Acronis
COMPUTE WITH CONFIDENCE
WWW.ACRONIS.CO.JP

Acronis® Backup & Recovery ™ 10 Advanced Server

ユーザーズガイド

目次

1. Acronis® Backup & Recovery™ 10 の概要

1.1. Acronis Backup & Recovery 10 の概要

Acronis Backup & Recovery 10 は、Acronis の特許取得済みのディスク イメージ作成技術およびベア メタル復元技術に基づき、次世代の障害回復ソリューションとして Acronis True Image Echo を継承しています。

Acronis Backup & Recovery 10 は、Acronis True Image Echo 製品ファミリから次の利点を継承しています。

- オペレーティング システム、全アプリケーション、およびデータを含む、ディスク全体またはボリューム全体のバックアップ
- 任意のハードウェアへのベア メタル復元
- ファイルとフォルダのバックアップおよび復元
- 1 台のコンピュータからエンタープライズまでのスケーラビリティ
- Windows 環境と Linux 環境両方のサポート
- 分散されたワークステーションやサーバーの集中管理
- ストレージ リソースの最適化のための専用サーバー

Acronis Backup & Recovery 10 には、組織が困難な復元時間目標を達成しながらも、資本支出やソフトウェアの保守コストを削減するために役立つ新しい利点があります。

- **既存の IT インフラストラクチャの活用**

  ストレージの消費およびネットワーク帯域幅の使用率を抑えるデータの重複除外

  バックアップ元とバックアップ先の両方のストレージでバックアップ データの重複除外を実現できる柔軟性の高い重複除外メカニズム

  自動テープ ライブラリのサポートの強化

  下位互換性および Acronis True Image Echo からの容易なアップグレード

- **高度に自動化されたデータ保護**

  バックアップ ポリシーによる総合的なデータ保護計画 (バックアップ、バックアップの保持とベリファイ)

  パラメータのカスタマイズが可能な組み込みのハノイの塔バックアップ スキームと GFS(Grandfather-Father-Son) バックアップ スキーム

  バックアップ開始のために選択できるさまざまなイベントと条件

- **ポリシー ベースの集中管理**

  コンピュータのグループへのバックアップ ポリシーの適用

  静的または動的なコンピュータのグループ化

  物理コンピュータまたは仮想コンピュータのグループ化

- **仮想環境による容易な作業**

  個別のコンピュータへのバックアップ ソフトウェアのインストールを必要としない仮想コンピュータのバックアップと復元

  VMware、Microsoft、Parallels、または Citrix の設定済み仮想コンピュータへのバックアップの変換

- **再設計された GUI**

  迅速で実用的な意思決定ができるダッシュボード

  すべての構成済みの操作と実行中の操作、および操作の成否が色分けされた概要表示

- **エンタープライズ レベルのセキュリティ**

  操作の実行およびバックアップのアクセスに必要なユーザー権限の制御

  最小限のユーザー権限によるサービスの実行

  バックアップ エージェントへのリモート アクセスの制限

  製品コンポーネント間での安全な通信

  コンポーネントの認証のためのサードパーティ証明書の利用

  データの転送およびストレージのためのデータ暗号化オプション

  ファイアウォールで保護された集中管理ストレージ ノードへのリモート コンピュータのバックアップ

1.2. はじめに

直接管理

1. Acronis Backup & Recovery 10 管理コンソールと Acronis Backup & Recovery 10 エージェントをインストールします。
2. コンソールを起動します。

   Windows

   ［スタート］メニューからコンソールを選択して起動します。

   Linux

   root または通常のユーザーとしてログインし、必要に応じてユーザーを切り替えます。次のコマンドを使用してコンソールを起動します。

   ```
   /usr/sbin/acronis_console
   ```

3. エージェントがインストールされているコンピュータにコンソールを接続します。

次の手順

次に行う操作について確認するには、「基本的な概念『ページ参照 30』」をご参照ください。

GUI 要素について理解するには、「管理コンソールの使用『ページ参照 11』」をご参照ください。

Linux で root 以外のユーザーがコンソールを起動できるようにする方法について確認するには、「ローカル接続の権限『ページ参照 89』」をご参照ください。

Linux を実行しているコンピュータへのリモート接続を有効にする方法について確認するには、「Linux でのリモート接続の権限『ページ参照 90』」をご参照ください。

集中管理

初めは、前の説明のように直接管理を使用して 1 台のコンピュータを管理することをお勧めします。

集中管理を開始する手順は、次のとおりです。

1. Acronis Backup & Recovery 10 管理サーバー『ページ参照 22』をインストールします。
2. データ保護が必要なコンピュータに Acronis Backup & Recovery 10 エージェントをインストールします。エージェントをインストールするときに、それぞれのコンピュータを管理サーバーに登録します。そのためには、インストール ウィザードのいずれかのウィンドウで、サーバーの IP アドレスまたは名前と集中管理を行う管理者のログイン情報を入力します。
3. 操作を行うコンピュータに Acronis Backup & Recovery 10 管理コンソール『ページ参照 25』をインストールします。Windows と Linux のコンソールのディストリビューションを選択できる場合は、Windows 上にインストールされたコンソールを使用することをお勧めします。Acronis ブータブル メディア ビルダをインストールします。
4. コンソールを起動します。ブータブル メディアを作成します。
5. コンソールを管理サーバーに接続します。

簡単な集中管理の方法

- **バックアップ**

[バックアップ] コントロールを使用し、バックアップするコンピュータを選択して、そのコンピュータ上にバックアップ計画『ページ参照 421』を作成します。複数のコンピュータ上に順番にバックアップ計画を作成することができます。

- **復元**

[復元] コントロールを使用して、データの復元が必要なコンピュータを選択し、そのコンピュータ上に復元タスクを作成します。複数のコンピュータ上に順番に復元タスクを作成することができます。

コンピュータ全体または起動しないオペレーティング システムを復元するには、ブータブル メディア『ページ参照 423』を使用します。管理サーバーを使用してブータブル メディアによる処理を制御することはできませんが、コンソールをサーバーから接続解除し、メディアから起動したコンピュータにそのコンソールを接続することができます。

- **計画とタスクの管理**

登録されているコンピュータ上に存在する計画とタスクを管理するには、**[ナビゲーション]** ツリーの **[コンピュータ] → [すべてのコンピュータ]** を選択し、各コンピュータを順番に選択します。下の **[情報]** ペインに、各コンピュータ上に存在している計画とタスクの状態と詳細が表示され、計画とタスクを開始、停止、編集、および削除することができます。

登録されているコンピュータ上に存在するすべてのタスクを表示する［**タスク**］ビューを使用することもできます。コンピュータ、バックアップ計画、その他のパラメータをフィルタとしてタスクに適用することができます。詳細については、コンテキスト ヘルプをご参照ください。

- **ログの表示**

登録されているコンピュータから収集された集中管理のログを表示するには、［**ナビゲーション**］ツリーで［**ログ**］を選択します。コンピュータ、バックアップ計画、その他のパラメータをフィルタとしてログ エントリに適用することができます。詳細については、コンテキスト ヘルプをご参照ください。

- **集中管理用格納域の作成**

すべてのバックアップ アーカイブを 1 つまたはいくつかのネットワーク上の場所に保存する場合は、集中管理用格納域をそれらの場所に作成します。格納域を作成した後は、［**ナビゲーション**］ツリーで［**格納域**］→［**集中管理**］→［'**格納域名**'］を選択することでその内容を表示および管理できます。格納域のショートカットが、登録されているすべてのコンピュータに配置されます。格納域の作成者または登録されているコンピュータのユーザーは、作成するバックアップ計画でその格納域をバックアップ先として指定できます。

高度な集中管理の方法

Acronis Backup & Recovery 10 が提供する集中管理機能を最大限に活用するために次のことを選択できます。

- **重複除外の使用**

1. Acronis Backup & Recovery 10 ストレージ ノード『ページ参照 23』をインストールし、管理サーバーに追加します。
2. ストレージ ノード上に重複除外された管理対象の格納域を作成します。
3. 重複除外された格納域にバックアップするすべてのコンピュータ上のエージェントに、Acronis 重複除外アドオンをインストールします。
4. 作成するバックアップ計画でバックアップ アーカイブの保存先として管理対象の格納域を使用するように設定します。

- **バックアップ計画の代わりのバックアップ ポリシーの作成**

集中管理用バックアップ ポリシーを設定し、［**すべてのコンピュータ**］グループに適用します。この方法により、1 回の操作で各コンピュータにバックアップ計画を配置します。トップ メニューから［**アクション**］→［**バックアップ ポリシーの作成**］を選択し、コンテキスト ヘルプをご参照ください。

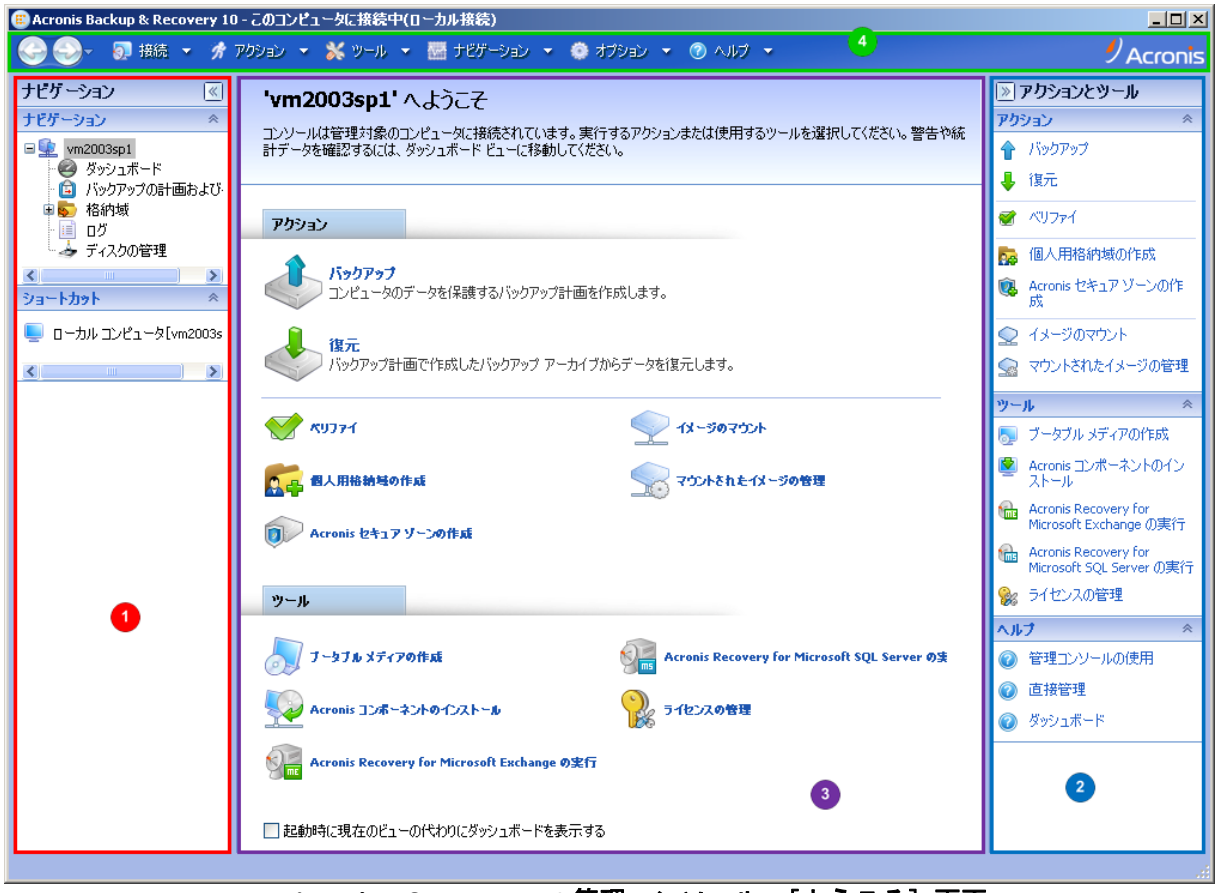
- **管理サーバーに登録されたコンピュータのグループ化**

登録されているコンピュータを適切なパラメータでグループ化し、いくつかのポリシーを作成して、各ポリシーを該当するコンピュータのグループに適用します。詳細については、「登録されたコンピュータのグループ化『ページ参照 71』」をご参照ください。

高度な集中管理の包括的な例については、「異種ネットワーク内での集中データ保護の設定『ページ参照 66』」をご参照ください。

1.2.1. 管理コンソールの使用

コンソールを管理対象のコンピュータ『ページ参照 426』または管理サーバー『ページ参照 429』に接続するとすぐに、それぞれの項目が管理コンソールに表示され(メニュー、［**ようこそ**］画面のワークスペース、［**ナビゲーション**］ペイン、［**アクションとツール**］ペイン内)、エージェントまたはサーバーに固有の操作を実行できるようになります。



Acronis Backup & Recovery 10 管理コンソール - ［ようこそ］画面

管理コンソールの主要な要素

	名前	説明
1	［**ナビゲーション**］ペイン	［**ナビゲーション**］ツリーと［**ショートカット**］バーがあり、さまざまなビューへ移動することができます(「［ナビゲーション］ペイン『ページ参照 12』」をご参照ください)。
2	［**アクションとツール**］ペイン	実行可能なアクションのセットのバーとツールのバーが表示されます(「［アクションとツール］ペイン『ページ参照 14』」をご参照ください)。

3	**ワークスペース**	バックアップ計画、ポリシー、タスクの作成、編集、管理、およびその他の操作を実行する主要な作業場所。メニュー、**［ナビゲーション］**ツリー、または**［アクションとツール］**ペインで選択した項目に応じて異なるビューとアクション ページ『ページ参照 16』が表示されます。
4	**メニュー バー**	プログラム ウィンドウの上部に表示され、両方のペインで使用可能なすべての操作を実行できます。メニュー項目は動的に変化します。

管理コンソールを快適に操作するには、1024x768 以上のディスプレイ解像度が必要です。

1.2.1.1. ［ナビゲーション］ペイン

［ナビゲーション］ペインには、**［ナビゲーション］**ツリーと**［ショートカット］**バーがあります。

［ナビゲーション］ツリー

［ナビゲーション］ツリーを使用して、各プログラム ビューに移動することができます。ビューは、コンソールが管理対象のコンピュータと管理サーバーのどちらに接続されているかによって異なります。

管理対象のコンピュータのビュー

コンソールが管理対象のコンピュータに接続されている場合は、［ナビゲーション］ツリーで次のビューを使用できます。

- **［コンピュータ名］** - ツリーのルートは**［ようこそ］**ビューとも呼ばれます。コンソールが現在接続されているコンピュータの名前が表示されます。このビューを使用して、管理対象のコンピュータ上で使用できる主な操作にすばやくアクセスすることができます。
  - **［ダッシュボード］** - 管理対象のコンピュータでデータが正常に保護されているかどうかを一目で確認するには、このビューを使用します。
  - **［バックアップの計画およびタスク］** - 管理対象のコンピュータ上のバックアップ計画およびタスクを管理するには、このビューを使用します。計画とタスクの実行、編集、停止、削除、それらの状態とステータスの表示、計画の監視を行います。
  - **［格納域］** - 個人用格納域およびそこに保存されるアーカイブの管理、新しい格納域の追加、既存の格納域の名前変更と削除、格納域のベリファイ、バックアップ内容の参照、仮想ドライブとしてのバックアップのマウントなどを行うには、このビューを使用します。
  - **［ログ］** - 管理対象のコンピュータ上でプログラムによって実行された処理に関する情報を調べるには、このビューを使用します。
  - **［ディスクの管理］** - コンピュータのハード ディスク ドライブに関する操作を実行するには、このビューを使用します。

管理サーバーのビュー

コンソールが管理サーバーに接続されている場合は、［ナビゲーション］ツリーで次のビューを使用できます。

- **［管理サーバー名］** - ツリーのルートは **［ようこそ］** ビューとも呼ばれます。コンソールが現在接続されている管理サーバーの名前が表示されます。このビューを使用して、管理サーバー上で使用できる主な操作にすばやくアクセスすることができます。
  - **［ダッシュボード］** - 管理サーバーに登録されたコンピュータでデータが正常に保護されているかどうかを一目で確認するには、このビューを使用します。
  - **［バックアップ ポリシー］** – 管理サーバー上に存在するバックアップ ポリシーを管理するには、このビューを使用します。
  - **［物理コンピュータ］** - 管理サーバーに登録されているコンピュータを管理するには、このビューを使用します。
  - **［仮想コンピュータ］** - 登録されている物理コンピュータおよびエージェント for ESX/ESXi がインストールされた登録されているコンピュータから仮想コンピュータを管理するには、このビューを使用します。
  - **［格納域］** - 集中管理用格納域とそこに保存されるアーカイブの管理(新しい管理対象の格納域と管理対象外の格納域の作成、既存の格納域の名前の変更と削除)を行うには、このビューを使用します。
  - **［ストレージ ノード］** - ストレージ ノードを管理するにはこのビューを使用します。ノードによって管理される集中管理用格納域を作成できるようにするためにストレージ ノードを追加します。
  - **［タスク］** - タスクの管理(タスクの実行、編集、停止、削除、タスクの状態の監視、タスクの履歴の確認)を行うには、このビューを使用します。
  - **［ログ］** - 管理対象のエンティティ グループの作成、ポリシーの適用、集中管理用格納域の管理などの集中管理操作の履歴、および登録されているコンピュータとストレージ ノードのローカル ログに記録された処理の履歴を参照するには、このビューを使用します。

［ショートカット］バー

［ショートカット］ バーは［ナビゲーション］ツリーの下に表示されます。このバーにショートカットとしてコンピュータを追加することで、必要なときに簡単にコンピュータに接続できます。

コンピュータにショートカットを追加する手順は、次のとおりです。

1. コンソールを管理対象のコンピュータに接続します。
2. ［ナビゲーション］ツリーでコンピュータの名前(［ナビゲーション］ツリーのルート要素)を右クリックし、**［ショートカットの作成］** をクリックします。

   コンソールとエージェントが同じコンピュータにインストールされている場合は、このコンピュータのショートカットが **[ローカル コンピュータ [コンピュータ名]]** として［ショートカット］バーに自動的に追加されます。

   コンソールが Acronis 管理サーバーに接続されている場合は、ショートカットが **［AMS [コンピュータ名]］** として自動的に追加されます。

1.2.1.2. ［アクションとツール］ペイン

［アクションとツール］ペインを使用すると、Acronis Backup & Recovery 10 を簡単かつ効率的に操作することができます。このペインのツールバーからプログラムの操作やツールをすばやく選択することができます。**［アクションとツール］**バーの項目はすべて、プログラム メニューにも表示されます。

バー

'[項目の名前]' アクション

いずれかのナビゲーション ビューで選択した項目に対して、実行可能な一連の操作が表示されます。操作をクリックすると、それぞれのアクション ページ『ページ参照 18』が表示されます。それぞれのナビゲーション ビューの項目ごとに独自の操作のセットがあります。バーの名前は、選択した項目に応じて変わります。たとえば、**［バックアップの計画およびタスク］**ビューで「*システムのバックアップ*」という名前のバックアップ計画を選択した場合、アクション バーの名前は**［'システムのバックアップ' アクション］**になり、バックアップ計画に対して一般的に実行される操作のセットが表示されます。

これらの操作はすべて、それぞれのメニュー項目からアクセスすることもできます。いずれかのナビゲーション ビューで項目を選択すると、メニュー バーにメニュー項目が表示されます。

［'項目名' アクション］バーの例

アクション

管理対象のコンピュータまたは管理サーバー上で実行できる一般的な操作の一覧が表示されます。すべてのビューで常に同じ一覧が表示されます。操作をクリックすると、それぞれのアクション ページ(「アクション ページ『ページ参照 18』」をご参照ください.)が表示されます。

これらの操作はすべて、［**アクション**］メニューからアクセスすることもできます。

管理対象のコンピュータおよび管理サーバーの［アクション］バー

ツール

Acronis のツールの一覧が表示されます。すべてのプログラム ビューで常に同じ一覧が表示されます。

これらのツールはすべて、［**ツール**］メニューからアクセスすることもできます。

［ツール］バー

ヘルプ

ヘルプ トピックの一覧が表示されます。Acronis Backup & Recovery 10 のそれぞれのビューおよびアクション ページごとに特定のヘルプ トピックの一覧が表示されます。

1.2.1.3. ペインの操作

ペインの展開または最小化の方法

デフォルトでは、［**ナビゲーション**］ペインが展開された状態で表示され、［**アクションとツール**］は最小化されます。追加のワークスペースを空けるためにペインを最小化する場合があります。このためには、ボタン( - ［**ナビゲーション**］ペインの場合、  - ［**アクションとツール**］ペインの場合)をクリックします。ペインが最小化され、ボタンの向きが変わります。ボタンをもう一度クリックするとペインが展開されます。

ペインの境界の変更方法

1. ペインの境界をポイントします。
2. ポインタが二重矢印になったら、ポインタをドラッグして境界を移動します。

管理コンソールは、ペインの境界の位置が変更されたことを「記憶」しています。次に管理コンソールを実行したときには、すべてのペインの境界が前回変更した位置に表示されます。

1.2.1.4. ワークスペース、ビュー、アクション ページ

コンソールの操作の大半はワークスペースで行います。ここで、バックアップ計画、ポリシー、タスクの作成、編集、管理、およびその他の操作を実行します。メイン領域には、メニュー、［**ナビゲーション**］ツリー、または［**アクションとツール**］ペインで選択した項目に応じて、異なるビューとアクション ページが表示されます。

ビュー

ビューは、［ナビゲーション］ペイン『ページ参照 12』の［**ナビゲーション**］ツリーで任意の項目をクリックするとワークスペースに表示されます。

[タスク] ビュー

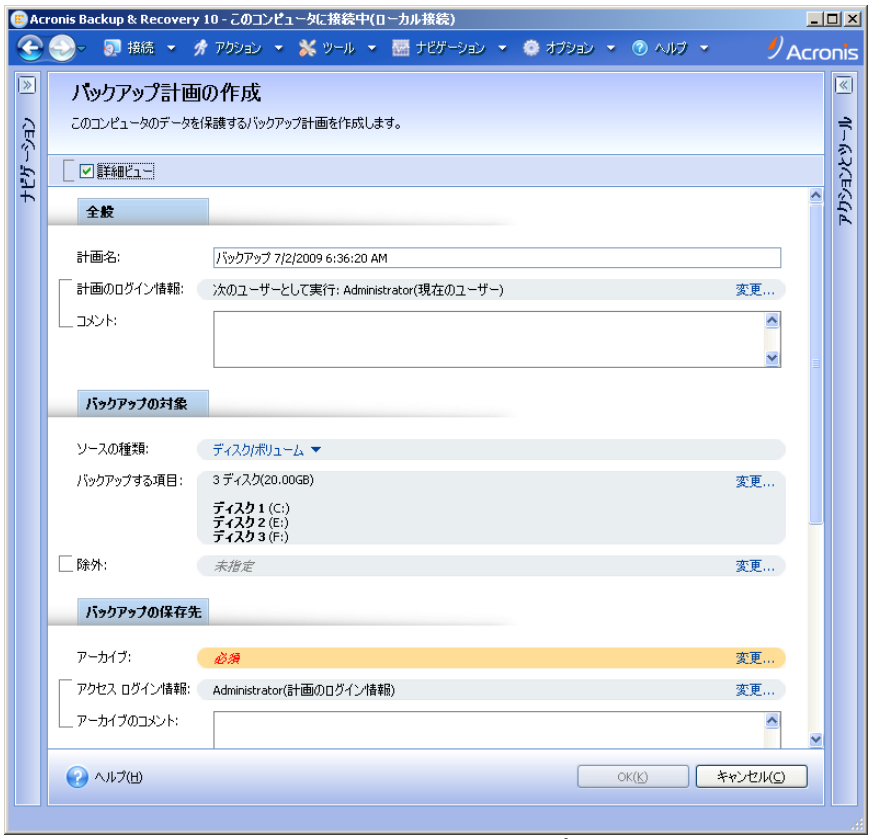
一般的なビューの操作方法

一般的に、すべてのビューに項目のテーブル、ボタンを備えたテーブル ツールバー、および **[情報]** パネルが含まれています。

- テーブルで必要な項目を検索するには、フィルタと並べ替えの機能を使用します。
- テーブルで目的の項目を選択します。
- **[情報]** パネル(デフォルトでは折りたたまれています)に項目の詳細が表示されます。
- 選択した項目についての操作を実行します。次のように、選択した項目について同じ操作を実行する方法がいくつかあります。
  - テーブル ツールバーのボタンをクリックする。
  - **[[項目の名前] アクション]** バー(**[アクションとツール]** ペイン)で項目をクリックする。
  - **[アクション]** メニューで項目を選択する。
  - 項目を右クリックし、コンテキスト メニューで操作を選択する。

アクション ページ

［**アクション**］メニューまたは［**アクションとツール**］ペインの［**アクション**］バーでいずれかのアクション項目をクリックすると、ワークスペースにアクション ページが表示されます。このページには、タスク、バックアップ計画、またはバックアップ ポリシーを作成して開始するために実行する必要のある手順が表示されます。

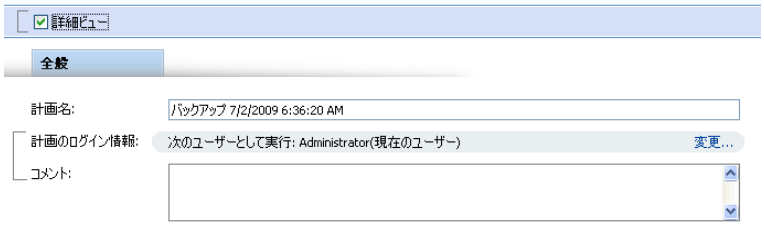


アクション ページ - バックアップ計画の作成

コントロールの使用と設定の指定

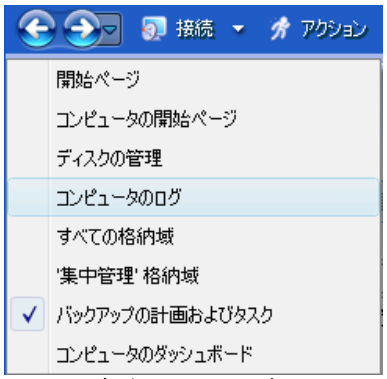
アクション ページには、基本と詳細の 2 つの表示方法があります。基本表示では、ログイン情報やコメントなどのフィールドは非表示になります。詳細表示を有効にすると使用可能なすべてのフィールドが表示されます。アクション ページの上部にある［**詳細ビュー**］チェックボックスをオンまたはオフにすることでビューを切り替えることができます。

ほとんどの設定は、それぞれの項目の右側にある［**変更...**］リンクをクリックすることで設定します。設定によっては、ドロップダウン リストから選択するか、ページのフィールドに手動で入力します。



アクション ページ - コントロール

Acronis Backup & Recovery 10 では、アクション ページで行った変更が記憶されます。たとえば、バックアップ計画の作成を開始した後で、計画の作成が完了する前に何らかの理由で別のビューに切り替えた場合、メニューで［**戻る**］ナビゲーション ボタンをクリックできます。または、いくつかの手順を進めた場合、**下**矢印をクリックして、計画の作成を開始したページを一覧から選択できます。このようにして、残りの手順を実行し、バックアップ計画の作成を完了することができます。



ナビゲーション ボタン

1.3. Acronis Backup & Recovery 10 コンポーネント

ここでは、Acronis Backup & Recovery 10 のコンポーネントとそれらの機能の簡単な説明の一覧を示します。

Acronis Backup & Recovery 10 には、次の 3 種類のコンポーネントが含まれています。

管理対象のコンピュータ用のコンポーネント(エージェント)

これらは、Acronis Backup & Recovery 10 によって管理されるコンピュータ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。各管理対象のコンピュータ上でエージェントが処理を実行するにはライセンスが必要です。エージェントには追加の機能を実行できるようにする複数の機能またはアドオンが含まれているので、追加のライセンスが必要になることがあります。

集中管理用のコンポーネント

これらのコンポーネントは、Acronis Backup & Recovery 10 の Advanced、SBS、Virtual の各エディションで提供され、集中管理機能を備えています。これらのコンポーネントの使用にライセンスは必要ありません。

コンソールとツール

コンソールはグラフィカル ユーザー インターフェイスを備えていて、エージェントや他の Acronis Backup & Recovery 10 コンポーネントにリモートから接続することができます。ブータブル メディア ビルダを使用して、エージェントや他のレスキュー ユーティリティをレスキュー環境で使用するためのブータブル メディアを作成することができます。レスキュー環境でエージェントのアドオンを使用できるかどうかは、メディア ビルダが動作しているコンピュータにアドオンがインストールされているかどうかによって異なります。

1.3.1. エージェント for Windows

このエージェントを使用して、Windows の下でディスク レベルおよびファイル レベルでデータを保護することができます。

ディスク バックアップ

ディスク レベルのデータ保護では、ディスクまたはボリューム ファイル システム全体とオペレーティング システムの起動に必要なすべての情報のバックアップ、またはセクタ単位でのすべてのディスク セクタのバックアップ(RAW モード)が基本になります。ディスクまたはボリュームのコピーを含むパッケージ形式のバックアップは、ディスク(ボリューム) バックアップまたはディスク(ボリューム) イメージと呼ばれます。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。

ファイル バックアップ

ファイル レベルのデータ保護では、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あるいはネットワーク共有上に存在するファイルおよびフォルダのバックアップが基本になります。ファイルは、元の場所にも別の場所にも復元できます。バックアップされたすべてのファイルとフォルダを復元することも個別に選択して復元することもできます。

1.3.1.1. Universal Restore

Universal Restore アドオンを使用すると、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で異なるハードウェアの復元機能を使用して、この機能を備えたブータブル メディアを作成することができます。Universal Restore は、ストレージ コントローラ、マザーボード、チップセットなどの Windows の起動にとって重要なデバイスの相違に対応できます。

1.3.1.2. 重複除外

エージェントでこのアドオンを使用すると、Acronis Backup & Recovery 10 ストレージ ノードによって管理されている重複除外格納域にデータをバックアップすることができます。

1.3.2. ブータブル コンポーネントとメディア ビルダ

エージェントのブータブル コンポーネントを使用すると、現在アクティブなオペレーティング システムがインストールされているボリュームの復元など、再起動を伴う処理が可能になります。処理が完了すると、コンピュータは再びそのオペレーティング システムで起動されます。ブータブル コンポーネントは Linux カーネルが基になっています。ブータブル コンポーネントをインストールせずに、ブータブル メディアを使用して再起動が必要な処理を実行することもできます。

Acronis ブータブル メディア ビルダは、ブータブル コンポーネントが含まれるブータブル メディア『ページ参照 423』を作成するための専用ツールです。エージェント for Windows と共に提供されるメディア ビルダでは、Windows 形式(C:、D:、¥¥server¥share)でボリュームおよびネットワークを表すブータブル メディアが作成されます。

Universal Restore アドオンを使用すると、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で異なるハードウェアの復元機能を使用して、この機能を備えたブータブル メディアを作成することができます。Universal Restore は、ストレージ コントローラ、マザーボード、チップセットなどの Windows の起動にとって重要なデバイスの相違に対応できます。

1.3.3. WinPE ISO ビルダ

Acronis WinPE ISO ビルダは、Windows プレインストール環境を基にしてブータブル メディア『ページ参照 423』を作成するための専用のツールです。このツールは、Windows を実行しているコンピュータにのみインストールできます。

1.3.4. エージェント for Linux

このエージェントを使用して、Linux の下でディスク レベルおよびファイル レベルでデータを保護することができます。

ディスク バックアップ

ディスク レベルのデータ保護では、ディスクまたはボリューム ファイル システム全体とオペレーティング システムの起動に必要なすべての情報のバックアップ、またはセクタ単位でのすべてのディスク セクタのバックアップ(RAW モード)が基本になります。ディスクまたはボリュームのコピーを含むパッケージ形式のバックアップは、ディスク(ボリューム) バックアップまたはディスク(ボリューム) イメージと呼ばれます。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。

ファイル バックアップ

ファイル レベルのデータ保護では、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あるいは smb または nfs プロトコルを使用してアクセスされるネットワーク共有上に存在するファイルおよびディレクトリのバックアップが基本になります。ファイルは、元の場所にも別の場所にも復元できます。バックアップされたすべてのファイルとディレクトリを復元することも個別に選択して復元することもできます。

1.3.4.1. ブータブル コンポーネントとメディア ビルダ

エージェントのブータブル コンポーネントを使用すると、現在アクティブなオペレーティング システムがインストールされているボリュームの復元など、再起動を伴う処理が可能になります。処理が完了すると、コンピュータは再びそのオペレーティング システムで起動されます。ブータブル コンポーネントは Linux カーネルが基になっています。ブータブル コンポーネントをインストールせずに、ブータブル メディアを使用して再起動が必要な処理を実行することもできます。

Acronis ブータブル メディア ビルダは、ブータブル コンポーネントが含まれるブータブル メディア『ページ参照 423』を作成するための専用ツールです。エージェント for Linux と共に提供されるメディア ビルダでは、Linux 形式(hda1、sdb2、smb://server/share)でボリュームおよびネットワークを表すブータブル メディアが作成されます。

1.3.4.2. 重複除外

エージェントでこのアドオンを使用すると、Acronis Backup & Recovery 10 ストレージ ノードによって管理されている重複除外格納域にデータをバックアップすることができます。

1.3.5. 集中管理用のコンポーネント

ここでは、Acronis Backup & Recovery 10 エディションに含まれ、集中管理機能を提供するコンポーネントについて説明します。これらのコンポーネントに加えて、データ保護が必要なすべてのコンピュータに Acronis Backup & Recovery 10 エージェントをインストールする必要があります。

1.3.5.1. 管理サーバー

Acronis Backup & Recovery 10 管理サーバーは、企業ネットワーク内のデータ保護を管理する中央のサーバーです。管理サーバーは、次の機能を管理者に提供します。

- Acronis Backup & Recovery 10 インフラストラクチャへの単一のエントリ ポイント
- バックアップ ポリシー『ページ参照 420』とグループを使用して多数のコンピュータ『ページ参照 416』上のデータを簡単に保護する方法
- 全社規模の監視機能
- 全社のバックアップ アーカイブ『ページ参照 420』を保存するための集中管理用格納域『ページ参照 427』を作成する機能
- ストレージ ノード『ページ参照 416』を管理する機能

ネットワーク上に複数の管理サーバーがある場合、それらのサーバーは独立して動作し、異なるコンピュータを管理し、異なる集中管理用格納域を使用してアーカイブを保存します。

管理サーバーのデータベース

管理サーバーは、次の 3 つの Microsoft SQL データベースを使用します。

- 登録されているコンピュータおよび管理者によって作成されたバックアップ ポリシーを含むその他の構成情報を保存する構成データベース。
- 登録されているコンピュータおよびストレージ ノードと管理サーバーを同期させるために使用される同期データベース。これは、頻繁に変更される処理データのデータベースです。
- 集中管理されるログを保存するレポート データベース。このデータベースは大きくなる場合があります。サイズは設定するログ レベルによって左右されます。

構成データベースと同期データベースは同じ Microsoft SQL Server(運用サーバーと呼ばれます)上に存在している必要があり、また管理サーバーと同じコンピュータにインストールすることが推奨されます。レポート データベースは同じ SQL サーバー上でも異なる SQL サーバー上でも構成できます。

管理サーバーをインストールするときに、運用サーバーとレポート サーバーの両方にどのサーバーを使用するかを選択できます。次の構成を選択できます。

1. インストール パッケージに付属し、同じコンピュータにインストールされる Microsoft SQL Server 2005 Express。この場合、3 つのデータベースを持つ SQL サーバー インスタンスが同じコンピュータ上に作成されます。
2. 以前に任意のコンピュータにインストールされている Microsoft SQL Server 2008(任意のエディション)
3. 以前に任意のコンピュータにインストールされている Microsoft SQL Server 2005(任意のエディション)

1.3.5.2. ストレージ ノード

Acronis Backup & Recovery 10 ストレージ ノードは、企業のデータ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、ネットワーク帯域幅、管理対象のコンピュータの CPU 負荷など)の使用を最適化することを目的としたサーバーです。この目的は、企業のバックアップ アーカイブ(管理対象の格納域)の専用ストレージとして機能する場所の作成と管理によって達成されます。

ストレージ ノードを使用すると、ハードウェア サポートの観点から拡張性と柔軟性に優れたストレージ インフラストラクチャを作成することができます。最大 20 のストレージ ノードを設定することが可能で、それぞれのノードが最大 20 の格納域を管理することができます。管理者は、Acronis Backup & Recovery 10 管理サーバー『ページ参照 429』からストレージ ノードを集中的に制御します。コンソールをストレージ ノードに直接接続することはできません。

ストレージ インフラストラクチャの設定

ストレージ ノードをインストールして管理サーバーに追加し(手順は管理対象のコンピュータの登録『ページ参照 429』に似ています)、集中管理用格納域『ページ参照 427』を作成します。集中管理用格納域を作成するときに、格納域のパス、格納域を管理するストレージ ノード、および格納域に対して実行する管理操作を指定します。

管理対象の格納域は次の場所に作成することができます。

- ストレージ ノードのローカルのハード ディスク ドライブ
- ネットワーク共有
- SAN(Storage Area Network)
- NAS(Network Attached Storage)
- ストレージ ノードにローカル接続されたテープ ライブラリ

管理操作は次のとおりです。

ストレージ ノード側のクリーンアップとベリファイ

管理対象外の格納域に保存されるアーカイブは、アーカイブを作成するエージェント『ページ参照 415』によって保持されます。これは、各エージェントが、データをアーカイブにバックアップするだけでなく、アーカイブに適用されるサービス タスク、およびバックアップ計画『ページ参照 421』によって指定された保持ルールとベリファイ ルールを実行することを意味します。管理対象のコンピュータの不要な CPU 負荷を取り除くために、サービス タスクの実行をストレージ ノードに任せることができます。タスクのスケジュールは、エージェントがインストールされたコンピュータ上に存在しており、そのコンピュータの時間とイベントを使用するため、スケジュールに従ってエージェントがストレージ ノード側のクリーンアップ『ページ参照 416』とストレージ ノード側のベリファイ『ページ参照 417』を開始する必要があります。そのためには、エージェントがオンラインになっている必要があります。それ以降の処理はストレージ ノードによって実行されます。

この機能を管理対象の格納域で無効にすることはできません。次の 2 つの操作はオプションです。

重複除外

管理対象の格納域は重複除外された格納域として設定することができます。つまり、同一のデータをこの格納域に一度だけバックアップし、バックアップ中のネットワーク使用量およびアーカイブによって使用されるストレージ容量を最小限に抑えます。詳細については、ユーザー ガイドの「重複除外『ページ参照 83』」をご参照ください。

暗号化

すべての読み書きがストレージ ノードによって透過的に暗号化および復号化されるように、管理対象の格納域を設定することができます。暗号化にはノード サーバーに保存された格納域専用の暗号化キーを使用します。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、格納域の内容はこのストレージ ノード自体にアクセスしなければ、復号化することはできません。

アーカイブがエージェントによって既に暗号化されている場合、ストレージ ノード側の暗号化はエージェントによって実行される暗号化によって適用されます。

1.3.5.3. PXE サーバー

Acronis PXE サーバーを使用すると、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コンピュータ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『ページ参照 423』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。

1.3.5.4. ライセンス サーバー

ライセンス サーバーを使用すると、Acronis 製品のライセンスを管理して、ライセンスが必要なコンポーネントをインストールすることができます。

Acronis ライセンス サーバーの詳細については、「Acronis ライセンス サーバーの使用」をご参照ください。

1.3.6. 管理コンソール

Acronis Backup & Recovery 10 管理コンソールは、Acronis Backup & Recovery 10 エージェントにリモートまたはローカルでアクセスするための管理ツールで、集中管理機能を備えたエディションでは Acronis Backup & Recovery 10 管理サーバーへのアクセスにも使用します。

コンソールには、Windows 上および Linux 上にインストールするための 2 つのディストリビューションがあります。どちらのディストリビューションでも任意の Acronis Backup & Recovery 10 エージェントおよび Acronis Backup & Recovery 10 管理サーバーに接続できますが、どちらか選択できる場合は Windows 用のコンソールを使用することをお勧めします。Linux 上にインストールするコンソールの機能には次のような制限があります。

- Acronis Backup & Recovery 10 コンポーネントのリモート インストールを使用できない。
- Active Directory の参照などの Active Directory 関連の機能を使用できない。

1.4. サポートされるオペレーティング システム

管理対象のコンピュータのコンポーネント

Acronis Backup & Recovery 10 エージェント for Windows

Acronis Backup & Recovery 10 Advanced Server

Acronis Backup & Recovery 10 Advanced Server Virtual Edition

- Windows Professional 2000 SP4/Professional XP SP2
- Windows Server 2000/Advanced Server 2000/Server 2003/Server 2008/SBS 2003/SBS 2008
- Windows XP Professional x64 Edition、Windows Server 2003/2008 の x64 Edition
- Windows Vista - Vista Home Basic および Vista Home Premium を除く、すべてのエディション

Virtual Edition に付属するエージェントは、単一の物理ホストでホストされる仮想コンピュータにインストールできます。

Acronis Backup & Recovery 10 Advanced Server SBS Edition

- Windows SBS 2003
- Windows SBS 2008

Acronis Backup & Recovery 10 Server for Windows

- Windows Professional 2000 SP4/Professional XP SP2
- Windows Server 2000/Advanced Server 2000/Server 2003/Server 2008/SBS 2003/SBS 2008
- Windows XP Professional x64 Edition、Windows Server 2003/2008 の x64 Edition
- Windows Vista - Vista Home Basic および Vista Home Premium を除く、すべてのエディション

エージェントへのリモート接続はできません。

Acronis Backup & Recovery 10 Advanced Workstation

- Windows Professional 2000 SP4/Professional XP SP2
- Windows XP Professional x64 Edition/Home Edition
- Windows Vista - すべてのエディション

Windows Home Edition にインストールされたエージェントへのリモート接続はできません。

Acronis Backup & Recovery 10 Workstation

- Windows Professional 2000 SP4/Professional XP SP2
- Windows XP Professional x64 Edition/Home Edition
- Windows Vista - すべてのエディション

エージェントへのリモート接続はできません。

Acronis Backup & Recovery 10 エージェント for Linux

Acronis Backup & Recovery 10 Advanced Server、Acronis Backup & Recovery 10 Advanced Server Virtual Edition、および Acronis Backup & Recovery 10 Server for Linux

- Linux 2.4.20 以降のカーネル(2.6.x カーネルを含む)および glibc 2.3.2 以降
- 以下を含む、さまざまな Linux ディストリビューション
  - Red Hat Enterprise Linux 4 および 5
  - CentOS 4 および 5
  - Fedora 9 および 10
  - Ubuntu 8.10(Intrepid Ibex)および 9.04(Jaunty Jackalope)
  - Debian 4(Lenny)および 5(Etch)
  - SUSE Linux Enterprise Server 10
  - openSUSE
  - Asianux
- 上記の Linux ディストリビューションの x64 版およびその他の Linux ディストリビューションもサポートされます。

  エージェント for Linux は、実際には 32 ビットの実行可能ファイルです。このエージェントは、認証のためにシステム ライブラリを使用します。64 ビットのディストリビューションでは、デフォルトでシステム ライブラリの 32 ビット バージョンがインストールされない場合があります。RHEL、CentOS、Fedora、または Scientific Linux などの 64 ビットの RedHat ベースのディストリビューションのエージェントを使用する場合は、次の 32 ビットのパッケージがシステムにインストールされていることを確認します。

pam.i386
libselinux.i386
libsepol.i386

これらのパッケージは、お使いの Linux ディストリビューションのレポジトリで使用できるようにしておく必要があります。

Virtual Edition に付属するエージェントは、単一の物理ホストでホストされる仮想コンピュータにインストールできます。

Acronis Backup & Recovery 10 エージェント for Hyper-V

- Windows Server 2008 x64 Edition(Hyper-V 使用)

このエージェントは、Acronis Backup & Recovery 10 エージェント for Windows に対するアドオンとして Hyper-V ホストにインストールされます。

Acronis Backup & Recovery 10 エージェント for ESX/ESXi

- VMware ESX Infrastructure 3.5 Update 2

エージェント for ESX/ESXi は、仮想アプライアンスとして提供されます。

エージェント for ESX/ESXi では、フリー ライセンス以外のすべての VMware ESXi ライセンスがサポートされます。これは、エージェントがリモートのコマンド ライン アプライアンスを使用するため、フリーの VMware ESXi では、このアプライアンスへのアクセスが読み取り専用のアクセスに制限されるためです。このエージェントは、VMware ESXi の評価期間中は動作します。フリーの VMware ESXi のプロダクト キーが入力されると、エージェント for ESX/ESXi は機能を停止します。

集中管理用のコンポーネント

Acronis ライセンス サーバー

- Windows Professional 2000 SP4/XP Professional SP2
- Windows Server 2000/Advanced Server 2000/Server 2003/SBS 2003/SBS 2008/Server 2008
- Windows XP Professional x64 Edition、Windows Server 2003/2008 の x64 Edition
- Windows Vista - Vista Home Basic および Vista Home Premium を除く、すべてのエディション

Acronis Backup & Recovery 10 管理コンソール

- Windows Professional 2000 SP4/XP Professional SP2
- Windows Server 2000/Advanced Server 2000/Server 2003/SBS 2003/BS 2008/Server 2008
- Windows XP Professional x64 Edition/Home Edition、Windows Server 2003/2008 の x64 Edition
- Windows Vista - すべてのエディション

Acronis Backup & Recovery 10 管理サーバーと Acronis Backup & Recovery 10 ストレージ ノード

- Windows Professional 2000 SP4/XP Professional SP2
- Windows Server 2000/Advanced Server 2000/Server 2003/SBS 2003/SBS 2008/Server 2008
- Windows XP Professional x64 Edition、Windows Server 2003/2008 の x64 Edition
- Windows Vista - Vista Home Basic および Vista Home Premium を除く、すべてのエディション

1.5. サポートされるファイル システム

Acronis Backup & Recovery 10 は、次のファイル システムをバックアップおよび復元できますが、次のような制限があります。

- FAT16/32
- NTFS
- Ext2/Ext3
- ReiserFS3 - Acronis Backup & Recovery 10 ストレージ ノード上に置かれているディスク バックアップから特定のファイルを選択して復元することはできません。
- ReiserFS4 - ボリュームの復元にはボリューム サイズの変更機能がありません。Acronis Backup & Recovery 10 ストレージ ノード上に置かれているディスク バックアップから特定のファイルを選択して復元することはできません。
- XFS - ボリュームの復元にはボリューム サイズの変更機能がありません。Acronis Backup & Recovery 10 ストレージ ノード上に置かれているディスク バックアップから特定のファイルを選択して復元することはできません。
- JFS - Acronis Backup & Recovery 10 ストレージ ノード上に置かれているディスク バックアップから特定のファイルを選択して復元することはできません。
- Linux SWAP

Acronis Backup & Recovery 10 は、破損したファイル システムやサポートされていないファイル システムを、セクタ単位でバックアップおよび復元することができます。

1.6. ハードウェア要件

ここでは、Acronis Backup & Recovery 10 コンポーネントをインストールして実行するためのハードウェアについて、最小要件と推奨される要件を示します。

Acronis Backup & Recovery 10 管理コンソール

項目	最小要件	推奨要件
コンピュータのプロセッサ	最新のプロセッサ、800MHz 以上 Itanium プラットフォームはサポートされません	1GHz 32 ビット(x86)または 64 ビット(x64)のプロセッサ
システム メモリ	128MB	512MB 以上
画面の解像度	800*600 ピクセル	1024*768 ピクセル以上
インストール先ディスクの空き領域	50MB	
その他のハードウェア	マウス	
		ネットワーク インターフェイス カードまたは仮想ネットワーク アダプタ
		ブータブル メディア作成用の CD-RW、DVD-RW ドライブ

Acronis Backup & Recovery 10 エージェント for Windows

項目	最小要件	推奨要件
システム メモリ	256MB	512MB 以上
インストール先ディスクの空き領域	100MB	

Acronis Backup & Recovery 10 エージェント for Linux

項目	最小要件	推奨要件
システム メモリ	256MB	512MB 以上
インストール先ディスクの空き領域	100MB	

Acronis Backup & Recovery 10 管理サーバー

項目	最小要件	推奨要件
システム メモリ	512MB	1GB 以上
インストール先ディスクの空き領域	25MB	
運用 SQL サーバーおよびレポート SQL サーバーで必要な領域	200MB	

Acronis Backup & Recovery 10 ストレージ ノード

項目	最小要件	推奨要件
システム メモリ	512MB	1.5GB 以上
インストール先ディスクの空き領域	40MB	
テープ データベースで必要な領域	10 アーカイブにつき約 1MB	

Acronis ライセンス サーバー

項目	最小要件	推奨要件
システム メモリ	128MB	256MB 以上
インストール先ディスクの空き領域	25MB	

1.7. サポート

Acronis テクニカル サポートへの連絡方法については、次のリンク先をご参照ください。
http://www.Acronis.co.jp/enterprise/support/

2. Acronis Backup & Recovery 10 について

ここの説明では、製品について明確に理解し、詳細な手順の説明がなくてもさまざまな状況で製品を使用できるようになることを目標としています。

2.1. 基本的な概念

Acronis Backup & Recovery 10 のグラフィカル ユーザー インターフェイスとドキュメントで使用される基本的な概念について理解しておいてください。詳しい知識のあるユーザーは、手順が示されたクイック スタート ガイドとしてこのセクションを利用してください。詳細については、コンテキスト ヘルプをご参照ください。

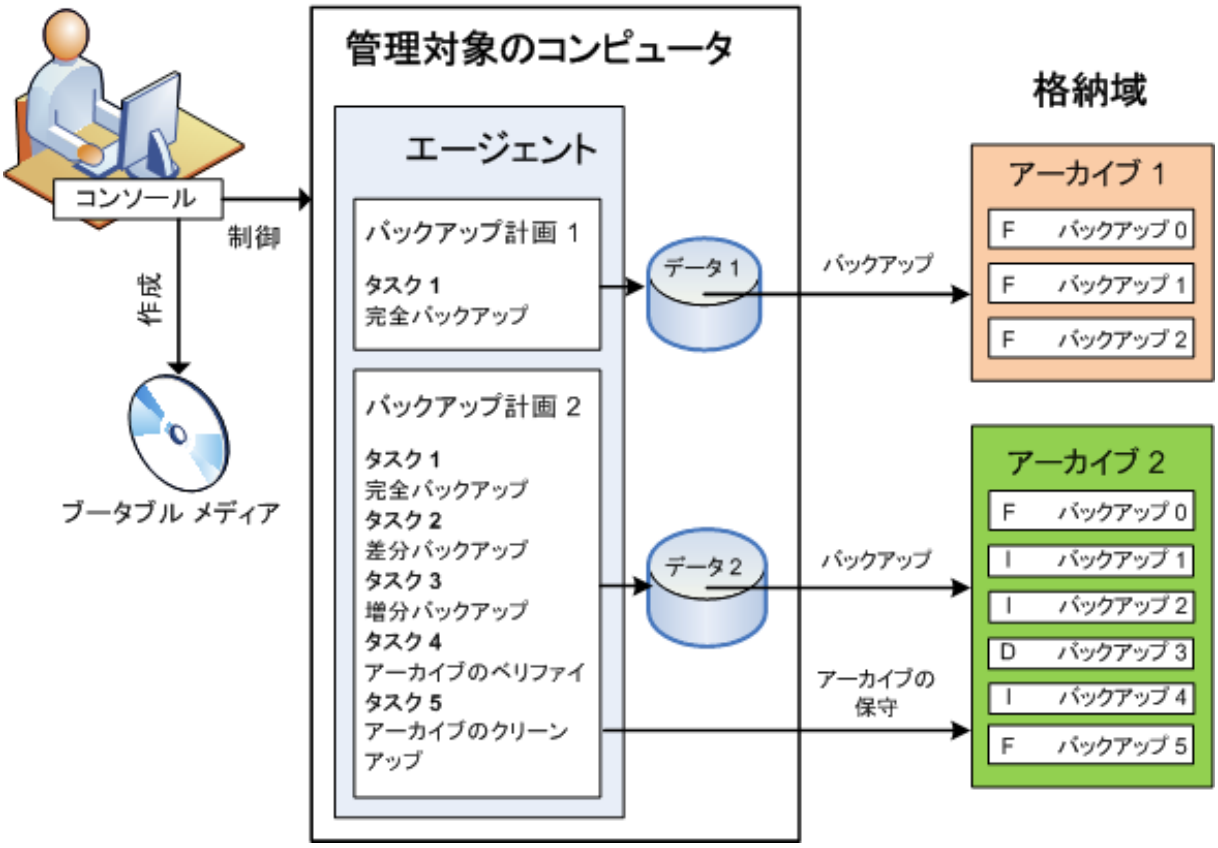
オペレーティング システムでのバックアップ

1. コンピュータのデータを保護するには、管理対象のコンピュータ『ページ参照 426』になるコンピュータに Acronis Backup & Recovery 10 エージェント『ページ参照 415』をインストールします。
2. グラフィカル ユーザー インターフェイスを使用してコンピュータを管理できるようにするには、エージェントと同じコンピュータまたは操作元になる任意のコンピュータに Acronis Backup & Recovery 10 管理コンソール『ページ参照 416』をインストールします。スタンドアロンの製品エディションの場合、コンソールはエージェントと共にインストールされるため、この手順をスキップしてください。
3. コンソールを起動します。システムの起動に失敗した場合にコンピュータのオペレーティング システムを復元できるようにするために、ブータブル メディア『ページ参照 423』を作成します。
4. コンソールを管理対象のコンピュータに接続します。
5. バックアップ計画『ページ参照 421』を作成します。

   バックアップ計画を作成するには、少なくとも、保護するデータと、バックアップ アーカイブ『ページ参照 420』を保存する場所を指定する必要があります。これらを指定すると、タスクが手動で開始されるたびにデータの完全バックアップ『ページ参照 420』を作成する 1 つのタスク『ページ参照 419』で構成される最小限のバックアップ計画が作成されます。複雑なバックアップ計画は、スケジュールにより実行され、完全バックアップ、増分バックアップ、または差分バックアップ『ページ参照 37』を作成し、バックアップのベリファイ『ページ参照 423』や古くなったバックアップの削除(アーカイブのクリーンアップ『ページ参照 415』)などのアーカイブ保守処理を実行する、複数のタスクから構成される場合があります。バックアップ処理は、前後に実行するバックアップ コマンド、ネットワーク帯域幅の調整、エラー対応、通知オプションなどのさまざまなバックアップ オプションを使用してカスタマイズできます。
6. **［バックアップの計画およびタスク］**ページを使用して、バックアップ計画とタスクに関する情報を表示し、それらの実行を監視します。操作ログを参照するには、**［ログ］**ページを使用します。

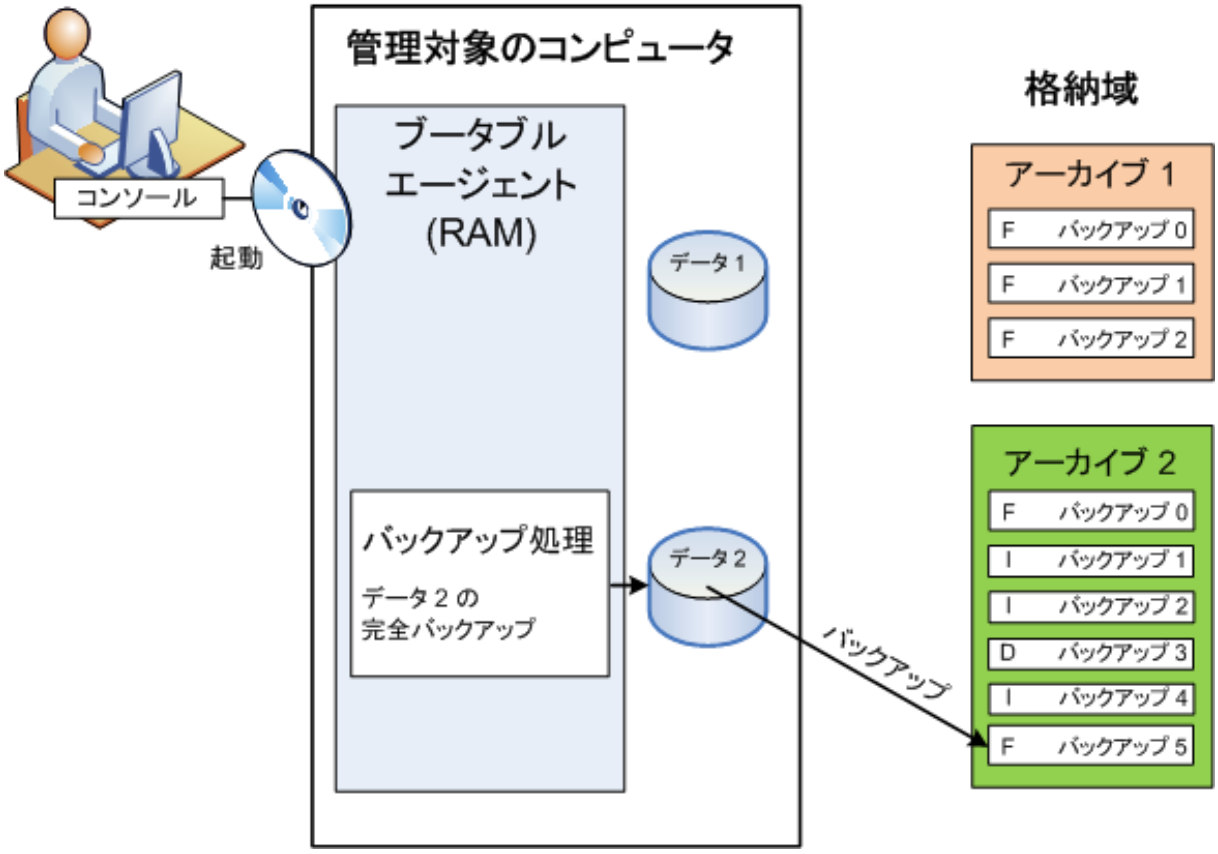
7. バックアップ アーカイブを保存する場所は、格納域『ページ参照 425』と呼ばれます。格納域の情報を表示するには、**［格納域］**ページに移動します。さらに特定の格納域に移動すると、アーカイブやバックアップを表示して、それらの手動操作(マウント、ベリファイ、削除、内容の表示)を実行することができます。また、復元するデータが含まれているバックアップを選択することもできます。

次の図は、前述の概念を示しています。詳細については、「用語集」をご参照ください。



ブータブル メディアを使用したバックアップ

ブータブル メディアを使用してコンピュータを起動し、簡単なバックアップ計画と同じ方法でバックアップ処理を設定して実行することができます。この方法は、起動に失敗したシステムからファイルや論理ボリュームを取り出す場合、オフラインのシステムのイメージを作成する場合、またはサポートされていないファイル システムをセクタ単位でバックアップする場合に役立ちます。



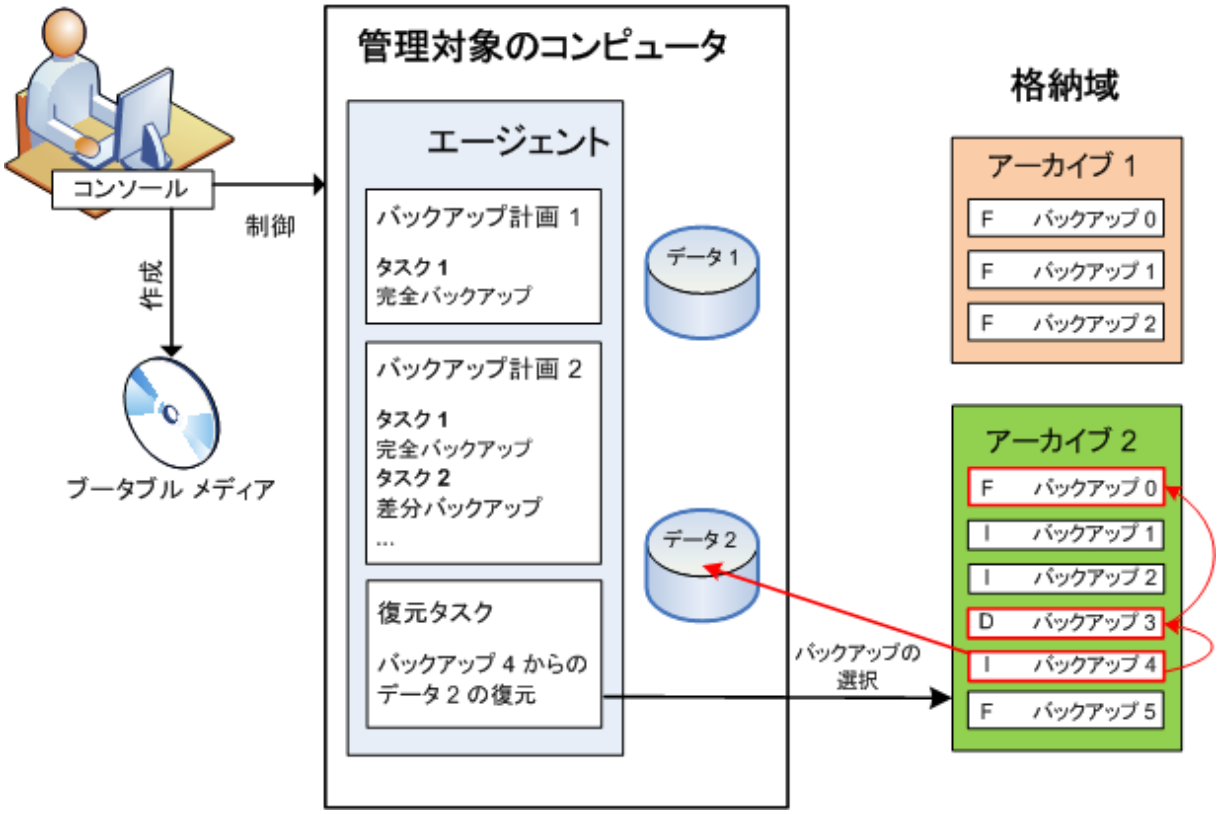
オペレーティング システムでの復元

データの復元の場合は、管理対象のコンピュータで復元タスクを作成します。格納域を指定してアーカイブを選択したら、バックアップの作成日時、またはより正確に、作成が開始された時刻を参考にバックアップを選択します。ほとんどの場合、データはその時点まで戻されます。

このルールに当てはまらない例:
トランザクション ログを含む 1 つのバックアップからデータベースを復元する場合(1 つのバックアップには複数の復元点があるため、さらに選択を行うことができます)。
スナップショットなしで作成されたファイル バックアップから複数のファイルを復元する場合(各ファイルは、バックアップに実際にコピーされた時点まで戻されます)。

また、データの復元先も指定します。復元処理は、前後に実行する復元コマンド、エラー対応、通知オプションなどの復元オプションを使用してカスタマイズできます。

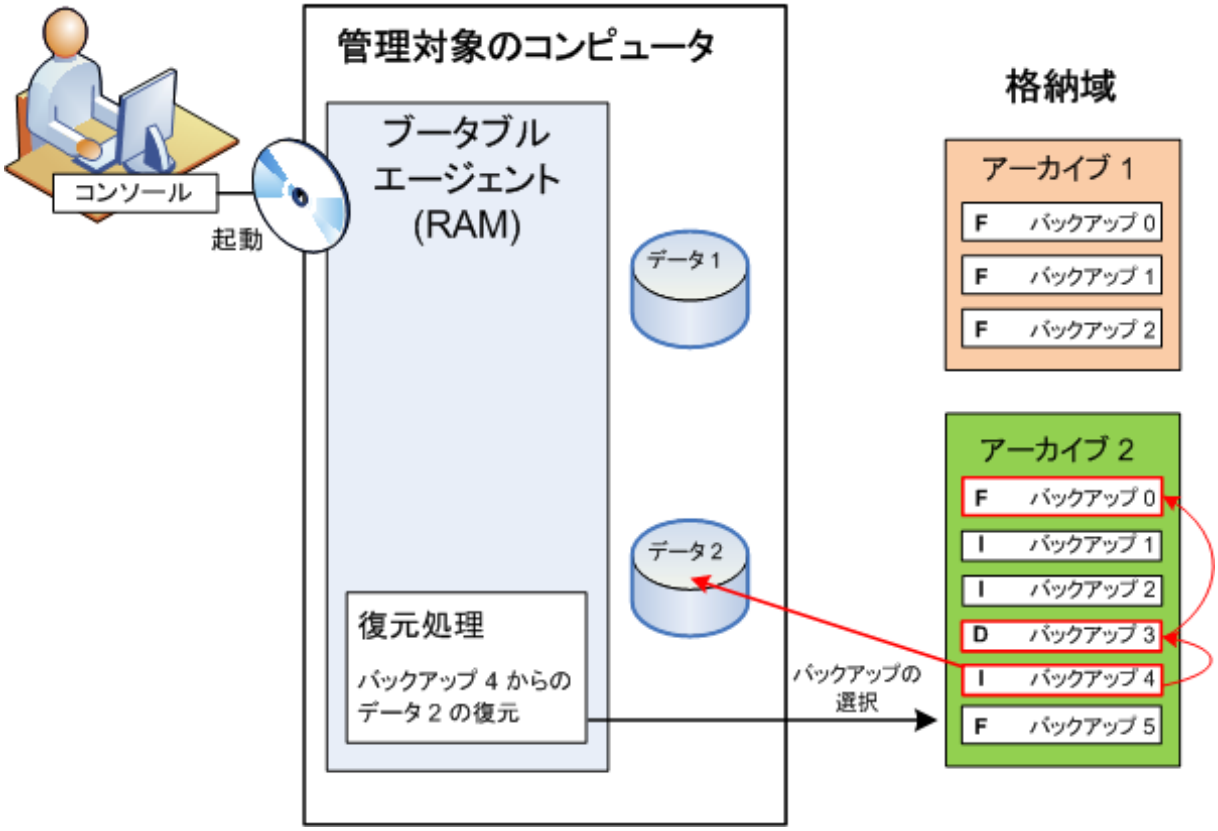
次の図は、オペレーティング システム(オンライン)でのデータ復元を示しています。復元処理が行われている間は、コンピュータでバックアップを行うことはできません。必要な場合は、コンソールを別のコンピュータに接続し、そのコンピュータで復元処理を設定することができます。この機能(リモートの並列復元)は Acronis Backup & Recovery 10 で初めて導入されたもので、以前の Acronis 製品には備わっていません。



ブータブル メディアを使用した復元

オペレーティング システムが配置されているボリュームなど、オペレーティング システムによってロックされたボリュームを復元するには、エージェントの一部であるブータブル環境を再起動する必要があります。復元が完了すると、復元されたオペレーティング システムが自動的にオンラインになります。

コンピュータの起動に失敗した場合や、ベア メタル状態のディスクにデータを復元する必要がある場合は、ブータブル メディアを使用してコンピュータを起動し、復元タスクと同じ方法で復元処理を設定します。次の図は、ブータブル メディアを使用した復元を示しています。



2.2. 管理対象のコンピュータ上のユーザー権限

Windows

Windows を実行しているコンピュータを管理する場合、ユーザーの管理権限の範囲はそのコンピュータ上のユーザー権限によって異なります。

一般ユーザー

Users グループのメンバなどの一般ユーザーには、以下の管理権限があります。

- アクセス許可を持っているファイルに対してファイル レベルのバックアップおよび復元を実行する。ただし、ファイル レベル バックアップのスナップショットは使用できない。
- バックアップの計画およびタスクを作成し、管理する。
- 他のユーザーが作成したバックアップの計画およびタスクを表示する(管理することはできない)。
- ローカルのイベント ログを表示する。

管理者ユーザー

Administrators または Backup Operators グループのメンバなど、コンピュータの管理者権限を持っているユーザーには、さらに以下の管理権限があります。

- コンピュータ全体またはコンピュータ上の任意のデータを、ディスク スナップショットを使用して、または使用せずに、バックアップおよび復元する。

Administrators グループのメンバは、さらに以下の操作も実行できます。

- コンピュータ上の任意のユーザーが所有しているバックアップの計画およびタスクの表示と管理を行う。

Linux

Linux を実行しているコンピュータを管理する場合、ユーザーはルート権限を保有または取得しているはずなので、以下を実行できます。

- 任意のデータまたはコンピュータ全体をバックアップまたは復元する。この際、コンピュータ上で、Acronis Backup & Recovery 10 エージェントのすべての操作とログ ファイルを完全に制御できます。
- オペレーティング システムに登録された任意のユーザーの所有するバックアップの計画およびタスクを管理する。

日常的にルートとしてシステムにログオンするのを避けるために、ルート ユーザーは一般ユーザーの資格でログオンしてから、必要に応じてユーザーの種類を切り替えることができます。

2.3. 所有者とログイン情報

ここでは、「所有者」の概念と、バックアップ計画(タスク)のログイン情報の意味について説明します。

計画(タスク)の所有者

ローカルのバックアップ計画の所有者は、その計画を作成したユーザーまたは最後に変更したユーザーです。

集中管理用バックアップ計画の所有者は、その計画の生成元である集中管理ポリシーを作成、または最後に変更した管理サーバーの管理者です。

バックアップ計画に属するタスクは、ローカル タスクか集中管理タスクかを問わず、バックアップ計画の所有者によって所有されます。

復元タスクなど、バックアップ計画に属さないタスクは、そのタスクを作成したユーザーまたは最後に変更したユーザーによって所有されます。

別のユーザーが所有する計画(タスク)の管理

コンピュータで管理者権限を持っているユーザーは、オペレーティング システムに登録されている任意のユーザーが所有するタスクおよびローカルのバックアップ計画を変更できます。

別のユーザーが所有する計画またはタスクを編集のために開くと、そのタスクに設定されていたすべてのパスワードが消去されます。これにより、「設定を変更して、パスワードはそのまま残す」トリックが防止されます。別のユーザーによって変更された計画(タスク)を編集しようとするたびに、警告が表示されます。警告が表示されたときには、次の 2 つの選択肢があります。

- **［キャンセル］**をクリックし、独自の計画またはタスクを作成します。元のタスクはそのまま残されます。
- 編集を続けます。その計画またはタスクの実行に必要なすべてのログイン情報を入力する必要があります。

アーカイブの所有者

アーカイブの所有者は、そのアーカイブを保存場所に保存したユーザーです。より正確に言うと、これは、バックアップ計画を作成したときに**［バックアップの保存先］**の手順でログイン情報にアカウントが指定されたユーザーです。デフォルトでは、計画のログイン情報が使用されます。

計画のログイン情報とタスクのログイン情報

コンピュータで実行されるタスクはすべて、ユーザーの代わりに実行されます。計画またはタスクを作成するときには、計画またはタスクの実行に使用するアカウントを明示的に指定するオプションを使用できます。このオプションを使用するかどうかは、計画またはタスクを手動で開始するか、スケジュールに従って実行するかによって異なります。

手動による開始

［計画(タスク)のログイン情報］の手順はスキップできます。タスクを開始するたびに、現在のログオンで使用したログイン情報を使ってタスクが実行されます。コンピュータで管理者権限を持っているすべてのユーザーも、タスクを開始できます。タスクはそのユーザーのログイン情報を使って実行されます。

タスクのログイン情報を明示的に指定した場合、そのタスクは、どのユーザーが実際にタスクを開始したかにかかわらず、常に同じログイン情報を使用して実行されます。タスクを明示的に指定するには、計画(タスク)の作成ページで、次の操作を行います。

1. **［詳細ビュー］**チェックボックスをオンにします。
2. **［全般］→［計画(タスク)のログイン情報］→［変更］**を選択します。
3. 計画（タスク）の実行に使用するログイン情報を入力します。

スケジュールされた開始または延期された開始

計画（タスク）のログイン情報は必須です。ログイン情報の手順をスキップした場合は、計画（タスク）の作成終了後にログイン情報の入力を求められます。

ログイン情報を指定する必要がある理由

スケジュールされたタスクまたは延期されたタスクは、任意のユーザーまたはタスクの所有者以外のユーザーがログオンしている、ログオンしていないにかかわらず(Windows の［ようこそ］画面が表示された状態になっている場合など)、実行される必要があります。これには、スケジュールされたタスクの開始時刻にコンピュータの電源がオンになっていれば(つまり、スタンバイや休止状態ではなければ)十分です。Acronis スケジューラでタスクを開始するのに、明示的に指定されたログイン情報が必要であるのはこのためです。

2.4. 完全バックアップ、増分バックアップ、差分バックアップ

Acronis Backup & Recovery 10 には、GFS(Grandfather-Father-Son)やハノイの塔などのよく使われるバックアップ スキームを使用する機能が用意されています。また、カスタムのバックアップ スキームを作成することもできます。すべてのバックアップ スキームは、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方法に基づいています。「スキーム」という用語は、実際には、これらのバックアップ方法を適用するアルゴリズムとアーカイブのクリーンアップを行うアルゴリズムを示しています。

これらのバックアップ方法は 1 つのバックアップ スキームの中でチームとして機能するため、それぞれの方法を相互に比較してもあまり意味がありません。これらのバックアップ方法は、それぞれの長所に応じて特定の役割を果たします。すべてのバックアップ方法の長所を生かし、すべてのバックアップ方法の短所の影響を軽減することにより、優れたバックアップ スキームとなります。たとえば、週単位の差分バックアップでは、そのバックアップに依存する日単位の増分バックアップの 1 週間分のセットと共にアーカイブを簡単に削除できるため、アーカイブのクリーンアップが容易になります。

完全バックアップ、増分バックアップ、または差分バックアップの方法でバックアップを行うと、それぞれに応じた種類のバックアップ『ページ参照 420』が作成されます。

完全バックアップ

完全バックアップでは、バックアップ対象に選択されたすべてのデータが保存されます。完全バックアップはすべてのアーカイブの基礎となり、増分バックアップと差分バックアップのベースを形成します。1 つのアーカイブに複数の完全バックアップが含まれる場合も、アーカイブが完全バックアップだけで構成される場合もあります。1 つの完全バックアップはそれ自体で完結しているので、完全バックアップからデータを復元するために、それ以外のバックアップにアクセスする必要はありません。

一般的に、完全バックアップは作成時間が最も長く、復元時間が最も短いバックアップ方法であるとみなされています。Acronis テクノロジでは、増分バックアップからの復元が完全バックアップからの復元と同じくらい高速な場合もあります。

完全バックアップが最適なのは次の場合です。

- システムを最初の状態に戻す必要がある場合
- この最初の状態が頻繁に変更されることはなく、定期的なバックアップが必要ない場合

例: インターネット カフェや学校の教室では、利用者や学生が加えた変更を管理者が元に戻すことが多く、ベースとなるバックアップを更新することがほとんどありません(インストール後はソフトウェアの更新のみが行われます)。この場合、バックアップに要する時間は重要ではなく、完全バックアップからシステムを復元するため復元時間は最短となります。信頼性向上のために、管理者が完全バックアップのコピーを複数用意することもできます。

増分バックアップ

増分バックアップは、**前回のバックアップ**に対するデータの変更点を保存します。増分バックアップからデータを復元するには、同じアーカイブの他のバックアップにアクセスする必要があります。

増分バックアップが最適なのは次の場合です。

- 保存した複数の状態のいずれかに戻せるようにする必要がある場合
- データの合計サイズと比べて、データの変更量が少ない傾向にある場合

一般的に、増分バックアップは完全バックアップより信頼性が低いとみなされています。これは、「チェーン」内の 1 つのバックアップが破損した場合、それ以降のバックアップが使用できなくなるためです。ただし、データの以前のバージョンを複数保存する必要がある場合、完全バックアップを複数保存する方法は選択肢にはなりません。これは、アーカイブが大きすぎることで信頼性の問題が大きくなるためです。

例: データベースのトランザクション ログのバックアップ。

差分バックアップ

差分バックアップは、**前回の完全バックアップ**に対するデータの変更点を保存します。差分バックアップからデータを復元するには、対応する完全バックアップにアクセスする必要があります。差分バックアップが最適なのは次の場合です。

- 最新のデータの状態だけを保存できればよい場合
- データの合計サイズと比べて、データの変更量が少ない傾向にある場合

一般的には、差分バックアップは作成時間が長くて復元時間が短く、増分バックアップは作成時間が短くて復元時間が長いと見なされています。実際には、同じ時点で同じ完全バックアップに追加された増分バックアップと差分バックアップに物理的な違いはありません。前述の違いは、複数の増分バックアップの作成後に(または作成する代わりに)差分バックアップを作成することを意味します。

ディスクの最適化後に作成された増分バックアップや差分バックアップのサイズが、通常より大幅に大きくなることがあります。これは、最適化によってディスク上のファイルの位置が変更され、バックアップにそれらの変更が反映されるためです。ディスクの最適化後に、完全バックアップを再作成することをお勧めします。

次の表は、一般的知識に基づいた、各バックアップ種類の長所と短所を示しています。実際には、これらのパラメータは、データ変更の量、速度、パターンのほか、データの性質、デバイスの物理的な仕様、設定したバックアップ/復元オプションなどの多くの要因に左右されます。最適なバックアップ スキームを選択するうえで最も参考になるのは実践結果です。

パラメータ	完全バックアップ	差分バックアップ	増分バックアップ
ストレージ領域	最大	中程度	最小
作成時間	最大	中程度	最小
復元時間	最小	中程度	最大

2.5. GFS バックアップ スキーム

ここでは、Acronis Backup & Recovery 10 における GFS(Grandfather-Father-Son)バックアップ スキームの実装について説明します。

このバックアップ スキームでは、1 日に 2 回以上のバックアップを行うことはできません。このスキームでは、日単位のバックアップ スケジュールで、日単位、週単位、および月単位の周期を指定し、日単位、週単位、および月単位のバックアップの保持期間を設定できます。日単位のバックアップは「Son」と呼ばれ、週単位のバックアップは「Father」、最も長期の月単位のバックアップは「Grandfather」と呼ばれます。

テープ ローテーション スキームとしての GFS

GFS は当初、テープ ローテーション スキームとして作成され、多くの場合そのように呼ばれていました。テープ ローテーション スキーム自体により、自動化が実現されるわけではありません。このスキームでは、次のことのみが決定されます。

- 必要とされる単位(復元点間の時間間隔)とロールバック期間での復元を実現するために必要なテープの本数
- 次のバックアップで上書きすべきテープ

テープ ローテーション スキームを使用すると、最小限のカートリッジ数で対応し、使用済みのテープを再利用することができます。GFS テープ ローテーション スキームのバリエーションについては、多数のインターネット リソースで解説されてます。ローカルに接続されたテープ デバイスにバックアップを行う場合は、どのバリエーションを使用してもかまいません。

Acronis による GFS

Acronis Backup & Recovery 10 では、GFS スキームに従ってデータを定期的にバックアップし、作成されたアーカイブをクリーンアップするバックアップ計画を簡単に設定できます。

バックアップ計画は通常どおりに作成します。バックアップ先については、HDD ベースのストレージ デバイスや自動テープ ライブラリなど、自動クリーンアップを実行できる任意のストレージ デバイスを選択します (クリーンアップ後にテープ上で解放される領域は、テープ全体が空きになるまで再使用できないため、テープ ライブラリで GFS『ページ参照 176』 を使用する場合は、さらにそのことについても考慮してください)。

以降では、GFS バックアップ スキームに特有の設定について説明します。

バックアップ計画の GFS 関連の設定

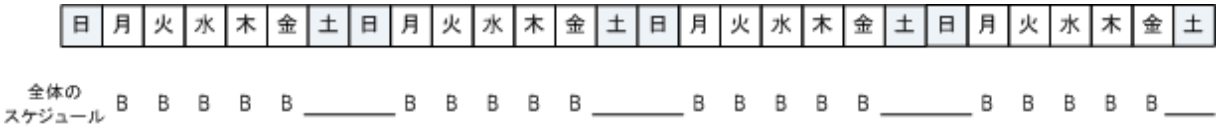
バックアップの開始時刻:

バックアップの実行日:

この手順では、バックアップ スケジュール全体を作成します。つまり、バックアップする必要のあるすべての日付を定義します。

平日の午後 8:00 にバックアップすると仮定します。定義した全体のスケジュールは次のようになります。

「B」は「バックアップ」を表します。



全体のスケジュール。
スケジュール: 平日の午後 8:00

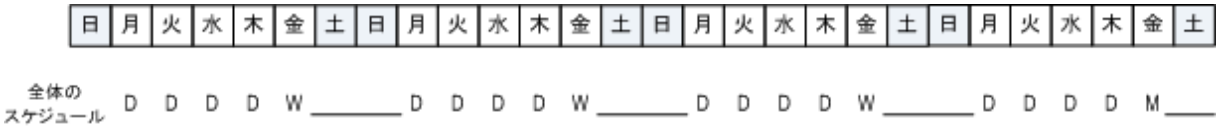
週単位/月単位

この手順では、スケジュールに日単位、週単位、および月単位の周期を設定します。

前の手順で選択した日付から曜日を選択します。この曜日に作成される最初、2 番目、3 番目のバックアップは週単位のバックアップと見なされます。この曜日の 4 番目に作成されるバックアップは月単位のバックアップと見なされます。その他の曜日に作成されるバックアップは日単位のバックアップと見なされます。

[週単位/月単位] のバックアップで金曜日を選択したとします。選択内容に従ってラベルを付けた全体のスケジュールは次のようになります。

「D」は日単位と見なされるバックアップを表します。「W」は週単位と見なされるバックアップを表します。「M」は月単位と見なされるバックアップを表します。

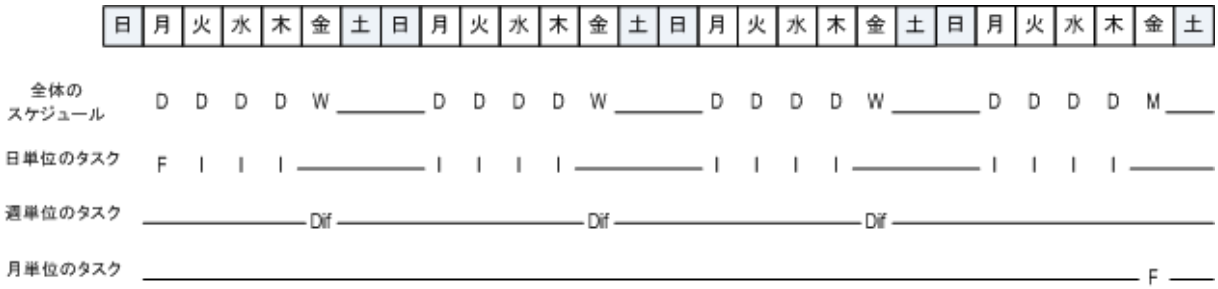


GFS スキームに従ってラベルを付けたスケジュール。
スケジュール: 平日の午後 8:00
週単位/月単位: 金曜日

Acronis では、統合が不要になるように、ストレージ領域の節約とクリーンアップの最適化に役立つ増分および差分のバックアップを使用します。バックアップ方法に関しては、週単位のバックアップは差分(Dif)、月単位のバックアップは完全(F)、日単位のバックアップは増分(I)です。初回のバックアップは常に完全バックアップです。

[週単位/月単位] パラメータにより、全体のスケジュールが日単位、週単位、および月単位のスケジュールに分割されます。

[週単位/月単位] のバックアップで金曜日を選択したとします。作成されるバックアップ タスクの実際のスケジュールは次のようになります。



GFS スキームに従って Acronis Backup & Recovery 10 により作成されるバックアップ タスク。
スケジュール: 平日の午後 8:00
週単位/月単位: 金曜日

バックアップの保持期間: 日単位

この手順では、日単位のバックアップの保持ルールを定義します。それぞれの日単位のバックアップの後にクリーンアップ タスクが実行され、指定よりも古い日単位のバックアップがすべて削除されます。

バックアップの保持期間: 週単位

この手順では、週単位のバックアップの保持ルールを定義します。それぞれの週単位のバックアップの後にクリーンアップ タスクが実行され、指定よりも古い週単位のバックアップがすべて削除されます。週単位のバックアップの保持期間を、日単位のバックアップの保持期間より短くすることはできません。通常は、数倍長い期間を設定します。

バックアップの保持期間: 月単位

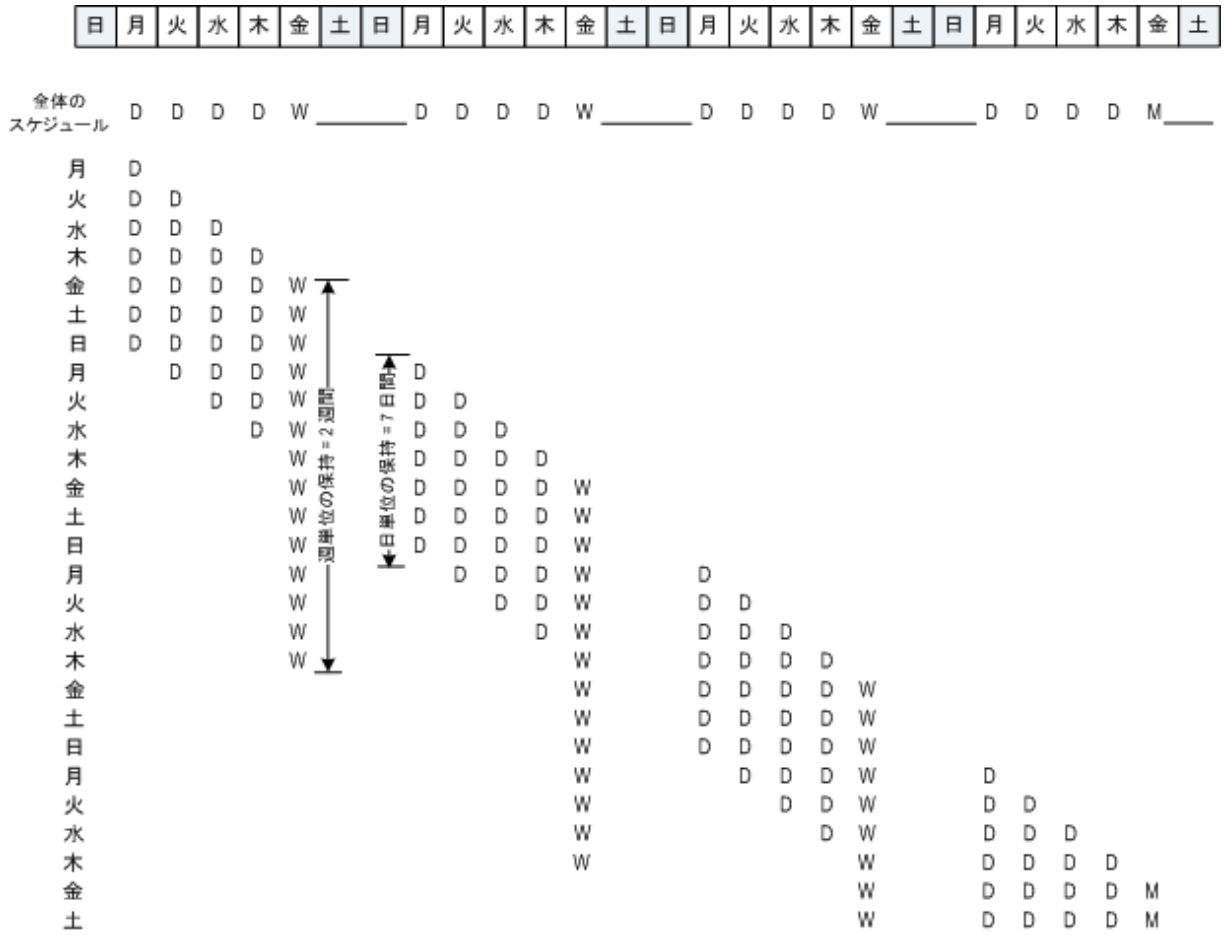
この手順では、月単位のバックアップの保持ルールを定義します。それぞれの月単位のバックアップの後にクリーンアップ タスクが実行され、指定よりも古い月単位のバックアップがすべて削除されます。月単位のバックアップの保持期間を、週単位のバックアップの保持期間より短くすることはできません。通常は、数倍長い期間を設定します。月単位のバックアップの保持期間を無限に設定することもできます。

作成されるアーカイブ: 理想的

日単位のバックアップを 7 日間、週単位のバックアップを 2 週間、月単位のバックアップを 6 か月保持するように選択したとします。すべてのバックアップがいっぱいになったときに、スキームの要求に応じてすぐに削除できる場合、バックアップ計画開始後のアーカイブは次のようになります。

左側の列は曜日を示しています。週の曜日ごとに、通常のバックアップと後続のクリーンアップが行われた後のアーカイブの内容が示されています。

「D」は日単位と見なされるバックアップを表します。「W」は週単位と見なされるバックアップを表します。「M」は月単位と見なされるバックアップを表します。



GFS スキームに従って作成された理想的なアーカイブ。
スケジュール: 平日の午後 8:00
週単位/月単位: 金曜日
日単位のバックアップの保持: 7 日
週単位のバックアップの保持: 2 週
月単位のバックアップの保持: 6 か月

3 週目から、週単位のバックアップが定期的に削除されます。6 か月後、月単位のバックアップの削除が始まります。週単位および月単位のバックアップの図は、尺度が週単位のこの図と同じようになります。

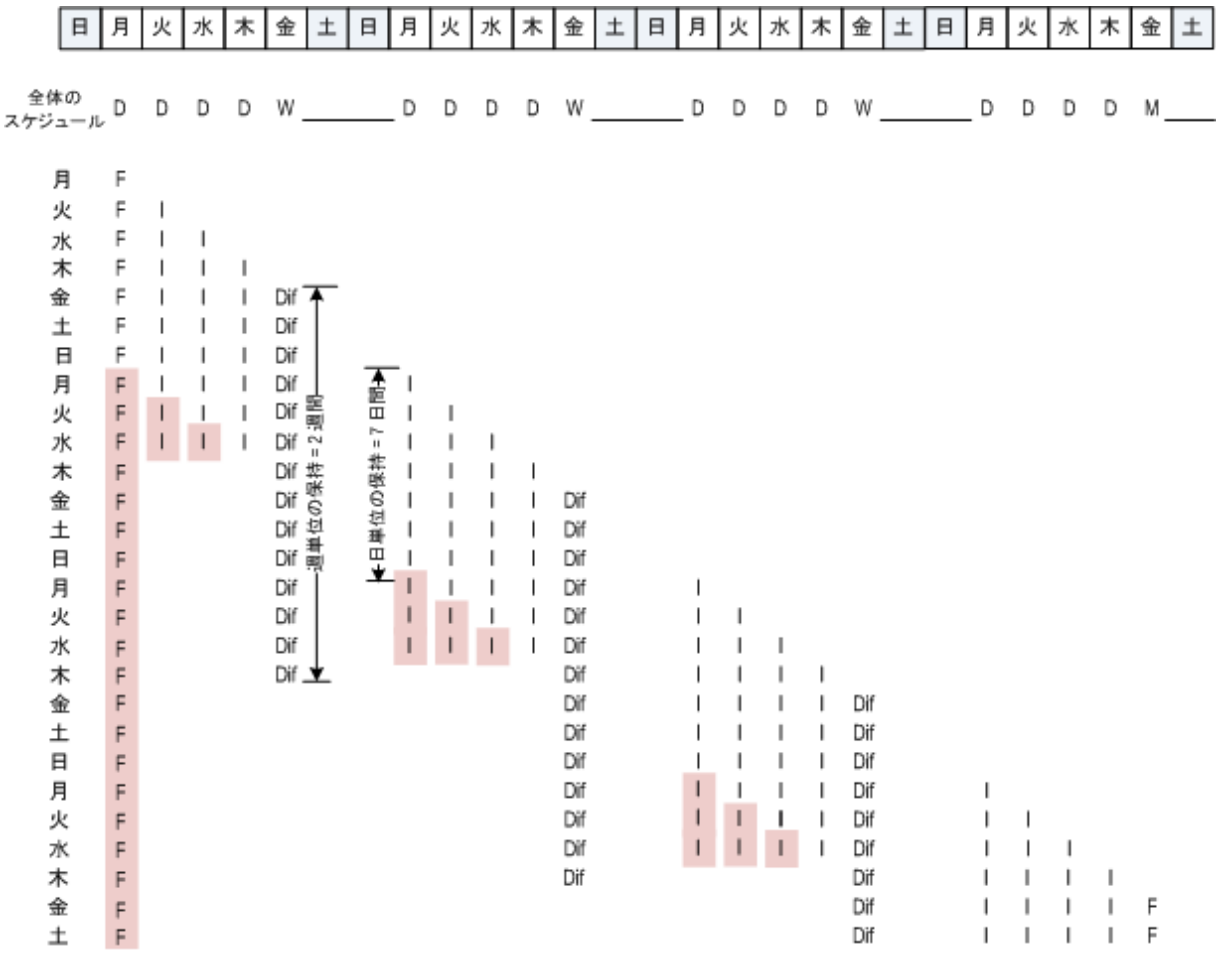
作成されるアーカイブ: 現実

実際には、アーカイブの内容は理想的なスキームによる場合とは多少異なるものになります。

差分および増分のバックアップ方法を使用する場合、あるバックアップに基づいて後続のバックアップが作成されていると、スキームの要求に応じてすぐに削除することができません。通常の統合は、システム リソースを使用しすぎるため利用できません。スキームの要求に従って依存関係のあるすべてのバックアップが削除されてチェーン全体が削除されるまで、プログラムが待機する必要があります。

バックアップ計画の最初の 1 か月は、実際には次のようになります。「F」は完全バックアップを表します。「Dif」は差分バックアップを表します。「I」は増分バックアップを表します。

依存関係のために予定の期間より長く存続するバックアップには、ピンク色のラベルが付けられています。初回の完全バックアップは、そのバックアップに基づく差分バックアップと増分バックアップがすべて削除されるとすぐに削除されます。



GFS スキームに従って Acronis Backup & Recovery 10 により作成されるアーカイブ。
スケジュール: 平日の午後 8:00
週単位/月単位: 金曜日
日単位のバックアップの保持: 7 日
週単位のバックアップの保持: 2 週
月単位のバックアップの保持: 6 か月

2.6. ハノイの塔バックアップ スキーム

頻繁なバックアップが必要な場合は、このようなバックアップを長期間保持するコストが常に問題になります。ハノイの塔(ToH)バックアップ スキームは妥協案として役立ちます。

ハノイの塔の概要

ハノイの塔バックアップ スキームは、同じ名前の数学的なパズルを基にしています。このパズルでは、中央に穴の開いた大きさの異なる複数の円盤と 3 本の杭があり、最初はすべての円盤が 1 番目の杭に大きいものが下になるようにサイズ順に積み重ねられています。すべての円盤を 3 番目の杭に移動したら完成です。一度に移動できる円盤は 1 つだけで、小さい円盤の上に大きい円盤を乗せることはできません。この解き方として、最初の円盤を他の円盤の移動ごと(1、3、5、7、9、11...回)、2 番目の円盤を 4 回間隔(2、6、10...回)、3 番目の円盤を 8 回間隔(4、12...回に移動)のように移動します。

たとえば、A、B、C、D、E というラベル付きの 5 つの円盤がある場合、この解き方では次の順序で円盤を移動します。

円盤＼移動	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
1	A		A		A		A		A		A		A		A		A		A		A		A		A		A		A		A
2		B				B				B				B				B				B				B				B	
3				C								C								C							C				
4								D																D							
5																E															

ハノイの塔バックアップ スキームはこれと同じパターンに基づいています。**移動**の代わりに**セッション**、**円盤**の代わりに**バックアップ レベル**によって処理します。一般に、N レベルのスキームのパターンには、2 の N 乗のセッションが含まれます。

このため、5 レベルのハノイの塔バックアップ スキームは、16 セッション(上の図の 1 から 16 までの移動)で構成されるパターンを繰り返します。

次の表は、5 レベルのバックアップ スキームのパターンを示しています。パターンは 16 セッションから構成されます。

バックアップ レベル＼セッション	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
1	A		A		A		A		A		A		A		A	
2		B				B				B				B		
3				C								C				
4								D								
5																E

ハノイの塔バックアップ スキームでは、レベルごとに 1 つだけバックアップを保持することになります。古いバックアップはすべて削除する必要があります。したがって、このスキームではデータ ストレージの効率が上がり、現時点に向けてバックアップが蓄積されます。4 つのバックアップがあれば、今日、昨日、3.5 日前、または 1 週間前のデータを復元できます。5 レベルのスキームでは、2 週間前にバックアップされたデータも復元できます。このように、バックアップ レベルを増やすたびに、データの最長復元期間が倍になります。

Acronis によるハノイの塔

ハノイの塔バックアップ スキームは一般に複雑すぎて、次に使用するメディアを頭で計算できません。しかし、Acronis Backup & Recovery 10 を使用すると、このバックアップ スキームの使用を自動化できます。バックアップ スキームは、バックアップ計画の作成時に設定できます。

このスキーム用の Acronis の実装には、次のような特徴があります。

- 最大 16 のバックアップ レベル
- 最初のレベル(A)での増分バックアップ - 最も頻度の高いバックアップ処理では時間とストレージを節約できますが、このようなバックアップからのデータの復元は、通常 3 つのバックアップにアクセスする必要があるので時間がかかります。
- 最後のレベル(5 レベル パターンでは E)での完全バックアップ - このスキームにおける最も頻度の低いバックアップで、時間がかかり、使用するストレージ領域も大きくなります。
- すべての中間レベル(5 レベル パターンでは B、C、D)での差分バックアップ。
- 一番最初のセッションでのバックアップは前の完全バックアップなしでは存在しない増分バックアップなので、完全バックアップがセッションでの増分バックアップの代わりに作成されます。
- このスキームでは、すべてのバックアップ レベルで最新のバックアップのみを保持し、そのレベルの他のバックアップを削除する必要があります。ただし、バックアップが別の増分バックアップまたは差分バックアップのベースになっているときは、バックアップの削除は延期されます。
- あるレベルでの古いバックアップは、そのレベルで新しいバックアップが正常に作成されるまで保持されます。

次の表は、5 レベルのバックアップ スキームのパターンを示しています。パターンは 16 セッションから構成されます。

バックアップ レベル \ セッション	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
1 (増分)		A		A		A		A		A		A		A		A
2 (差分)			B				B				B				B	
3 (差分)					C								C			
4 (差分)									D							
5 (完全)	E															

増分バックアップと差分バックアップを使用した結果、古いバックアップが他のバックアップのベースとなっていることによって、その削除が延期される状況が発生します。次の表は、セッション 9 で作成された差分バックアップ(D)がまだ存在しているために、セッション 1 で作成された完全バックアップ(E)の削除が、セッション 17 でセッション 25 まで延期される状況を示しています。この表で、バックアップが削除されたセルはすべて灰色表示になっています。

バックアップ レベル \ セッション	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
1 (増分)		A		A		A		A		A		A		A		A		A		A		A		A	
2 (差分)			B				B				B				B				B				B		
3 (差分)					C								C								C				
4 (差分)									D																D
5 (完全)	E																E								

セッション 9 で作成された差分バックアップ(D)は、新しい差分バックアップの作成が完了した後、セッション 25 で削除されます。このように、ハノイの塔バックアップ スキームに従い、Acronis によって作成されたバックアップ アーカイブには、このスキームの標準的なバックアップの他に最大 2 つの追加バックアップが含まれる場合があります。

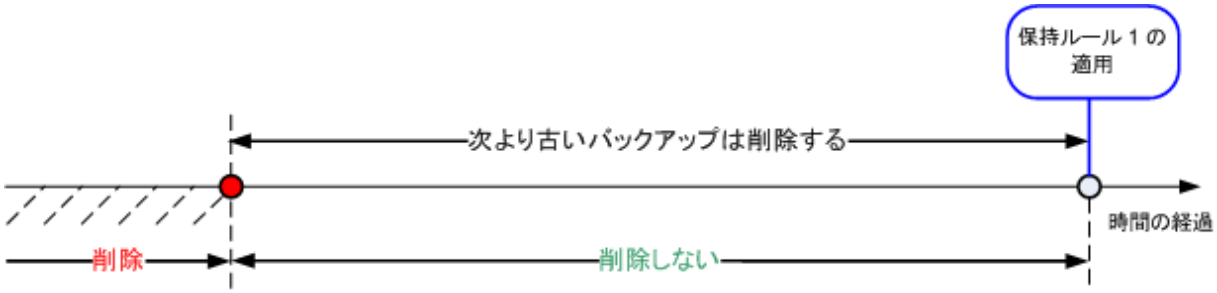
テープ ライブラリにハノイの塔を使用する方法については、「ハノイの塔テープ ローテーション方法の使用『ページ参照 184』」をご参照ください。

2.7. 保持ルール

バックアップ計画によって生成されたバックアップからは、アーカイブが作成されます。ここで説明する 2 つの保持ルールを使用すると、アーカイブのサイズを制限し、バックアップの保持期間を設定できます。

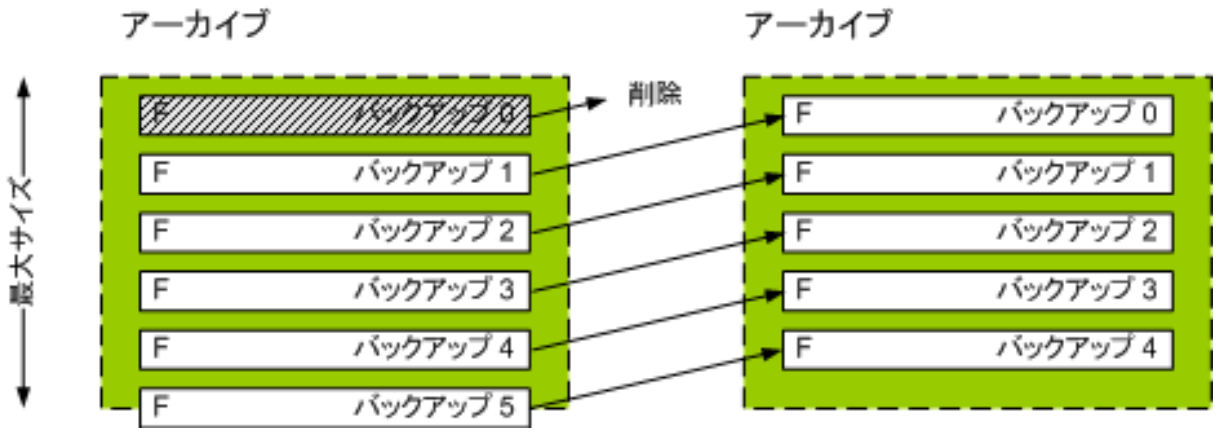
1. 次より古いバックアップは削除する

これは、保持ルールが適用された時点からさかのぼる期間です。保持ルールが適用されるたびに、この期間に対応する過去の日時が計算され、その時点より前に作成されたすべてのバックアップが削除されます。この時点より後に作成されたバックアップは削除されません。

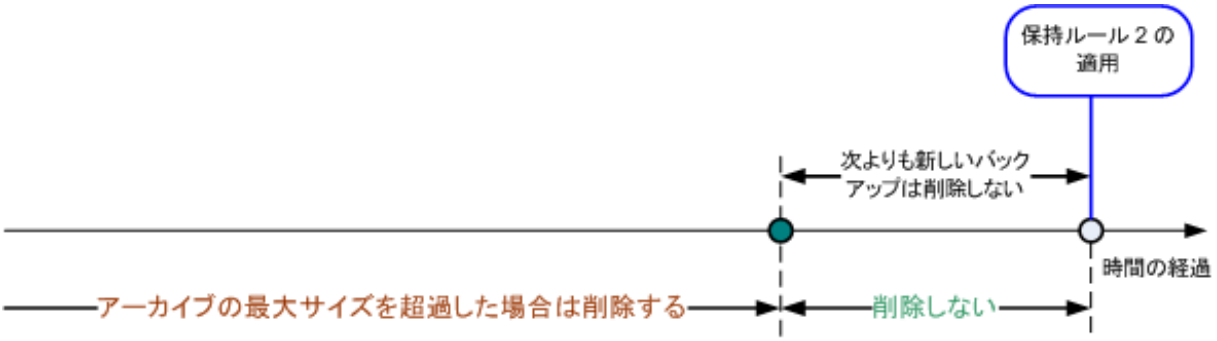


2. アーカイブ サイズを次の範囲内に収める

これはアーカイブの最大サイズです。保持ルールが適用されるたびに、ユーザーが設定した値とアーカイブの実際のサイズが比較され、アーカイブのサイズがその値内に維持されるように、最も古いバックアップが削除されます。下の図は、削除が行われる前後のアーカイブの内容を示しています。

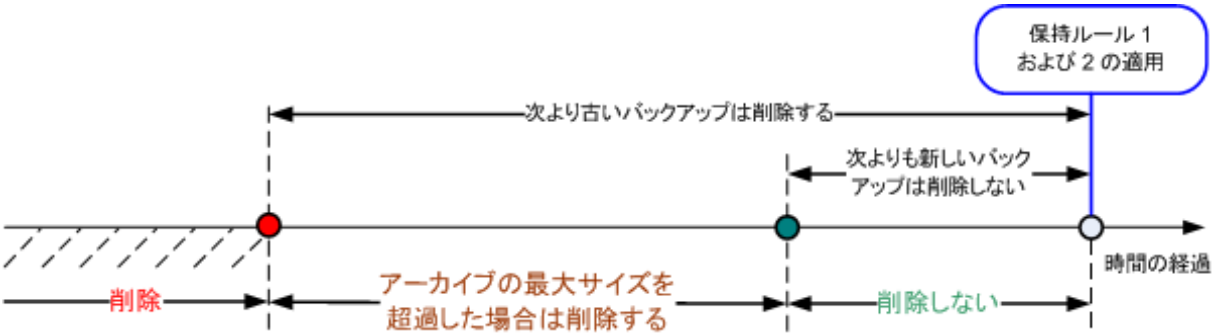


アーカイブの最大サイズが不適切に設定されている(小さすぎる)場合や、通常のバックアップが大きすぎる場合、1 つを除くすべてのバックアップが削除されるおそれもあります。新しいバックアップが削除されないようにするには、**[次よりも新しいバックアップは削除しない]** チェック ボックスをオンにして、バックアップを保持する必要のある最大期間を指定します。次の図は、これらを設定した結果のルールを示しています。



ルール 1 とルール 2 の組み合わせ

バックアップの保存期間とアーカイブのサイズの両方を制限できます。次の図は、これらを設定した結果のルールを示しています。



例

［次より古いバックアップは削除する］= 3 か月

［アーカイブ サイズを次の範囲内に収める］= 200GB

［次よりも新しいバックアップは削除しない］= 10 日

- 保持ルールが適用されるたびに、3 か月(正確には 90 日)より前に作成されたすべてのバックアップが削除されます。
- 削除後のアーカイブ サイズが 200GB より大きく、最も古いバックアップが 10 日より古い場合、そのバックアップが削除されます。
- その後、必要に応じて、アーカイブ サイズが事前に設定された制限まで小さくなるか、最も古いバックアップの経過時間が 10 日に達するまで、その次に古いバックアップが削除されます。

依存関係のあるバックアップの削除

どちらの保持ルールも、一部のバックアップが削除され、その他のバックアップが保持されることを想定しています。アーカイブ内に、相互に依存している増分および差分のバックアップや、それらのバックアップの基になった完全バックアップが含まれている場合はどうなるでしょうか。たとえば、古くなった完全バックアップを削除し、その増分の「子」を保持することはできません。

バックアップの削除が他のバックアップに影響を与える場合、次のいずれかのルールが適用されます。

- **依存するすべてのバックアップが削除の対象になるまでバックアップを保持する**

  古くなったバックアップは、それに依存するすべてのバックアップも古くなるまで保持されます。その後、通常のクリーンアップ中に、チェーン全体が一度に削除されます。このモードは、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が追加で必要になります。アーカイブのサイズやバックアップの保存期間が、ユーザーの指定した値を超える場合があります。
- **バックアップを統合する**

  削除対象のバックアップは、依存関係がある次のバックアップと統合されます。たとえば、保持ルールで、完全バックアップを削除しても、次の増分バックアップは保持する必要があるとします。バックアップは 1 つの完全バックアップに結合され、そのバックアップに増分バックアップの日付が付けられます。チェーンの中間から増分または差分のバックアップが削除されると、結果として残されるバックアップの種類は増分になります。

  このモードでは、各クリーンアップの後、アーカイブのサイズとバックアップの保存期間は、ユーザーが指定した範囲内になります。ただし、統合は多くの時間とシステム リソースを消費する場合があります。また、統合中に作成される一時ファイルのために、格納域に追加の領域も必要です。

統合に関する注意点

統合は削除の 1 つの方法に過ぎず、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。

統合によって作成されるバックアップには、常に最大限の圧縮が適用されます。つまり、統合によって繰り返されるクリーンアップの結果として、アーカイブ内のすべてのバックアップに最大限の圧縮が適用される可能性があります。

運用例

ストレージ デバイスの容量、設定する制限のパラメータ、およびクリーンアップの頻度の間でバランスを取ってください。保持ルールのロジックは、ストレージ デバイスの容量が、平均的なバックアップのサイズよりずっと大きく、アーカイブの最大サイズがストレージの物理容量には近づかず、適正な予備領域が残されることを前提としています。このため、クリーンアップ タスクを実行する間の期間に発生する可能性のあるアーカイブ サイズの超過は、ビジネス プロセスにとっては重要ではありません。クリーンアップの実行頻度が少ないほど、指定の期間より長く存続するバックアップの保存に必要な領域が増加します。

［格納域］『ページ参照 153』ページには、各格納域で使用できる空き領域に関する情報が表示されます。ときどきこのページを確認するようにしてください。空き領域(実際にはストレージ デバイスの空き領域)が 0 に近づく場合は、その格納域にある一部またはすべてのアーカイブに対する制限を厳しくすることが必要になる場合があります。

2.8. ダイナミック ボリュームのバックアップ(Windows)

ここでは、Acronis Backup & Recovery 10 を使用して、ダイナミック ボリューム『ページ参照 418』のバックアップと復元を行う方法について簡単に説明します。GUID パーティション テーブル(GPT)を使用するベーシック ディスクについても説明します。

ダイナミック ボリュームとは、ダイナミック ディスク『ページ参照 417』、より正確にはディスク グループ『ページ参照 419』に配置されたボリュームです。Acronis Backup & Recovery 10 では、次のダイナミック ボリュームの種類や RAID レベルがサポートされています。

- シンプル/スパン
- ストライプ(RAID 0)
- ミラー(RAID 1)
- ミラー化ストライプ(RAID 0+1)
- RAID 5

Acronis Backup & Recovery 10 では、ダイナミック ボリュームと、少し制限がありますがベーシック GPT ボリュームのバックアップと復元を行うことができます。

ダイナミック ボリュームのバックアップ

ダイナミック ボリュームとベーシック GPT ボリュームは、ベーシック MBR ボリュームと同じ方法でバックアップされます。GUI からバックアップ計画を作成するときは、すべての種類のボリュームを［**バックアップする項目**］として選択できます。コマンド ラインを使用するときは、DYN プレフィックスを付けてダイナミック ボリュームや GPT ボリュームを指定します。

コマンド ラインの例

```
trueimagecmd /create /partition:DYN1,DYN2 /asz
```

このコマンドは、DYN1 ボリュームと DYN2 ボリュームを Acronis セキュア ゾーンにバックアップします。

```
trueimagecmd /create /harddisk:DYN /asz
```

このコマンドは、システム内のすべてのダイナミック ボリュームを Acronis セキュア ゾーンにバックアップします。

ベーシック GPT ボリュームのブート コードのバックアップまたは復元は行われません。

ダイナミック ボリュームの復元

ダイナミック ボリュームは次の場所に復元できます。

- 任意の種類の既存ボリューム
- ディスク グループの未割り当て領域
- ベーシック ディスクの未割り当て領域

既存のボリュームへの復元

ダイナミック ボリュームを既存のボリュームに復元すると、復元先のボリューム(ベーシックまたはダイナミック)のデータはバックアップの内容で上書きされます。復元先のボリュームの種類(ベーシック、シンプル/スパン、ストライプ、ミラー、RAID 0+1、RAID 5)は変更されません。復元先のボリュームは、バックアップの内容を収容できる十分なサイズを持っている必要があります。

ディスク グループの未割り当て領域への復元

ダイナミック ボリュームをディスク グループの未割り当て領域に復元すると、復元元のボリュームの種類と内容の両方が復元されます。未割り当て領域は、バックアップの内容を収容する十分なサイズを持っている必要があります。未割り当て領域をディスク間に分散する方法も重要です。

例

ストライプ ボリュームでは、各ディスク上で均等な領域を消費します。

30GB のストライプ ボリュームを、2 つのディスクから構成されるディスク グループに復元するとします。各ディスクには、いくつかのボリュームと一定量の未割り当て領域があります。未割り当て領域の合計サイズは 40GB です。未割り当て領域がディスク間に均等(20GB と 20GB)に分散しているときは、復元の結果は必ずストライプ ボリュームになります。

ディスクの 1 つに 10GB、もう 1 つに 30GB の未割り当て領域があるときは、復元の結果は復元されるデータのサイズによって異なります。

- データのサイズが 20GB 未満のときは、1 つのディスクで 10GB 保持できるので、もう 1 つで残りの 10GB を保持します。このように、両方のディスクにストライプ ボリュームが作成され、2 番目のディスクの 20GB は未割り当てのままになります。

- データのサイズが 20GB を超えるときは、データは 2 つのディスクに均等に分散できませんが、1 つのシンプル ボリュームに収容できます。そこで、すべてのデータを収容するシンプル ボリュームが 2 番目のディスクに作成されます。最初のディスクはそのままになります。

