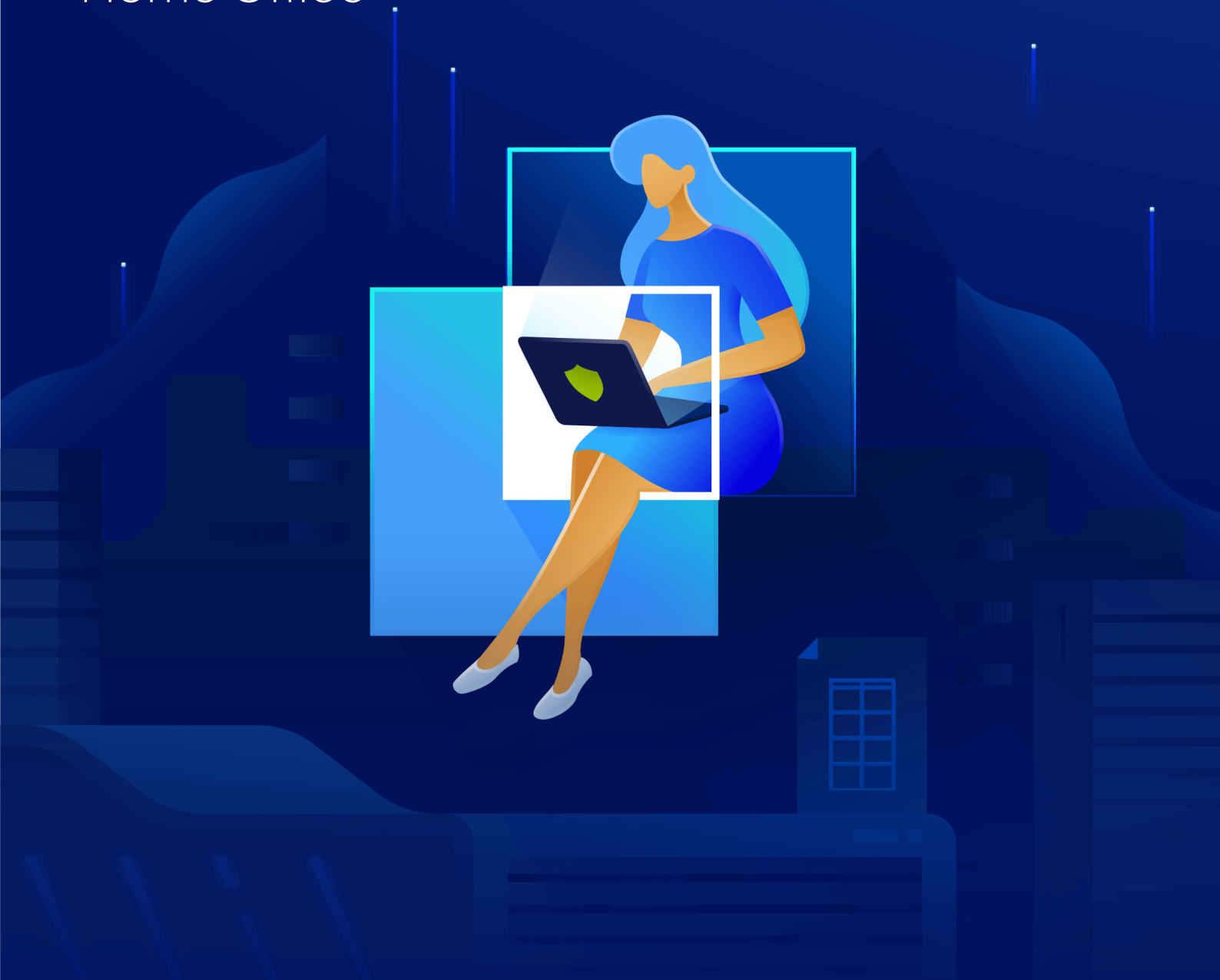
Acronis

acronis.com

Acronis Cyber Protect

Home Office



ユーザー ガイド

リビジョン：2023/06/21

目次

著作権情報

Acronis の特許取得済みの技術

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

はじめに

Acronis Cyber Protect Home Office とは

Acronis Cyber Protect Home Office は、すべての情報を安全に守るための完全なサイバープロテクションソリューションです。文書、写真、電子メール、選択したパーティション、さらにはディスク ドライブ全体をもバックアップすることができます。バックアップ対象には、オペレーティングシステム、アプリケーション、設定、その他すべてのデータが含まれます。その主な利点として、データ保護とセキュリティの機能があります。

バックアップがあれば、データの損失、重要なファイルやフォルダの誤削除、ハードディスクの完全クラッシュなどの障害や災害が発生した場合にコンピュータシステムをリカバリできます。

Online Backup を使用すると、ファイルやディスクを Acronis Cloud に保存できます。ご使用のコンピュータが紛失や盗難に遭ったり、または破壊されたりしても、データは保護され、必要に応じてデータを新しいデバイスに完全復元できます。

主な機能:

- ローカルストレージおよび Acronis Cloud へのディスクバックアップ
- ローカルストレージおよび Acronis Cloud へのファイルバックアップ
- ウィルス対策およびマルウェア対策保護
- Acronis ブータブルメディア
- ハード ディスクのクローン作成
- データアーカイブ
- 複数デバイスのデータ保護
- ファイル同期
- セキュリティ ツールおよびプライバシー ツール

注意
Acronis Startup Recovery Manager および Acronis ブータブルメディアを使って Acronis Cloud にバックアップを作成することはできません。

コンピューターを保護する方法については、「システムの保護」を参照してください。

Acronis True Image（2020 または 2021）および Acronis Cyber Protect Home Office で作成されたバックアップ

Acronis True Image 2020 では、新しいバックアップ形式として TIBX が導入されました。この形式では、信頼性と利便性がさらに向上しています。TIBX 形式は、内部ドライブ、外部ドライブ、ネットワークストレージを保存先として作成されるディスクバックアップで使用されます。

バックアップ ファイルの命名についての詳細は、"バックアップファイルの命名"（49ページ）を参照してください。

バックアップ スキーム

TIBX 形式によるバックアップでは、すべてのバックアップスキームがサポートされています。どのバックアップバージョンも別個のファイルとして保存される TIB 形式とは異なり、TIBX 形式ではフルバックアップと差分バックアップのバージョンは別個のファイルに保存されますが、増分バックアップバージョンは自動的にベースバックアップ（フルまたは差分）にマージされます。

TIBX 形式バックアップのクリーンアップ

不要になったバックアップバージョンをクリーンアップしたい場合は、自動クリーンアップ方式と手動クリーンアップ方式を使用します。

自動クリーンアップまたは手動クリーンアップが構成されている場合、クリーンアップ後、いくつかの補助的なファイルがストレージに残る場合があります。Windows では、これらのファイルのサイズが実際よりも大きく表示されることがあります。Windows のファイル プロパティにより、物理サイズを確認することができます。

注意
どんなファイルも手動で削除しないようにしてください！

ローカルバックアップを手動でクリーンアップする方法は、次のとおりです:

- フルバックアップは、その依存バージョンと共にのみ、削除できます。
- 差分バックアップバージョンは、他のどのバックアップバージョンとも独立して削除できます。
- 増分バックアップ:
  - 最後のバックアップチェーンの場合、増分バックアップがあれば削除してスペースを空けることができます。
  - 最後のバックアップチェーンではない場合、増分バックアップバージョンは、同じチェーンの他のすべての増分バックアップと共にのみ、削除できます。

TIB 形式が引き続き使用されるのはどのバックアップか

次のバックアップでは、引き続き TIB 形式がされます:

- ファイルレベルのバックアップ
- ノンストップバックアップ
- 認証バックアップ
- CD/DVD/Blu-ray、FTP、または Acronis Secure Zone を保存先として使用するバックアップ

.tibx アーカイブと .tib アーカイブの命名規則の違いの詳細については、「バックアップファイルの命名」を参照してください。

クリーンアップの詳細については、「バックアップ、バックアップバージョン、レプリカをクリーンアップする」を参照してください。

システム要件とサポートされるメディア

最小システム要件

Acronis Cyber Protect Home Office を実行するには次のハードウェアが必要です。

- Intel CORE 2 Duo（2GHz）プロセッサまたは同等品
  CPU が SSE 命令をサポートしている必要あり。
- 2 GB の RAM
- システム ハードディスク上に 7 GB の空き領域
- ブータブルメディア作成用の CD-RW/DVD-RW ドライブまたは USB ドライブ
  - Linux の場合、約 660 MB の空き領域が必要。
  - Windows の場合、約 700 MB の空き領域が必要。
- 1024 x 768 の画面解像度
- マウスまたはその他のポインティング デバイス（推奨）

警告
バックアップとリカバリが成功しても、仮想マシンでのインストールが保証されるわけではありません。

その他の要件

- 製品のアクティベーション、保護のアップデートのダウンロード、および Acronis Cloud を使用するすべての機能には、インターネットへの接続が必要です。お使いのコンピュータがインターネットに接続されていない場合は、インターネットに接続されている他のコンピュータを使用して製品を有効化できます。詳細については、「Acronis Cyber Protect Home Office の有効化」を参照してください。
- Acronis Cyber Protect Home Office を実行するための管理者権限が必要になります。

サポートされるオペレーティング システム

Acronis Cyber Protect Home Office は、次のオペレーティングシステムでテスト済みです。

- Windows 11
- Windows 10
- Windows 8.1
- Windows 8
- Windows 7 SP1（全エディション）
- Windows Home Server 2011

注意

- ベータビルドはサポートされていません。https://kb.acronis.com/content/60589 を参照してください。
- Windows Embedded、IoT エディション、Windows 10 LTSB、Windows 10 LTSC、および S モードの Windows 10 はサポートされていません。
- Acronis Cyber Protect Home Office を Windows 7、Windows 8、および Windows 8.1 で使用するには、Microsoft からの次のセキュリティ更新が必要になります: KB4474419 と KB4490628。https://kb.acronis.com/content/69302 を参照してください。

Acronis Cyber Protect Home Office では、Intel または AMD ベースの PC オペレーティングシステム（Linux® を含む）を実行するコンピューター上のディスク/パーティションをバックアップして復元するためのブータブル CD-R/DVD-R または USB ドライブを作成することもできます。

その他の Windows オペレーティングシステム上でソフトウェアが動作する可能性がありますが、保証されません。

警告

復元の成功が保証されるのは、サポートされるオペレーティングシステムの場合のみです。セクタ単位でのバックアップを使用してその他のオペレーティングシステムをバックアップすることもできますが、その場合、復元後に起動できなくなる可能性があります。

サポートされるファイル システム

- NTFS
- Ext2/Ext3/Ext4
- ReiserFS(3) [1]
- Linux SWAP [2]
- HFS+/HFSX [3]
- FAT16/32/exFAT[4]

ファイルシステムがサポート対象外または破損している場合も、Acronis Cyber Protect Home Office ではデータをセクタ単位でコピーできます。

サポートされているインターネット接続タイプ

以下の表に、製品の機能でサポートされているインターネット接続タイプをまとめます。

[1]ファイルシステムは、ディスクまたはパーティションのバックアップ/復元処理においてのみサポートされます。

[2]ファイルシステムは、ディスクまたはパーティションのバックアップ/復元処理においてのみサポートされます。

[3]ディスクの復元、パーティションの復元、クローン作成の操作はサポートされますが、サイズ変更はできません。

[4]ディスクの復元、パーティションの復元、クローン作成の操作はサポートされますが、サイズ変更はできません。

	インターネット接続タイプ				
	Windows の Acronis コンソール		Acronis ブータブルメディア		
	Windowsで確立されるすべての接続	プロキシサーバー	イーサネットケーブル	WiFi	プロキシサーバー
Acronis Cloud へのディスクレベルおよびファイルレベルのバックアップ	+	-	-	-	-
Acronis Cloud からのディスクレベルの復元	+	-	+	+	-
Acronis Cloud からのファイルレベルの復元	+	-	-	-	-
データの同期	+	-	-	-	-
製品の有効化	+	- *	-	-	-
製品のアップデート	+	- * *	-	-	-

* アクティブ化コードを使用して製品をアクティブ化できます。詳細については、「Acronis Cyber Protect Home Office のアクティブ化」の「**他のコンピューターからのアクティブ化**」を参照してください。

* * 製品をアップデートするには、Acronis の Web サイトから最新の製品バージョンをダウンロードし、現在のバージョンを上書きしてインストールします。

サポートされるストレージ メディア

- ハードディスク ドライブ（HDD）
- ソリッドステートドライブ（SSD）
- ネットワーク上のストレージデバイス
- FTP サーバー

注意
FTP サーバー側がパッシブモードのファイル転送を許可している必要があります。Acronis Cyber Protect Home Office は、FTP サーバーに直接バックアップするときに、バックアップを 2 GB ずつのサイズのファイルに分割します。

- CD-R/RW、DVD-R/RW、DVD+R（2 層ディスクの DVD+R を含む）、DVD+RW、DVD-RAM、BD-R、BD-RE
- USB 1.1/2.0/3.0、USB-C、eSATA、FireWire（IEEE-1394）、SCSI、および PC カードストレージデバイス

ダイナミックディスクを操作する場合の制限事項

- ダイナミックディスクでは、Acronis Secure Zone の作成はサポートされていません。
- ダイナミック ボリュームをダイナミック ボリュームとしてリカバリするときに、手動でサイズを変更することはできません。
- Try&Decide®を使用してダイナミックディスクを保護することはできません。
- ディスクのクローン作成処理は、ダイナミック ディスクではサポートされていません。

バックアップ元のコンピュータのファイアウォール設定では、ポート 20 および 21 が TCP プロトコルと UDP プロトコル用に開いており、機能するようになっていることが必要です。Windows の**ルーティングとリモート アクセス** サービスは無効にする必要があります。

Acronis Cyber Protect Home Office のインストールとアンインストール

Acronis Cyber Protect Home Office をインストールするには、次のようにします。

1. Acronis Web サイト（ https://go.acronis.com/home-office）から Acronis Cyber Protect Home Office セットアップファイルをダウンロードします。
2. セットアップ ファイルを実行します。

   Acronis Cyber Protect Home Office は、セットアップ処理を開始する前に Web サイトで新しいバージョンの有無を確認します。新しいバージョンがある場合は、インストール用に表示されます。
3. インストールの種類を選択してください。
   - **[インストール]** をクリックすると、デフォルトのインストールが開始します。
   - **[カスタムインストール]** をクリックすると、必要なコンポーネントを選択できます。
     - **バックアップおよび主要な保護**。このコンポーネントは以下のものに不可欠です。
       - "データのバックアップ"（55ページ）
       - "データの復元"（106ページ）
       - "脆弱性アセスメント"（166ページ）
       - "データのアーカイブ"（149ページ）
       - "データの共有"（154ページ）
       - "データの同期"（170ページ）
       - "ディスクのクローン作成と移行"（175ページ）
       - "ツール"（191ページ）
     - **ランサムウェア対策保護、クリプトマイニング検出、ビデオ会議保護**。詳細については、"Active Protection"（160ページ） をご参照ください。
     - **リアルタイム保護、ウイルス対策スキャン、および Web フィルタリング**。 詳細については、"Active Protection"（160ページ） および "ウィルス対策スキャン"（164ページ） をご参照ください。
     - **Try&Decide ツール**。Windows のメモリ整合性機能を使用している場合は、互換性の問題を避

けるため、このコンポーネントをインストールしないでください。詳細については、"Try&Decide"（207ページ） をご参照ください。

Acronis Cyber Protect Home Office がシステムパーティションにインストールされます（通常は C ドライブ）。

4. インストールが完了したら、**[アプリケーションを開始]** をクリックします。
5. Acronis Cyber Protect Home Office および Bonjour の使用許諾契約の条件を読んで同意します。

   Bonjourソフトウェアは、NASデバイスのアドバンストサポートとしてコンピュータにインストールされます。ソフトウェアは、いつでもアンインストールできます。

   また、Acronis カスタマ エクスペリエンス プログラムへの参加に同意できます。この設定は、いつでも変更できます。
6. **[アクティベーション]** ウィンドウで、次のいずれかを実行できます。
   - Acronis Cyber Protect Home Office を有効化するには、シリアルナンバーを入力して、**[有効化]** をクリックします。製品が有効化されます。
   - Acronis アカウントにサインインするには、**[サインイン]** をクリックします。詳細については、「Acronis アカウント」を参照してください。
   - 試用版を使用するには、**[試用の開始]** をクリックします。

Acronis Cyber Protect Home Office のエラーからリカバリする手順は、次のとおりです。

Acronis Cyber Protect Home Office が動作しなくなったりエラーが発生したりした場合は、ファイルが破損している可能性があります。このような問題に対処するには、まずプログラムを復旧する必要があります。そのためには、Acronis Cyber Protect Home Office インストーラを再度実行します。インストーラによりコンピューター上の Acronis Cyber Protect Home Office が検出され、変更するか削除するかの確認を求められます。

Acronis Cyber Protect Home Office のコンポーネントを追加または削除するには

- Windows 11 をご利用の場合は、**[スタート]** → **[設定]** → **[アプリ]** → **Acronis Cyber Protect Home Office** → **[変更]** の順にクリックします。
- Windows 10 をご利用の場合は、**[スタート]** → **[設定]** → **[アプリ]** → **Acronis Cyber Protect Home Office** → **[変更]** の順にクリックします。
- Windows 8 をご利用の場合は、**[設定]** アイコンをクリックし、**[コントロール パネル]** →**[プログラムのアンインストール]** → **[Acronis Cyber Protect Home Office]** → **[変更]** の順に選択します。
- Windows 7 をご利用の場合は、**[スタート]** → **[コントロール パネル]** → **[プログラムのアンインストール]** → **[Acronis Cyber Protect Home Office]** → **[変更]** の順にクリックします。

インストーラで、**[変更]** をクリックします。次に、必要なコンポーネントのチェックボックスをオンまたはオフにします。削除を完了するために、コンピューターの再起動が必要になる場合があります。

Acronis Cyber Protect Home Office を完全にアンインストールするには

- Windows 11 をご利用の場合は、**[スタート]** → **[設定]** → **[アプリ]** → **Acronis Cyber Protect Home Office** → **[アンインストール]** の順にクリックします。
- Windows 10 をご利用の場合は、**[スタート]** → **[設定]** → **[アプリ]** → **Acronis Cyber Protect Home Office** → **[アンインストール]** の順にクリックします。

- Windows 8 をご利用の場合は、**[設定]** アイコンをクリックし、**[コントロール パネル]** →**[プログラムのアンインストール]** → **[Acronis Cyber Protect Home Office]** → **[アンインストール]** の順に選択します。
- Windows 7 をご利用の場合は、**[スタート]** → **[コントロール パネル]** → **[プログラムのアンインストール]** → **[Acronis Cyber Protect Home Office]** → **[アンインストール]** の順にクリックします。

画面の指示に従って操作します。削除を完了するために、コンピュータの再起動が必要になる場合があります。

注意
"Acronis Secure Zone"（212ページ） または "Acronis Nonstop Backup"（46ページ） を使用した場合は、表示されるウィンドウでゾーンストレージとNonstop Backupストレージの処理を選択します。

Acronis Cyber Protect Home Officeの有効化

Acronis Cyber Protect Home Office を使用するには、インターネット経由でこれを有効化する必要があります。有効化しない場合、製品の全機能の利用有効期間は 30 日です。この期間にアクティブ化しないと、リカバリ以外のすべての機能が利用できなくなります。コンピューターを初めてインターネットに接続し、ログイン名とパスワードを使用して Acronis Cyber Protect Home Office にログインすると、製品が自動的にアクティブ化されます。

アクティブ化されている製品の数が多すぎる問題

「有効化されている製品の数が多すぎます」という問題には、以下の原因が考えられます。

- **Acronis Cyber Protect Home Office がインストールされているコンピュータの数が最大数を超えている。**
  たとえば、コンピュータ 1 台分のライセンスまたはシリアルナンバーを所有するユーザーが、2 台目のコンピュータに Acronis Cyber Protect Home Office をインストールする場合などです。
  解決策：
  - 新しいシリアルナンバーを入力します。新しいシリアルナンバーを所有していない場合、Acronis ビルトインストアまたは Acronis Web サイトで購入できます。
  - 製品がすでにアクティブ化されているコンピュータから新しいコンピュータにライセンスを移動します。そのためには、ライセンスの移動元のコンピュータを選択します。選択したコンピュータで Acronis Cyber Protect Home Office が無効化されることに注意してください。
- **Windows を再インストールするか、コンピューターのハードウェアを変更する。**
  例えば、ご使用のコンピュータのマザーボードまたはプロセッサをアップグレードしたとします。この場合、ご使用のコンピューターは新しいコンピューターと認識されるため、Acronis Cyber Protect Home Office は無効化されます。
  解決策：
  ご使用のコンピューターで Acronis Cyber Protect Home Office を再有効化するには、リストからそのコンピューターを古い名前で選択します。

サブスクリプションライセンスを手動で管理する

Acronis Cyber Protect Home Office のサブスクリプションベースのバージョンを使用している場合、Acronis Web サイトでライセンスを手動で管理することができます。次の処理を実行できます。

- コンピュータ間でのライセンスの移動
- アカウント間でのライセンスの転送
- コンピュータからのライセンスの削除
- 製品のアクティブ化の解決（「アクティブ化されている製品の数が多すぎる」問題を含む）
- 新規ライセンスの購入

ライセンスを管理するには、次のようにします。

1. https://account.acronis.com/ にアクセスし、Acronis アカウントでサインインします。
2. **[製品]** セクションで、Acronis Cyber Protect Home Office を見つけて **[管理]** をクリックします。

試用版情報

一般的な制約条件

試用版の Acronis Cyber Protect Home Office は、30 日間の試用期間のみ機能します。以下の制約があります。

- ディスクのクローン作成は利用できません。
- Acronis ブータブルメディア から起動する場合は、リカバリ操作のみ可能です。

同期

データの同期は制限なく使用できますが、試用期間が切れると次のようになります。

- お使いのコンピュータは、すべての同期から除外されます。製品版の Acronis Cyber Protect Home Office を有効化すると、同期に再び接続できるようになります。
- 全バージョンの同期ファイルは、Acronis Cloud から完全に削除されます。

Acronis Cloud

試用期間中、クラウドのストレージ容量は1,000 GBになります。この領域を使用して、オンライン上のバックアップ、アーカイブ、各バージョンの同期ファイルを保存できます。試用期間終了後 30 日間、Acronis Cloud はリカバリ専用モードで動作します。この期間が過ぎると Acronis Cloud サービスは利用できなくなり、Cloud のデータはすべて削除されます。

製品版の購入

製品版は、Acronis Web サイトで、またはアプリ内課金機能を使用して入手できます。詳細については、「Acronis Cyber Protect Home Office のアップグレード」を参照してください。

Acronis Cyber Protect Home Office のアップグレード

Acronis Cyber Protect Home Office のアップデートが Acronis Web サイトで入手可能であれば、ダウンロードできます。Acronis True Image（2017 以降）を現在お持ちの場合は、新しいバージョンによって自動的にアップデートされます。古いバージョンを削除してソフトウェアを再インストールする必要はありません。現在のバージョンが古い場合には、まず現在のバージョンをアンインストールすることをおすすめします。

以前のバージョンの Acronis Cyber Protect Home Office で作成されたバックアップは、製品の新しいバージョンとの完全な互換性があります。アップグレード後、すべてのバックアップがバックアップリストに自動的に追加されます。

新しいバージョンのプログラムで作成されたバックアップが、前のバージョンのプログラムと互換性を持たない場合があります。Acronis Cyber Protect Home Office を以前のバージョンに戻した場合は、その古いバージョンでバックアップを再度作成する必要があります。同じ理由により、Acronis Cyber Protect Home Office をアップグレードするたびに、新たにブータブルメディアを作成することを強くおすすめします。

製品版を購入するには、次のようにします。

1. Acronis Cyber Protect Home Office を開始します。
2. サイドバーの **[アカウント]** をクリックし、**[製品版を購入]** をクリックします。ビルトイン ストアが開きます。
3. 購入するライセンスを選択し、**[今すぐ購入]** をクリックします。
4. 支払い情報を指定します。

Acronis Cyber Protect Home Office をアップデートするには、次のようにします。

1. Acronis Cyber Protect Home Office を開始します。
2. サイドバーで **[アカウント]** をクリックします。
   利用可能な新しいバージョンがある場合は、現在のビルド番号の横にメッセージが表示されます。
3. **[ダウンロードとインストール]** をクリックします。

   注意
   ダウンロードを開始する前に、ファイアウォールによってダウンロード処理がブロックされないようにしてください。

4. 新しいバージョンがダウンロードされたら、**[今すぐインストール]** をクリックします。

アップデートの確認を自動的に行うには、**[設定]** タブに移動して、**[起動時にアップデートを自動確認]** チェックボックスをオンにしてください。

ビルトイン ストア

Acronis Cyber Protect Home Office には、アプリ内ストアがあります。このストアを利用することで、次のことが可能になります。

- Acronis Cyber Protect Home Office の製品版を購入する。
- Acronis Cyber Protect Home Office のサブスクリプションを購入する。
- Acronis Cloud の追加のストレージスペースを購入する。

アプリ内ストアにアクセスするには、[**アカウント**] タブに移動して、[**Acronis ストア**] をクリックします。アプリ内ストアが開き、利用可能な購入オプションがすべて表示されます。

サポートセンターのホームページ

Acronis Cyber Protect Home Office に関してご質問がある場合は、https://www.acronis.com/support/ をご覧ください。

はじめに

ユーザーインターフェイスの言語

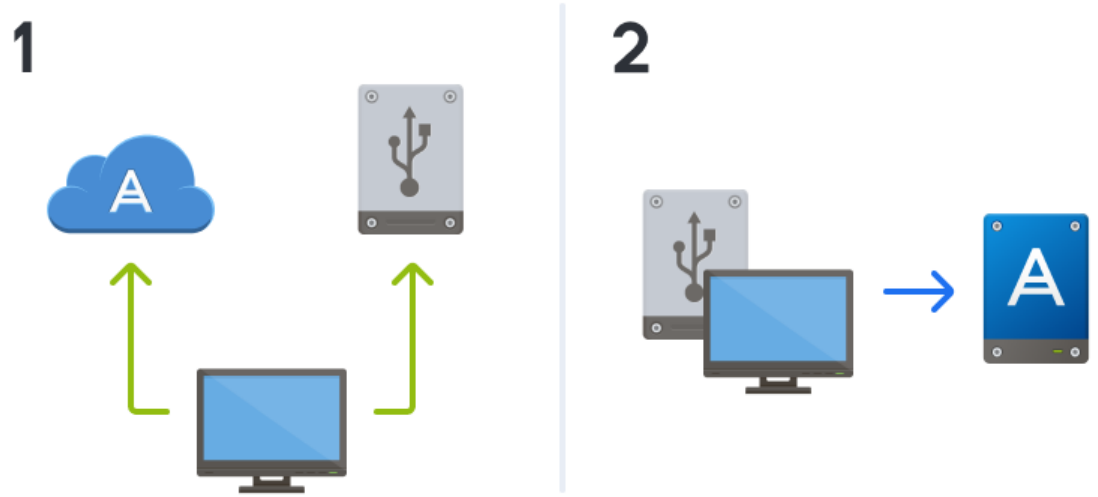
使用を開始する前に、Acronis Cyber Protect Home Office ユーザーインターフェースで希望する言語を選択します。デフォルトでは、Windowsの表示言語に従って設定されます。

ユーザーインターフェースの言語を変更するには、次の手順を実行します。

1. Acronis Cyber Protect Home Office を開始します。
2. **[設定]** セクションで、リストの中からご希望の言語を選択します。

システムの保護

1. コンピュータをバックアップします。
2. Acronis ブータブルメディア を作成します。



また、「必要なときにブータブルメディアを確実に使用できるようにする」で説明したとおりに、ブータブルメディアをテストすることをお勧めします。

コンピュータのバックアップ中

コンピュータをバックアップするタイミング

システムでの重要なイベントの後は毎回新しいバックアップ バージョンを作成します。

イベントの例:

- 新しいコンピュータを購入した。
- コンピュータに Windows を再インストールした。

- 新しいコンピュータで、すべてのシステム設定（例: 時刻、日付、言語）を構成し、必要なプログラムをすべてインストールした。
- 重要なシステム アップデート。

注意
正常な状態のディスクを保存するため、バックアップの前にウイルスをスキャンすることを勧めします。このためには、ウイルス対策ソフトウェアを使用してください。この操作には長時間かかる場合があることに注意してください。

コンピュータのバックアップを作成する方法

システムを保護するには、次の2種類の方法があります。

- **PC全体のバックアップ（推奨）**
  Acronis Cyber Protect Home Office は、内蔵ハードドライブすべてをディスクモードでバックアップします。バックアップ対象は、オペレーティングシステム、インストールされているプログラム、システムの設定、写真、音楽、ドキュメントなどの個人データすべてです。 詳細については、「PCのすべてのデータのバックアップ」を参照してください。
- **システムディスクのバックアップ**
  システムパーティションまたはシステムドライブ全体をバックアップすることができます。詳細については、「ディスクとパーティションのバックアップ」を参照してください。

システム保護のための主要な方法としてノンストップバックアップを使うことはおすすめしません。このテクノロジーの主な目的が、頻繁に変更されるファイルを保護することであるためです。システムの安全のため、ほかのスケジュールをご使用ください。"カスタム スキームの例"（70ページ） の例を参照してください。Nonstop Backup の機能について詳しくは、"Acronis Nonstop Backup"（46ページ） を参照してください。

コンピューターをバックアップするには、次の手順を実行します。

1. Acronis Cyber Protect Home Office を開始します。
2. サイドバーで **[バックアップ]** をクリックします。
   今回が最初のバックアップの場合、バックアップ設定画面が表示されます。既に一覧表示されているバックアップがある場合は、**[バックアップアップの追加]** をクリックします。
3. **[バックアップ ソース]** アイコンをクリックし、**[コンピュータ全体]** を選択します。
   システムディスクのみをバックアップする場合は、**[ディスクとパーティション]** をクリックし、システムパーティション（通常はC:）とシステム予約パーティション（存在する場合）を選択します。
4. **[バックアップの保存先]** アイコンをクリックし、バックアップの保存場所を選択します（以下の推奨事項を参照してください）。
5. **[今すぐバックアップ]** をクリックします。

以上により、バックアップの一覧に新しいバックアップボックスが表示されます。今後、新しいバージョンのバックアップを作成するには、リストからバックアップボックスを選択して、**[今すぐバックアップ]** をクリックします。

ディスクのバックアップを保存する場所

- **可** - 通常の内蔵ハードディスク。
- **良** - Acronis Secure Zone。これは、ローカル ハードドライブにある、バックアップを保存するための安全な専用パーティションです。
- **優** - Acronis Cloud または外部ハードディスク。

詳細については、「バックアップの保存場所の決定」を参照してください。

必要なバックアップ バージョンの数

ほとんどの場合、PC全体のコンテンツまたはシステムディスクのバックアップバージョンは2〜3個、最大で4〜6個必要です（バックアップを作成するタイミングについては、上記の情報を参照してください）。自動クリーンアップルールを使用すると、バックアップバージョンの数を制御できます。詳細については、「カスタムスキーム」を参照してください。

最初のバックアップ バージョン（完全バックアップ バージョン）が最も重要であることに留意してください。このバージョンは、ディスクに保存されているすべてのデータを含むため、最も大きいバックアップ バージョンです。以降のバックアップ バージョン（増分バックアップ バージョンおよび差分バックアップ バージョン）は、異なるスキームで整理することができます。これらのバージョンには、データの変更のみが含まれています。これが、増分バックアップ バージョンおよび差分バックアップ バージョンには完全バックアップ バージョンが必要であり、完全バックアップ バージョンが非常に重要である理由です。

デフォルトでは、ディスクのバックアップは増分スキームを使用して作成されます。ほとんどの場合、このスキームが最適です。

注意
詳しい知識があるユーザー向け: 2 〜 3個の完全バックアップバージョンを作成し、異なるストレージデバイスに保存することをおすすめします。この方法で信頼性を大幅に高めることができます。

Acronis ブータブルメディア の作成

Acronis ブータブルメディア とは、CD、DVD、USB フラッシュドライブ、またはその他のリムーバブルメディアで、Windows が起動しなくなったときにそこから Acronis Cyber Protect Home Office を実行できるものです。Acronis メディアビルダー を使用してブート可能なメディアを作成できます。

Acronis ブータブルメディア を作成するには、以下の手順に従います。

1. CD/DVD を挿入するか USB ドライブ (USB フラッシュドライブ、または HDD/SSD 外付けドライブ) を接続します。
2. Acronis Cyber Protect Home Office を開始します。
3. サイドバーで **[ツール]** をクリックし、**[ブータブル メディア ビルダ]** をクリックします。
4. 最初の手順では、**[シンプル]** を選択します。
5. ブータブル メディアの作成に使用するデバイスを選択します。
6. **[実行]** をクリックします。

Acronis ブータブルメディア を使用するには、以下の手順に従います。

Acronis ブータブルメディア は、Windows を起動できないときにコンピューターをリカバリするために使用します。

1. ブータブルメディアをコンピュータに接続します（CD/DVD を挿入します。または、USB ドライブを接続します）。
2. Acronis ブータブルメディア が最初の起動デバイスになるように、BIOS で起動順を並べ替えます。詳細については、「BIOS での起動順の並べ替え」を参照してください。
3. ブータブルメディアからコンピューターを起動して、**[Acronis Cyber Protect Home Office]** を選択します。
   Acronis Cyber Protect Home Office が読み込まれたら、これを使用してコンピューターを復元できます。

詳細については、「Acronis メディアビルダー」を参照してください。

PCのすべてのデータのバックアップ

PC全体のバックアップについて

PC全体のバックアップは、コンピュータ上のすべてのコンテンツをバックアップする最も簡単な方法です。どのデータを保護する必要があるかわからない場合には、このオプションを選択することをおすすめします。システムパーティションのみをバックアップする場合、詳細については「ディスクとパーティションのバックアップ」を参照してください。

バックアップタイプとして [コンピュータ全体] を選択すると、Acronis Cyber Protect Home Office はディスクモードで内部のハードディスクドライブをすべてバックアップします。バックアップ対象は、オペレーティングシステム、インストールされているプログラム、システムの設定、写真、音楽、ドキュメントなどの個人データすべてです。

PC全体のバックアップからの復元も簡単です。必要な操作は、データを戻す時点の選択だけです。Acronis Cyber Protect Home Office はバックアップからすべてのデータを元の場所に復元します。具体的なディスクやパーティションを選択して復元することはできません。また、デフォルトの保存先を変更することもできません。こうした制限を避ける必要がある場合は、通常のディスクレベルのバックアップ方法でデータをバックアップすることをおすすめします。詳細については、「ディスクとパーティションのバックアップ」を参照してください。

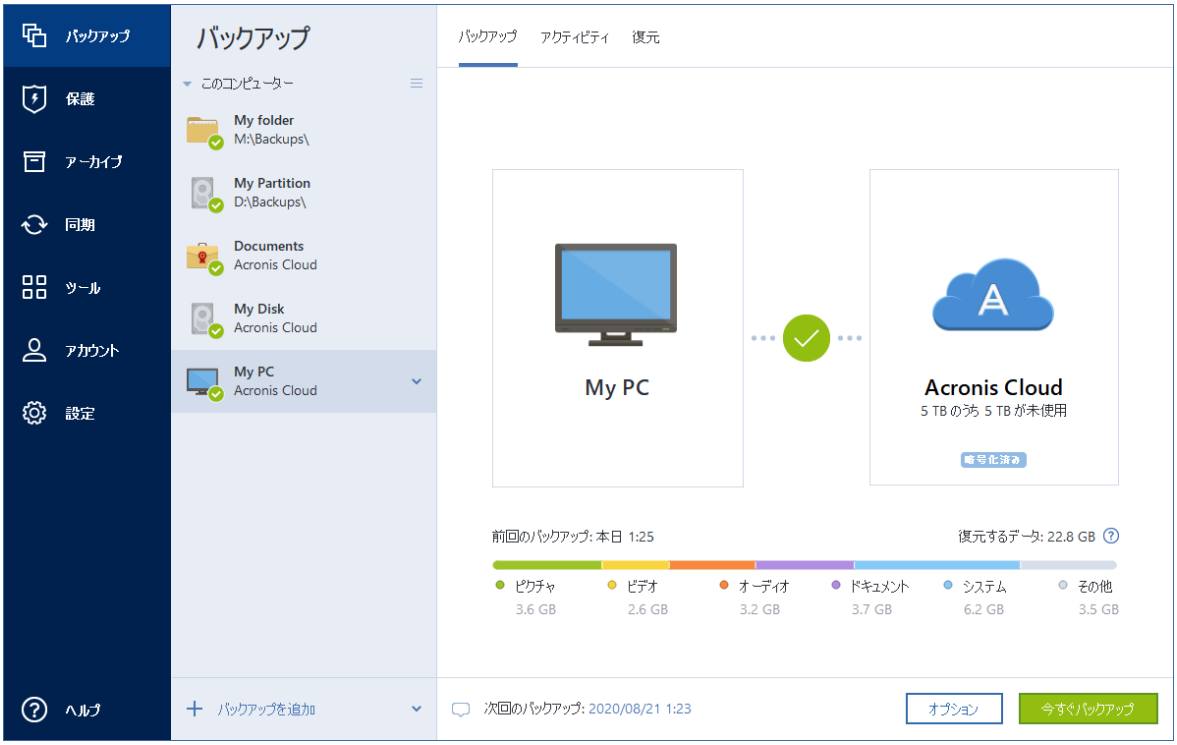
PC全体のバックアップから特定のファイルやフォルダを復元することもできます。詳細については、「ファイルやフォルダのバックアップ」を参照してください。

PC全体のバックアップにダイナミックディスクが含まれている場合、データをパーティションモードで復元します。つまり、復元対象のパーティションを選択したり、復元先を変更したりできます。詳細については、「ダイナミック/GPTディスクおよびボリュームのリカバリについて」を参照してください。

コンピュータ全体のバックアップを作成するには、次の手順を実行します。

1. Acronis Cyber Protect Home Office を開始します。
2. サイドバーで **[バックアップ]** をクリックします。
3. バックアップリストの下部にあるプラス記号をクリックします。
4. **[バックアップ ソース]** アイコンをクリックし、**[コンピュータ全体]** を選択します。

5. **[バックアップの保存先]** アイコンをクリックし、バックアップの保存先を選択します。
   コンピューターのバックアップは、Acronis Cloud、ローカルストレージ、またはネットワークストレージに作成することをお勧めします。詳細については、「バックアップの保存場所の決定」を参照してください。



6. （オプションの手順）バックアップのオプションを設定するには、**[オプション]** をクリックします。詳細については、「バックアップオプション」を参照してください。
7. **[今すぐバックアップ]** をクリックします。

注意
Acronis Cloud にデータをバックアップする場合は、最初のバックアップが完了するまでにかなり時間がかかることがあります。以降のバックアップ処理は、ファイルに対する変更のみがインターネットを使って転送されるので、大幅に速くなります。

さらに、https://goo.gl/KjW5sM のビデオ解説（英語）をご覧ください。

以下も参照してください: バックアップとディスクのクローン作成の違い

Acronis Survival Kit の作成

障害発生時にコンピューターをリカバリするために必要な 2 つの重要なコンポーネントとして、システムディスクのバックアップとAcronis ブータブルメディアがあります。ほとんどの場合、これらのコンポーネントは別々に保管されます。たとえば、システムバックアップは外付けドライブまたは Acronis Cloud に置かれ、ブータブルメディアは小さな USB フラッシュドライブです。Acronis Survival Kit は、両方のコンポーネントをまとめたもので、障害が発生した場合にコンピューターを復元するために必要なすべてのものを 1 つのデバイスに備えることができます。これは、Acronis ブータブルメディアファイルと、システムパーティションのバックアップ、コンピュータ全体、またはすべてのディスク

バックアップが入った外付けのハードディスクドライブです。さらに、データのバックアップを通常のバックアップとして使用できます。保護する必要のある任意のデータをこれに含めて、通常のバックアップとしてそれを更新するスケジュールを設定できます。また、外付けハードドライブは Acronis Survival Kit 専用として予約されるわけではありません。ブータブルメディアが占めるディスク領域はわずか 2 GB で、残りの領域を（Acronis Survival Kit の機能である）システムパーティションやコンピューター全体のバックアップと共有したり、他のバックアップ、個人データ、フォトなど他の任意のデータと共有したりすることができます。ただし 1 つの外付けハードディスクには 1 つの Acronis Survival Kit のみを保持してください。

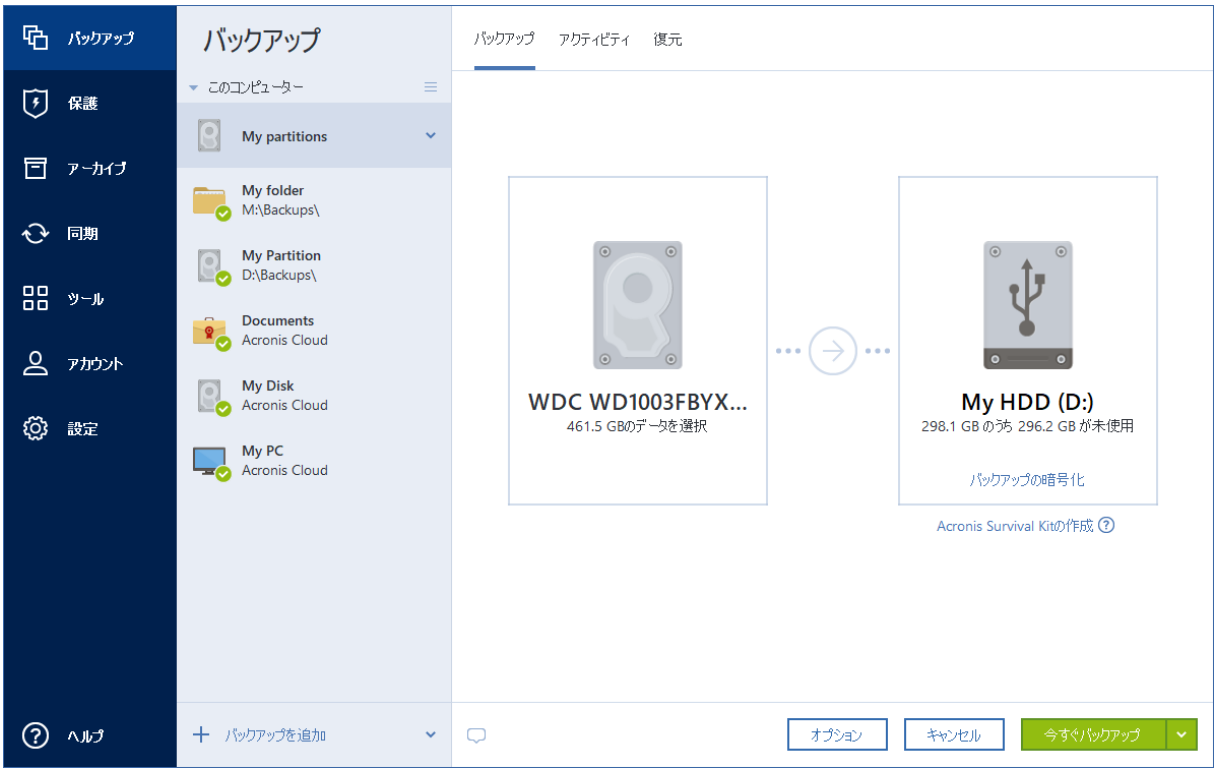
この外付けハードディスクに保存されるバックアップの数にかかわらず、コンピューターをリカバリするにはただ 1 つの Acronis Survival Kit だけが必要です。ブータブルメディア コンポーネントとシステムパーティションまたはコンピュータ全体のバックアップの両方が同じコンピュータ用、または同じ構成の複数コンピュータ用に作成された場合、その両方が共に機能します。

Acronis Survival Kit 用のデバイスとして使用できるデバイスには、以下のものがあります。

- **外付けハードディスクドライブ**
  32 GB より大きく、NTFS、FAT32、または exFAT ファイルシステムを備えている必要があります。ドライブが別のファイルシステムである場合、Acronis Cyber Protect Home Office はドライブのフォーマットを勧めます。
- **USB フラッシュドライブ**
  最小サイズが 32 GB の MBR フラッシュドライブにする必要があります。GPT フラッシュドライブを使用する場合は、Acronis Cyber Protect Home Office がドライブを MBR にフォーマットするように提案します。フラッシュドライブは Windows 10（ビルド 1703 以降）および Windows 11 のみでサポートされることに注意してください。

Acronis Survival Kit を作成するには、次のようにします。

システムパーティションのバックアップ、コンピューター全体、またはすべてのディスクバックアップを設定し、宛先として外付けのハードディスクドライブを選択すると、Acronis Cyber Protect Home Office は Acronis Survival Kit の作成を提案します。



1. **[今すぐバックアップ]** または **[Acronis Survival Kit の作成]** をクリックします。
2. 表示されたウィンドウで、**[作成]** をクリックします。

   Acronis Cyber Protect Home Office は選択されたドライブに小さなパーティションを作成して、そこにブートファイルを書き込みます。これを作成するために、既存のボリュームのいずれかのサイズが変更されます。ディスクが GPT ではなく、NTFS、FAT32、exFAT とは異なるファイルシステムを持つ場合、Acronis Cyber Protect Home Office はディスクのフォーマットを推奨します。ディスクをフォーマットすると、そのディスクに保存されているすべてのデータが消去されることに注意してください。
3. ブート ファイルが正常にドライブに書き込まれると、そのAcronis ブータブルメディアを使用して、コンピューターをリカバリすることができます。Acronis Survival Kit の作成を完了するには、システムパーティションのバックアップ、コンピューター全体、またはすべてのディスクバックアップをこのドライブに保存する必要があります。これを行うには、**[今すぐバックアップ]** をクリックします。この手順をスキップする場合、後からこのドライブにバックアップを作成することを忘れないでください。詳細については、「ディスクとパーティションのバックアップ」を参照してください。

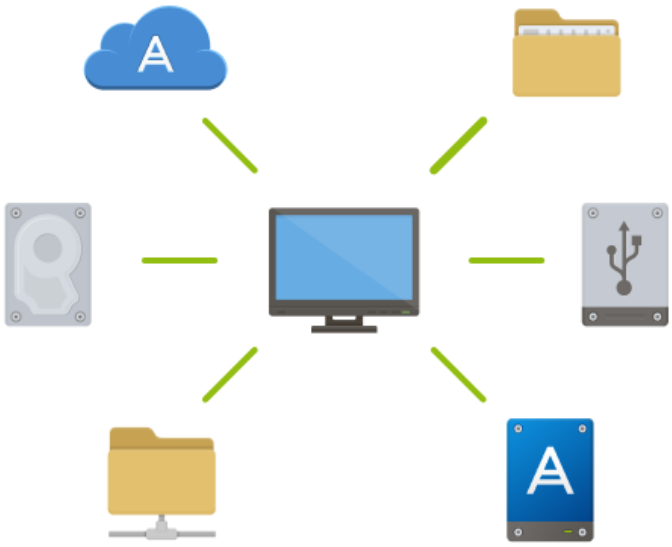
   Acronis Survival Kit の準備ができたら、それを使用してコンピューターをリカバリできます。詳細については、「同じディスクへのシステムのリカバリ」を参照してください。

外付けデバイスに Survival Kit のバックアップ作成を設定するごとに、Acronis Cyber Protect Home Office はそのバージョンを確認します。Survival Kit の最新バージョンが利用できる場合、Acronis Cyber Protect Home Office は外付けデバイスの Survival Kit を更新することを提案します。

ファイルのバックアップ

文書、写真、音楽のファイル、ビデオのファイルなどのファイルを保護するために、そのファイルを含むパーティション全体をバックアップする必要はありません。具体的なファイルとフォルダをバックアップして、以下のストレージ タイプに保存することができます。

- **ローカルまたはネットワーク ストレージ**
  時間がかからず、簡単です。ほとんど変更されないファイルの保護に使用します。
- **Acronis Cloud**
  信頼性が高いタイプです。重要なファイルや、デバイス間またはユーザー間で共有するファイルの保護に使用します。
  Acronis Cloud を使用するには、Acronis アカウントと、Acronis Cloud サービスのサブスクリプションが必要です。
  詳細については、「"サブスクリプション情報"（35ページ）」を参照してください。



ファイルやフォルダをバックアップする手順は、次のとおりです。

1. Acronis Cyber Protect Home Office を開始します。
2. サイドバーで **[バックアップ]** をクリックします。
3. **[バックアップ ソース]** アイコンをクリックし、**[ファイルとフォルダ]** を選択します。
4. 表示されたウィンドウで、バックアップするファイルやフォルダの横にあるチェック ボックスをオンにし、**[OK]** をクリックします。
5. **[バックアップの保存先]** アイコンをクリックし、バックアップの保存先を選択します。
   - **Acronis Cloud** - マイアカウントにサインインし、**[OK]** をクリックします。
   - **外付けドライブ**: 外付けドライブがコンピュータに接続されている場合は、リストからそのドライブを選択できます。

- **NAS**: 検出されたNASデバイスのリストからNASを選択します。NAS が 1 つしかない場合、Acronis Cyber Protect Home Office はデフォルトでその NAS をバックアップの保存先として使用するように提案します。
- **参照**: フォルダ ツリーから保存先を選択します。

6. **[今すぐバックアップ]** をクリックします。

詳細については、「ファイルやフォルダのバックアップ」を参照してください。

さらに、https://goo.gl/i4J1AN のビデオ解説（英語）をご覧ください。

ハードディスクドライブのクローン作成

ハード ディスク ドライブのクローン作成が必要な理由

ハード ディスク ドライブの空き領域が不足してデータを保存できない場合は、容量の大きい新しいハード ディスク ドライブを購入し、すべてのデータをその新しいドライブに転送することが必要になる可能性があります。通常のコピー処理では、新しいハード ディスク ドライブを古いハード ディスク ドライブとまったく同じように使用することはできません。たとえば、File Explorerを開いて、すべてのファイルとフォルダを新しいハードディスクドライブにコピーしても、Windowsは新しいハードディスクドライブから起動しません。ディスクのクローン作成ユーティリティでは、すべてのデータを複製し、Windowsを新しいハードディスクドライブでブータブルにすることができます。

開始する前に

転送先（新しい）ドライブをコンピュータに取り付けてから、転送元ドライブを別の場所（外付けのUSBエンクロージャなど）に取り付けることをお勧めします。これは特にラップトップ コンピュータの場合に重要です。

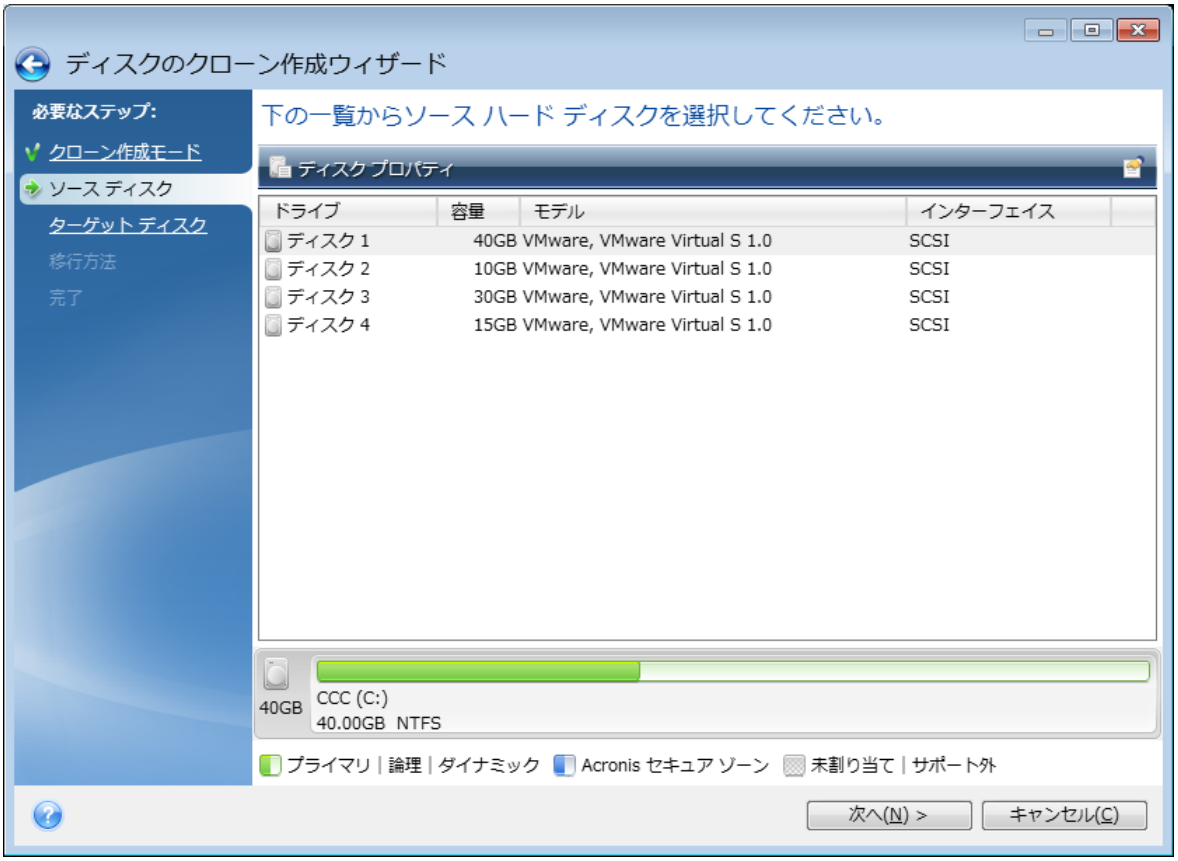
注意
古いハードディスクドライブと新しいハードディスクドライブは同じコントローラーモード（IDE、AHCI など）で動作させることをお勧めします。モードが異なる場合、新しいハードドライブからコンピュータを起動できなくなる可能性があります。

ディスクのクローン作成

1. ツールバーの **[ツール]** をクリックし、**[ディスクのクローン作成]** をクリックします。
2. **[クローン作成モード]** で、転送モードとして **[自動]** を選択することをお勧めします。この場合、パーティションは新しいハードディスクドライブの大きさに比例してサイズが変更されます。**[手動]** モードでは、さらに柔軟に対応できます。手動モードの詳細については、「ディスクのクローン作成ウィザード」を参照してください。

   注意
   ディスクが 2 つ検出されて、一方にパーティションがあり、他方にはない場合は、パーティションのあるディスクが自動的にソース ディスクとして認識され、パーティションのないディスクがターゲット ディスクとして認識されます。これに該当する場合は、以降のステップが省略され、クローン作成の概要画面が表示されます。

3. **[ソース ディスク]** で、クローンを作成するディスクを選択します。



4. **[ターゲット ディスク]** で、クローン データの保存先ディスクを選択します。

注意
パーティションが作成されていないディスクがある場合は、そのディスクが自動的に移行先と見なされるため、このステップは省略されます。

5. **[完了]** で、指定した設定がニーズに合っていることを確認してから、**[実行]** をクリックします。

デフォルトでは、クローン作成処理が完了すると、コンピューターは Acronis Cyber Protect Home Office により自動的にシャットダウンされます。これにより、マスターとスレーブのジャンパ位置を変更し、1 台のハード ディスクを取り外すことができます。

さらに、https://goo.gl/bjWRLL のビデオ解説（英語）をご覧ください。

コンピュータのリカバリ

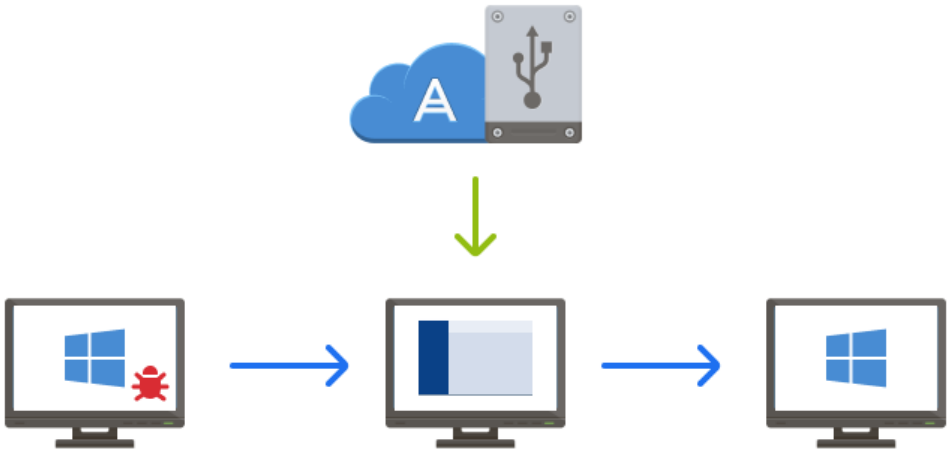
システムディスクのリカバリは重要な処理です。開始する前に、以下のヘルプトピックにある詳細な説明を参照することをお勧めします。

- 異常停止の原因を特定する
- リカバリの準備
- 同じディスクへのシステムのリカバリ

次の異なる2つのケースを例にあげます。

1. Windows は正しく動作していないが、Acronis Cyber Protect Home Office は起動できる。
2. Windowsを起動できない（たとえば、コンピュータの電源を入れても画面に表示される内容が通常とは異なる）。

ケース1. Windowsが正しく動作しない場合のコンピュータのリカバリ方法

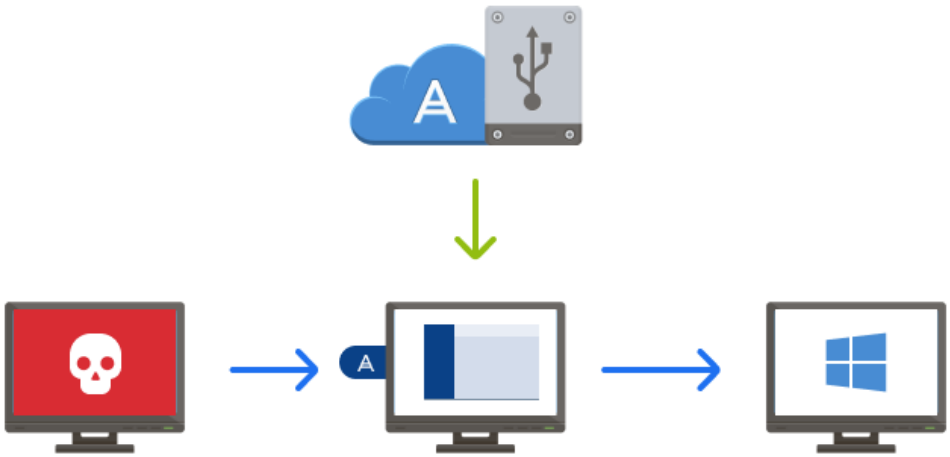


1. Acronis Cyber Protect Home Office を開始します。
2. サイドバーで **[バックアップ]** をクリックします。

3. バックアップ リストから、システム ディスクが格納されているバックアップを選択します。 バックアップされている場所は、ローカルストレージ、ネットワークストレージ、または Acronis Cloud にあります。
4. 右側のペインで、**[リカバリ]** をクリックします。
5. バックアップの種類に応じて、**[PCをリカバリ]**、または **[ディスクをリカバリ]** をクリックします。
6. 表示されたウィンドウで、バックアップバージョン（特定の日時のデータ状態）を選択します。
7. リカバリするシステムパーティションとシステム予約パーティション（存在する場合）を選択します。
8. **[今すぐリカバリ]** をクリックします。

注意
処理を完了するには、Acronis Cyber Protect Home Office でシステムを再起動する必要があります。

ケース2. Windowsを起動できない場合のコンピュータのリカバリ方法



1. Acronis ブータブルメディア をコンピューターに接続し、専用のスタンドアロン版の Acronis Cyber Protect Home Office を実行します。
   詳細については、「手順 2 Acronis ブータブルメディア の作成」と「BIOS での起動順の並べ替え」を参照してください。
2. [ようこそ] 画面で、**[リカバリ]** の下にある **[マイ ディスク]** を選択します。
3. リカバリに使用するシステム ディスク バックアップを選択します。バックアップを右クリックして、**[リカバリ]** を選択します。
   バックアップが表示されない場合には、**[参照]** をクリックし、バックアップのパスを手動で指定します。 同じウィンドウで、Acronis Cloud に接続してオンラインバックアップを選択することもできます。詳細については、「Acronis Cloud からのシステムの復元」を参照してください。
4. **[リカバリの方法]** で、**[ディスクまたはパーティション全体をリカバリする]** を選択します。

5. **[リカバリ元]** 画面で、システム パーティション（通常は C）を選択します。システム パーティションは Pri フラグ、Act フラグでも識別できます。システム予約パーティションも選択します（存在する場合）。
6. パーティションの設定をすべてそのままにし、**[完了]** をクリックしてもかまいません。
7. 処理の概要を確認して **[実行]** をクリックします。
8. 処理が終了したら、スタンドアロン版の Acronis Cyber Protect Home Office を終了し、ブータブルメディアがある場合はそれを取り外して、リカバリされたシステムパーティションから起動します。必要な状態まで Windows をリカバリしたことを確認してから、元の起動順序を復元します。

Acronis アカウント

次の場合に Acronis アカウントが必要になります。

- Acronis 製品を登録する。
- Acronis Cloud にバックアップする。
- データの同期化
- データのアーカイブ作成

Acronis アカウントを作成するには、次のようにします。

1. サイドバーの **[アカウント]** をクリックし、**[サインインまたはアカウントの作成]** をクリックします。
2. **[アカウントの作成]** をクリックします。
3. 登録フォームに入力します。必要なデータを提供し、利用規約に同意し、さらにオプションで、ニュースとプロモーション情報を時々受け取るようにサブスクライブします。

   注意
   個人データを安全に維持するために、オンラインバックアップ用の強力なパスワードを選択して、悪意のある第三者に知られないように保護し、時々変更してください。

4. **[アカウントの作成]** をクリックします。
5. 登録した電子メールアドレスに電子メール メッセージが送信されます。このメッセージを開き、アカウントの作成を確認して登録を完了します。

お持ちの Acronis アカウントでサインインするには、次の手順を実行します。

1. サイドバーの **[アカウント]** をクリックし、**[サインインまたはアカウントの作成]** をクリックします。
2. 登録する電子メールアドレスとパスワードを入力し、**[サインイン]** をクリックします。

Acronis のマイアカウントからサインアウトするには、次の手順を実行します。

1. サイドバーで **[アカウント]** をクリックします。
2. 電子メールアドレスをクリックし、**[サインアウト]** を選択します。

Acronis Cloud の操作

注意
お住まいの地域では、Acronis Cloud をご利用いただけません。詳細は、https://kb.acronis.com/content/4541 を参照してください。

リモート ストレージ

一方、Acronis Cloud は、バックアップを保存するために使用できる安全なリモートストレージです。

- ファイルやフォルダのバックアップ
- パーティションやディスクのバックアップ
- 同期したファイルやフォルダの各バージョン

ファイルはリモートストレージに保管されるので、コンピュータが盗難や火災に遭っても、データは保護されます。災害やデータ破損が発生した場合でも、ファイルはもちろん、コンピュータ全体の内容を復元することもできます。

1つのアカウントで、複数のコンピュータのデータを保存したり、iOSおよびAndroidオペレーティングシステムを実行しているすべてのモバイルデバイスのデータを保存したりできます。

Acronis Cloud の使用を開始するには、サービスへのサブスクリプションが必要になります。詳細については、「サブスクリプション情報」を参照してください。

ウェブ アプリケーション

また、Acronis Cloud は、Acronis Cloud に保存したデータのリカバリと管理に使用できる Web アプリケーションでもあります。インターネットに接続されている任意のコンピュータを使用して、アプリケーションを操作することができます。

アプリケーションにアクセスするには、https://www.acronis.com/my/online-backup/webrestore/ に移動し、Acronis アカウントにログインします。

データのセキュリティを確保する方法

Acronis Cloud をストレージとして使用している場合は、個人用ファイルが犯罪者に悪用されないようにする必要があります。モバイルデバイスの場合はすべてのデータがインターネット経由で転送されるので特に注意する必要があります。

アクロニスはデータの安全性を保証します。第 1 に、インターネットと LAN の両方で暗号化されたプロトコル（SSL、TLS）を使用してすべてのデータを転送します。データにアクセスするには、アカウントの電子メールアドレスとパスワードを入力することによってアカウントにサインインします。第 2 に、保護された Wi-Fi ネットワークだけを使用してデータをバックアップするよう選択できます。その場合、Acronis Cloud に転送される際のデータが完全に保護されます。[設定] で、安全な **[バックアップ用の Wi-Fi ネットワーク]** を選択してください。

サブスクリプション情報

Acronis Cloud を使用する Acronis Cyber Protect Home Office 機能（オンラインバックアップ、クラウドアーカイブ、クラウド同期など）を使用する場合は、Acronis Cloud Storage へのサブスクリプションが必要です。サブスクリプションを申し込むには、Acronis Cyber Protect Home Office を起動して **[アカウント]** タブに移動し、トライアルサブスクリプションを開始するか、製品版のサブスクリプションを購入するかを選択します。

注意
Acronis Cloud は、公正使用ポリシーの対象になります。詳細については、https://kb.acronis.com/ati/fairusage を参照してください。

試用版

試用版を有効化すると、Acronis Cyber Protect Home Office 試用期間にわたる 1,000 GB のストレージと Acronis Cloud 無料サブスクリプションがマイアカウントに自動的に割り当てられます。詳細については、「試用版情報」を参照してください。

製品版

お使いのバージョンの Acronis Cyber Protect Home Office の **[アカウント]** セクション、または Acronis Web サイトで製品版の Acronis Cloud サブスクリプションが購入できます。詳細については、「Acronis Cyber Protect Home Office のアップグレード」を参照してください。

基本的な概念

ここでは、プログラムの動作のしくみを理解するうえで役立つと思われる、基本的な概念について説明します。

バックアップとリカバリ

バックアップとは、元のデータが失われてもそのコピーから**リカバリ**できるように、データのコピーを作成しておくことを指します。

バックアップの主な目的は 2 つあります。

- 1つは、オペレーティングシステムが破損した場合や起動しない場合に復元するという目的です（災害復旧といいます）。災害からのコンピュータの保護の詳細については、「システムの保護」を参照してください。
- もう1つは、ファイルやフォルダが誤って削除されたり破損した後に、特定のファイルやフォルダを復元するという目的です。

Acronis Cyber Protect Home Office は、この最初の目的を達成するために、ディスク（またはパーティション）イメージの作成機能を備え、第 2 の目的のために、ファイルレベルバックアップ作成機能を備えています。

リカバリの方法:

- **完全リカバリ**: 元のロケーションまたは新しいロケーションにリカバリできます。
  元のロケーションを選択すると、バックアップのデータで完全に上書きされます。新しいロケーションの場合、データはバックアップから新しいロケーションに単にコピーされます。
- **増分リカバリ**: 元のロケーションのみへ、クラウドバックアップのみからのリカバリを実行します。
  リカバリ開始前に、元のロケーションのファイルとバックアップ内のファイルのファイル属性（ファイルサイズ、最終更新日など）が比較されます。一致しなかったファイルはリカバリ用にマークが付けられ、その他のファイルはリカバリ中スキップされます。このように完全リカバリとは異なり、Acronis Cyber Protect Home Office は変更されたファイルだけをリカバリします。この方法ではリカバリ時間が大きく削減され、Acronis Cloud からのリカバリ中のインターネットトラフィックが節約されます。

バックアップ バージョン

バックアップ バージョンは、それぞれのバックアップ処理中に作成された単独または複数のファイルです。作成されるバージョンの数は、バックアップが実行された回数と常に同じになります。つまり、バージョンはそれぞれ特定の時点を表しており、その時点の状態にシステムやデータを復元することができます。

バックアップ バージョンは、完全バックアップ、増分バックアップ、および差分バックアップを表しています。「完全バックアップ、増分バックアップ、差分バックアップ」を参照してください。

バックアップ バージョンは、ファイル バージョンと似ています。ファイルバージョンという考えは、「以前のバージョンのファイル」と呼ばれているWindowsの機能を使用しているユーザーにはよく知られています。この機能を使用すると、ファイルを特定の日時における状態に復元できます。バックアップ バージョンを使用すると、同様の方法でデータをリカバリできます。

ディスクのクローン作成

これは、1 つのディスク ドライブの内容全体を別のディスク ドライブにコピーする処理です。たとえば、オペレーティング システム、アプリケーション、およびデータのクローンを、より容量の多い新しいディスクに作成する場合などに、この機能が必要となる場合があります。このことは 2 つの方法で実行できます。

- ディスクのクローン作成ユーティリティを使用する方法。
- 古いディスクドライブをバックアップし、その後新しいディスクドライブにリカバリする方法。

バックアップ ファイルの形式

Acronis Cyber Protect Home Office では通常、バックアップデータは独自の TIBX 形式で圧縮して保存されます。.tibx ファイルのバックアップのデータは、Windows 環境またはリカバリ環境で Acronis Cyber Protect Home Office を使用した場合にのみ復元できます。

Acronis Nonstop Backupでは、データおよびメタデータ用に特殊な隠しストレージが使用されています。バックアップ データは圧縮され、約 1 GB の複数のファイルに分割されます。また、これらのファイルには独自の形式が採用されており、保存されたデータは、Acronis Cyber Protect Home Office のみを使用して復元できます。

バックアップのベリファイ

バックアップのベリファイ機能を使用すれば、データをリカバリできるかどうかを確認できます。バックアップされるデータブロックにはチェックサム値が追加されます。バックアップベリファイの実行時に、Acronis Cyber Protect Home Office はバックアップファイルを開いてチェックサム値を再計算し、保存されているチェックサム値と比較します。比較した値がすべて一致していれば、そのバックアップファイルは破損していません。

スケジュール設定

作成したバックアップを実際に役立てるには、可能な限り最新のバックアップを作成しておく必要があります。バックアップを自動的かつ定期的に実行するには、バックアップのスケジュールを作成します。

バックアップの削除

不要になったバックアップとバックアップバージョンを削除する場合は、Acronis Cyber Protect Home Office に用意されているツールを使用してください。詳細については、「バックアップとバックアップバージョンの削除」を参照してください。

Acronis Cyber Protect Home Office は、バックアップに関する情報をメタデータ情報データベースに保存します。そのため、不要なバックアップファイルをFile Explorerで削除しても、バックアップに関する情報はデータベースから削除されません。その結果、既に存在していないバックアップに対してもプログラムが処理を実行しようとして、エラーが発生します。

ファイル バックアップとディスク/パーティション イメージの違い

ファイルとフォルダをバックアップする場合、ファイルとフォルダ ツリーのみが圧縮されて保存されます。

ディスク/パーティションのバックアップは、ファイルとフォルダのバックアップとは異なります。Acronis Cyber Protect Home Office では、ディスクまたはパーティションの正確なスナップショットが保存されます。この処理は「ディスク イメージの作成」または「ディスク バックアップの作成」と呼ばれ、作成されたバックアップは一般的に「ディスク/パーティション イメージ」または「ディスク/パーティション バックアップ」と呼ばれます。

ディスク/パーティション バックアップに含まれるもの

ディスク/パーティションのバックアップには、ディスクまたはパーティションに保存されているすべてのデータが含まれます。

1. マスター ブート レコード（MBR）があるハード ディスクのゼロ トラック（MBR ディスク バックアップのみに適用）。
2. 以下を含む、1 つ以上のパーティション
   a. ブート コード。
   b. サービス ファイル、ファイル アロケーション テーブル（FAT）、およびパーティション ブート レコードを含むファイルシステム メタ データ。
   c. オペレーティング システム（システム ファイル、レジストリ、ドライバ）、ユーザー データ、およびソフトウェア アプリケーションを含むファイルシステム データ。
3. システム予約済みパーティション（存在する場合）。
4. EFI システム パーティション（存在する場合）（GPT ディスク バックアップにのみ適用）。

ディスク バックアップから除外されるもの

イメージファイルのサイズを減らしてイメージの作成速度を速めるため、Acronis Cyber Protect Home Office では、データが含まれているハードディスクセクタのみがデフォルトで保存されます。

Acronis Cyber Protect Home Office では、次のファイルがディスクバックアップから除外されます。

- pagefile.sys
- hiberfil.sys（コンピュータが休止状態に移行するときに RAM の内容を保持するファイル）

このデフォルトの方法は、セクタ単位モードをオンにすることで、変更できます。この場合、Acronis Cyber Protect Home Office では、含まれるデータだけではなく、すべてのハードディスクセクタがコピーされます。

また、Acronis Cyber Protect Home Office でシステムパーティションまたはディスクを Acronis Cloud にバックアップする場合は、次のデータが除外されます。

- 通常は次の場所にあるTempフォルダ:
  - C:¥Windows¥Temp¥
  - C:¥Users¥<username>¥AppData¥Local¥Temp
- System Volume Information フォルダ（通常は C:¥System Volume Information¥ にあります）
- ごみ箱
- ウェブブラウザの一時データ:
  - インターネット一時ファイル
  - Cookie
  - 履歴
  - キャッシュ
- .tib ファイルと .tibx ファイル
- .tmp ファイル
- .~ ファイル

完全バックアップ、増分バックアップ、差分バックアップ

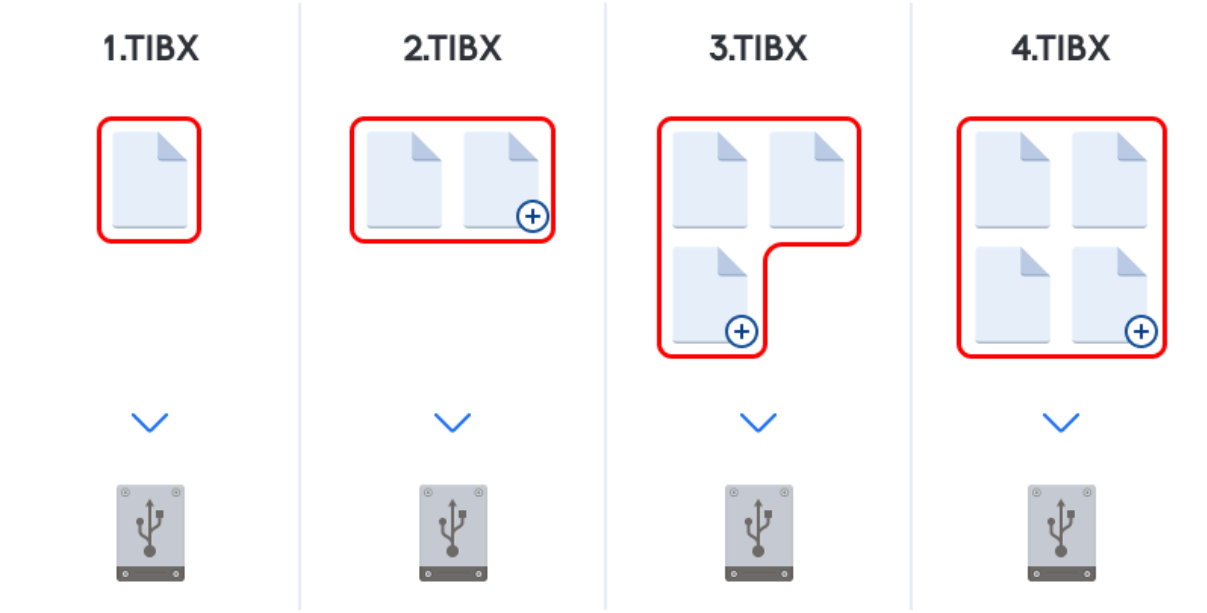
Acronis Cyber Protect Home Office では、完全、増分、差分の 3 つのバックアップメソッドが提供されます。

完全バックアップ

完全バックアップ処理（別名「完全バックアップ バージョン」）の結果には、バックアップ作成時のすべてのデータが含まれます。

例: 毎日、ドキュメントの 1 ページを書き、完全バックアップを使用してバックアップします。Acronis Cyber Protect Home Office は、バックアップを実行するたびにドキュメント全体を保存します。

1.tibx、2.tibx、3.tibx、4.tibx — 完全バックアップバージョンのファイル。



追加情報

完全バックアップ バージョンは、増分バックアップや差分バックアップの基になるデータとなります。スタンドアロンのバックアップとしても使用できます。スタンドアロンの完全バックアップは、システムを最初の状態に戻すことが多い場合や、複数のバックアップ バージョンを管理することが望ましくない場合に最適なソリューションです。

復元: 上の例では、4.tibx ファイルから作業全体を復元するには、1 つのバックアップバージョン (4.tib) だけが必要になります。

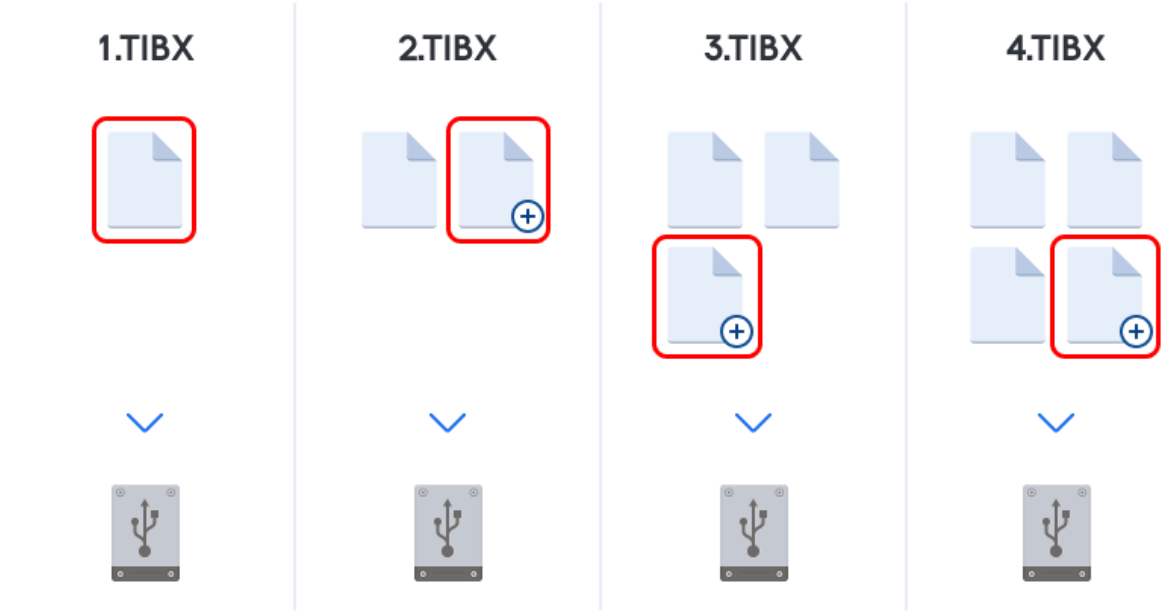
増分バックアップ

増分バックアップ処理（別名「増分バックアップ バージョン」）の結果には、前回のバックアップ以降に変更されたファイルのみが含まれます。

例: 毎日、ドキュメントの 1 ページを書き、増分バックアップを使用してバックアップします。Acronis Cyber Protect Home Office は、バックアップを実行するたびに新しいページを保存します。

注意: 作成する最初のバックアップバージョンは必ず完全バックアップである必要があります。

- 1.tibx — 完全バックアップバージョンのファイル。
- 2.tibx、3.tibx、4.tibx — 増分バックアップバージョンのファイル。



追加情報

増分バックアップは、頻繁なバックアップと特定の時点に戻す機能が必要な場合に非常に便利です。一般に、増分バックアップ バージョンは完全バージョンや差分バージョンに比べてかなり小さくなります。一方、増分バージョンでは、リカバリの実行時にプログラムでの処理が増加します。

復元: 上の例で 4.tibx ファイルから作業全体を復元するには、すべてのバックアップバージョン (1.tibx、2.tibx、3.tibx、4.tibx) が必要になります。そのため、1 つの増分バックアップ バージョンを失ったり、破損したりすると、それ以降のすべての増分バックアップ バージョンが使用できなくなります。

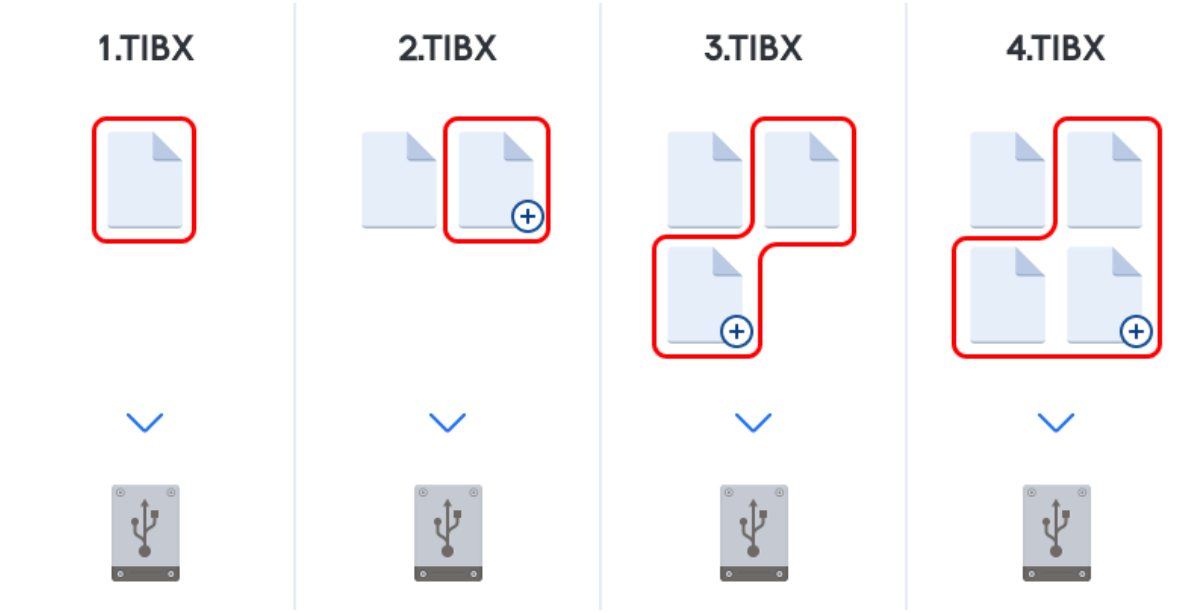
差分バックアップ

差分バックアップ処理（別名「差分バックアップ バージョン」）の結果には、前回の完全バックアップ以降に変更されたファイルのみが含まれます。

例: 毎日、ドキュメントの 1 ページを書き、差分バックアップを使用してバックアップします。Acronis Cyber Protect Home Office は、完全バックアップバージョンに保存された最初のページ以外のドキュメント全体を保存します。

