

検討項目② 機器の廃棄・データ消去について【補足資料】



総務省

令和7年 6月23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

政府統一基準群とガイドライン①

- 政府統一基準群、ガイドラインともに情報を復元不可能な状態にすることを規定。

政府統一基準群 (※)

第3部 情報の取扱い 3.1 情報の取扱い

3.1.1 情報の取扱い

【遵守事項】

(7) 情報の消去

- (a) 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。
- (b) 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。
- (c) 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。

※「政府機関等のサイバーセキュリティ対策のための統一基準（令和5年度版）」「政府機関等の対策基準策定のためのガイドライン（令和5年度版）」

ガイドライン

第3編

2. 情報資産の分類と管理

【例文】

(2) 情報資産の管理

⑩情報資産の廃棄等

(ア) 情報資産の廃棄やリース返却等を行う者は、情報を記録している電磁的記録媒体について、その情報の機密性に応じ、情報を復元できないように処置しなければならない。

(イ) 情報資産の廃棄やリース返却等を行う者は、行った処理について、日時、担当者及び処理内容を記録しなければならない。

(ウ) 情報資産の廃棄やリース返却等を行う者は、情報セキュリティ管理者の許可を得なければならない。

4. 物理的セキュリティ 4.1. サーバ等の管理

【例文】

(7) 機器の廃棄等

情報システム管理者は、機器を廃棄、リース返却等をする場合、機器内部の記憶装置から、全ての情報を消去の上、復元不可能な状態にする措置を講じなければならない。

政府統一基準群とガイドライン②

■ 政府統一基準群

- **機密性の高い情報**（※）に係る方法と一般的な方法の例（磁気媒体とフラッシュメモリ媒体については特殊な手段により情報が読み出されるリスクが存在）の2つに分けて、電磁的記録媒体に記録されている情報の抹消方法を表で規定

※ 要機密情報（機密性2及び機密性3情報）に限らず、積極的に公表していない情報等、復元されるリスクを許容できない情報があることを想定し、当該情報を含めて「機密性の高い情報」と記載。

■ ガイドライン

- **機密性に応じて**情報システム機器の廃棄を行う（詳細は表で規定）。

政府統一基準群（※）

第3部 情報の取扱い 3.1 情報の取扱い

3.1.1 情報の取扱い

（解説）

- 遵守事項3.1.1(7)(b)「抹消する」について

（略）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を、

機密性の高さに応じて分けた以下二つの表において例示する。

磁気媒体及びフラッシュメモリ媒体に対して、「表3.1.1-1 情報の抹消方法の例」に記載の方法を用いた場合、特殊な手段を用いることによって情報（断片を含む）が読み出されるリスクが存在する。当該リスクを許容できないような機密性の高い情報を抹消する場合は、「表3.1.1-2 機密性の高い情報の抹消方法の例」に記載の方法を用いるとよい。

※「政府機関等の対策基準策定のためのガイドライン（令和5年度版）」

ガイドライン

第3編

4. 物理的セキュリティ 4.1. サーバ等の管理

【例文】

（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。

通知の内容は現在ガイドラインで規定

政府統一基準群（図表）① – 機密性の高い情報 –

■ 記憶媒体単位で抹消方式について記載されており、物理的破壊以外の方法も示されている。

表3.1.1-2 機密性の高い情報の抹消方法の例

磁気媒体（ハードディスクやフロッピーディスク等）	
抹消方式	注意点
（ハードディスクの場合） 暗号化消去 を行う方法	返却時の情報の抹消方法として暗号化消去を採用する場合は、OSやハードウェアの機能により、電磁的記録媒体へ書き込まれる情報が自動的に暗号化されるように設定された端末やサーバ装置等を導入し、運用の全期間を通じて暗号化することが前提となる。また、暗号化された情報の復号に用いる鍵については、基本対策事項7.1.5(1)-3 b)で策定を求めている管理手順に従って適切に管理するとともに、暗号化消去を行う際にはバックアップも含め鍵を確実に消去することが重要である。
（ハードディスクの場合） ATA コマンド の「Enhanced SECURITY ERASE UNIT」コマンドを使用する方法	コマンドがサポートされていることに注意が必要である。
（ハードディスクの場合） SCSIコマンド の「SCSI SANITIZE」コマンドや「SCSI Format」コマンドを使用する方法	コマンドがサポートされていることに注意が必要である。
磁気媒体を 消磁 装置に入れて当該媒体内の全てのデータを抹消する方法	（ハードディスクの場合） ハードディスクの磁気記録方式（水平磁気記録方式又は垂直磁気記録方式）に対応した消磁装置を用いる必要がある。 また、消磁装置は、装置の特性上経時的な劣化や、連続使用による温度上昇の影響を受けることに注意が必要である。
物理的に破壊 する方法	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、穿孔する際の穴の場所等の破壊の方法によっては、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。

