

検討項目② 機器の廃棄・データ消去について



総務省

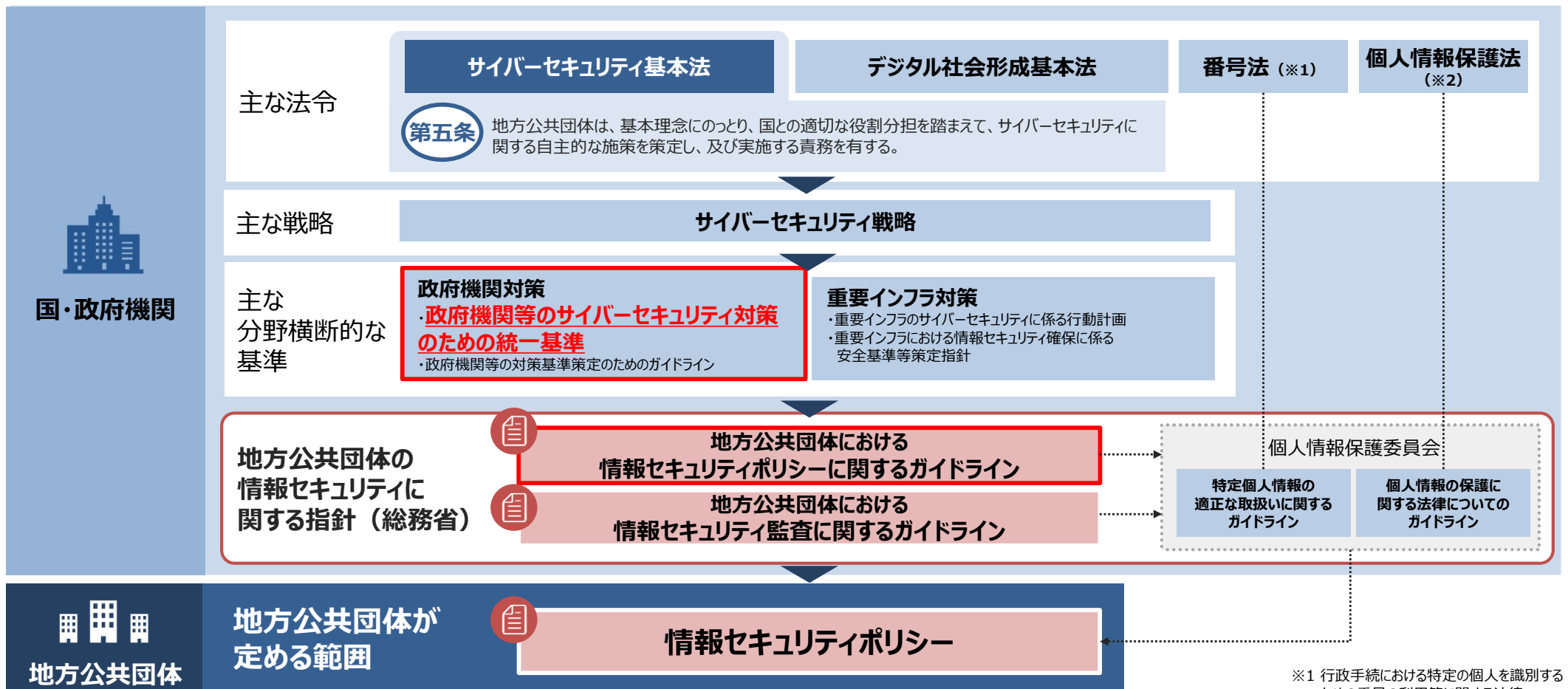
令和7年 6月23日

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

「政府機関等のサイバーセキュリティ対策のための統一基準」について

- サイバーセキュリティ基本法の枠組みの中で、「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」（以下「政府統一基準」という。）において国・政府機関に必要なセキュリティ対策を規定することとされている。
- 国・政府機関と整合性のとれたセキュリティ対策を地方公共団体にも提示する必要があることから、政府統一基準の改定内容を、ガイドラインに反映させている。



※1 行政手続における特定の個人を識別するための番号の利用等に関する法律

※2 個人情報の保護に関する法律

第17回検討会で提示した方針

- 今年3月の第17回の検討会で、機器の廃棄・データ消去に係る方法については、政府統一基準群等を踏まえ、整理することになった。
- まずは**政府統一基準群とガイドラインを比較し、どのような共通項・差異があるかについて整理**する。

