県情報を保存するために使用した情報機器からの情報流出防止策

令和２年１月

総務局 ICT 推進部情報システム課

目 次

用語の定義　本書で使用する用語は次のとおり定義する。

リース契約	サーバやパソコン等県で使用する情報機器の賃貸借契約
県職員	リース契約を締結、もしくは実際にサーバやパソコン等を使用、管理している神奈川県の職員
契約事業者	リース契約を締結している事業者（リース元）もしくは正当な手続きを経て業務の全部又は一部を実施する事業者
抹消措置	全ての情報を消去した上、復元不可能な状態にする措置 （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（平成 30 年 9 月版））
情報機器	サーバやパソコン等、県のデータを保存したり、一時的に利用する機器
県の管理下	県職員の作業や確認ができる状態や場所（サーバ等機器の設置場所が原則）
契約事業者への返却前	情報機器を県の管理下から搬出する前の状態（管理責任は県）
契約事業者への返却後	情報機器を県の管理下から搬出した後の状態（搬送中を含む、管理責任は契約事業者）
磁気破壊専用装置	ハードディスクに強力な電気を瞬間的に照射し磁場を作り出すことで、電磁的記録を破壊しデータ復元できなくする装置
物理破壊専用装置	ハードディスクや SSD を粉砕、穿孔、変形することで、ドライブから情報を読み取ることができないよう物理的に破壊する装置
データ消去専用ソフトウェア	ハードディスクに保存されたデータを上書きすることで、データ復旧ソフトウェアを使用しても、データの復元ができないようにする専用ソフトウェア（ここでは外部権威機関の認証があり、県の検証により有効性が確認できたもののみ対象とする）
シリアル番号	情報機器の記録媒体部分（HDD 等）に割り振られた個体を識別するための機器固有番号
NIST	米国国立標準技術研究所 SP800-88：NIST が発表した、最新のデータ抹消に関する世界的な規格文書

■ 第一章 概要

1 目的

令和元年 11 月 26 日に発覚し、12 月６日に公表した「県がリース契約満了により返却したハードディスクの盗難（以下「本件」という。）」では、リース会社からハードディスク（以下「HDD」という。）のデータ消去（物理破壊）作業を請け負ったデータ消去会社の社員により、作業前のHDD18 本が盗まれ、オークションにより転売された。

当該HDDはデータが存在しないフォーマット後の状態であったが、購入者が９本のHDDにデータ復元ソフトウェアを使用したことで、県のデータが外部に出てしまう結果となった。

このことで、県民に対し多大なる不安と心配をかけると同時に、県の情報管理に対する信用が著しく失墜してしまったため、徹底的な原因究明とそれに基づく再発防止策を早急に策定、実施することで、二度と県の情報が外部に出ないよう、時代に即した情報管理を実践する。

2 原因

本件においては、契約関係の中で不法行為（盗難）が行われたことで、県の情報が外部に出てしまった一次的な要因もあるが、県がリース会社と締結していた契約内容が不完全であり、また履行確認作業の不備等、県の対応に多くの課題があったことが根本的な原因である。

また、個人情報を含む重要情報が保存されていた HDD 等のデータ消去についても、従前からの方法に甘んじており、不法行為であっても起こりうるリスクとして想定できていなかったことも原因の一端である。

原因１　契約内容不備・リース元の責務が不明確
・データ消去作業の実施主体が不明確
・データ消去方法、対象が不明確
・データ消去証明書の内容が不明確
・データ消去証明書の提出期限なし

原因２　県の監督責任・機器返却後は関与なし
・データ消去作業立会い未実施
・データ消去証明書の提出に対する督促不備

3 基本方針

徹底した再発防止と適正かつ厳格な情報管理を行うため、抹消措置実施の基本方針を次のとおり定める。

基本方針１　**Ⅰ個人情報、Ⅱ重要情報を含む場合の抹消措置**
住民情報等の重要情報が大量に保存された機器内部の記録装置については、物理的破壊または磁気的破壊により抹消措置を行う（令和元年 12 月６日付「総務省事務連絡」）

基本方針２　**Ⅲ公開情報のみの場合の抹消措置**
Ⅰ個人情報、Ⅱ重要情報を含まない機器内部の記録装置については、物理的破壊または磁気的破壊もしくはデータ消去専用ソフトウェアによる抹消措置を行う

