ストレージ製品へのセキュリティ機能の実装

Implementation of Security Functions in Storage Devices

山川　輝二　■YAMAKAWA Teruji
荒牧　康人　■ARAMAKI Yasuto
梅澤　健太郎　■UMESAWA Kentaro

情報セキュリティが重要度を増しているなか，ストレージ製品に要求されるセキュリティ機能はその用途により様々である。個人ユースが多いモバイル機器向け製品ではパソコン（PC）の盗難や紛失時にデータ流出の防止効果を要求され，データセンターなどで用いられるエンタープライズ向け製品ではサーバに使用されているHDD（ハードディスクドライブ）やSSD（ソリッドステートドライブ）の故障や経年劣化による廃却後のデータ流出防止を低コストで保証することが要求される。

東芝は，これらストレージ製品への様々なセキュリティ要求に迅速に応えるため，要求に共通するセキュリティの基本処理で構成されるライブラリを全ストレージ製品で利用してファームウェアの共通化を実現するとともに，その信頼性向上のために設計と実装の正しさを保証するセキュリティ第三者認証の取得に取り組んでいる。

With the growing importance of information security, demand has been increasing for the implementation of appropriate security functions in storage devices such as hard disk drives (HDDs) and solid-state drives (SSDs) according to their applications. In the field of storage products for personal mobile devices, it is necessary to prevent unauthorized leakage of data in the event of loss or theft of a mobile device. In the field of storage products for enterprise use such as data center servers, on the other hand, it is necessary to provide quick and secure data erasing in the event of failure or at the time of disposal of HDDs and SSDs at low cost.

To fulfill these diverse requirements, Toshiba has been developing firmware common to both personal and enterprise storage products using libraries with the necessary security functions, and has also been making efforts to obtain third-party certifications based on a security validation program to certify the design and implementation of these security functions.

1　まえがき

情報セキュリティは日々重要性を増しつつあり，これに伴い情報のセキュリティに関する技術も日々進化している。これらの技術によって守られる情報はストレージ製品に格納されている。従来はUSB（Universal Serial Bus）メモリやPCの紛失や盗難による情報の流出を防ぐための技術が主であったが，クラウドストレージの広がりとともにデータセンターに格納されている個人情報の流出を防ぐための技術も重要性を増している。ここでは，こうした情勢のなかでストレージ製品に求められている情報セキュリティと，それらを実現するための東芝の取組みについて述べる。

2　SEDの現状

2.1　SEDの市場と市場要求

HDDやSSDの市場は，大きく二つに分けられる。個人ユースが主となるモバイル系と，データセンターなど企業向けサーバが主となるエンタープライズ系である。必要な暗号化技術は，これら市場の特徴によって異なる。

モバイル系分野では，ノートPCやデスクトップPCに内蔵又は外付けされるHDDやSSDが対象であり，これらPCや，HDD，SSDなどの盗難や紛失により発生するデータ流出の保護・抑止機能が要求される。技術的には，第三者がデータを読み出せないように，パスワード認証機能やデータの暗号化機能が要求される。

一方，エンタープライズ系分野の場合には，装置はデータセンターのセキュリティルームなどに設置されるため，盗難・紛失対策の要求は少なく，サーバに使用されているHDDやSSDが故障や経年劣化により廃却された後にデータが流出するのを低コストで防止することが要求される。技術的には，データの暗号化機能及び，鍵消去や鍵交換によって暗号論理的にデータを無効化する機能が要求される。

廃却したHDDやSSDからデータが流出するのを避けるため，従来は，廃却時に時間をかけて全データをダミーデータで上書きしたり，装置そのものを物理的に破壊していた。しかし，HDDやSSDの故障時にはデータを上書きできないことや，大容量化に伴いデータを上書きする時間が延伸してコストが増大することが大きな問題となっていた。暗号技術を採用した装置では，装置が故障しても暗号化によりデータが保護されるのに加え，使用している暗号鍵を交換すること（Crypto Erase）でHDDやSSD内の全データを一瞬で無効化できるた

め，安全で低コストな廃却方法を提供できる。

またストレージレンタルサービスしているデータセンターでは，データ無効化機能により，他顧客へのレンタル変更を瞬時にできる。

このような背景の下，書込み時にデータを自動的に暗号化する機能を内蔵した“自己暗号化ドライブ（SED：Self Encrypting Drive）”に対する市場要求が高まりつつある。

2.2 SEDが準拠するセキュリティ規格

セキュリティの課題への対応としてSEDが準拠すべきセキュリティ規格とその目的を**表1**に示す。

TCG（Trusted Computing Group）規格に準拠したSEDに共通の主要機能は，データ暗号化及び，ディスクの部分領域ごとのアクセス制御（レンジ管理機能）である。また，TCG Opal SSCではプリブートモードが追加で規格化されている(1)。

