データ消去証明推進研究会

データ消去証明　ガイドブック

2017 年 6 月

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

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市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の担保するためのび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したことによることが目立っております。PC の再利用による海外への販売や、個人向けパソコン（以下、PC）のネットオークションを利用した転売によるデータディスク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を把握したり端末の紛失や盗難の際には資産管理等で把握したりすることができますが、廃棄やリユース目的で販売したディスクからのデータ流出は悪用されてからしか漏えいがあったことを把握することができません。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サービス提供者が保管しているデータの消去は、論理的な消去のみとなり、物理ディスクの消去においての規定がありません。

このようなことから、データを消去したい側がデータを消去したこと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「データ消去証明推進研究会」を設立するものである。本研究会では、最新のデータ保管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、今後増加していく 2012 年以降の発売された Microsoft Windows 用 PC に内蔵された状態の HDD／SSD について規定策定を実施し、今後、他の OS を搭載した PC および、単体ディスク、スマートフォン、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パソコンの内蔵ハードディスク（HDD）1 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：

　機密データ抹消に関する高信頼性を社会的に実現するために以下を目的にする。PC、スマートフォン、タブレットなど（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適正抹消を行い、電子証明書による署名の業界標準ガイドラインの策定

実施主体：

　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

実施方法：

　データ抹消に関する技術、知見をお持ちの会員企業および、協会外の定例研究会への参加ならびにガイドライン策定にあたり執筆にご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、スマートフォンを含んだ IoT 機器の IT 資産の多くは、機密データを含んでおり、このデータを保護するということは重要な課題となってきます。また、今後は、ビックデータの活用の普及により、爆発的なデータの増加が見込まれます。それらの機器が保管し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れば、情報社会においての大きな問題となります。規定に基づき、完全かつ安全に機密情報の処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ことになります。

多数の厳密な業界基準および政府規制により、企業の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強制されました。そのため組織は、情報漏えいを防ぐために取っている手段を証明するための証跡管理を行う環境を持つことを求められています。証跡の証明することを法令化し市民および刑事責任のみならず、財務責務、会社の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され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 に対して詳細かつ実効的な手順を定めた法令がなく、組織の判断に任せられている。IT 犯罪における証拠保全＝データフォレンジックという点からは好ましいことではあるが、リユースや廃棄する立場からみると、大きなリスクとなっている。

２）日本の各団体における消去への取り組み

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。
出典：ISO/IEC27001:2013

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

本章では、PC における状況について紹介いたします。

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ったが、ノート型やタブレット型の 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 で全て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、個人情報保護法が施行された以降、この保存されたデータの取扱いが非常に重要となっています。普段の業務利用においては、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・盗難の場合、また、PC の廃却や再利用の場合に、PC に保存されたデータの漏えいを防ぐために、データの消去は重要となっています。

PC 内蔵記憶媒体のデータ消去を行うためには、その内蔵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 の内蔵記憶媒体は、磁気ハードディスクからフラッシュメモリの大容量化/低価格化により、メモリディスクの採用が増えてきています。またインターフェースの仕様は、IDE から ATA や PCIe などへとより高速なインターフェースへ進化しています。

また、記憶媒体の容量も急激に増えており、磁気ハードディスクでは、数テラバイト(TB)もの容量になっています。

また、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、取り外すことが出来なくっており、内蔵記憶媒体を取り出して記憶媒体単体でのデータ消去が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だったが、2012 年(Windows 8)以降殆どの PC では、BIOS に変わって UEFI（Unified Extensible Firmware Interface)が採用されているため、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パーティション形式（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)があったが、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が利用できるようになっており、今後大容量のデータに対する消去方法及び実施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、その目的(廃棄/再利用/遠隔消去など)や状態(媒体単体/PC 内蔵)に適した方法で行うことが重要です。

第４章　データの特性ごとの消去の選択

１）データの特性について

データ消去をビジネスとして請け負っている企業にヒヤリングを実施いたしました。データ消去を依頼してくる顧客は、ほとんどが法人団体で個人での委託は年に数件程度となります。法人顧客としては、主に上場している会社が多く、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る。また、第三者機関による消去を実施した証明書の保管を義務付けております。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 の 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が、近年では、米国国立標準技術研究所が NIST SP800-88 で、「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」と記載したものを、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）が和訳を公開しています。また、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触れると共に、上書き後のベリファイを推奨しています。

