

総務省ガイドラインの変更に対応したデータ消去

総務省は、2023年3月に「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」を改定しました。今回の改定ポイントとともに、JECCグループのデジタルリユースが提供する、ガイドラインに準拠したデータ消去サービスについて紹介します。

■ ガイドラインの改定ポイント

行政データの情報漏えいに対する意識の高まりをふまえ、総務省では継続的にガイドラインを見直し、セキュリティ対策の強化を促してきました。2023年3月の改定では、情報システム機器を廃棄する際やリース返却の際に、情報を復元困難な状態にする措置の徹底を求めています。具体的には、廃棄・リース返却時のポイントとして「①データ消去により復元困難な状態にすること」、「②復元ツールを用いてもデータが読めないようにすること」、「③完了証明書などデータ消去の結果・証明を残すこと」の3点を挙げるとともに、情報の機密性に依拠して3段階のレベルを定め、レベルに応じたデータ消去の手法や対応を求めています（図1）。

このうち、特に機密レベルの高い「マイナンバー利用事務系に該当」では、いったん庁舎内で「Clear」レベル以上のデータ消去を行った上で委託事業者等に引き渡し、事業者による「Destroy」レベルの対応が完了するまで立ち会って確認することを求めています。ただし、立ち会いについてはカメラによるリアルタイム監視や映像記録の確認でも代替可能としています。

■ 推奨されるソフトウェアによるデータ消去

データ消去には、さまざまな方法があります（図2）。

（図1）情報の機密密度に応じたデータ消去

機密密度レベル	データ消去
マイナンバー利用事務系に該当	Destroy（破壊） 確実に復元を不可能にするレベル
機密性2	Purge（除去） 研究所レベルの攻撃にも耐えられるレベル
機密性1	Clear（消去） 一般的に入手可能な復元ツールでは復元困難なレベル

確実な消去法としては、まず物理的な破壊・粉碎がイメージされますが、SDGsの観点からは逆行します。その点、ソフトウェア消去であればリース・レンタル機器でも確実な消去が可能であり、機器の再利用によって、新規で購入調達するよりも環境負荷を低減させる効果があります。

近年では、従来のHDDに替わってSSDを搭載する情報機器が増えており、従来のソフトでは対応が困難ですが、米国国立標準技術研究所（NIST）規格に準拠したソフトであれば、確実なデータ消去が可能です。

■ デジタルリユースでの対応

デジタルリユースではガイドラインの改定以前から、米国国立標準技術研究所（NIST）規格に沿ったデータ消去サービスを提供しています。

同社は世界最高水準のデータ消去技術を持つBlanco社の日本における「Gold ITAD パートナー」兼「認定オンサイトデータ消去サービスパートナー」であり、全拠点でQMS・ISMSを取得しています。官公庁、自治体を含む案件を多く手がけ、2022年度では短期間に機器1万台、HDD/SSD2万台のデータを消去した事例もあり、年間では30万台以上のデータ消去実績を有しています。

● お問い合わせ

デジタルリユースが扱う商品・サービスの詳しい内容につきましては、下記までお気軽にお問い合わせください。

デジタルリユース株式会社 営業部
TEL：03-5370-8313

（図2）データ消去のさまざまな方法

消去方法	ソフトウェア消去	磁気消去	物理破壊・粉碎
HDD対応	○	○	○
SSD対応	○	×	○
SDGs視点	○	×	×

機密度が非常に高い場合は「ソフトウェア消去+磁気または破壊・粉碎」を推奨