テクノロジー・ペーパー

サーバ、NAS、およびSANアレイ向け自己暗号化ドライブ

はじめに

この資料では、ハードディスク・ドライブが所有者の管理から離れた場合に、ドライブに保存されているデータをセキュアに保護する課題について検討します。自己暗号化ドライブ（SED : Self-Encripting Drive）は、1. ユーザのデータを暗号化して保存、2. ドライブが紛失したり盗難に遭った場合、自動的にロックしてデータを安全に保護、3. 暗号キーの更新にてセキュアな瞬時消去（instant secure erase）を行い読み取りを不可にする、など優れた機能を提供します。付録 A と B では、最初に SED と、ドライブ上のデータをセキュアに保護する他の暗号テクノロジーとの比較について説明します。次に、セキュアな消去と自動ロック SED テクノロジーについての詳しい解説を行い、SED がサーバ、NAS、SAN アレイ、仮想化環境、RAID、JBOD などで、どのように活用されるかについて説明します。

概要

ハードディスク・ドライブが移動または廃棄され、物理的に保護されていたデータ・センターから外部に搬出された場合、これらのドライブ上のデータは非常に大きいリスクにさらされます。IT 部門では、以下のような理由でドライブが定常的に廃棄されます。

- 修理、リース契約の満了のためのドライブの返却
- ドライブの置換えに伴う廃棄
- 他の目的で使用するための移動

ほとんどすべてのドライブが、いずれはデータ・センターから外部に搬出されることになります。シーゲイトでは、世界中で毎日 50,000 台のドライブがデータ・センターから廃棄されていると推定しています。データ・センターから外部に搬出されたドライブに保存されいる企業情報は、意図的に消去されない限り、引き続き読み取ることができます。データが RAID アレイ内で複数のドライブにストライピングされている場合でも、今日の大容量アレイでの通常のシングル・ストライピングでは数百人分の氏名や個人情報を読み取るには十分な大きさであるため、データ盗難の被害を受ける可能性があります。

サーバ、NAS、およびSANアレイ向け自己暗号化ドライブ

ドライブ管理の問題と廃棄コスト

データの漏洩を防止する取組みや個人情報に関する法令で必要とされる顧客への通知を確実に行うため、企業は、ドライブが管理下から離れる場合や悪用される前に、廃棄ドライブからデータを消去する方法を数多く試してきました。廃棄するドライブ上のデータを読取り不能にする方法は、現在、多くの人的な作業に依存しており、技術的ミスや人的なミスの影響を受けます。

今日の廃棄ドライブの処理方法における欠点は、台数が多いことと容量が大きすぎることです。

- ドライブのデータを上書きするには、膨大な時間、とコストがかかり、貴重なシステム・リソースを専有してしまいます。物理フォーマットを掛けない簡易的な上書きでは再割当てされたセクターを上書きできないため、読取り可能なデータが残ってしまいます。
- ドライブを消磁するか、または物理的に破壊するにしてもコストがかかります。ドライブの種類ごとに消磁の強さを最適に調整することは難しく、ドライブ上に読取り可能なデータが残る可能性があります。また、リースやレンタル品としてドライブを使用した場合に、期間満了時の返却に際してドライブを一方的に破壊することはできません。
- 一部の企業では、ドライブを安全に廃棄する唯一の方法は、ドライブを永久に倉庫に保管することと考えています。しかし、この方法は、ドライブの管理に人間が関わる以上、ドライブは紛失や盗難の危険性があり、安全とは言えません。
- 他の企業では、専門の廃棄サービスを利用しています。これは、内部のレポートや監査に加えて、このサービスのコストが発生することになります。このサービスを受けるためにドライブを外部に持ち出すことは、ドライブのデータをリスクにさらすことになり、より問題が発生しやすくなります。ドライブをわずか 1 台紛失したとしても、漏洩したデータを補償するには企業にとって莫大なコストがかかります。

これらの欠点を如実に表す一例として、IBM 社に返品されるドライブの 90% が読取り可能であったという同社の調査結果があります。重要な点はここにあります。つまり、データ・センターから搬出されるのは単なるドライブではなく、そこにはデータが格納されているということです。

暗号化

古いシステムがデータ・センターから廃棄されるたびに、数千テラバイトものデータもデータ・センターから搬出されます。しかし、これらのハードディスク・ドライブが、すべて自動的にかつ透過的に暗号化されており、瞬時にセキュアな消去が可能である場合を考えてみてください。米国のほとんどの州で、個人情報に関する法令が施行されていますが、暗号化されたデータの場合には、データ漏洩に関する報告の義務が免除されています。データが流出した場合のコストは、平均 660 万ドル[1] かかるため、ミスは許されません。

暗号化の使用を必要とするセキュリティ・ポリシーの採用を IT 部門が避けてきたのは、パフォーマンス、拡張性、複雑さに課題があるためでした。また、自社のデータをいつでも確実に解読できるように処理するキー管理についての知識が乏しい方には、暗号化は危険であるように思われていました。自己暗号化ドライブは、将来的に廃棄対象となるドライブを運用段階の始めから、ドライブを容易にかつ手頃なコストで暗号化することで、これらの問題を包括的に解決します。

ここでは 2 つのケースについて説明します。

- キー管理を必要としないセキュアな消去を提供する SED
- キーのライフサイクル管理を行うことで、盗難などからデータをセキュアに保護する自動ロック SED

1 出典：2008 Annual Study: Cost of a Data Breach, Ponemon Institute, February 2009

サーバ、NAS、およびSANアレイ向け自己暗号化ドライブ

キー管理を必要としないセキュアな消去

自己暗号化ドライブでは、暗号化による消去を行うことで瞬時にデータを消去できます。SED を通常の状況で使用している場合は、所有者が、ドライブのデータをアクセスするために、認証キー（認証情報またはパスワードとも呼ばれる）を管理する必要はありません。SED は、データをドライブに書き込む際に暗号化を行い、読み出す際に復号化を行います。これらのすべてが、所有者からの認証キーを必要とせずに行われます。

このドライブを廃棄したり再使用する場合、所有者はドライブに対して暗号化による消去を実行するコマンドを送信します。暗号化による消去を実行すると、暗号化されているドライブ内の暗号キーが置き換わります。これにより、以前のキーを使用して暗号化されたデータを復号化することが不可能になります。（セキュアな消去の機能については付録 A で説明しています。）

自己暗号化ドライブでは、ドライブ管理や廃棄コストの問題がなくなるため、IT 運用の経費が削減されます。米国政府の標準暗号化方式を採用した SED のデータ・セキュリティは、IT 効率を低下させることなく、個人情報に関する法令に確実に準拠できます。また、SED では、以下のような理由により、ドライブを返却する場合の消去処理が簡単になり、再利用する場合もハードウェアの価値を維持できます。

- ドライブを上書きしたり破壊する必要性がなくなる
- 保証サービスを受ける場合やリース期限が切れた場合にドライブを返却するときでも情報漏洩が防げる
- ドライブを別の目的で安全に再利用可能

キーのライフサイクル管理機能による自動ロック自己暗号化ドライブ

廃棄する際に SED を使用してセキュアな消去を行う他にも、ドライブの所有者は、SED を自動ロック・モードで使用して盗難からデータを保護することができます。社内にもかかわらず発生しえるドライブの盗難や紛失は、あらゆる規模のビジネスで大きな関心事となっています。また、物理的に強力なセキュリティを持たない企業やオフィスの管理者は、外部からの盗難の脅威に対する脆弱性に直面しています。

