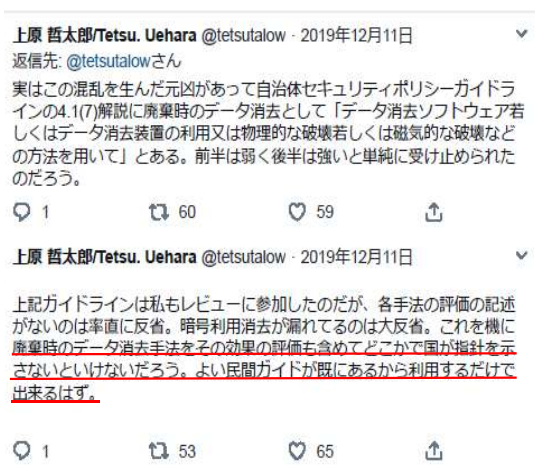
デジタル記録とデータ消去

HDD、SSDとデータ抹消（NIST SP800-88）

データ適正消去実行証明協議会
技術顧問　　沼田　理
（ADEC：Association of Data Erase Certification）
https://adec-cert.jp/

データ抹消ガイドラインの有り方は？



神奈川県の情報流出防止策

神奈川県庁総務局ICT推進部情報システム課の発表した
「県情報を保存するために使用した情報機器からの情報流出防止策」
https://www.pref.kanagawa.jp/docs/fz7/cnt/documents/boshisaku.pdf　から抜粋
第二章 対策
1 対 策 1
（1）抹消措置の方法
ア 契約事業者への返却前 ➡ ① データ消去（専用ソフトウェア又は磁気的破壊）【県職員】
② 磁気的破壊【契約事業者】
③ 物理的破壊【契約事業者】

（ア） 職員によるデータ消去（専用ソフトウェア又は磁気的破壊）を実施してから、更に契約事業者による磁気的破壊及び物理的破壊を行う
（イ） 職員による磁気的破壊によるデータ消去は、専用ソフトウェアによるデータ消去が困難なサーバ等に限って実施
（ウ） 磁気的破壊は専用の装置を使用し、マーカーでの確認やログを記録するなど実施結果が可視化できること（職員の磁気的破壊は情報システム課が提供する装置を使用して実施）
（エ） 粉砕、穿孔、変形等、ドライブから情報を読み取ることができないよう、HDD を物理的に破壊
（オ） HDD の場合は磁気ディスクが、SSD の場合はフラッシュメモリがすべて確実に破壊される専用機器による処理であること
（カ） 抹消措置の実施有無を目視で確認できないことから、磁気的破壊のみの抹消措置は不可
（キ） 物理的破壊のみの抹消措置でも、データを復元できる恐れがあることから磁気的破壊と合わせた抹消措置が必要

NIST等の規定を良く調査して作成しているが、完全に実施するにはハードルが高いのでは？（私的見解です）

5月22日総務省の広報資料

自治体情報セキュリティ対策の
見直しのポイント

総務省

2020年５月

地方公共団体における情報セ
ポリシーに関するガイドライ
に係る検討会

これまでの議論の経過

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の改定等に係る検討会

■構成員

石井夏生利	中央大学国際情報学部教授
上原哲太郎	立命館大学情報理工学部教授
岡村　久道	弁護士　京都大学大学院医学研究科講師
（座長）佐々木良一	東京電機大学総合研究所特命
庄司　昌彦	武蔵大学社会学部メディア社
長峯　道宏	千葉市総務局情報経営部業務
塗師　敏男	横浜市総務局しごと改革室IC
半田　嘉正	富山県経営管理部情報政策課
三輪　信雄	総務省最高情報セキュリティ
若杉　健次	港区総務部情報政策課長（20

■オブザーバ
総務省自治行政局住民制度課
総務省サイバーセキュリティ統括官室
地方公共団体情報システム機構

開催実績

	【主な議
■ 第１回（令和元年12月3日）	・検討会の ・新たな自
■ 第２回（令和元年12月23日）	・ワーキン ・新たな自
■ 第３回（令和２年１月31日）	・ワーキン ・新たな自
■ 第４回（令和２年2月28日）	・ワーキン ・新たな自
■ 第５回　※書面開催（令和２年４月20日）	・自治体情
■ 第６回（令和２年５月15日）	・自治体情 ・今後の進

ポイント③：昨今の重大インシデントを踏まえた対策強化

（１）情報システム機器の廃棄時におけるセキュリティの確保

発生した事案

✓ 昨年12月6日、神奈川県において、リース契約満了により返却したハードディスクの盗難による情報流出が発生

⇒ 同日、**当面の対応**として、重要情報が大量に保存された記憶装置については、**物理的な破壊又は磁気的な破壊の方法により行うとともに、地方公共団体の職員が当該措置の完了まで立ち会いを行うなど確実な履行の担保**を要請

再発防止策の概要

① **ワーキンググループでの検討結果を踏まえて**、情報システム機器を廃棄、リース返却等をする場合、機器内部の記憶装置からの情報漏えいのリスクを軽減する観点から、**情報の機密性に応じた方法**により、**情報を復元困難な状態にする措置を徹底する必要がある**ことを助言

（参考）

分類	機器の廃棄の方法	廃棄の確認の方法
マイナンバー利用事務系に該当するもの	**①物理的な方法による破壊**（注）	**・職員による立ち会いによる確認** **・庁内において情報の復元が困難な状態までデータの消去を行った上で、物理的破壊の完了証明書の確認**
機密性２以上に該当するもの	①物理的な方法による破壊、②磁気的な方法による破壊、③ＯＳ等からのアクセスが不可能な領域も含めた領域をデータ消去装置又はデータ消去ソフトウェアによる上書き消去、④ブロック消去、⑤暗号化消去　のうちいずれかの方法を選択	適切な方法による確認
機密性１に該当するもの	上記①～⑤の方法の他、⑥ＯＳ等からアクセス可能な全てのストレージ領域をデータ消去装置又はデータ消去ソフトウェアによる上書き消去　のうちいずれかの方法を選択	適切な方法による確認

（注）リース契約による場合も、リース契約終了後、物理的破壊を行う旨、予め入札における仕様に明記の上、契約に位置付けることが望ましい。

② 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の改定時に上記内容を記載

9

今回のセミナー講演者について 蛇足です!

2018年10月24日のFacebookより

佐々木 良一
2018年10月24日 ·

ドリルはダメだが、トリムを有効にしておいて、ファイルの消去をすれば、特別のところを除いては、復元できないと思っているが、何かあるのかな。

TECHTARGET.ITMEDIA.CO.JP
SSDの廃棄方法と、SSDが「ドリルで穴を開けても復旧可能」な理由
使用済みのSSDを寄付するのは素晴らしいことのように思える。だが、データの安全を保ちたいなら話は別だ。SSDの廃棄とリサイクルは思って...

しもがいと だい、他20人　　コメント15件 シェア3件

いいね！　コメント　シェアする

沼田 理 TRIMは直接的な消去コマンドでは無いので、ブロックイレースのタイミングはコントローラに依存してしまうので、「あらゆる条件下での消去を保証する」事は出来ないと認識しています。

勿論、一般的なPCの使用条件に限定し、バックグラウンド動作の時間さえ確保できれば、特に問題となるようなことは起こらないと思いますが、、、

いいね！ · 返信する · 1年前

佐々木 良一 コメントありがとうございます。私の認識と基本的に同じですが、確かにタイミングの問題はありますね。ブロックイレースは、消去の直後と聞いているのですが具体的にどのぐらいの時間でやっているのでしょうね。
また、海外では対応に暗号化を使ってようですが、日本ではどうなんでしょうね。

いいね！ · 返信する · 1年前

佐々木 良一 前田さんのレポートの話で、2015年3月に実施された情報処理学会ＣＳＥＣ研究会で、うちの学生が次のような論文を発表したのを思い出しました。
山前碧　小林裕太　上原哲太郎　佐々木良一「SSD上の消去ファイルの復元可能性の実験と評価」　情報処理学会ＣＳＥＣ研究会（2015年3月）
トリムをオンとオフにして復元実験をいろいろやっていました。今見るとオンにした場合には直後にやっても復元できないという結果を出していました。直後というのが実際にはどのぐらいの時間か今になっては正確にはわからないのですが、結構早く復元できなくなるようですね。ただし、「100%信用することは危険が伴うと思っています。」というのはおっしゃる通りです。

いいね！ · 返信する · 1年前

沼田 理 前田さんのレポートは2015年12月のもので、今内容を調べたら、その山前さんの論文を引用している部分がありました。

3.1 SSD上の消去ファイルの復元可能性の実験と評価...
もっと見る

いいね！ · 返信する · 1年前 · 編集済み

上原 哲太郎 山前君のあと、うちの卒論生の泉君に3社ほどのSSDコントローラを試してもらったのですが、Trimつかうと5分と持たなかったですね。あっという間に0クリアされたセクタに置き換わりました。

いいね！ · 返信する · 1年前

沼田 理 それは、"論理セクタが置き換わった（リマップされた）"のであって、必ずしも"物理セクタ（ブロック）がイレースされた"ことでは無いのではないかと思うのですが。その辺はいかがですか？

すいません、改めて自己紹介しておきますと、... もっと見る

いいね！ · 返信する · 1年前 · 編集済み

佐々木 良一 皆様書き込みありがとうございます。トリムを使えば情報が復元されるリスクは、非常に小さいですが、完全な消去を保証するものでない点よくわかりました。最初この記事をアップしようかどうか迷ったのですが、いろいろなことがわかりアップしてよかったと思っています。

いいね！ · 返信する · 1年前

しもがいと だい 是非こちらにご参加の皆様とご関係者の方々にお尋ねしたいのですが、次の各言葉の処理内容はどのように認識されていらっしゃいますでしょうか？実は自分が読んだことのある文書によっては、使われ方が違うようなので、是非正しい意味（言葉遣い）を知りたいとおもっております。

1：ブロックイレース... もっと見る

いいね！ · 返信する · 1年前

上原 哲太郎 ブロックイレースはいいですよね。ガベージコレクションは「消去対象ページ（＝ガベージ）を1つのブロックに集める行為」だと理解しています。ハウスキーピングはガベージコレクションとブロックイレースを合わせた行為という理解。トリムは「Trimコマンドに対する処理」でいいと思うので消去対象セクタをコントローラが認識してフラグ立てたら十分だと思いますが、Trimという単語の語感からかハウスキーピング全体を指して使う人がいるような気がします。

