証拠保全先媒体のデータ抹消に関する報告書

2016 年 4 月 11 日

特定非営利活動法人デジタル・フォレンジック研究会

「データ消去」分科会

目次

1. 位置づけ

特定非営利活動法人デジタル・フォレンジック研究会より発行されている証拠保全ガイドライン[28][29]では、インシデントレスポンス時に必要と考えられる資機材等の準備の一つとして、フォーマット済みのクリーンな媒体（ハードディスク、CD-R 等の各種メディア）の準備が求められている。しかし、媒体の多様化や大容量化に伴い、このようなクリーンな媒体の準備に関してまとめておく必要があると考える。なお、証拠保全ガイドラインでは、以下のように一切のデータがない無データ状態のものを用意することを求めている。

> 4.1.1 媒体のチェック
>
> 複製先に用いる媒体は、あらかじめ書込み／読込み等のデバイスチェックを行い、正常に動作する状態のものを用意する。尚、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。
>
> 4.1.2 無データ状態
>
> 複製先に用いる媒体は、全て、一切のデータが存在しない状態（ファイルの通常削除レベルではなく、バイナリレベルで一切のデータの存在が確認できない状態）のものを用意する。但し、物理複製に関しても、複製に使用するツールが、複製元の不良セクターをゼロ値等に置き換え、複製先に保存する場合はこの限りではない。

このような状況を考慮し「データ消去」分科会は第 11 期（2014 年）に活動を開始した。そして第 11 期および第 12 期において、証拠保全先媒体に対する適切なデータ消去のためのガイドラインの策定を目標とし、国内外の文献調査や実態調査、ツール評価等を行ってきた。2 年間の活動の中では、プライバシ保護や情報漏えい対策等の観点からの意見も出されたが、証拠保全のためのクリーンな媒体の準備に絞って活動を進めてきた。後述するように無データ状態を完全に満たす媒体の準備は難しいとの結論に達したため、ガイドライン策定から得られた知見の公開へと目標をシフトした。[1][2][3][4][5][6][7]および本報告により、これらの知見について報告する。

本報告で扱う媒体の種類については、ハードディスク（HDD）またはソリッドステートドライブ（SSD）に限定し、ハイブリッド HDD のような両者の組合せは扱わない。現在広く PC で利用されている SATA 接続で、容量も PC で使われる程度のもの（HDD は 1TB 以上、SSD は 100GB 以上）を想定した。

媒体をクリーンにするための技術として利用できるものは、PC（その内部の HDD や SSD）の譲渡や破棄に伴うデータの抹消技術（データの復旧が困難な状態にする技術）である[1]。

[1] 「抹消」については 2.1 節を参照のこと。

例えば、NIST 800-88 Rev.1[22]の 2.5 節では、Clear、Purge、Destroy に大別されている[2]。証拠保全媒体として利用することを考えると、Destroy （破壊）を除くことになる。

2. 国内の動向

媒体をクリーンにするための技術として流用できるものとして、PC（その内部の HDD や SSD）の譲渡や破棄に伴うデータの抹消技術がある。例えば多くの PC では、破棄に伴う情報漏えい防止の観点等から、内蔵 HDD 内のデータ抹消方法等があらかじめ提供されている。また、譲渡や破棄を想定した市販の抹消ソフトも複数ある。本章では、

- 特定非営利活動法人デジタル・フォレンジック研究会（以下 IDF）
- 一般社団法人情報機器リユース・リサイクル協会（以下 RITEA）
- 一般社団法人 電子情報技術産業協会（以下 JEITA）

の動向を中心に述べる。

2.1. 府省庁対策基準策定のためのガイドラインにおける記述

内閣官房情報セキュリティセンターから、2014 年 5 月 19 日に「府省庁対策基準策定のためのガイドライン」[37]が公開されている。第 3 部「情報の取り扱い」（p.75）には、電磁的記録媒体に記録されている情報を抹消するための方法について以下のように記述されている。

> 電磁的記録媒体に記録されている情報を抹消するための方法としては、例えば、次の方法が挙げられる。
> ・ データ抹消ソフトウェア（もとのデータに異なるランダムなデータを複数回上書きすることでデータを抹消するソフトウェア）によりファイルを抹消する方法
> ・ ハードディスクを消磁装置に入れてディスク内の全てのデータを抹消する方法
> ・ 媒体を物理的に破壊する方法