自動ロック・モードで SED を使用する場合、認証キーによってドライブをセキュアに保護します。この方法でセキュアに保護する場合、ドライブのデータ暗号キーはドライブの電源がオフにされるたびにロックされます。つまり、SED の電源がオフにされたりドライブが引き抜かれた瞬間にドライブのデータは自動的にロックされます。

その後、SED の電源がオンになると、ホストとの間で認証プロセスを経てから、暗号キーのロックが解除され、データへのアクセスが可能となります。この方法は、ドライブの紛失や内外部からの盗難に対して有効な対策となります。

認証キーのライフサイクル管理は IBM Tivoli Key Lifecycle Manager（旧 Encryption Key Manager）によって管理できます。これは、認証キーの生成、保護、格納、バックアップを一括管理する Java ベースのソフトウェアです。このソフトウェアは、すべての形態のストレージおよび他のセキュリティ・アプリケーションにおけるキー管理の要件をサポートする統合されたキー管理サービスです。IBM 社、LSI 社、シーゲイトは、OASIS（Organization for the Advancement of Structured Information Standards、構造化情報標準促進協会）のオープン・スタンダード・プロセスを促進するために、KMIP（Key Management Interoperability Protocol）を OASIS に提出しました。プラットフォームがベンダーに依存しないという特長により、IBM Tivoli Key Lifecycle Manager は、企業内で増え続ける暗号キーを管理するための簡単で効率的な方法を提供します。

自己暗号化ドライブの自動ロックモードと IBM Tivoli Key Lifecycle Manager の詳細については、付録 A で説明しています。

自己暗号化ドライブの所有者は、最初に SED をセキュアな消去のみのモードで使用して、後で SED を自動ロックモードに変更することができます。その後、再利用するためにセキュアな消去を実行すると、このドライブはセキュアな消去のみのモードで使用できるようになります。そのため、最初の通常の運用では、ドライブの所有者が必要なときにセキュアな消去を行えるよう、SED をセキュアな消去のみのモードにしておくことができます。その後、盗難に備える必要性が高くなった場合に、ドライブの所有者は、既存の暗号キーを暗号化する認証キーを作成して、SED を自動ロックモードで使用できます。次に、SED がセキュアに消去されて再利用される場合、新しい所有者は、このドライブを自動ロック・モードに設定せずに、セキュアな消去のみのモードで使用し、最終的にドライブを廃棄するときにデータをセキュアに消去できます。

サーバ、NAS、およびSANアレイ向け自己暗号化ドライブ

セキュアな消去のために自己暗号化ドライブを使用するだけでも、ドライブを安全に廃棄する手段が提供されます。しかし、SED を自動ロック・モードで使用することで、より多くの利点が提供されます。つまり、認証に関係なく、ドライブまたはシステムがデータ・センターから搬出された瞬間にドライブはロックされます。データ・センターの管理者は、データの保護について、これ以上の心配も作業も必要ありません。これにより、ドライブが誤って扱われた場合の漏洩が回避され、組織の内部や外部での盗難の脅威からデータが保護されます。

ハードディスク・ドライブ上のデータをセキュアに保護するテクノロジーの比較

ひとつの暗号テクノロジーで、すべての脅威からすべてのデータのセキュリティを効率的かつ効果的に保護できるわけではありません。さまざまな脅威から保護するために、さまざまなテクノロジーが使用されます。たとえば、自己暗号化ドライブでは、ドライブが所有者の管理を離れても、データは脅威からセキュアに保護されます。しかし、データ・センター内で起こるある種の脅威に対してはデータを保護できません。攻撃者が、サーバにアクセスできれば、それはロックされていないドライブにアクセスできることを意味し、ドライブから暗号化されていないテキストを読み取ることができることになります。つまり、SED 暗号化テクノロジーは、データ・センターのアクセス制御に代わるものではなく、それを補完するものでもないことを認識してください。

データをセキュアに保護することは、移動するデータの保護に置き換わるものではなく、補完的なものです。ファイル・システムのネットワークを介して転送されるデータのほとんどは、NAS のイーサネット経由であっても、SAN のブロック・レベルの転送であっても、物理的に IT ストレージ管理者の管理下にありセキュリティ上のリスクはないと考えられます。物理的に管理者の管理下にないデータの移動の場合、少量のデータを暗号化する短期セッション暗号キーを使用する IPSec または FC over IP が、最も広く使用され、確立されているデータの暗号化の方法です。このセッション・セキュリティの方法を使用する代わりに、ハードディスク・ドライブ上だけでなく、ファブリックでもデータの暗号化を行う方法が、より優れた解決方法であると考えられる場合があります。しかし、この方法には根本的な欠陥があります。それは、単一の暗号キーのみによって暗号化された大量のテキストが露呈される一方、長期間有効となる暗号キーも露呈されることで、セキュリティを向上させるのではなく、むしろ低下させ、より複雑化させています。データの移動中も暗号化が必要な場合は、IPSec または FC over IP を使用するべきです。以下の理由により、ドライブ上の暗号化データは、ドライブ上で最もその効果を発揮します。

アプリケーション、データベース、OS、ファイル・システムの暗号化（図 1 参照）は、すべてデータ・センター内で発生するドライブ上のデータに対する脅威（データベース管理者、ファイルまたはシステムの管理者、ハッカーによる）を防止するためのテクノロジーです。しかし、このような暗号化を伴うアプリケーション、データベース、OS、ファイル・システムでは、著しくパフォーマンスが低下し、非スケーラブルな変更が必要となるため、データの特定の箇所以上を暗号化するのは現実的ではありません。管理者は、最も機密性の高いデータのみに対して暗号化を行うことでこの制約に対処しています。

これにより、管理者は機密性の高いデータを識別し場所を特定するために、データの分類に依存することになります。しかし、この処理では、機密性の高いすべてのデータを特定することができないことは広く認識されています。特に、機密性の高い情報が、保護されている環境から保護されていない環境にコピーされた場合には、データの分類は困難で労力を必要とし、管理が難しくなります。その結果、機密性の高い大量のデータが、暗号化されずにディスク・ドライブに書き込まれることになります。これらのデータは、ドライブがその役目を終えて廃棄されても長期に渡ってそのドライブに維持されたままになる可能性があります。

原則論 : セキュリティは HDD に掛けるのがベスト

そのため、フルディスク暗号化を実現するには、ファイル・システムのダウンストリームにおける暗号化テクノロジーを使用することになります。この方法により、データの分類を行う際に機密データを検出できなかった場合の問題が解決されます。これらのテクノロジーにより、データの管理者は、煩雑でコストのかかる作業であった、データがデータ・センターの管理から離れる際のデータの機密性の分類に関する責任から開放されます。暗号化は、ファブリック、RAID コントローラ、またはハードディスク・ドライブのすべてで行うことができますが、どこで行うべきでしょうか。