IPA/ISEC は、 政府や企業の経営者、セキュリティ担当者などが、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、一般に公開
https://www.ipa.go.jp/security/publications/nist/

２）現状の消去方式の選択方法

消去方法においては、データの特性からデータ消去方法の選択ではなく、消去業者に一律に同じ方法で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依頼されるが同じように、PC の保存されているデータ種類や特性に関係なく、一律に同じ方法を選択されることが多いとのことです。

データ消去請負会社は、複数の消去方法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ようになっております。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）を無償で提供し、個別の消去証明書においては有償とし、ソフトウェアの場合は、消去ソフトから出力されるフォーマットを利用、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の画像を添付し提供しております。また、消去方式以外に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、項目としては作業現場の入館制限、外部接続された機器の排除、作業員への研修制度、複数人の結果検証などがあげられます。そのため、消去方式よりも消去する際の環境や場所などのマネジメントによってセキュリティレベルが大きく影響されることになります。今後は、実施した環境をランク分けすることにより、より信頼度の高い証明となります。

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 円とは幅があります。

※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　データ消去の証明とは

ディスクの種類や保管方法によってデータを完全に消去したことを証明するのは非常に困難であることがわかります。このため消去ソフトウェアによりデータを完全に上書きし消去ログを残すことや、物理的破壊の証拠を残すことにより消去の証明を行っています。

１．HDD の消去証明

１）ソフトウェアによる消去

一般社団法人 情報機器 リユース・リサイクル協会（RETIA）では、専用消去ソフトウェアでデータを上書き後に専任のデータ復元業者へ依頼し、データを復元することができなかったソフトウェアのみを RITEA 認証の消去ソフトウェアとして紹介しています。

・RITEA データ消去方式に対する見解

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、「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。
HDD にインストールされた OS に依存せず、OS やファイルが壊れて起動でき

なくなった場合でも、HDD データ消去ができること。
但し、今回の対象機器分野は、PC・ワークステーション・サーバ(全て「x86」系アーキテクチャー)としています。

・HDD データ消去ソフトウェア資格の調査内容

当協会が今回認定する PC 用 HDD データ消去ソフトウェア資格の調査内容は、以下のものから構成されています。

（1）評価内容

	調査項目	調査内容	調査方法
1	データ消去評価	データ消去後、間違いなくデータ消去されていること。	HDD の全てのセクタの内容について、消去ソフトウェアと別な専用ソフトウェア、または専用装置を用いて、消去確認を行う。
2	OS 非依存性評価	OS とファームウェアの間のソフトウェアインターフェースが UEFI か BIOS であるか、また、データ消去可能な PC の OS 名が HDD データ消去ソフトウェアのカタログ等の仕様に明示されており、UEFI または BIOS の適用範囲内で、HDD にインストールされた OS に依存せず、消去が可能であること。	消去ソフトウェアがそれ自身で起動及び実行できることの確認を行う。
3	HDD 不具合検出評価	HDD に何らかの異常があった場合にそれを検出できること。	コントローラー異常やプラッタ（HDD の円盤部）異常のサンプル HDD に対してデータ消去を行った場合に、エラーを表示し、作業を一度停止することの確認を行う。
4	処理終了メッセージ評価	消去処理が終わった場合のメッセージ出力、またはログ（履歴管理）ファイルに記録された内容が適切であること。	正常終了または異常終了のメッセージやエラー情報が、表示またはログファイルに設定されていること等の確認を行う。
5	証明書機能評価※	データ消去後に、情報を収集してデータ消去作業終了（完了）書の電子データが作成できること。または、データ消去作業終	消去ソフトウェアでこの作業が行えることの確認を行う。

		了（完了）書の元となる情報を収集して、表示またはログファイルに記録することができること。 この情報とは、 1．消去日時 2．PC 装置の型名 3．PC 装置の製造番号 4．消去方式 5．HDD の型名 6．HDD のシリアル番号 7．HDD 容量 を示す。	

2）磁気消去システムによる消去

ハードディスクの型番や製造番号などの消去作業の記録（消去ログ）を残すことにより消去の証明に使用します。

3）物理的破壊

ディスクを物理的に破壊した場合は、ハードディスクの型番や製造番号などの写真を撮り消去の証明として使用します。

2．SSD のデータ消去

SSD のデータ消去については、現在、ガイドラインに相当するものは、NIST の SP800-88rev.1 があるが、技術の進歩が急速なため、ガイドラインの改訂が今後の課題となっています。現時点では次に記載するような SSD の特性を踏まえたデータ消去のガイドラインとして、HDD と同様に消去のログを残すことにより、消去の証明として使用します。