2.2. IDF の出版物における記述

IDF は、「法執行機関を始めとして、他の官公庁、民間企業において「デジタル・フォレンジック」の普及・促進を図り健全な IT 社会の実現に貢献する」ために設立された組織である（[39]の一部より）。

IDF ではデジタル・フォレンジック事典を過去 2 回（2006 年[33]と 2014 年[34]）出版している。2006 年に出版されたデジタル・フォレンジック事典[33]の 9.2.1 節では、ハードディスク消去ツールが紹介されており、

---

[2] 2006 年に発行された NIST 800-88[21]の 2.4 節の表 2-1 では、Disposal、Clearing、Purging、Destroying として言及されている。

> コピー先となるハードディスクにデータが書かれていたならば、その残留データが証拠となるデータを汚染し、証拠性を失う可能性がある

との記述がある。

2014 年に出版されたデジタル・フォレンジック事典[34]では、消去ツールの紹介はなされていないが、付録 3「データ復旧と証拠保全」で沼田が HDD のリードエラーや不良セクタ（バッドセクタ）等が与える証拠保全への影響等を述べている。

また、IDF は 2010 年に証拠保全ガイドラインを公開し、2013 年 9 月には第 3 版[28]が、2015 年 3 月には第 4 版[29]が公開された。いずれの版でも 1.3 節で、インシデントレスポンス時に必要と考えられる資機材等の準備の一つとして、フォーマット済みのクリーンな媒体（ハードディスク、CD-R 等の各種メディア）の準備を求めている。また、いずれも 4.1 節で複製（コピー）先に用いる媒体のチェックと無データ状態に関して言及している。

2.3. RITEA のガイドライン

RITEA は、「情報機器リユース・リサイクル（再資源化）に係わる良質な事業者の育成、また、情報機器に関係する各事業者の協力による良質なリユース情報機器の認知度向上及び普及活動により我が国リユース情報機器市場の発展を図ること、また、情報機器のリサイクル推進による我が国への貢献を目的とする」組織である[38]。なお、証拠保全のためのクリーンな媒体の準備という観点からはリサイクルではなく、リユースに関する技術が重要である。「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」[32]内のデータ抹消方法に関する記述を以下に示す。

> 情報機器の HDD 内に記録されたデータを消去する方法としては、専用装置で電気的・磁気的に塗りつぶしを行う方法や HDD を物理的に破壊する方法もありますが、情報機器の長寿命化や循環型社会実現に貢献する「リユース」の見地からは、「専用消去ソフトウェアによる HDD データ消去方法」が望ましいと考えます。
>
> 但し、今日では、OS 等の再セットアップ（リカバリ）データを HDD 内の特別な領域に保存している情報機器も増加しており、HDD 全領域をデータ消去するという定義は、必ずしも適切ではなくなっていることへの配慮が必要と考えます。
>
> また、HDD のデータ領域に対して、特定しない英数字によるパターン等で 1 回以上の書き込みを行い、元々あったデータの塗り潰し消去を行えば、現状ではデータの復旧は困難と考えます。
>
> 専用 HDD データ消去ソフトウェアとしては、以下の特徴を満たすべきと考えます。
>
> HDD のデータ領域に特定しない英数字によるパターン等で 1 回以上書き込みを行い（OS の再セットアップ（リカバリ）領域等を除く）、元々あったデータの塗り潰し消去を行うこと。

作業終了後に作業が正常に終了したか、エラーが発生したかのログ情報を記録に残すことができること。

なお、RITEA では、情報機器 3R&データ消去ガイドブック[30]を 2012 年に出版している。概要編、法令編、実務編から構成されている。そこには、PC 内ハードディスクドライブやスマートフォンのデータ消去ソフトウェアの資格に関する記載がある。なお[30]は 2014 年に改訂版[31]が出版されており、やはり概要編、法令編、実務編から構成されている。また、タブレットに関する記述等が追加されている。また、いずれの版でも情報機器のデータ消去作業について章が設けられている。

2.4. JEITA のガイドライン

JEITA は、「電子機器、電子部品の健全な生産、貿易及び消費の増進を図ることにより、電子情報技術産業の総合的な発展に資し、わが国経済の発展と文化の興隆に寄与することを目的とした業界団体」である[27]。「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」[36] 内のデータ消去方法に関する記述を以下に示す。