	バックアップ元(ソース):		
復元先:	**ダイナミック ボリューム**	**ベーシック MBR ボリューム**	**ベーシック GPT ボリューム**
ダイナミック ボリューム	ダイナミック ボリューム ターゲットと同じ種類	ダイナミック ボリューム ターゲットと同じ種類	ダイナミック ボリューム ターゲットと同じ種類
未割り当て領域(ディスク グループ)	ダイナミック ボリューム ソースと同じ種類	ダイナミック ボリューム シンプル	なし
ベーシック MBR ボリューム	ベーシック MBR ボリューム	ベーシック MBR ボリューム	ベーシック MBR ボリューム
ベーシック GPT ボリューム	ベーシック GPT ボリューム	ベーシック GPT ボリューム	ベーシック GPT ボリューム
未割り当て領域(ベーシック MBR ディスク)	ベーシック MBR ボリューム	ベーシック MBR ボリューム	ベーシック MBR ボリューム
未割り当て領域(ベーシック GPT ディスク)	ベーシック GPT ボリューム	ベーシック GPT ボリューム	ベーシック GPT ボリューム

復元時のボリュームの移動とサイズ変更

復元結果のベーシック ボリューム(MBR と GPT)は、復元時にサイズを変更したり、ディスク上のボリュームの場所を変更したりすることができます。復元結果のダイナミック ボリュームは、移動やサイズ変更を行うことができません。

ディスク グループとボリュームの準備

ダイナミック ボリュームをベア メタル状態のディスクに復元するには、復元先のハードウェア上にディスク グループを作成しておく必要があります。

状況によっては、既存のディスク グループに未割り当て領域を作成するか、増やす必要もあります。これを実行するには、ボリュームを削除するか、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。

復元先のボリュームの種類(ベーシック、シンプル/スパン、ストライプ、ミラー、RAID 0+1、RAID 5)の変更が必要になる場合があります。変更するには、ターゲット ボリュームを削除し、未割り当てになった領域に新しいボリュームを作成します。

Acronis Backup & Recovery 10 に含まれる便利なディスク管理ユーティリティを使用すると、前述の処理をオペレーティング システムおよびベア メタル状態のディスクの両方で実行できます。Acronis Disk Director Lite の詳細については、「ディスクの管理『ページ参照 316』」をご参照ください。

2.9. LVM ボリュームのバックアップ(Linux)

ここでは、Linux LVM(Logical Volume Manager) によって管理されるボリューム(論理ボリュームと呼ばれます) を、Acronis Backup & Recovery 10 を使用してバックアップおよび復元する方法について簡単に説明します。

Linux with 2.6.x カーネルまたは Linux ベースのブータブル メディアで Acronis Backup & Recovery 10 エージェント for Linux を実行すると、このようなボリュームのアクセス、バックアップ、および復元を行うことができます。

1 つ以上の論理ボリュームのデータをバックアップし、以前に作成した論理ボリュームまたはベーシック(MBR)ディスクやボリュームにそのデータを復元できます。同様に、ベーシック ボリュームから論理ボリュームへのデータの復元も可能です。いずれの場合も、ボリュームの内容のみがバックアップまたは復元されます。復元先ボリュームの種類やその他のプロパティは変更されません。

論理ボリュームのバックアップからベーシック MBR ディスクに復元されたシステムでは、カーネルがルート ファイル システムを論理ボリュームからマウントしようとするので、起動できません。システムを起動するには、LVM を使用しないようにローダー設定と /etc/fstab を変更し、「起動のトラブルシューティング『ページ参照 276』」の説明に従ってブート ローダーを再度有効にします。

論理ボリュームをベーシック MBR ボリュームに復元するときは、復元結果のボリュームのサイズを変更できます。

対応する論理ボリューム構造を持たないターゲット コンピュータ(ベア メタル状態のディスクなど)に論理ボリュームを復元するには、次のいずれかの方法を使用して、論理ボリュームとグループを作成する必要があります。

- ソース コンピュータへの最初のディスクのバックアップを実行する前に、次のコマンドを実行します。

  ```
  trueimagecmd --dumpraidinfo
  ```

  これにより、コンピュータの論理ボリューム構造が **/etc/Acronis** ディレクトリに保存されます。このディレクトリのあるボリュームを、バックアップするボリュームの一覧に含めます。

  復元を実行する前に、ブータブル メディアで **restoreraids.sh** スクリプトを使用して構造を作成します。
- または、**lvm** ユーティリティを使用して手動で構造を作成してから復元を実行することもできます。この手順は、Linux またはブータブル メディアのいずれかで実行できます。

論理ボリュームを復元する方法の詳細については、「MD デバイスと論理ボリュームの復元『ページ参照 309』」をご参照ください。

ボリューム構造がコンピュータ上に既に存在する場合(ボリューム上の一部のデータが失われたが、ハード ディスクを交換していない場合など)、ボリューム構造を作成する必要はありません。

バックアップする論理ボリュームの選択方法

論理ボリュームは、バックアップ可能なボリュームの一覧の最後に表示されます。論理ボリュームに含まれるベーシック ボリュームも、［種類］列が［なし］で一覧に表示されます。バックアップ元としてこのようなパーティションを選択すると、セクタ単位でイメージが作成されます。通常では、セクタ単位のイメージを作成する必要はありません。利用可能なすべてのディスクをバックアップするには、すべての論理ボリュームと、論理ボリュームに属さないベーシック ボリュームを指定します。

論理ボリュームは GPT(GUID パーティション テーブル)パーティションです。論理ボリュームは**［ダイナミック ボリュームと GPT ボリューム］**の下に表示されます。

次のコマンドで取得されるボリュームの一覧の例を示します。

```
trueimagecmd --list
```

GUI にも同様のテーブルが表示されます。

```
Num  Partition             Flags       Start      Size       Type
_____________________________________________________________________
Disk 1:
1-1  hda1 (/boot)         Pri,Act     63         208782     Ext3
1-2  hda2                 Pri         208845     8177085    None
Disk 2:
2-1  hdb1                 Pri,Act     63         8385867    None
Disk 3:
3-1  hdd1                 Pri,Act     63         1219617    Ext3
3-2  Acronis Secure Zone  Pri         1219680    2974608    FAT32

Dynamic & GPT Volumes:
DYN1 VolGroup00-LogVol00                         15269888   Ext3
DYN2 VolGroup00-LogVol01                         1048576    Linux Swap
```

このシステムには 3 つの物理ディスク(Disk 1、Disk 2、Disk 3)があります。2 つの論理ボリューム DYN1 と DYN2 は、ベーシック ボリューム 1-2 と 2-1 にまたがって配置されています。Disk 3 には、通常はバックアップされない Acronis セキュア ゾーンがあります。

論理ボリューム DYN1 をバックアップするには、ボリューム DYN1 を選択します。

3 つのハード ディスクをすべてバックアップするには、ボリューム 1-1、3-1、DYN1、および DYN2 を選択します。

Disk 2、ボリューム 1-2 またはボリューム 2-1 を選択すると、セクタ単位のバックアップが作成されます。

コマンドライン インターフェイスを使用して論理ボリューム DYN1 をバックアップするには、次のコマンドを実行します(バックアップの名前は /home/backup.tib と想定します)。

```
trueimagecmd --partition:dyn1 --filename:/home/backup.tib --create
```

役に立つリンク:

- http://tldp.org/HOWTO/LVM-HOWTO/

2.10. RAID アレイのバックアップ(Linux)

Acronis Backup & Recovery 10 エージェント for Linux では、Linux のソフトウェア RAID デバイス(マルチディスク デバイスまたは MD デバイスと呼ばれます)とハードウェア RAID アレイのバックアップと復元を行うことができます。

ソフトウェア RAID アレイ

ソフトウェア RAID アレイ(MD デバイス) は、複数のボリュームを結合して、まとまったブロック デバイス(/dev/md0、/dev/md1、...、/dev/md31)を作成します。この情報は、/etc/raidtab またはこれらのボリュームの専用の領域に保存されます。

バックアップ

アクティブな(マウントされた)ソフトウェア アレイは、論理ボリュームと同じ方法でバックアップできます。アレイは、バックアップ可能なボリュームの一覧の最後に表示されます。

ソフトウェア アレイに含まれるベーシック ボリュームは、そのファイル システムが破損しているか、またはファイル システムがないボリュームとして表示されます。このようなボリュームは復元できないので、ソフトウェア アレイがマウントされているときにボリュームをバックアップする意味はありません。

例

--list コマンドで取得されるボリュームの一覧の例を示します。GUI にも同様のテーブルが表示されます。

このシステムでは、2 つのベーシック ボリューム sdc1 と sdd1 上に RAID-1 が構成されています。

```
Num  Partition            Flags       Start      Size       Type
---- -------------------- ----------- ---------- ---------- -----------
Disk 1:
1-1  sda1                 Pri,Act      63         208782     Ext3
1-2  sda2                 Pri          208845     15550920   ReiserFS
1-3  sda3                 Pri          15759765   1012095    Linux Swap
Disk 2:
    Table                             0                     Table
    Unallocated                       1          16771859   Unallocated
Disk 3:
3-1  sdc1                 Pri          63         16755732   Ext3
    Unallocated                       16755795   16065      Unallocated
Disk 4:
4-1  sdd1                 Pri          63         16755732   None
    Unallocated                       16755795   16065      Unallocated
Disk 5:
    Table                             0                     Table
```

```
    Unallocated                          1          16771859   Unallocated
Dynamic & GPT Volumes:
DYN1 md0                                             33511168   Ext3
                          Disk: 5     0          63
                          Disk:4     0          63
```

RAID アレイは次のようにバックアップできます。

```
trueimagecmd --create --partition:DYN1 --filename:/tmp/raid.tib
--progress:on
```

グラフィック ユーザー インターフェイスで、［**DYN1**］チェックボックスをオンにします。

復元

ソフトウェア RAID アレイのパラメータはバックアップされないので、ベーシック ボリューム、未割り当て領域、または以前に構成済みのアレイにのみ復元できます。復元は Linux または Linux ベースのブータブル メディアで実行できます。

ブータブル メディアから起動すると、ブータブル エージェントはソフトウェア ディスク アレイのパラメータにアクセスして構成しようとします。ただし、必要な情報が失われている場合は、アレイを自動的に構成することができません。この場合は、**mdadm** などのコマンドを使用してソフトウェア アレイを手動で作成してから、復元処理を再開します。

たとえば、次のコマンドにより、ベーシック ボリューム /dev/sdc1 と /dev/sdd1 に RAID-1 構成の MD デバイス /dev/md0 を作成します。

```
mdadm --create /dev/md0 --level=1 --raid-devices=2 /dev/sd[cd]1
```

Linux およびブータブル メディアでのソフトウェア RAID アレイの復元の詳細については、「MD デバイスの復元(Linux)『ページ参照 279』」および「MD デバイスと論理ボリュームの復元『ページ参照 309』」をご参照ください。

ハードウェア RAID アレイ

Linux のハードウェア RAID アレイでは、複数の物理ドライブを結合して、パーティション操作が可能な 1 つのディスクを作成します。ハードウェア RAID アレイに関連したファイルは、通常 /dev/ataraid にあります。ハードウェア RAID アレイは、一般のハード ディスクと同じ方法でバックアップできます。

ハードウェア RAID アレイの一部である物理ドライブは他のディスクと共に表示されますが、パーティション テーブルが破損しているか、またはパーティション テーブルがないものとして表示されます。このようなディスクをバックアップしても、復元できないので意味がありません。

2.11. テープのサポート

Acronis Backup & Recovery 10 では、ストレージ デバイスとしてテープ ライブラリ、オートローダー、SCSI テープ ドライブ、および USB テープ ドライブがサポートされています。テープ デバイスは、管理対象のコンピュータにローカルに接続するか(この場合は、Acronis Backup & Recovery 10 エージェントによってテープの読み取りと書き込みを行います)、Acronis Backup & Recovery 10 ストレージ ノード『ページ参照 23』経由でアクセスします。ストレージ ノードでは、テープ ライブラリとオートローダー『ページ参照 163』の完全な自動処理が保証されます。

異なるテープ アクセス方法で作成されたバックアップ アーカイブは、形式も異なります。ストレージ ノードによって書き込まれたテープは、エージェントによって読み取ることができません。

Linux ベースまたは PE ベースのブータブル メディアでは、ローカル アクセスおよびストレージ ノード経由のアクセスの両方を使用してバックアップと復元を行うことができます。ブータブル メディアを使用して作成されたバックアップは、オペレーティング システムで実行している Acronis Backup & Recovery 10 エージェントを使用して復元できます。

2.11.1. テープ互換性の表

次の表は、Acronis Backup & Recovery 10 の Acronis True Image Echo と Acronis True Image 9.1 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ついてまとめたものです。Acronis Backup & Recovery 10 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。

			コンピュータ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			
			ABR10 ブータブル メディア	ABR10 エージェント for Windows	ABR10 エージェント for Linux	ABR10 ストレージ ノード
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	ATIE 9.1	+	+	+	+
		ATIE 9.5	+	+	+	+
		ATIE 9.7	+	+	+	+
		ABR10	+	+	+	+
	エージェント for Windows	ATIE 9.1	+	+	+	+
		ATIE 9.5	-	-	-	+
		ATIE 9.7	-	-	-	+
		ABR10	+	+	+	+
	エージェント	ATIE 9.1	+	+	+	+

	for Linux	ATIE 9.5	+	+	+	+
		ATIE 9.7	+	+	+	+
		ABR10	+	+	+	+
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	ATIE 9.1	+	+	+	+
		ATIE 9.5	-	-	-	+
		ATIE 9.7	-	-	-	+
	ストレージ ノード	ABR10	-	-	-	+

2.11.2. 単一のテープ ドライブの使用

管理対象のコンピュータにローカルに接続したテープ ドライブは、ストレージ デバイスとして、ローカルのバックアップ計画で使用できます。ローカル接続のオートローダーまたはテープ ライブラリの機能は、一般のテープ ドライブに制限されます。つまり、プログラムで処理できるのは現在マウントされているテープだけで、テープは手動でマウントする必要があります。

ローカル接続のテープ デバイスへのバックアップ

バックアップ計画を作成するときは、ローカル接続のテープ デバイスをバックアップの保存先として選択できます。テープにバックアップするときは、アーカイブ名は不要です。

アーカイブは複数のテープにまたがってもかまいませんが、完全バックアップは 1 つしか含めることができません。増分バックアップの数は無制限に含めることができます。完全バックアップを作成するたびに、新しいテープで開始し、新しいアーカイブを作成します。テープがいっぱいになると、新しいテープの挿入を求めるダイアログ ウィンドウが表示されます。

空でないテープの内容は、確認後に上書きされます。この確認ダイアログは表示しないようにすることができます。このオプションについては、「その他の設定『ページ参照 139』」をご参照ください。

回避策

複数のアーカイブをテープに保存する場合(たとえば、ボリューム C とボリューム D を別々にバックアップする場合)は、2 番目のボリュームの最初のバックアップを作成するときに、完全バックアップではなく増分バックアップ モードを選択します。その他の状況では、以前に作成したアーカイブに変更を追加するために増分バックアップを使用します。

テープの巻き戻しのためにしばらく待たされることがあります。品質の劣化したテープや古いテープだけでなく、磁気ヘッドの汚れによっても、待ち時間が長くなることがあります。

制限

1. 1 つのアーカイブに複数の完全バックアップを含めることはできません。
2. 個々のファイルはディスク バックアップから復元できません。
3. クリーンアップ時に手動または自動でテープからバックアップを削除することはできません。ローカル接続のテープへのバックアップ時には、自動クリーンアップを使用する保存ルールやバックアップ スキーム(GFS、ハノイの塔)は GUI で無効になっています。
4. テープ ドライブには個人用格納域を作成できません。
5. テープに保存されたバックアップからはオペレーティング システムの存在を検出できないので、Linux ボリュームまたは Windows のシステム以外のボリュームを復元するときでも、すべてのディスクまたはボリュームの復元に Acronis Universal Restore『ページ参照 414』をお勧めします。
6. テープからの復元時には、Acronis Active Restore『ページ参照 413』 は使用できません。

ローカル接続のテープ デバイスからの復元

復元タスクを作成する前に、復元が必要なバックアップが含まれるテープを挿入またはマウントします。復元タスクを作成するときは、使用可能なロケーションの一覧からテープ デバイスを選択してから、バックアップを選択します。復元が開始された後で、復元のためにテープが必要な場合は、他のテープを要求するメッセージが表示されます。

2.12. Acronis 独自のテクノロジ

ここでは、Acronis Backup & Recovery 10 が Acronis True Image Echo および Acronis True Image 9.1 製品ファミリから継承している独自のテクノロジについて説明します。

2.12.1. Acronis セキュア ゾーン

Acronis セキュア ゾーンは、管理対象のコンピュータのディスク領域にバックアップ アーカイブを保存できる安全なパーティションです。このため、同じディスクに保存したバックアップからディスクを復元することができます。

セキュア ゾーンには、Acronis ディスク管理ツールなどの特定の Windows アプリケーションを使用してアクセスできます。

ディスクの物理的な障害が発生すると、そこに配置されたゾーンとアーカイブは失われます。このため、Acronis セキュア ゾーンを唯一のバックアップの保存場所にはしないでください。エンタープライズ環境では、通常の場所が一時的に利用できなかったり、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の場所として Acronis セキュア ゾーンを使用できます。

利点

Acronis セキュア ゾーン:

- 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る。
- ソフトウェアの誤動作、ウィルス攻撃、オペレータによるエラーからデータ保護するためのコスト効率のよい便利な方法を提供する。
- 内部のアーカイブ ストレージなので、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る。このことは、モバイル ユーザーにとって特に便利です。
- 保存先の二重化『ページ参照 134』バックアップの使用時に主要バックアップ先として利用できる。

制限

- セキュア ゾーンは、ダイナミック ディスク上または GPT パーティション スタイルを使用するディスク上に作成することはできません。

Acronis セキュア ゾーンの管理

Acronis セキュア ゾーンは、個人用格納域『ページ参照 425』と見なされます。セキュア ゾーンは、管理対象のコンピュータに作成されると、**［個人用格納域］**の一覧に常に表示されます。集中管理用バックアップ計画『ページ参照 427』では、Acronis セキュア ゾーンとローカルの計画『ページ参照 424』を使用できます。

Acronis セキュア ゾーンを以前に使用したことがある場合は、機能が大幅に変更されていることに注意してください。セキュア ゾーンでは、自動クリーンアップ、つまり、古いアーカイブの削除は実行されなくなりました。自動クリーンアップ付きのバックアップ スキームを使用してセキュア ゾーンにバックアップするか、アーカイブ管理機能を使用して古いバックアップを手動で削除してください。

新しい Acronis セキュア ゾーンの動作では、次の操作を行うことができます。

- セキュア ゾーンに配置されているアーカイブ、および各アーカイブに含まれるバックアップを表示する。
- バックアップの内容を確認する。
- バックアップから物理ディスクにファイルをコピーするために、ディスク バックアップをマウントする。
- アーカイブと、アーカイブに含まれているバックアップを安全に削除する。

Acronis セキュア ゾーンで利用できる処理の詳細については、「個人用格納域『ページ参照 191』」をご参照ください。

Acronis True Image Echo からのアップグレード

Acronis True Image Echo から Acronis Backup & Recovery 10 にアップグレードする場合、Acronis セキュア ゾーンでは Echo で作成されたアーカイブが保持されます。セキュア ゾーンは個人用格納域の一覧に表示され、古いアーカイブを復元に利用できるようになります。

有効になっている Acronis リカバリ マネージャをアップグレードするには、一度無効にしてから再度有効にします。Acronis リカバリ マネージャが有効になっていない場合は、アップグレードするために必要な操作はありません。

2.12.2. Acronis リカバリ マネージャ

ブータブル エージェント『ページ参照 422』の改訂版をシステム ディスクに置き、起動時に［F11］キーを押すと起動するように設定できます。これにより、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ブータブル メディアまたはネットワーク接続が不要になります。この機能の商標名は「Acronis リカバリ マネージャ」です。

Acronis リカバリ マネージャは、モバイル ユーザーにとって特に役に立ちます。障害が発生した場合、ユーザーはコンピュータを再起動し、［Press F11 for Acronis 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の復元を実行します。ユーザーは、移動中に Acronis リカバリ マネージャを使用してバックアップすることもできます。Acronis セキュア ゾーン『ページ参照 58』は、バックアップおよび復元処理で役立ちます。

GRUB ブート ローダーがインストールされているコンピュータでは、［F11］を押す代わりに、ブート メニューから Acronis リカバリ マネージャを選択します。

Acronis リカバリ マネージャの有効化と無効化

Acronis リカバリ マネージャの使用を有効にする操作を「有効化」と呼びます。Acronis セキュア ゾーンを作成する『ページ参照 292』ときは、Acronis リカバリ マネージャを有効にすることをお勧めします。

Acronis セキュア ゾーンを作成すると、**［Acronis セキュア ゾーンの管理］**操作を使用して、いつでも Acronis リカバリ マネージャを有効または無効にすることができます。無効にすると、起動時の［Press F11 for Acronis Startup Recovery Manager...］というメッセージが表示されなくなります(または、該当するエントリが GRUB のブート メニューから削除されます)。つまり、システムが起動できないときは、ブータブル メディアが必要になります。

制限

Acronis リカバリ マネージャ:

- ダイナミック ディスク上または GPT パーティション スタイルを使用するディスク上に作成することはできません。
- 有効化後、LILO や GRUB などのブート ローダーを手動で設定する必要があります。
- 有効化後、サードパーティ製ローダーの再有効化が必要です。

2.12.3. Universal Restore(Acronis Backup & Recovery 10 Universal Restore)

Acronis Backup & Recovery 10 Universal Restore は、異なるハードウェアや仮想コンピュータでの復元と Windows の起動を支援する Acronis 独自のテクノロジです。Universal Restore は、ストレージ コントローラ、マザーボード、チップセットなどのオペレーティング システムの起動にとって重要なデバイスの相違に対応できます。

Acronis Backup & Recovery 10 Universal Restore の目的

システムは、ディスク バックアップ(イメージ)からバックアップ元のシステムまたは同一構成のハードウェアに容易に復元できます。ただし、ハードウェア障害などの状況で、マザーボードを交換したり、バージョンの異なるプロセッサを使用していると、復元されたシステムが起動できないことがあります。システムを新しくてより強力なコンピュータに移行しようとしても、同じように起動できない問題が起きます。新しいハードウェアが、イメージに含まれている最も重要なドライバと互換性がないからです。

Microsoft System Preparation Tool (sysprep) を使用してもこの問題は解決しません。Sysprep でインストールできるドライバはプラグ アンド プレイのデバイス (サウンド カード、ネットワーク アダプタ、ビデオ カードなど) 用のドライバに限られているためです。システムの HAL (Hardware Abstraction Layer)と大容量記憶装置デバイス ドライバに関しては、ソース コンピュータとターゲット コンピュータで同じである必要があります(Microsoft サポート技術情報の文書番号 302577 と 216915 をご参照ください)。

Universal Restore テクノロジは、重要な HAL および大容量記憶装置のドライバを置き換えることによって、ハードウェアに依存しないシステムの復元の効率的なソリューションを提供します。

Universal Restore は次の操作に使用できます。

1. さまざまなハードウェアで障害が発生したシステムの迅速な復元
2. ハードウェアに依存しないオペレーティング システムのクローン作成と配置
3. 物理コンピュータから物理コンピュータ、物理コンピュータから仮想コンピュータ、および仮想コンピュータから物理コンピュータへの移行

Universal Restore の原理

1. HAL および大容量記憶装置のドライバの自動選択

   Universal Restore は、指定したネットワーク フォルダ、リムーバブル メディア、および復元中のシステムのデフォルト ドライバ ストレージ フォルダでドライバを検索します。検出されたすべてのドライバの互換性レベルが分析され、ターゲット ハードウェアに最適な HAL と大容量記憶装置のドライバがインストールされます。ネットワーク アダプタ用のドライバも検索され、オペレーティング システムに渡されます。オペレーティング システムは最初の起動時に、ドライバを自動的にインストールします。

   Windows のデフォルトのドライバ ストレージ フォルダは、レジストリ キー HKEY_LOCAL_MACHINE¥SOFTWARE¥Microsoft¥Windows¥Current version¥DevicePath で指定されています。通常、このストレージ フォルダは WINDOWS/inf です。

2. 大容量記憶装置のドライバの手動選択

   ターゲット ハードウェアに装着されているハードディスク用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）がわかっている場合は、ドライバの検索とインストールを自動的に行う処理を無視して、手動で適切なドライバをインストールすることができます。

3. プラグ アンド プレイ デバイス用のドライバのインストール

   Universal Restore では、組み込みのプラグ アンド プレイの検出および設定処理を利用して、ビデオ、オーディオ、USB など、システム起動時に重要ではないデバイスのハードウェアの違いに対処します。Windows はログオン段階でこの処理を行い、新しいハードウェアの一部が検出されないときは、後で手動でドライバをインストールできます。

Universal Restore と Microsoft Sysprep

Universal Restore はシステムの準備ツールではありません。Universal Restore は、Microsoft System Preparation Tool(Sysprep)で準備したシステムのイメージを含め、Acronis 製品を使用して作成した任意の Windows イメージに適用できます。両方のツールを同じシステムで使用する例を次に示します。

Universal Restore は、復元後、ドメインへの再参加やネットワーク ユーザー プロファイルの再マップを行うことなく直ちにシステムを実行できるよう、セキュリティ識別子(SID)とユーザー プロファイル設定を除去しません。復元されたシステムでこれらの設定を変更する場合には、Sysprep を使用してシステムを準備し、必要に応じて Universal Restore を使用して、システムのイメージ作成と復元を行うことができます。

制限

次の場合は Universal Restore を使用できません。

- Acronis リカバリ マネージャ(［F11］を使用)を使用してコンピュータを起動する場合
- バックアップ イメージが Acronis セキュア ゾーンにある場合
- Acronis Active Restore を使用する場合

これは、これらの機能が主に同じコンピュータ上での簡単なデータ復元を目的としているためです。

Universal Restore は Linux を復元する場合には使用できません。

Universal Restore の入手方法

Universal Restore は、Acronis Backup & Recovery 10 Advanced Server SBS Edition と Acronis Backup & Recovery 10 Advanced Server Virtual Edition に無償で付属しています。

その他の製品用の Universal Restore は別製品として販売されています。これは独立した機能としてセットアップ ファイルからインストールされ、別のライセンスが必要となります。新しくインストールしたアドオンを起動用の環境で機能させるには、ブータブル メディアを再作成する必要があります。

2.12.4. Acronis Active Restore

Active Restore は、システムの復元の開始直後にシステムをオンラインにする Acronis 独自のテクノロジです。

Acronis Recovery for Microsoft Exchange を使い慣れているお客様は、この製品では Active Restore を使用して、復元の開始直後に Exchange インフォメーション ストアを使用できることに注意してください。インフォメーション ストアの復元は同じテクノロジをベースにしていますが、ここで説明するオペレーティング システムの復元とはまったく異なる方法で行われます。

サポートされるオペレーティング システム

Acronis Active Restore は、Windows 2000 以降の Windows を復元するときに使用できます。

制限

サポートされるアーカイブ ロケーションはローカル ドライブだけです。より正確には、コンピュータの BIOS 経由で使用できる任意のデバイスです。これには、Acronis セキュア ゾーン、USB ハード ドライブ、フラッシュ ドライブ、または内蔵ハード ドライブが該当します。

動作

復元処理を設定するときに、復元するディスクまたはボリュームをバックアップから選択します。Acronis Backup & Recovery 10 は、バックアップ内の選択されたディスクまたはボリュームをスキャンします。このスキャンにより、サポートされるオペレーティング システムが検出されると、［Acronis Active Restore］オプションが選択可能になります。

このオプションを有効にしないと、システムの復元は通常の方法で行われ、コンピュータが使用可能になるのは復元の完了後となります。

このオプションを有効にすると、処理手順は次のようになります。

システムの復元が開始されると、オペレーティング システムはバックアップから起動します。コンピュータが使用可能になり、必要なサービスを提供できるようになります。要求された処理に必要なデータが最高の優先度で復元され、それ以外のすべてのデータはバックグラウンドで復元されます。

要求に対する処理が復元と同時に実行されるので、復元オプションで復元の優先度を［**低**］に設定しても、システムの処理速度は低下することがあります。このように、パフォーマンスは一時的に低下しますが、システムの停止時間は最小限に抑えられます。

使用例

1. システムの稼働時間が効率の基準の 1 つであるとき。

   例: クライアント指向のオンライン サービス、Web ショップ、投票所。

2. システム領域とストレージ領域の比率が、大幅にストレージに偏っているとき。

   保存場所として使用されているコンピュータでは、オペレーティング システムの占有するセグメント領域は小さく、他のディスク領域はすべて動画、音声、その他のマルチメディア ファイルなどのストレージ領域として使用されます。このようなストレージの量はシステムと比較して非常に大きく、実質的にすべての復元時間がファイルの復元に費やされ、これらのファイルは復元が完了するまで使用できません。

   Acronis Active Restore を選択すると、システムは短時間で使用可能な状態になります。ユーザーはストレージから必要なファイルを開いて使用しながら、すぐに必要のない残りのファイルはバックグラウンドで復元することができます。

   例: 動画コレクション ストレージ、音楽コレクション ストレージ、マルチメディア ストレージ。

使用方法

1. システム ディスクまたはボリュームをシステムの BIOS からアクセスできる場所にバックアップします。これには、Acronis セキュア ゾーン、USB ハード ドライブ、フラッシュ ドライブ、または内蔵ハード ドライブが該当します。

   オペレーティング システムとローダーが別のボリュームにあるときは、必ず両方のボリュームをバックアップに含めてください。また、ボリュームはまとめて復元する必要があります。そうしないと、オペレーティング システムが起動しなくなる危険性があります。

2. ブータブル メディアを作成します。

3. システムの障害が発生したら、ブータブル メディアを使用してコンピュータを起動します。コンソールを開き、ブータブル エージェントに接続します。

4. システムの復元を次のように設定します。システム ディスクまたはボリュームを選択し、［**Acronis Active Restore を使用する**］チェックボックスをオンにします。

   Acronis Active Restore は、起動と後続の復元のため、バックアップ スキャン時に最初に検出したオペレーティング システムを選択します。結果を予測できるようにしたい場合は、Active Restore を使用して複数のオペレーティング システムを復元しないでください。マルチブート システムを復元するときは、システム ボリュームを一度に 1 つだけ選択してボリュームを起動します。

5. システムの復元が開始されると、オペレーティング システムはバックアップから起動します。システム トレイには Acronis Active Restore のアイコンが表示されます。コンピュータが使用可能になり、必要なサービスを提供できるようになります。ユーザーにはすぐにドライブ ツリーとアイコンが表示され、まだ復元されていない場合でも、ファイルを開いたり、アプリケーションを起動できます。

   Acronis Active Restore ドライバはシステム クエリをインターセプトし、要求された処理に必要なファイルの復元に最高の優先度を設定します。このオンザフライの復元が進む間、継続する復元処理はバックグラウンドに移されます。

［スタート］メニューのコマンドを使用してコンピュータをログオフ、シャットダウン、または休止状態にしようとすると、復元が完了するまで現在のセッションの終了は自動的に延期されます。ただし、電源ボタンを使ってコンピュータをオフにすると、最後の起動以降にシステムに対して行われた変更はすべて失われ、システムは部分的にも復元されません。この状況では、あらためてブータブル メディアから復元処理を開始するのが唯一のソリューションになります。

6. バックグラウンドの復元は、選択したボリュームがすべて復元されるまで続行され、ログ エントリが作成されて、システム トレイから Acronis Active Restore のアイコンが消えます。

2.13. 集中管理について

ここでは、Acronis Backup & Recovery 10 を使用した集中管理データの保護の概要について説明します。このセクションを参照する前に、1 台のコンピュータ上のデータを保護する方法『ページ参照 30』について理解しておくことをお勧めします。

2.13.1. 基本的な概念

バックアップ ポリシーの適用とその実行の追跡

1 台のコンピュータ上のデータを保護するには、保護するさまざまなデータの種類に応じて 1 つまたは複数のエージェント『ページ参照 415』をコンピュータにインストールします。そのコンピュータにコンソールを接続し、1 つまたは複数のバックアップ計画『ページ参照 421』を作成します。

それでは、何百台ものコンピュータを管理する必要があるときはどうでしょうか。たとえば、システム ドライブやユーザーのドキュメントをバックアップする必要があるとき、それぞれのバックアップ計画はよく似ていても、コンピュータごとに計画を作成するのは時間がかかります。また、それぞれのコンピュータで別個に計画の実行を追跡するのも時間がかかります。

複数のコンピュータに対して管理操作を設定するには、Acronis Backup & Recovery 10 管理サーバー『ページ参照 429』をインストールし、サーバーに各コンピュータを登録『ページ参照 429』します。登録した後でコンピュータのグループを作成すると、複数のコンピュータをまとめて管理できるようになります。バックアップ ポリシー『ページ参照 420』と呼ばれる共通のバックアップ計画を設定することにより、すべてのコンピュータまたは選択したコンピュータを保護できます。

コンピュータのグループにポリシーを適用すると、管理サーバーによって各コンピュータにポリシーが配置されます。それぞれのコンピュータ上で、バックアップする項目がエージェントによって検索され、対応する集中管理用計画『ページ参照 427』が作成されます。それぞれのポリシーのステータスを 1 つの画面で監視し、必要に応じてそれぞれのコンピュータ、計画、またはタスクに移動して、そのステータスとログ エントリを確認できます。また、管理サーバーでは、ローカルで実行されるエージェントの活動を監視および管理することもできます。

各コンピュータではなく、管理サーバーにコンソールを接続し、1 か所の管理コンピュータを経由してすべての管理操作を実行するので、この管理方法は集中管理『ページ参照 426』と呼ばれます。

集中管理では、各コンピュータでの直接管理『ページ参照 429』も可能です。各コンピュータのコンソールに接続し、直接管理操作を実行できます。ただし、集中管理用バックアップ計画は、入念に設定されたポリシーが自動的に機能し、人の介入が必要になることはほとんどないので、管理サーバーを経由してのみ管理できます。

管理サーバーを使用すると、1 つまたは複数の集中管理用アーカイブ ストレージ(集中管理用格納域『ページ参照 427』)を作成して、登録したコンピュータで共有することができます。集中管理用格納域は、バックアップ ポリシーのほかに、直接管理を使用して登録済みのコンピュータに作成したバックアップ計画でも使用できます。

管理対象のアーカイブ ストレージの構成

集中管理用格納域にはどの程度の容量が必要か。大きなバックアップを格納域に転送すると、ネットワークが混雑する原因となるか。オンラインで運用サーバーのバックアップを実行すると、サーバーのパフォーマンスに影響を与えるか。集中管理されたバックアップで会社のビジネス プロセスのパフォーマンスが低下しないようにしたり、データ保護に必要なリソースを最小限に抑えるには、Acronis Backup & Recovery 10 ストレージ ノード『ページ参照 416』をインストールし、1 つまたは複数の集中管理用格納域を管理するように構成します。このような格納域は、管理対象の格納域『ページ参照 426』と呼ばれます。

エージェントは、ストレージ ノードを使用して、管理対象の格納域に転送する前にバックアップを重複除外『ページ参照 429』したり、既に格納域に保存されているバックアップを重複除外したりできます。重複除外によって、バックアップの転送量が減り、ストレージ領域が節約されます。また、ストレージ ノードは、通常はエージェントが実行するアーカイブに関する操作(ベリファイやクリーンアップなど)を実行し、管理対象のコンピュータに過剰な処理負荷がかかるのを防ぎます。さらに、Acronis Backup & Recovery 10 ストレージ ノードでは、バックアップ アーカイブを格納するための集中管理用格納域として、テープ ライブラリを使用できます。

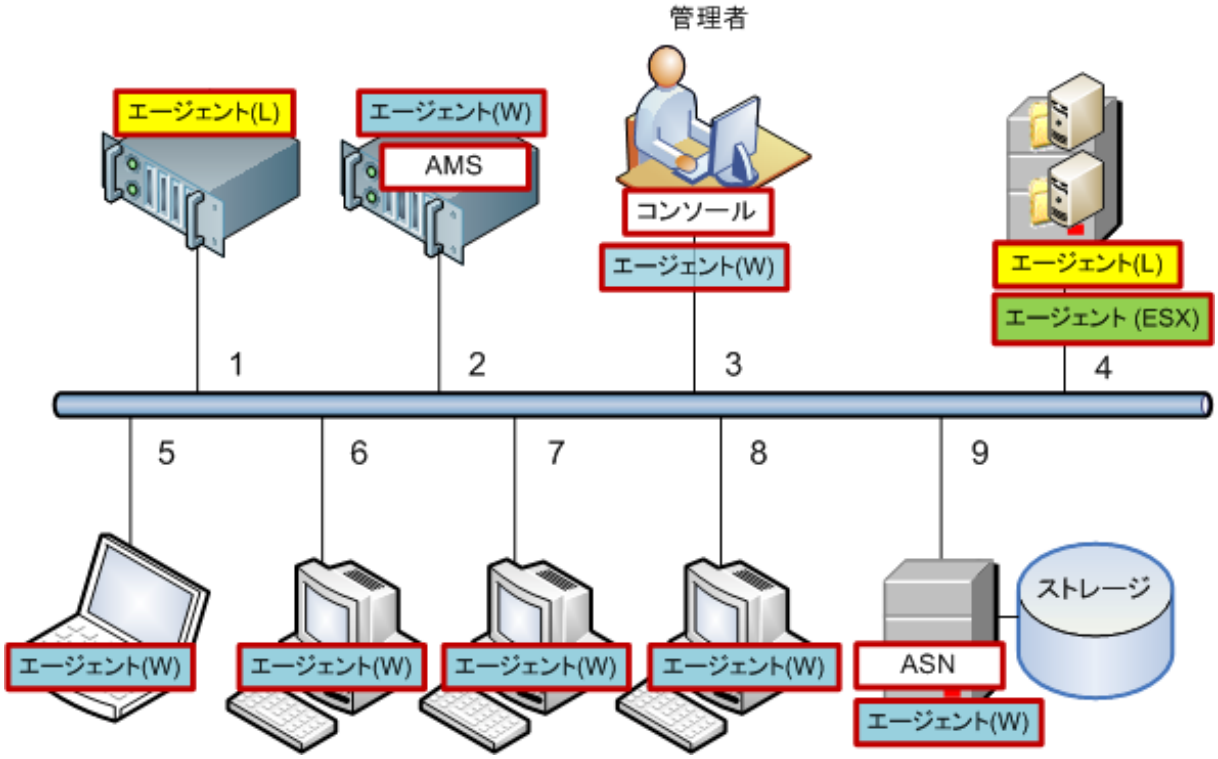
それぞれが多数の格納域を管理する複数のストレージ ノードを設定し、Acronis Backup & Recovery 10 管理サーバーからそれらのストレージ ノードを集中的に制御することができます。

ストレージ ノードの詳細については、「Acronis Backup & Recovery 10 ストレージ ノード『ページ参照 23』」をご参照ください。

2.13.2. 異種ネットワーク内での集中データ保護の設定

ネットワーク インフラストラクチャに、Windows と Linux を実行しているサーバー(1、2、9)とコンピュータ(3、5 ～ 8)があるとします。2 つのゲスト システムをホストする VMware ESX サーバー(4)もあります。

サーバー全体、コンピュータ上のユーザー データ、および仮想コンピュータを保護する必要があります。そこで、データ保護の状態を追跡できるようにすること、バックアップ アーカイブに重複する情報が格納されないようにすること、および古いバックアップを適切な時期にストレージから削除することを計画します。これらの目標は、必要なデータ項目を重複除外された集中管理用格納域に定期的にバックアップすることにより達成できます。



Acronis インフラストラクチャの設定

1. 操作を行うコンピュータ**(3)**に Acronis Backup & Recovery 10 管理コンソール「**コンソール**」をインストールします。このコンソールでは、GUI(Graphical User Interface; グラフィカル ユーザー インターフェイス)を使用して他の Acronis コンポーネントにアクセスして管理することができます。
2. Windows サーバーの 1 台**(2)**に Acronis Backup & Recovery 10 管理サーバー「**AMS**」をインストールします。管理サーバーは、Acronis インフラストラクチャに対する単一の入り口として機能します。
3. コンピュータのディスク、ボリューム、またはファイルをバックアップする各コンピュータに Acronis Backup & Recovery 10 エージェントをインストールします。
   - **エージェント(W)** - エージェント for Windows
   - **エージェント(L)** - エージェント for Linux

     ESX サーバーは Linux Red Hat に基づいているので、エージェント for Linux をこの仮想化製品上にインストールできます。サーバーが ext2 ファイル システムまたは ext3 ファイル システムを使用しているときは、そのサーバーのディスク、ボリューム、またはファイルをバックアップできます。ネイティブの ESX ファイル システムは、セクタ単位でのみバックアップすることができます。

エージェントをインストールするときに、それぞれのコンピュータを管理サーバーに登録します。コンピュータを登録するには、インストール ウィザードの該当するウィンドウで、サーバーの名前または IP アドレスとサーバーの管理者ログイン情報を入力します。または、後でサーバー名または IP アドレスを使用して、コンピュータを管理サーバーに追加します。

4. ホストから仮想コンピュータをバックアップする「**エージェント(ESX)**」用の Acronis Backup & Recovery 10 エージェントを ESX サーバー**(4)**にインストールします。このエージェントは仮想アプライアンスとして提供されます。
5. Windows サーバーの 1 台**(9)**に Acronis Backup & Recovery 10 ストレージ ノード「**ASN**」をインストールします。ストレージ ノードでは、バックアップ アーカイブを格納するためのインフラストラクチャを構成して重複除外機能を使用することができます。ホストに十分な能力があるときは、管理サーバーと共にストレージ ノードをインストールできます。

   ストレージ ノードをインストールするときに、エージェントと同じ方法で、管理サーバーにノードを登録します。

インストールのヒント

- AMS と ASN の両方をコンピュータのオペレーティング システムにインストールすることもできます。
- ネットワーク上に複数のストレージ ノードを配置することができます。各ノードで、最高 20 台のローカル格納域またはリモート格納域を管理できます。
- 1 回のインストール手順で複数の Acronis Backup & Recovery 10 コンポーネントをコンピュータにインストールできます。
- Active Directory ドメインでは、グループ ポリシーを使用してコンポーネントを配置できます。

ストレージ ノードの設定

ストレージ ノードを使用する前に、ノードの格納域にバックアップするすべてのユーザーが、ノードに Windows アカウントを持っていることを確認します。

- ストレージ ノードが Active Directory ドメイン内に配置されているときは、すべてのドメイン ユーザーがノードにバックアップを作成することが可能で、すべてのドメイン管理者がノードの管理者になります。
- ワークグループでは、ノードにバックアップする各ユーザーのローカル ユーザー アカウントを作成します。Administrators グループのメンバが、ノードの管理者になります。必要に応じて、後で他のアカウントを追加することができます。

1. コンソールを実行し、管理サーバーに接続します。
2. 「集中管理用格納域の操作『ページ参照 157』」の説明に従って管理対象の格納域を作成します。管理対象の格納域を作成するときに重複除外を有効にします。

グループとポリシーの設定

コンピュータのグループの構成が必要になる状況とその理由については、「登録されたコンピュータのグループ化『ページ参照 71』」で詳細に説明します。ここでは、前述の Acronis Backup & Recovery 10 の実装によってサポートされるいくつかのシナリオについて説明します。

2.13.2.1. サーバーの保護

ほとんどの場合、サーバーの役割に応じて、各サーバーに個別のバックアップ計画を作成します。ただし、少なくとも 1 回はサーバー全体の完全バックアップを実行する必要があります。ソフトウェアをインストールまたは更新してからリロケーションなどを行うまでの間に、保守ウィンドウまたはバックアップ ウィンドウでサーバーのバックアップを実行することができます。ここで説明する例では、サーバー全体を定期的にバックアップする必要はありません。バックアップの数は多くないため、古いバックアップを手動で削除することができます。

1. ストレージ ノードの管理対象の格納域に**すべてのボリューム**をバックアップするポリシーを作成します。手動で起動する［**後でバックアップ**］とバックアップの種類［**完全**］を選択します。
2. たとえば、S_1 という名前で静的なグループを作成します。このグループにすべてのサーバーを追加します(管理対象の格納域がローカル ノードのドライブ上にないときには、ストレージ ノードを追加できます。ローカル ドライブ上にあるときは、アーカイブ ストレージはその管理対象格納域にバックアップされます)。
3. S_1 グループにポリシーを適用します。ポリシーが各サーバーに正常に配置されたことを確認します。ポリシーの配置状態が［**配置中**］から［**配置済み**］に変わり、そのステータスは［**OK**］になっている必要があります。各サーバーに作成されたバックアップ計画を確認する手順は、次のとおりです。
   a. ［**すべてのコンピュータ**］グループまたは S_1 グループに移動します。
   b. サーバーを選択します。
   c. ［**情報**］ペインの［**バックアップの計画およびタスク**］タブを選択します。

いずれかのサーバーのバックアップが必要なときは、前述したバックアップ計画に移動し、計画を選択して実行します。

2.13.2.2. ワークステーションの保護

ここでは、最も一般的なスケジュールとして、ユーザーのデフォルトのドキュメント フォルダに対する週単位の完全バックアップと日単位の増分バックアップを設定する方法について説明します。また、保持するバックアップは最新の 7 日分のみとします。

1. ストレージ ノードの管理対象の格納域に**すべてのプロファイルのフォルダ**をバックアップするポリシーを作成します。これにより、ユーザー プロファイルのあるフォルダ(Windows XP では C:¥Documents and Settings など)がバックアップされます。［**カスタム**］バックアップ スキームを選択します。
   a. 完全バックアップを次のようにスケジュールします。**週単位**、1 週間ごとの日曜日、タスクを午前 12:00:00 に 1 回実行。詳細設定: Wake-on-LAN はオン。また、ネットワークの使用率およびストレージ ノードの CPU 負荷を最適化するため、バックアップの開始時刻に時間枠を設定することもできます。
   b. 増分バックアップを次のようにスケジュールします。**週単位**、1 週間ごとの平日、タスクを午後 08:00:00 に 1 回実行。必要に応じて詳細設定も行います。

c. 保持のルールを次のように設定します。**次より古いバックアップは削除する**: 7 日。**依存関係のあるバックアップを削除する場合:** バックアップの統合。残りのルールはデフォルト設定をそのまま使用します。［**保持のルールの適用**］に［**バックアップ後**］を設定します。

2. たとえば、W_1 という名前のダイナミック グループを作成します。条件として **%Windows%XP%** と **%Windows%Vista%** を指定します。この方法では、後から管理サーバーに登録するすべてのワークステーションがこのグループに追加され、同じポリシーによって保護されます。
3. W_1 グループにポリシーを適用します。ポリシーが各ワークステーションに正常に配置されたことを確認します。ポリシーの配置状態が［**配置中**］から［**配置済み**］に変わり、そのステータスは［**OK**］になっている必要があります。各ワークステーションに作成されたバックアップ計画を確認する手順は、次のとおりです。

   a. ［**すべてのコンピュータ**］グループまたは W_1 グループに移動します。

   b. ワークステーションを選択します。

   c. ［**情報**］ペインの［**バックアップの計画およびタスク**］タブを選択します。

   ワークステーションに対して作成されたタスクも［**タスク**］ビューで確認できます。
4. ［**ダッシュボード**］ビューまたは［**タスク**］ビューを使用して、ポリシーに関連した日単位のアクティビティを確認します。すべてのタスクが指定どおりに実行されていることを確認した後は、ポリシーの状態は［**バックアップ ポリシー**］ビューでのみ確認できます。

日単位でのデータの保護には、GFS バックアップ スキームまたはハノイの塔バックアップ スキームを使用することもできます。

2.13.2.3. 仮想コンピュータの保護

Acronis Backup & Recovery 10 エージェント for ESX を使用すると、次のような複数の方法で仮想コンピュータを柔軟に保護できます。

- コンソールを仮想アプライアンス(エージェント for ESX)に接続し、仮想コンピュータの一部または前部をバックアップするバックアップ計画を作成する。
- コンソールを仮想アプライアンス(エージェント for ESX)に接続し、コンピュータごとに個別のバックアップ計画を作成する。この計画では、指定したボリュームをバックアップします。
- 仮想アプライアンス(エージェント for ESX)を管理サーバーに登録する。仮想アプライアンスを除くすべての仮想コンピュータは、［**すべての仮想コンピュータ**］グループに表示されます。これらのコンピュータをグループ化し、ディスクやボリュームのバックアップ先とする任意のポリシーを適用できます。
- エージェント for Windows またはエージェント for Linux を各仮想コンピュータにインストールし、コンピュータを管理サーバーに登録する。コンピュータは物理コンピュータと見なされます。これらのコンピュータにバックアップ ポリシーを適用したり、コンピュータごとに個別にバックアップ計画を作成できます。いずれかのコンピュータが物理コンピュータのダイナミック グループに対して設定されたメンバシップ条件を満たすと、そのコンピュータはグループに適用されるポリシーによって保護されます。

Virtual Edition 以外の Advanced Edition(Acronis Backup & Recovery 10 Advanced Server、Advanced Server SBS Edition、および Advanced Workstation)では、上記の最後の方法だけを使用できます。

2.13.3. 登録されたコンピュータのグループ化

管理サーバーにコンピュータを登録『ページ参照 429』するとすぐに、**[すべてのコンピュータ]** ビルトイン グループ『ページ参照 422』にそのコンピュータが表示されます。このグループにバックアップ ポリシーを適用することによって、登録されているすべてのコンピュータを保護します。各コンピュータの役割が異なるときは、1 つのポリシーで十分に対応できないことがあります。バックアップされるデータはそれぞれの部門に固有で、一部のデータは頻繁にバックアップが必要なのに対し、他のデータは 1 年に 2 回で十分なことがあります。そのため、コンピュータの異なるセットに適用できるさまざまなポリシーを作成する必要がある場合があります。この場合は、カスタム グループの作成を検討します。

2.13.3.1. 静的グループと動的グループ

カスタム グループに含めるコンピュータを明示的に指定できます。たとえば、各経理担当者のコンピュータをすべて選択するとします。経理部門のポリシーをそのグループに適用すると、経理担当者のコンピュータ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。このようなグループは、管理者が明示的にコンピュータを追加または削除しない限りその内容は変更されないため、静的『ページ参照 427』グループと呼ばれます。

一方、経理部門で別個の Active Directory 組織単位を構成している場合は、手動の操作は必要ありません。この経理 OU をグループ メンバシップの条件として指定します。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その OU に追加するとすぐに、そのコンピュータはグループに追加され、自動的に保護されます。このようなグループは内容が自動的に変更されるため、動的『ページ参照 417』グループと呼ばれます。

2.13.3.2. 動的なグループ化の条件

Acronis Backup & Recovery 10 管理サーバーでは、次の動的なメンバシップの条件が適用されます。

- オペレーティング システム(OS)
- Active Directory の組織単位(OU)
- IP アドレス範囲

動的なグループに対して複数の条件を指定できます。たとえば、"OS が Windows 2000 に等しい、OS が Windows 2003 に等しい、OU が経理に等しい" という一連の条件は、"Windows 2000 または Windows 2003 が動作し、経理組織単位に属するすべてのコンピュータ" と解釈されます。

[すべてのコンピュータ] グループは、すべての登録済みコンピュータを含む、という単一の設定済みの条件を持つ動的なグループと考えることができます。

2.13.3.3. カスタム グループの使用

管理者は、グループ化を使用して、会社の部門別、Active Directory 組織単位別、ユーザーのさまざまな集団別、サイトの場所別などの条件でデータの保護を設定できます。AD OU の条件を最大限に活用するには、管理サーバーでの Active Directory 階層の作成を検討します。IP アドレスの範囲別にグループ化すると、ネットワーク トポロジを考慮に入れることができます。

作成するグループは入れ子にすることができます。管理サーバーは、最大 500 グループを保持することができます。1 台のコンピュータが、複数のグループのメンバになることができます。

物理コンピュータに加え、登録された仮想サーバー上でホストされる仮想コンピュータもグループ化できます。仮想コンピュータには、そのプロパティに応じて独自のグループ化条件を設定します。

2.13.3.4. 例

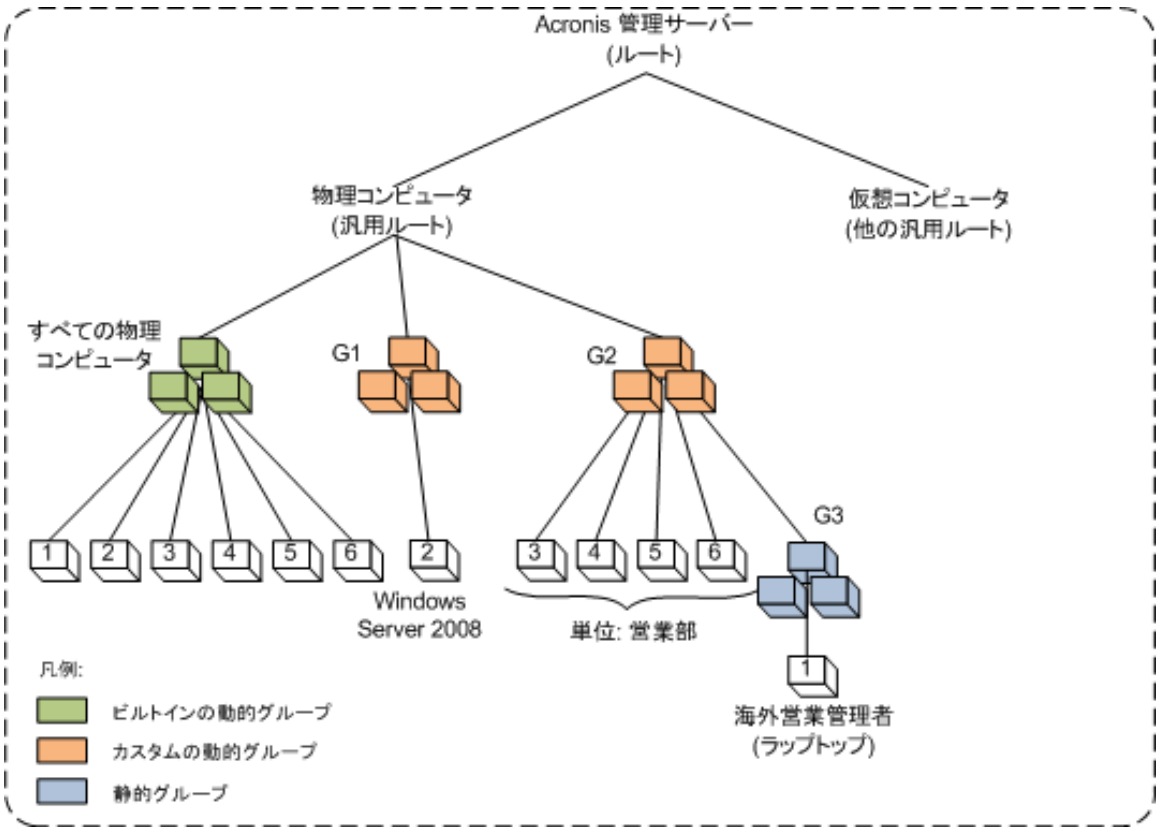
次の図は、グループ階層の例を示しています。

管理サーバーに 6 台のコンピュータが登録されています。

1 - 海外営業管理者のラップトップ コンピュータ (Windows Vista)

2 - 企業データベースと共有ドキュメント ストレージを保持するサーバー(Windows Server 2008)

3、4、5、6 - "営業部" AD 組織単位の営業担当者のコンピュータ (Windows XP)



グループ階層の例

サーバーのバックアップ ポリシーは、ワークステーションとは異なるポリシーにする必要があります。管理者は、サーバー オペレーティング システムがインストールされたコンピュータを含む動的な G1 グループを作成し、そのグループにバックアップ ポリシーを適用します。ネットワークに追加され、管理サーバーに登録されるサーバーはすべてこのグループのメンバーとなり、ポリシーが自動的に適用されます。

営業担当者のワークステーションを別のポリシーで保護するために、管理者は AD OU の条件を使用して動的な G2 グループを作成します。コンピュータの OU メンバシップに関する変更はすべて、G2 メンバシップに反映されます。新しい OU メンバに適切なポリシーを適用し、OU から削除されたコンピュータのポリシーを取り消します。

海外営業管理者のラップトップ コンピュータはこの OU に含まれませんが、営業部のコンピュータが使用するデータの一部を保持しています。このデータをバックアップするには、管理者はラップトップ コンピュータを "強制的" に G2 に追加する必要があります。これは、静的なグループ(G3)を作成し、この静的なグループを動的なグループ内に移動することにより実現できます。親グループ(G2)に適用されるポリシーは子グループ(G3)にも適用されますが、G3 のメンバは G2 のメンバとは見なされないため、その動的な性質は失われません。

実際には、管理者はほとんどの場合、海外営業管理者のコンピュータをいずれのグループにも含めず、そのコンピュータに直接ポリシーを適用すると思われます。この例は、単にさまざまな種類のグループが入れ子になった状態を示すためのものです。複数のグループ メンバがあるときは、グループを入れ子にすると便利です。

2.13.3.5. カスタム グループの操作

汎用ルート(物理コンピュータまたは仮想コンピュータ)または既存のグループ内に空のグループを作成し、手動でコンピュータを追加する(静的グループ)か、動的グループのメンバシップの条件を追加して、グループを設定します。次の操作を実行することもできます。

- グループを編集して次の操作を実行する。
  - グループ名を変更する。
  - グループの説明を変更する。
  - 動的なメンバシップの条件を変更する。
- 静的グループにメンバシップの条件を追加して動的グループに変換する。
- 次の 2 つのオプションから選択して、動的グループを静的グループに変換する。
  - グループ メンバを保持する。
  - グループ メンバを削除する。
- グループをルートから別のグループに移動する(任意のグループの種類から任意のグループの種類へ)。
- グループを親グループからルートに移動する。
- グループをある親グループから別の親グループに移動する(任意のグループの種類から任意のグループの種類へ)。
- グループを削除する。つまり、すべてのコンピュータのグループに残っているグループ メンバの参加を解除する。

バックアップ ポリシーが適用されているグループを操作すると、メンバのコンピュータのポリシーが変更されます。その時点でコンピュータを使用できないか接続できないときは、処理は保留になり、コンピュータが使用できるようになるとすぐに処理が実行されます。

この操作を実行する方法については、「グループの操作『ページ参照 358』」をご参照ください。

2.13.4. コンピュータとグループのポリシー

ここでは、管理サーバーによって実行されるポリシーの自動的な配置および取り消しについて説明します。これらの処理は、コンピュータおよびさまざまな組み合わせで入れ子になったコンピュータのグループに 1 つまたは多数のポリシーを適用するとき、コンピュータおよびグループのポリシーを取り消すとき、あるいはコンピュータまたはグループをあるグループから別のグループに移動するときに、実行されます。

バックアップ ポリシーが適用されているグループを操作すると、メンバのコンピュータのポリシーが変更されます。グループの移動、削除、作成、静的なグループへのコンピュータの追加、または動的な条件によるグループへのコンピュータの追加など、どの階層の変更からも膨大な数の継承の変更が発生する可能性があります。実行する操作で意図した結果が得られるように、また Acronis Backup & Recovery 10 管理サーバーの自動化された操作による結果を理解できるように、このセクションの内容を十分に理解してください。

適用、配置、および取り消しについて

適用 - ポリシーを適用すると、1 台以上のコンピュータの間に対応関係が確立されます。この処理は管理サーバーのデータベース内で実行され、短時間で完了します。

配置 - ポリシーを配置すると、確立された対応関係がコンピュータに転送されます。具体的には、ポリシーによって指定された構成に従って、各コンピュータに一連のタスクが作成されます。

取り消し - ポリシーを取り消すと、適用と配置の操作全体に対して逆の操作が実行されます。取り消しによってポリシーと 1 台以上のコンピュータ間の対応関係が解除され、コンピュータからタスクが削除されます。

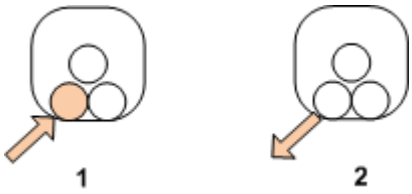
その時点でコンピュータを使用できないか接続できないときは、使用できるようになったときに変更がコンピュータに反映されます。これは、複数のコンピュータへのポリシーの配置が瞬間的な操作ではないことを示します。取り消しのときも同様です。この 2 つの処理は時間がかかることがあるため、管理サーバーは、ポリシーの蓄積されたステータスだけでなく、操作する各コンピュータの個々のステータスを追跡して表示します。

2.13.4.1. コンピュータまたはグループのポリシー

次の図では、番号付けされた方法はそれぞれ、番号付けされた操作の結果を示しています。

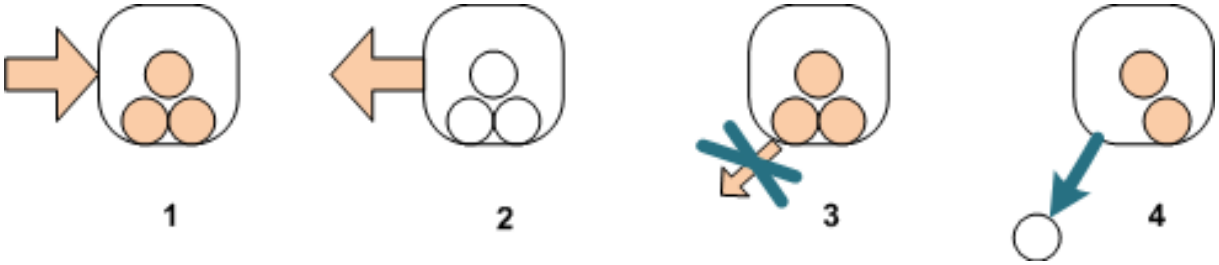
コンテナはグループを表し、色付けされた円はポリシーが適用されたコンピュータを表します。濃く色付けされた円は同じポリシーが 2 回適用されたコンピュータを表し、白い円はポリシーが適用されていないコンピュータを表します。

コンピュータのポリシー



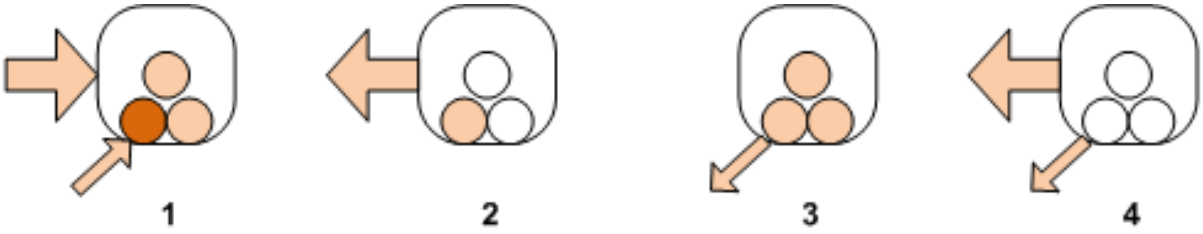
1. ポリシーはコンピュータに適用できます。
2. ポリシーはコンピュータから取り消すことができます。

グループのポリシー



1. ポリシーはグループに適用できます。
2. ポリシーはグループから取り消すことができます。
3. グループに適用されたポリシーは、コンピュータで取り消すことはできません。
4. コンピュータのポリシーを取り消すには、グループからそのコンピュータを削除します。

グループおよびコンピュータでの同一ポリシー



1. 同じポリシーをグループとコンピュータに適用できます。同じポリシーが 2 回適用されもコンピュータに変化はありませんが、ポリシーが 2 回適用されたことはサーバーに記録されています。
2. グループからポリシーを取り消しても、そのポリシーはコンピュータに適用されたままになります。
3. コンピュータからポリシーを取り消しても、そのポリシーはグループに適用されたままであるため、コンピュータでも適用されたままになります。
4. コンピュータからポリシーを完全に取り消すには、グループとコンピュータの両方のポリシーを取り消します。

2.13.4.2. コンピュータでの操作

ここでは、グループのコンピュータを移動、コピー、または削除したときに、コンピュータのポリシーに対して実行される処理を簡単に説明します。

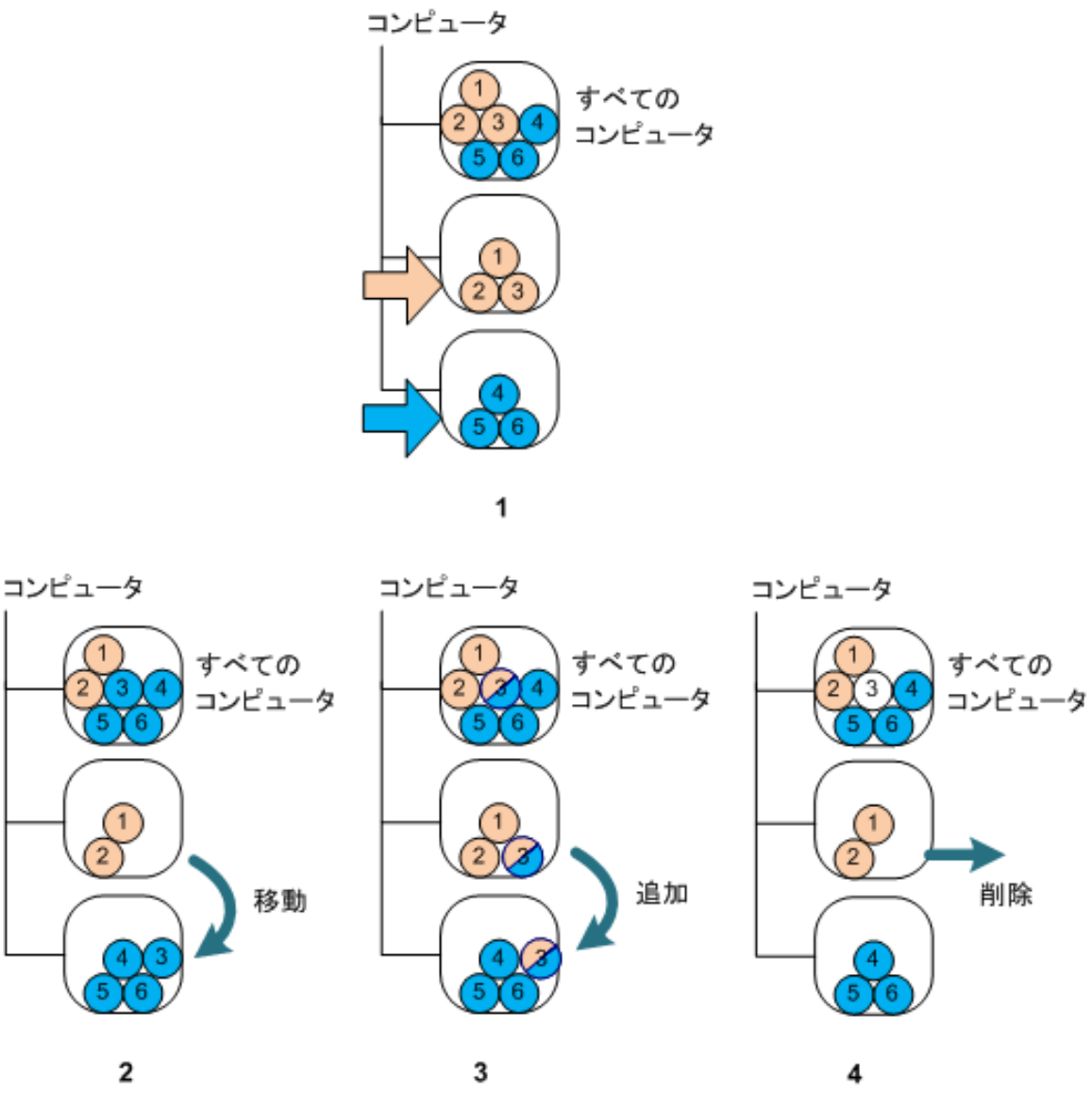
次の図で、コンテナはグループを表し、1 色の円は 1 つのポリシーが適用されたコンピュータを表します。2 色の円は 2 つのポリシーが適用されたコンピュータを表し、白い円はポリシーが適用されていないコンピュータを表します。

1. 最初の状態です。2 つのカスタム グループに異なるコンピュータが含まれています。一方のグループにあるポリシーが適用され、もう一方のグループには別のポリシーが適用されています。次の各スキームは、指定されたそれぞれの操作の結果を示しています。

2. **別のグループに移動:** コンピュータ #3 を、あるグループから別のグループに移動します。"オレンジ色" のポリシーは取り消され、"青色" のポリシーがコンピュータに適用されます。

3. **別のグループに追加:** コンピュータ #3 を別のグループに追加します。このコンピュータは両方のグループのメンバになります。"青色" のポリシーが適用されますが、そのコンピュータの "オレンジ色" のポリシーも適用されたままになります。

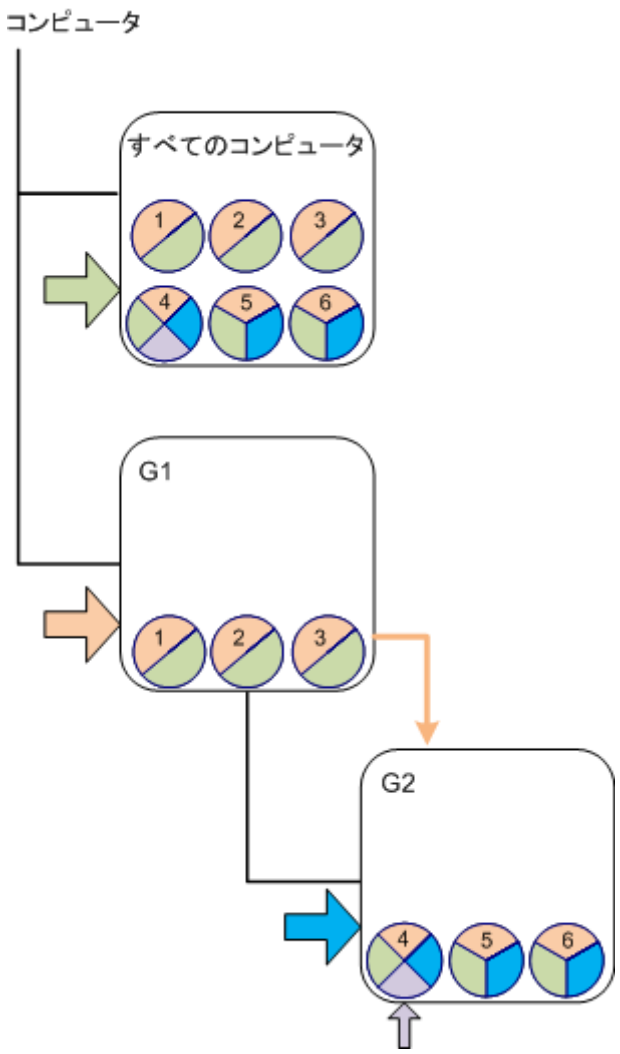
4. **グループから削除:** コンピュータ #3 をグループから削除します。コンピュータの "オレンジ色" のポリシーが取り消されます。このコンピュータは、［**すべてのコンピュータ**］グループに残されます。



2.13.4.3. ポリシーの継承

ポリシーの継承は、あるコンピュータが［**すべてのコンピュータ**］グループのほかに 1 つのグループについてのみ、そのメンバになることができると仮定すると、簡単に理解することができます。この簡略化されたアプローチから説明を始めます。

次の図で、コンテナはグループを表し、2 色の円は 2 つのポリシーが適用されたコンピュータを表します。3 色の円は 3 つのポリシーが適用されたコンピュータを表し、それ以上も同様です。



[すべてのコンピュータ]グループのほかに、ルートにカスタムの G1 グループがあり、さらに G1 の子としてカスタムの G2 グループがあります。

[すべてのコンピュータ]グループに適用される "緑色" のポリシーは、すべてのコンピュータに継承されます。

G1 に適用される "オレンジ色" のポリシーは、G1 のメンバに加え、その直接と間接両方のすべての子グループに継承されます。

G2 に適用される "青色" のポリシーは、G2 に子グループがないため、G2 のメンバにのみ継承されます。

"紫色" のポリシーは、コンピュータ #4 に直接適用されます。このポリシーは、コンピュータのいずれのグループのメンバシップにも関係なく、コンピュータ #4 用として存在します。

ここで、ルートに G3 グループを作成するとします。このグループにポリシーを適用しないと、そのメンバはすべて "緑色" になります。ただし、たとえばコンピュータ #1 を G3 に追加すると、G3 は "オレンジ色" のポリシーと関係なくても、このコンピュータに "オレンジ色" と "緑色" 両方のポリシーが適用されます。

このため、同じコンピュータが複数のグループに含まれているときは、階層の最上位からポリシーの継承を追跡することは困難です。

実際には、コンピュータ側から継承を表示すると簡単に確認できます。そのためには、コンピュータが含まれた任意のグループに移動し、コンピュータを選択して、**[情報]** ペインの **[バックアップ ポリシー]** タブを選択します。**[継承]** 列に、そのコンピュータにポリシーが継承されるかまたは直接適用されるかが表示されます。**[継承の参照]** をクリックし、ポリシーの継承の順序を表示します。この例では、ポリシー名、**[継承]** 列、および継承の順序は次のとおりです。

コンピュータ	ポリシー名	継承	継承の順序
#1、#2、または #3	"緑色"	継承	すべてのコンピュータ -> #1、#2、または #3
	"オレンジ色"	継承	G1 -> #1、#2、または #3
#4	"緑色"	継承	すべてのコンピュータ -> #4
	"オレンジ色"	継承	G1 -> G2 -> #4
	"青色"	継承	G2 -> #4
	"紫色"	直接適用	
#5 または #6	"緑色"	継承	すべてのコンピュータ -> #5 または #6
	"オレンジ色"	継承	G1 -> G2 -> #5 または #6
	"青色"	継承	G2 -> #5 または #6

2.13.5. バックアップ ポリシーの状態とステータス

集中管理は、管理者がいくつかの簡単に理解できるパラメータを使用して、製品インフラストラクチャ全体の状態を監視できることを前提としています。バックアップ ポリシーの状態とステータスは、それらのパラメータに格納されます。インフラストラクチャの最下部(管理対象のコンピュータのタスク)で問題が発生すると、ポリシー ステータスに問題が蓄積されます。管理者はひと目見ただけでステータスを確認できます。ステータスが［OK］でないときは、数回クリックするだけで問題の詳細情報に移動できます。

ここでは、管理サーバーに表示されるポリシーの状態とステータスについて説明します。

2.13.5.1. コンピュータへのポリシーの配置状態

このパラメータを表示するには、ツリーでコンピュータが含まれたグループを選択し、コンピュータを選択して、［**情報**］ペインの［**バックアップ ポリシー**］タブを選択します。

コンピュータまたはコンピュータのグループにポリシーを適用すると、サーバーによってコンピュータにポリシーが配置されます。それぞれのコンピュータで、エージェントによってバックアップ計画が作成されます。ポリシーがコンピュータに転送され、バックアップ計画が作成されている間、そのコンピュータのポリシーの配置状態は［**配置中**］になります。

バックアップ計画の作成が正常に完了すると、コンピュータのポリシーの状態は［**配置済み**］になります。

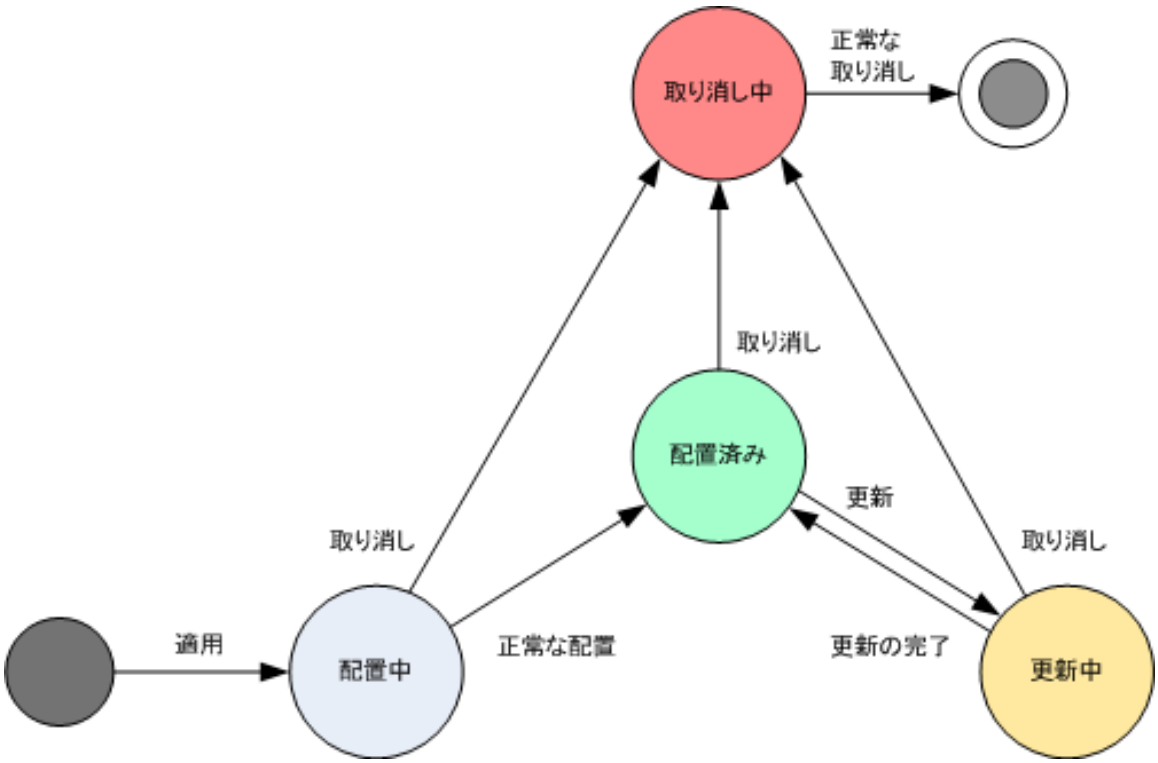
何らかの理由でポリシーの変更が必要になることがあります。変更を承認すると、ポリシーが配置されているすべてのコンピュータのポリシーが管理サーバーによって更新されます。変更内容がコンピュータに転送され、エージェントによってバックアップ計画が更新されている間、そのコンピュータのポリシーの状態は［**更新中**］になります。ポリシーの更新が完了すると、状態は再び［**配置済み**］になります。この状態は、ポリシーが正常に機能し、現在このポリシーに対する変更は行われていないことを示します。

配置の実行中に変更されたポリシーは、状態が［**配置中**］のままになります。管理サーバーは、最初から変更済みになっているポリシーの配置のみを開始します。

コンピュータまたはコンピュータが含まれたグループのポリシーの取り消しが必要になることがあります。変更を承認すると、管理サーバーによってコンピュータのポリシーが取り消されます。変更内容がコンピュータに転送され、エージェントによってバックアップ計画が削除されている間、そのコンピュータのポリシーの状態は［**取り消し中**］になります。

コンピュータがあるグループから別のグループに移動するように、グループ化の条件を変更したりコンピュータのプロパティを変更することができます。この変更を行うことにより、あるポリシーが取り消されて別のポリシーに配置されます。この場合、コンピュータの最初のポリシーの状態は［**取り消し中**］になり、2 番目のポリシーの状態は［**配置中**］になります。それぞれのポリシーは GUI に同時に表示されるか、1 つずつ順に表示されます。

バックアップ ポリシーの状態の図



2.13.5.2. コンピュータのポリシー ステータス

このパラメータを表示するには、ツリーでコンピュータのグループを選択し、コンピュータを選択して、［**情報**］ペインの［**バックアップ ポリシー**］タブを選択します。

それぞれの状態によって、バックアップ ポリシーは、［**エラー**］、［**警告**］、［**OK**］のいずれかになります。ポリシーの状態が［**配置済み**］のとき、そのステータスはポリシーが正常に実行されているかどうかを示します。ポリシーがその他の状態のとき、そのステータスはポリシーが正常に変更されているかどうかを示します。

バックアップするデータがコンピュータ上に見つからない場合のポリシー ステータス

バックアップ ポリシーは、選択ルール『ページ参照 428』を満たすデータが存在しないコンピュータに適用される可能性があります。今後データが見つかると想定されるので、ポリシーの配置時にエラーや警告は記録されません。バックアップ計画は通常どおりに作成され、ポリシーの状態は［**配置済み**］に変わります。

バックアップ タスクの開始時にバックアップするデータが見つからないと、そのタスクは中止され、ポリシーの状態は［**エラー**］に変わります。1 つ以上のデータ項目が見つかると、バックアップ タスクは警告を伴って正常終了します。ポリシーの状態もそれに応じて変わります。

バックアップ タスクはポリシーで指定したスケジュールに合わせて開始され、すべてのデータ項目がコンピュータ上に存在するか、存在しないデータ項目を除外するようにポリシーが編集されるまで同じ結果になります。

例

選択規則で、ポリシーによってボリューム D: と F: をバックアップする必要のあることが指定されているとします。このポリシーは、Linux コンピュータと Windows コンピュータの両方に適用されます。最初のバックアップが開始されると、このようなボリュームのない Linux コンピュータおよび Windows コンピュータでのポリシーの状態は［**エラー**］になります。D: ボリュームまたは F: ボリュームがある Windows コンピュータでのポリシーの状態は、エラーで終わるイベントが発生しない限り、［**警告**］になります。

［System］ボリュームと /dev/sda1 ボリュームをバックアップする必要のあるポリシーの状態は、Windows コンピュータでは /dev/sda が見つからないため、また /dev/sda1 ボリュームのある Linux コンピュータでは［System］ボリュームが見つからないため、［**警告**］になります。SCSI デバイスのない Linux コンピュータでのポリシーの状態は［**エラー**］になります。

詳細を次の表に示します。

状態	ステータス	説明
配置中	**エラー**	配置ログにエラーが記録されています。たとえば、ディスク領域が不足しているなど。
	警告	配置ログに警告が記録されています。配置中にコンピュータがオフラインになった、N 日間接続できないなど。
	OK	配置ログにエラーおよび警告は記録されていません。
配置済み	**エラー**	対応するバックアップ計画のステータスが［**エラー**］です。
	警告	対応するバックアップ計画のステータスが［**警告**］です。
	OK	対応するバックアップ計画のステータスが［**OK**］です。
更新中	**エラー**	更新ログにエラーが記録されています。ロックされたタスクを削除できない、Acronis サービスを停止できないなど。
	警告	更新ログに警告が記録されています。
	OK	更新ログにエラーおよび警告は記録されていません。
取り消し中	**エラー**	取り消しログにエラーが記録されています。
	警告	取り消しログに警告が記録されています。
	OK	取り消しログにエラーおよび警告は記録されていません。

バックアップ ポリシーには、特定のコンピュータに関連する配置の状態とステータスのほかに、コンピュータのグループへの配置の状態とステータスおよびポリシーの蓄積された配置の状態とステータスがあります。

2.13.5.3. グループへのポリシーの配置状態

このパラメータを表示するには、ツリーで［**コンピュータ**］を選択し、グループを選択して、［**情報**］ペインの［**バックアップ ポリシー**］タブを選択します。

この状態は、グループおよびその子グループに含まれるコンピュータへのポリシーの配置状態の組み合わせとして定義されます。

たとえば、コンピュータ A および B で構成されるグループにポリシーを適用したとします。両方のコンピュータへの配置が実行されている間、グループのポリシーの状態は "配置中" になります。コンピュータの 1 台への配置が完了したときに、他のコンピュータへの配置が続行中の場合、状態は "配置中、配置済み" になります。両方のコンピュータへの配置が完了すると、状態は "配置済み" になります。

2.13.5.4. グループのポリシーのステータス

このパラメータを表示するには、ツリーで［**コンピュータ**］を選択し、グループを選択して、［**情報**］ペインの［**バックアップ ポリシー**］タブを選択します。

このステータスには、グループおよびその子グループに含まれる各コンピュータのポリシーのうち、最も重大なステータスが定義されます。現在いずれのコンピュータにもポリシーが適用されていないとき、ステータスは "OK" になります。

2.13.5.5. ポリシーの蓄積された状態とステータス

バックアップ ポリシーには、特定のコンピュータまたはグループに関連する配置の状態とステータスのほかに、蓄積された配置の状態と蓄積されたステータスがあります。

バックアップ ポリシーの蓄積された状態

このパラメータを表示するには、ツリーで［**バックアップ ポリシー**］を選択します。［**配置の状態**］列に、それぞれのポリシーの蓄積された配置の状態が表示されます。

この状態は、ポリシーが(直接または継承を通じて)適用されるすべてのコンピュータへのポリシーの配置状態の組み合わせとして定義されます。現在いずれのコンピュータにもポリシーが適用されていないとき、配置の状態は設定されず、列に "未適用" と表示されます。

たとえば、コンピュータ A にポリシーを適用したとします。ポリシーは正常に配置されました。次に、ポリシーを変更し、コンピュータ B および C で構成されたグループにすぐにそのポリシーを適用します。A のポリシーを更新し、B と C に配置する必要があります。この処理が実行されている間、ポリシーの蓄積された状態は "更新中、配置中" のように表示され、次に "更新中、配置済み" または "配置済み、配置中" に変わり、通常、最後は "配置済み" になります。

バックアップ ポリシーの蓄積されたステータス

このパラメータを表示するには、ツリーで［**バックアップ ポリシー**］を選択します。［**ステータス**］列に、それぞれのポリシーの蓄積されたステータスが表示されます。

このステータスは、適用対象となるすべてのコンピュータ中で、最もエラー レベルの高いポリシーのステータスとして定義されます。いずれのコンピュータにもポリシーが適用されていないとき、ステータスは "OK" になります。

2.13.6. 重複除外

ここでは、同一のデータをアーカイブに一度だけ保存することによってデータの重複をなくすように設計されたメカニズムである重複除外について説明します。

2.13.6.1. 概要

重複除外とは、データの反復を検出して同一のデータを 1 回だけ保存することで、データによって使用されるストレージ領域を最小限に抑える処理です。

たとえば、重複除外が有効になっている管理対象の格納域に同じファイルが 2 つ含まれる場合は、同じアーカイブにあるか別のアーカイブにあるかに関係なく、このファイルは 1 回だけ保存され、2 番目のファイルの代わりにそのファイルへのリンクが保存されます。

重複除外によってネットワーク負荷も軽減できます。バックアップ時に、あるファイルまたはディスク ブロックが、既に保存されているものと同じであることが検出されると、その内容はネットワーク経由で転送されません。

重複除外は、ディスク レベルのバックアップではディスク ブロックに対して実行され(ブロック レベルの重複除外)、ファイル レベルのバックアップではファイルに対して実行されます(ファイル レベルの重複除外)。

Acronis Backup & Recovery 10 では、重複除外は次の 2 つの手順から構成されます。

ソースでの重複除外

バックアップ時に管理対象のコンピュータで実行されます。Acronis Backup & Recovery 10 エージェントは、ストレージ ノードを使用して重複除外可能なデータを判断し、既に格納域に複製が存在するデータを転送しません。

ターゲットでの重複除外

バックアップの完了後に格納域で実行されます。ストレージ ノードは、格納域のアーカイブを分析し、格納域のデータを重複除外します。

バックアップ計画を作成する際には、その計画のソースでの重複除外を無効にできます。これによってバックアップの処理速度は速くなりますが、ネットワークとストレージ ノードの負荷は大きくなります。

重複除外された格納域

重複除外が有効になっている集中管理用格納域は、*重複除外された格納域*と呼ばれます。集中管理用格納域を作成する際には、重複除外を有効にするかどうかを指定できます。テープ デバイスには重複除外された格納域を作成することはできません。

重複除外データベース

重複除外された格納域を管理している Acronis Backup & Recovery 10 ストレージ ノードは、格納域に保存されたすべての項目(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)のハッシュ値が含まれる重複除外データベースを保持します。

重複除外データベースは、格納域の作成時に［**集中管理用格納域の作成**］の［**データベースのパス**］で指定したフォルダに保存されます。重複除外データベースはローカル フォルダにのみ作成できます。

重複除外データベースのサイズは、格納域に存在するアーカイブの合計サイズの約 1% です。つまり、1TB の新しい(重複しない)データごとに、データベースに約 10GB が追加されます。

格納域にアーカイブおよびメタデータを含むサービス フォルダが保持されている場合に、データベースが破損したり、ストレージ ノードが失われると、新しいストレージ ノードによって格納域が再スキャンされ、データベースが再作成されます。

2.13.6.2. 重複除外が最も効果的な場合

重複除外が最大の効果を発揮するのは、次の場合です。

- **完全バックアップ モード**で複数のソースから類似のデータをバックアップする場合。これには、単一のソースからネットワークを介して配置されたオペレーティング システムやアプリケーションをバックアップする場合などが該当します。

  たとえば、類似した 100 のシステムを重複除外格納域にバックアップする場合、通常の格納域にバックアップした場合に比べ、アーカイブの占める総領域は減少します。ベスト プラクティスとしては、まず、類似したシステムの 1 つをバックアップします。この結果、Acronis Backup & Recovery 10 ストレージ ノードは、すべてのシステムのファイルを重複除外項目の候補として登録します。これにより、複数のバックアップを同時に実行するかどうかにかかわらず、ソースでの効果的な重複除外によってバックアップ プロセスが高速になり、ネットワーク トラフィックが減少します。
- **データに対する変更も類似**しているときに、異なるソースから類似のデータの**増分バックアップ**を実行する場合。これは、これらのシステムに更新を配置し、増分バックアップを適用する場合などが該当します。この場合も、最初に 1 台のコンピュータをバックアップしてから、残りのコンピュータを一度にすべてまたは 1 台ずつバックアップすることをお勧めします。
- データ内容自体には変更がないが、**場所に変更があった**データの**増分バックアップ**を実行する場合。これには、複数のデータがネットワーク上または 1 つのシステム内を巡回する場合などが該当します。データは移動するごとに増分バックアップに含められ、このバックアップは新しいデータを含んでいなくてもかなり大きくなります。重複除外はこの問題の解決に役立ちます。項目が新しい場所に現れるごとに、項目自体ではなく項目の参照が保存されます。

重複除外と増分バックアップ

データがランダムに変更される場合、次の理由のため、増分バックアップでの重複除外はあまり効果がありません。

- 変更されていない重複除外項目は増分バックアップには含まれません。
- 変更された重複除外項目は、もはや同じではなくなっているため重複除外されません。

2.13.6.3. 重複除外比

重複除外比は、重複除外格納域でのアーカイブのサイズと、重複除外しない格納域で占めるサイズとの比率を表します。重複除外比が高くなると、重複除外のメリットが大きくなります。

たとえば、2 台のコンピュータから内容が同じ 2 つのファイルをバックアップするとします。各ファイルのサイズが 1GB である場合、重複除外しない格納域のバックアップ サイズは約 2GB ですが、重複除外格納域ではわずか 1GB ほどです。この場合、重複除外比は 2:1 になります。

反対に、2 つのファイルの内容が異なる場合、重複除外しない格納域と重複除外格納域のバックアップ サイズは同じ(2GB)になり、重複除外比は 1:1 になります。

予想される比率

状況によっては重複除外比は非常に高くなりますが(前の例では、コンピュータ数が増えるに従い、比率は 3:1、4:1 のようになります)、一般的な環境での妥当な予想比率は 1.2:1 から 1.6:1 の間になります。

より現実的な例として、類似のディスクを備えた 2 台のコンピュータのファイルレベルまたはディスクレベルのバックアップを実行するとします。どちらのコンピュータでも、両方のコンピュータに共通したファイルが、50% のディスク領域(たとえば 1GB)を占め、それぞれのコンピュータに固有のファイルが、残りの 50%(残りの 1GB)を占めます。

重複除外格納域では、この場合の最初のコンピュータのバックアック サイズは 2GB になり、2 番目のバックアップ サイズは 1GB になります。重複除外しない格納域では、バックアップは合計で 4GB を占めます。この結果、重複除外比は 4:3、つまり約 1.33:1 になります。

同様に、3 台のコンピュータの場合、比率は 1.5:1 になり、4 台のコンピュータの場合は 1.6:1 になります。このようなコンピュータがさらに多数同じ格納域にバックアップされると、比率は 2:1 に近づきます。これは、20TB ストレージ デバイスの代わりに 10TB デバイスを購入するだけで済むこと意味します。

実際に減少する容量は、バックアップされるデータの種類、バックアップの頻度、バックアップの保存期間などさまざまな要因に影響されます。

2.13.6.4. 重複除外のしくみ

ソースでの重複除外

重複除外格納域へのバックアップを実行すると、Acronis Backup & Recovery 10 エージェントは、バックアップされている項目(ディスク バックアップではディスク ブロック、ファイル バックアップではファイル)を読み取り、各ブロックのフィンガープリントを計算します。このフィンガープリントは*ハッシュ値*とも呼ばれ、格納域内の項目の内容を一意に表します。

エージェントは格納域に項目を送信する前に、重複除外データベースに照会して、項目のハッシュ値がすでに格納されている項目のハッシュ値と同じかどうかを調べます。

同じである場合、エージェントは、項目のハッシュ値だけを送信します。同じでない場合、項目自体を送信します。

暗号化されたファイルや標準サイズ外のディスク ブロックなどの一部の項目は重複除外できないので、エージェントは常にハッシュ値を計算せずにこれらの項目を格納域に転送します。ファイル レベルとディスク レベルの重複除外の制限の詳細については、「重複除外の制限『ページ参照 87』」をご参照ください。

ターゲットでの重複除外

重複除外格納域へのバックアップが完了した後、ストレージ ノードは、次のように格納域のデータを重複除外します。

1. アーカイブから格納域内の専用フォルダに項目(ディスク ブロックまたはファイル)を移動し、重複した項目をそこに一度だけ保存します。このフォルダは重複除外データ ストアと呼ばれます。重複除外できない項目は、アーカイブ内に残されます。
2. アーカイブ内では、移動された項目が、対応する参照に置き換えられます。

この結果、格納域には一意の重複除外された項目が多数含まれ、項目への 1 つまたは複数の参照が格納域のアーカイブから各項目に与えられます。

圧縮タスク

クリーンアップにより、または手動で 1 つまたは複数のバックアップやアーカイブを格納域から削除した後、どのアーカイブからも参照されなくなった項目が格納域に残る場合があります。このような項目は圧縮タスクで削除されます。これは、ストレージ ノードによって実行されるスケジュールされたタスクです。

デフォルトでは、圧縮タスクは毎週日曜日の夜 03:00 に実行されます。「ストレージ ノードでの操作『ページ参照 364』」の「圧縮タスク スケジュールの変更」での説明に従って、タスクのスケジュールを変更できます。［**タスク**］ビューから、手動でタスクを開始または停止することもできます。

2.13.6.5. 重複除外の制限

ブロック レベルの重複除外の制限

重複除外された格納域に存在するアーカイブへのディスク バックアップでは、次の場合、ボリュームのディスク ブロックの重複除外は実行されません。

- ボリュームが圧縮されている
- クラスタ 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

> ***ヒント:*** *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 であるため、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アロケーション ユニット サイズの例としては、他に 8KB、16KB、64KB があります。*

- アーカイブをパスワードで保護している

> ***ヒント:*** *アーカイブ内のデータを保護しながら、重複除外も有効にするには、アーカイブをパスワードで保護せずに、重複除外する格納域そのものをパスワードで暗号化します。これは、格納域の作成時に行うことができます。*

重複除外されなかったディスク ブロックは、重複除外されない格納域にあるため、アーカイブに保存されます。

ファイルレベルの重複除外の制限

重複除外された格納域に存在するアーカイブへのファイル バックアップでは、次の場合、ファイルの重複除外は実行されません。

- ファイルが暗号化され、バックアップ オプションの［**暗号化されたファイルを暗号化解除された状態でアーカイブに格納する**］チェックボックスがオフになっている(デフォルトではオフ)
- ファイルのサイズが 4KB より小さい
- アーカイブをパスワードで保護している

重複除外されなかったファイルは、重複除外されない格納域にある場合と同じように、アーカイブに保存されます。

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、ファイルは 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。

2.13.7. 集中管理の権限

ここでは、ローカルおよびリモートでのコンピュータの管理、Acronis Backup & Recovery 10 管理サーバーに登録されたコンピュータの管理、および Acronis Backup & Recovery 10 ストレージ ノードに対するアクセスと管理に必要なユーザーの権限について説明します。

2.13.7.1. 管理対象コンピュータへの接続の種類

管理対象コンピュータへの接続には、ローカル接続とリモート接続の 2 種類あります。

ローカル接続

ローカル接続は、コンピュータ上の Acronis Backup & Recovery 10 管理コンソールと、同じコンピュータ上の Acronis Backup & Recovery 10 エージェントとの間で確立されます。

ローカル接続を確立する手順は、次のとおりです。

- ツールバーで［**接続**］をクリックし、［**新しい接続**］をポイントして、［**このコンピュータの管理**］をクリックします。

リモート接続

リモート接続は、あるコンピュータ上の Acronis Backup & Recovery 10 管理コンソールと、別のコンピュータ上の Acronis Backup & Recovery 10 エージェントとの間で確立されます。

リモート接続を確立するには、ログオン情報の指定が必要になる場合があります。

リモート接続を確立する手順は、次のとおりです。

1. ツールバーで［**接続**］をクリックし、［**新しい接続**］をポイントして、［**リモート コンピュータの管理**］をクリックします。
2. ［**コンピュータ**］で、接続先のリモート コンピュータの名前または IP アドレスを入力または選択します。または［**参照**］をクリックして、一覧からコンピュータを選択します。
3. 接続に使用するログオン情報を指定するには、［**オプション**］をクリックし、［**ユーザー名**］ボックスと［**パスワード**］ボックスにそれぞれユーザー名とパスワードを入力します。Windows では、［**ユーザー名**］ボックスを空白のままにした場合、コンソールの実行に使用されているログオン情報が使用されます。
4. 指定したユーザー名のパスワードを保存するには、［**パスワードを保存する**］チェックボックスをオンにします。パスワードは、コンソールが実行されているコンピュータ上の安全なストレージに保存されます。

2.13.7.2. ローカル接続の権限

Windows

Windows を実行するコンピュータ上でのローカル接続は、そのコンピュータで「ローカル ログオン」のユーザー権限を持っている任意のユーザーが確立できます。

Linux

Linux を実行するコンピュータ上でローカル接続を確立したり、そのコンピュータを管理したりするには、そのコンピュータの root 権限が必要です。

root ユーザーとしてローカル接続を確立する手順は、次のとおりです。

1. root ユーザーとしてログオンしている場合は、次のコマンドを実行します。

   ```
   /usr/sbin/acronis_console
   ```

   それ以外の場合は、次のコマンドを実行します。

   ```
   su -c /usr/sbin/acronis_console
   ```

2. ［**このコンピュータの管理**］をクリックします。

root 以外のユーザーがコンソールを起動できるようにする手順は、次のとおりです。

- root ユーザーとして、**visudo** などのコマンドを使用して **/etc/sudoers** というファイルにコンソールの起動を許可する root 以外のユーザーの名前を追加します。

注意: *この手順の結果、root 以外のユーザーは root 権限を使用してコンソールを起動できるだけでなく、root ユーザーとして他の操作も実行できるようになります。*

root 以外のユーザーとしてローカル接続を確立する手順は、次のとおりです。

1. 前の手順で説明されているように、ログインしているユーザーが root ユーザーによってコンソールの起動を許可されていることを確認します。
2. 次のコマンドを実行します。

```
sudo /usr/sbin/acronis_console
```

3. **［このコンピュータの管理］**をクリックします。

2.13.7.3. Windows でのリモート接続の権限

Windows を実行するコンピュータでリモート接続を確立するユーザーは、そのコンピュータの Acronis Remote Users セキュリティ グループのメンバである必要があります。

リモート接続が確立されると、そのユーザーは、「管理対象のコンピュータ上のユーザー権限『ページ参照 34』」で説明されているように、リモート コンピュータに対する管理権限が付与されます。

注意: *ユーザー アカウント制御(UAC)が有効な、ドメインの一部ではない Windows Vista を実行するリモート コンピュータでは、ビルトインの Administrator ユーザーのみがデータのバックアップとディスク管理操作を実行できます。この制限を克服するには、コンピュータをドメインに含めるか、コンピュータ上で UAC を無効にします(UAC はデフォルトで有効です)。*

Acronis セキュリティ グループおよびそのデフォルトのメンバの詳細については、「Acronis セキュリティ グループ『ページ参照 92』」をご参照ください。

2.13.7.4. Linux でのリモート接続の権限

Linux を実行するコンピュータへのリモート接続は、root ユーザーによる接続を含めて、Linux-PAM(Pluggable Authentication Modules for Linux)を使用して設定される認証ポリシーに従って確立されます。

認証ポリシーを正しく動作させるには、お使いの Linux ディストリビューション用の Linux-PAM の最新版をインストールしておくことをお勧めします。Linux-PAM の最新の安定したソース コードは、Linux-PAM ソース コードの Web ページから入手できます。

root ユーザーとしてのリモート接続

root ユーザーによるリモート接続は、Acronis Backup & Recovery 10 エージェント for Linux のインストール時に作成される /etc/pam.d/Acronisagent ファイルによって自動的に設定される、Acronis エージェントの認証ポリシーに従って確立されます。このファイルの内容は次のものです。

```
#%PAM-1.0
auth     required     pam_unix.so
auth     required     pam_rootok.so
account  required     pam_unix.so
```

root 以外のユーザーとしてのリモート接続

root ユーザーとしてシステムにアクセスすることは制限する必要があります。このため、root ユーザーは root 以外のログイン情報を使用したリモート管理を有効にする認証ポリシーを作成することができます。

そのようなポリシーの 2 つの例を次に示します。

***注意**: この結果、指定された root 以外のユーザーは、root ユーザーと同様にリモートからコンピュータに接続できるようになります。セキュリティ上のベスト プラクティスは、強力なパスワードを要求することなどによって、ユーザー アカウントが容易に盗用されないようにすることです。*

例 1

この認証ポリシーでは pam_succeed_if モジュールを使用し、カーネル バージョン 2.6 以降の Linux ディストリビューションで動作します。カーネル バージョン 2.4 で動作する認証ポリシーについては、この次の例をご参照ください。

root ユーザーとして、次の手順を実行します。

1. 次のコマンドを実行して、**Acronis_Trusted** グループ アカウントを作成します。
   ```
   groupadd Acronis_Trusted
   ```
2. リモート接続を許可する root 以外のユーザーの名前を**Acronis_Trusted** グループに追加します。たとえば、既存のユーザーの user_a をグループに追加するには、次のコマンドを実行します。
   ```
   usermod -G Acronis_Trusted user_a
   ```
3. 次の内容で、**/etc/pam.d/Acronisagent-trusted** ファイルを作成します。
   ```
   #%PAM-1.0
   auth       required   pam_unix.so
   auth       required   pam_succeed_if.so user ingroup Acronis_Trusted
   account    required   pam_unix.so
   ```

例 2

Red Hat Linux と VMware® ESX™ 3.5 Upgrade 2 を含む Linux ディストリビューションのカーネル バージョン 2.4 では、pam_succeed_if.so モジュールがサポートされていないため、上記の認証ポリシーが動作しない場合があります。

その場合は、次の認証ポリシーを使用します。

1. root ユーザーとして、**/etc/pam.d/Acronis_trusted_users** ファイルを作成します。
2. コンピュータの管理を許可する root 以外のユーザーの名前を、1 行に 1 ユーザーずつこのファイルに追加します。たとえば、user_a、user_b、および user_c を追加する場合は、このファイルに次の 3 行を追加します。
   ```
   user_a
   user_b
   user_c
   ```
   必要に応じて、このファイルに root ユーザーも追加します。

3. 次の内容で、**/etc/pam.d/Acronisagent-trusted** ファイルを作成します。

```
#%PAM-1.0
auth     required     pam_unix.so
auth     required     pam_listfile.so item=user sense=allow
file=/etc/pam.d/Acronis_trusted_users onerr=fail
account  required     pam_unix.so
```

2.13.7.5. Acronis セキュリティ グループ

Windows を実行しているコンピュータでは、Acronis セキュリティ グループは、リモートでコンピュータを管理し、Acronis Backup & Recovery 10 管理サーバー管理者として操作できるユーザーを特定します。

これらのグループは、Acronis Backup & Recovery 10 エージェントまたは Acronis Backup & Recovery 10 管理サーバーのインストール時に作成されます。インストールの際に、各グループに含まれるユーザーを指定できます。

Acronis Backup & Recovery 10 エージェント

Acronis Backup & Recovery 10 エージェント for Windows がコンピュータにインストールされるときに、**Acronis Remote Users** グループが作成(または更新)されます。

このグループのメンバであるユーザは、Acronis Backup & Recovery 10 管理コンソールを使用して、「管理対象コンピュータでのユーザーの権限『ページ参照 34』」で説明されている管理権限に従って、リモートからコンピュータを管理できます。

デフォルトでは、このグループには Administrators グループのすべてのメンバが含まれています。

Acronis Backup & Recovery 10 管理サーバー

Acronis Backup & Recovery 10 管理サーバーをコンピュータにインストールするときに、次の 2 つのグループが作成(または更新)されます。

Acronis Centralized Admins

このグループのメンバであるユーザーが管理サーバー管理者です。管理サーバー管理者は、Acronis Backup & Recovery 10 管理コンソールを使用して管理サーバーに接続できます。Acronis セキュリティ グループの内容とは関係なく、登録されたコンピュータの管理者権限のあるユーザーと同じ管理権限を持ちます。

管理サーバーに *リモート*で接続するには、管理サーバーの管理者は、Acronis Remote Users グループのメンバでもある必要があります。

Acronis Centralized Admins グループのメンバでなければ、Administrators グループのメンバであっても、どのユーザーも管理サーバーの管理者にはなれません。

デフォルトでは、このグループには Administrators グループのすべてのメンバが含まれています。

Acronis Remote Users

このグループのメンバであるユーザーは、Acronis Centralized Admins グループのメンバでもある場合に、Acronis Backup & Recovery 10 管理コンソールを使用して、リモートで管理サーバーに接続できます。

デフォルトでは、このグループには Administrators グループのすべてのメンバが含まれています。

ドメイン コントローラでの場合

コンピュータが Active Directory ドメインのドメイン コントローラである場合、Acronis セキュリティ グループの名前とデフォルトの内容が異なります。

- グループ名は、**Acronis Remote Users** と **Acronis Centralized Admins** ではなく、それぞれ *DCNAME* **$ Acronis Remote Users** と *DCNAME* **$ Acronis Centralized Admins** という名前になります。ここで、*DCNAME* はドメイン コントローラの NetBIOS 名です。それぞれのドル記号の両側には単一のスペースがあります。
- Administrators グループの全メンバの名前を具体的に含める代わりに、Administrators グループ自体を含めます。

ヒント: *適切なグループ名にするために、ドメイン コントローラへの Acronis コンポーネントのインストールは、ドメイン コントローラ自体のセットアップ終了後に行ってください。ドメイン コントローラのセットアップ前にコンポーネントをインストールした場合は、*DCNAME ***$ Acronis Remote Users*** *と* DCNAME ***$ Acronis Centralized Admins*** *グループを手動で作成し、新しく作成したグループに Acronis Remote Users と Acronis Centralized Admins のメンバを含めます。*

2.13.7.6. 管理サーバー管理者権限

通常、Acronis Backup & Recovery 10 管理サーバー管理者は、登録されたコンピュータの Acronis Managed Machine Service(Acronis サービスとも呼ばれます)に代わってそのコンピュータを操作し、サービスと同じ権限を所有します。

または、管理サーバー管理者は、バックアップ ポリシーの作成時に、登録されたコンピュータで集中管理用バックアップ計画を実行するユーザー アカウントを明示的に指定することもできます。この場合、このユーザー アカウントは、集中管理用ポリシーを配置するすべてのコンピュータ上に存在する必要があります。これは必ずしも効率的ではありません。

ユーザーを管理サーバー管理者にするには、管理サーバーがインストールされたコンピュータの Acronis Centralized Admins グループのメンバに加える必要があります。

2.13.7.7. ストレージ ノードでのユーザー権限

Acronis Backup & Recovery 10 ストレージ ノードでのユーザーの権限範囲は、ストレージ ノードがインストールされたコンピュータでのユーザーの権限によって異なります。

ストレージ ノードの Users グループのメンバなど、通常のユーザーは次の操作を実行できます。

- ストレージ ノードによって管理される任意の集中管理用格納域にアーカイブを作成する。
- ユーザーが所有するアーカイブを表示および管理する。

ストレージ ノードの Administrators グループのメンバであるユーザーは、さらに次の操作を実行できます。

- ストレージ ノードで管理される任意の集中管理用格納域内のアーカイブを表示および管理する。
- ユーザーが、Acronis Backup & Recovery 10 管理サーバー管理者でもある場合、ストレージ ノードで管理される集中管理用格納域を作成する。
- 「ストレージ ノードでの操作『ページ参照 364』」の「圧縮タスク スケジュールの変更」での説明に従って、圧縮タスクのスケジュールを変更する。

これらの追加権限を持つユーザーは、ストレージ ノード管理者とも呼ばれます。

ユーザー アカウントに関する推奨事項

ストレージ ノードで管理される集中管理用格納域にユーザーがアクセスできるようにするには、ネットワークからストレージ ノードにアクセスする権限をこれらのユーザーに与える必要があります。

すべてのユーザーは、通常、Domain Users グループのメンバであり、ストレージ ノードにアクセスできます。ユーザーのコンピュータと、ストレージ ノードのあるコンピュータの両方が、1 つの Active Directory ドメイン内にある場合、通常はこれ以上の手順を行う必要はありません。

そうでない場合、ストレージ ノードがインストールされているコンピュータにユーザー アカウントを作成する必要があります。ユーザーが所有するアーカイブだけにアクセスできるように、ストレージ ノードにアクセスするユーザーごとに個別のユーザー アカウントを作成することをお勧めします。

アカウントを作成するときには、次のガイドラインに従ってください。

- ストレージ ノード管理者の役割を与えるユーザーの場合、そのアカウントを **Administrators** グループに追加します。
- それ以外のユーザーの場合、そのアカウントを **Users** グループに追加します。

コンピュータ管理者の追加権限

あるコンピュータの Administrators グループのメンバであるユーザーは、ストレージ ノードでのアカウントの種類とは無関係に、管理対象の格納域内に*そのコンピュータから*作成されたすべてのアーカイブを表示および管理できます。

例

コンピュータ上の UserA と UserB という 2 人のユーザーが、このコンピュータからストレージ ノードで管理される集中管理用格納域へのバックアップを実行するとします。ストレージ ノードで、これらのユーザーにそれぞれ UserA_SN と UserB_SN という通常(非管理者)のアカウントを与えます。

通常、UserA は、UserA が作成した(および UserA_SN が所有する)アーカイブだけにアクセスでき、UserB は、UserB が作成した(および UserB_SN が所有する)アーカイブだけにアクセスできます。

ただし、UserA がそのコンピュータの Administrators グループのメンバである場合、UserA のストレージ ノードでのアカウントが通常のものだったとしても、このユーザーはさらに UserB が作成したアーカイブにそのコンピュータからアクセスできます。

2.13.7.8. Acronis サービスの権限

Windows では、ほとんどの Acronis コンポーネントはサービスとして動作します。サービスは、Administrator などのユーザー アカウントか、Local System などのシステム アカウントのどちらかのアカウントで実行します。

セキュリティ上のベスト プラクティスは、そのサービスで必要な最小限のユーザー権限だけを所有する専用のユーザー アカウントで各サービスを実行することです。

サービスとして実行するコンポーネントをインストールするときに、サービスを実行するアカウントとして、コンポーネントのデフォルト アカウントか既存のアカウントのどちらかを指定できます。

次の表は、各コンポーネントのサービスで必要なユーザー権限とユーザー アカウントのデフォルト名を示しています。

コンポーネント名	サービス名	必要なユーザー権限	デフォルトのユーザー アカウント
Acronis Backup & Recovery 10 エージェント	**Acronis Managed Machine Service**	サービスとしてログオン ファイルとディレクトリのバックアップ ローカルにログオン ファイルとディレクトリの復元 システムのシャットダウン	**Acronis Agent User**
Acronis Backup & Recovery 10 管理サーバー	**Acronis Management Server Service**	サービスとしてログオン	**AMS User**
Acronis Backup & Recovery 10 ストレージ ノード	**Acronis Storage Node Service**	サービスとしてログオン	**ASN User**

これらのユーザーは、値のクエリー、値の設定、サブキーの作成、サブキーの列挙、通知、削除、および読み取り制御の権限を持ち、レジストリキー HKEY_LOCAL_MACHINE¥SOFTWARE¥Acronis(Acronis レジストリ キーと呼ばれます)へのアクセスも認められています。

重要: *Acronis サービスのユーザー アカウントを指定できるのは、インストール時のみです。インストール後にアカウントを変更する必要がある場合は、対応するコンポーネントを再インストールして行います。サービス スナップインなどを使用して手動でアカウントを変更しないでください。*

さらに、システム アカウントで実行する 2 つの Acronis サービスがあります。

- **Acronis Scheduler2 Servic** は、Acronis コンポーネントのタスクのスケジューリングを提供します。このサービスは Local System アカウントで実行し、別のアカウントでは実行できません。
- **Acronis Remote Agent Service** は、Acronis コンポーネント間での接続を提供します。このサービスは Network Service アカウントで実行し、別のアカウントでは実行できません。

