ハードディスクのデータ消去に関する規格と方法

磁気データ消去装置　ERAZER PRO の紹介

消去装置　SSDERAZER の紹介

リ・バース株式会社

2020 年 2 月

概要

電子媒体は保存が容易く利便性、コスト削減、環境配慮の面でも行政、企業共に不可欠な情報機器となっています。反面、たったひとつの媒体の保護を怠っただけで、膨大な情報が流出する危険性を常に考慮しなければなりません。イギリス企業の comparitech によると中古ハードディスクの市場では約 60％の製品から元所有者のデータが復元されるという実験結果が発表されています。
電子媒体の進歩にあわせ、扱う情報量は爆発的に加速する中、法令や規制によって組織には情報漏洩を防ぐ手段と証明を義務付けられています。その中で媒体の廃棄や返却など、ユーザーの管理から離れる場合の処理について実効的な判断材料が認知されていません。
この文書では特に PC、サーバーで大量に使用されているハードディスクの消去について最新の情報と共に弊社が開発製造した消去装置をご紹介いたします。

現在行われているハードディスクの消去方法について

■上書き消去…保存されているデータに別のデータを上書きすることで元のデータを消去

- 有料から無料まで多種のソフトウェア
- 外部からプログラムを実行する専用装置

■磁気消去…強力な磁気の照射で消去（消磁）

- 自動の専用消去装置
- 強力な磁石を使用した製品

■物理破壊…ディスクを破壊し利用出来ない状態にする

- プラッター（記録域）部に穿孔する、ドリル又は専用装置を使用
- 強力なシュレッダーで粉砕

各団体の消去方針

■ ISO/IEC 27001:2013 11.2.7

記憶媒体を内蔵した全ての装置は、処分又は再利用する前に、全ての取扱いに慎重を要するデータ及びライセンス供与されたソフトウェアを消去していること、又はセキュリティを保って上書きしていることを確実にするために、検証しなければならない

■ 政府機関等の対策基準策定のためのガイドライン (平成 30 年)
内閣官房 内閣サイバーセキュリティセンター

遵守事項
(7) 情報の消去
(a) 職員等は、電磁的記録媒体に保存された情報が職務上不要となった場合は、速やかに情報を消去すること。
(b) 職員等は、電磁的記録媒体を廃棄する場合には、当該記録媒体内に情報が残留した状態とならないよう、全ての情報を復元できないように抹消すること。
遵守事項 3.1.1(7)(b)「抹消する」について
「ファイル削除」の操作ではファイル管理のリンクが切断されるだけであり、ファイルの情報自体は抹消されずに電磁的記録媒体に残留した状態となっているおそれがある。電磁的記録媒体に記録されている情報を抹消するための方法としては、例えば、次の方法が挙げられる。
データ抹消ソフトウェア（もとのデータに異なるランダムなデータを複数回上書きすることでデータを抹消するソフトウェア）によりファイルを抹消する方法
ハードディスクを消磁装置に入れてディスク内の全てのデータを抹消する方法
媒体を物理的に破壊する方法
また、媒体を物理的に破壊する方法としては、例えば、次の方法が挙げられる。（フロッピーディスク等の磁気媒体の場合）当該媒体を切断するなどして情報を記録している内部の円盤を破壊する方法
（CD-R/RW、DVD-R/RW 等の光学媒体の場合）カッター等を利用してラベル面側から同心円状に多数の傷を付け、情報を記録している記録層を破壊する方法
（媒体全般）メディアシュレッダーやメディアクラッシャー等の専用の機器を用いて破壊する方法
また、ファイルの情報に別の情報を上書きした場合であっても、特殊な手段を用いることにより残留磁気から当該情報を復元される可能性があるため、特に機密性の高い情報の抹消に当たっては、留意する必要がある。
なお、職員等自らが情報を抹消することが不可能な場合は、あらかじめ抹消の手段と抹消の措置を行う者を情報システム又は課室等の組織の単位で定めて実施してもよい。

■ 地方公共団体における情報セキュリティポリシーに関するガイドライン (平成 30 年)
総務省

4 . 物理的セキュリティ
(7) 機器の廃棄等
情報システム管理者は、機器を廃棄、リース返却等をする場合、機器内部の記憶装置から、全ての情報を消去の上、復元不可能な状態にする措置を講じなければならない。
パソコンが不要になった場合やリース返却等を行う場合には、ハードディスクから情報を消去する必要がある。（注５）情報を消去する場合、オペレーティングシステム（OS）の機能による初期化だけでは、再度復元される可能性がある。データ消去ソフトウェア若しくはデータ消去装置の利用又は物理的な破壊若しくは磁気的な破壊などの方法を用いて、全ての情報を復元が困難な状態にし、情報が漏えいする可能性を低減しなければならない。

