Dell™ NetVault™ Backup Plug-in for Standard Encryption 2.2

ユーザーズ・ガイド

凡例

△ **注意：注意アイコンは、指示に従わなかった場合に、ハードウェアの損傷やデータの損失につながる可能性があることを表しています。**

⚠ **警告：警告アイコンは、潜在的な資産の損害、個人の負傷または死亡の可能性を表しています。**

ⓘ **重要**、**メモ**、**ヒント**、**モバイル**、または**ビデオ**：情報アイコンは、サポート情報を表しています。

Plug-in for Standard Encryption ユーザーズ・ガイド
更新 — 2014 年 4 月
ソフトウェアのバージョン — 2.2
NVG-122-2.2-EN-01

目次

1

概要

Dell™ NetVault™ Backup Plug-in for Standard Encryption について

Dell™ NetVault™ Backup（NetVault Backup）は、2 種類の暗号化製品を提供しています。

- **Dell™ NetVault™ Backup Plug-in for Standard Encryption（Plug-in for Standard Encryption）** — Plug-in for Standard Encryption は、データを保護して規制要件を遵守するために、CAST-128 アルゴリズムをサポートしています。

  CAST-128 は 12 または 16 ラウンドの Feistel ネットワークで、ブロック・サイズは 64 ビット、キー・サイズは 40 ～ 128 ビットですが 8 の倍数でのみ使用できます。

- **Dell™ NetVault™ Backup Plug-in for Advanced Encryption（Plug-in for Advanced Encryption）** — Plug-in for Advanced Encryption は、データを保護して規制要件を遵守するために、AES-256 および CAST-256 アルゴリズムをサポートしています。

  - **CAST-256** — CAST-256 は CAST-128 と同じエレメントを使用しますが、ブロック・サイズは 64 ビットの 2 倍となる 128 ビットに対応しています。利用可能なキー・サイズは 128、160、192、224、および 256 ビットです。CAST-256 は、汎用 Feistel ネットワーク内にアレンジされた、48 ラウンド構成（12「クワッド・ラウンド」と呼ばれることもある）です。
  - **AES-256** — AES は米国政府が採用している暗号化標準規格です。標準規格は 3 つのブロック暗号 AES-128、AES-192、および AES-256 で成り立っています。各 AES 暗号はブロック・サイズが 128 ビットで、キー・サイズはそれぞれ 128、192、および 256 ビットになります。

NetVault Backup 暗号化アーキテクチャは、ECB（Electronic Codebook Mode）の操作のみをサポートしています。これは、各データ・ブロックが個別に暗号化されることを意味しています。2 つ以上の連続するブロックに同一のデータが含まれている場合、それらのブロックの暗号化形式も同一になります。

NetVault Backup クライアントにこれらの暗号化プラグインをインストールすると、ネットワーク上でバックアップ・デバイスに転送されるデータが暗号化されます。このデータは、クライアントにリストアされるまで暗号化されたままです。また、暗号化がセカンダリ・バックアップのみに必要な場合、暗号化するかどうかをジョブ単位で指定できます。たとえば、プライマリ・バックアップは暗号化せず、セカンダリ・コピー・バックアップだけを暗号化することができます。これにより、バックアップ所要時間を短縮できます。さらに、ディスク・ベースのストレージ・デバイスの使用時に、ジョブ単位重複排除機能を併用することにより、重複排除されていない非暗号化データから重複排除済みデータを抽出できます。これにより、重複排除の割合と重複排除処理のパフォーマンスを最適化できます。

Plug-in for Standard Encryption および Plug-in for Advanced Encryption は個別にインストール、ライセンスされます。

Plug-in for Standard Encryption および Plug-in for Standard Encryption と互換性がない NetVault Backup プラグインの一覧について詳しくは、それぞれのリリース・ノートを参照してください。

対象ユーザ

本ガイドは、バックアップ管理者と、組織のバックアップ戦略計画および実装について責任を持つ、その他の技術担当者を対象としています。暗号化ソリューションを理解していることを前提にしています。

