ストレージ システム内の重要企業データを保護するために

著者: Marc Anthony

お客様のデータは不正アクセスに対してどの程度安全に保護されていますか?
サイバー攻撃は驚異的な勢いで企業に脅威をもたらしています。ハッカー達はますます高度なツールとテクニックを使ってネットワークの防御をかいくぐり、重要な企業情報を盗み取ろうとします。

サイバー犯罪の増加により、システムを保護すると同時に高まり続ける性能への要求を満たす事が、データセンター事業者にとってかつてないほど重要な課題となっています。

不適切なサイバー セキュリティによって生じる損失
業績の悪化、ブランド力の低下、顧客からの信頼の喪失から企業を保護するためにデータセキュリティが重要である事は、各種の調査により示されています。

- 68%の大企業は、サイバー セキュリティ問題が増加していると認識しています(出典: Accenture)。
- 2020 年上半期において 3600 万件の情報がデータ漏洩により外部へ暴露されました(出典: RiskBased)。
- データ漏洩の平均損失額は事件あたり$386 万であり、収益の損失がその 40% ($152 万)を占めます(出典: IBM)。
- 顧客の 70%は、データ漏洩が発生した事業者の利用を停止すると述べています(出典: Gemalto)。

以上の通り、セキュリティを疎かにする事は決してできません。特にサービス プロバイダ、データホスト、ビジネス パートナーとして信用を得るには、データセキュリティが極めて重要です。

データセンター インフラストラクチャを保護するには複数の重複した戦略が必要です。これにはサプライチェーンのセキュリティ、信頼できるプラットフォームのサポート、実行中のデータセキュリティ、データのライフサイクル管理が含まれます。このような包括的ストラテジの鍵となるのが、保存データ(data-at-rest)のセキュリティです。

保存データ セキュリティのタイプ
HDD および SDD ドライブ内の保存データへの不正アクセスを防ぐ方法は各種ありますが、暗号化が最も効果的です。暗号化は、一意鍵を使わない限り解読できないようにデータをコード化します。データの暗号化処理は、ソフトウェアまたはハードウェア方式で実行できます。

- **ソフトウェア方式の暗号化**は、オペレーティング システムレベルでアプリケーション ソフトウェアを使って、ドライブへの書き込み時にデータを暗号化し、ドライブからの読み出し時にデータを復号します。ソフトウェア暗号化は、主なオペレーティング システムと全メーカーの HDD および SDD で使えます。このソフトウェア アプローチは計算負荷が高いため、I/O レイテンシが増加する事により I/O 性能は低下します。処理能力が不足している場合、メイン CPU 上で動作する他のアプリケーションの性能が低下します。

- **自己暗号化ドライブ(SED)**は、データの暗号化/復号を内部のハードウェア でサポートします。この暗号処理はレイテンシまたは I/O 性能に対してほとんど(または全く)影響を及ぼさず、ホスト オペレーティングシステムまたはホスト CPU に対して透過的に実行されます。しかし、既存の HDD および SDD を SED に交換する必要があるため、費用がかかる上にシステムが複雑化します。

- **暗号対応ストレージ アダプタ**は、内部のハードウェアを介して暗号化/復号を管理します。この方式はストレージ サブシステム (アダプタ キャッシュ、接続ケーブル、エクスパンダを含むドライバまでの全経路)上のデータを保護します。暗号処理はホスト オペレーティング システムとホスト CPU に対して透過的に実行され、レイテンシまたは I/O 性能に対する影響は極小です。暗号対応ストレージ アダプタは標準的な SSD および HDD をサポートし、1 つのアダプタで複数のドライブを暗号化できるため、システムの複雑化とコストを抑える事ができます。

暗号化の実装方法を適切に選定するには、最先端セキュリティ技術を提供可能な信頼できるパートナーが必要です。

Microchip 社: ストレージ デバイスのトップ サプライヤ
Microchip 社は、30 年以上にわたってお客様のニーズに応えるストレージ製品を提供してきました。弊社のストレージ製品はデスクトップ PC 用から始まり、現在は世界トップクラスのデータセンター パートナーに提供しています。お客様がデータセンターの性能と可用性を最適化できるよう、弊社はデータセンター業界およびエコシステム ベンダーと密接に連携し、他社製ストレージとの相互動作性と統合性を最大限に高めたクラストップ レベルのテクノロジとツールを提供しています。弊社の SmartROC/IOC シリコンベース HBA および RAID アダプタは、世界中の 3000 万以上のサーバで使われています。

Adaptec® maxCrypto 対応 SmartRAID 3162-8i /e RAID アダプタは、業界で唯一のコントローラ ベース暗号ソリューションです。このソリューションは 256 ビット AES インライン暗号化を採用する事により、高度な暗号処理を提供します。特定のコントローラに割り当てられた一意鍵が削除されると、ドライブに保存されたデータは即座に解読不能な安全な状態になります。

maxCrypto 対応 SmartRAID 3162-8i /e RAID アダプタは、1 つで最大 238 台の SAS または SATA デバイス(SAS エクスパンダを使用)のデータを保護でき、レイテンシと I/O 性能にはほとんど影響を及ぼしません。maxCrypto は RAID ボリュームをサポートする全メーカーの SAS および SATA HDD および SSD をサポートし、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できます。

まとめ
ハッカーによる企業データの窃盗はこれまで以上に激化しており、常に最先端の高度な保存データ保護ソリューションが求められます。暗号化ソリューションには各種の選択肢が存在しますが、ソフトウェア方式はアプリケーションの性能を低下させる一方、SED 方式は既存の HDD/SSD を交換する必要があるためコストがかかります。

Adaptec maxCrypto アダプタは業界で唯一のコントローラ ベース暗号ソリューションであり、ソフトウェア方式よりも性能的に優れる上に SED 方式よりも柔軟で安全です。弊社の maxCrypto 対応 SmartRAID 3162-8i /e RAID アダプタは、最大で 238 台の SAS または SATA デバイス内のデータを保護できます。maxCrypto は全メーカーの SAS および SATA HDD および SDD をサポートし、既存のインフラストラクチャにシームレスに統合できます。

Microchip 社の Adaptec maxCrypto 対応アダプタの詳細は、こちらでご覧ください。