

みんなのための デジタル・フォレンジック



東京電機大学教授
(内閣官房情報セキュリティ補佐官)
佐々木良一



目次

- 1 . デジタル・フォレンジックとは
- 2 . 警察のためのデジタル・フォレンジック
- 3 . PCユーザのためのデジタル・フォレンジック
- 4 . 企業のためのデジタル・フォレンジック
- 5 . 今後の動向



目次

- 1 . デジタル・フォレンジックとは
- 2 . 警察のためのデジタル・フォレンジック
- 3 . PCユーザのためのデジタル・フォレンジック
- 4 . 企業のためのデジタル・フォレンジック
- 5 . 今後の動向

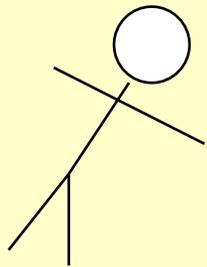


デジタル・フォレンジックのイメージ

Forensicというのは「法の」とか「法廷の」という意味を持つ形容詞や、「捜査や法廷で役に立つもの」の意味を持つ名詞(通常Forensics)

Forensic Medicine: 「法医学」
捜査や裁判に医学知識を利用する学問

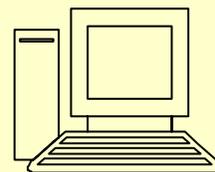
殺人事件



死因は？、
凶器は？、
犯人の血液型は？

Digital Forensics: 「デジタル・フォレンジック」
捜査や裁判のために情報処理技術を用いデジタルデータの証拠性を確保するための技術と手順

不正侵入



侵入手口は？
侵入経路は？

デジタル・フォレンジック研究会

デジタル・フォレンジック研究会
The Institute of Digital Forensics

研究会概要... 会長挨拶 設立の趣旨 対象領域 定款 役員構成

役員構成

会長	辻井 重男	情報セキュリティ大学院大学 学長
副会長	安富 潔	慶應義塾大学大学院法務研究科・法学部教授・弁護士
理事	林 祐一郎	情報セキュリティ大学院大学 副学長
	佐々木 良一	東京電機大学 工学部 情報メディア学科 教授
	高橋 郁夫	弁護士
	須川 賢洋	新潟大学法学部 法政コミュニケーション学科 助手
	萩原 栄幸	(社)コンピュータソフトウェア著作権協会 技術顧問
	舟橋 信	(財)未来工学研究所 参与
	町村 泰貴	南山大学大学院 法務研究科 教授
	石井 徹哉	千葉大学 法経学部 助教授
	上原 哲太郎	京都大学大学院 工学研究科附属情報センター 助教授
	秋山 昌範	国立国際医療センター 医療情報システム開発研究部 部長
	古川 俊治	慶應義塾大学大学院法務研究科・医学部 助教授 兼 TMC総合総合法律事務所 弁護士
	守本 正宏	(株)UBIC 代表取締役社長
	石井 正敏	(株)NTTデータ ナショナルセキュリティビジネスユニット長
	丸谷 俊博	(株)フォーカスシステムズ 新規事業推進室 室長
	向井 徹	シーア・インサイト・セキュリティ(株) 代表取締役社長
	伊藤 一泰	(株)金融システム総合研究所 取締役
佐藤 慶浩	日本ヒューレット・パッカド(株) 個人情報保護対策室 室長	
小向 太郎	(株)情報通信総合研究所 政策研究グループ シニアリサーチャー	
監事	丸山 満彦	(監)トーマツ エンタープライズリスクサービス部 シニアマネージャー
	熊平 美香	(財)クマヒラセキュリティ財団 専務理事

2004年発足
会長: 辻井重男中央大学教授
副会長: 安富潔慶応大学教授

2011年より佐々木良一が会長
<http://www.digitalforensic.jp/>

BACK TOP

デジタル・フォレンジックのユーザは？

警察などの法執行機関

PCユーザなどの個人

企業などの組織



目次

- 1 . デジタル・フォレンジックとは
- 2 . 警察のためのデジタル・フォレンジック
- 3 . PCユーザのためのデジタル・フォレンジック
- 4 . 企業のためのデジタル・フォレンジック
- 5 . 今後の動向