基本方針３　**基本方針１、基本方針２とも機器が県の管理下にあるうちに、抹消措置の作業完了までを職員が立ち合い確認することで、絶対に情報漏洩を起こさない**

4　対象･範囲

本件を受け策定する再発防止策は、情報を保存する機器、保存する情報の種別により、基本方針に基づいて対策方法を分類する。なお、リース契約ではなく買い取りを行った機器についても同様とする。また、情報を保存する機器等が県の管理下にない ASP サービス、クラウドサービスについては、対応方法を別途検討する。

5　個別実施手順

本書は、３の基本方針と４の対象・範囲に基づき全所属が守るべき「県情報を保存するために使用した情報機器からの情報流出防止策」をまとめたものであるが、各章に規定されている内容を逸脱、拡大解釈しない限りにおいて、各局の実情に合わせて個別の実施手順を作成できるものとする。

ただし、個別実施手順の作成においては、その内容について施行前に情報システム課の承認を受けるものとする。

6　個別事案対応

本書は、県が扱う情報の流出を防止するため全庁的に守るべき対策基準をまとめたものであるが、どうしても原則に従った対応が困難な場合には、個別の事情について情報システム課及び関係所属と事前に協議し、対応方法を検討するものとする。

ただし、その場合においても、３の基本方針に反する対応は認めないものとする。

■ 第二章 対策

1 **対策 1**

（1）抹消措置の方法

ア　契約事業者への返却前　➡　**① データ消去（専用ソフトウェア又は磁気的破壊）【県職員】**
② 磁気的破壊【契約事業者】
③ 物理的破壊【契約事業者】

（ア）　職員によるデータ消去（専用ソフトウェア又は磁気的破壊）を実施してから、更に契約事業者による磁気的破壊及び物理的破壊を行う
（イ）　職員による磁気的破壊によるデータ消去は、専用ソフトウェアによるデータ消去が困難なサーバ等に限って実施
（ウ）　磁気的破壊は専用の装置を使用し、マーカーでの確認やログを記録するなど実施結果が可視化できること（職員の磁気的破壊は情報システム課が提供する装置を使用して実施）
（エ）　粉砕、穿孔、変形等、ドライブから情報を読み取ることができないよう、HDD を物理的に破壊
（オ）　HDD の場合は磁気ディスクが、SSD の場合はフラッシュメモリがすべて確実に破壊される専用機器による処理であること
（カ）　抹消措置の実施有無を目視で確認できないことから、磁気的破壊のみの抹消措置は不可
（キ）　物理的破壊のみの抹消措置でも、データを復元できる恐れがあることから磁気的破壊と合わせた抹消措置が必要
（ク）　県の管理下で、職員（２名以上）確認のもと磁気的破壊及び物理的破壊を実施
（ケ）　検査用機器や医療用機器等、専用ハードウェアやセンサ等を含め構成される特殊な情報機器については、製造メーカ等に物理的破壊の方法等を確認する

イ　契約事業者への返却後　➡　**④ 産業廃棄物として処理【契約事業者】**

（ア）　契約事業者は再度抹消措置を行う必要はない
（イ）　物理的破壊を行った HDD は、産業廃棄物として金属リサイクルや最終処理を行う
（ウ）　契約事業者は再委託を行う産廃事業者について、事前に県に書面等による確認をとる

（2）抹消措置の対象

サーバに搭載されているＨＤＤ（Ⅰ個人情報、Ⅱ重要情報を保存したもの）
・ディスク装置のHDDを含む

（3）抹消措置の実施場所

契約事業者への返却前　➡　**サーバ等機器の設置場所（県の管理下）**
・県コンピュータセンターに設置した情報機器はデータセンター施設内
・県施設に設置した情報機器は設置施設内

（4）留意事項

ア　HDDの取り出し作業
・サーバからHDDを取り出す作業を県職員が実施した場合、破損により損害賠償が生じる可能性があることから、抹消措置は原則契約事業者が実施する