注意: 作成する最初のバックアップバージョンは必ず完全バックアップである必要があります。

- 1.tibx — 完全バックアップバージョンのファイル。
- 2.tibx、3.tibx、4.tibx — 差分バックアップバージョンのファイル。



追加情報

差分バックアップは、前述の 2 つの方法の中間的な方法です。完全バックアップよりもかかる時間と領域は少ないですが、増分バックアップよりは多くなります。差分バックアップバージョンからデータをリカバリする場合、Acronis Cyber Protect Home Office には差分バージョンと最後の完全バージョンのみが必要です。そのため、差分バージョンからのリカバリは、増分バージョンからのリカバリより単純で、信頼性が高くなります。

復元: 上の例で 4.tibx ファイルから作業全体を復元するには、2つのバックアップバージョン (1.tibx および 4.tibx) が必要になります。

目的のバックアップ方法を選択するには、通常、カスタム バックアップ スキームを設定する必要があります。詳細については、「カスタム スキーム」を参照してください。

注意
ディスクを最適化した後に、増分バックアップ、または差分バックアップを作成すると、通常に比べかなり大きなサイズになります。これは、ディスクの最適化プログラムによってディスク上のファイルの位置が変更され、バックアップにこれらの変更が反映されるためです。このため、ディスク最適化後に、完全バックアップを再度作成することをお勧めします。

Changed Block Tracker (CBT)

CBTテクノロジにより、ローカル増分または差分のディスクレベルのバックアップバージョンを作成する場合にバックアップ処理を迅速に行うことができます。ディスクコンテンツに対する変更は、ブロックレベルで継続的に追跡されます。バックアップが開始されたら、それらの変更をバックアップにすぐに保存することができます。

バックアップの保存場所の決定

Acronis Cyber Protect Home Office では、さまざまなストレージデバイスがサポートされています。詳細については、"サポートされるストレージ メディア"（14ページ） をご参照ください。

次の表にデータバックアップの保存先の候補を示します。

	HDD*	SSD*	USB フラッシュドライブ	Acronis Cloud	NASやNDASなどのファイルサーバー	ネットワーク共有	SMB	FTP	DVD	メモリカード
MBRパーティションまたはディスク全体（HDD、SSD）	+	+	+	+	+	+	+	+	+	+
GPT/ダイナミックボリュームまたはディスク	+	+	+	+	+	+	+	+	+	+
ファイルとフォルダ	+	+	+	+	+	+	+	+	+	+

* 内蔵または外付け。

ローカルハードドライブへのバックアップは最もシンプルなオプションですが、データのセキュリティを強化するためにオフサイトにバックアップを保存することをおすすめします。

推奨されるストレージメディア:

1. **Acronis Cloud**
2. **外付けドライブ**

   デスクトップPCで外付けのUSBハードドライブを使用する場合には、短いケーブルを使用してドライブを背面のコネクタに接続することをおすすめします。
3. **NASやNDASなどのホームファイルサーバー**

   Windows の場合とブータブルメディアからの起動の場合の両方について、選択したバックアップストレージが Acronis Cyber Protect Home Office によって検出されるかどうかを確認してください。

   NDAS対応のストレージデバイスにアクセスするには、多くの場合NDASデバイスID（20文字）と書き込みキー（5文字）を指定する必要があります。書き込みキーを使用すると、NDAS対応のデバイスを書き込みモード（バックアップの保存など）で使用できます。通常、デバイス ID と書き込み

キーは NDAS デバイスの底面のステッカーまたはエンクロージャの内側に記載されています。ステッカーが見つからない場合は、NDAS デバイスの製造元に問い合わせてこの情報を入手してください。

4. **ネットワーク共有**
   「認証の設定」も参照してください。
5. **FTPサーバー**
   「FTP接続」も参照してください。
6. **光学ディスク（CD、DVD、BD）**
   DVD-R、DVD+R などの空の光学ディスクは非常に価格が安いため、最も低コストなバックアップソリューションではありますが、時間は一番かかります。
   ディスクが 4 枚以上になる場合はディスクの入れ替えが頻繁になるため、DVD 以外の方法でバックアップすることを強くおすすめします。DVDへのバックアップ以外に方法がない場合、すべてのDVDをハードディスク上のフォルダにコピーし、そのフォルダから復元することをおすすめします。

バックアップ用の新しいディスクを準備する

新しい内蔵または外付けのハードドライブは Acronis Cyber Protect Home Office で認識されない場合があります。この場合、オペレーティングシステムのツールを使用してディスクステータスを **[オンライン]** にして、ディスクを初期化します。

ディスクステータスを [オンライン] に変更する手順は、次のとおりです。

1. **[ディスクの管理]** を開きます。これを行うには、**[コントロール パネル]** → **[システムとセキュリティ]** → **[管理ツール]** の順に選択します。**[コンピューターの管理]** を選択して **[ディスクの管理]** をクリックします。
2. **[オフライン]** と表示されているディスクを見つけます。ディスクを右クリックして、**[オンライン]** をクリックします。
3. ディスクステータスが **[オンライン]** に変更されます。その後、ディスクを初期化することができます。

ディスクを初期化する手順は、次のとおりです。

1. **[ディスクの管理]** を開きます。これを行うには、**[コントロール パネル]** → **[システムとセキュリティ]** → **[管理ツール]** の順に選択します。**[コンピューターの管理]** を選択して **[ディスクの管理]** をクリックします。
2. **[初期化されていません]** と表示されているディスクを見つけます。ディスクを右クリックして、**[ディスクの初期化]** をクリックします。
3. ディスクのパーティションテーブル（MBRまたはGPT）を選択して、**[OK]** をクリックします。
4. （オプションの手順）ディスクにボリュームを作成するには、ディスクを右クリックし、**[新しいシンプル ボリューム]** をクリックして、ウィザードの手順に従って新しいボリュームを設定します。ボリュームをもう1つ作成するには、この手順を繰り返します。

FTP接続

Acronis Cyber Protect Home Office を使用すれば、FTP サーバーにバックアップを保存できます。

新しいFTP接続を作成するには、バックアップストレージの選択時に **[FTP接続]** をクリックし、開いたウィンドウに次の情報を入力します。

- FTPサーバーへのパス（例: my.server.com）
- ポート
- ユーザー名
- パスワード

設定を確認するには、**[接続のテスト]** ボタンをクリックします。コンピュータで、指定したFTPサーバーに対する接続が試行されます。テスト接続が確立された場合、**[接続]** ボタンをクリックして、FTP接続を追加します。

作成したFTP接続は、フォルダツリーに表示されます。接続を選択し、使用するバックアップストレージを参照します。

注意
単に FTP サーバーのルートフォルダを開いても、ユーザーのホームディレクトリに移動することはありません。

注意
FTPサーバーから直接復元するデータの場合、バックアップはそれぞれが2 GB以下のファイルで構成される必要があります。

注意
このため、Acronis Cyber Protect Home Office は、FTP サーバーに直接バックアップするときにバックアップを 2 GB ずつのサイズのファイルに分割します。バックアップを後でFTPサーバーに転送するためにハードディスクにバックアップする場合は、バックアップオプションでファイルサイズを設定することでバックアップを2 GBずつのファイルに分割することができます。

注意
FTPサーバー側がパッシブモードのファイル転送を許可している必要があります。

注意
バックアップ元のコンピュータのファイアウォール設定では、ポート20および21がTCPプロトコルとUDPプロトコル用に開いており、機能するようになっていることが必要です。Windows の**ルーティングとリモート アクセス** サービスは無効にする必要があります。

認証設定

ネットワーク上のコンピュータに接続する場合、通常、ネットワーク共有にアクセスするために必要なログイン情報を入力する必要があります。たとえば、バックアップストレージを選択する際にこの操作が必要になることがあります。ネットワーク上のコンピュータの名前を選択すると、**[認証設定]** ウィンドウが自動的に表示されます。

必要に応じて、ユーザー名とパスワードを指定し、**[接続のテスト]** をクリックします。テストが成功した場合は、**[接続]** をクリックします。

トラブルシューティング

バックアップストレージとして使用する予定のネットワーク共有を作成する場合は、以下の条件のうち少なくとも 1 つを満たしていることを確認してください。

- 共有フォルダが置かれているコンピュータのWindowsアカウントにパスワードが設定されている。
- Windowsのパスワード保護共有が無効になっている。
  たとえば、Windows 7では、**[コントロール パネル]** → **[ネットワークとインターネット]** → **[ネットワークと共有センター]** → **[共有の詳細設定]** → [パスワード保護の共有を無効にする] でこの設定を確認できます。

これらの条件のいずれも満たしていない場合は、共有フォルダに接続できません。

Acronis Nonstop Backup

Acronis Nonstop Backupを利用すると、ディスクとファイルを簡単に保護することができます。ディスク全体や個々のファイル、別のバージョンをリカバリすることができます。

Acronis Nonstop Backupの主要な目的はデータ（ファイル、フォルダ、連絡先など）の継続的な保護ですが、パーティションの保護に使用することもできます。パーティション全体の保護を選択すると、イメージ リカバリ手順を使用して、パーティション全体をリカバリできるようになります。

システムを保護するための主要な手段として、ノンストップバックアップを使用することはおすすめしません。システムの安全のため、ほかのスケジュールをご使用ください。例と詳細については、「カスタムスキームの例」を参照してください。

Nonstop Backupの制限

- ノンストップ バックアップを 1 つのみ作成できます。
- Acronis Cloud は、ディスクレベルのノンストップバックアップの保存先として使用できません。
- Windowsライブラリ（ドキュメント、ミュージックなど）は、ディスクレベルのノンストップバックアップでのみ保護されます。
- 外付けハードドライブに保存されているデータを保護することはできません。
- Nonstop BackupとTry&Decideを同時に有効にすることはできません。

動作

Acronis Nonstop Backupを起動すると、保護対象として選択されているデータの、最初の完全バックアップが実行されます。その後、Acronis Nonstop Backupによって、保護対象のファイル（開いているファイルを含む）が継続的にチェックされます。変更が検出されると、変更されたデータがバックアップされます。増分バックアップ処理の最短間隔は5分です。この機能によって、指定した時間の状態にシステムをリカバリすることが可能になります。

Acronis Nonstop Backupでは、ディスク上のファイルの変更が確認されますが、メモリ内は確認されません。例えば、Word での作業中に長時間保存していない場合、Word 文書内の現在の変更内容はバックアップされません。

このバックアップ頻度ではストレージはすぐにいっぱいになると思われるかも知れません。ですが、Acronis Cyber Protect Home Office は「デルタ」と呼ばれるもののみをバックアップするため、その心配はありません。これは、変更があったファイルのファイル全体ではなく、古いバージョンと新しいバージョンの相違点のみがバックアップされることを意味します。たとえば、Microsoft Outlook または Windows メールを使用している場合、pst ファイルのサイズが非常に大きい場合があります。また、電子メールを受信または送信するたびにファイルの内容が変わります。変更があるたびに pst ファイル全体をバックアップするとストレージスペースを消費しすぎるため、Acronis Cyber Protect Home Office は最初にバックアップしたファイルと共に、変更された部分のみをバックアップします。

保持ルール

ローカルバックアップ

Acronis Nonstop Backupでは、過去 24 時間分のバックアップがすべて保持されます。それよりも古いバックアップは日単位で統合され、過去30日分が保持されます。また、週単位のバックアップは、Nonstop Backupデータの保存先に空きがある限り保持されます。

統合は、深夜 0 時から午前 1 時の間に毎日実行されます。最初の統合は、Nonstop Backup を開始した後、少なくとも 24 時間経ってから実行されます。たとえば、Nonstop Backup を 7 月 12 日の午前 10 時にオンにしたと仮定します。この場合、最初の統合は、7 月 14 日の深夜 0 時から午前 1 時の間に実行されます。これ以降、データの統合は、毎日同じ時刻に実行されます。午前 00:00 から 01:00 の間にコンピュータの電源が入っていない場合は、コンピュータを起動したときに統合が開始されます。Nonstop Backup を一時的に無効にした場合は、次に有効したときに統合を開始します。

クラウドバックアップ

Acronis Cyber Protect Home Office は次のバージョンのバックアップのみを保持します。

- 過去 1 時間のすべてのバージョン
- 過去 24時間の 1時間ごとの最初のバージョン
- 前の週の各日の最初のバージョン
- 前の月の週ごとの最初のバージョン
- 各月の最初のバージョン

他のすべてのバージョンは自動的に削除されます。保持ルールはあらかじめ設定されており、変更することはできません。

Acronis Nonstop Backup のデータストレージ

Acronis Nonstop Backup のデータストレージは、ローカルハードディスクドライブ（内蔵と外付けの両方）または Acronis Cloud に作成できます。

多くの場合、Nonstop Backup のデータストレージには外付けのハードディスクを使用するのが最も良い方法です。（USB 3.0 を含む）USB、eSATA、FireWire、および SCSI のいずれかのインターフェイスを持つ外付けディスクを使用できます。

NASをストレージとして使用することもできますが、SMBプロトコルを使用したアクセスが必須になるという制限があります。ストレージに使用する NAS 共有がローカル ディスクとしてマップされるかど

うかは問われません。共有にログインが必要な場合は、正確なユーザー名とパスワードを指定する必要があります。詳細については、「認証設定」を参照してください。Acronis Cyber Protect Home Office では認証情報が記憶され、共有に対するその後の接続ではログインは必要ありません。

外付けハードディスクまたは NAS を使用できない場合は、Nonstop Backup を内蔵ディスク（ダイナミック ディスクを含む）に保存することができます。保護されるパーティションは、ノンストップ バックアップのストレージとしては使用できないことに留意してください。 コンピューターにハードディスクドライブが 1 つしかなく、その中にパーティションが 1 つしかない環境で Acronis Nonstop Backup を使用したい場合は、Acronis Secure Zone を作成してこれを Nonstop Backup のデータストレージとして使用できます。

Acronis Cyber Protect Home Office は、Acronis Nonstop Backup のデータストレージを作成する前に、選択した保存先に十分な空き領域があるかどうか確認します。保護するデータ量に 1.2 が乗算され、この乗算の計算結果の値と使用可能な容量が比較されます。保存先の空き容量がこの条件を満たした場合に、そのロケーションを Nonstop Backup データの保存先として使用します。

Nonstop Backup - FAQ

Acronis Nonstop Backupが一時停止するのはなぜですか？- これは、Acronis Nonstop Backupの設計上の動作です。システムの負荷が重大レベルに達すると、Acronis Nonstop Backupは Windows からオーバーロードアラームを受信して自動的に一時停止します。これは、他のアプリケーションによる Windows の負荷を軽減する役割を果たします。過負荷は、多くのリソースを必要とするアプリケーションを実行することにより発生する場合があります（ウィルス対策ソフトウェアによるシステム完全スキャンの実行など）。

このような場合、Nonstop Backup は自動的に一時停止し、ユーザーが再起動することはできません。一時停止の後、Acronis Nonstop Backupでは、1 時間後にシステムの負荷が軽減されてから再起動を試行します。

Acronis Nonstop Backupの自動再起動は 6 回試行されます。つまり、最初の自動再起動の後、Acronis Nonstop Backupは 1 時間ごとに 5 回再起動を試行します。

試行が 6 回失敗したら、Acronis Nonstop Backupは次の設定日まで待機します。翌日、自動再起動の回数が自動的にリセットされます。中断されない場合は、Acronis Nonstop Backupは 1 日に 6 回再起動を試行します。

再起動試行回数は、次のいずれかを実行することでリセットできます。

- Acronis Nonstop Backupサービスの再起動
- コンピュータの再起動

Acronis Nonstop Backupサービスを再起動しても、再起動の試行回数が 0 にリセットされるだけです。システムが依然として過負荷の状態にある場合、Acronis Nonstop Backupは再び一時停止になります。Acronis Nonstop Backupサービスの再起動については、https://kb.acronis.com/content/14708 を参照してください。

コンピュータを再起動すると、負荷および再起動回数がリセットされます。システムが再度過負荷状態になると、Acronis Nonstop Backupは一時停止します。

Acronis Nonstop Backupを実行するときに CPU の負荷が高くなることがあります。どうしてですか？- これは、Acronis Nonstop Backupの想定内の動作です。Acronis Nonstop Backupの一時停止中に大量の保護対象データが変更された場合、一時停止から再起動するときに発生することがあります。

たとえば、システムパーティションを保護するために使用している Acronis Nonstop Backupを手動で一時停止してから新しいアプリケーションをインストールするとします。この場合、Acronis Nonstop Backupを再起動したとき、しばらく CPU に負荷がかかります。ただし、処理（afcdpsrv.exe）は正常に戻ります。

これは、データが継続的に保護されていることを確認するために、Acronis Nonstop Backupが、バックアップされたデータを一時停止中に変更されたデータと比較してチェックする必要があるためです。変更されたデータが大量にある場合、処理にしばらく時間がかかり、CPU の負荷が高くなる場合があります。チェックが終了し、変更されたデータがすべてバックアップされた後、Acronis Nonstop Backupは正常に戻ります。

Acronis Nonstop Backupストレージは、ローカルハードディスクの FAT32 パーティションでも利用できますか？- はい、FAT32 と NTFS パーティションはストレージに使用できます。

Acronis Nonstop Backupストレージは、ネットワーク共有や NAS で設定できますか？- はい、Acronis Nonstop Backupは、ネットワーク共有、マップされたドライブ、NAS、その他のネットワーク接続デバイスをサポートします。ただし、制限事項として、これらは SMB プロトコルを使用する必要があります。

バックアップファイルの命名

バックアップが作成されたときのバージョンに応じて、名前が異なります。

Acronis True Image (2020 または 2021) および Acronis Cyber Protect Home Office で作成されたバックアップファイルの命名規則

バックアップファイルの名前は、バックアップの名前と増分カウンタだけからなります。バックアップ方法、バックアップチェーン番号、バックアップバージョン番号、ボリューム番号などの追加情報はまったく含まれません。

バックアップ名はたとえば次のようになります。

1. `my_documents.tibx`
2. `my_documents_0001.tibx`
3. `my_documents_0002.tibx`
4. `my_documents_0003.tibx`

完全バックアップと差分バックアップは別々のファイルに保存され、増分バックアップは自動的に完全バックアップに結合されます。

次のバックアップでは、引き続き TIB の形式および名前付け規則が使用されます:

- Acronis Cloud 以外のすべての保存先へのファイルレベルのバックアップ。Acronis Cloud へのファイルレベルのバックアップは .tibx 形式で行われます。

- ノンストップバックアップ
- 認証バックアップ
- CD/DVD/Blu-ray、FTP、または Secure Zone を保存先として使用するバックアップ

Acronis True Image 2020 より前のバージョンで作成されたバックアップファイルの命名規則

TIB バックアップファイル名には次の属性があります。

- バックアップ名
- バックアップ方法（full、inc、diff: 完全、増分、差分）
- バックアップチェーン[1]番号（b#形式）
- バックアップバージョン[2]番号（s# 形式）
- ボリューム番号（v#形式）

  たとえば、バックアップを複数のファイルに分割するとこの属性は変更されます。詳細については、「バックアップの分割」を参照してください。

たとえば、バックアップ名は次のようになります。

1. `my_documents_full_b1_s1_v1.tib`
2. `my_documents_full_b2_s1_v1.tib`
3. `my_documents_inc_b2_s2_v1.tib`
4. `my_documents_inc_b2_s3_v1.tib`

新たにバックアップを作成しているときに、既に同じ名前のファイルが存在する場合、プログラムによって古いファイルは削除されず、新しいファイルに「-number」サフィックスが追加されて、`my_documents_inc_b2_s2_v1-2.tib` のようになります。

Windowsとの統合

インストール時に Acronis Cyber Protect Home Office は Windows と緊密に統合されます。この統合により、コンピュータの能力を最大限に引き出すことができます。

Acronis Cyber Protect Home Office は以下のコンポーネントを統合します。

- Windows の **[スタート]** メニューに表示される Acronis のアイテム
- タスクバーの Acronis Cyber Protect Home Office ボタン
- ショートカットメニューコマンド

Windows の [スタート] メニュー

---

[1]最初の完全バックアップバージョンと、後続の 1 つまたは複数の増分または差分バックアップバージョンから構成される、最低 2 つのバックアップバージョンからなる一連のバックアップバージョンです。バックアップ バージョン チェーンは、次の完全バックアップ バージョン（存在する場合）まで続きます。

[2]単一のバックアップ操作の結果。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単独または一連のファイルです。Acronis Cyber Protect Home Office によって作成されるバックアップバージョンファイルの拡張子は .tibx です。バックアップバージョンの統合による TIBX ファイルもバックアップバージョンと呼ばれます。

[スタート] メニューに、Acronis コマンド、ツール、およびユーティリティが表示されます。これらを使用して Acronis Cyber Protect Home Office 機能にアクセスできます。アプリケーションを起動する必要はありません。

タスクバーの Acronis Cyber Protect Home Office ボタン

Windows タスクバーの Acronis Cyber Protect Home Office ボタンにより、Acronis Cyber Protect Home Office の処理の進行状況と結果を表示することができます。

トレイ通知センター

Acronis Cyber Protect Home Office が開いているときは、操作のステータスが表示されます。ただしバックアップなどの操作には時間がかかる可能性があるので、結果を知るために Acronis Cyber Protect Home Office を開いたままにしておく必要はありません。

トレイ通知センターには最近の通知が一か所に表示され、Acronis Cyber Protect Home Office を開かなくても、必要なときに重要な操作ステータスを確認できます。Acronis トレイ通知センターに表示される通知は、バックアップ操作の結果情報や、Acronis Cyber Protect Home Office からのその他の重要通知です。トレイ通知センターは最小化され、トレイの Acronis Cyber Protect Home Office の下で非表示になります。

ショートカットメニューコマンド

ショートカットメニューコマンドにアクセスするには、File Explorer を開いて、選択したアイテムを右クリックし、Acronis Cyber Protect Home Office をポイントしてコマンドを選択します。

- 新しいファイルレベルのバックアップを作成するには、**[新しいファイルのバックアップ]** を選択します。
- 新しいディスクレベルのバックアップを作成するには、**[新しいディスクのバックアップ]** を選択します。
- ディスクレベルバックアップ（.tibx ファイル）をマウントするには、**[マウント]** を選択します。
- バックアップ（.tibx ファイル）を検証するには、**[ベリファイ]** を選択します。

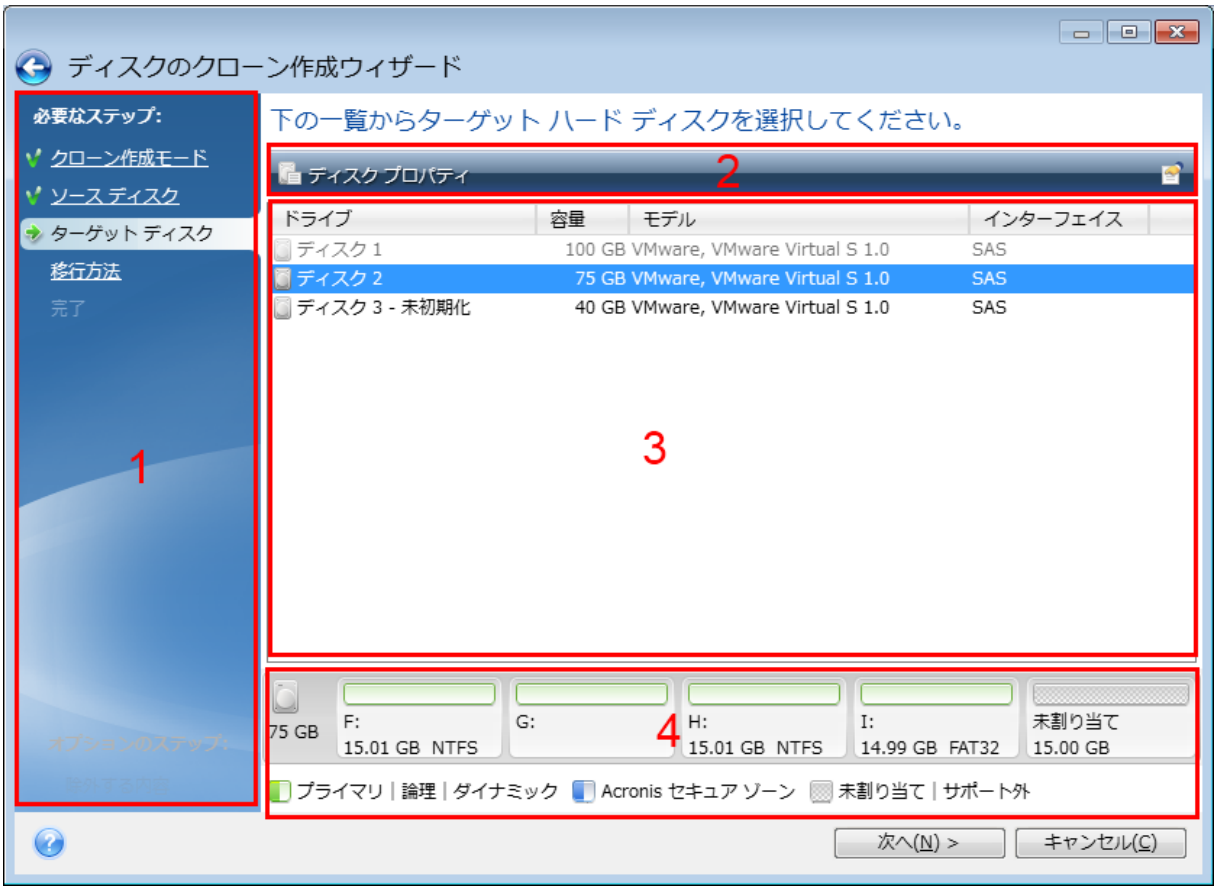
File Explorerでのファイルレベルの復元

1. File Explorer で、リカバリするデータが含まれているバックアップファイル（.tibx ファイル）をダブルクリックします。
2. ファイルおよびフォルダを、通常のディスクの場合と同様に、コンピュータ上の任意の場所にコピーまたはドラッグします。

ウィザード

利用可能な Acronis Cyber Protect Home Office ツールおよびユーティリティを使用する際、ほとんどの場合ウィザードが表示されるので、指示に従って処理を進めることが可能です。

たとえば、次のスクリーンショットをご覧ください。



ウィザード ウィンドウは、通常、次の領域で構成されています。

1. 処理を完了するうえで必要なステップのリスト。完了したステップの横には緑のチェックマークが表示されます。緑の矢印は現在処理中のステップを示します。すべてのステップが完了すると、**[完了]** ステップで概要画面が表示されます。概要を確認し、 **[実行]** をクリックして処理を開始します。
2. 領域 3 で選択するオブジェクトを管理するためのボタンが表示されたツールバー。
   たとえば、次のようになります。
   - **[詳細]**: 選択したバックアップに関する詳細な情報を提供するウィンドウが表示されます。
   - **[プロパティ]**: 選択した項目のプロパティ ウィンドウが表示されます。
   - **[新しいパーティションの作成]**: 新しいパーティションの設定を行えるウィンドウが表示されます。
   - **[項目]**: 表示する表の列とその表示順序を選択できます。
3. 項目を選択し、設定を変更する主要領域。
4. 領域 3 で選択する項目についての追加情報が表示される領域。

バックアップ、リカバリ、およびクローン作成に関する FAQ

- **150 GB のシステムパーティションがありますが、このパーティションで使用されている領域は 80 GB のみです。Acronis Cyber Protect Home Office にはバックアップには何が含められますか？** -

デフォルトで、Acronis Cyber Protect Home Office には、データを含むハードディスクセクタのみをコピーするため、バックアップには 80 GB のみが含まれます。セクタ単位モードを選択することもできます。このようなバックアップモードが必要なのは特殊な場合のみです。詳細については、「イメージ作成モード」を参照してください。セクタ単位モードのバックアップの作成中には、プログラムによって使用済みと未使用の両方のハードディスクセクタがコピーされるため、通常バックアップファイルは非常に大きくなります。

- **システムディスクのバックアップにドライバ、ドキュメント、画像などが含まれますか？** - はい、システムディスクのバックアップにはドライバが含まれ、さらにマイドキュメントフォルダのデフォルトのロケーションを変えていない場合、マイドキュメントフォルダとそのサブフォルダの内容も含まれます。PCに搭載されたハードディスクが1台のみの場合、このバックアップに、オペレーティングシステム、アプリケーション、およびデータのすべてが含まれます。
- **ノートブックに搭載されている古いハードディスクドライブがほとんどいっぱいになりました。容量の大きなHDDを新しく購入しました。Windows、プログラム、およびデータを新しいディスクに転送するにはどうすればよいですか？** - 古いハードディスクのクローンを新しいハードディスク上に作成するか、古いハードディスクをバックアップして、そのバックアップを新しいハードディスクにリカバリします。通常は、古いハードディスクのパーティションレイアウトに応じて最適な方法が決まります。
- **古いシステムのハードディスクをSSDに移行したいと思います。Acronis Cyber Protect Home Officeを使用してこの操作を実行できますか？** - はい、Acronis Cyber Protect Home Office にはその機能があります。.詳細については、「HDD から SSD へのシステムの移行」を参照してください。
- **システムを新しいディスクに移行するための最適な方法は何ですか？クローン作成またはバックアップとリカバリのどちらですか？** - バックアップと復元による方法の方が柔軟性があります。クローン作成を使用する場合でも、古いハードディスクのバックアップを作成することを強くお勧めします。それによって、クローン作成中に元のハードディスクに問題が発生した場合でも、データは安全に守られます。たとえば、ユーザーが間違ったディスクをターゲットとして選択し、そのためにシステムディスクが消去されることがあります。また、複数のバックアップを作成することで冗長性を持たせたりセキュリティを強化したりすることができます。
- **パーティションまたはディスク全体のどちらをバックアップすればよいですか？** - ほとんどの場合、ディスク全体をバックアップする方がまさっています。ただし、場合によってはパーティションのバックアップが推奨されることもあります。たとえば、1 つのハードディスクに、システム（ドライブ文字 C）とデータ（ドライブ文字 D）という 2 つのパーティションがあるとします。システムパーティションの**マイドキュメント**フォルダとサブフォルダには仕事用のドキュメントが保存されています。データパーティションにはビデオ、画像、音楽のファイルが保存されています。システムパーティションのみをバックアップする場合は、ディスク全体をバックアップする必要はありません。この場合、パーティションバックアップで十分です。さらに、（システムファイルではなく）データのみをバックアップする場合は、ファイルバックアップを作成できます。ただし、バックアップストレージに十分な領域がある場合は、ディスク全体のバックアップを少なくとも 1 つ作成することをお勧めします。
- **Acronis Cyber Protect Home Office は RAID をサポートしますか？** - Acronis Cyber Protect Home Office は、一般的なハードウェア RAID アレイをすべてサポートします。ダイナミックディスクでのソフトウェア RAID 構成もサポートされています。Acronis ブータブルメディア は、一般的なハードウェア RAID コントローラーのほとんどをサポートしています。標準的な Acronis ブータブルメディ

ア で RAID が 1 つのボリュームとして認識されない場合、メディアに適切なドライバがありません。その場合は WinPE ベースのメディアを作成して、必要なドライバをそこに追加することができます（詳細モードで）。

データのバックアップ

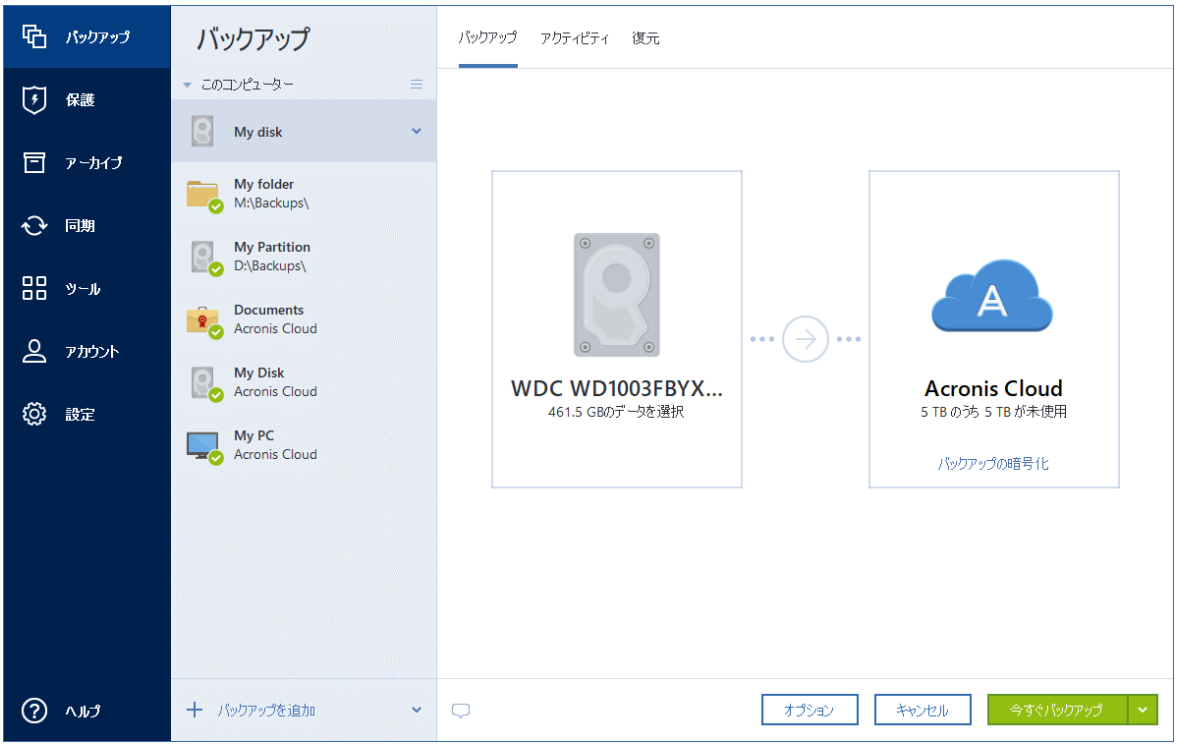
ディスクとパーティションのバックアップ

ファイルのバックアップとは対照的に、ディスクやパーティションのバックアップには、ディスクやパーティションに保存されているすべてのデータが含まれます。この種類のバックアップは通常、システムディスク全体のシステムパーティションの正確なコピーを作成するために使用されます。このバックアップを行うと、Windowsが正しく動作しなかったり起動しない場合にコンピュータを復元することが可能になります。

パーティションまたはディスクをバックアップするには、次の手順を実行します。

1. Acronis Cyber Protect Home Office を開始します。
2. サイドバーで **[バックアップ]** をクリックします。
3. **[バックアップの追加]** をクリックします。
4. （オプション）バックアップの名前を変更するには、バックアップ名の横にある矢印をクリックし、**[名前の変更]** をクリックして、新しい名前を入力します。
5. **[バックアップ対象]** 領域をクリックし、**[ディスクとパーティション]** を選択します。
6. 表示されたウィンドウで、バックアップするディスクやパーティションの横にあるチェックボックスをオンにし、**[OK]** をクリックします。
   非表示のパーティションを表示するには、**[パーティションの完全な一覧]** をクリックします。

注意
ダイナミック ディスクをバックアップするには、パーティション モードのみを使用できます。



7. [**バックアップの保存先**] 領域をクリックし、バックアップの保存先を選択します。
   - **Acronis Cloud** - マイアカウントにサインインし、[**OK**] をクリックします。
   - **外付けドライブ**: 外付けドライブがコンピュータに接続されている場合は、リストからそのドライブを選択できます。
   - **NAS**: 検出されたNASデバイスのリストからNASを選択します。NAS が 1 つしかない場合、Acronis Cyber Protect Home Office はデフォルトでその NAS をバックアップの保存先として使用するように提案します。
   - **参照**: フォルダ ツリーから保存先を選択します。

   注意
   システム パーティションのバックアップをダイナミック ディスクに保存することは避けるようにしてください。システム パーティションは Linux 環境でリカバリされるからです。Linux と Windows では、ダイナミック ディスクの動作が異なります。その結果、リカバリ中に問題が発生する可能性があります。

8. （オプションの手順）バックアップのオプションを設定するには、[**オプション**] をクリックします。詳細については、「バックアップオプション」を参照してください。
9. （オプションの手順）[**コメントを追加**] アイコンをクリックして、バックアップバージョンにコメントを入力します。バックアップのコメントは、データをリカバリするときなど、あとで必要なバージョンを検索するときに役立ちます。
10. 次のいずれかを実行します。
    - バックアップを直ちに実行するには、[**今すぐバックアップ**] をクリックします。
    - 後でバックアップを実行する、またはスケジュールに基づいてバックアップを実行するには、[**今すぐバックアップ**] ボタンの右側にある矢印をクリックし、[**後で実行**] をクリックします。

注意
Acronis Cloud にデータをバックアップする場合は、最初のバックアップが完了するまでにかなり時間がかかることがあります。以降のバックアップ処理は、ファイルに対する変更のみがインターネットを使って転送されるので、大幅に速くなります。

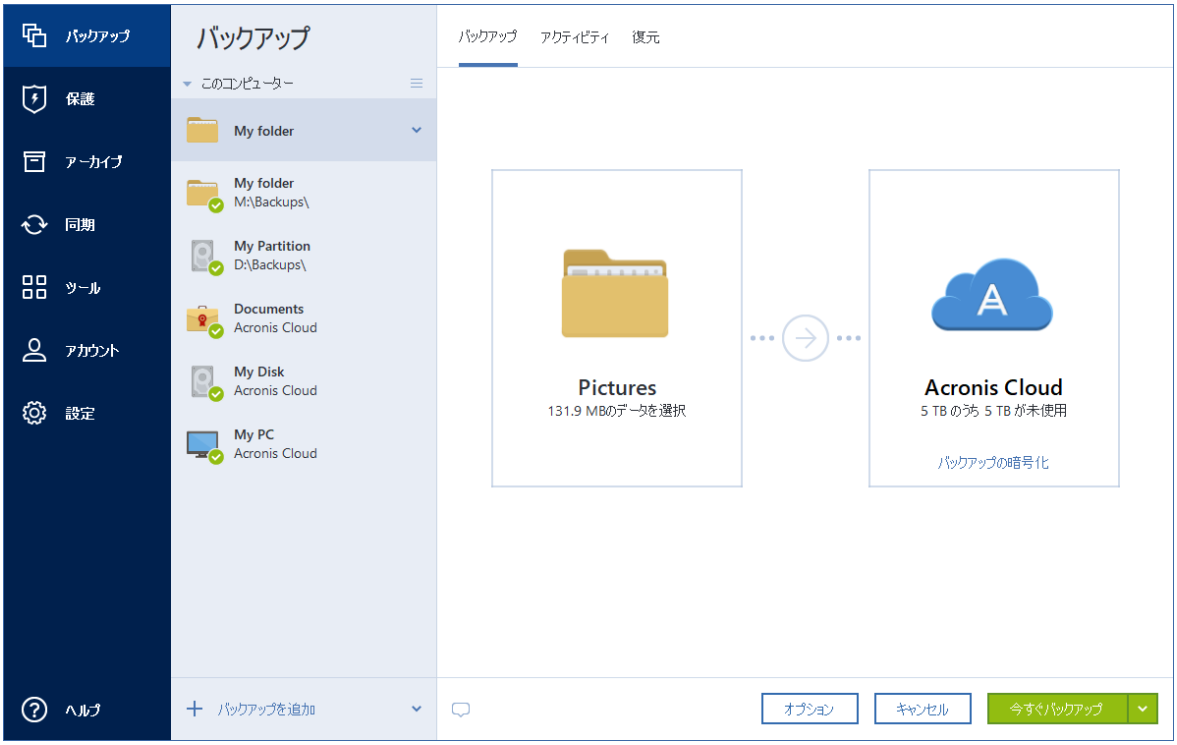
注意
オンラインバックアップの開始後、Acronis Cyber Protect Home Office を閉じることができます。バックアッププロセスはバックグラウンドモードで続行されます。バックアップを一時停止した場合、コンピュータの電源をオフにした場合、またはインターネット接続を切断した場合は、[今すぐバックアップ] をクリックするか、インターネット接続を復元するとバックアップが再開されます。バックアップを中断しても、データが2回アップロードされることはありません。

ファイルやフォルダのバックアップ

ドキュメント、写真、音楽のファイル、ビデオのファイルなどのファイルを保護するために、ファイルを含むパーティション全体をバックアップする必要はありません。特定のファイルやフォルダをバックアップできます。

ファイルやフォルダをバックアップする手順は、次のとおりです。

1. Acronis Cyber Protect Home Office を開始します。
2. サイドバーで **[バックアップ]** をクリックします。
3. **[バックアップの追加]** をクリックします。
4. （オプション）バックアップの名前を変更するには、バックアップ名の横にある矢印をクリックし、**[名前の変更]** をクリックして、新しい名前を入力します。
5. **[バックアップ対象]** 領域をクリックし、**[ファイルとフォルダ]** を選択します。
6. 表示されたウィンドウで、バックアップするファイルやフォルダの横にあるチェック ボックスをオンにし、**[OK]** をクリックします。



7. **[バックアップの保存先]** 領域をクリックし、バックアップの保存先を選択します。
   - **Acronis Cloud** - マイアカウントにサインインし、**[OK]** をクリックします。
     Acronis アカウントをお持ちでない場合は、**[アカウントの作成]** をクリックして E メールアドレスとパスワードを入力し、**[アカウントの作成]** ボタンをクリックします。詳細については、「Acronis アカウント」を参照してください。
   - **外付けドライブ**: 外付けドライブがコンピュータに接続されている場合は、リストからそのドライブを選択できます。
   - **NAS**: 検出されたNASデバイスのリストからNASを選択します。NAS が 1 つしかない場合、Acronis Cyber Protect Home Office はデフォルトでその NAS をバックアップの保存先として使用するように提案します。
   - **参照**: フォルダ ツリーから保存先を選択します。
8. （オプションの手順）バックアップのオプションを設定するには、**[オプション]** をクリックします。詳細については、「バックアップオプション」を参照してください。
9. （オプションの手順）**[コメントを追加]** アイコンをクリックして、バックアップバージョンにコメントを入力します。バックアップのコメントは、データをリカバリするときなど、あとで必要なバージョンを検索するときに役立ちます。

10. 次のいずれかを実行します。
    - バックアップを直ちに実行するには、**[今すぐバックアップ]** をクリックします。
    - 後でバックアップを実行する、またはスケジュールに基づいてバックアップを実行するには、**[今すぐバックアップ]** ボタンの右側にある下向きの矢印をクリックし、**[後で実行]** をクリックします。

注意
Acronis Cloud にデータをバックアップする場合は、最初のバックアップが完了するまでにかなり時間がかかることがあります。以降のバックアップ処理は、ファイルに対する変更のみがインターネットを使って転送されるので、大幅に速くなります。

さらに、https://goo.gl/i4J1AN のビデオ解説（英語）をご覧ください。

モバイルデバイスのバックアップ

iOS または Android のスマートフォンがあれば、Acronis Cyber Protect Home Office を使用して、写真、ビデオファイル、連絡先、カレンダーなどのモバイルデータを保護できます。 詳細については、「Acronis Mobile」を参照してください。

バックアップを開始する前に、バックアップの保存先として Acronis Cloud またはコンピューター上のローカルストレージを選択します。保存先を後から変更することはできますが、両方の保存先に同時にバックアップすることはできません。データを Acronis Cloud にバックアップするには、Acronis Mobile アプリを使用します。詳細については、「Acronis Cloud へのモバイルデバイスのバックアップ」を参照してください。

コンピュータ上のローカルストレージにモバイルデータをバックアップするには、次のようにします。

1. 次を確認してください。
    - Acronis True Image (2017 以降)、または Acronis Cyber Protect Home Office がコンピューターにインストールされている。
    - モバイルデバイスに Acronis Mobile アプリがインストールされている。
    - モバイルデバイスとコンピュータが同一のWi-Fiネットワークに接続している。
2. コンピュータで次の手順を実行します。
    a. Acronis True Image (2017 以降) または Acronis Cyber Protect Home Office を起動します。
    b. サイドバーの **[バックアップ]** をクリックして、**[バックアップの追加]** をクリックします。
    c. **[バックアップ対象]** 領域をクリックし、**[モバイルデバイス]** を選択します。
    QR コードが表示されます。このウィンドウは閉じないでください。
3. モバイルデバイスで次の手順を実行します。
    a. Acronis Mobile を開始します。
    b. プラスアイコンをタップして、バックアップを作成します。モバイルデバイスを初めてバックアップする場合は、このステップが発生しないことに注意してください。
    c. バックアップ先としてコンピュータを選択します。
    d. **[QRコードのスキャン]** をタップし、コンピュータ画面上のQRコードにカメラを向けて、モバイルデバイスがコンピュータに接続されるまで待ちます。

e. バックアップするデータカテゴリを選択するか、すべてをバックアップする場合は **[確認]** をタップします。
f. Acronis Mobile に個人データへのアクセスを許可します。
g. （オプションの手順）バックアップを暗号化して保護するためのパスワードを入力します。暗号化しない場合は、**[Skip Encryption（暗号化をスキップ）]** をタップします。
h. **[バックアップを開始]** をタップします。

バックアップ開始後は、コンピュータやモバイルデバイスのどのアプリケーションでも進行状況を確認できますが、エラーおよび警告メッセージが表示されるのはモバイルアプリのみです。

コンピュータの Acronis Cyber Protect Home Office と Acronis Mobile アプリは両方とも閉じてかまいません。バックアップはバックグラウンドモードで継続されます。

データの変更（たとえば、新しい写真など）を自動的にバックアップする場合は、**[自動バックアップ]** 設定がオンになっていることを確認します。この設定がオフの場合、新しいデータは **[バックアップ]** をタップするまでバックアップされません。詳細については、「モバイルアプリの設定」を参照してください。

モバイルバックアップの保存先をローカルストレージから Acronis Cloud に変更すると、モバイルデバイスとコンピューター間の接続が失われ、Acronis Cyber Protect Home Office はリスト内のモバイルバックアップをモバイルデバイスに関連付けなくなります。この場合、保存先をローカルストレージに戻すには、この接続を復元する必要があります。接続は、エラーによって失われる場合もあります。接続を復元するには、Acronis Cyber Protect Home Office のバックアップリストでモバイルバックアップを選択してから、**[再接続]** をクリックし、モバイルデバイスで QR コードをスキャンします。その後は、同じ設定でバックアップが通常通りに続行されます。

Acronis Mobile

注意
お住まいの地域では、Acronis Cloud をご利用いただけません。詳細は、https://kb.acronis.com/content/4541 を参照してください。

Acronis Mobile を使用すれば、データを Acronis Cloud か、コンピュータ上のローカルストレージにバックアップして、データが損失または破損した場合に復元できます。クラウドストレージへのバックアップには Acronis アカウントと Acronis Cloud のサブスクリプションが必要になります。

Acronis Mobile の主な機能とサポートされているデバイスについての詳細は、Acronis Mobile 関連の文書を参照してください。

これらのアプリはどこにありますか？

Apple App Store または Google Play で、Acronis Mobile の詳細情報を確認してダウンロードすることができます。

- iOS デバイス向け Acronis Mobile: https://go.acronis.com/atimobile/download/iOS
- Android デバイス向け Acronis Mobile: https://go.acronis.com/atimobile/download/Android

モバイルバックアップのローカルのバックアップ先

モバイルデータをコンピューターにバックアップする場合、Acronis Mobile によってバックアップがデフォルトのフォルダ（C:¥ProgramData¥Acronis Mobile Backup Data¥acronis-local-data¥）に保存されます。デフォルトフォルダを変更する場合、acronis-local-data フォルダは選択した場所に移動されます。すべての新しいモバイルデータは新しい場所にバックアップされます。

注意
すべてのモバイルバックアップは常に同一フォルダに保存され、分割保存されることはありません。

モバイルバックアップのローカルの保存先を変更する手順は、次のとおりです。

1. サイドバーで **[設定]** をクリックし、**[モバイルバックアップの場所]** オプションを探します。
2. **[モバイルバックアップの場所]** セクションで、**[変更]** をクリックします。**[ロケーションの変更]** ウィンドウが表示されます。
3. 次に**[場所の選択]** をクリックしてバックアップの新しい保存先を選択します。注意: 選択できるのは内蔵ハードドライブの場所のみです。

新しい場所を最初の場所に変更するには、**[デフォルトにリセット]** をクリックします。

Office 365 データのバックアップ

Office 365 データをバックアップする理由

Microsoft Office 365 for Home はクラウドサービスのセットですが、それでも定期的なバックアップをすればユーザーエラーや意図的な悪意のある操作から保護する追加のレイヤが得られます。Acronis Cyber Protect Home Office を使用すれば、安全な Acronis Cloud にバックアップすることにより、Microsoft Outlook メールボックスと Microsoft OneDrive データを保護することができます。Acronis Cloud にアップロードした後、すべてのコンテンツをいつでもどのデバイスからでも使用できるようになります。Office 365 の保持期間が過ぎた後でも、削除したアイテムをバックアップからリカバリすることができます。

Office 365 データのバックアップ

Outlook メールボックスでバックアップ可能なデータ:

- すべてのフォルダ
- 電子メールメッセージ
- 添付ファイル

注意
共有メールボックスやグループメールボックスはバックアップできません。

OneDrive でバックアップ可能なデータ:

- すべてのファイルとフォルダ

Office 365 データをバックアップするには:

1. 次のいずれかを実行してオンラインダッシュボードを開きます。
   - https://cloud.acronis.comのリンクをクリックします。
   - Acronis Cyber Protect Home Office のサイドバーで、[**バックアップ**]、[**バックアップの追加**]、[**バックアップ対象**] 領域の順にクリックしてから、[**Cloud サービス**] を選択します。
2. Acronis アカウントにサインインします。
3. サイドバーで、[**リソース**]、[**追加**] の順にクリックしてから、[**Microsoft Office 365 for Home**] を選択します。
4. メッセージが表示されたら、Microsoft アカウントにログインします。
5. [**バックアップ対象**] 領域で、バックアップするアイテムを選択します。
   - アカウント全体
   - Outlook
   - OneDrive
6. [**完了**] をクリックします。
7. [**クリーンアップ**] ペインを介して、バックアップ用のクリーンアップルールを設定できます。バックアップを暗号化してパスワードで保護することもできます。終了したら、[**適用**] をクリックします。
8. バックアップを開始するには、[**今すぐ実行**] をクリックします。

バックアップ オプション

バックアップを作成するときに、追加オプションを変更して、バックアップ処理を微調整することができます。オプションのウィンドウを開くには、バックアップのソースまたはターゲットを選択してから [**オプション**] をクリックします。

バックアップの種類（ディスクレベル バックアップ、ファイルレベル バックアップ、オンライン バックアップ、ノンストップ バックアップ）によりオプションは完全に独立しているため、オプションを個別に設定する必要があります。

アプリケーションをインストールすると、すべてのオプションは初期値に設定されます。これらのオプションは、現在のバックアップ処理のためだけに変更することも、今後のすべてのバックアップ向けに変更することも可能です。[**デフォルトとして保存する**] チェックボックスをオンにすると、変更した設定が今後のバックアップ作業すべてにデフォルトで適用されます。

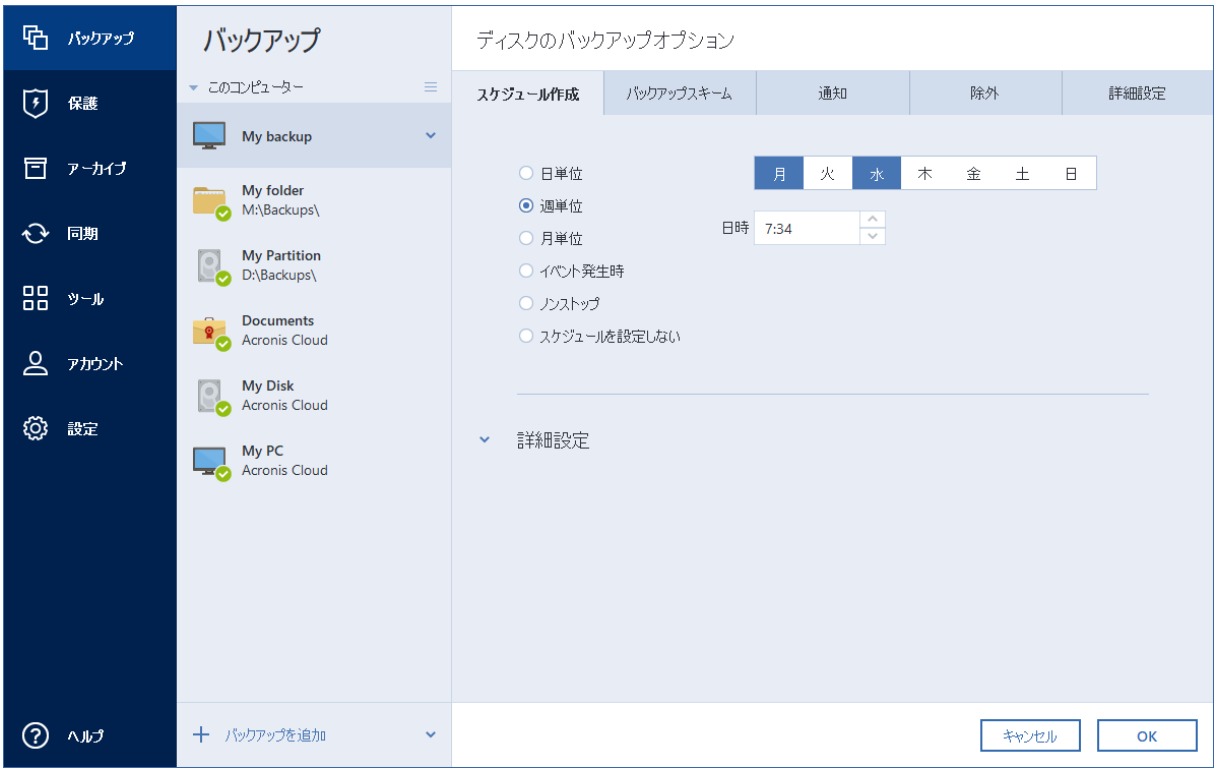
製品の初回インストール後に変更したオプションをすべてリセットする場合は、[**初期設定にリセット**] ボタンをクリックします。これにより現在のバックアップの設定のみがリセットされることに注意してください。今後のすべてのバックアップでの設定をリセットするには、[**初期設定にリセット**] をクリックし、[**設定をデフォルトとして保存する**] のチェックボックスをオンにしてから、[**OK**] をクリックします。

さらに、https://goo.gl/bKZyaG のビデオ解説（英語）をご覧ください。

スケジュール設定

場所: [**オプション**] > [**スケジュール**]

[**スケジュール**] タブを使用すると、バックアップを指定し、スケジュール設定をベリファイできます。



バックアップの定期的な作成またはベリファイのスケジュールを指定することができます。

- [日単位]: 処理は 1 日 1 回以上実行されます。
- [週単位]: 処理は 1 週間に 1 回、または 1 週間に複数回、指定した曜日に実行されます。
- [月単位]: 処理は 1 か月に 1 回、または 1 か月に複数回、指定した日に実行されます。
- [イベント発生時]: 処理はイベントの発生時に実行されます。
- [ノンストップ]: 処理は 5 分おきに実行されます。
- [**スケジュールを設定しない**]: 現在の処理に対してスケジューラがオフになります。この場合、バックアップやベリファイはそれぞれ、メイン ウィンドウで [**今すぐバックアップ**] または [**ベリファイ**] をクリックした場合にのみ実行されます。

詳細設定

[**詳細設定**] をクリックすると、バックアップおよびベリファイの次の追加設定を指定できます。

- [**コンピュータがロックされたか、スクリーンセーバーが実行中にのみバックアップする**]: スケジュールされた処理の実行を、コンピューターが使用中でない状態（スクリーンセーバーが表示される、またはコンピューターがロックされている状態）になるまで延期する場合には、このチェックボックスをオンにします。ベリファイのスケジュールの場合、チェックボックスが [**コンピュータのアイドル時にのみベリファイを実行する**] に変化します。
- [**スリープ/休止状態のコンピュータを起動**]: スリープ/休止状態のコンピューターを起動して、スケジュールされた処理を実行する場合には、このチェックボックスをオンにします。
- [**コンピュータをスリープ/休止状態にしない**]: 長時間のバックアップで、コンピューターがスリープモードや休止モードに入ったためにバックアップが中断しないようにするには、このチェックボックスをオンにします。

- **[実行されなかった処理をシステム起動後の指定時間に実行（分単位）]**: スケジュールされた時刻にコンピューターの電源がオフになっていて処理が実行されなかった場合に、次のシステム起動時に未実行の処理を実行させる場合には、このチェックボックスをオンにします。

  さらに、システムを起動して一定時間後にバックアップを開始するために、時間遅延を設定できます。たとえば、システム起動の 20 分後にバックアップを開始するには、該当するボックスに「20」と入力します。
- **[外部デバイスが接続された場合に未実行の処理を実行する]**（USB フラッシュドライブへのバックアップまたは USB フラッシュドライブにあるバックアップのベリファイをスケジュール設定している場合のオプション）: スケジュールされた時刻に USB フラッシュドライブが接続されていなかった場合に、USB フラッシュドライブの接続時に未実行の処理を実行する場合には、このチェックボックスをオンにします。

日単位のバックアップのパラメータ

日単位のバックアップの作成または検証では、次のパラメータを設定することができます。

- **[毎]** - ドロップダウンリストから日ごとの処理の間隔を選択します（例: 2 時間ごと）。
- **[1 日に一度]** - 1 日に 1 回、指定した時刻に処理が実行されます。
- **[一日二回]** - 1 日に 2 回処理が実行されます。それぞれの処理について時刻を選択します。

[詳細設定] の説明については、「スケジュール設定」を参照してください。

週単位のバックアップのパラメータ

週単位のバックアップの作成または検証では、次のパラメータを設定することができます。

- **[曜日]** - 処理を実行する曜日を選択します。
- **[時刻]** - 処理の開始時刻を選択します。

[詳細設定] の説明については、「スケジュール設定」を参照してください。

月単位のバックアップのパラメータ

月単位のバックアップの作成または検証では、次のパラメータを設定することができます。

- **[毎]** - ドロップダウンリストから週の番号と曜日を選択します。たとえば、**[毎月第 1 月曜日]** を選択すると、処理は毎月第 1 月曜日に実行されます。
- **[月の指定日]** - バックアップの日付を選択します。たとえば、月の 10 日と最終日に処理を実行できます。
- **[時刻]** - 処理の開始時刻を選択します。

[詳細設定] の説明については、「スケジュール設定」を参照してください。

イベント発生時の実行パラメータ

イベント発生時のバックアップの作成または検証では、次のパラメータを設定することができます。

- **[1 日 1 回のみ]**: 当日そのイベントが最初に発生したときのみ処理を実行する場合は、このチェックボックスをオンにします。

- イベントにより実行するバックアップの作成または検証を指定します。
  - **[外部デバイスが接続されている場合]**: 以前にバックアップの宛先として使用したのと同じデバイス（USB フラッシュドライブまたは外部 HDD）がコンピューターに接続されるたびに処理が開始されます。Windowsは外部デバイスとして認識することに注意してください。
  - **[ユーザー ログオン]**: 現在のユーザーがオペレーティングシステムにログオンするたびに処理が開始されます。
  - **[ユーザー ログオフ]**: 現在のユーザーがオペレーティングシステムからログオフするたびに処理が開始されます。
  - **[システム シャットダウンまたは再起動]**: コンピューターのシャットダウン時または再起動時に毎回処理が開始されます。
  - **[システム起動時に遅延（分単位）]**: オペレーティングシステムが起動するたびに、指定した遅延後に処理が開始されます。

[詳細設定] の説明については、「スケジュール設定」を参照してください。

バックアップ スキーム

場所: **[オプション]** > **[バックアップスキーム]**

バックアップスキームとスケジューラを使用して、バックアップ ストラテジーを設定できます。このスキームを使用することで、バックアップ ストレージ領域の使用を最適化し、データ ストレージの信頼性を向上させ、使用しなくなったバックアック バージョンを自動的に削除することができます。

注意
オンラインバックアップの場合、バックアップスキームはデフォルトで設定されており、変更できません。最初は完全バックアップが作成され、その後は増分バックアップが作成されます。

バックアップスキームでは、以下のパラメータを定義します。

- バックアップバージョン作成の際に使用するバックアップ方法（完全、差分、増分）
- 別の方法で作成したバックアップ バージョンのシーケンス
- バージョンのクリーンアップ ルール

Acronis Cyber Protect Home Office で選択可能なバックアップスキームは次のとおりです。

- **単一バージョンスキーム** - 最小限のバックアップストレージを使用する場合にこのスキームを選択します。
- **バージョンチェーンスキーム** - 多くの場合に最適なスキームです。
- **増分スキーム** - 5 つの増分バージョンが作成されるごとに完全バージョンを作成する場合に選択します。これはデフォルトのスキームです。
- **差分スキーム** - 最初の完全バックアップの後で差分バックアップのみを作成する場合に選択します。
- **カスタムスキーム** - バックアップスキームを手動で設定する場合に選択します。

既存のバックアップのバックアップスキームは簡単に変更できます。バックアップスキームを変更してもバックアップチェーンの整合性には影響しないため、以前の任意のバックアップバージョンからデータをリカバリすることができます。

注意
DVD/BD などの光学メディアにバックアップするときは、バックアップスキームを変更できません。この場合、Acronis Cyber Protect Home Office はデフォルトで完全バックアップのみのカスタムスキームを使用します。これは、プログラムが光学メディアに保存されたバックアップを統合できないためです。

単一バージョン スキーム

このバックアップスキームは、ディスクバックアップとファイルバックアップで同一です（スケジューラ設定は除く）。

このスキームでは完全なバックアップバージョンが作成されます。このバージョンは、指定したスケジュール時間や手動バックアップの実行時に上書きされます。この処理では、新しいバージョンが作成された後に古いバージョンが削除されます。

注意
一番最初のファイルは補助的な用途のために継続的に使用され、これには実際のデータが保存されません。これを削除しないでください。

ディスクバックアップのバックアップスケジュール設定: 月単位。

ファイルバックアップのバックアップスケジュール設定: 日単位。

結果: 単一で最新の完全バックアップ バージョンが作成されます。

必要なストレージ領域: 最小

バージョンチェーンスキーム

このバックアップスキームは、ディスクバックアップとファイルバックアップで異なります。

ディスクバックアップのバージョンチェーン

最初に完全バックアップバージョンが作成されます。このバージョンは、手動で削除されるまで保存されます。これ以降、指定のスケジュールに従って（または手動バックアップの実行時に）、1 つの完全バックアップバージョンと、5 つの差分バックアップバージョンが作成されます。続いて、同じく 1 つの完全バックアップバージョンと、5 つの差分バックアップバージョンが再作成され、これが繰り返されます。作成したバージョンは 6 ヵ月間保存されます。この期間が経過すると、（最初の完全バージョン以外の）最も古いバックアップバージョンを削除してもよいかどうかが分析されます。この結果は、バージョンの最小限の数（8）およびバージョンチェーンの一貫性によって変わります。同じバックアップ方法で新しいバージョンが作成されると、最も古いバージョンが 1 つずつ削除されます（たとえば最も古い差分バージョンは、最新の差分バージョンの作成後に削除されます）。まず最も古い差分バージョンが削除され、次に最も古い完全バージョンが削除されます。

バックアップスケジュール設定: 月単位。

結果: 直近の 6ヵ月間のバックアップバージョンが月単位で保持されます（最初の完全バックアップバージョンを含む。このバージョンは、さらに長期間保管可能）。

必要なストレージ領域: バージョンの数とサイズによって異なります。

ファイルバックアップのバージョンチェーン

指定のスケジュールに従って（または手動バックアップの実行時に）、1 つの完全バックアップバージョンと、6 つの増分バックアップバージョンが作成されます。続いて、同じく 1 つの完全バックアップバージョンと、6 つの増分バックアップバージョンが再作成され、これが繰り返されます。作成したバージョンは 1ヵ月間保存されます。この期間が経過すると、最も古いバックアップバージョンを削除してよいかどうかが分析されます。この結果は、バージョンチェーンの一貫性によって変わります。一貫性を維持するために、新しい類似のバージョンチェーンの作成後に、最も古い 1 つの完全バックアップバージョンと 6 つの増分バックアップバージョンが、チェーンごとに削除されます。

バックアップスケジュール設定: 日単位。

結果: 直近の 1ヵ月間の、毎日のバックアップバージョンが保持されます。

必要なストレージ領域: バージョンの数とサイズによって異なります。

カスタム スキーム

Acronis Cyber Protect Home Office を使用して、独自のバックアップスキームを作成することもできます。事前定義されたバックアップ スキームに基づいてスキームを作成することもできます。事前定義されたスキームを選択して自身の要件に合わせて変更し、その変更後のスキームを新しいものとして保存します。

注意
既存の事前定義されたバックアップ スキームは、上書きできません。

また、完全バックアップ、差分バックアップ、または増分バックアップのバージョンを参考にして、カスタム スキームをゼロから作成することもできます。

したがって、まず該当のボックスでバックアップ方法を 1 つ選択してください。

- 完全
  完全バックアップ バージョンのみを作成する場合は、この方法を選択します。
- 増分
  完全バックアップ バージョンと増分バックアップ バージョンのみを含むバックアップ チェーンを作成する場合は、この方法を選択します。
  以下のオプションのうちの 1 つを使用してスキームを設定できます。
  - **[最初の完全バージョン後は、増分バージョンだけ作成する]** - バックアップバージョンチェーンを 1 つだけ作成する場合は、このオプションを選択します。このオプションでは自動クリーンアップを使用できません。
  - **[次のバージョンごとに完全バージョンを作成する:[n] 増分バージョン]** - 複数のバックアップバージョンチェーンを作成する場合は、このオプションを選択します。このバックアップスキームは信頼性の高いものですが、使用領域が多くなります。
- 差分
  完全バックアップ バージョンと差分バックアップ バージョンのみを含むバックアップ チェーンを作成する場合は、この方法を選択します。
  以下のオプションのうちの 1 つを使用してスキームを設定できます。
  - **[最初の完全バージョン後は、差分バージョンだけ作成する]** - バックアップバージョンチェーンを 1 つだけ作成する場合は、このオプションを選択します。このオプションでは自動クリーンアップを使用できません。
  - **[次のバージョンごとに完全バージョンを作成する:[n] 差分バージョン]** - 複数のバックアップバージョンチェーンを作成する場合は、このオプションを選択します。このバックアップスキームは信頼性の高いものですが、使用領域が多くなります。

自動クリーンアップをオンにする

- **[古いバージョンのクリーンアップルール]** - 使用しなくなったバックアップバージョンを自動的に削除するには、以下のクリーンアップルールのうちの 1 つを設定します。

- **[次の期間が経過したバージョンを削除する [定義した期間]]**（完全バックアップの場合のみ使用可能） - バックアップバージョンの保存期間を限定する場合は、このオプションを選択します。指定した期間を超過したバージョンは、すべて自動的に削除されます。
- **[次の期間が経過したバージョン チェーンを削除する [定義した期間]]**（増分バックアップと差分バックアップでのみ使用可能） - バックアップバージョンチェーンの保存期間を限定する場合は、このオプションを選択します。最も古いバージョンチェーンは、指定した期間をそのチェーンの最新のバックアップバージョンが超過した場合にのみ削除されます。
- **[最大 [n] つの最新バージョンを保存する]**（完全バックアップの場合のみ使用可能） - バックアップバージョンの最大数を制限する場合は、このオプションを選択します。バージョン数が指定値を超えると、最も古いバックアップ バージョンが自動的に削除されます。
- **[最大 [n] つの最新のバージョンチェーンを保存する]**（増分バックアップと差分バックアップでのみ使用可能） - バックアップバージョンチェーンの最大数を制限する場合は、このオプションを選択します。バージョン チェーン数が指定値を超えると、最も古いバックアップバージョンチェーンが自動的に削除されます。
- **[バックアップを次のサイズ以下に保つ [定義したサイズ]]**（ローカルバックアップには使用不可） - バックアップの最大サイズを制限する場合は、このオプションを選択します。新しいバックアップ バージョンが作成された後に、バックアップの合計サイズが、指定した値を超えているかどうかが確認されます。指定した値を超えている場合は、古いバックアップ バージョンが削除されます。

- **[バックアップの最初のバージョンは削除しない]** - 初期のデータ状態を維持する場合は、このチェックボックスをオンにします。最初の完全バックアップ バージョンが 2 つ作成されます。最初のバージョンは自動クリーンアップから除外され、手動で削除するまで保存されます。 増分または差分バックアップを選択した場合、最初のバックアップ チェーンは 2 番目の完全バックアップ バージョンから開始されます。3 番目のバックアップ バージョンのみが増分または差分バックアップになります。完全メソッドでこのチェックボックスをオンにすると、**[最大 [n] つの最新バージョンを保存する]** チェックボックスが、**[1+[n] つの最新バージョンを保存する]** に変わります。

カスタムバックアップスキームの管理

既存のバックアップスキームに何らかの変更を加えた場合、変更したスキームを新しいものとして保存できます。その場合、そのバックアップスキームに新しい名前を指定する必要があります。

- 既存のカスタムスキームを上書きすることもできます。
- 既存の事前定義されたバックアップ スキームは、上書きできません。
- スキーム名には、そのOSでファイル名に使用できるすべての文字（記号）を使用できます。バックアップスキーム名の最大長は、255文字です。
- カスタムバックアップスキームは、最高16個まで作成できます。

カスタムバックアップスキームを作成した後は、バックアップを設定するときに他の既存のバックアップスキームと同様に使用できます。

また、カスタムバックアップスキームを保存しないで使用することもできます。その場合は、作成したときのバックアップでのみ使用され、他のバックアップには使用できません。

カスタムバックアップスキームが必要なくなった場合は、削除できます。バックアップスキームを削除するには、バックアップスキームのリストで削除するスキームを選択し、**[削除]** をクリックして、**[スキームを削除]** ウィンドウで確認します。

注意
事前定義されたバックアップスキームは、削除できません。

カスタム スキームの例

1. PC全体のバックアップ「2つの完全バックアップ」

事例: コンピューター上のすべてのデータを 2 つの完全バックアップを使用して保護し、月に 1 度バックアップをアップデートするようにします。カスタムバックアップスキームを使用して実行する方法について説明します。

1. PC全体のバックアップの設定を開始します。 詳細については、「PCのすべてのデータのバックアップ」を参照してください。
2. バックアップ対象として [コンピュータ全体] が選択されていることを確認します。
3. **[オプション]** をクリックして **[スケジュール]** タブを開き、**[月単位]** をクリックして、日付（たとえば、20日）を指定します。これで、毎月の指定した日付にバックアップバージョンが作成されるようになります。次に、バックアップ処理の開始時刻を指定します。
4. **[バックアップスキーム]** タブを開き、**[増分スキーム]** の代わりに **[カスタムスキーム]** を選択します。
5. **[バックアップの方法]** ボックスで、ドロップダウンリストから **[完全]** を選択します。
6. バージョン数を制限するには、**[最大 [n] つの最新バージョンを保存する]** をクリックして、**2** と入力または選択し、**[OK]** をクリックします。
   この場合、プログラムは新しい完全バックアップを毎月20日に作成します。3つ目のバージョンを作成した後は、最も古いバージョンは自動的に削除されます。
7. すべての設定が正しいことを確認して、**[今すぐバックアップ]** をクリックします。初回バックアップをスケジューラで指定した時刻にのみ実行するようにするには、**[今すぐバックアップ]** ボタンの右側にある下向き矢印をクリックして、ドロップダウンリストで **[後で実行]** を選択します。

2. ファイル バックアップ: 日単位の増分バックアップと週単位の完全バックアップ

ケース: 毎日作業するファイルやフォルダがあります。毎日の作業をバックアップする必要があり、データの状態を過去 3 週間の任意の日に復元できるようにすることを計画します。カスタム バックアップスキームを使用して、これを実行する方法について説明します。

1. ファイル バックアップの設定を開始します。詳細については、「ファイルやフォルダのバックアップ」を参照してください。
2. **[オプション]** をクリックして **[スケジュール]** タブを開き、**[日単位]** をクリックして、バックアップ処理の開始時刻を指定します。たとえば、毎日の作業を午後 8 時に終了する場合、その時刻または少し後（午後 8 時 5 分）を開始時刻に指定します。
3. **[バックアップスキーム]** タブを開き、**[増分スキーム]** の代わりに **[カスタムスキーム]** を選択します。

4. **[バックアップの方法]** ボックスで、ドロップダウンリストから **[増分]** を選択します。
5. **[次のバージョンごとに完全バージョンを作成する: [n] 増分バージョン]** をクリックして、**6** を入力するか、または選択します。

   この場合、プログラムは最初に初回の完全バックアップバージョンを作成し（バックアップ処理の設定方法にかかわらず、初回バックアップバージョンは完全バックアップになります）、6つの増分バックアップを日ごとに作成します。その後、1つの完全バックアップと6つの増分バックアップを再度作成します。このように新しい完全バージョンはすべてちょうど 1 週間の期間で作成されます。
6. バージョンの保存期間を制限するには、**[自動クリーンアップをオンにします]** をクリックします。
7. **[次の期間が経過したバージョン チェーンを削除する [定義した期間]]** をクリックして、**21** を入力するか、または選択して、**[OK]** をクリックします。
8. すべての設定が正しいことを確認して、**[今すぐバックアップ]** をクリックします。初回バックアップをスケジューラで指定した時刻にのみ実行するようにするには、**[今すぐバックアップ]** ボタンの右側にある下向き矢印をクリックして、ドロップダウンリストで **[後で実行]** を選択します。

3. ディスク バックアップ: 完全バージョン 2 ヵ月ごとと差分バックアップ月 2 回

ケース: システムパーティションを月2回バックアップし、新しい完全バックアップバージョンを2ヵ月ごとに作成する必要があります。また、バックアップバージョンの保存に使用するディスク領域は、100 GB 以下にします。カスタム バックアップ スキームを使用して、これを実行する方法について説明します。

1. ディスク バックアップの設定を開始します。「ディスクとパーティションのバックアップ」を参照してください。
2. システムパーティション（通常はC:）をバックアップ対象して選択します。
3. **[オプション]** をクリックして **[スケジュール]** タブを開き、**[月単位]** をクリックして、たとえば、毎月1日と15日を指定します。これにより、約2週間ごとにバックアップバージョンが作成されます。次に、バックアップ処理の開始時刻を指定します。
4. **[バックアップスキーム]** タブを開き、**[増分スキーム]** の代わりに **[カスタムスキーム]** を選択します。
5. **[バックアップの方法]** ボックスで、ドロップダウンリストから **[差分]** を選択します。
6. **[次のバージョンごとに完全バージョンを作成する: [n] 差分バージョン]** をクリックして、**3** を入力するか、または選択します。

   この場合、プログラムは最初に初回の完全バックアップバージョンを作成し（バックアップ処理の設定方法にかかわらず、初回バックアップバージョンは完全バックアップになります）、3つの差分バージョンを約2週間ごとに作成します。そして再び1つの完全バックアップと3つの差分バックアップを作成します。このように新しい完全バージョンは 2 ヵ月ごとに作成されます。
7. バージョンの保存領域を制限するには、**[自動クリーンアップをオンにします]** をクリックします。
8. **[バックアップのサイズを次のサイズ以下に保つ [定義したサイズ]]** をクリックして、**100 GB** を入力するか、または選択して、**[OK]** をクリックします。

注意
バックアップの合計サイズが 100 GB を超えた場合、Acronis Cyber Protect Home Office は既存のバックアップバージョンをクリーンアップして、残りのバージョンがサイズ制限を満たすようにします。プログラムは、1つの完全バックアップバージョンと3つの差分バックアップバージョンで構成される、最も古いバックアップチェーンを削除します。

9. すべての設定が正しいことを確認して、**[今すぐバックアップ]** をクリックします。初回バックアップをスケジューラで指定した時刻にのみ実行するようにするには、**[今すぐバックアップ]** ボタンの右側にある下向き矢印をクリックして、ドロップダウンリストで **[後で実行]** を選択します。

バックアップ処理の通知

場所: **[オプション]** > **[通知]**

バックアップまたはリカバリの処理には 1 時間以上かかる場合があります。Acronis Cyber Protect Home Office では、この処理の終了時に E メールで通知を受け取ることができます。また、処理中に発行されたメッセージや、処理完了後の完全な処理ログもプログラムによって送信されます。

デフォルトでは、すべての通知設定が無効になっています。

空きディスク領域のしきい値

バックアップストレージの空き領域が指定のしきい値より少なくなったときに、通知を受け取ることができます。バックアップの開始後、選択したバックアップ保存先の空き領域が指定値よりも既に少ないことが Acronis Cyber Protect Home Office によって検出された場合には、プログラムで実際のバックアップ処理は開始されず、空き領域が少ない旨の通知メッセージが直ちに表示されます。メッセージには次の3つの選択肢が示されます。メッセージを無視してバックアップを続行する、バックアップを保存する別の場所を参照する、バックアップをキャンセルする、の中からいずれかを選択します。

バックアップの実行中に空き領域が指定値より少なくなった場合にも、プログラムにより同じメッセージが表示されるため、同様の選択を行う必要があります。

Acronis Cyber Protect Home Office では、次のストレージデバイスの空き領域をチェックすることができます。ローカルハードドライブ、USB カードと USB ドライブ、ネットワーク共有（SMB）。FTP サーバーとCD/DVDドライブでは、このオプションを有効にすることはできません。

ディスクの空き領域のしきい値を設定するには、次の手順を実行します。

1. **[ディスクの空き領域が不十分なときに通知メッセージを表示する]** チェックボックスをオンにします。
2. **[ディスクの空き領域が次のサイズ未満になったときに通知する]** ボックスにしきい値を入力します。

注意
[エラー処理] 設定で **[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）]** チェックボックスがオンになっている場合、メッセージは表示されません。

電子メールによる通知

1. **[処理状態に関する電子メール通知を送信する]** チェックボックスを選択します。
2. 電子メールを設定します。
   - **[宛先]** フィールドに電子メール 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。
   - **[サーバー設定]** フィールドに送信メールサーバー（SMTP）を入力します。
   - 送信メール サーバーのポート番号を設定します。デフォルトでは、ポートは25に設定されます。
   - メールに必要な暗号化を選択します。
   - 必要に応じて、**[SMTP 認証]** チェック ボックスを選択し、対応するフィールドにユーザー名とパスワードを入力します。
3. 設定が正しいかどうかをチェックするには、**[テスト メッセージを送信する]** ボタンをクリックします。

テストメッセージの送信に失敗した場合

1. **[拡張設定を表示]** をクリックします。
2. 追加の電子メール設定を行います。
   - **[差出人]** フィールドに送信者のメールアドレスを入力します。指定するアドレスが不明な場合は、たとえば、aaa@bbb.com のような標準形式で任意のアドレスを入力します。
   - 必要に応じて、**[件名]** フィールドのメッセージの件名を変更します。
     バックアップステータスを簡単にチェックするために、電子メールメッセージの件名に最も重要な情報を追加できます。入力可能なテキストラベルは次のとおりです。
     - %BACKUP_NAME%: バックアップ名
     - %COMPUTER_NAME%: バックアップが開始されたコンピューター名
     - %OPERATION_STATUS%: バックアップまたは他の処理の結果
       たとえば、次のように入力します: バックアップのステータス %BACKUP_NAME%: %OPERATION_STATUS% (%COMPUTER_NAME%)
   - **[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、その下に受信メールサーバー（POP3）を入力します。
   - 受信メール サーバーのポート番号を設定します。デフォルトでは、ポートは110に設定されます。
3. **[テストメッセージを送信する]** ボタンをもう一度クリックします。

その他の通知設定

- **[処理が正常に完了したら通知を送信する]** - 処理の完了に関する通知を送信するには、このチェックボックスをオンにします。
- **[処理が失敗したら通知を送信する]** - 処理の失敗に関する通知を送信するには、このチェックボックスをオンにします。
- **[ユーザーの操作が必要な場合に通知を送信する]** - 処理メッセージを添付して通知を送信するには、このチェックボックスをオンにします。

- **[完全なログを通知に含める]** - 処理の詳細なログを添付して通知を送信するには、このチェックボックスをオンにします。

注意
特定のバックアップについてのみ電子メール通知を受け取ります。 すべてのバックアップについて通知がほしい場合は、オンラインダッシュボードでメール通知を設定します。詳細については、「メール通知」を参照してください。どちらの方法も互いに独立して機能し、同時に使用できます。