地方公共団体からの意見（機器の廃棄について）

意見：機器の廃棄について

図表 41 「情報の機密性に応じた機器の廃棄等の方法」について、**(1)の「機器の廃棄等の方法」を(2)と同等にして良いのではないか。**「研究所レベルの攻撃」とあるが、近年のHDDやSSDに対して、(2)以外の(3)に記載された対策を実施したあとに、研究所レベルの方法でデータを取り出すことができた事例や論文等があればご教示されたい。

【理由】

- ・ (2)の方法でデータ消去としては十分であるため。リース契約では原則として物品はリース会社に返却すべきであるため。
- ・ (1)のすべての記憶媒体を分解・粉砕・溶解・焼却・細断等の方法(良くある「穴開け」のみでは要件を満たさないと解釈しています)で破壊するにはコストが高すぎるため。

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。

図表 41 情報の機密性に応じた機器の廃棄等の方法（抜粋）

対応方針

- 機器の廃棄方法については、**政府統一基準群（「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）」の「(7) 情報の消去」）等を踏まえ、詳細な検討が必要。**

政府統一基準群とガイドラインの比較（まとめ）①

- 政府統一基準群とガイドラインは両方とも、**情報の機密性に応じて**、情報を復元困難な状態にする措置を実施することを規定。
- 政府統一基準群はガイドラインと異なり、**機密性が高い情報に係る方法と一般的な方法の2つに区分**。

政府統一基準群

情報を復元困難な状態にする措置

補足資料 P1

- 電磁的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**ことを規定。

機密性分類の考慮

補足資料 P2

- 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旨を規定。

分類方法

政府統一基準群：
補足資料P2～6

ガイドライン：
補足資料P2,7,8

- 電磁的記録媒体に記録されている**情報の抹消の方法を、①機密性の高い情報に係る方法 ②一般的な方法の2つに区分の上、記憶媒体の種類（以下）ごとに規定**。

- ・ 磁気媒体
- ・ フラッシュメモリ媒体
- ・ 光学媒体

ガイドライン

- **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**とし、以下について規定。

- ・ 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。
- ・ 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。

- **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ことを原則としている。

- 記憶媒体の廃棄方法について、**①マイナンバー利用事務系の住民情報 ②その他自治体機密性2以上 ③自治体機密性1の3つに区分**し規定。

- (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
- (2) 自治体機密性分類2以上を保存する記憶媒体
- (3) 自治体機密性1を保存する記憶媒体

政府統一基準群とガイドラインの比較（まとめ）②

- 政府統一基準群では、機密性の高い情報に係る方法について、暗号化消去や物理的破壊以外も規定。
- ガイドラインでは、マイナンバー利用事務系の領域における住民情報を特別に扱い、物理的破壊と暗号化消去のみ認めており、その他自治体機密性 2 以上の情報に係る方法についても、政府統一基準群と差異がある。
- 情報が読みだされるリスクが許容される、機密性の低い情報に係る方法についても、政府統一基準で規定されている方法で、ガイドラインに規定されていないものがある。

政府統一基準群

機密性の高い情報

※ 要機密情報（機密性 2, 3）等復元されるリスクを許容できない情報

政府統一基準群：
補足資料 P3, 4

ガイドライン：
補足資料 P7

■ 磁気媒体

- ・ 暗号化消去（ハードディスク）
- ・ ATAコマンド（ハードディスク）
- ・ SCSIコマンド（ハードディスク）
- ・ 消磁
- ・ 物理的破壊

暗号化消去は、高速であることと部分的な抹消が可能な観点から、機密性の高さによらず推奨されている

補足資料 P9

■ フラッシュメモリ媒体

- ・ 暗号化消去（SSD）
- ・ ATAコマンド（SSD）
- ・ SCSIコマンド（SSD）
- ・ NVMe（PCIe）コマンド（SSD）
- ・ 物理的破壊

