応般 Jr.

神奈川県ハードディスク流出事件
― HDD 廃棄時にデータ消去はどうあるべきか―

上原哲太郎 | 立命館大学　情報理工学部

事件の経緯

2019 年 12 月，インターネットオークションにおいて販売されていたハードディスクドライブ（HDD）内から神奈川県の行政文書が大量に発見されたことが報じられた[1]．持ち出されたデータ量が膨大であったこと，税に関する記録など機微性が高い情報が含まれていたこと，流出経路がリサイクル事業者の従業員による盗難であり，社会的影響が大きいことから広い関心を集めた．

新聞報道など[1), 2)]によると，事件の経緯は以下の通りである．2019 年 2 月末，神奈川県（以下，県と略す）において庁内ファイルサーバの更新が行われ，リースされていた旧サーバがリース会社 F 社に返却された．当該リース契約では，データ漏洩を防ぐため返却後，F 社側でデータ復旧が不可能とされる方法で当該サーバの HDD の消去作業を行うこととされており，また作業完了後に消去証明書を神奈川県に提出する旨が定められていた．

F 社はこの HDD の消去作業を，情報機器のリサイクルや廃棄業務を行っている B 社に行わせるため売却し，B 社は F 社の指示で HDD を直接県から引き取った．両社の売買契約では，HDD が動作すればデータを専用ソフトで消去し，動かなければ物理的に破壊するとされていた．

当該 HDD は B 社施設において消去と破壊作業に供された．この際，その作業に従事していた B 社従業員が HDD のうち 18 台を持ち帰り，オークションにおいて転売した．7 月下旬，このうち 9 台を落札した人が当該 HDD 内にデータが残存していることに気づき，調べたところ神奈川県に関係する文書が大量に含まれていることから，朝日新聞社に相談した[3]．朝日新聞社は調査を行った上で 11 月下旬に県に通知し，12 月 6 日に報道したことでデータの流出が公になった．

事故原因の分析

本事件の直接的な原因は，B 社において廃棄処分に供される HDD の個体管理が不十分であったほか，そもそも B 社の作業拠点において盗難防止策が十分でなかったことである．B 社テクニカルセンターでは IC カードと指紋認証による入退室管理が行われており，従業員による持ち出しを防ぐための手荷物検査も行われていたが，早朝や深夜に出退勤する場合には手荷物検査は行われていなかった．元従業員は早朝に出勤しており，すでに廃棄対象になっていた HDD であれば容易に持ち出せたとしている．B 社は当該業務を登録範囲として ISO/IEC 27001 認証（ISMS 認証）を取得しているが，この認証が作業品質の十分な担保になっていなかったことは大きな問題であろう．

なお一般に，記憶媒体を持つ機器のリース契約においては，返却時のデータ消去は利用者側の責任で行う．しかし県とF社の契約においては，リース契約の中に返却時のデータ消去とその完了報告書の提出が含まれていた．F社は実際には自社ではその作業を行わずにHDDをB社に売却しており，B社は記者会見において，県のHDD処分に関する契約において消去作業の完了報告書の提出を求められていないとしている．F社とB社の間の契約については県に伝わっていなかったため，結果的に県にとっては当該機器が管理下を離れた後に，作業内容も，その結果も知り得ない状態でデータ消去作業が行われていたことになる．

このような矛盾が生まれた背景には，公共調達における入札制度固有の問題が考えられる．HDDの安全な消去や廃棄という作業を，各HDD個体の作業履歴を保存しながら確実に履行することはコスト負担が高い．当該リース契約においては，機器撤去作業にかかる費用をすべて含んだ額で入札が行われているため，実際の撤去作業に際しては調達仕様に明示がなければ各HDD個体に対して消去証明を作成することはないと思われる．リース契約内にデータ消去作業を含める場合，その作業の質を担保するためには，契約内で作業内容や作業完了報告書への記載事項について詳細を定めておくべきであろう．

そもそも本来，データ漏洩の防止のためには，データが自らの管理を離れる時点で適切に消去されるべきである．実は県はF社への返却前に，別の事業者にHDD消去作業を業務委託していたが，その作業が適切ではなかった．どのような技術的手段でHDDの消去をすればファイルが回復不能になるのか，作業発注者にも受注者にも理解されていなかったのである．

HDDのデータ消去の在り方

本事件の直後に総務省は各自治体に通知を発し，重要な情報が大量に保管されたHDDについて「物理的または磁気的破壊をすること」「作業に自治体職員が立ち会うこと」を求めた．しかし，リース機器やデータセンタ上の契約サーバなど，機器の所有権が利用者にない場合には，HDDのデータ消去を物理的に行うことは容易ではなく，論理的なデータ消去に頼らざるを得ない．

論理的なデータ消去に関する技術的基準については，米国NIST SP800-88Rev.1[4]が広く参照されている（表-1）．同文書では，記憶媒体の消去をその重要度と再利用の有無等に応じてClear, Purge, Destroyの3種類のいずれかの処理を行うことを求めている．HDDにおいては，ClearはHDDのユーザ領域全域にわたる最低1回の上書きを意味するが，これでは代替セクタ領域等にわずかな情報が残存する可能性がある．そこでPurgeでは，ATA☆1

☆1 ANSIで定められた，最も普及しているHDDインタフェース規格．

表-1 NIST SP800-88Rev.1に基づくATA HDD消去の分類と課題（課題は筆者による）
Categories and their issues on ATA HDD Sanitization Methods based on NIST SP800-88Rev.1

