KASPERSKY lab

暗号化の実践的導入

www.kaspersky.co.jp

暗号化の実践的導入の手引き

プロアクティブなデータ保護は、ビジネスにおける喫緊の課題です。カスペルスキーは、データの暗号化と保護に関連するベストプラクティスの実践を支援しています。

暗号化に関するビジネスケース

2005 年以降に漏洩した情報数は、**8 億 1,600 万件**以上です。[1]2015 年の最初の 4か月間だけでも、**1 億 100 万件**の情報が漏洩しました。[2]

大規模な情報漏洩は、ほぼ毎週のように大きなニュースになっています。Identity Theft Resource Center は、2014 年を「データ侵害の年」と名付け、データ紛失と情報漏洩の 2 大要因として、モバイルデバイスやリムーバブルデバイスへのデータの保管と、従業員による機密データへの不正アクセスに起因する内部侵害を挙げました。[3]カスペルスキーが調査した企業の約20%が、デバイスの盗難が直接の原因で、データ紛失の被害に遭っています。[4]

カスペルスキーの調査から、2014 年に発生したデータ紛失インシデントの平均被害額は、大企業で **636,000 ドル**、中小企業で **33,000 ドル**にのぼることがわかりました。[5]デバイスを物理的に紛失しなくても、機密データの紛失は発生します。ビジネス上の機密情報や知的財産が、マルウェア攻撃の主なターゲットとなっています。

問題は、侵害による直接的な損失や得意客の喪失、会社の信用の低下（72% の企業がインシデントの公表を余儀なくされました[6]）だけではありません。主要国の多くで、データセキュリティとプライバシーに関する法律が定められ、多くの管轄組織が機密データの暗号化を企業に義務付けるようになりました。

日本における個人情報保護法、米国のHIPAAやSOX、英国のData Prevention Act、EUのData Protection Directiveなど、世界各国の当局が機密データのプロアクティブな保護を企業に求めるようになっています。たとえば英国では、情報コミッショナー（ICO）が、「暗号化によってデータが保護されていない場所」で発生したデータ紛失には規制措置をとる可能性があると発表しました。

ノートPCの盗難、ストレージデバイスの紛失、あるいはマルウェアによるデータの盗難といった問題に直面しても、暗号化を行っていれば、犯罪者や不正な閲覧者にとって機密データは利用が非常に難しくなります。

それでは、暗号化の実践的な導入方法とはどのようなものでしょうか。

1 Privacy Rights Clearing House:http://www.privacyrights.org/data-breach
2 Identity Theft Resource Center 2015:http://www.idtheftcenter.org/images/breach/ITRCBreachStatsReport2015.pdf
3 Identity Theft Resource Center 2015:http://www.idtheftcenter.org/Press-Releases/2014breachstatistics.html
4 Kaspersky Lab:2014 IT Security Risks Report
5 Kaspersky Lab:2014 IT Security Risks Report
6 Kaspersky Lab:2014 IT Security Risks Report

暗号化の実践的な導入方法

カスペルスキーの暗号化テクノロジーは、偶発的な紛失や、デバイスの盗難、標的型攻撃によるマルウェアなどの攻撃から貴重なデータを保護します。

1. 第一にポリシー、次にテクノロジー

多くのセキュリティ戦略と同様に、暗号化の導入時に最初に着手すべきことは、ポリシーの確立です。暗号化の対象は、ディスクドライブ全体でしょうか。リムーバブルストレージデバイスでしょうか。それとも特定の種類のデータ、ファイル、フォルダーだけが対象でしょうか。たとえば特定の文書を一部のユーザーだけが閲覧できるようにしたい場合もあるでしょう。これらを部分的に採用することも検討できます。

大半の企業では、然るべきユーザーが然るべきタイミングで情報にアクセスできることが優先されます。的確なポリシーを適切なテクノロジーと組み合わせれば、セキュリティに関して妥協することなく目的を達成できます。

推奨される最初のステップ:

- **すべての関係者に協力を求める** - 情報システム、営業、財務、人事などの関係者の意見を聞いて、セキュリティの強化が必要な情報の種類を特定します。
- **アクセスを制御する** – 全員が鍵を持っていては、ドアを施錠する意味がありません。関係者と連携して、どの情報にどのユーザーがいつアクセスする必要があるかを特定します。追加の対策として、アクセス制御を定期的に監査して適切な状態を維持することが重要です。
- **コンプライアンスニーズを把握する** – 日本の個人情報保護法、米国のHIPAAやSOX、EUのData Protection Directive、英国のData Prevention Act、その他PCI DSSなどが挙げられます。世界で増え続けるデータ保護規制について詳しくない場合は、精通している同僚やセキュリティ・コンサルタントなどの協力を求めましょう。企業でのデータ保護やデータ交換の方法を管理する規制、法律、ガイドライン、その他の外部要因を特定し、これらに準拠するようにポリシーを策定する必要があります（たとえば、顧客のクレジットカードデータや従業員のマイナンバーを自動的に暗号化する、など）。
- **アクセスの可否を決定する** - ポリシーを文書化し、社内で導入に必要となる承認を得て、エンドユーザーに伝達します。エンドユーザーには、自社の機密データを扱う、派遣社員などの社外の関係者も含まれます。ポリシーに同意しないエンドユーザーには、データへのアクセス権を付与しません。
- **データをバックアップする** – 新しいソフトウェアをインストールする場合は、事前にデータをバックアップするのが最適ですが、それは暗号化を導入する場合でも変わりません。暗号化プログラムを実施する前に、必ずエンドユーザーの全データをバックアップしてください。
- **ユーザー負担を最小化する** – シングルサインオンをサポートするテクノロジーを実装して、エンドユーザーの負担と操作を最小限に抑えます。

2. フルディスク暗号化か、ファイルレベルの暗号化か

結論を言うと、両方を採用するのが効果的です。

暗号化ソリューションには、一般にフルディスク暗号化（FDE）を行うものとファイルレベルの暗号化（FLE）を行うものがあり、それぞれに利点があります。

FDE（Full Disk Encryption）の利点

FDE は、盗難や紛失からデータを保護する最も効果的な方法の 1 つです。FDE を使用していれば、デバイスに何が起こっても、データが判読不可能であり、犯罪者や不正な閲覧者にとって無意味な情報となります。

- FDE は、「ディスク上の保存データ」をハードウェアに近いレベルで保護します。つまり、ディスクのセクターが 1 つ残らず暗号化されるということです。この場合、ハードディスク上のデータが、ファイルコンテンツ、メタデータ、ファイルシステム情報、ディレクトリ構造を含めてすべて暗号化されます。暗号化されたディスク上のデータには、認証されたユーザーしかアクセスできません。FDE テクノロジーは、ハードディスクの他に、リムーバブルメディア（USB ドライブや USB エンクロージャ内のハードディスクなど）にも適用できます。

- 起動前認証（PBA）の設定を検討します。この認証では、OS が起動する前に、ユーザーに認証情報の提示と認証が要求され、セキュリティをさらに強化することができます。犯罪者など不正にディスクを入手した者は、ハードディスクの表面から直接データを読み取ることも、OS を起動することもできません。

  カスペルスキーの暗号化テクノロジーでは、PBA にオプションでシングルサインオンを適用できるほか、QWERTY 以外のキーボード配列を使用している場合でも PBA を使用できます。また、2 段階認証を使用したスマートカードとトークンの認証をサポートしており、パスワードを追加する必要がないため、ユーザーがストレスなく利用できます。

- 後ほど問題が生じないよう、インストール**前に**コンピューターとの互換性をチェックできる暗号化ソリューションを選びます。UEFI ベースのプラットフォーム（Windows 8 以降を搭載した最新の PC）をサポートするソリューションであれば、今後も確実に使い続けることができます。

  同様に、Intel の Xeon および Core プロセッサファミリー（と一部の AMD 製プロセッサ）での暗号化を高速化する Advanced Encryption Standard（AES）の拡張機能 Intel AES NI や、最新の GPT ディスク規格がサポートされていれば、包括的な暗号化戦略が可能になります。

- リムーバブルディスクで FDE 暗号化を使用すると、企業内で安全にデータを共有できます。

- FDE の導入時の検討すべき項目として、エンドユーザーの選択操作を不要にすることも重要です。アクセスをシングルサインオン（SSO）にすれば、エンドユーザーが暗号化を意識することはありません。2 段階認証は、ユーザー名やパスワードを追加することなく、保護をいっそう強化するとともに、使いやすさをさらに高めます。また、暗号化の管理を管理者の役割や職務に応じて柔軟に設定でき、暗号化管理の複雑さを軽減することができます。

FDE の最大のメリットは、すべてが暗号化されるため、リスクポイントであるユーザーに起因するトラブルが低減される点です。難点としては、送信中のデータ（デバイス間で共有される情報など）を保護できないことが挙げられます。しかし、ベストプラクティスを実践し、FLE にも対応するソリューションを選択すれば、この点が問題となることはありません。

FLE（File Level Encryption）の利点

ファイルシステムレベルで機能する FLE は、「ディスク上の保存データ」を保護するだけでなく、「使用中」のデータを守ることもできます。FLE を使用することで、任意のデバイス上の特定のファイルやフォルダーを暗号化できます。また、暗号化したファイルを暗号化したままネットワーク経由でコピーすることも可能です。これにより、格納場所やコピー先にかかわらず、特定の情報が不正に閲覧されないようにすることができます。管理者は、アプリケーションの種類や特定のディレクトリなど管理者の定義に基づいてファイルを自動的に暗号化できます。属性には、場所（[マイドキュメント]フォルダー内のすべてのファイルなど）、ファイルの種類（すべてのテキストファイル、すべての Excel スプレッドシートなど）、ファイルを作成したアプリケーションの名称などがあります。たとえば、Microsoft Word によって作成されたデータを、フォルダーやディスクに関係なく暗号化することができます。

