データ抹消に関する米国文書（規格）及び HDD、SSD の技術解説

2016 年 4 月 11 日
株式会社 DD-RESCUE
沼田　理

米国における、情報セキュリティーを目的とした磁気記録媒体のデータ抹消に関する技術解説・報告書として、UCSD (カリフォルニア大サンジエゴ校) CMRR (Center for Magnetic Recording Research: 磁気記録研究センター) 2007 年発表の Tutorial on Disk Drive Data Sanitization や、米国の公的機関である NISP（National Industrial Security Program）や NIST（米国国立標準技術研究所）の発行文書が知られているが、NISP や NIST では文書の改訂が継続的に行われている。その改訂の行われる元となった理由や技術的背景を理解せずに議論を行うことは、砂上に楼閣を築くに等しいので、ハードディスクドライブ（HDD）の磁気記録および上書き抹消、また抹消後の復旧手法とされる技法について概要を解説する。また、最近普及の進んだ NAND 型フラシュメモリーを使用した SSD で用いられている技術についての解説も含め、証拠保全用媒体に対するデータ抹消の課題を明確にする。

１．データ抹消に関する米国文書

１．１．一般的に流通している HDD のデータ抹消・復旧に関わる噂の否定

（１）．HDD に用いられている技術以外のデータ抽出手段

「プラッタ（磁気ディスク）上から直接磁気イメージを読み出し、ユーザデータを抽出する方法が存在する」、また「上書きを免れたトラック（セクタ）のエッジ部分から情報を読み出す方法もある」とも言われているが、上記 UCSD の文書 Tutorial on Disk Drive Data Sanitization（2007 年）の Computer Forensics Data Recovery 章で否定されている。

（２）．完全抹消のためには複数回の上書きが必要

Peter Gutmann の提唱した必要回数 35 回説や、DoD 規格（1995 年）による 3 回などの上書き回数による抹消の効果についても、Tutorial on Disk Drive Data Sanitization 中の Nondestructive Data Erasure 章で、「上書き回数に関わる抹消能力評価を行った結果、1 回でも複数回でも抹消能力に差がないことが判明したため、U.S. National Security Agency (米国家安全保障局)が 1 回の上書きに Information Assurance Approval (情報保証承認)を発行した」と説明され、複数回の上書きの必要性も否定されている。

１．２．米国の公的文書・規格・報告書の上書きに関する記述概要

（１）．NISP　DoD（米国国防総省）：

現時点に於いて、多くのデータ抹消ソフトウェアの紹介文で「データの完全抹消を行うための方法」の根拠とされているものが、NISP（National Industrial Security Program）が 1995 年 2 月に発行したオペレーティングマニュアル DoD（Department of Defense：国防総省）5220.22-M に於いて、「全てのマッピング可能なセクタに何らかの文字で上書きを行った後、その補数の文字で上書きを行い、さらにランダムな文字コードで上書き処理を行う」と具体的な手法を明記したことによって、世界的に DoD 規格の完全抹消の方法の地位を得たが、2006 年 2 月に改訂された同文書では、最高機密の保護を目的とした方法としては「上書き抹消」は取り消され、「外部磁界による減磁（消去)」、または「物理的な破壊」のみが最高機密に対する漏洩防止手段とされた。

（２）. NIST（米国国立標準技術研究所）: 2006 年 9 月に発表した Special Publication 800-88 で、「2001 年以降に生産された、15GBytes 以上の ATAHDD では、データの完全抹消は、研究の結果 1 回上書きするだけで効果的に抹消することが可能であり、ATA コマンド（原文では[ファームウェア]）として実装された Secure Erase の実行で良い」（ATA コマンドの実行では、DCO や HPA などの隠し領域や、不良セクタとして代替処理を受けた部分も含めて、論理アドレスが付与された領域全てに上書きが実行される）としていたが、2014 年 12 月の

改定では、「1 回の上書き」で「研究所レベルの高度な読み出し方法を試行しても、データの読み出しは不可能である」ことは認めた上で、「SSD などのフラッシュメモリーを使用した記憶媒体を例に、予備やウェアレベリングを目的とした領域や、製造上存在する余剰な領域などのような、製造者のみが管理する領域の存在を危惧し、コマンドが期待通りに（物理的に書き込み可能な全ての範囲に対して有効な状態に）実装されている否かについては製造者の信頼と保証に頼らざるを得ないことを理由に、「Secure Erase を含むすべての上書き」を媒体の完全な抹消のための手段から除外し、最高機密に対する抹消の手段を「外部磁界による減磁」と、「物理的な破壊」に限定した。また、Seagate の暗号化機能を搭載した HDD（Self-Encrypting Drives：SEDs）の発売（2008 年）に対応し、暗号化による抹消（Cryptographic Erase：CE）についても言及している。

（3）．UCSD（カリフォルニア大サンジエゴ校）CMRR（Center for Magnetic Recording Research: 磁気記録研究センター）：2007 年発表の Tutorial on Disk Drive Data Sanitization では、既に紹介した内容のほかに、2006 年 NIST SP800-88 によって認定された Secure Erase の誕生の背景として、UCSD の CMMR が、「DoD 5220.22-M によって規定された上書き方法（OS 上で動作するプログラムを利用した、3 回の上書きによる抹消）では、論理アドレス（LBA）の付与された範囲しか対処の範囲とされないが、論理アドレスは、実際に使用可能な最大記録容量よりも低く設定される場合があり、また代替処理されたブロックや、DCO や HPA などの隠し領域も対処の範囲外となってしまうことを理由とした」ことの紹介や、水平（面内）磁気記録方式と垂直磁気記録に用いられる磁気材料の違いによって要求される外部磁界による減磁(消去)に要求される磁界の大きさに差異が存在すること、熱アシスト磁気記録やフラッシュメモリーを併用したハイブリッド HDD の登場などの科学技術の進歩により、データの完全抹消の難易度がますます高度になって行くことに対する懸念も記述している。

但し、この文書に於ける Secure Erase の機能の紹介は、CMRR のサイトからダウンロード可能な Secure Erase の実行プログラムと一致せず、暗号化を利用した抹消方法と説明されている Enhanced Secure Erase は、大阪データ復旧の下垣内氏による実験などで、「隠し領域や代替処理されたセクタなどの OS からは認識アクセス不能な領域を含む抹消機能となっている」ことが判明しており、暗号化を利用したデータ抹消方法は、前述の NIST 文書に於ける Cryptographic Erase（CE）を指すものと思われる。

また、2011 年発表の Reliably Erasing Data From Flash-Based Solid State Drives では、①内装されたコマンド（(Enhanced) Secure Erase と推定される）による抹消を行っても、コマンドが期待通りに（物理的に書き込み可能な全ての範囲に対して有効な状態に）実装されていないものが存在すること。②全 LBA に対する上書き抹消を 2 回繰り返すことによって、通常はデータの抹消が可能であるが、全ての場合ではないこと。③HDD を基準に作られた、個別ファイルの完全抹消技術は SSD には効果が無いことを報告している。

１．３．米国文書の示している内容

HDD は、記録密度の向上とコストダウンを目的とした技術の進歩により、過去（特に 2000 年以前）と比較すると変化が大きく、完全なデータ抹消の方法に関しても、過去の報告書や評価結果をそのまま適用するのではなく、製品の進歩に追従すべく改訂が実施され、最新の NIST 文書 SP800-88r1（2014 年 12 月改訂）では、実際にパソコンなどのシステムに組み込まれて使用されている HDD には、①パソコンなどの製造業者が、そのパソコンなどのシステムを必要に応じて初期化する（製品購入時の状況に戻す）作業を行うことを目的としたデータを保存しておくために設定した隠し領域や、使用中に不良として検出され、代替処理を行ったブロック（セクタ）など、OS からは認識・アクセス不能な領域や、②製造上発生した、論理アドレスの付与されていない余剰領域や、製造工程上で判明した欠陥を補うために用いられる代替領域、製造当事者だけしか知り得ない（ファームウェアなどの）動作上で使用される領域など、現存する上書きによる抹消を目的としたソフトウェアやコマンドでは処理の及ばない領域の存在を危惧し、上書き抹消を最高機密の漏洩を防ぐための完全なデー