バックアップからの項目の除外

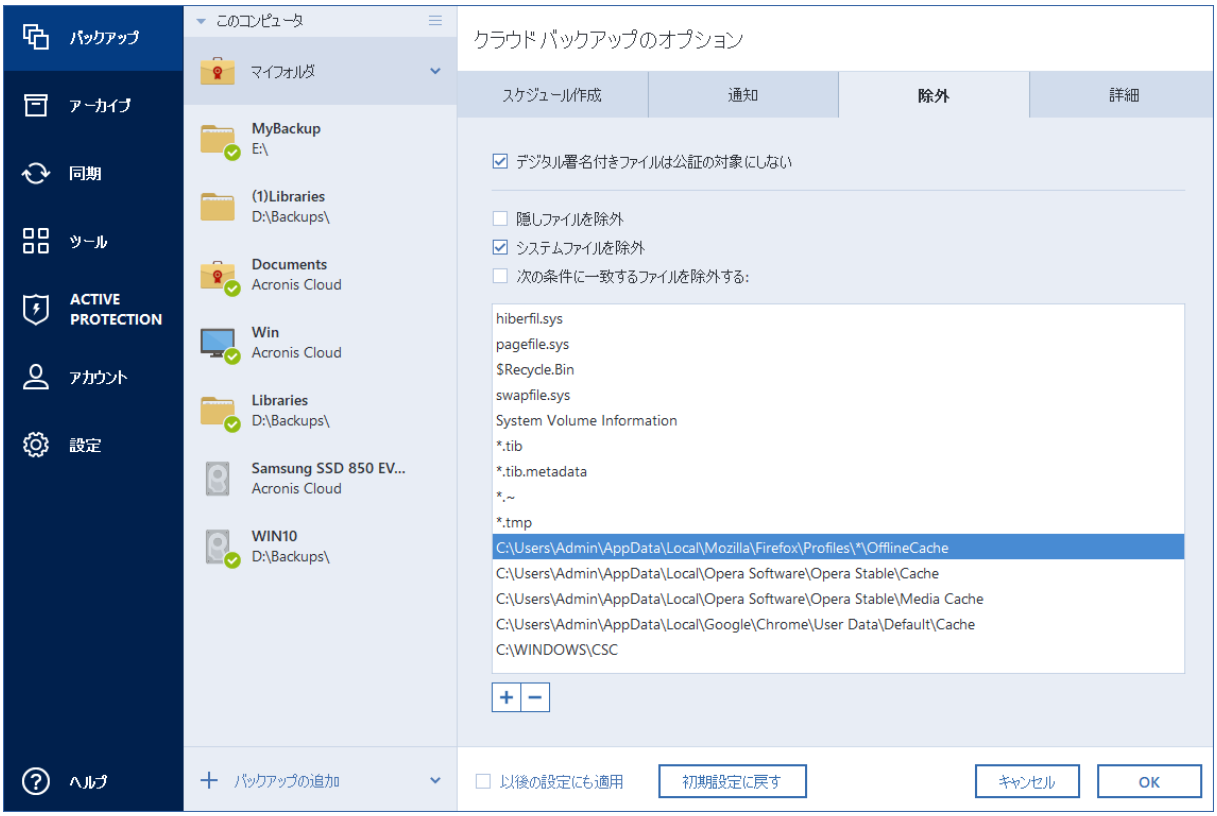
場所: **[オプション]** > **[除外]**

バックアップから不要なファイルを除外する場合は、バックアップ オプションの **[除外]** タブで該当するファイルの種類を指定します。ディスクのバックアップ、ファイルのバックアップ、またはオンラインバックアップに対して、除外を指定できます。

バックアップ対象として特定のファイルを選択した場合、除外設定で除外することはできません。除外設定は、バックアップ対象として指定されたパーティション、ディスク、またはフォルダ内に存在するファイルにのみ適用できます。

デフォルトの除外設定を使用する方法

アプリケーションをインストールすると、すべての除外設定は初期値に設定されます。これらのオプションは、現在のバックアップ処理のためだけに変更することも、今後のすべてのバックアップ向けに変更することも可能です。**[デフォルトとして保存する]** チェックボックスをオンにすると、変更した設定が今後のバックアップ作業すべてにデフォルトで適用されます。製品のインストール後に変更した設定をすべて初期値にリセットする場合は、**[初期設定にリセット]** ボタンをクリックします。



除外の対象と方法を次に示します。

バックアップからファイルを除外するときに使用できるオプションは次のとおりです。

- **[デジタル署名されたファイルは認証しない]**（認証バックアップの場合にのみ使用できます）: 認証バックアップの主な目的は、個人ファイルを保護することです。そのため、デジタル認証されたシステムファイル、アプリケーションファイル、その他のファイルをバックアップする必要はありません。これらのファイルを除外するには、対応するチェックボックスをオンにします。
- **[隠しファイルを除外]**: 隠しファイルと隠しフォルダをファイルレベルのバックアップから除外するには、このチェックボックスをオンにします。
- **[システムファイルを除外]**: システムファイルとシステムフォルダをファイルレベルのバックアップから除外するには、このチェックボックスをオンにします。

指定した条件と一致するファイルを除外することができます。除外する場合、**[次の条件に一致するファイルを除外する]** チェックボックスをオンにし、プラス記号をクリックして、除外条件を入力します。

注意
システム パーティションのバックアップから隠しファイルやシステム ファイルを除外することはお勧めできません。

除外基準を追加するには、次の手順を実行します。

- バックアップから除外するファイル名を、次のように明示的に入力します。
  - file.ext - 該当するファイルはすべてバックアップから除外されます。
  - C:¥file.ext: C: ドライブにある file.ext ファイルが除外されます。

- 次のように、ワイルドカード文字（* および ?）を使用できます。
  - *.ext: 拡張子が .ext のファイルがすべて除外されます。
  - ??name.ext: 拡張子が .ext で、ファイル名が合計 6 文字（最初の 2 文字が任意の文字（??）で、残りの部分が name）のすべてのファイルが除外されます。
- ディスクレベルのバックアップからフォルダを除外するには、プラス記号をクリックし、省略記号ボタン（[...]）をクリックしてディレクトリツリーに移動します。除外するフォルダを選択して、**[OK]** をクリックします。

間違って追加した条件を削除するには、条件を選択し、マイナス記号をクリックします。

イメージ作成モード

場所: **[オプション]** > **[詳細]** > **[イメージ作成モード]**

このオプションは、バックアップ先に Acronis Cloud を使用しているバックアップでは使用できません。

これらのパラメータを使用して、データが含まれるセクタと、パーティションまたはハードディスク全体のコピーを作成できます。たとえば、Acronis Cyber Protect Home Office がサポートしていないオペレーティングシステムが含まれているパーティションまたはディスクをバックアップする場合に便利なことがあります。このモードでは、より多くの処理時間がかかり、通常より大きいイメージファイルが作成されることに留意してください。

- セクタ単位のイメージを作成するには、**[セクタ単位でバックアップする]** チェックボックスをオンにします。
- ディスクのすべての未割り当ての領域をバックアップに含めるには、**[未割り当て領域をバックアップする]** チェックボックスをオンにします。
  このチェックボックスは、**[セクタ単位でバックアップする]** チェックボックスがオンの場合にのみ使用できます。

バックアップの保護

場所: [バックアップ] ダッシュボード > **[オプション]** > **[詳細]** > **[バックアップの保護]**

注意
このトピックは、ローカルバックアップとネットワークバックアップを対象としています。クラウドバックアップの保護の詳細については、「オンラインバックアップ保護」を参照してください。

バックアップはデフォルトではパスワード保護されていませんが、パスワードを設定してバックアップファイルを保護することができます。

注意
既存のバックアップのバックアップ保護オプションを変更することはできません。

バックアップを保護する手順は、次のとおりです。

1. バックアップ用のパスワードを対応するフィールドに入力します。パスワードはできる限り想像しにくいものにするため、8文字以上の、アルファベット（大文字と小文字の両方を使用することが望ましい）と数字を含むものにしてください。

   注意
   パスワードを取得することはできません。バックアップの保護に指定したパスワードは控えておいてください。

2. 先に入力したパスワードの確認用に、対応するフィールドにパスワードをもう一度入力します。
3. （任意の手順）機密データの安全性を高めるため、業界標準の強力な AES（Advanced Encryption Standard）暗号化アルゴリズムを使用してバックアップを暗号化することもできます。AES には、パフォーマンスと保護強度に応じて、キーの長さが 3 種類あり（128、192、256 ビット）、いずれかを選択できます。

   ほとんどの場合は、暗号キーの長さは 128 ビットで十分です。キーが長いほど、データのセキュリティは向上します。ただし、192 ビットや 256 ビットの長さのキーを使用すると、バックアップ処理の速度が大幅に低下します。

   AES 暗号を使用する場合は、以下のキーのいずれかを選択します。
   - **[AES 128]**: 128 ビット暗号キーを使用します。
   - **[AES 192]**: 192 ビット暗号キーを使用します。
   - **[AES 256]**: 256 ビット暗号キーを使用します。

   バックアップを暗号化せず、パスワードによる保護のみを行う場合は、**[暗号化しない]** を選択します。
4. バックアップの設定値を指定したら、**[OK]** をクリックします。

パスワードで保護されたバックアップにアクセスするには

Acronis Cyber Protect Home Office は、バックアップを変更するたびにパスワードを要求します。

- バックアップからのデータの復元
- 設定の編集
- マウント
- 移動

バックアップにアクセスするには、正しいパスワードを指定する必要があります。安全上の理由から、パスワードが分からない場合にリカバリする方法はありません。

オンラインバックアップ

場所: **[オプション]** > **[詳細]** > **[バックアップ保護]**

Acronis Cloud のデータを不正アクセスから保護するために、暗号化を使用することができます。この場合、データをバックアップすると、AES-256 アルゴリズムを使用してデータが暗号化され、Acronis Cloud に保存されます。データの暗号化と暗号化解除を行うためには、パスワードが必要です。パスワードは、オンラインバックアップを設定するときに指定します。任意の文字の組み合わせを指定できます。パスワードには、半角英数字のみをご使用ください。なお、大文字/小文字は区別されます。

警告
オンラインバックアップのパスワードを取得することはできません。バックアップの保護に指定したパスワードは控えておいてください。

暗号化されたデータにアクセスすると、パスワードの入力を求められます。

注意
既存のオンラインバックアップのパスワードを設定または変更することはできません。

バックアップ処理前後に実行するコマンド

場所: **[オプション]** > **[詳細]** > **[処理の前後に実行するコマンド]**

このオプションは、バックアップ先に Acronis Cloud を使用しているバックアップでは使用できません。

バックアップ処理の前後に自動的に実行するコマンド（またはバッチファイル）を指定することができます。

たとえば、バックアップを開始する前に特定のWindowsプロセスを開始/停止することや、バックアップ対象のデータを調べることができます。

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。

- **[カスタムコマンドを使用する]** チェックボックスをオンにします。
- バックアップ処理の開始前に実行するコマンドを **[処理前に実行するコマンド]** フィールドで選択します。新しいコマンドを作成する、または新しいバッチファイルを選択するには、**[編集]** ボタンをクリックします。
- バックアップ処理の終了後に実行するコマンドを **[処理後に実行するコマンド]** フィールドで選択します。新しいコマンドを作成する、または新しいバッチファイルを選択するには、**[編集]** ボタンをクリックします。

対話式のコマンド、すなわちユーザーの入力を要求するコマンド（例えば **pause**）は実行しないでください。これらのコマンドは、サポートされていません。

バックアップ用ユーザーコマンドの編集

バックアップ処理の前または後に実行するユーザーコマンドを指定することができます。

- **[コマンド]** フィールドにコマンドを入力するか、一覧から選択します。**[...]** をクリックすると、バッチファイルを選択できます。
- **[作業ディレクトリ]** フィールドに、コマンド実行のためのパスを入力するか、入力済みのパスの一覧から選択します。
- **[引数]** フィールドに、コマンド実行引数を入力するか、一覧から選択します。

[コマンドの実行が完了するまで処理を行わない] パラメータを無効にすると（デフォルトでは有効）、コマンド実行と並行してバックアップ処理を実行できます。

[ユーザーコマンドが失敗したら処理を中止する] パラメータを有効にした場合は（デフォルトでは有効）、コマンド実行でエラーが発生すると処理が中止されます。

入力したコマンドをテストするには、**[コマンドのテスト]** ボタンをクリックします。

バックアップの分割

場所: **[オプション]** > **[詳細]** > **[バックアップの分割]**

注意
Acronis Cyber Protect Home Office では、既存のバックアップを分割することはできません。バックアップの分割は作成時のみ可能です。

このオプションは、バックアップ先に Acronis Cloud を使用しているバックアップでは使用できません。

サイズの大きいバックアップを、元のバックアップを構成するいくつかのファイルに分割することができます。また、リムーバブルメディアに書き込めるようにバックアップを分割することもできます。

デフォルトの設定は **[自動]** です。この設定では、Acronis Cyber Protect Home Office 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:

- 選択したディスクに十分な空き領域があり、予想ファイル サイズがファイルシステムの許容範囲内である場合は、1 つのバックアップ ファイルを作成します。
- ストレージディスクに十分な空き領域があっても、予想ファイル サイズがファイルシステムの許容範囲を超える場合、プログラムは自動的にイメージを複数のファイルに分割します。
- ハードディスクに、イメージを保存するだけの十分な空き領域がない場合、プログラムは警告を表示し、問題への対処方法の入力を求めます。空き領域を増やして続行するか、別のディスクを選択することができます。

CD-R/RW、DVD-R/RW、DVD+R/RW、および BD-R/RE にバックアップする場合:

- Acronis Cyber Protect Home Office は、前のディスクの残り容量がなくなると新しい空ディスクを挿入するようにメッセージを表示します。

また、ドロップダウンリストからファイル サイズを選択することもできます。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。後で CD-R/RW、DVD-R/RW、DVD+R/RW、または BD-R/RE にバックアップを書き込むためにハードディスクにバックアップを保存する場合には、この機能が役立ちます。

注意
CD-R/RW、DVD-R/RW、DVD+R/RW、および BD-R/RE に直接イメージを作成すると、ハードディスクに作成するよりも大幅に時間がかかる場合があります。

バックアップのベリファイ オプション

場所: **[オプション]** > **[詳細]** > **[ベリファイ]**

このオプションは、バックアップ先に Acronis Cloud を使用しているバックアップでは使用できません。

次のような設定が可能です。

- **[完了するたびにバックアップをバリデートする]** - バックアップの直後にバックアップバージョンの整合性をチェックする場合に選択します。重要なデータやシステムディスクをバックアップする場合はこのオプションを有効にすることをお勧めします。
  - **[最新のバックアップバージョンのみをバリデートする]** - バックアップの最新のスライスをクイック検証します。
  - **[バックアップ全体をバリデート]**
- **[スケジュールに従ったバックアップのベリファイ]** - バックアップのベリファイのスケジュールを設定して、バックアップが正常な状態に保たれていることを確認する場合に選択します。
  - **[完了後に最新バージョンのバックアップ]**
  - **[完了時にバックアップ全体]**

  デフォルトの設定は次のとおりです。
  - **間隔** - 月 1 回。
  - **日付** - バックアップが開始された日。
  - **時間** - バックアップが開始された時刻 + 15 分。

バックアップのコンテキストメニューから、手動でベリファイの開始を設定することもできます。

これを実行するには、バックアップを右クリックして次から選択します。

- **[すべてのバージョンをバリデート]**
- **最新バージョンのベリファイ**

  例: 7 月 15 日の 12:00 にバックアップ処理を開始するとします。バックアップ バージョンは、12:05 に作成されます。コンピュータが「スクリーンセーバー」の状態であれば、ベリファイは 12:15 に実行されます。そうでない場合、ベリファイは実行されません。1 ヵ月後、8 月 15 日の 12:15 に、ベリファイが再び開始されます。以前と同様、コンピュータは「スクリーンセーバー」の状態である必要があります。同様に、9 月 15 日にも同じことが行われます。

  デフォルト設定を変更して、独自のスケジュールを指定することもできます。詳細については、「スケジュール設定」を参照してください。

バックアップの予備コピー

場所: **[オプション]** > **[詳細]** > **[バックアップの予備コピー]**

バックアップ先として Acronis Cloud を使用するバックアップ、および Acronis True Image（2020 または 2021）ならびに Acronis Cyber Protect Home Office で作成されたローカルバックアップでは、このオプションを使用できません。

バックアップの予備コピーは、通常のバックアップの直後に作成された、独立した完全バックアップ バージョンです。データの変更分しか含まれない増分バックアップまたは差分バックアップのバージョンを作成する場合でも、予備コピーには、通常のバックアップとして選択したすべてのデータが含めら

れます。バックアップの予備コピーは、ファイルシステム、ネットワーク ドライブ、USB フラッシュドライブなどに保存できます。

注意
予備コピーの保存先として、CD/DVD はサポートされていません。

予備コピーを作成する手順は、次のとおりです。

1. [**バックアップの予備コピーを作成する**] チェックボックスをオンにします。
2. バックアップ コピーの保存先を指定します。
3. 予備コピーの形式を選択します。これは、Acronis バックアップ（.tibx ファイル）として作成することもできますし、選択した場所にソースファイルをそのまま変更せずにコピーすることもできます。
4. （オプションの手順）予備コピーをパスワードで保護します。
   他のバックアップ オプションはすべてソース バックアップから引き継がれます。

リムーバブル メディアの設定

場所: [**オプション**] > [**詳細**] > [**リムーバブルメディアの設定**]

リムーバブル メディアにバックアップする際には、追加コンポーネントを書き込むことで、このメディアをブータブルにすることができます。このようにすると、別のブータブル ディスクが不要になります。

警告
フラッシュドライブが NTFS または exFAT でフォーマットされている場合、Acronis Cyber Protect Home Office でブータブルメディアは作成できません。ドライブは、FAT16またはFAT32ファイルシステムにしてください。

次の設定を使用できます。

- [**Acronis Cyber Protect Home Office をメディアに配置する**] - 接続されているストレージデバイスのインターフェースとして USB、PC カード（旧称: PCMCIA）、SCSI を使用する場合は、このオプションを選択することを強くお勧めします。
- [**Acronis Cyber Protect Home Office（64 ビット）をメディアに配置する**] - 64 ビットシステム用の同じオプションです。
- [**Acronis System Reportをメディアに配置する**] - プログラムの問題が発生したときに、システムに関する情報を収集するために使用するシステムレポートを生成する場合には、このオプションを選択します。レポート生成は、ブータブルメディアから Acronis Cyber Protect Home Office を起動する前でも実行可能です。生成されたシステム レポートは、USB フラッシュ ドライブに保存できます。
- [**Acronis System Report（64 ビット）をメディアに配置する**] - 64 ビットシステム用の同じオプションです。
- [**リムーバブルメディアにバックアップを作成する際に最初のメディアの挿入を求める**] - リムーバブルメディアにバックアップする際に、[**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させる場合には、このオプションを選択します。デフォルトの設定（このオプションを選択）では、リムーバブルメディアへのバックアップはユーザーがその場にいないとできない可能性があります。

これはプログラムが、メッセージを表示して **[OK]** がクリックされるのを待つからです。したがって、リムーバブル メディアへのバックアップをスケジュールする場合は、応答を要求するメッセージ表示を無効にする必要があります。こうしておくと、リムーバブル メディアが利用可能（CD-R/RW が挿入されているなど）であれば、バックアップを無人で実行できます。

他の Acronis 製品がコンピューターにインストールされている場合は、それらのプログラムのコンポーネントのブータブル版も同様に利用できます。

32 ビットまたは 64 ビットのコンポーネント

Acronis Cyber Protect Home Office および Acronis System Reportのバージョンがお使いのコンピューターと互換性があるかどうかに注意してください。

	32 ビットコンポーネント	**64 ビットコンポーネント**
BIOS ベースの 32 ビットコンピューター	+	-
BIOS ベースの 64 ビットコンピューター	+	+
EFI ベースの 32 ビットコンピューター	+	-
EFI ベースの 64 ビットコンピューター	-	+

エラー処理

Acronis Cyber Protect Home Office でバックアップの実行中にエラーが発生すると、バックアップ処理が停止され、メッセージが表示されて、エラーへの対応に関するユーザーからの指示を待つ状態になります。エラー処理ポリシーを設定し、この設定ルールに従って Acronis Cyber Protect Home Office にエラーを処理させることで、バックアップ処理を停止せずに継続させることができます。

注意
このトピックは、バックアップ先がローカルまたはネットワークにある場合に適用されます。 バックアップ先に Acronis Cloud を使用する場合のバックアップのエラー処理オプションについては、「Cloud でのバックアップとレプリケーションのエラー処理」を参照してください。

エラー処理ポリシーを設定する手順は、次のとおりです。

1. [バックアップ] ダッシュボード > **[オプション]** > **[詳細]** > **[エラー処理]** の順に選択します。
2. エラー処理ポリシーを設定します。
   - **[処理中にメッセージやダイアログを表示しない（サイレントモード）]**: この設定を有効にすると、バックアップ処理中のエラーが無視されます。バックアップ処理を制御できない場合に便利です。
   - **[不良セクタを無視する]**: このオプションは、ディスクとパーティションのバックアップの場合のみ使用できます。このオプションを有効にすると、ハードディスク上に不良セクタがある場合でもバックアップを正常に完了できます。

     たとえば次のような場合など、ハードディスクが故障しつつある場合に、このチェックボックスをオンにすることをおすすめします。

- ハードディスクドライブの動作中にかなり大きな異音や摩擦音が発生している場合。
- S.M.A.R.T.システムによってハードディスクドライブの問題が検出され、可能な限り早くドライブをバックアップするよう促された場合。

このチェックボックスをオフのままにした場合、ドライブ上に不良セクタがあると考えられるためにバックアップが失敗することがあります。

- **[Acronis Secure Zone に十分な空き領域がない場合、最も古いバックアップを削除する]**（デフォルトで有効）：スケジュールに従った Acronis Secure Zone への無人バックアップを計画する場合は、このチェックボックスをオンにしておくことをお勧めします。オンにしないと、バックアップ操作中に Acronis Secure Zone が満杯の場合に、Acronis Cyber Protect Home Office のバックアップが中断され、ユーザーの操作が必要になります。このメッセージは、**[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）]** 設定が有効な場合にも表示されます。
- **[バックアップが失敗した場合は再試行する]**: このオプションを指定すると、何らかの理由でバックアップが失敗したときにバックアップが自動的に再試行されます。試行回数および試行間隔を指定できます。バックアップが繰り返しエラーで中断される場合、バックアップは作成されません。

注意
スケジュール設定されたバックアップ処理はすべての試行が完了するまで開始されません。

3. **[OK]** をクリックします。

Cloud でのバックアップとレプリケーションのエラー処理

Cloud へのバックアップやレプリケーションが失敗した場合に再試行するよう Acronis Cyber Protect Home Office を設定できます。

再試行回数と試行間隔を設定する手順は、次のとおりです。

1. **[バックアップ]** ダッシュボードで Cloud へのバックアップをクリックし、**[オプション]** をクリックして **[詳細]** タブに移動します。
2. **[エラー処理]** で、**[バックアップが失敗した場合は試行を繰り返す]** チェックボックスをオンにし、試行回数（1～99）と試行間隔を選択します。
3. **[OK]** をクリックします。

これ以降、選択したバックアップ オブジェクトの Cloud へのバックアップ処理とレプリケーション処理には新しい設定が適用されます。

注意
スケジュール設定されたバックアップ処理は、バックアップの繰り返しが完了するまで開始されません。

バックアップ用のファイル レベルのセキュリティ設定

場所: **[オプション]** > **[詳細]** > **[ファイルレベルのセキュリティ設定]**

注意
このオプションは、ファイルレベルのバックアップでのみ使用可能です。

このオプションは、バックアップ先に Acronis Cloud を使用しているバックアップでは使用できません。

バックアップするファイルのセキュリティ設定を次のように指定できます。

- **[バックアップにファイルのセキュリティ設定を保持する]**: このオプションを選択すると、バックアップ ファイルのすべてのセキュリティ プロパティ（グループまたはユーザーに割り当てられる許可）が、将来のリカバリに備えて保存されます。
  デフォルトでは、ファイルとフォルダは元の Windows セキュリティ設定（ファイルの **[プロパティ]** -> **[セキュリティ]** で設定される、各ユーザーまたはユーザー グループに与えられる書き込み、読み取り、実行などの許可）と共にバックアップに保存されます。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上でリカバリしようとしているユーザーに、アクセス許可が与えられていない場合は、そのファイルの読み取りや変更ができなくなる可能性があります。
  このような問題を回避するため、バックアップの際にファイルのセキュリティ設定を保存するのを無効にすることができます。このようにすれば、リカバリされたファイル/フォルダのアクセス許可は常に、リカバリ先のフォルダ（親フォルダ、ルートにリカバリされる場合は親ディスク）から継承されます。
  または、ファイルのセキュリティ設定をリカバリ時に無効化できます。これは、ファイルのセキュリティ設定がバックアップに保存されている場合でも可能です。結果は同じになります。
- **[暗号化されたファイルを暗号化解除された状態でバックアップに格納する]**（デフォルト設定は [無効]）: バックアップに暗号化ファイルが含まれており、リカバリ後にそのファイルをすべてのユーザーからアクセス可能にしたい場合は、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のファイル/フォルダを読むことができます。暗号化されたファイルを別のコンピュータにリカバリする場合にも、暗号化解除が役立つことがあります。
  Windows XP 以降のオペレーティング システムで利用可能な暗号化機能を使用しない場合は、このオプションは無視してください。ファイル/フォルダの暗号化を設定するには、**[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]** の順に選択します。

コンピュータのシャットダウン

場所: **[オプション]** > **[詳細]** > **[コンピュータのシャットダウン]**

次のようなオプションの設定が可能です。

- **[コンピューターをシャットダウンするときに現在の処理をすべて停止する]** - ディスクバックアップなど、Acronis Cyber Protect Home Office が長い処理を実行中にコンピューターをオフにしようとすると、この処理によりシャットダウンが抑制されます。このチェックボックスをオンにすると、シャットダウンの前に Acronis Cyber Protect Home Office が自動的に現在の処理をすべて停止します。これには約 2 分かかります。次回の Acronis Cyber Protect Home Office の実行時に、停止したバックアップが再開されます。
- **[バックアップの完了後にコンピュータをシャットダウンする]** - 設定するバックアップ処理に時間がかかることが分かっている場合は、このオプションを選択します。これにより、処理が完了するまで

待つ必要がなくなります。プログラムはバックアップを実行し、自動的にコンピュータの電源を切ります。

このオプションは、バックアップのスケジュールを設定する場合にも便利です。たとえば、すべての作業を保存するには、平日の夕方に毎日バックアップを実行できます。バックアップのスケジュールを設定して、チェックボックスをオンにします。この設定の場合、仕事が完了したら、そのままコンピュータから離れることができます。なぜなら、重要なデータがバックアップされ、コンピュータの電源が切られることがわかっているからです。

バックアップ処理のパフォーマンス

ローカルの保存先へバックアップする場合の場所: **[オプション]** > **[詳細]** > **[パフォーマンス]**

Acronis Cloud へバックアップする場合の場所: **[オプション]** > **[詳細]** > **[パフォーマンスとネットワーク]**

圧縮レベル

バックアップの圧縮レベルを次の中から選択することができます。

- **[なし]**: データが圧縮されずにコピーされるため、バックアップファイルのサイズは非常に大きくなります。
- **[通常]**: 推奨されるデータ圧縮レベルです（デフォルトの設定）。
- **[高]**: バックアップファイルが高い圧縮レベルで圧縮されるため、バックアップの作成時間が長くなります。
- **[最大]**: バックアップは最高圧縮レベルで圧縮されるため、バックアップの作成時間が最も長くなります。

注意
最適なデータ圧縮レベルは、バックアップに保存されるファイルの種類によって異なります。たとえば、.jpg、.pdf、.mp3など、既に圧縮されたファイルを含むバックアップでは、最高圧縮レベルで圧縮してもバックアップサイズが大幅に縮小されることはありません。

注意
既存のバックアップの圧縮レベルを設定または変更することはできません。

処理の優先順位

バックアップ処理や復元処理の優先度を変更すると、（優先度の上げ下げによって）バックアップの処理速度を速くしたり遅くしたりできますが、実行中の他のプログラムのパフォーマンスに悪影響を及ぼす可能性もあります。システムで実行中の処理の優先度に応じて、処理に割り当てられるCPUやシステムリソースの使用量が決定されます。処理の優先度を下げると、他のCPUタスクで使用されるリソースを増やすことができます。バックアップや復元の優先度を上げると、実行中の他の処理からリソースを取得することができ、処理の速度が向上します。優先度変更の効果は、全体的な CPU の使用状況およびその他の要因に応じて異なります。

処理の優先度は、次のいずれかに設定することができます。

- **[低]**（デフォルトで有効）: バックアップ処理や復元処理の速度は低下しますが、他のプログラムのパフォーマンスは向上します。
- **[通常]**: バックアップ処理や復元処理に他の処理と同じ優先度が割り当てられます。
- **[高]**: バックアップ処理や復元処理の速度は向上しますが、他のプログラムのパフォーマンスは低下します。このオプションを選択すると、Acronis Cyber Protect Home Office による CPU 使用率が 100% になる場合があるので注意してください。

ネットワーク接続の転送速度

Acronis Cloud にデータをバックアップする場合、Acronis Cyber Protect Home Office の接続速度を変更できます。速度の低下を気にすることなくインターネットやネットワークリソースを使用できる接続速度を設定します。

接続速度を設定する場合は、次のいずれかのオプションを選択します。

- **最大**
  データ転送速度は、システム構成の最大値になります。
- **カスタム**
  データのアップロード速度の最大値を指定できます。

バックアップのスナップショット

警告
このオプションは、詳しい知識のあるユーザー向けです。どのオプションを選択すれば良いかわからない場合は、デフォルト設定を変更しないでください。

ディスクまたはパーティションのバックアップ処理には時間がかかることがあるため、この処理の実行中に、一部のバックアップファイルが使用中であったり、ロックされていたり、または変更中であることがあります。たとえば、ドキュメントを編集し、頻繁に保存することがあります。Acronis Cyber Protect Home Office がファイルを 1 つずつバックアップした場合、開いているファイルはバックアップの開始以降に変更され、異なる時点でバックアップに保存されている可能性があります。したがって、バックアップのデータの整合性が失われる可能性があります。これを回避するため、Acronis Cyber Protect Home Office によりいわゆるスナップショットが作成されます。スナップショットは、バックアップ対象データを特定の時点の状態に修正します。この処理はバックアップ開始前に実行されるため、データの整合性が保証されます。

[バックアップのスナップショット] リストからオプションを 1 つ選択します。

- **[スナップショットなし]** - スナップショットは作成されません。通常のコピー操作としてファイルが1つずつバックアップされます。
- **[VSS]** - このオプションはディスクレベルおよびコンピュータ全体のバックアップのデフォルトであり、バックアップのデータの整合性が保証されます。

警告
システムのバックアップでは、このオプションのみが推奨されます。異なるスナップショットタイプを使用して作成されたバックアップから復元すると、コンピュータが起動しなくなる可能性があります。

- **[Acronis スナップショット]** - 古いバージョンの Acronis Cyber Protect Home Office で使用された Acronis ドライバを使用してスナップショットが作成されます。
- **[ライタなしの VSS]** - このオプションは、ファイルレベルのバックアップのデフォルトです。VSS ライタは、スナップショットが作成されることをアプリケーションに通知する特殊な VSS コンポーネントです。これにより、アプリケーションはデータをスナップショットに向けて準備できます。このライタは、大量のファイル操作を実行しデータの整合性を必要とするアプリケーション（データベースなど）に必要です。このようなアプリケーションはホームコンピュータにはインストールされないため、ライタを使用する必要はありません。また、このオプションはファイルレベルのバックアップにかかる時間を削減します。

バックアップ用データセンターの選択

場所: **[オプション]** > **[詳細]** > **[データセンター]**

注意
このオプションはオンライン バックアップでのみ使用できます。

Acronis Cloud にバックアップを作成すると、各国の Acronis データセンターの 1 つにデータがアップロードされます。はじめに、データセンターは、Acronis アカウントの作成時の場所に最も近い場所が指定されます。それ以降は、デフォルトの場合、オンライン バックアップや同期済みファイルは同じデータ センターに保存されます。

他の国に居住している場合、またはデフォルトのデータ センターが現在地から最も近い場所ではない場合、バックアップ用のデータ センターを手動で設定することをお勧めします。データ アップロード速度を大幅に高めることができます。

注意
既存のバックアップに対しては、データセンターを変更できません。

ラップトップ電源の設定

場所: **[設定]** > **[バッテリセーバー]**

注意
この設定は、バッテリを搭載したコンピュータ（ラップトップ、UPSに接続されたコンピュータ）でのみ使用できます。

バックアップを長時間実行すると、バッテリの電源が非常に速く消耗する可能性があります。ラップトップで作業するときに電源が周りにない場合や、コンピュータが停電後にUPSに切り替えられている場合は、バッテリ電源を節約することをお勧めします。

バッテリの充電を節約する手順は、次のとおりです。

- サイドバーの **[設定]** > **[バッテリセーバー]** をクリックし、**[バッテリ電力がこれを下回る場合はバックアップしない]** チェックボックスをオンにして、電力の節約を開始するバッテリレベルをスライダで正確に設定します。

この設定をオンにすると、ラップトップ電源アダプタを取り外すか、停電時にコンピュータで UPS を使用した場合、バッテリの残り電力がスライダレベル以下になったら、現在のすべてのバックアップが一時停止されて、スケジュール済みバックアップは開始しません。電源アダプタを再び取り付けるか電源が復旧すると、一時停止されていたバックアップが再開されます。この設定のために実行されていなかったスケジュール済みバックアップも開始されます。

この設定は、バックアップ機能を完全にはブロックしません。いつでもバックアップを手動で開始できます。

ローカルモバイルバックアップは、この設定の影響を受けません。モバイルデータは、通常どおりコンピュータ上のローカルストレージにバックアップされます。

Acronis Cloud へのバックアップ用の Wi-Fi ネットワーク

場所: **[設定]** > **[バックアップに Wi-Fi ネットワークを使用]**

Acronis Cloud にデータをバックアップする場合、保護されていない Wi-Fi ネットワークで個人データが伝送されるときのセキュリティが懸念されることがあります。個人データの盗難のリスクを避けるには、保護された Wi-Fi ネットワークだけを使用することを強くお勧めします。

データを保護するには、次のようにします。

1. サイドバーで **[設定]** > **[バックアップに Wi-Fi ネットワークを使用]** をクリックして、**[ネットワークを設定]** をクリックします。
2. **[バックアップに Wi-Fi ネットワークを使用]** ウィンドウに、現在使用可能な Wi-Fi ネットワークと、使用可能でない保存済みネットワークがすべて表示されます。その中で、データのバックアップに使用するネットワークの横のチェックボックスをオンにします。

ネットワークをいくつか選択した場合、コンピュータがそれらのいずれにも接続できないと、現在のすべてのバックアップが一時停止され、スケジュール済みバックアップは開始しません。コンピュータがこのいずれかのネットワークに接続されると、一時停止したバックアップが再開されます。この設定のために実行されていなかったスケジュール済みバックアップも開始されます。

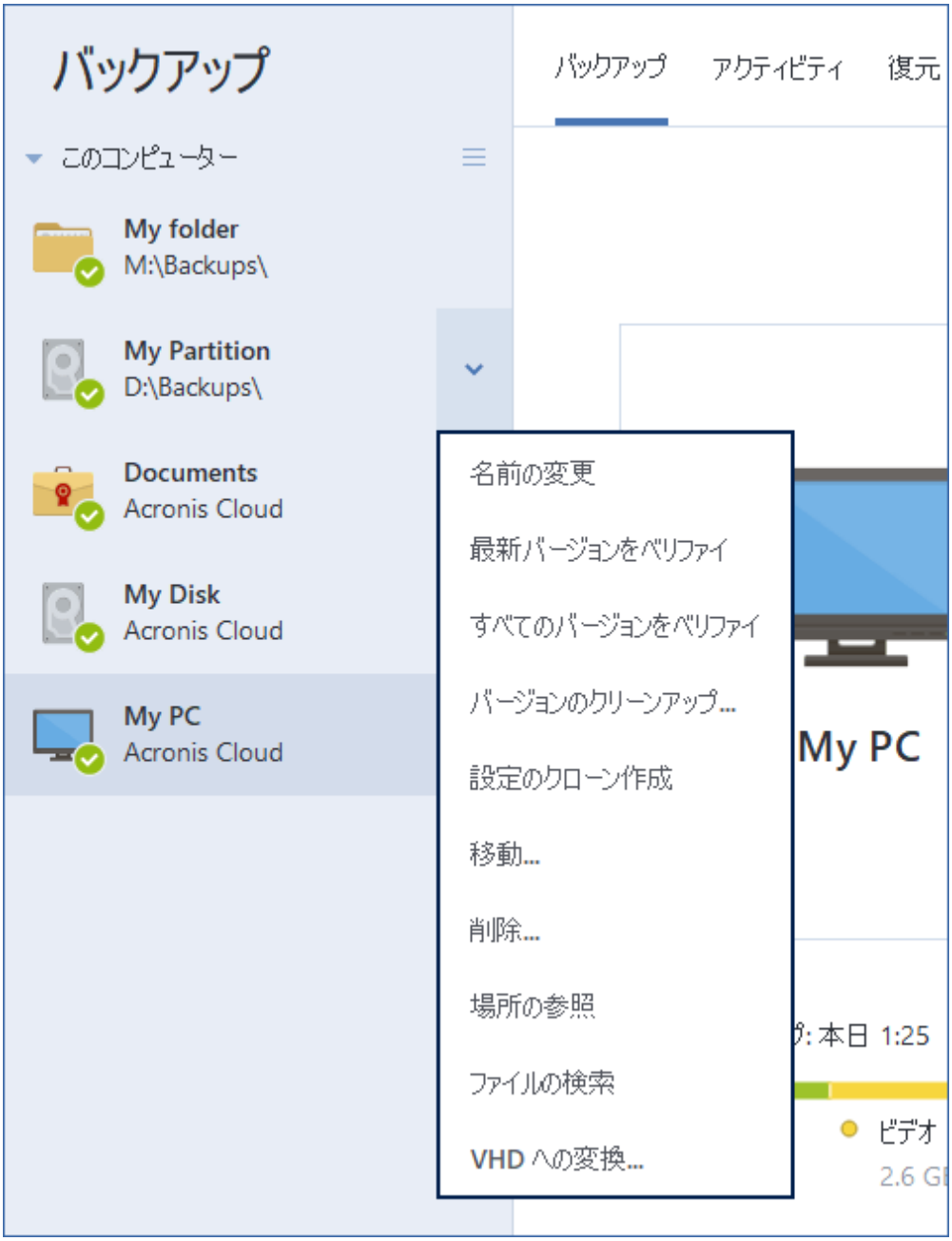
新しい Wi-Fi ネットワークを使ってデータをバックアップするには、**[バックアップに Wi-Fi ネットワークを使用]** ウィンドウ内でそれを選択するだけです。新しいネットワークを使用する必要が生じるたびに、これを行うことができます。

ローカルモバイルバックアップは、この設定の影響を受けません。モバイルデータは、通常どおりにコンピュータ上のローカルストレージにバックアップされます。

バックアップの操作

バックアップ処理メニュー

バックアップ処理メニューからは、選択したバックアップに関して実行できるその他の操作に簡単にアクセスできます。



バックアップ処理メニューには次の項目が含まれる場合があります。

- **[名前の変更]**（Acronis Cloud へのバックアップには使用できません） - リスト内のバックアップに新しい名前を設定します。バックアップファイルの名前は変更されません。

- **[再設定]**（バックアップの一覧に手動で追加したバックアップの場合） - 以前のバージョンによって作成されたバックアップの設定を行います。この項目は、別のコンピュータで作成し、設定をインポートせずにバックアップ リストに追加したバックアップでも表示されます。
  バックアップの設定がない場合、**[今すぐバックアップ]** をクリックしてバックアップを更新することはできません。また、バックアップの設定を編集することも、設定のクローンを作成することもできません。
- **[再設定]**（オンライン バックアップの場合） - 選択したオンライン バックアップを現在のコンピューターにバインドします。そのためには、この項目をクリックし、バックアップの設定を再度行います。1 台のコンピュータでアクティブにできるのは、1 つのオンライン バックアップのみです。
- **[最新バージョンをバリデート]** - バックアップの最新スライスのクイック検証を開始します。
- **[すべてのバージョンをバリデート]** - バックアップのすべてのスライスのベリファイを開始します。
- **[古いバージョンのクリーンアップ]** - 不要になったバックアップ バージョンを削除します。
- **[設定のクローン作成]** - 初期のバックアップ設定を持つ、**（1）[最初のバックアップの名前]** という名前の新しい空のバックアップボックスを作成します。設定を変更して保存し、クローンのバックアップボックスで **[今すぐバックアップ]** をクリックします。
- **[移動]** - すべてのバックアップファイルを他の保存先に移動します。後続のバックアップ バージョンは新しい場所に保存されます。
  バックアップ設定を編集してバックアップの保存先を変更した場合は、新しいバックアップ バージョンのみが新しい場所に保存されます。以前のバックアップ バージョンは、元の場所に残ります。
- **[削除]** - バックアップの種類に応じて、そのロケーションからバックアップを完全に消去するか、バックアップボックスのみを削除するかを選択できます。バックアップ ボックスを削除する場合、バックアップファイルはそのロケーションに残り、後でバックアップをリストに追加することができます。バックアップを完全に削除した場合、削除を元に戻すことはできません。
- **[場所を開く]** - バックアップファイルが格納されているフォルダを開きます。
- **[ファイルの検索]** - 検索フィールドにファイルやフォルダの名前を入力して、バックアップに含まれる特定のファイルまたはフォルダを検索します。
- **[VHD に変換]**（ディスクレベルのバックアップの場合） - 選択した Acronis バックアップバージョン（.tibx ファイル）を仮想ハードディスク（.vhd（x）ファイル）に変換します。最初のバックアップ バージョンは変更されません。

バックアップアクティビティと統計

バックアップ履歴やバックアップに含まれているファイルの種類などのバックアップに関する追加情報を、**[アクティビティ]** タブと **[バックアップ]** タブに表示することができます。**[アクティビティ]** タブには、選択したバックアップに対して実行された（作成以降の）操作リスト、操作状況、統計が含まれています。これは、バックアップモードでバックアップに何が生じていたかを突き止める必要があるときに便利です。たとえば、スケジュールされたバックアップ操作の数や状況、バックアップデータのサイズ、バックアップ検証の結果などです。

バックアップの最初のバージョンを作成するときに、**[バックアップ]** タブに、バックアップの内容がファイルの種類ごとに図表形式で表示されます。

[アクティビティ] タブ

注意
ノンストップバックアップとモバイルバックアップには、アクティビティのフィードがありません。

バックアップアクティビティを表示する手順は、次のとおりです。

1. サイドバーで **[バックアップ]** をクリックします。
2. バックアップリストで、履歴を表示するバックアップを選択します。
3. 右側のペインで **[アクティビティ]** をクリックします。

表示対象と分析対象:

- バックアップ操作とその状況（正常、失敗、キャンセル、中断など）
- バックアップに対して実行された操作とその状況
- エラーメッセージ
- バックアップのコメント
- バックアップ操作の詳細。これには、次のものが含まれます。
  - **[バックアップ済み]**: 最新のバックアップバージョンのデータのサイズ。

    ファイルレベルのバックアップの場合、Acronis Cyber Protect Home Office によってバックアップするファイルのサイズが計算されます。このパラメータの値は、完全バックアップバージョンの [復元するデータ] の値と同等です。差分バックアップと増分バックアップでは通常、[復元するデータ] よりも小さくなります。これは、Acronis Cyber Protect Home Office ではリカバリに以前のバージョンのデータが追加で使用されるためです。

    ディスクレベルのバックアップの場合、Acronis Cyber Protect Home Office によってバックアップするデータが含まれているハードドライブセクタのサイズが計算されます。セクタにはファイルへのハードリンクが含まれている可能性があるため、ディスクレベルの完全バックアップバージョンでも、このパラメータの値は、[復元するデータ] パラメータの値よりも小さくなる可能性があります。
  - **[速度]**: バックアップ操作の速度。
  - **[経過時間]**: バックアップ操作にかかった時間。
  - **[復元するデータ]**: 最新のバックアップバージョンからリカバリできるデータのサイズ。
  - **[方式]**: バックアップ操作の方法（完全、増分、または差分）。

詳細については、ナレッジベース http://kb.acronis.com/content/60104 を参照してください。

[バックアップ] タブ

バックアップを作成するときに、最新のバックアップバージョンに含まれている各種のバックアップファイルの統計を表示することができます。

カラーセグメントをポイントして、ファイルの数と各データカテゴリの合計サイズを表示します。

- ピクチャ
- ビデオファイル
- オーディオファイル
- ドキュメント
- システムファイル
- 隠しシステムファイルを含む、他のファイルタイプ

[復元対象のデータ] には、バックアップ対象として選択した元のデータのサイズが表示されます。

リスト内でのバックアップの並べ替え

デフォルトでは、バックアップは作成日の新しい順に並べ替えられます。順序を変更するには、バックアップリストの上部にある並べ替えの種類から適切なものを選択します。次の選択肢があります。

コマンド		説明
並べ替え基準	**名前**	このコマンドは、すべてのバックアップをアルファベット順に並べ替えます。 順序を逆にするには、**[Z→A]** を選択します。
	作成日	このコマンドは、すべてのバックアップを新しい順に並べ替えます。 順序を逆にするには、**[古い順]** を選択します。
	アップデート日	このコマンドは、すべてのバックアップを最新の日付順に並べ替えます。バックアップバージョンが新しいほど、リストの上位に配置されます。 順序を逆にするには、**[参照頻度の低い順]** を選択します。
	サイズ	このコマンドは、すべてのバックアップをサイズの大きい順に並べ替えます。 順序を逆にするには、**[小さい順]** を選択します。
	対象の種類	このコマンドは、すべてのバックアップを対象の種類ごとに並べ替えます。
	保存先の種類	このコマンドは、すべてのバックアップを保存先の種類ごとに並べ替えます。

Acronis Cloud にバックアップをレプリケートする

レプリケートする理由

バックアップはデータを保護する手段となりますが、それに加えて、予期せずコンピュータが破損した場合に備えてすべてのローカルバックアップを Acronis Cloud にレプリケートすることをお勧めします。もちろん 2 つのバックアップ計画を作って、1 つをローカルコンピューターに、もう 1 つを Acronis Cloud にそれぞれバックアップすることもできます。しかしバックアップ計画をセットアップする際に自動レプリケーションは時間の節約につながり、レプリカの作成作業はもう 1 つのバックアップの作成よりも素早く完了します。レプリカとはバックアップのコピーであり、どこからでもアクセス可能な保護手段となります。

レプリケーションの有効化

レプリケーションはデフォルトで無効です。 Acronis True Image（2020 または 2021）または Acronis Cyber Protect Home Office で設定したローカルの場所を使って（外付けまたは内蔵ディスクに）ディスク、パーティション、またはマシン全体を保存する任意のローカルバックアップに対して、レプリケーションを有効にできます。 レプリケーションは、バックアップ計画の特殊なタブの中で有効にすることができます。

バックアップから Acronis Cloud へのレプリケーションを有効化するには、次のようにします。

1. バックアップの一覧表示から、レプリケーションの対象となるバックアップを選択して **[レプリカ]** タブを開きます。
2. **[レプリケート]** をクリックします。これでレプリケーションが有効になり、通常のバックアップの作成時にレプリケーションが開始するようになります。Acronis Cyber Protect Home Office は閉じてもかまいません。バックアップとレプリケーションの両方のプロセスがバックグラウンドモードで継続されます。
3. （オプションの手順）**[オプション]**、**[詳細]**、**[Acronis Cloud へのレプリケーション]** の順にクリックすると、バックアップのレプリケーションの保存場所であるデータセンターが表示されます。 の クリーンアップ設定を構成すると、領域の使用を最適化できます。

レプリケートしたデータの保護

レプリケートされたデータは、Secure Socket Layer（SSL）を使用して Acronis Cloud にアップロードされます。

クラウドでは、暗号化設定に従いデータが保存されます。暗号化パスワードが設定されていない場合、レプリケートされたデータは暗号化せずに保存されます。設定されている場合、データは AES-256 で暗号化されます。

バックアップのベリファイ

ベリファイ処理でバックアップからデータを復元できるかどうかが確認されます。

たとえば、システムのリカバリ前のバックアップの検証は重要です。破損したバックアップでリカバリを開始すると、処理が失敗し、コンピューターが起動できなくなる可能性があります。ブータブルメディアを使用してシステムパーティションのバックアップを検証することをお勧めします。その他のバックアップは Windows で検証できます。「リカバリの準備」と「基本的な概念」も参照してください。

Windows でバックアップ全体を検証するには、次の手順を実行します。

1. Acronis Cyber Protect Home Office を起動し、サイドバーの **[バックアップ]** をクリックします。
2. [バックアップ] リストで、検証対象バックアップの横にある下矢印アイコンをクリックし、**[ベリファイ]** をクリックします。

スタンドアロン版の Acronis Cyber Protect Home Office（ブータブルメディア）で、特定のバックアップバージョンまたはバックアップ全体を検証するには、次の手順を実行します。

1. **[復元]**タブで、ベリファイするバージョンを含むバックアップを見つけます。バックアップがリストに表示されていない場合、**[バックアップの参照]** をクリックし、バックアップのパスを指定します。Acronis Cyber Protect Home Office がこのバックアップをリストに追加します。
2. バックアップまたは特定のバージョンを右クリックし、**[ベリファイ]** をクリックします。**ベリファイウィザード**が開きます。
3. **[実行]** をクリックします。

バックアップの保存先の分散

バックアップの設定を編集するときにバックアップの保存先を変更して、バックアップのバージョンをそれぞれ別の場所に保存することができます。たとえば、最初の完全バックアップを外付けの USB ハードドライブに保存した後に、バックアップの設定を編集して、バックアップの保存先を USB スティックに変更することができます。

後続の増分または差分バックアップは、USBスティックに書き込まれます。

注意
バックアップを光学ディスクに継続して実行することはできません。

注意
Acronis Secure Zone および FTP サーバーには、バックアップ全体のみを含めることができます。

バックアップをその場で分割する

現在のバックアップ操作を完了するための十分な空き領域が宛先ストレージ (CD-R/RW または DVD-R/RW) にない場合、警告メッセージが表示されます。

バックアップを完了するには、以下のいずれかを実行します。

- ディスク上の領域の一部を解放して、**[再試行]** をクリックします。
- **[参照]** をクリックし、別のストレージデバイスを選択します。
- **[フォーマット]** をクリックし、ディスク上のすべてのデータを消去してから、バックアップ操作に進みます。

バックアップのバージョンが別の場所に保存されている場合は、復元時にそれらの場所を指定しなければならないことがあります。

既存のバックアップをリストに追加する

Acronis Cyber Protect Home Office バックアップを過去の製品バージョンで作成したり、他のコンピュータからコピーしたりした場合、Acronis Cyber Protect Home Office を起動するたびに、コンピュータでこのようなバックアップがスキャンされ、自動的にバックアップの一覧に追加されます。

リストに表示されないバックアップについては、手動で追加することができます。

バックアップを手動で追加するには、次のようにします。

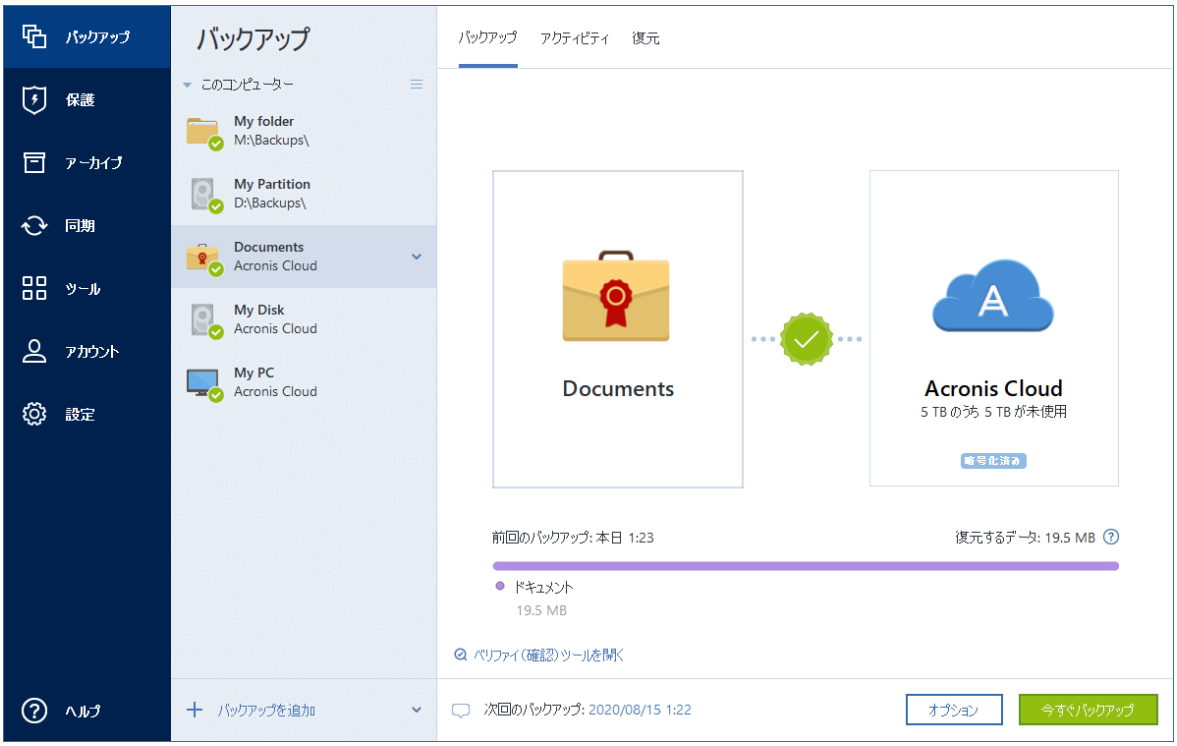
1. **[バックアップ]** セクションで、バックアップリストの下部にある矢印アイコンをクリックし、**[既存のバックアップを追加]** をクリックします。ウィンドウが開き、コンピュータ上に存在するバックアップを参照できます。
2. バックアップバージョン（.tibx ファイル）を選択し、**[追加]** をクリックします。
   バックアップ全体がリストに追加されます。

認証バックアップ

Acronis Cyber Protect Home Office は、ブロックチェーン技術を使用してファイルを不正な変更から保護できます。これにより、正しいバックアップファイルからデータを復元できることが保証されます。法律文書など信頼性の証明が求められるファイルは、このタイプのバックアップを使用して保護することをお勧めします。詳細については、「ブロックチェーン技術の使用」を参照してください。

ファイルとフォルダの認証バックアップを作成する手順

1. Acronis Cyber Protect Home Office を開始します。
2. サイドバーで **[バックアップ]** をクリックします。
3. **[バックアップの追加]** をクリックします。
4. （オプション）バックアップの名前を変更するには、バックアップ名の横にある矢印をクリックし、**[名前の変更]** をクリックして、新しい名前を入力します。
5. **[バックアップ対象]** 領域をクリックし、**[認証するファイル]** を選択します。
6. 表示されたウィンドウで、バックアップするファイルやフォルダの横にあるチェック ボックスをオンにし、**[OK]** をクリックします。



7. **[バックアップの保存先]** 領域をクリックし、バックアップの保存先を選択します。
   - **Acronis Cloud** - Acronis のマイアカウントにサインインし、**[OK]** をクリックします。
     Acronis アカウントをお持ちでない場合は、**[アカウントの作成]** をクリックして E メールアドレスとパスワードを入力し、**[アカウントの作成]** ボタンをクリックします。詳細については、「Acronis アカウント」を参照してください。
   - **外付けドライブ**: 外付けドライブがコンピュータに接続されている場合は、リストからそのドライブを選択できます。
   - **NAS**: 検出されたNASデバイスのリストからNASを選択します。NAS が 1 つしかない場合、Acronis Cyber Protect Home Office はデフォルトでその NAS をバックアップの保存先として使用するように提案します。
   - **参照**: フォルダ ツリーから保存先を選択します。
8. （オプションの手順）バックアップのオプションを設定するには、**[オプション]** をクリックします。詳細については、「バックアップオプション」を参照してください。
   デジタル署名のあるファイルをバックアップから除外するには、**[除外]** タブの **[デジタル署名されたファイルは認証しない]** チェックボックスをオンにします。詳細については、「バックアップからの項目の除外」を参照してください。
9. （オプションの手順）**[コメントを追加]** アイコンをクリックして、バックアップバージョンにコメントを入力します。バックアップのコメントは、データをリカバリするときなど、あとで必要なバージョンを検索するときに役立ちます。
10. 次のいずれかを実行します。
    - バックアップを直ちに実行するには、**[今すぐバックアップ]** をクリックします。
    - 後でバックアップを実行する、またはスケジュールに基づいてバックアップを実行するには、**[今すぐバックアップ]** ボタンの右側にある下向きの矢印をクリックし、**[後で実行]** をクリックします。

注意
Acronis Cloud にデータをバックアップする場合は、最初のバックアップが完了するまでにかなり時間がかかることがあります。以降のバックアップ処理は、ファイルに対する変更のみがインターネットを使って転送されるので、大幅に速くなります。

さらに、https://goo.gl/WjUoPZ のビデオ解説（英語）をご覧ください。

ブロックチェーン技術の使用

Acronis Cyber Protect Home Office は、ブロックチェーン技術を使用してバックアップファイルをトップレベルのセキュリティで保護します。この技術により、ファイルが不正ソフトウェアによって変更されていないこと、および復元時に正しいバックアップファイルからデータを復元できることが保証されます。

ブロックチェーンとは

ブロックチェーンは、トランザクションとそのシーケンスに関する情報を格納するデータベースです。一般に、トランザクションは財務処理や各種資産の処理などに関するイベントを意味します。トランザクションはブロックにまとめられ、ブロックがデータベースに1つずつ書き込まれ、ブロックチェーンを形成します。すべてのトランザクションとすべてのブロックに一意の識別番号が割り振られています。どのブロックにもチェーンの以前のブロックすべての情報が格納されていることが重要です。データベースに書き込まれたトランザクション情報は、誰もいかなる手段でも変更できません。同じくトランザクションシーケンスも変更できません。データベース内の情報を変更しようとしても、任意のデータベースユーザーによって簡単に見破られます。これは、正しくないトランザクションやブロックに関する情報がそれ以降のどのブロックにも存在しないためです。このテクノロジにより、データベースに格納されているデータが正当で、特定の人物に属しており、誰にも変更されていないことが保証されます。ブロックチェーンの詳細については、https://en.wikipedia.org/wiki/Blockchain_(database)を参照してください。

Acronis Cyber Protect Home Office でのブロックチェーン技術の使用方法

不正な変更からファイルを保護するため、Acronis Cyber Protect Home Office は Acronis 認証テクノロジを使用します。これは、任意のデータオブジェクトおよびデータストリームにタイムスタンプとフィンガープリントを付けるための汎用ソリューションです。大量のデータをブロックチェーンデータベースに格納できないため、Acronis Cyber Protect Home Office はファイルのハッシュコードだけを Acronis 認証サービスに送ります。

ハッシュコードは、ハッシュ関数によって生成される固定サイズの一意の番号です。このコードは、バックアップファイルなどの任意のデータセットを数学的に定義します。バックアップファイルを変更すると、そのハッシュコードも変更されます。したがって、ファイルが変更されているかどうかを確認する場合、最初に生成されたハッシュコードとファイルの現在の状態を比較するだけで済みます。コードが一致した場合、ファイルが誰にも変更されていないことが保証されます。

Acronis 認証は、ファイルのハッシュコードを受け取ると、新しい 1 つのハッシュコードを計算し、ブロックチェーンベースの Ethereum データベースにそのハッシュコードを送ります。イーサリアムの詳細については、https://www.ethereum.org/を参照してください。

ハッシュコードがデータベースに送られると、そのハッシュコードを計算するために使用したファイルが、Acronis 認証によって認証されます。「ファイルの真正性の検証」で説明されている手順に従うと、ファイルの真正性をいつでも簡単に検証できます。すべての認証されたファイルには、認証証明書があります。認証証明書は、ファイルがブロックチェーン技術によって保護されていることの文書による証明です。証明書には、ファイルに関する一般的な情報と、ファイルの真正性を手動で検証するために利用できる技術的な詳細が含まれています。詳細については、「ファイルの真正性の手動検証」を参照してください。

ファイルの真正性の検証

Acronis Cyber Protect Home Office は、ブロックチェーン技術を使用してバックアップファイルを不正な変更から保護できます。これにより、正しいバックアップファイルからデータを復元できることが保証されます。

Acronis Cyber Protect Home Office でファイルの真正性を検証するには、次のようにします。

1. Acronis Cyber Protect Home Office を開始します。
2. サイドバーで **[バックアップ]** をクリックします。
3. バックアップリストから、復元するファイルを含む認証バックアップを選択します。
4. 右側のペインで、**[復元]** タブをクリックします。
5. 必要なファイルを参照し、メニューアイコン（ ）をクリックし、次のいずれかをクリックします。
   - **[認証の確認]**: ファイルセキュリティに関する詳細情報を含む証明書が Web ブラウザで表示されます。
   - **[検証]**: Acronis Cyber Protect Home Office はファイルの真正性を検証します。

ファイル検証ツールでファイルの信頼性を検証する手順

1. 次のいずれかの方法で、ファイル検証ツールを起動します。
   - Web ブラウザで、https://notary.acronis.com/verify を開きます。
   - Acronis Cyber Protect Home Office のサイドバーの **[バックアップ]** をクリックし、認証バックアップを選択し、右側のパネルで **[ファイル検証ツールを起動]** をクリックします。
2. 検証するファイルをエクスプローラーで参照し、そのファイルを Web ブラウザ ウィンドウにドラッグします。

認証バックアップが Acronis Cloud に格納されている場合は、バックアップファイルの真正性を Acronis Cloud Web アプリケーションで検証することもできます。

Acronis Cloud でファイルの真正性を検証するには、次のようにします。

1. https://www.acronis.com/my/online-backup/webrestore/ に移動し、Acronis アカウントにログインします。
2. サイドバーで **[バックアップ]** をクリックします。
3. バックアップリストから、復元するファイルを含む認証バックアップを選択します。
4. 必要なファイルを参照し、それをチェックマークで選択します。次に、右サイドバーの **[検証]** をクリックします。

ファイルの真正性の手動検証

ファイルの真正性を検証する最も簡単な方法は、Acronis Cyber Protect Home Office または Acronis Cloud Web アプリケーションの **[検証]** コマンドを使用することです。詳細については、「ファイルの真正性の検証」を参照してください。この簡単な方法に加え、ユーザーが自分で検証手順を段階的に実行することもできます。

ファイルの真正性を手動で検証するには、次のようにします。

手順1. ファイルのMD5ハッシュを計算する

1. Windows PowerShellを起動します。
2. たとえば、C:¥Users¥フォルダにあるpicture.pngファイルのmd5ハッシュを計算するには、次のように入力します。

   ```
   $($(CertUtil -hashfile "C:\Users\picture.png" MD5)[1] -replace " ","")
   ```

   md5ハッシュの例: eea16ade1edf2750a46bb6bffb2e45a2
3. 計算したmd5ハッシュが認証証明書のデータフィールドのeTagに一致することを確認します。ファイル証明書の取得の詳細については、「ファイルの真正性の検証」を参照してください。

手順2. ROOTがブロックチェーンに保存されていることを確認する

1. ブロックチェーンエクスプローラ（たとえばhttps://etherscan.io/）を開きます。
2. 証明書のTRANSACTION IDを検索フィールドに入力します。
3. [イベントログ] タブの [データ] フィールドが証明書の ROOT 値と同等であることを確認します。

手順 3. ハッシュがツリーに含まれていることを確認する

1. コマンドラインユーティリティをGitHubリポジトリhttps://github.com/acronis/notary-verifyhash/releasesからダウンロードします。
2. https://github.com/acronis/notary-verifyhashの指示に従います。

Acronis ASign

Acronis ASign とは

Acronis ASign とは、複数の人がファイルを電子的に署名するためのオンラインサービスです。ファイルは、バックアップ、アーカイブ、または同期を使用して事前に Acronis Cloud にアップロードされている必要があります。署名されたファイルの保護を強化するには、ファイルに Acronis Notary を使用した公証と保護を行います。

ASign ソリューションは、さまざまな種類の契約書、同意書、証明書、金融書類、公文書など、任意の電子ドキュメントの署名に使用できます。

ファイルへの署名

Acronis Cloud でファイルに署名する手順は、次のとおりです。

1. https://www.acronis.com/my/online-backup/webrestore/ に移動し、Acronis アカウントにログインします。
2. 必要なファイルを参照し、ファイル名をクリックして、表示されるメニューで **[署名用に送信]** を選択します。
3. ファイルに署名した後で招待を送信する相手の電子メールアドレスを入力します。
   ファイルに対してすべての署名者による署名がされた後、Acronis Notary がファイルを公証し、署名証明書を生成します。

この機能の詳細については、Acronis ASign Web ヘルプ（https://www.acronis.com/ja-jp/support/documentation/ATI2017ASign/）（英語）を参照してください。

バックアップ、バックアップバージョン、レプリカをクリーンアップする

不要になったバックアップとバックアップバージョンを削除するには、Acronis Cyber Protect Home Office が提供するツールを使用します。

Acronis Cyber Protect Home Office は、バックアップに関する情報をメタデータ情報データベースに保存します。そのため、不要なバックアップファイルを File Explorer で削除しても、バックアップに関する情報はデータベースから削除されません。その結果、既に存在していないバックアップに対してもプログラムが処理を実行しようとして、エラーが発生します。

バックアップ全体とそのレプリカを削除する

[バックアップ] セクションで、削除対象バックアップの横にある下矢印アイコンをクリックし、**[削除]** をクリックします。

バックアップの種類に応じて、このコマンドではバックアップをそのロケーションから完全に削除する場合があり、バックアップを完全に（すべてのファイルとともに）削除するか、リストだけから削除するかを選択できる場合もあります。表示されたリストからバックアップを削除すると、バックアップファイルはそのロケーションに残り、後でバックアップをリストに追加することができます。バックアップを完全に削除した場合、削除を元に戻すことはできません。

バックアップを削除すると、そのレプリカも自動的に一緒に削除されます。ローカルバックアップを削除してそのレプリカを引き続き保持することはできません。ただし、レプリカだけを削除してローカルバックアップを保持することは可能です。

バックアップレプリカ全体を削除する

元のバックアップと一緒にレプリカを削除することも、レプリカを別個に削除することもできます。バックアップと一緒に削除するには、上記の方法に従ってバックアップを削除してください。

バックアップを削除せずにレプリカを削除するには、**[バックアップ]** セクションで、削除するレプリカを含むバックアップの横にある下矢印アイコンをクリックしてから、**[レプリカの削除]** をクリックします。

バックアップバージョンの自動クリーンアップ

1. **[バックアップ]** セクションに移動します。
2. バックアップの一覧から、レプリカバージョンのクリーンアップの対象となるバックアップを選択して、**[オプション]** をクリックします。
3. **[バックアップスキーム]** タブで **[カスタムスキーム]** を選択します。バックアップの種類を選択して **[自動クリーンアップをオンにする]** をクリックします。
4. バックアップのクリーンアップルールを設定します。
   詳細については、「カスタムスキーム」を参照してください。

注意
クリーンアップ後、いくつかの補助的なファイルがストレージに残る場合があります。それらを削除しないでください。

レプリカバージョンの自動クリーンアップ

1. **[バックアップ]** セクションに移動します。
2. バックアップの一覧から、レプリカバージョンのクリーンアップの対象となるバックアップを選択して、**[オプション]** をクリックします。
3. **[詳細]** タブで、**[Acronis Cloud のクリーンアップ]** タブを開きます。
   - **[最大保存バックアップバージョン数]** オプションを使用して、保存するレプリカバージョンの最大数を制限する値を入力します。
   - **[この期間が経過したバックアップバージョンを削除する]** チェックボックスをオンにしてから、古いバージョンを保持する期間の上限を入力します。新しいバージョンから順番に保持され、その他のすべてのバージョンは自動的に削除されます。

バックアップバージョンの手動でのクリーンアップ

不要になったバックアップバージョンを削除する場合は、アプリケーションに用意されているツールを使用してください。たとえば、エクスプローラーを使用して Acronis Cyber Protect Home Office の外部でバックアップバージョンファイルを削除すると、バックアップに対する操作でエラーが発生します。

次のバックアップのバージョンは手動では削除できません。

- CD、DVD、BD、Acronis Secure Zone に保存されているバックアップ。
- ノンストップバックアップ。
- 認証バックアップ。

特定のバックアップバージョンをクリーンアップする手順は、次のとおりです。

1. Acronis Cyber Protect Home Office を開始します。
2. **[バックアップ]** セクションで、クリーンアップするバックアップの横にある下矢印アイコンをクリックし、**[Clean up versions]** をクリックします。
   これにより、**[Clean up backup versions]** ウィンドウが開きます。

3. 必要なバージョンを選択し、**[削除]** をクリックします。
4. 確認要求で **[削除]** をクリックします。

クリーンアップ処理が終わるまで待ちます。クリーンアップ後、いくつかの補助的なファイルがストレージに残る場合があります。それらを削除しないでください。

依存するバージョンがあるバージョンのクリーンアップ

削除するバックアップバージョンを選択するときには、削除するバージョンに依存するバージョンが存在する可能性があることに注意してください。この場合、削除するバージョンからのデータの復元は不可能になるため、依存するバージョンも削除するものとして選択されます。

- **完全バックアップを選択した場合**: 次の完全バージョンまでの、依存するすべての差分バージョンと増分バージョンも選択されます。つまり、バックアップバージョンチェーン全体が削除されます。
- **差分バックアップを選択した場合**: バックアップバージョンチェーン内の依存するすべての増分バージョンも選択されます。
- **増分バックアップを選択した場合**: バックアップバージョンチェーン内の依存するすべての増分バージョンも選択されます。

参照

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 Cloud からのデータの削除。

Acronis Cloud でのスペースのクリーンアップ

1. https://www.acronis.com/my/online-backup/webrestore/に移動し、Acronis アカウントにログインします。Acronis Cloud の Web アプリケーションが開きます。
2. Web アプリケーションの左サイドバーで **[アカウント]** をクリックします。
3. **Acronis Cloud** 行で、**[クリーンアップ]** をクリックします。
4. 削除対象となるバージョンを選択:
   - 一定期間が経過したバージョン。
   - 最近のいくつかのバージョンを除くすべての古いバージョン。

警告
ご注意ください。削除したバージョンは、復元することができません。

不要になったクラウドバックアップを削除してクリーンアップする方法もあります。この場合、バックアップのすべてのバージョン履歴が Acronis Cloud から削除されます。

Acronis Cloud からのデータの削除

Acronis Cloud 上の空き領域は限られているため、古いデータや不要になったデータをクリーンアップしてクラウド領域を管理する必要があります。クリーンアップは Acronis Cyber Protect Home Office で実行できます。Acronis Cloud Web アプリケーションでも実行できます。

バックアップ全体を削除する

最も抜本的な方法は、Acronis Cloud 上のバックアップ全体を削除する方法です。バックアップが削除されると、そのすべてのデータが完全に消去されます。削除されたデータを復元することはできません。

Acronis Cyber Protect Home Office で、次の手順を実行します。

削除対象バックアップの横にある下矢印アイコンをクリックし、**[削除]** をクリックします。対象となるバックアップと、そのバージョン、設定、スケジュールがすべて削除されます。

Acronis Cloud Web アプリケーションで、次の手順を実行します。

1. https://www.acronis.com/my/online-backup/webrestore/ に移動し、Acronis アカウントにログインします。
2. **[バックアップ]** タブで、削除するバックアップに移動します。
3. バックアップのサイズをクリックすると、詳細ビューが表示されます。
4. 詳細ビューで **[削除]** をクリックします。

バックアップは Acronis Cloud から削除されますが、その設定とスケジュールはすべて、Acronis Cyber Protect Home Office アプリケーションに残ったままになることに注意してください。

クラウドへのバックアップのバージョンの削除

Acronis Cyber Protect Home Office で、次の手順を実行します。

1. 削除対象バックアップの横にある下矢印アイコンをクリックし、**[古いバージョンのクリーンアップ]** をクリックします。
   バックアップバージョンのリストが開きます。
2. 削除するバージョンを選択し、**[削除]** をクリックします。

注意
Acronis Cloud のクォータのアップデートには最大 1 日かかる場合があります。

Acronis Cloud Web アプリケーションで、次の手順を実行します。

1. https://www.acronis.com/my/online-backup/webrestore/ に移動し、Acronis アカウントにログインします。
2. **[バックアップ]** タブで、削除するバージョンのバックアップのサイズをクリックします。
   バックアップの詳細ビューが開きます。
3. 詳細ビューで、**[クリーンアップ]** をクリックします。
   選択した期間より古いバージョンを削除するか、最近のバージョンを除くすべてのバージョンをクリーンアップするかを選択できます。
4. 削除するものを構成して、**[今すぐクリーンアップ]** をクリックします。
5. 確認ダイアログで、**[削除]** をクリックします。

操作が完了すると、クリーンアップ手順のステータスが表示されます。

クラウドへのバックアップレプリカのバージョンの削除

Acronis Cyber Protect Home Office で、次の手順を実行します。

1. **[バックアップ]** セクションで、クラウドにレプリケートされたローカルバックアップを見つけ、下矢印をクリックして、**[古いバージョンのクリーンアップ]** を選択します。
   これにより、[バックアップバージョンのクリーンアップ] ダイアログが開きます。
2. **[バージョンの削除元]** から、**[Acronis Cloud]** を選択します。
   バックアップレプリカのバージョンのリストが表示されます。
3. 削除するレプリカバージョンを選択し、**[削除]** をクリックします。
4. 確認ダイアログで、**[削除]** をクリックします。

注意
Acronis Cloud のクォータのアップデートには最大 1 日かかる場合があります。

Acronis Cloud Web アプリケーションで、次の手順を実行します。

1. https://www.acronis.com/my/online-backup/webrestore/ に移動し、Acronis アカウントにログインします。
2. **[バックアップ]** タブで、削除するバージョンのバックアップレプリカのサイズをクリックします。
   バックアップレプリカの詳細ビューが開きます。
3. 詳細ビューで、**[クリーンアップ]** をクリックします。
   選択した期間より古いバージョンを削除するか、最近のバージョンを除くすべてのバージョンをクリーンアップするかを選択できます。
4. 削除するものを構成して、**[今すぐクリーンアップ]** をクリックします。
5. 確認ダイアログで、**[削除]** をクリックします。

操作が完了すると、クリーンアップ手順のステータスが表示されます。

ワンタイムクリーンアップ

Acronis Cloud がいっぱいの場合、または空き領域が不足しているときは、Acronis Cloud Web アプリケーションのクリーンアップツールを使用することをお勧めします。このツールを使用すると、素早く簡単に Cloud で非常に多くの領域を解放できます。

注意
暗号化されているものも含め、バックアップを個別にクリーンアップできます。パスワードが要求されます。

1. https://www.acronis.com/my/online-backup/webrestore/ に移動し、Acronis アカウントにログインします。
2. **[バックアップ]** タブで、削除するバックアップに移動します。
3. **[クリーンアップ]** ボタンをクリックします。

4. 開いているウィンドウで、クリーンアップ設定を行ってから、[**今すぐクリーンアップ**] をクリックします。

暗号化されていないすべてのバックアップに対して 1 回限りのクリーンアップを実行するには、次のオプションを使用します。

1. [**アカウント**] タブに移動します。
2. [**クリーンアップ**] ボタンをクリックします。

データの復元

ディスクとパーティションのリカバリ

クラッシュ後のシステムの復元

コンピュータが起動に失敗した場合、「クラッシュの原因を特定する」で説明されているヒントを参考にして、まず原因を特定することをおすすめします。クラッシュがオペレーティングシステムの破損によって発生した場合は、バックアップを使用してシステムを復元します。「リカバリの準備」を参照して準備を完了し、システム復元の手順に進みます。

異常停止の原因を特定する

システムが異常停止する原因には、2つの基本的な要因があります。

- **ハードウェア障害**

  この場合は、ハードウェア メーカーのサービス センターに問い合わせることをお勧めします。その前に、いくつかの検査を実行することもできます。ケーブル、コネクタ、外付けデバイスの電源などを確認します。その後、コンピュータを再起動してください。ハードウェアに問題がある場合は、Power-On Self Test（POST）を通じて障害が通知されます。

  POSTによってハードウェア障害が見つからなかった場合、BIOSを開始して、システムのハードディスクドライブが認識されているかどうかを確認します。BIOSを開始するには、POSTシーケンス中に必要なキーの組み合わせ（**Del** キー、**F1** キー、**Ctrl**+**Alt**+**Esc** キー、**Ctrl**+**Esc** キーなど。ご使用のBIOSによります）を押します。通常は起動テスト中に、必要なキーの組み合わせを示すメッセージが表示されます。このキーの組み合わせを押すと、セットアップメニューが表示されます。ハードディスク自動検出ユーティリティを選択します。通常は、「Standard CMOS Setup」または「Advanced CMOS setup」の下に表示されています。ユーティリティによってシステムドライブが検出されなかった場合、システムドライブに障害が発生しているので、ドライブを交換する必要があります。
- **オペレーティングシステムの損傷（Windowsを起動できない場合）**

  POSTによって、システムのハードディスクドライブが正常に検出された場合、異常停止の原因は、ウイルス、マルウェア、または起動に必要なシステムファイルの破損が考えられます。この場合は、システムディスクまたはシステムパーティションのバックアップを使用してシステムをリカバリしてください。詳細については、「システムの復元」を参照してください。

リカバリの準備

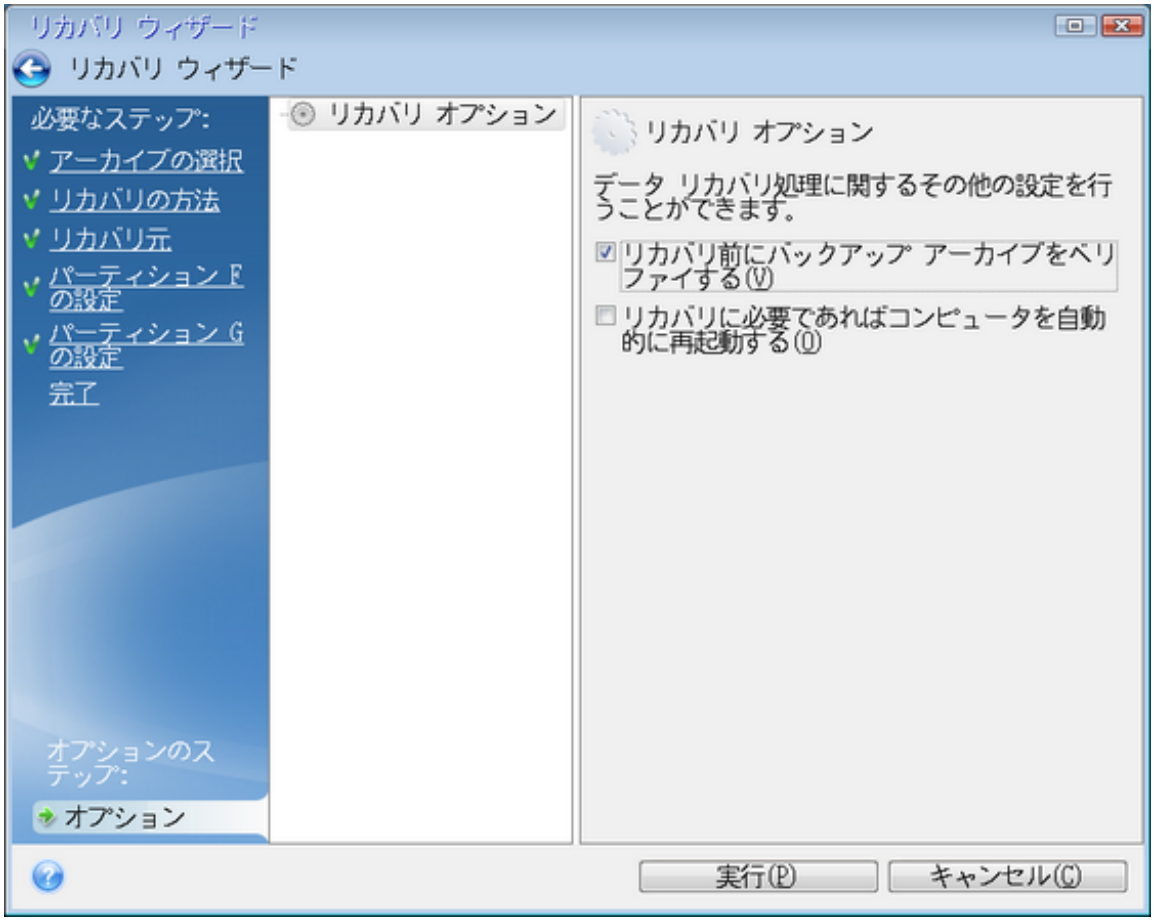
リカバリの前に以下の操作を実行することをお勧めします。

- ウィルスまたはマルウェア攻撃のためにクラッシュが発生したことが疑われる場合、コンピュータがウィルスに感染しているかどうかスキャンします。
- ブータブルメディアの配下に予備のハードドライブがある場合、予備のハードドライブへの復元テストを試します。

- ブータブルメディアの配下でイメージをベリファイします。Windowsでのベリファイ中に読み取ることのできるバックアップは、**Linux環境でも常に読み取れるとは限りません。**