- FLE を使用すれば、きめ細かな情報アクセスポリシーを柔軟に適用できます。（管理者が設定したポリシーに従って）機密と定義されたデータだけが暗号化されるため、さまざまなデータが使用されるケースもサポートされます。

- FLE はシステム保守の際にも簡単で安全に行えます。ソフトウェアファイルやシステムファイルが開いている間も、暗号化されたファイルのデータは保護され続けているため、更新やその他の保守作業を円滑に進めることができます。たとえば、CFO が極秘情報をシステム管理者の目にふれさせたくないと考えている場合、FLE で対応できます。

- FLE では効果的なアプリケーション権限コントロールがサポートされるため、管理者は特定のアプリケーションや使用シナリオに対して明確な暗号化ルールを設定できます。管理者はアプリケーション権限コントロールを利用して、暗号化データをその暗号化形式で提供するタイミングを決定できるほか、特定のアプリケーションに対して暗号化データへのアクセスを完全にブロックすることも可能です。たとえば次のような目的で使用されます。

  - 暗号化データを、データの復元先であるエンドポイントでのポリシー設定に関係なく、転送中、格納中、復元中も暗号化したままにすることで、安全なバックアップを簡単に行えるようにするため。

  - 通常のメッセージ交換を制限することなく、暗号化ファイルを IM 経由で交換できないようにするため。

FDE と FLE を組み合わせた暗号化アプローチを採用することで、両方のアプローチの優れた点を利用できます。たとえば、デスクトップ PC にのみファイルレベルの暗号化を選択し、ノートPCにはフルディスク暗号化を適用できます。

3. リムーバブルメディアの暗号化

現在では、USB フラッシュドライブの容量が 100 GB を超え、手のひらより小さいポータブルドライブにテラバイト単位のデータを保存できるようになりました。このため、機密情報が、背広のポケットに入ったままクリーニングに出されたり、空港でセキュリティトレイに置き忘れられたり、ポケットから落ちてしまったりする可能性が十分にあります。

ユーザーの不注意や事故をコントロールすることはできませんが、その結果をコントロールすることは可能です。

機密データをエンドポイントからリムーバブルデバイスに転送する際には、必ず暗号化しなければなりません。これは、FDE ポリシーまたは FLE ポリシーをすべてのデバイスに適用することで可能になります。これにより、デバイスの紛失や盗難が発生しても、機密データの安全が確保されます。

さらに、広範なデバイスコントロール機能が統合されており、特定のシリアル番号のデバイスという詳細なレベルまで、きめ細かくポリシーを適用することができます。

機密データを扱う際は、境界の内側でも外側でも、いわゆる「ポータブルモード」を利用する必要があります。たとえば、会議でプレゼンテーションを行うために、暗号化ソフトウェアがインストールされていない公共のコンピューターにフラッシュドライブからデータを転送するとします。ノートPCからプレゼンテーション用システムにデータを転送する間もデータを保護する必要がありますが、「ポータブルモード」を使用すれば対処できます。このモードでは、暗号化されたリムーバブルメディア上のデータを、暗号化ソフトウェアがインストールされていないコンピューターにも透過的に転送して使用することができます。

業界が認めた安全な暗号化の選択

暗号化戦略の善し悪しは、その基盤となるテクノロジーによって決まります。簡単に解読されてしまう暗号化アルゴリズムでは意味がありません。鍵長 256 ビットの Advanced Encryption Standard（AES）に対応し、キー管理とキーエスクロー（暗号鍵の供託）が容易な暗号化ソリューションを選択する必要があります。Intel® AES-NI テクノロジー、UEFI および GPT プラットフォームがサポートされていれば、長期にわたって有効な戦略となるでしょう。

キーの重要性を軽視すべきではありません。暗号化アルゴリズムの強度は、解読に必要なキーの強度次第です。簡単に破られるキーでは、暗号化プログラム全体が無意味になります。同様に、効果的な暗号化には効果的なキー管理が不可欠です。世界一強力な鍵をドアに取り付けても、玄関マットの下に鍵を置いては意味がありません。

