消去方式の確立と有効性の証明

～検証可能なデータ消去技術～

2022年12月6日

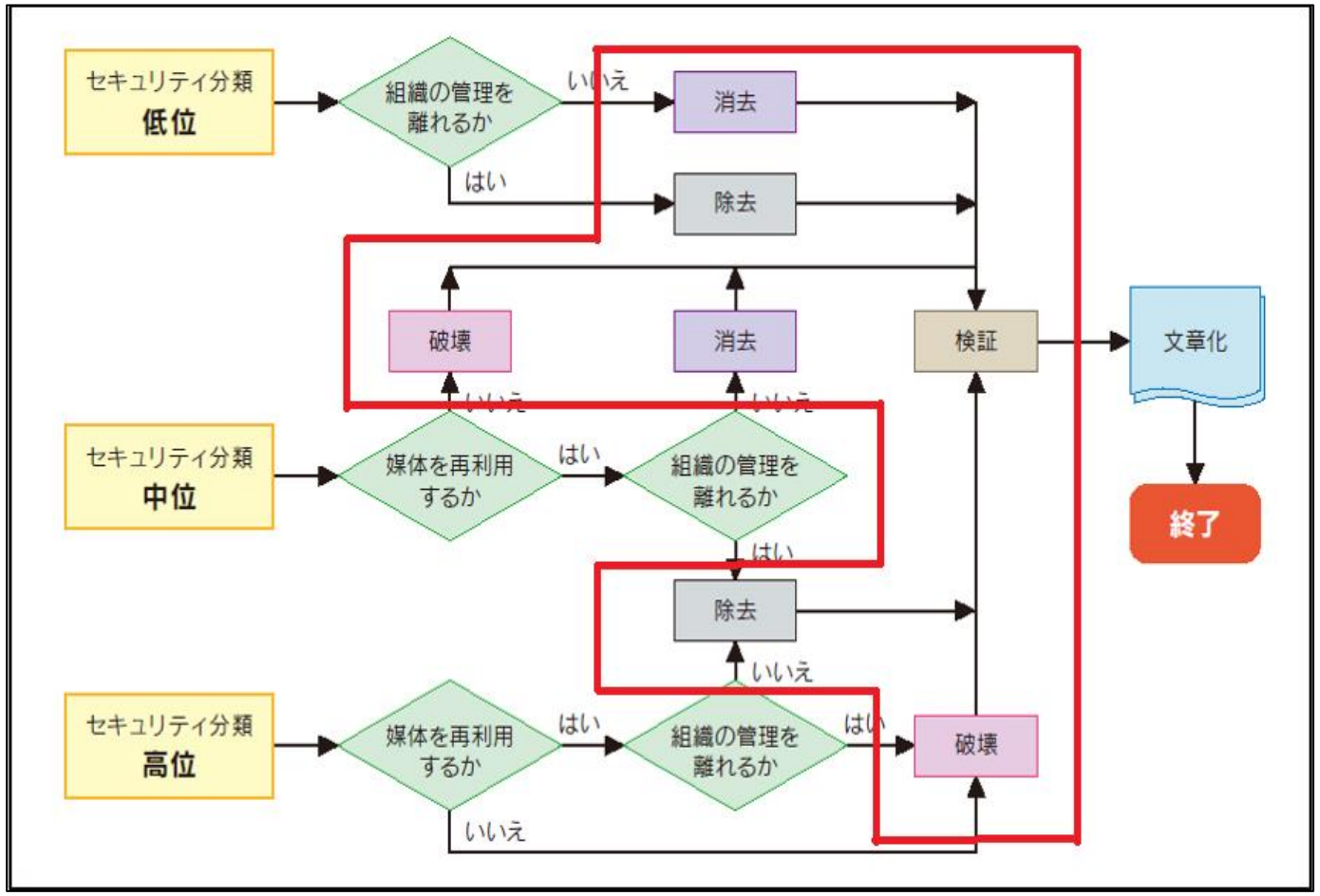
ADEC　消去技術認証委員会　委員

堀　芳之

ADEC：Association of Data Erase Certification

https://www.adec-cert.jp

消去技術認証委員会の目的



赤枠で囲まれた

・消去（Clear）

・除去（Purge）

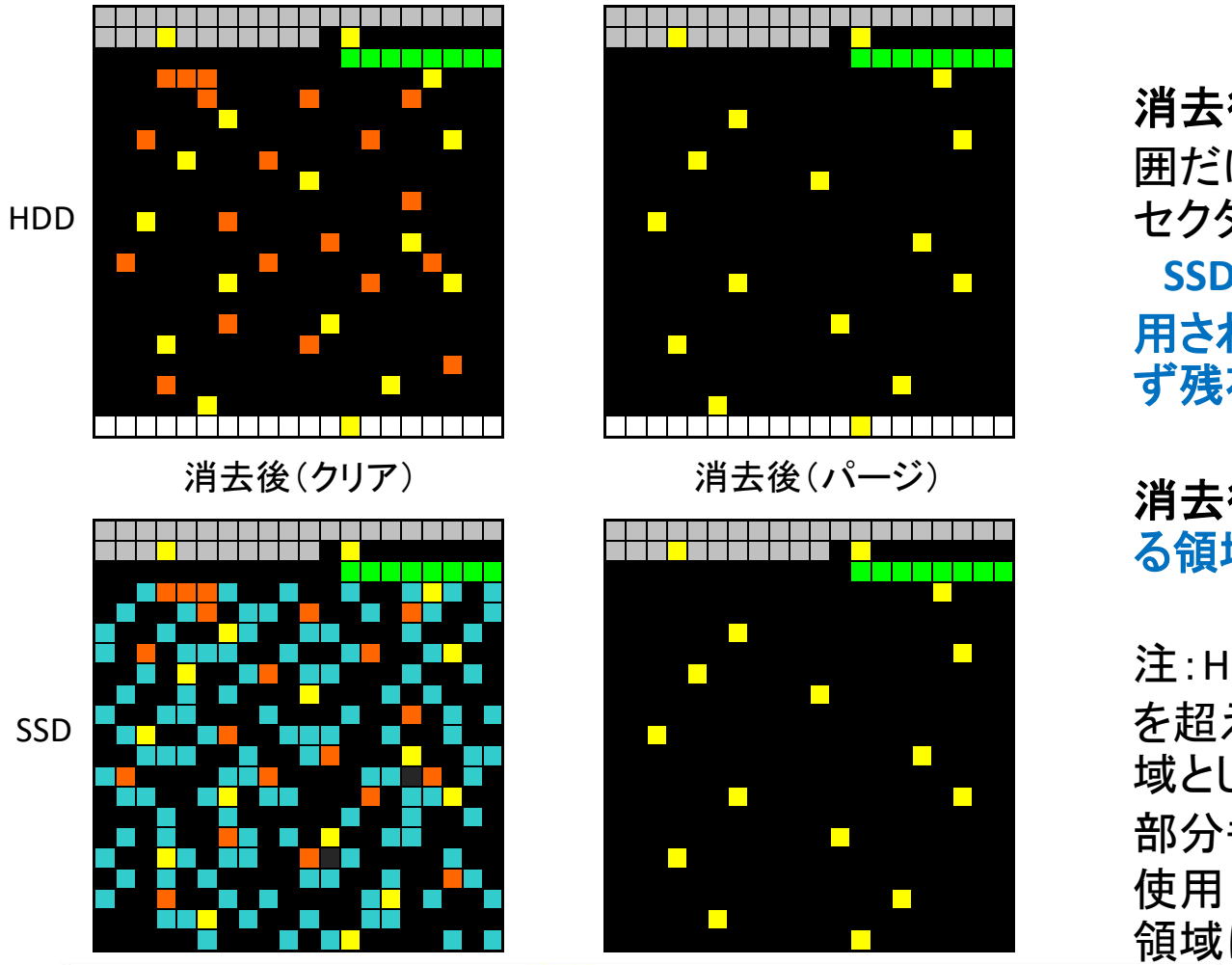
・破壊（Destroy）の方式に対して、実現可能な技術論とその検証方法を確立することを目的とする。

消去（Clear）と除去（Purge）

・消去
　記憶媒体上の「OSが認識できる領域」のデータを抹消。
⇒一般的な復元ソフトなどでは復元できない抹消方式

・除去
　記憶媒体上の「あらゆる領域に書き込まれたユーザデータ」を抹消。
⇒専門的な設備を持つ研究所などでも復元できない抹消方式

消去と除去の動作の違い



消去後（クリア）では、OS経由でアクセス可能な範囲だけが消去され、媒体の使用中に発生した欠陥セクタ（データ有り）はそのまま残存する。

SSDでは、システム動作（データキャッシュ）に使用されたオーバ・プロビジョニングも対象に含まれず残存する。

消去後（パージ）では、**データの書き込みが行われる領域全てが消去対象**となる。

注：HDDにおいては、製造時に規定する記憶容量を超えた領域を余剰なアクセス不可能な未使用領域としているが、SSDでは規定の記憶容量を超えた部分もオーバ・プロビジョニングとして利用するため、使用（データの更新・新規書込み）によって未使用領域は消滅する。

抹消方式の検証（ClearとPurgeの差異）

・HDDの場合

通常ではアクセスできない不良セクタに有意なデータが残っていれば除去ではない。