HDDやSSDにおけるデータ暗号機能は，コントローラに実装された暗号回路を用いて，書き込まれるデータを暗号化し，読み出すデータを復号する機能である。TCG規格ではデータの暗号化にAES（Advanced Encryption Standard）暗号の利用モードであるXTSやCBCを用いる。鍵長については128ビット以上という規定しかないが，当社のSEDではデータの長期的な安全性を図って256ビットの鍵長を用いている。

レンジ管理機能は，HDDやSSD内のディスク領域をいくつかに分割して利用する仕組みである。分割された各領域は異なる暗号鍵で保護され，それぞれ独立したユーザーだけが利用できる（**図1**）。IEEE 1667（電気電子技術者協会規格1667）ではMicrosoft® BitLocker®(注1)で使われている暗号ドライブのeDrive仕様で実装するように規定されているが，ISV（Independent Software Vendor）が提供するTCG Opal SSC（Security Subsystem Class）とは排他的な関係にあるため，HDDやSSDでの実装がどのようになるかは現時点で不透明な状況である。

表1．SEDが準拠するセキュリティ規格
Security standards for self-encrypting drives (SEDs)

分野	セキュリティ規格	目的
モバイル系	ATA Security Feature Set	パスワード認証 データ暗号化 レンジ管理
	TCG Opal SSC	
	IEEE1667	
エンタープライズ系	TCG Enterprise SSC	レンジ管理 Crypto Erase
	T10・T13 Sanitize	Crypto Erase

ATA：Advanced Technology Attachment

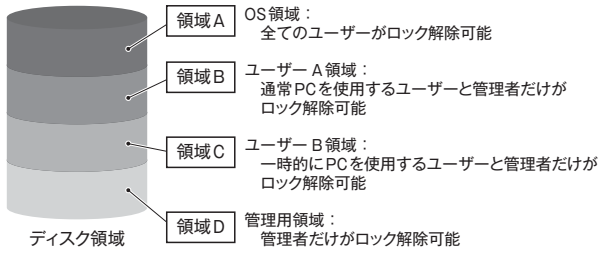

図1．レンジ管理機能の使用例 ― ユーザーごとに領域を設定した場合，ユーザーがロックを解除しないかぎり，設定された領域にアクセスできない。この機能によりユーザー情報を保護する。
Example of use of logical block address (LBA) ranges in disk space

2.3 東芝でのSEDの実装形態

2.2節で述べた様々なセキュリティ規格に対応したエンタープライズ及びモバイル向け製品を開発するため，当社はストレージセキュリティの設計と開発を担当する共通部門を設立した。この部門でセキュリティ規格を分析し，パスワード認証や，アクセス制御，乱数生成，鍵管理などセキュリティ規格に共通の基本処理を実装した共通ライブラリを作成し，それをHDD及びSSDで共用することで各種製品に対応している。そして，この共通ライブラリの基本処理を利用して，セキュリティ規格で要求されるレンジ開閉制御といった上位のセキュリティ機能を実現している。また，この部門では，T10及びT13それぞれに定義されたTCG規格向けのコマンド（Trusted Send/Receive，Security Protocol In/Out）を処理するエンタープライズあるいはモバイル向け製品共通のファームウェアも実装している。これにより，開発効率を高めるとともに，同一セキュリティ規格をサポートした当社ストレージ製品において，セキュリティ関係のコマンドに対するホストから見た挙動を統一し，顧客がHDDとSSDで相互移行しやすいようにしている。

HDDやSSDの構成，及びパスワード（PIN）認証のシーケンスを**図2**に示す。例えば，TCG Opal SSCでのPIN認証のシーケンスは，Trusted Sendコマンドのパラメータとして PINが送付され，TCG処理部で適切にデコードされた後，セキュリティ基本処理部でPIN認証処理により確認される。正しいPINと認定された場合には，そのユーザーが管理する領域への書込み及び読出しのアクセスが可能になる。

2.4 東芝のセキュリティ第三者認証への対応

TCG規格などのセキュリティ機能を実現する標準化規格への対応は必要ではあるが，実際の製品が安全であることの判断基準としては不十分である。製品のセキュリティ品質についての客観的な指標を与える方法としてセキュリティ第三者認証制度がある。HDDやSSDなどのストレージの分野では，NIST（米国国立標準技術研究所）FIPS 140（Federal Information Processing Standard 140）(注2)に基づく，CMVP（Cryptographic Module Validation Program）制度が現在の主流である。

CMVP認証の取得は，米国政府調達では必須になってお

（注1） Microsoft，BitLockerは，米国Microsoft Corporationの米国及びその他の国における商標。
（注2） 2013年9月時点では2001年発行のFIPS140-2に基づき試験されており，2014年に改訂版のFIPS140-3が発行予定である。

