2015/12/03

3 週にわたり、私、日東造機株式会社の唐鎌が、データ消去に関する欧米や日本の動向についてお伝えしています。今回は第二章　データ消去についてお話しします。

第一章　欧米の磁気消去・物理破壊の変遷と日本の動向 ≫

第二章　信頼できるデータ消去方法の種類と利用時の注意点

第三章　日東造機の新たな挑戦（12/10 公開予定）

DB-50Pro

情報システムの担当者はデータ消去方法には、次の 3 通りあることはご存知だと思いますが、ここに改めてパソコン 3R に関わるデータセキュリティについて述べます。

買い替えし譲渡・廃棄する旧機のパソコンやスマートフォンのデータ消去、信頼しているけどしっかりデータ消去されているのだろうか？

パソコン内 HDD（情報を記録する装置）のデータ消去“信頼しているけど”とか、“しっかり”とかデータ消去の必要性や解決方策について問いました。

2005 年データ消去の脆弱性について啓発活動する“キャッチコピー”フレーズがこの問いでした。

そして、データ消去とかデータ抹消とかの言葉から　“消え去る”、“完璧に消す”を連想し、多くの方がこの言葉に安心しました。

勿論、3 つのデータ消去手法は、それぞれ一長一短で譲渡・廃棄の仕方は企業によって異なりますが、当時の企業認識は下記の 3 つでした。

①リース品だからリース会社に一任した。

②自社購入だが、まだ役立つのであればとパソコンリユース事業者へ一任した。

③産業廃棄物して産廃収集、中間処理業者に一任した。

いかがでしょうか？。
一任で・・・で安心・安全だと言えるでしょうか！　信用しているけど・・・人はかならずミスを犯します。
その程度も、日常の“うっかり”から体調不良時の“うっかり”や心が混乱している時の“うっかり”と様々で、情報が残ったままの HDD がデータ消去の確認をしないまま中古市場で販売されることが話題（NHK　廃棄パソコンにデータが残っていた）にもなりました。
そして今、これまでのデータ消去の 3 つの指針（JEITA/PC3Rweb 参照）は大きな技術革新により、見直しが求められています。
その理由は・・・。
新しいキーワード①”垂直記録 HDD”、②”フラッシュメモリー”、③”磁気シールド ”というハード的な技術革新と④データ消去は目の前が原則。⑤どのような方法で上書き消去したかのログがとれること。・・・というヒューマン的な脆弱性にスポットが当っています。
では、現在の日本のデータ消去の指針はどうなっているのでしょうか？
自治体の多くがホームページでリンクしている PC3R 推進協会のパソコンの廃棄・譲渡時におけるハードディスク上のデータ消去に関する留意事項（出典：PC3R 及び JEITA）や、マイナンバー制度では特定個人情報等が記録された機器及び電子媒体等を廃棄する場合、専用のデータ削除ソフトウェアの利用又は物理的な破壊等により、復元不可能な手段を採用と記されています。

この記事の目次 [hide]

PC3R や JEITA による消去方法

①専用ソフトにて HDD 全体を固定パターン等にて一回以上、上書きすることにより塗りつぶしてデータを消す方法
②専用装置にて強磁場（磁界）をかけて消す方法

③HDD に対して物理的に破壊する方法

①上書き し塗りつぶしてデータを消す

この場合、基本は 2 進数固定パターンで、一回上書きを行うことによって、十分消去することが可能ですが、念の為　2 回上書きすれば、ほぼ復元は不可能だと言える。
なお、最近の HDD はデータ量、消去レベルによって数十分から数十時間かかることや、OS が認識できない領域も消去するには特別な消去ソフトが必要であるとか、通常の IDE 接

続の HDD 上のデータなら消去できる一方で、サーバーやストレージ機に使われる別の接続形式（SCSI、RAID など）では、制限や対応していない場合があります。
したがいまして消去が正常に終了したか、エラーが発生したかといった記録（ログ）がとれる消去ソフトが推奨されています。

②強磁場（磁界）をかけて消す

HDD 書き込み磁力（抗磁力）の 1、3 倍以上（10000oe）の強磁場を照射し NS 層を破壊消去します。
尚、確かに消去／消磁されたことの証明が困難であることから最近では物理的な破壊と併用される場合が多いようです。
その理由は・・・