  ブータブル メディアでは、バックアップをベリファイする方法が 2 つあります。

  - バックアップを手動でベリファイするには、[**リカバリ**] タブでバックアップを右クリックし、[**ベリファイ**] を選択します。
  - リカバリの前に自動的にバックアップをベリファイするには、**リカバリ ウィザード**の [**オプション**] 手順で、[**リカバリ前にバックアップ アーカイブをベリファイする**] チェック ボックスをオンにします。



- ハードドライブのすべてのパーティションに一意の名前（ラベル）を割り当てます。これにより、バックアップを含むディスクを見つけることが容易になります。

  ブータブルメディアを使用すると、Windows でのドライブの識別方法とは異なるディスクドライブ文字が作成されることがあります。たとえば、ブータブルメディアでの D: ディスクが、Windows の E: ディスクに対応していることもあります。

同じディスクへのシステムのリカバリ

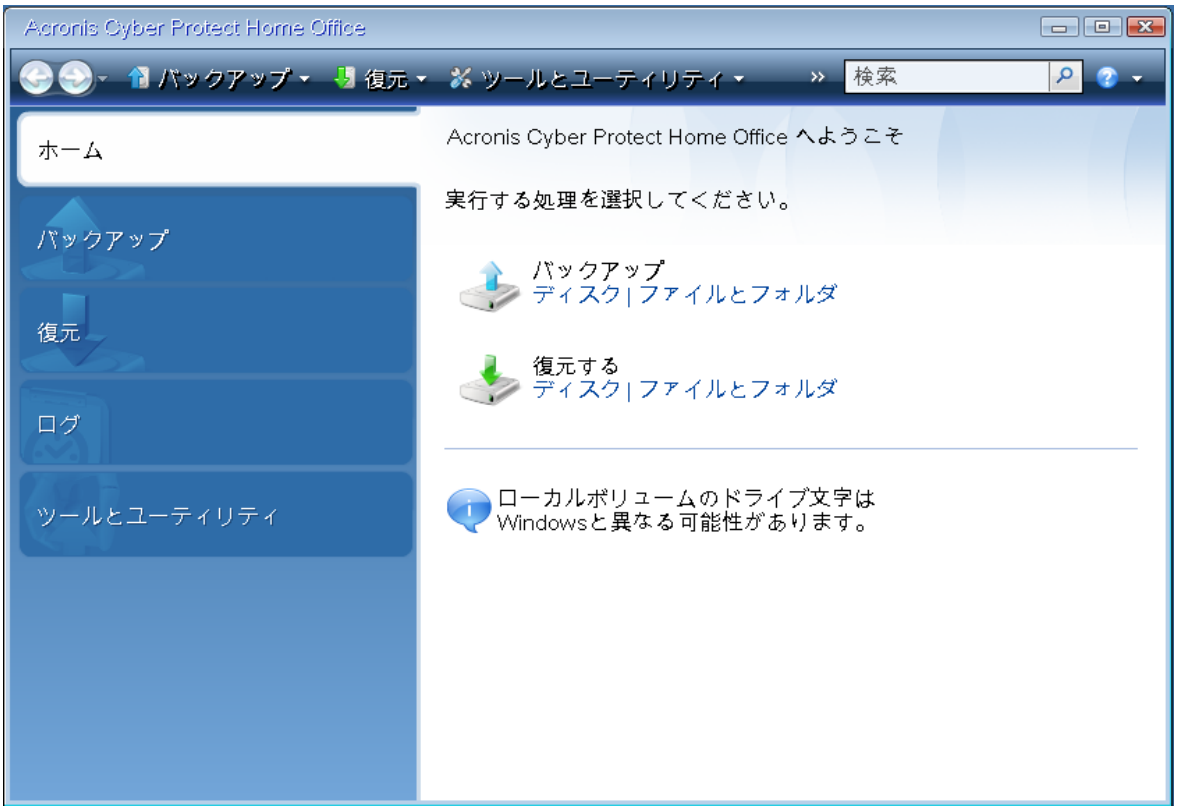
始める前に、「リカバリの準備」で説明している手順を実行することをお勧めします。

システムをリカバリするには、次の手順を実行します。

1. リカバリに使用するバックアップが外部ドライブに格納されている場合は、その外部ドライブを接続して電源を入れます。

2. BIOS で起動順序を設定して、Acronis ブータブルメディア（CD、DVD、または USB ドライブ）を最初の起動デバイスにします。「BIOSまたはUEFI BIOSでの起動順の並べ替え」を参照してください。

   UEFI コンピュータを使用する場合、UEFI BIOS のブータブルメディアの起動モードに注意してください。起動モードはバックアップのシステムの種類と一致するようにしてください。バックアップにBIOSシステムが含まれている場合はBIOSモードでブータブルメディアを起動してください。システムがUEFIの場合は、UEFIモードが設定されていることを確認してください。
3. Acronis ブータブルメディア から起動して、**[Acronis Cyber Protect Home Office]** を選択します。
4. **[ホーム]** 画面で、**[リカバリ]** の下にある **[マイディスク]** を選択します。

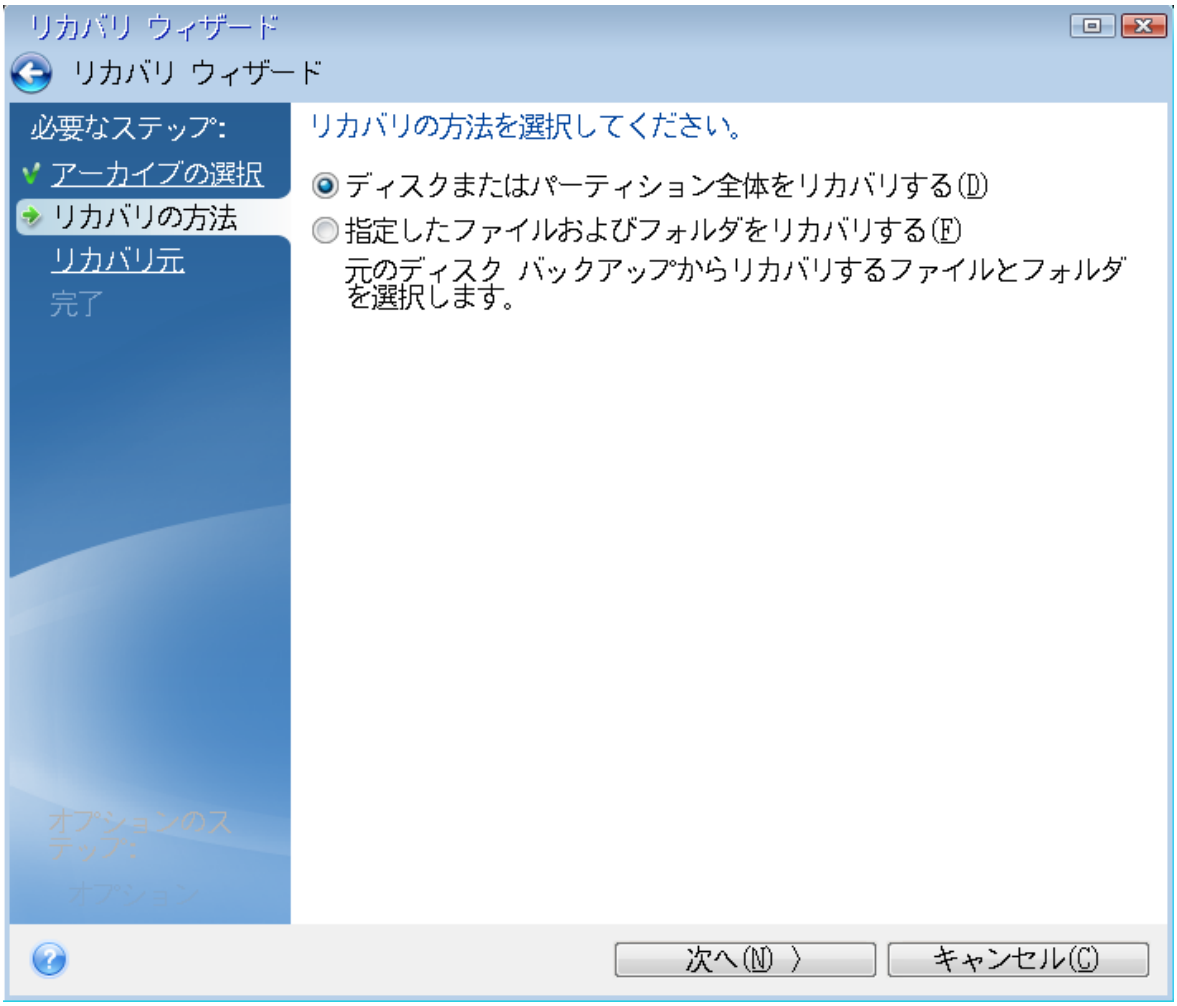


5. リカバリに使用するシステムディスクまたはパーティションバックアップを選択します。

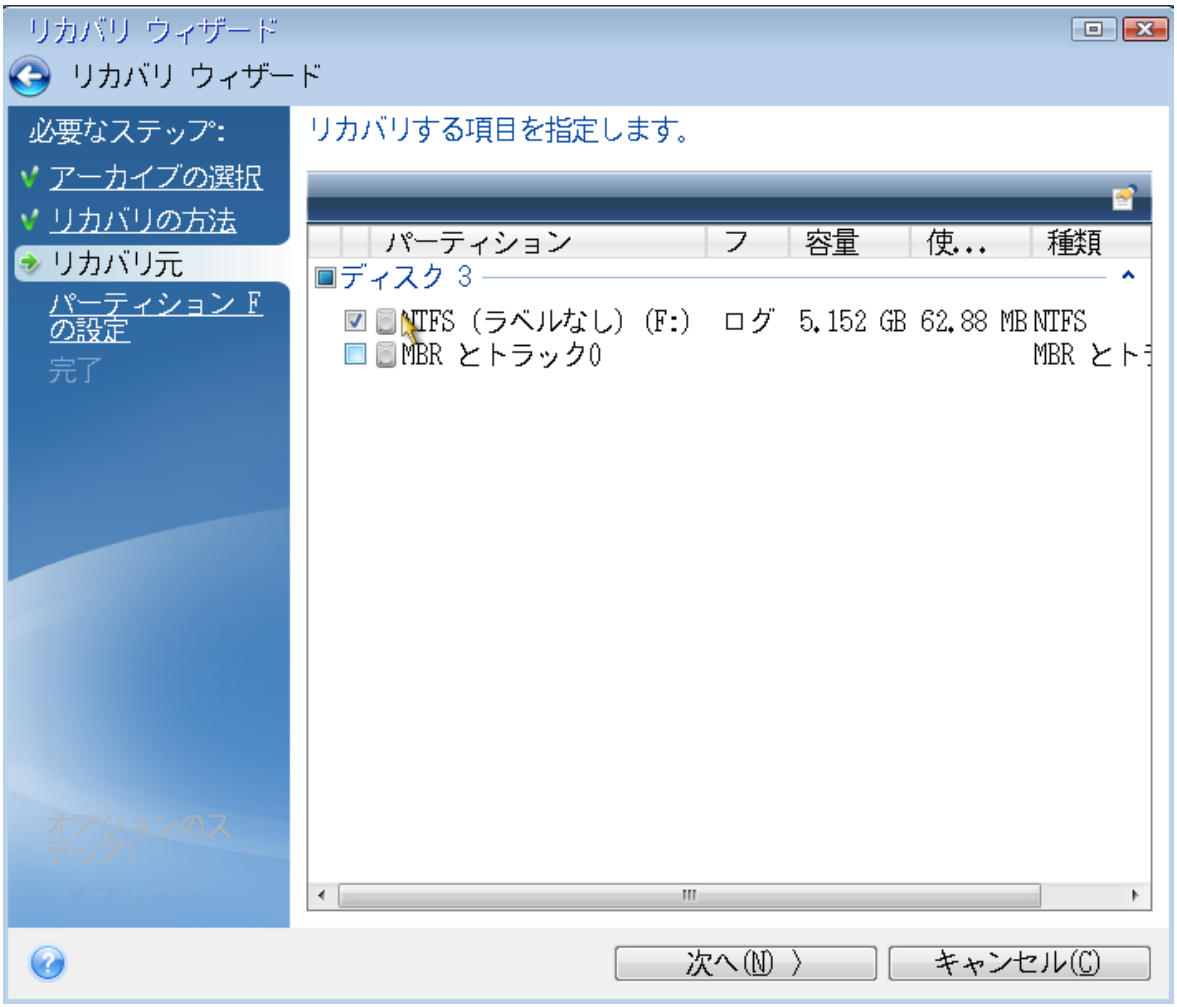
   バックアップが表示されない場合には、**[参照]** をクリックし、バックアップのパスを手動で指定します。

   注意

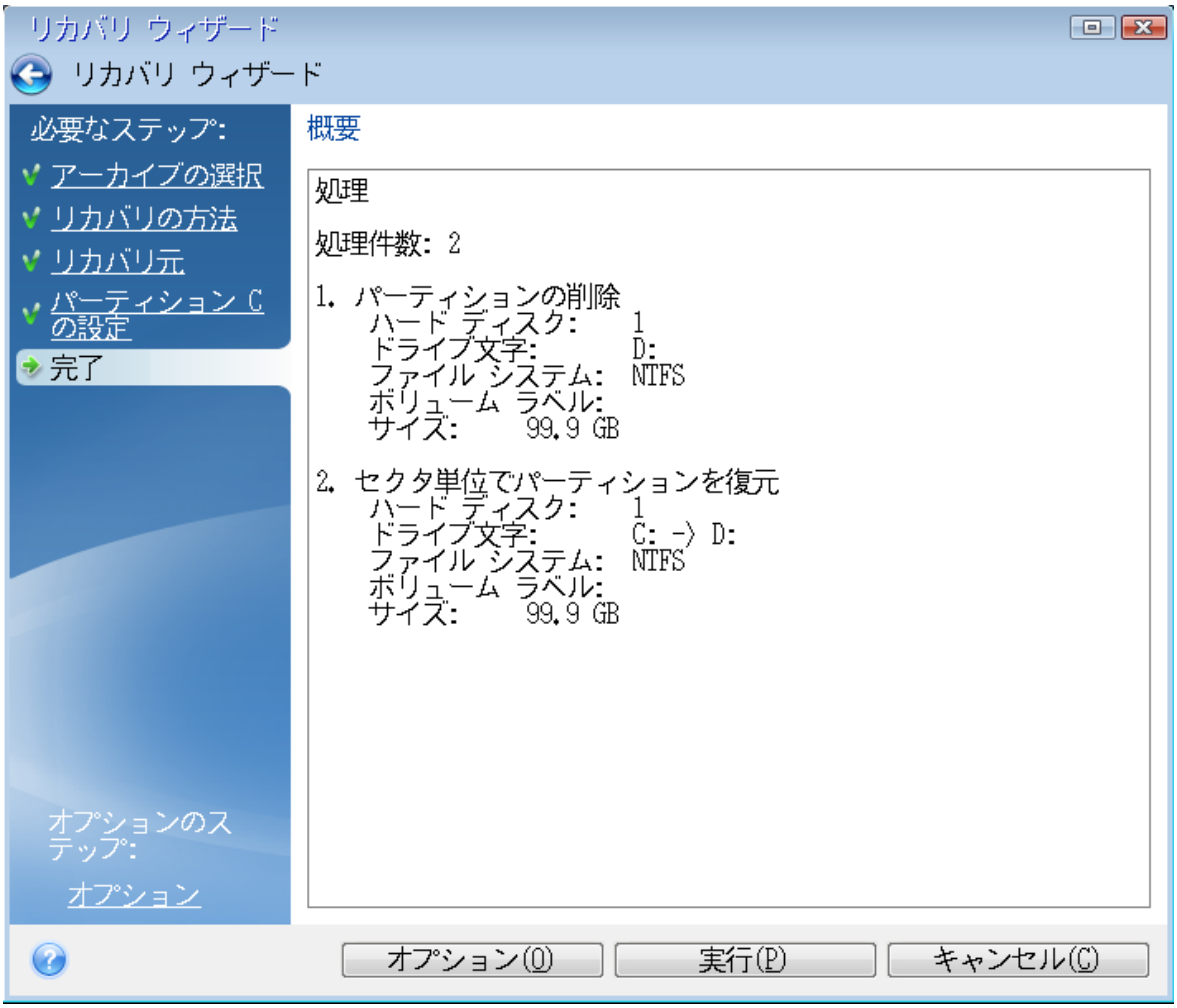
   バックアップがUSBドライブにあり、ドライブが正しく認識されない場合は、USBポートのバージョンを確認してください。バージョンがUSB 3.0またはUSB 3.1の場合は、ドライブをUSB 2.0ポートに接続し直してください。
6. **[リカバリの方法]** ステップで **[ディスクまたはパーティション全体をリカバリする]** を選択します。



7. [オプション] **復元ポイント** ステップで、システムをどの時点の状態に復元するか、日時を選択します。
8. **[リカバリ元]** 画面で、システム パーティション（通常は C）を選択します。システム パーティションの文字が異なる場合は、**[フラグ]** 列を使用してパーティションを選択します。**[プライマリ]** および **[アクティブ]** フラグが設定されている必要があります。システム予約済みパーティションがある場合には、それも選択します。



9. **パーティション C の設定**（または、異なる場合は実際のシステムパーティションの文字）の手順で、デフォルトの設定を確認し、正しい場合は **[次へ]** をクリックします。正しくない場合は、必要に応じて設定を変更した後、**[次へ]** をクリックします。容量が異なる新しいハードディスクにリカバリする場合は設定を変更する必要があります。
10. **[完了]** の画面で処理の概要を確認します。パーティションのサイズを変更していない場合は、**[パーティションの削除]** 項目と **[パーティションのリカバリ]** 項目のサイズが一致している必要があります。概要を確認して、**[実行]** をクリックします。



11. 処理が終了したら、Acronis Cyber Protect Home Office のスタンドアロン版を終了し、Acronis ブータブルメディアを取り出して、リカバリされたシステムパーティションから起動します。必要な状態まで Windows をリカバリしたことを確認してから、元の起動順序を復元します。

ブータブルメディア配下の新しいディスクへのシステムのリカバリ

始める前に、「リカバリの準備」で説明している準備作業の実行をおすすめします。新しいディスクのフォーマットは、リカバリ処理の中で実行されるので、実行する必要はありません。

注意
古いハードディスクドライブと新しいハードディスクドライブは同じコントローラーモード（IDE、AHCI など）で動作させることをお勧めします。モードが異なる場合、新しいハードドライブからコンピュータを起動できなくなる可能性があります。

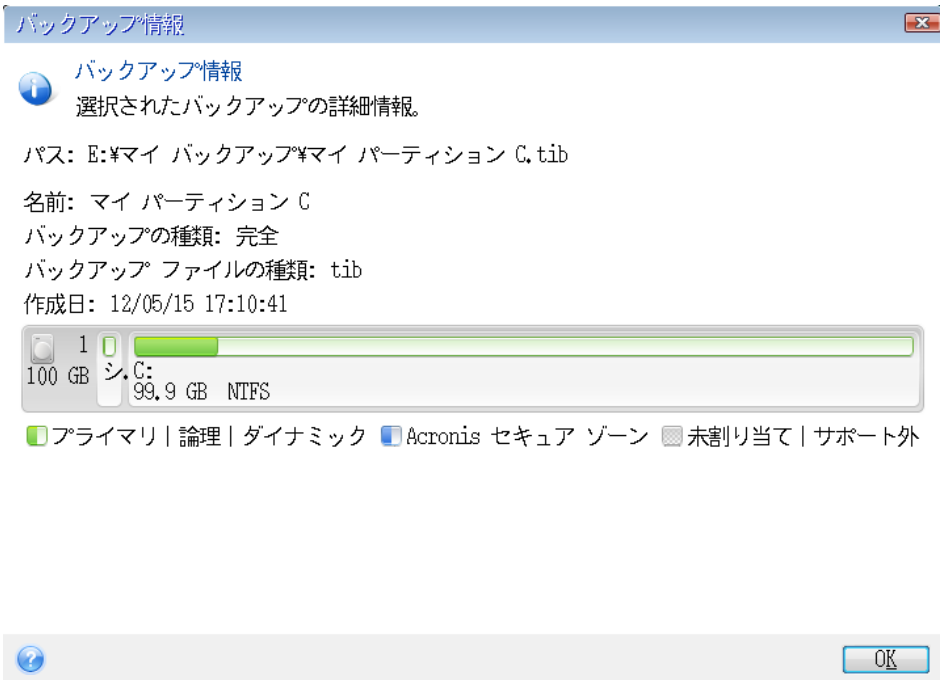
新しいディスクにシステムをリカバリするには、次の手順を実行します。

1. 新しいハードディスクドライブはコンピュータ内の同じ場所に取り付け、元のドライブで使用したものと同じケーブルおよびコネクタを使用します。難しい場合には、新しいドライブを使用する場所に取り付けてください。

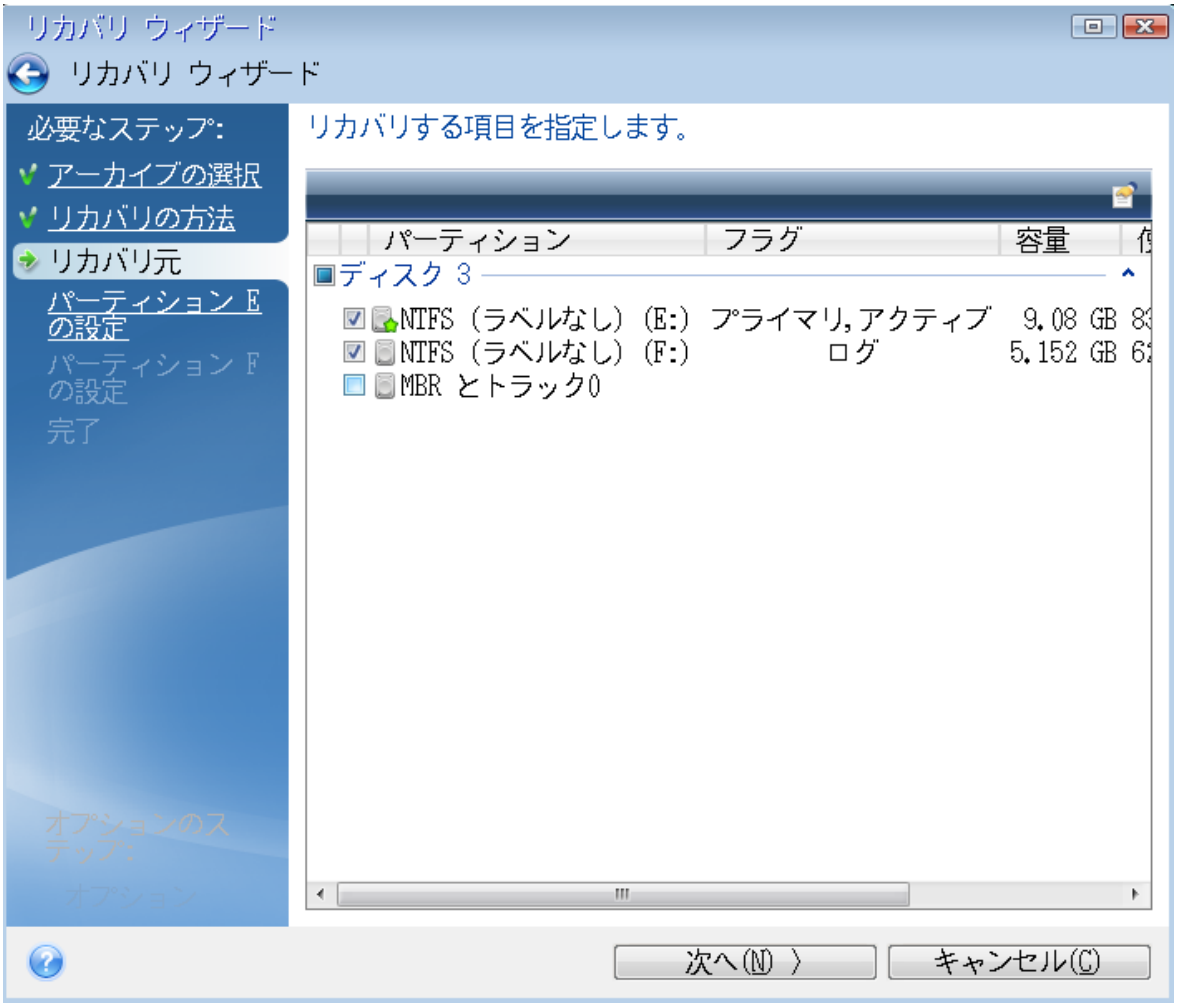
2. リカバリに使用するバックアップが外部ドライブに格納されている場合は、その外部ドライブを接続して電源を入れます。
3. BIOS で起動順序を設定して、ブータブルメディア（CD、DVD、または USB スティック）を最初のブートデバイスにします。「BIOSまたはUEFI BIOSでの起動順の並べ替え」を参照してください。
   UEFI コンピュータを使用する場合、UEFI BIOS のブータブルメディアの起動モードに注意してください。起動モードはバックアップのシステムの種類と一致するようにしてください。バックアップにBIOSシステムが含まれている場合はBIOSモードでブータブルメディアを起動してください。システムがUEFIの場合は、UEFIモードが設定されていることを確認してください。
4. ブータブルメディアから起動して、**[Acronis Cyber Protect Home Office]** を選択します。
5. **[ホーム]** 画面で、**[リカバリ]** の下にある **[マイディスク]** を選択します。
6. リカバリに使用するシステムディスクまたはパーティションバックアップを選択します。バックアップが表示されない場合には、**[参照]** をクリックし、バックアップのパスを手動で指定します。

注意
バックアップがUSBドライブにあり、ドライブが正しく認識されない場合は、USBポートのバージョンを確認してください。バージョンがUSB 3.0またはUSB 3.1の場合は、ドライブをUSB 2.0ポートに接続し直してください。

7. 隠しパーティション（システム予約パーティション、PCの製造元が作成した隠しパーティションなど）がある場合は、ウィザードのツールバーの **[詳細]** をクリックします。隠しパーティションの場所とサイズは新しいディスクで同じにする必要があるため、それらのパラメータを控えておいてください。

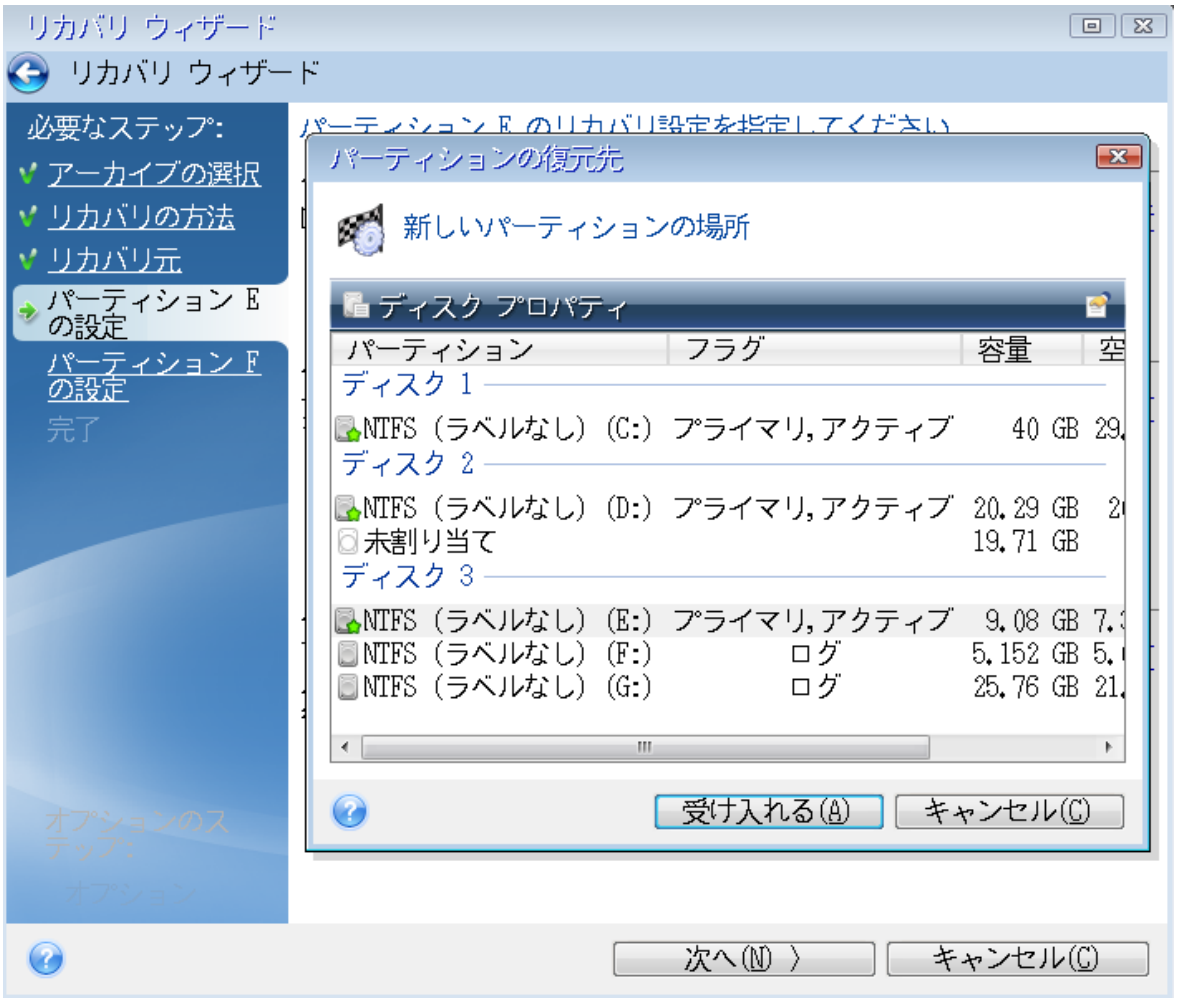


8. **[リカバリの方法]** ステップで **[ディスクまたはパーティション全体をリカバリする]** を選択します。
9. **[リカバリ元]** の手順で、リカバリするパーティションのチェックボックスをオンにします。
   ディスク全体を選択する場合、ディスクの [MBRとトラック 0] も復元されます。

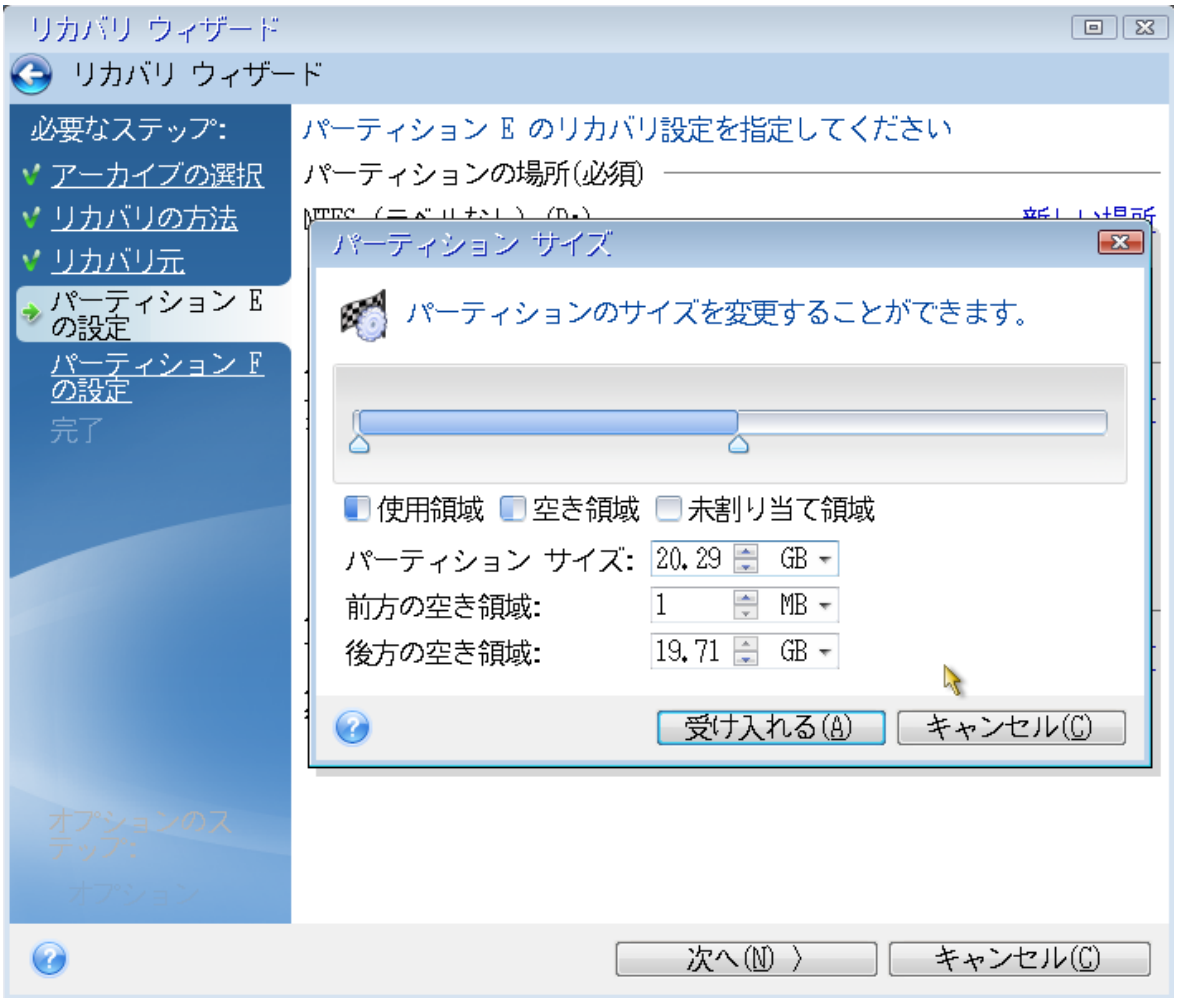


パーティションを選択すると、該当する [**パーティションの設定**] の手順が表示されます。これらの手順は、ドライブ文字のないパーティション（隠しパーティションには通常、ドライブ文字はありません）から開始します。次に、パーティションのドライブ文字の昇順に進みます。この順序は変更できません。この順序は、ハードディスク上のパーティションの物理的順序とは異なる場合があります。

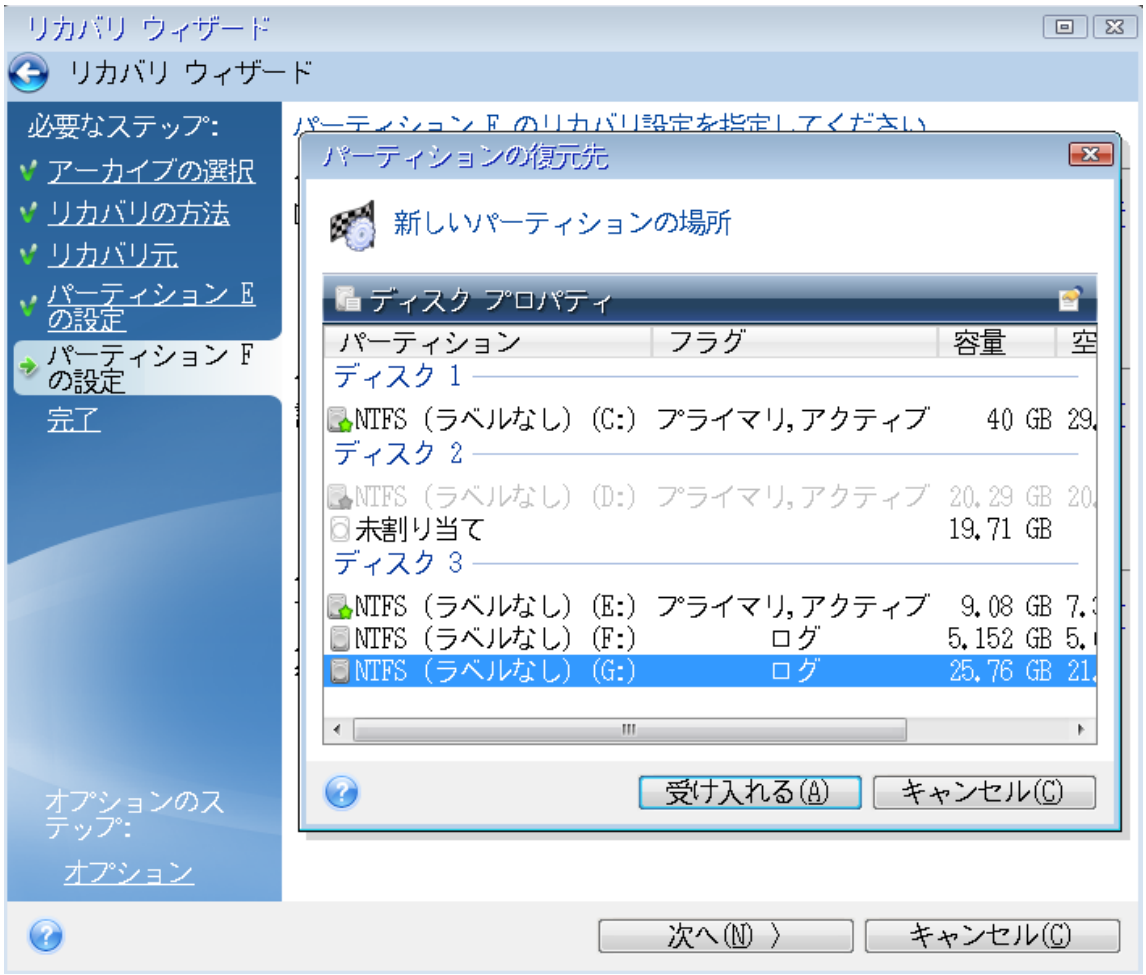
10. 隠しパーティションの設定の手順（通常は「パーティション1-1の設定」という名前）で、次の設定を指定します。
    - **場所** - [**新しい場所**] をクリックし、割り当てられた名前または容量によって新しいディスクを選択し、[**確定**] をクリックします。



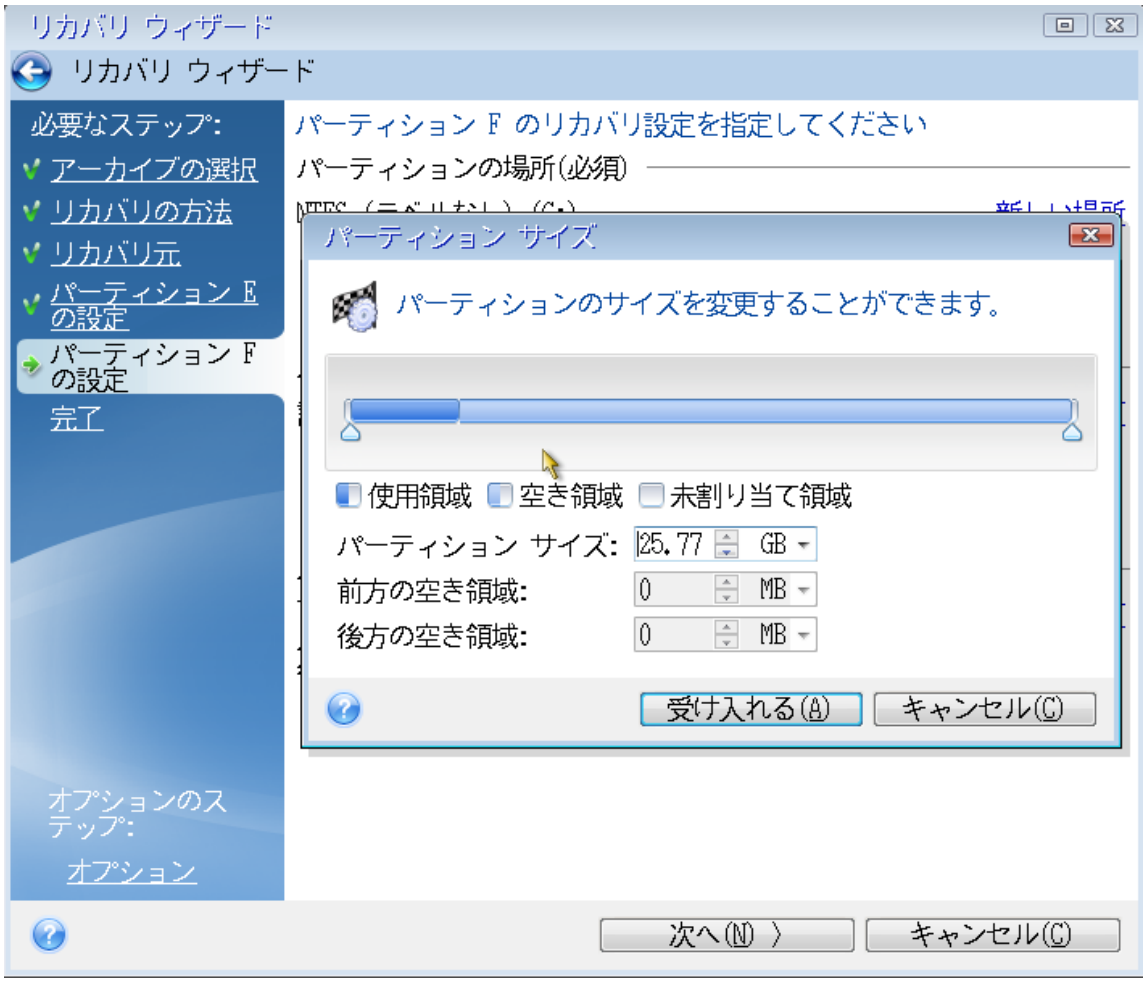
- **種類** - パーティションの種類を確認し、必要に応じて変更します。システム予約済みパーティション（存在する場合）がプライマリパーティションであり、アクティブに設定されていることを確認します。
- **サイズ** - [パーティションサイズ] の領域で **[デフォルトを変更]** をクリックします。デフォルトでは、新しいディスク全体がパーティションに使用されます。[パーティションサイズ] フィールドに正しいサイズを入力します（この値は **[リカバリ元]** の手順で確認できます）。次に、必要に応じて、[バックアップ情報] ウィンドウに表示されていた場所と同じ場所に、このパーティションをドラッグします。**[確定]** をクリックします。



11. [**パーティションCの設定**] の手順で、2番目のパーティションの設定を指定します。このパーティションは、ここではシステムパーティションです。
    - [**新しい場所**] をクリックしてから、パーティションを配置するディスク上の未割り当て領域を選択します。



- パーティションの種類を必要に応じて変更します。システム パーティションは、プライマリにする必要があります。
- パーティションのサイズを指定します。デフォルトでは元のサイズと同じです。通常、このパーティションの後ろには空き領域はないため、新しいディスク上の未割り当て領域のすべてを 2 番目のパーティションに割り当てます。**[確定]** をクリックしてから **[次へ]** をクリックします。



12. 実行する処理の概要を注意深く確認して、**[実行]** をクリックします。

リカバリ完了時

コンピューターを起動する前に、古いドライブがあれば取り外してください。Windowsの起動中に新しいドライブと古いドライブの両方が認識された場合、Windowsの起動に問題が生じます。古いドライブを容量の大きい新しいドライブにアップグレードする場合は、初回起動前に古いドライブを取り外してください。

ブータブルメディアを取り外し、コンピュータで Windows を起動します。新しいハードウェア（ハード ドライブ）が見つかったため Windows を再起動する必要があると表示される場合があります。システムが正常に動作することを確認してから、元の起動順序に戻します。

Acronis Universal Restore

システムを別のハードウェアに復元すると、ターゲットコンピュータが起動できなくなることがあります。これは、新しいハードウェアが、イメージに含まれている重要なドライバと互換性がないからです。Acronis Universal Restore を使用すると、ターゲットコンピューターを起動できるようになります。詳細については、「Acronis Universal Restore」を参照してください。

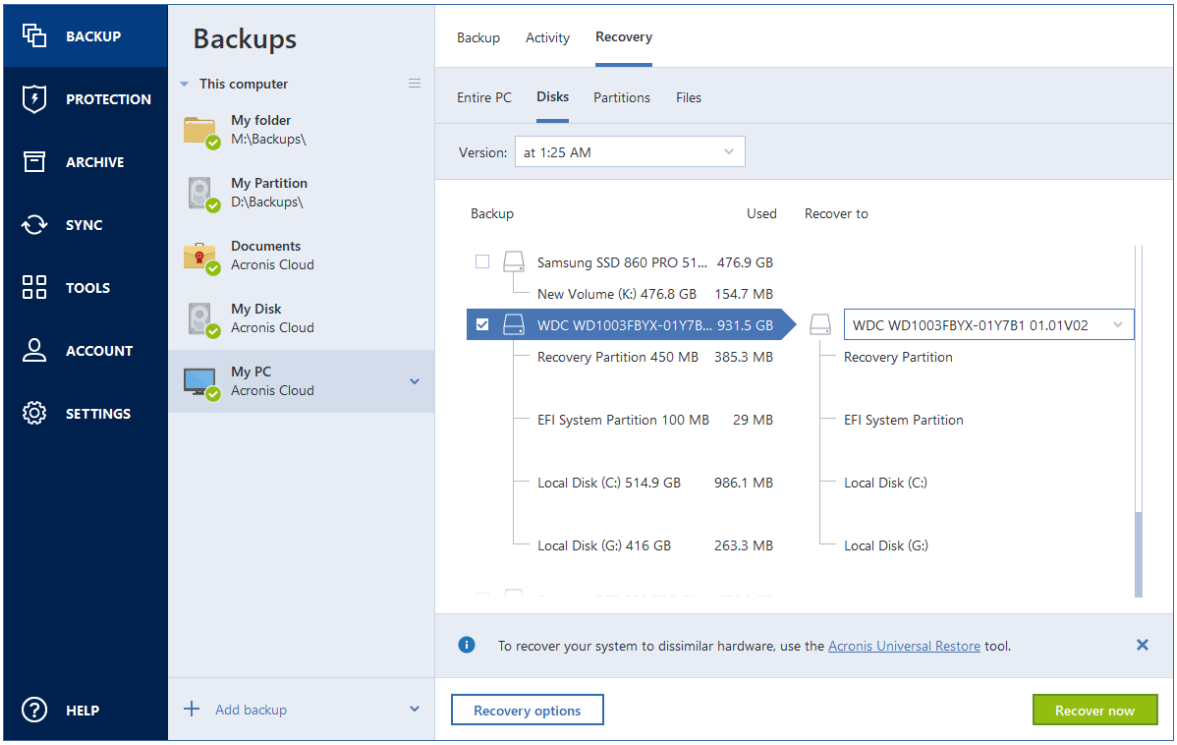
パーティションとディスクのリカバリ

ローカルストレージ、ネットワークストレージ、または Acronis Cloud にあるバックアップからディスクをリカバリすることができます。

注意
インターネット接続の速度によっては、Acronis Cloud からのディスクリカバリに長時間かかることがあります。

パーティションやディスクをリカバリする手順は、次のとおりです。

1. Acronis Cyber Protect Home Office を開始します。
2. Acronis Cloud からデータをリカバリする場合、Acronis アカウントにサインイン済みであることを確認してください。
3. [**バックアップ**] セクションで、リカバリするパーティションまたはディスクが含まれているバックアップを選択し、[**リカバリ**] タブを開き、[**ディスクのリカバリ**] をクリックします。
4. [**バックアップバージョン**] の一覧で、リカバリするバックアップバージョンをバックアップの日付と時刻で選択します。



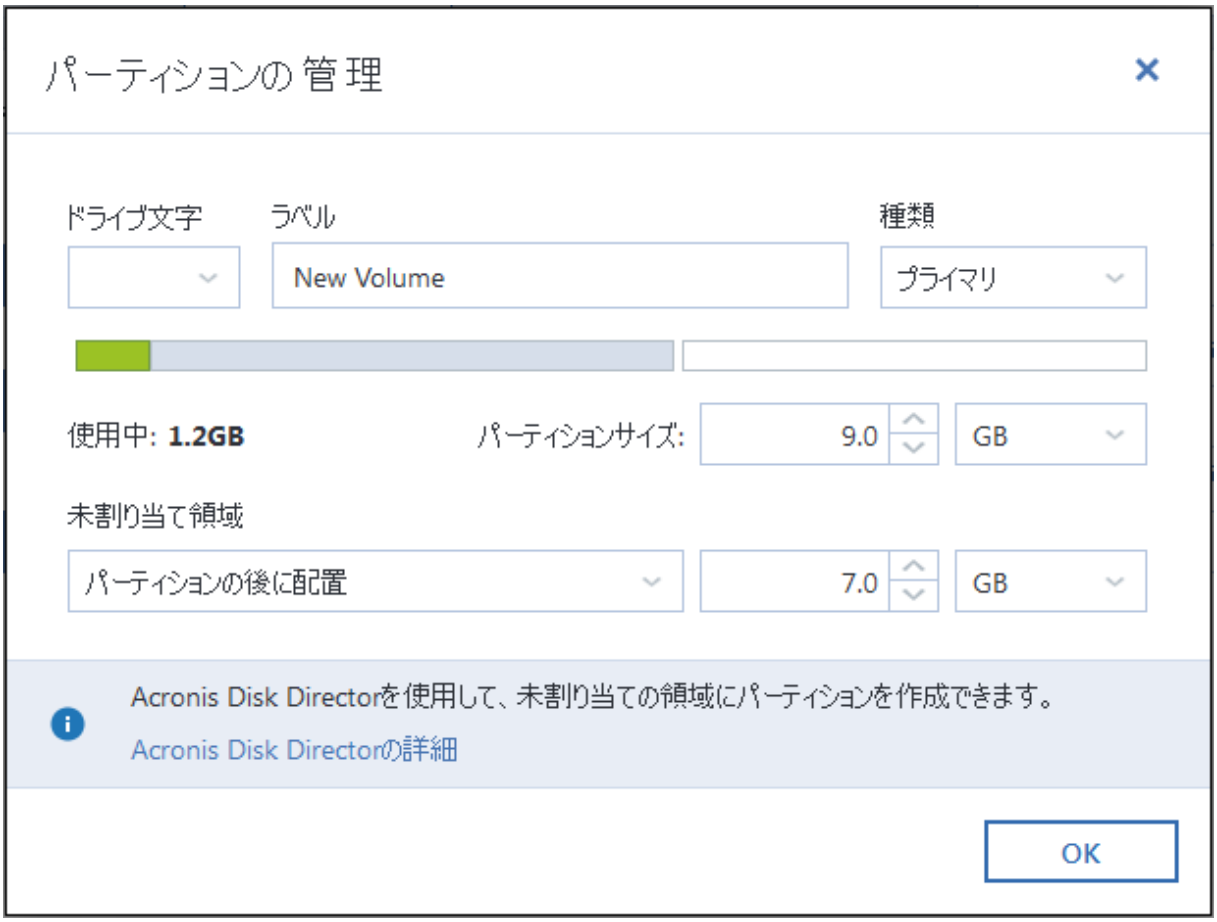
5. ディスクをリカバリするには [**ディスク**] タブを選択し、特定のパーティションをリカバリするには [**パーティション**] タブを選択します。リカバリするオブジェクトを選択します。
6. パーティション名の下にあるリカバリ先のフィールドで、リカバリ先パーティションを選択します。適切でないパーティションは赤い枠線で示されます。リカバリ先のパーティション上のデータは、リカバリされるデータおよびファイルシステムによって置き換えられるため、すべて失われます。

注意
元のパーティションにリカバリする場合、パーティション領域に少なくとも5 %の空き領域が必要です。その領域がない場合、[**今すぐリカバリ**] ボタンは使用できません。

7. （オプション）ディスク リカバリ処理に追加パラメータを設定する場合には、[**復元オプション**] をクリックします。
8. 選択し終わったら、[**今すぐリカバリ**] をクリックしてリカバリを開始します。

パーティションのプロパティ

ベーシックディスクにパーティションを復元するときに、パーティションのプロパティを変更できます。[**パーティションのプロパティ**] ウィンドウを開くには、復元先のパーティションの横にある [**プロパティ**] をクリックします。



以下のパーティションプロパティを変更できます。

- **文字**
- **ラベル**
- **種類**
  パーティションをプライマリ、プライマリアクティブ、論理にすることができます。
- **サイズ**

パーティションのサイズを変更するには、画面の水平バー上でマウスを使用して右の境界をドラッグします。パーティションに特定のサイズを割り当てるには、**[合計サイズ]** フィールドに適切な数字を入力します。未割り当て領域の位置をパーティションの前後で選択することもできます。

統合拡張ファームウェア インターフェイス（UEFI）

Acronis Cyber Protect Home Office では **BIOS** から **UEFI** システムに変換することもできます。

UEFI とは

統合拡張ファームウェア インターフェイス（UEFI）は、起動サービスやランタイム サービスのための標準的な構文を設定することにより、ソフトウェアの相互運用性を向上させる仕様です。UEFI の詳細については、https://www.uefi.org（英語）にアクセスしてください。

次のオペレーティング システムは UEFI テクノロジをサポートしています。

- Windows 8（x86）以降のx86エディションのWindows。
- Windows Vista SP1（x64）以降のx64エディションのWindows。

UEFI を選択する理由

- **BIOS との互換性**: 互換性サポート モジュール（CSM）により、UEFI ベースのシステムは BIOS ベースのオペレーティング システムも起動できます。
- **大容量ディスクからの起動**: UEFI ベースのシステムは、2^32 セクタを超えるディスク サイズに対応できる GPT パーティション レイアウトをサポートしています。
- **CPU に依存しないアーキテクチャ**: UEFI は、どのプロセッサ アーキテクチャでも同様に機能します。
- **CPU に依存しないドライバ**: UEFI 仕様には EFI バイト コード（EBC）が含まれており、あらゆるシステムで実行できる EBC イメージ（ドライバ）を作成できます。
- **柔軟な Pre-OS 環境**: UEFI ベースのシステムはあらゆるハードウェアで起動できます。
- **モジュール式の設計**: UEFI では、他のコンポーネントに影響を与えることなく、1 つのコンポーネントをアップデートできます。

注意
UEFI は新しいテクノロジであるため、すべてのシステムでサポートされているわけではありません。お使いのコンピュータが UEFI をサポートしているかについては、各ハードウェア メーカーまでお問い合わせください。

BIOS で UEFI を有効にする方法

以下に、BIOS で UEFI を有効/無効にする一般的な方法を示します。

1. 起動中に、画面上のメッセージに表示されたキーを押して、BIOS 設定プログラムを起動します。通常は Del キーまたは F2 キーです。
2. 矢印キーを使用して **[起動オプション]** メニューを起動します。
3. **[UEFI 起動]** 項目で [有効]（ご使用のシステムで UEFI を**オフ**にする場合は [無効]）を選択します。
4. **[設定を保存して終了]** に移動して、**Enter** キーを押し、変更を保存して、システムを起動します。

UEFI を有効にする方法についてサポートが必要な場合は、ハードウェア製造元にお問い合わせください。

元のシステムをより容量の大きいハード ドライブに移行する方法

Acronis Cyber Protect Home Office では、以前作成したアーカイブから、2^32 バイト（通常の 512 バイトの論理セクタのディスクの場合は 2 TB、4 KB（4096 バイト）の論理セクタのディスクの場合は 16 TB）を超えるハードディスクドライブにシステムを移行または復元できるようになりました。

これを実行するには、Acronis メディアを使用するか、Acronis Cyber Protect Home Office がインストールされた UEFI ベースのオペレーティングシステムで起動します。

Acronis メディアを使用してシステムを移行する手順は、次のとおりです。

1. Acronis メディアからシステムを起動します。
2. ブートメニューで **Acronis Cyber Protect Home Office（製品版）**を選択してメディアからの起動を継続します。
3. 該当するウィザード（**復元**または**クローン作成**）を起動して、指示に従います。

UEFI ベースのオペレーティングシステムでシステムを移行する手順は、次のとおりです。

1. UEFI 対応の Windows オペレーティング システムを起動します。
2. Acronis Cyber Protect Home Office を実行して、**[バックアップとリカバリ]** タブを選択し、ツールバーの **[リカバリ]** をクリックして、指示に従います。

パーティション レイアウト

パーティション レイアウトによって、オペレーティング システムがハード ドライブ上のパーティションを整理する方法が決まります。

- **MBR（マスターブートレコード）**: 512バイトのブートセクタで、ハードディスクの第1セクタです。ディスクのプライマリパーティションテーブルを格納するために使用されます。
  MBR は標準的なパーティション スキームです。ほとんどのハード ドライブで使用されています。MBR の主な制約としては、ハード ディスクのサイズを最大 2 TB までしかサポートしていないことが挙げられます。そのため、大容量ハード ドライブを使用しても 2 TB を超える領域を使用できません。
- **GPT（GUID パーティション テーブル）**: MBR よりも新しい、標準的なハード ディスク用パーティション テーブル レイアウト。
  GPT では最大 9.4 ZB（9.4 x 10^21 バイト）までのディスク/パーティション サイズが可能です。
  次の表は、GPT ディスクの読み取りや GPT ディスクからの起動を、どのオペレーティング システムがサポートしているかを示しています。

	GPT ディスクを読み取り可能	GPT ディスクから起動可能
Windows XP x32	×	×
Windows XP x64	○	×

Windows Vista x32	○	×
Windows Vista x64	○	×
Windows Vista x64 SP1 以降	○	○
Windows 7 x32	○	×
Windows 7 x64	○	○
Windows 8 x32	○	○
Windows 8 x64	○	○
Windows 8.1 x32	○	○
Windows 8.1 x64	○	○
Windows 10 x32	○	○
Windows 10 x64	○	○
Windows 11	○	○

表1: ターゲットディスクが2 TBを超えている

下の表は、ソースディスクを大容量ハードディスク（2 TBを超えるもの）に移行する場合に使用可能なオプションを示しています。

ソースディスクが MBR の場合、ターゲットディスクを MBR のままにするか、Acronis Cyber Protect Home Office を使用して GPT に変換するかを選択する必要があります。

各オプションの長所と短所は、お使いのシステムのパラメータによって異なります。多くは、ターゲットディスクのブータビリティと大容量ディスクの領域全体を使用できるかどうかに関係しています。

	システムは BIOS 起動である（Windows または Acronis ブータブルメディア）	**システムは UEFI 起動である（Windows または Acronis ブータブルメディア）**
ソースディスクは MBR であり、OS は UEFI をサポートしていない	クローン作成後、パーティションスタイルはMBRのままとなります。クローン作成したオペレーティングシステムにAcronis Busドライバがインストールされます。また、MBRは2 TBを超えるハードドライブをサポートしていないため、2 TBを超えるディスク領域は使用できません。すべてのディスク領域を使用するには、パーティションスタイルを GPT に変更するか、または処理完了後に Acronis Cyber Protect Home Office を再起動し、Acronis Extended Capacity Manager を使用して、2 TB を超えるディスク領域を新しいディスクの追加ツールで認識できるようにする必要があり	次のいずれかの移行方法を選択できます。 • **ソースパーティションを変更せずにコピーする** パーティションスタイルはMBRのままとなりますが、処理が完了すると、オペレーティングシステムはUEFI起動されません。クローン作成したオペレーティングシステムにAcronis Busドライバがインストールされます。また、MBRは2 TBを超えるハードドライブをサポートしていないため、2 TBを超えるディスク領域は使用できません。すべてのディスク領域を使用するには、パーティションスタイルを GPT に変更するか、または処理完了後に Acronis Cyber Protect

	ます。	Home Office を再起動し、Acronis Extended Capacity Manager を使用して、2 TB を超えるディスク領域を新しいディスクの追加ツールで認識できるようにする必要があります。 • **パーティションスタイルをGPTに変換する** ターゲットのパーティションがGPTスタイルに変換されます。お使いのオペレーティングシステムはUEFIをサポートしていないため、システムディスクではないディスクとして使用できます。すべてのディスク領域を使用できます。
ソースディスクはMBRであり、OSはUEFIをサポートしている	パーティションスタイルは移行後もMBRのままとなります。クローン作成したオペレーティングシステムにAcronis Busドライバがインストールされます。MBRは2 TBを超えるハードドライブをサポートしていないため、2 TBを超えるディスク領域は使用できません。すべてのディスク領域を使用するには、パーティションスタイルを GPT に変更するか、または処理完了後に Acronis Cyber Protect Home Office を再起動し、Acronis Extended Capacity Manager を使用して、2 TB を超えるディスク領域を新しいディスクの追加ツールで認識できるようにする必要があります。	ターゲットディスクのパーティションスタイルは自動的にGPTに変換されます。このディスクは、UEFI起動用として使用できます。また、すべてのディスク領域を使用できます。
ソースディスクはMBRであり、OSはWindows以外またはOSがない	次のいずれかの移行方法を選択できます。 • **ソースパーティションを変更せずにコピーする** パーティションスタイルはMBRのままとなります。MBRは2 TBを超えるハードドライブをサポートしていないため、2 TBを超えるディスク領域は使用できません。すべてのディスク領域を使用するには、パーティションスタイルを GPT に変更するか、または処理完了後に Acronis Cyber Protect Home Office を再起動し、Acronis Extended Capacity Manager を使用して、2 TB を超えるディスク領域を新しいディスクの追加ツールで認識できるようにする必要があります。 • **パーティションスタイルをGPTに変換する** 処理完了後、パーティションスタイルはGPTに変換されます。ソースディスクに	次のいずれかの移行方法を選択できます。 • **ソースパーティションを変更せずにコピーする** パーティションスタイルはMBRのままとなります。MBRは2 TBを超えるハードドライブをサポートしていないため、2 TBを超えるディスク領域は使用できません。すべてのディスク領域を使用するには、パーティションスタイルを GPT に変更するか、または処理完了後に Acronis Cyber Protect Home Office を再起動し、Acronis Extended Capacity Manager を使用して、2 TB を超えるディスク領域を新しいディスクの追加ツールで認識できるようにする必要があります。 • **パーティションスタイルをGPTに変換する** ターゲットのパーティションがGPTスタイルに変換されます。ソースディスクにWindows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ため、ターゲットディスクを起動用として

	Windows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ため、ターゲットディスクを起動用として使用できません。すべてのディスク領域を使用できます。	使用できません。また、すべてのディスク領域を使用できます。
ソースディスクはGPTであり、OSはUEFIをサポートしている	パーティションスタイルは移行後もGPTのままとなります。お使いのオペレーティングシステムはGPTからのBIOS起動をサポートしていないため、処理完了後、システムはBIOSから起動できなくなります。すべてのディスク領域を使用できます。	この処理は、パーティションレイアウトにもディスクのブータビリティにも影響しません。パーティションスタイルはGPTのままとなり、ターゲットディスクはUEFI起動が可能となります。すべてのディスク領域を使用できます。
ソースディスクはGPTであり、OSはWindows以外またはOSがない	この処理は、パーティションレイアウトにもディスクのブータビリティにも影響しません。パーティションスタイルはGPTのままとなり、ターゲットディスクは起動できません。すべてのディスク領域を使用できます。	この処理は、パーティションレイアウトにもディスクのブータビリティにも影響しません。パーティションスタイルはGPTのままとなり、ターゲットディスクはUEFI起動できません。すべてのディスク領域を使用できます。

表2: ターゲットディスクが2 TB未満

下の表は、ソースディスクを2 TB未満のハードディスクに移行する場合に使用可能なオプションを示しています。

ソースディスクが MBR の場合、ターゲットディスクを MBR のままにするか、Acronis Cyber Protect Home Office を使用して GPT に変換するかを選択する必要があります。

各オプションの長所と短所は、お使いのシステムのパラメータによって異なります。多くは、ターゲットディスクのブータビリティに関係しています。

	システムは BIOS 起動である（Windows または Acronis ブータブルメディア）	**システムは UEFI 起動である（Windows または Acronis ブータブルメディア）**
ソースディスクは MBR であり、OS は UEFI をサポートしていない	この処理は、パーティションレイアウトにもディスクのブータビリティにも影響しません。パーティションスタイルはMBRのままとなり、ターゲットディスクはBIOS起動が可能となります。すべてのディスク領域を使用できます。	処理完了後、パーティションスタイルはMBRのままとなります。お使いのオペレーティングシステムではサポートされていないため、UEFI起動はできません。
ソースディスクはMBRであり、OSはUEFIをサポートしている	この処理は、パーティションレイアウトにもディスクのブータビリティにも影響しません。パーティションスタイルはMBRのままとなり、ターゲットディスクはBIOS起動が可能となります。すべてのディスク領域を使用できます。	ターゲットのパーティションがGPTスタイルに変換され、ターゲットディスクのUEFI起動が可能になります。すべてのディスク領域を使用できます。
ソースディスクはMBR	次のいずれかの移行方法を選択できます。 • **ソースパーティションを変更せずにコピーす**	次のいずれかの移行方法を選択できます。 • **ソースパーティションを変更せずにコ**

であり、OSはWindows以外またはOSがない	**る** パーティションスタイルはMBRのままとなります。システムにWindowsオペレーティングシステムが搭載されていないため、ターゲットディスクは起動できません。 • **パーティションスタイルをGPTに変換する** お使いのオペレーティングシステムはGPTからのBIOS起動をサポートしていないため、ターゲットディスクはGPTスタイルに変換され、システムディスクではないディスクとして使用されます。	**ピーする** パーティションスタイルはMBRのままとなります。システムにWindowsオペレーティングシステムが搭載されていないため、ターゲットディスクは起動できません。 • **パーティションスタイルをGPTに変換する** お使いのシステムにWindowsオペレーティングシステムが搭載されていないため、ターゲットのパーティションはGPTスタイルに変換され、システムディスクではないディスクとして使用されます。
ソースディスクはGPTであり、OSはUEFIをサポートしている	処理完了後、パーティションスタイルはGPTのままとなります。お使いのオペレーティングシステムはGPTからのBIOS起動をサポートしていないため、システムはBIOSから起動できなくなります。	処理完了後、パーティションスタイルはGPTのままとなり、オペレーティングシステムはUEFI起動が可能となります。
ソースディスクはGPTであり、OSはWindows以外またはOSがない	処理完了後、パーティションスタイルはGPTのままとなります。お使いのオペレーティングシステムはGPTからのBIOS起動をサポートしていないため、システムはBIOSから起動できなくなります。	処理完了後、パーティションスタイルはGPTのままとなります。お使いのシステムにはWindowsオペレーティングシステムが搭載されていないため、システムは起動できません。

移行方法

Acronis Cyber Protect Home Office では、リカバリ処理完了後にターゲットディスクのパーティションレイアウトを選択できます。

- **MBR（マスター ブート セクタ）**: ディスクのプライマリ パーティション テーブルを格納するための 512 バイトのブート セクタ。ディスクの第 1 セクタです。
- **GPT（GUIDパーティションテーブル）**: 標準的なハードディスク用パーティションテーブルレイアウト。GPT では最大 9.4 ZB（9.4 x 10^21 バイト）までのディスク/パーティション サイズが可能です。

このウィザードを使用すると、リカバリ中にパーティションレイアウトを変換することも、レイアウトを変更せずに、そのまま復元することもできます。

- **[変更せずにパーティションをコピー]**: このオプションを選択すると、パーティションレイアウトを変更せずに、そのままシステムを移行できます。この場合、2 TBを超えるディスク領域は使用できません。2 TB を超えるディスク領域を割り当てるには、Acronis Extended Capacity Manager を使用してください。

- **[パーティションをコピーし、システム用ではないGPTスタイルでディスクを使用する]**: このオプションを選択すると、パーティションをGPTレイアウトに変換できます。

Acronis Cyber Protect Home Office では **BIOS** から **UEFI** システムに変換することもできます。

BIOSモードシステム、MBR、UEFIのサポートなし

このウィザードのステップでは、ターゲットハードディスクを選択する必要があります。

現在のシステム:

システム: BIOSモード

ソースパーティションスタイル: MBR

ソースディスクのオペレーティングシステム: Windows、UEFI起動のサポートなし

ターゲットディスクサイズ: 2 TB未満

選択したディスクにシステムを移行した場合:

システム: BIOSモード

パーティションスタイル: MBR

オペレーティングシステム: Windows、UEFI起動のサポートなし

ディスクサイズ: すべてのディスク領域が使用可能

移行手順の詳細については、「移行方法」セクションを参照してください。

BIOSモードシステム、MBR、UEFIのサポート

このウィザードのステップでは、ターゲットハードディスクを選択する必要があります。

現在のシステム:

システム: BIOSモード

ソースパーティションスタイル: MBR

ソースディスクのオペレーティングシステム: Windows、UEFI起動をサポート

ターゲットディスクサイズ: 2 TB未満

選択したディスクにシステムを移行した場合:

システム: BIOSモード

パーティションスタイル: MBR

オペレーティングシステム: Windows、UEFI起動をサポート

ディスクサイズ: すべてのディスク領域が使用可能

移行手順の詳細については、「移行方法」セクションを参照してください。

BIOSモードシステム、MBR、Windowsなし

Acronis Cyber Protect Home Office では、処理完了後にターゲットディスクのパーティションレイアウ

トを選択できます。

現在のシステム:

システム: BIOSモード

ソースパーティションスタイル: MBR

ソースディスクのオペレーティングシステム: Windows以外またはOSなし

ターゲットディスクサイズ: 2 TB未満

これらのシステムパラメータでは、次のいずれかを選択できます。

1. **変更せずにパーティションをコピー**

ターゲットディスクのパーティションスタイルをMBRのままにします。

移行後のターゲットディスク:

システム: BIOSモード

パーティションスタイル: MBR

オペレーティングシステム: Windows以外またはOSなし

ディスクサイズ: すべてのディスク領域が使用可能

2. **パーティションをコピーし、システム用ではないGPTスタイルでディスクを使用する**

パーティションスタイルをGPTに変換できます。

移行後のターゲットディスク:

システム: BIOS起動非対応

パーティションスタイル: GPT

オペレーティングシステム: Windows以外またはOSなし

ディスクサイズ: すべてのディスク領域が使用可能

警告
移行後、ターゲットディスクはシステム用ではないディスクとしてのみ使用できます。Acronis Cyber Protect Home Office が Windows XP x32 オペレーティングシステムで実行されている場合は、このオプションを選択できません。

移行手順の詳細については、「移行方法」セクションを参照してください。

BIOSモードシステム、GPT、UEFIサポート

このウィザードのステップでは、ターゲットハードディスクを選択する必要があります。

現在のシステム:

システム: BIOSモード

ソースパーティションスタイル: GPT

ソースディスクのオペレーティングシステム: Windows、UEFI起動をサポート

選択したディスクにシステムを移行した場合:

システム: BIOS起動非対応

パーティションスタイル: GPT

オペレーティングシステム: Windows、UEFI起動をサポート

ディスクサイズ: すべてのディスク領域が使用可能

警告
移行した後は、オペレーティングシステムはターゲットハードディスクの BIOS から起動できません。移行後にターゲットディスクから起動するには、システムで UEFI 起動を有効にし（「Unified Extensible Firmware Interface」セクションを参照）、処理を再度開始してください。

移行手順の詳細については、「移行方法」セクションを参照してください。

BIOSモードシステム、GPT、Windowsなし

このウィザードのステップでは、ターゲットハードディスクを選択する必要があります。

現在のシステム:

システム: BIOSモード

ソースパーティションスタイル: GPT

ソースディスクのオペレーティングシステム: Windows以外またはOSなし

選択したディスクにシステムを移行した場合:

システム: BIOSモード

パーティションスタイル: GPT

オペレーティングシステム: Windows以外またはOSなし

ディスクサイズ: すべてのディスク領域が使用可能

移行手順の詳細については、「移行方法」セクションを参照してください。

UEFIモードシステム、MBR、UEFIのサポートなし

このウィザードのステップでは、ターゲットハードディスクを選択する必要があります。

現在のシステム:

システム: UEFIモード

ソースパーティションスタイル: MBR

ソースディスクのオペレーティングシステム: Windows、UEFI起動のサポートなし

ターゲットディスクサイズ: 2 TB未満

選択したディスクにシステムを移行した場合:

システム: UEFI起動非対応

パーティションスタイル: MBR

オペレーティングシステム: Windows、UEFI起動のサポートなし

ディスクサイズ: すべてのディスク領域が使用可能

警告
オペレーティングシステムはターゲットディスクから UEFI で起動できない場合があります。

移行手順の詳細については、「移行方法」セクションを参照してください。

サポートされるUEFIモードシステム、MBR、UEFI

このウィザードのステップでは、ターゲットハードディスクを選択する必要があります。

現在のシステム:

システム: UEFIモード

ソースパーティションスタイル: MBR

ソースディスクのオペレーティングシステム: Windows、UEFI起動をサポート

選択したディスクにシステムを移行した場合:

移行後、ターゲットディスクのパーティションスタイルはGPTに変換され、ターゲットディスクから起動できるようになります。

移行後のターゲットディスク:

システム: UEFIモード

パーティションスタイル: GPT

オペレーティングシステム: Windows、UEFI起動をサポート

ディスクサイズ: すべてのディスク領域が使用可能

移行手順の詳細については、「移行方法」セクションを参照してください。

UEFIモードシステム、MBR、Windowsなし

Acronis Cyber Protect Home Office では、処理完了後にターゲットディスクのパーティションレイアウトを選択できます。

現在のシステム:

システム: UEFIモード

ソースパーティションスタイル: MBR

ソースディスクのオペレーティングシステム: Windows以外またはOSなし

ターゲットディスクサイズ: 2 TB未満

これらのシステムパラメータでは、次のいずれかを選択できます。

1. **変更せずにパーティションをコピー**

ターゲットディスクのパーティションスタイルをMBRのままにします。

移行後のターゲットディスク:

システム: UEFIモード

パーティションスタイル: MBR

オペレーティングシステム: Windows以外またはOSなし

ディスクサイズ: すべてのディスク領域が使用可能

2. **パーティションをコピーし、システム用ではないGPTスタイルでディスクを使用する**

パーティションスタイルをGPTに変換できます。

移行後のターゲットディスク:

システム: UEFI起動非対応

パーティションスタイル: GPT

オペレーティングシステム: Windows以外またはOSなし

ディスクサイズ: すべてのディスク領域が使用可能

警告
移行後、ターゲットディスクはシステム用ではないディスクとしてのみ使用できます。

移行手順の詳細については、「移行方法」セクションを参照してください。

UEFIモードシステム、GPT、UEFIのサポート

このウィザードのステップでは、ターゲットハードディスクを選択する必要があります。

現在のシステム:

システム: UEFIモード

ソースパーティションスタイル: GPT

オペレーティングシステム: Windows、UEFI 起動をサポート

選択したディスクにシステムを移行した場合:

システム: UEFIモード

パーティションスタイル: GPT

ディスクサイズ: すべてのディスク領域が使用可能

移行手順の詳細については、「移行方法」セクションを参照してください。

UEFIモードシステム、GPT、Windowsなし

このウィザードのステップでは、ターゲットハードディスクを選択する必要があります。

現在のシステム:

システム: UEFIモード

ソースパーティションスタイル: GPT

オペレーティングシステム: Windows以外またはOSなし

選択したディスクにシステムを移行した場合:

システム: UEFIモード

パーティションスタイル: GPT

ディスクサイズ: すべてのディスク領域が使用可能

移行手順の詳細については、「移行方法」セクションを参照してください。

ダイナミック/GPTディスクおよびボリュームの復元について

ダイナミックボリュームの復元

ローカルハードドライブの次のロケーションへダイナミックボリュームを復元することができます。

- **ダイナミックボリューム**

  注意
  ダイナミックディスクに復元する際に、手動でダイナミックボリュームのサイズを変更することはサポートされていません。リカバリ中にダイナミックボリュームのサイズを変更する必要がある場合は、ベーシックディスクに復元する必要があります。

  - **元の場所（同じダイナミックボリュームへ）**
    ターゲットボリュームの種類は変更されません。
  - **別のダイナミックディスクまたはボリューム**
    ターゲットボリュームの種類は変更されません。たとえば、ダイナミックストライプボリュームをダイナミックスパンボリュームに復元すると、ターゲットボリュームはスパンのままです。
  - **ダイナミックグループの未割り当て領域**
    リカバリしたボリュームの種類は、バックアップでの種類と同じになります。
- **ベーシックボリュームまたはディスク**
  ターゲットボリュームはベーシックのままです。
- **ベアメタルリカバリ**
  ダイナミックボリュームを新しい未フォーマットディスクに「ベアメタルリカバリ」を行うと、復元されたボリュームはベーシックになります。復元されたボリュームをダイナミックのままにしておきたい場合は、ターゲットディスクをダイナミックとして準備（パーティションが設定され、フォー

マットされている）する必要があります。これは、Windows ディスク管理スナップインなどの、サードパーティのツールを使用して行うことができます。

ベーシックボリュームおよびディスクの復元

- ベーシックボリュームをダイナミックグループの未割り当て領域に復元すると、復元されたボリュームはダイナミックになります。
- ベーシックディスクを2つのディスクから構成されるダイナミックグループのダイナミックディスクに復元すると、復元されたディスクはベーシックのままです。リカバリの実行先のダイナミックディスクは「見つからない」状態となり、2つ目のディスク上のスパン/ストライプダイナミックボリュームは「エラー」になります。

リカバリ後のパーティションのスタイル

ターゲットディスクのパーティションのスタイルは、ご使用のコンピュータがUEFIをサポートしているかどうか、およびシステムがBIOS起動であるか、UEFI起動であるかどうかによって異なります。以下の表を参照してください。

	システムは BIOS 起動である（Windows または Acronis ブータブルメディア）	**システムは UEFI 起動である（Windows または Acronis ブータブルメディア）**
ソースディスクは MBR であり、OS は UEFI をサポートしていない	この処理は、パーティションレイアウトにもディスクのブータビリティにも影響しません。パーティションスタイルはMBRのままとなり、ターゲットディスクはBIOS起動が可能となります。	処理完了後、パーティションスタイルはGPTに変換されます。お使いのオペレーティングシステムではサポートされていないため、UEFI起動はできません。
ソースディスクはMBRであり、OSはUEFIをサポートしている	この処理は、パーティションレイアウトにもディスクのブータビリティにも影響しません。パーティションスタイルはMBRのままとなり、ターゲットディスクはBIOS起動が可能となります。	ターゲットのパーティションがGPTスタイルに変換され、ターゲットディスクのUEFI起動が可能になります。「UEFIシステムへの復元の例」を参照してください。
ソースディスクはGPTであり、OSはUEFIをサポートしている	処理完了後、パーティションスタイルはGPTのままとなります。お使いのオペレーティングシステムはGPTからのBIOS起動をサポートしていないため、システムはBIOSから起動できなくなります。	処理完了後、パーティションスタイルはGPTのままとなり、オペレーティングシステムはUEFI起動が可能となります。

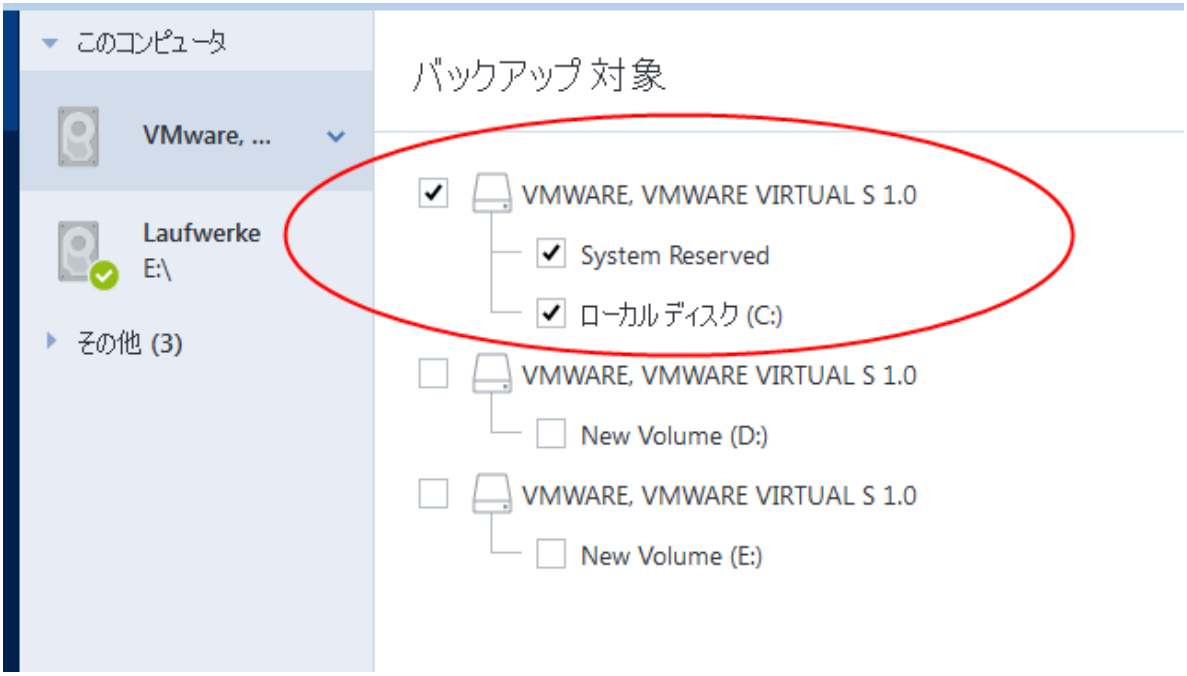
UEFIシステムへの復元の例

次に、以下の条件でシステムを転送する例を挙げます。

- ソースディスクはMBRであり、OSはUEFIをサポートしている。
- ターゲットシステムはUEFI起動である。
- 古いハードディスクドライブと新しいハードディスクドライブは同じコントローラモード（IDE、AHCIなど）で動作する。

