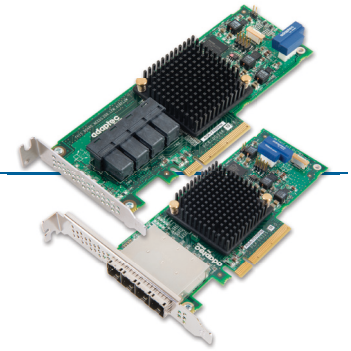
Adaptec maxCrypto：ラインレート速度で優れたオンザフライのデータ暗号化



はじめに

企業は、顧客情報、機密の会社書類やコミュニケーション、財務記録、従業員給与の記録、およびその他の機密データを保護しようとするため、データセキュリティは、データセンタやクラウドコンピューティング環境において最優先事項の一つとなっています。

データセンタ管理者は、ウェブサービスやファイルサービス、データベース、オンライントランザクション処理（OLTP）、Microsoft Exchange Server、および高性能コンピューティング(HPC)といった大規模アプリケーションのために絶えず増加しつづける性能要求を満たしながら、データを保護しなければならないという課題に直面しています。

データセキュリティへの脅威

セキュリティへの取り組みは従来、インターネットベースの脅威からデータを保護することに焦点を当ててきましたが、データセンタは、もはやいくつかの一般的なシナリオによって提示される物理的なセキュリティの脅威を無視することはできません。

ストレージドライブの処分

ストレージデバイスが回収される際は、ゴミ箱あさり（ダンプスターダイビング）泥棒対策として、データへのアクセスを不能状態にする必要があります。これを行うには2つの方法があります。

第1の方法はデータワイピング(消去)で、ドライブ全体へ不要なデータを書き込む方法です。これにより、有用なデータに上書きします。上書きされるデータは、一般的にはゼロの連続だったり、様々なランダムパターンだったりします。ストレージデバイスの大きさや速度によりますが、この処理に数時間かかることがあります。サーバ全体が回収される場合は、接続されているすべてのドライブからデータを消去するのに数日かかる場合があります。さらに、ハードディスクドライブ（HDD）とソリッドステートドライブ（SSD）のように、異なるストレージデバイスでは異なるツールや異なるデータ消去方法が必要となるかもしれません。

第2の方法は、ハンマーやシュレッダー、または他の破壊ツールを使用してデバイスを物理的に破壊することです。しかし、これもまた、プロセスを完了すまでに時間がかかる可能性があり、処理がしっかり行われていない場合には、回収されたデバイスから、精通した泥棒がデータを収集できる結果となる場合も考えられます。

故障ドライブの返却

ストレージデバイスが故障して交換のためにベンダーへ返却する必要がある場合には、機密データはストレージデバイスから取り除かれるべきです。これは、動作不能となったデバイスからのデータを消去してから廃棄するというシナリオと同じ課題をもたらします。

盗難

ファイアウォールやその他のネットワークセキュリティツールは、ハッカーからデータを安全に保つために非常に効果的ですが、物理的な盗難（不正者によるストレージドライブの窃盗）の脅威が残っています。

前述のそれぞれの状況に理想的なソリューションは、ドライブ上のデータを操作する方法です。それによって、例えデータを見る権限のない誰かがデータを調べようとしても、データが読めない、あるいは役に立たないようにすることができます。

データ暗号化

暗号化は唯一、許可された関係者のみが読み取ることができるように情報を符号化する方法です。情報は、暗号キーを用いて符号化され、復号キーがなければ誰も読むことはできません。暗号化には、対称型および非対称型の2種類があります。

対称暗号化では、同じキーが暗号化と復号化の両方に使用されます。もし、キーが傷つけられると、セキュリティは壊されます。したがって、このモデルにおける暗号キーの管理は重要かつ複雑なプロセスとなります。

非対称暗号化では、暗号化と複合化で別々のキーを使用します。復号化キーはハードウェア内で非公開にしますが、暗号化キーはソフトウェアでの実装により公開することができます。このモデルでは対称型暗号化よりも高いレベルのセキュリティを提供します。

ハイライト

- HDDとSSD用のAdaptec maxCryptoデータ暗号化
- 6Gb/秒アダプテック7Heシリーズ HBAファミリで利用可能
  - 1つのHBAで複数のドライブを暗号化し資本コストと展開の複雑さを削減
  - 既存のデータセンタインフラストラクチャやすべてブランドのHDD、SSDとの互換性
  - データセンタは会社全体にわたって均一で拡張性のある戦略が展開可能に
- オンザフライでのハードウェアベースの暗号化
  - レイテンシへの影響を最小限に抑えたラインレート速度
  - キー管理用ソフトウェア不要
  - 暗号化キーはOSから独立しているため、ウイルスやその他の攻撃からの脅威を排除
- 最高の暗号化と機能
  - 業界をリードするInfineon SLE95050暗号化デバイス
  - 256ビットAES暗号化
  - 先進の楕円曲線暗号（ECC）対数
  - 非対称キー認証
- ディスクのデータサイズおよびデータ構造を維持
  - 使用可能ディスク容量やメインテナンス技術への悪影響なし