2.13.8. Acronis Backup & Recovery 10 コンポーネント間での通信

ここでは、Acronis Backup & Recovery 10 コンポーネントが、安全な認証と暗号化を使用して互いに通信する方法について説明します。

また、通信設定の構成、通信用のネットワーク ポートの選択、およびセキュリティ証明書の管理に関する情報についても説明します。

2.13.8.1. 安全な通信

Acronis Backup & Recovery 10 は、ローカル エリア ネットワーク内と境界ネットワーク(非武装地帯、DMZ とも呼ばれます)のコンポーネント間で転送されるデータを保護する機能を提供します。

Acronis Backup & Recovery 10 コンポーネント間の安全な通信を確保するメカニズムには、次の 2 つがあります。

- **安全な認証** - SSL(Secure Sockets Layer)プロトコルを使用することによって、接続の確立に必要な証明書を安全に転送します。
- **暗号化通信** - 転送されるデータを暗号化することによって、Acronis Backup & Recovery 10 エージェントと Acronis Backup & Recovery 10 ストレージ ノードとの間など、2 つのコンポーネント間で情報を安全に転送します。

安全な認証とデータ暗号化設定の設定手順については、「通信オプションの構成『ページ参照 97』」をご参照ください。

安全な認証に使用する SSL 証明書の管理方法については、「SSL 証明書『ページ参照 103』」をご参照ください。

注意: *Acronis True Image Echo ファミリのコンポーネントなど、以前の Acronis 製品のコンポーネントは、安全な認証でもデータ暗号化設定でも、Acronis Backup & Recovery 10 コンポーネントに接続できません。*

2.13.8.2. クライアントおよびサーバー アプリケーション

安全な通信プロセスには、次の 2 つの利害関係者が存在します。

- **クライアント アプリケーション**(クライアント) - 接続を確立しようとするアプリケーション。
- **サーバー アプリケーション**(サーバー) - クライアントが接続しようとするアプリケーションです。

たとえば、Acronis Backup & Recovery 10 管理コンソールがリモート コンピュータの Acronis Backup & Recovery 10 エージェントに接続している場合、前者がクライアントで後者がサーバーです。

Acronis コンポーネントは、次の表に示すように、クライアント アプリケーション、サーバー アプリケーション、またはその両方として機能できます。

コンポーネント名	クライアントとして機能	サーバーとして機能
Acronis Backup & Recovery 10 管理コンソール	はい	いいえ
Acronis Backup & Recovery 10 エージェント	はい	はい
Acronis Backup & Recovery 10 管理サーバー	はい	はい
Acronis Backup & Recovery 10 ストレージ ノード	はい	はい
Acronis PXE サーバー	いいえ	はい
Acronis Backup & Recovery 10 ブータブル エージェント	はい	はい

2.13.8.3. 通信設定の構成

Acronis 管理用テンプレートを使用することによって、1 つまたは複数のコンピュータにインストールされた Acronis Backup & Recovery 10 コンポーネントに対して、転送するデータを暗号化するかどうかなどの通信設定を構成できます。管理用テンプレートを読み込む方法については、「Acronis 管理用テンプレートの読み込み方法『ページ参照 102』」をご参照ください。

単一のコンピュータに適用する場合、管理用テンプレートはコンピュータ上のすべてのコンポーネントの通信設定を定義します。ドメインまたは組織単位に適用する場合、そのドメインまたは組織単位内にあるコンピュータ上のすべてのコンポーネントの通信設定を定義します。

通信設定を構成する手順は、次のとおりです。

1. **［スタート］**をクリックし、**［ファイル名を指定して実行］**をクリックして、**「gpedit.msc」**と入力します。
2. **［グループ ポリシー］**コンソールで**［コンピュータの構成］**を展開し、**［管理用テンプレート］**を展開して、［Acronis］をクリックします。
3. 右側の［Acronis］ペインで、構成する通信オプションをダブルクリックします。管理用テンプレートには、次のオプションが含まれます(各オプションについてはこのトピックで後述します)。
   - **リモート エージェント ポート**
   - **クライアント暗号化オプション**
   - **サーバー暗号化オプション**
4. 新しい通信設定を有効にするには、実行している Acronis コンポーネントをすべて再起動します(できれば Windows を再起動します)。再起動が不可能な場合は、必ず次の操作を行ってください。
   - Acronis Backup & Recovery 10 管理コンソールを実行している場合は、これを閉じて再度起動します。
   - Acronis Backup & Recovery 10 エージェント for Windows や Acronis Backup & Recovery 10 管理サーバーなどの他の Acronis コンポーネントを実行している場合は、Windows の **サービス** スナップインから対応するサービスを再起動します。

リモート エージェント ポート

コンポーネントが他の Acronis コンポーネントとの送受信を行うために使用するポートを指定します。

次のいずれかを選択します。

未指定

コンポーネントは、デフォルトの TCP ポート番号の 9876 を使用します。

有効

コンポーネントは、指定したポートを使用します。ポート番号を**［Server TCP Port］**に入力します。

無効

［未指定］と同じです。

ネットワーク ポートの詳細および Linux とブータブル環境でネットワーク ポートを指定する方法の詳細については、「ネットワーク ポート構成『ページ参照 101』」をご参照ください。

クライアント暗号化オプション

コンポーネントがクライアント アプリケーションとして動作する場合に転送されるデータを暗号化するかどうか、および自己署名 SSL 証明書を信頼するかどうかを指定します。

次のいずれかを選択します。

未指定

コンポーネントは、可能な場合は暗号化を使用し、自己署名 SSL 証明書を信頼するデフォルトの設定を使用します(次のオプションをご参照ください)。

有効

暗号化は有効になります。［**暗号化**］で、次のいずれかを選択します。

有効

データ転送は、サーバー アプリケーションで暗号化が有効になっている場合は暗号化され、無効になっている場合は暗号化されません。

無効

暗号化は無効になり、暗号化を必要とするサーバー アプリケーションとの接続は確立されません。

必須

データ転送は、サーバー アプリケーションで暗号化が有効になっている場合のみ実行され、暗号化されます(「サーバー暗号化オプション」をご参照ください)。

認証パラメータ

［**Trust self-signed certificates**］チェックボックスをオンにすると、クライアントは Acronis Backup & Recovery 10 コンポーネントのインストール中に作成される証明書などの自己署名 SSL 証明書を使用するサーバー アプリケーションに接続できます(「SSL 証明書『ページ参照 103』」をご参照ください)。

このチェックボックスは、環境に公開キー基盤(PKI)がある場合を除き、オンにしておく必要があります。

［**Use Agent Certificate Authentication**］で、次のいずれかを選択します。

［**Do not use**］

SSL 証明書の使用は無効になります。SSL 証明書の使用を必要とするサーバー アプリケーションとの接続は確立されません。

［**Use if possible**］

SSL 証明書の使用は有効です。クライアントは、サーバー アプリケーションで SSL 証明書の使用が有効になっている場合はその証明書を使用し、無効になっている場合は使用しません。

［**Always use**］

SSL 証明書の使用は有効です。接続は、サーバー アプリケーションで SSL 証明書の使用が有効になっている場合のみ確立されます。

無効

［**未指定**］と同じです。

サーバー暗号化オプション

コンポーネントがサーバー アプリケーションとして動作する場合に、転送されるデータを暗号化するかどうかを指定します。

次のいずれかを選択します。

未指定

コンポーネントは、可能な場合は暗号化を使用するデフォルトの設定を使用します(次のオプションをご参照ください)。

有効

暗号化が有効になります。［**暗号化**］で、次のいずれかを選択します。

有効

データ転送は、クライアント アプリケーションで暗号化が有効になっている場合は暗号化され、無効になっている場合は暗号化されません。

無効

暗号化は無効になり、暗号化を必要とするクライアント アプリケーションとの接続は確立されません。

必須

データ転送は、クライアント アプリケーションで暗号化が有効になっている場合のみ実行され、暗号化されます(「クライアント暗号化オプション」をご参照ください)。

認証パラメータ

［**Use Agent Certificate Authentication**］で、次のいずれかを選択します。

使用しない

SSL 証明書の使用は無効になります。SSL 証明書の使用を必要とするクライアント アプリケーションとの接続は確立されません。

Use if possible

SSL 証明書の使用は有効です。サーバーは、クライアント アプリケーションで SSL 証明書の使用が有効になっている場合はその証明書を使用し、無効になっている場合は使用しません。

Always use

SSL 証明書の使用は有効です。接続は、クライアント アプリケーションで SSL 証明書の使用が有効になっている場合のみ確立されます。

無効

［**未指定**］と同じです。

2.13.8.4. ネットワーク ポート構成

Acronis Backup & Recovery 10 コンポーネントは、デフォルトで 9876/TCP ネットワーク通信ポートを使用します。サーバーはこのポートで着信接続をリッスンします。このポートは、デフォルトで Acronis クライアントでも使用されます。Windows ファイアウォール以外のファイアウォールを使用している場合は、コンポーネントのインストール時に、ポートが開いていることを確認するか、手動でポートを開くように求められます。

インストール後、必要な値に合わせて、またはセキュリティの目的で、いつでもポートを変更できます。この操作には、Acronis リモート エージェント(Windows の場合)または Acronis_agent(Linux の場合)サービスを再起動する必要があります。

サーバー側でポートを変更した後、<Server-IP>:<port> または <Server-hostname>:<port> の URL 表記を使用して、サーバーに接続します。

注意: *NAT(Network Address Translation; ネットワーク アドレス変換)を使用する場合、ポート マッピングを設定してポートを構成することもできます。*

オペレーティング システムでのポートの構成

Windows

ポートの番号を変更できるようにするには、「通信設定の構成『ページ参照 97』」の「リモート エージェント ポート」の説明に従って、Acronis に用意されている管理用テンプレートを読み込んで構成します。

Linux

/etc/Acronis/Policies/Agent.config ファイルでポートを指定します。Acronis_agent デーモンを再起動します。

ブータブル環境でのポートの構成

Acronis ブータブル メディアを作成する場合、Acronis Backup & Recovery 10 ブータブル エージェントで使用されるネットワーク ポートをあらかじめ構成するオプションがあります。次のいずれかを選択できます。

- デフォルトのポート(9876)
- 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、エージェントはデフォルトのポート番号を使用します。

2.13.8.5. Acronis 管理用テンプレートの適用方法

Acronis が提供する管理用テンプレートによって、暗号化された通信設定を含むセキュリティに関連する機能を調整できます。Microsoft グループ ポリシーのメカニズムを介して、単一のコンピュータまたはドメインにテンプレートのポリシーの設定を適用できます。

Acronis 管理用テンプレートを読み込む手順は、次のとおりです。

1. Windows グループ ポリシー オブジェクト エディタ(%windir%¥system32¥gpedit.msc)を実行します。
2. 編集するグループ ポリシー オブジェクト(GPO)を開きます。
3. **［コンピュータの構成］**を展開します。
4. **［管理用テンプレート］**を右クリックします。
5. **［テンプレートの追加と削除］**をクリックします。
6. **［追加］**をクリックします。
7. Acronis 管理用テンプレート(¥Program files¥Common Files¥Acronis¥Agent¥Acronis_agent.adm または ¥Program files¥Acronis¥BackupAndRecovery¥Acronis_agent.adm)を選択し、**［開く］**をクリックします。

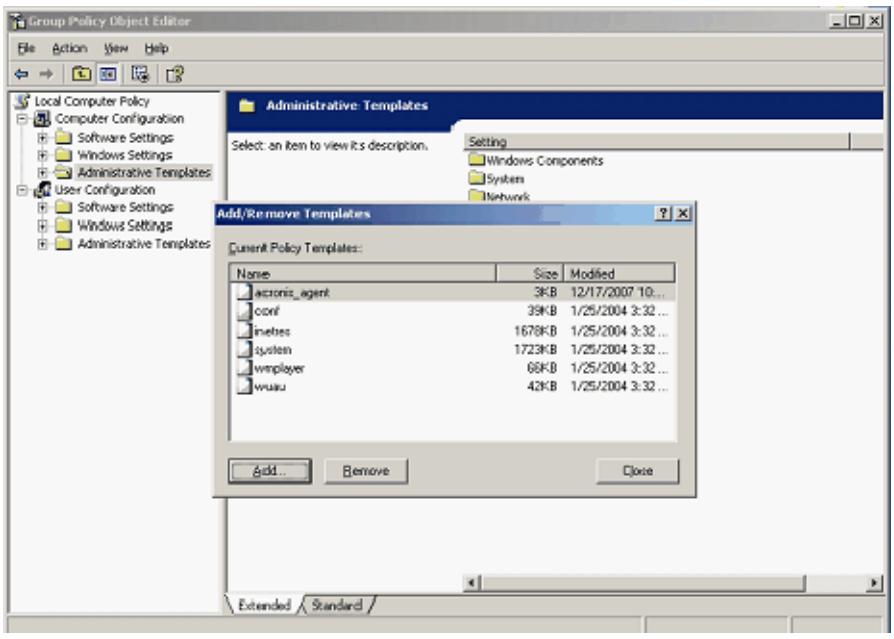
テンプレートが読み込まれたら、それを開いて必要な設定を編集できます。テンプレートの読み込み、または設定の編集が完了したら、設定したコンポーネントまたはそのサービスの一部を再起動する必要があります。

Windows GPO エディタの詳細については、次のページをご参照ください。

http://msdn2.microsoft.com/en-us/library/aa374163.aspx

グループ ポリシーの詳細については、次のページをご参照ください。

http://msdn2.microsoft.com/en-us/library/aa374177.aspx



2.13.8.6. SSL 証明書

Acronis Backup & Recovery 10 コンポーネントは、安全な認証に SSL(Secure Sockets Layer)証明書を使用します。

コンポーネントの SSL 証明書は、次の 2 つの種類のいずれかになります。

- **自己署名証明書** - Acronis コンポーネントのインストール時に自動的に生成された証明書など。
- **非自己署名証明書** - サードパーティの CA(Certificate Authority; 認証局) (たとえば、VeriSign® や Thawte™ などのパブリック CA)、または組織の CA が発行する証明書など。

証明書パス

コンピュータにインストールされたすべての Acronis コンポーネントは、サーバー アプリケーションとして機能する場合、サーバー証明書と呼ばれる SSL 証明書を使用します。

Windows では、証明書パスとサーバー証明書のファイル名は、レジストリ キー HKEY_LOCAL_MACHINE¥SOFTWARE¥Acronis¥Encryption¥Server で指定されます。デフォルトのパスは %SystemDrive%¥Program Files¥Common Files¥Acronis¥Agent です。

信頼性を確保するため、証明書は「証明書 (ローカル コンピュータ) ¥Acronis Trusted Certificates」にある Windows 証明書ストアに保存されます。

自己署名証明書の場合、証明書の拇印(フィンガープリントやハッシュとも呼ばれます)が、今後のホスト識別に使用されます。クライアントが以前に自己署名証明書を使用してサーバーに接続しており、再度接続を確立しようとした場合、サーバーは、証明書の拇印が以前に使用されたものと同じであるかどうかを調べます。

ローカル コンピュータの証明書の一覧が［**証明書**］コンソールに表示されない場合は、次の手順を使用できます。

コンピュータの証明書の一覧を開く手順は、次のとおりです。

1. ［**スタート**］をクリックし、［**ファイル名を指定して実行**］をクリックして、「**mmc**」と入力します。
2. コンソールの［**ファイル**］メニューで、［**スナップインの追加と削除**］をクリックします。
3. ［**スナップインの追加と削除**］ダイアログ ボックスで［**追加**］をクリックします。
4. ［**スタンドアロン スナップインの追加**］ダイアログ ボックスで［**証明書**］をダブルクリックします。
5. ［**コンピュータ アカウント**］をクリックして、［**次へ**］をクリックします。
6. ［**ローカル コンピュータ**］をクリックして、［**完了**］をクリックします。

   ***ヒント**: または、リモート コンピュータの証明書の一覧を管理できます。これを行うには、［**別のコンピュータ**］をクリックし、リモート コンピュータの名前を入力します。*

7. ［**閉じる**］をクリックして［**スタンドアロン スナップインの追加**］ダイアログ ボックスを閉じ、［**OK**］をクリックして［**スナップインの追加と削除**］ダイアログ ボックスを閉じます。

自己署名証明書

Windows を実行しているコンピュータで、証明書の場所にサーバー証明書がない場合、Acronis Backup & Recovery 10 管理コンソール以外のすべての Acronis コンポーネントのインストール中に、自己署名サーバー証明書が自動的に生成され、インストールされます。

自己署名証明書の生成後にコンピュータの名前を変更した場合、証明書は使用できず、新しい証明書を生成する必要があります。

新しい自己署名証明書を生成する手順は、次のとおりです。

1. Administrators グループのメンバとしてログオンします。
2. **[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。
3. 次のコマンドを実行します(引用符に注意してください)。

   ```
   "%CommonProgramFiles%¥Acronis¥Utils¥acroniscert" --reinstall
   ```

4. Windows を再起動するか、実行している Acronis サービスを再起動します。

非自己署名証明書

自己署名証明書に代わる方法として、Acronis 証明書コマンドライン ユーティリティを使用することによって、信頼されたサードパーティ証明書、または組織の CA が作成した証明書を使用するオプションがあります。

サードパーティ証明書をインストールする手順は、次のとおりです。

1. **[スタート]** をクリックし、**[ファイル名を指定して実行]** をクリックして、**「certmgr.msc」** と入力します。
2. **[証明書]** コンソールで、インストールする証明書の名前をダブルクリックします。
3. **[詳細]** タブのフィールドの一覧で、**[拇印]** をクリックします。
4. 証明書の拇印(**20 99 00 b6 3d 95 57 28 14 0c d1 36 22 d8 c6 87 a4 eb 00 85** のような文字列)と呼ばれるフィールドの値を選択してコピーします。
5. **[スタート]** メニューをクリックし、**[ファイル名を指定して実行]** をクリックして、**[名前]** ボックスで次のように入力します。

   ```
   "%CommonProgramFiles%¥Acronis¥Utils¥acroniscert.exe" --install "20 99 00 b6 3d 95 57 28 14 0c d1 36 22 d8 c6 87 a4 eb 00 85"
   ```

   (引用符に注意し、ここに示したサンプルの拇印を、使用する証明書の拇印に置き換えてください)

3. オプション

ここでは、グラフィカル ユーザー インターフェイスを使用して構成できる、Acronis Backup & Recovery 10 のオプションについて説明します。このセクションの内容は、Acronis Backup & Recovery 10 のスタンドアロンと Advanced Edition の両方に対して適用できます。

3.1. コンソール オプション

コンソール オプションでは、Acronis Backup & Recovery 10 のグラフィカル ユーザー インターフェイスに情報を表示する方法を定義します。

コンソール オプションにアクセスするには、トップ メニューから **[オプション] → [コンソール オプション]** を選択します。

3.1.1. スタートアップ ページ

このオプションでは、コンソールを管理対象のコンピュータまたは管理サーバーに接続する際に **[ようこそ]** 画面を表示するか、または **[ダッシュボード]** を表示するかを定義します。

デフォルトの設定 - **[ようこそ]** 画面

選択するには、**[コンソールをコンピュータに接続した際にダッシュボード ビューを表示する]** チェックボックスをオンまたはオフにします。

このオプションは、**[ようこそ] 画面でも設定できます。[ようこそ]** 画面で **[起動時に現在のビューの代わりにダッシュボードを表示する] チェックボックスをオンにすると、上記の設定はこれに従って更新されます。**

3.1.2. ポップアップ メッセージ

ユーザーによる操作が必要なタスクの通知

このオプションは、コンソールが管理対象のコンピュータまたは管理サーバーに接続されている場合に有効です。

このオプションでは、ユーザーによる操作を必要とする 1 つ以上のタスクがある場合にポップアップウィンドウを表示するかどうかを定義します。このウィンドウによって、同じ場所のすべてのタスクに対して再起動の確認やディスク領域を解放した後の再試行などの設定を指定できます。少なくとも 1 つのタスクでユーザーの操作が必要になるまで、管理対象のコンピュータの **[ダッシュボード]** からいつでもこのウィンドウを開くことができます。または、**[タスク]** ビューでタスクの実行状態を確認し、それぞれのタスクに対する設定を **[情報]** ペインで指定することもできます。

デフォルトの設定 - **オン**

選択するには、**[手動操作が必要なことを通知するメッセージ ウィンドウをポップアップ表示する]** チェックボックスをオンまたはオフにします。

タスクの実行結果の通知

このオプションは、コンソールが管理対象のコンピュータに接続されている場合にのみ有効です。

このオプションでは、タスクの実行結果に関するポップアップ メッセージ(正常終了、失敗、または警告を伴った正常終了)を表示するかどうかを定義します。ポップアップ メッセージの表示を無効にした場合、タスクの実行状態と結果は、［**タスク**］ビューで確認できます。

デフォルトの設定 - すべての結果に対して**オン**

それぞれの結果に対して個々に正常終了、失敗、または警告を伴った正常終了を設定するには、それぞれのチェックボックスをオンまたはオフにします。

3.1.3. 時刻ベースのアラート

前回のバックアップ

このオプションは、コンソールが管理対象のコンピュータ『ページ参照 426』または管理サーバー『ページ参照 429』に接続されている場合に有効です。

このオプションでは、管理対象のコンピュータで一定期間バックアップが実行されなかった場合に警告するかどうかを定義します。ビジネスにとって問題と見なす期間を設定できます。

デフォルトの設定 - 前回コンピュータで成功したバックアップが完了してから **5 日**以上経過している場合に警告します。

アラートは、［**ダッシュボード**］の［**アラート**］セクションに表示されます。コンソールが管理サーバーに接続されている場合、この設定は各コンピュータの［**前回のバックアップ**］列の値のカラー スキームを制御します。

前回の接続

このオプションは、コンソールが管理サーバーまたは登録済みのコンピュータ『ページ参照 428』に接続されている場合に有効です。

このオプションでは、登録済みのコンピュータと管理サーバーの間で一定時間接続が確立されなかった場合に、そのコンピュータへのネットワーク接続の失敗などによって、コンピュータが集中管理されていない可能性があることを警告するかどうかを定義します。問題であると見なす時間の長さを設定できます。

デフォルトの設定 - 前回コンピュータが管理サーバーに接続してから **5 日**以上経過している場合に警告します。

アラートは、［**ダッシュボード**］の［**アラート**］セクションに表示されます。コンソールが管理サーバーに接続されている場合、この設定は各コンピュータの［**前回の接続**］列の値のカラー スキームを制御します。

3.1.4. タスクの数

このオプションは、コンソールが管理サーバーに接続されている場合にのみ有効です。

このオプションでは、［**タスク**］ビューに 1 回に表示するタスクの数を定義します。［**タスク**］ビューにあるフィルタを使用して、表示するタスクの数を制限することもできます。

デフォルトの設定 - **400**。設定可能な範囲は、**20 ～ 500** です。

選択するには、［**タスクの数**］ドロップ ダウン メニューから目的の値を選択します。

3.1.5. フォント

このオプションは、コンソールが管理対象のコンピュータまたは管理サーバーに接続されている場合に有効です。

このオプションでは、Acronis Backup & Recovery 10 のグラフィカル ユーザー インターフェイスで使用するフォントを定義します。［**メニュー**］の設定は、ドロップ ダウン メニューとコンテキスト メニューに影響します。［**アプリケーション**］の設定は、その他の GUI 要素に影響します。

デフォルトの設定 - ［**<システム デフォルト>**］フォント(メニューとアプリケーションの両方のインターフェイス項目に対して)

選択するには、それぞれのコンボボックスからフォントを選択し、フォントのプロパティを設定します。右のボタンをクリックすると、フォントの外観をプレビューできます。

3.2. 管理サーバー オプション

管理サーバー オプションによって、Acronis Backup & Recovery 10 管理サーバーの動作を調整できます。

管理サーバー オプションにアクセスするには、コンソールを管理サーバーに接続し、トップ メニューから［**オプション**］→［**管理サーバー オプション**］を選択します。

3.2.1. ログ レベル

このオプションでは、管理サーバーが登録済みのコンピュータから専用データベースに保存されている集中管理のログにイベントを収集する必要があるかどうかを定義します。このログは、［**ログ**］ビューで使用できます。このオプションでは、すべてのイベントを収集するか、収集するイベントの種類を選択できます。イベントの収集を完全に無効にすると、集中管理のログには管理サーバー自身のログのみが保存されます。

デフォルトの設定 - **［すべてのイベント］の［ログを収集する］。**

［ログに記録するイベントの種類］コンボボックスを使用して、収集するイベントの種類を指定します。

- **［すべてのイベント］**– 管理サーバーに登録されているすべてのコンピュータで発生したすべてのイベント(情報、警告、およびエラー)が集中管理のログに記録されます。
- **［エラーと警告］** - 警告とエラーが集中管理のログに記録されます。
- **［エラーのみ］** - エラーのみが集中管理のログに記録されます。

イベントの収集を無効にするには、**［ログを収集する］**チェックボックスをオフにします。

3.2.2. イベント トレース

管理サーバーでは、管理サーバー自体のログの他に、Windows のアプリケーション イベント ログにもイベントを記録するように設定できます。

また、簡易ネットワーク管理プロトコル(SNMP)オブジェクトを、指定した SNMP マネージャに送信するように設定できます。

3.2.2.1. Windows イベント ログ

このオプションでは、管理サーバーが、自身のイベントを 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、または **[コントロール パネル] → [管理ツール] → [イベント ビューア]** を選択します。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。

デフォルトの設定 - **オフ**

このオプションを有効にするには、**［イベントをログに記録する］**チェックボックスをオンにします。

［ログに記録するイベントの種類］チェックボックスを使用して、Windows のアプリケーション イベント ログに記録するイベントにフィルタを設定します。

- **［すべてのイベント］** - すべてのイベント(情報、警告、およびエラー)
- **［エラーと警告］**
- **［エラーのみ］**

このオプションを無効にするには、**［イベントをログに記録する］**チェックボックスをオフにします。

3.2.2.2. SNMP 通知

このオプションでは、管理サーバーが、指定した簡易ネットワーク管理プロトコル(SNMP)マネージャに自身のイベントを送信する必要があるかどうかを定義します。送信するイベントの種類を選択できます。

Acronis Backup & Recovery 10 は、次の簡易ネットワーク管理プロトコル(SNMP)オブジェクトを SNMP 管理アプリケーションに送信します。

1.3.6.1.4.1.24769.100.200.1.0 - イベントの種類を特定する文字列(情報、警告、エラー)

1.3.6.1.4.1.24769.100.200.2.0 - イベントの説明テキストを含む文字列(Acronis Backup & Recovery 10 によってログに記録されるメッセージと同じです)。

デフォルトの設定 - **オフ**

SNMP メッセージの送信を設定する手順は、次のとおりです。

1. **[SNMP サーバーにメッセージを送信する]** チェックボックスをオンにします。
2. 次のように適切なオプションを指定します。
   - **[送信するイベントの種類]** - **[すべてのイベント]**、**[エラーと警告]**、または **[エラーのみ]** のいずれかから送信するイベントの種類を選択します。
   - **[サーバー名/IP]** - メッセージの送信先となる SNMP 管理アプリケーションを実行するホストの名前または IP アドレスを入力します。
   - **[コミュニティ]** - SNMP 管理アプリケーションを実行するホストと送信元コンピュータの両方が所属する SNMP コミュニティの名前を入力します。一般的なコミュニティは "public" です。

SNMP メッセージの送信を無効にするには、**[SNMP サーバーにメッセージを送信する]** チェックボックスをオフにします。

メッセージは、UDP 経由で送信されます。

3.3. コンピュータ オプション

管理対象のコンピュータで動作するすべての Acronis Backup & Recovery 10 エージェントの一般的な動作はコンピュータ オプションによって定義されるため、これらのオプションはコンピュータ固有と見なすことができます。

コンピュータ オプションにアクセスするには、管理対象のコンピュータにコンソールを接続し、トップ メニューから **[オプション]** → **[コンピュータ オプション]** を選択します。

3.3.1. コンピュータの管理

このオプションでは、コンピュータを Acronis Backup & Recovery 10 管理サーバーによって集中管理する必要があるかどうかを定義します。

Acronis Backup & Recovery 10 エージェントをインストールする際に、管理サーバーにコンピュータを登録することができます。コンピュータが登録されていない場合、ここで［**集中管理**］を選択すると、登録『ページ参照 429』が開始されます。または、コンピュータをサーバー側の管理サーバーに追加することもできます。3 つの登録方法すべてにおいて、サーバーの管理者権限が必要です。

登録済みのコンピュータで［**スタンドアロン管理**］を選択すると、サーバーとコンピュータ間の通信が停止されます。管理サーバーから一定期間コンピュータに接続できなかったというアラートが通知されると、管理者はサーバーからそのコンピュータを削除するか、または再度登録することができます。

デフォルトの設定 - ［**スタンドアロン管理**］

コンピュータに集中管理を設定する手順は、次のとおりです。

1. ［**集中管理**］を選択します。
2. ［**管理サーバー(IP/名前)**］を指定します。
3. 管理サーバーの管理者のユーザー名とパスワードの入力を求めるプロンプトに対して、それらを指定します。入力したデータが正しい場合、［**OK**］をクリックすることが可能になり、コンピュータが管理サーバーに登録されます。正しくない場合は、データを再入力するか、または［**スタンドアロン管理**］を選択します。

集中管理を無効にする場合は、［**スタンドアロン管理**］を選択します。

3.3.2. イベント トレース

管理対象のコンピュータで動作するエージェントによって生成されたイベントを Windows のアプリケーション イベント ログに表示したり、指定した SNMP マネージャに送信したりすることができます。イベント トレース オプションをここ以外で変更していなければ、ローカルのすべてのバックアップ計画およびこのコンピュータ上で作成されるすべてのタスクに対してこの設定が有効になります。

ここでの設定は、バックアップ中または復元中に発生するイベントについてのみ、デフォルトのバックアップ オプションおよび復元オプション『ページ参照 113』で、上書きすることができます。この場合、ここでの設定は、アーカイブのベリファイまたはクリーンアップなどの、バックアップと復元以外の操作に対して有効になります。

デフォルトのバックアップ オプションと復元オプションの設定は、バックアップ計画や復元タスクを作成するときに、さらに上書きすることができます。この場合、取得する設定は、個別の計画または個別のタスクのものになります。

3.3.2.1. 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。

このオプションは、ブータブル メディアから起動した場合には使用できません。

このオプションでは、管理対象のコンピュータで動作するエージェントが、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、または［**コントロール パネル**］→［**管理ツール**］→［**イベント ビューア**］を選択します。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。

ここでの設定は、バックアップ中または復元中に発生するイベントについてのみ、デフォルトのバックアップ オプションおよび復元オプション『ページ参照 113』で、上書きすることができます。この場合、ここでの設定は、アーカイブのベリファイまたはクリーンアップなどの、バックアップと復元以外の処理に対して有効になります。

デフォルトのバックアップ オプションと復元オプションの設定は、バックアップ計画や復元タスクを作成するときに、さらに上書きすることができます。この場合、取得する設定は、個別の計画または個別のタスクのものになります。

デフォルトの設定 - **オフ**

このオプションを有効にするには、［**イベントをログに記録する**］チェックボックスをオンにします。

［**ログに記録するイベントの種類**］チェックボックスを使用して、Windows のアプリケーション イベント ログに記録するイベントにフィルタを設定します。

- ［**すべてのイベント**］– すべてのイベント(情報、警告、およびエラー)
- ［**エラーと警告**］
- ［**エラーのみ**］

このオプションを無効にするには、［**イベントをログに記録する**］チェックボックスをオフにします。

3.3.2.2. SNMP 通知

このオプションは、Windows および Linux オペレーティング システムの両方で有効です。

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は使用できません。

このオプションでは、管理対象のコンピュータで動作するエージェントが、イベントを指定した簡易ネットワーク管理プロトコル(SNMP)マネージャに送信する必要があるかどうかを定義します。送信するイベントの種類を選択できます。

ここでの設定は、バックアップ中または復元中に発生するイベントについてのみ、デフォルトのバックアップ オプションおよび復元オプション『ページ参照 113』で、上書きすることができます。この場合、ここでの設定は、アーカイブのベリファイまたはクリーンアップなどの、バックアップと復元以外の処理に対して有効になります。

デフォルトのバックアップ オプションと復元オプションの設定は、バックアップ計画や復元タスクを作成するときに、さらに上書きすることができます。この場合、取得する設定は、計画に固有またはタスクに固有のものになります。

Acronis Backup & Recovery 10 は、次の簡易ネットワーク管理プロトコル(SNMP)オブジェクトを SNMP 管理アプリケーションに送信します。

1.3.6.1.4.1.24769.100.200.1.0 - イベントの種類を特定する文字列(情報、警告、エラー)

1.3.6.1.4.1.24769.100.200.2.0 - イベントの説明テキストを含む文字列(Acronis Backup & Recovery 10 によってログに記録されるメッセージと同じです)。

デフォルトの設定 - **オフ**

SNMP メッセージの送信を設定する手順は、次のとおりです。

1. **［SNMP サーバーにメッセージを送信する］**チェックボックスをオンにします。
2. 次のように適切なオプションを指定します。
   - **［送信するイベントの種類］**- **［すべてのイベント］**、**［エラーと警告］**、または **［エラーのみ］**のいずれかから送信するイベントの種類を選択します。
   - **［サーバー名/IP］**- メッセージの送信先となる SNMP 管理アプリケーションを実行するホストの名前または IP アドレスを入力します。
   - **［コミュニティ］**- SNMP 管理アプリケーションを実行するホストと送信元コンピュータの両方が所属する SNMP コミュニティの名前を入力します。一般的なコミュニティは "public" です。

SNMP メッセージの送信を無効にするには、**［SNMP サーバーにメッセージを送信する］**チェックボックスをオフにします。

メッセージは、UDP 経由で送信されます。

次のセクションには、受信コンピュータの SNMP サービスの設定『ページ参照 112』に関する追加情報が含まれます。

3.3.2.3. 受信コンピュータでの SNMP サービスの設定

Windows

Windows を実行するコンピュータに SNMP サービスをインストールする手順は、次のとおりです。

1. **［スタート］→［コントロール パネル］→［プログラムの追加と削除］→［Windows コンポーネントの追加と削除］**を選択します。
2. **［管理とモニタ ツール］**を選択します。
3. **［詳細］**をクリックします。
4. **［簡易ネットワーク管理プロトコル(SNMP)］**チェックボックスをオンにします。
5. **［OK］**をクリックします。

オペレーティング システムのインストール ディスクにある lmmib2.dll が必要になる場合があります。

Linux

Linux を実行するコンピュータで SNMP メッセージを受け取るには、net-snmp(RHEL と SUSE 用)または snmpd(Debian 用)パッケージをインストールする必要があります。

SNMP は、**snmpconf** コマンドを使用して設定できます。デフォルトのコンフィギュレーション ファイルは、/etc/snmp ディレクトリにあります。

- /etc/snmp/snmpd.conf - Net-SNMP SNMP エージェントのコンフィギュレーション ファイル
- /etc/snmp/snmptrapd.conf - Net-SNMP トラップ デーモンのコンフィギュレーション ファイル

3.4. デフォルトのバックアップおよび復元オプション

3.4.1. デフォルトのバックアップ オプション

各 Acronis エージェントには、独自のデフォルトのバックアップ オプションがあります。エージェントがインストールされると、デフォルトのオプションは、ドキュメントで**デフォルトの設定**と呼ばれる、あらかじめ定義された値になります。バックアップ計画を作成する場合は、デフォルトのオプションを使用するか、この計画のみで固有なカスタムの値でデフォルトのオプションを上書きできます。

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自体をカスタマイズすることもできます。新しい値は、後でこのコンピュータで作成するすべてのバックアップ計画に対してデフォルトで使用されます。

デフォルトのバックアップ オプションを表示して変更するには、コンソールを管理対象のコンピュータに接続し、上部のメニューから［**オプション**］→［**デフォルトのバックアップと復元のオプション**］→［**デフォルトのバックアップ オプション**］を選択します。

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項目によって異なります。

- エージェントが動作する環境(Windows、Linux、ブータブル メディア)
- バックアップするデータの種類(ディスク、ファイル)
- バックアップの保存先(ネットワーク上の場所またはローカル ディスク)
- バックアップ スキーム(今すぐバックアップ、またはスケジューラの使用)

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。

	エージェント for Windows		エージェント for Linux		ブータブル メディア (Linux ベースまたは PE ベース)	
	ディスク バック アップ	ファイル バック アップ	ディスク バック アップ	ファイル バック アップ	ディスク バック アップ	ファイル バック アップ
アーカイブの保護『ページ参照 116』 (パスワードと暗号化)	+	+	+	+	+	+
バックアップから除外するファイル『ページ参照 117』	+	+	+	+	+	+
バックアップの前後に実行するコマンド『ページ参照 118』	+	+	+	+	PE のみ	PE のみ
データ取り込みの前後に実行するコマンド『ページ参照 120』	+	+	+	+	-	-
マルチボリューム スナップショット『ページ参照 123』	+	+	-	-	-	-
ファイル レベル バックアップのスナップショット『ページ参照 123』	-	+	-	+	-	-
VSS の使用『ページ参照 124』	+	+	-	-	-	-
圧縮レベル『ページ参照 125』	+	+	+	+	+	+
バックアップのパフォーマンス:						
バックアップの優先度『ページ参照 125』	+	+	+	+	-	-
HDD 書き込み速度『ページ参照 126』	保存先: HDD	保存先: HDD	保存先: HDD	保存先: HDD	保存先: HDD	保存先: HDD
ネットワークの接続速度『ページ参照 126』	保存先: ネットワーク共有	保存先: ネットワーク共有	保存先: ネットワーク共有	保存先: ネットワーク共有	保存先: ネットワーク共有	保存先: ネットワーク共有
高速の増分/差分バックアップ『ページ参照 131』	+	-	+	-	+	-
バックアップの分割『ページ参照 131』	+	+	+	+	+	+

ファイル レベルのセキュリティ『ページ参照 132』:						
アーカイブにファイルのセキュリティ設定を保存する	-	+	-	-	-	-
暗号化されたファイルを復号化された状態でアーカイブに格納する	-	+	-	-	-	-
メディア コンポーネント『ページ参照 133』	保存先: リムーバブル メディア	保存先: リムーバブル メディア	保存先: リムーバブル メディア	保存先: リムーバブル メディア	-	-
エラーの処理『ページ参照 134』:						
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)	+	+	+	+	+	+
エラーが発生した場合は再試行する	+	+	+	+	+	+
不良セクタを無視する	+	+	+	+	+	+
保存先の二重化『ページ参照 134』	保存先: ローカル	保存先: ローカル	保存先: ローカル	保存先: ローカル	-	-
タスクの開始条件『ページ参照 135』	+	+	+	+	-	-
タスク失敗時の処理『ページ参照 137』	+	+	+	+	-	-
テープ サポート『ページ参照 138』	保存先: テープ ライブラリ上の管理対象の格納域	保存先: テープ ライブラリ上の管理対象の格納域	保存先: テープ ライブラリ上の管理対象の格納域	保存先: テープ ライブラリ上の管理対象の格納域	保存先: テープ ライブラリ上の管理対象の格納域	保存先: テープ ライブラリ上の管理対象の格納域
その他の設定『ページ参照 139』:						
ユーザーの確認を求めることなくテープのデータを上書きする	保存先: テープ	保存先: テープ	保存先: テープ	保存先: テープ	保存先: テープ	保存先: テープ
バックアップ終了後にメディアをマウント解除する	保存先: リムーバブル メディア	保存先: リムーバブル メディア	保存先: リムーバブル メディア	保存先: リムーバブル メディア	保存先: リムーバブル メディア	保存先: リムーバブル メディア
リムーバブル メディアにバックアップ アーカイブを作成する場合に、最初のメディアの挿入を求める	保存先: リムーバブル メディア	保存先: リムーバブル メディア	保存先: リムーバブル メディア	保存先: リムーバブル メディア	保存先: リムーバブル メディア	保存先: リムーバブル メディア

作成後にバックアップをベリファイする	-	-	-	-	+	+
アーカイブ ビットをリセットする	-	+	-	-	-	+
バックアップの後に再起動する	-	-	-	-	+	+
統合バックアップから完全バックアップを作成する	+	+	+	+	+	+
通知:						
電子メール『ページ参照 127』	+	+	+	+	-	-
ポップアップウィンドウ『ページ参照 128』	+	+	+	+	-	-
イベント トレース:						
Windows イベント ログ『ページ参照 129』	+	+	-	-	-	-
SNMP『ページ参照 130』	+	+	+	+	-	-

3.4.1.1. アーカイブの保護

このオプションは、Windows と Linux オペレーティング システム、およびブータブル メディアで有効です。

このオプションは、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に対して有効です。

デフォルトの設定 - **オフ**

権限のないアクセスからアーカイブを保護する手順は、次のとおりです。

1. **［アーカイブにパスワードを設定する］**チェックボックスをオンにします。
2. **［パスワードの入力］フィールドにパスワードを入力します。**
3. **［パスワードの確認入力］**フィールドにパスワードを再入力します。
4. 次のいずれかを選択します。
   - **［暗号化しない］** – アーカイブはパスワードのみで保護されます。
   - **［AES 128］** – アーカイブは、128 ビットのキーの AES(Advanced Standard Encryption)アルゴリズムを使用して暗号化されます。
   - **［AES 192］** – アーカイブは、192 ビットのキーの AES アルゴリズムを使用して暗号化されます。
   - **［AES 256］** – アーカイブは、256 ビットのキーの AES アルゴリズムを使用して暗号化されます。
5. **［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アーカイブ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 ファイルに保存されませんが、パスワードのハッシュがベリファイには使用されます。この 2 段階のセキュリティにより、バックアップ データは権限のない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。

3.4.1.2. バックアップから除外するファイル

このオプションは、Windows と Linux オペレーティング システム、およびブータブル メディアで有効です。.

このオプションは、ディスク レベルのバックアップでは、NTFS ファイル システムと FAT ファイル システムのみで有効です。このオプションは、ファイル レベルのバックアップでは、サポートされているすべてのファイル システムに対して有効です。

このオプションでは、バックアップ処理中にスキップして、バックアップ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。

デフォルトの設定 - **[次の条件に一致するファイルを除外: *.tmp、*.~、*.bak]**

除外するファイルおよびフォルダを指定する手順は、次のとおりです。

次のいずれかのパラメータを設定します。

- **すべての隠しファイルおよびフォルダを除外**

  隠しファイル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。

- **すべてのシステム ファイルおよびフォルダを除外**

  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設定されてい場合、フォルダの内容はシステム属性を設定されていないファイルを含みすべて除外されます。

***attrib** コマンドを使用してファイルまたはフォルダのファイル/フォルダ プロパティ内の属性を表示することができます。詳細については、Windows の［ヘルプとサポート］をご参照ください。*

- **次の条件に一致するファイルを除外**

  一覧内のいずれかの条件(ファイル マスクと呼ばれます)に一致するファイル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。ファイル マスクの一覧を作成するには、**［追加］**、**［編集］**、**［削除］**、および**［すべて削除］**ボタンを使用します。

  1 つ以上のワイルドカード文字(* および ?)をファイル マスク内で使用することができます。

  アスタリスク(*)はファイル名内の 0 個以上の文字の代用として使用します。たとえば、ファイル マスク Doc*.txt は Doc.txt、Document.txt などの文字と一致します。

疑問符(?)はファイル名内の厳密に 1 文字の代用として使用します。たとえば、ファイルマスク Doc?.txt は Doc1.txt、Docs.txt などのファイルと一致しますが、Doc.txt、Doc11.txt などのファイルとは一致しません。

除外の例

条件	例	説明
名前	File1.log	File1.log という名前のすべてのファイルを除外します。
パス	C:¥Finance¥test.log	C:¥Finance フォルダに置かれている test.log という名前のファイルを除外します。
マスク(*)	*.log	.log 拡張子の付いたすべてのファイルを除外します。
マスク(?)	my???.log	5 文字で最初が「my」で始まる名前のすべての .log ファイルを除外します。

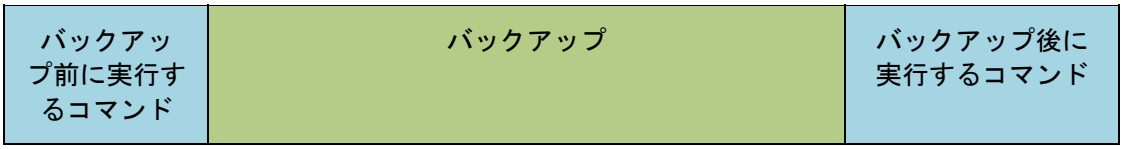
上記の設定は、明示的にバックアップ対象として選択されたファイルまたはフォルダには適用されません。たとえば、MyFolder というフォルダとこのフォルダの外部にある MyFile.tmp というファイルをバックアップ対象に選択して、すべての .tmp ファイルをスキップするように選択したとします。この場合、バックアップ処理中に MyFolder フォルダ内のすべての .tmp ファイルはスキップされますが、MyFile.tmp ファイルはスキップされません。

3.4.1.3. バックアップ処理の前後に実行するコマンド

このオプションは、Windows と Linux オペレーティング システム、および PE ベースのブータブル メディアで有効です。

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
- バックアップの終了後にアーカイブを別の場所にコピーする

「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。

バックアップ処理の前後に実行するコマンドを指定する手順は、次のとおりです。

1. 次のオプションをオンにして、バックアップ処理の前後に実行するコマンドの実行を有効にします。
   - **［バックアップの前に実行］**
   - **［バックアップの後に実行］**
2. 次のいずれかを実行します。
   - **［編集］**をクリックして、新しいコマンドまたはバッチ ファイルを指定する
   - 既存のコマンドまたはバッチ ファイルをドロップ ダウン リストから選択する
3. **［OK］**をクリックします。

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. **［コマンド］**フィールドにコマンドを入力するか、またはバッチ ファイルを選択します。「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。
2. **［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。
3. **［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。
4. 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。
5. **［コマンドのテスト］**をクリックして、コマンドが正しいかどうかを確認します。

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、復元タスクを失敗させる	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				
	デフォルト 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、タスクを中止します。	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。

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. **［コマンド］**フィールドにコマンドを入力するか、またはバッチ ファイルを選択します。
2. **［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。
3. **［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。
4. コマンドの実行の成功がバックアップ戦略にとって非常に重要である場合は、**［コマンドの実行に失敗した場合、復元タスクを失敗させる］**チェックボックスをオンにします。コマンドの実行が失敗した場合、結果として生成される TIB ファイルと一時ファイルが削除され(可能な場合)、タスクは中止されます。

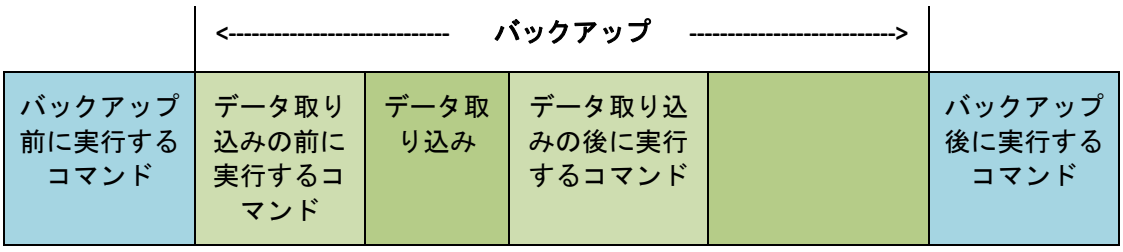
   このチェックボックスがオフになっていると、コマンドの実行結果はタスクの実行の失敗または成功に影響しません。コマンドの実行結果は、**［ダッシュボード］**に表示されるログまたはエラーと警告を確認することによって追跡できます。
5. **［コマンドのテスト］**をクリックして、コマンドが正しいかどうかを確認します。

3.4.1.4. データ取り込みの前後に実行するコマンド

このオプションは、Windows および Linux オペレーティング システムの両方で有効です。

このオプションによって、バックアップ処理の始めに Acronis Backup & Recovery 10 によって、データ取り込み(データ スナップショットの作成)の前後に自動的に実行されるコマンドを定義できます。

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。



［ボリューム シャドウ コピー サービス］『ページ参照 124』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 サスペンド→データ取り込み→VSS 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。バックアップ処理の前後に実行するコマンド『ページ参照 118』とは異なり、データ取り込みの前後に実行するコマンドはデータ取り込み処理の前後に数秒間で実行されます。これに対し、バックアップ処理全体はバックアップするデータの量によっては、はるかに時間がかかることがあります。このため、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になります。

データ取り込みの前後に実行するコマンドを指定する手順は、次のとおりです。

1. 次のオプションをオンにして、データ取り込みの前後に実行するコマンドの実行を有効にします。
   - **［データ取り込みの前に実行する］**
   - **［データ取り込みの後に実行する］**
2. 次のいずれかを実行します。
   - **［編集］**をクリックして、新しいコマンドまたはバッチ ファイルを指定する
   - 既存のコマンドまたはバッチ ファイルをドロップ ダウン リストから選択する
3. **［OK］**をクリックします。

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. **［コマンド］**フィールドにコマンドを入力するか、またはバッチ ファイルを選択します。「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。
2. **［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。
3. **［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。
4. 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。
5. **［コマンドのテスト］**をクリックして、コマンドが正しいかどうかを確認します。

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 タスクを失敗させる	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取り込みを実行しない	オン	オン	オフ	オフ

結果				
	デフォルト 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、タスクを中止します。	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。

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. **[コマンド]** フィールドにコマンドを入力するか、またはバッチ ファイルを選択します。「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。
2. **[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。
3. **[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。
4. 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。
5. **[コマンドのテスト]** をクリックして、コマンドが正しいかどうかを確認します。

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、復元タスクを失敗させる	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				
	デフォルト 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。コマンドの実行に失敗した場合、TIB ファイルと一時ファイルを削除してタスクを中止します。	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。

3.4.1.5. 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のみで有効です。Windows と Linux オペレーティング システム.

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。*

デフォルトの設定 - **［可能な場合はスナップショットを作成する］**

次のいずれかを選択します。

- **［常にスナップショットを作成する］**
  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。同一時点のファイルが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にのみ、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することは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使用するには、バックアップ計画を Administrator または Backup Operator の権限を持つアカウントで実行する必要があります。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。
- **［可能な場合はスナップショットを作成する］**
  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。
- **［スナップショットを作成しない］**
  常に直接ファイルをバックアップします。Administrator または Backup Operator 権限は必要ありません。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。

3.4.1.6. 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 オペレーティング システムの場合にのみ有効です。

このオプションは、ディスク レベルのバックアップに適用されます。このオプションは、スナップショットを作成することによってファイル レベルのバックアップを実行する際の、ファイル レベルのバックアップにも適用されます (［ファイル レベルのバックアップのスナップショット］『ページ参照 123』オプションによって、ファイル レベルのバックアップ中にスナップショットを作成するかどうかを指定できます)。

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作成するか、または 1 つずつ作成するかを指定します。

デフォルトの設定 - **［有効］**

このオプションを **［有効］**に設定すると、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作成されます。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**］に設定すると、ボリュームのスナップショットが 1 つずつ作成されます。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。

3.4.1.7. ボリューム シャドウ コピー サービス

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(Acronis VSS または Microsoft VSS)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、Acronis Backup & Recovery 10 がデータ スナップショットを作成する時点において、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。データの整合性が維持されているにより、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。

デフォルトの設定 - **［VSS を使用してスナップショットを作成する］**

Acronis Backup & Recovery 10 は、コンピュータで実行中のオペレーティング システム、およびコンピュータが Active Directory ドメインのメンバであるかどうかに基づいて、VSS プロバイダを自動的に選択します。

［VSS を使用せずにスナップショットを作成する］

お使いのデータベースが VSS と互換性がない場合は、このオプションを選択します。データのスナップショットは Acronis Backup & Recovery 10 によって取得されます。バックアップ処理は最も高速ですが、スナップショットの作成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。データが整合性のある状態でバックアップされるように、データ取り込みの前後に実行するコマンド『ページ参照 120』を使用して、スナップショットの作成前後に実行するコマンドを指定することができます。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。

ボリューム シャドウ コピー ライタ

VSS 対応のアプリケーションのデータをバックアップする前に、オペレーティング システム内に存在するライタの一覧を調べて、これらのアプリケーションのボリューム シャドウ コピー ライタが有効になっていることを確認しておく必要があります。この一覧を表示するには、次のコマンドを実行します。

```
vssadmin list writers
```

注意: *Microsoft Windows Small Business Server 2003 では、Microsoft Exchange Server 2003 用のライタはデフォルトで無効になっています。有効にする手順については、対応する Microsoft のヘルプとサポートの記事 http://support.microsoft.com/kb/838183/en をご参照ください。*

3.4.1.8. 圧縮レベル

このオプションは、Windows と Linux オペレーティング システム、およびブータブル メディアで有効です。

このオプションでは、バックアップするデータに適用される圧縮レベルを定義します。

デフォルトの設定 - **［標準］**

最適なデータの圧縮レベルは、バックアップされるデータの種類によって異なります。たとえば、既に圧縮されている .jpg、.pdf、.mp3 などの形式のファイルがアーカイブに含まれている場合は、最高の圧縮レベルを適用してもアーカイブのサイズはそれほど縮小されません。ただし、.doc、.xls などの形式のファイルは圧縮効果が高くなります。

圧縮レベルを指定する手順は、次のとおりです。

次のいずれかを選択します。

- **［なし］** - データは圧縮されずにコピーされます。最終的なバックアップ サイズは最大になります。
- **［標準］** - ほとんどの場合にお勧めします。
- **［高い］** - 最終的なバックアップ サイズは、一般に **［標準］** より小さくなります。
- **［最大］** - データは可能な限り圧縮されます。バックアップ時間は最も長くなります。リムーバブル メディアにバックアップする場合は、［最大］を選択すると空のリムーバブル ディスクの必要枚数を減らすことができます。

3.4.1.9. バックアップのパフォーマンス

このグループのオプションを使用して、バックアップ処理に割り当てるネットワークとシステムのリソース量を指定します。

［バックアップのパフォーマンス］オプションは、バックアップの処理速度に顕著な影響を及ぼす場合があります。バックアップの処理速度は、システム全体の構成やバックアップ時に入出力を行うデバイスの物理的な特性に依存します。

バックアップの優先度

このオプションは、Windows および Linux オペレーティング システムの両方で有効です。

システムで実行されるプロセスの優先度によって、そのプロセスに割り当てられる CPU やシステムのリソース量が決まります。バックアップの優先度を下げると、他のアプリケーションのためのリソースを増やすことができます。バックアップの優先度を上げると、バックアップ アプリケーションに割り当てる CPU などのリソースを増やすようにオペレーティング システムに要求することによって、バックアップの処理速度が上がる場合があります。ただし、その効果は、全体的な CPU の使用率およびディスク入出力速度、ネットワーク トラフィックなどのその他の要素に依存します。

デフォルトの設定 - **［低］**

バックアップ処理の優先度を指定する手順は、次のとおりです。

次のいずれかを選択します。

- **［低］**- より多くのリソースをコンピュータ上で動作する他のプロセスのために残し、バックアップ処理が占有するリソースを最小限にします。
- **［通常］**- 他のプロセスと同等のリソースを割り当て、通常の速度でバックアップ処理を実行します。
- **［高］**- 他のプロセスからリソースを取り上げることによって、バックアップの処理速度を最大にします。

HDD 書き込み速度

このオプションは、Windows と Linux オペレーティング システム、およびブータブル メディアで有効です。

このオプションは、バックアップされるコンピュータの内蔵(固定)ハード ディスクがバックアップ保存先として選択された場合に使用できます。

Acronis セキュア ゾーンなどの固定ハード ディスクへのバックアップは、大量のデータをディスクに書き込む必要があるため、オペレーティング システムやアプリケーションのパフォーマンスを低下させる場合があります。バックアップ処理によるハード ディスクの使用を必要なレベルまで制限することができます。

デフォルトの設定 - **［最大］**

HDD 書き込み速度をバックアップ用に設定する手順は、次のとおりです。

次のいずれかを実行します。

- **［書き込み先ハード ディスクの最大速度を 100% とする書き込み速度］**をクリックし、スライダをドラッグするか、またはボックスでパーセント値を選択します。
- **［KB/秒で指定する書き込み速度］**をクリックし、書き込み速度を KB/秒の単位で入力します。

ネットワークの接続速度

このオプションは、Windows と Linux オペレーティング システム、およびブータブル メディアで有効です。

このオプションは、バックアップ保存先としてネットワーク上の場所(ネットワーク共有、管理対象の格納域、または FTP/SFTP サーバー)が選択された場合に使用できます。

このオプションでは、バックアップ データの転送に割り当てるネットワーク接続の帯域幅を定義します。

デフォルトで速度は［最大］に設定されます。つまり、バックアップ データの転送時に使用可能なすべてのネットワーク帯域幅が使用されます。このオプションを使用すると、他のネットワーク活動のためにネットワーク帯域幅の一部を予約できます。

デフォルトの設定 - **［最大］**

バックアップのためのネットワークの接続速度を設定する手順は、次のとおりです。

次のいずれかを実行します。

- **［ネットワーク接続の推定最大速度の割合として示される転送速度］**をクリックし、スライダをドラッグするか、またはボックスでパーセント値を選択力します。
- **［KB/秒で示される転送速度］**をクリックし、バックアップ データ転送時の帯域幅制限値を KB/秒の単位で入力します。

3.4.1.10. 通知

Acronis Backup & Recovery 10 には、電子メールまたはメッセージング サービスによってバックアップの完了をユーザーに通知する機能があります。

電子メール

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。

このオプションは、ブータブル メディアから起動した場合には使用できません。

このオプションによって、タスクの完全なログと共に、バックアップ タスクの正常終了、失敗、またはユーザーによる操作が必要な場合について通知する電子メールを受け取ることができます。

デフォルトの設定 - **オフ**

電子メールによる通知を設定する手順は、次のとおりです。

1. **［電子メールによる通知を送信する］**チェックボックスをオンにして、通知を有効にします。
2. **［電子メール アドレス］**フィールドに、通知の送信先の電子メール 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. **［送信する通知］**で、次の中から適切なチェックボックスをオンにします。
   - **［バックアップが正常に終了した場合］**- バックアップ タスクが正常終了した場合に通知を送信します。
   - **［バックアップが失敗した場合］**- バックアップ タスクが失敗した場合に通知を送信します。

   ［ユーザーによる操作が必要な場合］チェックボックスは常にオンです。
4. 電子メール メッセージにバックアップに関連するログ エントリを含める場合は、**［すべてのログを通知する］**チェックボックスをオンにします。

5. **［追加の電子メール パラメータ］**をクリックし、次のように追加の電子メール パラメータを設定して、**［OK］**をクリックします。
   - **［差出人］**- メッセージの送信元となるユーザーの電子メール アドレスを入力します。このフィールドが空白の場合、差出人アドレスには宛先アドレスが使用されます。
   - **［暗号化を使用する］**- メール サーバーへの暗号化された接続を選択できます。SSL 暗号化または TLS 暗号化のいずれかの種類を選択できます。
   - 一部のインターネット サービス プロバイダでは、送信が許可される前に受信メール サーバーによる認証が要求されます。その場合は、**［受信メール サーバーにログオンする］**チェックボックスをオンにして POP サーバーを有効にし、次の設定を行います。
     - **［受信メール サーバー(POP)］**- POP サーバーの名前を入力します。
     - **［ポート］**– POP サーバーのポートを設定します。デフォルトでは、ポートは 110 に設定されます。
     - **［ユーザー名］**- ユーザー名を入力します。
     - **［パスワード］**- パスワードを入力します。
   - **［指定した送信メール サーバーを使用する］**チェックボックスをオンにして SMTP サーバーを有効にし、次の設定を行います。
     - **［送信メール サーバー(SMTP)］**- SMTP サーバーの名前を入力します。
     - **［ポート］**– SMTP サーバーのポートを設定します。デフォルトでは、ポートは 25 に設定されます。
     - **［ユーザー名］**- ユーザー名を入力します。
     - **［パスワード］**- パスワードを入力します。
6. **［電子メールのテスト メッセージを送信する］**をクリックし、設定が正しいかどうかを確認します。

メッセンジャー サービス(WinPopup)

このオプションは、送信元コンピュータのオペレーティング システムが Windows または Linux で、受信コンピュータのオペレーティング システムが Windows の場合のみ利用できます。

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は使用できません。

このオプションによって、バックアップ タスクの正常終了、失敗、またはユーザーによる操作が必要性な場合について、ポップアップウィンドウによる通知を受け取ることができます。

デフォルトの設定 - **オフ**
ポップアップウィンドウによる通知を設定する前に、タスクを実行するコンピュータとメッセージを受け取るコンピュータの両方で Messenger サービスが開始されていることを確認します。

Microsoft Windows Server 2003 ファミリでは、Messenger サービスはデフォルトでは開始されません。サービスのスタートアップの種類を［自動］に変更してからサービスを開始します。

ポップアップウィンドウによる通知を設定する手順は、次のとおりです。

1. **［ポップアップウィンドウによる通知を送信する］**チェックボックスをオンにします。
2. **［コンピュータ名］**フィールドに、通知の送信先となるコンピュータの名前を入力します。複数の名前はサポートされていません。

［送信する通知］で、次の中から適切なチェックボックスをオンにします。

- **［バックアップが正常に終了した場合］**- バックアップ処理が正常終了した場合に通知を送信します。
- **［バックアップが失敗した場合］**- バックアップ処理が失敗した場合に通知を送信します。

［ユーザーによる操作が必要な場合］- 処理中にユーザーによる操作が必要になった場合、通知を送信します。常にオンです。

［テスト メッセージを送信する］をクリックし、設定が正しいかどうかを確認します。

3.4.1.11. イベント トレース

管理対象のコンピュータで実行されたバックアップ処理のイベントを Windows のアプリケーション イベント ログに表示したり、指定した SNMP マネージャに送信したりすることができます。

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。

このオプションは、ブータブル メディアから起動した場合には使用できません。

このオプションでは、管理対象のコンピュータで動作するエージェントが、バックアップ処理のイベントを 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、または **［コントロール パネル］→［管理ツール］→［イベント ビューア］**を選択します。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。

デフォルトの設定 - **［コンピュータ オプションの設定を使用する］**

バックアップ処理のイベントを Windows のアプリケーション イベント ログに記録するかどうかを選択する手順は、次のとおりです。

次のいずれかを選択します。

- **［コンピュータ オプションの設定を使用する］**- コンピュータ オプションで指定された設定を使用します。詳細については、「コンピュータ オプション『ページ参照 109』」をご参照ください。

- **［次の種類のイベントをログに記録する］**- バックアップ処理のイベントをアプリケーション イベント ログに記録します。ログに記録するイベントの種類を指定します。
  - **［すべてのイベント］**- すべてのイベント(情報、警告、およびエラー)をログに記録します。
  - **［エラーと警告］**
  - **［エラーのみ］**
- **［ログに記録しない］**- バックアップ処理のイベントをアプリケーション イベント ログに記録しません。

SNMP 通知

このオプションは、Windows および Linux オペレーティング システムの両方で有効です。

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は使用できません。

このオプションでは、管理対象のコンピュータで動作するエージェントが、バックアップ処理のイベントを指定した簡易ネットワーク管理プロトコル(SNMP)マネージャに送信する必要があるかどうかを定義します。送信するイベントの種類を選択できます。

Acronis Backup & Recovery 10 は、次の簡易ネットワーク管理プロトコル(SNMP)オブジェクトを SNMP 管理アプリケーションに送信します。

1.3.6.1.4.1.24769.100.200.1.0 - イベントの種類を特定する文字列(情報、警告、エラー) 。

1.3.6.1.4.1.24769.100.200.2.0 - イベントの説明テキストを含む文字列(Acronis Backup & Recovery 10 によってログに記録されるメッセージと同じです)。

デフォルトの設定 - **［コンピュータ オプションの設定を使用する］**

バックアップ処理のイベントを SNMP マネージャに送信するかどうかを選択する手順は、次のとおりです。

次のいずれかを選択します。

- **［コンピュータ オプションの設定を使用する］**– コンピュータ オプションで指定された設定を使用します。詳細については、「コンピュータ オプション『ページ参照 109』」をご参照ください。
- **［バックアップ処理イベントに対して個別に SNMP 通知を送信する］**– 指定した SNMP マネージャにバックアップ処理のイベントを送信します。
  - **［送信するイベントの種類］**- **［すべてのイベント］**、**［エラーと警告］**、または **［エラーのみ］**のいずれかから送信するイベントの種類を選択します。
  - **［サーバー名/IP］**- メッセージの送信先となる SNMP 管理アプリケーションを実行するホストの名前または IP アドレスを入力します。
  - **［コミュニティ］**- SNMP 管理アプリケーションを実行するホストと送信元コンピュータの両方が所属する SNMP コミュニティの名前を入力します。一般的なコミュニティは "public" です。

［テスト メッセージを送信する］をクリックし、設定が正しいかどうかを確認します。

- ［SNMP 通知を送信しない］- バックアップ処理イベントの SNMP マネージャへの送信を無効にします。

3.4.1.12. 高速の増分/差分バックアップ

このオプションは、Windows と Linux オペレーティング システム、およびブータブル メディアで有効です。

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。

このオプションでは、ファイルの変更をファイル サイズとタイム スタンプを使用して検出するか、ファイルの内容をアーカイブに保存されているファイルと比較することによって検出するかを定義します。

デフォルトの設定 - **オン**

増分/差分バックアップは、変更されたデータのみを取り込みます。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アーカイブに保存されている内容と比較されます。

3.4.1.13. バックアップの分割

このオプションは、Windows と Linux オペレーティング システム、およびブータブル メディアで有効です。

このオプションでは、バックアップを分割する方法を定義します。

デフォルトの設定 - ［自動］

次の設定を使用できます。

［自動］

この設定を使用すると、Acronis Backup & Recovery 10 は次のように動作します。

- **ハード ディスクにバックアップする場合**

  推定されるファイル サイズをバックアップ保存先ディスクのファイル システムが許容できる場合、単一のバックアップ ファイルが作成されます。

  推定されるファイル サイズをバックアップ保存先ディスクのファイル システムが許容できない場合、バックアップは自動的に複数のファイルに分割されます。このような状況は、最大ファイル サイズに 4GB の制限がある FAT16 および FAT32 ファイル システムにバックアップを保存する場合に発生します。

  バックアップの作成中にバックアップ保存先ディスクの空き領域が不足すると、タスクは［ユーザーによる操作が必要］状態に移行します。領域をさらに解放して、操作を再試行できます。この場合、生成されるバックアップは再試行の前後で分割されます。

- **リムーバブル メディアにバックアップする場合**(CD、DVD、またはテープ デバイスが管理対象のコンピュータにローカル接続されている)

  タスクは［**ユーザーによる操作が必要**］状態に移行し、前のメディアがいっぱいになると新しいメディアを要求します。

［固定サイズ］

必要なファイル 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。バックアップは、指定したサイズの複数のファイルに分割されます。この機能は、後で複数の CD または DVD にバックアップを書き込むことを目的としている場合に役立ちます。FTP サーバーから直接データを復元するには、バックアップ ファイルを 2GB 以内のサイズに分割する必要があるため、FTP サーバーに保存するバックアップも分割することが必要となる場合があります。

3.4.1.14. ファイル レベルのセキュリティ

これらのオプションは、Windows オペレーティング システムのファイル レベルのバックアップのみで有効です。

［暗号化されたファイルを暗号化解除された状態でアーカイブに格納する］

このオプションでは、バックアップ アーカイブに保存する前にファイルの暗号化を解除するかどうかを定義します。

デフォルトの設定 - **オフ**

暗号化を使用しない場合、このオプションは無視されます。バックアップに暗号化されたファイルが含まれていて、復元後にすべてのユーザーがアクセスできるようにする場合は、このオプションをオンにします。オフにすると、ファイル/フォルダを暗号化したユーザーのみがそれらを読むことができます。暗号化の解除は、暗号化されたファイルを別のコンピュータに復元する場合にも役立ちます。

ファイルの暗号化は、暗号化ファイル システム(EFS)を搭載した NTFS ファイル システムを使用する Windows でも使用できます。ファイルまたはフォルダの暗号化の設定にアクセスするには、 ***［プロパティ］→［全般］→［詳細設定］→［内容を暗号化してデータをセキュリティで保護する］*** *を選択します。*

［アーカイブにファイルのセキュリティ設定を保持する］

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バックアップするかどうかを定義します。

デフォルトの設定 - **オン**

このオプションをオンにすると、ファイルとフォルダは、ユーザーまたはユーザー グループごとの元のアクセス許可(ファイルの読み取り、書き込み、または実行)と共にアーカイブに保存されます。アクセス許可で指定されているユーザー アカウント以外のアカウントでセキュリティで保護されたファイルまたはフォルダをコンピュータに復元すると、このファイルを読み取りまたは変更できなくなる場合があります。

このような問題を完全に解決するには、アーカイブにファイルのセキュリティ設定を保持する設定を無効にします。復元されたファイルとフォルダは、常に復元されたフォルダまたはディスクのアクセス許可を継承します(ルートに復元された場合)。

または、セキュリティ設定の復元『ページ参照 146』がアーカイブで使用できる場合でも、それを無効にすることができます。結果は同じになります。つまり、ファイルは親フォルダのアクセス許可を継承します。

*ファイルまたはフォルダの NTFS アクセス許可にアクセスするには、**［プロパティ］→［セキュリティ］**を選択します。*

3.4.1.15. メディア コンポーネント

このオプションは、バックアップ保存先がリムーバブル メディアの場合、Windows と Linux のオペレーティング システムの両方で有効です。

リムーバブル メディアにバックアップする場合は、追加のコンポーネントを書き込むことによって、このメディアを通常の Linux ベースのブータブル メディア『ページ参照 423』のように機能させることができます。その結果、個別のブータブル メディアは必要なくなります。

デフォルトの設定 - **選択なし**

ブータブル メディアに保存するコンポーネントのチェックボックスをオンにします。

- **［One-Click Restore］**は、リムーバブル メディアに保存されているディスク バックアップから簡単に復元するために最小限必要な追加機能です。メディアからコンピュータを起動し、**［Acronis One-click Restore の実行］**をクリックすると、同じメディアに含まれるバックアップから直ちにディスクが復元されます。

  ***注意:** One-Click 操作では、復元するボリュームを選択する場合などのユーザーによる選択は想定されていないため、Acronis One-Click Restore では、常にディスク全体が復元されます。ディスクに複数のボリュームがあるときに Acronis One-Click Restore を使用する場合は、バックアップにすべてのボリュームを含めるようにします。バックアップに含まれないボリュームはすべて失われます。*

- **［ブータブル エージェント］**は、Acronis Backup & Recovery 10 エージェントのほとんどの機能を含む Linux カーネル ベースのブータブル レスキュー ユーティリティです。復元中にさらに多くの機能を必要とする場合は、このコンポーネントをメディアに書き込んでください。通常のブータブル メディアと同様に、Active Restore または Universal Restore を使用して復元処理を設定できます。

Windows コンピュータに Acronis Disk Director Lite がインストールされている場合は、さらに 1 つのコンポーネントを選択できます。

- **［Acronis Disk Director Lite］**は、ディスクのクローン作成、ベーシック ボリュームとダイナミック ボリュームの作成、削除、変換などの操作を可能にするディスク管理ツールで、MBR と GPT と間でのディスク パーティション スタイルの変換、ディスク ラベルの変更などの追加の操作を行うことができます。このコンポーネントをメディアに追加すると、データを復元する前にコンピュータ上でディスク構成を準備できます。

3.4.1.16. エラー対応

これらのオプションは、Windows と Linux オペレーティング システム、およびブータブル メディアで有効です。

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。

[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)]

デフォルトの設定 - **オフ**

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。

[エラーが発生した場合は再試行する]

デフォルトの設定 - **オン、試行回数: 5 回、試行間隔: 30 秒**

修復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 5 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。

[不良セクタを無視する]

デフォルトの設定 - **オフ**

このオプションをオフにすると、不良セクタが検出されるたびに、バックアップ処理を続行するか中止するかの判断をユーザーに求めるポップアップウィンドウが表示されます。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。

3.4.1.17. 保存先の二重化

第一のバックアップ保存先が *ローカル フォルダまたは Acronis セキュア ゾーン*で、第二のバックアップ保存先が *別のローカル フォルダまたはネットワーク共有*である場合、このオプションは Windows と Linux オペレーティング システムの両方で有効です。管理対象の格納域と FTP サーバーは、第二のバックアップ保存先としてサポートされません。

デフォルトの設定 - **オフ**

保存先の二重化を有効にすると、エージェントはローカルに作成されたそれぞれのバックアップを、ネットワーク共有などの第二のバックアップ保存先に自動的にコピーします。第一のバックアップ保存先へのバックアップが完了すると、エージェントは更新されたアーカイブの内容を第二のアーカイブの内容と比較し、第二のバックアップ保存先にすべての新規バックアップと抜けているバックアップをコピーします。

このオプションを使用すると、中間的な場所として内部ドライブに高速にコンピュータ バックアップを行い、そのバックアップをネットワークに保存することができます。これは、ネットワークが低速であるか、ビジーである場合、およびバックアップ処理に時間がかかる場合に役立ちます。リモートの場所に直接バックアップを作成する場合と異なり、コピーを転送しているときにネットワーク接続が切断してもバックアップ処理に影響しません。

その他の利点

- レプリケーションによって、アーカイブの信頼性が高まります。
- モバイル ユーザーは、出先から Acronis セキュア ゾーンにポータブル コンピュータのバックアップを作成できます。ポータブル コンピュータを企業ネットワークに接続すると、最初のバックアップ処理の後は、アーカイブに対して行われたすべての変更が社内のコピーに転送されます。

第一のバックアップ保存先としてパスワードで保護された Acronis セキュア ゾーンを選択する場合は、第二のバックアップ保存先のアーカイブはパスワードで保護されないことに注意してください。

保存先を二重化する手順は、次のとおりです。

1. **［保存先を二重化する］**チェックボックスをオンにします。
2. 第二のバックアップ保存先を選択するか、バックアップ保存先のフルパスを手動で入力します。
3. **［OK］**をクリックします。

第二のバックアップ保存先のログイン情報を入力する必要がある場合もあります。入力を求められたら、ログイン情報を入力します。

3.4.1.18. 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。

このオプションは、ブータブル メディアから起動した場合には使用できません。

このオプションでは、バックアップ 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、「スケジューリング『ページ参照 199』」と「条件『ページ参照 212』」をご参照ください。

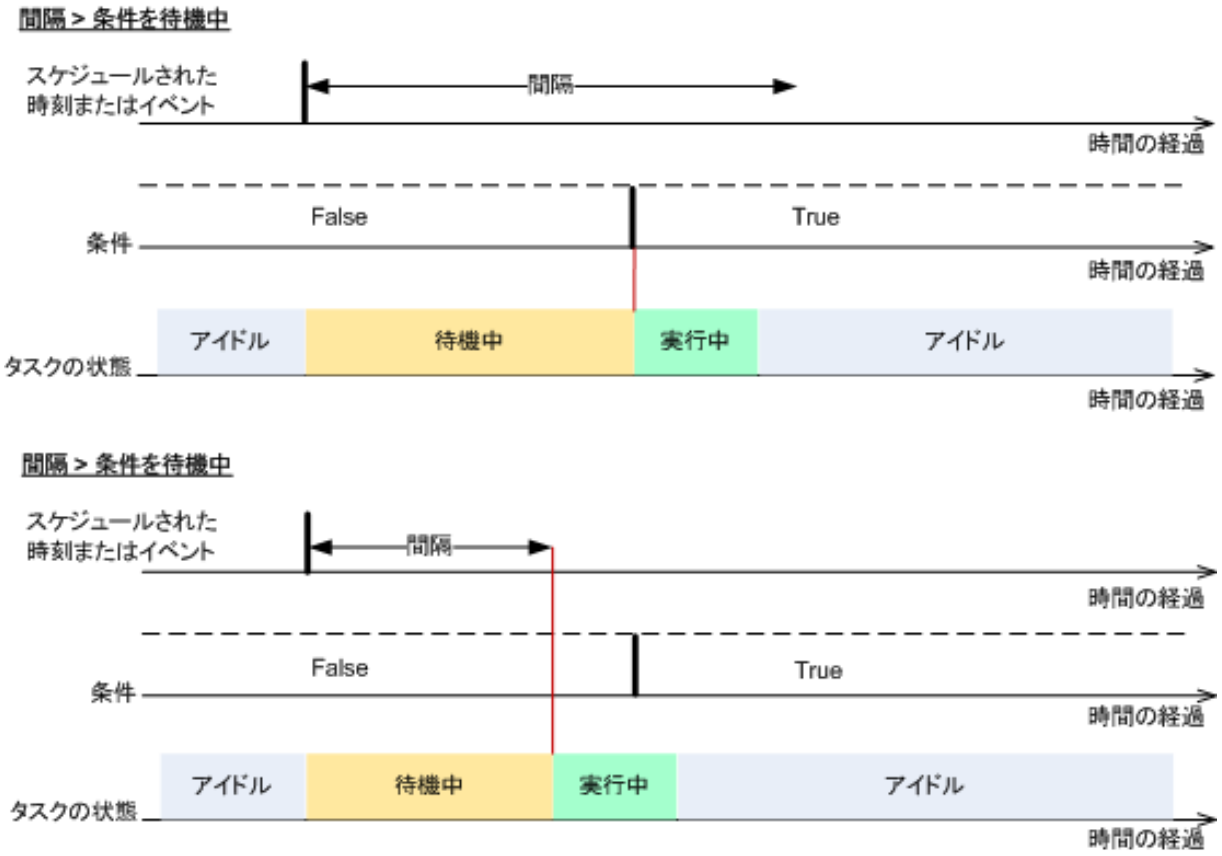
デフォルトの設定 - **［条件が満たされるまで待機する］**

[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。

長期間条件が満たされず、バックアップの遅延によ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、または最大遅延時間が経過すると、タスクが起動されます。

時間に関する説明図: 条件が満たされるまで待機する



[タスクの実行をスキップする]

指定した時間ちょうどにデータをバックアップする必要がある場合など、バックアップの遅延を容認できない場合もあります。特に、比較的頻繁にイベントが発生するような場合は、条件が満たされるまで待たずにバックアップをスキップすることには意味があります。

3.4.1.19. タスクの失敗への対応

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。

このオプションは、ブータブル メディアから起動した場合には使用できません。

このオプションでは、バックアップ計画のいずれかのタスクが失敗した場合の動作を指定します。

デフォルトの設定 - **[バックアップ計画の実行を続行する]**

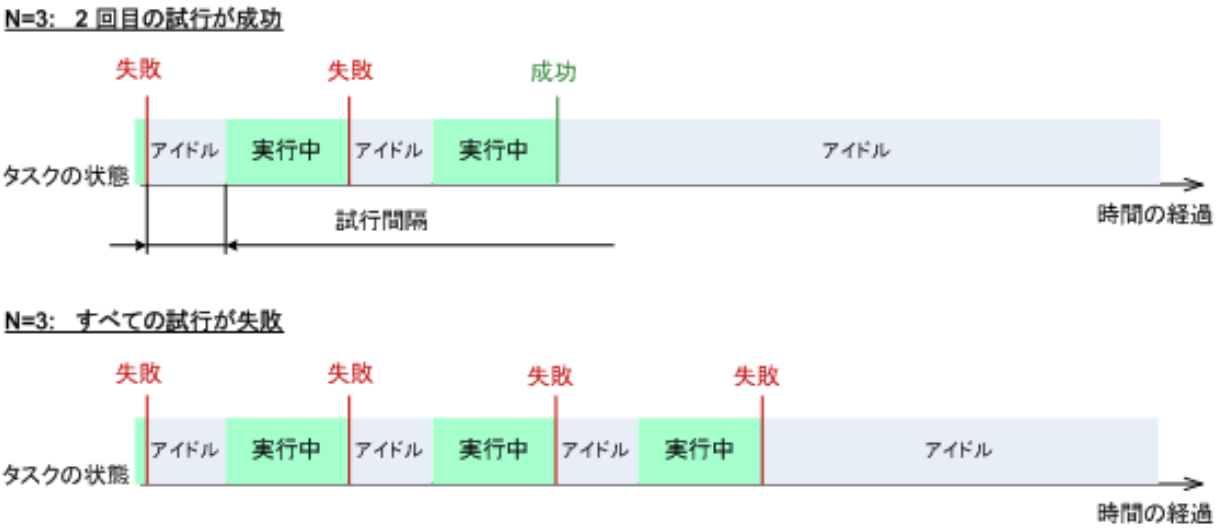
[バックアップ計画の実行を停止する]

失敗の原因を特定して解決するための時間を確保するために、計画のスケジュールは一時的に無効になります。**[バックアップの計画およびタスク]** ビューの ▶ ボタンを使用して計画の実行を再開するまで、計画のすべてのタスクはスケジュールに従って開始されることはありません。

[バックアップ計画の実行を続行する]

計画のタスクは、エラーが発生しなかった場合と同様にスケジュールに従って実行されます。

さらに、失敗したタスクを再試行することもできます。**[失敗したタスクを再び開始する]** チェックボックスをオンにし、試行回数および試行間隔を指定します。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。



バックアップ計画の誤りによってタスクが失敗した場合は、タスクがアイドル状態の間に計画を編集できます。タスクが実行中の場合は、バックアップ計画を編集する前にタスクを停止する必要があります。

3.4.1.20. テープ サポート

これらのオプションは、バックアップ先がテープ ライブラリにある管理対象の格納域であるときに有効です。

[**テープ サポート**] オプションを使用すると、バックアップ タスクでバックアップをテープ間に分散する方法を指定できます。

テープ オプションの組み合わせによっては、テープ ライブラリ全体および各テープの使用効率が低下することがあります。これらのオプションを変更する必要性が特にないときは、テープ オプションを変更せずにそのままにしてください。

1 つのアーカイブに対して複数のテープを使用できます。このような状況では、**テープ セット**を使用してデータのバックアップを保持します。

テープ セットとは、特定の保護されたデータのバックアップを含む 1 本以上のテープからなる論理グループです。テープ セットには他のデータのバックアップを入れることもできます。

個別のテープ セットとは、特定の保護されたデータのバックアップのみが入っているテープ セットです。他のバックアップを個別のテープ セットに書き込むことはできません。

(作成するバックアップ ポリシー/計画で) [個別のテープ セットを使用する]

デフォルトの設定 - **オフ**

このオプションを変更しないままにすると、作成中のポリシーまたは計画に属するバックアップが、別のバックアップ ポリシーによって書き込まれたバックアップが入っていて、別のコンピュータのデータで構成されるテープに書き込まれる場合があります。同様に、他のポリシーによるバックアップが、このポリシーによるバックアップが入っているテープに書き込まれる場合があります。すべてのテープはプログラムによって自動的に管理されるので、このようなテープによる問題は発生しません。

このオプションを有効にすると、作成中のポリシーまたは計画に属するバックアップが個別のテープ セットに保存されます。他のバックアップはこのテープ セットに書き込まれません。

管理サーバーにコンソールが接続されている場合

[**個別のテープ セットを使用する**] オプションでは、さらに正確な定義が可能です。作成するバックアップ ポリシーで、すべてのコンピュータに対して 1 つのテープ セットを使用するか、または 1 台のコンピュータごとに 1 つのテープ セットを使用することができます。

デフォルトでは、[**すべてのコンピュータで 1 つのテープ セットを使用する**] オプションが選択されます。通常、このオプションを選択すると、[**コンピュータごとに個別のテープ セットを使用する**] オプションを選択したときよりもテープの使用効率が高くなります。ただし、特定のコンピュータのバックアップ テープをサイト外に保存するなどの特別な要件があるときは、2 番目のオプションが役立ちます。

[個別のテープ セットを使用する] オプションをオンにすると、現在テープ ライブラリ デバイスにないテープにバックアップを書き込むことが必要になる場合があります。この状況での対応を定義してください。

- **[ユーザーによる操作を要求する]** - バックアップ タスクは **[ユーザーによる操作が必要]** 状態に移行し、必要なラベルの付いたテープがテープ ライブラリ デバイスにロードされるのを待機します。
- **[空きテープを使用する]** - バックアップは空のテープに書き込まれるので、操作が一時停止するのはライブラリに空のテープがない場合だけです。

[常に空きテープを使用する]

下のオプションを変更しないままにすると、各バックアップは **[個別のテープ セットを使用する]** オプションによって指定したテープに書き込まれます。下のいずれかのオプションをオンにすると、完全バックアップ、増分バックアップ、または差分バックアップを作成するたびに新しいテープがテープ セットに追加されます。

- **[各完全バックアップ]**

デフォルトの設定 - **オフ**

このオプションをオンにすると、完全バックアップはそれぞれ空のテープに書き込まれます。特にこの操作のためにテープがドライブにロードされます。 **[個別のテープ セットを使用する]** オプションがオンのときは、同じデータの増分バックアップと差分バックアップだけがテープに追加されます。

- **[各差分バックアップ]**

デフォルトの設定 - **オフ**

このオプションをオンにすると、差分バックアップはそれぞれ空のテープに書き込まれます。このオプションは、完全バックアップごとに空のテープを使用するときだけ選択できます。

- **[各増分バックアップ]**

デフォルトの設定 - **オフ**

このオプションをオンにすると、増分バックアップはそれぞれ空のテープに書き込まれます。このオプションは、完全バックアップと差分バックアップごとに空のテープを使用するときだけ選択できます。

3.4.1.21. その他の設定

次のチェックボックスをオンまたはオフにして、バックアップ処理のその他の設定を指定します。

[ユーザーの確認を求めることなくテープのデータを上書きする]

このオプションは、テープ デバイスにバックアップする場合にのみ有効です。

デフォルトの設定 - **オフ**

ローカル接続されているテープ デバイス内の空ではないテープにバックアップを開始すると、テープ上のデータが失われることを警告するメッセージが表示されます。この警告を無効にするには、このチェックボックスをオンにします。

[バックアップ終了後にメディアをマウント解除する]

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。

このオプションは、リムーバブル メディア(CD、DVD、テープ、またはフロッピー ディスク)にバックアップする場合に有効です。

デフォルトの設定 - **オフ**

バックアップ完了後には、バックアップ保存先の CD/DVD のメディアを取り出すか、またはテープのマウントを解除できます。

[リムーバブル メディアへのバックアップ時に最初のメディアを要求する]

このオプションは、リムーバブル メディアにバックアップする場合にのみ有効です。

このオプションでは、リムーバブル メディアにバックアップする場合に、**[最初のメディアを挿入してください]**というメッセージを表示するかどうかを定義します。

デフォルトの設定 - **オン**

このオプションをオンにした場合、メッセージ ボックスで［OK］がクリックされるまで実行を待機するため、ユーザーがコンピュータから離れているとリムーバブル メディアへのバックアップを実行できない場合があります。したがって、リムーバブル メディアへのバックアップのスケジュールを作成する場合は、このメッセージを無効にする必要があります。メッセージを無効にしておくと、DVD がドライブに挿入されている場合など、リムーバブル メディアが使用可能な場合は、タスクを無人で実行できます。

[アーカイブ ビットをリセットする]

このオプションは、Windows オペレーティング システムおよびブータブル メディアのファイル レベルのバックアップのみで有効です。

デフォルトの設定 - **オフ**

Windows オペレーティング システムでは、各ファイルには**［ファイルをアーカイブ可能にする］**属性があり、**［ファイル］**→**［プロパティ］**→**［全般］**→**［詳細設定］**→**［アーカイブ属性およびインデックス属性］**を選択することで設定できます。この属性はアーカイブ ビットとも呼ばれ、オペレーティング システムによってファイルが変更されるたびに設定され、バックアップ アプリケーションがそのファイルをバックアップに保存するたびにリセットできます。アーカイブ ビット値は、データベースなどのさまざまなアプリケーションによって使用されます。

[アーカイブ ビットをリセットする] チェックボックスをオンにすると、Acronis Backup & Recovery 10 はバックアップするすべてのファイルのアーカイブ ビットをリセットします。Acronis Backup & Recovery 10 自体は、アーカイブ ビット値を使用しません。増分バックアップまたは差分バックアップを実行する場合は、前回ファイルが保存されたときのファイル サイズと日付/時刻によって、ファイルが変更されたかどうかが判断されます。

[バックアップ処理の終了後にコンピュータを自動的に再起動する]

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のみ使用できます。

デフォルトの設定 - **オフ**

このオプションをオンにすると、Acronis Backup & Recovery 10 は、バックアップ処理が完了した後でコンピュータを再起動します。

たとえば、デフォルトでコンピュータがハード ディスク ドライブから起動される場合、このチェックボックスをオンすると、コンピュータは再起動され、ブータブル エージェントがバックアップの作成を完了するとすぐにオペレーティング システムが起動されます。

[バックアップを格納域に転送した後にのみ、バックアップを重複除外する (ソースで重複除外しない)]

このオプションは、バックアップ保存先が重複除外された格納域の場合、Windows と Linux のオペレーティング システム、およびブータブル メディアで有効です。

デフォルトの設定 - **オフ**

このオプションをオンにすると、ソースにおけるバックアップの重複除外がオフになり、重複除外はバックアップが格納域に保存された後に Acronis Backup & Recovery 10 ストレージ ノードによって実行されます。これは、ターゲットにおける重複除外と呼ばれます。

ソースにおける重複除外をオフにすると、バックアップ処理が高速化される場合がありますが、ネットワーク トラフィックとストレージ ノードの負荷が増大することがあります。格納域内のバックアップの最終的なサイズは、ソースにおける重複除外のオン/オフとは関係ありません。

ソースにおける重複除外とターゲットにおける重複除外については、「重複除外の概要『ページ参照 83』」をご参照ください。

3.4.2. デフォルトの復元オプション

各 Acronis エージェントには、独自のデフォルトの復元オプションがあります。エージェントがインストールされると、デフォルトのオプションは、ドキュメントで**デフォルトの設定**と呼ばれる、あらかじめ定義された値になります。復元タスクを作成する場合は、デフォルトのオプションを使用するか、このタスクのみで固有なカスタムの値でデフォルトのオプションを上書きできます。

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自体をカスタマイズすることもできます。新しい値は、後でこのコンピュータで作成するすべての復元タスクに対してデフォルトで使用されます。

デフォルトの復元オプションを表示して変更するには、コンソールを管理対象のコンピュータに接続し、上部のメニューから［**オプション**］→［**デフォルトのバックアップと復元のオプション**］→［**デフォルトの復元オプション**］を選択します。

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項目によって異なります。

- エージェントが動作する環境(Windows、Linux、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)
- ディスク バックアップから復元されるオペレーティング システム(Windows、Linux)

次の表は、使用可能な復元オプションを示しています。

	エージェント for Windows		**エージェント for Linux**		**ブータブル メディア (Linux ベースまたは PE ベース)**	
	ディスクの復元	**ファイルの復元 (ディスクのバックアップも含む)**	**ディスクの復元**	**ファイルの復元 (ディスクのバックアップも含む)**	**ディスクの復元**	**ファイルの復元 (ディスクのバックアップも含む)**
復元の前後に実行するコマンド『ページ参照 143』	+	+	+	+	PE のみ	PE のみ
復元の優先度『ページ参照 145』	+	+	+	+	-	-
ファイル レベルのセキュリティ『ページ参照 146』:						
セキュリティ設定付きでファイルを復元する	-	+	-	+	-	+
エラー対応『ページ参照 149』:						
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)	+	+	+	+	+	+
エラーが発生した場合は再試行する	+	+	+	+	+	+

その他の設定『ページ参照 150』:						
復元されたファイルに現在の日時を設定する	-	+	-	+	-	+
復元前にバックアップアーカイブをベリファイする	+	+	+	+	+	+
復元後にファイル システムを確認する	+	-	+	-	+	-
復元処理で必要な場合、自動的にコンピュータを再起動する	+	+	+	+	-	-
復元後に SID を変更する	Windows の復元	-	Windows の復元	-	Windows の復元	-
通知:						
電子メール『ページ参照 146』	+	+	+	+	-	-
Win ポップアップ『ページ参照 147』	+	+	+	+	-	-
イベントのトレース:						
Windows イベント ログ『ページ参照 148』	+	+	-	-	-	-
SNMP『ページ参照 149』	+	+	+	+	-	-

3.4.2.1. 処理の前後に実行するコマンド

このオプションは、Windows と Linux オペレーティング システム、および PE ベースのブータブル メディアで有効です。.

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。

処理の前後に実行するコマンドを指定する手順は、次のとおりです。

1. 次のオプションをオンにして、処理の前後に実行するコマンドの実行を有効にします。
   - **［復元の前に実行する］**
   - **［復元の後に実行する］**
2. 次のいずれかを実行します。
   - **［編集］**をクリックして、新しいコマンドまたはバッチ ファイルを指定する
   - 既存のコマンドまたはバッチ ファイルをドロップ ダウン リストから選択する
3. **［OK］**をクリックします。

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. **［コマンド］**フィールドにコマンドを入力するか、またはバッチ ファイルを選択します。「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。
2. **［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。
3. **［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。
4. 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。
5. **［コマンドのテスト］**をクリックして、コマンドが正しいかどうかを確認します。

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、復元タスクを失敗させる］	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				
	デフォルト 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、タスクを中止します。	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。

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. **［コマンド］**フィールドにコマンドを入力するか、またはバッチ ファイルを選択します。
2. **［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。
3. **［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。
4. コマンドの実行の成功が非常に重要である場合は、**［コマンドの実行に失敗した場合、バックアップ タスクを失敗させる］**チェックボックスをオンにします。コマンドの実行に失敗した場合、タスクの実行結果は［失敗］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タスクの実行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、**［ダッシュボード］**に表示されるログまたはエラーと警告を確認することによって追跡できます。
5. **［コマンドのテスト］**をクリックして、コマンドが正しいかどうかを確認します。

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。

3.4.2.2. 復元の優先度

このオプションは、Windows および Linux オペレーティング システムの両方で有効です。

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は使用できません。

システムで実行されるプロセスの優先度によって、そのプロセスに割り当てられる CPU やシステムのリソース量が決まります。復元処理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、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。

デフォルトの設定 - **［通常］**

復元処理の優先度を指定する手順は、次のとおりです。

次のいずれかを選択します。

- **［低］**- より多くのリソースをコンピュータ上で動作する他のプロセスのために残し、復元処理が占有するリソースを最小限にします。
- **［通常］**- 他のプロセスと同等のリソースを割り当て、標準の速度で復元処理を実行します。
- **［高］**- 他のプロセスからリソースを取り上げることによって、復元の処理速度を最大にします。

3.4.2.3. ファイル レベルのセキュリティ

このオプションは、Windows ファイルのファイル レベルのバックアップからの復元のみで有効です。

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。

デフォルトの設定 - **[セキュリティ設定付きでファイルを復元する]**

ファイルに対する NTFS アクセス許可がバックアップ中『ページ参照 132』に保持されていた場合、アクセス許可を復元するか、ファイルを復元するフォルダから NTFS アクセス許可を継承するかを選択できます。

3.4.2.4. 通知

Acronis Backup & Recovery 10 には、電子メールまたはメッセージング サービスによって復元の完了をユーザーに通知する機能があります。

電子メール

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。

このオプションは、ブータブル メディアから起動した場合には使用できません。

このオプションによって、タスクの完全なログと共に、復元タスクの正常終了、失敗、またはユーザーによる操作が必要な場合について通知する電子メールを受け取ることができます。

デフォルトの設定 - **オフ**

電子メールによる通知を設定する手順は、次のとおりです。

1. **[電子メールによる通知を送信する]** チェックボックスをオンにして、通知を有効にします。
2. **[電子メール アドレス]** フィールドに、通知の送信先の電子メール 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. **[送信する通知]** で、次の中から適切なチェックボックスをオンにします。
   - **[バックアップが正常に終了した場合]** – バックアップ タスクが正常終了した場合に通知を送信します。
   - **[バックアップが失敗した場合]** - バックアップ タスクが失敗した場合に通知を送信します。

   [ユーザーによる操作が必要な場合] チェックボックスは常にオンです。
4. 電子メール メッセージにバックアップに関連するログ エントリを含める場合は、**[すべてのログを通知する]** チェックボックスをオンにします。

5. **［追加の電子メール パラメータ］**をクリックし、次のように追加の電子メール パラメータを設定して、**［OK］**をクリックします。
   - **［差出人］**- メッセージの送信元となるユーザーの電子メール アドレスを入力します。このフィールドが空白の場合、差出人アドレスには宛先アドレスが使用されます。
   - **［暗号化を使用する］**– メール サーバーへの暗号化された接続を選択できます。SSL 暗号化または TLS 暗号化のいずれかの種類を選択できます。
   - 一部のインターネット サービス プロバイダでは、送信が許可される前に受信メール サーバーによる認証が要求されます。その場合は、**［受信メール サーバーにログオンする］**チェックボックスをオンにして POP サーバーを有効にし、次の設定を行います。
     - **［受信メール サーバー(POP)］**- POP サーバーの名前を入力します。
     - **［ポート］**- POP サーバーのポートを設定します。デフォルトでは、ポートは 110 に設定されます。
     - **［ユーザー名］**- ユーザー名を入力します。
     - **［パスワード］**- パスワードを入力します。
   - **［指定した送信メール サーバーを使用する］**チェックボックスをオンにして SMTP サーバーを有効にし、次の設定を行います。
     - **［送信メール サーバー(SMTP)］**- SMTP サーバーの名前を入力します。
     - **［ポート］**- SMTP サーバーのポートを設定します。デフォルトでは、ポートは 25 に設定されます。
     - **［ユーザー名］**- ユーザー名を入力します。
     - **［パスワード］**- パスワードを入力します。

［電子メールのテスト メッセージを送信する］をクリックし、設定が正しいかどうかを確認します。

メッセンジャー サービス(WinPopup)

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。

このオプションは、ブータブル メディアから起動した場合には使用できません。

このオプションによって、復元タスクの正常終了、失敗、またはユーザーによる操作が必要な場合について、ポップアップウィンドウによる通知を受け取ることができます。

デフォルトの設定 - **オフ**

ポップアップウィンドウによる通知を設定する前に、タスクを実行するコンピュータとメッセージを受け取るコンピュータの両方で Messenger サービスが開始されていることを確認します。

Microsoft Windows Server 2003 ファミリでは、Messenger サービスはデフォルトでは開始されません。サービスのスタートアップの種類を［自動］に変更してからサービスを開始します。

ポップアップウィンドウによる通知を設定する手順は、次のとおりです。

1. **［ポップアップウィンドウによる通知を送信する］**チェックボックスをオンにします。
2. **［コンピュータ名］**フィールドに、通知の送信先となるコンピュータの名前を入力します。複数の名前はサポートされていません。
3. **［送信する通知］**で、次の中から適切なチェックボックスをオンにします。
   - **［復元が正常に終了した場合］**- 復元タスクが正常終了した場合に通知を送信します。
   - **［復元が失敗した場合］**- 復元タスクが失敗した場合に通知を送信します。

   ［ユーザーによる操作が必要な場合］- 処理中にユーザーによる操作が必要になった場合、通知を送信します。常にオンです。
4. **［テスト メッセージの送信］**をクリックし、設定が正しいかどうかを確認します。

3.4.2.5. イベント トレース

管理対象のコンピュータで実行された復元処理のイベントを Windows のアプリケーション イベント ログに表示したり、指定した SNMP マネージャに送信したりすることができます。

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。

このオプションは、ブータブル メディアから起動した場合には使用できません。

このオプションでは、管理対象のコンピュータで動作するエージェントが、復元処理のイベントを 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、または**［コントロール パネル］→［管理ツール］→［イベント ビューア］**を選択します。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。

デフォルトの設定 - **［コンピュータ オプションの設定を使用する］**

復元処理のイベントを Windows のアプリケーション イベント ログに記録するかどうかを選択する手順は、次のとおりです。

次のいずれかを選択します。

- **［コンピュータ オプションの設定を使用する］**- コンピュータ オプションで指定された設定を使用します。詳細については、「コンピュータ オプション『ページ参照 109』」をご参照ください。
- **［次の種類のイベントをログに記録する］**- 復元処理のイベントをアプリケーション イベント ログに記録します。ログに記録するイベントの種類を指定します。
  - **［すべてのイベント］**- すべてのイベント(情報、警告、およびエラー)をログに記録します。
  - **［エラーと警告］**
  - **［エラーのみ］**
- **［ログに記録しない］**- 復元処理のイベントをアプリケーション イベント ログに記録しません。

SNMP 通知

このオプションは、Windows および Linux オペレーティング システムの両方で有効です。

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は使用できません。

このオプションでは、管理対象のコンピュータで動作するエージェントが、指定した簡易ネットワーク管理プロトコル(SNMP)マネージャに復元処理のイベントを送信する必要があるかどうかを定義します。送信するイベントの種類を選択できます。

Acronis Backup & Recovery 10 は、次の簡易ネットワーク管理プロトコル(SNMP)オブジェクトを SNMP 管理アプリケーションに送信します。

1.3.6.1.4.1.24769.100.200.1.0 - イベントの種類を特定する文字列(情報、警告、エラー)

1.3.6.1.4.1.24769.100.200.2.0 - イベントの説明テキストを含む文字列(Acronis Backup & Recovery 10 によってログに記録されるメッセージと同じです)。

デフォルトの設定 - **[コンピュータ オプションの設定を使用する]**

復元処理のイベントを SNMP マネージャに送信するかどうかを選択する手順は、次のとおりです。

次のいずれかを選択します。

- **[コンピュータ オプションの設定を使用する]** - コンピュータ オプションで指定された設定を使用します。詳細については、「コンピュータ オプション『ページ参照 109』」をご参照ください。
- **[復元処理イベントに対して個別に SNMP 通知を送信する]**– 指定した SNMP マネージャに復元処理のイベントを送信します。
  - **[送信するイベントの種類]** - **[すべてのイベント]**、**[エラーと警告]**、または **[エラーのみ]** のいずれかから送信するイベントの種類を選択します。
  - **[サーバー名/IP]** - メッセージの送信先となる SNMP 管理アプリケーションを実行するホストの名前または IP アドレスを入力します。
  - **[コミュニティ]** - SNMP 管理アプリケーションを実行するホストと送信元コンピュータの両方が所属する SNMP コミュニティの名前を入力します。一般的なコミュニティは "public" です。

  [テスト メッセージを送信する] をクリックし、設定が正しいかどうかを確認します。

[SNMP 通知を送信しない] - 復元処理イベントの SNMP マネージャへの送信を無効にします。

3.4.2.6. エラーの処理

これらのオプションは、Windows と Linux オペレーティング システム、およびブータブル メディアで有効です。

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。

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)

デフォルトの設定 - **オフ**

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。

[エラーが発生した場合は再試行する]

デフォルトの設定 - **オン、試行回数: 5 回、試行間隔: 30 秒**

修復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、ネットワーク上の場所が使用できない場合、30 秒ごとに 5 回までその場所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。

3.4.2.7. その他の設定

次のチェックボックスをオンまたはオフにして、復元処理のその他の設定を指定します。

[復元されたファイルに現在の日時を設定する]

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。

デフォルトの設定 - **オン**

このオプションでは、ファイルの日付/時刻をアーカイブから復元するか、現在の日付/時刻を割り当てるかを定義します。

[復元前にバックアップをベリファイする]

デフォルトの設定 - **オフ**

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。

[復元後にファイル システムを確認する]

このオプションは、ディスクまたはボリュームを復元する場合にのみ有効です。

ブータブル メディアから起動した場合、このオプションは NTFS ファイル システムに対しては使用できません。

デフォルトの設定 - **オフ**

このオプションでは、ディスクまたはボリュームを復元した後に、ファイル システムの整合性を確認するかどうかを定義します。

[復元処理で必要な場合、自動的にコンピュータを再起動する]

このオプションは、オペレーティング システムを実行するコンピュータ上で復元を実行する場合に有効です。

デフォルトの設定 - **オフ**

このオプションでは、復元で必要な場合に、自動的にコンピュータを再起動するかどうかを定義します。これは、復元するボリュームがオペレーティング システムによってロックされている場合などが該当します。

[復元後にコンピュータを再起動する]

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。

デフォルトの設定 - **オフ**

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。

[復元の完了後に SID を変更する]

デフォルトの設定 - **オフ**

Acronis Backup & Recovery 10 は、復元されたシステムに対して一意のセキュリティ識別子(SID)を生成できます。元の環境にシステムを復元する場合、または元のシステムを置き換えるシステム レプリカを作成する場合、新しい SID は必要はありません。同じワークグループまたはドメインで元のシステムと復元するシステムを並行して運用する場合は、新しい SID を生成します。

3.4.2.8. VM 電源管理

これらのオプションは、仮想サーバー上の仮想コンピュータで有効です。

また、これらのオプションは、仮想コンピュータ用の Acronis エージェントが仮想サーバーにインストールされている場合にのみ使用できます。

[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]

デフォルトの設定 - **オン**

既存の仮想コンピュータがオンラインになっている場合、そのコンピュータに復元することはできません。したがって、復元タスクが開始されるとすぐに、コンピュータの電源が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。

復元の前に仮想コンピュータの電源を手動でオフにする場合は、このオプションのチェックボックスをオフにします。

復元が完了したら、ターゲット仮想コンピュータの電源をオンにします。

デフォルトの設定 - **オフ**

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。

仮想コンピュータの電源を自動的に投入する必要がある場合は、このオプションのチェックボックスをオンにします。

4. 格納域

格納域とは、バックアップ アーカイブを保存する場所です。格納域は、簡単に使用したり管理できるように、アーカイブのメタデータに関連付けられています。このメタデータを参照することにより、格納域に保存されたアーカイブとバックアップの処理をすばやく簡単に行うことができます。

格納域は、ローカル ドライブまたはネットワーク上のドライブ、取り外し可能なメディア、または Acronis Backup & Recovery 10 ストレージ ノードにアタッチしたテープ デバイス上に構成できます。

格納域のサイズまたは格納域内のバックアップの数を制限する設定はありません。クリーンアップを使用して各アーカイブのサイズを制限できますが、格納域に保存するアーカイブの合計サイズはストレージのサイズによってのみ制限されます。

格納域を作成する理由

バックアップ アーカイブの保存先ごとに格納域を作成することをお勧めします。このことによって、次のように作業が簡単になります。

格納域への迅速なアクセス

アーカイブの保存先となるフォルダのパスを記憶しておく必要はありません。格納域の一覧を使用すると、バックアップ計画またはタスクの作成時にアーカイブまたはアーカイブの保存先を選択する必要がある場合に、フォルダ ツリーをたどることなくすばやくアクセスできます。

簡単なアーカイブ管理

格納域は、［**ナビゲーション**］ペインからのアクセスに使用できます。格納域を選択した後で、そこに保存されたアーカイブを参照して、次のアーカイブ管理操作を実行できます。

- 各アーカイブに含まれているバックアップの一覧を取得する。
- バックアップからデータを復元する。
- バックアップの内容を調べる。
- 格納域内のすべてのアーカイブまたは個々のアーカイブやバックアップをベリファイする。
- バックアップから物理ディスクにファイルをコピーするために、ボリューム バックアップをマウントする。
- アーカイブと、アーカイブに含まれているバックアップを安全に削除する。

格納域を作成しておくことを強くお勧めしますが、必須ではありません。ショートカットを使用せずに、常にアーカイブの格納域のフル パスを指定することもできます。格納域を作成しなくても、アーカイブとバックアップの削除を除く上記のすべての操作を実行することができます。

格納域を作成する操作を実行すると、［**ナビゲーション**］ペインの［**格納域**］セクションに格納域名が追加されます。

集中管理用格納域と個人用格納域

集中管理用格納域とは、管理サーバーの管理者によって割り当てられ、バックアップ アーカイブのストレージとして使用されるネットワーク上の場所です。集中管理用格納域は、ストレージ ノード(管理対象の格納域)によって管理することも管理対象外にすることもできます。

コンソールを管理対象のコンピュータに直接接続して格納域を作成した場合、この格納域は個人用格納域と呼ばれます。個人用格納域は、管理対象のコンピュータごとに固有です。

[格納域] ビューの操作方法

[格納域](ナビゲーション ペイン上) - 格納域ツリーの最上部にある要素。この項目をクリックすると、集中管理用格納域と個人用格納域のグループが表示されます。

[集中管理]。このグループは、コンソールが管理対象のコンピュータまたは管理サーバーに接続されている場合に有効です。このグループを展開すると、管理サーバーの管理者が追加した集中管理用格納域の一覧が表示されます。

格納域ツリー内の任意の集中管理用格納域をクリックすると、この格納域の詳細ビュー『ページ参照 156』が開き、格納域『ページ参照 157』とそこに保存されたアーカイブ『ページ参照 195』およびバックアップ『ページ参照 196』に対して操作を実行できます。

[個人用]。このグループは、コンソールが管理対象のコンピュータに接続されている場合に有効です。このグループを展開すると、管理対象のコンピュータで作成された個人用格納域の一覧が表示されます。

格納域ツリー内の任意の個人用格納域をクリックすると、この格納域の詳細ビュー『ページ参照 192』が開き、格納域『ページ参照 193』とそこに保存されたアーカイブ『ページ参照 195』およびバックアップ『ページ参照 196』に対して操作を実行できます。

4.1. 集中管理用格納域

集中管理用格納域とは、管理サーバーの管理者によって割り当てられ、バックアップ アーカイブのストレージとして使用されるネットワーク上の場所です。集中管理用格納域は、ストレージ ノードによって管理することも管理対象外にすることもできます。集中管理用格納域に保存されるアーカイブの合計数とサイズは、ストレージのサイズによってのみ制限されます。

管理サーバーの管理者が集中管理用格納域の作成を実行するとすぐに、サーバーに登録されているコンピュータすべてに格納域のパスと名前が配布されます。格納域のショートカットが、**[格納域]の[集中管理]**グループ内のコンピュータ上に表示されます。ローカルの計画を含むコンピュータに存在するすべてのバックアップ計画で集中管理用格納域を使用することができます。

管理サーバーに登録されていないコンピュータ上では、集中管理用格納域にバックアップする権限を持つユーザーが格納域のフル パスを指定することで、バックアップを実行できます。格納域が管理対象である場合は、格納域に保存される他のアーカイブと同様に、ユーザーのアーカイブがストレージ ノードによって管理されます。

管理対象の格納域

管理対象の格納域とは、ストレージ ノードによって管理される集中管理用格納域です。ストレージ ノードは、管理対象の格納域に保存された各アーカイブに対して、ストレージ ノード側のクリーンアップ『ページ参照 416』およびストレージ ノード側のベリファイ『ページ参照 417』を実行します。管理対象の格納域を作成する場合、管理者は、ストレージ ノードが実行するその他の処理(重複除外『ページ参照 83』、暗号化)を指定することができます。管理処理はキャンセルすることも無効にすることもできません。これらの処理は、格納域が削除されない限り、格納域に保存されているすべてのアーカイブに対して実行されます。

管理対象の格納域は自己完結型です。つまり、ストレージ ノードが格納域を管理するために必要なすべてのメタデータが含まれています。ストレージ ノードが失われたりデータベースが破損した場合は、新しいストレージ ノードがメタデータを取得してデータベースを再作成します。格納域が別のストレージ ノードに接続される場合、同じ手順が実行されます。

管理対象の格納域へのアクセス

管理対象の格納域にバックアップするには、ユーザーは、ストレージ ノードがインストールされているコンピュータのアカウントが必要になります。格納域におけるユーザーの権限の範囲は、ストレージ ノード上のユーザーの権限によって異なります。Users グループのメンバであるユーザーは、自身のアーカイブを表示および管理できます。Administrators グループのメンバは、ストレージ ノードに保存されたすべてのアーカイブを表示および管理できます。管理対象のコンピュータの Administrators グループのメンバであるユーザーは、このコンピュータの任意のユーザーが作成したアーカイブを表示および管理できます。

ユーザー権限によって異なる権限の詳細については、「ストレージ ノードでのユーザー権限『ページ参照 93』」をご参照ください。

管理対象外の格納域

管理対象外の格納域とは、ストレージ ノードによって管理されない集中管理用格納域です。管理対象外の格納域にアクセスするには、ユーザーは、ネットワークからその場所にアクセスする権限が必要になります。

管理対象外の格納域内のファイルに対する読み取り/書き込みアクセス許可を持つユーザーは、次の操作を行うことができます。

- 管理対象外の格納域にデータをバックアップする。
- 管理対象外の格納域に配置されたバックアップからデータを復元する。
- 管理対象外の格納域に配置されたすべてのアーカイブを表示および管理する。

4.1.1. ［集中管理用格納域］ビューを使用した作業

ここでは、**［集中管理用格納域］**ビューの主要な要素について簡単に説明し、それらの使用方法を示します。

［格納域］ツールバー

このツールバーには、選択した集中管理用格納域を使用した操作を実行できる操作ボタンが含まれています。詳細については、「集中管理用格納域での操作『ページ参照 157』」をご参照ください。

汎例付きの円グラフ

円グラフを見ると、格納域の負荷を推測することができます。これには、格納域の空き領域と使用中の領域の比率が示されます。円グラフは、格納域がテープ ライブラリに配置される場合には使用できません。

- 空き領域。格納域が配置されたストレージ デバイス上の領域です。たとえば、格納域がハード ディスク上に配置されている場合、格納域の空き領域は該当するボリュームの空き領域になります。

- 使用中の領域。バックアップ アーカイブとそのメタデータ(格納域に配置されている場合)の合計サイズです。

汎例には、格納域に関する次の情報が表示されます。

- (管理対象の格納域のみ)格納域を管理するストレージ ノードの名前
- 格納域のフル パス
- 格納域に保存されているアーカイブとバックアップの合計数
- 元のデータ サイズに対する使用中の領域の比率
- (管理対象の格納域のみ)重複除外『ページ参照 83』の状態(オン、オフ)
- (管理対象の格納域のみ)暗号化の状態(はい、いいえ)