タ抹消手段とすることは取り消されているが、この決定は技術論としての「HDD における上書きによる抹消」を否定しているのではなく、SSD に存在が認められる公称容量を超えて存在する、内部動作専用に割り振られた領域のように、HDD においても製造当事者しか知り得ない、「外部からのアクセスでは上書き抹消を行う事が難しく、データの存在を否定することが不可能な領域が存在している可能性」を危惧しているように、製品に採用されている技術情報の収集に努め改訂していることに注目する必要がある。

２．HDD の磁気記録

２．１．飽和磁気記録と未飽和磁気記録

既に過去の遺物とも称される、カセットテープやビデオテープレコーダに使われる磁気テープでは、記録される情報がアナログ信号であるため、信号の強さに比例した磁力をテープに記録する。この方法では、テープに使用されている磁性体の飽和磁束密度に到達しない範囲で記録を行うために「未飽和磁気記録方式」と呼ばれる。

未飽和磁気記録では、完全に磁気の存在しない状態の上に新規の信号を書き込むのでなければ、従来から存在する磁気の影響を受けるので、事前に消去ヘッドを用いた準備作業（消去：磁気の存在しない状態を作り出すこと）が必要となる。

一方、FDD や HDD の円盤（ディスク、プラッタ）では、デジタルデータの記録であるため、書き込み磁束の強さに段階的な変化は必要なく、使用されている磁性体が N 極または S 局の飽和磁束密度に達するように書き込む「飽和磁気記録方式」が用いられる。

飽和磁気記録では、使用されている磁性体がこれ以上の磁束密度を持つことの出来ない限界に達する磁束密度を与えることによって書き込みを行うため、既に磁化されている（データが存在する）上に書き込みを行っても、そのデータの影響は受けることはないため、事前にデータの消去を行う必要は無く、上書き行為が消去を兼ねる上書き記録が成立する。

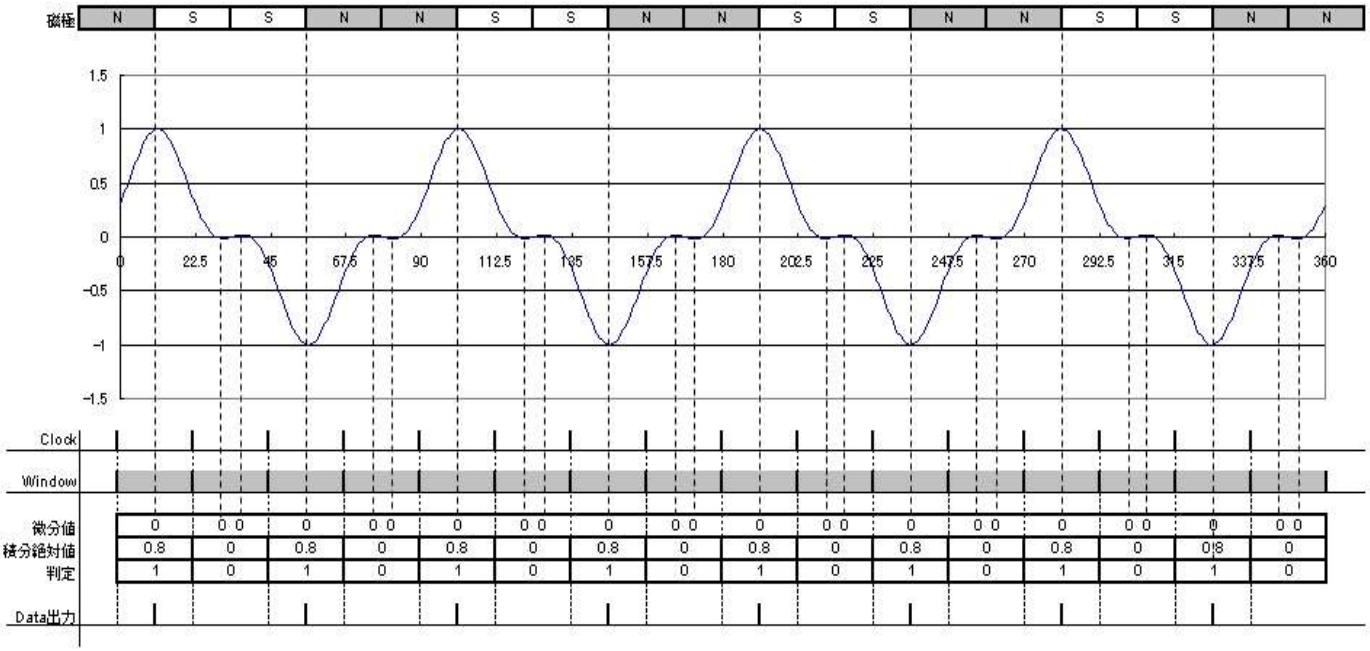
２．２．磁気ヘッドの特性

円盤やテープの磁性体のデータの読み書きを行う部品を磁気ヘッドと呼び、磁性体に書き込まれた磁束を鉄心で拾い、鉄心に巻かれたコイルによって、磁束の変動を誘起電圧として取り出す仕組みであるため、ヘッドの読み取り特性は微分特性となる。ヘッドの微分特性とは、ヘッドを通過する磁束（磁石の力）をΦとすると、その磁束の変化に比例した電気信号を得ることの出来る特性を指し、ヘッドの出力信号をｖ、時間をｔとすると、

ｖ＝⊿Φ／⊿ｔ　（ヘッドの出力＝磁束の変化量）となる。

故に、N 極から S 極に、S 極から N 極へと極性が切り替わる時点の出力電圧が一番大きく、N 極や S 極が連続した場合は、出力電圧は最小値（0V）となる。

２．３．磁気―デジタル信号変換の原理



前頁の図は、X 軸が時間軸であり、22.5 毎に存在する Clock で区切られ、この区間をデータウィンドウと呼ぶ。この中で波形のピーク検出（微分器による、傾き“０”の検出）を行い、更に積分器を用いた平均電圧の絶対値と併せて、双方の論理判定（AND）を行っている。

例：判定条件：微分値≒0 と積分値>|0.5|⇒“１”
　　微分値≒0 と積分値<|0.5|⇒“０”

として、時間を追って順番に説明すると、

ⅰ．データウィンドウ：0～22.5 では、
　⑴微分器によるピーク（接線の傾き”0”）有り、微分値≒0、
　⑵積分器による平均電圧：0.8 >|0.5|　⇒“１”

ⅱ．データウィンドウ：22.5～45 では、
　⑴微分器によるピーク（接線の傾き”0”）有り、微分値≒0、
　⑵積分器による平均電圧：0<|0.5|　⇒“０”

ⅲ．データウィンドウ：45～67.5 では、
　⑴微分器によるピーク（接線の傾き”0”）有り、微分値≒0、
　⑵積分器による平均電圧：0.8>|0.5|　⇒“１”

ⅳ．データウィンドウ：67.5～90 では、
　⑴微分器によるピーク（接線の傾き”0”）有り、微分値≒0、
　⑵積分器による平均電圧：0<|0.5|　⇒“０”

となり、“１”、“０”、“１”、“０”のデジタル信号が得られる。

２．４．上書きの実態

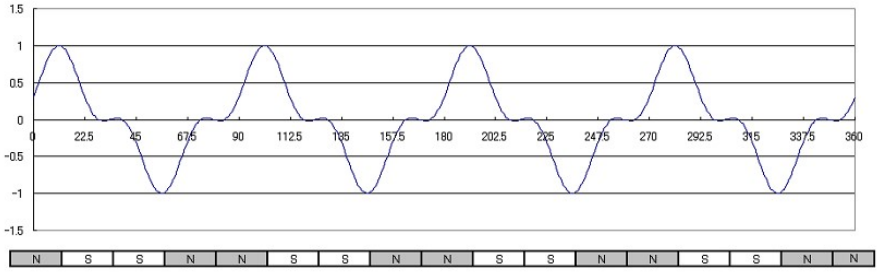
飽和磁気記録方式では、原理では一度上書されると、古いデータがはみ出して残っている部分が存在しない限り、古いデータの影響（残留磁束）は存在しないが、実際の HDD では磁性体に対する着磁（通電）時間に制限が存在することにより、**従来書き込んであった磁束の 1/20～1/30 程度の磁束が、上書きした磁束に影響を及ぼす。**この現象が Acronis True Image 2015 のマニュアル「8.5.3 ハードディスクの消去方法　漏洩のメカニズム」に記載されている下記内容の根拠となっていると推定できる。