■ 光学媒体

- ・ 物理的破壊

■ 磁気媒体

- ・ 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）

■ フラッシュメモリ媒体

- ・ 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）
- ・ ATAコマンド（SSD）

ガイドライン

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

- ・ 物理的破壊
- ・ 暗号化消去（クラウドサービスの利用に係る箇所規定）

補足資料 P9

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（マイナンバー利用事務系における住民情報以外）

- *
 - ・ 物理的破壊
 - ・ 磁気的な方法による破壊
 - ・ OS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
 - ・ ブロック消去
 - ・ 暗号化消去

自治体機密性 1 に該当する情報を保存する記憶媒体

* 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

特殊な手段により情報が読みだされるリスクを許容

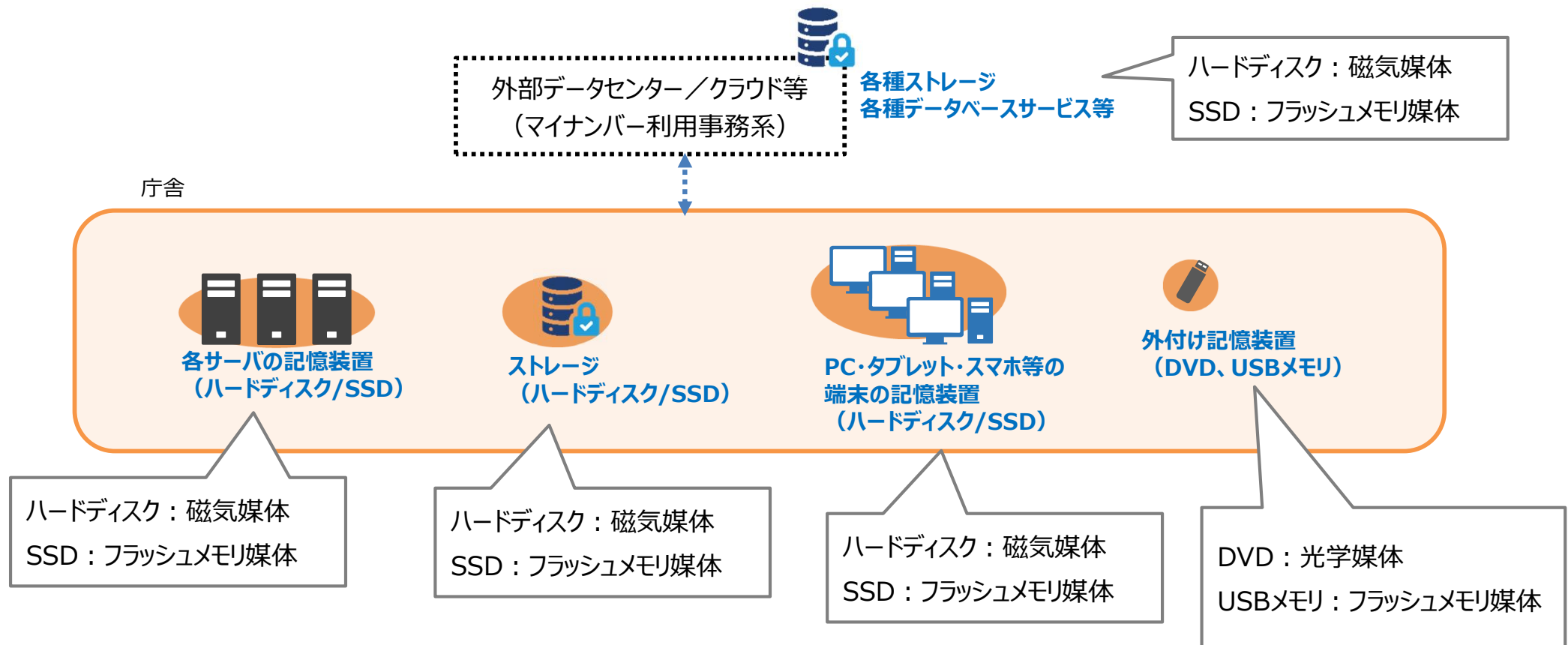
政府統一基準群：
補足資料 P5, 6

ガイドライン：
補足資料 P8

記憶媒体について

- 地方公共団体が業務で利用する記憶媒体は、政府統一基準群にあるように磁気媒体、フラッシュメモリ媒体、光学媒体に分類できる。

<例：マイナンバー利用事務系における主な記憶媒体>



過去の議論について

- マイナンバー利用事務系の領域で取り扱われる機器については、住民への説明責任等への観点から、物理的破壊が最も確実な方法とされた。

WGにおける議論の概要について

令和2年1月31日検討会資料

(機密性高の機器の廃棄方法及び履行確認の方法について)

