デジタル・フォレンジックの有効性
－セキュリティマネジメントからみたＰＣデータ抹消について－

伊藤忠テクノソリューションズ株式会社
山口　大輔

組織の情報セキュリティ維持・向上には、基準となるガイドラインに従い、セキュリティ管理のためのルールを作ることが欠かせない。現在、これらセキュリティマネジメントのためのガイドラインには、国際規格、国内での規格、私的ガイドラインなど様々なものがあり、それぞれに特徴を持つ。

しかしながら廃棄するＰＣに対して詳細かつ実効的な手順を定めたものは皆無であり、組織としてさらに有効的な手法を適用するに任せられている。

これは、ＩＴ犯罪が発生した場合における証拠保全＝データフォレンジックという点からは好ましいことではあるが、ＰＣを廃棄する側からみると、大きなリスクとなっている。

本稿はＰＣ廃棄時のデータ抹消について、各種ガイドラインからの要求と、実際に適用される高等教育機関の状況について取り纏めている。

１．各種ガイドラインから要求されるＰＣデータ抹消

組織の情報セキュリティ維持・向上には、基準となるガイドラインに従い、セキュリティ管理のためのルールを作ることが欠かせない。現在、これらセキュリティマネジメントのためのガイドラインには、国際規格、国内での規格、私的ガイドラインなど様々なものがあり、それぞれに特徴を持つ。

しかしながら廃棄するＰＣに対して詳細かつ実効的な手順を定めたものは皆無であり、組織としてさらに有効的な手法を適用するに任せられている。

これは、ＩＴ犯罪が発生した場合における証拠保全＝データフォレンジックという点からは好ましいことではあるが、ＰＣを廃棄する側からみると、大きなリスクとなっている。

特に近年、個人ユーザにおけるＰＣ操作対象は、オンラインバンキング、ネット販売、保険の申し込み､官庁への申請､健康管理など多義にわたり､それぞれが機微な情報を入力、利用する場面が多くなっている。それらの情報は、アプリケーションレベルでローカルディスクに残さない配慮が為されているものもあるが、いまだにそういったことには無頓着なものも見受けられる。

従って、例えばＰＣ廃棄におけるデータ抹消には、簡潔かつ完全な手法やガイドラインが求められるはずであるが､上記の理由からそれらに完全に触れるガイドラインは存在しない。

本編では、ＰＣ廃棄のリスクについて、セキュリティマネジメントから見た検証を行っている。

１．１ ＩＳＯ２７００１

現在、国内で最も普及するセキュリティ管理のためのガイドラインである。国際標準化機構により制定され、最新版は２０１３年に発効している。

関連ガイドラインはＩＳＯ２７００１及びＩＳＯ２７００２で構成され、２７００１はセキュリティマネジメント導入のための要求事項、２７００２はそれらを導入した場合の解説・例示となっている。

「記憶媒体を内蔵した装置」とは、ＰＣなどのＩＴ機器を指す。もちろん、大型サーバーやタブレット端末なども対象範囲となる。これらには、「セキュリティを保って上書きしていること」との要求となり、各組織では、これを自組織の実情に従い、具体的手順を考案する。

一般的には、極めて機微な情報を扱った装置では、究極は物理的破壊となるだろうし、単純情報を扱った組織（例えば配布用販売資料を作った、セミナー資料を作ったなど）では、そこまでの「上書き」は必要ないだろう。

しかしここには具体的基準は無い。何が「機微」な情報で、どんなものが「公開しても大丈夫」であるかは、組織が決定しなければならない。

今回、データ消去分科会では、さまざまな抹消の手法や、そこにまつわるリスクの研究を行ってきた。しかしながら現時点でこれらの情報は一般的ではなく、有効的な「上書き」が為されている保証はない。

右は実施の手引きである。

前述のとおり、ISO27002 は具体的手順を説明したものである。この中では物理的破壊を推奨しており、再利用は想定していない。現在のＩＴ資産運用では、その寿命まで使いきることは珍しく、一般的にはリユース機器などで再利用される。こういった場合への具体的ガイドはない。

