検討会後修正

総務省セキュリティポリシーガイドライン改定
「機器の廃棄・データ消去」における補足について

総 務 省

令和８年３月16日

自治行政局住民制度課
サイバーセキュリティ対策室

はじめに

本資料は、総務省「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」（以下、「ガイドライン」という。）における機器消去・データ消去に関する改定案（令和8年3月改定）について補足説明するものである。

ガイドラインではこれまで、マイナンバー利用事務系の領域において住民情報を保存する記録媒体における機器の廃棄等は、「当該媒体を分解・粉砕・溶解・焼却・細断などによって物理的に破壊し、確実に復元を不可能とすることが適当である」と示し、物理的に破壊することのみを求めていたところ。

物理破壊においては、機器のリユース（再利用）が困難になることやコスト等の課題があることから、「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等に係る検討会」において機器の廃棄対応について検討を行ってきた。検討結果を踏まえたガイドラインの改定案について本資料にて説明する。

「機器の廃棄・データ消去」に関する現行のガイドラインの記載内容

対策基準解説4.1. サーバ等の管理　iii －67～ iii －68（令和7年3月版）

（７）機器の廃棄等【解説】
情報システム機器が不要になった場合やリース返却等を行う場合には、機器内部の記憶装置からの情報漏えいのリスクを軽減する観点から、情報を復元困難な状態にする措置を徹底する必要がある。この場合、一般的に入手可能な復元ツールの利用によっても復元が困難な状態とすることが重要であり、OS 及び記憶装置の初期化（フォーマット等）による方法は、ハードディスク等の記憶演算子にはデータの記憶が残った状態となるため、適当でないことに留意が必要である。また、原則として、以下の表に記載されている方法により、記録されている情報の機密性に応じて、情報システム機器の廃棄等を行わなければならない。なお、運用にあたっては、「情報システム機器の廃棄等時におけるセキュリティの確保について」（令和2 年5 月22 日総行情第77 号 総務省自治行政局地域情報政策室長通知）を参照されたい。

分類	機器の廃棄等の方法	確実な履行を担保する方法
（１）**マイナンバー利用事務系の領域において住民情報を保存する記憶媒体** ※マイナンバー利用事務系：社会保障、地方税、防災、戸籍事務等に関する情報システム及びデータ	**当該媒体を分解・粉砕・溶解・焼却・細断などによって物理的に破壊し、確実に復元を不可能とすることが適当である。** なお、対象となる機器について、リース契約により調達する場合においても、リース契約終了後、当該機器の記憶媒体については、物理的に破壊を行う。この場合、予め仕様に明記のうえ、機器の廃棄方法を契約において明記することが望ましい。	職員が左記措置の完了まで立ち会いによる確認を行うほか、庁舎内において後述（３）で記述する情報の復元が困難な状態までデータの消去を行った上で、委託事業者等に引き渡しを行い、委託事業者等が物理的な破壊を実施し、当該破壊の完了証明書により確認する。当該完了証明書については、破壊の証拠写真が添付されるとともに、その提出期限が定められていることが望ましい。 なお、**職員による左記措置の完了までの立ち会いについては、委託先事業者の作業状況が確認出来る場合、カメラによるリアルタイムでの監視やカメラ映像の記録の確認などで代替できる。**
（２）自治体機密性２以上に該当する情報を保存する記憶媒体（上記（１）に該当するものを除く。）	一般的に入手可能な復元ツールの利用を超えた、研究所レベルの攻撃からも耐えられるレベルの抹消を行うことが適当である。 具体的には、①物理的な方法による破壊、②磁気的な方法による破壊、③OS等からのアクセスが不可能な領域も含めた領域のデータ消去装置又はデータ消去ソフトウェアによる上書き消去、④ブロック消去、⑤暗号化消去のうちいずれかの方法を選択することが適当である。	庁舎内において後述（３）で記述する情報の復元が困難な状態までデータの消去を行った上で、委託事業者等に引き渡しを行い、抹消措置の完了証明書により確認する方法など適切な方法により確認を行う。
（３）自治体機密性１に該当する情報を保存する記憶媒体	一般的に入手可能な復元ツールの利用によっても復元が困難な状態に消去することが適当である。 具体的には、（２）に記述した方法①～⑤のほか、OS等からアクセス可能な全てのストレージ領域をデータ消去装置又はデータ消去ソフトウェアにより上書き消去する方法がある。 OS及び記憶装置の初期化（フォーマット等）による方法は、HDDの記憶演算子にはデータの記憶が残った状態となるため、適当ではない	庁舎内において消去を実施し、職員が作業完了を確認する方法など適切な方法により確認を行う。
※上記（１）は、オンプレミスの場合を想定したもの（ハウジングやプライベートクラウドを含む）		

物理破壊を実施

委託先の作業の職員の作業立ち会いまたは、監視カメラ等の映像記録の確認が必要

図表41　情報の機密性に応じた機器の廃棄等の方法

「機器の廃棄・データ消去」に関するガイドライン改定（令和8年3月版）のポイント

マイナンバー利用事務系の領域において住民情報を保存する記録媒体の廃棄方法

- 物理破壊における処理方法を明確化（穿孔処理、圧壊処理、シュレッダーによる粉砕を例示※）
- 物理破壊以外の措置（除去※※）も可能とする
- 媒体別の処理方法を明示

※9頁に処理イメージを紹介
※※6頁に除去の方法について紹介

マイナンバー利用事務系の領域において住民情報を保存する記録媒体の廃棄の職員の立ち合い等

- 職員の立ち合いは、自治体管理下（自庁内）での作業のみとし委託先による委託先の作業における職員の作業立ち合いは求めない（作業完了証明書の確認で代替）

その他

- 暗号化消去における留意点（鍵の消去、消去時の記録等）について追記

マイナンバー利用事務系の領域において住民情報を保存する記録媒体の廃棄方法

ガイドライン令和7年3月版と令和8年3月版の比較（機器の廃棄）

機器の廃棄・データ消去の方法（令和7年3月版と令和8年月版の比較）

	機器の廃棄／令和7年3月版	**機器の廃棄／令和8年3月版**
マイナンバー利用事務系の領域において住民情報を保存する記録媒体	物理破壊（**分解・粉砕・溶解・焼却・細断など**）のみの廃棄	• 物理破壊（**細断以外に穿孔処理や圧壊処理も可能**）または、**除去（除去専用コマンド、消磁、暗号化消去による消去）**による廃棄 **記録媒体によっては物理破壊以外も可能**
自治体機密性２以上に該当する情報を保存する記録媒体（上記マイナンバー利用事務系の領域において住民情報を保存する記録媒体に該当するものを除く。）	以下いずれかによる対応 ①物理的な方法による破壊 ②磁気的な方法による破壊 ③OS等からのアクセスが不可能な領域も含めた領域のデータ消去装置又はデータ消去ソフトウェアによる上書き消去 ④ブロック消去 ⑤暗号化消去のうちいずれかの方法を選択する	• マイナンバー利用事務系の領域において住民情報を保存する記録媒体と同様 **媒体別に機器の廃棄・データ消去の方法を明記**
自治体機密性１に該当する情報を保存する記録媒体	上記①～⑤のほか、 上書き消去（OS等からアクセス可能な全てのストレージ領域をデータ消去装置又はデータ消去ソフトウェアにより上書き消去する）を実施	• **光学媒体は破壊による廃棄** • **ハードディスク、USBメモリ、SSDは消去（消去ソフトウェアを利用した上書き消去や消去専用コマンドによる消去）**を実施 • **除去**による対応も可能

データ抹消方法（破壊・除去・消去）

■ 機器における抹消方法について、**破壊・除去・消去**の３つの方法について定義をした。マイナンバー利用事務系及び機密性2以上に該当する情報の機器の廃棄、データ消去については、**破壊・除去**を行う。
■ 各抹消方法における残存リスク等を確認し機器の廃棄を行うこと。

