ストレージ製品へのセキュリティ機能の実装

東芝デバイス&ストレージ(株)

近年、個人情報保護に対する要求の高まりから、ストレージ製品の情報セキュリティが重要性を増しています。当社のHDD製品は、個人ユースでのモバイル機器向け製品だけでなく、デジタル複合機向け製品やデータセンター向けをはじめとしたエンタープライズ製品など、各分野に適した製品をラインアップしており、各分野に合わせて適切な情報セキュリティ技術を備えたHDDを提供しています。

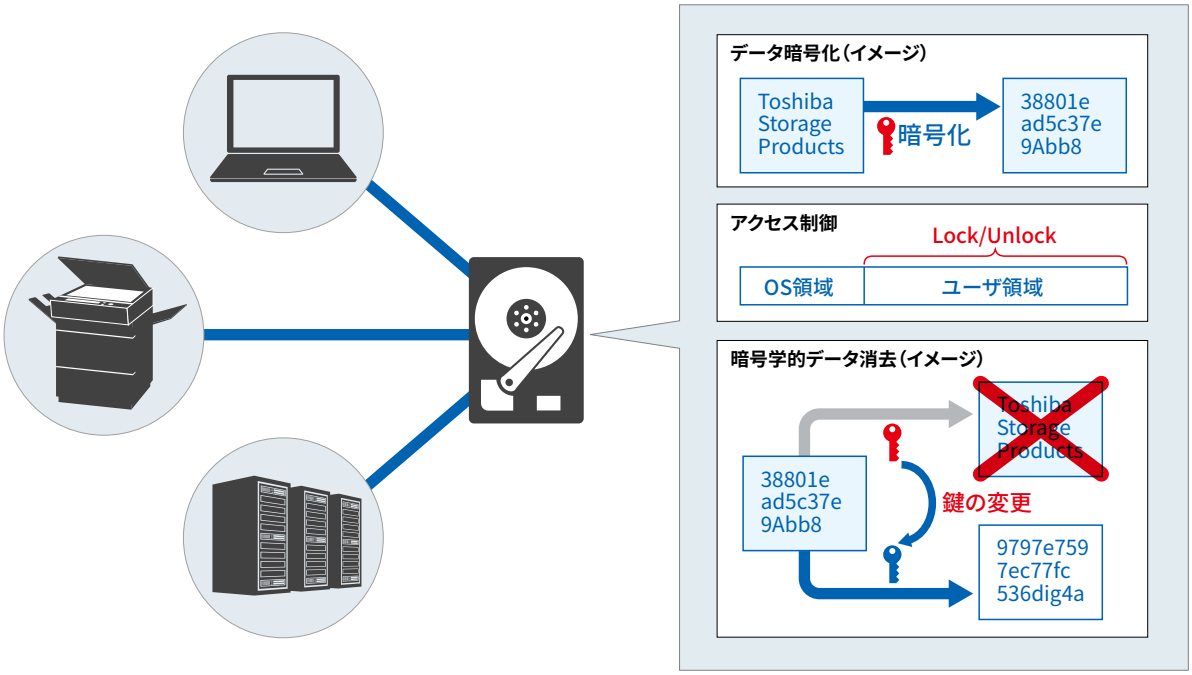
ストレージ製品に求められるセキュリティ要件として、まずHDDの盗難や紛失により発生するデータ流出の保護と抑止機能があります。また、廃却後にデータが流出することを防止するため、データを完全に消去する機能も求められています。

当社ではこうした顧客ニーズに応えるため、自己暗号化ドライブ(SED※1)を開発、提供しています。クラウドデータセンター用の大容量で高性能なニアラインHDDでは、データの書き込み時にHDD内で自動的に暗号化して保存します。データ暗号化にはNIST※2(アメリカ国立標準技術研究所)で定められた標準暗号規格であるAES※3を用いています。またATA※4Security Feature Set(ATA機の場合)やTCG※5 Opal SSC※6、TCG Enterprise SSCによるアクセス制御機能もサポートし、保護されたデータをパスワード認証なしに取得することを防止します。これら機能により、データ保護と流出抑止を実現しています。

さらに、廃却時のデータ完全消去についても、データの暗号化鍵を変更することで暗号学的に瞬時にデータ無効化できる技術(Cryptographic Erase)を搭載し、コストをかけてデータを上書きすることなく全データの無効化を実現しています。

当社 HDD の暗号アルゴリズム実装は、米国政府の FIPS PUB 140-3 に基づく暗号アルゴリズム試験 CAVP※7 を取得(A1637, A1638, A1645)しており、高い信頼性が保証されています。更に MG09*CP18/16TA※8 製品では、2020 年から開始された米国政府の暗号モジュール認証、FIPS PUB 140-3 に基づく CMVP※9 の取得も進めており、暗号モジュールとしての HDD 全体の設計、実装、動作を第三者機関により多角的に評価しています。

※1 SED: Self-Encrypting Drive
※2 NIST: National Institute of Standards and Technology
※3 AES: Advanced Encryption Standard
※4 ATA: Advanced Technology Attachment
※5 TCG: Trusted Computing Group
※6 SSC: Security Subsystem Class
※7 CAVP: Cryptographic Algorithm Validation Program
※8 MG09*CP18/16TA: MG09SCP18TA, MG09ACP18TA, MG09SCP16TA, MG09ACP16TA
※9 CMVP: Cryptographic Module Validation Program



ストレージ製品のセキュリティ機能のイメージ