ISO27001 規格 A.11.2.7
「装置のセキュリティを保った処分又は再利用」
管理策
記憶媒体を内蔵した全ての装置は、処分又は再利用する前に、全ての取扱いに慎重を要するデータ及びライセンス供与されたソフトウェアを消去していること、又はセキュリティを保って上書きしていることを確実にするために、検証しなければならない。
出所：ISO27001(ISO)[1]

ISO27002 規格 11.2.7
実施の手引
装置は、処分又は再利用する前に、記憶媒体が内蔵されているか否かを確かめるために検証することが望ましい。
秘密情報又は著作権のある情報を格納した記憶媒体は、物理的に破壊することが望ましく、又はその情報を破壊、消去若しくは上書きすることが望ましい。消去又は上書きには、標準的な消去又は初期化の機能を利用するよりも、元の情報を媒体から取り出せなくする技術を利用することが望ましい。
出所：ISO27002(ISO)[2]

１．２　ＰＣＩＤＳＳ

クレジットカード操作をビジネスとする組織に対する特定ガイドラインである。

近年、クレジットカードデータは、大量の漏えいが発生している。多くのＷｅｂサイトはカード番号のみで買い物が可能であり、ＩＴシステムの脆弱性をついた外部攻撃が多発しているためである。さらに攻撃側の技術も格段に進歩しており、カードデータを扱う組織では、細心の注意が必要となっている。

こういった事情のなか、ＰＣＩＤＳＳは海外クレジットカードブランド５社が規定する PCI Security Standards Council が開発するフォーラム規格であり、ＩＴシステム全般から、セキュリティレベルを上昇させるためのガイドラインとなっている。

要求される内容は右記の通り。

ＩＳＯ２７００１に比べて、指定プログラムでの抹消が要求されており、さらに強固な手順となっている。カード犯罪があった場合、データフォレンジックの観点からは、より証拠確保が困難になっている。

> 9.8.2 電子媒体上のカード会員データが、安全な削除に関して業界が承認した標準に従った安全なワイププログラムによって、またはそれ以外の場合は媒体の物理的な破壊によって、回復不能になっていることを確認する。
> 出所：PCIDSS(PCI Data security council)[3]

１．３ マイナンバー

マイナンバーの管理は本年から開始されるものである。

これらは、特定個人情報保護委員会発行の「特定個人情報の適正な取扱いに関するガイドライン」で規定される。

もとより、個人情報の管理、マイナンバーの管理においては、ＩＴシステムの問題ではなく、事業者の収集、情報廃棄などが規定されるもので、主に紙ベースの情報に適用されるものである。

しかしながら現在、組織として従業者から預かったマイナンバーデータについて、紙ベースで管理する企業は少数派であり、ほとんどがＩＴシステムで管理される。従って、ＰＣなどに記録された場合には、廃棄の問題が浮上し、組織内で個別ＰＣのハードディスクに記録されるとすると、むしろ根が深い。

このあたりは推進した総務省も認識しており、同ガイドラインには別添として、「特定個人情報に関する安全管理措置」が付属する。別添には、2-E-d 項に、「個人番号の削除、機器及び電子媒体等の廃棄」という要求項目があり、データ抹消について触れている。

> 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する。
> 出所：「特定個人情報の適正な取扱いに関するガイドライン」(特定個人情報保護委員会)[4]

同ガイドラインでは、使用済ＰＣなどを廃棄する場合、専用のデータ削除ソフトによる抹消を求めている。ガイドラインが一般事業者を想定しているとすれば、「専用のデータ削除ソフトウェア」は一般的に販売されるデータ抹消
ソフトを想定していると思われるが、これについても、これまでの「データ消去」分科会で検討を重ねてきたように、一般的なものが完全に抹消するものではないことは周知の通りである。