図表41 データ抹消方法（令和8年3月版）

抹消方法		説明	残存リスク等
マイナンバー利用事務系 機密性２以上に該当する情報	破壊	• 細断、切断などの手法によりデータを格納した記録媒体を**完全に破壊**する。 • **ハードディスク(以下、「HDD」という。)**は、**情報を記録している内部の円盤を物理的に破壊**する必要がある • フラッシュメモリベースのストレージデバイス(以下、「**SSD**」という。)は、HDD向けの粉砕シュレッダーでは、細断の細かさ等の点からフラッシュメモリチップを完全には破壊できない。**確実に内部のチップを破壊**すること。	• 一般的な物理破壊装置では、破片から記録された情報を読み取ることでデータの復元の可能性がある。（**専用の破壊装置やHDD/SSDシュレッダーを利用**） • **穿孔**する際は、**専用の破壊装置を利用しないと、円盤に損傷を与えられないことや、最下層の円盤まで損傷を与えることができない**点に注意が必要である。
	除去	• 記録媒体**専用のコマンドを使用**して**記録媒体の全エリアを抹消**する。 • その他の抹消方法として、復号鍵の消去（以下、「**暗号化消去**」という。）　、**消磁**等の手法がある。	• 記録媒体を機器から取り出し、直接記録媒体内の読み取りを行ったとしてもデータの復元は不可能。 • 記録媒体によっては、**専用コマンドがサポートされていない場合がある**。 • 専用コマンドが**正常に動作し、除去が完了したか確認**が必要。 • 故障時は専用コマンドを利用できない可能性があることに留意する。
	消去	• データ抹消ソフトウェア、 記録媒体専用のコマンドを使用し**OS 等からアクセス可能な領域を抹消**する。 • 利用者がアクセス可能な全てのストレージ領域を**非機密データで上書き**し、対象のデータを非機密データにする。	• 一般的に入手可能な復元ツールの利用によるデータの復元は困難。 • **OSから認識できない領域のデータは抹消されない**。 • 記録媒体を機器から取り出し、直接記録媒体内を読み取りを行うことでOSから認識できない領域のデータの復元は可能。 • SSDの場合はOSからアクセスできない領域にデータが残るため、SSDからフラッシュメモリデバイスを取り出し直接、データを読み取ることで、**元のデータを復元できる可能性**がある。

マイナンバー利用事務系の領域において住民情報を保存する記録媒体の廃棄方法

■ 抹消方法、媒体別の具体的な廃棄等の方法について以下の図に示す。
■ 破壊・除去の選択の判断として、例えば「**リユースを行わない場合は破壊**を行い、**リユースを行う場合は除去**を実施する」ということが考えられるが、除去の場合は、処理前と処理後の状態が写真等での確認が難しいことから、ログ等の証跡などを確認することが求められる。

図表42 情報の機密性に応じた機器の廃棄等の方法（令和8年3月版）

分類	抹消方法	廃棄等の方法	
（１）**マイナンバー利用事務系の領域において住民情報を保存する記録媒体** ※マイナンバー利用事務系：社会保障、地方税、防災、戸籍事務等に関する情報システム及びデータ **記録媒体がHDD・SSDの場合は、破壊か除去か抹消方法の選択が可能**	**破壊** **リユース不可**	HDD	当該媒体を**細断、変形するなど**して情報を記録している内部の円盤を物理的に破壊する必要がある。HDDの場合、筐体に対して不適当なサイズの円盤を組み込んでいるものが存在しており、**穿孔**する際は、円盤を確実に損傷するため多点方式で最下層の円盤まで損傷を与えることができる**専用破壊装置を利用**する必要がある。
		SSD	当該媒体を**切断するなど**して情報を記録している**内部のメモリチップを破壊**する方法が例として挙げられる。HDD向けの一般的な物理的破壊方法では、裁断の細かさ等の点からフラッシュメモリ媒体を完全には破壊できないため、**専用の破壊装置を使用**し、メモリチップを破壊する必要がある。
		USBメモリ	
		光学媒体	• **メディアシュレッダー**や**メディアクラッシャー**等の機器にて記録層を破壊
	除去 **リユース可（消磁の場合はリユース不可の場合あり）**	HDD	• **暗号化消去** • ATA コマンドの「**SECURITY ERASE UNIT**」コマンドを「**Enhanced Erase mode**」で使用 • SCSIコマンドの「**SCSI SANITIZE**」コマンドや「**SCSI Format**」コマンドを使用 • **消磁**
		SSD	• **暗号化消去** • ATA コマンドの「**BLOCK ERASE**」コマンドを使用 • SCSIコマンドの「**SCSI SANITIZE**」コマンドや「**SCSI Format**」コマンドを使用 • NVMe（PCIe）コマンドの「**NVM Express Format**」コマンドや「**NVM Express SANITIZE**」コマンドを使用

機密性2以上、機密性1以上に該当する情報保存する記録媒体の廃棄方法

（前頁の表からの続き）

分類	抹消方法		廃棄等の方法
（２）**自治体機密性２以上に該当する情報を保存する記録媒体** （上記（１）に該当するものを除く。） **（１）マイナンバー利用事務系の領域において住民情報を保存する記録媒体と抹消方法は同じ**	**破壊** **リユース不可**	HDD	当該媒体を**細断、変形するなど**して情報を記録している内部の円盤を物理的に破壊する必要がある。HDDの場合、筐体に対して不適当なサイズの円盤を組み込んでいるものが存在しており、**穿孔**する際は、円盤を確実に損傷するため多点方式で最下層の円盤まで損傷を与えることができる**専用破壊装置を利用**する必要がある。
		SSD	当該媒体を**切断するなど**して情報を記録している**内部のメモリチップを破壊**する方法が例として挙げられる。HDD向けの一般的な物理的破壊方法では、裁断の細かさ等の点からフラッシュメモリ媒体を完全には破壊できないため、**専用の破壊装置を使用**し、メモリチップを破壊する必要がある。
		USBメモリ	
		光学媒体	• **メディアシュレッダー**や**メディアクラッシャー**等の機器にて記録層を破壊
	除去 **リユース可（消磁の場合はリユース不可の場合あり）**	HDD	• **暗号化消去** • ATA コマンドの「**SECURITY ERASE UNIT**」コマンドを「**Enhanced Erase mode**」で使用 • SCSIコマンドの「**SCSI SANITIZE**」コマンドや「**SCSI Format**」コマンドを使用 • **消磁**
		SSD	• **暗号化消去** • ATA コマンドの「**BLOCK ERASE**」コマンドを使用 • SCSIコマンドの「**SCSI SANITIZE**」コマンドや「**SCSI Format**」コマンドを使用 • NVMe（PCIe）コマンドの「**NVM Express Format**」コマンドや「**NVM Express SANITIZE**」コマンドを使用
（３）自治体機密性１に該当する情報を保存する記録媒体 （HDD、USBメモリ、SSDにおいては、上記（２）の抹消方法の除去も可）	**破壊**	光学媒体	• メディアシュレッダーやメディアクラッシャー等の機器にて記録層を破壊
	消去	HDD	• **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1回以上、上書きすることでデータを消去するソフトウェア）によりファイルを抹消する方法
		USBメモリ	• **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**2回※以上、上書きする**ことでデータを消去するソフトウェア）によりファイルを抹消する
		SSD	• **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**2回※以上、上書きする**ことでデータを消去するソフトウェア）によりファイルを抹消する • ATAコマンドの「**SECURITY ERASE UNIT**」コマンドを「**Normal Erase mode**」で使用する方法

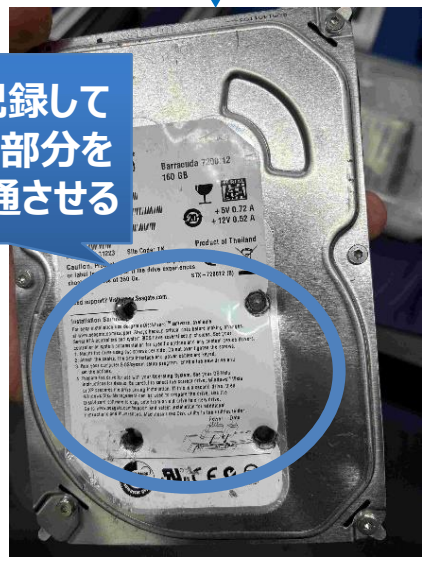
※USBメモリ、SSDというフラッシュメモリタイプは、データ書き込み回数に制限があることからウェアレベリングと呼ばれるディスク領域全体を均一に使用する機能がある。これによりデータ抹消ソフトウェアによる上書きの１回の実施では消去すべき情報が残る可能性があるが、２回以上の上書きにより、当該情報は抹消される。

