入れます。
- ユーザーのホーム ディレクトリ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ディレクトリをバックアップするには、**/Applications** を指定します。

システム状態の選択

システム状態のバックアップは、Windows 7以降のWindows OSを実行しているマシンで使用できます。

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の構成をバックアップするには、VMwareエージェントはTCPポート22でESXiホストへのSSH接続を使用します。ファイアウォールでこの接続がブロックされていないことを確認してください。
- 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 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。
- 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. **[バックアップ]** 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）

パフォーマンス上の理由から、通常は定期的なバックアップを実行する間隔はかなり長くなります。システムが突然損傷を受けると、最後のバックアップからシステム障害までの間のデータ変更は失われます。

継続的データ保護機能を使用すると、スケジュールの中に組み込まれているバックアップとバックアップの間でも、選択したデータの変更を以下のようにして継続的にバックアップできます。

- 指定のファイル/フォルダの変更をトラックすることによって
- 指定のアプリケーションによるファイル変更をトラックすることによって

バックアップ対象として選択したデータから、継続的データ保護の対象にするファイルを選択できます。選択したファイルのすべての変更がバックアップされます。そうしたファイルを最終変更時間の状態にリカバリできます。

現時点では、以下のオペレーティングシステムで**継続的データ保護**機能がサポートされています。

- Windows 7以降
- Windows Server 2008 R2以降

サポートされているファイルシステム:NTFSのみ、ローカルフォルダのみ（共有フォルダはサポートされていません）。

[継続的データ保護] オプションは **[アプリケーションバックアップ]** オプションと両立しません。

注意
エディションが異なると、機能も異なります。このドキュメントに記載されているいくつかの機能は、ご利用のライセンスでは使用できない場合があります。各エディションに含まれる機能の詳細については、「Acronis Cyber Protect 15エディションのクラウド配置を含んだ比較」を参照してください。

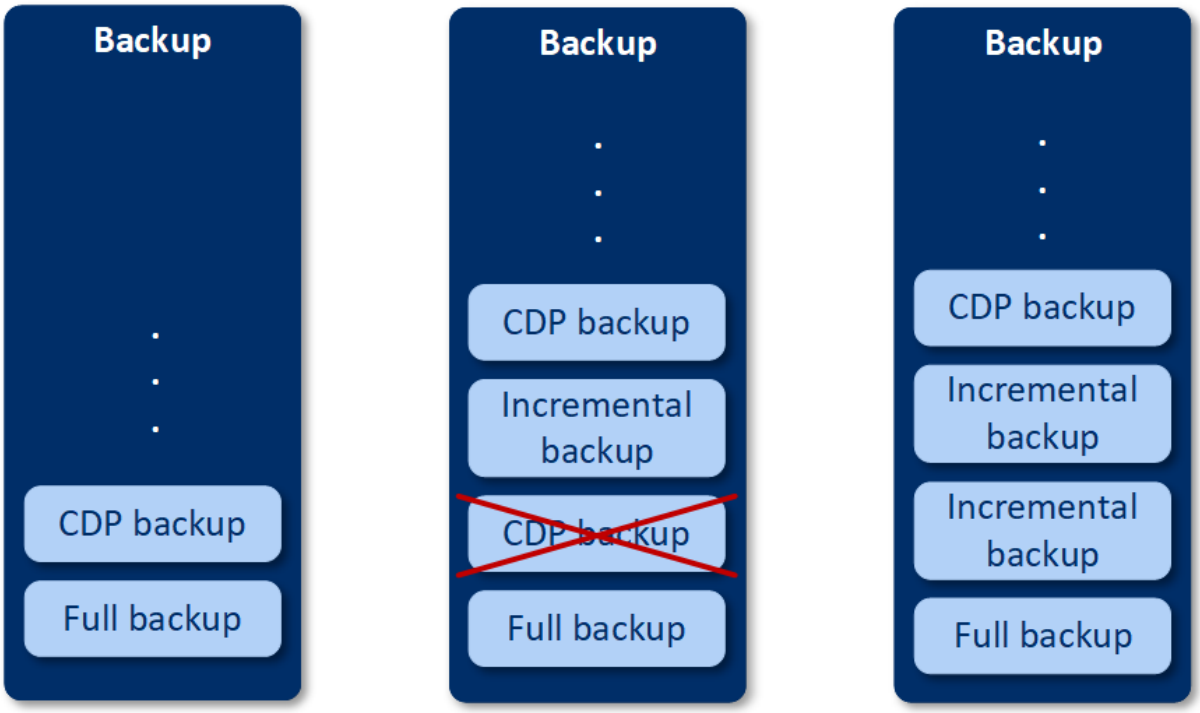
仕組み

継続的に作成するバックアップのことをCDPバックアップと呼びます。CDPバックアップを作成するには、完全バックアップまたは増分バックアップを事前に作成しておくことが必要です。

バックアップモジュールと**継続的データ保護**を有効にした保護計画を初めて実行する場合は、まず完全バックアップが作成されます。 その直後に、選択/変更したファイル/フォルダのCDPバックアップが作成されます。CDPバックアップには常に、選択したデータが最新の状態で保存されます。選択したファイル/フォルダに変更を加えると、新しいCDPバックアップが作成されるのではなく、すべての変更がその同じCDPバックアップに記録されます。

スケジュールに組み込まれている増分バックアップの時刻になると、CDPバックアップが削除され、増分バックアップの完了後に新しいCDPバックアップが作成されます。

そのようにして、CDPバックアップはバックアップチェーンの中で常に最新の状態で保存され、保護対象のファイル/フォルダの最新の状態が保持されます。



バックアップモジュールの保護計画が既に有効になっている状態で**継続的データ保護**を有効にした場合は、バックアップチェーンに完全バックアップが既に存在しているので、そのオプションを有効にした直後にCDPバックアップが作成されます。

継続的データ保護でサポートされているデータソースとバックアップ先

継続的データ保護を実行するには、以下のデータソースで以下の項目を指定します。

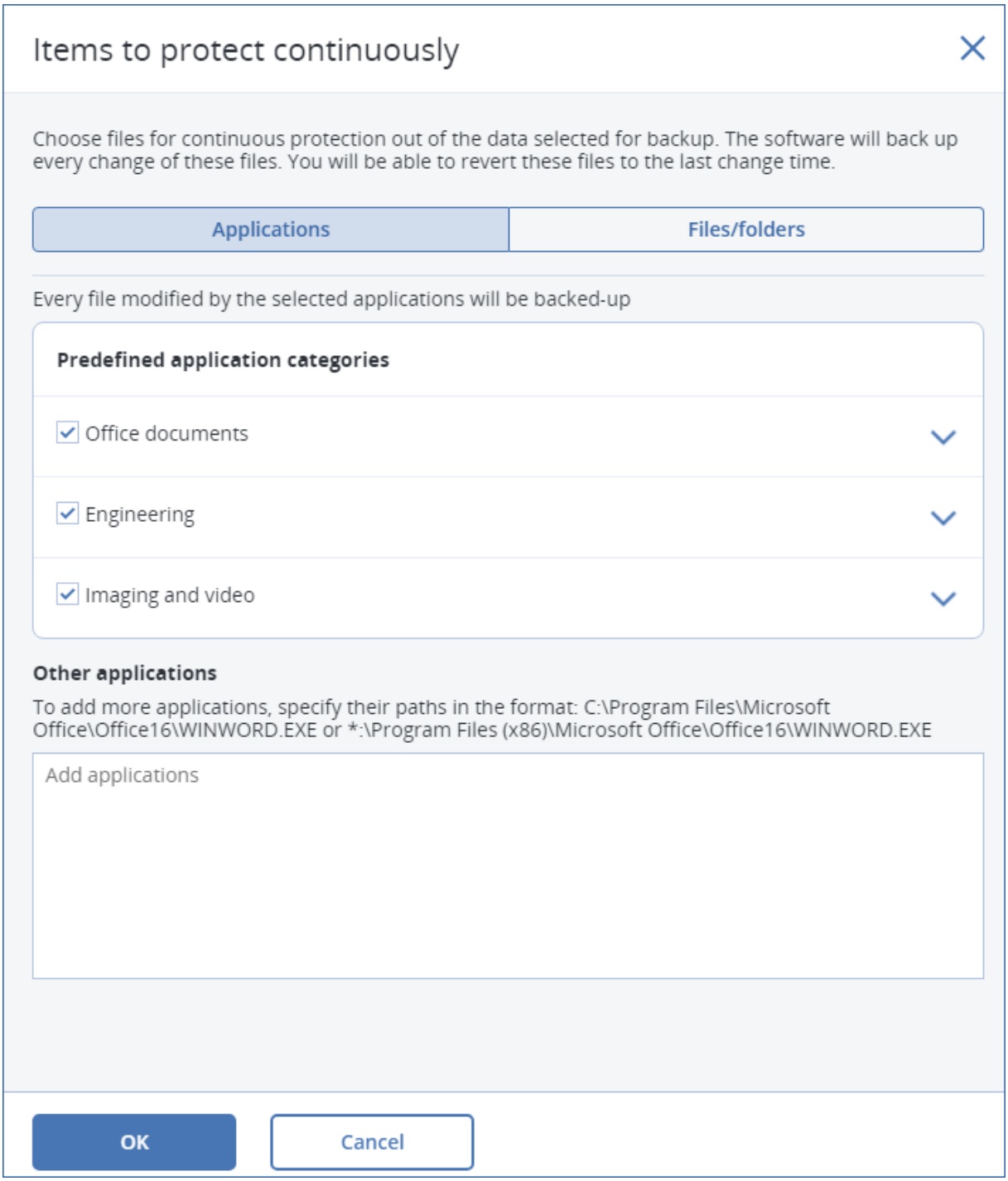
バックアップの対象	バックアップする項目
コンピュータ全体	ファイル/フォルダまたはアプリケーションのいずれかを指定する必要があります
ディスク/ボリューム	ディスク/ボリュームと、ファイル/フォルダまたはアプリケーションのいずれかを指定する必要があります
ファイル/フォルダ	ファイル/フォルダを指定する必要があります アプリケーションも指定できます（必須ではありません）

継続的データ保護では、以下のバックアップ先がサポートされています。

- ローカルフォルダ
- ネットワークフォルダ
- スクリプトで定義したロケーション
- クラウドストレージ
- Acronis Cyber Infrastructure

継続的データ保護でデバイスを保護する手順

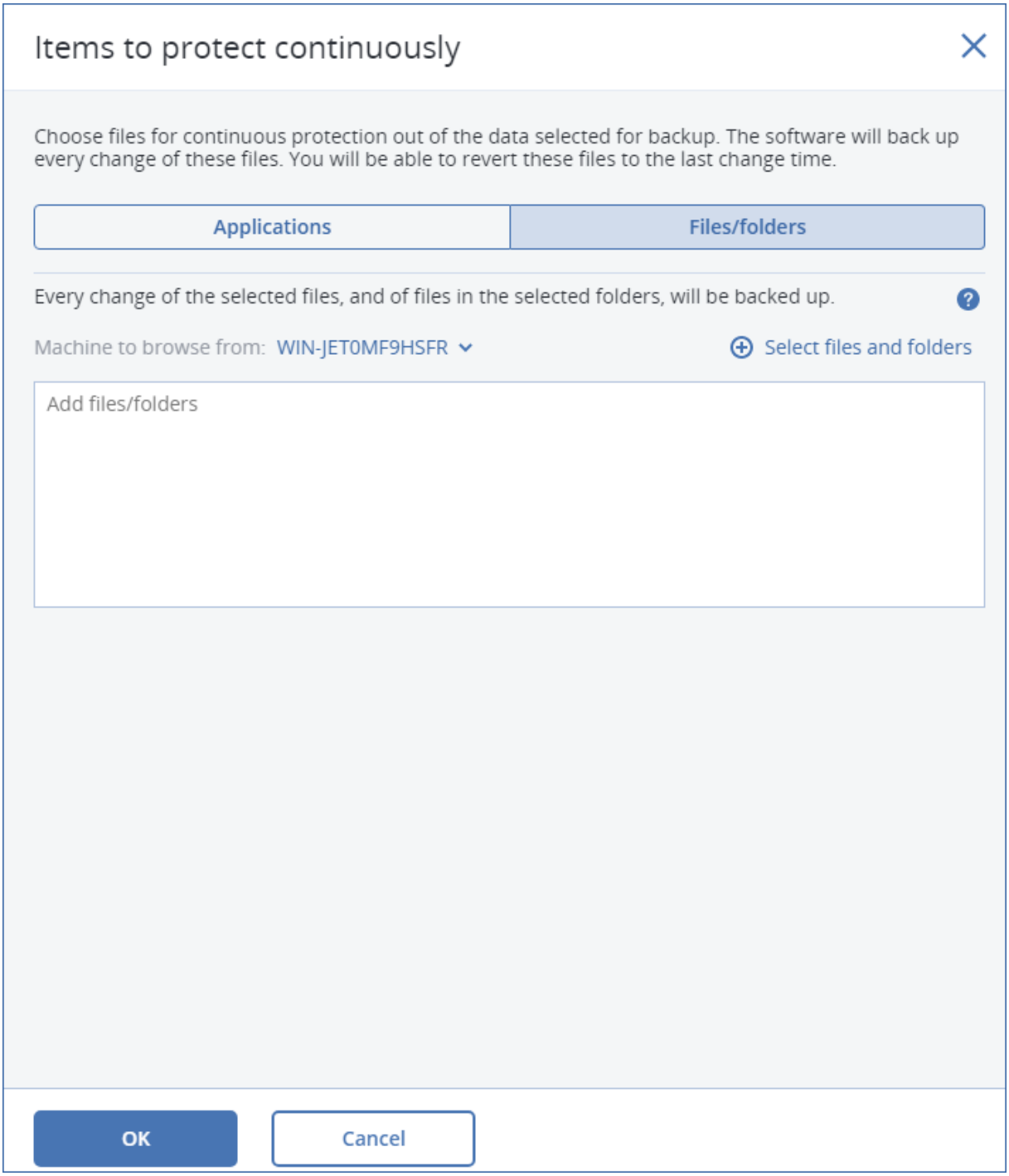
1. Cyber Protect ウェブ コンソールで、**バックアップ**モジュールを有効にした保護計画を作成します。
2. **[継続的データ保護（CDP）]** オプションを有効にします。
3. **[継続的な保護対象のアイテム]** を指定します。
   - **アプリケーション**（選択したアプリケーションで変更されたすべてのファイルがバックアップされます）。CDPバックアップでOffice文書を保護する場合は、このオプションを使用するようお勧めします。



- 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指定する場合は、対象のアプリケーションの実行可能ファイルのパスを定義してください。以下のいずれかの形式を使用できます。

  ```
  C:\Program Files\Microsoft Office\Office16\WINWORD.EXE
  ```
  OR
  ```
  *:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
  ```
  - **ファイル/フォルダ**（指定のロケーションで変更されたすべてのファイルがバックアップされま

す）。絶えず変更されるファイルやフォルダを保護する場合は、このオプションを使用するようお勧めします。



1. **参照元マシン** - 継続的データ保護の対象として選択するファイル/フォルダが入っているマシンを指定します。

   [ファイルとフォルダの選択] をクリックして、指定したマシンにあるファイル/フォルダを選択します。

重要
手動でフォルダ全体を指定して、そのフォルダ内のすべてのファイルを継続的にバックアップする場合は、以下のようなマスクを使用します。
正しいパス:D:¥Data¥*
間違ったパス:D:¥Data¥

テキストフィールドで、バックアップするファイル/フォルダを選択するためのルールを指定することもできます。ルールを定義する詳しい方法については、「ファイル/フォルダの選択」を参照してください。準備ができたら、**[完了]** をクリックします。

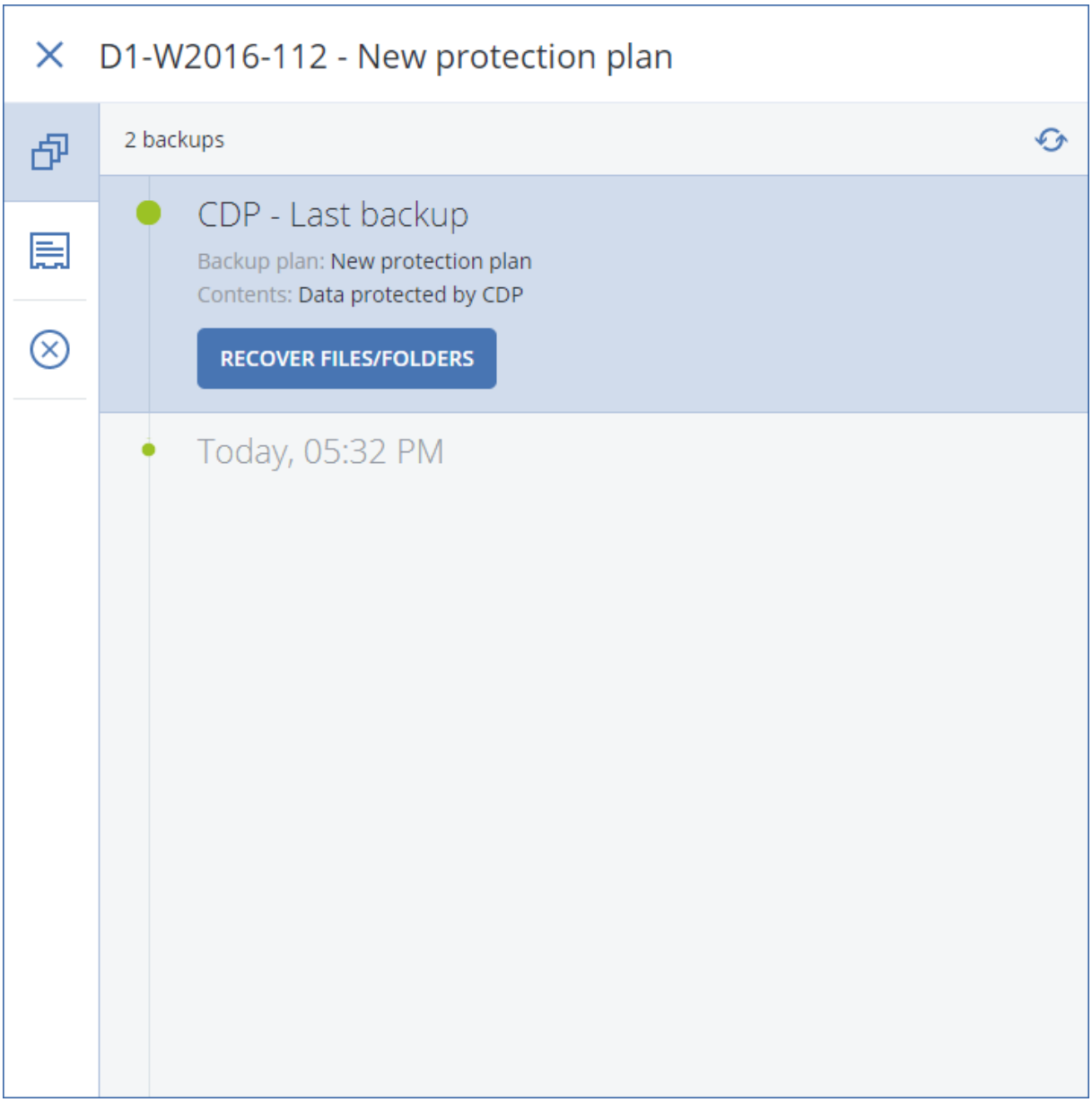
2. **[作成]** をクリックします。

選択したマシンに、継続的データ保護が有効になった保護計画が割り当てられます。最初の定期的なバックアップの後に、CDPで保護されているデータの最新コピーが継続的に作成されます。アプリケーションを基準にして定義したデータと、ファイル/フォルダを基準にして定義したデータの両方がバックアップされます。

継続的にバックアップするデータは、バックアップモジュールで定義されている保持ポリシーに基づいて保存されます。

継続的に保護されているバックアップを見分ける方法

継続的に保護されているバックアップにはCDPの接頭部が付きます。



マシン全体を最新の状態にリカバリする方法

マシン全体を最新の状態にリカバリするために、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）]** オプションを使用できます。

CDPバックアップからマシン全体をリカバリすることも、ファイル/フォルダをリカバリすることも可能です。マシン全体をリカバリすれば、マシン全体が最新の状態になり、ファイル/フォルダをリカバリすれば、そのファイル/フォルダが最新の状態になります。

バックアップ先の選択

重要
このセクション内に記載されているいくつかの機能は、オンプレミスデプロイメントでのみ使用できます。

バックアップロケーションを選択するには

1. **[バックアップ先]** をクリックします。
2. 次のいずれかを実行します。
   - 以前使用したバックアップロケーションまたは事前に定義されたバックアップロケーションを選択します。
   - **[ロケーションの追加]** をクリックし、新しいバックアップロケーションを追加します。

サポートされるロケーション

- **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。
- **Acronis Cyber Infrastructure**
  Acronis Cyber Infrastructureは、データ冗長性と自動自己回復機能を備えた信頼性に優れたソフトウェア定義ストレージとして使用できます。このストレージは、Microsoft Azure、または S3 や Swift と互換性のあるさまざまなストレージソリューションにバックアップを保存するためのゲートウェイとして設定できます。また、このストレージでは NFS バックエンドを使用することもできます。詳細については、「Acronis Cyber Infrastructureについて」を参照してください。

重要
macOSマシンでは、Acronis Cyber Infrastructureへのバックアップを使用できません。

- **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マシンに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。
  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について」を参照してください。
- **SFTP**
  SFTPサーバーの名前またはアドレスを入力します。次の表記がサポートされています。
  `sftp://<サーバー>`
  `sftp://<サーバー>/<フォルダ>`
  ユーザー名とパスワードを入力すると、サーバーフォルダを参照できます。
  どちらの表記でも、ポート、ユーザー名、パスワードも指定できます。
  `sftp://<サーバー>:<ポート>/<フォルダ>`
  `sftp://<ユーザー名>@<サーバー>:<ポート>/<フォルダ>`
  `sftp://<ユーザー名>:<パスワード>@<サーバー>:<ポート>/<フォルダ>`
  ポート番号が指定されていない場合は、ポート22が使用されます。
  パスワードなしの SFTP アクセスが設定されているユーザーは、SFTP にバックアップすることはできません。
  FTPサーバーへのバックアップはサポートされていません。

詳細ストレージオプション

- **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);
```

- 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");
```

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。したがって、C:\BackupとC:\backupは、Cyber Protectウェブ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。

- 次の**VBScript**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。

- **Storage Node**

  Storage Nodeは、企業データの保護に必要なさまざまなリソース（企業のストレージ容量、ネットワークの帯域幅、本番サーバーのCPU負荷など）の使用を最適化するように設計されたサーバーです。この目的は、企業のバックアップの専用ストレージとして機能するロケーション（管理対象ロケーション）を編成し、管理することで達成されます。

  以前作成したロケーションを選択したり、**[ロケーションの追加]** > **[Storage Node]** を選択して新しいロケーションを作成したりできます。設定の詳細については、「管理対象ロケーションの追加」を参照してください。

  Storage Node のユーザー名とパスワードの指定を求めるメッセージが表示されることがあります。Storage Node がインストールされているマシン上の次の Windows グループのメンバーは、Storage Node 上のすべての管理対象ロケーションにアクセスできます。

  - **管理者**
  - **AcronisASNリモートユーザー**

    Storage Node をインストールするときに、このグループが自動的に作成されます。デフォルトでは、このグループは空です。このグループにユーザーを手動で追加できます。

- **テープ**

  テープデバイスがバックアップ対象コンピュータまたはStorage Nodeに接続されている場合、ロケーションリストにデフォルトのテーププールが表示されます。このプールは自動で作成されます。

  デフォルトのプールを選択したり、**[ロケーションの追加]** > **[テープ]** を選択して新しいプールを作成したりできます。プールの設定の詳細については、「プールの作成」を参照してください。

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 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

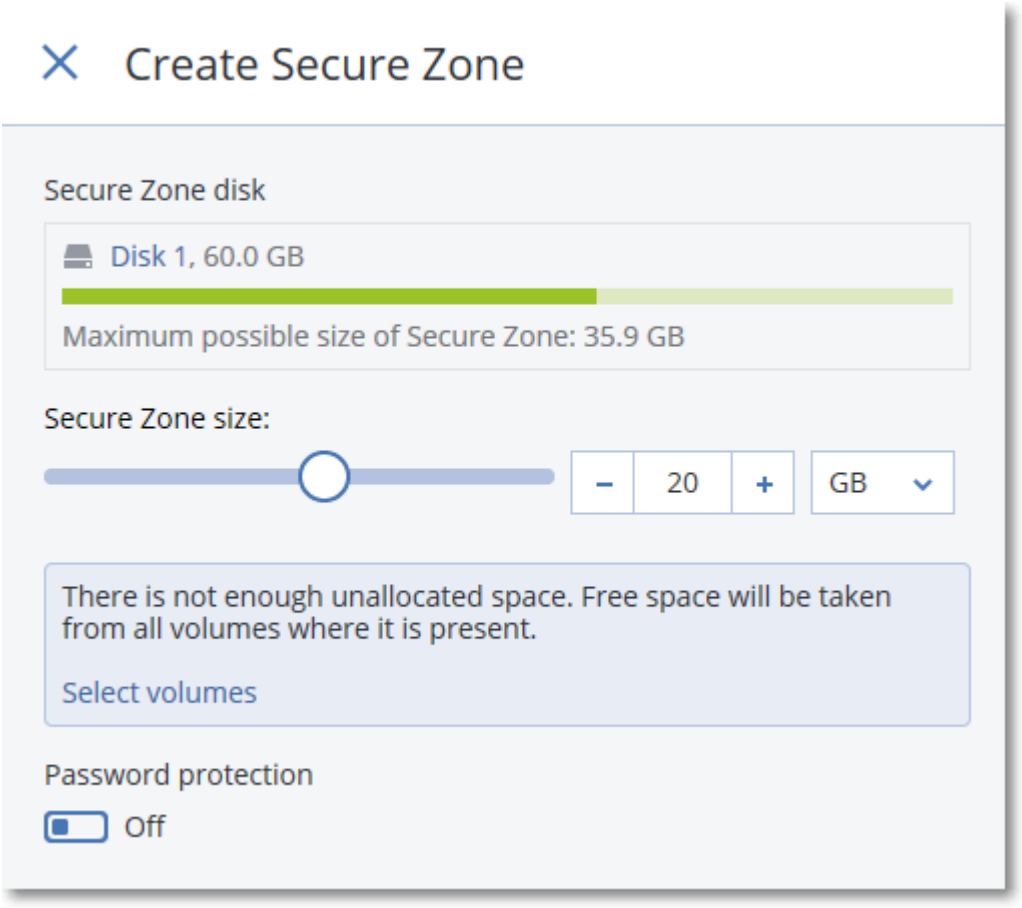
- Secure Zoneは、常にハードディスクの末尾に作成されます。
- ディスクの末尾に未割り当ての領域がない、または十分にないがボリュームの間に未割り当ての領域がある場合は、ディスクの末尾に未割り当ての領域を追加するためにボリュームが移動します。
- すべての未割り当ての領域を集めてもまだ十分ではない場合は、選択したボリュームから空き領域が取得され、それに合わせてボリュームのサイズが縮小されます。
- ただし、一時ファイルを作成する場合など、オペレーティング システムとアプリケーションが動作できるようにするにはボリュームに空き領域が必要です。空き領域がボリュームの合計サイズの25 %を下回っているか、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。

Acronis Cyber Infrastructureについて

Acronis Cyber Protect 15は、Acronis Cyber Infrastructure 3.5 Update 5 以降との統合をサポートしています。

macOS マシンでは、Acronis Cyber Infrastructure へのバックアップを使用できません。

デプロイ

Acronis Cyber Infrastructure を使用するには、オンプレミスのベアメタルに配置します。製品を最大限に活用するには、最低でも5台の物理サーバーを使用することをお勧めします。ゲートウェイ機能だけが必要な場合は、1 台の物理サーバーまたは仮想サーバーを使用するか、必要な台数のサーバーでゲートウェイクラスターを設定します。

管理サーバーと Acronis Cyber Infrastructure で時刻の設定が同期されていることを確認します。Acronis Cyber Infrastructure の時刻設定は、デプロイ中に設定できます。ネットワークタイムプロトコル（NTP）での時刻の同期はデフォルトで有効になっています。

Acronis Cyber Infrastructure の複数のインスタンスを配置し、同じ管理サーバーに登録できます。

登録

登録は Acronis Cyber Infrastructure の Web インターフェースで行います。Acronis Cyber Infrastructure は、組織管理者によってのみ、また組織内でのみ登録できます。一度登録すると、すべての組織部署でストレージが利用できるようになります。任意の部署または組織に対してバックアップロケーションとして追加できます。

逆の操作（登録解除）は Acronis Cyber Protect インターフェースにて行われます。**[設定]** > **[Storage Node]** をクリックし、必要な Acronis Cyber Infrastructure をクリックし、**[削除]** をクリックします。

バックアップの保存先の追加

Acronis Cyber Infrastructure のインスタンス 1 つごとに 1 つのバックアップロケーションのみを部署または組織に追加できます。部署レベルで追加されたロケーションは、この部署の管理者と組織管理者が利用できます。組織レベルで追加されたロケーションは、組織管理者のみが利用できます。

ロケーションを追加する際は、作成して名前を入力します。既存のロケーションを新しい管理サーバーまたは別の管理サーバーに追加する必要がある場合は、**[既存のロケーションを使用する...]** チェックボックスを選択し、**[参照]** をクリックして、リストからロケーションを選択します。

Acronis Cyber Infrastructure の複数のインスタンスが管理サーバーに登録されている場合は、ロケーションを追加する際に Cyber Infrastructure のインスタンスを選択できます。

バックアップスキーム、操作、制限事項

ブータブルメディアから Acronis Cyber Infrastructure に直接アクセスすることはできません。Acronis Cyber Infrastructure を操作するには、メディアを管理サーバーに登録して、Cyber Protect ウェブ コンソールからそのメディアを管理します。

コマンドラインインターフェースから Acronis Cyber Infrastructure にアクセスすることはできません。

利用可能なバックアップスキームおよびバックアップの操作の面で、Acronis Cyber Infrastructure はクラウド ストレージと似ています。唯一の違いは、保護計画の実行中に Acronis Cyber Infrastructure からバックアップをレプリケーションできる点です。

マニュアル

Acronis の Web サイトで Acronis Cyber Infrastructure の文書をすべて確認できます。

スケジュール

重要
このセクション内に記載されているいくつかの機能は、オンプレミスデプロイメントでのみ使用できます。

スケジュールには、エージェントがインストールされたオペレーティングシステムの時間設定（タイムゾーンを含む）が使用されます。VMwareエージェント（仮想アプライアンス）のタイムゾーンは、エージェントのインターフェースで設定できます。

たとえば、保護計画が21:00に実行されるようスケジュールされ、異なるタイムゾーンに位置する複数のマシンに適用されている場合、バックアップはそれぞれのマシンのローカル時刻が21:00になったときに始まります。

スケジュールの設定内容はバックアップ先によってそれぞれ異なります。

クラウドストレージにバックアップする場合

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。バックアップを実行する時刻を選択できます。

バックアップを頻繁に実行する場合、スライダを移動して、バックアップ スケジュールを指定できます。

時刻ではなくイベント別にバックアップをスケジュールすることができます。これを実行するには、スケジュールの選択時にイベントの種類を選択します。詳細については、「イベント別のスケジュール」を参照してください。

重要
最初のバックアップは完全バックアップとなるため、最も時間がかかります。その後のバックアップはすべて増分となり、バックアップに要する時間は大幅に短縮されます。

別のロケーションにバックアップする場合

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中からひとつ選択できます。バックアップスキームとは、バックアップスケジュールやバックアップ方法などが含まれている保護計画の一部です。

[バックアップ スキーム] で、次のいずれかを選択します。

- **常に増分（単一ファイル）**
  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。バックアップを実行する時刻を選択できます。
  バックアップを頻繁に実行する場合、スライダを移動して、バックアップ スケジュールを指定できます。
  バックアップは新しい単一ファイル バックアップ形式[1]を使用します。

[1]新しいバックアップ形式は、ファイルのチェーンではなく、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 1 つの .tib 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、例えばSFTPサーバーにバックアップする際には使用できません。

このスキームは、テープデバイスまたはSFTPサーバーにバックアップする場合には使用できません。

- **常に完全**

  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。バックアップを実行する時刻を選択できます。

  バックアップを頻繁に実行する場合、スライダを移動して、バックアップ スケジュールを指定できます。

  すべてのバックアップが完全バックアップで実行されます。

- **週単位で完全、日単位で増分**

  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。バックアップを実行する曜日と時間を修正できます。

  完全バックアップは週に1回作成されます。その他は、増分のバックアップになります。完全バックアップが作成される曜日は、[**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て、[**バックアップ オプション**] > [**週単位のバックアップ**]）によります。

- **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。バックアップを実行するこれらのスケジュールと時刻を変更できます。

  このバックアップスキームは、保護計画パネルでは [**カスタム**] として表示されます。

- **カスタム**

  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 スケジュールを指定します。

  SQLデータ、Exchangeデータ、またはシステム状態をバックアップする際には、差分バックアップはできません。

バックアップスキームでは、時刻ではなくイベント別にバックアップをスケジュールすることができます。これを実行するには、スケジュールの選択時にイベントの種類を選択します。詳細については、「イベント別のスケジュール」を参照してください。

追加のスケジュールオプション

どのバックアップ先に対しても、次の設定を行うことができます。

- 条件が満たされた場合にのみスケジュールされたバックアップが実行されるように、バックアップの開始条件を指定します。詳細については、「開始条件」を参照してください。
- 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。スケジュールが無効な間は、バックアップを手動で開始しないかぎり、保持ルールが適用されません。
- スケジュールされた時間から遅延を導入します。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。

  ギア アイコンをクリックしてから、[**バックアップ オプション**] > [**スケジューリング**] をクリックします。[**開始時間を時間枠内で割り振る**] を選択し、最大遅延を指定します。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。

注意
クラウド配置では、このオプションはデフォルトで有効であり、最大遅延は30分に設定されています。オンプレミス配置では、デフォルトはすべてのバックアップをスケジュールどおりに開始します。

- **[詳細を表示]** をクリックして次のオプションにアクセスします。
  - **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**（デフォルトでは無効）
  - **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**（デフォルトでは有効）
    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。
  - **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**（デフォルトでは無効）
    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。このオプションは、マシンの電源が入っていない場合は無効です。つまり、このオプションでは Wake-on-LAN 機能は使用しません。

イベント別のスケジュール

保護計画のスケジュールの設定では、スケジュールの選択時にイベントの種類を選択できます。バックアップはイベントが発生するとすぐ開始されます。

次のいずれかのイベントを選択できます。

- **前回のバックアップからの経過時間**
  同じ保護計画内で前回の正常なバックアップが完了してからの時間です。時間の長さを指定できます。

注意
スケジュールはバックアップが成功したイベントに基づきます。このため、バックアップが失敗する場合、オペレーターが手動で計画を実行し、実行が正常に完了するまで、スケジューラーによりジョブが再実行されることはありません。

- **ユーザーがシステムにログインするとき**
  デフォルトで、任意のユーザーのログインによりバックアップが開始されます。任意ユーザーを特定のユーザーアカウントに変更できます。
- **ユーザーがシステムからログオフするとき**
  デフォルトで、任意のユーザーのログオフによりバックアップが開始されます。任意ユーザーを特定のユーザーアカウントに変更できます。

注意
バックアップ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違うからです。

- **システムの起動時**
- **システムのシャットダウン時**
- **Windowsイベントログ イベント発生時**
  イベントのプロパティを指定する必要があります。

Windows、Linux、およびmacOSで各種データ向けに使用できるイベントを次の表に示します。

バックアップ対象	前回のバックアップからの経過時間	ユーザーがシステムにログインするとき	ユーザーがシステムからログオフするとき	システムの起動時	システムのシャットダウン時	Windows イベントログ イベントの発生時
ディスク/ボリュームまたはファイル(物理コンピュータ)	Windows、Linux、macOS	Windows	Windows	Windows、Linux、macOS	Windows	Windows
ディスク/ボリューム（仮想マシン）	Windows、Linux	–	–	–	–	–
ESXi構成	Windows、Linux	–	–	–	–	–
Microsoft 365メールボックス	Windows	–	–	–	–	Windows
Exchangeのデータベースとメールボックス	Windows	–	–	–	–	Windows
SQLデータベース	Windows	–	–	–	–	Windows

Windows イベント ログ イベントの発生時

アプリケーションログ、**セキュリティ**ログ、**システム**ログなどのイベントログの1つに特定のWindowsイベントが記録されたときに、バックアップを開始するようにスケジュールできます。

たとえば、ハードディスクドライブで障害が発生しそうな状況がWindowsによって検出された時点でデータの緊急完全バックアップをすぐに自動的に実行するように保護計画を設定できます。

イベントを参照し、イベントのプロパティを表示するには、**[コンピュータの管理]** コンソールから利用できる **[イベントビューア]** スナップインを使用します。**セキュリティ**ログを開くには、**アドミニストレータグループ**のメンバーである必要があります。

イベントのプロパティ

[ログ名]

ログの名前を指定します。一覧から標準のログの名前（**[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、ログ名を入力します。例:**Microsoft Office Sessions**

[イベントソース]

イベントソースを指定します。これは通常、**[ディスク]** のように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を示します。

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、大文字小文字が区別されません。そのため、「**service**」という文字列を指定した場合、**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]

イベントの種類として、**[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]

イベント番号を指定します。通常、同じソースのイベントの中から特定の種類のイベントを識別します。

たとえば、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:"不良ブロック" 緊急バックアップ

通常、ハード ディスク上で 1 つ以上の不良ブロックが突然検出されると、そのハード ディスクに間もなく障害が発生することを示しています。このような状況が発生した場合に直ちにハードディスクのデータをバックアップするための保護計画を作成するとします。

Windowsによってハードディスクに不良ブロックが検出されると、イベントソースが**ディスク**でイベント番号が**7**のイベントが**システム**ログに記録されます。このイベントの種類は**エラー**です。

計画を作成する際に、**[スケジュール]** セクションで次の値を設定します。

- **[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
不良ブロックが存在してもそのバックアップを完了できるようにするには、バックアップが不良ブロックを無視するように設定する必要があります。そのためには、**[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

この設定を使用すると、スケジューラで特定の条件に従ってより柔軟にバックアップタスクを実行できるようになります。複数条件を設定した場合、バックアップを開始するにはそれらの条件が同時に満たされる必要があります。バックアップを手動で開始した場合は、開始条件は無効になります。

これらの設定にアクセスするには、保護計画のスケジュールを設定するときに **[詳細を表示]** をクリックします。

指定した条件（または複数の条件のいずれか）を満たさない場合のスケジューラの動作は、[バックアップの開始条件] バックアップオプションで定義します。条件が長期間満たされず、バックアップがさらに遅れる危険性が高まっている場合に、条件にかかわらずバックアップを実行するまでの間隔を設定できます。

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。

バックアップ対象	ディスク/ボリュームまたはファイル(物理コンピュータ)	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	Windows	–	–	–	–	–
バックアップロケーションのホストが利用可能	Windows、Linux、macOS	Windows、Linux	Windows、Linux	Windows	Windows	Windows

ユーザーがログオフ	Windows	–	–	–	–	–
時間間隔が適合	Windows、Linux、macOS	Windows、Linux	–	–	–	–
バッテリー電源を節電する	Windows	–	–	–	–	–
従量制課金接続時には開始しない	Windows	–	–	–	–	–
指定したWi-Fiネットワークへの接続時には開始しない	Windows	–	–	–	–	–
デバイスのIPアドレスをチェックデバイ	Windows	–	–	–	–	–

ユーザーはアイドルです

[ユーザーはアイドルです] 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21:00、できればユーザーがアイドル状態のときに、コンピュータでバックアップを実行します。23:00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:毎日実行。開始時刻:**21:00**。
- 条件:**ユーザーがアイドル状態の場合**。
- バックアップ開始条件:**条件が満たされるまで待機**し、**2時間が経過するとバックアップを実行**。

結果は次のようになります。

（1）21:00の前にユーザーがアイドルになっていれば、バックアップは21:00に開始されます。

（2）21:00から23:00の間にユーザーがアイドルになった場合、バックアップはユーザーがアイドルになると直ちに開始されます。

（3）23:00になってもユーザーがアクティブな場合、バックアップは23:00に強制的に開始されます。

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可能です] は、バックアップの保存先をホストしているコンピュータ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対して有効です。

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

データを毎平日の21:00にネットワークフォルダにバックアップするとします。また、このフォルダをホストしているコンピュータが保守作業などのために使用できない場合は、バックアップをスキップし、翌平日のスケジュールされている開始時刻まで待ちます。

- スケジュール:毎日、月曜日から金曜日まで実行。開始時刻:**21:00**。
- 条件:**バックアップロケーションのホストが利用可能な場合**。
- 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。

（1）21:00になり、ホストを使用できる場合、バックアップは直ちに開始されます。

（2）21:00になったが、ホストを使用できない場合、バックアップは翌平日にホストを使用できれば開始されます。

（3）平日の21:00にホストをいつまでも使用できないでいると、バックアップはいつまでたっても開始されません。

ユーザーがログオフ

すべてのユーザーがWindowsからログオフするまで、バックアップを保留にできます。

例

毎週金曜日の20:00に、できればすべてのユーザーがログオフしている状態でバックアップを実行します。ただし、まだログオンしているユーザーが23:00にいても、バックアップは強制的に実行します。

- スケジュール:週単位、毎金曜日。開始時刻:**20:00**。
- 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。

（1）20:00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20:00に開始されます。

（2）最後のユーザーが20:00～23:00にログオフした場合は、そのユーザーのログオフ後すぐにバックアップが開始されます。

（3）23:00になってもユーザーがログインしていた場合でも、バックアップは23:00に開始されます。

以下の開始・終了時刻に該当

バックアップ開始時刻を、指定した期間内に制限します。

例

ある企業では、ユーザーデータとサーバーのバックアップ用に、同じNAS（Network Attached Storage）上の異なるロケーションを使用しています。就業時間は08:00から17:00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16:30以降です。毎日23:00に会社のサーバーをバックアップします。このため、ネットワークの帯域幅をすべて利用できるように、この時刻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と想定されるため、バックアップ開始時間は遅くても22:00です。指定した期間内にユーザーがまだログオンしているとき、またはその期間以外の時刻にログオフしても、ユーザーデータをバックアップしません。つまり、バックアップの実行をスキップします。

- 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:**16:30**から**22:00**までの**期間の範囲内に収まる場合**。
- 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。

（1）ユーザーが16:30から22:00の間にログオフすると、ログオフの直後にバックアップが開始されます。

（2）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

デバイス（ノート PC またはタブレット）が電源に接続されていない場合にバックアップしないようにします。バックアップオプションのバックアップ開始条件の値によって、デバイス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。

- **バッテリー動作時には開始しない**
  デバイスが電源に接続されている場合のみ、バックアップを開始します。
- **バッテリー残量が次の値より高い場合は開始する**
  デバイス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

データを月曜日～金曜日の 21:00 にバックアップするとします。デバイスが電源に接続されていない場合（たとえば、ユーザーが遅い時間帯の会議に出席している場合）、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、ユーザーがデバイスを電源に接続するまで待機します。

- スケジュール:毎日、月曜日から金曜日まで実行。開始時刻:21:00。
- 条件:**[バッテリー電源を節電する]**、**[バッテリー動作時には開始しない]**。
- 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。

（1）21:00 になり、デバイスが電源に接続されている場合、直ちにバックアップが開始されます。

（2）21:00 になり、デバイスがバッテリー電源を使用している場合、デバイスが電源に接続されると直ちに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

Windows で従量制課金が設定された接続を使用してデバイス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）しないようにします。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。

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別の方法として、**[従量制課金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。「X」をクリックすると、これらの名前をリストから削除できます。

例

データを月曜日～金曜日の 21:00 にバックアップするとします。デバイスが従量制課金接続を使用してインターネットに接続されている場合（たとえば、ユーザーが出張中の場合）、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、次の平日のスケジュール設定された開始まで待機します。

- スケジュール:毎日、月曜日から金曜日まで実行。開始時刻:21:00。
- 条件:**従量制課金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。

（1）21:00 になり、デバイスが従量制課金接続でインターネットに接続されていない場合、直ちにバックアップが開始されます。

（2）21:00 になり、デバイスが従量制課金接続でインターネットに接続されている場合、次の平日にバックアップが開始されます。

（3）平日の 21:00 にデバイスが常に従量制課金接続でインターネットに接続されている場合、バックアップは開始されません。

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

デバイス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）しないようにします。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、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、バックアップは開始されません。「Johnの iPhone」、「phone_wifi」、または「my_PHONE_wifi」。

この条件は、デバイスが携帯電話のホットスポットでインターネットに接続されている場合に、バックアップしないようにする場合に便利です。

モバイルホットスポット経由でバックアップしないようにする別の方法として、**[従量制課金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。「X」をクリックすると、これらの名前をリストから削除できます。

例

データを月曜日～金曜日の 21:00 にバックアップするとします。デバイスがモバイルホットスポットでインターネットに接続されている場合（たとえば、ノート PC がテザリングモードで接続されている場合）、バックアップをスキップし、次の平日のスケジュール設定された開始時まで待機します。

- スケジュール:毎日、月曜日から金曜日まで実行。開始時刻:21:00。
- 条件:**[次の Wi-Fi ネットワークへの接続時には開始しない]**、**[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。

（1）21:00 になり、マシンが指定したネットワークに接続されていない場合、直ちにバックアップが開始されます。

（2）21:00 になり、マシンが指定したネットワークに接続されている場合、次の平日にバックアップが開始されます。

（3）平日の 21:00 に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、バックアップは開始されません。

デバイスのIPアドレスをチェック

デバイスの 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）しないようにします。次から選択できます。

- **次の IP アドレスの範囲外なら開始する**
- **次の IP アドレスの範囲内なら開始する**

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。

この条件は、ユーザーが海外にいて、データ転送の料金が高額になるのを回避する場合に便利です。また、Virtual Private Network（VPN）接続のバックアップを防ぐ場合も役立ちます。

例

データを月曜日～金曜日の 21:00 にバックアップするとします。デバイスが VPN トンネル（たとえば、ユーザーが自宅で作業を行っている場合）を使用して企業ネットワークに接続されている場合に、バックアップをスキップし、ユーザーがデバイスをオフィスに持ってくるまで待機します。

- スケジュール:毎日、月曜日から金曜日まで実行。開始時刻:21:00。
- 条件:**デバイスの IP アドレスを確認し、IP が次の範囲の外部のものであれば開始します。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。

（1）21:00 になり、マシンの IP アドレスが指定した範囲外の場合、直ちにバックアップが開始されます。

（2）21:00 になり、マシンの IP アドレスが指定した範囲内の場合、デバイスが VPN 以外の IP アドレスを取得したら直ちにバックアップが開始されます。

（3）マシンの IP アドレスが、平日の 21:00 には常に指定した範囲内である場合は、バックアップは開始されません。

保持ルール

重要
このセクション内に記載されているいくつかの機能は、オンプレミスデプロイメントでのみ使用できます。

1. **[バックアップ保持期間]** をクリックします。
2. **[クリーンアップ]** で、次のいずれかを選択します。

- **バックアップ期間**（デフォルト）
  保護計画で作成されたバックアップを保持する期間を指定します。デフォルトでは、バックアップ設定[1]それぞれに保持ルールが適用されます。単一のルールをすべてのバックアップに使用する場合は、[**すべてのバックアップセットの単一のルールに切り替え**] をクリックします。
- **バックアップの数**
  バックアップの最大数を指定して、保持します。
- **バックアップの合計サイズ別**
  保持するバックアップの最大合計サイズを指定します。
  この設定では、[**常時増分バックアップ（単一ファイル）**] のバックアップスキームを利用できません。またSFTPサーバーやテープデバイスにバックアップすることもできません。
- **バックアップを無期限に保存する**

3. クリーンアップを開始する時期を選択します。
   - **バックアップ後**（デフォルト）
     保持ルールは新しいバックアップの作成後に適用されます。
   - **バックアップ前**
     保持ルールは新しいバックアップの作成前に適用されます。
     この設定は、Microsoft SQL ServerクラスタまたはMicrosoft Exchange Serverクラスタのバックアップでは使用できません。

その他の注意点

- 保護計画によって作成された最終バックアップは、ほとんどのケースにおいて保持されます。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この限りではありません。

  警告
  このような保持ルールを適用した状態でバックアップを削除すると、バックアップに障害が発生した場合でも、使用できるバックアップが存在しないためデータを復元できなくなります。

- テープに保存されているバックアップは、そのテープが上書きされない限り削除されません。
- バックアップスキームとバックアップ形式に基づき、各バックアップが別個のファイルとして保存されている場合、そのファイルはすべての依存（増分でも差分でも）バックアップの有効期間が過ぎるまで削除できません。そのため、削除が延期されるバックアップデータがあることを想定したバック

[1]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、月の初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初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、その日の初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、該当時間の初めに最初のバックアップが作成されます。

アップ先の保存領域の設計が必要になります。また、バックアップの期間、数、サイズが指定値を超える可能性が生じます。

この動作は、[バックアップの統合] バックアップオプションを使用して変更できます。

- 保持ルールは保護計画の一部です。保護計画がマシンで取り消されるか削除される場合、またはマシン自体が管理サーバーから削除される場合は直ちに、マシンのバックアップの動作が停止します。今後この計画でバックアップを作成する必要がない場合は、「バックアップの削除」で説明されている手順に従い、それらを削除します。

暗号化

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。

重要
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。

保護計画での暗号化

暗号化を有効にするには、保護計画を作成するときに、暗号化設定を指定します。保護計画の適用後に暗号化設定を修正することはできません。別の暗号化設定を使用するには、新しい保護計画を作成します。

保護計画で暗号化設定を指定する手順

1. 保護計画ペインで、**[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. 次の暗号化アルゴリズムのいずれかを選択します。
   - **[AES 128]**: バックアップは、128 ビット キーの AES（高度暗号化標準）アルゴリズムを使用して暗号化されます。
   - **[AES 192]**: バックアップは、192 ビット キーの AES アルゴリズムを使用して暗号化されます。
   - **[AES 256]**: バックアップは、256 ビット キーの AES アルゴリズムを使用して暗号化されます。
4. **[OK]** をクリックします。

マシンプロパティとして暗号化

このオプションは、複数のコンピュータのバックアップを処理する管理者向けです。各マシン固有の暗号化パスワードが必要な場合、または保護計画の暗号化設定に関係なく、バックアップの暗号化を適用する必要がある場合は、各マシンについて個別の暗号化設定を保存します。バックアップは、256 ビット キーの AES アルゴリズムを使用して暗号化されます。

マシンに暗号化設定を保存すると、保護計画に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。

- **マシンに適用される予定の保護計画。**マシンに保存された暗号化設定が、保護計画の暗号化設定よりも優先されます。バックアップは、保護計画で暗号化が無効な場合でも、すべて暗号化されます。

このオプションはエージェントfor VMwareを実行するコンピュータで使用できます。ただし、複数のエージェントfor VMwareが同じvCenter Serverに接続されている場合は注意してください。すべてのエージェントで同じ暗号化設定を使用する必要があります。これはエージェント間で一種のロードバランシングが発生するためです。

暗号化設定を保存した後、以下のように変更したり、リセットしたりできます。

重要
このマシンで実行される保護計画が既にバックアップを作成している場合、暗号化設定を変更すると、この計画が失敗します。バックアップを続行するには、新しい計画を作成します。

コンピュータに暗号化設定を保存する手順

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. 次のスクリプトを実行します。
   - Windowsの場合：**<インストール パス>¥PyShell¥bin¥acropsh.exe -m manage_creds --set-password <暗号化パスワード>**
     ここで、**<インストール パス>**は保護エージェントのインストールパスです。デフォルト設定では、クラウド配置は **%ProgramFiles%¥BackupClient** になり、オンプレミス配置は **%ProgramFiles%¥Acronis** になります。
   - Linuxの場合：**/usr/sbin/acropsh -m manage_creds --set-password <暗号化パスワード>**

コンピュータの暗号化設定をリセットする手順

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. 次のスクリプトを実行します。
   - Windowsの場合：**<インストール パス>¥PyShell¥bin¥acropsh.exe -m manage_creds --reset**
     ここで、**<インストール パス>**は保護エージェントのインストールパスです。デフォルト設定では、クラウド配置は **%ProgramFiles%¥BackupClient** になり、オンプレミス配置は **%ProgramFiles%¥Acronis** になります。
   - Linuxの場合：**/usr/sbin/acropsh -m manage_creds --reset**

Cyber Protect Monitor を使用して暗号化設定を変更するには

1. WindowsまたはmacOSで、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 Monitor** 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. 次のいずれかを実行します。
   - **[このマシンの特定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して確認します。

- **[保護計画で指定された暗号化設定を使用]** を選択します。

6. **[OK]** をクリックします。

暗号化の動作方法

AES 暗号化アルゴリズムは、暗号ブロック連鎖（CBC）モードで動作し、ランダムに生成されるキーを使用します。キーの長さは 128、192、または 256 ビットからユーザーが指定できます。キーのサイズが大きいほどバックアップを暗号化する時間は長くなりますが、データの安全性は高まります。

次に、暗号化キーは、パスワードの SHA-256 ハッシュをキーとして使用して、AES-256 で暗号化されます。パスワード自体はディスクまたはバックアップに保存されませんが、パスワードのハッシュが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。

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、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
- バックアップの保存先が、重複除外または暗号化が有効になっている管理対象ロケーションの場合

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。

仮想コンピュータへの変換

重要
このセクション内に記載されているいくつかの機能は、オンプレミスデプロイメントでのみ使用できます。

仮想コンピュータへの変換は、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。

変換方法

- **定期的に実行される変換**
  定期的に実行される変換を設定する方法は 2 つあります。
  - **変換を保護計画の一部にする**
    変換は、バックアップ後に毎回実行（プライマリロケーションに設定されている場合）されるか、レプリケーション後に毎回実行（セカンダリまたはそれ以降のロケーションに設定されている場合）されます。
  - **別の変換計画を作成する**
    この方法では、個別の変換スケジュールを指定できます。
- **新しい仮想マシンに復元する**
  この方法では、復元対象のディスクを選択して、各仮想ディスクに対して設定を調整できます。この方法は、物理マシンから仮想マシンへの移行を実行する場合など、一度または時々変換を実行する場合に使用します。

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、エージェントが作成可能な仮想マシンの種類を示しています。

VM の種類	エージェント for VMware	エージェント for Hyper-V	エージェント for Windows	エージェント for Linux	エージェント for Mac	Scale Computing HC3エージェント
VMware ESXi	+	–	–	–	–	–
Microsoft Hyper-V	–	+	–	–	–	–
VMware Workstation	+	+	+	+	–	–
VHDXファイル	+	+	+	+	–	–
Scale Computing HC3	–	–	–	–	–	+

制限事項

- Windowsエージェント、VMwareエージェント（Windows）、およびHyper-Vエージェント（Windows）はNFSに保存されているバックアップを変換できません。
- NFSまたはSFTPサーバーに保存されているバックアップを別個の変換計画で変換することはできません。
- 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。
- バックアップは、別の変換計画でのみScale Computing HC3仮想マシンに変換できます。
- 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ESXiおよびHyper-V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。

2番目の事例では、仮想マシンの実行中のみ、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。

保護計画での仮想マシンへの変換

保護計画に含まれる任意のバックアップまたはレプリケーションロケーションで仮想マシンへの変換を設定できます。バックアップまたはレプリケーション後に毎回変換が実行されます。

前提条件と制限事項についての情報は、「変換に関する注意点」を参照してください。

保護計画で仮想マシンへの変換を設定するには

1. 変換を実行するバックアップロケーションを決めます。
2. 保護計画ペインで、そのロケーションの **[VM に変換]** をクリックします。
3. **[変換]** スイッチを有効にします。
4. **[変換先]** で、ターゲット仮想コンピュータ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**
   - **VMware Workstation**
   - **VHDXファイル**
5. 次のいずれかを実行します。
   - VMware ESXiとHyper-V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. （オプション）**[変換を実行するエージェント]** をクリックし、エージェントを選択します。
   このエージェントは、バックアップを実行するエージェントの場合（デフォルト）もあれば、別のコンピュータにインストールされたエージェントの場合もあります。後者の場合は、ネットワークフォルダなどの共有のロケーションにバックアップを保存して、他のマシンからバックアップにアクセスできるようにする必要があります。
7. （オプション）VMware ESXiとHyper-Vについては、次の操作を実行することもできます。

- **[データストア]**（ESXi）または **[パス]**（Hyper-V）をクリックしてから、仮想コンピュータのデータストア（ストレージ）を選択します。
- 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、VMware ESXiの場合は **[シン]**、Hyper-Vの場合は **[容量可変]** です。
- **[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。

8. **[完了]** をクリックします。

VM への定期的な変換の動作

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、新しい仮想コンピュータが作成されます。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、新しい仮想コンピュータが作成されます。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、既存の仮想コンピュータが、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

仮想コンピュータをアップデートできるようにするため、仮想コンピュータの中間スナップショットがいくつか保存され、**Backup…**や**Replica…**という名前が付けられます。ファイル名は変更しないでください。不必要なスナップショットは自動的に削除されます。

最新の**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。コンピュータ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、コンピュータの使用中に、そのコンピュータに対して行った変更内容を取り消したい場合などです。

他のスナップショットは、ソフトウェアによって内部的に使用されます。

レプリケーション

重要
このセクション内に記載されているいくつかの機能は、オンプレミスデプロイメントでのみ使用できます。

このセクションでは、保護計画の一環としてのバックアップのレプリケーションについて説明します。個別のレプリケーション計画作成の詳細については、「オフホストのデータ処理」を参照してください。

バックアップのレプリケーションを有効にすると、各バックアップは作成後すぐ別のロケーションにコピーされます。以前のバックアップがレプリケートされなかった（たとえば、ネットワーク接続が失われた）場合、最後に成功したレプリケーションのあとに表示されたバックアップもすべてレプリケートされます。

レプリケートされたバックアップは、元のロケーションに残るバックアップには依存しません。逆も同じです。他のロケーションにアクセスすることなく、すべてのバックアップからデータを復元できます。

使用例

- **信頼性の高い災害復旧計画**
  オンサイト（その場での復元）とオフサイト（ローカル ストレージの障害や自然災害などからのバックアップの保護）の両方でバックアップを保存します。
- **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**
  コストの高い記憶域スペースを使い過ぎないようにするために、保持ルールに従って、高速ストレージから古いバックアップを削除します。

サポートされるロケーション

次のロケーションからバックアップをレプリケートできます。

- ローカル フォルダ
- ネットワーク フォルダ
- Secure Zone
- SFTPサーバー
- Storage Nodeによって管理されるロケーション

次のロケーションにバックアップをレプリケートできます。

- 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
- SFTPサーバー
- Storage Nodeによって管理されるロケーション
- テープ デバイス

バックアップのレプリケーションを有効にするには

1. 保護計画パネルで、**[ロケーションの追加]** をクリックします。
   [ロケーションの追加] コントロールは、最後に選択したバックアップまたはレプリケーションのロケーションからのレプリケーションがサポートされる場合にのみ利用できます。
2. バックアップのレプリケーション先となるロケーションを指定します。
3. [オプション] **[保持期間]** で、「保持ルール」の説明に従い、選択したロケーションの保持ルールを変更します。
4. （オプション）**[VMに変換]** で、「仮想コンピュータへの変換」の説明に従い、仮想コンピュータへの変換の設定を指定します。
5. （オプション）[ギアアイコン] > [**パフォーマンスとバックアップウィンドウ**] の順にクリックし、「パフォーマンスとバックアップウィンドウ」に記述されている通り、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。これらの設定は、レプリケーションパフォーマンスを定義します。
6. （オプション）バックアップをレプリケートするすべてのロケーションについて、手順1～5を繰り返します。プライマリロケーションを含めて連続5ロケーションまでのコピーまたは移動がサポートされています。

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"（344ページ）」を参照してください。

Advancedライセンスを持つユーザーのための考慮事項

ヒント

クラウドストレージからのバックアップのレプリケーションを設定するには、別のレプリケーション計画を作成します。詳細については、「オフホストのデータ処理」を参照してください。

制限事項

- Storage Nodeで管理されるロケーションからローカルフォルダへのバックアップのレプリケーションはサポートされていません。ローカル フォルダは、バックアップを作成したエージェントがインストールされているコンピュータ上のフォルダを意味します。
- 重複除外を有効にした管理対象ロケーションへのバックアップのレプリケーションは、バックアップ形式が**バージョン12**であるバックアップではサポートされません。

操作を実行するコンピュータ

バックアップのレプリケーションは、どのロケーションからであっても、バックアップを作成したエージェントによって開始され、次のように実行されます。

- ロケーションがStorage Nodeの管理対象でない場合、そのエージェントによって実行されます。
- ロケーションが管理対象である場合、対応するStorage Nodeによって実行されます。ただし、管理されたロケーションからクラウドストレージへのバックアップのレプリケーションは、バックアップを作成したエージェントによって実行されます。

以上の説明から分かるとおり、操作が実行されるのは、エージェントが存在するコンピュータの電源がオンになっている場合のみです。

管理されたロケーション間のバックアップのレプリケーション

1つの管理対象ロケーションから別の管理されたロケーションへのバックアップのレプリケーションは、Storage Nodeによって実行されます。

ターゲットのロケーションに対する重複除外が有効な場合（異なるStorage Node上に存在する可能性があります）、ソースStorage Nodeは、ターゲットのロケーションに存在しないデータのブロックのみを送信します。言い換えると、エージェントと同じように、Storage Nodeがソースでの重複除外を実行します。これにより、地理的に離れたストレージ ノード間でデータをレプリケートするときにネットワーク トラフィックが節約されます。

手動でのバックアップの開始

1. 保護計画が少なくとも1つ適用されているマシンを選択します。
2. **[バックアップ]** をクリックします。
3. 複数の保護計画が適用されている場合は、保護計画を選択します。
4. 次のいずれかを実行します。
   - **[今すぐ実行]** をクリックします。増分バックアップが作成されます。
   - バックアップスキームに幾つかのバックアップ方法が含まれる場合、使用する方法を選択できます。**[今すぐ実行]** ボタンの矢印をクリックし、**[完全、増分]** または **[差分]** を選択します。

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です。

バックアップの進行状況が、コンピュータの **[ステータス]** 列に表示されます。

バックアップ オプション

重要
このセクション内に記載されているいくつかの機能は、オンプレミスデプロイメントでのみ使用できます。

バックアップオプションを変更するには、保護計画名の横にあるギアアイコンをクリックして、[**バックアップオプション**] 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	Scale Computing	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）	+	-	-	-	-	-	+	+	+	+
クラスタバックアップモード	-	-	-	-	-	-	-	-	-	+
圧縮レベル	+	+	+	+	+	+	+	+	+	+
電子メールによる通知	+	+	+	+	+	+	+	+	+	+
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										
ファイルフィルタ	+	+	+	+	+	+	+	+	+	-
ファイルレベルのバックアップのスナップショット	-	-	-	+	+	+	-	-	-	-
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										
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	+	+	+	+	+	+	+	-	-	+
SAN ハードウェアスナップ	-	-	-	-	-	-	+	-	-	-

ショット										
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	+	+	+	+	+	+	+	+	+	+
テープ管理	+	+	+	+	+	+	+	+	+	+
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）	+	-	-	+	-	-	-	+	-	+
仮想コンピュータ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。

- バックアップ先がテープデバイスまたは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。

テープに保存されているバックアップを統合することはできません。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。テープに保存されたバックアップは、テープが上書きまたは消去された場合にのみ GUI から消えます。

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。

これらの名前は、ファイルマネージャでバックアップロケーションを参照する際に確認できます。

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（従来の形式）
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	

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呼ばれる）は、保護計画の作成時または編集時に定義できます。

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。

バックアップファイル名を変更すると、次回のバックアップが完全バックアップになります。ただし、同じコンピュータの既存のバックアップのファイル名を指定した場合を除きます。既存のファイル名を指定した場合は、保護計画のスケジュールに応じて、完全バックアップ、増分バックアップ、差分バックアップのいずれかが作成されます。

ファイルマネージャから参照できないロケーション（クラウドストレージ、テープデバイスなど）のバックアップファイル名を設定できることに注意してください。これは、**[バックアップストレージ]** タブでカスタム名を表示する場合に役立ちます。

バックアップファイル名が表示される場所

[バックアップストレージ] タブを選択し、バックアップのグループを選択します。

- 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。

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。

デフォルトのバックアップファイル名

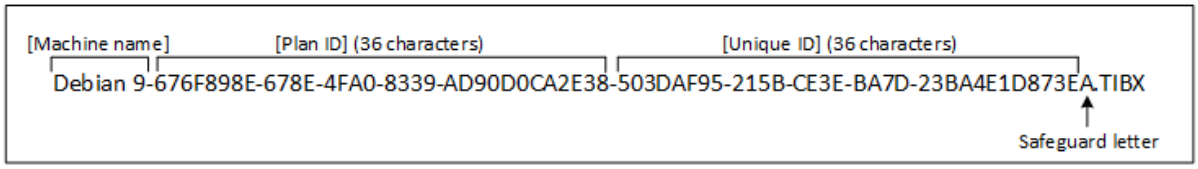
デフォルトのバックアップファイル名は、**[マシン名]**-**[計画 ID]**-**[一意の ID]**Aです。

メールボックス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、**[メールボックス ID]**_**メールボックス**_**[計画 ID]**Aです。

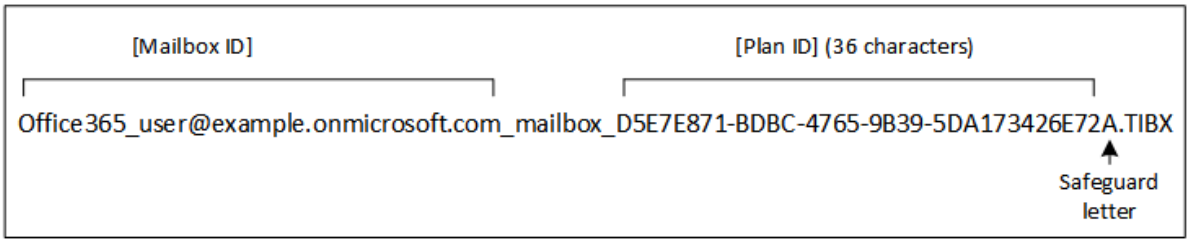
名前は次の変数で構成されます。

- **[マシン名]** この変数は、バックアップされるデータの種類に関係なく（Microsoft 365メールボックスを除く）、マシン名（Cyber ProtectWeb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。Microsoft 365メールボックスの場合は、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。
- **[計画 ID]** この変数は、保護計画の固有の ID 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。
- **[一意の ID]** この変数は、選択したマシンまたはメールボックスの固有の ID に置き換えられます。マシンの名前またはメールボックスのUPNを変更しても、この値は変更されません。
- **[メールボックス ID]** この変数はメールボックスの UPN に置き換えられます。
- 「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、メールボックス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
...
```

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11形式の場合:

```
MyBackup.xml
MyBackup.tib
```

その他のバックアップスキームを設定したバージョン11形式の場合:

```
MyBackup.xml
MyBackup_2016_9_13_14_49_20_403F.tib
MyBackup_2016_9_14_14_43_00_221F.tib
MyBackup_2016_9_15_14_45_56_300F.tib
...
```

変数の使用

デフォルトで使用される変数のほかに、保護計画名に置き換えられる **[計画名]** 変数を使用できます。

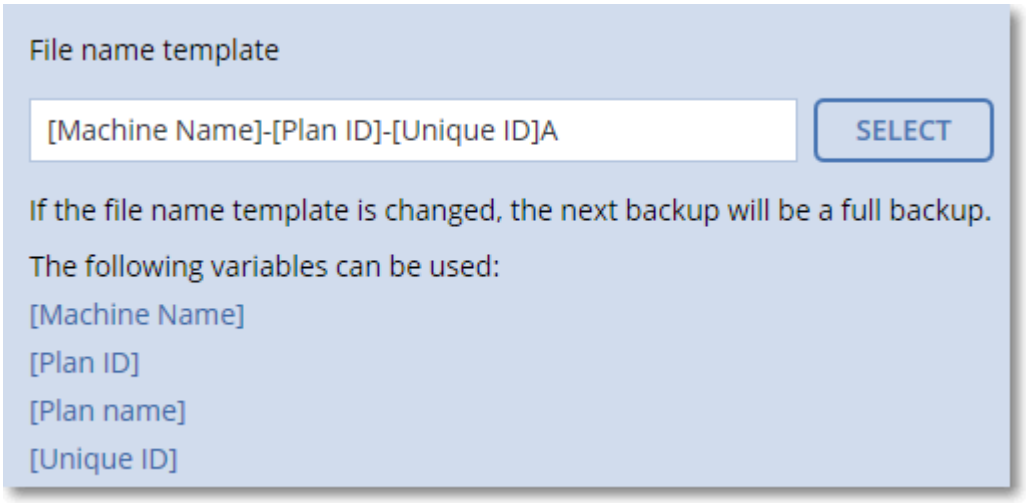
バックアップ対象として複数のマシンまたはメールボックスを選択する場合は、バックアップファイル名に **[マシン名]**、**[メールボックス ID]**、または **[一意の ID]** 変数を含める必要があります。

バックアップファイル名と単純化されたファイル名

プレーンテキストや変数を使用すると、以前の Acronis Cyber Protect バージョンで使用していたのと同じファイル名を作成できます。ただし、単純化されたファイル名を再作成することはできません。バージョン12では、単一ファイル形式を使用した場合を除き、ファイル名にはタイムスタンプが付加されます。

使用例

- **ユーザーフレンドリーなファイル名を表示する**
  ファイルマネージャ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。
- **既存のバックアップシーケンスを続行する**
  保護計画を 1 台のマシンに適用し、Cyber Protect ウェブ コンソールからこのマシンを削除するか、エージェントと構成設定をアンインストールする必要があると仮定します。マシンを追加し直した後か、エージェントをインストールし直した後に、保護計画を強制的に実行して、同じバックアップまたはバックアップシーケンスを続行できます。これを実行するには、保護計画のバックアップオプションで **[ファイル名をバックアップ]** をクリックしてから、**[選択]** をクリックして任意のバックアップを選択します。
  [参照] ボタンをクリックすると、保護計画ペインの **[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。このロケーション以外は参照できません。



- **以前の製品バージョンからアップグレードする**
  アップグレード中に保護計画が自動的に移行されなかった場合は、計画を作成し直して、古いバックアップファイルを指すように指定します。バックアップ対象として1台のマシンのみを選択した場合は、**[参照]** をクリックして、目的のバックアップを選択します。バックアップ対象として複数のマシンを選択した場合は、変数を使用して古いバックアップファイル名を作成し直します。

注意
単一のデバイス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。

バックアップ形式

このオプションは、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。レガシーバックアップ形式のバージョン11を使用する保護計画でのみ使用できます。この場合、新しい形式のバージョン12に変更できます。この変更を行った後は、オプションが使用できなくなります。

このオプションは、メールボックスのバックアップの場合は選択できません。メールボックスのバックアップの形式は、必ず新しい形式です。

デフォルト設定:**自動選択**。

次のいずれかを選択できます。

- **自動選択**
  以前の製品バージョンで作成された保護計画でバックアップを追加しない場合は、バージョン 12 の形式が使用されます。
- **バージョン12**
  高速バックアップ・復元には、この新しい形式が推奨されます。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。
  この形式では、保持ルールとして **[バックアップの合計サイズ別]** を選択することはできません。
- **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。以前の製品バージョンで作成されたバックアップの最後にバックアップを追加することができます。
  完全、増分、差分バックアップを別々のファイルで保存する場合は、この形式を使用します（**[常に増分（単一ファイル）]**を除くすべてのバックアップスキーム）。
  この形式は、バックアップ先（またはレプリケーション先）の管理対象ロケーションで、重複除外または暗号化が有効になっている場合に、自動的に選択されます。形式を **[バージョン12]** に変更すると、バックアップは失敗します。

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。ファイル名を定義するには、[バックアップファイル名] オプションを使用します。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（従来の形式）
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	

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。
- バックアップ先（またはレプリケーション先）が、重複除外が有効になっている管理対象ロケーションである場合には、バックアップが失敗します。

アーカイブ内の重複除外

バージョン12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。

アーカイブ内の重複除外はクライアント側の重複除外を使用します。次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。

バックアップのベリファイ

ベリファイは、バックアップからデータを復元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、作成後すぐにベリファイされます。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**。

ベリファイでは、バックアップから復元されるすべてのデータブロックのチェックサムが計算されます。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、ベリファイされます。

サイズの小さい増分/差分バックアップでも、ベリファイには時間がかかります。これは、バックアップに物理的に含まれているデータだけでなく、バックアップの選択によって復元可能となったすべての

データもベリファイされるためです。このベリファイには、以前に作成したバックアップへのアクセスが必要となります。

ベリファイの成功は復元の成功の可能性が高いことを示しますが、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。オペレーティングシステムをバックアップする場合、ブータブルメディアから予備のハードドライブに復元テストを実行するか、ESXiまたはHyper-Vの環境でバックアップから仮想マシンを実行することをおすすめします。

Changed Block Tracking（CBT）

このオプションは、仮想マシンとWindowsを実行する物理マシンのディスクレベルのバックアップで有効です。これは、Microsoft SQL Serverデータベースおよび Microsoft Exchange Serverデータベースのバックアップでも有効です。

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

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:**可能な場合はパッシブコピー**。

次の中からひとつ選択できます。

- **可能な場合はパッシブコピー**
  すべてのパッシブコピーがオフラインの場合、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

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。

電子メールによる通知

このオプションでは、バックアップ中に発生したイベントに関する電子メールによる通知を設定できます。

このオプションを使用できるのは、オンプレミスの配置のみです。クラウドの配置では、デフォルトの設定は、アカウント作成時にアカウントごとに設定されます。

デフォルト設定:**システム設定を使用します。**

システム設定を使用するか、この計画専用にカスタマイズされた値でデフォルトの設定を上書きできます。 システム設定は「電子メールによる通知」に説明されている方法で構成されます。

重要
システム設定が変更されると、システム設定を使用するすべての保護計画に影響を及ぼします。

このオプションを有効にする前に、**電子メールサーバー**設定が構成されていることを確認します。

保護計画に関するEメール通知をカスタマイズするには

1. **[この保護計画の設定をカスタマイズ]** を選択します。
2. **[受信者の電子メールアドレス]** フィールドに送信先電子メールアドレスを入力します。複数のアドレスをセミコロンで区切って入力することもできます。
3. （オプション）**[件名]** で、電子メール通知の件名を変更します。
   たとえば次のような変数を使用できます。
   - **[アラート]** - アラート概要。
   - **[デバイス]** - デバイス名。
   - **[計画]** - アラートが生成された計画の名前。
   - [ManagementServer] - 管理サーバーがインストールされているマシンのホスト名。
   - **[部署]** - マシンが属している部署名。

   デフォルトの件名は、**[アラート] デバイス: [デバイス] 計画: [計画]**

4. 通知を受信するイベントのチェックボックスを選択します。バックアップ中に発生するすべてのアラートのリストから選択できます（重要度別）。

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。

たとえば、ネットワーク上のバックアップ保存先が使用できないか、接続できない場合、30秒ごとに30回までバックアップ保存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。

クラウドストレージ

クラウドストレージをバックアップ先として選択すると、オプション値が自動的に **[有効]** に設定されます。**試行回数:300。試行間隔:30 秒。**

この場合、実際の試行回数は無制限ですが、バックアップの失敗前のタイムアウトは次のように計算されます。（300 秒 + **試行間隔**） * （**試行回数** + 1）。

例：

- デフォルト値では、（300 秒 + 30 秒） * （300 + 1） = 99330 秒、つまり～ 27.6 時間後にバックアップが失敗します。
- **試行回数**を 1 に、**試行間隔** 1 秒に設定すると、（300 秒 + 1 秒） * （1 + 1） = 602 秒、または約 10 分後にバックアップが失敗します。

計算されたタイムアウトが 30 分を超え、データ転送がまだ開始されていない場合、実際のタイムアウトは 30 分に設定されます。

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。

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

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できます。

ファイルフィルタは、特に記載がない限り、ディスクレベルとファイルレベルの両方のバックアップで使用できます。

ファイルフィルタは、エージェントレスモードで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）への適用には有効になりません。

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]** 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。

特定の条件に一致するファイルを含めるか除外する

反対に機能する2つのオプションがあります。

- **次の条件と一致するファイルだけをバックアップする**
  例:コンピュータ全体のバックアップを選択し、フィルタ条件で **C:¥File.exe** を指定した場合、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] で **[バージョン11]** が選択されており、バックアップ先がクラウドストレージでない場合は、ファイルレベルのバックアップではこのフィルタは無効になります。

- **次の条件に一致するファイルをバックアップしない**
  例:コンピュータ全体のバックアップを選択し、フィルタ条件で **C:¥File.exe** を指定した場合、このファイルのみがスキップされます。

両方のオプションは同時に使用できます。その場合、後のオプションが前のオプションより優先されます。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。

条件

- **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 と Linux/macOS いずれの場合も、ファイルまたはフォルダのパスにスラッシュを使用できます（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。

  フルパスフィルタには、ドライブ文字（Windows の場合）やルートディレクトリ（Linux や macOS の場合）が含まれます。たとえば、ファイルのフルパスは **C:¥TempFile.tmp** のようにとなります。ドライブ文字やルートディレクトリを含むフィルタ（**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（たとえば、**Temp¥*** や **Temp¥File.tmp**）や、アスタリスクで始まるフィルタ（たとえば、***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。

- **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。

条件では、名前は大文字/小文字は区別されません。たとえば、**C:¥Temp** を指定した場合、**C:¥TEMP** と **C:¥temp** などが選択されます。

1 つ以上のワイルドカード文字（*、**、?）を条件に使用できます。これらの文字は、フルパス内でもファイルまたはフォルダ名でも使用できます。

ファイル名でアスタリスク（*）は 0 個以上の文字の代用として使用できます。たとえば、**Doc*.txt** という条件は **Doc.txt** や **Document.txt** などのファイルと一致します。

（**バージョン12**形式のバックアップのみ）ファイル名とパスに2つ並んだアスタリスク（**）を含めると、0個以上の文字（スラッシュを含む）の代用として使用できます。たとえば、「****/Docs/**.txt**」という条件は、「**Docs**」というフォルダ配下、およびそのすべてのサブフォルダ配下にある、すべてのテキストファイル（.txt）と一致します。

ファイル名で疑問符（?）は厳密に 1 文字として代用されます。たとえば、**Doc?.txt** という条件は、**Doc1.txt** や **Docs.txt** などのファイルと一致しますが、**Doc.txt** や **Doc11.txt** などのファイルとは一致しません。

非表示のファイルとフォルダをすべて除外する

このチェック ボックスを選択すると、**隠しファイル**属性が指定されたファイルおよびフォルダ（Windows によってサポートされているファイル システムの場合）またはピリオド（.）で始まるファイルおよびフォルダ（Ext2 や Ext3 など、Linux のファイル システムの場合）がスキップされます。フォルダが隠しファイルの場合、フォルダの内容は（隠しファイルになっていないファイルを含み）すべて除外されます。

システムファイルとフォルダを除外する

このオプションは、Windows対応のファイル システムでのみ有効です。**システム**属性が指定されているファイルとフォルダをスキップする場合は、このチェック ボックスをオンにします。フォルダに**システム**属性が指定されている場合、フォルダの内容は（**システム**属性が指定されていないファイルも含めて）すべて除外されます。

注意
ファイル属性またはフォルダ属性は、ファイル/フォルダのプロパティ内で表示できるほか、属性コマンドを使用して表示することも可能です。詳細については、Windows の [ヘルプとサポート センター] をご参照ください。

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**
  常にファイルを直接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

ウイルスやマルウェアやランサムウェアによって、マシンで不正なアクティビティが実行されることがあります。いろいろなプログラムによってマシンのデータが盗まれたり変更されたりするケースについても調査が必要です。そうしたアクティビティについて調査が必要だとしても、デジタル痕跡がマシンに残っていなければ、調査は不可能です。残念ながら、痕跡（ファイルやトレースなど）が削除されたり、マシン自体が使用不可になったりすることもあります。

[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で使用できるデジタル痕跡を収集できます。デジタル痕跡として使用できるのは、使用されていないディスクスペースのスナップショット、メモリダンプ、実行中のプロセスのスナップショットです。**[フォレンジックデータ]** 機能は、マシン全体のバックアップでしか使用できません。

現時点で **[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OSバージョンのWindowsマシンだけです。

- Windows 8.1、Windows 10
- Windows Server 2012 R2～Windows Server 2019

注意

• バックアップモジュールを組み込んだ保護計画をマシンに適用した後に、フォレンジックデータ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ます。

• フォレンジックデータ収集を使用したバックアップは、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には対応していません。

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サポートされているのは、以下の場所です。

- クラウドストレージ
- ローカルフォルダ

注意
1.ローカルフォルダの場合は、USBで接続した外付けハードディスクのローカルフォルダだけがサポートされています。
2.ローカルダイナミックディスクは、フォレンジックバックアップの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通常含まれないディスク領域を分析できます。

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 ウェブ 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、**[計画]** 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. **[ダッシュボード]** > **[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 ウェブ 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、**[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。

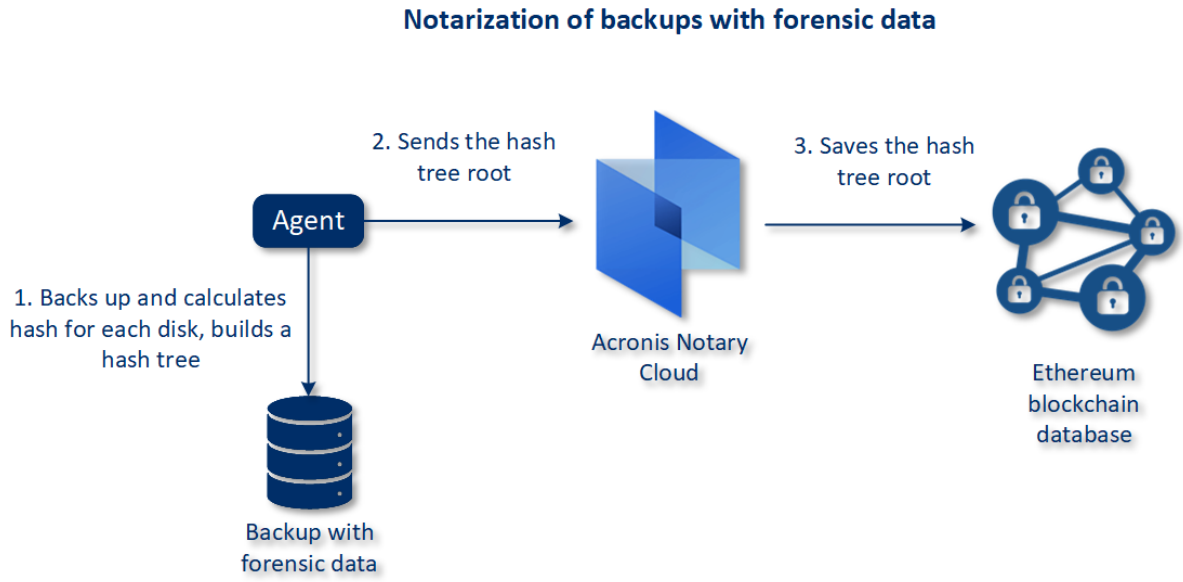
エージェントはバックアップ時に、バックアップディスクのハッシュコードを計算し、ハッシュツリーを作成し、そのツリーをバックアップに保存し、ハッシュツリーのルートをノータリー（公証）サービスに送信します。ノータリー（公証）サービスで、ハッシュツリーのルートが Ethereum ブロックチェーンデータベースに保存され、この値が変更されていないことが確認されます。

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 Protect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。以下の場所にあります。`C:\Program Files\Acronis\BackupAndRecovery`.

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\Default\<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
```

```
Output template:
```

```
GUID   Date   Date timestamp
----   ------ --------------
<guid> <date> <timestamp>
```

<guid> - バックアップGUID。

<date> - バックアップの作成日。次の形式になります:DD.MM.YYYY HH24:MM:SS。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-256アルゴリズムを使用して復元ポイントの指定の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	ウェブ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アドレス> - 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
	<証明書パス> - Cyber 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 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。バックアップが高速に進み、ボリュームグループに未割り当て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デフォルトを変更することをおすすめします。
- **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。

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**。
- マシンが選択されていない場合（[**計画**] > [**バックアップ**] ページで保護計画の作成から開始した場合に該当します）:**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

ユーザーはワンクリック復元を使用して、マシンの最新のディスクバックアップから自動リカバリを実行できます。これは、マシン全体のバックアップ、またはこのマシンの特定のディスクやボリュームのバックアップになります。

この機能は、管理者がStartup Recovery Managerとともに有効化した後、ユーザーのマシンからアクセスできるようになります。管理者がこの操作を実行する場合、必ずコマンドラインインターフェースを使用する必要があります。Startup Recovery Managerおよびワンクリック復元を有効化する方法については、『コマンドラインリファレンス』を参照してください。

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:

1. Secure Zone
2. ネットワークストレージ
3. クラウドストレージ

特定のタイプのストレージが利用できないか、そのストレージにディスクバックアップがない場合、ユーザーに次のタイプのストレージを使用するように促すメッセージが表示されます。

ディスクバックアップを含む複数のバックアップセット（アーカイブとも呼ばれる）がストレージに存在する場合、ワンクリック復元では、前回アップデートされたバックアップセットが選択されます。ユーザーは別のバックアップセットを選択することはできません。

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
- 自動的に選択されたバックアップセット内の特定のバックアップ（復元ポイントとも呼ばれる）からの復元

