テクニカルホワイトペーパー

Veritas Backup Exec

セキュリティと暗号

2020 年 4 月

ベリタステクノロジーズ合同会社
テクノロジーセールス&マーケティング本部

VERITAS
The truth in information.

免責事項

ベリタステクノロジーズ合同会社は、この文書の著作権を留保します。 また、記載された内容の無謬性を保証しません。Veritas Backup Exec は将来に渡って仕様を変更する可能性を常に含み、これらは予告なく行われることもあります。なお、当ドキュメントの内容は参考資料として、読者の責任において管理/配布されるようお願いいたします。

目次

免責事項 2

1. VERITAS BACKUP EXEC 4

2. エグゼクティブサマリ 5

3. 暗号化の必要性 5

4. BACKUP EXEC での暗号化 6

5. ソフトウェア暗号化 7

6. 連邦情報処理標準（FIPS）140-2 準拠のソフトウェア暗号化 8

7. ハードウェア暗号化 9

8. 暗号化キー 10

9. 専用キーと共通キー 11

10. パスフレーズ 11

11. 暗号化キー管理 12

12. 暗号キーの追跡変更 14

13. BACKUP EXEC データベース暗号キー 15

14. BACK EXEC データベースへのセキュアな SQL 接続 16

15. SSL を利用したネットワークセキュリティ層 18

16. 圧縮を用いた暗号化 20

17. バックアップ実行時の安全なコンソール管理 20

アイデンティティ認証 20

セッションロック 21

18. ファイアウォールでのバックアップ実行 21

19. ベストプラクティス 21

20. ベリタスへの脆弱性報告 22

21. サマリ 23

22. 詳細はこちら 23

1. Veritas Backup Exec

Veritas Backup Exec™ は、障壁のないバックアップソリューションです。何をバックアップするか、どこに保存するか、料金はお客様が選択します。オンプレミスからクラウドへのバックアップ、クラウド内でのワークロードの保護、クラウドからのリカバリ、オンプレミスストレージへの接続など、あらゆる段階でデータを安全かつ利用可能な状態に保ちます。Backup Exec を使用することで、拡大を続けるソリューション・ファミリーに接続して、ビジネスを自信を持って運営することができます。

Backup Exec は、永続ライセンスまたは期間限定のサブスクリプション・ライセンスで購入でき、必要な機能レベル（ブロンズ、シルバー、ゴールド）に応じて購入できます。ブロンズ・エディションは、最も経済的なオプションです。シルバーエディションは、最も使用されている機能を提供しています。ゴールド・エディションには、Backup Exec で利用できるすべての機能が含まれています。ご購入は、バックアップする必要のあるフロントエンド・データの量に応じて決定されます。選択したライセンス・セットは、必要な数量でご利用いただけます。

Backup Exec は、外部の脅威からの包括的な保護を提供します。そのため、想像を絶するような事態が発生した場合でも、重要なデータはバックアップされ、迅速かつ簡単に復旧することができます。

- 統合された 128/256 ビット AES 暗号化により、データのセキュリティリスクを軽減します。
- Backup Exec とクラウド・ターゲット間のセキュア・ソケット・レイヤー（SSL）接続によるデータ転送
- 容易な設定と管理のための統合された暗号化キー管理システム
- Secure Console Management は、Backup Exec コンソールのセキュリティを強化します。
- ペイメントカード業界のデータセキュリティ基準に対応。(PCI DSS) 3.1/3.2 規格
- FIPS 140-2 準拠 ソフトウェア暗号化
- TLS 1.2 をサポート
- Backup Exec データベースの機密コンテンツを保護するために使用される 256 ビット AES 対称暗号化アルゴリズム。
- 暗号化標準 T10 を使用するストレージデバイスのハードウェア暗号化をサポートします。
- トランジット時と休止時にデータを暗号化し、完全なデータセキュリティを実現
- 無償で Backup Exec に含まれています。

2. エグゼクティブサマリ

企業とそのデータに対するセキュリティとコンプライアンスのリスクは、これまで以上に大きくなっています。企業は、データを内部に保存し、外部に持ち出す際に、安全かつ確実な方法でデータが保護されているかどうかに依存しています。新たなコンプライアンス規制の出現に伴い、データの損失は、規制やコンプライアンス上の懸念事項の追加を含め、収益に悪影響を及ぼす可能性があります。

企業のバックアップに暗号化戦略を導入することは、データの完全性と可用性を保護する上で重要な役割を果たします。

3. 暗号化の必要性

データ盗難、テープ紛失、ランサムウェア、暗号化されていないデータを含む顧客記録の漏洩などの見出しが頻繁に登場しています。これらの出来事は、バックアップ作業中に作成されたデータのコピーを含む、重要かつ機密性の高い企業データの保護に重点を置く必要性を強調しています。

お客様の機密データに対するリスクの窓は、お客様のデータの価値が高まるにつれて拡大していきます。これらのリスクには、以下のようなものがあります。

- セキュリティのためにオフサイトに持ち出された暗号化されていないリムーバブルメディアは、他のほとんどの企業データに比べてセキュリティが低い。
- テープやリムーバブルメディアの盗難は、メディアの大きさから追跡が困難な大きなリスクです。
- テープを紛失したり、保護されていないまま放置されたりすると、データが第三者に渡ってしまう可能性があります。
- テープが不正な目的でコピーされたり、複製されたりしたかどうかを見分ける方法はありません。
- テープは、最も安全な方法ではなく、低コストの方法でオフサイトに持ち出されることが多い。
- オペレータは、システムにリダイレクトされたテープの不正なリストアを開始することができます。

暗号化は、ポータブルメディア上のデータを保護するための最も効果的な方法です。アナリスト、政府、法執行機関、規制機関は暗号化の重要性についてアドバイスを続けていますが、まだ多くの企業はバックアッププロセスの一部として暗号化を導入していません。この決定の主な理由は、暗号化によってプロセスに複雑なレイヤーが追加される可能性があることと、バックアップやリストアのプロセスを正常に完了するために必要な時間が長くなることです。

4. Backup Exec での暗号化

Backup Exec は、データを暗号化する機能を提供します。データを暗号化すると、不正アクセスからデータを保護します。データにアクセスしようとする者は、あなたが作成した暗号化キーを持っていなければなりません。Backup Exec はソフトウェア暗号化を提供しますが、T10 規格でハードウェア暗号化を提供するデバイスもサポートしています。Backup Exec は、バックアップ・ジョブに使用するストレージ・デバイスを指定すると、暗号化を設定します。