いいね！ · 返信する · 1年前

しもがいと だい 上原先生、ありがとうございます。長い質問で申し訳ございませんが、以下につきましてもどうぞよろしくお願いいたしますm(_ _)m

1．ブロックイレース... もっと見る

いいね！ · 返信する · 1年前

沼田 理 長文です。

1．ブロックイレースについて... もっと見る

いいね！ · 返信する · 1年前

講師自己紹介

- 氏名：沼田　理　（ぬまた　まこと）
- 経歴
  - 電子部品、オーディオ関連企業、オランダPHILIPS社などで技術開発業務に従事。
  - 1986年より（株）ワイ・イー・データに於いて、FDD、HDD、テープドライブなど磁気記憶装置の設計開発に携わる。
  - 2001年：データ復旧のパイオニア、オントラック事業部に異動、
    2006年：事業部長。
  - 2010年～日本データ復旧協会事務局長、データ復旧関連複数社の顧問。
    技術情報、Web原稿の提供、
    IDF（デジタル・フォレンジック研究会）データ消去分科会メンバー
  - 2019年～ADEC（データ適正消去実行証明協議会）技術顧問
    KLDiscovery Ontrack社　技術担当広報（20年4月～一時帰休中）
    （旧 Kroll Ontrack）

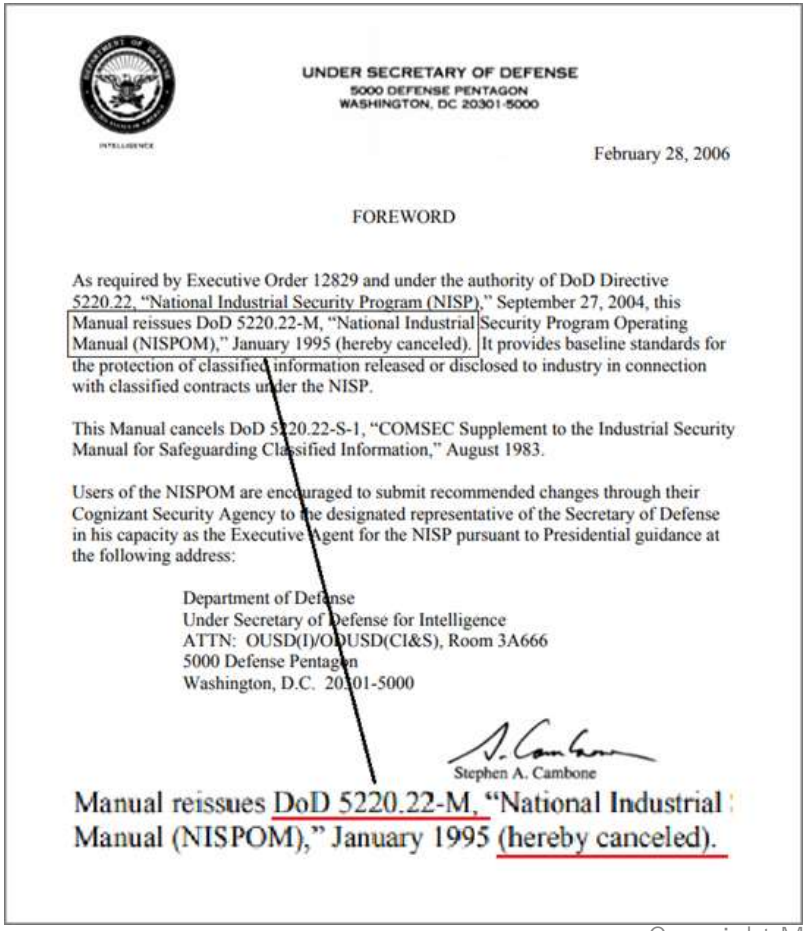
データ消去ガイドラインの現状

- **日本では、JEITA**（一般社団法人電子情報技術産業協会）より2002年4月11日に、「パソコンの廃棄・譲渡時のハードディスク上のデータ消去に関するガイドライン」、**RITEA**（一般社団法人情報機器リユース・リサイクル協会）より2007年2月19日に、「情報機器の売却・譲渡時におけるハードディスクのデータ消去に 関するガイドライン」が発表され、更に**NISC**（内閣サイバーセキュリティセンター）から2018年7月25日に、「府省庁対策基準策定のためのガイドライン」が発表されているが、**「データ消去の手段」についての具体的な技術論は現在に於いても存在しない。**
- **世界では、**最も先進的な立場にあるアメリカの国防総省（Department of Defense: DoD）が、**1973 年に「DoD 5200.28-M」に、現在においても標準的である3回の上書き方式を提唱**した事に始まり、米国商務省（Department of Commerce）傘下の**NIST（National Institute of Standards and Technology：米国標準技術研究所)が、紙媒体を含む情報の抹消方法を整理したSP800-88を2006年**に発表し、標準化に向けた取り組みを行っている。また、技術の進化に対応した改訂も行われ、**2014年12月に発行されたRev.1が最終版。**
- **物理的な破壊、外部磁気による電子記憶のデータ抹消については、**
  アメリカのNSA/CSS（National Security Agency/ Central Security Service）の、
  Evaluated Products List for Hard Disk Destruction Devices
  Evaluated Products List for Magnetic Degaussers （2019 Dec.が最終版）

USAのガイドライン

- DoD（国防総省：Department of Defense）
  - 1973年「DoD 5200.28-M」
    - 現在においての標準的とも言える、3回の上書き方式を提唱
  - 1995年「5220.22-M Supplement.1」
    - **上書 3 回**（固定値、補数、乱数、その後検証を実施）方式を発表
  - 2006年 2 月
    - **データ消去の具体的な方法等の記載を取り消し。**
- NIST（国立標準技術研究所：National Institute of Standards and Technology）
  - 2006年SP800-88
    - **2001年以降に製造された15GB 以上のATAディスクに ついては、上書き抹消を行う場合の上書き回数は1 回で十分である。**
    - **ATAコマンドを利用したSecureErase**の使用を、HDDの全領域の消去が可能であり最高機密の機密情報に対する抹消手段として容認。
  - 2014年12月　SP800-88rev.1
    - **SecureEraseを含む上書き消去を、電子記憶媒体には製造者のみが管理可能な領域が存在し、その領域に対するアクセス手段が存在しない理由により、最高機密に対する抹消手段から除外。**
    - 暗号化抹消（Cryptographic Erase：CE）やSSD、スマホ等について言及・追加

HDDのデータ消去時の上書き回数



UNDER SECRETARY OF DEFENSE
5000 DEFENSE PENTAGON
WASHINGTON, DC 20301-5000

February 28, 2006

FOREWORD

As required by Executive Order 12829 and under the authority of DoD Directive 5220.22, "National Industrial Security Program (NISP)," September 27, 2004, this Manual reissues DoD 5220.22-M, "National Industrial Security Program Operating Manual (NISPOM)," January 1995 (hereby canceled). It provides baseline standards for the protection of classified information released or disclosed to industry in connection with classified contracts under the NISP.

This Manual cancels DoD 5220.22-S-1, "COMSEC Supplement to the Industrial Security Manual for Safeguarding Classified Information," August 1983.

Users of the NISPOM are encouraged to submit recommended changes through their Cognizant Security Agency to the designated representative of the Secretary of Defense in his capacity as the Executive Agent for the NISP pursuant to Presidential guidance at the following address:

Department of Defense
Under Secretary of Defense for Intelligence
ATTN: OUSD(I)/OUSD(CI&S), Room 3A666
5000 Defense Pentagon
Washington, D.C. 20301-5000

Stephen A. Cambone

Manual reissues DoD 5220.22-M, "National Industrial
Manual (NISPOM)," January 1995 (hereby canceled).

- 米国においても、**国防総省規格DoD 5220.22-M、米国国家安全保障局方式NSA 130-1によって定められた3回上書き**およびベリファイを選択・指定していることが多いが、この規格は**2006年2月に改版され、過去に記載されていたデータ消去の具体的な方法等の記載は一切取り消された。**
- 2006年に米国国立標準技術研究所(NIST)が発表したSP800-88では、「**2001年以降に生産された、15GBytes以上のHDDはデータは、研究の結果1回上書きするだけで効果的に消去することが可能**」と明記された。**理由：大容量化による下層データのはみだし幅の微小化**）