サーバ、NAS、およびSANアレイ向け自己暗号化ドライブ

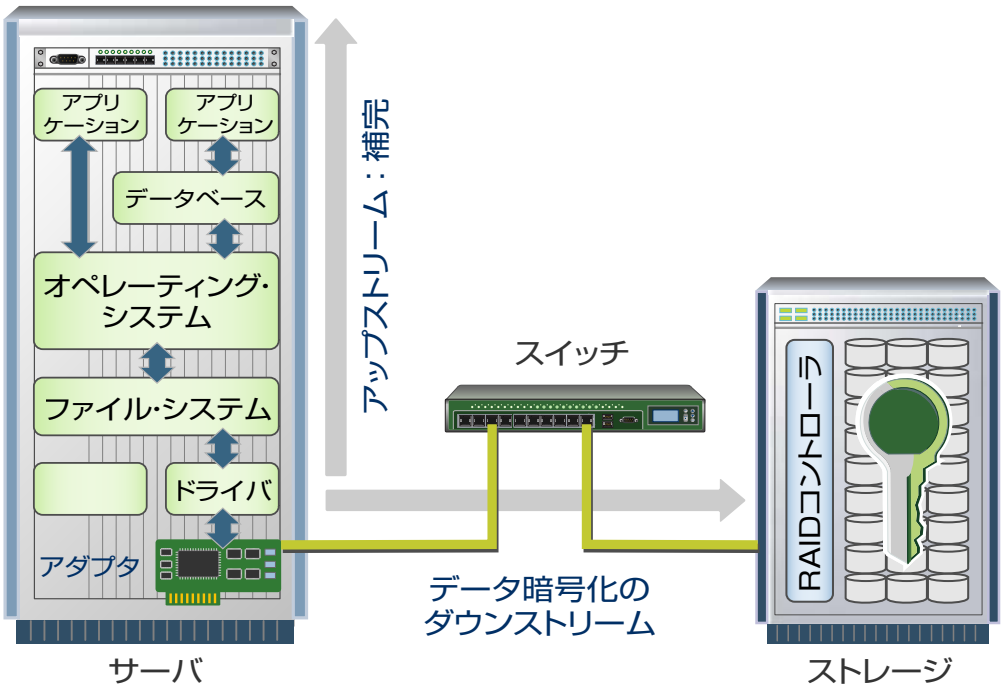


図 1.

数年前、シーゲイトがドライブの暗号化を始める以前、米国のNSA（National Security Agency）がデータ・セキュリティにおける問題の分析を行い、暗号化を行う最適な場所はハードディスク・ドライブであると結論を下しました。データの保護機能は可能な限りデータに近づけるべきであるというセキュリティに関するよく知られた格言があります。このことから、データが置かれているハードディスク・ドライブ内での暗号化が、最適な方法となります。SED は、フルディスク暗号化を実現するための優れたテクノロジーであり、次のような利点を提供するとともに、サーバのダイレクト・アッタッチド・ストレージ、ＳＡＮ、NAS ストレージの TCO を削減します。

- **キー管理の簡略化**：SED では、データ暗号キーを追跡および管理する必要はありません。SED をセキュアな消去のみのために使用する場合は、認証キーの追跡と管理も不要になります。
- **テクノロジーの標準化によるコスト削減**：業界標準のテクノロジーの採用により、コストを削減できるだけでなく、SAN、NAS、サーバ、デスクトップ、ノート、ポータブルの各ストレージ・プラットフォームで共通のテクノロジーを使用できるようになります。
- **最適なストレージ効率**：**従来の暗号化方式と異**なり、SED ではデータ圧縮や重複排除が可能になるため、ディスク・ストレージのキャパシティを最大限に活用できます。
- **データ保全性の向上**：SED では、Protection Information（情報保護）の使用が可能になります。これは、ハードディスク・ドライブの信頼性と保証に影響を与えることなくデータの保全性を確保するための将来採用される機能です。
- **パフォーマンスと拡張性の最大化**：SED は、直線的かつ自動的な拡張が可能でありながら、ドライブの最大速度で動作します。
- **データ分類が不要**：**暗号対象を決定するための、データ**分類作業を必要としないため、コストと時間の浪費を排して、最大のパフォーマンスを維持します。
- **再暗号化の低減**：SED では、暗号キーがディスクの外部に露呈されることがないので、キーの再設定や再暗号化の必要性が低減されます。
- **優れたセキュリティ**：NSA によって認定された最初の SED モデルです。SED では、ストレージ・ファブリックの暗号化を不要にします。暗号化されたテキストとキーを長時間露呈することが無いため、セキュリティを脆弱化させることがありません。SED を使用する場合、ネットワーク経由の暗号化は、移動中のデータをセキュアに保護するための別の専用テクノロジーに委ねます。

サーバ、NAS、およびSANアレイ向け自己暗号化ドライブ

自己暗号化ドライブの標準化は、購入コストも低減します。主要なハードディスク・ドライブ 6 社は、Trusted Computing Group（TCG）によって発行されたエンタープライズ向けの最終仕様を共同で策定しました。この仕様は、自己暗号化ドライブを開発し管理するための標準規格として策定されています。この仕様によって、異なるベンダー間の SED の相互運用性が確保されます。このように相互運用性が確保されることにより、市場競争が加速され、ソリューション・ビルダーやエンド・ユーザ向けの価格はより安価になります。歴史的にも、ハードディスク・ドライブ業界は、業界全体に渡る標準規格によって生産台数の拡大（つまり価格の低下）を繰り返してきました。このような規模での展開は、ASIC 内部の暗号化ロジック増加分も最小に抑え、結果的に部材コストをセーブします。（付録 B では、ハードディスク・ドライブの暗号化テクノロジーの比較および SED の利点について詳しく説明しています。）

結論

サーバ、SAN、NAS アレイの管理者には、データを暗号化する正当な理由があります。自己暗号化ドライブは、今までセキュリティに関して必要性と問題意識を持ちながらも、なかなか採用に踏み切れなかった IT 担当者に朗報となります。

自己暗号化ドライブの利点は明確です。セキュアな瞬間消去によって、キーを管理することなくドライブを廃棄できるので、IT の運用費用が削減されます。さらに、自己暗号化ドライブでは、ドライブを再利用する場合や、保守、保証、リース期限の満了により返品する場合にセキュリティが確保されるため、単品ドライブとしての資産価値を維持できます。自動ロック SED は、ドライブを盗まれたり紛失した場合、またシステムからドライブが取り外された時点で自動的にデータをセキュアに保護します。ドライブが盗難に遭ったとしても、それによってデータが漏洩することは決してありません。

自己暗号化ドライブはさまざまな利点を提供します。暗号キーは、ドライブを離れることがないため、データをリカバリする場合に暗号キーを追跡したり管理する必要がなく、所有者自身のデータが復号化できなくなるような心配は軽減されます。追跡または管理する必要があるのは、認証キーのみです。認証キーはディザスター・リカバリ・センターでセキュアにバックアップ、複製、およびミラー化できます。SED をセキュアな瞬間消去のみのために使用する場合には、認証キーを必要としません。

通常のストレージ管理、OS、アプリケーション、データベースを変更することのないよう、SED の暗号化は、自動的かつ透過的に行われます。ストレージ・システムでのデータの効果的な圧縮および重複排除による大幅なコスト節減は、完全に維持されます。さらに、パフォーマンスは、直線的かつ自動的に拡張されます。パフォーマンスを低下させることなくすべてのデータを暗号化できるので、多大なコストと時間を費やすデータの分類は必要ありません。