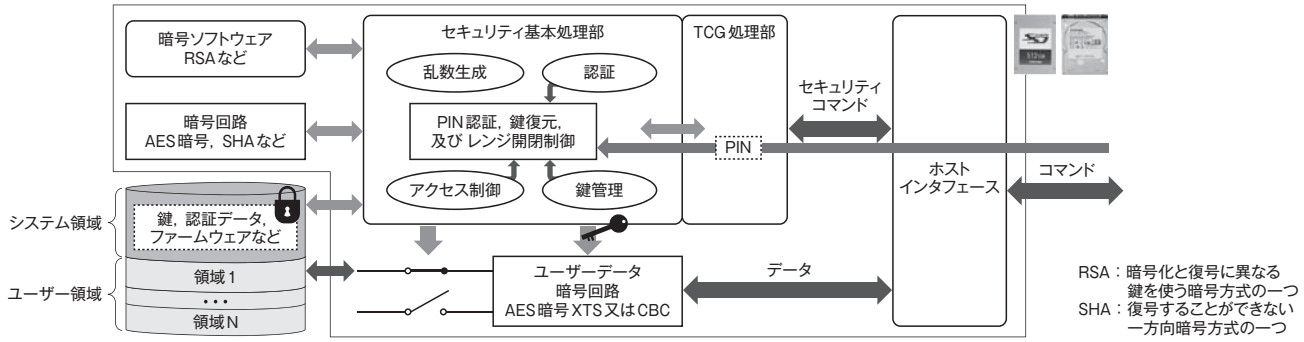

図2．HDDやSSDの構成とPIN認証 — ホストから送付されたPINにより認証処理，鍵設定，及び領域の開閉制御が行われる。
Configuration and personal identification number (PIN) authentication of HDD and SSD

り，取得件数は年々増加している。ストレージ以外での主な取得分野としてはファイアウォール製品などのネットワーク機器やソフトウェア暗号ライブラリがある。

CMVPでは，安全性を米国政府が公認した暗号アルゴリズムが正しく実装されるとともに，暗号機能が利用する暗号鍵などの重要情報が適切に保護されていることが求められる。製品を利用した暗号アルゴリズムの実装正当性テストや，重要情報の消去機能についての実機確認，エントロピー源の評価，回路構成の目視やプローブなどの物理攻撃への耐性の確認（**図3**）などが特徴である。

当社は，JCMVP（Japan CMVP）を取得した経験も踏まえて，2012年8月からCMVP認証取得を本格的に開始した。まず，2.3節で述べた共通ライブラリについて，設計段階からFIPS140を考慮して暗号アルゴリズムの実装や暗号鍵などのパラメータの扱いを実装して準備を整えた。そして，この共通のセキュリティ実装をベースに，セキュリティ認証専任のチームがエンタープライズ向けかモバイル向けか，及びHDDかSSDかを問わず対応することでCMVP認証の取得コストを最小化しようとしている。2013年12月現在，TCG Opal SSC及び当社独自の暗号機能であるWipe™ Technologyに対応したモバイルHDDが試験機関での認証を終了し，NISTによる最終評価中である。これに引き続いてエンタープライズ向けHDDやSSD，モバイル向けSSDなどについてもCMVP認証取得の準備中であり，順次，認証を取得していく予定である。またCMVP認証のノウハウは，HDDやSSDだけでなくUFS（Universal Flash Storage）やe・MMC™(注3)などのメモリ製品にも適用可能である。

図3．物理攻撃対策 — タンパシールにより物理攻撃から保護されているモバイル向けHDDの例である。
Physical attack countermeasure using tamper seal

3　SEDの今後の課題

3.1　モバイル系の課題

モバイル系分野の今後の課題として，次の点が挙げられる。

(1)　TCG Opal SSCの方向性が不透明　　TCG Opal SSCの策定を主導してきたISVが想定する企業での持出し機器管理などのユースケースとMicrosoft社が想定するモバイルPCでの個人データの保護というユースケースが整合していない。着目するユースケースの違いにより，TCG Opal SSCのコンプライアンステストが複数存在し，対応コストが高い状況である。テストの共通化の観点からもどちらのユースケースが主流となるかの見極めや関連各社への適切な働きかけが必要である。

(2)　物理攻撃への耐性向上　　不特定多数が存在する環境など，利用環境の物理セキュリティがエンタープライズ系分野と比較して低い。そのため，現時点のセキュリティ規格では暗号化されずに入出力されるPINのバストレースや，HDDやSSDが装置から持ち出されたうえで解析される場合があることも課題である。Wipe™ Technologyを実装したストレージではこれらの課題への対策も提供している(1)。

(3)　DEVSLP対応　　Intel社の低電スリープモード（DEVSLP）対応の要件として，省電力モードとなったドライブは復帰時に認証を必要とせずにユーザーデータ

