エンドポイント暗号化テクノロジーの選択方法

TechCenter

目次

－承諾依頼－

本資料はTechCenter のために作成された一般的な設定紹介の参考資料です。
この資料に基づいて設定いただく前にTechCenterに記載の、以下サポートに関する記載に同意してご活用下さい。
http://ja.community.dell.com/techcenter/other-dell-related/

以下TechCenter より抜粋
Dell テックセンターのサイトへようこそ。このサイトは、Dell のユーザの皆様に技術的な事柄についてディスカッションや情報交換をしていただくサイトです。皆様のディスカッションが進むようにデルの方からも資料を提供させていただきますが正式な製品のサポートに関してはこのサイトの下部のサポートサイトへご連絡ください (サポートチームでは Twitter で最新サポート情報を提供しております。こちらもよろしくお願いします)。デルは、本サイトの内容の真実性や有効性について責任を有するものではございませんので、ユーザの皆様にてご判断いただきますようお願いします。なお製品購入に関するご質問は下記のバナーをクリックしてお問い合わせください。弊社の担当者よりご連絡させていただきます。

エンドポイント暗号化テクノロジーの選択方法

はじめに

今日、非常に多くのベンダーがエンドポイント暗号化ソリューションを提供しています。多くの企業のIT担当者は、どのソリューションを選択するのが最適なのか、判断することが非常に困難な状況となっています。このホワイトペーパーでは代表的な暗号化テクノロジーについて解説し、どのテクノロジーを導入するのが最良の選択であるかをガイドし、それぞれについてベネフィットあるいは注意点について説明します。DELLが提供するDell Data Protection | Encryption により、非常に高度なデータ保護を実現するとともに、性能あるいはコストに対するインパクトを最小限に抑えられます。

今日の暗号化テクノロジーは大きく分けて以下の３つに分類することができます。

- ソフトウェアフルディスク暗号化
- データセントリック暗号化
- 自己暗号化ドライブ

このホワイトペーパーではハイレベルでの、それぞれの暗号化テクノロジーの特徴、動作を説明し、これにより選択をする上でのガイドラインを提供します。どのテクノロジーの採用が貴社にとって最適か、判断できるようになります。

ソフトウェアフルディスク暗号化（FDE）の実装方法と課題

ソフトウェアフルディスク暗号化（FDE：Full Disk Encryption）はハードディスクの全てのセクターを暗号化します。ただし、ブートプロセスに必要な重要ファイルについてはこの暗号化の対象外となります。多くのバージョンのテクノロジーが存在します。最終的な目標は許可されないユーザからデータを護るということです。
FDEの実装はIBMオリジナルPCのころから続いているPCの起動方法に依存しています。BIOSに依存しない方法で起動するために、マスターブートレコード（MBR）がアクティブなブータブルディスクの“サイド－トラック－セクター”で指定される場所に存在し、トラディショナルなBIOSブートを起動しなければなりません。
このMBR（ドライブの512バイトのセクター）はブートローダを起動します。制御がブートローダに渡ると、カーネルがロードされ、ファイルシステムマネージャがロードされます。さらに、基本的なデバイスドライバーのセットがアクティブ状態になり、ユーザインターフェイスデバイスが利用可能な状態となります。

実装方法

実装方法は様々ですが、ブートローダにより起動される時点で暗号化の処理は始まっています。これは、大半の実装において、MBRには暗号化されていない部分が存在するということを意味しています。しかしながら、ブートドライブにおける暗号化されていない部分の大きさは実装方式により異なります。
一般的には、ソフトウェアベースのFDEインプリメンテーションはRTOS（リアルタイムオペレーティングシステム）の一部として、Linux OSを起動することで、ブート処理のカスタマイズを実現し、攻撃の対象となるリスクを低減しています。しかしながら、ブートの方法自体は変化しているわけではありません。ユーザの使用するOSのマスターブートレコードは暗号化のためのOSのマスターブートレコードで置き換えられます。起動に必要となるMBRの条件はユーザOSのMBRと違いがありません。暗号化のためのOSを起動し、暗号化されたユーザOSを起動します。
ユーザOSが起動すると、暗号化のためのOSはユーザOSから見るとフィルタとしての機能を果たします。つまり、システムストレージトランザクションをインターセプトし、暗号化あるいは復号化の要求を処理し、ユーザOSにデータを渡します。
また、ユーザOSのAPI、カーネルコンポーネント、ドライバーにフックを仕掛けるという方法をとっている暗号化製品も存在します。

