廃棄/返却PCの情報セキュリティ
情報漏洩の現状と求められる対策

(株)IT企画　才所 敏明
toshiaki.saisho@advanced-it.co.jp

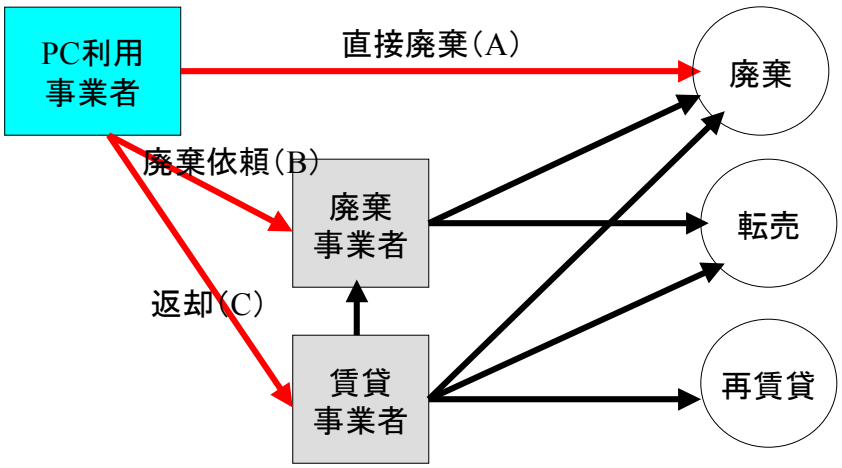
説明項目一覧

＊PC利用と情報セキュリティ課題
＊使用終了後のPCの行方
＊廃棄/返却PCからの情報漏洩事件
＊廃棄PC内のデータの安全性に関する誤解
＊廃棄/返却PCからの情報漏洩防止のために
＊ PC内データの復元不能化のアプローチ
＊データ消去に関する誤解
＊完全データ消去とは
＊データ消去方式例
＊データの復元不能化を明記するガイドライン例
＊廃棄/返却PCの情報漏洩対策

PC利用と情報セキュリティ課題

使用開始	使用中	使用終了
マスタ管理	ソフトウェア管理	データ消去
キッティング	マルウェア対策	
	アクセス管理	
	ログ管理	
	機器管理	
	データ管理	
	リカバリ対策	

使用終了後のPCの行方



廃棄/返却PCからの情報漏洩事件

A: 廃棄PCからの情報漏洩
- 三重県四日市市役所
- 福岡県中央警察署
- 大阪府岸和田市

B: 廃棄事業者経由の情報漏洩
- 千葉県鴨川市・南部林業事務所

C: 賃貸事業者経由の情報漏洩
- 静岡市・公立小中学校
- 岩手県・県生物工学研究所
- 消防庁・武蔵野消防署境出張所
- トヨタ系自動車販売会社・ネッツトヨタ水戸

廃棄/返却PC内の データの安全性に関する誤解

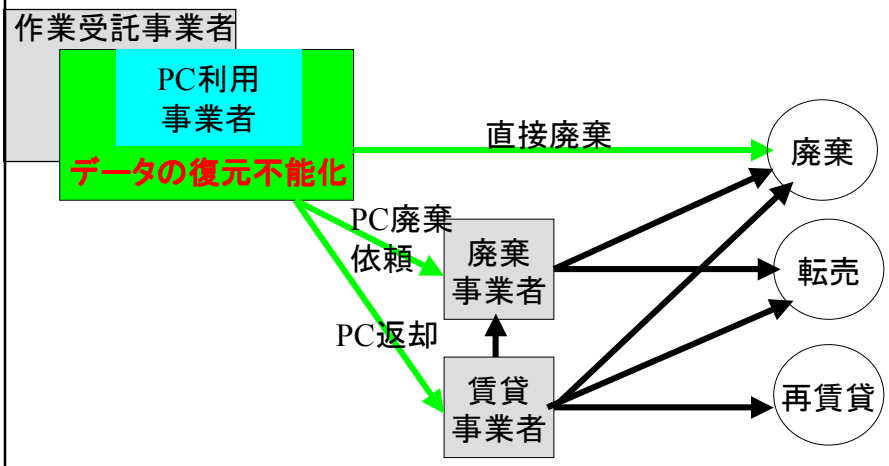
PC・ファイルは、パスワード付きだから安全
- パスワードは簡単に破られる可能性有り！

ファイル・ディスクは、暗号化されているから安全
- 原則はその通り
- だが、鍵情報がPC内に格納されていないか？

PCは、壊れて電源が入らないから安全
- 取り外したHDDを、他のPCで利用可能！

廃棄事業者/リース事業者に依頼すれば,プロだから大丈夫
- 本当にPC内のデータは完全に消去してくれるのか？

廃棄/返却PCからの情報漏洩防止のために



PC利用事業者は、自らの責任において、データの復元不能化を行う必要がある

PC内データの復元不能化のアプローチ

HDDを物理的に破壊
　HDDは再利用不可

HDD上のデータを磁気的に消去（消磁）
　原則、HDDは再利用不可

HDD上のデータを上書きにより消去
　HDDは再利用可能

HDDの物理的破壊

- PCの電源が入らない/HDが認識されない場合は、データ完全消去ソフトが使えず、また、消去中にシークエラーが頻発して消去作業が完了できなかったりする場合も、データはディスクに残ったままの状態になり、データ復旧サービスなど、専門的なサービスの利用により、一部または全部のデータの復元が可能で、危険。
- このような場合、HDDの物理的破壊が有効だが、破壊の程度によっては、一部のデータが読み取られる危険性が残る。