マルチレイヤ・セキュリティの選択

エンドユーザーやデバイスの紛失だけがデータ消失の原因ではありません。サイバー犯罪者が開発するマルウェアは日増しに高度化し、システムにアクセスして密かにデータを盗みだすようになったため、何年も不正にアクセスされていることが発覚しないケースが増えています。暗号化を、盗まれたデータを無意味なものにするために利用するだけでなく、より幅の広い総合的なセキュリティ戦略の一部と捉えた方が、はるかに高い効果を発揮します。総合的なセキュリティ戦略とは、高性能なアンチマルウェア、デバイスコントロール、アプリケーションコントロールが連動して、システムへの不正アクセスと機密データ盗難の可能性を低減するものです。

暗号化のベストプラクティスは、アンチマルウェアとコントロールベースのセキュリティ対策と合わせて組み込まなければ完成しません。これらのセキュリティ対策により、情報漏洩につながるさまざまな脆弱性のスキャン、検知、管理を行いつつ、悪意あるコードを検知して削減することができます。そして、エンドユーザーの操作を最小限に抑えて実施する必要があります。

パスワードを忘れた場合への対応

ユーザーは、USB キーやスマートフォンを紛失するのと同じように、パスワードを忘れることがあります。

高性能なハードウェアや OS であっても、障害が発生して、ユーザーが重要な情報にアクセスできなくなることはあります。暗号化キーを格納するストレージやエスクローは、一元管理する必要があります。これにより、緊急時も容易にデータを復号化できるようになります。

優れた暗号化ソリューションには、次のようなケースで管理者が簡単にデータを復元できるツールが用意されています。

- エンドユーザーが復元を必要とするケース（パスワードを忘れた場合など）
- 管理者が保守のため、あるいは技術的な問題（OS がロードされない、ハードディスクに修理の必要な物理的な損傷があるなど）が発生したために復元を必要とするケース

ユーザーがパスワードを忘れた場合は、それに代わる認証手段として、ユーザーに一連の質問への回答を求めることができます。

一元的な管理

暗号化は、非常に複雑であり、実装と管理が難しいと言われてきました。その主な原因は、従来の古いソリューションが、アンチマルウェアやその他の IT セキュリティ技術と切り離されていたためです。エンドポイントコントロール、アンチマルウェア、暗号化などのさまざまなソリューションを管理する場合、たとえそれらが同じベンダー製であっても、費用が高額なだけでなく、導入フェーズにおいて長い時間を要します。購入、スタッフ教育、展開、ポリシー管理、保守、アップグレードのすべてを、コンポーネントごとに個別のプロジェクトとして扱わなければなりません。

すべてが統合されたマルチレイヤ・セキュリティソリューションは、時間と費用を節約できるだけでなく、ソフトウェアの導入を手間をかけずに行うことができます。

管理が容易なソリューションはさらに効果的です。単一のコンソールで単一のポリシー管理が可能なソリューションを選択すれば、投資を抑えられるほか、個別に管理されている多数のコンポーネント間の互換性の問題を解消できます。

エンドポイントの暗号化の設定は、アンチマルウェア保護やデバイスコントロールなど、他のすべてのエンドポイントセキュリティの設定と同じポリシーで適用することが望ましいです。たとえば IT 部門は、承認されたリムーバブルメディアをノート PC に接続することを許可するだけでなく、そのデバイスに暗号化ポリシーを適用することもできます。緊密に統合されたテクノロジープラットフォームには、システム全体のパフォーマンスを向上させるという付加的なメリットもあります。

結論

Kaspersky Endpoint Security for Business は、暗号化を容易に短時間で導入することが可能です。

カスペルスキーが提供する業界トップクラスのアンチマルウェア、エンドポイントコントロール、管理の各テクノロジーが統合されており、真のマルチレイヤーセキュリティを可能にします。これにより、アンチマルウェアやデバイスコントロールといったセキュリティ設定と同じポリシーで、暗号化の設定を適用することができます。複数のソリューションを個別に配備して管理する必要はありません。暗号化が展開される前に、ネットワークハードウェアの互換性が自動的にチェックされます。また、UEFI および GPT プラットフォームが標準でサポートされます。

この新たなアプローチを可能にしたのがカスペルスキーのプラットフォームです。カスペルスキーは、シームレスに連携するソフトウェアとテクノロジーを自社で開発し、寄せ集めのソリューションではなく、統合されたセキュリティプラットフォームを提供します。

カスペルスキーのエンドポイント・セキュリティ製品では、暗号化を含む、さまざまなセキュリティ機能や管理機能がシームレスに統合され、低コストで容易な導入が可能となり、より強固なセキュリティを実現することができます。

Memo

30日間利用可能な無料試用版ダウンロード：http://www.kaspersky.co.jp/trials#tab=tab-3

最新情報はウェブサイトをご確認ください ▶ http://www.kaspersky.co.jp/business-security

KASPERSKY

株式会社カスペルスキー

カスペルスキー Web サイト　www.kaspersky.co.jp/
ご購入相談窓口　jp-sales@kaspersky.com

製品・サービスに関するお問い合わせは下記へ