2016 年 4 月 8 日

日本のＰＣリユースにおけるデータ消去について

株式会社アセットアソシエイツ
代表取締役　伊藤修司

＜１＞ＰＣリユースのデータ消去

現在、国内に流通しているリユースＰＣ（ＨＤＤ、ＳＳＤを含む）は、さまざまな仕様、方法によりデータ消去が実施されている。主な消去方法は、ソフトウェアによる上書き消去、物理的に破壊する方法、強磁気によるデータの消去／破壊の３つがある。

その中でもソフトウェアによる上書き消去については注意が必要である。

無料の消去ソフト、市販の消去ソフト、業者向け消去ソフトなど様々なソフトウェアが流通しているが、完全にデータが消去できるか検証されていない可能性がある。

これら未検証の消去ソフトで処理されたリユースＰＣ（ＨＤＤ、ＳＳＤを含む）も、データ消去済みの無データ状態として取り扱われているが、これらの記憶媒体は消去が不完全でデータが残存している可能性がある。

物理的に破壊する方法は、ドリルや専用の破壊機を用いて実施する。

ＨＤＤは、プラッタを変形させれば現在の技術ではデータを読み出すことは、ほぼ不可能といってよい。ＳＳＤは、チップを破壊して使用不能にする。

強磁気によるデータ消去は、ＨＤＤなどの磁性体の記憶媒体に対して有効な方法であり、ＳＳＤなどの半導体を使用した記憶媒体のデータを消去／破壊することはできない。

ＨＤＤの場合、強力な磁気によりデータを完全に消去／破壊するので、データの読み出しや復元も不可能となり、ハードウェアとして認識もしない状態になり使用不能になる。

リユースＰＣ（ＨＤＤ、ＳＳＤを含む）を証拠保全先の記憶媒体として使用する場合、まず無データ状態であることを確認する必要があるが、現在それを確認するためのガイドラインやデータ消去基準はない。

リユースＰＣからの情報漏洩の防止及び証拠保全先の適正な記憶媒体として確保するため、無データ状態であることを確認できる国内共通のデータ消去基準及びデータ消去ガイドラインの策定が必要である。

＜２＞国内のデータ消去ガイドライン

現在、国内のガイドラインは一般社団法人情報機器リユース・リサイクル協会（ＲＩＴＥＡ）の「情報機器の売却・譲渡時におけるハードディスクのデータ消去に関するガイドライン（http://www.ritea.or.jp/eh_guide.html）」及び、一般社団法人電子情報技術産業協会（ＪＥＩＴＡ）の「パソコンの廃棄・譲渡時におけるＨＤＤ上のデータ消去に関する留意事項（http://home.jeita.or.jp/page_file/20110511155520_8vAEy2Fi5d.pdf）」などがある。

ＲＩＴＥＡのデータ消去に対する見解は、次の通りである。

情報機器の HDD 内に記録されたデータを消去する方法としては、専用装置で電気的・磁気的に塗りつぶしを行う方法や HDD を物理的に破壊する方法もありますが、情報機器の長寿命化や循環型社会実現に貢献する「リユース」の見地からは、「専用消去ソフトウェアによる HDD データ消去方法」が望ましいと考えます。但し、今日では、OS 等の再セットアップ(リカバリ)データを HDD 内の特別な領域に保存している情報機器も増加しており、HDD 全領域をデータ消去するという定義は、必ずしも適切ではなくなっていることへの配慮が必要と考えます。また、HDD のデータ領域に対して、特定しない英数字によるパターン等で 1 回以上の書き込みを行い、元々あったデータの塗り潰し消去を行えば、現状ではデータの復旧は困難と考えます。

専用 HDD データ消去ソフトウェアとしては、以下の特徴を満たすべきと考えます。

HDD のデータ領域に特定しない英数字によるパターン等で 1 回以上書き込みを行い(OS の再セットアップ(リカバリ)領域等を除く)、元々あったデータの塗り潰し消去を行うこと。

作業終了後に作業が正常に終了したか、エラーが発生したかのログ情報を記録に残すことができること。 HDD にインストールされた OS に依存せず、OS やファイルが壊れて起動できなくなった場合でも、HDD データ消去ができること。但し、今回の対象機器分野は、パソコン・ワークステーション・サーバ(全て「x86」系アーキテクチャー)としています。

使用済スマートフォンのユーザーデータの消去を行うには、使用者による「オールリセット」操作を行った後に、対応事業者による「スマートフォンデータ消去ソフトウェアを用いたメモリ部のユーザーデータ消去の実施」が望ましいと考えます。なお、上記に示すように、スマートフォンの「リサイクル」の場合は、使用済スマートフォンを鍵付きの頑丈な壊れない箱等に入れ、厳重な注意をしながら、情報機器リサイクル事業者へ送り、そこで解体・破壊・選別等を行うか、そのまま製錬所まで輸送することも考えられますが、この場合は、関係事業者による強力な協力体制構築等、運用上の徹底が必要となります。