HDD上のデータの磁気的消去（消磁）

- データは、磁区と呼ばれる非常に小さな領域に対して磁気の配列を変えることで磁場の向きを変化させるという方法でハードディスク、フロッピーディスク、磁気テープなどの磁気メディアに記録される。
- 消磁は特に決まった方向を持たないランダムなパターンを磁区に残し、結果としてデータを修復できない状態にする
- いくつかの磁区は消磁をしたあとでも磁気の配列がランダム化されない場合があり、こういった磁区が持っている情報を残留磁気と呼ぶ。
- 適切な消磁を行うことで、データを再構築できないような小さい残留磁気しか残さなくすることが可能。

HDD上のデータを上書きにより消去

- HDDの再利用が可能な消去方法
- ただし、HDDへの完全なアクセスが不可能な場合は、データが残る危険性が残る
- その場合は、HDDの再利用は困難になるが、磁気的に消去（消磁）する方が安全

PC内データの消去に関する誤解

ファイル/ディレクトリの削除処理 ➔ ×
　単にごみ箱に移動させるだけ
　すぐに元に戻すことができる
ごみ箱からの削除（空にする） ➔ ×
　ファイル/ディレクトリの管理情報から削除されるだけ
　データの実体は残っている
　専用のツールにより、簡単に復元できる
HDDを再フォーマット ➔ ？
　物理フォーマット（ゼロファイル）の場合は ➔ ○
　論理フォーマットの場合は ➔ ×
　　ファイル/ディレクトリの管理情報を初期化するだけ
　　データの実体は初期化せず、残っている
　　専用のツールにより、簡単に復元できる
OSの再インストール/リカバリ ➔ ？

データ消去方式例

方式	書き込みデータ	合計書き込み回数
0x00書き込み	0x00	任意
0xFF書込み	0xFF	任意
ランダム書き込み	乱数	任意
米国国防総省方式（DoD5220.22-M）	任意の文字、 その文字の補数、 乱数	3回（＋検証）
米国国家安全保障局方式（NSA）	乱数で生成された文字、 別の乱数で生成された文字、 任意の数値	3回（＋検証）
米国陸軍方式（AR380-19）	乱数、 任意の文字、 その文字の補数	3回（＋検証）
Gutmann方式	乱数4回、 固定値27回、 乱数4回	35回

PC内データの
確実な復元不能化のために

HDDを物理的に破壊
　但し、事前に消磁しておく方が望ましい
　HDDは再利用不可

HDD上のデータを磁気的に消去（消磁）
　原則、HDDは再利用不可

HDD上のデータを上書きにより消去
　HDDは再利用可能

廃棄PC/返却PCのデータ消去が明記されているガイドライン例（１）

- 内閣官房情報セキュリティセンター（NISC)
  - 「政府機関の情報セキュリティ対策のための統一基準（第4版）（平成21年度修正）解説書」
  - 独立行政法人　Ａ　機構の情報セキュリティ対策のための管理基準/技術基準
- 経済産業省（METI)
  - 情報セキュリティ管理基準（平成２０年改正版）
  - (IPA)中小企業における組織的な情報セキュリティ対策ガイドライン　平成21年3月
- 厚生労働省
  - 医療情報システムの安全管理に関するガイドライン 第4.1版　平成22年2月
- 総務省
  - 地方公共団体における情報セキュリティポリシーに関するガイドライン(平成22年11 月版)

廃棄PC/返却PCのデータ消去が明記されているガイドライン例（２）

- 文部科学省
  - 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
- 国土交通省
  - 情報セキュリティガイドライン
- 経済産業省（METI)
  - 情報セキュリティ監査手続ガイドライン 平成21 年7 月
- 総務省
  - 監査ガイドライン情報セキュリティ対策別関連表（地方公共団体における 情報資産のリスク分析・評価 に関する手引きの別冊）

廃棄/返却PCの情報漏洩対策（まとめ）

＊情報および情報機器の管理者、管理組織が責任をもって情報の復元不能化を実施する必要がある。

＊データの復元不能化のためには以下の方法を採用する。

廃棄の場合

データを磁気的に消去（消磁）

データを上書きにより消去

返却（他への転用）の場合

データを上書きにより消去

＊PC/HDD等の廃棄/返却に関する規程、手順書にて、データの復元不能化の必要性、具体的手順を明記し、周知徹底しておく。

＊データの復元不能化を実施したエビデンスを、確実に残しておく（監査対応）。

終