大相撲八百長問題

2011年に発覚した、日本相撲協会の現役の大相撲力士による大相撲本場所での取組での八百長への関与に関する問題

前年2010年に起きた大相撲野球賭博問題の捜査において、賭博に関与した力士から証拠として押収した携帯電話のメールを調べていて発覚



大相撲八百長問題

2011年に発覚した、日本相撲協会の現役の大相撲力士による大相撲本場所での取組での八百長への関与に関する問題

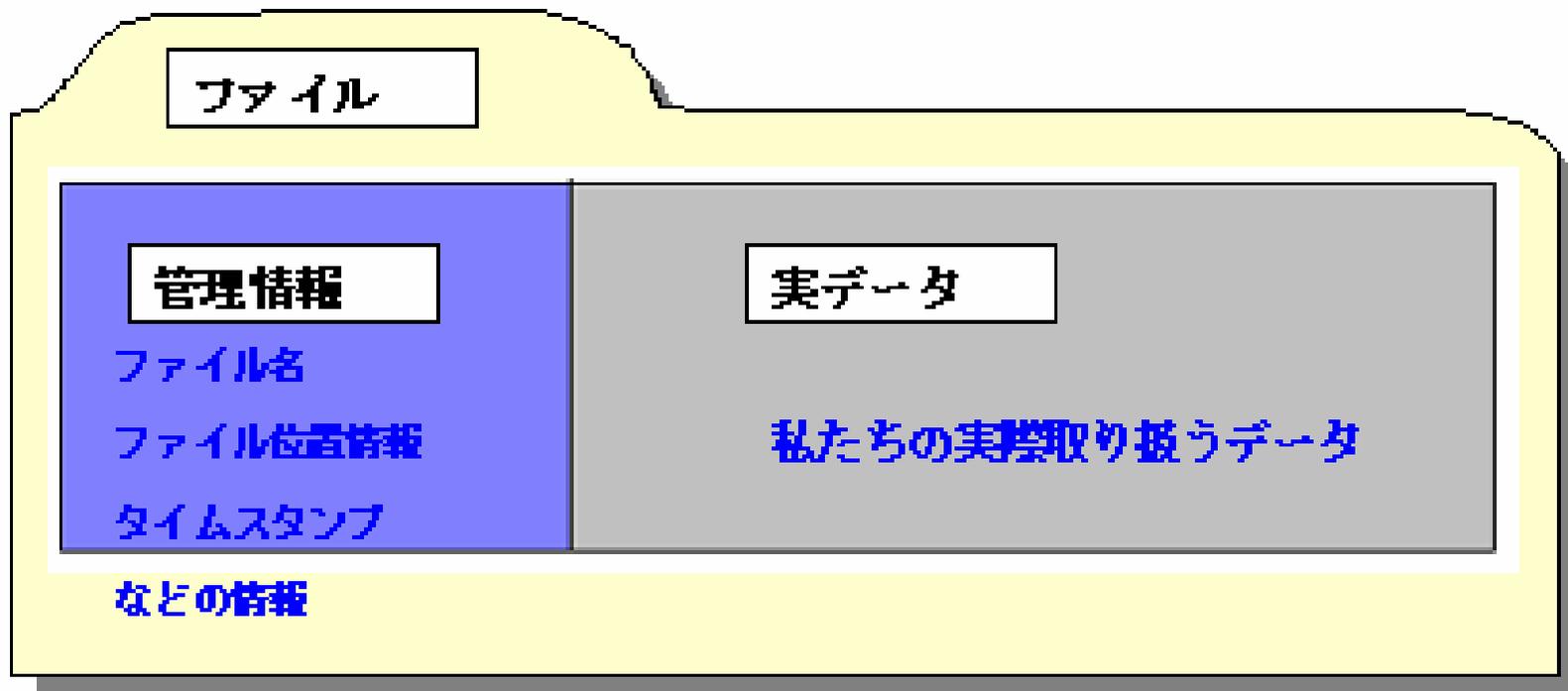
前年2010年に起きた大相撲野球賭博問題の捜査において、賭博に関与した力士から証拠として押収した携帯電話のメールを調べていて発覚