パソコンの HDD 上に記録されたデータを消去する現在有効な方法としては、下記の方法があります。
①専用ソフトにて HDD 全体を固定パターン等にて一回以上、上書きすることにより
塗りつぶしてデータを消す方法
②専用装置にて電気的、磁気的に塗りつぶす方法
（場合によっては物理的な破壊を伴う場合もある）
③HDD に対して物理的に破壊する方法

3. 海外の動向

海外の動向は、[2][4]に詳しい。ここでは、[2][4]と重複するが National Institute of Standards and Technology（以下 NIST）のデータ抹消に関するガイドライン SP800-88[21]および SP800-88 Rev.1 [22]や、Center for Magnetic Recording Research（CMRR）[3]からの情報について言及する。CMRR に所属する研究者の論文等については 4 章で扱う。

3.1. NIST の SP800-88 について

National Institute of Standards and Technology（NIST） は、データ抹消に関するガイドラインとして、NIST Special Publication 800-88 Guidelines for Media Sanitization[21]

[3] 2015 年 7 月より Center for Memory and Recording Research

を 2006 年に、同 Rev.1[22]を 2014 年に公開している。なお、2006 年の版[21]の和訳[35]が公開されている。

3.1.1. SP800-88（2006 年）について

NIST の SP800-88[21]はデータ抹消に関するガイドラインである。2.4 節の表 2-1 において、抹消の方法は Disposal、Cleaning、Purging、Destroying の 4 つに大別されている。本報告に関連するのは Cleaning と Purging である。なお 2.3 節では、

> That is、 for ATA disk drives manufactured after 2001 （over 15 GB） clearing by overwriting the media once is adequate to protect the media from both keyboard and laboratory attack。

という記載がある。つまり、2001 年以降に製造された 15GB 以上の ATA ディスクについては上書き抹消を行う場合の上書き回数は 1 回で十分であることが述べられている。また、Purging では、本報告でも取り扱う Secure Erase についても言及されている。NIST の SP800-88[21]の付録 A では、様々なメディア（ATA Hard Drives を含む）に対する（最低限の） 抹消に関する推奨方法が述べられている。HDD の推奨方法としては、上書き抹消に加え、（Enhanced） Secure Erase、消磁機（Degausser）の利用等が挙げられている。

3.1.2. SP800-88 Rev.1（2014 年）について

NIST の SP800-88Rev.1 [22]は SP800-88[21]の改訂版であり、データ抹消に関するガイドラインである。2.5 節において Disposal に関する記述もあるが、抹消の方法は Clean、Purge、Destroy の 3 つに大別されている。本報告に関連するのは Clean と Purge である。2006 年の版と比較して、暗号化（Cryptographic Erase（CE））についてかなり言及していること、SSD 等の新しいメディアにも言及していることが挙げられる。また、SP800-88Rev.1[22]の付録 A では、やはり様々なメディア（ATA Hard Drives や ATA Solid State Drives を含む）に対する（最低限の） 抹消に関する推奨方法が述べられている。HDD や SSD の推奨方法としては、上書き抹消に加え、ATA の Sanitize Device 機能（OVERWRITE EXT、 CRYPTO SCRAMBLE EXT（Cryptographic Erase）、 BLOCK ERASE EXT）や Security 機能（SECURITY ERASE UNIT（本報告で扱う（Enhanced） Secure Erase））等が挙げられている。

また、抹消結果の検証についても 4.7 節で述べられている。例えばアクセス可能な領域を全てゼロ（全ビットを 0）で上書き抹消する場合は、その抹消が正しく行われていることはアクセス可能な領域を読み込み全てゼロであるかを検証すればよい。抹消を行う組織次第だが、ランダムに選んだ一部分の領域の検証についても言及されている。

媒体内の暗号化に関しては 2.6 節に記述されており、考え方を説明する。デバイス側（媒体側）で常に暗号化を行い、暗号化されたデータを保存する。暗号化および復号のための鍵は適切に（例えばデバイス側（媒体側）で適切に）管理する。この鍵のみ（サイズは小さい）を抹消すれば、暗号化されたデータを媒体から取得できたとしても、元データを得ることは現実的な時間では不可能となる。もちろん、鍵の管理が適切になされていること、適切な暗号化 （適切なアルゴリズムの選択を含む）が行われていること、暗号化機能を有効にした後にデータの保存をすること等が条件である。なお、[22]の付録 E にて、デバイス側の抹消に関する実装を確認することの困難性（不可能性）について言及されている。