ワンクリック復元でマシンをリカバリする

前提条件

- 管理者が選択したマシンのワンクリック復元を有効化しました。
- 選択したマシンについて、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。
3. 任意の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、キーボードの1キーを押します。
   - 前回アップデートされたバックアップセットに含まれる別のバックアップをリカバリするには、キーボードの2キーを押します。
     - 任意のバックアップ（復元ポイントとも呼ばれる）を選択するには、キーボードの該当する数字キーを押します。

グラフィックユーザーインターフェースが起動し、その後表示されなくなります。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。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。

保護計画で指定したロケーションごとに、このオプションを別々に設定できます。レプリケーションロケーションに対してこのオプションを設定するには、ロケーション名の横にあるギアアイコンをクリックし、[**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。

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、仮想マシンへの変換）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の場合は **[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。

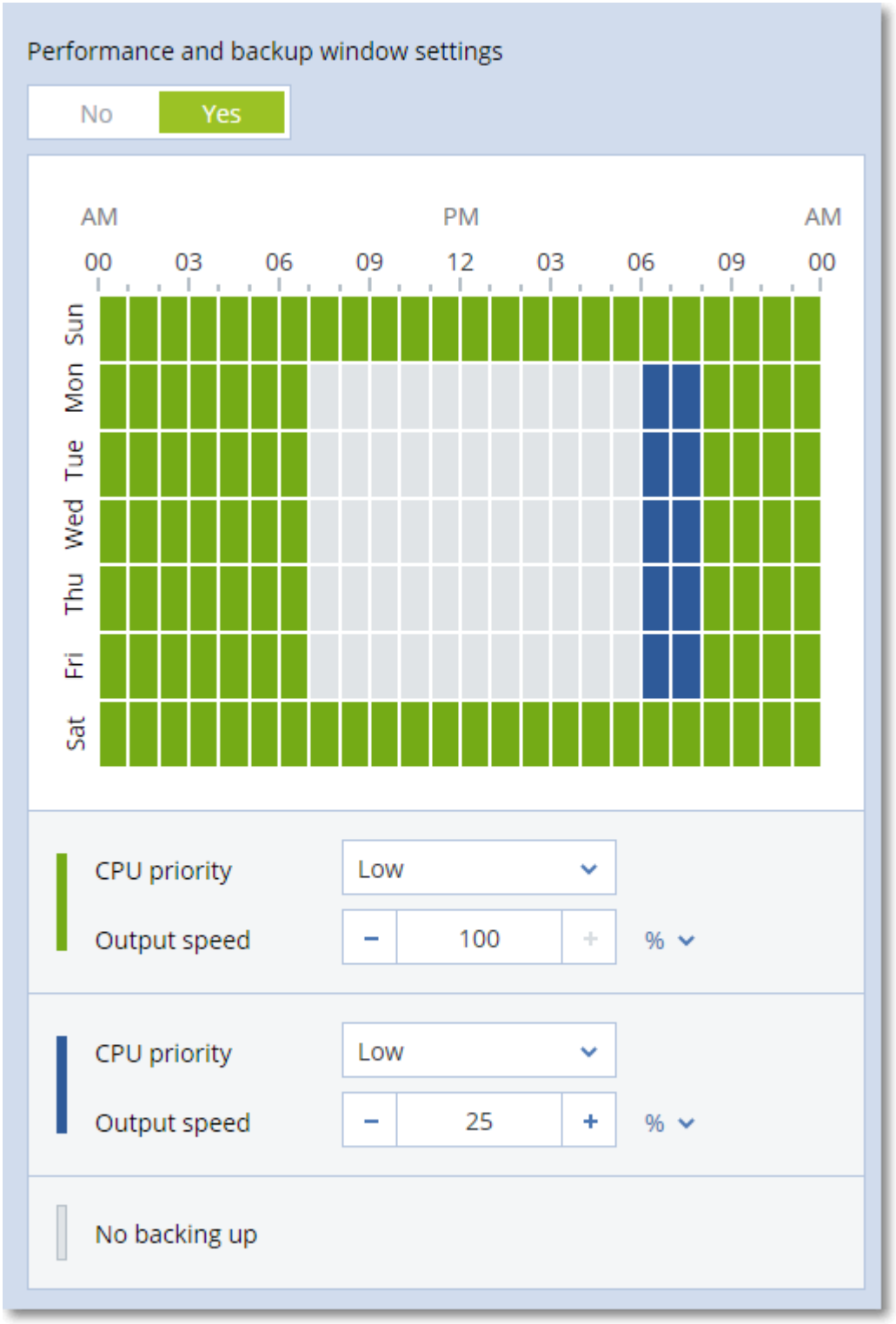
スケジュール済みバックアップがブロックされても、バックアップは手動で開始できます。最後にバックアップが許可された時間のパフォーマンスパラメーターが使用されます。

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。

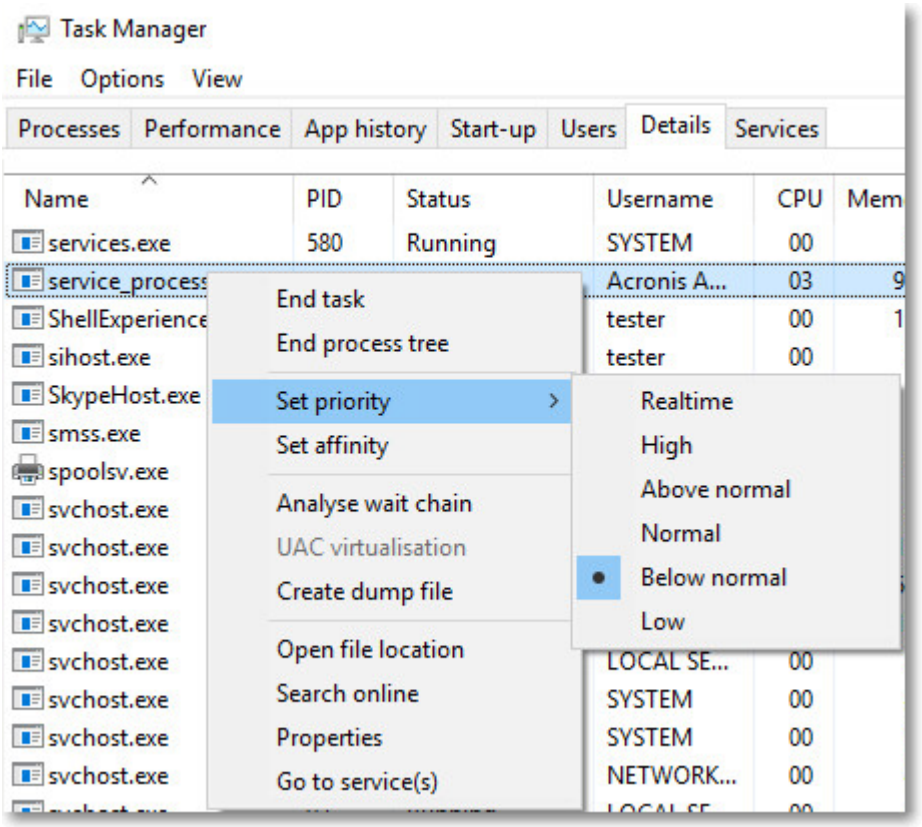
低 - Windowsの場合は **[通常以下]** に相当。

通常 - Windowsの場合は **[通常]** に相当。

高: - Windowsの場合は **[高]** に相当します。

この設定では、バックアップ処理に割り当てられるCPUとシステムリソースの量を決定します。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。

このオプションでは、Windowsではバックアッププロセスの優先度（**service_process.exe**）、LinuxやOS Xではバックアッププロセスのnice値（**service_process**）を設定します。



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有効です。

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、およびHyper-V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。ブータブルメディアの下で作成されるバックアップはサポートされていません。

このオプションは、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、物理データ配送サービスを使用して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かどうかを決定します。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。

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、オンプレミスデプロイの組織管理者およびクラウドデプロイメントの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. 新しい保護計画を作成します。この計画では、**物理データ配送**バックアップオプションを有効にします。
   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。

   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。

2. 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インターフェースにアクセスするには、次のいずれかを実行します。
   - オンプレミス配置の場合: Acronisアカウントにログインし、**[物理データ配送]** の下にある **[トラックコンソールに移動する]** をクリックします。
   - クラウドデプロイの場合: 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。
3. 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』で説明する梱包手順に必ず従ってください。

4. 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。

このプログラムでは、ポストバックアップコマンドを実行した後でレプリケーションが実行されます。

「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。

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、データ取り込み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。

<table>
<tr><td></td><td colspan="4"><---------- バックアップ ----------
-----></td><td></td></tr>
<tr><td>バックアップ前に実行するコマンド</td><td>データ取り込みの前に実行するコマンド</td><td colspan="2">データ取り込み</td><td>データ取り込みの後に実行するコマンド</td><td>バックアップ後に実行するコマンド</td></tr>
</table>

[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た場合、コマンドの実行とMicrosoft VSSアクションの順序は次のようになります。

「データ取り込み前」のコマンド→ VSS の一時停止→データ取り込み→ VSS の再開→「データ取り込み後」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	オン	オン	オフ	オフ

実行しない]				
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。

* 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。

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。

SANハードウェアスナップショット

このオプションは、VMware ESXi仮想コンピュータのバックアップに対して有効です。

デフォルト設定:**無効**。

このオプションでは、バックアップの実行時にSANスナップショットを使用するかどうかを指定します。

このオプションが無効の場合、仮想ディスクの内容はVMwareスナップショットから読み取られます。スナップショットは、バックアップが処理されている間保持されます。

このオプションが有効の場合、仮想ディスクの内容はSANスナップショットから読み取られます。VMwareスナップショットは、仮想ディスクを整合性のとれた状態にするために作成され、短期間保持されます。SANスナップショットから読み取り不可の場合、バックアップは失敗します。

このオプションを有効にする前に、「SANハードウェアスナップショットの使用」に挙げられている要件を確認して実施してください。

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コンピュータは何台かを定義します。

デフォルト設定:

- オンプレミスデプロイ:**すべてのバックアップを正確にスケジュール通りに開始する。**
- クラウドデプロイ:**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**
  このオプションは、保護計画が複数の仮想マシンに対して適用された場合にのみ利用できます。このオプションでは、指定された保護計画の実行時にエージェントが同時にバックアップを実行できる仮想マシンの数を定義します。
  エージェントが保護計画に従って複数のマシンのバックアップを一度に開始する必要がある場合、2台のマシンが選択されます。（バックアップのパフォーマンスを最適化するために、エージェントは

別のストレージに格納されているコンピュータを一致させようとします）。2 つのバックアップのいずれかが完了すると、エージェントは 3 番目のコンピュータを選択し、以降同様に選択していきます。

エージェントが同時にバックアップできる仮想コンピュータの数は変更できます。最大値は 10 です。ただし、時間が重複する複数の保護計画がエージェントによって実行されている場合、それらのオプションで指定された数が合計されます。実行されている保護計画の数にかかわらず、エージェントで同時にバックアップできる仮想マシンの合計数を制限できます。

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。

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

このオプションは、**[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]** の各バックアップスキームで有効です。

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。

デフォルト設定:**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。

テープ管理

以下のオプションは、バックアップ先がテープ デバイスである場合に有効です。

テープに保存されたディスクのバックアップからのファイルの復元を有効にする

デフォルト設定:**無効**。

このチェック ボックスをオンにすると、それぞれのバックアップで、テープデバイスが接続されているマシンのハードディスクにソフトウェアが補助ファイルを作成します。これらの補助ファイルがそのままの状態を保持していれば、ディスク バックアップからファイルを復元できます。 それぞれのバックアップが保存されているテープが消去、削除、または上書きされると、これらのファイルは自動的に削除されます。

補助ファイルのロケーションは、次のとおりです。

- Windows XPおよびServer 2003の場合: **%ALLUSERSPROFILE%¥Application Data¥Acronis¥BackupAndRecovery¥TapeLocation**。
- Windows 7およびそれ以降のバージョンのWindowsの場合: **%PROGRAMDATA%¥Acronis¥BackupAndRecovery¥TapeLocation**。
- Linuxの場合: **/var/lib/Acronis/BackupAndRecovery/TapeLocation**。

これらの補助ファイルで占有される領域は、それぞれのバックアップのファイル数によって異なります。約 20,000 ファイルを含むディスクの完全バックアップの場合（通常のワークステーション ディスクのバックアップ）、補助ファイルは約 150 MB を占有します。250,000 ファイルを含むサーバーの完全バックアップでは、約 700 MB の補助ファイルが生成されます。個別のファイルを復元する必要がない場合は、このチェック ボックスをオフにしたままにしてディスク領域を節約できます。

バックアップ中に補助ファイルが作成されなかった、または削除された場合でも、そのバックアップを格納したテープを再スキャンすると補助ファイルを作成できます。

各マシンの正常なバックアップの後にテープをスロットに戻す

デフォルト設定:**有効**。

このオプションを無効にすると、テープを使用した操作が完了した後にテープがドライブ内に残ります。そうでない場合、テープは操作前にあったスロットに戻されます。保護計画に従って、バックアップに続いて他の操作（バックアップのベリファイや他のロケーションへのレプリケーションなど）が実行される場合、テープはそれらの操作の終了後にスロットに戻されます。

このオプションと [**各マシンのバックアップが正常に終了した後にテープを取り出す**] オプションの両方が有効な場合、テープが取り出されます。

各マシンの正常なバックアップの後にテープを取り出す

デフォルト設定:**無効**。

このチェックボックスがオンの場合、各コンピュータのバックアップが正常に終了するとテープが取り出されます。保護計画に従って、バックアップに続いて他の操作（バックアップのベリファイや他のロケーションへのレプリケーションなど）が実行される場合、テープはそれらの操作の終了後に取り出されます。

完全バックアップの作成時にスタンドアロン テープドライブのテープを上書きする

デフォルト設定:**無効**。

このオプションは、スタンドアロンのテープ ドライブにのみ適用されます。このオプションを有効にすると、完全バックアップが作成されるたびにドライブに挿入されているテープが上書きされます。

次のテープデバイスとドライブを使用する

このオプションで、保護計画で使用されるテープデバイスとテープドライブを指定できます。

テーププールには、Storage Node、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、またはその両方のマシンに接続されている、すべてのテープデバイスのテープが含まれます。テーププールをバックアップロケーションとして選択すると、テープデバイスが接続されているマシンを間接的に選択することになります。デフォルトでは、バックアップによって、そのマシンに接続されている任意のテープデバイスの任意のテープドライブを介してテープに書き込むことができます。デバイスまたはドライブの一部が見つからないか操作できない場合、保護計画では、使用可能なものが使用されます。

[**選択したデバイスとドライブのみ**] をクリックして、一覧からテープデバイスとテープドライブを選択することができます。1 つのデバイス全体を選択すると、そのデバイスのすべてのドライブが選択されます。これは、保護計画で、そのうちのどのドライブでも使用できることを意味します。選択したデバイスまたはドライブが見つからないか操作できない場合、他のデバイスを選択しなければ、バックアップは失敗します。

このオプションを使用することで、複数のエージェントで実行される、複数のドライブを持つ大型のテープライブラリへのバックアップを制御できます。たとえば、大型のファイルサーバーまたはファイル共有のバックアップは、同じバックアップウィンドウに複数のエージェントがマシンをバックアップする場合は開始されないことがあります。その理由は、これらのエージェントによってすべてのドライブが占有されるためです。エージェントにドライブ 2 とドライブ 3 の使用を許可すると、ドライブ 1 がファイル共有をバックアップするエージェント用に予約されます。

マルチストリーミング

デフォルト設定:**無効**。

マルチストリーミングを使用すると、1つのエージェントからのデータを複数のストリームに分割し、それらのストリームを同時に異なるテープに書き込むことができます。これにより、バックアップ時間が短縮されます。マルチストリーミングは、テープドライブと比較してエージェントのスループットが高いときに特に有効です。

[**マルチストリーミング**] チェックボックスは、[**選択したデバイスとドライブのみ**] オプションで2台以上のテープドライブを選択したときのみ使用可能になります。選択したドライブの台数がエージェントからの同時ストリームの数になります。選択したドライブがバックアップ開始時に使用できない場合、そのバックアップは失敗します。

マルチストリーミングまたはマルチストリーミングとマルチプレクシングの両方によって作成されたバックアップで復元するには、そのバックアップの作成に使用したのと同じかそれ以上の台数のドライブが必要です。

既存の保護計画のマルチストリーミング設定は変更できません。別の設定を使用するか選択したテープドライブを変更するには、新しい保護計画を作成します。

マルチストリーミングは、ローカルに接続されたテープドライブとストレージノードに接続されたテープドライブの両方で使用できます。

マルチプレクシング

デフォルト設定:**無効**。

マルチプレクシングを使用すると、複数のエージェントからのデータストリームを単一のテープに書き出すことができます。これにより、高速のテープドライブを有効活用できます。デフォルトでは、マルチプレクシング係数（単一のテープにデータを送信するエージェントの数）は2に設定されています。マルチプレクシング係数は10まで上げることができます。

マルチプレクシングは、多数のバックアップ操作が実行される大規模環境で使用すると便利です。ただし、マルチプレクシングによって単一バックアップのパフォーマンスが向上することはありません。

大規模環境で最速のバックアップを達成するには、エージェント、ネットワーク、テープドライブのスループットを分析する必要があります。その後、分析結果に従ってマルチプレクシング係数を設定します。これにより、過剰マルチプレクシングを避けることができます。たとえば、エージェントのデータ転送速度が70Mbit/s、テープドライブの書き込み速度が250Mbit/sで、ネットワークでボトルネックが発生していない場合は、マルチプレクシング係数を3に設定します。このときマルチプレクシング係数を4にすると、過剰マルチプレクシングとなり、バックアップのパフォーマンスが低下します。通常、マルチプレクシング係数は2〜5に設定します。

構造上、マルチプレクシングによって作成されたバックアップの復元は低速になります。マルチプレクシング係数が大きいほど、復元に時間がかかります。1つのマルチプレクシングテープに書き込まれた複数のバックアップを同時に復元することはできません。

マルチプレクシング用に1つ以上の個々のテープドライブを明示的に選択することもできますし、使用可能な任意のテープドライブにマルチプレクシングオプションを使用することもできます。マルチプレクシングは、ローカル接続のテープドライブには使用できません。

既存の保護計画のマルチプレクシング設定は変更できません。別の設定を使用するには、新しい保護計画を作成します。

保護計画では、マルチストリーミングとマルチプレクシングを次のように組み合わせて使用できます。

- **マルチストリーミングとマルチプレクシングのオプションを両方ともオフにします。**
  各エージェントが単一のテープドライブにデータを送信します。
- **マルチストリーミングオプションのみ選択します。**
  各エージェントが2台以上のテープドライブに同時にデータを送信します。

- **マルチプレクシングオプションのみ選択します。**
  各エージェントが、単一のテープドライブにデータを送信します。そのテープドライブは、複数のエージェントから同時にデータストリームを受け入れます。1台のテープドライブが受け入れ可能なストリームの最大数は、保護計画で設定し、動的には変更できません。
- **マルチストリーミングとマルチプレクシングのオプションを両方ともオンにします。**
  各エージェントが、2台以上のテープドライブにデータを送信します。それらのテープドライブは、複数のエージェントから同時にデータストリームを受け入れます。

1台のテープドライブに同時に異なる方式でバックアップを書き出すことはできません。マルチプレクシング方式か非マルチプレクシング方式のどちらかで書き出されます。どちらの方式で書き出されるかは、どちらの保護計画が最初に開始されたかによって決まります。

バックアップに選択されたテーププール内でテープの設定を使用

デフォルト設定:**無効**。

同じプール内の複数のテープを、**テープセット**と呼ばれるグループにまとめることができます。

このオプションを無効のままにすると、データが同じプールに所属するすべてのテープにバックアップされます。このオプションが有効の場合、事前に定義されたルールまたはカスタムルールに従ってバックアップを分割できます。

- **コンピュータごとに個別のテープセットを使用する**（ルールを 1 つ選択する:**バックアップの種類**、**デバイスの種類**、**デバイスの名前**、**日**、**曜日**、**月**、**年**、**年月日**）
  このオプションを選択すると、事前に定義されたルールに従ってテープセットを整理できます。たとえば、曜日ごとにテープセットを用意したり、各マシンのバックアップを個別のテープセットに保存したりできます。
- **テープセットのカスタムルールを指定**
  このオプションを選択すると、独自のルールに従ってテープセットを整理できます。ルールには次の変数を使用できます。

変数の構文	変数の説明	使用可能な値
`[Resource Name]`	各コンピュータのバックアップが個別のテープセットに保存されます。	Management Serverに登録されているコンピュータの名前。
`[Backup Type]`	完全、増分、差分のバックアップが個別のテープセットに保存されます。	`full`, `inc`, `diff`
`[Resource Type]`	各種コンピュータのバックアップが個別のテープセットに保存されます。	`Server essentials`, `Server`, `Workstation`, `Physical machine`, `VMware Virtual Machine`, `Virtual-PC Virtual Machine`, `Virtual Server Virtual Machine`, `Hyper-V Virtual Machine`, `Parallels`

		Virtual Machine, XEN Virtual Machine, KVM Virtual Machine, RHEV Virtual Machine, Parallels Cloud Virtual Machine
[Day]	毎月のそれぞれの日に作成されたバックアップが個別のテープセットに保存されます。	01、02、03、...、31
[Weekday]	毎週の各曜日に作成されたバックアップが個別のテープセットに保存されます。	Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, Saturday
[Month]	1年の各月に作成されたバックアップが個別のテープセットに保存されます。	January, February, March, April, May, June, July, August, September, October, November, December
[Year]	各年に作成されたバックアップが個別のテープセットに保存されます。	2017、2018、...

- たとえば、ルールを [Resource Name]-[Backup Type] のように指定すると、保護計画が適用される各マシンの完全、増分、差分バックアップがそれぞれ個別のテープの設定に作成されます。

個々のテープにテープセットを指定することもできます。その場合、バックアップはまず、保護計画に指定されている式の値にテープの設定値が合致するテープに書き込まれます。続いて、必要があれば、同じプールから別のテープが用意されます。その後は、プールが補充可能であれば、**空きテープ**プールのテープが使用されます。

たとえば、バックアップオプションとしてテープセットMondayをテープ1に、Tuesdayをテープ2に、のように設定したうえでWeekdayを指定すると、週の対応する曜日に適切なテープが使用されます。

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。試行は、試行が正常終了するか、または指定した回数の試行が行われると停止します。

デフォルト設定:**無効**。

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」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 システムの場合にのみ有効です。

このオプションでは、ボリュームシャドウコピーサービス（VSS）プロバイダがVSS対応アプリケーションにバックアップが開始されることを通知する必要があるかどうかを定義します。これにより、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整合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。

デフォルト設定:**有効。自動的にスナップショットプロバイダを選択。**

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すすめします。

お使いのデータベースがVSSと互換性がない場合は、このオプションを無効にします。スナップショットは迅速に取得できますが、スナップショットの取得時にトランザクションを完了していないアプリケーションのデータの整合性は保証されません。データ取り込みの前後に実行するコマンドを使用することで、整合性がある状態でデータをバックアップできます。たとえば、すべてのトランザクションを完了するように、データベースを停止してすべてのキャッシュをフラッシュするための、データ取り込みの前のコマンドを指定します。また、スナップショットの作成後にデータベース処理を再開するための、データ取り込みの後に実行するコマンドを指定します。

注意
この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。

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。

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。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またはHyper-V Integration Servicesを使用し、仮想コンピュータ内でVSSを適用します。

デフォルト設定:**有効**。

このオプションを有効にすると、スナップショットを作成する前に、仮想マシンで実行するすべてのVSS対応アプリケーションの処理が完了します。[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、静止スナップショットの障害が解消されない場合、アプリケーションのバックアップが無効となり、非静止スナップショットが取得されます。アプリケーションのバックアップが有効な場合、バックアップが失敗します。

このオプションを無効にした場合、非静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。VSS 対応アプリケーションが実行されてい

ない仮想マシンでも、常時このオプションを有効にしておくことをお勧めいたします。有効になっていない場合、取得されたバックアップ内のファイルシステムの整合性が保証されません。

注意
このオプションはScale Computing HC3仮想マシンには影響しません。それらのマシンでは、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、保持ルールとバックアップスキームで「毎週」となっているバックアップを設定します。「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。

復元元	復元方法
物理コンピュータ（Windows または Linux）	Webインターフェースを使用 ブータブルメディアを使用
物理コンピュータ（Mac）	ブータブルメディアを使用
仮想マシン（VMware、Hyper-V、またはScale Computing HC3）	Webインターフェースを使用 ブータブルメディアを使用
ESXi構成	ブータブルメディアを使用
ファイル/フォルダ	Webインターフェースを使用 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	Webインターフェースを使用
SQLデータベース	Webインターフェースを使用
Exchangeデータベース	Webインターフェースを使用
Exchangeメールボックス	Webインターフェースを使用
Microsoft 365メールボックス	Webインターフェースを使用
Oracle データベース	Oracle Explorer ツールの使用

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

オペレーティングシステムのバックアップイメージはマルウェアに感染する恐れがあり、そのイメージからリカバリするとマシンが再感染する可能性があります。

安全な復元を使用すると、リカバリプロセスで統合アンチマルウェアスキャンとマルウェア削除の機能を使用して、感染の再発を防止できます。

制限事項:

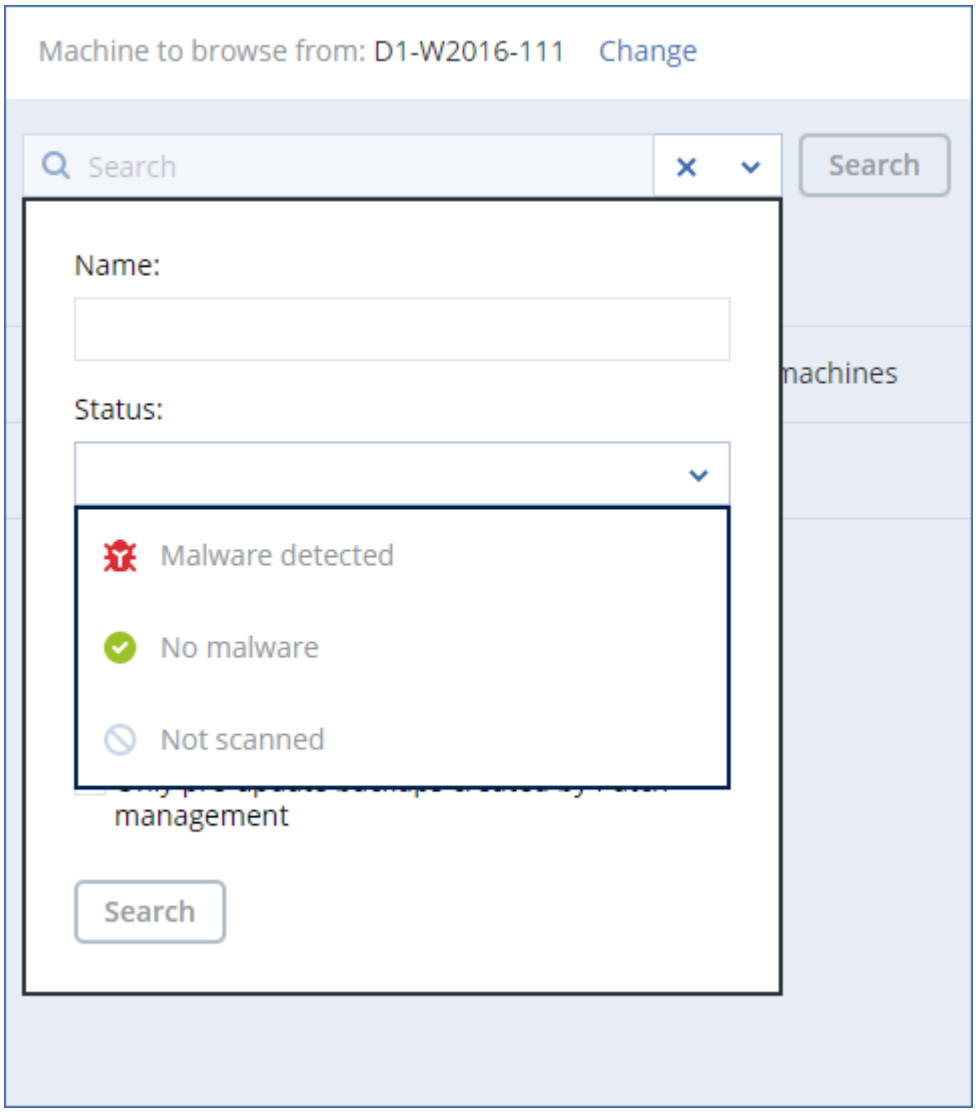
- 安全な復元がサポートされているのは、Windowsエージェントがインストールされている Windows 物理マシンまたは仮想マシンに限られます。
- サポートされているバックアップタイプは、**[マシン全体]** か **[ディスク/ボリューム]** のみです。
- NTFSファイルシステムのボリュームのみがサポートされています。NTFS以外のパーティションは、マルウェアのスキャンなしでリカバリされます。
- 安全な復元は、継続的データ保護（CDP）バックアップではサポートされていません。最後の定期的なバックアップに基づいて、CDPバックアップのデータなしでマシンがリカバリされます。CDPデータを復元する場合は、**ファイル/フォルダ**の復元を実行します。

仕組み

復元プロセスの実行時に [安全な復元] オプションを有効にすると、システムで以下の処理が実行されます。

1. イメージバックアップでマルウェアに関するスキャンが実行され、感染しているファイルにマークが付けられます。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。
   - **マルウェアはありません** - バックアップのスキャン時にマルウェアは検出されませんでした。
   - **マルウェアが検出されました** - バックアップのスキャン時にマルウェアが検出されました。
   - **スキャンされていません** - バックアップでマルウェアに関するスキャンが実行されていませんでした。
2. 選択したマシンがバックアップに基づいて復元されます。
3. 検出されたマルウェアが削除されます。

ステータスパラメータを使用して、バックアップをフィルタリングできます。



ブータブルメディアの作成

ブータブルメディアとは、オペレーティングシステムを使用することなくエージェントを実行できるCD、DVD、USB フラッシュドライブ、またはその他のリムーバルメディアのことです。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復元を目的としています。

ディスクレベルの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おすすめします。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のブータブル メディアの作成手順

1. ブータブルメディアISOファイルをダウンロードします。ファイル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 > **[ダウンロード]** > **[ブータブルメディア]** の順にクリックします。
2. 次の手順のいずれかを実行します。

- ISOファイルをCD/DVDに書き込みます。
- 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。
- ISOファイルを CD/DVD ドライブとして、復元する仮想マシンに接続します。

または、ブータブルメディアを作成するにはブータブルメディアビルダーを使用します。

macOS の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。

マシンの復元

物理マシンをリカバリする

このセクションでは、Cyber Protect Webコンソールを使用して物理マシンをリカバリする方法について説明します。

以下のいずれかをリカバリする必要がある場合、Cyber Protect Webコンソールではなくブータブルメディアを使用します。

- macOSオペレーティングシステム
- 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。

オペレーティングシステムの復元、およびBitLockerまたはCheckPoint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。詳細については、"再起動を伴う復元"（314ページ）を参照してください。

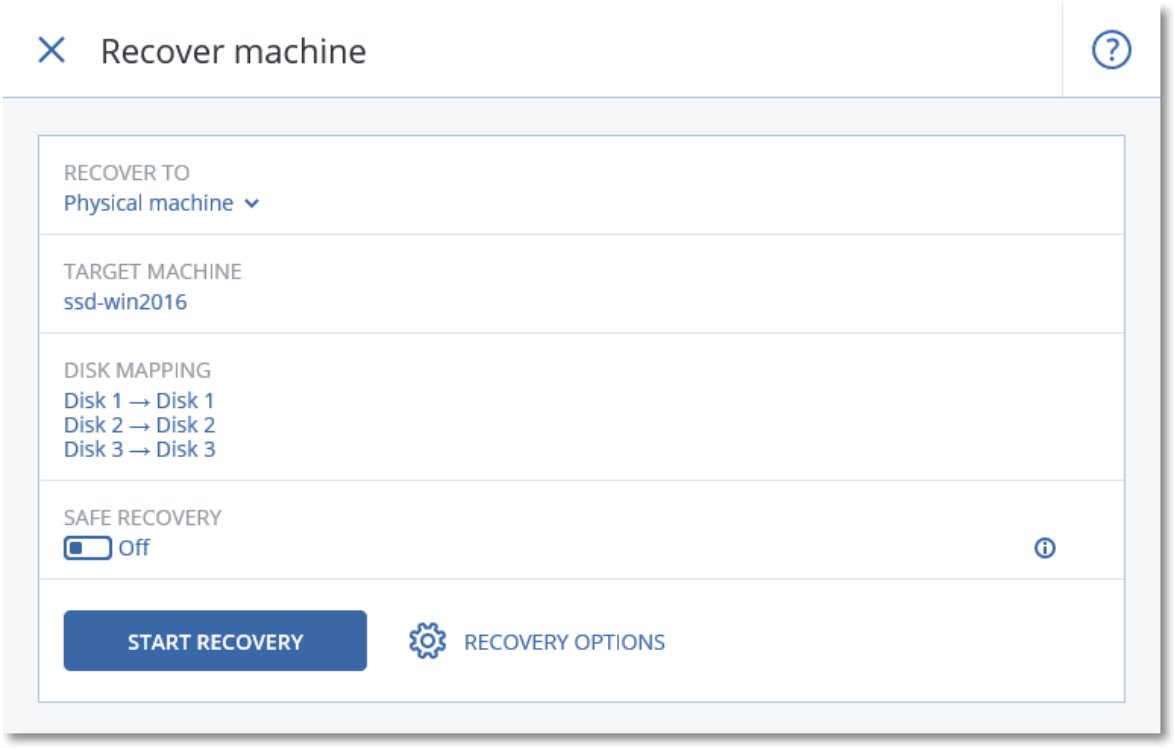
物理コンピュータの復元手順

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。

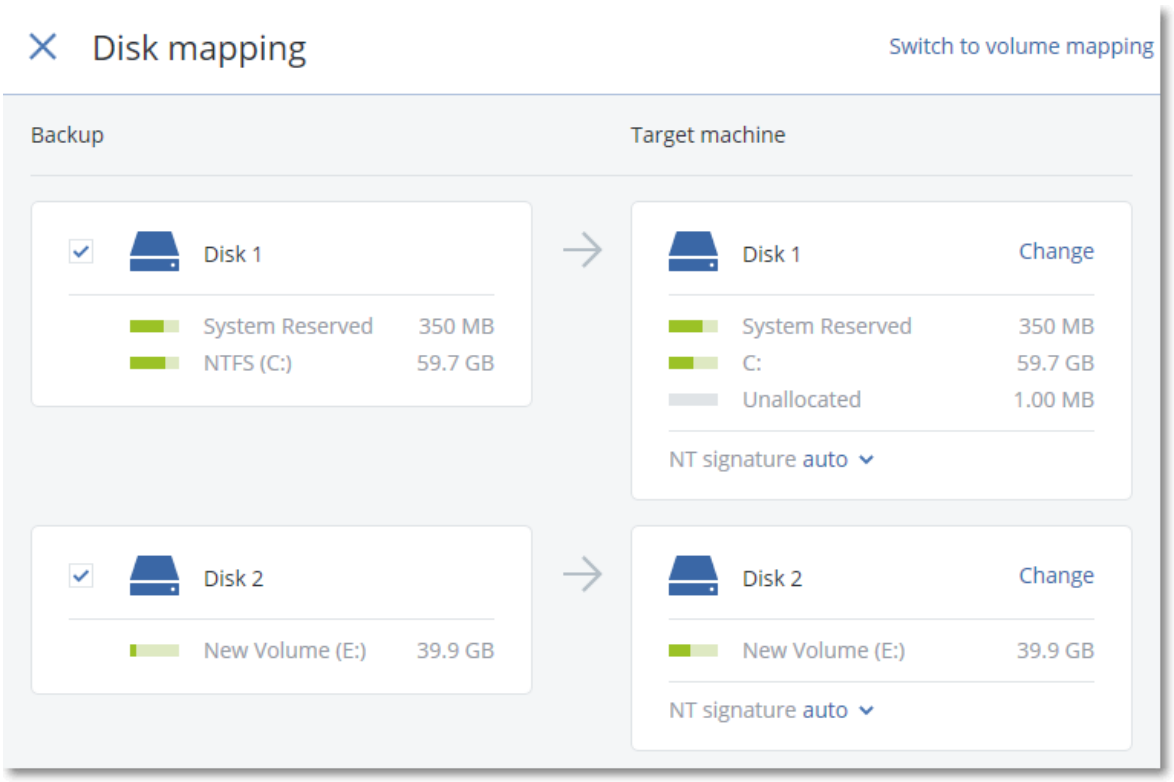
   コンピュータがオフラインになっている場合、リカバリ ポイントは表示されません。次の手順のいずれかを実行します。

- 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、**[ターゲットマシン]** 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、またはマッピングが正常に行われなかった場合は、**[ディスクマッピング]** 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。
   また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、復元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. （オプション）**[安全な復元]** スイッチを有効にして、マルウェアに関するバックアップスキャンを実行します。マルウェアが検出された場合、バックアップにマークが付けられ、復元プロセスの完了直後に削除されます。
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。

物理マシンを仮想マシンにリカバリする

物理マシンのバックアップを仮想マシンにリカバリできます。

ターゲットの仮想化ハイパーバイザーに関連するエージェントが、現在の環境に少なくとも1つインストールされ、管理サーバーに登録されている場合、仮想マシンへのリカバリが可能です。例えば、VMware ESXiへの復元を行う場合は、VMwareエージェントが現在の環境にインストールされ、管理サーバーに登録されている必要があります。

一部のオプションはクラウド配置でのみ利用可能です。

物理マシンから仮想マシンへのマイグレーション（P2V）でサポートされるパスの詳細については、"コンピュータの移行"（499ページ）を参照してください:

注意
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。
   - マシンをリカバリします（"ブータブルメディアを使用したディスクとボリュームの復元"（314 ページ）を参照）。
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. **[ターゲットマシン]** をクリックします。
   a. ハイパーバイザーを選択します。

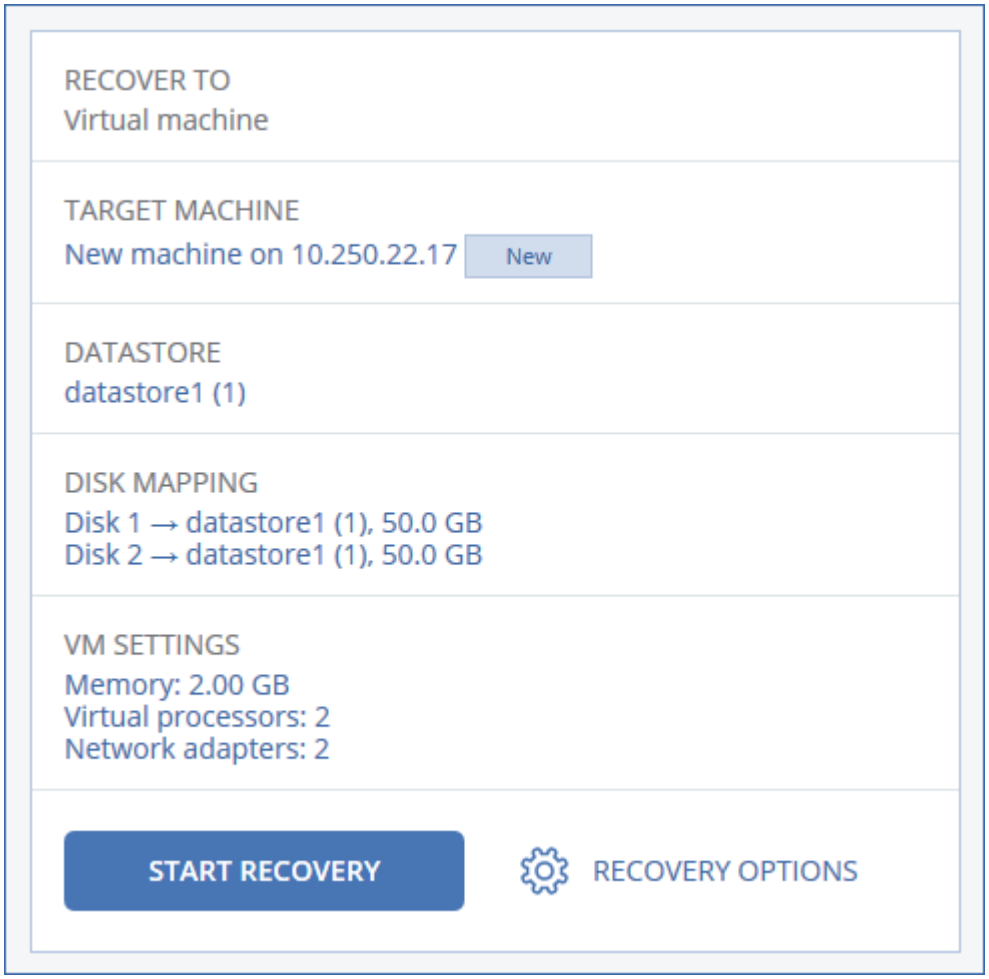
      注意
      該当のハイパーバイザーのエージェントが、現在の環境に少なくとも1つインストールされ、管理サーバーに登録されている必要があります。

   b. 新規または既存のマシンにリカバリするかどうかを選択します。ターゲットマシンのディスク構成とバックアップのディスク構成を完全に一致させる必要はないため、新規のマシンを選択することをお勧めします。
   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。
8. （オプション）（新しいマシンにリカバリする場合）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選択するには、**[ディスクマッピング]** 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。

注意
VirtuozzoコンテナまたはVirtuozzo Hybrid Infrastructure仮想マシンをリカバリ中の場合は、これらの設定を変更できません。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、VirtuozzoおよびRed Hat Virtualization/oVirtの場合）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するには、**[VM設定]** をクリックします。



9. **[復元を開始]** をクリックします。
10. （既存の仮想マシンにリカバリする場合）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

仮想マシンのバックアップを物理マシンまたは他の仮想マシンにリカバリできます。

ターゲットの仮想化ハイパーバイザーに関連するエージェントが、現在の環境に少なくとも1つインストールされ、管理サーバーに登録されている場合、仮想マシンへのリカバリが可能です。例えば、

VMware ESXiへの復元を行う場合は、VMwareエージェントが現在の環境にインストールされ、管理サーバーに登録されている必要があります。

一部のオプションはクラウド配置でのみ利用可能です。

仮想マシンから物理マシン（V2P）または仮想マシンから仮想マシン（V2V）のマイグレーションでサポートされるパスの詳細については、"コンピュータの移行"（499ページ）を参照してください。

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。

重要
仮想マシンに他のマシンをリカバリする場合は、仮想マシン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）。

仮想コンピュータの復元手順

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. （物理マシンに復元する場合）[**リカバリ先**] で [**物理マシン**] を選択します。
   ターゲットマシン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、物理マシンへの復元が可能です。この場合、"物理マシンをリカバリする"（307ページ）の手順4に進んでください。それ以外の場合は、ブータブルメディアを使用して、仮想マシンから物理マシン（V2P）のマイグレーション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、元のマシンがターゲットマシンとして選択されています。別の仮想コンピュータに復元するには、[**ターゲットマシン**] 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。

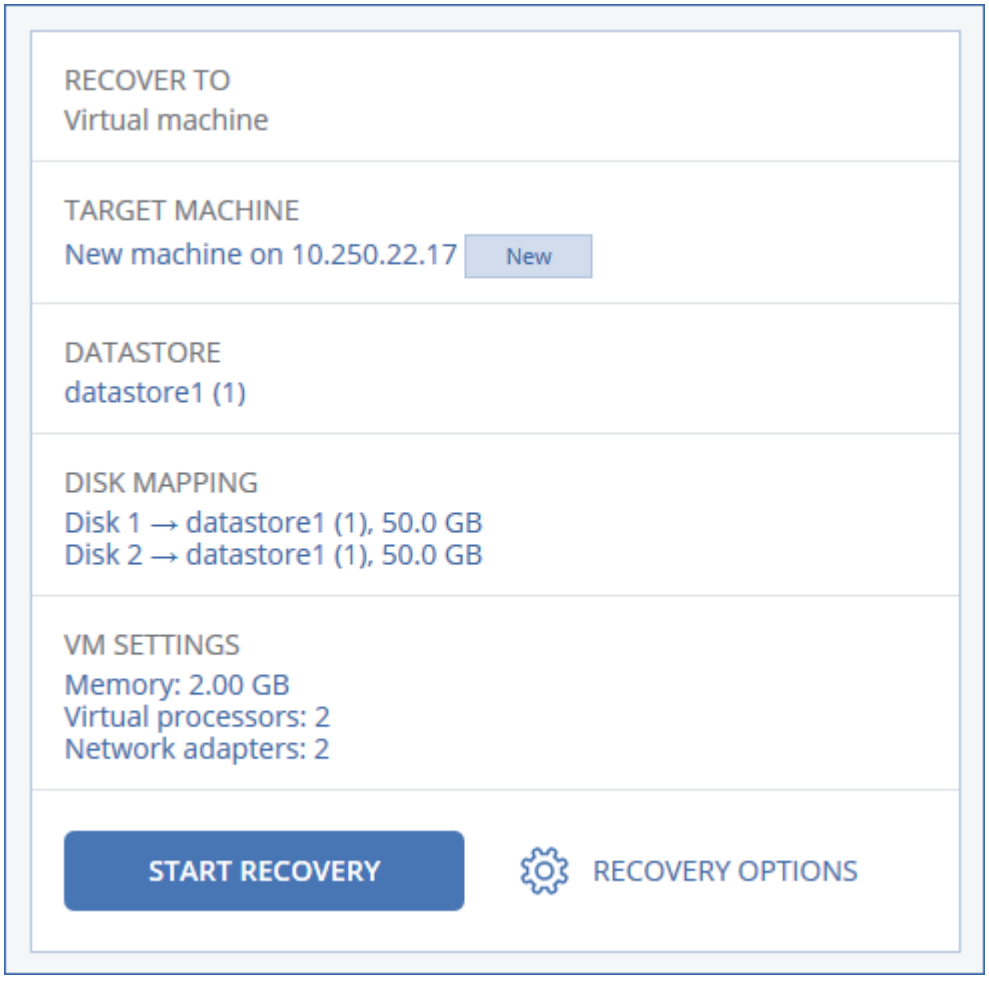
      注意
      該当のハイパーバイザーのエージェントが、現在の環境に少なくとも1つインストールされ、管理サーバーに登録されている必要があります。

   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。
   c. ホストを選択し、新しいマシン名を指定するか、既存のターゲットマシンを選択します。
   d. [**OK**] をクリックします。
5. （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。
6. （オプション） （新しいマシンにリカバリする場合）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選択するには、**[ディスクマッピング]** 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。

  注意
  VirtuozzoコンテナまたはVirtuozzo Hybrid Infrastructure仮想マシンをリカバリ中の場合は、これらの設定を変更できません。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、VirtuozzoおよびRed Hat Virtualization/oVirtの場合）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するには、**[VM設定]** をクリックします。



7. **[復元を開始]** をクリックします。
8. （既存の仮想マシンにリカバリする場合）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。

再起動を伴う復元

以下をリカバリする場合、再起動が必要です:

- オペレーティングシステム
- BitLockerまたはCheckPointで暗号化されたボリューム

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。

要件

- 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の空き容量がなければなりません。そうでない場合、復元は失敗します。
- 暗号化されたシステムボリュームを復元する場合、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。

トラブルシューティング

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。

ブータブルメディアを使用したディスクとボリュームの復元

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"（306ページ）」を参照してください。

ブータブルメディアを使用してディスクまたはボリュームをリカバリするには

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. （macOSの場合のみ）APFSでフォーマットされたボリュームを別のマシンやベアメタルにリカバリする場合は、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. 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/welcome を参照してください。
   c. **[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。

注意
MacOS 11 Big Sur以降、システムボリュームをバックアップおよびリカバリできません。ブータブルmacOSシステムをリカバリするには、データボリュームを復元してから、そこにmacOSをインストールする必要があります。

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 アドレスとポートを指定します。それ以外の場合は、この手順をスキップします。
5. [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。
   - 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。

   [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. **[バックアップコンテンツ]** で、**[ディスク]** または **[ボリューム]** を選択して、リカバリする項目を選択します。**[OK]** をクリックし、選択を確定します。

重要
バックアップされたマシンにダイナミックディスクまたは論理ボリューム（LVM）が存在する場合は、**[ボリューム]** を選択します。

10. **[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。

11. （macOSの場合のみ）APFSでフォーマットされたデータボリュームをブータブルmacOSシステムとしてリカバリするには、**macOSインストールセクション**で、**[復元したmacOSデータボリューム上にmacOSをインストールする]** チェックボックスをオンにしたままにします。
    復元後、システムは再起動し、macOSのインストールが自動的に開始されます。インストーラで必要なファイルをダウンロードするにはインターネット接続が必要です。

APFSでフォーマットされたデータボリュームをブータブルシステムとしてリカバリする必要がない場合は、**[復元したmacOSデータボリューム上にmacOSをインストールする]** チェックボックスをオフにします。このボリュームは、手動でmacOSをインストールすることで、後でブータブルにできます。

12. （Linuxの場合のみ）バックアップされたマシンに論理ボリューム（LVM）が存在し、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。
    c. 選択内容を確認入力します。
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。

Universal Restore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コントローラー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ます。見つかったドライバへのパスが、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的な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

Webインターフェイスを使用したファイルの復元

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。
   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」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。
8. **[復元]** をクリックします。
   [復元先] に、次のいずれかが表示されます。
   - 復元するファイルが元々存在していたマシン（エージェントがこのマシンにインストールされている場合）。

- VMware エージェント、Hyper-V エージェント、または Scale Computing HC3 エージェントがインストールされているマシン（ESXi、Hyper-V、または Scale Computing HC3 仮想マシンにファイルが元々存在していた場合）。

これは、復元先のコンピュータです。必要に応じて、別のコンピュータを選択できます。

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。
   - 元のロケーション（元のコンピュータに復元する場合）
   - 復元先のコンピュータのローカルフォルダ

     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

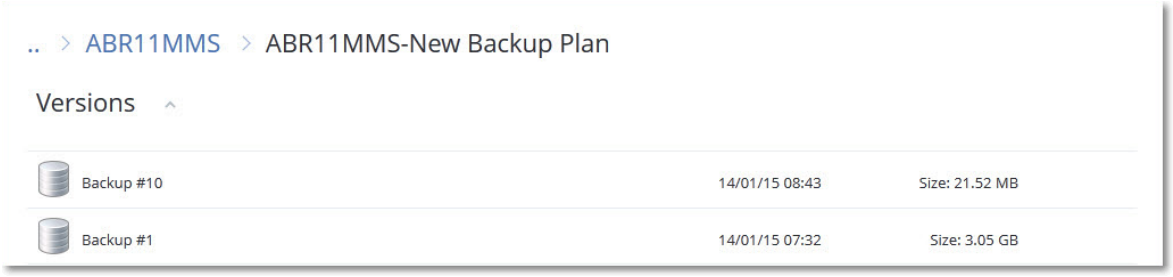
クラウドストレージからファイルを復元する場合、クラウドストレージを参照し、バックアップの内容を表示し、必要なファイルをダウンロードします。

制限事項

- システム状態のバックアップ、SQLデータベース、Exchangeデータベースは参照できません。
- ダウンロードを円滑に行うには、一度にダウンロードするサイズを100MBまでにしてください。大量のデータをクラウドから取得するには、ファイル復元手順を使用します。

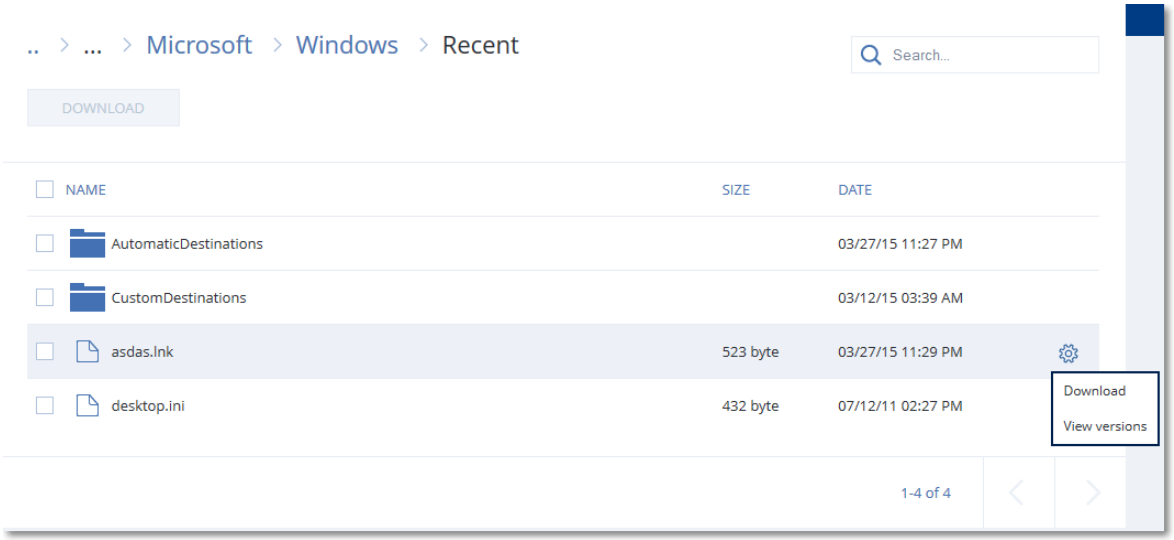
クラウドストレージからファイルをダウンロードする手順

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]** > **[その他の復元方法...]** > **[ファイルのダウンロード]** の順にクリックします。
3. 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。
4. （ディスクレベルバックアップを参照する場合）**[バージョン]** で、復元対象のファイルが含まれているバックアップをクリックします。



（ファイルレベルのバックアップを参照する場合）選択したファイルの右にある歯車アイコンで、次の手順でバックアップ日時を選択できます。デフォルト設定では、最新のバックアップからファイルが復元されます。

5. 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の一覧を取得します。



6. 復元するデータの左に表示されているチェックボックスを選択し、**[ダウンロード]** をクリックします。

   選択したファイルが1つの場合は、そのままダウンロードされます。複数のファイルを選択した場合、選択したデータは.zipファイルにアーカイブされます。

7. データの保存先を選択し、**[保存]** 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

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インターフェイスを使用したファイルの復元」セクションの手順1～6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 アドレスとポートを指定します。それ以外の場合は、この手順をスキップします。
4. [ようこそ] 画面で、 **[復元]** をクリックします。
5. **[データの選択]** をクリック後、**[参照]** をクリックします。
6. 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。
   - 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。

   [OK] をクリックし、選択を確定します。
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. **[バックアップ内容]** で **[フォルダ/ファイル]** を選択します。
9. 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。
10. **[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。
11. （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。
12. **[OK]** をクリックして復元を開始します。

注意
テープロケーションは多くの領域を必要とし、LinuxブータブルメディアやWinPEブータブルメディアで再スキャンおよびリカバリを行う際には、RAMが不足する可能性があります。Linuxの場合、ディスク上または共有上のデータを保存するには、別のロケーションにマウントする必要があります。
Acronis Cyber Backup Advanced Workstation:テープロケーションフォルダの変更（KB27445）を参照してください。WindowsPEの場合、現時点では回避策がありません。

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+。
- 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。

システム状態の復元

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、「ブータブル メディアの作成」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、Scale Computing HC3	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	-	-	-	+	+	+	+	-	-
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	-	-	-	-	-	-	-	+	-
"テープ管理"（333 ページ）>迅速な復元のためにディスク キャッシュを使用します	-	-	-	+	+	+	-	-	-
Windows イベントログ	+	-	-	+	-	-	-	Hyper-V のみ	+
復元後に電源オンにする	-	-	-	-	-	-	+	-	-

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復元する前にバックアップが破損していないことをベリファイ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**。

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。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情報の整合性をチェックすることで、ベリファイされます。

サイズの小さい増分/差分バックアップでも、ベリファイには時間がかかります。これは、バックアップに物理的に含まれているデータだけでなく、バックアップの選択によって復元可能となったすべてのデータもベリファイされるためです。このベリファイには、以前に作成したバックアップへのアクセスが必要となります。

注意
Acronisのデータセンター内にあり、Acronisパートナーの提供するクラウド ストレージでは、ベリファイの機能が利用できます。

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。そのため、バックアップ元と同じディスクへのデータリカバリが、ディスクのボリュームレイアウトが変更されていない場合に特に、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。

物理マシンの場合、ブロックレベルでのデータの比較は、時間のかかる処理です。バックアップストレージへの接続スピードが速いと、データの差異を計算するよりも短い時間でディスク全体を復元できます。そのため、バックアップストレージへの接続が低速の場合にのみ、このオプションを有効にすることをお勧めします（たとえば、バックアップがクラウドストレージやリモートネットワークフォルダに保存されている場合）。

物理マシンを復元する場合、事前設定はバックアップロケーションによって異なります。

- バックアップロケーションがクラウドストレージの場合、事前設定は次のようになります。**有効**。
- その他のバックアップロケーションの場合、事前設定は次のようになります。**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**。

この設定では、バックアップ処理に割り当てられるCPUとシステムリソースの量を決定します。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。

テープ管理

たとえば次のようなテープ管理復元オプションを使用できます。

迅速な復元のためにディスク キャッシュを使用します

デフォルト設定:**無効**。

イメージアーカイブからファイルを復元する場合、**迅速な復元のためにディスク キャッシュを使用します**オプションを使用することを強くお勧めします。使用しない場合、復元操作に長い時間がかかる場合があります。このオプションを使用すると、テープの読み取りは連続して行われ、中断や巻き戻しがありません。

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、またはScale Computing HC3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（コンピューター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、Scale Computing HC3 エージェントの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**。

復元後に電源オンにする

このオプションは、ブータブル メディアから起動した場合に使用できます。

デフォルト設定:**無効**。

このオプションによって、ユーザーによる操作なしに復元されたオペレーティング システムでコンピュータを再起動できます。

災害復旧

この機能は Acronis Cyber Protect のクラウド配置でのみ使用可能です。この機能の詳細については、https://www.acronis.com/support/documentation/DisasterRecovery/index.html#43224.html を参照してください。

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] タブには、管理サーバーで登録されたことがあるすべてのマシンのバックアップが表示されます。これには、オフラインコンピュータと登録されないコンピュータが含まれます。

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。クラウドデプロイメントでは、管理者は、同じグループと子グループに属するアカウントの代わりにバックアップを表示できます。このアカウントは **[参照元マシン]** で間接的に選択されます。**[バックアップストレージ]** タブには、このマシンの登録先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。

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。

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、バックアップをエクスポートすることや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。

バックアップストレージタブを使用して復元ポイントを選択する手順

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、**[ターゲットマシン]** 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、**[参照元マシン]** 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。

読み取り/書き込みモード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コンピュータの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復元します。

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。デフォルトでは、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、次のいずれかをクリックします。
   - **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。
   - **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. ボリュームが読み取り/書き込みモード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

ベリファイは、バックアップからデータを復元できるかどうかを確認する処理です。この操作の詳細については、「"ベリファイ"（346ページ）」を参照してください。

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"（337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。エクスポートを使用すると、特定のバックアップを増分および差分バックアップ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。

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。

エクスポートしたバックアップのバックアップファイル名は、バックアップ形式オプションの値に依存します:

- あらゆるバックアップスキームにおいて、**バージョン12**形式の場合、シーケンス番号を除き、バックアップファイル名は、元のバックアップの名前と同じになります。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。
- 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11**形式の場合、バックアップファイル名は元のバックアップのバックアップファイル名と完全に一致します。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、すべてのエクスポート操作により、以前にエクスポートされたバックアップが上書きされます。
- その他のバックアップスキームにおいて、**バージョン11**形式の場合、タイムスタンプを除き、バックアップファイル名は、元のバックアップの名前と同じになります。エクスポートされたバックアップのタイムスタンプは、エクスポートが実行された時間に対応します。

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。
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

警告
バックアップを削除すると、そのデータは永久に消去されます。削除されたデータは復元できません。

オンラインで Cyber Protect ウェブ コンソールに存在するマシンのバックアップを削除するには

1. **[すべてのデバイス]** タブで、バックアップを削除するマシンを選択します。
2. **[復元]** をクリックします。
3. 削除するバックアップがある場所を選択します。
4. 次のいずれかを実行します。
   - 単一のバックアップを削除するには、削除するバックアップを選択し、ギアアイコンをクリックしてから **[削除]** をクリックします。
   - 選択した場所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。
5. 操作を確定します。

コンピュータのバックアップを削除するには

1. **[バックアップストレージ]** タブで、バックアップを削除す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. グループを選択します。
3. 次のいずれかを実行します。

- 単一のバックアップを削除するには、**[バックアップを表示]** をクリックして、削除するバックアップを選択し、ギアアイコンをクリックしてから **[削除]** をクリックします。
- 選択したグループを削除するには、**[削除]** をクリックします。

4. 操作を確定します。

クラウドストレージから直接バックアップを削除する手順

1. 「クラウドストレージからのファイルのダウンロード」を参照して、クラウドストレージにログインします。
2. 削除対象のバックアップがあるマシンの名前をクリックします。
   1つ以上のバックアップグループが表示されます。
3. 削除対象のバックアップグループに対応するギアアイコンをクリックします。
4. **[削除]** をクリックします。
5. 処理を確認します。

[計画] タブ

Advancedライセンスの場合、**[計画]** タブを使用して、保護計画などの計画を管理できます。

[計画] タブの各セクションには、特定の種類の計画がすべて用意されています。以下のセクションがあります。

- **保護**
- **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**
- **検証**
- **クリーンアップ**
- **VMへの変換**
- **VMレプリケーション**
- **ブータブルメディア**。このセクションには、ブータブルメディアからブートされるマシン用に作成され、該当するメディアのにみ適用される保護計画が表示されます。

各セクションでは、計画の実行を、作成、編集、無効化、有効化、削除、開始、監視することができます。

クローン作成および停止は、保護計画でのみ利用可能です。**[デバイス]** タブからバックアップを停止する場合と異なり、保護計画を停止すると、その計画が適用されるすべてのデバイスでバックアップが停止します。複数デバイスのバックアップ開始時刻が設定した時間枠内に分散している場合に、保護計画を停止すると、実行中のバックアップが停止するか、バックアップが開始されなくなります。

また、計画をファイルにエクスポートしたり、以前エクスポートした計画をインポートしたりもできます。

オフホストのデータ処理

レプリケーション、ベリファイ、保持ルールの適用など、保護計画に含まれるほとんどのアクションは、バックアップを実行するエージェントによって実行されます。これによって、バックアップ処理が完了した後でも、エージェントを実行しているマシンにはさらに負荷がかかります。

マルウェア対策スキャン、レプリケーション、ベリファイ、クリーンアップ、変換の計画を保護計画から分離することによって、次の操作を柔軟に実行できます。

- これらの処理を実行するために別のエージェントを選択する
- これらの処理をオフピーク時にスケジュール設定し、ネットワークの帯域幅の消費を最小限に抑える
- 専用エージェントのセットアップが計画に含まれてない場合は、これらの処理を営業時間外に設定する

Storage Nodeを使用している場合は、同じコンピュータに専用エージェントをインストールするのが効果的です。

エージェント実行中マシンの時間設定を使用するバックアップおよびVMレプリケーションとは異なり、オフホストのデータ処理計画は管理サーバーマシンの時間設定に従って実行されます。

バックアップスキャンの計画

サポートされるロケーション

次のロケーションのバックアップのマルウェアをスキャンできます。**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**。スキャンされたマシンにインストールされたエージェントのみが**ローカルフォルダ**ロケーションにアクセスできます。

バックアップスキャンと制限事項の詳細については、「バックアップのマルウェア対策スキャン」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 ウェブ コンソールで、**[計画]** > **[バックアップスキャン]** をクリックします。
2. **[計画の作成]** をクリックします。
3. （オプション）計画名を変更するには、デフォルト名の横の鉛筆アイコンをクリックします。
4. スキャンエージェントを選択します。
5. スキャンするバックアップロケーションまたは個々のバックアップを選択します。
   一度に複数のバックアップロケーションを選択できます。1 つの計画に複数の個別のバックアップを含めるには、バックアップを 1 つずつ追加する必要があります。
6. （**クラウド ストレージ**または**ネットワークフォルダ**が選択された場合）入力が求められた場合は、バックアップストレージにアクセスするための資格情報を入力します。
7. （暗号化されたバックアップが選択された場合）バックアップにアクセスするためのパスワードを入力します。格納域または複数の暗号化されたバックアップを選択した場合は、1 つのパスワードを指定できます。特定のバックアップのパスワードが正しくない場合は、アラートが表示されます。正しいパスワードが入力されたバックアップのみがスキャンされます。
8. スキャンのスケジュールを構成します。
9. 準備ができたら、**[作成]** をクリックします。

バックアップスキャン計画が作成されます。

バックアップのレプリケーション

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	+	+
NFSフォルダ	–	–
Secure Zone	–	–
SFTPサーバー	–	–
管理対象ロケーション*	+	+
テープ デバイス	–	+

* トピック "Advancedライセンスを持つユーザーのための考慮事項"（251ページ） で説明されている制限事項をチェックしてください。

バックアップのレプリケーション計画を作成する

1. **[計画]** > **[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。
   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. **[エージェント]** をクリックし、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。
   ソースとターゲットの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。
5. **[レプリケーションする項目]** をクリックし、この計画でレプリケーション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。
6. **[ターゲット]** をクリックし、対象のロケーションを指定します。
7. （オプション）**[レプリケーション方法]** で、レプリケーションするバックアップを選択します。次のいずれかを選択できます。
   - **すべてのバックアップ**（デフォルト）
   - **完全バックアップのみ**
   - **最後のバックアップのみ**
8. （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。
9. （オプション）**[保持ルール]** をクリックし、「保持ルール」の説明に従ってターゲットロケーションの保持ルールを指定します。
10. **[レプリケーションする項目]** 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。
11. （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。
12. **[作成]** をクリックします。

ベリファイ

ベリファイは、バックアップからデータを復元できるかどうかを確認する処理です。

バックアップロケーションのベリファイでは、そのロケーションに格納されているすべてのバックアップをベリファイします。

仕組み

ベリファイ計画では、2 つのベリファイ方法が用意されています。両方の方法を選択した場合は、連続して処理が実行されます。

- **バックアップに保存されている各データブロックのチェックサムを計算する**
  チェックサムの計算によるベリファイの詳細については、「バックアップのベリファイ」を参照してください。
- **バックアップから仮想マシンを実行する**
  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。この方法を使用するには、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。
  エージェントはバックアップから仮想マシンを実行し、VMware Tools または Hyper-V Heartbeat Service に接続して、オペレーティングシステムが正常に起動したことを確認します。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。
  ベリファイ計画とベリファイ対象のバックアップの数に関わらず、ベリファイ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。

ベリファイが失敗した場合は、**[概要]** タブの **[アクティビティ]** セクションで詳細情報を確認できます。

サポートされるロケーション

次の表は、ベリファイ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	チェックサムの計算	VMの実行
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	+	+
NFSフォルダ	–	–
Secure Zone	–	–
SFTPサーバー	–	–
管理対象ロケーション	+	+

テープ デバイス	+	−

新しいベリファイ計画を作成する

1. **[計画]** > **[ベリファイ]** 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. **[エージェント]** をクリックし、ベリファイを実行するエージェントを選択します。
   バックアップから仮想マシンを実行することでベリファイを実行する場合は、VMwareエージェントまたは Hyper-Vエージェントを選択します。それ以外の場合は、管理サーバーに登録されていて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します。
5. **[ベリファイする項目]** をクリックし、この計画でベリファイ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。
6. （オプション）**[ベリファイの対象]** で、ベリファイするバックアップを選択します。次のいずれかを選択できます。
   - **すべてのバックアップ**
   - **最後のバックアップのみ**
7. （オプション）**[ベリファイ方法]** をクリックし、次のいずれかの方法を選択します。
   - **チェックサムのベリファイ**
     バックアップに保存されている各データブロックのチェックサムを計算します。
   - **仮想コンピュータとしての実行**
     仮想マシンが各バックアップから実行されます。
8. **[仮想マシンとしての実行]** を選択した場合:
   a. **[ターゲットマシン]** をクリックし、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）をクリックし、仮想コンピュータのデータストアを選択します。
   c. （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、VMware ESXiの場合は **[シン]**、Hyper-Vの場合は **[容量可変]** です。
   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。

注意
バックアップから仮想マシンを実行して、ゲストオペレーティングシステムのハイパーバイザーツール（VMware ToolsまたはHyper-V Integration Services）から報告された仮想マシンのハートビートステータスを検証するために、**VMハートビート**スイッチは常に有効になっています。このスイッチは、今後のリリース用に設計されており、操作することはできません。

9. （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。
10. **[ベリファイする項目]** 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。
11. （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。
12. **[作成]** をクリックします。

クリーンアップ

クリーンアップは、古くなったバックアップを保持ルールに従って削除する操作です。

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、SFTP サーバー、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。

新しいクリーンアップ計画を作成する

1. **[計画]** > **[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。
   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. **[エージェント]** をクリックし、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。
5. **[クリーンアップする項目]** をクリックし、この計画でクリーンアップ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。
6. （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。
7. （オプション）**[保持ルール]** をクリックし、「保持ルール」の説明に従って保持ルールを指定します。
8. **[クリーンアップする項目]** 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。

9. （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。
10. **[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。

前提条件と制限事項についての情報は、「変換に関する注意点」を参照してください。

仮想マシンへの変換計画の作成

1. **[計画]** > **[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、ターゲット仮想コンピュータ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 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。

ブータブル メディア

重要
このセクション内に記載されているいくつかの機能は、オンプレミスデプロイメントでのみ使用できます。

ブータブル メディア

ブータブルメディアは、物理メディア（CD、DVD、USBフラッシュドライブ、またはマシンのBIOSによって起動デバイスとしてサポートされるその他のリムーバブルメディア）です。ブータブルメディアを使用すると、オペレーティングシステムを使用せずに、Linuxベースの環境またはWindowsプレインストール環境（WinPE）を起動して、保護エージェントを実行できます。

ブータブル メディアは次の状況で最も多く使用されます。

- 起動できないオペレーティングシステムの復元
- 破損したシステム内に残存するデータへのアクセスとバックアップ
- ベアメタル状態のディスクへのオペレーティングシステムの配置
- ベアメタル状態のディスクへのベーシックボリュームまたはダイナミックボリュームの作成
- サポートされていないファイルシステムを使用しているディスクのセクタ単位のバックアップ
- 実行中のアプリケーションによってデータがロックされている、データへのアクセスが制限されている、などの理由でオンラインでバックアップできないデータのオフラインバックアップ。

Acronis PXE Server、Windows 展開サービス（WDS）、またはリモートインストールサービス（RIS）からネットワークブートを使用してマシンを起動することもできます。アップロードされたブータブルコンポーネントを含むこれらのサーバーは、ブータブル メディアの一種と考えることもできます。同じウィザードを使用して、ブータブルメディアを作成したり、PXEサーバーまたはWDS/RISを設定できます。

ブータブルメディアの作成か、既成のブータブルメディアのダウンロードか

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独自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。全機能を備えたブータブルメディアの場合は、Acronis Cyber Protect ライセンスキーを指定する必要があります。このキーがない場合、ブータブルメディアでは復元操作のみを実行できます。

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。

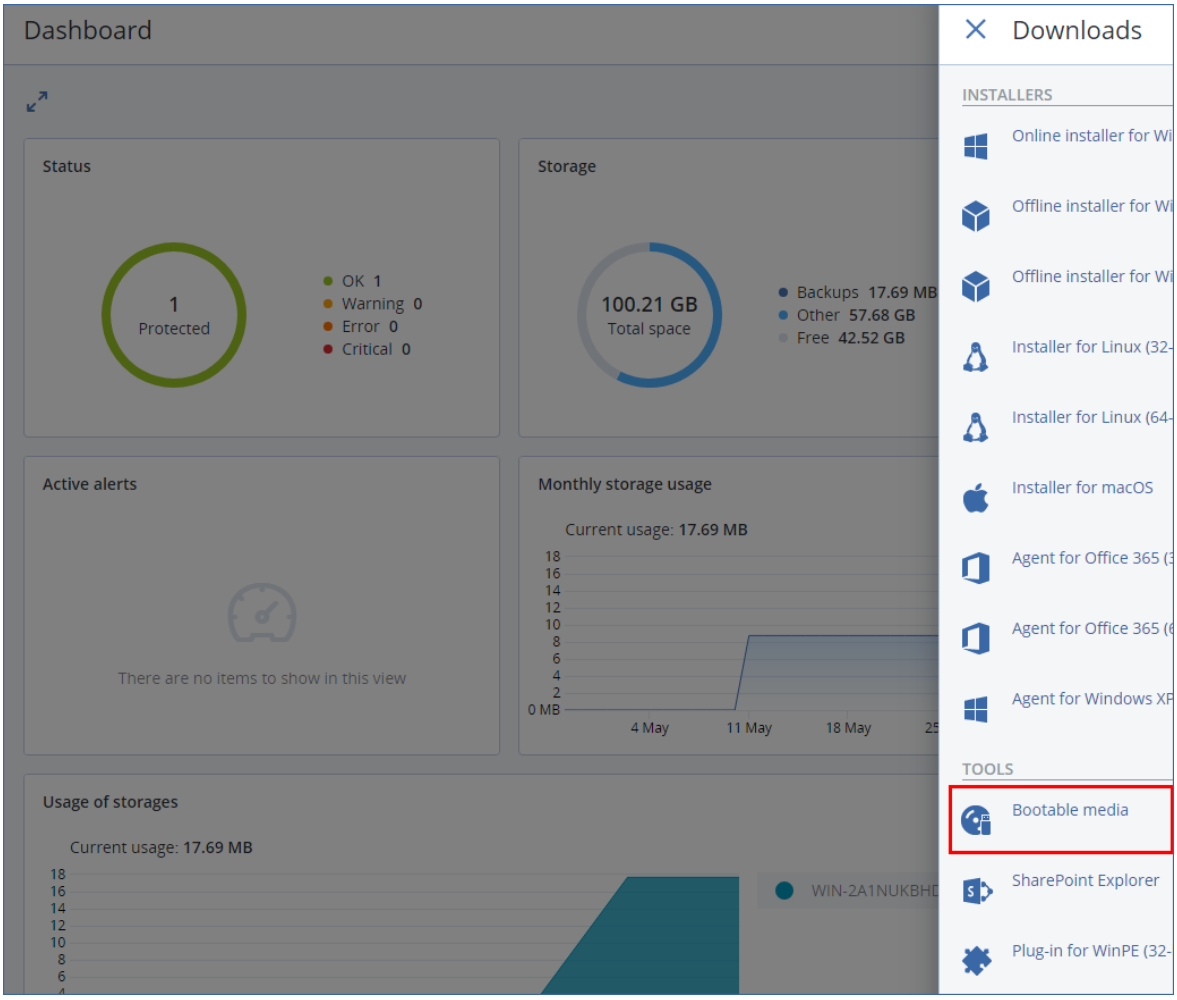
また、既成のブータブルメディアをダウンロードすることもできます（Linuxベースのみ）。ダウンロードしたブータブルメディアは、復元操作と Acronis Universal Restore へのアクセスにのみ使用できます。データをバックアップしたり、バックアップをバリデートまたはエクスポートしたり、ディスクを

管理したり、そのブータブルメディアメディアでスクリプトを使用したりすることはできません。ダウンロードしたブータブルメディアはmacOSコンピューターには適合しません。

注意
既成のブータブルメディアはStorage Node、テープロケーション、およびSFTPロケーションをサポートしません。オンプレミス配置でこれらのストレージロケーションを使用する場合は、ブータブルメディアビルダーを使用して独自のブータブルメディアを作成する必要があります。
https://kb.acronis.co.jp/content/61566を参照してください。

既成のブータブルメディアをダウンロードする場合

1. Cyber Protect ウェブ 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。
2. **[ブータブルメディア]** を選択します。



オンラインで入手可能なフリーツールを使用して、ダウンロードしたISOファイルをCD/DVDに保存するか、ブータブルUSBフラッシュドライブを作成します。UEFIマシンを起動する必要がある場合は`ISO to USB`または`RUFUS`を使用します。BIOSマシンの場合は、`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。

Cyber Protect ウェブ コンソールにアクセスできない場合は、次のようにして Acronis カスタマーポータルの自分のアカウントから既成のブータブルメディアをダウンロードできます。

1. https://account.acronis.co.jp にアクセスします。
2. Acronis Cyber Protect に移動して、[**ダウンロード**] をクリックします。
3. 表示されるページで、**追加のダウンロード**に移動して、[**ブータブルメディア ISO（Window 用と Linux 用）**] をクリックします。

Linuxベースのブータブルメディアか、WinPE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、ブータブル保護エージェントが含まれています。このエージェントは、ベア メタル状態のディスクや、破損していたりサポートされていないファイル システムを使用しているコンピュータを含め、任意の PC 互換ハードウェアから起動でき、操作を実行することができます。操作の構成と制御は、Cyber Protect ウェブ コンソールでローカルでもリモートでも行うことができます。

Linux ベースのメディアでサポートされたハードウェアの一覧については、
http://kb.acronis.com/content/55310を参照してください。

WinPE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Acronisプラグインが含まれています。

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 Acronis Cyber Protect 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 コントローラのサポートや RAID アレイの特定のレベルのみのサポートなど、一部の Linux 関連のブータブル メディア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。

- PE ベースのブータブル メディアでコンピュータを起動する場合、バックアップ先として CD、DVD、または Blu-ray ディスク（BD）などの光学メディアを選択できません。

ブータブルメディアビルダー

ブータブル メディア ビルダは、ブータブル メディアを作成するための専用のツールです。オンプレミス配置でのみ使用できます。

ブータブルメディアビルダは、Management Serverをインストールするときにデフォルトでインストールされます。WindowsまたはLinuxを実行するコンピュータで個別のメディアビルダをインストールできます。サポートされているオペレーティングシステムは対応するエージェントと同じです。

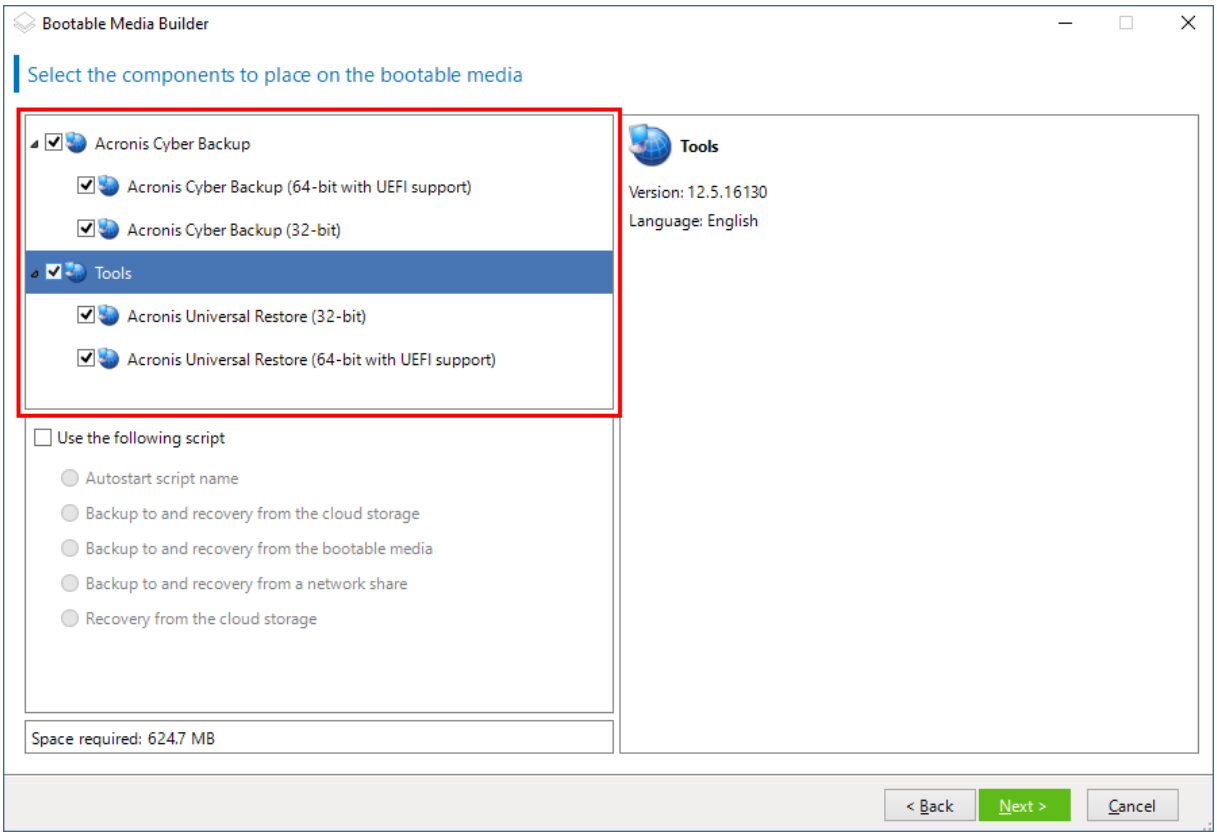
メディアビルダを使用する理由

Cyber Protect ウェブ コンソールでダウンロードできる既成のブータブルメディアは、復元でのみ使用できます。このメディアはLinuxカーネルに基づきます。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。

- メディアビルダーでは、全機能を備えた、バックアップ機能付きのLinuxベースおよびWinPEベースのカスタムブータブルメディアを作成できます。
- 物理ブータブルメディアの作成とは別に、Windows Deployment Services（WDS）にコンポーネントをアップロードし、ネットワークブートを使用できます。
- 既成のブータブルメディアはStorage Node、テープロケーション、およびSFTPロケーションをサポートしません。ローカルのオンプレミス配置でこれらのストレージロケーションを使用する場合は、ブータブルメディアビルダーを使用して独自のブータブルメディアを作成する必要があります。https://kb.acronis.co.jp/content/61566を参照してください。

32ビットまたは64ビット

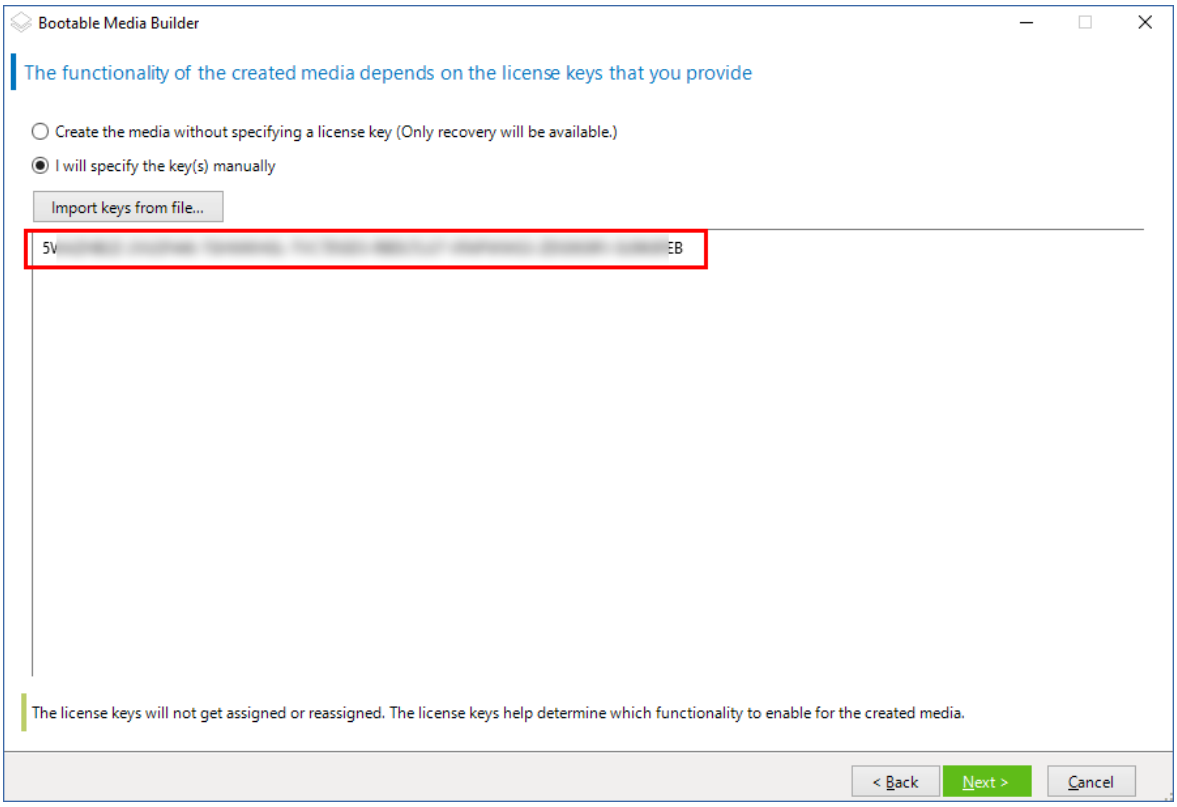
ブータブルメディアビルダーは、32ビットと64ビットの両方のコンポーネントを含むメディアを作成します。UEFI（Unified Extensible Firmware Interface）を使用するマシンを起動するには、通常は64ビットメディアが必要です。