消去していたはずだが



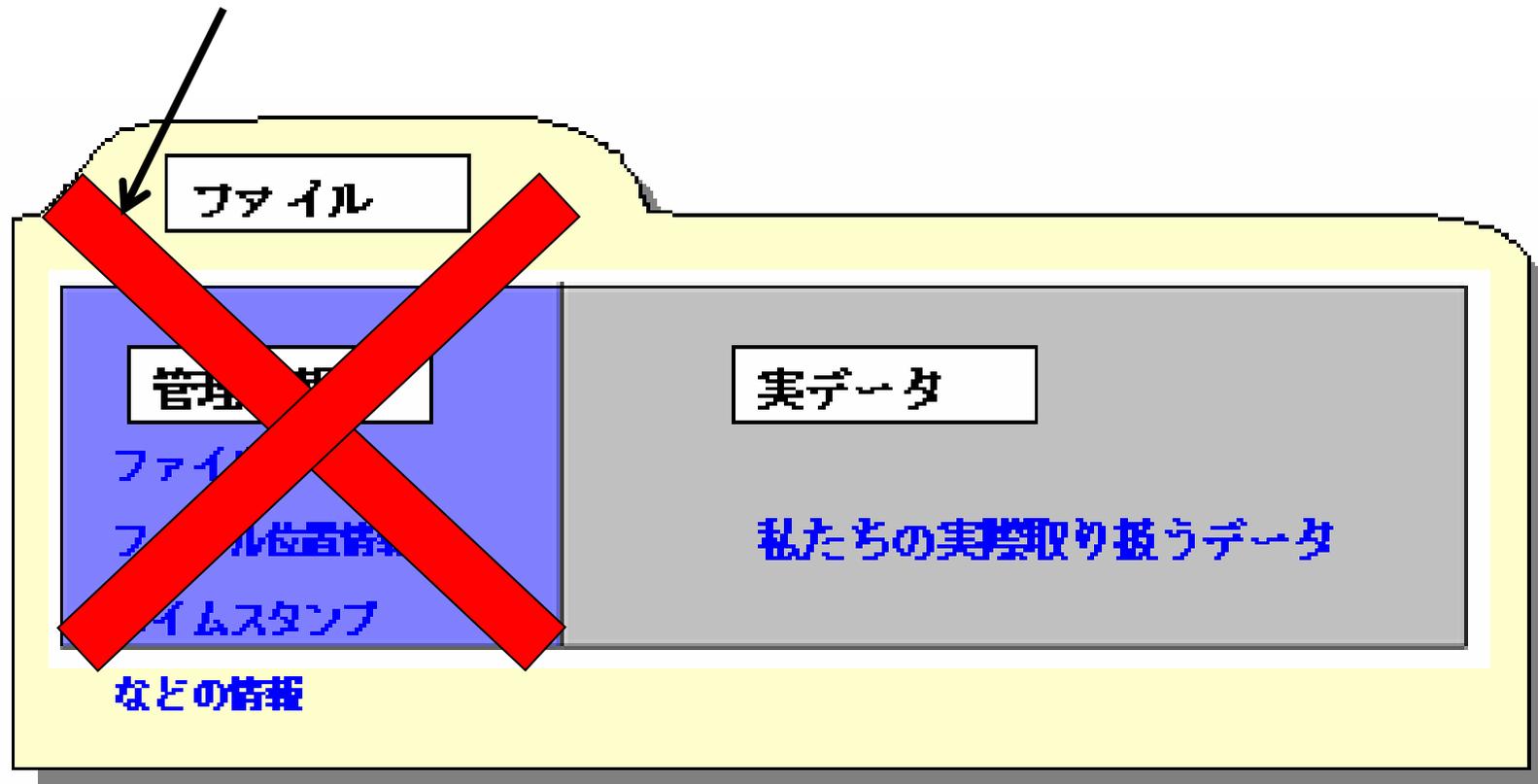
データ消去とは(1)

- データとファイル構造
 - “データ”は PCや携帯内に「ファイル」として存在



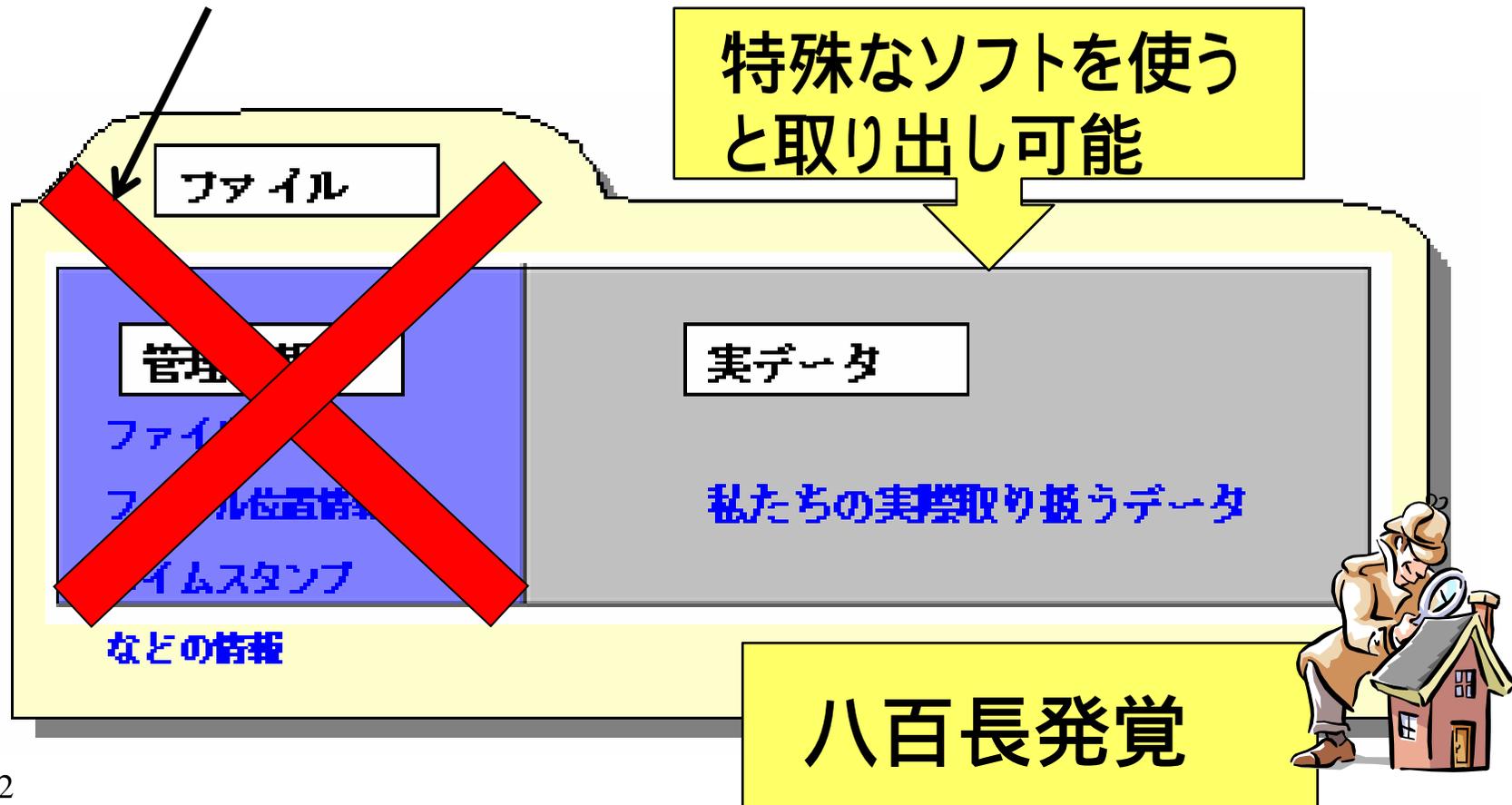
データ消去とは(2)

