データ抹消に関する性能評価報告

2016 年 4 月 10 日
情報セキュリティ大学院大学
宇野幸治，土井洋

1. はじめに

証拠保全作業において，クリーンな媒体の準備が必要である．媒体をクリーンにすることを媒体内のデータの抹消ととらえているが，このためには市販の抹消ソフトなどを用いて媒体(HDD や SSD 等)の抹消を行うことが想定される．媒体内のデータの抹消を行う場合，媒体内の全てのデータへの上書きを行うことが多く，例えば Hughes 等の論文[1]の表 1 に示されている方法では”Block overwrite”に相当する．NIST SP 800-88 Rev.1 [4]では Clear に相当し，RITEA[7]や JEITA[9]における 1 回以上の書き込みに相当する．

Hughes 等は 2009 年の論文[1]で HDD に対して 3 回上書きとその検証を行う場合，半日程度を要すると評価するとともに，(Enhanced) Secure Erase が高速であることについても言及している．Hughes 等がこれらの結果を示してから現在に至るまで，CPU の性能向上，(SATA 等の)データ転送速度の向上を含め，PC 等の性能は向上している．同時に，HDD や SSD 等の媒体の容量も飛躍的に増大しており，また I/O 速度も向上している．SSD は 2015 年時点では広く普及しており，容量がやや少ないがデータの読み書きは高速である．これらの媒体に対してデータ抹消ツールの評価を行うことが本報告の目的である．対象媒体を SATA 接続の HDD(2 種類)と SSD(1 種類)に絞り，市販ソフトや機器(HDD の複製機に付随している抹消機能等)を利用して抹消性能評価を行った．

2. 評価対象ソフトおよび機器

本調査においては，「データ消去」分科会メンバーから提供された市販ソフト 3 種類でまずは評価を開始した．その後，同分科会メンバーからのコメントを反映させ，フリーウェアの抹消ツール(DBAN)，Linux の抹消に係るコマンド(dd および shred)，及びデュプリケータの抹消機能を用いて評価を行った．ソフトや機器の情報を表 1 に示す．

CD 起動可能なものがいくつかある．これらのソフトは PC 破棄時に使うことを想定しているものも少なくなく，その場合には OS 非依存で CD 起動可能であることは重要である．なお，市販ソフトには HDD の抹消に関する記述があったが，SSD への対応については 1 つのみが言及していた．D は Darik's Boot and Nuke(DBAN)と呼ばれるフリーウェアである[1]．E と F は Linux (CentOS 7.1)のコマンドである．また，G はディスクのコピーを主目的とする機器である．

[1]フリーウェアであり抹消の保証まではしていない([3]には e.g. DBAN does not detect or securely erase SSDs)と記載されていた．

表 1 上書き抹消評価に用いたソフト，機器などの情報

名称	分類	起動方法
A	市販ソフト	Windows プログラム/CD 起動
B	市販ソフト	Windows プログラム/CD 起動
C	市販ソフト	CD 起動
D	DBAN 2.2.8	CD 起動
E	dd コマンド (Linux)	CentOS 7.1 のコマンド
F	shred コマンド(Linux)	CentOS 7.1 のコマンド
G	デュプリケータ	デュプリケータの抹消機能

(Enhanced) Secure Erase についても評価した．ソフトや機器の情報を表 2 に示す．後述するように評価対象の SSD が Intel 製であることから, Intel が提供するソフト[6]を評価対象 H とした．I はフリーウェア，J は市販ソフトである．なお，H は Secure Erase のみを，I と J は Secure Erase と Enhanced Secure Erase を選択可能であった.

表 2 (Enhanced) Secure Erase を利用したソフトの情報

名称	分類	起動方法
H	SSD メーカ(Intel)のソフト	Windows プログラム
I	フリーウェア	Windows プログラム
J	市販ソフト	その他

3. 抹消方法について

製品 A，B，C では，製品により選択可能な方式は多少異なるが，

0 で抹消，乱数値による抹消，NCSC 方式，米国陸軍方式，米国海軍方式，
米国国防総省方式，NATO 方式，Gutmann 方式，ランダムランダムゼロ，
ドイツ標準方式 VSITR，NSA 方式

が選択できた.