物理破壊を行う専用機器と破壊後のイメージ

専用物理破壊装置
HDDユニット装着時

穿孔
破壊

HDD
破壊後

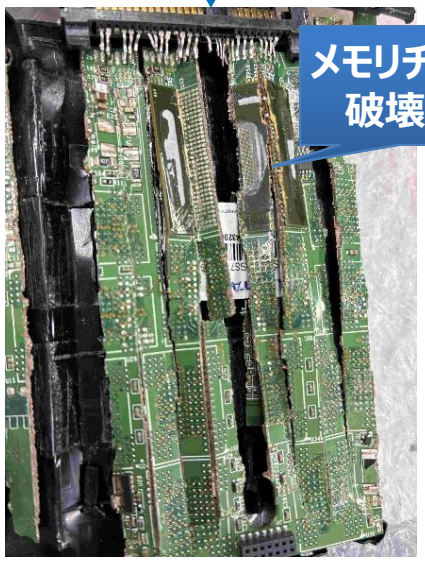


情報を記録している円盤部分を4ヵ所貫通させる

SSD用
圧壊ユニット

圧壊
処理

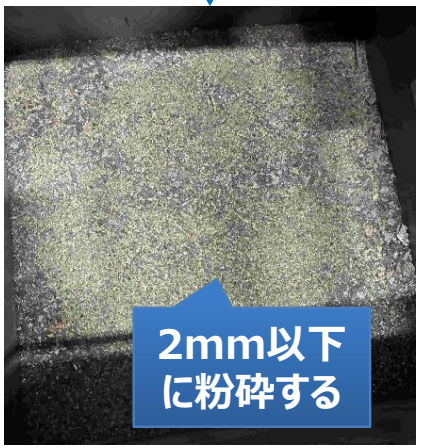
SSD
破壊後



メモリチップを破壊する

専用物理破壊装置
専用シュレッダー

SSD
破壊後



2mm以下に粉砕する

HDD
破壊後

HDDは細かな粉砕は困難

除去（消磁）の留意点

アメリカ国家安全保障局（National Security Agency: NSA）及び中央保安局（Central Security Service: CSS）では、NSA/CSS Evaluated Products List for Magnetic Degaussers July 2025評価済み製品リスト（**磁気消磁装置**）を公開している。

https://www.nsa.gov/Portals/75/NSAEPLMagneticDegaussersJuly2025.pdf?ver=uuQksnBGVKQqCmcsW1s_jw%3d%3d

IMPORTANT REMINDERS(重要な注意事項)において、**ハイブリットタイプやHAMRは破壊装置のリストを参照**する旨が示されているとおり、以下のデバイスは消磁装置ではデータ抹消は不可のため留意すること。

■ **ハイブリッドタイプ(Solid State Hybrid Drive : SSHD)**

- 大容量のデータを保存可能なHDDと、高速アクセスが可能なSSDを組み合わせた記録装置

■ **HAMRとMAMR**

データの記録密度を大幅に向上する次世代の大容量化技術を採用した記録装置

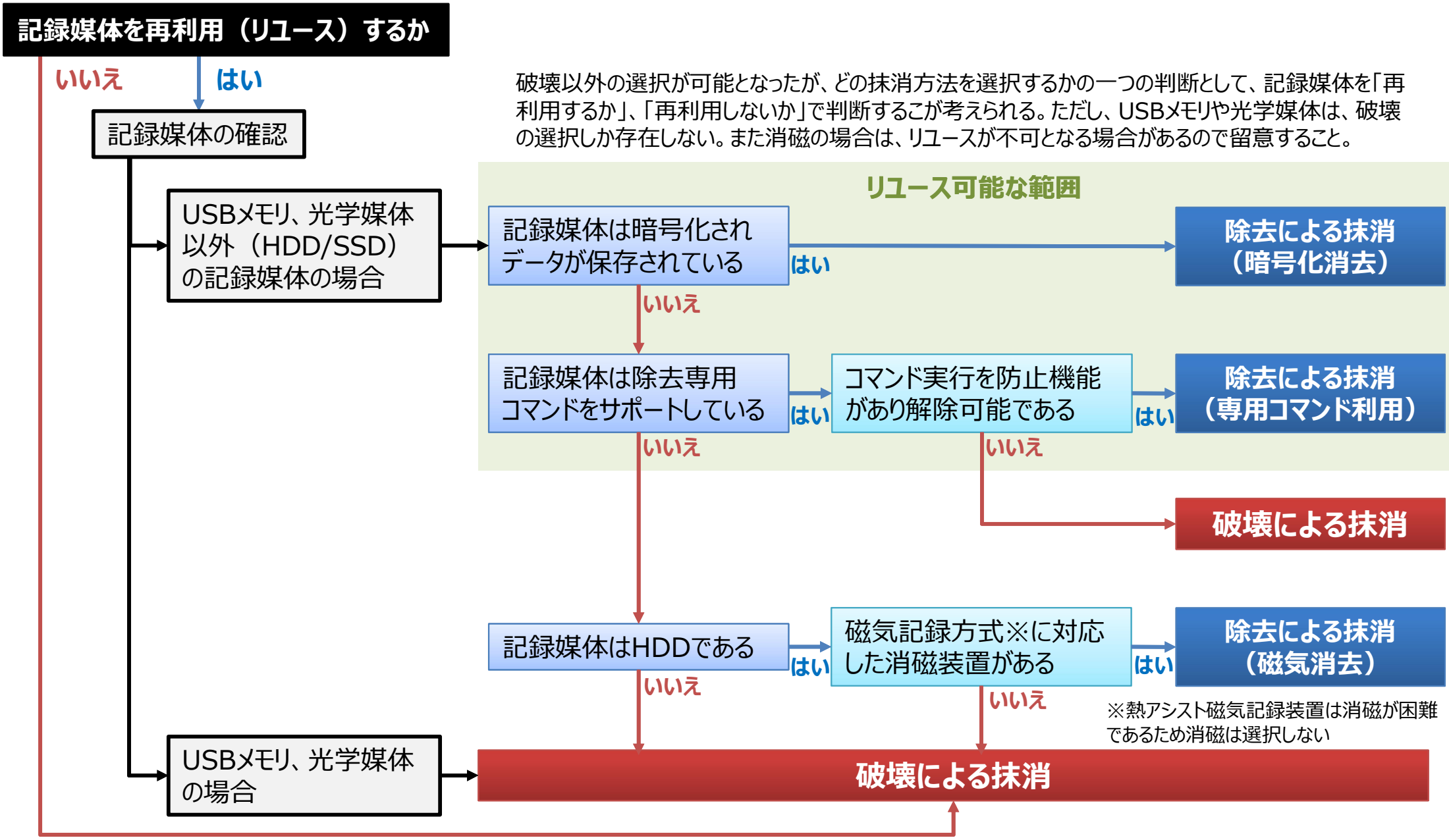
- HAMR （Heat-Assisted Magnetic Recording） （熱アシスト磁気記録）
  レーザー光線によって記録ディスクを瞬間的に加熱し記録する。
- MAMR （Microwave-Assisted Magnetic Recording ） （マイクロ波アシスト磁気記録）
  マイクロ波を利用してデータ記録を行う。

■ そのほか

- 消磁装置は消磁能力について確認する。

破壊・除去の選択フロー（例）

マイナンバー利用事務系の領域において住民情報を保存する記録媒体の機器廃棄・データ消去のフロー（例）

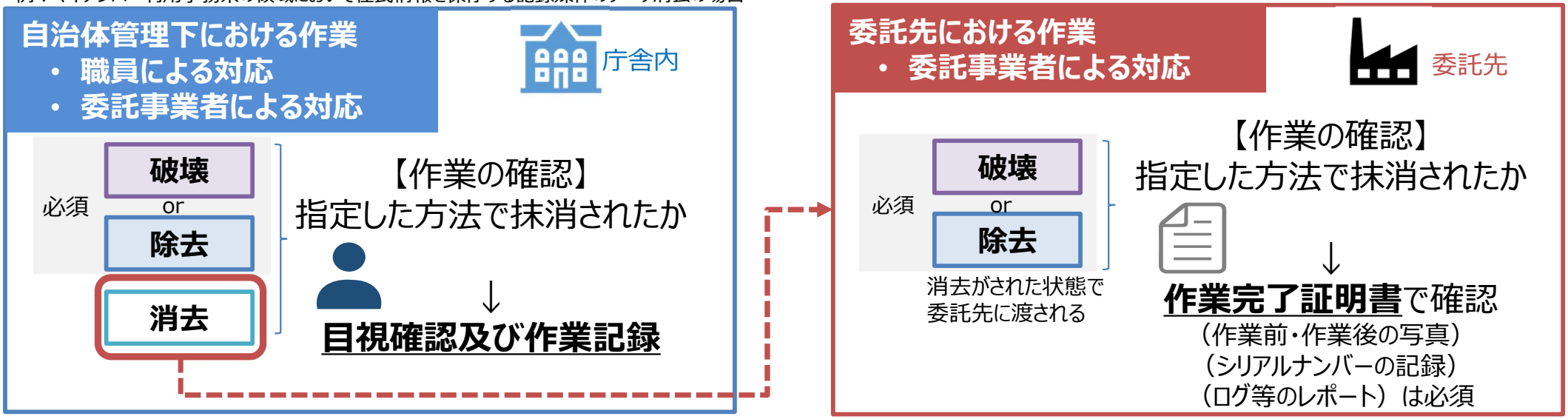


マイナンバー利用事務系の領域において住民情報を保存する記録媒体の廃棄の職員の立ち合い等（作業プロセス）

マイナンバー利用事務系の領域において住民情報を保存する記録媒体の廃棄の職員の立ち合い

- **自治体管理下における作業**においては、職員の立ち合いにより指定した方法でデータ抹消されたか目視確認と作業の記録を取ることを必須とする。
- **委託先における委託事業者の作業**においては、職員の立ち合いまでは求めない。ただし、作業完了証明書で指定した方法でデータが抹消されたかか確証をもとに確認を行うことを必須とする。