政府統一基準群（図表）② – 機密性の高い情報 –

- 記憶媒体単位で抹消方式について記載されており、物理的破壊以外の方法も示されている。

フラッシュメモリ媒体（SSDやUSBメモリ等）	
抹消方式	注意点
（SSDの場合） 暗号化消去 を行う方法	返却時の情報の抹消方法として暗号化消去を採用する場合は、OSやハードウェアの機能により、電磁的記録媒体へ書き込まれる情報が自動的に暗号化されるように設定された端末やサーバ装置等を導入し、運用の全期間を通じて暗号化することが前提となる。また、暗号化された情報の復号に用いる鍵については、基本対策事項7.1.5(1)-3 b)で策定を求めている管理手順に従って適切に管理するとともに、暗号化消去を行う際にはバックアップも含め鍵を確実に消去することが重要である。
（SSDの場合） ATA コマンド の「BLOCK ERASE」コマンドを使用する方法	コマンドがサポートされていることに注意が必要である。
（SSDの場合） SCSIコマンド の「SCSI SANITIZE」コマンドや「SCSI Format」コマンドを使用する方法	コマンドがサポートされていることに注意が必要である。
（SSDの場合） NVMe（PCIe）コマンド の「NVMe Express Format」コマンドや「NVMe Express SANITIZE」コマンドを使用する方法	コマンドがサポートされていることに注意が必要である。
物理的に破壊 する方法	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。この場合、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使用しないこと。

光学媒体（CD-R/RW、DVD-R/RW等）	
抹消方式	注意点
物理的に破壊 する方法	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を用いることによって情報を記録している記録層を破壊する必要がある。なお、専用の機器は電磁的記録媒体に応じて存在するため、光学媒体以外の電磁的記録媒体を物理的に破壊する際においても、それぞれに対応した専用の機器を用いるとよい。

政府統一基準群（図表）③ – 一般的な方法 –

- 記憶媒体単位で抹消方式について記載されており、磁気媒体とフラッシュメモリ媒体に係るこれらの方式は、「特殊な手段を用いることによって情報（断片を含む）が読み出されるリスクが存在する」（「政府機関等の対策基準策定のためのガイドライン（令和5年度版）」3.1.1 情報の取扱い（解説））とされている。

表3.1.1-1情報の抹消方法の例

磁気媒体（ハードディスクやフロッピーディスク等）	
抹消方式	注意点
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	（ハードディスクの場合） データ抹消ソフトウェアがハードディスクの不良セクタ用の退避領域及びOSが認識不可能な隠し領域にアクセスすることができない場合、当該領域に対して上書きが行われないことに注意が必要である。
フラッシュメモリ媒体（SSDやUSBメモリ等）	
抹消方式	注意点
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抹消するソフトウェア）によりファイルを抹消する方法	ソリッドステートドライブ（以下本解説において「SSD」という）等のフラッシュメモリタイプの電磁的記録媒体は、データ書き込み回数に制限（寿命）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や動作の高速化等を目的に、媒体本体のファームウェアが管理する領域を持っており、データ抹消ソフトウェアによる上書きを1回実施した場合は実際にはデータの書き込みが行われず、消去すべき情報がそのまま残ってしまう現象が発生する可能性があるが、2回以上の上書きとすることにより、当該情報は抹消される。 また、データ抹消ソフトウェアが不良セクタ用の退避領域及びOSが認識不可能な隠し領域にアクセスすることが出来ない場合、当該領域に対して上書きが行われないことに注意が必要である。
（SSDの場合） ATA コマンド の「SECURITY ERASE UNIT」コマンドを使用する方法	コマンドがサポートされていることに注意が必要である。 また、OSが認識できないため、不良セクタ用の退避領域に対してコマンドによる上書きが行われないことや、USB接続ではサポートされないことに注意が必要である。

政府統一基準群（図表）④ – 一般的な方法 –

- 記憶媒体単位で抹消方式について記載されている。
- 光学媒体については、機密性の高い情報に係る方法と同様、物理的破壊のみが抹消方式として例示。

光学媒体（CD-R/RW、DVD-R/RW等）	
抹消方式	注意点
物理的に破壊する方法	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を用いることによって情報を記録している記録層を破壊する必要がある。なお、専用の機器は電磁的記録媒体に応じて存在するため、光学媒体以外の電磁的記録媒体を物理的に破壊する際においても、それぞれに対応した専用の機器を用いるとよい。

ガイドライン（図表）① – 機密性の高い情報 –

- ガイドラインでは、**マイナンバー利用事務系における住民情報、自治体機密性2以上の情報**に該当する情報、自治体機密性1に該当する情報の3つに分類（前者2つが機密性の高い情報）。
- **マイナンバー利用事務系における住民情報については物理的破壊のみ規定**しているが、自治体機密性2以上の情報については物理的破壊以外についても規定している。