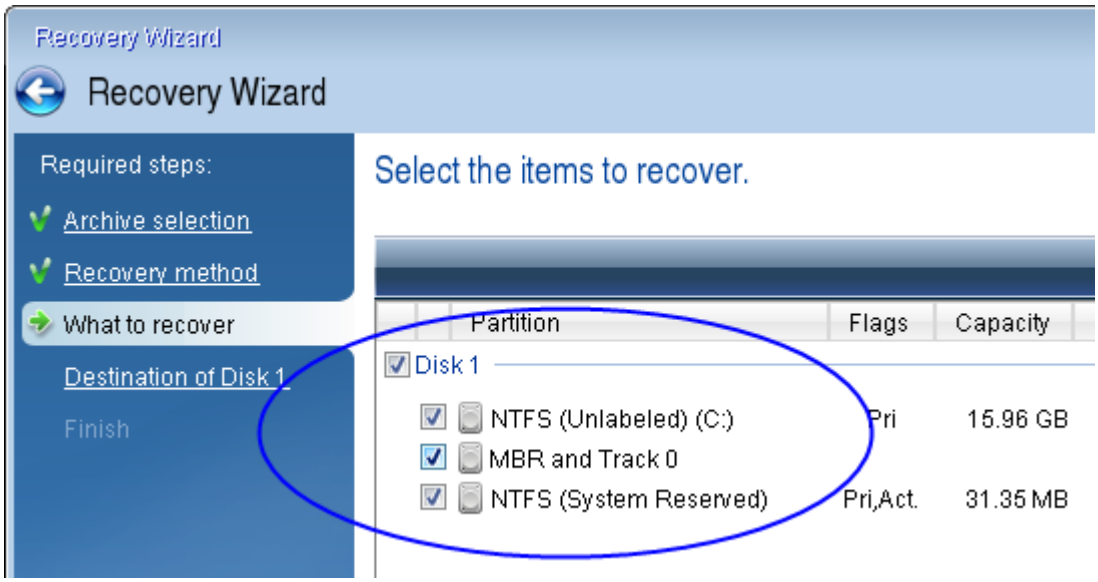
手順を開始する前に、以下があることを確認してください。

- **Acronis ブータブルメディア。**
  詳細については、Acronis ブータブルメディア の作成を参照してください。
- **ディスクモードで作成されたシステムディスクのバックアップ。**
  このバックアップを作成するには、ディスクモードに切り替えてから、システムパーティションがあるハードドライブを選択します。詳細については、「ディスクとパーティションのバックアップ」を参照してください。



MBR ディスクから UEFI 起動のコンピューターにシステムを転送するには、次の手順を実行します。

1. UEFI モードで Acronis ブータブルメディア から起動して、[Acronis Cyber Protect Home Office] を選択します。
2. **リカバリウィザード**を実行して、「システムの復元」で説明されている手順を実行します。
3. **[復元元]** で、ディスク名の横にあるチェックボックスをオンにして、システムディスク全体を選択します。
   下の例では、**[ディスク1]** のチェックボックスをオンにします。



4. **[完了]** で、**[実行]** をクリックします。

操作が完了すると、復元先ディスクはGPTスタイルに変換されて、UEFIモードで起動できるようになります。

リカバリ後は、UEFI モードでコンピューターを起動してください。システムディスクの起動モードをUEFIのブートマネージャのユーザーインターフェイスで変更する必要がある場合があります。

BIOSまたはUEFI BIOSでの起動順の並べ替え

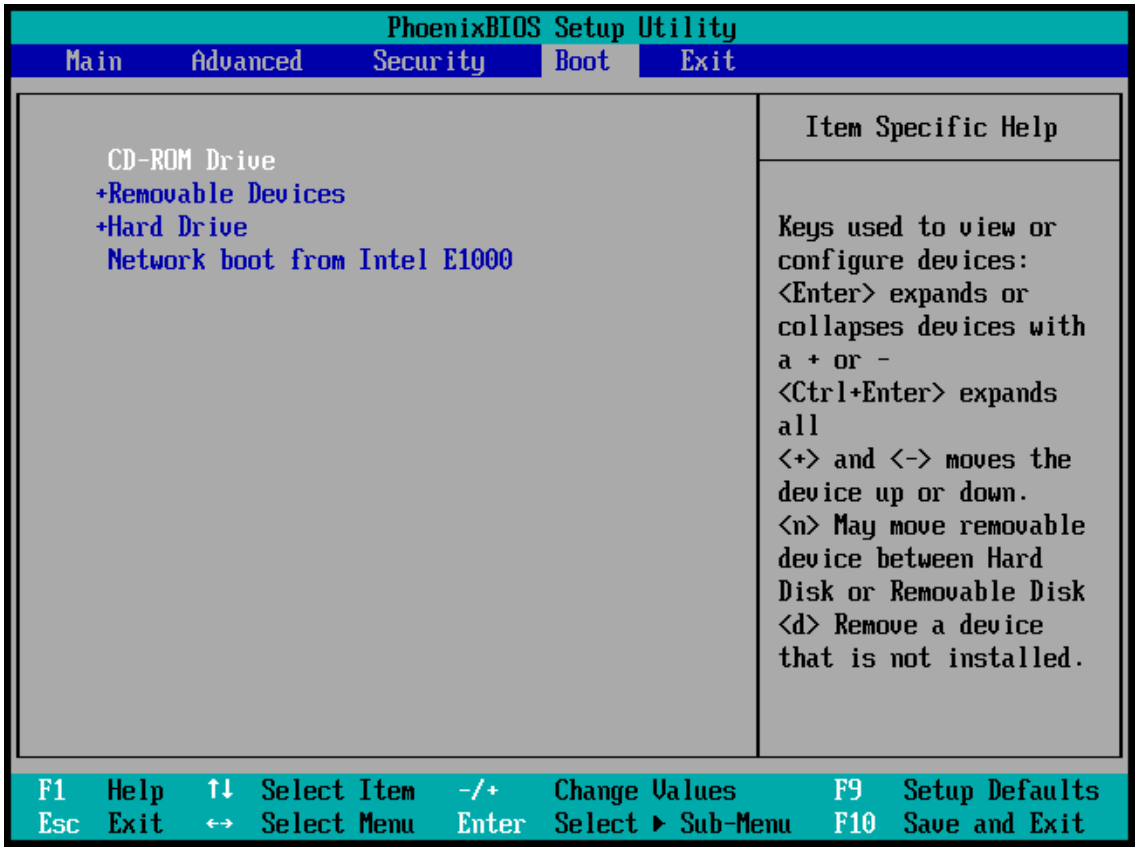
Acronis ブータブルメディア からコンピューターを起動するためには、そのメディアが最初の起動デバイスとなるように、起動順序を割り当てる必要があります。起動順は、コンピュータのファームウェアインターフェイスに応じて、BIOSかUEFI BIOSで変更されます。手順は、どちらの場合も非常によく似ています。

Acronis ブータブルメディア からブートする手順は、次のとおりです。

1. USB フラッシュドライブまたは外付けドライブをブータブルメディアとして使用している場合は、USB ポートに接続します。
2. コンピュータの電源を入れます。Power-On Self Test（POST）の実行中、BIOSまたはUEFI BIOSに移るために押す必要があるキーの組み合わせが表示されます。
3. キーの組み合わせを押します（たとえば、**Delキー、F1キー、Ctrl+Alt+Escキー、Ctrl+Escキー**）。BIOSまたはUEFI BIOSのセットアップユーティリティが開きます。なお、ユーティリティごとに表示、項目のセット、名称などが異なります。

> **注意**
> マザーボードの中には、いわゆるブートメニューが用意されているものもあります。ブートメニューは、特定のキーまたはキーの組み合わせ、たとえば **F12** キーなどを押すと開きます。ブートメニューを使用すれば、BIOSまたはUEFI BIOS設定を変更することなく、ブータブルデバイスのリストからブートデバイスを選択できます。

4. CDまたはDVDをブータブルメディアとして使用している場合は、CDまたはDVDをCDドライブまたはDVDドライブに挿入します。
5. ブータブルメディア（CD、DVD、または USB ドライブ）を最初の起動デバイスにします。
   a. キーボードの矢印キーを使用してブート順序の設定に移動します。
   b. ブータブルメディアのデバイスの上にマウスポインタを置き、リスト内の最初の項目にします。通常は、プラス記号キーとマイナス記号キーを使用して順序を変更できます。



6. BIOSまたはUEFI BIOSを終了して変更内容を保存します。コンピューターが Acronis ブータブルメディア から起動します。

注意
コンピュータが最初のデバイスからの起動に失敗した場合は、起動するまで、2台目以降のデバイスからの起動が試みられます。

Acronis Cloudからのディスクの復元

Acronis Cloud からのディスクの復元は、通常のハードディスクドライブからの復元と非常によく似ています。

- Windows と Acronis Cyber Protect Home Office が起動できる場合は、「パーティションとディスクの復元」を参照してください。
- Windows を起動できない場合は、「Acronis Cloud からのシステムの復元」を参照してください。

動作

コンピュータがイーサネットケーブルまたはWiFi経由でインターネットに接続されている必要があります。Acronis Cyber Protect Home Office は、WPA-Personal、WPA2-Personal、WPA2-Enterprise など、いくつかのワイヤレスセキュリティプロトコルをサポートしています。

元のロケーションへの復元

ディスクを元のロケーションに復元するとき、Acronis Cyber Protect Home Office はディスク領域全体をコンピューターにダウンロードしません。ディスクをスキャンしてデータの変更を検索し、イメージ内のファイルと異なるファイルのみを復元します。この技術により、ディスクを復元するためにダウンロードする必要があるデータの量が大幅に軽減されます。

新しいロケーションへの復元

ディスクを別のロケーションまたは未割り当ての領域に復元するとき、処理はローカルストレージからの復元とほとんど変わりません。唯一の相違点はデータを書き込む方法です。Acronis Cyber Protect Home Office では、連続的にではなく、個別のブロックごとにデータをダウンロードして書き込みます。この技術によりリカバリ速度と処理全体の信頼性が向上しています。

リカバリが中断した場合

Acronis Cloud からのディスク復元はインターネット接続を使用するので、通常は長い時間がかかります。通常のハードディスクからの復元と比較すると、復元が中断する可能性は高くなります。

リカバリの中断が考えられる理由

- インターネット接続が切断された。
- Acronis Cloud への接続が切断された。
- 意図的または誤って復元をキャンセルした。
- 電源供給に問題がある。

接続の問題でリカバリが完了しない場合、Acronis Cyber Protect Home Office では自動で Acronis Cloud への再接続と、リカバリ処理の再開が試行されます。このような場合は、インターネット接続設定を確認することをおすすめします。すべての自動試行が失敗した場合は、接続が回復したときに、もう一度手動で復元を実行してください。

その他の場合は、手動で再度復元を実行し、リカバリが完了することを確認してください。

中断の理由にかかわらず、Acronis Cyber Protect Home Office ではリカバリが最初から開始されることはありません。処理が再開され、復元されていないデータのみがダウンロードされます。

Acronis Cloud からのシステムの復元

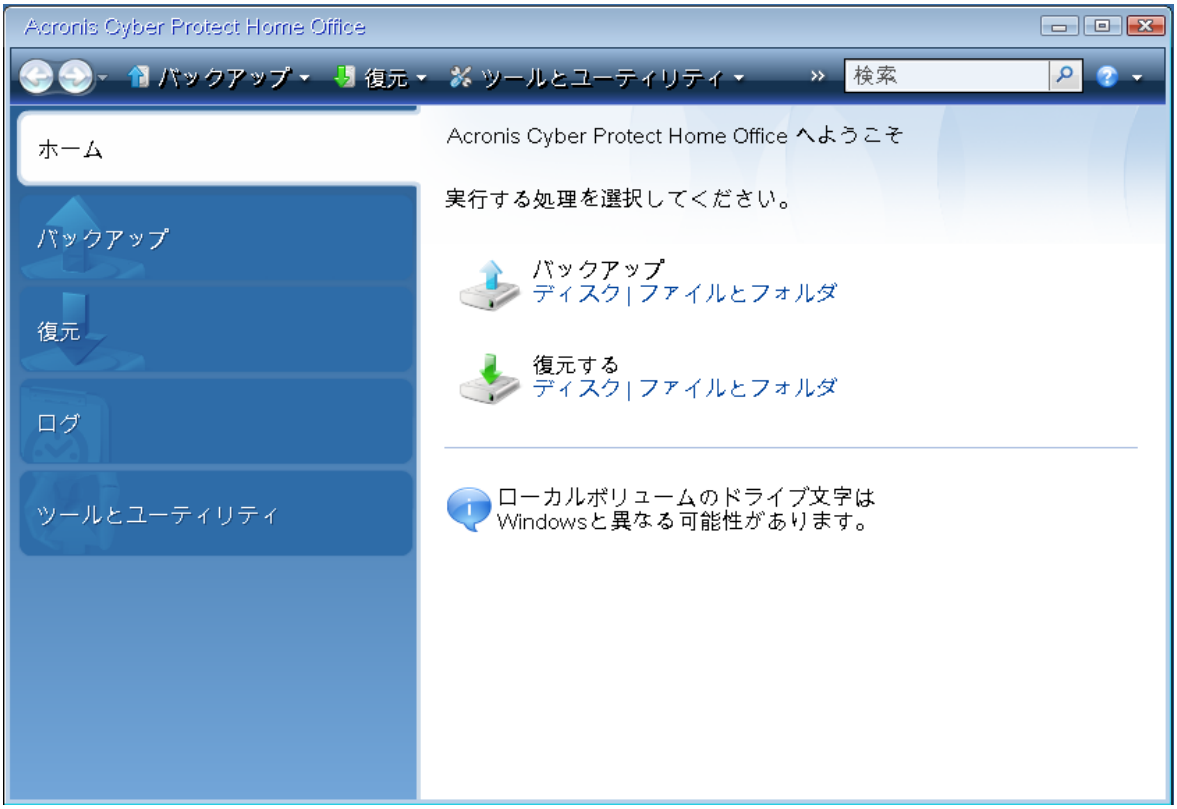
注意
インターネット接続の速度によっては、Acronis Cloud からのディスクリカバリに長時間かかることがあります。

始める前に、「リカバリの準備」で説明している準備作業の実行をおすすめします。システムを新しいディスクに復元する場合、その新しいディスクをフォーマットする必要はありません。フォーマットはリカバリ処理で行われます。

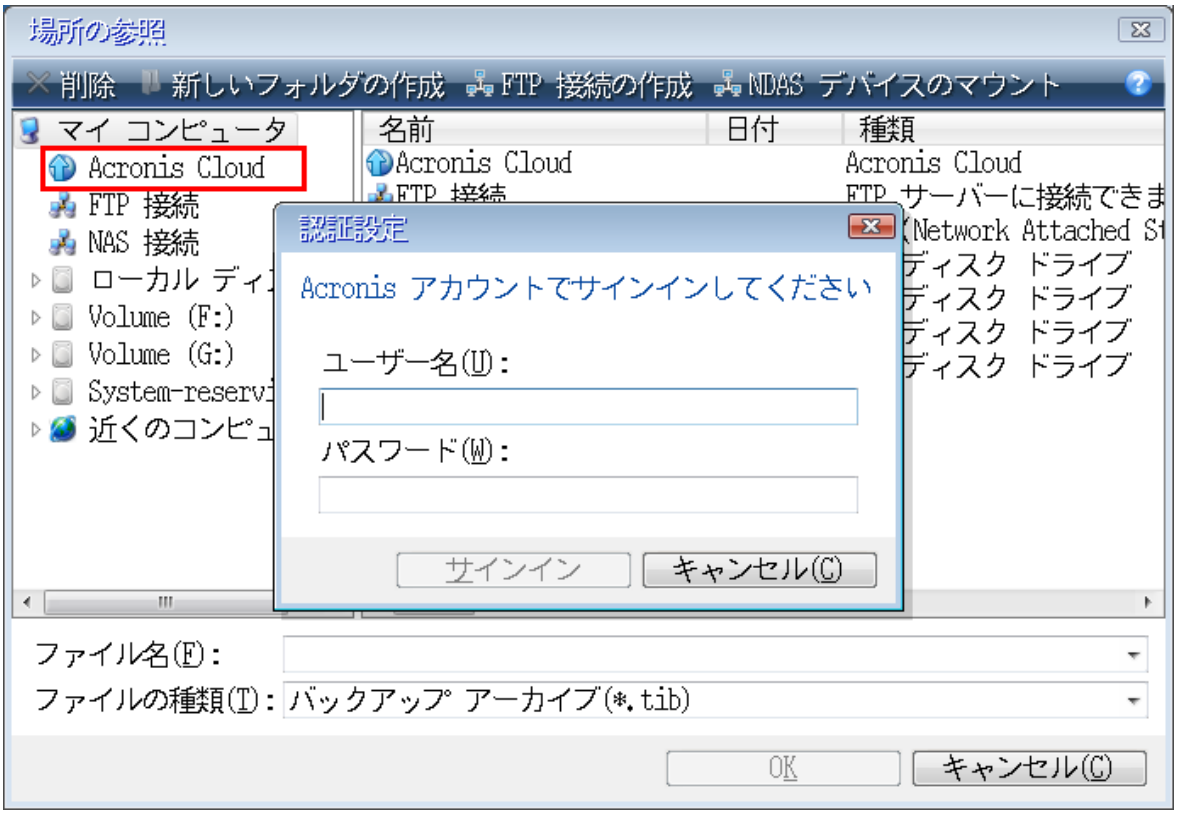
この手順を開始する前に、コンピューターがイーサネットケーブルまたは Wi-Fi 経由でインターネットに接続されていることを確認してください。

Acronis Cloud からシステムディスクを復元する手順は、次のとおりです。

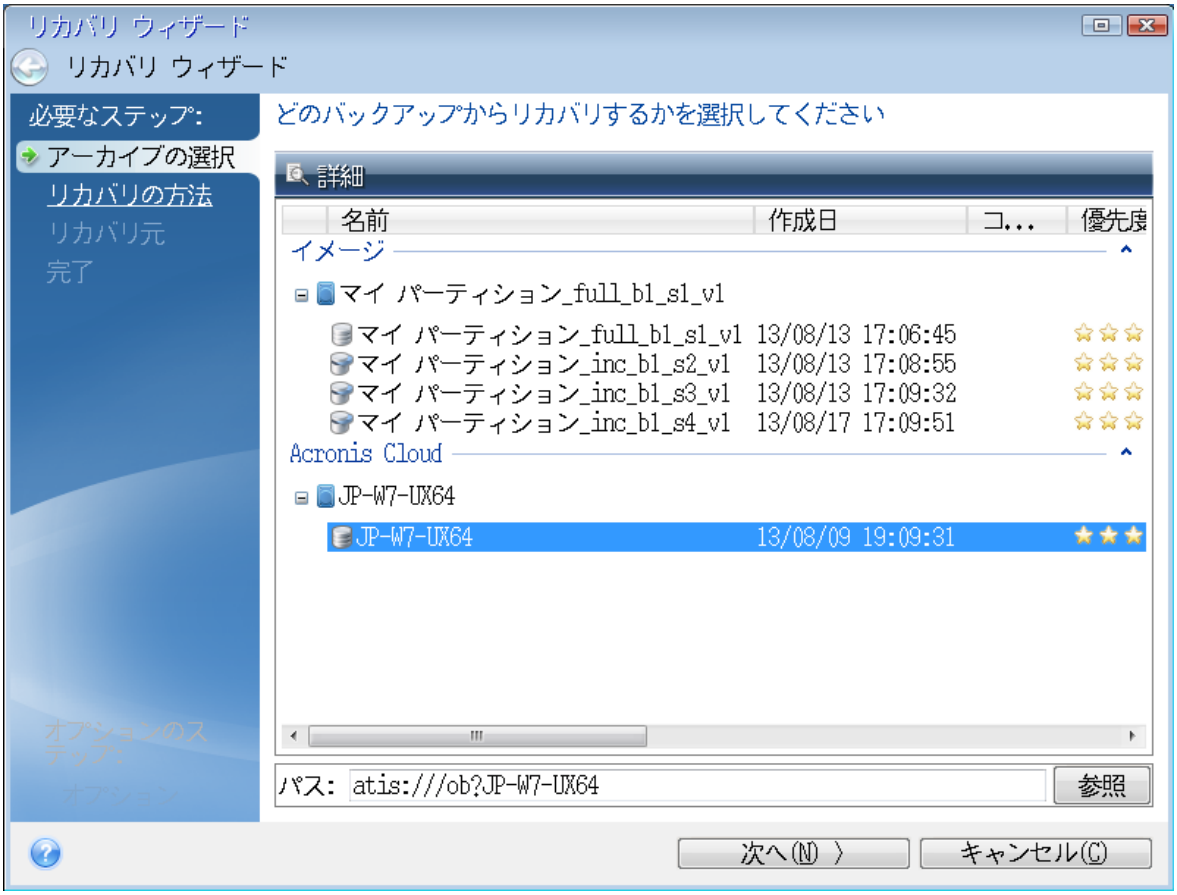
1. BIOS で起動順序を設定して、Acronis ブータブルメディア（CD、DVD、または USB スティック）を最初の起動デバイスにします。「BIOS での起動順の並び替え」を参照してください。
2. ブータブルメディアから起動して、**[Acronis Cyber Protect Home Office]** を選択します。
3. **[ホーム]** 画面で、**[リカバリ]** の下にある **[マイディスク]** を選択します。



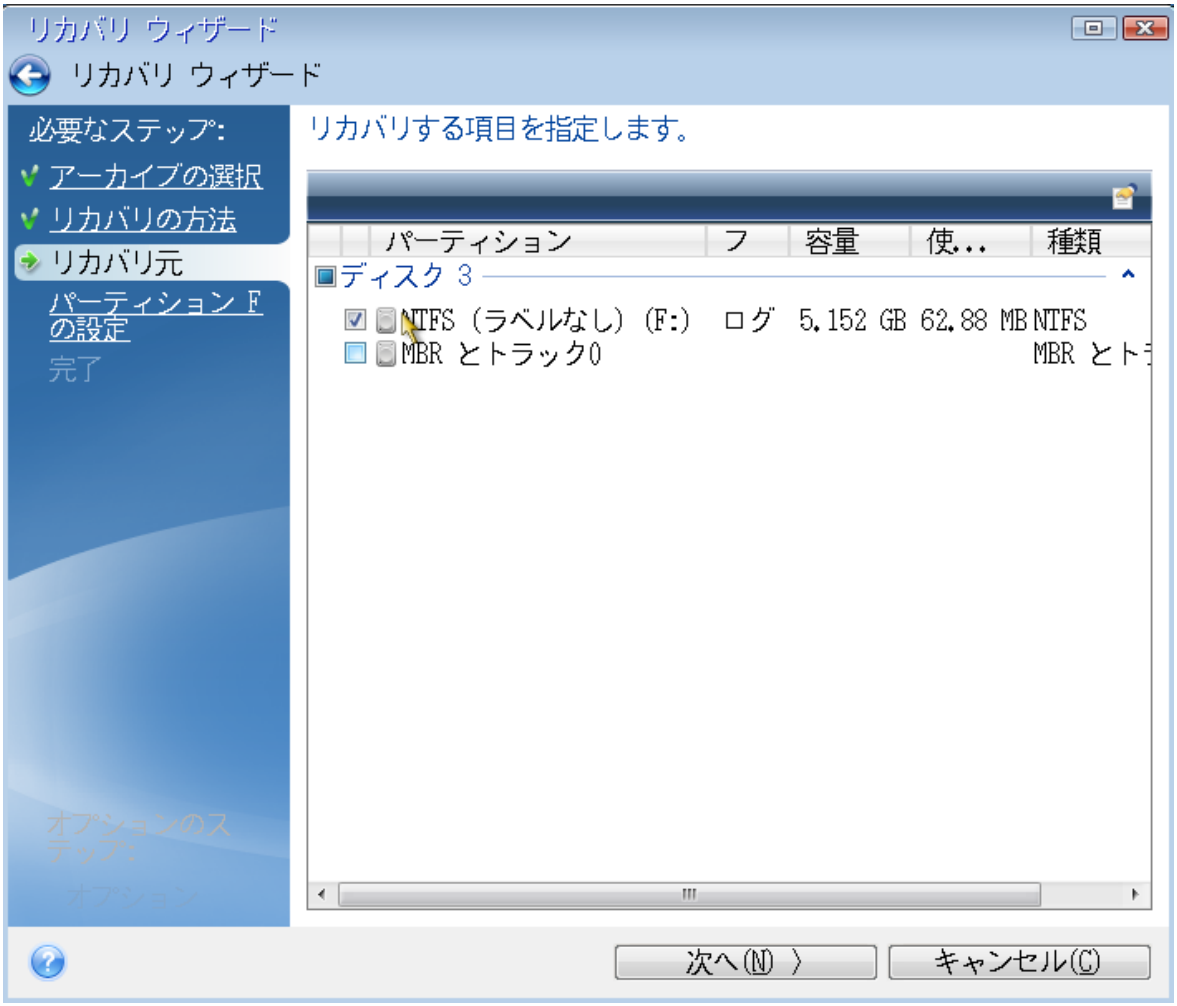
4. 利用可能なバックアップの一覧に、システムディスクまたはシステムパーティションのオンラインバックアップを追加するには、**[参照]** をクリックします。
5. 表示されたウィンドウのディレクトリツリーで、Acronis Cloud を選択し、Acronis アカウントの資格情報を入力します。



6. 復元に使用するバックアップを選択し、**[OK]** をクリックします。
7. **[アーカイブの選択]** のステップで、オンラインバックアップを選択し、**[次へ]** をクリックします。



8. [**リカバリの方法**] のステップで、[**ディスクまたはパーティション全体を復元する**] を選択します。
9. [**復元元**] で、システムパーティション（通常はC）とシステム予約パーティション（存在する場合）を選択します。こうしたパーティションは **Pri** フラグ、**Act** フラグでも識別できます。



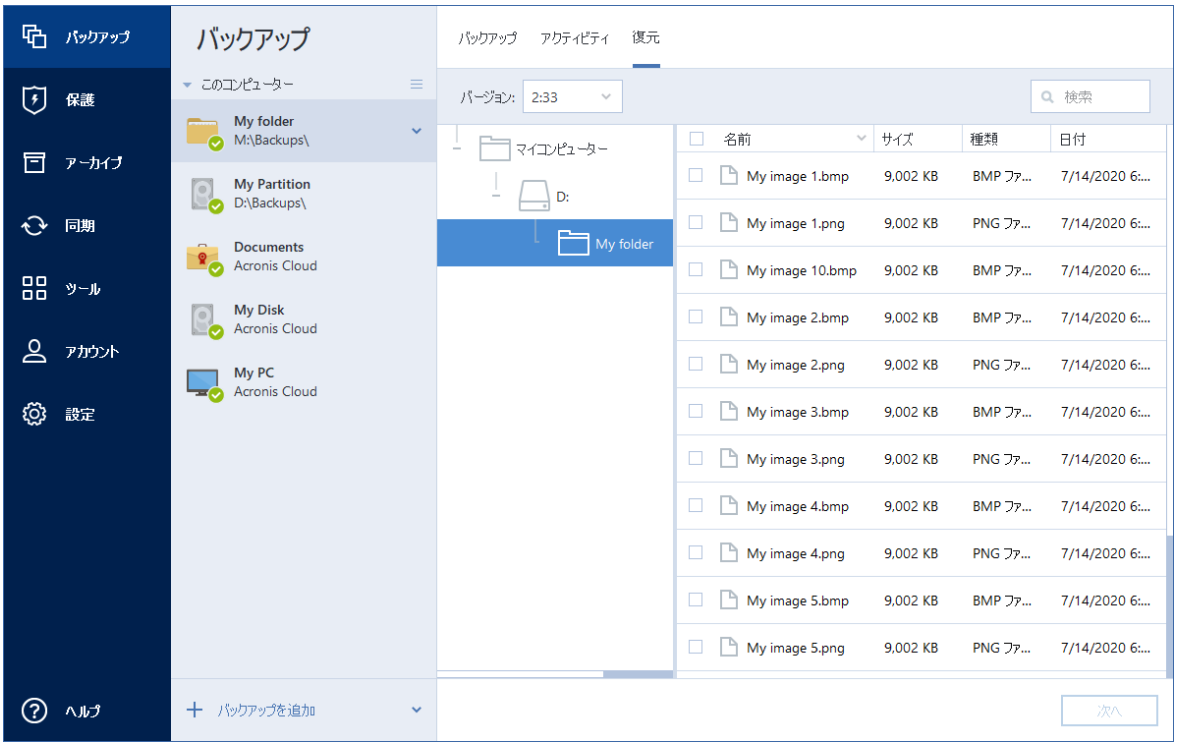
10. [**パーティション C の設定**]（またはシステムパーティションが C 以外の場合は該当するドライブ文字）で、必要に応じて設定を変更します。たとえば、容量が異なる新しいハードディスクに復元する場合は、設定を変更する必要があります。
11. [**完了**] の画面で処理の概要を確認します。パーティションのサイズを変更していない場合は、[**パーティションの削除**] 項目と [**パーティションのリカバリ**] 項目のサイズが一致している必要があります。[**実行**] をクリックします。
12. リカバリが完了したら、スタンドアロン版の Acronis Cyber Protect Home Office を終了し、ブータブルメディアを取り外します。復元されたシステムパーティションから起動します。必要な状態までWindowsをリカバリしたことを確認してから、元の起動順序を復元します。

ファイルとフォルダのリカバリ

バックアップされたファイルとフォルダは、Acronis Cyber Protect Home Office や、File Explorer、Acronis Cloud で参照およびリカバリできます。 ファイルレベルとディスクレベルのバックアップからファイルやフォルダをリカバリできます。

Acronis Cyber Protect Home Office でデータを復元する場合は、次のようにします。

1. サイドバーで **[バックアップ]** をクリックします。
2. バックアップの一覧から、リカバリするファイルやフォルダを含むバックアップを選択し、**[復元]** タブを開きます。
3. [オプション] ツールバーの **[バージョン]** ドロップダウンリストで、バックアップの必要な日時を選択します。デフォルトでは、最新のバックアップが復元されます。
4. 復元するファイルまたはフォルダに対応するチェックボックスを選択し、**[次へ]** をクリックします。



5. [オプション] デフォルトで、データは元のロケーションに復元されます。変更するには、ツールバーの **[参照]** をクリックしてから、必要な宛先フォルダを選択します。
6. [オプション] リカバリ処理のオプション（リカバリ処理の優先度、ファイルレベルのセキュリティ設定など）を設定します。オプションを設定するには、**[復元オプション]** をクリックします。ここで設定するオプションは、現在のリカバリ処理にのみ適用されます。
7. リカバリ処理を開始するには、**[今すぐリカバリする]** ボタンをクリックします。

   選択されたファイルバージョンは指定された宛先にダウンロードされます。

   [キャンセル] をクリックすると、リカバリは中止されます。なお、リカバリを中止してもリカバリ先のフォルダが変更される場合があります。

File Explorer でデータをリカバリするには、次の手順を実行します。

1. 対応する .tibx ファイルをダブルクリックし、リカバリするファイルまたはフォルダまで移動して参照します。
2. ファイルまたはフォルダをハード ディスクにコピーします。

注意
コピーしたファイルの「圧縮」属性と「暗号化」属性は失われます。これらの属性を維持したい場合は、バックアップをリカバリすることをお勧めします。

Acronis Cloud でデータを復元する場合は、次のようにします。

1. 左サイドバーで **[バックアップ]** をクリックします。
2. バックアップリストから、リカバリするデータを含むバックアップを選択します。
3. 必要なデータが含まれるバックアップバージョンを選択します。これを行うには、最後のバックアップ操作の日付を確認します。
4. ファイルおよびフォルダのリストから、復元するものを選択します。
5. [オプション] ファイル (フォルダではない) の特殊なバージョンを復元できます。これを行うには、右サイドバーの **[バージョン]** をクリックしてから、必要なバージョンラインのダウンロードアイコンをクリックします。
6. 復元を開始するには、右サイドバーの **[ダウンロード]** をクリックします。
   選択したデータはデフォルトのダウンロードフォルダにコピーされます。

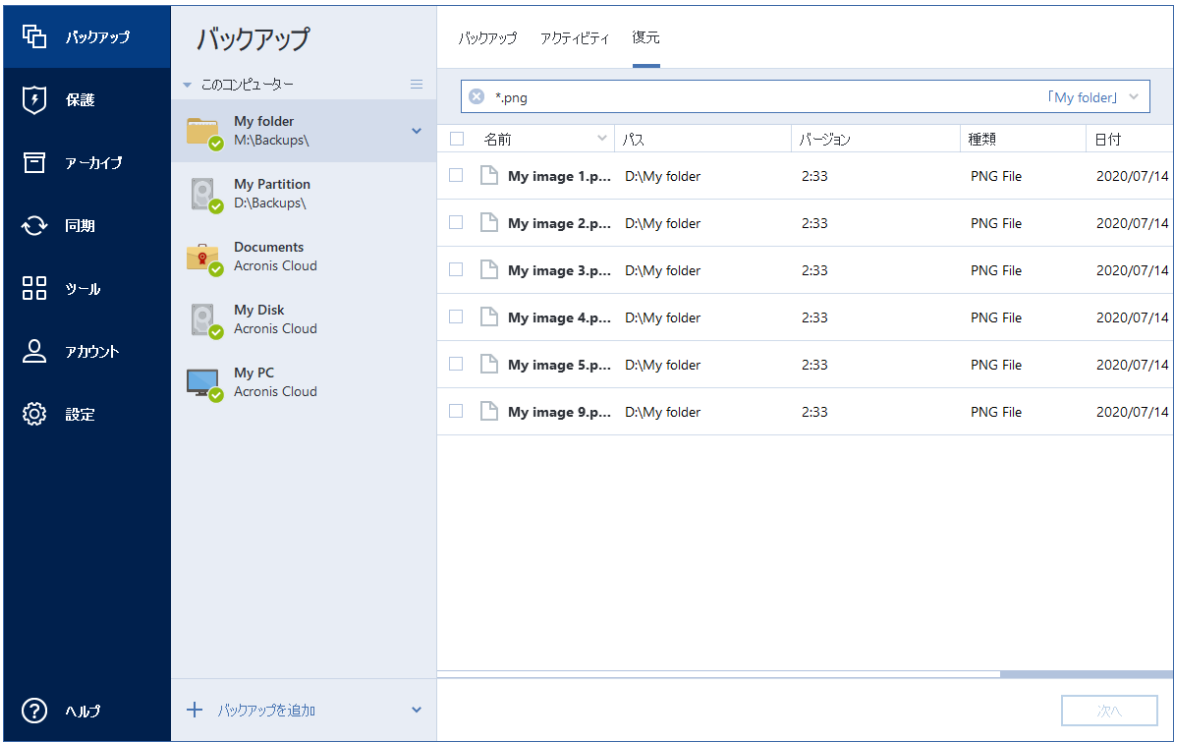
注意
複数のファイルとフォルダを選択した場合は、それらが zip アーカイブに格納されます。

バックアップの内容の検索

ローカルバックアップからデータを復元する際、選択したバックアップ内に保存された特定のファイルやフォルダを検索できます。

ファイルやフォルダを検索する手順は、次のとおりです。

1. 「パーティションとディスクのリカバリ」または「ファイルとフォルダのリカバリ」の説明に従ってデータの復元を開始します。
2. 復元するファイルやフォルダを選択する際、**[検索]** フィールドにファイル名またはフォルダ名を入力します。検索結果が表示されます。
   一般的なWindowsのワイルドカード文字（*および?）も使用できます。たとえば、拡張子が「**.exe**」のファイルを検索するには、「***.exe**」と入力します。「my」で始まる5文字のファイル名が付いた「.exe」ファイルをすべて検索するには、「**my???.exe**」と入力します。



3. デフォルトでは、Acronis Cyber Protect Home Office は前の手順で選択したフォルダを検索します。バックアップ全体を検索対象にするには、下矢印をクリックして、**[すべてのバックアップ]** をクリックします。

   前の手順に戻るには、検索テキストを削除して、クロスアイコンをクリックします。
4. 検索完了後、復元するファイルを選択したら、**[次へ]** をクリックします。

注意
[バージョン] 項目に注意してください。異なるバックアップバージョンに属するファイルやフォルダを同時に復元することはできません。

Office 365 データの復元

Acronis Cyber Protect Home Office を使用すると、電子メールメッセージ、ファイルとフォルダ、プロフィール情報、およびその他のデータの消失から個人の Office 365 アカウントを保護することができます。アカウントデータのクラウドバックアップがある場合、それらのデータを参照して特定のアイテムを復元できます。

復元可能なアイテム

メールボックスバックアップから復元が可能なアイテムは次のとおりです。

- メールボックス全体
- 電子メールメッセージ
- 添付ファイル

OneDrive バックアップから復元が可能なアイテムは次のとおりです。

- OneDrive 全体
- バックアップされたファイルとフォルダ

Office 365 データの復元

データを参照して復元するには、次のようにします。

1. 次のいずれかを実行してオンラインダッシュボードを開きます。
   - https://cloud.acronis.comのリンクをクリックします。
   - Acronis Cyber Protect Home Office のサイドバーで、[**アカウント**]、[**オンラインダッシュボードを開く**] の順にクリックします。
2. Acronis アカウントにサインインします。
3. サイドバーで、［**リソース**］ をクリックし、Office 365 バックアップボックスを探してから、[**復元**] をクリックします。
4. バックアップの一覧を参照します。必要に応じて、フィルタを使用して内容でバックアップを検索します。
5. バックアップを選択したら、[**復元...**] をクリックして、復元するデータを選択します。
   - OneDrive 全体または特定のファイルとフォルダ。
   - メールボックス全体または特定のメッセージ。

   特定のアイテムの復元を選択すると、オンラインダッシュボードで、バックアップされたアイテムの一覧が表示されます。これらのアイテムを参照したり、内容を表示できます。また、検索を使用して特定のアイテムを見つけることもできます（一部のデータの種類には未対応）。

   アイテムを選択した後、実行する操作を選択できます（データの種類に応じて、一部の操作は使用できないことがあります）。
   - [**内容の表示**] — クリックすると、アイテムの詳細を表示したり、アイテムを最大サイズで開くことができます。
   - [**Send as email（電子メールとして送信）**]: メッセージを選択した受信者に送信する場合にクリックします。
   - [**Show versions（バージョンの表示）**]: アイテムのバージョンを表示する場合にクリックします。
   - [**復元**]: 復元するアイテムの場所を指定する場合にクリックします。アイテムによっては、共有権限を復元することもできます。
   - [**ダウンロード**] — クリックすると、選択したファイルをダウンロードできます。
6. [**Start recovery（復元の開始）**]をクリックします。

リカバリ オプション

ディスク/パーティションやファイル リカバリ処理のオプションを設定できます。アプリケーションをインストールすると、すべてのオプションは初期値に設定されます。それらのオプションは、現在のリカバリ処理用のみに、または、その後のすべてのリカバリ処理用に変更できます。[**設定をデフォルトとして保存する**] チェックボックスをオンにすると、変更した設定が今後のリカバリ作業すべてにデフォルトで適用されます。

ディスク リカバリ オプションとファイル リカバリ オプションは完全に独立しており、個別に設定する必要があるので注意してください。

製品のインストール後に変更したオプションをすべて初期値にリセットする場合は、**[初期設定にリセット]** ボタンをクリックします。

ディスクリカバリモード

場所: **[復元オプション]** > **[拡張]** > **[ディスクリカバリモード]**

このオプションを使用して、イメージバックアップのディスクリカバリモードを選択できます。

- **[セクタ単位の復元]** - ディスクまたはパーティションの使用済み　　クタと未使用セクタの両方を復元する場合にこのチェックボックスをオンにします。このオプションが有効になるのは、セクタ単位バックアップの復元を選択した場合のみです。

リカバリの前後に実行するコマンド

場所: **[復元オプション]** > **[詳細]** > **[処理の前後に実行するコマンド]**

リカバリ処理の前後に自動的に実行するコマンド（またはバッチファイル）を指定することができます。

たとえば、復元を開始する前に特定のWindowsプロセスを開始/停止することや、リカバリ対象データのウィルスの有無を調べることができます。

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。

- リカバリ処理の開始前に実行するコマンドを **[処理前に実行するコマンド]** フィールドで選択します。新しいコマンドを作成する、または新しいバッチファイルを選択するには、**[編集]** ボタンをクリックします。
- リカバリ処理の終了後に実行するコマンドを **[処理後に実行するコマンド]** フィールドで選択します。新しいコマンドを作成する、または新しいバッチファイルを選択するには、**[編集]** ボタンをクリックします。

ユーザーの入力を必要とする対話型のコマンド（pauseなど）は実行しないでください。これらのコマンドは、サポートされていません。

リカバリ用ユーザーコマンドの編集

リカバリの前または後に実行するコマンドを指定することができます。

- **[コマンド]** フィールドにコマンドを入力するか、一覧から選択します。**[...]** をクリックすると、バッチファイルを選択できます。
- **[作業ディレクトリ]** フィールドに、コマンド実行のためのパスを入力するか、入力済みのパスの一覧から選択します。
- **[引数]** フィールドに、コマンド実行引数を入力するか、一覧から選択します。

[コマンドの実行が完了するまで処理を行わない]（デフォルトでは有効）パラメータを無効にすると、コマンド実行と同時にリカバリ処理を実行できます。

[ユーザーコマンドが失敗したら処理を中止する] パラメータを有効にした場合は（デフォルトでは有効）、コマンド実行でエラーが発生すると処理が中止されます。

入力したコマンドをテストするには、**[コマンドのテスト]** ボタンをクリックします。

ベリファイオプション

場所: **[復元オプション]** > **[詳細]** > **[ベリファイ]**

- **[リカバリ前にバックアップをベリファイする]**: リカバリ前にバックアップの整合性を確認するには、このオプションを有効にします。
- **[リカバリ後にファイルシステムをチェックする]**: 復元されたパーティションでファイルシステムの整合性を確認するには、このオプションを有効にします。

注意
確認できるのはFAT16/32およびNTFSファイルシステムのみです。

注意
システムパーティションを元の場所に復元する場合のように、リカバリ中に再起動が必要な場合は、ファイルシステムはチェックされません。

コンピュータの再起動

場所: **[復元オプション]** > **[詳細]** > **[コンピュータの再起動]**

リカバリで必要な場合に自動的にコンピュータを再起動させるには、**[復元に必要であればコンピュータを自動的に再起動する]** チェックボックスをオンにします。このオプションは、オペレーティングシステムによってロックされているパーティションを復元する必要がある場合に使用します。

ファイルリカバリオプション

場所:**[復元オプション]** > **[詳細]** > **[ファイルリカバリオプション]**

次のファイルリカバリオプションを選択できます。

- **[元のセキュリティ設定でファイルを復元する]** - ファイルのセキュリティ設定がバックアップ中に保存された場合 （「バックアップ用のファイルレベルのセキュリティ設定」を参照） 、ファイルのセキュリティ設定を復元するか、復元先のフォルダのセキュリティ設定をファイルに継承させるかを選択できます。このオプションは、ファイルまたはフォルダのバックアップからファイルをリカバリする場合にのみ有効です。
- **[リカバリされたファイルに現在の日時を設定する]** - ファイルの日付/時刻をバックアップからリカバリするか、現在の日付/時刻を割り当てるかを選択することができます。デフォルトでは、バックアップの日付と時刻が割り当てられます。

ファイル上書きオプション

ロケーション: **[復元オプション]** > **[詳細]** > **[ファイル上書きオプション]**

バックアップにあるファイルと同じファイル名が復元先フォルダで見つかった場合の処理を選択します。

注意
このオプションは、（ディスクとパーティションではなく）ファイルとフォルダの復元時のみ利用できます。

ハードディスク上のファイルをバックアップのファイルで上書きする場合は、**[既存のファイルを上書きする]** チェックボックスをオンにします。このチェックボックスがオフの場合、バックアップよりも新しいファイルとフォルダはディスク上に保持されます。

一部のファイルは上書きする必要がない場合:

- すべての隠しファイルと隠しフォルダの上書きを無効にするには、**[隠しファイルと隠しフォルダ]** チェックボックス選択します。このオプションは、ローカルの保存先およびネットワーク共有へのファイルレベルのバックアップで利用できます。
- すべてのシステムファイルとシステムフォルダの上書きを無効にするには、**[システムファイルとシステムフォルダ]** チェックボックスを選択します。このオプションは、ローカルの保存先およびネットワーク共有へのファイルレベルのバックアップで利用できます。
- すべての新しいファイルとフォルダの上書きを無効にするには、**[復元するものよりも新しいファイルとフォルダ]** チェックボックスを選択します。
- 上書きしたくないカスタムファイルとカスタムフォルダの一覧を管理するには、**[特定のファイルやフォルダを追加する]** をクリックします。このオプションは、ローカルの保存先およびネットワーク共有へのファイルレベルのバックアップで利用できます。
  - 特定のファイルの上書きを無効にするには、[+] アイコンをクリックして除外条件を作成します。
  - 条件の指定には、一般的な Windows のワイルドカード文字を使用できます。たとえば、拡張子**.exe**を持つすべてのファイルを保護するには、***.exe**を追加します。**My???.exe**を追加すると、「my」で始まり 5 文字で構成される名前が付いた拡張子 .exe のファイルがすべて保護されます。

条件を削除するには、目的の条件を選択して [-] アイコンをクリックします。

リカバリ処理のパフォーマンス

場所: **復元オプション** > **拡張** > **パフォーマンス**

次のような設定の構成が可能です。

処理の優先順位

バックアップ処理や復元処理の優先度を変更すると、（優先度の上げ下げによって）バックアップの処理速度を速くしたり遅くしたりできますが、実行中の他のプログラムのパフォーマンスに悪影響を及ぼす可能性もあります。システムで実行中の処理の優先度に応じて、処理に割り当てられるCPUやシステムリソースの使用量が決定されます。処理の優先度を下げると、他のCPUタスクで使用されるリソースを増やすことができます。バックアップや復元の優先度を上げると、実行中の他の処理からリソースを取得することができ、処理の速度が向上します。優先度変更の効果は、全体的な CPU の使用状況およびその他の要因に応じて異なります。

処理の優先度は、次のいずれかに設定することができます。

- **[低]**（デフォルトで有効）：バックアップ処理や復元処理の速度は低下しますが、他のプログラムのパフォーマンスは向上します。
- **[通常]**: バックアップ処理や復元処理に他の処理と同じ優先度が割り当てられます。
- **[高]**: バックアップ処理や復元処理の速度は向上しますが、他のプログラムのパフォーマンスは低下します。このオプションを選択すると、Acronis Cyber Protect Home Office による CPU 使用率が 100% になる場合があるので注意してください。

リカバリ処理の通知

場所: **[復元オプション]** > **[通知]**

バックアップまたはリカバリの処理には 1 時間以上かかる場合があります。Acronis Cyber Protect Home Office では、この処理の終了時に E メールで通知を受け取ることができます。また、処理中に発行されたメッセージや、処理完了後の完全な処理ログもプログラムによって送信されます。

デフォルトでは、すべての通知は無効になっています。

空きディスク領域のしきい値

復元ストレージの空き領域が指定のしきい値より少なくなったときに、通知を受け取ることができます。バックアップの開始後、選択したバックアップ保存先の空き領域が指定値よりも既に少ないことが Acronis Cyber Protect Home Office によって検出された場合には、プログラムで実際の復元処理は開始されず、空き領域が少ない旨の通知メッセージが直ちに表示されます。メッセージには次の 3 つの選択肢が示されます。メッセージを無視して復元を続行する、復元を保存する別の場所を参照する、復元をキャンセルする、の中からいずれかを選択します。

復元の実行中に空き領域が指定値より少なくなった場合にも、プログラムにより同じメッセージが表示されるため、同様の選択を行う必要があります。

ディスクの空き領域のしきい値を設定するには、次の手順を実行します。

- **[ディスクの空き領域が不十分なときに通知メッセージを表示する]** チェックボックスをオンにします。
- **[サイズ]** ボックスでしきい値を入力または選択し、単位を選択します。

Acronis Cyber Protect Home Office では、次のストレージデバイスの空き領域をチェックすることができます。

- ローカルハードドライブ
- USBカードおよびドライブ
- ネットワーク共有（SMB）

注意
[エラー処理] 設定で **[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）]** チェックボックスがオンになっている場合、メッセージは表示されません。

注意
CD/DVDドライブについては、このオプションを有効にすることはできません。

電子メールによる通知

1. **[処理状態に関する電子メール通知を送信する]** チェックボックスを選択します。
2. 電子メールを設定します。
   - **[宛先]** フィールドに電子メール アドレスを入力します。複数の電子メール 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。
   - **[サーバー設定]** フィールドに送信メールサーバー（SMTP）を入力します。
   - 送信メール サーバーのポート番号を設定します。デフォルトの場合、ポート番号は 25 に設定されます。
   - 必要に応じて、**[SMTP 認証]** チェック ボックスを選択し、対応するフィールドにユーザー名とパスワードを入力します。
3. 設定が正しいかどうかをチェックするには、**[テスト メッセージを送信する]** ボタンをクリックします。

テストメッセージの送信に失敗した場合

1. **[拡張設定を表示]** をクリックします。
2. 追加の電子メール設定を行います。
   - **[差出人]** フィールドに電子メール送信者のアドレスを入力します。指定するアドレスが不明な場合は、たとえば、aaa@bbb.com のような標準形式で任意のアドレスを入力します。
   - 必要に応じて、**[件名]** フィールドのメッセージの件名を変更します。
   - **[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ます。
   - 受信メール サーバー（POP3）を **[POP3 サーバー]** フィールドに入力します。
   - 受信メール サーバーのポート番号を設定します。デフォルトの場合、ポート番号は 110 に設定されます。
3. **[テストメッセージを送信する]** ボタンをもう一度クリックします。

その他の通知設定

- 処理の完了に関する通知を送信するには、**[処理が正常に完了したら通知を送信する]** チェックボックスをオンにします。
- 処理の失敗に関する通知を送信するには、**[処理が失敗したら通知を送信する]** チェックボックスをオンにします。
- 処理メッセージを添付して通知を送信するには、**[ユーザーの操作が必要な場合に通知を送信する]** チェックボックスをオンにします。
- 処理の詳細なログを添付して通知を送信するには、**[完全なログを通知に含める]** チェックボックスをオンにします。

データのアーカイブ

データのアーカイブについて

データのアーカイブは、サイズの大きいファイルや使用頻度の低いファイルを Acronis Cloud、NAS、外付けハードドライブ、または USB フラッシュドライブに移動できるツールです。このツールを実行するたびに、選択したフォルダ内のデータが解析されて、Acronis Cloud へのアップロードやローカルストレージへの移動の対象となる推奨のファイルが示されます。アーカイブするファイルやフォルダを選択できます。アーカイブへの移動が完了すると、これらのファイルのローカルコピーは削除されます。これらのファイルへのリンクは、Acronis Drive という特定の場所に保存されます。この場所には、File Explorerから通常のフォルダとしてアクセスできます。ファイルのリンクをダブルクリックすると、ローカルフォルダに保存されている場合と同じようにファイルが開きます。ファイルが Acronis Cloud にアーカイブされている場合は、最初にファイルがコンピュータにダウンロードされます。ファイルへのアクセスおよび管理は、Acronis Cloud でも問題なく行うことができます。

データのアーカイブの主な機能は次のとおりです。

- **ストレージを解放して空き容量を増やす**
  通常、最新の大容量ハードドライブの空き領域は、オペレーティングシステムやアプリケーションではなく、写真やドキュメントなどのユーザーデータによって使用されます。大半のデータは必要に応じて使用するので、常にローカルドライブに保存する必要はありません。データのアーカイブによって、よく使用するファイルのために空き領域を解放できます。
- **クラウドアーカイブとローカルアーカイブ**
  アーカイブの保存先の種類として Acronis Cloud またはローカルストレージ（内部ハードドライブ、外付けハードドライブ、NAS、USB フラッシュドライブなど）を選択できます。保存先として Acronis Cloud を選択するたびに、選択されたデータが同一のクラウドアーカイブに保存されます。新しくアーカイブを作成する代わりに既存のアーカイブを選択することができますが、ローカルアーカイブは互いに独立しており、それぞれ異なる名前、保存先、暗号化の設定などが可能です。ローカルアーカイブの数は制限されていません。
- **すべてのデバイスからクラウドアーカイブへ簡単にアクセス**
  Acronis Cloud にファイルをアーカイブした場合、Acronis Cyber Protect Home Office、Acronis Cyber Protect Home Office モバイルアプリケーション、および Acronis Cloud Web アプリケーションを使用してファイルにアクセスすることができます。これらのアプリケーションは、Windows、macOS、iOS および Android（タブレットとスマートフォン）のデバイスで利用可能です。
- **クラウドアーカイブでのデータ保護**
  Acronis Cloud に保存したデータは、破損や災害から保護されます。たとえば、ローカルのハードドライブでエラーが発生した場合、ファイルを新しいハードドライブにダウンロードできます。また、データは暗号化された状態で保存されます。他のユーザーにデータにアクセスされないようにすることができます。
- **ファイルの共有**

Acronis Cloud にファイルをアップロードすると、公開リンクを作成できます。このリンクは、友人とファイルを共有したり、フォーラムやソーシャルネットワークに投稿したりするときに使用できます。

- **ファイルバージョン**
  ファイルの編集と Acronis Cloud へのアップロードを繰り返した場合、Acronis Cyber Protect Home Office ではそれぞれのファイルバージョンでの変更がすべて保持されます。前のバージョンのファイルを選択して、デバイスにダウンロードすることが可能です。

アーカイブから除外されるもの

アーカイブのサイズを縮小し、システムの破損のおそれをなくすため、Acronis Cyber Protect Home Office では、デフォルトで、以下のデータをアーカイブの対象外としています。

- pagefile.sys
- swapfile.sys
- Tempフォルダ
- System Volume Informationフォルダ
- ごみ箱
- ウェブブラウザの一時データ:
  - インターネット一時ファイル
  - キャッシュ
- .tibx ファイル
- .tib.metadataファイル
- .tmp ファイル
- .~ ファイル

完全なファイルリストについては、ナレッジベースの記事 https://kb.acronis.com/content/58297 を参照してください。

クラウドアーカイブとオンラインバックアップ

Acronis Cloud へのデータのアーカイブは、オンラインバックアップと似ていますが、多くの相違点があります。

	オンラインバックアップ	クラウドアーカイブ
機能の目的	オペレーティングシステムの破損、ハードウェア障害、個別ファイルの紛失からのデータの保護。	ローカルストレージデバイスのクリーンアップおよび Acronis Cloud へのデータの移動。
データの保護	• コンピュータ上の各データの全体的な保護（特にオペレーティングシステム）。 • 使用頻度の高いファイルの保護。	使用頻度の低いファイルや古いファイル（個人的なドキュメントや写真など）の保護。
ソース	手動選択。	自動的に検出されたファイルを手動で選択。

	オンラインバックアップ	クラウドアーカイブ
データの選択		
ソースデータの処理	ソースデータは元の場所に保持。	ソースデータは元の場所から削除。このことにより、ハードドライブやラップトップが盗難被害にあっても、データが不正に操作されることはありません。
データの編集頻度	編集頻度が高いデータの場合はバックアップ。通常、データのアップデートに応じて、バックアップは複数のバージョンが存在します。	ほとんど編集しないデータの場合はアーカイブ。ファイルは、ほとんどの場合、バージョンが作成されません。

データのアーカイブ作成

データのアーカイブ機能により、古いファイルや使用頻度の低いファイルを Acronis Cloud またはローカルストレージに移動して、ストレージスペースを解放することができます。詳細については、「データのアーカイブについて」を参照してください。

データのアーカイブを作成するには、次の手順を実行します。

1. Acronis Cyber Protect Home Office を起動して、**[アーカイブ]** セクションに移動します。
2. （オプションの手順）データのアーカイブ作成機能の概要を確認する場合は、[はじめに] のスライドを表示します。
3. 次のいずれかを実行します。
   - デフォルトのWindowsのユーザーフォルダ（通常、C:¥Users¥[ユーザー名]）のファイルを分析するには、**[ホームフォルダの分析]** をクリックします。
   - カスタムフォルダ内のファイルを分析するには、下矢印をクリックし、**[他のフォルダを選択]** をクリックして、分析するフォルダを選択します。

   Acronis Cyber Protect Home Office では、コンピューター上のファイルが分析されます。この処理には数分かかる場合があります。
4. 左側の領域でデータカテゴリを選択します。次に、右側の領域で、アーカイブするファイルやフォルダを選択します。

   検出されたファイルを選択すると、ファイルのサイズや日時（最終更新日）などで並べ替えることができます。ファイルを並べ替えるには、適切な列ヘッダーをクリックします。
5. **[ターゲットの選択]** をクリックし、Acronis Cloud、またはアーカイブ対象ファイル用にカスタマイズしたローカルの保存先を選択します。
6. （オプションの手順）**[オプション]** をクリックして、**[データセンター]** や **[暗号化]** などのアーカイブオプションを設定します。詳細については、「データのアーカイブ用オプション」を参照してください。
7. **[アーカイブ]** をクリックします。
8. アーカイブにファイルが移動されると、ファイルはコンピュータから自動的に削除されます。

さらに、https://goo.gl/eEkNj2 のビデオ解説（英語）をご覧ください。

データのアーカイブ用オプション

データセンター

Acronis Cloud にファイルをアーカイブすると、各国の Acronis データセンターの 1 つにファイルがアップロードされます。はじめに、データセンターは、Acronis アカウントの作成時の場所に最も近い場所が指定されます。デフォルトではそれ以降、アーカイブされたファイルは同一のデータセンターに保存されます。

他の国に居住している場合、またはデフォルトのデータセンターが現在地から最も近い場所ではない場合、アーカイブ用のデータセンターを手動で設定することをおすすめします。データ アップロード速度を大幅に高めることができます。

注意
アーカイブ処理の開始後にデータセンターを変更することはできません。

データセンターを選択するには、次の手順を実行します。

1. 最初にアーカイブ処理を設定する際に、**[オプション]** をクリックします。
2. 現在地から最も近い国を選択します。

暗号化

アーカイブされたデータを不正アクセスから保護するために、アーカイブを業界標準のAES（Advanced Encryption Standard）暗号化アルゴリズムで256ビットの長さのキーを使用して暗号化できます。

注意
既存のアーカイブのアーカイブ暗号化オプションを設定または変更することはできません。

アーカイブを暗号化する手順は、次のとおりです。

1. 最初にアーカイブ処理を設定する際に、**[オプション]** をクリックします。
2. **[AES-256アルゴリズムを使用してアーカイブを暗号化]** チェックボックスをオンにします。
3. アーカイブ用のパスワードを対応するフィールドに入力します。パスワードはできる限り想像しにくいものにするため、8文字以上の、アルファベット（大文字と小文字の両方を使用することが望ましい）と数字を含むものにしてください。

   注意
   パスワードを取得することはできません。アーカイブの保護用に指定したパスワードは控えておいてください。

Acronis Cyber Protect Home Office は、アーカイブを変更するたびにパスワードの入力を要求します。アーカイブにアクセスするには、正しいパスワードを指定する必要があります。

アーカイブ済みファイルへのアクセス

ファイルが正常にアーカイブされると、次の方法でアーカイブにアクセスできます。

- **File Explorer**

  ファイルエクスプローラーを起動し、[お気に入り] の **[Acronis Drive]** をクリックします。

  ファイルは読み取り専用モードで操作できます。ファイルを変更するには、まずファイルを別のフォルダにコピーします。
- **Acronis Cloud**（クラウドアーカイブの場合のみ）

  次のいずれかの方法で、Acronis Cloud Web アプリケーションを起動します。
  - Acronis Cyber Protect Home Office を起動し、**[アーカイブ]** をクリックして、**[Web ブラウザで表示する]** をクリックします。
  - https://www.acronis.com/my/online-backup/webrestore/に移動し、アカウントにログインします。

データの共有

Acronis Cloud のバックアップおよびアーカイブに保管されているファイルおよびフォルダを共有できます。

1. Acronis Cyber Protect Home Office サイドバーで **[アカウント]** をクリックします。
2. **[Acronis Cloud Storage]** セクションで、**[データの参照]** をクリックします。
   Acronis Cloud ブラウザページにリダイレクトされます。
3. 共有する内容に応じて、次の手順を実行します。
   - バックアップからファイルまたはフォルダを共有する場合は、左サイドバーで **[バックアップ]** をクリックします。チェックマークを付けて必要なファイルまたはフォルダを選択します。
   - アーカイブからファイルまたはフォルダを共有する場合は、左サイドバーで **[アーカイブ]** をクリックします。チェックマークを付けて必要なファイルまたはフォルダを選択します。
4. 右サイドバーで、**[リンクの共有]** をクリックしてください。
5. [オプション] 共有オプションを設定できます。これを行うには、リンクウィンドウで **[リンクの設定]** をクリックします。パスワードを適用し、有効期限を設定し、ダウンロードの量を制限することができます。
6. リンクウィンドウで、**[リンクのコピー]** をクリックし、それを閉じます。

これで、このリンクを共有できるようになります。共有ファイルを表示するには、左サイドバーで **[共有]** をクリックします。ここで任意のファイルを選択し、右側のサイドバーでそのリンクをコピーしたり、リンク設定を構成したり、削除したりすることができます。

家族間のデータ保護

家族間のデータ保護とは

家族間のデータ保護は、クロスプラットフォーム統合ソリューションであり、同一アカウントで共有するすべてのコンピュータ、スマートフォン、およびタブレットの保護ステータスを追跡および制御することができます。これらのデバイスのユーザーは同じアカウントにサインインする必要があるため、通常は家族の全員がユーザーになります。通常、家族の全員がこの機能を使用できますが、家族の中には技術的な経験をお持ちの方がいることも多くなっています。そのため、その方が家族のデータを保護するのに適任と言えます。

複数のデバイスの保護状況の追跡および制御には、ウェブベースのオンラインダッシュボードを使用します。これはインターネットに接続しているコンピュータであればアクセスが可能です。このウェブアプリケーションを使用して、ご家庭でも次のようなIT管理を実行できます。

- Windows、macOS、iOS、および Android が動作する、ご家庭内のすべてのデバイスのバックアップの現状を管理。
- 新しいデバイスをリストに追加。
- 任意のコンピュータで任意のバックアップを手動で起動。
- 任意の種類（コンピュータ全体、ファイルレベル、ディスクレベル）の新しいバックアップをWindowsおよびMacに作成。
- 既存のバックアップの設定を変更。
- Acronis Cloud にある任意のバックアップ（Windows、Mac、および iOS や Android を実行しているデバイスからのバックアップなど）からデータをリカバリ。
- 製品に関連する問題の一部を解決。

Web管理画面への新しいデバイスの追加

バックアップのリモート管理などのWeb管理画面のメリットをすべて活用するには、最初にデバイスをデバイスリストに追加する必要があります。

新しいデバイスを追加する手順は、次のとおりです。

1. デバイスに Acronis Cyber Protect Home Office をインストールします。
   - Windows および macOS 用のインストールファイルは、Acronis の Web サイトでダウンロードできます。
   - Acronis Cyber Protect Home Office を iOS および Android デバイスにインストールするには、「Acronis Cyber Protect Home Office モバイルアプリのインストール」に記載されている手順に従います。
2. Acronis Cyber Protect Home Office を起動して、ご自身のアカウントにサインインします。

また、Web管理画面インターフェイスを使用してデバイスを追加することもできます。

オンラインダッシュボードを使用して新しいデバイスを追加する手順は、次のとおりです。

1. 追加するデバイスから、Web管理画面（https://cloud.acronis.com）を開きます。
2. ご自身のアカウントでサインインします。
3. **[リソース]** タブで **[追加]** をクリックします。
4. Acronis Cyber Protect Home Office をダウンロードしてインストールします。
5. Acronis Cyber Protect Home Office を起動し、同じ Acronis アカウントにサインインします。

データのリモートバックアップ

Web ベースのオンラインダッシュボードを使用して、同じアカウントを共有している任意のコンピューター（Windows または Mac）のバックアップを設定および実行できます。

バックアップを行う前に、次の手順を実行して、コンピューターにアクセスできることを確認します。

1. https://cloud.acronis.comでWeb管理画面を開きます。
2. ご自身のアカウントでサインインします。
3. **[リソース]** タブで、バックアップするコンピュータを見つけます。
   - コンピュータが見つからない場合は、先にリストに追加する必要があります。リストに追加するには、対象のコンピューターに Acronis Cyber Protect Home Office をインストールし、アプリケーションを起動して、自身のアカウントでサインインします。詳細については、「新しいデバイスの追加」を参照してください。
   - コンピュータがオフラインの場合は、コンピュータの電源がオンになっていることとインターネットに接続されていることを確認します。

コンピューター上に最初のバックアップを作成する手順は、次のとおりです。

1. Web管理画面を開き、バックアップ対象のデータを含むコンピュータを見つけます。
2. **[バックアップを有効化する]** をクリックして、新しいバックアップの次のような項目を設定します。
   - バックアップの種類（コンピュータ全体、ディスクレベル、またはファイルレベル）
   - バックアップするデータ
   - バックアップの保存先
   - スケジュール作成
   - 保持ルール
   - データの暗号化
3. バックアップを設定したら、**[設定]** をクリックして、**[今すぐ実行]** をクリックします。

既存のバックアップの新しいバージョンを作成する手順は、次のとおりです。

1. Web管理画面を開き、バックアップ対象のデータを含むコンピュータを見つけます。
2. **[今すぐバックアップ]** をクリックして、アップデートするバックアップを選択します。

既存のバックアップの設定を変更する手順は、次のとおりです。

1. Web管理画面を開き、バックアップのソースであるコンピュータを見つけます。
2. 歯車アイコンをクリックして **[バックアップ]** をクリックし、再設定するバックアップを見つけます。

3. バックアップ名の横にある歯車アイコンをクリックして、次のいずれかをクリックします。
   - 主要な設定を変更するには、**[編集]** をクリックします。
   - その他のオプションを変更するには、**[バックアップオプション]** をクリックします。
4. **[変更を保存]** をクリックします。

新しいバックアップを作成する手順は、次のとおりです。

1. Web管理画面を開き、バックアップ対象のデータを含むコンピュータを見つけます。
2. 歯車アイコンをクリックして、**[バックアップ]** をクリックします。
3. **[バックアップ計画の追加]** をクリックします。
   - 事前定義された設定でバックアップを作成するには、**[適用]** をクリックします。コンピューター全体が Acronis Cloud にバックアップされます。
   - カスタム設定を使用してバックアップを作成するには、**[新規作成]** をクリックし、設定を変更して、**[適用]** をクリックします。
4. バックアップを開始するには、**[今すぐ実行]** をクリックします。

オンラインダッシュボードでのデータの復元

ウェブベースのオンラインダッシュボードを使用すると、複数のデバイス（Windows、Mac、スマートフォン、タブレットなど）からアップロードされた任意のオンラインバックアップでデータを復元できます。

オンラインバックアップからデータを復元するには、次の手順を実行します。

1. https://cloud.acronis.comでWeb管理画面を開きます。
2. ご自身のアカウントでサインインします。
3. **[リソース]** タブで、復元するデータのバックアップ元デバイスを見つけます。デバイスがオフラインの場合は、デバイスの電源がオンになっていることとインターネットに接続されていることを確認します。
4. データの復元元に応じて、以下の操作を行います。
   - コンピュータ: **[リカバリする]** をクリックします。Acronis Cloud Web アプリケーションが起動し、データの参照とリカバリが行えます。
   - モバイルデバイス: **[リカバリする]** をクリックします。左側のパネルで、バックアップバージョンをバックアップ日時で選択します。右側のパネルで復元する項目を選択してから、**[ダウンロード]** をクリックします。

電子メールによる通知

バックアップ操作は長時間かかる場合があります。バックアップのステータスと完了した時を追跡するには、オンラインダッシュボードでメール通知を設定します。

E メール通知を設定する手順は、次のとおりです。

1. オンラインダッシュボードでメール通知を開きます。このことは 2 つの方法で実行できます。
   - オンラインダッシュボードで、右上隅のアカウント アイコンをクリックしてから、**[メール通知]** を選択します。
   - お使いの Acronis Cyber Protect Home Office アプリケーションで、**[設定]** をクリックしてから、**[メール通知設定の変更]** をクリックします。
2. **[通知を送信する対象]** で、対象にする情報を選択します。
   - エラー
   - 警告
   - バックアップ正常終了
3. **[受信者の電子メールアドレス]** フィールドに、送信先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。
4. **[件名]** の [オプションの手順] で、メール通知の件名を変更します。
   次のような変数を使用できます。
   - [computer_name]—コンピュータの名前
   - [operation_status]—どの操作が完了したかが示されたステータス
   - [backup_name]—バックアップの名前

   デフォルトの件名は、[computer_name] - [operation_status] - [backup_name] です。

設定を保存した後、Windows と macOS を実行しているすべてのファミリーデバイスのすべてのバックアップに関する情報を Acronis サーバーから受け取ります。

保護

Acronis Cyber Protect Home Office は、以下のようなデータ保護を提供します。

- Active Protection は、通常の作業中に常にバックグラウンドで実行され、コンピュータをリアルタイムで保護します。
- ウィルス対策スキャンはオンデマンドで実行され、システム全体で不審なソフトウェアを徹底的に検出します。
- 脆弱性アセスメントは、バックグラウンドで実行される日単位のスキャンであり、システムとアプリの脆弱性を検出して、それらの重大度を評価します。

注意
この保護は、Acronis Cyber Protect Home Office UI でのみ有効または無効にできます。タスク マネージャまたは他の外部ツールを使って手動でプロセスを停止することはできません。

Active Protection をカバーするライセンスを持っていても、対応するコンポーネントがインストールされていない場合は、それを追加できます。詳細については、"Active Protection の設定"（162ページ）をご参照ください。

リアルタイム保護、ウイルス対策スキャン、ビデオ会議保護、Web フィルタリングをカバーするライセンスを持っていても、対応するコンポーネントがインストールされていない場合は、それを追加できます。詳細については、"Active Protection の設定"（162ページ） をご参照ください。

[保護] ダッシュボード

[保護] ダッシュボードには、**Active Protection**、**ウイルス対策スキャン**、および**脆弱性アセスメント**の各プロセスに関する統計データが表示され、保護ステータスの制御や保護設定へのアクセスが行えます。

[保護] ダッシュボードにアクセスするには、 サイドバーにある **[保護]** をクリックします。

ダッシュボードの **[概要]** タブでは、次の操作が行えます。

- 欠落している保護コンポーネントをインストールします。これを行うには、**[インストール]** をクリックし、表示されている指示を従います。
- Active Protection の状況に関する統計情報を表示する。
- 検出された問題数、検疫された項目数、保護の除外数を表示する。
- **ウィルス対策スキャン**の最新レポートを表示する。これを表示するには、**[スキャン レポート]** をクリックします。
- スケジュール設定された次回のスキャン時刻を表示する。
- フルまたはクイックの**ウィルス対策スキャン**を手動で実行する。これを行うには、**[フルスキャンを実行する]** または **[クイックスキャンを実行する]** をクリックします。
- 検出された脆弱性の最新レポートを表示し、そこから新しいスキャンを実行します。これを表示するには、**[検出された脆弱性]** をクリックします。

- 事前に設定した期間（30 分、1 時間、4 時間、再起動まで）、保護全体を停止します。これを行うには、**[保護の停止]** をクリックして期間を選択します。

注意
保護をオフにすると、Active Protection が無効になります。 スケジュール設定したオンデマンド スキャンは開始されません。

ダッシュボードの **[アクティビティ]** タブで、保護の状況および設定に適用した変更のログを表示できます。

Active Protection

コンピューターを悪意のあるソフトウェアからリアルタイムで保護するため、Acronis Cyber Protect Home Office は Acronis Active Protection 技術を使用します。

Active Protection は、コンピュータの通常運用中に常にチェックを行います。Acronis Active Protection は、ユーザーのファイルの他に、Acronis Cyber Protect Home Office アプリケーションファイル、バックアップ、ハードドライブのマスターブートレコードを保護します。

Active Protection は、次の複数の保護レベルで構成されており、それぞれ独立して有効化できます。

- ランサムウェア対策保護
- リアルタイム保護
- Web フィルタリング

ランサムウェア対策保護

ランサムウェアはファイルを暗号化し、暗号化キーの対価を要求します。クリプトマイニング マルウェアは、バックグラウンドで数値計算を行うことで、コンピューターの処理能力とネットワークトラフィックを盗みます。

ランサムウェア対策保護サービスが有効な場合、コンピュータで実行されているプロセスがリアルタイムで監視されます。ファイルの暗号化や暗号通貨のマイニングを試みるサードパーティのプロセスを検出すると、ユーザーに通知され、プロセスを継続するかブロックするかを尋ねられます。

プロセスによるアクティビティの継続を許可するには、**[信頼する]** をクリックします。プロセスが安全で正当なものかどうかが不明な場合は、**[検疫]** をクリックすることをお勧めします。クリックすると、プロセスは **[検疫]** に追加され、アクティビティがブロックされます。

プロセスのブロック後に、ファイルが暗号化されていないかどうか、または破損していないかどうかを確認することをお勧めします。暗号化されているまたは破損している場合には、**[変更されたファイルを復元する]** をクリックします。Acronis Cyber Protect Home Office は、リカバリする最新のファイルバージョンを次の場所から検索します。

- プロセスの検証中に前もって作成したファイルの一時コピー
- ローカルバックアップ
- クラウドバックアップ

Acronis Cyber Protect Home Office が適切な一時コピーを見つけた場合には、それからファイルを復元します。 復元する適切なファイルの一時コピーがない場合、Acronis Cyber Protect Home Office はローカルおよびクラウドからバックアップコピーを検索し、両方の場所で見つけたコピーの作成日付を比較して、使用可能な暗号化されていない最新コピーからファイルを復元します。

注意
Acronis Cyber Protect Home Office は、パスワード保護されたバックアップからのファイルの復元をサポートしていません。

プロセスのブロック後にファイルを自動的に復元するよう Acronis Cyber Protect Home Office を設定するには、Active Protection 設定で **[プロセスをブロックした後に自動的にファイルを復元する]** チェックボックスをオンにします。「Active Protection の設定」を参照してください。

リアルタイム保護

リアルタイム保護が有効な場合、ユーザーが使用するファイルを常にチェックして、疑わしいアクティビティ、ウィルス、その他の不審な危険因子からコンピューターをリアルタイムで保護します。

リアルタイム保護には、次の追加保護オプションが付属しています。

- 動作分析 - 悪意のあるプロセスを特定するために、Active Protection は動作ヒューリスティックを使用します。これは、あるプロセスによって実行された一連のアクションを、悪意のある動作パターンのデータベースに記録された一連のイベントと比較します。このアプローチにより、Active Protection はその典型的な動作によって新しいマルウェアを検出できます。
- エクスプロイト防止 - Active Protection は、マシンで実行されているプロセスの動作を分析し、異常なアクティビティを検出します。これにより、感染したプロセスが、システムにインストールされている他のソフトウェアの脆弱性を拡散して悪用するのを防ぎます。Active Protection は、いくつかのエクスプロイト防止方法を採用しています。
  - メモリ保護は、メモリページの実行権限に対する不審な変更を検出して阻止します。悪意のあるプロセスは、このような変更をページプロパティに適用して、スタックやヒープなど、実行不可能なメモリ領域からのシェルコードの実行を可能にします。
  - 権限昇格保護は、不正なコードまたはアプリケーションによって行われた特権の昇格の試みを検出して阻止します。悪意のあるコードによって権限昇格が使用され、攻撃されたマシンに完全にアクセスし、重要で機密性の高いタスクを実行します。許可されていないコードは、重要なシステムリソースへのアクセスやシステム設定の変更を行うことはできません。
  - コードインジェクション保護は、リモートプロセスへの悪意のあるコードインジェクションを検出して阻止します。コードインジェクションは、アプリケーションの悪意をクリーンプロセスまたは良性プロセスの背後に隠して、マルウェア対策製品による検出を回避するために使用されます。

次のようなスキャンの種類からいずれかを選択できます。

- **スマートオンアクセス**検出では、プログラムがバックグラウンドで実行され、システムの電源が入っている間、ウイルスやその他の悪意のある脅威がないか、アクティブかつ継続的にマシンシステムがスキャンされます。マルウェアは、ファイルが実行されているとき、およびファイルを開いて読み取り/編集を行うなどのさまざまな操作中に検出されます。

- **実行時** 検出では、実行可能ファイルのみが実行時にスキャンされ、それらがクリーンで、マシンやデータにいかなる損傷も与えないことが確認されます。感染したファイルのコピーは気付かれません。

リアルタイム保護チェックの結果は、保護ダッシュボードの **[アクティビティ]** タブで確認できます。

Web フィルタリング

多くのマルウェアは、不審なサイトまたは感染したサイトから配信され、「ドライブバイ ダウンロード」と呼ばれる感染手法を使用します。

Web フィルタリングは、有害な可能性のある Web サイトや信頼されない Web リソースを開こうとした場合に、アクセスをブロックすることで保護します。有害な可能性のある Web サイトを判定するために、Web フィルタリングは保護の更新のデータベースを使用します。Web フィルタリングのデータベースには、詐欺およびフィッシングの URL を含む Web サイトに関する情報も含まれています。Web フィルタリングリストに例外項目を設定して、データベースに定義されているルールを変更できます。

Web フィルタリングの運用には 2 つのモードがあります。

- **[完全ブロック]** - Web サイトへのアクセスが完全にブロックされます。
- **[通知のみ]** - 通知が表示されますが、ユーザーは Web サイトにアクセスできます。

Active Protection の設定

Active Protection の設定にアクセスするには

1. サイドバーの **[保護]** をクリックしてから **[設定]** をクリックし、**[Active Protection]** タブに移動します。
2. （オプションの手順）Active Protection がインストールされていない場合、**[Active Protection とウイルス対策スキャンの取得]** の **[インストール]** をクリックしてから、表示されている指示に従います。

ランサムウェア対策保護を構成する

1. **[ランサムウェア対策保護]** をオンに切り替え、ランサムウェア対策保護を有効にします。
   有効にすると、バックグラウンドで実行される有害な可能性のあるアプリケーションやプロセスからコンピューターが保護されます。
2. 有効にするオプションを選択します。
   - **[プロセスをブロックした後に自動的にファイルを復元する]**: プロセスをブロックしても、ファイルが既に変更されている可能性があります。このチェックボックスをオンにすると、Acronis Cyber Protect Home Office は以下の手順でファイルを復元します。
     Acronis Cyber Protect Home Office は、リカバリする最新のファイルバージョンを次の場所から検索します。
     - プロセスの検証中に前もって作成したファイルの一時コピー
     - ローカルバックアップ
     - クラウドバックアップ

Acronis Cyber Protect Home Office が適切な一時コピーを見つけた場合には、それからファイルを復元します。 復元する適切なファイルの一時コピーがない場合、Acronis Cyber Protect Home Office はローカルおよびクラウドからバックアップコピーを検索し、両方の場所で見つけたコピーの作成日付を比較して、使用可能な変更されていない最新コピーからファイルを復元します。

注意
Acronis Cyber Protect Home Office は、パスワード保護されたバックアップからのファイルの復元をサポートしていません。

- **[バックアップファイルをランサムウェアから保護する]**: Acronis Cyber Protect Home Office はそれ自体のプロセスとバックアップをランサムウェアから保護します。 アーカイブも保護されます。
- **[ネットワーク共有と NAS を保護する]**: Acronis Cyber Protect Home Office は、アクセス可能なネットワーク共有と NAS デバイスを監視し保護します。ランサムウェア攻撃の影響を受けたファイルのリカバリ場所も指定できます。
- **[違法なクリプトマイニングからコンピュータを保護する]**: クリプトマイニング マルウェアからコンピューターを防御する場合に、このチェックボックスをオンにします。

3. **[OK]** をクリックします。

リアルタイム保護を設定する手順は、次のとおりです。

1. （オプションの手順）リアルタイム保護がインストールされていない場合、**[完全な保護の取得]** の **[インストール]** をクリックしてから、表示されている指示に従います。
2. **[リアルタイム保護]** をオンに切り替え、リアルタイム保護を有効にします。
   有効にすると、リアルタイム保護により、使用するすべてのファイルでマルウェアがチェックされます。
3. ファイルをチェックするタイミングを選択します。
   - **[スマートオンアクセス]**: システムのすべてのアクティビティが監視され、アクセス時にファイルがスキャンされます。
   - **[実行時]**: 実行可能ファイルのみが起動時にスキャンされ、コンピュータに悪影響がないことが確認されます。
4. 検出したオブジェクトに対する処理をドロップダウンリストから選択します。
   - **[ブロックして通知]**: マルウェアのアクティビティが疑われるプロセスをブロックし、通知します。
   - **[検疫]**: マルウェアのアクティビティが疑われるプロセスをブロックし、実行可能ファイルを検疫フォルダに移動します。
5. 追加の保護オプションを有効にします。
   - **[プロセスの悪意のある動作を検出する]**: Active Protection が新しいマルウェアをその典型的な動作によって検出してブロックできるようにします。
   - **[悪意のあるプロセスがシステムのソフトウェアの脆弱性を悪用することを検出して阻止する（実験）]**: システム上の他のプロセスのバグや脆弱性を悪用しようとするプロセスを Active Protection が検出してブロックできるようにします。

