ADEC

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 版

2019 年 7 月

目次

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、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。

しかし、情報漏えい事故を紐解いてみると外部からの侵入よりも大きな被害は内部からのデータ流出やモバイル端末の紛失によることが多くなっているのが実態です。PC の再利用を目的とした海外への販売や、個人向けパソコン（以下、PC と表記する）などのデジタルデバイスをネットオークション転売によるデータドライブからの情報漏えい事件も発生しております。社内ネットワークへの侵入においてはログによる侵入形跡の把握や端末の紛失や盗難の際には資産管理等で把握することができますが、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。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。

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の状況を正しく把握することが必要となります。このたび、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」を設立いたしました。本協議会では、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いきます。本ガイドラインでは、2012 年以降に発売された PC をはじめ、デジタルデバイスに内蔵された状態の SATA インターフェースを持つ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故事例

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

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業界標準ガイドラインの策定

実施主体：データ適正消去実行証明協議会

実施方法：

　データ抹消に関する技術、知見を持つ会員企業および、協議会外から参加ならびにガイドライン策定にあたり執筆に協力いただける企業を募集

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ということが重要な課題となっています。また、今後は、ビック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すが、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	・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	・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。

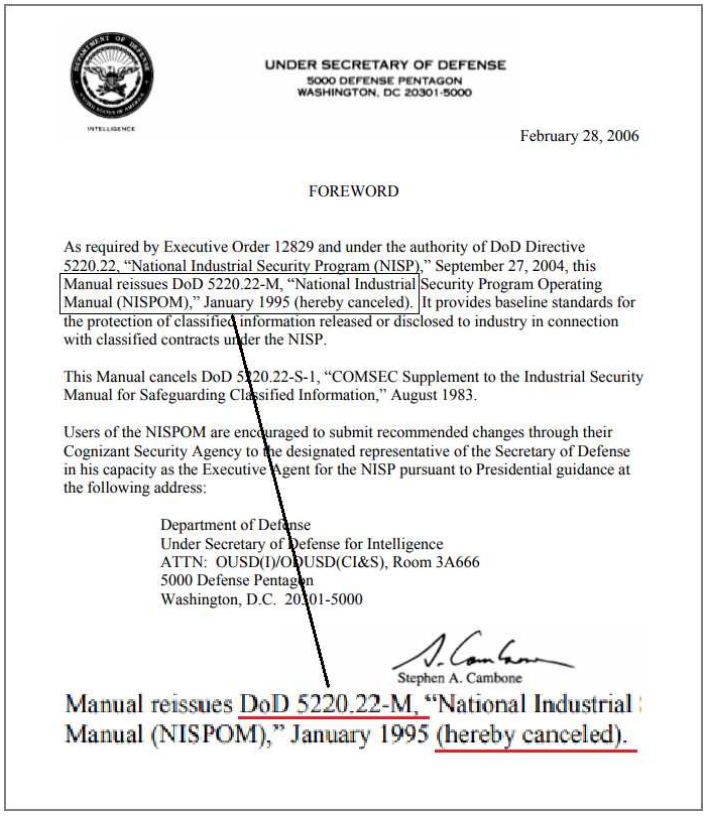
以前は、殆どの PC に BIOS(Basic Input/Output System)が搭載されており、専用プログラムは、この BIOS を介してハードウェアを操作することでデータ消去プログラムを実行することが可能でしたが、2012 年(Windows 8)以降殆どの PC では、BIOS に変わって UEFI（Unified Extensible Firmware Interface)を採用しているため、専用プログラムの UEFI 対応が必要になっています。また BIOS では、内蔵記憶媒体に対して MBR(Master Boot Record)形式が使われていたため容量に制限(約 2T 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、



UNDER SECRETARY OF DEFENSE
5000 DEFENSE PENTAGON
WASHINGTON, DC 20301-5000

February 28, 2006

FOREWORD

As required by Executive Order 12829 and under the authority of DoD Directive 5220.22, "National Industrial Security Program (NISP)," September 27, 2004, this Manual reissues DoD 5220.22-M, "National Industrial Security Program Operating Manual (NISPOM)," January 1995 (hereby canceled). It provides baseline standards for the protection of classified information released or disclosed to industry in connection with classified contracts under the NISP.

This Manual cancels DoD 5220.22-S-1, "COMSEC Supplement to the Industrial Security Manual for Safeguarding Classified Information," August 1983.

Users of the NISPOM are encouraged to submit recommended changes through their Cognizant Security Agency to the designated representative of the Secretary of Defense in his capacity as the Executive Agent for the NISP pursuant to Presidential guidance at the following address:

Department of Defense
Under Secretary of Defense for Intelligence
ATTN: OUSD(I)/ODUSD(CI&S), Room 3A666
5000 Defense Pentagon
Washington, D.C. 20301-5000

Stephen A. Cambone

Manual reissues DoD 5220.22-M, "National Industrial
Manual (NISPOM)," January 1995 (hereby canceled).