Backup Exec は 2 つのセキュリティ・レベルの暗号化をサポートしています。128 ビット AES（Advanced Encryption Standard）と 256 ビット AES です。256 ビット AES 暗号化は、128 ビット AES よりも暗号化キーが長いため、より強力なセキュリティ・レベルを提供します。

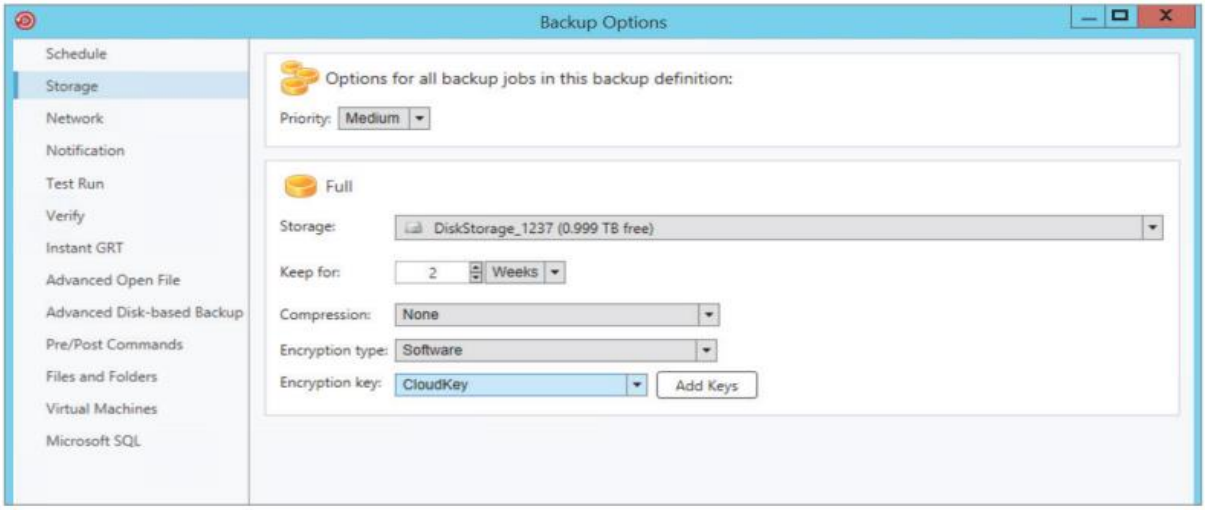

図 1: バックアップオプションの暗号化キーオプション

しかし、128 ビット AES 暗号化の方が、バックアップジョブをより迅速に処理することができます。T10 標準を使用したハードウェア暗号化には 256 ビット AES が必要です。バックアップジョブの複製を行う場合、すでに暗号化されているバックアップセットを再度暗号化はしません。ただし、暗号化されていないバックアップセットを暗号化することはできます。

Backup Exec がソフトウェアの暗号化に使用する Advanced Encryption Standard (AES)の詳細については、以下のドキュメントを参照してください。

http://en.wikipedia.org/wiki/Advanced_Encryption_Standard

5. ソフトウェア暗号化

Backup Exec をインストールすると、インストール・プログラムは、Backup Exec サーバと Backup Exec エージェントを使用するリモート・コンピュータに暗号化ソフトウェアをインストールします。Backup Exec は、Backup Exec エージェントを使用するコンピュータでデータを暗号化し、暗号化されたデータを Backup Exec サーバに転送します。そして、Backup Exec は暗号化されたデータをセット単位でパブリック・クラウド・ストレージ・ターゲット（AWS、Azure、Google など）、テープ、またはディスク・ストレージに書き込みます。

Backup Exec は、以下のタイプのデータを暗号化します。

- ファイルや Microsoft Exchange データベースなどのユーザーデータ。
- ファイル名、属性、オペレーティングシステム情報などのメタデータ。
- テープ上のカタログファイルやディレクトリ情報。

Backup Exec は、Backup Exec のメタデータやディスク上のカタログ・ファイルおよびディレクトリ情報を暗号化しません。バックアップ・ジョブに暗号化を伴うソフトウェア圧縮を使用することができます。最初に Backup Exec がファイルを圧縮してから暗号化します。ただし、暗号化圧縮とソフトウェア圧縮の両方を使用すると、バックアップ・ジョブの完了までに時間がかかります。

ベリタスでは、ソフトウェア暗号化でのハードウェア圧縮の使用を避けることをお勧めします。ハードウェア圧縮は暗号化後に実行されます。データは暗号化処理中にランダム化されます。圧縮は、ランダム化されたデータに対しては効果的に機能しません。

6. 連邦情報処理標準（FIPS）140-2 準拠のソフトウェア暗号化

Backup Exec では、FIPS 140-2 規格に準拠したソフトウェア暗号化を有効にすることができます。このオプションを選択した場合、256 ビット AES 暗号化キーを使用する必要があります。このオプションは Windows コンピュータでのみ使用可能です。