イ　買い取り機器

・買い取り機器の場合は、情報システム課の指導・支援のもと、県職員がすべて（１－① ～ １－④）の抹消措置を行う

（５）抹消措置実施後の確認

ア　契約事業者への返却前　➡　**目視確認（チェックリスト記載）と写真記録**

（ア）　対象のＨＤＤであることをシリアル番号により確認し、物理的破壊を施されたことを県職員が目視確認しチェックリストに記載

（イ）　抹消措置実施後は、シリアル番号と物理的破壊が分かるよう写真で記録

イ　契約事業者への返却後　➡　**マニュフェストを含む処理完了報告書**

（ア）　産業廃棄物処理の実施は、マニュフェスト（産業廃棄物管理伝票）と処理時の写真記録を含む処理完了報告書により確認

（６）抹消措置実施手順

ア　抹消措置計画の作成

（ア）　物理的破壊を行うＨＤＤのシリアル番号を一覧化（チェックリスト）するとともに、処理の方法、対象物及び本数、場所、実施日等について計画を作成する【県職員】

（イ）　上記計画について、所属長の承認を受ける【県職員】

イ　抹消措置の実施

（ア）　必ず複数名立会いクロスチェックを行う【県職員】

（イ）　サーバ（またはディスク装置）のＨＤＤのシリアル番号を確認し、データ消去専用ソフトウェアによる上書き消去を行う【県職員】

（ウ）　サーバ（またはディスク装置）からＨＤＤを取り出す【契約事業者】

（エ）　シリアル番号により対象のＨＤＤであることを確認する【県職員】

（オ）　ＨＤＤの磁気的破壊を行い、磁気照射ログを取得する【県職員】

（カ）　ＨＤＤを物理破壊専用装置で破壊する【契約事業者】

（キ）　ＨＤＤのシリアル番号と物理的破壊がわかるよう写真撮影する【県職員】

（ク）　ＨＤＤのシリアル番号一覧（チェックリスト）を確認し、契約事業者にサーバ（ＨＤＤ含む）を引き渡す、また、授受簿等により引き渡しを記録する【県職員】

ウ　抹消措置実施後（契約事業者への返却後）の確認

（ア）　シリアル番号一覧（チェックリスト）と撮影した写真により処理完了を所属長に報告し、確認印をもらう【県職員】

（イ）　契約事業者が提出する処理完了報告書（マニュフェスト、産廃処理時の記録写真を含む）により、最終処分を確認する【県職員】

■ 第二章 対策

2 対策２

（１）抹消措置の方法

ア　契約事業者への返却前　➡　**① データ消去専用ソフトウェアによる上書き消去【県職員】**

（ア）　上書き回数は１回以上とする
※DoD 方式（３回上書き）やグートマン方式（35 回上書き）等の複数回以上の上書きを求める方式もあるが、「技術の高度化により現在では、１回上書きすることによる消去で十分（NIST SP800-88）」とされている

（イ）　ユーザデータ領域（リカバリ領域、OS 管理データ領域、クリップ領域）を対象に処理を行う

（ウ）　代替処理用予備領域、再割り当て済みセクタ、再割り当て用予備領域も対象に含め処理を実施することを推奨

（エ）　SSD の場合 SECURITY ERASE UNIT コマンドによる実施を推奨（ファームウェアに実装している場合）

（オ）　データ消去専用ソフトウェアは、検証（外部権威機関の認証、県組織内による検証）によりデータ消去の有効性が確認されたもののみ使用可

（カ）　データ消去専用ソフトウェアは、データ消去の完了が画面で確認できること

（キ）　県の管理下で、職員（２名以上）確認のもとデータ消去を実施

イ　契約事業者への返却後　➡　**② データ消去専用ソフトウェアによる上書き消去【契約事業者】**

（ア）　県がデータ消去を実施しているが、再度同様の抹消措置を行う

（２）抹消措置の対象

ア　**サーバに搭載されているＨＤＤ（Ⅲ公開情報のみ保存）**
※破損等によりＨＤＤがソフトウェアによるデータ消去ができない場合は、対策１を実施

イ　**パソコン機器内部のＨＤＤ又はＳＳＤ**

（３）抹消措置の実施場所

契約事業者への返却前　➡　**サーバ等機器の設置場所（県の管理下）**

・県コンピュータセンターに設置した情報機器はデータセンター施設内
・県施設に設置した情報機器は設置施設内

（４）留意事項

ア　作業実施者
・サーバ、共通利用パソコン、所属調達パソコンともに、県職員がサーバ等機器の設置場所において、上書き消去を行う

イ　買い取り機器等
・機器の再利用を行わない場合（買い取りを含む）、または破損等によりＨＤ又はＳＳＤがソフトウェアによるデータ消去ができない場合は、対策１（物理的破壊-産廃処理）を実施

