資料２
一部非公開

検討項目②
機器の廃棄・データ消去について

総 務 省

令和８年 １月14日

総務省自治行政局住民制度課
サイバーセキュリティ対策室

前回いただいたご意見

前回の検討会では、国際的な動向を踏まえながらも自治体が実際に対応可能な手順を示すことが重要というご意見をいただいた。

検討項目	視点	発言要旨
機器の廃棄・データ消去方法	**1.政府統一基準群の記載内容との整合**	• NIST、IEEE等の**国際的な動向**や政府機関等との調整を行いながら今後の検討が必要となってくるのではないか。 • 個人情報保護法における「**個人データ消去**」の記載を確認し、違いについて言及しておく必要があるのではないか。
	2.機器の廃棄・データ消去等におけるプロセスの整理	**【破壊の記載】** • 物理破壊の手法として**「細断」**や**「切断」**と記載しているが、**委託事業者が実際にできるのかが不明**であり、委託事業者により**対応可否が異なる**場合が考えられる。そのため、ガイドラインに記載した方法が**必須なのか、推奨なのか明確にした方が良い**のではないか。 • 補足資料にメディアの種類ごとの適切な破壊方法をわかりやすい形で記載するのはどうか。 **【作業の立ち合い】** • マイナンバー利用事務系の情報資産を扱う記憶媒体の物理破壊作業を外部委託する場合における**職員の立会い**については、庁舎内での破壊作業に限らず、**庁舎外で実施される場合も対象となるかどうかを明確にした方が良い**のではないか。 **【ガイドライン改定内容】** • 自治体機密性2以上を取り扱う業務においては、個人情報を扱う場合があるので、個人情報保護法における安全管理措置に関する対応について言及しておいた方が良いのではないか。 • 除去や消去が出来ない場合は、物理破壊を行うといった記載もあった方が良いのではないか。 • 定期保守及び修理に関する対応についてガイドラインの改定案が示されたが、端末のHDDやSSDが故障し修理交換を行う場合の元の記憶媒体に関する廃棄について、もう少し分かりやすく記載した方が良いのではないか。

1．政府統一基準群の記載内容との整合（国際的な動向の確認）

NIST SP800-88 Rev2（Initial Public Draft）が2025年7月に公開、9月に確定版が公開された。
リユース等を踏まえ**暗号化消去の留意事項について追記**するのは如何か。

NIST SP800-88 Rev2

- 情報の機密性に応じた消去方法のフローについてはRev1から大きな変更はない。
- デバイス毎（HDD、SSD等）の消去方法に関してはIEEE2883を参照する構成に変更された。
- 暗号化消去に関する留意事項が示されている。

＜NIST SP800-88Rev2の主な変更内容＞

抹消方法	Rev1との 記載内容の主な違い
消去 **（Clear）**	主な違いはなし
除去 **（Purge）**	• 論理/仮想ストレージなどは、**暗号化消去が唯一の実行可能**なPurgeサニタイゼーション技術と言及（**暗号強度、暗号鍵の管理などについて留意事項を記載**） • 高い磁力を持つ磁気デバイスは、消磁は効果がない可能性を示唆
破壊 **（Destroy）**	• 曲げたり、切ったり、ストレージデバイスに穴をあけたりするような技術は、部分的な損傷を与えるだけで、最先端の研究室レベルの技術においては、アクセス可能な部分を残す可能性を示唆 ➢「分解」、「焼却」、「溶解」、「粉砕」、「細断」等の破壊について言及（Rev1とは変更なし）

＜NIST SP800-88Rev2を参考にガイドライン追記内容＞

項目	留意事項
暗号化消去の前提条件	• 情報を記憶媒体に格納する前に**記憶媒体の暗号化機能を有効**にしておく。 • 記憶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。
鍵の削除	• **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、記憶媒体名、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）

１．政府統一基準群の記載内容との整合（個人情報保護法との関係）

抹消方法における「消去」に関する説明に、個人情報保護法における「個人データの消去」関する記載を追加するのは如何か。

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）

3-4-1 データ内容の正確性の確保等（法第22条関係）

法第22条
　個人情報取扱事業者は、利用目的の達成に必要な範囲内において、個人データを正確かつ最新の内容に保つとともに、利用する必要がなくなったときは、当該**個人データを遅滞なく消去**するよう努めなければならない。