例：マイナンバー利用事務系の領域において住民情報を保存する記録媒体のデータ消去の場合



マイナンバー利用事務系の領域において住民情報を保存する記録媒体を管理区域又は取扱区域から外へ移動させる場合（委託先に廃棄を依頼）は、**「消去」は必須**

マイナンバー利用事務系の領域において住民情報を保存する記録媒体を廃棄する場合は、除去以上の対応が必須となる。
（**除去以上の作業を委託先で実施することは可能**）

指定した方法でデータ抹消されたか目視で確認することと作業の過程を記録することを重視する

自治体機密性2以上の情報資産において個人情報が含まれている場合は、上記と同様の対応を行う

現行のガイドラインと改定案の比較（職員の作業立ち合い）

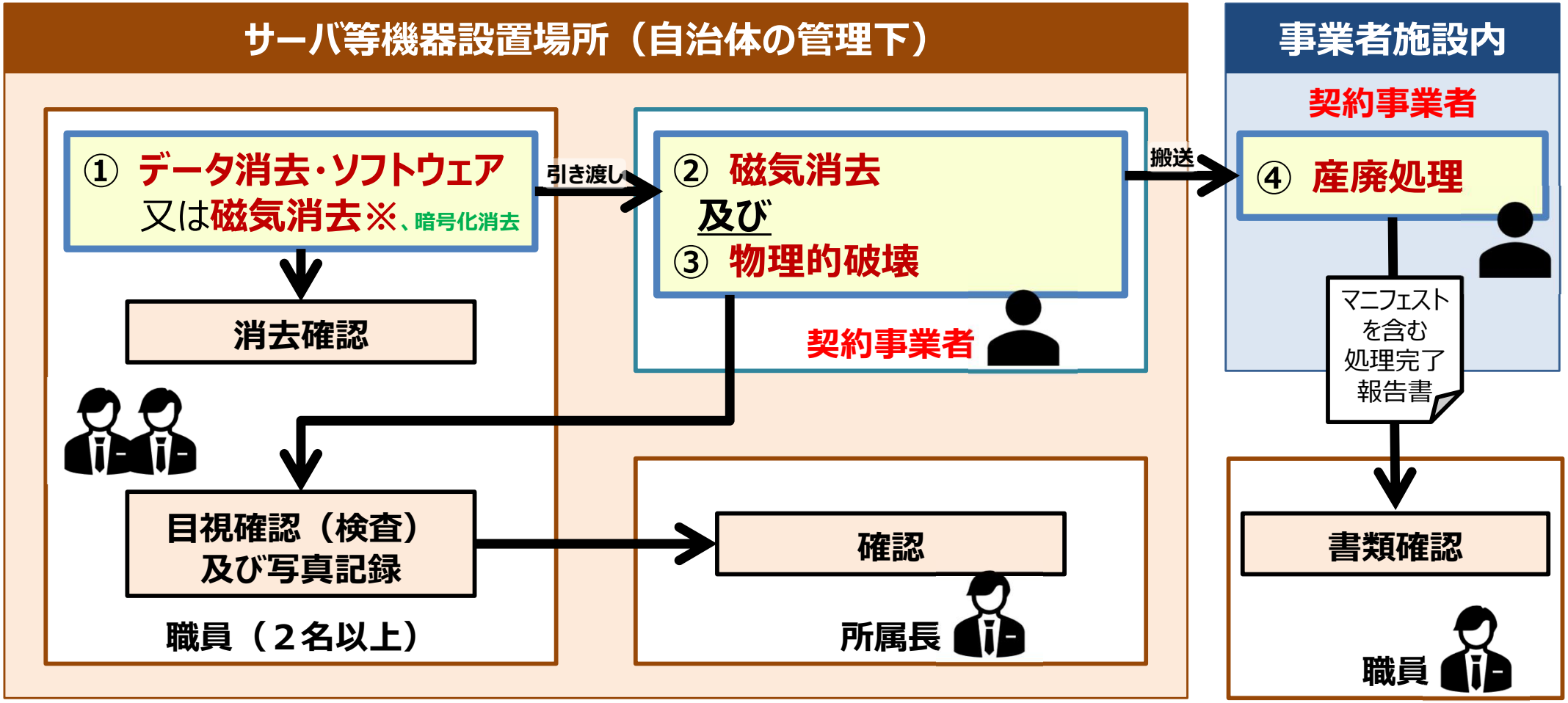
機器の廃棄・データ消去における職員の立ち合い（令和7年3月版と令和8年月版の比較）

	職員の立ち合い／令和7年3月版	**職員の立ち合い／令和8年3月版**
マイナンバー利用事務系の領域において住民情報を保存する記録媒体	• 自庁内で作業を行う場合立ち合いが必要 • 委託先事業者の作業の立ち合い（自庁内、委託先）または、監視カメラ等の映像記録の確認 **職員の立ち合いの範囲を明確化**	• **自庁内で作業**を行う場合、**立ち合いが必要**（職員による作業、委託先事業者の作業） • **委託先での委託先事業者によるデータ抹消作業の立ち合いは必要なし**（ただし作業完了証明書の確認は必須）
自治体機密性２以上に該当する情報を保存する記録媒体（（上記マイナンバー利用事務系の領域において住民情報を保存する記録媒体に該当するものを除く。）	• 立ち合いにおける言及はなし • 作業完了証明書の確認は必須 **個人情報が含まれる場合は、マイナンバー利用事務系の領域における対応と同様の措置を行う**	• 自庁内で作業を行う場合、立ち合いが必要（職員による作業、委託先事業者の作業） • 委託先での委託先事業者によるデータ抹消作業の立ち合いは必要なし（ただし作業完了証明書の確認は必須） • **個人情報が含まれる場合**は、自庁内で「消去」した上で、委託先事業者に引き渡す。 • 作業完了証明書の確認は必須
自治体機密性１に該当する情報を保存する記録媒体	• 言及なし	• **作業完了証明書の確認は必須**

事例：機器の廃棄・データ消去等におけるプロセス（リースの場合）

■ **個人情報を含む重要な情報**を含む記録媒体（**リース**の場合）を廃棄する場合、自治体の管理下において一次的なデータが復元困難な消去作業を行った上で契約事業者に引き渡し、職員の立ち合いのもと磁気的破壊と物理破壊（HDDの場合は穿孔破壊、SSDは圧壊処理）を行っている。その後、産業廃棄物の処理を依頼し、マニフェスト含む書類を確認する。これにより、産業廃棄物の処理までの一連のプロセスの確立され、重要な情報の廃棄に関する管理が徹底できている。