（５）抹消措置実施後の確認

ア　契約事業者への返却前　➡　**画面による完了確認（チェックリスト）と写真記録**

（ア）　ＨＤＤ又はＳＳＤがデータ消去されたことを県職員が画面により確認

（イ）　サーバの場合、対象のＨＤＤであることをシリアル番号により確認（チェックリスト）

（ウ）　パソコンの場合、対象のパソコンであることをエンドシステム番号とシリアル番号により確認（チェックリスト）

（エ）　抹消措置実施後は、データ消去完了画面とシリアル番号（パソコンの場合はエンドシステム番号とシリアル番号）が分かるよう写真により記録

イ　契約事業者への返却後　➡　**データ消去証明書（写真添付、シリアル番号等が確認できる一覧）**

（ア）　契約事業者が行うデータ消去は、データ消去証明書（対象機器の処理が完了したことが分かる写真を添付）により確認

（６）抹消措置実施手順

ア　抹消措置計画の作成

（ア）　専用ソフトウェアによりデータ消去を行うＨＤＤ又はＳＳＤのシリアル番号（パソコンの場合はエンドシステム番号とシリアル番号）を一覧化（チェックリスト）するとともに、処理の方法、対象物及び本数、場所、実施日等について計画を作成する【県職員】

（イ）　上記計画について、所属長の承認を受ける【県職員】

イ　抹消措置の実施

（ア）　県職員は必ず複数名立会いクロスチェックを行う【県職員】

（イ）　ＨＤＤ又はＳＳＤのシリアル番号（パソコンの場合はエンドシステム番号とシリアル番号）を確認し、データ消去専用ソフトウェアによる上書き消去を行う【県職員】

（ウ）　シリアル番号（パソコンの場合はエンドシステム番号とシリアル番号）と消去完了画面がわかるよう写真撮影する【県職員】

（エ）　契約事業者にサーバ（ＨＤＤ含む）またはパソコンを引き渡す、また、授受簿等により引き渡しを記録する【県職員】

ウ　抹消措置実施後（契約事業者への返却後）の確認

（ア）　シリアル番号（パソコンの場合はエンドシステム番号とシリアル番号）一覧（チェックリスト）と撮影した写真により処理完了を所属長に報告し、確認印をもらう【県職員】

（イ）　契約事業者が提出するデータ消去証明書により、契約事業者が再度データ消去を実施したことを確認する【県職員】

■ 第二章 対策

3 対策３

（１）抹消措置の方法

ア　契約事業者への返却前　➡　**① 機器付属の初期化ツールによる消去【県職員】**

（ア）　機器付属の初期化ツールによる消去は１回とする
※「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が可能（NIST SP800-88Rev.1)」とされている

（イ）　全ての設定の初期化後、初期設定画面表示が確認できること

（ウ）　県の管理下で、職員（２名以上）確認のもとデータ消去を実施

イ　契約事業者への返却後　➡　**② 機器付属の初期化ツールによる消去【契約事業者】**

（ア）　県が全ての設定の初期化をしているが、再度同様の抹消措置を行う

（２）　抹消措置の対象

タブレット（iOS 端末）

（３）抹消措置の実施場所

契約事業者への返却前　➡　**タブレットの使用場所（県の管理下）**

（４）留意事項

ア　買い取り機器等

・機器の再利用を行わない場合（買い取りを含む）、または破損等によりタブレットが初期化ツールにより全ての設定の初期化ができない場合は、対策１（物理的破壊-産廃処理）を実施

（５）抹消措置実施後の確認

ア　契約事業者への返却前　➡　**画面による完了確認（チェックリスト）と写真記録**

（ア）　タブレットの全ての設定の初期化されたことを県職員が画面（初期設定画面表示）により確認

（イ）　対象のタブレットであることをシリアル番号により確認（チェックリスト）

（ウ）　抹消措置実施後は、初期設定画面とシリアル番号が分かるよう写真により記録

イ　契約事業者への返却後　➡　**データ消去証明書（シリアル番号等が確認できる一覧）**

（ア）　契約事業者が行う全ての設定の初期化は、データ消去証明書により確認

（６）抹消措置実施手順

ア　抹消措置計画の作成

（ア）　機器付属の初期化ツールにより全ての設定の初期化を行うタブレットのシリアル番号を一覧化（チェックリスト）するとともに、処理の方法、対象物及び本数、場所、実施日等について計画を作成する【県職員】