これらについては、今後問題視されてくるものと思われる。

１．４ クラウド環境におけるデータ抹消

１．４．１ Cloud Security Alliance によるガイドライン

近年、クラウドコンピューティングという名称で、遠隔地にあるコンピュータ施設をネットワーク利用する手法が進んでいる。もともとは営業管理などのアプリケーションを共同利用する程度であったが、ここ数年、データセンタをベースにした整備がすすみ、その概念は劇的に進化しつつある。

> Cloud Security Alliance (CSA)
> FS-07 Site equipment
> Policies and procedures shall be established for securing and asset management for the use and secure disposal of equipment maintained and used outside the organization's premise.
> 組織の構外で保管され、使用される装置については、使用や確実な処分に関する資産管理の方針や手続きが確立されなければならない。出所 : Cloud Security Alliance[9]

クラウド環境では、組織が専用に利用するプライベートクラウド、一般多数が利用するパブリッククラウドがあるが、パブリッククラウドでは、入力したデータがどこにあるのか、基本的にはわからない。データ抹消についても、抹消するオペレーションは用意されているものの、保持されるデータが完全に抹消される保証はない。

また、クラウドといっても、ベースはどこかにハードウエアがある。ハードウエアがあれば寿命もあり、それらの廃棄も発生し、処理方法は現在確立している手法で行われる（はずである）

現在、クラウド環境にすべてを移管する状況にあり、例えば個人情報などもクラウド管理されることが考えられる。移管するデータ量も莫大になり、リスクも巨大であるはずであるが、クラウドそのものが新しい概念であるため、それを規制／規程するガイドラインは少ない。

現在数種類のものがあるが、データ抹消に関しては、「信頼性あるデータ抹消を行うこと」程度の記述が多く、各事業者に任せられている状況である。

１．４．２ Amazon Web Service によるガイドライン

代表的パブリッククラウドとして、米国 Amazon 社の提供する Amazon Web Services があり、公開されるホワイトペーパーでは、ストレージのデータ抹消について、その実施方法を公開している。このドキュメントは一般的に適用されるガイドラインということではなく、あくまで Amazon 社の提供するパブリッククラウドに対して、その詳細を説明しているものであるが、公開文書であるため、データ抹消は記載の通りに行われているものと考えられる。

抹消手法は具体的に DoD5220、NIST800-88 に規定されるものを引用しており、さらに物理的破壊までを規定する。国内複数社もクラウド基盤を提供しているが、ここまで具体的な文書を公開（つまり利用者にとっては契約文書に近い）している例はなく、国内各社と米国社で、セキュリティ意識の違いが読み取れる。

Amazon Web Services
ストレージデバイスの廃棄
AWS の処理手順には、ストレージデバイスが製品寿命に達した場合に、顧客データが権限のない人々に流出しないようにする廃棄プロセスが含まれています。AWS は、DoD 5220.22-M（「National Industrial Security Program OperatingManual（国立産業セキュリティプログラム作業マニュアル）」）または NIST 800-88（「Guidelines for Media Sanitization（メディア衛生のためのガイドライン）」）に詳細が記載されている技術を用いて、廃棄プロセスの一環としてデータを破棄します。廃棄された磁気ストレージデバイスはすべて業界標準の方法に従って消磁され、物理的に破壊されます。出所：Amazon Web Services: Overview of Security Processes[6]

１．５ 教育機関におけるデータ抹消

高等教育機関におけるＩＴセキュリティでは、国立情報学研究所（ＮＩＩ）の発行する「高等教育機関の情報セキュリティ対策のためのサンプル規程集」が標準ガイドラインとなっている。

大学をはじめ、学生を抱える教育機関では多くの個人情報を抱える。

これら個人情報は成績などの学業情報もあるが、近年では両親や友人関係、疾病情報など、多岐に及ぶ。これにはメンタル関連の聞き取り記録などもあり、管理上、高レベルの機微情報と言える。従って、情報セキュリティ管理は厳密に行わなければならず、組織