- データ消去の行っている事



データの取り出し

- データ消去の行っている事



目次

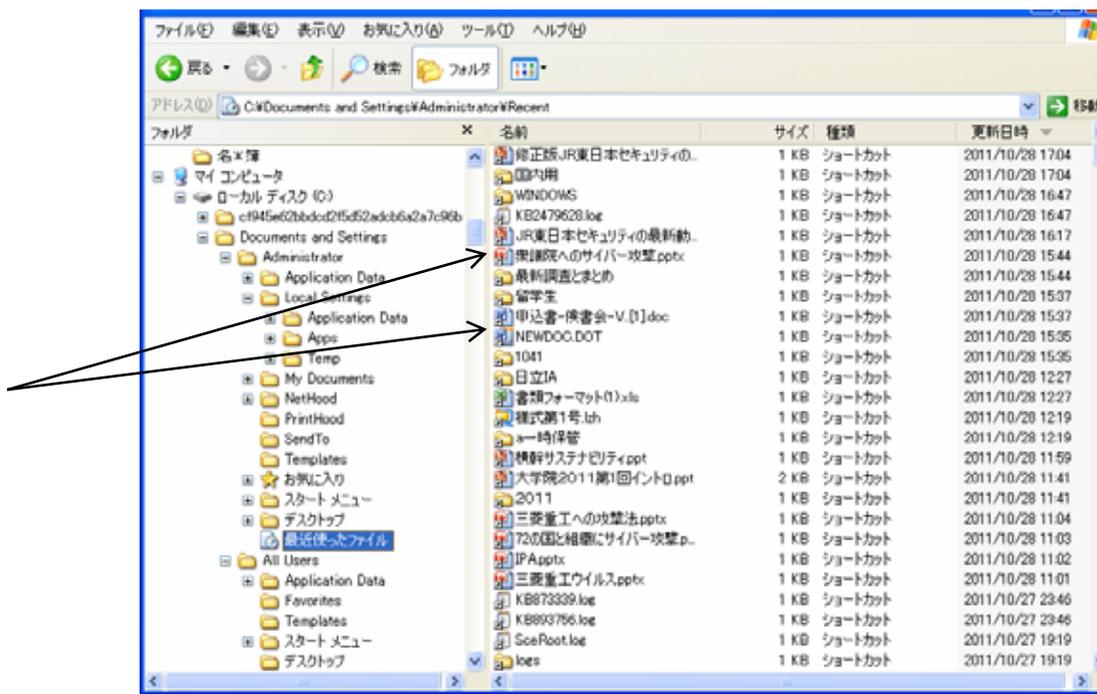
- 1 . デジタル・フォレンジックとは
- 2 . 警察のためのデジタル・フォレンジック
- 3 . PCユーザのためのデジタル・フォレンジック
- 4 . 企業のためのデジタル・フォレンジック
- 5 . 今後の動向



デジタル・フォレンジックの知識 があるといんなことが分かる

C:\¥Documents&Setting¥<ユーザ>¥Recentを調べると最近使ったファイルがわかる。(Windows XPの場合)