解説
（略）
「**個人データの消去**」とは、当該個人データを個人データとして使えなくすることであり、当該データを削除することのほか、当該データから特定の個人を識別できないようにすること等を含む。

データの抹消方法における「消去」

図表XX データ抹消方法

図表をガイドラインに追加予定

抹消方法：消去*
説明：

- データ抹消ソフトウェア、記憶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のデータを抹消する。
- 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（01）で上書きし（以下、「上書き消去」という）、対象のデータを非機密データ化する。

*個人情報保護法における「個人データの消去」については、当該データを削除することのほか、当該データから特定の個人を識別できないようにすること等を含んでいる。
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）3-4-1を参照されたい。

2.機器の廃棄・データ消去等におけるプロセスの整理（実態ヒアリングの結果①）

委託事業者等に対し現状のデータ消去の対応状況とガイドライン改定案に対する対応可否についてヒアリングを実施
【委託事業者（リース会社3社・データ消去事業者）、機器メーカー、自治体】

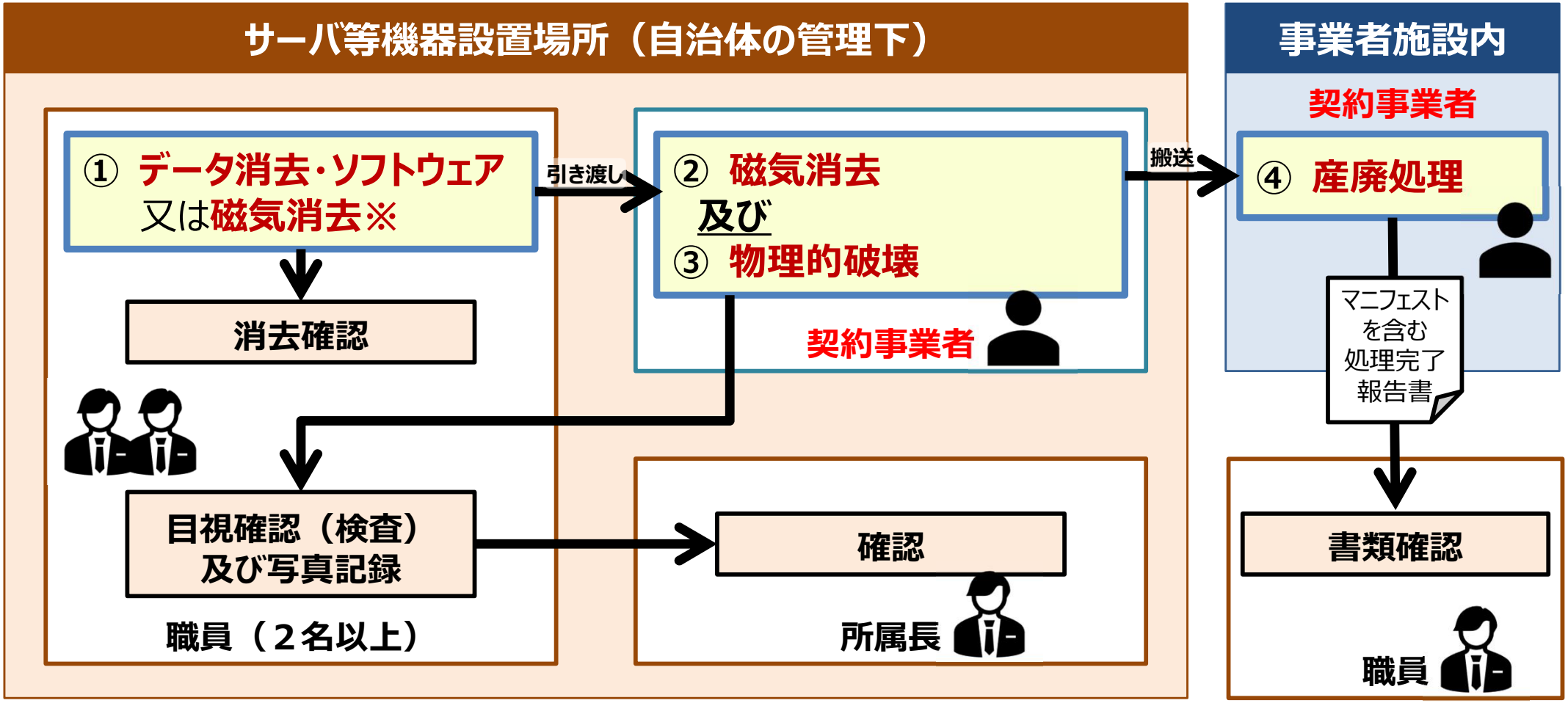
- HDDの破壊では、**専用の破壊機で穿孔（せんこう）破壊**処理をしているケースが多い。
- SSDの破壊では、**専用の破壊機で圧壊処理**を実施しているケースが多い。作業報告書に破壊前と破壊後の写真を掲載する場合は、**細断や粉砕処理は難しい**という意見や**高額な専用機器が必要**なことから**コストが高くなる**という意見があった。
- リース会社によると多くの自治体では、物理破壊の詳細方法がリース仕様書の定められていないという意見があった。（「物理破壊」のみの記載が多い）