3.2. Center for Magnetic Recording Research（CMRR）について

カリフォルニア大学の研究機関 Center for Magnetic Recording Research に所属する研究者達が、データ抹消に関連したいくつかの報告を出している[9][10][11]。また、Secure Erase のツールである HDDErase も公開している[4]。

4. 抹消に関する調査・研究動向

国内外の調査・研究動向、「データ消去」分科会の報告等を述べる。これらの報告から、HDD や SSD に対して一切のデータがない無データ状態のものを用意することは困難と考えられる。

4.1. 海外の調査・研究動向

Garfinkel、Shelat は、2003 年の論文 Remembrance of Data Passed: A Study of Disk Sanitization Practices[8]で中古 HDD 内部からかなりの情報を得ることができたことを報告している。その結果を受け、個人や組織等に対してより適切なデータ抹消に関する必要性や重要性を述べている。

Hughes、 Coughlin は、2007 年の論文 Tutorial on Disk Drive Data Sanitization[10]で HDD の抹消手法に要する時間や特徴を示している。同等のことは、次節で紹介する[11]でも述べられている。上書き抹消の回数を増やすことについての効率や効果にも言及している。また、[10]には以下の記述もある。

> The U.S. National Security Agency published an Information Assurance Approval of single pass overwrite、 after technical testing at CMRR showed that multiple on-track overwrite passes gave no additional erasure。

Hughes、Coughlin、Commins は 2009 年の論文 Disposal of Disk and Tape Data by Secure

[4] HDDErase については、CMRR ではサポートを終了している模様[23]。

Sanitization[11]において、表 1 に示す 5 つの方法を用い、抹消の速さ（100GB のデータ抹消について評価）、またそのセキュリティレベルの高さをそれぞれ分類している。

表 1[11]に示されている抹消方法とその特徴

	方法	所要時間	セキュリティ
1	OS 上でファイルを削除	数分	Low
2	DoD5220（米国国防総省方式）	半日程度	Medium
3	Secure Erase	30 分～3 時間	High
4	Enhanced Secure Erase	数ミリ秒	High
5	物理破壊又は磁気破壊	数秒～数分	Highest

これらの方法に対する安全性については以下のようにコメントを付している。まず、OS 上でファイルを削除する方法 1 は、実際のデータは完全に消えてはおらず、市販の復元ソフトで復元可能である。方法 2 では、3 回の上書きと 1 回の検証（verify）を行う DoD5220（米国国防総省方式）を想定しているが、不良セクタの発生等により再割り当てされた領域等は抹消されない可能性がある。（Enhanced）Secure Erase は広範囲のデータを抹消可能である（[1][2][3][24]も参照のこと）。なお、物理破壊又は磁気破壊を行った場合、そのセキュリティレベルは最も高いが、証拠保全先媒体としては利用できない。

Wei、 Grupp、 Spada、 Swanson は 2011 年の論文 Reliably Erasing Data From Flash-Based Solid State Drives[19]において、SSD に対する上書き抹消の有効性評価結果を示している。調査対象とした SSD によっては、1 回の上書き抹消では不十分であることが述べられている。また、多くの場合、2 回の上書きにより、ディスクの抹消が達成されたと述べられている（[2]も参考にされたい）。

4.2. 国内の調査・研究動向

佐藤、芦野、上原、佐々木は 2006 年にネットオークションに出品された PC のデータの抹消状況に関するアンケート結果を報告している[17]。また、実際に購入して復元実験も試みている。本分科会で実施したデータ抹消に関する実態調査[5]はこの研究の影響を大きく受けている。

林、佐々木は 2013 年に HDD 上で削除したファイルの復元可能性について[12]、山前、小林、上原、佐々木は 2015 年に SSD 上で消去したファイルの復元可能性について[18]、各々実験結果を報告している。[18]では、まず PC 上のファイルを削除（更にごみ箱を空に）し、通常通り使用した後に復元ソフトで当該ファイルの復元可能性を評価している。更に、SSD の Trim 機能の設定の ON/OFF により、復元可能性に差異が生じたことが報告されている。

前田は、2015 年にデジタル・フォレンジックの観点から、HDD と SSD のデータ復元の差異について報告している[14]。SSD については、アーキテクチャ、および予備の領域に関する調査結果も報告している。更に、前田と湯淺は 2015 年に Over Provisioned Capacity と呼ばれる予備の領域からの新たなデータ抽出手法を提案している[15]。

