

RDX にバックアップしたデータをランサムウェアから守るソリューション

BackupExec の『ランサムウェアレジリエンス』機能を利用して RDX にバックアップする方法のご案内

はじめに

本書は、Veritas Technologies 社のバックアップソフトウェア「BackupExec」のランサムウェアレジリエンス機能を利用して、RDX ドライブにバックアップしたデータをランサムウェアから保護する方法についてご紹介することを目的としています。

BackupExec は、中小規模企業向けのバックアップソフトとして国内外で最もよく知られるバックアップソフトウェアの一つで、物理環境・仮想環境・クラウドデータのバックアップ向けに 45,000 社以上の企業で利用されるソフトウェアです。

RDX は、OverlandTandberg 社がライセンスを持つディスクカートリッジデバイスで、テープとディスクの両方の長所を兼ね備えることで中小規模企業向けのバックアップデバイスのデファクトスタンダードとなっています。ドライブから取り外し可能な RDX データカートリッジと、PC・サーバに接続する RDX ドライブから成る製品です。

本書手順で使用した環境



初版：2023 年 5 月 25 日
タンベルグデータ株式会社

バックアップ対象に Windows Active Directory、Microsoft Exchange Server、Hyper-V などの特殊なデータが含まれていない場合（GRT 対応バックアップではない場合）

↓

バージョン 20.4 以降の BackupExec ではデフォルトでランサムウェアレジリエンス機能が有効になっているため、ランサムウェア対策に特別な手順は必要ありません。

以下の手順ではまず一般的な（上記の特殊なデータが含まれていない）システムの全体バックアップ（イメージバックアップ）を取得し、ランサムウェアから保護されていることを確認する手順まで記載しています。

その後、ExchangeServer や Hyper-V などがバックアップ対象に含まれる場合についての設定手順についてもご案内いたします。

ステップ 1. BackupExec 上で RDX をバックアップデバイスとして構成する

本例では、E:ドライブとして Windows から認識された RDX のボリューム（4TB カートリッジ）を BackupExec 上でストレージ設定します。



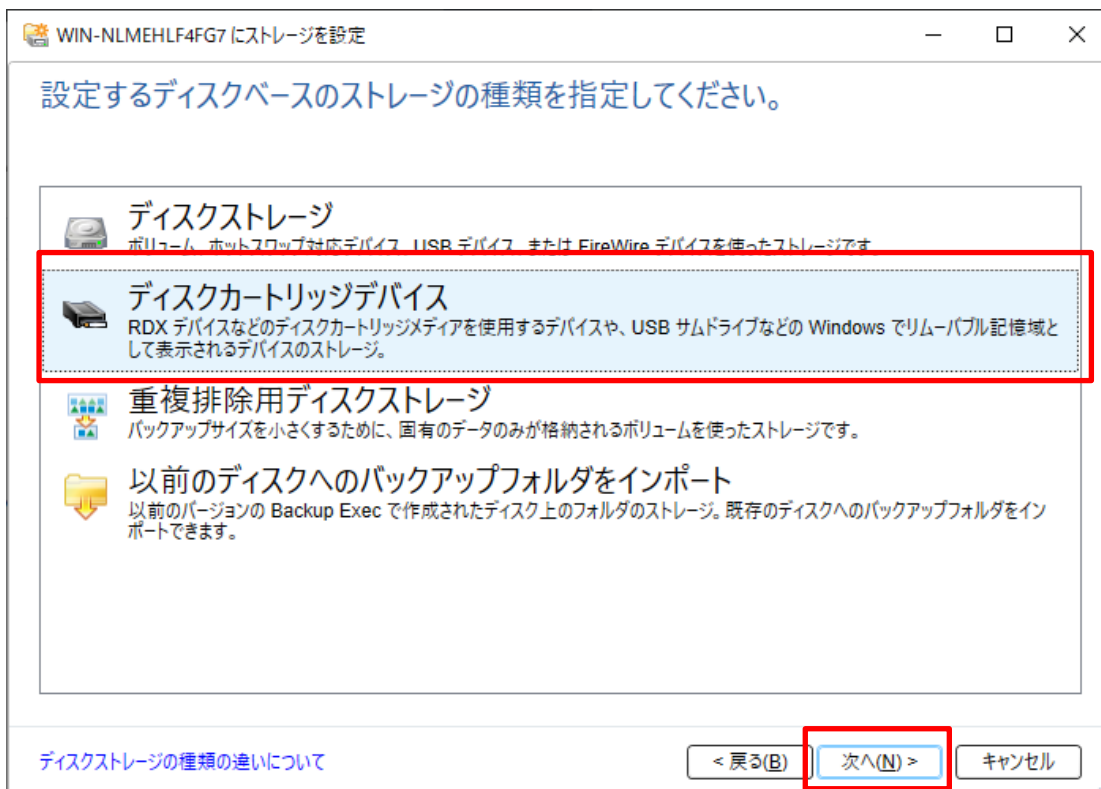
BackupExec を開き、「ストレージ」画面を開き、「ストレージを設定」ボタンを押します。