・**１TB/プラッタの物理的寸法（TDKヘッド工場による）**

トラック間隔：70nm
書込み幅　　：55nm
読み出し幅　：35nm
トラッキング要求精度：8nm

コロナウイルスの直径が
約0.1μm=100nmですから、
トラック幅はその半分程度。

NIST SP800-88の特徴

1）データ（情報）の重要（機密）性・ランク

低度：情報が漏えいした場合の影響は限定的なレベル。

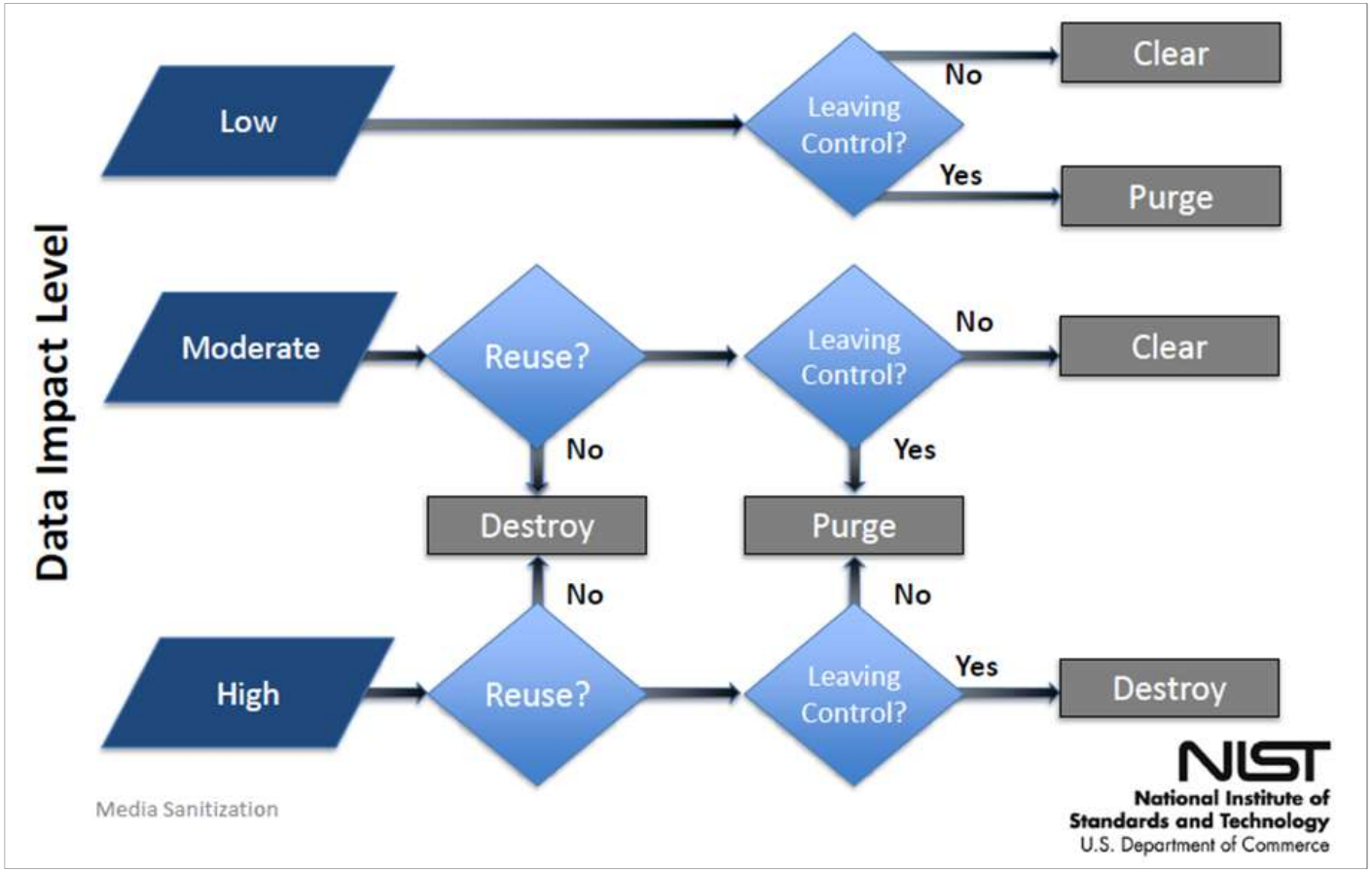
中度：情報が漏えいした場合、重大な悪影響を及ぼすレベル。

高度：情報が漏えいした場合、危機的・致命的な悪影響を及ぼすレベル。

2）抹消の種別・ランク

「Clear(消去)」　：Resistant to keyboard attacks.
一般的に入手できるツールを利用した攻撃に対して耐えられること。
「Purge(除去)」　：Resistant to laboratory attacks.
研究所レベルの攻撃に対して耐えられること。
「Destroy(破壊)」：Resistant to recreation of media.
媒体の再生（再組立等）に対して耐えられること。

NIST SP800-88Rev.1



注：米国政府・行政機関向けの判断基準を示す。

- 抹消方法は、

①「**情報の機密度**」と、

② データ抹消後の

「**記憶媒体の管理方**」

を勘案して、

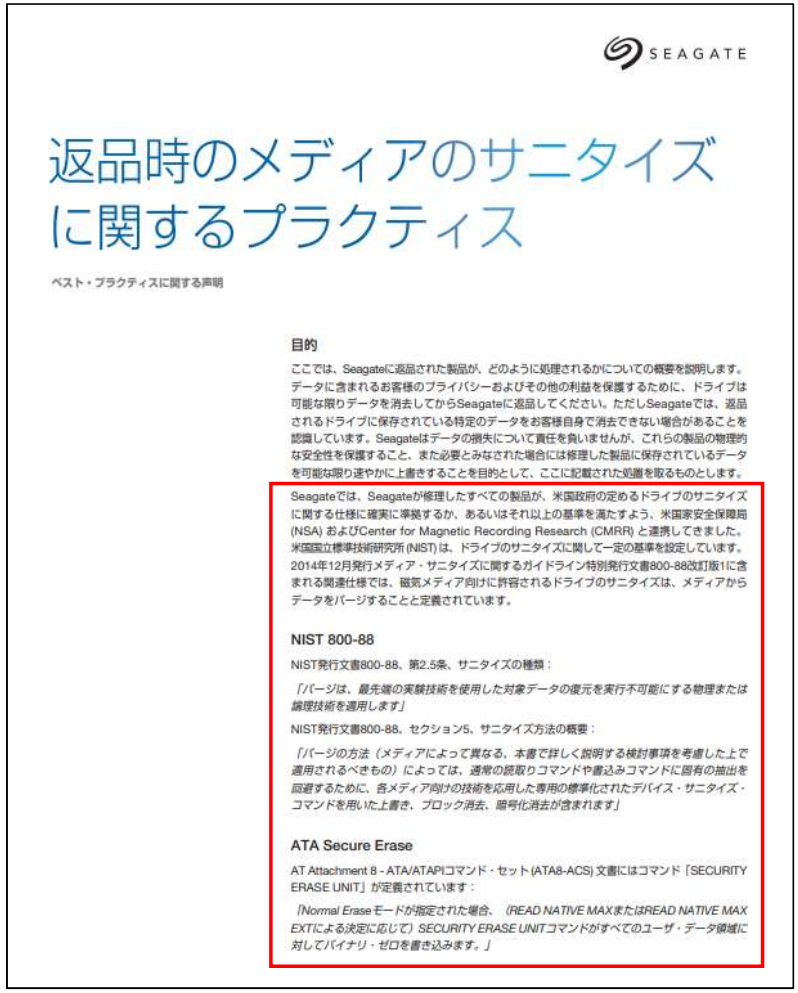
③**データの所有者・管理者**

の責任で選択決定する。

情報の機密度による、抹消ランク選択の具体例（ADECによる）

機密度	抹消ランク	消去方法(HDD)	情報の種類	対象
高 ↑	Destroy(破壊)	物理的破壊 ~~外部磁界等による消去~~	行政、官公庁に属する情報のうち高度な機密性を持つ情報	企業・法人、官公庁の機密性の高いサーバ等
	Purge(除去)	ANSI消去コマンド、暗号化消去、外部磁界等による消去	個人情報データベース企業秘密、知財情報、経営情報など	
	Clear(消去)	上書消去 DoD規格等の（複数回も含む）	個人のプライバシー、企業・法人の業務関連情報など日常的な情報	個人用PC、企業・法人の通常業務用PC 暗号化ソフト使用PC

NIST SP800-88とHDDメーカ



SEAGATE

返品時のメディアのサニタイズに関するプラクティス

ベスト・プラクティスに関する声明

目的

ここでは、Seagateに返品された製品が、どのように処理されるかについての概要を説明します。データに含まれるお客様のプライバシーおよびその他の利益を保護するために、ドライブは可能な限りデータを消去してからSeagateに返品してください。ただしSeagateでは、返品されるドライブに保存されている特定のデータをお客様自身で消去できない場合があることを認識しています。Seagateはデータの損失について責任を負いませんが、これらの製品の物理的な安全性を保護すること、また必要とみなされた場合には修理した製品に保存されているデータを可能な限り速やかに上書きすることを目的として、ここに記載された処置を取るものとします。

Seagateでは、Seagateが修理したすべての製品が、米国政府の定めるドライブのサニタイズに関する仕様に確実に準拠するか、あるいはそれ以上の基準を満たすよう、米国家安全保障局(NSA) およびCenter for Magnetic Recording Research (CMRR) と連携してきました。米国国立標準技術研究所 (NIST) は、ドライブのサニタイズに関して一定の基準を設定しています。2014年12月発行メディア・サニタイズに関するガイドライン特別発行文書800-88改訂版1に含まれる関連仕様では、磁気メディア向けに許容されるドライブのサニタイズは、メディアからデータをパージすることと定義されています。

NIST 800-88

NIST発行文書800-88、第2.5条、サニタイズの種類：

「パージは、最先端の実験技術を使用した対象データの復元を実行不可能にする物理または論理技術を適用します」

NIST発行文書800-88、セクション5、サニタイズ方法の概要：

「パージの方法（メディアによって異なる、本書で詳しく説明する検討事項を考慮した上で適用されるべきもの）によっては、通常の読取りコマンドや書込みコマンドに固有の抽出を回避するために、各メディア向けの技術を応用した専用の標準化されたデバイス・サニタイズ・コマンドを用いた上書き、ブロック消去、暗号化消去が含まれます」

ATA Secure Erase

AT Attachment 8 - ATA/ATAPIコマンド・セット (ATA8-ACS) 文書にはコマンド「SECURITY ERASE UNIT」が定義されています：

「Normal Eraseモードが指定された場合、（READ NATIVE MAXまたはREAD NATIVE MAX EXTによる決定に応じて）SECURITY ERASE UNITコマンドがすべてのユーザ・データ領域に対してバイナリ・ゼロを書き込みます。」

返品時のメディアのサニタイズに関するプラクティス（Seagate）
https://www.seagate.com/files/www-content/support-content/warranty/_shared/Files/media-sanitization-practices-032116_JP.pdf

Seagateでは、Seagateが修理したすべての製品が、米国政府の定めるドライブのサニタイズに関する仕様に確実に準拠するか、あるいはそれ以上の基準を満たすよう、米国家安全保障局(NSA) および**Center for Magnetic Recording Research (CMRR)** と連携してきました。
米国国立標準技術研究所 (NIST) は、ドライブのサニタイズに関して一定の基準を設定しています。
2014年12月発行メディア・サニタイズに関するガイドライン特別発行文書800-88改訂版1に含まれる関連仕様では、磁気メディア向けに許容されるドライブのサニタイズは、メディアからデータをパージすることと定義されています。