（イ）　上記計画について、所属長の承認を受ける【県職員】

イ　抹消措置の実施

（ア）　県職員は必ず複数名立会いクロスチェックを行う【県職員】

（イ）　タブレットのシリアル番号を確認し、初期化ツールによる消去を行う【県職員】

（ウ）　シリアル番号と消去完了画面（初期設定画面）がわかるよう写真撮影する【県職員】

（エ）　契約事業者にタブレットを引き渡す、また、授受簿等により引き渡しを記録する【県職員】

ウ　抹消措置実施後（契約事業者への返却後）の確認

（ア）　シリアル番号一覧（チェックリスト）と撮影した写真により処理完了を所属長に報告し、確認印をもらう【県職員】

（イ）　契約事業者が提出するデータ消去証明書により、契約事業者が再度データ消去を実施したことを確認する【県職員】

■ 第二章 対策

4 情報機器・保存情報別の対策

情報機器	保存情報	対策方法
サーバ	Ⅰ 個人情報、Ⅱ 重要情報 を含む	**対策 1**
	Ⅲ 公開情報 のみ	**対策 2**
パソコン	–	**対策 2**
タブレット	–	**対策 3**

■ 第三章 契約

本件発生の主原因であるリース契約内容の不備を検証し、今後の再発を徹底的に防止するため、リース契約において情報機器を調達する際の記載事項（特記事項、仕様書）や留意する事項を定める。なお、特別な記載がある項目を除き、リース契約ではなく買い取りにより情報機器を調達する場合においても同様とする。

1 シリアル番号の管理

契約開始から終了（最終的な抹消措置の完了）までの全ての期間、記録媒体を適切に管理するため、リースする情報機器のシリアル番号の提出を契約事業者に義務付ける。また、情報機器内の記録媒体の更新等の際は、速やかに情報の更新を行う。

2 抹消措置計画

リース契約満了の遅くとも１カ月前までに、情報機器の抹消措置に係る実施計画（抹消措置実施事業者、スケジュール、手法等）の提出を義務付ける。

3 抹消措置の実施

（1）対 策 1

契約事業者への返却前に、県がデータ消去専用ソフトウェアによるデータ消去を行うための期間（抹消措置計画内で決定、ただし１カ月を超えない範囲とする）を設定する。

第二章１（６）イのとおり、サーバ等機器の設置場所において県職員立ち合いのもと、磁気的破壊及び物理的破壊による抹消措置を実施するとともに、産業廃棄物処理業者発行の廃棄証明書の写しの提出を、契約事業者に義務付ける（抹消措置計画内で決定、ただし２カ月を超えない範囲とする）。

（2）対 策 2

契約事業者への返却前に、県がデータ消去専用ソフトウェアによるデータ消去を行うための期間（抹消措置計画内で決定、ただし１カ月を超えない範囲とする）を設定する。

契約事業者への返却後、データ消去専用ソフトウェア等による抹消措置を実施し、そのデータ消去証明書の提出を、契約事業者に義務付ける（抹消措置計画内で決定、ただし２カ月を超えない範囲とする）。

（3）対 策 3

契約事業者への返却前に、県が機器付属の初期化ツールによるデータ消去を行うための期間（抹消措置計画内で決定、ただし１カ月を超えない範囲とする）を設定する。

契約事業者への返却後、機器付属の初期化ツールによる抹消措置を実施し、そのデータ消去証明書の提出を、契約事業者に義務付ける（抹消措置計画内で決定、ただし２カ月を超えない範囲とする）。