注意
検出されたすべてのオブジェクトは即時にブロックされます。これらは検疫に移動されず、検出された問題のリストにも追加されません。

Web フィルタリングを設定する手順

1. （オプションの手順）Web フィルタリングがインストールされていない場合、**[完全な保護の取得]** の **[インストール]** をクリックしてから、表示される指示に従います。
2. **[Web フィルタリング]** トグルをオンに切り替え、潜在的に有害な Web サイトや信頼できない Web リソースからユーザーを保護します。
3. **[不審な URL 検出時の操作]** ドロップダウンメニューから、検出された不審な URL に対する処理を選択します。
   - **[完全ブロック]**: Web サイトへのアクセスが完全にブロックされます。
   - **[ブロックして通知]**: Web サイトはブロックされますが、続行することもできます。
4. 信頼された、またはブロックされた Web サイトのリストを設定するには、**[例外を管理する]** をクリックします。
   a. 新しい URL をリストに追加するには、**[URL の追加]** をクリックします。
   b. 有効な URL 名を入力します。そのドメインは例外に追加されます。

   注意
   入力したドメインのすべてのアドレスが信頼またはブロックの対象として扱われます。たとえば、信頼されたドメインとして xyz.com を入力すると、xyz.com のすべてのパスやサブドメインが信頼として扱われます。

   c. ドロップダウンメニューから、**[許可]** または **[ブロック]** を選択します。許可された Web サイトの危険因子はスキャンされません。ブロックされた Web サイトは開かないか、開こうとすると通知が届きます。
   d. **[URL の追加]** をクリックします。
   e. **[適用]** をクリックします。

ウィルス対策スキャン

ウィルス対策スキャンは、Acronis Cyber Protect Home Office のウィルス対策保護およびマルウェア対策保護のコンポーネントの 1 つです。オンデマンド（手動または事前に設定した間隔）でマルウェアをチェックすることにより、コンピュータを保護します。

2 種類のスキャンから選択できます。

- **フル**スキャンはコンピュータ全体でウィルスをチェックします。フルスキャンは、除外リストで定義した除外ファイルまたはフォルダを除く、すべてのファイルとプロセス（またはファイルとプロセスのサブセット）を検証して、マルウェアを検出します。
- **クイック**スキャンは特定のファイルやフォルダのみをチェックします。クイックスキャンは、ウィルスが存在する可能性の高い特定のフォルダを検証して、マルウェアを検出します。

また、アーカイブファイル、外部ドライブ、新規および変更されたファイルのみといった、スキャン対象も選択できます。

注意
スキャン処理の実行時にスリープモードまたは休止モードに入らないよう Acronis Cyber Protect Home Office を設定できます。デフォルトでは、このオプションが選択されていることに注意してください。

CPU 負荷が高い場合、デフォルトではウィルス対策スキャンの優先度が下げられ、他のアプリケーションが適切に実行されるようにします。これによりスキャンが遅くなります。このオプションを無効にすると、スキャンを速くすることができます。

ウィルス対策スキャンの詳細を含む **[スキャンの詳細レポート]** ウィンドウを表示するには、**[スキャンレポート]** ボタンをクリックします。

ウィルス対策スキャンの設定

ウイルス対策の設定にアクセスするには、サイドバーの **[保護]** をクリックした後に **[設定]** をクリックして、**[ウイルス対策]** タブに移動します。

検出時の操作を設定する手順は、次のとおりです。

有効にするオプションを選択します。

- **[検疫]** - デフォルトではこのオプションが設定されています。Acronis Cyber Protect Home Office がマルウェアの可能性のある危険因子を検出すると、プロセスを停止し、疑わしいファイルを検疫フォルダに移動します。
- **[通知のみ]** - 疑わしいプロセスを検出すると、マルウェアの可能性のある危険因子についての情報がユーザーに通知されます。

スキャン タイプを設定する手順は、次のとおりです。

実行するスキャン タイプを選択します。

- **[完全]** - デフォルトではこのオプションが設定されています。Acronis Cyber Protect Home Office はコンピュータ全体をチェックします。
- **[クイック]** - Acronis Cyber Protect Home Office は危険因子を含む可能性の高い特定のフォルダのみをチェックします。

ウィルス対策スキャンのスケジュールを設定する手順は、次のとおりです。

いずれかのチェックボックスをオンにして、スキャン プロセスの開始時刻を設定します。

- **[日単位]** - 毎日特定の時刻にスキャンを実行します。
- **[週単位]** - 週の特定の曜日にスキャンを実行します。曜日と時刻を設定します。
- **[月単位]** - 月の特定の日にスキャンを実行します。
- **[システムの起動時]** - オペレーティングシステムが起動するたびにスキャンを実行します。
- **[スケジュールを設定しない]** - 特定時刻でのスキャンの実行を設定しません。

スキャン対象を設定する手順は、次のとおりです。

次のチェックボックスをオンにします。

- **[これより大きいアーカイブ ファイルをスキャンしない]**。矢印を使用して値を選択します。
- **[外部ドライブをスキャン]**
- **[ネットワーク共有と NAS をスキャン]**
- **[新しいファイルと変更されたファイルのみスキャン]**

ウィルス対策スキャン中のシステムの動作を設定する手順は、次のとおりです。

ウィルス対策スキャンが完了する前にシステムがシャットダウンされることがあります。そのような場合には、**[起動時に未実行のタスクを実行]** チェックボックスをオンにして、Acronis Cyber Protect Home Office がシステムの起動時にスキャンを再開するよう設定します。

さらに、**[スリープモードまたは休止モードを抑制]** オプションを有効にすれば、スキャン処理の実行中にコンピューターがシャットダウンしないようにできます。

CPU の負荷が大きい場合にウィルス対策スキャンの優先度を下げて、他のアプリケーションが適切に実行されるようにできます。このオプションはデフォルトで有効ですが、スキャン速度は遅くなります。スキャン速度を速くするには、**[他のアプリケーションを優先する]** チェックボックスをオフにします。

ウィルス対策スキャンを設定したら、**[OK]** をクリックします。

脆弱性アセスメント

脆弱性アセスメントは、Acronis Cyber Protect Home Office のウィルス対策保護およびマルウェア対策保護のコンポーネントの 1 つです。これは、バックグラウンドで実行される日単位のスキャンであり、システムとアプリの脆弱性を検出して、それらの重大度を評価します。必要に応じて、スキャンを手動で実行することもできます。

注意
脆弱性データベースを更新するには、安定したインターネット接続が必要です。

脆弱性を表示するには、以下を実行します。

1. 左サイドバーで **[保護]** をクリックします。
2. **[脆弱性アセスメント]** の **[概要]** タブで、**[検出された脆弱性]** をクリックします。レポートが表示されます。
3. 新規スキャンを実行するには、**[スキャンの実行]** をクリックします。
4. （オプション） **[詳細情報]** ウィンドウを表示するには、脆弱性の名前の横にある情報アイコンをクリックします。
5. （オプション） 脆弱性の詳細情報を表示するには、その名前の横にある矢印をクリックします。この情報を含む Web ページが表示されます。
6. 検出された問題を解決するには、影響を受けるアプリケーションの最新の更新をインストールします。次に、もう一度スキャンして、脆弱性が修正されていることを確認します。それらが解消されない場合は、それはいくつかのアプリがまだシステムが危険にさらされるかもしれないことを意味します。データを完全に保護するには、オペレーティングシステムをバックアップし、マルウェア対策保護を有効にします。

脆弱性アセスメントを構成するには、以下を実行します。

1. 左サイドバーで、**[保護]** をクリックしてから、**[設定]** をクリックします。
2. **[脆弱性アセスメント]** タブに移動し、トグルをオンまたはオフに切り替えて、脆弱性スキャンを有効または無効にします。

検出された問題の管理

ウィルス対策スキャンで検出時の処理が **[ブロックして通知]** に設定されている場合、検出された問題のリストが作成されます。このリストを確認して、信頼するか、検疫に移動するかを決定する必要があります。

検出された問題を確認して管理する手順は、次のとおりです。

1. 検出された問題にアクセスするには、次の 2 つの方法があります。
   - **[保護]** ダッシュボードで、**[検出された問題]** をクリックします。
   - **[保護]** ダッシュボードで **[設定]** をクリックし、**[詳細]** タブに移動します。
     a. （オプションの手順）リアルタイム保護、ウイルス対策スキャン、ビデオ会議保護、Web フィルタリングコンポーネントが欠落している場合、**[インストール]** をクリックし、表示される指示に従います。
     b. **[検出された問題]** で、**[管理]** をクリックします。
2. リストにある問題のチェックボックスをオンにして、処理方法を選択します。
   - 保護の除外のリストにファイルまたはプロセスを追加するには、**[信頼する]** をクリックします。

     注意
     ファイルまたはプロセスを信頼するよう選択すると、これ以降、ウイルス対策スキャンの対象から除外されます。
   - ファイルまたはプロセスを検疫に移動するには、**[検疫]** をクリックします。
3. **[閉じる]** をクリックします。

検疫内のファイルの管理

Active Protection とウィルス対策スキャンは、ブロックされたファイルを設定に基づいて検疫に移動できます。 検疫は、感染したファイルや疑わしいファイルをコンピューターとデータから切り離すために使用される、特殊なストレージです。アプリケーションファイルを検疫内に配置すると、ブロックされたアプリケーションが潜在的に有害なアクションを実行するリスクを最小限に抑えることができます。

デフォルトでは、ファイルは 30 日間検疫に保持され、その後コンピュータから削除されます。期限内に検疫内のファイルを確認して、保持するか削除するかを決定することができます。また、検疫内でのデフォルトの保持期間を変更することもできます。

検疫からファイルをリストアまたは削除する手順は、次のとおりです。

1. **[保護]** ダッシュボードで、**[検疫]** をクリックします。
2. 検疫リストで項目を選択します。

- 項目を元の場所に戻すには、**[復元]** をクリックします。
- 項目を削除するには、**[PC から削除]** をクリックします。

3. **[閉じる]** をクリックします。

検疫からファイルを自動的に削除する期間を設定する手順は、次のとおりです。

1. **[保護]** ダッシュボードで **[設定]** をクリックし、**[詳細]** タブをクリックします。
2. **[検疫]** セクションで、検疫された項目を保持する日数を選択します。
3. **[OK]** をクリックします。

保護の除外の設定

Active Protection とウィルス対策スキャンは、保護データベースにある定義を使用して、可能性のある危険因子を識別します。実行可能ファイルやフォルダを信頼する場合には、それらを保護の除外リストに追加すれば、Acronis Cyber Protect Home Office にスキャンをスキップさせることができます。

注意
リアルタイム保護、ウイルス対策スキャン、Web フィルタリングのコンポーネントがインストールされていない場合、実行可能ファイルはフォルダではなく、[保護の除外] にのみ追加できます。

このコンポーネントをインストールすると、既存の Active Protection の除外がウイルス対策スキャンにも適用されます。

ファイルまたはフォルダを保護の除外リストに追加する手順は、次のとおりです。

1. **[保護]** ダッシュボードで、**[保護の除外]** をクリックします。
2. **[除外の追加]** メニューから、除外対象を選択します。
   - **[ファイルの追加]** - 実行可能ファイルやその他のファイルをスキャンおよび Active Protection から除外します。
   - **フォルダの追加** - （オプション。リアルタイム保護、ウイルス対策スキャン、Web フィルタリングのコンポーネントがインストールされている場合）フォルダをスキャンおよび Active Protection から除外します。
3. 除外する項目を参照して、**[開く]** をクリックします。
4. 除外する別の項目を追加するか、**[保存]** をクリックしてリストを更新します。

保護の除外リストからファイルまたはフォルダを削除する手順は、次のとおりです。

1. **[保護]** ダッシュボードで、**[保護の除外]** をクリックします。
2. 保護の除外リストで、削除する項目のチェックボックスをオンにして、**[削除]** をクリックします。
3. **[保存]** をクリックして、リストを更新します。

Web フィルタリングの保護の除外を設定する手順については、「Active Protection の設定」を参照してください。

ビデオ会議アプリ保護

Zoom、Cisco Webex Meetings、Microsoft Teams は、Web 会議や打ち合わせのために広く使用されています。Acronis Cyber Protect Home Office によるランサムウェア対策機能は、これらのコラボレーションアプリケーションを以下のようにしてデフォルトで保護します。

- コードインジェクションからアプリケーション プロセスを保護
- アプリケーション プロセスによる疑わしい操作を阻止

保護の更新のダウンロード

デフォルトで、Acronis Cyber Protect Home Office は保護の更新を自動的にダウンロードします。保護のデータベースとコンポーネントの状況を確認したり、保護の更新の自動ダウンロードを無効にしたりできます。

保護の更新の状況を確認する手順は、次のとおりです。

1. **[保護]** ダッシュボードで **[設定]** をクリックし、**[詳細]** タブをクリックします。
2. 下にある**[保護の更新]** セクションに移動します。
   セクションの下部に、最新のデータベース バージョンとダウンロード日付が表示されます。

保護の更新の自動ダウンロードを無効にする手順は、次のとおりです。

注意
保護の効果を最大にするためにも、保護の自動更新を無効にすることはお勧めできません。

1. **[保護]** ダッシュボードで **[設定]** をクリックし、**[詳細]** タブをクリックします。
2. 下にある**[保護の更新]** セクションに移動します。
3. **[保護の更新を自動的にダウンロードする]** チェックボックスをオフにします。

最新の保護の更新をダウンロードする手順は、次のとおりです。

保護の更新の自動ダウンロードが無効な場合、手動で更新を確認してダウンロードできます。

1. **[保護]** ダッシュボードで **[設定]** をクリックし、**[詳細]** タブをクリックします。
2. 下にある**[保護の更新]** セクションに移動します。
3. **[更新の確認]** をクリックします。このオプションは、**[保護の更新を自動的にダウンロードする]** チェックボックスが選択されていない場合にのみ、使用可能です。
4. 保護の更新が最新でない場合には、**[アップデート]** をクリックします。

データの同期

同期機能について

同期機能の主な利点

- すべてのコンピュータで同じデータ（ドキュメント、写真、ビデオなど）を保持できます。いつでもどこでも簡単にデータを利用できます。ファイルを電子メールで自分に送ったり、常に USB ドライブを携帯したりする必要はなくなります。
- 必要な数だけ同期を作成することができます。
- Acronis Cloud は同期されたファイルおよびそれらのファイルのバージョンを維持します。これにより、必要なときにいつでも前のファイルのバージョンに戻すことができます。

  注意
  この機能を使用するには、Acronis Cloud Storage サブスクリプションが必要になります。詳細については、サブスクリプション情報を参照してください。

- また、アプリケーションをインストールせずにウェブ ブラウザを使用して Cloud にアクセスすることもできます。
- 2 つ以上のコンピューター間の同期を直接作成するときには、Acronis Cloud サブスクリプションは必要ありません。

同期可能な対象と不可能な対象

2 つ以上のフォルダに保存されたデータは、同期することができます。これらのフォルダを配置できる場所、およびその場所に格納できるデータについて考えてみましょう。

ストレージの種類

同期処理は、次の対象の間で実行できます。

- 2 台以上のコンピュータにある 2 つ以上のフォルダ。
- 1 台以上のコンピューターと Acronis Cloud。
  Acronis Cloud には常に同期されたファイルの最新バージョンが含まれます。また、同期に参加する Acronis Cloud のフォルダは選択できません。そのようなフォルダは自動的に作成されます。

1 回の同期処理では、コンピュータごとに 1 つの同期フォルダを割り当てることができます。

注意
1 つのファイルのみ同期用に選択することはできません。ファイルを同期するには、該当のファイルが入っているフォルダを選択します。

データの種類

次のデータを同期することができます。

- 以下に示すファイルを除く、すべてのファイル（写真、音楽、ビデオ、ドキュメントなど）

  注意
  ネイティブの FAT32 および NTFS ファイル属性のみが同期されます。同期されるフォルダが異なるファイル システムに属している場合、両方のファイル システムでサポートされる属性のみが同期されます。

- 同期フォルダ内のその他のフォルダ（つまり、同期サブフォルダ）とその内容

次のデータは同期することができません。

- ディスクとパーティション
- システム ファイルとフォルダ
- 隠しファイルとフォルダ
- 一時ファイルとフォルダ
- システム レジストリ
- データベース
- 電子メール プログラムのデータ（Microsoft Outlook およびその他のプログラムを含む）
- 個別のファイルまたはフォルダとして表現できないその他のデータ（たとえば、アドレス帳の連絡先など）
- Windowsライブラリ（ドキュメント、ミュージックなど）

同期アイコン

同期の操作をしている間は特別なアイコンが表示されます。各アイコンは次の情報を示します。

- 同期の種類と現在の状態（このアイコンは通知領域に表示されます）。
- 同期されたファイルとフォルダの現在の状態（このアイコンはFile Explorerに表示されます）。

通知領域

同期の状態のアイコン:

アイコン	説明
	同期が通常モードで動作しています。
	同期が一時停止されています。
	前回の同期でエラーが発生しました。

File Explorer

ファイルとフォルダの同期状態アイコン:

アイコン	説明
	ファイルまたはフォルダが同期されています。
	ファイルまたはフォルダは現在同期中です。
	エラーのためにファイルまたはフォルダが同期されていません。

同期されるフォルダの同期の種類アイコン:

アイコン	説明
	Acronis Cloud と同期します。
	ローカルエリアネットワークを介して同期されるコンピュータ間の同期。

同期の作成

同期の新規作成を開始する前に、次の条件が満たされていることを確認してください。

- Acronis アカウントを持っている。
- 同期に Acronis Cloud を含める場合は、Acronis Cloud ストレージへのサブスクリプションが必要です。詳細については、「"サブスクリプション情報"（35ページ）」を参照してください。
- Acronis Cyber Protect Home Office または Acronis True Image（2012 以降）のバージョンがすべてのコンピューターにインストールされている。
- ローカルの接続が確立されている（LAN 経由でコンピュータを接続する場合）。
- すべてのコンピュータがインターネットに接続できる。

ファイルやフォルダを同期する手順は、次のとおりです。

1. サイドバーで **[同期]** をクリックします。
2. サインインしていない場合は、Acronis アカウントの資格情報を入力してください。
3. **[同期の追加]** をクリックします。
4. 新しい同期に Acronis Cloud を含めるかどうかを決定し、適切な同期の種類を選択します。
5. 同期するフォルダを選択し、**[OK]** をクリックします。
6. この同期に参加するには、他のコンピューターで Acronis Cyber Protect Home Office を起動し、同期セクションでこの同期を選択し、**[同期に参加]** をクリックして、同期するフォルダを選択します。

同期されるファイルのバージョン

Acronis Cyber Protect Home Office では、同期の結果としてファイルに適用された変更を元に戻すことができます。一部のファイルに不適切な変更が適用されたとわかった場合は、そのファイルの以前の

バージョンを参照し、正しいバージョンを選択して、そのバージョンにロールバックできます。詳細については、「以前のファイル バージョンへの復帰」を参照してください。

すべてのバージョンは Acronis Cloud に保存され、インターネット経由でアクセスできます。Acronis Cloud を使用するには、Acronis Cloud サービスのサブスクリプションが必要です。詳細については、サブスクリプション情報を参照してください。

古いバージョンを削除するには、Acronis Cloud の Web アプリケーションでクリーンアップ操作を行ってください。詳細については、「Acronis Cloud で領域をクリーンアップする方法」を参照してください。

警告
Acronis Cyber Protect Home Office の試用版を使用している場合、試用期間が切れると、保存されているすべてのバージョン（最新バージョンを含む）が Cloud から削除されます。

以前のファイルバージョンへの復帰

同期の履歴を Acronis Cloud に保存している場合、現在のバージョンの同期ファイルを以前のバージョンに戻すことができます。望ましくない同期処理を一部取り消す場合は、この方法が役立ちます。

以前のファイルバージョンに戻すには、次の手順に従います。

1. **[同期]** セクションで必要なファイルを含む同期ボックスを見つけます。**[Acronis Cloud]** リンクをクリックします。
2. 同期項目のリストがWebブラウザに表示されたら、前のバージョンに戻すファイルを選択します。右側の歯車アイコンをクリックします。表示されるメニューで **[バージョンの表示]** を選択します。
3. ロールバックするバージョンを選択します。バージョンの正確な日付と時刻が表示されます。現在のバージョンは、その時点における状態に戻されます。
4. **[復元する]** をクリックして続行します。選択したバージョンがCloudの最新バージョンになります。次に、同期を所有しているコンピュータにダウンロードされます。

削除されたファイルをリカバリする方法

誤って同期からファイルを削除することがあります。その場合、削除してしまったファイルをリカバリする必要があります。Acronis Cloud にファイルのバージョンが保持されている同期では、この処理を実行できる場合があります。

ただし、削除されたファイルが Cloud のクリーンアップ中に完全に削除されていないことが条件になります。

削除されたファイルをリカバリする手順は、次のとおりです。

1. Acronis Cyber Protect Home Office を開始します。
2. サイドバーの **[同期]** をクリックし、リカバリ対象のファイルが含まれる同期を選択して、**Acronis Cloud** のリンクをクリックします。
3. **[ファイル]** タブをクリックし、削除したファイルが含まれていた同期を選択します。
4. 同期を選択すると、ファイルとフォルダのリストが表示されます。

5. **[削除済みを表示]** チェックボックスをオンにし、リカバリする削除済みファイルを選択します。
6. **[リカバリする]** ボタンをクリックして、削除したファイルを元のフォルダにリカバリします。

同期の削除

1. サイドバーで **[同期]** をクリックします。
2. サインインしていない場合は、Acronis アカウントの資格情報を入力してください。
3. 同期リストから、削除する同期を選択し、矢印アイコンをクリックして **[削除]** をクリックします。

この操作では、同期されたフォルダ間のリンクが解除されるだけです。同期されていたファイルは元の場所に残り、どんな方法でも変更されなくなります。

ディスクのクローン作成と移行

これは、1 つのディスク ドライブの内容全体を別のディスク ドライブにコピーする処理です。たとえば、容量の大きい新しいディスクに、オペレーティング システム、アプリケーション、データのクローンを作成する場合、この処理が必要になることがあります。このことは 2 つの方法で実行できます。

- ディスクのクローン作成ユーティリティを使用する方法。
- 古いディスクドライブをバックアップし、その後新しいディスクドライブに復元する方法。

以下も参照してください: バックアップとディスクのクローン作成の違い

ディスクのクローン作成ユーティリティ

ディスクのクローン作成ユーティリティを使用すると、ディスクのパーティションを別のハードディスクにコピーして、ハードディスクドライブのクローンを作成できます。

開始する前に:

- 容量の大きいハードディスクにシステムのクローンを作成する場合は、転送先の（新しい）ドライブをクローンを使用する場所に取り付け、転送元のドライブを別の場所（外付けのUSBエンクロージャなど）に取り付けることをおすすめします。これは特にラップトップ コンピュータの場合に重要です。

  注意
  古いハードディスクドライブと新しいハードディスクドライブは同じコントローラーモード（IDE、AHCI など）で動作させることをお勧めします。モードが異なる場合、新しいハードドライブからコンピュータを起動できなくなる可能性があります。

  注意
  Windows を使用して、外付け USB ハードドライブにディスクのクローンを作成した場合、そこから起動できない場合があります。代わりに、内蔵 SSD または HDD にクローンを作成することをお勧めします。

- ディスクのクローン作成ユーティリティは、マルチブートシステムをサポートしていません。
- プログラムの画面では、破損したパーティションの左上の隅に、赤い丸に白い「x」のマークが付きます。クローン作成を開始する前に、適切なオペレーティングシステムツールを使用して、ディスクにエラーがないかどうかを調べ、エラーがあれば修正する必要があります。
- 安全措置として、元のディスク全体のバックアップを作成することを強くお勧めします。それによって、クローン作成中に元のハードディスクに問題が発生した場合でも、データは安全に守られます。そのようなバックアップを作成する方法の詳細は、「パーティションとディスクのバックアップ」を参照してください。バックアップを作成したら、確実にベリファイしてください。

ディスクのクローン作成ウィザード

開始する前に、ディスクのクローン作成ユーティリティ に関する一般的な情報を参照しておくことをお勧めします。UEFI コンピュータを使用しており、ブータブルメディアからクローン作成処理を開始する

ことにした場合、UEFI BIOS のブータブルメディアの起動モードに注意してください。起動モードはバックアップのシステムの種類と一致するようにしてください。バックアップにBIOSシステムが含まれている場合はBIOSモードでブータブルメディアを起動してください。システムがUEFIの場合は、UEFIモードが設定されていることを確認してください。

ディスクのクローンを作成する手順は、次のとおりです。

1. Acronis Cyber Protect Home Office を開始します。
2. ツールバーの **[ツール]** をクリックし、**[ディスクのクローン作成]** をクリックします。
3. **[クローン作成モード]** で、転送モードを選択します。
   - **自動**: ほとんどの場合は自動モードの使用をお勧めします。
   - **手動**: 手動モードではさまざまなデータ転送に対応できます。手動モードは、ディスク パーティション レイアウトの変更が必要な場合に役立ちます。

   注意
   ディスクが 2 つ検出されて、一方にパーティションがあり、他方にはない場合は、パーティションのあるディスクが自動的にソース ディスクとして認識され、パーティションのないディスクがターゲット ディスクとして認識されます。これに該当する場合は、以降のステップが省略され、**[概要]** 画面が表示されます。

4. **[ソース ディスク]** で、クローンを作成するディスクを選択します。

   注意
   Acronis Cyber Protect Home Office はダイナミックディスクのクローン作成には対応していません。

5. **[ターゲット ディスク]** で、クローン データの保存先ディスクを選択します。
   選択したターゲットディスクにパーティションがある場合は、パーティションの削除を確認する必要があります。実際にデータが消去されるのは、ウィザードの最後の手順で **[実行]** をクリックした場合のみです。

   注意
   パーティションが作成されていないディスクがある場合は、そのディスクが自動的に移行先と見なされるため、このステップは省略されます。

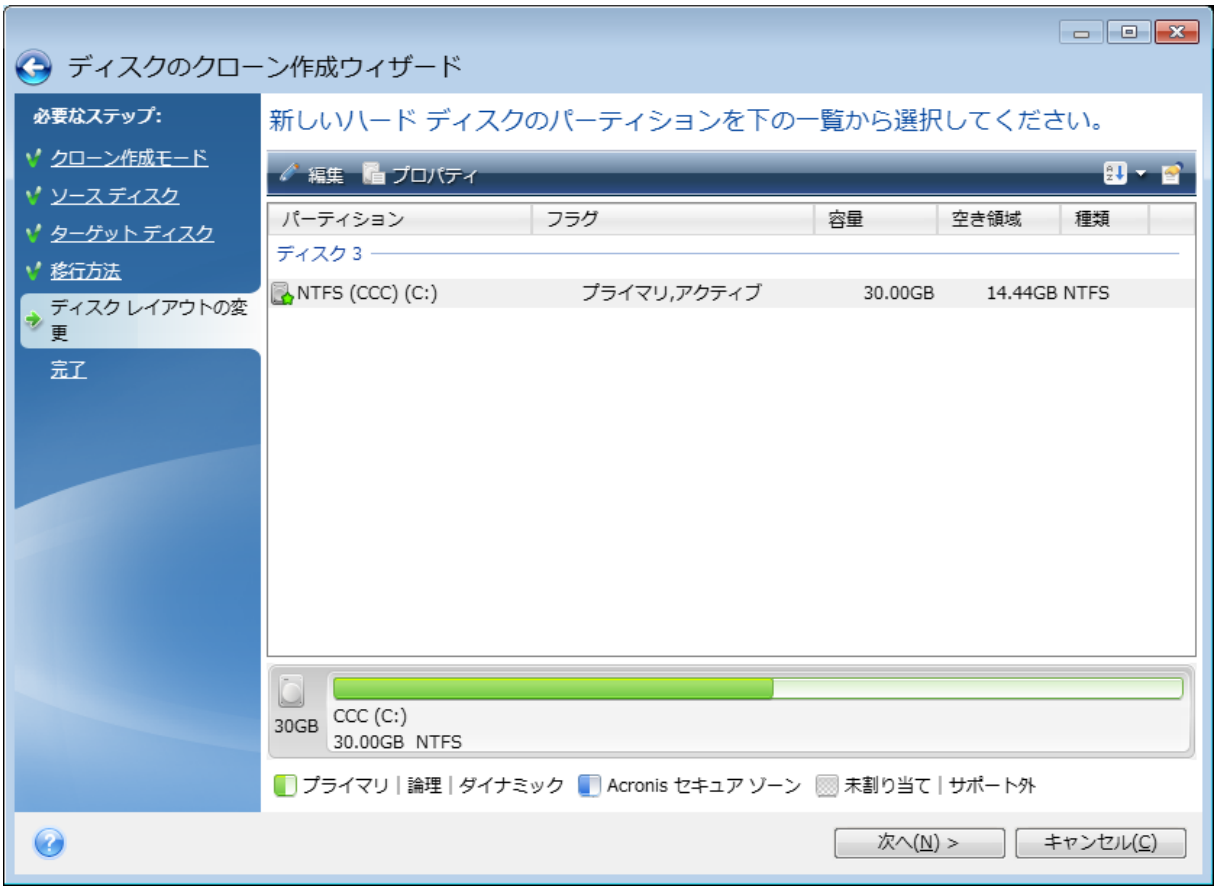
6. [この手順を使用できるのはソースディスクに OS がインストールされている場合のみです]。**[ディスクの使用状況]** の手順で、クローンを使用する方法を選択します。
   - **このマシンのディスクを交換する**: システムディスクデータがコピーされ、クローンが起動可能になります。この PC でシステムディスクを新しいものと交換するには、このクローンを使用します。
   - **別のマシンで使用する**: システムディスクデータがコピーされ、クローンが起動可能になります。このクローンを使用して、すべてのデータをブータブルディスク上の別の PC に転送します。
   - **データディスクとして使用する**: ディスクデータがコピーされます。このクローンは非ブータブルデータドライブとして使用されます。

7. [この手順を使用できるのは手動のクローン作成モードの場合のみです。][**移行方法**] で、データの移行方法を選択します。
   - **現状のまま**: 古いパーティション1つにつき1つの新しいパーティションが、同一のサイズ、種類、ファイルシステム、ラベルで作成されます。使用されない領域は未割り当てになります。
   - **移行先にあわせる**: 新しいディスク領域が、各パーティションの元の大きさに比例して配分されます。
   - **手動**: 新しいサイズとその他のパラメータを指定できます。
8. [この手順を使用できるのは手動のクローン作成モードの場合のみです。][**ディスクレイアウトの変更**] で、ターゲットディスクに作成するパーティションの設定を編集できます。詳細については、「手動パーティション操作」を参照してください。
9. [オプションの手順] [**除外する内容**] で、クローンを作成しないファイルやフォルダを指定できます。詳細については、「クローン作成からの項目の除外」を参照してください。
10. [**完了**] で、指定した設定がニーズに合っていることを確認してから、[**実行**] をクリックします。

何らかの原因でクローン作成処理が停止した場合は、処理をもう一度設定して開始する必要があります。データは消去されません。クローンの作成中に Acronis Cyber Protect Home Office によってオリジナルディスクやそこに保存されているデータが変更されることはありません。

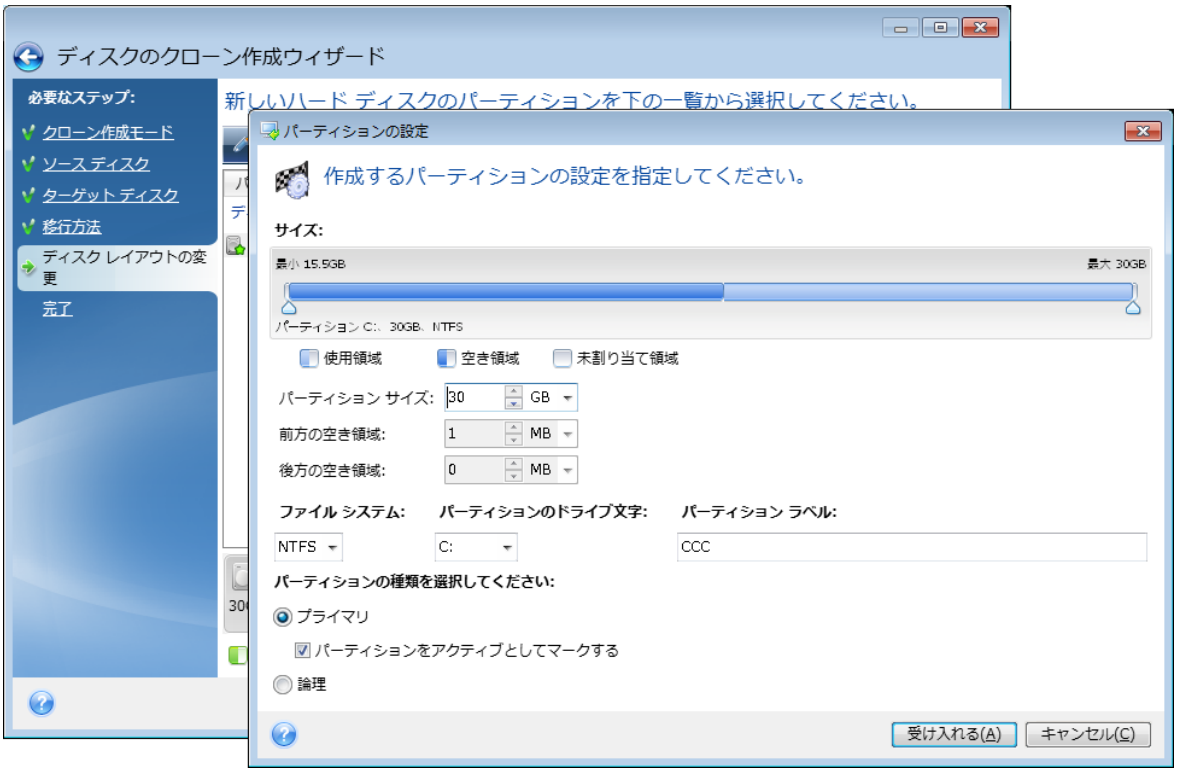
手動パーティション操作

移行方法として [手動] を選択した場合は、新しいディスクのパーティションのサイズを変更できます。デフォルトでは、ソースディスクとターゲットディスクの容量の比率に応じて、サイズが変更されます。



パーティションを編集する手順は、次のとおりです。

1. パーティションを選択し、**[編集]** をクリックします。[パーティションの設定] ウィンドウが開きます。



2. パーティション用に以下の設定を指定します。
   - サイズと位置
   - ファイル システム
   - パーティションの種類（MBRディスクでのみ使用可能）
   - パーティションのドライブ文字とラベル

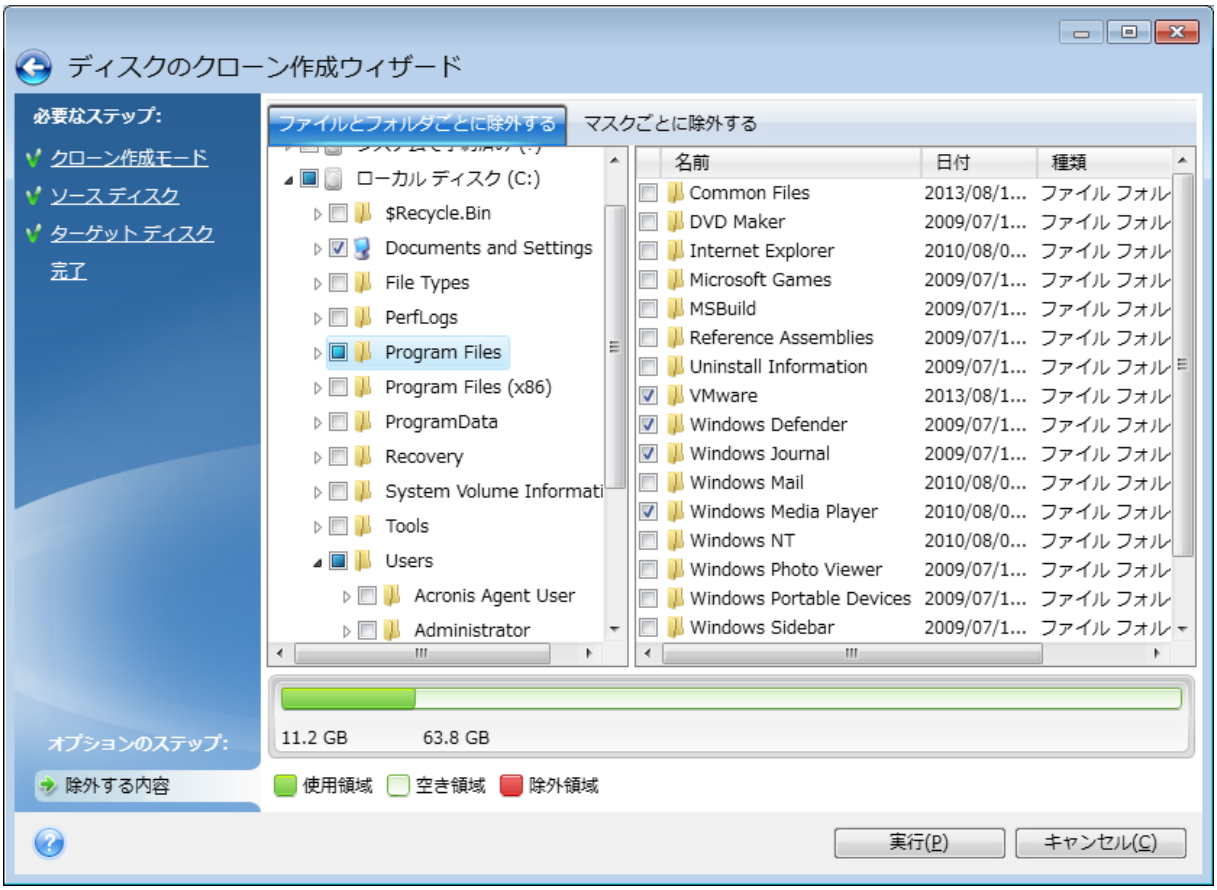
   詳細については、「パーティションの設定」を参照してください。
3. **[確定]** をクリックします。

警告
このウィンドウのサイドバーで、ウィザードの前の手順のいずれかをクリックすると、選択されたサイズと位置の変更内容がすべてリセットされるため、再度指定する必要があります。

クローン作成からの項目の除外

ソースディスクから特定のファイルのクローンを作成しない場合は（たとえば、宛先ディスクがソースディスクよりも小さい場合）、**除外するもの**ステップで、除外するものを選択できます。

注意
システムパーティションのクローンを作成する場合に、隠しファイルやシステムファイルを除外することはおすすめできません。



ファイルとフォルダを除外する方法は2つあります。

- **[ファイルとフォルダごとに除外する]** - このタブでは、フォルダツリーから特定のファイルとフォルダを選択できます。
- **[マスクごとに除外する]** - このタブでは、マスクによりファイルのグループを、名前やパスにより個々のファイルを除外できます。

  除外基準を追加するには、**[追加]** をクリックし、ファイル名、パス、またはマスクを入力し、**[OK]** をクリックします。追加できるファイルとマスクの数に制限はありません。

除外基準の例

- 明示的なファイル名を入力できます。
  - file.ext - 該当するファイルはすべてクローン作成から除外されます。
  - C:¥file.ext: C: ドライブにある file.ext ファイルが除外されます。
- 次のように、ワイルドカード文字（* および ?）を使用できます。
  - *.ext: 拡張子が .ext のファイルがすべて除外されます。
  - ??name.ext: 拡張子が .ext で、ファイル名が合計 6 文字（最初の 2 文字が任意の文字（??）で、残りの部分が name）のすべてのファイルが除外されます。
- フォルダのパスを入力できます。
  - C:¥my pictures - C: ディスクの マイピクチャ フォルダは除外されます。

右側ペインの対応するボタンを使用して、除外基準を編集および削除できます。

移行方法

Acronis Cyber Protect Home Office では、クローン作成処理完了後にターゲットディスクのパーティションレイアウトを選択できます。

- **MBR（マスター ブート セクタ）**: ディスクのプライマリ パーティション テーブルを格納するための 512 バイトのブート セクタ。ディスクの第 1 セクタです。
- **GPT（GUIDパーティションテーブル）**: 標準的なハードディスク用パーティションテーブルレイアウト。GPT では最大 9.4 ZB（9.4 x 10^21 バイト）までのディスク/パーティション サイズが可能です。

このウィザードを使用して、クローン作成処理中にパーティションレイアウトを変換したり、レイアウトを変更せずにそのままクローンを作成したりできます。

- **[変更せずにパーティションをコピー]**: このオプションを選択すると、パーティションレイアウトを変更せずに、そのままシステムを移行できます。この場合、2 TBを超えるディスク領域は使用できません。2 TB を超えるディスク領域を割り当てるには、Acronis Extended Capacity Manager を使用してください。
- **[パーティションをコピーし、システム用ではないGPTスタイルでディスクを使用する]**: このオプションを選択すると、パーティションをGPTレイアウトに変換できます。

Acronis Cyber Protect Home Office では **BIOS** から **UEFI** システムに変換することもできます。詳細については、「Unified Extensible Firmware Interface」を参照してください。

BIOSモードシステム、MBR、UEFIのサポートなし

このウィザードのステップでは、ターゲットハードディスクを選択する必要があります。

現在のシステム:

システム: BIOSモード

ソースパーティションスタイル: MBR

ソースディスクのオペレーティングシステム: Windows、UEFI起動のサポートなし

ターゲットディスクサイズ: 2 TB未満

選択したディスクにシステムを移行した場合:

システム: BIOSモード

パーティションスタイル: MBR

オペレーティングシステム: Windows、UEFI起動のサポートなし

ディスクサイズ: すべてのディスク領域が使用可能

移行手順の詳細については、「移行方法」セクションを参照してください。

BIOSモードシステム、MBR、UEFIのサポート

このウィザードのステップでは、ターゲットハードディスクを選択する必要があります。

現在のシステム:

システム: BIOSモード

ソースパーティションスタイル: MBR

ソースディスクのオペレーティングシステム: Windows、UEFI起動をサポート

ターゲットディスクサイズ: 2 TB未満

選択したディスクにシステムを移行した場合:

システム: BIOSモード

パーティションスタイル: MBR

オペレーティングシステム: Windows、UEFI起動をサポート

ディスクサイズ: すべてのディスク領域が使用可能

移行手順の詳細については、「移行方法」セクションを参照してください。

BIOSモードシステム、MBR、Windowsなし

Acronis Cyber Protect Home Office では、処理完了後にターゲットディスクのパーティションレイアウトを選択できます。

現在のシステム:

システム: BIOSモード

ソースパーティションスタイル: MBR

ソースディスクのオペレーティングシステム: Windows以外またはOSなし

ターゲットディスクサイズ: 2 TB未満

これらのシステムパラメータでは、次のいずれかを選択できます。

1. **変更せずにパーティションをコピー**

ターゲットディスクのパーティションスタイルをMBRのままにします。

移行後のターゲットディスク:

システム: BIOSモード

パーティションスタイル: MBR

オペレーティングシステム: Windows以外またはOSなし

ディスクサイズ: すべてのディスク領域が使用可能

2. **パーティションをコピーし、システム用ではないGPTスタイルでディスクを使用する**

パーティションスタイルをGPTに変換できます。

移行後のターゲットディスク:

システム: BIOS起動非対応

パーティションスタイル: GPT

オペレーティングシステム: Windows以外またはOSなし

ディスクサイズ: すべてのディスク領域が使用可能

警告
移行後、ターゲットディスクはシステム用ではないディスクとしてのみ使用できます。Acronis Cyber Protect Home Office が Windows XP x32 オペレーティングシステムで実行されている場合は、このオプションを選択できません。

移行手順の詳細については、「移行方法」セクションを参照してください。

BIOSモードシステム、GPT、UEFIサポート

このウィザードのステップでは、ターゲットハードディスクを選択する必要があります。

現在のシステム:

システム: BIOSモード

ソースパーティションスタイル: GPT

ソースディスクのオペレーティングシステム: Windows、UEFI起動をサポート

選択したディスクにシステムを移行した場合:

システム: BIOS起動非対応

パーティションスタイル: GPT

オペレーティングシステム: Windows、UEFI起動をサポート

ディスクサイズ: すべてのディスク領域が使用可能

警告
移行した後は、オペレーティングシステムはターゲットハードディスクの BIOS から起動できません。移行後にターゲットディスクから起動するには、システムで UEFI 起動を有効にし（「Unified Extensible Firmware Interface」セクションを参照）、処理を再度開始してください。

移行手順の詳細については、「移行方法」セクションを参照してください。

BIOSモードシステム、GPT、Windowsなし

このウィザードのステップでは、ターゲットハードディスクを選択する必要があります。

現在のシステム:

システム: BIOSモード

ソースパーティションスタイル: GPT

ソースディスクのオペレーティングシステム: Windows以外またはOSなし

選択したディスクにシステムを移行した場合:

システム: BIOSモード

パーティションスタイル: GPT

オペレーティングシステム: Windows以外またはOSなし

ディスクサイズ: すべてのディスク領域が使用可能

移行手順の詳細については、「移行方法」セクションを参照してください。

UEFIモードシステム、MBR、UEFIのサポートなし

このウィザードのステップでは、ターゲットハードディスクを選択する必要があります。

現在のシステム:

システム: UEFIモード

ソースパーティションスタイル: MBR

ソースディスクのオペレーティングシステム: Windows、UEFI起動のサポートなし

ターゲットディスクサイズ: 2 TB未満

選択したディスクにシステムを移行した場合:

システム: UEFI起動非対応

パーティションスタイル: MBR

オペレーティングシステム: Windows、UEFI起動のサポートなし

ディスクサイズ: すべてのディスク領域が使用可能

警告

オペレーティングシステムはターゲットディスクから UEFI で起動できない場合があります。

移行手順の詳細については、「移行方法」セクションを参照してください。

サポートされるUEFIモードシステム、MBR、UEFI

このウィザードのステップでは、ターゲットハードディスクを選択する必要があります。

現在のシステム:

システム: UEFIモード

ソースパーティションスタイル: MBR

ソースディスクのオペレーティングシステム: Windows、UEFI起動をサポート

選択したディスクにシステムを移行した場合:

移行後、ターゲットディスクのパーティションスタイルはGPTに変換され、ターゲットディスクから起動できるようになります。

移行後のターゲットディスク:

システム: UEFIモード

パーティションスタイル: GPT

オペレーティングシステム: Windows、UEFI起動をサポート

ディスクサイズ: すべてのディスク領域が使用可能

移行手順の詳細については、「移行方法」セクションを参照してください。

UEFIモードシステム、MBR、Windowsなし

Acronis Cyber Protect Home Office では、処理完了後にターゲットディスクのパーティションレイアウトを選択できます。

現在のシステム:

システム: UEFIモード

ソースパーティションスタイル: MBR

ソースディスクのオペレーティングシステム: Windows以外またはOSなし

ターゲットディスクサイズ: 2 TB未満

これらのシステムパラメータでは、次のいずれかを選択できます。

1. **変更せずにパーティションをコピー**

ターゲットディスクのパーティションスタイルをMBRのままにします。

移行後のターゲットディスク:

システム: UEFIモード

パーティションスタイル: MBR

オペレーティングシステム: Windows以外またはOSなし

ディスクサイズ: すべてのディスク領域が使用可能

2. **パーティションをコピーし、システム用ではないGPTスタイルでディスクを使用する**

パーティションスタイルをGPTに変換できます。

移行後のターゲットディスク:

システム: UEFI起動非対応

パーティションスタイル: GPT

オペレーティングシステム: Windows以外またはOSなし

ディスクサイズ: すべてのディスク領域が使用可能

警告
移行後、ターゲットディスクはシステム用ではないディスクとしてのみ使用できます。

移行手順の詳細については、「移行方法」セクションを参照してください。

UEFIモードシステム、GPT、UEFIのサポート

このウィザードのステップでは、ターゲットハードディスクを選択する必要があります。

現在のシステム:

システム: UEFIモード

ソースパーティションスタイル: GPT

オペレーティングシステム: Windows、UEFI 起動をサポート

選択したディスクにシステムを移行した場合:

システム: UEFIモード

パーティションスタイル: GPT

ディスクサイズ: すべてのディスク領域が使用可能

移行手順の詳細については、「移行方法」セクションを参照してください。

UEFIモードシステム、GPT、Windowsなし

このウィザードのステップでは、ターゲットハードディスクを選択する必要があります。

現在のシステム:

システム: UEFIモード

ソースパーティションスタイル: GPT

オペレーティングシステム: Windows以外またはOSなし

選択したディスクにシステムを移行した場合:

システム: UEFIモード

パーティションスタイル: GPT

ディスクサイズ: すべてのディスク領域が使用可能

移行手順の詳細については、「移行方法」セクションを参照してください。

HDDからSSDへのシステムの移行

最初に、Acronis Cyber Protect Home Office が、Windows と Acronis ブータブルメディア の両方で新しい SSD を検出することを確認してください。問題がある場合は、「Acronis Cyber Protect Home Office が SSD を認識しない場合の処理」を参照してください。

SSD のサイズ

SSDの容量は通常はHDDよりも少ないため、古いハードディスクの使用済み領域がSSDのサイズを超えている場合があります。その場合、移行を実行することはできません。

システムディスク上のデータ量を減らすため、次のことを試してください。

- データファイルを古いハードディスクから別の場所（たとえば、内蔵または外付けの別のハードディスクドライブ）に移動します。
- データファイル（ドキュメント、画像、オーディオファイルなど）の.zipファイルを作成し、元のファイルを削除します。
- Windowsのディスククリーンアップユーティリティを使用してハードディスクのクリーンアップを実行します。

Windowsを安定して動作させるためには、システムパーティション上に数GBの空き領域が必要です。

選択する移行モード

システムディスクが1つのパーティションで構成されている場合（隠しシステム予約パーティションは数えません）、クローンツールを使用してSSDに移行することができます。詳細については、「ハードディスクのクローン作成」を参照してください。

ただし、ほとんどの場合はバックアップとリカバリを使用することをお勧めします。この方法の方が柔軟性に優れ、移行をより詳細に管理できます。「バックアップとリカバリを使用した SSD への移行」を参照してください。

Acronis Cyber Protect Home Office が SSD を認識しない場合の処理

Acronis Cyber Protect Home Office が SSD を認識しないことがあります。

このような場合には、SSD が BIOS で認識されているかどうかを確認します。

コンピュータの BIOS に SSD が表示されない場合は、電源ケーブルおよびデータ ケーブルが適切に接続されていることを確認します。BIOS と SATA ドライバのアップデートを試行します。これらの推奨策の効果がない場合は、SSD 製造元のサポートチームに問い合わせてください。

コンピューターの BIOS に SSD が表示される場合

1. オペレーティングシステムに応じて、[検索] フィールドまたは [ファイル名を指定して実行] フィールドに cmd と入力し、**Enter** キーを押します。
2. コマンドプロンプトに次のコマンドを入力します。

```
diskpart
list disk
```

画面には、コンピューターに接続されているディスクが表示されます。SSD のディスク番号を見つけます。サイズを参照しながら確認します。

3. ディスクを選択するには、次のコマンドを実行します。

```
select disk N
```

この例では、SSD のディスク番号は N です。

4. SSD からすべての情報を削除し、MBR をデフォルト設定に上書きするには、次のコマンドを実行します。

```
clean
exit
exit
```

Acronis Cyber Protect Home Office を起動し、SSD が検出されるかどうかを確認します。SSD が検出される場合は、新しいディスクの追加ツールを使用して、ディスク領域全体を占めるパーティションを 1 つディスク上に作成します。パーティションを作成するときに、パーティションの前に空き領域が 1 MB あることを確認します。詳細については、「新しいハード ディスクの追加」を参照してください。

Acronis ブータブルメディア が SSD を認識するかどうかを確認するには、次のようにします。

1. Acronis ブータブルメディア から起動します。
2. メイン メニューで **[ツールとユーティリティ]** -> **[新しいディスクの追加]** を選択すると、**[ディスクの選択]** 画面にシステム内のすべてのハード ディスクに関する情報が表示されます。この情報を使用して、リカバリ環境で SSD が検出されているかどうかを確認します。
3. 画面に SSD が表示されている場合は、**[キャンセル]** をクリックします。

ブータブルメディアで SSD が認識されず、SSD コントローラモードが AHCI である場合には、モードを IDE（または一部の BIOS ブランドでは ATA）に変更して問題が解決されるかどうかを確認します。

警告
注意モードを変更した後に Windows を起動しないでください。ここで起動するとシステムに重大な問題が発生する場合があります。Windowsを起動する前にモードをAHCIに戻す必要があります。

モードを変更した後でブータブルメディアが SSD を検出する場合は、次の手順に従ってブータブルメディアでリカバリまたはクローン作成を行うことができます。

1. コンピュータをシャットダウンします。
2. BIOS を起動し、モードを AHCI から IDE（または一部の BIOS ブランドでは ATA）に変更します。
3. Acronis ブータブルメディア から起動します。
4. ディスクのリカバリまたはクローン作成を行います。
5. BIOS を起動し、IDE を AHCI に戻します。
6. Windows を起動します。

上記の推奨策の効果がない場合の処理

WinPE ベースのブータブルメディアを作成してみることができます。このメディアに、必要なドライバがある場合があります。詳細については、「Acronis ブータブルメディア の作成」を参照してください。

バックアップとリカバリを使用した SSD への移行

サポートされているすべてのオペレーティング システムについて、次の手順を使用できます。最初に、システムディスクが1つのパーティションで構成されている単純なケースについて考えてみます。Windows 7以降では、システムディスクに隠しシステム予約パーティションがある場合があります。

パーティションが含まれていない（ディスク領域が未割り当てである）空のSSDにシステムを移行することをおすすめします。ご使用の SSD が新しく、それまでに使用したことがない場合、パーティションはありません。

システムを SSD に移行する手順は、次のとおりです。

1. Acronis Cyber Protect Home Office を開始します。
2. Acronis ブータブルメディア がまだない場合は、作成します。これを実行するには、**[ツール]** セクションで **[ブータブルメディアの作成]** をクリックして、画面に表示される指示に従ってください。
3. システムハードディスクとSSD以外のハードディスクにシステムドライブ全体をディスクバックアップモードでバックアップします。
4. コンピュータの電源を切り、システム ハード ディスクを取り外します。
5. SSD をハード ディスクが装着されていたスロットにマウントします。

   注意
   一部の SSD ブランドでは、SSD を PCI Express スロットに挿入する必要があります。

6. Acronis ブータブルメディア から起動します。
7. バックアップをリカバリに使用できることをベリファイします。ベリファイするには、左側のペインで **[リカバリ]** をクリックし、バックアップを選択します。右クリックし、ショートカット メニューで **[ベリファイ]** を選択し、**[実行]** をクリックします。
8. ベリファイが終了したら、バックアップを右クリックし、ショートカット メニューで **[リカバリする]** を選択します。
9. [リカバリの方法] で **[ディスクまたはパーティション全体をリカバリする]** を選択し、**[次へ]** をクリックします。
10. [リカバリ元] でシステム ディスクを選択します。
11. **[新しい場所]** をクリックし、システム ディスクの新しいロケーションとして SSD を選択し、**[許可]** をクリックします。
12. 次に、**[実行]** をクリックしてリカバリを開始します。
13. リカバリが完了したら、Acronis Cyber Protect Home Office のスタンドアロン版を終了します。
14. SSD から起動し、Windows とアプリケーションが正しく機能することを確認します。

多くのノートブックで見られるように、システム ハード ディスクに隠しリカバリ パーティションまたは診断パーティションが含まれている場合、手順は異なります。通常は、SSD へのリカバリ中に手動でパーティションのサイズを変更する必要があります。手順については、「隠しパーティションを含むディスクのリカバリ」を参照してください。

ツール

保護ツール

- "Acronis Universal Restore"（239ページ）
- "Acronis Startup Recovery Manager"（205ページ）
- "Acronis メディアビルダー"（192ページ）
- "Acronis Secure Zone"（212ページ）
- "Try&Decide"（207ページ）

ディスクのクローン作成

- "ディスクのクローン作成ユーティリティ"（175ページ）

セキュリティとプライバシー

- "Acronis DriveCleanser"（222ページ）
- "システムのクリーンアップ"（228ページ）

ディスクの管理

- "新しいハードディスクの追加"（217ページ）

イメージのマウント

- "バックアップイメージのマウント"（235ページ）
- "イメージのアンマウント"（236ページ）

Acronis Cloud Backup Download

Acronis Cloud Backup Download は、インターネット接続が不安定な場合でも、クラウドバックアップを安全にダウンロードできるツールです。接続が切断されてもダウンロードは途中でキャンセルされず、一時停止され、後ほど再開することができます。さらに、ダウンロードしたバックアップからの復元は、クラウドからの復元よりも非常に高速です。

Acronis Cloud Backup Download をインストールするには、次のようにします。

1. 次のいずれかの方法で、 ツールをダウンロードします。
   - Acronis Cyber Protect Home Office で、[**ツール**] セクションに移動します。[**Acronis Cloud Backup Download**] をクリックして、ダウンロードページに移動します。次に、必要なバージョンのツールを選択してダウンロードします。
   - https://www.acronis.com/my/online-backup/webrestore/ に移動し、Acronis アカウントにログインします。サイドバーで、[**バックアップ**] をクリックしてから、リカバリするファイルのバックアップを選択します。詳細ビューで、[**ダウンロード**] をクリックします。次に、[**Cloud Backup のダウンロード**] ウィンドウで、[**ツールのダウンロード**] をクリックします。次に、必要なバージョンのツールを選択してダウンロードします。
   - https://go.acronis.com/cloud-backup-download にあるダウンロードページに移動します。次に、必要なバージョンのツールを選択してダウンロードします。

注意
以前にインストール済みの場合でも、ツールはダウンロードされます。

2. 実行可能ファイルを解凍して実行します。
3. ライセンス契約に同意して、サインインします。

クラウド バックアップのダウンロード

重要
ディスク、パーティション、またはマシン全体のバックアップのみ、TIBX 形式でダウンロードできます。ファイルまたはフォルダのバックアップは、Acronis Cloud Backup Download ではダウンロードできません。

1. Acronis Cloud Backup Download ツールを開始してサインインします。
2. **[Acronis Cloud Backup Download]** ウィンドウで、ダウンロードするバックアップを選択します。
3. **[ダウンロードするバックアップを選択]** ウィンドウで、特定のバックアップまたはバックアップセット全体を選択します。
4. （オプションの手順） バックアップが暗号化されている場合は、パスワードを入力します。
5. ダウンロード先を選択し、**[保存]** をクリックします。

.tibx ファイルのダウンロードが開始されます。必要に応じて一時停止したり、キャンセルしたりすることができます。

ダウンロードされたバックアップを使用する方法

- データのバックアップを継続する場合は、バックアップを "既存のバックアップをリストに追加する"（95ページ） で説明されているように Acronis Cyber Protect Home Office に追加します。
- "ディスクとパーティションのリカバリ"（106ページ） で説明されているように、データをバックアップから復元します。
- "Acronis ブータブルメディア の作成"（194ページ） で説明されているように、ブータブルメディアを作成します。
- "Acronis Survival Kit の作成"（25ページ） で説明されているように、Acronis Survival Kit を作成します。
- "バックアップイメージのマウント"（235ページ） で説明されているように、ダウンロード済みのバックアップをマウントします。

Acronis メディアビルダー

Acronis メディアビルダー では、USB フラッシュドライブ、外付けドライブ、または空の CD/DVD をブータブルにすることができます。Windows が起動できない場合は、ブータブルメディアを使用してスタンドアロン版の Acronis Cyber Protect Home Office を実行し、コンピューターをリカバリします。

以下のさまざまなタイプのブータブル メディアを作成できます。

- **Acronis ブータブルメディア**
  通常は、このタイプを選択してください。
- **Acronis プラグイン を伴う WinPE ベースのメディア**
  プレインストール環境で Acronis Cyber Protect Home Office を実行すると、コンピューターのハードウェアとの互換性が向上する場合があります。これは、プレインストール環境に Windows ドライバが使用されているためです。
  Acronis ブータブルメディア からコンピューターを起動できなかった場合には、この種類のメディアを作成することをお勧めします。
  このオプションを使用するには、以下のコンポーネントのうちいずれかをインストールしておく必要があります。
  - Windows 自動インストール キット（AIK）。
    WinPE 3.0を作成するにはこのコンポーネントが必要です。
  - Windows アセスメント & デプロイメント キット（ADK）。
    WinPE 4.0、WinPE 5.0、およびWinPE 10.0を作成するには、このコンポーネントが必要です。
- **Acronis プラグイン を伴う WinRE ベースのメディア**
  このタイプのブータブルメディアは WinPE ベースのメディアに似ていますが、WADK または WAIK を Microsoft Web サイトからダウンロードする必要がないという重要な利点があります。Windows 復元環境はWindows Vista以降のWindowsバージョンに既に組み込まれています。Acronis Cyber Protect Home Office は、システムにあるそれらのファイルを使用して WinRE ベースのメディアを作成します。WinPEベースのメディアと同様、ハードウェアとの互換性を向上させるためにドライバを追加することができます。ただし WinRE ベースのメディアは、それが作成されたコンピュータ、または同じオペレーティング システムのコンピュータでのみ使用可能です。

メモ

- Acronis Cyber Protect Home Office をアップデートするたびに、新しいブータブルメディアを作成することをお勧めします。
- 非光学メディアを使用する場合、メディアのファイルシステムは FAT16 または FAT32 でなければなりません。
- Acronis メディアビルダー では、x64 WinPE 3.0、WinPE 4.0、WinPE 5.0、および WinPE 10.0 のみがサポートされます。
- コンピュータは下記の要件を満たす必要があります。
  - WinPE 3.0の場合: 256 MB以上のRAM
  - WinPE 4.0の場合: 512 MB以上のRAM
  - WinPE 5.0の場合: 1 GB以上のRAM
  - WinPE 10.0の場合: 512 MB以上のRAM
- Acronis メディアビルダー が USB フラッシュドライブを認識しない場合は、Acronis ナレッジベースの記事（https://kb.acronis.com/content/1526）で説明されている手順を試してください。
- ブータブルメディアから起動する場合、Ext2/Ext3/Ext4、ReiserFS、Linux SWAP ファイルシステムのディスクやパーティションにバックアップすることはできません。
- ブータブルメディアから起動する際にスタンドアロン版の Acronis Cyber Protect Home Office を使用する場合は、Windows XP 以降のオペレーティングシステムの暗号化機能で暗号化されたファイル

やフォルダを復元することはできません。 詳細については、「バックアップ用のファイルレベルのセキュリティ設定」を参照してください。 ただし、Acronis Cyber Protect Home Office の暗号化機能を使用して暗号化されたバックアップは復元できます。

- Survival Kit が既に入っているドライブにブータブルメディアを作成する場合、Acronis メディアビルダー はドライブ全体のフォーマットを行わずに、隠しパーティションのみを上書きしてブータブルメディアを作成します。

Acronis ブータブルメディア の作成

1. USB フラッシュドライブ、または外付けドライブ (HDD/SSD) を差し込むか、空の CD または DVD を挿入します。
2. Acronis Cyber Protect Home Office を開始します。
3. **[ツール]** セクションの **[Bootable Rescue Media Builder]** をクリックします。
4. 作成方法を選択します。
   - **[シンプル]**: この方法が最も簡単です。Acronis Cyber Protect Home Office は、コンピューターに最適なメディアの種類を選択します。Windows 7 以降のバージョンを使用する場合、WinRE ベースのメディアが作成されます。
   - **[詳細]**—このオプションではメディアの種類を選択できます。これは、自分のコンピュータ用だけでなく、異なる Windows バージョンを実行しているコンピュータ用のブータブルメディアを作成できることを意味します。詳細については、「Acronis メディアビルダー」を参照してください。

     Linux ベースのメディアを選択する場合、メディアに置く Acronis Cyber Protect Home Office コンポーネントを選択します。選択するコンポーネントにターゲットコンピュータのアーキテクチャとの互換性があることを確認してください。 詳細については、「リムーバブルメディアの設定」を参照してください。

     WinRE ベースまたは WinPE ベースのメディアを選択する場合は、次のようにします。
     - メディアのアーキテクチャの種類として 32 ビットまたは 64 ビットを選択します。なお、32 ビットのブータブルメディアは 32 ビットのコンピュータでのみ使用できます。64 ビットのメディアには 32 ビットのコンピュータと 64 ビットのコンピュータ両方との互換性があります。
     - ブータブルメディアの作成に使用するツールキットを選択します。WAIK または WADK を選択し、選択したキットがコンピュータにインストールされていない場合、まず Microsoft Web サイトからダウンロードし、必須コンポーネントである Deployment ツールと Windows プレインストール環境（Windows PE）をインストールする必要があります。

       WinPE ファイルが既にコンピューターにあり、デフォルト以外のフォルダに格納されている場合、必要な作業はその場所を指定することだけです。これにより、Acronis プラグイン が既存の WinPE イメージに追加されます。
     - ハードウェアとの互換性を向上させるために、メディアに追加するドライバを選択することができます。
5. メディアの作成先を選択します。
   - **CD**
   - **DVD**
   - **外付けドライブ**
   - **USB フラッシュ ドライブ**

サポートされていないファイルシステムがドライブにあると、Acronis Cyber Protect Home Office によって FAT ファイルシステムへのフォーマットが自動的に選択されます。

警告
完全にフォーマットすると、ディスク上のデータはすべて消去されます。

- **ISO イメージ ファイル**

  .iso ファイルの名前とターゲット フォルダを指定してください。

  .iso ファイルが作成されたら、CD または DVD に書き込むことができます。たとえば、Windows 7 以降では、内蔵の書き込みツールを使用してこれを行えます。File Explorerで、作成したISOイメージファイルをダブルクリックし、**[書き込み]** をクリックします。
- **WIM イメージ ファイル**（WinPE ベースのメディアの場合のみ選択可能）

  Acronis Cyber Protect Home Office によって、Acronis プラグイン が Windows AIK または Windows ADK から .wim ファイルに追加されます。新しい .wim ファイルの名前とターゲット フォルダを指定する必要があります。

  .wimファイルを使用してブータブルメディアを作成するには、最初にそのファイルを.isoファイルに変更しておく必要があります。詳細については、「.wimファイルからの.isoファイルの作成」を参照してください。

注意
Acronis メディアビルダー は、このドライブに Survival Kit が既に作成されていることを検出すると、ドライブ全体をフォーマットするのではなくブータブルメディアの隠しパーティションだけを上書きおよび更新しようとします。

6. **[実行]** をクリックします。

Acronis ブータブルメディア 起動パラメータ

Acronis ブータブルメディア のスタートアップパラメータを設定して、メディアのブートオプションを構成すると、さまざまなハードウェアとの互換性を向上させることができます。nousb、nomouse、noapic などのオプションが利用できます。上級ユーザー向けに用意されているパラメータです。
Acronis ブータブルメディア からの起動をテスト中にハードウェアの互換性の問題が発生した場合は、Acronis サポートセンターにお問い合わせください。

スタートアップパラメータを追加する手順は、次のとおりです。

1. **[パラメータ]** フィールドにコマンドを入力します。スペースで区切って、複数のコマンドを入力できます。
2. 続行するには、**[次へ]** をクリックしてください。

Linuxカーネルを起動する前に適用できる追加パラメータ

説明

次のパラメータを使用すると、Linuxカーネルを特殊モードで読み込むことができます。

- **acpi=off**

ACPI を無効にします。ハードウェアの特定の構成に役立ちます。

- **noapic**

APIC（Advanced Programmable Interrupt Controller）を無効にします。ハードウェアの特定の構成に役立ちます。

- **nousb**

USBモジュールの読み込みを無効にします。

- **nousb2**

USB 2.0のサポートを無効にします。このオプションを指定しても、USB 1.1デバイスは動作します。このオプションを指定すると、USB 2.0モードでは動作しない一部のUSBドライブをUSB 1.1モードで使用できます。

- **quiet**

このパラメータはデフォルトで有効になっており、起動メッセージは表示されません。このパラメータを削除すると、Linux カーネルが読み込まれるときに起動メッセージが表示されるようになり、 プログラムが実行される前にコマンド シェルが提供されます。

- **nodma**

すべてのIDEディスクドライブのDMAを無効にします。カーネルが一部のハードウェアでフリーズするのを防ぎます。

- **nofw**

FireWire（IEEE1394）のサポートを無効にします。

- **nopcmcia**

PCMCIAハードウェアの検出を無効にします。

- **nomouse**

マウスのサポートを無効にします。

- **[モジュール名]=off**

モジュールを無効にします（例: **sata_sis=off**）。

- **pci=bios**

PCI BIOSの使用を強制し、ハードウェアデバイスには直接アクセスしません。たとえば、コンピュータが標準以外のPCIホストブリッジを備えているような場合にこのパラメータを使用することがあります。

- **pci=nobios**

PCI BIOSの使用を無効にします。ハードウェアへの直接アクセスのみを許可します。たとえば、BIOSが原因で起動時にクラッシュが発生すると考えられる場合にこのパラメータを使用することがあります。

- **pci=biosirq**

PCI BIOSの呼び出しを使用して、割り込みルーティングテーブルを取得します。これらの呼び出しは、一部のコンピュータではバグがあり、使用するとコンピュータがフリーズしますが、他のコンピュータでは、割り込みルーティングテーブルを取得する唯一の方法です。カーネルがIRQを割り当てることができない場合、またはマザーボード上のセカンダリPCIバスを検出できない場合は、このオプションを試してください。

- **vga=ask**

現在のビデオカードで使用できるビデオモードの一覧を取得し、ビデオカードとモニタに最適なビデオモードを選択できるようにします。自動的に選択されたビデオモードがお使いのハードウェアに適合しない場合は、このオプションを試してください。

既存の.wimイメージへのドライバの追加

Acronis プラグイン を含む基本的な WinPE ディスクに、ストレージデバイスコントローラーなどのお使いのハードウェアのドライバが含まれていないことがあります。これを追加する最も簡単な方法は、Acronis メディアビルダー で詳細モードを選択し、追加するドライバを指定することです。Acronis プラグイン を使って ISO ファイルを作成する前に、既存の .wim ファイルに手動でドライバを追加することができます。

警告
注意.inf ファイル拡張子が付いたドライバのみを追加できます。

以下の手順は、MSDN の記事（https://technet.microsoft.com/ にあります）を基にしています。

カスタムの Windows PE イメージを作成するには、次の手順を実行します。

1. Acronis プラグイン を含む .wim ファイルがない場合は、Acronis メディアビルダー を開始して、WinPE ベースのメディアのターゲットとして **[WIM ファイル]** を選択し、これを作成します。詳細については、Acronis ブータブルメディア の作成を参照してください。
2. お使いのWindows AIKまたはWindows ADKのバージョンに応じて、以下のいずれかを実行してください。
   - **[スタート]** メニューで、**[Microsoft Windows AIK]** をクリックし、**[Windows PE ツール コマンド プロンプト]** を右クリックして **[管理者として実行]** を選択します。
   - **[スタート]** メニューで、**[Microsoft Windows AIK]** をクリックし、**[Deployment ツールのコマンド プロンプト]** を右クリックして **[管理者として実行]** を選択します。
   - **[スタート]** メニューで、**[Windows キット]**、**[Windows ADK]** とクリックし、**[展開およびイメージング ツール環境]** を右クリックして **[管理者として実行]** を選択します。
3. 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。

   ```
   copype amd64 C:\winpe_x64
   ```

4. .wimファイルをたとえばC:¥winpe_x64¥フォルダにコピーします。このファイルのデフォルトの名前は、AcronisBootablePEMedia.wim です。

5. DISMツールを使用して基本イメージをローカルディレクトリにマウントします。これを行うには、次のように入力します。

```
Dism /Mount-Wim /WimFile:C:\winpe_x64\AcronisBootablePEMedia.wim /index:1
/MountDir:C:\winpe_x64\mount
```

6. DISMコマンドとAdd-Driverオプションを使用してハードウェアドライバを追加します。たとえば、C:¥drivers¥フォルダにあるMydriver.infドライバを追加するには、次のように入力します。

```
Dism /image:C:\winpe_x64\mount /Add-Driver /driver:C:\drivers\mydriver.inf
```

7. 追加するドライバごとに上記の手順を繰り返してください。
8. DISMコマンドを使用して、変更を適用します。

```
Dism /Unmount-Wim /MountDir:C:\winpe_x64\mount /Commit
```

9. 生成された.wimファイルからPEイメージ（.isoファイル）を作成します。詳細については、「.wim ファイルからの .iso ファイルの作成」を参照してください。

.wim ファイルからの .iso ファイルの作成

.wim ファイルを使用してブータブルメディアを作成するには、まずそのファイルを .iso ファイルに変換しておく必要があります。

生成された .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。

1. お使いのWindows AIKまたはWindows ADKのバージョンに応じて、以下のいずれかを実行してください。
   - **[スタート]** メニューで、**[Microsoft Windows AIK]** をクリックし、**[Windows PE ツール コマンド プロンプト]** を右クリックして **[管理者として実行]** を選択します。
   - **[スタート]** メニューで、**[Microsoft Windows AIK]** をクリックし、**[Deployment ツールのコマンド プロンプト]** を右クリックして **[管理者として実行]** を選択します。
   - **[スタート]** メニューで、**[Windows キット]**、**[Windows ADK]** とクリックし、**[展開およびイメージング ツール環境]** を右クリックして **[管理者として実行]** を選択します。
2. 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。

```
copype amd64 C:\winpe_x64
```

3. 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（たとえば、AcronisBootablePEMedia.wim）に置き換えます。AcronisBootablePEMedia.wim ファイルが c:¥ にある場合は、次のように入力します。

   WinPE 3.0 の場合

```
copy c:\AcronisBootablePEMedia.wim c:\winpe_x64\ISO\sources\boot.wim
```

   WinPE 4.0、WinPE 5.0、 またはWinPE 10.0の場合: 次を入力してください。

```
copy "c:\AcronisBootablePEMedia.wim" c:\winpe_x64\media\sources\boot.wim
```

4. **Oscdimg**ツールを使用します。.isoファイルを作成するには、次のように入力します。

   ```
   oscdimg -n -bc:\winpe_x64\etfsboot.com c:\winpe_x64\ISO c:\winpe_x64\winpe_x64.iso
   ```

   また、BIOSベースのコンピュータおよびUEFIベースのコンピュータでメディアをブータブルにするには、次のように入力します。

   ```
   oscdimg -m -o -u2 -udfver102 -bootdata:2#p0,e,bc:\winpe_
   x64\fwfiles\etfsboot.com#pEF,e,bc:\winpe_x64\fwfiles\efisys.bin c:\winpe_x64\media
   c:\winpe_x64\winpe_x64.iso
   ```

5. サードパーティのツールを使用して .iso ファイルを CD に書き込むと、Acronis Cyber Protect Home Office が格納されたブータブル Windows PE ディスクが作成されます。

必要なときにブータブルメディアを確実に使用できるようにする

必要に応じてコンピュータを正常に復元できるように、ブータブルメディアからのコンピュータの起動をテストしておく必要があります。さらに、ブータブルメディアがコンピュータのデバイス（ハードドライブ、マウス、キーボード、ネットワークアダプタなど）をすべて認識することを確認する必要もあります。

ブータブル CD を含むボックス版の製品を購入し、Acronis Cyber Protect Home Office をアップデートしていない場合は、その CD をテストすることができます。それ以外の場合は、新しいブータブルメディアを作成してください。詳細については、Acronis ブータブルメディア の作成を参照してください。

ブータブルメディアをテストするには、次の手順を実行します。

注意
バックアップの保存用に外部ドライブを使用する場合、ブータブル CD から起動する前にそのドライブを接続しておく必要があります。接続しておかないと、そのドライブは検出されません。

1. ブータブルメディアから起動できるように、コンピュータを設定します。次に、ブータブルメディアデバイス（CD-ROM/DVD-ROM ドライブまたは USB ドライブ）を最初のブート デバイスにします。詳細については、「BIOS での起動順の並べ替え」を参照してください。
2. ブータブル CD がある場合は、「Press any key to boot from CD」というプロンプトが表示されたらすぐに任意のキーを押して CD からの起動を開始します。5 秒以内にキーを押さなかった場合は、コンピュータを再起動する必要があります。
3. ブートメニューが表示されたら、[**Acronis Cyber Protect Home Office**] を選択します。

注意
ワイヤレス マウスが動作しない場合は、有線マウスに交換してみてください。キーボードについても、同様です。

注意
別のマウスやキーボードがない場合は、Acronis サポートセンターにご連絡ください。ご利用のマウスとキーボードのモデルに対応したドライバを含むカスタムブータブル CD を作成いたします。適切なドライバを見つけてカスタムブータブル CD を作成するには、ある程度の時間がかかることをご了承ください。また、一部のモデルには、対応できないことがあります。

4. プログラムが開始したら、バックアップからいくつかのファイルを復元してみることをお勧めします。復元をテストすることにより、そのブータブル CD を復元に使用できることを確認できます。さらに、システムのすべてのハードディスク ドライブがプログラムによって検出されるかどうかも確認できます。

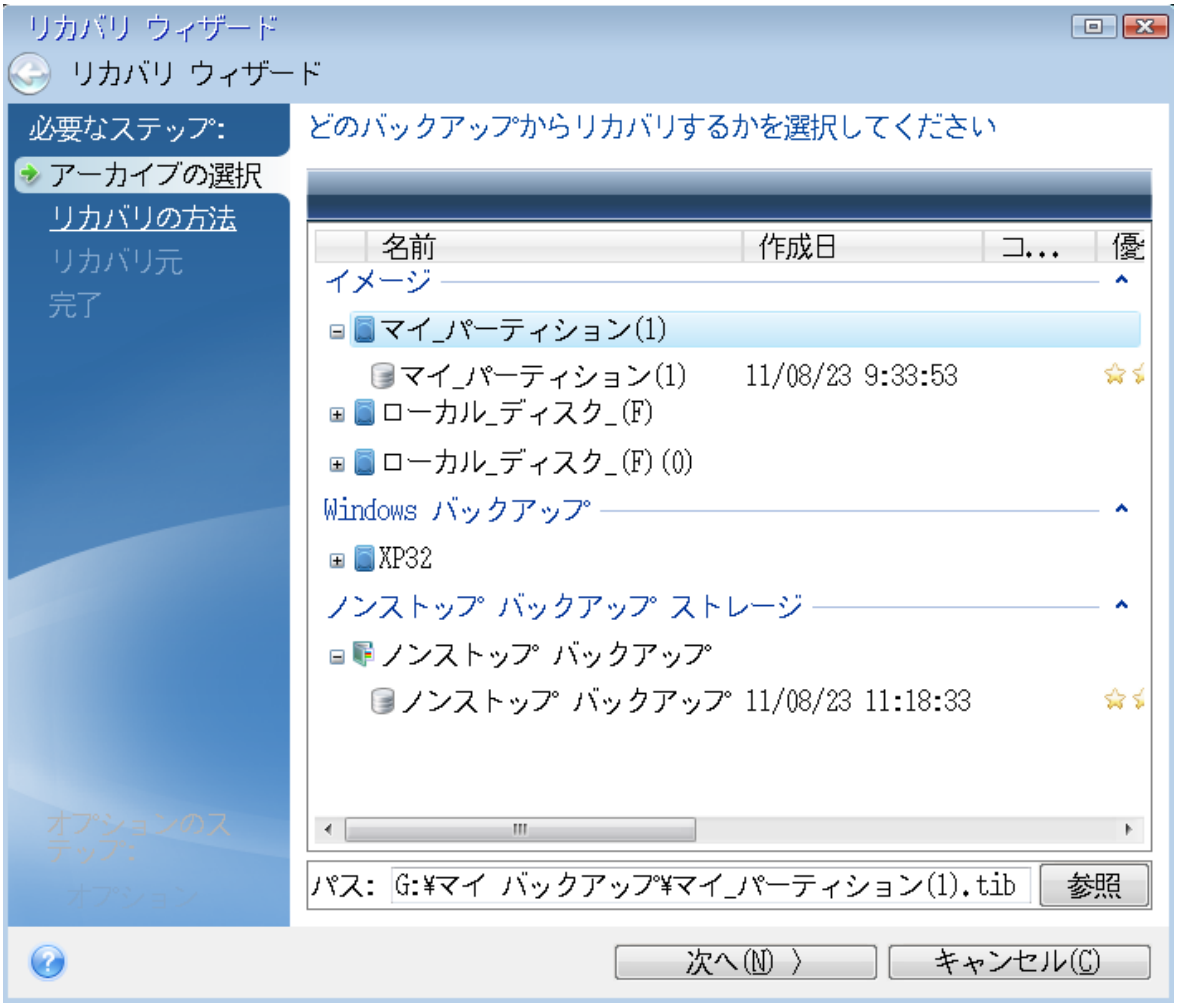
注意
予備のハードドライブがある場合、そのハードドライブへのシステムパーティションの復元をテストすることを強くおすすめします。

リカバリをテストし、同時にドライブとネットワーク アダプタをチェックするには、次の手順を実行します。

1. ファイルのバックアップがある場合、ツールバーで [**リカバリ**] -> [**ファイルのリカバリ**] をクリックして、リカバリ ウィザードを起動します。

注意
ディスクとパーティションのバックアップだけがある場合でも、リカバリ ウィザードを開始して同様の手順を実行します。その場合、[**リカバリの方法**] のステップで [**指定したファイルおよびフォルダをリカバリする**] を選択してください。