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 回上書きおよびベリファイを選択・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 技術本部 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）

SP800-88 は、2014 年 12 月に Rev.1 として改版が行われ、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ていますが、まだ和訳は公開されていません。

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、電磁または破砕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、破砕方式の 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、消磁方式や破砕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になりますので、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）上書消去方式	**2,500 円**
（2）消磁方式	**2,500 円**
（3）破砕方式	**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）

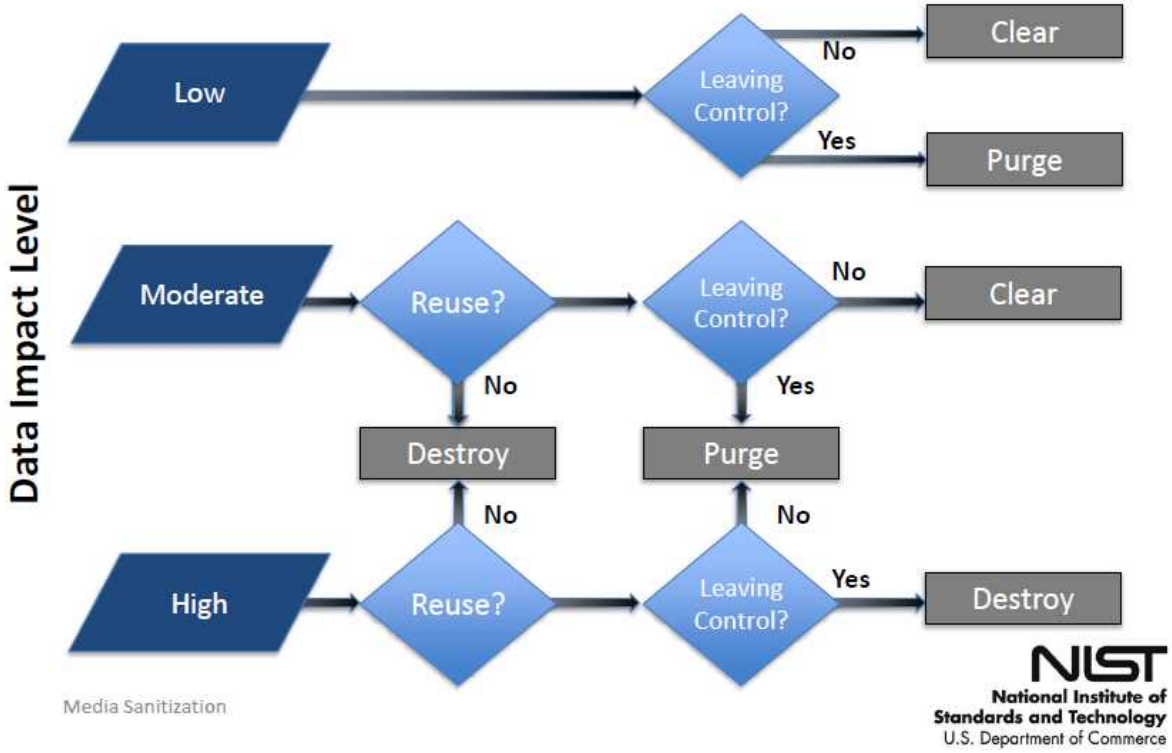
第５章　記憶媒体のデータ抹消（NIST SP800-88Rev.1）

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、本章で用いる「抹消」とは、情報を消し去り、何もない状態にする「消去」だけではなく、暗号化等で内容を判別・復旧することが不可能にする行為全般を指します。

１．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。

２．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を上書きする。

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。
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)」
消磁設備や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。

３．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（Device Command Overlay：装置構成オーバレイ）や HPA（Host Protected Area：秘密領域・保護領域）等の、OS が認識出来ない領域が存在するために、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消去用のソフトウェアでは、グートマン方式による 35 回の上書きを行ったとしても、これらの領域に対する上書きをすることはできません。

この問題を解決した消去方式が SECURE ERASE で、2001 年に ANSI（American National Standards Institute：米国国家規格協会）によって、ファームウェア（プログラム）で設定した消去動作を実行する 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)」の手段として認定していま

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領域が更に存在すること、また実際の動作を第三者が確認することが出来ないことを理由に「Purge(除去)」に格下げされ、「実行後に全 LBA 領域に対するゼロ（全ビット 0）で 1 回の上書き抹消を行い、その後に確認作業（Verify）を行うことも要求されています。

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、「再割り当て済セクタ」に対して上書き行われるか否か、の差となります。

４．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、データ抹消の抹消は、書き込まれたデータの物理的な保存場所に対する消去ではなく、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 と標記する）」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リモー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。