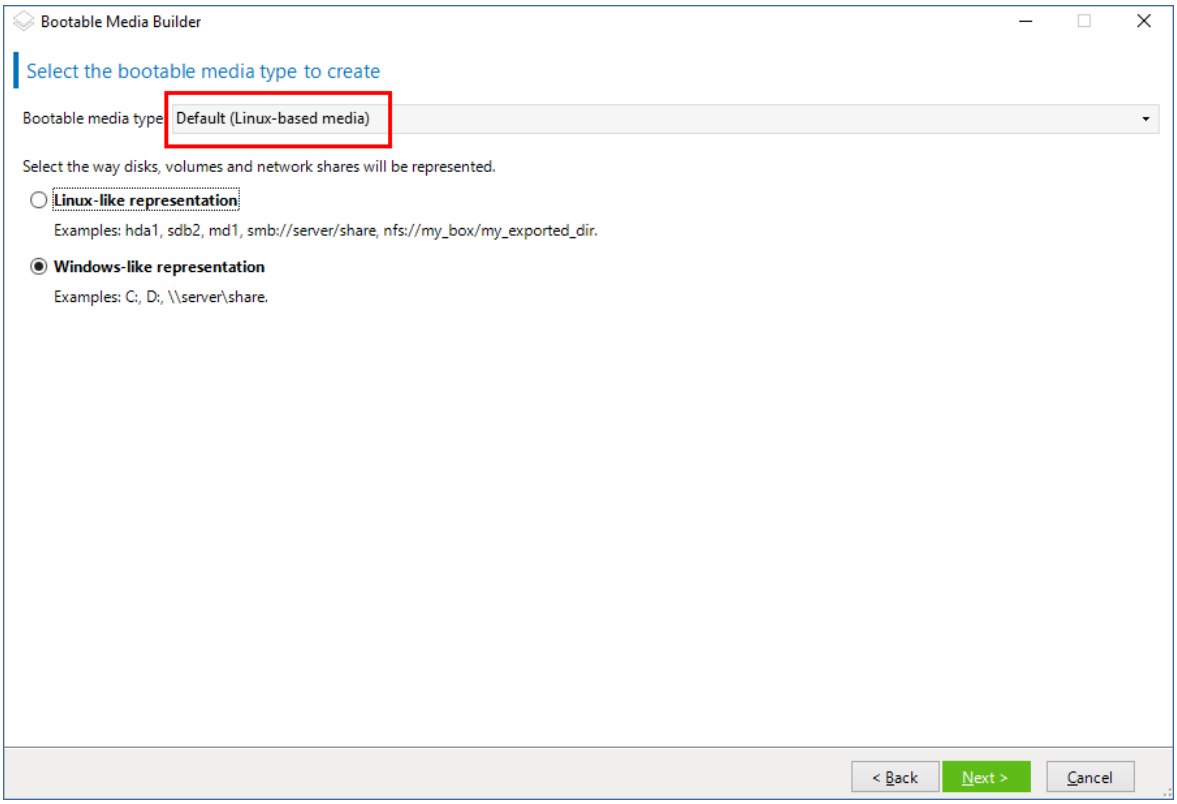
Linux ベースのブータブル メディア

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. 全機能を備えたブータブルメディアを作成するには、Acronis Cyber Protectライセンスキーを指定します。このキーは、ブータブルメディアに含まれる機能を決定するために使用されます。どのマシンからもライセンスが取り消されることはありません。
   ライセンスキーを指定しない場合、作成されるブータブルメディアは復元操作でのみ使用できます。



3. [**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。
   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と同様のボリューム表記を行うメディアは、ボリュームをたとえばhda1、sdb2のように表示します。復元の開始前に、MD ドライブおよび論理ボリューム（LVM）を再構築しようとします。
   - Windowsと同様のボリューム表記を行うメディアは、ボリュームをたとえばC:、D:のように表示します。これは、動的ボリューム（LDM）にアクセスします。



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。

   たとえば、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。

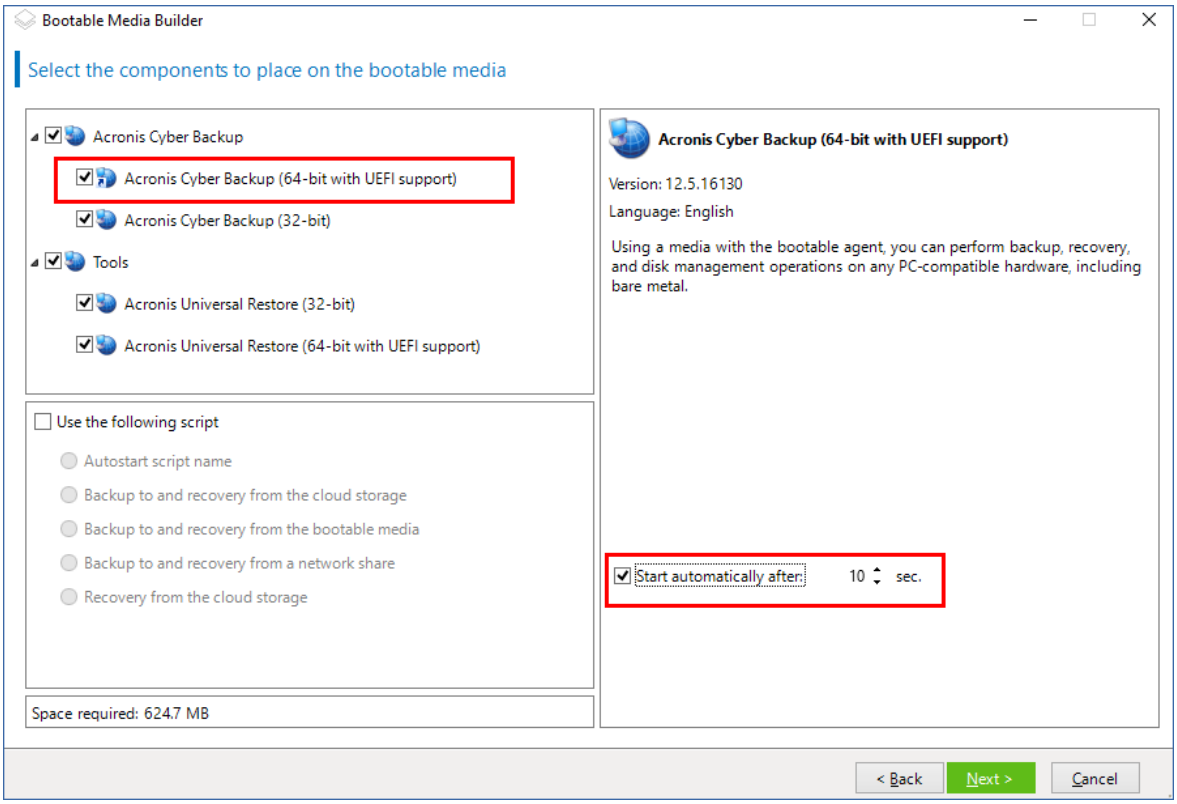
   利用可能なパラメータの詳細情報については、「カーネルパラメータ」を参照してください。
5. （オプション）ブータブルメディアで使用する言語を選択します。
6. メディアに配置する次のいずれかのコンポーネント、または両方のコンポーネントを選択します:

   Acronis Cyber Protect ブータブルエージェント、Universal Restore（異なるハードウェアでシステムのリストアを計画している場合）

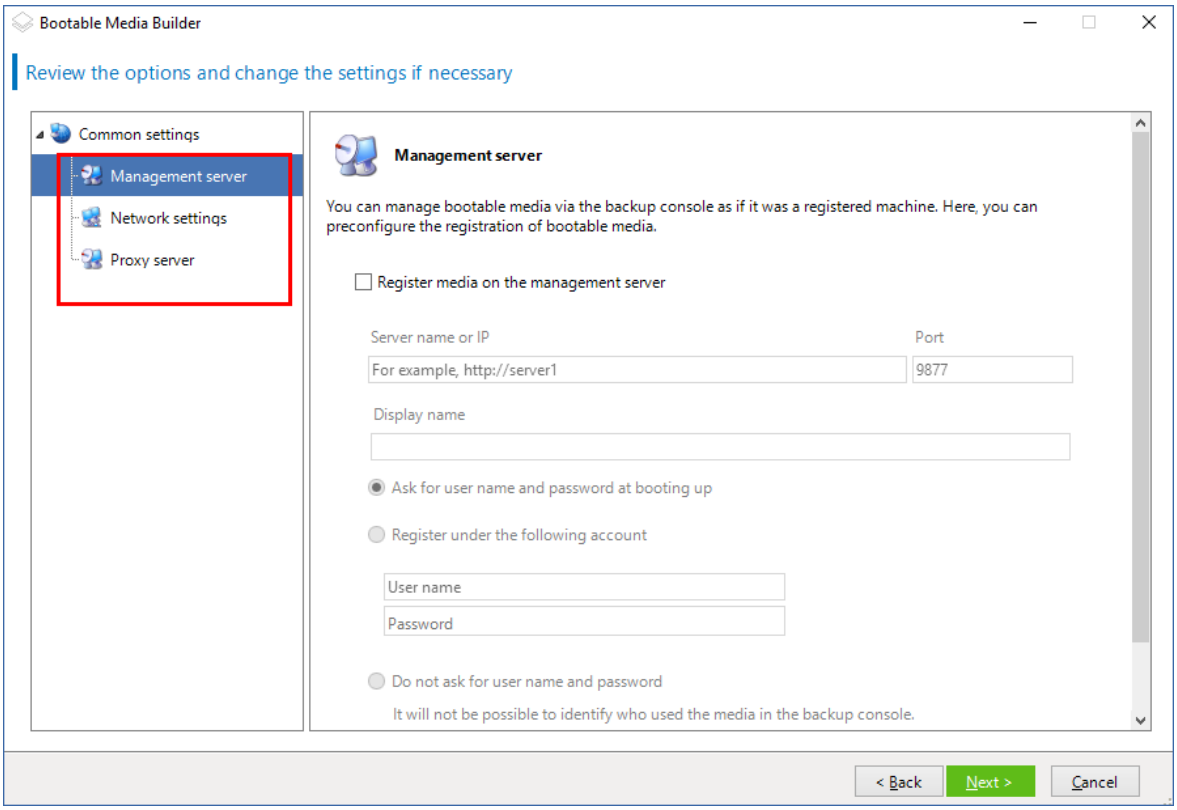
   ブータブルエージェントを使用すると、ベアメタルを含むすべてのPC/AT互換機でバックアップ、復元、ディスク管理操作を実行できます。

   Universal Restoreを使用すると、異なるハードウェアまたは仮想マシンに復元されたオペレーティングシステムを起動できます。このツールは、オペレーティングシステムの起動にとって重要なデバイス（ストレージコントローラー、マザーボード、チップセットなど）のドライバを検索しインストールします。
7. （オプション）ブートメニューのタイムアウト時間と、タイムアウトしたときに自動的に起動するコンポーネントを指定します。指定するには、左上のペインにある必要なコンポーネントをクリックし、その時間を設定します。これにより、WDS/RISから起動するときに、無人のオンサイト操作ができます。

   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。



8. （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。
9. （オプション）起動時にメディアをManagement Server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、「管理サーバー」を参照してください。



10. （オプション）ネットワーク設定を指定します。コンピュータのネットワーク アダプタに割り当てる TCP/IP 設定です。 詳細については、"ネットワーク設定"（370ページ）を参照してください。
11. （オプション）ネットワークポートを指定します。ブータブルエージェントが受信接続をリッスンするTCPポートです。
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. メディアの種類を選択します。次の操作を実行できます。
    - ISOイメージを作成します。次に、CD/DVDにイメージを保存します。保存したイメージは、ブータブルUSBフラッシュドライブの作成や仮想マシンへの接続に使用できます。
    - ZIPファイルを作成します。
    - Acronis PXE Server への選択したコンポーネントのアップロード。
    - WDS/RIS への選択したコンポーネントのアップロード。
14. （オプション）Universal Restoreで使用するWindowsシステムドライバを追加します。Universal Restoreがメディアに追加され、WDS/RIS以外のメディアが選択されている場合にこのウィンドウが表示されます。
15. 確認が表示される場合は、WDS/RISのホスト名/IPアドレスと資格情報、またはメディアISOファイルへのパスを指定します。
16. 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

このウィンドウでは、Linux カーネル パラメータを 1 つ以上指定できます。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、一般的に、ブータブル メディアの操作中に問題が発生すると使用されます。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、コンピュータ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。

このパラメータを指定しない場合、コマンド プロンプトが表示される前に、すべてのスタートアップ 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下で作業するときは、CTRL + SHIFT キーを使用して使用可能なレイアウトを循環させます。

ブータブルメディアのスクリプト

ブータブルメディアで所定の操作一式を実行する場合は、ブータブルメディアビルダでのメディア作成中にスクリプトを指定できます。そのメディアでブートするたび、ユーザーインターフェイスが表示される代わりにこのスクリプトが実行されます。

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を使用したバックアップと復元（**entire_pc_cloud**）
- ブータブルメディアを使用したバックアップと復元（**entire_pc_local**）
- ネットワーク共有を使用したバックアップと復元（**entire_pc_share**）
- クラウドストレージからの復元（**golden_image**）

スクリプトは、ブータブルメディアビルダ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を使用したバックアップと復元

このスクリプトは、マシンをクラウドストレージにバックアップ、またはこのスクリプトによってクラウドストレージに作成された直近のバックアップからマシンを復元します。スクリプトを開始すると、ユーザーはバックアップ、復元、ユーザーインターフェイスの起動の中から選択するよう求められます。

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. クラウドストレージのユーザー名とパスワード
2. （オプション）スクリプトによってバックアップの暗号化またはバックアップへのアクセスに使用されるパスワード

ブータブルメディアを使用したバックアップと復元

このスクリプトは、マシンをブータブルメディアにバックアップ、またはこのスクリプトによって同じメディアに作成された直近のバックアップからマシンを復元します。スクリプトを開始すると、ユーザーはバックアップ、復元、ユーザーインターフェイスの起動の中から選択するよう求められます。

ブータブルメディアビルダでは、スクリプトによってバックアップの暗号化またはバックアップへのアクセスに使用されるパスワードを指定できます。

ネットワーク共有を使用したバックアップと復元

このスクリプトは、コンピュータをネットワーク共有にバックアップ、またはネットワーク共有に置かれた直近のバックアップからコンピュータを復元します。スクリプトを開始すると、ユーザーはバックアップ、復元、ユーザーインターフェイスの起動の中から選択するよう求められます。

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. ネットワーク共有パス。
2. ネットワーク共有のユーザー名とパスワード。
3. （オプション）バックアップファイル名。デフォルト値は、**AutoBackup**です。スクリプトによってバックアップを既存のバックアップに追加する場合、またはデフォルト以外の名前を持つバックアップから復元する場合は、デフォルト値をこのバックアップのファイル名に変更します。

   バックアップファイル名を確認するには

   a. Cyber Protectウェブコンソールで、**[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。
4. （オプション）スクリプトによってバックアップの暗号化またはバックアップへのアクセスに使用されるパスワード

クラウドストレージからのバックアップ

このスクリプトは、クラウドストレージに置かれた直近のバックアップからコンピュータを復元します。スクリプトを開始すると、ユーザーは次の項目を指定するよう求められます。

1. クラウドストレージのユーザー名とパスワード
2. バックアップが暗号化されている場合はパスワード

このクラウドストレージアカウントでは、1台のコンピュータのみのバックアップを保存することを推奨します。そうしないと、別のコンピュータのバックアップが現在のコンピュータのバックアップよりも新しい場合、スクリプトは別のコンピュータのバックアップを選択します。

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	**種類**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 （**スピナー**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 （**スピナー**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 （**スピナー**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	コントロール値が空（0）または（1）でないこと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

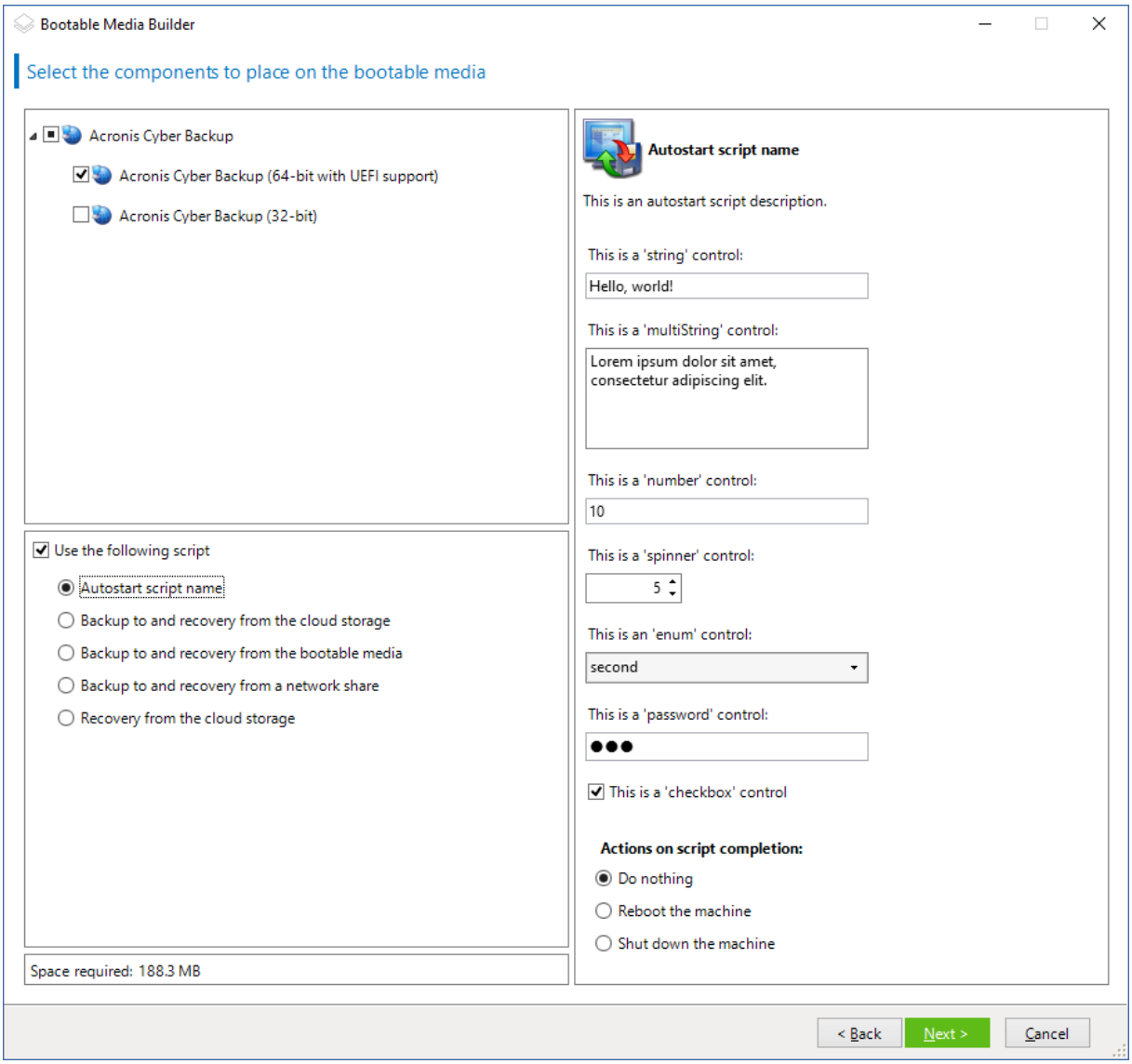
checkbox	2つの状態（選択されていない状態または選択された状態）があるチェックボックス。

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":"Autostart script name",
        "description":"This is an autostart script description.",
        "variables": {
                "var_string": {
                        "displayName":"VAR_STRING",
                        "type":"string", "order": 1,
                        "description":"This is a 'string' control:", "default": "Hello, world!"
                },
                "var_multistring": {
                        "displayName":"VAR_MULTISTRING",
                        "type":"multiString", "order": 2,
                        "description":"This is a 'multiString' control:",
                        "default":"Lorem ipsum dolor sit amet,\nconsectetur adipiscing elit."
                },
                "var_number": {
                        "displayName":"VAR_NUMBER",
                        "type":"number", "order": 3,
                        "description":"This is a 'number' control:", "default": 10
                },
                "var_spinner": {
                        "displayName":"VAR_SPINNER",
                        "type":"spinner", "order": 4,
                        "description":"This is a 'spinner' control:",
                        "min":1, "max":10, "step": 1, "default": 5
                },
                "var_enum": {
```

```
                "displayName":"VAR_ENUM",
                "type":"enum", "order": 5,
                "description":"This is an 'enum' control:",
                "items": ["first", "second", "third"], "default": "second"
        },
        "var_password": {
                "displayName":"VAR_PASSWORD",
                "type":"password", "order": 6,
                "description":"This is a 'password' control:", "default": "qwe"
        },
        "var_checkbox": {
                "displayName":"VAR_CHECKBOX",
                "type":"checkbox", "order": 7,
                "description":"This is a 'checkbox' control", "default":1
        }
    }
}
```

ブータブルメディアビルダでは、次のように表示されます。



管理サーバー

ブータブルメディアを作成する際に、Management Serverへのメディア登録を事前に設定できます。

メディアを登録することによって、登録済みのマシンのように、Cyber Protect ウェブ コンソールからメディアを管理できます。リモートアクセスが使いやすいだけではなく、管理者は、ブータブルメディアで実行されるすべての処理を追跡できるようになります。処理は **[アクティビティ]** に記録されているため、誰がいつ処理を開始したかを確認することができます。

登録が事前に設定されていない場合は、マシンをメディアから起動した後でもメディアを登録することができます。

Management Serverで登録を事前に設定するには

1. **[Management Serverでメディアを登録]** チェックボックスをオンにします。
2. **[サーバーの名前またはIP]** にManagement Serverがインストールされているマシンのホスト名またはIPアドレスを指定します。次のいずれかの形式を使用できます。

- http://<**サーバー**>。例: http://10.250.10.10、http://server1
- <**IPアドレス**>例:10.250.10.10
- <**ホスト名**>。例: server1、server1.example.com

3. [**ポート**] にManagement Serverにアクセスするために使用されるポートを指定します。デフォルト値は9877です。
4. [**表示名**] に、Cyber Protect ウェブ コンソール内でのこのマシンの表示名を指定します。このフィールドを空にすると、表示名は次のいずれかに設定されます。
   - コンピュータが以前にManagement Serverに登録された場合は、同じ名前になります。
   - その他の場合は、コンピュータの完全修飾ドメイン名（FQDN）またはIPアドレスのいずれかが使用されます。
5. メディアをManagement Serverに登録するために使用するアカウントを選択します。次から選択できます。
   - [**起動時にユーザー名とパスワードを確認**]

     メディアからマシンを起動する際に、資格情報を毎回入力する必要があります。

     登録には、アカウントが管理サーバーの管理者の一覧に含まれている必要があります（[**設定**] > [**アカウント**]）。Cyber Protect ウェブ コンソールでは、指定したアカウントに付与された許可に従って、組織の下または特定の部署の下でメディアを利用できるようになります。

     ブータブルメディアのインターフェイスでは、[**ツール**] > [**Management Serverでメディアを登録**] をクリックすることで、ユーザー名およびパスワードを変更できるようになります。
   - [**次のアカウントで登録**]

     メディアからマシンを起動する際に、マシンは毎回自動的に登録されます。

     指定するアカウントは、管理サーバーの管理者の一覧に含まれている必要があります（[**設定**] > [**アカウント**]）。Cyber Protect ウェブ コンソールでは、指定したアカウントに付与された許可に従って、組織の下または特定の部署の下でメディアを利用できるようになります。

     ブータブルメディアのインターフェイスで、登録パラメータを変更することはできません。

ネットワーク設定

ブータブル メディアを作成するときに、ブータブル エージェントで使用するネットワーク接続をあらかじめ設定することができます。次のパラメータをあらかじめ設定できます。

- 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

コンピュータでブータブル エージェントが起動すると、コンピュータのネットワーク インターフェイス カード（NIC）に設定が適用されます。設定があらかじめ設定されていない場合、DHCP 自動設定が使用されます。コンピュータでブータブル 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設定

最大で 10 個のネットワーク インターフェイス カードの TCP/IP 設定をあらかじめ設定できます。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 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、必要に応じて、存在しない NIC の設定を構成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コンピュータだけでなく、任意のコンピュータのブータブル メディアをカスタマイズできます。そのためには、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し、以下同様にします。そのコンピュータでブータブル 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、運用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のネットワーク アダプタの 1 つを使用できます。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。

ネットワーク ポート

ブータブルメディアを作成するときに、ブータブルエージェントが acrocmd ユーティリティから受信接続をリッスンするネットワーク ポートをあらかじめ設定しておくことができます。選択肢は次のとおりです。

- デフォルトのポート
- 現在使用中のポート
- 新しいポート（ポート番号を入力）

ポートがあらかじめ設定されていないときは、エージェントはポート番号(9876)を使用します。

Universal Restore のドライバ

ブータブル メディアを作成する際に、Windows ドライバをメディアに追加できます。Universal Restore はこのドライバを使用して、異なるハードウェアに移行した Windows を起動します。

次の処理を実行するように Universal Restore を設定できます。

- ブータブル メディア内で、復元先ハードウェアに最も適したドライバを検索する。
- 明示的に指定した大容量記憶装置のドライバをブータブル メディアから取得する。この処理は、復元先ハードウェアにハード ディスク用の特定の大容量記憶装置コントローラ（SCSI、RAID、ファイバ チャネル アダプタなど）が搭載されているときに必要になります。

ドライバは、ブータブル メディア上で表示可能な Drivers フォルダに格納されます。ドライバは復元先コンピュータの RAM には読み込まれないため、Universal Restore で操作を実行している間は、メディアを挿入または接続したままにしておく必要があります。

リムーバブル メディア、その ISO、またはフラッシュ ドライブなどの取り外し可能なメディアを作成している場合、ブータブル メディアにドライバを追加できます。WDS/RISではドライバをアップロードできません。

ドライバは、INF ファイルまたはそのファイルが格納されているフォルダを追加することで、グループ単位でのみ一覧に追加できます。INF ファイルから個々のドライバを選択することはできませんが、メディア ビルダには参照用としてファイルの内容が表示されます。

ドライバを追加する手順は、次のとおりです。

1. **[追加]** をクリックし、INF ファイルまたは INF ファイルが格納されているフォルダを参照します。
2. INF ファイルまたはフォルダを選択します。
3. **[OK]** をクリックします。

ドライバは、INF ファイルを削除することにより、グループ単位のみで一覧から削除できます。

ドライバを削除する手順は、次のとおりです。

1. INF ファイルを選択します。
2. **[削除]** をクリックします。

WinPE ベースのブータブル メディア

ブータブルメディアビルダーには、Acronis Cyber ProtectをWinPEと統合するための2つの方法が用意されています。

- プラグインが組み込まれた PE ISO を最初から作成する。
- 将来使用する目的で（手動でのISO作成、イメージへの他のツールの追加など）、Acronisプラグインをwimファイルに追加する。

準備作業を追加することなくWinREベースのPE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PEイメージを作成することもできます。

WinREベースのPEイメージ

WinREベースのイメージの作成は、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、8.1、10（32ビットおよび64ビット）
- Windows Server 2012、2016、2019（64ビット）

PE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（Windows 10用PE）

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。

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。

注意
Windows PE 4.0以降に基づくブータブルメディアではディスク管理機能は使用できません。つまり、ディスク管理はWindows 7以前のオペレーティングシステムについてサポートされています。Windows 8以降でディスク管理操作を実行するには、Acronis Disk Directorをインストールする必要があります。詳細については、KB記事: https://kb.acronis.com/content/47031を参照してください。

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修正できるようにするには、Windows Automated Installation Kit（AIK）がインストールされている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。AIK がインストールされているコンピュータがない場合は、次の手順に従って準備します。

AIK がインストールされているコンピュータを準備する手順は、次のとおりです。

1. Windows 自動インストール キットをダウンロードしてインストールします。
   Automated Installation Kit (AIK) for Windows Vista (PE 2.0):
   http://www.microsoft.com/Downloads/details.aspx?familyid=C7D4BC6D-15F3-4284-9123-679830D629F2&displaylang=en
   Automated Installation Kit (AIK) for Windows Vista SP1 and Windows Server 2008 (PE 2.1):
   http://www.microsoft.com/downloads/details.aspx?FamilyID=94bb6e34-d890-4932-81a5-5b50c657de08&DisplayLang=en
   Automated Installation Kit (AIK) for Windows 7 (PE 3.0):
   http://www.microsoft.com/downloads/details.aspx?familyid=696DD665-9F76-4177-A811-39C26D3B3B34&displaylang=en
   Automated Installation Kit (AIK) Supplement for Windows 7 SP1 (PE 3.1):

http://www.microsoft.com/download/en/details.aspx?id=5188
上記のリンクには、インストールのシステム要件も含まれています。

2. （オプション）WAIK を DVD に書き込むかフラッシュ ドライブにコピーします。
3. キットから Microsoft .NET Framework をインストールします（ハードウェアにより NETFXx86 か NETFXx64 のどちらか）。
4. Microsoft Core XML（MSXML）5.0 または 6.0 Parser をインストールします。
5. Windows AIK をインストールします。
6. 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。

Windows AIK に同梱のヘルプ マニュアルを使用して、操作に慣れることをお勧めします。ドキュメントにアクセスするには、[スタート] メニューから **[Microsoft Windows AIK]** → **[ドキュメント]** を選択します。

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、Windows アセスメント & デプロイメント キット（ADK）がインストールされている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。ADK がインストールされているコンピュータがない場合は、次の手順に従って準備します。

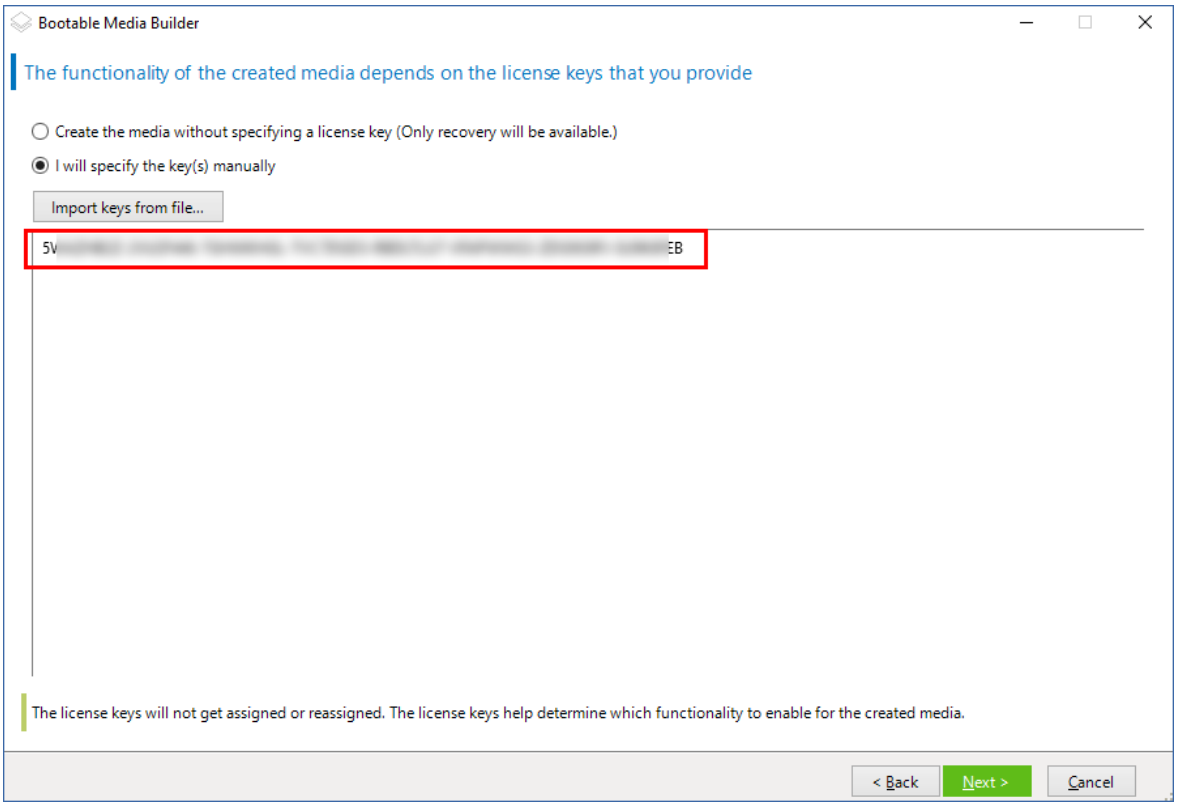
ADK がインストールされているコンピュータを準備する手順は、次のとおりです。

1. アセスメント & デプロイメント キットのセットアップ プログラムをダウンロードします。
   Windows 8（PE 4.0）用のアセスメント & デプロイメント キット（ADK）：
   http://www.microsoft.com/en-us/download/details.aspx?id=30652。
   Windows 8.1（PE 5.0）用のアセスメント & デプロイメント キット（ADK）：
   http://www.microsoft.com/ja-jp/download/details.aspx?id=39982。
   Windows 10（Windows 10 用 PE）用 Windows アセスメント & デプロイメントキット（ADK）：
   https://msdn.microsoft.com/en-us/windows/hardware/dn913721%28v=vs.8.5%29.aspx。
   上記のリンクには、インストールのシステム要件も含まれています。
2. アセスメント & デプロイメント キットをコンピュータにインストールします。
3. 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。

Acronis プラグインの WinPE への追加

WinPE に Acronis プラグインを追加するには、次の操作を実行します。

1. ブータブルメディアビルダーを起動します。
2. 全機能を備えたブータブルメディアを作成するには、Acronis Cyber Protectライセンスキーを指定します。このキーは、ブータブルメディアに含まれる機能を決定するために使用されます。どのマシンからもライセンスが取り消されることはありません。
   ライセンスキーを指定しない場合、作成されるブータブルメディアは復元操作でのみ使用できます。



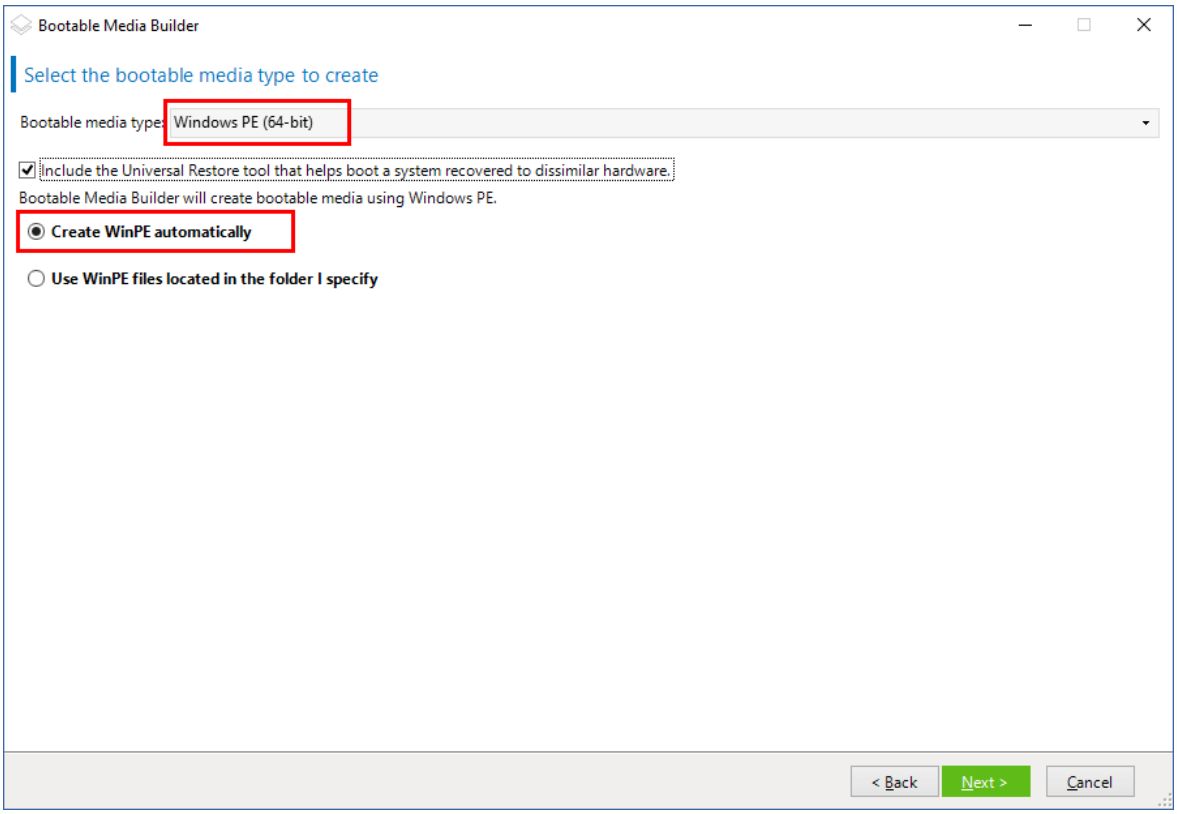
3. **[ブータブルメディアの種類]** で、**[Windows PE]** または **[Windows PE（64ビット）]** を選択します。UEFI（Unified Extensible Firmware Interface）を使用するコンピュータを起動するには、64 ビット メディアが必要です。

   [ブータブルメディアの種類] で**[Windows PE]** を選択した場合は、次の手順を最初に実行します。

   - **[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。
   - **%PROGRAM_FILES%¥Acronis¥BootableComponents¥WinPE32** にプラグインを保存します。

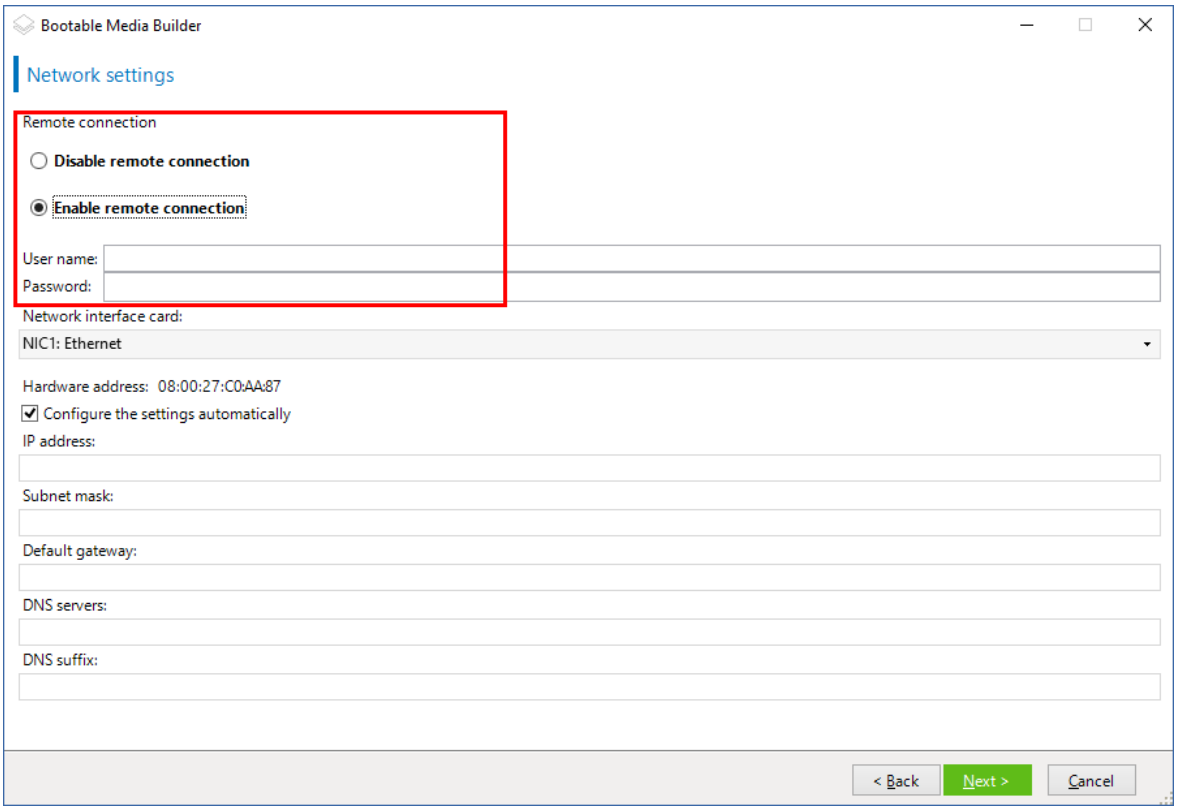
   オペレーティングシステムを異なるハードウェアまたは仮想コンピュータに復元し、システムのブータビリティを確保する必要がある場合は、**[Universal Restoreツールを含める...]** チェックボックスをオンにします。
4. **[WinPEを自動的に作成]** を選択します。

   適切なスクリプトが実行され、次のウィンドウに進みます。



5. ブータブルメディアで使用する言語を選択します。
6. メディアから起動したコンピュータへのリモート接続を有効にするかどうかを選択します。有効にする場合は、acrocmd ユーティリティが異なるマシンで実行されている場合にコマンドラインで指定するユーザー名とパスワードを入力します。これらのフィールドを空白のままにすると、資格情報がなくても、コマンドラインインターフェース経由でリモート接続が可能です。

   これらの資格情報は、Cyber Protect ウェブ コンソールから管理サーバーにメディアを登録するときにも必要になります。



7. コンピュータのネットワークアダプターのネットワーク設定を指定するか、DHCP自動構成を選択します。

注意
ネットワーク設定は、Acronis Cyber Protect 15 AdvancedおよびAcronis Cyber Protect 15 Backup Advancedのライセンスでのみ利用可能です。詳細な機能の比較については、こちらのナレッジベースの記事を参照してください。

8. （オプション）起動時にメディアをManagement Server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、「管理サーバー」を参照してください。
9. （オプション）Windows PE に追加する Windows ドライバを指定します。

Windows PE でコンピュータを起動すると、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 WinPE 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、64 ビット WinPE 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。

Universal Restore for Windowsの設定時にこの追加したドライバを指定することもできます。Universal Restore を使用するには、32 ビットまたは 64 ビットのどちらの Windows オペレーティングシステムを復元するかに応じて 32 ビットまたは 64 ビットの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 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。

10. ISO または WIM イメージを作成するか、またはメディアをサーバー（WDS、または RIS）にアップロードするかを選択します。
11. 作成するイメージ ファイルのフルパス（ファイル名を含む）を指定します。または、サーバーを指定し、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。
12. サマリー画面で設定を確認し、**[実行]** をクリックします。
13. サードパーティのツールを使用して .ISO を CD または DVD に書き込むか、ブータブルフラッシュドライブを準備します。

コンピュータが WinPE で起動すると、エージェントが自動的に起動します。

結果の 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。