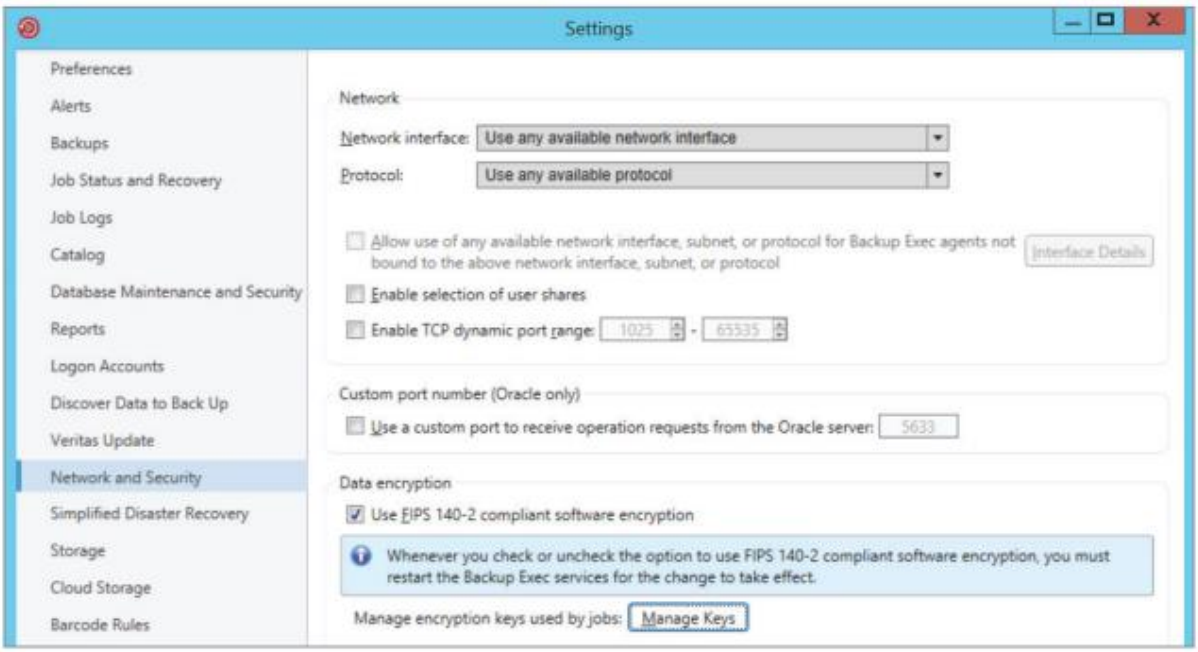

図 2：「ネットワークとセキュリティ」の FIPS 140-2 準拠ソフトウェア暗号化オプション

政府の一部の機関（米国および外国の両方）や政府と仕事をする請負業者（例：防衛省の請負業者）は、暗号が正しく実装されており、暗号が改ざんされていないことを保証する FIPS 140-2 を必要とすることがよくあります。

FIPS については以下の記事を参考にしてください。

http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf

図 3 に表示されているように、Veritas Backup Exec についてダイアログボックスで OpenSSL/FIPS バージョンを確認することができます。

7. ハードウェア暗号化

Backup Exec は、T10 暗号化標準を使用するストレージ・デバイスのハードウェア暗号化をサポートしています。ハードウェア暗号化を使用すると、データはホスト・コンピュータからストレージ・デバイスに転送され、デバイス上で暗号化されます。Backup Exec は、暗号化されたデータにアクセスするために使用される暗号化キーを管理します。

Backup Exec は、T10 暗号化のために承認されたデバイスのみをサポートしています。

対応機器の一覧は以下の URL で確認できます。https://www.veritas.com/support/en_US/article.000017788

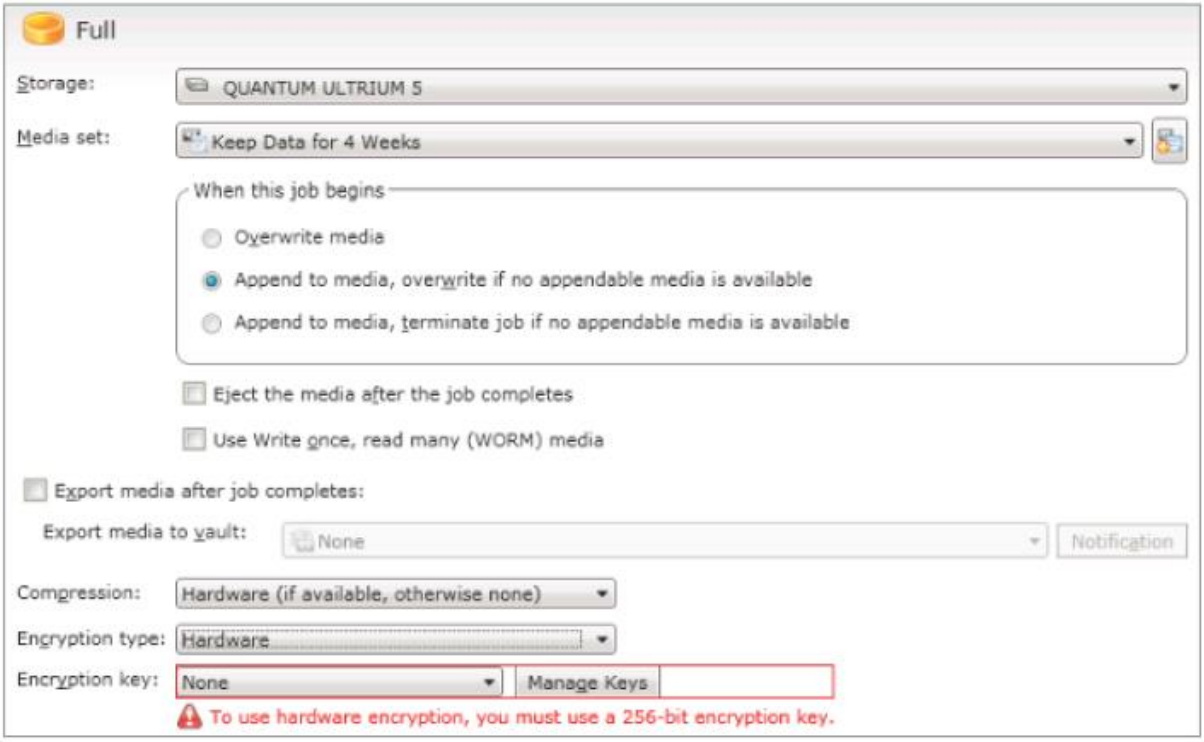

図 3：ハードウェア暗号化

注: T10 標準を使用するハードウェア暗号化には、256 ビット AES が必要です。Backup Exec では、少なくとも 16 文字のパスフレーズを使用しない限り、ジョブのハードウェア暗号化を有効にすることはできません。

8. 暗号化キー

Backup Exec で暗号化を使用するには、暗号化キーを作成する必要があります。ユーザが暗号化キーを作成すると、Backup Exec は、ログオンしたユーザのセキュリティ識別子に基づいた識別子でそのキーをマークします。キーを作成した人がキーの所有者になります。

合成バックアップに暗号化を使用する場合、関連するバックアップはすべて同じ暗号化キーを使用する必要があります。 ベースラインの作成後に暗号化キーを変更しないでください。 ベースライン バックアップに選択した暗号化キーは、関連するすべてのバックアップに自動的に適用されます。