4.3. 「データ消去」分科会からの報告等

下垣内は「データ消去」分科会において 2 度講演[5]している。HDD のデータ領域を 3 つに分類し議論を行い Secure Erase についても言及している。その詳細は[3]を参照のこと。

沼田は 2015 年に開催された「データ消去」分科会（第 11 期第 5 回）で、「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 －」と題して講演している。HDD のデータ消去（上書き消去）と、消去したデータを読み出すことができるとされている方法と可能性について、[10][21]等や Secure Erase 等についても言及しつつ講演している。この講演の一部に加え、SSD の仕組みに関する解説等については[2]を参照のこと。

飯泉は 2015 年に開催された「データ消去」分科会（第 12 期 第 3 回）で、「日本のＰＣリユースにおけるデータ消去」と題して講演している。PC のリユースの現場に即したデータ消去の考え方を、Secure Erase のトピックも交えて講演したものであり、その詳細は[13] を参照のこと。

伊藤は[1]において、PC リユース、PC 廃棄における現状について述べるとともに、Secure Erase についても言及している。

HDD に対するデータ抹消として現時点では、Enhanced Secure Erase を実行した後、全 LBA 領域に対するゼロ（全ビット 0）での上書き抹消を行うことで通常の場合は十分であると考えられる。なお、[2][3]で述べられているように、現時点では Enhanced Secure Erase が最も広範囲のデータを抹消できる。抹消が実行されたことの検証を行うなら全 LBA 領域がゼロであることを、もし許容されるならランダムに選択された一部分の領域がゼロであることを確認すればよい。なお、Enhanced Secure Erase がどのように動作するか、またそもそも対象媒体で提供されているか否かはその製造メーカ・機種・製品に依存することに注意する必要がある。

さて、証拠保全ガイドライン[28][29]では、証拠保全先媒体として一切のデータがない無データ状態のものを用意することを求めている。しかし、[2][3]で述べられているように、上記でも抹消できない領域（以下 PARADAIS[3]）が存在する。下垣内が[3]で述べているように様々なサイバー攻撃に関わることも考えられる領域だが、現状 PARADAIS に対する適切な抹消手段は存在しない。このことから、一度使用された HDD に対し無データ状態を完全に満たすようにデータ抹消を行うことは困難と考えられる。[2]で述べられている

[5] いずれも「データ消去」分科会登録メンバー限定。

ように、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が必要と言わざるを得ない。

SSD については、Over Provisioning のための領域等、膨大で制御困難な領域が存在することが知られている。これらの領域の抹消が困難であることは[19]でも指摘され、現時点でも依然として困難である[2][13]。また、Enhanced Secure Erase がどのように動作するか等についても、HDD の場合と同様の注意が必要である[6]。一度使用された SSD に対し、無データ状態を完全に満たすようにデータ抹消を行うことは HDD と比べて更に難しいと考えられる。

5. 抹消に関する性能評価

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。Hughes 等は 2009 年に 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している[11]。その後、PC 自体の性能は向上しており、かつ HDD や SSD 等の媒体の容量も飛躍的に増大している。SSD は 2009 年頃にはそれほど普及していなかったが、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。これらの媒体のデータ抹消が現実的な時間で可能かどうかを評価した。詳細は[6]を参照のこと。

HDD に対する上書き抹消性能はソフトウェアに大きく依存することが確認できた。現時点で広く普及している I/F（SATA3）を有する評価対象 HDD については、1TB の抹消に最速でも 1 時間 50 分程度を要するものが多かった[7]。（Enhanced）Secure Erase も同程度の時間を要した。

SSD に対する上書き抹消性能もソフトウェアに依存することが確認できた。なお、SSD に対する（Enhanced） Secure Erase は極めて高速であり、1 分以内に終了した。

また、乱数による上書き抹消の場合、乱数の生成方法が抹消時間に大きな影響を与えていることが確認できた。

6. 実態調査

[1][4][5]等により、国内外とも HDD については、DoD や米国国防総省方式のように複数回の上書き抹消を利用している組織が存在することが確認できた。マネジメントの観点からは、データ抹消作業についての抹消ログの取得とログ保存体制は重要と考えられ、必要に応じて抹消作業の体制の強化等（複数人で行う等）も視野に入れる必要があると考えられる。

---

[6] Enhanced Secure Erase の動作に関する言及や、Secure Erase に関する HDD と SSD の差等については、NIST SP800-88 rev.1 [22]における記述（p.33 や p.37）も参考にされたい。