抹消方法	リース会社	データ消去事業者	データ消去機器事業者	自治体
破壊（HDD）	指定が無い場合は、専用の破壊機で**穿孔破壊**	専用の破壊機で**穿孔破壊**（専用シュレッダー方式も可）	専用の**穿孔破壊機器** 専用のV字破壊機器を提供	専用の破壊機で**穿孔破壊**
破壊（SSD）	指定が無い場合は、専用の破壊機で**圧壊処理**	専用の破壊機で**圧壊処理**（**専用シュレッダー**による破壊も可）	専用の**圧壊機器** **専用シュレッダー**機器を提供	専用の破壊機で**圧壊処理**
除去	除去専用コマンドまたは暗号化消去（専用コマンドで対応できない場合は、物理破壊を行う）	磁気消去 (NSA認定機器を利用) 除去専用コマンド ソフトウェアを利用した消去	磁気消去 (NSA認定機器も提供) 除去専用コマンド ソフトウェアを利用した消去	磁気消去 (NSA認定機器を利用) 除去専用コマンド ソフトウェアを利用した消去
消去	除去専用コマンドを実行（対応していない場合、上書き消去＋検証を行う）	ソフトウェアを利用した消去	ソフトウェアを利用した消去	ソフトウェアを利用した消去

2.機器の廃棄・データ消去等におけるプロセスの整理（実態ヒアリングの結果②a）

■ **個人情報を含む重要な情報**を含む記憶媒体（**リース**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（リースの場合）