■ パソコンの廃棄・譲渡時におけるハードディスク上のデータ消去に関する留意事項（2018 年）
一般社団法人 電子情報技術産業協会 (JEITA)

パソコンのストレージの状況	データ消去方法例
(1) パソコンとストレージが稼働する場合	・専用ソフトウェアにてデータ消去 ・専用装置にてデータ消去 ・ストレージを物理的に破壊
(2) パソコン本体は稼働しないが、 ストレージは稼働する場合	・他の稼働可能なパソコンにストレージを接続して 専用ソフトウェアにてデータ消去 ・磁気消去装置にてデータ消去 ・ストレージを物理的に破壊
(3) ストレージが稼働しない場合	・ストレージを物理的に破壊

データ消去における最新の世界規格

国内で最も有名なデータ消去方式の規格に米国国防総省による DoD 5220.22-M が挙げられます。ディスク内のデータを完全に消去するために 3 回の上書き（固定値、補正値、ランダム）を行うというものです。組織によっては 7 回上書きや 35 回上書きを行っている場合もありシェア、フリー問わず多くのソフトウェアが現在でもこれらの規格を基準にしています。ただし改版された同文書の中ではデータ消去の方法については言及されなくなっています。

2006 年以降、新しく基準とされているのが米国商務省に属する NIST（National Institute of Standards and Technology：米国国立標準技術研究所）が発表した Special Publication 800-88 です。

現在では米国の多くの政府機関がこの規格を支持し採用しています。

国内では独立行政法人情報処理推進機構（IPA:Information-technology Promotion Agency, Japan）が和訳した資料を公開しています。

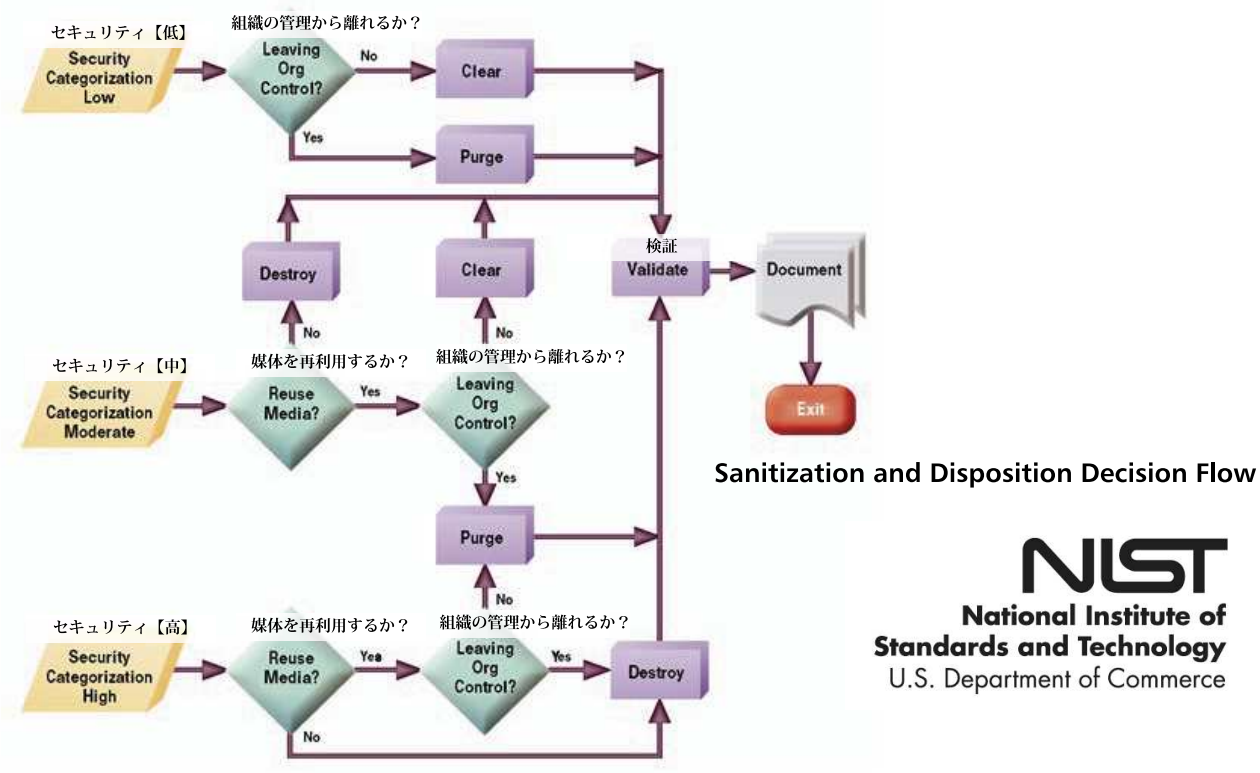
https://www.ipa.go.jp/security/publications/nist/