復元のために暗号化されたデータを選択すると、Backup Exec は、データの暗号化キーがデータベースで利用可能であることを確認します。いずれかのキーが利用できない場合、Backup Exec は、不足しているキーを再作成するように促します。 ジョブの実行をスケジュールした後にキーを削除すると、ジョブは失敗します。

カタログ・ジョブの実行中に Backup Exec が暗号化キーを見つけられない場合、Backup Exec はアラートを送信します。パスフレーズがわかれば、不足している暗号化キーを再作成することができます。Simplified Disaster Recovery (SDR)は、以前に暗号化されたバックアップセットを使用したコンピュータのリカバリをサポートしています。バックアップ中に暗号化された Simplified Disaster Recovery バックアップがある場合、Recover This Computer ウィザードは、リカバリを完了するために必要な暗号化されたバックアップセットのパスフレーズを要求します。

9. 専用キーと共通キー

Backup Exec には、以下のような暗号化キーの種類があります。

暗号キーのタイプ	定義
Common	誰でもバックアップジョブ中にデータを暗号化し、暗号化されたデータを復元するためにキーを使用することができます。
Restricted	バックアップ・ジョブ中に誰でもキーを使用してデータを暗号化することができますが、キーの所有者以外のユーザはパス・フレーズを知っている必要があります。キーの所有者以外のユーザが暗号化されたデータを復元しようとすると、Backup Exec はパスフレーズの入力をユーザに促します。キーの正しいパスフレーズを提供できない場合、データをリストアすることはできません。

10. パスフレーズ

暗号化キーにはパスワードに似たパスフレーズが必要です。パスフレーズは通常、パスワードよりも長く、複数の単語またはテキストのグループで構成されます。良いパスフレーズは 8 文字から 128 文字の間です。128 ビット AES 暗号化の最小文字数は 8 文字です。256 ビット AES 暗号化の最小文字数は 16 文字です。ベリタスでは、最小文字数以上の文字を使用することをお勧めします。

注: T10 標準を使用するハードウェア暗号化には、256 ビット AES が必要です。Backup Exec では、少なくとも 16 文字のパスフレーズを使用しない限り、ジョブのハードウェア暗号化を有効にすることはできません。

また、良いパスフレーズには、大文字と小文字、数字、特殊文字の組み合わせが含まれています。パスフレーズに文学的な引用文を使用するのは避けるべきです。

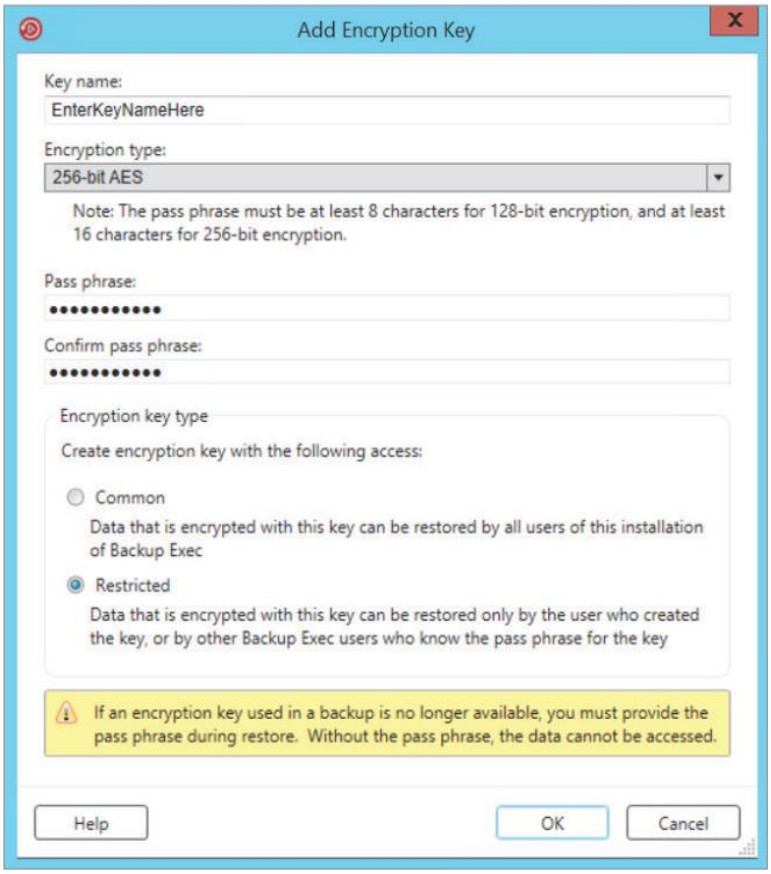

図 4：暗号化キーの追加

パスフレーズには、32～126 の文字である印刷可能な ASCII 文字のみを含めることができます。ASCII 文字 32 は、キーボードのスペースバーを使用して入力されるスペース文字です。ASCII 文字 33～126 には、次のものが含まれます。

! " # $ % & ' ( ) * + , - . / 0 1 2 3 4 5 6 7 8 9 : ; < = > ? @

ABCDEFGHIJKLMNOPQRSTUVWXYZ

[¥] ^ _ ‘abcdefghijklmnopqrstuvwxyz{|}

11. 暗号化キー管理

ユーザが暗号化キーを作成すると、Backup Exec は、ログオンしたユーザのセキュリティ識別子に基づいた識別子でそのキーをマークします。キーを作成した人がキーの所有者になります。

Backup Exec は、暗号化キーを Backup Exec データベースに保存します。ただし、Backup Exec はキーのパスフレーズを保存しません。各キーの所有者は、キーのパスフレーズを記憶する責任があります。

キーを保護するために、ベリタスでは以下を推奨しています。

- パスフレーズの文書化されたログを保管してください。暗号化されたバックアップセットとは別の物理的な安全な場所にログを保管してください。

- Backup Exec データベースをバックアップします。データベースはキーの記録を保持します。

注記：Backup Exec データベースのバックアップがなく、パスフレーズを覚えていない場合、暗号化されたメディアからデータを復元することはできません。また、ベリタスでは、このような状況で暗号化されたデータを復元することはできません。

Backup Exec サーバで作成されたキーは、その Backup Exec サーバに固有のものです。Backup Exec サーバ間でキーを移動することはできません。ただし、既存のパスフレーズを使用して、別の Backup Exec サーバに新しいキーを作成することはできます。パスフレーズは常に同じキーを生成します。また、誤ってキーを削除してしまった場合、パスフレーズを使用してキーを再作成することができます。