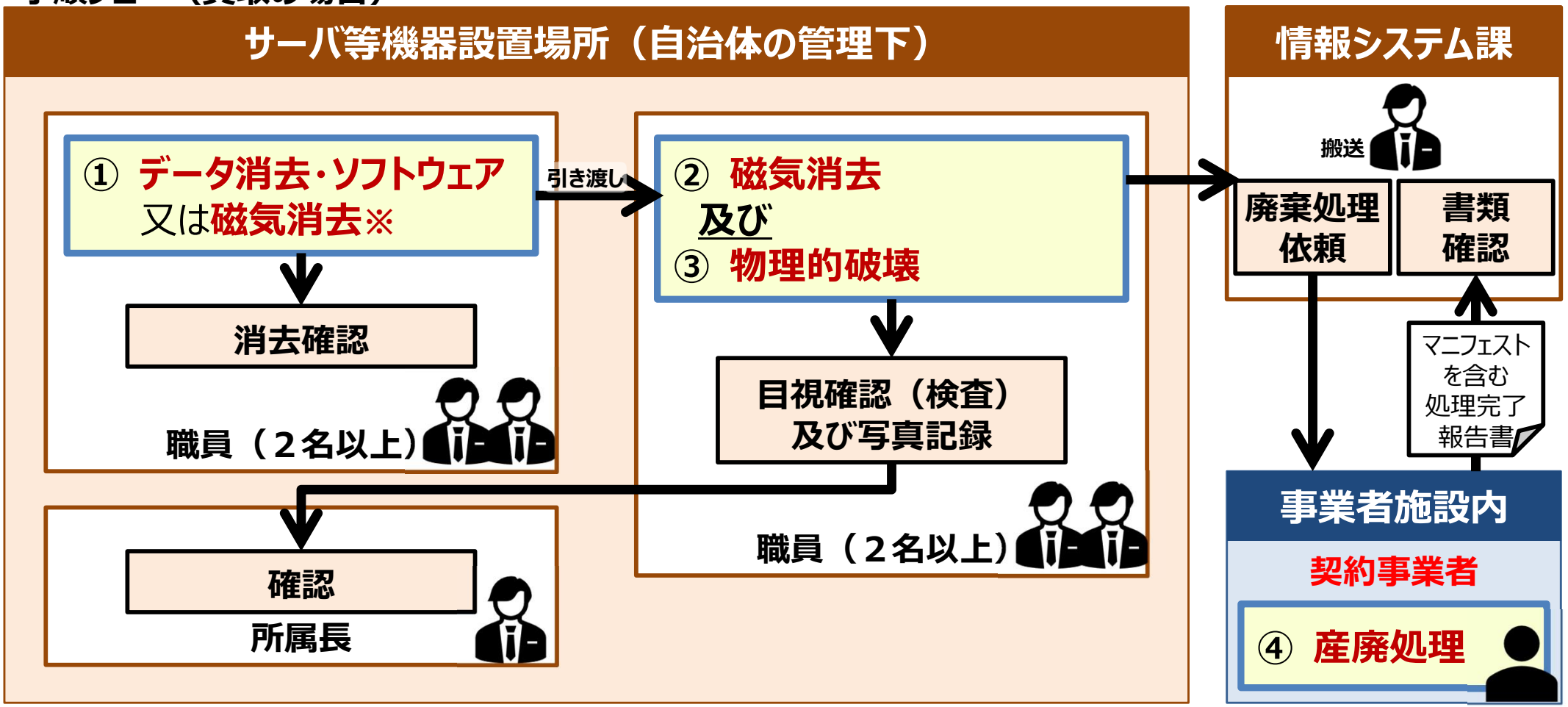


※ ソフトウェアによるデータ消去が困難なサーバ等は職員による磁気消去を実施
（その場合、契約事業者による磁気消去は不要）

2.機器の廃棄・データ消去等におけるプロセスの整理（実態ヒアリングの結果②b）

■ **個人情報を含む重要な情報**を含む記憶媒体（**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

2.機器の廃棄・データ消去等におけるプロセスの整理（破壊の記載）

「物理破壊」の実態としては、専用の破壊機で穿孔破壊や圧壊処理を行っていることから
統一基準群の内容を踏まえつつも確実な処理を行う手順についてガイドラインや補足資料に追加するのは如何か。

第19回検討会資料におけるガイドライン改定案（「図表XX 情報の機密性に応じた機器の廃棄等の方法」の破壊に関する記載箇所）

分類	抹消方法	機器の廃棄等の方法	
（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	破壊	ハードディスク	• 細断（情報記録している内部のディスクを物理的に破壊）
		SSD	• 切断（内部のメモリチップを破壊）
		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専用の機器にて記録層を破壊

ガイドライン改定案修正内容（「図表XX 情報の機密性に応じた機器の廃棄等の方法」の破壊に関する記載箇所）

		機器の廃棄等の方法
（１）マイナ 系の領域にお 保存する記憶 ※マイナンバ 社会保障、地方税、防災、戸 籍事務等に関 及びデータ	破壊	当該媒体を**細断するなど**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。ハードディスクの場合、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。
		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。ハードディスク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。
		• **メディアシュレッダーやメディアクラッシャー**等の専用の機器にて記録層を破壊

- **統一基準群記載の内容を参考に、「細断など」と明記することで「細断」は例示とする。**
- **穿孔の際の留意点を記載し、「穿孔」の場合における確実な処理に関する補足等を（処理前・処理後の写真等）補足資料に明記する。**

- **統一基準群記載の内容を参考に、「切断など」と明記することで「切断」を例示とする。**
- **メモリチップを破壊する方法として「圧壊処理」や「専用機器によるシュレッダー」があることを補足資料に明記する。**

CD/DVDやフロッピーディスク等のメディアシュレッダーの種類等は補足資料に追記する。

2.機器の廃棄・データ消去等におけるプロセスの整理（作業の立ち合い）

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のデータ消去作業における**「立ち合い」**については、
自治体の管理下（庁舎内）でデータが復元できない状態となっていることを「目視等」による確認と作業記録を残すことを求め、
委託先の作業においては「立ち合い」までは求めず、作業完了報告書を確認することで「立ち合い」の代替とするのは如何か。