この文書の中では米国各政府機関に向けてハードディスクだけでなく SSD などのフラッシュメモリ、CD/DVD などの光学メディア、紙媒体まで、情報漏えい防止のために各媒体ごとにデータの処理方法を提示しています。

保存されているデータの機密、重要性からセキュリティレベルを分類し、チャートに従って処理を決定します。

Special Publication 800-88　媒体のサニタイズに関するガイドライン

※サニタイズ…データを再現・取り出せないよう削除する方法



ハードディスクのデータを消去する場合の処理方法

【Clearing（消去)】 …復旧ツールなどでデータを取り出せない処理
○有効性が確認されている上書き方法、ツールを使って媒体の消去を行う

【Purging（除去)】 …研究施設レベルの技術でも復旧出来ない処理
○ATA デバイスにサニタイズ機能が組み込まれている場合はそのコマンドを使用する
（Enhanced Secure Erase,Secure Erase,Cryptographic Erase（暗号化消去）など）
○消磁装置を使用する

【Destroying（破壊)】 …媒体自体を再現出来ない状態にする処理
○裁断、分解、粉砕、焼却

Special Publication 800-88 の中で ATA ハードディスクドライブのうち 2001 年以降に製造された 15GB 超えのドライブに限り 1 回の上書きによる消去で【Purging（除去)】と同程度の効果が望めるとされた事で固定値 1 回の上書きが主流になる。しかし 2014 年の Special Publication 800-88 Revision1(改訂版) の中でこの記述は削除され上書きに関しては複数回の書き込みも選択肢に入れるよう変更された。ハードディスクには外部ソフトウェアがアクセス出来ない HPA/DCO 領域や製造者しか認識しえない領域が存在することが確認され、それらの領域に対して消去が行われたかユーザー側で確認が出来ない事から書き込み回数よりもツールの性能、技術を重視するようになっている。
ディスク側が対応していれば Enhanced Secure Erase,Secure Erase,Cryptographic Erase などは強力な消去処理として期待出来る。これらのコマンドは製造時にファームウェアに組み込まれた内部プログラムで実行すると隠し領域を含めた全領域の消去を行う。ただしユーザー側で実証出来ない以上、期待通りの消去が行われたかは製造側の保証に頼らざるを得ない。
消磁は磁気媒体の消去方法として以前から採用され、NSA（米国国家安全保障局）のストレージデバイスの消去マニュアル（NSA/CSS STORAGE DEVICE SANITIZATION MANUAL 2014）では消磁装置と破壊処理のみ認めている。消磁装置には現在主流の垂直記録方式の HDD を消去出来ない製品があることに注意しなければならない。ハイブリッド式（半導体＋磁気）や HAMR（熱アシスト磁気記録方式）など超高密度の記録デバイスの存在にも触れている。

磁気データ消去装置 ERAZER PRO のご紹介

消去対象：ハードディスク (水平・垂直)/VHS/CMT/LTO/DLT/DDS/DAT/FD など磁気記録メディア

ERAZER PRO-S01 [EPS01-302]

ERAZER PRO は Special Publication 800-88 において【Purging（除去）】処理にあたる消磁装置です。
ERAZER（旧シリーズ）は 2009 年に販売を開始し、業界で初めて水平 / 垂直、両方式のハードディスクの消去を可能にした製品です。
社内での設計製造に拘り高い消去能力を維持したまま安全、静音、省電力、省スペースを重視し、販売を開始して以降、行政機関や企業様に広くご利用頂き 2014 年には特許（第５６０８９１７号）を取得しました。2018 年には ERAZER PRO シリーズとしてバージョンアップしました。

安全に、安心してご利用頂くために

消磁装置は強力な磁界を発生させるために高電圧を扱う製品です。内部で発生した磁力が外部に漏れ周辺の人体や機器に影響を与える危険性があります。実際に消磁装置の中には操作する人を装置から離れさせたり、長時間使用しないよう注意されている物があります。