格納域の内容

［格納域の内容］セクションには、アーカイブ テーブルとツールバーが含まれています。アーカイブ テーブルには、格納域に保存されているアーカイブとバックアップが表示されます。アーカイブ ツールバーを使用して、選択したアーカイブとバックアップに対する操作を実行します。バックアップの一覧は、アーカイブの名前の左側にある「+」記号をクリックすると展開されます。すべてのアーカイブは、次のタブのいずれかで種類ごとにグループ化されます。

- **［ディスク アーカイブ］**タブには、ディスク バックアップまたはボリューム バックアップ(イメージ)を含むすべてのアーカイブが一覧表示されます。
- **［ファイル アーカイブ］**タブには、ファイル バックアップを含むすべてのアーカイブが一覧表示されます。

関連セクション:

格納域に保存されたアーカイブの操作『ページ参照 195』

バックアップの操作『ページ参照 196』

アーカイブのフィルタ処理と並べ替え『ページ参照 198』

[アクションとツール] ペインのバー

- **[格納域名]** - 格納域ツリー内の格納域をクリックする際に、**[アクション]** バーが使用できます。格納域のツールバーの操作を複製します。
- **[アーカイブ名]** - アーカイブ テーブルのアーカイブを選択する際に、**[アクション]** バーが使用できます。アーカイブのツールバーの操作を複製します。
- **[バックアップ名]** - アーカイブを展開して、そのバックアップのいずれかをクリックする際に、**[アクション]** バーが使用できます。アーカイブのツールバーの操作を複製します。

4.1.2. 集中管理用格納域での操作

ここで説明するすべての操作は、格納域ツールバーで対応するボタンをクリックすると実行されます。これらの操作は、**[格納域名] アクション** バー(**[アクションとツール]** ペイン) と、メイン メニューの **[格納域名] アクション** 項目からアクセスすることもできます。

集中管理用格納域を使用して操作を実行するためのガイドラインを次に示します。

目的	操作手順
管理対象の格納域または管理対象外の格納域を作成する	1 **[作成]** をクリックします。 2 **[種類]** フィールドで、格納域の種類として **[管理対象]** と **[管理対象外]** のいずれかを選択します。 集中管理用格納域の作成手順については、以下のセクションで詳しく説明しています。 • 管理対象の集中管理用格納域の作成『ページ参照 159』 • 管理対象外の集中管理用格納域の作成『ページ参照 162』
管理対象の格納域または管理対象外の格納域を編集する	1 格納域を選択します。 2 **[編集]** をクリックします。 選択した格納域(管理対象または管理対象外)に応じて、それぞれの [編集] ページが開きます。 • **[管理対象の格納域の編集]** ページでは、暗号化パスワード(格納域が暗号化されている場合)と [コメント] フィールドを変更できます。 • **[管理対象外の格納域の編集]** ページでは、[コメント] フィールドだけを編集できます。

格納域をベリファイする	1　格納域を選択します。 2　**［ベリファイ］**をクリックします。 ［ベリファイ］『ページ参照 282』ページが開き、既に選択されている格納域がソースとして表示されます。格納域のベリファイでは、この格納域内のすべてのアーカイブが確認されます。
格納域を削除する	1　格納域を選択します。 2　**［削除］**をクリックします。 格納域に保存されているアーカイブを保持するか、格納域と共にすべてのアーカイブを削除するかどうかを確認するメッセージが表示されます。この格納域を使用する計画とタスクは失敗します。 管理対象の格納域のアーカイブを保持するよう選択した場合、格納域はストレージ ノードから切り離されます。後から、同じストレージ ノードまたは別のストレージ ノードにこの格納域を接続することができます。
管理対象外の格納域を参照する	1　管理対象外の格納域を選択します。 2　**［参照］**をクリックします。 格納域は、標準のファイル マネージャ プログラムを使用して参照することができます。
内容を保持したまま削除された管理対象の格納域を接続する	**［アタッチ］**をクリックします。 管理対象の格納域をストレージ ノードに接続する手順については、「管理対象の格納域の接続『ページ参照 162』」で詳しく説明しています。
格納域にアクセスするためのユーザー ログイン情報を変更する	**［ユーザーの変更］**をクリックします。 ユーザー ログイン情報の変更は、共有ストレージにのみ存在する格納域で有効です。
格納域の情報を更新する	**［更新］**をクリックします。 格納域の内容の確認中に、アーカイブを格納域に追加、削除、変更することができます。**［更新］**をクリックして、格納域の情報を最新の変更内容によって更新します。
管理対象の格納域上のテープ ライブラリでの操作	
テープ ラベルを定義し、管理対象の格納域にあるテープ ライブラリの一覧の収集を実行する	**［テープの管理］**をクリックします。 **［テープ管理］**ウィンドウで、テープのラベルを定義し、一覧を更新します。詳細については、「テープ ライブラリの管理『ページ参照 170』」をご参照ください。
管理対象の格納域にあるテープを再スキャンする	**［テープの再スキャン］**をクリックします。 再スキャンでは、ユーザーが選択したテープの内容に関する情報を読み取り、ストレージ ノード データベースを更新します。 この操作については、「再スキャン『ページ参照 171』」で詳しく説明しています。

4.1.2.1. 管理対象の集中管理用格納域の作成

管理対象の集中管理用格納域を作成する手順は、次のとおりです。

格納域

[名前]

格納域の一意の名前を指定します。2 つの集中管理用格納域を同じ名前で作成することはできません。

[コメント]

(オプション)作成する格納域の特徴を表す説明を入力します。

[種類]

[管理対象] を選択します。

[ストレージ ノード]

格納域を管理する Acronis Backup & Recovery 10 ストレージ ノードを選択します。ストレージ ノードのアクセス ログイン情報の入力が必要になる場合があります。

[パス] 『ページ参照 160』

格納域を作成する場所を指定します。管理対象の集中管理用格納域は、ネットワーク共有、SAN、NAS、またはストレージ ノードのローカルのハード ディスク ドライブに配置することができます。

[データベースのパス] 『ページ参照 160』

格納域専用のデータベースの作成先となる、ストレージ サーバー上のローカル フォルダを指定します。このデータベースには、アーカイブをカタログ化し、重複除外を実行するために必要となるメタデータが保存されます。

[重複除外]

(オプション)格納域でアーカイブの重複除外を有効にするかどうかを選択します。重複除外により、アーカイブおよびバックアップ トラフィックによって使用されるストレージ領域が最小限に抑えられます。重複したファイルやディスク ブロックなどの冗長なデータを解消することによって、格納域内のアーカイブのサイズが縮小されます。

重複除外をテープ デバイス上で実行することはできません。

重複除外のしくみの詳細については、「重複除外『ページ参照 83』」をご参照ください。

[圧縮]

(オプション)重複除外データ ストアを圧縮するかどうかを選択します。この設定は、重複除外が有効な場合にのみ使用できます。

［暗号化］『ページ参照 161』

(オプション)暗号化で格納域を保護するかどうかを選択します。格納域に書き込まれるすべてのデータは暗号化され、格納域から読み取られるすべてのデータはストレージ ノードで透過的に暗号化解除されます。このとき、ストレージ ノードに保存されている格納域専用の暗号化キーが使用されます。

すべての必要な処理を実行したら、**［OK］**をクリックして、管理対象の格納域の作成を実行します。

格納域のパス

管理対象の格納域の作成先のパスを指定する手順は、次のとおりです。

1. フォルダのフル パスを**［パス］**フィールドに入力するか、フォルダ ツリーから目的のフォルダを選択します。管理対象の格納域は次の場所で構成できます。
   - ストレージ ノードのローカルのハード ディスク ドライブ
   - ネットワーク共有
   - SAN(Storage Area Network)
   - NAS(Network Attached Storage)
   - ストレージ ノードにローカル接続されたテープ ライブラリ

   選択した場所に格納域用の新しいフォルダを作成するには、**［フォルダの作成］**をクリックします。
2. **［OK］**をクリックします。

格納域は、空のフォルダにのみ作成できます。

重複除外された管理対象の格納域を FAT 32 ボリューム上に作成することは推奨されません。これは、このような格納域が、すべての重複除外された項目を 2 つの大きいファイルに保存するためです。FAT ファイル システムにおける最大ファイル サイズは 4GB に制限されているため、ストレージ ノードがこの制限に到達した場合に動作を停止する可能性があります。

*フォルダのアクセス許可では、ストレージ ノードのサービスを実行するユーザー アカウント(デフォルトでは、**ASN User**)に対して、フォルダへの書き込みを許可する必要があります。アクセス許可を割り当てる際には、(**［Everyone］**だけではなく)ユーザー アカウントを明示的に指定します。*

格納域データベースのパス

格納域データベースの作成先のパスを指定する手順は、次のとおりです。

1. ストレージ ノードの**［ローカル フォルダ］**で、目的のフォルダを選択するか、**［パス］**フィールドにフォルダのフル パスを入力します。

   データベース用の新しいフォルダを作成するには、**［フォルダの作成］**をクリックします。
2. **［OK］**をクリックします。

格納域のデータベース用のフォルダを選択する際は、以下の考慮事項に従います。

- フォルダのサイズが大規模になる可能性があります。使用済みの領域 8TB につき 200GB、つまり約 2.5% を使用する可能性があります。
- フォルダのアクセス許可では、ストレージ ノードのサービスを実行するユーザー アカウント(デフォルトでは、**ASN User**)に対して、フォルダへの書き込みを許可する必要があります。アクセス許可を割り当てる際には、(［**Everyone**］だけではなく)ユーザー アカウントを明示的に指定します。

格納域の暗号化

暗号化によって格納域を保護する場合、格納域に書き込まれるすべてのデータは暗号化され、格納域から読み取られるすべてのデータはストレージ ノード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格納域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、格納域の内容はストレージ ノードにアクセスしなければ、暗号化解除することはできません。

この暗号化は、バックアップ計画で指定されてエージェントによって実行されるアーカイブの暗号化とは関係ありません。既にアーカイブが暗号化されている場合、ストレージ ノード側の暗号化は、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。

暗号化を使用して格納域を保護する手順は、次のとおりです。

1. ［**暗号化する**］チェックボックスをオンにします。
2. ［**パスワードの入力**］**フィールドにパスワードを入力します。**
3. ［**パスワードの確認入力**］フィールドにパスワードを再入力します。
4. 次のいずれかを選択します。
   - ［**AES 128**］- 格納域の内容は、128 ビットのキーの AES(Advanced Standard Encryption)アルゴリズムを使用して暗号化されます。
   - ［**AES 192**］- 格納域の内容は、192 ビットのキーの AES アルゴリズムを使用して暗号化されます。
   - ［**AES 256**］- 格納域の内容は、256 ビットのキーの AES アルゴリズムを使用して暗号化されます。
5. ［**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格納域に保存されたアーカイブを暗号化する時間は長くなりますが、アーカイブ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に保存されませんが、パスワード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、アーカイブは権限のない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。

4.1.2.2. 管理対象外の集中管理用格納域の作成

管理対象外の集中管理用格納域を作成する手順は、次のとおりです。

格納域

［名前］

格納域の一意の名前を指定します。2 つの集中管理用格納域を同じ名前で作成することはできません。

［コメント］

格納域の特徴を表す説明を入力します。

［種類］

［管理対象外］を選択します。

［パス］『ページ参照 162』

格納域を作成する場所を指定します。

すべての必要な処理を実行したら、**［OK］**をクリックして、管理対象外の集中管理用格納域の作成を実行します。

格納域のパス

管理対象の格納域の作成先のパスを指定する手順は、次のとおりです。

1. フォルダのフル パスを**［パス］**フィールドに入力するか、フォルダ ツリーから目的のフォルダを選択します。管理対象外の格納域は次の場所で構成できます。
   - ネットワーク共有
   - SAN(Storage Area Network)
   - NAS(Network Attached Storage)
   - FTP サーバーおよび SFTP サーバー

   FTP 仕様の原文に記載されているように、FTP サーバーにアクセスするのに必要なログイン情報は、ネットワーク上をテキスト形式で転送されます。このことは、ユーザー名とパスワードが、パケット スニファを使用した盗聴者によって傍受される可能性があることを意味します。

   格納域用の新しいフォルダを作成するには、  **［フォルダの作成］**をクリックします。

   格納域は、空のフォルダにのみ作成できます。

2. **［OK］**をクリックします。

4.1.2.3. 管理対象の格納域の接続

ストレージ ノードによって管理される格納域は、別のストレージ ノードに接続することができます。ストレージ ノードのハードウェアを取り外す場合、ストレージ ノードが失われた場合、またはストレージ ノード間の負荷分散を行う場合に、これを行う必要がある場合があります。この結果、最初のノードが格納域の管理を停止します。2 番目のノードは、格納域内のアーカイブをスキャンし、格納域に対応するデータベースを作成して書き込み、格納域の管理を開始します。

管理対象の格納域を削除する際に、格納域に含まれているアーカイブを保持することができます。このような削除の結果生じた場所も、同じストレージ ノードまたは別のストレージ ノードに接続することができます。

個人用格納域または管理対象外の集中管理用格納域は接続できません。

管理対象の格納域をストレージ ノードに接続する手順は、次のとおりです。

格納域

[ストレージ ノード]

格納域を管理する Acronis Backup & Recovery 10 ストレージ ノードを選択します。

[パス]

アーカイブが保存されている場所のパスを指定します。

[データベースのパス]

格納域専用のデータベースの作成先となる、ストレージ サーバー上のローカル フォルダを指定します。このデータベースには、アーカイブをカタログ化し、重複除外を実行するために必要となるメタデータが保存されます。

[パスワード]

暗号化された格納域の場合は、暗号化パスワードを指定します。

すべての必要な手順を実行したら、**[OK]** をクリックして、格納域の接続を実行します。この手順は、ストレージ ノードがアーカイブをスキャンし、データベースにメタデータを書き込み、格納域が当初から重複除外されていた場合にアーカイブを重複除外する必要があるため、かなり長い間続く場合があります。

4.1.3. テープ ライブラリ

ここでは、バックアップ アーカイブを保存する格納域として自動テープ デバイスを使用する方法について詳細に説明します。

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 カートリッジを保持する複数(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 カートリッジを移動するための 1 つ以上のローダー(自動メカニズム)
- バーコード リーダー(オプション)

4.1.3.1. 概要

Acronis Backup & Recovery 10 では、Acronis Backup & Recovery 10 ストレージ ノードによってテープ ライブラリを完全にサポートします。ストレージ ノードは、テープ ライブラリが接続されたコンピュータにインストールする必要があります。ストレージ ノードでは、アーカイブを保持するために複数のテープ ライブラリを同時に使用できます。

テープ ライブラリ メディアを管理するため、ストレージ ノードは Windows のリムーバブル記憶域マネージャ(RSM)を使用します。詳細については、「RSM メディア プール『ページ参照 166』」をご参照ください。

ストレージ ノードの専用データベースは、テープに書き込まれるバックアップ内容に関する情報を保持します。これにより、一部の操作(クリーンアップ『ページ参照 415』など)は、メディアにアクセスせずに高速で実行できます。内容に関する情報はデータベースに保存されているので、テープ ライブラリがオフのときでも、テープに入っているバックアップ アーカイブの内容をコンソールから表示できます。データの増分バックアップまたは差分バックアップを作成するために、プログラムは、完全バックアップの入っているテープのロード、マウント、巻き戻し、読み取りを行う代わりに、データベースを使用します。ただし、バックアップのベリファイ『ページ参照 423』や、バックアップからのデータの復元などの操作では、テープを読み取る必要があります。

テープ ライブラリはエージェントをインストールしたコンピュータにローカルで接続できますが、この状況では、テープ ライブラリが単独のテープ ドライブと見なされます。エージェントはこのようなデバイスを使用してデータ バックアップを読み書きできますが、バックアップの形式は、ストレージ ノードによって書き込まれたテープ上のバックアップの形式と異なります。Acronis Backup & Recovery 10 を使用して、製品の別バージョンの異なるコンポーネントによって書き込まれたテープ上のアーカイブの読み取りの詳細については、「テープ互換性の表『ページ参照 56』」をご参照ください。

Acronis Backup & Recovery 10 を使用すると、メディアによるバックアップの分散を設定できます。たとえば、個別のテープ セットを使用して特定のデータをバックアップできます。他のすべてのデータのバックアップは、この個別のテープ セットに含まれない、現在マウントされているテープに書き込まれます。詳細については、「テープ サポート『ページ参照 138』」をご参照ください。

バックアップ スキーム(GFS(Grandfather-Father-Son)『ページ参照 39』、ハノイの塔『ページ参照 43』)は、テープ ライブラリでのバックアップに対して効果的なスケジュールや保持ルールを作成する上で大いに役立ちます。バックアップ スキームとテープ オプションを組み合わせると、バックアップの削除後に空と見なされるテープを自動モードで再利用できます。詳細については、「テープ ローテーション『ページ参照 174』」をご参照ください。

4.1.3.2. ハードウェア

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 カートリッジを保持する複数(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 カートリッジを移動するための 1 つ以上のローダー(自動メカニズム)
- バーコード リーダー(オプション)

テープごとに、次の内容の特別なラベルをカートリッジの側面に貼る場合があります。

- 通常はローダーに取り付けた特別のリーダーによってスキャンするバーコード
- 読み取り可能バーコードのデジタル値

これらのラベルは、テープ ライブラリ内または特にサイト外のストレージにあるテープの識別に使用します。

テープ ライブラリ内のすべてのカートリッジにバーコードが付いていると、ライブラリはソフトウェアによってすぐに自動管理できます。

テープ ライブラリは、大容量のデータ ストレージにとってコスト効率のよいソリューションです。そのうえ、データ セキュリティ強化のためにカートリッジをサイト外に保管できるので、テープはアーカイブに最適です。ただし、データが少量の場合でも、テープ ライブラリからの読み取りは他の種類のデータ ストレージからの読み取りより大幅に時間がかかります(数秒から数分)。テープの最適な使用方法は、「読み書き要求をより少なく、データ量をより大きくする」ことです。したがって、大量のデータの規則正しいアクセスの方が、少量のデータのランダム アクセスよりテープ ライブラリに適しています。

4.1.3.3. 制限

テープ ライブラリの使用には次の制限があります。

1. テープ上に保存されたアーカイブの統合『ページ参照 429』操作はできません。1 つの個別バックアップをテープから削除することもできません。テープに保存されたバックアップをすべて削除することは可能です。ただし、この操作を行うと、削除されたバックアップをベースとして、他のテープに保存されているすべての増分バックアップと差分バックアップがデータの復元に使用できなくなります。**[カスタム]** バックアップ計画の保持ルールの **[依存関係のあるバックアップを削除する場合]** → **[バックアップの統合]** オプションは無効になります。 **[依存するすべてのバックアップが削除の対象になるまでバックアップを保持する]** オプションのみ使用できます。
2. テープ ストレージ デバイス上に保存されたアーカイブの重複除外『ページ参照 429』はできません。
3. テープに保存されたディスク バックアップからのファイルの復元は可能ですが、非常に長い時間がかかることがあります。

4. ストレージ ノードによって書き込まれたバックアップを含むテープはテープ形式が異なるので、エージェントをインストール済みのコンピュータにローカル接続したテープ デバイスで読み取ることができません。Acronis Backup & Recovery 10 を使用して、製品の別バージョンの異なるコンポーネントによって書き込まれたテープ上のアーカイブの読み取りの詳細については、「テープ互換性の表『ページ参照 56』」をご参照ください。
5. バーコード プリンタは使用しません。

4.1.3.4. RSM メディア プール

Acronis Backup & Recovery 10 は、Windows のリムーバブル記憶域マネージャ(RSM)を使用して、テープ ライブラリで使用するテープ カートリッジを管理します。

さまざまなプログラムから個別にメディアにアクセスするため、RSM は論理メディア グループである「メディア プール」を使用します。マネージャには、**システム**と**アプリケーション**という 2 つのカテゴリのメディア プールがあります。

システム メディア プールには、**空き**プール、**インポート** プール、および**非認識**プールがあります。**システム** プールは、アプリケーションによって現在使用されていないメディアを保持します。**空き**プールは空と見なされ、アプリケーションから使用できるメディアを保持します。**インポート** プールと**非認識**プールは、特定のライブラリでの新しいメディア用の一時的なプールです。

アプリケーションは、RSM を通して、適切な名前を持つ専用プールの取得、**空き**プールから専用プールへのメディアの移動、適切な目的による専用プールのメディアの使用、**空き**プールへのメディアの返却などを行います。

Acronis Backup & Recovery 10 ストレージ ノードは、**Acronis** プールに属するテープを管理します。

テープ ライブラリのスロットに未使用テープを入れると、すべてのテープは自動的に**空き**プールに入ります。

テープが使用済みのときは、RSM はそのテープに関連した登録アプリケーションを探します。アプリケーションが見つからないと、RSM はテープを**非認識**プールに移動します。アプリケーションが見つからず、RSM データベースにテープに関する情報がない場合、テープは**インポート** プールに移動されます。RSM データベースに情報があれば、テープはそのアプリケーションの専用プールに移動されます。

Acronis Backup & Recovery 10 ストレージ ノードの RSM は、Acronis True Image Echo、Acronis True Image 9.1 製品ファミリ、および Acronis Backup & Recovery 10 のコンポーネントによって書き込まれたテープを検出できます。ストレージ ノードは、一覧の収集『ページ参照 171』操作で、Acronis 形式で書き込まれたすべてのテープを **Acronis** プールに保存します。

Acronis Backup & Recovery 10 コンポーネントは**非認識**プールを使用しません。このプールからテープを強制的に利用するには、リムーバブル記憶域スナップイン(**［コントロール パネル］→［管理ツール］→［コンピュータの管理］→［リムーバブル記憶域］→［メディア］**)を使用して、テープを**空き**プールに移動します。

***空き**プールに移動されたテープは空だと見なされ、アプリケーションから書き込めるようになります。したがって、テープ データは失われます。*

テープからすべてのバックアップが削除されても、そのテープは**空き**プールに戻りません。テープは、再利用のための空のテープとして **Acronis** プールに残ります。ストレージ ノードは、新しいテープが必要になると、最初に **Acronis** プールにある空のテープを探し、次に**空き**プールを探します。

その後、Acronis Backup & Recovery 10 ストレージ ノードは、**Acronis** プールに属するテープだけを処理します。

4.1.3.5. テープ ライブラリの操作

Acronis Backup & Recovery 10 ストレージ ノードがインストールされたコンピュータにテープ ライブラリ デバイスを接続しているときは、ストレージ ノードの管理下にあるデバイス上にアーカイブ格納域を作成するだけで、テープ ライブラリにバックアップできます。

前提条件

テープ ライブラリ デバイスは、デバイス製造元のインストール手順に従って、Windows を実行しているコンピュータにインストールする必要があります。

使用する Windows のバージョンにリムーバブル記憶域マネージャ(RSM)が存在するときは、有効にする必要があります。

Microsoft Windows XP および Microsoft Windows Server 2003 の場合:

- リムーバブル記憶域マネージャはオペレーティング システムの一部として、最初から有効になっています。

Microsoft Windows Server 2008 でリムーバブル記憶域マネージャを有効にする場合:

1. **［管理ツール］→［サーバー マネージャ］→［機能］→［機能の追加］**をクリックします。
2. **［リムーバブル記憶域マネージャ］**チェックボックスをオンにします。

Microsoft Windows Vista でリムーバブル記憶域マネージャを有効にする場合:

1. **［コントロール パネル］→［プログラム］→［プログラムと機能］→[Windows の機能の有効化または無効化]**をクリックします。
2. **［リムーバブル記憶域の管理］**チェックボックスをオンにします。

ライブラリのスロットにテープ カートリッジを入れます。テープにバーコードがなかったり、バーコードが破損しているときは、後で識別できるようにテープ ラベルを定義できます。

Acronis Backup & Recovery 10 管理サーバーと Acronis Backup & Recovery 10 管理コンソールをローカル コンピュータまたはリモート コンピュータにインストールし、テープ ライブラリ デバイスを持つコンピュータに Acronis Backup & Recovery 10 ストレージ ノードをインストールして、管理サーバーに登録する必要があります。

管理対象の格納域としてのテープ ライブラリ

テープ ライブラリを使用したデータ保護操作を可能にするには、テープ ライブラリに管理対象の格納域を作成する必要があります。格納域は、コンソールの［**集中管理用格納域**］ビューから作成できます。詳細については、「管理対象の集中管理用格納域の作成『ページ参照 159』」をご参照ください。

しかし、最も簡単なのは、［**ストレージ ノード**］ビューから格納域を作成する方法です。テープ ライブラリが接続されているストレージ ノードを選択してから、［**格納域の作成**］をクリックします。［**集中管理用格納域の作成**］ページが表示され、あらかじめ選択されたパラメータが設定されます。必要な操作は、格納域の**名前**を指定してから、［**OK**］をクリックするだけです。

格納域が作成されると、コンソールの［**集中管理用格納域**］ビューからアクセスできます。これで、テープ ライブラリをバックアップに使用できます。

Acronis Backup & Recovery 10 では、テープ デバイスごとに 1 つの格納域しか作成できません。

テープ ライブラリ内のすべてのカートリッジにバーコードが付いていて、選択したバックアップ スキームに十分なテープが RSM の**空き**プールにあれば、ライブラリは完全に自動で動作できます。

すべてのテープ ライブラリのスロットが空でも、格納域の操作を開始できます。バックアップ操作中にテープ ライブラリのスロットに利用可能なテープがないときは、テープのロードを求める［**タスクはユーザーによる操作が必要**］ウィンドウが表示されます。

テープのバーコードを読み取れないときは、テープのラベルを求める別の［**タスクはユーザーによる操作が必要**］ウィンドウが表示されます。

テープ ライブラリ格納域での操作

コンソールの［**ナビゲーション**］ペインでテープ ライブラリ格納域が選択されていると、［**集中管理用格納域**］ページのツールバーに、テープ ライブラリだけに使用する次の 2 つの操作も表示されます。

- ［**テープの管理**］では［**テープの管理**］ウィンドウが表示されます。このウィンドウから、ライブラリのスロットに関する情報の更新、スロットにあるテープの一覧の収集、テープのラベルの定義を行うことができます。テープに割り当てる新しいラベルがあるときは、この操作によってテープを一時的に取り出し、カートリッジの外側に同じラベルを作成できます。
- ［**テープの再スキャン**］では**[テープの再スキャン]**ウィンドウが表示されます。このウィンドウから、スロットを選択し、再スキャン『ページ参照 171』手順を開始して、指定したテープの内容に関する特別な情報を読み取ることができます。

また、テープ ライブラリ格納域の［**編集**］、［**削除**］、［**ベリファイ**］、［**更新**］の機能も実行できます。

これらの機能には、テープ ライブラリに固有の特徴があることに注意してください。**[編集]** 操作では、**[再スキャン]** 操作なしでテープ ライブラリ デバイスを編集できます。**[削除]** 操作により、選択したテープ ライブラリ格納域上のすべての情報がストレージ ノード データベースから消去されます。つまり、テープ ライブラリ デバイス上のデータがストレージ ノードによって使用されていても、すべてのテープの内容データが削除されます。

[削除] 操作では、テープにアクセスすることなく、格納域の内容がストレージ ノード データベースから削除されます。この格納域を使用する計画とタスクは失敗します。

*テープ ライブラリ上で削除中の集中管理用格納域に属しているバックアップ アーカイブも同様に削除されますが、これらのアーカイブは、**[再スキャン]** 操作によって任意のストレージ ノードから復元できます。*

ライブラリ内のテープ上にあるアーカイブの操作

現在の格納域がテープ ライブラリのときは、コンソールの **[集中管理用格納域]** ビューで選択したバックアップ アーカイブに対する共通アーカイブ データ管理機能として、**[ベリファイ]**、**[削除]**、**[すべてのアーカイブの削除]** があります。ストレージ ノード データベースでの削除は、テープにアクセスすることなく実行されます。テープ ライブラリ格納域から削除したバックアップ アーカイブは、削除後に、アーカイブのデータが入っているすべてのテープに対して実行する［再スキャン］『ページ参照 171』操作によって復元できます。

バックアップが削除されたテープの **[再スキャン]** 操作により、ストレージ ノード データベース内のバックアップの内容に基づいて情報が再作成されるので、そのバックアップを復元できます。

すべてのバックアップがテープから削除されると、テープは空だと見なされます。したがって、そのテープへの最初の書き込みの後、削除されたバックアップは失われて元に戻せません。

テープ ライブラリへのバックアップ

バックアップ先がテープ ライブラリであるバックアップ ポリシー/計画の作成では、他のストレージ デバイスと同じやり方でバックアップを設定します。相違点は、バックアップ ポリシー/計画の作成時に設定できる追加のテープ サポート『ページ参照 138』オプションだけです。これらのオプションにより、作成されたバックアップ ポリシー/計画でテープ ライブラリからテープを使用する方法を指定できます。ただし、オプションのデフォルト設定の方が、テープ ライブラリ全体の使用効率とテープごとの使用効率のいずれも高くなります。

テープ オプションを表示または変更するには、一番上のメニューから **[オプション]** → **[デフォルトのバックアップと復元のオプション]** → **[デフォルトのバックアップ オプション]** → **[テープ サポート]** を選択します。

作成されるバックアップ ポリシー/計画の設定を変更するには、**[バックアップ ポリシーの作成]** / **[バックアップ計画の作成]** ページの **[バックアップ オプション]** で、**[変更...]** をクリックします。表示される **[バックアップ オプション]** ウィンドウの **[テープ サポート]** ページでは、あらかじめ定義された値が設定されています。

テープへのバックアップ時にテープの最後まで達すると、空のテープが自動的にマウントされ、新しいテープで処理が続行されます。

バックアップ タスクの実行中、コンソールから次のテープ固有の情報を参照できます。

- バックアップ操作で現在使用されているテープ数
- 現時点までにタスクで使用されたテープのラベル(バックアップ分割の場合)
- 現在書き込み中のテープのラベル

テープ ライブラリからの復元

テープ デバイス上にあるアーカイブからのデータの復元は、他のストレージ デバイスと同じ方法で実行されます。

復元時には、復元タスクの作成を開始し、テープ デバイス格納域、アーカイブ、およびデータを復元するバックアップを選択します。タスクの作成時に、プログラムはテープにアクセスする代わりに、ストレージ ノード データベースを使用します。ただし、復元するデータ(ファイルや特定のボリューム)を選択するには 1 本以上のテープの読み取りが必要なため、時間がかかる場合があります。

プログラムはテープを見つけて、正しい順序で自動的に挿入します。必要なテープが見つからないときは、**［タスクはユーザーによる操作が必要］**ウィンドウが表示されます。

データの復元操作では、いくつかのテープへのアクセスが必要になる場合があることに注意してください。たとえば、増分バックアップからのデータの復元では、通常、データ バックアップを含む次のテープのロード、マウント、巻き戻し、および読み取りが必要になります。

- データの復元のために選択した増分バックアップが入っているテープ
- 選択した増分バックアップの前に作成された最後の完全バックアップが入っているテープ
- 最後の完全バックアップの後、選択した増分バックアップの前に作成された最後の差分バックアップが入っているテープ(必要な場合)
- 選択した増分バックアップの前の最後の完全バックアップまたは差分バックアップの後に作成されたすべての増分バックアップが入っているテープ(必要な場合)

復元タスクの実行中、管理コンソールから次のテープ固有の情報を参照できます。

- 操作に必要なすべてのテープのラベル
- 現在読み取り中のテープのラベル
- 既に読み取られたテープのラベル
- 読み取りのために待機中のテープのラベル、および現在の状態に関する情報(ロード済みかどうか)

4.1.3.6. テープ ライブラリの管理

テープ ライブラリを管理するために、製品には次のタスクや手順が用意されています。

- 一覧の収集『ページ参照 171』
- 再スキャン『ページ参照 171』
- ラベル設定『ページ参照 172』

テープ ライブラリ上の管理対象の格納域にアクセスできるユーザーは、これらの操作を実行できます。ただし、数分から数時間、場合によっては数日かかる操作もあるので、複数のユーザーがテープ ライブラリのドライブを同時に管理することはできません。たとえば、あるユーザーがテープ ライブラリの［**再スキャン**］タスクを開始すると、他のユーザーが同じタスクの実行を要求しても、既に格納域で実行中なのですべて自動的に取り消されます。

一覧の収集

ストレージ ノードでは、テープ操作のためにそれぞれのデータベース内にあるテープの情報が必要です。このため、格納域が作成された後の次の手順は、通常、テープの一覧を収集することです。

一覧の収集手は、ストレージ ノードがテープ ライブラリのスロットに現在ロードされているテープを認識する手順です。この手順は比較的高速で、通常はテープのデータを読み取らずに、カートリッジのバーコードを読み取ります。バーコードを読み取れないと、GUID 識別子だけを読み取るためにテープがマウントされます。

［**一覧の収集**］手順は、最近追加されたテープにアクセスする必要があるときに、ユーザーが手動で実行するか、自動で実行できます。

この手順を開始するには、コンソールの［**ナビゲーション**］ペインでテープ ライブラリ格納域を選択し、［**テープの管理**］をクリックして、［**テープの管理**］ウィンドウの［**一覧収集の開始**］をクリックします。

一覧の収集が完了すると、ライブラリに現在ロードされているテープの一覧が表示されます。

この手順は、テープ ライブラリのスロットに新しいテープをロードするたびに実行してください。

再スキャン

前述のように、ストレージ ノードはテープとその内容に関する情報を専用データベースに保持します。［**再スキャン**］タスクにより、ユーザーが選択したテープの内容に関する情報を読み取り、データベースを更新します。

このタスクには長い時間がかかるので、手動でのみ開始します。タスクを開始する前に、再スキャンするテープが入っている各スロットを選択する必要があります。

［**再スキャン**］タスクは、次の状況で実行します。

- ストレージ ノードが知らないテープ
- ストレージ ノード データベースが失われたか、破損している
- 内容が古いテープ(テープの内容が別のストレージ ノードまたは手動で変更された場合など)

テープの再スキャンの際には、削除されたバックアップを保持しているテープがあることに留意してください。タスクが完了すると、このようなバックアップはすべてストレージ ノード データベースに復元され、データの復元のためにアクセスできるようになります。

再スキャン時に、テープ ラベルはストレージ ノード データベースに保存されます。この手順のために選択されたスロットにまだラベルを持っていないテープが入っていると、テープの［**再スキャン**］タスクが一時停止して、ラベル設定『ページ参照 172』手順が実行されます。

ラベル設定

データの復元のために必要なテープが見つからないと、［**タスクはユーザーによる操作が必要**］ウィンドウが表示され、ユーザーはテープ ライブラリのスロットにテープを挿入するように求められます。このため、すべてのテープ カートリッジにはバーコードまたは他の読み取り可能なラベルが必要です。

テープにラベルがないときは、テープを使用する前に定義する必要があります。

バーコード ラベルではなく特定のラベル(たとえば、フォルダ C:¥work のファイル バックアップ専用のテープに対して MyWork というラベル)をテープに適用する必要があるときも、同様に［**ラベル設定**］手順を使用します。

この手順を開始するには、コンソールの［**ナビゲーション**］ペインでテープ ライブラリ格納域を選択し、ツールバーの［**テープの管理**］をクリックします。［**テープの管理**］ウィンドウにライブラリのスロット一覧が表示されます。ウィンドウ内のすべてのスロットには関連付けられたデータ フィールドがあり、スロットと関連付けられたテープまたは空のスロットについての情報が含まれます。スロットに **Acronis** プールのテープが入っていると、スロットのデータ フィールドにはそのテープのラベルを表示されます。デフォルトでは、バーコードの付いた未使用のテープのラベルはバーコードと同じになります。バーコードがないか、破損していると、ラベル名が自動的に作成されます。ユーザーは提示されたラベルをそのまま使用するか、独自のラベルをテキストで指定できます。

テープに独自のラベルを定義するには、関連するデータ フィールドを選択し、新しいラベルを入力します。次に、［**テープの取り出し**］をクリックし、(ラベルと関連付ける)テープ カートリッジに同じラベルを書き込んで、同じスロットに戻します。

必要なテープ ラベルをすべて指定したら、［**ラベルの設定**］をクリックして、ストレージ ノード データベースにラベルを保存します。

4.1.3.7. テープ サポート

これらのオプションは、バックアップ先がテープ ライブラリにある管理対象の格納域であるときに有効です。

［**テープ サポート**］オプションを使用すると、バックアップ タスクでバックアップをテープ間に分散する方法を指定できます。

テープ オプションの組み合わせによっては、テープ ライブラリ全体および各テープの使用効率が低下することがあります。これらのオプションを変更する必要性が特にないときは、テープ オプションを変更せずにそのままにしてください。

1 つのアーカイブに対して複数のテープを使用できます。このような状況では、**テープ セット**を使用してデータのバックアップを保持します。

テープ セットとは、特定の保護されたデータのバックアップを含む 1 本以上のテープからなる論理グループです。テープ セットには他のデータのバックアップを入れることもできます。

個別のテープ セットとは、特定の保護されたデータのバックアップのみが入っているテープ セットです。他のバックアップを個別のテープ セットに書き込むことはできません。

(作成するバックアップ ポリシー/計画で) [個別のテープ セットを使用する]

デフォルトの設定 - **オフ**

このオプションを変更しないままにすると、作成中のポリシーまたは計画に属するバックアップが、別のバックアップ ポリシーによって書き込まれたバックアップが入っていて、別のコンピュータのデータで構成されるテープに書き込まれる場合があります。同様に、他のポリシーによるバックアップが、このポリシーによるバックアップが入っているテープに書き込まれる場合があります。すべてのテープはプログラムによって自動的に管理されるので、このようなテープによる問題は発生しません。

このオプションを有効にすると、作成中のポリシーまたは計画に属するバックアップが個別のテープ セットに保存されます。他のバックアップはこのテープ セットに書き込まれません。

管理サーバーにコンソールが接続されている場合

[個別のテープ セットを使用する] オプションでは、さらに正確な定義が可能です。作成するバックアップ ポリシーで、すべてのコンピュータに対して 1 つのテープ セットを使用するか、または 1 台のコンピュータごとに 1 つのテープ セットを使用することができます。

デフォルトでは、**[すべてのコンピュータで 1 つのテープ セットを使用する]** オプションが選択されます。通常、このオプションを選択すると、**[コンピュータごとに個別のテープ セットを使用する]** オプションを選択したときよりもテープの使用効率が高くなります。ただし、特定のコンピュータのバックアップ テープをサイト外に保存するなどの特別な要件があるときは、2 番目のオプションが役立ちます。

[個別のテープ セットを使用する] オプションをオンにすると、現在テープ ライブラリ デバイスにないテープにバックアップを書き込むことが必要になる場合があります。この状況での対応を定義してください。

- **[ユーザーによる操作を要求する]** - バックアップ タスクは **[ユーザーによる操作が必要]** 状態に移行し、必要なラベルの付いたテープがテープ ライブラリ デバイスにロードされるのを待機します。
- **[空きテープを使用する]** - バックアップは空のテープに書き込まれるので、操作が一時停止するのはライブラリに空のテープがない場合だけです。

[常に空きテープを使用する]

下のオプションを変更しないままにすると、各バックアップは［**個別のテープ セットを使用する**］オプションによって指定したテープに書き込まれます。下のいずれかのオプションをオンにすると、完全バックアップ、増分バックアップ、または差分バックアップを作成するたびに新しいテープがテープ セットに追加されます。

- ［**各完全バックアップ**］

デフォルトの設定 - **オフ**

このオプションをオンにすると、完全バックアップはそれぞれ空のテープに書き込まれます。特にこの操作のためにテープがドライブにロードされます。［**個別のテープ セットを使用する**］オプションがオンのときは、同じデータの増分バックアップと差分バックアップだけがテープに追加されます。

- ［**各差分バックアップ**］

デフォルトの設定 - **オフ**

このオプションをオンにすると、差分バックアップはそれぞれ空のテープに書き込まれます。このオプションは、完全バックアップごとに空のテープを使用するときだけ選択できます。

- ［**各増分バックアップ**］

デフォルトの設定 - **オフ**

このオプションをオンにすると、増分バックアップはそれぞれ空のテープに書き込まれます。このオプションは、完全バックアップと差分バックアップごとに空のテープを使用するときだけ選択できます。

4.1.3.8. テープ ローテーション

テープからすべてのバックアップを削除すると、つまりそのテープの最後のバックアップに関する情報がストレージ ノード データベースから削除されると、そのテープは空だと見なされ、バックアップ サイクルで再利用できるようになります。同じテープのローテーションによって最小限のカートリッジ数で対応し、使用済みのテープを再利用することができます。

Acronis Backup & Recovery 10 を使用すると、テープ ライブラリへのバックアップ時にテープ ローテーションを完全に自動化できます。

ここでは、テープ ローテーション用のバックアップ スキームとテープ オプションを選択する際に役立つ情報について説明します。

テープ ローテーション スキームに必要なテープ数を計算する方法については、「テープ計画『ページ参照 188』」をご参照ください。

バックアップ スキームの選択

バックアップ先がテープ ライブラリであるバックアップ ポリシー/計画を作成するときは、バックアップ スキームとして、［**今すぐバックアップ**］、［**後でバックアップ**］、［**GFS(Grandfather-Father-Son)**］、［**ハノイの塔**］、または［**カスタム**］を使用できます。テープ上のアーカイブに対してバックアップの統合はできないので、［**シンプル**］スキームは無効になっています。

Acronis Backup & Recovery 10 では、［**GFS(Grandfather-Father-Son)**］スキーム、［**ハノイの塔**］スキーム、および［**カスタム**］スキームのテープ ローテーションを自動化できます。

Grandfather-Father-Son『ページ参照 39』(GFS)とハノイの塔『ページ参照 43』(ToH)は、テープ ライブラリ デバイスで最もよく使用されるバックアップ スキームです。これらのスキームは、バックアップ アーカイブのサイズ、アーカイブから利用可能な復元点の数、およびアーカイブに必要なテープの数が最適になるように調整されています。

バックアップ アーカイブの直近数日間の日単位のバックアップ、直近数週間の週単位のバックアップ、および月単位のバックアップを使用して復元する必要があるときは、［**GFS(Grandfather-Father-Son)**］スキームが最も好ましいバックアップ スキームです。

主な目的が、小規模なテープ ライブラリに永続的にロードされる使用済みテープの数を最小限に抑えながら、長期にわたってデータを保護することなら、最適な選択肢は［**ハノイの塔**］スキームになります。

［**カスタム**］スキームを使用すると、バックアップ スケジュールと保持ルールを指定して必要なテープ ローテーションを定義できます。このスキームは、［**GFS(Grandfather-Father-Son)**］スキームや［**ハノイの塔**］スキームの使用では不十分なときに使用します。たとえば、保護するデータのサイズがテープのサイズより大幅に小さいときは、標準の日単位/週単位/月単位の完全バックアップ、いくつかのシンプルな保持ルール、およびデフォルトのテープ オプションを使用する［**カスタム**］バックアップ スキームの使用が最適です。

選択の基準

作成するバックアップ ポリシー/計画のテープ ローテーション スキームを設計しようとするときは、常に次の項目を検討する必要があります。

- 保護するデータのサイズ
- 日単位のデータ変更のおおよそのサイズ
- 週単位のデータ変更のおおよそのサイズ
- バックアップ スキームに関する要件(バックアップ操作の頻度、速度、および所要時間)
- バックアップの保持に関する要件(バックアップを保持する最短/最長期間、サイト外のテープ カートリッジに保存する必要があるかどうか)
- テープ ライブラリの機能(ドライブ数、ローダー数、スロット数、利用可能なテープ数、テープの容量)
- データの復元に関する要件(最大所要時間)

実際の状況に関連する項目をすべて分析し、主な選択の基準を確立する必要があります。次に、バックアップ スキームを選択し、テープ オプションを指定します。

どのバックアップ スキームも、さまざまなテープ オプションと組み合わせることにより、テープおよびデバイスの使用効率が大幅に変わってくることに注意してください。

分析事例

次の状況でテープ ローテーションを自動化する必要があるとします。

- 保護するデータのサイズが約 320GB
- 日単位のデータ変更のサイズが約 16GB
- 週単位のデータ変更のサイズが約 40GB 以下
- テープ容量が 400GB

この状況に対して GFS スキームや ToH スキームをさまざまなテープ オプションを組み合わせた結果を分析してみます。

以下のすべての分析例では実際の状況を単純化していますが、テープへのバックアップに関する一般的な概念を示しています。

事例の図の凡例

すべての日単位/増分バックアップ(16GB)は緑の四角で表示されます:

週単位/差分バックアップ(40GB)は青の四角で表示されます:

すべての月単位の完全バックアップ(320GB)はオレンジで表示されます:

テープ全体(400GB)は灰色で表示されます:

GFS(Grandfather-Father-Son)テープ ローテーション スキームの使用

GFS バックアップ スキームのテープ ローテーションは、作成するバックアップ ポリシー/計画で指定したテープ オプションによって主に定義されます。

GFS が次のように設定されていると仮定します。

- **バックアップの開始時刻: 11:00:00 PM**
- **バックアップの実行日: 平日**
- **週単位/月単位: 金曜日**
- **バックアップの保持期間: 日単位は 2 週間、週単位は 2 か月、月単位は 1 年**

主な目的は、この設定でテープ ローテーションを完全自動化することです。

この GFS スキームの実装では、月単位のバックアップは完全バックアップ、週単位のバックアップは差分バックアップ、日単位のバックアップは増分バックアップです。初回のバックアップは常に完全バックアップです。したがって、このバックアップ ポリシー/計画を水曜日に開始し、完全バックアップを毎月第 4 金曜日に作成する場合、水曜日の初回のバックアップは増分バックアップではなく完全バックアップになります。

以下のセクションでは、GFS スキームとさまざまなテープ オプションとの組み合わせを示す分析例を紹介します。

- GFS 例 1『ページ参照 177』。**［個別のテープ セットを使用する］**オプションはオン。**［常に空きテープを使用する］**オプションはすべてオフ。ローテーションには 25 本のテープが必要。
- GFS 例 2『ページ参照 180』。**［個別のテープ セットを使用する］**オプションはオン。**［常に空きテープを使用する: 各完全バックアップ］**オプションはオン。他の**［常に空きテープを使用する］**オプションはオフ。ローテーションには 16 本のテープが必要。
- GFS 例 3『ページ参照 182』。**［個別のテープ セットを使用する］**オプションはオン。**［常に空きテープを使用する］**オプションはすべてオン。ローテーションには 28 本のテープが必要。

これらの例は、自動ローテーションに必要なテープ数がテープ オプションによって異なることを示しています。テープ ライブラリに自動ローテーションのために十分なテープがないときは、ライブラリに空のテープをロードするよう求める**［タスクはユーザーによる操作が必要］**ウィンドウが何回か表示されます。

GFS 例 1

このバックアップ計画では次のテープ オプションを使用すると仮定します。

- **［個別のテープ セットを使用する］**オプションはオン
- **［常に空きテープを使用する: 各完全バックアップ］**オプションはオフ
- **［常に空きテープを使用する: 各増分バックアップ］**オプションはオフ
- **［常に空きテープを使用する: 各差分バックアップ］**オプションはオフ

初回のバックアップ操作が 1 月 1 日の金曜日にスケジュールされているとします。その日の午後 11:00 に、初回の完全バックアップ(テープ全体のサイズ 400GB 上の 320GB)が作成されます。**［個別のテープ セットを使用する］**オプションがオンなので、現在マウントされているテープは取り出されます(空のテープではない場合)。次に、特にこのデータのバックアップ用の空のテープがロードされます。このテープは、下の図で番号 01 とマークされています。「分析事例『ページ参照 176』」で示した凡例に従って、このデータの完全バックアップは図ではオレンジの四角で表示されています。

指定した GFS バックアップ スキームの設定により、データをバックアップするのは**平日**だけなので、次回のバックアップは 1 月 4 日の月曜日の同時刻(**午後 11:00**)に作成されます。**［常に空きテープを使用する: 各増分バックアップ］**オプションがオフなので、このバックアップは同じテープ 01 に書き込まれる増分バックアップ(16GB)です。このバックアップは、図では緑の四角で表示されています。

次の 3 回の増分バックアップは、1 月 1 日、5 日、6 日、および 7 日に書き込まれます。この結果、テープ上の空き領域はこの時点で 16GB しかありません。

[常に空きテープを使用する: 各差分バックアップ] オプションがオフなので、1 月 8 日のデータの差分バックアップ(40GB)は同じテープ 01 に書き込まれます。ただし、バックアップの先頭 16 GB を書き込むと、テープの最後に達します。このため、このテープはマウント解除され、ローダーによってドライブからスロットに取り出されます。さらに、空のテープが同じドライブにロードされてマウントされてから、新しいテープの先頭へのバックアップ(残りの 24GB)が続行されます。

次の図は、この時点でのデータのバックアップ アーカイブを示しています。この差分バックアップは、図では青の四角で表示されています。緑の四角内の番号 1 は、この年最初の週の月曜日に作成された増分バックアップをマークしています。

その後、次のバックアップがテープ 02 に書き込まれます。

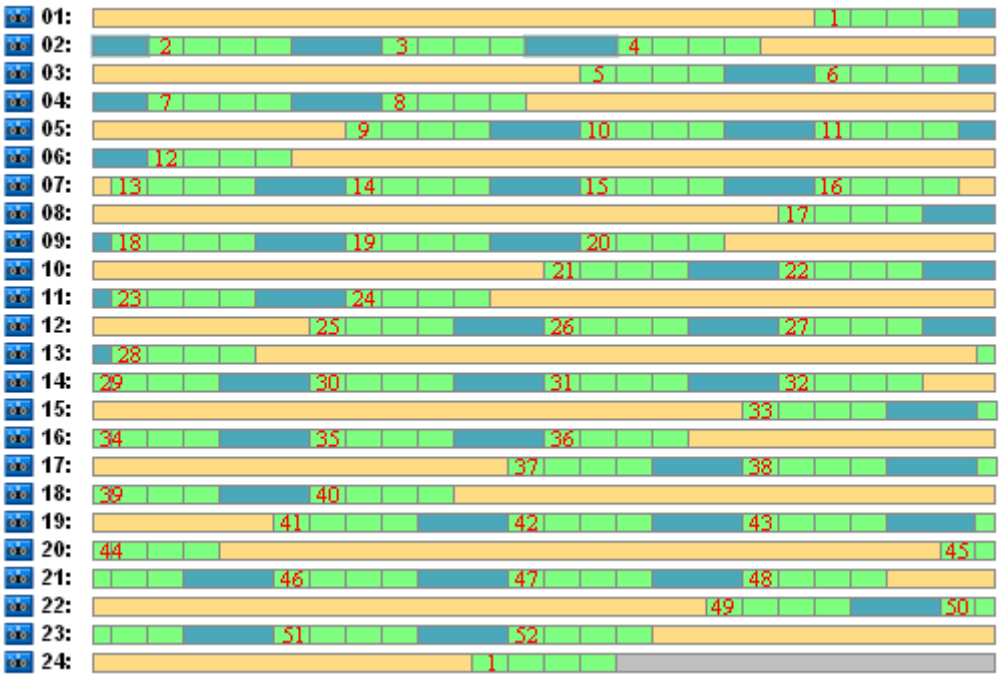
- 2 週目の 4 つの増分バックアップと 1 つの差分バックアップ
- 3 週目の 4 つの増分バックアップと 1 つの差分バックアップ
- 4 週目の 4 つの増分バックアップ

次回の完全バックアップ(320 GB)は、4 週目の金曜日に書き込まれます。ただし、現時点でテープ 02 の空き領域は 104GB しかありません。このため、テープの最後に達すると、空のテープ 03 の先頭から書き込みが続行されます。

GFS スキームでは、各バックアップ操作の後に **[クリーンアップ]** タスクが開始されることに注意してください。このタスクにより、古いバックアップがすべて削除されます。次の図は、現在までに削除されたバックアップを濃い灰色の四角で示しています。

削除されたバックアップは物理的にはまだテープ上に存在しますが、バックアップに関する情報はストレージ ノード データベースから削除されます。

下の図は、事実上削除されたバックアップと、GFS バックアップ スキームと指定したテープ オプションとの組み合わせによる年間のテープの使用状況を示しています。緑の四角内の番号は、この年の対応する週の月曜日に作成された増分バックアップをマークしています。



1 年目のテープの使用状況

次の図は、翌年の最初の金曜日の時点におけるテープの事実上の使用状況を、削除されたバックアップではなく空き領域によって示しています。この時点で、差分バックアップ(青の四角)はテープ 24 に書き込まれます。

テープ 01 に保存された完全バックアップは、52 週目の金曜日に次回の完全バックアップがテープ 23 および 24 上に作成された後で削除されます。テープ 01 のバックアップはすべて削除されているので、テープは空と見なされ、再利用が可能です。

この例をさらに分析すると、データのバックアップを保存するために必要な最大テープ数は 25 であることが証明されます。この最後のテープは、翌年の 16 週目に使用されます。

上記の図は、データの復元のため、完全バックアップ用に 1、2 本のテープ、差分バックアップ用に 2、3 本のテープ、増分バックアップ用に 2、3 本のテープが必要であることを示しています。

たとえば、52 週目の月曜日に作成されたバックアップからデータを復元する必要があると、このタスクで次のテープが必要になります。

- 増分バックアップ(52 でマーク)と 51 週目の金曜日に作成された差分バックアップが入っているテープ 23
- 48 週目の金曜日に作成された完全バックアップが入っているテープ 21 とテープ 22

この例は、GFS スキームと指定したテープ オプションの組み合わせによる次の短所を示しています。

- 一般に、データの復元という時間のかかる処理では、1 本(「1 年目のテープの使用状況」の図で示したバックアップの場合は 3%)、2 本(65%) 、または 3 本(32%)のテープのロード、マウント、巻き戻し、読み取りが必要になる
- 月単位のバックアップのサイズがテープのサイズより少ないときは、13 回の月単位の完全バックアップを保存するために 22 本のテープを使用するので、データの保存コストはさらに高くなる
- データのバックアップの年間ローテーションのために 25 本のテープが必要になる

GFS 例 2

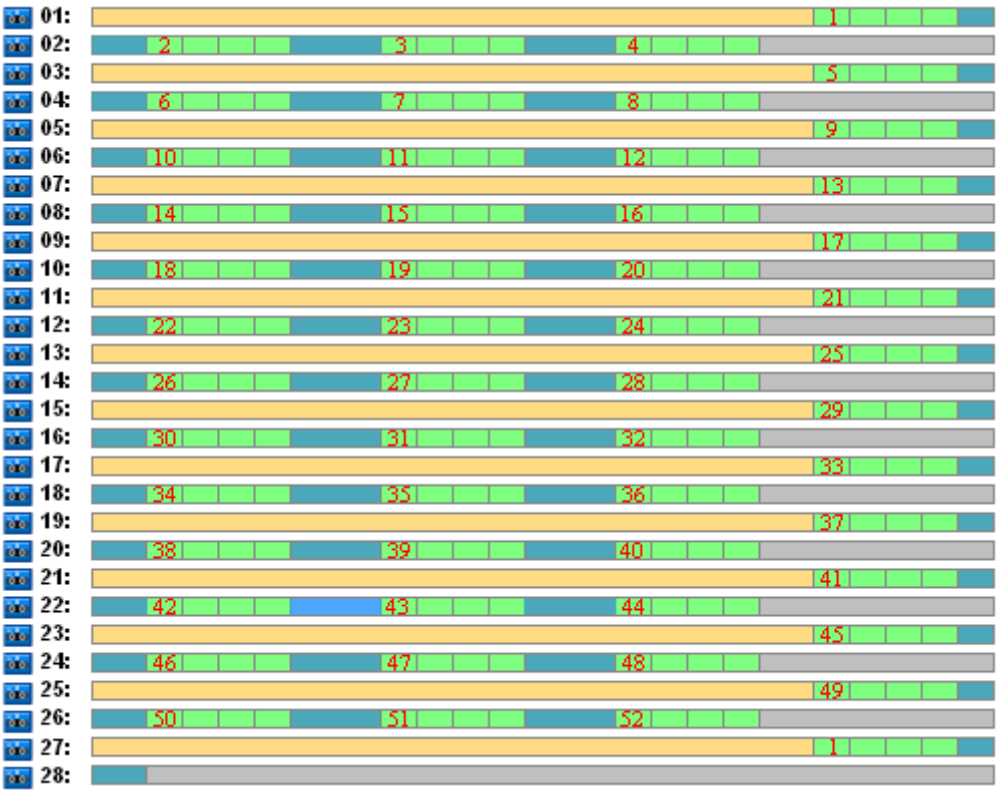
このバックアップ計画では次のテープ オプションを使用すると仮定します。

- **[個別のテープ セットを使用する]** オプションはオン
- **[常に空きテープを使用する: 各完全バックアップ]** オプションはオン
- **[常に空きテープを使用する: 各増分バックアップ]** オプションはオフ
- **[常に空きテープを使用する: 各差分バックアップ]** オプションはオフ

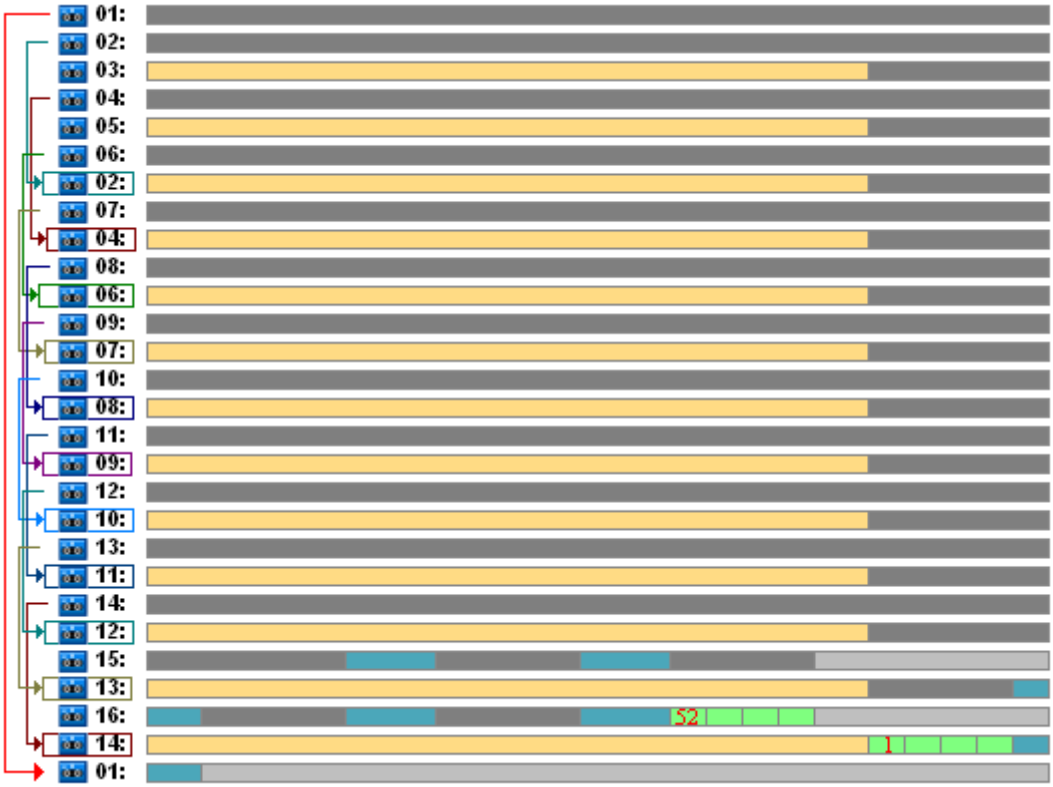
この例と前の例の違いは 1 つだけです。 **[常に空きテープを使用する: 各完全バックアップ]** オプションのオン/オフの違いです。

下の図は、事実上削除されたバックアップと、GFS バックアップ スキームと指定したテープ オプションとの組み合わせによる年間のテープの使用状況を示しています。緑の四角内の番号は、この年の対応する週の月曜日に作成された増分バックアップをマークしています。

すべてのバックアップを 1 年間保持する必要があると、アーカイブに 28 本のテープが必要になります。



GFS バックアップ スキームでは古いバックアップは自動削除されるので、2 年目の最初の金曜日に、テープには次の図で示すバックアップだけが保持されます。



この図は、この事例に対して **GFS 例 2** のテープ ローテーション スキームの方が **GFS 例 1** より適切であることを示しています。この分析事例での **GFS 例 2** のテープ ローテーション スキームには次の長所があります。

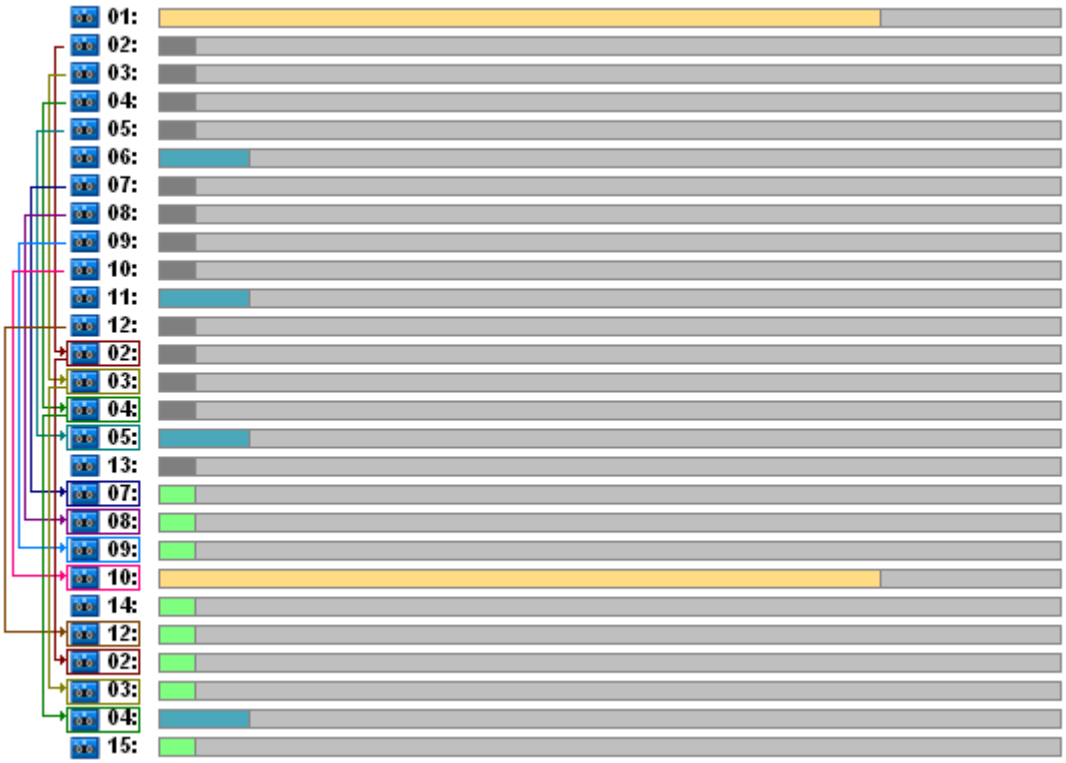
- 使用するテープは 25 本ではなく 16 本になる
- データの復元タスクに必要なテープは 1 本(25%)または 2 本(75%)になる
- 完全バックアップからのデータの復元に必要なテープは 1 本だけで、増分バックアップや差分バックアップからデータをより速く復元できる

GFS 例 3

このバックアップ計画では次のテープ オプションを使用すると仮定します。

- **［個別のテープ セットを使用する］**オプションはオン
- **［常に空きテープを使用する: 各完全バックアップ］**オプションはオン
- **［常に空きテープを使用する: 各増分バックアップ］**オプションはオン
- **［常に空きテープを使用する: 各差分バックアップ］**オプションはオン

これらのオプションは、GFS の標準的なテープ ローテーション スキームを定義しています。次の図は、この分析事例に対し、日単位のバックアップに 8 本のテープ、週単位のバックアップに 6 本のテープ、月単位のバックアップに 13 本のテープ(4 週間のサイクルは 1 年に 13 回)を使用するローテーション スキームの開始状況を示しています。また、次回のバックアップ用に 1 本のテープが必要です。このローテーション スキームをオプションと組み合わせると、合計 28 本のテープが必要になります。



データを復元するには、完全バックアップでは 1 本のテープ、差分バックアップでは 2 本のテープ、増分バックアップでは 2、3 本のテープが必要です。

このスキームには次の長所があります。

- どの完全バックアップを利用するときも必要なテープは 1 本だけである
- バックアップの削除によってテープが解放されて再利用できる

主な短所は、必要なテープ数が増えて、使用率は 5 ～ 10% だということです。

日単位のバックアップを 1 週間(バックアップは 4 回)、週単位のバックアップを 1 か月(バックアップは 4 回) 保持する必要があると、必要なテープ数は合計 4+4+13+1＝22 本になります。

ハノイの塔テープ ローテーション スキームの使用

ToH スキームでローテーションに必要なテープ数は、GFS スキームと比較して少なくなります。したがって、ToH スキームは小規模なテープ ライブラリ、特にオートローダーで最適な選択肢です。

ToH スキームを選択すると、スキームのスケジュールとレベル数を指定できます。

ハノイの塔を週単位のバックアップに適用するときは 5 レベル、日単位のバックアップに適用するときは 8 レベルにすることをお勧めします。最初の状況では、ローテーションは 16 回の週単位のセッションから構成されるので、ロールバック期間は 112 日になります。2 番目の状況では、テープ ローテーションは 128 回の日単位のセッションで構成され、ロールバック期間は 128 日になります。

レベルを追加するごとに、セッション数が倍になるだけでなく、最も古いバックアップ期間も倍になります。

「分析事例」で説明した事例に戻り、次の ToH 設定を想定します。

- **スケジュール: 1 日に 1 回 11:00 PM にタスクを開始する。1 回だけ。**
- **レベル数: 5**

5 レベルのハノイの塔スキームを使用すると、ロールバック期間は 16 日になりますが、スキームの使用例の分析は簡単になります。ここでは、レベル 1 ～ 5 のバックアップをそれぞれ文字 A、B、C、D、E で示します。アーカイブ内のバックアップ順序のローテーション テンプレートは E-A-B-A-C-A-B-A-D-A-B-A-C-A-B-A となります。5 レベルの ToH スキームでは、最初のレベル(A)のバックアップはすべて増分バックアップ、5 番目のレベル(E)は完全バックアップです。また、その他の 2 ～ 4 番目のレベル(B、C、D)のバックアップは差分バックアップです。

ToH スキームのテープ ローテーションはテープ オプションに大きく左右されますが、テープ オプションのデフォルト設定では、必ずしもテープおよびテープ ライブラリ全体の使用が最適化されません。

目的は、ローテーションのテープ数を最小にするために必要なテープ オプションの選択です。

以下のセクションでは、ToH スキームとさまざまなテープ オプションとの組み合わせを示す分析例を紹介します。

- ToH 例 1『ページ参照 185』。**［個別のテープ セットを使用する］**オプションはオン。**［常に空きテープを使用する］**オプションはすべてオフ。ローテーションには 5 本のテープが必要。
- ToH 例 2『ページ参照 186』。**［個別のテープ セットを使用する］**オプションはオン。**［常に空きテープを使用する: 各完全バックアップ］**オプションはオン。他の**［常に空きテープを使用する］**オプションはオフ。ローテーションには 4 本のテープが必要。
- ToH 例 3『ページ参照 187』。**［個別のテープ セットを使用する］**オプションはオン。**［常に空きテープを使用する］**オプションはすべてオン。ローテーションには 7 本のテープが必要。

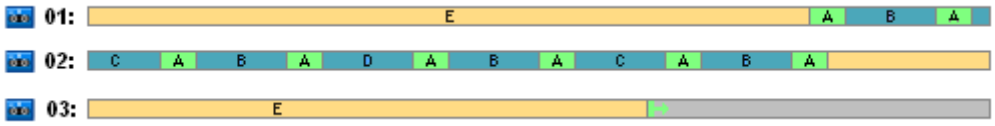
ToH 例 2 には 4 本のテープが必要で、これはこの事例で最小です。したがって、このテープ オプション設定は他の例のオプションと比較して最適な選択肢です。

ToH 例 1

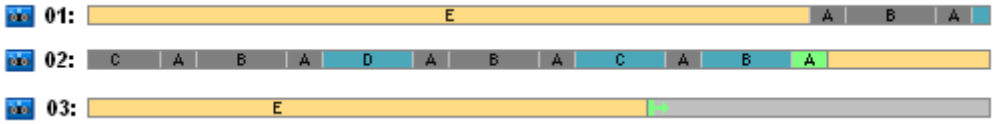
このバックアップ計画では次のテープ オプションを使用すると仮定します。

- **［個別のテープ セットを使用する］**オプションはオン
- **［常に空きテープを使用する: 各完全バックアップ］**オプションはオフ
- **［常に空きテープを使用する: 各増分バックアップ］**オプションはオフ
- **［常に空きテープを使用する: 各差分バックアップ］**オプションはオフ

下の図は、ToH スキームと前述のテープ オプションを組み合わせたテープの使用状況です。このスキームの繰り返し部分は 16 回のバックアップ セッションです。図は、17 回目のセッション終了時のバックアップ アーカイブの状態を示しています。



ハノイの塔スキームでは各レベルのバックアップは 1 つしか存在しないので、古いバックアップはすべて自動的に削除されます。次の図では、削除されたバックアップは濃い灰色の四角で示されています。削除されたバックアップは実際にはテープ上にまだ保存されていますが、バックアップに関する情報はストレージ ノード データベースから削除されます。



図には、この時点でテープ 01 に保存されている完全バックアップがあります。このバックアップを削除できないのは、テープ 02 に保存されている有効な差分バックアップ(D、C、B)および増分バックアップ(A)のベースであるためです。この完全バックアップの削除は、これらの 4 つのバックアップがすべて削除されるまで延期されます。

次の図は、レベル D で新しいバックアップを作成する前のテープの内容を示しています。

この時点でデータ アーカイブは 4 本のテープに保存され、書き込まれているバックアップのサイズはこの例で最大です。ただし、今後、完全バックアップがテープの最後に書き込まれると、アーカイブは 5 本のテープに保存されることになります。

次回のバックアップがレベル D で作成された後、テープ 01 は解放されて再利用できます。

この分析事例では、ToH スキームと指定したオプションの組み合わせは次の特性を持ちます。

- 最後の図で示すように、データの復元のため、最大 3 本のテープのロードとマウント(テープ 1 本 - 16%、テープ 2 本 - 72%、テープ 3 本 - 12%)、および 1回(6%)、2 回(50%)、または 3 回(44%)のバックアップの巻き戻しと読み取りが必要
- 5 レベル スキームではこの事例のために最大 5 本のテープが必要

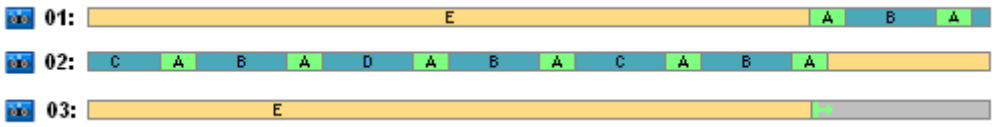
ToH 例 2

このバックアップ計画では次のテープ オプションを使用すると仮定します。

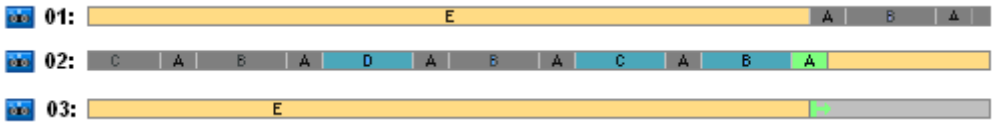
- **[個別のテープ セットを使用する]** オプションはオン
- **[常に空きテープを使用する: 各完全バックアップ]** オプションはオン
- **[常に空きテープを使用する: 各増分バックアップ]** オプションはオフ
- **[常に空きテープを使用する: 各差分バックアップ]** オプションはオフ

ToH 例 2 と **ToH 例 1** の違いは、**[常に空きテープを使用する: 各完全バックアップ]** オプションがオンになっていることだけです。

最初の図は、ToH スキームと前述のテープ オプションを組み合わせたテープの使用状況です。このスキームの繰り返し部分は 16 回のバックアップ セッションです。図は、17 回目のセッション終了時のバックアップ アーカイブの状態を示しています。

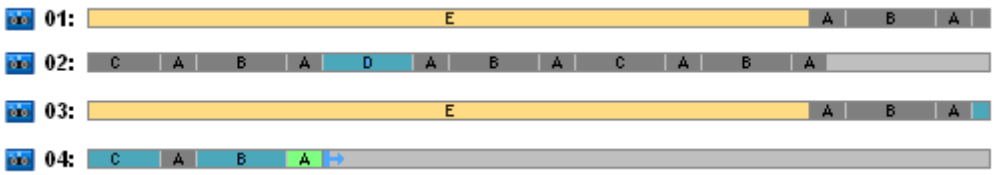


下の図では、この時点で削除されているバックアップは濃い灰色の四角で示されています。



この図は、最初の完全バックアップが差分バックアップ D、C、B のベース、および増分バックアップ A のベースなので、レベル E に 2 つの完全バックアップがあることを示しています。したがって、完全バックアップの削除は、バックアップ D、C、B、A がすべて削除されるまで延期されます。

次の図は、レベル D で新しいバックアップを作成する前のテープの使用状況を示しています。



この時点で、バックアップ アーカイブは 4 本のテープに保存されています。これはこの例で必要な最大テープ数です。

次回のバックアップがレベル D で作成された後、テープ 01 と 02 の両方が解放されて再利用できます。

この分析事例では、ToH スキームと指定したオプションの組み合わせは次の特性を持ちます。

- データの復元のため、1 本(25%)または 2 本(75%)のテープに保持されているバックアップにアクセスする必要がある
- 5 レベルのスキームでは最大 4 本のテープが必要になる

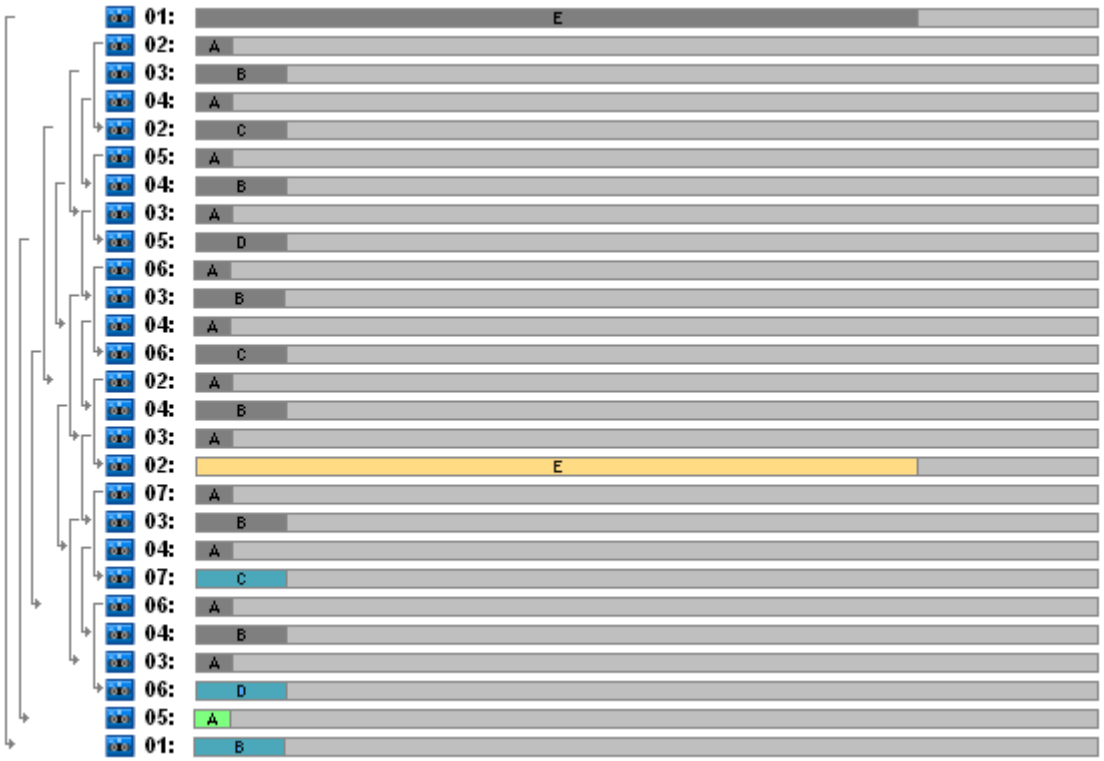
この特定の事例では、**［常に空きテープを使用する: 各完全バックアップ］**オプションがオンであることで、ライブラリ内のテープの使用効率が大幅に上がっています。

ToH 例 3

このバックアップ計画では次のテープ オプションを使用すると仮定します。

- **［個別のテープ セットを使用する］**オプションはオン
- **［常に空きテープを使用する: 各完全バックアップ］**オプションはオン
- **［常に空きテープを使用する: 各増分バックアップ］**オプションはオン
- **［常に空きテープを使用する: 各差分バックアップ］**オプションはオン

次の図は、ToH スキームとこれらのオプションによるテープ ローテーションを示しています。



ローテーションで使用する最大テープ数は 7 本で、標準的な 5 レベルの ToH スキームより多くなります。

追加の 2 本のテープの用途は次のとおりです。

1. 他のレベルのバックアップでベースとなっている古い完全バックアップの保持(削除の延期)
2. あるレベルで新しいバックアップが正常に作成されるまでの、そのレベルの古いバックアップの保持

この例では、テープの使用効率が低下しています。さらに、データの復元のため、1本(完全バックアップ、6%)、2 本(差分バックアップ、44%)、または 3 本(増分バックアップ、50%)のテープに保存されているバックアップにアクセスする必要があります。このため、操作にかかる時間は、平均して前の例より長くなります。

テープ計画

バックアップ スキームとテープ オプションを指定したら、テープ ローテーションの完全自動化のために必要な最小テープ数を決定する必要があります。

テープ計画を簡単にするため、計算したテープ数に他のデータのバックアップが含まれる可能性は排除します。つまり、**［個別のテープ セットを使用する］**オプションはオンです。

テープ数を計算するには、次の項目について考慮する必要があります。

- 完全バックアップのサイズ
- 増分バックアップの平均サイズ
- 差分バックアップの平均サイズ
- データのバックアップに指定する圧縮レベル
- テープ ローテーション スキーム(バックアップの頻度、保持ルール)
- テープ追加オプション
- サイト外のテープ カートリッジ アーカイブのサポート要件

上記の考慮事項で可能なすべての組み合わせに必要なテープ数を計算できる共通式はありません。ただし、ある状況でのテープ数を決定する一般的な方法として、次の手順があります。

1. 最初のバックアップが削除されるまでのバックアップ系列を描きます。
2. テープ追加オプションを考慮します。バックアップ系列がテープ セットに分割される場合があります。
3. 各テープ セットのテープ数を計算します。
4. 計算値の合計がこの事例で必要な合計テープ数になります。

テープ計画: 例 1

次の特性を持つ事例を考えます。

- 完全バックアップのサイズは **F_GB**
- 増分バックアップの平均サイズは **I_GB**
- 差分バックアップの平均サイズは **D_GB**
- 圧縮レベルの平均圧縮率は **CL**
- 選択したテープ ローテーション スキームは **4** レベルの**ハノイの塔**
- テープ オプション:
  - **［個別のテープ セットを使用する］**オプションはオン
  - **［常に空きテープを使用する: 各完全バックアップ］**オプションはオフ
  - **［常に空きテープを使用する: 各増分バックアップ］**オプションはオフ
  - **［常に空きテープを使用する: 各差分バックアップ］**オプションはオフ
- テープ サイズは **T_GB**

4 レベル(A、B、C、D)のハノイの塔スキームでは、最初のバックアップが削除される前に、テープ上に D(完全)、A、B、A、C、A、B、A、D、A、B、A、C のバックアップを指定します。指定したテープ オプションではバックアップに空のテープを使用する必要がないので、一連のバックアップが自動的に分割され、現在のテープの最後に達すると新しいテープで続行されます。計算するテープ セットは 1 つです。

必要なテープ数の合計 = ((2 × F_GB ＋ 6 × I_GB ＋ 5 × D_GB) × CL ／ T_GB)の切り上げ + 1

ToH 例 1『ページ参照 185』について示した上記の計算式は、5 レベルのハノイの塔バックアップ スキームおよび同じテープ オプションに基づきます。一連のバックアップは、E(完全)、A、B、A、C、A、B、A、D、A、B、A、C、A、B、A、E、A、B、A、C、A、B、A、D でした。

必要なテープ数の合計 = ((2 × F_GB ＋ 12 × I_GB ＋ 11 × D_GB) × CL ／ T_GB)の切り上げ + 1 = ((2 × 320 ＋ 12 × 16 ＋ 11 × 40) × 1 ／ 400)の切り上げ + 1 = (3.18) の切り上げ + 1 = 5 (テープ)

テープ計画: 例 2

次の特性を持つ事例を考えます。

- 完全バックアップのサイズは **F_GB**
- 増分バックアップの平均サイズは **I_GB**
- 差分バックアップの平均サイズは **D_GB**
- 圧縮レベルの平均圧縮率は **CL**
- 選択したテンプレート ローテーション スキームは次の設定の **［カスタム］**:
  - **完全バックアップ: 10 日ごと**
  - **差分バックアップ: 2 日ごと**
  - **増分バックアップ: 1 日ごと、6 時間ごと**
  - **保持ルール: 5 日より古いバックアップを削除**

- テープ オプション:
  - **［個別のテープ セットを使用する］**オプションはオン
  - **［常に空きテープを使用する: 各完全バックアップ］**オプションはオン
  - **［常に空きテープを使用する: 各増分バックアップ］**オプションはオフ
  - **［常に空きテープを使用する: 各差分バックアップ］**オプションはオフ
- テープ サイズは **T_GB**

この事例は、2 つのセクションからなる一連のバックアップを定義します。下の図は最初のバックアップを削除する前のセクションです。この図では、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をそれぞれオレンジ、青、および緑の四角で示しています。

この時点で、いくつかのバックアップがクリーンアップ タスクによって削除されます。濃い色で示された古いバックアップは有効なバックアップのベースになっているため、このバックアップの削除は延期されます。

テープ サイズとバックアップのサイズの正確な相関関係は不明なので、削除後に空になるテープ数は確定できません。このため、計算ではこの状況は考慮しません。

テープ セット 01 には、バックアップを保存するために (((F_GB ＋ 4 × D_GB ＋ 5 × 7 × I_GB)× CL ／ T_GB)の切り上げ)本のテープが含まれます。テープ セット 02 には、(((F_GB ＋ 1 × D_GB ＋ 7 × I_GB)× CL ／ T_GB)の切り上げ)本のテープが必要です。計算値の合計がこの事例で必要な合計テープ数になります。

4.1.3.9. さまざまな状況での対応

- **バックアップの入ったテープをテープ ライブラリ間で移動する必要があるときの対応**

  1. Acronis Backup & Recovery 10 ストレージ ノードがインストールされた同じコンピュータに両方のテープ ライブラリが接続されている(つまり、ライブラリが同じストレージ ノードによって管理されている)ときは、ストレージ ノード データベースに、移動されるテープの内容に関する必要な情報がすべて含まれます。したがって、実行する必要があるのは、テープがあるライブラリ上の管理対象の格納域に対して一覧の収集『ページ参照 171』手順を実行することだけです。
  2. 別のストレージ ノードによって管理されているテープ ライブラリにテープを移動するときは、再配置済みテープをそれぞれ再スキャン『ページ参照 171』して、テープに含まれるバックアップに関する情報をストレージ ノードに提供する必要があります。

- **ローカル テープ デバイスのテープ ライブラリからテープを使用する必要があるときの対応**

  Acronis エージェントは、ストレージ ノードが使用する形式と異なる形式のテープにバックアップを作成します。この理由から、ストレージ ノードに接続されたテープ デバイスと管理対象のコンピュータに接続されたテープ デバイス間でテープを交換できません。つまり、ストレージ ノードによって書き込まれたテープは、ローカル接続のテープ デバイスで読み取ることができません。ただし、ストレージ ノードは、エージェントによって書き込まれたテープを読み取ることができます。Acronis Backup & Recovery 10 でのテープ形式の互換性の詳細については、「テープ互換性の表『ページ参照 56』」をご参照ください。

- **ストレージ ノードを再インストールしたり、テープ ライブラリを別のコンピュータに接続する必要があるときの対応**

  テープ ライブラリが接続されているコンピュータにストレージ ノードをインストールし、テープ ライブラリ上に集中管理用格納域を作成してから、バックアップが含まれる各テープを再スキャンします。

- **ストレージ ノードが失われ、テープからデータを復元する必要があるときの対応**

  復元するデータが入っているテープがわかっており、ストレージ ノードによって管理されている格納域を持つテープ デバイスがあるときは、テープ カートリッジをそのデバイスに挿入し、コンソールの［**集中管理用格納域**］ビューに移動して格納域を選択します。次に、テープを再スキャンし、データを復元するアーカイブとバックアップを選択して、復元タスクを作成します。

  復元するデータが入っているテープがわからないときは、データが見つかるまで各テープを再スキャンする必要があります。一般に、必要なすべての手順は上で説明した手順と同じですが、1 本のテープではなく、数本のテープを再スキャンする必要があります。

- **Echo テープからデータを復元する必要があるときの対応**

  「テープ互換性の表『ページ参照 56』」の表を参照して、テープからデータを読み取ることができる Acronis Backup & Recovery 10 コンポーネントを探します。

4.2. 個人用格納域

コンソールを管理対象のコンピュータに直接接続して格納域を作成した場合、この格納域は個人用格納域と呼ばれます。個人用格納域は、管理対象のコンピュータごとに固有です。個人用格納域は、システムにログイン可能なすべてのユーザーに表示されます。個人用格納域にバックアップするためのユーザーの権限は、格納域が配置されているフォルダまたはデバイスに対するユーザーのアクセス許可によって決まります。

個人用格納域は、取り外し可能なメディア、またはリムーバブル メディア上に構成できます。Acronis セキュア ゾーンは、システムにログイン可能なすべてのユーザーが利用できる個人用格納域と見なされます。

個人用格納域は、ローカルのバックアップ計画またはローカル タスクで使用できます。集中管理用バックアップ計画は、Acronis セキュア ゾーン以外の個人用格納域を使用することはできません。

個人用格納域の共有

複数のコンピュータで、物理的に同じ場所、つまり同じ共有フォルダを参照することができますが、各コンピュータは［**格納域**］ツリーに固有のショートカットを持ちます。共有フォルダにバックアップするユーザーは、このフォルダに対するアクセス許可に応じて、他のユーザーのアーカイブを表示したり管理したりすることができます。アーカイブを識別しやすくするため、［**個人用格納域**］ビューには、各アーカイブの所有者を表示する［**所有者**］項目が用意されています。所有者の概念の詳細については、「所有者とログイン情報『ページ参照 35』」をご参照ください。

メタデータ

バックアップ中に、**.meta** フォルダがすべての個人用格納域に作成されます。このフォルダには、アーカイブの所有者やコンピュータ名など、格納域に保存されているアーカイブとバックアップに関する追加情報が含まれています。誤って .meta フォルダを削除した場合、次回格納域にアクセスするときにこのフォルダは自動的に再作成されます。ただし、所有者名やコンピュータ名などの一部の情報は失われます。

4.2.1. ［個人用格納域］ビューを使用した作業

ここでは、［**個人用格納域**］ビューの主要な要素について簡単に説明し、それらの使用方法を示します。

［格納域］ツールバー

このツールバーには、選択した個人用格納域を使用した操作を実行できる操作ボタンが含まれています。詳細については、「個人用格納域での操作『ページ参照 193』」をご参照ください。

汎例付きの円グラフ

円グラフを見ると、格納域の負荷を推測することができます。これには、格納域の空き領域と使用中の領域の比率が示されます。

- 空き領域。格納域が配置されたストレージ デバイス上の領域です。たとえば、格納域がハード ディスク上に配置されている場合、格納域の空き領域は該当するボリュームの空き領域になります。

- 使用中の領域。バックアップ アーカイブとそのメタデータ(格納域に配置されている場合)の合計サイズです。ユーザーがこのフォルダに保存するその他のファイルはカウントされません。

汎例には、格納域に関する次の情報が表示されます。

- 格納域のフル パス
- 格納域に保存されているアーカイブとバックアップの合計数
- 元のデータ サイズに対する使用中の領域の比率

格納域の内容

[格納域の内容] セクションには、アーカイブ テーブルとツールバーが含まれています。アーカイブ テーブルには、格納域に保存されているアーカイブとバックアップが表示されます。アーカイブ ツールバーを使用して、選択したアーカイブとバックアップに対する操作を実行します。バックアップの一覧は、アーカイブの名前の左側にある「+」記号をクリックすると展開されます。すべてのアーカイブは、次のタブのいずれかで種類ごとにグループ化されます。

- **[ディスク アーカイブ]** タブには、ディスク バックアップまたはボリューム バックアップ (イメージ)を含むすべてのアーカイブが一覧表示されます。
- **[ファイル アーカイブ]** タブには、ファイル バックアップを含むすべてのアーカイブが一覧表示されます。

関連セクション:

格納域に保存されたアーカイブの操作『ページ参照 195』

バックアップの操作『ページ参照 196』

アーカイブのフィルタ処理と並べ替え『ページ参照 198』

[アクションとツール] ペインのバー

- **[格納域名]** - 格納域ツリー内の格納域をクリックする際に、**[アクション]** バーが使用できます。格納域のツールバーの操作を複製します。
- **[アーカイブ名]** - アーカイブ テーブルのアーカイブを選択する際に、**[アクション]** バーが使用できます。アーカイブのツールバーの操作を複製します。
- **[バックアップ名]** - アーカイブを展開して、そのバックアップのいずれかをクリックする際に、**[アクション]** バーが使用できます。アーカイブのツールバーの操作を複製します。

4.2.2. 個人用格納域での操作

格納域の操作(作成以外)を実行するには、最初に格納域を選択する必要があります。

次に説明するすべての操作は、ツールバーで対応するボタンをクリックすると実行されます。これらの操作は、それぞれ、**[格納域名] アクション** バー(**[アクションとツール]** ペイン)と、メイン メニューの **[格納域名] アクション**項目からアクセスすることもできます。

個人用格納域を使用して操作を実行するためのガイドラインを次に示します。

目的	操作手順
個人用格納域を作成する	**[作成]** をクリックします。 個人用格納域の作成手順については、「個人用格納域の作成『ページ参照 194』」で詳しく説明しています。
格納域にアクセスするためのユーザー アカウントを変更する	**[ユーザーの変更]** をクリックします。 表示されたダイアログ ボックスで、格納域にアクセスするために必要なログイン情報を入力します。

Acronis セキュア ゾーンを作成する	**［Acronis セキュア ゾーンの作成］**をクリックします。 Acronis セキュア ゾーンの作成手順については、「Acronis セキュア ゾーンの作成『ページ参照 292』」で詳しく説明しています。
格納域の内容を参照する	**［参照］**をクリックします。 表示された［参照］ウィンドウで、選択した格納域の内容を確認します。
格納域をベリファイする	**［ベリファイ］**をクリックします。 ［ベリファイ］『ページ参照 282』ページが開き、既に選択されているこの格納域がソースとして表示されます。格納域のベリファイでは、この格納域に保存されているすべてのアーカイブが確認されます。
格納域を削除する	**［削除］**をクリックします。 削除操作では、フォルダのショートカットだけが**［格納域］**ビューから自動的に削除されます。フォルダ自体はそのまま残されます。フォルダに含まれているアーカイブを保持するか削除するかを選択できます。
格納域のテーブル情報を更新する	**［更新］**をクリックします。 格納域の内容の確認中に、アーカイブの格納域への追加、削除、変更を行うことができます。**［更新］**をクリックして、格納域の情報を最新の変更内容によって更新します。

4.2.2.1. 個人用格納域の作成

個人用格納域を作成する手順は、次のとおりです。

1. **［名前］**フィールドに、作成する格納域の名前を入力します。
2. (オプション)**［コメント］**フィールドに、格納域の説明を追加します。
3. **［パス］**フィールドで、**［変更...］**をクリックします。
   開かれた**［個人用格納域のパス］**ウィンドウで、格納域として使用されるフォルダのパスを指定します。個人用格納域は、取り外し可能なメディア、リムーバブル メディア、ネットワーク共有、または FTP 上に構成できます。
4. **［OK］**をクリックします。この結果、作成された格納域が格納域ツリーの**［個人用］**グループに表示されます。

4.2.2.2. 個人用格納域の結合と移動

既存の格納域をある場所から別の場所に移動する必要がある場合の手順

次の手順に従います。

1. ファイルの移動中に、どのバックアップ計画も既存の格納域を使用しないようにするか、指定した計画のスケジュールを一時的に無効にします『ページ参照 230』。
2. サードパーティ製のファイル マネージャを使用して、格納域フォルダとそのすべてのアーカイブを新しい場所に手動で移動します。
3. 新しい格納域を作成します。

4. バックアップ計画およびタスクを編集します。保存先を新しい格納域にリダイレクトします。
5. 現在の格納域を削除します。

2 つの格納域を結合する方法

2 つの格納域 *A* と *B* を使用しているとします。両方の格納域はバックアップ計画で使用されています。格納域 *B* だけを残し、そこに格納域 *A* のアーカイブをすべて移動することにします。

この場合、次の手順に従います。

1. 結合中に、どのバックアップ計画も格納域 *A* を使用しないようにするか、指定した計画のスケジュールを一時的に無効にします『ページ参照 230』。
2. サードパーティ製のファイル マネージャを使用して、格納域 *B* にアーカイブを手動で移動します。
3. 格納域 *A* を使用するバックアップ計画を編集します。保存先を格納域 *B* にリダイレクトします。
4. 格納域ツリーで、格納域 *B* を選択し、アーカイブが表示されているかどうかを確認します。表示されていない場合は、**［更新］**をクリックします。
5. 格納域 *A* を削除します。

4.3. 共通の操作

4.3.1. 格納域に保存されたアーカイブの操作

アーカイブの操作を実行するには、最初にアーカイブを選択する必要があります。アーカイブがパスワードで保護されている場合、パスワードの入力を求められます。

次に説明するすべての操作は、ツールバーで対応するボタンをクリックすると実行されます。これらの操作は、それぞれ、**［アーカイブ名］アクション** バー(**［アクションとツール］**ペイン)と、メイン メニューの**［アーカイブ名］アクション**項目からアクセスすることもできます。

格納域に保存されているアーカイブを使用して操作を実行するためのガイドラインを次に示します。

目的	操作手順
アーカイブをベリファイする	**［ベリファイ］**をクリックします。 ソースとしてアーカイブがあらかじめ選択された状態で、**［ベリファイ］『ページ参照 282』ページが開きます。** アーカイブのベリファイでは、アーカイブのすべてのバックアップが確認されます。

単一のアーカイブまたは複数のアーカイブを削除する	1 削除する単一のアーカイブまたは複数のアーカイブを選択します。 2 **［削除］**をクリックします。 それぞれのアーカイブとバックアップに対してチェックボックスが付加された**［バックアップの削除］**『ページ参照 197』ウィンドウに選択内容が複製されます。選択内容を見直し、必要に応じて修正して(目的のアーカイブのチェックボックスをオンにします)、削除を確認します。
格納域のすべてのアーカイブを削除する	格納域の一覧にフィルタが適用されている場合、格納域の内容の一部しか表示されないことに注意してください。操作を開始する前に、保持する必要のあるアーカイブが格納域に含まれていないことを確認してください。 **［すべて削除］**をクリックします。 それぞれのアーカイブとバックアップに対してチェックボックスが付加された新しいウィンドウに選択内容が複製されます。選択内容を見直し、必要に応じて修正して、削除を確認します。

4.3.2. バックアップの操作

バックアップの操作を実行するには、最初にバックアップを選択する必要があります。バックアップを選択するには、アーカイブを展開してからバックアップをクリックします。アーカイブがパスワードで保護されている場合、パスワードの入力を求められます。

次に説明するすべての操作は、ツールバーで対応するボタンをクリックすると実行されます。これらの操作は、**［バックアップ名］アクション** バー(**［アクションとツール］**ペイン)と、メイン メニューの**［バックアップ名］アクション項目からアクセスすることもできます。**

バックアップを使用して操作を実行するためのガイドラインを次に示します。

目的	操作手順
別のウィンドウにバックアップの内容を表示する	**［内容の表示］**をクリックします。 **［バックアップ内容］**ウィンドウでバックアップ内容を確認します。
復元する	**［復元］**をクリックします。 復元元としてバックアップがあらかじめ選択された状態で、**［データの復元］**『ページ参照 257』ページが開きます。
仮想コンピュータとしてディスクまたはボリュームを復元する	ディスク バックアップを右クリックして、**［仮想コンピュータとして復元］**を選択します。 復元元としてバックアップがあらかじめ選択された状態で、**［データの復元］**『ページ参照 257』ページが開きます。新しい仮想コンピュータの場所と種類を選択して、通常のディスクまたはボリュームの復元と同様に操作します。
バックアップをベリファイする	**［ベリファイ］**をクリックします。 ソースとしてバックアップがあらかじめ選択された状態で、**［ベリファイ］『ページ参照 282』ページが開きます。ファイル バックアップのベリファイでは、バックアップからダミーの復元先に対してすべてのファイルの復元を疑似的に実行します。ディスク バックアップのベリファイでは、バックアップに保存されているすべてのデータ ブロックのチェックサムを計算します。**

単一または複数のバックアップを削除する	削除するバックアップのいずれかを選択して、［**削除**］をクリックします。 それぞれのアーカイブとバックアップに対してチェックボックスが付加された［**バックアップの削除**］『ページ参照 197』ウィンドウに選択内容が複製されます。選択内容を見直し、必要に応じて修正して(目的のバックアップのチェックボックスを選択します)、削除を確認します。
格納域のすべてのアーカイブとバックアップを削除する	格納域の一覧にフィルタが適用されている場合、格納域の内容の一部しか表示されないことに注意してください。操作を開始する前に、保持する必要のあるアーカイブが格納域に含まれていないことを確認してください。 ［**すべて削除**］をクリックします。 それぞれのアーカイブとバックアップに対してチェックボックスが付加された［**バックアップの削除**］『ページ参照 197』ウィンドウに選択内容が複製されます。選択内容を見直し、必要に応じて修正して、削除を確認します。

4.3.3. アーカイブとバックアップの削除

［**バックアップの削除**］ウィンドウには、格納域ビューと同じタブが表示されますが、それぞれのアーカイブとバックアップに対するチェックボックスも表示されます。削除するように選択したアーカイブまたはバックアップのチェックボックスはオンになっています。削除するアーカイブまたはバックアップを確認します。他のアーカイブとバックアップを削除する必要がある場合、それぞれのチェックボックスをオンにして、［**選択項目を削除**］をクリックし、削除を確認します。

このウィンドウのフィルタは、格納域ビューのアーカイブの一覧から取得されます。したがって、一部のフィルタがアーカイブの一覧に適用されている場合、これらのフィルタに対応するアーカイブとバックアップだけがここに表示されます。すべてのコンテンツを表示するには、すべてのフィルタのフィールドを消去します。

増分バックアップまたは差分バックアップのベースとなっているバックアップを削除した場合の動作

アーカイブの一貫性を保持するために、2 つのバックアップが統合されます。たとえば、完全バックアップを削除するが、次の増分バックアップは保持するとします。バックアップは 1 つの完全バックアップに結合され、そのバックアップに増分バックアップの日付が付けられます。チェーンの中間から増分または差分のバックアップを削除すると、結果として残されるバックアップの種類は増分になります。

統合は削除の 1 つの方法に過ぎず、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。

統合中に作成される一時ファイルのために使用される格納域には、十分な領域が必要です。統合によって作成されるバックアップには、常に最大限の圧縮が適用されます。

4.3.4. アーカイブのフィルタ処理と並べ替え

アーカイブ テーブル内のアーカイブのフィルタ処理と並べ替えを実行するためのガイドラインを次に示します。

目的	操作手順
任意の項目でバックアップアーカイブを並べ替える	アーカイブを昇順で並べ替えるには、項目のヘッダーをクリックします。 再度クリックすると、アーカイブは降順で並べ替えられます。
名前、所有者、コンピュータでアーカイブをフィルタ処理する	対応する項目のヘッダーの下にあるフィールドに、アーカイブ名(所有者名またはコンピュータ名)を入力します。 この結果、名前(所有者名またはコンピュータ名)が入力した値と完全に一致するか、部分的に一致するアーカイブの一覧が表示されます。

アーカイブ テーブルの設定

デフォルトでは、テーブルには 7 つの項目が表示され、他は非表示になっています。必要に応じて、表示されている項目を非表示にしたり、非表示の項目を再表示することができます。

列を表示または非表示にする手順は、次のとおりです。

1. 項目のヘッダーを右クリックしてコンテキスト メニューを開きます。チェックボックスをオンにしたメニュー項目が、表のヘッダー項目に表示されます。
2. 表示/非表示を切り換える項目をクリックします。

5. スケジューリング

Acronis スケジューラを使用すると、管理者は、バックアップ計画を会社の日常業務および社員の作業スタイルに適合させることができます。計画のタスクは、重要なデータを安全に保護しながら、体系的に開始されます。

このスケジューラでは、バックアップ計画が設定されているコンピュータのローカル時刻を使用します。スケジュールを作成する前に、コンピュータの日付と時刻を正しく設定してください。

スケジュール

タスクを実行する時刻を定義するには、1 つ以上のイベントを指定する必要があります。いずれかのイベントが発生するとすぐに、タスクが開始されます。Windows オペレーティング システムと Linux オペレーティング システムで指定できるイベントを次の表に示します。

イベント	Windows	Linux
時間: 日単位、週単位、月単位	+	+
最後の正常なバックアップが完了してから経過した時間 (経過時間を指定)	+	+
ユーザー ログオン (任意のユーザー、現在のユーザー、ユーザーのアカウントを指定)	+	-
ユーザー ログオフ (任意のユーザー、現在のユーザー、ユーザーのアカウントを指定)	+	-
システムの起動	+	+
空き領域の変更 (バックアップ用として選択したボリューム、またはバックアップ対象として選択したデータが格納されているボリュームの空き領域の変更量を指定)	+	-
Windows イベント ログのイベント (イベントのパラメータを指定)	+	-

条件

バックアップ操作のみの場合は、イベントのほかに 1 つ以上の条件を指定できます。いずれかのイベントが発生すると、スケジューラは条件をチェックし、その条件が満たされるときはタスクを実行します。複数の条件が指定されているときにタスクを実行するには、それらの条件のすべてが同時に満たされる必要があります。Windows オペレーティング システムと Linux オペレーティング システムで指定できる条件を次の表に示します。

タスクを実行するための必須条件	Windows	Linux
ユーザーがアイドル状態(スクリーン セーバーが実行中またはコンピュータがロックされている)	+	-
保存先のホストが使用可能	+	+
タスクの実行日時が指定された期間内に存在する	+	+
すべてのユーザーがログオフしている	+	-
最後の正常なバックアップが完了してから指定された期間が経過している	+	+

イベントが発生しても条件(または複数の条件のいずれか)を満たさないときのスケジューラの動作は、［タスクの開始条件］『ページ参照 135』バックアップ オプションで定義します。

よく寄せられる質問

- **前のタスクの実行が完了していないときにイベントが発生すると(および条件が指定されているときはそれを満たすと)どうなりますか。**
  イベントは無視されます。
- **スケジューラが前のイベントに必要な条件が満たされるのを待っているときに別のイベントが発生した場合はどうなりますか。**
  イベントは無視されます。
- **条件が長時間にわたって満たされなかったときはどうなりますか。**
  バックアップの遅れによって問題が発生する可能性があるときは、強制的に条件を満たす(ログオフするようにユーザーに通知する)か手動でタスクを実行します。この状況に自動的に対処するために、指定した時間が経過したら条件に関係なくタスクを実行するように設定できます。

5.1. 日単位のスケジュール

日単位のスケジュールは、Windows および Linux オペレーティング システムで有効です。

日単位のスケジュールを指定する手順は、次のとおりです。

［スケジュール］領域で、次のように適切なパラメータを選択します。

<...> 日に 1 回	何日ごとにタスクを実行するかを設定します。たとえば、［2 日に 1 回］と設定すると、1 日おきにタスクが開始されます。

［タスク実行日の実行間隔...］領域で、次のいずれかを選択します。

次の時間に 1 回のみ: <...>	タスクを 1 回実行する時刻を設定します。
間隔: <...> **開始時刻: <...> 終了時刻: <...>**	指定した時間内にタスクを再実行する回数を設定します。たとえば、タスクの頻度を「1 時間ごと、午前 10:00:00 から午後 10:00:00 まで」に設定すると、午前 10 時 から午後 10 時の間にタスクが 12 回実行されます。

［**有効期間...**］領域で、次のように設定します。

開始: <...>	スケジュールが有効になる日付を設定します(発効日)。このチェックボックスがオフのときは、上で指定した日時に最も近い時刻にタスクが開始されます。
終了: <...>	スケジュールが無効になる日付を設定します。このチェックボックスがオフのときは、無期限にタスクが実行されます。

詳細なスケジュール設定『ページ参照 210』は、Acronis Backup & Recovery 10 管理サーバーに登録されたコンピュータに対してのみ使用できます。これらの設定を指定するには、［**詳細設定**］領域の［**変更**］をクリックします。

設定した内容はすべて、ウィンドウの下部にある［**スケジュール**］フィールドに表示されます。

例

"単純な" 日単位のスケジュール

毎日午後 6 時にタスクを実行します。

スケジュールのパラメータは次のように設定します。

1. ［間隔:］**1** 日ごと。
2. ［次の時間に 1 回のみ:］**午後 06:00:00** に 1 回。
3. ［有効期間...］
   ［開始日:］**設定なし**。タスクが午後 6 時までに作成されたときは、その日にタスクが開始されます。午後 6 時すぎにタスクが作成されたときは、次の日の午後 6 時に開始されます。
   ［終了日:］**設定なし**。タスクは無期限に実行されます。

"3 時間の間隔で 3 か月間継続する" スケジュール

タスクを 3 時間ごとに実行します。タスクは特定の日付(たとえば、2009 年 9 月 15 日)に開始され、3 か月後に終了します。

スケジュールのパラメータは次のように設定します。

1. ［間隔:］**1** 日ごと。
2. ［次の間隔で実行:］**3** 時間ごと
   ［開始時刻:］**午前 12:00:00**(深夜) ［終了時刻:］**午後 09:00:00** - つまり、タスクは 3 時間の間隔で 1 日 8 回実行されます。午後 9 時でその日の最後の反復実行が終了した後、翌日になると深夜の午前 0 時からタスクの反復実行が再開されます。
3. ［有効期間...］
   ［開始日:］**2009 年 9 月 15 日**。たとえば、タスクの作成日が今日 2009 年 9 月 15 日で、タスクの作成時刻が午後 1 時 15 分のとき、この例では、最も近い間隔である午後 3 時になると、タスクが開始されます。
   ［終了日:］**2009 年 12 月 15 日**。タスクの実行はこの日付で終了しますが、タスク自体は引き続き［**タスク**］ビューに表示されます。

1 つのタスクに対する複数の日単位のスケジュール

1 日に複数回のタスクの実行が必要になり、それらを実行する間隔が異なる場合もあります。このようなときは、1 つのタスクに複数のスケジュールを追加します。

たとえば、2009 年 9 月 20 日から 3 日ごとに 1 日 5 回タスクを実行する必要があるとします。

- 1 回目午前 8 時
- 2 回目午後 12 時(正午)
- 3 回目午後 3 時
- 4 回目午後 5 時
- 5 回目午後 7 時

わかりやすい方法は、5 つの単純なスケジュールを追加することです。しかし、少し考えてみると、より適切な方法があることがわかります。つまり、1 回目と 2 回目のタスクの間隔は 4 時間で、3 回目、4 回目、および 5 回目の間隔はそれぞれ 2 時間です。この例では、2 つのスケジュールをタスクに追加する次の方法が最適です。

最初の日単位のスケジュール

1. ［間隔:］**3** 日ごと。
2. ［次の間隔で実行:］**4** 時間ごと。
   ［開始時刻:］**午前 08:00:00**［終了時刻:］**午後 12:00:00**。
3. ［有効期間...］
   ［開始日:］**2009 年 09 月 20 日**。
   ［終了日:］**設定なし**。

2 番目の日単位のスケジュール

1. ［間隔:］**3** 日ごと。
2. ［次の間隔で実行:］**2** 時間ごと。
   ［開始時刻:］**午後 03:00:00**［終了時刻:］**午後 19:00:00**。
3. ［有効期間...］
   ［開始日:］**2009 年 09 月 20 日**。
   ［終了日:］**設定なし**。

5.2. 週単位のスケジュール

週単位のスケジュールは、Windows および Linux オペレーティング システムで有効です。

週単位のスケジュールを指定する手順は、次のとおりです。

［**スケジュール**］領域で、次のように適切なパラメータを選択します。

間隔: <...> 週ごと: <...>	何週間ごとの何曜日にタスクを実行するかを指定します。たとえば、［**2** 週間に 1 回、**月曜日**］と設定すると、1 週間おきの月曜日にタスクが実行されます。

［**タスク実行日の実行間隔...**］領域で、次のいずれかを選択します。

次の時間に 1 回のみ: <...>	タスクを 1 回実行する時刻を設定します。
次の間隔で実行: <...> **開始時刻: <...> 終了時刻: <...>**	指定した期間内にタスクを実行する回数を設定します。たとえば、タスクの頻度を「**1** 時間ごと、**午前 10:00:00** から**午後 10:00:00 まで**」に設定すると、午前 10 時から午後 10 時の間にタスクが 12 回実行されます。

［**有効期間...**］領域で、次のように設定します。

開始日: <...>	スケジュールが有効になる日付を設定します(発効日)。このチェックボックスがオフのときは、上で指定した日時に最も近い時刻にタスクが開始されます。
終了日: <...>	スケジュールが無効になる日付を設定します。このチェックボックスがオフのときは、無期限にタスクが実行されます。

詳細なスケジュール設定『ページ参照 210』は、Acronis Backup & Recovery 10 管理サーバーに登録されたコンピュータに対してのみ使用できます。これらの設定を指定するには、［**詳細設定**］領域の［**変更**］をクリックします。

設定した内容はすべて、ウィンドウの下部にある［**スケジュール**］フィールドに表示されます。

例

"曜日" スケジュール

特定の日付(たとえば、2009 年 5 月 14 日)から 6 か月間にわたり、毎週金曜日の午後 10 時にタスクを実行します。

スケジュールのパラメータは次のように設定します。

1. ［間隔:］**1** 週ごと、**金曜日**。
2. ［次の時間に 1 回のみ:］**午後 10:00:00** に 1 回。
3. ［有効期間...］
   ［開始日:］**2009 年 05 月 13 日**。タスクは、最も近い金曜日の午後 10 時に開始されます。
   ［終了日:］**2009 年 11 月 13 日**。タスクの実行はこの日付で終了しますが、タスク自体はこの日付以降も引き続き［タスク］ビューに表示されます (この日付が金曜日でないときは、この日付より前の最後の金曜日で実行が終了します)。

このスケジュールは、カスタム バックアップ スキームを作成するときによく使用します。たとえば、"曜日" 指定のスケジュールを完全バックアップに追加し、増分バックアップを平日に実行するようにスケジュールします。詳細については、「カスタム バックアップ スキーム『ページ参照 253』」の「完全バックアップおよび増分バックアップとクリーンアップ」の例をご参照ください。

"平日" スケジュール

毎週、月曜日から金曜日の平日にタスクを実行します。平日は、午後 9 時の 1 回のみタスクを開始します。

スケジュールのパラメータは次のように設定します。

1. ［間隔:］**1** 週ごと、**<平日>** - ［<平日>］チェックボックスをオンにすると、対応するチェックボックス(**［月曜日］**、**［火曜日］**、**［水曜日］**、**［木曜日］**、および**［金曜日］**)が自動的にオンになり、残りの曜日はオフのままになります。
2. ［次の時間に 1 回のみ:］**午後 09:00:00** に 1 回。
3. ［有効期間...］

   ［開始日:］**空白**。たとえば、月曜日の午前 11 時 30 分にタスクを作成すると、同じ日の午後 9 時にタスクが開始されます。たとえば金曜日の午後 9 時すぎにタスクが作成されたときは、最も近い平日(この例では月曜日)の午後 9 時にタスクが開始されます。

   ［終了日:］**空白**。タスクは無期限に再実行されます。

このスケジュールは、カスタム バックアップ スキームを作成するときによく使用します。たとえば、"平日" のようなスケジュールを増分バックアップに追加して、完全バックアップを特定の曜日に実行するようにスケジュールします。詳細については、「カスタム バックアップ スキーム『ページ参照 253』」の「完全バックアップおよび増分バックアップとクリーンアップ」の例をご参照ください。

1 つのタスクに対する複数の週単位のスケジュール

異なる曜日に異なる間隔でタスクを実行する必要があるときは、対象となる曜日ごとにスケジュールを追加します。

たとえば、次のスケジュールでタスクを実行する必要があるとします。

- 月曜日: 午後 12 時(正午)と午後 9 時の 2 回
- 火曜日:午前 9 時から午後 9 時までの間 3 時間ごと
- 水曜日: 午前 9 時から午後 9 時までの間 3 時間ごと
- 木曜日: 午前 9 時から午後 9 時までの間 3 時間ごと
- 金曜日: 午後 12 時と午後 9 時の 2 回(月曜日と同じ)
- 土曜日: 午後 9 時に 1 回
- 日曜日: 午後 9 時に 1 回

