ＩＤＦ第１２期第３回「データ消去」分科会（２０１５．１０．８）

日本のPCリユースにおける データ消去

株式会社アセットアソシエイツ

データ消去とは・・・

OSやソフトウェア上での操作による削除では、
システム内にデータが残存する可能性がある。

残存したデータは様々な手法により
復元される可能性がある。

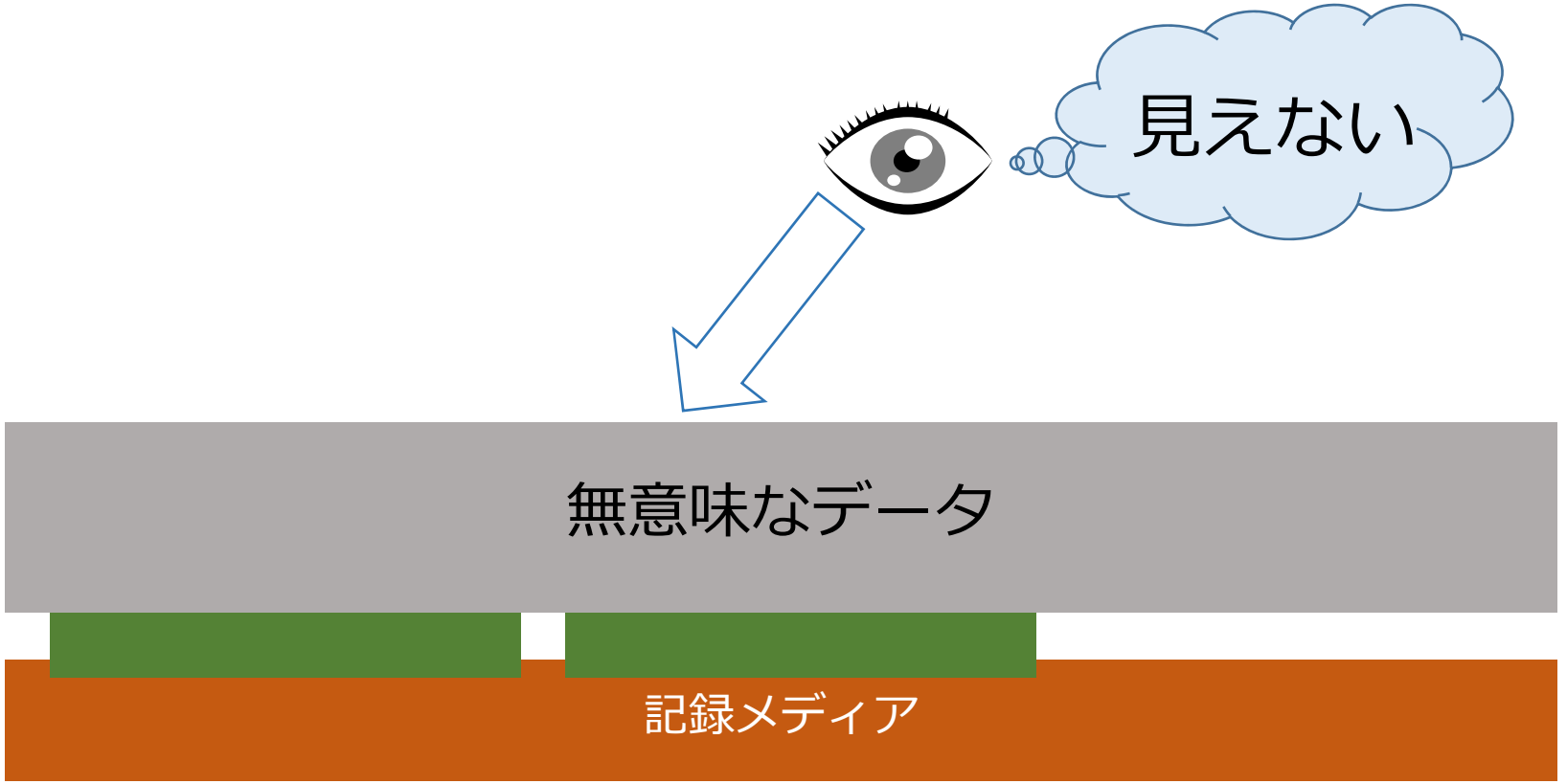
“データ消去”とは復元不可能な状態に
データを破壊する事である。

OS上から削除操作


使用中
使用中
データ（ファイル）
データ（ファイル）
記録メディア
空き区画の印をつける
空き区画
使用中
データ（ファイル）
データ（ファイル）
記録メディア

