

注目されているセキュリティ事故・事件に関する情報 ＜2020年3月版（第32号）＞（選り抜き版）

2020年3月27日
NTTデータ先端技術株式会社
セキュリティ事業本部

情報媒体廃棄方法のあり方

2019年11月に神奈川県庁で使用されていたHDDが、データ消去および廃棄を委託された会社で廃棄処分されずに転売される事件が発生しました。結果としてHDDに記録されていた行政文書が漏えいしたことで、世界的に情報媒体の廃棄方法に注目が集まることとなりました。本記事では、情報廃棄におけるサプライチェーン・リスクのリスクを軽減する方法について解説します。

情報媒体廃棄方法のあり方

1. はじめに

2019年11月に神奈川県庁で使用されていたHDDが、データ消去および廃棄を委託された会社で廃棄処分されずに盗難され、転売される事件が発生しました。

盗難経路は、リース会社がデータ消去および廃棄を委託している会社の社員がデータ消去作業前にHDDを盗みだしたというものでした。盗難に遭ったHDDはデータ消去委託先の会社の社員によりオークションサイトに出品/落札され、落札した方からの申告により事件が発覚しました。

なお、このHDDには、公開情報や個人情報を含む県の内部情報などが記録されていました。

※本事件は本書の記事『IPAから「情報セキュリティ10大脅威 2020」が公開されました』で紹介する「情報セキュリティ 10大脅威 2020」において、内部不正の例として取り上げられています。

2. 神奈川県庁HDD盗難事件のタイムライン

以下に本事件の対応のタイムラインを示します。

日付	内容
2019/11/26	オークションサイトを通じてHDDを購入した方(以下、A氏)から、神奈川県庁に「県の情報と思われる電子データを所持している。確認して欲しい」旨の連絡が入った
2019/11/27	- 神奈川県庁側が電子データに公開情報や個人情報を含む県の内部情報が含まれていることを確認した - A氏の証言によると「購入したHDD(計9台)についてデータ復元の処理を試みたところ、一部のファイルのデータ復元に成功した」とのことであった - 購入したHDDの内の1台がリース会社に返却したHDDのシリアルナンバーと一致しており、神奈川県庁がリース会社にHDDの外部流出について事実確認を指示した
2019/12/5	- リース会社の調査の結果、リース会社がデータ消去および廃棄を委託している会社の社員1名が18台のHDDをデータ消去作業前に盗み出し、オークションサイトに出品し、全て落札されていたことが明らかとなった - 神奈川県庁が、A氏よりHDD(計9台)の返却を受けた
2019/12/6	リース会社がデータ消去および廃棄を委託している会社からリース会社へ、「HDDを盗み出した社員を告発した」「所在が明らかになっていない残りの9台のHDDの回収は警察の捜査にゆだねる」旨の連絡があった
2019/12/21	神奈川県庁が、所在不明となっていたHDD(計9台)を回収した

※リース会社がデータ消去および廃棄を委託している会社の社員は、神奈川県庁のHDD以外にも、2016年から様々な組織のHDDやUSBメモリ、スマートフォンなど7000台超の情報機器をオークションサイトで転売していた

3. 神奈川県庁HDD盗難事件の問題点

神奈川県庁の発表(※)によると、神奈川県庁がリース期間満了により機器をリース会社に返却する場合、リース会社が「データ復旧が不可能とされている方法によりデータ消去作業を行うものとする」とされています。そのため、本事件は神奈川県庁の直接的な不祥事により発生したわけではなく、外部委託における情報セキュリティ上のサプライチェーン・リスクの管理の在り方に問題があり発生したものと考えられます。

※引用：神奈川県：リース契約満了により返却したハードディスクの盗難及び再発防止策等について
<https://www.pref.kanagawa.jp/docs/fz7/cnt/p0273317.html>