OS起動時の暗号化の方式

OS起動時の暗号化の方式には様々な実装方法があります。大半のものはバックグラウンドタスクとして非常に軽い処理として暗号化処理を行います。ソフトウェアベースのFDEは通常、ドライブの100%を暗号化しますが、ブート処理に必要な部分は暗号化しません。パーティションを意識するような実装をしているベンダーは非常に稀です。そのため、複数OSのサポートが必要とされる場合にはFDEソリューションが複数OSをサポートしているかを確認する必要があります。また、インストール順序に制約があることもしばしばあります。

暗号化が有効になっている場合に、いくつかのFDEソリューションではデータが破損に対応するためのウィンドウが非常に小さいとことがあります。典型的な暗号化の順序で言えば、最初にプログレステーブルを作成します。エンクリプションプロセスは暗号化されていないセクターを読み込み、暗号化して、セクターに書き戻します。そして、ファイルシステムのリンクを更新します。最後にプログレステーブルを更新します。これらの一連の処理をディスクの最終セクターに達するまで行います。もし、システムが使用中でない場合には、セクターの読み込み、書き込みは、プログレスマークの暗号化が必要なセクターに対して行われ、コンペアされます。ベンダーの破損ウィンドウは、ベンダー独自の破損率を低減させる方式により様々です。ベストプラクティスは暗号化を有効にし、初期暗号化をシステムが使用されない時間帯にスケジュールし、１回のセッションで完了することです。

有益なソリューションとして、バンドルされることが多いのは、指紋、スマートカード、多要素、顔認証などの一般的にOS外の機能として提供されないユーザ認証機能です。FDEソリューションを選択する場合には、認証および認証エラーのリカバリーおよびマイグレーション、パスワード忘れ、アクセストークンの紛失などに対応するための管理ツールについて検討するべきです。

FDEソリューションの課題

FDEソリューションはユーザOSの管理を難しくすることがあります。FDEソフトウェアにより、ユーザOSを管理するように設定する必要があります。FDEの管理インターフェイスは通常はベンダー独自のものであり、大半のケースでは個別のコンソールが必要となります。リカバリーあるいはマイグレーションはFDEが業界標準の技術でないために、独自の実装がされています。暗号鍵の管理はインプリメンテーションによって異なり、特定のエンタープライズキー管理アーキテクチャをサポートしているものと、そうでないものがあります。

また、ユーザによるハードディスクのデフラグを実行することが推奨されます。チェックディスクを複数回実行することでスムーズな導入ができます。

データセントリック暗号化

データセントリック暗号化はFDEとは異なり、ユーザファイルおよびフォルダーのみを暗号化します。アプリケーションおよびOSそのものは暗号化されません。このように、コンセプトは非常にシンプルですが、実装は簡単ではありません。アプリケーションによって作られる一時ファイル、フォルダーのコピー＆ペースト、バックアップファイル、ページファイル、スワップファイルなどが暗号化されないと、ユーザデータを護ることができません。

データセントリック暗号化はFDEにない魅力的な機能を持っています。柔軟なキー管理ポリシーが定義できます。暗号鍵はファイルがオープンされている間は、メモリに残っている必要があります。ファイルが閉じられたら、廃棄されなくてはいけません。ファイルがセカンダリードライブにバックアップされたら、ファイルは直ちに暗号化されなければいけません。