5．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。また消去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、従来のアドレスを付与することで、上書きが行われたように見せています。古いデータの書いてあ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

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（以下、アドレスと標記する）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、バックグランド作業用の余剰領域が用意されており、上書きによるデータ消去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、消去の目的としている上書き対象の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余剰領域に割り当てられることがあります。

６．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上書きは、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砕・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 準拠の消去コマンドが準備されています。

７．（参考）他に行われている SSD のデータ抹消の方法

SSD のデータ消去については、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 のデータを完全に消去するコマンドの 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。

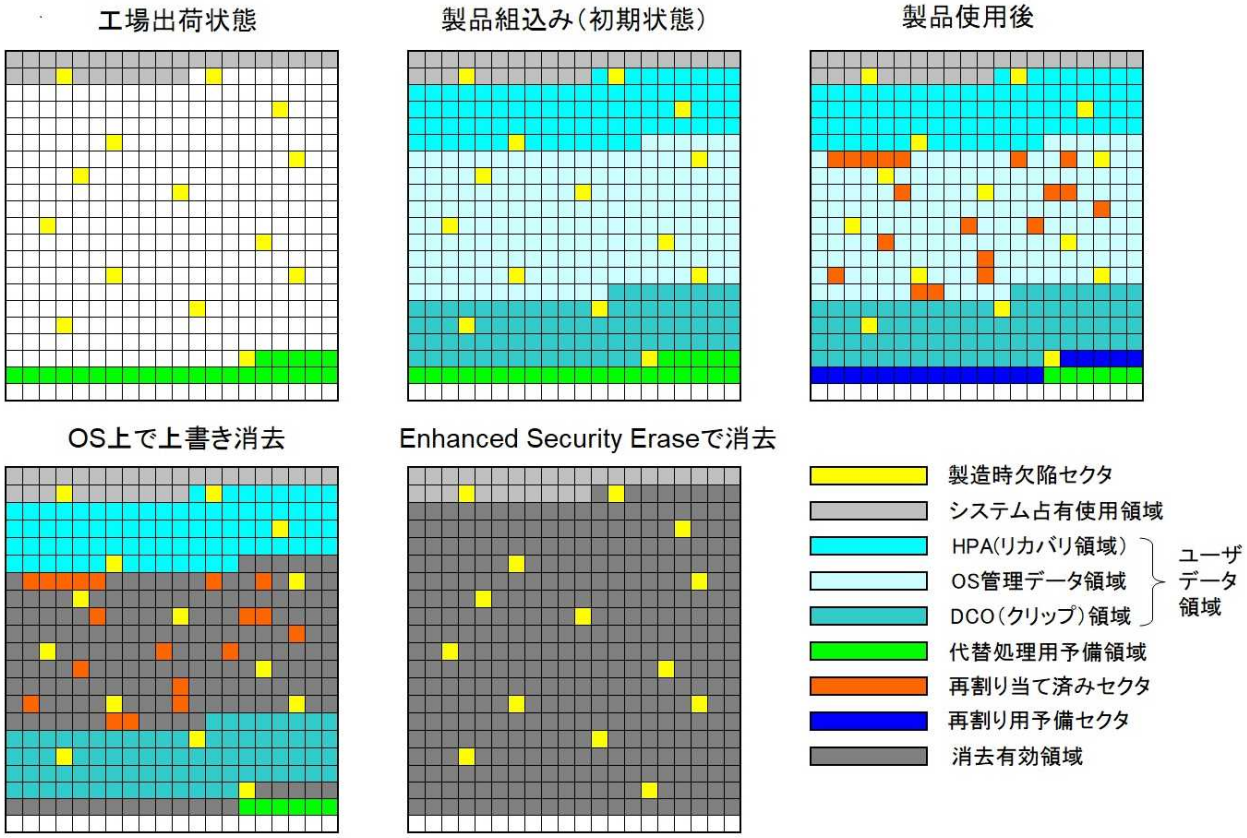
Trim は Windows7 以降の OS が持つコマンドであり、全ての OS が Trim コマンドをサポートしている訳ではありません。また、Trim は、直接的に消去を命令するコマンドではなく、不要になったページを SSD に伝えるコマンドであるため、いつブロック消去が実行されるかの保証はありません。（１時間程度でデータの復旧が不可能になったという論文もある。）データ消去を確実にするために、SSD 独自の制御として内部記録領域の情報更新を行う目的で、消去処理の最後に ATA コマンドの Standby Immediate を付加しバックグラウンド動作の促進処理を行う場合もあります。

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て、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．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 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 や、リカバリ領域等に使用する HPA 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（データ消去は行われない）。