参考資料

- 『Dell NetVault Backup インストール・ガイド』— このガイドでは、NetVault Backup サーバとクライアント・ソフトウェアのインストールに関する情報を記載しています。
- 『Dell NetVault Backup アドミニストレーターズ・ガイド』— このガイドは、データを保護するための NetVault Backup の設定、使用方法を説明しています。NetVault Backup のすべての特徴と機能に関する総合的な情報を提供しています。
- 『Dell NetVault Backup Command Line Interface Reference Guide』— このガイドは、NetVault Backup コマンド·ライン・ユーティリティの使用についての情報を提供しています。

これらのガイドは、https://support.software.dell.com/ からダウンロードできます。

重要： NetVault Backup は 10.0 から、NetVault Backup システムとインストールされているプラグインを設定、管理、監視するための、Web ベースのユーザ・インターフェイスを提供しています。このバージョンのプラグインのユーザーズ・ガイドに記載されている手順は、この新しい NetVault WebUI の使用を前提にしています。NetVault Backup コンソール（NetVault Backup 9.x および 8.x で使用できるユーザ・インターフェイス）による手順について詳しくは、古いバージョンのプラグインのドキュメントを参照してください。

2

バックアップ計画の策定

暗号化計画の概要

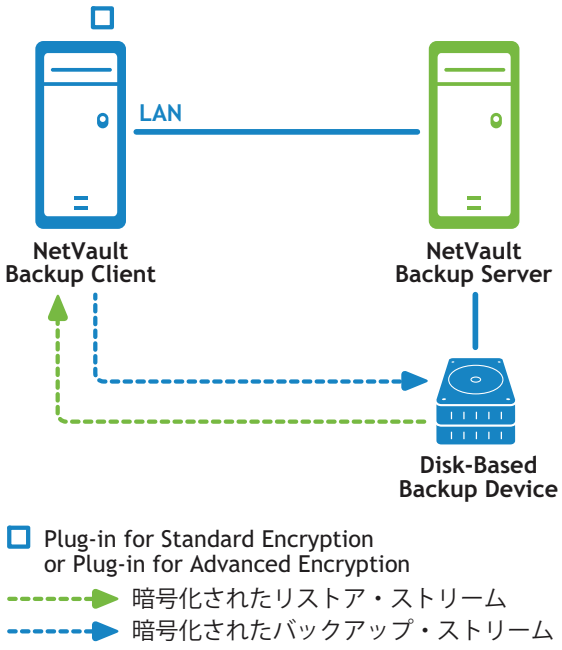
暗号化計画を策定する場合、以下の事項を決定する必要があります。

- 暗号化するバックアップ。
- 必要な暗号化アルゴリズム。
- プライマリ・バックアップまたはセカンダリ・バックアップの暗号化が必要かどうか。
- すべてのバックアップに対して暗号化を有効にするか、またはジョブ単位で有効にするか。

暗号化するバックアップの選択

NetVault Backup は、ソフトウェアベースの暗号化を実行します。バックアップ・ストリームは、プラグインがインストールされている NetVault Backup サーバまたはクライアントにより、選択したアルゴリズムを使って暗号化されます。暗号化されたデータ・ストリームはネットワーク経由でバックアップ・デバイスに転送されます。デバイスでは、暗号化状態で保持されます。リストア時には、暗号化されたバックアップがバックアップ・デバイスから、プラグインがインストールされているターゲット NetVault Backup クライアントに転送されます。このクライアントで復号化が行われます。

図 1. 暗号化バックアップとリストア・パス



NetVault Backup サーバへの Plug-in for Standard Encryption または Plug-in for Advanced Encryption のインストールは、NetVault データベース・バックアップなどのサーバに由来するバックアップを暗号化する場合にのみ必要になります。ビルトイン・プラグインまたはライセンス・プラグインが動作しているクライアントに由来するバックアップの暗号化には必要ありません。