[7] データ消去分科会では、抹消時間があまりに短すぎると、ツール自体の正当性を疑う必要があるとの意見も出された。

6.1. 企業におけるデータ抹消に関する実態調査

IDF「データ消去」分科会で、企業におけるデータ抹消に関する実態を明らかにする目的で、実態調査を企画した。2015 年 3 月 23 日から 2015 年 5 月 22 日まで、IDF のホームページ上で匿名の WEB アンケートとして実施した。このアンケートは[17]を参考にしながら、データの抹消に関する規定状況等を追加したものである。アンケートで得られた回答数は 59 件であった。アンケート結果の詳細は[5]を参照のこと。

アンケートに対する全ての回答で、不要になったまたは再利用のための PC の HDD のデータを、自社もしくは委託先の事業者にて何らかの手段で抹消していた。また、回答 26 件のうち 17 件が、抹消方式の 1 つとして米国国防総省方式を用いていた。次点は 0 で 1 回抹消するというものであった。また、物理破壊装置で破壊するとの回答も少なくなく、このことは[1]で述べられている現状とも合致する。回答 59 件のうち 41 件が、抹消方法に関する情報収集を全く行っていないこともわかった。

なお、IDF のホームページ上でのアンケートであったこと、アナウンスは IDF や「データ消去」分科会メンバーにより行われたことから、アンケート回答者の分布（フォレンジックやデータ抹消についてかなり理解が深い可能性が高い）については留意する必要がある。

6.2. 米国の州政府・大学等における抹消に関する実態調査

瀧澤は[4]において、リサイクルやリユースの市場拡大とそれらに関する脅威について述べた後、データ抹消規格およびその広がりについて報告している。更に公開されている情報セキュリティポリシー等に記載されている情報を元にデータ抹消（廃棄に伴う場合もある）に関する組織の方針や抹消の実態等の調査結果も報告している。その範囲は、連邦行政府、州政府（30 の州政府でデータ消去規定が確認された）や大学におよぶ。結果の詳細は[4]を参照のこと。DoD 準拠法、NIST 準拠法、Secure Erase 等を利用している機関が多く、州法で規定されている例（上書き抹消回数等）も確認された。上書き抹消は 1 回で十分と考えられるが、3 回の上書きを求める機関も見受けられた。

NIST SP800-88（[21][22]）等では、各媒体に含まれる情報の機密度等のリスク評価に基づくべきであること等が述べられ、データ消去に関する意思決定フローの例も示されている。また、近年は作業の検証および記録が重視される傾向にあることも述べている[4]。フォレンジックのためにクリーンな媒体の準備を行う場合、証拠として機能する必要があることを考慮した上で、抹消方法を決定する際の参考になると考えられる。

6.3. セキュリティマネジメントとデータ抹消

山口は[7]で、セキュリティマネジメントとデータ抹消の関係について報告している。代表的なガイドラインには、それぞれ媒体廃棄時の要求事項があるものの、具体的に手法を規定したものは少ないことが示されている。ISO27001/ISO27002、カードセキュリティ

のガイドライン PCIDSS、更にクラウド環境におけるデータ抹消に関する記載についての報告がなされている。また、国内のいくつかの機関（RITEA と IPA）や高等教育機関（大学等）で外部公開されている Web サイトから確認できた情報についてもまとめている。

7. おわりに

デジタル・フォレンジック研究会「データ消去」分科会は第 11 期（2014 年）に活動を開始した。そして第 11 期および第 12 期の 2 年間にわたる活動を経て、証拠保全のためのクリーンな媒体の準備に関する様々な知見を得ることができた。[1][2][3][4][5][6][7]および本報告により、これらの知見について報告した。

さて、[1][2][3]等で述べられているように HDD や SSD に対する一定以上のレベルでのデータ抹消は現時点では不可能に近い。証拠保全先媒体としての利用を考えると、媒体をクリーンに（無データ状態に）することも重要であるが、証拠として機能するための条件を満たした形でイメージファイルを保存することに注力することも視野に入れるべきと考える。これに関しては、デジタル・フォレンジック研究会「技術」分科会等との連携が必要になると考えている。

また、データ抹消が不可能な領域が存在するということは、そこに重要な情報が残っている可能性や、マルウェア等が潜んでいる可能性を排除できない。そのような領域へのアクセス等も（データ抹消（書き込み等）も重要だが、データの読み込みも）興味深い研究課題と考えている。