④ OS 上で上書き消去：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消去されるが、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 で消去：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．（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	消去方法	情報の種類	対象
高 ⇧	Destroy(破壊)	物理的破壊 外部磁界等による消去	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 消去コマンド、暗号化消去	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）上書消去	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消去と 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る。

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、消去作業は不要である。⇒「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消去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。

消去方式の判断は、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。

３．PC のリユースとリカバリ領域/区画

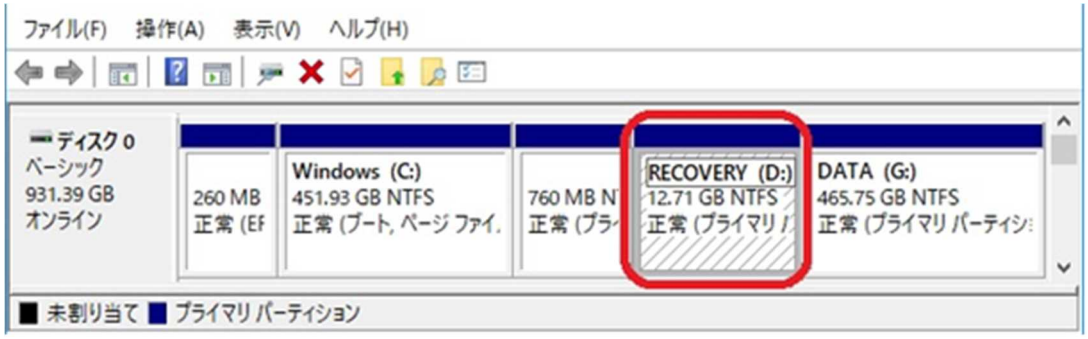
PC のデータ消去は、廃棄、レンタル、リース、リユースなど多種多様な情報セキュリティを目的としているため、媒体に記録されているユーザの作成した情報だけを消去し、購入時点の状態（初期状態）に復帰させることを目的とするデータが書き込まれている部分（リカバリ領域/区画）を消去範囲から除外することが要求される場合もあります。

１）「リカバリ領域/区画」について

PC を初期状態に戻すためのデータは、Windows XP を搭載した PC では、HDD 内に設定した OS を経由した上書きが不可能な HPA と呼ばれる領域に収納することが多く、NIST SP800-88 でも HPA の利用目的としてリカバリ領域を代表例としていますが、Windows 7（2009 年発売）以降では、HDD の大容量化によってフォーマット形式が MBR 方式から 2 TB を超える容量の取り扱いが可能な GPT 方式が主流となり、同時に OS から認識可能な領域中のパーティション（論理ドライブ：区画）を「リカバリ領域/区画」とすることが多くなり、マウント/アンマウント、アクセスも可能（NTFS フォーマット）であるため、Windows 10 の定期的な大規模なアップデートにも対応（定期的なシステムバックアップの実施など）できる利点もありますが、その反面「Clear(消去)」相当の消去方法でも、リカバリ目的のデータも区別されずに同時に消去されてしまうような弊害もあり、PC を初期状態に復帰させるためのデータが必要な場合は、データ消去を行う範囲から「リカバリ領域/区画」を除外することが必要な例が多くなっています。

・ドライブレター無しの例

・ドライブレター有りの例



２）「リカバリ領域/区画」を消去範囲から除外する場合のリスク

NIST SP800-88Rev.1 では、上書きによる消去では記憶媒体上にアクセス不能な、情報の記録が可能な部分が残存してしまうため、完全にデータを抹消するためには物理的破壊「Destroy(破壊)」が必要であるとし、OS 上で行う上書き消去では例え複数回繰り返し実行した場合でも「Clear(消去)」レベルであるとしています。上書き消去の範囲にさらにリカバリ領域/区画を加える場合には、下記のような PC の通常使用上では認識できない・存在しないはずの情報（データ）が書き込まれている場合はそのまま放置されることがリスクとして増加することになります。

①. マルウェア等と呼ばれる悪意のあるソフトウェア（コンピュータ・ウイルス）がその部分に潜んでいる場合、そのマルウェア本体

②. 上記の様な、悪意のあるソフトウェアによって、その部分に書き込まれた情報

③. ユーザの誤操作、または故意等により、その部分に書き込まれた情報

３）リカバリ領域/区画を消去範囲から除外する場合の注意点

本協議会は NIST や ISMS の、「消去レベルの選定は、情報の正当な所有者・管理者の判断によって決定すべきものである」との方針に従い、情報の所有者・管理者に対して上記のリスクを説明し、「情報漏えいなどの事象が発生した場合においてもその責任は、その消去方法を選択する判断を下した者にある」ことについて了承を得た場合に限定してリカバリ領域/区画を除外した消去を選択・実行することができるものとし、第三者にもその事実を明確に証明することのできる「データ適正消去証明書」の発行を行います。

