

ADECデータ適正消去実行証明協議会
消去技術認証基準委員会

データ消去技術 ガイドブック

第 2.3 版



2022 年 6 月

目次

はじめに	- 2 -
第1章 ガイドブック概要	- 4 -
第2章 データ消去について	- 5 -
第3章 データ消去対象の現状	- 8 -
第4章 データ(情報)の特性・種別ごとの消去方式の選択	- 9 -
第5章 記憶媒体のデータ抹消 (NIST SP800-88Rev.1)	- 11 -
第6章 ISMS (ISO/IEC27001) と NIST SP800-88	- 21 -
第7章 ソフトウェアについて	- 22 -
第8章 作業環境について	- 23 -
第9章 証明書について	- 23 -
第10章 証明書の技術と運営について	- 24 -
第11章 データ消去証明書の発行プロセス	- 29 -
第12章 まとめ	- 31 -
第13章 参考情報	- 32 -
協力団体・作成者・監修者	- 34 -

はじめに

昨今、日本経済成長の課題として取り上げられている少子高齢化の到来を目前に、官公庁及び企業において生産性や国民の利便性を向上させることが急務となっており、「働き方改革」は政府の重要政策のひとつに位置づけられていて、多様な働き方を可能にする社会を目指しています。その中で、世界における市場経済の急速な進展に対し資源の乏しい日本においては、IT 機器・技術を活用した新しいビジネスモデルの構築が必要不可欠となっています。

また、同時にモバイル端末等の急速な普及に加え、クラウドや行政の新しいインフラやサービスの安全性を担保するための関連法制度整備の課題は益々多くなってきています。一方、経済社会における情報化の急激な進展は、個人情報漏えいの危険も隣り合わせであります。情報漏えいによる被害が大きくなれば、成長の大きな阻害要因となってしまいます。今まで、情報セキュリティとして外部からの侵入を防衛すべく、あらゆる対策が施されてきました。

廃棄やリユース目的で販売された記憶媒体からのデータ流出は、悪用された事実によって初めて漏えいを把握することが大多数を占めています。2019 年末に発生した、某県庁で個人情報や機密情報を含む行政文書が保存されていた HDD 等の記憶媒体が転売されていた事件が報道で判明いたしました。データの消去・処分を専門会社に委託することは一般的に行われており、この事件のような情報漏洩を防ぐために、事業者には十分な対策が望まれる。廃棄の在り方について一般的にも注目を集めるようになって参りました。これに伴い、昨今、データ消去の業界では消去ランクに応じた消去方法が認知され、「どのランクのデータ消去を行われているか」を廃棄ルールで定め、消去業務を担う企業側で公表することが増えつつあります。また、利用者のデータを預かって管理しているデータセンターや、クラウドサービス提供している事業者が保管しているデータの消去は、論理的な消去のみであり、物理ドライブの消去に対する規定はありませんでしたが、総務省が地方自治体等に向けて公開する「地方公共団体における情報セキュリティポリシーに関するガイドライン」では取り扱うデータの機密性に依拠して消去ランクに定めることが推奨されることになりました。

このようなことから、データの消去を必要とする側が消去の実際状況を正しく把握することが必要となり、法執行機関を始めとして、他の官公庁、民間企業における「データ消去」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、一般社団法人コンピュータソフトウェア協会内に「データ適正消去実行証明協議会」を設立し、最新のデータ記憶媒体に合わせた消去証明の法整備を目指して、ガイドブックを策定いたしております。デジタルデバイスに内蔵された状態のハードディスクドライブ（以下、HDD と表記する）／ソリッドステートドライブ（以下、SSD と表記する）および、サーバー機器などシステム機器から取り外された状態の HDD/SSD について規定策定を行います。さらに、スマー

トフォン/タブレット端末、データセンター、IoT デバイス機器、クラウド上のデータについても議論を続けていきます。

データ消去における情報漏えい事件事例

2019年12月6日、神奈川県庁において、個人情報や機密情報を含む行政文書が保存されていた HDD 等の記憶媒体が転売されていたことが報道で判明いたしました。リース契約満了にともないリース会社に HDD を含む機器を返却した際、その機器の廃棄処分をリース会社よりデータ消去専門会社に委託していたが、この会社の作業者は廃棄処分を行わず、これら機器を持ち出しオークションサイトで転売しており入手した人がデータ復元ソフトを使用したところデータが復旧され漏洩しました。神奈川県庁が契約しているリース会社との契約では、「消去証明書」を送付する取り決めされていましたが、消去や廃棄を証明するエビデンスが提出されていませんでした。また、神奈川県庁がリース会社に返却する際 HDD は「初期化（フォーマット）」したのみで、データ復元可能な状態でした。

2017年2月23日、岐阜県美濃加茂市教育委員会は市内の中学校で使用され、業者に廃棄処分を委託した PC の内蔵 HDD1 台がインターネットのオークションで落札され、HDD に生徒ら約 750 人分の名前のデータが残っていたと発表した。流出経路を調べ損害賠償請求も検討している。廃棄処分を請け負ったのは学校教育向け情報システムを取り扱う名古屋市の企業。取材に対し、学校から引き取ったパソコンは複数の産廃業者に破壊処理を委託したが、このうちの 1 業者が HDD を有価物として破壊せず、HDD がオークションにかけられた可能性があるとも明らかにした。

出典元：美濃加茂市教育委員会 ホームページ

2008年6月、岩手県生物工学研究所のリース契約満了の PC の一部がインターネットオークションで無断転売され、流出していたことが発覚。リース元は仙台にある廃棄物処理業者に、データ消去を条件に回収を依頼したが実際には消去をしないまま無断で 25 台をインターネットオークションに出品。

出典元：ITPro 廃棄 PC の未消去データに潜んでいた情報流出のリスク

※本報告書に掲載されているすべての会社名、商品名、サービス名等は、該当する各社の商標又は登録商標です。本解説書中では、™ ® ©表記を省略しています。

第1章 ガイドブック概要

目的：

機密データの抹消に関する高い信頼性を社会的に実現するために、PC、スマートフォン、タブレット等（クライアント端末）の廃棄ならびにリユースにおけるデータの適正な抹消を行い、その事実を第三者機関として電子署名を有する証明書を発行するにあたり、業界標準とすべきガイドラインの公開

実施主体：データ適正消去実行証明協議会

実施方法：

現時点において最も進んでいる NIST（アメリカ国立標準技術研究所）の SP800-88Rev.1 に記載されている、米国政府・行政機関向けの電磁記憶媒体に対するデータ抹消の技術的な観点及び判断基準を、一般社会を対象として適用する場合のガイドラインとすることを目的として解説する

第2章 データ消去について

1) データ消去の必要性

PC、サーバー、スマートフォンを含んだIoT機器のIT資産の多くには、機密データが記録されており、このデータを保護することが重要な課題となっています。また、今後は、ビッグデータの活用が普及することにより、爆発的なデータ量の増加が見込まれます。それらの機器に記録されているデータの漏えいや流出により、第三者にデータが閲覧され悪用されることは、情報社会に於ける大きな問題となっています。正しい規定に基づき、完全かつ安全に機密情報の管理を行わなければ、情報漏えいの恐れ、さらには漏えいによる多大な損害を受ける可能性があります。

個人情報保護法等の法令や、多数の厳密な業界基準および政府規制により、企業の持つ機密情報を不正アクセスから守るために適切な手段を取ることが要求されました。そのため組織は、情報漏えいを防ぐために講じている手段を証明するための記録を残す環境を持つことを求められています。記録をもって証明を行うことを法令化し民事および刑事責任のみならず、財務責務、組織の社会的評判への影響という、取り返しのつかない損害を被らないように整備することが急務となっております。しかしながら、リユースや廃棄するPCに対しては、詳細かつ実効的な手順を定めた法令・規定はなく、組織の判断に任せられています。IT犯罪における電磁的証拠の検証＝デジタル・フォレンジックという点からは好ましいことであると言うことは出来ませんが、リユースや廃棄を行う立場からみると、大きなリスクとなっていて、正しい判断基準と処置方法が広く認識されているとは言い難い現状です。

2) 日本の各団体における消去への取り組み

現在公表されている主なものを以下に紹介します。

- ISO/IEC27001:2013 規格 A.11.2.7 (装置のセキュリティを保った処分又は再利用)

記憶媒体を内蔵した全ての装置は、処分又は再利用する前に、全ての取扱いに慎重を要するデータ及びライセンス供与されたソフトウェアを消去していること、又はセキュリティを保って上書きしていることを確実にするために、検証しなければならない。

- ISO/IEC27002:2013 規格 11.2.7

装置は、処分又は再利用する前に、記憶媒体が内蔵されているか否かを確かめるために検証することが望ましい。秘密情報又は著作権のある情報を格納した記憶媒体は、物理的に破壊することが望ましく、又はその情報を破壊、消去若しくは上書きすることが望ましい。消去又は上書きには、標準的な消去又は初期化の機能を利用するよりも、元の情報を媒体から取り出せなくする技術を利用することが望ましい。

出典：ISO/IEC27002:2013

- PCIDSS

電子媒体上のカード会員データが、安全な削除に関して業界が承認した標準に従った安全なワイププログラムによって、またはそれ以外の場合は媒体の物理的な破壊によって、回復不能になっていることを確認する。

出典：PCIDSS(PCI Data security council)