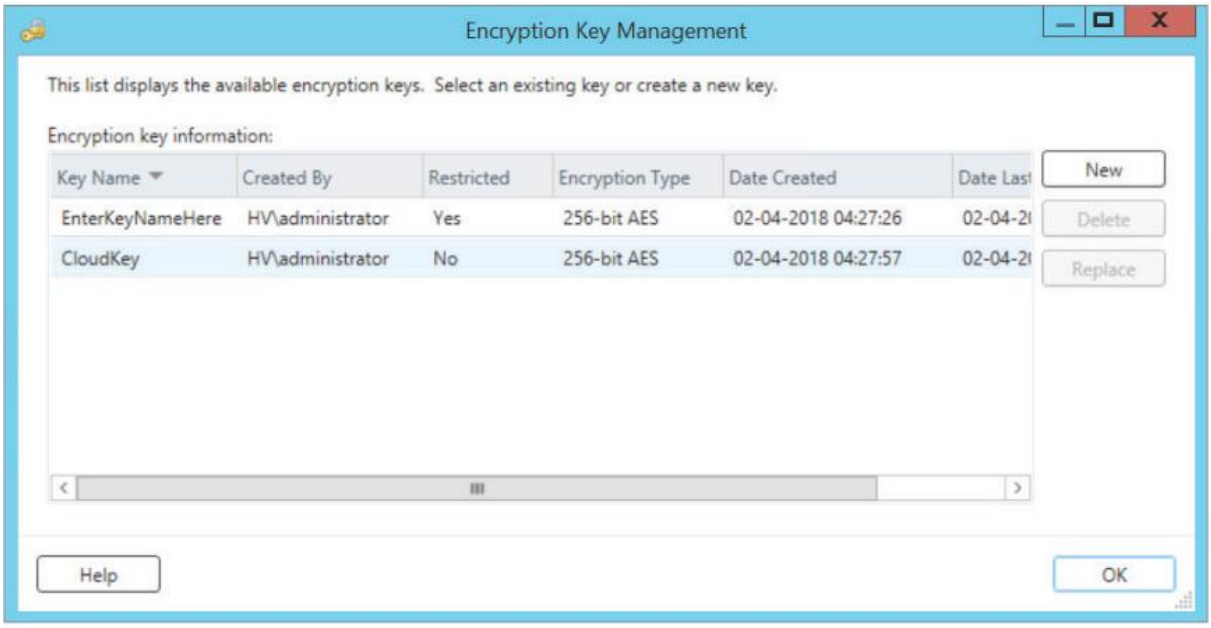

図 5：暗号化キーの管理

Backup Exec データベースが Backup Exec サーバ上で破損し、新しいデータベースに置き換えられた場合、元のデータベースに保存されていた暗号化キーをすべて手動で再作成する必要があります。

ある Backup Exec サーバから別の Backup Exec サーバにデータベースを移動した場合、新しい Backup Exec サーバが以下の基準を満たしている限り、暗号化キーはそのまま残ります。

- オリジナルの Backup Exec サーバと同じユーザ・アカウントを持っている。
- オリジナルの Backup Exec サーバと同じドメインにある。

12. 暗号キーの追跡変更

Backup Exec には、暗号化キーへの変更を含め、Backup Exec の設定に加えられたほとんどの構成変更を追跡するための包括的な監査ログ機能が含まれています。監査ログは、Backup Exec コンソールの [Tools/Audit Log]メニューから簡単にアクセスできます（図 5 を参照）。

Backup Exec Audit Log で追跡します。

- 新しい暗号化キーの作成
- 暗号化キーの削除
- 暗号化キーの変更
- 変更を行ったユーザーのユーザー名
- 変更日時
- 変更点の説明

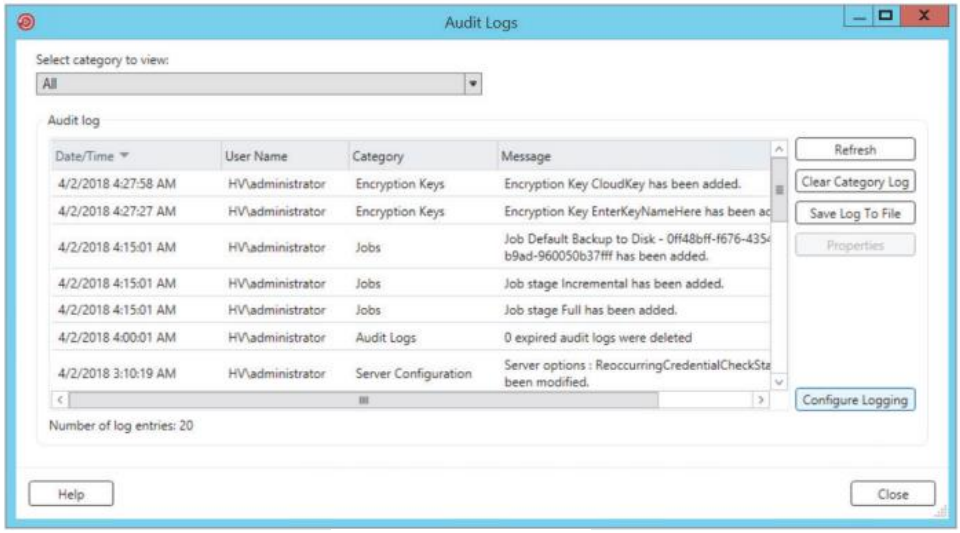

図 6：監査ログ

監査ログには、活動の日時、誰がそれを実行したか、何の活動だったか、活動の説明が表示されます。

13. Backup Exec データベース暗号キー

Backup Exec は、暗号化を使用して Backup Exec データベースに機密情報を保存します。Backup Exec をインストールまたはアップグレードすると、データベース暗号化キーが自動的に作成されます。データベース暗号化キーは、ログインアカウントのような情報を暗号化するために使用されます。

資格情報や暗号化されたバックアップ・ジョブに使用されるキーなどの情報が含まれています。これは、Backup Exec インストール ディレクトリの Data フォルダに保存されます。