製品による解説によると, 書き込むデータとしては 0, 何らかの固定値, およびその補数, 擬似乱数などであった．また，書き込み回数は 1 回だけのものや，合計 3 回のものなどがあり，最大のものは Gutmann 方式の 35 回であった．A，B，C のいずれも選択可能だったのは，0 で抹消，乱数値による抹消，および米国国防総省方式であり，抹消回数を選択できるものもあった．D，E，F でも 0 で抹消，乱数値による抹消が可能である．なお，乱数値による抹消については，固定パターンで上書きするものと乱数生成源を用いるものがある．適切な乱数生成源(例えば，Linux の場合/dev/urandom)を用いる場合は，乱数の生成に時間を要することに注意が必要である．G はデュプリケータであり，乱数値による抹消が可能である.

(Enhanced) Secure Erase はデバイス(HDD や SSD)に命令を送れば，あとはデバイス内で抹消処理を行う．SSD に対しては，SSD 製造メーカが提供する H に加え，I と J が対応している．HDD に対しては I と J が対応している．

本評価では，抹消に要する性能評価が目的であるため，0 で 1 回上書き，及び乱数値による 1 回上書きに要する性能評価に絞ることとした．また，(Enhanced) Secure Erase についても性能評価も行った．

4. 評価対象等について

評価においては，PC 自体の性能差の影響も評価するために，性能の低い PC(PC-A)と性能の高い PC(PC-B)の 2 種類を用いた．実験に使用した 2 台の PC は購入直後の状態で，OS のアップデートは実行せず，ネットワーク接続もしなかった．

また，評価対象媒体として HDD を 2 種類用意した．2 種類の HDD の主な仕様を A.2 に示す．HDD-1 はやや古い HDD である．これに比べて HDD-2 は新しい[2]．SSD は 1 台だけを評価した．SSD の主な仕様も A.2 を参照のこと．

5. 上書き抹消の評価

上書き抹消は, 特に HDD の場合かなりの時間を要するため, 一度しか試行できなかった．詳細は A.3 を参照のこと．

HDD に対する上書き抹消については，利用するツールにより抹消時間にはかなりのばらつきが生じることがわかった. 特に HDD-1(やや古い HDD であり, インタフェースも古い)については，抹消時間のばらつきが顕著であった．一方，HDD-2 に対する 0 による抹消については，A(Win および CD 起動)，C(CD 起動)，D(CD 起動)，F(コマンド)では，揃って 1 時間 50 分程度で終了した．デュプリケータ G による抹消でも，HDD-2 では 1 時間 50 分程度で終了した．これらの実験では乱数で抹消する実験も行ったが，方式によって乱数を生成するアルゴリズムが異なることに注意が必要である．例えば E では[8]に示されているように乱数生成源として/dev/urandom を利用したが，抹消に時間を要した．これは乱数の生成に多くの時間を要したと考えられる. D も乱数生成源は/dev/urandom ではないものの, 多くの時間を要したと考えられる．

SSD に対する上書き抹消に要する時間は総じて短いが，容量差(HDD-2 は SSD のおよそ 8 倍)を考慮する必要がある．インタフェースが同一(SATA3)である SSD と HDD-2 については，ツールにもよるが，容量差を考慮すると上書き抹消性能に顕著な差が見られないものもあった．

---

[2] HDD-2 については，メーカーからデータ抹消などを含むツールが提供されている．一部の情報を A.1 に示す．

6. Secure Erase の評価

Secure Erase 及び Enhanced Secure Erase は PC からの膨大な数の書き込み命令により抹消が行われるわけではない．デバイス(HDD や SSD)内で処理を行うので，PC やインタフェースの性能差等は全くなかった．詳細は A.4 を参照のこと．

HDD-1 は(Enhanced) Secure Erase をサポートしていなかった．HDD-2 については，ツールに関係なく Secure Erase 及び Enhanced Secure Erase のいずれも，1 時間 50 分程度で終了した．