- 教育関係の情報機器取り扱いのガイドライン

第四十八条 1. 教職員等は、電磁的記録媒体に保存された情報が職務上不要となった場合は、速やかに情報を消去すること。2. 教職員等は、電磁的記録媒体を廃棄する場合には、当該記録媒体内に情報が残留した状態とならないよう、全ての情報を復元できないように抹消すること。3. 教職員等は、要機密情報である書面を廃棄する場合には、復元が困難な状態にすること。

出典：C2101 情報機器ガイドライン（国立情報学研究所）

- RITEA（一般社団法人 情報機器 リユース・リサイクル協会）

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。

出典：「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」

- IPA（独立行政法人 情報処理推進機構）

「企業組織における最低限の情報セキュリティ対策のしおり」で、PC 廃棄の際の手順として、確認する手法を記載している。「公開重要情報の入った PC・記憶媒体を廃棄する場合は、消去ソフトを利用したり、業者に消去を依頼したりするなどのように、電子データが読めなくなるような処理をしていますか？」

出典：IPA「企業組織における最低限の情報セキュリティ対策のしおり」

- 一般社団法人電子情報技術産業協会（JEITA）の「PC の廃棄・譲渡時における HDD 上のデータ消去に関する推奨方法について

PC の ディスクの状況	データ消去方法例
PC とディスクが稼働する場合	<ul style="list-style-type: none"> ・専用ソフトにてデータ消去 ・専用装置にてデータ消去 ・ディスクを物理的に破壊
PC 本体は稼働しないが、ディスクは稼働する場合	<ul style="list-style-type: none"> ・稼働する PC に ディスク を接続し専用ソフトにてデータ消去 ・専用装置にてデータ消去

	・ディスクを物理的に破壊
ディスクが稼働しない場合 ・ディスクを物理的に破壊	・ディスクを物理的に破壊

- IDF 研究会（特定非営利活動法人デジタル・フォレンジック研究会）

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。しかし、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ている。

- 内閣官房情報セキュリティセンター

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」が公開されている。第3部「情報の取り扱い」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

第3章 データ消去対象の現状

現在殆どの業務の中で PC が使用されており、デスクトップ型からノートブック型やタブレット型と業務形態に合わせたタイプの PC が使用されています。

以前は、事務所内ではデスクトップ型を使用し、外出時にはノート型やタブレット型を使用することがありましたが、ノート型やタブレット型 PC の高性能化や大画面化、薄型軽量化により、事務所内から外出時まで、1つの PC で業務を行うことが多くなっています。

このような1つの PC で多くの業務を行えるようになったことと、PC 内蔵の記憶媒体の大容量化により、PC の中には多くのデータが保存されている状況です。

しかし、個人情報保護法の施行以降、この保存されたデータの取扱い方法が非常に重要となっています。日常の業務上の利用においては、管理された運用方法に乗っ取り、このデータは利用されていますが、例えば、PC の紛失・盗難等に遭遇した場合、また、PC の廃却や再利用を行う場合に、PC に保存されたデータの漏えいを防ぐことを目的として、適切なデータの消去を行うことが重要となっています。

PC に内蔵された記憶媒体のデータ消去を行うためには、その記憶媒体に適した消去方法を実行する必要があります。

PC に内蔵された記憶媒体は、フラッシュメモリの大容量化/低価格化により、HDD から高速性で優位にある SSD へと変化しています。またインターフェースの仕様は、IDE から ATA や PCIe 等へとより高速なインターフェースへと進化しています。記憶容量も急激に増えており、HDD では、数テラバイト(TB)もの容量になっています。更に、PC の構造も薄型軽量化により、従来取り外しが容易だった内蔵記憶媒体も、取り外すことが難しくなっており、内蔵記憶媒体を取り出して記憶媒体単体でデータ消去を行うことも難しくなっています。

内蔵記憶媒体が取り外せない場合、データ消去を行うには、その PC を専用プログラムで起動し、データ消去プログラムを確実に実行させることが必要です。

以前は、殆どの PC に BIOS(Basic Input/Output System)が搭載されており、専用プログラムは、この BIOS を介してハードウェアを操作することでデータ消去プログラムを実行することが可能でしたが、2012年(Windows 8)以降殆どの PC では、BIOS に変わって UEFI(Unified Extensible Firmware Interface)を採用しているため、専用プログラムの UEFI 対応が必要になっています。また BIOS では、内蔵記憶媒体に対して MBR(Master Boot Record)形式が使われていたため容量に制限(約 2T バイト未満)がありましたが、UEFI の採用により、新たに GPT(Globally Unique Identifier Partition Table)形式に対応し、大容量の内蔵記憶媒体の利用が可能になっているので、今後は大容量のデータに対する消去の方法も考慮することが必要です。

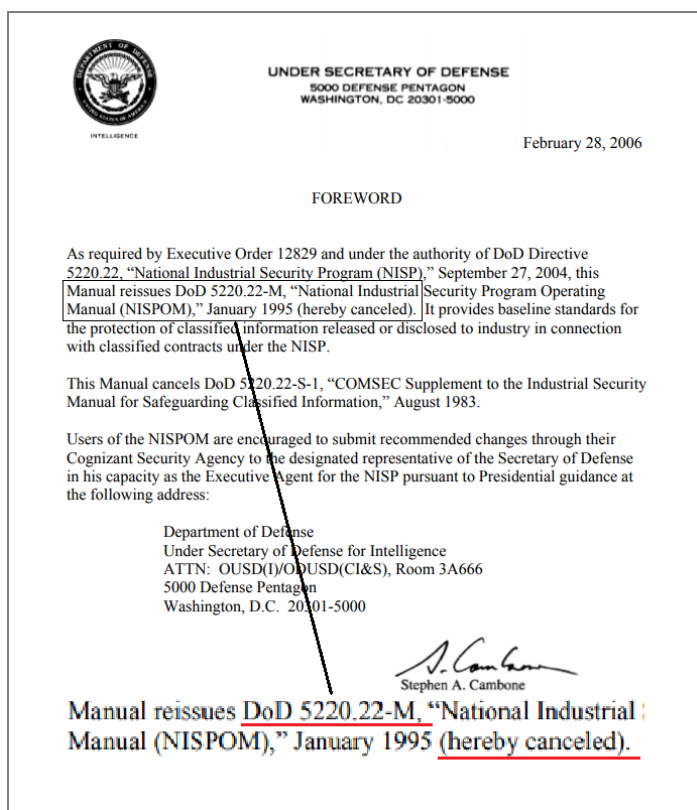
このようにデータ消去を行うためには、保存されているデータの機密度とその目的(廃棄/

再利用/遠隔消去等)や状態(媒体単体/PC 内蔵)に適した方法を選択することが重要です。

第4章 データ(情報)の特性・種別ごとの消去方式の選択

1) データ(情報)の特性・種別について

記憶媒体のデータ消去を業務としている企業に対するヒヤリングの結果では、データ消去の依頼は、ほとんどが法人団体からであり、個人からの委託は年に数件程度となっています。法人顧客では、主に上場している企業が多く、IT 監査(プライバシーポリシー)において、PCの廃棄の際は適切な消去方法を用いることを義務付けていて、更に第三者機関による消去を実施した証明書の保管も義務付けてられています。その際のデータ消去方式



は、**米国国防総省規格 DoD 5220.22-M、米国国家安全保障局方式 NSA 130-1**によって定められた3回上書きおよびペリファイを選択・指定していることが多いのですが、この規格は2006年2月に改版され、過去に記載されていたデータ消去の具体的な方法等の記載は一切取り消されています。

新たな規格として2006年に米国国立標準技術研究所(NIST)が発表したSP800-88では、「2001年以降に生産された、15GBytes以上のHDDはデータの完全消去は、研究の結果1回上書きするだけで効果的に消去することが可能」と記載されたことにより、米国の行政機関では規定の変更作業が進行中であり、国内ではIPA/ISEC(独立行政法人情報処理推進機構 セキュリティ

センター)はこの文書の和訳を2009年9月に公開していますが、あまり知られていないようです。(出典元: IDF データ消去分科会による調査報告書)

IPA/ISECは、2014年12月にSSDやeMMC、タブレットPCや携帯電話、スマートフォンについても新たに記憶媒体として追加記載し、Rev.1として改版されたものの和訳を2021年11月に公開しています。

IPA/ISECは、政府や企業の経営者、セキュリティ担当者等が、自組織の情報セキュリティ対策を向上させることに役立つ資料として、海外の規格等を一般に公開しています。

<https://www.ipa.go.jp/security/publications/nist/>

2) 現在の消去方式の選択方法

消去方式については、情報の特性・種別によってデータ消去方式を選択するのではなく、消去業者に一律に同じ方式を依頼していることが多く、金融、政府機関からの依頼では、電磁または破碎による消去を選択されるが、一般企業と同様に、PCの保存されているデータ種類や特性に関係なく、一律に同じ方式を選択されることが多いとのことです。