■ SSD データ消去の特性

1）データ消去方式（ブロック消去）

SSD はデータの書き換えをページ単位で行うことができません。ブロック単位でデータを消去した上で、新しいデータを書き込むことになります。ブロック消去の際には、元々あったデータは他のブロックにコピーされるためデータが残ってしまうことになります。

2）ウェアレベリングと予備ブロック

SSD に搭載されている NAND 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、SSD に搭載されているコントローラ

ーは各ブロックの書き込み回数を平準化するようにウェアレベリングを行っています。

また、SSD には予備ブロックが用意されており、ゼロライト方式等の上書きによるデータ消去を実施すると、ウェアレベリングにより上書き対象のブロックには書き込みは行わず予備ブロックに書き込みを行い、元のブロックはデータが残ったまま予備ブロックとなることがあります。

■ SSD データ消去の方法

1）Secure Erase

SSD の多くは、データを完全に消去する Secure Erase のコマンドが用意されています。本コマンドを用いて SSD データ消去を行う方法です。

（課題）

以下のことより Secure Erase を利用したデータ消去が実行できないことがあります。

・SSD メーカーが仕様を公開していないため利用できないケース

・PC メーカーが UEFI（BIOS）で、Secure Erase を防止する機能（フリーズロック）を実装し、Secure Erase が利用できないケース

2）Crypto Erase

SSD のデータを削除するのではなく、データを強固な暗号アルゴリズムで暗号化し、第 3 者による閲覧を不可能にするデータ消去を行う方法です。

（課題）

暗号化技術が輸出規制に該当するため、本データ消去方法は国内のみで運用となります。

3）上書き消去

SSD の特性（ウエアレベリングや予備ブロック等）を考慮し、特定しない英数字によるパターン等で 2～3 回以上書き込みを行い、元データを上書きするデータ消去方法です。

（課題）

不良ブロックがある場合には、同ブロック内のデータは消去できません。

4）Format & Trim

SSD を Format した後、Trim コマンドによってデータを完全に消去する方法です。

（課題）

SSD が Trim コマンドに対応していない場合には、完全なデータ消去が行えません。

5）物理破壊

SSD が正常に動作しない場合は、1）、2）、3）、4）の方法によるデータ消去を行うことができません。その場合には、以下のいずれかの方法を行う必要があります。

・強制的に電荷をかけるデータ消去

・HDD のような穴開けでは無く、NAND フラッシュメモリを確実に破壊するための万力等による破壊

（課題）物理的な破壊のため、SSD をリユースできません。

データ消去を確実にするためにも、SSD 独自の制御として内部記録領域の情報更新を行うための処理が必要な場合がある。例えば消去処理の最後に ATA コマンドの Standby Immediate を実行する等である。

第６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、本人認証など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る。

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になります。その場合に、鍵配布の場合もデジタル署名の場合も、相手の公開鍵は本当に正しいものであるかどうかになる。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生成を防ぐためには、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証明書とする必要があると考える。このために信頼できる第三者機関（CA：Certification Authority）が、公開鍵が発行する PC（ディスク）を証明する時限設定をした秘密鍵を用いて消去を実行後に公開鍵を発行して証明書を発行する仕組みとする。CA は消去前の秘密鍵と消去完了後の証明書の公開鍵を結合させ、CA の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）相手の公開鍵の有効性を信用することができる。

（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いたします。

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 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（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る。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、 ケーブルラックなどの設備から、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。

電源設備

安定的な受電、停電や法定点検など、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。

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。

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など、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。

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。

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などを実現する。

侵入検知対策

侵入検知システム(IDS/IPS)などによる、不正アクセス検知、マルウェアやウイルスチェックなど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など、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など、幅広い対応を行う。

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。

・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来年から始まる。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ある。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する。

・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る。これ等の基準はかなり厳しい内容となっている。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る。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など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る。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などを義務付けている。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る。また認定は 1 年で、継続する場合再調査を受けることを義務付けている。

４．登録業務の信頼性と運用

登録機関やリポジトリなど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る。

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、失効などの認証サービスを提供する認証局が、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る。