バックアップの暗号化および復号化プロセスは、NetVault Backup サーバまたはクライアントにインストールされているプラグインが行います。これらのプロセスは、マシン上のリソースを消費します。暗号化プロセスによりバックアップの実行時間が長くなります。また、復号化プロセスによりリストアの実行時間が長くなります。暗号化が必要なバックアップを判断する際には、クライアントのパフォーマンス、バックアップ・ウィンドウ、およびリストア時間に与える影響を考慮する必要があります。簡単に言うと、パフォーマンス、バックアップ・ウィンドウ、およびリストア時間に与える影響よりもセキュリティ要件の方が重要な場合にのみ、バックアップを暗号化する必要があります。

暗号化アルゴリズムの選択

NetVault Backup には、バックアップの暗号化と複合化に使用できる複数のアルゴリズムが用意されています。各 NetVault Backup クライアントが別の暗号化アルゴリズムを使用することはできますが、ある特定のクライアントからのバックアップにはすべて同じアルゴリズムを使用する必要があります。

リストア時には、バックアップ時に使用したのと同じ暗号化アルゴリズムを使用する必要があります。この時点以降は、前に使用したのと別のアルゴリズムを使用することも可能です。ただし、以前のアルゴリズムを使用したバックアップのリストア時には、データを正しくリストアするために、バックアップが使用したアルゴリズムを NetVault Backup サーバまたはクライアントに設定する必要があります。たとえば、以前のバックアップでは CAST-128 アルゴリズムを使用しており、現在のバックアップは AES-256 アルゴリズムを使用している場合、以前のバックアップのリストア時には、サーバまたはクライアンのプラグインが CAST-128 アルゴリズムを使用するように設定しないと、リストアが失敗してしまいます。

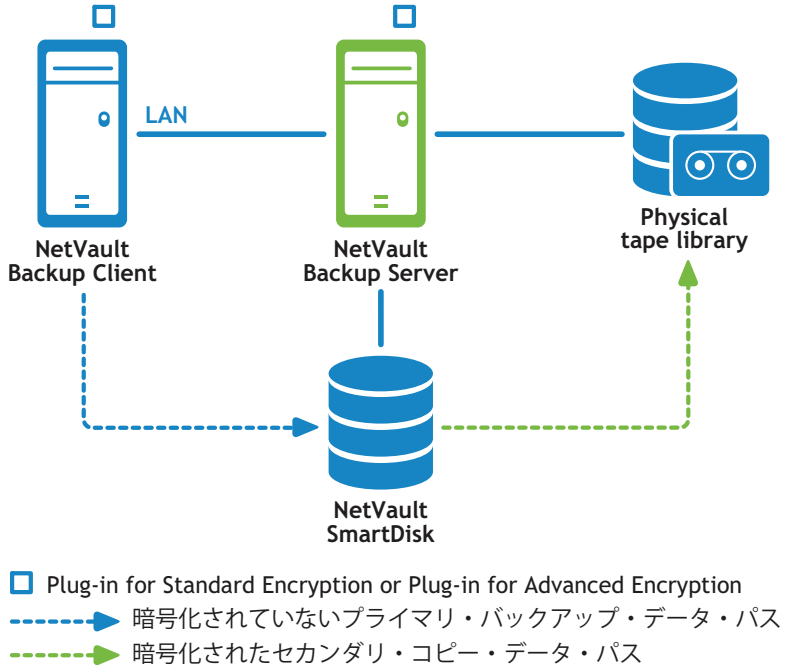
プライマリまたはセカンダリ・バックアップの暗号化

バックアップ・ジョブは、プライマリ・バックアップセカンダリ・コピーの 1 つ、または必要に応じて 2 つのフェーズから成り立っています。プライマリ・バックアップは、選択したバックアップ・デバイスへのデータ・ストリームのバックアップです。一般的にこれらのバックアップは、高速なリストアをかのイニえるためにローカル・ストレージ・デバイスに対して行われます。セカンダリ・コピーはプライマリ・バックアップの別のバックアップ・デバイスへの複製またはデータ・コピーです。通常これらのバックアップは、リモートのディスク・ベースのストレージ・デバイスまたはディザスタ・リカバリの目的でサイト外にテープを保管する物理テープ・ライブラリをターゲットにしています。