同じ時刻を組み合わせることにより、次の 3 つのスケジュールをタスクに追加することができます。

最初のスケジュール

1. ［間隔:］**1** 週ごと、**月曜日**、**金曜日**。
2. ［次の間隔で実行:］**9** 時間ごと
   ［開始時刻:］**午後 12:00:00** ［終了時刻:］**午後 09:00:00**。
3. ［有効期間...］
   ［開始日:］**設定なし**。
   ［終了日:］**設定なし**。

2 番目のスケジュール

1. ［間隔:］**1** 週ごと、**火曜日**、**水曜日**、**木曜日**。
2. ［次の間隔で実行:］**3** 時間ごと
   ［開始時刻:］**午前 09:00:00**［終了時刻:］**午後 09:00:00**
3. ［有効期間...］
   ［開始日:］**設定なし**。
   ［終了日:］**設定なし**。

3 番目のスケジュール

1. ［間隔:］**1** 週ごと、**土曜日**、**日曜日**。
2. ［次の時間に 1 回のみ:］**午後 09:00:00** に 1 回。
3. ［有効期間...］
   ［開始日:］**設定なし**。
   ［終了日:］**設定なし**。

5.3. 月単位のスケジュール

月単位のスケジュールは、Windows および Linux オペレーティング システムで有効です。

月単位のスケジュールを指定する手順は、次のとおりです。

［スケジュール］領域で、次のように適切なパラメータを選択します。

月: <...>	タスクを実行する特定の月を選択します。
日: <...>	選択した月の、タスクを実行する特定の日を選択します。実際の日付ではなく、月の最終日を選択することもできます。
実行曜日: <...> <...>	タスクを実行する特定の曜日を選択します。

［タスク実行日の実行間隔...］領域で、次のいずれかを選択します。

次の時間に 1 回のみ: <...>	タスクを 1 回実行する時刻を設定します。
次の間隔で実行: <...> **開始時刻: <...> 終了時刻: <...>**	指定した期間内にタスクを実行する回数を設定します。たとえば、タスクの頻度を「**1** 時間ごと、**午前 10:00:00** から**午後 10:00:00 まで**」に設定すると、午前 10 時から午後 10 時の間にタスクが 12 回実行されます。

［有効期間...］領域で、次のように設定します。

開始日: <...>	スケジュールが有効になる日付を設定します(発効日)。このチェックボックスがオフのときは、上で指定した日時に最も近い時刻にタスクが開始されます。
終了日: <...>	スケジュールが無効になる日付を設定します。このチェックボックスがオフのときは、無期限にタスクが実行されます。

詳細なスケジュール設定『ページ参照 210』は、Acronis Backup & Recovery 10 管理サーバーに登録されたコンピュータに対してのみ使用できます。これらの設定を指定するには、**［詳細設定］**領域の**［変更］**をクリックします。

設定した内容はすべて、ウィンドウの下部にある**［スケジュール］**フィールドに表示されます。

例

"毎月の最終日" スケジュール

毎月の最終日の午後 10 時に 1 回タスクを実行します。

スケジュールのパラメータは次のように設定します。

1. ［月:］**<毎月>**。
2. ［日:］**最終日**。実際の日付ではなく、毎月の最終日にタスクを実行します。
3. ［次の時間に 1 回のみ:］**午後 10:00:00** に 1 回。
4. ［有効期間...］
   ［開始日:］**空白**。
   ［終了日:］**空白**。

このスケジュールは、カスタム バックアップ スキームを作成するときによく使用します。たとえば、"毎月の最終日" スケジュールを完全バックアップに追加し、差分バックアップを週に 1 回、増分バックアップを平日に実行するようにスケジュールします。詳細については、「カスタム バックアップ スキーム『ページ参照 253』」の「月単位の完全バックアップ、週単位の差分バックアップ、日単位の増分バックアップとクリーンアップ」の例をご参照ください。

"季節" スケジュール

2009 年と 2010 年の北半球の秋にあたるすべての平日にタスクを実行します。平日は、午前 0 時(真夜中)から午後 6 時まで 6 時間ごとにタスクを実行します。

スケジュールのパラメータは次のように設定します。

1. ［月:］**9月、10月、11月**。
2. ［実行曜日:］**<すべて>の<平日>**。
3. ［次の間隔で実行:］**6** 時間ごと。
   ［開始時刻:］**午前 12:00:00**［終了時刻:］**午後 06:00:00**。

4. ［有効期間...］
   ［開始日:］**2009 年 08 月 30 日**。タスクが実際に開始されるのは、9 月の最初の平日です。この日付を設定することにより、2009 年にタスクを開始することを定義しています。
   ［終了日:］**2010 年 12 月 01 日**。タスクが実際に終了するのは、11 月の最後の平日です。この日付を設定することにより、北半球の秋が終わると、2010 年までタスクを中断することを定義しています。

1 つのタスクに対する複数の月単位のスケジュール

月ごとに別の日または別の週に異なる時間間隔でタスクを実行する必要があるときは、対象となる月ごとにスケジュールを追加します。

次のタスクが 2009 年 11 月 1 日に有効になるとします。

- 北半球の冬にあたる平日は、毎日午後 10 時にタスクを 1 回実行します。
- 北半球の春と秋にあたる平日は、毎日 12 時間ごとにタスクを実行します。
- 北半球の夏の間は、毎月 1 日と 15 日の午後 10 時にタスクを実行します。

この例では、次の 3 つのスケジュールをタスクに追加します。

最初のスケジュール

1. ［月:］**12月、1月、2月**。
2. ［実行曜日:］**<すべて>の<平日>**
3. ［次の時間に 1 回のみ:］**午後 10:00:00** に 1 回。
4. ［有効期間...］
   ［開始日:］**2009 年 11 月 01 日**。
   ［終了日:］**設定なし**。

2 番目のスケジュール

1. ［月:］**3 月、4月、5月、9月、10月、11月**
2. ［実行曜日:］**<すべて>の<平日>**
3. ［次の間隔で実行:］**12 時間**ごと
   ［開始時刻:］**午前 12:00:00**［終了時刻:］**午後 12:00:00**。
4. ［有効期間...］
   ［開始日:］**2009 年 11 月 01 日**。
   ［終了日:］**設定なし**。

3 番目のスケジュール

1. ［月:］**6月、7月、8月**。
2. ［日:］**1** 日と **15** 日。
3. ［次の時間に 1 回のみ:］**午後 10:00:00** に 1 回。
4. ［有効期間...］
   ［開始日:］**2009 年 11 月 01 日**。
   ［終了日:］**設定なし**。

5.4. Windows イベント ログ イベントの発生時

この種類のスケジュールは、Windows オペレーティング システムの場合にのみ有効です。

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 タスク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することが Windows によって検出されたときはすぐに、データの緊急完全バックアップを自動的に実行するようにバックアップ計画を設定できます。

パラメータ

［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「Microsoft Office Sessions」**のように入力します。

［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、イベントが発生する原因となったプログラムまたはシステム コンポーネントを示し、**［ディスク］**などを指定します。

［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バックアップ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**］領域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タスクを完了できるようにするには、タスク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****［エラー対応］****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。*

Vista での更新前のバックアップ

たとえば、Windows で更新プログラムをインストールするたびに、Windows がインストールされているボリュームをバックアップするバックアップ計画を作成し、システムのバックアップを自動的に実行するとします。

1 つ以上の更新プログラムをダウンロードしてそれらをインストールするスケジュールを設定すると、Microsoft Windows Vista オペレーティング システムによって、イベント ソースが **Microsoft-Windows-WindowsUpdateClient** でイベント番号が **18** 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**情報**です。

計画を作成する際に、［**スケジュール**］領域で次の値を設定します。

- ［**ログ名**］: **システム**
- ［**イベント ソース**］: **Microsoft-Windows-WindowsUpdateClient**
- ［**イベントの種類**］: **情報**
- ［**イベント ID**］: **18**

ヒント: *Microsoft Windows XP を実行しているコンピュータで同様のバックアップ計画を設定するには、****［イベント ソース］****のテキストを* ***Windows Update Agent*** *に置き換え、その他のフィールドには同じ値を設定します。*

イベント ビューアでのイベントの表示方法

イベント ビューアでログを開く手順は、次のとおりです。

1. デスクトップまたは［**スタート**］メニューで、［**マイ コンピュータ**］を右クリックし、［**管理**］をクリックします。
2. ［**コンピュータの管理**］コンソールで、［**システム ツール**］を展開し、［**イベント ビューア**］を展開します。
3. ［**イベント ビューア**］で、［**アプリケーション**］など、表示するログの名前をクリックします。

> ***注意:*** *セキュリティ ログ(［**セキュリティ**］)を開くには、Administrators グループのメンバである必要があります。*

イベント ソースとイベント番号を含む、イベントのプロパティを表示する手順は、次のとおりです。

1. ［**イベント ビューア**］で、［**アプリケーション**］など、表示するログの名前をクリックします。

> ***注意:*** *セキュリティ ログ(［**セキュリティ**］)を開くには、Administrators グループのメンバである必要があります。*

2. 右側のペインのイベントの一覧で、プロパティを表示するイベントの名前をダブルクリックします。
3. ［**イベントのプロパティ**］ダイアログボックスの、［**ソース**］フィールドにイベント ソースが表示され、［**イベント ID**］フィールドにイベント番号が表示されます。

表示された内容を確認したら、［**OK**］をクリックして［**イベントのプロパティ**］ダイアログボックスを閉じます。

5.5. スケジュールの詳細設定

Acronis Backup & Recovery 10 管理サーバーに登録されているコンピュータの日単位、週単位、月単位のスケジュールを選択するときに、次の詳細設定を使用することができます。

Wake-on-LAN を使用する

この設定は、バックアップ ポリシーまたはバックアップ計画を作成するときに使用できます。

この設定を有効にすると、Acronis Backup & Recovery 10 管理サーバーは、バックアップの開始がスケジュールされているときに、Wake-on-LAN (WOL)機能を使用してオフになっている登録済みのコンピュータを起動します。

各コンピュータ上のバックアップ タスクの開始に遅延が指定されている場合(次の設定をご参照ください)、管理サーバーは、それらの遅延に従ってコンピュータを起動します。

この設定を使用する前に、登録されているコンピュータの Wake-on-LAN が有効になっていることを確認してください。コンピュータの BIOS(basic input/output system)の設定、ネットワークアダプタの設定、およびオペレーティング システムの設定は、電源オフの状態からコンピュータを起動できるように設定する必要があります(S5 または G2 電源状態とも呼ばれます)。

開始時間を時間枠内で割り振る

この設定は、バックアップ ポリシーを作成するときにのみ使用できます。

この設定が有効になっている場合、登録されている各コンピュータ上のバックアップ タスクは、ポリシーで設定された開始時刻から特定の遅延時間が経過した後に開始されます。これにより、タスクの実際の開始時刻が特定の時間内に割り振られます。

複数のコンピュータをネットワーク上の場所にバックアップするためのバックアップ ポリシーを作成するときに、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。

遅延値は、0 から指定した最大遅延値までの間で、選択した割り振り方法に従って決定されます。

各コンピュータの遅延値は、ポリシーがコンピュータに配置されるときに決定され、ポリシー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。

条件がある場合は、各コンピュータ上でタスクの実際の開始時刻に条件がチェックされます。

この設定の例を次に示します。

例 1

次のスケジュールのバックアップ ポリシーを 3 台のコンピュータに配置すると仮定します。

タスクの実行: **日単位**
次の時間に 1 回実行: **午後 09:00:00**

開始時間を時間枠内で割り振る
最大遅延時間: **1 時間**
割り振り方法: **ランダム**

すると、たとえば次のように各コンピュータ上のタスクの開始時刻が、午前 09:00:00 と午前 09:59:59 の間の任意の時間になります。

最初のコンピュータ: 毎日午前 09:30:03

2 台目のコンピュータ: 毎日午前 09:00:00

3 台目のコンピュータ: 毎日午前 09:59:59

例 2

次のスケジュールのバックアップ ポリシーを 3 台のコンピュータに配置すると仮定します。

タスクの実行: **日単位**
間隔: **2 時間** 開始: **09:00:00 AM** 終了: **11:00:00 AM**

開始時間を時間枠内で割り振る
最大遅延時間: **1 時間**
割り振り方法: **ランダム**

すると、たとえば次のように各コンピュータ上のタスクの最初の実行の時刻が、午前 09:00:00 と午前 09:59:59 の間の任意の時刻になり、最初の実行と 2 回目の実行の間の間隔が正確に 2 時間になります。

最初のコンピュータ: 毎日午前 09:30:03 と午前 11:30:03

2 台目のコンピュータ: 毎日午前 09:00:00 と午前 11:00:00

3 台目のコンピュータ: 毎日午前 09:59:59 と午前 11:59:59

詳細設定を指定する手順は、次のとおりです。

1. 管理サーバーまたは管理サーバーに登録されているコンピュータに接続し、バックアップ ポリシーまたはバックアップ計画の作成を開始します。
2. **［バックアップ方法］**で、［シンプル］、［ハノイの塔］、または［カスタム］いずれかのスキームを選択し、**［変更］**をクリックして、スキームのスケジュールを指定します。
3. **［タスクの実行］**の下で、**［日単位］**、**［週単位］**、または**［月単位］**を選択します。
4. **［詳細設定］**領域で、**［変更］**をクリックします。
5. Wake-on-LAN 機能の使用を有効にするには、**［Wake-on-LAN を使用する］**チェックボックスをオンにします。
6. 集中管理されるバックアップ タスクの開始時刻を割り振るには、**［開始時間を時間枠内で割り振る］**チェックボックスをオンにして、最大遅延値と割り振り方法を指定します。

5.6. 条件

条件を使用すると、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。指定したイベントが発生すると(使用可能なイベントの一覧については「スケジューリング」をご参照ください)、スケジューラは指定された条件をチェックし、条件が満たされるとタスクを実行します。

イベントが発生しても条件(または複数の条件のいずれか)を満たさないときのスケジューラの動作は、**［タスクの開始条件］**『ページ参照 135』バックアップ オプションで定義します。このオプションで、バックアップ方針に対する条件の重要度を指定できます。

- 条件は必須 - すべての条件が満たされるまで、バックアップ タスクの実行は保留されます。
- 条件は必須ではないが、バックアップ タスク実行の優先度は高 - 指定された期間内は、タスクの実行が保留されます。指定された期間が経過すると、条件が満たされなくてもタスクが実行されます。この設定では、長期間にわたって条件が満たされず、それ以上の遅延は望ましくないときに、プログラムによってその状況に自動的に対応します。

- バックアップ タスクの開始時刻が重要 - バックアップ タスクを開始する時刻に条件が満たされていない場合、タスクはスキップされます。タスクの実行をスキップする方法は、特にイベントが比較的頻繁に発生する場合など、指定された時刻を厳密に守ってデータのバックアップを開始する必要があるときに適しています。

複数の条件の追加

タスクを実行するには、複数の条件が同時に満たされる必要があります。

例:

管理対象のコンピュータの空き領域が 1GB 以上変更された後、すべてのユーザーがログオフし、前回のバックアップから 12 時間以上経過した場合にのみ、バックアップ タスクを実行するとします。

スケジュール、条件、および［**タスクの開始条件**］バックアップ オプションを次のように設定します。

- スケジュール: **空き領域が変更された場合**、値: 空き領域に最低 **1GB** の変更があった場合にタスクを実行する。
- 条件: **ユーザーのログオフ**、値: すべてのユーザーがログオフした場合にのみスケジュールに従ってタスクを実行する。
- 条件: **前回のバックアップからの経過時間**、値: 前回のバックアップから経過した時間が **12 時間**。
- タスクの開始条件: **条件が満たされるまで待機する**。

スケジューラは、空き領域が 1GB 以上変更された場合に、両方の条件が同時に満たされるまで待機してから、バックアップ タスクを実行します。

5.6.1. ユーザーがアイドル状態

適用対象: Windows

"ユーザーがアイドル状態" は、管理対象の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ことを示します。

例:

毎日午後 9 時、ユーザーがアイドル状態のときに、管理対象のコンピュータでバックアップ タスクを実行します。午後 11 時なってもユーザーがアクティブなときは、タスクを強制的に実行します。

- イベント: **日単位**、**1** 日ごと、**午後 09:00:00** に 1 回。
- 条件: **ユーザーがアイドル状態**。
- タスクの開始条件: **条件が満たされるまで待機する**、次の時間が経過するとタスクを実行する: **2** 時間。

結果は次のようになります。

(1)午後 9 時前にユーザーがアイドル状態になっていると、バックアップ タスクは午後 9 時に開始されます。

(2)午後 9 時から午後 11 時の間にユーザーがアイドル状態になると、ユーザーがアイドル状態になった直後にバックアップ タスクが開始されます。

(3)午後 11 時になってもユーザーがアクティブなときは、バックアップ タスクが強制的に開始されます。

5.6.2. 保存先のホストが使用可能

適用対象: Windows、Linux

"保存先のホストが使用可能" は、ネットワーク上のドライブでアーカイブの保存先をホストしているコンピュータが使用可能であることを示します。

例:

ネットワーク上の保存先に対するデータのバックアップを、平日の午後 9 時に実行します。その時点で、保守作業などのために保存先のホストを使用できないときは、バックアップをスキップし、次の平日まで待ってからタスクを実行します。バックアップに失敗する可能性があるときは、バックアップ タスクを開始しないことが前提となります。

- イベント: **週単位、1** 週間ごとの **<平日>、午後 09:00:00** に 1 回。
- 条件: **保存先のホストが使用可能**
- タスクの開始条件: **タスクの実行をスキップする**。

結果は次のようになります。

(1)午後 9 時に保存先のホストを使用できる場合、時間どおりにバックアップ タスクが開始されます。

(2)午後 9 時の時点でホストを使用できない場合、次の平日にホストを使用できれば、その時点でバックアップ タスクが開始されます。

(3)平日の午後 9 時に保存先のホストを使用できない限り、タスクは開始されません。

5.6.3. 期間の範囲内に収める

適用対象: Windows、Linux

バックアップ タスクを開始する時刻を、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)上の異なる場所を使用しています。就業時間は午前 8 時から午後 5 時までです。ユーザーのデータはユーザーがログオフしたらすぐにバックアップする必要がありますが、実行できる時間は午後 4:30 から午後 10 時までの間です。毎日午後 11 時に会社のサーバーをバックアップします。このため、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。上限を午後 10 時に指定すると、ユーザー データのバックアップ時間は 1 時間を超えないことが前提となります。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、タスクの実行をスキップします。

- イベント: **グオフするとき**、次のユーザー: **すべてのユーザー**
- 条件: **期間の範囲内に収める、午後 04:30:00** から**午後 10:00:00** まで。
- タスクの開始条件: **タスクの実行をスキップする**。

結果は次のようになります。

(1)ユーザーが午後 4 時半から午後 10 時の間にログオフすると、ログオフの直後にバックアップ タスクが開始されます。

(2)ユーザーがその期間以外の時刻にログオフすると、タスクはスキップされます。

その他の例

タスクが特定の時刻に実行されるようにスケジュールされていて、この時刻が指定された期間の範囲外の場合

たとえば、次のように設定されているとします。

- イベント: **日単位、1** 日ごと、**午後 03:00:00** に 1 回。
- 条件: **期間の範囲内に収める、午後 06:00:00** から**午後 11:59:59** まで。

この例では、タスクが実行されるかどうかおよび時刻は、タスクの開始条件によって異なります。

- タスクの開始条件が［**タスクの実行をスキップする**］の場合は、タスクが実行されることはありません。
- タスクの開始条件が［**条件が満たされるまで待機する**］で、［**次の時間が経過するとタスクを実行する**］チェックボックスが*オフ*の場合は、タスク(午後 3 時に実行するようにスケジュール)は、条件が満たされる午後 6 時に開始されます。
- タスクの開始条件が［**条件が満たされるまで待機する**］で、［**次の時間が経過するとタスクを実行する**］チェックボックスが*オン*、待機時間が **1 時間**の場合、タスク(午後 3 時に実行するようにスケジュール)は、待機期間が終了する午後 4 時に開始されます。

5.6.4. ユーザーのログオフ

適用対象: Windows

管理対象のコンピュータで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 タスクの実行を保留にすることができます。

例

毎月第 1 金曜日と第 3 金曜日の午後 8 時に、すべてのユーザーがログオフ状態のときはバックアップ タスクを実行します。いずれかのユーザーが午後 11 時にログオンしたままの状態であっても、強制的にタスクを実行します。

- イベント: **月単位**、月: **<すべて>**、実行日: **<第 1>**、**<第 3> <金曜日>**、**午後 08:00:00** に 1 回。
- 条件: **ユーザーのログオフ**。
- タスクの開始条件: **条件が満たされるまで待機する**、次の時間が経過するとタスクを実行する: **3** 時間。

結果は次のようになります。

(1)午後 8 時にすべてのユーザーがログオフ状態のとき、バックアップ タスクは午後 8 時に開始されます。

(2)最後のユーザーが午後 8 時から午後 11 時の間にログオフすると、ユーザーがログオフした直後にバックアップ タスクが開始されます。

(3)午後 11 時になってもいずれかのユーザーがログオンしているときは、バックアップ タスクが強制的に開始されます。

5.6.5. 前回のバックアップからの経過時間

適用対象: Windows、Linux

前回バックアップが正常に完了してから指定された期間が経過するまで、バックアップ タスクの実行を保留にすることができます。

例:

管理対象のコンピュータの空き領域が 1GB 以上変更されていても、前回のバックアップが正常に完了してから 12 時間以上経過した場合にのみ、バックアップ タスクを実行します。

- イベント: **空き領域が変更された場合**、空き領域に最低 **1GB** の変更があった場合にタスクを実行する。
- 条件: **前回のバックアップからの経過時間**、前回のバックアップからの経過時間: **12** 時間ごと。
- タスクの開始条件: **条件が満たされるまで待機する**。

結果は次のようになります。

(1)前回のバックアップが正常に完了してから 12 時間が経過する前に、空き領域が 1GB 以上変更されたとき、スケジューラは 12 時間が経過するまで待機してから、タスクを開始します。

(2)前回のバックアップが正常に完了してから 12 時間が経過した後で、空き領域が 1GB 以上変更されたとき、バックアップ タスクは即座に開始されます。

(3)空き領域が 1GB 以上変更されなかった場合、タスクは開始されません。必要な場合は、［バックアップの計画およびタスク］ビューで、バックアップを手動で開始することができます。

6. 直接管理

ここでは、コンソールとエージェントの直接接続を使用して、管理対象のコンピュータ上で直接実行できる操作について説明します。このセクションの内容は、Acronis Backup & Recovery 10 のスタンドアロンと Advanced Edition の両方に対して適用できます。

6.1. 管理対象のコンピュータの管理

ここでは、管理対象のコンピュータに接続されているコンソールのナビゲーション ツリーで使用できるビューと、各ビューの使用方法について説明します。

6.1.1. ダッシュボード

コンピュータ上のデータが正常に保護されているかどうかをすばやく評価するには、ダッシュボードを使用します。ダッシュボードには Acronis Backup & Recovery 10 エージェントの活動の概要が表示され、問題をすばやく特定して解決することができます。

アラート

［アラート］セクションでは、コンピュータで発生した問題についてユーザーの注意を促し、その問題を修正したり、調査する手段を提供します。最も重大な問題は最上部に表示されます。その時点でアラートまたは警告がない場合は、「アラートまたは警告はありません。」と表示されます。

アラートの種類

下の表は、表示される可能性のあるメッセージの種類を示しています。

	説明	推奨	コメント
	失敗したタスク: X	解決	**［解決］**により、失敗したタスクの**［バックアップの計画とタスク］**ビューが開きます。このビューで失敗の原因を調べることができます。
	ユーザーによる操作が必要なタスク: X	解決	タスクがユーザーによる操作を必要とするたびに、［ダッシュボード］には、どのアクションを実行する必要があるかを知らせるメッセージが表示されます(新しい CD の挿入や、エラー時の停止/再試行/無視など)。
	現在のエディションのライセンスを確認できませんでした。あと X 日でこのソフトウェアは使用できなくなります。 Acronis ライセンス サーバーで有効なライセンスを保有していることを確認してください。	接続	Acronis Backup & Recovery 10 エージェントは、起動時にAcronis ライセンス サーバーに接続し、その後は、エージェント構成パラメータの指定に基づいて 1 ～ 5 日ごと(デフォルトは 1 日)に接続します。 エージェント構成パラメータ(デフォルトは 30 日)の指定に基づいて、ライセンスの確認が 1 ～ 60 日間失敗すると、エージェントはライセンスの確認が成功するまで停止します。

	現在のエディションについてライセンスを X 日間確認できていません。Acronis ライセンス サーバーが使用できないか、ライセンス キーのデータが破損しています。Acronis ライセンス サーバーに接続でき、ライセンスを管理するために実行可能かどうかを確認してください。 Acronis ライセンス サーバーで有効なライセンスを保有していることを確認してください。	接続	Acronis Backup & Recovery 10 が停止しました。過去 *X* 日間、エージェントは、Acronis ライセンス サーバーでライセンスが有効かどうかをチェックできませんでした。 これはおそらく、ライセンス サーバーが使用できなくなっていることが原因です。ライセンスがライセンス サーバーに存在していること、またはライセンス キーのデータが破損していないことを確認してください。 ライセンスの確認に成功すると、エージェントは動作を開始します。
	製品の試用版をご利用いただける期間は、あと *X* 日です Acronis ライセンス サーバーで有効なライセンスを保有していることを確認してください。	接続	製品の試用版をインストールすると、試用期間の終了まで残っている日数のカウントダウンが開始されます。
	試用期間が終了しました。インストーラを起動し、製品版のライセンス キーを入力してください。 Acronis ライセンス サーバーで有効なライセンスを保有していることを確認してください。	接続	15 日の試用期間が終了しました。製品版のライセンス キーを入力してください。
	格納域の空き領域が少なくなっています: X	格納域の表示	**[格納域の表示]** により **[格納域]** ビューが表示されます。ここでは、格納域のサイズ、空き領域、および内容を確認でき、空き領域を増やすために必要な手順を実行できます。
	ブータブル メディアは作成されませんでした	今すぐ作成	コンピュータが起動できない場合にオペレーティング システムを復元できるようにするには、次の手順を行う必要があります。 1 システム ボリューム(およびブート ボリューム(異なる場合))をバックアップします。 2 少なくとも 1 つのブータブル メディア『ページ参照 423』を作成します。 **[今すぐ作成]** によりブータブル メディア ビルダ『ページ参照 424』が起動されます。

⚠	*X* 日間バックアップが作成されていません	今すぐバックアップ	［ダッシュボード］には、比較的長期間、コンピュータ上でデータがバックアップされていないことを示す警告が表示されます。 **［今すぐバックアップ］**により**［バックアップ計画の作成］**ページが表示されます。ここでは、バックアップ操作を簡単に構成し実行できます。 問題と見なす期間を構成するには、**［オプション］→［コンソール オプション］→［時間ベースのアラート］**を選択します。
⚠	管理サーバーに X 日間接続していません	コンピュータの表示	この種類のメッセージは、管理サーバーに登録されているコンピュータに表示されます。［ダッシュボード］には、接続が失われたか、サーバーが利用できない可能性があり、この結果、コンピュータが集中管理されていないことを警告するメッセージが表示されます。

活動

カレンダから、コンピュータ上の Acronis Backup & Recovery 10 エージェントの活動履歴を調べることができます。強調表示された日付を右クリックして**［ログの表示］**を選択すると、日付によってフィルタ処理されたログ エントリの一覧が表示されます。

［表示］セクション(カレンダの右側)から、エラーの存在や重大度に応じて強調表示する活動を選択できます。

	判断方法
エラー	この日付のログに「エラー」エントリが 1 つでもあると、日付は赤で強調表示されます。
警告	この日付のログには「エラー」エントリがないが、「警告」エントリが 1 つでもあると、日付は黄色で強調表示されます。
情報	この日付のログに「情報」エントリしかないときは、日付は緑で強調表示されます(標準の活動)。

［当日の選択］リンクには現在の日付が選択されます。

システム ビュー

バックアップ計画の要約された統計データ、タスク、前回のバックアップに関する簡単な情報が表示されます。関連情報を取得するには、このセクションの項目をクリックします。これにより、あらかじめフィルタ処理された計画またはタスクを示す**［バックアップの計画およびタスク］**『ページ参照 221』ビューが表示されます。たとえば、**［バックアップ計画］**の下にある**［ローカル］**をクリックすると、**［バックアップの計画およびタスク］**ビューが開き、**［ローカル］**でフィルタ処理されたバックアップ計画が表示されます。

6.1.1.1. ［タスクはユーザーによる操作が必要］

このウィンドウには、ユーザーによる操作が必要となるすべてのタスクが 1 か所にまとめられます。このウィンドウによって、タスクごとに、再起動の確認やディスク領域を解放した後の再試行などの設定を指定できます。少なくとも 1 つのタスクでユーザーの操作が必要になるまで、管理対象のコンピュータの［**ダッシュボード**］『ページ参照 218』からいつでもこのウィンドウを開くことができます。

［**このウィンドウを表示しない(タスクの詳細とダッシュボードでこの情報を確認する)**］パラメータのチェックボックスをオンにすると、このタスクは**ダッシュボード**上に他のアラートや警告と共に表示されます。

または、［**バックアップの計画およびタスク**］『ページ参照 221』ビューでタスクの実行状態を確認し、それぞれのタスクに対する設定を［**情報**］ペイン(または［**タスクの詳細**］『ページ参照 230』ウィンドウ)で指定することもできます。

6.1.2. バックアップの計画およびタスク

［**バックアップの計画およびタスク**］ビューには、常に指定したコンピュータのデータ保護に関する情報が表示されます。これにより、バックアップ計画とタスクを監視および管理できます。

バックアップ計画とは、指定したコンピュータ上で指定したデータを保護する方法を定義したルールのセットです。物理的には、バックアップ計画は管理対象のコンピュータ上で実行するために設定されるタスクの集まりです。バックアップ計画によってコンピュータで現在実行されている処理を特定するには、バックアップ計画の実行状態『ページ参照 222』を確認します。バックアップ計画の状態は、計画のタスクの状態を累積したものです。バックアップ計画のステータス『ページ参照 223』により、データが正常に保護されているかどうかを評価できます。

タスクとは、特定の時刻になるか特定のイベントが発生したときに、コンピュータで実行される一連の操作です。タスクの現在の進行状況を追跡するには、タスクの状態『ページ参照 223』を調べます。タスクのステータス『ページ参照 225』をチェックして、タスクの結果を確認します。

操作方法

- フィルタを使用して、バックアップ計画テーブルから目的のバックアップ計画(タスク)を表示します。デフォルトでは、管理対象のコンピュータのすべての計画が名前順にテーブルに表示されます。不要な項目を非表示にしたり、非表示の項目を再表示することもできます。詳細については、「バックアップ計画およびタスクのフィルタ処理と並べ替え『ページ参照 229』」をご参照ください。
- バックアップ テーブルで、バックアップ計画(タスク)を選択します。
- ツールバーのボタンを使用して、選択した計画(タスク)の操作を行います。詳細については、「バックアップ計画およびタスクでの操作『ページ参照 225』」をご参照ください。作成された計画およびタスクの実行、編集、停止、および削除を行うことができます。

- **［情報］**ペインを使用して、選択した計画(タスク)に関する詳細情報を確認します。ペインはデフォルトでは折りたたまれています。ペインを展開するには、  をクリックします。また、ペインの内容は、**計画の詳細**『ページ参照 232』ウィンドウと**タスクの詳細**『ページ参照 230』ウィンドウにそれぞれ重複して表示されます。

6.1.2.1. 状態とステータスについて

バックアップ計画の実行状態

バックアップ計画の実行状態は、**［アイドル］**、**［待機中］**、**［実行中］**、**［停止中］**、**［ユーザーによる操作が必要］**のいずれかになります。

計画の状態は、計画のタスクの状態を累積したものであるため、計画の状態名はタスクの状態名と同じです。

	状態	判断方法	対処方法
1	**［ユーザーによる操作が必要］**	少なくとも 1 つのタスクでユーザーによる操作が必要です。 それ以外の場合は、2 をご参照ください。	ユーザーによる操作が必要なタスク(必要な操作が表示されます)を特定します。次に、タスクを停止するか、タスクが実行できるようにします(メディアの交換、格納域への領域の追加、読み取りエラーの無視、存在しない Acronis セキュア ゾーンの作成など)。
2	**［実行中］**	少なくとも 1 つのタスクが実行中です。 それ以外の場合は、3 をご参照ください。	操作は必要ありません。
3	**［待機中］**	少なくとも 1 つのタスクが待機中です。 それ以外の場合は、4 をご参照ください。	条件が満たされるのを待機している場合。この状況は正常ですが、バックアップの遅延が長くなると、危険性が高まります。この場合の解決策は最大遅延時間を設定するか、条件を強制的に満たすことです(ユーザーへのログオフの指示、必要なネットワーク接続の有効化)。 別のタスクによってロックされている必要なリソースを待機している場合。タスクの開始が遅れたり、特定の理由によってタスクの実行が通常より大幅に長引いて、別のタスクが開始できなくなると、一時的な待機が発生することがあります。障害となっているタスクが終了すると、この状況は自動的に解決します。あるタスクに時間がかかりすぎているために次のタスクが開始できないときは、そのタスクを停止することを検討してください。 計画が正しくスケジュールされていないために、タスクがいつまでも重複している可能性があります。この場合は、計画を編集することで解決します。
4	**［停止中］**	少なくとも 1 つのタスクが停止中です。 それ以外の場合は、5 をご参照ください。	操作は必要ありません。
5	**［アイドル］**	すべてのタスクがアイドルです。	操作は必要ありません。

バックアップ計画のステータス

バックアップ計画のステータスは、**エラー、警告、OK** のいずれかになります。

バックアップ計画のステータスは、その計画のタスクの最後の実行結果から導かれます。

	状態	判断方法	対処方法
1	**エラー**	少なくとも 1 つのタスクが失敗しました。 それ以外の場合は、2 をご参照ください。	失敗したタスクを特定します。このためには、タスクのログを確認して失敗の原因を特定してから、次の 1 つ以上の操作を行います。 • 失敗の原因を取り除きます。このためには、必要に応じて、失敗したタスクを手動で開始します。 • ローカルの計画が失敗していた場合は、今後失敗しないようにローカルの計画を編集します。 • 集中管理用計画が失敗していた場合は、管理サーバーでバックアップ ポリシーを編集します。 バックアップ計画またはポリシーの作成時に、管理者は、バックアップ計画のステータスが「エラー」になったら直ちに実行を停止するオプションをオンにできます。バックアップ計画の実行を再開するには、［再起動］を使用します。
2	**警告**	少なくとも 1 つのタスクが警告を伴って正常終了しました。 それ以外の場合は、3 をご参照ください。	ログを表示して警告を確認します。このためには、必要に応じて、今後の警告や失敗を防止するための操作を行います。
3	**OK**	すべてのタスクが正常に完了しました。	操作は必要ありません。どのタスクもまだ開始されていなかったり、一部のタスクが停止したか停止しようとしているために、バックアップ計画が OK になっている可能性があります。このような状況も正常と見なされてしまいます。

タスクの状態

タスクの状態は、**［アイドル］**、**［待機中］**、**［実行中］**、**［停止中］**、**［ユーザーによる操作が必要］**のいずれかになります。タスクの初期状態は**［アイドル］**です。

タスクを手動で開始するか、スケジュールで指定されたイベントが発生すると、タスクの状態は**［実行中］**または**［待機中］**になります。

［実行中］

スケジュールで指定されたイベントが発生し、バックアップ計画で設定されたすべての条件が満たされ、必要なリソースをロックする他のタスクが実行されていない場合は、タスクの状態は**［実行中］**に変化します。この状況では、タスクの実行を妨げるものは何もありません。

[待機中]

タスクを開始しようとしたが、同じリソースを使用する別のタスクが既に実行中の場合は、タスクの状態は**[待機中]**に変化します。特に、複数のバックアップ タスクまたは復元タスクを 1 台のコンピュータ上で同時に実行することはできません。1 つのバックアップ タスクと 1 つの復元タスクを同時に実行することもできません。他のタスクによってリソースのロックが解除されると、待機中のタスクの状態は**[実行中]**になります。

スケジュールで指定されたイベントが発生したが、バックアップ計画で設定された条件が満たされない場合も、タスクの状態が**[待機中]**に変化することがあります。詳細については、「タスクの開始条件『ページ参照 135』」をご参照ください。

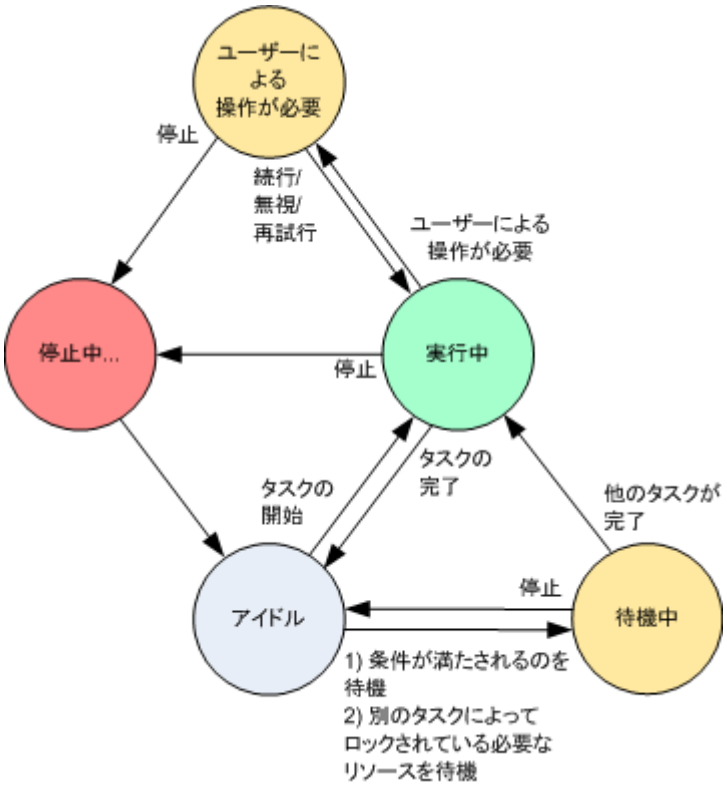
[ユーザーによる操作が必要]

実行中のタスクにより、メディアの交換、読み取りエラーの無視などでユーザーによる操作が必要になると、タスクの状態が**[ユーザーによる操作が必要]**に変化することがあります。タスクの次の状態は、**[停止中]**(ユーザーがタスクの停止を選択した場合)、または**[実行中]**(無視、再試行、または再起動など、タスクの状態を**[実行中]**に移行する別の操作を選択した場合)になります。

[停止中]

ユーザーは、実行中のタスク、またはユーザーによる操作が必要なタスクの実行を停止することができます。タスクの状態は**[停止中]**に変化し、その後**[アイドル]**に変化します。待機中のタスクも停止することができます。この状況では、タスクは実行中ではないため、停止するとキューから削除されます。

タスクの状態遷移図



タスクのステータス

タスクのステータスは、**エラー**、**警告**、**OK** のいずれかになります。

タスクのステータスは、そのタスクの前回の実行結果から導かれます。

	ステータス	判断方法	対処方法
1	**エラー**	前回の結果が「失敗」	失敗したタスクを特定します。このためには、タスクのログを確認して失敗の原因を特定してから、次の 1 つ以上の操作を行います。 • 失敗の原因を取り除きます。このためには、必要に応じて、失敗したタスクを手動で開始します。 • 今後失敗しないように失敗したタスクを編集します。 • ローカルの計画が失敗していた場合は、今後失敗しないようにローカルの計画を編集します。 • 集中管理用計画が失敗していた場合は、管理サーバーでバックアップ ポリシーを編集します。
2	**警告**	前回の結果が「警告を伴った正常終了」	ログを表示して警告を確認します。このためには、必要に応じて、今後の警告や失敗を防止するための操作を実行します。
3	**OK**	前回の結果が「正常終了」、「-」、または「停止」	操作は必要ありません。 「-」という状態は、タスクが開始されていないか、タスクが開始されたがまだ終了していないために結果が不明であることを意味します。

6.1.2.2. バックアップ計画およびタスクを使用した作業

バックアップ計画およびタスクでの操作

バックアップ計画およびタスクを使用して操作を実行するためのガイドラインを次に示します。

目的	操作手順
計画またはタスクの詳細の表示	**バックアップ計画** **［詳細の表示］**をクリックします。 **［計画の詳細］**『ページ参照 232』ウィンドウで、計画の詳細を確認します。 **タスク** **［詳細の表示］**をクリックします。 **［タスクの詳細］**『ページ参照 230』ウィンドウで、タスクの詳細を確認します。

計画またはタスクのログの表示	**バックアップ計画**  **［ログの表示］**をクリックします。 計画に関連したログ エントリの一覧を含む**［ログ］**『ページ参照 233』ビューが表示されます。 **タスク**  **［ログの表示］**をクリックします。 タスクに関連したログ エントリの一覧を含む**［ログ］**『ページ参照 233』ビューが表示されます。
計画またはタスクの実行	**バックアップ計画** **［実行］**をクリックします。 **［バックアップ計画の実行］**『ページ参照 229』ウィンドウで、実行するタスクを選択します。 バックアップ計画を実行すると、その計画から選択したタスクがスケジュールや条件にかかわらず直ちに開始されます。 *バックアップ計画を実行できない理由* • 適切な権限がない コンピュータの管理者権限を持たないユーザーは、他のユーザーが所有する計画を実行することはできません。 **タスク** **［実行］**をクリックします。 タスクは、スケジュールや条件にかかわらず直ちに実行されます。
計画またはタスクの停止	**バックアップ計画** **［停止］**をクリックします。 実行中のバックアップ計画を停止すると、そのタスクがすべて停止されます。したがって、すべてのタスク処理は中断されます。 **タスク** **［停止］**をクリックします。 *タスクを停止した場合の動作* 一般に、タスクを停止すると、その処理(バックアップ、復元、ベリファイ、エクスポート、変換、移行)が中断されます。タスクの状態は、まず［停止中］に変化し、次に［アイドル］になります。タスクのスケジュール(作成されている場合)は、引き続き有効です。処理を完了するには、タスクを再実行する必要があります。 • 復元タスク(ディスク バックアップから): ターゲット ボリュームは削除され、その領域は未割り当てになります。復元が正常終了しなかった場合も同じ結果になります。「失われた」ボリュームを復元するには、タスクを再実行する必要があります。 • 復元タスク(ファイル バックアップから): 中断された処理によって、復元先のフォルダが変更される可能性があります。タスクをどの時点で停止したかによって、復元されるファイルと復元されないファイルが発生します。すべてのファイルを復元するには、タスクを再実行する必要があります。

計画またはタスクの編集	**バックアップ計画** **［編集］**をクリックします。 バックアップ計画の編集は、作成『ページ参照 236』のときと同じ方法で行いますが、次の**制限事項**があります。 作成されたアーカイブが空ではない(つまり、バックアップが含まれる)場合は、バックアップ計画を編集する際に、すべてのバックアップ スキームのオプションを使用できないことがあります。 1 バックアップ スキームを GFS(Grandfather-Father-Son)またはハノイの塔に変更できない。 2 ハノイの塔スキームを使用すると、レベル数を変更できない。 他のすべての場合は、バックアップ スキームの変更が可能で、既存のアーカイブが新しいバックアップ スキームで作成されているかのように機能します。空のアーカイブでは、すべての変更が可能です。 *バックアップ計画を編集できない理由* • バックアップ計画が現在実行中である 現在実行中のバックアップ計画は編集できません。 • 適切な権限がない コンピュータの管理者権限を持たないユーザーは、他のユーザーが所有する計画を編集することはできません。 • バックアップ計画が集中管理されている 集中管理用バックアップ計画を直接編集することはできません。元のバックアップ ポリシーを編集する必要があります。 **タスク** **［編集］**をクリックします。 *タスクを編集できない理由* • タスクがバックアップ計画に属している 直接編集できるのは、復元タスクなど、バックアップ計画に属していないタスクだけです。ローカルのバックアップ計画に属しているタスクを変更する必要がある場合は、バックアップ計画を編集します。集中管理用バックアップ計画に属しているタスクは、その計画の生成元である集中管理ポリシーを編集することで変更できます。これを実行できるのは、管理サーバーの管理者だけです。 • 適切な権限がない コンピュータの管理者権限を持たないユーザーは、他のユーザーが所有するタスクを変更することはできません。

計画またはタスクの削除	**バックアップ計画** **［削除］**をクリックします。 *バックアップ計画を削除した場合の動作* 計画を削除すると、そのタスクはすべて削除されます。 *バックアップ計画を削除できない理由* • バックアップ計画の状態が「実行中」である バックアップ計画のタスクが 1 つ以上実行されている場合は、そのバックアップ計画を削除することはできません。 • 適切な権限がない コンピュータの管理者権限を持たないユーザーは、他のユーザーが所有する計画を削除することはできません。 • バックアップ計画が集中管理されている 集中管理用計画は、管理サーバーの管理者が、その計画の生成元であるバックアップ ポリシーを取り消すことによって削除できます。 **タスク** **［削除］**をクリックします。 *タスクを削除できない理由* • タスクがバックアップ計画に属している バックアップ計画に属しているタスクは、計画と別に削除することはできません。計画を編集してタスクを削除するか、計画全体を削除します。 • 適切な権限がない コンピュータの管理者権限を持たないユーザーは、他のユーザーが所有するタスクを削除することはできません。
テーブルの更新	**［更新］**をクリックします。 管理コンソールにより、コンピュータに存在するバックアップ計画とタスクの一覧が最新情報で更新されます。一覧はイベントに基づいて自動的に更新されますが、待ち時間があるため、データは管理対象のコンピュータから直ちに取得されないことがあります。手動で更新すると、確実に最新データが表示されます。

バックアップ計画およびタスクのフィルタ処理と並べ替え

目的	操作手順
名前、状態、ステータス、種類、ロケーションなどによるバックアップ計画およびタスクの並べ替え	バックアップ計画およびタスクを昇順で並べ替えるには、項目のヘッダーをクリックします。 再度クリックすると、計画およびタスクは降順で並べ替えられます。
名前または所有者による計画/タスクのフィルタ処理	対応するヘッダー名の下にあるフィールドに、計画名、タスク名、または所有者名を入力します。 この結果、名前または所有者名が入力した値と完全に一致するか、部分的に一致するタスクの一覧が表示されます。
状態、ステータス、種類、ロケーション、前回の結果、スケジュールによる計画およびタスクのフィルタ処理	対応するヘッダーの下にあるフィールドで、一覧から必要な値を選択します。

バックアップ計画とタスク テーブルの設定

デフォルトでは、テーブルには 6 つの項目が表示され、他は非表示になっています。必要に応じて、表示されている項目を非表示にしたり、非表示の項目を再表示することができます。

列を表示または非表示にする手順は、次のとおりです。

1. 項目のヘッダーを右クリックしてコンテキスト メニューを開きます。チェックボックスをオンにしたメニュー項目が、表のヘッダー項目に表示されます。
2. 表示/非表示を切り換える項目をクリックします。

バックアップ計画の実行

バックアップ計画は、そのタスクが 1 つ以上実行されている場合は実行中と見なされます。**[バックアップ計画の実行]** ウィンドウでは、スケジュールに関係なく、選択したバックアップ計画のタスクを手動で実行できます。

選択したバックアップ計画のタスクを実行する手順は、次のとおりです。

1. 実行する必要があるバックアップ計画のタスクを選択します。確実に選択するため、ウィンドウの下部にあるタブに収集されたタスク情報を確認します。この情報は、**[タスクの詳細]** 『ページ参照 230』ウィンドウにも重複して表示されます。
2. **[OK]** をクリックします。

バックアップ計画の一時的な無効化

サードパーティ製のファイル管理ソフトを使用して格納域の間でアーカイブを移動する際は、バックアップ計画を一時的に無効にする必要があります。

これは、カスタムのバックアップ スキームを使用するバックアップ計画にのみ適用されます。

バックアップ計画を無効にする手順は、次のとおりです。

1. **[編集]**をクリックします。
2. バックアップ計画のスケジュール オプションを入力し、**[開始日]** パラメータや **[終了日]** パラメータを変更して、必要な期間のスケジュールを無効にします。

タスクの詳細

[タスクの詳細]ウィンドウ(**[情報]**パネルにも表示されます)には、選択したタスクのすべての情報がまとめて表示されます。

タスクに対してユーザーによる操作が必要な場合は、メッセージと操作ボタンがタブの上に表示されます。メッセージには、問題に関する簡単な説明が含まれます。ボタンを使用すると、タスクやバックアップ計画の再試行または停止を行うことができます。

タスクの種類

タスク名	説明
バックアップ(ディスク)	ディスクやボリュームをバックアップします。
バックアップ(ファイル)	ファイルやフォルダをバックアップします。
バックアップ(仮想コンピュータ)	仮想コンピュータ全体またはそのボリュームをバックアップします。
復元(ディスク)	ディスク バックアップを復元します。
復元(ファイル)	ファイルやフォルダを復元します。
復元(ボリューム)	ディスク バックアップからボリュームを復元します。
復元(MBR)	マスタ ブート レコードを復元します。
復元(ディスクから既存の VM へ)	ディスク/ボリューム バックアップから既存の仮想コンピュータに復元します。
復元(ディスクから新しい VM へ)	ディスク/ボリューム バックアップから新しい仮想コンピュータに復元します。
復元(既存の VM)	仮想コンピュータ バックアップから既存の仮想コンピュータに復元します。
復元(新しい VM)	仮想コンピュータ バックアップから新しい仮想コンピュータに復元します。
ベリファイ(アーカイブ)	1 つのアーカイブをベリファイします。
ベリファイ(バックアップ)	バックアップをベリファイします。

ベリファイ(格納域)	格納域に格納されているすべてのアーカイブをベリファイします。
クリーンアップ	保持ルールに従って、バックアップ アーカイブからバックアップを削除します。
ASZ の作成	Acronis セキュア ゾーンを作成します。
ASZ の管理	Acronis セキュア ゾーンのサイズの変更、パスワードの変更、削除を行います。
ディスクの管理	ディスク管理操作
圧縮	ストレージ ノードでサービス タスクを実行します。
インデックス作成	バックアップの完了後に、ストレージ ノードによって格納域で実行される重複除外タスクです。

タスクの種類とタスクが実行中かどうかに応じて、次のタブがいくつか表示されます。

[タスク]

[タスク] タブは、すべての種類のタスクに共通です。選択したタスクに関する一般的な情報が表示されます。

[アーカイブ]

[アーカイブ] タブは、バックアップ、アーカイブのベリファイ、およびクリーンアップの各タスクに使用できます。

アーカイブの名前、種類、サイズ、格納場所などに関する情報が表示されます。

[バックアップ]

[バックアップ] タブは、復元、バックアップのベリファイ、およびエクスポートの各タスクに使用できます。

バックアップを作成した際に、選択したバックアップの種類(完全、増分、差分)、アーカイブの情報、バックアップが格納されている格納域の詳細が表示されます。

[設定]

[設定] タブには、スケジュールの設定およびデフォルト値から変更されたオプションに関する情報が表示されます。

[進行状況]

[進行状況] タブは、タスクの実行中に使用できます。このタブは、すべての種類のタスクに共通です。このタブには、タスクの進行状況、経過時間、およびその他のパラメータに関する情報が表示されます。

バックアップ計画の詳細

[バックアップ計画の詳細] ウィンドウ(**[情報]** ペインにも重複して表示されます)には、選択したバックアップ計画に関するすべての情報が 4 つのタブに集約されます。

計画のいずれかのタスクでユーザーによる操作が必要な場合は、それぞれのメッセージがタブの上部に表示されます。メッセージには、問題に関する簡単な説明、および適切な操作を選択したり、計画を停止するための操作ボタンが含まれます。

バックアップ計画

[バックアップ計画] タブには、選択した計画に関する次の一般的な情報が示されます。

- **[名前]** - バックアップ計画の名前。
- **[ロケーション]** - 計画が、直接管理を使用して管理対象のコンピュータ上に作成された計画(ローカル)であるか、または管理サーバーからバックアップ ポリシーを配置されてコンピュータに表示された計画(集中管理)であるか。
- **[ポリシー]** (集中管理用ロケーションを使用したバックアップ計画用) - 配置することによりバックアップ計画を作成したバックアップ ポリシーの名前。
- **[アカウント]** - 計画を実行するアカウントの名前。
- **[所有者]** - 計画を作成または最後に変更したユーザーの名前。
- **[状態]** - バックアップ計画の実行状態『ページ参照 222』。
- **[ステータス]** - バックアップ計画のステータス『ページ参照 223』。
- **[スケジュール]** - タスクのスケジュールが設定されたか、または手動で開始するように設定されたか。
- **[前回のバックアップ]** - 前回のバックアップから経過した時間。
- **[作成]** - バックアップ計画の作成日。
- **[コメント]** - 計画の説明(入力可能な場合)。

ソース

[ソース] タブには、バックアップ対象に選択されたデータに関する次の情報が示されます。

- **[ソースの種類]** - バックアップ対象に選択されたデータの種類『ページ参照 239』。
- **[バックアップする項目]** - バックアップ対象に選択された項目とそのサイズ。

保存先

[保存先] タブには、次の情報が示されます。

- **[場所]** - アーカイブが保存される格納域の名前またはフォルダへのパス。
- **[アーカイブ名]** - アーカイブの名前。
- **[アーカイブのコメント]** - アーカイブに関するコメント(記入可能な場合)。

設定

［**設定**］タブには、次の情報が示されます。

- ［**バックアップ スキーム**］- 選択されたバックアップ スキームと、スケジュールでのそのすべての設定。
- ［**ベリファイ**］(選択された場合) - ベリファイの実行前後のイベントとベリファイのスケジュール。
- ［**バックアップ オプション**］- デフォルトの値から変更されたバックアップ オプション。

6.1.3. ログ

ログには、コンピュータ上で Acronis Backup & Recovery 10 によって実行された処理、またはユーザーがプログラムを使用して行った操作の履歴が保存されます。たとえば、ユーザーがタスクを編集すると、そのエントリがログに追加されます。プログラムによってタスクが実行されると、複数のエントリが追加されます。ログを使用すると、操作やタスクの実行結果(失敗した理由など)を調べることができます。

ログ エントリの操作方法

- 必要なログ エントリを表示するには、フィルタを使用します。不要な項目を非表示にしたり、非表示の項目を再表示することもできます。詳細については、「ログ エントリのフィルタ処理と並べ替え『ページ参照 235』」をご参照ください。
- ログ エントリを操作するには、ログ テーブルで 1 つまたは複数のログ エントリを選択します。詳細については、「ログ エントリの操作『ページ参照 234』」をご参照ください。
- ［**情報**］ペインを使用して、選択したログ エントリに関する詳細情報を確認します。ペインはデフォルトでは折りたたまれています。ペインを展開するには、 をクリックします。このペインの内容は、［**ログ エントリの詳細**］『ページ参照 235』ウィンドウにも重複して表示されます。

あらかじめフィルタ処理されたログ エントリを持つログのオープン

他の管理ビュー(［**ダッシュボード**］、［**バックアップの計画およびタスク**］)で項目を選択した後、［**ログ**］ビューを開くと、当該の項目のあらかじめフィルタ処理されたログ エントリが表示されます。したがって、ユーザーがログ テーブルのフィルタを構成する必要はありません。

ビュー	アクション
ダッシュボード	予定表で、強調表示された日付を右クリックして、［**ログの表示**］を選択します。［**ログ**］ビューに、既に当該の日付でフィルタ処理されたログ エントリの一覧が表示されます。
バックアップの計画およびタスク	バックアップの計画またはタスクを選択して、［**ログの表示**］をクリックします。［ログ］ビューに、選択した計画またはタスクに関連したログ エントリの一覧が表示されます。

6.1.3.1. ログ エントリの操作

次に説明するすべての操作は、ログの**ツールバー**で対応する項目をクリックすると実行されます。また、すべての操作は、コンテキスト メニュー(ログ エントリを右クリックして表示)、または［**ログ**］アクション バー(［**アクションとツール**］ペイン上)からも実行できます。

ログ エントリの操作を実行するためのガイドラインを次に示します。

目的	操作手順
単一のログ エントリの選択	該当するログ エントリをクリックします。
複数のログ エントリの選択	• *非連続*：［**Ctrl**］キーを押しながら、ログ エントリを 1 つずつクリックします。 • *連続*：1 つのログ エントリを選択し、次に［**Shift**］キーを押しながら別のエントリをクリックします。最初に選択したエントリと最後に選択したエントリの間にあるすべてのエントリが選択されます。
ログ エントリの詳細の表示	1 ログ エントリを 1 つ選択します。 2 次のいずれかを実行します。 • **［詳細の表示］**をクリックします。そのログ エントリの詳細が別のウィンドウに表示されます。 • ［情報］ペインのボタンをクリックして［情報］ペインを展開します。
選択したログ エントリのファイルへの保存	1 1 つまたは複数のログ エントリを選択します。 2 **［選択項目をファイルに保存］**をクリックします。 3 開いたウィンドウで、ファイルのパスと名前を指定します。
すべてのログ エントリのファイルへの保存	1 フィルタが設定されないようにします。 2 **［すべてをファイルに保存］**をクリックします。 3 開いたウィンドウで、ファイルのパスと名前を指定します。
フィルタ処理されたすべてのログ エントリのファイルへの保存	1 フィルタを設定して、フィルタ条件を満たすログ エントリの一覧を取得します。 2 **すべてをファイルに保存］**をクリックします。 3 開いたウィンドウで、ファイルのパスと名前を指定します。この結果、その一覧のログ エントリが保存されます。
すべてのログ エントリの削除	**［ログの消去］**をクリックします。 すべてのログ エントリがログから削除され、新しいログ エントリが作成されます。このエントリには、エントリを削除したユーザーと日時に関する情報が含まれます。

6.1.3.2. ログ エントリのフィルタ処理と並べ替え

ログ エントリのフィルタ処理と並べ替えを実行するためのガイドラインを次に示します。

目的	操作手順
指定した期間のログ エントリの表示	1 ［**開始**］フィールドで、表示するログ エントリの開始日を選択します。 2 ［**終了**］フィールドで、表示するログ エントリの終了日を選択します。
種類によるログ エントリのフィルタ処理	ツールバーの次のボタンを押すか、放します。 エラー メッセージのフィルタ 警告メッセージのフィルタ 情報メッセージのフィルタ
元のバックアップ計画または管理対象のエンティティの種類によるログ エントリのフィルタ処理	［**バックアップ計画**］(または［**管理対象のエンティティの種類**］)項目のヘッダーで、バックアップ計画または管理対象のエンティティの種類を一覧から選択します。
タスク、管理対象のエンティティ、コンピュータ、コード、所有者によるログ エントリのフィルタ処理	必要な値(タスク名、コンピュータ名、所有者名など)をそれぞれの項目のヘッダーの下にあるフィールドに入力します。 この結果、入力した値と完全に一致するか、部分的に一致するログ エントリの一覧が表示されます。
日時によるログ エントリの並べ替え	ログ エントリを昇順で並べ替えるには、項目のヘッダーをクリックします。再度クリックすると、ログ エントリは降順で並べ替えられます。

ログ テーブルの設定

デフォルトでは、テーブルに 7 つの項目が表示され、その他の項目は非表示になります。必要に応じて、表示されている項目を非表示にしたり、非表示の項目を再表示することができます。

列を表示または非表示にする手順は、次のとおりです。

1. 項目のヘッダーを右クリックしてコンテキスト メニューを開きます。チェックボックスをオンにしたメニュー項目が、表のヘッダー項目に表示されます。
2. 表示/非表示を切り換える項目をクリックします。

6.1.3.3. ログ エントリの詳細

選択したログ エントリに関する詳細情報が表示され、詳細をクリップボードにコピーすることができます。

詳細をコピーするには、［**クリップボードにコピー**］ボタンをクリックします。

ログ エントリのデータ フィールド

ローカルのログ エントリには、次のデータ フィールドがあります。

- **［種類］**- イベントの種類(エラー、警告、情報)
- **［日付］**- イベントが発生した日付と時刻
- **［バックアップ計画］**- イベントが関連付けられているバックアップ計画(存在する場合)
- **［タスク］**- イベントが関連付けられているタスク(存在する場合)
- **［コード］**- イベントのプログラム コード。プログラム内のすべての種類のイベントには、独自のコードがあります。コードは、Acronis サポート サービスが問題を解決するために使用する整数です。
- **［モジュール］**- イベントが発生したプログラム モジュールの番号。Acronis サポート サービスが問題を解決するために使用する整数です。
- **［所有者］**- バックアップ計画の所有者のユーザー名(オペレーティング システムにおいてのみ)
- **［メッセージ］**- イベントの説明テキスト

コピーしたログ エントリの詳細は、次のような内容になります。

```
-------------------------ログ エントリの詳細-------------------------
種類:                   情報
日時:                   DD.MM.YYYY HH:MM:SS
バックアップ計画:       バックアップ計画名
タスク:                 タスク名
メッセージ:             操作の説明
コード:                 12(3x45678A)
モジュール:             モジュール名
所有者:                 計画の所有者
-------------------------------------------------------------------
```

日時の形式は、ロケールの設定によって異なります。

6.2. バックアップ計画の作成

最初のバックアップ計画『ページ参照 421』を作成する前に、Acronis Backup & Recovery 10 で使用される基本的な概念『ページ参照 30』について理解しておいてください。

バックアップ計画を作成する手順は、次のとおりです。

全般

計画名

(オプション)バックアップ計画の一意の名前を入力します。わかりやすい名前にすると他の計画と区別することができます。

計画のログイン情報『ページ参照 239』

(オプション)バックアップ計画は、計画を作成したユーザーの代わりに実行されます。計画のアカウント ログイン情報は、必要に応じて変更することができます。このオプションにアクセスするには、［**詳細ビュー**］チェックボックスをオンにします。

コメント

(オプション)バックアップ計画の説明を入力します。このオプションにアクセスするには、［**詳細ビュー**］チェックボックスをオンにします。

バックアップ元

ソースの種類『ページ参照 239』

バックアップするデータの種類を選択します。データの種類はコンピュータにインストールされているエージェントによって異なります。

バックアップする項目『ページ参照 240』

バックアップするデータ項目を指定します。バックアップする項目の一覧は、前に指定したデータの種類によって異なります。

アクセス ログイン情報『ページ参照 241』

(オプション)計画のアカウントがデータにアクセスする権限を持っていない場合は、ソース データのログイン情報を指定します。このオプションにアクセスするには、［**詳細ビュー**］チェックボックスをオンにします。

除外『ページ参照 242』

(オプション)バックアップから除外するファイルの種類を設定します。このオプションにアクセスするには、［**詳細ビュー**］チェックボックスをオンにします。

バックアップの保存先

アーカイブ『ページ参照 243』

バックアップ アーカイブの保存先のパスとアーカイブ名を指定します。アーカイブ名は保存先の中で一意な名前にすることをお勧めします。デフォルトのアーカイブ名は Archive(N) です。N は、選択した保存先内のアーカイブの連番です。

アクセス ログイン情報『ページ参照 245』

(オプション)計画のアカウントが保存先にアクセスする権限を持っていない場合は、保存先のログイン情報を指定します。このオプションにアクセスするには、［**詳細ビュー**］チェックボックスをオンにします。

アーカイブのコメント

(オプション)アーカイブのコメントを入力します。このオプションにアクセスするには、［**詳細ビュー**］チェックボックスをオンにします。

バックアップ方法

バックアップ スキーム『ページ参照 245』

データのバックアップの実行時期と実行間隔を指定し、作成したバックアップ アーカイブを選択した保存先に保存する期間を定義して、アーカイブのクリーンアップ処理のスケジュールを設定します。GFS(Grandfather-Father-Son)、ハノイの塔などのよく知られた最適化されたバックアップ スキームを使用して、カスタム バックアップ スキームを作成するか、データを 1 回だけバックアップします。

アーカイブのベリファイ

ベリファイの実行時期『ページ参照 256』

(オプション)ベリファイの実行時期と実行間隔、およびアーカイブ全体またはアーカイブ内の前回のバックアップのどちらをベリファイするかを定義します。

バックアップ オプション

設定

(オプション)バックアップの前後に実行するコマンド、バックアップ ストリームに割り当てられるネットワークの最大帯域幅、バックアップ アーカイブの圧縮レベルなどのバックアップ操作のパラメータを設定します。このセクションで何も指定しない場合は、デフォルト値『ページ参照 113』が使用されます。

いずれかの設定をデフォルト値から変更すると、新しい行に新しく設定した値が表示されます。設定のステータスが［**デフォルト**］から［**カスタム**］に変更されます。設定を再び変更すると、新しい値がデフォルト値ではない場合に行が表示されます。デフォルト値が設定されると、行が非表示になるので、［**バックアップ計画の作成**］ページのこのセクションには常にデフォルト値と異なる設定のみが表示されます。

すべての設定をデフォルト値にリセットするには、［**デフォルトにリセット**］をクリックします。

すべての必要な処理を実行したら、［**OK**］をクリックしてバックアップ計画を作成します。

その後で、パスワード『ページ参照 238』を要求される場合があります。

作成した計画は、［**バックアップの計画およびタスク**］『ページ参照 221』ビューでテストおよび管理のためにアクセスできます。

6.2.1. パスワードを要求される理由

スケジュールされたタスクまたは延期されたタスクは、ログオンしているユーザーに関係なく実行される必要があります。タスクを実行するログイン情報を明示的に指定していない場合は、プログラムによって、現在ログオンしているユーザーのアカウントが提示されます。パスワードを入力するか、別のアカウントを指定するか、またはスケジュールされたタスクを手動で開始するタスクに変更します。

6.2.2. バックアップ計画のログイン情報

計画のタスクを実行するアカウントのログイン情報を指定します。

ログイン情報を指定する手順は、次のとおりです。

1. 次のいずれかを選択します。
   - **現在のログイン情報を使用する**

     タスクは、タスクを起動するユーザーがログインしたときのログイン情報を使用して実行されます。スケジュールに従っていずれかのタスクを実行する必要がある場合は、計画の作成を完了する際に現在のユーザーのパスワードを入力するよう求められます。
   - **次のログイン情報を使用する**

     タスクは、手動で開始されるか、スケジュールに従って実行されるかにかかわらず、常にユーザーが指定するログイン情報を使用して実行されます。

     次の項目を指定します。
     - **［ユーザー名］**- Active Directory ユーザー アカウントの名前を入力する場合は、ドメイン名(DOMAIN¥ユーザー名またはユーザー名@ドメイン)も指定してください。
     - **［パスワード］**- アカウントのパスワード。
2. **［OK］**をクリックします。

ユーザー権限に応じて使用可能になる操作の詳細については、「管理対象のコンピュータ上のユーザー権限『ページ参照 34』」をご参照ください。

6.2.3. ［ソースの種類］

管理対象のコンピュータでバックアップするデータの種類を選択します。使用可能なデータの種類の一覧は、コンピュータで実行しているエージェントによって異なります。

［ファイル］

Acronis Backup & Recovery 10 エージェント for Windows(またはエージェント for Linux)がインストールされている場合に使用できます。

特定のファイルとフォルダをバックアップするには、このオプションを選択します。

すべての設定およびアプリケーションとともにオペレーティング システムを復元するつもりはないが、現在のプロジェクトなどの特定のデータだけを保護する予定の場合は、ファイルのバックアップを選択します。これによりアーカイブ サイズが減少するので、ストレージ領域を節約できます。

［ディスク/ボリューム］

Acronis Backup & Recovery 10 エージェント for Windows(またはエージェント for Linux)がインストールされている場合に使用できます。

ディスクまたはボリュームをバックアップするには、このオプションを選択します。ディスクまたはボリュームをバックアップするには、Administrator または Backup Operator の権限が必要です。

ディスクおよびボリュームをバックアップすると、重大なデータ損傷やハードウェア障害が発生した場合にシステム全体を復元できます。バックアップ手順はファイルのコピーよりも高速で、大量のデータをバックアップする場合にバックアップ処理を大幅に高速化できます。

Linux ユーザー向けの注意: *ボリュームのバックアップを開始する前に、ext2 ファイル システムなどの非ジャーナリング ファイル システムを含むすべてのボリュームをマウント解除しておくことをお勧めします。マウント解除しないと、復元時に破損したファイルが含まれる可能性があり、サイズ変更を伴うこれらのボリュームの復元が失敗することがあります。*

6.2.4. バックアップする項目

バックアップする項目は、前に選択したソースの種類『ページ参照 239』によって決まります。

6.2.4.1. ディスクとボリュームの選択

バックアップするディスクまたはボリュームを指定する手順は、次のとおりです。

1. バックアップするディスクまたはボリュームのチェックボックスをオンにします。ディスクやボリュームの任意の組み合わせを指定することができます。

   オペレーティング システムとローダーが別のボリュームにあるときは、必ず両方のボリュームをバックアップに含めてください。また、これらのボリュームはまとめて復元する必要があります。そうしないと、オペレーティング システムが起動しなくなる危険性があります。

2. (オプション)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には、**[セクタ単位でバックアップ]** チェックボックスをオンにします。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)。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ドライブをバックアップするときに使用します。

3. **[OK]** をクリックします。

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

サポートされているファイル システムのディスクまたはボリュームのバックアップでは、セクタ単位のオプションをオフにした場合、データを含むセクタのみが保存されます。これにより、作成されるバックアップのサイズが小さくなり、バックアップと復元の処理速度が向上します。

Windows

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)はバックアップされません。復元後は、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。

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。GPT ボリュームのブート コードはバックアップされません。

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。

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フォルダ、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。

6.2.4.2. ファイルとフォルダの選択

バックアップするファイルまたはフォルダを選択する手順は、次のとおりです。

1. ローカル フォルダのツリー項目を展開して、入れ子になったファイルとフォルダを表示します。
2. ツリー内の対応するチェックボックスをオンにして項目を選択します。フォルダのチェックボックスをオンにすると、そのすべての内容(ファイルとフォルダ)がバックアップされます。これは、将来そのフォルダに作成される新しいファイルにも適用されます。

   ファイル ベースのバックアップは、オペレーティング システムの復元には不十分です。オペレーティング システムを復元するには、ディスク バックアップを実行する必要があります。

   ウィンドウの右側のテーブルを使用して、入れ子になった項目を参照および選択します。**[名前]** 列の見出しの横にあるチェックボックスをオンにすると、テーブル内のすべての項目が自動的に選択されます。このチェックボックスをオフにすると、すべての項目が自動的に選択解除されます。
3. **[OK]** をクリックします。

6.2.5. ソースのアクセス ログイン情報

バックアップするデータにアクセスするために必要なログイン情報を指定します。

ログイン情報を指定する手順は、次のとおりです。

1. 次のいずれかを選択します。
   - **計画のログイン情報を使用する**

     [全般] セクションで指定されたバックアップ計画のアカウントのログイン情報を使用して、ソース データにアクセスします。
   - **[次のログイン情報を使用する]**

     ユーザーが指定するログイン情報を使用して、そのデータ ソースにアクセスします。計画のアカウントがデータにアクセスする権限を持っていない場合にこのオプションを使用します。

次の項目を指定します。

- **［ユーザー名］**- Active Directory ユーザー アカウントの名前を入力する場合は、ドメイン名(DOMAIN¥ユーザー名またはユーザー名@ドメイン)も指定してください。
- **［パスワード］**- アカウントのパスワード。

2. **［OK］**をクリックします。

6.2.6. 除外

バックアップから除外するファイルの種類を設定します。たとえば、データベース、隠しファイルと隠しフォルダ、システム ファイルとシステム フォルダ、特定の拡張子が付いたファイルをアーカイブに保存したくない場合があります。

除外するファイルおよびフォルダを指定する手順は、次のとおりです。

次のいずれかのパラメータを設定します。

- **すべての隠しファイルおよびフォルダを除外**

  隠しファイル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。

- **すべてのシステム ファイルおよびフォルダを除外**

  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設定されてい場合、フォルダの内容はシステム属性を設定されていないファイルを含みすべて除外されます。

***attrib** コマンドを使用してファイルまたはフォルダのファイル/フォルダ プロパティ内の属性を表示することができます。詳細については、Windows の［ヘルプとサポート］をご参照ください。*

- **次の条件に一致するファイルを除外**

  一覧内のいずれかの条件(ファイル マスクと呼ばれます)に一致するファイル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。ファイル マスクの一覧を作成するには、**［追加］**、**［編集］**、**［削除］**、および**［すべて削除］**ボタンを使用します。

  1 つ以上のワイルドカード文字(* および ?)をファイル マスク内で使用することができます。

  アスタリスク(*)はファイル名内の 0 個以上の文字の代用として使用します。たとえば、ファイル マスク Doc*.txt は Doc.txt、Document.txt などの文字と一致します。

  疑問符(?)はファイル名内の厳密に 1 文字の代用として使用します。たとえば、ファイルマスク Doc?.txt は Doc1.txt、Docs.txt などのファイルと一致しますが、Doc.txt、Doc11.txt などのファイルとは一致しません。

除外の例

条件	例	説明
名前	File1.log	File1.log という名前のすべてのファイルを除外します。
パス	C:¥Finance¥test.log	C:¥Finance フォルダに置かれている test.log という名前のファイルを除外します。
マスク(*)	*.log	.log 拡張子の付いたすべてのファイルを除外します。
マスク(?)	my???.log	5 文字で最初が「my」で始まる名前のすべての .log ファイルを除外します。

6.2.7. アーカイブ

アーカイブの保存場所と名前を指定します。

1. 保存先の選択

保存先の完全なパスを［**パス**］フィールドに入力するか、フォルダ ツリーから保存先を選択します。

- 集中管理用格納域にデータをバックアップするには、［**集中管理**］グループを展開し、格納域をクリックします。
- 個人用格納域にデータをバックアップするには、［**個人用**］グループを展開し、格納域をクリックします。
- コンピュータ上のローカル フォルダにデータをバックアップするには、［**ローカル フォルダ**］グループを展開し、目的のフォルダをクリックします。
- ネットワーク共有にデータをバックアップするには、［**ネットワーク フォルダ**］グループを展開し、目的のネットワーク コンピュータを選択して、共有フォルダをクリックします。ネットワーク共有がアクセス ログイン情報を必要とする場合は、それらの情報が要求されます。

> ***Linux ユーザー向けの注意: /mnt/share*** *などのマウント ポイントにマウントされている CIFS(Common Internet File System)のネットワーク共有を指定するには、ネットワーク共有そのものではなく、このマウント ポイントを選択します。*

- **FTP** サーバーまたは **SFTP** サーバーにデータをバックアップするには、［**パス**］フィールドにサーバー名またはアドレスを次のように入力します。

  ftp://ftp_server:port _number または **sftp://sftp_server:port number**

  ポート番号が指定されていない場合、ポート 21 が FTP 用に、ポート 22 が SFTP 用に使用されます。

  アクセス ログイン情報を入力すると、サーバー上のフォルダが使用できるようになります。サーバー上の適切なフォルダをクリックします。

  匿名アクセスがサーバーによって許可されている場合、匿名ユーザーとしてサーバーにアクセスすることができます。匿名ユーザーとしてアクセスするには、ログイン情報を入力する代わりに、［**匿名アクセスを使用する**］をクリックします。

FTP 仕様の原文に記載されているように、FTP サーバーにアクセスするのに必要なログイン情報は、ネットワーク上をテキスト形式で転送されます。このことは、ユーザー名とパスワードが、パケット スニファを使用した盗聴者によって傍受される可能性があることを意味します。

- ローカル接続したテープ デバイスにデータをバックアップするには、［**テープ ドライブ**］グループを展開し、目的のデバイスをクリックします。

2. アーカイブ テーブルの使用

正しい保存先を選択できるように、選択した各場所に含まれているアーカイブの名前がテーブルに表示されます。アーカイブの保存場所の内容を確認しているとき、別のユーザーまたはスケジュール設定された処理によって、アーカイブが追加、削除、または変更されることがあります。［**更新**］を使用すれば、アーカイブの一覧を更新できます。

3. 新しいアーカイブの名前付け

アーカイブの保存先を選択すると、プログラムにより新しいアーカイブの名前が生成され、［**名前**］フィールドに表示されます。この名前は通常、「Archive(1)」のようになります。生成された名前は、選択した場所内で一意です。自動的に生成された名前をそのまま使用する場合は、［**OK**］をクリックします。別の名前を使用する場合は、一意の名前を入力し、［**OK**］をクリックします。

既存のアーカイブへのバックアップ

既存のアーカイブにバックアップするバックアップ計画を設定できます。これを行うには、アーカイブ テーブルでアーカイブを選択するか、アーカイブ名を［**名前**］フィールドに入力します。アーカイブがパスワードで保護されている場合、パスワードの入力を求めるポップアップウィンドウが表示されます。

既存のアーカイブを選択すると、そのアーカイブを使用する別のバックアップ計画の領域に影響を与えることになります。別の計画が中止されている場合は、このことは問題にはなりませんが、通常は「1 つのバックアップ計画に対して 1 つのアーカイブを使用する」というルールに従う必要があります。このルールに従わなくてもプログラムは機能しますが、いくつかの特別な場合を除き、実用的または効率的ではありません。

2 つ以上の計画を同じアーカイブにバックアップすべきではない理由

1. 異なるソースを同じアーカイブにバックアップすると、操作性の観点からアーカイブの使用が困難になります。復元する際には、少しでも早く復元を完了させることが重要になりますが、異なるソースが同じアーカイブにバックアップされていると、復元すべきアーカイブの内容の見極めが複雑になってしまいます。

   同じアーカイブを操作するバックアップ計画は、同じデータ項目をバックアップする必要があります(たとえば、両方の計画がボリューム C をバックアップする)。

2. 複数の保持ルールをアーカイブに適用すると、アーカイブの内容が予測不能になります。それぞれのルールがアーカイブ全体に適用されるので、あるバックアップ計画に含まれるバックアップは、別のバックアップ計画に含まれるバックアップとともに簡単に削除されてしまう可能性があります。GFS およびハノイの塔のバックアップ スキームの標準的な動作は期待すべきではありません。

   通常、複雑なバックアップ計画はそれぞれ独自のアーカイブにバックアップします。

6.2.8. アーカイブの保存先のアクセス ログイン情報

バックアップ アーカイブの保存先にアクセスするために必要なログイン情報を指定します。名前が指定されたユーザーがアーカイブの所有者と見なされます。

ログイン情報を指定する手順は、次のとおりです。

1. 次のいずれかを選択します。
   - **計画のログイン情報を使用する**

     [全般] セクションで指定されたバックアップ計画のアカウントのログイン情報を使用して、ソース データにアクセスします。
   - **[次のログイン情報を使用する]**

     ユーザーが指定するログイン情報を使用して、そのデータ ソースにアクセスします。計画のアカウントが保存先にアクセスする権限を持っていない場合にこのオプションを使用します。ネットワーク共有またはストレージ ノードの格納域に対しては、特別なログイン情報を指定する必要がある場合があります。

     次の項目を指定します。

     - **[ユーザー名]** - Active Directory ユーザー アカウントの名前を入力する場合は、ドメイン名(DOMAIN¥ユーザー名またはユーザー名@ドメイン)も指定してください。
     - **[パスワード]** - アカウントのパスワード。
2. **[OK]** をクリックします。

警告: *FTP 仕様の原文に記載されているように、FTP サーバーにアクセスするのに必要なログイン情報は、ネットワーク上をテキスト形式で転送されます。このことは、ユーザー名とパスワードが、パケット スニファを使用した盗聴者によって傍受される可能性があることを意味します。*

6.2.9. バックアップ スキーム

次の使用可能なバックアップ スキームのいずれかを選択します。

- **[今すぐバックアップ]** - 手動で開始するためのバックアップ タスクを作成し、作成後すぐにタスクを実行します。
- **[後でバックアップ]** - 手動で開始するためのバックアップ タスクを作成するか、将来 1 回だけ実行するタスクをスケジュールします。
- **[シンプル]** - データのバックアップの実行時期と実行間隔をスケジュールし、保持のルールを指定します。
- **[GFS(Grandfather-Father-Son)]** - Grandfather-Father-Son(祖父–父–息子)のバックアップ スキームを使用します。このスキームでは、1 日に 2 回以上データのバックアップを行うことはできません。日単位のバックアップを実行する曜日を設定し、それらの日の中から週単位または月単位のバックアップの日を選択します。次に、日単位(「Son」と呼ばれます)、週単位(「Father」と呼ばれます)、月単位(「Grandfather」と呼ばれます)のバックアップの保存期間を設定します。期限切れになったバックアップは自動的に削除されます。

- **[ハノイの塔]** - ハノイの塔バックアップ スキームを使用します。バックアップ(セッション)の実行時期と実行間隔をスケジュールし、バックアップ レベル数(最大 16)を選択します。このスキームでは、1 日に複数回データをバックアップすることができます。バックアップ スケジュールを設定し、バックアップ レベルを選択することによって、ロールバック期間(いつでも戻ることができる保証されたセッション数)が自動的に取得されます。自動クリーンアップ メカニズムは、期限切れになったバックアップを削除し、各レベルの最新のバックアップを保持することによって必要なロールバック期間を維持します。
- **[カスタム]** - カスタム スキームを作成して、会社に最適なバックアップ戦略を自由に設定することができます。異なるバックアップの種類に対する複数のスケジュールの指定、条件の追加、保持のルールの指定を行うことができます。

6.2.9.1. 「今すぐバックアップ」スキーム

「**今すぐバックアップ**」スキームでは、ページの下部にある **[OK]** ボタンをクリックするとすぐにバックアップが実行されます。

[バックアップの種類] フィールドで、完全バックアップ、増分バックアップまたは差分バックアップ『ページ参照 37』のどれを作成するかを選択します。

6.2.9.2. 「後でバックアップ」スキーム

「後でバックアップ」スキームでは、指定した日時にバックアップが 1 回だけ実行されます。

次の項目に適切な値を指定します。

バックアップの種類	完全、増分、または差分のいずれかのバックアップの種類を選択します。アーカイブ内に完全バックアップがない場合は、選択に関係なく完全バックアップが作成されます。
日付と時刻	バックアップを開始する日時を指定します。
タスクを手動で開始する	バックアップ タスクをスケジュールする必要がなく後で手動で開始する場合は、このチェックボックスをオンにします。

6.2.9.3. 「シンプル」スキーム

シンプル バックアップ スキームでは、データのバックアップの実行時期と実行間隔のみをスケジュールし、保持のルールを設定します。最初は完全バックアップが作成されます。次のバックアップは増分になります。

シンプル バックアップ スキームを設定するには、次の項目に適切な値を指定します。

バックアップ	バックアップ スケジュール(データのバックアップの実行時期と実行間隔)を設定します。 スケジュールの設定の詳細については、「スケジュール『ページ参照 199』」をご参照ください。
保持のルール	シンプル スキームでは、1 つの保持ルール『ページ参照 46』のみを使用できます。バックアップの保存期間を設定します。

6.2.9.4. 「GFS(Grandfather-Father-Son」スキーム

概要

- 日単位の増分バックアップ、週単位の差分バックアップ、月単位の完全バックアップ
- 週単位および月単位のバックアップのカスタム日付
- 各種類のバックアップのカスタム保存期間

説明

日単位(D)、週単位(W)、および月単位(M)の一連のバックアップを定期的に生成するバックアップ計画を設定すると仮定します。通常は次のような方法でこれを実行します。次の表に、2 か月間のこの計画の例を示します。

	月	火	水	木	金	土	日
1/1 — 1/7	D	D	D	D	W	-	-
1/8 — 1/14	D	D	D	D	W	-	-
1/15 — 1/21	D	D	D	D	W	-	-
1/22 — 1/28	D	D	D	D	M	-	-
1/29 — 2/4	D	D	D	D	W	-	-
2/5 — 2/11	D	D	D	D	W	-	-
2/12 — 2/18	D	D	D	D	W	-	-
2/19 — 2/25	D	D	D	D	M	-	-
2/26 — 3/4	D	D	D	D	W	-	-

日単位のバックアップは、金曜日を除くすべての平日に実行され、金曜日には週単位および月単位のバックアップが実行されます。月単位のバックアップは毎月第 4 金曜日に実行され、週単位のバックアップは他のすべての金曜日に実行されます。

- 月単位(Grandfather)のバックアップは完全バックアップ。
- 週単位(Father)のバックアップは差分。
- 日単位(Son)のバックアップは増分。

パラメータ

GFS(Grandfather-Father-Son)スキームでは、次のパラメータを設定できます。

バックアップの開始時刻:	バックアップを開始する時刻を指定します。デフォルト値は午後 12 時です。
バックアップの実行日:	バックアップを実行する日付を指定します。デフォルト値は平日です。
週単位/月単位:	**[バックアップの実行日]** フィールドで選択した日のうちどの日を週単位または月単位のバックアップ用に予約するかを指定します。月単位のバックアップは毎月 4 番目のその曜日に実行されます。デフォルト値は金曜日です。
バックアップの保存期間:	バックアップをアーカイブ内に保存する期間を指定します。期間は、時間、日、週、月、年で設定できます。月単位のバックアップでは、無期限に保存する場合は **[無期限に保持]** を選択することもできます。 各バックアップの種類のデフォルト値は次のとおりです。 日単位: 1 週間(推奨される最小値) 週単位: 1 か月間(バックアップの保存期間 1 か月は 4 週間と同じです) 月単位: 無期限 週単位のバックアップの保存期間は日単位のバックアップより長くする必要があり、月単位のバックアップの保存期間は週単位のバックアップの保存期間より長くする必要があります。 日単位のバックアップの保存期間を 1 週間以上に設定することをお勧めします。

常に、バックアップは、そのバックアップに直接依存しているすべてのバックアップも削除対象になるまで削除されません。このため、有効期限が数日経過した週単位または月単位のバックアップがアーカイブ内に残っている場合があります。

スケジュールによって最初に日単位または週単位のバックアップが開始される場合は、代わりに完全バックアップが作成されます。

例

先週の各曜日、先月の各週

多くのユーザーが役立つと考える GFS バックアップ スキームについて考えてみましょう。

- 週末を含む毎日ファイルをバックアップする。
- 過去 7 日間の任意の日付のファイルを復元できる。
- 先月の週単位のバックアップにアクセスできる。
- 月単位のバックアップを無期限に保存する。

バックアップ スキームのパラメータを次のように設定できます。

- バックアップの開始時刻: **午後 11:00**
- バックアップの実行日: **毎日**
- 週単位/月単位: **土曜日**(例)
- バックアップの保存期間:
  - 日単位: **1 週間**
  - 週単位: **1 か月**
  - 月単位: **無期限**

結果として、日単位、週単位、月単位のバックアップのアーカイブが作成されます。日単位のバックアップは作成後 7 日間使用できます。たとえば、1 月 1 日(日曜日)の日単位のバックアップは次の 1 月 8 日(日曜日)まで使用できます。1 月 7 日(土曜日)の最初の週単位のバックアップは、2 月 7 日までシステムに保存されます。月単位のバックアップは削除されません。

ストレージの制限

大きなアーカイブを保存するために膨大なサイズの格納域を用意したくない場合は、バックアップの保存期間が短くなるように GFS スキームを設定し、同時に不測のデータ損失が発生した場合に情報を復元できるようにすることができます。

次のような要件があると仮定します。

- 各平日の最後にバックアップを実行する。
- 誤って削除されたかまたは不注意で変更されたファイルを、比較的早期に見つかった場合に復元できる。
- 週単位のバックアップに作成後 10 日間アクセスできる。
- 月単位のバックアップを半年間保存する。

バックアップ スキームのパラメータを次のように設定できます。

- バックアップの開始時刻: **午後 6:00**
- バックアップの実行日: **平日**
- 週単位/月単位: **金曜日**

- バックアップの保存期間:
  - 日単位: **1 週間**
  - 週単位: **10 日**
  - 月単位: **6 か月**

このスキームを使用すると、破損したファイルの以前のバージョンを日単位のバックアップから 1 週間にわたり復元でき、週単位のバックアップに 10 日間アクセスできます。それぞれの月単位の完全バックアップは、作成日から 6 か月間使用できます。

作業スケジュール

非常勤の会計コンサルタントとして、火曜日と木曜日に会社で作業をしているとします。これらの日には、自分のラップトップ コンピュータで会計文書や財務諸表の変更、スプレッドシートの更新などを行います。このデータをバックアップするために、次の作業を行います。

- 火曜日と木曜日に行った財務諸表やスプレッドシートなどに対する変更の追跡(日単位の増分バックアップ)。
- 先月以降のファイルの変更に関する週単位の要約の作成(金曜日の週単位の差分バックアップ)。
- 月単位のファイルの完全バックアップ。

また、日単位のバックアップを含め、最近 6 か月のすべてのバックアップにアクセスできるようにします。

このような目的には、次の GFS スキームが適しています。

- バックアップの開始時刻: **午後 11 時 30 分**
- バックアップの実行日: **火曜日、木曜日、金曜日**
- 週単位/月単位: **金曜日**
- バックアップの保存期間:
  - 日単位: **6 か月**
  - 週単位: **6 か月**
  - 月単位: **5 年**

これで、火曜日と木曜日に日単位の増分バックアップが作成され、金曜日は週単位と月単位のバックアップが実行されます。［**週単位/月単位**］フィールドで［**金曜日**］を選択するには、まず［**バックアップの実行日**］フィールドでその曜日を選択しておく必要があります。

このようなアーカイブを作成すると、作業の最初の日と最後の日の会計文書の比較、すべての文書の 5 年間にわたる履歴の保持などを行うことができます。

日単位のバックアップなし

次のような少し変わった GFS スキームについて考えてみます。

- バックアップの開始時刻: **午後 12:00**
- バックアップの実行日: **金曜日**
- 週単位/月単位: **金曜日**

- バックアップの保存期間:
  - 日単位: **1 週間**
  - 週単位: **1 か月**
  - 月単位: **無期限**

このスキームでは、バックアップは金曜日にのみ実行されます。これにより、金曜日に週単位または月単位のバックアップが実行され、日単位のバックアップを行う他の曜日は残っていません。そのため、作成される "祖父-父" アーカイブは、週単位の差分バックアップと月単位の完全バックアップのみで構成されます。

GFS を使用するとこのようなアーカイブを作成することもできますが、この状況にはカスタムスキームのほうがより柔軟に対応できます。

6.2.9.5. 「ハノイの塔」スキーム

概要

- 最大 16 レベルの完全バックアップ、差分バックアップ、および増分バックアップ
- 次のレベルのバックアップは、前のレベルのバックアップの 2 倍希薄になる。
- 一度に 1 つ各レベルのバックアップが保存される。
- 新しいバックアップほど密度が高くなる。

パラメータ

ハノイの塔スキームでは、次のパラメータを設定できます。

スケジュール	日単位『ページ参照 200』、週単位『ページ参照 203』、または月単位『ページ参照 205』のスケジュールを設定します。スケジュールのパラメータを設定すると、シンプル スケジュール(例: 1 日おきに午前 10 時にバックアップ タスクを実行する単純な日単位のスケジュール)およびより複雑なスケジュール(例: 1 月 15 日から 3 日おきにタスクを実行し、指定した日の午前 10 時から午後 10 時までの間に 2 時間おきにタスクを繰り返すような複雑な日単位のスケジュール)を作成できます。このように、複雑なスケジュールではスキームを実行するセッションを指定します。下の説明では、「日」を「スケジュールされたセッション」に置き換えることができます。
レベル数	2 から 16 までのバックアップ レベルを選択します。詳細については、以下の例をご参照ください。
ロールバック期間	アーカイブ内でいつでも戻ることができる保証されたセッション数。スケジュールのパラメータと選択したレベル数に応じて自動的に計算されます。詳細については、以下の例をご参照ください。

例

[**スケジュール**] パラメータを次のように設定します。

- 繰り返し: 1 日に 1 回
- 間隔: 午後 6 時に 1 回のみ

レベル数: 4

このスキームのスケジュールの最初の 14 日間(14 セッション)は次のようになります。同じ数字は同じバックアップ レベルを示します。

1	2	3	4	5	6	7	8	9	10	11	12	13	14
4	1	2	1	3	1	2	1	4	1	2	1	3	1

レベルが異なるバックアップは種類が異なります。

- *最後のレベル*(この場合はレベル4)のバックアップは完全。
- *中間レベル*(2、3)のバックアップは差分。
- *最初のレベル*(1)のバックアップは増分。

クリーンアップ メカニズムにより、各レベルの最新のバックアップのみが保持されます。次に、新しい完全バックアップを作成する前の日である 8 日目のアーカイブの状態を示します。

1	2	3	4	5	6	7	8
4	1	2	1	3	1	2	1

このスキームではデータ ストレージの効率が上がり、現時点に近いほどバックアップの間隔は密となります。4 つのバックアップがあれば、今日、昨日、半週前、または 1 週間前のデータを復元できます。

ロールバック期間

アーカイブ内で戻ることができる日数は、日によって異なります。保証されている最少日数はロールバック期間と呼ばれます。

次の表は、さまざまなレベルのスキームの完全バックアップとロールバック期間を示しています。

レベル数	完全バックアップの周期	復元可能日数	ロールバック期間
2	2 日	1 ～ 2 日	1 日
3	4 日	2 ～ 5 日	2 日
4	8 日	4 ～ 11 日	4 日
5	16 日	8 ～ 23 日	8 日
6	32 日	16 ～ 47 日	16 日

レベルが 1 つ増えると完全バックアップおよびロールバックの期間が 2 倍になります。

復元可能日数が異なる理由を確認するために、もう一度前の例を見てみましょう。

12 日目には次のバックアップがあります(背景が灰色の数字は削除されたバックアップを表します)。

1	2	3	4	5	6	7	8	9	10	11	12
4	1	2	1	3	1	2	1	4	1	2	1

新しいレベル 3 の差分バックアップはまだ作成されていないので、5 日目のバックアップがまだ保存されています。このバックアップは 1 日目の完全バックアップに依存しているので、この完全バックアップも使用可能です。これにより 11 日前まで戻ることが可能になるので、これが最善のシナリオです。

ただし、次の日には、新しい第 3 レベルの差分バックアップが作成され、古い完全バックアップは削除されます。

1	2	3	4	5	6	7	8	9	10	11	12	13
4	1	2	1	3	1	2	1	4	1	2	1	3

これにより、復元可能日は 4 日間のみとなるので、これは最悪のシナリオです。

14 日目の復元可能日は 5 日間です。復元可能日は再び減少に変わるまで後続の日にも増加していきます。

1	2	3	4	5	6	7	8	9	10	11	12	13	14
4	1	2	1	3	1	2	1	4	1	2	1	3	1

ロールバック期間は、最悪の状況でも保証されている日数を示します。4 レベルのスキームの場合は 4 日間です。

6.2.9.6. カスタム バックアップ スキーム

概要

- 各種類のバックアップのカスタム スケジュールと条件
- カスタムのスケジュールと保持ルール

パラメータ

パラメータ	意味
完全バックアップ	完全バックアップを実行するスケジュールと条件を指定します。 たとえば、毎週日曜日の午前 1 時にすべてのユーザーがログオフした後すぐに完全バックアップを実行するように設定することができます。
増分	増分バックアップを実行するスケジュールと条件を指定します。 タスクを実行したときにアーカイブにバックアップが含まれていない場合は、増分バックアップの代わりに完全バックアップが作成されます。
差分	差分バックアップを実行するスケジュールと条件を指定します。 タスクを実行したときにアーカイブに完全バックアップが含まれていない場合は、差分バックアップの代わりに完全バックアップが作成されます。
保持のルール	アーカイブに適用する保持ルールを指定します。 たとえば、6 か月以上経過しているすべてのバックアップを削除するようにクリーンアップ処理を設定することができます。
ルールの適用 (保持のルールが設定されている場合のみ)	保持のルール『ページ参照 46』を適用する時期を指定します。 たとえば、各バックアップ後およびスケジュールされた日時にクリーンアップ処理を実行するように設定することができます。 このオプションは、**［保持のルール］**で少なくとも 1 つの保持のルールを設定している場合のみ使用可能です。
クリーンアップ スケジュール (**［スケジュールに従う］**を選択している場合のみ)	アーカイブ クリーンアップのスケジュールを指定します。 たとえば、各月の最後の日に開始されるようにクリーンアップをスケジュールすることができます。 このオプションは、**［ルールの適用］**で**［スケジュールに従う］**を選択した場合のみ使用可能です。

例

週単位の完全バックアップ

次のバックアップ スキームでは、毎週金曜日の夜に完全バックアップが実行されます。

完全バックアップ: スケジュール: 週単位、金曜日ごと、午後 10:00

ここでは、**［完全バックアップ］**の**［スケジュール］**以外のパラメータはすべて空白のままになります。アーカイブ内のすべてのバックアップは無期限に保持されます(アーカイブのクリーンアップは実行されません)。

完全バックアップおよび増分バックアップとクリーンアップ

次のようなスキームを使用したアーカイブは、毎週の完全バックアップと毎日の増分バックアップで構成されます。完全バックアップを開始するには、すべてのユーザーがログオフする必要があります。

完全バックアップ: スケジュール: 週単位、金曜日ごと、午後 10:00

完全バックアップ: 条件: ユーザーのログオフ

増分: スケジュール: 週単位、すべての平日、午後 9:00

さらに、1 年以上経過しているすべてのバックアップをアーカイブから削除し、新しいバックアップを作成する際にクリーンアップを実行します。

保持ルール: 12 か月経過したバックアップを削除

ルールの適用: バックアップ後

デフォルトでは、1 年以上経過している完全バックアップは、これに依存するすべての増分バックアップが削除対象にならない限り削除されません。詳細については、「保持ルール『ページ参照 46』」をご参照ください。

月単位の完全バックアップ、週単位の差分バックアップ、および日単位の増分バックアップとクリーンアップ

この例は、カスタム スキームで利用できるすべてのオプションの使用方法を示しています。

月単位で完全バックアップ、週単位で差分バックアップ、および日単位で増分バックアップを作成するスキームが必要だとします。このときのバックアップ スケジュールは次のようになります。

完全バックアップ: スケジュール: 月単位、毎月の**最終日曜日、午後 9:00**

増分: スケジュール: 週単位、すべての**平日、午後 7:00**

差分: スケジュール: 週単位、土曜日ごと、午後 8:00

さらに、バックアップ タスクを開始するための条件を追加することができます。この条件は、それぞれのバックアップの種類の［**条件**］フィールドに設定します。

完全バックアップ: 条件: ロケーションが使用可能

増分: 条件: ユーザーのログオフ

差分: 条件: ユーザーがアイドル状態

これにより、本来は午後 9:00 にスケジュールされている完全バックアップが、実際にはそれより遅く、バックアップ ロケーションが使用できるようになった直後に開始されることがあります。同様に、増分バックアップと差分バックアップのバックアップ タスクはそれぞれ、すべてのユーザーがログオフするまで、およびユーザーがアイドル状態になるまで待機します。

最後に、アーカイブの保持ルールを作成します。作成後 6 か月以内のバックアップのみを保持し、各バックアップ タスクの終了後および毎月の最終日にクリーンアップを実行します。

保持ルール: 6 か月経過したバックアップを削除

ルールの適用: バックアップ後、スケジュールに従う

クリーンアップ スケジュール: 月単位、毎月の最終日、午後 10:00

デフォルトでは、バックアップは、そのバックアップに依存し、保持する必要があるバックアップがあるときは削除されません。たとえば、完全バックアップが削除の対象となっても、そのバックアップに依存する増分バックアップまたは差分バックアップがあるときは、依存するバックアップもすべて削除できるようになるまで、完全バックアップの削除は延期されます。

詳細については、「保持ルール『ページ参照 46』」をご参照ください。

生成されるタスク

すべてのカスタム スキームは常に 3 つのバックアップ タスクを生成し、保持のルールが指定されている場合はさらにクリーンアップ タスクを生成します。タスクの一覧内で各タスクは［**スケジュール済み**］(スケジュールが設定されている場合)または［**手動**］(スケジュールが設定されていない場合)と表示されます。

スケジュールされているかどうかに関係なく、いつでも任意のバックアップ タスクまたはクリーンアップ タスクを手動で実行することができます。

前の例の冒頭では、完全バックアップのスケジュールのみを設定しました。しかし、それでもスキームにより 3 つのバックアップ タスクが生成され、次の種類のバックアップを手動で開始することができます。

- 完全バックアップを毎週金曜日の午後 10 時に実行する。
- 増分バックアップを手動で実行する。
- 差分バックアップを手動で実行する。

左側のペインの［**バックアップの計画およびタスク**］セクションでタスクの一覧からこれらのバックアップ タスクを選択して、実行できます。

バックアップ スキームで保持のルールも指定している場合は、スキームは 4 つのタスク(3 つのバックアップ タスクと 1 つのクリーンアップ タスク)が生成されます。

6.2.10. アーカイブのベリファイ

バックアップ データが復元可能かどうかを確認するにはベリファイ タスクを設定します。バックアップのベリファイ結果が不合格の場合は、ベリファイ タスクが失敗し、バックアップ計画がのステータスがエラーになります。

ベリファイを設定するには、次のパラメータを指定します。

1. ［**ベリファイの実行時期**］- ベリファイを実行する時期を選択します。ベリファイは多くのリソースを使用する処理なので、管理対象のコンピュータのピーク時以外にベリファイを**スケジュール**するのが効果的です。これに対し、ベリファイがデータ保護戦略の主要な部分になっていて、バックアップされたデータに破損がなく正常に復元できるかどうかをすぐに知りたい場合は、バックアップ作成後すぐにベリファイを開始することを検討してください。

2. **[ベリファイの対象]** - アーカイブ全体またはアーカイブ内の前回のバックアップのどちらをベリファイするかを選択します。ファイル バックアップのベリファイでは、バックアップからダミーの復元先に対してすべてのファイルの復元を疑似的に実行します。ボリューム バックアップのベリファイでは、バックアップに保存されているすべてのデータ ブロックのチェックサムを計算します。アーカイブのベリファイでは、すべてのアーカイブのバックアップをベリファイするので、長い時間がかかり多くのシステム リソースを使用する場合があります。
3. **[ベリファイのスケジュール]** (手順 1 でスケジュールに従うように選択した場合のみ表示されます) - ベリファイのスケジュールを設定します。詳細については、「スケジュール『ページ参照 199』」をご参照ください。

6.3. データの復元

データを復元する場合は、まず、最も機能的な方法を検討します。コンソールを**オペレーティング システムを実行する管理対象のコンピュータ**に接続し、復元タスクを作成します。

管理対象のコンピュータの**オペレーティング システムが起動しない場合**、または**ベア メタル状態のディスクにデータを復元する**必要がある場合は、ブータブル メディア『ページ参照 423』からコンピュータを起動するか、Acronis リカバリ マネージャ『ページ参照 60』を使用します。次に、復元タスクを作成します。

Acronis Universal Restore『ページ参照 61』を使用すると、**異なるハードウェア上の Windows** または仮想コンピュータを復元して起動することができます。

復元中に、**Windows システムを数秒以内にオンラインにすることができます**。Acronis Backup & Recovery 10 は、独自の Acronis Active Restore『ページ参照 63』 テクノロジを使用して、システムが物理ディスク上にある場合と同様に、バックアップ内に見つかったオペレーティング システムからコンピュータを起動します。システムが使用可能になり、必要なサービスを提供できるようになります。したがって、システムのダウンタイムは最小になります。

ダイナミック ボリュームは、既存のボリューム上(ディスク グループの未割り当て領域、またはベーシック ディスクの未割り当て領域)に復元できます。ダイナミック ボリュームの復元の詳細については、「Microsoft LDM(ダイナミック ボリューム)『ページ参照 49』」をご参照ください。

Acronis Backup & Recovery 10 エージェント for Windows には、**VMware Workstation、Microsoft Virtual PC、Parallels Workstation、または Citrix XenServer Virtual Appliance のいずれかの種類の新しい仮想コンピュータ**にディスク(ボリューム)のバックアップを復元する機能があります。次に、仮想アプライアンスを XenServer にインポートできます。VMware Workstation コンピュータは、VMware OVF ツールを使用して OVF(Open Virtualization Format)に変換できます。Acronis Backup & Recovery 10 エージェント for Hyper-V(またはエージェント for ESX/ESXi)を使用すると、新しい仮想コンピュータをそれぞれの仮想サーバー上に作成できます。

復元する前にターゲット ディスクの準備が必要になる場合があります。Acronis Backup & Recovery 10 には、ターゲット ハードウェア(オペレーティング システムおよびベア メタル状態のディスクの両方)において、ボリュームの作成または削除、ディスク パーティション形式の変換、ディスク グループの作成、およびその他のディスク管理操作を実行できるようにするための便利なディスク管理ユーティリティが用意されています。Acronis Disk Director LV の詳細については、「ディスクの管理『ページ参照 316』」をご参照ください。

復元タスクを作成する手順は、次のとおりです。

[全般]

[タスク名]

(オプション)復元タスクの一意の名前を入力します。わかりやすい名前にすると、容易に他のタスクと区別することができます。

[タスクのログイン情報]『ページ参照 260』

(オプション)タスクは、タスクを作成したユーザーの代わりに実行されます。タスク アカウントのログイン情報は、必要に応じて変更することができます。このオプションにアクセスするには、**[詳細ビュー]**チェックボックスをオンにします。

[復元元]

[アーカイブ]『ページ参照 260』

データの復元元のアーカイブを選択します。

[データの種類]『ページ参照 261』

対象:ディスクの復元

選択したディスク バックアップからの復元を必要とするデータの種類を選択します。

[コンテンツ]『ページ参照 261』

復元するバックアップおよびその内容を選択します。

[アクセス ログイン情報]『ページ参照 263』

(オプション)タスク アカウントがアーカイブの保存先に対するアクセス権限を持っていない場合は、アーカイブの保存先のログイン情報を指定します。このオプションにアクセスするには、**[詳細ビュー]**チェックボックスをオンにします。

[復元先]

このセクションは、必要なバックアップが選択され、復元するデータの種類が定義された後に表示されます。ここで指定するパラメータは、復元するデータの種類によって異なります。

[ディスク]『ページ参照 263』

[ボリューム]『ページ参照 265』

[Acronis Active Restore]

(オプション)Windows 2000 から Windows を復元する場合は、**[Acronis Active Restore]**チェックボックスを使用できます。Acronis Active Restore は、復元の開始直後にシステムをオンラインにします。オペレーティング システムはバックアップ イメージから起動して、コンピュータが使用可能になり、必要なサービスを提供できるようになります。要求された処理に必要なデータが最高の優先度で復元され、それ以外のすべてのデータはバックグラウンドで復元されます。

詳細については、「Acronis Active Restore『ページ参照 63』」をご参照ください。

［ファイル］『ページ参照 270』

復元先のログイン情報を指定する必要がある場合があります。ブータブル メディアを使用して起動されたコンピュータで実行する場合は、この手順をスキップします。

［アクセス ログイン情報］『ページ参照 272』

(オプション)タスクのログイン情報によって選択したデータの復元が有効にならない場合は、復元先のログイン情報を指定します。このオプションにアクセスするには、**［詳細ビュー］**チェックボックスをオンにします。

［復元の実行時期］

［復元］『ページ参照 272』

復元を開始する時期を選択します。タスクは、作成直後に開始するか、後で指定した日時に実行するようにスケジュールするか、または手動で実行するために保存することもできます。

(オプション)Acronis Universal Restore

対象: Windows OS およびシステム ボリュームの復元

［Universal Restore］『ページ参照 272』

異なるハードウェアで復元して Windows を起動する必要がある場合は、Acronis Universal Restore を使用します。

［自動ドライバ検索］

HAL、大容量記憶装置、およびネットワーク アダプタのドライバを検索する場所を指定します。Acronis Universal Restore は、ターゲット ハードウェアに適しているドライバをインストールします。

［インストールする大容量記憶装置ドライバ］

(オプション)自動ドライバ検索によって適切なドライバが見つからない場合は、手動で大容量記憶装置のドライバを指定します。このオプションにアクセスするには、**［詳細ビュー］**チェックボックスをオンにします。

［復元オプション］

［設定］

(オプション)復元処理は、復元の前後に実行するコマンド、復元の優先度、エラーの処理、通知オプションなどの復元オプションを構成することでカスタマイズできます。このセクションで何も指定しない場合は、デフォルト値『ページ参照 141』が使用されます。

いずれかの設定をデフォルト値から変更すると、新しい行に新しく設定した値が表示されます。設定のステータスが**［デフォルト］**から**［カスタム］**に変更されます。設定を再度変更すると、新しい値がデフォルト値ではない場合に行が表示されます。デフォルト値が設定されると、行が非表示になるので、**［設定］**セクションには、常にデフォルト値と異なる設定のみが表示されます。

［デフォルトにリセット］をクリックすると、すべての値がデフォルト値にリセットされます。

必要なすべての手順を完了したら、［**OK**］をクリックして復元タスクの作成をコミットします。

6.3.1. タスクのログイン情報

タスクを実行するアカウントのログイン情報を指定します。

ログイン情報を指定する手順は、次のとおりです。

1. 次のいずれかを選択します。
   - **現在のログイン情報を使用する**

     タスクは、タスクを起動するユーザーがログインしたときのログイン情報を使用して実行されます。スケジュールを設定してタスクを実行する場合は、タスクの作成を完了する際に現在のユーザーのパスワードを入力するよう求められます。
   - **次のログイン情報を使用する**

     タスクは、手動で開始されるか、スケジュールに従って実行されるかにかかわらず、常にユーザーが指定するログイン情報を使用して実行されます。

     次の項目を指定します。
     - ［**ユーザー名**］- Active Directory ユーザー アカウントの名前を入力する場合は、ドメイン名(DOMAIN¥ユーザー名またはユーザー名@ドメイン)も指定してください。
     - ［**パスワード**］- アカウントのパスワード。
2. ［**OK**］をクリックします。

Acronis Backup & Recovery 10 のログイン情報の詳細については、「所有者とログイン情報『ページ参照 35』」をご参照ください。

ユーザー権限に応じて使用可能になる操作の詳細については、「管理対象のコンピュータ上のユーザー権限『ページ参照 34』」をご参照ください。

6.3.2. アーカイブの選択

アーカイブの選択

1. 場所のフル パスを［**パス**］フィールドに入力するか、**フォルダ ツリー**から目的のフォルダを選択します。
   - アーカイブが集中管理用格納域に保存されている場合、［**集中管理**］グループを展開し、格納域をクリックします。
   - アーカイブが個人用格納域に保存されている場合、［**個人用**］グループを展開し、格納域をクリックします。
   - アーカイブがコンピュータ上のローカル フォルダに保存されている場合、［**ローカル フォルダ**］グループを展開し、目的のフォルダをクリックします。

   複数枚の DVD などのリムーバブル メディアにアーカイブがある場合は、まず最後に作成した DVD を挿入し、以降はメッセージに従って 1 枚目のディスクから順に挿入してください。
   - アーカイブがネットワーク共有に保存されている場合、［**ネットワーク フォルダ**］グループを展開し、ネットワーク上の必要なコンピュータを選択して、共有フォルダをクリックします。ネットワーク共有がアクセス ログイン情報を必要とする場合は、それらの情報が要求されます。

***Linux ユーザー向けの注意: /mnt/share** などのマウント ポイントにマウントされている CIFS(Common Internet File System)のネットワーク共有を指定するには、ネットワーク共有そのものではなく、このマウント ポイントを選択します。*

- アーカイブが **FTP** サーバーまたは **SFTP** サーバーに保存されている場合、［**パス**］フィールドにサーバーの名前またはアドレスを次のように入力します。

  ftp://ftp_server:port _number または **sftp://sftp_server:port number**

  ポート番号が指定されていない場合、ポート 21 が FTP 用に、ポート 22 が SFTP 用に使用されます。

  アクセス ログイン情報を入力すると、サーバー上のフォルダが使用できるようになります。サーバー上の適切なフォルダをクリックします。

  匿名アクセスがサーバーによって許可されている場合、匿名ユーザーとしてサーバーにアクセスすることができます。匿名ユーザーとしてアクセスするには、ログイン情報を入力する代わりに、［**匿名アクセスを使用する**］をクリックします。

FTP 仕様の原文に記載されているように、FTP サーバーにアクセスするのに必要なログイン情報は、ネットワーク上をテキスト形式で転送されます。このことは、ユーザー名とパスワードが、パケット スニファを使用した盗聴者によって傍受される可能性があることを意味します。

- ローカル接続したテープ デバイスにアーカイブが保存されている場合、［**テープ ドライブ**］グループを展開し、目的のデバイスをクリックします。

2. ツリーの右側にある表からアーカイブを選択します。この表には、選択した格納域またはフォルダに含まれているアーカイブの名前が表示されます。

   アーカイブの保存場所の内容を確認しているとき、別のユーザーまたはスケジュール設定された処理によって、アーカイブが追加、削除、または変更されることがあります。［**更新**］を使用すれば、アーカイブの一覧を更新できます。

   ［**アーカイブの表示**］と［**TIB ファイルの表示**］を使用すると、名前によってアーカイブを表示するか、アーカイブを TIB ファイルとして物理的に表示するかを切り替えることができます。

3. ［**OK**］をクリックします。

6.3.3. データの種類

選択したディスク バックアップから復元するデータの種類を選択します。

- ［**ディスク**］- ディスクを復元します。
- ［**ボリューム**］- ボリュームを復元します。
- ［**ファイル**］- 特定のファイルとフォルダを復元します。

6.3.4. 復元対象の選択

このウィンドウに表示される内容は、アーカイブに保存されているデータの種類によって異なります。

6.3.4.1. ディスク/ボリュームの選択

復元するバックアップおよびディスク/ボリュームを選択する手順は、次のとおりです。

1. 作成日時によって、連続している増分バックアップの 1 つを選択します。このようにして、ディスクのデータの状態を特定の時点に戻すことができます。

   復元する項目を指定します。デフォルトでは、選択したバックアップのすべての項目が選択されます。特定の項目を復元しない場合は、その項目をオフにします。ディスク/ボリュームに関する情報を取得するには、右クリックしてから［**情報**］をクリックします。