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憶媒体のデータ消去の場合

自治体管理下における作業
- **職員による対応**
- **委託事業者による対応**

庁舎内

必須 **破壊** or **除去**

消去

【作業の確認】
データが復元困難な状態に
なっているか
↓
目視確認及び作業記録

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**

委託先における作業
- **委託事業者による対応**

委託先

必須 **破壊** or **除去**

消去がされた状態で
委託先に渡される

【作業の確認】
データが復元困難な状態に
なっているか
↓
作業完了報告書で確認
（作業前・作業後の写真）
（シリアルナンバーの記録）
（ログ等のレポート）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
記憶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）

データが復元困難な状態になっている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

ガイドラインの改定案（１）

解説の本文にデータの抹消方法に関する記述や機器の廃棄等の留意点について追記する。

現行：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。

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

改定案：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、機器内部の記憶**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 及び記憶**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**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。~~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。~~

（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XX「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XX「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。

項目	留意事項
暗号化消去の前提条件	• 情報を記憶媒体に格納する前に記憶媒体の暗号化機能を有効にしておく。 • 記憶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。
鍵の削除	• 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、記憶媒体名、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XX　暗号化消去における留意事項

ガイドラインの改定案（２）

抹消方法（破壊・除去・消去）に関する説明（以下の表）を追加（前回提示案の差分を**赤字**で記載）

【追加】図表XX データ抹消方法

抹消方法	説明	残存リスク等
破壊	• **細断、切断などの手法によりデータを格納した記憶媒体を完全に破壊**する。 • **HDD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、ハードディスク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デバイスを完全には破壊できない。確実に内部のデバイスを破壊すること。	• **一般的な物理破壊装置では**、細断の大きさにより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	• 記憶媒体専用のコマンドを使用して**記憶媒体の全エリアを抹消**する。 • その他の抹消方法として、**復号鍵の抹消（以下、「暗号化消去」という。）**、**消磁**等の手法がある。	• 記憶媒体を機器から取り出し、直接記憶媒体内を読み取りを行ったとしてもデータの復元は不可能。 • 記憶媒体によっては、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。
消去※	• データ抹消ソフトウェア、記憶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（01）で上書き**し（以下、上書き消去という）、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。 • 記憶媒体を機器から取り出し、直接記憶媒体内を読み取りを行うことでデータの復元はが可能。 • 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。

※個人情報保護法における「個人データの消去」については、当該データを削除することのほか、当該データから特定の個人を識別できないようにすること等を含んでいる。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）3-4-1を参照されたい。

ガイドラインの改定案（３）

統一基準群と同様に媒体別の廃棄等の方法を記載する。（前回提示案の差分を**赤字**で記載）

【更新】図表XX 情報の機密性に応じた機器の廃棄等の方法

統一基準群の記載内容を参考に改定する

分類	抹消方法	機器の廃棄等の方法	
（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	破壊	ハードディスク	**当該媒体を細断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。ハードディスクの場合、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。ハードディスク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専用の機器にて記録層を破壊
	除去	ハードディスク	• ATA コマンドの「Enhanced SECURITY ERASE UNIT」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 • 消磁 • 暗号化消去
		SSD	• 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 • 暗号化消去

破壊以外に除去も選択可能

ガイドラインの改定案（３）

（前回提示案の差分を**赤字**で記載）

（前頁の表からの続き）

統一基準群の記載内容を参考に改定する

分類	抹消方法		機器の廃棄等の方法
（２）**自治体機密性２以上に該当する情報を保存する記憶媒体**（上記（１）に該当するものを除く。）	破壊	ハードディスク	**当該媒体を細断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。ハードディスクの場合、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。ハードディスク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専用の機器にて記録層を破壊
	除去	ハードディスク	• ATA コマンドの「Enhanced SECURITY ERASE UNIT」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 • 消磁 • 暗号化消去
		SSD	• 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 • 暗号化消去
（３）**自治体機密性１に該当する情報を保存する記憶媒体**（**ハードディスク、USBメモリ、SSDにおいては、**上記（２）の抹消方法の除去選択も可）	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専用の機器にて記録層を破壊
	消去	ハードディスク	• 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」コマンドを使用する方法

ガイドラインの改定案（４）

【新規】図表XX 確実な履行を担保する方法　　（前回提示案の差分を**赤字**で記載）

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	**破壊**	各抹消方法における履行の担保	**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憶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、メディアシュレッダーやメディアクラッシャー等の専用の機器にて記録層を破壊
		作業手続きにおける履行の担保	**庁舎外に持ち出す場合** • 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。 • 委託事業者先にて破壊の抹消を行う場合は、庁舎内において（３）で記述する情報の復元が困難な状態まで抹消を行った上で、委託事業者等に引き渡しを行う。 **作業を委託する場合** • 職員が**庁舎内における委託事業者の破壊作業の立ち会いを行うなどして、データが復元できないことを目視で確認し、作業記録**を行うほか、庁舎内において（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**行ったことを目視で確認し、記録をしたうえで**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**（処理前と処理後）、記憶媒体におけるシリアルナンバー**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。 ~~• 職員による庁委託先事業者の破壊作業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。~~