SSD についても，ツールに関係なく Secure Erase 及び Enhanced Secure Erase のいずれも，1 分未満(実際は数十秒程度)で終了した．なお，SSD については，連続して Secure Erase を行うと，1 回目が 10 秒程度，2 回目以降が数秒程度で終了するという事象が時々発生した．そこで，あらかじめデータを書き込んだ後に Secure Erase による抹消実験を行った．いずれの場合も，最大でも 1 分未満で終了した．

なお，PC 起動時に HDD や SSD は通常は Security Frozen 状態になる．また，Security Frozen 状態の HDD や SSD に対しては，(Enhanced) Secure Erase は使えず，抹消オペレーションとしてその解除(HDD や SSD に接続されているケーブルの抜き差し)が必要であった．

7. まとめ

HDD および SSD に対し，市販ソフトを含めたいくつかのデータ抹消ツールの評価を行った. 今回の評価では, 120GB の SSD や最大で 1TB の HDD に対しての評価であったが，上書き抹消については，ツールにより抹消時間にかなりのばらつきが生じることを確認できた. HDD(HDD-2)に対しては一部のツールや(Enhanced) Secure Erase は 1 時間 50 分程度で終了することを確認できた．SSD に対しては (Enhanced) Secure Erase は 1 分以内に終了することを確認できた．

乱数による抹消を行う際に擬似乱数生成を必要とする場合，その生成コストの影響が大きいことも確認できた．なお，Secure Erase 及び Enhanced Secure Erase は，Security Frozen 状態の解除のオペレーションが煩雑である．

参考文献

[1] Hughes, Coughlin, Commins, Disposal of Disk and Tape Data by Secure Sanitization, IEEE Security & Privacy, Vol. 7, Issue 4, pp.29-34 (2009).

[2] Acronis True Image WD Edition マニュアル, Acronis International GmbH. http://supportdownloads.wdc.com/downloads.aspx?lang=jp&fid=wdsfDesktop_Blue (2016 年 1 月 31 日確認)

[3] Darik's Boot And Nuke (DBAN). http://www.dban.org/ (2016 年 3 月 6 日確認)

[4] Guidelines for Media Sanitization, NIST Special Publication 800-88 Rev. 1 (2014).

[5] HDDErase Ver. 4.0. http://cmrr.ucsd.edu/people/Hughes/secure-erase.html (2016 年 3 月 27 日確認)

[6] Intel SSD Toolbox v3.3.3, Intel Corporation. https://downloadcenter.intel.com/ja/download/18455/-Solid-State-Drive-Toolbox (2016 年 1 月 30 日確認)

[7] 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，一般社団法人情報機器リユース・リサイクル協会. http://www.ritea.or.jp/eh_guide.html(2016 年 1 月 30 日確認)

[8] データの完全消去，ウィキペディア. https://ja.wikipedia.org/wiki/%E3%83%87%E3%83%BC%E3%82%BF%E3%81%AE%E5%AE%8C%E5%85%A8%E6%B6%88%E5%8E%BB (2016 年 2 月 14 日確認)

[9] パソコンの廃棄・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 ，一般社団法人 電子情報技術産業協会 (2010). http://home.jeita.or.jp/page_file/20110511155520_8vAEy2Fi5d.pdf (2016 年 1 月 30 日確認)

付録 A　抹消性能評価

A.1 評価用 HDD メーカが提供する抹消方法

本評価の対象の媒体の一つとして，Western Digital 社の HDD を選択した．この HDD に関連したツールとして，Acronis True Image WD Edition をダウンロードできる．これには，ディスクの破棄などを想定した抹消に関する機能があるので参考情報として紹介する．マニュアル[2]には「ハードディスクの消去方法」に関する記述があり，漏えいのメカニズムとして

> 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。

図 1　ハードディスクの消去方法(Acronis True Image WD Edition マニュアルより抜粋)

と記載されている．また，消去方法として，米国国防総省準拠 DoD5220.22-M 方式，米国海軍準拠 NAVSO P-5239-26-RLL 方式，米国海軍準拠 NAVSO P-5239-26-MFM 方式，ドイツ VSITR 方式，ロシア GOST P50739-95 方式，グートマン（Peter Gutmann）方式，Bruce Schneier 方式，高速(全セクタに対して論理値ゼロ(数値 0x00)で抹消)が選択可能と記載されている．