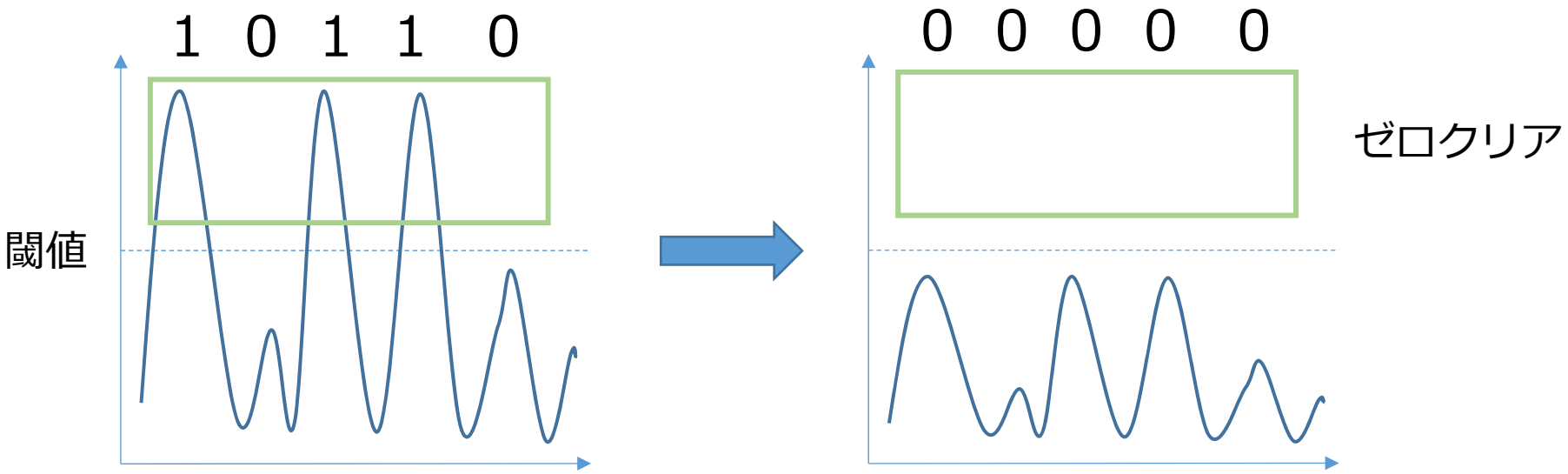
データ消去のソフトウェア的手法

データ消去ツールでは無意味なデータを上書きすることにより
残存するデータの復元を不可能な状態にする。

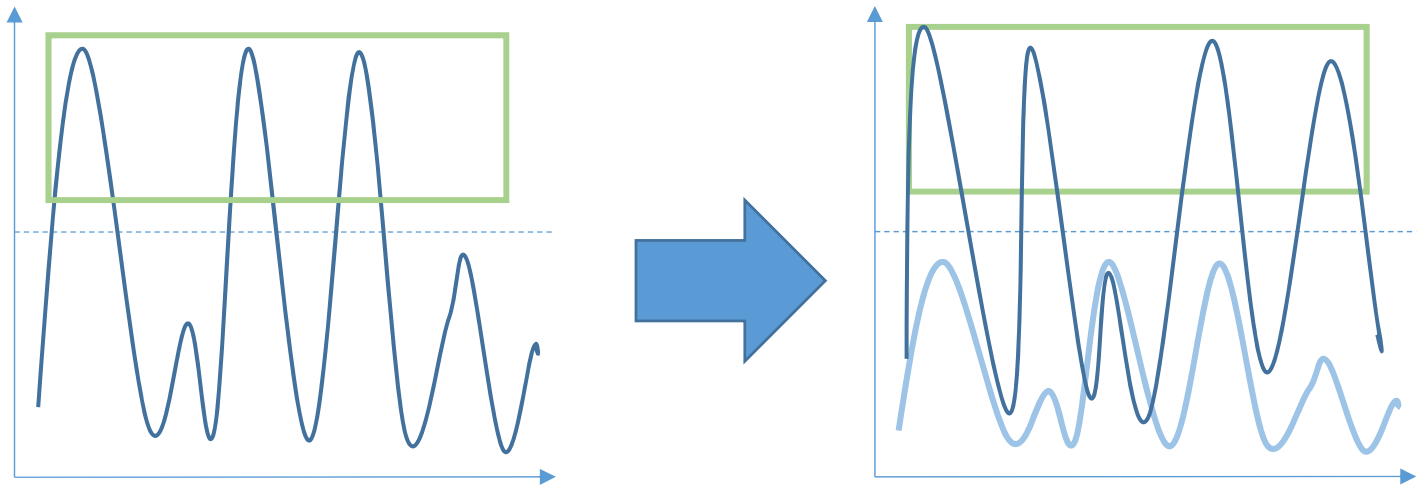


データの残留

※　アナログデータで記録する磁気メディアではデータが残存する可能性がある。



データの残留



複数回ランダムデータを書き込むことにより
残留したデータの推測を難しくする。

NSA方式やDoD5220.22-Mなどの所謂消去アルゴリズム

データの残留

複数回の書き込みによるデータ破壊はフロッピーディスクや
データ密度の低い旧式の磁気メディアを対象としたもの。

高密度なハードディスク等の残留磁気によるデータ復元は
事実上不可能と言われている。

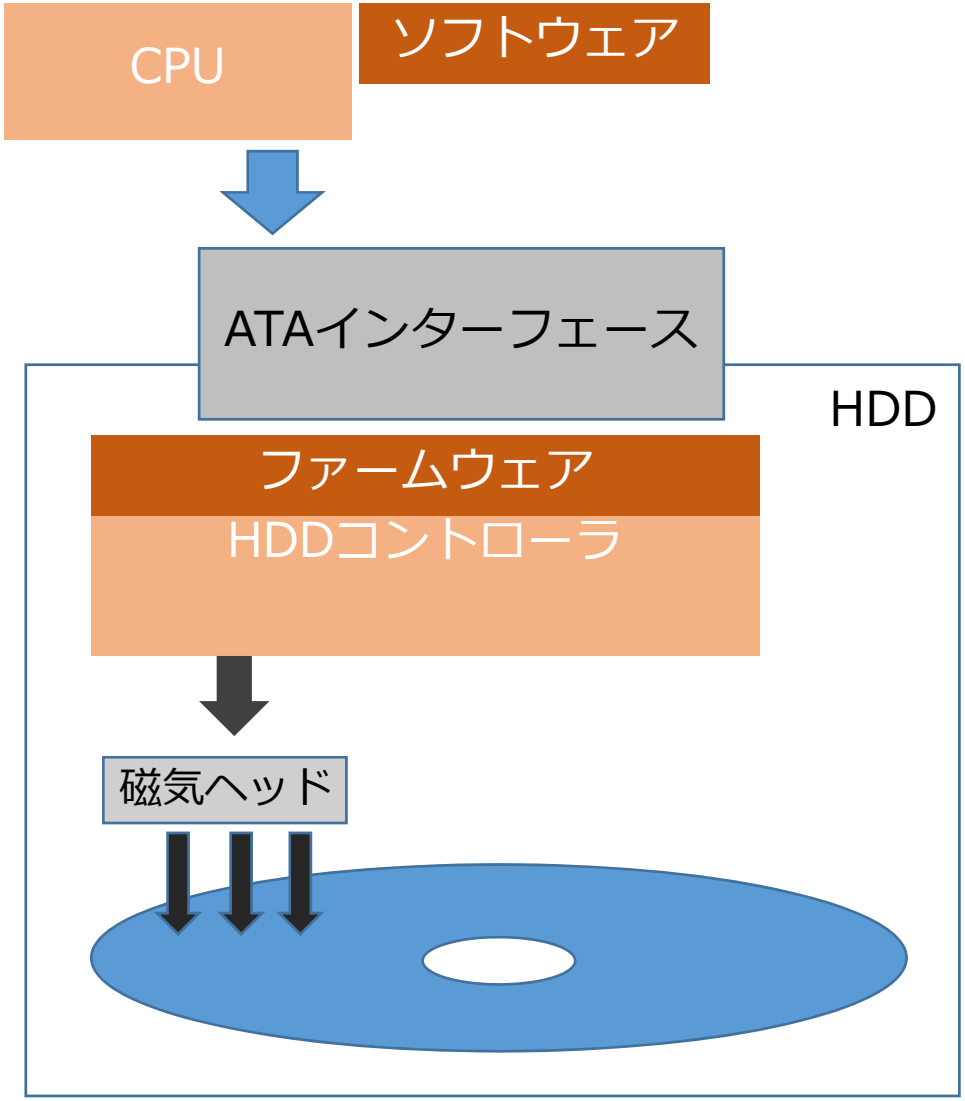
※ JEITA「パソコンの廃棄・譲渡時におけるHDD上のデータ消去に関するガイドライン」