ファイル名



自分が最近使っていないファイルがあると、誰かがそのファイルを見た可能性やウイルスによって処理されている可能性がある。

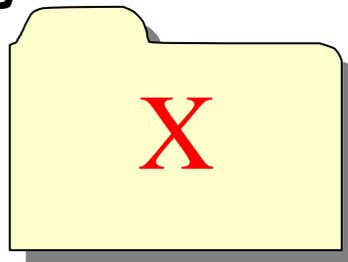
誤って消去したファイルを 復元できる

- フリーの復元ソフト



直後なら復元可能

【消去ファイル】



データ復元はデジタル・フォレンジックの重要技術

3.11の津波で海水につかったPC



写真はデータサルベージ社提供



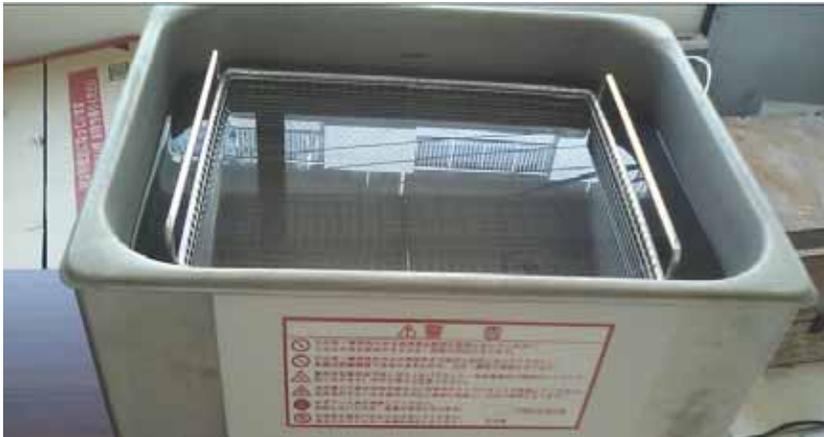
(ハードディスク部)

思い出深い写真や大切な
データも入っている
はたしてデータ復元はできるか？

データ復元の試み

震災の直後からデータ復元会社の有志らが現地で
復元活動

いろいろな方法でディスク表面の汚れを除去後復元処理
(写真は1%の塩酸水につけているところ)



水没後1週間以内なら
80 - 90%のディスク
からデータ復元

写真はデータサルベージ社提供

目次

- 1 . デジタル・フォレンジックとは
- 2 . 警察のためのデジタル・フォレンジック
- 3 . PCユーザのためのデジタル・フォレンジック
- 4 . 企業のためのデジタル・フォレンジック
- 5 . 今後の動向



