HDDのセキュリティ規格 及び想定外の使用によって瞬時にデータを無効化する2.5型HDD

Self-Encrypting 2.5-inch Hard Disk Drives Equipped with Wiping Technology to Reduce Information Security Risks

山川　輝二　■YAMAKAWA Teruji
中島　一雄　■NAKASHIMA Kazuo
市村　正太郎　■ICHIMURA Shotaro

ICT（情報通信技術）社会の発展とともに，情報システムに蓄えられる情報量は飛躍的に増えている。それに伴い，情報のセキュリティリスクも確実に高まっている。この状況に対処するため，HDD（ハードディスクドライブ）業界では，HDDに保存されるデータを暗号化して管理するための規格が策定されている。TCG（Trusted Computing Group）のHDD向け規格には“プリブートモード”と“レンジ設定”の機能が定義されており，それらの機能を動作させることによりネットワーク上で高度な認証を使って一元管理できるようにしている。

東芝は，TCGのHDD向け規格に基づく機能に加え，機器認証でHDDとシステムのペアが外れたと認識されたとき，HDD上のデータを自動的に無効化する当社独自の技術を搭載した“忘れ去るHDD（Wipe Technology HDD）”を開発した。

With the increasing volume of data stored in information systems as a result of the expansion of information and communication technology (ICT), safeguarding the security of information systems is now a crucial issue. In response to this situation, the Trusted Computing Group™ (TCG) provides a specification for self-encrypting drives to avoid various security risks including data breaches. The specification defines two functions-pre-boot mode and multi-locking range-which allow users to consolidate self-encrypting drives via a network.

Toshiba has developed a unique technology that invalidates encryption keys and data when a drive is removed from its housing or connected to an unauthorized host system. We have implemented this system in our TCG-standard-based encryption products including self-encrypting 2.5-inch hard disk drives (HDDs).

1　まえがき

近年，コンピュータなどの情報機器に保存されるデータの価値はますます高くなり，機器の盗難や紛失による情報漏えいのリスクが問題になっている。米国では，MFP（Multi Function Peripheral）に保存されたコピー及びプリントデータの漏えいリスクが2010年に報道されて大きな社会問題になった。

パソコン（PC）や，コピー機，スキャナなど情報機器の記憶装置に情報が保存されている状態，いわゆるData-at-Restでの情報を守るため，近年，情報を暗号化して保存する方法が採用されてきている。情報を暗号化する方式は，ソフトウェアによるものと，HDDなどハードウェアによるものの二通りに大別される。どちらの方式とも，暗号化の速度や強度の観点からNIST（米国国立標準技術研究所）が推奨するAES（Advanced Encryption Standard）256ビット暗号が採用されている。

これらのうちハードウェアによる情報の保護については，セキュリティ情報機器の標準化を目的にする非営利団体TCG（Trusted Computing Group）によって規格化が進められており，HDDについては情報を暗号化して管理するためのコマンドインタフェースが策定されている。

東芝は，このTCG規格に基づいた暗号化機能に，当社独自の“忘れ去るHDD技術（Wipe Technology）”を加えたHDD MKxx61GSYGシリーズを開発した。ここでは，MKxx61GSYGシリーズHDDに採用した，TCG規格に基づく機能とWipe Technologyの概要，及びこの技術の採用による機器のライフサイクル全体を通したセキュリティ強化について述べる。

2　TCG規格 Opal SSCに基づく機能

TCGは，主に企業用PC環境向けに高度なセキュリティソリューションを実現するモバイルHDD用規格としてOpal SSC（Security Subsystem Class）仕様を2009年に規格化した。

Opal SSC仕様に準拠したHDDは，データの暗号化機能の他，高いセキュリティ機能であるユーザー権限の階層構造や，プリブートモード，レンジ機能などを，アプリケーションソフトウェアと組み合わせてシステム上で動作させることができる。

ユーザー権限の階層構造では，Administrator及びUserの2種類のユーザー権限によってアクセスをコントロールして，従来BIOS（Basic Input/Output System）(注1)上でしか管理されていなかったHDDに対するパスワードをアプリケーションソフ

（注1）　PCに接続された機器（ハードウェア）を制御するシステムで，OSやアプリケーションソフトウェアに対して，機器にアクセスするシステムとしての役割を果たす。

トウェア上から管理できるようになり，Administrator権限による一元管理が実現できる。

プリブートモードは，PC起動時に基本ソフトウェア（OS）に先立って専用のプリブート領域が起動する仕組みである。プリブート領域にユーザー認証画面などのデータを設定しておき，PC起動時にユーザー認証を行い，認証に成功したときだけ通常のOSを起動させる機能である。これにより，例えばPCは，生体認証やICカードなどの高度な手段で認証した後だけOS起動ができ，高いセキュリティ環境が構築できるようになる（**図1**）。