NIST SP800-88と日本の官公庁

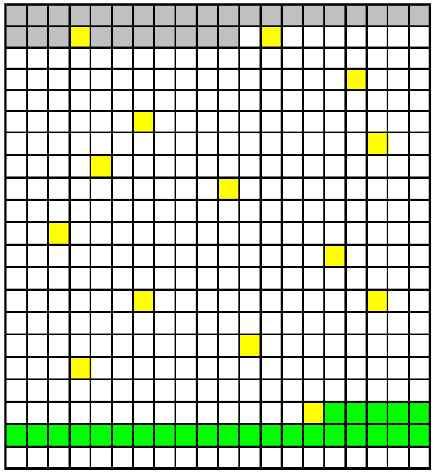
- 電気通信事業における個人情報保護に関するガイドライン

  （平成16年総務省告示第695号。最終改正平成22年総務省告示第276号）の解説に対する意見及びそれに対する考え方

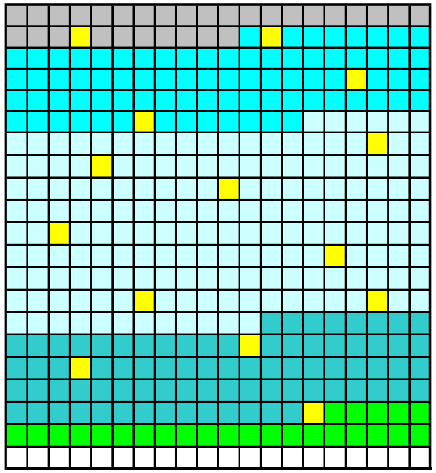
	（個人）	
意見４	データの削除方式について、技術的に確証のとれた削除方法を規定するべき。	
第２２条　（漏えい等が発生した場合の対応） （解説） （２）②　ii 【７、８頁】	データ削除方法の規定 単純なデータ削除では、復元可能であるため、技術的な確証のとれた削除方法を規定する必要がある。例：現米国国家安全保障局（NSA）推奨方式、金融庁推奨方式など） （個人） 複合鍵や暗号化された情報の削除につきまして、単純なデータ削除では、復元可能であるため、ガイドラインでは技術的な確証のとれた削除方法を規定する必要があると考えます。 （例：現米国国家安全保障局（NSA）推奨方式、金融庁推奨方式など） （株式会社メトロジー）	復元可能な方法であれば削除がなされていないと考えます。適切な削除方法としては、例えば、JEITAの「パソコン廃棄・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」に則った手法（例：専用ソフトウェアによるデータ消去）、あるいはNIST 800-88でPurging（実験室レベルでデータ復元不可能と定義）に分類されている手法（例：Secure Eraseコマンド）又は相当の手法（例：ATA Enhanced Secure Eraseコマンド）を想定しております。
意見５	遠隔操作により復号鍵の削除だけではなく、特定データそのものを削除する	

HDDの内部領域とデータ消去-1

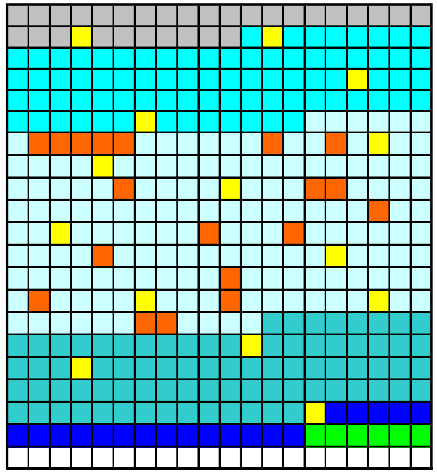
①工場出荷（物理フォーマット後）



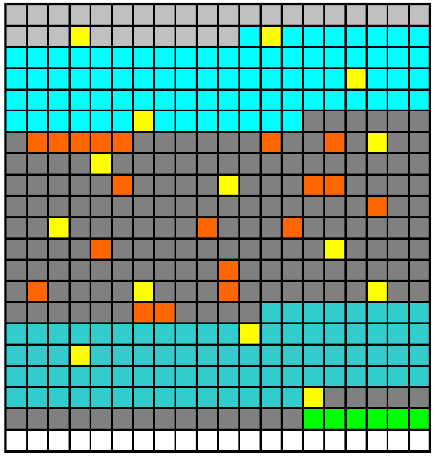
②製品組込み（初期状態）



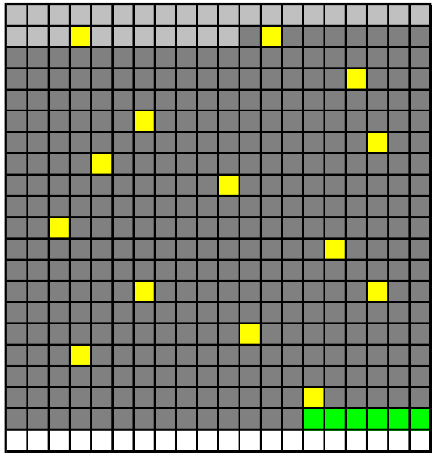
③製品使用中・使用後

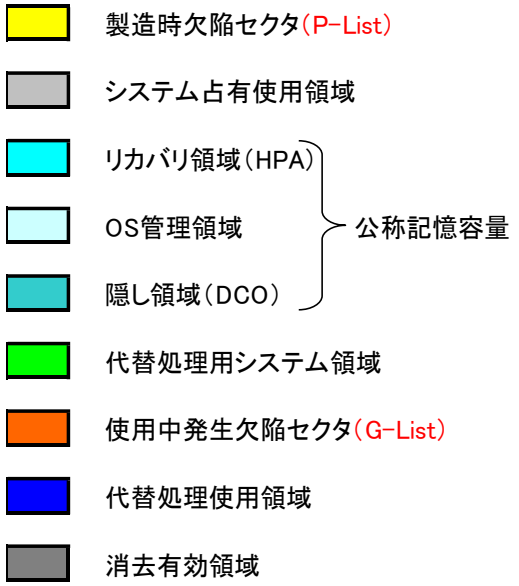


④OS上のソフトで上書き消去（クリア）



⑤Enhanced Secure Erase（コマンド）で消去（パージ）





HDDの内部領域とデータ消去- 2

①工場出荷状態：物理フォーマット時に欠陥の検出されたセクタは、「製造時欠陥セクタ」P-Listとしてシステム情報上に記録され、アクセス範囲から除外される。HDDのファームウェア等が書き込まれる部分をシステム占有使用領域として確保、使用中に「不良セクタ」が発生した場合に代替処理を行うための「代替処理用予備領域」も確保、ユーザ・データ領域として公称記憶容量と一致する領域に対してLBAを 0 から順番に割り当て、残った部分は未使用（余剰）領域となる。

②製品組み込み（初期状態）：必要に応じて、ユーザ・データ領域内に容量の大きな媒体をサービス用として旧型のPC用の小さい容量に一致させるためのDCOや、リカバリ領域等に使用するHPAを、OSが認識しない隠し領域として作成する。残りの部分がOSやユーザ作成データ等を保存する領域となる。

③製品使用後：使用中にリードエラーが検出されると、リトライ処理が行われ、同一セクタで頻発する場合は、リフレッシュ処理やペンディング処理が行われ、読み出したデータを「代替処理用予備領域」に書き込み、リードエラーの発生した元のセクタのLBAを付与し、元のセクタはOSのアクセス範囲から除外される「再割り当て済セクタ」としてG-List（ディフェクトリスト）に記録される。**この時、元のセクタに書き込まれているデータに対する消去は行われない。**

④OS上で上書き消去（Clear）：OS経由でアクセス可能な範囲に対して上書き消去が実行されるが、**システム占有使用領域、製造時欠陥セクタ、HPA、DOCや、代替処理による「再割り当て済セクタ」、未使用（余剰）領域には書き込み処理は行われない。**これは、**グートマン方式による35回等の複数回の上書きを実行しても変化することは無い。**

⑤Enhanced Security Eraseで消去（Purge）：Enhanced Security Eraseでは**LBAの付与されている範囲全てと「再割り当て済セクタ（LBAが付与された履歴のあるセクタ）」に対する消去**が行われるが、**システム占有使用領域、製造時欠陥セクタ、未使用（余剰）領域は消去は行われない。この部分を抹消しようとすると、物理的な手段（Destroy）が必要になる。**

データ消去ランク選定の理由例-1

１）Clear(消去)

HPAは、PCを購入時点の初期状態に復帰させるリカバリ機能のための情報が記録されており、PCの使用によってユーザが作成した情報の保存が行われる領域ではない。

DCOは容量の大きな記憶媒体を旧型の容量の小さなPCのサービスパーツとして使用するための意図的な容量削減を目的に設定した領域であり、PCの使用によってユーザが作製した情報の保存が行われる領域ではない。

「再割り当て済セクタ」は、一般的なデータ復旧やデジタル・フォレンジック用途のソフトウェアではアクセス不能であり、セクタ単位のデータの断片の可能性が高く、ファイル全体が読み出される可能性は低いので、消去作業は不要であり、OSが管理している領域が消去できればそれ以上の必要は無い。

２）Purge(除去)

HPA、DCO、「再割り当て済セクタ」やSSDの余剰領域（オーバプロビショニング）にアクセスしデータの読み出すことは、ソフトウェアでは不可能であるが、一部のデータ復旧やデジタル・フォレンジックを行う事業者の所有する機器を用いることによりアクセスすることは可能であると共に、データ復旧業者からの聴取結果では、取り扱うデータ復旧案件のうち約6割の原因がリードエラーであり、その大部分が読み取り可能であることから、情報の重要度、マルウェア存在の可能性等により万全を期すためには消去を行なうことが必要である。

データ消去ランク選定理由の例-2

３）Destroy(破壊)

2015年2月に情報セキュリティ関連業者であるKasperskyが、
https://blog.kaspersky.com/equationhddmalware/7623/　において、HDDのファームウェア領域に潜むマルウェアの存在を公表し、Googleも2016年2月に発表したレポート
http://research.google.com/pubs/archive/44830.pdf　において、第一の一般的な問題は、最近のHDDの持つファームウェアのサイズと複雑さは、（HDDやホストを攻撃するセキュリティバグを含む）バグにつながるということである。HDDのファームウェアアタックは可能であるだけでなく、既に使われたようである。これを解決するために、ファームウェアの真正性を保証し、許可なく行われる改竄から保証することが容易でなければいけないことは明白であり、長期的には他のシステムに既に導入されているような堅固な防御技術を適用しなければならない。我々は、短期的にはディスクへの物理的アクセスを制限することや、ファームウェアを書き直す能力を持つホストOSから不正コードを隔離することによって、この問題に対する解決を図る。と表明している。

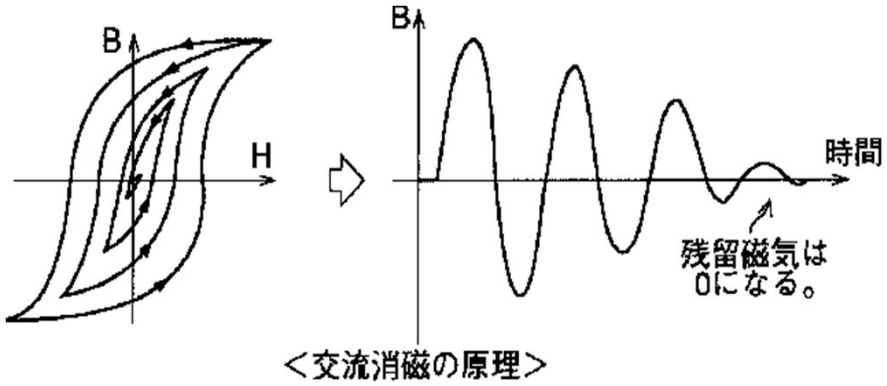
　またウェブカメラやルータ等の電子機器の不正なファームウェアの存在が否定できない現状では、どのような領域であってもユーザが作成した情報の存在を絶対的に否定することは出来ず、抹消作業が行われないことが判明している領域が存在することを許容することは出来ず、万全を期す必要がある。