自己暗号化ドライブは、最適な管理性、相互運用性、コスト効率を実現するために標準規格をベースとしています。この標準規格の策定には、主要なハードディスク・ドライブのメーカーが参加しています。主要なストレージ・ベンダーが OASIS の Key Management Interoperability Protocol をサポートすることを確約しているため、キー管理もまた相互運用性が確保されるようになってきています。SED は、標準製品に搭載されるよう設計されており、通常のストレージ・アップグレードのサイクルで導入可能です。

つまり、他の暗号化技術と比べると、ドライブで行われる暗号化は、優れたコスト効率、パフォーマンス、管理性、およびセキュリティを提供します。これが、多くの著名なアナリスト、システム・メーカー、および NSA などの政府機関がドライブで暗号化を行うべきであると結論を出した理由です。結論として、SED は、サーバ、SAN、および NAS アレイにおけるセキュリティを向上させ、TCO（Total Cost of Ownership）を低下させる飛躍的な効果をもたらします。

SED の使用により、ドライブの廃棄コストが低下し、IT に関する問題が軽減されるため、多くの企業が、セキュリティ・ポリシーに SED の導入を考えています。セキュリティ・ポリシーの策定者は、可能であれば、今後購入するハードディスク・ドライブをすべて SED にするよう、セキュリティ・ポリシーに明記することを考えるべきです。IBM 社と LSI 社は、自己暗号化ドライブを自社のソリューションに搭載することを推進しています。また、シーゲイトは、ハードディスク・ドライブの製品ポートフォリオ全体に SED を取り入れることを急速に進めています。他のハードディスク・ドライブ・ベンダーも SED を発表しており、すべてのハードディスク・ドライブが自己暗号化ドライブになるのもそう長くはありません。

サーバ、NAS、およびSANアレイ向け自己暗号化ドライブ

付録 A：自己暗号化ドライブ・テクノロジー

新規に入手した自己暗号化ドライブ

工場出荷時の自己暗号化ドライブ（SED）には、ランダムに生成された暗号キーがあらかじめ組み込まれています。SED は、フルディスク暗号化を自動的に実行します。これは、書込みを実行する際に、ドライブがテキストを受け取り、それをディスク上に書き込む前に、ドライブに組み込まれている暗号キーを使用して暗号化します。読出しを実行する場合は、暗号化されているディスク上のデータを復号化してから、データをドライブの外に転送します。通常の運用では、SED はシステムに完全に透過的です。つまり、システムからは、SED は非暗号化ドライブと同じように見えます。自己暗号化ドライブでは、暗号化の処理が誤って停止することはなく、常に暗号化が実行されます。

所有者が新規にドライブを入手した時点では、ドライブに組み込まれた暗号キーは、暗号化されていないテキスト形式です。この状態は、ドライブが自動ロック・モードになり、認証キーが設定されるまで続きます。ドライブは、データを書き込む際に暗号化を行い、読み出す際に復号化を行います。しかし、認証キーを設定しない場合は、誰でもドライブのデータの書込みと読出しが可能です。

ドライブの設定は非常に簡単です。所有者は、SED を自動ロック・モードで使用するか、またはセキュアな消去のみで使用するかを決める必要があります。これらの使用方法については以下で説明します。

セキュアな消去テクノロジー

所有者が、セキュアな消去のみで使用する場合は、ドライブを通常の運用どおりに使用開始できます。セキュアな消去のみのモードとは、所有者がデータを復号化するために、認証キーまたはパスワードを必要としないことを意味します。この場合、認証キーの管理を誤り、データの損失を招くようなことはありません。

SED テクノロジーによって、ドライブの廃棄や再利用が大幅に簡略化されます。ドライブを再利用する所有者は、キーの消去を行うだけで、暗号キーを置き換えることができます。暗号キーが消去されると、ドライブ内でランダムに生成された新しい暗号キーに置き換わります。キーの更新後は、ディスクに書き込まれた旧データを読み取ることはできなくなります。以前のキーを使用して暗号化された古いデータは、新しい暗号キーで復号化しても判読不能なデータとなります（図 2 参照）。ドライブは、工場出荷時と同じ状態になり、新しい所有者にとって、セキュアな消去のみのモードでも自動ロック・モードでもすぐに使用できる状態になります。

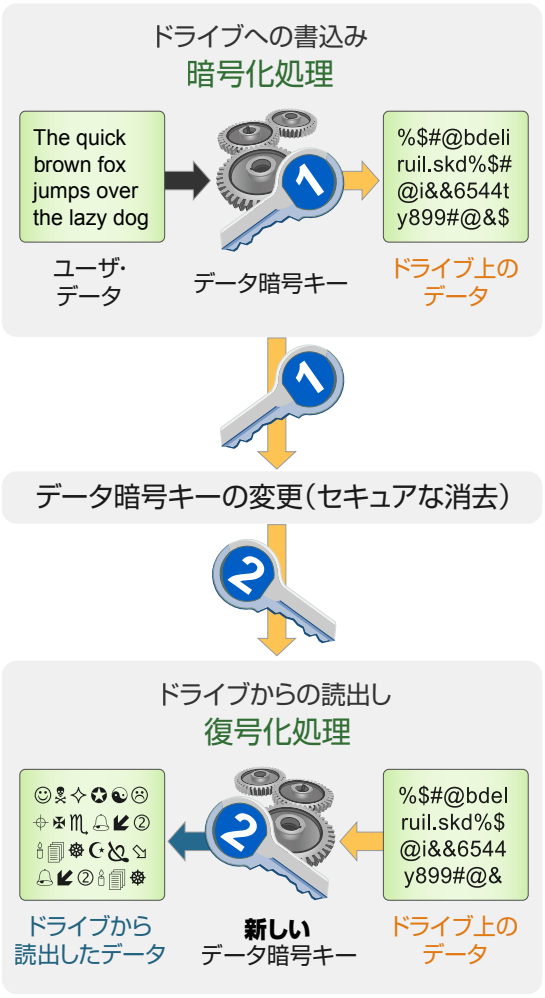


図 2.

サーバ、NAS、およびSANアレイ向け自己暗号化ドライブ

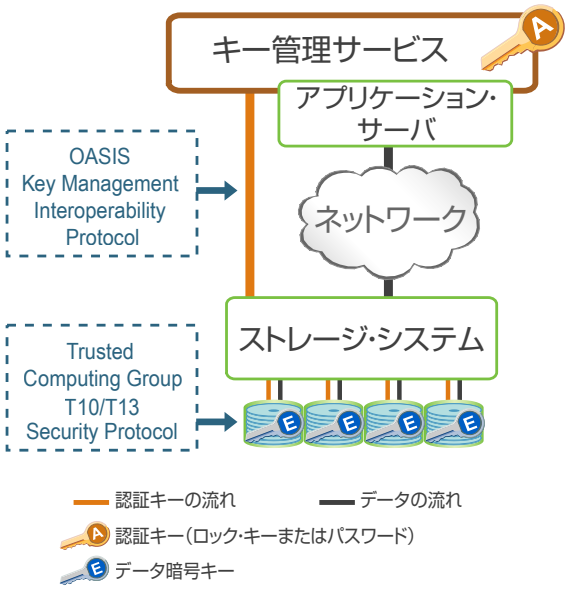


図 3.