レンジ機能は，HDD内のディスク領域をいくつかのセキュアな領域(注2)に分割して利用する仕組みである。分割された各領域は，それぞれ異なる暗号鍵によって保護され，それぞれ独立したユーザーだけが利用できる。これにより，例えば異なる領域にユーザー用のデータと管理者用のデータを別々に記録し保護するなど，記録する情報の特性に合わせてディスク領域を使い分けることで，セキュアなデータ管理が実現できる（**図2**）。

TCG規格ではこれらの機能を規格化して，高度な認証及びネットワークによる一元管理をできるようにした。

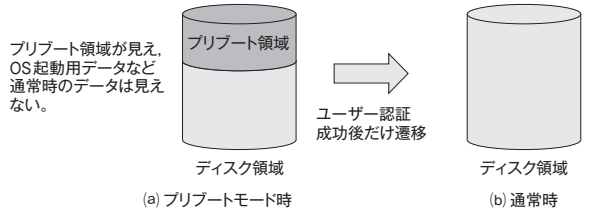

図1．プリブートモード ― 通常はディスク領域は全域見えるが，プリブートモードを使うと認証が完了するまで先頭領域はプリブート領域を見せる。これによって，OS自体を秘匿する。
Pre-boot mode

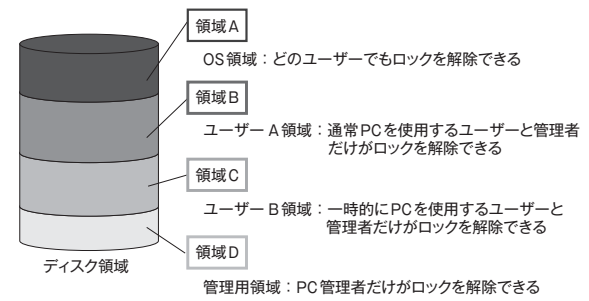

図2．レンジ機能の使用例 ― ユーザーごとにレンジを設定した場合，ユーザーがロックを解除しないかぎり，設定された領域にアクセスできない。この動作によって，ユーザー情報を保護する。
Example of use of logical block address (LBA) ranges

（注2） 暗号や防御ソフトウェアによって，外部からの攻撃や浸入，改ざんなどの危険から保護された領域。

3 Wipe Technology HDD

3.1 より高度な保護機能

TCG規格が規格化されたことでHDDの暗号化技術が認知されつつある状況ではあるが，従来のHDD暗号化技術では，HDDに保存された情報はパスワードによって保護されており，パスワードが漏れてしまうと情報が漏れてしまうという課題が残っている。

そこで当社は，HDD暗号化の技術を元に，より高度にユーザー情報を保護し，かつシステムへの親和性を高めたセキュリティ対策を実現する方法として，Wipe Technologyを開発した。この技術では，次に示す場合も情報を保護できるように，暗号化HDDが自動的に記録データを無効化する仕組みにした。

(1) パスワードが漏れたとしても企業からの情報漏えいを防げること。
(2) IT管理者の変更や廃却業者への引渡しなどオーナーが変更されたとしても，製品のライフサイクルを通した鍵管理が可能であること。

こうして開発したWipe Technology HDDは次のような特長を持っている。

(1) 暗号化機能の応用ソリューション
(2) HDD取外しなど，想定外のアタックに対する強力なプロテクション
(3) 製品ライフサイクルを通してのプロテクション
(4) 瞬間無効化による，廃却又は再利用時のコスト削減

当社は最初のWipe Technology HDDの機能である“電源供給が断たれたときにデータを無効化する”機能（Wipe1）を2010年8月に開発し，技術発表を行った。反響は大きかったが，その反面，次のような課題が明らかになってきた。

(1) 搭載システムが省電力モードになった際にデータが無効化されてしまう。
(2) 停電などの場合でも，安定してHDDへの電源を供給する必要がある。
(3) 電源状況と連動した動作であるため，応用範囲が限定される。

そこで当社は，“HDDがシステム内にあるうちはデータを無効化せず，システムから取り外した際に無効化する”という本来あるべき姿に向かって検討を進め，最終的に“機器認証”を実施することが必要であるという結論に至り，次に述べる“Wipe2”を開発した。

Wipe2ではHDDとシステムがペアを作り，ペアが外れたときに暗号鍵を消去し，データを自動的に無効化する技術を世界で初めて(注3)開発して採用した。ペアの確認には機器認証を用いることにした。この方式では電源の状況に依存しない

