Implementation of security features in storage products

Toshiba Electronic Devices & Storage Corporation

In recent years, with the growing demand for personal data protection, the importance of information security of storage products is increasing. Toshiba's hard disk drive (HDD) product lineup includes not only HDDs for personal mobile devices but also HDDs designed for various fields such as those for digital multifunction printers (MFPs) and enterprise HDDs for data centers and other operations. We offer HDDs incorporating appropriate information security technology to meet the needs of each field.

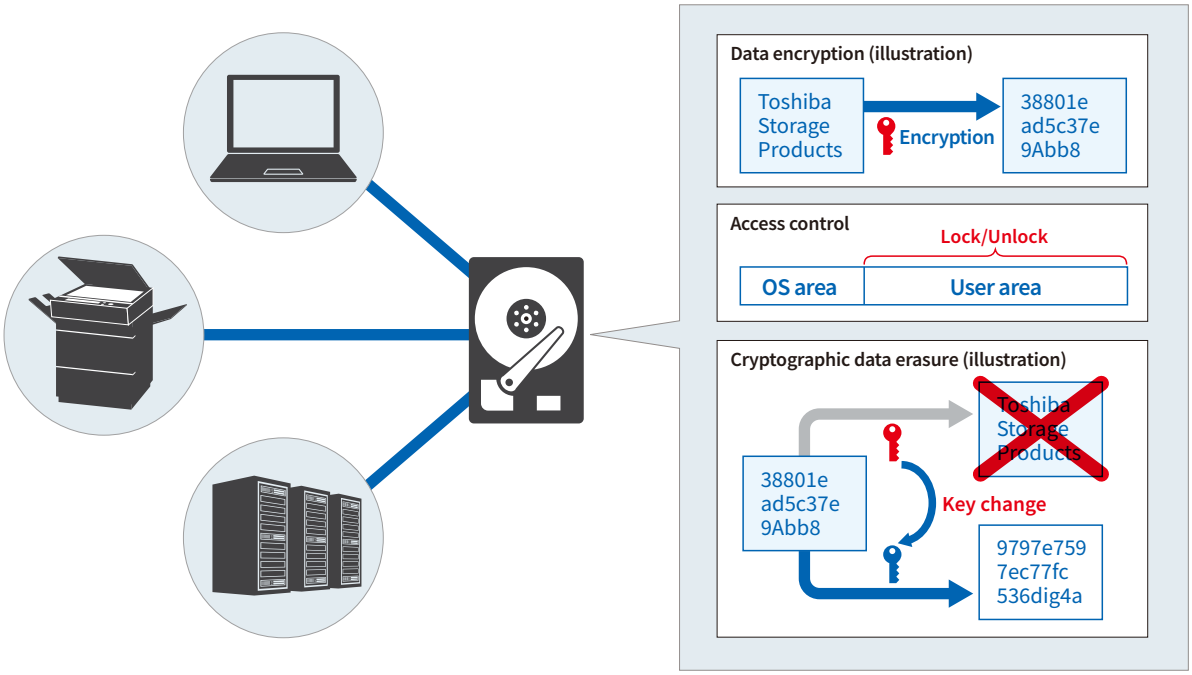
Security requirements for storage products include protection and deterrence functions to prevent data leakage due to theft or loss of HDDs. A function for completely erasing all data is also required for HDDs to prevent data leakage after disposal.

To meet these customer requirements, we provide self-encrypting drives (SEDs). Our high-capacity, high-performance nearline HDDs for cloud data centers automatically encrypt and store the written data. For data encryption, we use AES*1, a standard encryption algorithm established by the US National Institute of Standards and Technology (NIST). Our HDDs also support access control functions using the ATA*2 Security Feature Set (for ATA devices), TCG*3 Opal SSC*4, and TCG Enterprise SSC to prevent acquisition of protected data without password authentication. These functions provide data protection and leakage prevention.

Furthermore, in regard to the complete erasure of data at the time of disposal, our HDDs are equipped with a technology called Cryptographic Erase that can instantly invalidate all data cryptographically by changing the encryption key, eliminating the need to overwrite data at a significant cost.

The cryptographic algorithm implemented in our HDDs has been certified by CAVP*5 (A6635, A6705, A6706, A6707), a cryptographic algorithm validation program based on the US government's FIPS PUB 140-3, guaranteeing high reliability. Moreover, our MG09*CP18/16TA*6 HDDs have been certified by CMVP*7 (#4771, #4813), a cryptographic module validation program released in 2020 based on FIPS PUB 140-3. The entire HDD unit has been evaluated as a cryptographic module by a third-party organization from various perspectives, including its design, implementation, and operation.

*1 AES: Advanced Encryption Standard
*2 ATA: Advanced Technology Attachment
*3 TCG: Trusted Computing Group
*4 SSC: Security Subsystem Class
*5 CAVP: Cryptographic Algorithm Validation Program
*6 MG09*CP18/16TA: MG09SCP18TA, MG09ACP18TA, MG09SCP16TA, MG09ACP16TA
*7 CMVP: Cryptographic Module Validation Program



Security features available with storage products