キーおよび自動ロック・モードでの自己暗号化ドライブの管理

SED を自動ロック・モードで使用する場合、SED は、ドライブのロックを解除して読み書きを行うために外部から提供される認証キーを必要とします。自動ロックモードの SED を所有しているデータ・センターでは、認証キーの格納、管理、処理を行うキー管理サービス、およびこれらの認証キーを適切なドライブに割り当てることが可能なストレージ・システムを使用しています（図 3 参照）。シーゲイト、IBM 社、および LSI 社は、共同でそれぞれのテクノロジーを結集し、IBM System Storage DS8000 や IBM System Storage DS5000 などの暗号化ソリューションを実現しています。

従来からの機能に加え、このストレージ・システムでは、セキュアに保護されたボリューム・グループを定義し、キー管理サービスから認証キーを取得して適切なドライブに割り当てられます。図 3 のオレンジ色の線は、この操作を示しています。この方法では、ストレージ・システムは、暗号化機能をホスト、OS、データベース、アプリケーションに対して透過的なものにします。

電源を投入して認証が完了すると、暗号化はストレージ・システム全体に透過的となるため、ストレージ・システムは従来どおりの機能を実行することができます。図 3 の灰色の線は、暗号化されていないテキスト・データの流れを示しています。ストレージ・システムは、非暗号化データのデータ圧縮および重複排除向けに最適化されています。

キー管理サービスでは、関連する認証キーと暗号キーの企業規模での作成、割当て、管理を行うために、ソフトウェアまたはハードウェア・ベースでのキー格納を採用することがあります。効率的にキーを管理するには、サービスとキーを不正なアクセスから確実に保護するよう、キー管理を組織内の既存のセキュリティ・ポリシーに統合する必要があります。

さらに、キー管理システムの効率を高めるには、バックアップ、同期、ライフサイクル管理、監査、および長期間のデータ保持の各機能も備える必要があります。高可用性ソリューションやディザスタ・リカバリ・ソリューションを利用できる場合は、キー管理サービスの展開が大幅に簡略化されます。

IBM Tivoli Key Lifecycle Manager（旧 Encryption Key Manager）は、IBM の自己暗号化機能を持つテープ・ドライブおよびフルディスク暗号化機能を持つIBM System Storage DS8000 で使用される、認証キーの生成、保護、格納、維持管理を行う Java ベースのソフトウェアです。IBM Tivoli Key Lifecycle Manager は、Java ベースのアプリケーションであるため、z/OS、i5/OS、AIX、Linux、HP-UX、Sun Solaris、Windows の各オペレーティング・システムで動作します。このアプリケーションは、高い可用性を確保するために、組織内の数箇所に展開して、共有可能なリソースとして使用できるよう設計されています。

プラットフォームがベンダーに依存しないという特長と、企業内で最もセキュアなサーバ・プラットフォームで既存のセキュリティ・ポリシーと高可用性環境を利用できる機能によって、IBM Tivoli Key Lifecycle Manager は企業内で増え続ける暗号キーを管理するための簡単で効率的な方法を提供します。

サーバ、NAS、およびSANアレイ向け自己暗号化ドライブ

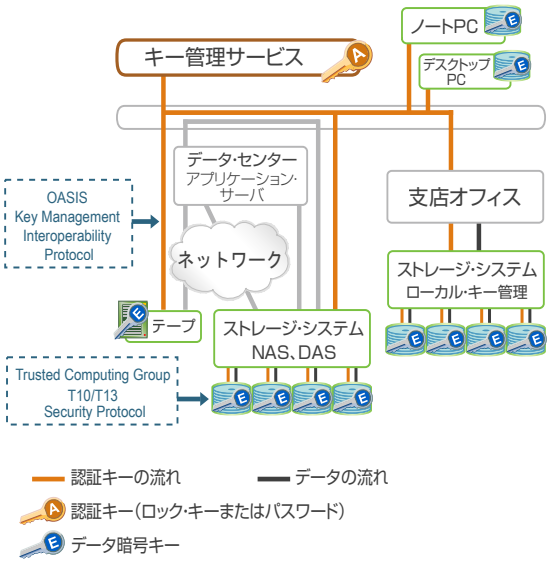


図 4.

IBM Tivoli Key Lifecycle Manager は、セキュアな場所に一括管理されているキー情報の使用を許可された時点で、キー・サービスを提供します。これはキー管理用の複数のプロトコルをサポートし、証明書、対称キー、非対称キーを管理する独自のアプローチです。ユーザは、これらのキーと証明書の作成、インポート、配布、バックアップ、アーカイブ、およびライフサイクル管理を、カスタマイズ可能な GUI（Graphical User Interface）を使用して一括して行うことができます。また、IBM Tivoli Key Lifecycle Manager の透過的な暗号化実装では、キーは一元化された場所で生成および提供されますが、暗号化されていない状態で送信されたり格納されることはありません。

このテクノロジーは、図 4 に示すように、データ・センター全体に適用されます。自己暗号化ドライブは、データ・センター、オフィス、SOHO などで使用されているストレージ・アレイ、SAN、NAS、サーバなどに搭載される可能性があります。統合されたキー管理サービスでは、すべての形態のストレージとその他のセキュリティ・アプリケーションでのキー管理に対する要件がサポートされます。

自動ロック自己暗号化ドライブ・テクノロジー

自己暗号化ドライブを自動ロック・モードにする場合、ドライブの所有者は、セキュリティを強化するために、新しい SED でセキュアな消去を行い、最初に暗号キーを変更することができます。これにより、ドライブの保管時での攻撃からもドライブが保護されます。所有者は、次に、ドライブの外部ラベルに記載されている SID（所有者であることを証明するセキュリティ ID）を最初に入力することで、認証キーを設定します。これは、ドライブが暗号キーを暗号化するために使用されます。これで SED の自動ロック・モードが設定され、ドライブはセキュアに保護された状態になります。つまり、ドライブの電源を切るとロックされ、電源を再び投入すると、ロックを解除するための認証が要求されます。自動ロック・モードの SED では、暗号キーと認証キーの両方が機能して、ドライブに保存されているデータにアクセスすることができます。

認証を使用するように設定された自動ロック・モードの SED には、データを解読する際の手がかりとなる情報は含まれていません。検出されたとしても、表示されるのは暗号化されたデータです。以下に簡単にドライブのロックを解除するプロセスについて説明します。これで上の文の意味がおわかりになるでしょう。ロック解除のプロセスはドライブに電源を入れる際の処理の一部として実行され、これによって暗号化されたデータへのアクセスが可能になります。ドライブは認証情報（認証キー）を受け取ることで、認証されているユーザがドライブにアクセスしていることを確認します。