企業では従業員の不正の 監視が必要

ある社員が、企業の機密情報を不正に入手し外部に持ち出している疑いが



十分な証拠のないまま処分をしようとするとな逆に訴訟の可能性が



疑わしい従業員のPC(会社所有)の調査



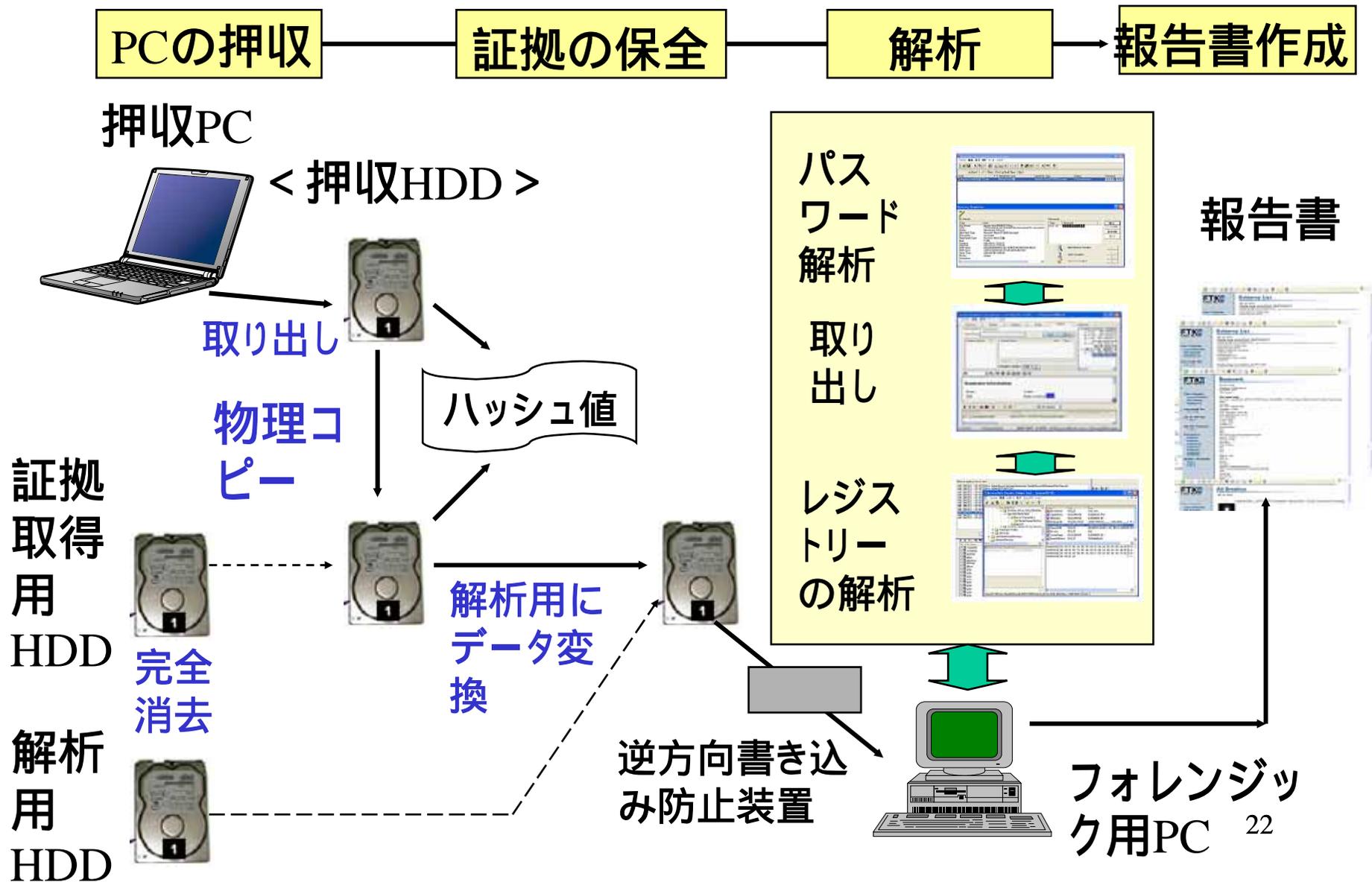
デジタル・フォレンジックツールの比較

名称など	開発者 (販売会社)	機能など	備考
Encase (1997年発売)	Guidance Software社 (商品)	PC内のデータの復元 メインメモリのデータ の監視など 報告書の作成など	
Ultimate Tool Kit (2004年発売)	Access Data社 (同上)	証拠性保全のための 総合的ツールキット (PC内のデータの復元、 パスワード解読、報告 書の作成など)	Forensic Tool Kitが中心