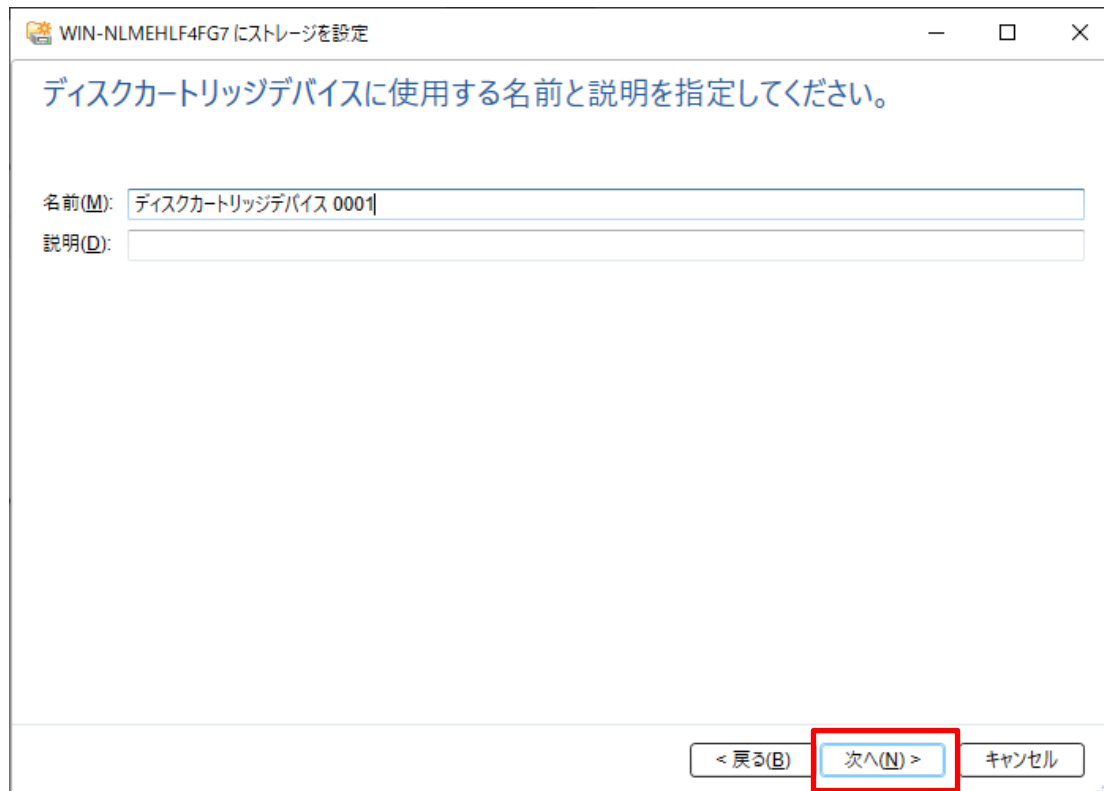
「ディスクベースのストレージ」を選び次に進みます。



「ディスクカートリッジデバイス」を選び次へ進みます。



BackupExec 上でのこのデバイスの名前を決めます。この例ではデフォルトのまま進みます。



WIN-NLMEHLF4FG7 にストレージを設定

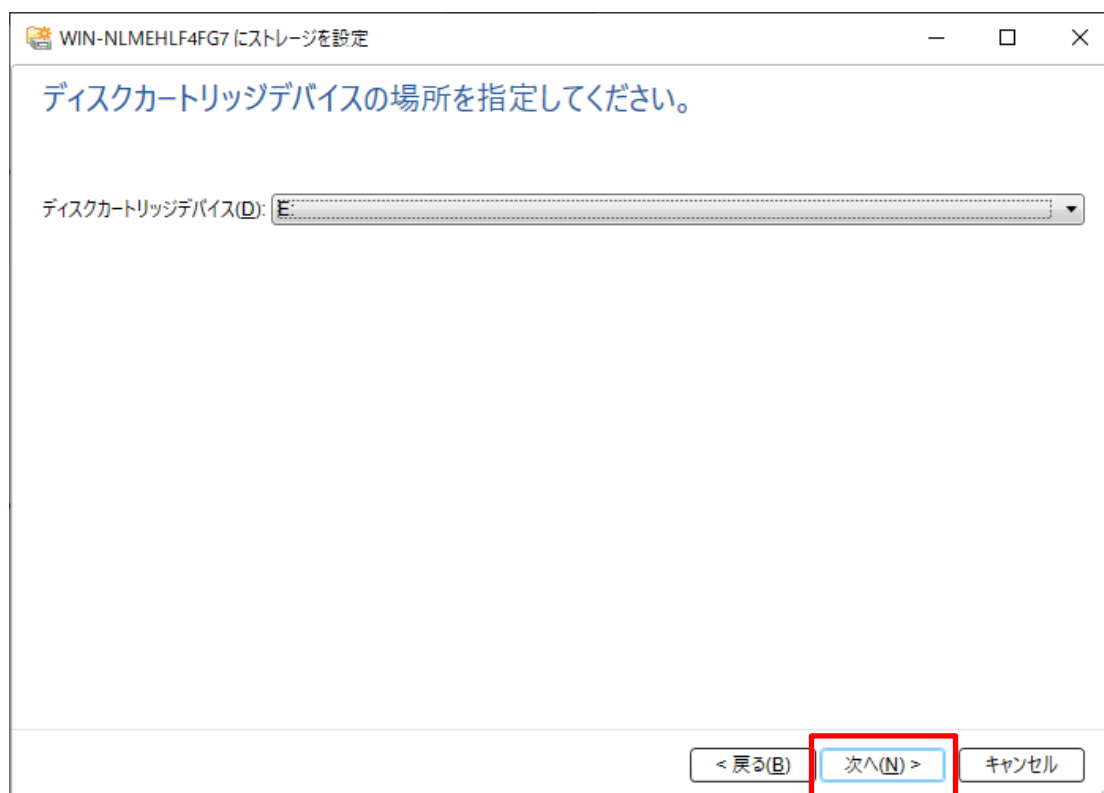
ディスクカートリッジデバイスに使用する名前と説明を指定してください。

名前(M): ディスクカートリッジデバイス 0001

説明(D):