サーバ、NAS、およびSANアレイ向け自己暗号化ドライブ

以下では、すでにセキュアに保護されているドライブの認証プロセスの手順を説明します（図 5 参照）。

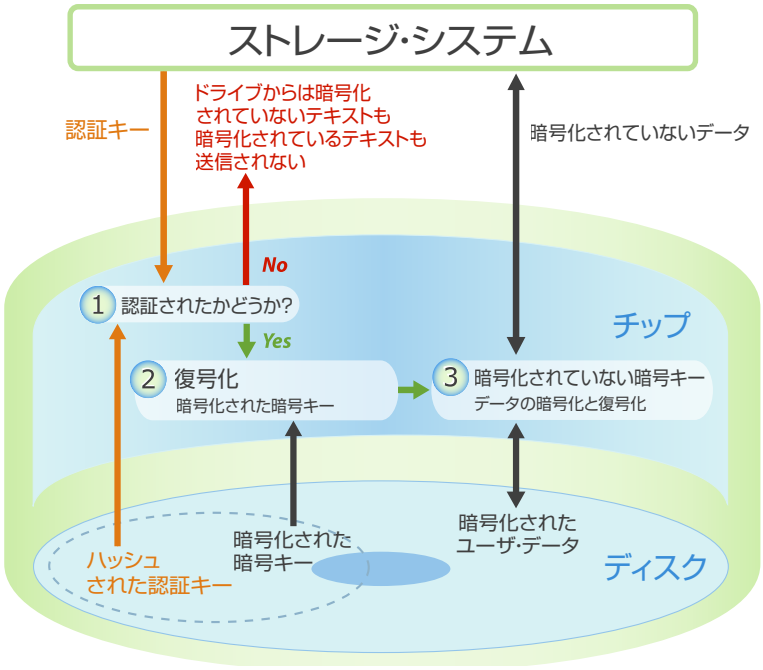


図 5.

1. 認証

- ストレージ・システムがキー管理サービスから認証キーを取得し、ロックされている適切なドライブに転送します。
- ドライブは、あらかじめ認証キーをハッシュして、ディスク上のセキュア領域に保存しています。そのキーと、キー管理サービスから送られたキーとを比較照合します。
- 2 つのハッシュされた認証キーの値が一致しない場合、認証プロセスは終了し、ディスクからのデータの読取りは許可されません。ドライブはロックされたままになります。また、ドライブから暗号化されたテキストが読み出されることもありません。

2. 暗号化された暗号キーの復号化

- 2 つのハッシュが一致した場合は、ドライブのロックが解除されます。ストレージ・システムから取得した認証キーを使用して、ディスクのセキュアな領域に保存されている暗号キーのコピーが復号化されます。この暗号キーは、以前に認証キーによって暗号化されたものです。認証プロセスが正常に終了すると、ドライブは次に電源が切られるまでロックが解除された状態になります。この認証プロセスが行われるのは、ドライブの電源を最初に入れるときのみです。個々の読み書きの操作では行われません。

3. 復号化された暗号キーによるデータの暗号化と復号化

- 次に、復号化されたテキストの暗号キーを使用して、ディスクに書き込むデータが暗号化され、また、ディスクから読み取るデータが復号化されます。
- 暗号化と復号化はバックグラウンドで透過的に行われるため、ドライブは通常どおりのデータ転送を行います。

ドライブを自動ロック・モードにすると、セキュアな消去が実行された場合にのみ、セキュア消去のみのモードに戻ります。所有者がドライブを再利用したり廃棄する場合は、セキュアな消去を実行して、暗号キーを置き換えるだけです。つまり、自動ロック・モードのドライブをセキュアな消去のみのモードにすることで、他のユーザがこのドライブを使用できるようになります。

サーバ、NAS、およびSANアレイ向け自己暗号化ドライブ

付録 B：ハードディスク・ドライブ上のデータをセキュアに保護するテクノロジーの比較

すべての脅威からデータを保護する包括的な暗号化の方法はありません。それぞれの方法には、コスト、相互運用性、パフォーマンス、待ち時間などの考慮すべき問題があるため、暗号化を行う場所を選択するときには注意が必要です。データの暗号化には以下のようなさまざまな形態があります。

- ホストベースのソフトウェア
- 暗号化機能を備えたハードウェア・アプライアンス
- アダプタ、スイッチ、RAID コントローラ、ハードディスク・ドライブなどに搭載されている暗号化 ASIC

SAN、NAS、サーバに直接接続されたストレージのデータについて、暗号化する場所とその方法を評価する場合、保存している場所になるべく近いところで暗号化を行うことが最善の解決策となります。つまり、暗号化をハードディスク・ドライブで行うのことが、最善の解決策となります。

キー管理および相互運用性の簡略化

SED では、暗号キーがドライブから離れることがないため、キー管理が大幅に簡略化されます。これにより、暗号キーを追跡したり管理する必要がなくなります。さらに、暗号化された暗号キーのコピーはドライブの複数の場所に保存されるので、データを復元可能な状態に維持するために、データ・センター管理者が暗号キーをエスクロー（第三者預託）する必要もありません。

暗号キーのすべてのコピーが失われるような場合には、ドライブ自体が故障している可能性が高く、データはいずれにしても読取り不能になるため、暗号キーをエスクローする必要がないのは SED のみです。また、データが冗長化されるたびに暗号キーのコピーも自動的に追加されます。つまり、データが別の自己暗号化ドライブにミラーリングされると、新しいドライブは、暗号化された暗号キーのセットを独自に持つことになります。対照的に、ファブリックやコントローラでの暗号化では、終端でのデータの読み書きを可能にするための暗号キーの追跡、管理、およびエスクローが課題になります。

スイッチまたはアダプタで行うハードウェアによる暗号化に関しては、大きな課題が存在します。データが保存されている場所とは別の場所で暗号

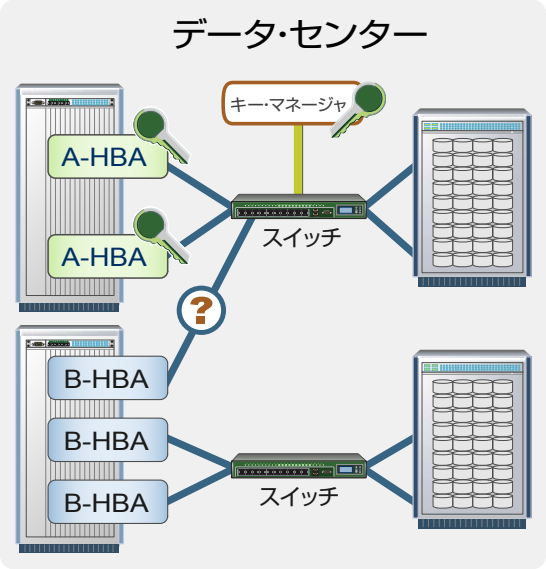


図 6.