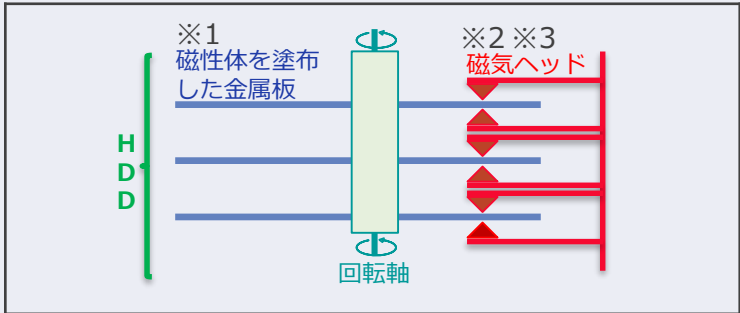
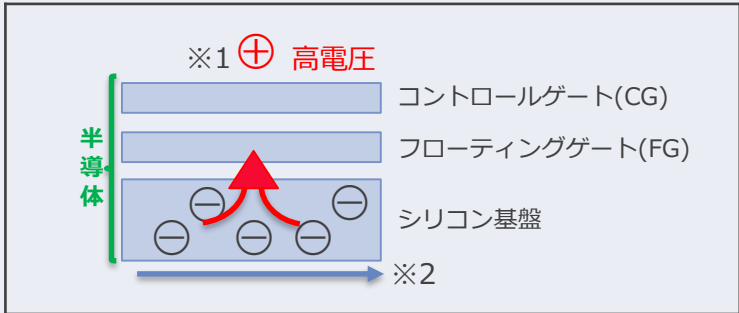
4. 情報媒体におけるデータの扱い方

サプライチェーン・リスクを考えるうえで、まずはHDDなど不揮発性の情報媒体(以下、情報媒体)におけるデータの扱い方を正しく知識として身につける必要があります。そのため、次スライドから以下に示す仕組みについて説明します。

データ記録の仕組み	情報媒体毎のデータ記録の仕組みについて説明します
データ消去の仕組み	主に磁気媒体(HDD)を例に、データ消去の仕組みについて説明します
データ復元の仕組み	主に磁気媒体(HDD)を例に、データ復元の仕組みについて説明します
廃棄方法の種類とデータ復元の可否	情報媒体毎に有効な廃棄方法について説明します。

5. データ記録の仕組み

まずは「データ記録」について説明します。データ記録の仕組みは情報媒体毎に大きく異なります。以下に代表的な情報媒体におけるデータ記録の仕組みを図示します。

情報媒体	磁気媒体	半導体
	HDD	SSD/USBメモリなど
仕組み	磁性体の磁化  ※1 磁性体を塗布した金属板 ※2 ※3 磁気ヘッド HDD 回転軸 ※1:磁性体を塗布した金属板が回転軸に沿って高速回転 ※2:磁気ヘッドが磁性体を磁化してデータを記録 ※3:磁化されたデータを磁気ヘッドが読み取る	電子の移動  ※1 ⊕ 高電圧 半導体 コントロールゲート(CG) フローティングゲート(FG) シリコン基盤 ※2 ※1:CG側で高電圧をかけることにより、シリコン基板上の電子を、電子を貯めたり抜いたりすることのできるFGに移動させデータを記録 ※2:シリコン基板上の電子の量により電流の流れやすさが異なり、その電流の流れやすさでデータを読み取る
	特徴	- 金属板上の僅かな傷でもデータが損なわれる - 磁気ヘッドなどが故障しても記録/読み出しはできなくなるが、金属板が無事であれば、クリーンルームなど特殊環境でデータの読み取りは可能

6. データ消去の仕組み (1/3)

続いて「データ消去」について、磁気媒体を例に説明します。

情報媒体上のデータ記録領域に1つのファイルをデータとして記録する際、必ずしもデータは「磁性体を塗布した金属板」の物理的に連続した箇所書き込まれるわけではありません。非連続箇所にデータを書き込んでも1つのファイルとして認識できるのは、記録した箇所を記した情報をファイルのデータとは別にメタ情報として保持しているためです。