データ消去業者は、一般的に複数の消去方式をメニュー化しており、ソフトウェアによる上書き消去、消磁方式、破碎方式の3種類から選択できる場合が多いようです。証明書については、消去作業を実施したことを報告する報告書（実施台数、消去方式、実施日時）は無償で提供し、個別の消去証明書については有償とし、ソフトウェアを使用する場合は、消去ソフトから出力されるフォーマットを利用したレポート、消磁方式や破碎方式においては作業現場または実施後の対象媒体の画像を添付し提供しています。また、業者ごとに作業現場のセキュリティレベルに大きな違いがあり、作業現場の入退管理、外部に接続できる機器の排除、作業員への研修制度、複数人の相互監視・検証等が行われています。このように、消去方式だけでなく消去作業を行う際の環境等の管理によっても、セキュリティレベルも大きく影響を受けることとなりますので、作業環境の管理状態をランク分けすることによって、より信頼度の高い証明を行うことも必要となっています。

参考：データ消去方法による費用例（平成28年10月時点）

データ消去プラン	料金（税別）
(1) 上書き消去方式	2,500 円
(2) 消磁方式	2,500 円
(3) 破碎方式	2,500 円

作業報告書は無料、個別収去証明書は有償の場合が多く、その金額は100円～2,000円と幅があります。

※ヒヤリング先：データ消去請負事業 計5社

大塚商会様：法人向けデータ消去

リコージャパン様：PCデータイレースサービス

小規模データ消去請負会社（匿名）

大手PC買取会社（匿名）

大手情報機器リース会社（匿名）

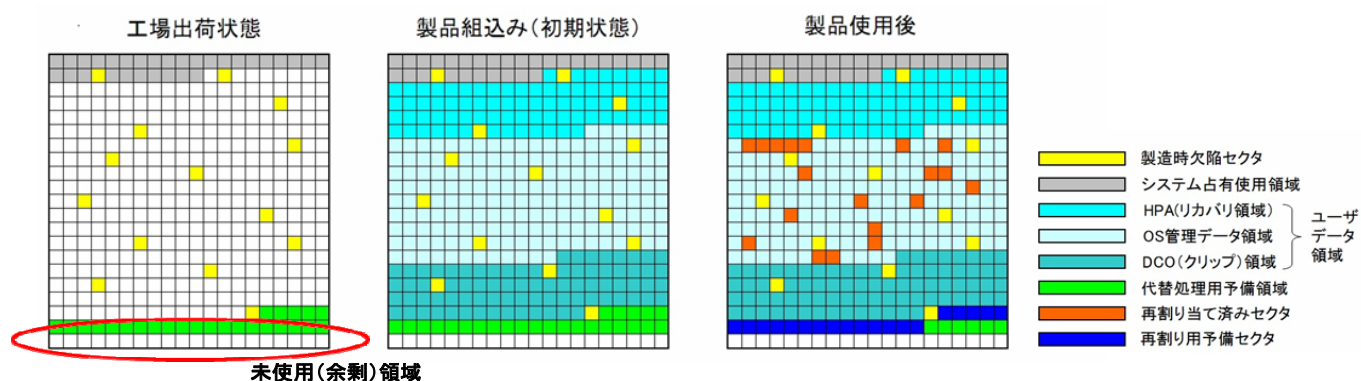
第5章 記憶媒体のデータ抹消 (NIST SP800-88Rev.1)

前章で紹介したように、最新のデータ(情報)の抹消に関する世界的な規格文書は、NIST が2014年12月に発行したSP800-88Rev.1です。この文書は、HDDやSSDのような電子記憶媒体だけでなく、CD/DVDのような光学媒体や、紙に印字されたハードコピー等も含めた、情報の漏えい防止を目的としたデータ抹消の方法について提案・解説しています。

尚、本章から第9章で用いる「抹消」とは、従来から一般的に用いられている「米国防総省規格 DoD 5220.22-M」によって定められた3回上書き等の手法による「消去」だけではなく、暗号化や物理的破壊等で情報を読み出すことを不可能にする行為全般を指します。

1. 記憶媒体内の領域と情報の残存リスク

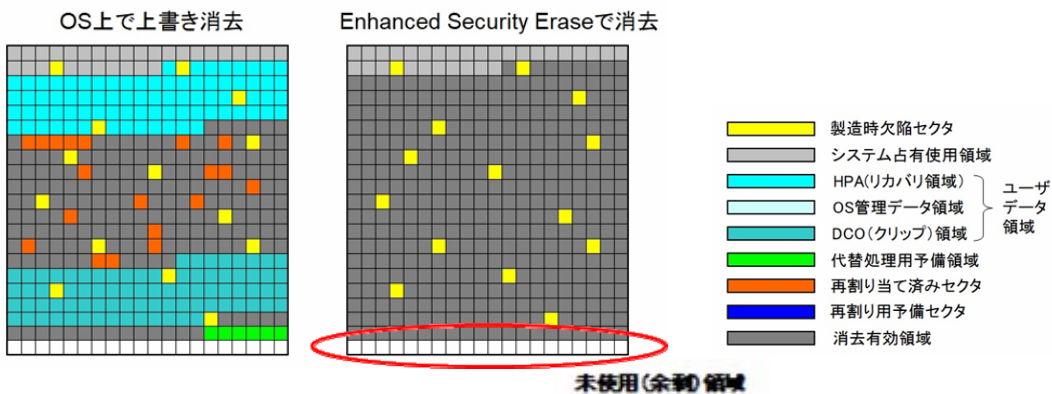
HDDを例に、内部に存在する領域と動作を説明します。



注：この図は概念であり、実際の HPA や DCO 等の領域の物理的な位置・配置を示す図ではありません。

- ① 工場出荷状態：物理フォーマット時に欠陥の検出されたセクタは、「製造時欠陥セクタ」としてシステム情報上に記録されアクセス範囲から除外される。HDD のファームウェア等が書き込まれる部分をシステム占有使用領域として確保し、使用中に「不良セクタ」が発生した場合に代替処理を行うための代替処理用予備領域も確保、ユーザ・データ領域として、公称記憶容量と一致する領域に対して LBA (Logical Block Address：論理ブロックアドレス)を0から順番に割り当て、残った部分を未使用領域とする。
- ② 製品組み込み (初期状態)：必要に応じてユーザ・データ領域内に容量の大きな媒体をサービス用として旧型の PC 用の小さな容量に一致させるための DCO (Device Configuration Overlay：装置構成オーバーレイ)や、リカバリ領域等に使用する HPA (Host Protected Area：秘密領域・保護領域)を作成する。残りの部分が OS やユーザ作成データ等を保存する領域となる。
- ③ 製品使用後：使用中にリードエラーが検出されると、リトライ処理が行われ、同一セクタで頻発する場合は、読みだしたデータを「代替処理用予備領域」に書き込み、リードエラーの発生したセクタの LBA を付与し、元のセクタは OS のアクセス範囲から除外

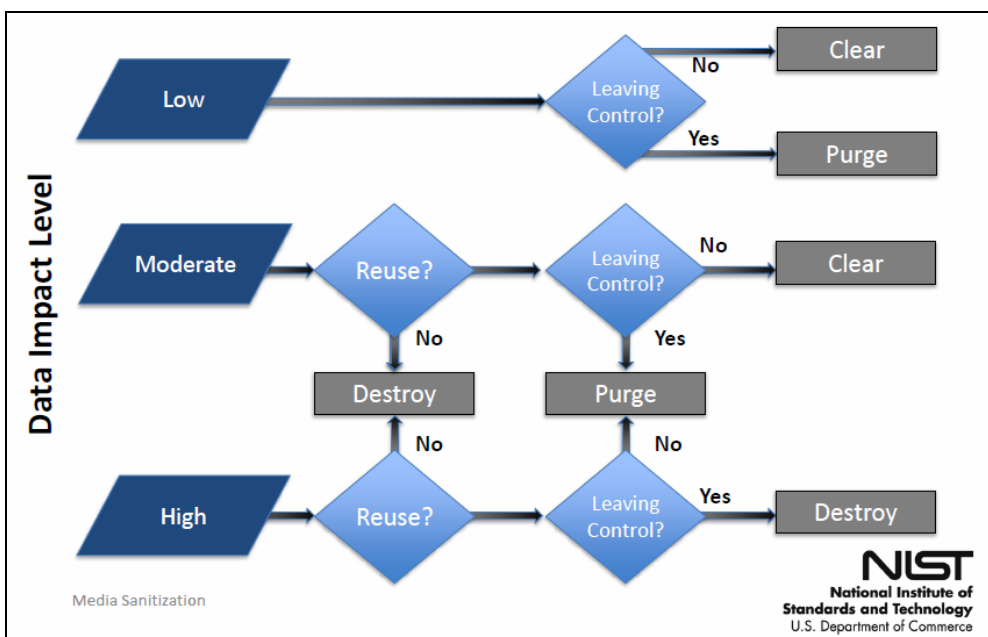
される「再割り当て済セクタ」となる。(データの抹消は行われない)



- ④ OS 上で上書き (Clear:消去) : OS 経由でアクセス可能な範囲の全てに対して上書き処理が実行されるが、OS では認識できないシステム占有使用領域、製造時欠陥セクタ、HPA、DOC や代替処理による「再割り当て済セクタ」、未使用領域には書き込み処理は行われない。これは、複数回の上書きを実行しても変化することは無い。
- ⑤ Enhanced Security Erase で上書き (Purge:除去) : Enhanced Security Erase では LBA の与えられている範囲全てと「再割り当て済セクタ」に対するアクセスが行われるので、システム占有使用領域、製造時欠陥セクタ、未使用領域以外の全ての範囲に対して上書き処理が行われる。