一般的に、ハード ディスクに 1 と書き込まれた場合、ディスク装置によって 1 と読み出され、0 と書き込まれた場合は、0 と読み出されます。 しかし、0 の上に 1 と書き込まれた場合、読み出された値はたとえば 0.95 になり、その逆も同様で、1 の上に 1 と書き込まれた場合、結果は 1.05 となります。このような違いは、コントローラにとっては無関係です。しかし、特殊な機器を使用すれば、「下に隠れている」0 と 1 のシーケンスを簡単に読み取ることができます。

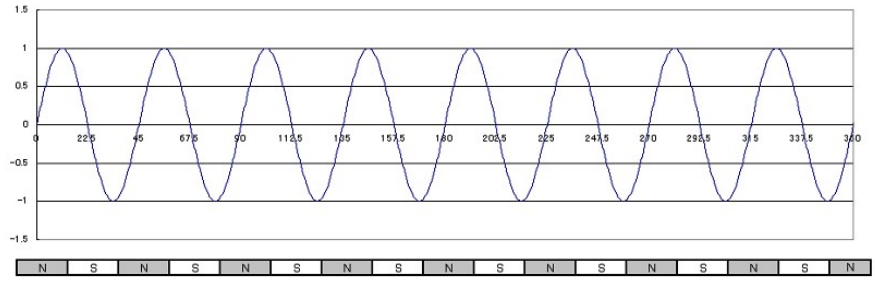
引用元：Acronis True Image 2015 マニュアル（ATI2015_userguide_ja-JP.pdf）pp.166
　　Acronis International GmbH
　　http://dl2.acronis.com/u/pdf/ATI2015_userguide_ja-JP.pdf

・残留磁気の影響によるアナログ波形：

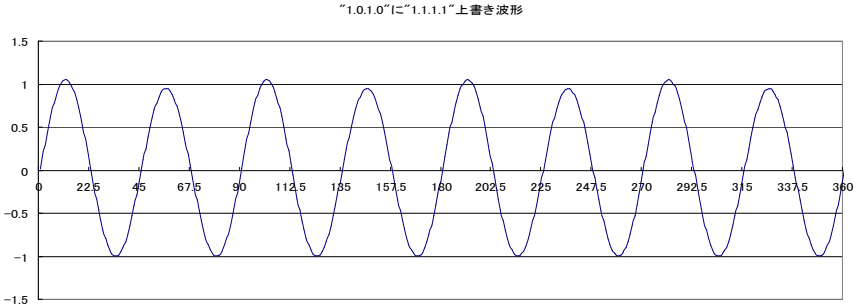
① 元の“1，0，1，0”波形



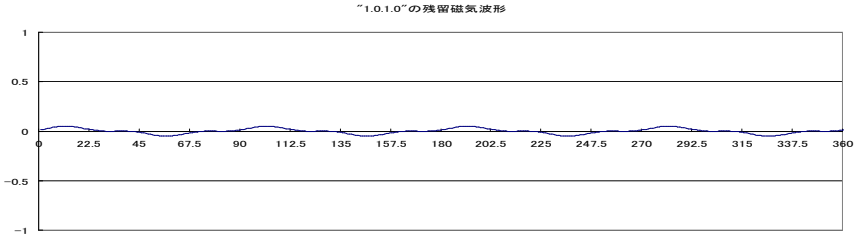
② 上書を行う“1，1，1，1”波形



③ “1，0，1，0，”に“1，1，1，1”が上書された波形



④ “1，0，1，0”の残留分を取り出した波形



このように、**上書したデータを「専用のフィルター」を用いて取り除くことが可能であれば、元データの 1/20 程度に減衰したデータを得ることが可能になる**。しかし現実の場面では、この波形の大きさが、ヘッドや配線の引き回しで拾う外来ノイズよりも十分に大きく、明確に分離可能であることが絶対的な条件であり、影響の残り方もヘッドと磁気ディスクの組み合わせ毎の特性によって、波形歪の発生などの影響があり、製造メーカ、機種、製造ロットや固体による違いも存在し、実際にデータとして復元することは非常に困難であり、専用の特殊な機器や装置も実在せず、実際に作業を行っているデータ復旧業者も実在しないが、「残留磁束を利用したデータ復旧は可能」という噂の根拠とされ、また磁性体の特性から、上書き回数を重ねる度に約 1/20 毎ずつ減少し、2 度の上書きで 1/400、3 度で 1/8000 までの減衰が見込まれることから、複数回の上書きを求める根拠となっている。

（以上の説明は、薄膜コイルを含む巻き線型の線形特性を持つヘッドを前提とする。）

２．５．現在の HDD に使用されているヘッドの特性

1993 年頃から HDD のヘッドは大容量化を目的として開発・採用された、コイルによる電磁気方式は書込み機能だけに限定し、読み出し機能は高感度な MR（磁気－抵抗変化）半導体を採用したヘッドが開発され、現在は更に進んだ“TMR：Tunnel Magneto Resistance effect（トンネル磁気抵抗効果)”や“GMR：Giant Magneto Resistance effect（巨大磁気抵抗効果)”素子となり、その特性は、磁界の変化（強さ）とヘッド出力が比例関係にあるような線形ではなく、図-1 のように特定の閾値をもって切り替わるデジタルスイッチ的な特性であるために、上書データの磁束の中に含まれる残留磁束のような小さな磁束の変化を定量的に検出することは不可能となり、巻き線型ヘッドではサインカーブとなる（１，１，１，１）データであっても、TMR ヘッドの出力波形では図-2 に示されるようになるため、残留磁束の痕跡を波形から見出すことはほぼ不可能となった。このために、**現在では、一度でも上書きされた過去のデータを残留磁気からヘッドを用いて読み出すことを実現するためには、専用の特殊なヘッドを新たに開発することが必要となる。**

図-1　TMR 素子特性参考図：
引用元：産総研
https://www.aist.go.jp/aist_j/press_release/pr2004/pr20040907/pr20040907.html

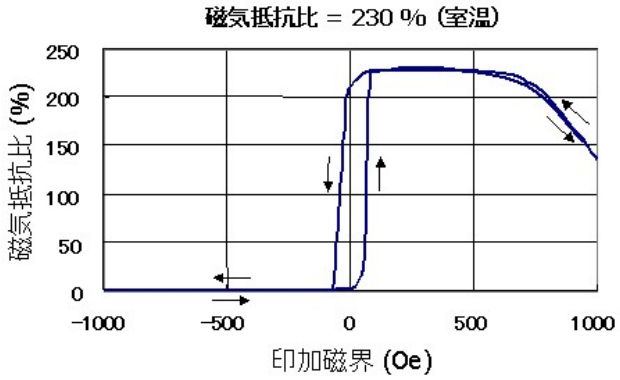
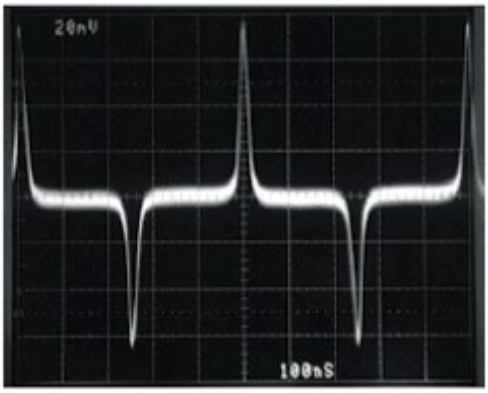


図-2　ヘッド出力波形参考図：
引用元：技術研究組合　長先端電子技術開発機構
http://aset.la.coocan.jp/kenkyu/kenkyu_seika_comp_2.html