セキュリティ要件により、プライマリ・バックアップとセカンダリ・コピーの両方を暗号化する必要があるかどうかを判断します。たとえば、セキュリティ要件に社内ネットワーク外に送信または保管されるバックアップのみ暗号化が必要であると規定されている場合は（遠隔地にある物理テープに保管されるバックアップなど）、物理テープ・ライブラリを対象にしたセカンダリ・コピー・バックアップのみを暗号化する必要があることになります。ただし、セキュリティ要件にネットワーク上に伝送されるデータ、またはディスク・ベースのバックアップ・デバイスが社内ネットワーク内に存在している場合でもそのデバイスに保管するデータを暗号化する必要があると規定されている場合は、プライマリ・バックアップとセカンダリ・コピーの両方を暗号化する必要があります。

暗号化データは、重複排除がうまく機能しません。そのため、重複排除をサポートしているストレージ・デバイスに対してプライマリ・バックアップを実行する場合は、セカンダリ・コピー・バックアップのみ暗号化する方が有益です。プライマリ・バックアップを重複排除し、セカンダリ・バックアップを暗号化することで、暗号化と重複排除の両方の利点を活用することができます。

図 2. 暗号化されないプライマリ・バックアップと暗号化されたセカンダリ・コピー・バックアップ



すべてまたは特定のバックアップの暗号化

Plug-in for Standard Encryption または Plug-in for Advanced Encryption をインストールしたら、プラグインをインストールした NetVault Backup サーバまたはクライアント上のすべてのバックアップに対する暗号化を有効にすることができます。また、特定のジョブに対する暗号化を有効にすることも可能です。また、プライマリ・バックアップのみまたはセカンダリ・バックアップのみに対して有効にすることもできます。そうすることにより、暗号化と重複排除の両方の利点を活用することができます。たとえば、プライマリ・バックアップで重複排除を行って、セカンダリ・コピーで暗号化することができます。

ジョブ・レベルの暗号化オプションは、以下のような状況に利用できます。

- サーバまたはクライアントにインストールされているプラグインが、Plug-in for Standard Encryption または Plug-in for Advanced Encryption と互換性がない場合。
- サーバまたはクライアントの特定のバックアップのみ暗号化が必要な場合。
- プライマリ・バックアップの暗号化は不要で、オフサイトで保護するセカンダリ・バックアップの暗号化が必要である場合。
- プライマリ・バックアップが重複排除機能をサポートしているストレージ・デバイスを対象としている場合。

以下の状況下では、NetVault Backup サーバおよびクライアントがそのバックアップすべてを暗号化するように設定する必要があります。

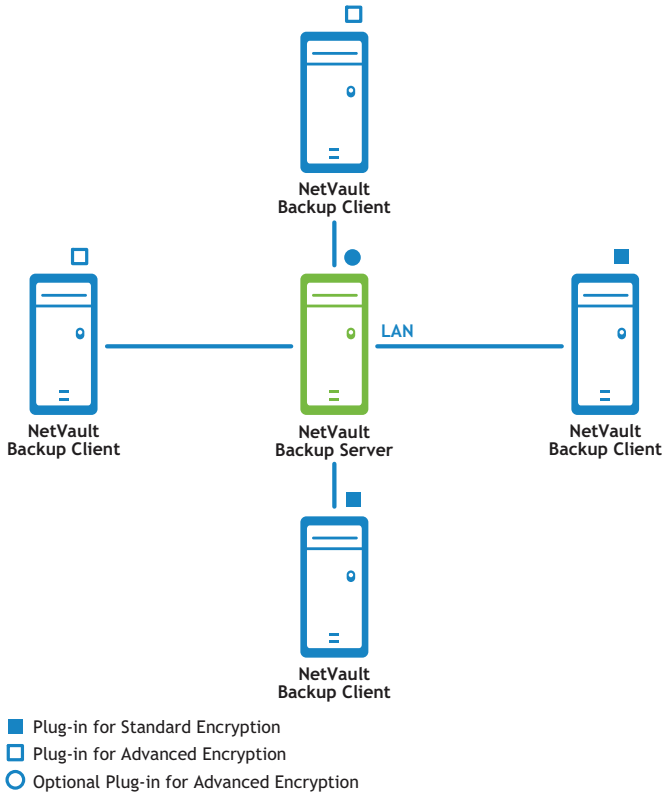
- サーバまたはクライアントにインストールされているすべてのプラグインが、Plug-in for Standard Encryption または Plug-in for Advanced Encryption と互換性がある。
- サーバまたはクライアントのすべてのバックアップに暗号化が必要である。
- プライマリおよびセカンダリ・バックアップの両方に暗号化が必要である。
- 重複排除用にバックアップが選択されていない。