第四十八条 教職員等は、電磁的記録媒体に保存された情報が職務上不要となった場合は、速やかに情報を消去すること。
２ 教職員等は、電磁的記録媒体を廃棄する場合には、当該記録媒体内に情報が残留した状態とならないよう、全ての情報を復元できないように抹消すること。
３ 教職員等は、要機密情報である書面を廃棄する場合には、復元が困難な状態にすること。
出所：「C2101 情報機器ガイドライン」（国立情報学研究所）[7]

外への情報漏えいは完全に遮断される必要がある。

ガイドラインには、物理的破壊、抹消ツールの活用など、具体的規程がなされている。しかしながら抹消ツールの選定は組織に任されており、一般的には選定良否による抹消有効性は異なる。

またこれらを参照する学校組織はさまざまな組織文化の集合体であること、また研究業務は独立性を必要とすることなどから、上部組織からの統制が取りにくい。

学校組織では、組織への実効性ある展開が課題となる。

１．６ 関係団体におけるデータ抹消

情報機器のリユース、リサイクル事業者が参加する専門団体「一般社団法人　情報機器リユース・リサイクル協会（ＲＩＴＥＡ）」でも関連ガイドラインを定めている。

同社団に参加する事業者は、一次使用したＰＣに対してデータ抹消を行っており、そういった意味では抹消プロセスの専門家ということができる。

ガイドラインでは、Windows コマンドによるデータ抹消、初期化、抹消困難な領域の存在などに触れると同時に、専用ソフトウエアの利用を推奨している。

ガイドライン上、抹消は利用者の責任とするのではなく、具体的脅威に触れている点など、具体的な指針と言えるだろう。

> 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。
> 出所：「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」(一般社団法人　情報機器リユース・リサイクル協会)[8]

１．７ ＩＰＡにおけるデータ消去ガイドライン

独立行政法人　情報処理推進機構では、さまざまなガイドラインを発行している。そのうち「企業組織における最低限の情報セキュリティ対策のしおり」では、情報セキュリティ対策を紹介すると共に、ＰＣ廃棄の際の手順なども公開している。

本ガイドラインは、利用者に質疑応答形式で手順実施を促しており、消去ソフトの利用、または専門業者への抹消依頼を促している。

特記すべきは、不揮発性メモリ（フラッシュメモリ）抹消への注意喚起であろう。「データ消去分科会」でも検討されたように、フラッシュメモリについては、その特性上、抹消不可能領域が残り得る。ガイドラインでは具体的処理については言及していないが、それらの注意については問題提起を行っている。

> 重要情報の入ったパソコン・記憶媒体を廃棄する場合は、消去ソフトを利用したり、業者に消去を依頼するなどのように、電子データが読めなくなるような処理をしていますか？
> 出所：「企業組織における最低限の情報セキュリティ対策のしおり」（ＩＰＡ)[9]

１．８ 各ガイドラインにおけるデータ抹消の確認・検証

各ガイドラインとも、データ抹消についての要求はあるものの、実施結果の検証まで踏み込んでいるものは少ない。

例示として、PCIDSS(PCI Data security council)[3] では、基準 9.8.2 において、次のように要求している。「電子媒体上のカード会員データが、安全な削除に関して業界が承認した標準に従った安全なワイププログラムによって、またはそれ以外の場合は媒体の物理的な破壊によって、回復不能になっていることを確認する」となっており、物理破壊を選択した場合には回復不能を確認することを要求しているものの、抹消ソフトを用いた場合には、確認までを要求しているわけではない。別例として ISO27002(ISO)[2] では、8.3.2 媒体の処分で「多くの業者が、媒体の収集及び処分のサービスを提供している。十分な管理策及び経験をもつ適切な外部関係者を選定することに、注意を払う。」との要求があるが、信頼ある外部委託先を選定することを求めているものの、実施確認までを求めているわけではない。