判断の基準	処理の種類	技術的手段	課題
重要性高かつ組織管理を離れる または 重要性中・再利用なし	Destroy	定められた機器や手順で物理的に破壊するか磁気的に破壊する	十分破壊しなければ磁気力顕微鏡によりデータが読める可能性が残る 磁気的破壊は消去確認が困難
重要性高・再利用あり，かつ組織管理下に残る または 重要性中・再利用あり，かつ組織管理を離れる または 重要性低・組織管理を離れる	Purge	ATAで定められたEXT OVERWRITEやSECURITY ERASE UNITなど専用コマンドで上書きかCryptographic Eraseを行う	正しく実行されたことを確認する必要 正しく実装されていない機器が見つかっている
重要性中・再利用あり，組織管理下に残る または 重要性低・組織管理下に残る	Clear	定められたツールを用いて固定値で最低1回上書きする	代替セクタにデータが残留する

のSecure Erase機能等を用いたHDDコントローラによる消去，または利用時に全データを暗号化しておき，廃棄時に鍵を消去するCryptographic Erase（以下CE）を求めている．Destroyでは，物理的または磁気的な破壊を求めている．我が国でもデジタル・フォレンジック研究会「データ消去」分科会の報告書[☆2]において同文書の内容を中心に消去技術について詳しく分析している．データ適正消去実行証明協議会はHDD等がどのように消去されたかを証明する手順と証明書の書式を標準化している[☆3]．

これらの基準が存在する中で，最も大きな問題は我が国ではCEに関する十分な技術的評価が行われていないことであろう．国が公表している各種ガイドラインにおいても，HDD等の媒体の消去に際しCEをどう位置づけるかは明記されていない．暗号技術検討会（CRYPTREC）においてもCEに関して検討されたことはなく，HDD暗号化向けの暗号利用モードXTSに関する安全性評価が行われた程度である[5]．HDDはその大容量化に伴い，ユーザ領域全域への書き込みにかかる時間が1台あたり数時間を要するようになったため，データ上書きによる消去作業は困難になってきており，代替策としてCEの利用が望まれる．ユーザ領域の消去では残存データの心配があるソリッドステートドライブ（SSD）を使用する際や，データ消去を利用者が確認することが一般に困難なデータセンタやクラウドの利用時にもCEは有効である．

しかし，CEを安全に運用するためには暗号化方式の選択と鍵管理に注意を要する．たとえば，暗号鍵が容易に複製可能である場合には，CE実行時には複製された鍵がすべて消去したことが確認できなければならないからである．近年暗号化機能を内蔵したHDDやSSDとしてSelf Encrypting Drive（SED）が普及しはじめており，Trusted Computing Groupが定めたOpalなどの規格化も進んでいる．SEDは媒体内に鍵が保存されているため鍵管理が容易になり，CEが確実に実行されたことが確認しやすい．このSEDの利用を含め，まずはCEの運用に関する技術的な要件を定めることが必要であろう．

また，CEを含めた論理的消去やHDDの磁気的破壊については，データが復元不可能になったことを外形上確認しにくいという問題もある．特にSSDについてはSecure Erase機能の実装が適切でない媒体が発見されている問題もあるため，いかにデータが消去されたことを確認し，その証跡を残すべきかという運用上の問題についても標準的なガイドラインが必要と思われる．

この事件を機にHDD等の記憶媒体の破壊による廃棄が増加し，情報機器の再利用が阻害されることは，環境負荷の増加や情報システム運用の社会的コスト上昇を招きかねない．むしろこの事件がHDD等の論理消去やCEのための技術的要件の整理と標準的な運用法確立の契機となることを望みたい．

参考文献

1) 神奈川県文書，大規模流出　個人の納税情報など　廃棄業者社員，HDD転売，朝日新聞朝刊，2019年12月6日．
2) 神奈川県のハードディスク 廃棄業者がネット競売に，NHK政治マガジン，https://www.nhk.or.jp/politics/articles/statement/27177.html, 2019年12月6日．
3) （データはどこへ　HDD流出）難なく復元5000万件…絶句　落札男性「背筋寒くなった」，朝日新聞朝刊，2019年12月7日．
4) Kissel, R., Regenscheid, A., Scholl, M. and Stine, K.: Guidelines for Media Sanitization, NIST SP800-SP88 revision 1 (2014).
5) 峯松一彦：暗号利用モードXTSの安全性に関する調査及び評価，CRYPTREC外部調査報告書 EX-2801-2018 (2019).

（2020年1月13日受付）

上原哲太郎（正会員） t-uehara@fc.ritsumei.ac.jp

和歌山大学，京都大学，総務省を経て2013年より立命館大学情報理工学部教授．デジタル・フォレンジック研究会副会長，芦屋市CIO補佐官．専門はサイバーセキュリティ，システム管理．自治体情報システムの調達や運用にも詳しい．

☆2 デジタル・フォレンジック研究会「証拠保全先媒体のデータ抹消に関する報告書」，https://digitalforensic.jp/home/act/products/data_report/ (2016).

☆3 データ適正消去実行証明協議会消去技術認証基準委員会「データ消去技術ガイドブック」第2版，https://adec-cert.jp/guidebook/pdf/DATAWIPEGUIDEBOOK.pdf (2019).