図 7：ホーム画面のデータベース暗号化キー

以下の各シナリオで Backup Exec Database 暗号化キーを提供する必要があります。

- Backup Exec サーバの手動によるディザスタリカバリの実行
- Simplified Disaster Recovery(SDR)を使用した Backup Exec サーバのディザスターリカバリの実行
- あるコンピュータから別のコンピュータへの Backup Exec の移行
- Backup Exec サーバ上のデータベース暗号化キーが破損していたり、行方不明になってしまった場合の解決

ベリタスでは、必要に応じて後でアクセスできるように、Backup Exec データベース暗号化キーを安全な場所にエクスポートすることをお勧めします。データベースの暗号化キーを、以下の条件を満たす場所にエクスポートしてください。

- 宛先は、ドライブレターに割り当てられた物理ボリュームか、UNC パスで指定されたネットワーク共有のいずれかです。(ドライブ文字にマップされたネットワーク共有はサポートされていません)

- 宛先には十分なディスク容量があります。

- 宛先は、Backup Exec サーバからアクセスできます。

- Backup Exec は書き込み先への書き込み権限を持っています。

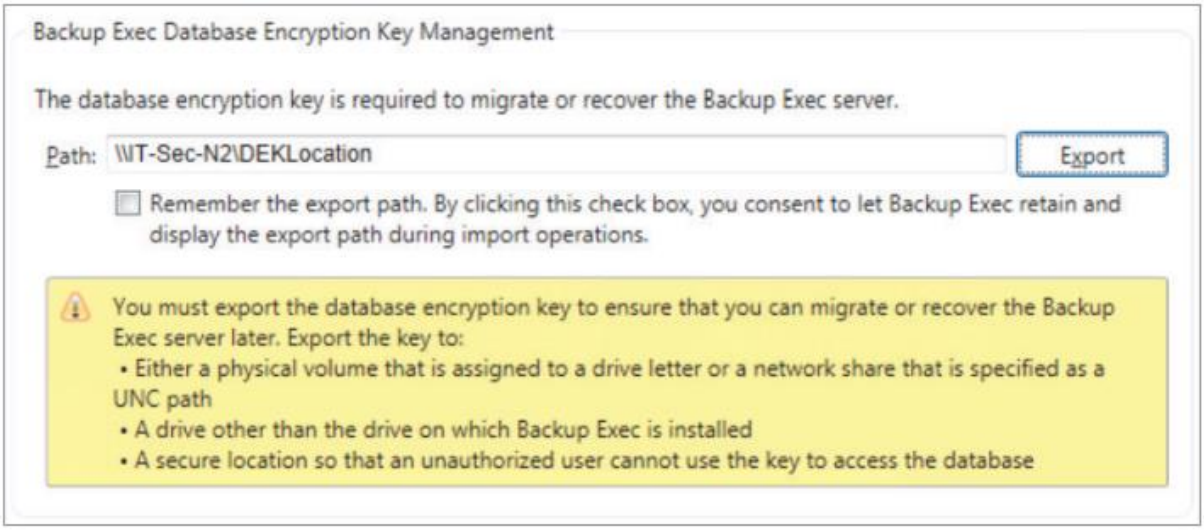

図 8：Backup Exec データベース暗号化キーの管理

14. Back Exec データベースへのセキュアな SQL 接続

Backup Exec データベースには、ユーザ・アカウントの資格情報やバックアップされたデータなど、組織に関する機密情報が含まれています。Microsoft SQL Server の Backup Exec データベースへの接続を保護することは、外部からのアクセスからネットワークを保護するための重要なステップです。Microsoft では、SQL Server とアプリケーション間で転送されるデータがネットワークを横断する際には、いつでも SSL 暗号化を使用することを推奨しています。

Backup Exec サービスと SQL インスタンス間のデータ転送は、以下のシナリオでネットワーク上を移動することができます。

- Backup Exec データベースを集中型データベースとして構成し、CASO 環境の中央管理サーバに配置します。管理された Backup Exec サーバを使用している場合や共有ストレージを使用している場合など、このシナリオのバリエーションでは、データはネットワークを横断して移動することもできます。
- Backup Exec サービスがネットワーク経由でデータベースにアクセスする必要があるように、Backup Exec データベースにリモート SQL インスタンスを使用します。

Backup Exec は、"BKUPEXEC "というデフォルトのローカル SQL Express インスタンスを使用している場合、自動的に SSL 暗号化を有効にします。他の SQL Server インスタンスを使用するように Backup Exec を構成する場合は、自分で暗号化を構成する必要があります。

SQL Server は証明書を使用してデータを暗号化します。独自の証明書を生成することもできますし、SQL Server に自動生成された自己署名証明書を使用させることもできます。デフォルトでは、Backup Exec は SQL Server が自動的に生成する自己署名証明書を使用します。ただし、ベリタスでは、セキュリティを高めるために独自の証明書を作成して使用することを推奨しています。

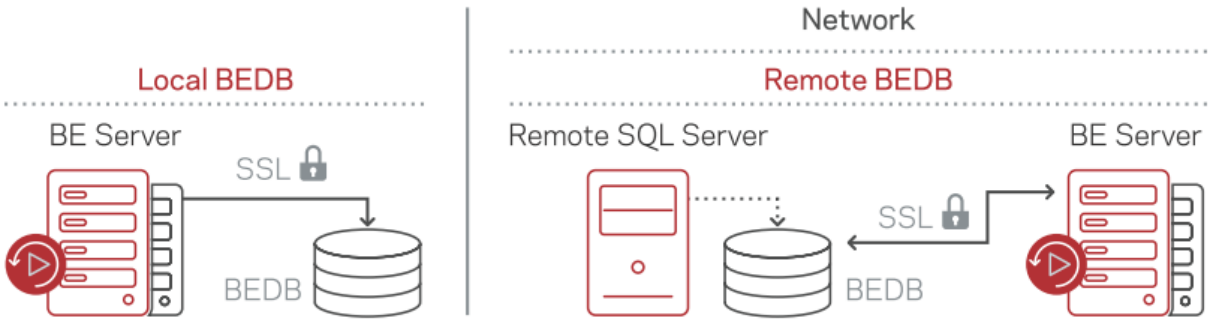

図 9: セキュアな SQL 接続

注記：暗号化を使用すると、SQL Server と Backup Exec Database 間の通信のパフォーマンスに影響を与える可能性があります。これには、データを暗号化して復号化するための時間だけでなく、ネットワークを横断する余分なラウンドトリップが必要になります。