  ```
  copy c:\AcronisMedia.wim c:\winpe_x86\ISO\sources\boot.wim
  ```

- **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。

Windows PE のカスタマイズの詳細については、『Windowsプリインストール環境（Windows PE 2.xおよび3.x）ユーザーズ ガイド』（Winpe.chm）を参照してください。Windows PE 4.0以降のカスタマイズについては、Microsoft TechNet Libraryを参照してください。

メディアから起動したコンピュータへの接続

ブータブルメディアからコンピュータが起動すると、コンピュータ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

現在の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、マシンの各ネットワークインターフェイスカード（NIC）の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、コンピュータ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。

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。

リモート接続

メディアにリモート接続するには、「Management Serverでのメディアの登録」の説明に従って、メディアをManagement Serverに登録します。

Management Serverでメディアを登録

ブータブルメディアを登録することによって、登録済みのマシンのように、Cyber Protectウェブコンソールからメディアを管理できます。これは、ブート方法（物理メディア、Startup Recovery Manager Acronis PXE Server、WDSまたはRIS）に関係なく、すべてのブータブルメディアに適用されます。ただし、macOSで作成されたブータブルメディアを登録することはできません。

Acronis Cyber ProtectのAdvancedライセンスが1つ以上管理サーバーに追加されている場合にのみ、メディアを登録できます。

メディアUIからメディアを登録できます。

登録パラメータは、ブータブルメディアビルダのManagement Serverのオプションで事前に設定できます。すべての登録パラメータが事前に設定されていると、メディアはCyber Protectウェブコンソールに自動的に表示されます。パラメータの一部だけが事前に設定されている場合、次の手順のいくつかは利用できないことがあります。

メディアUIからのメディアの登録

メディアは、ブータブルメディアビルダを使用してダウンロードまたは作成できます。

メディアUIからメディアを登録するには

1. メディアからコンピュータを起動します。
2. 次のいずれかを実行します。
   - 起動ウィンドウの **[Management Server]** で **[編集]** をクリックします。
   - ブータブルメディアのインターフェイスで、**[ツール]** > **[Management Serverでメディアを登録]** をクリックします。
3. **[登録]** で、Management Serverがインストールされているコンピュータのホスト名またはIPアドレスを指定します。次のいずれかの形式を使用できます。
   - `http://<サーバー>`。例: `http://10.250.10.10`、`http://server1`
   - `<IPアドレス>`例:`10.250.10.10`
   - `<ホスト名>`。例: `server`、`server1.example.com`
4. **[ユーザー名]** および **[パスワード]** に、管理サーバーの管理者の一覧に含まれているアカウントの資格情報を入力します（**[設定]** > **[アカウント]**）。Cyber Protectウェブコンソールでは、指定したアカウントに付与された許可に従って、組織の下または特定の部署の下でメディアを利用できるようになります。
5. **[表示名]** に、Cyber Protectウェブコンソール内でのこのマシンの表示名を指定します。このフィールドを空にすると、表示名は次のいずれかに設定されます。
   - コンピュータが以前にManagement Serverに登録された場合は、同じ名前になります。
   - その他の場合は、コンピュータの完全修飾ドメイン名（FQDN）またはIPアドレスのいずれかが使用されます。
6. **[OK]** 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バックアップおよび復元操作に似ています。違いは次のとおりです。

1. Windows 形式のボリューム表示のブータブルメディアでは、ボリュームのドライブ文字は Windows の文字と同じになります。Windows のドライブ文字が無いボリューム（ 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いている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. ブータブルメディアを使用して作成したバックアップの名前は、簡易ファイル名 です。標準の名前がバックアップに割り当てられるのは、それらのバックアップが標準ファイル名前付けが使用されて

いる既存のアーカイブに追加される場合か、保存先で簡易ファイル名がサポートされていない場合のみです。

4. Linux 形式のボリュームのブータブルメディアでは、バックアップを NTFS 形式のボリュームに書き込むことはできません。必要に応じて、Windows 形式のボリューム表示のメディアに切り替えます。ブータブルメディアボリューム表示を切り替えるには、**[ツール]** > **[ボリューム表示の変更]** をクリックします。
5. 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。
6. 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。
7. 集中管理用格納域が［**アーカイブ**］ウィンドウのフォルダ ツリーに表示されない。
   管理対象の格納域を表示するには、以下の文字列を **[パス]** フィールドに入力します。
   bsp://node_address/vault_name/
   管理対象外の集中管理格納域にアクセスするには、格納域のフォルダのフル パスを入力します。
   アクセス ログイン情報を入力すると、格納域に配置されているアーカイブの一覧が表示されます。

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**」という入力し、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。

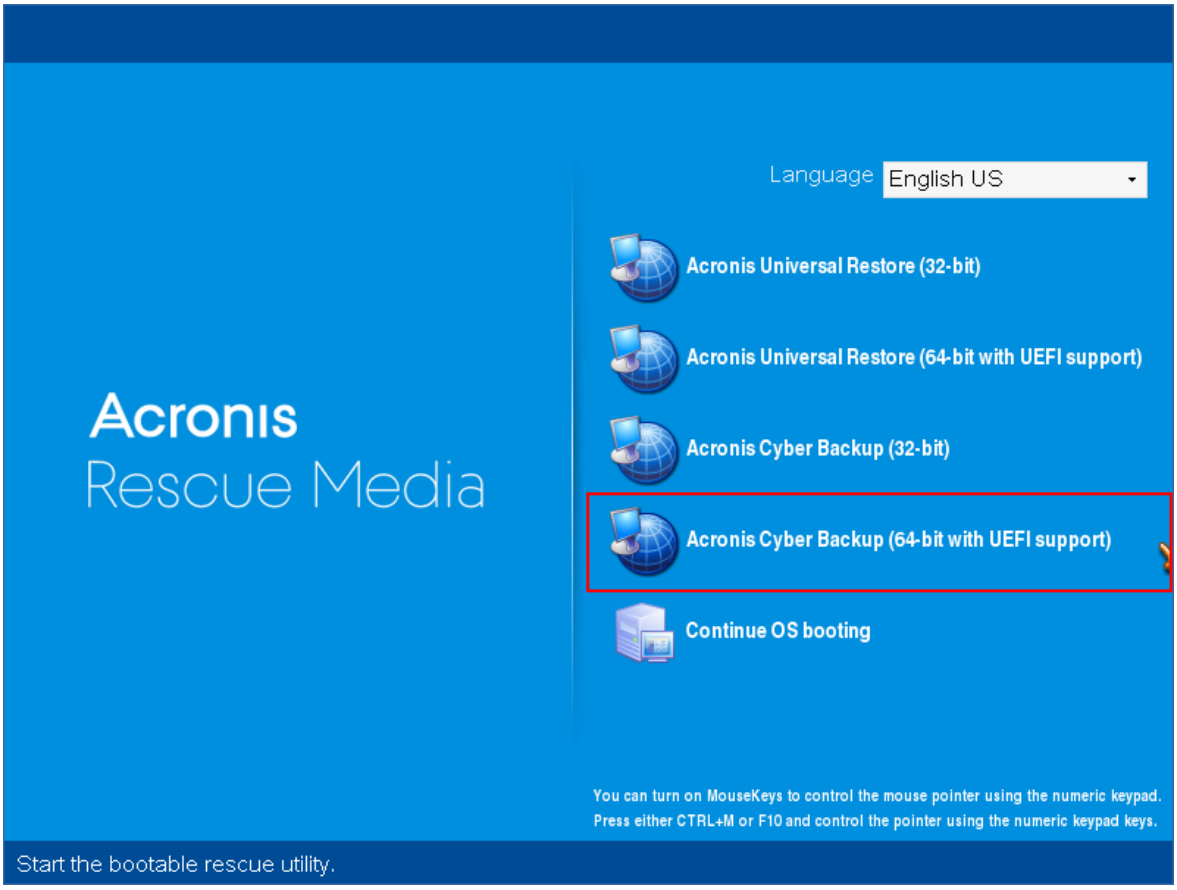
特定のハードウェア構成を起動する度に、この手順を繰り返したくない場合は、**[Linux カーネルパラメータ]** ウィンドウで適切なモード番号（ **vga=0x318** など）を入力して、ブータブルメディアを再作成します。

オンプレミスでのブータブルメディアによるバックアップ

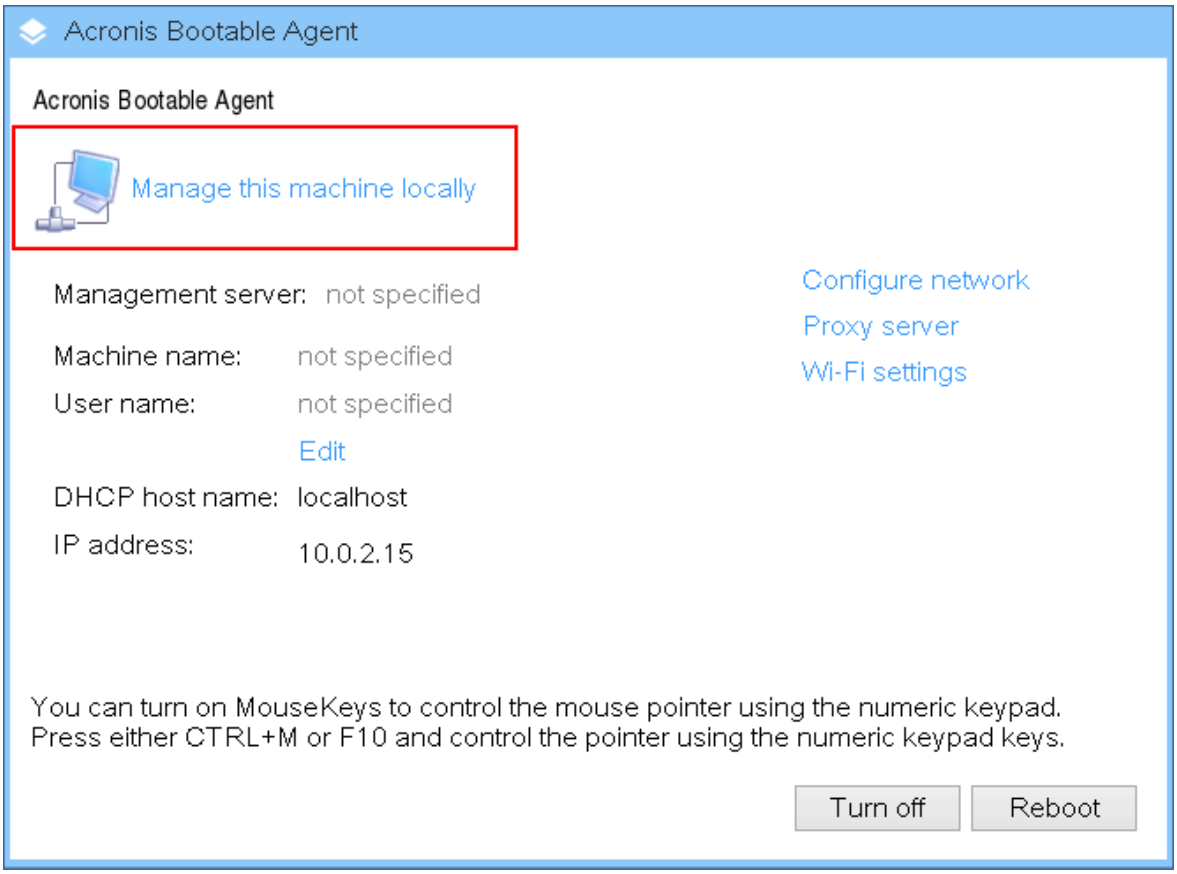
ブータブルメディアビルダーと、Acronis Cyber Protect ライセンスキーで作成したブータブルメディアでのみデータをバックアップできます。ブータブル メディアの作成方法については、「Linux ベースのブータブルメディア」または「Windows PE ベースのブータブルメディア」を参照してください。

ブータブルメディアでデータをバックアップする

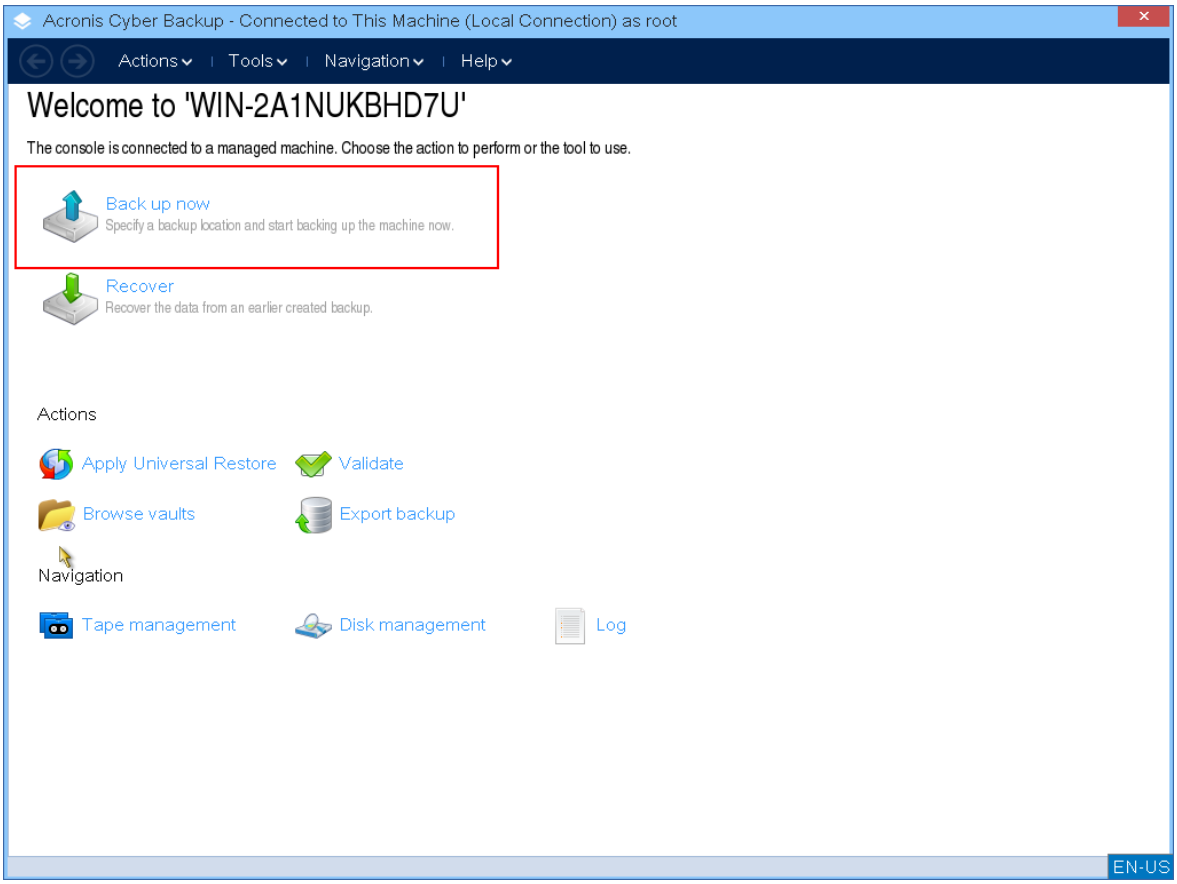
1. Acronis ブータブルレスキューメディアから起動します。



2. ローカルのマシンをバックアップするには、**[このコンピュータをローカルで管理]** をクリックします。リモート接続については、管理サーバーでのメディアの登録を参照してください。



3. [**今すぐバックアップ**] をクリックします。

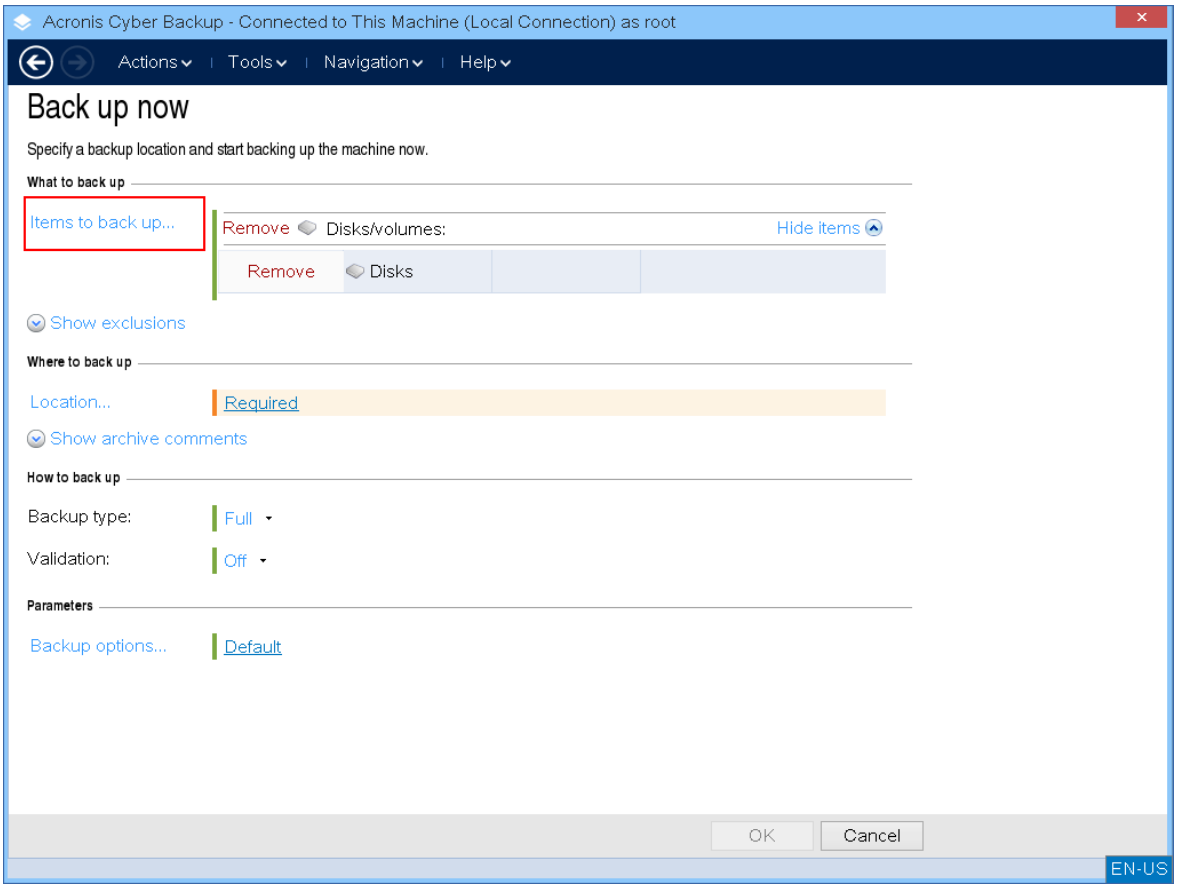


4. リムーバブルではないマシンのディスクはすべて自動的にバックアップ対象として選択されます。バックアップされるデータを変更するには、[**バックアップするアイテム**] をクリックし、任意のディスクまたはボリュームを選択します。

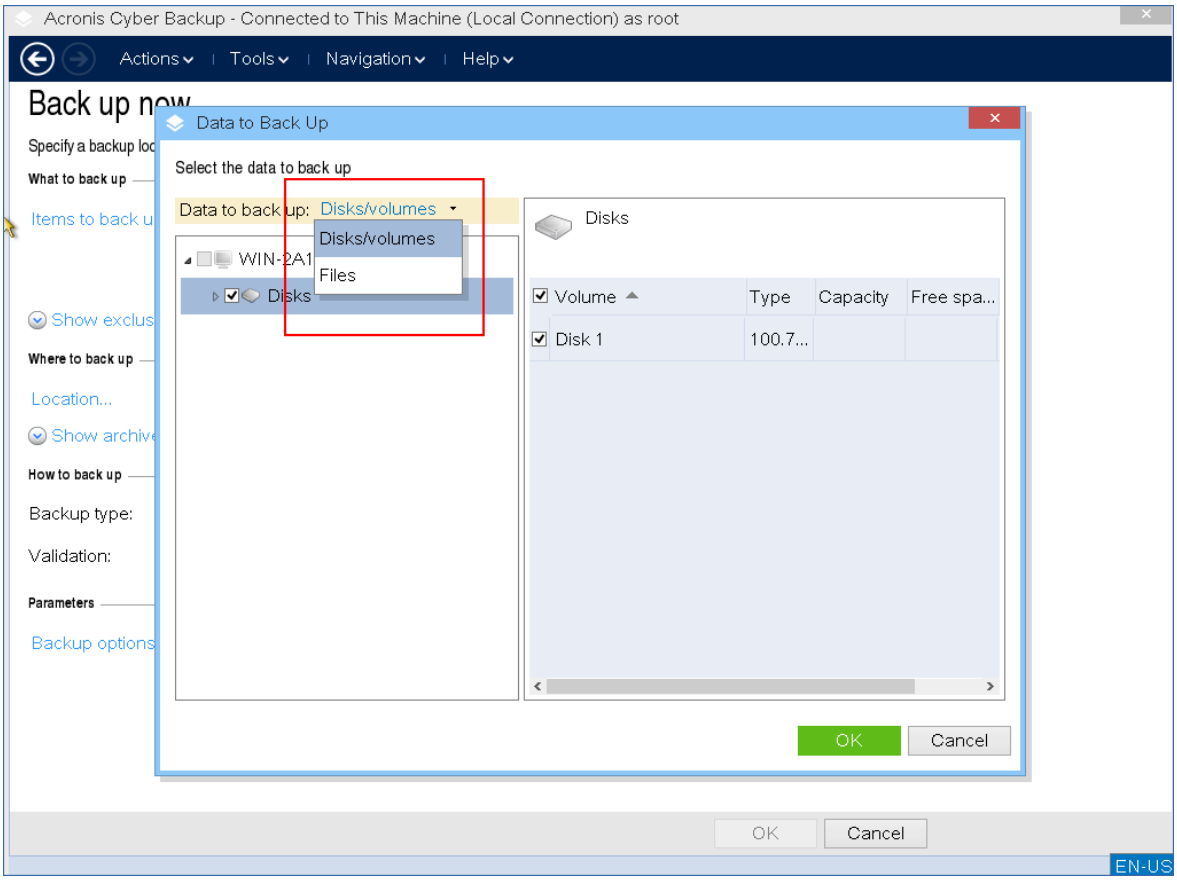
   バックアップするデータを選択するときには、次のメッセージが表示される場合があります。「このマシンを直接選択することはできません。以前のバージョンのエージェントがコンピュータにインストールされています。このマシンをバックアップ対象として選択するには、ポリシー ルールを使用してください。」これは安全に無視できる GUI の問題です。続行して、バックアップする個別のディスクまたはボリュームを選択してください。

注意

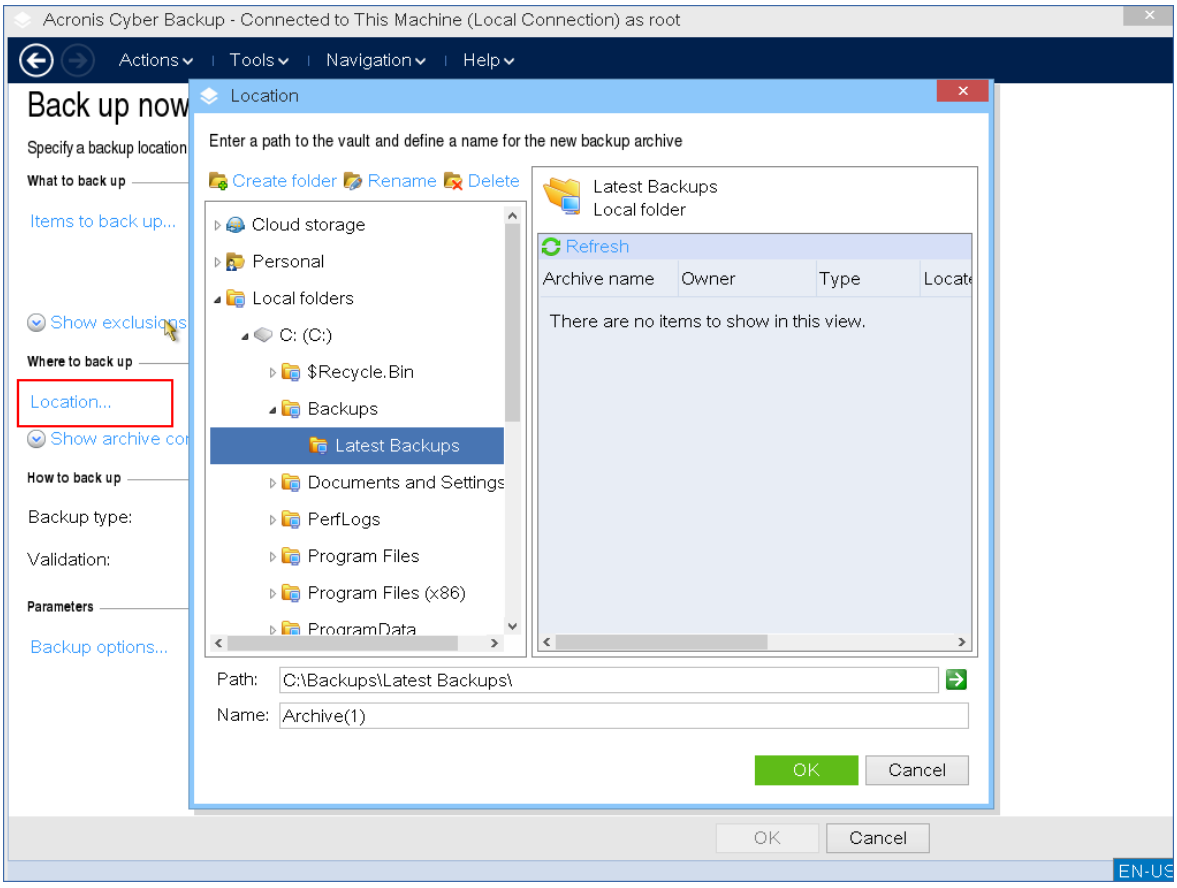
Linux ベースのブータブルメディアでは、Windows とは異なるドライブ文字が表示される場合があります。サイズやラベルで必要なドライブまたはパーティションを識別してください。



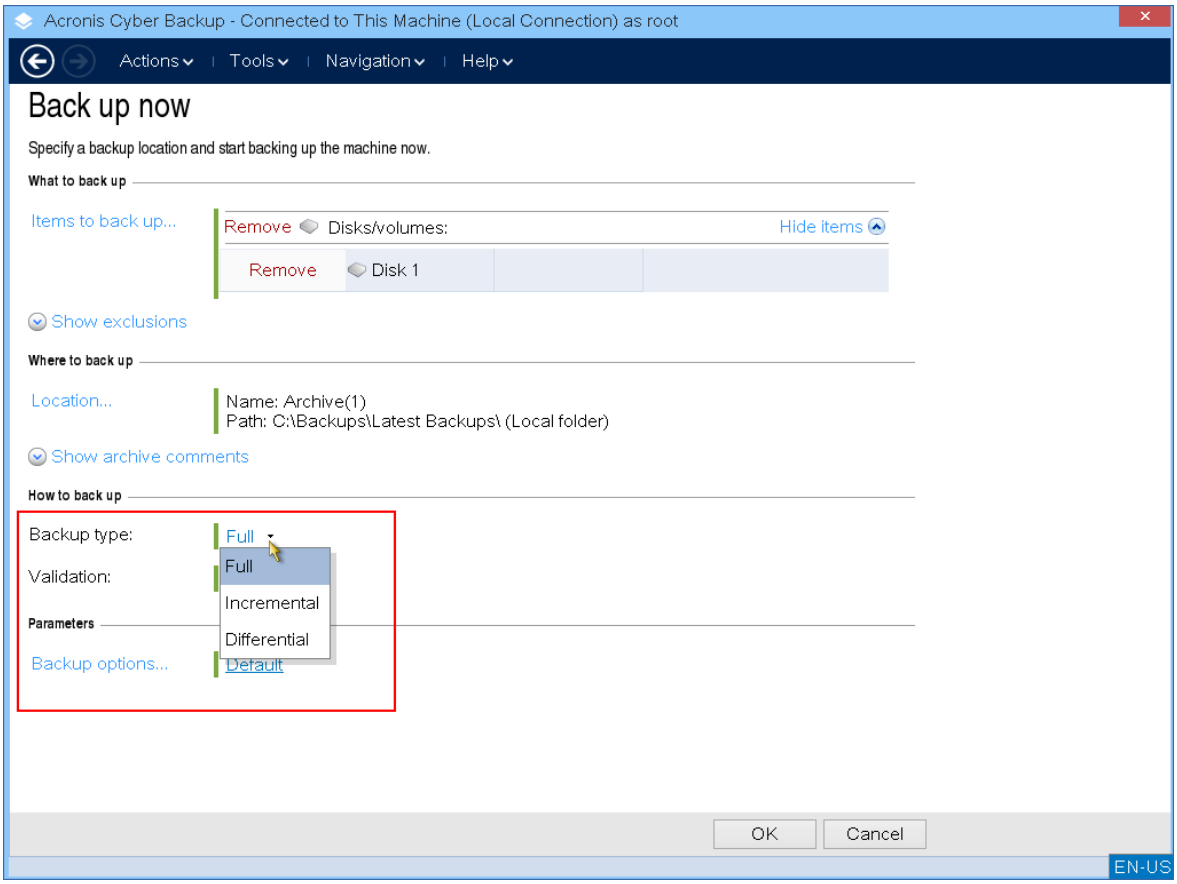
5. ディスクではなく、ファイルまたはフォルダをバックアップする必要がある場合、[**バックアップするデータ**] で [**ファイル**] に切り替えます。
   ブータブルメディアでは、ディスク/パーティションおよびファイル/フォルダのみを使用できます。データベースバックアップなどの他の種類のバックアップは、実行中のオペレーティングシステムでのみ利用できます。



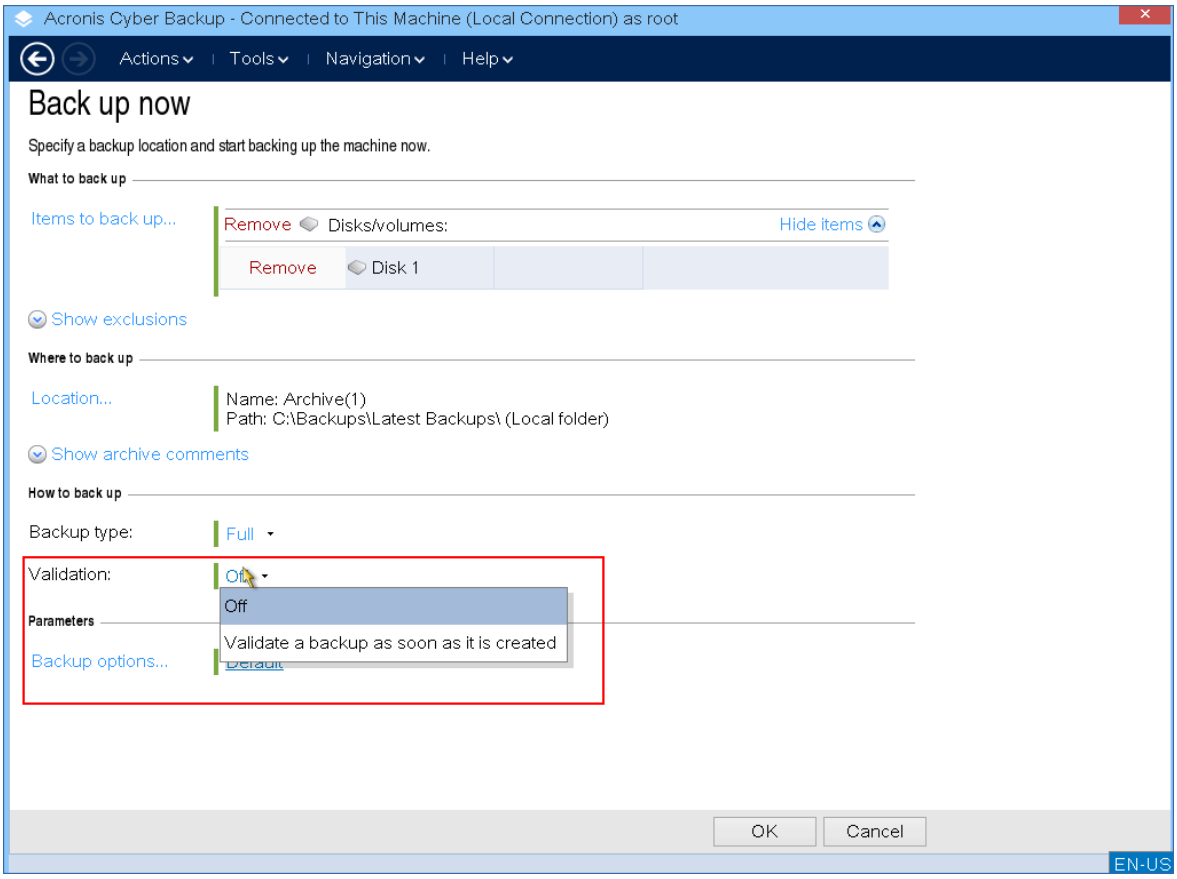
6. [**ロケーション**] をクリックし、バックアップの保存先を選択します。



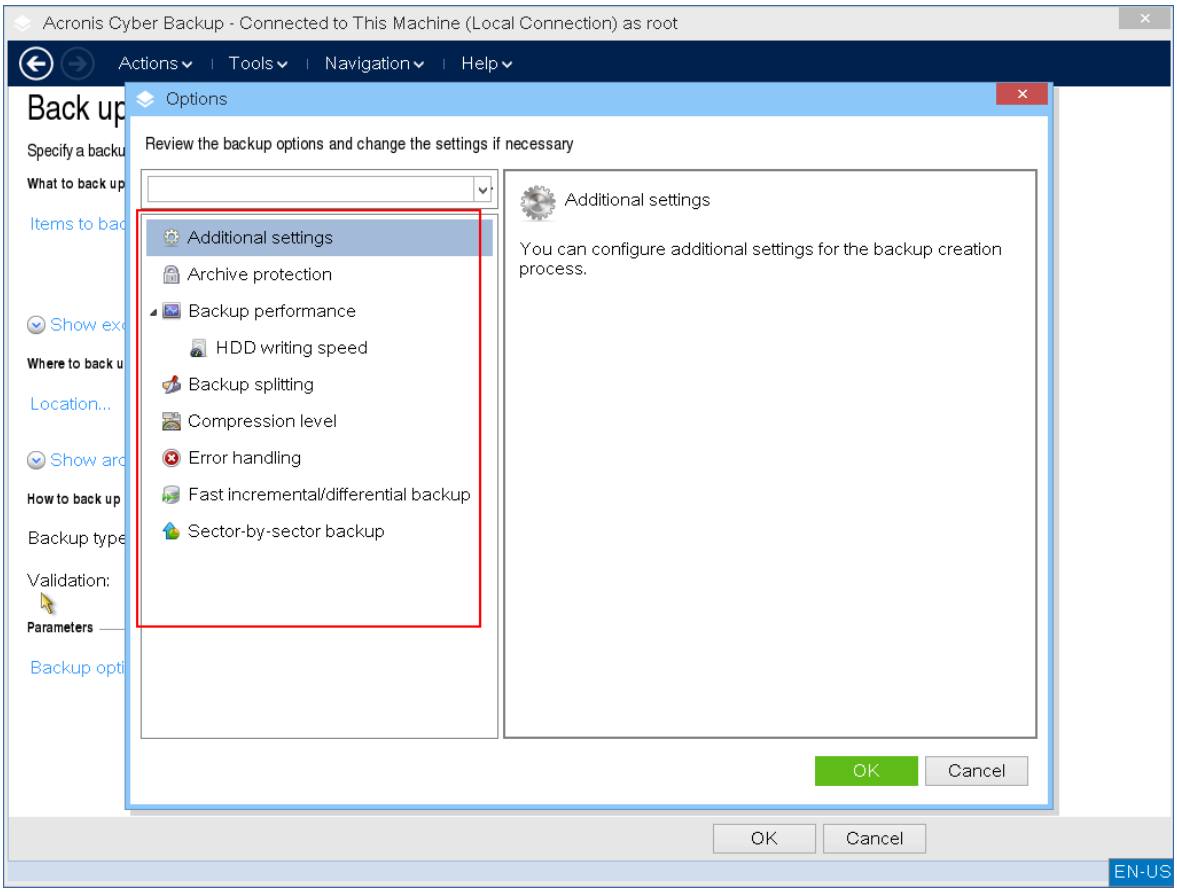
7. バックアップのロケーションと名前を指定します。
8. バックアップの種類を指定します。そのロケーションでの最初のバックアップを行うと、完全バックアップが作成されます。バックアップのチェーンを続行する場合は、**[増分]** または **[差分]** を選択できます。バックアップタイプの詳細については、https://kb.acronis.com/content/1536を参照してください。



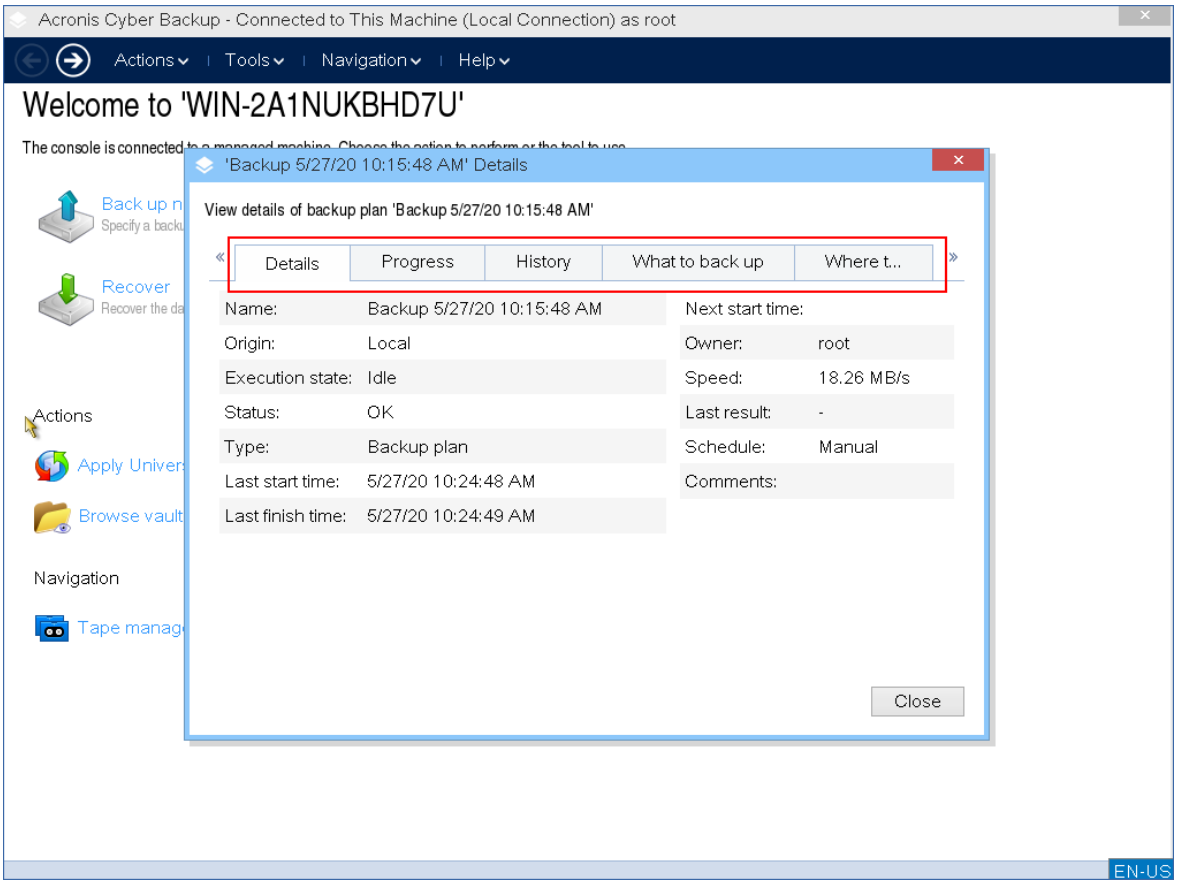
9. （オプション）バックアップファイルをバリデートする場合は、**バックアップを作成後すぐにバリデート**を選択します。



10. （オプション）バックアップファイルのパスワード、バックアップスプリッティング、エラー処理など、必要なバックアップオプションを指定します。



11. **[OK]** をクリックしてバックアップを開始します。
    ブータブルメディアはディスクからデータを読み取り、.tib ファイルに圧縮してから、このファイルを選択したロケーションに書き込みます。実行中のアプリケーションがないため、ディスクスナップショットは作成されません。
12. 表示されるウィンドウでは、バックアップタスクステータスと、バックアップの詳細情報を確認できます。

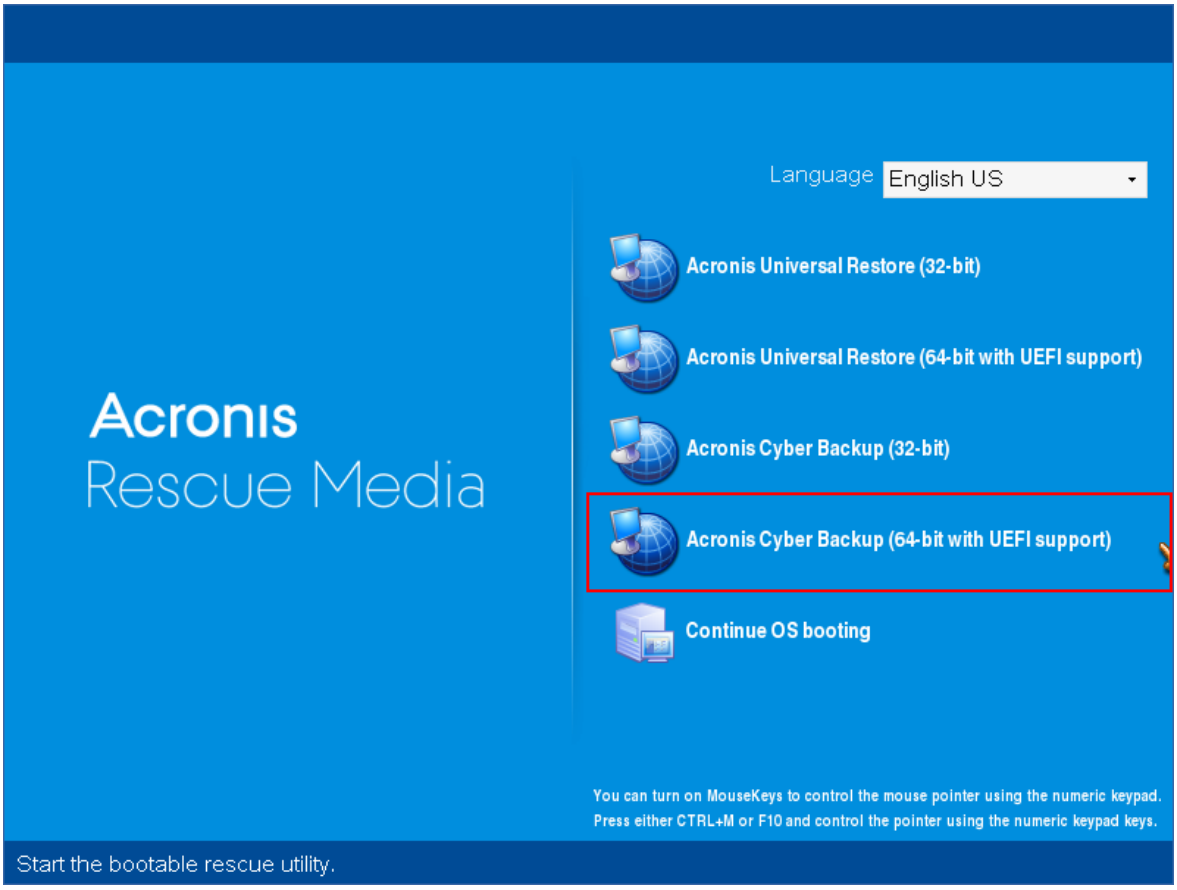


オンプレミスでのブータブルメディアによる復元

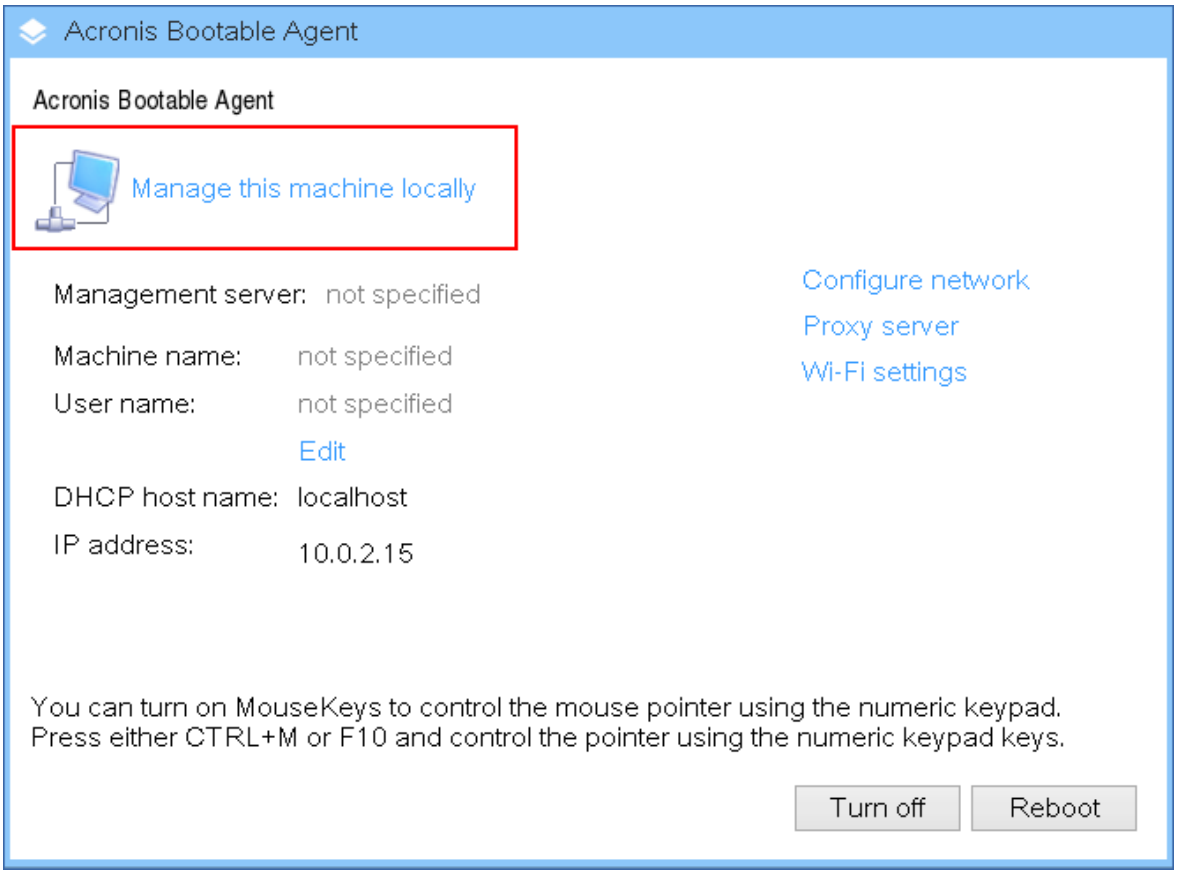
復元操作は、ブータブルメディアビルダーで作成されたブータブルメディアと、ダウンロードされた既成ブータブルメディアの両方で使用できます。

ブータブルメディアでデータをリカバリする

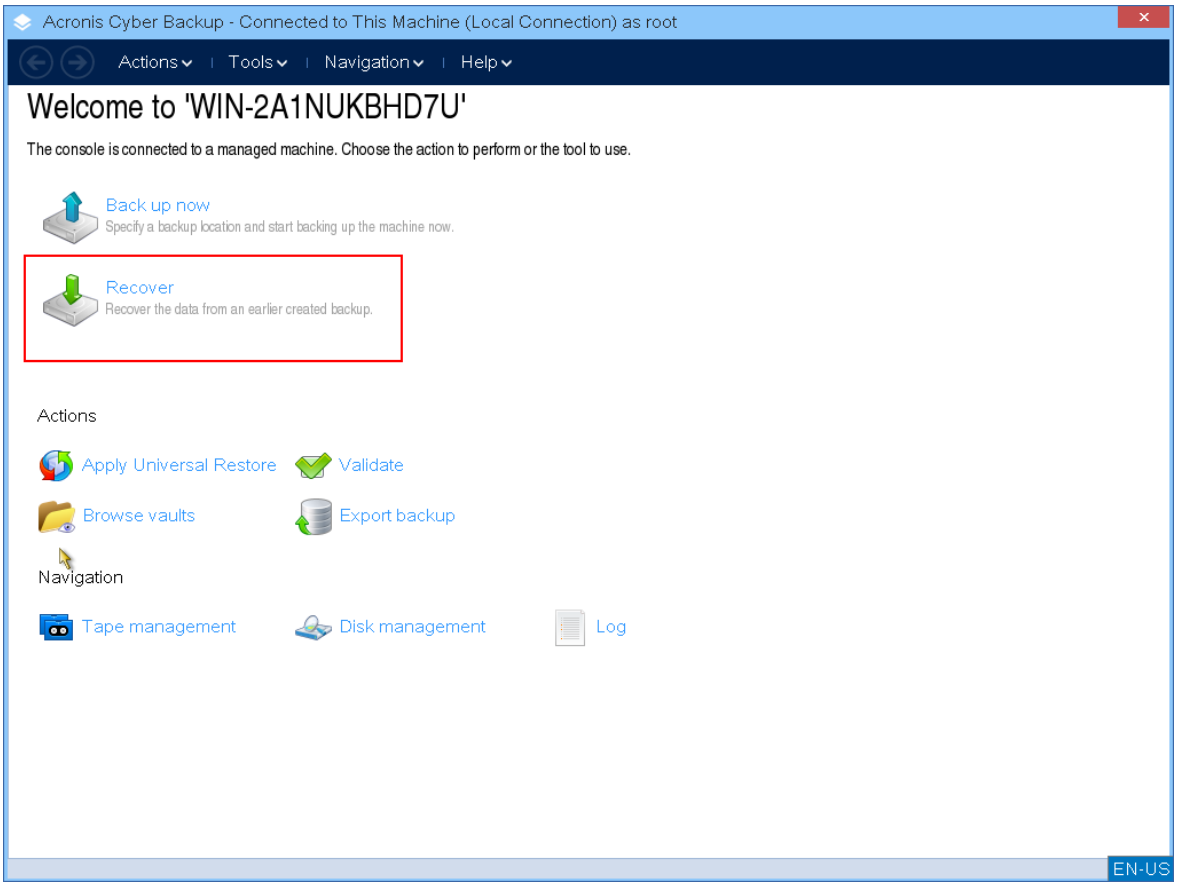
1. Acronisブータブルレスキューメディアから起動します。



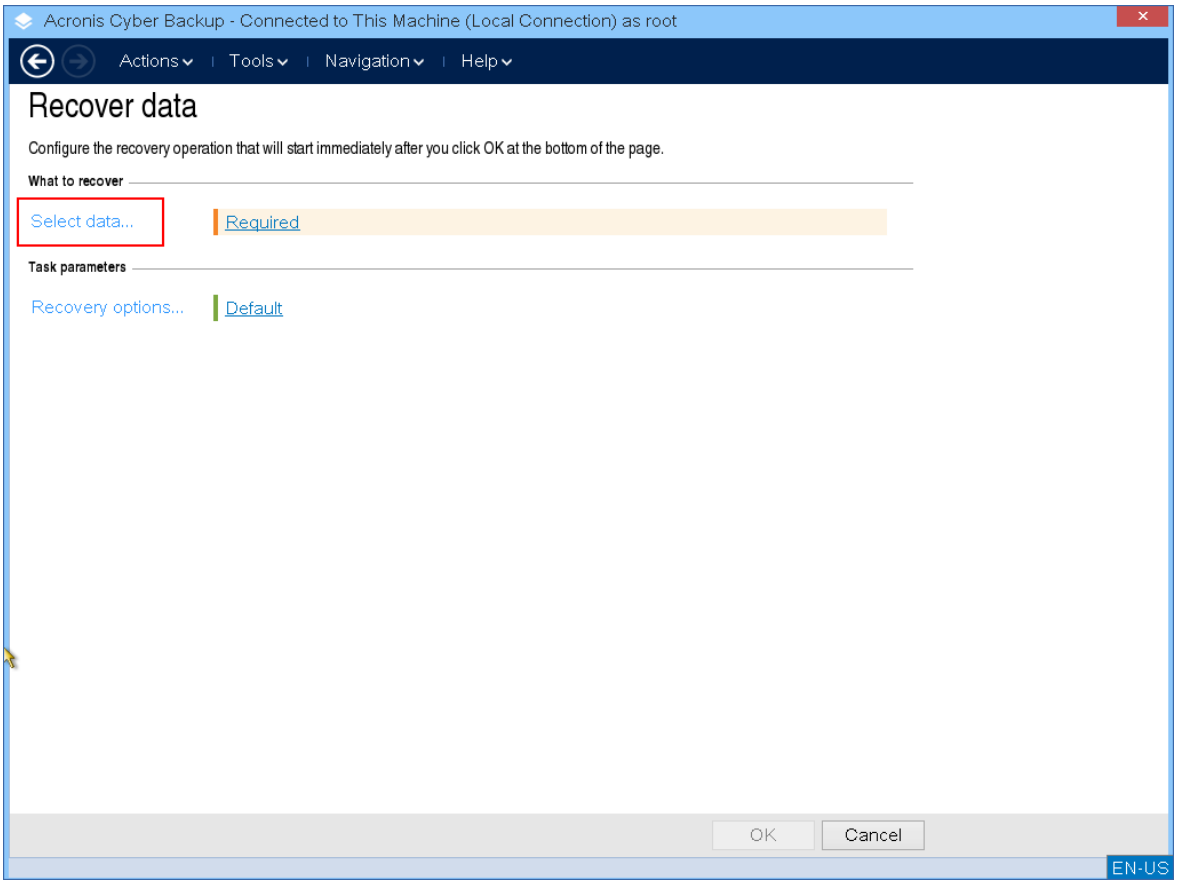
2. ローカルのマシンにデータをリカバリするには、**[このコンピュータをローカルで管理]** をクリックします。リモート接続については、管理サーバーでのメディアの登録を参照してください。



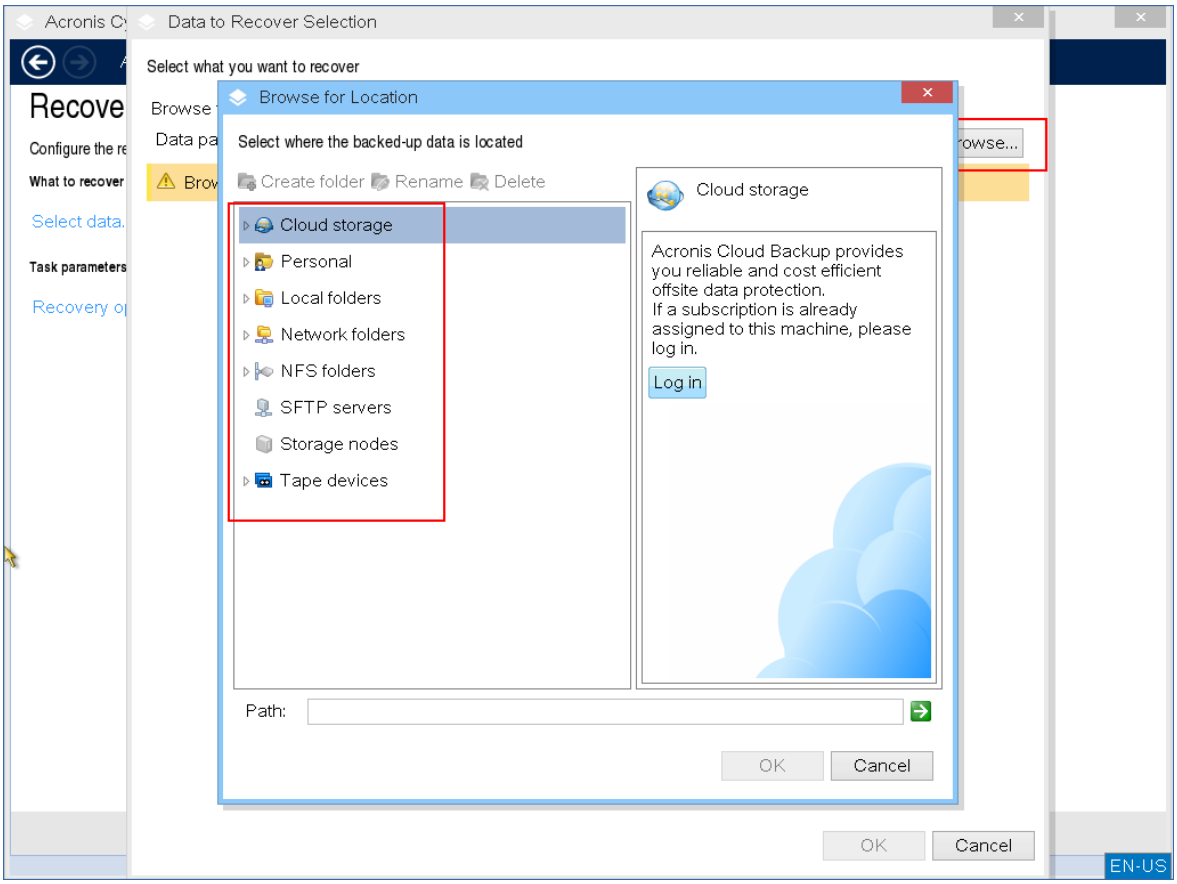
3. **[復元]** をクリックします。



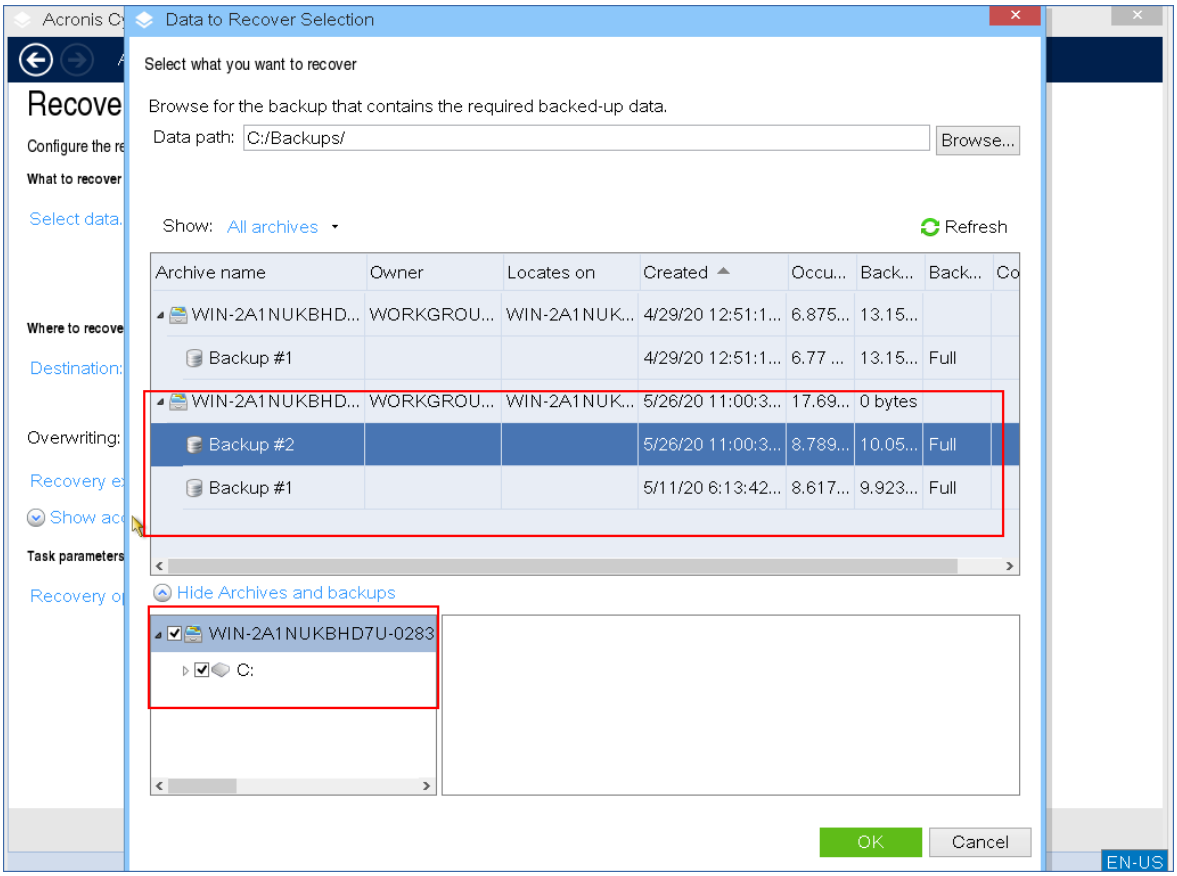
4. [**復元元**] で [**データの選択**] をクリックします。



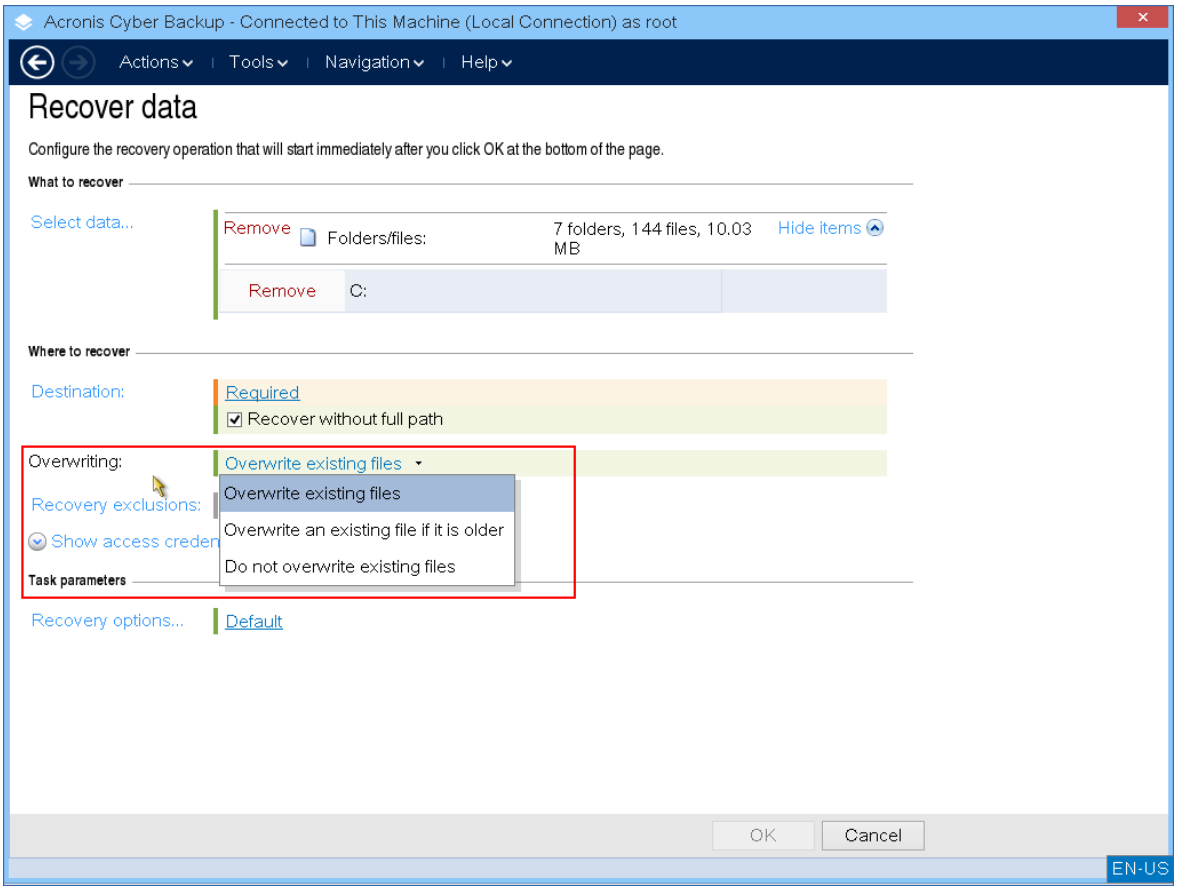
5. **[参照]** をクリックし、バックアップロケーションを選択します。



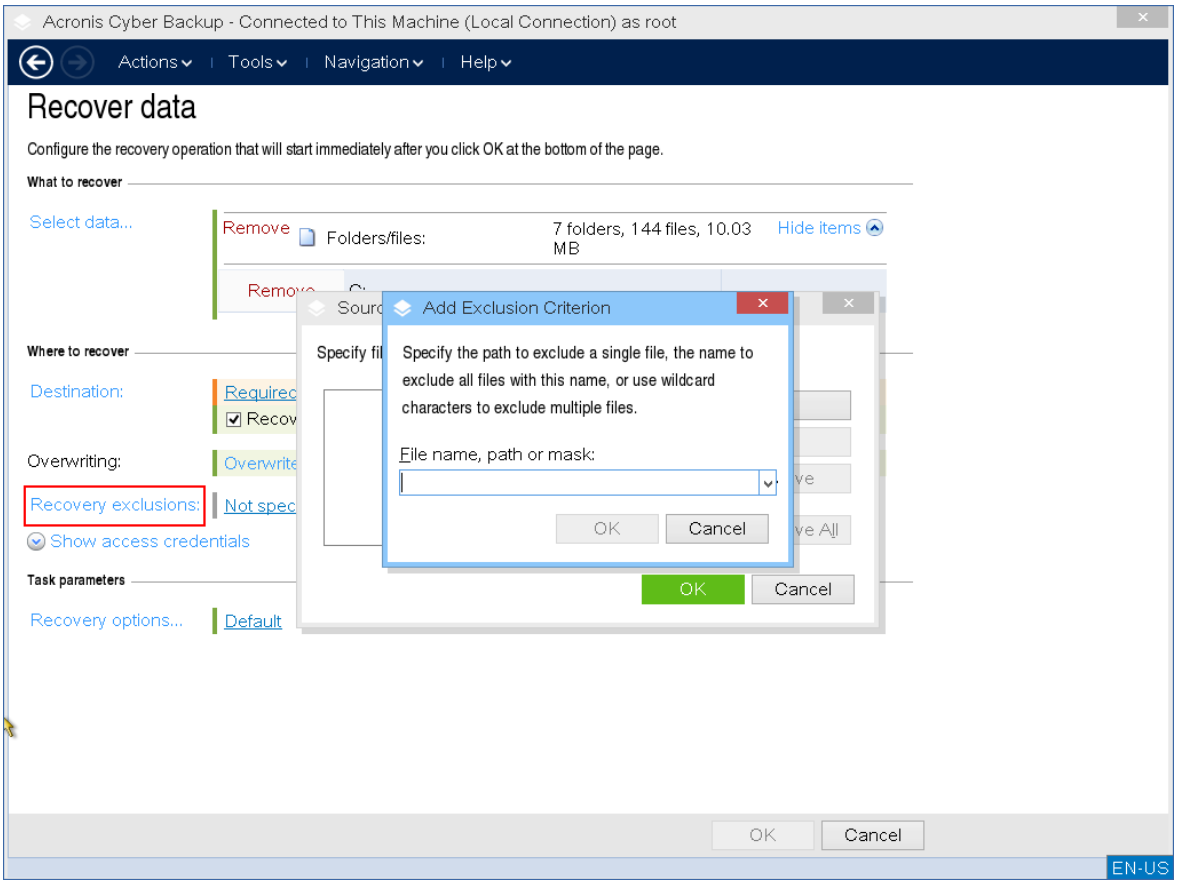
6. リカバリするバックアップファイルを選択します。



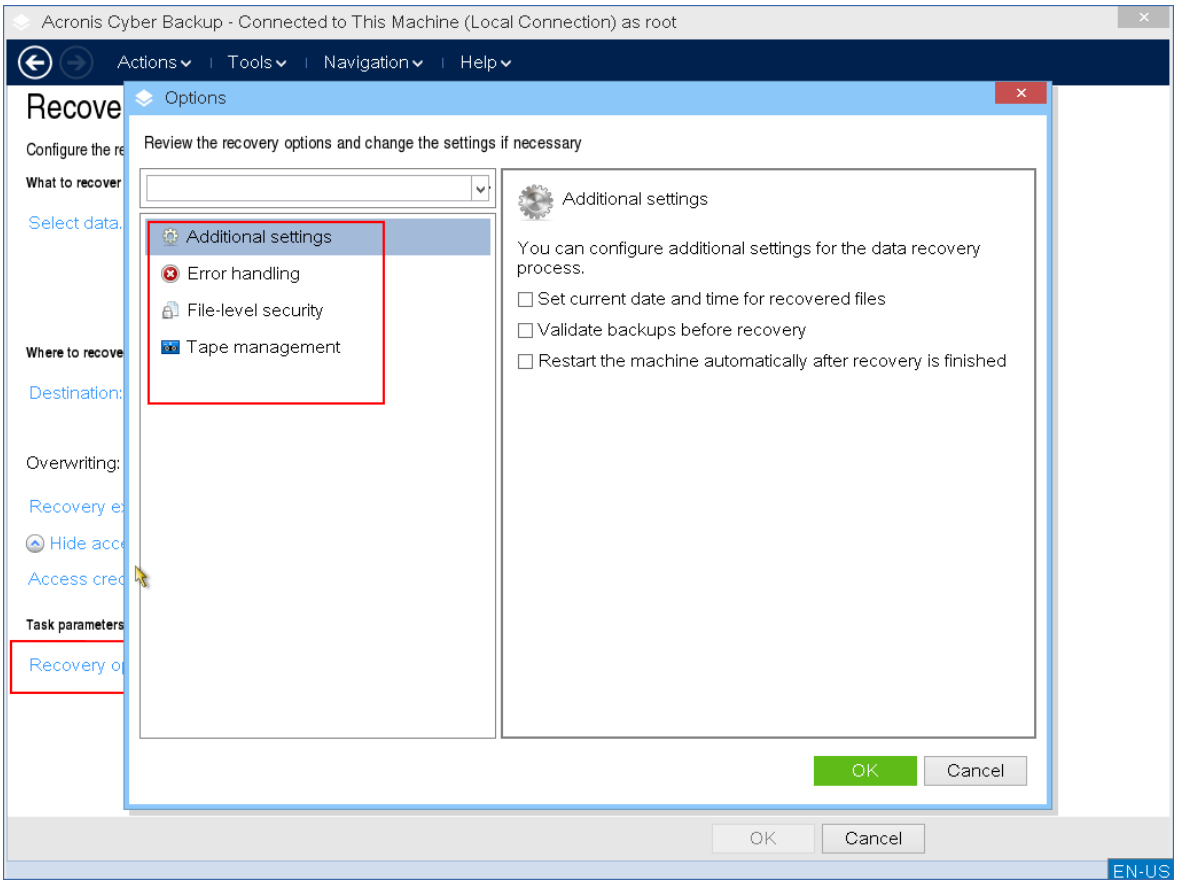
7. 左下のペインで、リカバリするドライブ/ボリューム（またはファイル/フォルダ）を選択し、**[OK]**をクリックします。
8. （オプション）上書きルールを構成します。



9. （オプション）リカバリ除外を構成します。



10. （オプション）復元オプションを構成します。



11. 設定が正しいことを確認し、**OK**をクリックします。

注意
データを異なるハードウェアにリカバリするには、Acronis Universal Restoreを使用する必要があります。バックアップがAcronis Secure Zoneに保存されている場合、
Acronis Universal Restoreは使用できません。

ブータブルメディアによるディスク管理

Acronis ブータブルメディアでは、Acronis Cyber Protect でバックアップされたボリュームイメージをリカバリするために、ディスク/ボリューム構成を準備できます。

ボリュームをバックアップしてイメージを安全なストレージに保管した後で、HDD の交換やハードウェアの損失のため、コンピュータのディスク構成を変更することがあります。このような場合、必要なディスク構成を再作成して、ボリューム イメージを全く以前どおりに、または必要に応じてディスクやボリューム構成を変更して復元できます。

考えられるデータ損失を回避するため、必要な予防措置をすべて行ってください。

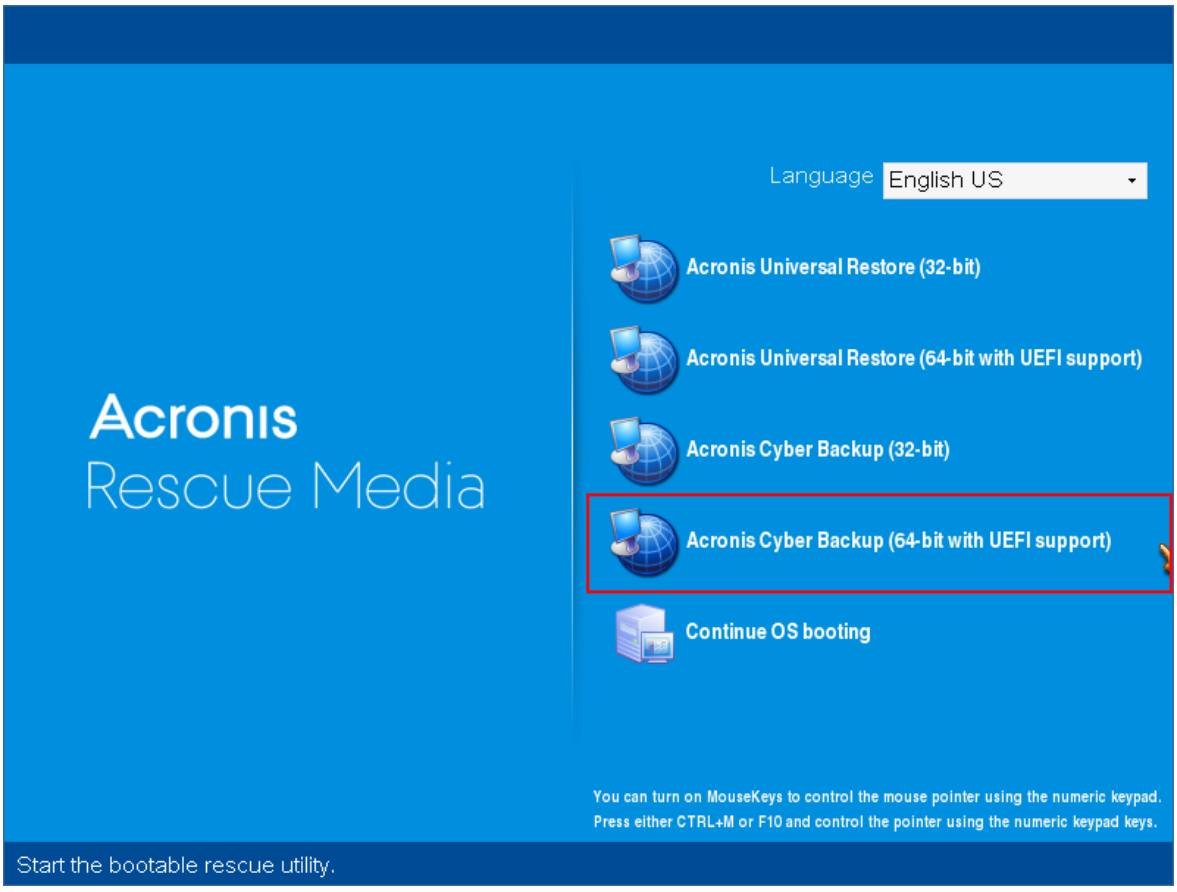
重要
ディスクやボリュームに対するすべての操作には、データ損傷に関する一定のリスクがあります。システム、ブータブルボリューム、またはデータボリュームに対する操作は十分に注意して実行し、起動処理やハードディスクデータストレージで問題が生じる可能性を回避する必要があります。
ハードディスクやボリュームの操作には一定の時間がかかります。処理中の停電、不注意によるマシンのオフ、またはリセット ボタンの誤操作は、ボリュームの損傷やデータ損失につながる可能性があります。

ベアメタル状態のディスク、起動できないコンピュータ、Windows 以外のマシンでも、ディスク管理操作を実行できます。ブータブルメディアビルダーと、Acronis Cyber Protect ライセンスキーで作成したブータブルメディアが必要になります。ブータブル メディアの作成方法については、「Linux ベースのブータブルメディア」または「Windows PE ベースのブータブルメディア」を参照してください。

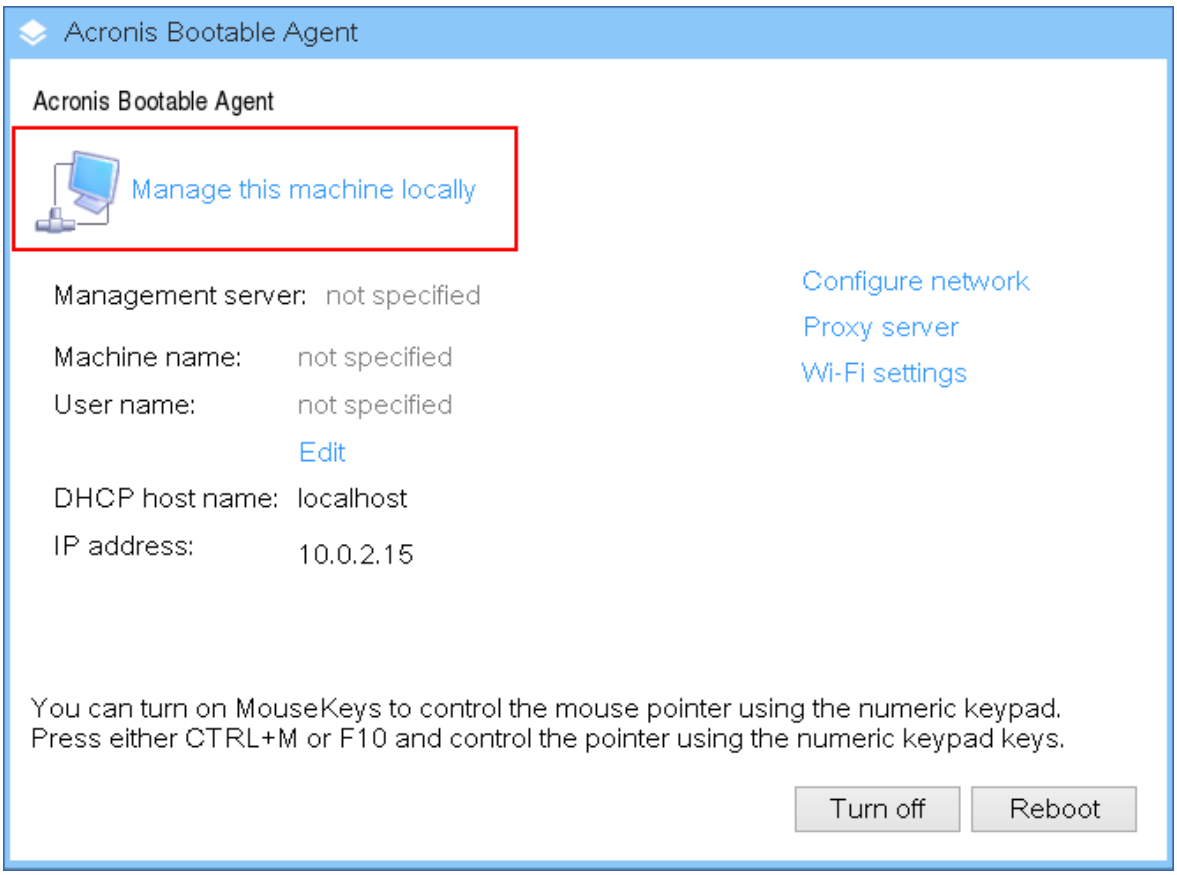
注意
Windows PE 4.0以降に基づくブータブルメディアではディスク管理機能は使用できません。つまり、ディスク管理はWindows 7以前のオペレーティングシステムについてサポートされています。Windows 8以降でディスク管理操作を実行するには、Acronis Disk Directorをインストールする必要があります。詳細については、KB記事: https://kb.acronis.com/content/47031を参照してください。

ディスク管理操作を実行する

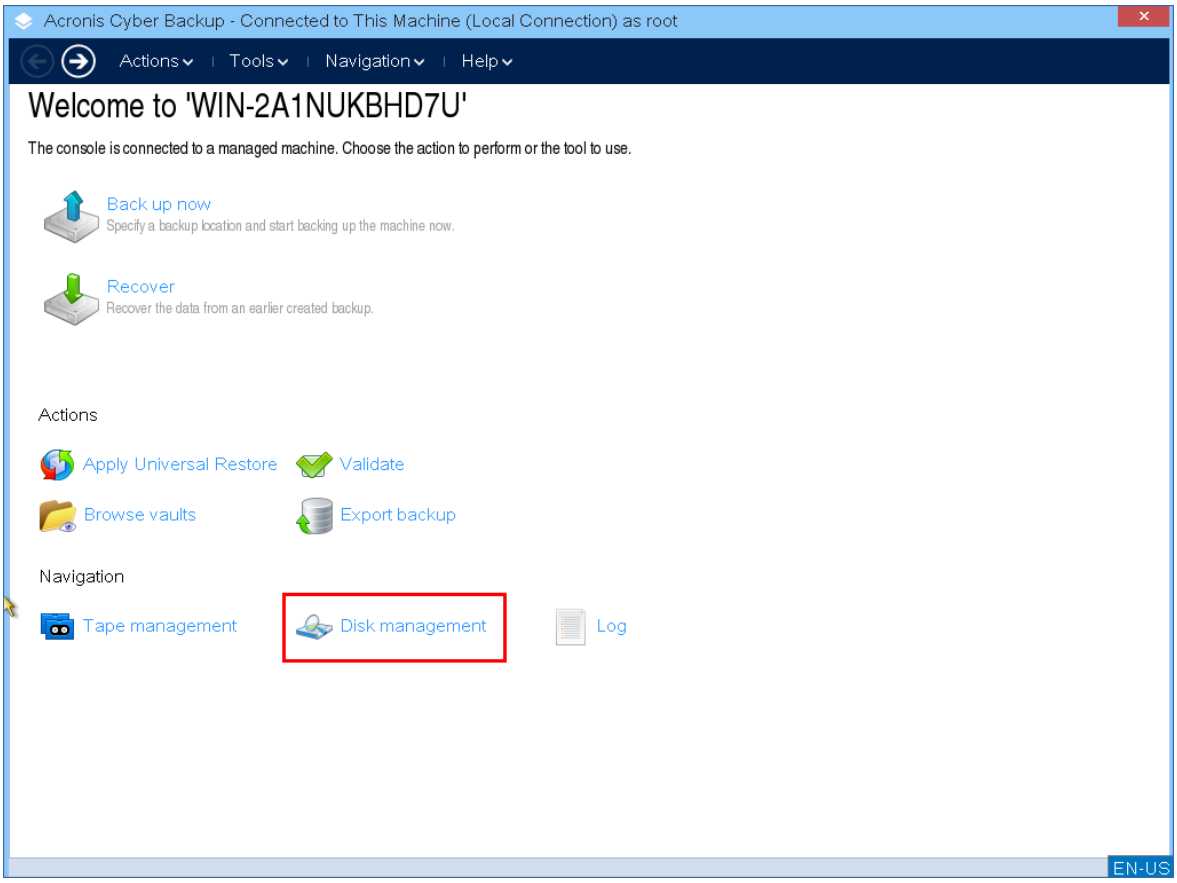
1. Acronis ブータブルレスキューメディアから起動します。



2. ローカルのマシンで作業するには、**[このコンピュータをローカルで管理]** をクリックします。リモート接続については、管理サーバーでのメディアの登録を参照してください。



3. **[ディスク管理]** をクリックします。



注意

コンピュータに記憶域スペースが構成されている場合は、ブータブル メディアでのディスク管理操作が正しく機能しないことがあります。

サポートされるファイル システム

ブータブルメディアでは、次のファイルシステムによるディスク管理をサポートします。

- FAT 16/32
- NTFS

別のファイルシステムのボリュームで操作を実行する必要がある場合は、Acronis Disk Directorを使用してください。完全版では、次のファイル システムのディスクとボリュームを管理するツールやユーティリティが利用できます。

- FAT 16/32
- NTFS
- Ext2
- Ext3
- HFS+
- HFSX
- ReiserFS

- JFS
- Linux SWAP

基本的な予防措置

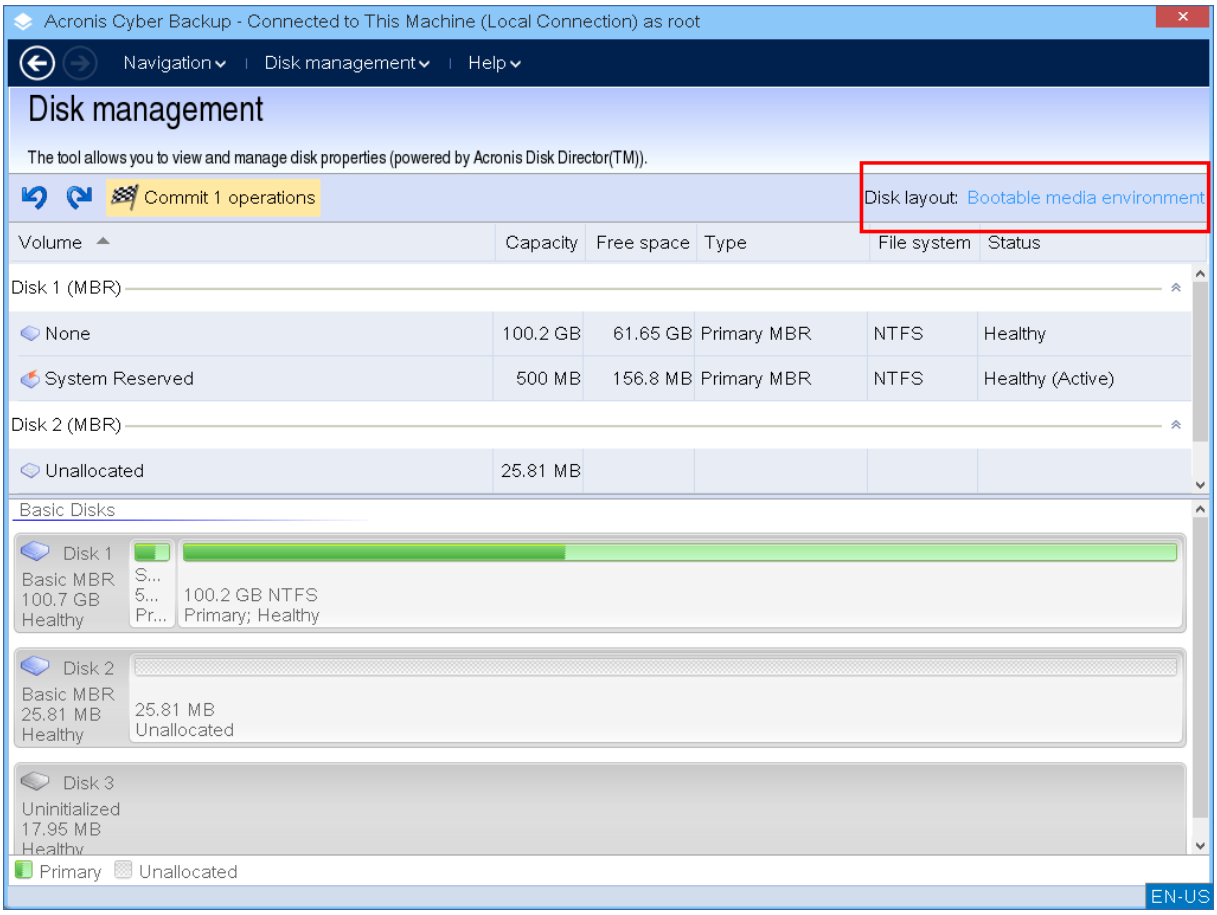
考えられるディスクまたはボリューム構成の損傷やデータ損失を回避するため、必要な予防措置をすべて行い、次のガイドラインに従ってください。

1. ボリュームを作成または管理するディスクをバックアップします。最も重要なデータを別のハードディスク、ネットワーク共有、またはリムーバブルメディアにバックアップしておくと、データの安全性が確保されている状態でディスク ボリュームを操作できます。
2. ディスクをテストして、完全に機能すること、および不良セクタやファイル システム エラーがないことを確認します。
3. 低レベルでディスクにアクセスする他のソフトウェアを実行しているときは、ディスクやボリュームの処理を実行しないでください。

ディスク管理用のオペレーティング システムの選択

複数のオペレーティング システムを持つコンピュータでは、ディスクとボリュームの表示方法は現在実行中のオペレーティング システムによって異なります。同じボリュームでも、オペレーティングシステムが異なると、文字が異なる場合があります。

ディスク管理操作を実行する場合は、オペレーティングシステムが表示されるディスクレイアウトを指定する必要があります。このためには、**ディスクレイアウト**ラベルの横のオペレーティングシステム名をクリックし、開くウィンドウで任意のオペレーティングシステムを選択します。



ディスク処理

ブータブルメディアでは、次のディスク管理操作を実行できます。

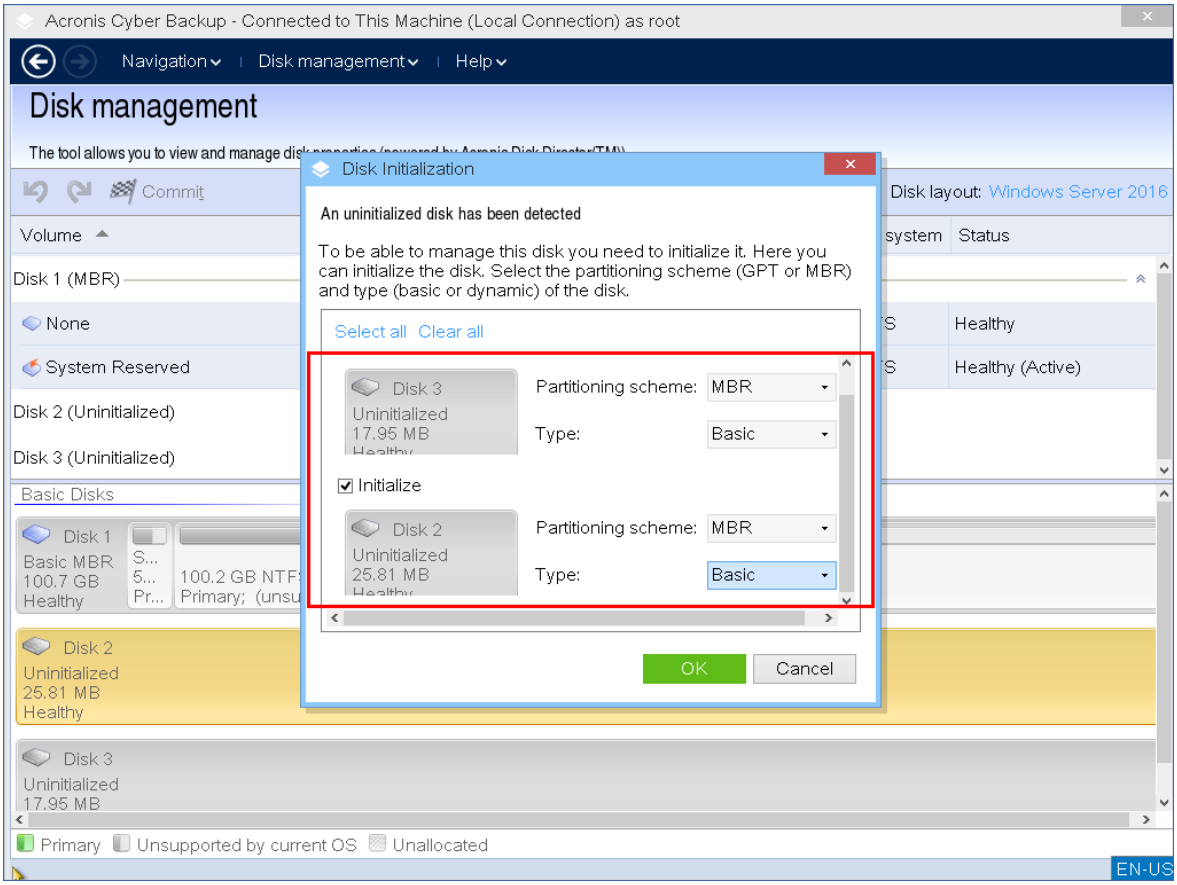
- ディスクの初期化 - システムに新しく追加されたハードウェアを初期化します。
- ベーシックディスククローニング - ソースのベーシック MBR ディスクからターゲットディスクに全データを転送します。
- ディスク変換:MBR から GPT へ - MBR パーティション テーブルを GPT に変換します。
- ディスク変換:GPT から MBR へ - GPT パーティション テーブルを MBR に変換します。
- ディスク変換:ベーシックからダイナミックへ - ベーシックディスクをダイナミックディスクに変換します。
- ディスク変換:ダイナミックからベーシックへ - ダイナミックディスクをベーシックディスクに変換します。

ディスクの初期化

ブータブルメディアでは、初期化されていないディスクが淡色表示のアイコンを持つ灰色のブロックで表示され、ディスクがシステムで使用できないことを示します。

ディスクを初期化する

1. 任意のディスクを右クリックし、**[初期化]**をクリックします。
2. **ディスクの初期化**ウィンドウで、ディスクのパーティション化スキーム（MBR または GPT）、およびディスクの種類（ベーシックまたはダイナミック）を設定します。
3. **[OK]** をクリックすると、保留中のディスク初期化処理が追加されます。
4. 追加された処理を完了するには、コミットします。操作をコミットせずにプログラムを終了すると、操作を事実上キャンセルすることになります。
5. 初期化後、ディスク領域は割り当てられていません。使用するには、ボリュームを作成する必要があります。



ベーシック ディスクのクローン作成

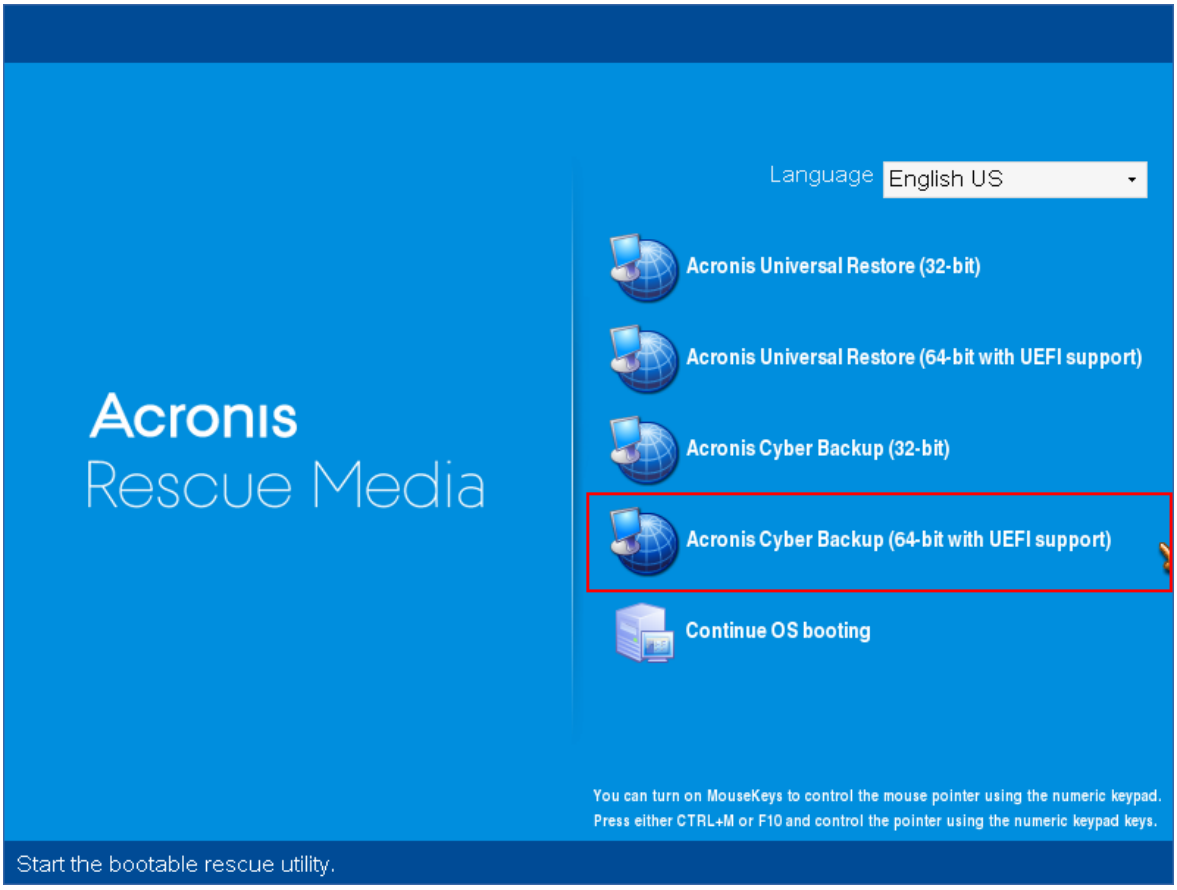
全機能を備えた Linux ベースのブータブルメディアを使用して、ベーシック MBR ディスクのクローンを作成できます。ディスククローニングは、ダウンロードできる既成のブータブルメディアや、ライセンスキーなしで作成されるブータブルメディアでは使用できません。

注意

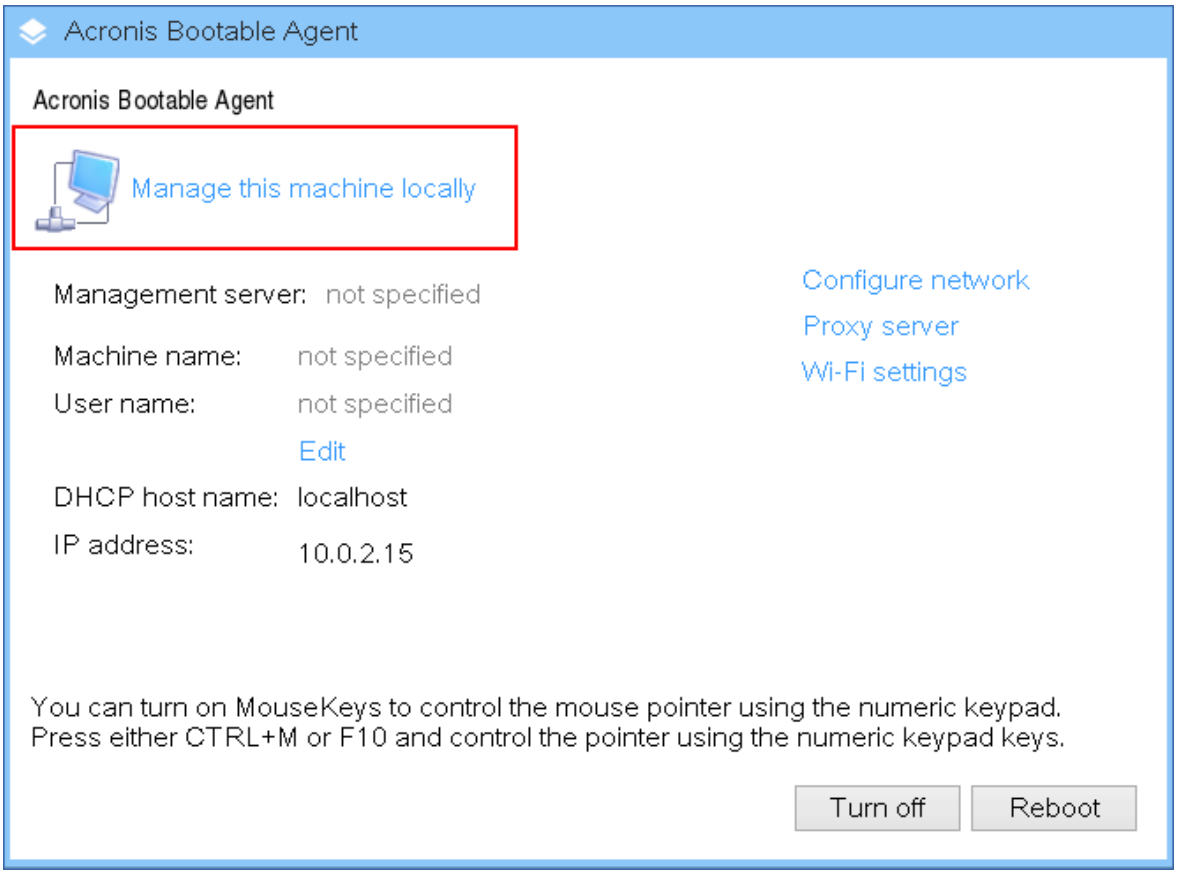
Acronis Cyber Protect コマンドラインユーティリティを使用して、ディスクをクローンすることもできます。

ブータブルメディアでベーシックディスクのクローンを作成する

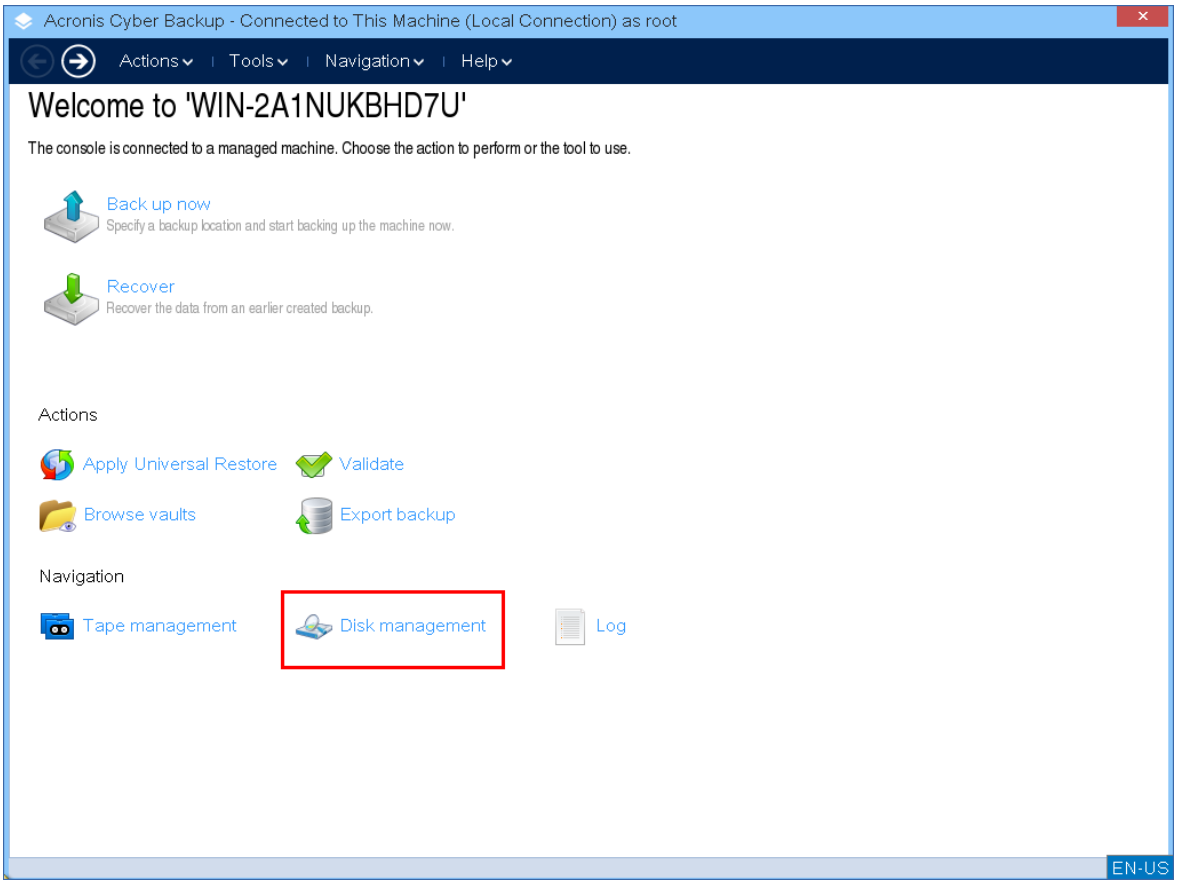
1. Acronis ブータブルレスキューメディアから起動します。



2. ローカルのマシンのディスクをクローンするには、[**このコンピュータをローカルで管理**] をクリックします。リモート接続については、管理サーバーでのメディアの登録を参照してください。

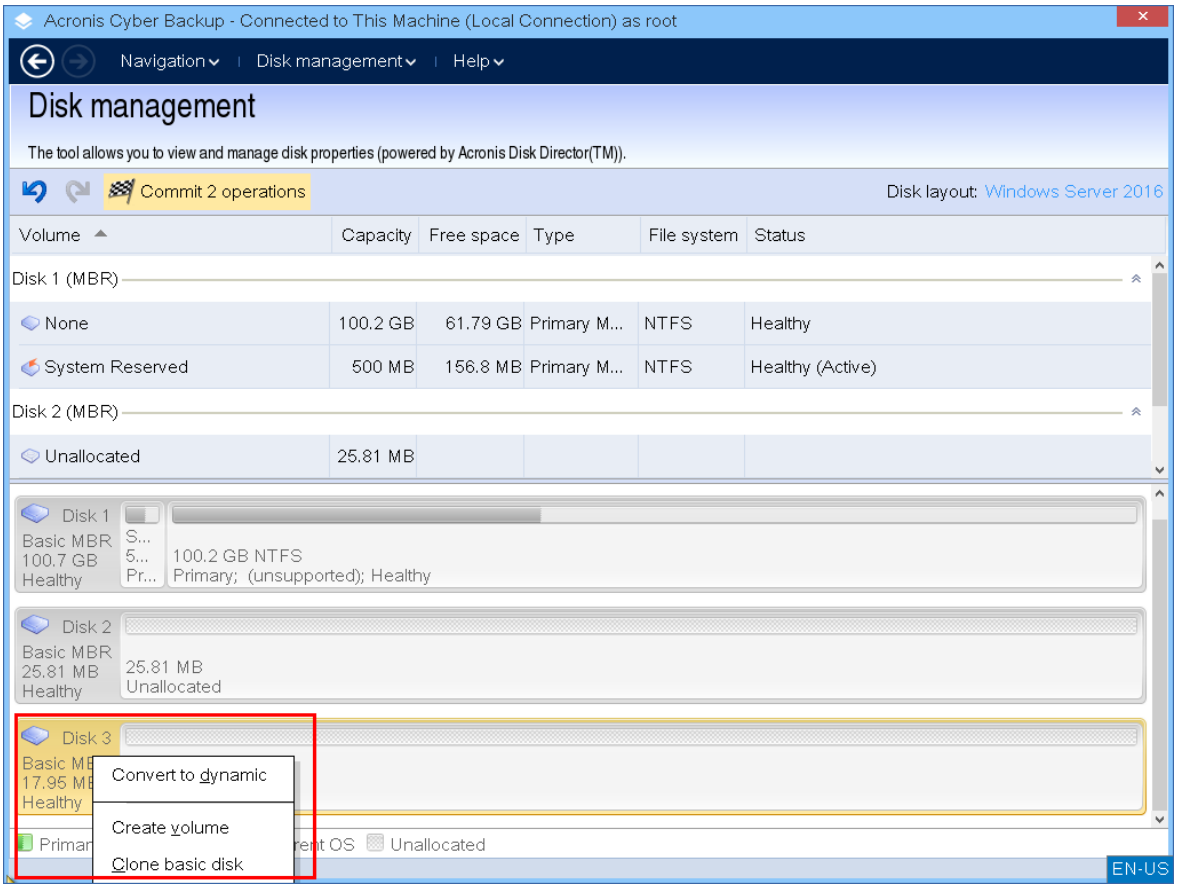


3. **[ディスク管理]** をクリックします。

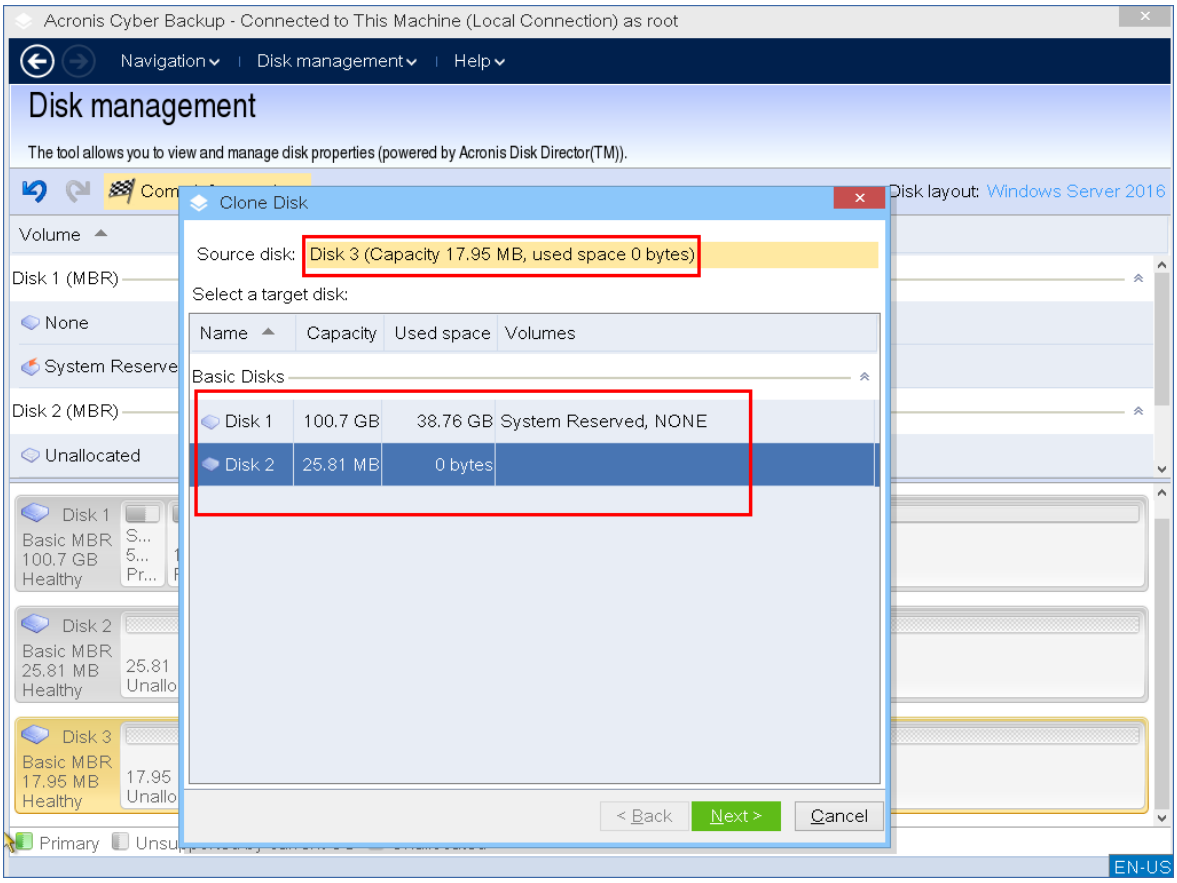


4. 使用可能なディスクが表示されます。クローンするディスクを右クリックし、[**ベーシックディスクのクローン**]をクリックします。

注意
クローンできるのはディスク全体のみです。パーティションクローン作成を使用できません。



5. 可能性があるターゲットディスクの一覧が表示されます。損失なくソースディスクのすべてのデータを保持する十分な容量がある場合には、ターゲットディスクを選択できます。ターゲットディスクを選択して、**[次へ]** をクリックします。

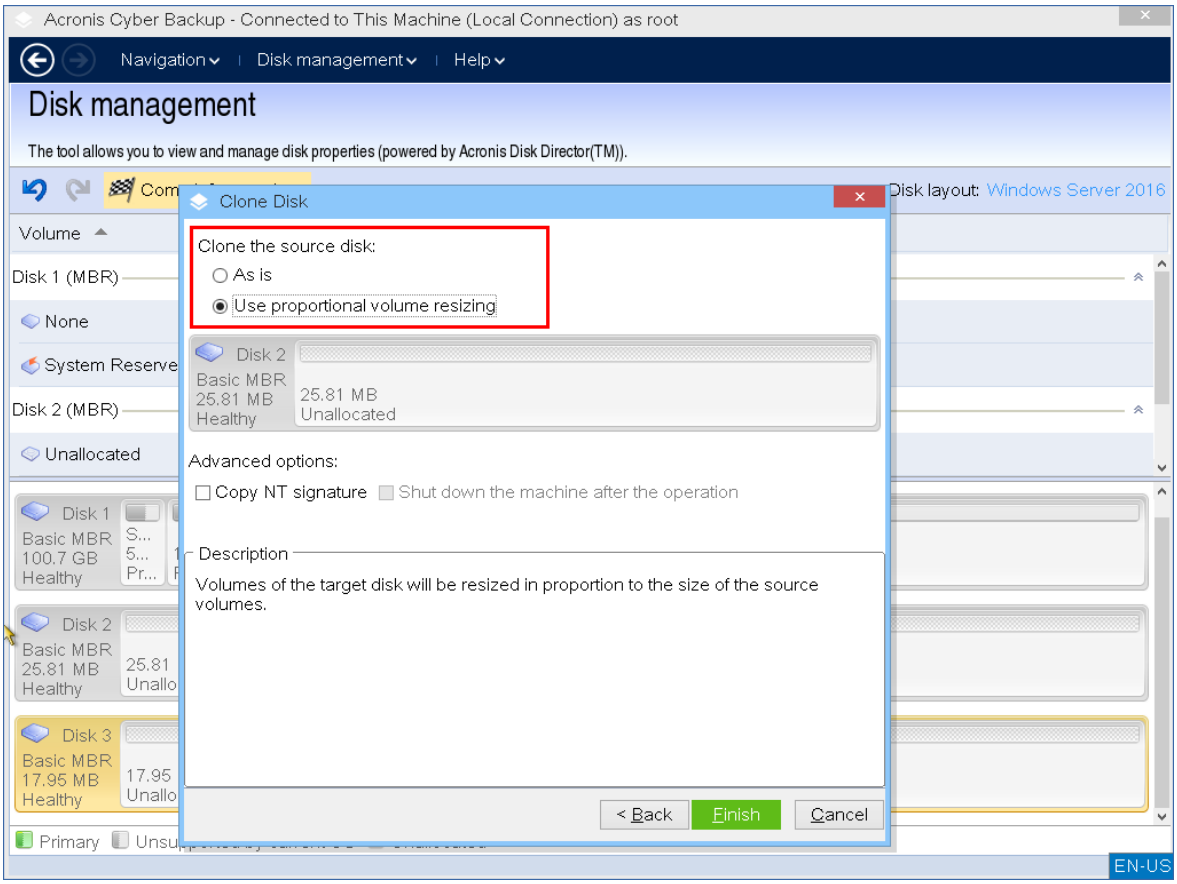


ターゲットディスクのほうが大きい場合、ディスクをそのままクローンするか、」」の未割り当ての領域を残さないようにソースディスクボリュームを比例的にサイズ調整（デフォルトオプション）することができます。

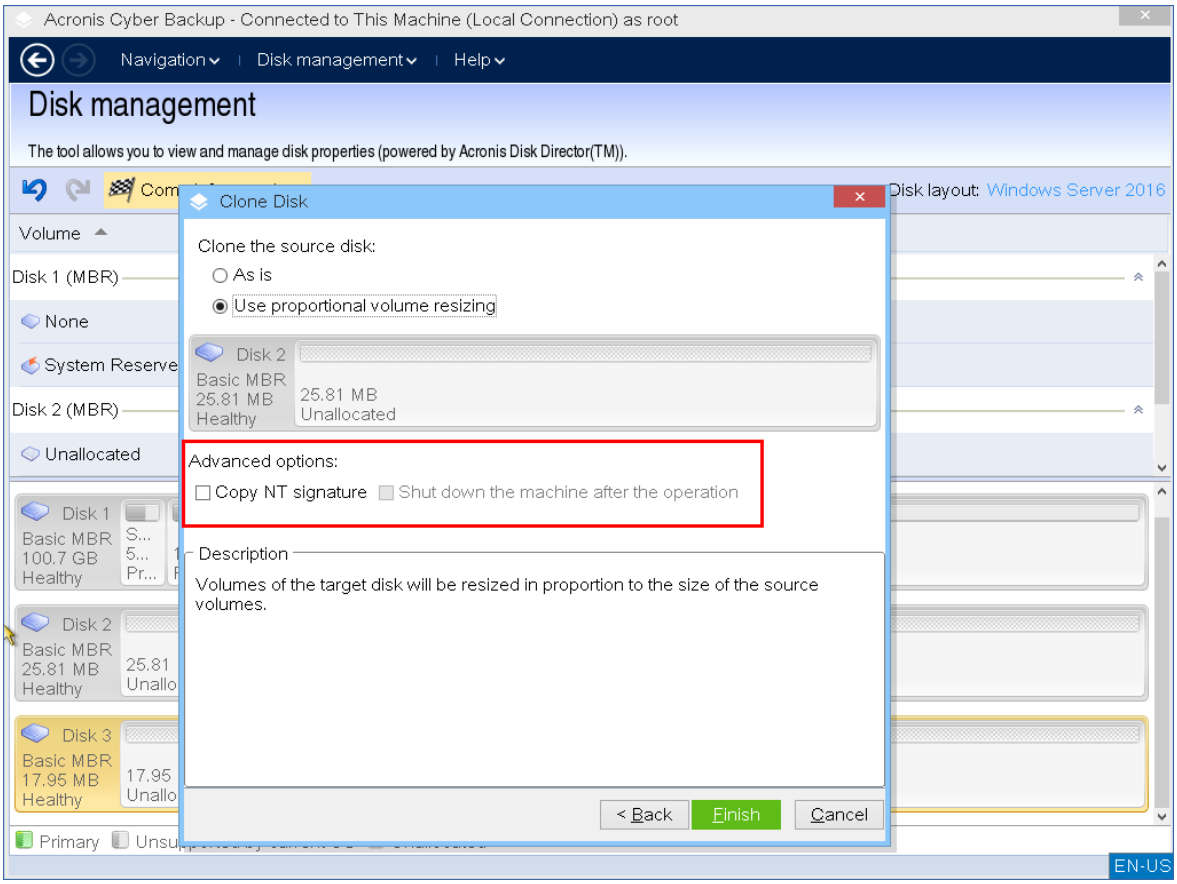
ターゲットディスクの方が小さい場合は、比例サイズ調整のみを使用できます。比例サイズ調整で安全なクローン作成ができない場合は、操作を続行できません。

重要

ターゲットディスクにデータがある場合、警告が表示されます。「選択したターゲットディスクは空ではありません。そのボリュームのデータは上書きされます。」続行する場合、現在ターゲットディスクにあるすべてのデータが失われ、元に戻せません。



6. NT シグニチャをコピーするかどうかを選択します。



システムボリュームを構成しているディスクのクローンを作成する場合、ターゲット ディスクボリュームでもオペレーティングシステムのブータビリティを保つ必要があります。つまり、オペレーティングシステムが、MBR ディスク レコードに保持されたディスク NT シグニチャと一致するシステムボリューム情報（ボリュームのドライブ文字など）を持つ必要があります。ただし、オペレーティングシステムのもとでは、2 つのディスクが同じ NT シグニチャを持つと正しく機能できません。

マシンにシステムボリュームを構成しているディスクが 2 つあり、同じ NT シグネチャを持っている場合、起動時に最初のディスクからオペレーティングシステムが実行され、2 番目のディスクで同じシグネチャが検出されます。その際に、自動的に新しい一意の NT シグニチャが生成され、2 番目のディスクにはそのシグネチャが割り当てられます。その結果、2 番目のディスク上のすべてのボリュームはそのドライブ文字を失います。ドライブ文字がないため、パスは有効ではなくなり、プログラムからそのディスク上のファイルは見えなくなります。そのディスク上のオペレーティング システムは起動できなくなります。

ターゲットディスク ボリュームでシステムのブータビリティを保つには、次の手順を実行できます。

a. **NT シグニチャをコピーする** – ターゲット ディスクにコピーされたレジストリキーと一致するソース ディスク NT シグニチャをターゲットディスクに設定します。

   このためには、**[NT シグニチャのコピー]** チェックボックスをオンにします。

   次のような警告が表示されます。「ハードディスクにオペレーティングシステムが存在する場合は、コンピュータを再起動する前に、マシンからソースまたはターゲットのハード ディスク ドライブをアンインストールしてください。そうしなければ、OS は 2 台のディスクのうち最初の

ディスクから起動され、2 番目のディスクの OS は起動できなくなります。」

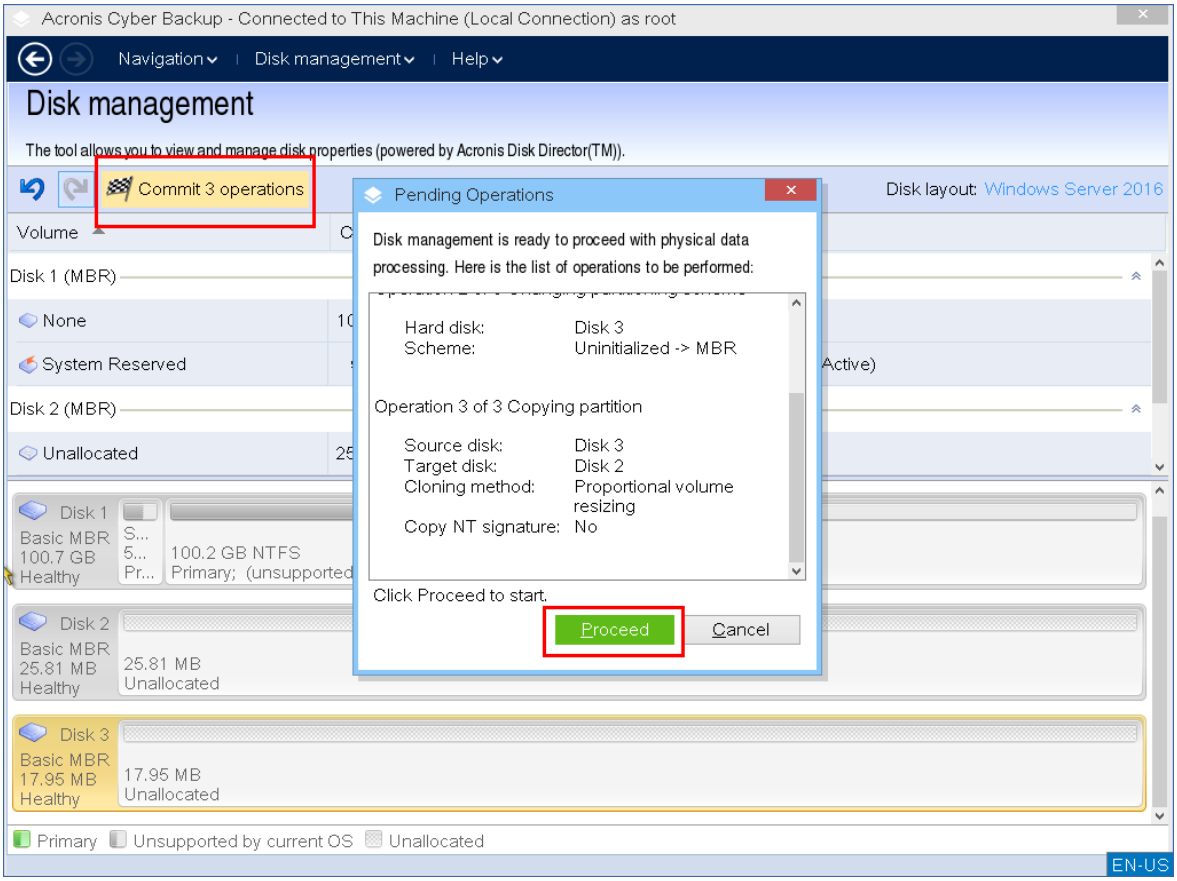
［**クローンの作成処理後にマシンの電源を切る**］チェックボックスが選択され、自動的に無効になります。

b. **NT シグニチャを保持する** – 従来のターゲットディスクの署名は変更せず、そのシグニチャに応じてオペレーティングシステムを更新します。

このためには、必要に応じて **[NT シグニチャのコピー]** チェックボックスをクリックしてオフにします。

［**クローンの作成処理後にマシンの電源を切る**］チェックボックスが自動的にオフになります。

7. **[完了]** をクリックすると、保留中のディスククローニング処理を追加します。
8. **[コミット]** をクリックし、**[保留中の処理]** ウィンドウで **[実行]** をクリックします。操作をコミットせずにプログラムを終了すると、操作を事実上キャンセルすることになります。



9. NT シグニチャをコピーする場合は、操作が完了し、コンピューターがオフになるまで待ってから、ソースまたはターゲットハードディスクドライブのどちらかをマシンから切断します。

ディスク変換:MBR から GPT

次の要件がある場合は、MBR ベーシックディスクを GPT ベーシックディスクに変換することができます。

- 1 つのディスクに 5 つ以上のプライマリボリューム
- データ損失に備えて、ディスクの信頼性を高める。

重要
現在オペレーティングシステムを実行中のブートボリュームを含むベーシック MBR ディスクを GPT に変換することはできません。

ベーシック MBR ディスクをベーシック GPT ディスクに変換する

1. クローンするディスクを右クリックし、**[GPT に変更]**をクリックします。
2. **[OK]** をクリックすると、MBR から GPT へのディスク変換の保留中の処理を追加します。
3. 追加された処理を完了するには、コミットします。操作をコミットせずにプログラムを終了すると、操作を事実上キャンセルすることになります。

注意
GPT パーティション ディスクは、パーティション領域の最後に、バックアップ領域に必要な領域を予約します。この領域には、GPT ヘッダーとパーティション テーブルのコピーが保存れます。ディスクがいっぱいで、ボリューム サイズを自動的に小さくすることができない場合、MBR ディスクから GPT への変換操作は失敗します。
処理は元に戻せません。MBR ディスクに属するプライマリボリュームがあり、ディスクを最初に GPT に変換してから MBR に戻す場合、このボリュームは論理ボリュームになり、システムボリュームとしては使用できなくなります。

ダイナミック ディスク変換:MBR から GPT

ブータブルメディアは、ダイナミックディスクについては MBR から GPT への直接の変換をサポートしていません。ただし、次の変換を実行することにより、この目的を実現できます。

1. MBR ディスク変換: ダイナミックからベーシックへ は **[ベーシックへの変換]** 操作を使用します。
2. ベーシックディスク変換：**[GPT への変換]** 操作を使用して MBR から GPT に変換します。
3. GPT ディスク変換: ベーシックからダイナミックへ は **[ダイナミックへの変換]** 操作を使用します。

ディスク変換:GPT から MBR

GPT ディスクをサポートしない OS をインストールする予定がある場合、GPT ディスクから MBR への変換も、

重要
現在オペレーティングシステムを実行中のブートボリュームを含むベーシック GPT ディスクを MBR に変換することはできません。

GPT ディスクを MBR に変換する

1. クローンするディスクを右クリックし、**[MBR に変更]**をクリックします。
2. **[OK]** をクリックすると、保留中の GPT から MBR へのディスク変換処理が追加されます。
3. 追加された処理を完了するには、コミットします。操作をコミットせずにプログラムを終了すると、操作を事実上キャンセルすることになります。

注意
操作後、このディスクのボリュームは論理になります。この変更を元に戻すことはできません。

ディスク変換: ベーシックからダイナミックへ

次の場合には、ベーシックディスクをダイナミックに変換する場合があります。

- ダイナミックディスクグループの一部としてディスクを使用する計画
- データ ストレージ用にディスクの信頼性を高める場合

ベーシックディスクをダイナミックディスクに変換する

1. 変換するディスクを右クリックし、**[動的に変更]**をクリックします。
2. **[OK]** をクリックします。

すぐに変換が実行され、必要に応じてマシンが再起動されます。

注意
ダイナミック ディスクは、物理ディスクの最後の 1 メガバイトを使用して、各ダイナミック ボリュームの 4 レベルの記述(ボリューム - コンポーネント - パーティション - ディスク)を含むデータベースを保存します。ダイナミックへの変換中にベーシックディスクが満杯で、ボリュームのサイズを自動的に減らせないことが判明した場合は、処理が失敗します。
システムボリュームを構成するディスクを変換するには一定の時間がかかります。電源の停止、予期しないマシンの停止、動作中の過失によるリセットボタンの押下の場合はブータビリティが失われる可能性があります。

Windows のディスクの管理とは異なり、このプログラムでは、操作後にディスク上の**オフライン オペレーティングシステム**のブータビリティが保証されます。

ディスク変換: ダイナミックからベーシックへ

たとえば、ダイナミックディスクをサポートしないオペレーティングシステムを使用する場合など、ダイナミックディスクをベーシックディスクに戻したい場合があります。

ダイナミックディスクをベーシックディスクに変換する

1. 変換するディスクを右クリックし、**[ベーシックに変更]**をクリックします。
2. **[OK]** をクリックします。

すぐに変換が実行され、必要に応じてマシンが再起動されます。

注意
この操作は、スパン、ストライプ、または RAID-5 ボリュームを含むダイナミックディスクには使用できません。

変換後、ディスク領域の最後の 8MB は、将来、ベーシック ディスクからダイナミック ディスクに変換するために予約されます。場合によっては、使用可能な未割り当て領域と、提示された最大ボリュームサイズが異なることがあります（たとえば、一方のミラーのサイズにより他方のミラーのサイズが決ま

る場合や、ディスク領域の最後の 8MB がベーシック ディスクからダイナミック ディスクへの将来の変換用に予約されている場合など）。

注意
システムボリュームを構成するディスクを変換するには一定の時間がかかります。電源の停止、予期しないマシンの電源オフ、処理中の過失によるリセットボタンの押下をした場合は、ブータビリティが失われる可能性があります。

Windows のディスクの管理とは異なり、このプログラムでは次のことが保証されます。

- シンプル ボリュームおよびミラーボリュームの**データの保存された**ボリュームを含むダイナミック ディスクをベーシック ディスクに安全に変換
- マルチブートシステムで、処理中に**オフライン**だったシステムのブータビリティ

ボリューム処理

ブータブルメディアでは、ボリュームで次の操作を実行できます。

- ボリュームの作成 - 新しいボリュームを作成します。
- ［ボリュームの削除］ - 選択したボリュームを削除します。
- ［アクティブに設定］ - インストールされている OS でマシンが起動できるように、選択したボリュームをアクティブに設定します。
- ［ドライブ文字の変更］ - 選択したボリュームのドライブ文字を変更します。
- ［ラベルの変更］ - 選択したボリュームラベルを変更します。
- ボリュームのフォーマット - ファイルシステムのボリュームをフォーマットします。

ダイナミック ボリュームの種類

シンプル ボリューム

単一の物理ディスク上の空き領域から作成されたボリューム。ディスク上の 1 つの領域で構成することも、複数の領域から構成することもでき、LDM（Logical Disk Manager）によって仮想的に連結されます。信頼性の向上、速度の改善、サイズの追加におけるメリットはありません。

スパン ボリューム

複数の物理ディスクから LDM が仮想的に連結した空きディスク領域から作成されたボリューム。最大 32 のディスクを 1 つのボリュームに含めて、ハードウェア サイズの制限を解決できます。ただし、1 つのディスクが失敗した場合でも、すべてのデータが失われます。また、ボリューム全体を壊さずにスパンボリュームの一部を取り除くことができません。そのため、スパンボリュームでは、信頼性が向上したり、I/O 速度が改善したりすることはありません。

ストライプ ボリューム

ボリューム（RAID 0 ）は同じサイズのデータのストライプから構成され、ボリュームの各ディスクに書き込まれます。つまり、ストライプボリュームを作成するには、2 つ以上のダイナミックディ

スクが必要です。ストライプボリューム内のディスクは同一である必要はありませんが、ボリュームに含めるそれぞれのディスクに利用可能な未使用領域が存在する必要があります。ボリュームのサイズは最も小さな領域のサイズに従います。I/O が複数のディスクにまたがっているので、ストライプ ボリューム上のデータへのアクセスは、通常、単一の物理ディスク上の同じデータへのアクセスよりも高速になります。

ストライプボリュームの作成はパフォーマンスを改善するためであり、信頼性の向上を目的としていません。ストライプボリュームには、冗長な情報は含まれません。

ミラー ボリューム

データが 2 つの同一の物理ディスク上に複製された、フォールト トレラントなボリュームであり、RAID 1 とも呼ばれます。一方のディスク上のすべてのデータが他方のディスクにコピーされ、データの冗長性をもたらします。システム ボリュームやブート ボリュームを含め、ほとんどすべてのボリュームをミラー化できます。どちらかのディスクに障害が発生しても、もう一方のディスクからデータにアクセスできます。残念ながら、ミラー ボリュームを使用する場合、サイズとパフォーマンスに関するハードウェア制限はより厳しくなります。

ミラー ストライプ ボリューム

ストライプ レイアウトの高速な I/O とミラー タイプの冗長性の利点を組み合わせた、フォールト トレラントなボリュームであり、RAID 1+0 とも呼ばれます。ディスクとボリュームのサイズ比率が低いという、ミラー アーキテクチャの短所をそのまま継承しています。

RAID-5

データが 3 つ以上のディスクのアレイにわたってストライプされる、フォールト トレラントなボリューム。ディスクは同一である必要はありませんが、ボリューム内の各ディスクで利用できる未割り当て領域のブロックは同じサイズにする必要があります。パリティ（障害が発生した場合にデータの再編成に使用できる計算値）もまた、ディスクアレイにわたってストライプされます。常にデータとは別のディスクに保存されます。物理ディスクに障害が発生した場合、障害のあるディスク上にあった RAID-5 ボリュームの部分は、残りのデータとパリティから再度作成できます。RAID-5 ボリュームは、信頼性におけるメリットがあり、ミラーよりもディスクとボリュームのサイズ比率が高いため、物理ディスクのサイズ制限を克服できます。

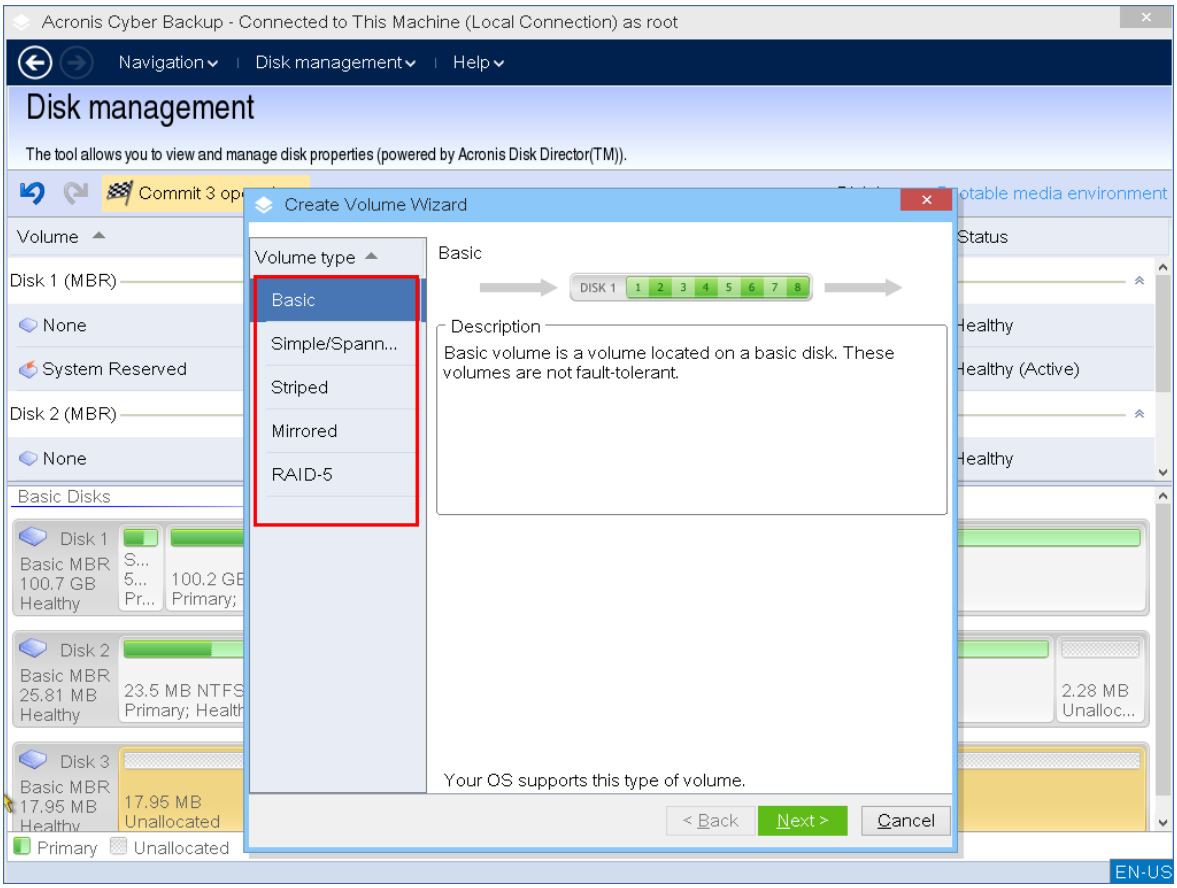
ボリュームの作成

新しいボリュームには次のような操作が必要な場合があります。

- 以前に保存したバックアップ コピーを「以前の状態のまま」の設定で復元する
- 同じ種類のファイルをまとめて別々に保存する（たとえば、MP3 コレクションやビデオ ファイルを別のボリュームに保存する）
- 特別なボリューム上に他のボリュームまたはディスクのバックアップ（イメージ）を保存する
- 新しいオペレーティングシステム（またはスワップファイル）を新しいボリュームにインストールする
- 新しいハードウェアをマシンに追加する。

ボリュームを作成する

1. ディスクの未割り当ての領域を右クリックし、**[ボリュームの作成]** をクリックします。**ボリューム作成ウィザード**が開きます。



2. ボリュームの種類を選択します。次から選択できます。
   - ベーシック
   - シンプル/スパン
   - ストライプ
   - ミラー
   - RAID-5

   現在のオペレーティングシステムが選択した種類のボリュームをサポートしていない場合は、警告が表示され、**[次へ]** ボタンが無効になります。続行するには、別の種類のボリュームを選択する必要があります。
3. 未割り当ての領域を指定するか、保存先ディスクを選択します。
   - ベーシックボリュームでは、選択したディスクで未割り当ての領域を指定します。
   - シンプル/スパンボリュームで、1 つ以上の保存先ディスクを選択します。
   - ミラーボリュームでは、2 つの保存先ディスクを選択します。
   - ストライプボリュームでは、2 つ以上の保存先ディスクを選択します。
   - RAID-5 ボリュームでは、3 つの保存先ディスクを選択します。

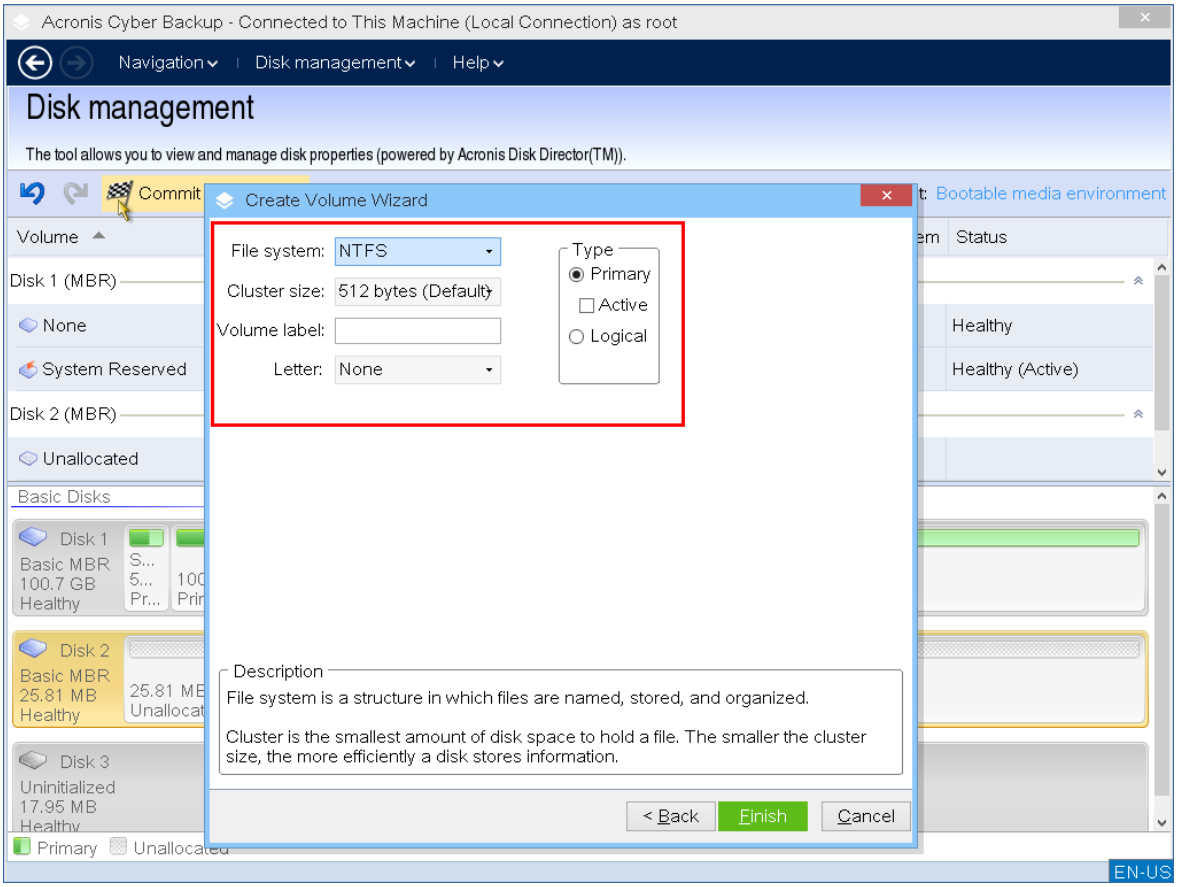
   ダイナミックボリュームを作成していて、ターゲットに 1 つ以上の**ベーシック**ディスクを選択した場合、選択したディスクが自動的にダイナミックに変換されるという警告が表示されます。

4. ボリュームのサイズを設定します。

   最大値には、通常、最大限の未割り当て領域が含まれます。場合によっては、提示された最大値が異なることがあります（たとえば、一方のミラーのサイズにより他方のミラーのサイズが決まる場合や、ディスク領域の最後の 8MB がベーシック ディスクからダイナミック ディスクへの将来の変換用に予約されている場合など）。

   ディスクの未割り当ての領域がボリュームより大きい場合は、ディスクの新しいベーシックボリュームの位置を選択できます。

5. ボリュームオプションを設定します。



ボリュームの **[ドライブ文字]**（デフォルトでは、アルファベット順で最初の空いているドライブ文字）と、オプションで **[ラベル]**（デフォルトでは、なし）を割り当てることができます。**[ファイルシステム]** と **[クラスターサイズ]** も指定する必要があります。

ファイルシステムオプション:

- FAT16（ボリューム サイズが 2 GB を超えて設定されている場合は無効）
- FAT32（ボリューム サイズが 2 TB を超えて設定されている場合は無効）
- NTFS
- ボリュームを未フォーマットのままにします。

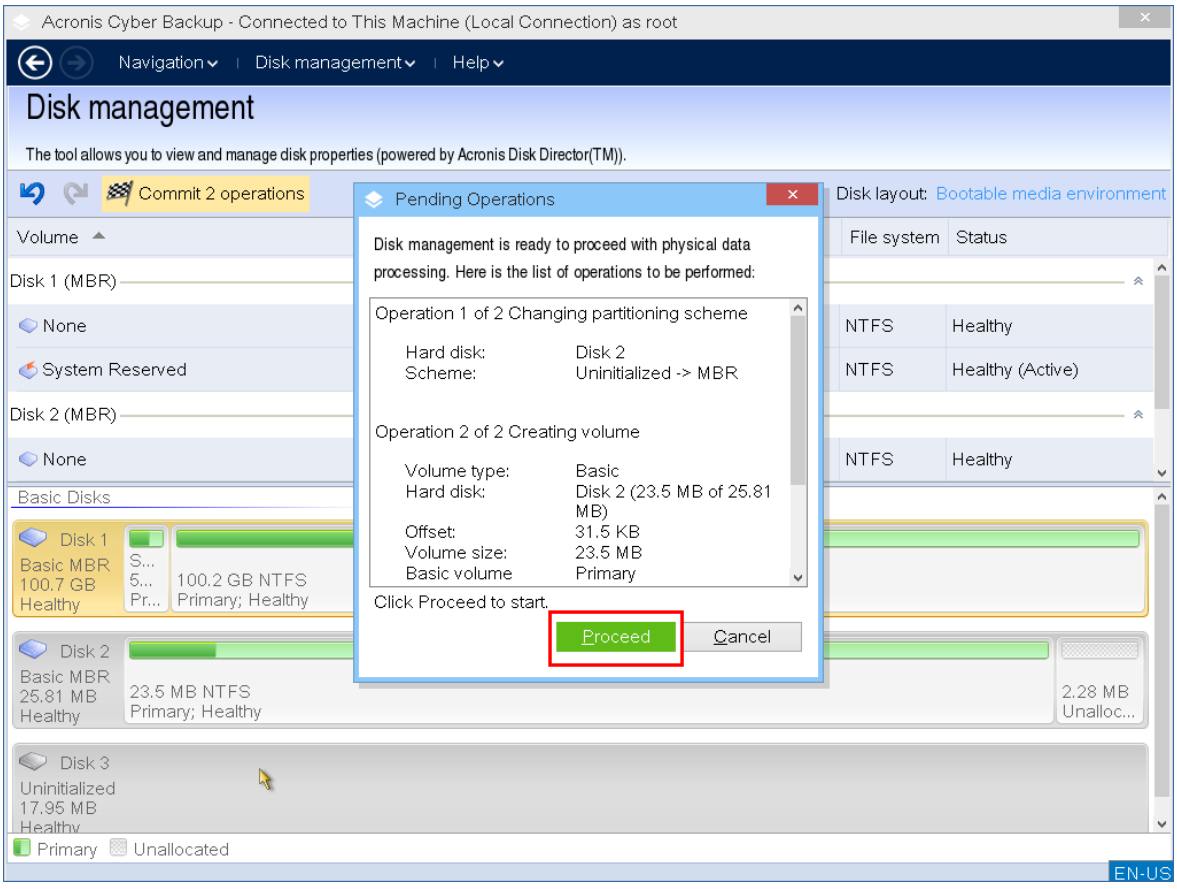
クラスターサイズの設定では、各ファイルシステムの事前設定された容量内で任意の数値を選択できます。デフォルトで提案されたクラスターサイズは、選択したファイルシステムのボリュームに最適です。FAT16/FAT32 に 64KB のクラスタ サイズを設定した場合、または NTFS に 8 ～ 64KB のク

ラスターサイズを設定した場合、Windows はボリュームをマウントできますが、一部のプログラム（セットアップ プログラムなど）がディスク容量を正しく計算できない場合があります。

ベーシックボリュームはシステムボリュームにすることができるので、ベーシックボリュームを作成している場合、ボリュームの種類を［**プライマリ**］（［**アクティブプライマリ**］）または［**論理**］から選択できます。通常は、オペレーティングシステムをボリュームにインストールするときに、**プライマリ**を選択します。オペレーティングシステムをこのボリュームにインストールしてマシンの起動時に、起動させる場合は、［**アクティブ**］(デフォルト)値を選択します。［**プライマリ**］ボタンを選択しない場合、［**アクティブ**］オプションは有効になりません。ボリュームがデータ ストレージ用の場合は、［**論理**］を選択します。

注意
ベーシックディスクには、最大 4 つのプライマリボリュームを含めることができます。既に最大数のボリュームが存在している場合は、ディスクをダイナミック ディスクに変換する必要があります。ダイナミック ディスクを選択しなければ、［**アクティブ**］オプションと［**プライマリ**］オプションは無効で、ボリュームの種類は［**論理ボリューム**］しか選択できません。

6. ［**コミット**］をクリックし、［**保留中の処理**］ウィンドウで［**実行**］をクリックします。操作をコミットせずにプログラムを終了すると、操作を事実上キャンセルすることになります。



ボリュームの削除

ボリュームを削除する

1. 削除するボリュームを右クリックします。
2. [**ボリュームの削除**] をクリックします。

> **注意**
> このボリューム上のすべてのデータは失われ、元に戻せません。

3. [**OK**] をクリックすると、保留中のボリューム削除処理が追加されます。
4. 追加された処理を完了するには、コミットします。操作をコミットせずにプログラムを終了すると、操作を事実上キャンセルすることになります。

ボリュームを削除すると、その領域は未割り当てディスク領域に追加されます。新しいボリュームを作成するか、別のボリュームの種類に変更するために使用できます。

アクティブ ボリュームの設定

複数のプライマリ ボリュームがある場合、ブート ボリュームとして 1 つを指定する必要があります。これを行うには、ボリュームをアクティブに設定します。1 台のディスクのアクティブボリュームは 1 つだけです。

ボリュームをアクティブに設定する

1. ベーシック MBR ディスク上の任意のプライマリボリュームを選択し、[**アクティブに設定**]をクリックします。
   システムにアクティブなボリュームが他にない場合、アクティブ ボリュームの設定が保留中の操作に追加されます。システムに別のアクティブボリュームが存在する場合、最初に以前のアクティブボリュームを非アクティブに設定する必要があることを示す警告が表示されます。

> **注意**
> 新しいアクティブボリュームを設定すると、以前のアクティブボリュームのドライブ文字が変更されたり、インストールされている一部のプログラムの動作が停止する場合があることに注意してください。

2. [**OK**] をクリックすると、アクティブボリュームを設定する保留中の処理を追加します。

> **注意**
> 新しいアクティブボリュームにオペレーティングシステムがある場合でも、マシンがそのボリュームから起動できないことがあります。新しいボリュームをアクティブに設定するという決定を確認する必要があります。

3. 追加された処理を完了するには、コミットします。操作をコミットせずにプログラムを終了すると、操作を事実上キャンセルすることになります。

ボリュームのドライブ文字の変更

Windows オペレーティング システムは、起動時にハード ディスク ボリュームにドライブ文字（C:、D: など）を割り当てます。これらのドライブ文字は、ボリュームでファイルやフォルダを見つけるためにアプリケーションとオペレーティング システムで使用されます。追加のディスクを接続したり、既存の

ディスクのボリュームを作成または削除すると、システム構成が変更される場合があります。この結果、一部のアプリケーションが通常どおり機能しなくなったり、ユーザー ファイルが自動で検出されず開けなくなる場合があります。これを回避するには、オペレーティング システムによって自動的にボリュームに割り当てられたドライブ文字を手動で変更します。

オペレーティングシステムによってボリュームに割り当てられたドライブ文字を変更する

1. 任意のボリュームを右クリックし、**[文字の変更]**をクリックします。
2. **[文字の変更]** ウィンドウで新しい文字を選択します。
3. **[OK]** をクリックすると、保留中のボリュームのドライブ文字割り当て処理が追加されます。
4. 追加された処理を完了するには、コミットします。操作をコミットせずにプログラムを終了すると、操作を事実上キャンセルすることになります。

ボリューム ラベルの変更

ボリューム ラベルは、オプションの属性です。この名前をボリュームに割り当てると簡単に認識できるようになります。

ボリュームラベルを変更するには

1. 任意のボリュームを右クリックし、**[ラベルの変更]**をクリックします。
2. **［ラベルの変更］** ウィンドウのテキスト フィールドに新しいラベルを入力します。
3. **[OK]** をクリックすると、ボリュームラベルの変更の保留中の操作を追加します。
4. 追加された処理を完了するには、コミットします。操作をコミットせずにプログラムを終了すると、操作を事実上キャンセルすることになります。

ボリュームのフォーマット

次のような目的でファイル システムを変更する場合に、ボリュームをフォーマットします。

- FAT16 または FAT32 ファイルシステムのクラスターサイズのために未利用となっている領域を利用する場合
- このボリュームに存在するデータを破壊するための、ある程度信頼できる簡単な方法として使用する場合

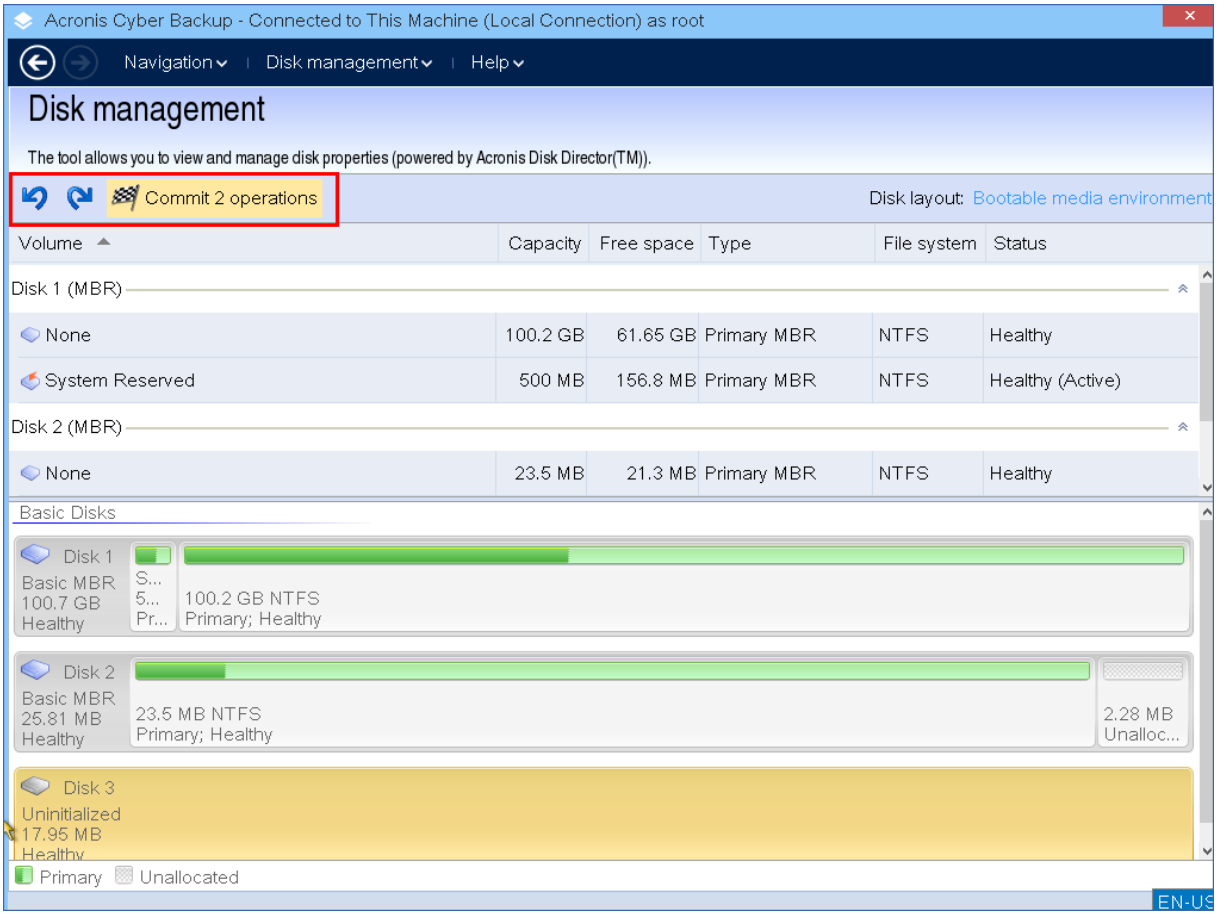
ボリュームをフォーマットする

1. 任意のボリュームを右クリックし、**[フォーマット]**をクリックします。
2. クラスターサイズとファイルシステムを選択します。ファイルシステムオプション:
   - FAT16（ボリューム サイズが 2 GB を超えて設定されている場合は無効）
   - FAT32（ボリューム サイズが 2 TB を超えて設定されている場合は無効）
   - NTFS
3. **[OK]** をクリックすると、保留中のボリュームのフォーマット処理が追加されます。
4. 追加された処理を完了するには、コミットします。操作をコミットせずにプログラムを終了すると、操作を事実上キャンセルすることになります。

保留中の操作

コミットコマンドを発行して確認するまで、すべての処理は保留中と見なされます。この方法によって、すべての計画された操作を制御したり、目的の変更を再確認したり、必要に応じて実行前に操作を取り消したりすることができます。

[ディスク管理] ビューには、保留中の操作を対象として **[元に戻す]**、**[やり直す]**、**[コミット]** 操作を実行するためのアイコンを含むツールバーがあります。これらの操作は、**[ディスク管理]** メニューからも開始できます。



計画されたすべての操作は、保留中の操作の一覧に追加されます。

［**元に戻す**］操作を使用すると、一覧の最後の操作を元に戻すことができます。この操作は、一覧が空でない場合に利用できます。

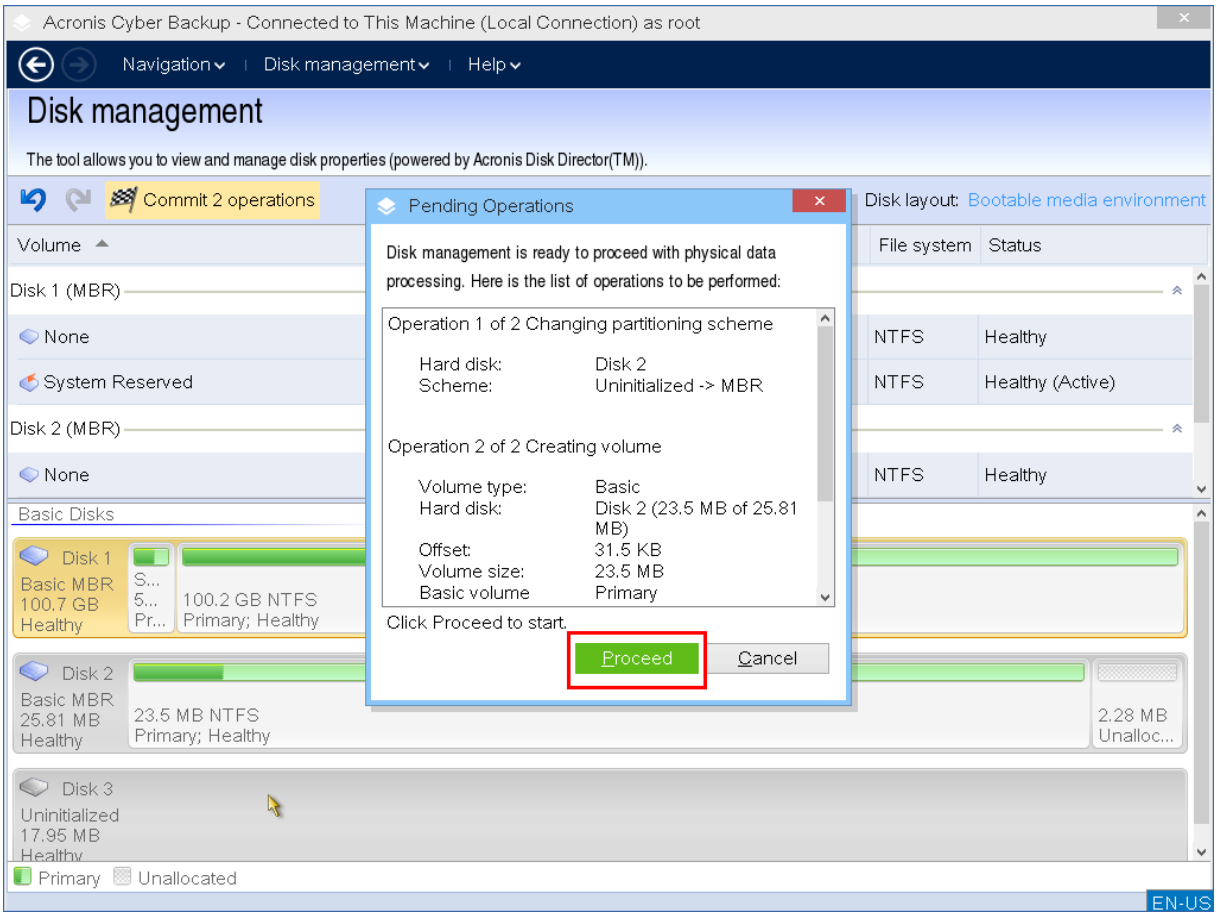
［**やり直す**］操作を使用すると、元に戻した最後の保留中の操作を復帰できます。

［**コミット**］操作を実行すると、［**保留中の操作**］ウィンドウが表示されます。このウィンドウでは、保留中の操作の一覧を確認できます。

実行を起動するには、**続行**をクリックします。

注意
[実行] 操作を選択した後は、操作を元に戻すことはできません。

コミットメントを続行しない場合は、**[キャンセル]** をクリックします。この場合、保留中の操作の一覧に対する変更は行われません。保留中の操作をコミットせずにプログラムを終了すると、操作を事実上キャンセルすることになります。）



ブータブルメディアのリモート操作

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（"Management Serverでメディアを登録"（379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]** に表示されるようになります。

Webインターフェースを使用してリモートでメディアを管理できます。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。

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。

   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"（271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、**[リカバリ]** 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"（325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、**[リカバリ]** > **[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（"物理マシンをリカバリする"（307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"（325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。

iSCSIデバイスの構成

このセクションでは、ブータブルメディアで作業しているときに、Internet Small Computer System Interface（iSCSI）デバイスを構成する方法について説明します。以下の手順を実行すると、ブータブルメディアからブートされたマシンにローカル接続しているように、これらのデバイスを使用できるようになります。

iSCSIターゲットサーバー（または**ターゲットポータル**）は、iSCSIデバイスをホストするサーバーです。**iSCSIターゲット**は、ターゲットサーバー上のコンポーネントです。このコンポーネントはデバイスを共有したり、デバイスにアクセスすることを許可されたiSCSIイニシエータのリストを作成したりします。**iSCSIイニシエータ**は、マシン上のコンポーネントです。このコンポーネントはマシンとiSCSIターゲットとの間の通信を提供します。ブータブルメディアからブートされたマシン上のiSCSIデバイスへのアクセスを構成する際、そのデバイスのiSCSIターゲットポータルと、ターゲットにリストされているiSCSIイニシエータの1つを指定する必要があります。ターゲットが複数のデバイスを共有する場合は、それらすべてにアクセスできるようになります。

LinuxベースのブータブルメディアにiSCSI デバイスを追加するには

1. **[ツール]** > **[iSCSI/NDASデバイスの構成]** をクリックします。
2. **[ホストの追加]** をクリックします。
3. iSCSI ターゲットポータルのホストの IP アドレスとポート番号、およびデバイスへのアクセスが許可された任意の iSCSI イニシエータの名前を指定します。

4. ホストの認証が要求される場合は、ユーザー名とパスワードを入力します。
5. **[OK]** をクリックします。
6. リストから iSCSI ターゲットを選択して、**[接続]** をクリックします。
7. iSCSI ターゲットの設定で CHAP 認証が有効になっている場合は、iSCSI ターゲットにアクセスするための資格情報を入力するよう求められます。iSCSI ターゲットの設定と同じユーザー名とターゲットシークレットを指定します。**[OK]** をクリックします。
8. **[閉じる]** をクリックしてウィンドウを閉じます。

PEベースのブータブルメディアにiSCSIデバイスを追加するには

1. **[ツール]** > **[iSCSIセットアップの実行]** をクリックします。
2. **[検出]** タブをクリックします。
3. **[ターゲットポータル]** で **[追加]** をクリックし、iSCSI ターゲットポータルの IP アドレスとポートを指定します。**[OK]** をクリックします。
4. **[一般]** タブ、**[変更]** の順にクリックし、デバイスへのアクセスが許可された任意の iSCSI イニシエータの名前を指定します。
5. **[ターゲット]** タブ、**[更新]** の順にクリックし、リストで iSCSI ターゲットを選択してから **[接続]** をクリックします。**[OK]** をクリックして iSCSI ターゲットに接続します。
6. iSCSI ターゲットの設定で CHAP 認証が有効になっている場合は、**認証失敗**のエラーが表示されます。この場合は、**[接続]**、**[詳細]** の順にクリックし、**[CHAP ログインを有効にする]** チェックボックスを選択して、iSCSI ターゲットの設定と同じユーザー名とターゲットシークレットを指定します。**[OK]** をクリックしてウィンドウを閉じてから、**[OK]** をクリックして iSCSI ターゲットに接続します。
7. **[OK]** をクリックしてウィンドウを閉じます。

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。

Startup Recovery Managerは、特にモバイルユーザーにとって便利です。エラーが発生した場合は、マシンを再起動し、「**Acronis Startup Recovery Managerを起動するには、F11を押してください...**」というメッセージが表示されたらF11キーを押します。プログラムが開始され、復元を実行できます。GRUBブートローダーがインストールされているマシンでは、再起動中にF11キーを押す代わりに、ブートメニューからStartup Recovery Managerを選択します。

ユーザーは、移動中にStartup Recovery Managerを使用してバックアップすることもできます。

Startup Recovery Managerを使用するには、まず有効化する必要があります。このようにして、起動時の「**Acronis Startup Recovery Managerを起動するには、F11を押してください**」というメッセージを有効にできます（またGRUBブートローダーを使用している場合は、**Startup Recovery Manager**項目をGRUBメニューに追加します）。

注意
暗号化されていないシステムボリュームを含むマシンでStartup Recovery Managerを有効化するには、該当のマシンに少なくとも100MBの空き容量が必要になります。マシンの再起動を伴う復元操作には、さらに100MBの容量が必要です。

BitLockerで暗号化されたボリュームを含むマシンに、少なくとも1つの非暗号化ボリュームがある場合、Startup Recovery Managerを有効化できます。非暗号化ボリュームには、少なくとも500MBの空き領域が必要です。マシンの再起動が必要な復元操作では、マシンに500MBの追加の空き容量が必要になります。

重要
Startup Recovery Managerが有効化されていない場合、ワンクリック復元で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。

GRUBブートローダーを使用しており、それがマスターブートレコード（MBR）内にインストールされている場合を除き、Startup Recovery Managerをアクティベーションすると、そのブートコードでMBRが上書きされます。従って、このようなブートローダーがインストールされている場合は、再度有効化が必要になる可能性があります。

Linuxでは、GRUB以外のブートローダー（LILOなど）を使用する場合、Startup Recovery Managerを有効化する前に、MBRではなくLinuxのルート（またはブート）パーティションブートレコードにインストールすることを検討できます。または、アクティブ化した後に手動でブート ローダーを再設定してください。

Startup Recovery Managerの有効化

WindowsエージェントまたはLinuxエージェントを実行しているマシンでは、Cyber Protect Webコンソールを使用してStartup Recovery Managerを有効化できます。

Cyber Protectウェブコンソールで Startup Recovery Managerを有効化するには

1. 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。
4. ソフトウェアによってStartup Recovery Managerが有効化されるのを待ちます。

エージェントがないマシンで Startup Recovery Managerを有効化するには

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. **[ツール]** > **[Startup Recovery Managerの有効化]** をクリックします。
3. ソフトウェアによってStartup Recovery Managerが有効化されるのを待ちます。

Startup Recovery Managerの無効化

Startup Recovery Managerを無効化するには、アクティベーションの手順を繰り返し、それぞれの反対の操作を選択します。無効化すると、起動時の「**Acronis Startup Recovery Managerを起動するに**

は、F11を押してください」というメッセージ（またはGRUBのメニュー項目）が無効になります。

Startup Recovery Managerが有効化されていない状態で、システムの起動に失敗した場合、システムをリカバリするには次のいずれかを実行する必要があります。

- 別のブータブルメディアからコンピュータを起動する
- PXE ServerまたはMicrosoftリモートインストールサービス（RIS）からネットワークブートを使用する

Acronis PXE Server

Acronis PXE Serverを使用すると、ネットワーク経由でAcronisブータブルコンポーネントを使用してマシンを起動することができます。

ネットワーク ブートには次の利点があります。

- 起動する必要のあるシステムにブータブルメディアをインストールする技術者を現地で待機させる必要がなくなります。
- グループ操作の実行では、物理的なブータブル メディアを使用するときに比べて、複数のコンピュータを起動するのに必要な時間が短縮されます。

ブータブルコンポーネントは、Acronisブータブルメディアビルダーを使用してAcronis PXE Serverにアップロードします。ブータブルコンポーネントをアップロードするには、ブータブルメディアビルダを起動してから、「Linuxベースのブータブルメディア」で説明されている詳細な手順に従います。

Acronis PXE Serverから複数のマシンを起動する方法は、ネットワークにDHCP（Dynamic Host Control Protocol）サーバーが存在する環境に適しています。DHCP サーバーが存在すると、起動したコンピュータのネットワーク インターフェイスは自動的に IP アドレスを取得できます。

制限事項:

Acronis PXE Serverは、UEFIブートローダーをサポートしません。

Acronis PXE Server のインストール

Acronis PXE Server をインストールする手順は、次のとおりです。

1. 管理者としてログオンし、Acronis Cyber Protect プログラムの設定を起動します。
2. （オプション）プログラムの設定の言語を変更するには、**[言語の設定]** をクリックします。
3. ライセンス契約とプライバシーステートメントに同意して、**[次へ]** をクリックします。
4. **[インストール設定のカスタマイズ]** をクリックします。
5. **[インストールする項目]** の横にある **[変更]** をクリックします。
6. **[PXE Server]** チェックボックスをオンにします。このコンピュータに他のコンポーネントをインストールしない場合は、対応するチェック ボックスをオフにします。 **[完了]** をクリックして先に進んでください。
7. （オプション）他のインストール設定を変更します。

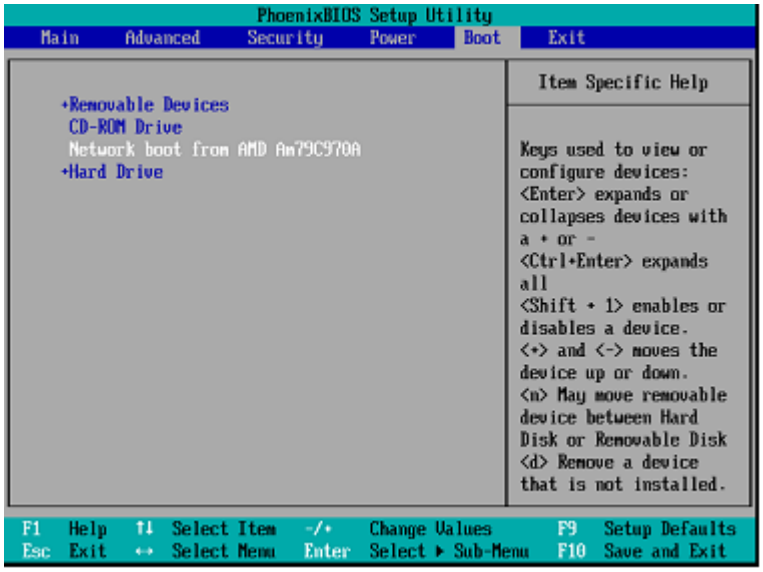
8. [**インストール**] をクリックして、インストールを続行します。
9. インストールが完了した後、［**閉じる**］をクリックします。

Acronis PXE Server は、インストールが完了すると直ちにサービスとして動作します。その後は、システムが再起動するたびに自動的に起動されます。他の Windows サービスと同様に、Acronis PXE Server を停止および開始できます。

PXE から起動するコンピュータの設定

ベア メタル状態のディスクの場合は、コンピュータの BIOS でネットワーク ブートがサポートされているだけで起動できます。

ハード ディスクにオペレーティング システムがインストールされているコンピュータでは、ネットワーク インターフェイス カードが最初のブート デバイスになるか、少なくともハード ディスク デバイスより前に起動されるように BIOS を設定する必要があります。適切な BIOS 設定の 1 つの例を次に示します。ブータブル メディアを挿入しないと、コンピュータはネットワークから起動します。



一部の BIOS のバージョンでは、ブート デバイスの一覧にネットワーク インターフェイス カードを表示するには、そのカードを有効にして変更内容を BIOS に保存する必要があります。

ハードウェアに複数のネットワーク インターフェイス カードがあるときは、BIOS でサポートされているカードにネットワーク ケーブルが接続されていることを確認してください。

サブネットをまたがる操作

Acronis PXE Serverが（スイッチを越えて）別のサブネットを操作できるようにするには、PXEトラフィックを中継するようにスイッチを設定します。PXEサーバーのIPアドレスは、DHCPサーバーのアドレスと同様、IPヘルパー機能を使用してインターフェースごとに構成されます。詳細については、https://docs.microsoft.com/ja-jp/troubleshoot/mem/configmgr/boot-from-pxe-serverを参照してください。

モバイル デバイスの保護

バックアップアプリにより、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

バックアップアプリは、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。

- iOS10.3以降（iPhone、iPod、およびiPad）
- Android 5.0以降

バックアップできる内容

- 連絡先
- 写真
- 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。
- **自動バックアップ**機能は、デフォルトで有効になっています。この設定がオンの場合:
  - Android 7.0以降の場合、バックアップアプリは新しいデータを即座に自動検出し、クラウドにアップロードします。
  - Android 5および6の場合、変更は3時間ごとに確認されます。アプリの設定で、自動バックアップをオフにすることもできます。
- **[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、バックアップアプリは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。
- エネルギーを節約する2つの方法があります。
  - デフォルトで無効になっている **[充電中にバックアップ]** 機能。この設定がオンの場合、バックアップ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、バックアップアプリはデバイスのバッテリー残量が少なくないときにのみ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。このオプションは、Android 8以降で使用できます。

- 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ウェブ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し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。
- バックアップアプリでは、最新のデータバージョンのみを復元できます。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ウェブコンソールを使用します。
- [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。

バックアップアプリの入手先

1. モバイル デバイスでブラウザを開き、https://backup.acronis.comに移動します。
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]** > **[追加]**をクリックします。
4. **[モバイル デバイス]** でデバイスの種類を選択します。
   デバイスの種類によってアプリ ストアまたはGoogle Playにリダイレクトされます。
5. （iOSデバイスのみ）**[取得]** をクリックします。
6. **[インストール]** をクリックして、バックアップ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。

[セットアップ] をタップして初回のバックアップを作成します。

1. 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。
2. [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。

3. **[バックアップ]** をタップします。
4. 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。

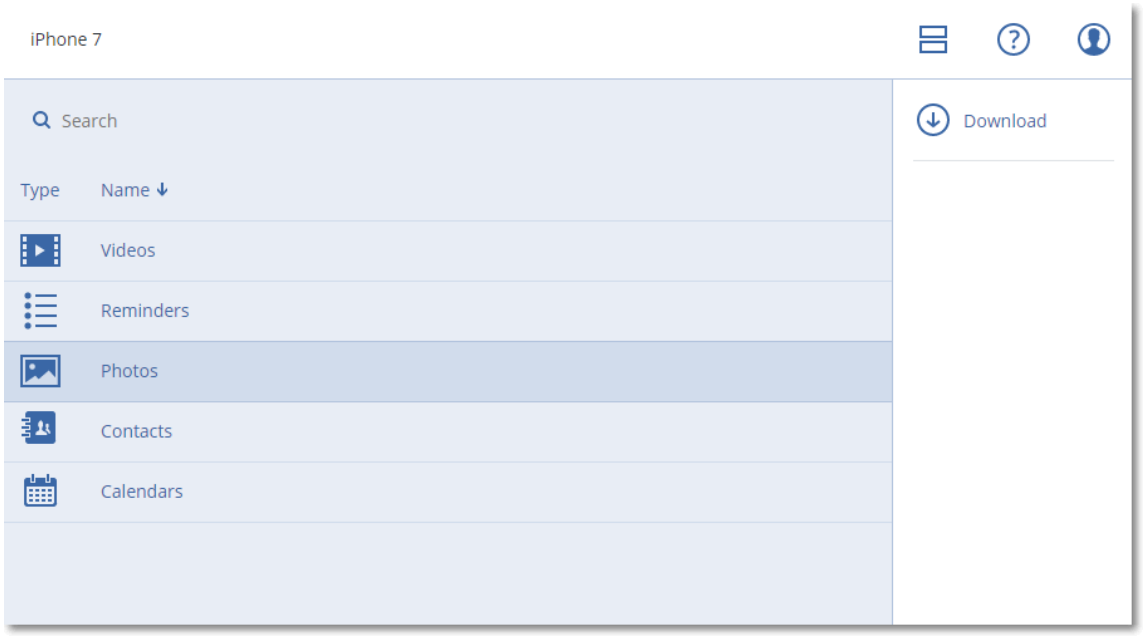
バックアップが開始されます。

モバイルデバイスにデータを復元する方法

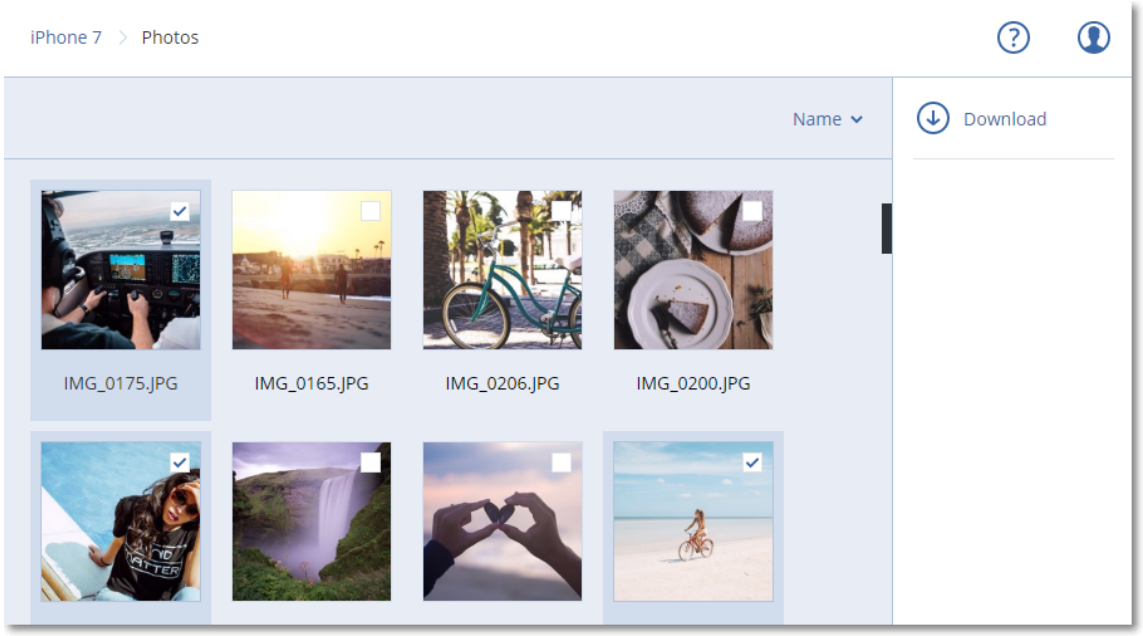
1. バックアップアプリを開きます。
2. **[参照]** をタップします。
3. デバイス名をタップします。
4. 次のいずれかを実行します。
   - バックアップされたデータをすべて復元するには、**[すべて復元]** をタップします。これ以上の操作は不要です。
   - データ カテゴリを 1 つ以上復元するには、**[選択]** をタップしてから必要なデータ カテゴリのチェック ボックスをタップします。**[復元]** をタップします。これ以上の操作は不要です。
   - 同一のデータ カテゴリに属しているデータ アイテムを復元するには、そのデータ カテゴリをタップします。手順に従って進めます。
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ウェブ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ウェブコンソールの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。

Microsoft アプリケーションの保護

重要
このセクション内に記載されているいくつかの機能は、オンプレミスデプロイメントでのみ使用できます。

Microsoft SQL ServerとMicrosoft Exchange Serverの保護

これら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。

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、https://kb.acronis.com/content/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であること。
- 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。
- ユーザーアカウント制御（UAC）がマシンで無効であること。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。
- ユーザーアカウント制御（UAC）がマシンで無効であること。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」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 1 つ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」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」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することができます。
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

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。

   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、**[デバイス]** > **[Microsoft SQL]** > **[データベース]** にAAGおよびAAG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 SQLをインストールするには、AAG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。

2. 「SQLデータベースの選択」に従って、バックアップするAAGかデータベースセットを選択します。

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

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。

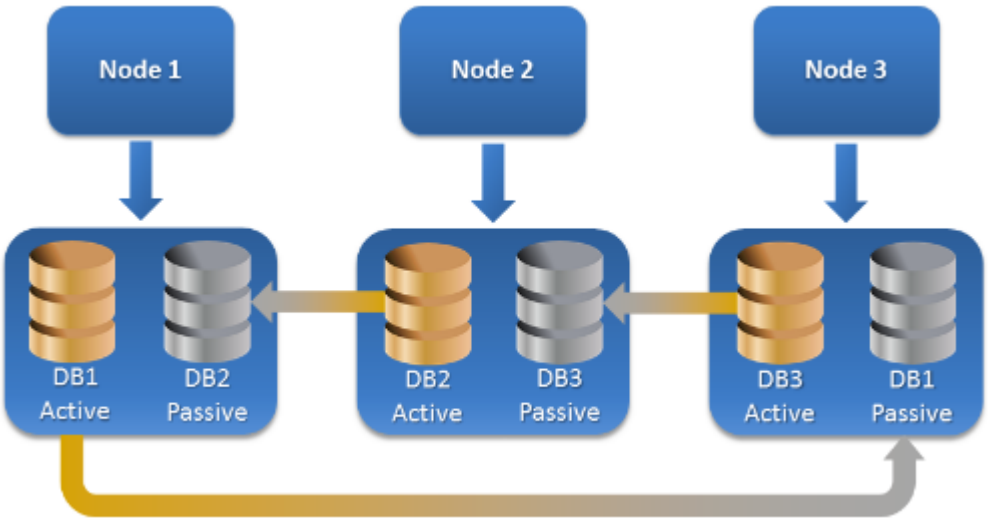
クラスター認識型バックアップ

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 ウェブコンソールの **[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ときに、「Exchange Serverデータの選択」の説明に従ってDAGを選択します。
2. [クラスタ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。
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」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

アプリケーションアウェア型のディスクレベルバックアップは、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。

1. 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。

2. 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。
3. 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。
4. 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）と VMware エージェント（Linux）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。これら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。

他の要件は、"前提条件"（438ページ）および"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"（446ページ）に記載されています。

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:

  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:

  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ポリシーを無効化できない場合は、アプリケーション認識型バックアップを構成するときに、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。

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. **[バックアップ]** 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

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。

SQLサーバーインスタンスを実行しているマシンにSQLエージェントがインストールされている場合、SQLサーバーインスタンスにSQLデータベースをリカバリできます。

Windows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サーバー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。

代わりに、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。これは、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必要がある場合に役立ちます。「SQL Serverデータベースの接続」に従い、SQLデータベースファイルをSQL サーバー インスタンスに接続できます。

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。

システムデータベースは、基本的にユーザー データベースと同じ方式で復元されます。システムデータベースの復元の特性については、「システムデータベースの復元」で詳しく説明しています。

SQLデータベースをSQLサーバーインスタンスに復元するには

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 SQL]** 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 SQL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、SQLデータベース復元のターゲット 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]** > **[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、**[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]** > **[データベースをインスタンスに]** 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。データベースの復元先として別のSQLサーバーインスタンス（同じマシンで実行中）を選択できます。

   データベースを別のものとして同じインスタンスに復元するには

   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. （オプション）（データベースを元のインスタンスに復元して新しいデータベースにした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、以下のいずれかを選択します。
   - **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 サーバー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。

7. **[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。

SQL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 SQL]** 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 SQLまたはエージェントfor VMware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、SQLデータベース復元のターゲット 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]** > **[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。
   - 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。

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

このセクションでは、Exchangeメールボックスとメールボックスアイテムをデータベースバックアップ、アプリケーション認識型バックアップ、およびメールボックスバックアップからリカバリする方法について説明します。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。

復元できるアイテム：

- 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"（441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
- 電子メールメッセージ
- 予定表のイベント
- 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。

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

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メールボックスの保護"（463ページ）を参照してください。

メールボックスの復元

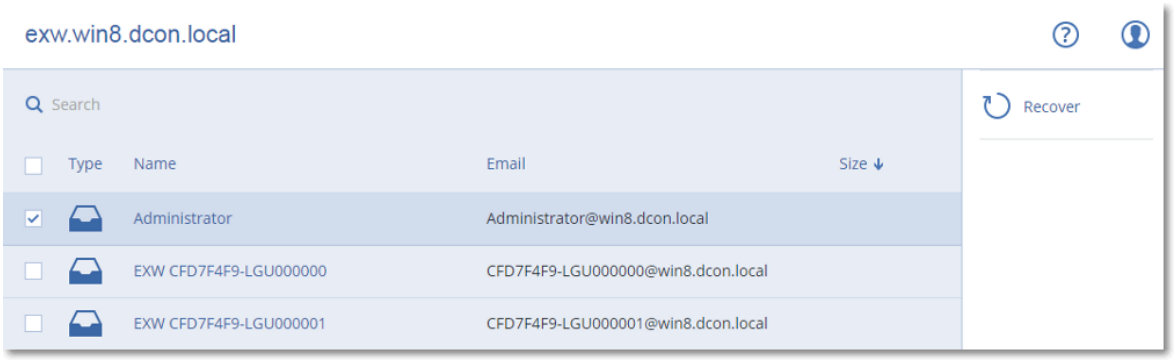
アプリケーション認識型バックアップまたはデータベースバックアップからメールボックスを復元するには

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Agent for Office 365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 Office 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 Office 365 エージェントをインストールします。
   - 組織で Office 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、Office 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 Office 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"（449ページ）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Agent for Office 365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 Office 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 Office 365 エージェントをインストールします。
   - 組織で Office 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、Office 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。

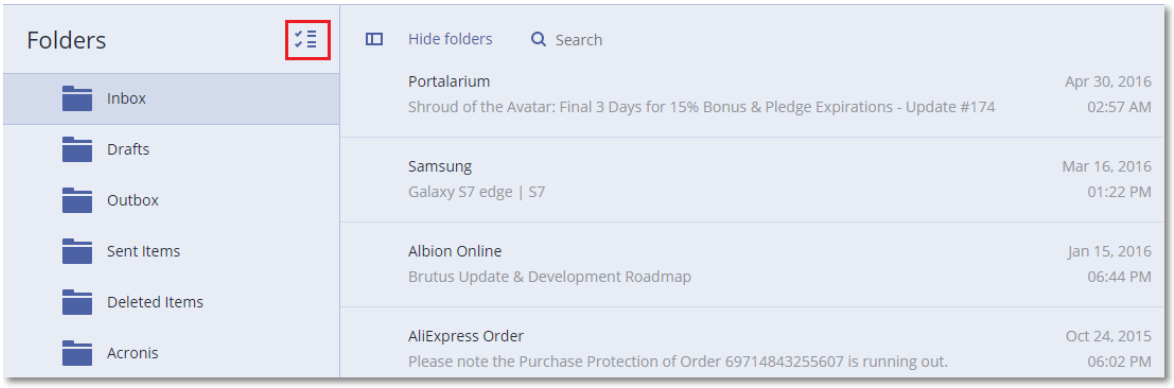
   上記のアクションのいずれかで参照用に選択されたコンピュータが、オフラインである元のコンピュータの代わりに、復元を実行します。
5. **[復元]** > **[Exchangeメールボックス]** の順にクリックします。
6. 復元するアイテムが元々存在していたメールボックスをクリックします。
7. 復元するアイテムを選択します。

   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 Office 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"（449ページ）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]** > **[電子メールメッセージ]** 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 Microsoft 365にリカバリするとき、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、Agent for Office 365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。

Microsoft 365メールボックスの保護

重要
このセクションでAcronis Cyber Protectのオンプレミス配置を有効化します。クラウド配置を使用している場合は、
https://www.acronis.com/support/documentation/CyberProtectionService/#protecting-microsoft-365-data.htmlを参照してください。

ライセンスオプションの詳細については、「Microsoft 365向けAcronis Cyber Backupのライセンス」を参照してください。

Microsoft 365メールボックスをバックアップする理由

Microsoft 365はクラウドサービスですが、定期的にバックアップすることで、ユーザーのエラーや意図的な悪意のある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の理由から必要な場合も、Microsoft 365メールボックスのローカルコピーを保存できます。

復元

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
- 電子メールメッセージ
- 予定表のイベント
- 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。

復元は、Microsoft 365またはライブExchange Serverに対して実行できます。

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、IDが一致する既存のアイテムは上書きされます。メールボックスが既存の Exchange Server メールボックスに復元された場合は、ID が一致する既存のアイテムはそのまま保存されます。復元されたアイテムは、その横に配置されます。

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。

制限事項

- 保護計画を 500 以上のメールボックスに適用するとバックアップの作成速度が低下する場合があります。大量のメールボックスを保護するために、幾つかの保護計画を作成し、別々の時に実行するようスケジュールします。
- 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。
- 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。
- 新しいMicrosoft 365メールボックスに復元することはできません。まず新しいMicrosoft 365ユーザーを手動で作成してから、そのユーザーのメールボックスにアイテムをリカバリする必要があります。
- 別のMicrosoft 365組織への復元はサポートされていません。
- Microsoft 365でサポートされている一部のアイテムの種類またはプロパティは、Exchange Serverでサポートされていない場合があります。これらは、Exchange Server への復元中にスキップされます。

Microsoft 365組織の追加

Microsoft組織を追加するには、アプリケーションID、アプリケーションキー、Microsoft 365テナントIDの情報が必要です。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」を参照してください。

Microsoft 365組織を追加するには

1. Office 365エージェントを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します。1つの組織にはエージェント for Office 365は1つのみである必要があります。
2. Cyber Protectウェブコンソールで、[**Microsoft Office 365**] をクリックします。
3. 開くウィンドウで、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。
4. [**サインイン**]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**] タブのCyber ProtectWebコンソールに表示されます。

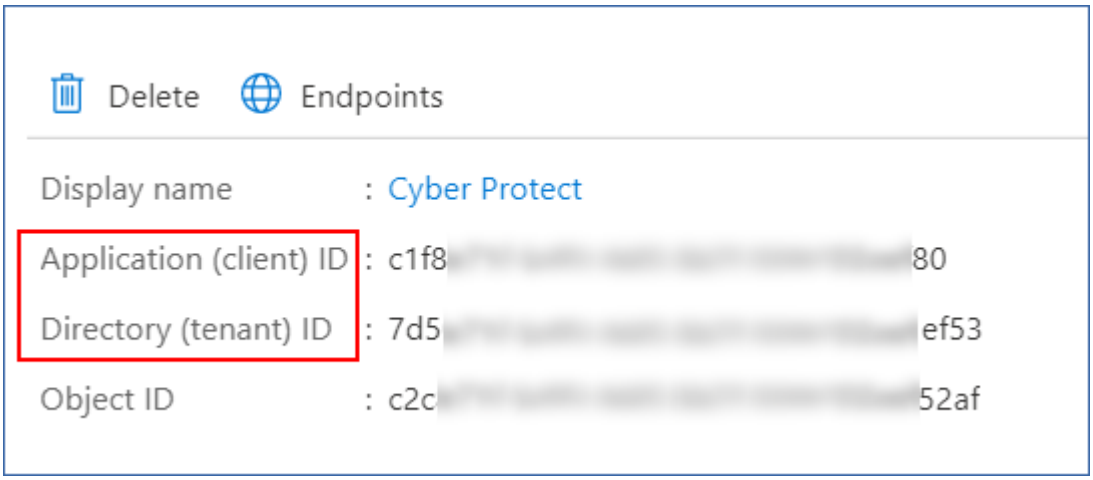
アプリケーション ID とアプリケーションシークレットの取得

Microsoft 365の新しい認証を使用するには、Azure Active Directoryでカスタムアプリケーションを作成し、特定のAPIを許可する必要があります。このように、ウェブコンソールを表示するために必要な**アプリケーションID**、**アプリケーションシークレット**、**ディレクトリ（テナント）ID**を取得します。

Azure Active Directory でアプリケーションを作成する

1. Azure ポータル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 Protect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。

アプリケーションが作成されました。Azure ポータルで、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。



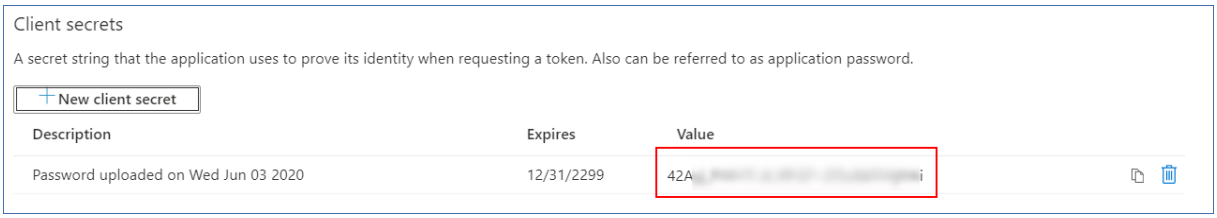
Azure ポータルでアプリケーションを作成する方法の詳細については、Microsoft 文書を参照してください。

必要な API 許可をアプリケーションに付与する

1. Azure ポータルで、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. Azure ポータルで、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. Cyber ProtectWebコンソールで、**[デバイス]** > **[Microsoft Office 365]** に進みます。
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」を参照してください。
5. **[サインイン]**をクリックします。

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。

メールボックスを選択する方法

1. Cyber ProtectWebコンソールで、**[デバイス]** > **[Microsoft Office 365]** に進みます。
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. （Exchange Serverに復元する場合のみ）復元するメールボックスを所有するユーザーのユーザー名と同じログオン名のExchangeユーザーが存在することを確認します。存在しない場合は、ユーザーを作成します。このユーザーの要件一覧については、"ユーザーアカウントに関する要件"（456ページ）を参照してください。
2. Cyber ProtectWebコンソールで、**[デバイス]** > **[Microsoft Office 365]** に進みます。
3. 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。

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。
5. **[復元]** >**[メールボックス]** の順にクリックします。
6. Exchange Serverに復元するには、**[復元先]** で **[Microsoft Exchange]** を選択します。"メールボックスの復元"（457ページ）の手順9以降に従って復元を続行します。ここでは、その他の手順は不要です。

   Microsoft 365に復元するには、**[復元先]** の値をデフォルトの **[Microsoft Office 365]** のままにします。
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。

メールボックスのアイテムの復元

1. （Exchange Serverに復元する場合のみ）復元するメールボックスを所有するユーザーのユーザー名と同じログオン名のExchangeユーザーが存在することを確認します。存在しない場合は、ユーザーを作成します。このユーザーの要件一覧については、"ユーザーアカウントに関する要件"（456ページ）を参照してください。
2. Cyber ProtectWebコンソールで、**[デバイス]** > **[Microsoft Office 365]** に進みます。
3. 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。
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。
5. **[復元]** > **[電子メールメッセージ]** の順にクリックします。
6. 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] のアイコン（  ）をクリックします。

7. **[復元]** をクリックします。
8. Exchange Serverに復元するには、**[復元先]** で **[Microsoft Exchange]** を選択します。
   Microsoft 365に復元するには、**[復元先]** の値をデフォルトの **[Microsoft Office 365]** のままにします。
9. （Exchange Serverに復元する場合のみ）**復元先のマシンを選択または変更するには、[Microsoft Exchange Serverを搭載するターゲットマシン]** をクリックしてします。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。
   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。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"（449ページ）に記載されています。
10. **[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。
11. （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。
12. **[復元を開始]** をクリックします。

Google Workspaceデータを保護

この機能は Acronis Cyber Protect のクラウド配置でのみ使用可能です。この機能の詳細については、https://www.acronis.com/support/documentation/CyberProtectionService/#protecting-google-workspace-data.htmlを参照してください。

Oracle データベースの保護

Oracleデータベースの保護については、https://dl.managed-protection.com/u/pdf/AcronisCyberProtect_15_OracleBackup_whitepaper.pdfで入手できる個別の文書に記載されています。

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。

この一時仮想コンピュータを実行するのは3日間までにしてください。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。

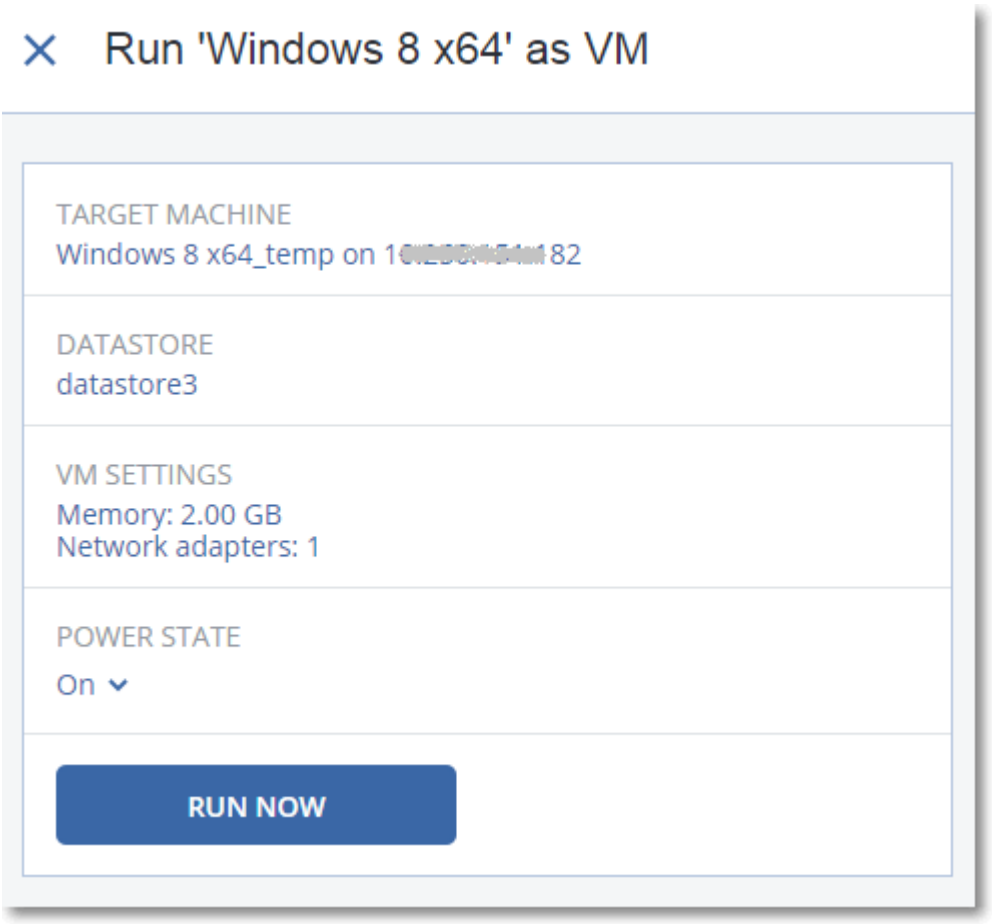
前提条件

- 1つまたは複数のVMwareエージェントまたはHyper-Vエージェントをサイバープロテクション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、Storage Node 上、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マシン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。SFTPサーバー、テープデバイス、Secure Zoneに格納されたバックアップからは仮想コンピュータを実行できません。
- 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。

コンピュータの削除

vSphere/Hyper-Vで直接一時仮想コンピュータ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ことがあります。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、確定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。確定を実行する計画があり、選択の余地がある場合は、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。

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

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。

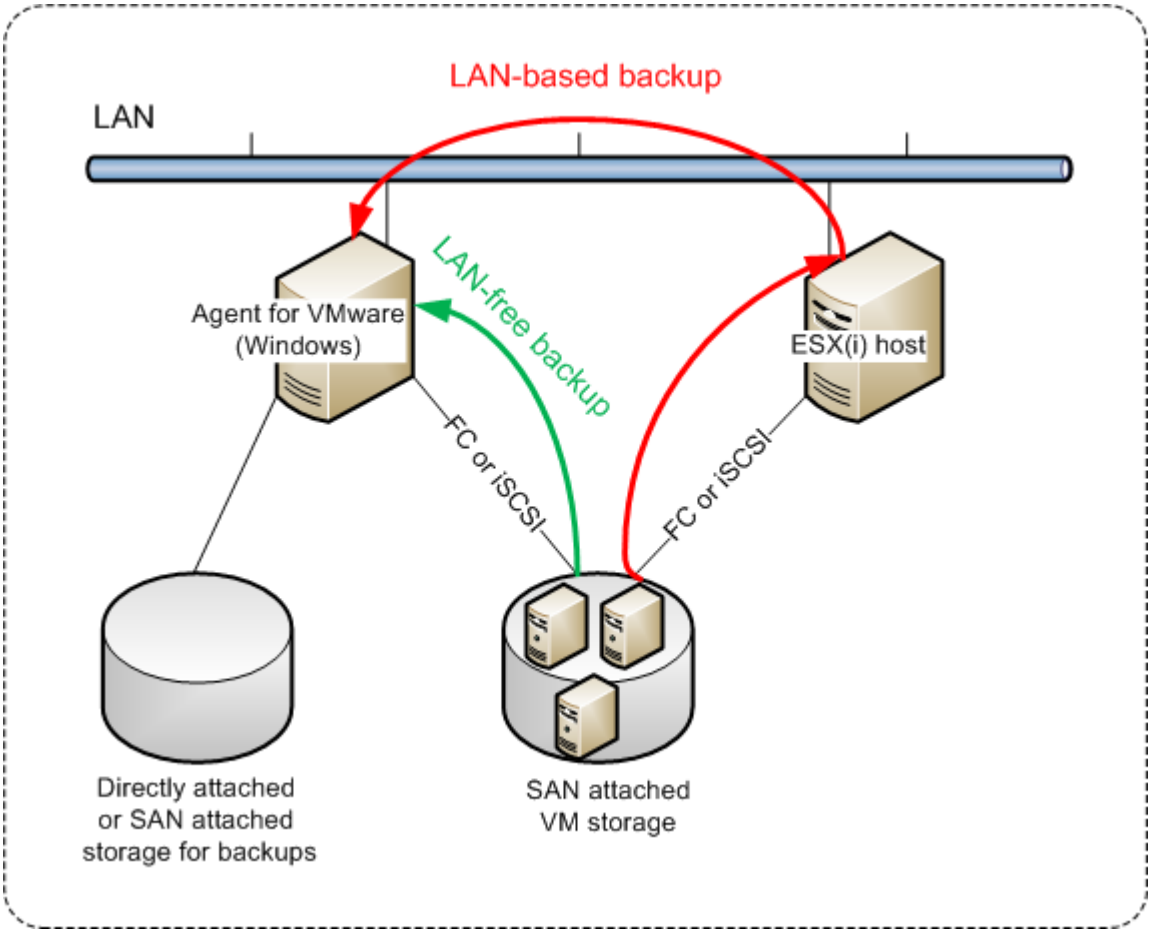
LAN フリー バックアップ

運用 ESXi ホストの負荷が非常に高く、仮想アプライアンスの実行が望ましくない場合、ESXi インフラストラクチャ外部にある物理コンピュータへのエージェント for VMware（Windows）のインストールを検討してください。

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。

     LUN の初期化を回避するために、VMwareエージェント（Windows）のインストール時に **[SAN ポリシー]** が自動的に **[すべてオフライン]** に設定されます。

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）。

制限事項

- 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。

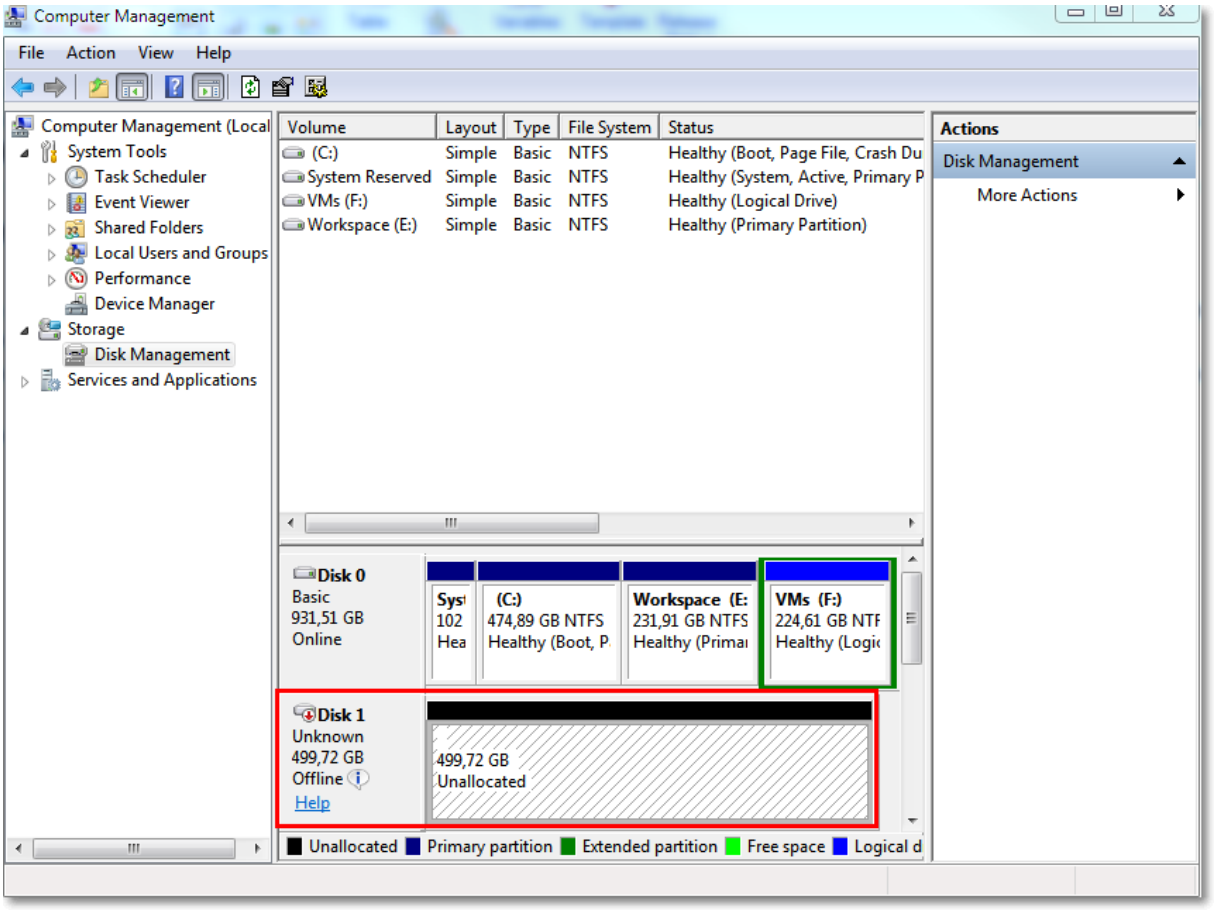
iSCSI イニシエーターの設定手順

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。



SANハードウェアスナップショットの使用

VMware vSphereでストレージエリアネットワーク（SAN）ストレージシステムをデータストアとして使用する場合は、エージェントfor VMware（Windows）を有効にして、バックアップの実行時にSANハードウェアスナップショットを使用できます。

重要
NetApp SANストレージのみサポートされています。

SANハードウェアスナップショットを使用する理由

一貫性のあるバックアップを作成するためには、エージェントfor VMwareに仮想コンピュータスナップショットが必要です。エージェントは仮想ディスクの内容をスナップショットから読み込むので、スナップショットはバックアップ処理中を通して保持される必要があります。

エージェントはデフォルトで、ESXiホストによって作成されたネイティブVMwareスナップショットを使用します。スナップショットが保持されている間、仮想ディスクファイルは読み取り専用状態にあり、ホストはディスクの変更内容をすべて別個のデルタファイルに書き込みます。バックアップ処理が完了すると、ホストはスナップショットを削除します。言い換えると、デルタファイルを仮想ディスクファイルと結合します。

スナップショットの維持と削除はどちらも仮想コンピュータのパフォーマンスを左右します。仮想ディスクが大きく、データの変更が速いと、処理に時間がかかり、その間のパフォーマンスが低下することがあります。極端な例として、複数のコンピュータのバックアップを同時に実行すると、増大するデルタファイルがデータストアをほぼ専有してしまい、仮想コンピュータの電源がすべてオフになる可能性があります。

ハイパーバイザのリソース利用率は、スナップショットをSANに移すことで削減できます。この場合、一連の処理は次のようになります。

1. 仮想ディスクを整合性のとれた状態にするために、バックアップ処理の冒頭でESXiによってVMwareスナップショットが作成されます。
2. SANによって、仮想コンピュータとそのVMwareスナップショットを含むボリュームまたはLUNのハードウェアスナップショットが作成されます。普通、この処理にかかる時間は数秒です。
3. ESXiによってVMwareスナップショットが削除されます。エージェントfor VMwareが仮想ディスクの内容をSANハードウェアスナップショットから読み込みます。

VMwareスナップショットは数秒しか維持されないので、仮想コンピュータのパフォーマンス低下は最小限に抑えられます。

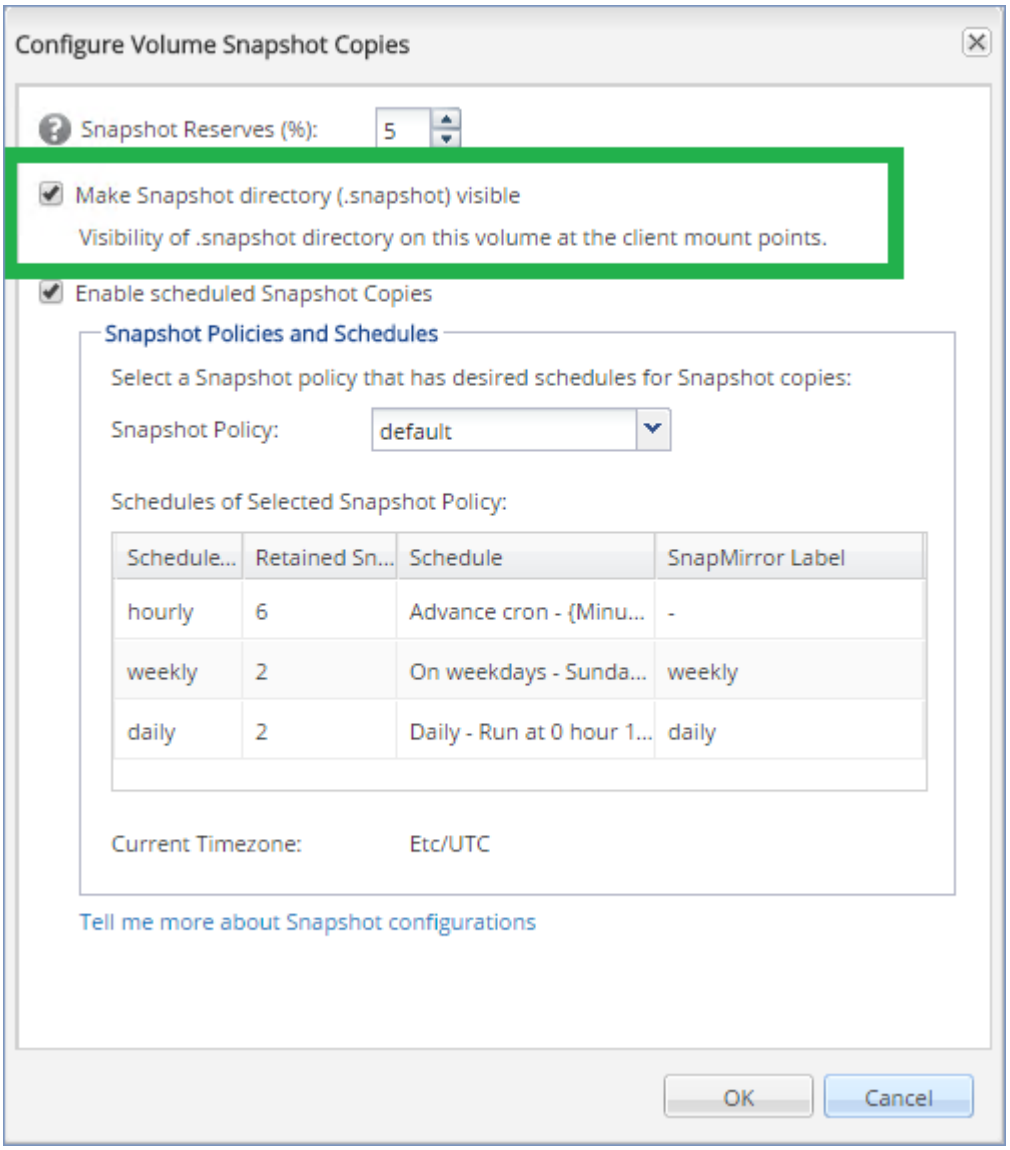
SANハードウェアスナップショットを使用するために必要なもの

仮想コンピュータのバックアップを実行する際にSANハードウェアスナップショットを使用する場合は、次のすべてに該当することを確認します。

- NetApp SANストレージが「NetApp SANストレージ要件」に記載されている要件を満たしている。
- エージェントfor VMware（Windows）を実行しているコンピュータが「エージェントfor VMwareを実行しているマシンの設定」の説明に沿って構成されている。
- SANストレージがManagement Serverに登録されている。
- （上記の登録に含まれなかったエージェントfor VMwareがある場合）SANストレージ上に存在する仮想コンピュータが、「仮想コンピュータのバインド」の説明に沿ってSAN対応エージェントに割り当てられている。
- [SANハードウェアスナップショット] バックアップオプションが保護計画で有効になっている。

NetApp SANストレージ要件

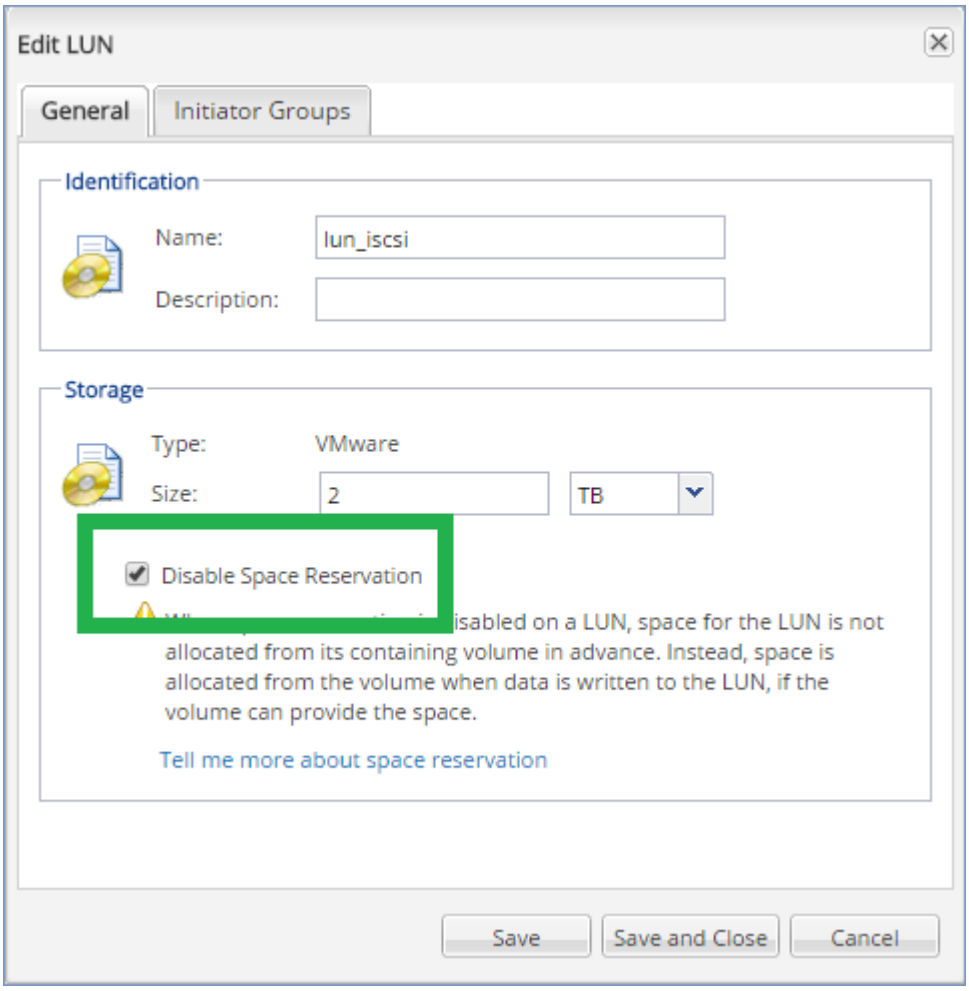
- SANストレージは、NFSまたはiSCSIデータストアとして使用する必要があります。
- SANは、**Clustered Data ONTAP（cDOT）**モードでData ONTAP 8.1以降を実行している必要があります。**7-mode**モードはサポートされていません。
- NetApp OnCommand System Managerで、**データストアが置かれているボリュームに対して、[Snapshot copies（スナップショットのコピー）] > [設定] > [Make Snapshot directory (.snapshot) visible（スナップショットディレクトリ（.snapshot）の表示）]** チェックボックスをオンにする必要があります。



- （NFSデータストア）データベース作成時に指定したStorage Virtual Machine（SVM）で、Windows NFSv3クライアントからNFS共有へのアクセスを有効にする必要があります。アクセスは、次のコマンドによって有効にできます。