米中間のHUAWEIの5Gインフラ機器使用問題に類似レベル？？

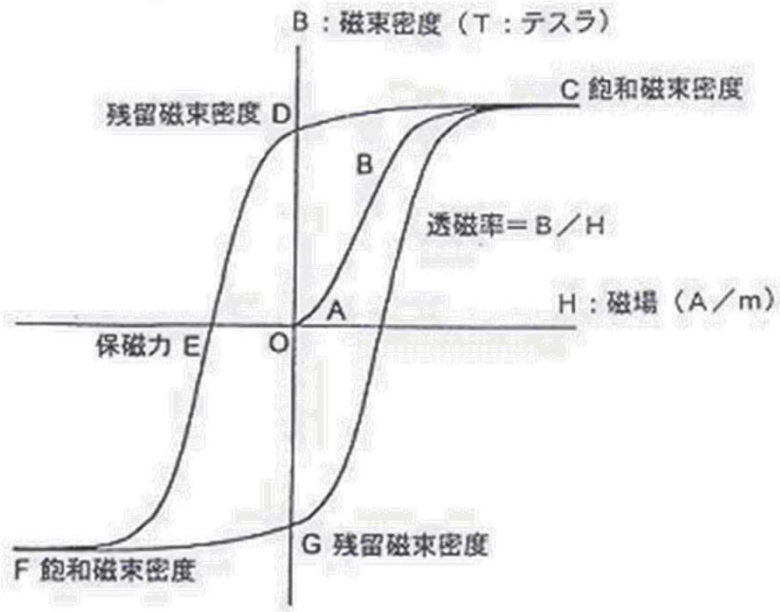
デジタル磁気記録の基本- 1

HDD/FDDでは消去動作は存在しない。

- デジタル磁気記録は、
  飽和磁気記録であり、
  上書＝消去である。



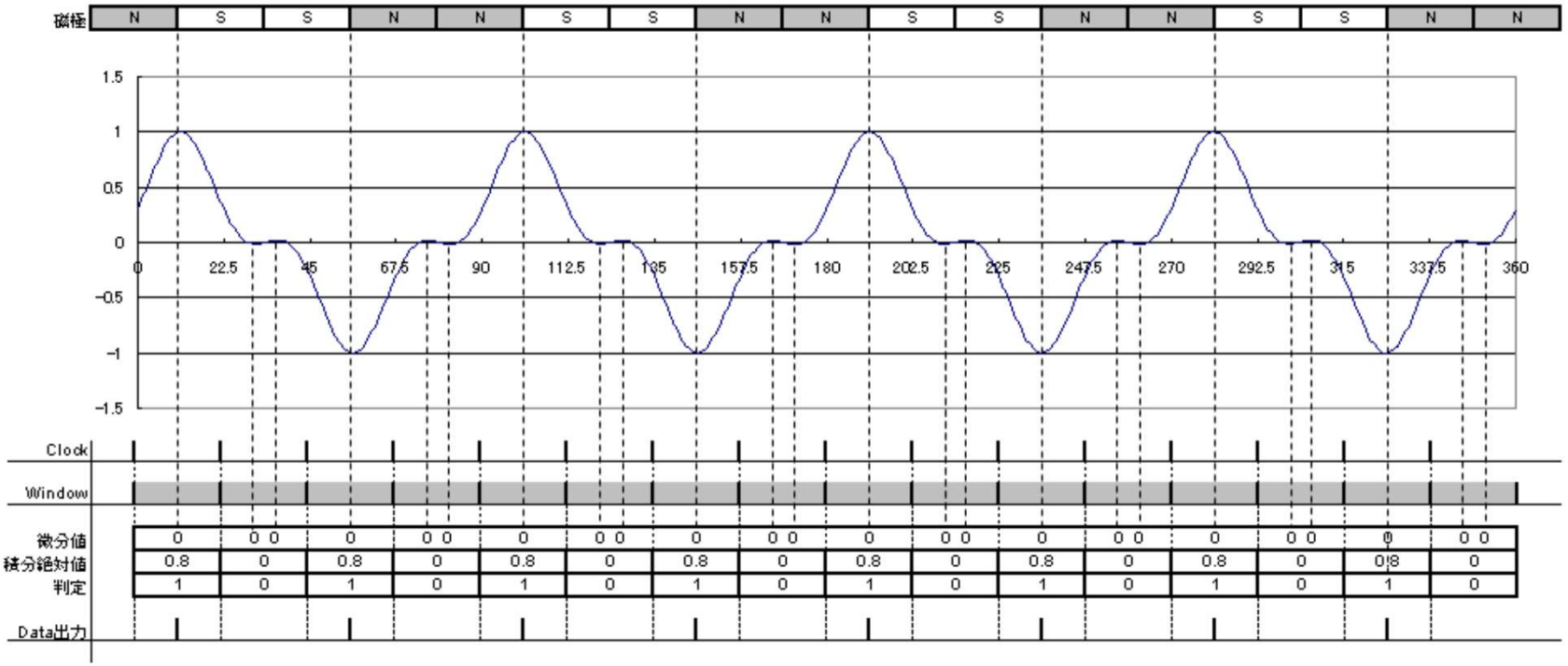
<交流消磁の原理>



B－H曲線（磁気ヒステリシス曲線）

デジタル磁気記録の基本- 2

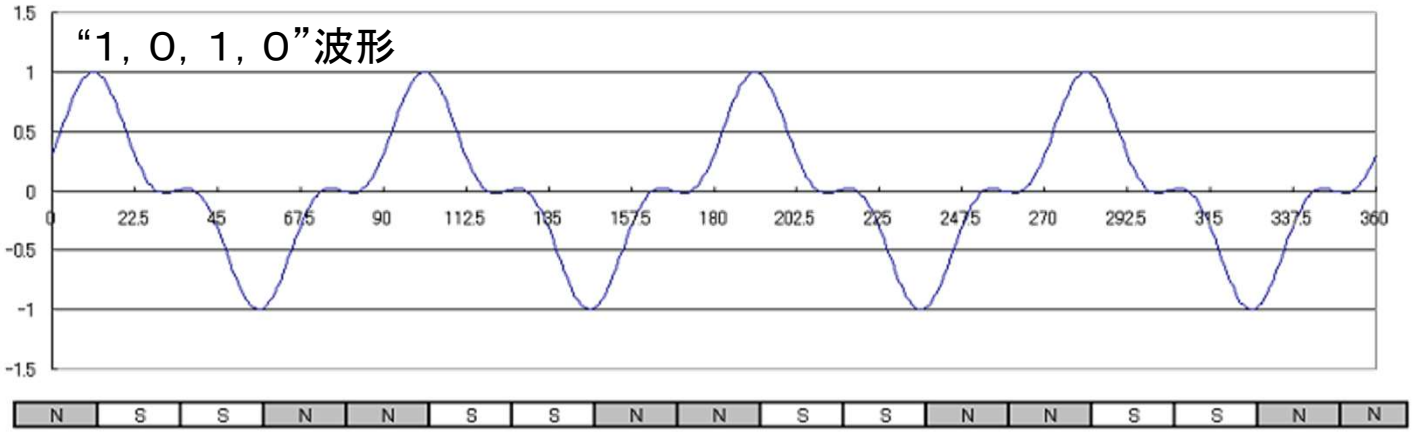
円盤上の磁気ーデジタル信号の生成

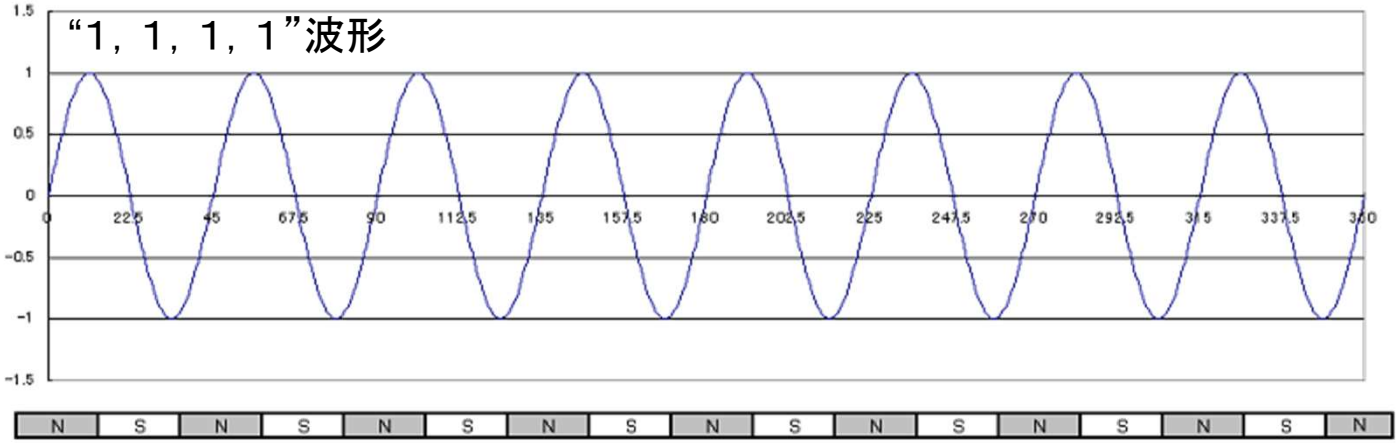


例： 微分値≒0 and 積分値>|0.5|⇒”1”　 微分値≒0 and 積分値<|0.5|⇒”0”

