# ハードディスク(HDD)処分の基本方針

## 1. 県の情報を保存したサーバー、パソコン、外付け HDD の処分原則

【重要情報のうち特定個人情報】

1. 県の管理下にあるうちに、物理的破壊を行う。実施者、実施日等の作業記録を残す。
2. 県職員が対応できない場合には、処分の完了まで県が責任を持って管理できる場合に限り、外部の者に委託することができる。外部の者による処分作業には、情報の復元が困難な状態まで、データの消去を県の管理下で行った上、物理的破壊が完了した旨の証明書を求める。この場合も、実施者、実施日等の作業記録を残す。

【重要情報及び一般情報】

1. 県職員が処分作業するほか、外部の者に処分を委託することができる。
2. 職員が処分作業する場合には、勤務時間に作業し、作業記録を残す。
3. 外部の者に処分を委託する場合には、守秘義務契約を結び、処分の方法(データ消去、物理的破壊等)を指定し、情報の復元が困難な状態までデータの消去を県の管理下で行った上、抹消措置が完了した旨の証明書を提出させる。

【重要情報】
① 島根県個人情報保護条例に規定する個人情報
② 島根県情報公開条例に規定する非公開情報
③ 所属長等が重要情報と同等の取扱いが必要と認めた情報

【一般情報】
重要情報以外の全ての情報

※「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 号通知) に基づき作成

## 2. 外部に委託する場合の措置

⑴ 外部の者の責務

委託する外部の者に対して、以下の対応をとらせることを必須とする(破壊後の粗大ゴミ等産業廃棄物として処理するだけの場合には、廃棄物処理法の規定による。)。

① 返却、廃棄、交換に係る処分計画書の提出(最低でも実施の一月前)

役割分担、対象 HDD、処分の方法、処分の作業場所、処分後の HDD の用途、再委託の有無、再委託先、再委託先の管理方法等を明らかにする。

② 県から持ち出した HDD のシリアル番号のリストなど一意に特定できる証拠書類の提出(実施後、速やかに県に提出)

③ 廃棄(消去)証明書の提出(期限を定める)、②の書類と突き合わせ。

（廃棄証明書の参考様式は、所属長及びセキュリティ担当者の情報セキュリティ対策実施手順書を参照）

④　処分の方法は、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をデータ消去装置又はデータ消去ソフトによる上書き消去、④ブロック消去、⑤暗号化消去　のうちのいずれかの方法を選択する。（特定個人情報は、①に限る。）

※一般情報の処分の場合は、OS 等からｱｸｾｽ可能な全てのｽﾄﾚｰｼﾞ領域をﾃﾞｰﾀ消去ｿﾌﾄｳｪｱにより上書き消去することも可とする。

⑵　県職員の責務

①　外部の者に処分を委託する場合には、委託する外部の者から提出された処分計画により処分の全体像を把握する。

②　HDD のデータ復元ができないことを職員が確認できるポイント（消去コマンド実行時、物理破壊後の保管時等）を協議して決定し、立ち会う。立ち会う時間は勤務時間内とする。

※OS の初期化、および記憶装置の初期化（ﾌｫｰﾏｯﾄ等）による方法はﾃﾞｰﾀが復元される可能性があるため不可。

※ユーザデータ領域（リカバリ領域、クリップ領域）及び再割り当て済みセクタにデータ保存している場合、ソフトウエアでは読み出し不可能であるが、データ復旧やデジタルフォレンジックを行う機器等を用いることによりデータにアクセスすることが可能となるため注意が必要。

③　故障時の部品交換時は、職員の立ち会いは不要とするが、守秘義務契約を結び、処分の方法を確認し、完了後に証明書を提出させる。

⑶　第三者による消去証明

消去作業者自身ではなく第三者による証明を一般社団法人コンピュータソフトウエア協会が「データ適正消去実行証明書」発行事業として行っているので利用することも推奨する。

## ３．現行契約にかかる当面の対応（特にリース物件のサーバー）

⑴　契約内容の確認（契約終了後の取扱い、撤去作業者、処分方法、処分作業者、処分後の履行確認方法等）

⑵　契約変更の協議（リース物件のうち HDD の所有権の移転、職員立ち会いの可否、立ち会いポイント等）し、対応可能ならば契約変更

⑶　対応が不明な場合には、情報システム推進課に個別に相談

## 4. 今後の対応（情報システム更新時等）

⑴　新システム構想時には、情報システム推進課の仮想サーバー基盤（オープン基盤、セキュリティクラウド基盤）の利用を検討する。（更新する情報システムの側は、専用の HDD がないので廃止届提出のみで完了。）

⑵　仮想サーバ基盤を使わない場合には、調達仕様書に契約終了時の HDD の処分に係る対応を詳細に明記する。

※重要情報のうち特定個人情報については、リース契約の場合も、終了後物理的破壊を行う旨を明記すること。

⑶　HDD 全体の暗号化（HDD を取り出して別の機器に接続しても解読不可能になる。）、もしくは HDD 内にデータを暗号化して保存する技術を導入する。

**参考情報（R2.3 月時点）**

○　「データ消去」とは、データを上書きすることによって「データ復元ソフトを使っても復元できないようにすること」であるが、日本政府が認定したデータ消去に関する規格はない。

○　データ消去に関する世界的な規格として、NIST（米国国立標準技術研究所）が 2006 年に策定した SP800-88 があり、「ディスク全域に固定値1回の上書きを行うことで十分である。」とされた。

　また、2014 年の改定版であるリビジョン1では、「ディスク全域に固定値1回の上書きを行うことで、研究所レベルの高度な読み出し方法を試行しても、 データの読み出しは不可能である。」としている。

○　神奈川県が公表した HDD 盗難事件の根本原因は以下のとおりとされている。「ハードディスク（HDD）処分の基本的方針（P10、11）」は、この根本原因に対応していると考える。

　　原因1　契約内容不備（データ消去作業の実施主体不明確など）
　　原因2　県の監督責任（機器返却後は関与なしなど）

「県情報を保存するために使用した情報機器からの情報流出防止策」
（令和2年1月神奈川県総務局 ICT 推進部情報システム課）から抜粋

○　神奈川県総務局市原 ICT 推進部長の自治体 CIO フォーラムでの発言（令和 2 年 2 月）

「HDD はデータ消去専用ソフトで消去すれば復元できないことを自分で確認した。」

○　SSD の取扱いについては HDD に準ずることを原則とする。
　※製造者のみが管理する領域等のデータ消去に留意が必要。

○　HDD の処分に関し、サーバーの HDD については、「システム管理者向けセキュリティ共通実施手順書」に、パソコンや外付け HDD の処分方法については、「所属長及びセキュリティ担当者の情報セキュリティ対策実施手順書」に明記している。（*今後、順次改定する。*）

○　サービス利用の契約終了時の取扱いについては別途検討する　が、
当面は、「データ消去の証明書を徴収すること」を契約時に明記すること。