3

プラグインのインストール

システム構築の概要

図 1. システム構築の概要



Plug-in for Standard Encryption または Plug-in for Advanced Encryption は、バックアップを暗号化するすべての NetVault Backup クライアントにインストールする必要があります。各クライアントに対して、個別のライセンス・キーを入手する必要があります。サーバおよびクライアントを、別の暗号アルゴリズムを使用するように設定することができます（サーバまたはクライアントを使って暗号化セカンダリ・コピーを作成する場合を除く）。

たとえば、クライアントが AES-256 アルゴリズムを使用するように設定されており、暗号化されたセカンダリ・コピーを作成するためにサーバを使用する場合、クライアントがセカンダリ・コピー・バックアップをリストアするために、サーバも AES-256 アルゴリズムを使用するように設定する必要があります。

プラグインのインストール

プラグインをインストールするには

1 ［ナビゲーション］パネルで、**［ガイド付き設定］**をクリックして、次に**［NetVault 設定ウィザード］**ページで**［プラグインのインストール］**をクリックします。**［NetVault Backup クライアント］**リストで、プラグインをインストールするクライアントを選択します。この方法では複数のクライアントを選択することができます。

> 複数のクライアントを選択する場合、プラグインのバイナリ・ファイルがターゲットクライアントの OS とプラットフォームと互換性があることを確認する必要があります。

- または -

［ナビゲーション］パネルで、**［クライアント管理］**をクリックします。**［NetVault Backup クライアント］**リストで、プラグインをインストールするクライアントを選択し、**［管理］**をクリックします。インストールされているソフトウェアのテーブルの右下にある、［プラグインのインストール］ボタン（  ）をクリックします。

2 **［プラグイン ファイルの選択］**をクリックして、参照ウィンドウからプラグイン用 **.npk** インストレーション・ファイルの場所（インストール用 CD または Web サイトからファイルをダウンロードして保存したディレクトリなど）を探します。

3 プラグイン用のプラットフォーム固有のバイナリ・ファイルを選択します。ファイル名は以下の表に記載されています（**x-x-x-x** はバージョン、ビルド、およびプラットフォーム番号を表しています）。

表 1. サポートしている暗号アルゴリズムのバイナリ・ファイル

暗号アルゴリズム	バイナリ・ファイル名
CAST-128	cst-x-x-x-x.npk
CAST-256	cst2-x-x-x-x.npk
AES-256	aes-x-x-x-x.npk

［次へ］をクリックすると、インストールが開始されます。

4 インストールが正常に完了すると、メッセージが表示されます。

プラグインの削除

プラグインを削除するには

1 ［ナビゲーション］パネルで、**［クライアント管理］**をクリックします。

2 **［NetVault Backup クライアント］**リストから、クライアントを選択して、**［管理］**をクリックします。

3 ［インストール済のプラグイン］テーブルから、削除するアルゴリズムを選択します。以下のオプションを利用できます。

- CAST-128 Encryption
- CAST-256 Encryption
- AES-256 Encryption

［プラグインの削除］ボタン（  ）をクリックします。

4 **［確認］**ダイアログ・ボックスで、**［削除］**をクリックします。

4

プラグインの設定

デフォルト設定の構成

プラグインのデフォルトを設定するには

1 ［ナビゲーション］パネルで、**［設定変更］**をクリックして、次に**［設定］**ページで目的に応じて［サーバ設定］または［クライアント設定］をクリックします。