  ```
  vserver nfs modify -vserver [SVM name] -v3-ms-dos-client enable
  ```

  詳細については、NetAppのベストプラクティスに関するドキュメント（https://kb.netapp.com/support/s/article/ka21A0000000k89QAA/top-windows-nfsv3-0-issues-workarounds-and-best-practices）を参照してください。
- （iSCSIデータストア）NetApp OnCommand System Managerで、データストアが置かれているiSCSI LUNに対して、[**Disable Space Reservation（領域予約の無効化）**] チェックボックスをオンにする必要があります。



エージェントfor VMwareを実行しているマシンの設定

SANストレージがNFSまたはiSCSIデータストアとして使用されているかどうかに応じて、以下の該当するセクションを参照してください。

iSCSIイニシエータの設定

次のすべてに当てはまることを確認します。

- Microsoft iSCSIイニシエータがインストールされている。
- Microsoft iSCSIイニシエータサービスのスタートアップの種類が、**[自動]** または **[手動]** に設定されている。この設定は、**サービス**スナップインで行うことができます。
- iSCSIイニシエータが、「LANフリーバックアップ」の例示セクションで説明しているとおりに設定されている。

NFSクライアントの設定

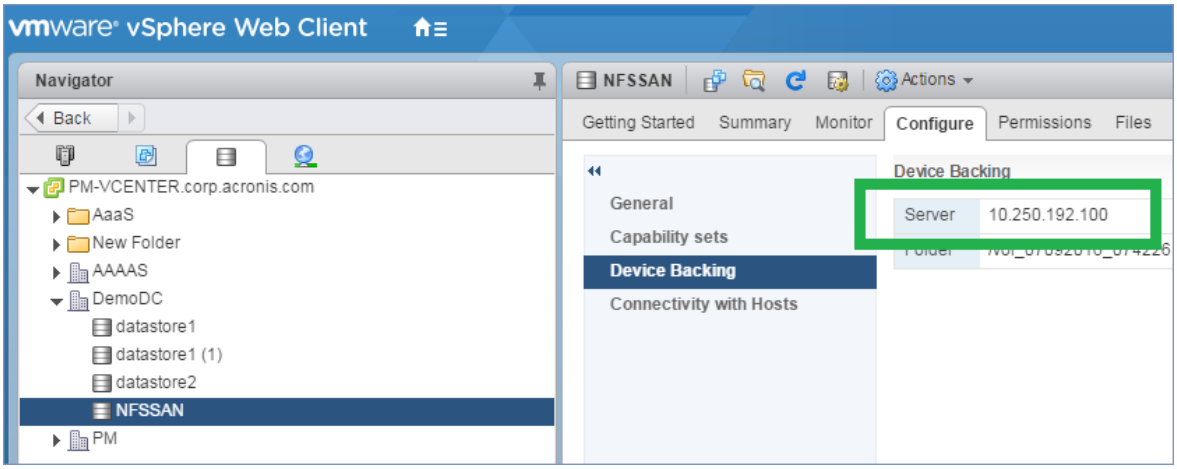
次のすべてに当てはまることを確認します。

- **NFS用Microsoftサービス**（Windows Server 2008の場合）または**NFSクライアント**（Windows Server 2012以降の場合）がインストールされている。

- NFSクライアントが匿名アクセス用に設定されている。この操作は、次の手順で実行できます。
  a. レジストリ エディタを開きます。
  b. 次のレジストリキーを見つけます。**HKEY_LOCAL_MACHINE¥SOFTWARE¥Microsoft¥ClientForNFS¥CurrentVersion¥Default**
  c. このキーで、**AnonymousUID**という名前の新しい**DWORD**値を作成し、その値データを0に設定します。
  d. 同じキーで、**AnonymousGID**という名前の新しい**DWORD**値を作成し、その値データを0に設定します。
  e. コンピュータを再起動します。

Management ServerへのSANストレージの登録

1. **[設定]** > **[SANストレージ]** をクリックします。
2. **[ストレージの追加]** をクリックします。
3. （オプション）**[名前]** でストレージ名を変更します。
   この名前は **[SANストレージ]** タブに表示されます。
4. **[ホスト名またはIPアドレス]** に、データストア作成時に指定したNetAppストレージ仮想コンピュータ（SVMまたはファイラー）を指定します。
   VMware vSphere Web Clientで必要な情報を確認するには、データストアを選択し、**[設定]** > **[デバイスバッキング]** をクリックします。ホスト名またはIPアドレスは **[サーバー]** フィールドに表示されます。



5. **[ユーザー名]** および **[パスワード]** にSVM管理者の資格情報を指定します。

重要
指定するアカウントは、NetAppシステム全体の管理者ではなく、SVMのローカル管理者である必要があります。

既存のユーザーを指定することも、新しいユーザーを作成するもできます。新しいユーザーを作成するには、NetApp OnCommand System Managerで **[構成]** > **[セキュリティ]** > **[ユーザー]** に移動し、新しいユーザーを作成します。

6. このSANデバイスの読み取り権限が付与される1つ以上のエージェントfor VMware（Windows）を選択します。
7. **[追加]** をクリックします。

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:¥**）。

仮想コンピュータのバインド

このセクションでは、Management Server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、自動的にエージェントfor VMware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、Management Serverは同じアルゴリズムを使用してコンピュータを再配分します。

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。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Management Serverから削除すると、エージェントに割り当てられたコンピュータ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

[エージェントfor VMware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

エージェントfor VMware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エージェントfor VMware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）コンピュータはエージェントfor VMware（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。
- SANハードウェアスナップショットを使用している場合は、手動バインドが必要です。SANデータストア上に存在するコンピータでSANハードウェアスナップショットが構成されているエージェントfor VMware（Windows）をバインドしてください。
- 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。

VM 移行のサポート

このセクションでは、vSphere クラスターの一部である ESXi ホスト間の移行を含む、vSphere 環境内での仮想マシンの移行時に期待されることについて説明します。

vMotion

vMotion では、仮想コンピュータの状態と構成が別のホストに移動されますが、仮想コンピュータのディスクは共有ストレージの同じ場所に残ります。

- エージェント for VMware（仮想アプライアンス）の vMotion はサポートされておらず、無効になります。
- 仮想コンピュータの vMotion はバックアップ時に無効になります。バックアップは移行の完了後も継続して実行されます。

Storage vMotion

Storage vMotion では、データ ストア間で仮想コンピュータのディスクが移動されます。

- エージェント for VMware（仮想アプライアンス）の Storage vMotion はサポートされておらず、無効になります。
- 仮想コンピュータの Storage vMotion はバックアップ時に無効になります。バックアップは移行後も継続して実行されます。

仮想環境の管理

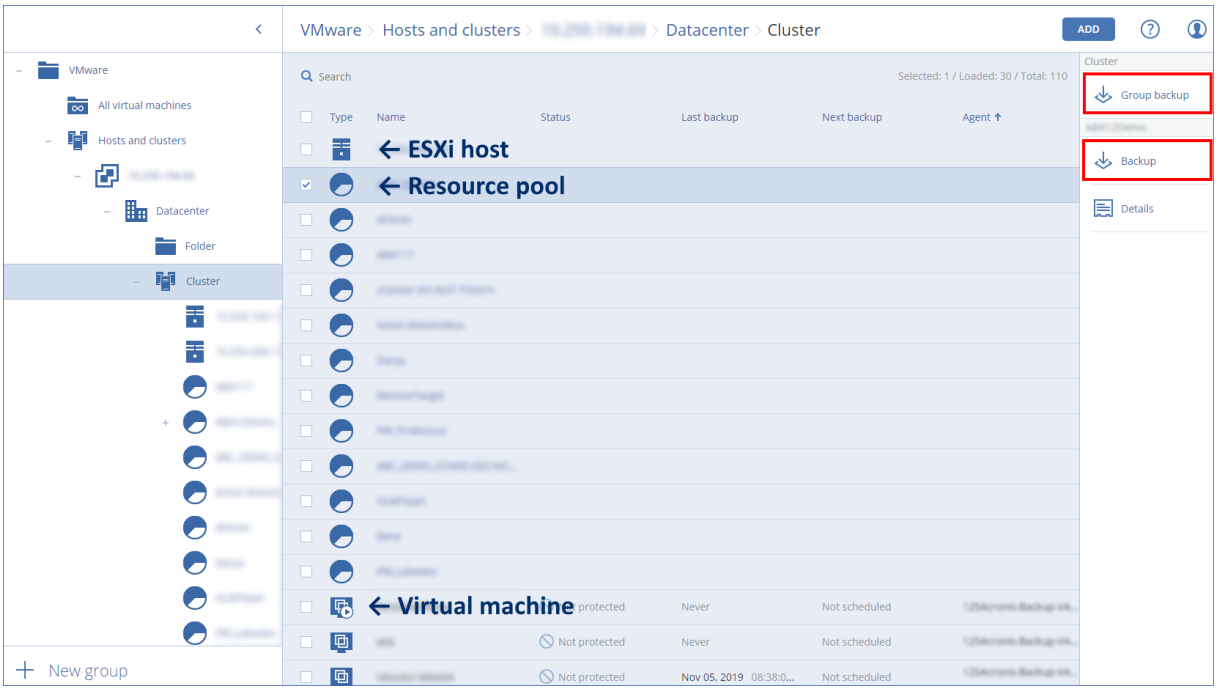
ネイティブ表示でvSphere、Hyper-V、Virtuozzo環境を表示できます。対応するエージェントがインストールおよび登録されると、**[デバイス]** の下に **[VMware]**、**[Hyper-V]**、または **[Virtuozzo]** の各タブが表示されます。

[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、**[バックアップ]** 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、**[グループのバックアップ]** をクリックします。

例えば、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。**[バックアップ]** 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。**[グループのバックアップ]** をクリックすると、選択した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。



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、エージェントfor VMware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 សុ តេ ឥតា សុ សុ តេ 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

このセクションでは、ESXi仮想コンピュータでの処理と仮想アプライアンスの配置に必要な権限について説明します。

注意
仮想マシンのバックアップを有効にするには、vStorage APIをESXiホストにインストールする必要があります。https://kb.acronis.com/content/14931を参照してください。

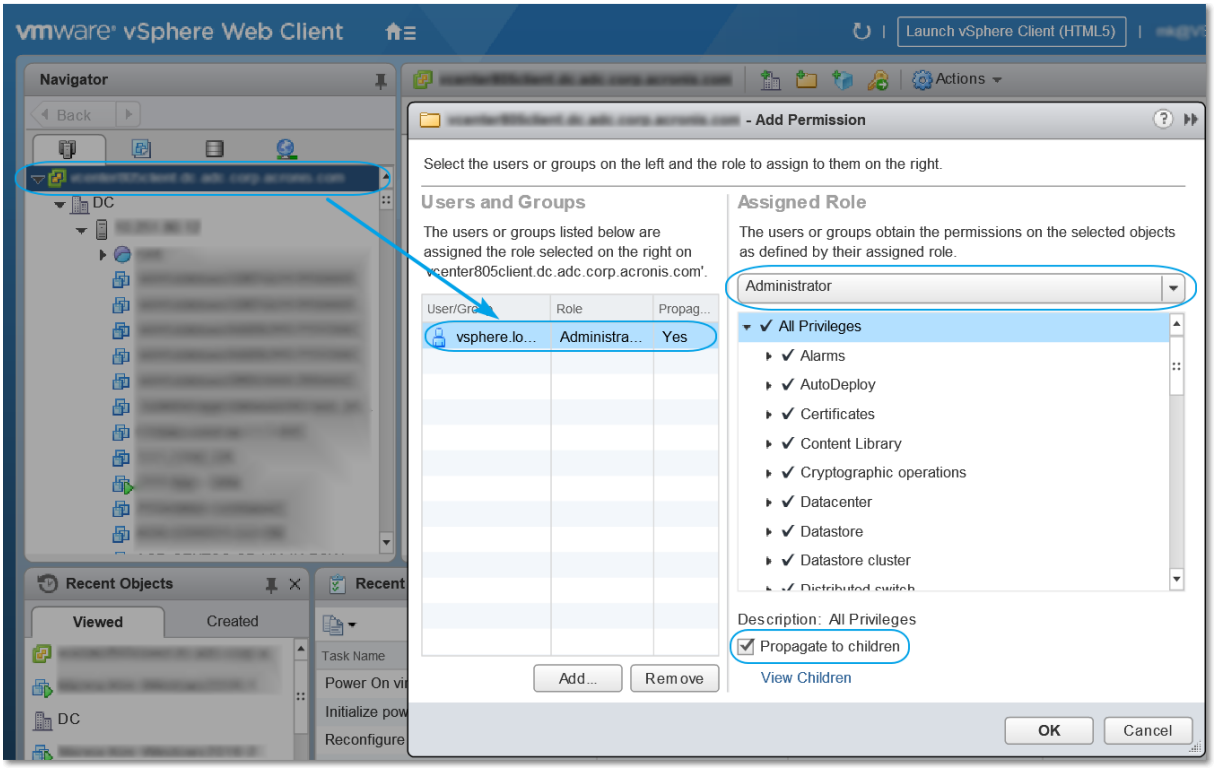
vCenterオブジェクト（仮想マシン、ESXiホスト、クラスター、vCenterなど）で操作を実行する場合は、VMwareエージェントが、ユーザーが指定したvSphere資格情報に基づいてvCenterやESXiホストで認証を行います。VMwareエージェントからvSphereへの接続で使用するvSphereアカウントは、vSphereインフラストラクチャのvCenterレベルから始まるあらゆるレベルで必要な権限を持っていなければなりません。

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。後でアカウントの変更が必要になった場合は、「仮想環境環境の管理」セクション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、以下の手順を実行します。

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	VA の配置
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	VM 自動起動構成					+
	ストレージパーティションの構成				+	
ホスト > インベントリ	クラスタの変更					+
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		+	+	+	+
	インポート					+
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		+	+		
	コンソールとの相互作用					+
	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		+	+	+	+
	移動					+
	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	**スナップショットの作成**	+		+	+	+

[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。
   エージェント for Hyper-V 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. エージェント for Hyper-V をクラスタの各ノードにインストールします。
3. 管理サーバーにすべてのエージェントを登録します。

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。

バックアップ済みのディスクを新しい Hyper-V 仮想マシンに復元する場合、または Hyper-V 仮想マシンの変換を保護計画内で実行する場合、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、指定された保護計画の実行時にエージェントが同時にバックアップを実行できる仮想マシンの数を定義します。

複数の保護計画の時間が重複する場合、保護計画のバックアップオプションで指定された数が合計されます。結果として得られる合計数がプログラムで10に制限されていても、計画の重複はバックアップの作成速度に影響を及ぼし、ホストと仮想マシンのストレージの両方に過剰な負荷をかけます。

VMwareエージェントまたはHyper-Vエージェントで同時にバックアップできる仮想マシンの合計数をさらに削減できます。

VMwareエージェント（Windows）またはHyper-Vエージェントでバックアップできる仮想マシンの合計数を制限するには

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、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\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. 次の手順でエージェントを再起動します。
   a. **[スタート]** メニューで、**[ファイル名を指定して実行]** をクリックし、「**cmd**」と入力します。
   b. **[OK]** をクリックします。
   c. 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）またはVMwareエージェント（Linux）でバックアップできる仮想マシンの合計数を制限するには

1. エージェントを実行しているマシンで、コマンドシェルを実行します。
   - **VMwareエージェント（仮想アプライアンス）:** 仮想アプライアンスUIで、CTRL+SHIFT+F2キーを押します。
   - **VMware エージェント（Linux）:**Acronis Cyber Protect アプライアンスを実行しているマシンにルートユーザーとしてログインします。パスワードは Cyber Protect ウェブ コンソールと同じです。
2. **vi**などのテキストエディタでファイル**/etc/Acronis/MMS.config**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`は設定する制限の10進値で置換します。
5. ファイルを保存します。
6. エージェントを再起動します。

- **VMware エージェント（仮想アプライアンス）:** reboot コマンドを実行します。
- **VMware（Linux）エージェント:** 次のコマンドを実行します。