化を行うことは、ソリューションがより複雑化し、エラーを発生させる機会を増やすことになります。たとえば、仮想環境においてデータの復号化が必要なときに、正しいキーが使用できる状態になっていない場合があります。共有する装置が増えると特定のキーを共有する必要があるエンティティの数も増え、ファブリック内を移動する多くのキーを追跡することには、露呈、複雑性、パフォーマンスの問題を必然的に伴います。

暗号化 ASIC を搭載したアダプタでは、オンボードの暗号化をサポートしていないベンダーのアダプタとの相互運用性の問題があります。アダプタに搭載されているハードウェアで暗号化されたデータは、同じ暗号化アルゴリズムを使用し、同じキー管理インフラストラクチャへのアクセスが可能な、互換性のあるハードウェアでなければ読み出すことはできません。たとえば、図 6 の下部にあるサーバ内の青色で示されている HBA（Host Bus Adapter）は、ターゲット上で暗号化されたデータを読み取ることができません。また、キー・マネージャあるいは暗号化機能を持つスイッチでも認証することができません。これは HBA がキー・マネージャにアクセスできないかまたはハードウェアの暗号化に互換性がないためです。

自己暗号化ドライブでは、暗号キーがドライブを離れることがないため本来の管理性が提供されます。さらに、異なる暗号化アルゴリズムを持つハードディスク・ドライブを既存のアレイに追加する

サーバ、NAS、およびSANアレイ向け自己暗号化ドライブ

のも簡単です。暗号化アルゴリズムはシステムにとっては透過的であるため、データ･センターでは、さまざまな暗号化アルゴリズムを同じアレイに混在させることが可能になります。新しいドライブの登場や、ハードディスク・ドライブに新しい暗号化テクノロジーが搭載されても、暗号化をサポートするストレージ・システム内の従来のドライブと併用することができ、新しいドライブの高度な保護機能に合わせて変更を行う必要はありません。

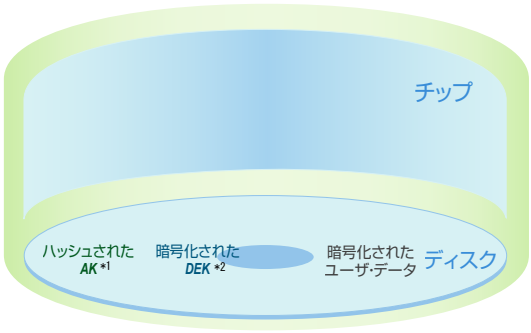
また、キー管理も相互運用性が確保される傾向にあります。IBM 社、LSI 社、シーゲイトは、OASIS オープン標準のプロセスを通じて提案した Key Management Interoperability Protocol をサポートする予定です。

政府（米国）で採用されているセキュリティ

自己暗号化ドライブは高度なセキュリティ機能を提供します。この高度なセキュリティ機能によって、将来のより厳しい規制のために、データ･セキュリティ・ソリューションを変更したり置換える必要性を減らすことも可能になります。前にも説明しましたが、SED は、ストレージ・ファブリックを不要に暗号化し、長期間有効となる暗号化されたテキストとキーを露呈することによって、セキュリティを脆弱化することはありません。SED は、他のどのフルディスク暗号化テクノロジーよりもセキュリティを強化することが可能なその他の利点も提供します。

NSA（National Security Agency: 米国家安全保障局）は、米国政府機関と安全保障にかかわるその契約会社で使用されるコンピュータ内の情報を保護するために、Momentus® 5400 FDE ハードディスク・ドライブを自己暗号化ドライブとして初めて認定しました。また、この最初のモデルに採用されている暗号化アルゴリズムは NIST AES FIPS-197 に準拠したものです。シーゲイトは、将来の SED でも同様の認定を受ける作業を行っています。

図 7 には、攻撃者がセキュアなドライブ（ドライブの電源が切られたことでロックされている）を手に入れた場合に、取得できるものを示しています。暗号キーはドライブ自身が生成した一意なもので、ドライブを離れることはありません。さらに、暗号化されていない暗号キーはどこにも存在しません。ドライブ内に保持されているのは暗号化された暗号キーのみです。ドライブには、解読の手がかりとなる読取り可能な情報はありません。認証キーの指紋（ハッシュ）があるだけです。さらに、ハードディスク・ドライブは、「コールドブート」攻撃を受けやすいメモリーの類を使用しません。



*1　AK：認証キー　　*2　DEK：データ暗号化キー

図 7.

データと暗号キーはいずれも AES 128 アルゴリズムを使用して暗号化されます。この暗号化アルゴリズムは、米国政府の機密情報の保護に使用する暗号化方式に認定されています。ドライブを設計する場合、シーゲイトでは攻撃者がドライブの設計に詳しく、データを解読する手がかりとなる情報がドライブのどこに保存されているかについて、よく理解しているものと仮定しています。データを解読するための手がかりとなるようなものはドライブ上にないため、ドライブの設計や構造についての詳細を知ったとしても攻撃者には何の役にも立ちません。同様に、1 台のドライブにアクセスできたとしても、これによって他のドライブに簡単にアクセスできるというようなことはありません。

一般的には、暗号化されたテキストの露呈が攻撃者を助ける場合があります。たとえば、ドライブのファイル・システムの構造がよく知られている場合、ある特定のセクターには常に既知の値が含まれているため、暗号化を解読するために利用される可能性があります。同様に、データベースの構造もよく知られています。自己暗号化ドライブに特有の利点は、SED からは暗号化されたテキストを転送しないという点です。これにより、このタイプの攻撃が回避されることになります。

認証の失敗が事前に設定した回数を超えた場合、SED には、その後の認証を受け付けないようにする強固な機能があります。対照的に、他の方法で暗号化された SED 以外のドライブを攻撃する場合は、無期限に認証を試みることができ、ドライブは無防備な状態になってしまいます。また、SED ではファームウェアのダウンロードが保護されているため、攻撃者は改造したファームウェアをドライブに送り込むことはできません。攻撃に対する脆弱性を最小にするために、シーゲイトは SED のセキュリティに裏口（バック・ドア）を設置していません。

サーバ、NAS、およびSANアレイ向け自己暗号化ドライブ

最速のパフォーマンスを維持し、データの分類の必要性を低減

自己暗号化ドライブは、インターフェイスの最大転送速度を満たす専用の暗号化エンジンを搭載しています。SED の暗号化エンジンはコントローラ ASIC 内にあります。個々のドライブ・ポートは、ポートの最大速度を満たす専用の暗号化エンジンを使用します。暗号化によってシステムの動作が遅くなることはありません。

SED のパフォーマンスは、直線的かつ自動的に拡張します。ドライブが追加されると、暗号化の帯域幅も同様に拡張されます。データ・センター管理者は、アレイにドライブを追加したり、データ・センターにアレイを追加する際に、暗号化の負荷分散の心配をする必要はありません。

SED では、パフォーマンスを低下させることなくすべてのデータを暗号化できるため、暗号対象を選別するためにデータを分類する必要がほとんどなくなります。従来は、このデータの分類作業に多大な労力を費やしていました。さらに、分類されたデータが、データ保護されている環境から保護されていない環境にコピーできる場合は、これらのデータの管理が困難になります。SED の導入により、データを分類する必要性が減ることで、データ・センターでの暗号化の管理は大幅に簡略化されることになります。

効率的な圧縮および重複排除の維持

ストレージ・システムのデータ圧縮および重複排除の機能は、ストレージ・コストを大幅に削減する方法を提供しますが、データの圧縮と重複排除を実行するときに、データが暗号化されておらず、ストレージ・システムが暗号化されていないデータに最適化されている場合だけです。SED を使用すると、効率的にデータの圧縮と重複排除を行うストレージ・システムの機能は完全に維持されます。

データ保全性の保護情報における標準仕様の維持

SED は、将来のデータ保全性である PI をサポートしています。PI（Protection Information、Data Integrity Feature とも呼ばれる）は、T10 SCSI ベースのエンドツーエンドデータ保護仕様です。この SCSI プロトコル標準を SAS システムおよびファイバ・チャネル・システムに実装することにより、データ・パスの各エレメントはデータを検査してデータの破損が起きていないことを確認できるようになります。これはデータに付属された特別な情報を使用して実行されますが、エレメントを通過するデータが暗号化されている場合には実行されません。