< 戻る(B) 次へ(N) > キャンセル

ディスクカートリッジデバイスとして構成するディスクを選択する画面になりますので、RDX のボリューム（本例では E: ドライブ）を選択します。



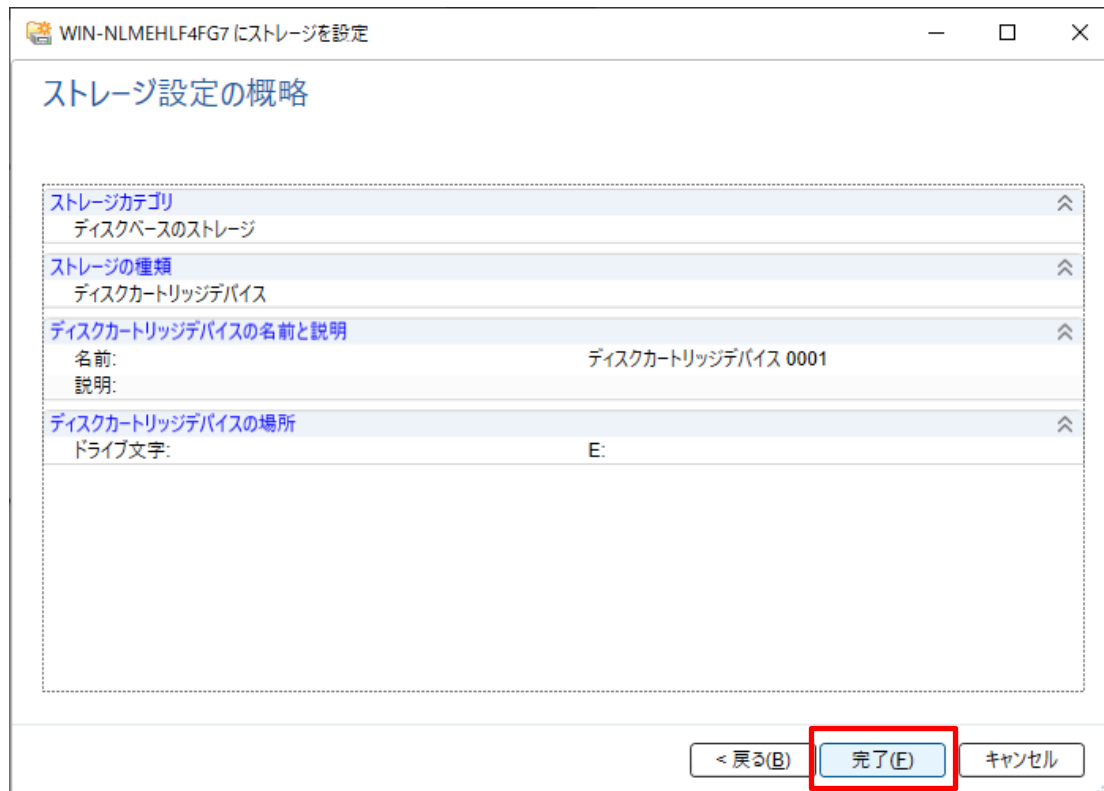
WIN-NLMEHLF4FG7 にストレージを設定

ディスクカートリッジデバイスの場所を指定してください。

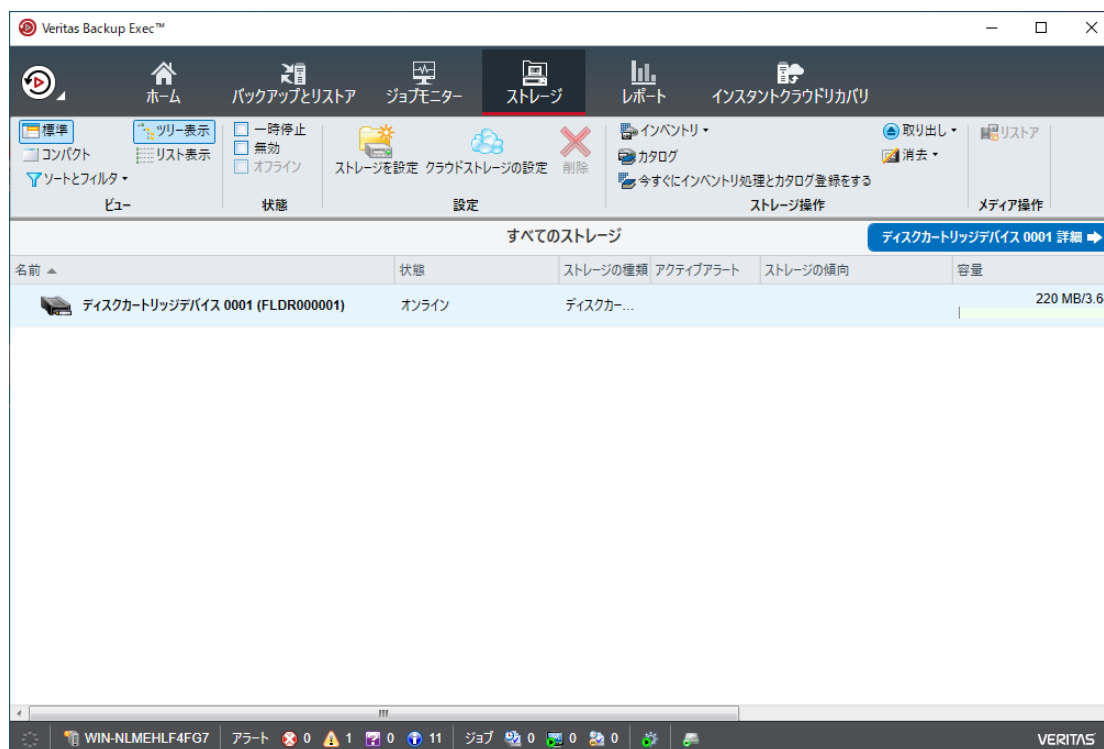
ディスクカートリッジデバイス(D): E:

< 戻る(B) 次へ(N) > キャンセル

設定内容を確認して、「完了」ボタンを押します。



「ストレージ」画面にディスクカートリッジデバイス 0001 が追加されていることを確認します。

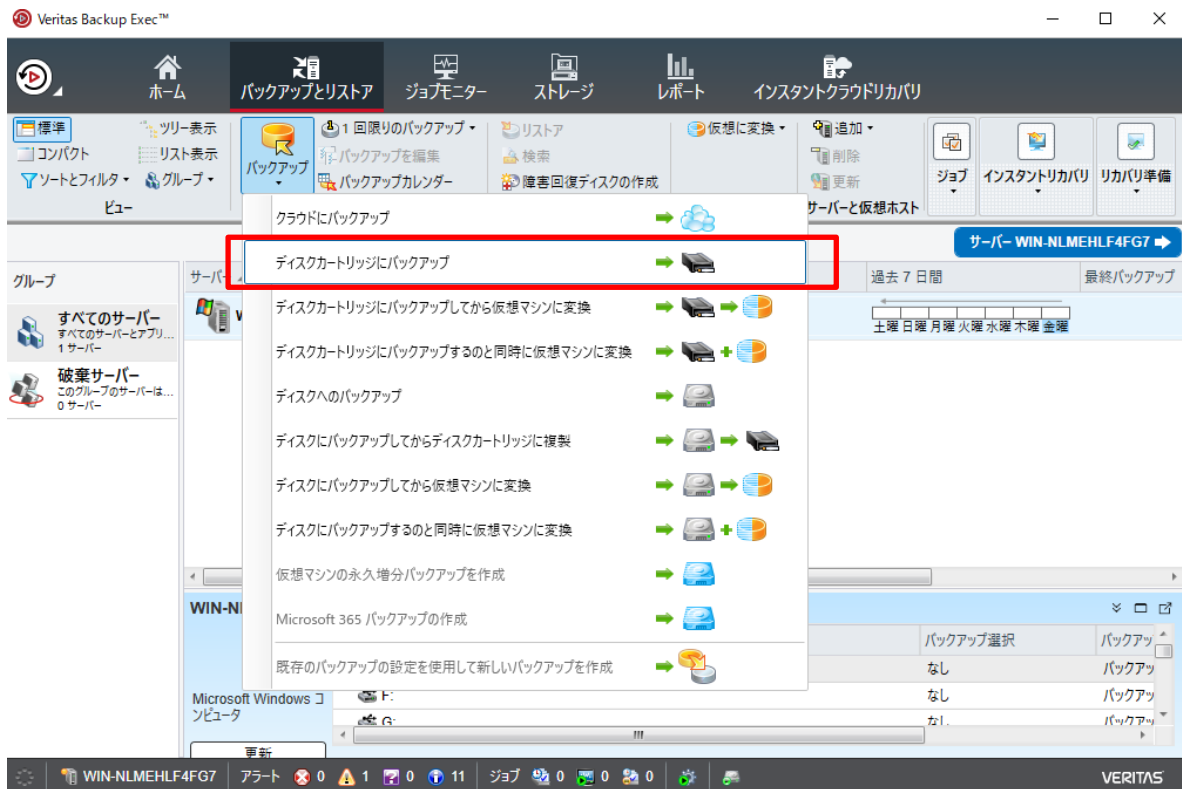


※ランサムウェアレジリエンス機能となる「ディスクストレージのロックダウンステータス」は最初から有効になっています。

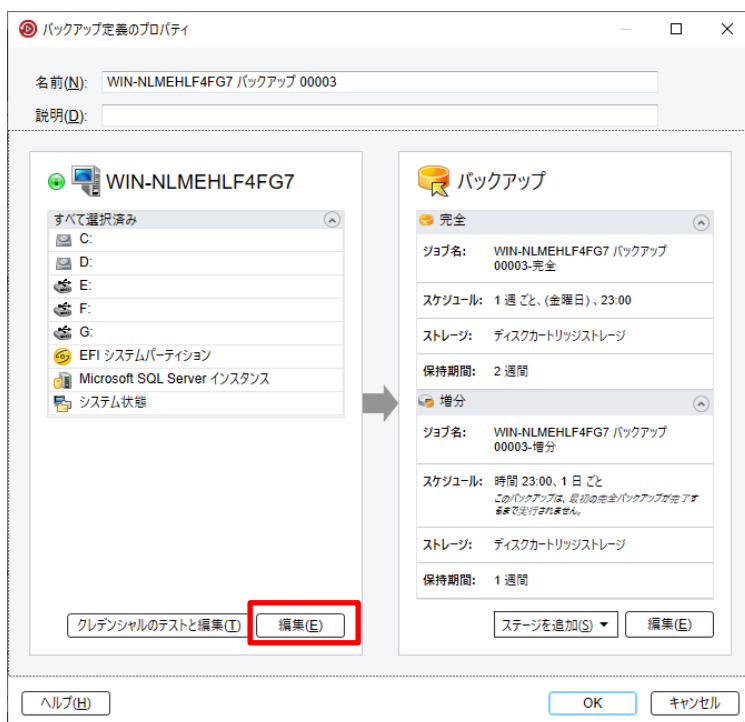


ステップ2. バックアップジョブを作成する

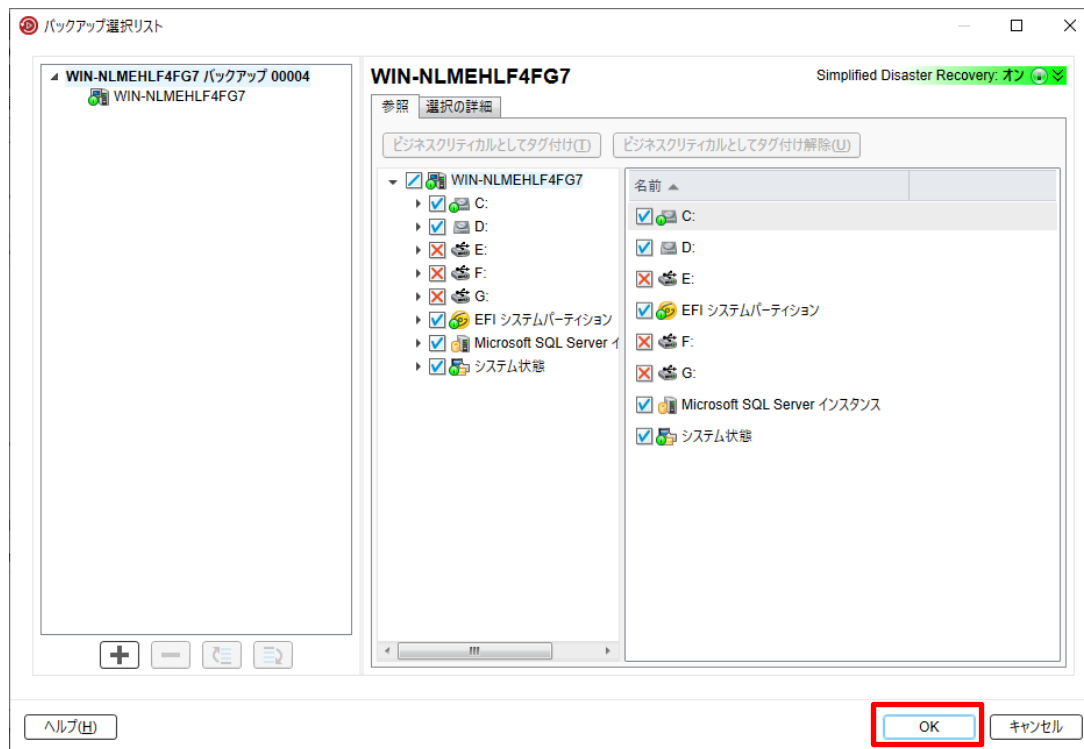
「バックアップとリストア」画面で「バックアップ」ボタンのメニューを出し、「ディスクカートリッジにバックアップ」を選択します。



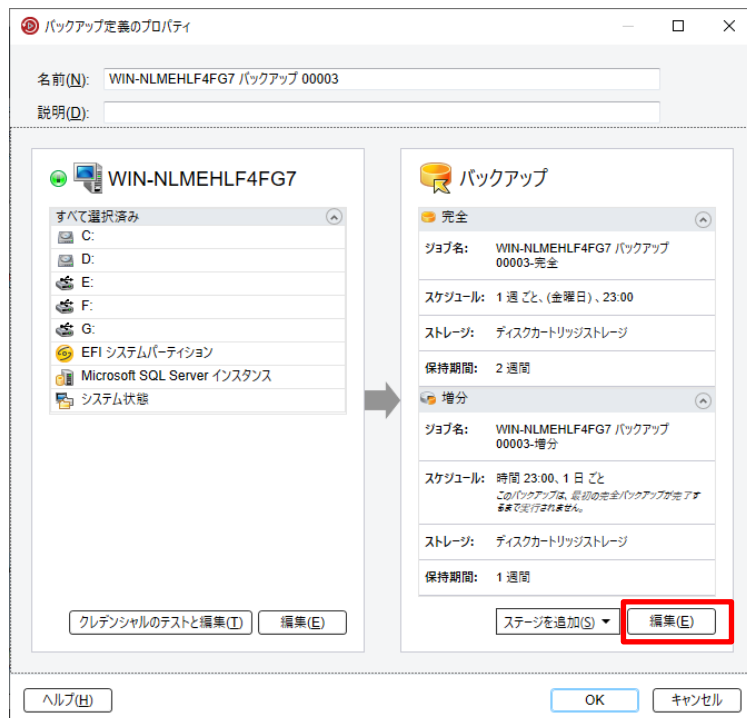
左側にバックアップ対象、右側にバックアップ先の設定画面が出るので、まず左側のバックアップ対象の「編集」ボタンを押します。



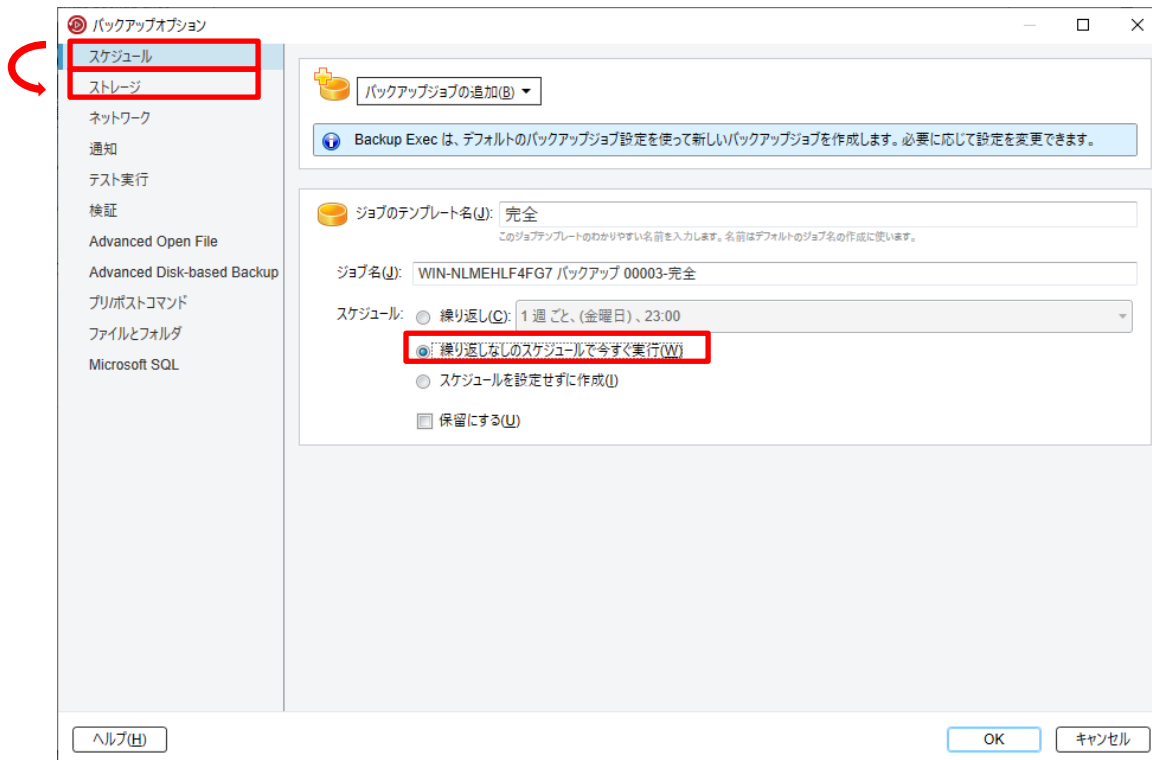
バックアップしたい項目を選択して「OK」をします。本例ではシステム全体をバックアップするので、バックアップ先となる E:ドライブや空の DVD ドライブなどを除く全てを選択しています。