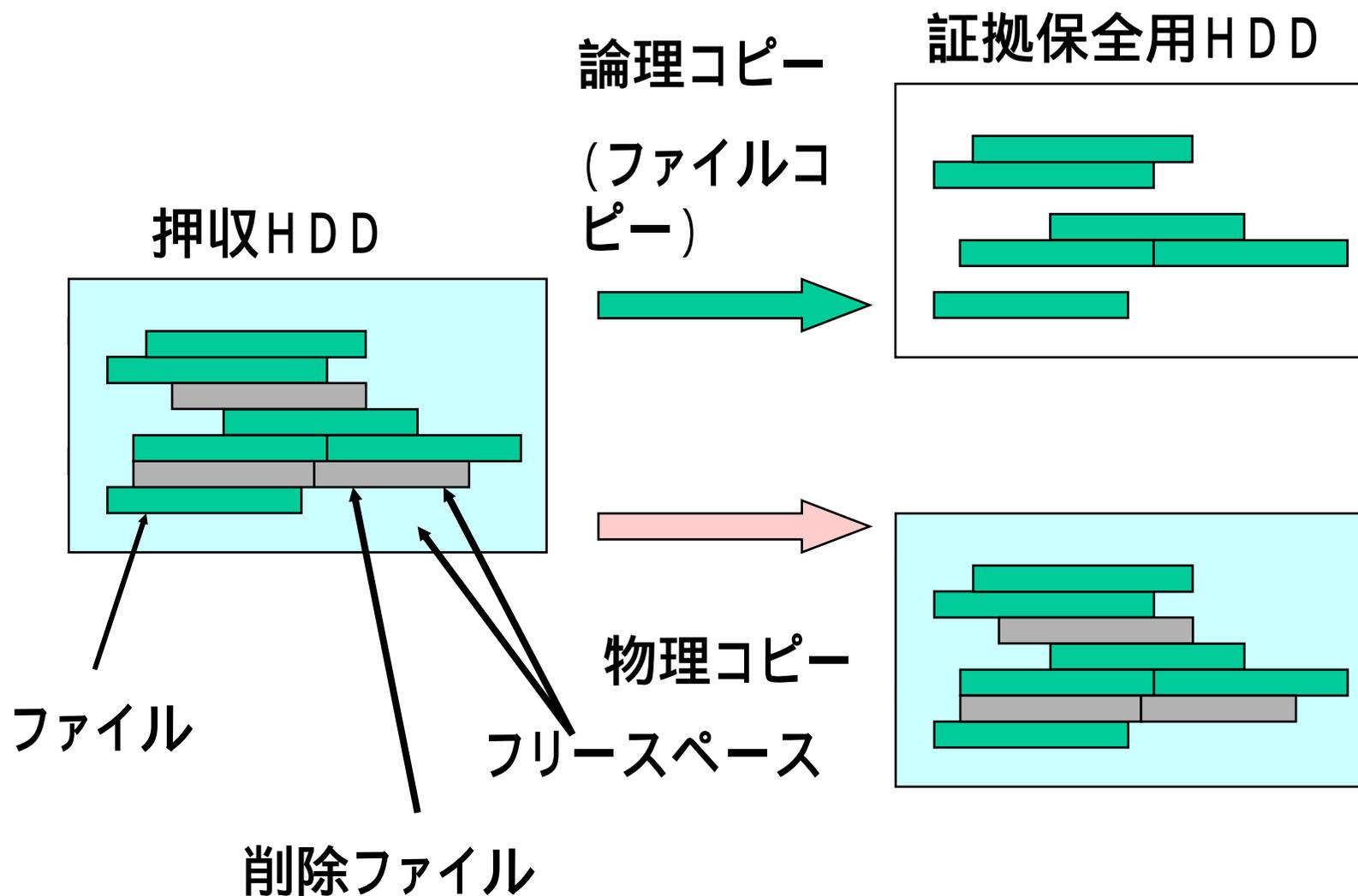
AccessData社の製品

The screenshot shows a Microsoft Internet Explorer browser window displaying the website for UBIC (Intelligence for Security). The browser's address bar shows the URL <http://www.ubic.co.jp/Ultimate.htm>. The website features a navigation menu with links for 'CEOメッセージ', 'UBIC事業内容', 'UBICパートナー', '会社概要', '個人情報取扱', and 'お問い合わせ'. A main banner at the top reads 'デジタル・フォレンジックを通じ 安心安全な社会を' and 'Digital Forensic System Integrator UBIC, Inc'. Below this, there are buttons for 'Forensic Hardware', 'Forensic Software', 'HDD Copy Tool', and 'Site Map'. The 'Forensic Software' section is highlighted, with sub-links for 'Ultimate Toolkit', 'Forensic Toolkit', 'Registry Viewer', 'PRTK & DNA', and 'Support & Training'. The 'Ultimate Toolkit' is prominently featured with the text 'The complete AccessData Software Kit' and a description: 'Ultimate Toolkitはコンピュータの監査と調査データ保護に必要な全てのツールを一つにまとめた、オールインワン・パッケージングツールです。'. To the right of this text is a 'TOP' button. Below the main text, there are several product tiles: 'Forensic Toolkit' (Find Computer Evidence Quickly and Easily), 'Registry Viewer' (Find Registry Data Quickly & Easily), 'Password Recovery Toolkit' (Recover Passwords Quickly & Easily), 'WipeDrive 3.0' (Completely Eliminate Hard Drive Data), and 'Distributed Network Attack' (Putting Idle Time to Work). An arrow points from the 'Forensic Toolkit' tile towards the Japanese characters '中心' (Center). At the bottom left, there is a section for 'Forensic製品の販売に関するお問合せ' (Contact for forensic product sales) with the 'Focus Systems' logo. The browser's status bar at the bottom right shows 'インターネット' (Internet).

デジタル・フォレンジックの手順



物理コピーと論理コピー



書き込み防止装置



レジストリーとは



レジストリ (Registry)

Windows 95以降で、各種の環境設定やドライバの指定、アプリケーションの関連付けなどの情報を保存しているファイル。Windows 3.1で使われていたINIファイルが発展したもの。各種のプロパティや設定メニューを変更すると、そのほとんどはレジストリに保存される。INIファイルの場合はアプリケーションごとに用意されるため、アプリケーションが増えてくると管理が複雑になった。同時に、INIファイルの多くはテキスト・ファイルであるため、だれでも簡単に編集できるが、これが逆に動作不良などのトラブルの元にもなっていた。そこでWindows 95以降では、すべての設定情報をレジストリで一元管理し、バイナリ・ファイルとして保存することで簡単に内容を変更できないようにした。