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、データ消去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)」に適応する消去（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に対する上書き）が実行できることを認識することが不可欠であるので、本協議会の認証評価もこれに従って行われます。

（参考）現在までの調査結果では、現存するデータ消去ソフトや装置には、ATA コマンドの Security Erase Unit コマンドでは規定されていない付加機能として、消去範囲が OS を介して消去することが可能な範囲に留めることや、消去動作完了後に消去済である 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が、消去動作以前の状態で存在（情報の書き戻しと推定）するものもあるようですが、この点は認証評価の対象には含めません。また、ソフトと PC や記憶媒体との組み合わせによる問題の発生等もソフトウェアの製造・販売者の責任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消去方法の選択だけでではなく、作業環境の管理や作業者に対する教育等を含めたマネー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、データ消去作業に対しても必要十分なマネー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消去業務に限定した、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．データ消去を行ったパソコンおよび記憶媒体の情報
2．消去作業の情報として、消去実行事業者名、消去ソフトウェア名、実行日時、消去方法、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消去作業の結果、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、公開鍵ペア（公開鍵と秘密鍵）によって、公開鍵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、相手の公開鍵の真正性の確認が必要です。公開鍵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、公開鍵を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（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結合させ、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	RFC2459：X.509 標準の証明書と失効リストのプロファイル RFC****：属性証明書のプロファイル（ドラフト）
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	RFC2527：証明書ポリシ（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）
認証パス構築、検証	RFC****：認証パス構築と検証のための PKI クライアント機能の委任サーバー（ドラフト）
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ポリシーを遵守させ、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となる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（情報セキュリティマネジメントシステム適合性評価制度）

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 17799（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る。

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、認証局の定めたポリシーを遵守し、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認証局は、用途に応じて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
https://www.jipdec.or.jp/archives/publications/J0004040

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）レスポンダ

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）を登記サーバーに送信し、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）を登記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認証局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、その証明書が有効であったことを検証するために、その生成を証明する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、任意のディ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

消去したデータを巡って係争があった場合に備えて、長期的に保存する必要があります。このような長期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、今までのデータ消去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消去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、過去の消去に関する規格に囚われ、完全な消去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、適切なデータ消去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消去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、消去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きます。

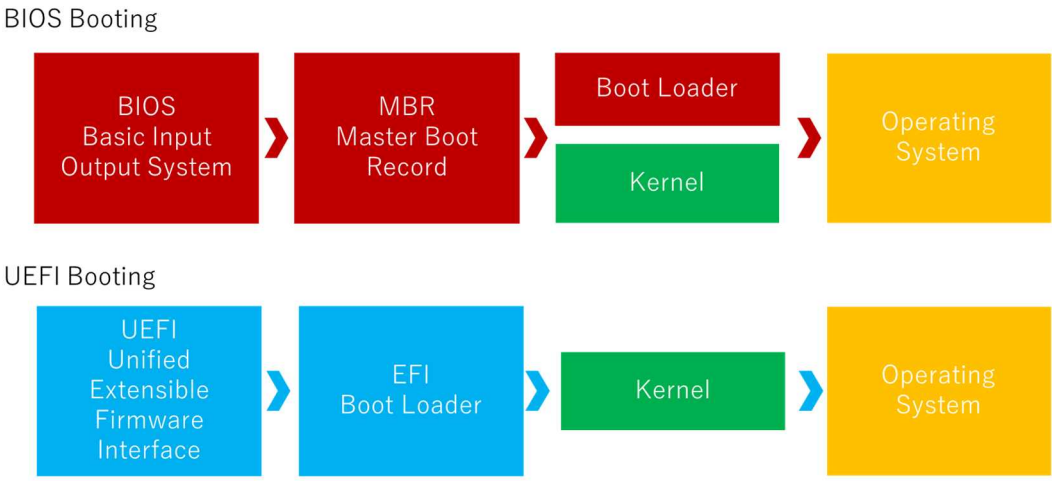
参考にした出典元：
・特定非営利活動法人デジタル・フォレンジック研究会（以下 IDF）
・一般社団法人情報機器リユース・リサイクル協会（以下 RITEA）
・一般社団法人 電子情報技術産業協会（以下 JEITA）

（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（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。



協力団体・協力者

協力団体：
一般社団法人コンピュータソフトウェア協会（Computer Software Association of Japan）

会長：荻原 紀男（株式会社豆蔵ホールディングス 代表取締役会長兼社長）
設立：1986（昭和 61 年）2 月
会員：624 社・団体（平成 31 年 4 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
CSAJ 事務局 TEL：03-3560-8440
URL：https://www.csaj.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