種別	説明
ファイルのメタ情報	ファイルのデータそのものではなく、そのデータを表す属性や関連する情報(※)を記録したデータを指す ※Windows(NTFS)の例： - ファイル名 - 格納先フォルダ - タイムスタンプ(作成日時/更新日時/最終アクセス日時) - ファイル所有者 - “ファイルのデータ”の情報媒体上の配置情報
ファイルのデータ	情報媒体上に場合によっては断片化して記録されるファイルのデータそのものを指す

6. データ消去の仕組み (2/3)

ファイル削除の直後はファイルのメタ情報およびファイルのデータが情報媒体に記録されているため、容易(※1)にファイルとして読み取ることができます。その後別のファイルの情報で上書きされることにより、元々のファイルのデータが情報媒体から存在しなくなります。以下にファイル削除操作前後のファイルのメタ情報およびデータの状態を示します。

状態	削除前	削除直後	削除後①	削除後②	削除後③
	ファイル削除操作直前 (※2)	ファイル削除操作直後 (※3)	メタ情報が 別のデータで上書きされた	ファイルのデータが 別のデータで上書きされた	メタ情報および ファイルのデータが 別のデータで上書きされた
ファイルの メタ情報	ファイルa のメタ情報	ファイルa のメタ情報  削除済み フラグ	ファイルb のメタ情報	ファイルa  削除済み フラグ	ファイルb のメタ情報
ファイルの データ	ファイルa の断片-1 ファイルa の断片-2 ファイルa の断片-3	ファイルa の断片-1 ファイルa の断片-2 ファイルa の断片-3	ファイルa の断片-1 ファイルa の断片-2 ファイルa の断片-3	ファイルc の断片-1 ファイルc の断片-2 ファイルd の断片-1	ファイルc の断片-1 ファイルc の断片-2 ファイルd の断片-1

※1.例：いわゆるMicrosoft Windowsにおける「ごみ箱からもとに戻す操作を行う」など

※2.いわゆるMicrosoft Windowsにおける「ごみ箱」に入った状態も含まれます

※3.いわゆるMicrosoft Windowsにおける「ごみ箱」からも削除した状態を指します

※4.参考：デジタル・フォレンジック研究会：書籍 基礎から学ぶデジタル・フォレンジック

<https://digitalforensic.jp/home/act/products/df-forensic/>

6. データ消去の仕組み (3/3)

先述の通り、ファイルを削除しただけでは情報媒体上にデータが残存するため、ファイルのデータを完全に消去するためには「完全消去」の操作を行う必要があります。完全消去の操作を行うことで、削除済みフラグが立ったデータ領域は別のデータで上書きされ、削除する前のファイルを読み取ることはできなくなります。

状態	削除前	削除直後	完全消去
	ファイル削除操作直前(※1)	ファイル削除操作直後(※2)	完全消去操作後(※3)
ファイルの メタ情報	ファイルa のメタ情報	ファイルa のメタ情報  削除済み フラグ	-
ファイルの データ	ファイルa の断片-1 ファイルa の断片-2 ファイルa の断片-3	ファイルa の断片-1 ファイルa の断片-2 ファイルa の断片-3	-

※1.いわゆるMicrosoft Windowsにおける「ごみ箱」に入った状態も含まれます

※2.いわゆるMicrosoft Windowsにおける「ごみ箱」からも削除した状態を指します

※3.完全消去には、データ領域を固定値で上書きするゼロライト消去や、データ領域を乱数で上書きするランダムライト消去など様々な方法があります

7. データ復元の仕組み (1/3)

続いて「データ復元」について、同様に磁気媒体を例に説明します。

いわゆるMicrosoft Windowsで言うところの「ごみ箱を空にする」操作を行った後など、一般的な方法では読み取れなくなったファイルを読み取る操作のことを「データ復元」と呼び、データ復元用のソフトウェア(※1)を使用することで削除する前のファイルを読み取ることができる可能性があります。(※2)