２．６．HDD のヘッドとプラッタ、データトラック

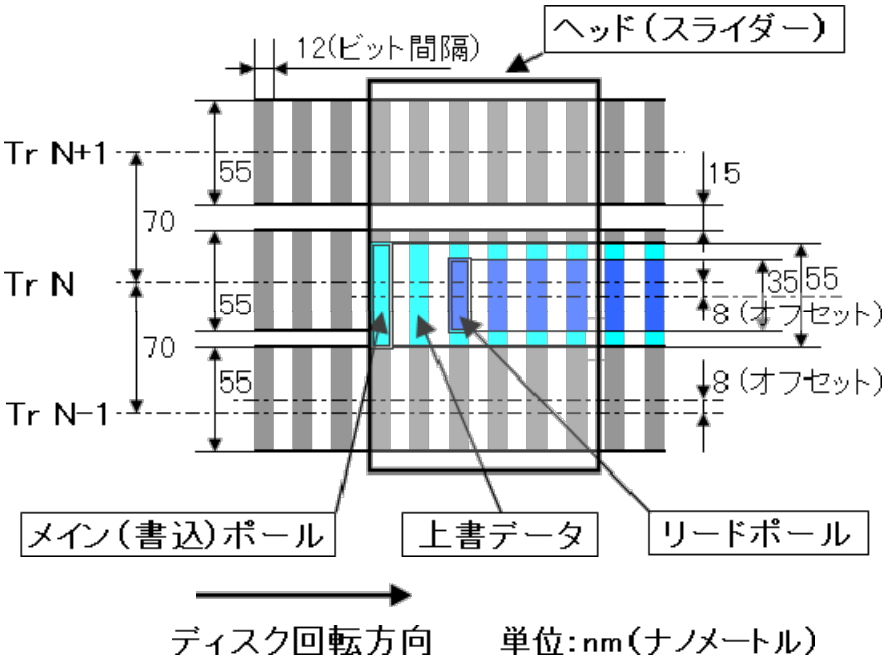
HDD は、内部がどの様に作られていても、「書き込まれた情報が全く変化する事無く、必要なときに読み出すことができること」が、求められている最大の要求事項であり、それ以上の詳細については、全くの「ブラックボックス」であったとしても、接続インターフェイスから見た互換性が保たれていれば使用上の障害は存在せず、その理由によりヘッドやプラッタ、データトラックなどには、公式に規格として決められた数値は存在せず、製造メーカも公開はしていないが、プラッタ 1 枚当たりの記録容量 1 TB の HDD に用いられる垂直磁化方式用のヘッドについて、国内に存在する HDD のヘッドの製造業者から直接入手した数値は次に示す通りである。

・ライトポール幅：　　55 nm
・リードポール幅：　　35 nm

これと、東芝レビューVol.66 No.8 (2011)や、Vol.66 No.11 (2011)などで一部公開されている数値と併せると、

・トラック間隔：　　70 nm
・隣接トラック間隔：　15 nm
・トラッキング要求精度：　7～8 nm
・データビット間隔：　12 nm

となり、データトラックとヘッドの関係は下図のように表すことができる。



図の説明：
ヘッドの位置制御の最悪状態で上書きされた状態を示すために、
①　Tr N-1 位置：Tr N 方向に 8nm（トラッキング精度の最大値）オフセットして図示。
②　Tr N の上書データ位置：Tr N-1 方向に 8nm（トラッキング精度の最大値）オフセットして図示。

この結果、最悪状態として、
③　上記①により、Tr N の Tr N+1 側に**幅 8nm の過去のデータの「はみ出し部分」が発生。**
④　上記②により、Tr N の上書データと Tr N-1 のデータの間の隙間はゼロ。
となる。

２．６．１．「はみ出し部分」（幅）8nm に対する考察：
　トラッキング要求精度 8nm とは、HDD の性格上、トラック位置や間隔の物理的数値はあくまで目安であり、要求される絶対的な物理位置を示す規格ではなく、同一トラックにヘッドをシークした場合のサーボ（位置制御機能）の、「繰り返し再現性の精度」であり、データ書き込み時の位置と読み取り時の差であるとともに、前回データを書き込んだ位置と上書き時の位置との差も意味し、確率計算で用いられる正規分布の 3σ 値（99.7%確率）であるとすると、「はみ出し部分」の大きさと発生率の関係は、

1σ ≒（2.7nm）を超える確率：31.7%
2σ ≒（5.4nm）を超える確率： 4.5%
3σ ≒（8.0nm）を超える確率： 0.3%

と想定される。

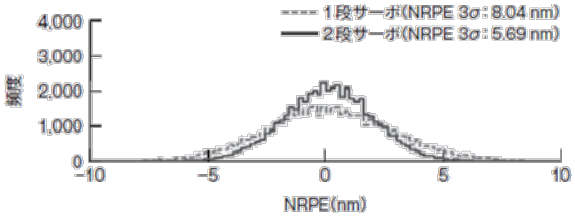


図11. ヘッドの位置決め精度（NRPEヒストグラム）—NRPEの分布（3σ値）を約30％低減できた。
Head positioning accuracies of single-stage and dual-stage servos (non-repeatable positioning error [NRPE] histogram)

右図　1段サーボ位置決め精度 参照
（NPPE 3σ ：8.04 nm）
引用元：佐々木康貴，原武生，
位置決め精度の改善と広帯域化を実現する HDD 用 2 段アクチュエータ，
東芝レビュー Vol.66, No.11, pp.60-63 (2011)

２．６．２．「はみ出し部分」のデータの読み出し

現在の HDD のヘッドは、既に説明したように、GMR や TMR 素子による非線形特性であり、書き込み幅と読み取り幅に約 20nm（片側 10nm）の差をマージンとして用意しているので、故意にヘッドのトラッキング位置制御時の基準位置を変更するなどの手法を用いても、ヘッドを利用して「はみ出し部分」のデータ（アナログ波形）を、線形特性を持った巻き線型ヘッドを用いた抽出のような作業を行うことは不可能と言える。また、特定のセクタで、要求精度を超える大きな書き込み位置ズレが発生し、リードリトライの動作頻度が高い場合は、そのセクタは異常であると自動的に判定され、そのセクタから読み出したデータを書き直す「リフレッシュ機能」も内蔵しているため、「要求精度を超えるような大きなはみ出し部分」も、HDD の使用中に漸減する可能性が大きい。