```
sudo service acronis_mms restart
```

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仮想マシン*	Virtuozzoコンテナ*	Virtuozzo Hybrid Infrastructure仮想マシン*	Scale Computing HC3仮想マシン	RHV/oVirt仮想マシン*
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仮想マシン*	+	+	+	+	-	+	+	+
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*	+	+	+	-	-	+	+	+

*クラウド配置でのみ利用可能。

移行の実行手順については、次のセクションを参照してください。

- 物理環境から仮想環境（P2V） - "物理マシンを仮想マシンにリカバリする"（309ページ）
- 仮想環境間（V2V） - "仮想コンピュータの復元"（311ページ）
- 仮想環境から物理環境（V2P） - "仮想コンピュータの復元"（311ページ）または"ブータブルメディアを使用したディスクとボリュームの復元"（314ページ）

V2P移行はWebインターフェイスで実行しますが、特定の場合にはブータブルメディアを使用することをお勧めします。場合によっては、ESXiまたはHyper-Vへの移行でメディアを使用できます。

メディアでは次のことができます。

- 論理ボリューム（LVM）を含むLinuxマシンのP2VおよびV2P移行を実行します。バックアップおよびリカバリ用ブータブルメディアの作成には、Linuxエージェントまたはブータブルメディアを使用します。
- 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ブを提供します。

Windows AzureおよびAmazon EC2仮想コンピュータ

Windows AzureまたはAmazon EC2仮想マシンをバックアップするには、マシンに保護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、クラウドの配置で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。

物理コンピュータとの違いは、Windows AzureおよびAmazon EC2仮想コンピュータは、ブータブルメディアから起動できないことです。新しいWindows AzureまたはAmazon EC2仮想コンピュータに復元する必要がある場合は、次の手順に従います。

Windows AzureまたはAmazon EC2仮想コンピュータとしてコンピュータを復元する手順

1. Windows AzureまたはAmazon EC2のイメージ/テンプレートから、新しい仮想コンピュータを作成します。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。

ネットワーク要件

バックアップされたコンピュータにインストールされたエージェントは、ネットワーク上でManagement Serverと通信できる必要があります。

オンプレミスデプロイ

- エージェントとManagement Serverの両方がAzure/EC2クラウドにインストールされている場合、すべてのコンピュータが同じネットワークにあります。追加の操作は不要です。
- Management ServerがAzure/EC2クラウド外にある場合、クラウドのコンピュータはManagement Serverがインストールされているローカルネットワークへのネットワークアクセスがありません。こ

のようなコンピュータにインストールされたエージェントがManagement Serverと通信できるようにするには、ローカル（オンプレミス）とクラウド（Azure/EC2）ネットワーク間の仮想プライベートネットワーク（VPN）接続を作成する必要があります。VPN接続を作成する手順については、次の記事を参照してください。

Amazon EC2: http://docs.aws.amazon.com/ja_jp/AmazonVPC/latest/UserGuide/VPC_VPN.html

Windows Azure: https://docs.microsoft.com/ja-jp/azure/vpn-gateway/vpn-gateway-howto-site-to-site-resource-manager-portal

クラウドデプロイ

クラウド配置の場合、管理サーバーはいずれかのAcronisデータセンターにあり、エージェントからアクセスできます。追加の操作は不要です。

SAP HANA の保護

SAP HANAの保護については、https://dl.managed-protection.com/u/pdf/AcronisCyberProtect_15_SAP_HANA_whitepaper_en-US.pdfで入手できる個別の文書に記載されています。

マルウェア対策とWeb保護

Cyber Protect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Windows Defender Antivirusを管理できます。

ウイルスおよびマルウェア対策保護

ウイルスおよびマルウェア対策保護モジュールを使用すると、最近のマルウェアに関するあらゆる脅威からWindowsマシンやmacOSマシンを保護できます。ただし、マルウェア対策保護の一部であるActive Protection機能は、macOSマシンではサポートされていません。サポート対象のマルウェア対策機能の一覧を参照してください。オペレーティングシステムがサポートする機能。

Acronis Cyber Protect は、Windows Security Center でサポートされており、そこに登録されます。

ウイルスおよびマルウェア対策保護モジュールをマシンに適用する時点ですでにサードパーティのウイルス対策ソリューション機能でマシンが保護されていた場合は、互換性やパフォーマンスの問題を回避するために、アラートが生成され、そのリアルタイム保護機能が停止します。Acronis Cyber Protect ウイルスおよびマルウェア対策保護の全機能を有効にするために、サードパーティのウイルス対策機能を無効にするか、アンインストールする必要があります。

以下のマルウェア対策機能を利用できます。

- 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する機能（Windows、macOS）
- 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）
- 危険なファイルを隔離に移動する
- 社内の信頼できるアプリケーションをホワイトリストに追加する機能

ウイルスおよびマルウェア対策保護のモジュールでは、2種類のスキャンが可能です。

- リアルタイム保護スキャン
- オンデマンドマルウェアスキャン

リアルタイム保護スキャン

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、マシンで実行されたり開かれたりするすべてのファイルをチェックします。

以下のタイプのスキャンのいずれかを選択できます。

- 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。

オンデマンドマルウェアスキャン

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。

[ダッシュボード] > **[概要]** > [最近影響を受けたもの] ウィジェットで、マルウェア対策スキャンの結果を監視できます。

ウイルスおよびマルウェア対策保護の設定

ウイルスおよびマルウェア対策保護モジュールによる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。

ウイルスおよびマルウェア対策保護モジュールでは、以下の設定を指定できます。

Active Protection

Active Protectionは、システムをランサムウェアと暗号通貨採掘マルウェアから保護します。ランサムウェアは、ファイルを暗号化し、暗号化キーのための身代金（ランサム）を要求します。暗号通貨採掘マルウェアはバックグラウンドで数学的計算を実行し、それにより処理能力とネットワークトラフィックを盗みます。

Acronis Cyber ProtectのCyber Backup 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。Acronis Cyber Protect の Protect エディションの場合、Active Protection は、ウイルス対策およびマルウェア対策保護モジュールの一部となります。

Active Protectionは、以下のオペレーティングシステムを実行しているマシンで使用できます。

- デスクトップオペレーティングシステム:Windows 7 Service Pack 1以降
  Windows 7を実行しているマシンでは、Windows 7用の更新プログラム（KB2533623）がインストールされていることを確認してください。
- サーバーオペレーティングシステム:Windows Server 2008 R2以降。

コンピュータには、エージェントfor Windowsがインストールされている必要があります。

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、追加のアクションが構成で指定されている場合はそれら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。

既定の設定:**有効**。

Active Protectionの設定

[検出時のアクション] で、ランサムウェアのアクティビティを検出したときに実行されるアクションを選択し、**[完了]** をクリックします。

次のいずれかを選択できます。

- **通知のみ**
  プロセスに関するアラートを生成します。
- **[プロセスの停止]**
  アラートを生成し、プロセスを停止します。
- **[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**

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] オプションでは、ウイルスおよびマルウェア対策保護によって、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。

このオプションは、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、このオプション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、**C:¥ProgramData¥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:**有効**。

サーバー側保護機能

このオプションでは、ウイルスおよびマルウェア対策保護が、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からの外部受信接続から、共有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。

既定の設定:**無効**。

信頼できる接続とブロックされた接続を設定する

[信頼できる] タブで、データ変更を許可する接続を指定します。ユーザー名とIPアドレスを定義する必要があります。

[ブロック] タブで、データ変更を許可しない接続を指定します。ユーザー名とIPアドレスを定義する必要があります。

自己防御機能

自己防御機能は、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設定ファイル、Secure Zone、ローカルフォルダ内のバックアップへの不正な変更を防止します。この機能は無効にしないことをお勧めします。

既定の設定:**有効**。

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] オプションは、**自己防御機能**が有効になっているときに有効です。

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。

このオプションでは、バックアップファイルが自己保護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。

このオプション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。

このオプション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**。

クリプトマイニングプロセス検出

このオプションは、ウイルスおよびマルウェア対策保護が、潜在的なクリプトマイニングマルウェアを検出するかどうかを定義します。

暗号通貨採掘マルウェアは、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。その実行を防ぐために、クリプトマイニングマルウェアを **[有害なプロセス]** リストに追加することをお勧めします。

既定の設定:**有効**。

クリプトマイニングプロセス検出設定

クリプトマイニングのアクティビティを検出したときに実行されるアクションを選択し、**[完了]** をクリックします。次のいずれかを選択できます。

- **通知のみ**
  クリプトマイニングの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ます。
- **[プロセスの停止]**
  クリプトマイニングの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、プロセスが停止します。

既定の設定:**[プロセスの停止]**

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して保持するためのフォルダです。

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日数を定義します。

既定の設定:**30日**

振る舞い検知

Acronis Cyber Protectは、振る舞い検知を使用してお使いのシステムを保護します。悪意のあるプロセスを特定するため、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アクションを比較します。つまり、典型的な振る舞いによって新しいマルウェアが検出されます。

既定の設定:**有効**。

振る舞い検知設定

[検出時のアクション] で、マルウェアのアクティビティを検出したときに実行されるアクションを選択し、**[完了]** をクリックします。

次のいずれかを選択できます。

- **通知のみ**
  マルウェアの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ます。
- **[プロセスの停止]**
  マルウェアの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、プロセスが停止します。
- **検疫**
  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。

既定の設定:**検疫**

リアルタイム保護

リアルタイム保護では、システムの電源がオンになっている間、マシンシステムにウイルスや他の脅威がないかどうかを常時チェックします。

既定の設定:**有効**。

リアルタイム保護の検出時のアクションを設定する

[検出時のアクション] 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、**[完了]** をクリックします。

次のいずれかを選択できます。

- **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**
  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。

既定の設定:**検疫**

リアルタイム保護のスキャンモードを設定する

[スキャンモード] 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、**[完了]** をクリックします。

次のいずれかを選択できます。

- **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可能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。

既定の設定:**スマートオンアクセス**

スケジュールスキャン

スケジュールスキャンの設定を有効にして、マシンでマルウェアのチェックを行うスケジュールを定義できます。

検出時のアクション:

- **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。

既定の設定:**検疫**

スキャンの種類:

- **完全**
  フルスキャンは、すべてのファイルをチェックするのでクリックスキャンよりもかなり時間がかかります。
- **クイック**
  クイックスキャンでは、マシンの中でマルウェアが存在しそうな場所だけをスキャンします。
- **カスタム**
  カスタムスキャンでは、管理者が保護計画で選択したファイル/フォルダがチェックされます。

1つの保護計画で、3種類のスキャン処理（**クイック**、**完全**、**カスタム**スキャン）のスケジュールを設定できます。

デフォルトの設定:

- **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。
- **カスタム**スキャンはデフォルトで無効化されています。

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。

- **時刻でスケジュール** - 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。

既定の設定:**時刻でスケジュール**

スケジュールの種類:

- **月次** - 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します。
- **日次** - タスクを実行する週中の日を選択しします。
- **毎時** - 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。

既定の設定:**日単位**

開始時間 - 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 - 設定したスケジュールが有効な日付範囲を指定します。

開始条件 - すべての条件を定義して、どの条件が同時に満たされたときにタスクを実行するか指定します。

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"（235ページ）」に説明されています。 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。

新しいファイルと変更されたファイルだけをスキャン - 新しく作成されたファイルと変更されたファイルだけをスキャンします。

既定の設定:**有効**。

フルスキャンをスケジューリングする場合、2つの追加オプションを利用できます。

- **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**
    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。
    既定の設定:**16**
  - **最大サイズ**
    スキャンするアーカイブファイルの最大サイズ。
    既定の設定:**無制限**
- **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スストレージデバイス**（フラッシュドライブや外部ハードドライブなど）
  - **CD/DVD**

除外

ヒューリスティック分析によって使用されるリソースを最小限にするために、また、いわゆる誤検知（信頼されているプログラムがランサムウェアと見なされてしまうこと）をなくすために、次の設定を定義することができます。

[信頼できる] タブで、以下の指定ができます。

- マルウェアとは絶対に見なされないプロセス。Microsoftが署名したプロセスは常に信頼されます。
- ファイル変更を監視しないフォルダ。
- スケジュールに基づくスキャンを実行しないファイルとフォルダ。

[ブロック] タブで、以下の指定ができます。

- 常にブロックするプロセス。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。
- すべてのプロセスをブロックするフォルダ。

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`。

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 0 個以上の文字の代用として使用します。疑問符（?）は厳密に 1 文字として代用されます。`%AppData%` などの環境変数は使用できません。

既定の設定:デフォルトでは除外は定義されていません。

URLフィルタ処理

詳細な説明については URL フィルタリングを参照してください。

Active Protection

Acronis Cyber Protect の Cyber Backup Edition の場合、Active Protection は保護計画の個別のモジュールです。このモジュールには、以下の設定があります。

- 検出時のアクション
- 自己防御
- 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

Acronis Cyber Protect の Protect エディションの場合、Active Protection は、ウイルス対策およびマルウェア対策保護モジュールの一部となります。

Active Protectionは、以下のオペレーティングシステムを実行しているマシンで使用できます。

- デスクトップオペレーティングシステム:Windows 7 Service Pack 1以降
  Windows 7を実行しているマシンでは、Windows 7用の更新プログラム（KB2533623）がインストールされていることを確認してください。
- サーバーオペレーティングシステム:Windows Server 2008 R2以降。

コンピュータには、エージェントfor Windowsがインストールされている必要があります。

Active Protectionとその設定の詳細については、「"ウイルスおよびマルウェア対策保護の設定"（504 ページ）」を参照してください。

Windows Defender Antivirus

Windows Defender Antivirus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から導入されました。

Windows Defender Antivirusモジュールを使用すれば、Windows Defender Antivirusのセキュリティポリシーを設定して、Cyber Protectウェブ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、Windows Defender Antivirusがインストールされているマシンです。

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。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。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

Windows Defender Antivirus スケジュール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** - マシン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マシンから削除します。
- **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。

  Windows 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、マルウェアがマシン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。

Windows 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 Windows Defender Antivirus ユーザーインターフェースを利用できなくなります。Cyber Protectウェブコンソールで Windows Defender Antivirus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

Windows Defender Antivirus の詳細設定については、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。

Windows 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。

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 ウェブ 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マシンです。

Microsoft Security Essentials の設定は、Microsoft Windows Defender Antivirus の設定とほとんど同じですが、リアルタイム保護の設定がなく、Cyber Protect ウェブ コンソールから除外を定義できません。

URLフィルタリング

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 フィルタリングを使用すれば、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 サイトへのアクセスをブロックすることができます。

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。41 個以上の Web サイトカテゴリに対して、異なるアクセスポリシーを構成できます。

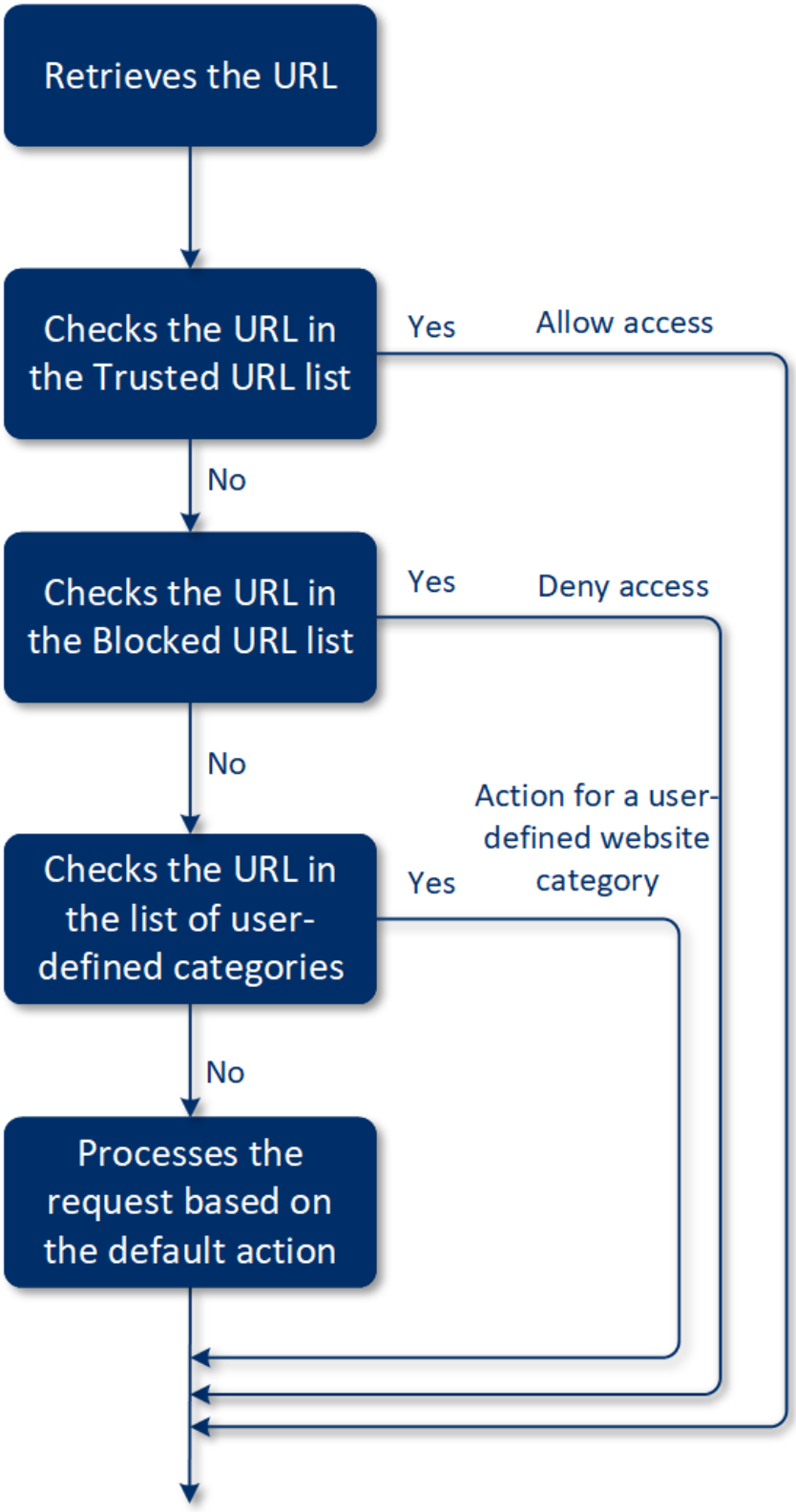
現時点では、Windows マシンの HTTP/HTTPS 接続がプロテクション エージェントトによってチェックされます。

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
URL フィルタリング機能が有効なサードパーティ製のウイルス対策ソリューションと同時に、URL フィルタリングを使用した場合、競合が発生する可能性があります。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。
互換性またはパフォーマンスの問題が発生した場合は、サードパーティ製ソリューションをアンインストールするか、保護計画の URL フィルタリングモジュールを無効にしてください

仕組み

ユーザーはリンクに従うか、ブラウザのアドレスバーに URL を入力します。インターセプターが URL を取得してプロテクション エージェントに送信します。プロテクション エージェントは URL を解析し、データベースを確認してから、判定をインターセプターに返します。URL が禁止されている場合、インターセプターは URL へのアクセスをブロックし、このコンテンツの表示が許可されていないことをユーザーに通知します。



URL フィルタリングを構成する

1. URL フィルタリング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構成します（下記参照）。
3. 任意の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、**[ダッシュボード]** > **[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、以下の設定を構成できます。

悪意あるWebサイトへのアクセス

ユーザーが有害な Web サイトを開こうとしたときのアクションを指定します。

- **ブロック**– 悪意のある Web サイトへのアクセスがブロックされ、アラートが生成されます。
- **常にユーザーに確認** – ユーザーは Web サイトに進むか戻るかを選択する必要があります。

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ポリシーを次のように設定できます。デフォルトでは、すべてのカテゴリの Web サイトへのアクセスが許可されます。

	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	**ギャンブル**	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**	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

	アおよびフィットネス	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	**違法なダウンロード**	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。 • 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、カーマスー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。

[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] チェックボックスをオンにすると、カテゴリでブロックされた URL の通知がトレイに表示されます。Web サイトに複数のサブドメインが存在する場合、それらに対する通知も生成されるので、通知が膨大な量になる可能性があります。

除外

安全だと分かっている URL は、信頼できる URL のリストに追加できます。脅威になる URL は、ブロックする URL のリストに追加できます。

URL をリストに追加する

1. 保護計画の URL フィルタリングモジュールで、**[除外]** をクリックします。
2. 任意のリストを選択します。**信頼**または**ブロック**
3. **[追加]** をクリックします。
4. URL または IP アドレスを指定し、チェックマークをクリックします。

URL除外の例:

- xyz.comを信頼済み/非信頼済みとして追加すると、追加した場所に応じて、xyz.comドメイン内のすべてのアドレスが信頼済み/非信頼済みとして扱われます。
- 特定のサブドメインを追加したい場合、例えば**mail.xyz.com**を信頼済み/非信頼済みとして追加すれば、すべての**xyz.com**アドレスが信頼済み/非信頼済みとなることはありません。
- IPv4を信頼済み/非信頼済みとして追加する場合、以下の形式にする必要があります。**20.53.203.50**。
- 同時に複数のURL除外を追加する場合は、必ず各項目を改行してしてください:

  acronis.com

  mail.xyz.com

  20.53.203.50

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、**[マルウェアからの保護]** > **[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** - 検疫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。
- **復元** - 検疫されたファイルを変更しないでそのまま元のロケーションに戻します。元のロケーションに同じ名前のファイルが存在する場合は、復元するファイルによって上書きされます。

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%\%product_name%\Quarantine`

Mac/Linuxマシンの場合: `/usr/local/share/%product_name%/quarantine`

企業ホワイトリスト

重要
社内向けホワイトリストでは、スキャンサービスが管理サーバーにインストールされている必要があります。

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。

Cyber Protect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、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。

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の計画"（344ページ）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ウェブコンソールで、**[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ウェブコンソールで、**[マルウェア対策保護]** > **[隔離]** 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**
  企業アプリケーションがホワイトリストに追加され、偽陽性の検出確率を低減します。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

バックアップから感染ファイルを復元することを防ぐため、バックアップのマルウェアスキャンを実行できます。バックアップスキャンはWindowsオペレーティングシステムでのみサポートされます。これは、Cyber Protect管理サーバーにスキャンサービスがインストールされている場合にのみ使用できます。

バックアップのマルウェア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。

注意
セキュリティとパフォーマンス上の理由から、スキャンには専用のマシンを使用することをお勧めします。このマシンにより、スキャンされるすべてのバックアップにアクセスできます。

スキャンの結果は、ダッシュボードの「バックアップスキャンの詳細」ウィジェットで確認できます。また、**[バックアップストレージ]** > **[ロケーション]**> **[<バックアップ名>]** でバックアップステータスを確認することもできます。バックアップスキャンが実行されていない場合は、バックアップが **[スキャンされていません]** のステータスになります。バックアップスキャンが実行されると、バックアップのステータスは次のいずれかに更新されます。

- **マルウェアはありません**
- **マルウェアが検出されました**

制限事項

- マルウェアのスキャンに対応しているのは、[**マシン全体**] か [**ディスク/ボリューム**] のバックアップタイプのみです。
- GPTおよび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だけがスキャンの対象になります。
- サポートされているバックアップロケーション:**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**。
- 継続的データ保護（CDP）復元ポイントがあるバックアップもスキャン対象として選択できますが、これらの復元ポイントはスキャン対象から除外されます。通常の復元ポイントのみがスキャンされます。
- マシン全体の安全な復元のためにCDPバックアップを選択した場合は、CDP復元ポイントのデータなしでマシンが安全に復元されます。CDPデータを復元する場合は、**ファイル/フォルダ**の復元を実行します。

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、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 Protectによりコラボレーション用のツールを保護することができます。

Zoom、Cisco Webex Meetings、Microsoft Teamsの保護設定は似ています。次の例では、Zoomの構成を検討します。

Zoom保護を設定する

1. コラボレーション用の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ウェブ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

脆弱性診断とパッチ管理

脆弱性診断（VA）とは、システムの脆弱性を検出し、数値化して優先順位を付けるプロセスのことです。保護計画の脆弱性診断モジュールを使用することで、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実行する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"（528ページ）を参照してください。
- Linux（CentOS 7/Virtuozzo/Acronis Cyber Infrastructure）の各マシン。詳細については、"サポートされているLinux製品"（530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を実行する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"（528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. 脆弱性評価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、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. その情報を利用して、どの脆弱性を解決する必要があるかを決定できます。

[ダッシュボード] > **[概要]** > **脆弱性/既存の脆弱性**のウィジェットで、脆弱性評価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でサポートされています。

サポート対象のMicrosoft製品

デスクトップオペレーティングシステム

- Windows 7（Enterprise、Professional、Ultimate）
- Windows 8
- Windows 8.1
- Windows 10

サーバー オペレーティング システム

- 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 Sharepoint Server 2016
- Microsoft Sharepoint Server 2016

Windowsでサポートされているサードパーティ製品

Cyber Protectは、リモート作業の利用事例で非常に重要であるコラボレーションツールやVPNクライアントなど、幅広いサードパーティアプリの脆弱性評価とパッチ適用をサポートします。

Windowsがサポートするサードパーティ製品のリストの完全版については、
https://kb.acronis.com/content/62853を参照してください。

サポートされているLinux製品

脆弱性診断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 7.0.11
- Virtuozzo 7.0.10（320）
- Virtuozzo 7.0.9（539）
- Virtuozzo 7.0.8（524）
- CentOS 7.x
- Acronis Cyber Infrastructure 3.x
- Acronisストレージ2.4.0
- Acronisストレージ2.2.0

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"（199ページ）」を参照してください。脆弱性診断のスキャンは、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のサポート対象のサードパーティ製品の詳細については、
    https://kb.acronis.com/content/62853を参照してください）。
- 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評価スキャンを実行するスケジュールを定義します。

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。

- **時刻でスケジュール** - 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。

既定の設定:**時刻でスケジュール**

スケジュールの種類:

- **月次** - 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します。
- **日次** - タスクを実行する週中の日を選択しします。
- **毎時** - 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。

既定の設定:**日単位**

開始時間 - 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 - 設定したスケジュールが有効な日付範囲を指定します。

開始条件 - すべての条件を定義して、どの条件が同時に満たされたときにタスクを実行するか指定します。

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"（235ページ）」に説明されています。 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。

1. Cyber Protectウェブコンソールで、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"（530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、**[ダッシュボード]** > **[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ウェブコンソールで、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"（530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、**[ダッシュボード]** > **[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、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、使用できる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 ウェブ 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. インストールするパッチを選択します**[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. 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。
   - **いいえ** - パッチ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。
   - **はい** - パッチのインストール後に常に再起動を開始します。ただし、遅延時間を指定できます。

   バックアップが完了するまで再起動しないでください - バックアッププロセスの実行中にマシンを再起動した場合は、バックアップが完了するまで再起動が延期されます。
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

パッチ管理機能を使用して、以下の操作を実行できます。

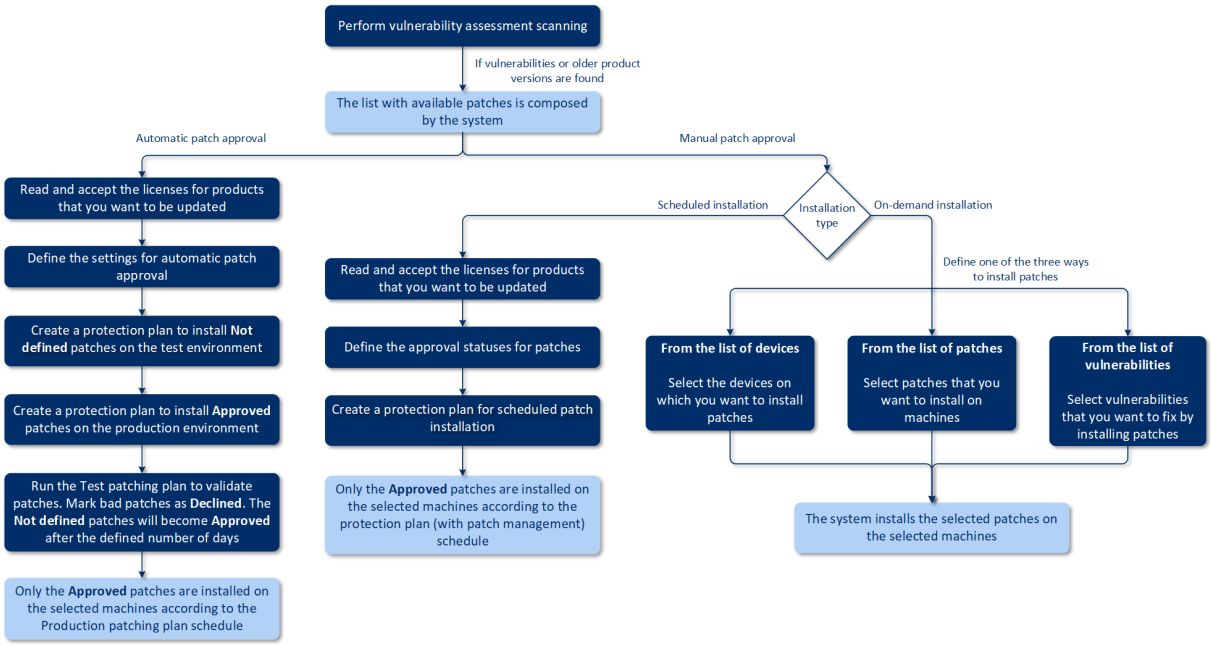
- OSレベルとアプリケーションレベルのアップデートをインストールする
- パッチを手動または自動で承認する

- 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、適用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に適用する再起動オプションを定義する

Cyber Protect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。

仕組み

自動または手動のパッチ承認を設定できます。下のスキームで、自動と手動の両方のパッチ承認ワークフローを確認できます。



1. まず、**脆弱性診断**のモジュールを有効にした保護計画を使用して、脆弱性診断スキャンを少なくとも1回実行する必要があります。スキャンを実行すると、検出された脆弱性と使用可能なパッチのリストがシステムによって作成されます。
2. その後、自動パッチ承認を設定するか、手動パッチ承認アプローチを使用できます。
3. パッチをインストールする方法（スケジュールモードまたはオンデマンドモード）を定義します。オンデマンドのパッチインストールは、設定に応じて以下の3つの方法で実行できます。
   - パッチのリスト（**[ソフトウェア管理]** > **[パッチ]**）に進み、必要なパッチをインストールします。
   - 脆弱性のリスト（**[ソフトウェア管理]** > **[脆弱性]**）に進み、パッチのインストールを含む修復プロセスを開始します。
   - デバイスのリスト（**[デバイス]** > **[すべてのデバイス]**）に進み、アップデート対象のマシンを選択し、そのマシンにパッチをインストールします。

[ダッシュボード] > **[概要]** > **パッチインストール履歴**のウィジェットで、パッチインストールの結果を監視できます。

パッチ管理の設定

パッチ管理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。保護計画を使用して、定義したマシンに自動的にインストールする Microsoft 製品や Windows OS 向け他のサードパーティ製品のアップデートを指定できます。

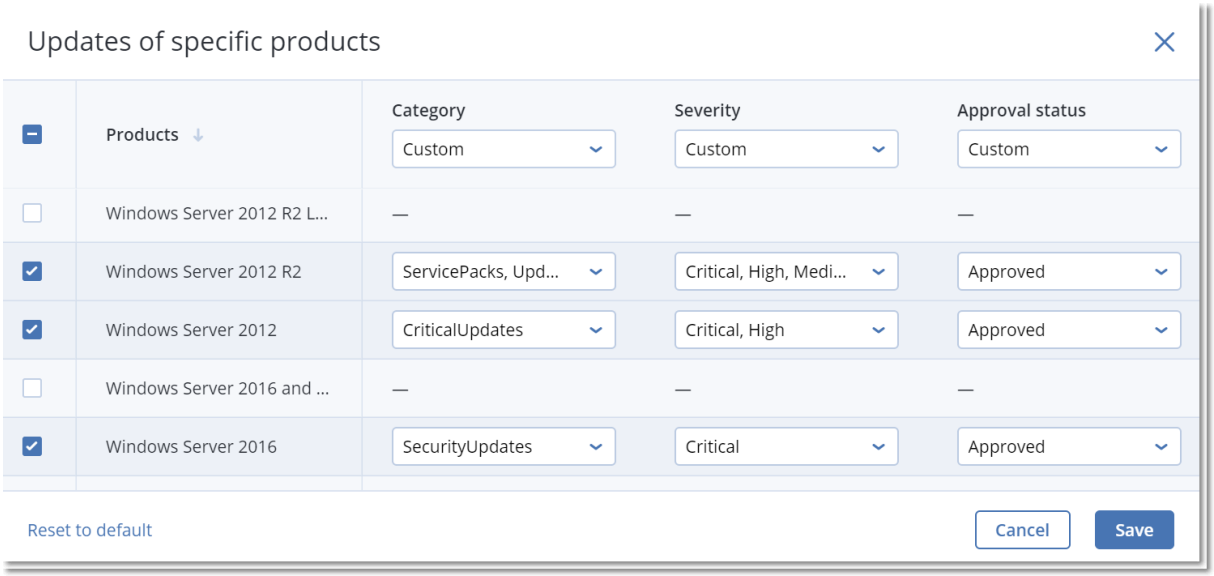
パッチ管理のモジュールでは、以下の設定を指定できます。

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。

インストールするアップデートを選択します。

- **すべてのアップデート**
- **セキュリティアップデートと重要なアップデートのみ**
- **[特定の製品のアップデート]**:製品ごとにカスタム設定を定義できます。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。



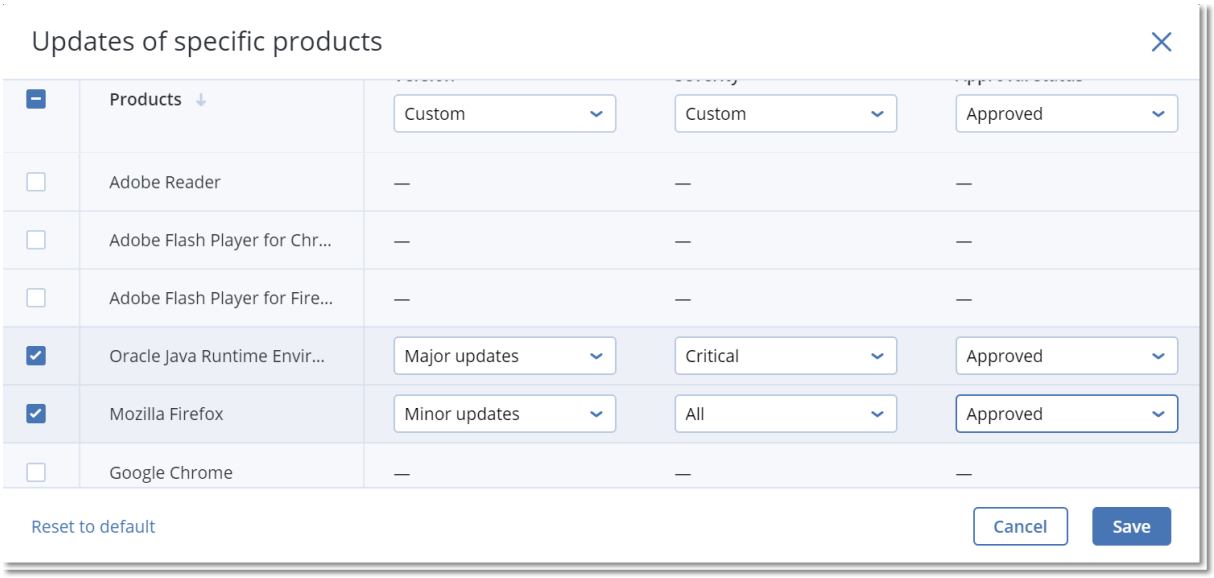
Windowsサードパーティ製品

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。

インストールするアップデートを選択します。

- **[メジャーアップデートのみ]** の場合は、有効な最新バージョンのアップデートをインストールします。

- **[マイナーアップデートのみ]** の場合は、マイナーバージョンのアップデートをインストールします。
- **[特定の製品のアップデート]**:製品ごとにカスタム設定を定義できます。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。



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を定義します。

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。

- **時刻でスケジュール** - 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。

既定の設定:**時刻でスケジュール**

スケジュールの種類:

- **月次** - 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します。
- **日次** - タスクを実行する週中の日を選択しします。
- **毎時** - 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。

既定の設定:**日単位**

開始時間 - 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 - 設定したスケジュールが有効な日付範囲を指定します。

開始条件 - すべての条件を定義して、どの条件が同時に満たされたときにタスクを実行するか指定します。

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"（235ページ）」に説明されています。 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。

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。これにより、パッチのインストールが失敗した場合に、元の状態にロールバックできます。**[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。

パッチのリストの管理

脆弱性診断が完了したら、**[ソフトウェア管理]** > **[パッチ]** で有効なパッチを確認できます。

名前	説明
名前	パッチの名前
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
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。
Microsoft KB	Microsoft 製品のパッチの場合は、KB の記事の ID が表示されます
リリース日	パッチがリリースされた日付
マシン	影響を受けたマシンの数

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。保護計画で、どのアップデートをインストールするかをステータスに基づいて定義できます。 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 • **未定義** - パッチのステータスが不明なので、確認が必要です
ライセンス契約	• よく読んだ上で同意 • 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
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

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。その仕組みを以下にまとめます。

仕組み

テスト環境と本番環境という2つの環境があるとします。テスト環境でパッチのインストールをテストし、何も問題がないことを確認します。テスト環境でパッチのインストールをテストしてから、本番環境で安全なパッチの自動インストールを実行できます。

自動パッチ承認の設定

自動パッチ承認を設定する手順

1. アップデートを計画している製品のベンダーごとに、ライセンス契約を読んで同意する必要があります。そうしないと、自動パッチインストールを実行できません。
2. 自動承認の設定を構成します。
3. **パッチ管理**のモジュールを有効にした保護計画を準備し（「テストパッチ」など）、テスト環境のマシンに適用します。パッチの承認ステータスが **[未定義]** 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。

4. **パッチ管理**のモジュールを有効にした保護計画を準備し（「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。
5. 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 **[未定義]** のままで構いませんが、正常に動作していないマシンのステータスは **[拒否済み]** に設定する必要があります。
6. **[自動承認]** オプションで設定した日数に応じて、**[未定義]** のパッチが **[承認済み]** になります。
7. 本番パッチの計画を起動すると、**[承認済み]** のパッチだけが本番マシンにインストールされます。

手動ステップを以下にまとめます。

ステップ1アップデートする製品のライセンス契約を読んで、同意する

1. Cyber Protect ウェブ コンソールで **[ソフトウェア管理]** > **[パッチ]** に進みます。
2. パッチを選択し、ライセンス契約を読んで同意します。

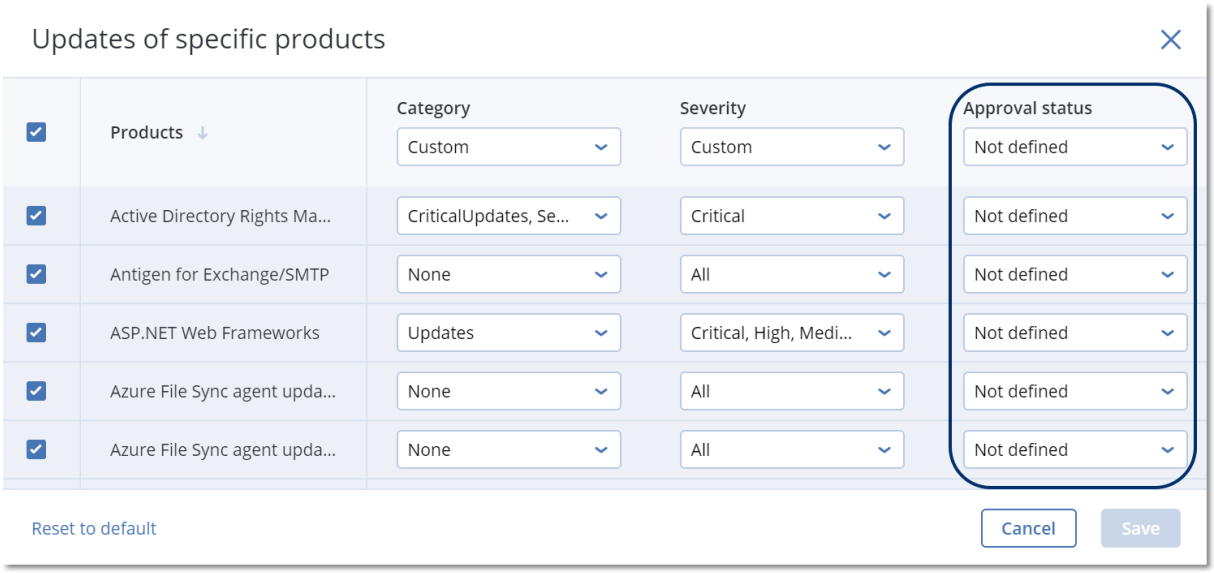
ステップ2自動承認の設定を構成する

1. Cyber Protect ウェブ 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. **[自動承認]** オプションを有効にして、日数を指定します。パッチインストールを最初に試みてから指定の日数が経過すると、**[未定義]** ステータスのパッチが **[承認済み]** に自動的に変わります。
   たとえば、10日を指定したとします。テストマシンでテストパッチの計画を実行し、パッチをインストールします。マシンに損傷を与えたパッチを **[拒否済み]** にし、その他のパッチは **[未定義]** のままにしておきます。10 日後、**[未定義]** ステータスのパッチが自動的に **[承認済み]** に切り替わります。
4. **[使用許諾契約の自動承認]** オプションを有効にします。そうすると、パッチのインストール時にライセンスへの同意が自動的に処理され、ユーザーによる確認が不要になります。

ステップ3テストパッチの保護計画を準備する

1. Cyber Protect ウェブ コンソールで **[計画]** > **[保護]** に進みます。
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. Microsoft製品とサードパーティ製品でどのアップデートをインストールするかを定義し、スケジュールやアップデート前のバックアップを設定します。これらの設定の詳細については、「パッチ管理の設定」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で **[承認ステータス]** を **[未定義]** に設定してください。アップデートの時刻になると、テスト環境で選択したマシンに **[未定義]** のパッチだけがインストールされます。



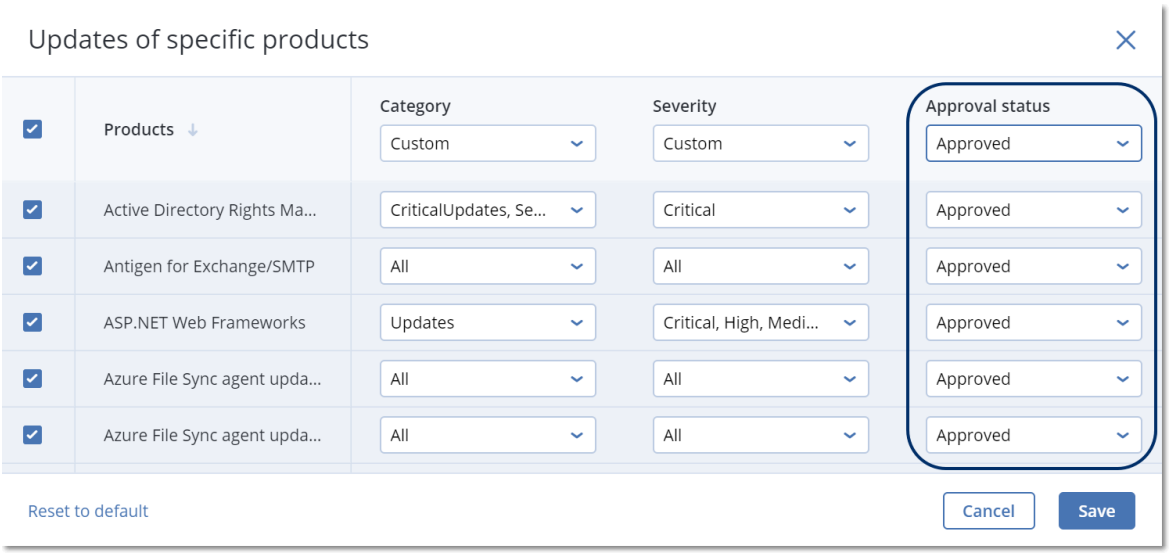
ステップ4本番パッチの保護計画を準備する

1. Cyber Protect ウェブ コンソールで **[計画]** > **[保護]** に進みます。
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. Microsoft製品とサードパーティ製品でどのアップデートをインストールするかを定義し、スケジュールやアップデート前のバックアップを設定します。これらの設定の詳細については、「パッチ管理の設定」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で **[承認ステータス]** を **[承認済み]** に設定してください。アップデートの時刻になると、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。

注意



ステップ5テストパッチの保護計画を実行して、結果を確認する

1. テストパッチの保護計画を実行します（スケジュールモードまたはオンデマンドモード）。
2. インストールしたパッチのうち、どれが安全で、どれが安全でないかを確認します。
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。

手動パッチ承認

手動パッチ承認のプロセスを以下にまとめます。

1. Cyber Protect ウェブ 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、ライセンス契約を読んで同意します。
3. インストールを承認するパッチの **[承認ステータス]** を **[承認済み]** に設定します。
4. パッチ管理のモジュールを有効にした保護計画を作成します。スケジュールを設定するか、オンデマンドで計画を起動します。オンデマンドの場合は、パッチ管理のモジュールの設定で **[今すぐ実行]** をクリックします。

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。

オンデマンドのパッチインストール

オンデマンドのパッチインストールは、設定に応じて以下の3つの方法で実行できます。

- パッチのリスト（**[ソフトウェア管理]** > **[パッチ]**）に進み、必要なパッチをインストールします。
- 脆弱性のリスト（**[ソフトウェア管理]** > **[脆弱性]**）に進み、パッチのインストールを含む修復プロセスを開始します。
- デバイスのリスト（**[デバイス]** > **[すべてのデバイス]**）に進み、アップデート対象のマシンを選択し、そのマシンにパッチをインストールします。

パッチのリストからパッチをインストールする方法を以下にまとめます。

1. Cyber Protectウェブコンソールで **[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. 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. パッチのインストール後に再起動を開始するかどうかを定義します。
   - **いいえ** - パッチの適用後に再起動を開始しません。
   - **必要な場合** - パッチを適用するために必要な場合に限って再起動します。
   - **常に** - パッチの適用後に常に再起動を開始します。後から再起動するように指定することも常に可能です。

   バックアップが完了するまで再起動しないでください - バックアッププロセスの実行中にマシンを再起動した場合は、バックアップが完了するまで再起動が延期されます。
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。

リスト内のパッチのライフタイム

パッチのリストをいつも最新の状態にしておくために、[**ソフトウェア管理**] > [**パッチ**] > [**設定**] に進み、[**リスト内のライフタイム**] オプションを指定します。

[**リスト内のライフタイム**] オプションでは、検出された有効なパッチをパッチリストに入れておく期間を定義します。通常は、パッチのないすべてのマシンにパッチがインストールされるか、定義済みの期間が経過すると、リストからパッチが削除されます。

- **永久** - パッチは常にリストに存在します。
- **7 日** - インストールの 7 日後にパッチが削除されます。
  たとえば、2つのマシンにパッチをインストールするとします。1つはオンラインで、もう1つはオフラインです。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** - インストールの 30 日後にパッチが削除されます。

スマート保護

脅威フィード

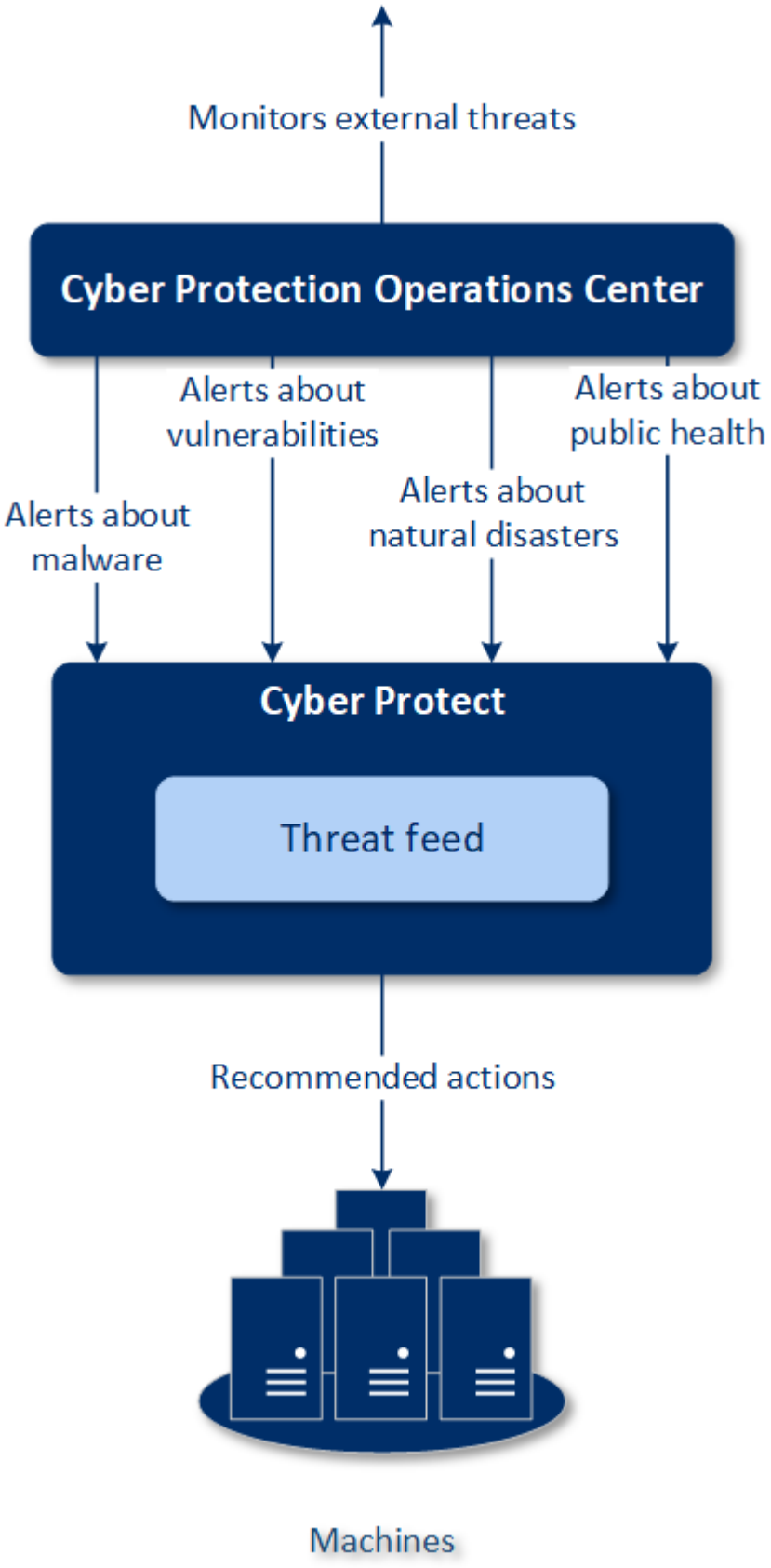
Acronisサイバープロテクションオペレーションセンター（CPOC）は、セキュリティアラートを生成して、関連する地域だけに送信します。セキュリティアラートによって、データ保護に影響を及ぼす世界規模のイベント（マルウェア、脆弱性、自然災害、公衆衛生など）に関する情報を確認できます。脅威フィードによって知らされるあらゆる潜在的な脅威についての情報を活用し、そうした脅威を回避することも可能になります。

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幾つかのアクションによって解決できます。今後の脅威について知らせるだけで推奨アクションのないアラートもあります。

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ウェブコンソールの**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ウェブコンソールで **[ダッシュボード]** > **[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を有効にし、アクションを適用するマシンを選択します。以下のアクションがあります。

- **脆弱性診断** - 選択した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
- **マルウェアからの保護** - 選択したマシンの完全スキャンを実行します
- **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** - 保護されているマシンや保護されていないマシンをバックアップします

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

脅威フィードアラートは、次の期間の後に自動的にクリーンアップされます。

- 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検出する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 ウェブ 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。
   ファイル拡張子ごと、ロケーションごとに、保護されていないファイルの一覧が表示されます。ファイル拡張子でこのリストをフィルタリングできます。
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。

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。

- **時刻でスケジュール** - 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。

既定の設定:**時刻でスケジュール**

スケジュールの種類:

- **月次** - 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します。
- **日次** - タスクを実行する週中の日を選択しします。
- **毎時** - 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。

既定の設定:**日単位**

開始時間 - 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 - 設定したスケジュールが有効な日付範囲を指定します。

開始条件 - すべての条件を定義して、どの条件が同時に満たされたときにタスクを実行するか指定します。

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"（235ページ）」に説明されています。 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。

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。

リモートデスクトップアクセス

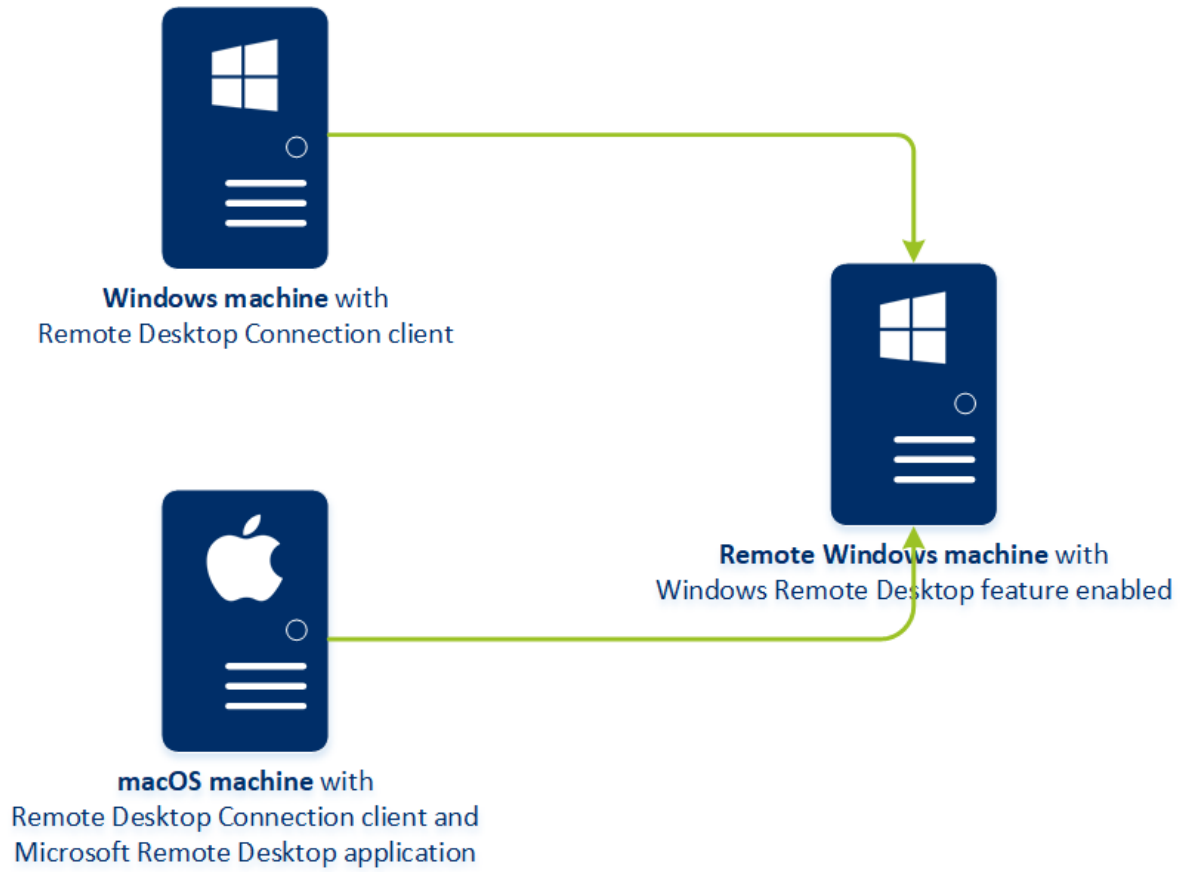
リモートアクセス（RDPクライアントとHTML5クライアント）

Cyber Protectにはリモートアクセス機能が用意されています。ウェブコンソールからユーザーのマシンにリモート接続して、そのマシンを管理できます。この機能を使用すると、マシンで問題が発生したユーザーを簡単にサポートできます。

前提条件:

- プロテクションエージェントがリモートのマシンにインストールされ、管理サーバーに登録されます。
- マシンには適切なCyber Protectライセンスが割り当てられています。
- リモートデスクトップ接続クライアントが、接続を初期化するマシンにインストールされます。
- RDP接続が初期化されたマシンは、ホスト名で管理サーバーにアクセスできる必要があります。DNS設定が適切に構成されているか、または管理サーバーのホスト名がhostsファイルに含まれている必要があります。

WindowsマシンとmacOSマシンの両方からリモート接続を確率できること。



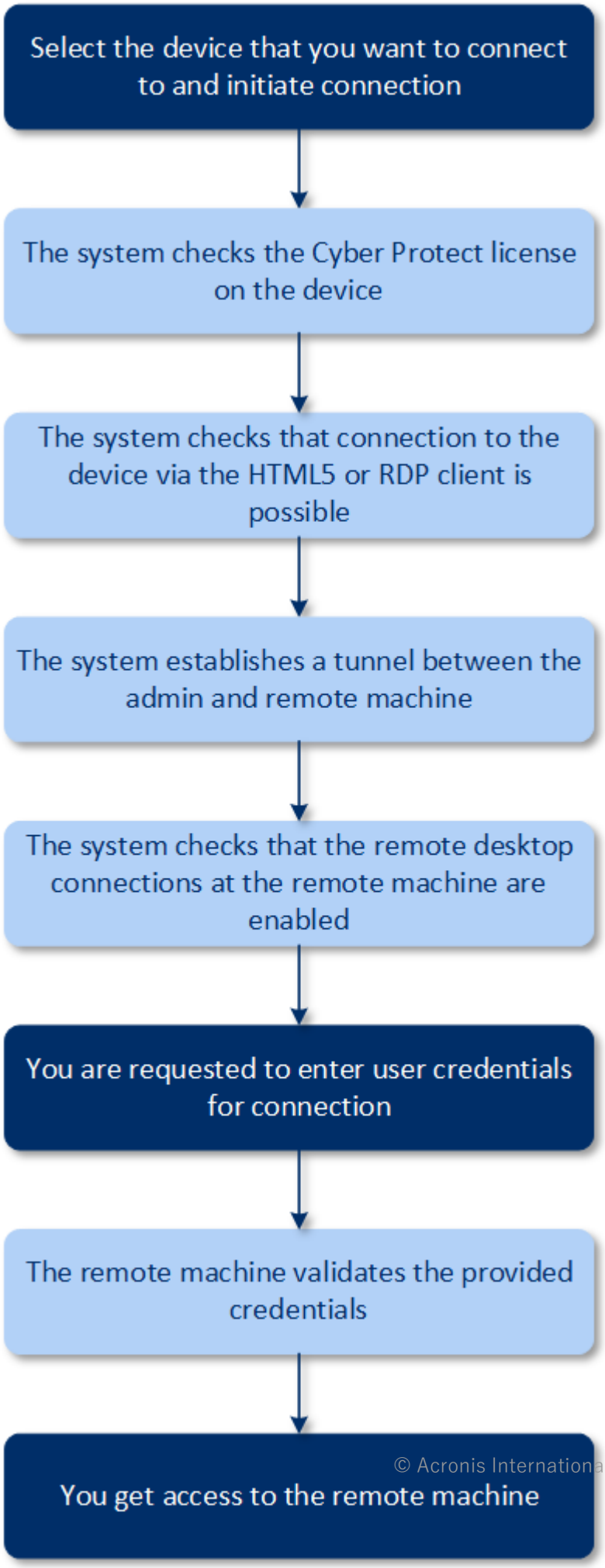
リモートアクセス機能は、Windowsのリモートデスクトップ機能を備えたWindowsマシンへの接続で利用できます。そのため、Windows 10 HomeやmacOSシステムなどへのリモートアクセスはできません。

macOSマシンからリモートのマシンへの接続を確立するには、macOSマシンに次のアプリケーションがインストールされていることを確認します。

- リモートデスクトップ接続クライアント
- Microsoft Remote Desktopアプリケーション

仕組み

リモートのマシンに接続しようとすると、そのマシンにCyber Protectライセンスがあるかどうかがチェックされます。さらに、HTML5クライアント経由またはRDPクライアント経由の接続が可能かどうかもチェックされます。その後、ユーザーがRDPクライアント経由またはHTML5クライアント経由の接続を開始します。リモートのマシンへのトンネルが確立され、リモートのマシンでリモートデスクトップ接続が有効になっているかどうかがチェックされます。次に資格情報を入力し、ベリファイが実行された後、リモートのマシンにアクセスできます。



リモートのマシンに接続する方法

リモートのマシンに接続するには、以下の手順を実行します。

1. Cyber Protectウェブコンソールで **[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のマシンをクリックし、**[サイバープロテクションデスクトップ]** > **[RDPクライアント経由で接続]** または **[HTML5クライアント経由で接続]** をクリックします。

   注意
   HTML5クライアントを介した接続は、管理サーバーがLinuxマシンにインストールされている場合にのみ使用できます。

3. （オプションとして、RDPクライアント経由の接続限定で）リモートデスクトップ接続クライアントをダウンロードしてインストールします。リモートのマシンへの接続を開始します。
4. リモートのマシンにアクセスするためのログイン情報とパスワードを指定して、**[接続]** をクリックします。

リモートのマシンに接続して、そのマシンを管理できるようになります。

リモート接続を共有

自宅で作業している従業員は、オフィスのコンピューターにアクセスしなければならない場合がありますが、組織でリモート接続用にVPNや他のツールが構成されていない可能性があります。Cyber ProtectにはRDPリンクをユーザーと共有する機能があるため、マシンへのリモートアクセスが可能です。

リモート接続の共有機能を有効にするには

1. Cyber Protectのウェブコンソールで、**[設定]** > **[保護機能]** > **[リモート接続]** に移動します。
2. **[リモートデスクトップ接続を共有]** チェックボックスを選択します。

これにより、Cyber Protectウェブコンソールでデバイスを選択するときに、新しいオプション **[リモート接続の共有]** が表示されるようになります。

リモート接続をユーザーと共有するには

1. Cyber Protectウェブコンソールで **[デバイス]** > **[すべてのデバイス]** に進みます。
2. リモート接続を提供するデバイスを選択します。
3. **[リモート接続を共有]** をクリックします。
4. **[リンクの取得]** をクリックします。開いているウィンドウで、生成されたリンクをコピーします。デバイスへのリモートアクセスが必要なユーザーとこのリンクを共有できます。リンクは10時間有効です。

リンクを取得した後、Eメールや他の通信手段で共有できます。リンクを共有されたユーザーは、リンクをクリックしてから接続タイプを選択する必要があります。

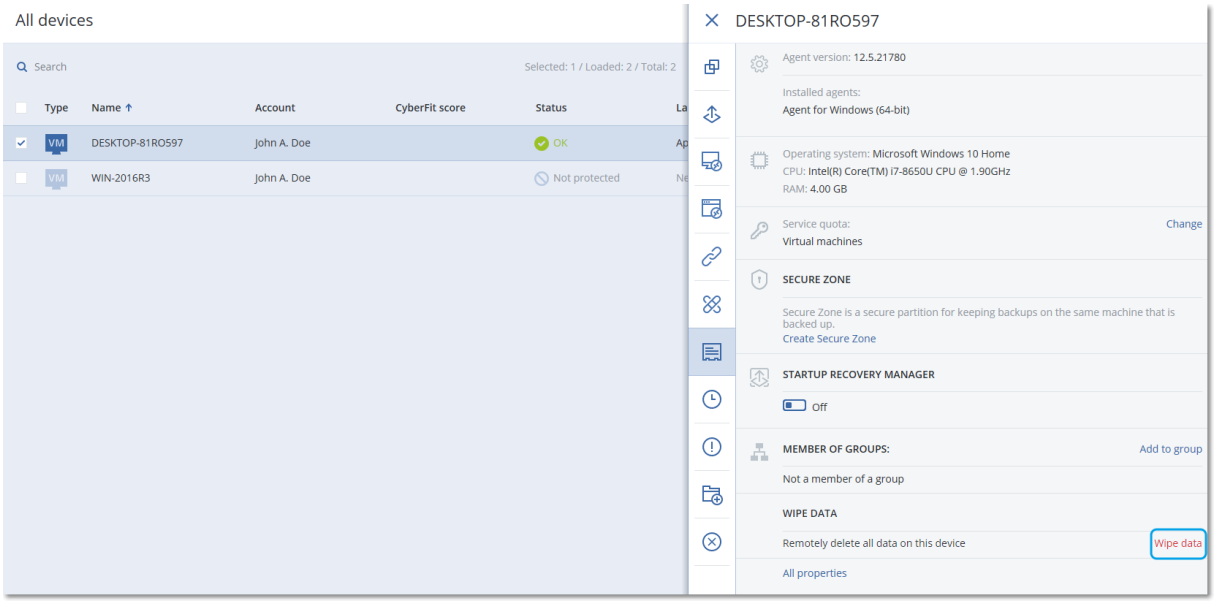
- RDPクライアント経由で接続します。
  この接続では、リモート接続クライアントのダウンロードとインストールを確認します。

- HTML5クライアント経由で接続します。
  この接続では、RDPクライアントをユーザーのマシンにインストールする必要がありません。ユーザーはログイン画面にリダイレクトされ、マシンにアクセスするための資格情報を入力する必要があります。

リモートワイプ

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 Protect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 10を実行す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ウェブコンソールで **[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
   [ダッシュボード] > **[アクティビティ]** では、ワイプ処理の詳細と開始したユーザーを確認できます。

デバイスグループ

デバイスグループの目的は、登録されている大量のデバイスを簡単に管理することです。

保護計画はグループに適用できます。グループに新しいデバイスが表示されると、そのデバイスは計画によって保護されます。グループから削除されたデバイスは、計画によって保護されなくなります。グループに適用された計画をグループのメンバーで取り消すことはできません。グループ自体でのみ取り消すことができます。

同じ種類のデバイスのみをグループに追加できます。例えば、[**Hyper-V**]では、Hyper-V仮想コンピュータのグループを作成できます。[**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を作成できます。[**すべてのデバイス**] では、グループは作成できません。

1台のデバイスは、複数のグループのメンバーになることができます。

ビルトイングループ

登録されたデバイスは、[**デバイス**] タブのいずれかのビルトインルートグループに表示されます。

ルートグループを編集または削除することはできません。ルートグループに計画を適用することはできません。

一部のルートグループには、ビルトインサブルートグループが含まれています。これらのグループを編集または削除することはできません。ただし、ビルトインサブルートグループに計画を適用することは可能です。

カスタム グループ

マシンの役割はそれぞれ違うので、1つの保護計画ではビルトイングループのすべてのデバイスを十分に保護できない場合があります。バックアップされたデータは各部門に固有であるため、一部のデータは頻繁にバックアップが必要なのに対し、その他のデータは1年に2回程度のバックアップで十分なことがあります。このため、マシンのセットごとにさまざまな保護計画を作成することになります。このような場合は、カスタム グループの作成を検討します。

カスタム グループには、1 つ以上の入れ子になったグループを含めることができます。すべてのカスタム グループは、編集または削除が可能です。次の種類のカスタムグループがあります。

- **静的グループ**

  静的グループには、手動で追加したマシンが含まれています。マシンを明示的に追加または削除した場合を除き、静的グループの内容が変更されることはありません。

  例:経理部門のカスタムグループを作成し、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。保護計画をこのグループに適用すると、経理担当者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、新しいコンピュータを手動で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、グループ作成時に指定した検索条件に従って自動的に追加されたマシンが含まれています。ダイナミック グループの内容は自動的に変更されます。マシンは、指定した条件が満たされるまでグループに残ります。

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。この場合、グループメンバーシップの条件に部分的なマシン名を指定し、そのグループに保護計画を適用します。新しい経理担当者が入社した場合は、新しいマシンが登録と同時にグループに追加され、自動的に保護されます。

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。この場合、グループメンバーシップの条件に経理OUを指定し、そのグループに保護計画を適用します。新しい経理担当者が入社した場合は、新しいマシンが登録および OU への追加（操作の順番に関係なく）と同時にグループに追加され、自動的に保護されます。

静的グループの作成

1. **[デバイス]** をクリックし、静的グループを作成するデバイスを含んでいるビルトイングループを選択します。
2. グループを作成するグループの横にあるギアアイコンをクリックします。
3. **[新しいグループ]** をクリックします。
4. グループ名を指定し、**[OK]** をクリックします。
   グループツリーに新しいグループが表示されます。

静的グループへのデバイスの追加

1. **[デバイス]** をクリックし、グループに追加する1つ以上のデバイスを選択します。
2. **[グループに追加]** をクリックします。
   選択したデバイスを追加できるグループのツリーが表示されます。
3. 新しいグループを作成する場合は、次の手順を実行します。それ以外の場合は、この手順をスキップします。
   a. グループを作成するグループを選択します。
   b. **[新しいグループ]** をクリックします。
   c. グループ名を指定し、**[OK]** をクリックします。
4. デバイスを追加するグループを選択して、**[完了]** をクリックします。

グループを選択して **[デバイスを追加]** をクリックすることでもデバイスを静的グループに追加することができます。

ダイナミックグループの作成

1. **[デバイス]** をクリックして、ダイナミックグループを作成するデバイスを含むグループを選択します。
2. 検索フィールドを使用してデバイスを検索します。次の複数の属性および演算子を使用できます。
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
グループ作成ではサポートされていない属性もあります。以下の検索クエリセクションの表を参照してください。

4. グループ名を指定し、[**OK**] をクリックします。

検索クエリ

次の表に、検索クエリで使用できる属性を示します。

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
`name`	• 物理コンピュータのホスト名 • 仮想コンピュータの名前 • 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	`name = 'en-00'`	はい
`parameters.MacAddress`	MACアドレス。	`parameters.MacAddress LIKE '00-22-4D-50-25-E5'`	はい
`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。	`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

	注意
	コメントフィールドに手動でテキストを追加した場合、Windowsの説明との自動同期が無効化されます。もう一度有効化するには、追加したコメントを消去します。
	
	お使いのデバイス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`
	
	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。
	
	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。
	
	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		

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
	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テキストを追加した場合、Windowsの説明との自動同期が無効化されます。もう一度有効化するには、追加したコメントを消去します。 • 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。 デバイスでは、どちらか一方、または両方のコメントを指定することができます。また両方とも空白にしておくこともできます。両方のコメントが指定されている場合、デバイスのコメ		

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
	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。		
`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
`cpuArch`	CPUのアーキテクチャ。 設定可能な値: • `'x64'` • `'x86'`	`cpuArch = 'x64'`	はい
`memorySize`	RAMのサイズ（MiB単位）。	`memorySize < 1024`	はい
`cpuName`	CPU名。	`cpuName LIKE '%XEON%'`	はい
`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
`tzOffset`	マシンのタイムゾーンのオ	`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
	フセット（単位: 分）。		
parameters.Architecture	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: • 'x86' • 'x64'	parameters.Architecture = 'x86'	はい
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 IN ('linux', 'macosx')	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。 • 'server' • 'workstation'	osProductType = 'server'	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' Hyper-V仮想マシン。 • 'pcs' Virtuozzo仮想マシン。 • 'hci' Virtuozzo Hybrid	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
	Infrastructure仮想マシン。 • `'scale'` Scale Computing HC3仮想マシン。 • `'ovirt'` oVirt仮想マシン		
`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。	`osVersionMminor = 1`	はい
`isOnline`	マシンのアベイラビリティー 設定可能な値: • `true` • `false`	`isOnline = true`	いいえ
`tenant`	デバイスが属している部署名	`tenant = 'Unit 1'`	はい
`tenantId`	デバイスが属している部署のID 部署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
`state`	デバイスの状態 設定可能な値: • `'idle'` • `'interactionRequired'`	`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
	• 'canceling' • 'backup' • 'recover' • 'install' • 'reboot' • 'failback' • 'testReplica' • 'run_from_image' • 'finalize' • 'failover' • 'replicate' • 'createAsz' • 'deleteAsz' • 'resizeAsz'		
status	リソースのステータス。 設定可能な値: • 'notProtected' • 'ok' • 'warning' • 'error' • 'critical'	status = 'ok'	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を取得するには、**[計画]** > **[バックアップ]** をクリックし、計画を選択して、**[ステータス]** 列の図をクリックして、ステータスをクリックします。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	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
	ス。		
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
ou	指定した Active Directory の組織単位（OU）に属するマシン。	ou IN ('RnD', 'Computers')	はい
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
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 > '2022-03-11' lastBackupTime <= '2022-03-11 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	lastBackupTryTime >= '2022-03-11'	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
	形式はYYYY-MM-DD HH:MMです。		
nextBackupTime	次回バックアップの時刻 形式はYYYY-MM-DD HH:MMです。	nextBackupTime >= '2022-08-11'	いいえ
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。 保護エージェントIDを取得するには、**[デバイス]** でマシンを選択し、**[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」の値を使用します。	hostId = '4B2A7A93-A44F-4155-BDE3-A023C57C9431'	はい
resourceType	リソースの種類。 設定可能な値: • 'machine' • 'virtual_machine.vmwesx' • 'virtual_machine.mshyperv' • 'virtual_machine.rhev' • 'virtual_machine.kvm' • 'virtual_machine.xen'	resourceType = 'machine' resourceType in ('mssql_aag_database', 'mssql_database')	はい
hasAsz	Acronis Secure Zone の物理マシンのプロテクションエージェント。 設定可能な値: • true • false	hasAsz=true	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
chassis	マシンのシャーシタイプ。 設定可能な値: • unknown • laptop • desktop • server • other	chassis='laptop'	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。たとえば、lastBackupTime = 2020-02-20の場合、検索結果には、lastBackupTime >= 2020-02-20 00:00とlastBackup time <= 2020-02-20 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。

演算子

次の表に、使用可能な演算子を示します。

演算子	意味	例
AND	論理積演算子。	name like 'en-00' AND tenant = 'Unit 1'
OR	論理和演算子。	state = 'backup' OR state = 'interactionRequired'
IN (<value1>,... <valueN>)	この演算子は、値のリストに式と一致する値があるかどうかを検証するために使用します。	osType IN ('windows', 'linux')
NOT	論理否定演算子。	NOT(osProductType = 'workstation')
NOT IN (<value1>,... <valueN>)	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 '**ワイルドカードパターン**'	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検証するために使用します。 次のワイルドカード演算子を使用できます。	name LIKE 'en-00' name LIKE '*en-00' name LIKE '*en-00*' name LIKE 'en-00_'

演算子	意味	例
	• *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。	
RANGE(<starting_value>, <ending_value>)	この演算子は、式が値の範囲内に含まれる（包含的）かどうかを検証するために使用します。	ip RANGE ('10.250.176.1','10.250.176.50')
= or ==	等しいことを表す演算子。	osProductType = 'server'
!= または <>	等しくないことを表す演算子。	id != '4B2A7A93-A44F-4155-BDE3-A023C57C9431'
<	小なりを表す演算子。	memorySize < 1024
>	大なりを表す演算子。	diskSize > 300GB
<=	以下を表す演算子。	lastBackupTime <= '2022-05-11 00:15'
>=	以上を表す演算子。	nextBackupTime >= '2022-09-11'

グループへの保護計画の適用

1. **[デバイス]** をクリックし、保護計画を適用するグループを含むビルトイングループを選択します。
   子グループのリストが表示されます。
2. 保護計画を適用するグループを選択します。
3. **[グループバックアップ]** をクリックします。
   ソフトウェアにより、グループに適用可能な保護計画のリストが表示されます。
4. 次のいずれかを実行します。
   - 既存の保護計画を展開してから、**[適用]** をクリックします。
   - **[新規作成]** をクリックしてから、「バックアップ」で説明されている方法で新しい保護計画を作成してください。

監視とレポート

[概要] ダッシュボードでは、保護されたインフラストラクチャの現在の状態を監視できます。

[レポート] セクションでは、保護されたインフラストラクチャに関して、オンデマンドおよびスケジュール済みのレポートを生成できます。このセクションは、Advanced ライセンスのみで使用できます。

概要ダッシュボード

概要ダッシュボードは、保護されたインフラストラクチャの概要を示す多数のカスタマイズ可能なウィジェットを提供します。円グラフ、表、グラフ、棒グラフ、一覧表として表示される20個以上のウィジェットから選択できます。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。ウィジェットの情報は、5 分間隔でアップデートされます。

Advanced ライセンスでは、ダッシュボードの現在の状態を .pdf または .xlsx 形式でダウンロードしたり、Eメールで送信したりすることもできます。ダッシュボードをメールで送信する場合は、**[電子メールサーバー]** 設定が構成されていることを確認します。

使用可能なウィジェットは、Cyber Protect の版によって異なります。デフォルトのウィジェットの一覧は次のとおりです。

ウィジェット	可用性	説明
サイバープロテクション	Cyber Backup エディションでは提供されていません	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。
保護ステータス	すべてのエディションで提供されています	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。
アクティビティ	すべてのエディションで提供されています	指定した期間中に実行されたテープアクティビティの概要を表示します。
アクティブアラート概要	すべてのエディションで提供されています	アラートタイプ別と重要度別に、アクティブアラートの概要を示します。
パッチインストールステータス	Cyber Backup エディションでは提供されていません	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。
カテゴリ別の未適用アップデー	Cyber Backup エディションでは提供されていません	未適用アップデートの数をカテゴリ別に表示します。

ト		
ディスク状態ステータス	Cyber Backup エディションでは提供されていません	ステータス別にディスク数を表示します。
デバイス	すべてのエディションで提供されています	環境内のデバイスに関する詳細情報を示します。
アクティブアラートの詳細	すべてのエディションで提供されています	アクティブアラートに関する詳細情報を示します。
既存の脆弱性	すべてのエディションで提供されています	環境内のオペレーティングシステムとアプリケーションの既存の脆弱性、および影響を受けたマシンを示します。
パッチインストール履歴	Cyber Backup エディションでは提供されていません	インストールされているパッチに関する詳細情報を示します。
最近影響を受けたもの	すべてのエディションで提供されています	最近感染したマシンに関する詳細情報を示します。
ロケーションサマリー	すべてのエディションで提供されています	バックアップロケーションに関する詳細情報を示します。

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鉛筆アイコンをクリックします。ウィジェットを編集したら、**[完了]** をクリックします。

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。

Cyber Protection

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

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。

- **保護されているマシン** - 保護計画が適用されているマシン。
- **保護されていない** - 保護計画が適用されていないマシン。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。

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。
- NVMeドライブの場合、ディスク状態の監視は、Windows APIを介してSMARTデータを送受信するドライブでのみサポートされています。ドライブから直接SMARTデータを読み取る必要があるNVMeドライブでは、ディスク状態の監視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。

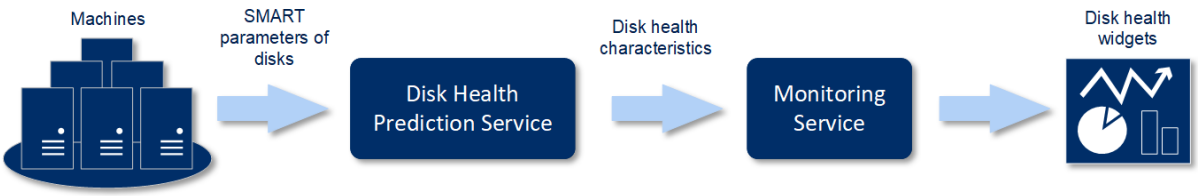
- **OK**
  ディスク状態が70～100%です。
- **警告**
  ディスク状態が30～70%です。
- **重大**
  ディスク状態が0～30%です。
- **ディスクデータの計算中**
  現在のディスク状態と予測を計算中です

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パラメーター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。

   予測期間は通常1ヵ月間です。
3. 監視サービスはこれらの特性情報を受信し、Cyber Protectウェブ 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

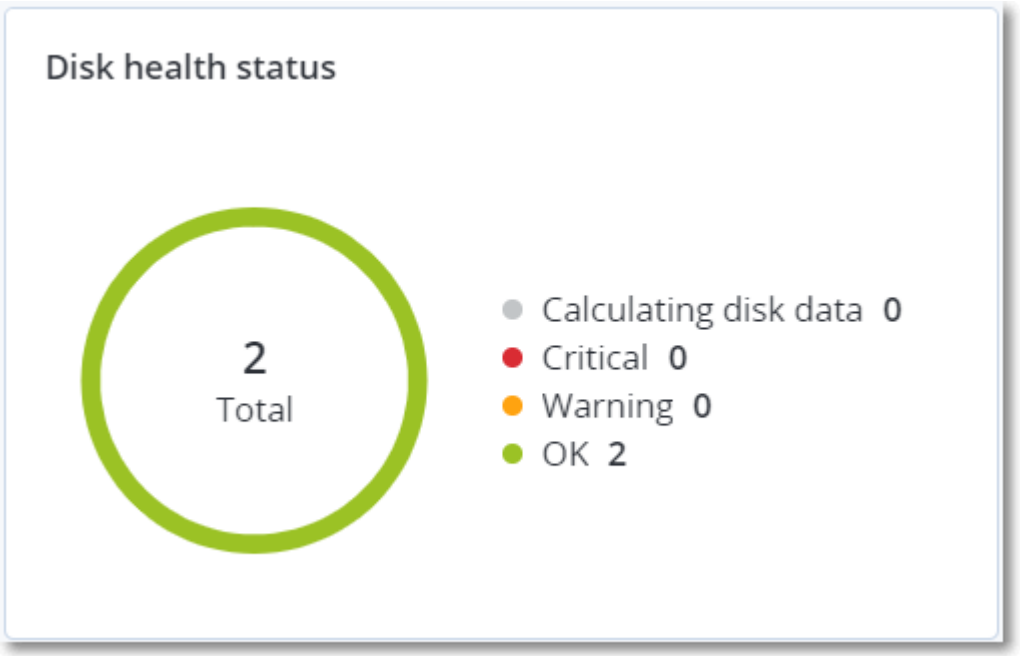
ディスク状態の監視結果は、Cyber Protectウェブ コンソールで利用できる以下のウィジェットに表示されます。

- **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 -
    選択した組織単位（OU）のすべてのマシンのディスクステータスに関する概要情報を表示します。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。ディスク状態ステータスが**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

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、組織単位（OU）/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。

保護されていないファイルの数とそのロケーションに関する詳細を表示するには、色付きのブロックにカーソルを置きます。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。

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。

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、インストールステータスによる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、マシンにインストールされているパッチに関する詳細情報を示します。

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

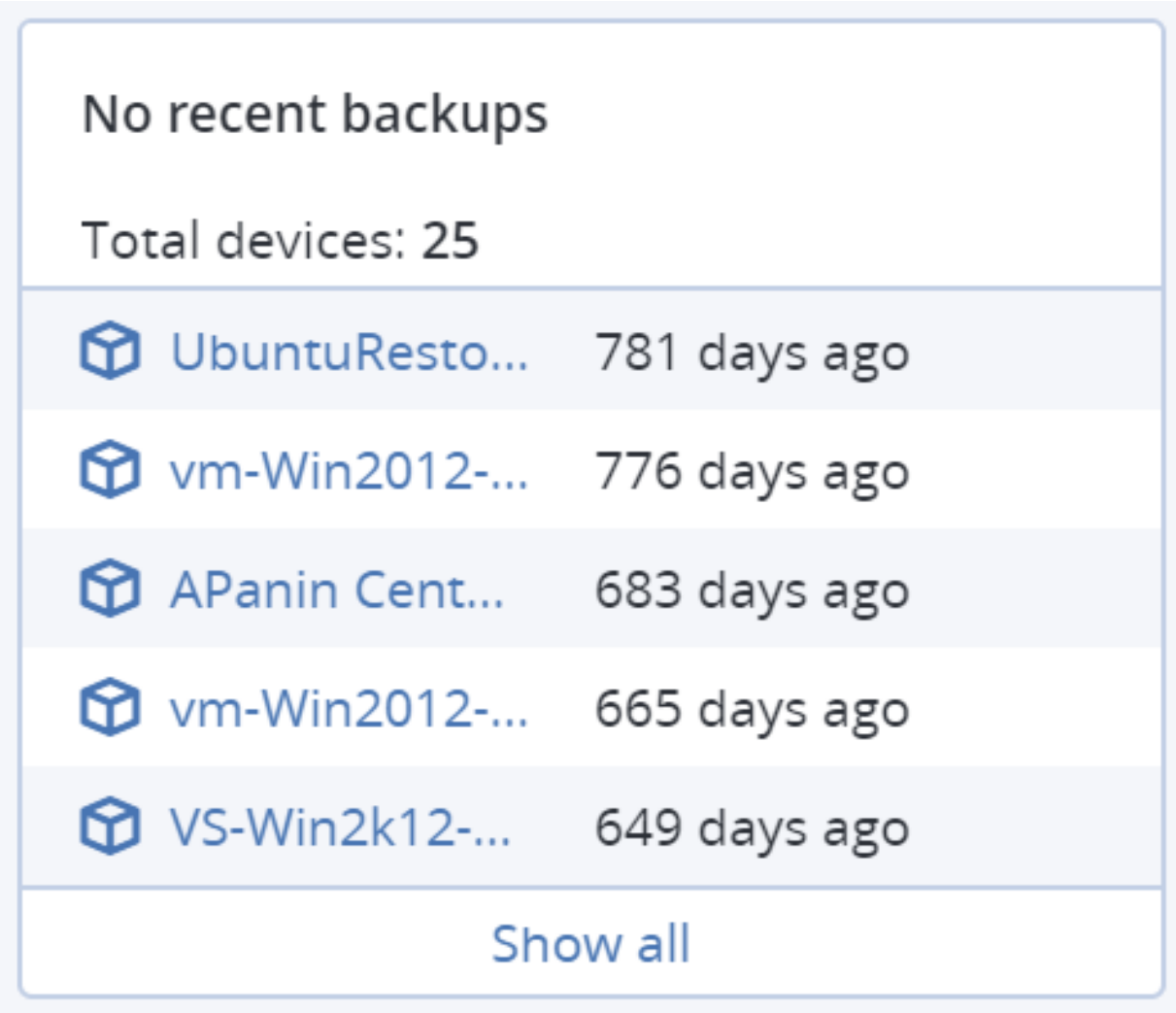
このウィジェットは、管理サーバーにスキャンサービスがインストールされている場合にのみ使用できます。このウィジェットは、バックアップで検出された脅威の詳細情報を示します。

最近影響を受けたもの

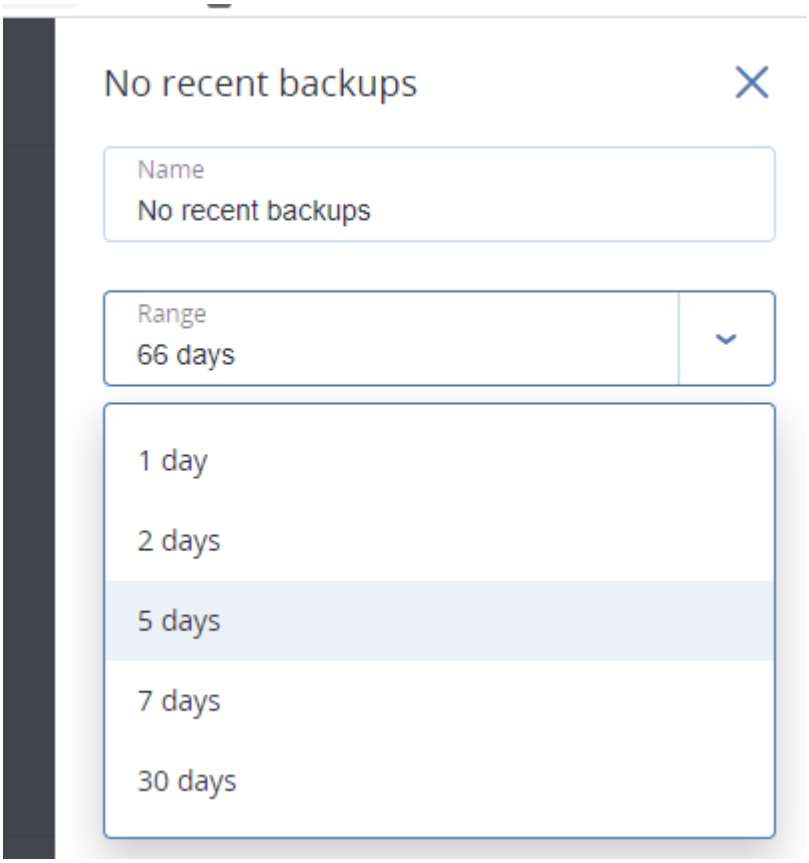
このウィジェットは、最近感染したマシンに関する詳細情報を示します。検出された脅威の種類と感染したファイルの数についての情報を見つけることができます。

最近のバックアップ取得なし

このウィジェットは、適用済みの保護計画を備えるワークロードで、最後に成功したバックアップの日付が、ウィジェット設定で指定された時間範囲よりも前になっているものを表示します。



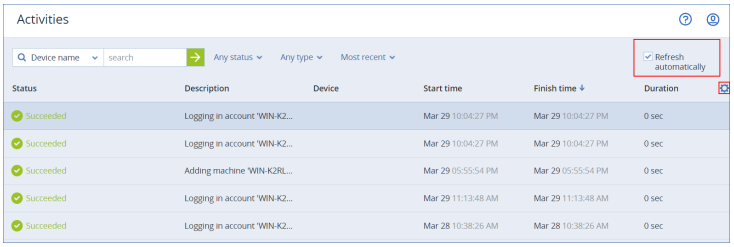
このウィジェットを追加すると、デフォルトでは、過去5日間の情報が表示されます。ドロップダウンメニューを使って別の期間を選択したり、手動で日数を入力したりすることもできます。入力可能な最大日数は180日です。



アクティビティタブ

[アクティビティ] タブでは、直近90日間のアクティビティの概要が表示されます。

[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。ただし、複数のアクティビティでアップデート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する可能性があります。



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**
  例えば、成功、失敗、進行中、キャンセルなどです。
- **タイプ**
  例えば、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。

デフォルトの保持期間を変更するには、task_manager.yaml構成ファイルを編集する必要があります。

保持期間を変更するには

1. 管理サーバーを実行しているマシンで、以下の設定ファイルをテキストエディタで開きます。
   - Windowsの場合: `%Program Files%\Acronis\TaskManager\task_manager.yaml`
   - Linuxの場合: `/usr/lib/Acronis/TaskManager/task_manager.yaml`
2. 次のセクションを見つけます。

   ```
   database:
     connection-string:""
     run-cleanup-at:"23:59"
     cleanup-batch-size:10
     max-cleanup-retries:10
     log-queries:false
     max-transaction-retries: 10
     shards:
      - connection-string: sqlite://task-manager.sqlite
        days-to-keep: 90
        space: "default"
        key: "00000000-0000-0000-0000-000000000000"
   ```

3. `days-to-keep` 行を任意に編集します。
   たとえば、次のようになります。

   ```
   days-to-keep:30
   ```

   注意
   必要に応じて保持期間を変更できます。保持期間を長くすると、管理サーバーのパフォーマンスが低下します。

4. **Acronis Service Manager Service**を再起動します（"Acronis Service Manager Serviceを再起動するには"（196ページ）を参照）。

レポート

定義済み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。

自分で管理する部署のレポートのみ設定できます。

レポートは設定されたスケジュールに合わせて電子メールで送信したりダウンロードしたりできます。レポートをメールで送信する場合は、**[電子メールサーバー]** 設定が構成されていることを確認してください。サードパーティ製のソフトウェアを使用してレポートを処理する場合は、レポートを.xlsx形式で特定のフォルダに保存するようスケジュールします。

使用可能なレポートはCyber Protectの版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	可用性	説明
アラート	Cyber Backup Advanced Cyber Protect Advanced	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	Cyber Protect Advanced	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。
バックアップ	Cyber Backup Advanced Cyber Protect Advanced	現在のバックアップと復元ポイントの詳細を表示します。
現在のステータス	Cyber Backup Advanced Cyber Protect Advanced	環境の現在のステータスを表示します。
日次のアクティビティ	Cyber Backup Advanced Cyber Protect Advanced	指定し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	Cyber Protect Advanced	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。
検出された脅威	Cyber Backup Advanced Cyber Protect Advanced	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なマシンの数を表示します。
検出されたマシン	Cyber Backup Advanced Cyber Protect Advanced	組織のネットワーク内で検出され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	Cyber Protect Advanced	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	Cyber Backup Advanced Cyber Protect Advanced	環境内のオペレーティングシステムとアプリケーションの既存の脆弱性、および影響を受けたマシンを示します。
ライセンス	Cyber Backup Advanced Cyber Protect Advanced	利用可能なライセンスの概要を表示します。
ロケーション	Cyber Backup Advanced Cyber Protect Advanced	指定された期間のバックアップロケーションの使用状況統計を表示します。
パッチ管理概要	Cyber Protect Advanced	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	Cyber Backup Advanced Cyber Protect Advanced	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。
テープアクティビティ	Cyber Backup Advanced Cyber Protect Advanced	過去24時間中に使用されたテープのリストを表示します。
週単位のアクティビティ	Cyber Backup Advanced Cyber Protect Advanced	指定した期間中に実行されたテープアクティビティの概要を表示します。

レポートの基本操作

- レポートを表示するには、その名前をクリックします。
- レポートを使用してさらに操作を実行するには、レポート行の省略記号アイコン（...）をクリックします。
  同じ操作がレポート内から利用可能です。

レポートを追加する

1. **[レポートの追加]** をクリックします。
2. 次のいずれかを実行します。

- 定義済みレポートを追加するには、その名前をクリックします。
- カスタマーのレポートを追加するには、[**カスタム**] をクリックします。**カスタム**という名前の新しいレポートが、レポートのリストに追加されます。このレポートを開き、ウィジェットを追加します。

3. （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。
4. （オプション）以下で説明するようにレポートを編集します。

レポートを編集するには

1. レポート名の横にある省略記号のアイコン（...）をクリックして、[**設定**] をクリックします。
2. レポートを編集します。次の操作を実行できます。
   - レポート名の変更
   - レポートに含まれるすべてのウィジェットの時間範囲の変更
   - .pdf または/および .xlsx 形式の電子メールでレポートの送信をスケジュール
3. [**保存**] をクリックします。

レポートのスケジュールを設定するには

1. レポートを選択し、［**スケジュール**］ クリックします。
2. [**スケジュールされたレポートの送信**] スイッチを有効にします。
3. レポートを電子メールで送信する、フォルダに保存する、またはこの両方を実行するように選択します。選択に応じて、電子メールアドレスを指定するか、フォルダパスを指定するか、どちらも指定します。
4. レポート形式として.pdfか.xlsx、または両方を選択します。
5. レポートの期間を選択します。1日、7日、または30日を選択します。
6. レポートが送信または保存される日時を選択します。
7. [**保存**] をクリックします。

レポート構造のエクスポートとインポート

レポート構造（ウィジェット一式やスケジュール設定）は、.jsonファイルにエクスポートしたり逆にインポートしたりできます。この機能は、Management Serverを再インストールしたり、レポート構造を別Management Serverにコピーしたりする場合に便利です。

レポート構造をエクスポートするには、レポートを選択し、［**エクスポート**］ クリックします。

レポート構造をインポートするには、レポートを選択し、[**レポートの作成**] をクリックして、[**インポート**] をクリックします。

レポートデータのダンプダンプ

レポートデータのダンプを.csvファイルに保存できます。ダンプには指定した時間範囲内の全レポートデータが（フィルタリングされずに）含まれます。

ソフトウェアはデータダンプをその場で生成します。範囲が長いと、処理に時間がかかることがあります。

レポートデータをダンプするには

1. レポートを選択し、［**開く**］ クリックします。
2. 右上隅にある省略記号アイコン（...）をクリックし、**[ダンプデータ]** をクリックします。
3. **[ロケーション]** で、.csvファイルのフォルダパスを指定します。
4. **[時間範囲]** で、時間の範囲を指定します。
5. **[保存]** をクリックします。

アラートの重大度の設定

アラートとは、実際の問題または潜在的な問題に関して警告するメッセージです。アラートはさまざまな方法で使用できます。

- **[概要]** タブの **[アラート]** セクションでは、現在のアラートを監視して問題を迅速に特定し、解決できます。
- **[デバイス]** では、デバイスのステータスがアラートから取得されます。**[ステータス]** 列では、問題のあるデバイスをフィルタで検出できます。
- 電子メール通知を設定するときに、通知をトリガするアラートを選択できます。

アラートの重大度は次のいずれかです。

- **重大**
- **エラー**
- **警告**

アラートの重大度を変更するには、またはアラートを完全に無効にするには、以下で説明するアラート設定ファイルを使用します。この操作では、Management Serverを再起動する必要があります。

アラートの重大度を変更しても、生成済みのアラートには影響しません。

アラート設定ファイル

設定ファイルは、Management Serverを実行しているマシン上にあります。

- Windowsの場合: `<installation_path>`**¥AlertManager¥alert_manager.yaml**
  <インストール パス>はManagement Serverのインストールパスです。デフォルト設定では、**%ProgramFiles%¥Acronis** となっています。
- Linux の場合: **/usr/lib/Acronis/AlertManager/alert_manager.yaml**

このファイルはYAML文書として構成されています。各アラートは `alertTypes` リスト内の要素です。

`name` キーは、アラートを識別します。

`severity` キーは、アラートの重大度を定義します。`critical`、`error`、または `warning` のいずれかの値を指定する必要があります。

オプションの `enabled` キーは、アラートが有効であるか無効であるかを定義します。この属性の値は `true` または `false` である必要があります。デフォルト（このキーがない状態）ではすべてのアラートが有効です。

アラートの重大度を変更するには、またはアラートを無効にするには

1. 管理サーバーがインストールされているマシン上のテキストエディタで**alert_manager.yaml**ファイルを開きます。
2. 変更または無効化したいアラートの場所を指定します。
3. 次のいずれかを実行します。
   - アラートの重大度を変更するには、`severity` キーの値を変更します。
   - アラートを無効化するには、`enabled` キーを追加し、その値を `false` に設定します。
4. ファイルを保存します。
5. 以下で説明するように、Management Serverサービスを再起動します。

WindowsでManagement Serverサービスを再起動するには

1. **[スタート]** メニューで、**[ファイル名を指定して実行]** をクリックし、「**cmd**」と入力します。
2. **[OK]** をクリックします。
3. 次のコマンドを実行します。