Secure Sockets Layer（SSL）の詳細と SQL Server への接続の暗号化については、Microsoft のナレッジベースを参照してください。

Microsoft では、SQL Server で独自の証明書を使用する際には、必ず遵守しなければならない要件があります。証明書には、自己署名のものと認証局から発行されたものがあります。認証局は、 組織のドメイン内にあるローカルの認証局または既知のサードパーティの認証局のいずれかになります。

マイクロソフトの認定要件については、以下のマイクロソフトの記事を参照してください。

Encrypting Connections to SQL Server

暗号化を構成する前に、使用する証明書を Backup Exec Database をホストするコンピュータのローカル証明書ストアにインポートする必要があります。

サーバーに証明書をインポートしてインストールする方法については、以下のマイクロソフトの記事を参照してください。

How to: Enable Encrypted Connections to the Database Engine (SQL Server Configuration Manager)

証明書をインポートするときは、SQL Server サービスが実行されているのと同じユーザーアカウントを使用する必要があります。

15. SSL を利用したネットワークセキュリティ層

Backup Exec は、エージェントから Backup Exec サーバへの SSL サポートを提供し、WAN、パブリック・クラウド、またはプライベート・クラウドを介してバックアップ・データを送信する企業にセキュリティの追加レイヤーを提供します。追加されたセキュリティ機能により、パブリック・インターネット接続を介して送信されるバックアップ・データの安全性を確保することができます。

証明書は、リモート・エージェントと Backup Exec Media Servers 間の通信が WAN、LAN、またはその他のインターネットベースの接続で安全であることを保証するために、SSL と組み合わせて使用されるようになりました。

Backup Exec は、機密情報を交換する前に、Backup Exec リモート・エージェントと Backup Exec サーバ間の信頼関係を確立し、Man-in-The-Middle (MiTM)の問題を回避します。これにより、エージェントから Backup Exec サーバへネットワークを越えてデータを転送するリスクを最小限に抑えることができます。

MiTM を悪用すると、攻撃者が認証後の NDMP コマンドを実行できるように特権が拡大する可能性があります。悪用を成功させるためには、攻撃者がネットワーク上で認可されたユーザであるか、または、以下のシステム上で認可されたシステム上で認可されていない存在である必要があります。

Backup Exec は、Backup Exec サーバと保護されたサーバ上のエージェントとの間の NDMP を介した SSL 制御接続に Transport Layer Security (TLS) 1.2 プロトコルを使用します（Backup Exec サーバ、Agent for Windows、および Agent for Linux でサポートされています）。

セキュリティを強化するために、お客様は Backup Exec サーバとエージェント間の NDMP を介した制御接続を SSL で有効にするために強力な暗号を使用します。TLS 接続はセキュリティ・スキャナーとの連携が良く、お客様に Backup Exec の使用に対する継続的な信頼を提供します。TLS 1.2 は、暗号ブロック・チェイニングや CBC、RC4 の弱点になりにくい AES-GCM 暗号スイートをサポートしています。

また、Backup Exec では、Backup Exec Server と Agent の SSL 通信に SHA-2 証明書を使用していました。SHA-2 SSL 証明書は、Backup Exec Server、Central Admin Server、Managed Backup Exec Server、Agent for Windows、Agent for Linux でサポートされています。SHA-2 証明書は、より高いセキュリティレベルで即時のメリットを提供します。

本物の CA（費用がかかるベリサインなど）によって署名された中間証明書を使用するのとは対照的に、各 Backup Exe Server は、独自の認証局（CA）にすることができます。これは証明書に署名する機能を持ち、それをリモート・エージェントにデプロイすることができます。これらの証明書を使用して Backup Exec サーバとリモート・エージェント間の信頼が確立されると、Backup Exec サーバとリモート・エージェントが相互に通信するために使用する NDMP 接続に対する MITM(Man-In-The-Middle)攻撃を防ぐことができます。

16. 圧縮を用いた暗号化

バックアップ・ジョブにソフトウェア圧縮とソフトウェア暗号化を使用した場合、Backup Exec は最初にファイルを圧縮してから暗号化します。その結果、バックアップが遅くなります。

バックアップジョブにハードウェア圧縮とソフトウェア暗号化を使用した場合、データは暗号化されてから圧縮されます。暗号化によってデータがランダム化されるため、適切に圧縮することができません。ベリタスでは、ハードウェア圧縮と暗号化の併用は避けることをお勧めします。

17. バックアップ実行時の安全なコンソール管理

Secure Console Management は、Backup Exec User Interface コンソールのセキュリティを強化します。

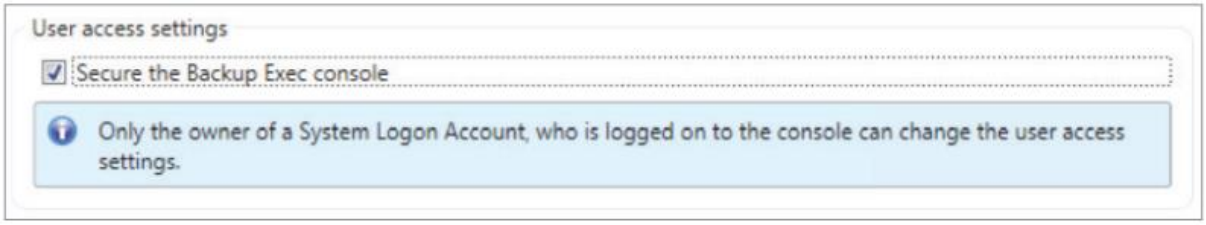

図 10：Backup Exec のセキュア・コンソール管理

Secure Console Management の一部として、Backup Exec が提供しています。

アイデンティティ認証

Secure Console Management チェックボックスを有効にすると、Identity Authentication が有効になります。これにより、BE ユーザ・インタフェースが起動したときに、Backup Exec が自動的に Windows ログイン・ユーザ・アカウントを使用してログインしようとすることはなくなりますが、代わりに、ユーザが Backup Exec コンソールにログインしようとするたびに、認証資格情報の入力が必要になります。

