# Wipe technology HDD
# IT機器に搭載されたHDDからの情報漏えい防止技術

## はじめに

**当社は 2011 年 4 月 13 日にセキュリティ機能を強化した 2.5 型 HDD（ハードディスクドライブ）を発表しました。**
**本 HDD は盗難による情報漏えい防止策や廃却時などのデータ無効化に有効な製品として、デジタル複合機、パソコンをはじめ、さまざまな IT 機器で利用が可能です。**

## 増加するセキュリティリスク

ICT（Information and Communication Technology）の発展とともにHDDなどの記憶装置の利用範囲も、従来のパソコンから、複合機（MFP）をはじめとするIT機器に大きく広がっています。また、HDDの記憶容量の増加とともに、各装置に蓄えられる情報量は飛躍的に増えています。それに伴い、蓄積された情報のセキュリティリスクも確実に高まっています。「事故で情報が漏えいしてしまった」という時代から、「機器に蓄えられた情報資産が意図的に狙われる」、という時代に突入しています。
2010年、米国で中古のMFPに搭載されたHDDから、保険会社の契約者情報、犯罪者の履歴情報、さらにはニューヨークのテロ現場付近のビルの設計図など、おびただしい数の重要情報が抽出できた、という報道がされ、米議会でも取り上げられました。この報道はHDDの取り外しといった、従来は考えられなかったアタックに対する保護が必要となったことを示唆しています。

## 従来の保護方法

従来の保護方法としては次のものがありますが、それぞれ課題もあります。

- ソフトウエアでのデータ暗号化： インストール時に数時間もの時間がかかる。
- 消去ソフトによる複数回のデータ上書き： HDDの大容量化に伴い、5-6時間もの時間がかかる。
- 物理破壊： 磁気消去や機械的破壊などの方法があるが大がかりな設備が必要になる。

## SEDの登場

暗号化機能を搭載したHDDはSED（Self Encrypting Drive）と呼ばれ、数年前から実用化されています。前述した従来方法に対して、処理時間やコストを軽減できる手段として有効です。
SEDは従来のソフトウエア暗号化に比較して以下のような特長を持っています。

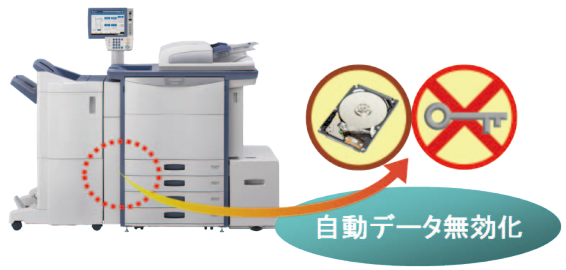
- 設定や廃却の際の手間がかからない。
  ・ソフトウエア暗号では、数時間にもわたるインストール作業が必要となりますが、SEDでは不要。
- システム性能を最大化可能。
  ・SEDの暗号演算はシステムのCPUではなく、HDDの暗号回路を使うので、システム側に負荷をかけない。これによりシステムＣＰＵはメールや表計算など本来の処理を高速に行うことが可能。

このようにSEDは従来方式に対し、多くの特長を持ちますが、一方、さらに高度なセキュリティを要求する用途では、以下の点の考慮が必要になります。

- システムからHDDを取り外し、さらにパスワードも漏えいした場合の対策
  ・HDDを取り外され、さらにパスワードも入手されてしまった場合、他のシステムでHDDに保存されたデータを解析され盗まれるリスクがある。

## 更なるセキュリティ向上のために Wipe Technology HDD を開発

当社は上記ケースのようなリスクへの対策をSED応用技術としてどのように講ずればよいかを検討し、Wipe Technologyとして発表（Wipe1）を行いました。(2010年8月発表)
本発表で紹介されたWipe1では、機器からHDDを取り外したり、HDDへの電源供給が断たれたりすると、HDDが自動で暗号鍵を消去し、データを無効化するという機能を持っています。
Wipe1は主にMFPでの利用を想定し、MFPからHDDが取り外された際の情報漏えいを防ぐことを目的としました。
運用例としては、次のように設定します。




Wipe1


Wipe2

- HDDのデータ領域を、無効化するエリアと無効化しないエリアに分ける。（無効化しないエリアも暗号によりデータを保護します。）
- 無効化するエリアにはPrint, Scan, Copyなどのデータ、無効化しないエリアにはシステムデータおよびFaxデータを配置。(Faxデータは運用面から、無効化されないようにしています)

これにより、MFPの電源を切った場合やHDDが取り外された場合に、Print, Scan, Copyのデータは無効化され、情報漏えいを防止することができます。

## Wipe2：顧客との対話を通じて進化

Wipe1の発表は大きな反響を呼びましたが、同時に以下の点が改善課題として浮上してきました。

- 省電力モードになっただけでデータが無効化してしまう。
- MFP以外の用途でも使いたいが、電源断でデータを無効化するのは実用上使いにくい。

そこで、HDDがシステム内にあるうちはデータを無効化せず、取り外された時だけ無効化する、というあるべき姿に向かって検討を進め、最終的に『機器認証』を利用した自動無効化の開発を重ね、Wipe2を完成させました。

Wipe2ではHDDとシステムとでペアを作り、ペア以外のシステムに接続されたときにHDDが暗号鍵を自動消去しデータを無効化します。ペアの確認には機器認証を用います。
機器認証とは、HDDとシステムが同じ認証コードを持っていて、データを読み書きする前にお互いを確認する機能です。

例えば、機器からHDDを取り外しても、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ません。一方、HDDを取り外し、別のシステム（パソコンなど）に接続すると、機器認証が成立しないため、HDDが自動でデータを無効化し、情報の漏えいを防ぎます。