第3編 4.1. サーバ等の管理（7）機器の廃棄等 図表41 情報の機密性に応じた機器の廃棄等の方法

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、いわゆる研究所レベルの攻撃からも耐えられるレベルで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。
※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）		

「いわゆる研究所レベルの攻撃からも耐えられるレベル」まで求めるか、政府統一基準群や技術動向を踏まえ要検討。

ガイドライン（図表）②－機密性の低い情報－

- 自治体機密性 1 に該当する情報について規定。

第 3 編 4.1. サーバ等の管理（7）機器の廃棄等 図表41 情報の機密性に応じた機器の廃棄等の方法

分類	機器の廃棄等の方法	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	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。

- 政府統一基準群では、高速であることと部分的な抹消が可能であることから、暗号化消去（暗号鍵の削除）を機密性の高さによらず優先的に検討すべきと規定した上で、クラウドサービスで取り扱った要機密情報の廃棄方法は暗号化消去等が考えられるとしている。
- ガイドラインにおいても、クラウドサービスにおける情報資産の破棄方法については、政府統一基準群と同様、方法の1つとして暗号化消去を挙げている。

政府統一基準群（※）

第3部 情報の取扱い 3.1 情報の取扱い

3.1.1 情報の取扱い

（解説）

● 遵守事項3.1.1(7)(b)「抹消する」について

（略）ただし、**暗号化消去は**、「表3.1.1-2 機密性の高い情報の抹消方法の例」に記載の方法ではあるが、**情報の抹消が高速に行えることや部分的な抹消が行えること等のメリットがあるため、機密性の高さによらず、抹消するための方法として優先的に検討するとよい。**

また、**クラウドサービスの利用を終了する際のクラウドサービスで取り扱った要機密情報を廃棄する方法は暗号化消去等が考えられる。**

（略）

※「政府機関等の対策基準策定のためのガイドライン（令和5年度版）」

ガイドライン

第3編

8. 業務委託と外部サービス（クラウドサービス）の利用

【例文】

（8）クラウドサービスを利用した情報システムの更改・廃棄時の対策

③クラウドサービス管理者は、クラウドサービス上で機密性の高い情報（住民情報等）を保存する場合は、機密性を維持するために暗号化するとともに、その**情報資産を破棄する際は、データ消去の方法の一つとして暗号化した鍵（暗号鍵）を削除**するなどにより、その情報資産を復元困難な状態としなければならない。

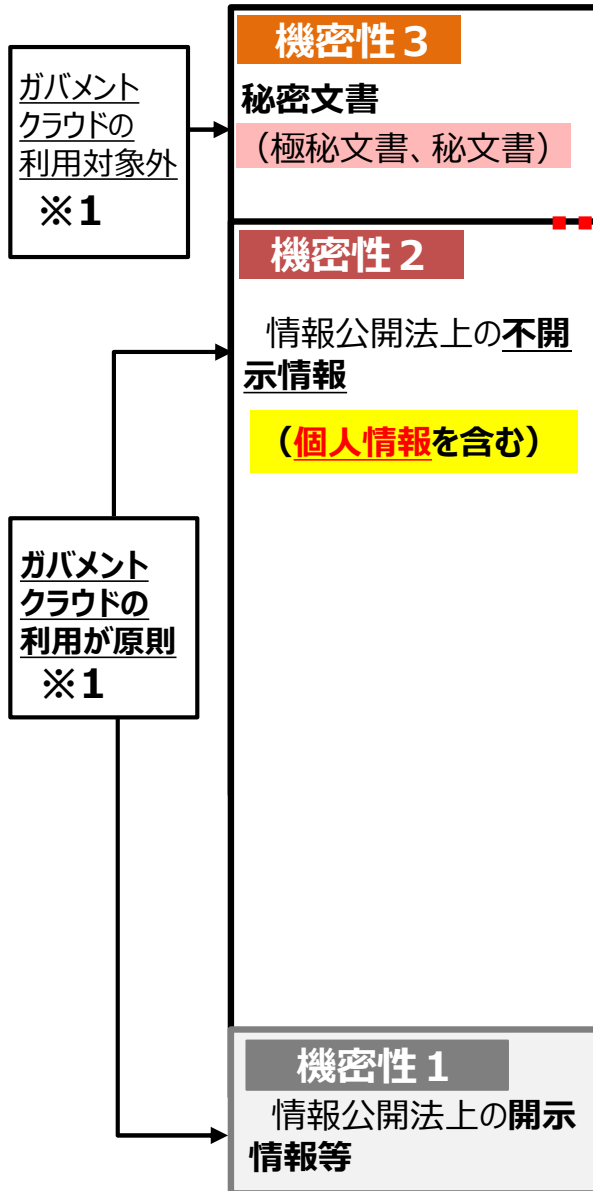
暗号化消去

情報を電磁的記録媒体に暗号化して記録しておき、情報の抹消が必要になった際に**情報の復号に用いる鍵を抹消することで情報の復号を不可能にし、情報を利用不能にする論理的削除方法。**