2. [**アーカイブのロケーション**] のステップでバックアップを選択し、[**次へ**] をクリックします。



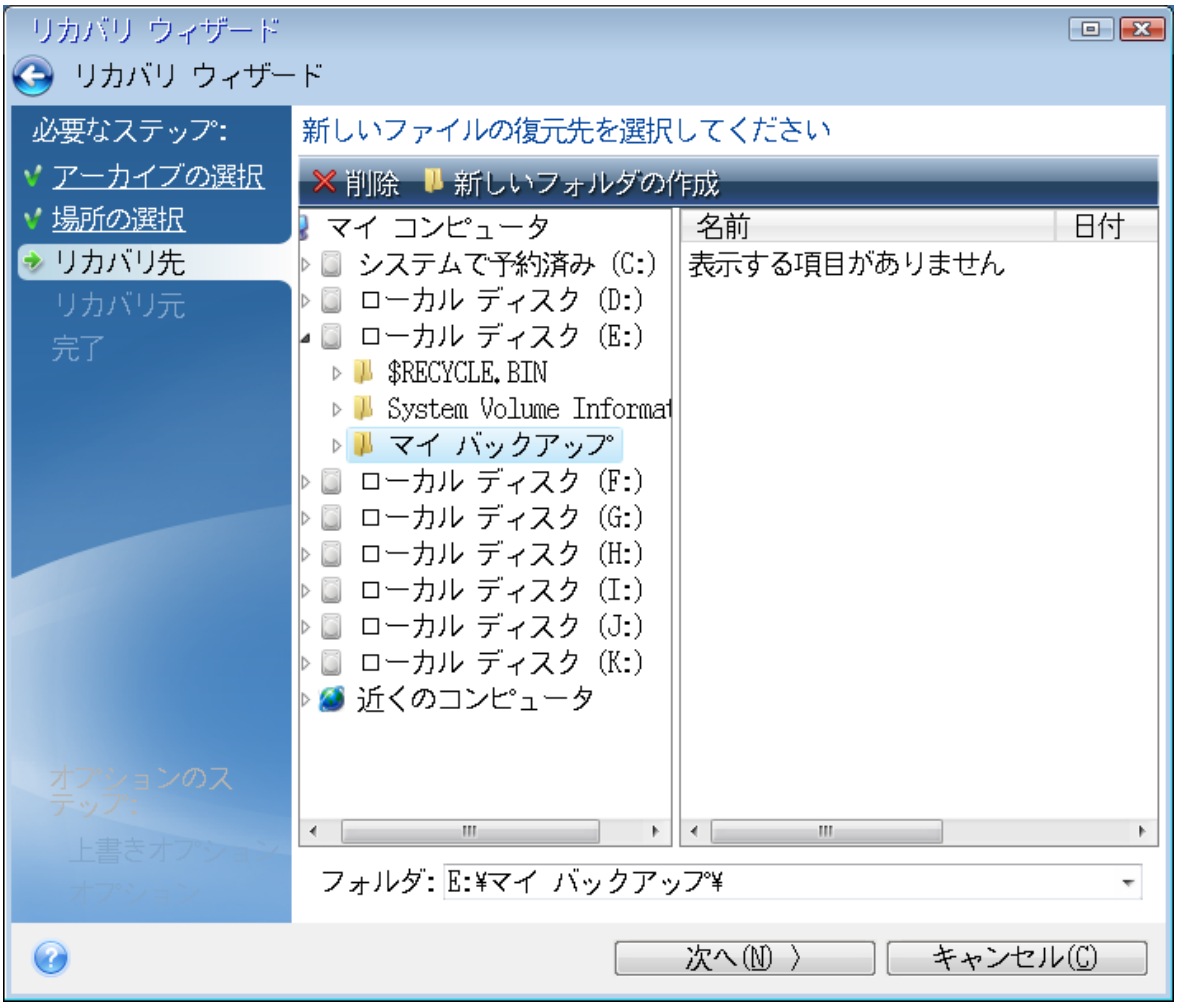
3. ブータブル CD でファイルを復元する場合、復元されるファイルに新しいロケーションのみを選択できます。したがって、[**ロケーションの選択**] ステップでは単に [**次へ**] をクリックしてください。
4. [**復元先**] ウィンドウが開いたら、[**マイ コンピュータ**] の下にすべてのドライブが表示されていることを確認します。

注意
バックアップをネットワークに保存する場合は、ネットワークにアクセスできることを確認してください。

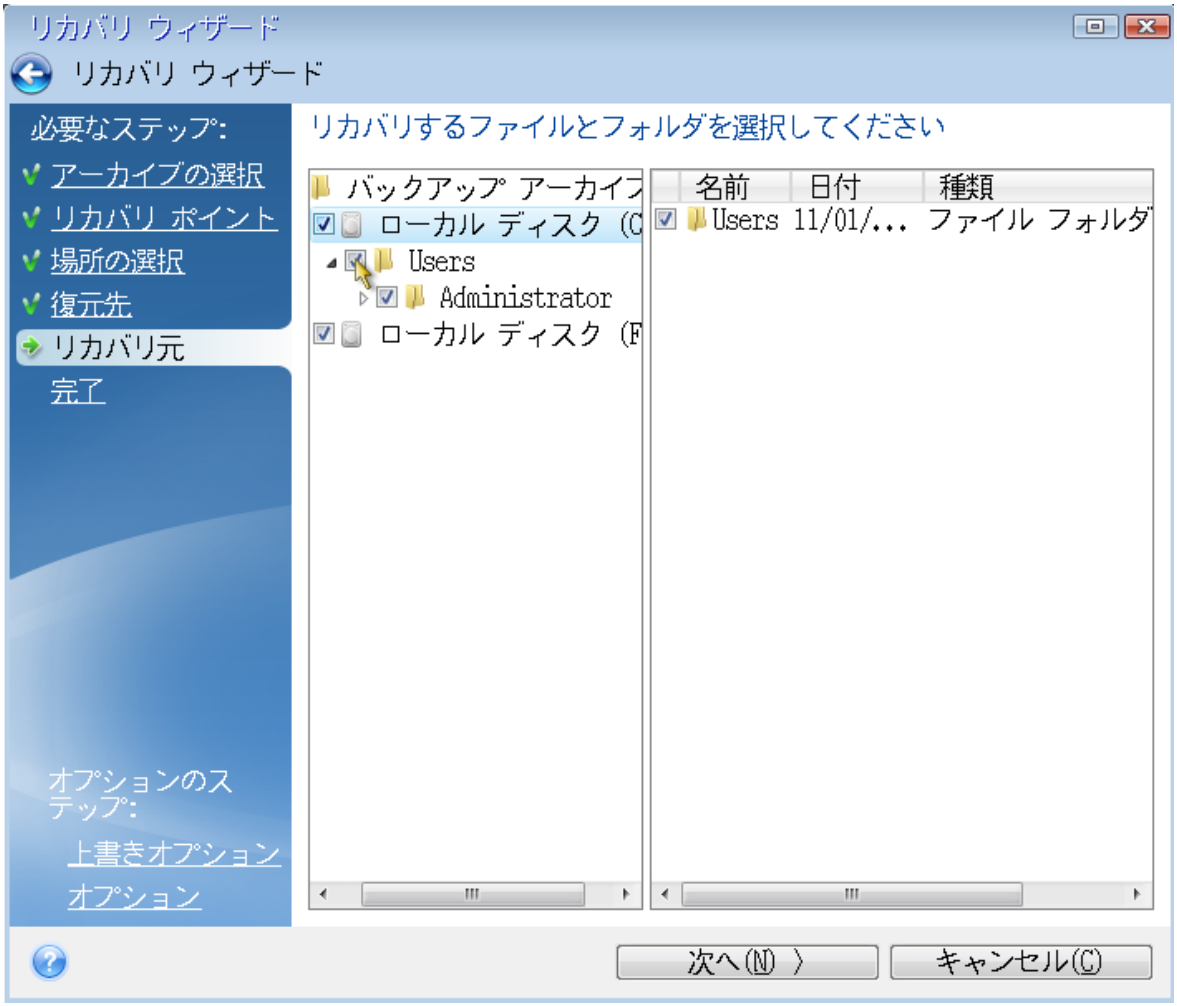
注意
ネットワークにコンピュータがまったく表示されないものの [**マイ コンピュータ**] の下に [**近くのコンピュータ**] アイコンが表示されている場合は、ネットワーク設定を手動で指定します。手動で指定するには、[**ツールとユーティリティ**] > [**オプション**] > [**ネットワークアダプタ**] で使用できるウィンドウを開きます。

注意

[マイコンピュータ] で **[近くのコンピュータ]** アイコンが表示されない場合は、ネットワークカードまたは Acronis Cyber Protect Home Office に付属しているカードドライバに問題がある可能性があります。



5. ファイルを保存する場所を選択して、**[次へ]** をクリックします。
6. リカバリするファイルのチェック ボックスをいくつかオンにして、**[次へ]** をクリックします。



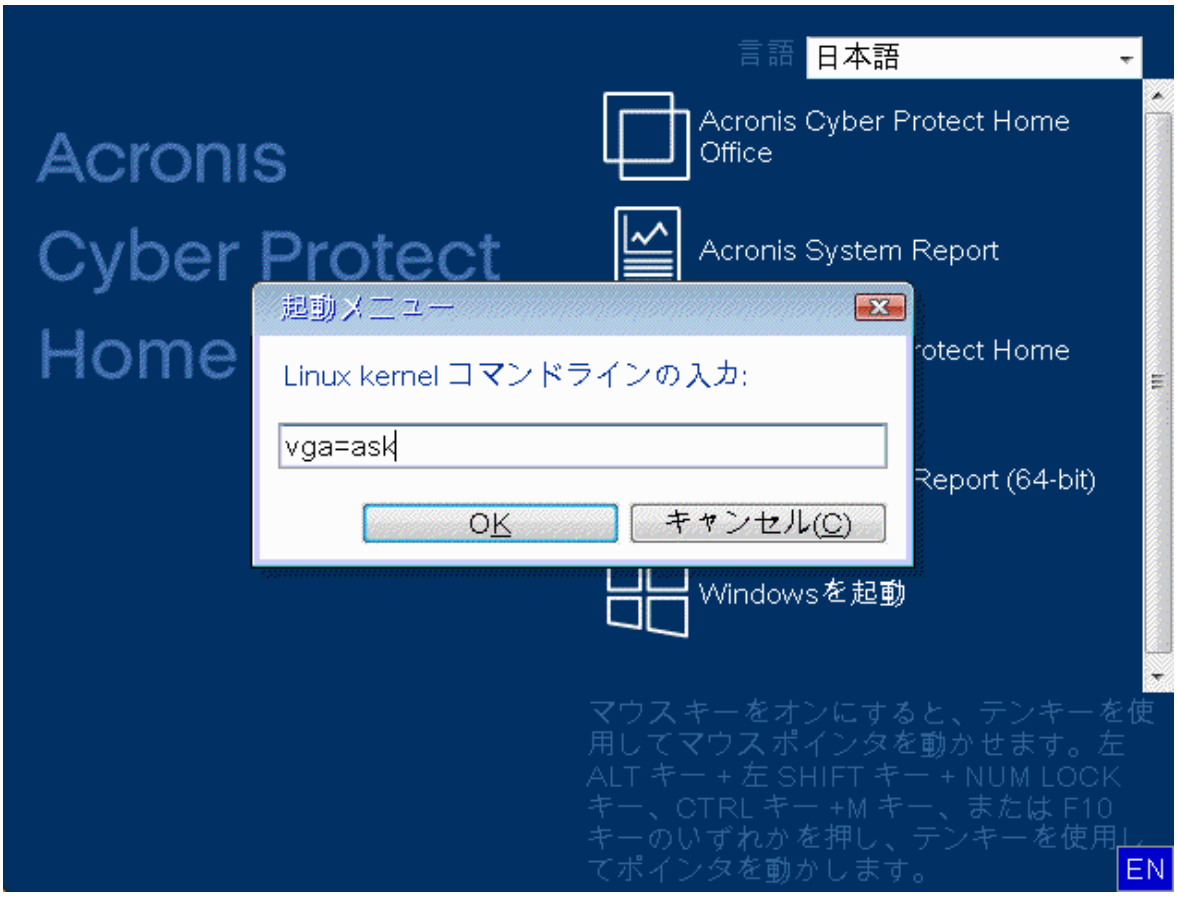
7. [概要] ウィンドウの **[実行]** をクリックして、リカバリを開始します。
8. リカバリが終了したら、スタンドアロン版の Acronis Cyber Protect Home Office を終了します。

これで、必要なときにこのブータブル CD を使用できることがある程度確実にわかりました。

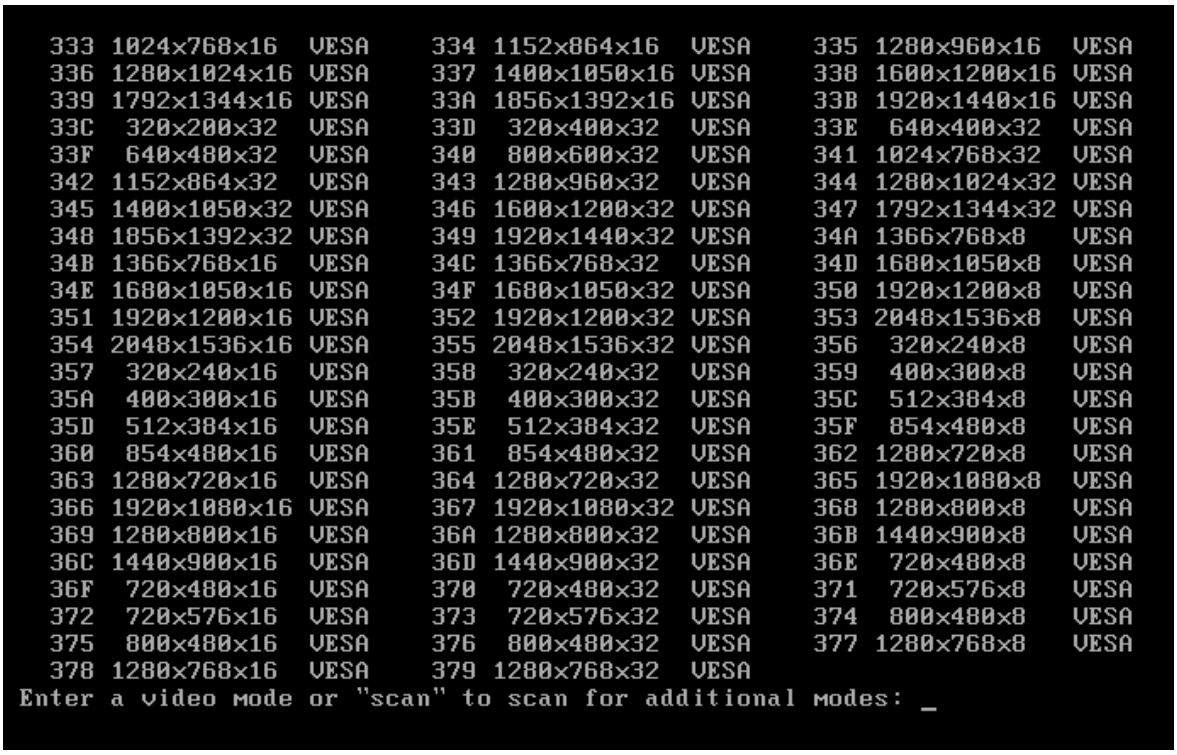
ブータブルメディアからの起動時におけるビデオモードの選択

ブータブルメディアからの起動時には、ビデオカードおよびモニタの仕様に応じて最適なビデオモードが自動で選択されます。ただし、使用しているハードウェアに適していないビデオモードが選択される場合もあります。このような場合は、次の手順で適切なビデオモードを選択できます。

1. ブータブルメディアからの起動を開始します。ブートメニューが表示されたら、**Acronis Cyber Protect Home Office** の項目にマウスポインタを置いて F11 キーを押します。
2. コマンドラインが表示されたら、**vga=ask** と入力して **[OK]** をクリックします。



3. ブートメニューで **[Acronis Cyber Protect Home Office]** を選択し、ブータブルメディアからの起動を継続します。使用できるビデオモードを表示するには、該当するメッセージが表示されたら Enter キーを押します。
4. 使用しているモニタに最適なビデオモードを選択し、その番号をコマンドラインに入力します。たとえば、「338」と入力すると、1600x1200x16のビデオモードが選択されます（下図参照）。



5. Acronis Cyber Protect Home Office が起動するまで待ってから、[ようこそ] 画面がモニタ上に適切に表示されていることを確認します。

他のビデオモードをテストするには、Acronis Cyber Protect Home Office を閉じてから上記の手順を繰り返してください。

ハードウェアに最適なビデオモードを見つけたら、そのビデオモードを自動的に選択する新しいブータブルメディアを作成できます。

これを行うには、Acronis メディアビルダー を起動して目的のメディアコンポーネントを選択し、[**ブータブルメディアの起動パラメータ**] のステップにおいてコマンドラインに接頭辞「0x」を付加してモードの番号を入力（この例では「0x338」）してから、通常通りにメディアを作成します。

Acronis Startup Recovery Manager

Acronis Startup Recovery Manager を使用すると、オペレーティングシステムを読み込まずに Acronis Cyber Protect Home Office を起動することができます。この機能を利用すれば、オペレーティングシステムが起動しなくなったときでも、Acronis Cyber Protect Home Office を使用して、破損したパーティションをリカバリすることができます。Acronis のリムーバブルメディアからコンピューターを起動する場合とは異なり、Acronis Cyber Protect Home Office の起動時には独立したメディアやネットワーク接続は必要ありません。

注意
Acronis Startup Recovery Manager は Windows を実行しているタブレットでは使用できません。

Acronis Startup Recovery Manager を有効化する手順は、次のとおりです

1. Acronis Cyber Protect Home Office を開始します。
2. [**ツール**] セクションで [**すべてのツール**] をクリックし、[**Acronis Startup Recovery Manager を有効化する**] をダブルクリックします。
3. 表示されたウィンドウで、[**アクティブ化する**] をクリックします。

障害が発生した場合、コンピューターの電源を投入し、「Press F11 for Acronis Startup Recovery Manager」というメッセージが表示されたら F11 キーを押します。これによってスタンドアロン版の Acronis Cyber Protect Home Office が起動します。このスタンドアロン版と完全版との違いはごくわずかです。

Acronis Startup Recovery Manager を無効化する手順は、次のとおりです

1. Acronis Cyber Protect Home Office を開始します。
2. [**ツール**] セクションで [**すべてのツール**] をクリックし、[**Acronis Startup Recovery Manager を有効化する**] をダブルクリックします。
3. 表示されたウィンドウで、[**無効化**] をクリックします。

追加情報

スタンドアロンモードの Acronis Cyber Protect Home Office で使用されるドライブ文字は、Windows がドライブの識別に使用する文字と異なる場合があります。たとえば、スタンドアロンの Acronis Cyber Protect Home Office での D: ディスクが、Windows の E: ディスクに対応していることもあります。ディスクのラベル、パーティション サイズ、ファイル システム、ドライブの性能、メーカー、およびモデル番号に関する情報を参照することによって、ディスクおよびパーティションを正しく特定することができます。

Try&Decide がオンの場合、以前に有効化した Acronis Startup Recovery Manager を使用することはできません。Try モードでコンピューターを再起動すると、Acronis Startup Recovery Manager を再び利用できるようになります。

Acronis Startup Recovery Manager の、他のローダーに対する影響

Acronis Startup Recovery Manager を有効化すると、MBR（マスターブートレコード）が Startup Recovery Manager のブートコードで上書きされます。サード パーティ製のブート マネージャがインストールされている場合は、スタートアップ リカバリ マネージャをアクティブ化した後に、そのブート マネージャを再度アクティブ化する必要があります。Linux ローダー（LiLo や GRUB など）の場合は、Acronis Startup Recovery Manager を有効にする前に、MBR ではなく Linux のルート（またはブート）パーティションブートレコードへのローダーのインストールを検討してください。

UEFI ブート メカニズムは BIOS のものと異なります。任意の OS ローダーまたはその他のブート プログラムは、対応するローダーへのパスを定義する、独自のブート変数を持ちます。すべてのローダーは、EFI システム パーティションと呼ばれる特別なパーティションに保存されます。UEFI モードのシステムで、Acronis Startup Recovery Manager を有効化すると、独自のブート変数が書き込まれ、ブート順序が変更されます。この変数は変数のリストに追加されますが、リスト内の変数自体は変更されません。すべてのローダーは独立しており、相互に影響しないため、Acronis Startup Recovery Manager の有効化の前後で、特に変更は必要ありません。

Try&Decide

注意
Try&Decide をインストールするには、Acronis Cyber Protect Home Office のインストール時にこのコンポーネントを選択するか、"Acronis Cyber Protect Home Office のインストールとアンインストール"（15ページ） で説明されているように、後でそれを追加することができます。

Try&Decide をオンにすると、コンピュータは Try モードになります。このようにしておけば、オペレーティング システム、プログラム、データに損傷を与える可能性を心配することなく、潜在的な危険性のある操作を実行できます。Try&Decide をオフにしたら、変更をコンピュータに適用するか、変更を破棄するかを指定します。

Try&Decide が役に立つ場合

次の操作を行う場合は事前に Try&Decide をオンにしておくことをお勧めします。

- システム設定を変更する際に、その変更がコンピュータにどのような影響を与えるかがわからない場合。
- システム アップデート、ドライバなどをインストールする場合。
- よく知らないアプリケーションをインストールする場合。
- 未知の差出人からの電子メール添付ファイルを開く場合。
- 危険なコンテンツが存在する可能性のあるウェブサイトにアクセスする場合。

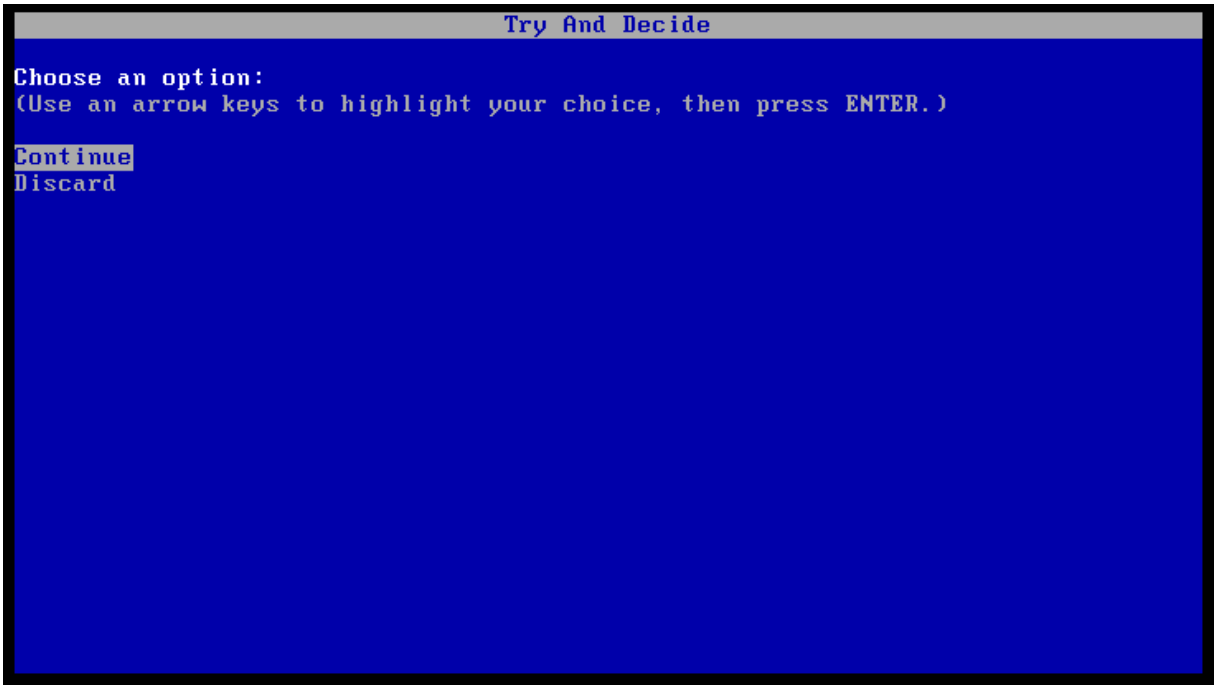
注意
Try モードで POP メールサーバーから電子メールをダウンロードしたり、新しいファイルの作成や既存の文書の編集を行ったりした後に、変更内容の破棄を選択した場合、それらのファイル、文書の変更内容、および電子メールは失われることにご注意ください。この場合は、新しいファイルや編集後の文書をUSBフラッシュドライブなどに保存し、USBドライブを取り外してから変更を破棄してください。

コンピュータを再起動した後のTry&Decideの動作

Try&Decide はオペレーティング システムを再起動しても継続されるため、必要に応じて有効のままにしておくことができます。

Try モードでの作業中に何らかの理由でコンピュータが再起動された場合は、オペレーティング システムの起動が開始する前に表示されるダイアログで、Try モードを停止して変更を破棄するか、Try モードを継続するかを選択できます。これにより、システム クラッシュを発生させた変更を破棄することができます。逆に、たとえばアプリケーションをインストールした後で再起動した場合などは、Windows が起動した後も継続して Try モードで作業することができます。

Try モードでコンピュータを再起動（ソフト リブート）するたびに、最大 500 MB の Try&Decide のハウスキーピング データが、仮想的な変更の保存先として選択したストレージに追加されます。



Try&Decide 使用上の制限

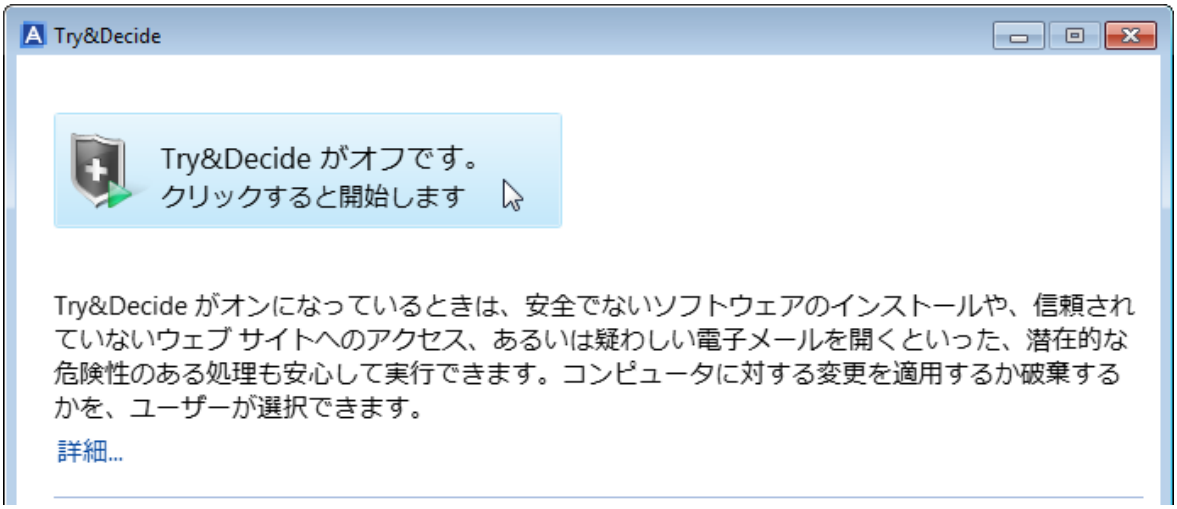
- Try&Decide は、Windows のメモリ整合性機能（Windows 11 ではデフォルトでオンになっている）とは互換性がありません。Try&Decide の互換性の問題を回避するには、Windows のセキュリティ設定のメモリ整合性をオフにすることができます。
- Windows 7、Windows 8、または Windows 10 を使用している場合、Try モードではコンピューターがアイドル状態のときでもプログラムがディスクの空き領域をかなり消費することがあります。これは、バックグラウンドで実行されるインデックス作成などのハウスキーピング処理のためです。
- Tryモードでの作業中は、システムのパフォーマンスが低下することに注意してください。また、特に数日間 Try モードをオンにしている場合など、変更を適用する処理には長い時間がかかることがあります。
- Try&Decide では、ディスクパーティションの変更は追跡できません。そのため、パーティションのサイズ変更やレイアウト変更など、パーティションに対する仮想操作に Try モードを使用することは

できません。また、Try&Decide と同時にディスク最適化やディスク エラー チェックのユーティリティを使用しないでください。同時に使用すると、ファイル システムが修復不可能なほど破損することや、システム ディスクが起動不能になることがあるからです。

- Try モードを開始すると、それ以前に Acronis Startup Recovery Manager がアクティブ化されていても、使用できなくなります。Try モードでコンピューターを再起動すると、Acronis Startup Recovery Manager を再び利用できるようになります。
- Try&Decide とNonstop Backupを同時に有効にすることはできません。Try モードを開始すると、Nonstop Backupが一時停止します。Try モードを停止すると、Nonstop Backupが再開されます。
- Try モードを開始すると、「休止」省電力モードを使用できなくなります。
- Try&Decideを使用してダイナミックディスクを保護することはできません。
- システム内のパーティションがBitLockerで暗号化されている場合、Try&Decideは機能しません。
- Try&Decide では Acronis Secure Zone は保護されず、仮変更用のストレージとして使用されます。

Try&Decide の使用

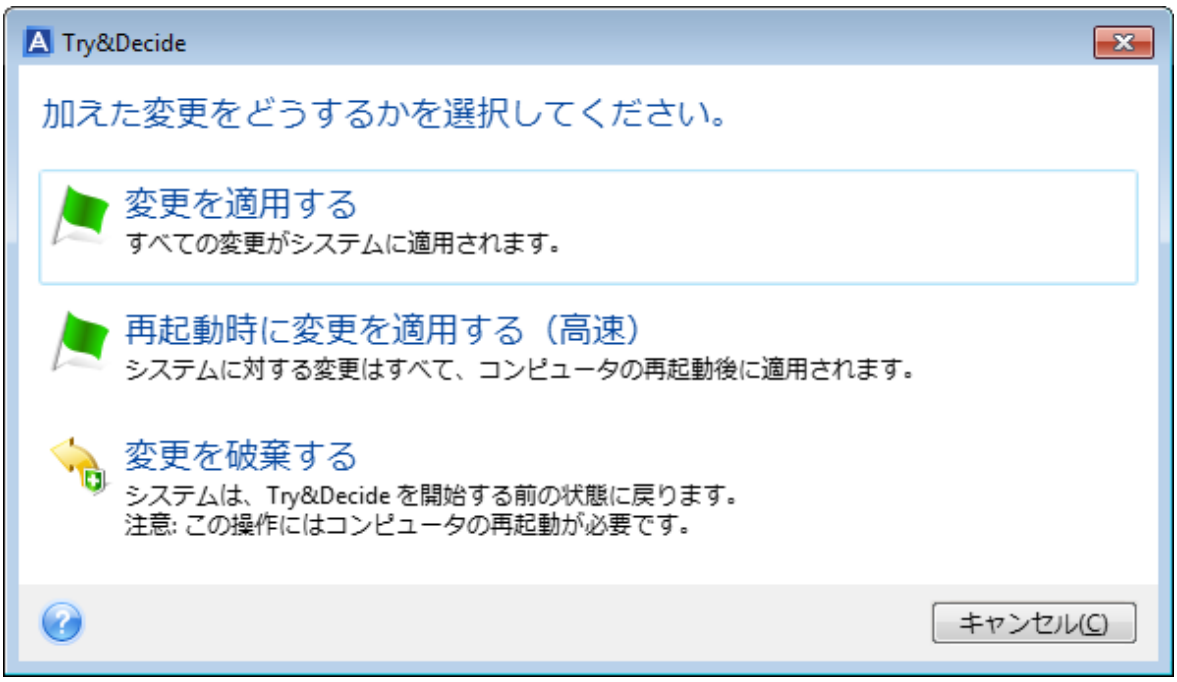
1. Acronis Cyber Protect Home Office を開始します。
2. [**ツール**] セクションで、[**Try&Decide**] をクリックします。
3. 必要に応じて、Try&Decide のオプションを設定します。詳細については、「Try&Decide のオプションと通知」を参照してください。
4. Try モードを開始するには、**Try&Decide** のアイコンをクリックします。OS とファイルに対するすべての変更の追跡が開始され、選択したディスクにすべての変更が一時的に保存されます。



5. 希望する変更をすべて実行します。

注意
仮変更の保存用として選択した場所のディスク領域が、変更を適用するために必要な最小限の容量しかないと、変更を適用するか、破棄するかを求めるメッセージが表示されます。この警告メッセージを無視すると、ディスクが満杯になったときに自動的にシステムが再起動されて、変更は破棄されます。

6. Try モードを停止するには、[**Try&Decide**] ウィンドウで **Try&Decide** のアイコンをクリックします。



7. 次のいずれかを選択します。
   - [**変更の適用**] を選択すると、システムに加えた変更が保存されます。
   - [**再起動して変更を適用**] を選択すると、変更の適用を短時間で実行できます。このボタンをクリックすると、コンピュータが再起動され、再起動中に変更が適用されます。
   - [**変更の破棄**] を選択すると、Try モードをオンにする前の状態にシステムを戻すことができます。このオプションを選択すると、次のオプションを含むポップアップウィンドウが表示されます: [**再起動して変更を破棄**] および [**再起動しない**]。[**再起動しない**] オプションを選択した場合、Try&Decide 機能はオンのままになり、変更は破棄されません。

注意
[**変更の破棄**] を選択して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コンピュータを再起動すると、Try モードでの作業に使用したオペレーティング システム以外は起動できなくなります。もう一度再起動すると、元の MBR がリカバリされて、他のオペレーティング システムも起動できるようになります。

Try&Decide のオプションと通知

[Try&Decide] ウィンドウで Try&Decide のオプションを変更できます。設定をデフォルト値に戻すには、[設定値をデフォルトにリセットする] をクリックします。

保護されたパーティション

この設定値を変更するには、次の手順を実行します。

1. 設定名の横のパーティションのドライブ文字をクリックします。[パーティションの選択] ウィンドウが表示されます。

2. 保護するパーティションを選択し、**[OK]** をクリックします。
   デフォルトでは、Try&Decide によってシステム パーティション（ディスク C）が保護されますが、システム内の他の任意のパーティションの保護を選択することもできます。

仮変更用のストレージ

この設定値を変更するには、次の手順を実行します。

1. 設定名の横のパーティションのドライブ文字をクリックします。[仮変更用のストレージ] ウィンドウが表示されます。
2. 仮変更用のストレージとして使用するパーティションを選択し、**[OK]** をクリックします。
   デフォルトでは、Try&Decideによってディスクの空き領域に情報が保存されます。

注意
複数のパーティションを保護するように選択した場合、保護するパーティションの中から仮変更の保存先を選択することはできません。また、外部ハードディスク ドライブは選択できません。

通知

デフォルトの通知設定を変更するには、**[警告の設定を変更します]** をクリックします。[設定] ウィンドウが表示されます。

- 残りのディスク空き領域: 仮変更用ストレージの空き領域が指定された値より少なくなると、通知メッセージが表示されます。
- Try&Decide開始からの経過時間: Try&Decideでの動作時間がユーザーの指定した時間を超えると、通知メッセージが表示されます。

Try&Decide: 典型的な使用例

Try&Decide機能は、さまざまな場合に役立ちます。以下にその例を示します。

ソフトウェアの評価

新しいソフトウェアをインストールする前にTryモードをオンにしておくと役立つ場合があります。たとえば、次の場合にTryモードをオンにしておくことをおすすめします。

- ウイルス対策ソフトウェアを選択する。
  ウイルス対策ソフトウェアをインストールすると、一部のアプリケーションの機能が損なわれる場合があります。また、ウイルス対策ソフトウェアをインストールした後に、アプリケーションが起動できなくなる場合もあります。ウイルス対策ソフトウェアの試用版をテストすることもできます。何らかの問題が発生した場合は、システムの変更を破棄して、他のベンダのウイルス対策ソフトウェアを試します。
- プログラムの試用版をインストールする。
  Windowsのコントロール パネルの [プログラムの追加と削除] コンポーネントでは、アプリケーションを完全に削除できるとは限りません。インストールしたプログラムが必要ない場合は、システムの変更を破棄します。この場合、Try&Decideでは痕跡を残さずにプログラムが削除されます。

- 疑わしいソフトウェアをインストールする。
  インストールするソフトウェアのベンダを信用していない場合や、ソフトウェアのソースが不明な場合には、このソフトウェアをインストールする前にTryモードをオンにします。何らかの問題が生じた場合は、Tryモードで行った変更を破棄します。

ファイルのリカバリ

ファイルを誤って削除してしまった後に、ごみ箱を空にしたとします。削除したファイルには重要な情報が含まれていたことに気付き、適切なソフトウェアを使用して、削除したファイルの回復を試みます。ただし、削除したファイルを回復する際に何らかの問題が発生し、回復を試みる前よりも状況が悪化する場合があります。このような場合は、次の手順を実行します。

- Tryモードをオンにします。
- 削除ファイルの回復ユーティリティを起動します。
- ユーティリティによってディスクをスキャンされ、削除したファイルまたはフォルダのエントリが検索されます。削除したエントリが見つかった場合はそのエントリが表示され、リカバリ可能なものを元に戻す機会が得られます。その際に、必要なファイルとは異なるファイルを誤って選択してしまうと、リカバリしたいファイルがユーティリティにより上書きされてしまう可能性があります。Try&Decideを使用していない場合、このようなエラーは致命的であり、ファイルは完全に失われてしまいます。
- これに対し、Tryモードがオンになっている場合は、間違った変更を破棄するだけで済み、再びTryモードをオンにしてから、正しいファイルの復元を試みることができます。ファイルの復元で最良の結果が得られるまで、このような試行を何回でも繰り返すことができます。

ウェブのプライバシー

アクセスしたWebサイトや開いたページを、誰にも知られたくない場合について考えてみましょう。プライバシーを守る権利はすべての人にあります。しかし、この際に問題になるのが、より速く快適にウェブサーフィンを行うために、サイトやページの情報の他にも、受信したクッキー、検索エンジンで実行したクエリ、入力したURLなどのさまざまな情報が、特殊な隠しファイルに保存されてしまうということです。また、これらの情報は、ブラウザのツールを使用してインターネット一時ファイルをクリアしたり、クッキーを削除したり、最近開いたウェブページの履歴をクリアしても、完全には削除されません。このため、特別なソフトウェアを使用すると、これらの情報に不正にアクセスできる場合があります。

Tryモードをオンにしておけば、安心してウェブサーフィンを楽しむことができます。後で使用履歴をすべて消去したい場合は、Tryモードで行った変更を破棄します。

Acronis Secure Zone

Acronis Secure Zone はバックアップの保存用にコンピューター上に作成できる安全な専用パーティションです。Acronis Secure Zone のファイルシステムは FAT32 です。

Acronis Secure Zone を作成すると、File Explorer では [**その他**] に表示されます。Acronis Secure Zone には通常のパーティションとしてアクセスできます。

Acronis Secure Zone がパスワードで保護されている場合、バージョンの詳細表示以外の操作にはパスワードの入力が必要です。

Acronis Secure Zone のクリーンアップ

Acronis Secure Zone に新しいバックアップ用の十分な空き領域がない場合は、次のような操作を行うことができます。

- バックアップ操作をキャンセルし、Acronis Secure Zone のサイズを大きくして、バックアップを再度実行します。
- バックアップ操作をキャンセルし、Acronis Secure Zone 内の一部のバックアップを手動で削除して、バックアップを再度実行します。
- 後に続くすべての増分バージョンや差分バージョンで同じタイプ（ファイル レベルまたはディスク レベル）の最も古いバックアップを自動的に削除するかどうかを確認します。その後も空き領域の不足が解消しない場合は、Acronis Cyber Protect Home Office に確認を求めるメッセージが表示され、次回の完全バックアップが削除されます。この操作は新しいバックアップ用の空き領域が十分に確保されるまで繰り返されます。以前のバックアップをすべて削除しても十分な空き領域がないと、バックアップはキャンセルされます。

ゾーンオーバーフローを回避するには

1. スケジュールされたバックアップを選択します。
2. **[オプション]** をクリックします。
3. **[詳細]** タブで、**[エラー処理]** セクションを展開します。
4. **[Acronis Secure Zone に十分な空き領域がない場合、最も古いバックアップを削除する]** チェックボックスを選択します。
5. **[OK]** をクリックします。

詳細については、「エラー処理」を参照してください。

Try モードでは、Acronis Secure Zone を仮のシステム変更用のストレージとして使用できません。Try&Decide セッションを停止すると、Try&Decide データは自動的にクリーンアップされます。

Acronis Cyber Protect Home Office では、Acronis Secure Zone 内のノンストップバックアップバージョンが自動的に削除されることはありません。このようなバージョンは手動でのみ削除することができます。詳細については、「Acronis Nonstop Backup のデータストレージ」を参照してください。

Acronis Secure Zone の作成および管理

1. **[スタート]** ボタン → **[Acronis]**（製品フォルダ） → **[Acronis Secure Zone]** の順にクリックします。

   Acronis Secure Zone の管理ウィザードが開きます。
2. 次のいずれかを実行します。

   Acronis Secure Zone を作成する場合は、場所とサイズを指定します。

   Acronis Secure Zone を変更する場合は、次のいずれかの操作を選択します。

- サイズの拡大/縮小
- 削除
- パスワードの変更

  ウィザードの手順に従います。

3. **[完了]** で、**[実行]** をクリックします。

注意
この処理は、コンピューターの再起動が必要になります。

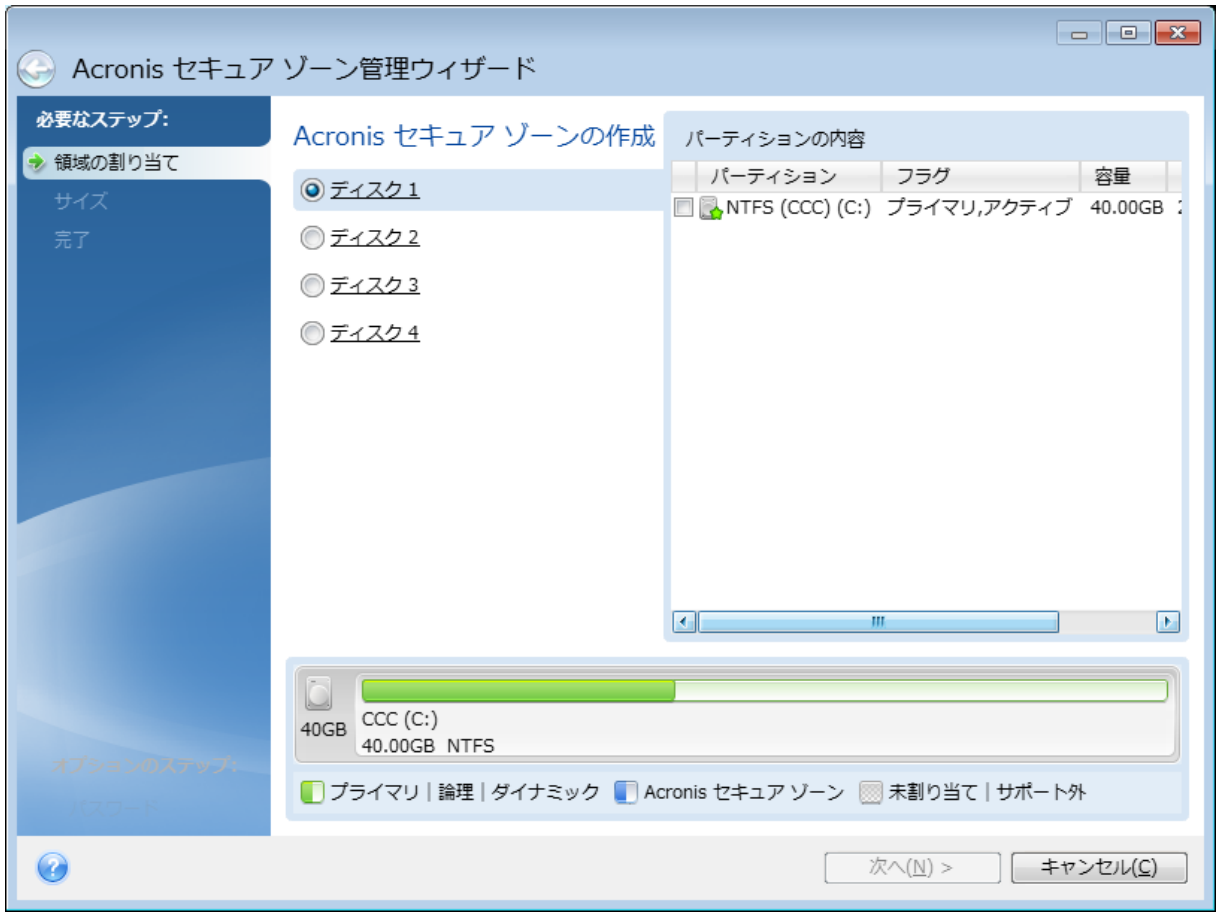
Acronis Secure Zone の場所

Acronis Secure Zone の場所を指定する手順は、次のとおりです。

1. Acronis Secure Zone を作成するハードディスクドライブを選択します。
2. 未割り当て領域や空き領域があるパーティションを1つ以上選択します。選択したパーティションは、Acronis Secure Zone に領域を追加する必要がある場合、サイズ調整されます。

   注意
   Acronis Secure Zone はダイナミックディスクおよびダイナミックボリュームには作成できません。

3. **[次へ]** をクリックします。

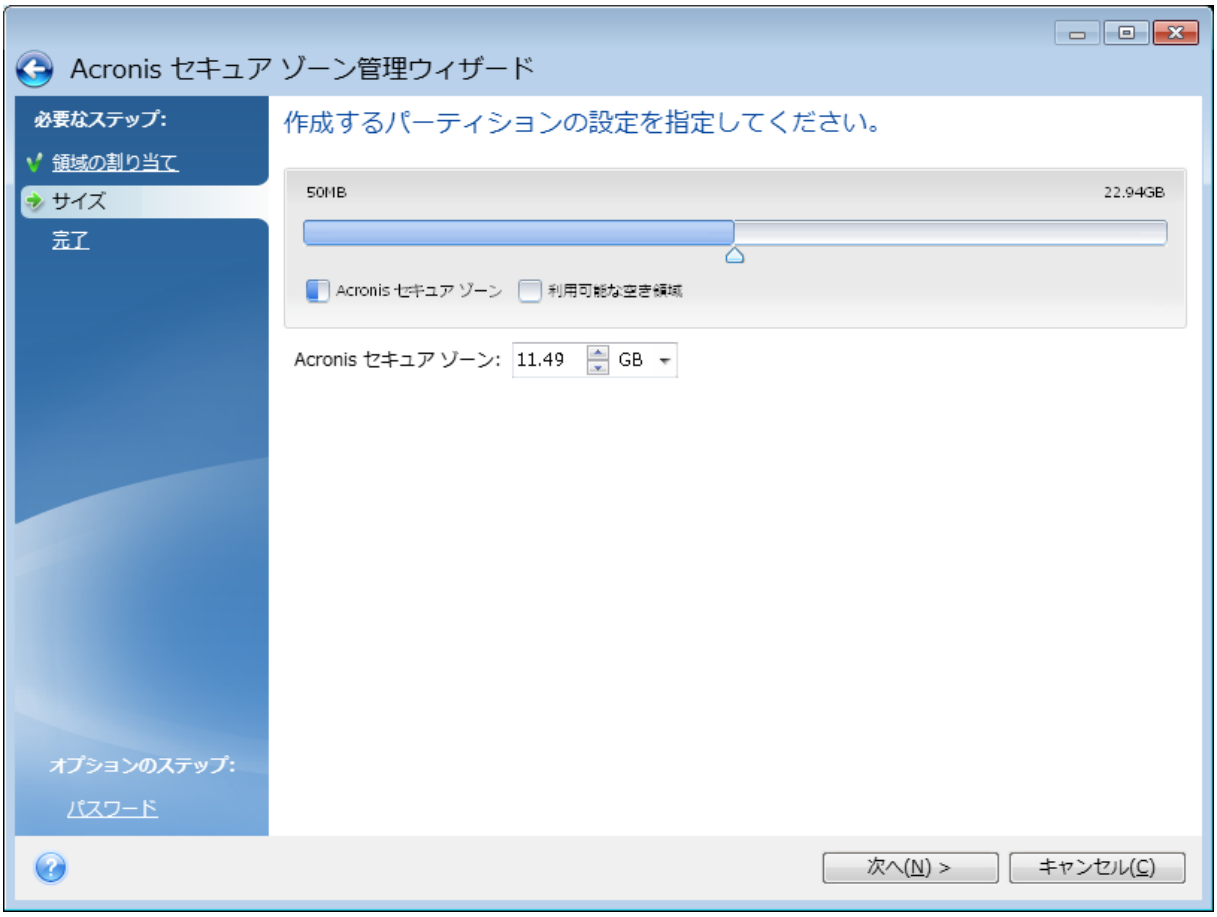


Acronis Secure Zone のサイズを拡大または縮小する手順は、次のとおりです。

1. Acronis Secure Zone のサイズを拡大するために領域を使用するパーティション、または Acronis Secure Zone のサイズの縮小後に解放される空き領域を割り当てるパーティションを選択します。未割り当ての領域が存在するパーティションも選択できます。
2. **[次へ]** をクリックします。

Acronis Secure Zone のサイズ

Acronis Secure Zone のサイズを指定するには、スライダを適切な位置までドラッグするか、正確な値を入力します。



最小サイズは、ハードディスクの構成により異なりますが、およそ50 MBです。最大サイズは、ディスクの未割り当て領域に、前の手順で選択したすべてのパーティション上の空き領域の合計を加えたものです。

Acronis Secure Zone を作成または拡大する際には、まず未割り当ての領域が使用されます。作成するゾーンのサイズに対して未割り当ての領域が不十分な場合は、選択したパーティションのサイズが縮小されます。パーティションのサイズ変更を行うと、コンピュータの再起動が必要になる場合があります。

Acronis Secure Zone のサイズを縮小する際に、ハードディスクに未割り当ての領域が存在する場合は、Acronis Secure Zone の縮小によって生じた領域と共に、その未割り当ての領域が、選択したパーティションに割り当てられます。したがって、ディスク上には未割り当ての領域はなくなります。

警告
システムパーティションを最小サイズに縮小すると、コンピューター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。

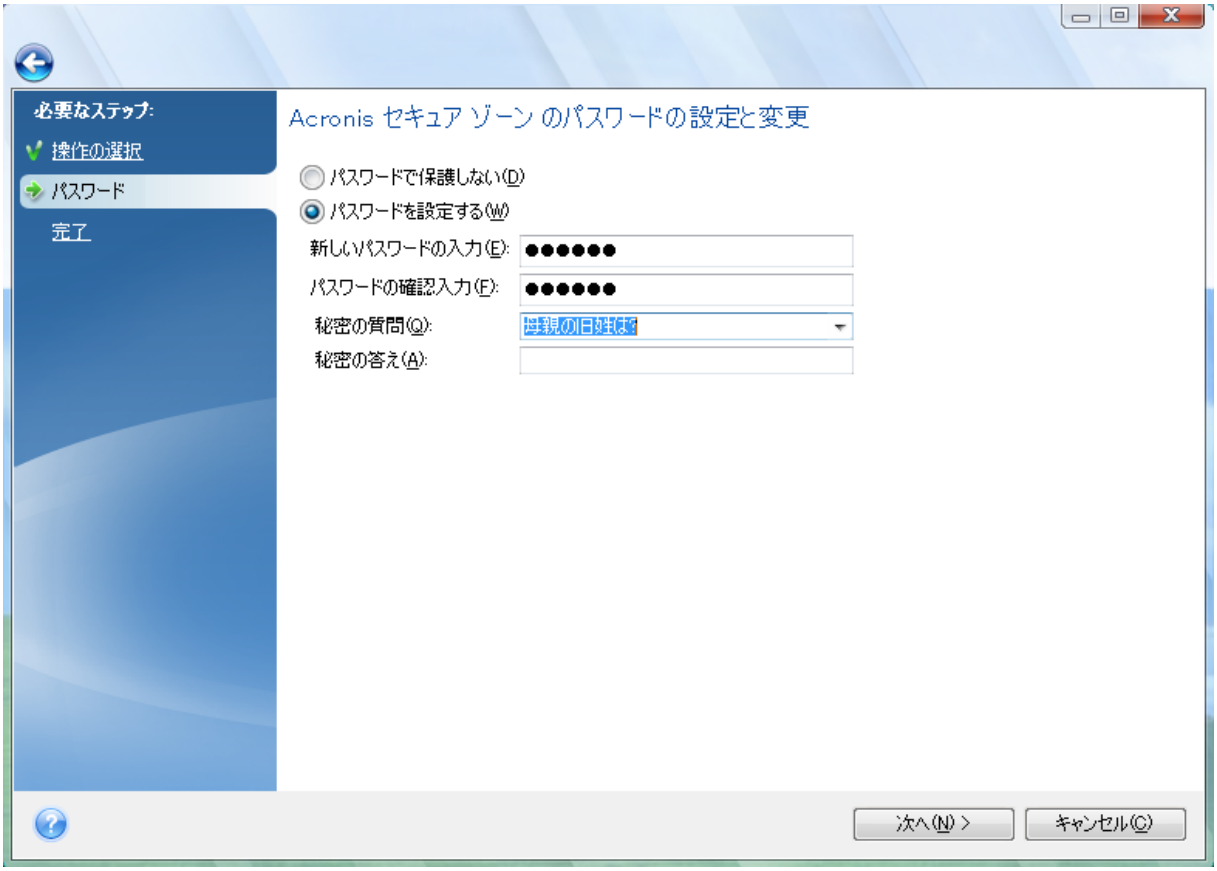
Acronis Secure Zone の保護

不正アクセスを防止するため、Acronis Secure Zone に対するパスワード保護を設定することができます。

パスワードを設定すると、プログラムは Acronis Secure Zone にあるデータのバックアップとリカバリ、イメージのマウント、バックアップの検証、または Acronis Secure Zone のサイズ変更や削除など、Acronis Secure Zone に関するどのような処理にもプログラムによりパスワードの入力が要求されます。

Acronis Secure Zone のパスワードを設定する手順は、次のとおりです。

1. **[パスワードを設定する]** を選択します。
2. **[新しいパスワードの入力]** 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]** フィールドに、先に入力したパスワードをもう一度入力します。
4. （オプションの手順）パスワードを忘れた場合に使用できる、本人確認用の秘密の質問を選択することもできます。一覧から秘密の質問を選択して、その答えを入力します。
5. 続行するには、**[次へ]** をクリックしてください。



注意
Acronis Cyber Protect Home Office の修復やアップデートはパスワードに影響しません。ただし、ディスク上に Acronis Secure Zone を残したままプログラムが削除され再度インストールされた場合、その Acronis Secure Zone のパスワードはリセットされます。

Acronis Secure Zone の削除

警告
Acronis Secure Zone を削除すると、そのゾーン内に保存されているバックアップはすべて自動的に消去されます。

Acronis Secure Zone から解放される領域を追加するパーティションを選択します。複数のパーティションを選択した場合、領域は各パーティションのサイズに比例して配分されます。

また、プログラムをアンインストールする際に Acronis Secure Zone の削除を選択することもできます。

新しいハードディスクの追加

ディスクの空き領域が不足してデータを保存できなくなったときには、古いハードディスクを新しい大容量のハードディスクに交換するか、データ保存専用の新しいハードディスクを追加して古いハードディスクのシステムをそのまま残しておきます。

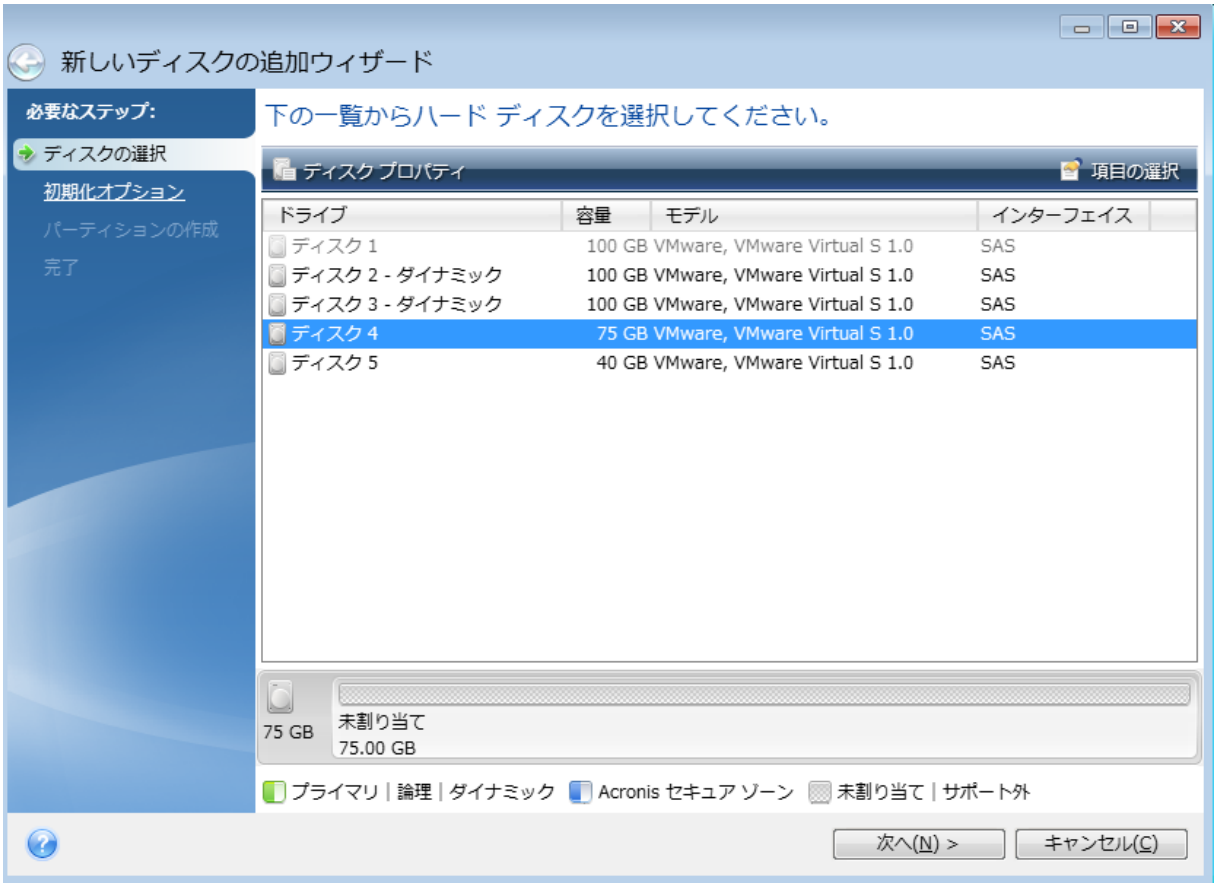
新しいハードディスクを追加する手順は、次のとおりです。

1. コンピュータをシャットダウンしてから、新しいディスクをインストールします。
2. コンピュータの電源を入れます。
3. **[スタート]** ボタン > **[Acronis]**（製品フォルダ）> **[新しいディスクの追加]** の順にクリックします。
4. ウィザードの手順に従います。
5. **[完了]** で、ディスクレイアウトが望みどおりに設定されていることを確認してから、**[実行]** をクリックします。

ハードディスクの選択

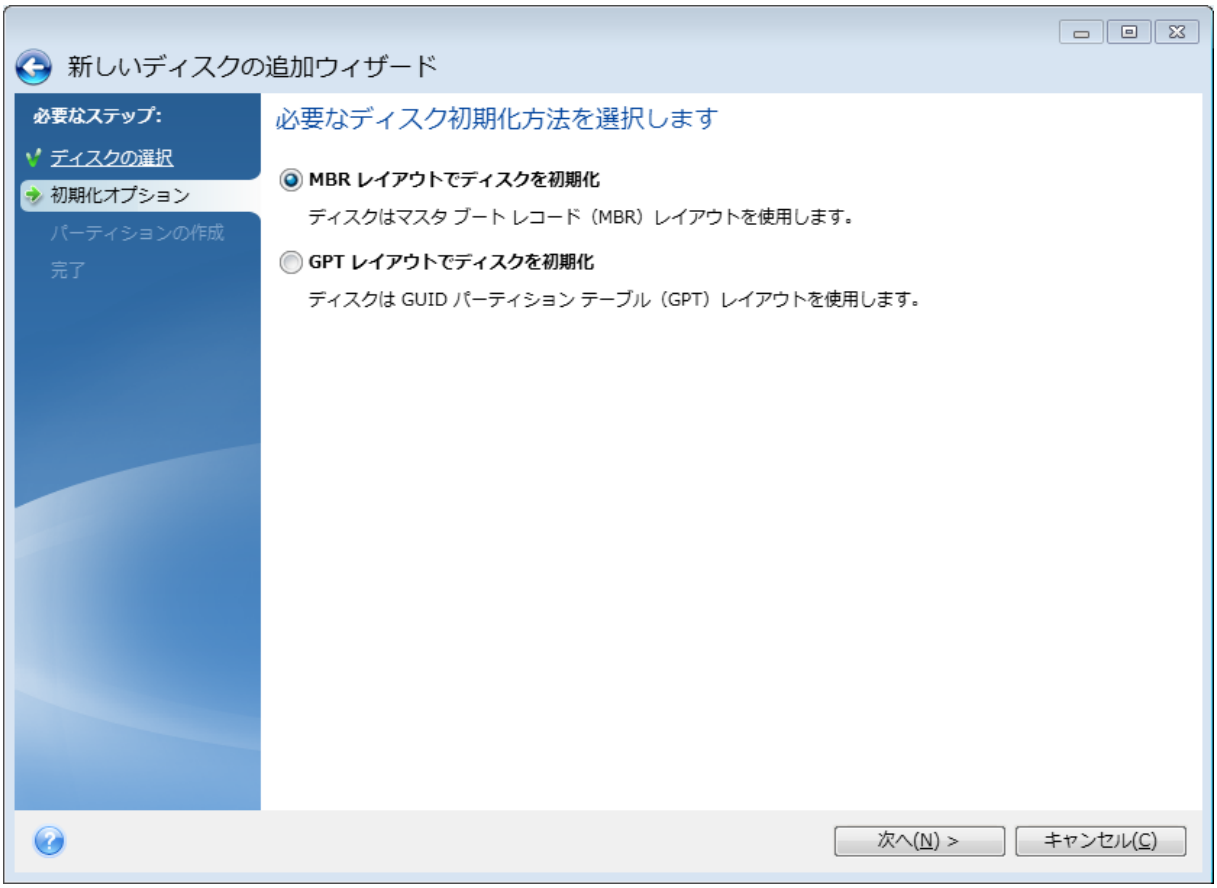
コンピュータに追加したハードディスクを選択します。複数のハードディスクを追加した場合は、そのうちの1台を選択し、**[次へ]** をクリックして先に進みます。後で、新しいディスクの追加ウィザードを起動し、別のディスクを追加することもできます。

注意
新しいディスクにパーティションがあると、これらのパーティションは削除されるという警告メッセージが Acronis Cyber Protect Home Office に表示されます。



初期化方法の選択

Acronis Cyber Protect Home Office は MBR と GPT の両方のパーティショニングに対応しています。GUID パーティション テーブル（GPT）は、ハード ディスクの新しいパーティショニング方法であり、従来の MBR よりもパーティショニング方法として優れています。オペレーティング システムが GPT ディスクをサポートする場合、新しいディスクを GPT ディスクとして初期化することを選択できます。



- GPT ディスクを追加するには、**[GPT レイアウトでディスクを初期化する]** をクリックします。
- MBR ディスクを追加するには、**[MBR レイアウトでディスクを初期化する]** をクリックします。

該当の初期化方法を選択したら、**[次へ]** をクリックします。

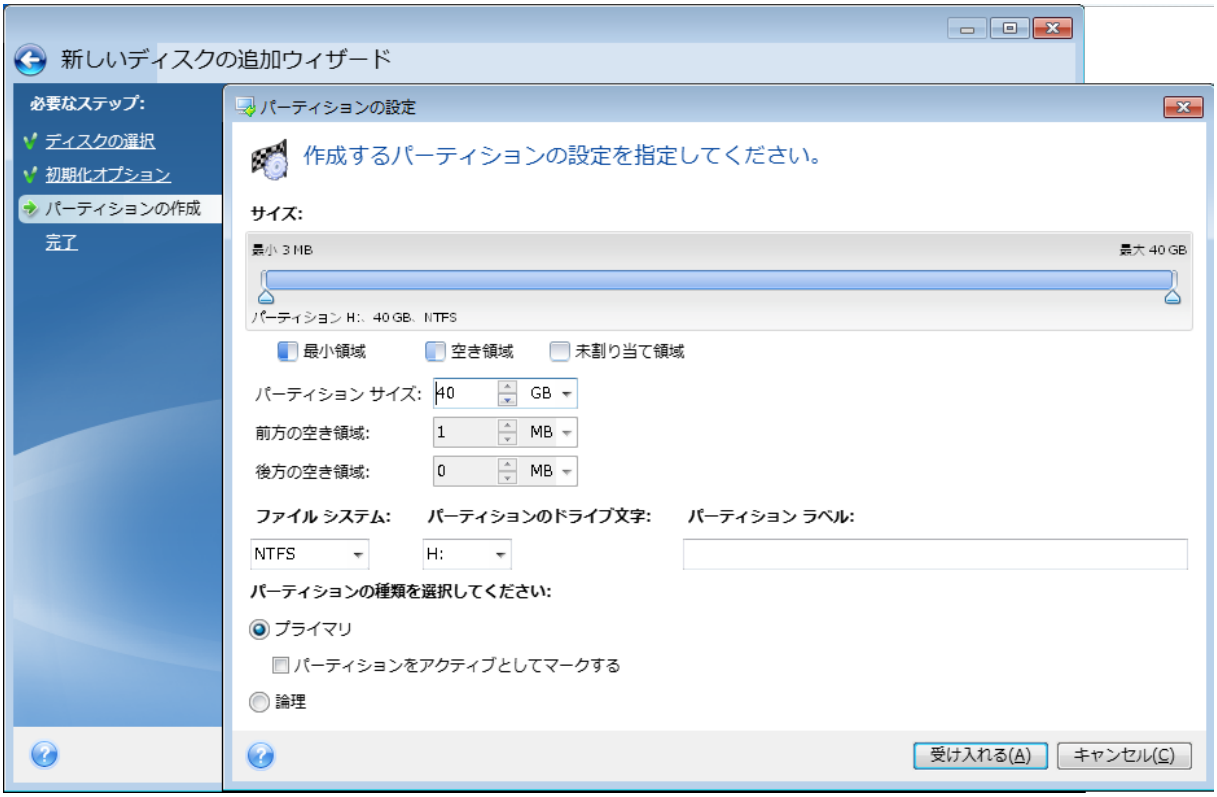
新しいパーティションの作成

ハードディスクの空き領域を使用するには、パーティションが作成されている必要があります。パーティショニングは、ハードディスクの空き領域を、パーティションと呼ばれる論理領域に分割する処理です。パーティションごとに、ドライブ文字を割り当てたり、独自のファイルシステムをインストールしたりして、別々のディスクとして利用することができます。

新しいパーティションを作成する手順は、次のとおりです。

1. ウィザードの **[パーティションの作成]** で未割り当て領域を選択してから、**[新しいパーティションを作成する]** をクリックします。
2. 作成するパーティションについて、以下の設定を指定します。
   - サイズと位置
   - ファイル システム
   - パーティションの種類（MBRディスクでのみ使用可能）
   - パーティションのドライブ文字とラベル

   詳細については、「パーティションの設定」を参照してください。
3. **[確定]** をクリックします。



パーティションの設定

サイズ

パーティションのサイズを変更するには、以下のいずれかを実行します。

- パーティションの境界にマース カーソルを置きます。カーソルが二重矢印になったら、この二重矢印をドラッグしてパーティションのサイズを拡大または縮小します。
- 希望するパーティションのサイズを **[パーティション サイズ]** フィールドに入力します。

パーティションを移動するには、以下のいずれかを実行します。

- パーティションを新しい位置までドラッグします。
- 希望するサイズを **[前方の空き領域]** フィールドまたは **[後方の空き領域]** フィールドに入力します。

注意
パーティションを作成する場合は、作成パーティションの前にシステムのニーズに合わせて未割り当て領域が予約されることがあります。

ファイル システム

パーティションをフォーマットしないままにするか、または次のファイル システムの種類から選択することができます。

- **[NTFS]** は、Windows NT、Windows 2000、Windows XP以降のオペレーティングシステムのネイティブのファイルシステムです。これらのオペレーティングシステムを使用している場合に選択して

ください。Windows 95/98/Me および DOS からは、NTFS パーティションにアクセスできないことに注意してください。

- **[FAT32]** は、FAT ファイル システムの 32 ビット版で、最大 2 TB のボリュームをサポートします。
- **[FAT 16]** は、DOS ネイティブのファイル システムです。ほとんどのオペレーティングシステムはこのファイル システムを認識します。ただし、ディスク ドライブのサイズが 4 GB を超える場合は、FAT16 でフォーマットすることはできません。
- **[Ext2]** は、Linux ネイティブのファイル システムです。十分に高速ですが、ジャーナリング ファイル システムではありません。
- **[Ext3]** は、Red Hat Linux Version 7.2 で正式に導入された、Linux のジャーナリング ファイル システムです。Ext2 との上位および下位互換性があります。複数のジャーナリング モードを備え、32 ビットおよび 64 ビット アーキテクチャの双方で、プラットフォームに依存しない幅広い互換性を実現します。
- **[Ext4]** は、Linux の新しいファイル システムです。このシステムでは、ext3 よりも機能が拡張されています。このシステムでは、ext2 および ext3 に対する下位互換性が完全に維持されています。ただし、ext3 の ext4 に対する上位互換性は限定的です。
- **[ReiserFS]** は、Linux のジャーナリング ファイル システムです。一般的に Ext2 より信頼性が高く高速です。Linux のデータ パーティションにはこれを選択します。
- **[Linux Swap]** は、Linux 用のスワップ パーティションです。Linux 用のスワップ領域を広げる必要がある場合に選択してください。

ドライブ文字

パーティションに割り当てるドライブ文字を選択します。**[自動]** を選択すると、アルファベット順で最初の未使用のドライブ文字が割り当てられます。

パーティション ラベル

パーティション ラベルは、パーティションを簡単に識別できるように割り当てる名前です。たとえば、オペレーティングシステムがインストールされているパーティションは System、データが保存されているパーティションは Data、などのように名前を付けます。パーティション ラベルはオプションの属性です。

パーティションの種類（これらの設定は、MBR ディスクのみで利用できます）

新しいパーティションの種類を「プライマリ」または「論理」として指定することができます。

- **プライマリ**: このパーティションからコンピュータを起動できるようにする場合は、このパラメータを選択します。それ以外の場合は、論理ドライブとして作成することをおすすめします。各ドライブを、4 つのプライマリ パーティションだけにするか、または 3 つのプライマリ パーティションと 1 つの拡張パーティションにすることができます。

注意
複数のプライマリパーティションがある場合に、アクティブになるのは一度に1つだけです。他のプライマリパーティションは隠しパーティションとなり、オペレーティングシステムからアクセスできなくなります。

  - **パーティションをアクティブとしてマークする**: このパーティションにオペレーティングシステムをインストールする予定の場合は、このチェック ボックスをオンにします。
- **[論理]**: このパーティションにオペレーティングシステムをインストールして起動する予定がない場合は、このパラメータを選択します。論理ドライブは、パーティション分割されて独立した単位として割り当てられた物理ディスクの一部ですが、それぞれ別のドライブとして機能します。

セキュリティ ツールおよびプライバシー ツール

Acronis DriveCleanser

Acronis DriveCleanser では、選択したハードディスクやパーティション上のすべてのデータを完全に消去できます。この消去には、既存のアルゴリズムのいずれかを使用するか、専用のアルゴリズムを作成できます。詳細については、「アルゴリズムの選択」を参照してください。

ハード ディスク ドライブのクローン作成が必要な理由

破棄対象の古いハード ディスク ドライブがフォーマットされている場合、データは完全に消去されないため、取得されてしまう可能性があります。これにより、個人情報が不正に利用されることも考えられます。こうしたことが起こらないよう、次に当てはまる場合は Acronis DriveCleanser を使用することをお勧めします。

- 古いハード ディスク ドライブを新しいハード ディスク ドライブに交換し、古いドライブをこれ以上使用する予定がない。
- 古いドライブを親戚や友人に譲る。
- 古いハード ディスク ドライブを売却する。

使用方法Acronis DriveCleanser

ディスク上のデータを完全に消去する手順は、次のとおりです。

1. **[スタート]** ボタン > **[Acronis]**（製品フォルダ）> **[Acronis DriveCleanser]** の順にクリックします。
   Acronis DriveCleanser ウィザードが開きます。
2. **[ソースの選択]** で、消去するディスクとパーティションを選択します。詳細については、「ソースの選択」を参照してください。
3. **[アルゴリズムの選択]** で、データの消去に使用するアルゴリズムを選択します。詳細については、「アルゴリズムの選択」を参照してください。
4. （オプションの手順）専用のアルゴリズムを作成することもできます。詳細については、「ユーザー定義アルゴリズムの作成」を参照してください。

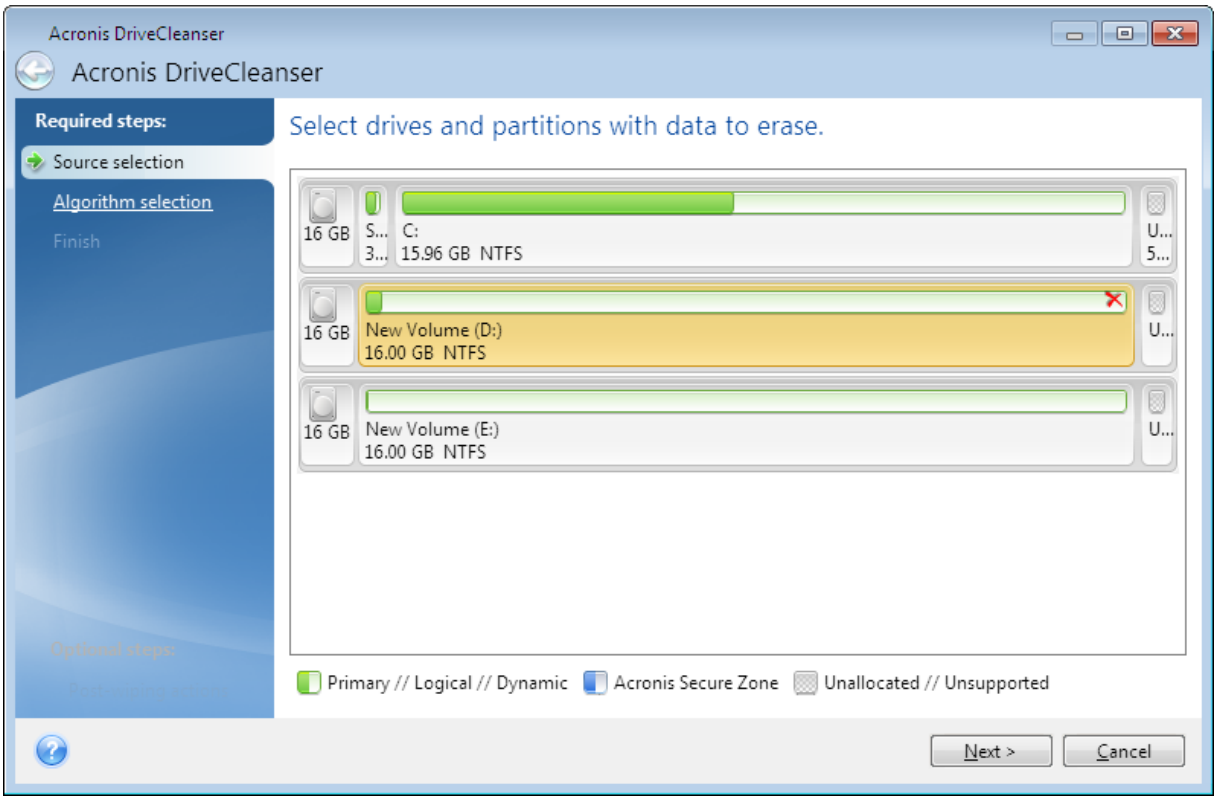
5. （オプションの手順）**[消去後の処理]** で、データの消去が完了したときのパーティションやディスクの処理方法を選択します。詳細については、「消去後の処理」を参照してください。
6. **[完了]** で、指定した設定が正しいことを確認します。処理を開始するには、**[選択されているパーティションを完全に消去する]** チェック ボックスをオンにし、**[実行]** をクリックします。

警告
選択したパーティションの合計サイズと選択したデータ消去アルゴリズムによっては、データ消去に数時間がかかることがあります。

ソースの選択

[ソースの選択] で、データを消去するディスクとパーティションを選択します。

- パーティションを選択するには、該当する四角形をクリックします。赤いマーク（）は、そのパーティションが選択されていることを示します。
- ハードディスク全体を選択するには、ディスクアイコン（）をクリックします。

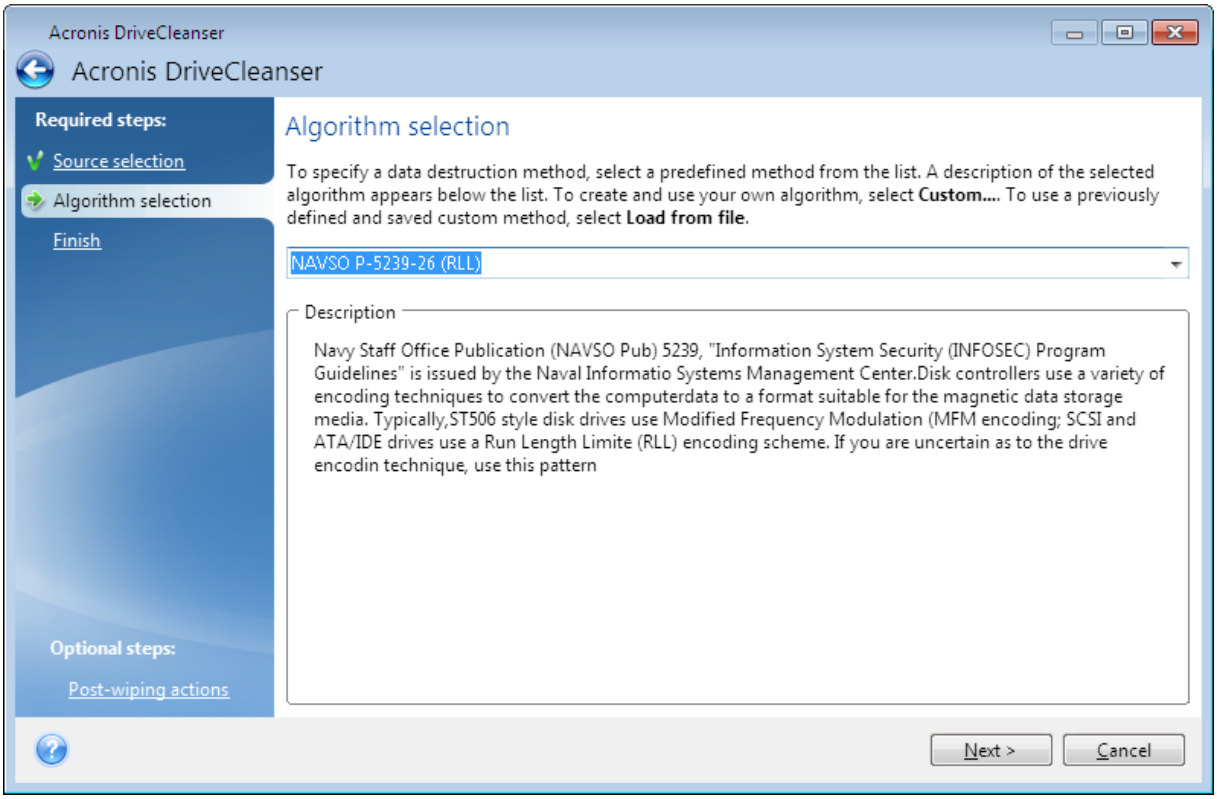


注意
Acronis DriveCleanser は、ダイナミックディスクおよび GPT ディスクのパーティションを削除できないため、これらのパーティションは表示されません。

アルゴリズムの選択

[アルゴリズムの選択] で、以下のいずれかを実行します。

- 既存のアルゴリズムのいずれかを使用するには、希望するアルゴリズムを選択します。詳細については、「ハードディスクの消去方法」を参照してください。
- （上級ユーザーのみ）ユーザー定義アルゴリズムを作成するには、**[ユーザー定義]** を選択します。**[アルゴリズムの定義]** でアルゴリズムの作成を続けます。後で、作成したアルゴリズムを拡張子 .alg のファイルに保存することができます。
- 以前保存したユーザー定義アルゴリズムを使用するには、**[ファイルから読み込む]** を選択し、アルゴリズムが保存されているファイルを選択します。



ハード ディスクの消去方法

情報をハード ディスクから削除するときに、安全ではない手段（たとえば Windows での単純な削除）を使用すると、その情報は簡単にリカバリできてしまいます。特殊な機器を使用すれば、繰り返し上書きされた情報でもリカバリできます。

ハード ディスクに格納されるデータは、1 と 0 の 2 進数のシーケンスとなっており、このことはディスクの部分ごとに磁化を変化させるという方法で表現されます。一般的に言って、ハード ディスクに書き込まれた 1 はハードディスク コントローラによって 1 として読み取られ、0 は 0 として読み取られます。ただし、0 に 1 を上書きすると、ある条件の下ではその結果は 0.95 となり、1 を 1 に上書きすると結果は 1.05 となります。このような違いは、コントローラにとっては無関係です。しかし、特殊な機器を使用すれば、「下に隠れている」0 と 1 のシーケンスを簡単に読み取ることができます。

情報の抹消方法

情報の抹消を保証する技術に関する具体的な理論は、Peter Gutmann 氏による論文で紹介されています。『Secure Deletion of Data from Magnetic and Solid-State Memory』（https://www.cs.auckland.ac.nz/~pgut001/pubs/secure_del.html）を参照してください。