においても1回固定データによる上書きで十分とされています。

PCデータ消去ソフトでは

数多くのデータ消去アルゴリズムがあるが、
日本の多くの現場では
0クリア、NSA方式、DoD5220.22-M方式が使われている。

※NSA方式やDoD方式は元々データ消去の基準が無かった頃からの
慣例で使用されている事が多いようです。

ドライブへのデータアクセス（ATAの場合）



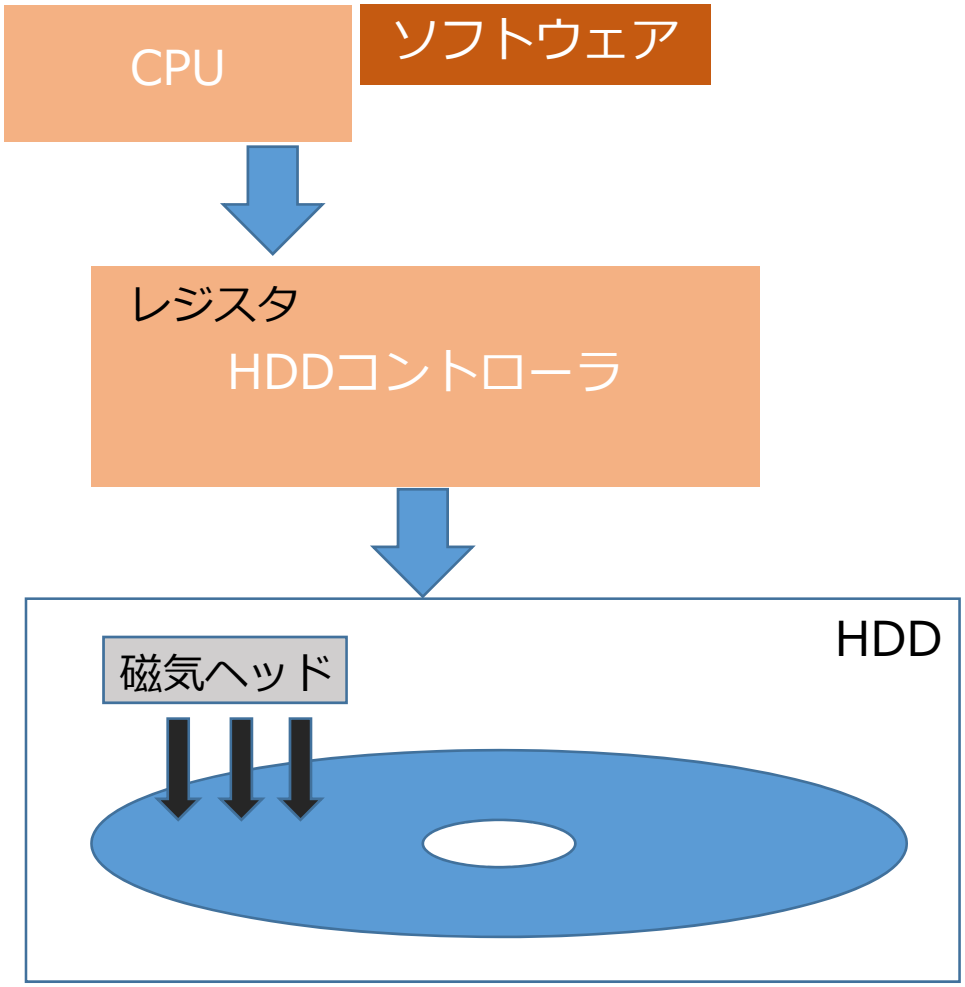
ハードディスクはATAというソフトウェアインターフェースによりアクセスする。

ATAは様々なコマンドが定義されているがコマンドに定義されていない操作をすることができない。

ドライブへのデータアクセス

ATA以前のHDDでは、
HDDコントローラはHDDの外部にあり
ヘッドやトラック位置を直接コントロール
して読み書きしていました。

ATA(IDE)は、この外部のコントローラを
HDDに予め内蔵したものが原型です。
そのため現在のバージョンでもヘッドを
直接制御していた当時のコマンド体系の
名残を多く残しています。