参考文献

[1] 伊藤修司，日本の PC リユースにおけるデータ消去について，特定非営利活動法人デジタル・フォレンジック研究会（2016).
https://digitalforensic.jp/wp-content/uploads/2016/02/pc-reuse.pdf

[2] 沼田理，データ抹消に関する米国文書(規格)及び HDD，SSD の技術解説，特定非営利活動法人デジタル・フォレンジック研究会（2016).
https://digitalforensic.jp/wp-content/uploads/2016/02/technical-aspect.pdf

[3] 下垣内太，消去アクセス難易度別にみる HDD のデータ領域 3 分類 ～論理セクタ・代替処理後の不良セクタ・PARADAIS～，特定非営利活動法人デジタル・フォレンジック研究会（2016).
https://digitalforensic.jp/wp-content/uploads/2016/02/3-categories-of-hdd-data.pdf

[4] 瀧澤和子，データ消去に関する海外規格の動向，特定非営利活動法人デジタル・フォレンジック研究会（2016).
https://digitalforensic.jp/wp-content/uploads/2016/02/standards.pdf

[5] 宇野幸治，データ抹消に関する実態調査，特定非営利活動法人デジタル・フォレンジック研究会（2016).
https://digitalforensic.jp/wp-content/uploads/2016/02/survey.pdf

[6] 宇野幸治，土井洋，データ抹消に関する性能評価報告，特定非営利活動法人デジタル・フォレンジック研究会（2016).
https://digitalforensic.jp/wp-content/uploads/2016/02/performance-evaluation-.pdf

[7] 山口大輔，デジタル・フォレンジックの有効性－セキュリティマネジメントからみた PC データ抹消について－，特定非営利活動法人デジタル・フォレンジック研究会（2016).
https://digitalforensic.jp/wp-content/uploads/2016/02/management.pdf

[8] Garfinkel, Shelat, Remembrance of Data Passed: A Study of Disk Sanitization Practices, IEEE Security & Privacy, Vol.1, Issue 1, pp.17-27 (2003)

[9] Hughes, Coughlin, Secure Erase of Disk Drive Data. http://www.tomcoughlin.com/Techpapers/Secure%20Erase%20Article%20for%20IDEMA,%20042502.pdf （2016 年 1 月 31 日確認)

[10] Hughes, Coughlin, Tutorial on Disk Drive Data Sanitization (2007).
http://cmrr.ucsd.edu/people/Hughes/documents/DataSanitizationTutorial.pdf（2016 年 4 月 1 日確認)

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

[12] 林健，佐々木良一，時間経過に着目した HDD のデータ復元に関する実験と解析，コンピュータセキュリティ(CSEC)研究会, 2013-CSEC-60(14) (2013).

[13] 飯泉康一，日本のＰＣリユースにおけるデータ消去，特定非営利活動法人デジタル・フォレンジック研究会，データ消去分科会(第 12 期 第 3 回)講演資料 (2015). https://digitalforensic.jp/2015/09/16/data-12-3/ (2016 年 1 月 31 日確認)

[14] 前田恭幸，NAND フラッシュメモリの SSD と HDD のデータ復元比較～Spare Capacity 及び Over Provisioned Capacity に着目して～，コンピュータセキュリティシンポジウム 2015, 2D2-1 pp.427-434 (2015).

[15] 前田恭幸，湯淺墾道，SSD の Over Provisioned Capacity からのデータ抽出手法，コンピュータセキュリティ(CSEC)研究会, 2015-CSEC-71(12) (2015).

[16] 仲嶋伸明，電子記録媒体のデータ消去ガイドライン，情報の科学と技術 Vol.56, No.12, pp.579-583，情報科学技術協会 (2006).

[17] 佐藤さつき，芦野祐樹，上原哲太郎，佐々木良一，ネットオークションに出品した PC のデータ抹消状況の調査・分析，コンピュータセキュリティ(CSEC)研究会，2006-CSEC-34(10) (2006).

[18] 山前碧，小林裕太，上原哲郎，佐々木良一， SSD 上の抹消ファイルの復元可能性の実験と評価，コンピュータセキュリティ(CSEC)研究会, 2015-CSEC-68(39) (2015).

[19] Wei, Grupp, Spada, Swanson, Reliably Erasing Data From Flash-Based Solid State Drives, Proc. of FAST'11: 9th USENIX Conference on File and Storage Technologies, pp.105-118 (2011).

[20] 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)

[21] Guidelines for Media Sanitization, NIST Special Publication 800-88 (2006).