磁気シールド

ERAZER PRO は発生した磁力を装置内部で処理する磁気シールドを備えており装置外部への磁力漏れは文具のマグネット以下で人体、機器共に危険はありません。

開閉センサー

誤作動防止のためタブが完全に入った状態でなければ磁力を照射しないよう設計されています。

磁力判定ランプ

発生磁力を毎回測定し、装置毎に設定された数値と比較した結果を操作者に分かりやすくお知らせします。

発生磁力規定以上

発生磁力規定未満

製品保証期間２年

ERAZER PRO は品質に妥協しない故障率が低い装置です。さらなる安心をお求めの場合は次項の保守延長パックをご検討ください。

磁気データ消去装置 ERAZER PRO をさらに使いやすく

専用オプション品

□ キャリングケース (PRO-T01/S01/M02/P02)

装置の輸送、保管に適した ERAZER PRO 専用ケース。上部のフタを空けると装置を取り出すことなく使用可能。

アルミ製の外装と内部クッション材で ERAZER 本体を外部衝撃から守ります。

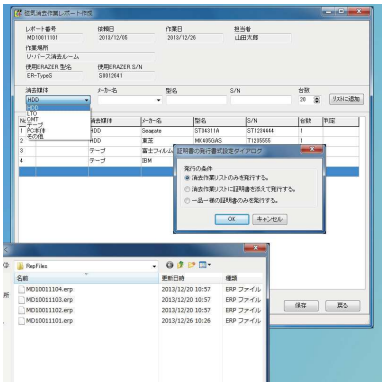
□ 保守延長パック

通常保証期間 2 年＋保守延長パック (1 年単位)、最大 5 年間の無償修理と点検でサポートします。

特典：修理基本料無料 (有償部品有) ・優先修理・修理時代品貸出・性能点検 (年 1 回)

□ LOG オプション機能 (消去作業管理ソフト ERAZER Report, バーコードスキャナ , セットアップ CD)

ERAZER と PC を接続し消去作業を PC で管理出来る機能です。管理ソフト上から作業リストや証明書を簡単に発行する事も出来ます。



バーコードプリンタを使用すれば QR コードを印刷し消去済の媒体に貼り付けることも出来ます。

バーコードのデザインはバーコードプリンタ付属の編集ソフトでカスタマイズも可能です。

QR コードに記録出来る情報

消去作業日時

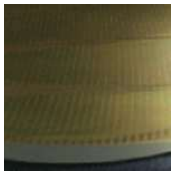
消去装置型番 / シリアル No

消去媒体の種類 / メーカー / 型番 / シリアル No

消去確認用キット

□ コロイドペン

磁気粒子 10nm のコロイド液を塗布するとサーボパターンが目視で確認出来ます。コロイドペンは塗りやすいペン型で消去前、消去後の状態を簡単に比較する事が出来ます。

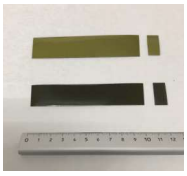


消去前

消去後

□ チェッカー

ERAZER PRO 内部で磁力が照射されたかの確認に使用できます。元は黄緑色ですが垂直に磁力があたった場合に黒く変色します。下図のように HDD に貼ることで黄緑と黒に色が分かれます。



垂直（黒色）

水平（黄緑）

ERAZER PRO 製品一覧

ERAZER PRO 本体

製品名	製品型番
PRO-T01	EPT01-302
PRO-T01 LOG 機能搭載	EPT01-332
PRO-S01	EPS01-302
PRO-S01 LOG 機能搭載	EPS01-332
PRO-M02	EPM02-302
PRO-M02 LOG 機能搭載	EPM02-332
PRO-P02	EPP02-302
PRO-P02 LOG 機能搭載	EPP02-332
PRO-L10	EPL10-302

ERAZER PRO オプション

製品名	製品型番
PRO-T01 用キャリングケース	CPT01-100
PRO-S01 用キャリングケース	CPS01-100
PRO-M/P02 用キャリングケース	CPM02-100
PRO-T01 用保守延長パック	HPT01-101
PRO-S01 用保守延長パック	HPS01-101
PRO-M02 用保守延長パック	HPM02-101
PRO-P02 用保守延長パック	HPP02-101
PRO-L10 用保守延長パック	HPL10-101

消去確認用キット

製品名	製品型番
チェッカー 30 (30 枚 SET)	PB10-100
チェッカー 60 (60 枚 SET)	PB11-100
コロイドペン	PC10-100