2. ［**OK**］をクリックします。

MBR の選択

一般的に、次のような場合はディスクの MBR を選択します。

- オペレーティング システムを起動できない
- ディスクが新しいため、MBR が存在しない
- カスタムまたは Windows 以外のブート ローダーを復元する(LILO、GRUB など)
- ディスクのジオメトリがバックアップに保存されているジオメトリと異なる

MBR の復元が必要になる状況は他にもありますが、上記のような状況が最も一般的です。

MBR をディスク間で復元する場合、Acronis Backup & Recovery 10 はトラック 0 を復元しますが、このことによりターゲット ディスクのパーティション テーブルとパーティション レイアウトが影響を受けることはありません。Acronis Backup & Recovery 10 は、復元後に Windows ローダーを自動的に更新するため、MBR が破損していない場合は、Windows システムで MBR とトラック 0 を復元する必要はありません。

6.3.4.2. ファイルの選択

復元するバックアップおよびファイルを選択する手順は、次のとおりです。

1. 作成日時によって、連続している増分バックアップの 1 つを選択します。ファイル/フォルダを特定の時点に戻すことができます。
2. アーカイブ ツリーで対応するチェックボックスをオンにすることによって、復元するファイルとフォルダを指定します。

   フォルダを選択すると、入れ子になっているすべてのフォルダとファイルが自動的に選択されます。

   アーカイブ ツリーの右にあるテーブルを使用して、入れ子になっている項目を選択します。［**名前**］列の見出しのチェックボックスをオンにすると、テーブル内のすべての項目が自動的に選択されます。このチェックボックスをオフにすると、すべての項目が自動的に選択解除されます。
3. ［**OK**］をクリックします。

6.3.5. 場所のアクセス ログイン情報

バックアップ アーカイブの保存先にアクセスするために必要なログイン情報を指定します。

ログイン情報を指定する手順は、次のとおりです。

1. 次のいずれかを選択します。
   - **［タスクのログイン情報を使用する］**

     ［全般］セクションで指定されたタスク アカウントのログイン情報を使用して、その場所にアクセスします。
   - **［次のログイン情報を使用する］**

     ユーザーが指定するログイン情報を使用して、その場所にアクセスします。タスク アカウントがその場所に対するアクセス許可を持っていない場合は、このオプションを使用します。ネットワーク共有またはストレージ ノードの格納域に対しては、特別なログイン情報を指定する必要がある場合があります。

     次の項目を指定します。
     - **［ユーザー名］**- Active Directory ユーザー アカウントの名前を入力する場合は、ドメイン名(DOMAIN¥ユーザー名またはユーザー名@ドメイン)も指定してください。
     - **［パスワード］**- アカウントのパスワード。
2. **［OK］**をクリックします。

FTP 仕様の原文に記載されているように、FTP サーバーにアクセスするのに必要なログイン情報は、ネットワーク上をテキスト形式で転送されます。このことは、ユーザー名とパスワードが、パケット スニファを使用した盗聴者によって傍受される可能性があることを意味します。

6.3.6. 復元先の選択

選択したデータを復元する復元先を指定します。

6.3.6.1. ディスク

使用できるディスクの復元先は、コンピュータで動作しているエージェントによって異なります。

復元先:

物理コンピュータ

Acronis Backup & Recovery 10 エージェント for Windows(またはエージェント for Linux)がインストールされている場合に使用できます。

選択したディスクは、コンソールが接続されているコンピュータの物理ディスクに復元されます。これを選択した場合は、次に示す通常のディスク マッピングの手順に進みます。

新しい仮想コンピュータ『ページ参照 268』

Acronis Backup & Recovery 10 エージェント for Windows がインストールされている場合

選択したディスクは、VMware Workstation、Microsoft Virtual PC、Parallels Workstation、または Citrix XenServer Virtual Appliance のいずれかの種類の新しい仮想コンピュータに復元されます。**仮想コンピュータのファイルは、指定した復元先に保存されます。**

Acronis Backup & Recovery 10 エージェント for Hyper-V(またはエージェント for ESX/ESXi)がインストールされている場合

これらのエージェントによって、指定した仮想サーバー上に新しい仮想コンピュータを作成できます。

新しい仮想コンピュータは自動的に構成され、ソース コンピュータの構成が可能な範囲でコピーされます。構成内容は、**［仮想コンピュータの設定］**『ページ参照 269』セクションに表示されます。設定を確認し、必要に応じて変更します。

その後、次に示す通常のディスク マッピングの手順に進みます。

既存の仮想コンピュータ

Acronis Backup & Recovery 10 エージェント for Hyper-V(またはエージェント for ESX/ESXi)がインストールされている場合に使用できます。

これを選択した場合は、仮想サーバーとターゲット仮想コンピュータを指定します。その後、次に示す通常のディスク マッピングの手順に進みます。

復元先のコンピュータは、復元前に電源が自動的にオフになることに注意してください。手動で電源をオフにする場合は、VM 電源管理オプションを変更します。

ディスク番号:

［ディスク番号(モデル)］『ページ参照 267』

各ソース ディスクに対して、復元先ディスクを選択します。

［NT シグネチャ］『ページ参照 265』

復元するディスクのシグネチャの処理方法を選択します。ディスクのシグネチャは、Windows および Linux カーネル バージョン 2.6 以降によって使用されます。

復元先ディスク

復元先のディスクを指定する手順は、次のとおりです。

1. 選択したディスクの復元先となるディスクを選択します。復元先のディスク領域には、少なくとも圧縮されていないイメージ データと同じサイズが必要です。
2. **［OK］**をクリックします。

復元先のディスクに保存されているすべてのデータは、バックアップ データで置き換えられるため、復元先に存在するバックアップされていない必要なデータに注意してください。

NT シグネチャ

ディスク バックアップと共に MBR を選択する場合、ターゲット ディスク ボリュームでもオペレーティング システムが起動できるように保つ必要があります。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 シグネ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 シグネチャを持つと正しく機能できません。

コンピュータにシステム 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 シグネチャが生成され、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、そのディスクに対するパスはすべて無効となり、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を起動できるように保つには、次のいずれかを選択します。

- **[新規作成]**
  ターゲット ハード ディスク ドライブに対して、新しい NT シグネチャが生成されます。
- **[バックアップから復元]**
  ターゲット ハード ディスクの NT シグネチャは、ディスク バックアップにあるシグネチャで置き換えられます。
  次のような理由により、ディスクのシグネチャの復元が必要になります。
  - Acronis Backup & Recovery 10 は、ソース ハード ディスクのシグネチャを使用してタスク スケジュールを作成します。同じディスク シグネチャを復元する場合は、前に作成されたタスクを再作成または編集する必要はありません。
  - 一部のインストール済みのアプリケーションは、ライセンス管理およびその他の目的のためにディスク シグネチャを使用します。
  - 復元されるディスク上のすべての Windows 復元ポイントを保持できるようにします。
  - Windows Vista の「以前のバージョン」の機能が使用する VSS スナップショットを復元します。
- **[既存のものを保持]**
  ターゲット ハード ディスクの既存の NT シグネチャがそのまま残ります。

6.3.6.2. ボリューム

使用できるボリュームの復元先は、コンピュータで動作しているエージェントによって異なります。

復元先:

物理コンピュータ

Acronis Backup & Recovery 10 エージェント for Windows(またはエージェント for Linux)がインストールされている場合に使用できます。

選択したボリュームは、コンソールが接続されているコンピュータの物理ディスクに復元されます。これを選択した場合は、次に示す通常のボリューム マッピングの手順に進みます。

新しい仮想コンピュータ『ページ参照 268』

Acronis Backup & Recovery 10 エージェント for Windows がインストールされている場合

選択したボリュームは、VMware Workstation、Microsoft Virtual PC、Parallels Workstation、または Citrix XenServer Virtual Appliance のいずれかの種類の新しい仮想コンピュータに復元されます。**仮想コンピュータのファイルは、指定した復元先に保存されます。**

Acronis Backup & Recovery 10 エージェント for Hyper-V(またはエージェント for ESX/ESXi)がインストールされている場合

これらのエージェントによって、指定した仮想サーバー上に新しい仮想コンピュータを作成できます。

新しい仮想コンピュータは自動的に構成され、ソース コンピュータの構成が可能な範囲でコピーされます。構成内容は、**[仮想コンピュータの設定]**『ページ参照 269』セクションに表示されます。設定を確認し、必要に応じて変更します。

その後、次に示す通常のボリューム マッピングの手順に進みます。

既存の仮想コンピュータ

Acronis Backup & Recovery 10 エージェント for Hyper-V(またはエージェント for ESX/ESXi)がインストールされている場合に使用できます。

これを選択した場合は、仮想サーバーとターゲット仮想コンピュータを指定します。その後、次に示す通常のボリューム マッピングの手順に進みます。

復元先のコンピュータは、復元前に電源が自動的にオフになることに注意してください。手動で電源をオフにする場合は、VM 電源管理オプションを変更します。

[ボリューム] [ドライブ文字]:

[ディスク番号/ボリューム]『ページ参照 267』

それぞれのソース ボリュームを復元先ディスクのボリュームまたは未割り当て領域に連続してマップします。

[サイズ]『ページ参照 267』

(オプション)復元するボリュームのサイズ、場所、およびその他のプロパティを変更します。

ボリュームの復元先

復元先のボリュームを指定する手順は、次のとおりです。

1. 選択したボリュームを復元するボリュームまたは未割り当て領域を選択します。復元先のボリューム/未割り当て領域には、少なくとも圧縮されていないイメージ データと同じサイズが必要です。
2. [OK] をクリックします。

復元先のボリュームに保存されているすべてのデータは、バックアップ データで置き換えられるため、復元先に存在するバックアップされていない必要なデータに注意してください。

ブータブル メディアを使用する場合

Windows スタイルのブータブル メディアで表示されるディスクのドライブ文字が Windows で識別されるドライブと異なることがあります。たとえば、レスキュー ユーティリティでの 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。

ご注意ください。安全のために、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。

Linux スタイルのブータブル メディアでは、ローカル ディスクとボリュームがマウントされていない状態(sda1、sda2...)で表示されます。

ボリュームのプロパティ

サイズと位置の変更

ボリュームをベーシック MBR ディスクに復元する場合は、ボリュームまたはボリュームの境界をマウスでドラッグするか、該当するフィールドに対応する値を入力すると、ボリュームのサイズや位置を変更できます。この機能を使用すると、復元されるボリューム間でハードディスク領域を再配分することができます。この場合、縮小するボリュームを最初に復元する必要があります。

プロパティ

[種類]

ベーシック MBR ディスクには、最大 4 つまでのプライマリ ボリュームまたは最大 3 つまでのプライマリ ボリュームと複数の論理ドライブを含めることができます。デフォルトでは、元のボリュームの種類が選択されます。この設定は、必要に応じて変更できます。

- **[プライマリ]** - プライマリ ボリュームに関する情報は、MBR パーティション テーブルに含まれています。ほとんどのオペレーティング システムは、最初のハード ディスクのプライマリ ボリュームからのみ起動が可能ですが、プライマリ ボリュームの数には制限があります。

  ベーシック MBR ディスクにシステム ボリュームを復元する場合は、[アクティブ] チェックボックスをオンにします。アクティブなボリュームは、オペレーティング システムの読み込みに使用されます。オペレーティング システムがインストールされていないボリュームに対して [アクティブ] を選択すると、コンピュータが起動できなります。論理ドライブまたはダイナミック ボリュームをアクティブに設定することはできません。

- ［**論理**］- 論理ボリュームに関する情報は、MBR ではなく拡張パーティション テーブルにあります。単一のディスク上の論理ボリュームの数に制限はありません。論理ボリュームをアクティブに設定することはできません。独自のボリュームとオペレーティング システムを含むシステム ボリュームを別のハード ディスクに復元する場合は、一般にデータのみが必要になります。この場合は、ボリュームを論理ボリュームとして復元することで、データのみにアクセスします。

ファイル システム

必要に応じて、ボリュームのファイル システムを変更します。デフォルトでは、元のボリュームのファイル システムが選択されます。Acronis Backup & Recovery 10 では、次のようにファイル システムを変換できます。FAT 16 → FAT 32 および Ext2 → Ext3。その他の形式をベースにしたファイル システムを使用するボリュームに対しては、このオプションは使用できません。

古い、容量の少ない FAT16 ディスクから新しいディスクにボリュームを復元するとします。大容量のハード ディスクでは、FAT16 は効率的ではなく、設定できない場合もあります。これは、FAT16 が最大 4GB までのボリュームしかサポートしておらず、ファイル システムを変更することなく、FAT16 ボリュームに対するこの 4GB の制限を超えるボリュームに復元することはできないためです。そこで、FAT16 から FAT32 にファイル システムを変更することが意味を持ちます。

古いオペレーティング システム(MS-DOS、Windows 95、Windows NT 3.x、4.x)は FAT32 をサポートしないため、ボリュームを復元した後にファイル システムを変更しても動作しません。これらは、一般に FAT16 ボリュームのみに復元できます。

論理ドライブ文字(Windows のみ)

復元したボリュームにドライブ文字を割り当てます。ドロップダウン リストから目的のドライブ文字を選択します。

- デフォルトの自動選択では、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。
- ［いいえ］を選択すると、復元されたボリュームにはドライブ文字が割り当てられず、OS に対して非表示になります。FAT および NTFS 以外で Windows からアクセスできないボリュームには、ドライブ文字を割り当てないでください。

6.3.6.3. 仮想コンピュータの種類/仮想サーバーの選択

新しい仮想コンピュータは、仮想サーバー(これには、Acronis Backup & Recovery 10 エージェント for Hyper-V(またはエージェント for ESX/ESXi)をインストールする必要があります)またはローカル フォルダやネットワーク接続を介してアクセスできるフォルダ上に作成できます。

新しい仮想コンピュータを作成する仮想サーバーを選択する手順は、次のとおりです。

1. ［**選択した仮想サーバー上に配置する**］オプションを選択します。
2. ウィンドウの左側で、仮想サーバーを選択します。ウィンドウの右側の部分を使用して、選択したサーバーの詳細を確認します。
3. ［**OK**］をクリックして、［**データの復元**］ページに戻ります。

仮想コンピュータの種類を選択する手順は、次のとおりです。

1. **［選択した種類の VM のファイルとして、指定したフォルダに保存する］**オプションを選択します。
2. ウィンドウの左側で、仮想コンピュータの種類を選択します。ウィンドウの右側の部分を使用して、選択した仮想コンピュータの種類の詳細を確認します。
3. **［OK］**をクリックして、**［データの復元］**ページに戻ります。

6.3.6.4. 仮想コンピュータの設定

次の仮想コンピュータの設定を構成できます。

［ストレージ］

初期設定: 仮想サーバーで新しいコンピュータが作成された場合の仮想サーバーのデフォルトストレージです。それ以外の場合は、現在のユーザーのドキュメント フォルダです。

これは、新しい仮想コンピュータを作成する場所です。仮想サーバー上のストレージを変更できるかどうかは、仮想化製品の製造元と設定によって異なります。VMware ESX では、複数のストレージを使用できます。Microsoft Hyper-V サーバーでは、任意のローカル フォルダに新しい仮想コンピュータを作成できます。

［メモリ］

初期設定: バックアップに含まれない場合、仮想サーバーのデフォルト設定になります。

これは、新しい仮想コンピュータに割り当てられたメモリ容量です。メモリの調整範囲は、ホストのハードウェア、ホストのオペレーティング システム、および仮想化製品の設定によって異なります。たとえば、仮想コンピュータはメモリの 30% まで使用できます。

［ディスク］

初期設定: ソース コンピュータのディスクの数とサイズです。

ディスクの数は、一般にソース コンピュータのディスクの数と同じですが、仮想化製品で設定されている制限により、プログラムがソース コンピュータのボリュームを確保するために、さらにディスクを追加する必要がある場合があります。コンピュータの構成に仮想ディスクを追加するか、場合によっては、指定されたディスクを削除できます。

［プロセッサ］

初期設定: バックアップに含まれない場合、または仮想サーバーでバックアップの設定がサポートされていない場合、デフォルトのサーバーの設定が使用されます。

これは、新しい仮想コンピュータのプロセッサの数です。ほとんどの場合、これは 1 に設定されます。コンピュータに複数のプロセッサを割り当てた場合の結果は保証されません。仮想プロセッサの数は、ホストの CPU の構成、仮想化製品、およびゲスト オペレーティング システムによって制限される場合があります。複数の仮想のプロセッサは、一般にマルチプロセッサ ホストで使用できます。マルチコア ホストの CPU またはハイパースレッドでは、単一プロセッサ ホスト上で複数の仮想プロセッサを使用できる場合があります。

6.3.6.5. ファイルの復元先

復元先を指定する手順は、次のとおりです。

1. バックアップ ファイルを復元する場所を選択します。
   - **［元のロケーション］**- ファイルとフォルダは、バックアップ内と同じパスに復元されます。たとえば、C:¥Documents¥Finance¥Reports¥ にあるすべてのファイルとフォルダをバックアップした場合、ファイルは同じパスに復元されます。フォルダが存在しない場合は、自動的に作成されます。
   - **［新しい場所］**- ファイルは、ツリー内で指定した場所に復元されます。**［フルパスを復元しない］**チェックボックスをオフにしない場合、ファイルとフォルダはフルパスを再作成せずに復元されます。
2. **［OK］**をクリックします。

除外

復元中に上書きされないように除外するファイルの種類を設定します。

除外するファイルおよびフォルダを指定する手順は、次のとおりです。

次のいずれかのパラメータを設定します。

- **すべての隠しファイルおよびフォルダを除外**

  隠しファイル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。

- **すべてのシステム ファイルおよびフォルダを除外**

  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設定されてい場合、フォルダの内容はシステム属性を設定されていないファイルを含みすべて除外されます。

***attrib** コマンドを使用してファイルまたはフォルダのファイル/フォルダ プロパティ内の属性を表示することができます。詳細については、Windows の［ヘルプとサポート］をご参照ください。*

- **次の条件に一致するファイルを除外**

  一覧内のいずれかの条件(ファイル マスクと呼ばれます)に一致するファイル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。ファイル マスクの一覧を作成するには、**［追加］**、**［編集］**、**［削除］**、および**［すべて削除］**ボタンを使用します。

  1 つ以上のワイルドカード文字(* および ?)をファイル マスク内で使用することができます。

  アスタリスク(*)はファイル名内の 0 個以上の文字の代用として使用します。たとえば、ファイル マスク Doc*.txt は Doc.txt、Document.txt などの文字と一致します。

  疑問符(?)はファイル名内の厳密に 1 文字の代用として使用します。たとえば、ファイルマスク Doc?.txt は Doc1.txt、Docs.txt などのファイルと一致しますが、Doc.txt、Doc11.txt などのファイルとは一致しません。

除外の例

条件	例	説明
名前	File1.log	File1.log という名前のすべてのファイルを除外します。
パス	C:¥Finance¥test.log	C:¥Finance フォルダに置かれている test.log という名前のファイルを除外します。
マスク(*)	*.log	.log 拡張子の付いたすべてのファイルを除外します。
マスク(?)	my???.log	5 文字で最初が「my」で始まる名前のすべての .log ファイルを除外します。

上記の設定は、明示的に復元対象として選択されたファイルまたはフォルダには適用されません。たとえば、MyFolder というフォルダとこのフォルダの外部にある MyFile.tmp というファイルをバックアップ対象に選択して、すべての .tmp ファイルをスキップするように選択したとします。この場合、復元処理中に MyFolder フォルダ内のすべての .tmp ファイルはスキップされますが、MyFile.tmp ファイルはスキップされません。

上書き

このオプションは、復元先フォルダに、バックアップ アーカイブにあるファイルと同じファイル名が見つかった場合の処理を選択します。

- **[既存のファイルを上書きする]** - バックアップにあるファイルをハード ディスクのファイルより優先します。
- **[既存のファイルが古い場合に上書きする]** - 最新のファイル修正をバックアップまたはディスクにかかわらず優先します。
- **[既存のファイルを上書きしない]** - ハード ディスク上のファイルをバックアップにあるファイルより優先します。

ファイルの上書きを許可した場合でも、次のファイルの上書きを防止する『ページ参照 270』ことができます。

- 隠しファイルとフォルダ
- システム ファイルとフォルダ
- 名前またはワイルドカードを使用して指定するすべてのファイル
- パスによって指定するすべてのフォルダ

6.3.7. 復元先のアクセス ログイン情報

ログイン情報を指定する手順は、次のとおりです。

1. 次のいずれかを選択します。
   - **［タスクのログイン情報を使用する］**
     ［全般］セクションで指定されたタスク アカウントのログイン情報を使用して、復元先にアクセスします。
   - **［次のログイン情報を使用する］**
     ユーザーが指定するログイン情報を使用して、復元先にアクセスします。タスク アカウントがその復元先に対するアクセス許可を持っていない場合は、このオプションを使用します。
     次の項目を指定します。
     - **［ユーザー名］**- Active Directory ユーザー アカウントの名前を入力する場合は、ドメイン名(DOMAIN¥ユーザー名またはユーザー名@ドメイン)も指定してください。
     - **［パスワード］**- アカウントのパスワード。
2. **［OK］**をクリックします。

6.3.8. ［復元の実行時期］

復元タスクを開始する時期を選択します。

- **［今すぐ］**- 最後の**［OK］**をクリックすると、直ちに復元タスクが開始されます。
- **［後で］**- 復元タスクは、指定した日時に開始されます。

タスクをスケジュールする必要がなく、後で手動で起動する場合は、**［このタスクは手動で開始されます(このタスクはスケジュールしないでください)。］**チェックボックスをオンにします。

6.3.9. ［Universal Restore］

異なるハードウェアで復元して Windows を起動する必要がある場合は、Acronis Backup & Recovery 10 Universal Restore を使用します。Universal Restore は、ストレージ コントローラ、マザーボード、チップセットなどのオペレーティング システムの起動にとって重要なデバイスの相違に対応できます。

Universal Restore テクノロジの詳細については、「Universal Restore『ページ参照 61』」をご参照ください。

Acronis Backup & Recovery 10 Universal Restore は、次の場合には使用できません。

- コンピュータが Acronis リカバリ マネージャ(［F11］キーを使用)によって起動された場合
- バックアップ イメージが Acronis セキュア ゾーンにある場合
- Acronis Active Restore『ページ参照 413』 を使用するよう選択した場合

これは、これらの機能が主に同じコンピュータ上での簡単なデータ復元を目的としているためです。

準備

Windows を異なるハードウェアに復元する前に、新しい HDD コントローラとチップセット用のドライバがあることを確認します。これらのドライバは、オペレーティング システムの起動に不可欠です。ハードウェア ベンダが提供する CD または DVD を使用するか、またはベンダの Web 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、*.sys、または *.oem です。*.exe、*.cab、または *.zip 形式でドライバをダウンロードした場合は、WinRAR(http://www.rarlab.com/)または Universal Extractor(http://legroom.net/software/uniextract)などのサードパーティ製アプリケーションを使用して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)を使用して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。

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、［**フォルダの検索**］フィールドにフォルダのパスを指定します。

復元中に、Universal Restore は指定されたフォルダのすべてのサブフォルダを再帰的に検索し、すべての利用可能な 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、復元するシステムにインストールします。Universal Restore は、ネットワーク アダプタのドライバも検索し、見つかったドライバのパスが Universal Restore によってオペレーティング システムに伝達されます。ハードウェアに複数のネットワーク インターフェイス カードがある場合、Universal Restore はすべてのカードのドライバの構成を試みます。指定された場所に互換性のあるドライバが見つからない場合、Universal Restore は問題のあるデバイスを特定し、ドライバのディスクまたはネットワーク パスを要求します。

Windows が起動すると、新しいハードウェアをインストールするための標準の手順が開始されます。ドライバに Microsoft Windows のシグネチャがある場合、ネットワーク アダプタ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。

［インストールする大容量記憶装置ドライバ］

このオプションにアクセスするには、**［詳細ビュー］**チェックボックスをオンにします。

ターゲット ハードウェアに RAID(特に NVIDIA RAID)、ファイバ チャネル アダプタなどの大容量記憶コントローラがある場合、**［ドライバ］**フィールドで適切なドライバを指定します。

ここで定義されたドライバが優先されます。さらに適切なドライバが見つかった場合でも、警告を表示してこのドライバがインストールされます。

このオプションは、自動ドライバ検索によってシステムを起動できなかった場合にのみ使用してください。

仮想コンピュータのドライバ

システムを新しい仮想コンピュータに復元する場合は、サポートされている仮想コンピュータに必要なドライバは明らかであるため、Universal Restore テクノロジはバックグラウンドで適用されます。

システムを SCSI ハード ディスク ドライブのコントローラを使用する既存の仮想コンピュータに復元する場合は、**［インストールする大容量記憶装置ドライバ］**の手順で仮想環境用の SCSI ドライバを指定する必要があります。仮想コンピュータのソフトウェアに同梱されている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の開発元の Web サイトからダウンロードしてください。

6.3.10. ディスク バックアップを仮想コンピュータに変換する方法

TIB ファイルを仮想ディスク ファイルに変換すると、追加の操作によって仮想ディスクを使用可能にする必要があるため、Acronis Backup & Recovery 10 は、ディスク バックアップを、設定済みで使用可能な新しい仮想コンピュータに復元する方法で変換を実行します。復元処理を構成するときに、ユーザーのニーズを満たすように仮想コンピュータの構成を調整できます。

Acronis Backup & Recovery 10 エージェント for Windows を使用すると、**VMware Workstation、Microsoft Virtual PC、Parallels Workstation、または Citrix XenServer Virtual Appliance のいずれかの種類の新しい仮想コンピュータにディスク(ボリューム)のバックアップを復元することができます。**

新しい仮想コンピュータのファイルは、選択したフォルダに保存されます。それぞれの仮想ソフトウェアを使用してコンピュータを起動するか、他の用途のためにコンピュータのファイルを準備することができます。Citrix XenServer Virtual Appliance は、Citrix XenCenter を使用して XenServer にインポートできます。VMware Workstation コンピュータは、VMware OVF ツールを使用して OVF(Open Virtualization Format)に変換できます。

Acronis Backup & Recovery 10 エージェント for Hyper-V または**エージェント for ESX/ESXi** を使用すると、ディスク(ボリューム)バックアップを**それぞれの仮想サーバー上の新しい仮想コンピュータに復元できます。**

ディスク バックアップを仮想コンピュータに変換する手順は、次のとおりです。

1. エージェント for Windows、エージェント for Hyper-V、またはエージェント for ESX/ESXi がインストールされているコンピュータにコンソールを接続します。
2. 次のいずれかを実行します。
   - ［**復元**］をクリックして、［**データの復元**］ページを開きます。「データの復元『ページ参照 257』」の説明に従って、復元タスクの作成を開始します。アーカイブを選択し、変換するディスク バックアップまたはボリューム バックアップを選択します。
   - ［**ナビゲーション**］ペインを使用して、アーカイブが保存されている格納域に移動します。アーカイブを選択し、変換するディスク バックアップまたはボリューム バックアップを選択します。［**仮想コンピュータとして復元**］をクリックします。［**データの復元**］ページが開き、あらかじめ選択されているバックアップが表示されます。
3. ［**データの種類**］で、変換対象に応じて［**ディスク**］または［**ボリューム**］を選択します。
4. ［**コンテンツ**］で、変換するディスクを選択するか、該当するディスクのマスタ ブート レコード(MBR)を含むボリュームを選択します。
5. ［**復元先**］で、［**新しい仮想コンピュータ**］を選択します。
6. ［**VM サーバー**］で、作成する新しい仮想コンピュータの種類、*つまり*仮想コンピュータを作成する仮想サーバーを選択します。
7. ［**VM 名**］に、新しい仮想コンピュータの名前を入力します。
8. (オプション)［**仮想コンピュータの設定**］**『ページ参照 269』を確認し、必要に応じて設定を変更します。ここで、新しい仮想コンピュータのパスを変更できます。**

   同じフォルダ内に、同じ種類のコンピュータを同じ名前で作成することはできません。同じ名前が原因でエラー メッセージが表示される場合は、VM 名またはパスを変更してください。

9. 各ソース ディスクまたは各ソース ボリュームと MBR に対して、復元先ディスクを選択します。

   Microsoft Virtual PC では、オペレーティング システムのローダーが存在するハード ディスク 1 上のディスクまたはボリュームに復元するようにしてください。そうしないと、オペレーティング システムが起動しなくなります。Virtual PC は BIOS 内の起動デバイスの順序に関する設定を無視するため、BIOS で起動デバイスの順序を変更してもこの問題を解決することはできません。

10. ［**復元の実行時期**］で、復元タスクを開始する時期を指定します。
11. (オプション)［**復元オプション**］を確認し、必要に応じてデフォルト値から設定を変更します。［**復元オプション**］→［**VM 電源管理**］を選択して、新しい仮想コンピュータを自動的に起動するか、または復元が完了した後で起動するかを指定できます。このオプションは、仮想サーバー上に新しいコンピュータを作成した場合にのみ使用できます。
12. ［**OK**］をクリックします。将来の復元タスクをスケジュールするときは、タスクを実行するためのログイン情報を指定します。

［**バックアップの計画およびタスク**］ビューが表示され、復元タスクの状態と進行状況を調べることができます。

6.3.11. 起動のトラブルシューティング

システムがバックアップ時に起動可能であれば、復元後にも起動できると予期されます。ただし、ボリュームのサイズ、場所、または復元先のドライブを変更する場合は特に、オペレーティング システムが保存して起動に使用する情報が復元する際には古くなっている可能性があります。Acronis Backup & Recovery 10 は、復元後に Windows ローダーを自動的に更新します。他のローダーも修復される場合がありますが、ローダーを再度有効化する必要がある場合もあります。特に Linux のボリュームを復元する場合は、Linux が正しく起動して読み込むことができるように、修正を適用するか、または起動を変更する必要もあります。

次に、ユーザーによる追加の操作を必要とする一般的な状況について示します。

復元したオペレーティング システムを起動できない理由

- **コンピュータの BIOS によって別の HDD から起動するように構成されている**

  解決策: オペレーティング システムが存在する HDD から起動するように BIOS を構成します。

- **システムが異なるハードウェアに復元されたため、新しいハードウェアはバックアップに含まれているほとんどの重要なドライバと互換性がない**

  Windows 用の解決策: もう一度ボリュームを復元します。復元を構成する際に、Acronis Universal Restore を使用するように選択し、適切な HAL と大容量記憶装置のドライバを指定します。

- **起動できないダイナミック ボリュームに Windows が復元された**

  解決策: ベーシック ボリューム、シンプル ボリューム、またはミラー ボリュームに Windows を復元します。

- **MBR が存在しないディスクにシステム ボリュームが復元された**

  MBR が存在しないディスクにシステム ボリュームを復元するように構成する場合は、システム ボリュームと共に MBR を復元するかどうかを確認するメッセージが表示されます。システムを起動可能にしない場合にのみ、復元しないことを選択してください。

  解決策: 対応するディスクの MBR と共にボリュームを再度復元します。

- **システムは、Acronis OS Selector を使用している**

  マスタ ブート レコード(MBR)はシステムの復元中に変更できるため、MBR を使用する Acronis OS Selector が動作しなくなる場合があります。この場合は、次のようにして Acronis OS Selector を再度有効化します。

  解決策: Acronis Disk Director のブータブル メディアからコンピュータを起動し、**［ツール］→［OS Selector の有効化］**を選択します。

- **システムは GRUB(GRand Unified Bootloader)を使用して、(raw、つまりセクタごとではなく)通常のバックアップから復元された**

  GRUB ローダーの一部が、ディスクまたはボリュームの先頭のいくつかのセクタに存在しています。残りは、いずれかのボリュームのファイル システム上に存在しています。システムの起動は、GRUB がディスクの先頭のいくつかのセクタ、および直接アクセス可能なファイル システムに存在する場合にのみ自動的に復元できます。それ以外の場合は、ユーザーは手動でブート ローダーを再度有効化する必要があります。

  解決策: ブート ローダーを再度有効化します。構成ファイルの修正が必要になる場合があります。

- **システムは LILO(Linux Loader)を使用して、(raw、つまりセクタごとではなく)通常のバックアップから復元された**

  LILO には、絶対セクタ番号に対する一連の参照が含まれているため、ソース ディスクと同じ絶対セクタ番号を持っているセクタにすべてのデータが復元される場合を除いて、自動的に修復することはできません。

  解決策: ブート ローダーを再度有効化します。前の項目で説明した理由により、ローダー構成ファイルの修正が必要になる場合があります。

- **システム ローダーが誤ったボリュームをポイントする**

  この現象は、システム ボリュームまたはブート ボリュームが元の場所に復元されない場合に発生する可能性があります。

  解決策:

  boot.ini または boot¥bcd ファイルを変更すると、Windows ローダーに対するこの問題を修正できます。Acronis Backup & Recovery 10 は、この処理を自動的に実行するため、問題はほとんど発生しません。

  GRUB ローダーと LILO ローダーに関しては、GRUB 構成ファイルを修正する必要があります。Linux ルート パーティションの数が変更された場合は、SWAP ボリュームに正しくアクセスできるように、/etc/fstab を変更することもお勧めします。

- **Linux が LVM ボリュームのバックアップからベーシック MBR ディスクに復元された**

  そのようなシステムのカーネルは、LVM ボリュームにルート ファイル システムをマウントしようとするため、システムを起動できません。

  解決策: LVM を使用しないようにローダーの構成と /etc/fstab を変更し、再度ブート ローダーを起動します。

6.3.11.1. GRUB を再度有効化して構成を変更する方法

一般に、適切な手順についてはブート ローダーのマニュアルを参照する必要があります。また、対応する Knowledge Base の記事を Acronis Web サイトで参照することもできます。

システム ディスク(ボリューム)を同じハードウェアに復元した場合に GRUB を再度有効化する方法の例を次に示します。

1. Linux を起動するかブータブル メディアから起動し、［Ctrl］+［Alt］+［F2］を押します。
2. 復元するシステムをマウントします。

```
mkdir /mnt/system/
mount -t ext3 /dev/sda2 /mnt/system/ # root partition
mount -t ext3 /dev/sda1 /mnt/system/boot/ # boot partition
```

3. **proc** および **dev** ファイル システムを、復元するシステムにマウントします。

```
mount -t proc none /mnt/system/proc/
mount -o bind /dev/ /mnt/system/dev/
```

4. 次のいずれかのコマンドを実行して、GRUB メニュー ファイルを保存します。

```
cp /mnt/system/boot/grub/menu.lst /mnt/system/boot/grub/menu.lst.backup
```

   または

```
cp /mnt/system/boot/grub/grub.conf /mnt/system/boot/grub/grub.conf.backup
```

5. **/mnt/system/boot/grub/menu.lst** ファイル(Debian、Ubuntu、および SUSE Linux ディストリビューション)または **/mnt/system/boot/grub/grub.conf** ファイル(Fedora および Red Hat Enterprise Linux ディストリビューション)を編集します。たとえば、次のように編集します。

```
vi /mnt/system/boot/grub/menu.lst
```

6. **menu.lst** ファイル(または **grub.conf**)内で、復元するシステムに対応するメニュー項目を見つけます。このメニュー項目は次のような形式になっています。

```
title Red Hat Enterprise Linux Server (2.6.24.4)
      root (hd0,0)
      kernel /vmlinuz-2.6.24.4 ro root=/dev/sda2 rhgb quiet
      initrd /initrd-2.6.24.4.img
```

これらの行は **title**、**root**、**kernel**、および **initrd** で始まっており、それぞれ次の内容を表します。

- メニュー項目のタイトル。
- Linux カーネルが置かれているデバイス。通常、これはブート パーティションまたはルート パーティションで、この例では **root (hd0,0)** です。
- デバイス上にあるカーネルとルート パーティションのパス。この例では、カーネルのパスは **/vmlinuz-2.6.24.4** で、ルート パーティションは **/dev/sda2** です。ルート パーティションは、ラベル(**root=LABEL=/** など)、識別子(**root=UUID=***some_uuid* の形式)、またはデバイス名(**root=/dev/sda2** など)で指定できます。
- デバイスの **initrd** サービスのパス。

7. ファイル **/mnt/system/etc/fstab** を編集して、復元の結果として変更されたデバイスの名前を修正します。
8. 次のいずれかのコマンドを実行して、GRUB シェルを開始します。

```
chroot /mnt/system/ /sbin/grub
```

または

```
chroot /mnt/system/ /usr/sbin/grub
```

9. GRUB が置かれているディスクを指定します。通常は、ブート パーティションまたはルート パーティションです。

```
root (hd0,0)
```

10. GRUB をインストールします。たとえば、GRUB を最初のディスクのマスタ ブート レコード(MBR)にインストールするには、次のコマンドを実行します。

```
setup (hd0)
```

11. GRUB シェルを終了します。

```
quit
```

12. マウントしたファイル システムのマウントを解除し、再起動します。

```
umount /mnt/system/dev/
umount /mnt/system/proc/
umount /mnt/system/boot/
umount /mnt/system/
reboot
```

13. ツールと、使用している Linux ディストリビューションのドキュメントを使用して、ブート ローダーを再設定します。たとえば、Debian および Ubuntu では、**/boot/grub/menu.lst** ファイル内のコメント行を編集して、**update-grub** スクリプトを実行する必要がある場合があります。これを行わないと、変更は有効になりません。

6.3.11.2. Windows ローダーについて

Windows NT/2000/XP/2003

ローダーの一部はパーティションのブート セクタにあり、残りは ntldr、boot.ini、ntdetect.com、ntbootdd.sys ファイルにあります。boot.ini は、ローダーの構成を含むテキスト ファイルです。例:

```
[boot loader]
timeout=30
default=multi(0)disk(0)rdisk(0)partition(1)¥WINDOWS
[operating systems]
multi(0)disk(0)rdisk(0)partition(1)¥WINDOWS="Microsoft Windows XP Professional"
/noexecute=optin /fastdetect
```

Windows Vista/2008

ローダーの一部はパーティションのブート セクタにあり、残りは bootmgr、boot¥bcd ファイルにあります。Windows の起動時に、boot¥bcd がレジストリ キー HKLM¥BCD00000000 にマウントされます。

6.3.12. MD デバイスの復元(Linux)

Linux でディスク バックアップから既存の MD デバイス(Linux Software RAID デバイスとも呼ばれます)への復元を実行する際には、復元時に**このデバイスが構築済み**であることを確認してください。

デバイスが構築済みでない場合は、**mdadm** ユーティリティを使用して構築してください。以下に 2 つの例を示します。

例 1。次のコマンドは、ボリューム /dev/sdb1 と /dev/sdc1 が組み合わせられたデバイス /dev/md0 を構築します。

```
mdadm --assemble /dev/md0 -ayes /dev/sdb1 /sdc1
```

例 2。次のコマンドは、ディスク /dev/sdb と /dev/sdc が組み合わせられたデバイス /dev/md0 を構築します。

```
mdadm --assemble /dev/md0 -ayes /dev/sdb /dev/sdc
```

MD デバイスの復元でコンピュータの再起動が必要な場合(通常、デバイスにブート ボリュームが含まれている場合)は、次のガイドラインに従ってください。

- MD デバイスのすべての部分がボリュームの場合(最初の例と同様に、典型的な実例です)、各ボリュームの種類(パーティションの種類またはシステム ID と呼ばれます)が **Linux raid automount** であり、このパーティションの種類の 16 進コードが 0xFD であることを確認してください。これにより、再起動後にデバイスが自動的に構築されることが保証されます。パーティションの種類を表示または変更するには、**fdisk** などのディスク パーティション ユーティリティを使用します。
- それ以外の場合(2 番目の例など)は、デバイスをブータブル メディアから復元します。この場合、再起動は必要ありません。アセンブリには **mdadm** ユーティリティを使用します。ブータブル メディアでは、「MD デバイスと論理ボリュームの復元『ページ参照 309』」で説明しているように、MD デバイスを手動で作成する必要がある場合があります。

6.3.13. ファイル バックアップからの膨大な数のファイルの復元

対象: Microsoft Windows Server 2003

ファイル バックアップから膨大な数のファイル(数十万から数百万)を同時に復元しようとすると、次の問題が発生することがあります。

- 復元処理が失敗し、"ファイルの読み取りエラーです" というメッセージが表示される。
- すべてのファイルが復元されない。

この問題の原因として最も可能性の高いのは、オペレーティング システムのキャッシュ マネージャによって復元処理に割り当てられたメモリ量が十分ではなかったことです。次に説明する方法で、この問題を回避するか、レジストリを変更して割り当てられるメモリ量を増やすことができます。

問題を解決するには、次のいずれかを行います。

- ファイルを複数のグループに分けて復元します。たとえば、100 万のファイルの復元時に問題が発生するときは、最初の 50 万のファイルを復元してから、残りの 50 万のファイルを復元します。
- レジストリを次のように変更します。

> ***注意**: この手順ではコンピュータの再起動が必要になります。レジストリを変更するときの標準の予防措置を行ってください。*

1. レジストリ エディタで、次のレジストリ サブキーを開きます。

```
HKEY_LOCAL_MACHINE¥SYSTEM¥CurrentControlSet¥Control¥Session Manager¥Memory Management
```

2. このサブキーに **PoolUsageMaximum** エントリを追加します。
   - エントリの種類: **DWORD 値**
   - 表記: **10 進**
   - 値: **40**

3. このサブキーに **PagedPoolSize**エントリを追加します。
   - エントリの種類: **DWORD 値**
   - 表記: **16 進**
   - 値: **FFFFFFFF**
4. レジストリ エディタを終了してから、コンピュータを再起動します。

この方法で問題が解決しないとき、またはレジストリ設定を追加する方法の詳細については、対応する Microsoft のヘルプとサポートの記事をご参照ください。

ヒント: *一般に、1 つのボリュームに多数のファイルが格納されているときは、ファイル レベルのバックアップではなく、ディスク レベルのバックアップの使用を検討してください。ディスク レベルのバックアップでは、ボリューム全体およびボリュームに格納されている特定のファイルを復元できます。*

6.3.14. ストレージ ノードの復元

Acronis Backup & Recovery 10 ストレージ ノードによって管理される集中管理用格納域へのデータのバックアップに加えて、ストレージ ノード自体がインストールされているコンピュータのディスク バックアップを実行する必要がある場合があります。

ここでは、ストレージ ノードと管理サーバーが異なるコンピュータにインストールされている場合に、管理サーバーに登録されているストレージ ノードを復元する方法について説明します(これらが同じコンピュータにインストールされている場合は、そのコンピュータを復元するだけで済みます)。

次のようなシナリオについて考えてみます。

- 管理サーバーと、ストレージ ノードが存在するコンピュータを保有しているとします。
- ストレージ ノードは管理サーバーに登録されています。
- 以前に、ストレージ ノードと共にこのコンピュータはバックアップされており、同じコンピュータまたは別のコンピュータ上でその復元が終了したところです。

復元したストレージ ノードを使用する前に、以下の手順を実行します。

- ストレージ ノードが同じコンピュータに復元されていて、バックアップと復元の間に、ストレージ ノードによって管理される集中管理用格納域が追加または削除されていない場合は、何も実行する必要はありません。
- それ以外の場合は、以下の手順を実行します。

  1. 管理サーバーに接続し、ストレージ ノードを削除します。

  注意: *ストレージ ノードによって管理されるすべての格納域も管理サーバーから削除されます。アーカイブが失われることはありません。*

  2. 復元されたストレージ ノードがインストールされているコンピュータを指定して、管理サーバーに再度ストレージ ノードを追加します。
  3. 必要な管理対象の格納域を再作成します。

6.4. 格納域、アーカイブ、および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。

ファイル バックアップのベリファイでは、バックアップからダミーの復元先に対してすべてのファイルの復元を疑似的に実行します。ディスクまたはボリュームのバックアップのベリファイでは、バックアップに保存されているすべてのデータ ブロックのチェックサムを計算します。両方の手順では、リソースを集中的に使用します。

アーカイブのベリファイでは、アーカイブのすべてのバックアップがベリファイされます。格納域(または場所)のベリファイでは、この格納域(場所)に保存されているすべてのアーカイブがベリファイされます。

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、ブータブル環境から予備のハード ディスク ドライブへの復元テストによってのみ復元の成功が保証されます。少なくとも、ブータブル メディアを使用してバックアップを正常にベリファイできることを確認してください。

ベリファイ タスクを作成するさまざまな方法

ベリファイ タスクを作成する最も一般的な方法は、［ベリファイ］ページを使用することです。この時点ですぐにベリファイできますが、アクセス許可がある任意のバックアップ、アーカイブ、またはロケーションに対してベリファイ スケジュールを設定することもできます。

アーカイブまたはそのアーカイブに含まれる最新バックアップのベリファイは、バックアップ計画の一部としてスケジュールできます。詳細については、「バックアップ計画の作成『ページ参照 236』」をご参照ください。

［ベリファイ］ページには、**［格納域］**『ページ参照 153』ビューからアクセスできます。ベリファイするオブジェクト(アーカイブ、バックアップ、または格納域)を右クリックし、コンテキスト メニューから**［ベリファイ］**を選択します。ソースとしてオブジェクトがあらかじめ選択された状態で、［ベリファイ］ページが開きます。必要な作業は、ベリファイの実行時期の指定、およびタスクの名前の指定（オプション）のみです。

ベリファイ タスクを作成する手順は、次のとおりです。

［全般］

［タスク名］

(オプション)ベリファイ タスクの一意の名前を入力します。わかりやすい名前にすると、容易に他のタスクと区別することができます。

［ログイン情報］『ページ参照 283』

(オプション)ベリファイ タスクは、タスクを作成したユーザーの代わりに実行されます。タスクのログイン情報は、必要に応じて変更することができます。このオプションにアクセスするには、**［詳細ビュー］**チェックボックスをオンにします。

[ベリファイの対象]

[ベリファイ]

ベリファイするオブジェクトを選択します。

[アーカイブ]『ページ参照 284』- この場合、アーカイブを指定する必要があります。

[バックアップ]『ページ参照 285』- 最初にアーカイブを指定し、次に、このアーカイブから必要なバックアップを選択します。

[格納域]『ページ参照 285』- ベリファイ用にアーカイブする格納域(または他の場所)を選択します。

[アクセス ログイン情報]『ページ参照 286』

(オプション)タスク アカウントがソースに対する十分なアクセス権限を持っていない場合は、ソースにアクセスするためのログイン情報を指定します。このオプションにアクセスするには、**[詳細ビュー]**チェックボックスをオンにします。

[ベリファイの実行時期]

[ベリファイ]『ページ参照 286』

ベリファイの実行時期と頻度を指定します。

必要なすべての手順を完了したら、**[OK]**をクリックしてベリファイ タスクを作成します。

6.4.1. タスクのログイン情報

タスクを実行するアカウントのログイン情報を指定します。

ログイン情報を指定する手順は、次のとおりです。

1. 次のいずれかを選択します。
   - **現在のログイン情報を使用する**

     タスクは、タスクを起動するユーザーがログインしたときのログイン情報を使用して実行されます。スケジュールを設定してタスクを実行する場合は、タスクの作成を完了する際に現在のユーザーのパスワードを入力するよう求められます。
   - **次のログイン情報を使用する**

     タスクは、手動で開始されるか、スケジュールに従って実行されるかにかかわらず、常にユーザーが指定するログイン情報を使用して実行されます。

     次の項目を指定します。
     - **[ユーザー名]**- Active Directory ユーザー アカウントの名前を入力する場合は、ドメイン名(DOMAIN¥ユーザー名またはユーザー名@ドメイン)も指定してください。
     - **[パスワード]**- アカウントのパスワード。
2. **[OK]**をクリックします。

Acronis Backup & Recovery 10 のログイン情報の詳細については、「所有者とログイン情報『ページ参照 35』」をご参照ください。

ユーザー権限に応じて使用可能になる操作の詳細については、「管理対象のコンピュータ上のユーザー権限『ページ参照 34』」をご参照ください。

6.4.2. アーカイブの選択

アーカイブの選択

1. 場所のフル パスを［**パス**］フィールドに入力するか、**フォルダ ツリー**から目的のフォルダを選択します。
   - アーカイブが集中管理用格納域に保存されている場合、［**集中管理**］グループを展開し、格納域をクリックします。
   - アーカイブが個人用格納域に保存されている場合、［**個人用**］グループを展開し、格納域をクリックします。
   - アーカイブがコンピュータ上のローカル フォルダに保存されている場合、［**ローカル フォルダ**］グループを展開し、目的のフォルダをクリックします。

複数枚の DVD などのリムーバブル メディアにアーカイブがある場合は、まず最後に作成した DVD を挿入し、以降はメッセージに従って 1 枚目のディスクから順に挿入してください。

   - アーカイブがネットワーク共有に保存されている場合、［**ネットワーク フォルダ**］グループを展開し、ネットワーク上の必要なコンピュータを選択して、共有フォルダをクリックします。ネットワーク共有がアクセス ログイン情報を必要とする場合は、それらの情報が要求されます。

Linux ユーザー向けの注意: */mnt/share などのマウント ポイントにマウントされている CIFS(Common Internet File System)のネットワーク共有を指定するには、ネットワーク共有そのものではなく、このマウント ポイントを選択します。*

   - アーカイブが **FTP** サーバーまたは **SFTP** サーバーに保存されている場合、［**パス**］フィールドにサーバーの名前またはアドレスを次のように入力します。

     ftp://ftp_server:port _number または **sftp://sftp_server:port number**

     ポート番号が指定されていない場合、ポート 21 が FTP 用に、ポート 22 が SFTP 用に使用されます。

     アクセス ログイン情報を入力すると、サーバー上のフォルダが使用できるようになります。サーバー上の適切なフォルダをクリックします。

     匿名アクセスがサーバーによって許可されている場合、匿名ユーザーとしてサーバーにアクセスすることができます。匿名ユーザーとしてアクセスするには、ログイン情報を入力する代わりに、［**匿名アクセスを使用する**］をクリックします。

FTP 仕様の原文に記載されているように、FTP サーバーにアクセスするのに必要なログイン情報は、ネットワーク上をテキスト形式で転送されます。このことは、ユーザー名とパスワードが、パケット スニファを使用した盗聴者によって傍受される可能性があることを意味します。

   - ローカル接続したテープ デバイスにアーカイブが保存されている場合、［**テープ ドライブ**］グループを展開し、目的のデバイスをクリックします。

2. ツリーの右側にある表からアーカイブを選択します。この表には、選択した格納域またはフォルダに含まれているアーカイブの名前が表示されます。

   アーカイブの保存場所の内容を確認しているとき、別のユーザーまたはスケジュール設定された処理によって、アーカイブが追加、削除、または変更されることがあります。［**更新**］を使用すれば、アーカイブの一覧を更新できます。

   ［**アーカイブの表示**］と［**TIB ファイルの表示**］を使用すると、名前によってアーカイブを表示するか、アーカイブを TIB ファイルとして物理的に表示するかを切り替えることができます。

3. ［**OK**］をクリックします。

6.4.3. バックアップの選択

ベリファイするバックアップを指定する手順は、次のとおりです。

1. 上部のペインで、作成日時によってバックアップを選択します。

   正しいバックアップを見つけることができるように、ウィンドウの下部に、選択したバックアップの内容が表示されます。

2. ［**OK**］をクリックします。

6.4.4. ロケーションの選択

場所を選択する手順は、次のとおりです。

場所のフル パスを［**パス**］フィールドに入力するか、**フォルダ ツリー**から目的の場所を選択します。

- 集中管理用格納域を選択するには、**[集中管理]** グループを展開し、適切な格納域をクリックします。
- 個人用格納域を選択するには、［**個人用**］グループを展開し、適切な格納域をクリックします。
- ローカル フォルダ(CD/DVD ドライブ、またはローカル接続のテープ デバイス)を選択するには、［**ローカル フォルダ**］グループを展開し、目的のフォルダをクリックします。
- ネットワーク共有を選択するには、［**ネットワーク フォルダ**］グループを展開し、目的のネットワーク コンピュータを選択して、共有フォルダをクリックします。ネットワーク共有がアクセス ログイン情報を必要とする場合は、それらの情報が要求されます。
- **FTP** サーバーまたは **SFTP** サーバーを選択するには、対応するグループを展開し、サーバー上の適切なフォルダをクリックします。

FTP 仕様の原文に記載されているように、FTP サーバーにアクセスするのに必要なログイン情報は、ネットワーク上をテキスト形式で転送されます。このことは、ユーザー名とパスワードが、パケット スニファを使用した盗聴者によって傍受される可能性があることを意味します。

アーカイブ テーブルの使用

正しいロケーションを選択できるように、選択した各ロケーションに含まれているアーカイブの名前がテーブルに表示されます。アーカイブの保存場所の内容を確認しているとき、別のユーザーまたはスケジュール設定された処理によって、アーカイブが追加、削除、または変更されることがあります。［**更新**］を使用すれば、アーカイブの一覧を更新できます。

［**アーカイブの表示**］と［**TIB ファイルの表示**］を使用すると、名前によってアーカイブを表示するか、アーカイブを TIB ファイルとして物理的に表示するかを切り替えることができます。

6.4.5. ソースのアクセス ログイン情報

バックアップ アーカイブの保存先にアクセスするために必要なログイン情報を指定します。

ログイン情報を指定する手順は、次のとおりです。

1. 次のいずれかを選択します。
   - ［**タスクのログイン情報を使用する**］

     ［全般］セクションで指定されたタスク アカウントのログイン情報を使用して、その場所にアクセスします。
   - ［**次のログイン情報を使用する**］

     ユーザーが指定するログイン情報を使用して、その場所にアクセスします。タスク アカウントがその場所に対するアクセス許可を持っていない場合は、このオプションを使用します。ネットワーク共有またはストレージ ノードの格納域に対しては、特別なログイン情報を指定する必要がある場合があります。

     次の項目を指定します。

     - ［**ユーザー名**］- Active Directory ユーザー アカウントの名前を入力する場合は、ドメイン名(DOMAIN¥ユーザー名またはユーザー名@ドメイン)も指定してください。
     - ［**パスワード**］- アカウントのパスワード。
2. ［**OK**］をクリックします。

FTP 仕様の原文に記載されているように、FTP サーバーにアクセスするのに必要なログイン情報は、ネットワーク上をテキスト形式で転送されます。このことは、ユーザー名とパスワードが、パケット スニファを使用した盗聴者によって傍受される可能性があることを意味します。

6.4.6. ベリファイの実行時期

ベリファイは多くのリソースを使用する処理なので、管理対象のコンピュータのピーク時以外にベリファイをスケジュールするのが効果的です。これに対し、データに破損がなく正常に復元できるかどうかをすぐに知りたい場合は、タスクの作成後すぐにベリファイを開始することを検討してください。

次のいずれかを選択します。

- **［今すぐ］** - ベリファイ タスクの作成直後、つまり、［ベリファイ］ページで［OK］をクリックした直後にタスクを開始します。
- **［後で］** - 指定した日時に 1 回だけベリファイ タスクを開始します。
  次のように適切なパラメータを指定します。
  - **［日付と時刻］** - タスクを開始する日付と時刻です。
  - **［このタスクは手動で開始されます(タスクをスケジュールしないでください)］** - 後から手動でタスクを開始する場合は、このチェックボックスをオンにします。
- **［スケジュールに従う］** - タスクをスケジュールします。スケジュール パラメータを構成する方法の詳細については、「スケジューリング『ページ参照 199』」をご参照ください。

6.5. イメージのマウント

ディスク バックアップ(イメージ)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。同じバックアップに含まれる複数のボリュームは、単一のマウント操作によってマウントできます。マウント操作は、Windows または Linux を実行している管理対象のコンピュータにコンソールが接続されている場合に実行できます。

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、バックアップの内容の変更(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の実行を行うことができます。

制限事項: *Acronis Backup & Recovery 10 のストレージ ノードに保存されているボリュームのバックアップをマウントすることはできません。*

使用例:

- **共有**: マウントされたイメージをネットワーク上のユーザーが簡単に共有できます。
- **"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イメージをマウントします。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。
- **オフラインでのウィルス除去**: コンピュータが攻撃された場合、管理者はコンピュータをシャットダウンし、ブータブル メディアで起動してイメージを作成します。次に、このイメージを読み取り/書き込みモードでマウントし、ウィルス対策プログラムでスキャンしてウィルスを除去してから、コンピュータを復元します。
- **エラー チェック**: ディスク エラーにより復元に失敗した場合、イメージを読み取り/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、マウントしたディスクにエラーがないかどうかをチェックします。

イメージをマウントするには、次の手順を実行します。

ソース

アーカイブ『ページ参照 288』

アーカイブの保存先のパスを指定し、ディスク バックアップを含むアーカイブを選択します。

[バックアップ]『ページ参照 289』

バックアップを選択します。

[アクセス ログイン情報]『ページ参照 290』

(オプション)アーカイブの保存先のログイン情報を指定します。このオプションにアクセスするには、**[詳細ビュー]** チェックボックスをオンにします。

マウントの設定

[ボリューム]『ページ参照 290』

マウントするボリュームを選択し、すべてのボリュームに対するマウントの設定を構成します。ドライブ文字を割り当てるか、マウント ポイントを入力し、読み取り/書き込みまたは読み取り専用のアクセス モードを選択します。

必要なすべての手順を完了したら、**[OK]** をクリックしてボリュームをマウントします。

6.5.1. アーカイブの選択

アーカイブの選択

1. 場所のフル パスを **[パス]** フィールドに入力するか、**フォルダ ツリー**から目的のフォルダを選択します。
   - アーカイブが集中管理用格納域に保存されている場合、**[集中管理]** グループを展開し、格納域をクリックします。
   - アーカイブが個人用格納域に保存されている場合、**[個人用]** グループを展開し、格納域をクリックします。
   - アーカイブがコンピュータ上のローカル フォルダに保存されている場合、**[ローカル フォルダ]** グループを展開し、目的のフォルダをクリックします。

複数枚の DVD などのリムーバブル メディアにアーカイブがある場合は、まず最後に作成した DVD を挿入し、以降はメッセージに従って 1 枚目のディスクから順に挿入してください。

   - アーカイブがネットワーク共有に保存されている場合、**[ネットワーク フォルダ]** グループを展開し、ネットワーク上の必要なコンピュータを選択して、共有フォルダをクリックします。ネットワーク共有がアクセス ログイン情報を必要とする場合は、それらの情報が要求されます。

Linux ユーザー向けの注意: */mnt/share などのマウント ポイントにマウントされている CIFS(Common Internet File System)のネットワーク共有を指定するには、ネットワーク共有そのものではなく、このマウント ポイントを選択します。*

- アーカイブが **FTP** サーバーまたは **SFTP** サーバーに保存されている場合、**[パス]** フィールドにサーバーの名前またはアドレスを次のように入力します。

  ftp://ftp_server:port _number または **sftp://sftp_server:port number**

  ポート番号が指定されていない場合、ポート 21 が FTP 用に、ポート 22 が SFTP 用に使用されます。

  アクセス ログイン情報を入力すると、サーバー上のフォルダが使用できるようになります。サーバー上の適切なフォルダをクリックします。

  匿名アクセスがサーバーによって許可されている場合、匿名ユーザーとしてサーバーにアクセスすることができます。匿名ユーザーとしてアクセスするには、ログイン情報を入力する代わりに、**［匿名アクセスを使用する］**をクリックします。

FTP 仕様の原文に記載されているように、FTP サーバーにアクセスするのに必要なログイン情報は、ネットワーク上をテキスト形式で転送されます。このことは、ユーザー名とパスワードが、パケット スニファを使用した盗聴者によって傍受される可能性があることを意味します。

- ローカル接続したテープ デバイスにアーカイブが保存されている場合、**［テープ ドライブ］**グループを展開し、目的のデバイスをクリックします。

2. ツリーの右側にある表からアーカイブを選択します。この表には、選択した格納域またはフォルダに含まれているアーカイブの名前が表示されます。

   アーカイブの保存場所の内容を確認しているとき、別のユーザーまたはスケジュール設定された処理によって、アーカイブが追加、削除、または変更されることがあります。**［更新］**を使用すれば、アーカイブの一覧を更新できます。

   ［アーカイブの表示］と**［TIB ファイルの表示］**を使用すると、名前によってアーカイブを表示するか、アーカイブを TIB ファイルとして物理的に表示するかを切り替えることができます。

3. **［OK］**をクリックします。

6.5.2. バックアップの選択

バックアップを選択する手順は、次のとおりです。

1. 作成日時によって、いずれかのバックアップを選択します。
2. 正しいバックアップを選択できるように、下部のテーブルには選択したバックアップに含まれているボリュームが表示されます。

   ボリュームに関する情報を取得するには、ボリュームを右クリックし、**［情報］**をクリックします。

3. **［OK］**をクリックします。

6.5.3. アクセス ログイン情報

ログイン情報を指定する手順は、次のとおりです。

1. 次のいずれかを選択します。
   - **［現在のユーザーのログイン情報を使用する］**
     現在のユーザーのログイン情報を使用して、その場所にアクセスします。
   - **［次のログイン情報を使用する］**
     ユーザーが指定するログイン情報を使用して、その場所にアクセスします。現在のユーザー アカウントがその場所に対するアクセス許可を持っていない場合は、このオプションを使用します。ネットワーク共有またはストレージ ノードの格納域に対しては、特別なログイン情報を指定する必要がある場合があります。
     次の項目を指定します。
     - **［ユーザー名］**- Active Directory ユーザー アカウントの名前を入力する場合は、ドメイン名(DOMAIN¥ユーザー名またはユーザー名@ドメイン)も指定してください。
     - **［パスワード］**- アカウントのパスワード。
2. **［OK］**をクリックします。

FTP 仕様の原文に記載されているように、FTP サーバーにアクセスするのに必要なログイン情報は、ネットワーク上をテキスト形式で転送されます。このことは、ユーザー名とパスワードが、パケット スニファを使用した盗聴者によって傍受される可能性があることを意味します。

6.5.4. ボリュームの選択

マウントするボリュームを選択し、選択した各ボリュームに対するマウント用のパラメータを次のように構成します。

1. マウントを必要とする各ボリュームのチェックボックスをオンにします。
2. 選択したボリュームをクリックして、マウント用のパラメータを設定します。
   - **［アクセス モード］**- ボリュームをマウントする際のモードを次の中から選択します。
     - **［読み取り専用］**- 変更内容をコミットせずにバックアップ内のファイルを参照して開く場合に有効にします。
     - **［読み取り/書き込み］**- このモードでは、バックアップの内容が変更されることを前提として、増分バックアップを作成して変更内容を取り込みます。
   - **［ドライブ文字の割り当て］**(Windows) - Acronis Backup & Recovery 10 は、マウントされたボリュームに未使用のドライブ文字を割り当てます。必要に応じて、ドロップダウン リストから別のドライブ文字を選択して割り当てます。
   - **［マウント ポイント］**(Linux) - ボリュームをマウントするディレクトリを指定します。
3. 複数のボリュームをマウントする場合は、前の手順で説明した要領で、すべてのボリュームをクリックしてマウント用のパラメータを設定します。
4. **［OK］**をクリックします。

6.6. マウントされているイメージの管理

ボリュームをマウントすると、ファイル マネージャを使用してバックアップに含まれているファイルとフォルダを選択し、必要なファイルを任意の場所にコピーすることができます。したがって、ボリュームのバックアップから少数のファイルとフォルダだけを取り出す場合は、復元手順を実行する必要はありません。

イメージの参照

マウントされているボリュームを参照すると、ボリュームの内容を表示したり変更したりすることができます(読み取り/書き込みモードでマウントされている場合)。

マウントされているボリュームを参照するには、テーブルからボリュームを選択し、  **[参照]**をクリックします。デフォルトのファイル マネージャのウィンドウが開き、マウントされているボリュームの内容を確認できます。

イメージのマウント解除

マウントされているボリュームの保守には、かなりのシステム リソースを必要とします。必要な処理が完了した後は、ボリュームのマウントを解除することをお勧めします。手動でマウントを解除しなければ、ボリュームはオペレーティング システムが再起動するまでマウントされたままになります。

イメージのマウントを解除するには、テーブルからボリュームを選択し、  **[マウント解除]**をクリックします。

マウントされているすべてのボリュームのマウントを解除するには、  **[すべてマウント解除]**をクリックします。

6.7. Acronis セキュア ゾーン

Acronis セキュア ゾーンは、管理対象のコンピュータのディスク領域にバックアップ アーカイブを保存できる安全なパーティションです。このため、同じディスクに保存したバックアップからディスクを復元することができます。

セキュア ゾーンには、Acronis ディスク管理ツールなどの特定の Windows アプリケーションを使用してアクセスできます。

Acronis セキュア ゾーンの利点と制限事項の詳細については、「Acronis 独自のテクノロジ」の「Acronis セキュア ゾーン『ページ参照 58』」をご参照ください。

6.7.1. Acronis セキュア ゾーンの作成

オペレーティング システムの実行中、またはブータブル メディアから起動して、Acronis セキュア ゾーンを作成することができます。

Acronis セキュア ゾーンを作成する手順は、次のとおりです。

領域

ディスク『ページ参照 293』

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。Acronis セキュア ゾーンは、未割り当て領域(使用可能な場合)またはボリュームの空き領域を使用して作成されます。

サイズ『ページ参照 293』

ゾーンの正確なサイズを指定します。現在アクティブなオペレーティング システムが含まれるボリュームなどのロックされたボリュームを移動またはサイズ変更するには、再起動する必要があります。

設定

パスワード『ページ参照 293』

(オプション)パスワードを使用して Acronis セキュア ゾーンを権限のないアクセスから保護します。Acronis リカバリ マネージャ『ページ参照 413』の使用を含むゾーンに関連するすべての操作で、パスワードの入力を求めるメッセージが表示されます。

Acronis リカバリ マネージャ『ページ参照 294』

(オプション)Acronis リカバリ マネージャの使用を有効にするには、**［有効化する］**を選択します。

GRUB ブート ローダーを使用しておらず、また GRUB ブート ローダーがマスタ ブート レコード(MBR)内にインストールされていない場合、Acronis リカバリ マネージャを有効化すると、そのブート コードで MBR が上書きされます。したがって、サードパーティ製のブート ローダーがインストールされている場合は、再度有効化する必要がある場合があります。

Linux で GRUB 以外のブート ローダー(LILO など)を使用する場合は、ASRM を有効化する前に、MBR ではなく Linux のルート(またはブート)パーティションのブート レコードにブート ローダーをインストールすることを検討してください。または、有効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。

Acronis リカバリ マネージャを無効にするには、**［有効化しない］**を選択します。

Acronis リカバリ マネージャは、後で［Acronis セキュア ゾーンの管理『ページ参照 295』］ページから有効化することができます。

必要な設定を構成したら、**［OK］**をクリックします。**［結果の確認］**『ページ参照 295』ウィンドウで、予定されるレイアウトを確認し、**［OK］**をクリックしてゾーンの作成を開始します。

6.7.1.1. Acronis セキュア ゾーン ディスク

Acronis セキュア ゾーンは、任意の固定ハード ディスク ドライブに配置することができます。Acronis セキュア ゾーンは、常にハード ディスクの末尾に作成されます。Acronis セキュア ゾーンは 1 台のコンピュータに 1 つだけ作成できます。Acronis セキュア ゾーンは、未割り当て領域(使用可能な場合)またはボリュームの空き領域を使用して作成されます。

Acronis セキュア ゾーンは、ダイナミック ディスク上または GPT パーティション スタイルを使用するディスク上に作成することはできません。

Acronis セキュア ゾーンの領域を割り当てる手順は、次のとおりです。

1. 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。デフォルトでは未割り当て領域が選択されます。Acronis セキュア ゾーンで使用可能な領域の合計が表示されます。
2. より多くの領域をゾーンに割り当てる必要がある場合は、空き領域を使用できるボリュームを選択することができます。選択内容に応じて、Acronis セキュア ゾーンで使用可能な領域の合計がもう一度表示されます。**［Acronis セキュア ゾーンのサイズ］**『ページ参照 293』ウィンドウでゾーンの正確なサイズを設定することができます。
3. **［OK］**をクリックします。

6.7.1.2. Acronis セキュア ゾーンのサイズ

Acronis セキュア ゾーン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 50MB になります。最大サイズは、ハード ディスクの未割り当て領域と、前の手順で選択したすべてのボリュームの空き領域の合計に等しくなります。

ブート ボリュームまたはシステム ボリュームの領域を使用する必要がある場合は、次の点に注意してください。

- 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、再起動する必要があります。
- システム ボリュームの空き領域をすべて使用すると、オペレーティング システムの動作が不安定になり、起動できなくなる場合もあります。ブート ボリュームまたはシステム ボリュームを選択する場合は、ゾーンに最大サイズを設定しないでください。

6.7.1.3. Acronis セキュア ゾーンのパスワード

パスワードを設定すると、Acronis セキュア ゾーンを権限のないアクセスから保護できます。データのバックアップと復元、アーカイブのベリファイ、［F11］キーを使用した Acronis リカバリ マネージャの使用、ゾーンのサイズ変更と削除など、ゾーンとゾーンに配置されているアーカイブに関連するすべての操作でパスワードを要求されます。

パスワードを設定する手順は、次のとおりです。

1. **［パスワードを使用する］**を選択します。
2. **［パスワードの入力］**フィールドに新しいパスワードを入力します。
3. **［パスワードの確認入力］**フィールドにパスワードを再入力します。
4. **［OK］**をクリックします。

パスワードを無効にする手順は、次のとおりです。

1. **［使用しない］**を選択します。
2. **［OK］**をクリックします。

6.7.1.4. Acronis リカバリ マネージャ

Acronis リカバリ マネージャはブータブル エージェント『ページ参照 422』の改定版で、システム ディスク上に常駐し、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。これにより、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別のメディアまたはネットワーク接続が不要になります。

［有効化する］

起動時の［Press F11 for Acronis Startup Recovery Manager...］というメッセージを有効にするか(GRUB ブート ローダーがない場合)、［Acronis リカバリ マネージャ］という項目を GRUB のメニューに追加します(GRUB がある場合)。システムが起動しない場合は、［F11］キーを押すか、メニューから選択することによってブータブル レスキュー ユーティリティを起動することができます。

GRUB ブート ローダーを使用しておらず、また GRUB ブート ローダーがマスタ ブート レコード(MBR)内にインストールされていない場合、Acronis リカバリ マネージャを有効化すると、そのブート コードで MBR が上書きされます。したがって、サードパーティ製のブート ローダーがインストールされている場合は、再度有効化する必要がある場合があります。

Linux で GRUB 以外のブート ローダー(LILO など)を使用する場合は、ASRM を有効化する前に、MBR ではなく Linux のルート(またはブート)パーティションのブート レコードにブート ローダーをインストールすることを検討してください。または、有効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。

［有効化しない］

起動時の［Press F11 for Acronis Startup Recovery Manager...］というメッセージ(または GRUB のメニュー項目)を無効にします。Acronis リカバリ マネージャが有効になっていない場合は、システムが起動しないときにシステムを復元するために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。
- Acronis PXE サーバーまたは 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。

詳細については、「ブータブル メディア『ページ参照 297』」をご参照ください。

6.7.1.5. 結果の確認

選択した設定に従って、［**結果の確認**］ウィンドウに予定されるパーティションのレイアウトが表示されます。レイアウトに問題がない場合は、［**OK**］をクリックし、Acronis セキュア ゾーンの作成を開始します。

ユーザー設定の処理方法

ここでは、Acronis セキュア ゾーンを作成する際に、複数のボリュームを持つディスクがどのように変換されるかについて説明します。

- Acronis セキュア ゾーンは、常にハード ディスクの末尾に作成されます。ボリュームの最終的なレイアウトを計算する際には、最初に、末尾にある未割り当て領域が使用されます。
- ディスクの末尾に十分な未割り当て領域がないがボリュームの間に未割り当て領域がある場合は、末尾に未割り当て領域を追加するためにボリュームが移動されます。
- すべての未割り当て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。ロックされているボリュームのサイズを変更すると再起動が必要になります。
- ただし、オペレーティング システムとアプリケーションが、一時ファイルを作成する場合など、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% 以下になる場合は、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、使用可能なゾーンを最大サイズに設定することはお勧めできません。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。

6.7.2. Acronis セキュア ゾーンの管理

Acronis セキュア ゾーンは、個人用格納域『ページ参照 425』と見なされます。セキュア ゾーンは、管理対象のコンピュータに作成されると、［**個人用格納域**］の一覧に常に表示されます。集中管理用バックアップ計画では Acronis セキュア ゾーンとローカルの計画を使用できます。

Acronis セキュア ゾーンを以前に使用したことがある場合は、機能が大幅に変更されていることに注意してください。セキュア ゾーンでは、自動クリーンアップ、つまり、古いアーカイブの削除は実行されなくなりました。自動クリーンアップ付きのバックアップ スキームを使用してセキュア ゾーンにバックアップするか、格納域管理機能を使用して古いアーカイブを手動で削除してください。

新しい Acronis セキュア ゾーンの動作では、次の操作を行うことができます。

- セキュア ゾーンに配置されているアーカイブ、および各アーカイブに含まれるバックアップを表示する。
- バックアップの内容を調べる。
- バックアップから物理ディスクにファイルをコピーするために、ボリューム バックアップをマウントする。
- アーカイブと、アーカイブに含まれるバックアップを安全に削除する。

格納域の操作の詳細については、「格納域『ページ参照 153』」をご参照ください。

6.7.2.1. Acronis セキュア ゾーンの拡大

Acronis セキュア ゾーンを拡大する手順は、次のとおりです。

1. **［Acronis セキュア ゾーンの管理］**ページで、**［拡大］**をクリックします。
2. Acronis セキュア ゾーンを拡大するために使用する空き領域が含まれるボリュームを選択します。
3. 次の操作によってゾーンの新しいサイズを指定します。
   - スライダをドラッグし、現在の値と最大値の間の任意のサイズを選択します。最大サイズは、ディスクの未割り当て領域と、選択したパーティションの空き領域の合計に等しくなります。
   - ［Acronis セキュア ゾーンのサイズ］フィールドに正確な値を入力します。

   ゾーンのサイズの拡大は、プログラムにより次のように行われます。
   - 最初に、未割り当て領域が使用されます。必要に応じて、ボリュームは移動されますが、サイズは変更されません。ロックされたボリュームが移動されると再起動が必要になります。
   - 十分な未割り当て領域がない場合は、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。ロックされたパーティションのサイズが変更されると再起動が必要になります。

   システム ボリュームを最小サイズに縮小すると、コンピュータのオペレーティング システムが起動しなくなることがあります。
4. **［OK］**をクリックします。

6.7.2.2. Acronis セキュア ゾーンの縮小

Acronis セキュア ゾーンを縮小する手順は、次のとおりです。

1. **［Acronis セキュア ゾーンの管理］**ページで、**［縮小］**をクリックします。
2. 縮小したゾーンの空き領域を受け取るボリュームを選択します。

3. 次の操作によってゾーンの新しいサイズを指定します。
   - スライダをドラッグし、現在の値と最小値の間の任意の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 50MB になります。
   - ［**Acronis セキュア ゾーンのサイズ**］フィールドに正確な値を入力します。
4. ［**OK**］をクリックします。

6.7.2.3. Acronis セキュア ゾーンの削除

プログラムをアンインストールせずにセキュア ゾーンを削除する手順は、次のとおりです。

1. ［**Acronis セキュア ゾーンの操作**］バー(［**アクションとツール**］ペイン)で、［**削除**］を選択します。
2. ［**Acronis セキュア ゾーンの削除**］ウィンドウで、セキュア ゾーンから解放される領域を追加するボリュームを選択し、［**OK**］をクリックします。
   複数のボリュームを選択した場合、領域は各パーティションのサイズに比例して分配されます。ボリュームを選択しない場合は、空き領域は未割り当てになります。

［**OK**］をクリックすると、Acronis Backup & Recovery 10 によってゾーンの削除が開始されます。

Acronis Backup & Recovery 10 エージェントをシステムから削除する際には、Acronis セキュア ゾーンとその内容を保持するか(これによりブータブル メディアから起動するときにデータの復元が可能になります)、または、Acronis セキュア ゾーンを削除するかのいずれかを選択できます。

6.8. ブータブル メディア

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 ドライブ、またはコンピュータの BIOS によってブート デバイスとしてサポートされるその他のメディア)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、任意の PC 互換コンピュータから 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、Acronis Backup & Recovery 10 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
- アクセス制限、アプリケーションの実行による連続的なロック、またはその他の原因のために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

コンピュータは、物理メディアを使用するか、Acronis PXE サーバー、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、上記の環境で起動することができます。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。

Linux ベースのブータブル メディア

Linux ベースのメディアには、Linux カーネルを基にした Acronis Backup & Recovery 10 ブータブル 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。この操作は、管理コンソールを使用して、ローカルでまたはリモートから設定および制御できます。

PE ベースのブータブル メディア

PE 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 Acronis Backup & Recovery 10 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 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 Backup & Recovery 10 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 互換ハードウェアを WinPE で起動すると、Acronis Backup & Recovery 10 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。Windows Vista または Windows Server 2008 のカーネルである PE 2.x に基づくメディアでは、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。

6.8.1. ブータブル メディアの作成方法

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、空のディスクを用意して、Acronis PXE サーバーをインストールするか、WDS/RIS を設定します。次に、ブータブル メディア ビルダを、管理コンソールから起動するか、**［ツール］→［ブータブル メディアの作成］**を選択して起動するか、別のコンポーネントとして起動します。ウィザードによって必要な操作が示されます。詳細については、「ブータブル メディア ビルダ『ページ参照 300』」をご参照ください。

PE ベースのブータブル メディア

WinPE 用 Acronis プラグインは、次のいずれかのカーネルに基づく WinPE ディストリビューションに追加できます。

- Windows XP Professional Service Pack 2(PE 1.5)
- Windows Server 2003 with Service Pack 1(PE 1.6)
- Windows Vista(PE 2.0)
- Windows Vista SP1 および Windows Server 2008(PE 2.1)

既に PE1.x ディストリビューションのメディアをお持ちの場合は、メディア ISO をローカル フォルダにアンパックし、［スタート］メニュー→［Acronis］から［Acronis WinPE ISO ビルダ］を選択して起動します。ウィザードによって必要な操作が示されます。詳細については、「WinPE 1.x への Acronis プラグインの追加『ページ参照 303』」をご参照ください。

PE 2.x イメージを作成または変更できるようにするには、Windows 自動インストール キット(AIK)がインストールされているコンピュータに Acronis WinPE ISO ビルダをインストールします。操作の詳細については、「WinPE 2.x への Acronis プラグインの追加『ページ参照 304』」で説明します。

WAIK 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。

1. Windows 自動インストール キット(WAIK)をダウンロードしてインストールします。
   Windows Vista 用の自動インストール キット(AIK)(PE 2.0):
   http://www.microsoft.com/Downloads/details.aspx?familyid=C7D4BC6D-15F3-4284-9123-679830D629F2&displaylang=ja
   Windows Vista SP1 および Windows Server 2008 用の自動インストール キット(AIK)(PE 2.1):
   http://www.microsoft.com/downloads/details.aspx?FamilyID=94bb6e34-d890-4932-81a5-5b50c657de08&DisplayLang=ja
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. このキットから Microsoft .NET Framework v.2.0(ハードウェアに応じて、NETFXx86 または NETFXx64)をインストールします。
4. このキットから Microsoft Core XML(MSXML)5.0 パーサーまたは 6.0 パーサーをインストールします。
5. このキットから Windows AIK をインストールします。
6. 同じコンピュータ上に Acronis WinPE ISO ビルダをインストールします。

Windows AIK で提供されているヘルプ ドキュメントの内容を把握しておく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。

Bart PE の使用

Bart PE ビルダを使用して、Acronis プラグイン付きの Bart PE イメージを作成できます。詳細については、「Windows ディストリビューションを使用した Acronis プラグイン付き Bart PE の作成『ページ参照 305』」をご参照ください。

6.8.1.1. ブータブル メディア ビルダ

物理メディアを作成するには、コンピュータに CD/DVD 書き込み用ドライブが搭載されているか、フラッシュ ドライブを接続できることが必要です。PXE または WDS/RIS を設定するには、コンピュータをネットワークに接続する必要があります。また、ブータブル メディア ビルダを使用すると、ブータブル ディスクの ISO イメージを作成できるため、後で空のディスクに書き込むことができます。

メディア ビルダを使用する際は、次の項目を指定する必要があります。

1. メディアに配置する Acronis ブータブル コンポーネント。
   - メディアを作成するコンピュータに Acronis Backup & Recovery 10 Universal Restore がインストールされている場合は、Universal Restore を有効にすることができます。
2. (オプション)起動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起動するコンポーネント。
   - 設定されていない場合、Acronis ローダーは、ユーザーが、オペレーティング システム(存在する場合)を起動するか、または Acronis コンポーネントを起動するかを選択するまで待機します。
   - たとえば、ブータブル エージェントに対して 10 秒を設定すると、起動メニューが表示されてから 10 秒後にブータブル エージェントが起動します。これにより、PXE サーバーまたは WDS/RIS から起動するときに、無人のオンサイト操作を実行できます。
3. (オプション)リモート ログイン設定。
   - エージェントへの接続時にコンソール側で入力するユーザー名とパスワード。これらのフィールドを空白のままにすると、プロンプト ウィンドウに任意の文字を入力するだけで接続できます。
4. (オプション)ネットワーク設定『ページ参照 301』。
   - 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。
5. (オプション)ネットワーク ポート『ページ参照 302』。
   - 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。
6. 作成するメディアの種類。次の操作を実行できます。
   - ハードウェア BIOS で CD、DVD、またはリムーバブル USB フラッシュ ドライブなどのその他のブータブル メディアからの起動が許可されている場合は、そのブータブル メディアの作成。
   - 後で空のディスクに書き込むための、ブータブル ディスクの ISO イメージの作成。
   - Acronis PXE サーバー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。
7. (オプション)Acronis Universal Restore で使用する Windows システム ドライバ『ページ参照 302』。このウィンドウは、Acronis Universal Restore アドオンがインストールされ、PXE および WDS/RIS 以外のメディアが選択されている場合にのみ表示されます。
8. メディア ISO ファイルのパス、あるいは、PXE や WDS/RIS の名前または IP とログイン情報。

ネットワークの設定

Acronis 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することができます。

- 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。設定があらかじめ構成されていない場合は、エージェントは DHCP 自動構成を使用します。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 が占有するスロット別に、プロセッサに最も近い側から順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用のブータブル メディアをカスタマイズできます。これを行うには、そのコンピュータのスロットの順序(NIC1 はプロセッサに最も近いスロットを占有し、NIC2 はその次のスロットを占有するなど)に従って NIC を設定します。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。自動構成でこの接続用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 設定を使用する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。次のいずれかを選択できます。

- 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、エージェントはデフォルトのポート番号(9876)を使用します。このポートは、Acronis Backup & Recovery 10 管理コンソールもデフォルトとして使用します。一時的なポート設定を使用できます。コンソールをエージェントに接続している間、URL 表記 <エージェントの IP>:<ポート> を使用して、特定のセッションのポートを指定します。

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。これらのドライバは、プロセッサ、マザーボード、または大容量記憶装置がバックアップ システムとは異なるコンピュータ上に Windows を復元する際に、Universal Restore によって使用されます。

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。

詳細については、「Universal Restore『ページ参照 272』」をご参照ください。

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。

ブータブル メディアへのドライバの追加は、次の状態のときに実行できます。

1. ブータブル メディアを作成するコンピュータに Acronis Backup & Recovery 10 Universal Restore アドオンがインストールされている。
2. 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。PXE サーバーや WDS/RIS に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することができます。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。

6.8.1.2. WinPE 1.x への Acronis プラグインの追加

WinPE 用 Acronis プラグインは次の環境に追加できます。

- Windows PE 2004(1.5)(Windows XP Professional Service Pack 2)
- Windows PE 2005(1.6)(Windows Server 2003 Service Pack 1)

Acronis プラグインを WinPE 1.x に追加する手順は、次のとおりです。

1. Acronis Backup & Recovery 10 セットアップ ファイルから WinPE 用 Acronis プラグインをインストールします。
2. WinPE 1.x ISO のすべてのファイルをハード ディスク上の別のフォルダにアンパックします。
3. ［スタート］メニューから［Acronis WinPE ISO ビルダ］を選択します。
4. WinPE ファイルが格納されているフォルダのパスを指定します。
5. Acronis プラグインのファイルが格納されているフォルダのパスを指定します(レジストリ キー HKEY_LOCAL_MACHINE¥SOFTWARE¥Acronis¥WinPE¥Settings¥WinPE でプラグインの場所を確認してください)。
6. 作成する ISO ファイルのフル パスを、ファイル名を含めて指定します。
7. 概要の画面で設定を確認し、**［実行］**をクリックします。
8. 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、フラッシュ ドライブにコピーします。

コンピュータが WinPE で起動すると、Acronis Backup & Recovery 10 が自動的に起動されます。

6.8.1.3. WinPE 2.x への Acronis プラグインの追加

Acronis WinPE ISO ビルダには、Acronis Backup & Recovery 10 を WinPE 2.x に統合する、次の 3 つの方法が用意されています。

- Acronis プラグインを既存の PE 2 ISO に追加する。この方法は、以前に設定済みで既に使用中の PE 2 ISO にプラグインを追加するときに便利です。
- プラグインが組み込まれた PE 2 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。

上記の操作のいずれかを実行できるようにするには、Windows 自動インストール キット(WAIK)がインストールされているコンピュータに Acronis WinPE ISO ビルダをインストールします。このようなコンピュータがない場合は、「ブータブル メディアの作成方法『ページ参照 298』」の説明に従って準備してください。

Acronis WinPE ISO ビルダは、x86 WinPE 2.x のみをサポートします。この WnPE ディストリビューションは、x64 ハードウェア上でも動作できます。

Win PE 2.0 に基づく PE イメージが動作するには、少なくとも 256MB の RAM が必要です。PE 2.0 の推奨されるメモリ サイズは 512MB です。

WinPE 2.x ISO への Acronis プラグインの追加

Acronis プラグインを WinPE 2.x ISO に追加する手順は、次のとおりです。

1. 次のいずれかを実行します。

   既存の Win PE 2 ISO にプラグインを追加する際に、Win PE 2 ISO のすべてのファイルをハード ディスク上の別のフォルダにアンパックします。

   新しい PE 2 ISO を作成する際に、次の操作を実行します。

   ［スタート］メニューから［**Microsoft Windows AIK**］→［**Windows PE ツールのコマンド プロンプト**］を選択します。

   copype.cmd スクリプトを実行し、Windows PE ファイルが格納されたフォルダを作成します。たとえば、コマンド プロンプトから次のように入力します。

   ```
   cd Program Files¥Windows AIK¥Tools¥PETools¥
   copype <arch> <destination>
   ```

   ここで、<arch> はハードウェア アーキテクチャ(x86、amd64、または ia64 を指定できますが、Acronis は x86 のみをサポートします)、<destination> はローカル フォルダのパスを表します。たとえば、次のようになります。

   ```
   copype x86 c:¥winpe_x86
   ```

2. ［スタート］メニューから［Acronis WinPE ISO ビルダ］を選択します。
3. WinPE ファイルが格納されたフォルダへのパスを指定します。
4. Acronis プラグイン ファイルが格納されたフォルダのパスを指定します (レジストリ キー HKEY_LOCAL_MACHINE¥SOFTWARE¥Acronis¥WinPE¥Settings¥WinPE でプラグインの場所を確認してください)。

5. ISO または WIM のイメージを作成するかどうかを選択します。
6. 作成するイメージ ファイルのフル パスを、ファイル名を含めて指定します。
7. 概要の画面で設定を確認し、［実行］をクリックします。
8. 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、フラッシュ ドライブにコピーします。

コンピュータが WinPE で起動すると、Acronis Backup & Recovery 10 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)を作成する手順は、次のとおりです。

- 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
```

WinPE 2.x WIM への Acronis プラグインの追加

1. ［スタート］メニューから［Acronis WinPE ISO ビルダ］を選択します。
2. 追加元の WINPE.WIM ファイルのパスを指定します。x86 ハードウェア用のこのファイルの標準のパスは、¥Program Files¥Windows AIK¥Tools¥PETools¥x86¥winpe.wim です。
3. Acronis プラグイン ファイルが格納されたフォルダのパスを指定します (レジストリ キー HKEY_LOCAL_MACHINE¥SOFTWARE¥Acronis¥WinPE¥Settings¥WinPE でプラグインの場所を確認してください)。
4. 作成する WIM ファイルのフル パスを、ファイル名を含めて指定します。
5. 概要の画面で設定を確認し、［実行］をクリックします。

結果の WIM ファイルから PE イメージ(ISO ファイル)を作成する方法については、前のセクションをご参照ください。

Windows PE のカスタマイズの詳細については、『Windows プレインストール環境 (Windows PE) ユーザーズ ガイド』(Winpe.chm)をご参照ください。

6.8.1.4. Windows ディストリビューションを使用した Acronis プラグイン付き Bart PE の作成

1. Bart PE ビルダを取得します。
2. Acronis Backup & Recovery 10 セットアップ ファイルから Acronis WinPE ISO ビルダをインストールします。

3. 現在のフォルダを WinPE 用 Acronis プラグインがインストールされているフォルダに変更します。デフォルトでは、C:¥Program Files¥Acronis¥WinPE¥WinPE です。

   プラグインがデフォルト以外のフォルダにインストールされている場合は、そのフォルダにパスを変更します(レジストリ キー HKEY_LOCAL_MACHINE¥SOFTWARE¥Acronis¥WinPE¥Settings¥WinPE でプラグインの場所を確認してください)。

4. 次のコマンドを実行します。

   ```
   export_license.bat
   ```

5. 現在のフォルダ(デフォルトでは、C:¥Program Files¥Acronis¥WinPE¥WinPE です)の内容を %BartPE folder%¥plugins¥Acronis にコピーします。
6. HDD に Windows インストール ファイルのコピーがない場合は、Windows ディストリビューション CD を挿入します。
7. Bart PE ビルダを起動します。
8. Windows インストール ファイルまたは Windows ディストリビューション CD のパスを指定します。
9. **[プラグイン]** をクリックし、Acronis プラグインが有効になっているかどうか確認します。無効になっているときは有効にします。
10. 出力フォルダと、作成する ISO ファイルへのファイル名を含むフル パスまたは作成するメディアのフル パスを指定します。
11. Bart PE を作成します。
12. ISO を CD または DVD に書き込むか(まだ書き込んでいない場合)、フラッシュ ドライブにコピーします。

コンピュータが Bart PE で起動し、ネットワーク接続の設定が完了したら、**[移動]** → **[システム]** → **[ストレージ]** → **[Acronis Backup & Recovery 10]** を選択して起動します。

6.8.2. 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。

リモート接続

リモートからこのコンピュータに接続するには、コンソール メニューの **[接続]** → **[リモート コンピュータの管理]** を選択し、コンピュータの IP アドレスの 1 つを指定します。ブータブル メディアを作成する際にユーザー名とパスワードを設定した場合は、そのユーザー名とパスワードを指定します。

ローカル接続

Acronis Backup & Recovery 10 管理コンソールは、ブータブル メディアに必ず用意されています。コンピュータ端末に物理的にアクセスできる場合は、誰でもこのコンソールを実行して接続できます。ブータブル エージェントのスタートアップ ウィンドウで **[管理コンソールの実行]** をクリックするだけで接続できます。

6.8.3. ブータブル メディア使用時の操作

ブータブル メディアを使用して起動したコンピュータでの操作は、オペレーティング システムでのバックアップと復元によく似ています。両者の違いは次のとおりです。

1. Windows スタイルのブータブル メディアで表示されるディスクのドライブ文字が Windows で識別されるドライブと異なることがある。たとえば、レスキュー ユーティリティでの 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。

   ご注意ください。安全のために、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 スタイルのブータブル メディアでは、ローカル ディスクとボリュームがマウント解除(sda1、sda2...)として表示されます。
3. メディアの GUI には［**ナビゲーション**］ツリーがない。ビューの間を移動するには、［**ナビゲーション**］を使用します。
4. タスクのスケジュールは設定できない。つまり、タスクはまったく作成されません。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。
5. ログは、現在のセッションの期間内だけ有効となる。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。
6. 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。

   管理対象の格納域にアクセスするには、次の文字列を［**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用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

メディアから起動されたコンピュータでは、ディスプレイ ビデオ モードはハードウェア構成(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。何らかの原因で、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 プロンプトに「**vga=ask**」というコマンドを追加し、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。

6.8.4. Linux ベースのブータブル メディアで使用できるコマンドとユーティリティの一覧

Linux ベースのブータブル メディアには、次のコマンドとコマンド ライン ユーティリティが用意されています。これらは、コマンド シェルから使用できます。コマンド シェルを起動するには、ブータブル メディアの管理コンソールで Ctrl+Alt+F2 キーを押します。

Acronis コマンド ライン ユーティリティ

- acronis
- asamba
- lash
- restoreraids
- trueimagecmd
- trueimagemnt

Linux のコマンドとユーティリティ

busybox	ifconfig	readcd
cat	init	reboot
cdrecord	insmod	rm
chmod	iscsiadm	rmmod
chown	kill	route
chroot	kpartx	scp
cp	ln	scsi_id
dd	ls	sed
df	lspci	sg_map26
dmesg	lvm	sh
dmraid	mc	sleep
e2fsck	mdadm	ssh
e2label	mkdir	sshd
echo	mke2fs	strace
egrep	mknod	swapoff
fdisk	mkswap	swapon
fsck	more	sysinfo

```
fxload      mount        tar
gawk        mtx          tune2fs
gpm         mv           udev
grep        parted       udevinfo
growisofs   pccardctl    udevstart
grub        ping         umount
gunzip      pktsetup     uuidgen
halt        poweroff     vconfig
hexdump     ps           vi
hotplug     raidautorun  zcat
```

6.8.5. MD デバイスと論理ボリュームの復元

MD デバイスとも呼ばれる Linux ソフトウェア RAID デバイスまたは論理ボリューム マネージャ (LVM)によって作成されたデバイスを復元するには、復元を開始する前に、対応するボリューム構造を作成する必要があります。

ボリューム構造は、以下のいずれかの方法で作成することができます。

- Linux ベースのブータブル メディアで提供されるスクリプトを使用する(「スクリプトを使用した論理ボリューム構造の作成」『ページ参照 309』をご参照ください)。この手順は、MD デバイスに対しては機能しません。
- **lvm** ユーティリティを使用する(「手動によるボリューム構造の作成」『ページ参照 310』をご参照ください)。

6.8.5.1. スクリプトを使用した論理ボリューム構造の作成

論理ボリューム構造を **/etc/Acronis** ディレクトリに保存し(「LVM ボリュームのバックアップ (Linux)」『ページ参照 52』をご参照ください)、このディレクトリが存在するボリュームがアーカイブに含まれるとします。論理ボリューム構造を作成するには、**restoreraids.sh** スクリプトを使用します。

1. Linux ベースのブータブル メディアからコンピュータを起動します。
2. **[Acronis ブータブル エージェント]** をクリックします。次に、**[管理コンソールの実行]** をクリックします。
3. ツール バーの **[アクション]** をクリックし、**[シェルの開始]** をクリックします。または、[Ctrl+Alt+F2] キーを押します。
4. アーカイブの完全ファイル名を指定して、**restoreraids.sh** スクリプトを実行します。たとえば、次のように指定します。

```
/bin/restoreraids.sh
smb://server/backups/linux_machine_2010_01_02_12_00_00_123D.tib
```

5. ［Ctrl+Alt+F1］キーを押すか、コマンド「**/bin/product**」を実行して管理コンソールに戻ります。
6. **［復元］**をクリックし、アーカイブのパスとその他の必要なパラメータを指定して、**［OK］**をクリックします。

スクリプトによってボリューム構造が作成できない(またはスクリプトがアーカイブ内に存在しない)場合、手動で構造を作成します。

6.8.5.2. 手動によるボリューム構造の作成

Linux ベースのブータブル メディアを使用して MD デバイスと論理ボリュームを復元するときの一般的な手順と、その復元の例を次に示します。Linux でも同様の手順を使用できます。

MD デバイスと論理ボリュームを復元する手順は、次のとおりです。

1. Linux ベースのブータブル メディアからコンピュータを起動します。
2. **［Acronis ブータブル エージェント］**をクリックします。次に、**［管理コンソールの実行］**をクリックします。
3. ツール バーの **［アクション］**をクリックし、**［シェルの開始］**をクリックします。または、［Ctrl+Alt+F2］キーを押します。
4. 必要に応じて、**trueimagecmd** ユーティリティを使用して、アーカイブに保存されているボリュームの構造を調べます。また、**trueimagemnt** ユーティリティを使用して、これらのボリュームの 1 つ以上を通常のボリュームと同様にマウントすることもできます(この後の「バックアップ ボリュームのマウント」をご参照ください)。
5. **mdadm** ユーティリティ(MD デバイスの場合)、**lvm** ユーティリティ(論理ボリュームの場合)、またはその両方を使用して、アーカイブ内の構造に従ってボリューム構造を作成します。

   ***注意:** 通常、Linux で使用可能な **pvcreate** や **vgcreate** などの論理ボリューム マネージャ ユーティリティはブータブル メディア環境に含まれていないため、**lvm pvcreate**、**lvm vgcreate** などの対応する引数付きで **lvm** ユーティリティを使用する必要があります。*

6. 以前に **trueimagemnt** ユーティリティを使用してバックアップをマウントしてある場合は、もう一度このユーティリティを使用してバックアップのマウントを解除します(この後の「バックアップ ボリュームのマウント」をご参照ください)。
7. ［Ctrl+Alt+F1］キーを押すか、コマンド「**/bin/product**」を実行して管理コンソールに戻ります。

   (この時点でコンピュータを再起動しないでください。再起動すると、ボリューム構造をもう一度作成しなければならなくなります。)
8. **［復元］**をクリックし、アーカイブのパスとその他の必要なパラメータを指定して、**［OK］**をクリックします。

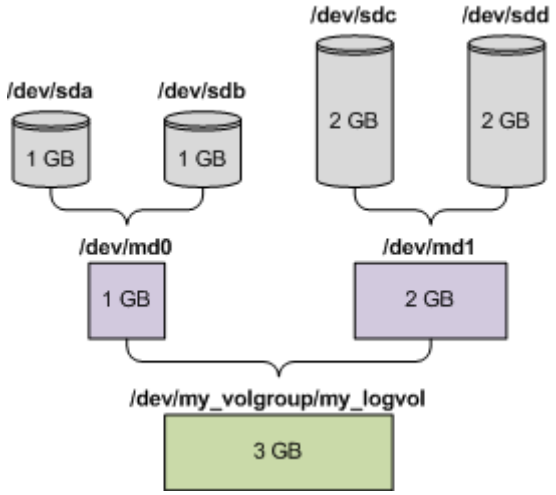
***注意:** リモートから Acronis Backup & Recovery 10 ブータブル エージェントに接続している場合はコマンド シェルを使用できないため、この手順は実行できません。*

例

以前に、次のディスク構成のコンピュータのディスク バックアップを実行したことがあるとします。

- コンピュータに 2 台の 1GB SCSI ハード ディスクと 2 台の 2GB SCSI ハード ディスクがあり、それぞれ **/dev/sda**、**/dev/sdb**、**/dev/sdc**、および **/dev/sdd** にマウントされている。
- 最初と 2 番目の 1 組のハード ディスクは、共に RAID-1 構成の 2 台の MD デバイスとして設定され、それぞれ **/dev/md0** と **/dev/md1** にマウントされている。
- 論理ボリュームは 2 台の MD デバイスに基づいており、**/dev/my_volgroup/my_logvol** にマウントされている。

この設定を次の図に示します。



次の手順を実行して、このアーカイブからデータを復元します。

手順 1: ボリューム構造の作成

1. Linux ベースのブータブル メディアからコンピュータを起動します。
2. 管理コンソールで、［Ctrl+Alt+F2］キーを押します。
3. 次のコマンドを実行して、MD デバイスを作成します。

```
mdadm --create /dev/md0 --level=1 --raid-devices=2 /dev/sd[ab]
mdadm --create /dev/md1 --level=1 --raid-devices=2 /dev/sd[cd]
```

4. 次のコマンドを実行して、論理ボリューム グループを作成します。

> ***注意: pvcreate** コマンドを実行すると、**/dev/md0** および **/dev/md1** デバイス上のデータがすべて消去されます。*

```
lvm pvcreate /dev/md0 /dev/md1
lvm vgcreate my_volgroup /dev/md0 /dev/md1
lvm vgdisplay
```

lvm vgdisplay コマンドの出力には、次に示すような行が含まれています。

```
--- Volume group ---
VG Name     my_volgroup
...
VG Access   read/write
VG Status   resizable
...
VG Size     1.99 GB
...
VG UUID     0qoQ4l-Vk7W-yDG3-uF1l-Q2AL-C0z0-vMeACu
```

5. 次のコマンドを実行して論理ボリュームを作成します。**-L** パラメータには、**VG Size** に示されたサイズを指定します。

```
lvm lvcreate -L1.99G --name my_logvol my_volgroup
```

6. 次のコマンドを実行して、ボリューム グループを有効にします。

```
lvm vgchange -a y my_volgroup
```

7. ［Ctrl+Alt+F1］キーを押して、管理コンソールに戻ります。

手順 2: 復元の開始

1. 管理コンソールで、**［復元］**をクリックします。
2. **［アーカイブ］**で、**［変更］**をクリックし、アーカイブの名前を指定します。
3. **［バックアップ］**で、**［変更］**をクリックし、データの復元に使用するバックアップを選択します。
4. **［データの種類］**で、**［ボリューム］**を選択します。
5. **［復元する項目］**で、**［my_volgroup-my_logvol］**の横のチェックボックスをオンにします。
6. **［復元先］**の下の**［変更］**をクリックし、手順 1 で作成した論理ボリュームを選択します。ボタンをクリックし、ディスクの一覧を展開します。
7. **［OK］**をクリックして復元を開始します。

ブータブル メディア環境で使用できるコマンドとユーティリティの一覧については、「Linux ベースのブータブル メディアで使用できるコマンドとユーティリティの一覧『ページ参照 308』」をご参照ください。**trueimagecmd** ユーティリティと **trueimagemnt** ユーティリティの詳細な説明については、Acronis Backup & Recovery 10 コマンド ライン リファレンスをご参照ください。

バックアップ ボリュームのマウント

たとえば、復元を開始する前に、ボリューム内のいくつかのファイルを確認するために、ディスク バックアップに保存されているボリュームのマウントが必要になることがあります。

バックアップボリュームをマウントする手順は、次のとおりです。

1. **--list** コマンドを使用して、バックアップに保存されているボリュームの一覧を表示します。たとえば、次のように表示されます。

   ```
   trueimagecmd --list --filename smb://server/backups/linux_machine.tib
   ```

   出力には、次に示すような行が含まれています。

   ```
   Num  Idx Partition Flags Start Size      Type
   ---- --- --------- ----- ----- --------- ------
   Disk 1:
   Table           0               Table
   Disk 2:
   Table           0               Table
   ...
   Dynamic & GPT Volumes:
   DYN1 4   my_volgroup-my_logvol 12533760  Ext2
   ```

   次の手順では、**Idx** 列に示されるボリュームのインデックスが必要になります。

2. **--mount** コマンドを使用して、**-i** パラメータにボリュームのインデックスを指定します。たとえば、次のように表示されます。

   ```
   trueimagemnt --mount /mnt --filename smb://server/backups/linux_machine.tib -i 4
   ```

   このコマンドで、バックアップのインデックスが 4 の論理ボリューム DYN1 が、マウント ポイント /mnt にマウントされます。

バックアップボリュームのマウントを解除する手順は、次のとおりです。

- **--unmount** コマンドを使用して、ボリュームのマウント ポイントをパラメータとして指定します。たとえば、次のように表示されます。

  ```
  trueimagemnt --unmount /mnt
  ```

6.8.6. Acronis PXE サーバー

Acronis PXE サーバーを使用すると、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コンピュータ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 ビルダを使用して Acronis PXE サーバー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(管理コンソールから起動するか、**[ツール]→[ブータブル メディアの作成]**を選択して起動するか、別のコンポーネントとして起動)、「ブータブル メディア ビルダ『ページ参照 300』」セクションで説明されている詳細な手順に従います。

Acronis PXE サーバーから複数のコンピュータを起動する方法は、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。DHCP が存在しない場合は、あらかじめ各コンピュータのブータブル エージェントを個別に設定し、PXE サーバーにアップロードする必要があります。

6.8.6.1. Acronis PXE サーバーのインストール

Acronis PXE サーバーをインストールする手順は、次のとおりです。

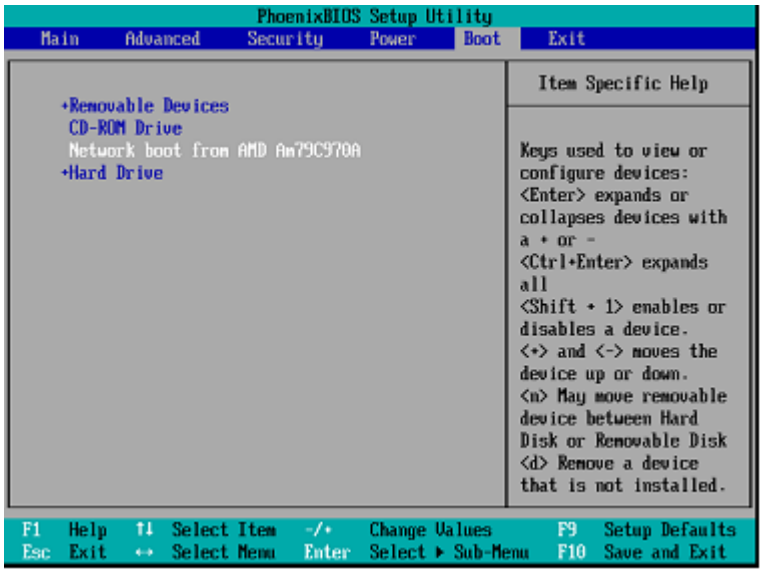
1. Acronis Backup & Recovery 10 セットアップ ファイルを実行します。
2. **[集中管理用のコンポーネント]**の一覧から Acronis PXE サーバーを選択します。
3. 画面の指示に従ってください。

Acronis PXE サーバーは、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。Acronis PXE サーバーは、他の Windows サービスと同じ方法で停止および起動できます。

6.8.6.2. 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。

6.8.6.3. 同じサーバー上の PXE と DHCP

Acronis PXE サーバーと DHCP サーバーが同じコンピュータにインストールされている場合は、文字列値「PXEClient」を使用してオプション 60 に対する「クライアント識別子」を DHCP サーバーに追加します。この操作は、次の手順で実行できます。