手順フロー（リースの場合）

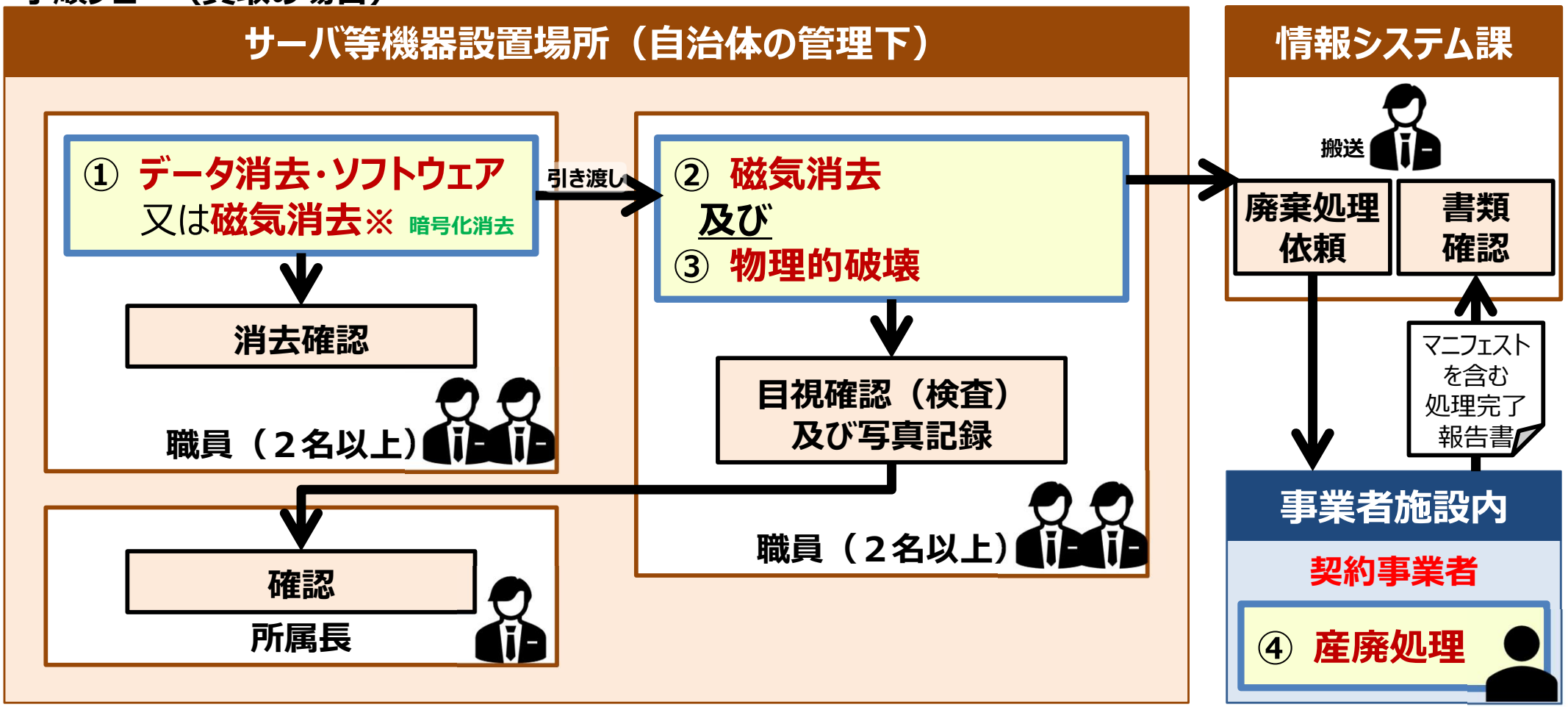


※ ソフトウェアによるデータ消去が困難なサーバ等は職員による磁気消去を実施
（その場合、契約事業者による磁気消去は不要）

事例：機器の廃棄・データ消去等におけるプロセス（買取の場合）

■ **個人情報を含む重要な情報**を含む記録媒体（**買取**の場合）を廃棄する場合、管理下において一次的なデータが復元困難な消去作業を行った上で、さらに、職員の立ち合いのもと磁気的破壊と物理破壊（HDDの場合は穿孔破壊、SSDは圧壊処理）を行っている。その後、産業廃棄物処理を依頼し、マニフェスト含む書類を確認する。

手順フロー（買取の場合）



※ ソフトウェアによるデータ消去が困難なサーバ等は、②の磁気消去から実施

確実な履行を担保する方法について①

■ 確実な履行を担保するための留意点について、抹消方法・作業手続きに関する観点で整理しガイドラインに掲載予定

図表43 確実な履行を担保する方法（令和8年3月版）

分類	抹消方法	確実な履行を担保する方法	
（１） **マイナンバー利用事務系の領域において住民情報を保存する記録媒体** ※マイナンバー利用事務系：社会保障、地方税、防災、戸籍事務等に関する情報システム及びデータ	**破壊**	各抹消方法における履行の担保 **専用の破壊装置を利用する旨を追記**	**細断、切断等による抹消** • 細断、切断等の手法により、データを格納した記録媒体を完全に破壊する。 • 細断による破壊はデータの取得ができない大きさまでデバイスを破壊する。 • HDDを穿孔する場合は、**専用の破壊装置を利用**する。 • SSDやUSBメモリを破壊する場合は、**専用の破壊装置やシュレッダーを利用**する。 • 光学媒体の場合は、光学媒体の記録層を破壊可能な**メディアシュレッダーやメディアクラッシャー等を利用**する。
		作業手続きにおける履行の担保 **番号法における安全管理措置の対応が必要** **職員の作業立ち合いに関する記載**	**作業場所等** • 庁舎内又は委託事業者先において破壊作業を実施する。 • 多数の破壊対象の端末を庁舎内の一室に一時保管する必要がある場合は、保管端末の一覧を作成するとともに、保管場所を施錠するなど、端末の紛失防止対策を講じること。 • 特定個人情報等が記録された電子媒体を管理区域又は取扱区域から外へ移動させる場合には、「**特定個人情報に関する安全管理措置（行政機関等編）**」を遵守する。 **作業を委託する場合** • **庁舎内で破壊作業を行う場合**は、職員は、**当該作業に立ち会うなどして、データが指定した方法で破壊したことを目視で確認するとともに、作業記録を作成**する。 • **委託事業者先で破壊作業を行う場合**は、**職員は、庁舎内において（３）に記載する「消去」によりデータ抹消を実施したことを目視で確認し記録を作成した上で、委託事業者に引き渡す**。破壊作業完了後、職員は、委託事業者が提出する**完了証明書**により作業内容を確認する。 • 当該**完了証明書**については、あらかじめ契約により、破壊処理の前後が確認できる証拠写真及び記録媒体のシリアルナンバーの添付並びに提出期限を定めておくこと。

確実な履行を担保する方法について②

（前頁の表からの続き）

<table>
<tr><th>分類</th><th>抹消方法</th><th colspan="2">確実な履行を担保する方法</th></tr>
<tr><td rowspan="2">（１）
マイナンバー利用事務系の領域において住民情報を保存する記録媒体

※マイナンバー利用事務系：社会保障、地方税、防災、戸籍事務等に関する情報システム及びデータ</td><td rowspan="2">除去

除去における留意点を追記</td><td>各抹消方法における履行の担保</td><td><u>暗号化消去</u>
• 暗号鍵はバックアップ等を含む複製を含めて、確実に消去する。
<u>コマンドによる抹消</u>
• 記録媒体がコマンドをサポートしていることを確認する。
• コマンドが正常に実行されたことを確認し、その記録を取得する。
• 記録媒体において誤操作によるコマンド実行を防ぐ機能がある場合は、その機能を解除してからコマンドを実行する。
<u>消磁による抹消</u>
• 磁気記録媒体に対応した消磁装置を用いて消磁を行う。
• 消磁装置は、経時的な劣化や、連続使用による温度上昇の影響を受けることがあることに注意する。
• SSDまたは磁気記録媒体に不揮発性や非磁性のデバイスが含まれている場合は消磁できないことを注意する。
<u>その他</u>
• 記録媒体がコマンドによる抹消や除去ソフトウェアに対応していない場合は、破壊を行う。</td></tr>
<tr><td>作業手続きにおける履行の担保

番号法における安全管理措置の対応が必要

職員の作業立ち合いに関する記載

委託仕様書に完了証明書の内容を盛り込む旨を追記</td><td><u>作業場所等</u>
• 庁舎内又は委託事業者先において除去作業を実施する。
• 多数の除去対象の端末を庁舎内の一室に一時保管する必要がある場合は、保管端末の一覧を作成するとともに、保管場所を施錠するなど、端末の紛失防止対策を講じること。
• 特定個人情報等が記録された電子媒体を管理区域又は取扱区域から外へ移動させる場合には、「特定個人情報に関する安全管理措置（行政機関等編）」を遵守する

<u>作業を委託する場合</u>
• 庁舎内で除去作業を行う場合は、職員は、当該作業に立ち会うなどして、データが指定した方法で除去したことを目視で確認するとともに、作業記録を作成する。
• 委託事業者先で除去作業を行う場合は、職員は、庁舎内において（３）に記載する「消去」によりデータ抹消を実施したことを目視で確認し記録を作成した上で、委託事業者に引き渡す。除去作業完了後、職員は、委託事業者が提出する完了証明書により作業内容を確認する。
• 当該完了証明書については、あらかじめ契約により、コマンド、消磁又は暗号化消去による抹消方法及び作業履歴の記載、作業が正常終了したことの証跡の添付並びに提出期限を定めておくこと。</td></tr>
</table>