```
net stop acrmngsrv
net start acrmngsrv
```

LinuxでManagement Serverサービスを再起動するには

1. **ターミナル**を開きます。
2. 任意のディレクトリで次のコマンドを実行します。

```
sudo service acronis_ams restart
```

詳細ストレージオプション

テープ デバイス

次のセクションでは、テープデバイスを使用してバックアップを保存する方法について詳しく説明します。

テープ デバイスについて

テープデバイスは、テープライブラリまたはスタンドアロンのテープドライブを示す一般名称です。

テープライブラリ（自動ライブラリ）は、次の機構を備えた大容量ストレージ デバイスです。

- 1 つ以上のテープ ドライブ
- テープを保持する複数（最大で数千）のスロット
- スロットとテープ ドライブ間でテープを移動するための 1 つ以上のチェンジャ（自動メカニズム）

バーコード リーダーやバーコード プリンタなど、その他のコンポーネントを備えている場合もあります。

テープライブラリの具体的な例としては、**オートローダー**があります。オートローダは、1 つのドライブ、複数のスロット、1 つのチェンジャおよびバーコード リーダー（オプション）を備えています。

スタンドアロンのテープドライブ（**ストリーマ**とも呼ばれます）は、1つのスロットを備え、一度に1つのテープしか保持できません。

テープ サポートの概要

プロテクション エージェントでは、データを直接または Storage Node を介してテープデバイスにバックアップできます。いずれの場合でも、テープ デバイスの操作は完全に自動化されます。複数のドライブが搭載されたテープデバイスを1つのStorage Nodeに接続すると、複数のエージェントによるテープへのバックアップを同時に実行することができます。

RSM とサードパーティ製ソフトウェアとの互換性

サードパーティ製ソフトウェアとの共存

独自のテープ管理ツールを備えたサードパーティ製ソフトウェアがインストールされているマシンでは、テープを使用して作業することはできません。このようなマシンでテープを使用するには、サードパーティ製のテープ管理ソフトウェアをアンインストールまたは無効にする必要があります。

Windowsリムーバブル記憶域マネージャ（RSM）とのインタラクション

プロテクション エージェントと Storage Node は RSM を使用しません。テープデバイスが検出されると、RSMからデバイスが無効化されます（ただし、他のソフトウェアで使用されている場合は除きます）。テープデバイスで作業するには、ユーザーもサードパーティ製ソフトウェアでも、RSMでデバイ

スを有効化しないようにしてください。RSM でテープ デバイスが有効化されていた場合は、テープ デバイスの検出を繰り返してください。

サポートされるハードウェア

Acronis Cyber Protectは外部SCSIデバイスをサポートします。外部 SCSI デバイスは、ファイバ チャネルに接続されているか、SCSI、iSCSI、Serial Attached SCSI（SAS）インターフェイスを使用するデバイスです。Acronis Cyber ProtectはUSB接続テープデバイスもサポートします。

Windowsでは、Acronis Cyber Protectは、デバイスのチェンジャーのドライバがインストールされていない場合でもテープデバイスにバックアップできます。そのようなテープデバイスは、**[デバイス マネージャ]** に **[不明なメディア チェンジャー]** として表示されます。ただし、デバイスのドライブのドライバはインストールされている必要があります。Linux およびブータブル メディアでは、ドライバのないテープ デバイスへのバックアップは実行できません。

IDE または SATA 接続のデバイスの認識は保証されません。認識されるかどうかは、オペレーティング システムに正しいドライバがインストールされているかどうかによります。

特定のデバイスがサポートされるかどうかを確認するには、http://kb.acronis.com/content/57237に記載のあるハードウェア互換性ツールを使用してください。テスト結果に関するレポートをAcronisに送信することもできます。サポートが確認されているハードウェアは、ハードウェアの互換性リスト（https://go.acronis.com/acronis-cyber-protect-advanced-tape-hcl）に記載されています。

テープ管理データベース

コンピュータに接続されているすべてのテープデバイスに関する情報は、テープ管理データベースに格納されます。デフォルトのデータベース パスは、次のとおりです。

- Windows XP/Server 2003の場合: `%ALLUSERSPROFILE%\Application Data\Acronis\BackupAndRecovery\ARSM\Database`
- Windows 7およびそれ以降のバージョンのWindowsの場合: `%PROGRAMDATA%\Acronis\BackupAndRecovery\ARSM\Database`。
- Linuxの場合: `/var/lib/Acronis/BackupAndRecovery/ARSM/Database`

データベースのサイズは、テープに格納されているアーカイブの数によって異なりますが、100バックアップあたり約10MBです。テープライブラリに数千ものバックアップが格納されている場合は、データベースが大きくなることがあります。このため、テープ データベースは別のボリュームに保存した方が望ましいことがあります。

Windows でデータベースを移動するには、次の手順を実行します。

1. リムーバブルストレージ管理サービスを停止します。
2. すべてのファイルをデフォルトのロケーションから新しいロケーションに移動します。
3. レジストリキー`HKEY_LOCAL_MACHINE\SOFTWARE\Acronis\ARSM\Settings`を検索します。
4. 新しいロケーションのパスをレジストリ値`ArsmDmlDbProtocol`で指定します。文字列には32,765文字まで指定できます。
5. リムーバブルストレージ管理サービスを開始します。

Linux でデータベースを移動するには、次の手順を実行します。

1. acronis_rsmサービスを停止します。
2. すべてのファイルをデフォルトのロケーションから新しいロケーションに移動します。
3. テキストエディタで構成ファイル/etc/Acronis/ARSM.configを開きます。
4. 行<value name="ArsmDmlDbProtocol" type="TString">に移動します。
5. この行の下にあるパスを変更します。
6. ファイルを保存します。
7. acronis_rsmサービスを開始します。

TapeLocationフォルダ

TapeLocationフォルダには、テープにバックアップされているすべてのボリュームに由来する、ファイルシステムメタデータのキャッシュが含まれています。

デフォルトのTapeLocationフォルダのパスは次のとおりです。

- Windows XP/Server 2003の場合: %ALLUSERSPROFILE%\Application Data\Acronis\BackupAndRecovery\TapeLocation
- Windows 7以降の場合: %PROGRAMDATA%\Acronis\BackupAndRecovery\TapeLocation
- Linuxの場合: /var/lib/Acronis/BackupAndRecovery/TapeLocation

TapeLocationフォルダのサイズは、テープに保存されているすべてのバックアップサイズの約0.5～1%になります。ファイル復元オプションが有効になっているディスクレベルバックアップの場合、バックアップされたファイルの数によっては、TapeLocationフォルダのサイズが上述値をわずかに超過する場合があります。

テープに書き込む場合のパラメータ

テープ書き込みパラメータ（ブロック サイズとキャッシュ サイズ）を使用すれば、最適なパフォーマンスを得られるようにソフトウェアを調整できます。テープへの書き込みには両方のパラメータが必要ですが、通常は、ブロック サイズの調整のみが必要になります。最適な値はテープ デバイスの種類やバックアップ対象のデータ（ファイル数やサイズ）によって異なります。

注意
ソフトウェアによるテープからの読み取り時には、テープへの書き込みに使用したのと同じブロックサイズが使用されます。テープ デバイスでこのブロック サイズがサポートされない場合、読み取りが失敗します。

パラメータはテープ デバイスを接続するコンピュータごとに設定します。エージェントやストレージ ノードがインストールされたコンピュータを使用することもできます。Windowsを実行するマシンでは、構成はレジストリで行われますが、Linuxマシンでは、構成ファイル **/etc/Acronis/BackupAndRecovery.config**が使用されます。

Windows では、それぞれのレジストリ キーと DWORD 値を作成します。Linuxでは、構成ファイルの末尾（</registry>タグの直前）に次のテキストを追加します。

```
<key name="TapeLocation">
     <value name="WriteCacheSize" type="Dword">
```

```
          "value"
     </value>
     <value name=DefaultBlockSize" type="Dword">
          "value"
     </value>
</key>
```

DefaultBlockSize

テープへの書き込みに使用されるブロック サイズ（バイト単位）です。

設定可能な値:0、32、64、128、256、512、1024、2048、4096、8192、16384、32768、65536、131072、262144、524288、1048576。

値が 0 またはパラメータがない場合は、ブロック サイズは次のように決定されます。

- Windows では、テープ デバイス ドライバの値が使用されます。
- Linuxでは、値が**64KB**になります。

レジストリキー（Windowsを実行するマシン）:**HKEY_LOCAL_MACHINE¥SOFTWARE¥Acronis¥BackupAndRecovery¥TapeLocation¥DefaultBlockSize**

/etc/Acronis/BackupAndRecovery.configの行（Linuxを実行するマシン）：

```
     <value name=DefaultBlockSize" type="Dword">
          "value"
     </value>
```

指定した値がテープドライブで使用できない場合は、使用可能な値になるまで、または値が32バイトになるまで、ソフトウェアが指定した値を2で割っていきます。使用可能な値が見つからない場合は、使用可能な値になるまで、または値が1MBになるまで、ソフトウェアが指定した値を2倍にしていきます。ドライブで使用できる値がない場合、バックアップは失敗します。

WriteCacheSize

テープへの書き込みに使用されるバッファ サイズ（バイト単位）です。

設定可能な値:0、32、64、128、256、512、1024、2048、4096、8192、16384、32768、65536、131072、262144、524288、1048576。ただし、**DefaultBlockSize**パラメーター値よりも小さな値は使用できません。

値が0またはパラメーターがない場合、バッファサイズは**1MB**になります。オペレーティングシステムがこの値をサポートしていない場合は、使用可能な値が見つかるまで、または**DefaultBlockSize**パラメーター値になるまで、ソフトウェアが指定した値を2で割っていきます。オペレーティング システムがサポートする値が見つからない場合、バックアップが失敗します。

レジストリキー（Windowsを実行するマシン）：
HKEY_LOCAL_MACHINE¥SOFTWARE¥Acronis¥BackupAndRecovery¥TapeLocation¥WriteCacheSize

/etc/Acronis/BackupAndRecovery.configの行（Linuxを実行するマシン）：

```
<value name="WriteCacheSize" type="Dword">
     "value"
</value>
```

0 以外の値で、オペレーティング システムがサポートしていない値を指定した場合、バックアップが失敗します。

テープ関連のバックアップオプション

[テープ管理] バックアップオプションを設定して、以下を決定します。

- テープに保存されたディスクのバックアップからのファイルの復元を有効にするかどうか。
- 保護計画の完了後にテープをスロットに戻すかどうか。
- バックアップが完了した後にテープを取り出すかどうか。
- 各完全バックアップで空きテープを使用するかどうか。
- 完全バックアップを作成するときに、テープを上書きするかどうか（スタンドアロンのテープ ドライブのみ対応）。
- 使用テープの区別にテープセットを使用するかどうか。たとえば、週の異なる曜日に作成されたバックアップや、異なるコンピュータの種類のバックアップなど。

並行操作

Acronis Cyber Protectでは、テープデバイスの複数のコンポーネントを同時に操作できます。ドライブを使用した操作中（バックアップ、復元、再スキャン、消去など）に、チェンジャーを使用した操作（別のスロットへのテープの移動、テープの取り出しなど）を開始できます。その逆も可能です。テープ ライブラリに複数のドライブが搭載されている場合、1 つのドライブを操作中に別のドライブを使用した操作を開始することも可能です。たとえば、同一のテープ ライブラリにある異なるドライブを使用して、複数のコンピュータを同時にバックアップまたは復元できます。

新しいテープデバイスの検出の操作を、他の操作と同時に実行することが可能です。インベントリ中に同時に実行できる操作は、新しいテープデバイスの検出のみです。

同時に実行できない操作は、キューに入れられます。

制限事項

テープデバイスの使用には次の制限があります。

1. マシンが32ビットLinuxベースのブータブルメディアから起動されている場合、テープデバイスはサポートされません。
2. 次の種類のデータはテープにバックアップできません。Microsoft 365メールボックス、Microsoft Exchangeメールボックス。
3. 物理コンピュータおよび仮想コンピュータのアプリケーション認識型バックアップは作成できません。
4. macOS では、管理対象のテープベースのロケーションへのファイルレベルのバックアップのみがサポートされています。

5. テープ上に格納されたバックアップの統合を行うことはできません。このため、テープにバックアップする際、**[常に増分]** バックアップスキームは利用できません。
6. テープ上に格納されたバックアップの重複除外を行うことはできません。
7. 削除されていないバックアップが格納されている場合、または他のテープに依存関係のあるバックアップが存在する場合、テープを自動的に上書きすることはできません。

   このルールの唯一の例外は、[完全バックアップの作成時にスタンドアロンテープドライブのテープを上書きする] オプションが有効になっている場合です。
8. 復元にオペレーティング システムの再起動が必要な場合、そのオペレーティング システム環境下でテープ上に保存されているバックアップからの復元を実行することはできません。このような復元を実行するには、ブータブル メディアを使用します。
9. テープに保存されているバックアップはベリファイできますが、テープベースのロケーション全体またはテープデバイスのベリファイを行うことはできません。
10. 管理対象であるテープベースのロケーションを暗号で保護することはできません。代わりにバックアップを暗号化します。
11. 1 つのバックアップを同時に複数のテープへ書き込んだり、複数のバックアップを 1 つのドライブを介して 1 つのテープに書き込んだりすることはできません。
12. ネットワークデータ管理プロトコル（NDMP）を使用するデバイスはサポートされていません。
13. バーコード プリンタはサポートされていません。
14. リニアテープファイルシステム（LTFS）形式のテープはサポートされていません。

旧Acronis製品によって書き込まれたテープの読み取り

次の表に、Acronis Cyber ProtectのAcronis True Image Echo、Acronis True Image 9.1、Acronis Backup & Recovery 10、Acronis Backup & Recovery 11、Acronis Backup 11.5、11.7、12.5および製品ファミリによって書き込まれたテープの読み取りに関する概要を示します。Acronis Cyber Protectのさまざまなコンポーネントによって書き込まれたテープの互換性も示されています。

Acronis Backup 11.5、11.7、12.5によって作成された再スキャン済みバックアップの場合は、増分バックアップと差分バックアップを追加できます。

	マシンに接続されたテープデバイスで読み取りが可能なアプリケーション			
	Acronis Cyber Protect ブータブルメディア	Acronis Cyber Protect Windows エージェント	Acronis Cyber Protect Linuxエージェント	Acronis Cyber Protect Storage Node

ローカル接続のテープデバイス（テープドライブまたはテープライブラリ）でテープへの書き込みを行ったアプリケーション	ブータブルメディア	9.1	+	+	+	+
		Echo	+	+	+	+
		ABR10	+	+	+	+
		ABR11/ Acronis Backup 11.5/11.7/12.5	+	+	+	-
	エージェント for Windows	9.1	+	+	+	+
		Echo	+	+	+	+
		ABR10	+	+	+	+
		ABR11/ Acronis Backup 11.5/11.7/12.5	+	+	+	-
	エージェント for Linux	9.1	+	+	+	+
		Echo	+	+	+	+
		ABR10	+	+	+	+
		ABR11/ Acronis Backup 11.5/11.7/12.5	+	+	+	-
テープデバイスでテープの書き込みに使用したコンピュータ	バックアップ サーバー	9.1	-	-	-	-
		Echo	-	-	-	-
	ストレージ ノード	ABR10	+	+	+	+
		ABR11/ Acronis Backup 11.5/11.7/12.5	+	+	+	+

テープ デバイスの操作

ローカル接続されたテープデバイスへのコンピュータのバックアップ

前提条件

- テープ ドライブがメーカーの指示に従ってコンピュータに接続されている。
- プロテクション エージェントがマシンにインストールされている。

バックアップの準備

1. テープをテープ デバイスにロードします。
2. Cyber Protect ウェブ コンソールにログインします。
3. **[設定]** > **[テープ管理]** で、コンピュータノードを展開し、**[テープデバイス]** をクリックします。
4. 接続されているテープデバイスが表示されていることを確認します。表示されていない場合は、**[デバイスの検出]** をクリックします。
5. テープインベントリの実行:
   a. テープデバイス名をクリックします。
   b. **[インベントリ]** をクリックして、ロードされているテープを検出します。**[完全一覧収集]** をオンにしたままにします。**[認識されないテープまたはインポートされたテープを空きテーププールに移動]** はオンにしないでください。**[今すぐインベントリを開始]** をクリックします。
   結果:ロードされたテープが、「インベントリ」セクションで指定されているとおりに適切なプールに移動されます。

   注意
   テープ デバイス全体の完全インベントリには、時間がかかることがあります。

   c. ロードされたテープが「**認識されないテープ**」または「**インポートされたテープ**」プールに送られており、それらをバックアップに使用する場合は、テープを「**空きテープ**」プールに手動で移動します。

   注意
   「**インポートされたテープ**」プールに送られたテープには、Acronis ソフトウェアによって書き込まれたバックアップが含まれています。それらのテープを「**空きテープ**」プールに移動する前に、これらのバックアップが必要ないことを確認してください。

バックアップ

「バックアップ」セクションで説明されている方法で保護計画を作成します。バックアップロケーションを指定するときに、**[テーププール 'Acronis']** を選択します。

結果

- バックアップが作成されるロケーションにアクセスするには、**[バックアップストレージ]** > **[テーププール 'Acronis']** をクリックします。
- バックアップが保存されたテープは**Acronis**プールに移動されます。

ストレージ ノードに接続されたテープ デバイスへのバックアップ

前提条件

- Storage NodeがManagement Serverに登録されています。
- テープ デバイスがメーカーの指示に従ってストレージ ノードに接続されています。

バックアップの準備

1. テープをテープ デバイスにロードします。
2. Cyber Protect ウェブ コンソールにログインします。
3. **[設定]** > **[テープ管理]** をクリックし、Storage Node名のノードを展開して、**[テープデバイス]** をクリックします。
4. 接続されているテープデバイスが表示されていることを確認します。表示されていない場合は、**[デバイスの検出]** をクリックします。
5. テープインベントリの実行:
   a. テープデバイス名をクリックします。
   b. **[インベントリ]** をクリックして、ロードされているテープを検出します。**[完全一覧収集]** をオンにしたままにします。**[認識されないテーププールまたはインポートされたテーププールを空きテーププールに移動]** はオンにしないでください。**[今すぐインベントリを開始]** をクリックします。

      結果:ロードされたテープが、「インベントリ」セクションで指定されているとおりに適切なプールに移動されます。

      注意
      テープ デバイス全体の完全インベントリには、時間がかかることがあります。

   c. ロードされたテープが「**認識されないテープ**」または「**インポートされたテープ**」プールに送られており、それらをバックアップに使用する場合は、テープを「**空きテープ**」プールに手動で移動します。

      注意
      「**インポートされたテープ**」プールに送られたテープには、Acronis ソフトウェアによって書き込まれたバックアップが含まれています。それらのテープを「**空きテープ**」プールに移動する前に、これらのバックアップが必要ないことを確認してください。

   d. **Acronis**プールにバックアップするか、新しいプールを作成するかを決めます。

      詳細:複数のプールがあると、コンピュータごとまたは会社の部門ごとに別々のテープセットを使用することができます。複数のプールを使用することで、異なる保護計画から作成された複数のバックアップが 1 つのテープ上で混同されるのを防ぐことができます。
   e. 選択したプールが、必要なときに**空きテープ**プールからテープを取得できる場合は、この手順をスキップしてください。

      そうでない場合は、テープを**空きテープ**プールから、選択したプールに移動します。

      ヒント:プールが**空きテープ**プールからテープを取得できるかどうかを調べるには、プールをクリックし、**[情報]** をクリックします。

バックアップ

「バックアップ」セクションで説明されている方法で保護計画を作成します。バックアップロケーションを指定するときに、作成したテーププールを選択します。

結果

- バックアップが作成されるロケーションにアクセスするには、**[バックアップ]** をクリックし、作成したテーププールの名前をクリックします。
- バックアップの保存されたテープが、選択したプールに移動されます。

テープ ライブラリの他の使用法に関するヒント

- 新しいテープをロードするたびに完全インベントリを実行する必要はありません。時間を短縮するには、「インベントリ」セクションの「高速インベントリと完全インベントリとの組み合わせ」に記載されている手順に従います。
- 同じテープライブラリ上に他のプールを作成し、バックアップの保存先としてそれらのプールのいずれかを選択することができます。

テープ デバイスから起動したオペレーティング システムでの復元

テープ デバイスから起動したオペレーティング システムで復元を実行するには

1. Cyber Protectウェブコンソールにログインします。
2. **[デバイス]** をクリックし、バックアップされたコンピュータを選択します。
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。
5. 復元に必要なテープの一覧が表示されます。不足しているテープは灰色表示されています。テープデバイスのスロットが空いている場合、それらのテープをデバイスにロードします。
6. その他の復元設定を構成します。
7. **[復元を開始]** をクリックして復元処理を開始します。
8. 何らかの理由により必要なテープのいずれかがロードされていない場合、必要なテープの識別子を示すメッセージが表示されます。以下の手順を実行します。
   a. テープをロードします。
   b. 高速インベントリを実行します。
   c. **[概要]** > **[アクティビティ]** をクリックし、**[ユーザーによる操作が必要]** ステータスの復元アクティビティをクリックします。
   d. **[詳細の表示]** をクリックし、**[再試行]** をクリックして復元を続行します。

テープの保存されているバックアップが表示されない場合の対処

テープの内容が格納されているデータベースが、何らかの理由により、失われているか破損している可能性があります。

データベースを復元するには、次の手順を実行します。

1. 高速インベントリを実行します。

   警告
   インベントリの実行中に **[認識されないテープおよびインポートされたテープを空きテーププールに移動]** をオンにしないでください。このスイッチをオンにすると、すべてのバックアップが失われてしまう可能性があります。

2. [認識されないテープ] プールを**再スキャン**します。その結果、ロードされているテープ（複数の場合あり）の内容が表示されます。
3. 検出されたバックアップのいずれかが、再スキャンされていない他のテープにまたがっている場合、プロンプトの指示に従　　てそれらのテープをロードして、再スキャンを実行します。

ローカル接続されたテープ ドライブのブータブル メディアによる復元

ローカル接続されたテープ ドライブからブータブルメディアによる復元を実行するには、次の手順に従います。

1. 復元に必要なテープをテープ デバイスにロードします。
2. ブータブル メディアからコンピュータを起動します。
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. iSCSIインターフェイスを使用してテープデバイスを接続している場合は、「iSCSIおよびNDASデバイスの構成」に従ってデバイスを構成します。
5. **[テープ管理]** をクリックします。
6. **[インベントリ]** をクリックします。
7. **[インベントリを行うオブジェクト]** でテープデバイスを選択します。
8. **[開始]** をクリックしてインベントリの実行を開始します。
9. インベントリの実行が完了したら、**[閉じる]** をクリックします。
10. **[アクション]** > **[復元]** をクリックします。
11. **[データの選択]** をクリック後、**[参照]** をクリックします。
12. **[テープデバイス]** を展開してから、必要なデバイスを選択します。再スキャンを確認するメッセージが表示されます。**[はい]** をクリックします。
13. **[認識されないテープ]** プールを選択します。
14. 再スキャンするテープを選択します。プールのテープすべてを選択するには、**[テープ名]** 列ヘッダーの横にあるチェックボックスをオンにします。
15. パスワードで保護されたバックアップがテープに含まれている場合は、対応するチェックボックスをオンにして、**[パスワード]** ボックスにバックアップのパスワードを入力します。パスワードを入力しなかった場合、またはパスワードが間違っていた場合、バックアップは検出されません。再スキャン後にバックアップが何も表示されなかった場合に備え、このことを覚えておいてください。

    ヒント:異なるパスワードで保護された複数のバックアップがテープに含まれている場合は、それぞれのパスワードを順次入力して再スキャンを繰り返す必要があります。
16. **[開始]** をクリックして、再スキャンを開始します。その結果、ロードされているテープ（複数の場合あり）の内容が表示されます。

17. 検出されたバックアップのいずれかが、再スキャンされていない他のテープにまたがっている場合、プロンプトの指示に従　　てそれらのテープをロードして、再スキャンを実行します。
18. 再スキャンが完了したら、**[OK]** をクリックします。
19. **[アーカイブ ビュー]** で復元するデータのバックアップを選択して、復元するデータを選択します。**[OK]** をクリックすると、**[データの復元]** ページに、復元に必要なテープの一覧が表示されます。不足しているテープは灰色表示されています。テープ デバイスのスロットが空いている場合、それらのテープをデバイスにロードします。
20. その他の復元設定を構成します。
21. **[OK]** をクリックして復元を開始します。
22. 何らかの理由により必要なテープのいずれかがロードされていない場合、必要なテープの識別子を示すメッセージが表示されます。以下の手順を実行します。
    a. テープをロードします。
    b. 高速インベントリを実行します。
    c. **[概要]** > **[アクティビティ]** をクリックし、**[ユーザーによる操作が必要]** ステータスの復元アクティビティをクリックします。
    d. **[詳細の表示]** をクリックし、**[再試行]** をクリックして復元を続行します。

ストレージ ノードに接続されたテープ ドライブのブータブル メディアによる復元

ストレージ ノードに接続されたテープ ドライブのブータブルメディアによる復元を実行するには、次の手順に従います。

1. 復元に必要なテープをテープ デバイスにロードします。
2. ブータブル メディアからコンピュータを起動します。
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. **[復元]** をクリックします。
5. **[データの選択]** をクリック後、**[参照]** をクリックします。
6. **[パス]** ボックスに`bsp://<Storage Nodeアドレス>/<プール名>/`を入力します。`<Storage Nodeアドレス>`は目的のバックアップが格納されているStorage NodeのIPアドレスで、**<プール名>**はテーププールの名前です。**[OK]** をクリックして、プールの資格情報を指定します。
7. バックアップを選択してから、復元するデータを選択してください。**[OK]** をクリックすると、**[データの復元]** ページに、復元に必要なテープの一覧が表示されます。不足しているテープは灰色表示されています。テープ デバイスのスロットが空いている場合、それらのテープをデバイスにロードします。
8. その他の復元設定を構成します。
9. **[OK]** をクリックして復元を開始します。
10. 何らかの理由により必要なテープのいずれかがロードされていない場合、必要なテープの識別子を示すメッセージが表示されます。以下の手順を実行します。
    a. テープをロードします。
    b. 高速インベントリを実行します。

c. **[概要]** > **[アクティビティ]** をクリックし、**[ユーザーによる操作が必要]** ステータスの復元アクティビティをクリックします。
d. **[詳細の表示]** をクリックし、**[再試行]** をクリックして復元を続行します。

テープ管理

テープ デバイスの検出

テープデバイスを検出する場合、 バックアップソフトウェアでは、マシンに接続されているテープデバイスを検出し、その情報をテープ管理データベースに格納します。検出されたテープデバイスはRSMから無効化されます。

通常、テープデバイスは、製品がインストールされたマシンへの接続時に自動的に検出されます。ただし、次のような場合には、テープデバイスを検出する必要があります。

- テープ デバイスを接続または再接続した後。
- テープデバイスが接続されているマシンにバックアップソフトウェアをインストールまたは再インストールした後。

テープ デバイスを検出するには

1. **[設定]** > **[テープ管理]** をクリックします。
2. テープデバイスが接続されたマシンを選択します。
3. **[デバイスの検出]** をクリックします。接続されているテープデバイス、ドライブおよびスロットが表示されます。

テープ プール

バックアップソフトウェアでは、テープの論理グループであるテープ プールが使用されます。事前定義されたテーププールには、**認識されないテープ**、**インポートされたテープ**、**空きテープ**、**Acronis**があります。また、独自のカスタム プールを作成することができます。

Acronisプールとカスタムプールはバックアップロケーションとしても使用できます。

事前に定義されたプール

認識されないテープ

このプールは、サードパーティ製のアプリケーションによって書き込まれたテープで構成されます。このようなテープに書き込むには、テープを**空きテープ**プールに明示的に移動する必要があります。このプールから**空きテープ**プール以外のプールにテープを移動することはできません。

インポートされたテープ

このプールは、別のStorage Nodeやエージェントに接続されたテープデバイスのAcronis Cyber Protectによって書き込まれたテープで構成されます。このようなテープに書き込むには、テープを**空きテープ**プールに明示的に移動する必要があります。このプールから**空きテープ**プール以外のプールにテープを移動することはできません。

空きテープ

このプールは、空き（空の）テープで構成されます。他のプールからこのプールにテープを手動で移動できます。

テープを **[空きテープ]** プールに移動すると、テープが空にされます。テープにバックアップが含まれている場合は、  アイコンが表示されます。そのテープの上書きが開始されると、バックアップに関連したデータがデータベースから削除されます。

Acronis

独自のプールを作成しない場合に、バックアップ用にデフォルトで使用されるテーププールです。通常、このプールは、少数のテープが存在する 1 つのテープ ドライブに適用されます。

カスタム プール

別のデータを個別にバックアップする場合は、複数のプールを作成する必要があります。たとえば、次のような場合にカスタム プールを作成します。

- 社内の他の部門とは別にバックアップを実行する
- 他のコンピュータとは別にバックアップを実行する
- システム ボリュームとユーザー データのバックアップを別個に実行する

プールを使用した操作

プールの作成

プールを作成するには

1. **[設定]** > **[テープ管理]** をクリックします。
2. テープデバイスが接続されているコンピュータまたはStorage Nodeを選択し、このコンピュータの **[テーププール]** をクリックします。
3. **[プールの作成]** をクリックします。
4. プールの名前を指定します。
5. （オプション）**[テープを「空きテープ」プールから自動的に取り出す...]** チェックボックスをオフにします。オフにすると、特定の時点で新しいプール内に含まれているテープのみが、バックアップに使用されます。
6. **[作成]** をクリックします。

プールの編集

Acronisプールまたは独自のカスタムプールのパラメータを編集することができます。

プールを編集するには

1. **[設定]** > **[テープ管理]** をクリックします。
2. テープデバイスが接続されているコンピュータまたはStorage Nodeを選択し、このコンピュータの **[テーププール]** をクリックします。
3. 目的のプールを選択して **[プールの編集]** をクリックします。

4. プールの名前または設定を変更することができます。プールの設定の詳細については、「プールの作成」を参照してください。
5. **[保存]** をクリックして、変更を保存します。

プールの削除

削除できるのは、カスタム プールのみです。事前に定義されているテーププール（**認識されないテープ**、**インポートされたテープ**、**空きテープ**、および**Acronis**）は削除できません。

注意
プールの削除後は、そのプールがバックアップロケーションとして設定されている保護計画の編集を忘れずに行ってください。編集を行わなければ、それらの保護計画は失敗します。

プールを削除するには

1. **[設定]** > **[テープ管理]** をクリックします。
2. テープデバイスが接続されているコンピュータまたはStorage Nodeを選択し、このコンピュータの **[テーププール]** をクリックします。
3. 目的のプールを選択して、**[削除]** をクリックします。
4. 削除されるプールのテープを削除後に移動するプールを選択します。
5. **[OK]** をクリックして、プールを削除します。

テープの操作

別スロットへの移動

次の場合にこの処理を使用します。

- テープ デバイスから複数のテープを同時に取り出す必要があります。
- お使いのテープ デバイスにはメール スロットがなく、取り出すテープが取り外し不可能なマガジン（複数可）のスロットに入っています。

1 つのスロット マガジンのスロットにすべてのテープを移動してから、手動でマガジンを取り出す必要があります。

別のスロットにテープを移動するには

1. **[設定]** > **[テープ管理]** をクリックします。
2. テープデバイスが接続されているコンピュータまたはStorage Nodeを選択し、このコンピュータの **[テーププール]** をクリックします。
3. 目的のテープが格納されたプールをクリックして、目的のテープを選択します。
4. **[スロットに移動]** をクリックします。
5. 選択したテープを移動する新しいスロットを選択します。
6. **[移動]** をクリックして処理を開始します。

別のプールへの移動

この操作を使用して、1 つまたは複数のテープを別のプールに移動することができます。

テープを **[空きテープ]** プールに移動すると、テープが空にされます。テープにバックアップが含まれている場合は、  アイコンが表示されます。そのテープの上書きが開始されると、バックアップに関連したデータがデータベースから削除されます。

特定の種類のテープに関する注意事項

- 書き込み保護されたWORM（Write-Once-Read-Many）テープおよび一度記録されたWORMテープを **[空きテープ]** プールに移動することはできません。
- クリーニングテープは常に**認識されないテープ**プールに表示され、他のプールに移動することはできません。

テープを別のプールに移動するには

1. **[設定]** > **[テープ管理]** をクリックします。
2. テープデバイスが接続されているコンピュータまたはStorage Nodeを選択し、このコンピュータの **[テーププール]** をクリックします。
3. 必要なテープが含まれるプールをクリックし、目的のテープを選択します。
4. **[プールに移動]** をクリックします。
5. （オプション）選択したテープ用の別のプールを作成する場合は、**[プールの作成]** をクリックします。「プールの作成」 の説明に従って操作を実行します。
6. テープの移動先のプールを選択します。
7. **[移動]** をクリックして、変更を保存します。

注意
テープに復元可能なバックアップがあり、テープを別のプールに移動する場合は、移動処理が完了した時点で、必ずバックアップストレージ以下の格納域をリフレッシュしてください。バックアップは、元のバックアップ先に関係なく、2番目のプールで使用できます。

一覧の収集

インベントリ処理では、テープ デバイスにロードされているテープが検出され、名前が付いていないテープに名前が割り当てられます。

一覧の収集方法

インベントリを実行する方法には、以下の2つがあります。

高速インベントリ

エージェントまたはStorage Nodeは、テープのバーコードをスキャンします。バーコードを利用することによって、以前に使用されていたプールにテープを素早く戻します。

この方法を選択すると、同じコンピュータに接続された同じテープ デバイスで使用されたテープが認識されます。その他のテープは「**認識されないテープ**」プールに送られます。

テープライブラリがバーコードリーダーを搭載していない場合は、すべてのテープが「**認識されないテープ**」プールに送られます。テープを認識させるには、このセクションで後述するように、完全インベントリを実行するか、高速インベントリと完全インベントリを組み合わせて実行します。

完全インベントリ

エージェントまたはStorage Nodeは、以前に書きこまれたタグを読み取り、ロードされたテープの内容に関するその他の情報を分析します。この方法を選択すると、空のテープ、および同じソフトウェアによって書き込まれた（使用したテープデバイスとマシンを問わず）テープを認識します。

以下の表に、完全インベントリの結果テープが移動されるプールを示します。

テープの使用を実行	テープの読み込みを実行	テープの移動先プール
エージェント	同じエージェント	以前にテープが存在していたプール
	別のエージェント	**インポートされたテープ**
	Storage Node	**インポートされたテープ**
Storage Node	同じ Storage Node	以前にテープが存在していたプール
	別の Storage Node	**インポートされたテープ**
	エージェント	**インポートされたテープ**
サードパーティのバックアップアプリケーション	エージェントまたは Storage Node	**認識されないテープ**

一部のテープは、種類によって特定のプールに移動されます。

テープの種類	テープの移動先プール
空のテープ	**空きテープ**
書き込み保護された空きテープ	**認識されないテープ**
クリーニング テープ	**認識されないテープ**

高速インベントリは、テープ デバイス全体に対して適用できます。完全インベントリは、テープデバイス全体、個々のドライブ、またはスロットに対して適用できます。スタンドアロンのテープドライブの場合は、高速インベントリを選択しても、必ず完全インベントリが実行されます。

高速インベントリと完全インベントリの組み合わせ

テープ デバイス全体の完全インベントリには、時間がかかることがあります。少数のテープに対してインベントリを実行する場合は、次の手順に従います。

1. テープ デバイスで高速インベントリを実行します。
2. **[認識されないテープ]** プールをクリックします。インベントリを実行するテープを検索し、それが占有しているスロットを確認します。
3. それらのスロットの完全インベントリを実行します。

インベントリ終了後の操作

[認識されないテープ] プールまたは **[インポートされたテープ]** プールに配置されたテープにバックアップする場合、テープを [空きテープ] プールに**移動**してから、**[Acronis]** プールまたはカスタムプールに移動します。バックアップ先のプールが補充可能である場合、**空きテープ**プールにテープを残すことができます。

認識されないテーププールまたは**インポートされたテープ**プールに配置されたテープから復元する場合、テープを再スキャンする必要があります。テープは、再スキャン中に選択したプールに移動され、テープに保存されているバックアップはそのロケーションに表示されます。

操作手順

1. **[設定]** > **[テープ管理]** をクリックします。
2. テープデバイスが接続されたマシンを選択し、インベントリを実行するテープデバイスを選択します。
3. **[インベントリ]** をクリックします。
4. （オプション）高速インベントリを選択する場合、**完全インベントリ**をオフにします。
5. （オプション）**[認識されないテープおよびインポートされたテープを空きテーププールに移動]** をオンにします。

   警告
   テープに格納されているデータを上書きしても問題がないと確信している場合のみ、このスイッチを有効にしてください。

6. **[今すぐインベントリを開始]** をクリックしてインベントリの実行を開始します。

再スキャン

テープの内容に関する情報は、専用のデータベースに保存されています。再スキャン処理では、テープの内容が読み込まれ、データベースの情報とテープに保存されているデータが一致しない場合は、データベースがアップデートされます。処理によって検出されたバックアップは、指定したプールに移動されます。

1 回の操作で、1 つのプールの複数のテープを再スキャンできます。選択できるのは、オンライン テープのみです。

マルチストリーミングまたはマルチストリーミングとマルチプレクシングの両方によって作成されたバックアップでテープを再スキャンするには、そのバックアップの作成に使用したのと同じかそれ以上の台数のドライブが必要です。このようなバックアップはスタンドアロンのテープドライブから再スキャンすることはできません。

次の場合に再スキャンを実行します。

- ストレージ ノードまたは管理対象のコンピュータのデータベースが失われたり、破損したりした場合。

- データベース内のテープに関する情報が古くなった場合（たとえば、テープの内容が別のストレージノードまたはエージェントによって変更されたなど）。
- ブータブル メディアでの作業中に、テープに保存されているバックアップにアクセスする場合。
- テープに関する情報をデータベースから誤って削除した場合。削除されたテープを再スキャンすると、そのテープに保存されているバックアップがデータベースに登録され、データを復元できるようになります。
- バックアップがテープから手動または保持ルールによって削除され、データを復元するために、そのバックアップを利用できるようにする場合。そのようなテープを再スキャンする前に、テープを取り出し、データベースからそのテープに関する情報を削除してから、そのテープをテープデバイスに再挿入します。

テープを再スキャンするには

1. **[設定]** > **[テープ管理]** をクリックします。
2. テープデバイスが接続されているコンピュータまたはStorage Nodeを選択し、このコンピュータの **[テープデバイス]** をクリックします。
3. テープをロードしたテープデバイスを選択します。
4. 高速インベントリを実行します。

   注意
   インベントリの実行中に **[認識されないテープおよびインポートされたテープを空きテーププールに移動]** スイッチを有効にしないでください。

5. **[認識されないテープ]** プールを選択します。高速インベントリの結果、このプールに大半のテープが送られます。他の任意のプールを再スキャンすることもできます。
6. [オプション] 個々のテープのみ再スキャンする場合は、それらを選択します。
7. **[再スキャン]** をクリックします。
8. 新たに検出されたバックアップが配置されるプールを選択します。
9. 必要な場合は、**[テープに保存されたディスクのバックアップからのファイルの復元を有効にする]** チェックボックスをオンにします。

   詳細このチェック ボックスをオンにすると、テープ デバイスが接続されているコンピュータのハード ディスクにソフトウェアが特別な補助ファイルを作成します。これらの補助ファイルがそのままの状態を保持していれば、ディスク バックアップからファイルを復元できます。テープにアプリケーション認識型バックアップが含まれている場合は、このチェックボックスを必ずオンにしてください。それ以外の場合、これら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。
10. パスワードで保護されたバックアップがテープに含まれている場合は、対応するチェックボックスをオンにし、そのバックアップのパスワードを指定します。パスワードを入力しなかった場合、またはパスワードが間違っていた場合、バックアップは削除されません。再スキャン後にバックアップが何も表示されなかった場合に備え、このことを覚えておいてください。

    ヒント:異なるパスワードで保護された複数のバックアップがテープに含まれている場合は、それぞれのパスワードを順次入力して再スキャンを繰り返す必要があります。
11. **[再スキャンの開始]** をクリックして、再スキャンを開始します。

結果:選択したテープは選択したプールに移動されます。そのテープに保存されだバックアップはこのプールで見つかります。バックアップが複数のテープに渡る場合、そのすべてのテープが再スキャンされない限りプールに表示されません。

名前の変更

ソフトウェアが新しいテープを検出すると、自動的に次の形式の名前を割り当てます。**Tape XXX**。**XXX**は一意の数値です。テープには、順に番号が付けられます。名前の変更処理によって、テープの名前を手動で変更できます。

テープの名前を変更するには

1. **[設定]** > **[テープ管理]** をクリックします。
2. テープデバイスが接続されているコンピュータまたはStorage Nodeを選択し、このコンピュータの **[テーププール]** をクリックします。
3. 目的のテープが格納されたプールをクリックして、目的のテープを選択します。
4. **[名前の変更]** をクリックします。
5. 選択したテープの新しい名前を入力します。
6. **[名前の変更]** をクリックして、変更を保存します。

消去

テープを物理的に消去すると、そのテープに保存されているバックアップはすべて削除され、バックアップに関する情報がデータベースから削除されます。ただし、テープ自体に関する情報はデータベースに残ります。

テープが **[認識されないテープ]** プールまたは **[インポートされたテープ]** プール内に存在していた場合、消去後に **[空きテープ]** プールに移動されます。その他のプール内に存在するテープは移動されません。

テープを消去するには

1. **[設定]** > **[テープ管理]** をクリックします。
2. テープデバイスが接続されているコンピュータまたはStorage Nodeを選択し、このコンピュータの **[テーププール]** をクリックします。
3. 必要なテープが含まれるプールをクリックし、目的のテープを選択します。
4. **[消去]** をクリックします。処理を確認するメッセージが表示されます。
5. 消去方法として 高速または完全を選択します。
6. **[消去]** をクリックして処理を開始します。
   詳細:消去操作をキャンセルすることはできません。

取り出し

テープ ライブラリからテープを正常に取り出すには、テープ ライブラリがメール スロットを備えており、そのスロットが、ユーザーまたは他のソフトウェアによってロックされていない必要があります。

テープを取り出すには

1. **[設定]** > **[テープ管理]** をクリックします。
2. テープデバイスが接続されているコンピュータまたはStorage Nodeを選択し、このコンピュータの **[テーププール]** をクリックします。
3. 必要なテープが含まれるプールをクリックし、目的のテープを選択します。
4. **[取り出し]** をクリックします。テープの説明を入力するように求めるメッセージが表示されます。テープを保管する物理的な場所の説明を記載しておくことをお勧めします。復元中、この説明が表示されるのでテープを簡単に見つけることができます。
5. **[OK]** をクリックして処理を開始します。

テープを手動または自動で取り出したら、そのテープに名前を書くことをお勧めします。

削除

削除処理によって、選択したテープに保存されているバックアップに関する情報、およびテープ自体に関する情報がデータベースから削除されます。

削除できるのは、オフラインの（取り出された）テープのみです。

テープを削除するには

1. **[設定]** > **[テープ管理]** をクリックします。
2. テープデバイスが接続されているコンピュータまたはStorage Nodeを選択し、このコンピュータの **[テーププール]** をクリックします。
3. 目的のテープが格納されたプールをクリックして、目的のテープを選択します。
4. **[削除]** をクリックします。処理を確認するメッセージが表示されます。
5. **[削除]** をクリックしてテープを削除します。

誤ってテープを削除してしまった場合の手順

消去されたテープとは異なり、削除されたテープのデータは、物理的に削除されていません。このようにして、削除されたテープに保存されていたバックアップを再度使用可能にできます。手順は次のとおりです。

1. テープをテープ デバイスにロードします。
2. 高速インベントリを実行して、テープを検出します。

> **注意**
> インベントリの実行中に **[認識されないテープおよびインポートされたテープを空きテーププールに移動]** スイッチを有効にしないでください。

3. 再スキャンを実行して、テープに保存されているデータとデータベースを照合します。

テープセットの指定

この操作では、テープのテープセットを指定できます。

テープセットとは、同じプール内にあるテープのグループのことです。

バックアップのオプションでテープセットを指定する場合は変数を使用できますが、ここでは文字列値のみ指定できます。

この操作は、所定のルールに従って特定のテープをバックアップしたい場合に実行します（月曜日のバックアップをテープ1に、火曜日のバックアップをテープ2に、など）。必要とされるテープそれぞれに所定のテープセットを指定したうえで、同じテープセットを指定するか、バックアップのオプションで適切な変数を使用します。

上記の例であれば、テープセット**月曜日**をテープ1に、**火曜日**をテープ2に、というように指定します。バックアップのオプションで、[**平日**] を指定します。このようにすると、適切なテープが週の該当する曜日に使用されます。

1本または複数本のテープのテープセットを指定するには

1. **[設定]** > **[テープ管理]** をクリックします。
2. テープデバイスが接続されているコンピュータまたはStorage Nodeを選択し、このコンピュータの **[テーププール]** をクリックします。
3. 必要なテープが含まれるプールをクリックし、目的のテープを選択します。
4. **[テープセット]** をクリックします。
5. テープセット名を入力します。選択したテープに別のテープがすでに指定されていた場合は、置き換えられます。別のを指定せずにテープセットからテープを除外するには、既存のテープセット名を削除します。
6. **[保存]** をクリックして、変更を保存します。

ストレージ ノード

Storage Nodeは、企業データの保護に必要なさまざまなリソース（企業のストレージ容量、ネットワークの帯域幅、本番サーバーのCPU負荷など）の使用を最適化するように設計されたサーバーです。これは、社内バックアップの専用ストレージロケーションとして機能するロケーション（管理対象ロケーション）を構築し、管理することで実現できます。

Acronis Storage Nodeの主な目的は、テープドライブやライブラリへの集中アクセスを可能にすることです。例えば、複数のデバイスから同一のテープドライブまたはライブラリ（テープの管理対象の格納域）にデータをバックアップしたりリカバリしたりする処理などが、集中アクセスにあたります。

別のユースケースは、高度な重複除外機能を有効にして、複数のデバイスにまたがって存在するデータで相互的な重複除外を実行し、そのデータを単一のロケーション（重複除外を有効にした管理対象の格納域）に保存するというものです。

Storage Nodeとカタログサービスのインストール

Storage Node をインストールする前に、マシンがシステム要件を満たしていることを確認してください。

Storage Nodeとカタログサービスは別々のマシンにインストールすることをお勧めします。カタログサービスを実行するマシンのシステム要件は、"カタログ作成のベストプラクティス"（617ページ）に記載されています。

Storage Node およびカタログサービスをインストールするには

1. 管理者としてログオンし、Acronis Cyber Protect プログラムの設定を起動します。
2. （オプション）プログラムの設定の言語を変更するには、**[言語の設定]** をクリックします。
3. ライセンス契約とプライバシーステートメントに同意して、**[次へ]** をクリックします。
4. **[プロテクション エージェントのインストール]** をクリックします。
5. **[インストール設定のカスタマイズ]** をクリックします。
6. **[インストールする項目]** の横にある **[変更]** をクリックします。
7. インストールするコンポーネントを選択します。
   - Storage Nodeをインストールする場合は、**[Storage Node]** チェックボックスを選択します。**[エージェントfor Windows]** チェックボックスが自動的にオンに設定されます。
   - カタログサービスをインストールする場合は、**[カタログサービス]** チェックボックスを選択します。
   - このコンピュータに他のコンポーネントをインストールしない場合は、対応するチェック ボックスをオフにします。

   ［**完了**］をクリックして先に進んでください。
8. コンポーネントを登録する管理サーバーを指定します。
   a. **[Acronis Cyber Protect Management Server]** の横で **[指定]** をクリックします。
   b. Management Serverがインストールされているコンピュータのホスト名または IPアドレスを指定します。
   c. 管理サーバーの管理者の資格情報または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、"手順1:登録トークンの生成"（175ページ）を参照してください。
   d. **[完了]** をクリックします。
9. 指定するよう求められたら、Storage Node やカタログサービスがインストールされているマシンを、組織に追加するか、部署の 1 つに追加するかを選択します。
   このプロンプトは、複数の部署を管理する場合、または部署が 1 つ以上ある組織を管理する場合に表示されます。それ以外の場合は、通知されることなく、マシンは管理対象の部署または組織に追加されます。詳細については、「管理者と部署」を参照してください。
10. （オプション）「インストール設定のカスタマイズ」の説明に従って他のインストール設定を変更します。
11. **[インストール]** をクリックして、インストールを続行します。
12. インストールが完了した後、［**閉じる**］をクリックします。

カタログサービスをAcronis Cyber Protect 15 Update 4にアップデートする

Acronis Cyber Protect 15 Update 4を使用して、カタログサービスを新しいバージョンにアップデートします。以前のバージョンで作成されたカタログデータと新しいバージョンの間には、直接の互換性がありません。

Acronis Cyber Protect 15 Update 4へのアップデート中、このデータを新しいバージョンのカタログサービスに手動でマイグレーションできます。または、マイグレーションをスキップして、後でカタロ

グデータを再作成することもできます。カタログデータを再作成する場合は、マイグレーションよりも時間がかかります。

カタログデータをマイグレーションするには

1. カタログサービスがインストールされているマシンで、Acronis Cyber Protectのプログラムの設定を実行します。
2. ライセンス契約とプライバシーステートメントに同意して、**[次へ]** をクリックします。
3. **[分かりました]** チェックボックスを選択して、**[アップデート]** をクリックします。
4. **[一時フォルダを指定する]** チェックボックスを選択します。
5. カタログデータをエクスポートするフォルダを指定します。
   エクスポートデータは暗号化されます。一時フォルダは、マイグレーションが完了すると自動的に削除されます。
6. **[完了]** をクリックします。

カタログデータのマイグレーションをスキップするには

1. カタログサービスがインストールされているマシンで、Acronis Cyber Protectのプログラムの設定を実行します。
2. ライセンス契約とプライバシーステートメントに同意して、**[次へ]** をクリックします。
3. **[分かりました]** チェックボックスを選択して、**[アップデート]** をクリックします。
4. **[一時フォルダを指定する]** チェックボックスをクリアします。
5. **[完了]** をクリックします。
6. 選択内容を確認入力します。

そのため、Acronis Cyber Protect 15 Update 4へのアップデート後、既存のカタログデータは利用できなくなります。カタログデータを再作成するには、バックアップを実行します。

注意
カタログサービス、Storage Node、および管理サーバーが別々のマシンで実行されている場合、この順序ですべてのマシンをAcronis Cyber Protect 15 Update 4にアップデートしてください。

1. 管理サーバー
2. Storage Node
3. カタログサービス

管理対象ロケーションの追加

管理対象ロケーションは次の場所に設定することができます。

- ローカルフォルダ:
  - Storage Node のローカルハードドライブ
  - オペレーティングシステムがローカル接続されたデバイスと認識する SAN ストレージ
- ネットワークフォルダ:
  - SMB/CIFS 共有
  - オペレーティングシステムがネットワークフォルダと認識する SAN ストレージ

  - NAS
- Storage Node にローカル接続されたテープデバイス。

  テープベースのロケーションは、テーププールの形式で作成されます。デフォルトでは 1 つのテーププールが存在します。このセクションで後述するように、必要に応じて別のテーププールを作成できます。

ローカルフォルダまたはネットワークフォルダに管理対象ロケーションを作成する手順

1. 次のいずれかを実行します。
   - **[バックアップストレージ]** > **[ロケーションの追加]** をクリックし、**[Storage Node]** をクリックします。
   - 保護計画を作成する場合は、**[バックアップ先]** > **[ロケーションの追加]** をクリックし、**[Storage Node]** をクリックします。
   - **[設定]** > **[Storage Node]** をクリックし、ロケーションを管理する Storage Node を選択して、**[ロケーションの追加]** をクリックします。
2. **[名前]** で、ロケーションの一意の名前を指定します。「一意」とは、同じ Storage Node が管理するロケーションで、同じ名前のものが他に存在しないことを意味します。
3. （オプション）ロケーションを管理する Storage Node を選択します。手順 1 で最後のオプションを選択した場合は、Storage Node を変更することはできません。
4. エージェントがロケーションへのアクセスに使用する Storage Node の名前または IP アドレスを選択します。

   デフォルトでは、Storage Node の名前が選択されています。DNS サーバーが名前から IP アドレスを解決できない場合（アクセスエラーが発生します）、この設定の変更が必要な場合があります。後でこの設定を変更するには、**[バックアップストレージ]** > 目的のロケーション > **[編集]** をクリックし、**[アドレス]** フィールドの値を変更します。
5. フォルダパスを入力するか、目的のフォルダを参照します。
6. **[完了]** をクリックします。指定されたフォルダへのアクセスがチェックされます。
7. （オプション）ロケーションでのバックアップ重複除外を有効にします。

   重複除外によって重複するディスクブロックを解消することで、バックアップトラフィックを最小限に抑え、ロケーションに格納されるバックアップのサイズを削減できます。

   重複除外の制限の詳細については、「重複除外の制限」を参照してください。
8. （重複除外を有効にした場合のみ）**[重複除外データベースのパス]** フィールドの値を指定または変更します。

   これは、Storage Node のローカルハードドライブ上のフォルダにする必要があります。システムのパフォーマンスを低下させないために、重複除外データベースと管理対象ロケーションは別々のディスクに作成することをお勧めします。

   重複除外データベースの詳細については、「重複除外のベストプラクティス」を参照してください。
9. （オプション）暗号化を使用してロケーションを保護するかどうかを選択します。ロケーションに書き込まれるすべてのデータは暗号化され、ロケーションから読み取られるすべてのデータはStorage Nodeによって透過的に暗号化解除されます。このとき、Storage Nodeに保存されているロケーション専用の暗号化キーが使用されます。

   暗号化の詳細については、「ロケーションの暗号化」を参照してください。

10. （オプション）そのロケーションに格納されているバックアップをカタログ化するかどうかを選択します。データカタログを使用すると、必要なバージョンのデータを簡単に見つけて復元対象として選択することができます。
    管理サーバーに複数のカタログサービスが登録されている場合、ロケーションに保存されるバックアップのカタログ化を行うサービスを選択できます。
    「カタログ化の有効化または無効化方法」に記載されているとおり、カタログ化は後で有効または無効にできます。
11. **[完了]** をクリックしてロケーションを作成します。

テープデバイスに管理対象ロケーションを作成する手順

1. **[バックアップストレージ]** > **[ロケーションの追加]** をクリックするか、保護計画の作成時に **[バックアップ先]** > **[ロケーションの追加]** をクリックします。
2. **[テープ]** をクリックします。
3. （オプション）ロケーションを管理する Storage Node を選択します。
4. 「プールの作成」の手順 4 以降を実行します。

注意
デフォルトでは、エージェントは Storage Node 名を使用して管理対象のテープベースのロケーションにアクセスします。エージェントがStorage NodeのIPアドレスを使用するようにするには、**[バックアップストレージ]** > 目的のロケーション > **[編集]** をクリックし、**[アドレス]** フィールドの値を変更します。

重複除外

重複除外の制限

一般的な制限

暗号化されたバックアップは重複除外できません。重複除外と暗号化を同時に使用したい場合、バックアップを暗号化せずに、重複除外と暗号化の両方が有効なロケーションを指定します。

ディスクレベル バックアップ

ディスク ブロックの重複除外は、クラスター サイズまたはブロック サイズとも呼ばれるボリュームのアロケーションユニット サイズが、4KB で割り切れない場合は実行できません。

注意
ほとんどのNTFSボリュームやext3ボリュームのアロケーションユニットサイズは、4KBです。そのため、ブロック レベルで重複除外できます。ブロック レベルの重複除外で使用できるその他のアロケーションユニット サイズは、8KB、16KB、64KB などです。

ファイルレベルのバックアップ

ファイルが暗号化されている場合、ファイルの重複除外は実行できません。

重複除外とNTFSデータストリーム

NTFSファイルシステムでは、ファイルが1つ以上の追加のデータセット（代替データストリーム）と関連付けられることがあります。

このようなファイルをバックアップする場合、代替データ ストリームもすべてバックアップされます。ただし、ファイルそのものが重複除外された場合でも、これらのストリームは重複除外されません。

重複除外のベスト プラクティス

重複除外は、多くの要因に左右される複雑なプロセスです。

重複除外の処理速度に影響を及ぼす最も重要な要因は、次のとおりです。

- 重複除外データベースへのアクセス速度
- ストレージ ノードの RAM 容量
- Storage Nodeで作成される重複除外ロケーションの数

重複除外のパフォーマンスを高めるには、推奨事項に従う必要があります。

重複除外データベースと重複除外ロケーションを別の物理デバイスに配置する

重複除外データベースには、ロケーションに保存されているすべての項目のハッシュ値が保存されます。ただし、暗号化されたファイルなどの重複除外できない項目は除きます。

重複除外データベースへのアクセス速度を上げるには、データベースとロケーションを別々の物理デバイスに配置する必要があります。

ロケーションとデータベースに専用デバイスを割り当てる方法が最適です。この方法が不可能である場合は、少なくとも、オペレーティングシステムがある同じディスクにロケーションまたはデータベースを配置しないでください。この配慮が必要な理由は、オペレーティング システムはハード ディスクでの読み取り/書き込みを多く実行するからです。これらの処理が実行されると、重複除外の実行速度が大幅に低下します。

重複除外データベースのディスクを選択する

- データベースは、固定ドライブに存在する必要があります。重複除外データベースを、取り外し可能な外部ドライブに置かないでください。
- データベースへのアクセス時間を最小化するには、マウントされたネットワークボリュームではなく、直接接続されたドライブに保存します。ネットワーク遅延により、重複除外のパフォーマンスが大幅に低下する場合があります。
- 重複除外データベースに必要とされるディスク領域は、次の計算式で予測することができます。

$$S=U*90/65536+10$$

ここでは

Sはディスクサイズ（単位は GB）です。

Uは重複除外データ ストアに保存される重複のないデータの予測容量（単位は GB）です。

例えば、重複除外データストアに保存される重複のないデータの予測容量が U=5TB である場合、重複除外データベースには、以下のように最低空き領域が必要です。

S = 5000 * 90 / 65536 +10 = 17 GB

重複除外ロケーションのディスクを選択する

データの消失を防ぐために、RAID10、5、または 6 の利用をお勧めします。フォールトトレラントでないため、RAID 0 は推奨されません。転送速度が比較的遅いため、RAID 1 は推奨されません。ローカルディスクまたは SAN は利用可能ですが、最適ではありません。

40～160MB の RAM（重複のないデータ 1TB あたり）

上限に達すると重複除外は停止しますが、バックアップと復元は引き続き機能します。Storage Node に RAM を追加すると、次のバックアップで重複除外が再開します。一般的に、RAM が増えると、保存できる一意のデータのボリュームが大きくなります。

各Storage Nodeでは重複除外ロケーションを1つに制限する

Storage Nodeでは、作成する重複除外ロケーションを1つのみにすることを強く推奨します。複数作成すると、利用可能なRAMのボリューム全体が、格納域の数に応じて分散される場合があります。

アプリケーション間でリソースの競合が発生しないようにする

Database Management Systems（DBMS）や Enterprise Resource Planning（ERP）システムなど、システム リソースを多く必要とするアプリケーションは、ストレージ ノードのコンピュータで実行しないようにします。

最低 2.5GHz のクロック レートを発揮するマルチコア プロセッサー

最低 4 コアで構成され、最低 2.5GHz のクロックレートのプロセッサーを使用することを推奨します。

ロケーションの十分な空き領域

ターゲットでの重複除外には、バックアップデータがロケーションに保存された直後に使用する領域と同程度の空き領域が必要になります。ソースで圧縮または重複除外を行っていない場合、この値は特定のバックアップ操作でバックアップされた元のデータと同じサイズになります。

高速 LAN

1 Gbit LAN を推奨します。この LAN では、重複除外により 5～6 のバックアップ操作を並行して実行できます。この際、実行速度が大幅に低下することはありません。

データの内容が類似している複数のコンピュータをバックアップする前に、代表的な 1 台のコンピュータをバックアップする

内容が類似している複数のコンピュータをバックアップするときは、1 台のコンピュータを最初にバックアップし、バックアップされたデータのインデックス付けが完了するまで待つことをお勧めします。インデックス付けの実行後、効率的な重複除外により、他のコンピュータはより迅速にバックアップされます。最初のコンピュータのバックアップに対してインデックス付けが実行されているため、多くのデータが既に重複除外データ ストアに含まれています。

異なるコンピュータを異なる時間帯にバックアップする

多くのコンピュータをバックアップする場合は、時間をずらしてバックアップ操作を展開していきます。時間をずらすことで、さまざまなスケジュールで複数の保護計画を作成します。

ロケーションの暗号化

暗号化によってロケーションを保護する場合、ロケーションに書き込まれるすべてのデータは暗号化され、ロケーションから読み取られるすべてのデータはStorage Nodeで透過的に暗号化解除されます。このとき、ノードに保存されているロケーション専用の暗号化キーが使用されます。ストレージメディアが盗まれたり権限のない人物によってアクセスされた場合でも、ロケーションの内容はStorage Nodeにアクセスしなければ、暗号化解除できません。

この暗号化は、保護計画で指定され、エージェントによって実行されるバックアップの暗号化とは関係ありません。既にバックアップが暗号化されている場合、Storage Node側の暗号化は、エージェントによって実行される暗号化よりも優先的に適用されます。

暗号化を使用してロケーションを保護するには

1. 暗号化キーの生成に使用する単語（パスワード）を指定して確認します。
   単語は大文字と小文字が区別されます。この単語はロケーションを別のStorage Nodeに接続するときにのみ要求されます。
2. 次の暗号化アルゴリズムのいずれかを選択します。
   - **[AES 128]**: ロケーションの内容は、128ビットキーの高速暗号化標準（AES）のアルゴリズムを使用して暗号化されます。
   - **[AES 192]**: ロケーションの内容は、192ビットキーのAESアルゴリズムを使用して暗号化されます。
   - **[AES 256]**: ロケーションの内容は、256ビットキーのAESアルゴリズムを使用して暗号化されます。
3. **[OK]** をクリックします。

AES 暗号化アルゴリズムは、暗号ブロック連鎖（CBC）モードで動作し、ランダムに生成されるキーを使用します。キーの長さは 128、192、または 256 ビットからユーザーが指定できます。キーのサイズが大きいほどロケーションに保存されたバックアップを暗号化する時間は長くなりますが、バックアップの安全性は高まります。

次に、暗号化キーは、選択された単語の SHA-256 ハッシュをキーとして使用して、AES-256 で暗号化されます。単語自体はディスクに保存されませんが、単語のハッシュがベリファイに使用されます。この2段階のセキュリティにより、バックアップは許可されていないアクセスから保護されますが、失われた単語を復元することはできません。

カタログ作成

データ カタログ

データカタログを使用すると、必要なバージョンのデータを簡単に見つけて復元対象として選択することができます。データカタログには、カタログ化が有効にされる、または有効にされた、管理対象ロケーションに保存されているデータが表示されます。

[カタログ] セクションは、管理サーバーに1つ以上のカタログサービスが登録されている場合にのみ、**[バックアップストレージ]** タブに表示されます。カタログサービスのインストールについては、「Storage Node とカタログサービスのインストール」を参照してください。

[カタログ] セクションは、組織管理者に対してのみ表示されます。

制限事項

カタログは、物理マシンのディスクレベルおよびファイルレベルのバックアップ、仮想マシンのバックアップに対してのみサポートされています。

次のデータはカタログには表示されません。

- 暗号化されたバックアップのデータ
- テープデバイスにバックアップされたデータ
- クラウドストレージにバックアップされたデータ
- 製品バージョンが 12.5 よりも前の Acronis Cyber Protect でバックアップされたデータ

復元するバックアップ済みデータの選択

1. **[バックアップストレージ]** > **[カタログ]** をクリックします。
2. 管理サーバーに複数のカタログサービスが登録されている場合、ロケーションに保存されるバックアップのカタログ化を行うサービスを選択します。

   注意
   ロケーションをカタログ化するサービスを表示するには、**[バックアップ]** > **[ストレージ]** > **[ロケーション]** > **[ロケーション]** でロケーションを選択し、**[詳細]** をクリックします。

3. 選択したカタログサービスによってカタログ化された管理対象ロケーションにバックアップされたマシンが表示されます。
   参照するか、検索を使用して、復元するデータを選択します。
   - **参照**
     マシンをダブルクリックして、バックアップ済みのディスク、ボリューム、フォルダ、ファイルを表示します。

     ディスクをリカバリするには、次のアイコンが付いたディスクを選択します。 

ボリュームを復元するには、ボリュームを含むディスクをダブルクリックし、ボリュームを選択します。

ファイルおよびフォルダを復元するには、それらがあるボリュームを参照します。フォルダのアイコンが付いたボリュームを参照できます。 

- **検索**

  検索フィールドに、目的のデータアイテムを識別する情報（マシン名、ファイル名、フォルダ名、ディスクラベルなど）を入力し、**[検索]** をクリックします。

  アスタリスク（*）と疑問符（?）をワイルドカードとして使用できます。

  検索の結果、名前の全部または一部が入力した値と一致するバックアップ済みデータアイテムの一覧が表示されます。

4. デフォルトでは、データは最新の復元可能な時点に戻されます。1 つのアイテムを選択した場合は、**[バージョン]** ボタンを使用して、復元ポイントを選択できます。
5. 必要なデータを選択して、次のいずれかを実行します。
   - **[復元]** をクリックして、「復元」の説明に従って、復元操作のパラメータを設定します。
   - （ファイルおよびフォルダの場合のみ）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。

カタログ作成のベストプラクティス

カタログ作成のパフォーマンスを向上させるには、以下の推奨事項に従ってください。

インストール

カタログサービスとStorage Nodeは別々のマシンにインストールすることをお勧めします。これらのコンポーネントを同じマシンにインストールすると、CPUリソースとRAMリソースについて競合が発生します。

複数のStorage NodeがManagement Serverに登録されている場合は、インデックス付けまたは検索のパフォーマンスが低下しない限り、1つのカタログサービスだけで十分です。たとえば、カタログ作成が24時間365日稼働している（つまり、カタログ作成アクティビティ間に一時停止がない）ことに気づいた場合は、別のマシンにもう1つカタログサービスをインストールします。その後、管理対象ロケーションの一部を削除し、新しいカタログサービスを使用して作成し直します。これらのロケーションに格納されているバックアップはそのまま保持されます。

システム要件

パラメータ	最小値	推奨値
CPUコアの数	2	4以上
RAM	8GB	16GB以上
ハード ディスク	7200 rpm HDD	SSD

Storage Nodeがインストールされているマシンとカタログサービスがインストールされているマシンの間のネットワーク接続	100Mbps	1Gbps

カタログ化の有効化または無効化方法

管理対象ロケーションのカタログ化が有効であれば、バックアップが作成されるのと同時に、ロケーションを指定された各バックアップの内容がデータカタログに追加されます。

カタログ化は管理対象ロケーションの追加時、または後で有効にできます。カタログ化を有効にすると、ロケーションに保存されそれ以前にはカタログ化されていなかったすべてのバックアップが、ロケーションへの次のバックアップ後にカタログ化されます。

特に、同じロケーションへ多くのマシンをバックアップする場合、カタログ化プロセスは時間がかかることがあります。カタログ化は、いつでも無効にできます。無効になる前に作成されたバックアップをカタログにする処理が完了します。新しく作成されたバックアップはカタログに含められません。

既存のロケーションに対してカタログ化を構成するには

1. **[バックアップストレージ]** > **[ロケーション]** をクリックします。
2. **[ロケーション]** をクリックして、カタログを構成する管理対象ロケーションを選択します。
3. **[編集]** をクリックします。
4. **[カタログサービス]** スイッチを有効または無効にします。
5. **[完了]** をクリックします。

システム設定

これらの設定はオンプレミスデプロイでのみ使用できます。

これらの設定にアクセスするには、**[設定]** > **[システム設定]** をクリックします。

[システム設定] セクションは、組織管理者に対してのみ表示されます。

電子メールによる通知

Management Serverから送信されるすべての電子メール通知で共通のグローバル設定を構成できます。

デフォルトのバックアップオプションでは、バックアップ中に発生するイベントについてのみ、これらの設定を上書きできます。この場合、グローバル設定はバックアップ以外の処理に対して有効になります。

保護計画を作成する場合、グローバル設定を使用するか、またはデフォルトのバックアップオプションで指定した設定を使用するかを選択できます。この計画専用にカスタマイズされた値で上書きすることもできます。

重要
Eメール通知のグローバル設定を変更すると、グローバル設定を使用するすべての保護計画に影響します。

これらの設定を構成する前に、**電子メールサーバー**設定が構成されていることを確認します。

電子メール通知のグローバル設定を構成するには

1. **[設定]** > **[システム設定]** > **[電子メール通知]** の順にクリックします。
2. **[受信者の電子メールアドレス]** フィールドに送信先電子メールアドレスを入力します。複数のアドレスをセミコロンで区切って入力することもできます。
3. （オプション）**[件名]** で、電子メール通知の件名を変更します。
   たとえば次のような変数を使用できます。
   - **[アラート]** - アラート概要。
   - **[デバイス]** - デバイス名。
   - **[計画]** - アラートが生成された計画の名前。
   - [ManagementServer] - 管理サーバーがインストールされているマシンのホスト名。
   - **[部署]** - マシンが属している部署名。

   デフォルトの件名は、**[アラート] デバイス: [デバイス] 計画: [計画]**
4. （オプション）**[アクティブなアラートに関する日次概要]** チェックボックスをオンにし、次のいずれかを実行します。
   a. 概要が送信される時刻を選択します。
   b. （オプション）**[[アクティブアラートなし] メッセージを送信しない]** チェックボックスをオンにします。
5. （オプション）電子メール通知で使用する言語を選択します。

6. 通知を受信するイベントのチェックボックスを選択します。発生する可能性のあるすべてのアラートのリストから選択できます（重要度別）。
7. **[保存]** をクリックします。

電子メールサーバー

Management Serverから電子メール通知を送信するために使用される電子メールサーバーを指定できます。

電子メールサーバーを指定する

1. **[設定]** > **[システム設定]** > **[電子メールサーバー]** をクリックします。
2. **[電子メールサービス]** で、次のいずれかを選択します。
   - **カスタム**
   - **Gmail**
   - **Yahoo Mail**
   - **Outlook.com**
3. （カスタム電子メールサービスのみ）次の設定を指定します。
   - **[SMTP サーバー]**に送信メール サーバー（SMTP）の名前を入力します。
   - **[SMTP サーバー]**に送信メール サーバーのポートを入力します。デフォルトでは、ポートは 25 に設定されます。
   - SSLまたはTLS暗号化を使用するかどうかを選択します。暗号化を無効にするには **[なし]** を選択してください。
   - SMTP サーバーに認証が必要な場合、**[SMTPサーバーには認証が必要です]** チェック ボックスを選択してから、SMTP サーバーにメッセージを送信するために使用されるアカウントの資格情報を指定します。SMTP サーバーで認証が必要かどうかわからない場合は、ネットワーク管理者または電子メール サービスプロバイダーに問い合わせてください。
4. （Gmail、Yahoo Mail、Outlook.comのみ）メッセージを送信するために使用するアカウントの資格情報を指定します。
5. （カスタム電子メールサービスのみ）**[差出人]** に差出人の名前を入力します。この名前は電子メール通知の**差出人**フィールドに表示されます。このフィールドを空にすると、メッセージには手順3または4で指定されたアカウントが含まれます。
6. （オプション）**[テストメッセージを送信する]** をクリックして、指定した設定で電子メール通知が正常に機能するかどうかを確認します。テストメッセージを送信する電子メールアドレスを入力します。

セキュリティ

これらのオプションを使用して、Acronis Cyber Protectオンプレミス配置のセキュリティを拡張します。

非アクティブのユーザーをログアウトさせる時間

このオプションを使用して、ユーザーが非アクティブだったために行われる自動ログアウトのタイムアウト時間を指定できます。設定されたタイムアウト時間が残り 1 分になると、ログインを継続するよう促すメッセージがユーザーに表示されます。継続しない場合、ユーザーはログアウトされ、保存されていない変更内容がすべて失われます。

デフォルト設定:**有効。タイムアウト:10分。**

現在のユーザーの前回ログインに関する通知を表示する

このオプションによって、ユーザーの前回の正常なログインの日時、前回の正常なログイン以降に認証に失敗した回数、前回の正常なログインで使用された IP アドレスを表示できます。この情報は、ユーザーがログインするたびに画面の下部に表示されます。

デフォルト設定:**無効。**

ローカルまたはドメインのパスワードの失効に関する警告を表示する

このオプションによって、ユーザーがAcronis Cyber Protect Management Serverにアクセスするためのパスワードが失効するときの表示が有効になります。管理サーバーがインストールされたマシンにユーザーがログオンするときに使用するローカルまたはドメインのパスワードが対象です。パスワードが失効するまでの時間が画面の下部と右上隅のアカウントメニューに表示されます。

デフォルト設定:**無効。**

アップデート

このオプションでは、組織管理者がウェブコンソールにサインインするたびにAcronis Cyber Protectの新しいバージョンを確認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、管理者は、「ソフトウェアのアップデートの確認」で説明されている手順でアップデートを手動で確認できます。

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、管理サーバー上のすべての保護計画で共通です。組織管理者は、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。新しい値は、変更後に作成されるすべての保護計画に対して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. 組織管理者として Cyber Protect ウェブ コンソールにログインします。
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。

保護の設定

保護設定を変更するには、Cyber ProtectWebコンソールで **[設定]** > **[保護]** に移動します。

具体的な設定や手順については、このセクションの各トピックを参照してください。

保護定義のアップデート

デフォルトでは、次に挙げるコンポーネントのすべてのプロテクション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。

- マルウェア対策
- 脆弱性診断
- パッチ管理

アップデータロールを持つエージェント

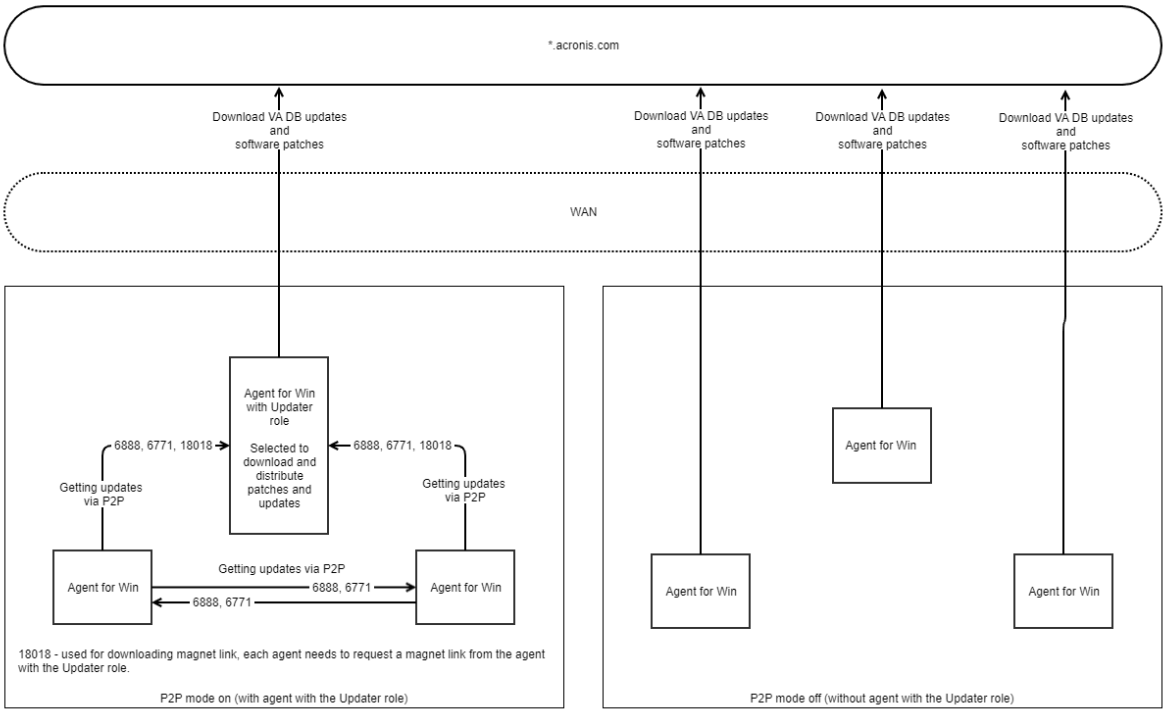
管理者は、利用している環境内で1つまたは複数のプロテクションエージェントを選択し、それらのエージェントにアップデータのロールを割り当てることで、ネットワークの帯域幅のトラフィックを最小限に抑えることができます。これにより、専用のエージェントがインターネットに接続し、アップデート情報をダウンロードできます。他のすべてのエージェントは、ピアツーピア技術を使用して専用のアップデータエージェントに接続し、そこからアップデートプログラムをダウンロードします。

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。

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。

環境内の複数のエージェントにアップデータのロールを割り当てることができます。つまり、アップデータのロールを割り当てられたエージェントがオフラインの場合、このロールを割り当てられた他のエージェントがアップデートされた保護定義のソースとして動作します。

次の図は、保護アップデートのダウンロードの各オプションを示しています。左側ではエージェントがアップデートロールを割り当てられています。そのエージェントはインターネットに接続して保護アップデートをダウンロードし、そのピアエージェントがアップデーターエージェントに接続して最新のアップデートを取得します。右側では、アップデートロールが割り当てられているエージェントはないので、すべてのエージェントがインターネットに接続し、保護アップデートをダウンロードします。



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. アップデータのロールを割り当てられたエージェントが稼働しているマシン上で、以下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. アクロニス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。

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ウェブコンソールで、**[設定]** > **[エージェント]** に移動します。
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。

アップデートのスケジュール設定

全エージェントの保護定義の自動アップデートをスケジュールしたり、選択したエージェントの保護定義を手動でアップデートしたりできます。

自動アップデートのスケジュールを設定するには

1. Cyber Protectウェブコンソールで、**[設定]** > **[保護]** > **[保護定義のアップデート]** に移動します。
2. **[スケジュール]** を選択します。
3. **スケジュールの種類**で、次のいずれかを選択します。
   - **日単位**

     保護定義のアップデートを実行する曜日を選択します。

     開始時間で、アップデートを開始する時間を選択します。
   - **時間単位**

     アップデートのスケジュールを詳細に設定します。

     次の間隔で実行で、アップデートを実行する頻度を設定します。

     開始時刻 ... **終了時刻**で、アップデートを実行する特定の時間範囲を指定します。

保護定義を手動でアップデートするには

1. Cyber Protectウェブコンソールで、**[設定]** > **[エージェント]** に移動します。
2. 保護定義をアップデートするエージェントのマシンを選択し、**[定義のアップデート]** をクリックします。

ダウンロードロケーションの変更

保護定義は、お使いのマシンでデフォルトに設定されている一時フォルダにダウンロードされ、Acronisプログラムフォルダに保管されます。

ダウンロード用の一時フォルダを変更するには

1. 管理サーバーマシンで、`atp-database-mirror.json`ファイルを開いて編集します。

   このファイルは以下のロケーションにあります:
   - Windows: `%programdata%\Acronis\AtpDatabaseMirror\`
   - Linux: `/var/lib/Acronis/AtpDatabaseMirror/`
2. 「`enable_user_config`」の値を`true`に変更します。

   ```
   {
   "sysconfig":
   {
   ...
   "enable_user_config": true
   }
   ...
   }
   ```
3. 管理サーバーマシンで、`config.json`ファイルを開いて編集します。

   このファイルは以下のロケーションにあります:
   - Windows: `%programdata%\Acronis\AtpDatabaseMirror\`
   - Linux: `/var/lib/Acronis/AtpDatabaseMirror/`
4. 以下の行を追加します: `"mirror_temp_dir": "<path_to_new_download_location>"`

たとえば、次のようになります。