スマートフォンのユーザーデータ領域に対して、特定しない英数字または意味のない数字のパターン等で 1 回以上の書き込みを行い、元々あったデータの塗り潰し消去を行えば、現状ではデータの復旧は困難と考えます。

スマートフォンデータ消去ソフトウェアとしては、以下の特徴を満たすべきと考えます。

１．スマートフォンのユーザーデータが入っているメモリ部に特定しない英数字または意味のない数字のパターン等で 1 回以上書き込みを行い、元々あったデータの塗り潰し消去を行うこと。

２．スマートフォンでは、パソコンのハードディスクドライブの場合と異なり、現状では、一般に、その装置自身でデータ消去ソフトウェアを動作させて、ユーザーデータが入っているメモリ部に消去データを直接書き込みする（上書きする）ことができないことから、パソコンで動作する「スマートフォンデータ消去ソフトウェア」を使用して、スマートフォンのデータフォーマットに合わせた形で、上記 1.のパターンの消去データを作成する。

消去データの作成とデータの消去方法としては、

ａ．パソコンで消去データを作成し、その消去データをパソコンとＵＳＢまたはネットワークで接続したスマートフォンへパソコンから転送し、データ消去を行う。

ｂ.パソコンとスマートフォンを一度ネットワークで接続して、パソコンからスマートフォンに対して、スマートフォン内で消去データの生成を指示するソフトウェアをパソコンから送り込み、その後、スマートフォン内で、上記 1.のパターンの消去データの生成を行い（この状態ではネットワークをはずしてよい）、データ消去を行う。 等が考えられる。

３．データ消去作業終了後に作業が正常に終了したか、エラーが発生したかの情報をスマートフォンに接続したパソコンに表示、またはスマートフォンに接続したパソコンのログファイルに記録を残すことができること。

４．データ消去作業終了後に、a.消去日付・時刻、b.スマートフォンの型名、c.スマートフォン毎に付加される通信端末識別番号、d.スマートフォンのメモリ容量、e.データ消去方式の各情報が収集でき、データ消去作業終了（完了）書作成等の為のデータが得られること。

ＪＥＩＴＡのガイドラインは、データ消去する有効な方法として次の方法を紹介している。

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専用装置にて電気的、磁気的に塗りつぶす方法

（場合によっては物理的な破壊を伴う場合もある）

③HDDに対して物理的に破壊する方法

データを消去する際に選択すべき方法としては、該当するパソコン及びハードディスクの状況に依存しますが、その一例を示すと下記のようになります。

パソコンのHDDの状況	データ消去方法例
(1)パソコンとHDDが稼働する場合	・専用ソフトにてデータ消去 ・専用装置にてデータ消去 ・HDDを物理的に破壊
(2)パソコン本体は稼働しないが、HDDは稼働する場合	・他の稼働可能なパソコンにHDDを接続して専用ソフトにてデータ消去 ・専用装置にてデータ消去 ・HDDを物理的に破壊
(3)HDDが稼働しない場合	・HDDを物理的に破壊

基本的にHDDデータ消去プログラムで1回固定データによる塗潰し消去を行えば十分で、2回消去を行えば一般的に完全といえるが、消去ソフトによるデータ消去に100%の責任を持つことは不可能であるともしている。

＜３＞データ消去方法

データ消去の方法は、「パソコンメーカー、ディスクメーカーが提供している記録媒体の消去方法を利用する」、「市販のデータ消去ソフトを利用する」、「物理破壊する」のが一般的である。

情報機器リユース・リサイクル協会（ＲＩＴＥＡ）は、データ消去ソフトに「資格（http://www.ritea.or.jp/eh_shikaku.html）」を設け、ＲＩＴＥＡ認定事業者には資格が付与された消去ソフトを使用することを義務付けている。

リユースＰＣの専門業者は、「データ消去ソフト」「物理破壊」「電磁波消去」などの方法を用いてデータ消去しているが、完全にデータが消去できているか確認する場合は少なく、ほとんどの記憶媒体が未確認のまま流通している。

そのため、企業は残存データがあっても情報漏洩を防止できる「物理破壊」に傾向しているが、「物理破壊」、「電磁波消去」はリユースできない欠点があり、さらに「物理破壊」はリサイクル処理における解体作業を困難にする欠点もある。

したがって、目的別に「リユースは消去ソフト」、「リサイクルは電磁波消去」、「データ漏洩防止は物理破壊」が推奨する消去方法となる。

＜４＞廃棄ＰＣのデータ消去

廃棄ＰＣは、リユース市場に流通しないのでデータが未消去でも安全だと誤解されることがあるが、実際は産業廃棄物処理会社で中間処理された後、排出時とほとんど同じ状態で有価売却され、リユース市場に流通する可能性がある。