この方式は電源断に依存しないため、安定的な運用かつさまざまなIT機器での利用が可能となります。

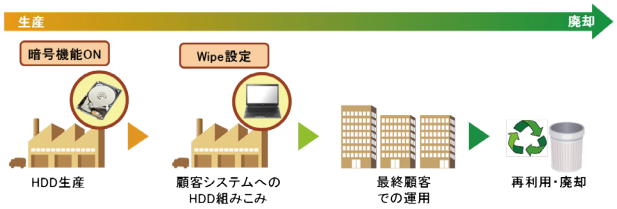
## 安全な機器認証

Wipe2では機器認証をデータ無効化の判定に使用するため、安全な認証方式を使う必要があり、チャレンジレスポンス方式を採用しています。この方式は認証を行うごとにシステム・HDD間に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、という特長を持ちます。


上図で、従来のパスワード送信では、認証を行う度に同じコードがシステム・HDD間を流れます。これは盗聴リスクを負うことになります。これに対し、チャレンジレスポンス方式では、HDDが生成したランダム値を使って、システムが認証コードを変換しHDDに送付します。HDDは自身が生成したランダム値と認証コードを使って、システムから送付された値が正しいかを判定することができます。この方式を使うと、ホストからのレスポンスが認証を行うごとに変化するので、盗聴による解析ができなくなります。

## 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可能とします。
IT管理者、利用者、再利用者、廃却業者と機器のライフサイクルの各フェーズでオーナが変わっても、HDDを取り外し、他のシステムでデータを取り出すような異常時にはHDD自体がデータを無効化するため、強固な漏えい防止が可能となります。




## ターゲット市場および利用シーン

Wipe Technology HDDは前述のWipe1、2に加え、機器からのコマンドによりデータを無効化する機能（SED機能の１つでWipe0と称します）を搭載しています。
Wipe Technology HDDの主なターゲット市場としては以下があげられます。

- PC市場： モバイル環境の発達に伴うセキュリティ強化
- MFP市場：オフィス内情報ハブとしてセキュリティ強化

利用シーンとしては、以下があげられます。

- IT機器からのHDD盗難対策
  ・電源断でデータ無効化 （Wipe1の機能）：システムの電源断、またはHDDの取り外し時にデータを無効化
  ・ 他の機器への接続でデータ無効化 （Wipe2の機能）：HDDを取り外し他の機器に接続された場合データを無効化
- 廃却・再利用対策
  ・ 機器からのコマンドでデータ無効化（Wipe0の機能）：廃却・再利用時にSEDの機能で、コマンドにより瞬間データ無効化
- 薄型クライアントPC
  ・ 電源断でデータ無効化 （Wipe1の機能）： 本来薄型クライアントPCにはHDDを搭載しないが、肥大化するアプリケーションを使うには大容量の揮発性ストレージが必要。Wipe1なら利用後に電源断することで毎回データ無効化

## まとめ

Wipe Technology HDDは機器のライフサイクルを通して情報漏えいを防止する強力なセキュリティソリューションです。顧客の情報漏えい防止シナリオに沿ったセキュリティ設定を施すことが可能で、以下の機能を持っています。

- Wipe 0：システムからのコマンドを受けてデータを無効化
- Wipe 1：電源断によりデータを無効化
- Wipe 2：シストレージがシステムを認証し、適合しない場合データを無効化

これにより、HDDの取り外しなど、想定外のアタックに対する確実な情報保護が可能になり、また、瞬間無効化により、廃却・再利用時のコスト削減にも大きく貢献します。
Wipe Technology HDDは現在、東芝のPC、MFPでの搭載検討が進んでおり、SSDでもWipe technology搭載の製品化が行われています。東芝はストレージ製品およびPCやMFPなどのIT機器で、高いセキュリティを実現することでICT社会の安心・安全の実現に貢献していきます。

## 参考　運用例

### MFPでの情報漏えい防止

● 〈シーン1〉HDDを盗まれても漏えいしない
・概要：HDDを他の機器につなぐと、その瞬間にデータを無効化する。
・従来：HDDの暗号機能は提供されてきたが、データ無効化されないため、**他の機器で解析されるリスク**があった。
・効果：盗難されてもデータ無効化が働くため情報**漏えいを防止**できる。


● 〈シーン2〉MFP返却時・廃却時にデータ無効化
・概要：管理者メニューからのコマンドで、HDDに記録されているデータを一瞬で無効化する。
・従来：データ上書き**消去に長時間**を要した。
・効果：MFP廃却時、リース返却時、HDDの廃却時などに、**一瞬でデータを無効化**できる。
長時間の上書きによる消去や、破壊などの手間が不要。


### PCでの情報漏えい防止

● 〈シーン1〉他のPCではデータ無効
・概要：HDDが盗まれても他のPCではデータ復号できない。元のPCのみで利用可能。
・従来：HDDが盗まれHDD**パスワードが漏れると、漏えいリスク**となる。
・効果：データ復号には機器認証とパスワードが必要。パスワードだけが漏れても、他のPCや解析機では**データ復号できない**。


● 〈シーン2〉廃却時・返却時、瞬時にデータ無効化
・概要：専用ソフトウェアツールで、HDDに記録されているデータを一瞬で無効化する。
・従来：データ上書き**消去に長時間**を要した。
・効果：PC廃却時、リース返却時、HDDの廃却時などに、一瞬でデータを無効化できる。
長時間の上書きによる消去や、破壊などの手間が不要。


＊設計および使用に際しては、本製品に関する最新の情報および本製品が使用される機器の取扱説明書などをご確認の上、これに従ってください。
＊その他の本ページに掲載の商品の名称は、それぞれ各社が商標として使用している場合があります。

ホームページ：**http://www.toshibastorage.com**