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 products for personal mobile devices, but also products designed for various fields, such as products for digital multifunction printers (MFPs) and enterprise products for data centers and other operations. We provide HDDs with 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 to prevent data leakage after disposal.

To meet these customer requirements, we develop and provide self-encrypting drives (SEDs). Our high-capacity, high-performance nearline HDDs for cloud data centers automatically encrypt and store data when they are input. 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 achieve data protection and leakage prevention.

Furthermore, in regard to the complete erasure of data at the time of disposal, our MDDs are equipped with a technology called Cryptographic Erase that can instantly invalidate data cryptographically by changing the encryption key of the data, thereby achieving the invalidation of all data without the need to overwrite it at cost.

The cryptographic algorithm implemented in our HDDs has been certified by the cryptographic algorithm test CAVP*5 (A1637, A1638, A1645) based on the US government's FIPS PUB 140-3, guaranteeing high reliability. Moreover, for our MG09*CP18/16TA*6 products, we are progressing with the acquisition of CMVP*7 certification based on FIPS PUB 140-3, the US government's cryptographic module certification that started in 2020, and a third-party organization carries out multi-faceted evaluation of the entire HDD unit as a cryptographic module in terms of 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

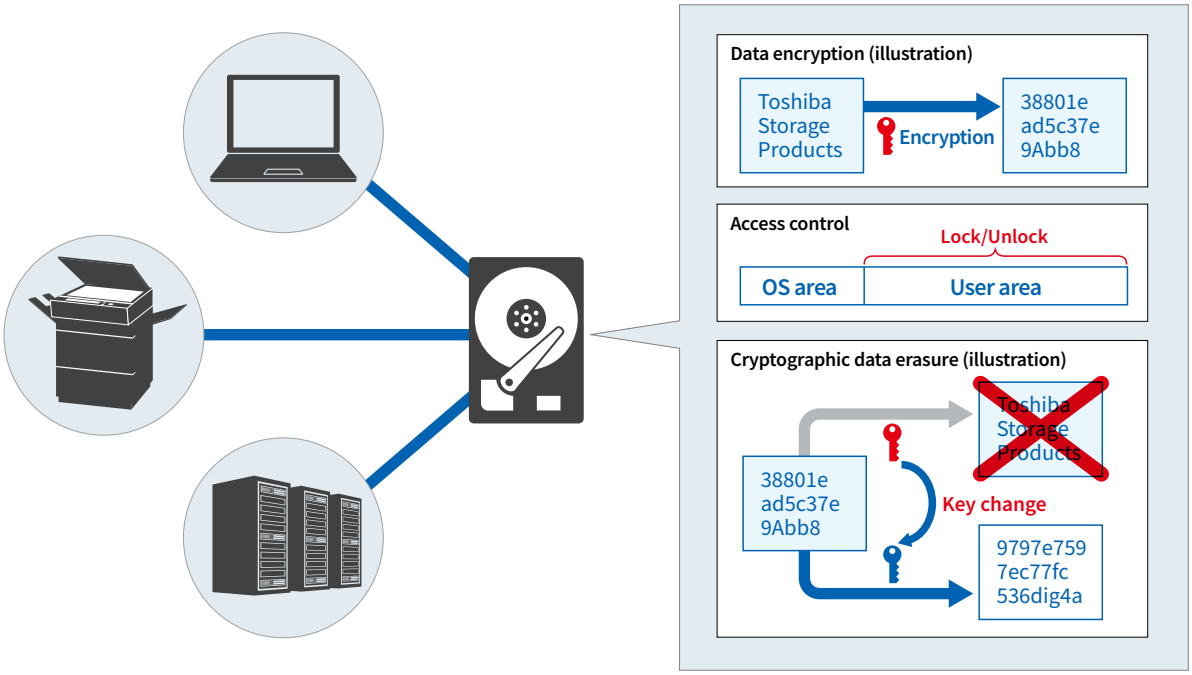

Image of security features in storage products