2. データ抹消方法の選択

SP800-88Rev.1 では、抹消方法の選択を情報の機密度と、データ抹消後にその記憶媒体をどのようにするのかの組み合わせによって、下図のように抹消方法を選択する事を推奨しています。



注：この図は、米国政府・行政機関向けの判断基準を表しています。

1) データ（情報）の重要（機密）性・ランク

- ・ 低度：情報が漏えいした場合の影響は限定的なレベル。
- ・ 中度：情報が漏えいした場合、重大な悪影響を及ぼすレベル。
- ・ 高度：情報が漏えいした場合、危機的・致命的な悪影響を及ぼすレベル。

2) 抹消の種別・ランク

- ・ 「Clear(消去)」：Resistant to keyboard attacks.
一般的に入手できるツールを利用した攻撃に対して耐えられること。
- ・ 「Purge(除去)」：Resistant to laboratory attacks.
研究所レベルの攻撃に対して耐えられること。
- ・ 「Destroy(破壊)」：Resistant to recreation of media.
媒体の再生（再組立等）に対して耐えられること。

3. HDD のデータ抹消のランクと方式

1) 「Clear(消去)」

政府機関の承認を受け、その有効性が確認されている上書き技術/方法/ツールを使って媒体の既存データに対する上書きを行なう、米国国防省規格等として従来から多く用いられている方法等。

2) 「Purge(除去)」

- ・ ATA コマンドの「Enhanced SECURITY ERASE UNIT」を使用する。
(Enhanced モードがサポートされていない媒体の場合は Normal モード)
- ・ Cryptographic Erase（暗号化消去）を行う。
- ・ 外部磁界等による消磁を行なう。

注：Cryptographic Erase とは、データを媒体上に暗号化して記録して置き、データの抹消が必要になった場合には、その暗号化に使用した「暗号化キー」だけを抹消することにより、データの復号を不可能にする方法。

3) 「Destroy(破壊)」

消磁設備と物理的破壊装置により、再使用不可能になるように破壊する。

注：消磁方式を用いる場合、2006,7 年以前に製造された機器は、それ以後主流となった垂直磁化方式の HDD に対しては、十分な消磁をできないことがあるので注意が必要。（詳細は、P-14 6. 物理破壊と外部磁界による抹消を参照ください）

4. HDD の SECURITY ERASE UNIT（SECURE ERASE）コマンド

HDD や SSD 等の電子記憶媒体では、使用中に発生した不良セクタの代替処理による「再割り当て済セクタ」や、製造者/販売者が任意に設定することが可能な、DCO や HPA 等の、

OS が認識出来ない領域が存在するために、従来から最も多く使用されている記憶媒体の外部からデータを与えて上書きを行う形式のデータ抹消用のソフトウェアでは、米国国防総省規格 DoD 5220.22-M による 3 回上書きや 35 回の上書きを行なうグートマン方式であっても OS 上で上書きが行われるにすぎないため、これらの領域に対する上書きは行われず上記の「Clear (消去)」の範囲に含まれます。

この問題を解決した抹消方式が SECURE ERASE で、2001 年に ANSI (American National Standards Institute : 米国国家規格協会) によって、HDD 本体に搭載されるファームウェア (プログラム) で設定した抹消動作を実行する ATA コマンド「SECURITY ERASE UNIT」として正式に規格化され SP800-88 の初版では完全なデータの抹消「Destroy(破壊)」の手段として認定されました。しかし、改版された SP800-88Rev.1 では製造者にしか認識できない未使用 (余剰) 領域が更に存在することを理由に「Purge(除去)」に格下げされました。

1) SECURITY ERASE UNIT コマンドの規格

ATA コマンドの ANSI によって規格化されている要求事項は、以下の通りです。

- ・ Normal Erase モードが指定された場合、すべてのユーザ・データ領域に対してバイナリ・ゼロを書き込む。
- ・ Enhanced Erase モードが指定された場合、再割り当てにより使用されなくなったセクタを含め、それまでに書き込まれたすべてのユーザ・データ領域に事前に設定されたデータ・パターンを書き込む。

注意 1. 「ユーザ・データ領域」とは、前述の HPA や DCO を含む、LBA (Logical Block Address : 論理ブロックアドレス)を与えられた全ての領域を指す。

注意 2. 「再割り当て済みセクタ」とは、記憶媒体が製造工場を出荷された後の使用中 (電源 ON 状態) で、リードエラーやリードリトライの発生頻度等より、媒体の自己判定によって「不良セクタ」と判定され、他の LBA 再割り当て専用のセクタにデータの複写を行った後に、LBA を失ったセクタを指す。

これにより、「Normal Erase モード」と「Enhanced Erase モード」との大きな違いは、「再割り当て済みセクタ」に対して上書きが行われるか否か、の差となります。

5. Cryptographic Erase (暗号化消去 : CE)

・ CE は、データが媒体に書き込まれるときに暗号化が実行される場合に使うことができる抹消手法であり、データの抹消は、書き込まれたデータの物理的な抹消ではなく、データの暗号化に使用される暗号化キーを抹消することによって行われます。

・ CE は非常に高速にデータの抹消を実現することができ、部分的な抹消、例えば記憶媒体の限定された一部の領域に対するデータの抹消にも利用することができます。部分的な抹消は、選択的抹消とも呼ばれ、クラウドコンピューティングやスマートフォンやタブレット型端末などのモバイルデバイスに対しても有効なデータ抹消の方法です。しかし、CE の問題点として、媒体の抹消に対する検証が難しいことが挙げられ、信頼できる検証方法

を取ることができない場合は、検証可能なデータ抹消方法を用いるか、または検証可能な抹消方法と組み合わせて使用することが必要となります。

・近年は、「自己暗号化ドライブ（以下、SED と表記する）」と呼ばれる常時暗号化を特徴とし、エンドユーザーが暗号化機能をオフにすることはできない記憶媒体も存在します。SED の特徴として挙げられるのは、暗号化キーが格納されている媒体上の場所に対し、機器側システムからの直結アクセスが可能とされていること、媒体が起動時に使用するファームウェア等の関連データの保存されているシステム領域などの明確に識別された領域を除いた、ユーザ領域として LBA の付与された領域に書き込まれるデータのすべてが暗号化されていることです。

1) CE をデータ抹消手段として有効に利用するための条件

- ・CE を必要とするすべてのデータがメディアに書き込まれる前に暗号化されている場合。
- ・暗号化キーが格納されている媒体上の場所（ターゲットデータの暗号化キーまたは関連するラッピングキー）が判明しており、適切な媒体固有のデータ抹消手法を使用してその領域を抹消することが可能な場合。
- ・CE を実行するための、機器に依存するコマンドを確実に使用することが可能な場合。

2) ソフトウェアによる暗号化消去の利用に対する留意点

- ・紛失したモバイル機器の迅速なりモトワイプの実行などを目的とする場合、CE を使用することが適切かつ有利ですが、暗号化キーが機器の外部に格納される場合（バックアップまたは外部預託）は、復号のために将来そのキーが使用される可能性があるため、「Purge(除去)」には相当しません。ソフトウェアによる暗号化消去ソリューションは、信頼できる暗号化キーの保護と管理の上で成り立ちます。

※日本国内においては、下記のように 2020 年から暗号化消去が、クラウドを対象とした各種基準やガイドラインに採用されるようになりました。

・クラウドシステムにおける暗号化消去

クラウドシステムに対しては、国内に於いても米国の FISMA（Federal Information Security Modernization Act：連邦情報セキュリティ近代化法 注：2014 年の改正により、Federal Information Security Management Act：連邦情報セキュリティ管理法から変更）に基づいて標準化されたクラウドソリューションの導入を目的に設立した、FedRAMP（Federal Risk and Authorization Management Program：米国連邦リスク承認管理プログラム）と、管理基準である SP800-53Rev.5 を参考に、「政府情報システムにおけるクラウドサービスのセキュリティ評価制度の基本的枠組みについて」（令和 2 年 1 月 30 日サイバーセキュリティ戦略本部決定）に基づき、内閣サイバーセキュリティセンター・デジタル庁・総務省・経済産業省が運営している ISMAP (Information system

Security Management and Assessment Program：政府情報システムのためのセキュリティ評価制度）が存在し、その管理基準において、

【1.3.14 消去(もしくは抹消)】

消去には、メディアを物理的に破壊する物理的消去、メディアを消磁装置により抹消する電磁的消去に加え、論理的消去も含む。論理的消去とは、元のデータを暗号化した後、暗号鍵を消去し、元のデータの復号を不可能にする方法を指す。

【1.3.15 暗号】

暗号技術検討会及び関連委員会（CRYPTREC）により安全性及び実装性能が確認された電子政府推奨暗号、又はそれと同等以上の安全性を有する暗号を指す。

と、明確な記載が行われ、それに引き続き NISC（National center of Incident readiness and Strategy for Cybersecurity：内閣サイバーセキュリティセンター）の「政府機関等のサイバーセキュリティ対策のための統一基準」（令和3年度版）においても、暗号化消去が以下の様に定義されました。