確実な履行を担保する方法について③

（前頁の表からの続き）

分類	抹消方法	確実な履行を担保する方法	
（２） **自治体機密性２以上に該当する情報を保存する記録媒体** **（上記（１）に該当するものを除く。）**	**破壊**	各抹消方法における履行の担保	マイナンバー利用事務系の領域において住民情報を保存する記録媒体における破壊と同様
		作業手続きにおける履行の担保 **個人情報保護法における安全管理措置の対応が必要** **個人情報が含まれる場合は、マイナンバー利用事務系の情報資産を廃棄する方法と同様**	**作業場所等** • 庁舎内又は委託事業者先において破壊作業を実施する。 • 多数の破壊対象の端末を庁舎内の一室に一時保管する必要がある場合は、保管端末の一覧を作成するとともに、保管場所を施錠するなど、端末の紛失防止対策を講じること。 • 個人情報が記録された電子媒体を管理区域又は取扱区域から外へ移動させる場合には、「**個人情報の保護に関する法律についてのガイドライン（通則編）10-5物理的安全管理措置**」を参考にし、容易に個人データが判明しないよう安全な方策を講じる。 **作業を委託する場合** • **庁舎内で破壊作業を行う場合**は、職員は、当該作業に立ち会うなどして、データが復元できないことを目視で確認するとともに、作業記録を作成する。 • **委託事業者先で破壊作業を行う場合**は、作業完了後、職員は、委託事業者が提出する完了証明書により作業内容を確認する。なお、**個人情報が記録されている場合**は、庁舎内において（３）に記載する「消去」によりデータ抹消を実施し、**職員が目視で確認し記録を作成した上で、委託事業者に引き渡す**こと。 • 当該完了証明書については、あらかじめ契約により、破壊処理の前後が確認できる証拠写真及び記録媒体のシリアルナンバーの添付並びに提出期限を定めておくこと
	除去	各抹消方法における履行の担保	マイナンバー利用事務系の領域において住民情報を保存する記録媒体における除去と同様
		作業手続きにおける履行の担保	作業を委託する場合 • 庁舎内で除去作業を行う場合は、職員は、当該作業に立ち会うなどして、データが復元できないことを目視で確認するとともに、作業記録を作成する。 • 委託事業者先で除去作業を行う場合は、作業完了後、職員は、委託事業者が提出する完了証明書により作業内容を確認する。なお、**個人情報が記録されている場合**は、庁舎内において（３）に記載する「消去」によりデータ抹消を実施し、職員が目視で確認し記録を作成した上で、委託事業者に引き渡すこと。 • 当該**完了証明書**については、あらかじめ契約により、コマンド、消磁又は暗号化消去による抹消方法及び作業履歴の記載、作業が正常終了したことの証跡の添付並びに提出期限を定めておくこと。

確実な履行を担保する方法について④

（前頁の表からの続き）

分類	抹消方法		確実な履行を担保する方法
（３） **自治体機密性１に該当する情報を保存する記録媒体**	**破壊**	各抹消方法における履行の担保	自治体機密性２以上に該当する情報を保存する記録媒体における破壊と同様
		作業手続きにおける履行の担保	自治体機密性２以上に該当する情報を保存する記録媒体における破壊と同様
	除去	各抹消方法における履行の担保	自治体機密性２以上に該当する情報を保存する記録媒体における除去と同様
		作業手続きにおける履行の担保	自治体機密性２以上に該当する情報を保存する記録媒体における除去と同様
	消去	各抹消方法における履行の担保 **上書き消去に関する記述を追記**	**コマンドによる抹消** • 記録媒体がコマンドをサポートしていることを確認する。 • コマンドが正常に実行されたことを確認し、その記録を取得する。 • 記録媒体において誤操作によるコマンド実行を防ぐ機能がある場合は、その機能を解除してからコマンドを実行する。 **データ抹消ソフトウェアによる抹消** • 利用者がアクセス可能な全てのストレージ領域を非機密データ（01）で上書きが可能なデータ抹消ソフトウェアにより、対象のデータを非機密データにする。
		作業手続きにおける履行の担保 **委託仕様書に完了証明書の内容を盛り込む旨を追記**	**作業場所等** ・庁舎内又は委託事業者等先において破壊作業を実施する。 ・多数の破壊対象の端末を庁舎内の一室に一時保管する必要がある場合は、保管端末の一覧を作成するとともに、保管場所を施錠するなど、端末の紛失防止対策を講じること。 **作業を委託する場合** ・庁舎内で破壊作業を行う場合は、職員は、当該作業に立ち会うなどして、データが復元できないことを目視で確認するとともに、作業記録を作成する。 ・委託事業者等先で作業を行う場合は、作業完了後、職員は、委託事業者等が提出する**完了証明書により作業内容を確認**する。 ・当該完了証明書については、あらかじめ契約により、抹消方法及び作業履歴の記載並びに提出期限を定めておくこと。

作業証明書の例

委託先に破壊・除去・消去を委託する場合は、作業完了証明書の委託契約時の仕様に定め提出を求めること。
以下は物理破壊における作業完了証明書の例を示す。

発行日 :2026年　　月　　日
証明書番号 :
マニフェスト番号:

物理破壊作業完了証明書

XXX市情報システム課　様

ＸＸＸＸＸＸＸ株式会社
東京都千代田区霞が関ｘｘｘｘｘｘｘｘｘ
電話番号ｘｘｘｘｘｘｘｘｘ
代表者ｘｘｘｘｘｘ　　印

当社は下記の通り物理破壊処理を実施したことをここに証明します。

作業名	住民情報システムサーバ及び端末における機器の廃棄・データ消去
代表型番	XXXXXX（別紙廃棄資産一覧表を参照）
代表シリアル番号	XXXXXX（別紙廃棄資産一覧表を参照）
メディアの種類	3.5 inch HDD
作業日時	2025/08/20　14:00
作業者	○○　○○○
作業場所	XXX市会議室 A
その他作業	未実施（消去作業をXXX市実施後、当社が物理破壊を実施）

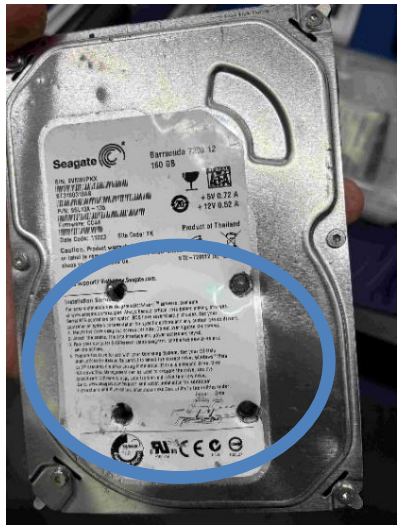
複数機器がある場合は一覧表で確認する

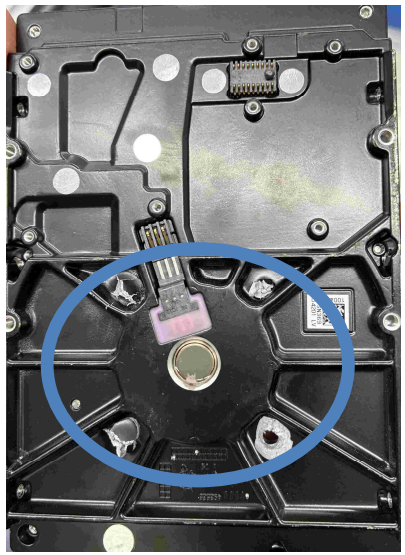
作業日時、作業者、作業場所を記録する

破壊前後の写真

破壊前（2025/08/20 14:00）

破壊後（2025/08/20 14:10）





破壊後の写真（ハードディスクの記録箇所の穴開け貫通状態を確認する）

事例　第三者機関による作業証明書の例

■ **第三者による消去証明書発行**

消去作業者自身ではなく第三者による証明書を発行している例として「一般社団法人ソフトウェア協会」が、データ適正消去実行証明書の発行事業を展開している。

■ **第三者による消去ソフト、消去実施事業者認証**

事業者のデータ消去ソフトの消去能力を第三者機関として検証し認証、及びデータ消去実施事業者の消去環境及び業務作業フローのセキュアレベルを評価した上で、第三者による認証を「データ適正消去実行証明協議会」にて実施している 。

消去証明書（第三者）のサンプル

発行日：2025/12/16
発行ID：7944006407-S

データ適正消去実行証明書

データ適正消去実行証明協議会（略称：ADEC(Association of Data Erase Certification)）は、本協議会が認証したデータ消去ソフトウェアおよび消去事業者により実施された消去の結果を下記の通り証明します。

①消去ドライブ情報（メディア情報）
＜消去ドライブ＞

ドライブの種類	HDD/ハイブリッドHDD
シリアル番号	Test-Drive-Serial-001
モデル名等	テストドライブ

消去対象機器（各情報）

＜対象機器情報＞

対象機器シリアル番号	Test-Product-Serial-001
対象機器メーカー名（型番等）	テストPC

消去内容

②実行した消去内容

管理番号	TestManagementNo001	事業者枝番号	TestBranchNo001
消去レベル	Clear	消去結果	正常消去
消去開始日時	2025/12/01 12:00:00	消去終了日時	2025/12/01 23:59:59