ATAの拡張

ATA

IDE　HDD制御

EIDE　大容量化

ATAPI　非HDD・光学ドライブ

：　コマンドの拡張

元々HDDの制御信号に近いものだったATAは拡張され様々な機能をサポートするためのコマンドが追加されていきました。

SSD

SSD（Solid State Drive）

半導体（フラッシュメモリ）を使用した記憶媒体。

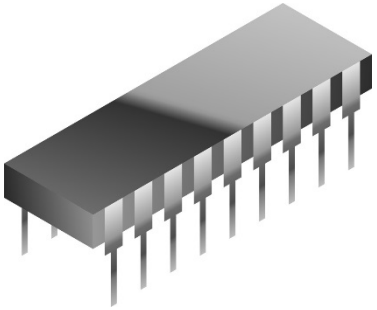
HDDと同様のソフトウェアインターフェースを持ち
HDDの置き換えを容易にしている。
（セクタ単位でアクセスするブロックデバイス）

主なハードウェアインターフェース
SATA、SAS、eMMC、NVMe・・・

フラッシュメモリ

フラッシュメモリとはEEPROMの一種

・電荷を注入することにより書き込んだデータを保持する
・電圧を掛けることにより消去（フラッシュ）
・ブロック単位での消去
・消去・書込み回数の制限、寿命

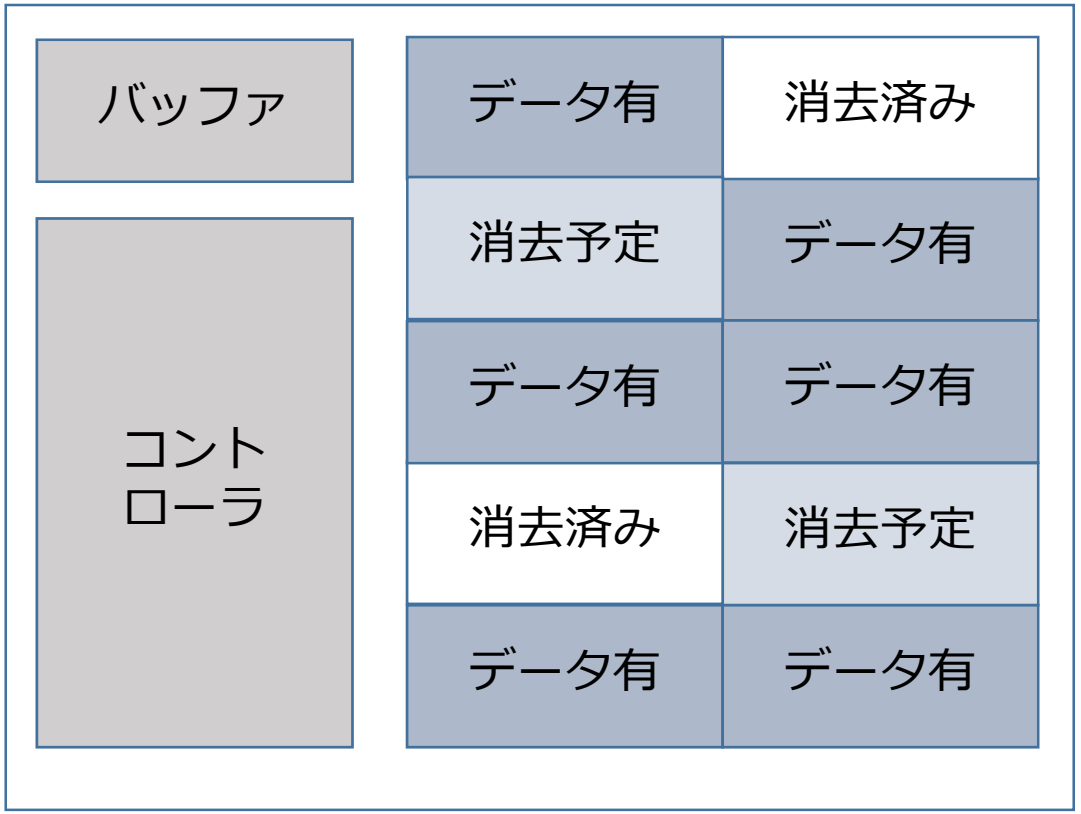


データを書き込む場合、
一旦消去を行ってから書き込みを行う。

※上書きが出来ない。

フラッシュメモリ

フラッシュメモリは
その特性上バイト単位での
アクセスは困難であるが、
HDD等と同様な