- ・「暗号化消去」とは、情報を電磁的記録メディアに暗号化して記録しておき、情報の抹消が必要になった際に情報の復号に用いる暗号鍵を抹消することで情報の復号を不可能にし、情報を利用不能にする論理的削除方法をいう。暗号化消去に用いられる暗号化機能の例としては、ソフトウェアによる暗号化（Windows の BitLocker 等）、ハードウェアによる暗号化（自己暗号化ドライブ（Self-Encrypting Drive）等）などがある。
- ・「情報の抹消」とは、電磁的記録メディアに記録された全ての情報を利用不能かつ復元が困難な状態にすることをいう。情報の抹消には、情報自体を消去することのほか、暗号技術検討会及び関連委員会（CRYPTREC）によって安全性が確認された暗号アルゴリズムを用いた暗号化消去や、情報を記録している記録メディアを物理的に破壊すること等も含まれる。削除の取消しや復元ツールで復元できる状態は、復元が困難な状態とはいえ、情報の抹消には該当しない。

これらは、2019年の神奈川県に於ける HDD 流出事件に端を発した「地方公共団体における情報セキュリティポリシーに関するガイドラインの改定」により、データの抹消方法の見直しが行われ、NIST SP800-88Rev.1 による「Purge（除去）」レベルの要求等が採用された影響が大きく、前述のようなクラウドシステムに於ける暗号化消去の優位性を認めた結果とすることができます。

6. 物理破壊と外部磁界による抹消

NIST SP80-88Rev.1 では物理破壊について「分解、粉碎、溶融、焼却。これらのデータ抹消方法は、媒体を完全に破壊するように設計されています。これらは通常、これらの活動を効果的、安全、かつ安全に実行するための特定の機能を備えた外部委託の金属破壊施設または認可を受けた焼却施設で実施されます。」と記載していますが、日本国内に於いてはその様な施設は存在せず、一般的には媒体に4箇所穴を開ける穿孔や、V字型に折り曲げる、細かく裁断する等の手法が用いられています。また外部磁界による抹消では、媒体を装置の磁気回路の内部に置き、誘起される磁界を印加するような専用の消磁設備・装置が用いられています。**本協議会はこれら機器のデータ抹消手段の有効性について、世界中のデータ復旧やデジタル・フォレンジックを業務としている事業者において、上記機器・装置により正しく処置された媒体からデータを読み出すことを可能としている事業者の存在は知られていないことにより、有効なデータ抹消の手段で有り得ると認識していますが、以下の点に留意することが必要です。**

1) 物理破壊・外部磁界による抹消に共通する留意点

・ソフトウェアによる抹消と異なり、抹消作業の実行に人の手が介入することを排除できないこと（悪意による不正行為を予防することが困難であること）が挙げられます。本協議会はこの理由により、これらのデータ抹消措置に対する「データ適正消去証明書」の発行を現在行っておりません。また、技術的な理由として後に記述するように、「プラッタ上の、上書きされていない磁気データを読み出す技術は存在する」ので、「物理破壊・破碎」に対してもその技術が有効であり、物理破壊措置が**単独**で使用された場合では「完全に復旧不能状態にデータを抹消した」と断言することは出来ません。また、「外部磁界の印加」の場合に於いては、プラッタの磁気が全く残留の無いレベルまで消磁されたと確認されない限り、そのデータを読み出す技術が有効であると共に、処理前、処理後の HDD を外観で判別することや、プラッタに印加された磁束が十分で有ったか否かを確認することにも困難が伴うので、これら物理的なデータ抹消手段を採用した場合に於いて、「消去（作業）証明書」を信頼のおけるエビデンスとするためには、具体的な抹消措置を行った個体、日時、担当者、使用機器等の情報及び、産業廃棄物処理の確認等を含め、データ抹消措置の詳細内容を第三者が疑義なく確認することを可能とするに足る項目・条件が網羅されている必要があります。

2) 物理破壊・破碎の留意点

・製品（HDD）によっては、3.5 インチの筐体に 2.5 インチのプラッタ（円盤）を組み込んでいるものも存在する、またそうでないものに於いても穴の場所（破壊の方法）によってはプラッタ（記録円盤）に損傷を与えることが出来ない可能性や、複数枚の最下層まで破壊出来ない可能性が存在するので、外観の目視確認だけで確実な処理が実行されたという判定が困難です。

・ソフトウェアによる上書きが1回で良いとされた理由は、上書きされた部分から以前に書き込まれたデータがはみ出す可能性を持つ幅が、現在の技術では読み出し不可能な程狭いことであり、それを理由に NIST SP800-88 に於いて「2001 年以降に生産された 15GB 以上の HDD では上書き回数は 1 回で十分である」と記載されました。つまり、上書きの行われていない場合は、プラッタを物理的に破砕した場合においても、その破片から最後に書き込まれたデータを読み出す技術が存在することを否定していません。ですから、完全なデータの抹消を必要とするのであれば、物理破壊・破砕においても事前処理として上書きや、後述する NSA の認定を受けた消磁装置による抹消等を行なうことが必要です。そして、NIST SP800-88Rev.1 では、プラッタの粉碎後のサイズに対する指定はありませんが、国家レベルの機密情報に対する規定である、米国の NSA/CSS (National Security Agency : アメリカ国家安全保障局/ Central Security Service : 中央保安部) 発表の NSA/CSS POLICY MANUAL 9-12 では、プラッタを一辺の長さが 2 mm 以下になるまで粉碎することを求めています。そして、最新版(2022 年 4 月)の NSA/CSS Evaluated Products List for Hard Disk Drive Destruction Devices に記載 (認定) されている日本製の物理破壊装置・機器は存在しません。

3) 外部磁界による抹消の留意点

・実際にデータが記録されているプラッタに十分な外部磁界が印加されたのか否かの判定が困難である。この理由は、外部磁界の印加によって媒体自体が動作不能になってしまうことが多く、仮に動作する (スピンドルモータ、ヘッドや制御基板などは異常が無く動作するが、データの読み出しだけが不可能である) 場合に於いても、プラッタ上のデータが、現存するあらゆる技術を用いても全く読み出し不能な状態に減磁されたのか否かを容易に確認することは不可能です。

- ・磁界に変動要因が存在するため、発生磁束の設計マージン、保守・管理が重要です。
 - ①磁界を発生させるための電磁石を構成するコイルに使用されている銅線の電気抵抗は、1°C当たり約 0.4%の割合で上昇するため、仮に 20°Cから 60°Cまで上昇した場合には電気抵抗が約 16%上昇し、これに伴い磁束も約 16%減少することになります。
 - ②パルス印加方式等を採用している場合が多く、内部の昇圧回路で高電圧を発生させ、コンデンサに充電をしているので、充電時間 (放電エネルギー) の管理が必要です。
 - ③コンデンサは、構造上急速な充放電による劣化 (容量の減少、等価直列抵抗の増加) が激しく、定期的な性能の確認検査を行なう必要があります。

これらの理由によって、最新版 (2022 年 4 月) の NSA/CSS Evaluated Products List for

Magnetic Degaussers に於いても、下記の注意事項が記載されています。

- ①すべての HDD 内のプラッタを変形させることによる物理的な破壊を伴う消磁を行うことを強く推奨します。
- ②このリストへの記載は、機器の継続的な性能を保証するものではありません。製造元に従って、または NSA / CSS 承認済みの磁場検証装置を使用して、機器を再テストする必要があります。

そして、このリストに記載（認定）されている日本製の製品は、1社1機種しか存在しません。

7. SSD の特徴

1) SSD はデータの書き換えをセクタ（ページ）単位の上書きで行うことができません。またイレース動作は複数のページの集合体であるブロック単位で行われます。書き換えは、データの書き込まれていないページに対して、新しいデータを書き込み、従来の論理アドレス（以下、アドレスと表記する）を付与することで、あたかも上書きが行われたように見せています。古いデータの残っているページは別のアドレスが与えられ、ブロック消去を待機する状況になります。

2) ウェアレベリングと余剰領域（オーバ・プロビジョニング）

SSD に搭載されている NAND 型フラッシュメモリには、データ書き込み回数に制限（寿命）があります。SSD の寿命を延ばすため、搭載されているコントローラーは各ページの書き込み回数を平準化するように論理アドレスの再振り当てをおこなっていて、これをウェアレベリングと呼んでいます。

また、SSD にはシステムが管理するバックグラウンド作業用の余剰領域が用意されており、上書きを実行した場合でもウェアレベリングによるアドレスの再振り当てによって、本来の目的である対象ページには書き込みは行われず、新規にそのアドレスが与えられた余剰領域上にあったページに書き込みを行い、元のページはデータが残ったまま別のページや余剰領域に割り当てられることがあります。

8. NIST SP800-88Rev.1 による SSD のデータ抹消のランクと方式

SSD の上記のような特徴を踏まえて NIST では以下の様に定めています。

1) 「Clear(消去)」

- ・ATA コマンドの「SECURITY ERASE UNIT」コマンドを使用する。
- ・政府機関の承認を受け、その有効性が確認されている上書き技術/方法/ツールを使って媒体を上書きする。(1回で媒体容量全てに書き込むことの出来る量の固定データ、或いは乱数のようなデータを複数回書き込む。) フラッシュメモリの媒体に対する書き込みは、媒体の寿命を短縮すること、古いデータがまだ残っている可能性がある LBA を持たない領域のデータを抹消できないことに留意すること。