ガイドラインの改定案（４）

（前頁の表からの続き）

（前回提示案の差分を**赤字**で記載）

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	**除去**	各抹消方法における履行の担保	**コマンドによる抹消** • 記憶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。 • 記憶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。 **消磁による抹消** • 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。 **暗号化消去** • 暗号鍵はバックアップ等を含む複製を含めて、確実に削除する。 **その他** • **記憶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。**
		作業手続きにおける履行の担保	**庁舎外に持ち出す場合** • 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。 • 委託事業者先にて除去や破壊の抹消を行う場合は、庁舎内において（３）で記述する情報の復元が困難な状態まで抹消を行った上で、委託事業者等に引き渡しを行う。 **作業を委託する場合** • **職員が庁舎内における委託事業者の除去作業の立ち会いを行うなどして、データが復元できないことを目視で確認し、作業記録を行うほか、庁舎内において（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ことを目視で確認し、記録をしたうえでで、委託事業者等に引き渡しを行い、委託事業者等が除去作業を実施し、当該除去の完了証明書により確認する。** • 委託事業者等がデータの抹消を実施する場合は、コマンド、消磁、暗号化消去の抹消方法や作業履歴が記載された完了証明書の納品する旨を仕様書に記載した上で契約を締結する。 • 作業証明書の仕様において作業が正常終了した証跡の添付する旨を記載する。

ガイドラインの改定案（４）

（前頁の表からの続き）

（前回提示案の差分を**赤字**で記載）

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憶媒体（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憶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	**庁舎外に持ち出す場合** • 委託事業者先にて破壊の抹消を行う場合は、庁舎内において（３）で記述する情報の復元が困難な状態まで抹消を行った上で、委託事業者等に引き渡しを行う。 **＜個人情報が含まれる場合＞** **• 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、「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。** • 委託事業者先にて破壊の抹消を行う場合は、庁舎内において（３）で記述する情報の復元が困難な状態まで抹消を行った上で、委託事業者等に引き渡しを行う。 **作業を委託する場合** • 委託事業者等に物理的な破壊作業を委託する場合、完了証明書により作業結果を確認する。 • 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。 **＜個人情報が含まれる場合＞** **• 職員が庁舎内における委託事業者の破壊作業の立ち会いを行うなどして、データが復元できないことを目視で確認し、作業記録を行うほか、庁舎内において（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ことを目視で確認し、記録をしたうえでで、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（処理前と処理後）、記憶媒体におけるシリアルナンバー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。**
	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憶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	

ガイドラインの改定案（４）

変更なし

（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憶媒体（上記（２）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	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憶媒体における破壊と同様
	消去	各抹消方法における履行の担保	**<u>コマンドによる抹消</u>** • 記憶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。 • 記憶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>データ抹消ソフトウェアによる抹消</u>** • 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	**<u>作業場所</u>** • 庁舎内または委託事業者先において消去を実施する。 **<u>作業を委託する場合</u>** • 委託事業者等がデータの抹消を実施する場合は、抹消方法や作業履歴が記載された完了証明書の納品する旨を仕様書に記載した上で契約を締結する。 • 作業証明書の仕様において作業が正常終了した証跡の添付する旨を記載する。

ガイドラインの改定案（５）

変更なし

機器等及び情報システムの調達時における機器の廃棄・データ消去の要件を明確化する旨を追加する。

現行：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。

改定案：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。

ガイドラインの改定案（５）

変更なし

業務委託（リース契約）の調達時における機器の廃棄・データ消去の要件を明確化する旨を追加する。

現行：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。

改定案：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。

ガイドラインの改定案（５）

機器の故障や保守における記憶媒体の交換時の機器の廃棄・データ消去の要件を明確化する旨を追加する。

現行：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。

改定案：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**。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。**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、**故障した記憶媒体等の破壊を行うとともに、**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。

故障時に機器交換などを行う際、故障した記憶媒体のデータ抹消（破壊）を行う旨を追加