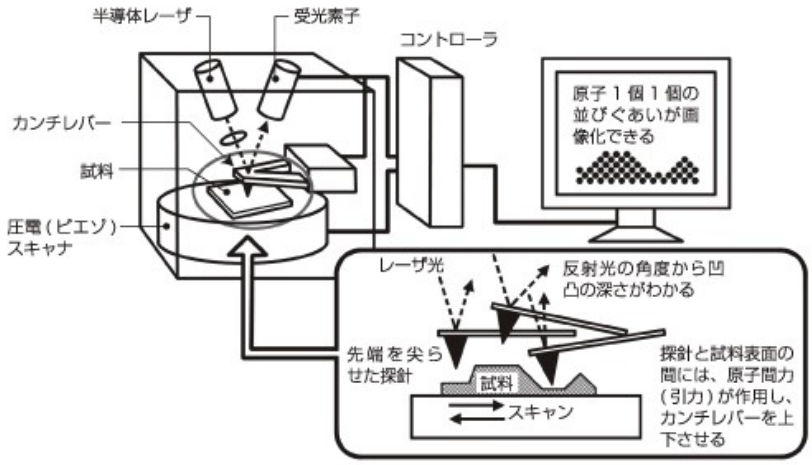
２．７．HDD に用いられている技術以外のデータ抽出手段

Peter Gutmann のレポートなどに記載されている、データ抽出手段として、「磁気力顕微鏡」が存在するので、その最新の機材の特性から実現性を検討する。

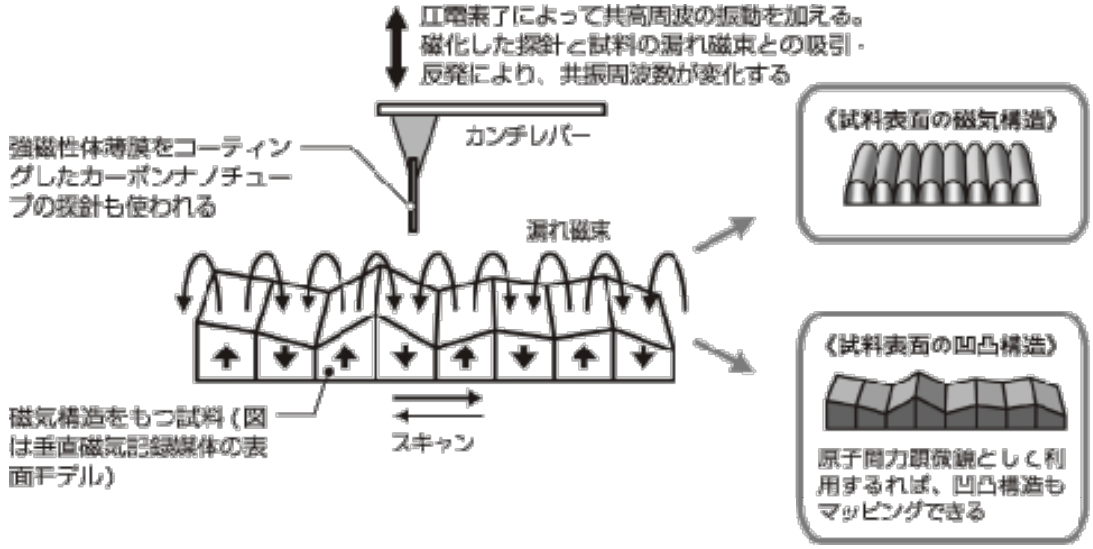
２．７．１．磁気力顕微鏡とは

磁気力顕微鏡とは、片持ち梁（カンチレバー）の先端にカーボンナノチューブの表面を磁性体の皮膜を施した極細の探針に働く、被観察物の磁力の変動を凸凹図形として「見える化」する機能を持つ装置である。

模式図や原理を、参考図-1,2 に示す。



参考図-1：プローブ型顕微鏡（原子間力顕微鏡）の基本原理
引用元：http://www.tdk.co.jp/techmag/ninja/daa00992.htm
TDK 株式会社　じしゃく忍法帳　第 107 回「ナノテクを結集した磁気力顕微鏡」の巻

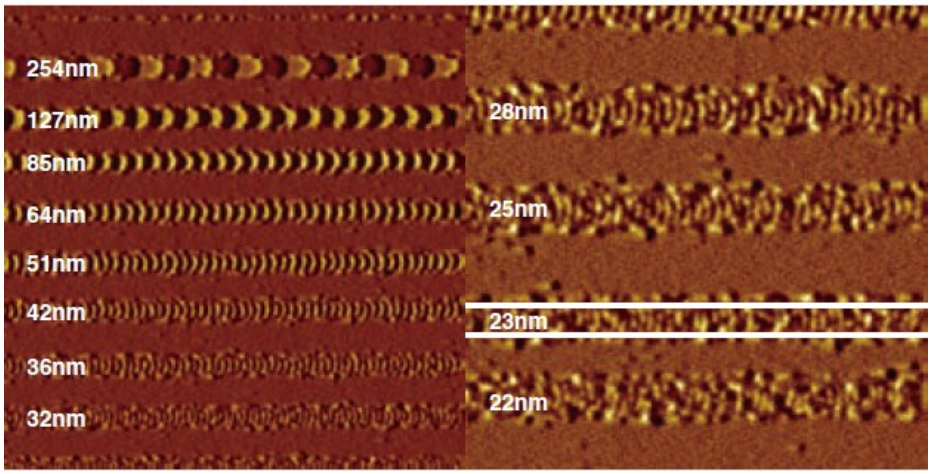


参考図-2：磁気力顕微鏡（MFM）の基本原理
引用元：http://www.tdk.co.jp/techmag/ninja/daa00993.htm
TDK 株式会社　じしゃく忍法帳　第 107 回「ナノテクを結集した磁気力顕微鏡」の巻

２．７．２．磁気力顕微鏡の測定限界

磁気力顕微鏡の解像度（測定限界：分解能）は、使用される探針の太さ（先端形状）で決定される原理上、探針の芯になるカーボンナノチューブの直径が 1nm 以下であっても、その上に蒸着によって形成する磁性体皮膜の厚さも加算されるために、10nm 程度が物理的な限界となり、形状の判定には 1 方向の測定点として 10 か所程度が必要とされるため、測定限界は、ビット間隔 12nm である 1 枚あたり容量 1TB のプラッタではなく、ビット間隔やトラック間隔が約 10 倍となる 1 枚当たり容量 10GB 程度のプラッタであり、ビット間隔よりも小さな、「はみ出し部分」や、残留磁束として存在する過去のデータの影響による僅かな磁気の僅かな変動を正確に検出することは不可能と結論付けざるを得ない。また、このような微小な測定は、温度変化の無い恒温室の中で、被測定物を高真空中に保つなどの手段を用いて空気の対流の影響も予防する必要もあり、ヘッドを使わずにプラッタ全体のデータを読み出すことの出来る施設・装置を実現することには大変な課題があることが理解できる。

参考画像：磁気力顕微鏡による HDD のプラッタ上のトラック画像



画像内の数字は、ビット長（縦筋の間隔）
引用元：http://www.toyo.co.jp/microscopy/products/detail/id=8300#undefined
磁気力顕微鏡(MFM)用プローブ

この磁気力顕微鏡の存在が、https://ja.wikipedia.org/wiki/データの完全消去（2016-02-12 閲覧） に記載されている、「たとえば、ドリルで穴を開けてプラッタを破壊したとしても、プラッタの残骸を最先端の残留磁気探索装置を用いて解析することにより、わずかな部分でも 1 ビットずつ手作業でデータを復活させていくことも出来る、ハードディスク・メーカーのシーゲイト・テクノロジーはそのような手法を保有していると公表している」が根拠としている、2006 年にシーゲイトに買収されたカナダのデータ復旧業者（Action Front Data Recovery Labs Inc.）が 2001、2 年頃 Web 上で発表した、プラッタからヘッドを用いる事無くデータを読み出すことができた」とするレポート（現在は閲覧不能）の源泉であるが、レポートの内容は、上書きによる「はみ出し部分」からではなく、残留磁束として残存する過去のデータでもなく、「現存するデータを、磁気ヘッドを使用する事なく読み出すことが出来た」の内容であったと記憶しているが、既に説明したように、「当時の HDD では可能でも、現在の HDD は測定限界以下であるため、実現不可能である」ことが裏付けられる。

２．８．HDD の上書き抹消に対するまとめ

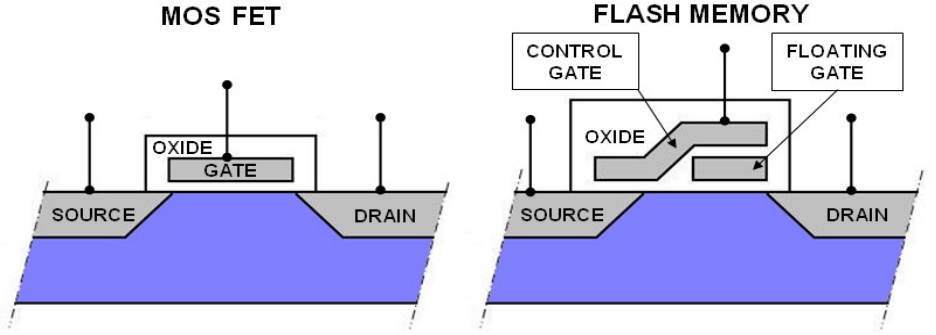
最新の技術の積極的な導入により記録容量を増加させている HDD に於いて、データの抹消を目的として用いられる「上書き抹消」を、10 年以上前に発表された「グートマン方式」による 35 回の上書きや、米国国防総省の定めた 3 回の上書きを、現在の HDD に対しても引き続き絶対的な規格とすることには合理性が存在せず、NIST SP800-88r1(2014 年 12 月) 改定版に記載されている、**「1 回の上書き」で「研究所レベルの高度な読み出し方法を試行しても、データの読み出しは不可能である」ことは、本報告書に於ける現実の数字を用いた解説により完結できた**と考えるが、同時に Enhanced Secure Erase を行ったとしても、「製造者のみが管理する領域の存在によって、HDD 上に書き込まれた全ての情報が抹消されたとは判定することが不可能である」ことも事実であり、その対応も検討事項として残存する。