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

初版協力者　一般社団法人コンピュータソフトウェア協会　データ消去証明推進研究会

CSAJ 会員協力者：

主　　査：田上　利博（サイバートラスト株式会社）

メ ン バ：加藤　貴　（ワンビ株式会社）

林　　眞樹（株式会社 IDC フロンティア）

後藤　浩志（AOS データ株式会社）

小林　潤　（さくらインターネット株式会社）

関根　文彦（ファイルフォース株式会社）

小田部祥子（ファイルフォース株式会社）

小島　茂　（株式会社ユビキタス）

橋本　真之（株式会社ユビキタス）

秋保　盛征（リコージャパン株式会社）

多賀谷俊之（リコージャパン株式会社）

意見提供者：

オブザーバ：本田　正　（アドバンスデザイン株式会社）

西本　有佑（アドバンスデザイン株式会社）

服部　達也（株式会社ウルトラエックス）

沼田　理　（デジタル・フォレンジック研究会）

伴場　聖令（株式会社豊通シスコム）

山川　輝二（株式会社東芝）

梅澤健太郎（株式会社東芝）

安藤　眞　（東芝クライアントソリューション株式会社）

上原　啓一（東芝クライアントソリューション株式会社）

栗原　秀行（東芝クライアントソリューション株式会社）

濱田　圭　（富士通クライアントコンピューティング株式会社）

齊藤　俊介（パナソニック株式会社）

協力団体：

特定非営利活動法人デジタル・フォレンジック研究会

APPENDIX-1
RAID システムのデータ消去

はじめに

本 APPENDIX は、今までの PC に搭載されている記憶媒体のデータ消去を対象に、消去技術認証基準委員会が作成した「データ消去技術ガイドライン」に、複数の電子記憶媒体を搭載した、RAID・サーバと称される機器を対象とするための注意点などの追補を行うためのものです。

本 APPENDIX で用いる「抹消」とは、データ消去技術ガイドライン第 5 章と同様に、情報を消し去り、何もない状態にする「消去」だけではなく、暗号化等で内容を判別・復旧することが不可能にする行為全般を指します。

１．NIST SP800-88 上の取り扱い

ADEC が基準として取り扱っている NIST SP800-88Rev.1 では、媒体の分類として、ドライブや SSD の接続インターフェイスによる区分は存在しますが、搭載する側のシステム（機器）による区分（パーソナルコンピュータ/サーバ等の種類）での分類は存在しません。そのために実際に用いられるデータの抹消手法について解説は、データ消去技術ガイドライン第 2.2.1 版、

第 5 章 記憶媒体のデータ抹消（NIST SP800-88Rev.1）を参照してください。

２．RAID・サーバに関する注意点

RAID システムに於いては、システムの耐障害性（RAID5 の場合 1 台、RAID 6 の場合 2 台）を超える媒体のデータの抹消を行なえば機器全体のデータ抹消が完了しセキュリティーが保たれるとの考えもあるようですが、それは重大な誤解であり、システムを構成する全ての電子記憶媒体のデータの抹消を行う必要が有ることの理解を得ることが必要です。

2019 年 7 月

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

APPENDIX-1
RAID システムのデータ消去

※参考情報

【RAID（Redundant Arrays of Independent Disks）とは】
引用元：https://www.a-d.co.jp/datarecovery/knowledgecenter/raid/001.html

RAID は、1988 年にカリフォルニア州立大学バークレー校の論文によって提唱された、Redundant Arrays of Independent Disks（独立した複数のディスクの冗長性配列）を省略した呼び方であって、物理的な複数のドライブを組み合わせて冗長性を持ったディスクアレイを構成する技術を指し、RAID０は冗長性を持たないことを理由に当初はその中に含まれていなかったが、冗長性の点を除き構成上の差が少ないため、冗長性が存在しないことを現わす“０”の RAID として呼称されている。RAID はこのように歴史的には新しい技術であるが、外部記憶装置の冗長性の確保や、高速化などの性能改善を目的として、広く使われている技術である。

１．RAID の代表的な種類

１）RAID０： “ストライピング”とも呼ばれる。ドライブの高速化を目的として、データを複数に区切って、区切られた各々のデータを、複数の別々のドライブに分散して書き込むことによって、書き込みに要する時間を短縮する方法であり、冗長性は存在せず、全体を構成している複数のドライブ中の１台でも故障すると、全体の故障となってしまう（冗長性を持たない）ため、データをドライブの故障から守ることは出来ない。

２）RAID１： “ミラーリング”とも呼ばれる。“ミラー（鏡）”の呼び方が示すように、２台のドライブに、同時に同一のデータを書き込み（複製を持つ）、１ 台のドライブが故障しても、もう一方のドライブの動作によってシステムダウンを予防することが出来る。