Adaptec maxCrypto：ラインレート速度で優れたオンザフライのデータ暗号化

暗号化プロセスには、ソフトウェアベースまたはハードウェアベースがあります。ソフトウェアベースの暗号化では CPUにより実行されますが、ハードウェアベースの暗号化では、ドライブ上またはストレージHBAカード上にあるスタンドアロンのチップセットにより実行されます。

ソフトウェアベースの暗号化

ソフトウェアベースの暗号化は、ドライブから読み込んだり書き込んだりするときにデータの暗号化と復号化を実行するアプリケーションを使用し、オペレーティングシステムによって管理されています。

ソフトウェアベースの暗号化の利点

- 通常、データ暗号化で最も安価なオプション
- ソフトウェアアプリケーションは主要なオペレーティングシステムで利用可能で、HDDおよびSSDのほとんどのブランドで動作する

ソフトウェアベースの暗号化の欠点

- 暗号化/復号化プロセスがCPUレベルで行われるので、ストレージシステムにレイテンシが追加される
- ソフトウェア暗号化を実行しているOSは、ウイルス、クラッシュやその他の脅威に対して脆弱

ハードウェアベースの自己暗号化ドライブ（SED）

自己暗号化SSDまたはHDDでは暗号化/復号化プロセスは、暗号化/復号化キーを含むチップセットを使用することにより、CPUやOSとは独立して実行されます。

SEDの利点

- 暗号化キーはOSから独立しており、ウイルスやその他の攻撃からの脅威を排除
- 専用ハードウェアが暗号化処理を行い、レイテンシやI/O性能に顕著な影響を与えない

SEDの欠点

- 新しいSEDを購入し（通常は非SEDよりも高いコストで）、展開する必要あり
- システム全体を保護するには、すべての既存のHDDとSSDをSEDに交換する必要あり
- HDDとSSDのベンダーで現在利用可能なオプションは限られている
- 既存の非暗号化ドライブから現在のデータを新しいSEDへ転送する必要あり
- 複数のSEDを管理するには統合されたキー管理ソフトウェアソリューションが必要
- 一部のSEDは取り外し不能キーを含むため、ドライブの処分またはベンダーへ返却する場合にデータが脆弱なままとなる

ストレージHBAによるハードウェアベースの暗号化

SEDのシナリオと同じく、暗号化対応のストレージHBAは、暗号化/復号化処理を行うオンボードのチップセットを搭載しています。

暗号化対応のストレージHBAの利点

- 暗号化キーはOSから独立しており、ウイルスやその他の攻撃からの脅威を排除
- 専用ハードウェアが暗号化処理を行い、レイテンシやI/O性能に顕著な影響を与えない
- データセンターの既存のインフラストラクチャやHDDとSSDのすべてのブランドと互換性があるため、現在のドライブをベンダーのSEDと交換する必要なし
- 一つのHBAで多数のドライブを暗号化でき、資本費用と展開の複雑さを削減
- ストレージHBAは通常、HDDやSSDより寿命が長く、頻繁に交換する必要がないため、さらなる資本費用を削減
- 統合されたキー管理ソフトウェアは不要

暗号化対応のストレージHBAの欠点：

- 既存のストレージHBAを暗号化対応のHBAへ交換が必要
- 暗号化でドライブの消去が実行されるため、もし、ドライブ上の既存のデータを保持したい場合には、暗号化を有効にする前に、必ずバックアップを実行する必要あり

Adaptec maxCrypto

6Gb/秒のAdaptec 7Heシリーズホストバスアダプタ（HBA） ファミリで利用可能なAdaptec maxCryptoハードウェア暗号化は、最高レベルのオンザフライのデータ暗号化/復号化をラインレート速度で提供し、レイテンシへの影響を最小限に抑えます。

Adaptec maxCryptoは業界をリードするInfineon SLE95050暗号化デバイスを搭載し、先進の楕円曲線暗号（ECC）対数と非対称キー認証を使用して優れた暗号化と機能性を提供します。キー管理ソフトウェアを必要としないため、データセンタが企業全体で均一で拡張性のある暗号化戦略を展開することを可能にします。

maxCryptoはHBAベースなので、既存のストレージインフラストラクチャと互換性があり、新しいHDDやSSDにする必要はありません。Adaptec 7Heは、しかしながら、テープや他の非ダイレクトアクセスデバイス上のデータは暗号化しません。暗号キーが外された場合には、HBAはテープをサポートします。また、RBOD用のマルチLUNサポートはまだ利用できませんが、暗号化はRBODと他のすべてのダイレクト·アクセス·デバイスのLUN0上で動作します。

Adaptec maxCryptoは、ディスクのデータサイズを変更せず、データ構造も変更しないので、使用可能なディスク容量や重複排除などのメインテナンス技術に対してマイナスの影響が全くありません。

Adaptec maxCryptoキーの使用例

各maxCryptoキーは、唯一の暗号キーと共に製造されます。Adaptec 7He HBAには、メディアストレージ用の携帯電話で使用されるものと同様のクリップインソケットが実装されています。