No.	アルゴリズム（書き込み方法）	工程数	記録
1.	米国国防省準拠DoD 5220.22-M方式	4	第 1 工程 – ランダムに選択された記号を各バイトの各セクタに書き込みます。第 2 工程 – 第 1 工程で書き込まれた値の補数を書き込みます。第 3 工程 – ランダムな記号を再び書き込みます。第 4 工程 – 書き込み結果を確認します。
2.	米国海軍準拠NAVSO P-5239-26-RLL方式	4	第 1 工程 – 0x01 を全セクタに書き込みます。第 2 工程 – 0x27FFFFFF を書き込みます。第 3 工程 – ランダムな記号のシーケンスを書き込みます。第 4 工程 – 確認します。
3.	米国海軍準拠NAVSO P-5239-26-MFM方式	4	第 1 工程 – 0x01 を全セクタに書き込みます。第 2 工程 – 0x7FFFFFFF を書き込みます。第 3 工程 – ランダムな記号のシーケンスを書き込みます。第 4 工程 – 確認します。
4.	ドイツVSITR方式	7	第 1 ～第 6 工程 – 0x00 と 0xFF を交互に書き込みます。第 7 工程 – 0xAA を書き込みます。つまり、0x00、0xFF、0x00、0xFF、0x00、0xFF、0xAA となります。
5.	ロシアGOST P50739-95方式	1	論理ゼロ（数値 0x00）を各セクタの各バイトに書き込みます（セキュリティレベルが 6 ～ 4 のシステムの場合）。 ランダムに選択された記号（数値）を各セクタ各バイトに書き込みます（セキュリティレベルが 3 ～ 1 のシステムの場合）。
6.	グートマン（Peter Gutmann）方式	35	非常に高度な方式。この方式は、ハードディスクの情報抹消についてのPeter Gutmann氏の理論に基づいている（『Secure Deletion of Data from Magnetic and Solid-State Memory』を参照）。
7.	Bruce Schneier方式	7	Bruce Schneierが著書『応用暗号論』で提唱している7回の工程で上書きする方法。第 1 工程では 0xFF、第 2 工程では 0x00 を書き込み、その後の 5 工程では暗号学的にセキュリティの高い擬似ランダムシーケンスを書き込みます。
8.	高速	1	全セクタに対して論理値ゼロ（数値0x00）で抹消。

ユーザー定義アルゴリズムの作成

消去アルゴリズムの定義

[アルゴリズムの定義] には、これから作成するアルゴリズムのテンプレートが表示されます。

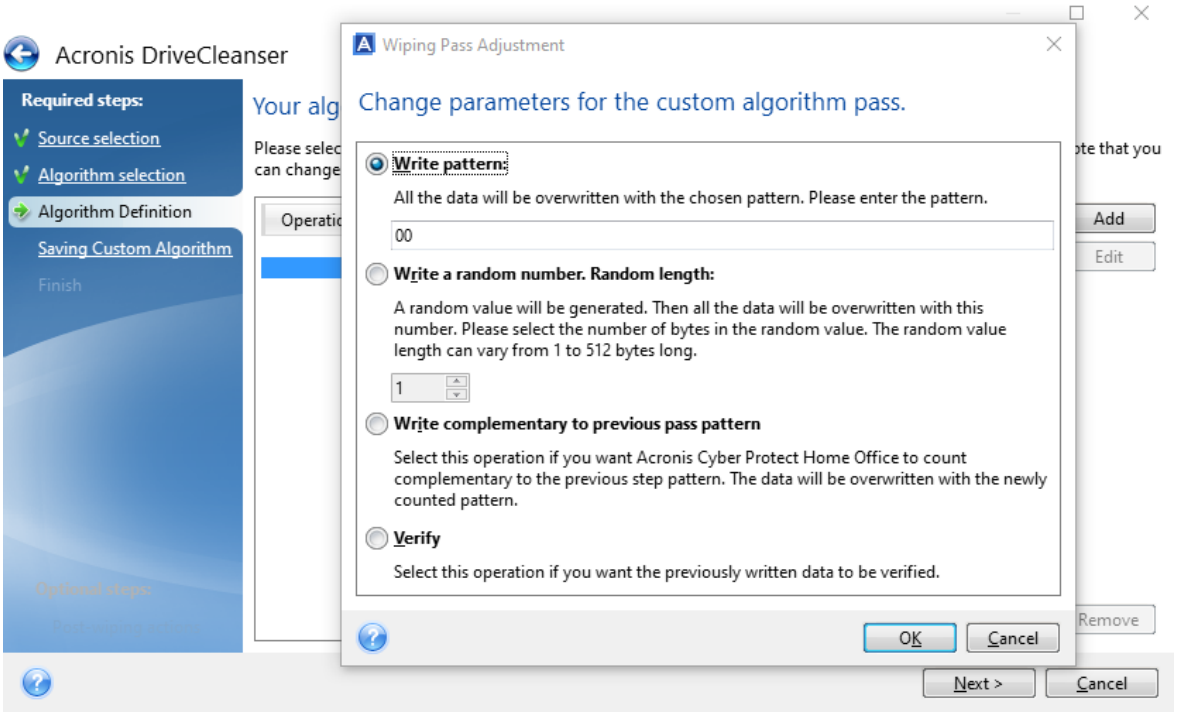
この表には次の内容が表示されています。

- 最初の列は処理の種類（記号をディスクに書き込む、書き込みを検証する）を示します。
- 2番目の列はディスクに書き込むデータのパターンを示します。

各行で、工程の際に実行する処理を定義します。アルゴリズムを作成するには、この表に、データを安全に消去するのに十分と思われる行を追加します。

新しい工程を追加する手順は、次のとおりです。

1. **[追加]** をクリックします。[消去時の工程の調整] ウィンドウが表示されます。



2. オプションを選択します。
   - **パターンを書き込む**

     0x00、0xAA、0xCDなど、16進数の値を入力します。これらの値は1バイトの長さですが、512バイトまで設定できます。このような値以外にも、512バイトまでの任意の長さで16進数のランダム値を入力できます。

     注意
     バイナリ値が10001010（0x8A）の場合、この補数のバイナリ値は01110101（0x75）となります。

   - **ランダムな値を書き込む。ランダムな長さ**

     ランダムな値の長さをバイト単位で指定します。
   - **前工程のパターンの補数を書き込む**

     Acronis Cyber Protect Home Office は前工程でディスクに書き込まれた値に補足値を追加します。
   - **ベリファイ**

     Acronis Cyber Protect Home Office は前工程でディスクに書き込まれた値を検証します。
3. **[OK]** をクリックします。

既存の工程を編集する手順は、次のとおりです。

1. 該当する行を選択して **[編集]** をクリックします。
   [消去時の工程の調整] ウィンドウが表示されます。

   注意
   複数の行を選択した場合、新しい設定は選択した工程すべてに適用されます。

2. 設定を変更して **[OK]** をクリックします。

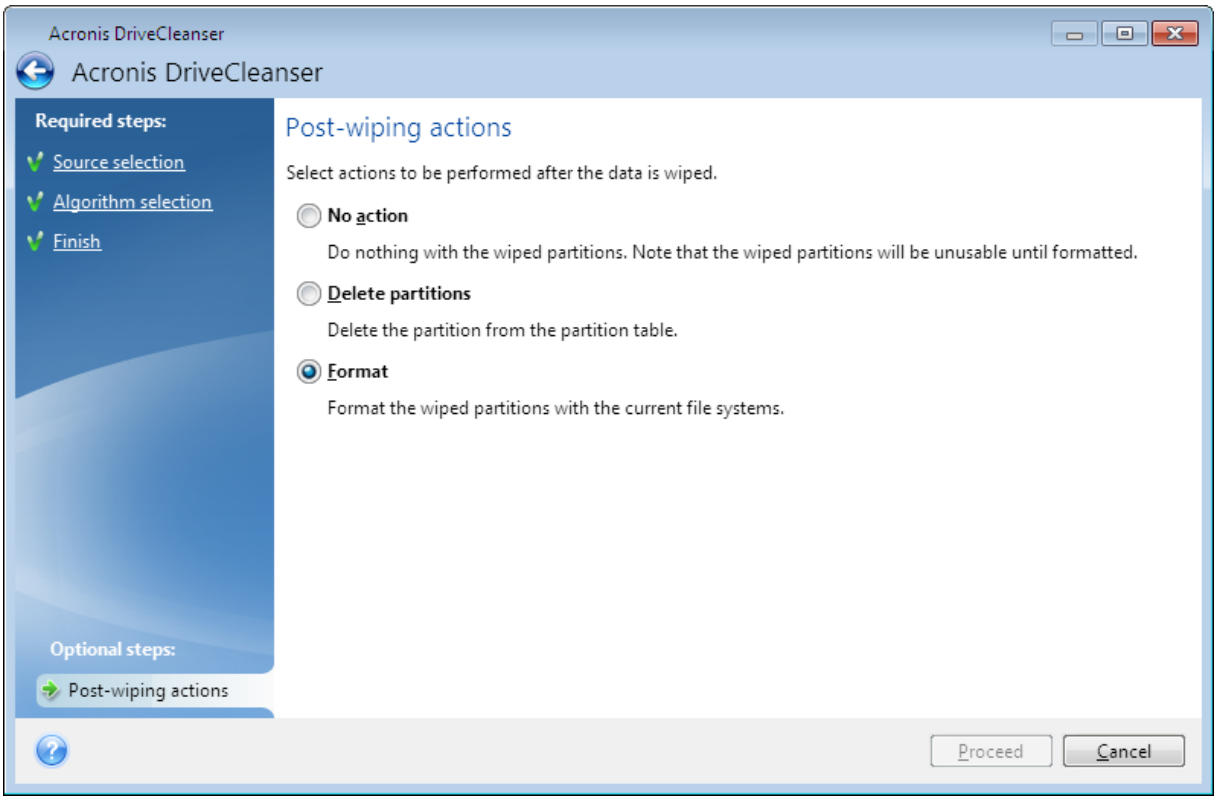
ファイルへのアルゴリズムの保存

1. **[ユーザー定義消去アルゴリズムの保存]** で、**[ファイルに保存]** を選択して **[次へ]** をクリックします。
2. 表示されるウィンドウで、ファイルの名前と場所を指定し、**[OK]** をクリックします。

消去後の処理

[消去後の処理] ウィンドウでは、データ消去対象として選択されたパーティションに対して実行する処理を選択できます。Acronis DriveCleanser では、3 つのオプションが用意されています。

- **[何もしない]**: 以下で選択されているアルゴリズムを使用してデータの消去のみを行います。
- **[パーティションを削除する]**: データを消去して、パーティションを削除します。
- **[フォーマットする]**: データを消去して、パーティションをフォーマットします（デフォルト）。



システムのクリーンアップ

システム クリーンアップ ウィザードを使用して、ユーザー名、パスワードなどの個人情報を含む、コンピュータ操作に関するすべての履歴を安全に削除することができます。

以下の処理を実行することができます。

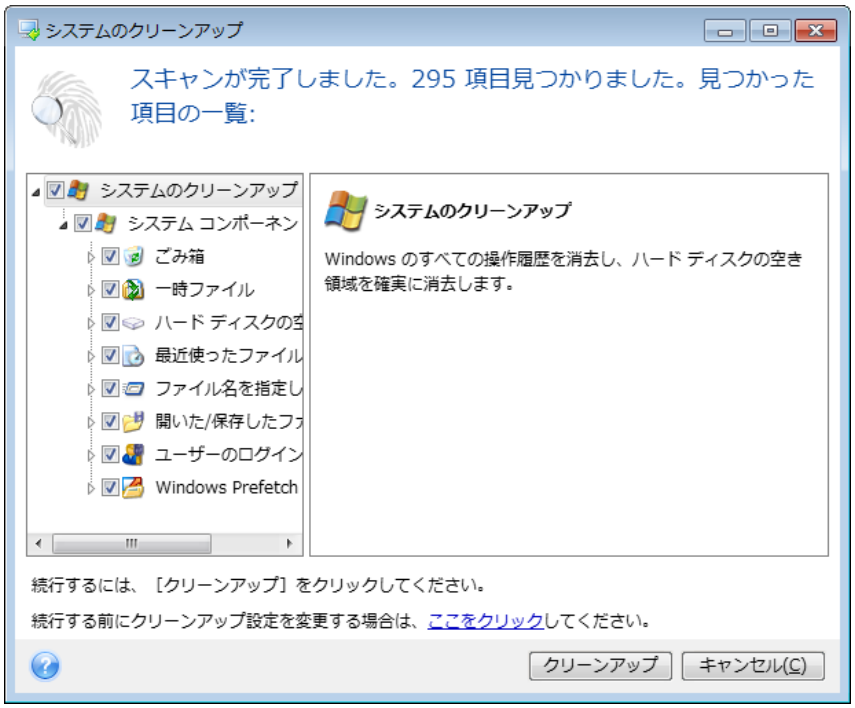
- **Windowsのごみ箱**のデータを安全に消去します。
- **一時ファイル**を、該当するWindowsフォルダから削除します。
- **ハードディスクの空き領域**に以前保存されていた情報の痕跡をクリーンアップします。
- 接続されているディスクやローカルエリアネットワーク内のコンピュータに対する**ファイルとコンピュータ検索**の履歴を削除します。
- **最近使ったドキュメント**の一覧を消去します。
- 「**ファイル名を指定して実行**」の一覧を消去します。
- **開いた/保存したファイル**の履歴を消去します。
- **ネットワーク認証情報**を使用してユーザーが接続したネットワークプレースの一覧を消去します。
- Windowsによって保存されている、最近実行したプログラムに関する情報を **Windows Prefetchディレクトリ** から消去します。

注意
Windows 7以降のオペレーティングシステムでは、ファイルやコンピュータの検索に関する情報は保存されません。また、開いたファイルや保存したファイルの情報は別の方法でレジストリに保存されますので、ウィザードでは異なる方法でその情報が表示されます。

注意
Windows はセッション終了までパスワードを保存するため、ネットワークユーザーの資格情報の一覧を消去しても、ログアウトまたはコンピューターの再起動によって現在の Windows セッションを終了するまでは処理は有効になりません。

システムクリーンアップウィザードを開始するには、[**スタート**] ボタン → [**Acronis**]（製品フォルダ）→ [**システムクリーンアップ**] の順にクリックします。

ウィザードを起動すると、Windows に保存されたユーザー操作の履歴が検索されます。検索が終了すると、ウィザード ウィンドウの上部に結果が表示されます。



検索結果を表示して、削除する項目を手動で選択することができます。

続行する前にクリーンアップ設定を変更する場合は、[**ここをクリック**] ハイパーリンク テキストをクリックしてください。

[**クリーンアップ**] をクリックすると、見つかった項目が削除されます。

クリーンアップの設定

クリーンアップの設定ウィンドウで、すべてのシステムコンポーネントのクリーンアップ設定を変更できます。設定の中には、すべてのコンポーネントに適用されるものもあります。

コンポーネントに対するクリーンアップの設定を変更する手順は、次のとおりです。

- ツリーの [**システムコンポーネント**] 項目を展開し、変更が必要なコンポーネントのクリーンアップ設定を選択します。クリーンアップウィザードでコンポーネントのスキャンを有効または無効にできます。この設定を行うには、[**有効**] チェックボックスをオンまたはオフにします。
  必要に応じて、コンポーネントを展開してさらにカスタマイズすることもできます。カスタマイズできる項目には、データ消去方法、消去するファイル、ローカルネットワーク内のコンピュータの検索に使用されたレジストリ検索文字列をクリーンアップするか否かなどがあります。カスタマイズするには、コンポーネントの近くにある三角形をクリックし、一覧からオプションを選択して設定を指定します。
- 目的のコンポーネントのプロパティを設定したら、[**OK**] をクリックして設定を保存します。これらの設定は、次回クリーンアップウィザードを起動したときにデフォルトとして使用されます。

変更したクリーンアップ設定はいつでもプログラムのデフォルト設定に戻すことができます。戻すには、[**デフォルトに戻す**] ボタンをクリックしてください。

システムコンポーネント:

- ごみ箱
- 一時ファイル
- ハードディスクの空き領域
- 検索したコンピュータの一覧
- 検索したファイルの一覧
- 最近使用したドキュメントの一覧
- ファイル名を指定して実行の一覧
- 開いた/保存したファイルの履歴
- ユーザーのログイン情報
- Windowsプリフェッチディレクトリ

デフォルトのクリーンアップオプション

クリーンアップのデフォルトのオプションは、**[データ消去方法]** オプションのページの **[クリックするとこの設定を変更できます]** リンクをクリックして変更できます。

デフォルトのクリーンアップオプションを変更する手順は、次のとおりです。

1. 変更が必要なコンポーネントのクリーンアップ設定をツリーから選択します。
2. オプションを変更したら、**[OK]** をクリックして設定を保存します。

変更したクリーンアップ設定はいつでもプログラムのデフォルト設定に戻すことができます。戻すには、**[デフォルトに戻す]** ボタンをクリックしてください。

全般

デフォルトでは、各クリーンアップ手順が終了するたびに [概要] ダイアログウィンドウが表示されます（**[概要の表示]** チェックボックスがオンになっている場合）。このウィンドウを表示する必要がない場合は、チェックボックスをオフにしてください。

クリーンアップオプション

システムクリーンアップには、よく知られているさまざまなデータ消去方法が使用されます。ここでは、他のすべてのコンポーネントでデフォルトで使用される共通のデータ消去方法を選択できます。

データ消去方法については、このガイドの「ハードディスクの消去方法」で詳しく説明されています。

特定のクリーンアップオプション

次のクリーンアップオプションをカスタマイズできます。

- データ消去方法
- デフォルトオプション
- ファイル
- ドライブ空き領域
- コンピュータ

- コマンド
- ネットワークプレースのフィルタ

データ消去方法

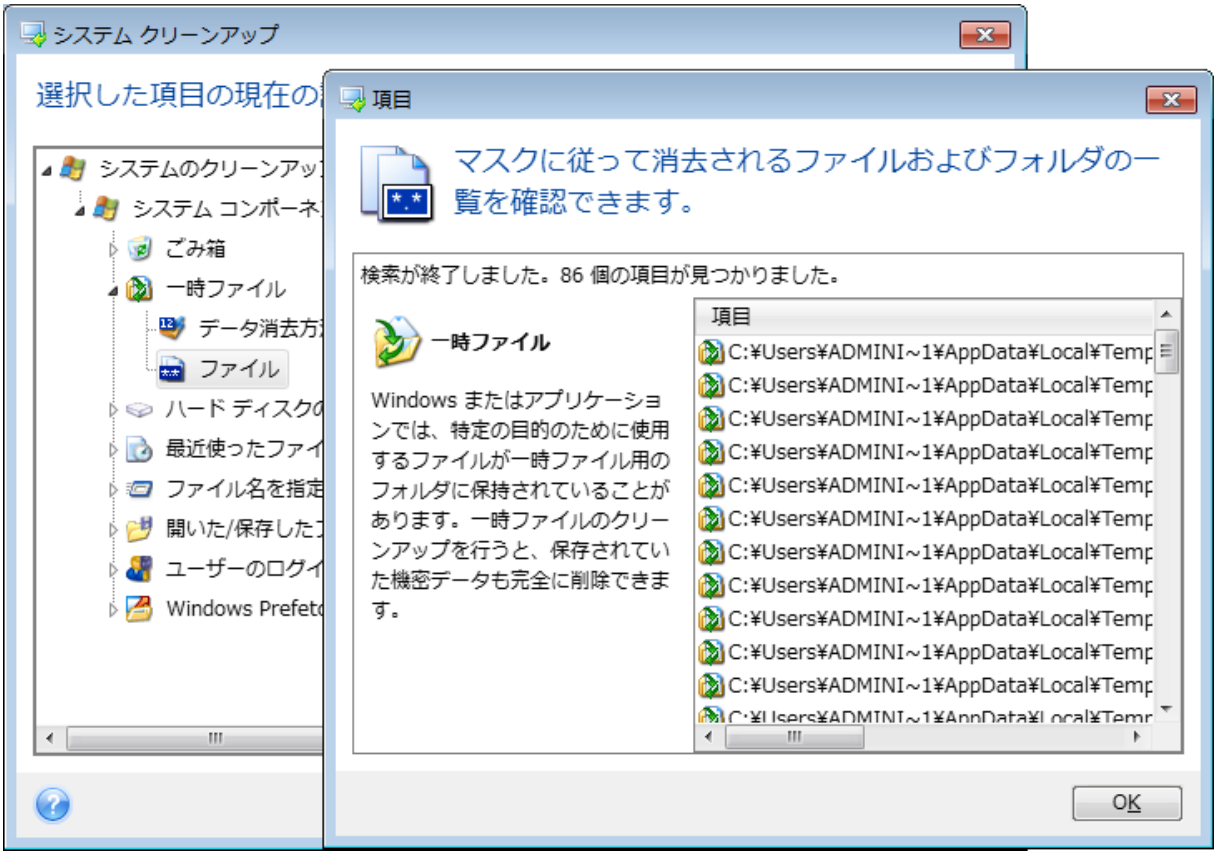
システムクリーンアップには、よく知られているさまざまなデータ消去方法が使用されます。ここでは使用するデータ消去方法を選択する必要があります。

- **[共通の方法を使用する]** - このパラメータがオンの場合は、デフォルトの方法が使用されます（初期設定は「高速」方式です）。
  別の消去方法をデフォルトとして設定するには、該当するリンクをクリックします。
- **[このコンポーネントにユーザー定義の方法を使用する]** - このパラメータを選択すると、あらかじめ設定されているデータ消去方法をドロップダウンリストから選択できます。

データ消去方法については、このガイドの「ハードディスクの消去方法」で詳しく説明されています。

ファイル

[ファイル] の設定では、システムクリーンアップウィザードによってクリーンアップするファイルを指定します。検索文字列を指定することもできます。



Windowsオペレーティングシステムでは、ファイル名の全体または一部を検索文字列で表現することができます。検索文字列には、任意の英数字と、カンマなどの記号およびワイルドカードを使用できます。値の例を次に示します。

- *.* - ファイル名や拡張子にかかわらず、すべてのファイルが削除されます。
- *.doc - 指定された拡張子ファイル（この例ではMicrosoft Wordの文書ファイル）が削除されます。
- read*.* - ファイル名が「read」で始まるファイルが拡張子に関係なくすべて削除されます。
- read?.* - 「read」で始まる5文字のファイル名を持つファイルが（5文字目は任意の文字）、拡張子に関係なくすべて削除されます。
  たとえば上記の最後の検索文字列では、read1.txtおよびready.docファイルは削除されますが、readyness.txtは、ファイル名が5文字より長いため削除されません（拡張子はファイル名の文字数に含まれません）。

検索文字列を複数入力するには、次の例のようにセミコロンで区切ります。

.bak;.tmp;*.~~~（検索文字列の間にスペースは不要）

検索文字列の1つ以上に名前が一致するファイルが、すべて削除されます。

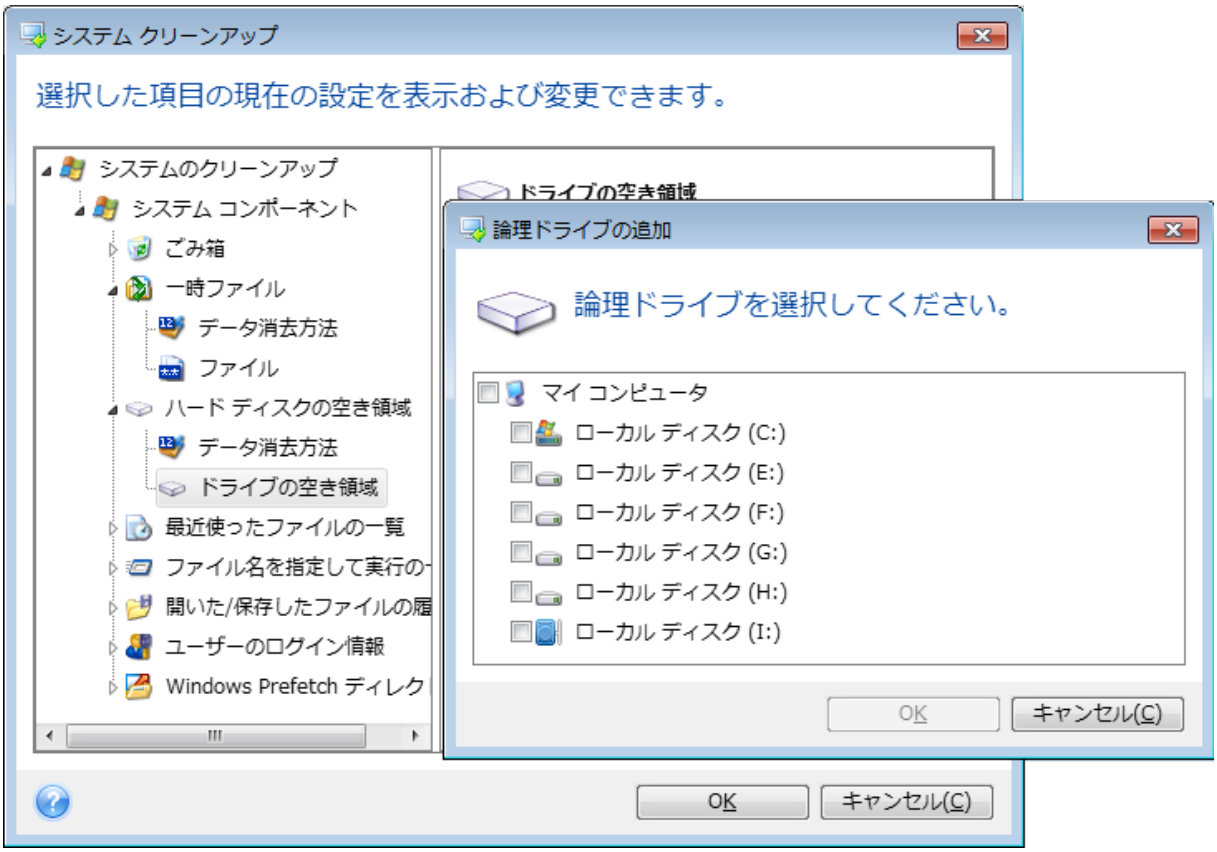
[ファイル] の設定値を入力した後で、検索文字列と一致するファイルの一覧を表示することができます。表示するには、**[ファイルの表示]** をクリックします。見つかったファイルの名前がウィンドウに表示されます。これらのファイルがクリーンアップの対象となります。

ドライブ空き領域

ここでは、空き領域をクリーンアップするドライブを手動で指定できます。デフォルトでは、使用可能なすべてのドライブの空き領域がシステムクリーンアップでクリーンアップされます。

このパラメータの設定を変更する場合は、**[削除]** ボタンを使用すると、空き領域をクリーンアップしないドライブを一覧から削除することができます。

そのドライブを再び一覧に追加するには、**[追加]** ボタンをクリックします。



コンピュータ

[コンピュータ] 設定は、ローカルネットワーク内のコンピュータの検索に使用したレジストリ検索文字列のクリーンアップに使用されます。この検索文字列に保持される情報は、ネットワーク内でユーザーが何を探していたかを表します。機密性を維持するには、このような項目も削除する必要があります。

[コンピュータ] 設定は、**[ファイル]** 設定と似ています。この文字列には、コンピュータ名の全体または一部をセミコロンで区切って入力します。指定できる数の制限はありません。コンピュータの検索文字列の削除は、Windowsの規則に従い、**[コンピュータ]** 設定値との比較に基づいて行われます。

ローカルネットワークコンピュータ検索文字列をすべて削除したい場合は、この設定をデフォルト値のままにしてください。デフォルト設定を復元する手順は、次のとおりです。

- **[検索したコンピュータの一覧]** コンポーネントを選択します。
- **[有効]** チェックボックスがオンになっていることを確認します。
- **[コンピュータ]** 設定を選択し、そのテキストボックスの内容が消去されていることを確認します。

こうすると、すべてのコンピュータ検索文字列がレジストリから削除されます。

[コンピュータ] の設定値を入力した後に、システムクリーンアップウィザードによってレジストリ内で検出された検索文字列を一覧表示することができます。表示するには、**[コンピュータの表示]** をクリックします。ネットワーク上で検索されたコンピュータ名（完全なコンピュータ名またはその一部）がウィンドウに表示されます。これらの項目が削除されます。

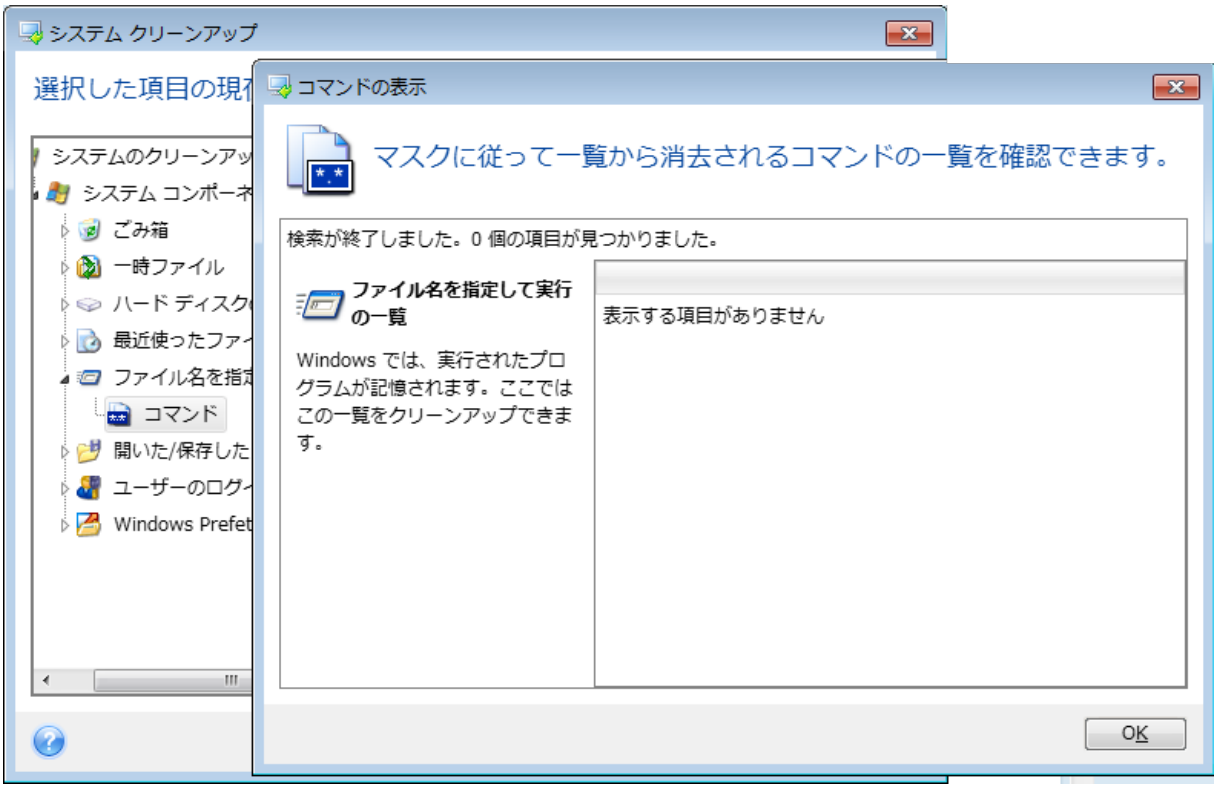
コマンドの設定

ここでは、**Windowsの実行一覧**のクリーンアップ時に削除するコマンドを選択できます。

このテンプレートには、任意のコマンド名を含めるか、次のようにコマンドの一部をセミコロンで区切って含めることができます。

help; cmd; reg

この手順により、名前に対応したコマンド、または入力した名前またはその一部を含むコマンドが削除されます。



ネットワークプレースのフィルタ

ここでは、過去に認証情報（ユーザー名およびパスワード）を入力して接続したネットワークプレース、サーバー、FTPサーバー、ネットワーク共有デバイスなどのホスト名またはIPアドレスを入力できます（セミコロンで区切って入力）。ホスト名やIPアドレスを入力するときは、* および？のワイルドカードを使用できます。

[ネットワークプレースを表示する] をクリックすると、削除しようとしている認証情報を使用して過去にアクセスしたネットワークプレースの一覧が表示されます。

プレビュー

スキャンが終了すると、その結果がウィザードウィンドウの上の部分に表示されます。デフォルトでは、クリーンアップ用にすべてのシステムコンポーネントがスキャンされます。どのコンポーネントを

スキャンし、どのコンポーネントをスキャン対象から除外するかをカスタマイズするには、クリーンアップのデフォルト設定を変更します。

検索結果を表示して、クリーンアップする項目の選択と残す項目の選択解除を手動で行うことができます。正しく選択できるように、どのコンポーネントにも簡単な説明が付いています。コンポーネントの名前をクリックすると、その説明がウィンドウの右側に表示されます。

コンポーネントを選択/選択解除する手順

- システムクリーンアップツリーの **[システムコンポーネント]** 項目を展開し、クリーンアップ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。コンポーネントをクリーンアップしない場合は、そのコンポーネントのチェックボックスをオフにします。
- 必要に応じて、コンポーネントを展開し、さらに下位の内容をオンまたはオフにすることもできます。

クリーンアップするコンポーネントを指定したら、**[クリーンアップ]** ボタンをクリックして先に進みます。

注意
Windows 7以降のオペレーティングシステムでは、ファイルやコンピュータの検索に関する情報は保存されません。また、開いた/保存したファイルの情報をレジストリに保存する方法も異なるため、ウィザードでのこの情報の表示方法も異なります。

クリーンアップの進行状況

処理のステータス ウィンドウでは、現在の処理の状態についての情報が表示されます。

進行状況バーは、選択した処理の完了レベルを示しています。

場合によっては、処理が完了するまでに時間がかかることがあります。このような場合に **[終了後コンピュータをシャットダウンする]** チェックボックスをオンにすると、処理が完了したときに Acronis Cyber Protect Home Office によってコンピューターがシャットダウンされます。

バックアップイメージのマウント

イメージを仮想ドライブとしてマウントすると、物理ドライブのようにファイルにアクセスできます。パーティションまたはディスクドライブ全体を含むローカルバックアップをマウントしてから、マウントするパーティションを選択することができます。マウント後:

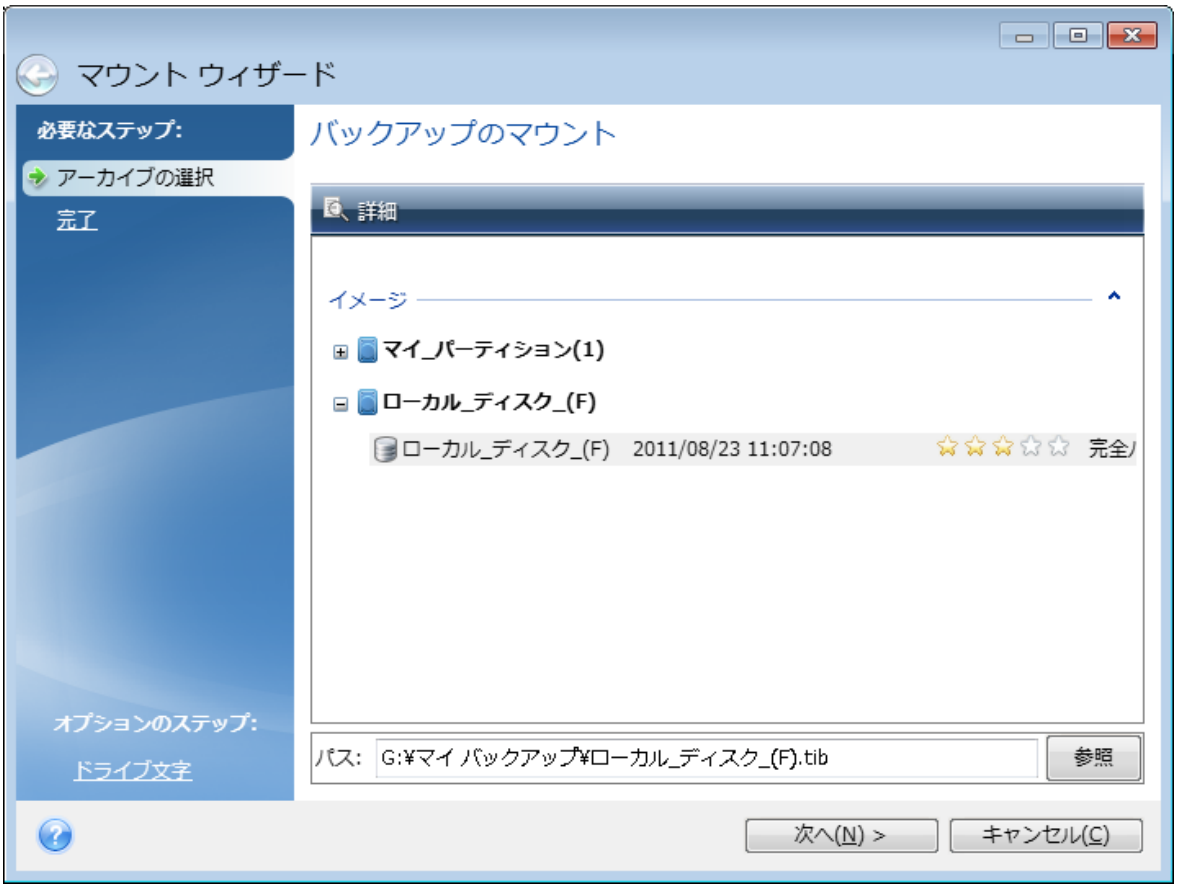
- マウントされたパーティションごとに、新しいディスクがシステムに表示されます。
- File Explorerやその他のファイルマネージャでイメージの内容を読み取り専用モードで確認できます。

注意
このセクションで説明した処理は、FAT および NTFS でファイル システムでのみサポートされます。

注意
ディスク バックアップが FTP サーバーに保存されている場合には、マウントできません。

イメージのマウント方法

1. File Explorer で、マウントするイメージファイルを右クリックし、**[マウント]** をクリックします。マウント ウィザードが開きます。
2. 作成日時に基づいてマウント対象のバックアップを選択します。これにより、特定時点のデータの状態を参照できます。



3. （オプションの手順）**[ドライブ文字]** で、仮想ディスクに割り当てる文字を **[マウント ドライブ文字]** ドロップダウン リストから選択します。パーティションをマウントしない場合は、ドロップダウン リストから **[マウントしない]** を選択するか、該当するパーティションのチェックボックスをオフにします。
4. **[実行]** をクリックします。
5. イメージが接続されると、File Explorerが起動し、仮想ディスクの内容が表示されます。

イメージのアンマウント

仮想ディスクの維持にはかなりのシステム リソースが消費されるため、必要な操作がすべて終了したら、仮想ディスクをマウント解除することをおすすめします。

イメージをマウント解除する手順は、次のとおりです。

1. File Explorerで、ディスクアイコンを右クリックして、**[マウント解除]** をクリックします。
2. コンピュータを再起動するかシャットダウンします。

.vhd（x）ファイルの使用方法

ディスクまたはパーティションの Acronis バックアップ（.tibx ファイル）は、仮想ハードディスク（.vhd（x）ファイル）に変換することができます。

.vhd（x）ファイルの使用方法

- 変換した .vhd（x）ファイルからコンピュータを起動して、バックアップが有効かどうか、また起動可能なオペレーティングシステムに復元できるかどうかをテストできます。
- 変換した .vhd（x）ファイルは、緊急時用に保管できます。たとえば、コンピュータが起動しないけれども、すぐに稼働する必要がある場合、.vhd（x）ファイルから起動できます。
- Windows 7 では、.vhd（x）ファイルを追加ドライブとしてマウントできます。.vhd（x）ファイルには、システムまたはシステム以外のどのようなパーティションでも含めることができます。
- 変換した .vhd（x）ファイルは、仮想コンピュータとして稼働することができます。

制限事項と追加情報

- ファイルのバックアップは、.vhd（x）ファイルに変換できません。
- 変換された .vhd（x）ファイルから起動するには、以下を含む必要があります。
  - 同じコンピュータのシステム パーティション。同じ .vhd（x）ファイルを使用して、他のコンピュータを起動することはできません。
  - Windows 7以降のオペレーティングシステム。
- 起動済みまたはマウント済みの .vhd（x）ファイルに加えた変更は .vhd（x）ファイルに保存されます。.vhd（x）ファイルから起動し、バックアップされなかったデータに変更を加えた場合、変更はライブシステムに影響を及ぼします。
- ブータブルメディアからの起動時に開始されるスタンドアロン版 Acronis Cyber Protect Home Office では、変換処理がサポートされていません。
- Acronis Cyber Protect Home Office は、元々複数のディスクドライブにあったダイナミックボリュームを含む .tibx ファイル（スパンまたはストライプダイナミックボリュームなど）を変換できません。

Acronis バックアップの変換

Windows 7 以降のバージョンの Enterprise エディションまたは Ultimate エディションを使用している場合は、システムパーティションの .tibx イメージを .vhd（x）形式に変換しておくと、変換後の .vhd（x）ファイルを使用してオペレーティングシステムを起動できるようになります。また、Acronis Cyber Protect Home Office を使用しなくてもイメージをマウントできるようになります。

Acronis のディスクイメージ（.tibx ファイル）を Windows バックアップ（.vhd（x）ファイル）に変換する手順は、次のとおりです。

1. Acronis Cyber Protect Home Office を開始します。
2. [**バックアップ**] セクションに移動します。

3. バックアップリストで、変換するバックアップの横にある下矢印アイコンをクリックし、**[VHDに変換]** をクリックします。
   バックアップがパスワードで保護されている場合は、Acronis Cyber Protect Home Office からパスワードの入力を求められます。作成された .vhd（x）ファイルはパスワードで保護されないことに注意してください。
4. 変換するバックアップのバージョンを選択します。
   増分バックアップを変換するには、それ以前のすべての増分バックアップと、元の完全バックアップが必要です。差分バックアップを変換するには、元の完全バックアップが必要です。変換の結果は必ず、完全バックアップになります。
5. 作成するファイルのパスを指定します。
   ファイルを作成する場所は、Acronis Cyber Protect Home Office によってサポートされるローカルストレージであればどれでもかまいません（Acronis Secure Zone と CD/DVD を除く）。さらに、SMB 共有に格納することもできます。
6. [オプションの手順] バックアップが変換されている間、**[完了後に仮想コンピュータを起動する]** チェックボックスをオンにすることができます。オンになっている場合、Acronis Cyber Protect Home Office はコンピューターを再起動し、作成された .vhd（x）ファイルを使用して Hyper-V 仮想マシンを実行します。

変換対象として選択した .tibx イメージに含まれるパーティションが、たとえば 2 つの物理ハードディスクドライブからのものである場合は、物理ドライブに合わせて 2 つの .vhd（x）ファイルが作成されます。

バックアップ設定のインポートとエクスポート

Acronis Cyber Protect Home Office を使用して、バックアップ設定をインポートおよびエクスポートすることができます。この機能は、新しいコンピューターに Acronis Cyber Protect Home Office をインストールした後に、設定を転送する必要がある場合に便利です。また、設定を保存することで、次のバージョンの Acronis Cyber Protect Home Office へのアップグレードも簡単に行えるようになります。

設定を転送することにより、新しいコンピュータでのバックアップの設定が大幅に簡単になります。設定をエクスポートして、それを別のコンピュータにインポートするだけです。設定は、スクリプト ファイルの形式でエクスポートされます。

設定の内容は、バックアップの種類に応じて異なります。「クラシック」ディスクのバックアップとファイルのバックアップの場合、設定は次の項目で構成されます。

- バックアップの項目一覧
- バックアップ オプション
- バックアップの保存先
- スケジュール
- バックアップ スキーム
- 自動クリーンアップのルール
- バックアップ バージョンの命名規則

ノンストップバックアップの設定は次のとおりです。

- ノンストッププロテクションの項目一覧
- Nonstop Backup データの保存場所（保存場所が複数存在する場合は、保存場所の一覧）

注意
あるコンピュータのオンラインバックアップ設定を別のコンピュータにインポートすることはできません。

バックアップの設定をエクスポートする手順は、次のとおりです。

1. Acronis Cyber Protect Home Office を開始します。
2. サイドバーで、**[設定]** > **[バックアップ設定の転送]** とクリックし、**[設定をファイルに保存する]** をクリックして、スクリプトファイルと設定の保存先を参照します。

バックアップの設定をインポートする手順は、次のとおりです。

1. 別のコンピューターで Acronis Cyber Protect Home Office を起動します。
2. サイドバーで、**[設定]** > **[バックアップ設定の転送]** とクリックし、**[ファイルから設定をインポートする]** をクリックして、スクリプトファイルのパスと設定を表示します。

設定をインポートした後に、新しい環境に合わせて一部の設定を変更しなければならないことがあります。たとえば、バックアップの項目一覧やバックアップの保存先などを変更しなければならないなどです。

別のコンピュータにバックアップをコピーする場合は、それらのバックアップの設定もエクスポートすることをお勧めします。これにより、コピーしたバックアップの機能を維持することができます。

Acronis Universal Restore

Acronis Universal Restore を使用すると、異なるハードウェア上にブータブルシステムのクローンを作成することができます。元のバックアップを作成したシステムとは異なるプロセッサ、マザーボード、または大容量記憶装置を搭載したコンピュータにシステムディスクをリカバリする場合は、このユーティリティを使用します。たとえば、壊れたマザーボードを交換した後や、システムをあるコンピュータから別のコンピュータに移行するときなどに役に立ちます。

どのような問題が解決されますか？

システムディスクイメージを、それが作成されたハードウェアまたは同一構成のハードウェアに、簡単に復元できます。ただし、異なる構成のハードウェアで実行した場合、復元されたシステムは起動しません。これは、新しいハードウェアが、イメージに含まれている重要なドライバと互換性がないからです。このユーティリティは、オペレーティングシステムの起動にとって重要なデバイス（ストレージコントローラ、マザーボード、チップセットなど）のドライバを検索してインストールします。

使用方法

別のハードウェアへの復元を開始する前に、以下があることを確認します。

- システムディスクのバックアップ または コンピュータ全体のバックアップ
- Acronis ブータブルメディア

- Acronis Universal ブートメディア

注意
Acronis Cyber Protect Home Office と Acronis Universal ブートメディアビルダーがコンピューターにインストールされている場合は、Acronis Cyber Protect Home Office と Acronis Universal ブートの両方を同じメディアに配置できます。詳細については、「Acronis Universal ブートメディアの作成」を参照してください。

システムを別のハードウェアに復元するには、次の手順を実行します。

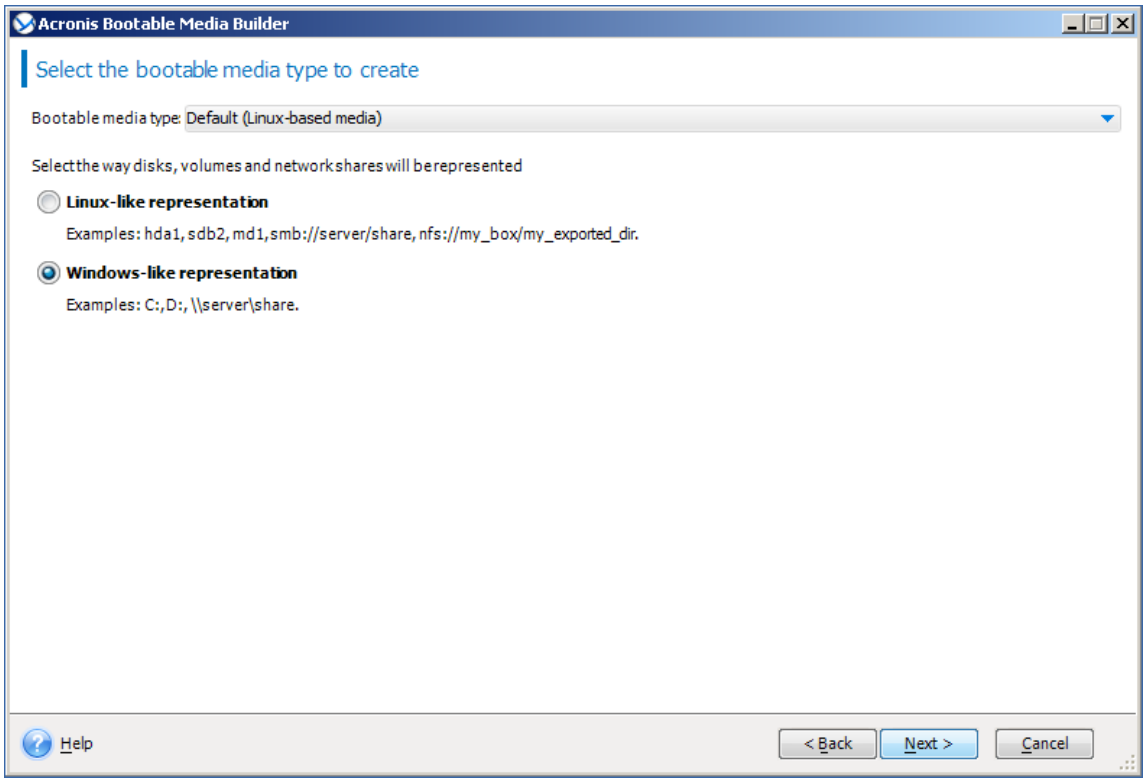
1. Acronis ブータブルメディア を使用してターゲットコンピューターを起動し、システムバックアップまたはコンピュータ全体のバックアップからシステムを復元します。詳細については、「ブータブルメディア配下の新しいディスクへのシステムの復元」を参照してください。
2. Acronis Universal ブートメディアを使用してターゲットコンピューターを起動し、画面の指示に従ってシステムをブータブルにします。詳細については、「Acronis Universal Restore の使用」を参照してください。

Acronis Universal ブートメディアの作成

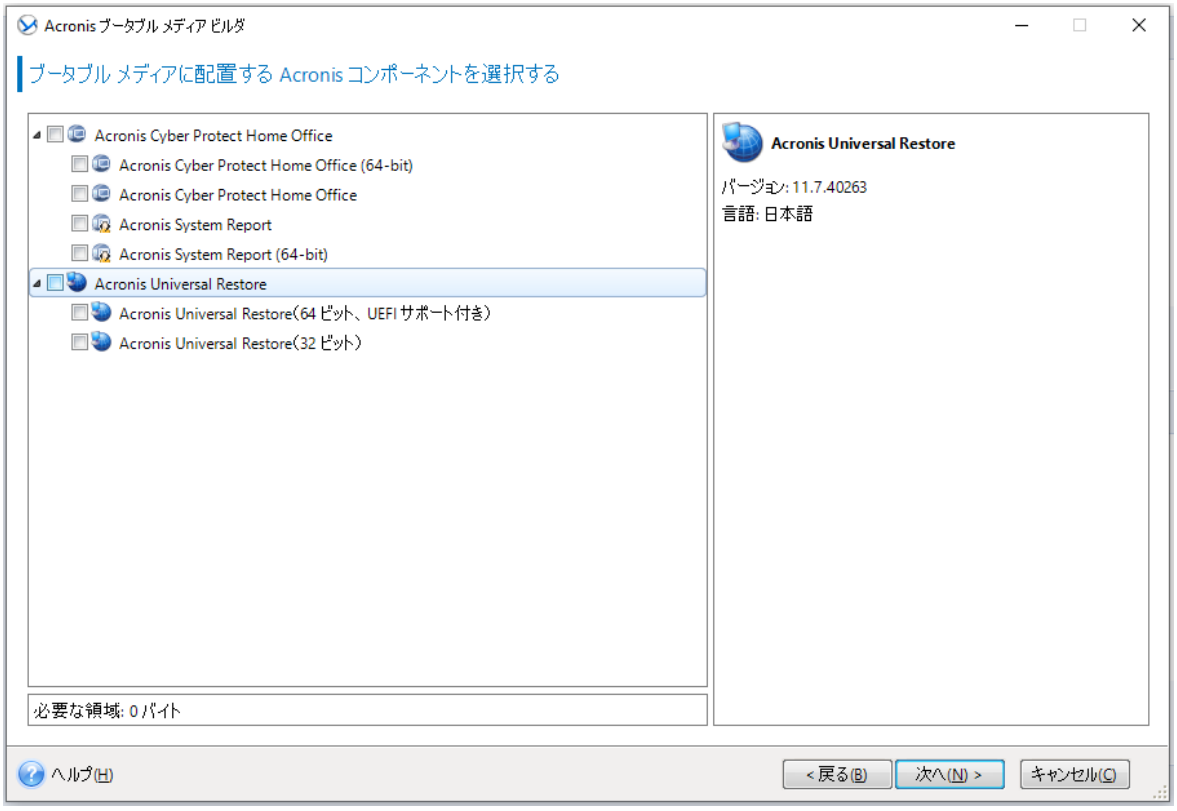
Acronis Universal ブートメディアは、コンピューターを異なるハードウェアにリカバリして起動できるようにするために使用します。詳細については、「Acronis Universal Restore」を参照してください。

Acronis Universal ブートメディアを作成する手順は、次のとおりです。

1. Acronis Cyber Protect Home Office を開始します。
2. **[ツール]** セクションで、**[Acronis Universal Restore]** をクリックします。
3. **[ダウンロード]** をクリックして、Acronis Universal ブートメディアビルダーをダウンロードします。
4. ダウンロードしたファイルを実行して、メディアビルダをインストールします。
5. USB フラッシュドライブを接続します。またはブータブルにする空の DVD を挿入します。
6. Acronis Universal ブートメディアビルダーを起動するには、次の手順のいずれかを実行します。
   - **[ツール]** セクションで、**[Acronis Universal Restore]** をクリックします。
   - **[スタート]** ボタンをクリックして、インストール済みプログラムのリストを表示し、**[Universal ブートメディアビルダの実行]** をクリックします。
7. 次を確認します。
   - ブータブルメディアの種類として Linux ベースメディアが選択されている。
   - ディスクおよびボリュームの表記方法として Windows 形式による表記が選択されている。



8. （オプション）Linux カーネルパラメータを指定します。詳細については、「ブータブルメディアの起動パラメータ」を参照してください。
9. メディア上に配置する Acronis コンポーネントを選択します。



32 ビットまたは 64 ビットのコンポーネントを選択できます。32 ビットコンポーネントは、64 ビットハードウェアで動作します。ただし、統合拡張ファームウェアインターフェイス（UEFI）が使用されている 64 ビットのコンピュータを起動するには、64 ビットコンポーネントが必要となります。

異なる種類のハードウェア上でメディアを使用するには、両方の種類のコンポーネントを選択します。作成されたメディアからコンピュータを起動するときに、ブートメニューで 32 ビットまたは 64 ビットのコンポーネントを選択することができます。

コンピューターに Acronis Cyber Protect Home Office がインストールされている場合は、それをメディアにコピーすることもできます。この場合、別のハードウェアへのリカバリに必要な、両方のコンポーネントを含む単一のブータブルメディアが作成できます。

10. メディアの作成先を選択します。
    - **CD**
    - **DVD**
    - **USB フラッシュ ドライブ**
    - **ISO イメージ ファイル**

      .iso ファイルの名前とターゲット フォルダを指定してください。

      .iso ファイルが作成されたら、CD または DVD に書き込むことができます。たとえば、Windows 7 以降では、内蔵の書き込みツールでこの操作を実行できます。File Explorerで、作成したISOイメージファイルをダブルクリックし、**[書き込み]** をクリックします。
11. Acronis Universal ブートで使用される大容量記憶装置ドライバを指定します。

    この時点ではドライバを追加する必要はありません。後で Acronis Universal ブートをコンピューターに適用するときに追加することができます。
12. **[実行]** をクリックします。

    メディアが作成されたら、コンピュータから取り外します。以上の手順で Acronis Universal ブートメディアを作成できます。

Acronis Universal Restore の使用

準備

ドライバの準備

Universal RestoreをWindowsオペレーティングシステムに適用する前に、新しいHDDコントローラとチップセット用のドライバを用意します。これらのドライバは、オペレーティングシステムの起動に不可欠です。ハードウェアベンダから提供されているCDまたはDVDを使用するか、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する場合、サードパーティ製のアプリケーションを使用してドライバを展開します。

ブータブル環境におけるドライバへのアクセスを確認

ブータブルメディアを使用する場合は、ドライバが保存されているデバイスにアクセスする権限を持っていることを確認します。デバイスがWindowsで使用可能であってもLinuxベースのメディアによって検出されない場合は、WinPEベースのメディアを使用してください。

Universal Restoreの設定

自動ドライバ検索

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検索する場所を指定します。

- ドライバがベンダのディスクまたはその他のリムーバブル メディアにある場合は、**[リムーバブル メディアの検索]** をオンにします。
- ドライバがネットワーク上のフォルダまたはブータブル メディアにある場合は、**[フォルダの追加]** をクリックして、フォルダのパスを指定します。

また、Universal RestoreではWindowsのデフォルトのドライバストレージフォルダ（通常はWINDOWS/inf）が自動的に検索されます。

インストールする大容量記憶装置ドライバ

次の場合、この設定が必要になります。

- ハードウェアに、RAID（特にNVIDIA RAID）やファイバチャネルアダプタなどの、固有の大容量記憶装置コントローラが存在する場合
- 自動ドライバ検索で、システムを起動できない場合

[ドライバの追加] をクリックして、適切なドライバを指定します。プログラムによってさらに適切なドライバが検出された場合でも、その警告が表示され、指定したドライバがインストールされます。

Universal Restoreのプロセス

必要な設定を行った後で、**[OK]** をクリックします。

プロセスの完了後、ネットワーク接続を設定し、ビデオアダプタ、USBなどのデバイスのドライバを指定できます。

トラブルシューティング

特に頻繁に発生する問題の解決

Acronis Cyber Protect Home Office で特に頻繁に発生する問題のリストをここに示します。該当する解決策については Acronis ナレッジベースを参照してください。

プログラム起動時のサインインに失敗する

エラー「このプロダクトキーの有効化限度数を超えました」

エラー「プロダクトキーが別のアカウントに登録されています」

ファイルエクスプローラーで参照するとき、ファイルとフォルダが表示されない

エラー「外付けドライブを接続してください」

Acronis Cloud へのバックアップで「書き込みエラー」、「ファイルの書き込み中にエラーが発生しました」、または「FES 要求が失敗しました」というエラーが発生して失敗する

新しいハードウェアへの復元後に、ドライバが見つからないことが原因でブルースクリーン（BSOD）エラー「Stop 0x0000007B」が発生する

一般的な解決策の一覧は、https://kb.acronis.com/true-image-known-solutions を参照してください。

復元の失敗に関するトラブルシューティング情報については、https://kb.acronis.com/content/46340 も参照してください。

Acronis System Report

Acronis サポートセンターへのお問い合わせの際には、通常、問題を解決するためにご使用のシステムに関する情報が必要になります。この情報を取得する処理は、簡単に実行できない場合や時間がかかる場合があります。

[システムレポートの生成] ツールを使うと、必要なすべての技術情報を含むシステムレポートが作成されます。この情報をファイルに保存し、必要に応じて、作成済みのファイルを問題報告に添付してサポートセンターに送信することができます。このようにツールを使えば、問題解決の手順を簡素化し、解決に要する時間を短縮することができます。

システムレポートを生成するには、以下のいずれかを実行します。

- サイドバーの **[ヘルプ]** をクリックして、**[システムレポートを生成する]** をクリックします。
- **Ctrl+F7** キーを押します。このキーの組み合わせは、Acronis Cyber Protect Home Office が他の処理を実行中であっても使用できます。
- Windows 11 を使用する場合、**[すべてのアプリ]** > **[Acronis]** > **[Acronis System Report]** をクリックします。
- Windows 10 を使用する場合、**[スタート]** メニューで、**[Acronis]** > **[Acronis System Report]** をクリックします。

- Windows 7 または 8 を使用する場合、**[スタート]** > **[すべてのプログラム]** > **[Acronis]** > **[Acronis System Report]** をクリックします。

レポート生成後に、次の操作を行います。

- 生成されたシステムレポートを保存するには、**[保存]** をクリックし、表示されたウィンドウで、作成されるファイルの保存場所を指定します。
- レポートを保存せずにメイン プログラム ウィンドウを終了するには、**[キャンセル]** をクリックします。

コンピュータが起動しないときにシステムレポートを生成するための個別のコンポーネントとして、このツールをブータブルメディアに含めることができます。メディアから起動した後、Acronis Cyber Protect Home Office を実行せずにレポートを生成できます。USB フラッシュドライブを接続し、**[Acronis System Report]** アイコンをクリックします。生成されたレポートはUSBフラッシュドライブに保存されます。

Acronis System Reportツールをブータブルメディアに含める手順は、次のとおりです。

1. **Acronis メディアビルダー** ウィザードの **[レスキューメディアに追加するコンポーネントの選択]** ページで、**[Acronis System Report]** チェックボックスをオンにします。
2. 続行するには、**[次へ]** をクリックしてください。

コマンド プロンプトからのシステム レポートの作成

1. 管理者として Windows コマンドプロセッサ（cmd.exe）を実行します。
2. 現在のディレクトリを Acronis Cyber Protect Home Office インストールフォルダに変更します。そのためには次のコマンドを入力します。

   ```
   cd C:\Program Files (x86)\Acronis\CyberProtectHomeOffice
   ```

3. システム レポート ファイルを作成するには、次のコマンドを入力します。

   ```
   SystemReport
   ```

   SystemReport.zip というファイルが現在のフォルダに作成されます。
   レポート ファイルに別の名前を付けるには、次の <file name> の代わりに新しい名前を入力します。

   ```
   SystemReport.exe /filename:<file name>
   ```

ブータブルメディアからシステムレポートを生成するには、次の手順を実行します。

1. Acronis ブータブルメディア がない場合は、作成します。詳細については、「Acronis メディアビルダー」を参照してください。
2. ブータブルメディア デバイス（CD、DVD、または USB ドライブ）が最初の起動デバイスになるように、BIOS で起動順を並べ替えます。詳細については、「BIOS での起動順の並べ替え」を参照してください。
3. Acronis ブータブルメディア から起動して、**[Acronis Cyber Protect Home Office]** を選択します。

注意
[Acronis Cyber Protect Home Office] をクリックする代わりに、USB フラッシュドライブを接続し、**[Acronis System Report]** をクリックすることもできます。この場合、レポートが生成されて、フラッシュドライブに自動的に保存されます。

4. [ヘルプ] アイコン（  ）の横にある矢印をクリックして、**[システムレポートの生成]** を選択します。
5. レポート生成後は、**[保存]** をクリックし、表示されたウィンドウで、作成されたファイルを保存するロケーションを指定します。
   レポートはZIPファイルにアーカイブされます。

Acronis Smart Error Reporting

プログラム処理でのエラーにより問題が発生すると、Acronis Cyber Protect Home Office では、対応するエラーメッセージが表示されます。エラーメッセージには、イベントコードと、エラーの簡単な説明が含まれています。

インターネットに接続できる場合

エラーを修正するための解決策が掲載されている Acronis ナレッジベースの記事を表示するには、**[ナレッジベース]** ボタンをクリックします。

確認ウィンドウが開きます。このウィンドウには、インターネットを介して Acronis ナレッジベースに送信される情報が一覧表示されます。**[OK]** をクリックして、情報の送信を許可します。

以降は確認なしで情報を送信したい場合、**[常に確認なしで送信する]** チェックボックスをオンにします。

インターネットに接続できない場合

1. エラーメッセージウィンドウで、**[詳細]** をクリックし、イベントコードを書き留めてください。
   コードは次のようになります。
   0x000101F6 - 通常のイベントコードの例です。
   0x00970007+0x00970016+0x00970002 - 複合的なイベントコードの例です。この種のコードは、下位レベルのプログラムモジュールで発生したエラーが上位レベルのモジュールに影響した場合に表示されることがあります。
2. インターネットに接続している場合や、インターネット接続を利用できる別のコンピュータを利用できる場合は、https://kb.acronis.com/errorcode/ でイベントコードを入力してください。

入力したイベントコードがナレッジベースで認識されない場合は、ナレッジベースには、その問題の解決策を含む記事が掲載されていません。そのようなときは、アクロニス カスタマーサービスでトラブルチケットをオープンしてください。

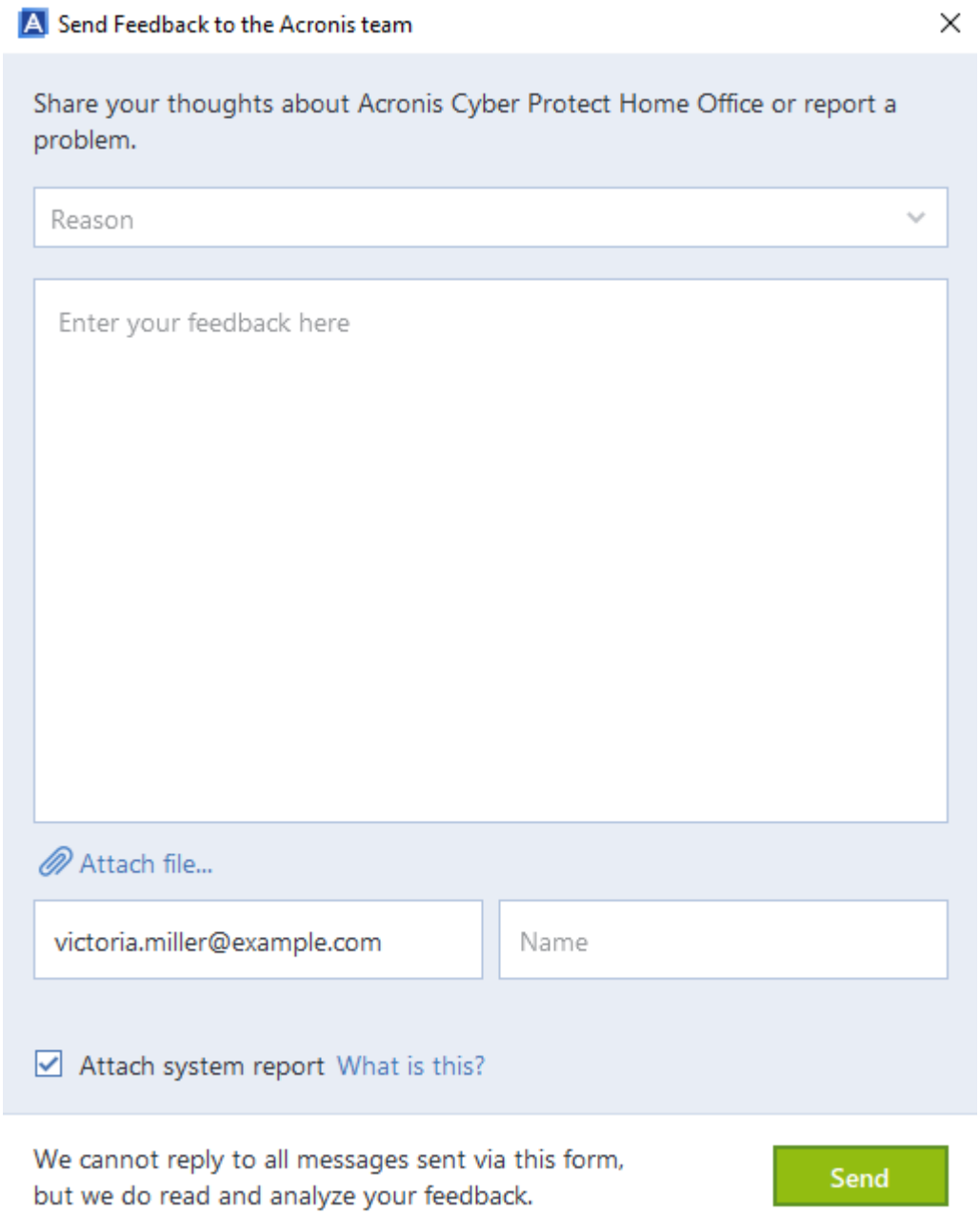
Acronis へのご意見の送信

Acronis では、製品やサービスの機能、信頼性、速度のさらなる向上を重ね、継続的な改善を実施しています。フィードバックフォームから、解決すべき不便な点や問題点をお寄せいただくことができます。いただいたご意見をもとに Acronis Cyber Protect Home Office を改善いたします。お手数ではございますが、製品へのご意見、新機能のご要望、問題のご報告などをぜひお知らせください。ご意見や問題の内容については必ず確認し、分析いたします。

注意
すべてのフィードバックメッセージへの返信は致しかねます。Acronis Cyber Protect Home Office に関して援助が必要な場合は、サポートセンターにお問い合わせください。

Acronis にご意見を送信するには、次の操作を実行します。

1. サイドバーの [**ヘルプ**] をクリックして、[**フィードバックの送信**] をクリックします。フィードバック フォームが開きます。



2. リストからご意見の内容を選択します。
3. 本文を入力します。
4. 名前と電子メール アドレスを入力します。
5. （オプションの手順）ファイルや Acronis システムレポートを添付することもできます。詳細については、「Acronis System Report」を参照してください。
   Acronis Cyber Protect Home Office で応答が停止した場合など、重大なエラーが発生した場合は、システムレポートを添付することをお勧めいたします。
6. **[送信]** をクリックします。

クラッシュダンプの収集方法

Acronis Cyber Protect Home Office または Windows の異常終了はさまざまな理由で発生する可能性があるので、異常終了のそれぞれの状況を個別に調べる必要があります。Acronis カスタマーサービスに次のような情報を提供すると役に立つことがあります。

Acronis Cyber Protect Home Office が異常終了した場合は、次の情報を提供してください。

1. 問題が発生する前に実行した手順の正確な順序の説明。
2. クラッシュダンプ。このようなダンプの収集方法については、Acronis サポートナレッジベース（KB）の記事（https://kb.acronis.com/content/27931）を参照してください。

Acronis Cyber Protect Home Office が原因で Windows が異常終了した場合は、次の情報を提供してください。

1. 問題が発生する前に実行した手順の正確な順序の説明。
2. Windowsのダンプファイル。このようなダンプの収集方法については、Acronis サポート KB の記事（https://kb.acronis.com/content/17639）を参照してください。

Acronis Cyber Protect Home Office が異常停止した場合は、次の情報を提供してください。

1. 問題が発生する前に実行した手順の正確な順序の説明。
2. プロセスのユーザーダンプ。Acronis サポート KB の記事（https://kb.acronis.com/content/6265）を参照してください。
3. Process Monitorのログ。Acronis サポート KB の記事（https://kb.acronis.com/content/2295）を参照してください。

この情報にアクセスできない場合は、ファイルをアップロードするための FTP リンクについて Acronis カスタマーサービスに問い合わせてください。

これらの情報は解決策を見つけるための時間の短縮に役立ちます。

Acronis カスタマ エクスペリエンス プログラム

Acronis カスタマ エクスペリエンス プログラム（CEP）は、Acronis のお客様が、Acronis 製品の機能、設計、および開発に貢献できる新しい手段です。このプログラムにより、お客様は、ホスト コンピュータや仮想マシンのハードウェア構成、使用頻度が最も多い（および少ない）機能、発生する問題の性質に関する情報など、さまざまな情報を提供できます。この情報を利用することで、Acronis 製品およびお客様が最もよく使用する機能を改善できます。

Acronis カスタマ エクスペリエンス プログラムに参加する、または参加をやめるには、次のようにします。

1. サイドバーで、**[設定]** をクリックしてください。
2. プログラムへの参加をやめるには、**[Acronis カスタマ エクスペリエンス プログラムに参加する]** のチェックボックスをオフにします。

このプログラムへの参加を選択された場合、技術的な情報が 90 日ごとに自動的に収集されます。氏名、住所、電話番号、キーボード入力などの個人データは収集されません。CEP への参加は任意です。ソフトウェアの改善と機能拡張を提供し、お客様のニーズをさらに満たしていくことを最終的な目的としています。

用語集

A

Acronis Active Protection

ランサムウェア（一部のファイルまたはシステム全体へのアクセスをブロックし、ブロック解除と引き換えに身代金を要求する悪意のあるソフトウェア）からデータを保護するテクノロジです。このテクノロジは、ヒューリスティックな方法に基づき、リアルタイムモードでコンピュータ上のプロセスを監視し、コンピュータ上のデータを暗号化しようとする試みをユーザーに通知します。ファイルが暗号化された場合でも、一時コピーまたはバックアップから復元できます。

Acronis Secure Zone

セキュリティで保護されている、ハードディスク上のバックアップ保存用のパーティションです。利点: 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。 制限事項: 1) Acronis Secure Zone はダイナミックディスクに作成できません。 2) ブータブルメディアから、Startup Recovery Manager または BartPE を使用して開始する場合、リカバリ環境内で Acronis Secure Zone をバックアップのロケーションとして使用することはできません。

Acronis Startup Recovery Manager

起動時に F11 キーを押すことでスタンドアロン版を開始できるようにする保護ツールです。Startup Recovery Manager を使用すると、ブータブルメディアが不要となります。 Startup Recovery Manager は、モバイルユーザーには特に役に立ちます。障害や災害が発生した場合、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復元を実行します。 制限事項: ダイナミック ディスク上に作成することはできません。LILO や GRUB などのブート ローダーを手動で設定する必要があります。サードパーティ製のローダーを再アクティブ化する必要があります。

Acronis ドライブ

ローカルアーカイブとクラウドアーカイブの両方を含む仮想ドライブです。このドライブは、File Explorer の [お気に入り] からアクセスでき、読み取り専用モードでアーカイブされたファイルにアクセスできます。

Acronis 認証

公証済ファイルがバックアップ後に変更されたかどうかをユーザーが確認できるテクノロジです。この認証では、公証対象として選択されたファイルのハッシュコードに基づきハッシュコードが計算され、ブロックチェーンベースのデータベースに送信されます。ブロックチェーン技術により、ハッシュコードが変更されないことが保証されます。したがって、確認するファイルのハッシュとデータベース内のハッシュを比較することで、ファイルの信頼性を簡単に確認できます。

S

Sync

データの同期と同じです。 同期オーナーのコンピュータで設定された同期設定。作成した同期は、該当する同期ボックスを使用して管理します。同期を作成しても、同期処理は開始されません。他のユーザーが、作成された同期に参加することができます。

あ

アーカイブ

アーカイブ操作により作成されるファイルです。このファイルには、ユーザーがアーカイブするよう選択した一連の圧縮ファイルが含まれています。アーカイブは、クラウドストレージ、または外付けのハードディスクドライブ、NAS といったローカルストレージに保存でき、仮想 Acronis ドライブ上で読み取り専用モードでアクセスできます。

アーカイブ処理

選択したファイルを圧縮し、クラウドストレージ、または外付けのハードディスクドライブ、NAS といったローカルストレージに移動する処理です。この処理の主な目的は、古いまたは大きなファイルを別のストレージに移動させることにより、ハードディスクドライブの空き領域を解放することです。圧縮後、ファイルは元の場所から削除され、仮想 Acronis ドライブ上で読み取り専用モードでアクセスできます。

お

オンラインバックアップ

オンラインバックアップ: Acronis Online Backup を使用して作成されるバックアップです。オンラインバックアップはクラウドと呼ばれる特別なストレージに保存され、インターネット経由でアクセスできます。オンラインバックアップの主な利点は、すべてのバックアップがリモートのロケーションに保存されることです。これにより、ユーザーのローカルなストレージに依存せず、すべてのバックアップデータの安全が保証されます。

て

ディスクバックアップ（イメージ）

ディスクまたはパーティション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です。通常はデータを含むセクタのみがコピーされますが、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も用意されています。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。

データの同期

データの同期は、2つ以上の同期したフォルダでデータが同一になるように保持する処理です。それらのフォルダは、同じコンピュータ上にある場合も、ローカルネットワークやインターネットで接続された別のコンピュータ上にある場合もあります。同期している一方のフォルダでファイルやサブフォルダを作成、コピー、修正、または削除すると、もう一方の同期フォルダでも同じアクションが自動的に実行されます。逆の方向でも同じルールが適用され、他の同期フォルダで何らかの変更があった場合、同期元のフォルダでも同じ変更が適用されます。

の

ノンストップバックアップ

ノンストップバックアップとは実際には、Acronis Nonstop Backup機能を使用して作成されたディスク/パーティションまたはファイルのバックアップです。これは、1 つの完全バックアップバージョンと、短い間隔で作成された一連の増分バックアップバージョンのセットです。ほぼ連続したデータの保護を実現し、必要に応じて任意の復元ポイントにおける以前のデータの状態に復元できます。

ノンストッププロテクション

ノンストッププロテクション: 有効にすると Nonstop Backupが実行される処理です。

は

バックアップ

バックアップ操作と同じです。 バックアップ設定を使用して作成、管理するバックアップバージョンのセットです。バックアップには、完全バックアップと増分バックアップの両方の方法で作成された複数のバックアップバージョンが含まれる場合があります。同じバックアップに属するバックアップバージョンは、通常同じ場所に保存されます。

バックアップ バージョン

単一のバックアップ操作の結果。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単独または一連のファイルです。Acronis Cyber Protect Home Office によって作成されるバックアップバージョンファイルの拡張子は .tibx です。バックアップバージョンの統合による TIBX ファイルもバックアップバージョンと呼ばれます。

バックアップ バージョン チェーン

最初の完全バックアップバージョンと、後続の 1 つまたは複数の増分または差分バックアップバージョンから構成される、最低 2 つのバックアップバージョンからなる一連のバックアップバージョンです。バックアップ バージョン チェーンは、次の完全バックアップ バージョン（存在する場合）まで続きます。

バックアップ設定

新しいバックアップの作成時にユーザーが設定するルールのセットです。このルールによって、バックアップ処理を制御します。後でバックアップ設定を編集し、バックアップ処理を変更または最適化することができます。

バックアップ操作

データを特定の日時の状態に戻すため、コンピュータのハードディスクに存在しているデータのコピーを作成する処理。

ふ

ブータブル メディア

Acronis Cyber Protect Home Office のスタンドアロン版を含む物理メディア（CD、DVD、USB ドライブ、またはコンピュータの BIOS によって起動デバイスとしてサポートされるその他のメディア）。 ブータブルメディアは次の操作に最もよく使用されます。起動できないオペレーティングシステムのリカバリ、破損したシステムで壊れずに残ったデータへのアクセスとバックアップ、ベアメタル上のオペレーティングシステムの配置、ベアメタル上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持つディスクのセクタ単位のバックアップ。

へ

ベリファイ

特定のバックアップバージョンからデータを復元できるかどうかを確認する処理です。完全バックアップバージョンの場合、完全バックアップバージョンのみがベリファイされます。差分バックアップバージョンの場合、最初の完全バックアップバージョンと選択された差分バックアップバージョンがベリファイされます。増分バックアップバージョンの場合、最初の完全バックアップバージョン、選択された増分バックアップバージョン、および選択された増分バックアップバージョンまでのバックアップバージョンのチェーン全体（ある場合）がベリファイされます。このチェーンに差分バックアップバージョンが1つでも含まれている場合、（最初の完全バックアップバージョンおよび選択した増分バックアップバージョンに加えて）チェーン内の最新の差分バックアッ

プバージョンのみがベリファイされ、その差分バックアップバージョンと選択した増分バックアップバージョンの間に作成された増分バックアップバージョンがあればそれらもすべてベリファイされます。

も

モバイルバックアップ

スマートフォン、タブレットなど、モバイルデバイスのファイルを含むバックアップ。

り

リカバリ

リカバリとは、壊れたデータをバックアップに保存されている以前の正常な状態に戻す処理のことです。

漢字

完全バックアップ

バックアップ対象として選択されたすべてのデータを保存するために使用されるバックアップ方法。 完全バックアップバージョンを作成するバックアップ処理。

完全バックアップバージョン

バックアップ対象として選択されたすべてのデータを含む、それ自体で完結するバックアップバージョン。完全バックアップバージョンからデータを復元する場合は、他のバックアップバージョンにアクセスする必要はありません。

疑わしいプロセス

Acronis Active Protection では、動作のヒューリスティックを使用し、プログラム（プロセス）によって実行されるアクションのチェーンを分析して、悪意のある動作パターンのデータベースにあるイベントのチェーンと比較します。プログラムがランサムウェアと類似した動作をし、ユーザーのファイルを変更しようとする場合、疑わしいプログラムと見なされます。

公証

ファイルの状態を「記憶」し、この状態を本物として定義する処理です。Acronis 認証では、公証対象として選択されたファイルのハッシュコードに基づきハッシュコードが計算され、このハッシュコードがブロックチェーンベースのデータベースに送信されます。

公証済ファイル

Acronis 認証により公証されたファイル。ファイルは、認証バックアップに追加された後に公証済となり、そのハッシュコードがブロックチェーンベースのデータベースに送信されます。

差分バックアップ

バックアップ内で直近の完全バックアップバージョンが作成されてから変更されたデータの保存に使用されるバックアップ方法。 差分バックアップバージョンを作成するバックアップ処理。

差分バックアップバージョン

差分バックアップバージョンには、前回の完全バックアップバージョンに対するデータの変更点が保存されます。差分バックアップバージョンからデータを復元するには、対応する完全バックアップバージョンにアクセスする必要があります。

増分バックアップ

バックアップ内で直近のバックアップバージョン（すべての種類）が作成されてから変更されたデータを保存するために使用されるバックアップ方法。 増分バックアップバージョンを作成するバックアップ処理。

増分バックアップバージョン

前回のバックアップバージョンに対するデータの変更点が保存されるバックアップバージョン。増分バックアップバージョンからデータを復元するには、同じバックアップから他のバックアップバージョンにアクセスする必要があります。

同期ファイルのバージョン

ファイルの変更のたびに、同期フォルダに作成される特定の状態のファイル。ファイルのバージョンは Acronis Cloud に保存できます。

認証バックアップ

Acronis 認証により公証されたファイルを含むバックアップ。

索引

ひ

ふ