“データ抹消に関する米国文書（規格）及び HDD、SSDの技術解説”について

2016年4月18日

株式会社　DD-RESCUE
沼田　理

自己紹介

- 沼田 理（ぬまた まこと）
- 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する。
  1986年より（株）ワイ・イー・データに於いて、
  FDDなど磁気記憶装置の設計開発業務に携わり、
  2001年：日本のデータ復旧事業の草分け的存在のオントラック事業部に異動、
  2006年：事業部長に就任、2010年3月定年退職。
  その後、日本データ復旧協会事務局長、
  株式会社データサルベージ社顧問などを歴任。
- 現在は、本当はフリー、データ復旧関連複数社で、顧問、また技術情報、Web原稿などを提供中。

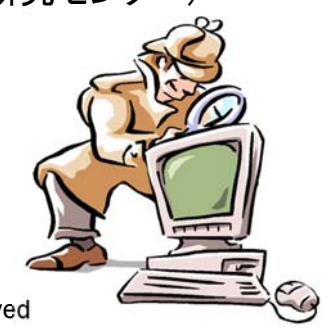
報告書：データ抹消に関する米国文書（規格）及び HDD、SSDの技術解説について

- ねらい

デジタル技術の先進国である米国のデータ抹消（消去）に関する規格は、記憶媒体に関わる技術の進歩に伴い、継続的に改訂が行われているが、Web上では未だにDoDやグートマン方式などの複数回の上書き消去理論や、磁気力顕微鏡によるデータの読み出しなど、もっともらしい、訳の分からない情報が出回っている。

「証拠保全先媒体のデータ抹消」に関して論ずるに必要な、HDDやSSDに於ける「データの書き込み及び消去」の、正しい基本的な技術や、製品化、高速化などを目的に開発、使用されている応用技術の実態を把握し、「証拠保全」のありかたを考える。

報告書　目次



2. HDDの磁気記録
  2．1．飽和磁気記録と未飽和磁気記録
  2．2．磁気ヘッドの特性
  2．3．磁気―デジタル信号変換の原理
  2．4．上書きの実態
  2．5．現在のHDDに使用されているヘッドの特性
  2．6．HDDのヘッドとプラッタ、データトラック
    2．6．1．「はみ出し部分」（幅）8nmに対する考察
    2．6．2．「はみ出し部分」のデータの読み出し
  2．7．HDDに用いられている技術以外のデータ抽出手段
    2．7．1．磁気力顕微鏡とは
    2．7．2．磁気力顕微鏡の測定限界
  2．8．HDDの上書き抹消に対するまとめ

2015年3月 「データ消去」分科会(第11 期 第5 回)
上書きされたデータは読み出せるのか？
― HDD の磁気記録の仕組みとデータ消去 ―
より、一部を文書化

3. SSDのデータ記録
  3．1．NAND型Flash ROMの動作と内部構造
    3．1．1．SSDの書き込み動作
    3．1．2．問題解決の手段
      ウェアレベリング、ECC・リフレッシュ、オーバープロビジョニング
    3．1．3．その他のSSD高速化技術
      ガベージ・コレクション、トリム
  3．2．SSDの注意点

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）

結論は？

- 純技術的には：
  HDDの場合は、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、1回上書きするだけで効果的に抹消することが可能。（「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。）

  ・消去手段は：ATAコマンドとして実装されたEnhanced 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）

以上：NIST　SP800-88 （2006年9月） 昨年の講演は、技術論のため此処までにとどめた。

- しかし、現存する製品の実態は：
  SSDの、予備やウェアレベリングを目的とした領域や、HDDにおいても製造上発生する余剰な領域のような、製造者のみが管理する領域（PARADAISなど）が存在するため、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に）動作するか否かについては、製造者の信頼と保証に頼らざるを得ず、Enhances Secure Eraseを含む現存する上書き抹消手段によって「記憶媒体がクリーンな状態」になることは保証されていない。

以上：NIST SP800-88r1 (2014年12月）

- SSDは、証拠保全先媒体としては不適格。特にSSD⇒SSDの複製作成時、複製後も電源ON時にコマンドやファームウェアが動作する可能性がある。

では、どうすれば？

- 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。
  - 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。
    リファービッシュ、初期不良返品の再選別、など

- 「物理的な複製媒体」ではなく、「イメージファイル」を作成する。
  - 媒体に残存している、消え残りデータの影響を受けない。

- 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。
  - 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、ファームウェア領域に潜むマルウェアや、PARADAIS領域に潜むデータの影響も、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可能。

最後に！

是非、報告書をダウンロードし、熟読いただければ幸いです。

https://digitalforensic.jp/wp-content/uploads/2016/02/technical-aspect.pdf

そして、Web上に氾濫している、根拠のない情報を
簡単に信じることは　避けていただきたい。