

# 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を改定

分類	機器廃棄等の方法	確実な履行を担保する方法
<p>(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</p> <p>* 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</p>	<p>当確媒体を分解・粉碎・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。</p> <p>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、物理的な破壊を行う。この場合は、予め仕様に明記のうえ、危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。</p>	<p>職員が左記措置の完了まで立ち合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けすが望ましい。</p>
<p>(2) 機密性2以上に該当する情報を保存する情報記憶媒体(上記(1)に該当するものを除く。)</p>	<p>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たえられるレベルで抹消を行うことが適当である。</p> <p>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。</p>	<p>庁舎内においては後述(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、抹消装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。</p>
<p>(3) 機密性1に該当する情報を保存する記憶媒体</p>	<p>一般的に入手可能な復元ツールの利用によっても復元困難な状態に消去することが適当である。</p> <p>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。</p> <p>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が残った状態となるため、適当ではない。</p>	<p>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。</p>
<p>* 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)</p>		

図表24 情報の機密性に応じた機器の廃棄等の方法