ブロックデバイスの置き換え
には適していると思われる。

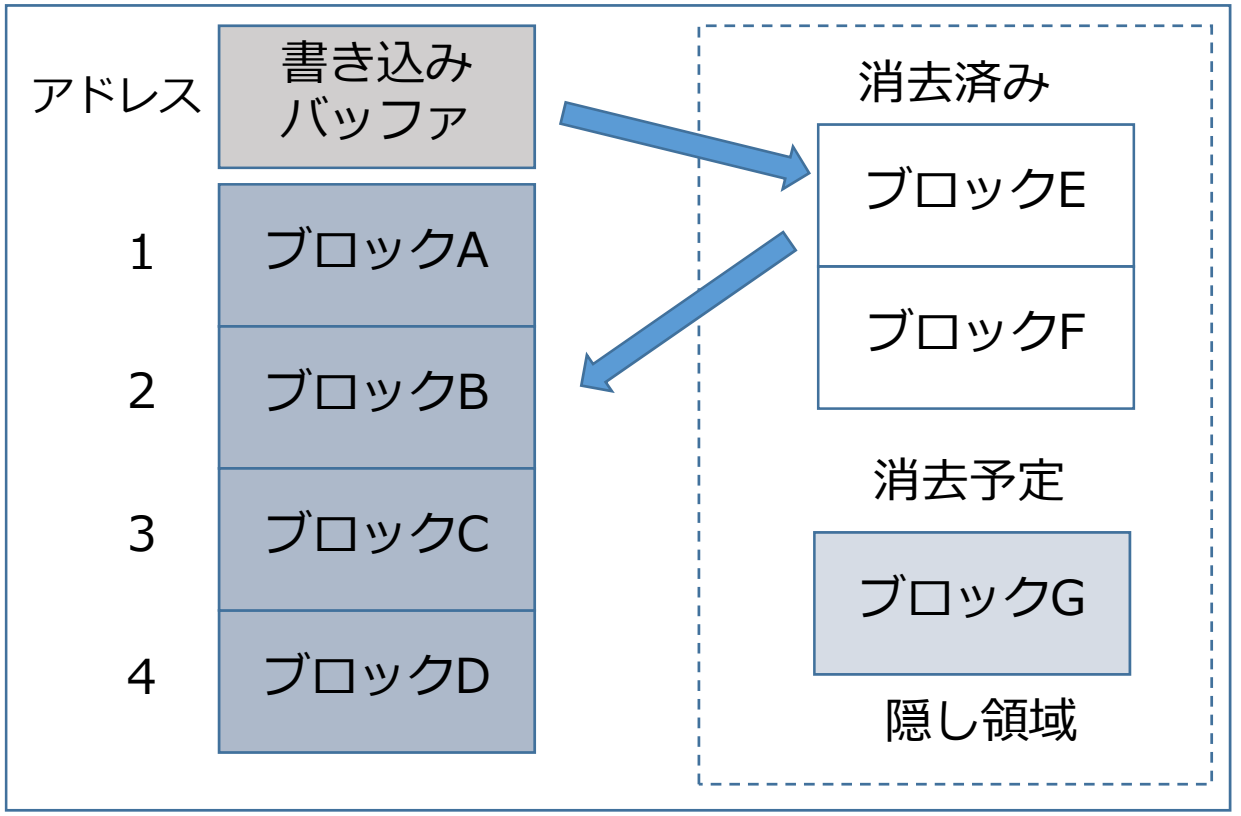


隠し領域の積極的な利用

アドレス２に書き込む場合

書込バッファに転送したデータを隠し領域に予め用意してある消去済みブロックに書き込む。

書き込んだブロックとブロックBを入れ替える。



隠し領域の積極的な利用

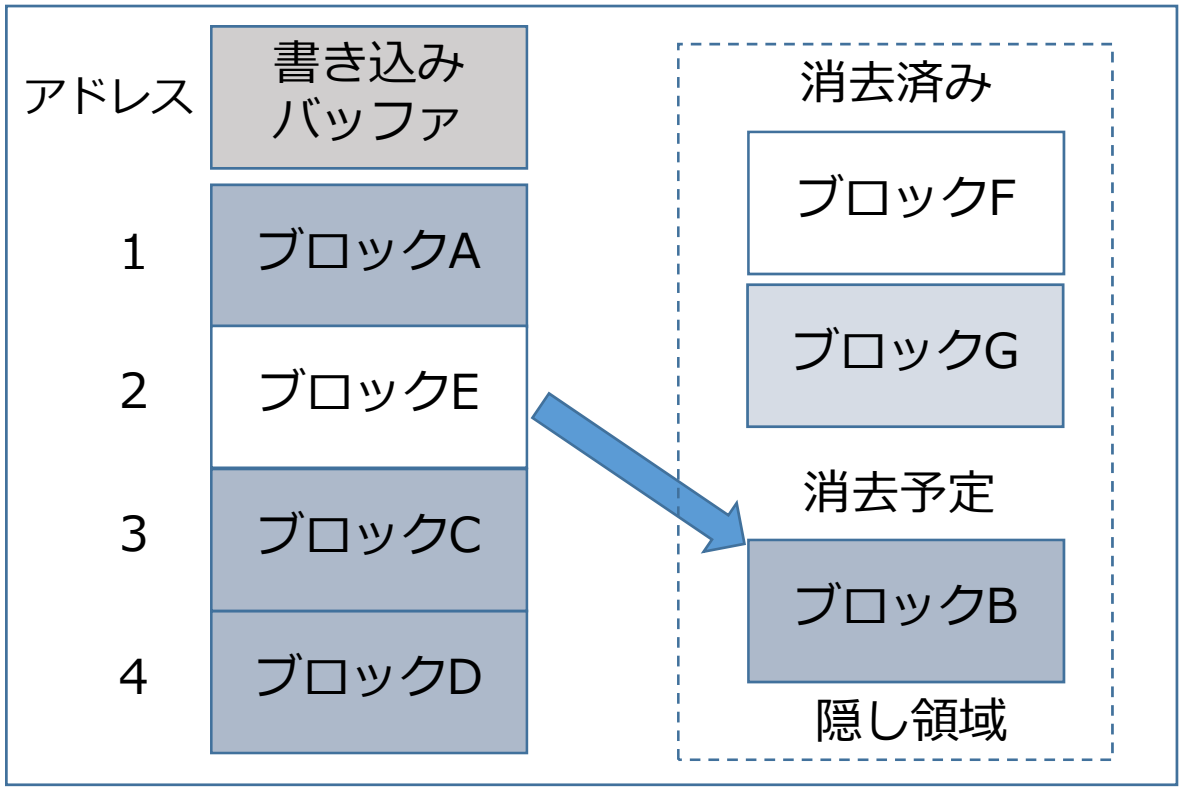
アドレス２に書き込む場合

書込バッファに転送した
データを隠し領域に予め
用意してある消去済み
ブロックに書き込む。

書き込んだブロックと
ブロックBを入れ替える。

隠し領域の
ブロックBは消去予定に。

隠し領域の消去予定ブロックは
バックグランドで消去。

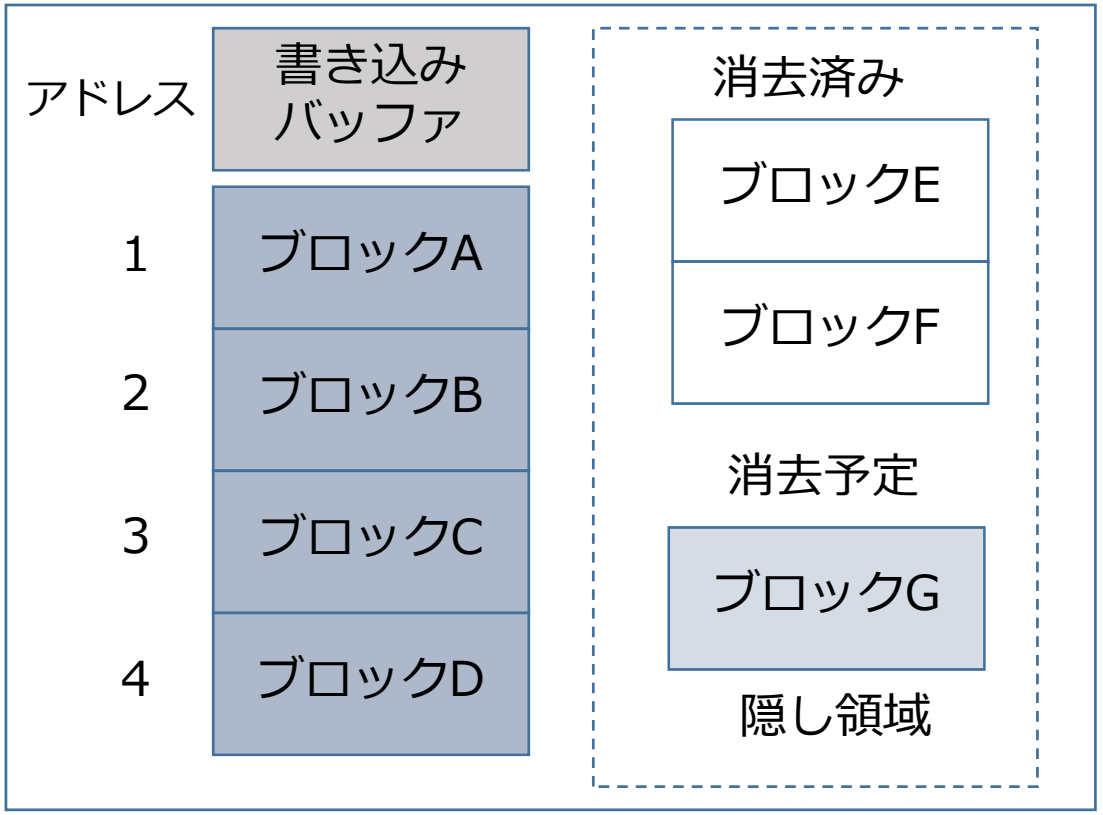


※速度の遅い消去・書込み処理の時間の隠蔽。
※消去書込みブロックの均一化。

SSDのデータ消去

SSDの消去・書込み処理は
ドライブ内で行われるため
外部インターフェースからは
直接見ることが出来ない。

SSDのソフトウェアインター
フェースは元々HDD用に定義
されたものを転用しているため
SSD内でのブロックの入れ替え
（ウェアレベリング）やブロック
消去の直接制御が出来ない。



SSDのデータ消去（Secure Erase）

ATAで定義されている消去コマンド（セキュリティコマンド群の中の１つ）

ATA規格での定義

Security Erase Unit

クリップ領域を含めたユーザーエリアにゼロを書き込み消去

Enhanced Security Erase Unit

ユーザーデータ及び、代替セクターをデータを書込み消去

SSDのデータ消去（Secure Erase）

ユーザー領域の消去を定義したコマンドであるが・・・

Security Erase Unitは元々HDDのために定義されたもの。
FlashROMには上書きを行わないと思われる
代替“Reallocation”領域の定義は？

ATA規格上で定義されているが実際の動作はドライブ内の
ファームウェアが行うためソフトウェア的な検証が出来ない。

SSDのデータ消去（Secure Erase）

ユーザー領域の消去を定義したコマンドであるが・・・

正しく消去処理が出来たのか、処理が定義されていない。
消去せよ・終了後に成功か失敗か出力せよ
としか定義されていない。
処理はドライブのファームウェアに任されているため、
消せない領域があったのか？
データ領域の状態など一切知ることは出来ない。