(参考) 政府統一基準群とガイドラインの機密性分類

国

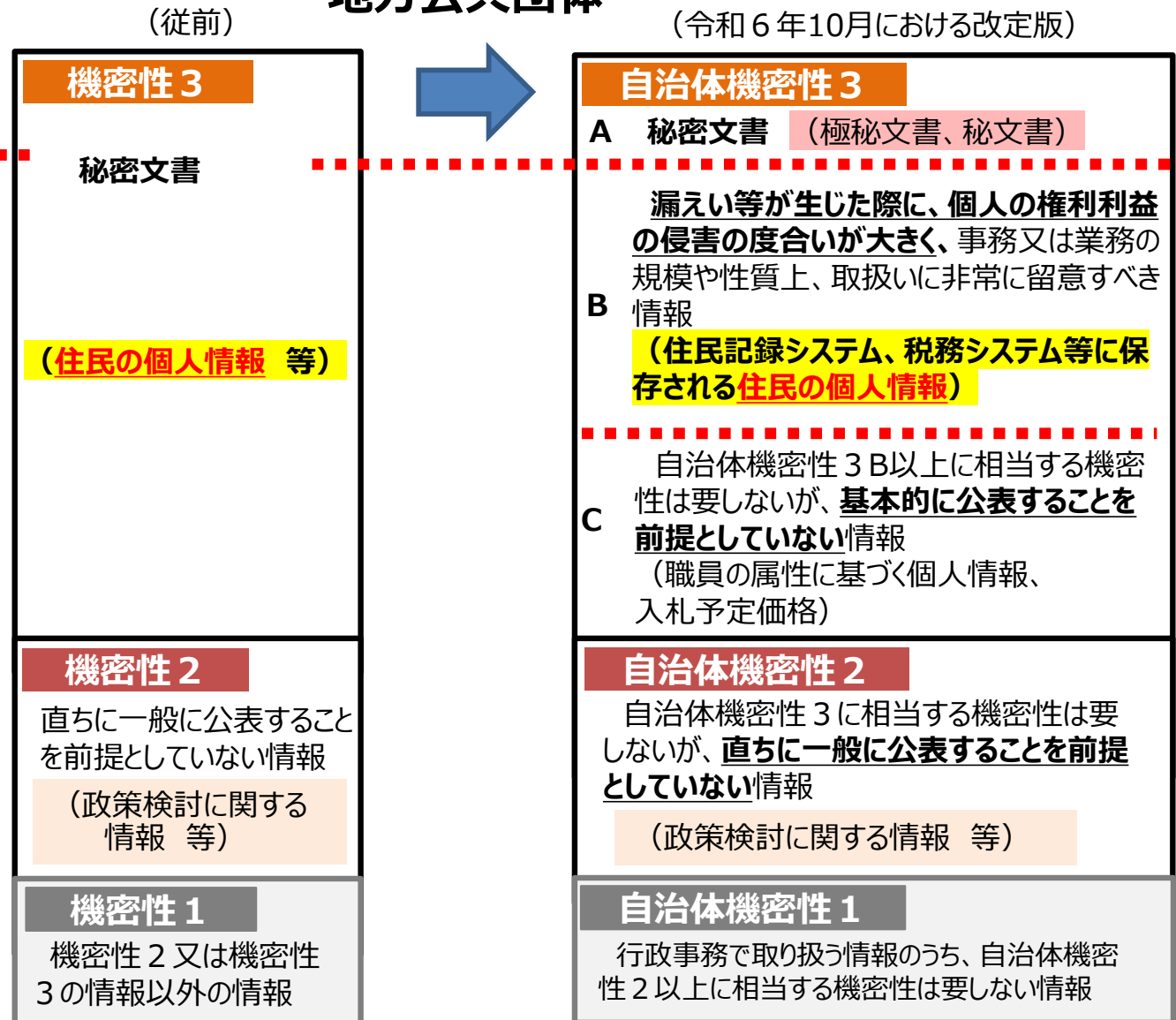
(政府機関等のサイバーセキュリティ対策のための統一基準群(政府統一基準群))



■ 政府統一基準群では、機密性 2 情報及び機密性 3 情報を「要機密情報」と定義している。

地方公共団体

(令和 6 年 10 月における改定版)



※ 1 政府情報システムにおけるクラウドサービスの適切な利用に係る基本方針 (令和 4 年 12 月 28 日 デジタル社会推進会議幹事会決定)