2) 「Purge(除去)」

- ・ ATA コマンドの「BLOCK ERASE」コマンドを使用する。
オプション：「BLOCK ERASE」が正常に動作した後、全 LBA に対しバイナリ値 1 を書き込み、再度「BLOCK ERASE」を実行する。
- ・ Cryptographic Erase (暗号化消去) を行う。

3) 「Destroy(破壊)」

- ・ 物理的破壊装置により、再使用不可能になるように粉碎・破壊する。

注：SSD の最新の接続インターフェースである NVMe でも ATA 準拠のデータを抹消するためのコマンドが準備されています。

8. (参考) 他に行われている SSD のデータ抹消の方法

SSD のデータの抹消については、NIST が SP800-88rev.1 で上記の様に定めていますが、技術の進歩が急速なため、以下のような抹消方式も用いられています。

1) Secure Erase (Security Erase Unit コマンド)

SSD の多くは、HDD のデータを完全に抹消するコマンドの Secure Erase に対応しています。

2) Format & Trim

SSD を Format した後、OS が発行する Trim コマンドによって、PC の動作中のバックグラウンド動作によってブロック消去を促進する方法です。


Trim は Windows7 以降の OS が持つコマンドであり、全ての OS が Trim コマンドをサポートしている訳ではありません。また、Trim は、直接的にデータの抹消を命令するコマンドではなく、不要になったページを SSD に伝えるコマンドであるため、いつブロック消去が実行されるかの保証はありません。(15 分～1 時間程度でデータの復旧が不可能になったという論文も存在する) データの抹消を確実にするために、SSD 独自の制御として内部記録領域の情報更新を行う目的で、処理の最後に ATA コマンドの Standby Immediate を付加しバックグラウンド動作の促進処理を行う場合もあります。

第6章 ISMS (ISO/IEC27001) と NIST SP800-88

PCを含むコンピュータシステムを取り扱う企業は、ISMS (ISO/IEC27001) 等の情報セキュリティマネジメントシステムの認証を取得していることが一般的になっていて、それらの認証を取得していることを「世界標準のセキュリティ管理体制」と謳っている例も見受けられますが、ISMSは絶対的な管理手法が定めているのではなく、所有する情報資産の特性によって、リスクアセスメントを行い、その組織の経営・管理責任者が決定した、適切な管理を行うことを求めている、リスクを完全に除去することが種々の条件により困難な場合は、「残留リスク」としてその脅威が残存することを組織の最高責任者が認知・承認することが出来れば、ISMSの認証を取得することの妨げにはなりません。前章で解説したNIST SP800-88に於いて、情報の重要性によって推奨されるデータ抹消のランクに差異が存在するのも、この考え方に従っている証であり、データの抹消手法の選択も、合法的な情報の所有者・管理者の判断によって選択されるべきものとしています。

1. (参考) 判断例：

※ 情報の機密度による、抹消ランク選択の具体例

機密度	抹消ランク	抹消方法	情報の種類	対象
高 	Destroy(破壊)	物理的破壊	行政、官公庁に属する情報のうち高度な機密性を持つ情報	企業・法人、官公庁の機密性の高いサーバー等
	Purge(除去)	ANSI データ抹消コマンド、暗号化、外部磁界等による抹消	個人情報データベース、企業秘密、知財情報、経営情報など	
	Clear(消去)	DoD 規格等の(複数回を含む) 上書き	個人のプライバシー、企業・法人の業務関連情報など日常的な情報	個人用 PC、企業・法人の通常業務用 PC 暗号化ソフト使用 PC

※ 抹消ランク決定理由の具体例

上記「記憶媒体内の領域と情報の残存リスク」から推測できるように、OSを介して行う上書きと Enhanced Security Erase の差は、HPA、DCO 及び「再割り当て済セクタ」に対する上書き処理の有無であるので、次ページのような考え方・判断をすることができます。

1) HPA は、PC を購入時点の初期状態に復帰させるリカバリ機能のための情報が記録されており、PC の使用によってユーザが作成した情報の保存が行われる領域ではない。

DCO は容量の大きな記憶媒体を旧型の容量の小さな PC のサービスパーツとして使用するための意図的な容量削減を目的に設定した領域であり、PC の使用によってユーザが作製した情報の保存が行われる領域ではない。

「再割り当て済セクタ」は、一般的なデータ復旧やデジタル・フォレンジック用途のソフトウェアではアクセス不能であり、セクタ単位のデータの断片の可能性が高く、ファイ

ル全体が読み出される可能性は低いので、抹消は不要である。⇒「Clear(消去)」を選択

2) HPA、DCO、「再割り当て済セクタ」にアクセスしデータの読み出すことは、上記の様にソフトウェアでは不可能であるが、一部のデータ復旧やデジタル・フォレンジックを行う事業者の所有する機器を用いることによりアクセスすることは可能であると共に、データ復旧業者からの聴取結果では、取り扱うデータ復旧案件のうち約 6 割の原因がリードエラーであり、その大部分が読み取り可能であることから、情報の重要度、マルウェア存在の可能性等により万全を期すためには抹消の実行が必要である。⇒「Purge(除去)」を選択

3) 2015 年 2 月に情報セキュリティ関連業者である Kaspersky が、<https://blog.kaspersky.com/equationhddmalware/7623/>において、HDD のファームウェア領域に潜むマルウェアの存在を公表し、Google も 2016 年 2 月に発表したレポート <http://research.google.com/pubs/archive/44830.pdf> において、第一の一般的な問題は、最近の HDD の持つファームウェアのサイズと複雑さは、(HDD やホストを攻撃するセキュリティバグを含む) バグにつながるということである。HDD のファームウェアアタックは可能であるだけでなく、既に使われたようである。これを解決するために、ファームウェアの真正性を保証し、許可なく行われる改竄から保証することが容易でなければいけないことは明白であり、長期的には他のシステムに既に導入されているような堅固な防御技術を適用しなければならない。我々は、短期的にはディスクへの物理的アクセスを制限することや、ファームウェアを書き直す能力を持つホスト OS から不正コードを隔離することによって、この問題に対する解決を図る。と表明している。またウェブカメラやルータ等の電子機器の不正なファームウェアの存在が否定できない現状では、どのような領域であってもユーザが作成した情報の存在を絶対的に否定することは出来ず、抹消作業が行われないことが判明している領域が存在することを許容することは出来ないので、万全を期す必要がある。⇒「Destroy(破壊)」を選択

ISMS では、上記の例の何れであっても、その判断が情報の正当な所有者/管理者によって行われたのであれば、問題とすることはありません。

抹消方式の判断は、その記憶媒体上に存在する情報の重要度と残存するリスクを総合的に判断して決定すべきものであるとしています。

第 7 章 ソフトウェアについて

これまで述べてきたように、データの抹消については情報の正当な所有者・管理者により判断・決定することが求められると共に、「Purge(除去)」に対応する抹消 (HPA や DCO を含む LBA が付与された全セクタと再割り当て済セクタ等に対する抹消) の判定が不可欠

であるため、本協議会の認証評価もこれに従ったランクの区分を行います。

現在までの調査結果では、現存するデータ消去ソフトウェアや装置には、抹消範囲が OS を介してアクセスすることが可能な範囲に留まる Clear 相当のものが多く、Purge に対応するソフトの場合に於いても、動作完了後に抹消済である HPA や DCO、システム領域に存在する再割り当て済セクタ情報を抹消動作以前の状態で存在させるものや、それらを解除してしまうものも存在しますが、この点は認証評価の対象には含めません。しかし、この動作の結果として、抹消実行後のドライブが搭載されている PC から認識できない、起動しないという事象が発生する場合があります。これらソフトウェアと PC や記憶媒体との組み合わせに起因する問題はソフトウェアの製造・販売者とソフトウェアを使用する者の間で対処するものとして認証評価の対象には含めないものとします。

第 8 章 作業環境について

4 章で述べたように、情報漏えいの予防は、情報システムの管理やデータ抹消方法の選択だけでなく、作業環境の管理や作業者に対する教育等を含めたマネジメントも大きな影響を与えます。情報セキュリティ環境の公的な認証制度として、プライバシーマーク（P マーク：JIS Q15001）、ISMS（ISO/IEC27001）が知られていますが、P マークは企業全体、ISMS は一定の組織を単位とし、P マークは個人情報に限定、ISMS はその組織の判断によって定められた情報の重要性に従ったセキュリティマネジメントの審査・認定を行う物であるため、それらの認証を取得しているからといって、データ抹消作業に対しても必要十分なマネジメントが行われていることを証明していると判断することは出来ません。

本協議会では、評価の対象を電子記憶媒体のデータの抹消業務に限定した、情報セキュリティに対する適切な環境管理及び作業者の教育等に関する認証制度を設け、データ消去証明書にもその環境管理のランクを記載することによる、より信頼性の高い証明書の発行を目指します。

第 9 章 証明書について

データ適正消去実行証明書に表記される内容は、下記の内容を含むものとします。

1. データ抹消を行ったパソコンおよび記憶媒体の情報
2. 抹消作業の情報として、抹消実行事業者名、ソフトウェア名、実行日時、抹消方法、HPA、DCO や再割り当て済セクタ、リカバリ領域/区画に関する情報を含む抹消作業の結果、及び残留するリスク等の特記事項