デジタル磁気記録の基本- 3

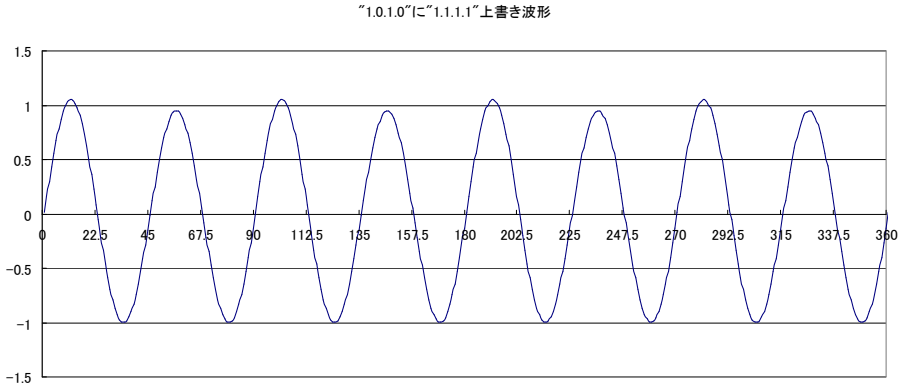
残留磁気





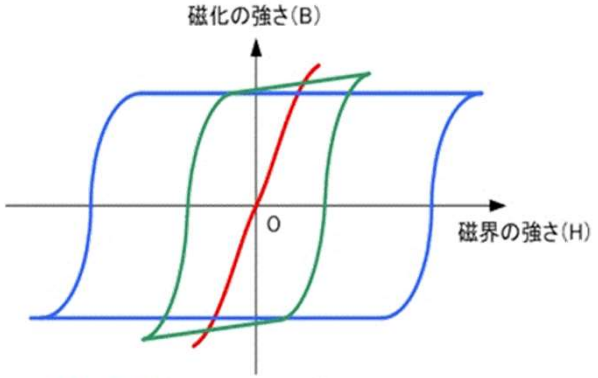
デジタル磁気記録の基本- 4

上書の実際



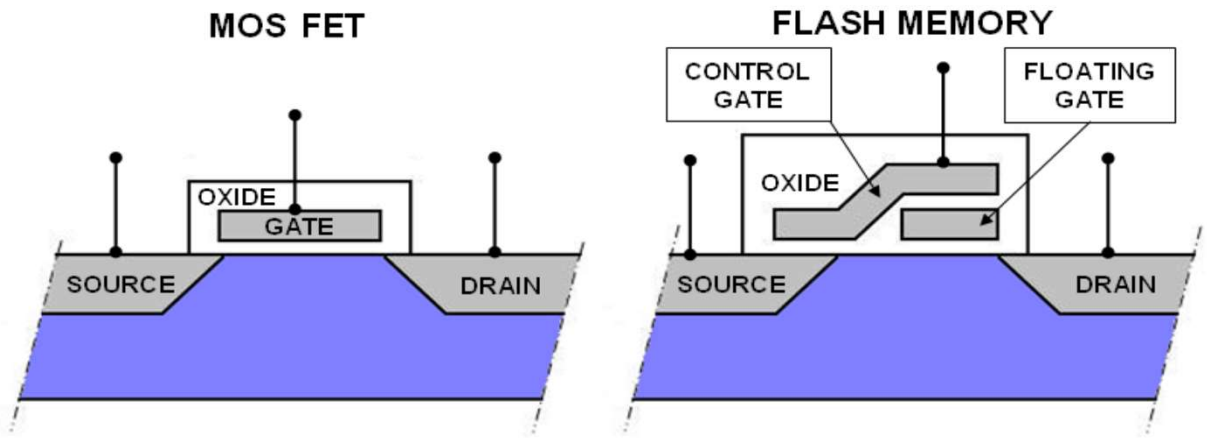
•古いデータは、約1/30～1/50程度に減衰するが、Read波形に歪となって影響が残る。

•その歪部分だけを取り出すことが出来れば、データ復旧することが、理論的には可能といえる。



フラッシュメモリとSSD-1

- SSDのデータ記録
  - NAND型Flash ROMの内部構造と動作



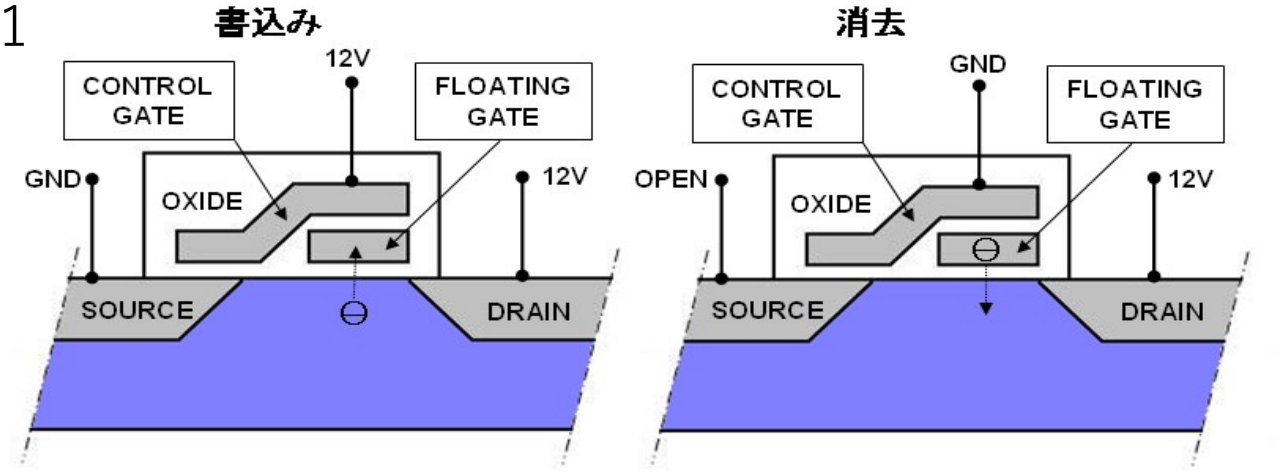
MOS（Metal-Oxide-Semiconductor）型FET（Field effect transistor：電界効果トランジスタ）と、

1. ソース（Source）とドレイン（Drain）電極が両端に設けられた半導体の中央部に、絶縁体（Oxide）で隔てられた　金属（Metal）の、印加電圧によってソース　－ドレイン間の抵抗値を制御するゲート（Gate）電極を持つ素子の構造に類似。

2. ゲート電極が制御ゲート（コントロールゲート：Control Gate）と浮遊ゲート（フローティングゲート：Floating Gate）の二重構造であることが相違点。

フラッシュメモリとSSD-2

- データ書込み/消去-1



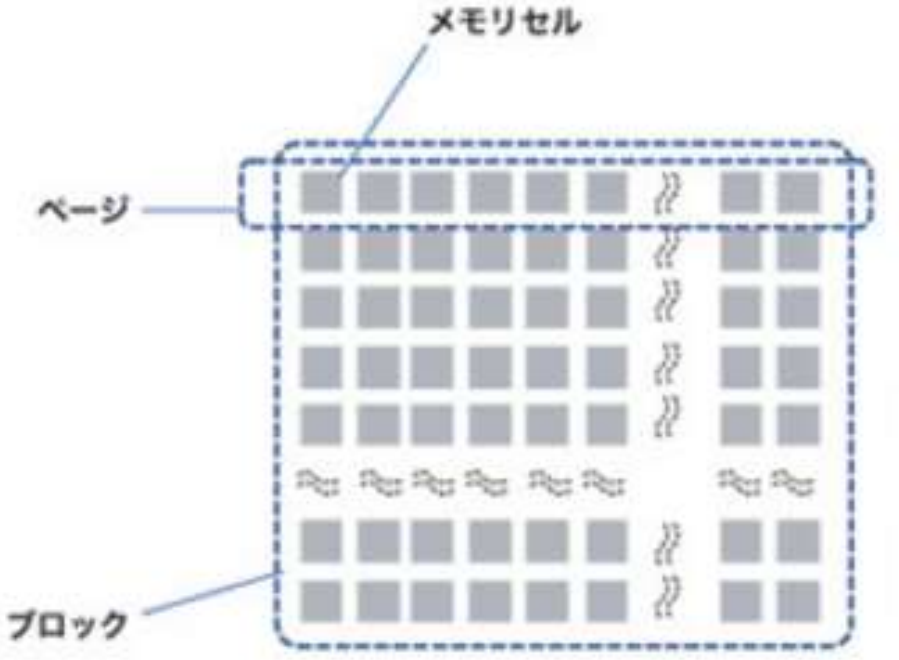
•コントロールゲートとソースードレイン間の半導体との相対的な電圧の操作によって、フロー ティングゲートへの電荷の注入(書き込み:充電)や放出(消去:放電)を行い、(フローティング) ゲートの電荷でソースードレイン間の抵抗に変化を与え、データの“0”、“1”を決定。

•MOS-FETは電源OFFによりゲートの電荷は消滅するが、フラッシュメモリーは電源停止後も、ゲート周囲が絶縁体であるため電荷が保持され不揮発となるが、自然放電による寿命も存在。

•フローティングゲートの電荷を、単純なON/OFF(“0”、“1”)の2値で制御する物がSLC型、中間レベルの段階的な判別を可能にした物がMLC型(4値)やTLC型(8値)。

フラッシュメモリとSSD- 3

- データ書込み/消去



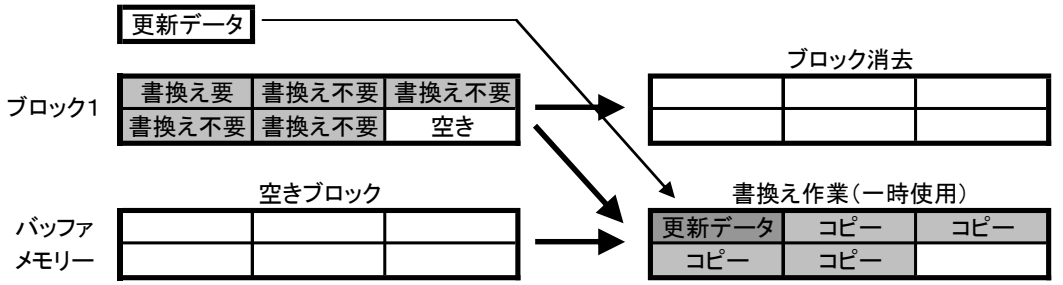
•HDDは、動作の最小単位は「セクタ」で、OSの管理は、そのセクタの集合体であるクラスタ