- 高度な機密性を有する情報が記憶されている機器については、その廃棄を契機とした情報漏えいを確実に防ぐ必要があり、マイナンバー利用事務系の領域において取り扱われるサーバ・ストレージ、PC端末等の機器の廃棄については、復元不可能な状態にする必要があることから、最も確実な方法と考えられる「物理的破壊」を原則的に行うとすること。

※ NIST SP800-88(Rev1)においても、物理的破壊は、「破壊(destroy)」と位置づけられている。

※ なお、デバイス専用のコマンドを使用して上書き・ブロック消去・暗号消去に相当する手法についても、今後の議論の動向によっては、検討の余地があると考えられる。

- 廃棄の確認については、データの抹消措置を外部委託する場合(リース企業に行わせる場合も含む。)も含め、物理的破壊の完了を確実に確認する必要があることから、当該措置の完了まで職員の立ち会いによることとするが、庁舎内において、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、その後、物理的破壊が完了した旨の証明書を求める手法も考えられること。

※ osの初期化はデータが復元される可能性があるため、適当でない。

※ 証明書においては、破壊の証拠写真が添付されるとともに、その提出期限を明記することが望ましい。

(WGにおける意見)

- 機密度で分けず考える考え方は理解するものの、住民や議会への説明を考えると、全て物理的破壊せざるを得なくなるのではないかと。
- 物理的破壊は、機器を破壊作業を行う場所に持ち出す必要があり、盗難等のリスクが発生しないか。
- 機器を持ち運ぶ前に、一旦データ消去をした上で、破壊作業を行う場所で破壊すれば理解されるのではないかと。
- 機器によっては、マイナンバー系とそれ以外で共用している場合があり、現場で仕分けできるかも問題。
- 現在、国内のガイドラインでは位置づけられていないが、パブリッククラウドまで考えれば、暗号化消去による解決が重要ではないか。政府内で議論することが望ましい。暗号化消去では、鍵管理と実装が重要。
- 履行確認等において、自治体の負担に考慮する必要がある。

今後の方針

機密性の高い情報

- 自治体機密性 2 以上の情報（マイナンバー利用事務系における住民情報を除く）を保存する記憶媒体については、記憶媒体の種類ごとに、政府統一基準群に示されている方法とそろえる方向としてはいかがか。
- マイナンバー利用事務系における住民情報を保存する記憶媒体に係る方法については、住民への説明責任等の観点も含め、他の自治体機密性 2 以上の情報に係る方法と、同様の扱いとしてよいか検討することとしてはいかがか。

機密性の低い情報（情報が読みだされるリスクを許容）

- 基本的に記憶媒体の種類ごとに、政府統一基準群に提示されている方法とそろえる方向としてはいかがか。

共通

- 上記のいずれについても、手法の具体については、政府統一基準群の記載や関係する民間事業者等に最新の技術動向について確認の上、手法の説明文の記載（※）についても検討する必要がある。

※ 例えば、自治体機密性 2 以上の情報を保存する記憶媒体に求められている、「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」という記載が適切なのか等を検討する必要がある。

- 職員が現場で処理方法に困らないよう、必要に応じて、詳細な手順についても補足する。

図表イメージ

分類	記憶媒体	抹消方法	注意点・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	磁気媒体	(ハードディスクの場合) …	
		…	
	フラッシュメモリ媒体	(SSDの場合) …	
		…	
	光学媒体	(略)	
※ (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）			

分類	記憶媒体	抹消方法	注意点・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。）	磁気媒体	(ハードディスクの場合) …	
		…	
	フラッシュメモリ媒体	(SSDの場合) …	
		…	
	光学媒体	(略)	

マイナンバー利用事務系における住民情報は分けて検討し、その他自治体機密性 2 以上と同じ方法で問題ないということであれば統合

分類	記憶媒体	抹消方法	注意点・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	磁気媒体	(ハードディスクの場合) …	
		…	
	フラッシュメモリ媒体	(SSDの場合) …	
		…	
	光学媒体	(略)	