これは中間処理が破砕することと誤解されているのが主な原因と考えられるが、中間処理

にはさまざまな方法があり、パソコンなどの電子機器であれば解体処理も適正な中間処理にあたる。例えば、パソコンを部品の状態まで解体処理し、各部品を有価売却しても制度的に問題はない。当然、その各部品にはＨＤＤなどの記憶媒体も含まれており、データ消去していなければデータが残存したＨＤＤなどがリユース市場に流通することになる。
したがって、廃棄ＰＣからの情報漏洩を防止するには、産業廃棄物処理会社に引き渡す前にデータ消去を実施するか、廃棄物の処分契約書にデータ消去に関する条項をいれて、情報漏えいのリスクを回避する必要がある。

＜５＞データ消去とは
記憶媒体の記憶領域に保存されたデータは、ＯＳやソフトウェア上での操作による削除ではシステム内にデータが残存する可能性がある。この残存したデータは様々な手法により復元される可能性がある為、「データ消去」とは復元不可能な状態にデータを破壊する事である。
データを破壊する為に、無意味なデータを複数回上書きして消去（破壊）する方法は、フロッピーディスクやデータ密度の低い旧式の磁気メディアが対象で、高密度なハードディスク等は１回の上書き消去で残留磁気によるデータの復元は事実上不可能である。
日本には数多くのデータ消去アルゴリズムがあるが、「０クリア方式」「ＮＳＡ方式」「ＤｏＤ５２２０．２２－M方式」が広く採用されている。
※データ消去アルゴリズム
０クリア方式・・・０データを１回上書き方式
ＮＳＡ方式・・・乱数２回、ゼロデータ１回の３回上書き方式
ＤｏＤ５２２０．２２－M方式・・・ゼロ、固定値、乱数の３回上書き方式

パソコンメーカー、ディスクメーカーが準備している消去方法で Secure Erase がある。
Secure Erase は、ATA で定義されている消去コマンドである。
Security Erase Unit はクリップ領域を含めたユーザーエリアにゼロを書き込み消去、Enhanced Security Erase Unit はユーザーデータ及び代替セクターにデータを書き込み消去する。しかし、Security Erase Unit コマンドがサポートされていないドライブもあるため、サポートしているコマンドの種類等により対応状況が異なる。
Security Erase は ATA 規格上で定義されているが、実際の動作はドライブ内のファームウェアが行うためソフトウェア的なデータ消去の検証ができず、正しく消去処理ができたのか、部分的に消去できない場所があったのか判断できない。
また、「消去せよ・終了後に成功か失敗か出力せよ」としか定義されておらず、処理はドライブのファームウェアに任されているため、消せない領域があったのかなど、データ領域の状態を一切知ることができない欠点があり、Secure Erase を実行しても、期待通りの動作結果が得られず、データが消去されていない状態も確認されている。

＜６＞まとめ

ＨＤＤは、全ＬＢＡ領域、代替処理のための領域に対して上書き消去を実施すればリユースでは問題ないレベルのデータ消去といえるが、証拠保全先としての使用は、不良セクタの残存データ、その他にも領域が存在する可能性があり、完全な無データ状態にすることが困難なため適さない。また、Ｇ－Ｌｉｓｔ（出荷後に生じた不良セクタに関する情報とその再配置情報）の情報から不良セクタの残存データに起因するリスクに対して考慮しておく必要がある。例えば、不良セクタを次の３つに区分したとすると、「１」の不良セクタは情報漏洩のリスクが残存する。

１．書き込み不可、読み出し可の不良セクタ

２．書き込み可、読み出し不可の不良セクタ

３．書き込み不可、読み出し不可の不良セクタ

ＳＳＤは、ウェアレベリング機能により特定のアドレスに書き込み出来ないため、上書き消去の概念がない。統計的な手法ではあるが、全ＬＢＡ領域、代替処理のための領域に対して２～３回の書き込みを実施すれば、ほぼ復元不可能な状態になるが、意図的に無データ状態にすることはＨＤＤよりも困難なため、証拠保全先としては不適格である。

しかし、Trim 機能により１日程度の時間経過により削除データを復元することが不可能であることも確認されている。したがって、全ＬＢＡ領域、代替処理のための領域に対して２～３回の書き込みを実施して、１日程度の時間を経過させて Trim 機能の効果を利用する手順により、リユースでは問題ないレベルのデータ消去といえる。

ＨＤＤ、ＳＳＤを証拠保全先とする場合、データ消去を実施して無データ状態にすることが困難であるため、工場出荷時の状態が保証されている新規媒体を購入する必要があるが、バルク品などは新品扱いでも開封した形跡がある物が販売されていることもあるため、リテール品を購入するなど注意が必要である。

リユースの場合、データ消去を実施すれば問題ないレベルと言えるが、Secure Erase は実行しても期待通りの動作結果が得られずデータが消去されていないこともあるため検証済みの消去ソフトを使用することが必要である。

ＰＣリユースは、情報漏洩防止の観点から取り扱いデータの機密性により分類し、その分類別に必要な消去ソフトの仕様、消去レベル、作業手順、管理方法などを定めた共通のガイドラインが必要である。