ハードディスクドライブ(HDD) は汎用品から高性能品まで様々であり、外部磁気の影響を考慮しないものや、書き込まれたデータを保護するため、金属ケースを磁気シールドしている高性能 HDD も存在します。
困ったことに、この「水平記録」から「垂直記録」HDD の登場や、USB メモリのようにフラッシュを使用したソリッドステートデバイス（SSD）を搭載した PC が広まり始めていますが、このような HDD やフラッシュメモリーは従来の磁気消去では消えません。

③物理的に破壊する

こうした一方で、HDD を物理的にドリルで穴を開けたり、中のディスクを破断して、読み取りできないようにする方法は見た目に破壊が確認できるデータ物理破壊になります。
専用の破壊機（クラッシャー）は HDD に孔をあけ折り曲げする製品や SSD に対してもメモリーチップ毎に破壊することで読み取りできないようにする専用機も登場しています。
以上から新たなデータ消去 3 つの手法が求められています。
（1）ソフトによる消去は HDD の全エリアを塗り潰し書き込みで消去し、操作ログが取れることが必要。

（2）強力磁場をかける消去は 10000 oe 以上を照射する。防衛省等、米軍とリンクする情報の場合、NSA T-4 認証の採用、消去の確認が取れない場合は物理破壊を併用する。

（3）専用の物理破壊機による目の前での物理的な破壊はもっとも脆弱性が少ない最善な方法である。

日東造機 CrusHBOx プロフェッショナルデータ消去複合機　DB-HYBRID（ディスクブレーカー　ハイブリッド）DDB-60HB－WH は 1 台で磁気消去と物理破壊が可能で防衛省等の官公庁・自治体様に採用いだいています。
また、手動機の HDB-20V は V 字に折り曲げる米国（NSA）指針に準拠、DB-50PRO は 4

箇所の孔を開けながらV・M字に折り曲げるDoD（米軍）方式の破壊が可能です。

国家機関　データ消去の脆弱性について

日本の情報セキュリティ対策の啓蒙活動や指針作りは経済産業省が監督する「IT セキュリティ評価及び認証制度」（制度）の評価機関が牽引しております。

評価機関によるセキュリティ評価結果はIPA 内の認証機関によって認証されます。本制度はISO/IEC15408(CC:Common >> CritEria)に基づいて運用されています。

この仕組みは現在世界26カ国が加盟するCCRA(CC承認アレンジメント)により認証書の流通を図っています。

CC は保護すべき資産に対する脅威（アタック）を明確にしてセキュリティ対策を検 証するための基準で、どの程度のセキュリティ対策が必要であるかは対象となる製品の目的、動作環境等によって変わります。

例えば複写機にも一般的にHDDが搭載されておりそのHDDの盗難により機密情報が漏れる可能性があるためCCによって認証された複写機にはHDDの暗号機能及び消去機能が搭載されています。

このようなHDDは問題がありませんが一般のPCに搭載されているHDDやSSDにはこのような対策が行われていません。特にSSDはいろいろいな部分に生データが記録されているため一般の上書き消去では完全なセキュリティの維持は厄介です。

よってHDD/SSDを廃棄するタイミングであれば物理破壊は非常に有効な手段となります。

完全なセキュリティはこの世に存在しないため、どこまでリスクを軽減できるかはデータ消去3つの手法も最終的には使用者が許容できるか否かです。

パソコンユーザーが、使用済みパソコンを廃棄する際に、ハードディスク上の重要なデータが流出するというトラブルを回避するためには、ハードディスクに記録された全データを、ユーザーの責任において消去することが非常に重要です。消去するためには、専用ソフトウェアあるいはサービスを利用するか、ハードディスク上のデータを物理的・磁気的に破壊して、読めなくすることを推奨します。

次回、第三章　日東造機の新たな挑戦です。

唐鎌益男

日東造機株式会社　IT事業部長

三央工業株式会社　顧問(日東造機グループ)　データ・セキュリティ・コンソーシアム　事務局長

日東造機株式会社の創業は昭和20年、創立は昭和25年（1950年)。

HDD 物理破壊機シェア NO.1　2004 年　第 1 回　情報セキュリティ EXPO から 2015 年まで連続 12 年、電子記録メディア破壊機 CrushBox シリーズ を出展しています。

所属：日東造機株式会社