データセントリック暗号化のドライブは性能的にはソフトウェアベースのFDEソリューションよりも高速です。データセントリック暗号化ドライブの管理は簡略化されており、追加のOSの暗号化機能や認証アプリケーションを導入する必要はありません。データセントリック暗号化ソリューションの認証はOS標準の機能であることが多く、暗号化の処理はバックグラウンドで実行されます。FDEとは異なり、ユーザファイル、データが割り当てられたセクターのみが暗号化されます。データの格納に使用されていないセクターが暗号化されることはありません。ファイルシステムテーブルは暗号化されていないので、ファイルおよびフォルダーが破損する可能性はFDEに比べると低く、復旧も大きな問題に発展する前に解消されることがほとんどです。
データセントリック暗号化では、リムーバブルメディアの保護を行うこともできます。

自己暗号化ドライブ（SED）

自己暗号化ドライブは暗号化機能が実装されたストレージデバイスです。内蔵された暗号化アクセラレータにより暗号化が行われます。標準的な規格としては、TCGの定めたOpal Security Subsystem Class Specification 2.0があります。このデバイスは標準SATAまたはOpalインターフェイスをサポートします。暗号化モードが有効になっている状態では、ドライブは異なるパスを使用します。一度、アンロックされると、インターフェイスは標準SATAとなります。OPAL標準は128/256bit AED暗号化をサポートします。暗号鍵はドライブの内部チップに保存され、取り出すことはできません。

SEDを有効にするには、ドライブにコマンドを送る必要があります。これにより、ドライブが暗号化モードになります。小さなパーティションがドライブに作成され、ブートコードが格納され利用可能な状態になります。このコードによってユーザが認証されます。セットアップの際には、ベンダー独自のソフトウェアがロードされます。これにより、リモートあるいはローカル管理コンソールで暗号化ポリシー、認証機能の管理を行うことができるようになります。OPALではブートコードのインターフェイスを定義していません。定義しているのは、ブートコードとドライバーのインターフェイスです。BIOSブートの際にはベンダーのSEDブートコードとBIOS間のコミュニケーションのみが行われます。BIOSとOSのマスターブートレコード間のコミュニケーションは発生しません。ブートコードはユーザとドライブとの認証をします。その後、通常のブートオペレーションに移行します。一般的には、SEDドライブでハードウェア暗号化を使用する場合にはパフォーマンス劣化は発生しません。

暗号鍵をドライブに格納しないので、キーのバックアップは存在しません。認証情報バックアップは暗号鍵のバックアップの代わりに使用され、リストアツールでSED認証に関する一連の処理をリカバリーできます。リストアツールの機能、方法、管理、手順等はSEDの管理機能を提供しているベンダーに依存します。SEDの現在のコマンドは非常にセキュリティを考慮した厳格なものになっています。

暗号化監査の機能

どの暗号化手法を選んだとしても、監査機能はマネージメントコンソールにて提供される機能です。法律にて定められている（個人情報保護法など）場合には、該当する団体・企業はその定めるところに従い、情報を保護する施策を実施すると同時に、その対応状況を確認できる仕掛けを持っている必要があります。管理コンソールの重要な機能として、管理データベースにアクセスして、特定の護るべきデータが暗号化されていることを確認できるということです。

Dell Data Protection | Encryption

デルはDell Data Protection | Encryption（DDP|E）という暗号化ソリューションを提供しています。これは、ファイルベースの暗号化をするものです。フルディスク暗号化で提供するのと同等の暗号化機能をファイルベースの機能として提供します。DDP|EはマイクロソフトWindowsの認証機能を使用しており、プリブート認証等のオーバーヘッドを掛けることがありません。また、OSを起動するために必要なWindowsのファイルは暗号化しません。他の暗号化ソフトはこれらのWindows OSファイルも暗号化しています。これは、プリブート認証のような特別な仕掛けを追加する必要がないということです。さらに、既存のWindowsの管理体系をAdministratorの特権管理を踏襲するために、パッチ管理が容易に行えるというメリットもあります。