Adaptec maxCrypto：ラインレート速度で優れたオンザフライのデータ暗号化

物理的にスロットにキーを挿入する、または検出することにより、暗号化を開始します。接続されているすべてのドライブは、同じ暗号化の状態を共有します - すべてが暗号化されるか、またはどれも暗号化されないかのどちらかです。 HBA BIOSは暗号化が有効になっているか無効かをを示すので、物理的にキーがインストールされているかHBAを検査しなくても暗号化の状態を確認することができます。

下記の表は、様々なシナリオでmaxCryptoキーを挿入、取り外し、交換した場合の結果を説明しています。

maxCryptoで暗号化されたHDDとSSDのデータは、キーなしでは役に立たないので、maxCryptoは、本文で既に述べた物理的なセキュリティの脅威に対処することができます： 寿命になったドライブは長時間のデータ消去処理せずに廃棄でき、故障したドライブもデータ漏洩の心配なくベンダーへ返すことができます。ドライブが盗難された場合でも、泥棒は、ハードウェアの一部を得ることができるだけで、その上に保存された貴重なデータは得ることはできません。

結論

データセンタは、顧客のID、会社の通信、財務記録などの機密データを保護するという、増加し続ける責任に直面しています。彼らは、インターネットベースの脅威に注目するにとどまらず、彼らのHDDやSSDに対する物理的なセキュリティリスクをも考慮しなければなりません。

データセンタがベンダーへ故障したドライブを返す時や長時間のデータ削除処理しないでドライブを廃棄する場合、ドライブが窃盗されやすい環境にある場合などはデータ漏洩の可能性があります。データが格納される時に暗号化することにより、データセンタは、データが格納されているドライブを有している場合であっても、権限のない者がデータを読み取ることができないことを保証することができます。

ソフトウェア暗号化は、コスト重視のソリューションですが、パフォーマンスの問題を引き起こし、ウイルスや、OSのクラッシュに対して脆弱です。自己暗号化ドライブ（SED）は、高性能なハードウェアベースのソリューションを提供していますが、大きな設備投資や管理が必要です。

ストレージHBAでの暗号化プロセス設置は、SEDよりも低い設備投資と容易な管理でハードウェアベースの暗号化の利点を提供します。

Adaptec maxCryptoは6Gb/秒 ホストバスアダプタ(HBA）のAdaptec 7Heシリーズファミリにハードウェアベースの暗号化を統合しており、レイテンシへの影響を最小限に抑えながら最高レベルのデータ暗号化/復号化を提供します。これは既存のストレージインフラストラクチャにシームレスに統合し、データセンタが企業全体で均一で拡張性のある暗号化戦略を展開するのを可能にします。

初期状態	暗号化済み？	アクション	結果
maxCryptoキー無しHBA	いいえ	maxCryptoキーを挿入	既存データを削除*, 新規データを暗号化
maxCryptoキー無しHBA	いいえ	maxCryptoキー無しのHBAへ交換	データは暗号化されない
maxCryptoキー無しHBA	いいえ	maxCryptoキー有りのHBAへ交換	既存データを削除*, 新規データを暗号化
maxCryptoキー無しHBA	いいえ	サードパーティHBAへ交換	データは暗号化されない
maxCryptoキー有りHBA	はい	maxCryptoキーを取り外し	既存データを削除*, 新規データは暗号化されない
maxCryptoキー有りHBA	はい	maxCrypto キーの故障	既存データを削除*, 新規データは暗号化されない
maxCryptoキー有りHBA	はい	maxCryptoキーを新しいmaxCryptoキーと交換	既存データを削除*, 新規データを暗号化
maxCryptoキー有りHBA	はい	最初のmaxCryptoキーを入れた新しいHBA へ交換	既存暗号化データはそのまま残り､続けて暗号化
maxCryptoキー有りHBA	はい	新しいmaxCryptoキーを入れた新しいHBA へ交換	既存データ削除*, 新規データを暗号化
maxCryptoキー有りHBA	はい	サードパーティHBAへ交換	既存データを削除*, 新規データは暗号化されない

*ユーザ確認後

adaptec by PMC
ピーエムシー･シエラ･ジャパン株式会社
チャネルストレージ事業部
〒164-0003 東京都中野区東中野5-5-5
徳舛ビル4階

お問い合わせ先: www.adaptec.co.jp/contact

Copyright PMC-Sierra, Inc. 2013. All rights reserved. PMC、PMC-SIERRA、Adaptec は、PMC-Sierra, Inc. の登録商標です。「Adaptec by PMC」は PMC-Sierra, Inc の商標です。その他、使われているすべての製品や会社名は、各権利所有者による商標の可能性があります。情報は印刷された時点において、正確であると確信していますが、本書中の誤記や情報の抜けに起因する結果に関して何ら責任を負うものではありません。また、記載された製品の仕様や情報等は予告無しに変更される可能性があります。

Part Number: TB_maxCrypto_071113_JA