A.2 評価対象について

評価においては，PC 自体の性能差を評価するために，性能の低い PC(PC-A)と性能の高い PC(PC-B)の 2 種類を用いた．PC-A および PC-B の主な仕様を表 3 に示す．

表 3　評価用 PC の仕様

	PC-A	PC-B
CPU	Celeron G1820 (2.70GHz)	Core i7-4790 (3.60GHz)
チップセット	インテル H81	インテル H97
メモリ	4GB DDR3 SDRAM	4GB DDR3 SDRAM
OS	Windows7 Home Premium 64bit	Windows7 Home Premium 64bit
接続 SATA ポート	SATA3(転送速度 6.0Gb/s)	SATA3(転送速度 6.0Gb/s)

CPU とチップセットはいずれも PC-B の方が高性能である．実験に使用した 2 台の PC は購入直後の状態で，OS のアップデートは実行せず，ネットワーク接続もしなかった．設

定も購入直後の状態のままとした．ただし，PC-B による DBAN の実験の際に起動時に不具合が発生した．そのため UEFI 画面で USB の xHCI 動作モードを無効に変更して評価を行った．

媒体として 2 種類の HDD を評価した．容量およびインタフェースが主な違いである．2 種類の HDD の主な仕様を表 4 に示す．

表 4　評価用 HDD の仕様

	HDD-1	HDD-2
メーカー	Seagate	Western Digital
容量	750GB	1TB
回転数	7200RPM	7200RPM
キャッシュサイズ	16MB	64MB
インタフェース	SATA2(転送速度 3.0Gb/s)	SATA3(転送速度 6.0Gb/s)

HDD-1 はやや古い HDD でありインタフェースも古い．これに比べて HDD-2 は新しいものである．

また，SSD は表 5 に示す Intel 製の 1 種類のみを評価した．

表 5　評価用 SSD の仕様

	SSD-1
メーカー	INTEL
容量	120GB
インタフェース	SATA3(転送速度 6.0Gb/s)

A.3 上書き抹消時間の評価

抹消に要した時間を示す．なお，各表内の”ー”記号はエラーの発生などのため抹消時間を得ることができなかったものである．値は分単位で切り捨てた．

HDD-1 に対する評価結果を表 6 に示す．製品 B を CD 起動した場合，起動直後に残り時間 530h 以上と表示されたため，CD 起動による実験は中止した．製品 C の場合，エラーが生じるなどの理由で多くの場合で評価ができなかったので，記載を見送った．HDD-1 では，後述する HDD-2 に較べて抹消性能(処理時間)にはかなりの差が生じた．

表 6　HDD-1 に対する評価

名称	起動方式	PC-A		PC-B	
		ゼロ	乱数	ゼロ	乱数
A	Win	03h15m	03h15m	03h15m	03h15m
	CD	113h01m	113h01m	112h55m	112h55m
B	Win	37h19m	31h39m	09h37m	09h37m
D	CD	23h51m	47h54m	13h54m	47h26m
E	Unix	12h58m	32h12m	13h54m	25h36m
F	Unix	30h05m	30h06m	30h07m	30h05m

HDD-2 に対する抹消評価結果を表 7 に示す．製品 B を CD 起動した場合，エラーが生じるなどの理由で一部の評価を断念した. HDD-2 に対する 0 による抹消については, A(Win および CD 起動)，C(CD 起動)，D(CD 起動)，F(コマンド)では，いずれも 1 時間 50 分程度で 1TB を抹消できたことになる．容量が大きいにもかかわらず HDD-1 より HDD-2 の方が抹消に要する時間が少ない場合が多かったが，インタフェースが高速なことに加え，記録密度が高いことなどが理由として考えられる．