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

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 クライアントなど）がある。

・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、消去したディスクが正しいプロセスで消去したことを証明するためのフローを表しています。最初に、消去したいディスクが入った 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）を登記サーバに送信して秘密鍵（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（ディスク情報）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。

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）に送る。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る。

・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る。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する。

第８章　まとめ

PC やディスク装置の進化や大容量化等に伴い、今までのデータ消去の手法が適応できず、ディスクの特性に適している消去方法を選択せざる得ない状況になっております。そのため知識を有する専門家の作業が必要で作業時間も増える傾向にあり、結果的には最適なデータ消去を実施せず、情報漏えいの事故が度々ニュースで取り上げられる事態となっています。

また、昨年よりマイナンバー制度が開始され、「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、機器及び電子媒体を廃棄する場合は専用のデータ削除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な手段を採用し、「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、不法投棄が行われていても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 3 者機関による PC 製造番号、HDD シリアル番号が記録された「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が万全でないと、作業待ちの一時保管段階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・監視等の物理セキュリティシステムの導入が徹底されていることを認定することが必要です。

このようなことから、本研究会では、「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果となりました。

第 9 章　参考情報

データ消去を証明するにあたり、消去技術においては、以下の団体において、データ消去の規定や技術について調査を実施し、規定しております。データ消去証明推進研究会では、このような団体の調査結果をもとに消去証明における規定を行っていきます。

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。I 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する。

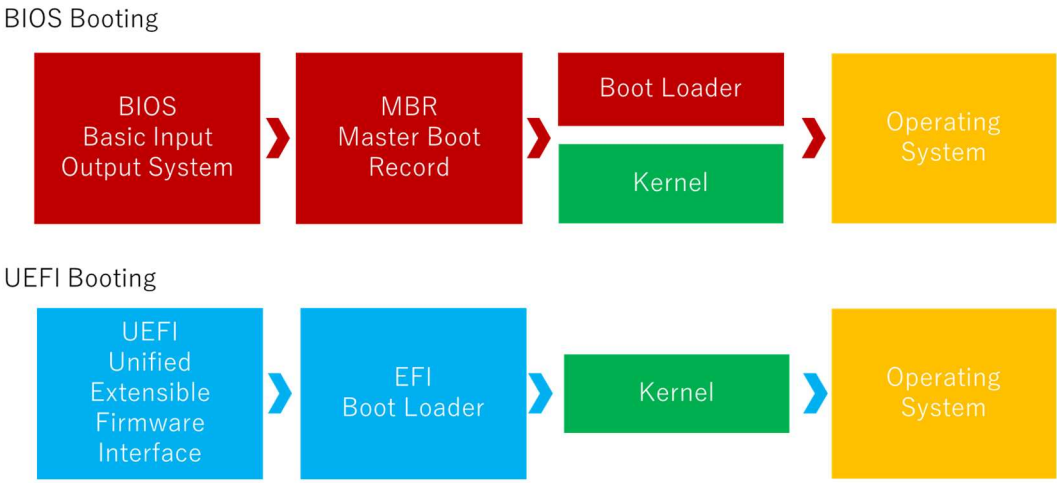
（参考）データ取り扱い機器の進化

BIOS と UEFI の違いによる消去について

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。



実施団体・協力団体・協力者

実施団体：
「イノベーションをリードするソフトウェア集団」
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 代表取締役社長）
設立：1986（昭和 61 年）2 月
会員：416 社・団体（平成 26 年 8 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。
活動：委員会・研究会を通して、ソフトウェアに係わる政策提言とりまとめ、調査研究、ベンチャー育成、情報交換、人的交流活動などを行う。また、各種セミナー・研修や視察ツアーなどを企画・開催し、旬な話題を情報発信。若手プログラマ発掘を目的とした U-22 プログラミング・コンテストの事務局を運営。世界最先端の技術・製品・サービス等が発表されるアジア最大級の IT エレクトロニクス産業のイベント「CEATEC JAPAN」を主催。など。
事業：プライバシーマーク審査事業、認定試験事業、パッケージソフトウェア品質認証事業を実施。

○ご入会に関するお問い合わせ先
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

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

データ消去証明ガイドブック

2017年6月14日　第1.0.0版

Computer Software Association of Japan
一般社団法人コンピュータソフトウェア協会
〒107-0052
東京都港区赤坂1-3-6
赤坂グレースビル
TEL：03-3560-8440
FAX：03-3560-8441
http://www.csaj.jp/