(注3)　e・MMCは，JEDEC Solid State Technology Associationの商標。

が読み書きできることが要求されている。ノートPCなどをDEVSLP状態とした後DEVSLPから復帰させると，そのまま動作する状態となってしまうため，DEVSLP状態としたノートPCなどの盗難ではDEVSLPからの復帰により情報が取得されてしまう，というセキュリティ上の問題が発生する。そのためドライブがDEVSLP状態から復帰する際のセキュリティ強化が必要である。

3.2 エンタープライズ系の課題

エンタープライズ系分野の今後の課題として，次の点が挙げられる。

(1) セキュアな障害解析手法の共通化　SEDにおいて，顧客データの保護と，修理・障害調査時のログやトレースなどのデータ収集は相反するものである。ファームウェア共通化の延長として，セキュアで可能な限り多くの場合に適用できる解析用データの収集方法の共通化と運用が必要である。

(2) リモートコピー機能を考慮したデータ消去方法　データセンター系のシステムでは，通常，地震などの災害対策や装置故障などによってデータが消失するのを防ぐため，リモートコピー機能を使用して遠隔地にバックアップを保存している。このため複数の同じデータが別のHDDやSSDに存在することになる。そこで，HDDやSSDを連携させて複数の同一データを管理し，消去する際は，全てのデータが消去されたことを確実に保証する方法が必要である。

3.3 CMVP認証取得の課題

CMVP認証取得に関わる課題として，次の点が挙げられる。

(1) 各種の制約事項への対応　CMVPでは認証を取得する対象製品のハードウェアやファームウェアのバージョン番号を明確に定義する必要があり，変更する場合には，再認証や再取得の作業が必要になる。特にエンタープライズ向けのHDDやSSDでは，顧客要求によるファームウェアのカスタマイズが頻繁に発生するため，取得したCMVP認証を維持し続けるためにはコストがかかる。また，現在，CMVP認証取得に8～10か月程度を要する。その大半は，NISTによる試験レポートの評価を待っている期間であり，ベンダーや認証機関が短縮することは難しい。一方で製品自体のライフサイクルは短くなる傾向があり，CMVP認証を取得しても市場で有効な期間が限定されるという問題がある。これらの制約を考慮した認証取得・販売戦略が必要である。

(2) コントローラ設計へのセキュリティ要求の反映　製品に搭載されるコントローラの設計には6か月から1年を要し，手戻りが発生した場合には時間や費用に与える影響が大きい。コントローラに実装される機能が，CMVP認証に関わる場合には十分な調査が必要である。このため，今後予想される，セキュリティ規格の改定による暗号実装の追加，FIPS140の改定(注2)，及び暗号アルゴリズム規格の動向（SHA3の追加やNISTのSP800-90B（Special Publication 800-90B）に関連したエントロピー評価方法の変更など）を確実に捉え，適切なタイミングでコントローラの設計にフィードバックしていくことが必要である。この作業負荷を軽減するには，ファームウェアにとどまらずセキュリティに関連するハードウェア設計の共通化などが必要である。

4 あとがき

近年の情報漏えい関連のニュースなどにより，情報に対する保護についての関心は高まってきている。当社は，これらの要求に応えるため安全なストレージ製品の開発に取り組んでいる。しかし，3章で述べたように様々な課題もあり，ストレージ製品のセキュリティの分野は技術も市場もまだ成熟しておらず，課題をどのように解決していくか，顧客の次の要求を予測して対応していくことが重要なミッションとなっている。また，欧州で議論されている“忘れる権利”のようにネットワーク上にある要求された情報を検索し削除していく機能をシステムソフトウェアと連携して動作させる機能の策定や，検索に最適化されたHDDやSSDの性能チューニングなど，一見セキュリティの分野に関係がないような技術との連携がセキュリティ製品に要求されてくることも考えられる。

このようにまだまだ技術的にも市場的にも成長できる分野であるため，これからも新しい機能を創造し，実現させた製品を提供することでセキュリティの分野で社会貢献していきたい。

文　献

(1) 山川輝二 他. 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. 東芝レビュー. 66, 8, 2011, p.44－46.

山川　輝二　YAMAKAWA Teruji
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 要素技術第二部参事。暗号化HDD及びSSDの開発に従事。
Storage Products Div.

荒牧　康人　ARAMAKI Yasuto
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 要素技術第二部主務。暗号化HDD及びSSDの開発に従事。
Storage Products Div.

梅澤　健太郎　UMESAWA Kentaro
セミコンダクター＆ストレージ社 システム・ソフトウェア推進センター ソフトウェア・プラットフォーム担当主務。ストレージ及び半導体製品のセキュリティ機能の設計・開発に従事。電子情報通信学会会員。
System & Software Solution Center