一方、自己暗号化ドライブ（SED）を使用する場合には、認証処理は通常のWindowsの認証とは別に行う必要があります。この機能はデルが独自にBIOSに組み込んだものを使用します。具体的には、Dell Data Protection | Security Toolsという製品です。デルはパスワードによる単純な認証だけでなく、トークン、バイオメトリックデバイスなどを利用できるソリューションを提供します。これらの設定はWindows上でウィザードにより簡単に行うことができ、セットアップ、プロセスの有効化、さらに、リモート管理もできます。トークンおよびバイオメトリックデバイスを使用して、BIOSからWindowsにログインすることができます。（シングルサインオン）
もちろん、設定によって、シングルサインオンではなく、多層認証として使用することもできます。

DDP|EはハイブリッドなソフトウェアベースのデータセントリックなFDEモデルを提供します。このモデルでは２セットのキーを使用します。共通キーはOSを保護するためのキー、ユニークキーはエンドユーザデータを護るキーです。IT部門の方は、共通キーを保有していればOSの管理業務（パッチの適用、OSの障害対応など）をユーザデータが漏洩する危険がない状態で行うことができます。エンドユーザの認証により、この２つのキーが提供され、システム、データにアクセスできる状態になります。

このハイブリッドモデルにより、OSの管理、アプリケーションの管理を特殊な暗号管理を意識せずに行うことができます。暗号化ドライブが別のシステムにセカンドドライブとしてアタッチされると、ブートファイル以外のデータは保護されます。これは、動作としては、FDEと全く同様の動作です。 2 階層のセキュリティレイヤーを提供しています。共通キーが盗まれた場合にも、ユーザデータは別のユニークキーで護られています。このユニークキーはユーザ毎に異なるキーなので、システム上に複数ユーザのデータが存在する場合にはそれぞれ別のキーにより解読する必要があります。システムのパフォーマンスはソフトウェアフルディスク暗号化と同等以上です。（これは、Intel AES-NIテクノロジーにより、AES暗号化の高速化が実現できたことによります。）マネージメントコンソールの高度なオプションにより、ポリシーの作成、適用を容易に行うことができます。

データセントリック暗号化、DDP|Eによりファイルを暗号化しますが、FDEとは異なり、必要のない空のセクターを暗号化にシステムリソース、時間を消費しません。セクターが使用されると暗号化が実行されます。また、削除ファイルがセクターに残っている場合、暗号化された状態を維持します。性能面でも従来はファイルの暗号化はCPUへの負荷が高く、ユーザビリティの低下があることから敬遠されることの多いソリューションでしたが、AES-NIテクノロジーの導入によりデファクトであるAES（DDP|Eでは鍵長は128または256ビットを選択可能）が非常に高速に動作し、システムへの負担が少ない。ベンダーによってはAESの鍵長を128ビットに固定し、性能への影響を軽減していることからも、このテクノロジーの有効性はあきらかである。
データ保護の要件が非常に厳しい場合には、ドライブにある全てのデータの暗号化（MBRを除く）を管理コンソールから選択することができます。デフォルトではファクトリーリカバリーパーティション、ダイアグパーティションは暗号化の対象になっていません。これに関しても、必要があれば暗号化対象にすることができます。

ファイルベースの暗号化に関して、多くの方が誤解されているのは、ユーザの操作が暗号化に必要であるという点です。DDP|Eではエンドユーザが暗号化にかかわる必要はありません。恐らく、導入後はDDP|Eの存在を全く意識することなく、業務を行えるはずです。Windowsがデータのアクセス、作成というリクエストを送ると、そのリクエストはフィルタに転送されます。これはポリシーを適用されたレイヤーです。これにより、データを含む全てのファイルタイプが暗号化されます。これには、ソースファイル、アプリケーションによって作られた一時ファイル、コピー＆ペーストされたファイル、ファイルプリントのデータ、スクリーンコピー＆ペースト、バックアップファイル、ページ、スワップファイルを含みます。