セッションロック

Secure Console Management チェックボックスを有効にすると、セッションロック機能が有効になります。

このため、BE User Interface セッションはロックされ、BE UI をロック解除するには再認証が必要になります。

18. ファイアウォールでのバックアップ実行

ファイアウォール環境では、Backup Exec は以下のようなメリットがあります。

- バックアップ・ネットワーク接続に使用されるポート数は最小限に抑えられています。
- Backup Exec サーバとリモート・システムのオープン・ポートは動的であり、ブラウジング、バックアップ、およびリストア操作時に高いレベルの柔軟性を提供します。
- 特定のファイアウォール ポート範囲を設定し、その範囲内でバックアップとリストアのネットワークを指定できます。特定の範囲を使用してデータ・トラフィックを分離し、高いレベルの信頼性を提供することができます。

20.1 リリースでは、Backup Exec は既存のインバウンド・ファイアウォール・ルールを強化し、必要なポートのみへのアクセスを提供し、それ以外のすべてのポートへのアクセスを制限するようになりました。これにより、セキュリティの失効や違反の可能性を最小限に抑えることができます。

19. ベストプラクティス

通常のベストプラクティスの一環として、ベリタスは強く推奨します。

- 管理システムまたは管理システムへのアクセスを特権ユーザーに制限する。
- 必要に応じて、リモートアクセスを信頼された/権限のあるシステムのみに制限する。
- 脅威による悪用の影響を制限するために、可能な限り最小の特権の原則の下で実行する。
- すべてのオペレーティングシステムとアプリケーションを最新のベンダーパッチで更新する。

- セキュリティに対する多層的なアプローチに従う。ファイアウォールとマルウェア対策アプリケーションの両方を最低でも実行し、複数のセキュリティ対策を行う。インバウンドとアウトバウンドの両方の脅威を検知し、保護するポイントを提供します。
- ネットワークおよびホストベースの侵入検知システムを導入して、ネットワークトラフィックを監視して、異常または不審な アクティビティを検出することができます。これは、潜在的な脆弱性の悪用に関連する攻撃や悪意のある活動の検出に役立つ可能性があります。
- 以下のようなことをして、強いパスフレーズを作りましょう。
    - 必要最低限の文字数以上の文字を使用してください。
    - 大文字と小文字、数字、特殊文字を組み合わせて使用してください。
    - パスフレーズには、文学的な引用は避けましょう。
    - パスフレーズは安全に保管しましょう。
- FIPS モードで Backup Exec Services を実行し、256 ビットの AES 暗号化を使用して FIPS に準拠します。
- ディスクベースのストレージにデータをバックアップする際にソフトウェアの暗号化を使用しない場合は、不正アクセスを防ぐためにファイルシステムの暗号化を使用します。

20. ベリタスへの脆弱性報告

ベリタスは、製品のセキュリティと適切な機能性を非常に重視しています。ベリタステクノロジーズは、安全なソフトウェア開発に対する積極的なアプローチを堅持しており、ソフトウェア開発プロセスのさまざまな段階でセキュリティレビューを実施しています。

さらに、ベリタスは製品やサービスのセキュリティだけでなく、お客様のデータのセキュリティにも力を入れています。ベリタスは、ソフトウェアセキュリティプロセスの継続的な改善に努めています。

このドキュメントでは、Veritas Backup Exec のセキュリティ機能と暗号化機能の概要を説明します。このドキュメントは以下を目的としています。これは要約であり、Backup Exec ソフトウェアのセキュリティおよび暗号化機能の包括的なリストではありません。

Backup Exec またはその他の Veritas 製品でセキュリティの問題が発見されたと思われる場合は、Veritas 認定リセラー/パートナーまたは Veritas テクニカルサポートにお問い合わせください。

21. サマリ

Backup Exec が提供する新しい暗号化とセキュリティ機能により、企業の重要かつ機密性の高いデータを、不正アクセスやセキュリティ上の脅威から安全な形式で簡単に保護することができます。128/256 ビット AES OpenSSL 暗号化による産業用の強力な暗号化機能と、Backup Exec ソフトウェアの使いやすさと柔軟な実装を組み合わせることで、必要な時に必要な場所で暗号化を行うことができます。

22. 詳細はこちら

Backup Exec web page	www.backupexec.com
Backup Exec admin guide	www.backupexec.com/admin
Backup Exec resources	www.backupexec.com/resources
Backup Exec compatibility	www.backupexec.com/compatibility
Backup Exec support	www.backupexec.com/support
Backup Exec training	www.backupexec.com/training
Backup Exec user forum	www.backupexec.com/forum

Backup Exec blogs	www.backupexec.com/blogs
60-day trialware for Backup Exec	www.backupexec.com/trybe
Backup Exec subscription	www.backupexec.com/subscription
Backup Exec promotions	www.backupexec.com/save
PartnerNet	https://partnernet.veritas.com/
Find a Backup Exec Partner	http://veritas.force.com/public

ベリタステクノロジーズについて

Veritas Technologies はエンタープライズデータ管理のグローバルリーダーです。複雑化した IT 環境においてデータ管理の簡素化を実現するために、世界の先進企業 50,000 社以上、Fortune 500 企業の 90 パーセントが、ベリタスのソリューションを導入しています。ベリタスのエンタープライズ・データサービス・プラットフォームは、お客様のデータ活用を推進するため、データ保護の自動化とデータリカバリを実現して、ビジネスに不可欠なアプリケーションの可用性を確保し、複雑化するデータ規制対応に必要なインサイトを提供します。ベリタスのソリューションは信頼性とスケーラビリティに優れ、500 以上のデータソースと 50 のクラウドを含む 150 以上のストレージ環境に対応しています。

VERITAS
The truth in information.

ベリタステクノロジーズ合同会社

https://www.veritas.com/ja/jp
〒107-0052 東京都港区赤坂 1-11-44 赤坂インターシティ 4F
ベリタスセールスインフォメーションセンター（法人のお客様向け製品購入に関する相談窓口）
■電話受付時間：10:00 ~ 12:00, 13:00 ~ 17:00 （土、日、祝日、年末年始を除く）
■電話番号：0120-99-000 （IP 電話からは 03-4531-1799）

© 2020 Veritas Technologies LLC. All rights reserved. Veritas および Veritas のロゴは、米国およびその他の国における Veritas Technologies LLC またはその関連会社の商標または登録商標です。その他の名称は、それぞれの所有者の商標である場合があります。