③認証消去ソフトウェア情報

消去ソフトウェア名	テストソフト
メーカー名	テストベンダー
認証番号	TestSoft123456789

消去に利用したソフトウェア情報

④認証消去事業者情報

事業者名	テスト事業者
事業所名	テスト事業所
事業所住所	東京都港区赤坂1-3-6赤坂グレースビル
レーティング	★★★
認証番号	TestOffice123456789

消去事業者

第三者機関名

【証明書発行元】
ADEC
データ適正消去実行証明協議会（ADEC）について
データの適正な消去の在り方を調査・研究し、その技術的な基準の策定とデータが適正に消去されたことを第三者機関が証明する制度の普及・啓発を推進する協議会です。

一般社団法人ソフトウェア協会（SAJ）について
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、我が国のIT産業の健全な発展と国民生活の向上に寄与することを目的としている一般社団法人です。

その他のガイドライン改定箇所①

■ 対策基準解説4.1（７）機器の廃棄等の箇所を改定

令和7年3月版：対策基準（解説）

4.1. サーバ等の管理

（７）機器の廃棄等

情報システム機器が不要になった場合やリース返却等を行う場合には、機器内部の記録装置からの情報漏えいのリスクを軽減する観点から、情報を復元困難な状態にする措置を徹底する必要がある。この場合、一般的に入手可能な復元ツールの利用によっても復元が困難な状態とすることが重要であり、OS 及び記憶装置の初期化（フォーマット等）による方法は、ハードディスク等の記録演算子にはデータの記憶が残った状態となるため、適当でないことに留意が必要である。また、原則として、以下の表に記載されている方法により、記録されている情報の機密性に応じて、情報システム機器の廃棄等を行わなければならない。なお、運用にあたっては、「情報システム機器の廃棄等時におけるセキュリティの確保について」（令和2 年5 月22 日総行情第77 号 総務省自治行政局地域情報政策室長通知）を参照されたい。

令和8年3月版：対策基準（解説）

4.1. サーバ等の管理

機器の故障時や予防保守時における交換時の廃棄について追記

（７）機器の廃棄等

情報システム機器が不要になった場合**（故障時や予防保守時における機器の交換を含む）**やリース返却等を行う場合には、機器内部の記録**媒体**からの情報漏えいのリスクを軽減する観点から、情報を復元困難な状態にする措置を徹底する必要がある。この場合、一般的に入手可能な復元ツールの利用によっても復元が困難な状態とすることが重要であり、OS 及び記録**媒体**の初期化（フォーマット等）による方法は、ハードディスク等の**記録媒体にデータの記録が残った状態となるため**、記録演算子にはデータの記録が残った状態となるため、適当でないことに留意が必要である。また、原則として、以下の表に記載されている**消去、除去、破壊の抹消**方法により、記録されている情報の機密性に応じて、**端末を含む**情報システム機器の廃棄等を行わなければならない。**（注１）機器等及び情報システムの廃棄までのライフサイクルを鑑み、図表42「情報の機密性に応じた機器の廃棄等の方法」を参考に、調達時（リース調達含む）に当該機器の廃棄時におけるデータの抹消方法についてあらかじめ調達の仕様に明記し、対応が可能な機器等を調達することが望ましい。**

（注２）暗号化消去を行う場合は、図表44「暗号化消去における留意事項」を参考にすること。なおクラウドサービス利用時おける暗号化消去については、第4編 8.業務委託と外部サービス（クラウドサービス）の利用）(8)③の解説を参照されたい。

データの抹消方法に関する記述を追加

各データ抹消方法が可能な機器等を選定する必要がある旨を追記

暗号化消去に関する留意点を追記

項目	留意事項
暗号化消去の前提条件	• 情報を記録媒体に格納する前に記録媒体の暗号化機能を有効にしておく。 • 記録媒体の暗号化機能が有効にされていない状態で情報を保存しない。
暗号の強度	• CRYPTREC暗号リスト（電子政府推奨暗号リスト）に記載されている強度の強い暗号アルゴリズムを使用する。
鍵の消去	• 鍵を確実に消去する。 • 鍵のバックアップがある場合は、バックアップも消去する。
暗号消去操作の記録	• 暗号化消去を実施したことを記録に残す。【記録の例】（実施日、記録媒体名、製造メーカー、シリアル番号、暗号方法（暗号化ソフト、バージョンなど）、実施者、確認者等）

図表44　暗号化消去における留意事項

その他のガイドライン改定箇所②

■ 対策基準解説6.3（２）機器等及び情報システムの調達の箇所に調達時に廃棄に関する仕様を含む旨を追記

令和7年3月版：対策基準（解説）

6.3.システム開発、導入、保守等

（２） 機器等及び情報システムの調達
機器等及び情報システムを調達する場合は、当該情報システムで取り扱う情報の重要性に応じて、機器等及び情報システムのライフサイクルで必要となるセキュリティ機能を洗い出し、調達要件に含める必要がある。例えば、アクセス制御の機能、パスワード設定機能、ログ取得機能、データの暗号化等である。
また、調達における透明性の確認を必要とする場合には、SBOM（Software Bill of Materials：ソフトウェア部品表）の作成、提供等を、調達時の評価項目とすることを機器等の選定基準として定めることも考えられる。

令和8年3月版：対策基準（解説）

6.3.システム開発、導入、保守等

（２） 機器等及び情報システムの調達
機器等及び情報システムを調達する場合は、当該情報システムで取り扱う情報の重要性に応じて、機器等及び情報システムのライフサイクルで必要となるセキュリティ機能を洗い出し、調達要件に含める必要がある。例えば、アクセス制御の機能、パスワード設定機能、ログ取得機能、データの暗号化等である。
なお、ライフサイクルには機器等及び情報システムの廃棄も含まれる。機器の調達時には、当該機器の廃棄時におけるデータの抹消方法について本ガイドラインの解説の第３編（第３章4.1. サーバ等の管理（７）機器の廃棄等）を参照し調達の仕様に明記し、契約に位置づけることが望ましい。
また、調達における透明性の確認を必要とする場合には、SBOM（Software Bill of Materials：ソフトウェア部品表）の作成、提供等を、調達時の評価項目とすることを機器等の選定基準として定めることも考えられる。

その他のガイドライン改定箇所③

■ 対策基準解説8.1（２）リース調達の仕様にリース終了時の機器の廃棄・データ消去の扱いを記載する旨を追記

令和7年3月版：対策基準（解説）

8.1.業務委託

（２） 業務委託実施前の対策
①業務委託前までに実施すべき事項
(略)
・委託業務終了時の情報資産の返還、廃棄等
委託業務終了時に、不要になった情報資産を返還させるか廃棄させるか等その取扱いについて明確に規定する必要がある。委託終了後の取扱いを明確にすることにより、不要になった情報資産から情報が漏えいする可能性を減らす。なお、マイナンバー利用事務系の領域において取り扱われる機器をリースにより調達しようとする場合には、当該機器についてリース契約終了後、物理的破壊を行う旨、入札における仕様に明記するとともに、契約に位置づけることが望ましい。

令和8年3月版：対策基準（解説）

8.1.業務委託

（２） 業務委託実施前の対策
①業務委託前までに実施すべき事項
(略)
・委託業務終了時の情報資産の返還、廃棄等
委託業務終了時に、不要になった情報資産を返還させるか廃棄させるか等その取扱いについて明確に規定する必要がある。委託終了後の取扱いを明確にすることにより、不要になった情報資産から情報が漏えいする可能性を減らす。~~なお、マイナンバー利用事務系の領域において取り扱われる~~機器をリースにより調達しようとする場合には、当該機器についてリース契約終了後の~~、物理的破壊を行う旨、~~**データの抹消方法について本ガイドラインの解説の第３編（第３章4.1. サーバ等の管理 （７） 機器の廃棄等）を参照し**入札における仕様に明記するとともに、契約に位置づけることが望ましい。

その他のガイドライン改定箇所④

■ 対策基準解説4.1（５）機器の修理・交換の際におけるデータの抹消に関する記述を追記

令和7年3月版：対策基準（解説）

4.1.サーバ等の管理

（５） 機器の定期保守及び修理

情報システムの安定的な運営のためには、定期的に保守を行うことが不可欠である。また、機器を修理に出す場合には、できる限り故障した部品を特定し、情報を消去できる場合は消去を行った上で引き渡すことにより、修理を委託する業者から情報が漏えいする可能性を低くしなければならない。内容を消去できないときは、守秘義務契約を締結するほか、秘密保持に関する体制や運用などが適正であることを確認しなければならない。