※契約期間の整理は別途調整する。

＜参考資料＞

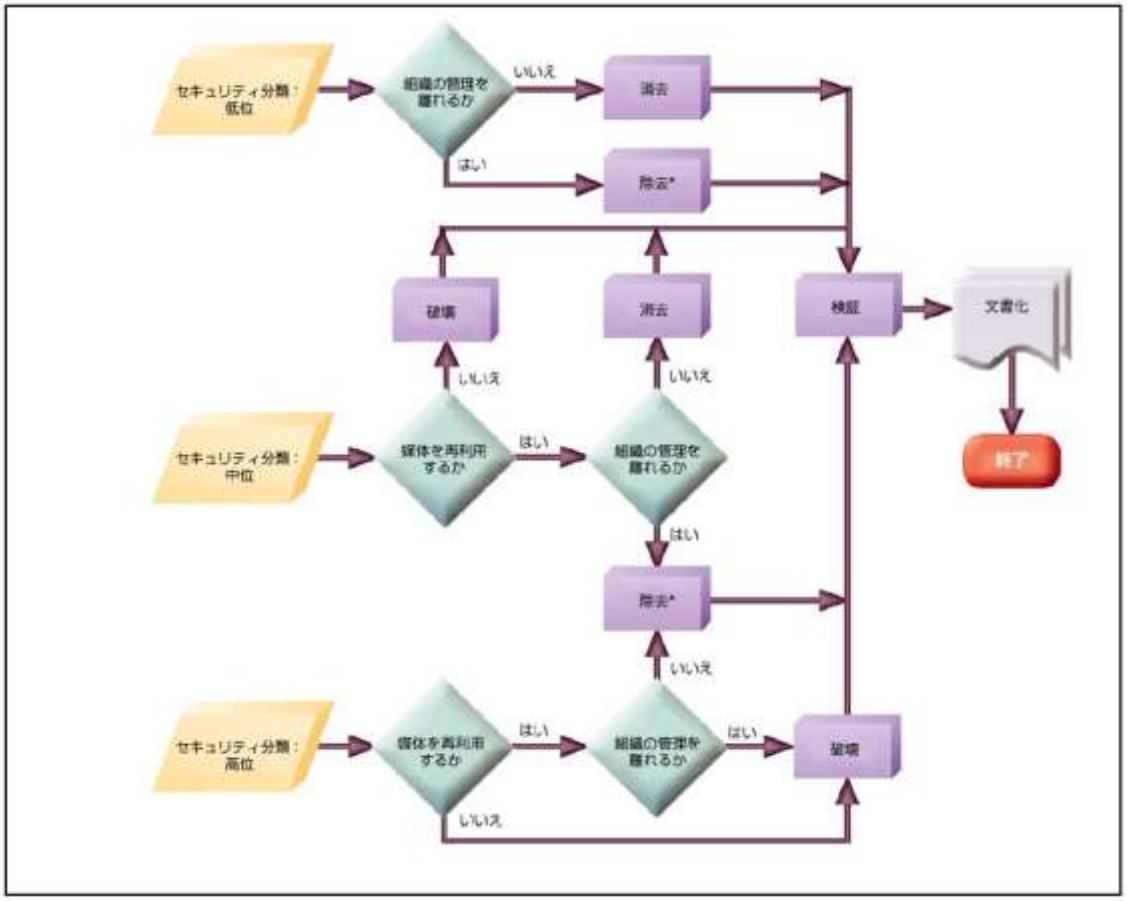
○　SP800-88

NIST が発表した、最新のデータ抹消に関する世界的な規格文書

2006 年発表、2009 年 IPA が和訳を公開、

2014 年 SP800-88 Rev.1 として改版（和約は公開されていない）

○　情報のサニタイズと処分に関する意思決定（NIST SP800-88 2006 版）



○　HDD のデータ抹消のランクと方式（データ適正消去実行証明協議会「データ消去技術ガイドブック第２版」）

（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。

○　データ消去に関する上書き回数（NIST SP800-88 2006 版）

技術の高度化により、磁気ディスクタイプの記憶媒体に関する従来のベストプラクティスが様変わりする状況が生まれた。基本的には、記憶媒体のトラック密度の変化やそれに伴う変化によって、媒体の消去と除去が同一になる状況が生まれた。つまり、2001 年以降に製造された ATA ディスクドライブ（15 GB 超）では、キーボード攻撃と実験環境室のどちらから媒体を保護するにも、媒体を一回上書きすることによる消去で十

分である。

○ 記録媒体内の領域と情報の残存リスクとSECURITY ERASE コマンド(「データ消去技術ガイドブック第２版」)
DCO：Device Command Overlay 装置構成オーバレイ
※ HPA と DCO は OS が認識できない領域
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ない
※ 上記の問題を解決した消去方式が SECURE ERASE で、2001 年に ANSI (American NationalStandards 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
SP800-88 で完全なデータの抹消「Purge(除去)」の手段

○ データ消去後の検証（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。