３）RAID０１/１０： “０１”も“１０”も、上記の“ストライピング”と“ミラーリング”を二重構造に組み合わせて“RAID０”の高速性と、“RAID１”のデータ保護の双方の特徴を得ることを目的とした方法。下層の方法を先頭に表記するので、“０１”は、“RAID０”の構成を２組用意して、複製することを意味するので、双方の“RAID０”の構成が必ずしも同一の必要性は存在しない(一方が２台構成、もう一方が３台構成でも理論上は構成することが出来る)。“１０”は、“RAID１”を２組用意して、ストライピングするので、ストライピングされたデータドライブが ２ 台ずつ存在することになり、夫々が同一の構成で同一容量のドライブであることが必要でるが、障害耐性もより強固なものとなる。

４）RAID２/３/４： ほとんど使用されていないので、説明を省略する。

興味のある方は、Wiki： http://ja.wikipedia.org/wiki/RAID に詳細な説明があるので、参照ください。

５）RAID５： 現時点において最も多く使われている方法。“RAID０”のように、データを複数に区切って別々のドライブに書き込むと同時に、元のデータ群から“パリティ（誤り訂

正符号）”を生成して、データと同じように、順番に別々のドライブに記録する方式で、1 台のドライブが故障しても、データが失われるのを予防することが出来るが、最低構成でも 3 台のドライブが必要であり、全体の記憶容量は、（全構成台数－１台）分となる。“RAID５”も他の RAID との複数層構成（“RAID５５”など）を用いることが出来る。障害の無い場合の読み出し速度は“RAID０”同様に高速化が期待できるが、書き込み時は、“パリティ”の生成時間が必要なため、速度が低下する。

６）RAID６： “RAID５”をさらに発展させた方法で、“パリティ”を 2 重に持つことで、2 台のドライブが故障してもデータが失われることを予防することが出来る。2 重化された“パリティ”の生成方法に規則は存在せず、同一の“パリティ”を 2 つ持たせても、全く別の算出方法の“パリティ”でも良い。このため、最低構成でも 4 台のドライブが必要となり、全体の記憶容量は（全構成台数－２台）分となる。“RAID６”も、他の“RAID”構成と同様に複数層構成（“RAID６５”など）を用いることは勿論可能である。障害の無い場合の読み出し速度は“RAID０”同様に高速化が期待できるが、書き込み時は、二重の“パリティ”の生成時間が必要なため、“RAID５”よりも更に速度が低下する。

２．ハードウェア RAID とソフトウェア RAID

“ハードウェア RAID”とは、メイン（マザー）ボードの拡張スロットに RAID 専用の拡張ボード（RAID カード）を増設し、そのボードにドライブを接続することによって構成する方法です。このため OS からは、1 台の論理ドライブとしてしか認識されませんが、“ソフトウェア RAID”は、最近の OS の機能を利用して構成するためコスト的には安価で済ませることが出来る方法で、OS の使用している CPU を使用して論理的に構成するため、当然 CPU の負荷が増大し、通常の処理が足を引っ張られ、低速になる場合もある。

３．RAID システムの構成媒体数

RAID の種類	最小構成媒体数	最大耐障害媒体数
0	2	無
1	2	1
０１/１０	4	2
5	3	1
6	4	2

2019 年 7 月
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

APPENDIX-2
スマートフォン・タブレット型端末のデータ消去

はじめに

スマートフォン/タブレット型端末のデータ消去に関しては、業界団体である「リユースモバイル ジャパン（RMJ）http://rm-j.jp/」内の、リユースモバイル関連ガイドライン検討会が、2019 年 3 月 8 日に発表した「リユースモバイルガイドライン初版（http://rm-j.jp/pdf/RMJ_Guidelines.pdf）」内の「利用者情報の消去について」で、国内法である個人情報保護法に基づいた要求事項等を公表しており、その中で今後の方向として

EU における GDPR（General Data Protection Regulation：一般データ保護規則）の施行等、個人情報の保護に関しては、世界的にも関心が高まっている。また、米国では、国防総省や国立標準技術研究所が、情報機器の処分・消去に関して基準を設けている。ガイドラインは、将来的にそのような国際情勢や国際基準も勘案して行くべきである。

と、記載されています。

本 APPENDIX は、このような状況下で、米国の国立標準技術研究所（NIST）が発表している、情報機器の情報漏えい防止対策の基準である文書 SP800-88Rev.1 を基に、消去技術認証基準委員会が検討を行い策定した、「スマートフォン/タブレット型端末（iOS 及び Android）の情報漏えいの予防を目的とするデータ抹消のためのガイドライン」です。

本 APPENDIX で用いる「抹消」とは、データ消去技術ガイドライン第 5 章と同様に、情報を消し去り、何もない状態にする「消去」だけではなく、暗号化等で内容を判別・復旧することが不可能にする行為全般を指します。

iOS 端末（iPhone / iPad）

１．データ抹消のランクと方式（NIST SP800-88Rev.1）

Apple 社製の iPhone 及び iPad においては、ハードウェア暗号化が動作するように初期状態で設定されているため、端末上の機能を利用したオールリセット（全ての設定の初期化）を行うことで、端末を使用するうえで書き込まれた情報の暗号化消去によるデータ抹消が完了します。