SED はデータ・パスの終端で暗号化を実行するので、SED が、データ・パス全域での PI をサポートする唯一のソリューションとなります。この優れたデータ保全性を実現する一方で、SED はハードディスク・ドライブの信頼性、可用性、保守性、保証などに影響を与えません。

標準化されたテクノロジーによるコストの削減

ハードディスク・ドライブのトップ 6 社（富士通、日立、Samsung、シーゲイト、東芝、Western Digital）は、TCG（Trusted Computing Group）によって最近発表された最終版のエンタープライズ仕様を共同で策定しました。この仕様は、自己暗号化ドライブを開発および管理する際の標準規格として策定されたもので、異なるベンダーの SED の相互運用性の確保を実現します。相互運用性が確保されることにより、市場競争が加速され、ソリューション・ビルダーやエンドユーザ向けの価格はより安価になります。

いずれは、すべてのベンダーから出荷されるすべてのドライブが自己暗号化ドライブになると予測されます（これらのベンダーの半数はすでに SED を出荷しています）。これらのドライブによって、ハードディスク・ドライブが所有者の管理から離れた際のデータ漏洩リスクは、今後無くなるものと考えられます。

サーバ、NAS、およびSANアレイ向け自己暗号化ドライブ

結果として、自己暗号化ストレージは以下のような多様なデバイスを含むすべての終端で使用されるようになります。

- サーバ、SAN、NAS アレイ（仮想化または非仮想化）、RAID、JBOD、個別のドライブ
- テープ・ドライブ
- SSD
- デスクトップ PC 向けドライブ
- ノート PC 向けドライブ
- ポータブル・ドライブ

再暗号化の必要性の低減

認証キーと暗号キーを分離することで、ドライブの所有者にとってはいくつかの管理上の利点があります。セキュリティ上の理由からユーザはパスワードを定期的に変更しますが、SED の場合は、暗号キー自体が暗号化され、ドライブを離れることがないため、データ・センター管理者は暗号キーを定期的に変更する必要はありません。これにより、労力を必要とするデータの復号化や再暗号化を行う面倒な作業をなくすことができます。

認証キーは、管理者が会社を退職したときなど、再暗号化することなく、いつでも変更できます。ストレージ管理者が替わった場合でも、暗号化されたデータに影響を与えることなく、ストレージへのアクセス権限はそのまま引き継がれます。

対照的に、コントローラおよびファブリックベースの暗号化では、データ暗号キーは、安全に格納するためのキー・マネージャと暗号化が実行されるポイントの間を移動し、キーのエスクローが必要になります。これらのデータ暗号キーは、認証キーほどセキュアではありません。そのため、定期的にキーを再生成する必要があり、パフォーマンスが大幅に低下するデータの再暗号化が必要になります。

移動中のデータの物理的な保護またはセッション暗号化

NAS に接続されているイーサネットであろうと SAN 上のブロック・レベルのデータであろうと、ファイル・システム上を移動する大量のデータのほとんどは、物理的に IT ストレージ管理者の管理下に置かれておりセキュリティのリスクがあるとは考えられていません。

物理的に IT ストレージ管理者の管理下に置かれていないファイル・システムのネットワークを経由してデータを移動する場合、ネットワーク上で転送されるデータを暗号化するために最も広く採用され、確立されている方法は短期セッション暗号キーを使用する方法です。単一の転送は、転送完了後に即座に削除されるセッション・キーで暗号化できます。また、後続の転送は新しい異なるセッション・キーによって保護されます。ハードディスク・ドライブのデータを暗号化するために使用する長期間有効となるキーとは異なり、短期間のみ有効となるキーはデータの脆弱性を最小化することができます。

セッション暗号化を使用する 3 つのシナリオ

シナリオ 1

データ・センターを離れて、ディザスタ・リカバリ用に SAN を遠隔地のオフィスや別の場所に拡張する、ファイバ・チャネルのファブリック接続では潜在的なリスクがあります。このような場合、FC over IP および IPsec によるデータの保護を使用してセキュリティに対応します。

シナリオ 2

ルーターおよびスイッチは IPsec のようなテクノロジーを使用して WAN を経由する SAN の保護および接続を行います。この種のセキュリティの脅威に対応する場合、スイッチおよびルーターが IPsec によるデータ暗号化をサポートしている限り、ホストベースまたはアダプタベースの暗号化は必要ありません。ファイバ・チャネル・テクノロジーでは 10km 程度の距離までしか届きませんが、IT 管理者は国境を越えるような距離でのデータの共有、保護、および移動が必要になることがあります。QLogic 社は、IP を介して SAN のトラフィックを転送できるルーターとスイッチを提供しています。これにより、WAN 経由の SAN 接続が可能になります。

サーバ、NAS、およびSANアレイ向け自己暗号化ドライブ

シナリオ 3

IP を使用して SAN をインターネットまたは専用回線まで拡張する場合、IPsec によるセキュリティがこれらのリモート接続上で使用されます。これにより、長距離を移動するデータが保護され、データのレプリケーション（複製）および SAN データ・デバイスの共有がサポートされ、確かなバックアップとビジネスの継続性が実現されます。WAN 接続では、短期的なキーでの SSL（Secure Sockets Layer）が使用されます。これにより、接続がセキュアに維持され、キーが長期間露呈されることがなくなります。

ファブリックに物理的なセキュリティ保護があるかどうかに関係なく、ハードディスク・ドライブが所有者の管理から離れた場合には、ドライブ上のデータをセキュアに保護する必要があります。上記で説明したセッション・セキュリティを使う代わりに、ハードディスク・ドライブのデータをセキュアに保護するファブリックでの暗号化を使用する方が、ハードディスク・ドライブだけではなくファブリックを移動するときにも暗号化されるので、長期的には適切なソリューションであるように思われるかもしれません。しかし、この方法には根本的な欠陥があります。それは、単一の暗号キーのみによって暗号化された大量のテキストが露呈される一方、長期間有効となる暗号キーも露呈されることで、セキュリティを向上させるのではなく、むしろ低下させ、より複雑化させています。

データの移動中も暗号化が必要な場合は、IPSec または FC over IP を使用してください。前の項で説明している理由により、ドライブ上の暗号化データは、ドライブ自体で最もその効果を発揮します。

その他の情報

ストレージ・セキュリティの詳細については、Trusted Computing Group: www.trustedcomputinggroup.org

Storage Networking Industry Association（SNIA）Storage Security Industry Forum（SSIF）: www.snia.org/forums/ssif/knowledge_center をご覧ください。

Self-Encrypting Drive ホワイト・ペーパー、Webcast およびパフォーマンス・デモ・ビデオについては、www.SEDSecuritySolutions.com をご覧ください。

南北アメリカ　Seagate Technology LLC 920 Disc Drive, Scotts Valley, California 95066, United States, 831-438-6550
アジア / 太平洋　Seagate Technology International Ltd. 7000 Ang Mo Kio Avenue 5, Singapore 569877, 65 6485 3888
ヨーロッパ、中近東、およびアフリカ　Seagate Technology SAS　130–136, rue de Silly, 92773, Boulogne-Billancourt Cedex, France 33 1-4186 10 00

TP600.1-0903JP、2009 年 3 月