２．高等教育機関におけるＰＣデータ抹消公開の状況

監督官庁は「高等教育機関の情報セキュリティ対策のためのサンプル規程集（国立情報学研究所)」を参照する（前項１.５に記述）ことを推奨するが、大学、研究機関など、高等教育機関の対応は様々である。以下にその実例を示す。

２．１ 北海道大学

対応する規程は「国立大学法人北海道大学情報セキュリティ対策規程」(平成２７年７月１日)[10]と思われるが、情報機器廃棄に関する規程は公開していないようである。

出所：北海道大学Ｗｅｂ
http://www.hokudai.ac.jp

２．２ 横浜国立大学

■端末を廃棄又は譲渡する場合は、ハードディスクやメモリに、重要な管理情報やその他重要な情報が残留することのないように、完全に抹消するか、物理的に破壊すること。(出所：「ＰＣ取扱いガイドライン」平成２２年３月２６日）[11]

これらについて、具体的手順は確認することができないようである。

出所：横浜国立大学Ｗｅｂ
http://www.ynu.ac.jp

２．３ 京都大学

■教職員等は、電磁的記録媒体を破棄する場合には、当該記録媒体内に情報が残留した状態とならないよう、全ての情報を復元できないように抹消するものとする。(出所：「京都大学情報セキュリティ対策基準」平成２１年３月２日）[12]

これらの手順も有効であるものの、「全ての情報を復元できないように抹消する」具体的手順までは公開されていない。

２．４ その他の大学機関

その他、国立大学、私立大学共に、一部の大学では情報セキュリティに関するポリシーを公開している。今回、ＰＣデータ抹消について、外部公開されているＷｅｂサイトから確認した結果は以下の通りである。

大学	データ消去に関する公開規程
青山学院大学	情報セキュリティに関する上位ポリシーは公開されているが、詳細規定まで確認できず
関西学院大学	利用者に関する情報セキュリティポリシーは公開されているが、管理に関する公開ガイドラインは確認できず
慶應義塾大学	公式サイトからはリンクできなかったが、ＩＴセンターサイトにデータ消去専用機器の具体的利用が推奨されている
法政大学	学校法人法政大学情報セキュリティポリシー（2014年４月１日制定施行） 第１９条　情報機器及び記録媒体を破棄する場合は，残存情報が第三者に読み取られることのないよう，情報セキュリティ対策を講じなければならない。
明治大学	情報セキュリティに関する上位ポリシーは公開されているが、詳細規定までは確認困難のようである

参考文献（全て 2016 年 4 月 1 日時点）

[1] JIS Q27001:2014(ISO27001:2013)
日本規格協会/International Organization for Standardization

[2] JIS Q27002:2014(ISO27002:2013)
日本規格協会/International Organization for Standardization

[3] Payment Card Industry Data Security Standard Version 3.0

[4] 特定個人情報の適正な取扱いに関するガイドライン（事業者編）,特定個人情報保護委員会(2014).

[5] Cloud Control Matrix1.4J, Cloud Security Alliance (2012)

[6] Introduction to AWS Security, amazon web service, pp.8 (2014)

[7] 高等教育機関の情報セキュリティ対策のためのサンプル規程集,　国立情報学研究所(2013)

[8] 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,一般社団法人　情報機器リユース・リサイクル協会(2012)

[9] 企業組織における最低限の情報セキュリティ対策のしおり, 独立行政法人情報処理推進機構(2015)
[10] 国立大学法人北海道大学情報セキュリティ規定, 国立大学法人北海道大学(2012)
http://www.hokudai.ac.jp/jimuk/reiki/reiki_honbun/u010RG00000767.html
[11] ＰＣ取扱ガイドライン, 横浜国立大学(2010)
http://www.ynu.ac.jp/about/information/security/pdf/secu05-1.pdf
[12] 京都大学情報セキュリティ対策基準, 京都大学(2009)
http://www.kyoto-u.ac.jp/ja/about/foundation/jseibi/security/kijyun.html