※暗号化消去についての詳細は、データ消去技術ガイドライン第 2.2.1 版、
第 5 章 記憶媒体のデータ抹消（NIST SP800-88Rev.1）
４．Cryptographic Erase（暗号化消去：CE）を参照してください。

１）「Clear(消去)」、「Purge(除去)」

本体上で、設定>一般>リセット>「すべてのコンテンツと設定を消去」を実行する。

２）「Destroy(破壊)」

焼却炉で機器を焼いて細断、解砕、粉砕、または焼却する。

注意：データ抹消操作の後、マニュアル操作にて、端末の複数の領域（ブラウザの履歴、ファイル、写真など）に移動して、操作が間違いなく実行され、情報が保持されていないことを確認してください。

Android 端末

１．データ抹消のランクと方式（NIST SP800-88Rev.1）

Android 端末は、機器の製造元とキャリアによる機器の仕様に依存します。そのため、工場出荷時データリセットオプションによって得ることのできる消去のレベルは、特定の機器の設計や、記憶媒体の基本的なファームウェアなどの詳細設計に依存し、iOS 端末と同様に暗号化消去機能が有効なものも存在しますが、有効な方法を一律に規定することは困難です。

１）「Clear(消去)」、

米国で販売されている Android 4.4.2 を搭載している Samsung Galaxy S5 では、工場出荷状態に戻すためのコマンドが用意されているので、設定＞ユーザーとバックアップ＞バックアップとリセット＞工場出荷時に戻す、を実行します。 他のバージョンの Android および他の機器については、製造・販売元の発行するユーザーマニュアルを参照してください。

２）「Purge(除去)」

「パージ（除去）」に工場出荷時のデータリセットを利用しようとするデバイスであれば、機器に使用されている記憶媒体の eMMC Secure Erase または Secure Trim コマンド、またはその他の同等の記憶媒体に対して直接動作するコマンドによる消去方法が使用されていることが必要です。

３）「Destroy(破壊)」

認可された焼却炉でデバイスを焼却して、細断、粉砕、粉砕、または焼却します。

２．ADEC の推奨するデータ抹消方法（Clear）

Android 端末に対するデータ抹消について、NIST では製造元やキャリアに各端末の詳細な仕様について確認し、最も有効なデータ抹消の方法を選択することを求めていますが、NIST が対象としている米国の官公庁においては、情報の所有者・管理者である個別の官公庁が、NIST の指導に従って選択した手段を用いることが最適であると言えるのであろうが、それと同等の作業を、日本国内の民間企業における標準的なデータ抹消の方法と規定することには無理があるので、ADEC では Android 端末に使用されている記憶媒体が eMMC であるため、同様の機能を持ち、同様に NAND 型フラッシュメモリーを使用している MMC や SSD に対応するデータ抹消手法を採用することが適当であると考えます。

※eMMC とは、embedded MMC の略で、MMC のコンポーネントを BGA パッケージに入れ、電子回路基板に直接実装して用いるものです。

１）「Clear(消去)」、（NIST SP800-88Rev1. による MMC に対する記述）
組織的に承認され、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複数回上書きする。

注意：データ抹消操作の後、マニュアル操作にて、端末の複数の領域（ブラウザの履歴、ファイル、写真など）に移動して、操作が間違いなく実行され、情報が保持されていないことを確認してください。

※この方法（複数回の上書き）は、ADEC における SSD を対象としたデータ抹消ソフトウェアの消去動作検証を目的とした検体の作成時に、LBA の付与されていない余剰領域（オーバプロビジョニング）上に消去検証用のダミーデータを書き込む際に用いることでも有効性が確認されています。それにも関わらず Purge として認めない理由は、スマートフォンやタブレット型機器の場合、上書きの対象が eMMC 全体であるか、一部に留まっているかについては、データ抹消の対象となる機器の仕様に依存していることによります。

３．スマートフォン/タブレット型端末に関する注意点
１）NFC（Near Field Communication）および FeliCa などによる近距離通信や非接触型 IC カード機能は国内特有の物であり、NIST SP800-88 にデータ抹消の規定は存在しません。また、これら機能を付加する目的で、機器の内部に専用のメモリーIC を搭載している例が多く、消去ソフトウェア等を利用してデータの抹消を行うことが困難であるため、端末の所有者が事前にその機能の消去（初期化）を実行していることを確認することが必要です。

２）「LINE」に代表されるクラウド上にデータを保存する Web アプリのデータの抹消は、端末本体上に残されるキャッシュを除いて、端末本体を利用したデータの抹消は不可能であることの理解を得ることが必要です。

2019 年 7 月
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