次に右側のバックアップ先に関する「編集」を押します。

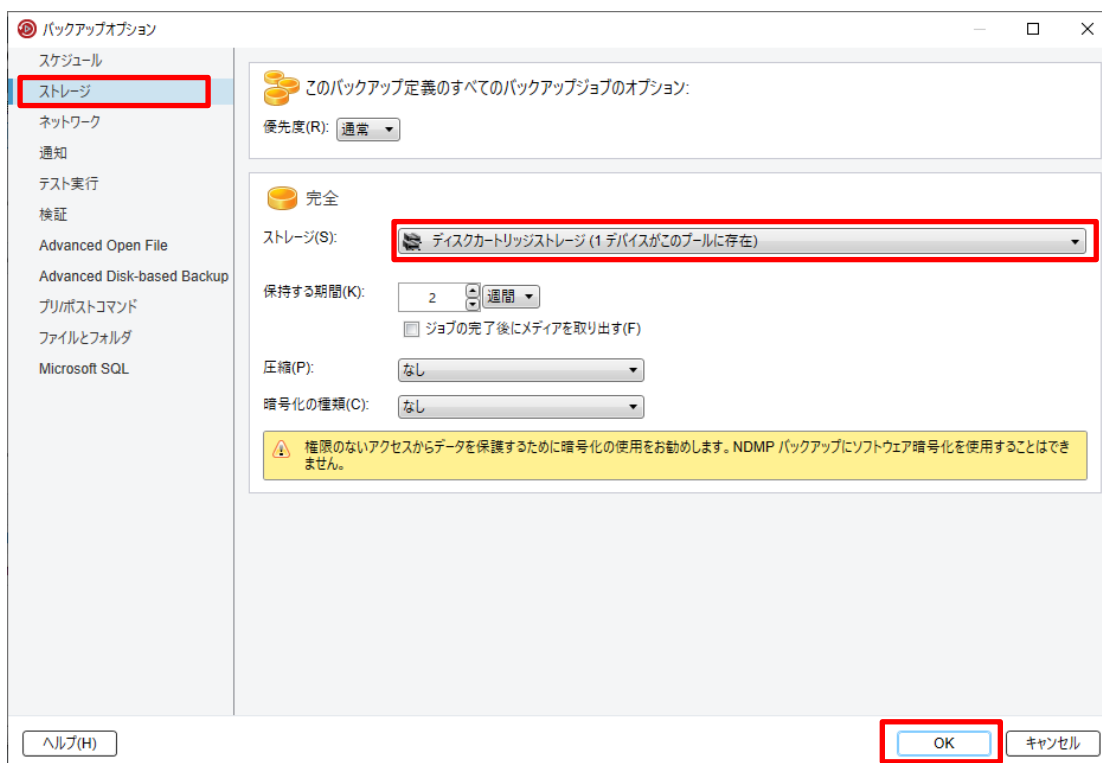


まずスケジュールを設定します。設定したいスケジュール内容に設定して（ここではまだ「OK」は押しません）、次の「ストレージ」設定に進みます。本例では1回きりの完全バックアップを作成するので、増分のウィンドウは削除し、「繰り返しなしのスケジュールで今すぐ実行」を選択しています。

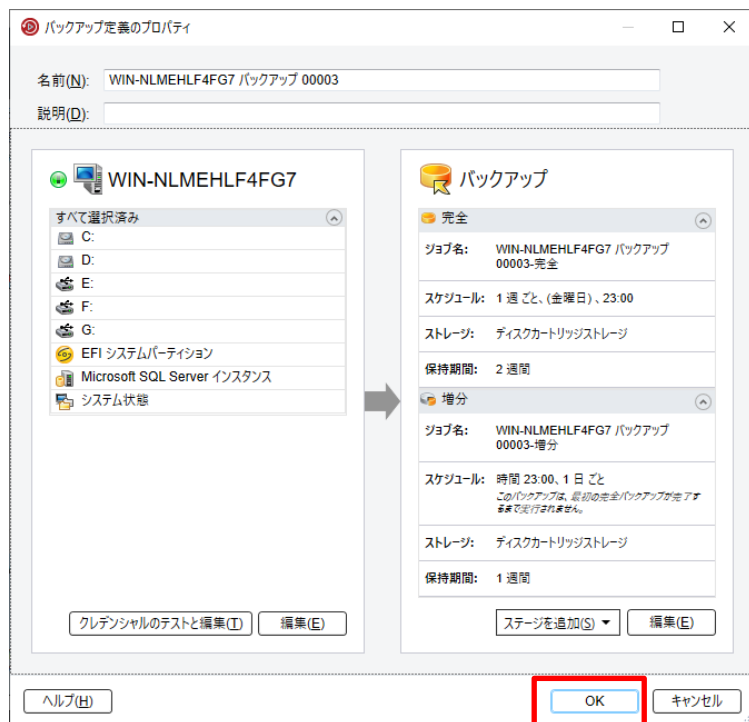


ストレージの設定で、バックアップ先のストレージが「ディスクカートリッジストレージ」になっていることを確認します。バックアップの完了後にカートリッジを取り出すオプションにチェックをつけることもできます。