```
C:¥WINDOWS¥system32>netsh
netsh>dhcp
netsh>dhcp>server ¥¥<サーバー名> または〈IP アドレス〉
netsh dhcp>add optiondef 60 PXEClient STRING 0 comment=”Option added for PXE support”
netsh dhcp>set optionvalue 60 STRING PXEClient
```

6.8.6.4. サブネットをまたがる操作

Acronis PXE サーバーが(ルーターを越えて)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ルーターを設定します。PXE サーバーの IP アドレスは、IP ヘルパー機能を使用して、DHCP サーバーのアドレスと同じようにインターフェイスごとに設定されます。詳細については、次をご参照ください。
http://support.microsoft.com/default.aspx/kb/257579

6.9. ディスクの管理

Acronis Disk Director Lite は、Acronis Backup & Recovery 10 ソフトウェアによって保存されたボリューム イメージを復元するために、コンピュータのディスクまたはボリューム構成を準備するツールです。

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に、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。このような状況で Acronis Disk Director Lite を使用すると、ユーザーは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の構造を変更して復元できます。

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 ボリューム、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慎重に行い、起動処理やハード ディスク データ ストレージで考えられる問題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、不注意によるコンピュータのオフ、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の損失につながる可能性があります。

Windows XP および Windows 2000 のダイナミック ディスクのボリュームに対するすべての操作では、管理者権限のあるアカウントで Acronis Managed Machine Service を実行する必要があります。

必要な予防措置『ページ参照 316』をすべて行って、考えられるデータの損失を回避してください。

6.9.1. 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造の損傷やデータの損失を回避するため、必要な予防措置をすべて行い、次の簡単なルールに従ってください。

1. 作成または管理するボリュームがあるディスクのイメージを作成します。最も重要なデータを別のハード ディスクまたは CD 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。

   Acronis Backup & Recovery 10 は、非常に効率のよい包括的なデータのバックアップおよび復元ソリューションです。作成されるデータまたはディスクのバックアップ コピーは圧縮されたアーカイブ ファイルに保存され、問題の発生時に復元できます。

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。これらのプログラムを終了してから Acronis Disk Director Lite を実行してください。

これらの簡単な予防措置により、偶発的なデータの損失を防ぐことができます。

6.9.2. Acronis Disk Director Lite の実行

Acronis Disk Director Lite は、Windows で実行することも、ブータブル メディアから起動することもできます。

Windows での Acronis Disk Director Lite の実行

Acronis Backup & Recovery 10 管理コンソールを実行し、管理対象のコンピュータに接続すると、［**ディスクの管理**］ビューがコンソールの［**ナビゲーション**］ツリーで使用できるようになります。ここから、Acronis Disk Director Lite を起動できます。

ブータブル メディアからの Acronis Disk Director Lite の実行

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 以外のコンピュータでも、Acronis Disk Director Lite を実行できます。この場合、Acronis ブータブル メディア ビルダで作成したブータブル メディア『ページ参照 423』からコンピュータを起動し、管理コンソールを実行してから、［**ディスクの管理**］をクリックします。

6.9.3. 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。

Windows オペレーティング システムが異なる場合、ボリュームのドライブ文字が異なることがあります。たとえば、ボリューム E: は、同じコンピュータにインストールされている別の Windows オペレーティング システムを起動すると、D: または L: と表示される場合があります (また、コンピュータにインストールされているすべての Windows OS でこのボリュームが同じドライブ文字 E: になる可能性もあります)。

ある Windows オペレーティング システム上に作成されたダイナミック ディスクは、別の Windows オペレーティング システムでは**形式の異なるディスク**と見なされるか、そのオペレーティング システムではサポートされない場合があります。

このようなコンピュータでディスク管理操作を実行する必要がある場合は、ディスク レイアウトを表示するオペレーティング システムを指定してからディスク管理操作を実行します。

現在選択されているオペレーティング システムの名前は、コンソール ツールバーの［**現在のディスク レイアウト:**］の後に表示されます。［**オペレーティング システムの選択**］ウィンドウで OS 名をクリックし、別のオペレーティング システムを選択します。ブータブル メディアでは、このウィンドウは［**ディスクの管理**］をクリックした後に表示されます。ディスク レイアウトは、選択したオペレーティング システムに従って表示されます。

6.9.4. ［ディスクの管理］ビュー

Acronis Disk Director Lite は、コンソールの［**ディスクの管理**］ビューから操作します。

ビューの上部には、データの並べ替えと列のカスタマイズが可能なディスクおよびボリューム テーブルと、ツールバーが表示されます。テーブルには、ディスク番号のほか、各ボリュームに割り当てられたドライブ文字、ラベル、種類、容量、空き領域のサイズ、使用領域のサイズ、ファイル システム、ステータスが表示されます。ツールバーは、保留中の操作『ページ参照 334』を対象とした［**元に戻す**］、［**やり直す**］、および［**コミット**］の各操作を実行するアイコンから構成されます。

ビューの下部にあるグラフィック パネルにも、すべてのディスクとそのボリュームが、基本データ(ラベル、ドライブ文字、サイズ、ステータス、種類、ファイル システム)が記された四角形として、図表形式で表されます。

ビューのどちらの部分にも、ボリューム作成に利用可能な未割り当てディスク領域がすべて表示されます。

操作の開始

すべての操作は次の方法で開始できます。

- ボリュームまたはディスクのコンテキスト メニューから(テーブルとグラフィック パネルの両方に配置)
- コンソールの［**ディスクの管理**］メニューから
- ［**アクションとツール**］ペインの［**操作**］バーから

*コンテキスト メニュー、［**ディスクの管理**］メニュー、［**操作**］バーで利用できる操作の一覧は、選択したボリュームまたはディスクの種類によって異なることに注意してください。未割り当て領域にも同じことが当てはまります。*

操作結果の表示

計画したすべてのディスクまたはボリューム操作の結果は、コンソールの［**ディスクの管理**］ビューにすぐに表示されます。たとえば、ボリュームを作成すると、すぐにテーブルに表示され、ビューの下部にも図表形式で表示されます。ボリュームのドライブ文字やラベルの変更など、ボリュームに何らかの変更があった場合も、すぐにビューに表示されます。

6.9.5. ディスク操作

Acronis Disk Director Lite には、ディスクに対して実行できる次の操作が含まれています。

- ディスクの初期化『ページ参照 319』- 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 ディスクのクローン作成『ページ参照 320』- ソースのベーシック MBR ディスクからターゲットに全データを転送します。
- ディスク変換: MBR から GPT『ページ参照 323』- 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『ページ参照 324』- 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『ページ参照 324』- 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『ページ参照 325』- 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。

完全版の Acronis Disk Director には、ディスクでの作業に使用するツールとユーティリティが多数用意されています。

Acronis Disk Director Lite は、ターゲット ディスクに排他的にアクセスする必要があります。つまり、このアプリケーションがアクセスしている間、他のディスク管理ユーティリティ(Windows のディスクの管理ユーティリティなど)はターゲット ボリュームにアクセスできません。ディスクをブロックできないことを示すメッセージが表示された場合は、このディスクを使用しているディスク管理アプリケーションを閉じてから、Acronis Disk Director Lite を再度起動します。ディスクを使用しているアプリケーションがわからない場合は、すべてのアプリケーションを終了してください。

6.9.5.1. ディスクの初期化

新しいディスクをコンピュータに追加すると、Acronis Disk Director Lite は構成変更を認識し、追加されたディスクをスキャンして、ディスクとボリュームの一覧に表示します。ディスクがまだ初期化されていない場合、またはファイル システムが認識できない場合、そのディスクにはプログラムをインストールすることもファイルを保存することもできません。

Acronis Disk Director Lite は、ディスクがシステムで使用できないこと、および初期化する必要があることを検出します。［**ディスクの管理**］ビューは、新たに検出したハードウェアを、淡色表示のアイコンを持つ灰色のブロックで表示し、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必要がある場合の手順は、次のとおりです。

1. 初期化するディスクを選択します。
2. 選択したボリュームを右クリックして、コンテキスト メニューで［**初期化**］をクリックします。ディスク番号、容量、および状態などの基本ハードウェア詳細を提供する［**ディスクの初期化**］ウィンドウが表示されるため、可能な処理を選択するのに役立ちます。
3. このウィンドウでは、ディスク パーティション 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)を設定できます。
4. ［**OK**］をクリックすると、ディスクの初期化が保留中の操作に追加されます

(追加した操作を完了するには、コミット『ページ参照 334』する必要があります。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)。

ディスク設定を変更するには、標準の Acronis Disk Director Lite ディスク ツールを使用して後から変更できます。

新しいディスクの状態は、コンソールの［**ディスクの管理**］ビューに図表形式で直ちに表示されます。今度はディスクのアイコンが灰色ではなく緑色で表示され、必要なディスク情報が表示されます。ただし、ディスク ブロックは灰色のままです。これは、初期化後、すべてのディスク領域はまだ未割り当てで、プログラムのインストールやファイルの保存には使用できないためです。使用できるようにするには、通常どおり［**ボリュームの作成**］操作に進みます。

6.9.5.2. ベーシック ディスクのクローン作成

場合によっては、すべてのディスク データを新しいディスクに転送する必要があります。これに該当するのは、システム ボリュームを拡張する場合や、新しいシステム レイアウトを開始する場合、ハードウェア障害が原因でディスク データを退避する場合などです。いずれの場合でも、すべてのソース ディスク データを現状とまったく同じ状態でターゲット ディスクに転送する必要があるために、［**ベーシック ディスクのクローン作成**］操作を行います。

Acronis Disk Director Lite では、ベーシック MBR ディスクに対してのみ操作を実行できます。

［**ベーシック ディスクのクローン作成**］操作を計画する手順は、次のとおりです。

1. クローンを作成するディスクを選択します。
2. クローン作成操作のターゲットとなるディスクを選択します。
3. クローン作成方法を選択し、詳細オプションを指定します。

新しいボリューム構造は、［**ディスクの管理**］ビューに図表形式で直ちに表示されます。

システム ディスクのクローンを作成する前に、Acronis リカバリ マネージャ『ページ参照 413』(ASRM) が有効になっている場合は無効にすることをお勧めします。無効にしないと、クローン作成されたオペレーティング システムが起動しない場合があります。クローン作成が完了した後で、ASRM を再度有効にすることができます。無効にできない場合は、ディスクのクローンを作成する際に、 ***［現状のまま］*** *を選択します。*

ソース ディスクとターゲット ディスクの選択

ディスクのパーティション一覧が表示され、ソース ディスクを選択するように求められます。そのディスクからデータが別のディスクに転送されます。

次の手順では、クローン作成操作のターゲットとなるディスクを選択します。ソース ディスクのデータを失うことなくすべて保持できる十分なサイズのあるディスクだけが選択できます。

ターゲットとして選択されたディスクにデータがある場合、「**警告: 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。**」という警告がユーザーに表示されます。これは、選択したターゲット ディスク上に現在保存されているデータはすべて失われ、回復できないことを意味します。

クローン作成方法と詳細オプション

[ベーシック ディスクのクローン作成]操作では、通常、ソース ディスクからの情報がターゲットに「**現状のまま**」転送されます。したがって、転送先のディスクが同じサイズの場合やさらに大きい場合でも、すべての情報を、ソースに保存されているとおりに転送できます。

ただし、利用できるハードウェアが多岐に及ぶため、通常、ターゲット ディスクとソース ディスクのサイズは異なります。ターゲット ディスクのほうが大きい場合、**[ボリュームに合わせてサイズを変更する]**オプションを選択して、ターゲット ディスクに未割り当て領域が残らないように、ソース ディスク ボリュームのサイズを変更することをお勧めします。**[ベーシック ディスクのクローン作成]**を「現状のまま」行うオプションもありますが、デフォルトのクローン作成方法は、未割り当ての領域が**ターゲット** ディスクに残らないように、すべての**ソース** ディスク ボリュームを比例的に拡大するオプションが選択されています。

ターゲット ディスクが小さい場合、クローン作成の**[現状のまま]**オプションは利用できず、**ソース** ディスク ボリュームのサイズを比例的に変更する必要があります。プログラムによって、**ターゲット** ディスクが分析され、**ソース** ディスクのデータを失うことなくすべて保持できるだけ十分なサイズであるかどうかが検証されます。サイズを比例的に変更して、データの損失なく**ソース** ディスク ボリュームの転送が可能であれば、ユーザーは操作を続行できます。ボリュームのサイズを比例的に変更しても、サイズ制限のために、すべての**ソース** ディスク データを**ターゲット** ディスクに安全に転送できない場合は、**[ベーシック ディスクのクローン作成]**操作を行うことはできず、ユーザーは操作を続行できません。

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は、**[詳細] オプション**に注意してください。

[完了]をクリックすると、ディスクのクローン作成が保留中の操作に追加されます

(追加した操作を完了するには、コミット『ページ参照 334』する必要があります。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)。

詳細オプションの使用

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 システムが起動できるように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 シグネ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 シグネチャを持つと正しく機能できません。

コンピュータにシステム 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 シグネチャが生成され、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、そのディスクに対するパスはすべて無効となり、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 ボリュームでもシステムが起動できるように保つには、次の 2 つの方法があります。

1. NT シグネチャをコピーする – 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 シグネチャをターゲットディスクに設定します。
2. NT シグネチャを保持する – 従来のターゲット ディスク シグネチャは変更せず、そのシグネチャに応じてオペレーティング システムを更新します。

NT シグネチャをコピーする必要がある場合の手順は、次のとおりです。

1. **[NT シグネチャのコピー]** 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、コンピュータ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。」 自動的に **[クローンの作成処理後にコンピュータの電源を切る]** チェック ボックスがオンになり、無効になります。
2. **[完了]** をクリックすると、保留中の操作に追加されます。
3. ツールバー上で **[コミット]** をクリックし、**[保留中の操作]** ウィンドウで **[実行]** をクリックします。
4. タスクが完了するまで待機します。
5. コンピュータの電源が切れるまで待機します。
6. 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コンピュータから切断します。
7. コンピュータを起動します。

NT シグネチャを残す必要がある場合の手順は、次のとおりです。

1. 必要に応じて、**[NT シグネチャのコピー]** チェック ボックスをオフにします。
2. 必要に応じて、**[クローンの作成処理後にコンピュータの電源を切る]** チェック ボックスをオフにします。
3. **[完了]** をクリックすると、保留中の操作に追加されます。
4. ツールバー上で **[コミット]** をクリックし、**[保留中の操作]** ウィンドウで **[実行]** をクリックします。
5. タスクが完了するまで待機します。

6.9.5.3. ディスク変換: MBR から GPT

次のように、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必要がある場合があります。

- 1 つのディスクに 5 つ以上のプライマリ ボリュームが必要な場合。
- データの損傷に備えて、ディスクの信頼性を高める必要がある場合。

ベーシック MBR ディスクをベーシック GPT に変換する必要がある場合の手順は、次のとおりです。

1. GPT に変換するベーシック MBR ディスクを選択します。
2. 選択したボリュームを右クリックして、コンテキスト メニューで **[GPT への変換]** をクリックします。
   MBR を GPT に変換しようとしていることを示す警告ウィンドウが表示されます。
3. **[OK]** をクリックすると、MBR から GPT へのディスク変換が保留中の操作に追加されます。

(追加した操作を完了するには、コミット『ページ参照 334』する必要があります。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。)

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されます。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。

この操作を元に戻すことはできません。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。

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、ディスクの MBR へ逆変換は、同じメニュー項目にある **[MBR への変換]** を使用して行うことができます。

ダイナミック ディスク変換: MBR から GPT

Acronis Disk Director Lite 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、プログラムで次の複数回の変換を実行することにより、結果的にこの変換を行うことができます。

1. MBR ディスク変換: ダイナミックからベーシック『ページ参照 325』- **[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: MBR から GPT - **[GPT への変換]** 操作を使用します。
3. GPT ディスク変換: ベーシックからダイナミック『ページ参照 324』- **[ダイナミックへの変換]** 操作を使用します。

6.9.5.4. 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、［**MBR への変換**］の操作を使用して行うことができます。

GPT ディスクを MBR に変換する必要がある場合の手順は、次のとおりです。

1. MBR に変換する GPT ディスクを選択します。
2. 選択したボリュームを右クリックして、コンテキスト メニューで［**MBR への変換**］をクリックします。

   GPT を MBR に変換しようとしていることを示す警告ウィンドウが表示されます。

   選択したディスクを GPT から MBR に変換すると、その際にシステム上で発生する可能性のあることについて説明が表示されます。たとえば、このような変換によってシステムがディスクにアクセスできなくなると、オペレーティング システムがこのような変換後にはディスクの読み込みを停止する、または選択した GPT ディスク上の一部のボリュームが MBR でアクセスできなくなる(たとえば、ディスクの先頭から 2TB を超えた位置に配置されたボリューム)などの障害についてここで警告されます。

   変換する GPT ディスクに属するボリュームは、操作の後は論理ボリュームになり、元に戻すことはできません。

3. ［**OK**］をクリックすると、GPT から MBR へのディスク変換が保留中の操作に追加されます。

(追加した操作を完了するには、コミット『ページ参照 334』する必要があります。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。)

6.9.5.5. ディスク変換: ベーシックからダイナミック

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のは、次のような場合があります。

- 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予定の場合。
- 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必要がある場合の手順は、次のとおりです。

1. ダイナミック ディスクに変換するベーシック ディスクを選択します。
2. 選択したボリュームを右クリックして、コンテキスト メニューで［**ダイナミックへの変換**］をクリックします。ベーシック ディスクがダイナミック ディスクに変換されることについて最終的な警告が表示されます。
3. この警告ウィンドウで［**OK**］をクリックすると、すぐに変換が実行され、必要に応じてコンピュータが再起動されます。

   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 ディスクへの変換中、ベーシック ディスクがいっぱいになり、ボリュームのサイズを自動的に縮小できない場合、ベーシック ディスクからダイナミック ディスクへの変換操作は失敗します。

ダイナミック ディスクをサポートしないコンピュータ上で OS の使用を開始する場合などのため、ダイナミック ディスクをベーシック ディスクに戻すことにした場合、同じメニュー項目にある［**ベーシックへの変換**］の操作を使用してディスクを変換できます。

システム ディスク変換

Acronis Disk Director Lite では、次の場合、ベーシック ディスクからダイナミック ディスクへの変換後にオペレーティング システムを再起動する必要はありません。

1. Windows 2008/Vista オペレーティング システムが 1 つだけディスクにインストールされている場合。
2. コンピュータがこのオペレーティング システムを実行する場合。

システム ボリュームを構成するディスクをベーシック ディスクからダイナミック ディスクに変換するには一定の時間がかかります。不注意によるコンピュータの電源オフ、誤ってリセット ボタンを押した場合などにより処理中に停電した場合、起動できなくな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**が起動できなくなることはありません。

6.9.5.6. ディスク変換: ダイナミックからベーシック

たとえば、ダイナミック ディスクをサポートしないコンピュータ上で OS の使用を開始する場合などのため、ダイナミック ディスクをベーシック ディスクに戻す必要がある場合があります。

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必要がある場合の手順は、次のとおりです。

1. ベーシック ディスクに変換するダイナミック ディスクを選択します。
2. 選択したボリュームを右クリックして、コンテキスト メニューで［**ベーシックへの変換**］をクリックします。ダイナミック ディスクがベーシック ディスクに変換されることについて最終的な警告が表示されます。

   選択したディスクをダイナミック ディスクからベーシック ディスクに変換した場合にシステムに発生する変化に関する説明が表示されます。たとえば、このような変換によってシステムがディスクにアクセスできなくなる場合、オペレーティング システムがこのような変換後、ディスクの読み込みを停止したり、またはベーシック ディスクに変換するディスクに、ダイナミック ディスクでのみサポートされる種類のボリュームが含まれる場合 (シンプル ボリューム以外のすべての種類のボリューム)、変換に起因するデータへの損傷の可能性があることについて、ここで警告が表示されます。

   この操作は、スパン、ストライプ、または RAID-5 のボリュームを含むダイナミック ディスクには使用できないことに注意してください。

3. この警告ウィンドウで［**OK**］をクリックすると、変換がすぐに実行されます。

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)。

システム ディスク変換

Acronis Disk Director Lite では、次の場合、ダイナミック ディスクからベーシック ディスクへの変換後にオペレーティング システムを再起動する必要はありません。

1. Windows 2008/Vista オペレーティング システムが 1 つだけディスクにインストールされている場合。
2. コンピュータがこのオペレーティング システムを実行する場合。

システム ボリュームを構成するディスクをダイナミック ディスクからベーシック ディスクに変換するには一定の時間がかかります。不注意によるコンピュータの電源オフ、誤ってリセット ボタンを押した場合などにより処理中に停電した場合、起動できなくな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**だったシステムを起動可能

6.9.6. ボリューム操作

Acronis Disk Director Lite では、ボリュームに対して次の操作を実行できます。

- ［ボリュームの作成］『ページ参照 327』- ［ボリュームの作成］ウィザードを使用して新しいボリュームを作成します。
- ［ボリュームの削除］『ページ参照 331』- 選択したボリュームを削除します。
- ［アクティブに設定］『ページ参照 332』- インストールされている OS でコンピュータ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］『ページ参照 332』- 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］『ページ参照 333』- 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］『ページ参照 334』- 必要なファイル システムにボリュームをフォーマットします。

完全版の Acronis Disk Director には、ボリュームでの作業に使用するツールとユーティリティが多数用意されています。

Acronis Disk Director Lite は、ターゲット ボリュームに排他的にアクセスする必要があります。つまり、このアプリケーションがアクセスしている間、他のディスク管理ユーティリティ(Windows のディスクの管理ユーティリティなど)はターゲット ボリュームにアクセスできません。ディスクをブロックできないことを示すメッセージが表示された場合は、このボリュームを使用しているディスク管理アプリケーションを閉じてから、Acronis Disk Director Lite を再度起動します。そのボリュームを使用しているアプリケーションが何かわからない場合は、すべてのアプリケーションを終了してください。

6.9.6.1. 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コンピュータに追加する。

Acronis Disk Director Lite でボリュームを作成するツールは、**ボリューム作成ウィザード**です。

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 サイズの制限を克服できます。ただし、1 つでもディスクに障害が生じると、すべてのデータが失われ、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 ボリュームには、信頼性の向上または I/O 速度の改善におけるメリットはありません。

ストライプ ボリューム

ボリューム内の各ディスクにわたって書き込まれた、均一サイズのデータのストライプから構成されるボリュームで、RAID 0 とも呼ばれます。つまり、ストライプ ボリュームを作成するには、複数の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、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 アーキテクチャの明白な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。また、パリティは常にデータ自体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。

ボリューム作成ウィザード

[ボリューム作成] ウィザードには、システムとアクティブを含むすべての種類のボリュームの作成、ファイル システムの選択、ラベルの設定、ドライブ文字の割り当て機能、およびその他のディスク管理機能が用意されています。

ウィザードのページでは、段階的に進めながら操作パラメータを入力したり、必要に応じて前のステップに戻り、以前に選択したオプションを変更することができます。選択を簡単に行えるように、各パラメータには詳細な説明が付けられています。

ボリュームを作成する場合の手順は、次のとおりです。

[ウィザード] バーで **[ボリュームの作成]** を選択するか、または、未割り当て領域を右クリックして表示されるコンテキスト メニューから **[ボリュームの作成]** を選択して、**[ボリュームの作成]** ウィザードを実行します。

作成するボリュームの種類の選択

手順の最初で、作成するボリュームの種類を指定する必要があります。次のボリュームの種類を利用できます。

- ベーシック
- シンプル/スパン
- ストライプ
- ミラー
- RAID-5

使用可能な各ボリューム アーキテクチャの利点と制限を適切に理解できるように、すべての種類のボリュームの簡単な説明が表示されます。

*コンピュータにインストールされている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、該当する警告が表示されます。この場合、**[次へ]** ボタンが無効になり、新しいボリュームの作成に進むには、別の種類のボリュームを選択する必要があります。*

[次へ] ボタンをクリックすると、ターゲット ディスクの選択『ページ参照 329』を行う次のウィザード ページに進みます。

ターゲット ディスクの選択

次のウィザード ページでは、ボリューム作成に使用する領域を含むディスクを選択するように求められます。

ベーシック ボリュームを作成する手順は、次のとおりです。

- ターゲット ディスクを選択し、ベーシック ボリュームを作成する未割り当て領域を指定します。

シンプル/スパン ボリュームを作成する手順は、次のとおりです。

- ボリュームを作成する 1 つ以上のターゲット ディスクを選択します。

ミラー ボリュームを作成する手順は、次のとおりです。

- ボリュームを作成する 2 つのディスクを選択します。

ストライプ ボリュームを作成する手順は、次のとおりです。

- ボリュームを作成するターゲット ディスクを 2 つ以上選択します。

RAID-5 ボリュームを作成する手順は、次のとおりです。

- ボリュームを作成するターゲット ディスクを 3 つ選択します。

ディスクを選択すると、選択したディスクの未割り当て領域のサイズと、前に選択したボリュームの種類の要件に従って、作成されるボリュームの最大サイズが計算されます。

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。

必要に応じて、作成するボリュームの種類に対して必要な数のディスクを選択に追加するように求められます。

[戻る] ボタンをクリックすると、作成するボリュームの種類の選択『ページ参照 329』を行う、前のページに戻ります。

[次へ] ボタンをクリックすると、ボリューム サイズの設定『ページ参照 330』を行う次のページに進みます。

ボリューム サイズの設定

ウィザードの 3 ページでは、これまで行った選択に従って、作成するボリュームのサイズを定義できます。スライダを使用して最小値と最大値の間で必要なサイズを選択するか、専用のウィンドウに必要な値を入力するか、スピンボックスをクリックして最小値と最大値の間の値を選択するか、ディスクの画像の境界をカーソールでドラッグします。

最大値には通常、最大限の未割り当て領域が含まれます。ただし、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)。

ベーシック ボリュームでは、ディスク上に未割り当て領域が残っている場合、ディスクでの新しいボリュームの位置も選択できます。

[戻る] ボタンをクリックすると、ターゲット ディスクの選択『ページ参照 329』を行う、前のページに戻ります。

[次へ] ボタンをクリックすると、ボリューム オプションの設定『ページ参照 330』を行う次のページに進みます。

ボリューム オプションの設定

次のウィザード ページでは、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。ここでは、**[ファイル システム]** と **[クラスタ サイズ]** も指定します。

ファイル システムを、FAT16(ボリューム サイズが 2GB 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 2TB を超えて設定されている場合は無効)、NTFS または **[未フォーマット]** から選択するように求められます。

クラスタ サイズの設定では、各ファイル システムの現在の容量内で任意の数値を選択できます。選択したファイル システムのボリュームに最適なクラスタ サイズが提示されることに注意してください。

システム ボリュームに設定できるベーシック ボリュームを作成している場合、このページの内容は異なります。その場合、ボリュームの **[種類]** を **[プライマリ]** (**[アクティブ]** かつ **[プライマリ]**)または **[論理]** から選択できます。

通常は、ボリュームにオペレーティング システムをインストールできる［**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コンピュータの起動時に、起動させる場合は、［**アクティブ**］(デフォルト)を選択します。［**プライマリ**］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。

*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。すで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。ベーシック ディスクのままでは、［**アクティブ**］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**］しか選択できません。このボリュームに OS をインストールしても起動できないことを示す警告メッセージが表示されます。*

*新しいボリューム ラベルを設定するときに、現在インストールされているオペレーティング システムでサポートされない文字を使用した場合は、警告が表示され、［**次へ**］ボタンが無効になります。新しいボリュームの作成を続行するには、ラベルを変更する必要があります。*

［**戻る**］ボタンをクリックすると、ボリューム サイズの設定『ページ参照 330』を行う、前のページに戻ります。

［**完了**］ボタンをクリックすると、操作の計画が完了します。

計画した操作を実行するには、ツールバーの［**コミット**］をクリックし、［**保留中の操作**］ウィンドウで［**実行**］をクリックします。

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 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。

6.9.6.2. ボリュームの削除

このバージョンの Acronis Disk Director Lite は、主に、以前に保存したボリューム イメージを復元できるようにベアメタル システムを準備するツールであるため、機能が制限されています。既存のボリュームの空き領域を使用した既存のボリュームのサイズ変更と新しいボリュームの作成機能は、このアプリケーションの完全版に含まれています。このバージョンでは、既存のディスク構成を変更せずに必要なディスク領域を解放するには、既存のボリュームを削除する以外に方法はありません。

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。この領域は、新しいボリュームを作成したり、別のボリュームの種類を変更するために使用できます。

ボリュームを削除する必要がある場合の手順は、次のとおりです。

1. 削除するハード ディスクとボリュームを選択します。
2. ［**操作**］サイドバー リストの［**ボリュームの削除**］または、同様の項目を選択するか、ツールバーの［**選択したボリュームの削除**］アイコンをクリックします。

ボリュームにデータが含まれている場合は、このボリューム上のすべてのデータは失われ、元に戻すことはできないことを示す警告が表示されます。

［**ボリュームの削除**］ウィンドウで［**OK**］をクリックすると、ボリュームの削除が保留中の操作に追加されます。

(追加した操作を完了するには、コミット『ページ参照 334』する必要があります。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。)

6.9.6.3. 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。ディスクにはアクティブなボリュームを 1 つしか設定できません。したがって、あるボリュームをアクティブに設定した場合、以前にアクティブだったボリュームは自動的に設定解除されます。

ボリュームをアクティブに設定する必要がある場合の手順は、次のとおりです。

1. アクティブに設定するベーシック MBR ディスク上のプライマリ ボリュームを選択します。
2. 選択したボリュームを右クリックして、コンテキスト メニューで［**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。

   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。

3. 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。［**警告**］ウィンドウで［**OK**］をクリックすると、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。

   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、コンピュータ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。

(追加した操作を完了するには、コミット『ページ参照 334』する必要があります。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。)

新しいボリューム構造は、［**ディスクの管理**］ビューに図表形式で直ちに表示されます。

6.9.6.4. 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必要がある場合の手順は、次のとおりです。

1. ドライブ文字を変更するボリュームを選択します。
2. 選択したボリュームを右クリックして、コンテキスト メニューで［**ドライブ文字の変更**］をクリックします。
3. ［**ドライブ文字の変更**］ウィンドウで新しいドライブ文字を選択します。
4. ［**ドライブ文字の変更**］ウィンドウで［**OK**］をクリックすると、ボリュームのドライブ文字の割り当てが保留中の操作に追加されます。

   (追加した操作を完了するには、コミット『ページ参照 334』する必要があります。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。)

新しいボリューム構造は、［**ディスクの管理**］ビューに図表形式で直ちに表示されます。

6.9.6.5. 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あり、認識しやすくするためにボリュームに割り当てられる名前です。たとえば、ボリュームには、SYSTEM(オペレーティング システムのあるボリューム)、PROGRAM(アプリケーション ボリューム)、DATA(データ ボリューム)などの名前が付けられますが、ラベルで示されたデータの種類しかそのボリュームに保存できないわけではありません。

Windows では、ボリューム ラベルは、エクスプローラのディスクおよびフォルダ ツリーに LABEL1(C:)、LABEL2(D:)、LABEL3(E:)のように表示されます。LABEL1、LABEL2、および LABEL3 はボリューム ラベルです。ボリューム ラベルは、アプリケーションからファイルを開いたり保存したりするすべての ダイアログ ボックスに表示されます。

ボリューム ラベルを変更する必要がある場合の手順は、次のとおりです。

1. 選択したボリュームを右クリックして、［**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. ［**ラベルの変更**］ウィンドウで［**OK**］をクリックすると、ボリューム ラベルの変更が保留中の操作に追加されます。

   新しいボリューム ラベルを設定するときに、現在インストールされているオペレーティング システムでサポートされない文字を使用した場合は、警告が表示され、[OK] ボタンが無効になります。ボリューム ラベルの変更を続行するには、サポートされる文字だけを使用する必要があります

   (追加した操作を完了するには、コミット『ページ参照 334』する必要があります。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)。

新しいラベルは、コンソールの［**ディスクの管理**］ビューに図表形式で直ちに表示されます。

6.9.6.6. 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 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場合の手順は、次のとおりです。

1. フォーマットするボリュームを選択します。
2. 選択したボリュームを右クリックして、コンテキスト メニューで**[フォーマット]**をクリックします。

   [ボリュームのフォーマット] ウィンドウが表示され、ここで新しいファイル システム オプションを設定できます。FAT16(ボリューム サイズが 2GB を超えている場合は無効)、FAT32 (ボリューム サイズが 2TB を超えている場合は無効)、または NTFS のいずれかの Windows ファイル システムを選択できます。

   必要に応じて、テキスト ウィンドウにボリューム ラベルを入力できます。デフォルトでは、このウィンドウは空白です。

   クラスタ サイズの設定では、各ファイル システムの現在の容量内で任意の数値を選択できます。選択したファイル システムのボリュームに最適なクラスタ サイズが提示されることに注意してください。
3. **[OK]** をクリックして **[ボリュームのフォーマット]** 操作を続行すると、ボリュームのフォーマットが保留中の操作に追加されます

   (追加した操作を完了するには、コミット『ページ参照 334』する必要があります。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)。

新しいボリューム構造は、 **[ディスクの管理]** ビューに図表形式で表示されます。

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 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。

6.9.7. 保留中の操作

手動モードまたはウィザードを使用してユーザーが準備したすべての操作は、ユーザーが特定のコマンドを発行して変更を確定するまでは保留中と見なされます。そのときまで、Acronis Disk Director Lite は、ディスクおよびボリュームで実行するように計画された操作で作成される新しいボリューム構造だけを示します。この方法によって、すべての計画された操作を制御できます。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。

ディスクで予定外の変更を実行しないようにするため、最初にすべての保留中の操作の一覧が表示されます。

［**ディスクの管理**］ビューには、保留中の操作を対象とした［**元に戻す**］、［**やり直す**］、［**コミット**］の各アクションを実行するアイコンのあるツールバーが表示されています。これらの操作は、コンソールの［**ディスクの管理**］メニューから実行することもできます。

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**］をクリックすると、保留中の操作が実行されます。［**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。［**キャンセル**］をクリックして、コミットを取り消すこともできます。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 Acronis Disk Director Lite を終了すると、これらの操作は事実上取り消されます。そのため、保留中の操作をコミットせずに［**ディスクの管理**］を終了しようとすると、警告が表示されます。

7. 集中管理

ここでは、集中管理用のコンポーネントを使用して集中的に実行できる操作について説明します。このセクションの内容は、Acronis Backup & Recovery 10 Advanced Edition に対してのみ適用できます。

7.1. Acronis Backup & Recovery 10 管理サーバーの管理

ここでは、管理サーバーに接続されているコンソールのナビゲーション ツリーで使用できるビューと、各ビューの使用方法について説明します。

7.1.1. ダッシュボード

登録済みのコンピュータ上のデータ保護の状態をすばやく評価するには、ダッシュボードを使用します。ダッシュボードには Acronis Backup & Recovery 10 エージェントの活動の概要が表示されるので、管理対象の格納域の空き領域を確認し、問題をすばやく特定して解決することができます。

アラート

［アラート］セクションでは、管理サーバー、登録済みのコンピュータ、集中管理用格納域で発生した問題についてユーザーの注意を促し、その問題を修正したり、調査する手段を提供します。最も重大な問題が最上部に表示されます。その時点でアラートまたは警告がない場合は、「アラートまたは警告はありません。」と表示されます。

アラートの種類

下の表は、表示される可能性のあるメッセージの種類を示しています。

	説明	推奨	コメント
	失敗したタスク: *X*	タスクの表示	**［タスクの表示］**をクリックすると、失敗したタスクの**［バックアップの計画およびタスク］**ビューが開きます。このビューで失敗の理由を調べることができます。
	ユーザーによる操作が必要なタスク: *X*	解決	管理サーバーのデータベースの少なくとも 1 つのタスクがユーザーによる操作を必要とする場合、［ダッシュボード］にアラートが表示されます。**［解決...］**をクリックすると、**［タスクはユーザーによる操作が必要］**ウィンドウが開きます。このウィンドウで、すべてのケースを調べて決定した操作を指定できます。

	X 台のコンピュータのライセンスを確認できませんでした	ログの表示	Acronis Backup & Recovery 10 エージェントは、起動時に Acronis ライセンス サーバーに接続し、その後は、エージェント構成パラメータの指定に基づいて 1 ～ 5 日ごとに接続します。少なくとも 1 つのエージェントでライセンスの確認が失敗した場合は、アラートが表示されます。これは、ライセンス サーバーが使用できない場合、またはライセンス キーのデータが破損している場合に発生します。［**ログの表示**］をクリックし、チェックの失敗の原因を確認します。 エージェント構成パラメータの指定に基づいて、ライセンスの確認が 1 ～ 60 日間失敗すると、エージェントはライセンスの確認が成功するまで停止します。
	格納域の空き領域が少なくなっています: *X*	格納域の表示	少なくとも 1 つの集中管理用格納域の空き容量が 10% 未満になると、アラートが表示されます。［**格納域の表示**］をクリックすると［**集中管理用格納域**］**『ページ参照 156』ビューが表示されます。このビューで、格納域のサイズ、空き領域、および内容を確認し、空き領域を増やすために必要な手順を実行できます。**
	ブータブル メディアは作成されませんでした	今すぐ作成	コンピュータが起動できない場合にオペレーティング システムを復元できるようにするには、次の手順を行う必要があります。 1 システム ボリューム(およびブート ボリューム(異なる場合))をバックアップします。 2 少なくとも 1 つのブータブル メディア『ページ参照 423』を作成します。 ［**今すぐ作成**］によりブータブル メディア ビルダ『ページ参照 424』が起動されます。
	Y 台のコンピュータで *X* 日間バックアップが作成されていません	一覧の表示	［ダッシュボード］に、一部の登録済みのコンピュータで一定時間データがバックアップされなかったことを示す警告が表示されます。 問題であると見なす時間の長さを構成するには、［**オプション**］→［**コンソール オプション**］→［**時間ベースのアラート**］を選択します。
	Y 台のコンピュータが *X* 日間管理サーバーに接続していません	コンピュータの表示	［ダッシュボード］に、一部の登録済みのコンピュータと管理サーバーの間で一定時間接続が確立されなかったこと、およびその結果、コンピュータが集中管理されなかった可能性があることを示す警告が表示されます。 ［**コンピュータの表示**］をクリックし、［前回の接続］フィールドでフィルタ処理されたコンピュータの一覧を含む［**コンピュータ**］ビューを開きます。 問題であると見なす時間の長さを構成するには、［**オプション**］→［**コンソール オプション**］→［**時間ベースのアラート**］を選択します。

⚠	設定を保護するために、管理サーバーをバックアップしておくことをお勧めします。エージェントを管理サーバー コンピュータにインストールし、そのコンピュータを AMS に追加します。	Acronis コンポーネントのインストール	Acronis Backup & Recovery 10 エージェント for Windows をインストールし、Acronis Backup & Recovery 10 管理サーバーが存在するコンピュータをバックアップします。 **[今すぐインストール]** をクリックし、インストール ウィザードを起動します。
⚠	Acronis Backup & Recovery 10 管理サーバーは、*X* 日間バックアップされていません	今すぐバックアップ	このアラートは、Acronis Backup & Recovery 10 エージェント for Windows が管理サーバーにインストールされている場合のみ表示されます。アラートに、管理サーバーで一定時間データがバックアップされなかったことを示す警告が表示されます。 **[今すぐバックアップ]** をクリックすると **[バックアップ計画の作成]** ページが表示されます。このページで、バックアップ操作を簡単に構成して実行できます。 問題であると見なす時間の長さを構成するには、**[オプション] → [コンソール オプション] → [時間ベースのアラート]** を選択します。

活動

積み上げ縦棒グラフによって、Acronis Backup & Recovery 10 エージェントの活動の日単位の履歴を確認できます。履歴はログ エントリに基づき、登録済みのコンピュータと管理サーバーから収集されます。グラフには、特定の日の各種類(エラー、警告、情報)のログ エントリの数が表示されます。

選択した日の統計情報は、グラフの右に表示されます。すべての統計フィールドは対話式なので、任意のフィールドをクリックすると、そのフィールドによって事前にフィルタ処理されたログ エントリが **[ログ]** ビューに表示されます。

グラフの最上部で、エラーの存在と重大度によって、表示する活動を選択できます。

[当日の選択] リンクには現在の日付が選択されます。

システム ビュー

[システム ビュー] セクションには、登録済みのコンピュータ、タスク、バックアップ ポリシー、および集中管理用バックアップ計画の統計情報の概要が表示されます。関連情報を取得するには、これらのセクションの項目(集中管理用バックアップ計画を除く)をクリックします。これにより、事前にフィルタ処理されたコンピュータ、タスク、またはバックアップ ポリシーが適切なビューに表示されます。たとえば、**[タスク]** の **[アイドル]** をクリックすると、**[アイドル]** 状態でフィルタ処理されたタスクを示す **[タスク]** ビューが開きます。

[システム ビュー] セクションに表示される情報は、管理サーバーがコンピュータと同期するたびに更新されます。他のセクションの情報は、10 分ごとおよびダッシュボードにアクセスするたびに更新されます。

格納域

[格納域] セクションには、集中管理対象の格納域に関する情報が表示されます。格納域は、名前別または使用領域別に並べ替えることができます。格納域がテープ ライブラリにある場合など、格納域の空き領域に関する情報を利用できないときもあります。格納域自体が使用できない場合(オフラインの場合)、「格納域は使用できません」というメッセージが表示されます。

7.1.2. バックアップ ポリシー

複数のコンピュータを全体として管理して保護できるようにするために、「バックアップ ポリシー」というバックアップ計画のテンプレートを作成できます。このテンプレートをコンピュータのグループに適用することによって、1 回の操作で複数のバックアップ計画を配置できます。バックアップ ポリシーは、Acronis Backup & Recovery 10 管理サーバーのみに存在します。

各コンピュータに個別に接続して、データが正しく保護されているかどうかを確認する必要はありません。代わりに、ポリシーが適用されるすべての管理対象のコンピュータの、ポリシーの蓄積されたステータス『ページ参照 340』を確認します。

バックアップ ポリシーの現在の状況(配置、取り消し、または更新)を確認するには、ポリシーの配置状態『ページ参照 339』を確認します。

バックアップ ポリシーのビューの操作方法

- **ツールバー**の操作ボタンを使用して新しいポリシーを作成するか、既存のポリシーをコンピュータに適用するか、またはバックアップ ポリシーを使用するその他の操作『ページ参照 342』を実行します。
- **[情報]** ペインのタブを使用して選択したポリシーに関する詳細情報を表示して、ポリシーの取り消し、ポリシーを適用するコンピュータ(グループ)の詳細の表示などの追加の操作を実行します。ペインはデフォルトで折りたたまれています。ペインを展開するには、  をクリックします。ペインの内容は、［ポリシーの詳細］『ページ参照 344』ウィンドウにも重複して表示されます。
- ポリシー テーブルを簡単に参照して確認するには、フィルタ処理と並べ替え『ページ参照 343』の機能を使用します。

7.1.2.1. バックアップ ポリシーの配置状態

バックアップ ポリシーの配置状態は、ポリシーが適用されるすべてのコンピュータのポリシーの配置状態の組み合わせで示されます。たとえば、ポリシーが 3 台のコンピュータに適用され、最初のコンピュータの状態が "配置中"、2 番目のコンピュータの状態が "更新中"、3 番目のコンピュータの状態が "配置済み" の場合、ポリシーの状態は "配置中、更新中、配置済み" になります。

コンピュータのグループのバックアップ ポリシーの配置状態は、グループを構成するコンピュータのポリシーの配置状態の組み合わせで示されます。

バックアップ ポリシーの配置状態の詳細については、「バックアップ ポリシーの状態とステータス『ページ参照 79』」をご参照ください。

7.1.2.2. バックアップ ポリシーのステータス

バックアップ ポリシーのステータスは、ポリシーが適用されるすべてのコンピュータのポリシー ステータスの蓄積されたステータスで示されます。たとえば、ポリシーが 3 台のコンピュータに適用され、最初のコンピュータのステータスが "OK"、2 番目のコンピュータのステータスが "警告"、3 番目のコンピュータのステータスが "エラー" の場合、ポリシーのステータスは "エラー" になります。

コンピュータのグループのバックアップ ポリシーのステータスは、グループに含まれるコンピュータのポリシー ステータスの蓄積されたステータスで示されます。

バックアップ ポリシーのステータスの概要を次の表に示します。

	ステータス	判断方法	対処方法
1	**エラー**	少なくとも 1 台のコンピュータのポリシー ステータスが "エラー" です。 それ以外の場合は、2 をご参照ください。	ログを表示するか失敗したタスクを確認し、失敗の原因を特定して、次の 1 つ以上の操作を行います。 • 失敗の原因を取り除きます。このためには、必要に応じて、失敗したタスクを手動で開始します。 • バックアップ ポリシーを編集し、今後の失敗の発生を防止します。
2	**警告**	少なくとも 1 台のコンピュータのポリシー ステータスが "警告" です。 それ以外の場合は、3 をご参照ください。	ログを表示して警告を確認します。このためには、必要に応じて、今後の警告や失敗を防止するための操作を実行します。
3	**OK**	すべてのコンピュータのポリシー ステータスが "OK" です。	操作は必要ありません。バックアップ ポリシーがどのコンピュータにも適用されていない場合も状態は "OK" になります。

ポリシーのステータスが "エラー" の場合

1. 失敗の原因を特定するには、次の 1 つ以上の操作を行います。
   - ［**エラー**］ハイパーリンクをクリックし、最新のエラーのログ エントリを確認します。
   - ポリシーを選択し、［**タスクの表示**］をクリックします。前回の結果が［**失敗**］のタスクを確認します。タスクを選択し、［**ログの表示**］をクリックします。ログ エントリを選択し、［**詳細の表示**］をクリックします。この方法は、ポリシーの状態が "配置済み" の場合、つまりポリシーのタスクが既に管理対象のコンピュータに存在している場合に役立ちます。
   - ポリシーを選択し、［**ログの表示**］をクリックします。"エラー" のログ エントリをチェックし、失敗の原因を特定します。ログ エントリを選択し、［**詳細の表示**］をクリックします。この方法は、ポリシーの配置、取り消し、または更新中にエラーが発生した場合に役立ちます。

[タスク] ビューで、[前回の結果 -> 失敗] フィルタを適用します(タスクが多すぎる場合)。失敗したタスクは、バックアップ計画別またはコンピュータ別に並べ替えることもできます。

[ログ] ビューで、エラー フィルタを適用します(ログ エントリが多すぎる場合)。"エラー" のエントリは、バックアップ計画、管理対象のエンティティ、またはコンピュータ別に並べ替えることもできます。

2. 失敗の原因がわかったら、次の 1 つ以上の操作を行います。
   - 失敗の原因を取り除きます。その後、バックアップ スキームの整合性を維持するために失敗したタスクを手動で開始できます(ポリシーが GFS またはハノイの塔バックアップ スキームを使用する場合など)。
   - バックアップ ポリシーを編集し、今後の失敗の発生を防止します。

[ダッシュボード] の [アクティビティ] セクションを使用して、"エラー" のログ エントリに迅速にアクセスします。

ポリシーのステータスが "警告" の場合

1. 警告の原因を特定するには、次の 1 つ以上の操作を行います。
   - **[警告]** ハイパーリンクをクリックし、最新の警告のログ エントリを確認します。
   - ポリシーを選択し、**[タスクの表示]** をクリックします。前回の結果が **[警告を伴う正常終了] のタスクを確認します。タスクを選択し、[ログの表示]** をクリックします。この方法は、ポリシーの状態が "配置済み" の場合、つまりポリシーのタスクが既に管理対象のコンピュータに存在している場合に役立ちます。
   - ポリシーを選択し、**[ログの表示]** をクリックします。"警告" のログ エントリをチェックし、警告の原因を特定します。ログ エントリを選択し、**[詳細の表示]** をクリックします。この方法は、ポリシーの配置、取り消し、または更新中に警告が発生した場合に役立ちます。

[タスク] ビューで、[前回の結果 -> 警告を伴う正常終了] フィルタを適用します(タスクの数が多すぎる場合)。警告を伴って正常終了したタスクは、バックアップ計画別またはコンピュータ別に並べ替えることもできます。

[ログ] ビューで、警告 フィルタを適用します(ログ エントリが多すぎる場合)。"警告" のエントリは、バックアップ計画、管理対象のエンティティ、またはコンピュータ別に並べ替えることもできます。

2. 警告の原因がわかったら、その後の警告または失敗を防止するためのアクションを実行できます。

[ダッシュボード] の [アクティビティ] セクションを使用して、"警告" のログ エントリに迅速にアクセスします。

ポリシー ステータスが "OK" の場合

操作は必要ありません。

7.1.2.3. バックアップ ポリシーの操作

次に説明するすべての操作は、タスクの**ツールバー**の対応する項目をクリックすると実行されます。これらの操作は、コンテキスト メニュー(選択したバックアップ ポリシーを右クリックする)または **[アクションとツール]** ペインの **['バックアップ ポリシー名' アクション]** バーを使用して実行することもできます。

バックアップ ポリシーを使用して操作を実行するためのガイドラインを次に示します。

目的	操作手順
バックアップ ポリシーの作成	**[バックアップ ポリシーの作成]** をクリックします。 バックアップ ポリシーを作成する手順は、「バックアップ ポリシーの作成『ページ参照 389』」で詳しく説明します。
コンピュータまたはグループへのポリシーの適用	**[適用]** をクリックします。 [コンピュータの選択]『ページ参照 343』ウィンドウで、選択したバックアップ ポリシーを適用するコンピュータ(グループ)を指定します。コンピュータがオフラインになっている場合、ポリシーはコンピュータが再びオンラインになったときに配置されます。
ポリシーの編集	**[編集]** をクリックします。 ポリシーの編集は、作成『ページ参照 389』と同様に実行します。ポリシーを編集すると、ポリシーが配置されているすべてのコンピュータのポリシーが管理サーバーによって更新されます。
ポリシーの削除	**[削除]** をクリックします。 ポリシーは配置されているコンピュータから取り消され、管理サーバーから削除されます。コンピュータがオフラインになっている場合、ポリシーはコンピュータが再びオンラインになったときに取り消されます。
ポリシーの詳細の表示またはポリシーの取り消し	**[詳細の表示]** をクリックします。 [ポリシーの詳細]『ページ参照 344』ウィンドウで、選択したポリシーの情報を確認します。そのウィンドウで、ポリシーが適用されているコンピュータまたはコンピュータのグループからポリシーを取り消すこともできます。
ポリシーのタスクの表示	**[タスクの表示]** をクリックします。 [タスク]『ページ参照 366』ビューに、選択したポリシーに関連するタスクの一覧が表示されます。
ポリシーのログの表示	**[ログの表示]** をクリックします。 [ログ]『ページ参照 369』ビューに、選択したポリシーに関連するログ エントリの一覧が表示されます。
ポリシー一覧の更新	**[更新]** をクリックします。 管理コンソールにより、管理サーバーの最新情報を使用してバックアップ ポリシーの一覧が更新されます。ポリシーの一覧はイベントに基づいて自動的に更新されますが、待ち時間があるため、データは管理サーバーから即座に取得されない場合があります。手動で更新すると、最新データを確実に表示できます。

コンピュータの選択

コンピュータまたはコンピュータのグループにバックアップ ポリシーを適用する手順は、次のとおりです。

1. 選択したバックアップ ポリシーを次のどちらに適用するかを指定します。
   - **グループ**
     グループ ツリーで、ポリシーを適用するグループを選択します。ウィンドウの右側に、選択したグループのコンピュータの一覧が表示されます。
   - **個々のコンピュータ**
     グループ ツリーで、目的のグループを選択します。次に、ウィンドウの右側で、バックアップ ポリシーを適用するコンピュータを選択します。
2. ［OK］をクリックします。

Acronis Backup & Recovery 10 管理サーバーによって、選択したコンピュータおよび選択したグループに属しているコンピュータにポリシーが配置されます。

バックアップ ポリシーのフィルタ処理と並べ替え

バックアップ ポリシーのフィルタ処理と並べ替えを実行するためのガイドラインを次に示します。

目的	操作手順
任意の項目によるバックアップ ポリシーの並べ替え	項目のヘッダーをクリックすると、バックアップ ポリシーが昇順で並べ替えられます。 再度クリックすると、バックアップ ポリシーは降順で並べ替えられます。
名前/所有者によるバックアップ ポリシーのフィルタ処理	対応する項目のヘッダーの下にあるフィールドにポリシー名/所有者名を入力します。 その結果、ポリシーまたはその所有者の名前の全体または一部が入力された値と一致するバックアップ ポリシーの一覧が表示されます。
配置状態、ステータス、バックアップ元の種類、前回の結果、スケジュールによるバックアップ ポリシーのフィルタ処理	対応する列のヘッダーの下のフィールドで、一覧から必要な値を選択します。

バックアップ ポリシー テーブルの設定

デフォルトでは、テーブルに 7 つの項目が表示され、その他の項目は非表示になります。個々のニーズと設定に応じて、項目の表示を調整できます。

列を表示または非表示にする手順は、次のとおりです。

1. 項目のヘッダーを右クリックしてコンテキスト メニューを開きます。チェックボックスをオンにしたメニュー項目が、表のヘッダー項目に表示されます。
2. 表示/非表示を切り換える項目をクリックします。

7.1.2.4. ポリシーの詳細

[ポリシーの詳細] ウィンドウでは、選択したバックアップ ポリシーに関するすべての情報が 5 つのタブにまとめられているので、ポリシーを適用するコンピュータおよびコンピュータのグループに対して操作を実行できます。

この情報は、**[情報]** ペインにも重複して表示されます。

バックアップ ポリシー

このタブには、選択したポリシーに関する情報が表示されます。

ソース

このタブには、バックアップするソースの種類およびソースの選択ルールに関する情報が表示されます。

ターゲット

このタブには、バックアップの保存先に関する情報が表示されます。

設定

このタブには、ポリシーに使用するバックアップ スキームおよびデフォルト設定から変更されたバックアップ オプションに関する情報が表示されます。

適用先

このタブには、選択したポリシーが適用されるコンピュータおよびそのグループの一覧が表示されます。

操作

目的	操作手順
コンピュータ(グループ)の詳細の表示	**[詳細の表示]** をクリックします。 [コンピュータの詳細]『ページ参照 352』/ [グループの詳細]『ページ参照 361』ウィンドウで、選択したコンピュータ(またはグループ)に関するすべての情報を確認します。
コンピュータ(グループ)のタスクの表示	**[タスクの表示]** をクリックします。 [タスク]『ページ参照 366』ビューに、選択したコンピュータ(グループ)で事前にフィルタ処理されたタスクの一覧が表示されます。
コンピュータ(グループ)のログの表示	**[ログの表示]** をクリックします。 [ログ]『ページ参照 369』ビューに、選択したコンピュータ(グループ)で事前にフィルタ処理されたログ エントリの一覧が表示されます。
コンピュータ(グループ)からのポリシーの取り消し	**[取り消し]** をクリックします。 管理サーバーによって、選択したコンピュータまたはコンピュータのグループからポリシーが取り消されます。ポリシー自体は、管理サーバーに残ります。

7.1.3. 物理コンピュータ

Acronis Backup & Recovery 10 を使用すると、管理者は複数のコンピュータ上でデータを保護したり、管理操作を実行したりすることができます。管理者は、コンピュータの名前または IP アドレスを使用して管理サーバーにコンピュータを追加し、Active Directory または テキスト ファイルからコンピュータをインポートします。コンピュータが管理サーバーに登録『ページ参照 429』されると、コンピュータのグループ化、バックアップ ポリシーの適用、データ保護に関連する活動の監視を行うことができます。

管理対象のコンピュータ上でデータが正常に保護されているかどうかを確認するために、管理サーバーの管理者はステータスをチェックします。コンピュータのステータスは、コンピュータ上に存在するすべてのバックアップ計画『ページ参照 222』(ローカルと集中管理の両方)およびコンピュータに適用されるすべてのバックアップ ポリシー『ページ参照 340』のうち最も重大なステータスに決定されます。ステータスは、［OK］、［警告］、または［エラー］のいずれかになります。

グループ

管理サーバーの管理者はコンピュータをグループ化することができます。1 台のコンピュータが、複数のグループのメンバになることができます。管理者が作成した任意のグループの内部に、1 つ以上の入れ子になったグループを作成することができます。

グループ化することで、会社の部門別、Active Directory ドメインまたはドメイン内の組織単位別、さまざまなユーザーの集団別、サイト ロケーション別などでデータ保護を編成することができます。

グループ化の主な目的は、1 つのポリシーで複数のコンピュータを保護することです。コンピュータをグループに追加すると、グループに適用されるポリシーがそのコンピュータに適用され、コンピュータ上のポリシーによって新しいタスクが作成されます。コンピュータをグループから削除すると、グループに適用されるポリシーがコンピュータから取り消され、ポリシーによって作成されたタスクが削除されます。

ビルトイン グループ - 管理サーバー上に常に存在するグループ。このグループを削除したり名前を変更したりすることはできません。ビルトイン グループ内に、入れ子になったグループに含めることはできません。バックアップ ポリシーをビルトイン グループに適用することができます。ビルトイン グループの例として、管理サーバーに登録されているすべてのコンピュータを含む **［すべての物理コンピュータ］** グループがあります。

カスタム グループ - 管理サーバー管理者によって手動で作成されるグループ。

- *静的グループ*
  静的グループには、管理者が手動でグループに追加したコンピュータが含まれます。静的メンバは、管理者がグループからメンバを削除するか、対応する管理対象のコンピュータを管理サーバーから削除するまでグループ内に残ります。

- *ダイナミック グループ*
  ダイナミック グループには、管理者が指定した条件に従って自動的に追加されたコンピュータが含まれます。条件を指定すると、管理サーバーが既存のコンピュータのプロパティの分析を開始し、新しく登録されるコンピュータもすべて分析します。特定の動的な条件を満たすコンピュータは、この動的な条件を使用するすべてのグループに追加されます。

コンピュータのグループ化の詳細については、「登録されたコンピュータのグループ化『ページ参照 71』」をご参照ください。

コンピュータとグループにポリシーを適用する方法については、「コンピュータとグループのポリシー『ページ参照 74』」をご参照ください。

コンピュータの操作方法

- 最初に、コンピュータを管理サーバーに追加します。コンピュータの追加は、**[物理コンピュータ]**ビューを選択するか、**ナビゲーション** ツリーで **[すべての物理コンピュータ]** を選択したときに行うことができます。
- 必要なコンピュータが含まれているグループを選択してからコンピュータを選択します。
- コンピュータの操作『ページ参照 346』を実行するには、**ツールバー**の操作ボタンを使用します。
- 選択したコンピュータに関する詳細情報を表示し、タスクの開始/停止、ポリシーの取り消し、ポリシーの継承の確認などの追加の操作を実行するには、**[情報]** パネルのタブを使用します。このパネルはデフォルトでは折りたたまれています。パネルを展開するには、をクリックします。このパネルの内容は、**[コンピュータの詳細]** 『ページ参照 352』ウィンドウにも重複して表示されます。
- フィルタ処理と並べ替え『ページ参照 357』機能を使用すると、目的のコンピュータを簡単に参照して調べることができます。

グループの操作方法

- **[物理コンピュータ]** ビューでグループを選択します。
- 選択したグループの操作『ページ参照 358』を実行するには、ツールバーの操作ボタンを使用します。
- 選択したグループに関する詳細情報を表示し、ポリシーの取り消し、ポリシーの継承の確認などの追加の操作を実行するには、**[情報]** パネルのタブを使用します。パネルはデフォルトでは折りたたまれています。パネルを展開するには、をクリックします。このパネルの内容は、**[グループの詳細]** 『ページ参照 361』ウィンドウにも重複して表示されます。

7.1.3.1. コンピュータの操作

管理サーバーへのコンピュータの登録

コンピュータを **[すべての物理コンピュータ]** グループに追加すると、そのコンピュータは管理サーバーに登録されます。登録されたコンピュータにはバックアップ ポリシーを配置したり、他の集中管理操作を実行したりすることができます。登録によって、コンピュータ上に存在するエージェントと管理サーバーの間に信頼関係が設定されます。

追加とインポートの操作は、**［物理コンピュータ］**ビューまたはナビゲーション ツリーの**［すべての物理コンピュータ］**グループを選択したときに使用できます。

目的	操作手順
管理サーバーへの新しいコンピュータの追加	**［AMS にコンピュータを追加する］**をクリックします。 **［コンピュータの追加］**『ページ参照 349』ウィンドウで、管理サーバーに追加する必要があるコンピュータを選択します。
Active Directory からのコンピュータのインポート	**［Active Directory からコンピュータをインポートする］**をクリックします。 **［Active Directory からコンピュータをインポートする］**『ページ参照 350』ウィンドウで、管理サーバーにインポートするコンピュータを指定するか、インポートする必要があるコンピュータが含まれる組織単位を指定します。
テキスト ファイルからのコンピュータのインポート	**［ファイルからコンピュータをインポートする］**をクリックします。 **［ファイルからコンピュータをインポートする］**『ページ参照 351』ウィンドウで、管理サーバーにインポートするコンピュータの名前(または IP アドレス)が含まれる .txt ファイルまたは .csv ファイルを参照します。

管理コンソールがエージェントをアドレス指定し、登録処理を開始します。登録にはエージェントが関与する必要があるので、コンピュータがオフラインのときは実行できません。

登録されているコンピュータにインストールされた追加のエージェントは、自動的に同じ管理サーバーに登録されます。複数のエージェントが一緒に登録および登録解除されます。

ポリシーの適用

目的	操作手順
コンピュータへのバックアップ ポリシーの適用	**［バックアップ ポリシーの適用］**をクリックします。 **［ポリシーの選択］**『ページ参照 351』ウィンドウで、選択したコンピュータに適用する必要があるバックアップ ポリシーを指定します。

グループ化の操作

目的	操作手順
カスタム静的グループまたはダイナミック グループの作成	**［グループの作成］**をクリックします。 **［グループの作成］**『ページ参照 359』ウィンドウで、グループの必要なパラメータを指定します。新しいグループが、選択したコンピュータがメンバになっているグループ(ビルトイン **すべての物理コンピュータ］**グループを除きます)内に作成されます。
別の静的グループへのコンピュータの追加	**［別のグループに追加］**をクリックします。 **［グループに追加］**『ページ参照 351』ウィンドウで、選択したコンピュータのコピー先のグループを指定します。コンピュータがメンバになっているグループに適用されるバックアップ ポリシーがコンピュータに適用されます。

カスタム グループ内のコンピュータの場合	
静的グループへのコンピュータの追加	 **[グループにコンピュータを追加する]** をクリックします。 **[グループにコンピュータを追加する]**『ページ参照 352』ウィンドウで、追加する必要があるコンピュータを選択します。
別の静的グループへのコンピュータの移動	 **[別のグループへの移動]** をクリックします。 **[グループへの移動]**『ページ参照 351』ウィンドウで、コンピュータの移動先のグループを選択します。 コンピュータが含まれていたグループに適用されるすべてのバックアップ ポリシーは取り消されます。コンピュータが現在メンバになっているグループに適用されるバックアップ ポリシーがコンピュータに配置されます。
現在の静的グループからのコンピュータの削除	 **[グループから削除]** をクリックします。 グループに適用されるバックアップ ポリシーが自動的にコンピュータから取り消されます。

管理サーバーからの選択したコンピュータの削除

目的	操作手順
管理サーバーからのコンピュータの削除	 **[AMS からコンピュータを削除する]** をクリックします。 結果として、バックアップ ポリシーが取り消され、集中管理用格納域へのショートカットがコンピュータから削除されます。この時点でコンピュータが使用できない場合は、管理サーバーからコンピュータを使用できるようになるとすぐにコンピュータ上でこれらの処理が実行されます。

その他の操作

直接管理操作	
コンピュータ上でのバックアップ計画の作成	 **[バックアップ]** をクリックします。 この操作の詳細については、「バックアップ計画の作成『ページ参照 236』」をご参照ください。
データの復元	 **[復元]** をクリックします。 この操作の詳細については、「データの復元『ページ参照 257』」をご参照ください。
コンピュータへの直接接続	 **[直接接続]** をクリックします。 管理対象のコンピュータへの直接接続を確立します。管理対象のコンピュータを管理できるようになり、すべての直接管理操作を実行できるようになります。

その他の操作	
コンピュータの詳細情報の表示	 **[詳細の表示]** をクリックします。 **[コンピュータの詳細]** 『ページ参照 352』ウィンドウで、コンピュータの情報を確認します。
コンピュータ上に存在するタスクの表示	 **[タスクの表示]** をクリックします。 **[タスク]** 『ページ参照 366』ビューには、コンピュータ上に存在するタスクの一覧が表示されます。
コンピュータのログ エントリの表示	 **[ログの表示]** をクリックします。 **[ログ] ビューには、コンピュータのログ エントリの一覧が表示されます。** 『ページ参照 369』
コンピュータの一覧の更新	 **[更新]** をクリックします。 管理コンソールによって、管理サーバーから取得したコンピュータの一覧が最新の情報に更新されます。コンピュータの一覧はイベントに基づいて自動的に更新されますが、待ち時間があるため、データは管理サーバーから直ちに取得されないことがあります。手動で更新すると、確実に最新データが表示されます。

管理サーバーへのコンピュータの追加

Acronis Backup & Recovery 10 管理サーバーから管理対象のコンピュータにバックアップ ポリシーを配置し、その他の集中管理操作を実行するには、管理サーバーにコンピュータを登録する必要があります。

コンピュータを登録する手順は、次のとおりです。

1. **[ナビゲーション]** ツリーで、  **[物理コンピュータ]** または  **[すべての物理コンピュータ]** を選択します。
2. ツールバーの  **[コンピュータの追加]** をクリックします。
3. **[IP/名前] フィールドで、コンピュータの名前または IP アドレスを入力し、[参照...]** をクリックして、ネットワーク上のコンピュータを参照します。
4. 有効なコンピュータのアカウントを指定するには、**[オプション>>]** をクリックして、次の項目を指定します。
   - **[ユーザー名]** - Active Directory ユーザー アカウントの名前を入力する場合は、ドメイン名(DOMAIN¥ユーザー名)も指定してください。
   - **[パスワード]** - アカウントのパスワード。

   後で接続するときのためにパスワードを保存するには、**[パスワードを保存する]** チェック ボックスをオンにします。
5. **[OK]** をクリックします。

コンピュータ側での登録の開始

Acronis Backup & Recovery 10 管理サーバーの管理者は、次のときにサーバーの名前または IP アドレスをエージェントに設定することができます。

- エージェントをインストールするとき
- コンソールとエージェントの接続を使用するとき

これにより、標準の登録手順が開始されます。

エージェントのインストール中にエージェントを登録するには、管理サーバーの管理者アカウントを使用してログインするか、サーバー管理者のログイン情報をプロンプトに入力する必要があります。

ローカルまたはリモートのコンソールとエージェントの接続を使用して登録を実行するには、管理サーバーの管理者ログイン情報を使用して接続するか、管理サーバーの管理者ログイン情報を入力する必要があります。接続した状態で、**[オプション]** - **[コンピュータ オプション]** - **[コンピュータの管理]** メニューを選択し、**[集中管理]** を選択して、管理サーバーの名前または IP アドレス、および管理サーバーの管理者ログイン情報を入力します。

Active Directory からのコンピュータのインポート

Active Directory からコンピュータをインポートする手順は、次のとおりです。

1. **[ナビゲーション]** ツリーで、**[物理コンピュータ]** または **[すべての物理コンピュータ]** を選択します。
2. ツールバーの **[Active Directory からコンピュータをインポートする]** をクリックします。
3. **[検索対象]** フィールドに、コンピュータ(または組織単位)の名前を入力し、**検索]** をクリックします。アスタリスク(*)を使用して、コンピュータ(または組織単位)の名前の 0 以上の文字を置き換えることができます。

   ウィンドウの左側には、入力した値と完全に一致するか、部分的に一致するコンピュータ(または組織単位)の名前が表示されます。インポートに追加する項目をクリックし、**[追加 >>]**をクリックします。項目がウィンドウの右側に移動されます。見つかったすべての項目を追加するには、 **[すべて追加>>]** をクリックします。

   1,000 以上の一致する項目が見つかった場合は、最初の 1,000 項目のみが表示されます。この場合、検索を絞り込んで再び実行することをお勧めします。

   ウィンドウの右側には、インポート用に選択した項目が表示されます。必要な場合は、それぞれの **[削除]** ボタンと **[すべて削除]** ボタンを使用して、間違って選択された項目を削除します。
4. **[OK]** をクリックしてインポートを開始します。

テキスト ファイルからのコンピュータのインポート

ファイルからコンピュータをインポートする手順は、次のとおりです。

1. **[ナビゲーション]** ツリーで、**[物理コンピュータ]** または **[すべての物理コンピュータ]** を選択します。
2. ツールバーの **[Active Directory からコンピュータをインポートする]** をクリックします。
3. **[フォルダ]** フィールドに、.txt ファイルまたは .csv ファイルのパスを入力するか、[参照] をクリックして **[参照]** ウィンドウでファイルを選択します。

   .txt ファイルまたは .csv ファイルにはコンピュータの名前または IP アドレスが含まれていて、コンピュータごとに改行されている必要があります。

   例:

   ```
   コンピュータ名 1
   コンピュータ名 2
   192.168.1.14
   192.168.1.15
   ```

4. **[OK]** をクリックしてインポートを開始します。

ポリシーの選択

選択したコンピュータ (グループ) にバックアップ ポリシーを適用する手順は、次のとおりです。

1. コンピュータ (グループ) に適用するバックアップ ポリシーを一覧から選択します。

必要なポリシーを表示するには、フィルタを使用します。

2. **[OK]** をクリックします。

別のグループへのコンピュータの追加

選択したコンピュータを別のグループに追加する手順は、次のとおりです。

1. コンピュータを追加するグループを選択します。
2. **[OK]** をクリックします。

追加するコンピュータは、複数のグループのメンバになります。結果として、最初のグループに適用されるバックアップ ポリシーはコンピュータ上に残り、2 番目、3 番目、およびそれ以降のグループに適用されるバックアップ ポリシーがコンピュータに配置されます。

別のグループへのコンピュータの移動

選択したコンピュータを別のグループに移動する手順は、次のとおりです。

1. グループ ツリーでコンピュータの移動先のグループを選択します。
2. **[OK]** をクリックします。

移動されるコンピュータは、元のグループを出て別のグループのメンバになります。結果として、最初のグループに適用されるバックアップ ポリシーはコンピュータから取り消され、2 番目のグループに適用されるバックアップ ポリシーがコンピュータに配置されます。

グループへのコンピュータの追加

コンピュータを選択したグループに追加する手順は、次のとおりです。

1. グループ ツリーで、追加する必要があるコンピュータが含まれるグループを選択します。
2. ウィンドウの右側で、コンピュータを選択します。
3. 他のグループからさらにコンピュータを追加するには、各グループについて手順 1 と 2 を繰り返します。
4. **[OK]** をクリックしてコンピュータを追加します。

コンピュータがグループに追加されると、グループに適用されていたポリシー(存在する場合)がコンピュータに配置されます。選択したコンピュータのいずれかがそのときに使用できないか接続できない場合、操作は管理サーバー内に保留として保持され、コンピュータが使用可能になるとすぐに実行されます。

コンピュータの詳細

選択したコンピュータに関するすべての情報が 4 つのタブに集約されます。管理サーバーの管理者は、コンピュータ上に存在するバックアップ計画とタスク、およびコンピュータに適用されるポリシーを使用して操作を実行することができます。

この情報は、**[情報]** パネルにも重複して表示されます。

コンピュータ

このタブには、登録されているコンピュータに関する次の情報が表示されます。

- **[名前]** - 選択したコンピュータの名前(Windows の **[コンピュータ名]** から取得されます)。
- **[IP アドレス]** - 選択したコンピュータの IP アドレス。
- **[ステータス]** - コンピュータのステータス。コンピュータ上に存在するすべてのバックアップ計画『ページ参照 222』(ローカルと集中管理の両方)およびコンピュータに適用されるバックアップ ポリシー『ページ参照 340』のうち最も重大なステータスに決定されます。
- **[前回の接続]** - 管理サーバーが前回コンピュータに接続してから経過した時間。
- **[前回正常に完了したバックアップ]** - 前回の正常なバックアップから経過した時間。
- **[アベイラビリティー]**:
  - **[オンライン]** - コンピュータを管理サーバーで使用できます。これは、管理サーバーからコンピュータへの前回の接続が正常に実行されたことを示します。接続は 2 分間隔で確立されます。
  - **[オフライン]** - コンピュータを管理サーバーで使用できません。コンピュータはオフになっているか、ネットワーク ケーブルが接続されていません。
  - **[不明]** - このステータスは、コンピュータの追加後または管理サーバーのサービス開始後、初めて管理サーバーとコンピュータの間の接続が確立されるまで表示されます。

- o **［取り消し］** - コンピュータが別の管理サーバーに登録されているか、**［オプション］→［コンピュータ オプション］→［コンピュータの管理］**『ページ参照 110』で**［スタンドアロン管理］**パラメータが選択されています。結果として、現在の管理サーバーからコンピュータを制御することができません。ただし、**［コンピュータの管理］**設定で管理サーバーのアドレスを指定することで、コンピュータを再び制御できるようになります。

- **［インストールされているエージェント］** - コンピュータにインストールされている Acronis エージェントの完全な名前。
- **［オペレーティング システム］** - コンピュータのエージェントが実行されるオペレーティング システム。
- **［プロセッサ］** - 管理対象のコンピュータで使用される CPU の種類。
- **［CPU クロック］** - CPU のクロック レート。
- **［RAM］** - メモリ サイズ。
- **［コメント］** - コンピュータの説明(Windows の**［コンピュータの説明］**から取得されます)。

バックアップ ポリシー

選択したコンピュータに適用されるバックアップ ポリシーの一覧が表示され、管理サーバー管理者が次の操作を実行することができます。

目的	操作手順
ポリシーの詳細の表示	**［詳細の表示］**をクリックします。 **［ポリシーの詳細］**『ページ参照 344』ウィンドウで、選択したバックアップ ポリシーに関連付けられているすべての情報を調べます。
ポリシーのタスクの表示	**［タスクの表示］**をクリックします。 **［タスク］**『ページ参照 366』ビューには、選択したバックアップ ポリシーに関連付けられているタスクの一覧が表示されます。
ポリシーのログの表示	**［ログの表示］**をクリックします。 **［ログ］**『ページ参照 369』ビューには、選択したバックアップ ポリシーに関連付けられているログ エントリの一覧が表示されます。
コンピュータからのポリシーの取り消し	**［取り消し］**をクリックします。 管理サーバーによってコンピュータからポリシーが取り消されます。ポリシー自体は管理サーバー上に残ります。 コンピュータがグループのメンバになっていて、ポリシーがグループに適用される場合は、最初にグループからコンピュータを削除しないと、そのコンピュータのポリシーを取り消すことはできません。
ポリシーの適用元の確認	**［継承の参照］**をクリックします。 **［継承順序］**『ページ参照 357』ウィンドウに、コンピュータに適用されたポリシーの継承の順序が表示されます。

フィルタ処理と並べ替え

バックアップ ポリシーのフィルタ処理と並べ替えは、［**バックアップ ポリシー**］ビューと同じ方法で実行します。詳細については、「バックアップ ポリシーのフィルタ処理と並べ替え『ページ参照 343』」をご参照ください。

計画およびタスク

選択したコンピュータ上に存在する計画(ローカルと集中管理の両方）およびタスクの一覧が表示されます。

操作

バックアップ計画およびタスクを使用して操作を実行するためのガイドラインを次に示します。

目的	操作手順
計画またはタスクの詳細の表示	**バックアップ計画** ［**詳細の表示**］をクリックします。 **[計画の詳細]**『ページ参照 232』ウィンドウで、計画の詳細を確認します。 **タスク** ［**詳細の表示**］をクリックします。 **[タスクの詳細]**『ページ参照 230』ウィンドウで、タスクの詳細を確認します。
計画またはタスクのログの表示	**バックアップ計画** ［**ログの表示**］をクリックします。 計画に関連したログ エントリの一覧を含む［**ログ**］『ページ参照 233』ビューが表示されます。 **タスク** ［**ログの表示**］をクリックします。 タスクに関連したログ エントリの一覧を含む［**ログ**］『ページ参照 233』ビューが表示されます。
計画またはタスクの実行	**バックアップ計画** ［**実行**］をクリックします。 **[バックアップ計画の実行]**『ページ参照 229』ウィンドウで、実行するタスクを選択します。 バックアップ計画を実行すると、その計画から選択したタスクがスケジュールや条件にかかわらず直ちに開始されます。 **タスク** ［**実行**］をクリックします。 タスクは、スケジュールや条件にかかわらず直ちに実行されます。

計画またはタスクの停止	**バックアップ計画** ［**停止**］をクリックします。 実行中のバックアップ計画を停止すると、そのタスクがすべて停止されます。したがって、すべてのタスク処理は中断されます。 **タスク** ［**停止**］をクリックします。 *タスクを停止した場合の動作* 一般に、タスクを停止すると、その処理(バックアップ、復元、ベリファイ、エクスポート、変換、移行)が中断されます。タスクの状態は、まず［停止中］に変化し、次に［アイドル］になります。タスクのスケジュール(作成されている場合)は、引き続き有効です。処理を完了するには、タスクを再実行する必要があります。 • 復元タスク(ディスク バックアップから): ターゲット ボリュームは削除され、その領域は未割り当てになります。復元が正常終了しなかった場合も同じ結果になります。「失われた」ボリュームを復元するには、タスクを再実行する必要があります。 • 復元タスク(ファイル バックアップから): 中断された処理によって、復元先のフォルダが変更される可能性があります。タスクをどの時点で停止したかによって、復元されるファイルと復元されないファイルが発生します。すべてのファイルを復元するには、タスクを再実行する必要があります。
計画またはタスクの編集	**バックアップ計画** ［**編集**］をクリックします。 バックアップ計画の編集は、作成『ページ参照 236』のときと同じ方法で行いますが、次の**制限事項**があります。 作成されたアーカイブが空ではない(つまり、バックアップが含まれる)場合は、バックアップ スキームのプロパティを変更できないことがあります。 1 バックアップ スキームを GFS(Grandfather-Father-Son)またはハノイの塔に変更できない。 2 ハノイの塔スキームを使用すると、レベル数を変更できない。 他のすべての場合は、バックアップ スキームの変更が可能で、既存のアーカイブが新しいバックアップ スキームで作成されているかのように機能します。空のアーカイブでは、すべての変更が可能です。 *バックアップ計画を編集できない理由* • バックアップ計画が現在実行中である 現在実行中のバックアップ計画は編集できません。 • バックアップ計画が集中管理されている 集中管理用バックアップ計画を直接編集することはできません。元のバックアップ ポリシーを編集する必要があります。 **タスク** ［**編集**］をクリックします。

	タスクを編集できない理由 • タスクがバックアップ計画に属している 直接編集できるのは、復元タスクなど、バックアップ計画に属していないタスクだけです。ローカルのバックアップ計画に属しているタスクを変更する必要がある場合は、バックアップ計画を編集します。集中管理用バックアップ計画に属しているタスクは、その計画の生成元である集中管理ポリシーを編集することで変更できます。
計画またはタスクの削除	**バックアップ計画** **［削除］**をクリックします。 *バックアップ計画を削除した場合の動作* 計画を削除すると、そのタスクはすべて削除されます。 *バックアップ計画を削除できない理由* • バックアップ計画の状態が「実行中」である バックアップ計画のタスクが 1 つ以上実行されている場合は、そのバックアップ計画を削除することはできません。 • バックアップ計画が集中管理されている 集中管理用計画は、管理サーバーの管理者が、その計画の生成元であるバックアップ ポリシーを取り消すことによって削除できます。 **タスク** **［削除］**をクリックします。 *タスクを削除できない理由* • タスクがバックアップ計画に属している バックアップ計画に属しているタスクは、計画と別に削除することはできません。計画を編集してタスクを削除するか、計画全体を削除します。
テーブルの更新	**［更新］**をクリックします。 管理コンソールにより、コンピュータに存在するバックアップ計画とタスクの一覧が最新情報で更新されます。一覧はイベントに基づいて自動的に更新されますが、待ち時間があるため、データは管理対象のコンピュータから直ちに取得されないことがあります。手動で更新すると、確実に最新データが表示されます。

フィルタ処理と並べ替え

バックアップ ポリシーのフィルタ処理と並べ替えは、直接管理の**［バックアップの計画およびタスク］**ビューと同じ方法で実行します。詳細については、「バックアップ計画およびタスクのフィルタ処理と並べ替え『ページ参照 229』」をご参照ください。

グループ

このタブは、選択したコンピュータが 1 つ以上のカスタム グループに追加されている場合にのみ表示され、コンピュータがメンバになっているグループの一覧が表示されます。

操作

目的	操作手順
グループの詳細の表示	 **［詳細の表示］**をクリックします。 ［グループの詳細］ウィンドウが表示され、このグループに関するすべての情報を参照することができます。
グループに関連付けられているタスクの表示	 **［タスクの表示］**をクリックします。 ［タスク］ビューが表示され、選択したバックアップ グループに関連付けられている事前にフィルタ処理されたタスクが表示されます。
グループに関連付けられているログの表示	 **［ログの表示］**をクリックします。 ［ログ］ビューが表示され、選択したグループの事前にフィルタ処理されたログ エントリが表示されます。
グループからのコンピュータの削除	 **［削除］**をクリックします。 親グループに配置された集中管理計画がこのコンピュータに適用されなくなります。

継承順序

［継承順序］ウィンドウで、コンピュータに適用されるポリシーの適用元を確認することができます。

コンピュータに直接適用されるポリシーは次のように表示されます。
 **コンピュータ名**

継承によってコンピュータに適用されるポリシーは次の例のように表示されます。
Group1 >  **Group2** > Group3 > Machine1

ルートにある *Group1* は、ポリシーが直接適用される *Group2* を含んでいます。*Group2* は、親からポリシーを継承して、*Machine1* にポリシーを個々に適用する子の *Group3* を含んでいます。

ポリシーが直接適用されるコンピュータ（またはグループ）は、太字で表示され、アイコンでマークが付けられます。

すべての項目は対話式で操作可能で、コンピュータまたはグループをクリックすると、その親グループのビューが開かれます。

コンピュータのフィルタ処理と並べ替え

目的	操作手順
項目を基準としたコンピュータの並べ替え	コンピュータを昇順で並べ替えるには、項目のヘッダーをクリックします。 再度クリックすると、コンピュータは降順で並べ替えられます。
名前を基準としたコンピュータのフィルタ処理	対応する項目のヘッダーの下にあるフィールドにコンピュータの名前を入力します。 この結果、名前が入力した値と完全に一致するか、部分的に一致するコンピュータの一覧が表示されます。

ステータス、前回の接続、前回のバックアップ、アベイラビリティーを基準としたコンピュータのフィルタ処理	対応する項目のヘッダーの下にあるフィールドで、一覧から必要な値を選択します。

コンピュータ テーブルの設定

デフォルトでは、テーブルには 5 つの項目が表示され、他は非表示になっています。必要に応じて、表示されている項目を非表示にしたり、非表示の項目を再表示することができます。

列を表示または非表示にする手順は、次のとおりです。

1. 項目のヘッダーを右クリックしてコンテキスト メニューを開きます。チェックボックスをオンにしたメニュー項目が、表のヘッダー項目に表示されます。
2. 表示/非表示を切り換える項目をクリックします。

7.1.3.2. グループの操作

[ナビゲーション] ツリーで **[物理コンピュータ]** を選択し、グループをクリックしたときに操作を実行できます。

選択したグループの操作を実行するためのガイドラインを次に示します。

目的	操作手順
カスタム静的グループまたはダイナミック グループの作成	**[グループの作成]** をクリックします。 **[グループの作成]** 『ページ参照 359』ウィンドウで、グループの必要なパラメータを指定します。 ルート フォルダ内(**物理コンピュータ**)またはカスタム グループ内にカスタム グループを作成することができます。
グループにバックアップ ポリシーを適用します。	**[バックアップ ポリシーの適用]** をクリックします。 **[ポリシーの選択]** 『ページ参照 351』ウィンドウで、選択したグループに適用する必要があるバックアップ ポリシーを指定します。選択したグループ内に子グループがある場合、バックアップ ポリシーは子グループにも適用されます。
グループの詳細情報の表示	**[詳細の表示]** をクリックします。 **[グループの詳細]** 『ページ参照 361』ウィンドウで、選択したグループの情報を確認します。
カスタム グループ/サブグループの名前の変更	**[名前の変更]** をクリックします。 **[名前]** 項目に選択したグループの新しい名前を入力します。 ビルトイン グループの名前を変更することはできません。
カスタム グループの編集	**[編集]** をクリックします。 **[グループの編集]** 『ページ参照 361』ウィンドウで、グループの必要なパラメータを変更します。

別のグループへのカスタム グループの移動	 **［移動先］**をクリックします。 **［グループへの移動］**『ページ参照 361』ウィンドウで、選択したグループの新しい親になるグループを指定します。
カスタム グループの削除	 **［削除］**をクリックします。 親グループを削除すると、その子グループも削除されます。親グループに適用され、子グループによって継承されるバックアップ ポリシーが、削除されるグループのすべてのメンバから取り消されます。メンバに直接適用されるポリシーは残ります。
グループの一覧の更新	 **［更新］**をクリックします。 管理コンソールによって、管理サーバーから取得したグループの一覧が最新の情報に更新されます。グループの一覧はイベントに基づいて自動的に更新されますが、待ち時間があるため、データは管理サーバーから直ちに取得されないことがあります。手動で更新すると、確実に最新データが表示されます。

カスタム静的グループまたはダイナミック グループの作成

グループを作成する手順は、次のとおりです。

1. **［名前］**フィールドに作成するグループの名前を入力します。
2. 次のようにグループの種類を選択します。
   a. **［静的］**- 手動で追加するコンピュータを含むグループを作成します。
   b. **［ダイナミック］**- 指定した条件に従って自動的に追加されるコンピュータを含むグループを作成します。

      ［条件の追加］をクリックし、条件のパターンを選択します。
      - **［オペレーティング システム］**
        選択したオペレーティング システムを実行しているすべてのコンピュータがダイナミック グループのメンバになります。
      - **［組織単位］**『ページ参照 360』
        指定した組織単位(OU)に属しているすべてのコンピュータが動的グループのメンバになります。
      - **［IP アドレス範囲］**
        指定した IP アドレスの範囲に含まれる IP アドレスを持つすべてのコンピュータがダイナミック グループのメンバになります。
3. **［コメント］**フィールドに、作成されるグループの説明を入力します。
4. **［OK］**をクリックします。

複数の条件の追加

複数の条件を追加した場合は、次のルールに従って条件が処理されます。

a) 同じ条件のすべての入力項目は論理和(OR)で結合されます。

たとえば、次の条件のセットがあるとします。

オペレーティング システム: Windows Server 2008

オペレーティング システム: Windows Server 2003

この場合、オペレーティング システムが Windows 2000 か Windows 2003 のすべてのコンピュータが同じグループに追加されます。

b) 異なる条件の入力項目は論理積(AND)によって結合されます。

たとえば、次の条件のセットがあるとします。

オペレーティング システム: Windows Server 2008

オペレーティング システム: Windows Server 2003

組織単位: SERVERS

IP アドレス範囲: 192.168.17.0 - 192.168.17.55

この場合、オペレーティング システムが Windows 2000 か Windows 2003 で、SERVERS 組織単位に属し、IP アドレスが 192.168.17.0～192.168.17.55 の範囲に含まれるすべてのコンピュータが同じグループに追加されます。

ダイナミック グループのメンバがグループ内に保持される期間

ダイナミック グループのメンバは、メンバが条件を満たしている限りグループ内に残ります。次の場合は、すぐにメンバがグループから自動的に削除されます。

- メンバが変更されて条件を満たさなくなったとき
- 管理者が条件を変更し、メンバがその条件を満たさなくなったとき

管理サーバーからコンピュータを削除する以外に、ビルトイン グループからコンピュータを手動で削除する方法はありません。

組織単位の条件

組織単位の条件は、管理サーバーが現在属しているドメインに対して *OU=OU1* のように指定します。

たとえば、ドメイン *us.corp.example.com* に OU1 (ルートにある OU) があり、OU1 に OU2 があり、OU2 に OU3 があるとします。この場合、OU3 のコンピュータを追加する必要があります。これにより、条件は *OU=OU3, OU=OU2, OU=OU1* となります。

OU3 に子コンテナがあり、そのコンテナのコンピュータもグループに追加する必要があるときは、**［子コンテナを含める］**チェックボックスをオンにします。

別のグループへのグループの移動

選択したグループを別のグループまたはルートに移動する手順は、次のとおりです。

1. グループ ツリーで、選択したグループの移動先のグループをクリックします。任意の種類のカスタム グループ(静的またはダイナミック)を任意の種類のカスタム グループまたはルート フォルダに移動することができます。

   コンピュータ ツリーのルート フォルダには*最初のレベルのグループ*が含まれています。他のグループを含むグループは、*親グループ*と呼ばれます。親グループ内のグループは、*子グループ*と呼ばれます。親グループに適用されるすべてのバックアップ ポリシーは子グループにも適用されます。

2. **[OK]** をクリックします。

カスタム グループの編集

カスタム グループの編集は、グループの作成『ページ参照 359』と同じ方法で行います。.

グループの種類を変更すると、グループが変換されます。任意のカスタム グループを静的グループからダイナミック グループに変換したり、その逆の変換を行ったりすることができます。

- 静的グループをダイナミック グループに変換するときは、グループの条件を指定します。その静的グループ内に存在している、指定された条件を満たさないすべてのメンバは、ダイナミック グループから削除されます。
- ダイナミック グループを静的グループに変換するときには、現在のグループの内容をそのまま残すか、グループを空にするか、どちらかのオプションを選択できます。

グループの詳細

選択したグループに関するすべての情報が 2 つのタブに集約されます。グループに適用されるポリシーを使用して操作を実行することができます。

この情報は、**[情報]** パネルにも重複して表示されます。

グループ

グループに関する次の情報が表示されます。

- **[名前]** - 選択したグループの名前
- **[親グループ]** (サブグループの場合のみ) - 親グループの名前
- **[コンピュータ]** - グループ内のコンピュータの数
- **[種類]** - グループの種類(静的またはダイナミック)
- **[条件]** (ダイナミック グループの場合のみ) - グループ化の条件
- **[コメント]** - グループの説明(指定した場合)

バックアップ ポリシー

グループに関連付けられているバックアップ ポリシーの一覧が表示され、次の操作を実行することができます。

目的	操作手順
ポリシーの詳細の表示	**［詳細の表示］**をクリックします。 ［ポリシーの詳細］『ページ参照 344』ウィンドウで、選択したバックアップ ポリシーに関連付けられているすべての情報を調べます。
ポリシーのタスクの表示	**［タスクの表示］**をクリックします。 ［タスク］『ページ参照 366』ビューには、選択したバックアップ ポリシーに関連付けられているタスクの一覧が表示されます。
ポリシーのログの表示	**［ログの表示］**をクリックします。 ［ログ］『ページ参照 369』ビューには、選択したバックアップ ポリシーに関連付けられているログ エントリの一覧が表示されます。
グループからのポリシーの取り消し	**［取り消し］**をクリックします。 管理サーバーによってグループからポリシーが取り消されます。変更がコンピュータに転送され、エージェントによってバックアップ計画が削除されている間、グループのポリシーの状態は**［取り消し中］**になります。ポリシー自体は管理サーバー上に残っています。
グループに適用されたポリシーの適用元の確認	**［継承の参照］**をクリックします。 **［継承順序］**『ページ参照 362』ウィンドウに、グループに適用されたポリシーの継承の順序が表示されます。

フィルタ処理と並べ替え

バックアップ ポリシーのフィルタ処理と並べ替えは、［バックアップ ポリシー］ビューと同じ方法で実行します。詳細については、「バックアップ ポリシーのフィルタ処理と並べ替え『ページ参照 343』」をご参照ください。

継承順序

［継承順序］ウィンドウで、グループに適用されるポリシーの適用元を確認することができます。

グループに直接適用されるポリシーは次のように表示されます。
グループ名

次の例は、継承を使用してグループに適用されるポリシーがどのように表示されるかを示しています。
Group1 > **Group2** > Group3

ルートにある *Group1* は、ポリシーが直接適用される *Group2* を含んでいます。*Group2* は、親からポリシーを継承する子の *Group3* を含んでいます。

ポリシーが直接適用されるグループは、太字で表示され、アイコンでマークが付けられます。

すべての項目は対話式で操作可能で、グループをクリックすると、その親グループのビューが開かれます。

7.1.4. ストレージ ノード

Acronis Backup & Recovery 10 ストレージ ノードにより、エンタープライズ データの保護に必要な各種のリソースの使用方法を最適化することができます。これは、エンタープライズ バックアップ アーカイブの専用ストレージとして機能する管理対象の格納域『ページ参照 426』を作成することによって達成されます。

ストレージ ノードによって次のことを実現できます。

- ストレージ ノード側のクリーンアップ『ページ参照 416』およびストレージ ノード側のベリファイ『ページ参照 417』を使用して、管理対象のコンピュータの不要な CPU 負荷を軽減する。
- 重複除外『ページ参照 83』を使用して、バックアップ トラフィックおよびアーカイブによって使用されるストレージ領域を大幅に削減する。
- ストレージ メディアが盗まれたり、悪意を持つ人物がアクセスした場合でも、暗号化された格納域『ページ参照 424』を使用してバックアップ アーカイブへのアクセスを防止する。

Acronis Backup & Recovery 10 ストレージ ノードの詳細については、「Acronis Backup & Recovery 10 ストレージ ノード『ページ参照 23』」をご参照ください。

[ストレージ ノード] ビューの主な要素

- **ツールバーがあるストレージ ノード一覧**

  このツールバーによって、選択したストレージ ノードに操作を実行『ページ参照 364』できます。ストレージ ノード一覧には、管理サーバーに追加されたオンラインおよびオフラインのストレージ ノードが表示されます。さらにストレージ ノードのバックアップとアーカイブの総数も表示されます。
- **情報ペイン**

  選択したストレージ ノードの詳細情報が表示され、圧縮タスクを管理できます。ペインはデフォルトでは折りたたまれています。ペインを展開するには、 をクリックします。ペインの内容は、**[ストレージ ノードの詳細]**『ページ参照 365』ウィンドウにも重複して表示されます。

ストレージ ノードの操作方法(一般的なワークフロー)

1. Acronis Backup & Recovery 10 ストレージ ノードをインストールします。
2. ストレージ ノードへのアクセスを許可する各ユーザーのユーザー アカウントを作成します。

   注意: *ストレージ ノードとユーザーのコンピュータの両方が同じ Active Directory ドメインにある場合は、この手順をスキップできます。*

   ストレージ ノードおよびその管理対象の格納域のユーザー権限については、「ストレージ ノードのユーザー権限『ページ参照 93』」をご参照ください。
3. Acronis Backup & Recovery 10 管理サーバーにストレージ ノードを追加『ページ参照 365』します。

4. 管理対象の格納域を作成します『ページ参照 159』。格納域へのパスを指定し、格納域を管理するストレージ ノードを選択して、重複除外、暗号化などの管理操作を選択します。
5. バックアップ ポリシー『ページ参照 389』または管理対象の格納域を使用するバックアップ計画を作成します。

7.1.4.1. ストレージ ノードの操作

次に説明するすべての操作は、ツールバーの対応するボタンをクリックすると実行されます。これらの操作には、［**ストレージ ノード**］バー(［**アクションとツール**］ペイン)とメイン メニューの［**ストレージ ノード**］項目からアクセスすることもできます。

管理サーバーに追加したストレージ ノードを使用して操作を実行するには、最初にストレージ ノードを選択してください。

ストレージ ノードを使用して操作を実行するためのガイドラインを次に示します。

目的	操作手順
管理サーバーへのストレージ ノードの追加	 ［**追加**］をクリックします。 ［ストレージ ノードの追加］『ページ参照 365』ウィンドウで、ストレージ ノードをインストールするコンピュータを指定します。 ストレージ ノードを追加すると、サーバーにコンピュータを追加する場合と同様に、管理サーバーとストレージ ノードの間に信頼関係が確立されます。ストレージ ノードを管理サーバーに追加すると、ノードに管理対象の格納域を作成できるようになります。
管理サーバーからのストレージ ノードの削除	 ［**削除**］をクリックします。 管理サーバーからストレージ ノードを削除すると、ストレージ ノードによって管理されていた格納域が格納域一覧『ページ参照 153』に表示されなくなり、操作を実行できなくなります。これらの格納域を使用するすべての計画とタスクは失敗します。このストレージ ノードのすべてのデータベースと格納域はそのまま残ります。 削除したストレージ ノードを管理サーバーに再び追加することもできます。その結果、ストレージ ノードが管理するすべての格納域が格納域一覧に表示され、すべての計画とタスクでこれらの格納域を再び使用できるようになります。
選択したストレージ ノードへの集中管理対象の格納域の作成	［**格納域の作成**］をクリックします。 ストレージ ノードが選択された状態で［集中管理用格納域の作成］『ページ参照 159』ページが開きます。残りの手順を実行して格納域を作成します。
圧縮タスクのスケジュールの変更	手動操作時またはクリーンアップ中に重複除外された格納域からバックアップを削除した後で、参照されていないデータが重複除外された格納域およびそのデータベースに表示されることがあります。圧縮手順では、より多くのストレージ領域を確保するために、このようなデータが削除されます。各ストレージ ノードで使用できる圧縮タスクは 1 つだけです。  ［**圧縮の再スケジュール**］をクリックします。 ［**スケジュール**］ウィンドウで、圧縮手順のスケジュールを設定します。設定には、時間イベント(日単位『ページ参照 200』、週単位『ページ参照 203』、および月単位『ページ参照 205』のスケジュール)のみ使用できます。 デフォルトの設定 - **1 週間**に 1 回、**日曜日**の **03:00:00 AM** にタスクを開始する。**一回**だけ。

ストレージ ノードの詳細の表示	**［詳細の表示］**をクリックします。 **［ストレージ ノードの詳細］**『ページ参照 365』ウィンドウで(内容は**［情報］**ペインにも重複して表示されます)、ストレージ ノードの情報およびこのノードによって管理される格納域に関する情報を確認します。タスクの開始と終了を手動で行って圧縮タスクを管理することもできます。
ストレージ ノード一覧の更新	**［更新］**をクリックします。 管理コンソールにより、管理サーバーの最新情報を使用してストレージ ノードの一覧が更新されます。ストレージ ノードの一覧はイベントに基づいて自動的に更新されますが、待ち時間があるため、データは管理サーバーから即座に取得されない場合があります。

ストレージ ノードの追加

ストレージノードを追加する手順は、次のとおりです。

1. **［IP/名前］**フィールドで、ストレージ ノードが存在するコンピュータの名前または IP アドレスを入力するか、**［参照...］**をクリックしてコンピュータのネットワークを参照します。
   ストレージ ノードの完全修飾ドメイン名(FQDN)、つまり、トップレベル ドメインで終了する完全に指定されたドメイン名を使用します。"127.0.0.1" または "localhost" をストレージ ノードの IP または名前として入力しないでください。ストレージ ノードを使用したポリシーが配置されると、各エージェントは、エージェントのホストにインストールされているかのようにストレージ ノードにアクセスしようとするため、管理サーバーとストレージ ノードが同じコンピュータ上にない場合は、これらの設定は適切ではありません。
2. コンピュータに対して有効なユーザー アカウントを設定するには、**［オプション>>］**をクリックして次の項目を指定します。
   - **［ユーザー名］**- Active Directory ユーザー アカウントの名前を入力する場合は、ドメイン名(DOMAIN¥ユーザー名またはユーザー名@ドメイン)も指定してください。ユーザー アカウントは、コンピュータの Administrators グループのメンバでなければなりません。
   - **［パスワード］**- アカウントのパスワード。

   ［パスワードを保存する］チェックボックスをオンにして、アカウントのパスワードを保存します。
3. **［OK］**をクリックします。

登録にはストレージ ノードが必要なので、コンピュータがオフラインのときは登録を実行することはできません。

7.1.4.2. ストレージ ノードの詳細

［ストレージ ノードの詳細］ウィンドウでは、選択した Acronis Backup & Recovery 10 ストレージ ノードに関するすべての情報が 4 つのタブにまとめられています。この情報は、**［情報］**ペインにも重複して表示されます。

ストレージ ノード プロパティ

このタブには、選択したストレージ ノードに関する次の情報が表示されます。

- **[名前]** - ストレージ ノードがインストールされているコンピュータの名前
- **[IP]** - ストレージ ノードがインストールされているコンピュータの IP アドレス
- **[アベイラビリティー]**:
  - **[不明]** - このステータスは、ストレージ ノードの追加後、または管理サーバーのサービスの起動後に、管理サーバーとストレージ ノードの間に最初の接続が確立されるまで表示されます。
  - **[オンライン]** - 管理サーバーは、ストレージ ノードを使用できます。つまり、管理サーバーとノードの最新の接続が成功したことを意味します。接続は、2 分ごとに確立されます。
  - **[オフライン]** - ストレージ ノードは使用できません。
  - **[取り消し]** - ストレージ ノードは、別の管理サーバーに登録されました。その結果、現在の管理サーバーからノードを制御することはできません。
- **[アーカイブ]** - ストレージ ノードによって管理されるすべての格納域に保存されているアーカイブの総数
- **[バックアップ]**- ストレージ ノードによって管理されるすべてのアーカイブに保存されているバックアップの総数

格納域

このタブには、ストレージ ノードによって管理される格納域の一覧が表示されます。

詳しく調べて操作を実行するために管理対象の格納域を開くには、格納域を選択してからタブのツールバーの **[格納域の表示]** をクリックします。**[集中管理用格納域]** 『ページ参照 154』ビューで、必要な操作を実行します。

サービス

このタブには、圧縮タスクのスケジュール パラメータが表示されます。

タスク

このタブで、管理サーバーの管理者は圧縮タスクを管理し、そのパラメータを確認できます。1 つのストレージ ノードに存在できる圧縮タスクは 1 つだけです。

7.1.5. タスク

[タスク] ビューでは、登録済みのコンピュータに存在するタスクを監視および管理できます。タスクの詳細、その状態、および実行結果を表示し、さらにタスクを実行、停止、および削除できます。

コンピュータで現在実行されているタスクを特定するには、タスクの実行状態を確認します。タスクのステータスによって、タスクが正常に実行されたかどうかを確認できます。

タスクの状態とステータスの詳細については、「タスクの状態『ページ参照 223』」および「タスクのステータス『ページ参照 225』」をご参照ください。

タスクの操作方法

- フィルタ処理と並べ替え『ページ参照 369』の機能を使用して、テーブルの目的のタスクを表示します。
- タスクを選択して操作を実行します。

7.1.5.1. タスクの操作

タスクを使用して操作を実行するためのガイドラインを次に示します。

目的	操作手順
タスクの詳細の表示	**[詳細の表示]** をクリックします。 [タスクの詳細]『ページ参照 230』ウィンドウで、選択したタスクに関連するすべての情報を確認します。
タスクのログの表示	**[ログの表示]** をクリックします。 [ログ]『ページ参照 369』ビューに、選択したタスクに関連するログ エントリの一覧が表示されます。
タスクの実行	**[実行]** をクリックします。 タスクは、スケジュールにかかわらず、即座に実行されます。
タスクの停止	**[停止]** をクリックします。 *タスクを停止した場合の動作* 一般に、タスクを停止すると、その処理(バックアップ、復元、ベリファイ、エクスポート、変換、移行)が中断されます。タスクの状態は、まず **[停止中]** に変化し、次に [アイドル] になります。タスクのスケジュール(作成されている場合)は、引き続き有効です。処理を完了するには、タスクを再実行する必要があります。 • **復元タスク(ディスク バックアップから)**: ターゲット ボリュームは削除され、その領域は未割り当てになります。復元が正常終了しなかった場合も同じ結果になります。「失われた」ボリュームを復元するには、タスクを再実行する必要があります。 • **復元タスク(ファイル バックアップから)**: 中断された処理によって、復元先のフォルダが変更される可能性があります。タスクを停止した時期によって、復元されるファイルと復元されないファイルがあります。すべてのファイルを復元するには、タスクを再実行する必要があります。

タスクの編集	**［編集］**をクリックします。 *タスクを編集できない理由* • **タスクがバックアップ計画に属している** 直接編集できるのは、復元タスクなど、バックアップ計画に属していないタスクだけです。ローカルのバックアップ計画に属しているタスクを変更する必要がある場合は、バックアップ計画を編集します。集中管理用バックアップ計画に属しているタスクは、その計画の生成元である集中管理ポリシーを編集することで変更できます。これを実行できるのは、管理サーバーの管理者だけです。 • **適切な権限がない** コンピュータの管理者権限を持たないユーザーは、他のユーザーが所有するタスクを変更することはできません。
タスクの削除	**［削除］**をクリックします。 *タスクを削除できない理由* • **タスクがバックアップ計画に属している** バックアップ計画に属しているタスクは、計画と別に削除することはできません。計画を編集してタスクを削除するか、計画全体を削除します。 • **適切な権限がない** コンピュータの管理者権限を持たないユーザーは、他のユーザーが所有するタスクを削除することはできません。 • **ビルトイン圧縮タスクである** 各ストレージ ノードに、圧縮タスクというビルトイン サービス タスクがあります。このタスクは削除できません。
タスク テーブルの更新	**［更新］**をクリックします。 管理コンソールにより、最新情報を使用してコンピュータに存在するタスクの一覧が更新されます。タスクの一覧はイベントに基づいて自動的に更新されますが、待ち時間があるため、データは管理対象のコンピュータから即座に取得されない場合があります。手動で更新すると、最新データを確実に表示できます。

7.1.5.2. タスクのフィルタ処理と並べ替え

タスクのフィルタ処理と並べ替えを実行するためのガイドラインを次に示します。

目的	操作手順
表示するタスクの数の設定	**[オプション]→[コンソール オプション]→[タスクの数]**『ページ参照 107』を選択し、目的の値を設定します。表示できるタスクの最大数は 500 です。タスクの数が指定した値を超える場合は、フィルタを使用して範囲を超えるタスクを表示します。
項目によるタスクの並べ替え	項目のヘッダーをクリックすると、タスクが昇順で並べ替えられます。 再度クリックすると、タスクは降順で並べ替えられます。
名前、所有者、またはバックアップ計画によるタスクのフィルタ処理	対応する項目のヘッダーの下にあるフィールドにタスクの名前(所有者名、またはバックアップ計画名)を入力します。 その結果、タスク名、所有者名、またはバックアップ計画名の全体または一部が入力された値と一致するタスクの一覧が表示されます。
種類、実行状態、ステータス、ロケーション、前回の結果、スケジュールによるタスクのフィルタ処理	対応するヘッダーの下にあるフィールドで、一覧から必要な値を選択します。

タスク テーブルの設定

デフォルトでは、テーブルに 8 つの項目が表示され、その他の項目は非表示になります。必要に応じて、表示されている項目を非表示にしたり、非表示の項目を再表示することができます。

列を表示または非表示にする手順は、次のとおりです。

1. 項目のヘッダーを右クリックしてコンテキスト メニューを開きます。チェックボックスをオンにしたメニュー項目が、表のヘッダー項目に表示されます。
2. 表示/非表示を切り換える項目をクリックします。

7.1.6. ログ

Acronis Backup & Recovery 10 のログには、ソフトウェアによってコンピュータで実行される操作またはユーザーがソフトウェアを使用してコンピュータで実行する操作の履歴が保存されます。たとえば、ユーザーがタスクを編集すると、ログにエントリが追加されます。ソフトウェアによってタスクが実行されると、現在の実行内容を表す複数のエントリが追加されます。

Acronis Backup & Recovery 10 におけるローカルおよび集中管理のログの記録

Acronis Backup & Recovery 10 には、イベントのローカルおよび集中管理のログがあります。

ローカルのイベント ログ

ローカルのイベント ログには、管理対象のコンピュータにおける Acronis Backup & Recovery 10 の処理に関する情報が含まれます。たとえば、バックアップ計画の作成、バックアップ計画の実行、個人用格納域におけるアーカイブの管理、復元タスクの実行によって、ローカル イベント ログにイベントが記録されます。実際には、ローカル イベント ログはコンピュータに保存されている XML ファイルのコレクションです。管理対象のコンピュータのローカル イベント ログには、コンソールがコンピュータに接続されているときにアクセスできます。ローカル イベントのログの記録を無効にすることはできません。

ブータブル メディアを使用して実行する操作もログに記録されますが、ログの保存期限は現在のセッションに制限されます。再起動するとログは削除されますが、メディアを使用してコンピュータが起動されている間にログをファイルに保存できます。

Acronis Backup & Recovery 10 ストレージ ノードには専用のローカル イベント ログがあります。このログのイベントには、集中管理のログを介してのみアクセスできます。

集中管理のイベント ログ

集中管理のイベント ログには、コンソールが管理サーバーに接続されているときにアクセスできます。集中管理のログでは、管理対象のエンティティ グループの作成、ポリシーの適用、集中管理用格納域の管理などの集中管理操作の履歴、および登録済みのコンピュータとストレージ ノードのローカル ログにログインした操作の履歴を確認できます。

実際には、集中管理のイベント ログは専用 Microsoft SQL データベースのテーブルです。このテーブルには、管理サーバーで発生したイベントのログ エントリおよび集中管理のログ エントリ形式に拡張されたローカル ログ エントリが含まれます。ローカル ログから集中管理のデータベースに収集するエントリの種類を選択できます。またはローカル エントリの収集を無効にすることもできます。詳細については、「ログ レベル『ページ参照 107』」をご参照ください。管理サーバーのイベント ログの記録は、調整することも無効にすることもできません。

SQL Express データベースには 4GB のデータベース サイズの制限があるので、集中管理のイベント ログのログ エントリの数に制限があることに注意してください。

ログ エントリの操作方法

- 集中管理のログに保存されるエントリの最大数は 50,000 です。表示できるエントリの最大数は 10,000 です。ログ エントリの数が 10,000 を超える場合は、フィルタ処理および並べ替えの機能を使用して、テーブルの目的のログ エントリを表示します。不要な項目を非表示にしたり、非表示の項目を再表示することもできます。詳細については、「ログ エントリのフィルタ処理と並べ替え『ページ参照 372』」をご参照ください。
- 操作を実行するログ エントリを選択します(複数選択可能)。詳細については、「ログ エントリの操作『ページ参照 371』」をご参照ください。
- **［情報］**ペインを使用して、選択したログ エントリに関する詳細情報を確認します。ペインはデフォルトでは折りたたまれています。ペインを展開するには、 をクリックします。このペインの内容は、**［ログ エントリの詳細］**『ページ参照 373』ウィンドウにも重複して表示されます。

事前にフィルタ処理されたログ エントリの［ログ］ビューを開く方法

他の管理ビュー(［ダッシュボード］、［コンピュータ］、［バックアップ ポリシー］、［タスク］)で選択した項目がある場合、目的の項目に対してフィルタ処理したログ エントリを含む［ログ］ビューを開くことができます。したがって、ログ テーブルで独自にフィルタを構成する必要はありません。

ビュー	アクション
ダッシュボード	予定表で、強調表示された日付を右クリックし、**［ログの表示］**をクリックします。［ログ］ビューに、既に当該の日付でフィルタ処理されたログ エントリの一覧が表示されます。
コンピュータ	単一のコンピュータまたはコンピュータのグループを選択し、**［ログの表示］**をクリックします。［ログ］ビューに、選択したコンピュータまたはコンピュータのグループに関連するログ エントリの一覧が表示されます。
バックアップ ポリシー	バックアップ ポリシーを選択し、**［ログの表示］**をクリックします。［ログ］ビューに、選択したポリシーに関連するログ エントリの一覧が表示されます。
タスク	タスクを選択し、**［ログの表示］**をクリックします。［ログ］ビューに、選択したタスクに属しているログ エントリが表示されます。

7.1.6.1. ログ エントリの操作

次に説明するすべての操作は、ログの**ツールバー**で対応する項目をクリックすると実行されます。また、すべての操作は、コンテキスト メニュー(ログ エントリを右クリックして表示)、または**［ログ］**アクション バー(**［アクションとツール］**ペイン上)からも実行できます。

ログ エントリの操作を実行するためのガイドラインを次に示します。

目的	操作手順
単一のログ エントリの選択	該当するログ エントリをクリックします。
複数のログ エントリの選択	• *非連続*: **[Ctrl]** キーを押しながら、ログ エントリを 1 つずつクリックします。 • *連続*: 1 つのログ エントリを選択し、次に**［Shift］**キーを押しながら別のエントリをクリックします。最初に選択したエントリと最後に選択したエントリの間にあるすべてのエントリが選択されます。
ログ エントリの詳細の表示	1 ログ エントリを 1 つ選択します。 2 次のいずれかを実行します。 • **［詳細の表示］**をクリックします。そのログ エントリの詳細が別のウィンドウに表示されます。 • ［情報］ペインのボタンをクリックして［情報］ペインを展開します。
選択したログ エントリのファイルへの保存	1 1 つまたは複数のログ エントリを選択します。 2 **［選択項目をファイルに保存］**をクリックします。 3 開いたウィンドウで、ファイルのパスと名前を指定します。

すべてのログ エントリのファイルへの保存	1 フィルタが設定されないようにします。 2  **[すべてをファイルに保存]** をクリックします。 3 開いたウィンドウで、ファイルのパスと名前を指定します。
フィルタ処理されたすべてのログ エントリのファイルへの保存	1 フィルタを設定して、フィルタ条件を満たすログ エントリの一覧を取得します。 2  **[すべてをファイルに保存]** をクリックします。 3 開いたウィンドウで、ファイルのパスと名前を指定します。この結果、その一覧のログ エントリが保存されます。
すべてのログ エントリの削除	 **[ログの消去]** をクリックします。 すべてのログ エントリがログから削除され、新しいログ エントリが作成されます。このエントリには、エントリを削除したユーザーと日時に関する情報が含まれます。
ログ出力レベルの設定	 **ログ出力レベルの設定]** をクリックします。 **[ログ レベル]** 『ページ参照 107』ウィンドウで、登録済みのコンピュータから集中管理のログにログ イベントを収集するかどうかを指定します。

7.1.6.2. ログ エントリのフィルタ処理と並べ替え

ログ エントリのフィルタ処理と並べ替えを実行するためのガイドラインを次に示します。

目的	操作手順
指定した期間のログ エントリの表示	1 **[開始]** フィールドで、表示するログ エントリの開始日を選択します。 2 **[終了]** フィールドで、表示するログ エントリの終了日を選択します。
種類によるログ エントリのフィルタ処理	ツールバーの次のボタンを押すか、放します。  エラー メッセージのフィルタ 警告メッセージのフィルタ  情報メッセージのフィルタ
元のバックアップ計画または管理対象のエンティティの種類によるログ エントリのフィルタ処理	**[バックアップ計画]** (または **[管理対象のエンティティの種類]**)項目のヘッダーで、バックアップ計画または管理対象のエンティティの種類を一覧から選択します。
タスク、管理対象のエンティティ、コンピュータ、コード、所有者によるログ エントリのフィルタ処理	必要な値(タスク名、コンピュータ名、所有者名など)をそれぞれの項目のヘッダーの下にあるフィールドに入力します。 この結果、入力した値と完全に一致するか、部分的に一致するログ エントリの一覧が表示されます。
日時によるログ エントリの並べ替え	ログ エントリを昇順で並べ替えるには、項目のヘッダーをクリックします。再度クリックすると、ログ エントリは降順で並べ替えられます。

ログ テーブルの設定

デフォルトでは、テーブルに 7 つの項目が表示され、その他の項目は非表示になります。必要に応じて、表示されている項目を非表示にしたり、非表示の項目を再表示することができます。

列を表示または非表示にする手順は、次のとおりです。

1. 項目のヘッダーを右クリックしてコンテキスト メニューを開きます。チェックボックスをオンにしたメニュー項目が、表のヘッダー項目に表示されます。
2. 表示/非表示を切り換える項目をクリックします。

7.1.6.3. 集中管理のログ エントリの詳細

選択したログ エントリに関する詳細情報が表示され、詳細をクリップボードにコピーすることができます。

詳細をコピーするには、**［クリップボードにコピー］**をクリックします。

ログ エントリのデータ フィールド

集中管理のログ エントリには、次のデータ フィールドがあります。

- **［種類］**- イベントの種類(エラー、警告、情報)
- **［日付］**- イベントが発生した日時
- **［ポリシー］** - イベントに関連するバックアップ ポリシー(存在する場合)
- **［タスク］**- イベントに関連するタスク(存在する場合)
- **［管理対象のエンティティの種類］**- イベントが発生した管理対象のエンティティの種類(存在する場合)
- **［管理対象のエンティティ］**- イベントが発生した管理対象のエンティティの名前(存在する場合)
- **［コンピュータ］**- イベントが発生したコンピュータの名前(存在する場合)
- **［コード］**- 空白またはイベントの種類がエラーのときはプログラム エラー コードです。エラー コードは、Acronis サポート サービスが問題を解決するために使用する整数です。
- **［モジュール］**- 空白またはエラーが発生したプログラム モジュールの番号です。Acronis サポート サービスが問題を解決するために使用する整数です。
- **［所有者］**- ポリシー/バックアップ計画の所有者『ページ参照 35』のユーザー名
- **［メッセージ］**- イベントの説明テキスト

コピーしたログ エントリの詳細は、次のような内容になります。