2 **［プラグイン］**で**［暗号化］**をクリックします。

3 以下の設定を行います。

表 1. プラグインのデフォルト設定

設定	説明
Encrypt ALL Backups on this Client	クライアントに Plug-in for Standard Encryption または Plug-in for Advanced Encryption をインストールすると、以下のような作業を行えます。 • そのクライアントで実施されるすべてのバックアップを暗号化する • そのクライアントで実施される特定のバックアップを暗号化する すべてのバックアップの暗号化を有効にするには、このチェック・ボックスを選択します。すべてのバックアップの暗号化を有効にすると、ジョブ単位の設定を変更することはできません。 特定のバックアップの暗号化を有効にする方法について詳しくは、「ジョブ・レベルの暗号化の実行」を参照してください。 NetVault Backup サーバまたはクライアントに由来するバックアップの、ジョブ・レベルの暗号化を実施する場合、すべてのバックアップを暗号化するようにはプラグインを設定しないようにする必要があります。
Encryption Key String	NetVault Backup マシンの暗号鍵として使用する文字列を入力します。 プラットフォームに応じて、使用できる文字やパスワード長が異なります。32 文字以下のパスワードを使用することをお勧めします。「A ～ Z」、「a ～ z」「0 ～ 9」、および「_」の文字セットを使用できます。プラットフォームによっては、これらの基準に従わない鍵文字列を使用できることはありますが、他の環境では使用できないこともあります。
Available Encryption Algorithms	バックアップに対して使用する、暗号アルゴリズムを選択します。インストールした製品に応じて、リストには CAST-128、CAST-256、および AES-256 のオプションが含まれます。

4 新しい設定を保存してダイアログ・ボックスを閉じるには、**［実行］**をクリックします。

暗号化バックアップは元の場所、または新しいターゲット・マシン上にリストアできます。どちらの場合でも、ターゲット・マシン上にプラグインをインストールする必要があり、またバックアップ実行時と同じように設定する必要があります（同じ**暗号鍵文字列**と**暗号アルゴリズム**を使用）。

5

プラグインの使用

すべてのバックアップの暗号化

特定の NetVault Backup クライアントから実行されるすべてのバックアップの暗号化が有効になっている場合、バックアップの暗号化に関するその他の要件はありません。バックアップおよびリストア手順について詳しくは、関連するプラグインのユーザーズ・ガイドを参照してください。

ジョブ・レベルの暗号化の実行

ジョブ・レベルの暗号化を使用して、プライマリ・バックアップ、セカンダリ・コピー、またはその両方を暗号化することができます。セキュリティ要件で、ネットワーク伝送時、またはディスク・ベースのバックアップ・デバイスが社内ネットワーク内に存在している場合でもそのデバイスへの保管時に、バックアップを暗号化する必要があると規定されている場合は、プライマリ・バックアップとセカンダリ・コピーの両方を暗号化することが役に立ちます。

ジョブ・レベルの暗号化設定は、バックアップ詳細設定セットで指定します。バックアップ・ジョブの詳細設定セットの作成について詳しくは、『Dell NetVault Backup アドミニストレーターズ・ガイド』を参照してください。

プライマリ・バックアップの暗号化

プライマリ・バックアップのジョブ・レベルの暗号化を有効にするには

1. バックアップ・ジョブ・ウィザードを開始して、**[詳細設定]** ページを開きます。詳しくは、『Dell NetVault Backup アドミニストレーターズ・ガイド』を参照してください。
2. **[詳細設定]** をクリックします。
3. **[詳細設定]** ダイアログ・ボックスで、**[暗号化の有効化]** チェック・ボックスを選択します。