（注3） 2011年4月時点，当社調べ。

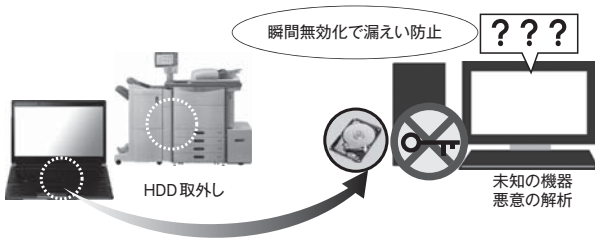

図3．Wipe2の動作 ― あらかじめ設定された機器以外に接続すると暗号鍵を消して，データを無効化する。
Operation of wiping technology

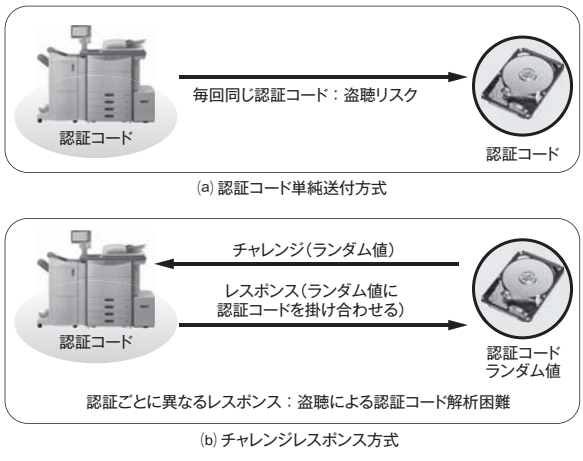

図4．Wipe2で採用している安全な認証方式 ― チャレンジレスポンス方式を採用しており，暗号鍵のセキュリティも強化している。
Host authentication methods

ため，安定して運用できるようになり，更に様々なIT機器で利用できるようにもなった。例えば，機器からHDDを取り外し，そのまま元のシステムに戻せば，機器認証が成立するため，データは無効化されない。一方，HDDを取り外し，データ解析用の別のシステム（PCなど）に接続すると，機器認証が成立しないため，HDDが自動的にデータを無効化し，情報の漏えいを防ぐことができる（**図3**）。

Wipe2では機器認証をデータ無効化の判定に使うため，安全な認証方式を採用する必要がある。そのためWipe2は，チャレンジレスポンス方式を採用している。この方式は認証を行うごとにシステムとHDDの間を流れる認証コードが変化するため，盗聴しても解析できないという特長を持つ（**図4**）。

3.2　機器のライフサイクルを通したプロテクション

Wipe Technologyは，機器のライフサイクルを通した情報漏えい防止を実現している。IT管理者から，利用者，廃却業者へと機器のライフサイクルに合わせてオーナーが変わっても，異常時にはHDD自体がデータを無効化するため，強固な漏えい防止ができる。

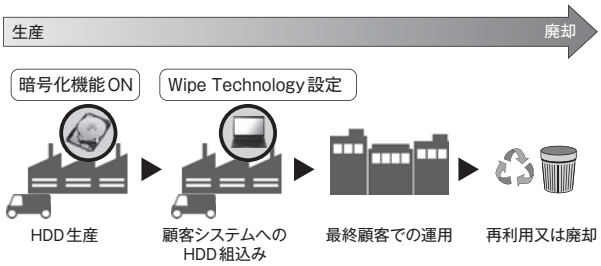

図5．製品のライフサイクル ― HDD出荷時には暗号化機能だけが動作しており，顧客システム組込み時にWipe Technologyを設定する。これによって，顧客の要望に合わせて機能を選択できる。また，再利用又は廃却時は，瞬時にデータを無効化できる。
Life cycle of HDD

図5に示すように，HDDの暗号化機能はHDD生産時に設定され，HDD組込みのフェーズで，各顧客のシステムに応じたWipe Technologyの設定を行う。

4　あとがき

暗号化機能を搭載したHDDは，従来の“暗号化する機能”から“データを無効化する機能”へと効果の示し方を変えることで，ユーザーの利用シーンに，よりいっそう適応したセキュリティソリューションに進化した。

今後，TCG規格 Opal SSCで標準化されたプリブートモードやレンジ機能をフルに利用することで，拡張性に富んだセキュリティソリューション創出ができると考えている。

当社はこれからも，ICT社会において安全にかつ安心して使用できる装置を提供し，ICT社会へ貢献していく。

山川　輝二　YAMAKAWA Teruji
セミコンダクター＆ストレージ社 青梅ストレージプロダクツ工場 設計第一部主務。暗号化HDDの開発に従事。
Ome Operations-Storage Products

中島　一雄　NAKASHIMA Kazuo
セミコンダクター＆ストレージ社 ストレージプロダクツ事業部 ストレージソルーション推進部参事。ストレージ応用商品の企画業務に従事。
Storage Products Div.

市村　正太郎　ICHIMURA Shotaro
セミコンダクター＆ストレージ社 青梅ストレージプロダクツ工場 設計第一部。暗号化HDDの開発に従事。
Ome Operations-Storage Products