第 10 章 証明書の技術と運営について

1. 証明書の認証技術と認証業務

PKI (Public Key Infrastructure) は、公開鍵暗号技術をベースとしてセキュリティの根幹であるプライバシー、情報の改ざんの検出、電子署名、本人認証等従来では困難であった課題を解決する普遍的なセキュリティのインフラストラクチャで、電子政府の認証基盤やセキュアな電子商取引の基盤として用いられています。

2. 認証システム基本技術

(1) 秘密鍵と公開鍵の利用

公開鍵暗号方式は、鍵ペア (公開鍵と秘密鍵) によって、PKI による対称鍵の暗号化での安全な対称鍵配送と、デジタル署名によるデータの改ざん検出と固有確認方法として用いられてきました。

データ消去証明の場合は、実行者が正しく消去したことの証明を第三者が確認できるような認証システムの構築を行うことが必要となります。その場合に、公開鍵配送の場合もデジタル署名の場合も、相手の鍵ペアの真正性の確認が必要です。鍵ペアのなりすましやチャレンジレスポンスによるランダムな合鍵生成による攻撃から守るためには、消去実行前と消去実行後で突き合わせた結果をもって公開鍵証明書とする必要があると考えます。このために信頼できる第三者機関の認証局 (CA: Certification Authority) が公開鍵を発行する PC (ドライブ) を証明する時限設定をした秘密鍵を用いて消去を行い、CA は消去実行後に消去前に発行した秘密鍵と消去完了後に発行する公開鍵を照合させ、デジタル署名を付した公開鍵証明書を発行します。公開鍵の利用者は、この CA を信頼して (CA のデジタル署名が正しい) 相手の公開鍵の真正性を確認することができます。

(2) PKI の標準体系

PKI の標準は ISO/ITU-T の X.509 公開鍵証明書を基礎とします。

証明書	RFC5280: X.509 標準の証明書と失効リストのプロファイル
証明書管理	RFC2510: 証明書の要求や管理プロトコルを定めた CMP RFC2511: 証明書要求管理フォーマット CRMF
PKI 操作関連	RFC2559、2587: リポジトリ操作プロトコルやスキーマ RFC2560: オンラインの証明書状態を問合せるプロトコル OCSP
CP/CPS	RFC3647: 証明書ポリシー (CP) と認証機関の認証局運用規程 (CPS) のフレームワーク
タイムスタンプ検証	RFC3029: 公証サーバー DVCS、データやデジタル署名の公証 RFC3161: タイムスタンププロトコル (TSP)

PKI アプリケーション	RFC2630：ASN.1 署名フォーマット RFC2632、2633：署名、暗号メール、S/MIME v3 RFC2246：Web/Browser の TLS 認証 RFC2409：IPsec/IKE、VPN 装置認証と鍵交換の方式
-----------------	--

3. 認証業務の信頼性と運用

認証業務を安全に遂行し、PKI サービスが利用者に信頼されるためには、システムのセキュリティ機能だけではなく運用系を含めた安全基準が求められます。また、外部登録機関やリポジトリ等と連携する場合には、認証局は外部登録機関に認証局の定めた各種のセキュリティ基準を遵守させ、信頼性や安全性の一貫性を保持することが望ましい。以下に認証業務のセキュリティに必要な標準や認定制度についての例を記載します。

(1) 各種のセキュリティ基準

- ・ 証明書ポリシー (CP)、認証局運用規定 (CPS)

認証機関の運用には証明書ポリシー (CP: Certificate Policy)、認証局運用規定 (CPS : Certification Practice Statement) を定め、証明書の使用目的やその責任を明確に表明すること。

- ・ WebTrust 認証による監査

認証局は Principles and Criteria for Certification Authorities および **WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security** の検証を年に一度、あるいは認証局の業務から独立した中立性を保つ監査人が必要と判断した時期に往査すること。

- ・ 認証局専用ファシリティ、運用実績

認証局は、一般的なデータセンターに相当する設備を備えた上で、さらに認証局運用に必要な各種設備を備えること。

耐震措置

地震によるお客様システムへの影響や人的被害を最小限に抑えるべく、空調機器や照明装置、ケーブルラック等の設備から、ラック、什器、ラック内各マシン・デバイスに至るまで、耐震、落下防止、転倒・移動防止等、各種必要な措置を講じること。

電源設備

安定的な受電、停電や法定点検等、万一の電力供給ストップに対しては UPS 及び自家発電機を備え、24 時間 365 日安定した電力を供給すること。

消火設備

消火設備を備え、火災時のマシン等への影響、マシン等に格納されている情報資産

への影響を最小限に抑えること。

空調設備

連続運転が可能な複数台の空調機を備え、マシンに最適な環境を維持します。また防水パンや漏水センサー等、設備異常時のマシン等への影響をできる限り少なくすること。

インターネット接続の冗長性

インターネットへの接続は冗長化され、可用性を高めること。

アクセス制御・認証

Firewall やルータ、その他各種アプリケーションを用い、認証局への不必要なアクセスの制限、アクセスの際の厳格な本人認証等を実現すること。

侵入検知対策

侵入検知システム(IDS/IPS)等による、不正アクセス検知、マルウェアやウイルスチェック等のセキュリティ対策を講じること。

・ 認証局専用オペレーション

高度な技術力と十分な経験をもつ専任の技術・運用オペレータが、認証局の運用に特化したポリシーに従い、認証局システムを安心・確実に運用すること。

運用ポリシー・手順

認証局の運用に特化して定めた『運用ポリシー』及び『手順』に従い、厳格な運用を行う。国内電子署名法の適用を受けられる認定認証局に求められる要件への対応等、常に時代に即したポリシーへの改善がなされていること。

専任オペレータ

認証局運用・鍵管理の他、認証システムに精通した運用オペレータ・技術スタッフによる対応が望ましい。

手順書をベースとしたシステムの起動・停止等はもとより、障害対応、パッチ適用前の動作検証等、幅広い対応を行うこと。

業務監査・セキュリティ監査

定期的な監査を行う。運用ポリシーおよび手順に従った運用がなされていることを定期的に監査し、また必要があれば是正措置を講じること。

- ・ 準拠法

CPS に基づく認証業務にかかわる紛争等については、日本国の法律が適用されること。

- ・ ISMS (Information Security Management System)

日本では情報システムのセキュリティ管理に関する評価制度が存在します。ISO/IEC 27001 (情報セキュリティマネジメント実施基準) に基づいて実施される評価認定制度です。事業者はこの基準に沿って自社のセキュリティポリシーを定め、組織を明確にし、保護資産を定めて人的物理的セキュリティを図り、運用管理規程を定め、ネットワークセキュリティ対策を行い、システムの開発保守方針を定め、関連する法律への準拠性を明確にしなければなりません。

- ・ 認証業務の認定基準

2001 年 4 月に施行された「電子署名及び認証業務認定に関する法律」では、法第 6 条で認証業務を認定するための認証設備基準、本人確認方法、運用方法の認定基準を省令等で定めるとして、対応する省令でこれらの基準が定められています。これらの基準はかなり厳しい内容となっており、法第 6 条 1 項では、認証設備は、入退出管理が行われる部屋で、権限がない者のネットワークおよび物理的な不正なアクセスを禁止する措置が取られ、証明書を発行する計算機は専用のマシンを使用し、天然災害に対処する措置が取られることとし、指針で詳しいガイドラインが示されています。法第 6 条 2 項の本人確認の方法は、住民票の写しと申請者の写真がある旅券または運転免許証等、または申請に用いた押印の印鑑証明書を提出することとしています。法第 6 条の 3 項の運用方法については、関連文書の記録、証明書に記載すべき事項、利用者への必要事項の公開、業務の管理規定の作成と実施等を義務付けています。また、認定を受けるためには認定申請を担当大臣に申請することと、指定調査機関の検査を受け、認定基準を満たすことを調査する事になっています。また認定は 1 年で、継続する場合再調査を受けることが義務付けられています。

4. 登録業務の信頼性と運用

登録機関やリポジトリ等認証局外部と連携する場合には、認証局の定めた各種のセキュリティ基準を遵守し、信頼性や安全性の一貫性を保持する義務があります。

5. 認証局運用における団体の取り組み

公開鍵暗号方式のシステムを利用した証明書の生成、開示、更新、失効等の認証サービスを提供する団体は、用途に応じた証明書およびそれらを管理する認証局がその信頼性および安全性を確立する必要があります。

出典：電子商取引実証推進協議会 (ECOM) 認証局検討ワーキンググループ

第 11 章 データ消去証明書の発行プロセス

認証システムの構成要素

PKI を構成するコンポーネントには図に示すように以下の 3 つの中核となる要素と、CA の発行する証明書と失効情報を使って認証、秘匿、デジタル署名のサービスを受ける PKI アプリケーション（PKI クライアント等）があります。

- ・公開鍵証明書と失効情報を発行する認証機関（CA）
- ・登録機関（RA）
- ・証明書や失効情報を公開するリポジトリ（Repository）やオンラインでの失効情報を提供する OCSP（Online Certificate Status Protocol）レスポнда

図：データ消去証明フロー



図は、消去したドライブが正しいプロセスで消去されたことを証明するためのフローを表しています。最初に、消去したいドライブが入った PC の情報を専用ツール（API）で暗号化または暗号化通信を用いて情報（CSV 等）を登録サーバーに送信し、秘密鍵（消去対象の証明書またはシリアルキー）を生成します。その後に、消去プログラムで消去を実行する際に秘密鍵を入力して消去を実行します。