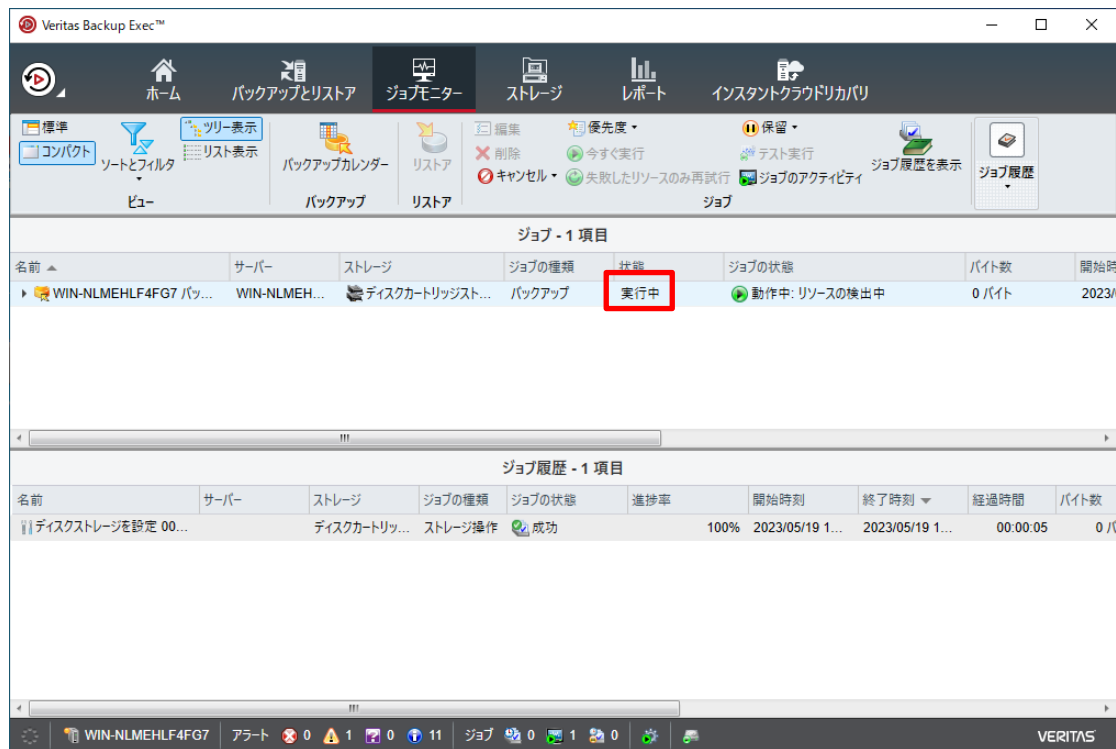
バックアップ先を確認したら「OK」を押します。



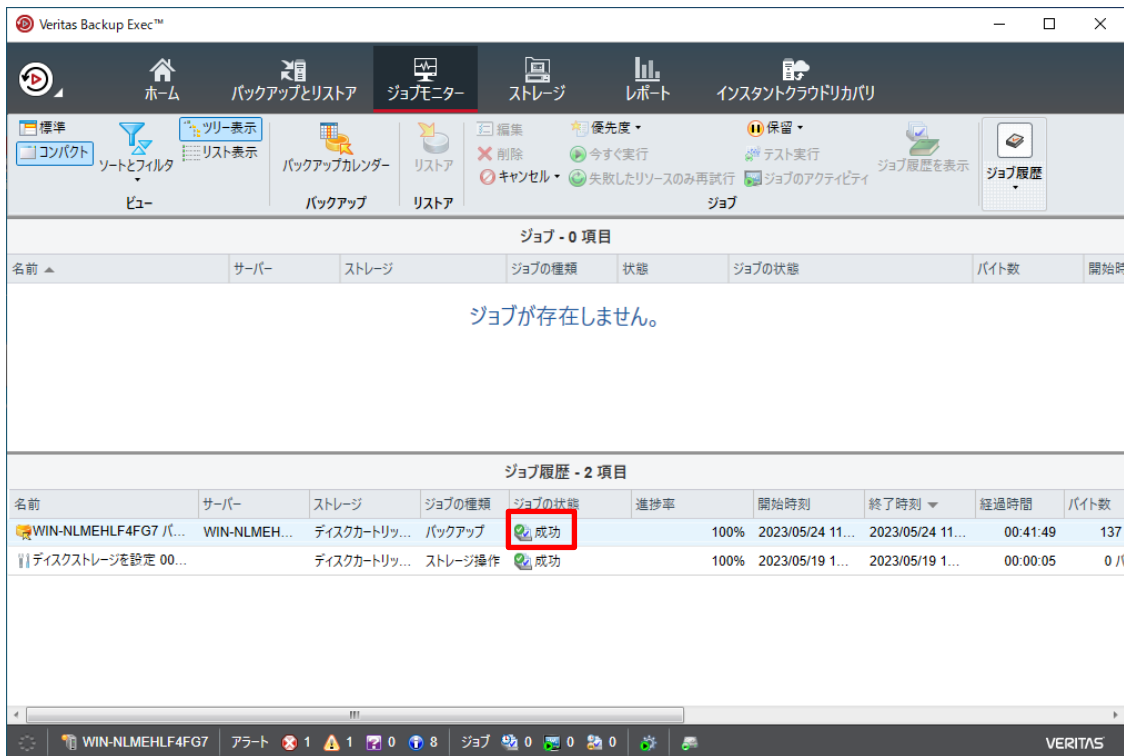
バックアップ対象、バックアップ先・スケジュールとも設定が終わったので、OK を押します。
 今回は「スケジュールせず今すぐ実行」を選択したので、OK を押したらすぐにバックアップが開始
 されます。



ジョブモニター画面を開き、バックアップが実行中になっていれば無事に開始されています。



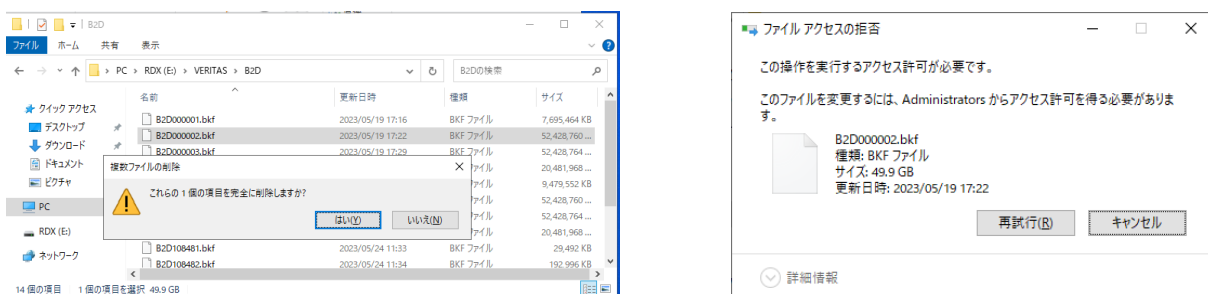
ジョブが「成功」となっていればバックアップ完了です。



バックアップが取得されると、RDX ドライブ内には「VERITAS」フォルダが作成されています。WindowsAD 等の特殊なバックアップが含まれていなければバックアップデータは全てこの「VERITAS」フォルダ内に取得され、BackupExec のランサムウェアレジリエンス機能によりこの VERITAS フォルダは保護されているため、VERITAS フォルダ内のファイルを手動で削除しようとしたり暗号化しようとしたりしても拒否されます。