•SSDでは、メモリーIC内部に構成されている「ページ」と、その集合体である「ブロック」単位で管理

- 書き込み動作は2、4、8Kバイトで構成されている「ページ」。
- 消去動作は32～256ページで構成されている「ブロック」。

フラッシュメモリとSSD-4

- データ書換基本動作
  - ・基本　（USBメモリやメモリーカード）



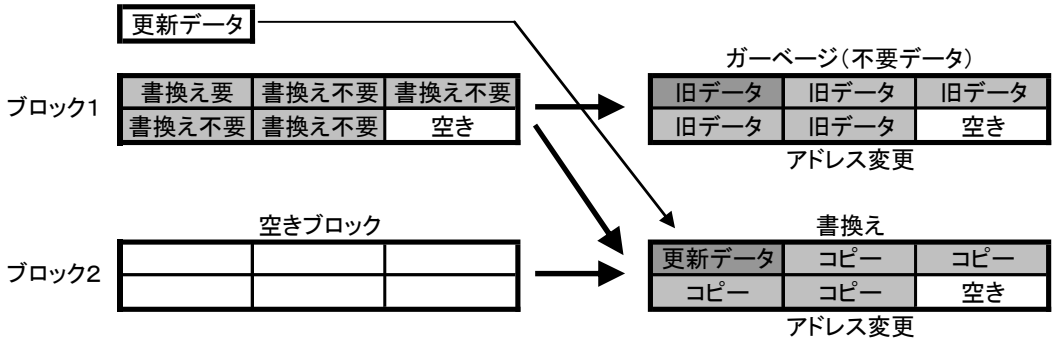
ⅰ．書き換えるページを含むブロック全体をすべてバッファー（メモリーや仮想メモリー）に読み出す

ⅱ．バッファー上で書き換えるページ部分のデータを書き換える

ⅲ．元のブロックのデータを消去する

ⅳ．バッファーの内容を元のブロックに書き戻す

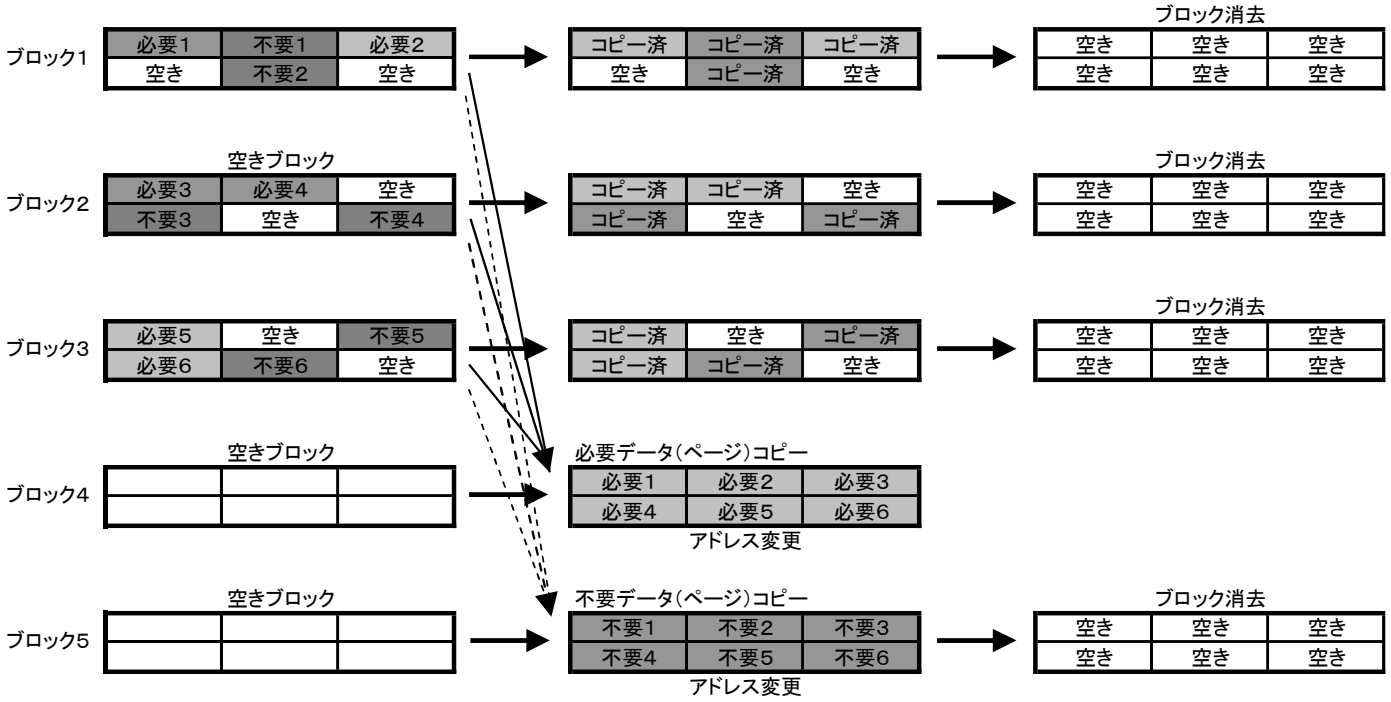
・高速化　（SSD）



・空きブロックが十分に存在する状態では　高速だが、空き容量の低下により動作速度が低下

フラッシュメモリとSSD-5

• データ書換高速化技術-1　・ガベージ・コレクション（Garbage Collection）



SSDの消去動作の基本単位であるブロックを効果的に使用するための技術で、データの断片化などによって、一つのブロック内に、必要なデータ（ページ）と不要となったガベージデータ（ページ）の混在が発生した場合に、必要データと不要データを、それぞれ別のブロックに集めることによって、消去可能なブロックを多く確保し、SSDのアイドル時間にそのブロックの消去・初期化を行い、新規のデータの書込み可能な状態にして準備・待機させることで、書込み・書き換え動作速度低下を予防する。
HDDのデフラグに類似

フラッシュメモリとSSD- 6

- データ書換高速化技術- 2
  （オーバ・プロビジョニング：Over Provisioning）

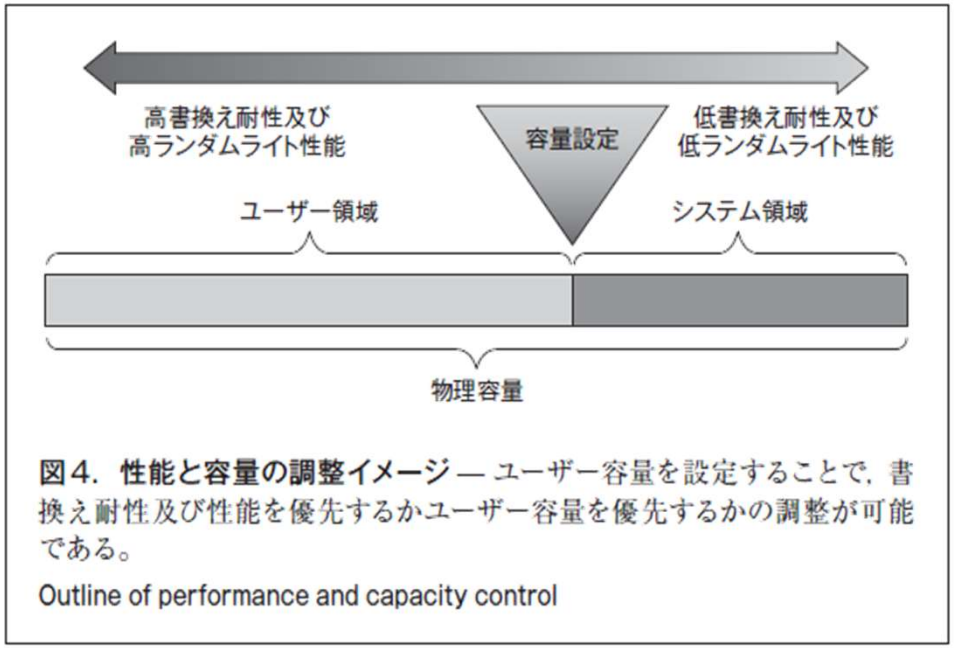


図4．性能と容量の調整イメージ― ユーザー容量を設定することで，書換え耐性及び性能を優先するかユーザー容量を優先するかの調整が可能である。

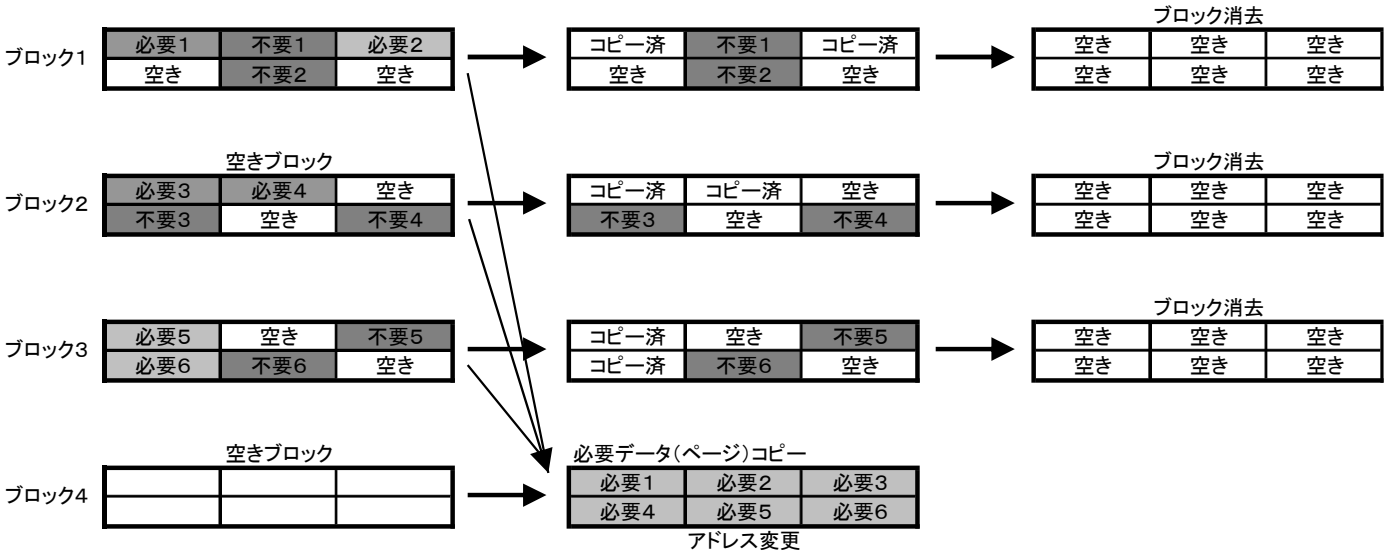
Outline of performance and capacity control