消去完了後に、秘密鍵と消去完了のステータス（消去方法、実行者、実行日等）を登録サーバーに送信します。その際に、インターネットに接続できなければ、他のデバイスから送信ができるようにします。PC 情報（ドライブ情報）から消去完了のステータスを登録サーバ（RA）から閲覧できるようにします。

- ・セキュア・タイムスタンプ

本証明書が失効していた場合や有効期限が切れていた場合、その証明書が対象のデジタル署名を実行した時点で有効であったことを検証するために、信頼できる時刻の付与が必要になります。

そのために PKI 技術を用いたセキュアなタイムスタンプを付与するようにします。

タイムスタンプ要求者は、任意のデジタルデータのハッシュ値を信頼できる第三者機関である TSA (Time Stamp Authority) に送ります。TSA は信頼できる時刻源から得た時間と要求者のハッシュ値を結合し、TSA の署名を付したタイムスタンプトークンを返します。この方式はシンプルプロトコルと言われ、RFC3161 として標準化されています。

- ・ 長期的署名検証の実施

抹消したデータを巡って係争があった場合に備えて、長期的にデジタル署名を保証する必要があります。このような長期的な署名の検証を可能とするためには、タイムスタンプを付与し、検証に必要であった証明書チェーンの全ての証明書やそれぞれの失効情報をすべて収集し一定のフォーマットに記録しておくことで、タイムスタンプと証明書、失効情報でタイムスタンプの時点で証明が正しかったことを後に確認できるようにします。

第12章 まとめ

PCや電磁記憶媒体の進化や大容量化等に伴い、今までのデータの抹消の手法では十分に適応できず、最近のドライブの特性に適している抹消方法が必要とされる状況になっています。また大容量化による当然の結果として作業時間も増加する傾向にあります。また、過去の規格に囚われ、完全な抹消結果を得ることが出来るといわれている長時間の作業を選択した場合に於いても、適切な結果を得ることができず、情報漏えいのリスクを残している結果となっている場合もあります。

また、マイナンバー制度が導入され、「特定個人情報の適正な取扱いに関するガイドライン」で定められる安全管理措置においては、機器及び電子記憶媒体等に記録されたマイナンバーは、必要なくなった段階で速やかなデータの削除を行い、機器及び電子記憶媒体を廃棄する場合は専用のデータ消去ソフトウェアの利用又は物理的な破壊により復元不可能になる手段を採用し、「個人番号若しくは特定個人情報ファイルを削除した記録を保存する。作業を委託する場合には、委託先が確実に削除又は廃棄したことについて、証明書等により確認する。」とされています。

PCの廃棄は、通常委託した産業廃棄物の処理が適正に実施されたかどうかを確認するための産業廃棄物管理票（マニフェスト）が作成されますが、その内容に関しては規定や法的な制約はなく、作業ミス、不正な処分、不法投棄が行われた場合には依頼元に責任が課せられる可能性があります。そのため第三者機関によるPC製造番号、HDDシリアル番号等が記録された「消去証明書」を発行することは極めて重要となります。

また、データ消去作業は委託元企業および委託先業者の施設のセキュリティ管理が万全でないと、作業待ちの一時保管段階や作業場所での盗難やデータ持ち出しが可能となり、データ漏えいのリスクが高まります。保管場所の厳重な施錠はもちろんのこと、各エリアへの入退室管理や防犯・監視等の物理的セキュリティシステムによる管理が徹底されていることを認証することが必要です。

このようなことから、本協議会では、「データの特性および利用範囲に適した抹消方法を選択するための情報の整理」、「データ消去実施者および環境を特定・記録し、抹消を実行されたことを第三者機関によって認証」の重要性を認識し、安全・確実なデータ消去の環境作りを行っていくことが急務であるという結論に至り、その模範となるべき項目をまとめ、本ガイドブックを作成いたしました。今後も電子記憶媒体の進化に合わせ、本ガイドブックも必要に応じた改訂を続けて行くことといたします。

第 13 章 参考情報

以下の団体における規定や技術について調査を実施し、ガイドラインの作成を行っています。データ適正消去実行証明協議会では、データ消去の証明を行うにあたり、このような団体の調査結果も取り入れることで適正な消去証明の発行に必要な規定の検討を行っています。

参考にした出典元：

- ・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）

（参考）NIST Special Publication 800-88

米国国立標準技術研究所（NIST：National Institute of Standards and Technology、以下、NIST と称す。）の情報技術ラボラトリー（ITL：Information Technology Laboratory）は、国家の測定および標準に関する基盤において技術的リーダーシップを提供することにより、米国の経済と公共福祉に貢献している。情報 技術ラボラトリーは、テストの実施、テスト技法の開発、参照データの作成、実装によるコンセプト実証、技術的 分析を通じて、情報技術の開発と生産的利用の発展に努めている。情報技術ラボラトリーの責務は、連邦政府の情報システムにおいて、費用対効果の高いセキュリティを施し、国家安全保障にかかわらない情報のプライバシーを確保するための、技術的、物理的、管理的および運用のための標準とガイドラインを策定することにある。NIST Special Publication 800 シリーズでは、情報システムセキュリティにおける情報技術ラボラトリーの調査、ガイドライン、普及活動ならびに産業界、政府機関および教育機関との共同活動について報告している。

（参考）データ取り扱い機器の進化

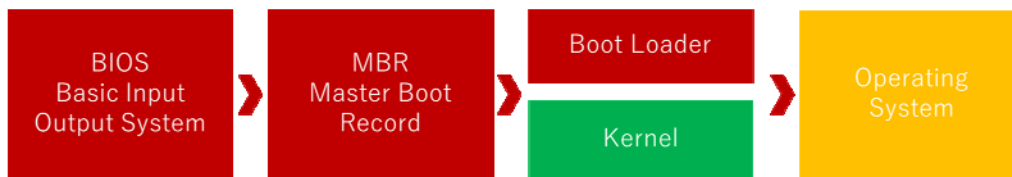
BIOS と UEFI の違いについて

2012 年以降、PC で主に使われている 64 ビット版の Windows 8 以降を搭載した製品では、「BIOS」（Basic Input/Output System の略称）というハードウェアファームウェアと OS を結びつけるインターフェースのかわりに、「UEFI」（Unified Extensive Firmware Interface の略称）という新しいインターフェースが採用されています。この UEFI 搭載 PC では、BIOS 搭載 PC 用に作られた従来からあるソフトウェア、特に PC 用データ消去ソフトウェアが動作せず、使用できないことが多く発生しています。

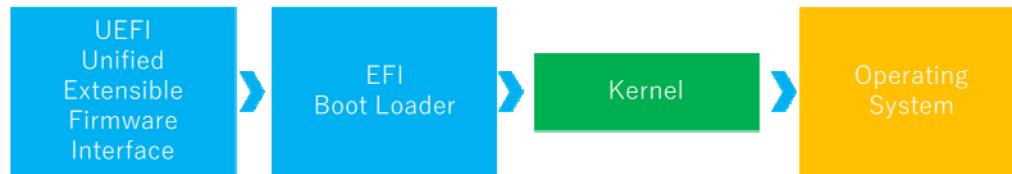
UEFI（Unified Extensible Firmware Interface）とは、Intel が BIOS（Basic Input/Output System）を「EFI」に置き換える目的で考案したファームウェアの仕様で UEFI フォーラム

によって仕様策定が進められています。BIOS から UEFI に移行することで、設計の自由度が増し、大幅に機能を強化できるようになります。UEFI は約 2.2TB 以上のディスクパーティションを OS 起動用のドライブとして利用可能になります。従来から使われている BIOS は、16 ビット PC に対応して開発された仕様であり、メモリアドレス空間が 1MB の制約がありますので、これらの制約を克服すべく開発された仕様が UEFI になります。

BIOS Booting



UEFI Booting



協力団体・作成者・監修者

協力団体：

一般社団法人ソフトウェア協会（Software Association of Japan）

会長：田中 邦裕（さくらインターネット株式会社 代表取締役社長）

設立：1986（昭和 61 年）2 月

会員：665 社・団体（令和 4 年 6 月現在）

目的：コンピュータソフトウェア製品に係わる企業が集まり、ソフトウェア産業の発展に係わる事業を通じて、我が国産業の健全な発展と国民生活の向上に寄与する。

協力：データ適正消去実行証明協議会（ADEC）が目的とする、PC 等の様々な IT デバイスのリユース／リサイクルによる循環型社会への貢献を実現するために、データ適正消去証明書の発行事業を担う。

○お問い合わせ先

SAJ 事務局 TEL：03-3560-8440

URL：https://www.saj.or.jp/

〒107-0052 東京都港区赤坂 1-3-6 赤坂グレースビル

第2版作成者

データ適正消去実行証明協議会（ADEC） 消去技術認証基準委員会

メンバ：アドバンスデザイン株式会社、
株式会社ウルトラエックス
株式会社ゲットイット
特定非営利活動法人デジタル・フォレンジック研究会、
株式会社パステムセゾン
ワンビ株式会社

監修者

データ適正消去実行証明協議会（ADEC） 認証判定委員会

委員長：佐々木良一氏（東京電機大学 名誉教授 兼 サイバーセキュリティ研究所
客員教授）

委員：手塚 悟氏（慶應義塾大学 環境情報学部 教授）

：満塩 尚史氏