

高性能FerriSSDs®

サイバーセキュリティ向けに 高度なデータ保護を実現する方法

ネットワーク、インフラの発達、アーキテクチャの複雑化によって狙いすましたサイバー攻撃が増大しています。

攻撃の巧妙化に対して検知能力が追い付かず、情報セキュリティ管理、必要要件、脅威そのものにも追いつくのが困難になっています。

セキュリティはサイバーセキュリティ会社に最重要です。事前対策として、ハッキングや不正アクセスに強く、防御可能なハードウェアを確保しておく必要があります。

Silicon Motion FerriSSD ドライブは最新の業界規格に適合したハードウェアベースのセキュリティに、追加の防御措置を組み込んでいます。これにはデジタル署名付きのファームウェアや、アラート発生からディスク上の全コンテンツの消去まで、といった改変応答が含まれています。

Silicon MotionのFerriSSDは、サイバーセキュリティ向けの高度なセキュリティ機能を実現 生活の一部になっているデータを保護

データセンターサーバー、コネクテッドカー、医療機器、ゲームシステム、産業用コントローラ、監視システム、小売り技術などの産業用コンピューティングは、現代の生活や仕事を可能にするために必要なシステムのほんの一部に過ぎません。システムのメモリに保存されたデータによって、ユーザー、組織、顧客に関する情報が明らかになるため、悪用されると損害が発生する可能性があります。データへのアクセスを企む者は、口座番号やクレジットカード番号などの金銭に関する情報の不正入手、企業の機密データや医療記録などの個人情報の発見、知的財産の盗難、設備や業務の妨害など様々な動機を持つ可能性があります。

ハッカーを排除し、貴重なデータを安全に保つことは、進化し続ける課題です。サイバー脅威はますます巧妙になり、また予測や感知が難しくなっています。今日、ネットワーク接続の普及と「常時化」そしてコネクテッドカーなどの新しいアプリケーションのモバイル化により、ハードディスクドライブ（HDD）やソリッドステートドライブ（SSD）などの大容量記憶媒体に保存されたシステムやユーザーのデータは、攻撃に対して脆弱になっています。

サイバーセキュリティエンジニアリング用フレームワークの確立

データへの不正アクセスを防止し、盗難や悪用から保護するためには、各種保護対策が必要です。これらの対策が目的にかない、かつ適切に実施されていることを確認するために、業界および規制機関は、新製品開発の中心にサイバーセキュリティを据える枠組みを確立しています。一例として、自動車業界の規格であるISO/SAE 21434:2021「自動車－サイバーセキュリティエンジニアリング」があります。これは、国際連合欧州経済委員会（UNECE）の国際規則UN155と密接に関連しており、製品開発者に認定されたサイバーセキュリティ管理システムを導入することが求められています。

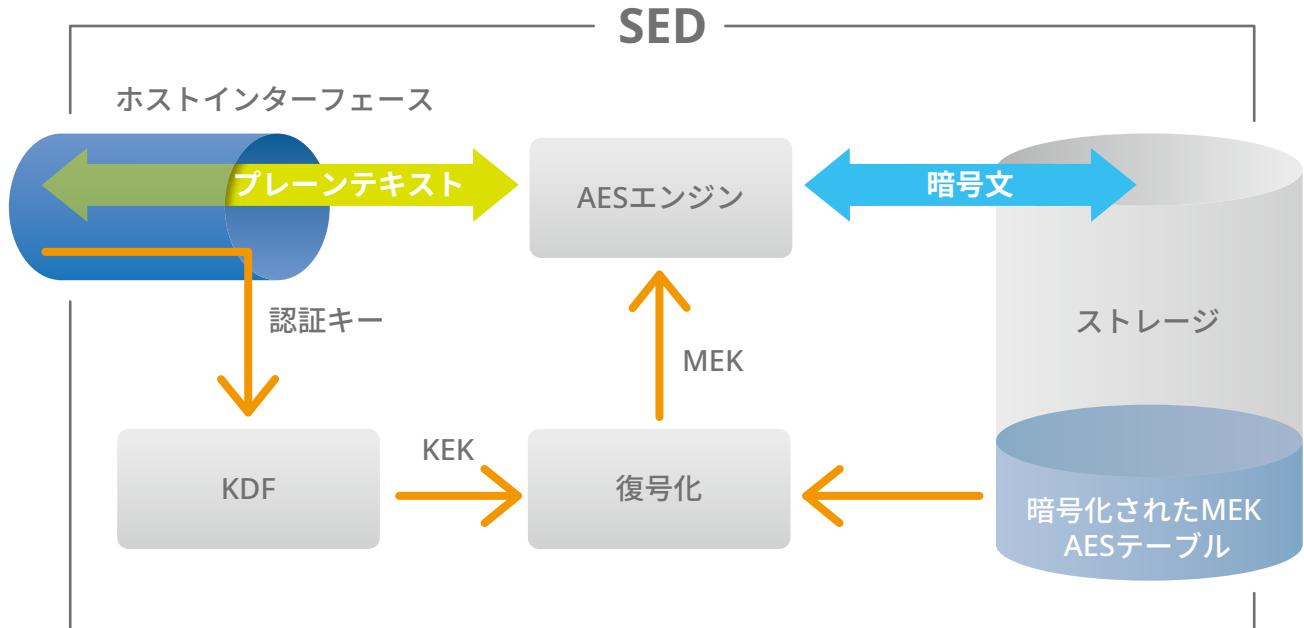
ISO/SAE 21434の適用範囲は、製品の設計から製造終了までの製品ライフサイクル全体をカバーしており、脆弱性の分析や現状最強のサイバーセキュリティ確保すべくセーフガードの設置も含まれています。リスク評価、サイバーセキュリティの脆弱性の特定と対処、リスクを軽減するアプリケーションやソフトウェア、ハードウェアのコンポーネントのテストなどの対策が必要です。車載電子システムのコンプライアンスは、2024年から2026年中に義務化される見通しです。Silicon MotionはSGSと提携して、すべてのプロセスをISO 21434に準拠し、2023年第4四半期までにサードパーティによる認証を取得する予定です。