次のスライドで2種類のデータ復元の方法(復元/カービング)を示します。

※1.データ復元の方法として、データ復元用のソフトウェアを使用する方法以外に、情報媒体上の残留磁気からデータを読み取る方法があるとされています。ただしこの方法は、実現可能性が疑問視されている他、非常に作業に時間を要し、高額な専用の装置が必要なため実施できる環境が限定されます。そのため特別に記すことがない限りは、本書の以降の説明はデータ復元用のソフトウェアによるデータ復元を指します。

※2.データ復元を試みた結果として、削除する前のファイルは読み取れず、メタ情報のみを読み取れる場合がありますが、この場合も注意が必要です。
メタ情報にはファイル名や作成者、タイムスタンプなどの情報が記されます。仮に第三者に知られてはならない情報がファイル名に記されている場合、メタ情報が読み取れただけで思わぬトラブルに発展する可能性があります。

※参考：デジタル・フォレンジック研究会：データ抹消に関する米国文書（規格）及びHDD、SSDの技術解説
<https://digitalforensic.jp/wp-content/uploads/2016/02/technical-aspect.pdf>

7. データ復元の仕組み (2/3)

復元

ファイルのメタ情報をもとに、データ復元の処理を行います。
そのため、ファイル削除直後であればメタ情報とデータが残存しているため、元のファイルを読み取ることができます。

ただし「データ消去の仕組み」における「削除後②」のようにデータが残存しない場合は、元のファイルは読み取ることができません。

一部「データ消去の仕組み」より再掲	状態	削除直後	削除後②-a	削除後②-b
		ファイル削除操作直後	ファイルのデータが別ファイルのデータで上書きされた	
	ファイルのメタ情報	ファイルaのメタ情報  削除済みフラグ	ファイルaのメタ情報  削除済みフラグ	ファイルaのメタ情報  削除済みフラグ
	ファイルのデータ	ファイルaの断片-1 ファイルaの断片-2 ファイルaの断片-3	ファイルcの断片-1 ファイルcの断片-2 ファイルdの断片-1	ファイルaの断片-1 ファイルaの断片-2 ファイルdの断片-1
	データ復元の可否	データが全て残存しているため、元のファイルが読み取れる	データが残存していないため、元のファイルは読み取れない	別のファイルと結合された不完全な状態の元のファイルが読み取れる(※)

※画像ファイルなどは、全てのデータが揃っていないくとも部分的にファイルとして開くことができるため、画像の一部を確認することができる場合があります。

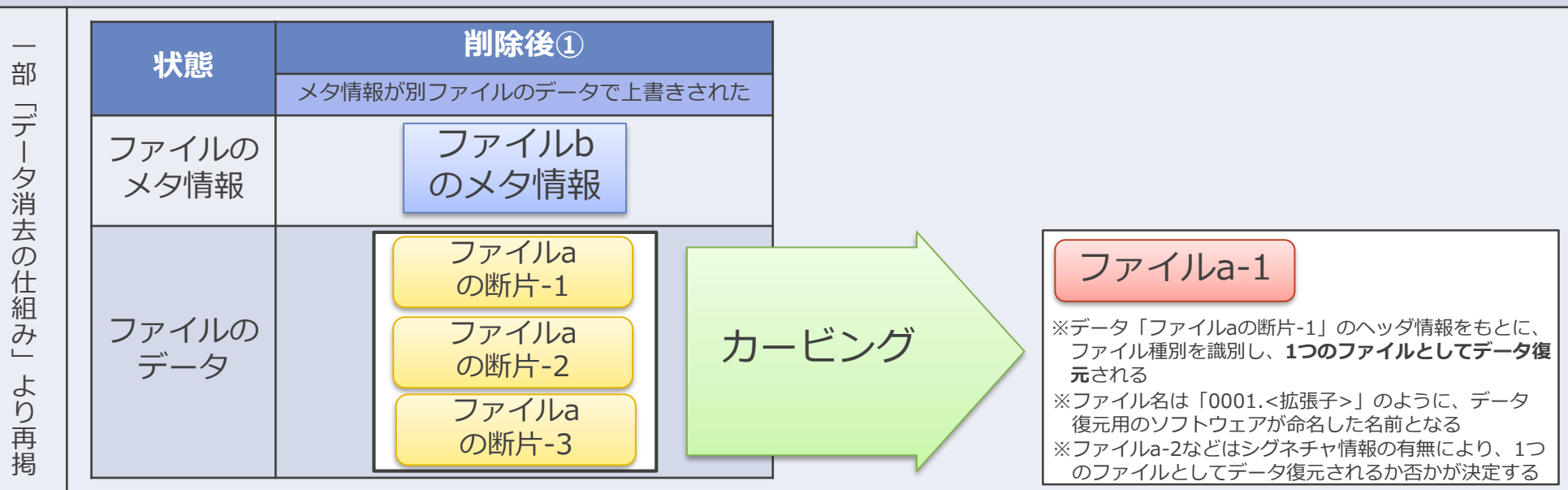
※参考：デジタル・フォレンジック研究会：書籍 基礎から学ぶデジタル・フォレンジック