•SSDの内部の物理的な記憶容量を
ユーザの使用する公称容量に対して
大きくし、システム（ファームウェア）動作
専用領域として確保し、実使用容量の
増加、ウェアレベリングや、不良ブロック
の置換などによって発生する書換え動作
時の作業領域の減少に対しても、十分な
作業領域を確保し高速動作を維持する。
（サーバ用途で最大30%程度）

•SSDの使用目的によってユーザ領域と
オーバ・プロビジョニング領域の比率を
ユーザが自由に設定可能なSSDもある。

フラッシュメモリとSSD-７

・データ書換高速化技術-3　　・トリム（TRIM）



SSDがHDDと異なる特性を持った記憶装置であることを、区別して取り扱うことを行うようになったWindows7以降のSSD専用のコマンドで、ファイルの削除・更新などで、不要なデータが書き込まれているセクタが発生した場合に、SSDのコントローラに対し、OSが不要なセクタアドレスを通知する機能。

トリムが有効ではない（対応したOS・SSDではない）場合は、ガベージ・コレクションによるデータ（ページ）の分別作業も、対象となるページ、ブロックに存在する全てのデータを対象とした書き換え動作によって行われるが、トリムが有効な場合は、通知を受けた消去可能なセクタ（データ）の移動動作（ガベージ・コレクション）は原則的には不要となるので、動作速度の低下を予防できる。**この動作は、直接の消去コマンドでは無く、バックグラウンド動作の予約である。実験結果として、データの復旧が不可能になるまでに15分～1時間を要したことが報告されている。**

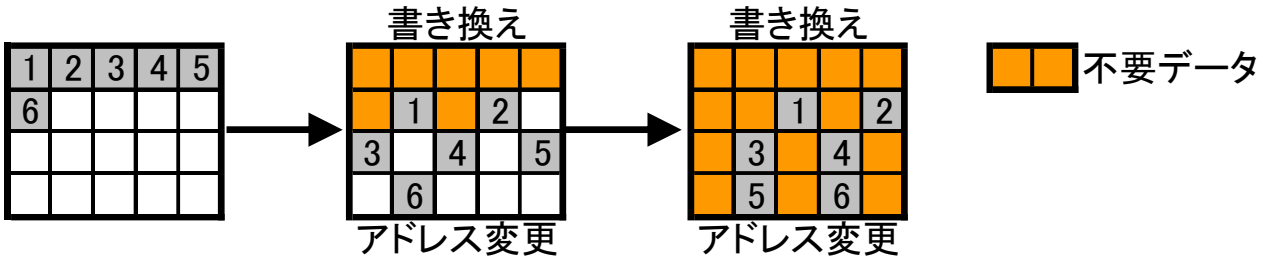
フラッシュメモリとSSD-8

- 長寿命化技術
  - ウェアレベリング

    特定のブロックへの書き換えが集中すると、メモリセルが劣化して、そのページ・ブロックが不良化してしまう。

    コントローラの特殊なアルゴリズムにより、書き換えが特定のページ・ブロックに集中しないように分散化させる。

    ページのアドレス変更は、書き換えと同時に行われるので、そのブロックに対する消去が行われるまで、不要となったデータが消去されずに残存する。



SSDのデータ消去（まとめ）

1）SSDに使用されているNAND型フラッシュメモリは、データの書き換えをセクタや、2,4,8KBで構成されているページ単位で行うことはできません。消去は32~256ページの集合体であるブロック単位で行われます。**書き換え動作は、データの書き込まれていないページに、新しいデータを書き込み、従来のLBAを付与**することで、上書きがされたように見せています。**古いデータの残っているページには別のアドレスが与えられ、ブロック消去が行われるまで、データが書き込まれた状態で待機**しています。

2）NAND型フラッシュメモリには、データ書き込み回数に制限（寿命）があるので、SSDの寿命を延ばすため、搭載されているコントローラーは各ページの書き込み回数（損傷度合い）を平準化するようにアドレスの再振り当てを行っていて、これをウェアレベリングと呼んでいます。

3）また、SSDにはシステムが管理する、バックグランド作業用の余剰領域（オーバ・プロビジョニング）が用意されており、上書きによるデータ消去を実行した場合でも、消去の目的としている上書き対象のページには書き込みは行われず、消去済みの空きページや、余剰領域上の消去済みページに書き込みを行い元のアドレスを付与し、**元のページはデータが残ったまま放置したり、余剰領域に割り当てることで動作の高速化**を図っています。

この理由により、**SSDのデータ消去はHDDと同様の1回の上書きでは十分なデータの消去を行うことは出来ず、クリア相当の消去を要求する場合でも、複数回の上書きが必要となります。**また、Enhanced SecureEraseでも、基本的には「LBAの付与されている範囲」と「（LBAの付与された履歴のある）再割り当て済みセクタ」が対象とされているため、**SP800-88Rev.1ではクリア**としている。

注：SSDのメーカによっては、SecureEraseコマンドでPurgeを満足するように設定しているものも存在する。

物理破壊はDestroyなのか？

Destroy（破壊）とは

HDDには、そのHDD自体が使用するファームウェア等を収納しているシステムエリア（SA）と、更に製造元のみがアクセス可能な、余剰な領域が存在する。それらに対する（上書き）消去は不可能であり、この部分を含めすべての領域に対する抹消は、技術論的に読み出しが不可能にすること。

物理破壊＝裁断・粉砕・溶解（NIST SP800-88Rev.1）

１）上書き消去が1回で良いとされている理由は、上書きされた部分から以前に書き込まれたデータのはみ出す可能性を持つ幅が、現在の技術では読み出し不可能な程狭いことが理由であり、そのためにNIST SP800-88に於いても「2001年以降に生産された15GB以上のHDDでは上書き回数は1回で十分である」としている。つまり、上書きの行われていない場合は、プラッタが物理的な損傷を受け、破砕されても、その破片から現在存在する技術で読み出すことの出来ることを否定していない。これにより、**完全なデータの抹消を求めるのであれば、物理破壊・破砕においても事前処理として、外部磁界による消去や、上書き消去を行なう**ことが必要。

参考：１TB/プラッタ上のデータトラック　書き込み幅：５５nm　トラック間隔：７０nm

要求トラッキング精度：８nm

２）製品（HDD）によっては、**3.5インチの筐体に2.5インチのプラッタ（円盤）を組み込んでいるものも存在**する、またそうでないものに於いても穴の場所（破壊の方法）によってはプラッタ（記録円盤）に損傷を与えることが出来ない可能性や、**複数枚の最下層まで破壊出来ない可能性**が存在し、**外観だけで確実な処理が実行されたという判定が困難**である。

外部磁気消去の問題点

１）十分な外部磁界が印加されたのか否かの判定が出来ない。

① 外部磁界の印加によって機器自体が動作不能になってしまうことが多く、また、動作する場合に於いても、プラッタ上のデータが、現存するあらゆる技術を用いても全く**読み出し不能な状態に消去されたのか否かを容易に確認することには困難**が伴う。

② 外部に磁気シール等を貼付し磁気印加の証明としている場合も存在するようだが、筐体や内部に存在する部品に、機器の内部を通過する磁束に影響を与えるような磁気回路を構成するような磁性体が用いられていないことを確認する事を行わずに、プラッタに印可された磁界の大きさを確認することは出来ない。また、磁気シールは磁束の定量的な判定に対する信頼性を持たない。

２）印加磁界に変動要因が存在する

① 磁界を発生させるための電磁石の**コイルの銅線の抵抗は、1℃当たり約0.4%の割合で上昇**するため、仮に**20℃から60℃まで上昇した場合には約16%磁界が減少**するので、機器（コイル内部）の温度管理等も必要である。

② コンデンサに対する充電時間の確保機能
パルス印加等の方式を採用している場合が多く、高電圧を必要とするため内部の昇圧回路を利用してコンデンサに充電をしているので、充電時間（放電エネルギー）管理が必要である。

③ **コンデンサは、構造上急速な充放電による劣化が激しい**ので、定期的な性能の確認検査が行われていなければ性能の保証は出来ない。

上記により、**印可磁界の数値管理が必須**であり、また**十分にマージンを有する設計性能が要求され、信頼できる組織によって最新のHDDのデータ抹消に対する有効性を認められている機器が稀**であり、機器の信頼性に欠ける。

NSA/CSS　2019　Dec.では？

Evaluated Products List for Hard Disk Destruction Devices より抜粋

ハードディスクドライブ破壊装置を単独で使用した場合、磁気ストレージ機器に対するデータ抹消には相当しません。

・本書に記載される**ハードディスクドライブの破壊装置は、磁気消磁装置と組み合わせて使用した場合にのみ磁気ハードディスクドライブのデータ抹消として認められます。**単体での使用は、NSA / CSS 9- 2ストレージデバイスのデータ抹消マニュアルに記載された緊急事態においてのみ認められます。

・粉砕は、NSA / CSSの9-12ストレージデバイスのデータ抹消マニュアルの指示に従い、プラッタが2ミリメートル角以下のサイズを達成することが無ければ、データ抹消には相当しません。

Evaluated Products List for Magnetic Degaussers より抜粋

・すべてのハードディスクドライブ内のプラッタを変形させることによる物理的な破壊を伴う消磁を行うことを強く推奨します。ハードディスクドライブ破壊装置については、NSA / CSS評価製品リストを参照してください。

・このリストへの記載は、機器の継続的な性能を保証するものではありません。製造元に従って、またはNSA / CSS承認済みの磁場検証装置を使用して、機器を再テストする必要があります。

注（私的見解）：現時点において、日本で行われている物理破壊や外部磁界による消磁を行ったHDDからのデータ復旧を行っている業者の存在は認識していない。

ISMS（ISO27001）で情報流出は防げるか？

業者の選定基準としてISMS（ISO27001）認証の取得を条件としているケースが見受けられるが（話題になったB社も認定事業者）、そもそもISMSはマネージメントの基準であり、管理（マネージ）がどのように行われているかを審査・認定するものであるため、**個別に存在するリスクの対策手法の規格ではない**ことを認識する必要がある。このように理解すれば、**ISMS認証取得を条件とすることの無意味**さが理解できるはず。

その上で、守るべき個別の最低条件を見極め、その対策を実現する具体的な手段を具体的に規定・ルール化することが必要であり、そのためには発注者にそれだけの知識が必要になることを避けることは出来ない。

ADECはデータ消去作業現場毎に審査を行なう、独自の消去プロセス認証制度を採用しています。（現在は、認証ソフト＋認証作業現場による消去証明書発行を業務としているが、神奈川県の事故後、作業所単独の認証要求が増加しているため対応を検討中）