３．SSD のデータ記録

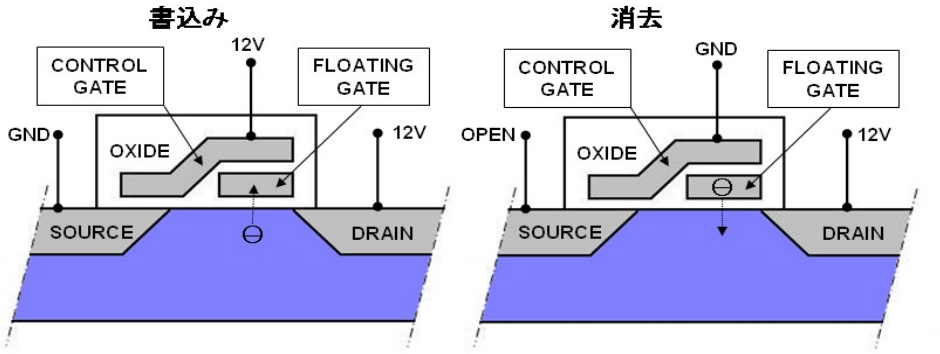
３．１．NAND 型 Flash ROM の動作と内部構造

HDD などのデジタル磁気記録は、飽和磁気記録方式であるため、記録されている磁極や磁力の強さに無関係に、その磁性体が磁気飽和するのに十分な磁界で加えることで新たな磁極が飽和磁束密度に達する“上書”が可能であるが、NAND 型 Flash ROM では、上書きを行おうとすると、既に書き込まれているデータと、書き込もうとするデータの差を演算し、夫々のセルに対する動作を決定し実行する必要が発生するため、動作の簡略化目的として、書き込みが必要であるセル全体に対し、初期化（消去）⇒書き込みを行う。このように、事前に初期状態に戻す“消去”が必要であることが、ROM に分類される理由でもある。

① NAND 型 Flash ROM のセルの構造：内部は下図のように、MOS（Metal-Oxide-Semiconductor）型 FET（Field effect transistor：電界効果トランジスタ）と呼ぶ、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ー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し、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である。



② データ書込み/消去： 下図のように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”を決定している。



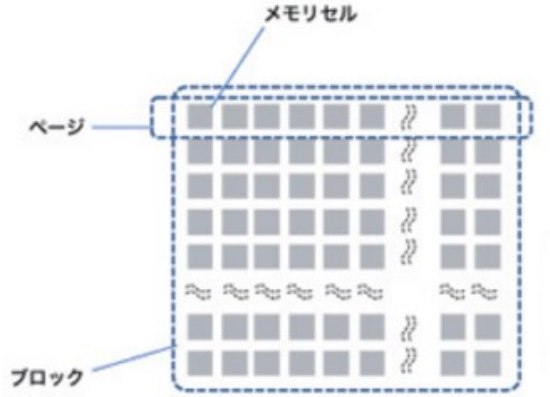
注：図で、電源電圧を 12V と表示しているが、通常の USB メモリーや SD カードなどは 3.3V の電源電圧を、内部の昇圧回路を利用し、“書込み、消去”を行っている。

この動作自体は MOS-FET のスイッチング動作と全く同様で、電源の供給が停止した場合に MOS-FET の場合はゲートの電荷は消滅してしまうが、フラッシュメモリーの場合は電源の供給が停止した後も、フローティングゲートの周囲が絶縁体であるため電荷が保持され、不揮発（電源を切ってもデータが保持される）となる。この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、中間のレベルの段階的な判別を可能にした物が MLC 型である。

③ フラッシュメモリーの問題点： フローティングゲートへの電荷の注入・放出動作によって周囲の絶縁体の劣化も同時に起こすため、繰り返し動作の回数に制限**「書き換え回数制限」**があり、また注入（充電）された電荷は周囲の絶縁体を通して少しずつ放電し、電源 ON や読み出し動作ではフローティングゲートへの電荷の再注入は行われないので、**「データ保持期間」**も 10 年程度が限界（使用開始後に書き込まれた場合は、保持期間も当然短くなる）となってしまう宿命が存在し、SLC 型であれば、ON と OFF の 2 値制御であるフローティングゲートの電荷を、MLC 型では通常 4 段階であるため、自然放電の影響が大きくなり、短寿命となる。

３．１．１．SSD の書き込み動作

HDD の場合コントローラ（ファームウェア）が管理している読み書きなどの動作の最小単位（物理フォーマットが行われた状態）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となっているが、SSD では、下図のようにメモリー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」単位であり、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」毎となる。（東芝 セミコンダクター&ストレージ社 フラッシュメモリーカタログ ）
http://toshiba.semicon-storage.com/info/docget.jsp?did=12524（catalog_ja_20150226.pdf）



参考図-3 フラッシュメモリーのセル、ページ、ブロック
引用元：
https://product.tdk.com/info/ja/techlibrary/archives/techjournal/vol01_ssd/contents06.html
TDK 株式会社 フラッシュストレージ
SHG2A シリーズ NAND 型フラッシュメモリの書き換え回数には上限がある