令和8年3月版：対策基準（解説）

4.1.サーバ等の管理

（５） 機器の定期保守及び修理

情報システムの安定的な運営のためには、定期的に保守を行うことが不可欠である。また、機器を修理に出す場合には、できる限り故障した部品を特定し、情報を消去できる場合は消去を行った上で引き渡すことにより、修理を委託する業者から情報が漏えいする可能性を低くしなければならない。内容を消去できないときは、守秘義務契約を締結するほか、秘密保持に関する体制や運用などが適正であることを確認しなければならない。**修理に伴い記録媒体を交換する場合は、当該記録媒体のデータを抹消すること。データの抹消方法について本ガイドラインの解説の第３編（第３章4.1. サーバ等の管理（７） 機器の廃棄等）を参照し、仕様に明記するとともに、契約に位置づけることが望ましい。**

その他（暗号化消去ついて）

暗号化消去

- 暗号化消去とは、データを暗号化した暗号鍵を消去してしまうことで、情報（データ）が復元困難な状態になることをいう。
- そのためには、情報（データ）を格納する記録媒体（ストレージデバイスやハードディスク等）が暗号化可能であることが必要となり、また、その暗号化機能を有効化が必須となる。
- 暗号化する際の暗号アルゴリズムも重要となり、CRYPTRECの電子政府推奨暗号リストに記載されているものを使用する。
- 暗号鍵を消去する際は、バックアップしている暗号鍵も消去することや記録（ログ）を残すことが必要となる。合わせて鍵の管理が重要となる。

図表44　暗号化消去における留意事項（令和8年3月版）

項目	留意事項
暗号化消去の前提条件	• 情報を記録媒体に格納する前に**記録媒体の暗号化機能を有効**にしておく。 • 記録媒体の暗号化機能が有効にされていない状態で情報を保存しない。
暗号の強度	• CRYPTREC暗号リスト（**電子政府推奨暗号リスト**）に記載されている**強度の強い暗号アルゴリズムを使用**する。
鍵の消去	• **鍵を確実に消去**すること。 • 鍵のバックアップがある場合は、**バックアップも消去**する。
暗号消去操作の記録	• 暗号化消去を実施したことを**記録に残す**。 【記録の例】（実施日、記録媒体名、製造メーカー、 シリアル番号、暗号方法（暗号化ソフト、バージョンなど）、実施者、確認者等）

（参考）鍵を確実に消去する手順

Windows端末（BitLocker)の場合、以下を実施する。

1. **バックアップした回復キーの消去**
   バックアップ時に指定した保存先から回復キーを消去する。
   主な指定可能な保存先は以下のとおり。
   - 回復キーを印刷した紙
   - Microsoft アカウント(Microsoft Entra ID,法人アカウントの場合)
   - USBメモリ
2. **端末のその他の鍵の消去**
   端末のTPM※の初期化によりTPM内の鍵を消去する。
   TPMの初期化には以下の方法がある。
   - Windowsの「ファイル名を指定して実行」で「tpm.msc」を実行し、TPM管理画面で「TPMのクリア」により消去
   - BIOSのTPM設定でクリアにより消去
     （BIOSの表示方法については端末ベンダーに確認すること）

※ただし、WindowsのBitLockerは、利用者自身で自己暗号化を無効にすることが可能なため、利用する際には注意が必要である。

※Trusted Platform Module（暗号化して鍵などと格納している耐タンパ性のあるチップ）

参考　BitLockerにおける複数のキー・プロテクターを削除する方法

■　BitLockerには複数の解除するための認証手段（キー・プロテクター）が存在する。消去手順を以下に示す。

1. BitLockerの状況確認
   manage-bde –status
   （「変換状態」が「使用領域のみ暗号化」である場合は、平文データが残存している可能性がある空き領域を暗号化
   manage-bde -wipefreespace C:）
2. BitLockerへのアクセス手段の確認
   manage-bde -protectors -get C:
3. すべての認証経路を削除（回復手段が無くなるため、自動的に保護がオフになる）
   manage-bde -protectors -delete C:※
4. 新しい回復キーを設定し、新しい回復キーは印刷・保存しない
   manage-bde -protectors -add C: -RecoveryPassword
5. 保護をオンに戻す
   manage-bde -protectors -enable C:
6. BitLockerの状況を再度確認し、認証経路が回復キー以外にないこと、保護がオンになっていることを確認
   manage-bde –status
7. 再起動し、BitLockerの回復キーの入力画面が出ることを確認
8. AD／Entra IDに回復キーをバックアップするポリシーを設定している場合は、ADからコンピュータを削除、またはIntuneでリタイア処理を実施する

※回復キーの“外部保存データ（Microsoft アカウントや印刷物）”が全て消える訳がではない

BitLocker回復キーとロック解除キーについて

- BitLockerには回復キーとは別にロック解除キーがある。利用目的が異なるため混同しないこと。
- BitLocker は、Windows のログオン前（OS 起動前）に **PIN やパスワード（ロック解除キー）** の入力を求める構成が可能であり、これにより、TPM の自動解除に加えてユーザー認証を追加することで、端末盗難時の不正起動を防ぎ、セキュリティを強化できる。
- 端末に異常が検知されると、BitLocker は回復モードに入り、通常の PIN／パスワード（ロック解除キー）では暗号解除ができなくなるため、暗号化された情報にアクセスするには、48桁の回復キーが必要となる。
- 暗号化消去を行う場合は、BitLocker のキー・プロテクター（復号に必要な鍵の保護手段）を削除することで、暗号化データを復号不能にする。機器を廃棄する場合は、バックアップした回復キーとTPMの初期化を行う。

回復キーとロック解除キーの違い

区分	回復キー	ロック解除キー
役割	非常時（BitLockerが通常解除できない場合）にのみ使用する48桁の解除キー	日常的な暗号化解除に使う認証（PIN/パスワード/USBキー）
利用シーン	BitLockerが通常解除できない場合、回復モード※で使用	通常起動時のロック解除に使用
バックアップ	紛失すると解除不可のため必ずMicrosoftアカウント等へ保管	ユーザーが再設定可能のため厳密なバックアップは不要

※ BIOS/UEFI の設定変更やアップデート、TPM が無効化・クリアされた場合、ハードウェア交換（SSD / マザーボード など）、起動順序やセキュアブートの変化等によりBitLocker が「通常の方法では安全確認できない」と判断し、ドライブのロックを解除しない状態

クラウドデータにおける暗号化消去について

- クラウドデータの暗号化消去とは、データを暗号化した暗号鍵を消去してしまうことで、情報（データ）が復元困難な状態になることをいう。
- そのためには、情報（データ）を格納する記録領域が暗号化され、かつ当該データの復号に必要な暗号鍵が消去可能な形で管理（鍵管理）されていることが必要となる。基本的には、鍵管理システム（KMS※1）において鍵の生成から消去までを一元的に行う。
- 暗号化する際の暗号アルゴリズムも重要となり、CRYPTRECの電子政府推奨暗号リストに記載されているものを使用する。
- 暗号鍵を消去する際は、バックアップしている暗号鍵も消去することや記録（ログ）を残すことが必要となる。

クラウドデータの暗号化消去における留意事項

項目	留意事項
暗号化消去の前提条件	• 情報を記録領域に格納する前に**記録領域の暗号化機能を有効**にしておく。 • 記録領域の暗号化機能が有効にされていない状態で情報を保存しない。
暗号の強度	• CRYPTREC暗号リスト（**電子政府推奨暗号リスト**）に記載されている**強度の強い暗号アルゴリズムを使用**する。
鍵の消去	• **鍵を確実に消去**すること。 • 鍵のバックアップがある場合は、**バックアップも消去**する。
暗号消去操作の記録	• 暗号化消去を実施したことを**記録に残す**。 **【記録の例】（鍵ID、鍵タイプ、削除操作日時、削除実行主体※、削除完了日時、削除状態、対象データ識別子、ログ整合性情報）**

削除実行主体とは、削除実行した「人、システム、サービスアカウント」を指す。

参考資料：ADEC暗号化認証基準ガイドライン
https://adec-cert.jp/files/certificationlist/cecc/CECC_GuideLine.pdf

（参考）鍵を確実に消去する手順

暗号鍵の消去は基本的にクラウド事業者が提供するKMS、またはHSM※2の管理インターフェースを通じて実行され、最終的にHSM内部から暗号鍵が消去されることが必要となる。

1. クラウドサービス上で暗号鍵の管理画面を開く
2. 消去したい鍵を選ぶ
3. 消去実行
4. 安全確認期間として消去待機状態に移行
5. 安全確認期間経過後、完全消去

安全確認期間はクラウドサービスにより日数に違いがあるため、消去前にあらかじめ確認しておくこと。

※1 Key Management Service(キーマネジメントサービスとはクラウドサービスにおいて、暗号鍵の生成、保管、管理、消去を安全に行うサービスの総称)
※2 Hardware Security Module（暗号鍵の生成、保管、管理する極めて耐タンパ性の高い機器）