システムディスクの保護に加えて、DDP|Eはリムーバブルメディアの暗号化機能も提供します。Windowsがドライブを付けて管理する光学ドライブを含む全てのドライブを管理できます。この機能によって、リムーバブルメディアのポリシーによる管理機能を提供します。

- 共用する場合のパスワード必須化、およびパスワード強度設定
- ロックするまでのパスワード試行回数
- メディアの共用不可設定
- 暗号化設定のためのメディアスキャン
- リードオンリーのポリシー設定
- 暗号化ステータスの監査

Hardware Crypto Accelerator(略称:HCA)

最高レベルでのパフォーマンスを要求するユーザ層に対しては、DDP|Eはデルが開発したハードウェア暗号化アクセラレータを提供します。これは、MBRを含む、ストレージデバイスの全セクターを暗号化します。暗号鍵は2重に保護され、OSからは見えないようになっています。保護はBIOSでユーザ認証が完了した時点から開始されます。ユーザ認証が成功すると、保護された認証キーコンテナがテストされ、ハードウェア認証がされます。このテストが成功すると、暗号鍵はハードウェア暗号化アクセラレータで認証されます。認証が完了して、アクセラレータが有効になると、全ての暗号化処理はこのアクセラレータを利用します。

コンプライアンスは多くの企業にとって、とても重要です。DDP|Eではテンプレートを提供することにより、容易にコンプライアンスを実現します。この機能はポリシーをデザインする専門の方がいない企業でも非常に少ない作業時間で作業が可能です。ポリシー設定になれたエンジニアがいる企業においては、ポリシーテンプレートにより短時間で導入した後に、カスタマイズすることもできます。保護のレベルは以下の通りです。

DDP|Eで提供する保護レベル

- システムの基本的な保護（固定およびリムーバブルドライブ）：共通キーにより全てまたは一部の固定ドライブ、システムドライブを暗号化し、リムーバブルメディアを使用する際にはパスワードを設定
- 全てのドライブを強力に護る：アプリケーション、データをユーザキーで暗号化する
- HIPPA テンプレート：HIPPA(Health Insurance portability and Accountability Act)に対応したテンプレート、ヘルスケア業界で有効な基本的なテンプレートを提供。全ての固定ドライブはSDE（システムデータ暗号化）ポリシーにて暗号化、アプリケーション、ユーザデータは共通キーで暗号化する。リムーバブルストレージのポリシーも含んでいます。
- Data Breach Regulatory: Sarbanes-Oxley Act(SOX)で、ファイナンシャル情報の保護を規定している。多くのファイナンシャル情報は電子化されているために、データの保管、転送時に暗号化するということはキーとなるポイントである。Gramm-Leach-Bliley(GLB)ではガイドラインとして暗号化までは要求していないが、FFIEC（Financial Institutions Examination Council）では暗号化を推奨している。FFIECでは重要情報の保管、転送時は情報漏洩のリスクを減らすためにデータの暗号化を必須としている。このテンプレートでは固定ドライブはシステムデータ暗号化（SDE）ポリシーにより暗号化し、ユーザデータは共通キーで暗号化する。リムーバブルストレージのポリシーも含んでいます。
- PCI Data セキュリティ標準：ペイメントカード業界の標準的なセキュリティ規格（PCI DSS）では多角的なセキュリティ標準であり、以下を含んでいます。セキュリティの管理、ポリシー管理、プロシジャ、ネットワークアーキテクチャ、ソフトウェアデザイン、その他のクリティカルな保護のための指針。この高度なセキュリティ標準規格は企業において積極的に顧客アカウント情報を護るということを意図して作られたものです。全ての固定ドライブはSDE（System Data Encryption）ポリシーで暗号化されます。アプリケーションおよびユーザデータは共通キーで護られます。このテンプレートはリムーバブルストレージのポリシーを含みます。