試しに削除しようとしても（左）、右図のようにアクセス拒否され失敗します



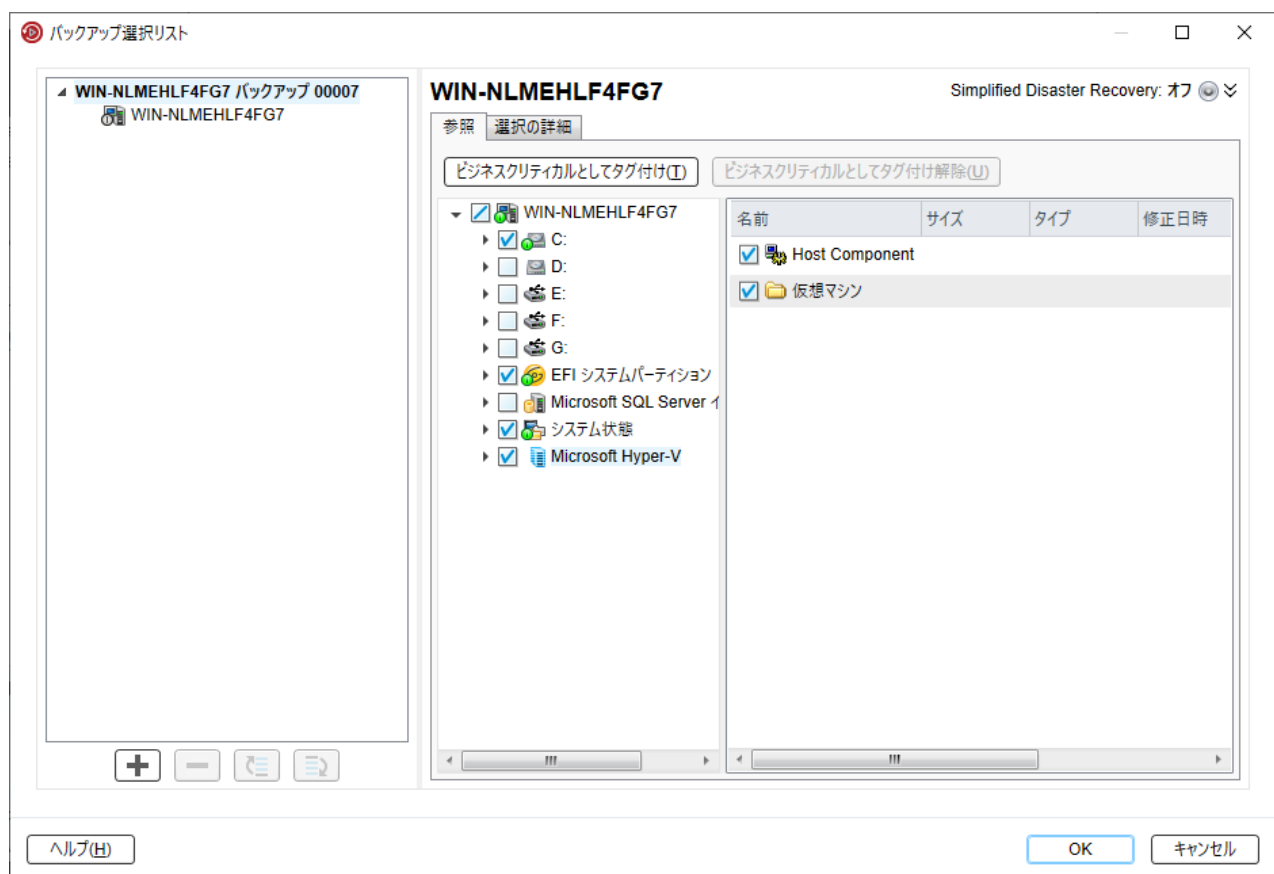
バックアップ対象に Windows Active Directory、Microsoft Exchange Server、Hyper-V などの特殊なデータが含まれている場合（GRT 対応バックアップの場合）

↓

BackupExec ではデフォルトでランサムウェアレジリエンス機能が有効になっているものの、**GRT 対応バックアップでは VERITAS フォルダの外にバックアップ関連データが作成され、ランサムウェアからの保護対象から外れるデータが生じます。**GRT バックアップは、AD や Exchange のメールデータ、仮想マシン内の個別データ等を個別にリストアすることを可能にする技術で、データ復元時の利便性を高めるもので、デフォルトで有効になっていますが、全てのデータを VERITAS フォルダ配下で保護したい場合は GRT 機能を無効にする必要があります。以下ではその手順を紹介しています。

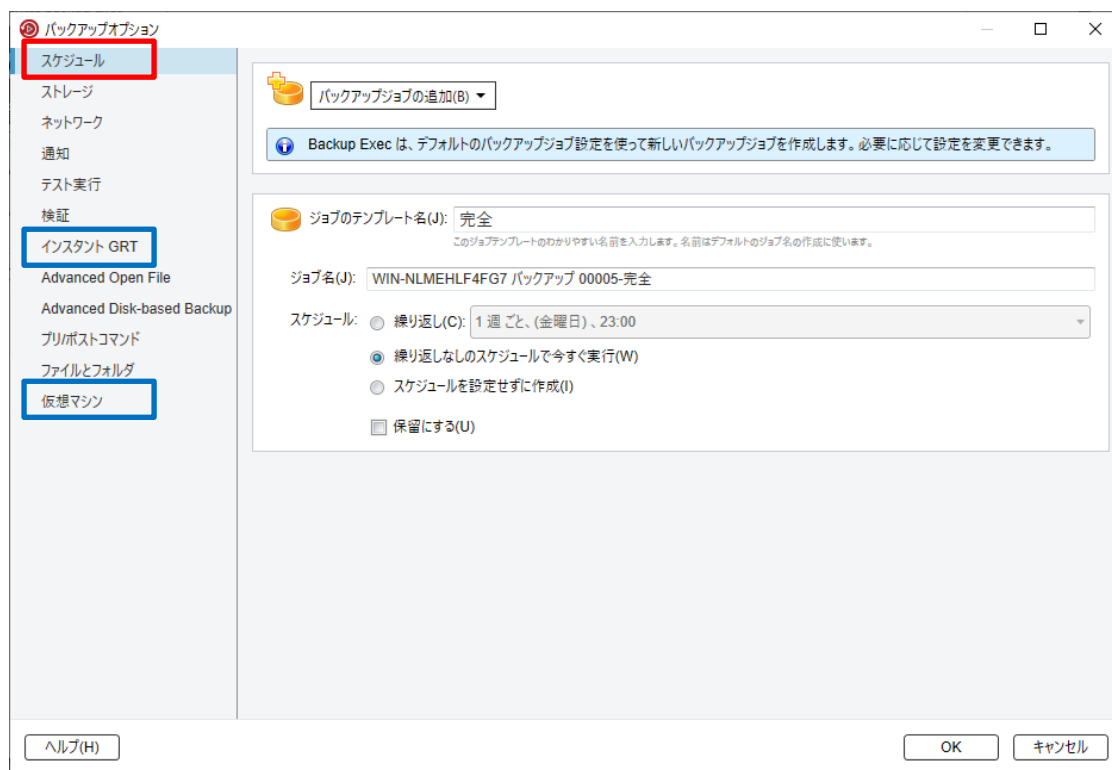
バックアップ設定までの手順は上記手順と同じです。

バックアップ対象の選択の画面で、以下例ではシステムデータと、GRT バックアップ対象とすることができる **Hyper-V** データをバックアップ対象として選択しています。