表 7　HDD-2 に対する評価

名称	起動方式	PC-A		PC-B	
		ゼロ	乱数	ゼロ	乱数
A	Win	01h49m	01h52m	01h49m	01h49m
	CD	01h52m	02h39m	01h52m	02h24m
B	Win	52h31m	48h18m	14h48m	13h39m
	CD	20h12m	－	－	－
C	CD	01h52m	01h52m	01h52m	01h52m
D	CD	01h57m	03h43m	01h52m	03h50m
E	Unix	05h17m	28h47m	04h50m	21h45m
F	Unix	01h52m	01h52m	01h52m	01h52m

デュプリケータ G による抹消評価結果は表 8 に示す. デュプリケータ G では，抹消に関して上書きパターンが 2 種類選択できたが，それらの性能差は今回評価した HDD-1 と HDD-2 では確認できなかった.

表 8　デュプリケータ(G)による評価

HDD-1	HDD-2
06h40m	01h51m

SSD に対する抹消評価結果を表 9 に示す．製品 B を CD 起動した場合につては，エラーが生じるなど現象が発生したため, 評価を断念した. SSD と HDD-2 の容量比はおおよそ 1:8 であることに注意されたい.

なお，SSD については，連続して Secure Erase を行うと，1 回目が 10 秒程度，2 回目以降が数秒程度で終了するという事象が時々発生した．そこで，SSD の上書き抹消においても事前にデータコピーを実施した場合としなかった場合で評価を試みたが，上書き抹消の場合には大きな差は生じなかった[3]．表 9 は事前にデータコピーをしなかった場合の評価結果である．

表 9　SSD に対する評価

名称	起動方式	PC-A		PC-B	
		ゼロ	乱数	ゼロ	乱数
A	Win	04m	16m	04m	13m
	CD	19m	36m	18m	34m
B	Win	12m	12m	11m	12m
C	CD	11m	27m	12m	26m
D	CD	05m	20m	06m	18m
E	Unix	26m	03h24m	30m	02h36m
F	Unix	04m	13m	04m	04m

A.4 (Enhanced) Secure Erase 実行時間の評価

Secure Erase (表 10 および表 11 では，S.E.と表記)および Enhanced Secure Erase(表 10 および表 11 では, E.S.E.と表記)の評価を行った. PC 起動時に HDD や SSD は Security Frozen 状態になることが多い．また，Security Frozen 状態の HDD や SSD に対しては，(Enhanced) Secure Erase は使えない．そのため，必要に応じて HDD や SSD から電源ケーブルの抜き差しを行い，この状態を解除した後に実験を行った.

H は SSD の開発元が提供する SSD 用のツールである．したがって，SSD のみを対象とした．なお，H では Secure Erase のみの提供であったため，Secure Erase のみを評価し

[3] 一部のツールは，対象が NTFS である場合は抹消に膨大な時間を要した.

た． Iはフリーウェアであり，J は市販ソフトである．HDD-1，HDD-2 及び SSD について評価を行う予定であったが，HDD-1 に対して(Enhanced) Secure Erase を試みたところ，未対応である旨のメッセージが表示された．

HDD(HDD-2)に対する評価結果を表 10 に示す．また SSD に対する評価結果を表 11 に示す．

表 10 HDD(HDD-2)に対する(Enhanced) Secure Erase による評価

名称	PC-A		PC-B	
	S.E.	E.S.E.	S.E.	E.S.E
I	01h51m	01h50m	01h50m	01h51m
J	01h52m	01h52m	01h52m	01h51m

表 11 SSD に対する(Enhanced) Secure Erase による評価

名称	PC-A		PC-B	
	S.E.	E.S.E	S.E.	E.S.E
H	0m	－	0m	－
I	0m	0m	0m	0m
J	0m	0m	0m	0m

なお，SSD に対する H および I の(Enhanced) Secure Erase はいずれも 1 分未満(10 秒程度)であった．J の場合も 1 分未満(35 秒程度)であった．

なお，HDD に対してかなり古い PC で Center for Magnetic Recording Research (CMRR)[4] から取得した HDDErase[5]の評価も行ったが，結果はほぼ同じ(HDD-1 は未対応，HDD-2 は(Enhanced) Secure Erase は 01h51m 程度を要した) であった．

[4] 2015 年 7 月より Center for Memory and Recording Research