インテリジェントガード - 暗号化：セキュリティの最前線

SSDは大容量ストレージとしての採用が進んでいます。可動部品がないため、静音性、高信頼性、堅牢性、低消費電力などの利点があります。さらに、高速のデータ読み取りと書き込みが可能なため、高速レスポンスと高いシステム性能を両立できます。ハッカーがデバイスに物理的にアクセスしてSSDデータを盗んだり、妨害したりする場合のプライバシー保護のため、ユーザーデータを暗号化することが一般的です。従来のフルディスク暗号化は、オペレーティングシステム内のソフトウェアモジュールによって実行されます。データは暗号化された状態でディスクから取り出され、PCIe/SATAインターフェースで転送後、コンピュータ内で復号化されます。

これに代わり、自己暗号化ドライブ（SED）は、暗号化および復号化を処理する独自のハードウェアを内蔵しています。オペレーティングシステム内のドライブコントローラは、ドライブの起動前認証、鍵の管理、TPM（Trusted Platform Module）などの安全なコンポーネントとのやり取りなどのプロセスを管理し、電源オン時にドライブ複合化のための認証情報を取得します。インターラクションは、ATコマンド、またはより一般的にはTCG（Trusted Computing Group）Opal規格で定義されたコマンドを使用して実行されます。MicrosoftのBitLockerは（ソフトウェアベースの暗号化の管理以外に）、追加のプロトコルとインターフェース仕様でOpalを使用してハードウェア暗号化されたSEDを管理できます。また、SEDの制御には独自のアプローチもあります。



ソフトウェアベースのアプローチとは異なり、SEDは瞬時に暗号化または復号化されるため、メインシステムのCPUの負担になりません。ディスクからデータを取り出す際には、ローカルで復号化され、暗号化されていない状態でPCIe/SATAインターフェースを経由してコンピュータに転送されます。モバイルデバイスや携帯電話では、効率性の高いハードウェアベースのアプローチで、エネルギー利用率の向上とバッテリー寿命の延長に貢献します。

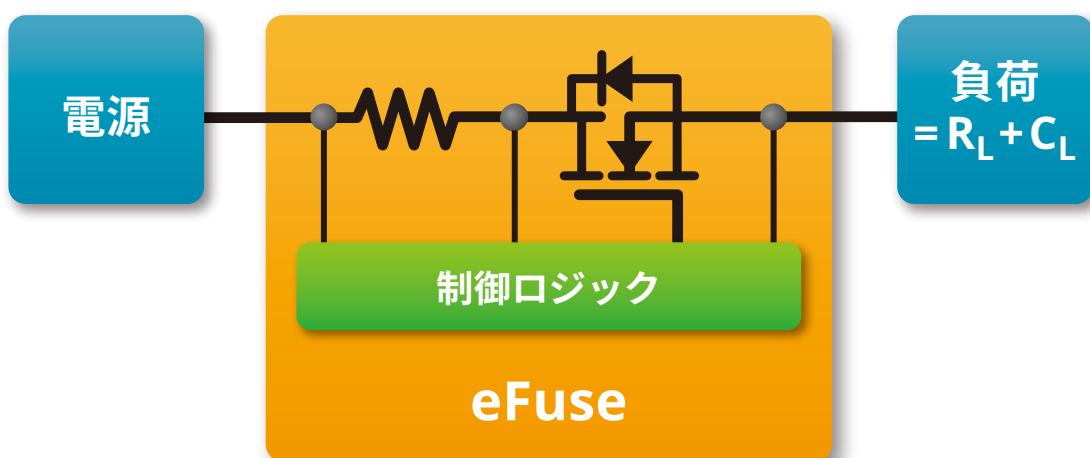
FerriSSDソリッドステートドライブは、最新のTCG規格であるOpal 2.0に準拠したハードウェア暗号化を実装しています。これにより、ディスクに保存されたデータへの不正なアクセスに対して、ドライブの安全性を可能な限り確保できます。フルディスク暗号化には、ブルートフォース攻撃への耐性に優れ、政府機関、金融機関、軍など採用されている業界標準の256ビット暗号アルゴリズム「AES-256」を使用しています。