<https://digitalforensic.jp/home/act/products/df-forensic/>

7. データ復元の仕組み (3/3)

カービング

ファイルのメタ情報に頼らず、データ本体を直接調査しデータ復元の処理を行います。
多くの場合、ファイルには種類を識別するための特徴となるヘッダ/フッタや構造情報が含まれており、シグネチャ情報と呼ばれます。カービングではデータに記録されたシグネチャ情報をもとに、データ復元を試みます。
メタ情報は失われているため、原則削除する前の1つの完全なファイルとしてデータ復元をすることはできません。
(※1)そのため、仮にデータ復元ができたとしても、実行ファイルなどは不完全な状態であるため開くことができません。しかし一部の種類のファイル(例：JPEGファイル)などは、全てのデータが揃っていなくとも、ファイルの内容の一部を確認することができる場合があります。
またメタ情報が失われているため、データ復元を行っても元のファイル名にはなりません。



※1.データサイズが著しく小さいなど、「磁性体を塗布した金属板」の物理的に連続した箇所にデータが書き込まれているような特殊なケースにおいて1つのファイルとしてデータ復元が可能な場合があります。ただしこの場合においても、メタ情報が失われているためファイル名などはもとに戻りません。

※2.参考：デジタル・フォレンジック研究会：書籍 基礎から学ぶデジタル・フォレンジック

<https://digitalforensic.jp/home/act/products/df-forensic/>

8. 廃棄方法の種類とデータ復元の可否

続いて代表的な情報媒体の「廃棄方法」を以下に示します。「破壊」と「読取不可」の2種類を組み合わせることでより高い効果が得られます。

廃棄方法			磁気媒体	半導体
破壊	破砕	破片が一定の大きさ以下になるまで物理的に破壊します。 どの情報媒体においても通用する廃棄方法です。	○	○
	穴あけ /折り曲げ	情報媒体に穴をあけ、もしくは折り曲げて破壊します。 半導体の場合はメモリチップ部分を確実に破壊することが重要です。	○	○
	消磁	強磁場を印加して磁気を消し去ります。 磁気媒体に対しては有効ですが、その他の媒体には効果はありません。	○	×
	溶解	溶解して破壊します。 どの情報媒体においても通用する廃棄方法です。 ただし溶解後の金属塊の処分方法に難があります。	○	○
読取不可	上書き (完全消去)	完全消去の方法でデータを上書きし、読み取れないようにします。	○	○
	暗号鍵 の破棄	情報媒体の利用開始時にドライブを暗号化し、情報媒体を廃棄する際に暗号鍵を破棄します。(※1)(※2)	○	○

※1.ドライブを暗号化する方法：例) Microsoft Windows BitLocker

※2.データを暗号化するタイミングは、情報媒体を廃棄する直前ではなく、情報媒体を使用している時から、できれば媒体全体を暗号化し使用することをお勧めします。これにより、情報媒体使用中に不意に盗難に遭っても第三者にデータを盗み見られることを防止することができます。

凡例)