デルの法人向けクライアントPC及びワークステーションでは、この最も強固なセキュリティ、FIPS 140-2、レベル3準拠を実現する、HCAをオプションで提供しています。

DDP | Hardware Crypto Acceleratorは、以下の仕様を満たす一部のDell Precision™、Latitude、OptiPlexのシステムでご利用いただけます。

サポート対象のオペレーティングシステム:

- Microsoft Windows 7 Ultimate/Enterprise/Professional
- Microsoft Windows XP Professional
- Microsoft Windows 8/8.1 （ダウングレード権を含む）

暗号化アルゴリズム:

- AES Rijndael Block Cipher
- Triple DES
- 関連HMACを使用するSHA-256、SHA-384、SHA-512

Latitudeファミリー

OptiPlexファミリー

Dell Precision™ファミリー

ソリューションの選択方法　まとめ

今日、お客様において選択できるソリューションの全てについて説明してまいりました。重要な顧客データの管理、リムーバブルメディアの使用などを考慮し、最適なソリューションを選択することになります。

最後に、検討にあたって重要な５つの指針についてご説明します。

レガシーシステムサポート：貴社におけるラップトップがどの構成をサポートしているのかを確認する必要があります。ファイルおよびフォルダーを暗号化するFDEは新しいPCでも古いPCでも動作します。SEDを選択する場合には注意が必要です。恐らく、大半の企業ではSEDドライブのPCとソフトウェアベースのFDEが混在することになると思います。したがって、２つの異なるソリューションを導入することになります。

ディプロイメント：ディプロイメントの容易性についても検討が必要です。FDEでは多くのベンダーはチェックディスクおよびデフラグを実施することで、システムエラーやディプロイの予期せぬ停止を防ぐことを推奨します。ファイベースのソリューション（DDP|E）の場合にはエージェントをインストールし、ポリシーを適用するだけであり、とても簡単にできます。

リムーバブルメディア：FDE, SEDのソリューションにおいては別途リムーバブルメディアの制御をするソフトウェアの購入が必要となります。このソリューションを導入しないことのリスクは非常に大きなものとなります。DDP|EではシステムドライブとリムーバブルドライブをまとめてProtectすることができます。

フレキシビリティ：一般的にはFDE、SED暗号化ポリシーでは暗号化をするか、しないかを選択、ファイルベースソリューション（DDP|E）ではより多くのオプションがあります。これは、ユーザの特性、データの重要性などにより決まります。同様の柔軟性はリムーバブルメディアに対しても適用できます。

管理、監査の機能：使用するツールが高度な管理機能、レポーティング、ポリシー管理を持っているかにより、どのようなセキュリティポリシーを実装でき、管理、監査ができるかが決定します。同時に、パッチ管理、認証などの代替ソリューションにより対応できる部分はないか慎重に評価をします。

ソリューションの選択によって、ビジネスプロセスを変更する必要があるかもしれません。
DDP|Eでは、現状の運用とまったく変わらない運用で導入・適用を実現できます。

貴社にとって最適なエンドポイント暗号化ソリューションをご選択いただく上で、本ガイドがお役にたてれば幸いです。
是非、ご検討ください。よろしくお願いいたします。

デル TechCenter

MEMO

デル TechCenter

DDP｜E 暗号化を含むDDPソリューションのご紹介は以下URLにて。
Dell.jp/ddp

デル 東京オフィスでDDPのデモを体験いただけます。

弊社三田の東京オフィスでは、お客様のご要望に応じて、
DDP｜E 暗号化を含むDDPソリューションのデモをご覧いただけます。
詳しくは弊社営業までお問い合わせください。