```
---------------------------ログ エントリの詳細---------------------------
種類:                          情報
日時:                          DD.MM.YYYY HH:MM:SS
バックアップ計画:              バックアップ計画名
タスク:                        タスク名
管理対象のエンティティの種類:  コンピュータ
管理対象のエンティティ:        ENTITY_NAME
コンピュータ:                  MACHINE_NAME
メッセージ:
操作の説明
コード:                        12(3x45678A)
モジュール:                    モジュール名
所有者:                        計画の所有者
------------------------------------------------------------------------
```

7.1.7. Acronis Backup & Recovery 10 コンポーネントの設定

Windows で Acronis Backup & Recovery 10 コンポーネントのさまざまなパラメータを設定するには、次の 3 つの方法があります。

- Acronis 管理用テンプレートを使用する。
- グラフィカル ユーザー インターフェイス(GUI)を使用する。
- Windows のレジストリを変更する。

Linux では、管理用テンプレートの使用やレジストリの変更の代わりに、対応するコンフィギュレーション ファイルを編集することによってパラメータを設定します。

管理用テンプレートを使用して設定したいずれかのパラメータの値が、グラフィカル ユーザー インターフェイスを使用して設定した値と異なる場合、テンプレート ベースのパラメータの値が優先され、直ちに有効になります。GUI に表示されるパラメータは、これに従って変更されます。

この後のトピックでは、それぞれの設定方法、および各設定方法によって設定できるパラメータについて説明します。

7.1.7.1. 管理用テンプレートを使用して設定されるパラメータ

Acronis 管理用テンプレートを使用して設定できる Acronis Backup & Recovery 10 コンポーネントのパラメータを次に示します。管理用テンプレートの適用方法については、「Acronis 管理用テンプレートの適用方法『ページ参照 102』」をご参照ください。

管理用テンプレートには、対応するトピックで説明されているように、Acronis Backup & Recovery 10 エージェント、Acronis Backup & Recovery 10 管理サーバー、および Acronis Backup & Recovery 10 ストレージ ノードの設定パラメータが含まれます。

Acronis Backup & Recovery 10 ストレージ ノード

Acronis 管理用テンプレートを使用して設定できる Acronis Backup & Recovery 10 ストレージ ノードのパラメータを次に示します。

[Client Connection Limit]

説明: バックアップまたは復元を実行するエージェントによる、ストレージ ノードへの同時接続数の最大値を指定します。

設定可能な値: **1 ～ 2147483647** の任意の整数

デフォルト値: **10**

Acronis Backup & Recovery 10 エージェントは、バックアップまたは復元の際にストレージ ノードに接続して、管理対象の格納域にアクセスします。**[Client Connection Limit]** パラメータでは、ストレージ ノードが同時に処理できる、このような接続の最大数を設定します。

この制限値に達すると、ストレージ ノードはデータをバックアップするエージェントからの接続を拒否し、そのバックアップ タスクは失敗します。

ただし、ストレージ ノードはデータを復元するエージェントからの接続については、この制限値より最大で 5 つ多い接続を受け入れます。

[Backup Queue Limit]

説明: ストレージ ノードのバックアップ キューの Acronis Backup & Recovery 10 コンポーネントの最大数を指定します。

設定可能な値: **1 ～ 2147483647** の任意の整数

デフォルト値: **50**

バックアップ キューは、接続数が同時接続の最大数に到達したときに、ストレージ ノードへの接続を待機している Acronis Backup & Recovery 10 コンポーネントの一覧です(前のパラメータをご参照ください)。

バックアップ キューのコンポーネントの数が **[Backup Queue Limit]** の値と等しくなったときに、別のコンポーネントが接続を確立しようとすると、ストレージ ノードはキューにそのコンポーネントを入れません。

この場合、コンポーネントのストレージ ノードへの接続は失敗します。コンポーネントが Acronis Backup & Recovery 10 エージェントである場合、対応するバックアップ タスクまたは復元タスクは［失敗］状態で停止します。

[Vault Warnings and Limits]

警告またはエラーがログに記録される、格納域内の空き領域のサイズ(絶対値とパーセント値の両方)を指定します。

このパラメータには、次の設定があります。

［**Vault Free Space Warning Limit**］

説明: 管理対象の格納域の空き領域のサイズを MB 単位で指定します。この値未満になると、ストレージ ノードのログに警告が記録されます。

設定可能な値: **0** ～ **2147483647** の任意の整数

デフォルト値: **200**

格納域の空き領域は、格納域が保存されているディスク ボリュームなどのメディアの空き領域のサイズです。

格納域の空き領域のサイズが［**Vault Free Space Warning Limit**］の値以下になると、問題が発生している格納域を示す警告がストレージ ノードのログに記録されます。ストレージ ノードの警告は、ダッシュボードに表示されます。

［**Vault Free Space Warning Percentage**］

説明: 合計サイズのパーセント値として管理対象の格納域の空き領域のサイズを指定します。この値未満になるとストレージ ノードのログに警告が記録されます。

設定可能な値: **0** ～ **100** の任意の整数

デフォルト値: **10**

格納域の合計サイズは、格納域の空き領域と格納域に含まれるすべてのアーカイブのサイズの合計です。

たとえば、2 つの格納域(格納域 A と格納域 B)の両方がディスク ボリュームに保存されているとします。さらに、格納域 A 内のアーカイブのサイズが 20GB で、格納域 B 内のアーカイブのサイズが 45GB であると仮定します。

このボリュームの空き領域が 5GB の場合は、ボリュームのサイズに関係なく、格納域 A の合計サイズは 20GB+5GB=25GB で、格納域 B の合計サイズは 45GB+5GB=50GB になります。

格納域の空き領域のパーセント値は、格納域の空き領域を格納域の合計サイズで除算したものです。前の例では、格納域 A の空き領域は 5GB÷25GB＝20% で、格納域 B の空き領域は 5GB÷50GB=10% になります。

格納域の空き領域のパーセント値が［**Vault Free Space Warning Percentage**］の値以下になると、問題が発生している格納域を示す警告がストレージ ノードのログに記録されます。ストレージ ノードの警告は、ダッシュボードに表示されます。

注意: *［Vault Free Space Warning Limit］パラメータと［Vault Free Space Warning Percentage］パラメータは、互いに独立しています。いずれかのしきい値に到達するたびに警告が記録されます。*

［**Vault Free Space Error Limit**］

説明: 管理対象の格納域の空き領域のサイズを MB 単位で指定します。この値未満になると、ストレージ ノードのログにエラーが記録され、格納域へのすべてのバックアップが禁止されます。

設定可能な値: **0** ～ **2147483647** の任意の整数

デフォルト値: **50**

格納域の空き領域のサイズが［**Vault Free Space Error Limit**］の値以下になると、ストレージ ノードのログにエラーが記録されます。格納域に対して実行されるバックアップは、格納域の空き領域が制限値より大きくなるまで失敗します。

［**Vault Database Free Space Warning Limit**］

説明: 管理対象の格納域のデータベースを含むボリュームの空き領域のサイズを MB 単位で指定します。この値未満になると、ストレージ ノードのログに警告が記録されます。

設定可能な値: **0 ～ 2147483647** の任意の整数

デフォルト値: **20**

管理対象の格納域のデータベースを含むボリュームの空き領域のサイズが［**Vault Database Free Space Warning Limit**］の値以下になると、問題が発生している格納域を示す警告がストレージ ノードのログに記録されます。ストレージ ノードの警告は、ダッシュボードに表示されます。

データベースは、格納域の作成時に［**データベースのパス**］で名前を指定した、ローカル フォルダのストレージ ノードに保存されます。

［**Vault Database FreeSpace Error Limit**］

説明: 管理対象の格納域のデータベースを含むボリュームの空き領域のサイズを MB 単位で指定します。この値未満になると、ストレージ ノードのログにエラーが記録され、格納域へのバックアップが禁止されます。

設定可能な値: **0 ～ 2147483647** の任意の整数

デフォルト値: **10**

管理対象の格納域のデータベースを含むディスクの空き領域のサイズが［**Vault Database Free Space Error Limit**］の値以下になると、ストレージ ノードのログにエラーが記録されます。格納域に対して実行されるバックアップは、空き領域のサイズが制限値より大きくなるまで失敗します。

ストレージ ノードのエラーは、ダッシュボードに表示されます。

データベースは、格納域の作成時に［**データベースのパス**］で名前を指定した、ローカル フォルダのストレージ ノードに保存されます。

Acronis Backup & Recovery 10 管理サーバー

Acronis 管理用テンプレートを使用して設定できる Acronis Backup & Recovery 10 管理サーバーのパラメータを次に示します。

［Collecting Logs］

Acronis Backup & Recovery 10 管理サーバーが管理するコンピュータからログ エントリを収集する時期を指定します。

このパラメータには、次の 2 つの設定があります。

［Trace State］

説明: コンポーネントのイベントに関するログ エントリを、登録されたコンピュータから収集するかどうかを指定します。

設定可能な値: **True** または **False**

デフォルト値: **True**

［**Trace Level**］

説明: 収集されるエントリの重大度の最小レベルを指定します。［**Trace Level**］の値以上のレベルであるエントリのみが収集されます。

設定可能な値: **0**(内部イベント)、**1**(デバッグ情報)、**2**(情報)、**3**(警告)、**4**(エラー)、または **5**(重大なエラー)

デフォルト値: **0**(すべてのエントリが収集されます)

［**Windows Event Log**］

Windows のアプリケーション イベント ログに Acronis Backup & Recovery 10 管理サーバーのイベントを記録する時期を指定します。

このパラメータには、次の 2 つの設定があります。

［**Trace State**］

説明: Acronis Backup & Recovery 10 管理サーバーのイベントをイベント ログに記録するかどうかを指定します。

設定可能な値: **True** または **False**

デフォルト値: **False**

［**Trace Level**］

説明: イベント ログに記録するイベントの重大度の最小レベルを指定します。
［**Trace Level**］の値以上のレベルであるイベントのみが収集されます。

設定可能な値: **0**(内部イベント)、**1**(デバッグ情報)、**2**(情報)、**3**(警告)、**4**(エラー)、または **5**(重大なエラー)

デフォルト値: **4**(［**Trace State**］が **True** に設定されている場合、エラーと重大なエラーのみが記録されます)

SNMP

簡易ネットワーク管理プロトコル(SNMP)を使用して通知を送信する、管理サーバーのイベントの種類を指定します。

このパラメータには、次の設定があります。

［**Trace State**］

説明: SNMP 通知を送信するかどうかを指定します。

設定可能な値: **True** または **False**

デフォルト値: **False**

［**Trace Level**］

説明: SNMP 通知を送信するイベントの重大度の最小レベルを指定します。
［**Trace Level**］の値以上のレベルであるイベントに関する通知のみが送信されます。

設定可能な値: **0**(内部イベント)、**1**(デバッグ情報)、**2**(情報)、**3**(警告)、**4**(エラー)、または **5**(重大なエラー)

デフォルト値: **4**(［**Trace State**］が **True** に設定されている場合、エラーと重大なエラーのみが送信されます)

[SNMP Address]

説明: SNMP サーバーのネットワーク名または IP アドレスを指定します。

設定可能な値: 0 ～ 32765 文字の任意の文字列

デフォルト値: 空の文字列

[SNMP Community]

説明: SNMP 通知のコミュニティ名を指定します。

設定可能な値: 0 ～ 32765 文字の任意の文字列

デフォルト値: **public**

[Synchronization]

Acronis Backup & Recovery 10 管理サーバーが登録済みのコンピュータに接続する方法を指定します。この接続により、集中管理用ポリシーの展開、ログとバックアップ計画の状態の取得、およびこれに類似した操作が行われます。これらの操作は総称して同期と呼ばれます。

このパラメータには、次の 6 つの設定があります。

[Maximum Connections]

説明: 同時に接続する同期接続の最大数を指定します。

設定可能な値: **1** ～ **500** の任意の整数

デフォルト値: **200**

オンライン登録されたコンピュータの総数が **[Maximum Connections]** の値を超えない場合、これらのコンピュータとの接続は常に保持され、管理サーバーは定期的に各コンピュータとの同期を実行します。

この値を超えている場合、同時接続に割り当てられている数に基づいた数の登録済みコンピュータに接続します。コンピュータの同期が完了すると、管理サーバーはそのコンピュータとの接続を切断し、解放された接続を使用して別のコンピュータと同期します(この操作を繰り返します)。

(注意: 同期の優先度が高いコンピュータとの接続は、多くの場合、常に保持されます。このことについては、この後で説明する「**[Period-High Priority]**」をご参照ください)。

同期接続は、Acronis Backup & Recovery 10 管理サーバーと Acronis Backup & Recovery 10 管理コンソール間の接続などとは関係ありません。

[Maximum Workers]

説明: 同期に使用するスレッドの最大数を指定します。

設定可能な値: **1** ～ **100** の任意の整数

デフォルト値: **30**

管理サーバーの処理では、ワーカー スレッドまたはワーカーと呼ばれる特別なスレッドを使用して、同期のために接続された登録済みのコンピュータの同期を実行します。

各ワーカーは、一度に 1 台ずつコンピュータを同期します。

接続されている同期対象のコンピュータは、利用可能なワーカーを待ちます。このため、実際のワーカー数が接続の最大数を超えることはありません(前の「［**Maximum Connections**］」をご参照ください)。

［Period］(秒単位)

説明: 同期の優先度が標準であるコンピュータ(特に、集中管理されたバックアップ タスクを現在実行していないコンピュータ)の同期を実行する間隔を秒単位で指定します。

設定可能な値: **120** ～ **2147483647** の任意の整数

デフォルト値: **120**

Acronis Backup & Recovery 10 管理サーバーは、利用可能なワーカー スレッドを使用し、標準の優先度の各コンピュータに対して、［**Period**］で指定されている間隔(秒単位)で同期を実行します(前の［**Maximum Workers**］をご参照ください)。

ワーカー スレッドの数が標準の優先度のコンピュータよりも少ない場合、実際の同期の間隔は、このパラメータの値よりも長くなる可能性があります。

［Period-High Priority］(秒単位)

説明: 同期の優先度が高いコンピュータ(特に、集中管理されたバックアップ タスクを現在実行しているコンピュータ)の同期を実行する間隔を秒単位で指定します。

設定可能な値: **15** ～ **2147483647** の任意の整数

デフォルト値: **15**

このパラメータは、この前で説明した［**Period**］パラメータに似ています。

［Real-Time Monitoring］

説明: 登録されたコンピュータに対して、ポーリング メカニズムを使用する代わりにリアルタイム監視を実行するかどうかを指定します。

設定可能な値: **True** または **False**

デフォルト値: **False**

デフォルトでは、Acronis Backup & Recovery 10 管理サーバーは、登録されたコンピュータに接続して同期を実行し、主にバックアップ ログなどのデータを取得します。この手法は、ポーリング メカニズムと呼ばれています。

［**Real-Time Monitoring**］を **True** に設定すると、管理サーバーは、新しいデータが出現するたびにそれを提供するようコンピュータに要求を送信し、この後でリッスン モードに入ります。この手法は、リアルタイム監視と呼ばれています。

集中管理されたバックアップ タスクの実行頻度が少ない場合などは、リアルタイム監視によってネットワーク トラフィックが減少する可能性があります。ただし、登録されたコンピュータが比較的少ない場合にのみ効果があります。

登録されたコンピュータの数が同時接続の最大数を超えている場合は、リアルタイム監視を有効にしないでください(前の「［**Maximum Connections**］」をご参照ください)。

[Second Connection Attempt]

説明: ホスト名を使用した接続に失敗した後に、前回使用した既知の IP アドレスを使用して登録されたコンピュータに接続するかどうかを指定します。

設定可能な値: **True** または **False**

デフォルト値: **False**

登録されたコンピュータに接続する場合、Acronis Backup & Recovery 10 管理サーバーは、最初にコンピュータのネットワーク名(コンピュータが名前で管理サーバーに追加された場合)を使用します。

[Second Connection Attempt] が **True** に設定されているときにネットワーク名を使用したコンピュータとの接続が失敗すると、管理サーバーはそのネットワーク名に関連付けられた前回の IP アドレスを使用して 2 回目の接続を試行します。

[Second Connection Atempt] は、固定 IP アドレスまたは DHCP のリース期間が長い場合など、コンピュータの IP アドレスは頻繁に変更されることがないが、ネットワークで DNS サーバーとの問題が頻繁に発生している場合にのみ **True** に設定することをお勧めします。

この設定は、IP アドレスによって管理サーバーに追加されたコンピュータには影響しません。

[Offline Period Threshold] (秒単位)

説明: オフラインになっている登録済みのコンピュータへの接続を試行する間隔の最大値を秒単位で指定します。

設定可能な値: **120 ～ 2147483647** の任意の整数

デフォルト値: **1800**

通常、管理サーバーは、登録済みのコンピュータそれぞれに特定の時間間隔で接続します(前の「**[Period]**」および「**[Period-High Priority]**」をご参照ください)。コンピュータがオフラインであることを管理サーバーが検出すると、この間隔の値は 2 倍に変更されます。その後、接続が試行され、オフラインであることが検出されるごとに、**[Offline Period Threshold]** に達するまで間隔の値が 2 倍に変更されます。コンピュータがオンラインに戻った場合、時間間隔は通常に戻ります。

この方法は、管理サーバーのリソースを有効に活用し、ネットワークの負荷を軽減することを目的としています。

Acronis Backup & Recovery 10 エージェント for Windows

Acronis 管理用テンプレートを使用して設定できる Acronis Backup & Recovery 10 エージェントのパラメータを次に示します。

［Licensing］

エージェントがライセンス サーバーでライセンスをチェックする頻度と、ライセンス サーバーなしで操作可能な期間を指定します。

［License Check Interval］(日単位)

説明: Acronis ライセンス サーバーでライセンスが利用可能かどうかを確認する間隔を日単位で指定します。

設定可能な値: **0** ～ **5** の任意の整数

デフォルト値: **1**

Acronis Backup & Recovery 10 エージェントは、ライセンス サーバーにライセンス キーがあるかどうかを定期的に確認します。最初の確認は Acronis Backup & Recovery 10 エージェントが起動されるたびに実行され、その後の確認は［**License Check Interval**］で指定されている間隔(日数)で実行されます。

エージェントがライセンス サーバーに接続できない場合は、エージェントのログに警告が記録されます。この警告は、ダッシュボードに表示されます。

この値を **0** にすると、ライセンスの確認は実行されません。ライセンスがない状態で［**Maximum Time Without License Server**］で指定されている日数が経過すると、Acronis Backup & Recovery 10 の機能が使用できなくなります(次のパラメータをご参照ください)。

この後の「［**License Server Connection Retry Interval**］」もご参照ください。

［Maximum Time Without License Server］(日単位)

説明: Acronis Backup & Recovery 10 の機能が無効化されずに正常に動作する期間を日単位で指定します。

設定可能な値: **0** ～ **60** の任意の整数

デフォルト値: **30**

Acronis ライセンス サーバーが使用できない場合、Acronis Backup & Recovery 10 は、インストール時または前回成功した確認日から数えて［**Maximum Time Without License Server**］で指定した日数だけ、すべての機能を使用できます。

［License Server Connection Retry Interval］(時間単位)

説明: Acronis ライセンス サーバーが使用できない場合に接続を試行する間隔を時間単位で指定します。

設定可能な値: **0** ～ **24** の任意の整数

デフォルト値: **1**

ライセンス キーの確認中に(前の「［**License Check Interval**］」をご参照ください)、Acronis Backup & Recovery 10 エージェントがライセンス サーバーに接続できなかった場合は、［**License Server Connection Retry Interval**］で指定されている間隔(時間数)で再接続を試行します。

この値を **0** にすると、再接続は試行されません。エージェントは［**License Check Interval**］で指定されている間隔によるライセンスの確認のみを行います。

［**License Server Address**］

説明: Acronis ライセンス サーバーのネットワーク名または IP アドレスを指定します。

設定可能な値: 0 ～ 32765 文字の任意の文字列

デフォルト値: 空の文字列

［**Windows Event Log**］

Windows のアプリケーション イベント ログに Acronis Backup & Recovery 10 エージェントのイベントを記録する時期を指定します。

このパラメータには、次の 2 つの設定があります。

［**Trace State**］

説明: エージェントのイベントをイベント ログに記録するかどうかを指定します。

設定可能な値: **True** または **False**

デフォルト値: **False**

［**Trace Level**］

説明: イベント ログに記録するイベントの重大度の最小レベルを指定します。［**Trace Level**］の値以上のレベルであるイベントのみが収集されます。

設定可能な値: **0**(内部イベント)、**1**(デバッグ情報)、**2**(情報)、**3**(警告)、**4**(エラー)、または **5**(重大なエラー)

デフォルト値: **4**(［**Trace State**］が **True** に設定されている場合、エラーと重大なエラーのみが記録されます)

［**SNMP**］

簡易ネットワーク管理プロトコル(SNMP)を使用して通知を送信する、エージェントのイベントの種類を指定します。

このパラメータには、次の設定があります。

［**Trace State**］

説明: SNMP 通知を送信するかどうかを指定します。

設定可能な値: **True** または **False**

デフォルト値: **False**

［**Trace Level**］

説明: SNMP 通知を送信するイベントの重大度の最小レベルを指定します。［**Trace Level**］の値以上のレベルであるイベントに関する通知のみが送信されます。

設定可能な値: **0**(内部イベント)、**1**(デバッグ情報)、**2**(情報)、**3**(警告)、**4**(エラー)、または **5**(重大なエラー)

デフォルト値: **4**(［**Trace State**］が **True** に設定されている場合、エラーと重大なエラーのみが記録されます)

[SNMP Address]

説明: SNMP サーバーのネットワーク名または IP アドレスを指定します。

設定可能な値: 0 ～ 32765 文字の任意の文字列

デフォルト値: 空の文字列

[SNMP Community]

説明: SNMP 通知のコミュニティ名を指定します。

設定可能な値: 0 ～ 32765 文字の任意の文字列

デフォルト値: **public**

Acronis Backup & Recovery 10

管理用テンプレートのこのセクションでは、次の Acronis Backup & Recovery 10 コンポーネントの接続パラメータとイベント トレース パラメータを指定します。

- Acronis Backup & Recovery 10 管理サーバー
- Acronis Backup & Recovery 10 エージェント
- Acronis Backup & Recovery 10 ストレージ ノード

接続パラメータ

[Remote Agent ports]

コンポーネントが他の Acronis コンポーネントとの送受信を行うために使用するポートを指定します。

次のいずれかを選択します。

[Not Configured]

コンポーネントは、デフォルトの TCP ポート番号の 9876 を使用します。

[Enabled]

コンポーネントは、指定したポートを使用します。ポート番号を **[Server TCP Port]** に入力します。

[Disabled]

[Not configured] と同じです。

[Client Encryption options]

コンポーネントがクライアント アプリケーションとして動作する場合に転送されるデータを暗号化するかどうか、および自己署名 SSL 証明書を信頼するかどうかを指定します。

次のいずれかを選択します。

[Not Configured]

コンポーネントは、可能な場合は暗号化を使用し、自己署名 SSL 証明書を信頼するデフォルトの設定を使用します(次のオプションをご参照ください)。

［**Enabled**］

暗号化が有効になります。［**Encryption**］で、次のいずれかを選択します。

［**Enabled**］

データ転送は、サーバー アプリケーションで暗号化が有効になっている場合は暗号化され、無効になっている場合は暗号化されません。

［**Disabled**］

暗号化は無効になり、暗号化を必要とするサーバー アプリケーションとの接続は確立されません。

［**Required**］

データ転送は、サーバー アプリケーションで暗号化が有効になっている場合のみ実行され、暗号化されます(「Server Encryption options」をご参照ください)。

［Authentication parameters］

［**Trust self-signed certificates**］チェックボックスをオンにすると、クライアントは Acronis Backup & Recovery 10 コンポーネントのインストール中に作成される証明書などの自己署名 SSL 証明書を使用するサーバー アプリケーションに接続できます(「SSL 証明書『ページ参照 103』」をご参照ください)。

このチェックボックスは、環境に公開キー基盤(PKI)がある場合を除き、オンにしておく必要があります。

［**Use Agent Certificate Authentication**］で、次のいずれかを選択します。

［**Do not use**］

SSL 証明書の使用は無効になります。SSL 証明書の使用を必要とするサーバー アプリケーションとの接続は確立されません。

［**Use if possible**］

SSL 証明書の使用は有効です。クライアントは、サーバー アプリケーションで SSL 証明書の使用が有効になっている場合はその証明書を使用し、無効になっている場合は使用しません。

［**Always use**］

SSL 証明書の使用は有効です。接続は、サーバー アプリケーションで SSL 証明書の使用が有効になっている場合のみ確立されます。

［**Disabled**］

［**Not configured**］と同じです。

［**Server Encryption options**］

コンポーネントがサーバー アプリケーションとして動作する場合に、転送されるデータを暗号化するかどうかを指定します。

次のいずれかを選択します。

［**Not Configured**］

コンポーネントは、可能な場合は暗号化を使用するデフォルトの設定を使用します(次のオプションをご参照ください)。

［**Enabled**］

暗号化が有効になります。［**Encryption**］で、次のいずれかを選択します。

［**Enabled**］

データ転送は、クライアント アプリケーションで暗号化が有効になっている場合は暗号化され、無効になっている場合は暗号化されません。

［**Disabled**］

暗号化は無効になり、暗号化を必要とするクライアント アプリケーションとの接続は確立されません。

［**Required**］

データ転送は、クライアント アプリケーションで暗号化が有効になっている場合のみ実行され、暗号化されます(「Client Encryption options」をご参照ください)。

［Authentication parameters］

［**Use Agent Certificate Authentication**］で、次のいずれかを選択します。

［**Do not use**］

SSL 証明書の使用は無効になります。SSL 証明書の使用を必要とするクライアント アプリケーションとの接続は確立されません。

［**Use if possible**］

SSL 証明書の使用は有効です。サーバーは、クライアント アプリケーションで SSL 証明書の使用が有効になっている場合はその証明書を使用し、無効になっている場合は使用しません。

［**Always use**］

SSL 証明書の使用は有効です。接続は、クライアント アプリケーションで SSL 証明書の使用が有効になっている場合のみ確立されます。

［**Disabled**］

［**Not configured**］と同じです。

イベント トレースのパラメータ

Windows では、Acronis Backup & Recovery 10 で発生したイベントをイベント ログまたはファイル、あるいはその両方に記録することができます。

各イベントは、次の表に示すように、イベントの重要度に基づいて 0 ～ 5 までのレベルに分けられます。

レベル	名前	説明
0	不明	重大度のレベルが不明または不適切なイベント
1	デバッグ	デバッグの用途で使用するイベント
2	情報	処理の正常終了またはサービスの開始などに関する情報提供を目的としたイベント
3	警告	格納域の空き領域の不足などの差し迫った問題に関するイベント
4	エラー	データまたは機能の消失を発生させたイベント
5	重大	エージェントの処理などの処理を停止させたイベント

イベント トレースのパラメータは、管理用テンプレートの次の設定で指定します。

［File Trace Minimal Level］

説明: ファイルに記録するイベントの重大度の最小レベルを指定します。［**File Trace Minimal Level**］以上のレベルであるイベントのみが収集されます。

設定可能な値:［**Unknown**］から［**Critical**］の任意の重大度レベル、またはイベントを記録しない場合は［**Blocked**］

デフォルト値: **2**(重大度レベルが 2 ～ 5 のイベントが記録されます)

ログ ファイルは、特定のコンポーネントの **%ALLUSERSPROFILE%¥Application Data¥Acronis** フォルダの **Logs** サブフォルダ内にあります。

［Win32 Trace Minimal Level］

説明: システム イベント ログに記録するイベントの重大度の最小レベルを指定します。［**Win32 Trace Minimal Level**］以上のレベルであるイベントのみが収集されます。

設定可能な値:［**Unknown**］から［**Critical**］の任意の重大度レベル、またはイベントを記録しない場合は［**Blocked**］

デフォルト値: **4**(エラーおよび重大なエラーに関するイベントが記録されます)

7.1.7.2. GUI を使用して設定するパラメータ

次のパラメータは、グラフィカル ユーザー インターフェイス(GUI)を使用して設定できます。

- Acronis Backup & Recovery 10 管理サーバー:［**Collecting Logs**］、［**Windows Event Log**］、［**SNMP**］、［**SNMP Address**］、および［**SNMP Community**］
- Acronis Backup & Recovery 10 エージェント:［**Windows Event Log**］、［**SNMP**］、［**SNMP Address**］、および［**SNMP Community**］

これらのパラメータについては、管理用テンプレートを使用した設定に関するトピックで説明されています。

7.1.7.3. Windows レジストリを使用して設定するパラメータ

次の 2 つのパラメータでは、Acronis Backup & Recovery 10 ストレージ ノードの内部データベース(管理対象の格納域に関する情報を含む)のパスを指定します。これらは、レジストリを編集することによってのみ変更できます。

変更する時期

［**DatabasePath**］で指定したフォルダのデータベースは、通常、サイズは小規模ですが、**［TapeDatabasePath］にあるテープ データベースは、テープ ライブラリに数千のアーカイブが存在する場合、サイズが大規模になる可能性があります。このため、テープ データベースはシステム ボリューム以外のボリュームに保存できます。**

パラメータ

重要: *これらのパラメータの変更は推奨されません。パラメータを変更する必要がある場合は、テープまたはテープ以外の対応する管理対象の格納域を作成する前に変更してください。これを行わない場合、これらの格納域に再接続するまで、ストレージ ノードは格納域にアクセスできなくなります。特に重複除外格納域の場合、格納域への再接続にはかなりの時間がかかります。*

［**DatabasePath**］

説明: Acronis Backup & Recovery 10 ストレージ ノードがテープ以外の格納域データベースを保存するフォルダを指定します。

このデータベースには、テープ格納域を除く、ストレージ ノードによって管理される格納域の一覧が含まれます(次のパラメータをご参照ください)。一般的なサイズは、数 KB 以内です。

設定可能な値: 0 ～ 32765 文字の任意の文字列

デフォルト値: **C:¥Program Files¥Acronis¥StorageNode**

レジストリ キー:
HKEY_LOCAL_MACHINE¥SOFTWARE¥Acronis¥ASN¥Configuration¥StorageNode¥DatabasePath

[TapesDatabasePath]

説明: Acronis Backup & Recovery 10 ストレージ ノードがテープ格納域データベースを保存するフォルダを指定します。

このデータベースには、ストレージ ノードによって管理されるテープ格納域の一覧が含まれます。格納域のサイズは、テープ ライブラリに保存されているアーカイブの数に依存しており、100 アーカイブあたり約 10MB です。

設定可能な値: 0 ～ 32765 文字の任意の文字列

デフォルト値: **C:¥Documents and Settings¥All Users¥Application Data¥Acronis¥BackupAndRecovery¥TapeLocation¥**

レジストリ キー:
HKLM¥SOFTWARE¥Acronis¥BackupAndRecovery¥TapeLocation¥TapesDatabasePath

7.2. バックアップ ポリシーの作成

バックアップ ポリシーは、Windows コンピュータと Linux コンピュータの両方に適用できます。

バックアップ ポリシーを作成する手順は、次のとおりです。

[全般]

[ポリシー名]

(オプション)バックアップ ポリシーの一意の名前を入力します。わかりやすい名前にすると他のポリシーと区別することができます。

[ソースの種類]

バックアップする項目の種類として、**[ディスク/ボリューム]** または **[ファイル]** を選択します。

[ポリシーのログイン情報] 『ページ参照 391』

(オプション)ポリシー アカウントのログイン情報は、必要に応じて変更することができます。このオプションにアクセスするには、**[詳細ビュー]** チェックボックスをオンにします。

[コメント]

(オプション)バックアップ ポリシーの説明を入力します。このオプションにアクセスするには、**[詳細ビュー]** チェックボックスをオンにします。

[バックアップの対象]

[バックアップする項目] 『ページ参照 392』

ポリシーの配置先の各コンピュータでバックアップするデータ項目を指定します。各コンピュータのエージェントにより、指定したルールを使用してデータ項目が検索されます。たとえば、選択ルールが［すべてのボリューム］の場合は、コンピュータ全体がバックアップされます。

[アクセス ログイン情報]『ページ参照 397』

(オプション)バックアップ ポリシー アカウントがデータに対するアクセス許可を持っていない場合は、ソース データへのログイン情報を指定します。このオプションにアクセスするには、**[詳細ビュー]**チェックボックスをオンにします。

[除外]『ページ参照 398』

(オプション)バックアップから除外するファイルの種類を設定します。このオプションにアクセスするには、**[詳細ビュー]**チェックボックスをオンにします。

[バックアップ先]

[アーカイブ]『ページ参照 399』

バックアップ アーカイブの保存先のパスとアーカイブ名を指定します。アーカイブ名は保存先の中で一意な名前にすることをお勧めします。保存先は、管理サーバーがポリシーの配置を開始する時点で使用可能な状態になっている必要があります。

[アクセス ログイン情報]『ページ参照 400』

(オプション)バックアップ ポリシー アカウントが保存先に対するアクセス許可を持っていない場合は、保存先のログイン情報を指定します。このオプションにアクセスするには、**[詳細ビュー]**チェックボックスをオンにします。

[アーカイブのコメント]

(オプション)アーカイブのコメントを入力します。このオプションにアクセスするには、**[詳細ビュー]**チェックボックスをオンにします。

バックアップ方法

[バックアップ スキーム]『ページ参照 401』

データのバックアップの実行時期と実行間隔を指定し、作成したバックアップ アーカイブを選択した保存先に保存する期間を定義して、アーカイブのクリーンアップ処理のスケジュールを設定します。GFS(Grandfather-Father-Son)、ハノイの塔などのよく知られた最適化されたバックアップ スキームを使用して、カスタム バックアップ スキームを作成するか、データを 1 回だけバックアップします。

[アーカイブのベリファイ]

[ベリファイの実行時期]

(オプション)ベリファイの実行時期と実行間隔、およびアーカイブ全体またはアーカイブ内の前回のバックアップのどちらをベリファイするかを定義します。

バックアップ オプション

［設定］

(オプション)バックアップの前後に実行するコマンド、バックアップ ストリームに割り当てられるネットワークの最大帯域幅、バックアップ アーカイブの圧縮レベルなどのバックアップ操作のパラメータを設定します。このセクションで何も指定しない場合は、管理サーバーに設定されているデフォルト値『ページ参照 113』が使用されます。

いずれかの設定をデフォルト値から変更すると、新しい行に新しく設定した値が表示されます。設定のステータスが［**デフォルト**］から［**カスタム**］に変更されます。設定を再度変更すると、新しい値がデフォルト値ではない場合に行が表示されます。デフォルト値が設定されると、行は非表示になるので、［**バックアップ ポリシーの作成**］ページのこのセクションには常にデフォルト値と異なる設定のみが表示されます。

すべての設定をデフォルト値にリセットするには、［**デフォルトにリセット**］をクリックします。

バックアップの処理中は、登録されたコンピュータのデフォルトのバックアップ オプションは無視されます。

すべての必要な処理を実行したら、［**OK**］をクリックしてバックアップ ポリシーを作成します。

7.2.1. ［ポリシーのログイン情報］

コンピュータで集中管理タスクを実行するときに使用するログイン情報を指定します。

ログイン情報を指定する手順は、次のとおりです。

1. 次のいずれかを選択します。
   - ［**Acronis サービスのログイン情報を使用する**］
     タスクは、手動で開始されるか、スケジュールに従って実行されるかにかかわらず、Acronis サービス アカウントを使用して実行されます。
   - ［**次のログイン情報を使用する**］
     タスクは、手動で開始されるか、スケジュールに従って実行されるかにかかわらず、ユーザーが指定するログイン情報を使用して実行されます。
     次の項目を指定します。
     - ［**ユーザー名**］- Active Directory ユーザー アカウントの名前を入力する場合は、ドメイン名(DOMAIN¥ユーザー名またはユーザー名@ドメイン)も指定してください。
     - ［**パスワード**］- アカウントのパスワード。
2. ［**OK**］をクリックします。

Acronis サービスのログイン情報の詳細については、「Acronis サービスの権限『ページ参照 95』」をご参照ください。

ユーザー権限に応じて使用可能になる操作の詳細については、「管理対象のコンピュータ上のユーザー権限『ページ参照 34』」をご参照ください。

7.2.2. ［バックアップする項目］

［全般］の［**ソースの種類**］フィールドで選択した、バックアップする項目の選択ルールを指定します。

バックアップするボリュームの選択ルール『ページ参照 392』

バックアップするファイルの選択ルール『ページ参照 395』

7.2.2.1. バックアップするボリュームの選択ルール

ポリシーを適用するコンピュータのバックアップ対象のボリュームに応じて、ボリュームの選択ルールを定義します。

ボリュームの選択ルールを定義する手順は、次のとおりです。

最初の行で、一覧からルールを選択するか、ルールを入力します。別のルールを追加するには、次の空白の行をクリックし、一覧からルールを選択するか、ルールを入力します。入力したルールはプログラムによって記憶され、次回ウィンドウを開いたときに、一覧でこれらのルールを選択することができます。

次の表は、一覧から選択できる定義済みのルールを示しています。

バックアップ対象	**［ボリューム］列の入力**	**［コメント］**
Windows と Linux のボリューム		
すべての ボリューム	入力または選択: **［すべての ボリューム］**	Windows を実行しているコンピュータではすべてのボリュームを表し、Linux を実行しているコンピュータではマウントされているすべてのボリュームを表します。
Windows のボリューム		
ボリューム C:	「**C:¥**」と入力するか、一覧から選択	
システム ボリューム	入力または選択: **［システム ボリューム］**	システム ボリュームには、Windows の起動に必要な、Ntldr、Boot.ini、Ntdetect.com などのハードウェア固有のファイルが格納されています。 コンピュータに複数の Windows オペレーティング システムがインストールされている場合でも、存在するシステム ボリュームは 1 つだけです。

ブート ボリューム	入力または選択: **［ブート ボリューム］**	登録されているコンピュータのブート ボリュームを表します。 ブート ボリュームには、Windows フォルダと Windows オペレーティング システムのサポート ファイルが格納されています(通常、Windows¥System32 フォルダにあります)。システム ボリュームと同じボリュームの場合もあります。 コンピュータに複数のオペレーティング システムがインストールされている場合は、エージェントが動作しているオペレーティング システムのブート ボリュームです。
すべての固定ボリューム	入力または選択: **［固定ボリューム］**	リムーバブル メディア以外のすべてのボリュームを表します。固定ボリュームには、SCSI、ATAPI、TA、SSA、SAS、SATA の各デバイスおよび RAID アレイがあります。
Linux のボリューム		
Linux コンピュータの最初の IDE ハード ディスクにある最初のパーティション	入力または選択: **/dev/hda1**	hda1 は、最初の IDE ハード ディスク ドライブの最初のパーティションの標準デバイス名です。詳細については、「Linux コンピュータに関する注意」をご参照ください。
Linux コンピュータの最初の SCSI ハード ディスクにある最初のパーティション	入力または選択: **/dev/sda1**	sda1 は、最初の SCSI ハード ディスク ドライブの最初のパーティションの標準デバイス名です。詳細については、「Linux コンピュータに関する注意」をご参照ください。
Linux コンピュータの最初のソフトウェア RAID ハード ディスクにある最初のパーティション	入力または選択: **/dev/md1**	md1 は、最初のソフトウェア RAID ドライブの最初のパーティションの標準デバイス名です。詳細については、「Linux コンピュータに関する注意」をご参照ください。

［All Volumes］や［System Volume］などのテンプレートの名前は、大文字と小文字が区別されません。このため、**［All volumes］**、**［all volumes］**などのように入力できます。

注意: *Acronis Backup & Recovery 10 エージェント for ESX/ESXi を使用して仮想コンピュータをバックアップする場合、**［All Volumes］**は使用可能な唯一のテンプレートになります。*

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

サポートされるファイル システムの場合、ディスク バックアップまたはボリューム バックアップで保存されるのは、データが格納されているセクタだけです。これにより、作成されるバックアップのサイズが小さくなり、バックアップと復元の処理速度が向上します。

Windows

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)はバックアップされません。復元後は、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。

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。GPT ボリュームのブート コードはバックアップされません。

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。

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フォルダ、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。

サポートされないファイル システムのボリュームは、セクタ単位でバックアップされます。

Linux コンピュータに関する注意

1 つの集中管理バックアップ ポリシーに Windows ボリュームと Linux ボリューム(パーティション)の両方を含めることができます。

たとえば、Windows コンピュータのボリューム **C:** および Linux コンピュータのパーティション **/dev/hda1** をバックアップするポリシーを設定できます。

Windows と異なり、Linux ではボリューム(パーティション)とフォルダ(ディレクトリ)の間に明確な区別はありません。Linux にはルート パーティション(/で表記)があり、ハード ディスク、ディレクトリ、システム デバイスなどのさまざまな種類の要素を接続(マウント)して、Windows のファイルやフォルダの構造に似たツリーを構成します。

たとえば、3 つのボリューム、つまり第 1 パーティション、第 2 パーティション、および第 3 パーティションに分割した 1 つのハード ディスクを Linux コンピュータに用意します。これらのパーティションは、ツリー内でそれぞれ /dev/hda1、/dev/hda2、および /dev/hda3 として参照できます。たとえば、第 3 パーティションのディスク バックアップを実行するには、**[バックアップするボリュームの選択ルール]** ダイアログボックスの行に「/dev/hda3」と入力します。

また、Linux パーティションはツリー内部の任意の場所にマウントすることができます。たとえば、/dev/hda3 を /home/usr/docs などのツリー内部の "サブディレクトリ" としてマウントできます。この例では、［ボリューム］フィールドに「/dev/hda3」または「/home/usr/docs」と入力して、第 3 パーティションのディスク バックアップを実行することができます。

通常、1 つの集中管理ポリシーを設定して Linux コンピュータのボリューム バックアップを実行するときは、［ボリューム］フィールドに入力するパスを、ディレクトリではなくパーティション(前の例では /dev/hda2 または /home/usr/docs)に対応させます。

Linux パーティションの標準の名前

/dev/hda1 などの名前には、Linux の IDE ハード ディスク パーティションに対する標準の名前付けの方法が適用されています。プレフィックス hd はディスクの種類(IDE)、a はシステムの最初の IDE ハード ディスク、1 はディスクの最初のパーティションを表します。

通常、Linux パーティションの標準の名前は次の 3 つの要素から構成されます。

- ディスクの種類 - hd は IDE ドライブ、sd は SCSI ドライブ、md はソフトウェア RAID ドライブ(たとえば、ダイナミック ボリューム)
- ディスク番号 - a は最初のディスク、b は 2 番目のディスクなど
- ディスク上のパーティション番号 - 1 は最初のパーティション、2 は 2 番目のパーティションなど

ディスクの種類に関係なく、選択したディスクをバックアップできるようにするには、**［バックアップするボリュームの選択ルール］**ダイアログボックスで、それぞれが使用可能なディスクの種類を表す 3 つのエントリを設定します。たとえば、1 つの集中管理ポリシーで各 Linux コンピュータの最初のハード ディスクをバックアップするには、［ボリューム］フィールドに次の行を入力します。

/dev/hda1

/dev/sda1

/dev/mda1

7.2.2.2. バックアップするファイルの選択ルール

ポリシーを適用するコンピュータのバックアップ対象のファイルおよびフォルダに応じて、ファイルの選択ルールを定義します。

ファイルの選択ルールを定義する手順は、次のとおりです。

最初の行で、一覧からルールを選択するか、ルールを入力します。別のルールを追加するには、次の空白の行をクリックし、一覧からルールを選択するか、ルールを入力します。

入力したルールはプログラムによって記憶され、次回ウィンドウを開いたときに、一覧でデフォルトのルールと共にこれらのルールを選択することができます。

Windows

フル パス

バックアップするフォルダおよびファイルを指します。ファイルまたはフォルダへのパスを明示的に指定すると、各コンピュータでこのパスによって正確に示される項目がバックアップされます。

バックアップ対象	[ファイルとフォルダ] 列での入力または選択
D:¥Work フォルダ内の Text.doc ファイル	**D:¥Work¥Text.doc**
C:¥Windows フォルダ	**C:¥Windows**

環境変数

一部の環境変数は、Windows フォルダを指します。フォルダおよびファイルへのフル パスの代わりにこれらの変数を使用すると、コンピュータ上の Windows のインストール先に関係なく、正しい Windows フォルダをバックアップすることができます。

バックアップ対象	[ファイルとフォルダ] 列での入力または選択	[コメント]
Program Files フォルダ	**%PROGRAMFILES%**	Program Files フォルダを指します(C:¥Program Files など)
Windows フォルダ	**%WINDIR%**	Windows がインストールされているフォルダを指します(C:¥Windows など)
• すべてのユーザー プロファイルの共通フォルダ (Windows XP) • すべてのユーザー プロファイル (Windows Vista)	**%ALLUSERSPROFILE%**	• *Windows XP*: すべてのユーザー プロファイルの共通データが格納されているフォルダを指します(C:¥Documents and Settings¥All Users など) • *Windows Vista*: 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を指します (C:¥ProgramData 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することができます。たとえば、コンピュータの Program Files フォルダ内の Acronis フォルダを参照するには、「**%PROGRAMFILES%¥Acronis**」と入力します。

テンプレート

テンプレートは環境変数に似ていますが、既にカスタマイズされています。

バックアップ対象	[ファイルとフォルダ] 列での入力または選択	[コメント]
コンピュータ上のすべてのボリュームのすべてのファイル	**[すべてのファイル]**	コンピュータ上のすべてのボリュームのすべてのファイルを指します。
コンピュータ上にあるすべてのユーザー プロファイル	**[すべてのプロファイル フォルダ]**	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を指します(たとえば、Windows XP では C:¥Documents and Settings¥、Windows Vista では C:¥ProgramData)

Linux

バックアップ対象	[ファイルとフォルダ] 列での入力または選択
/home/usr/docs にマウントされているボリューム /dev/hda3 のテキスト ファイル file.txt	**/dev/hda3/file.txt** または、 **/home/usr/docs/file.txt**
共通ユーザーのホーム ディレクトリ	**/home**
root ユーザーのホーム ディレクトリ	**/root**
すべてのユーザーに関連するプログラムのディレクトリ	**/usr**
システム構成ファイルのディレクトリ	**/etc**

7.2.3. ソースのアクセス ログイン情報

バックアップするデータにアクセスするために必要なログイン情報を指定します。

ログイン情報を指定する手順は、次のとおりです。

1. 次のいずれかを選択します。
   - **[ポリシーの実行アカウントを使用する]**
     [全般] セクションで指定されたバックアップ ポリシー アカウントのログイン情報を使用して、ソース データにアクセスします。
   - **[次のログイン情報を使用する]**
     ユーザーが指定するログイン情報を使用して、そのデータ ソースにアクセスします。ポリシー ログイン情報にデータに対するアクセス許可がない場合は、このオプションを使用します。
     次の項目を指定します。
     - **[ユーザー名]** - Active Directory ユーザー アカウントの名前を入力する場合は、ドメイン名(DOMAIN¥ユーザー名またはユーザー名@ドメイン)も指定してください。
     - **[パスワード]** - アカウントのパスワード。
2. **[OK]** をクリックします。

7.2.4. ［除外］

バックアップから除外するファイルの種類を設定します。たとえば、データベース、隠しファイルと隠しフォルダ、システム ファイルとシステム フォルダ、特定の拡張子が付いたファイルをアーカイブに保存したくない場合があります。

除外するファイルおよびフォルダを指定する手順は、次のとおりです。

次のいずれかのパラメータを設定します。

- **すべての隠しファイルおよびフォルダを除外**

  隠しファイル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。

- **すべてのシステム ファイルおよびフォルダを除外**

  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設定されてい場合、フォルダの内容はシステム属性を設定されていないファイルを含みすべて除外されます。

***attrib** コマンドを使用してファイルまたはフォルダのファイル/フォルダ プロパティ内の属性を表示することができます。詳細については、Windows の［ヘルプとサポート］をご参照ください。*

- **次の条件に一致するファイルを除外**

  一覧内のいずれかの条件(ファイル マスクと呼ばれます)に一致するファイル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。ファイル マスクの一覧を作成するには、**［追加］**、**［編集］**、**［削除］**、および**［すべて削除］**ボタンを使用します。

  1 つ以上のワイルドカード文字(* および ?)をファイル マスク内で使用することができます。

  アスタリスク(*)はファイル名内の 0 個以上の文字の代用として使用します。たとえば、ファイル マスク Doc*.txt は Doc.txt、Document.txt などの文字と一致します。

  疑問符(?)はファイル名内の厳密に 1 文字の代用として使用します。たとえば、ファイルマスク Doc?.txt は Doc1.txt、Docs.txt などのファイルと一致しますが、Doc.txt、Doc11.txt などのファイルとは一致しません。

除外の例

条件	例	説明
名前	File1.log	File1.log という名前のすべてのファイルを除外します。
パス	C:¥Finance¥test.log	C:¥Finance フォルダに置かれている test.log という名前のファイルを除外します。
マスク(*)	*.log	.log 拡張子の付いたすべてのファイルを除外します。
マスク(?)	my???.log	5 文字で最初が「my」で始まる名前のすべての .log ファイルを除外します。

7.2.5. ［アーカイブ］

アーカイブを保存する場所を指定し、新しいバックアップ アーカイブの名前を定義します。

1. アーカイブの保存先の選択

コンピュータのアーカイブを保存する場所を選択します。

- **［すべてのコンピュータのアーカイブを 1 つの場所に保存します］**
  - 集中管理用格納域にアーカイブを保存するには、**［集中管理］**グループを展開し、格納域をクリックします。
  - ネットワーク共有にアーカイブを保存するには、**［ネットワーク フォルダ］**グループを展開し、ネットワーク上の必要なコンピュータを選択して、共有フォルダをクリックします。ネットワーク共有がアクセス ログイン情報を必要とする場合は、それらの情報が要求されます。
  - **FTP** サーバーまたは **SFTP** サーバーにアーカイブを保存するには、対応するグループを展開して目的のサーバーに接続し、アーカイブの保存に使用するフォルダを選択します。

FTP 仕様の原文に記載されているように、FTP サーバーにアクセスするのに必要なログイン情報は、ネットワーク上をテキスト形式で転送されます。このことは、ユーザー名とパスワードが、パケット スニファを使用した盗聴者によって傍受される可能性があることを意味します。

- **［各コンピュータのアーカイブをコンピュータ上の指定されたフォルダに保存します］**

  ［パス］フィールドに、フォルダへのフル パスを入力します。このパスは、ポリシーを適用する各コンピュータに作成されます。
- **［各コンピュータのアーカイブをコンピュータの Acronis セキュア ゾーンに保存します］**

  Acronis セキュア ゾーンは、ポリシーを適用する各コンピュータに作成する必要があります。Acronis セキュア ゾーンを作成する方法については、「Acronis セキュア ゾーンの作成『ページ参照 292』」をご参照ください。

2. アーカイブの名前付け

各コンピュータのデータは、個別のアーカイブにバックアップされます。アーカイブの名前を指定します。

新しいアーカイブに対して共通の名前が生成され、**［名前］**フィールドに表示されます。この名前は、<ポリシー名>_<コンピュータ名>_Archive1 のようになります。自動的に生成された名前が不適切なときは、別の名前を付けてください。

［すべてのコンピュータのアーカイブを 1 つの場所に保存します］を選択したときは、保存先でユニークなアーカイブ名を指定するために変数を使用する必要があります。

1. **［変数を追加］**をクリックし、次を選択します。
   - **<コンピュータ名>** - コンピュータの名前に置き換えられます。
   - **<ポリシー名>** - バックアップ ポリシーの名前に置き換えられます。

この結果、[**名前**] フィールドに次のルールが表示されます。**<コンピュータ名>_<ポリシー名>_Archive1**

たとえば、*SYSTEM_BACKUP* という名前のバックアップ ポリシーを 3 台のコンピュータ(たとえば、*FINDEPT1*、*FINDEPT2*、*FINDEPT3*)に適用すると、ロケーションに次の 3 つのアーカイブが作成されます。

FINDEPT1_SYSTEM_BACKUP_Archive1

FINDEPT2_SYSTEM_BACKUP_Archive1

FINDEPT3_SYSTEM_BACKUP_Archive1

2. [**OK**] をクリックします。

名前は *ArchiveN* のように表示されます(*N* は連番)。保存先に既にアーカイブ *Archive1* が保存されていることが検出されると、自動的に *Archive2* という名前が表示されます。

7.2.6. 場所のアクセス ログイン情報

バックアップ アーカイブの保存先にアクセスするために必要なログイン情報を指定します。これらのログイン情報のユーザー名がアーカイブの所有者と見なされます。

ログイン情報を指定する手順は、次のとおりです。

1. 次のいずれかを選択します。
   - [**ポリシーの実行アカウントを使用する**]

     [全般] セクションで指定されたバックアップ ポリシーのログイン情報を使用して、その場所にアクセスします。
   - [**次のログイン情報を使用する**]

     ユーザーが指定するログイン情報を使用して、その場所にアクセスします。ポリシー ログイン情報に保存先に対するアクセス許可がない場合は、このオプションを使用します。ネットワーク共有またはストレージ ノードに対しては、特別なログイン情報を指定する必要がある場合があります。

     次の項目を指定します。

     - [**ユーザー名**] - Active Directory ユーザー アカウントの名前を入力する場合は、ドメイン名(DOMAIN¥ユーザー名またはユーザー名@ドメイン)も指定してください。
     - [**パスワード**] - アカウントのパスワード。
2. [**OK**] をクリックします。

警告: *FTP 仕様の原文に記載されているように、FTP サーバーにアクセスするのに必要なログイン情報は、ネットワーク上をテキスト形式で転送されます。このことは、ユーザー名とパスワードが、パケット スニファを使用した盗聴者によって傍受される可能性があることを意味します。*

7.2.7. バックアップ スキームの選択

次の使用可能なバックアップ スキームのいずれかを選択します。

- **[今すぐバックアップ]** - 手動で開始するためのバックアップ タスクを作成し、作成後すぐにタスクを実行します。
- **[後でバックアップ]** - 手動で開始するためのバックアップ タスクを作成するか、将来 1 回だけ実行するタスクをスケジュールします。
- **[シンプル]** - データのバックアップの実行時期と実行間隔をスケジュールし、保持のルールを指定します。
- **[GFS(Grandfather-Father-Son)]** - Grandfather-Father-Son(祖父- 父- 息子)のバックアップ スキームを使用します。このスキームでは、1 日に 2 回以上データのバックアップを行うことはできません。日単位のバックアップを実行する曜日を設定し、それらの日の中から週単位または月単位のバックアップの日を選択します。次に、日単位(「Son」と呼ばれます)、週単位(「Father」と呼ばれます)、月単位(「Grandfather」と呼ばれます)のバックアップの保存期間を設定します。期限切れになったバックアップは自動的に削除されます。
- **[ハノイの塔]** - ハノイの塔バックアップ スキームを使用します。バックアップ(セッション)の実行時期と実行間隔をスケジュールし、バックアップ レベル数(最大 16)を選択します。このスキームでは、1 日に複数回データをバックアップすることができます。バックアップ スケジュールを設定し、バックアップ レベルを選択することによって、ロールバック期間(いつでも戻ることができる保証されたセッション数)が自動的に取得されます。自動クリーンアップ メカニズムは、期限切れになったバックアップを削除し、各レベルの最新のバックアップを保持することによって必要なロールバック期間を維持します。
- **[カスタム]** - カスタム スキームを作成して、会社に最適なバックアップ戦略を自由に設定することができます。異なるバックアップの種類に対する複数のスケジュールの指定、条件の追加、保持のルールの指定を行うことができます。

7.2.7.1. 「今すぐバックアップ」スキーム

「**今すぐバックアップ**」スキームでは、ページの下部にある **[OK]** ボタンをクリックするとすぐにバックアップが実行されます。

[バックアップの種類] フィールドで、完全バックアップ、増分バックアップまたは差分バックアップ『ページ参照 37』のどれを作成するかを選択します。

7.2.7.2. 「後でバックアップ」スキーム

「後でバックアップ」スキームでは、指定した日時にバックアップが 1 回だけ実行されます。

次の項目に適切な値を指定します。

バックアップの種類	完全、増分、または差分のいずれかのバックアップの種類を選択します。アーカイブ内に完全バックアップがない場合は、選択に関係なく完全バックアップが作成されます。
日付と時刻	バックアップを開始する日時を指定します。
タスクを手動で開始する	バックアップ タスクをスケジュールする必要がなく後で手動で開始する場合は、このチェックボックスをオンにします。

7.2.7.3. 「シンプル」スキーム

シンプル バックアップ スキームでは、データのバックアップの実行時期と実行間隔のみをスケジュールし、保持のルールを設定します。最初は完全バックアップが作成されます。次のバックアップは増分になります。

シンプル バックアップ スキームを設定するには、次の項目に適切な値を指定します。

バックアップ	バックアップ スケジュール(データのバックアップの実行時期と実行間隔)を設定します。 スケジュールの設定の詳細については、「スケジュール『ページ参照 199』」をご参照ください。
保持のルール	シンプル スキームでは、1 つの保持ルール『ページ参照 46』のみを使用できます。バックアップの保存期間を設定します。

7.2.7.4. 「GFS(Grandfather-Father-Son」スキーム

概要

- 日単位の増分バックアップ、週単位の差分バックアップ、月単位の完全バックアップ
- 週単位および月単位のバックアップのカスタム日付
- 各種類のバックアップのカスタム保存期間

説明

日単位(D)、週単位(W)、および月単位(M)の一連のバックアップを定期的に生成するバックアップ計画を設定すると仮定します。通常は次のような方法でこれを実行します。次の表に、2 か月間のこの計画の例を示します。

	月	火	水	木	金	土	日
1/1 — 1/7	D	D	D	D	W	-	-
1/8 — 1/14	D	D	D	D	W	-	-
1/15 — 1/21	D	D	D	D	W	-	-
1/22 — 1/28	D	D	D	D	M	-	-
1/29 — 2/4	D	D	D	D	W	-	-
2/5 — 2/11	D	D	D	D	W	-	-
2/12 — 2/18	D	D	D	D	W	-	-
2/19 — 2/25	D	D	D	D	M	-	-
2/26 — 3/4	D	D	D	D	W	-	-

日単位のバックアップは、金曜日を除くすべての平日に実行され、金曜日には週単位および月単位のバックアップが実行されます。月単位のバックアップは毎月第 4 金曜日に実行され、週単位のバックアップは他のすべての金曜日に実行されます。

- 月単位(Grandfather)のバックアップは完全バックアップ。
- 週単位(Father)のバックアップは差分。
- 日単位(Son)のバックアップは増分。

パラメータ

GFS(Grandfather-Father-Son)スキームでは、次のパラメータを設定できます。

バックアップの開始時刻:	バックアップを開始する時刻を指定します。デフォルト値は午後 12 時です。
バックアップの実行日:	バックアップを実行する日付を指定します。デフォルト値は平日です。
週単位/月単位:	**[バックアップの実行日]** フィールドで選択した日のうちどの日を週単位または月単位のバックアップ用に予約するかを指定します。月単位のバックアップは毎月 4 番目のその曜日に実行されます。デフォルト値は金曜日です。

バックアップの保存期間:	バックアップをアーカイブ内に保存する期間を指定します。期間は、時間、日、週、月、年で設定できます。月単位のバックアップでは、無期限に保存する場合は［**無期限に保持**］を選択することもできます。 各バックアップの種類のデフォルト値は次のとおりです。 日単位: 1 週間(推奨される最小値) 週単位: 1 か月間(バックアップの保存期間 1 か月は 4 週間と同じです) 月単位: 無期限 週単位のバックアップの保存期間は日単位のバックアップより長くする必要があり、月単位のバックアップの保存期間は週単位のバックアップの保存期間より長くする必要があります。 日単位のバックアップの保存期間を 1 週間以上に設定することをお勧めします。

常に、バックアップは、そのバックアップに直接依存しているすべてのバックアップも削除対象になるまで削除されません。このため、有効期限が数日経過した週単位または月単位のバックアップがアーカイブ内に残っている場合があります。

スケジュールによって最初に日単位または週単位のバックアップが開始される場合は、代わりに完全バックアップが作成されます。

例

先週の各曜日、先月の各週

多くのユーザーが役立つと考える GFS バックアップ スキームについて考えてみましょう。

- 週末を含む毎日ファイルをバックアップする。
- 過去 7 日間の任意の日付のファイルを復元できる。
- 先月の週単位のバックアップにアクセスできる。
- 月単位のバックアップを無期限に保存する。

バックアップ スキームのパラメータを次のように設定できます。

- バックアップの開始時刻: **午後 11:00**
- バックアップの実行日: **毎日**
- 週単位/月単位: **土曜日**(例)
- バックアップの保存期間:
  - 日単位: **1 週間**
  - 週単位: **1 か月**
  - 月単位: **無期限**

結果として、日単位、週単位、月単位のバックアップのアーカイブが作成されます。日単位のバックアップは作成後 7 日間使用できます。たとえば、1 月 1 日(日曜日)の日単位のバックアップは次の 1 月 8 日(日曜日)まで使用できます。1 月 7 日(土曜日)の最初の週単位のバックアップは、2 月 7 日までシステムに保存されます。月単位のバックアップは削除されません。

ストレージの制限

大きなアーカイブを保存するために膨大なサイズの格納域を用意したくない場合は、バックアップの保存期間が短くなるように GFS スキームを設定し、同時に不測のデータ損失が発生した場合に情報を復元できるようにすることができます。

次のような要件があると仮定します。

- 各平日の最後にバックアップを実行する。
- 誤って削除されたかまたは不注意で変更されたファイルを、比較的早期に見つかった場合に復元できる。
- 週単位のバックアップに作成後 10 日間アクセスできる。
- 月単位のバックアップを半年間保存する。

バックアップ スキームのパラメータを次のように設定できます。

- バックアップの開始時刻: **午後 6:00**
- バックアップの実行日: **平日**
- 週単位/月単位: **金曜日**
- バックアップの保存期間:
  - 日単位: **1 週間**
  - 週単位: **10 日**
  - 月単位: **6 か月**

このスキームを使用すると、破損したファイルの以前のバージョンを日単位のバックアップから 1 週間にわたり復元でき、週単位のバックアップに 10 日間アクセスできます。それぞれの月単位の完全バックアップは、作成日から 6 か月間使用できます。

作業スケジュール

非常勤の会計コンサルタントとして、火曜日と木曜日に会社で作業をしているとします。これらの日には、自分のラップトップ コンピュータで会計文書や財務諸表の変更、スプレッドシートの更新などを行います。このデータをバックアップするために、次の作業を行います。

- 火曜日と木曜日に行った財務諸表やスプレッドシートなどに対する変更の追跡(日単位の増分バックアップ)。
- 先月以降のファイルの変更に関する週単位の要約の作成(金曜日の週単位の差分バックアップ)。
- 月単位のファイルの完全バックアップ。

また、日単位のバックアップを含め、最近 6 か月のすべてのバックアップにアクセスできるようにします。

このような目的には、次の GFS スキームが適しています。

- バックアップの開始時刻: **午後 11 時 30 分**
- バックアップの実行日: **火曜日、木曜日、金曜日**
- 週単位/月単位: **金曜日**
- バックアップの保存期間:
  - 日単位: **6 か月**
  - 週単位: **6 か月**
  - 月単位: **5 年**

これで、火曜日と木曜日に日単位の増分バックアップが作成され、金曜日は週単位と月単位のバックアップが実行されます。［**週単位/月単位**］フィールドで［**金曜日**］を選択するには、まず［**バックアップの実行日**］フィールドでその曜日を選択しておく必要があります。

このようなアーカイブを作成すると、作業の最初の日と最後の日の会計文書の比較、すべての文書の 5 年間にわたる履歴の保持などを行うことができます。

次のような少し変わった GFS スキームについて考えてみます。

- バックアップの開始時刻: **午後 12:00**
- バックアップの実行日: **金曜日**
- 週単位/月単位: **金曜日**
- バックアップの保存期間:
  - 日単位: **1 週間**
  - 週単位: **1 か月**
  - 月単位: **無期限**

このスキームでは、バックアップは金曜日にのみ実行されます。これにより、金曜日に週単位または月単位のバックアップが実行され、日単位のバックアップを行う他の曜日は残っていません。そのため、作成される "祖父-父" アーカイブは、週単位の差分バックアップと月単位の完全バックアップのみで構成されます。

GFS を使用するとこのようなアーカイブを作成することもできますが、この状況にはカスタムスキームのほうがより柔軟に対応できます。

7.2.7.5. 「ハノイの塔」スキーム

概要

- 最大 16 レベルの完全バックアップ、差分バックアップ、および増分バックアップ
- 次のレベルのバックアップは、前のレベルのバックアップの 2 倍希薄になる。
- 一度に 1 つ各レベルのバックアップが保存される。
- 新しいバックアップほど密度が高くなる。

パラメータ

ハノイの塔スキームでは、次のパラメータを設定できます。

スケジュール	日単位『ページ参照 200』、週単位『ページ参照 203』、または月単位『ページ参照 205』のスケジュールを設定します。スケジュールのパラメータを設定すると、シンプル スケジュール(例: 1 日おきに午前 10 時にバックアップ タスクを実行する単純な日単位のスケジュール)およびより複雑なスケジュール(例: 1 月 15 日から 3 日おきにタスクを実行し、指定した日の午前 10 時から午後 10 時までの間に 2 時間おきにタスクを繰り返すような複雑な日単位のスケジュール)を作成できます。このように、複雑なスケジュールではスキームを実行するセッションを指定します。下の説明では、「日」を「スケジュールされたセッション」に置き換えることができます。
レベル数	2 から 16 までのバックアップ レベルを選択します。詳細については、以下の例をご参照ください。
ロールバック期間	アーカイブ内でいつでも戻ることができる保証されたセッション数。スケジュールのパラメータと選択したレベル数に応じて自動的に計算されます。詳細については、以下の例をご参照ください。

例

[スケジュール] パラメータを次のように設定します。

- 繰り返し: 1 日に 1 回
- 間隔: 午後 6 時に 1 回のみ

レベル数: 4

このスキームのスケジュールの最初の 14 日間(14 セッション)は次のようになります。同じ数字は同じバックアップ レベルを示します。

1	2	3	4	5	6	7	8	9	10	11	12	13	14
4	1	2	1	3	1	2	1	4	1	2	1	3	1

レベルが異なるバックアップは種類が異なります。

- *最後のレベル*(この場合はレベル4)のバックアップは完全。
- *中間レベル*(2、3)のバックアップは差分。
- *最初のレベル*(1)のバックアップは増分。

クリーンアップ メカニズムにより、各レベルの最新のバックアップのみが保持されます。次に、新しい完全バックアップを作成する前の日である 8 日目のアーカイブの状態を示します。

1	2	3	4	5	6	7	8
4	1	2	1	3	1	2	1

このスキームではデータ ストレージの効率が上がり、現時点に近いほどバックアップの間隔は密となります。4 つのバックアップがあれば、今日、昨日、半週前、または 1 週間前のデータを復元できます。

ロールバック期間

アーカイブ内で戻ることができる日数は、日によって異なります。保証されている最少日数はロールバック期間と呼ばれます。

次の表は、さまざまなレベルのスキームの完全バックアップとロールバック期間を示しています。

レベル数	**完全バックアップの周期**	**復元可能日数**	**ロールバック期間**
2	2 日	1 ～ 2 日	1 日
3	4 日	2 ～ 5 日	2 日
4	8 日	4 ～ 11 日	4 日
5	16 日	8 ～ 23 日	8 日
6	32 日	16 ～ 47 日	16 日

レベルが 1 つ増えると完全バックアップおよびロールバックの期間が 2 倍になります。

復元可能日数が異なる理由を確認するために、もう一度前の例を見てみましょう。

12 日目には次のバックアップがあります(背景が灰色の数字は削除されたバックアップを表します)。

1	2	3	4	5	6	7	8	9	10	11	12
4	1	2	1	3	1	2	1	4	1	2	1

新しいレベル 3 の差分バックアップはまだ作成されていないので、5 日目のバックアップがまだ保存されています。このバックアップは 1 日目の完全バックアップに依存しているので、この完全バックアップも使用可能です。これにより 11 日前まで戻ることが可能になるので、これが最善のシナリオです。

ただし、次の日には、新しい第 3 レベルの差分バックアップが作成され、古い完全バックアップは削除されます。

1	2	3	4	5	6	7	8	9	10	11	12	13
4	1	2	1	3	1	2	1	4	1	2	1	3

これにより、復元可能日は 4 日間のみとなるので、これは最悪のシナリオです。

14 日目の復元可能日は 5 日間です。復元可能日は再び減少に変わるまで後続の日にも増加していきます。

1	2	3	4	5	6	7	8	9	10	11	12	13	14
4	1	2	1	3	1	2	1	4	1	2	1	3	1

ロールバック期間は、最悪の状況でも保証されている日数を示します。4 レベルのスキームの場合は 4 日間です。

7.2.7.6. カスタム バックアップ スキーム

概要

- 各種類のバックアップのカスタム スケジュールと条件
- カスタムのスケジュールと保持ルール

パラメータ

パラメータ	意味
完全バックアップ	完全バックアップを実行するスケジュールと条件を指定します。 たとえば、毎週日曜日の午前 1 時にすべてのユーザーがログオフした後すぐに完全バックアップを実行するように設定することができます。
増分	増分バックアップを実行するスケジュールと条件を指定します。 タスクを実行したときにアーカイブにバックアップが含まれていない場合は、増分バックアップの代わりに完全バックアップが作成されます。
差分	差分バックアップを実行するスケジュールと条件を指定します。 タスクを実行したときにアーカイブに完全バックアップが含まれていない場合は、差分バックアップの代わりに完全バックアップが作成されます。
保持のルール	アーカイブに適用する保持ルールを指定します。 たとえば、6 か月以上経過しているすべてのバックアップを削除するようにクリーンアップ処理を設定することができます。
ルールの適用 (保持のルールが設定されている場合のみ)	保持のルール『ページ参照 46』を適用する時期を指定します。 たとえば、各バックアップ後およびスケジュールされた日時にクリーンアップ処理を実行するように設定することができます。 このオプションは、［**保持のルール**］で少なくとも 1 つの保持のルールを設定している場合のみ使用可能です。

クリーンアップ スケジュール (**［スケジュールに従う］**を選択している場合のみ)	アーカイブ クリーンアップのスケジュールを指定します。 たとえば、各月の最後の日に開始されるようにクリーンアップをスケジュールすることができます。 このオプションは、**［ルールの適用］**で**［スケジュールに従う］**を選択した場合のみ使用可能です。

例

週単位の完全バックアップ

次のバックアップ スキームでは、毎週金曜日の夜に完全バックアップが実行されます。

完全バックアップ: **スケジュール: 週単位、金曜日ごと、午後 10:00**

ここでは、**［完全バックアップ］**の**［スケジュール］**以外のパラメータはすべて空白のままになります。アーカイブ内のすべてのバックアップは無期限に保持されます(アーカイブのクリーンアップは実行されません)。

完全バックアップおよび増分バックアップとクリーンアップ

次のようなスキームを使用したアーカイブは、毎週の完全バックアップと毎日の増分バックアップで構成されます。完全バックアップを開始するには、すべてのユーザーがログオフする必要があります。

完全バックアップ: スケジュール: 週単位、金曜日ごと、午後 10:00

完全バックアップ: 条件: ユーザーのログオフ

増分: スケジュール: 週単位、すべての平日、午後 9:00

さらに、1 年以上経過しているすべてのバックアップをアーカイブから削除し、新しいバックアップを作成する際にクリーンアップを実行します。

保持ルール: 12 か月経過したバックアップを削除

ルールの適用: バックアップ後

デフォルトでは、1 年以上経過している完全バックアップは、これに依存するすべての増分バックアップが削除対象にならない限り削除されません。詳細については、「保持ルール『ページ参照 46』」をご参照ください。

月単位の完全バックアップ、週単位の差分バックアップ、および日単位の増分バックアップとクリーンアップ

この例は、カスタム スキームで利用できるすべてのオプションの使用方法を示しています。

月単位で完全バックアップ、週単位で差分バックアップ、および日単位で増分バックアップを作成するスキームが必要だとします。このときのバックアップ スケジュールは次のようになります。

完全バックアップ: スケジュール: 月単位、毎月の最終日曜日、午後 9:00

増分: スケジュール: 週単位、すべての平日、午後 7:00

差分: スケジュール: 週単位、土曜日ごと、午後 8:00

さらに、バックアップ タスクを開始するための条件を追加することができます。この条件は、それぞれのバックアップの種類の［**条件**］フィールドに設定します。

完全バックアップ: 条件: ロケーションが使用可能

増分: 条件: ユーザーのログオフ

差分: 条件: ユーザーがアイドル状態

これにより、本来は午後 9:00 にスケジュールされている完全バックアップが、実際にはそれより遅く、バックアップ ロケーションが使用できるようになった直後に開始されることがあります。同様に、増分バックアップと差分バックアップのバックアップ タスクはそれぞれ、すべてのユーザーがログオフするまで、およびユーザーがアイドル状態になるまで待機します。

最後に、アーカイブの保持ルールを作成します。作成後 6 か月以内のバックアップのみを保持し、各バックアップ タスクの終了後および毎月の最終日にクリーンアップを実行します。

保持ルール: **6 か月**経過したバックアップを削除

ルールの適用: バックアップ後、スケジュールに従う

クリーンアップ スケジュール: 月単位、毎月の最終日、午後 10:00

デフォルトでは、バックアップは、そのバックアップに依存し、保持する必要があるバックアップがあるときは削除されません。たとえば、完全バックアップが削除の対象となっても、そのバックアップに依存する増分バックアップまたは差分バックアップがあるときは、依存するバックアップもすべて削除できるようになるまで、完全バックアップの削除は延期されます。

詳細については、「保持ルール『ページ参照 46』」をご参照ください。

生成されるタスク

すべてのカスタム スキームは常に 3 つのバックアップ タスクを生成し、保持のルールが指定されている場合はさらにクリーンアップ タスクを生成します。タスクの一覧内で各タスクは［**スケジュール済み**］(スケジュールが設定されている場合)または［**手動**］(スケジュールが設定されていない場合)と表示されます。

スケジュールされているかどうかに関係なく、いつでも任意のバックアップ タスクまたはクリーンアップ タスクを手動で実行することができます。

前の例の冒頭では、完全バックアップのスケジュールのみを設定しました。しかし、それでもスキームにより 3 つのバックアップ タスクが生成され、次の種類のバックアップを手動で開始することができます。

- 完全バックアップを毎週金曜日の午後 10 時に実行する。
- 増分バックアップを手動で実行する。
- 差分バックアップを手動で実行する。

左側のペインの［**バックアップの計画およびタスク**］セクションでタスクの一覧からこれらのバックアップ タスクを選択して、実行できます。

バックアップ スキームで保持のルールも指定している場合は、スキームは 4 つのタスク(3 つのバックアップ タスクと 1 つのクリーンアップ タスク)が生成されます。

7.2.8. ［アーカイブのベリファイ］

バックアップ データが復元可能かどうかを確認するにはベリファイ タスクを設定します。バックアップのベリファイ結果が不合格の場合は、ベリファイ タスクが失敗し、バックアップ計画がのステータスがエラーになります。

ベリファイを設定するには、次のパラメータを指定します。

1. **［ベリファイの実行時期］** - ベリファイを実行する時期を選択します。ベリファイは多くのリソースを使用する処理なので、管理対象のコンピュータのピーク時以外にベリファイを**スケジュール**するのが効果的です。これに対し、ベリファイがデータ保護戦略の主要な部分になっていて、バックアップされたデータに破損がなく正常に復元できるかどうかをすぐに知りたい場合は、バックアップ作成後すぐにベリファイを開始することを検討してください。
2. **［ベリファイの対象］** - アーカイブ全体またはアーカイブ内の前回のバックアップのどちらをベリファイするかを選択します。ファイル バックアップのベリファイでは、バックアップからダミーの復元先に対してすべてのファイルの復元を疑似的に実行します。ボリューム バックアップのベリファイでは、バックアップに保存されているすべてのデータ ブロックのチェックサムを計算します。アーカイブのベリファイでは、すべてのアーカイブのバックアップをベリファイするので、長い時間がかかり多くのシステム リソースを使用する場合があります。
3. **［ベリファイのスケジュール］** (手順 1 でスケジュールに従うように選択した場合のみ表示されます) - ベリファイのスケジュールを設定します。詳細については、「スケジュール『ページ参照 199』」をご参照ください。

用語集

A

Acronis Active Restore

システムの復元の開始直後にシステムをオンラインにする Acronis 独自のテクノロジ。システムはバックアップ『ページ参照 419』から起動して、コンピュータが使用可能になり、必要なサービスを提供できるようになります。 要求された処理に必要なデータが最高の優先度で復元され、それ以外のすべてのデータはバックグラウンドで復元されます。制限事項:

- バックアップは、ローカル ドライブ(ネットワーク ブート以外の BIOS 経由で使用可能なデバイス)に置かれている必要がある。
- Linux イメージでは動作不可。

Acronis セキュア ゾーン

管理対象のコンピュータ『ページ参照 426』内にあるバックアップ アーカイブ『ページ参照 415』を保存するための安全なボリューム。次のような利点があります。

- 同じディスクに保存したバックアップからディスクを復元することができる。
- ソフトウェアの誤動作、ウィルス攻撃、オペレータによるエラーからデータ保護するためのコスト効率のよい便利な方法を提供する。
- 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る。このことは、モバイル ユーザーにとって特に便利です。
- 二重化するバックアップの保存先の主要な場所として使用できる。

制限事項: Acronis セキュア ゾーンは、ダイナミック ディスク『ページ参照 417』上または GPT パーティション スタイルを使用するディスク上に作成することはできません。

Acronis セキュア ゾーンは、個人用格納域『ページ参照 429』と見なされます。

Acronis リカバリ マネージャ(ASRM)

ブータブル エージェント『ページ参照 422』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。Acronis リカバリ マネージャを使用すると、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ブータブル メディアまたはネットワーク接続が不要になります。

Acronis リカバリ マネージャは、モバイル ユーザーにとって特に役に立ちます。障害が発生した場合、ユーザーはコンピュータを再起動し、［Press F11 for Acronis 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の復元を実行します。

制限事項: ダイナミック ディスク『ページ参照 417』上に作成することはできません。LILO や GRUB などのブート ローダーの手動設定が必要です。サードパーティのローダーを再起動する必要があります。

G

GFS(Grandfather-Father-Son; 祖父-父-息子)

バックアップ アーカイブ『ページ参照 420』のサイズと使用できる復元点『ページ参照 429』の数の最適なバランスを保つことを目的としてよく使用されるバックアップ スキーム『ページ参照 420』。GFS を使用すると、直近の数日間については日単位のバックアップから復元し、直近の数週間については週単位のバックアップから復元し、そして過去の任意の時点については月単位のバックアップから復元することができます。

詳細については、「GFS バックアップ スキーム『ページ参照 39』」をご参照ください。

U

Universal Restore(Acronis Backup & Recovery 10 Universal Restore)

異なるハードウェアまたは仮想コンピュータ上での Windows の起動を支援する Acronis 独自のテクノロジ。Universal Restore は、ストレージ コントローラ、マザーボード、チップセットなどのオペレーティング システムの起動にとって重要なデバイスの相違に対応できます。

次の場合は Universal Restore を使用できません。

- Acronis リカバリ マネージャ『ページ参照 413』(F11 を使用)を使用してコンピュータを起動する場合
- 復元されるイメージが Acronis セキュア ゾーン『ページ参照 413』にある場合
- Acronis Active Restore『ページ参照 413』を使用する場合

これは、これらの機能が主に同じコンピュータ上の簡単なデータ復元を目的としているためです。

Universal Restore は Linux を復元する場合は使用できません。

W

Windows プレインストール環境(WinPE)

次のいずれかのカーネルを基にした最小限の Windows システム。

- Windows XP Professional Service Pack 2(PE 1.5)
- Windows Server 2003 with Service Pack 1(PE 1.6)
- Windows Vista(PE 2.0)
- Windows Vista SP1 および Windows Server 2008(PE 2.1)

WinPE は、一般的に、配置、テスト、診断、およびシステム修復のために OEM および企業によって使用されます。コンピュータは、PXE、CD-ROM、USB フラッシュ ドライブ、またはハード ディスクを使用して WinPE を起動できます。WinPE 用 Acronis プラグイン『ページ参照 414』を使用すると、Acronis Backup & Recovery 10 エージェント『ページ参照 415』をプレインストール環境で実行できます。

WinPE 用 Acronis プラグイン

Acronis Backup & Recovery 10 エージェント for Windows のプレインストール環境版。Acronis WinPE ISO ビルダを使用して、WinPE『ページ参照 414』 イメージにプラグインを追加することができます。結果のブータブル メディア『ページ参照 423』を使用すると、任意の PC 互換コンピュータを起動して、オペレーティング システムを使用せずにほとんどの(ある程度の制限がありますが)直接管理『ページ参照 429』操作を実行することができます。GUI を使用してローカルで、またはコンソール『ページ参照 416』を使用してリモートから操作を設定および制御することができます。

アーカイブ

「バックアップ スキーム『ページ参照 420』」をご参照ください。

イメージ

ディスク バックアップ『ページ参照 419』と同じです。

エージェント(Acronis Backup & Recovery 10 エージェント)

データのバックアップと復元を実行し、タスク管理やハード ディスクの操作などの他の管理操作をコンピュータ『ページ参照 416』上で実行できるようにするアプリケーション。

バックアップできるデータの種類はエージェントの種類によって異なります。Acronis Backup & Recovery 10 には、ディスクとファイルをバックアップするためのエージェント、および仮想化サーバー上に存在する仮想コンピュータをバックアップするためのエージェントが含まれています。

エージェント側のクリーンアップ

アーカイブ『ページ参照 415』を生成するバックアップ計画『ページ参照 421』に従って、エージェント『ページ参照 415』によって実行されるクリーンアップ『ページ参照 415』。エージェント側のクリーンアップは管理対象外の格納域『ページ参照 426』で実行されます。

エージェント側のベリファイ

アーカイブ『ページ参照 415』を生成するバックアップ計画『ページ参照 421』に従って、エージェント『ページ参照 415』によって実行されるベリファイ『ページ参照 423』。エージェント側のベリファイは管理対象外の格納域『ページ参照 426』で実行されます。

クリーンアップ

古いバックアップを除去するため、またはアーカイブが特定のサイズを超えないようにするために、バックアップ アーカイブ『ページ参照 420』からバックアップ『ページ参照 420』を削除すること。

クリーンアップには、アーカイブを生成するバックアップ計画『ページ参照 421』によって設定された保持ルールをアーカイブに適用する処理が含まれます。この処理では、アーカイブが最大サイズを超えているかどうか、およびバックアップが期限切れになっているかどうかを確認します。 この結果、保持ルールに違反しているかどうかに応じてバックアップが削除される場合があります。

詳細については、「保持ルール『ページ参照 46』」をご参照ください。

コンソール(Acronis Backup & Recovery 10 管理コンソール)

Acronis エージェント『ページ参照 415』および Acronis Backup & Recovery 10 管理サーバー『ページ参照 429』にリモート アクセスまたはローカル アクセスするためのツール。

管理者は、コンソールを管理サーバーに接続して、バックアップ ポリシー『ページ参照 420』を設定および管理したり、他の管理サーバー機能にアクセスしたりします。つまり、集中管理『ページ参照 426』を実行します。管理者は、コンソールとエージェントの直接接続を使用して直接管理『ページ参照 429』を実行します。

コンピュータ

オペレーティング システムのインストールによって一意に識別される物理コンピュータまたは仮想コンピュータ。複数のオペレーティング システムがインストールされたコンピュータ(マルチブート システム)は、複数のコンピュータと見なされます。

ストレージ ノード(Acronis Backup & Recovery 10 ストレージ ノード)

企業データの保護に必要となる各種リソースの使用を最適化するためのサーバー。これは、管理対象の格納域『ページ参照 426』を作成することによって達成されます。管理者はストレージ ノードによって次のことを実現できます。

- ストレージ ノード側のクリーンアップ『ページ参照 416』およびストレージ ノード側のベリファイ『ページ参照 417』を使用して、管理対象のコンピュータ『ページ参照 426』の不要な CPU 負荷を低減する。
- 非重複化『ページ参照 429』を使用して、バックアップ トラフィックおよびアーカイブ『ページ参照 420』によって使用されるストレージ領域を大幅に削減する。
- ストレージ メディアが盗まれたり、悪意を持つ人物がアクセスした場合でも、暗号化された格納域『ページ参照 424』を使用してバックアップ アーカイブへのアクセスを防止する。

ストレージ ノード側のクリーンアップ

管理対象の格納域『ページ参照 426』に保存されるアーカイブ『ページ参照 420』を生成するバックアップ計画『ページ参照 421』に従って、ストレージ ノード『ページ参照 416』によって実行されるクリーンアップ『ページ参照 415』。エージェント側のクリーンアップ『ページ参照 415』に代わるものとして、ストレージ ノード側のクリーンアップでは運用サーバーに不要な CPU 負荷をかけません。

クリーンアップ スケジュールは、エージェント『ページ参照 415』が存在するコンピュータ『ページ参照 416』上に存在しており、そのコンピュータの時間とイベントを使用するため、スケジュールされた時刻になるかイベントが発生するたびに、エージェントがストレージ ノード側のクリーンアップを開始する必要があります。そのためには、エージェントがオンラインになっている必要があります。

次の表に、Acronis Backup & Recovery 10 で使用されるクリーンアップの種類の概要を示します。

	クリーンアップ	
	エージェント側	**ストレージ ノード側**
適用先	アーカイブ	アーカイブ
開始	エージェント	エージェント
実行	エージェント	ストレージ ノード
スケジュール設定	バックアップ計画	バックアップ計画
保持ルール設定	バックアップ計画	バックアップ計画

ストレージ ノード側のベリファイ

ストレージ ノード『ページ参照 416』によって実行されるベリファイ『ページ参照 423』。管理対象のロケーション『ページ参照 426』に保存するアーカイブ『ページ参照 420』を生成するバックアップ計画『ページ参照 421』に従って実行される。エージェント側のベリファイ『ページ参照 415』に代わるものとして、ストレージ ノード側のベリファイでは運用サーバーに不要な CPU 負荷をかけません。

ダイナミック グループ

管理サーバー『ページ参照 429』が、管理者の指定したメンバシップ条件に従って自動的にメンバを構成するコンピュータ『ページ参照 416』のグループ。Acronis Backup & Recovery 10 では次のメンバシップ条件が提供されています。

- オペレーティング システム
- Active Directory の組織単位
- IP アドレス範囲

コンピュータは、コンピュータがグループの条件を満たす限りダイナミック グループ内に残ります。次の場合は、すぐにコンピュータがグループから自動的に削除されます。

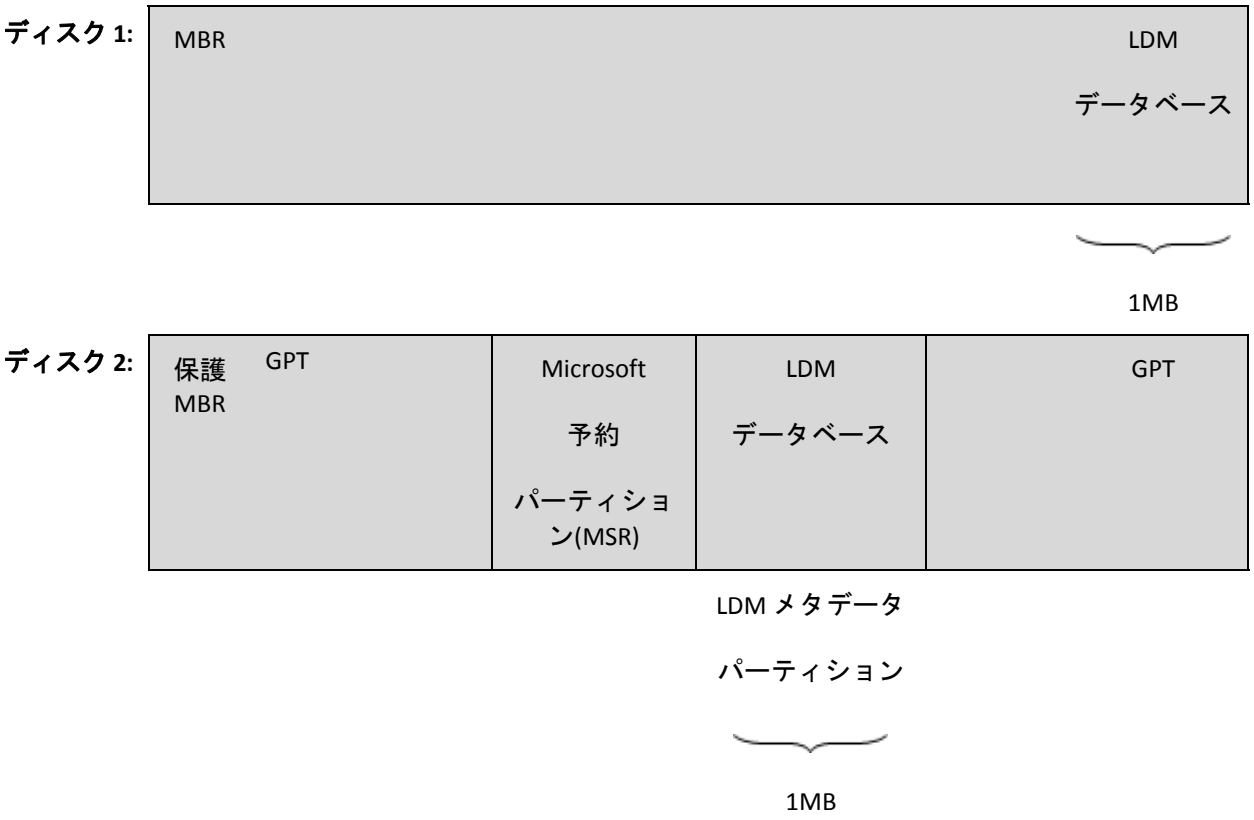
- コンピュータのプロパティが変更され、コンピュータが条件を満たさなくなったとき
- 管理者が条件を変更し、コンピュータがその条件を満たさなくなったとき

管理サーバーからコンピュータを削除する以外に、ビルトイン グループからコンピュータを手動で削除する方法はありません。

ダイナミック ディスク

Windows 2000 以降から提供されている論理ディスク マネージャ(LDM)によって管理されるハード ディスク。LDM を使用すると、ストレージ デバイス上でより柔軟にボリュームを割り当てることができるようになり、フォールト トレランスとパフォーマンスが向上し、ボリューム サイズを大きくすることができます。

ダイナミック ディスクではマスタ ブート レコード(MBR)または GUID パーティション テーブル(GPT)パーティション スタイルを使用できます。MBR または GPT に加えて、各ダイナミック ディスクには LDM がダイナミック ボリュームの設定を保存する隠しデータベースがあります。各ダイナミック ディスクにはディスク グループ内に存在するすべてのダイナミック ボリュームに関する完全な情報が保持され、これによりストレージの信頼性が向上します。このデータベースは、MBR ディスクの最後の 1MB を占有します。GPT ディスク上で、Windows は Microsoft 予約パーティション(MSR)から領域を取得して、専用の LDM メタデータ パーティションを作成します。



MBR(ディスク 1)と GPT(ディスク 2)ディスク上に作成されたダイナミック ディスク。

ダイナミック ディスクの詳細については、次の Microsoft サポート技術情報の記事をご参照ください。

Disk Management (Windows XP Professional Resource Kit)
http://technet.microsoft.com/en-us/library/bb457110.aspx

816307 Windows Server 2003 ベースのコンピュータでのダイナミック ディスクの使用に関する推奨事例 http://support.microsoft.com/kb/816307

ダイナミック ボリューム

ダイナミック ディスク『ページ参照 417』またはより正確にはディスク グループ『ページ参照 419』上にあるボリューム。ダイナミック ボリュームは複数のディスクに分散することができます。ダイナミック ボリュームは通常、次のような目的に応じて設定されます。

- ボリューム サイズを増やす(スパン ボリューム)
- アクセス時間を短縮する(ストライプ ボリューム)
- 冗長性を導入することでフォールト トレランスを実現する(ミラーおよび RAID-5 ボリューム)

タスク

Acronis Backup & Recovery 10 では、タスクは、特定の時刻になるか特定のイベントが発生したときに管理対象のコンピュータ『ページ参照 426』上で実行される一連のアクションのセットです。アクションは xml スクリプト ファイルで記述されます。開始条件(スケジュール)は保護されているレジストリ キー内に存在します。

ディスク グループ

一般的な設定データを LDM データベースに保存して一括管理できるようにする、複数のダイナミック ディスク『ページ参照 417』。通常、同じコンピュータ『ページ参照 416』内で作成されたすべてのダイナミック ディスクは、同じディスク グループのメンバになります。

LDM または別のディスク管理ツールによって最初のダイナミック ディスクが作成されるとすぐに、ディスク グループ名がレジストリ キー HKEY_LOCAL_MACHINE¥SYSTEM¥CurrentControlSet¥Services¥dmio¥Boot Info¥Primary Disk Group¥Name に設定されます。

次に作成またはインポートされるディスクは同じディスク グループに追加されます。少なくとも 1 つのメンバが存在している限り、そのグループは存在します。最後のダイナミック ディスクが切断されるかベーシック ディスクに変換されると、そのグループは使用が中止されますが、その名前は上記のレジストリ キーに保持されます。ダイナミック ディスクが作成または再接続されると、1 つ多い番号を付加した名前のディスク グループが作成されます。

別のコンピュータに移動した場合、ディスク グループは「外部」と見なされ、既存のディスク グループにインポートするまで使用することはできません。インポートによって、ローカル ディスクと外部ディスクの両方の設定データが更新され、1 つのエンティティになります。コンピュータ上にディスク グループが存在していない場合、外部グループはそのままの状態(元の名前)でインポートされます。

ディスク グループの詳細については、次の Microsoft サポート技術情報の記事をご参照ください。

222189 Description of Disk Groups in Windows Disk Management
http://support.microsoft.com/kb/222189/EN-US/

ディスク バックアップ(イメージ)

ディスクまたはボリュームのセクタ ベースのコピーをパッケージした形式のバックアップ『ページ参照 420』。通常は、データを含むセクタのみがコピーされます。Acronis Backup & Recovery 10 では、すべてのディスク セクタをそのままコピーするオプションが用意されています。これにより、サポートされていないファイル システムのイメージ作成が可能になります。

バックアップ

1 回のバックアップ操作『ページ参照 422』の結果。物理的には、特定の日時にバックアップされたデータのコピーを含むファイルまたはテープのレコードです。Acronis Backup & Recovery 10 によって作成されたバックアップ ファイルには TIB 拡張子が付けられます。バックアップの統合『ページ参照 429』の結果の TIB ファイルもバックアップと呼ばれます。

バックアップ アーカイブ(アーカイブ)

バックアップ計画『ページ参照 421』によって管理されているバックアップ『ページ参照 420』のセット。アーカイブには複数の完全バックアップ『ページ参照 425』に加えて、増分バックアップ『ページ参照 428』や差分バックアップ『ページ参照 429』も含めることができます。同じアーカイブに属するバックアップは、常に同じ場所に保存されます。複数のバックアップ計画で同じソースを同じアーカイブにバックアップすることができますが、「1 つのバックアップ計画に対して 1 つのアーカイブを使用する」ことが基本的なシナリオです。

アーカイブ内のバックアップは一般的にバックアップ計画によって管理されます。アーカイブの手動操作(ベリファイ『ページ参照 423』、内容の表示、バックアップのマウントと削除)は、Acronis Backup & Recovery 10 を使用して実行する必要があります。Windows エクスプローラやサードパーティのファイル管理ソフトなどの Acronis 以外のツールを使用してアーカイブを変更しないでください。

バックアップ オプション

バックアップの前後に実行するコマンド、バックアップ ストリームに割り当てるネットワークの最大帯域幅、データ圧縮レベルなどのバックアップ操作『ページ参照 422』の設定パラメータ。バックアップ オプションはバックアップ計画『ページ参照 421』の一部です。

バックアップ スキーム

バックアップ スケジュール、保持ルール(オプション)、およびクリーンアップ『ページ参照 415』スケジュールを含むバックアップ計画『ページ参照 421』の一部。たとえば、次のようなことができます。月末の日の午前 10 時に月単位の完全バックアップ『ページ参照 425』を実行し、日曜日の午後 10 時に増分バックアップ『ページ参照 428』を実行する。3 か月経過したバックアップを削除する。バックアップ操作が完了するたびにそのようなバックアップを確認する。

Acronis Backup & Recovery 10 では、GFS『ページ参照 413』 やハノイの塔『ページ参照 422』などの、有名な最適化されたバックアップ スキームを使用して、カスタム バックアップ スキームや 1 回のデータ バックアップを作成することができます。

バックアップ ポリシー(ポリシー)

管理サーバー『ページ参照 429』の管理者によって作成され、管理サーバーに保存されるバックアップ計画のテンプレート。バックアップ ポリシーには、バックアップ計画と同じルールが含まれていますが、バックアップするデータ項目の内容を明示的に指定していない場合があります。代わりに、環境変数などの選択ルール『ページ参照 428』を使用することができます。この選択の柔軟性により、バックアップ ポリシーを 1 箇所から複数のコンピュータに適用することができます。データ項目が明示的に指定されている場合(/dev/sda または C:¥Windows など)、ポリシーは、この正確なパスが見つかった各コンピュータ上でこの項目をバックアップします。

ポリシーをコンピュータのグループに適用することによって、管理者は、1 回の操作で複数のバックアップ計画を配置できます。

ポリシーを使用する際のワークフローは次のとおりです。

1. 管理者がバックアップ ポリシーを作成します。
2. 管理者がポリシーをコンピュータのグループまたは 1 台のコンピュータ『ページ参照 416』に適用します。
3. 管理サーバーがポリシーをコンピュータに配置します。
4. 各コンピュータ上で、コンピュータにインストールされているエージェント『ページ参照 415』が、選択ルールを使用してデータ項目を検索します。たとえば、選択ルールが［すべてのボリューム］の場合は、コンピュータ全体がバックアップされます。
5. 各コンピュータ上で、コンピュータにインストールされているエージェントが、ポリシーで指定された他のルールを使用してバックアップ計画『ページ参照 421』を作成します。このようなバックアップ計画は集中管理用計画『ページ参照 427』と呼ばれます。
6. 各コンピュータ上で、コンピュータにインストールされているエージェントが、計画を実行する集中管理タスク『ページ参照 427』のセットを作成します。

バックアップ計画(計画)

特定のコンピュータ上で特定のデータを保護する方法を指定したルールのセット。バックアップ計画では次のものを指定します。

- バックアップするデータ
- バックアップ アーカイブ『ページ参照 420』の保存場所(バックアップ アーカイブの名前と保存先)
- バックアップ スケジュールと保持ルール(オプション)を含むバックアップ スキーム『ページ参照 420』
- (オプション)アーカイブのベリファイ ルール『ページ参照 423』
- バックアップ オプション『ページ参照 420』

たとえば、バックアップ計画には次の情報を含めることができます。

- ボリューム C: のバックアップ**(計画によって保護するデータ)**。
- アーカイブに MySystemVolume という名前を付けて ¥¥server¥backups¥ に保存する**(バックアップ アーカイブ名と場所)**。
- 月末の日の午前 10 時に月単位の完全バックアップを実行し、日曜日の午後 10 時に増分バックアップを実行する。3 か月経過したバックアップを削除する**(バックアップ スキーム)**。
- バックアップを作成後すぐにベリファイする**(ベリファイ ルール)**。
- アーカイブをパスワードで保護する**(オプション)**。

物理的には、バックアップ計画は管理対象のコンピュータ『ページ参照 426』上で実行するために設定されるタスク『ページ参照 419』の集まりです。

バックアップ計画はコンピュータ上で直接作成するか（ローカルの計画）、バックアップ ポリシー『ページ参照 420』が配置されている場合は、コンピュータ上に表示することができます(集中管理用計画『ページ参照 427』)。

バックアップ操作

特定の日時のデータを復元するためにコンピュータ『ページ参照 416』のハード ディスク上に存在するデータのコピーを作成する処理。

ハノイの塔

バックアップ アーカイブ『ページ参照 420』のサイズと使用できる復元点『ページ参照 429』の数の最適なバランスを保つことを目的としてよく使用されるバックアップ スキーム『ページ参照 420』です。復元単位が 3 つのレベル(日単位、週単位、月単位)のみの GFS『ページ参照 413』 スキームとは異なり、ハノイの塔スキームは、バックアップの世代数が増えるにつれて、復元点間の時間間隔が短くなります。これにより、バックアップ ストレージを非常に効率よく使用することができます。

詳細については、「ハノイの塔バックアップ スキーム『ページ参照 43』」をご参照ください。

ビルトイン グループ

管理サーバー『ページ参照 429』上に常に存在するコンピュータのグループ。

管理サーバーには、すべての物理コンピュータ『ページ参照 429』とすべての仮想コンピュータ『ページ参照 429』という 2 つのビルトイン グループがあり、それぞれの種類のすべてのコンピュータが含まれています。

ビルトイン グループは削除することも、他のグループに移動することも、手動で変更することもできません。ビルトイン グループ内にカスタム グループを作成することはできません。管理サーバーからコンピュータを削除する以外に、ビルトイン グループから物理コンピュータを削除する方法はありません。仮想コンピュータは、ホスト サーバーを削除すると、結果的に削除されます。

バックアップ ポリシー『ページ参照 420』をビルトイン グループに適用することができます。

ブータブル エージェント

Acronis Backup & Recovery 10 エージェント『ページ参照 415』のほとんどの機能を含むブータブル レスキュー ユーティリティ。ブータブル エージェントは Linux カーネルが基になっています。コンピュータ『ページ参照 416』は、ブータブル メディア『ページ参照 423』または Acronis PXE サーバーを使用してブータブル エージェントを起動できます。GUI を使用してローカルで、またはコンソール『ページ参照 416』を使用してリモートから操作を設定および制御することができます。

ブータブル メディア

ブータブル エージェント『ページ参照 422』または WinPE 用 Acronis プラグイン『ページ参照 414』がインストールされた Windows プレインストール環境(WinPE)『ページ参照 414』を含む物理的なメディア(CD、DVD、USB フラッシュ ドライブ、またはコンピュータ『ページ参照 416』の BIOS によってブート デバイスとしてサポートされるその他のメディア)。コンピュータは、Acronis PXE サーバーまたは Microsoft リモート インストール サービス(RIS)からネットワーク ブートを使用して上記の環境で起動することもできます。ブータブル コンポーネントがアップロードされた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。

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『ページ参照 418』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
- アクセス制限、アプリケーションの実行による連続的なロック、またはその他の原因のために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

ベリファイ

バックアップ『ページ参照 420』からデータを復元できるかどうかを確認する処理。

ファイル バックアップのベリファイでは、バックアップからダミーの復元先に対してすべてのファイルの復元を疑似的に実行します。以前の製品バージョンでは、ファイル バックアップのヘッダーに含まれるメタデータに整合性があれば、バックアップは有効と見なされていました。現在の方法は、時間がかかりますが信頼性が向上しています。ボリューム バックアップのベリファイでは、バックアップに保存されているすべてのデータ ブロックのチェックサムを計算します。この処理も多くのリソースを消費します。

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 ディスク ドライブへの復元テストによってのみ将来の復元の成功が保証されます。

ベリファイ ルール

バックアップ計画『ページ参照 421』の一部。ベリファイ『ページ参照 423』を実行する頻度と時期、およびベリファイする対象がアーカイブ『ページ参照 420』全体か、アーカイブ内の前回のバックアップかを定義するルールです。

ポリシー

「バックアップ ポリシー『ページ参照 420』」をご参照ください。

メディア ビルダ

ブータブル メディア『ページ参照 423』を作成するための専用のツール。

ローカル タスク

ローカルのバックアップ計画『ページ参照 424』に属するタスク『ページ参照 419』、または復元タスクのようにどの計画にも属していないタスク。バックアップ計画に属しているローカル タスクは、計画を編集することによってのみ変更できます。他のローカル タスクは直接変更できます。

ローカルのバックアップ計画

直接管理『ページ参照 429』を使用して管理対象のコンピュータ『ページ参照 426』上に作成されたバックアップ計画『ページ参照 421』。

漢字

暗号化されたアーカイブ

ACE(Advanced Encryption Standard)に従って暗号化されたバックアップ アーカイブ『ページ参照 420』。アーカイブの暗号化オプションとパスワードをバックアップ オプション『ページ参照 420』で設定すると、そのアーカイブに属する各バックアップは、エージェント『ページ参照 415』によって暗号化されてから保存先に保存されます。

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。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 ファイルに保存されませんが、パスワードのハッシュがベリファイには使用されます。この 2 段階のセキュリティにより、バックアップ データは権限のない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。

暗号化された格納域

すべての読み書きが、ストレージ ノード『ページ参照 416』によって透過的に暗号化および暗号化解除される管理対象の格納域『ページ参照 426』。暗号化キーはノードに保存された格納域専用の暗号化キーを使用します。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、格納域の内容はストレージ ノードにアクセスしなければ、暗号化解除することはできません。暗号化されたアーカイブ『ページ参照 429』の暗号化は、エージェント『ページ参照 415』によって実行されます。

仮想コンピュータ

Acronis Backup & Recovery 10 管理サーバーでは、エージェント『ページ参照 415』をコンピュータにインストールせずに、そのコンピュータを仮想ホストからバックアップできる場合、コンピュータ『ページ参照 416』は仮想コンピュータと見なされます。仮想コンピュータ用の Acronis Backup & Recovery 10 エージェントがサーバーにインストールされていることを前提として、仮想コンピュータは、コンピュータをホストする仮想サーバーの登録後に管理サーバー上に表示されます。

格納域

バックアップ アーカイブ『ページ参照 420』を保存する場所。格納域はローカル ドライブ、ネットワーク上のドライブ、または外部 USB ドライブなどの取り外し可能なメディア上に作成することができます。格納域のサイズまたは格納域内のバックアップの数を制限する設定はありません。クリーンアップ『ページ参照 415』を使用して各アーカイブのサイズを制限できますが、格納域に保存するアーカイブの合計サイズはストレージのサイズによってのみ制限されます。

完全バックアップ

バックアップ用に選択されたすべてのデータを含む、それ自体で完結したバックアップ『ページ参照 420』。完全バックアップからデータを復元する場合は、他のバックアップにアクセスする必要はありません。

管理サーバー(Acronis Backup & Recovery 10 管理サーバー)

企業ネットワーク内のデータ保護を管理する中央のサーバー。Acronis Backup & Recovery 10 管理サーバーは、次の機能を管理者に提供します。

- Acronis Backup & Recovery 10 インフラストラクチャへの単一のエントリ ポイント
- バックアップ ポリシー『ページ参照 420』とグループを使用して多数のコンピュータ『ページ参照 416』上のデータを簡単に保護する方法
- 全社規模の監視機能
- 全社のバックアップ アーカイブ『ページ参照 420』を保存するための集中管理用格納域『ページ参照 427』を作成する機能
- ストレージ ノード『ページ参照 416』を管理する機能

ネットワーク上に複数の管理サーバーがある場合、それらのサーバーは独立して動作し、異なるコンピュータを管理し、異なる集中管理用格納域を使用してアーカイブを保存します。

管理対象のコンピュータ

少なくとも 1 つの Acronis Backup & Recovery 10 エージェント『ページ参照 415』がインストールされている物理コンピュータまたは仮想コンピュータ『ページ参照 416』。

管理対象の格納域

ストレージ ノード『ページ参照 416』によって管理される集中管理用格納域『ページ参照 427』。管理対象の格納域内のアーカイブ『ページ参照 420』は、次のようにしてアクセスできます。

bsp://node_address/vault_name/archive_name/

物理的には、管理対象の格納域は、ネットワーク共有、SAN、NAS、ストレージ ノードのローカルのハード ディスク ドライブ、またはストレージ ノードにローカル接続されたテープ ライブラリに置くことができます。ストレージ ノードは、管理対象の格納域に保存された各アーカイブに対して、ストレージ ノード側のクリーンアップ『ページ参照 416』およびストレージ ノード側のベリファイ『ページ参照 417』を実行します。管理者は、ストレージ ノードが実行するその他の処理(非重複化『ページ参照 429』、暗号化)を指定することができます。

管理対象の格納域は自己完結型です。つまり、ストレージ ノードが格納域を管理するために必要なすべてのメタデータが含まれています。ストレージ ノードが失われたりデータベースが破損した場合は、新しいストレージ ノードがメタデータを取得してデータベースを再作成します。格納域が別のストレージ ノードに接続される場合、同じ手順が実行されます。

管理対象外の格納域

管理対象の格納域『ページ参照 426』ではないすべての格納域『ページ参照 425』。

計画

「バックアップ計画『ページ参照 421』」をご参照ください。

個人用格納域

直接管理『ページ参照 429』を使用して作成された、ローカルまたはネットワーク上の格納域『ページ参照 425』。個人用格納域が作成されると、そのショートカットが **[ナビゲーション]** ペインの **[個人用格納域]** の下に表示されます。複数のコンピュータで、ネットワーク共有などの物理的に同じ場所を個人用格納域として使用できます。

差分バックアップ

差分バックアップは、前回の完全バックアップ『ページ参照 425』に対するデータの変更点を保存します。差分バックアップからデータを復元するには、対応する完全バックアップにアクセスする必要があります。

集中管理

Acronis Backup & Recovery 10 管理サーバー『ページ参照 429』と呼ばれる集中管理ユニットを使用した Acronis Backup & Recovery 10 インフラストラクチャの管理。集中管理操作には次のものが含まれます。

- バックアップ ポリシー『ページ参照 420』の作成、適用、および管理
- コンピュータ『ページ参照 416』の静的『ページ参照 427』グループおよびダイナミック グループ『ページ参照 417』の作成および管理
- コンピュータ上に存在するタスク『ページ参照 419』の管理
- アーカイブを保存するための集中管理用格納域『ページ参照 427』の作成および管理
- ストレージ ノード『ページ参照 416』の管理
- Acronis Backup & Recovery 10 コンポーネントの活動の監視、集中管理のログの表示など

集中管理タスク

集中管理用バックアップ計画『ページ参照 427』に属するタスク『ページ参照 419』。このようなタスクは、管理サーバー『ページ参照 429』からバックアップ ポリシー『ページ参照 420』を配置すると管理対象のコンピュータ『ページ参照 426』に表示され、バックアップ ポリシーを編集することによってのみ変更できます。

集中管理用バックアップ計画

管理サーバー『ページ参照 429』からバックアップ ポリシー『ページ参照 420』を配置すると管理対象のコンピュータ『ページ参照 426』上に表示されるバックアップ計画『ページ参照 421』。この計画は、バックアップ ポリシーを編集することによってのみ変更できます。

集中管理用格納域

管理サーバー『ページ参照 429』の管理者によって割り当てられ、バックアップ アーカイブ『ページ参照 420』のストレージとして使用されるネットワーク上の場所。集中管理用格納域は、ストレージ ノード『ページ参照 416』によって管理することも管理対象外にすることもできます。集中管理用格納域に保存されるアーカイブの合計数とサイズは、ストレージのサイズによってのみ制限されます。

管理サーバーの管理者が集中管理用格納域を作成するとすぐに、サーバーに登録されているコンピュータ『ページ参照 428』すべてに格納域名と格納域のパスが配布されます。格納域のショートカットが集中管理用格納域の一覧に記載されているコンピュータ上に表示されます。ローカルの計画を含むコンピュータに存在するすべてのバックアップ計画『ページ参照 421』で集中管理用格納域を使用することができます。

管理サーバーに登録されていないコンピュータ上では、集中管理用格納域にバックアップする権限を持つユーザーが格納域のフル パスを指定することで、バックアップを実行できます。格納域が管理対象である場合は、格納域に保存される他のアーカイブと同様に、ユーザーのアーカイブがストレージ ノードによって管理されます。

静的グループ

管理サーバー『ページ参照 429』の管理者が、手動でグループにコンピュータを追加することによって構成するコンピュータのグループ。コンピュータは、管理者がグループまたは管理サーバーからコンピュータを削除するまで静的グループ内に残ります。

選択ルール

バックアップ ポリシー『ページ参照 420』の一部。 管理サーバー『ページ参照 429』の管理者が、コンピュータ内でバックアップするデータを選択できるようにします。

増分バックアップ

前回のバックアップに対するデータの変更点を保存するバックアップ『ページ参照 420』。増分バックアップからデータを復元するには、同じアーカイブ『ページ参照 420』の他のバックアップにアクセスする必要があります。

直接管理

コンソール『ページ参照 416』とエージェント『ページ参照 415』の直接接続を使用して管理対象のコンピュータ『ページ参照 426』上で実行される管理操作。これに対し、操作が管理サーバー『ページ参照 429』上で設定され、サーバーによって管理対象のコンピュータに伝達される場合が集中管理『ページ参照 426』です。

直接管理操作には次のものが含まれます。

- ローカルのバックアップ計画『ページ参照 424』の作成および管理
- 復元タスクなどのローカル タスク『ページ参照 424』の作成および管理
- 個人用格納域『ページ参照 429』とそこに保存されるアーカイブの作成および管理
- コンピュータ上に存在する集中管理タスク『ページ参照 427』の状態、進行状況、およびプロパティの表示
- エージェントの処理ログの表示および管理
- ディスクのクローン作成、ボリュームの作成、ボリュームの変換などのディスク管理操作

ブータブル メディア『ページ参照 423』を使用した操作も、直接管理の一種です。一部の直接管理操作は、管理サーバーの GUI を使用して実行することもできますが、これには選択したコンピュータへの明示的または暗黙的な直接接続が前提になります。

登録

管理対象のコンピュータ『ページ参照 426』を管理サーバー『ページ参照 429』に追加する処理。

登録は、コンピュータ上に存在するエージェント『ページ参照 415』とサーバーの間に信頼関係を設定します。登録中に、コンソールは管理サーバーのクライアント証明書を取得してエージェントに渡し、エージェントはそれを使用して接続を試みるクライアントを認証します。これにより、信頼されるプリンシパル(管理サーバー)になりすましてネットワーク攻撃者が偽造した接続を確立することを防止できます。

登録済みのコンピュータ

管理サーバー『ページ参照 429』によって管理されるコンピュータ『ページ参照 416』。コンピュータは、一度に 1 つの管理サーバーに対してのみ登録できます。コンピュータは登録『ページ参照 429』処理を行うと、登録済みになります。

統合

同じアーカイブ『ページ参照 420』に属する複数のバックアップ『ページ参照 420』を 1 つのバックアップに結合すること。

統合は、手動によってまたはクリーンアップ『ページ参照 415』中にバックアップを削除するときに必要になる場合があります。たとえば、保持ルールのために、完全バックアップ『ページ参照 425』が期限切れになり削除する必要があっても、この完全バックアップの次の増分『ページ参照 428』バックアップは保持しなければならない場合があります。この場合、これらのバックアップは 1 つの完全バックアップに結合され、そのバックアップに増分バックアップの日付が付けられます。統合には多くの時間とシステム リソースが必要になることがあるため、保持ルールでは、依存関係のあるバックアップを削除しないオプションが提供されています。この例では、増分バックアップが期限切れになるまで完全バックアップも保持されます。両方のバックアップが期限切れになった時点で、両方とも削除されます。

非重複化

重複して出現する同一情報は一度だけ保存する方法。

Acronis Backup & Recovery 10 では、ストレージ ノード『ページ参照 416』に保存されているバックアップ アーカイブ『ページ参照 420』に非重複化テクノロジを適用することができます。これにより、アーカイブによって使用されるストレージ領域、バックアップ トラフィック、およびバックアップ中のネットワークの使用量が最小限に抑えられます。

非重複化された格納域

非重複化『ページ参照 429』が有効になっている管理対象の格納域『ページ参照 426』。

復元点

バックアップされたデータを復元することができる日時。

物理コンピュータ

Acronis Backup & Recovery 10 管理サーバーでは、物理コンピュータは登録済みのコンピュータ『ページ参照 428』と同じです。Acronis Backup & Recovery 10 エージェントがコンピュータ上にインストールされ、コンピュータが管理サーバーに登録されている場合、仮想コンピュータは物理コンピュータと見なされます。

索引

A

G

H

L

M

N

P

R

S

T

U

V

W

あ

い

う

え

お

か

き

く

け

こ

さ

し

す

せ

そ

た

ち

つ

て

と

な

に

ね

は

ひ

ふ

へ

ほ

ま

め

ゆ

ら

れ

ろ

わ