⇒検証可能なデータを書き込んだセクタを不良セクタとして認識させられれば、消去ソフトの挙動によりClearかPurgeかの判断が可能。
※SATAは可能。SASは最終検証中

・SSDの場合

書き込み動作中にアンマップされ、ERASEされる前の領域には情報が残っている場合がある。
アンマップされている領域は有効なアドレス（LBA）を持たないため、アクセスできない。
⇒SSDの記憶素子を基板上より取り外し（チップオフ）、検証可能なデータを別途書き込んだ状態で再装着し、消去ソフト実行後再度チップオフして内容を確認することでClearかPurgeの判断が可能。

有意なデータ(データ構造)の例

個人番号：1234-5678-9012

セキュリティコード：9876

郵便番号：123-4567

住所：東京都港区赤坂13-26-52 虎ノ門紛いビル

氏名：消去　太郎

電話番号：090-9876-0110

※こんな情報でも128バイト程度あれば記録できてしまう。

　セクタサイズ512バイトと仮定するなら4件残せる。

暗号化消去

ClearとPurgeにおいて、その主たる相違点は通常ではアクセスできない領域に残っている情報に到達できるかどうかに依存している。

もし、これらの情報がアクセス可能であったとしても、その情報そのものが暗号化されており、復号のための手段を持たなければ、Purge相当と考えられるのではないか。

⇒暗号化消去の優位性

- 暗号化キーを記録媒体と分離し、適切に管理すれば、情報漏洩の恐れはない。
- 暗号化キーを削除すれば、該当する記憶媒体にアクセスすることなく情報漏洩対策となる。

※現在技術認証委員会では、鍵管理の手法や運用プロセスを含む暗号化消去の標準化にも取り組んでいる。

今後の活動

- 磁気消去機
  多様な磁気記録媒体に対する、外部磁界照射によるデータ消去を行う磁気消去機の認証技術の確立

- 物理破壊装置
  非磁性体方式を含む記憶媒体に対する物理破壊装置の認証技術の確立