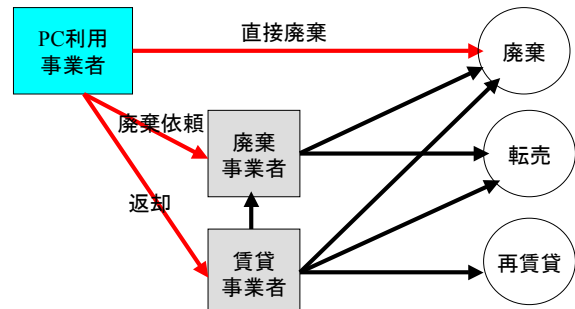


廃棄/返却PCの情報セキュリティ 情報漏洩の現状と求められる対策

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

使用終了後のPCの行方



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

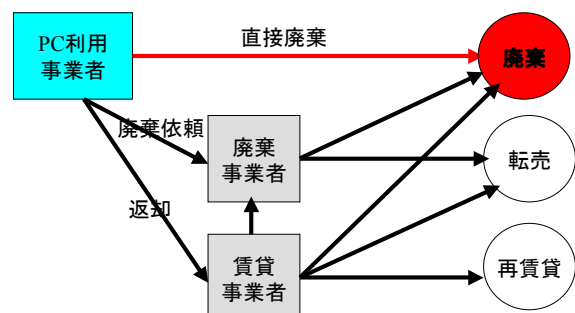
廃棄/返却PCからの情報漏洩事件

- 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
- 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・ネットヨタ水戸
- D: 業務委託先経由の情報漏洩
オリエントコーポレーション
カルビス

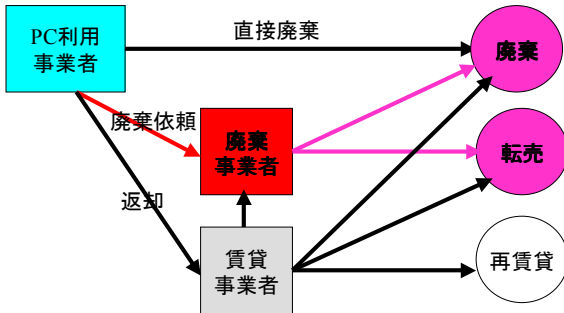
PC利用と情報セキュリティ課題

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	

A: 廃棄PCからの情報漏洩



B: 廃棄事業者経由の情報漏洩



廃棄/返却PC内のデータの安全性に関する誤解

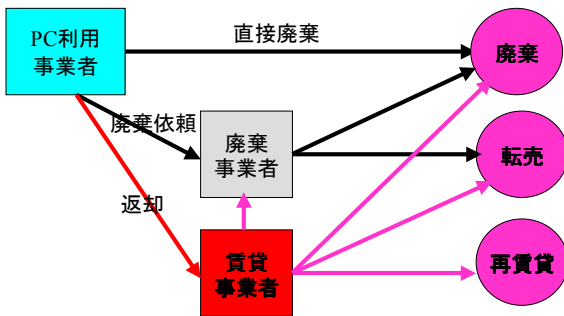
PC・ファイルは、パスワード付きだから安全
パスワードは簡単に破られる可能性有り

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？

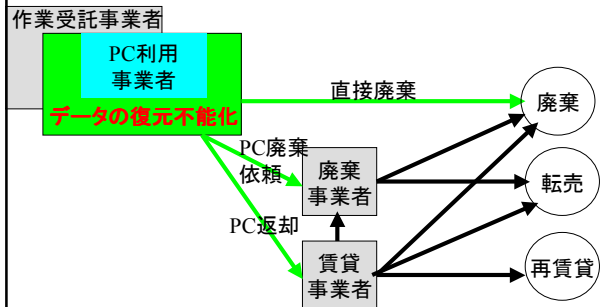
PCは、壊れて電源が入らないから安全
取り外したHDDを、他のPCで利用可能

廃棄事業者に依頼すれば、
PC内のデータは完全に消去してくれる

C: 賃貸事業者経由の情報漏洩

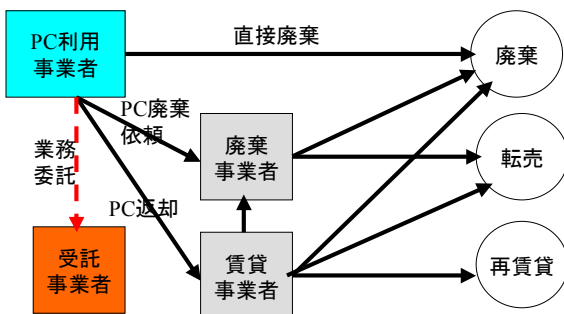


廃棄/返却PCからの情報漏洩防止のために



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

D: 業務委託先経由の情報漏洩



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

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 → ?

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)

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書き込み	0xFF	任意
ランダム書き込み	乱数	任意
米国防総省方式(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)
米国防軍方式(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

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)

- 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)

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/返却PCの情報漏洩対策

- データの復元不能化
- 廃棄の場合
HDDを物理的に破壊
HDD上のデータを磁気的に消去(消磁)
- 返却(他への転用)の場合
HDD上のデータを上書きにより消去

廃棄/返却PCの監査対応のために

- データの復元不能化の記録、
監査者が信頼できるエビデンスが重要