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

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

[24] Information technology - AT Attachment - Part 102: ATA/APAPI Command Set -2 (ACS-2), ISO/IEC 17760-102:2016 (2016).

[25] 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)

[26] Secure Erase, CMRR, UC San Diego. http://cmrr.ucsd.edu/people/Hughes/ secure-erase.html (2016 年 1 月 31 日確認)

[27] JEITA の活動と組織，一般社団法人 電子情報技術産業協会. http://www.jeita.or.jp/japanese/about/what/index.htm(2016 年 1 月 31 日確認)

[28] 証拠保全ガイドライン第 3 版，特定非営利活動法人デジタル・フォレンジック研究会「技術」分科会ワーキンググループ (2013). https://digitalforensic.jp/2013/09/30/guidelines-3/ (2016 年 1 月 30 日確認)

[29] 証拠保全ガイドライン第 4 版，特定非営利活動法人デジタル・フォレンジック研究会「技術」分科会ワーキンググループ (2015).
https://digitalforensic.jp/2015/03/06/guidelines-4/ (2016 年 1 月 30 日確認)
[30] 情報機器 3R&データ消去ガイドブック，一般社団法人情報機器リユース・リサイクル協会 (2012).
[31] 情報機器 3R&データ消去ガイドブック 改訂版，一般社団法人情報機器リユース・リサイクル協会 (2014).
[32] 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)
[33] デジタル・フォレンジック事典，特定非営利活動法人デジタル・フォレンジック研究会編，日科技連 (2006).
[34] 改訂版デジタル・フォレンジック事典，特定非営利活動法人デジタル・フォレンジック研究会編，日科技連 (2014).
[35] 媒体のサニタイズに関するガイドライン([21]の和訳)，独立行政法人情報処理推進機構及び NRI セキュアテクノロジーズ株式会社 (2009).
https://www.ipa.go.jp/files/000025355.pdf (2016 年 1 月 30 日確認)
[36] 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)
[37] 府省庁対策基準策定のためのガイドライン，内閣官房情報セキュリティセンター (2014).
http://www.nisc.go.jp/active/general/pdf/guide26.pdf (2016 年 3 月 27 日確認)
[38] 目的と事業内容，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/mokuteki.html(2016 年 1 月 31 日確認)
[39] 設立趣旨，特定非営利活動法人デジタル・フォレンジック研究会.
https://digitalforensic.jp/home/idf/syushi/ (2016 年 1 月 31 日確認)

「データ消去」分科会メンバー（所属は 2016 年 4 月現在）※五十音順

氏名	所属名
伊藤　修司	NPOデジタル・フォレンジック研究会 「データ消去」分科会　幹事 (株)アセットアソシエイツ　代表取締役
伊藤　文二	日本ダイレックス(株)ネットワーク技術グループ　開発技術チーム
宇野　幸治	NPOデジタル・フォレンジック研究会 「データ消去」分科会　幹事 情報セキュリティ大学院大学
緒方　健	おがたコンサルティング　代表
笠原　毅彦	桐蔭横浜大学大学院　法学研究科　教授
下垣内　太	大阪データ復旧(株)　代表取締役
砂原　圭太	(株)フォーカスシステムズ　サイバーフォレンジックセンター
瀧澤　和子	早稲田大学商学学術院総合研究所　WBS研究センター　招聘研究員
土井　洋	NPOデジタル・フォレンジック研究会　理事・「データ消去」分科会　主査 情報セキュリティ大学院大学　情報セキュリティ研究科　教授
沼田　理	(株)DD－RESCUE
林　紘一郎	情報セキュリティ大学院大学　情報セキュリティ研究科　教授
平岡　洋介	(株)ラック　サイバー救急センター
舟橋　信	NPOデジタル・フォレンジック研究会　理事 (株)UBIC　取締役
松本　隆	NPOデジタル・フォレンジック研究会　理事 SCSK(株)　セキュリティサービス部　エバンジェリスト
山口　大輔	伊藤忠テクノソリューションズ(株)エンタープライズシステム事業企画室 ビジネスソリューション推進部 エグゼクティブコンサルタント

IDF 事務局メンバー

丸谷　俊博	NPOデジタル・フォレンジック研究会　理事・事務局長
田中　友佳子	NPOデジタル・フォレンジック研究会　事務局員
細谷　美帆	NPOデジタル・フォレンジック研究会　事務局員