（1） データの書換え

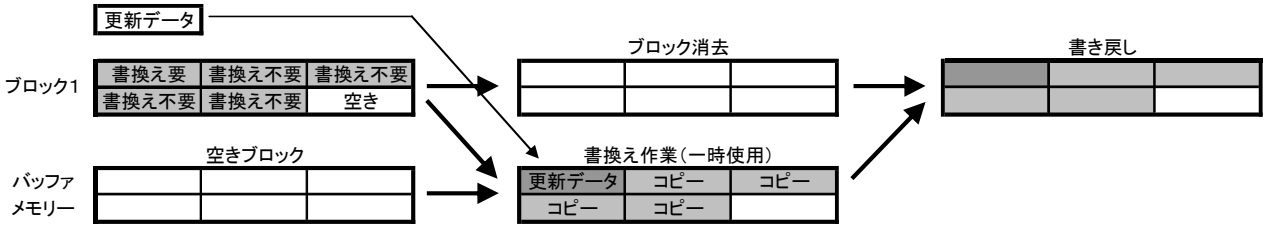
・基本的な動作　（下図参照）

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



この動作では、例えｌバイトの更新であっても「ブロック全体の読み出し⇒消去⇒書き込み」と長時間を要し、また１ブロック分の容量を持つバッファーが必要となる。

・SSD の一般的（高速化）動作　（下図参照）

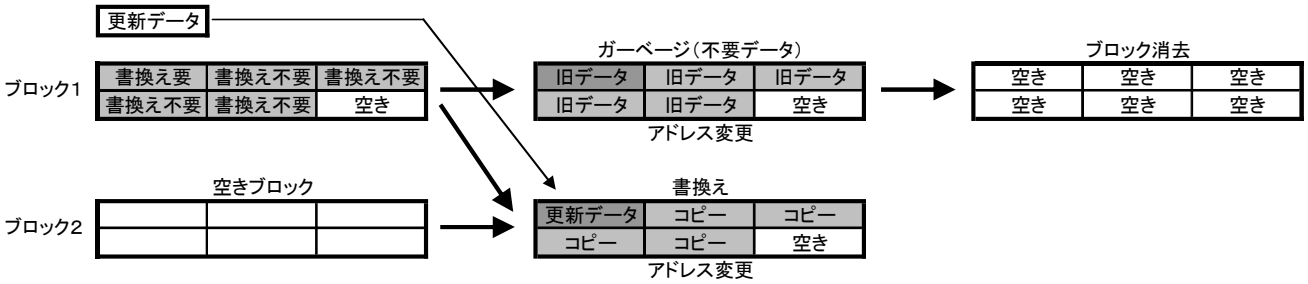
ⅰ．書き込み可能な「空きブロック：ブロック 2」を事前に用意

ⅱ．書き換えるページ以外のデータ（書換え不要データ）を「ブロック 2」にコピー

ⅲ．書き換えるページ（更新データ）を「ブロック 2」に書き込む

ⅳ．書き込んだ「ブロック 2」と、元の「ブロック 1」のアドレスを交換
（アドレステーブル更新）

ⅴ．不要になった「ブロック 1」のデータを消去し、次の書き込みに備える



この動作では、未使用の空きブロックが十分に存在する状態では高速化が図れるが、SSD に書き込まれているデータ容量の増加に伴い動作速度が低下する。

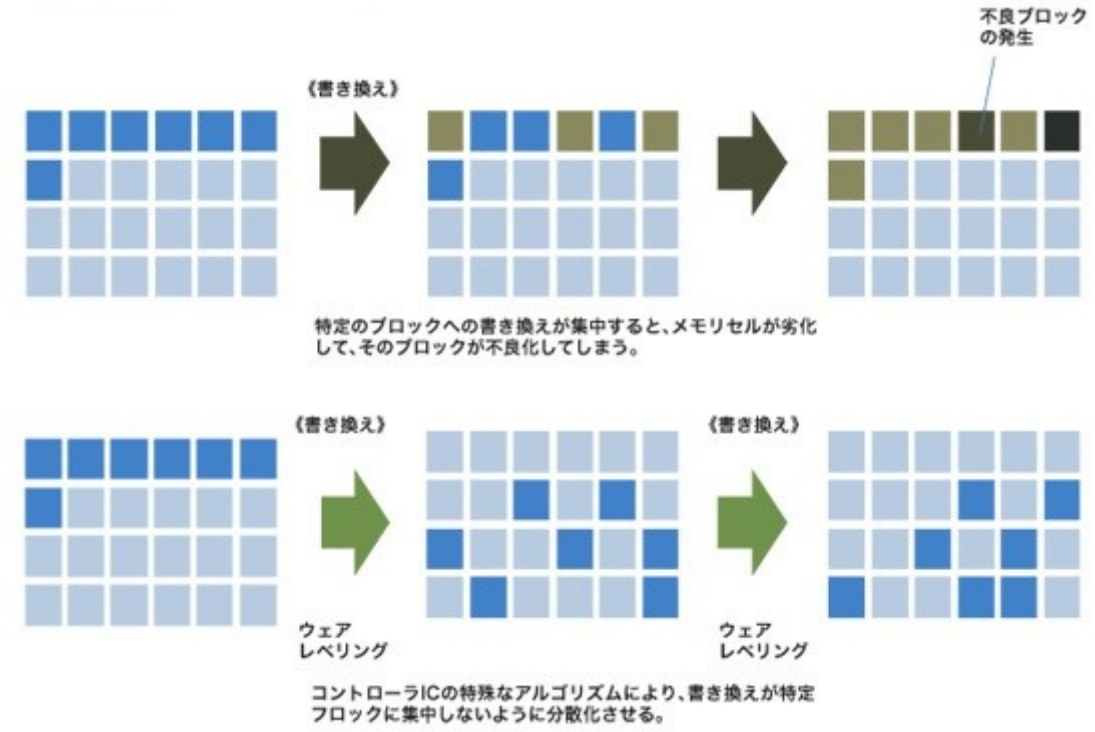
３．１．２．問題解決の手段

フラッシュメモリーの欠点である、「書き換え回数制限」や「データ保持時間」、「使用に伴う速度の低下」を解決するために SSD では、「ウェアレベリング（Wear Leveling）」や「リフレッシュ（Refresh）」、「オーバープロビジョニング（Over Provisioning）」と呼ばれる手段が採られている。

① ウェアレベリング（Wear Leveling）：　ウェアレベリングは、使用されているフラッシュメモリー全体のウェア（Wear：磨耗・消耗）をレベリング（Leveling：平準化・平均化）する手段で、SSD の持つプログラム（ファームウェア）で実行されるため、実際の動作内容は製造メーカに委ねられている。

目的：SSD を通常の HDD のように使用すると、物理的に先頭のページ（ブロック）から使用され、後方に位置するページ（ブロック）に書込みが行われる頃まで、初期から使用されているブロックが「書き換え回数制限」に到達し、SSD が短寿命になることを予防する。

方法：先頭から連続したブロックに書き込まれていたデータを、書き換えが必要となった時点で、使用頻度の少ない別のブロックに移動（コピー）し、そのブロックのアドレスを以前使われていたブロックのアドレスに変更し、再度書換えが必要となった時点では、また別の使用頻度の少ないブロックに移動（コピー）し、ブロックのアドレスを再度の変更を行う。



参考図-4 ウェアレベリング（概念図）
引用元：
https://product.tdk.com/info/ja/techlibrary/archives/techjournal/vol01_ssd/contents06.html
TDK 株式会社　フラッシュストレージ　SHG2A シリーズ
NAND 型フラッシュメモリの書き換え回数には上限がある

参考：ウェアレベリングの詳細なアルゴリズムは、SSD 製造メーカ各社が個別に技術開発を行っており、製造メーカや型番、製造時期などに依存し非公開であるが、特許の出願情報（特開 2011-70346：東芝や、特開 2012-174331：三星電子など）では、個別のセルやページ、ブロックなどの消耗状態を自己診断機能を用いて判定し、単純な書き込み回数基準ではなく、実際の消耗具合と合致した平準化を図る、より効率的な結果を得る方法も示されている。

② ECC リフレッシュ（ECC & Refresh）：　ECC リフレッシュは、ECC（Error Check and Correct：誤り訂正符号）とリフレッシュ（Refresh：再書込み）の組み合わせによって「データ保持時間」の限界に起因するエラーの発生を予防する手段で、SSD の持つプログラム（ファームウェア）で実行されるため、実際の動作内容は製造メーカに委ねられている。

目的：フラッシュメモリーは、通電やデータの読み出し動作ではフローティングゲートに対して電荷の注入は実行されないので、一度書き込まれた後は読み出しのみしか行われない OS のシステムファイルや、アーカイブファイルでは、フローティングゲートの電荷が漏れ出して低下する「データ保持時間」によるリードエラーが発生することを予防する。

方法：リードエラーが発生した場合、リードリトライ（メモリーセルの“0”、“1”の判定を行う閾値を変更し、データの読み出しを再試行する）によるデータの読み出しを試行し、再度読み出したデータによる、「消去（初期化）⇒書き込み」動作を強制的に実行することで、「データ保持時間」のリセットを図る。

参考：リフレッシュは、ウェアレベリングと併せて行われることもあり、元のページやブロックに対して書き込まれるとは限らず、実際の動作は製造メーカのファームウェアのプログラムに依存している。

③ オーバープロビジョニング（Over Provisioning）：　オーバープロビジョニングは、SSD の公称容量の領域（LBA）の他に、10%～30%の記憶容量をオーバー（Over：過剰・余剰）にプロビジョニング（Provisioning：供給・準備）することで、システム動作専用の領域を強制的に確保し、SSD のパフォーマンスの向上に役立てる手段。

目的：「書き換え回数」過剰による不良ブロック発生時の予備や、ウェアレベリング実行対象範囲の拡大、書き換え動作時の作業専用の「隠し領域」などシステム使用専用の領域を確保し、SSD の寿命の延長やパフォーマンスの向上を図る。

方法： SSD の内部の物理的な記憶容量（PBA）をユーザの使用する公称容量（LBA）に対して大きく用意し、システム（ファームウェア）動作専用領域として確保し、実使用容量の増加や不良ブロックの置換などによる、ウェアレベリングや書き換え動作時の作業領域の矮小化に対し、十分な作業領域を確保する。

参考： 最近は、SSD の使用目的によってユーザ領域とオーバー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 も発表され、以下の様に「書き換え動作時の作業用領域の確保」の重要性について解説されている。

・性能と容量調節

性能向上と容量増加にはトレードオフの関係がある。

PX04S ファミリーでは、前世代の SSD までは固定であった容量を、ユーザーが調整できるようにした。ユーザー容量を減らすとランダムライト性能が向上し、装置の書換えに対する耐久性も高くなる。逆にユーザー容量を増やすとランダムライト性能は下がり、装置の書換えに対する耐久性は低下する（図 4）。

例えば、データライト頻度が少なくリードが主であるユーザーに対しては、ランダムライト性能を下げ、より多くの記憶領域を提供することが可能であり、サーバ・ストレージシステム当たりの総記録容量を増加させることができる。