しかし、暗号化だけでは、起こりうるすべての攻撃に対する包括的な保護を実現できません。FerriSSDには、追加属性で自己暗号化されたドライブに対して一般的に行われる種類の攻撃を阻止できる利点があります。

デジタル署名によるファームウェア保護

その他的一般的な攻撃には、悪意のあるファームウェアをロードしてSSDを制御しようとするものがあります。これは、ディスクに対して保存されているコンテンツの強制的復号化、機密データの露出、ランサムウェアが起動する可能性があります。この種の攻撃を防ぐため、FerriSSDは、システム起動時に安全なデジタル署名の提示を必要とするファームウェア保護を実装しています。署名は電子ヒューズ（eFuse）を使用して実行されますが、製造時にディスクに焼き付けられるため、不変です。eFuseはアクセス不能で、固有のパスワード以外では署名認証プロセスを完了できず、Ferri SSDを起動できません。署名認証でエラーが発生すると、システムはホストプロセッサにセキュリティ警告を送信します。

また、安全なデジタル署名により、FerriSSDユニットに対してリモートでファームウェア更新を実行できます。



データのリフレッシュによるインテリジェントスキャン

物理的な攻撃にも強い、実績に裏付けされたプロアクティブなデータ保存性能を証明

FerriSSDは、最大1TBの記憶容量を持ち、16mm×20mmの表面実装型BGAパッケージに格納されています。これは、メインデバイスの筐体内、ホストプロセッサの近くのカードやマザーボードに搭載することができ、従来の外付けSSDよりも物理的な改ざんから守ることができます。

ハッカーが予定外の緊急メンテナンスを装って標的を攻撃しようとすることもあります。FerriSSDはこのような活動を検知した場合、ホストプロセッサに警告を送信します。

さらに、すべてのFerriSSDは、妨害が検出された場合にすべてのデータを瞬時に消去できるセキュアクリック消去機能に対応しています。また、突然の電断などの不測の事態が発生した際に、ユーザーデータを安全に保存するためのデータフラッシュシーケンスを起動するハードウェアピンも搭載されています。

まとめ

ソリッドステートディスクは、省電力、コンパクト、高性能という利点を備えた大容量ストレージでありながら、産業用、医療用、車載用など様々な用途に対応する堅牢性を兼ね備えています。データを安全に保管するためには、メインOSに含まれるソフトウェアやディスク自体に組み込まれたハードウェアによるフルディスク暗号化が不可欠です。

Silicon Motionの先進的なFerriSSDはハードウェアベースの暗号化を採用していますので、メインシステムCPUの負荷を増やすことなく動作し、ポータブルアプリケーションの性能、エネルギー効率、バッテリー寿命を向上することができます。暗号化による保護を強化・補強し、今日のサイバー脅威に対して最も効果的なセキュリティを実現するため、FerriSSDはデジタル署名によるファームウェア保護、改ざん検知、深刻な物理攻撃時の緊急消去などの最新技術を追加導入しています。

FerriSSD® BGA SSDソリューション

仕様

ホストインターフェース	SATA Gen3 PCIe Gen3x2、Gen4 (Q1'23適用可能)
容量	SLCモード:10/20/40/80/160GB、320GB (Q1'23) TLCモード:32/64/120/240/480GB、960GB (Q1'23)
フォームファクタ	20mm × 16mm BGA
エコ製品	RoHs 準拠/無ハロゲン
対応温度	コマーシャル用温度 (0°C~70°C) 工業用温度 (-40°C ~ 85°C)

FerriSSD®モジュールソリューション

フォームファクタ・寸法