SSDのデータ消去（Secure Erase）

ユーザー領域の消去を定義したコマンドであるが・・・

ドライブのファームウェアの
動作を信じるしかない

Secure Eraseのデータ消去作業上の問題点

PCリユース現場でのデータ消去作業時の問題

PCのデータ消去作業を行う場合多くの考慮すべき点がある。

様々な種類のドライブが様々な機種のPCに装着された状態で消去作業を行うため、多くの例外が発生する。

- 時間的制約
- 例外処理

Secure Eraseのデータ消去作業上の問題点

SECURITY ERASE UNIT コマンドがサポートされているか？

比較的新しいドライブの多くはサポートしているが
ドライブにより対応状況が異なる。

サポートしているコマンドの種類等により処理が異なってくる。

Secure Eraseのデータ消去作業上の問題点

実装上の問題

SECURITY ERASE UNIT が使用できる条件
　ドライブがFrozenモードではない。
　ドライブのパスワードが解除されている。

※Security Frozenモード
　Secure Eraseなどのコマンドは非常に危険なため、
　Freezeコマンドを発行することにより無効にすることができる。
　Frozenモードを解除するにはドライブの電源を切る事が必要。

多くのPCではPC起動時にBIOSによりFreezeコマンドを発行する。

Secure Eraseのデータ消去作業上の問題点

実装上の問題

Frozenモードを解除できるか？

Frozenモードを解除するにはドライブの電源を切る必要がある。

PCの電源が入っている状態でドライブの挿抜を行う。

解除できる可能性は比較的高いが物理的に不可能な場合が多い。

ソフト的に電源を切る。
PCの省電力機能などを利用してドライブの電源を切る。

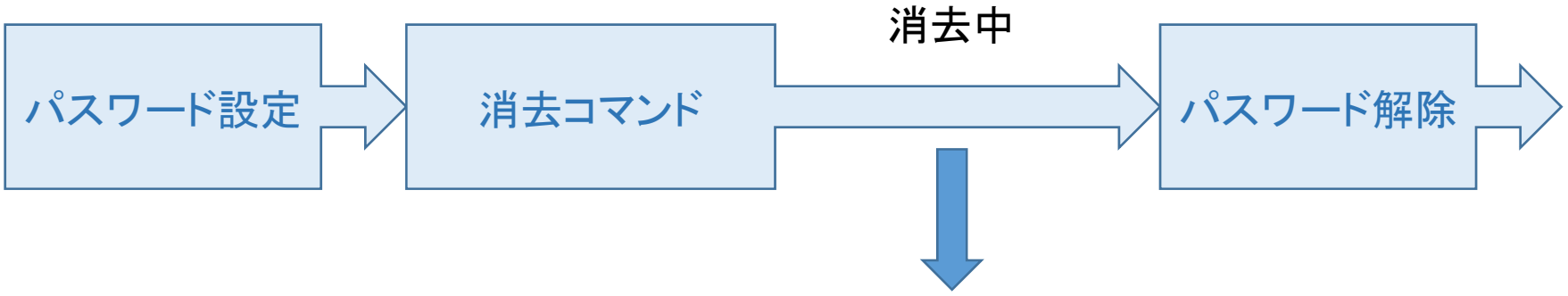
解除できるかどうかはPCの種類（設計）に依存する。

Secure Eraseのデータ消去作業上の問題点

作業上の問題

Security Eraseの動作中にPCの電源を切るとどうなるか？

Security Eraseコマンドを
実行するためにドライブパスワードを設定する。
このパスワードは消去終了後に解除する。



Secure Eraseのデータ消去作業上の問題点

作業上の問題

Security Eraseの動作中にPCの電源を切るとどうなるか？

多くのPCのBIOSはHDDにパスワードが設定されていると、
起動時に起動パスワードの入力が必要になる。

BIOS上で入力するパスワードは何かしらの変換をされている事があり、消去時に設定したパスワードを入力出来ない状態になる。

ドライブを取り外さないかぎり起動不可能なPCに・・・

Secure Eraseのデータ消去作業上の問題点

問題点

多くの例外が発生するため作業効率が非常に悪い。

作業結果の検証が難しい。(消去作業のエビデンスの発行)

Secure Eraseを行ったもの行わなかったものが混在する。

作業ミス等によりPCが起動不可能になる。

などなど・・・

データの読み書きコマンドによる消去

特徴

・読み書きコマンドはどのような環境でもほぼ必ず使用できる。
・書き込む処理・書き込んだデータのコンペア等
ソフトウェアにより行う事ができる。

非常に汎用性が高い・・・一方

・Secure Eraseのように隠し領域の積極的な消去が出来ない。

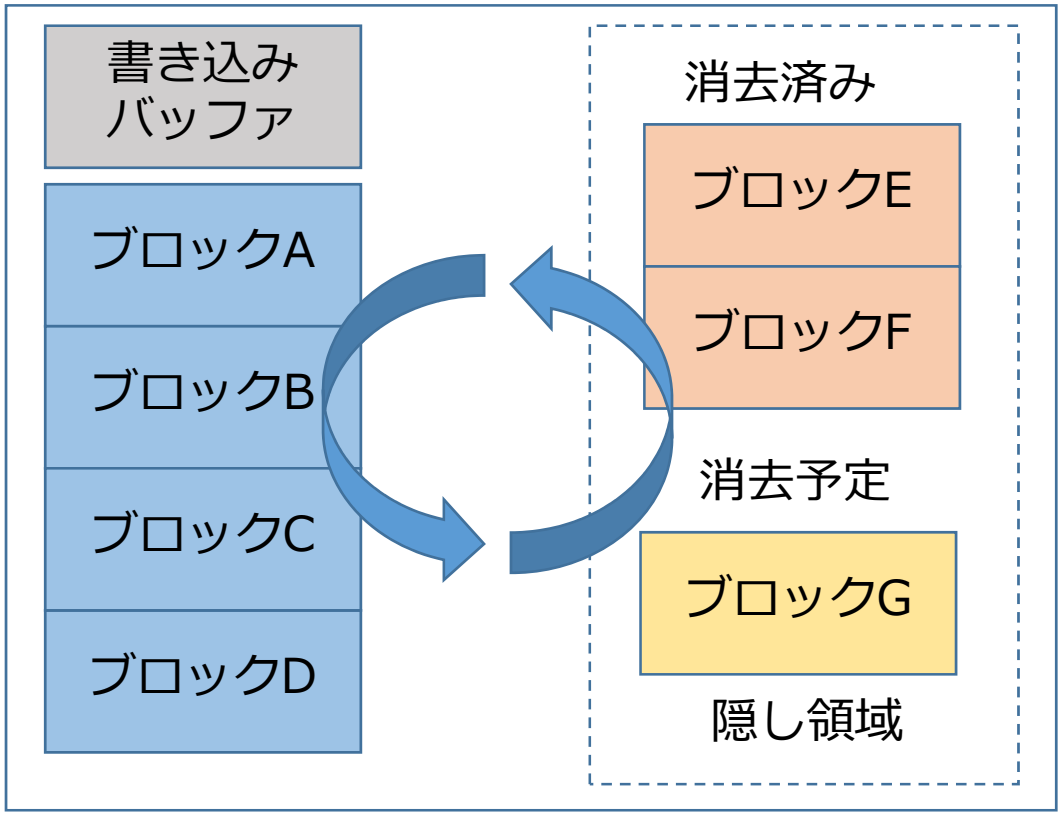
現在のHDDは１回データの上書きを行う事により
ほぼ復元不可能な状態になると言われている。