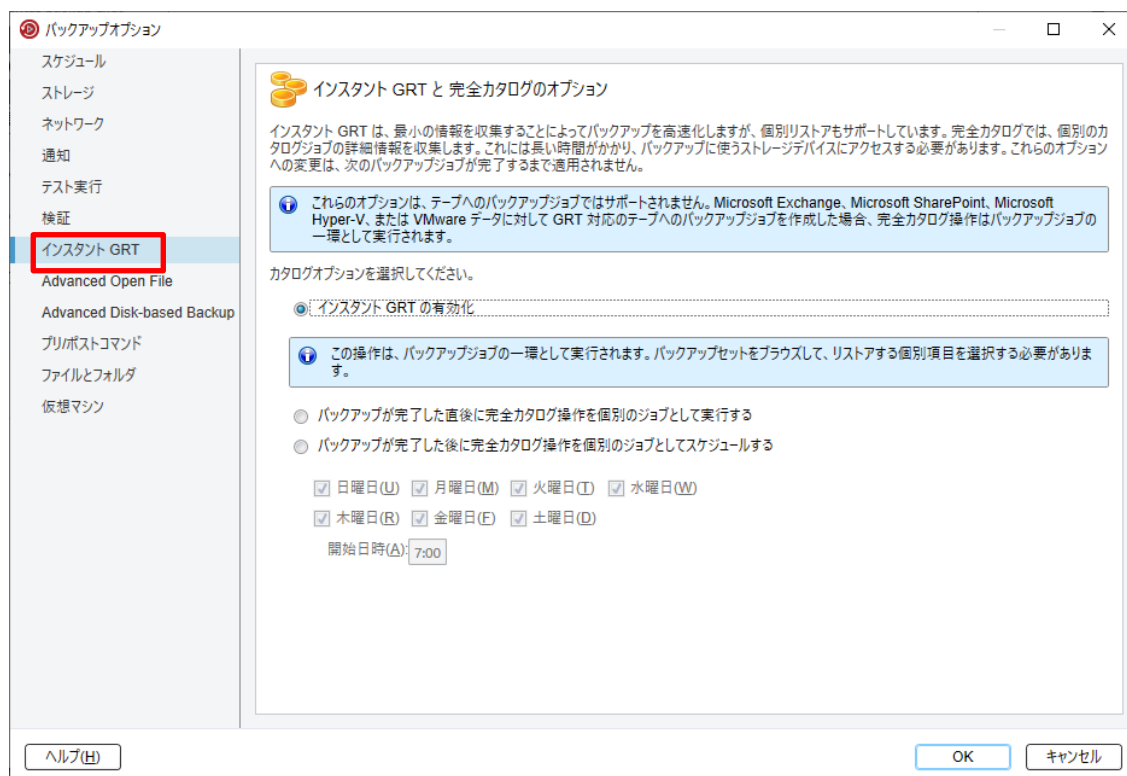


右側のバックアップオプションの編集画面では、先ほどの画面と異なり、「インスタント GRT」というメニューと「仮想マシン」というメニューが新しく表示されています。(バックアップ対象に Hyper-V が含まれたため)

本例では先ほど同様まずスケジュールで完全バックアップのみの「今すぐ実行」を選択しています。

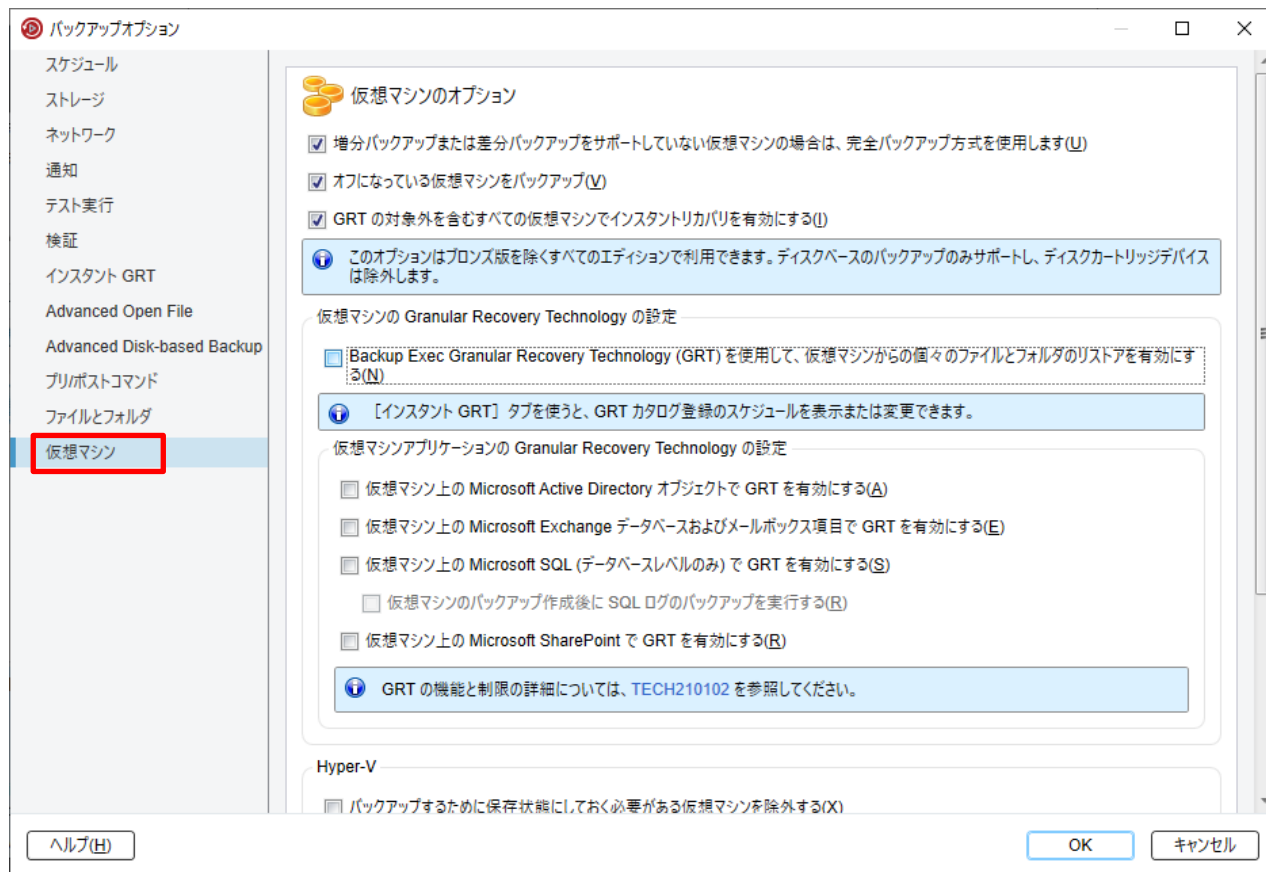


次に「インスタント GRT」のメニューでは、どれが選択されていても関係ありません。(次のページで GRT を無効にするため)



一番下の「仮想マシン」のオプション画面で、「BackupExec Granular Recovery Technology(GRT)」を使用して・・・」のチェックを外します。これで GRT が無効になります。

GRT 対象データが Hyper-V ではなく WindowsAD や Exchange 等の場合は、「仮想マシン」のメニューではなくそれぞれ対応したメニューから GRT の使用をオフにすることで同様に無効にできます。



OK でバックアップの設定は完了です。

以上