このように性能と容量を調節可能にすることで多様化する顧客要求に応えられる。

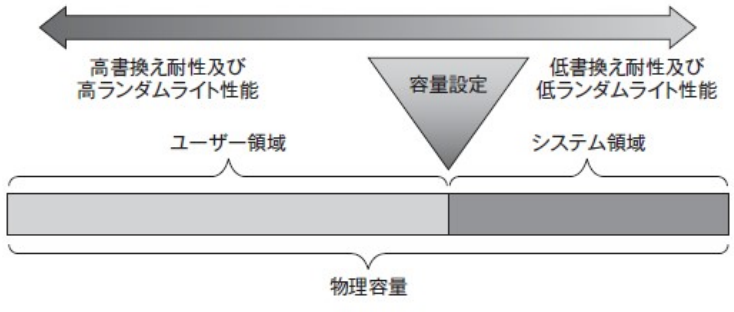


図4．性能と容量の調整イメージ — ユーザー容量を設定することで，書換え耐性及び性能を優先するかユーザー容量を優先するかの調整が可能である。

Outline of performance and capacity control

引用元：茂呂祐行,金子淳
多様化する顧客要求に柔軟に対応するエンタープライズ向け SAS インターフェース SSD
東芝レビュー Vol.70, No.8, pp.17-20 (2015)

３．１．３．その他の SSD 高速化技術

① ガベージ・コレクション（Garbage Collection）：　ガベージ・コレクションは、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、データのフラグメンテーション（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（Garbage：くず・ゴミ）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の分別を行い、それぞれ別のブロックにコレクション（Collection：収拾・集める）することによって、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。

② トリム（TRIM）：　トリムは、SSD が HDD と異なる特性を持った記憶装置であることを、明確に区別して取り扱うことを行うようになった Windows 7 以降の OS に存在するコマンドで、ファイルの削除・更新動作などにより、フラッシュメモリー上に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、上記のガベージ・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て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）の書き換えは不要と判定し作業量を削減することが可能となるので、SSD の動作速度の低下を予防できる。但し、これらの動作の詳細についての規定・規格は存在しないので、個別の SSD に於ける実際の動作の詳細は、製造メーカに委ねられている。

３．２．SSD の注意点

① SSD と HDD はコンピュータ上では、ほぼ同一の機能を持った「ドライブ：記憶装置」であるが故に、相違点を意識することなく取り扱う場面が多いと思われるが、半導体素子であることによる「上書きが不能で、消去動作が必要」であることが原因となり、例えば HDD においては最も単純な「削除データの復旧」のような場合であっても、SSD ではトリムやガベージ・コレクション、オーバープロビジョニング、ウェアレベリングの存在により、削除直後であってもそのページ（データ）をシステムが使用する領域に移動されてしまう可能性がある。また、データが複数のページやブロックに存在する場合では、ファームウェアの動作によってアドレスが変更されることにより、本来は存在しなかった断片化が発生する可能性の存在を否定することはできない。

② 消去を行った場合でも、OS やユーザがアクセス可能な領域だけの処置を行った場合は、消去済のはずの SSD に突然データが現れるような現象が発生する可能性の存在を否定することはできない。

③ Secure Erase による抹消に於いても、SSD に対するコマンドであるため、実動作は製造業者の定めた範囲（領域）に対し、製造業者の定めた動作によって、コマンドとして要求されている結果を得ること以外は定められていないので、例えば「実動作を、消去（初期化）済ブロックを検出し、そのブロックに対する処理を省くことで処理の高速化を図る」ことも可能であり、それが「データ抹消に関する性能評価報告」に記載されている Secure Erase を連続して実行した場合に初回よりも 2 回目の処理時間が短縮される現象の原因となっていると推定することもできる。

④ TRIM をサポートしている（Windows7 以降）の OS を使用している証拠保全対象媒体が SSD である場合に、SSD を証拠保全用媒体として複製を作成した場合、既に TRIM コマンドが発行されたが、未消去状態にあったデータが証拠保全対象媒体上に存在した場合、複製作成時やその後に証拠保全先媒体の電源 ON 時に、ファームウェアの自動動作によって、完全消去されてしまう可能性の存在を否定することはできない。

以上、思いつくままに SSD に於ける問題点を列挙したが、結論としては「証拠保全ガイドライン第４版」に記載されているように「フラッシュ系媒体は、代替領域等の隠し領域の都合上、無データ状態であることを確認することが難しいため、複製先として証拠保全に用いる場合は注意が必要である」ことだけでなく、「複製作成後にデータが変化する可能性も存在すること」を十分に認識することが重要であり、これらの問題を免れるためには、デュプリケート（コピー、クローン）による複製ではなく、イメージファイルの作成を行う必要がある。

４．証拠保全用媒体を対象とする「データ消去」（データの存在しない状態を作り出す）

現在選択可能な、最も広範囲にデータの消去を行う手段としては、OS では認識することの出来ない、DCO（Device Command Overlay：装置構成オーバレイ）や HPA（Host Protected Area：秘密領域・保護領域）などによる隠し領域、不良セクタとして検出され代替処理の行われた領域まで含めた消去を行うことのできる Enhanced Secure Erase の実行が最も理に適った方法だといえる。但し、媒体に対して発行されるコマンドであり、実際の動作は個別媒体のファームウェア（プログラム）に依存しているので、実行後に全 LBA 領域に対するゼロ（全ビット 0）で 1 回の上書き抹消を行い、その後に確認作業（Verify）を行う事が必要である。

しかし、これによっても、NIST 文書 SP800-88r1（2014 年 12 月）で指摘している、製造メーカに依存する領域や、大阪データ復旧の下垣内氏の提唱する「PARADAIS」に対する容易な消去手段が存在しないため、「証拠保全ガイドライン第４版」に記載されている「一切のデータが存在しない状態」をデータの抹消によって作り出すことは、残念ながら不可能と断言せざるを得ず、「新規の工場出荷状態が保たれ，何もデータの書き込まれていないクリーンな状態であることが保証されている媒体の購入」による必要があるが、市場に存在する単品販売の HDD は、流通経路に信頼の出来ない（製造業者の工場出荷状態が保たれていない）ものも存在するため、「新規に購入することをもって、クリーンな状態であることが保証される」ことにはならない。

このような難易度の非常に高い、「証拠保全先媒体のクリーンな状態」を要求することを避ける手段としては、証拠保全の手段として「物理的な複製媒体の作成」を選択するのではなく、「イメージファイルの作成」を選択することや、「マネージメントの強化」によることも可能なので、この方面により注力する必要がある。

マネージメントによる方法としては、「証拠保全ガイドライン」第 4 版「５．証拠保全作業中・証拠保全作業後」、「５．６．６．同一性の検証」に記載されている、「保全されたデータ・・・省略・・・に対してハッシュ値を算出する。・・・以下省略。と記載されているように、調査・解析作業終了後にもハッシュ値の取得を行い、原本、作成直後の複製、調査・解析作業終了後の複製の 3 件のハッシュ値を比較検証することで可能であるし、昨年カスペルスキーによって発表された HDD のデータ抹消の不可能な、起動シーケンス実行時に読み込まれる SA（System Area）のファームウェア領域に潜むマルウェアや、PARADAIS 領域に潜むデータによる影響は、証拠保全後の HDD の電源投入時毎にハッシュ値の再取得・確認を実行すれば検出することは可能である。

このように、HDD や SSD には「SA」、「製造メーカに依存する部分」や「PARADAIS」などの、データの抹消が不可能な領域が存在することを認識し、且つ、記録方式による特徴を理解した上で、個別案件の重要度や必要と予測される分析・解析内容・手法による条件などを勘案し、合理的な原本同一性の管理方法を選定する必要がある。

参考：　今回は触れていないが、最近の 6TB を超える大容量 HDD に導入されている「瓦記録」方式は、基本的には「追記型」であることにより、その解決法として SSD に於ける「オ

ーバープロビジョニング」に類似した、システムの管理する作業専用の領域の存在が説明されており、また、「データの書き換え」も SSD と同様な 2 段階動作が必要であり、通常の瓦記録方式ではない HDD と比較して動作が低速になる可能性も持つので、証拠保全先媒体として使用する場合は SSD と比較しても更に注意を払う必要がある。

引用元：下村和人, HDD の大容量化をけん引する瓦記録技術 東芝レビュー Vol.70, No.8, pp.29-32 (2015)

注意：本書に於ける「消去」とは、元のデータ（情報）を、フラッシュメモリーに於ける消去動作（初期化）や、飽和磁気記録に於ける、連続する“ゼロ”の上書きを行う事で消し去る（磁気反転の無い状態にする）手段を指し、「抹消」とは、「消去」や暗号化などの方法を用いて、データの復旧が困難な状態にすること全般を指す。