データの読み書きコマンドによる消去

現在のHDDは１回データの上書きを行う事によりほぼ復元不可能な状態になると言われているがSSDの場合は・・・

SSDは隠し領域を積極的に利用しながら動作するためHDDの様に一回上書きしただけでは、データが残った領域が隠し領域に隠れた状態になる。

隠し領域に入ったデータのブロックはバックグラウンドで消去されるが、その状況を外部から確認することは出来ない。



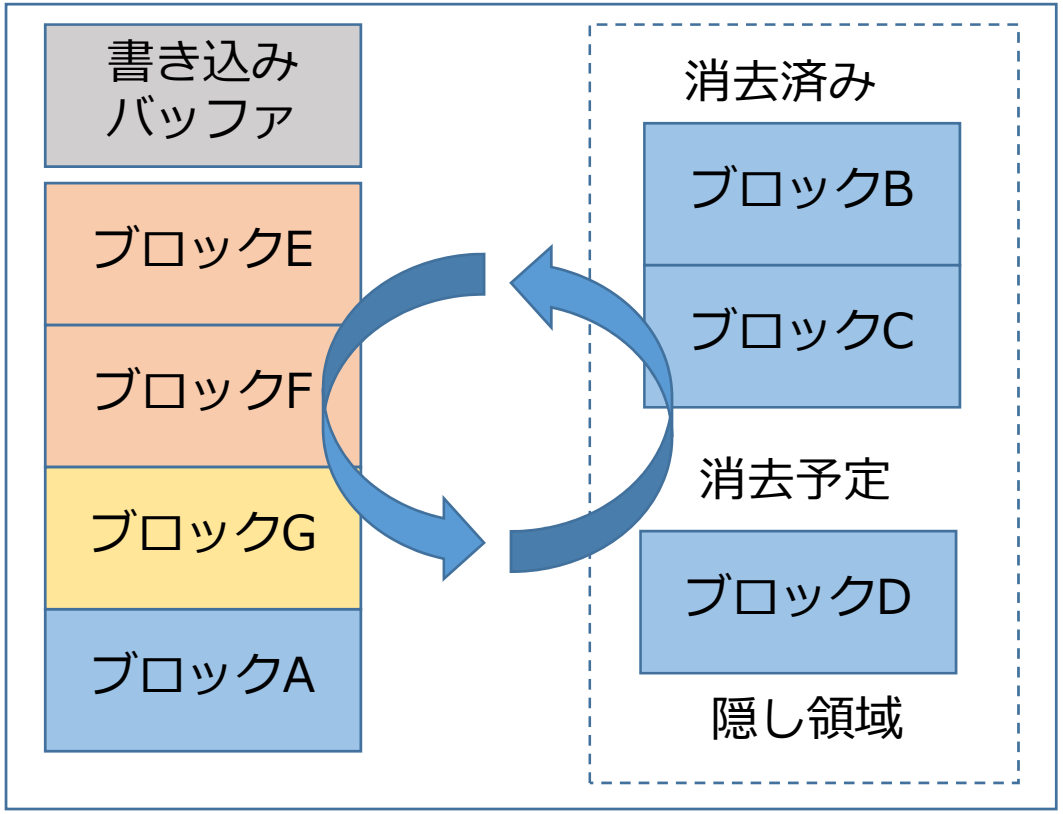
データの読み書きコマンドによる消去

SSDの特性を利用する

統計的な手法であるが、
SSDに２～３回の上書きを
することにより有効なデータ領域
と隠し領域がほぼ満遍なく入れ
替わり復元不可能な状態になる。

これはコントローラのウェア
レベリングの動作に依存するが、
FlashROMの特性上ほとんどの
コントローラは隠し領域全体を
入れ替える様に動作するようで
ある。

FlashROMの寿命を伸ばすため
一部の領域のみを入れ替える
可能性が少ない。



データの読み書きコマンドによる消去

ソフトウェア消去の考慮点は・・・

隠し領域を消去できるかどうかは
確率の問題になる。
SSDのコントローラ・ファームウェアに
依存するが統計的にはほぼ復元不可能な
状態になるようである。

ソフトウェア的なデータ復元は不可能。

隠し領域が消去されたか確認するには
SSDを破壊する必要がある。
(これはSecureEraseの場合も同様…)