○：データ復元処理でデータを読み出せる可能性は限りなく低い

×：データ復元処理でデータを読み出せる可能性がある

9. 産業廃棄物処分業者に委託する際の注意点

ここまでのスライドで技術的な側面から、情報媒体におけるデータ記録の仕組みについて説明しました。以降は運用的な側面から、神奈川県庁と同様の事件を防ぐためにとるべき対応について説明します。

データの廃棄を委託する業者に情報媒体を受け渡す前に、実施するべき対応は以下であると考えられます。

1 情報媒体をリース会社に返却しなくてよい契約を締結する

リース会社に情報媒体を返却する前提の契約となっている場合、「廃棄方法の種類とデータ復元の可否」で示した「破壊」の処理を行うことはできません。最終的に廃棄処分を委託する場合においても、自身で「破壊」していれば、「読取不可」の処理を失敗または実施し忘れたとしても漏えいのリスクは軽減できます。

2 廃棄のための対処を行ったうえで、情報媒体を委託先に引き渡す

「廃棄方法の種類とデータ復元の可否」に示すいずれかの対処(※1)を実施し、情報媒体から情報が読み取れない状態となっていれば、万が一廃棄処分の委託先に不手際があったとしても実被害は防ぐことができます。

3 サプライチェーン・リスクを軽減することを考慮した契約条件を検討し、締結する

外部委託を伴う業務における情報セキュリティ上のサプライチェーン・リスクの管理については、手引書(※2)がNISC(内閣サイバーセキュリティセンター)より発刊されています。本手引書における要点は以下の通りです。

- | | |
|---|---|
| ① | サプライチェーン・リスク対策計画について委託先と合意する |
| ② | 委託事業の実施において、サプライチェーン・リスクの対策要件を遵守していることを確認する |
| ③ | 必要に応じて委託先の監査を行う |

※1.「○」表記の対処をお勧めします。

※2.NISC：外部委託等における情報セキュリティ上のサプライチェーン・リスク対応のための仕様書策定手引書

<https://www.nisc.go.jp/conference/cs/taisaku/ciso/dai02/pdf/02shiryou0303.pdf>

10. まとめ

神奈川県警の事件は、外部委託における情報セキュリティ上のサプライチェーン・リスクの管理の在り方が問われる事件でした。

特に情報廃棄におけるサプライチェーン・リスクのリスクを軽減するためには、ファイル削除操作を行っても情報媒体に電子データが残存している可能性を認識し、「産業廃棄物処分業者に委託する際の注意点」に示すような産業廃棄物処分業者に委託する前に取るべき対応を適切に実施することが求められます。

11. 参考URL

- 神奈川県：リース契約満了により返却したハードディスクの盗難及び再発防止策等について
<https://www.pref.kanagawa.jp/docs/fz7/cnt/p0273317.html>
- NISC：外部委託等における情報セキュリティ上のサプライチェーン・リスク対応のための仕様書策定手引書
<https://www.nisc.go.jp/conference/cs/taisaku/ciso/dai02/pdf/02shiryou0303.pdf>
- デジタル・フォレンジック研究会：書籍 基礎から学ぶデジタル・フォレンジック
<https://digitalforensic.jp/home/act/products/df-forensic/>
- デジタル・フォレンジック研究会：データ抹消に関する米国文書（規格）及びHDD、SSDの技術解説
<https://digitalforensic.jp/wp-content/uploads/2016/02/technical-aspect.pdf>
- JEITA：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ガイドライン
https://home.jeita.or.jp/page_file/20181025154114_OcyNEMuIAs.pdf
- CSAT：データ消去証明 ガイドブック
https://www.csaj.jp/documents/NEWS/committee/datadelete/datadelete_guidebook_20170614.pdf
- ADP SECURITY MANUAL
<https://biotech.law.lsu.edu/blaw/dodd/corres/pdf2/p520028m.pdf>
- TIME&SPACE：ただいま超絶進化中！『フラッシュメモリ』の仕組み、教えます
<https://time-space.kddi.com/ict-keywords/kaisetsu/20160906/>
- リ・バース株式会社：SSDデータ消去について
<https://www.erazer.jp/q-a-1/q-a-ssd/>