```
{
        "mirror_temp_dir":"C:\\temp"
}
```

パスは、AppDataフォルダからの絶対パスまたは相対パスです。
フォルダが作成できない、または管理サーバーから該当のフォルダに書き込みができない場合、デフォルトのロケーションが使用されます。

キャッシュストレージオプション

キャッシュ済みのデータは次のロケーションに保管されています。

- Windows:C:\ProgramData\Acronis\Agent\var\atp-downloader\Cache
- Linuxの場合: /opt/acronis/var/atp-downloader/Cache
- macOSの場合: /Library/Application Support/Acronis/Agent/var/atp-downloader/Cache

古くなったキャッシュデータを消去するスケジュールを設定し、そのサイズに制限を設けることができます。アップデータエージェントを含むマシンとそうでないマシンで、異なる制限値を設定できます。

最新の保護定義のソース

最新の保護定義は次のロケーションからダウンロードできます。

- **クラウド**
  プロテクションエージェントがインターネットに接続して、Acronisクラウドから最新の保護定義をダウンロードします。デフォルトでは、管理サーバーに登録されているすべてのエージェントがアップデートを確認して配信します。アップデータのロールを使用するエージェントの詳細については、"保護定義のアップデート"（623ページ）を参照してください。
- **Cyber Protect管理サーバー**
  このオプションを使用すれば、エージェントがインターネットに接続する必要はありません。管理サーバーに保護定義が格納されており、エージェントは管理サーバーにだけ接続します。ただし、管理サーバーは、最新の保護定義をダウンロードするためにインターネットに接続する必要があります。
- **カスタムWebサーバー**
  このオプションは、トラブルシューティングとテストを目的とする場合、またはエアギャップ環境で使用する場合に適合します。詳細については、"エアギャップ環境での保護定義のアップデート"（627ページ）を参照してください。通常このオプションは、Acronisサポートチームから指示のあったときにだけ選択するようにしてください。

リモート接続

リモート接続を有効にすると、**RDPクライアント経由で接続**および**HTML5クライアント経由で接続**オプションが、Cyber ProtectWebコンソールの右側のメニューにある**サイバープロテクションデスクトッ**

プに表示されます。**[デバイス]** タブでワークロードを選択すると、右側のメニューが開きます。

リモート接続を有効化または無効化すると、組織のすべてのユーザーに影響が及びます。

リモート接続を有効にするには

1. Cyber Protectウェブコンソールで、**[設定]** > **[保護]** に移動します。
2. **[リモート接続]** をクリックして、**[リモートデスクトップ接続]** スイッチを有効化します。

さらに、リモート接続の共有を有効にすることができます。このオプションを使用すると、選択したワークロードにリモートでアクセスするリンクを生成できます。これらのリンクは、他のユーザーと共有できます。

リモート接続を共有するには

1. Cyber Protectウェブコンソールで、**[設定]** > **[保護]** に移動します。
2. **[リモートデスクトップ接続を共有]** チェックボックスを選択します。

これにより、Cyber ProtectWebコンソールの **[リモート接続を共有]** オプションが、右側メニューの **[サイバープロテクションデスクトップ]** 以下に表示されます。

エアギャップ環境での保護定義のアップデート

Acronis Cyber Protectでは、エアギャップ環境での保護定義のアップデートがサポートされています。

エアギャップ環境で保護定義をアップデートするには

1. インターネットにアクセスできるセカンダリの管理サーバーをエアギャップ環境の外部にインストールします。
   その方法の詳細については、"Management Serverのインストール"（82ページ）を参照してください。
2. オンライン管理サーバーからリムーバブルドライブに保護定義をコピーし、エアギャップ環境にあるHTTPサーバーに転送します。
   この手順の詳細については、"オンライン管理サーバーへの定義のダウンロード"（627ページ）および"HTTPサーバーに定義ファイルを転送する"（629ページ）を参照してください。
3. エアギャップ環境の管理サーバーで、アップデートされた保護定義のソースとしてHTTPサーバーを構成します。
   この手順の詳細については、"エアギャップ環境で動作する管理サーバーの定義ソースの構成"（629ページ）を参照してください。

オンライン管理サーバーへの定義のダウンロード

インターネットにアクセスできるセカンダリの管理サーバーをインストールした後、最新の保護定義ファイルをダウンロードし、USBフラッシュメモリーや外付けハードディスクなどのリムーバブルドライブにコピーします。

保護定義ファイルをダウンロードしてコピーするには

1. オンライン管理サーバーが稼働しているマシンで、AtpDatabaseMirrorフォルダをデスクトップまたはTempフォルダなど、任意のロケーションにコピーします。

   AtpDatabaseMirrorフォルダは以下のロケーションにあります:

   - Windowsの場合: %ProgramData%\Acronis\
   - Linuxの場合: /usr/lib/Acronis/
2. atp_database_mirror.jsonファイルを開いて編集します。ファイルは以下のロケーションにあります:

   - Windows: %Program Files%\Acronis\AtpDatabaseMirror

   注意
   Windowsの場合、このフォルダは前のステップで使用したフォルダと同一ではありません。

   - Linux: /usr/lib/Acronis/AppDatabaseMonitor
3. database_mirror.jsonファイルを以下のように編集します。
   a. 「enable_appdata_as_root」の値をfalseに変更します。
   b. 「local_path」のすべてのエントリーの値を、保護定義を保存するロケーションの絶対パスに変更します。
4. atp_database_mirror.jsonファイルの変更内容を保存します。
5. オンライン管理サーバーのあるマシンで、次のコマンドを使用して**Acronis Management Server Service**サービスを停止します。

   - Windows（コマンドプロンプト）:

   ```
   sc stop AcrMngSrv
   ```

   - Linux（ターミナル）:

   ```
   sudo systemctl stop acronis_ams.service
   ```
6. 任意のロケーションにコピーしたAtpDatabaseMirrorフォルダ内で、以下のコマンドを使用してAtpDatabaseMirrorツールを起動します。

   - Windows（コマンドプロンプト）:

   ```
   atp_database_mirror.exe -config atp_database_mirror.json
   ```

   - Linux（ターミナル）:

   ```
   sudo ./atp_database_mirror -config atp_database_mirror.json
   ```

   「local_path」で指定したフォルダにすべてのアップデートがダウンロードされると、コマンドプロンプトまたはターミナルウィンドウに次の行が表示されます。

   ```
   standing by for 1m0s
   ```
7. CTRL+Cを押して、AtpDatabaseMirrorツールを停止します。
8. 「local_path」で指定したフォルダ内のファイルをリムーバブルドライブにコピーします。

次に、リムーバブルドライブのファイルをエアギャップ環境にあるHTTPサーバーにコピーする必要があります。エアギャップ環境で動作する管理サーバーをHTTPサーバーとして使用することができます。詳細については、"HTTPサーバーに定義ファイルを転送する"（629ページ）を参照してください。

HTTPサーバーに定義ファイルを転送する

エアギャップ環境で保護定義を配布するには、専用のHTTPサーバーが必要です。エアギャップ環境で動作する管理サーバーをHTTPサーバーとして使用することができます。

保護定義をHTTPサーバーに転送するには

1. HTTPサーバーを実行するマシン上で、保護定義ファイルを任意のフォルダにコピーします。
2. 保護定義をコピーしたフォルダから、HTTPサーバーを起動します。
   例えばPythonを使用して、以下のようなコマンドを実行できます。

   ```
   python -m http.server 8080
   ```

   注意
   任意のHTTPサーバーを利用できます。
3. 保護定義をコピーしたフォルダで、以下の`update-index.json`ファイルを開き、編集します。
   - `./ngmp/update-index.json`
   - `./vapm/update-index.json`
4. 両方の`update-index.json`ファイルで、すべての `products > os > arch > components > versions > url`フィールドを、次のように編集します。
   a. `IP`および**ポート**の値として、利用しているHTTPサーバーのIPアドレスとポートを設定します。
   b. パスの他の部分は変更しないでください。
   例えば、192.168.1.10がHTTPサーバーのIPアドレスで、8080がポートである場合、`"url": "http://192.168.1.10:8080/ngmp/win64/ngmp.zip"`となります。`/ngmp/win64/ngmp.zip`の部分は変更しないでください。
5. 編集した内容を両方の`update-index.json`ファイルに保存します。

次に、エアギャップ環境で動作する管理サーバーの保護定義ソースを構成する必要があります。詳細については、"エアギャップ環境で動作する管理サーバーの定義ソースの構成"（629ページ）を参照してください。

エアギャップ環境で動作する管理サーバーの定義ソースの構成

HTTPサーバーを構成した後、これを保護定義のソースとして、エアギャップ環境で動作する管理サーバーに構成する必要があります。

エアギャップ環境で動作する管理サーバーの保護定義ソースを構成するには

1. エアギャップ環境で動作する管理サーバーのCyber ProtectWebコンソールで、**[設定]** > **[保護]** > **[保護定義のアップデート]** に移動します。

2. **[定義]** を選択します。
3. **[カスタム]** を選択し、以下のパスを指定します。

   - **ウイルス対策とマルウェア対策の定義**の場合:

     `http://<IP address of your HTTP server>:8080/scanner`
   - **高度な検出の定義**の場合:

     `http://<IP address of your HTTP server>:8080/ngmp`
   - **脆弱性診断とパッチ管理の定義**の場合:

     `http://<IP address of your HTTP server>:8080/vapm`

   この結果、エアギャップ環境にあるエージェントは、現在のHTTPサーバーから保護定義をダウンロードすることになります。

ユーザーアカウントと組織部署の管理

オンプレミスデプロイ

このセクションで説明する機能は、組織管理者のみが利用できます。

これらの設定にアクセスするには、**[設定]** > **[アカウント]** をクリックします。

部署および管理アカウント

部署および管理アカウントを管理するには、Cyber Protectウェブコンソールで、**[設定]** > **[アカウント]** に移動します。**[アカウント]** パネルには、**組織**グループとその部署（存在する場合）のツリー、および選択されている階層レベルの管理アカウントのリストが表示されます。

部署

組織グループは、管理サーバーをインストールするときに自動で作成されます。Acronis Cyber Protect Advanced ライセンスでは、部署と呼ばれる子グループを作成して（通常これは組織の部署や部門に対応します）、部署に対して管理アカウントを追加できます。この方法によって、対応する部署に厳密に限定されたアクセス許可を持つ他のユーザーに、保護管理を委任できます。部署の作成方法については、"部署の作成"（635ページ）を参照してください。

すべての部署で、子部署を作成できます。親部署の管理アカウントには、すべての子部署に対する管理者権限が付与されています。**組織**グループは最上位の親部署であり、このレベルの管理アカウントには組織に属するすべての部署に対する同様の権限が付与されています。

管理アカウント

Cyber Protectウェブコンソールにサインインできるアカウントはすべて、管理アカウントです。

Cyber Protectウェブコンソールでは、どの部署の管理アカウントでも、その部署が属する階層以下のレベルの要素を表示したり、管理したりすることができます。たとえば、組織の管理アカウントは、最上位レベルのアクセス権を持っているため、この組織のすべての部署にアクセスできます。一方、特定の部署の管理アカウントは、自らの部署とその子部署のみにアクセスすることができます。

どのアカウントが管理アカウントになれますか？

管理サーバーがActive Directoryドメインに参加しているWindowsマシンにインストールされている場合は、ローカルのユーザー、またはActive Directoryドメインフォレスト内のユーザー/ユーザーグループに管理者権限を付与できます。

デフォルトでは、管理サーバーとActive Directoryドメインコントローラーの間に、SSL/TLSで保護された接続が確立されます。SSL/TLS接続が不可能な場合は、接続が確立されません。ただし、`auth-connector.json5`ファイルを編集することで、セキュアでない接続を許可することができます。

セキュアな接続を使用するには、Active Directoryで必ずLDAP over SSL（LDAPS）を構成するようにします。

Active DirectoryでLDAPSを構成するには

1. ドメインコントローラーで、Microsoftの要件を満たすLDAPS証明書を作成し、インストールします。
   これらを実行する方法の詳細については、Microsoftマニュアルの「サードパーティの証明機関を使用してLDAP over SSLを有効にする」を参照してください。
2. ドメインコントローラーで**Microsoft管理コンソール**を開き、**[証明書（ローカルコンピュータ）]** > **[証明書]** に、**証明書**が存在することを確認します。
3. ドメイン コントローラを再起動します。
4. LDAPSが有効になっていることを確認します。

ドメインコントローラーへのセキュアでない接続を許可するには

1. 管理サーバーがインストールされたマシンにログインします。
2. `auth-connector.json5`ファイルを開き、編集します。
   `auth-connector.json5`ファイルは`%APPDATA%\Acronis\AuthConnector`に配置されています。
3. **[同期]** セクションに移動し、「**connectionMode**」の各行で、「**ssl_only**」を「**auto**」に置き換えます。
   [auto]モードでは、TLS接続が不可能な場合、セキュアでない接続が確立されます。
4. **Acronis Service Manager Service**を再起動します（"Acronis Service Manager Serviceを再起動するには"（196ページ）を参照）。

注意
管理サーバーがActive Directoryドメインに参加していない場合、また管理サーバーがLinuxマシンにインストールされている場合は、ローカルユーザーとグループにのみ管理者権限を付与できます。

管理サーバーに管理者アカウントを追加する方法については、"管理アカウントを追加"（634ページ）を参照してください。

管理アカウントロール

それぞれの管理アカウントには、特定のタスクに必要な事前定義の権限を付与されたロールが割り当てられています。管理アカウントのロールは以下の通りです。

- **管理者**
  このロールには、組織または部署に対する完全な管理者向けアクセス権が付与されます。
- **読み取り専用**
  このロールには、Cyber Protectウェブコンソールに対する読み取りの専用アクセス権が付与されます。システムレポートなどの診断用データの収集のみが許可されます。読み取り専用ロールでは、バックアップを参照したり、バックアップされたメールボックスの内容を参照したりすることはできません。
- **監査者**
  このロールには、Cyber Protectウェブコンソールの **[アクティビティ]** タブに対する読み取り専用のアクセス権が付与されます。このタブの詳細については、"アクティビティタブ"（580ページ）を参

照してください。このロールでは、管理サーバーのシステム情報などのデータを収集したり、エクスポートしたりすることはできません。

ロールでの変更はすべて [**アクティビティ**] タブに表示されます。

ロールの継承

親部署のロールはその子部署に継承されます。親部署と子部署で同じユーザーアカウントに異なるロールが割り当てられた場合、両方のロールを持つことになります。

また、ロールは特定のユーザーアカウントに明示的に割り当てるか、ユーザーグループから継承することができます。つまり、ユーザーアカウントは、個別に割り当てられたロールと継承されたロールの両方を持ちます。

ユーザーアカウントに異なるロール（割り当てられたロールと継承されたロール）が割り当てられている場合、それらのロールで許可されているオブジェクトにアクセスし、許可されているアクションを実行できます。例えば、ユーザーアカウントに読み取り専用ロールが割り当てられ、管理者ロールを継承している場合は、管理者権限を行使できます。

重要
Cyber Protect ウェブ コンソールでは、現在の部署に明示的に割り当てられているロールのみが表示されます。継承されたロールと相違している可能性があっても、表示されることはありません。継承されたロールによって問題が生じることを避けるため、管理者ロール、読み取り専用ロール、および監査者ロールは別々のアカウントやグループに割り当てることを強くお勧めします。

デフォルトの管理者

Windowsの場合

Management Serverをコンピュータにインストールするときに、次のことが生じます。

- **Acronis 集中管理**ユーザーグループがマシンに作成されます。
  ドメインコントローラーで、このグループに DCNAME **$ Acronis Centralized Admins** という名前が付けられます。ここで、DCNAME はドメインコントローラーの NetBIOS 名です。
- **Administrators** グループのすべてのメンバーが**Acronis 集中管理**グループに追加されます。マシンがドメインに所属しており、またドメインコントローラーではない場合、ローカル（非ドメイン）ユーザーは除外されます。ドメインコントローラーでは、非ドメインのユーザーは存在しません。
- **Acronis 集中管理**グループと **Administrators** グループが**組織管理者**として管理サーバーに追加されます。マシンがドメインに所属しており、またドメインコントローラーではない場合、ローカル（非ドメイン）ユーザーが組織管理者になることのないよう、**Administrators** グループは追加されません。

アドミニストレータグループは、組織管理者のリストから削除することができます。一方、**Acronis 集中管理**グループは削除できません。通常は発生しないケースですが、すべての組織管理者を削除してしまった場合は、Windows で**Acronis集中管理**グループにアカウントを追加し、そのアカウントを使用して Cyber Protect ウェブ コンソールにログインすることができます。

Linuxの場合

管理サーバーがマシンにインストールされる際に、**root** ユーザーが**組織管理者**として管理サーバーに追加されます。

後述するように、それ以外の Linux ユーザーを管理サーバーの管理者リストに追加し、このリストから **root** ユーザーを削除することができます。通常は発生しないケースですが、すべての組織管理者が削除された場合は、`acronis_asm` サービスを再起動できます。その場合は、**root** ユーザーが組織管理者として自動的に再度追加されます。

複数の部署における管理アカウント

アカウントには、任意の数の部署に対する管理者権限を付与することができます。そのようなアカウント（組織レベルの管理アカウントの場合も同様）については、Cyber Protect ウェブコンソールで部署選択が表示されます。この選択機能を使用することで、該当のアカウントで各部署を個別に表示および管理できます。

組織のすべての部署に対するアクセス許可を持つアカウントが、組織レベルのアクセス許可を持つわけではありません。組織レベルの管理アカウントは、**組織**グループに明示的に追加する必要があります。

コンピュータを部署へ追加する方法

管理者がWebインターフェース経由でコンピュータを追加するとき、コンピュータはその管理者が管理している部署に追加されます。管理者が複数の部署を管理している場合、コンピュータは部署セレクタで選択された部署に追加されます。そのため、管理者は **[追加]** をクリックする前に部署を選択する必要があります。

エージェントをローカルでインストールする場合、管理者はそれらの資格情報を提供します。コンピュータはその管理者が管理している部署に追加されます。管理者が複数の部署を管理している場合、コンピュータを追加する部署を選択するようにインストーラから求められます。

管理アカウントを追加

注意
この機能はStandardエディションとEssentialsエディションでは使用できません。

アカウントを追加するには

1. **[設定]** > **[アカウント]** の順にクリックします。
   Management Serverの管理者リストと部署のツリー（存在する場合）が表示されます。
2. 管理者を追加する **[組織]** を選択するか、部署を選択します。
3. **[アカウントの追加]** をクリックします。
4. **[ドメイン]** で、追加するユーザーアカウントを含むドメインを選択します。管理サーバーが Active Directory ドメインに参加していない場合、または Linux にインストールされている場合は、追加できるのはローカルユーザーのみです。
5. ユーザー名またはユーザーグループ名を検索します。

6. ユーザーまたはグループの名前の横にある [+] をクリックします。
7. アカウントのロールを選択します。
8. （オプション）追加するすべてのユーザーまたはグループについて、手順4～6を繰り返します。
9. 完了したら、**[完了]** をクリックします。
10. （Linux の場合のみ）以下の記述のとおり、AcronisモジュールのLinux Pluggable Authentication Module（PAM）構成にユーザー名を追加します。

AcronisのPAM構成にユーザー名を追加するには

この手順は、Linuxマシン上で動作する管理サーバーとAcronis Cyber Protectのオールインワン型アプライアンスに適用されます。

1. 管理サーバーを実行するマシンで、root ユーザーとして **/etc/security/acronisagent.conf** ファイルをテキストエディタで開きます。
2. このファイルに、管理サーバーの管理者として追加したユーザー名を、1 行に 1 ユーザーずつ追加します。
3. ファイルを保存して閉じます。

部署の作成

1. **[設定]** > **[アカウント]** の順にクリックします。
2. Management Serverの管理者リストと部署のツリー（存在する場合）が表示されます。
3. **[組織]** または新しい部署の親部署を選択します。
4. **[部署の作成]** をクリックします。
5. 新しい部署の名前を指定し、**[作成]** をクリックします。

クラウドデプロイ

ユーザーアカウントと組織部署の管理は、管理ポータルで行うことができます。管理ポータルにアクセスするには、サイバープロテクションサービスにログインするときに **[管理ポータル]** をクリックするか、右上隅にある  アイコンをクリックしてから、**[管理ポータル]** をクリックします。管理者権限を持つユーザーだけがこのポータルにアクセスできます。

ユーザーアカウントと組織部署の管理については、管理ポータルの管理者ガイドを参照してください。この文書にアクセスするには、管理ポータルの「？」アイコンをクリックします。

このセクションでは、サイバープロテクションサービスの管理に関連するその他の情報をまとめます。

制限値（クォータ）

制限値（クォータ）はユーザーによるサービスの使用を制限できます。容量を設定するには、**[ユーザー]** タブでユーザーを選択し、**[制限値（クォータ）]** セクションで鉛筆アイコンをクリックします。

指定した容量を超過すると、ユーザーの電子メールアドレスに通知が送信されます。追加容量を設定していない場合は、容量は「ソフト」と見なされます。これは、サイバープロテクションサービスの使用に関する制限が適用されていないことを表します。

追加容量を指定することもできます。追加容量により、ユーザーは指定された値の分だけ制限値（クォータ）を超過することができます。追加容量を超過すると、サイバープロテクションサービスの使用に関する制限が適用されます。

バックアップ

クラウドストレージの制限値（クォータ）、ローカルバックアップの制限値（クォータ）、およびユーザーが保護できるマシン/デバイス/メールボックスの最大数を指定できます。以下の各項目に対して容量を設定できます。

- **クラウドストレージ**
- **ワークステーション**
- **サーバー**
- **Windows Server Essentials**
- **仮想ホスト**
- **ユニバーサル**

  この制限値（クォータ）は、上記の 4 つのうちの任意の制限値（クォータ）の代わりに使用できます。ワークステーション、サーバー、Windows Server Essentials、仮想ホスト。
- **モバイル デバイス**
- **Microsoft 365メールボックス**
- **ローカルバックアップ**

マシン/デバイス/メールボックスは、少なくとも1つの保護計画が適用されていれば、保護されていると見なされます。モバイルデバイスは、最初のバックアップが実行された後に、保護されます。

クラウドストレージの制限値（クォータ）追加容量を超過すると、バックアップは失敗します。複数のデバイスで超過が発生すると、ユーザーは保護計画をそれ以外のデバイスに適用できなくなります。

ローカルバックアップの制限値（クォータ）は、クラウドインフラストラクチャを使用して作成されたローカルバックアップの合計サイズを制限します。この制限値（クォータ）には追加容量を設定できません。

災害復旧

これらの制限値（クォータ）は、サービスプロバイダーによって企業全体に適用されます。企業管理者は管理ポータルで制限値（クォータ）と使用状況を表示できますが、ユーザーの制限値（クォータ）は設定できません。

- **ディザスタリカバリストレージ**

  このストレージは、プライマリサーバーとリカバリ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。

  制限値（クォータ）が無効になると、すべてのサーバーが削除されます。 ウェブ コンソールから **[クラウド復元サイト]** タブが消えます。

- **コンピュートポイント**
  この制限値（クォータ）は、請求期間中にプライマリおよびリカバリサーバーによって消費されるCPU および RAM リソースを制限します。この制限値（クォータ）の追加容量に達した場合、すべてのプライマリおよびリカバリサーバーがシャットダウンされます。次の請求期間の開始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完全な暦月です。
  制限値（クォータ）が無効に設定されている場合、請求期間に関係なくサーバーを使用することはできません。
- **パブリック IP アドレス**
  この制限値（クォータ）は、プライマリサーバーとリカバリサーバーに割り当てることができるパブリック IP アドレスの数を制限します。この制限値（クォータ）の追加容量に達した場合、それ以上サーバーにパブリックIPアドレスを有効にできなくなります。サーバー設定で **[パブリック IP アドレス]** チェックボックスをオフにすると、サーバーがパブリック IP アドレスを使用できないようにすることができます。その後、別のサーバーにパブリック IP アドレスを使用させることができます。パブリック IP アドレスは通常同じものではありません。
  制限値（クォータ）が無効にされている場合、すべてのサーバーがパブリックIPアドレスの使用を停止し、インターネットから到達できなくなります。
- **クラウドサーバー**
  この制限値（クォータ）はプライマリサーバーとリカバリサーバーの総数を制限します。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やリカバリサーバーを作成することはできません。
  クォータが無効になっている場合、サーバーはCyber Protect ウェブ コンソールに表示されますが、利用できる操作は **[削除]** のみです。
- **インターネットアクセス**
  この制限値（クォータ）は、プライマリサーバーとリカバリサーバーからのインターネットアクセスを有効または無効にします。
  制限値（クォータ）が無効になると、プライマリサーバーとリカバリサーバーはすぐにインターネットから切断されます。サーバープロパティの **[インターネットアクセス]** スイッチがクリアされ、無効になります。

通知

ユーザーの通知設定を変更するには、**[ユーザー]** タブでユーザーを選択し、**[設定]** セクションで鉛筆アイコンをクリックします。次の通知設定を使用できます。

- **クォータの超過に関する通知**（デフォルトで有効）
  容量の超過に関する通知。
- **定期使用状況レポート**
  毎月の最初の日に送信される、以下で説明している使用状況レポート。
- **失敗に関する通知**、**警告通知**、および**成功の通知**（デフォルトで無効）
  保護計画の実行結果および各デバイスのディザスタリカバリ操作の結果に関する通知。
- **アクティブアラートに関する日次概要**（デフォルトで有効）

バックアップの失敗、実行されていないバックアップなどの問題について記載された概要。概要は10:00（データセンターの時間）に送信されます。この時点で問題がない場合は、概要は送信されません。

通知はすべてユーザーの電子メールアドレスに送信されます。

レポート

サイバープロテクションサービスの使用に関するレポートには、組織または部署に関する以下のデータも含まれます。

- 部署、ユーザー、デバイスの種類ごとのバックアップのサイズ。
- 部署、ユーザー、デバイスの種類ごとの保護されたデバイスの数。
- 部署、ユーザー、デバイスの種類ごとの価格。
- バックアップの合計サイズ
- 保護されたデバイスの合計数。
- 合計価格

コマンド ライン リファレンス

コマンドラインリファレンスは、https://www.acronis.com/en-us/support/documentation/AcronisCyberProtect_15_Command_Line_Reference/index.htmlから入手できる個別の文書です。

トラブルシューティング

このセクションでは、エージェントのログを .zip ファイルに保存する方法について説明します。不明な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。

ログを取得する手順

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. **[システム情報の収集]** をクリックします。
3. 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。

用語集

S

Startup Recovery Manager

ブータブル エージェントの改訂版。システムディスクに常駐し、起動時に [F11] キーを押すと起動するように設定されています。Startup Recovery Managerを使用すると、ブータブルレスキューユーティリティを起動するためのレスキューメディアまたはネットワーク接続が不要になります。 Startup Recovery Managerは、モバイルユーザーに特に便利です。障害が発生した場合、ユーザーはマシンを再起動し、「Press F11 for Startup Recovery Manager…」というプロンプトに対してF11キーを押して、通常のブータブルメディアと同じ方法でデータ復元を実行します。 制限事項: WindowsローダーおよびGRUB以外のローダーは、再アクティベーションが必要です。

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、月の初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初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、その日の初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、該当時間の初めに最初のバックアップが作成されます。

漢字

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。

管理対象ロケーション

Storage Nodeによって管理されるバックアップロケーション。 管理対象ロケーションは、物理的にネットワーク共有、SAN、NAS、Storage Nodeのローカルハードディスクドライブ、またはStorage Nodeにローカル接続されたテープライブラリに配置できます。Storage Nodeは、管理対象ロケーションに保存される各バックアップを（保護計画に処理が含まれている場合）クリーンアップおよびベリファイします。Storage Nodeが実行するその他の処理（重複除外、暗号化）を指定することができます。

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

新しいバックアップ形式は、ファイルのチェーンではなく、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 1 つの .tib 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、例えばSFTPサーバーにバックアップする際には使用できません。

索引

.

.mst トランスフォームファイルの作成とインストールパッケージの抽出 106, 139

.mst トランスフォームを使用した製品のインストール 107, 140

[

[計画] タブ 343

3

32ビットまたは64ビット 354

4

40～160MB の RAM（重複のないデータ 1TB あたり） 614

A

AAGに含まれるデータベースのバックアップ 442

AAGに含まれるデータベースの復元 443

Acronis Cyber Infrastructureについて 228

Acronis Cyber Protect 15エディション 17

Acronis Cyber Protect 15にアップグレードする 178

Acronis Cyber Protect アプライアンス 91

Acronis Cyber Protectのネットワーク接続図 78

Acronis Cyber Protectをユーザーの環境で他のセキュリティソリューションと併用する 51

Acronis PXE Server 430

Acronis PXE Server のインストール 430

Acronis の特許取得済みの技術 16

Acronis プラグインの WinPE への追加 374

AcronisCyber Protect 15 Update 2以前のライセンス 41

AcronisCyber Protect 15 Update 3以降のライセンス 21

Acronisアカウント、ローカルとクラウドコンソール 23

Active Protection 504, 511

Active Protectionの設定 505

Advancedライセンスを持つユーザーのための考慮事項 251

Always On可用性グループ（AAG）の保護 442

ASignを使用したファイルの署名 322

autostart.jsonの構造 365

C

calculate hash 280

Changed Block Tracking（CBT） 267, 478

CPUの優先度 287

Cyber Protect Webコンソールからマシンを追加する 93

Cyber Protect ウェブ コンソールへのアクセス 182

Cyber Protection 571

Cyber Protectウェブ コンソールからマシンを削除する 180

Cyber Protectウェブコンソールからデータをレビューする方法 434

Cyber Protectウェブコンソール表示 197

D

DefaultBlockSize 590

Dell EMC Data Domainストレージの機能 73

E

ESXi仮想マシンの追加要件 447

ESXi仮想マシンの要件 439

ESXi構成の選択 215

ESXi構成の復元 325

Exchange Server データベースのマウント 455

Exchange Server に復元 456

Exchange Serverクラスタの概要 443

Exchange Serverデータの選択 441

Exchange Serverメールボックスの選択 448

Exchange クラスタ データのバックアップ 445

Exchange メールボックスとメールボックスのアイテムを復元 455

Exchangeエージェント（メールボックスバックアップ用） 54

Exchangeクラスタデータの復元 445

Exchangeデータベースの復元 453

F

Flashback 331

G

get content 280

Google Workspaceデータを保護 469

H

HTTPS接続によるWebコンソールへのログインのみを許可する 189

HTTPサーバーに定義ファイルを転送する 629

Hyper-V仮想マシンの要件 439

I

Internet Explorer、Microsoft Edge、Opera、およびGoogle Chromeの設定 183

iSCSIイニシエータの設定 486

iSCSIデバイスの構成 427

L

LAN フリー バックアップ 480

Linux 122, 155, 213

Linux でのインストール 90, 104

Linux での無人インストールまたはインストール解除 114, 145

Linux における Universal Restore 318

Linux ベース 353

Linux ベースのブータブル メディア 355

Linuxのルール 211

Linuxの場合 58, 133, 135, 180, 183, 634

Linuxの選択ルール 214

Linuxパッケージ 67

Linuxベースのブータブルメディアか、WinPEベースのブータブルメディアか 353

Linuxマシンの脆弱性診断 532

Linuxを実行するコンピュータの追加 98

list backups 278

list content 279

LVMのスナップショット 282

M

Mac 213

macOS 123, 155

macOS でのインストール 105

MacOS のルール 212

macOS の選択ルール 215

macOS を実行するマシンの追加 98

macOSでの無人インストールまたはインストール解除 118

macOSの場合 133, 137, 180

macOSの無人インストールとインストール解除 151

Macユーザー向けの注意事項 304

Management Serverでメディアを登録 379

Management Serverのインストール 82

Management Serverのデータベース 86

Management ServerへのSANストレージの登録 487

Management Serverロケーション 45

McAfee Endpoint Encryption および PGP Whole Disk Encryption 72

Microsoft 365アクセス認証の変更 466

Microsoft 365への復元 456

Microsoft 365メールボックスの保護 463

Microsoft 365メールボックスをバックアップする理由 463

Microsoft 365組織の追加 464

Microsoft BitLocker Drive EncryptionとCheckPoint Harmony Endpoint 72

Microsoft Exchange Server 268

Microsoft Exchange Server のライブラリのコピー 461

Microsoft Security Essentials 514

Microsoft SharePointの保護 436

Microsoft SQL Server 267

Microsoft SQL ServerとMicrosoft Exchange Serverの保護 436

Microsoft アプリケーションの保護 436

Microsoft製品 535

Mozilla Firefoxの設定 184

N

NetApp SANストレージ要件 484

NFS 209

NFSクライアントの設定 486

Notaryサービスを使用したファイル真正性のベリファイ 321

O

Oracle エージェント 55

Oracle データベースの保護 470

OVFテンプレートからエージェント for VMware（仮想アプライアンス）のデプロイ 165

OVFテンプレートのロケーション 166

OVFテンプレートの配置 166

oVirt（仮想アプライアンス）エージェントをデプロイ中 156

P

PEイメージ 373

PXE から起動するコンピュータの設定 431

R

RAID-5 418

RSM とサードパーティ製ソフトウェアとの互換性 587

S

SANハードウェアスナップショット 294

SANハードウェアスナップショットの使用 483

SANハードウェアスナップショットを使用するために必要なもの 484

SANハードウェアスナップショットを使用する理由 483

SAP HANA の保護 502

Scale Computing HC3 エージェント – 必要なロール 174

Scale Computing HC3 エージェント（仮想アプライアンス）の配置 168

Scale Computing HC3 クラスターの追加 101

Scale Computing HC3エージェント（仮想アプライアンス） 57

Secure Zone 209

Secure Zoneのバージョン情報 226

Secure Zoneの作成方法 227

Secure Zoneの削除方法 228

Secure Zoneの使用方法 71

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 226

Secure Zoneを使用する理由 226

SFTPサーバーとテープデバイス 208

SIDの変更 334

SQL Server データベースの接続 452

SQL Server高可用性ソリューションの概要 442

SQL データベースの復元 449

SQL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）、Active Directoryエージェント 54

SQLサーバーまたはExchangeサーバーのアクセス認証の変更 462

SQLデータベースの選択 440

SSL証明書の設定 193

Startup Recovery Manager 428

Startup Recovery Managerの無効化 429

Startup Recovery Managerの有効化 429

Storage Node インストールパラメータ 114

Storage Node（オンプレミスデプロイメントのみ） 59

Storage Nodeとカタログサービスのインストール 608

Storage vMotion 491

T

TapeLocationフォルダ 589

U

Universal Restore のドライバ 371

Universal Restoreの使用 316

Universal Restoreの設定 317

Universal Restoreプロセス 318

URLフィルタリング 515

URLフィルタ処理 511

URLフィルタ処理の設定 517

V

vCenterまたはESXiホストの追加 98

Virtuozzo Hybrid Infrastructureエージェント（仮想アプライアンス）の配置 156

VLAN の追加 378

VM への定期的な変換の動作 249

VM 移行のサポート 491

vMotion 491

VMware vSphere での作業 474

VMware エージェント - 必要な権限 493

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 131

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 271

VMの電源管理 334, 479

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 493

VSS完全バックアップの有効化 302

W

Webインターフェイスを使用したVMwareエージェント（仮想アプライアンス）のデプロイ 99

Webインターフェイスを使用したファイルの復元 319

Webコンソールにカスタムメッセージを追加します 190

Windows 122, 154, 212

Windows AzureおよびAmazon EC2仮想コンピュータ 500

Windows Defender Antivirus 512

Windows XP SP2エージェント 60

Windows イベント ログ イベントの発生時 234

Windows でのインストール 82, 102

Windows での無人インストールまたはインストール解除 106, 139

Windows、Linux、macOS のルール 211

Windowsイベントログ 303, 334

Windowsサードパーティ製品 535

Windowsでサポートされているサードパーティ製品 529

WindowsにおけるUniversal Restore 316

Windowsのルール 211

Windowsの場合 58, 132, 134, 179, 182, 633

Windowsの選択ルール 214

Windowsマシンのログオンアカウントの変更 137

Windowsマシンの脆弱性診断 532

Windowsリムーバブル記憶域マネージャ（RSM）とのインタラクション 587

Windowsを実行するコンピュータの追加 93

Windowsを実行するマシンに関する追加の要件 447

WinPE ベースのブータブル メディア 372

WinPEベース 353

WinREベースのPEイメージ 372

WriteCacheSize 590

あ

アーカイブ内の重複除外 266

アカウントのアクティブ化 129

アクティビティタブ 580

アクティブ ボリュームの設定 422

アップデータロールを持つエージェント 623

アップデート 60, 621

アップデートのスケジュール設定 624

アップデート前のバックアップ 537

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 464

アプリケーションの復元 437

アプリケーション間でリソースの競合が発生しないようにする 614

アプリケーション認識型バックアップ 445

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 446

アプリケーション認識型バックアップのその他の要件 438

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。 446

アラート 259

アラートの重大度の設定 585

アラート設定ファイル 585

い

いくつのエージェントが必要ですか。 165, 169

イベントのプロパティ 234

イベント別のスケジュール 232

インストール 44, 60, 90, 100, 104, 617

インストールするコンポーネント 83

インストールするコンポーネントの選択 161

インストールする前に 90, 99, 104, 129, 316

インストールする大容量記憶装置ドライバ 317

インストールパラメータ 108, 115, 141, 146

インストール解除パラメータ 114, 117, 144, 150

インストール概要 44

インストール設定のカスタマイズ 83

インベントリ終了後の操作 604

う

ウイルスおよびマルウェア対策保護 503

ウイルスおよびマルウェア対策保護の設定 504

え

エアギャップ環境での保護定義のアップデート 627

エアギャップ環境で動作する管理サーバーの定義ソースの構成 629

エージェント 47, 53

エージェント for Hyper-V 57

エージェント for Linux 55

エージェント for Mac 56

エージェント for Office 365 54

エージェント for VMware（Windows） 57

エージェント for VMware（Windows）のインストール 99

エージェント for VMware（仮想アプライアンス） 56

エージェント for VMware（仮想アプライアンス）の削除 180

エージェント for Windows 53

エージェントfor VMwareを実行しているマシンの設定 486

エージェントインストールパラメータ 113, 116

エージェントのアップデート 177

エージェントのインストール 134

エージェントのシステム要件 165, 168

エージェントの自動DRSを無効にする 165

エージェントの自動割り当ての無効化 490

エージェントをローカルでインストールする 102

エラーが発生した場合は再試行する 270

エラー処理 270, 479

お

オプションの説明 281

オフホストのデータ処理 343

オフラインのオンプレミス管理サーバー 23

オフライン管理サーバーに割り当てるライセンスクォータを減らす 34

オペレーティングシステムでサポートされるCyber Protectの機能 17

オリジナルのイニシャル RAM ディスクへの復元 318

オンデマンドのパッチインストール 542

オンデマンドマルウェアスキャン 504

オンプレミスでのブータブルメディアによるバックアップ 381

オンプレミスでのブータブルメディアによる復元 391

オンプレミスデプロイ 44, 82, 166, 176, 182, 500, 631

オンプレミス管理サーバー 22

オンラインのオンプレミス管理サーバー 23

オンライン管理サーバーへの定義のダウンロード 627

か

カーネル パラメータ 359

カスタム グループ 556

カスタム プール 600

カスタムスクリプト 364

カタログサービスのインストールパラメータ 114

カタログサービスをAcronis Cyber Protect 15 Update 4にアップデートする 609

カタログ化の有効化または無効化方法 618

カタログ作成 616

カタログ作成のベストプラクティス 617

カテゴリ別の未適用アップデート 578

き

キャッシュストレージオプション 626

く

クラウド ストレージからのバックアップ 364

クラウドストレージ 270

クラウドストレージからのファイルのダウンロード 320

クラウドストレージにバックアップする場合 230

クラウドストレージを使用したバックアップと復元 363

クラウドデプロイ 45, 129, 177, 183, 501, 635

クラウドデプロイの場合 166

クラウド管理サーバー 22

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 442

クラスターバックアップモード 267

クラスター認識型バックアップ 444

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 444

クラスタ化された Hyper-V コンピュータのバックアップ 497

クリーンアップ 348

クリプトマイニングプロセス検出 506

クリプトマイニングプロセス検出設定 507

グループへの保護計画の適用 568

グループポリシーによるエージェントの配置 174

こ

コマンド ライン リファレンス 639

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 527

コントロールの種類 366

コンピュータの移行 499

コンピュータの確定 473

コンピュータの削除 473

コンピュータの実行 472

コンピュータを部署へ追加する方法 634

コンポーネント 47

さ

サードパーティ製ソフトウェアとの共存 587

サーバー側保護機能 505

サービスのログオン アカウント 84

サービスログオンアカウントに必要なユーザー権限 85

サブスクリプションライセンスの管理 41

サブネットをまたがる操作 431

サポートされているLinux製品 530

サポートされているクラスタ構成 442, 444

サポートされている仮想マシンの種類 246

サポートされる Microsoft SharePoint のバージョン 62

サポートされる Microsoft SQL Server のバージョン 61

サポートされるMicrosoft Exchange Serverのバージョン 61

サポートされるオペレーティング システムと環境 53

サポートされるハードウェア 588

サポートされるファイル システム 75, 403

サポートされるモバイル デバイス 432

サポートされるロケーション 223, 250, 344, 346, 348

サポートされる仮想環境プラットフォーム 62

サポート対象の Oracle データベースのバージョン 62

サポート対象の SAP HANA バージョン 62

サポート対象のMicrosoft製品 528

サポート対象のMicrosoft製品とサードパーティ製品 528

し

システムデータベースの復元 451

システムファイルとフォルダを除外する 273

システム状態の選択 215

システム状態の復元 324

システム設定 619

システム要件 74, 617

シンプル ボリューム 417

す

スキャンサービス 88

スキャンサービスのデータベース 89

スキャン対象 530

スクリプトのファイル 364

スケジューリング 294

スケジュール 229, 530, 536, 547

スケジュールスキャン 508, 512

スケジュール設定の条件が満たされるまで待機する 301

ステップ1アップデートする製品のライセンス契約を読んで、同意する 540

ステップ2自動承認の設定を構成する 540

ステップ3テストパッチの保護計画を準備する 540

ステップ4本番パッチの保護計画を準備する 541

ステップ5テストパッチの保護計画を実行して、結果を確認する 542

ストライプ ボリューム 417

ストレージ ノード 608

ストレージ ノードに接続されたテープ デバイスへのバックアップ 594

ストレージ ノードに接続されたテープ ドライブのブータブル メディアによる復元 598

スパン ボリューム 417

すべてのアラートの削除 546

スマート保護 544

せ

セキュリティ 620

セクタ単位のバックアップ 295

そ

ソースマシンの処理 124

その他のコンポーネント 50

その他のパラメータ 143, 148

その他の操作 92

その他の注意点 242

ソフトウェアのアップデート 92

ソフトウェアのアップデートの確認 123

ソフトウェアのインストール 91

ソフトウェア固有の復元手順 72

ソフトウェア要件 52

た

ターゲットマシン上での処理 126

ダイナミック ディスク変換

MBR から GPT 415

ダイナミック ボリュームの種類 417

ダイナミックグループの作成 557

ダウンロードロケーションの変更 625

タスクの開始条件 300

タスクの実行をスキップする 301

タスク失敗時の処理 300

て

ディスクとボリュームの選択 210

ディスクの初期化 405

ディスクプロビジョニング 479

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 212

ディスクレベル バックアップ 612

ディスク管理用のオペレーティング システムの選択 404

ディスク処理 405

ディスク状態アラート 576

ディスク状態ウィジェット 573

ディスク状態監視 571

ディスク変換

GPT から MBR 415

MBR から GPT 414

ダイナミックからベーシックへ 416

ベーシックからダイナミックへ 416

ディスプレイ モードの設定 381

データ カタログ 616

データのバックアップを開始する方法 433

データの重複除外 78

データの内容が類似している複数のコンピュータをバックアップする前に、代表的な 1 台のコンピュータをバックアップする 614

データベースのバックアップ 440

データベース可用性グループ（DAG）の保護 443

データ取り込みの後に実行するコマンド 293

データ取り込みの前に実行するコマンド 292

データ取り込みの前後に実行するコマンド 291

データ保護マップ 546, 576

データ保護マップの設定 547

テープ サポートの概要 587

テープ デバイス 587

テープ デバイスから起動したオペレーティング システムでの復元 596

テープ デバイスについて 587

テープ デバイスの検出 599

テープ デバイスの操作 593

テープ プール 599

テープ ライブラリの他の使用法に関するヒント 596

テープセットの指定 607

テープに書き込む場合のパラメータ 589

テープに保存されたディスクのバックアップからのファイルの復元を有効にする 296

テープの操作 601

テープの保存されているバックアップが表示されない場合の対処 596

テープ管理 295, 333, 599

テープ管理データベース 588

テープ関連のバックアップオプション 591

デバイスグループ 556

デバイスのIPアドレスをチェック 241

デバイスの計画とグループの計画の競合 201

デフォルトのアクション 512

デフォルトのバックアップ オプション 621

デフォルトのバックアップファイル名 262

デフォルトの管理者 633

デプロイ 228

と

トップレベルオブジェクト 365

どのアカウントが管理アカウントになれますか？ 631

ドメインコントローラの保護 437

ドライバの準備 316

トラブルシューティング 163, 314, 640

な

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。 445

ね

ネットワーク ポート 371

ネットワークフォルダの保護 505

ネットワーク共有を使用したバックアップと復元 363

ネットワーク接続図 - Cyber Protectプロセス 79

ネットワーク設定 370, 378

ネットワーク要件 500

の

ノータリゼーション 245

ノータリゼーションの使用方法 245

は

バックアップ 204, 594-595, 636

バックアップ オプション 253

バックアップ ファイル名 261

バックアップアプリの入手先 433

バックアップウィンドウ 286

バックアップからのボリュームのマウント 338

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） 471

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 276

バックアップから実行しているマシンの確定 474

バックアップスキーム、操作、制限事項 229

バックアップスキャンの計画 344

バックアップスキャンの詳細 578

バックアップストレージタブ 337

バックアップデータを取得するための「tibxread」ツール 277

バックアップできる内容 432

バックアップに選択されたテーププール内でテープの設定を使用 299

バックアップのエクスポート 340

バックアップのベリファイ 339

バックアップのベリファイ 266, 327

バックアップのマルウェア対策スキャン 525

バックアップのレプリケーション 344

バックアップの合計サイズ別 209

バックアップの削除 341

バックアップの準備 594-595

バックアップの操作 337

バックアップの統合 260

バックアップの保存先の追加 229

バックアップファイルについて 261

バックアップファイル名が表示される場所 261

バックアップファイル名と単純化されたファイル名 263

バックアップファイル名の制限 262

バックアップモジュールのチートシート 206

バックアップロケーションのホストが利用できる状態 237

バックアップ形式 264

バックアップ形式とバックアップファイル 265

バックアップ形式のバージョン12（TIBX）への変更 266

バックアップ後に実行するコマンド 291

バックアップ先の選択 223

バックアップ前に実行するコマンド 290

バックアップ対象の選択 209

バックアップ中の出力速度 288

パッチインストールウィジェット 577

パッチインストールステータス 577

パッチインストール概要 577

パッチインストール履歴 577

パッチのリストの管理 537

パッチ管理 533

パッチ管理の設定 535

バッテリー電源を節約 238

パフォーマンス 332, 479

パフォーマンスとバックアップウィンドウ 285

パラメータ 360

ひ

ビルトイングループ 556

ヒント 251

ふ

ファイルが検疫フォルダに移される仕組み 523

ファイルとフォルダの選択 213

ファイルの除外 330

ファイルの日付と時刻 329

ファイルの復元 319

ファイルフィルタ 271

ファイルレベルのセキュリティ 330

ファイルレベルのバックアップ 612

ファイルレベルのバックアップのスナップショット 273

フィルタリングするカテゴリ 517

ブータブル メディア 351

ブータブルメディアにおいて 134

ブータブルメディアによるディスク管理 400

ブータブルメディアのスクリプト 362

ブータブルメディアのリモート操作 425

ブータブルメディアのローカル処理 380

ブータブルメディアの作成 306

ブータブルメディアの作成か、既成のブータブルメディアのダウンロードか 351

ブータブルメディアビルダー 354

ブータブルメディアを使用したディスクとボリュームの復元 314

ブータブルメディアを使用したバックアップと復元 363

ブータブルメディアを使用したファイルの復元 323

プールの作成 600

プールの削除 601

プールの編集 600

プールを使用した操作 600

フェールオーバーの停止 477

フェールバック 478

フェールバック オプション 479

フォレンジックデータ 274

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 276

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 277

フォレンジックバックアップのプロセス 275

フルパスの復元 331

プロキシサーバー 89

プロキシサーバー設定 132

プロセスがバックアップを変更することを許可する 506

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 131

へ

ベーシック ディスクのクローン作成 406

ベリファイ 346

ほ

ポート 89

ポリシールールを使用 210, 214

ボリューム シャドウ コピー サービス（VSS） 301

ボリューム ラベルの変更 423

ボリュームのドライブ文字の変更 422

ボリュームのフォーマット 423

ボリュームの作成 418

ボリュームの削除 421

ボリューム処理 417

ホワイトリストに登録されている項目の詳細を表示 525

ホワイトリストへの自動追加 524

ホワイトリストへの手動追加 524

ホワイトリスト設定 524

ま

マウントポイント 283, 331

マシンの検疫ロケーション 523

マシンの自動検出 156

マシンの手動登録 120, 153

マシンの復元 307

マシンプロパティとして暗号化 243

マシン全体を最新の状態にリカバリする方法 222

マシン全体を選択する 209

マスターデータベースの復元 452

マニュアル 229

マルウェア対策とWeb保護 503

マルチストリーミング 297

マルチプレクシング 298

マルチボリュームスナップショット 284

み

ミラー ストライプ ボリューム 418

ミラー ボリューム 418

め

メールボックスおよびメールボックスアイテムの復元 466

メールボックスのアイテムの復元 459, 467

メールボックスのバックアップ 447

メールボックスの選択 466

メールボックスの復元 457, 466

メディアUIからのメディアの登録 379

メディアから起動したコンピュータへの接続 378

メディアビルダを使用する理由 354

も

モバイル デバイスの保護 432

モバイルデバイスにデータを復元する方法 434

ゆ

ユーザー アクセス制御（UAC）の要件 95

ユーザーアカウントと組織部署の管理 631

ユーザーアカウントに関する要件 456

ユーザーがログオフ 237

ユーザーはアイドルです 236

ユーザー権限を割り当てる方法 138

ら

ライセンス 21

ライセンスクォータを別の管理サーバーに転送する 33

ライセンスの管理 25

ライセンスの問題 202

ライセンス種類 21

り

リアルタイム保護 508, 513

リアルタイム保護スキャン 503

リアルタイム保護のスキャンモードを設定する 508

リアルタイム保護の検出時のアクションを設定する 508

リスト内のパッチのライフタイム 543

リモート インストールのコンポーネント 97

リモートアクセス（RDPクライアントとHTML5クライアント） 550

リモートインストールの前提条件 94
リモートデスクトップアクセス 550
リモートのマシンに接続する方法 553
リモートワイプ 555
リモート接続 379, 626
リモート接続を共有 553

れ

レガシー機能のパラメータ 150
レプリカのテスト 476
レプリカの用途 475
レプリカへのフェールオーバー 477
レプリケーション 250
レプリケーションオプション 478
レプリケーションとバックアップ 475
レプリケーション計画の作成 476
レポート 581, 638
レポートデータのダンプダンプ 584
レポートの基本操作 583
レポート構造のエクスポートとインポート 584
レポジトリからのパッケージのインストール 69

ろ

ローカルイントラネットサイトのリストへのコンソールの追加 184
ローカルに接続されたストレージの使用 488
ローカルバックアップからファイルを抽出 324
ローカルまたはドメインのパスワードの失効に関する警告を表示する 621
ローカル接続 379
ローカル接続されたテープ ドライブのブータブル メディアによる復元 597
ローカル接続されたテープデバイスへのコンピュータのバックアップ 593
ロールの継承 633
ログオンアカウントで必要な権限 138
ログの切り詰め 282
ロケーションの暗号化 615
ロケーションの十分な空き領域 614

わ

ワークロードへのライセンスの割り当て 38
ワンクリック復元 284
ワンクリック復元でマシンをリカバリする 285

漢字

悪意あるWebサイトへのアクセス 517
圧縮レベル 269
安全な復元 305
暗号化 243
暗号化ソフトウェアとの互換性 71
暗号化の動作方法 245
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 240
以下の開始・終了時刻に該当 238
異なるコンピュータを異なる時間帯にバックアップする 615
一般的なインストール ルール 71
一般的な制限 612
一般的な要件 438
一覧の収集 602
一覧の収集方法 602
永久ライセンスの管理 42
永続的フェールオーバーの実行 478

演算子 567

仮想アプライアンスのデプロイ 169

仮想アプライアンスの設定 166, 169

仮想コンピュータのバインド 489

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） 302, 479

仮想コンピュータのレプリケーション 474

仮想コンピュータの特別な操作 471

仮想コンピュータの復元 311

仮想コンピュータへの変換 246, 349

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 249

仮想サーバー上に仮想コンピュータを作成する場合 249

仮想環境の管理 492

開始する前に 165, 168

開始条件 235

概要ダッシュボード 569

各Storage Nodeでは重複除外ロケーションを1つに制限する 614

各マシンの正常なバックアップの後にテープをスロットに戻す 296

各マシンの正常なバックアップの後にテープを取り出す 296

拡張子と例外ルール 548

確定と標準復元 474

確定に関する注意点 474

隔離されたファイルをホワイトリストに追加する 524

完全バックアップの作成時にスタンドアロン テープドライブのテープを上書きする 297

監視とレポート 569

管理アカウント 631

管理アカウントロール 632

管理アカウントを追加 634

管理サーバー 369

管理サーバー（オンプレミスデプロイメントのみ） 58

管理サーバーインストールパラメータ 112, 116

管理サーバーにライセンスキーを追加する 41

管理サーバーの種類 22

管理サーバーの登録解除 39

管理サーバーの有効化 27

管理サーバーへのライセンス割り当て 30

管理サーバーをマイグレーションする 124

管理されたロケーション間のバックアップのレプリケーション 252

管理対象ロケーション 209

管理対象ロケーションの追加 610

企業ホワイトリスト 523

基本パラメータ 141, 146

基本的な予防措置 404

既にインストールされているエージェント for VMwareの登録 100

既存の仮想アプライアンスをアップデートする 176

既存の脆弱性 577

既知の問題 39

起動モード 328

起動用の環境におけるドライバへのアクセスを確認 317

旧Acronis製品によって書き込まれたテープの読み取り 592

共通バックアップ ルール 71

共通パラメータ 108, 115

脅威フィード 544

継続的データ保護（CDP） 216

継続的データ保護でサポートされているデータソースとバックアップ先 218

継続的に保護されているバックアップを見分ける方法 221

計画の競合の解決 201

結果 594, 596

検疫 507, 522

検疫されたファイルの管理 523

検索クエリ 558

検出されたマシン 571

検出されたマシンの管理 163

検出された脆弱性の管理 532

検出された保護されていないファイルの管理 547

現在のAcronisアカウントにライセンスを追加 26

現在のユーザーの前回ログインに関する通知を表示する 621

言語の変更 183

高速 LAN 614

高速の増分/差分バックアップ 271

再スキャン 604

再起動を伴う復元 314

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 330

再配分 489

最近のバックアップ取得なし 578

最近影響を受けたもの 578

最新の保護定義のソース 626

最低 2.5GHz のクロック レートを発揮するマルチコア プロセッサー 614

災害復旧 336, 636

削除 607

仕組み 217, 245, 276, 305, 346, 504, 515, 534, 539, 544, 546, 551, 572

使用可能なバックアップ オプション 253

使用可能な復元オプション 326

使用例 250, 264, 338, 471, 475, 491

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 259

事前に定義されたプール 599

次のテープデバイスとドライブを使用する 297

自己署名証明書の使用 193

自己防御機能 506

自動ドライバ検索 317

自動パッチ承認 539

自動パッチ承認の設定 539

自動検出と手動検出 159

自動検出の仕組み 157

取り出し 606

手順 3

グループ ポリシー オブジェクトの設定 175

手順1 129

登録トークンの生成 175

手順2 130

.mstトランスフォームファイルの作成とインストールパッケージの抽出 175

手順3 130

手順4 131

手動でのバックアップの開始 252

手動でのパラメータ指定による製品のインストールやインストール解除 107, 140

手動のパッケージインストール 69

手動バインド 490

手動パッチ承認 542

週単位のバックアップ 303

従量制課金の接続時には開始しない 239

重複除外 612

重複除外データベースと重複除外ロケーションを別の物理デバイスに配置する 613

重複除外のベスト プラクティス 613

重複除外の制限 612

準備

WinPE 2.x および 3.x 373

WinPE 4.0 以降 374

処理の前後のコマンド 290, 332, 479

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） 270, 330

初期レプリカのシード 479

除外 510, 514, 522

消去 606

詳細 513

詳細ストレージオプション 224, 587

常に増分（単一ファイル） 209

情報パラメータ 117, 149

条件 272

信頼されたサイトのリストへのコンソールの追加 186

信頼できる接続とブロックされた接続を設定する 506

信頼できる認証局が発行した証明書の使用 194

振る舞い検知 507

振る舞い検知設定 507

迅速な復元のためにディスク キャッシュを使用します 333

推奨 Web ブラウザ 52

推奨事項 329

制限事項 39, 52, 60, 66, 90-91, 93, 208, 216, 226, 247, 252, 320, 329, 464, 475, 482, 526, 572, 591, 616

制限値（クォータ） 635

製品のアンインストール 179

静的グループの作成 557

静的グループへのデバイスの追加 557

脆弱性のあるマシン 577

脆弱性診断 528

脆弱性診断ウィジェット 577

脆弱性診断とパッチ管理 528

脆弱性診断の設定 530

前提条件 124, 156, 174, 177, 190, 216, 285, 438, 471, 593-594

操作を実行するコンピュータ 252

操作手順 604

著作権情報 16

直接選択 210, 213

追加のスケジュールオプション 231

通知 637

定期的に実行されるESXiおよびHyper-Vへの変換とバックアップからの仮想マシンの実行 248

定義済みスクリプト 362

適用済みの計画と競合する計画 201

電子メールサーバー 620

電子メールによる通知 269, 619

登録 229

登録パラメータ 142, 147

登録済みの VMwareエージェントの設定 101

統合Windows認証のためのWebブラウザの設定 183

同時にバックアップされる仮想マシンの合計数の制限 497

特殊文字やブランクスペースを使用したパスワード 123, 155

特定の条件に一致するファイルを含めるか除外する 271

配置エージェント 96

配置エージェントの動作について 96

配分アルゴリズム 489

配分結果の表示 489

非アクティブのユーザーをログアウトさせる時間 621

非表示のファイルとフォルダをすべて除外する 273

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 68

必要なユーザー権限 449

不良セクタを無視する 270

部署 631

部署および管理アカウント 631

部署の作成 635

復元 304, 463

復元オプション 325

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。 334

復元されたコンピュータの高可用性 497

復元するバックアップ済みデータの選択 616

復元のチートシート 304

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 334

復元後に実行するコマンド 333

復元後に電源オンにする 335

復元前に実行するコマンド 332

複数のネットワーク接続の事前設定 371

複数の計画のデバイスへの適用 201

複数の部署における管理アカウント 634

物理データ配送 289

物理データ配送サービスについて 289

物理データ配送プロセスの概要 289

物理マシンをリカバリする 307

物理マシンを仮想マシンにリカバリする 309

分割 295

並行操作 591

別スロットへの移動 601

別のプールへの移動 601

別のロケーションにバックアップする場合 230

変換に関する注意点 246

変換方法 246

変数オブジェクト 365

変数の使用 263

変数を含まない名前 263

保護ステータス 571

保護の設定 623

保護計画での暗号化 243

保護計画での仮想マシンへの変換 248

保護計画で実行できるアクション 202

保護計画とモジュール 199

保護計画の作成 199

保護計画を使用した操作 202

保護定義のアップデート 623

保持ルール 241

保留中の操作 424

無人インストールまたはインストール解除 106, 139

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 108, 141, 146

名前の変更 606

要件 314, 324, 338

留意事項 432

例 118-120, 122, 144, 150-152, 154, 236-241

"不良ブロック" 緊急バックアップ 234

Fedora 14にパッケージを手動でインストールする 70