セカンダリ・コピーの暗号化

NetVault Backup は、セカンダリ・コピーを作成するために以下の手段を提供しています。

- **複製** — この方式では、元のバックアップにリンクしている正確なコピーを作成します。バックアップがセグメントに分割されて、それらのセグメントがストレージ・デバイスにコピーされます。リストア時に、プライマリおよびセカンダリ・コピーのセグメントは交換できます。リストア時に暗号化されていないセグメントと暗号化されたセグメントを混在させることはできないため、複製方式を使って作成されたセカンダリ・コピーの暗号化を有効または無効にすることはできません。複製方式では、元のセーブセットが暗号化されている場合、暗号化されたセカンダリ・コピーが作成されます。プライマリ・バックアップが暗号化されていない場合は、セカンダリ・コピーも暗号化されません。

- **データ・コピー** — この方式が推奨されるのは、オフサイト・ストレージ用にセカンダリ・コピーが作成される場合です。データ・コピー方式では、バックアップがセグメントに分割されて、それらのセグメントがバックアップ・デバイスにコピーされます。リストア時には、データを復元するためにプライマリまたはセカンダリ・コピーが使用されます。プライマリおよびセカンダリ・コピーのセグメントは交換できませすん。そのため、プライマリ・コピーが暗号化されていなくてもデータ・コピーで暗号化を使用できます。これは、プライマリ・バックアップで重複排除オプションを使用するような場合に役立ちます。

セカンダリ・コピーのジョブ・レベルの暗号化を有効にするには

1. バックアップ・ジョブ・ウィザードを開始して、**[詳細設定]** ページを開きます。詳しくは、『Dell NetVault Backup アドミニストレーターズ・ガイド』を参照してください。
2. **[セカンダリ・コピー]** をクリックします。
3. **[セカンダリ・コピー]** ダイアログ・ボックスで、**[セカンダリ・コピーの作成]** チェック・ボックスを選択します。
4. **[セカンダリ・コピーのみ暗号化]** チェック・ボックスを選択します。このオプションは、データ・コピー方式を選択した場合にのみ利用できます。

   プライマリ・コピーが暗号化されている場合、**[セカンダリ・コピーのみ暗号化]** チェック・ボックスの指定にかかわらず、暗号化されたセーブセットが自動的に作成されます。したがって、このオプションが役立つのは、暗号化されていないプライマリ・コピーを暗号化してセカンダリ・コピーを作成するときだけです。

   [セカンダリ・コピーのみ暗号化] チェック・ボックスを選択した場合、暗号化されたプライマリ・コピーは再暗号化されません。このようなセカンダリ・コピーからデータをリストアするには、プライマリ・コピーの暗号化キーを使用する必要があります。

Dell について

Dell はお客様の声を大切にし、常に製品やサービスの向上に努めております。詳しくは、www.software.dell.com を参照してください。

Dell へのお問い合わせ

テクニカル・サポート：
オンライン サポート

販売製品に関するご質問：
03-5908-3511

電子メール：
Sales.JP@quest.com

テクニカル・サポート用リソース

テクニカル・サポートは、有効なメンテナンス契約が付いた Dell ソフトウェアをご購入のお客様、およびトライアル版をご使用のお客様がご利用いただけます。サポート・ポータルにアクセスするには、https://support.software.dell.com/jp に移動してください。

サポート・ポータルには、問題を素早く自力で解決するために役立つ自己支援ツールが用意されており、1 年中毎日 24 時間ご利用いただけます。また、このポータルのオンライン・サービス・リクエスト・システムを利用して、製品サポート・エンジニアに直接アクセスすることもできます。

このサイトでは、以下の作業を行えます。

- サービス・リクエスト（案件）の作成、更新、管理
- Knowledge Base 記事の参照
- 製品に関するお知らせの入手
- ソフトウェアのダウンロードトライアル版のソフトウェアについては、Trial Downloads（トライアル版のダウンロード）に移動してください。
- 入門ビデオの表示
- コミュニティでのディスカッション