データコピー＆消去装置 SSDERAZER のご紹介

消去対象：ATA ハードディスク (パラレル & シリアル)/SSD（Solid State Drive）/CompactFlash/CFast

SSDERAZER miniPro3 [EZM03-200]

SSDERAZER は Special Publication 800-88 において【Clearing（消去)】処理の能力を持った装置です。
近年 HDD と共に PC 内外部の記憶装置として普及が進んでいる SSD(Solid State Drive)は USB メモリや SD カードと同じく NAND 型フラッシュメモリに分類される記憶装置です。磁気記録メディアではないため消磁装置ではデータの消去が行なえません。消磁装置に代わりこのメディアのデータを消去するための装置が SSDERAZER シリーズです。

ATA ハードディスク向け【Clearing（消去)】としての機能 (コマンド)

完全消去　…ディスク全域に “00” を上書き
DoD 消去（3 回）…ディスク全域に “00” “FF” “Random” で 3 回上書き
DoD 消去（7 回）…ディスク全域に “00” “FF” “Random” “96” “00” “FF” “Random” で 7 回上書き

SSD（Solid State Drive）向け【Clearing（消去)】としての機能 (コマンド)　※SSD 用

Secure Erase　…SSD 内部で実行するプログラム、上書き処理と違い数秒程度で完全にデータを消去
Enhanced Secure Erase　…Secure Erase の拡張、代替処理されたセクタを含めて消去

補助機能 (コマンド)

HPA/DCO 解除　…通常は上書き処理が出来ないメーカーが設定した隠し領域を開放する。隠し領域が存在する場合は解除した後に消去コマンドを実行することが望ましい。
ログ出力　…実行した処理をテキストファイル (LOG_DATA_*.txt) で出力する (EZZ02-200 のみ非搭載)

テキストサンプル

```
Task: Full Erase          実行した作業

Copy Area: N/A            SSDERAZER各種設定
Smaller Target: N/A
Unknown Format: N/A
HPA: N/A
DCO: N/A
Performance: Compatibility
Mode: Synchronous

Source:                   マスターの内容（型番、シリアルNo、全体容量、データ容量）
      Device Model:   N/A
      Series Number:  N/A
      Capacity:  N/A
      Data size: N/A
Result:                   実行結果（総数、成功、失敗、実行時間）
      Total:     1
      Pass :     1
      Fail :     0
      Spend Time :  00:24:10

[Detail Target Records] ターゲットの内容（ポート番号、結果、開始時刻、実行時間
                                ターゲット型番、容量、シリアルNo）
Port     Result     Start Time          Spend Time      Devi
-------------------------------------------------------------
0001     Pass       2020/01/06 09:37    00:24:09        FUJI
```

データコピー＆消去装置 SSDERAZER シリーズ比較

搭載している消去機能、対応メディアなどは各モデルに違いはありません。
非同期モード …rotePro のみに搭載。各ポートの処理が独立して進行するので処理が終わったポートから順次メディアを入れ替えることが可能。

	同時消去数	コピー機能	ログ出力	非同期モード	専用付属品
SSDERAZER	2				
SSDERAZER miniPro2	2	●	●		キャリングバッグ
SSDERAZER miniPro3	3	●	●		キャリングバッグ
SSDERAZER rotePro4	4	●	●	●	
SSDERAZER rotePro9	9	●	●	●	

データコピー＆消去装置 SSDERAZER オプション
各種変換アダプター

SSDERAZER シリーズは SATA ドライブだけでなくオプションの変換アダプターを使用することで異なる規格のドライブに対応しています。
標準対応：SATA
アダプタ対応：IDE/miniSATA/NGFF(M.2)/microSATA/CF/CFast

CompactFlash を CF→SATA 変換アダプターに接続した状態

SSDERAZER 製品一覧

SSDERAZER 本体

製品名	製品型番
SSDERAZER	EZZ02-200
SSDERAZER miniPro2	EZM02-200
SSDERAZER miniPro3	EZM03-200
SSDERAZER rotePro4	EZR04-200
SSDERAZER rotePro9	EZR09-200

SSDERAZER オプション

製品名	製品型番
IDE→SATA 変換アダプター	EOID-100
miniSATA→SATA 変換アダプター	EOMS-100
NGFF(M.2)→SATA 変換アダプター	EONG-100
microSATA→SATA 変換アダプター	EOMI-100
CF→SATA 変換アダプター	EOCF-100
CFast→SATA 変換アダプター	EOFA-100