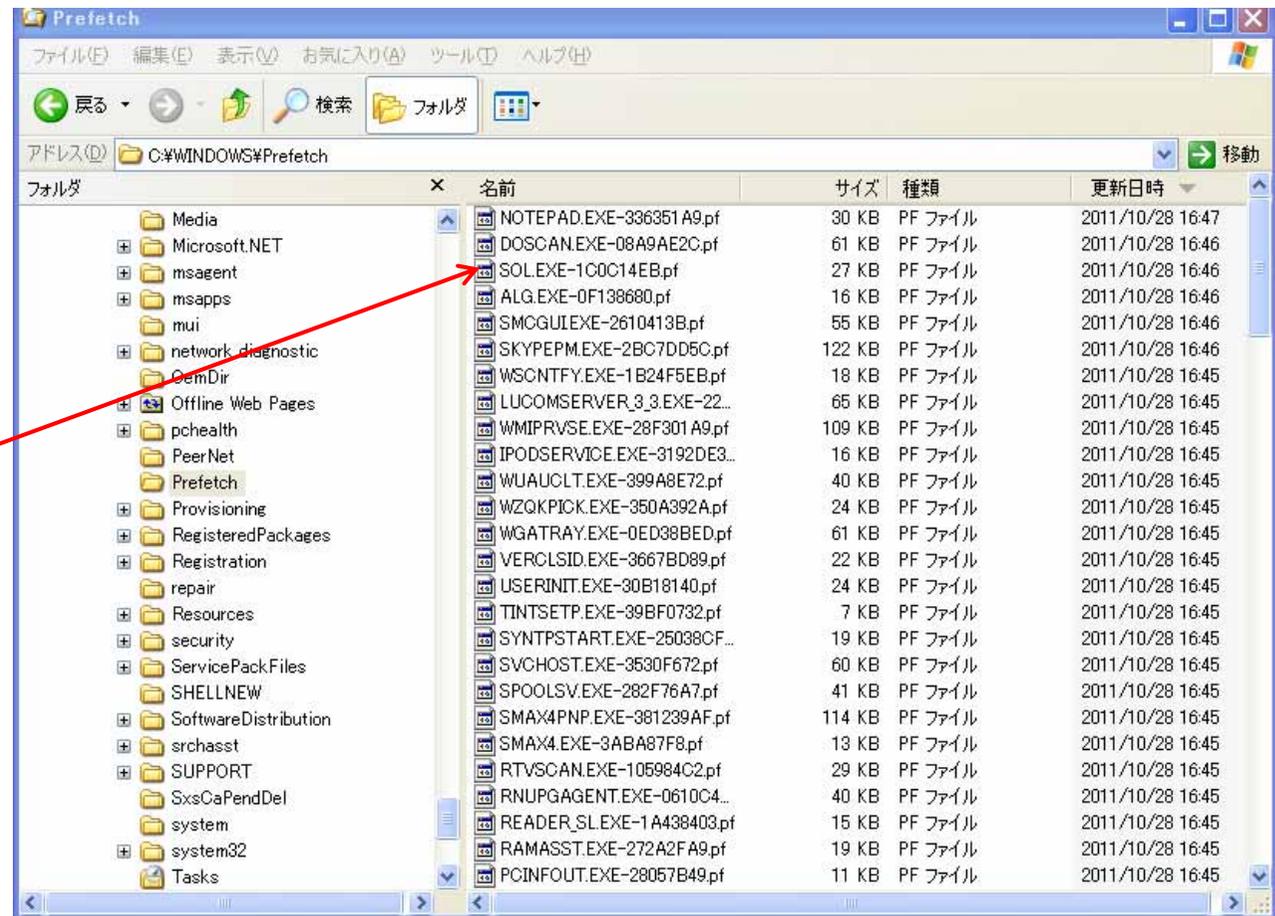
ツールを使わなくてもこんなことが分かる(1)

プリフェッチ

C:¥WINDOWS¥prefetch
を調べると最近使ったプログラムがわかる。

この例だと、16:45に
sol.exeを実行したことが示
されている。

Windows-XPの
場合



名前	サイズ	種類	更新日時
NOTEPAD.EXE-336351A9.pf	30 KB	PF ファイル	2011/10/28 16:47
DOSCAN.EXE-08A9AE2C.pf	61 KB	PF ファイル	2011/10/28 16:46
SOLE.EXE-1C0C14EB.pf	27 KB	PF ファイル	2011/10/28 16:46
ALG.EXE-0F139680.pf	16 KB	PF ファイル	2011/10/28 16:46
SMCGUI.EXE-2610413B.pf	55 KB	PF ファイル	2011/10/28 16:46
SKYPEPM.EXE-2BC7DD5C.pf	122 KB	PF ファイル	2011/10/28 16:46
WSCNTFY.EXE-1B24F5EB.pf	18 KB	PF ファイル	2011/10/28 16:45
LUCOMSERVER_3_3.EXE-22...	65 KB	PF ファイル	2011/10/28 16:45
WMIPRVSE.EXE-28F301A9.pf	109 KB	PF ファイル	2011/10/28 16:45
IPODSERVICE.EXE-3192DE3...	16 KB	PF ファイル	2011/10/28 16:45
WUAUCLT.EXE-399A8E72.pf	40 KB	PF ファイル	2011/10/28 16:45
WZQKPICK.EXE-350A392A.pf	24 KB	PF ファイル	2011/10/28 16:45
WGATRAY.EXE-0ED38BED.pf	61 KB	PF ファイル	2011/10/28 16:45
VERCLSID.EXE-3667BD89.pf	22 KB	PF ファイル	2011/10/28 16:45
USERINIT.EXE-30B18140.pf	24 KB	PF ファイル	2011/10/28 16:45
TINTSETP.EXE-39BF0732.pf	7 KB	PF ファイル	2011/10/28 16:45
SYNTPSTART.EXE-25038CF...	19 KB	PF ファイル	2011/10/28 16:45
SVCHOST.EXE-3530F672.pf	60 KB	PF ファイル	2011/10/28 16:45
SPOOLSV.EXE-282F76A7.pf	41 KB	PF ファイル	2011/10/28 16:45
SMAX4PNP.EXE-381239AF.pf	114 KB	PF ファイル	2011/10/28 16:45
SMAX4.EXE-3ABA87F8.pf	13 KB	PF ファイル	2011/10/28 16:45
RTVSCAN.EXE-105984C2.pf	29 KB	PF ファイル	2011/10/28 16:45
RNUPGAGENT.EXE-0610C4...	40 KB	PF ファイル	2011/10/28 16:45
READER_SL.EXE-1A438403.pf	15 KB	PF ファイル	2011/10/28 16:45
RAMASST.EXE-272A2FA9.pf	19 KB	PF ファイル	2011/10/28 16:45
PCINFOUT.EXE-28057B49.pf	11 KB	PF ファイル	2011/10/28 16:45

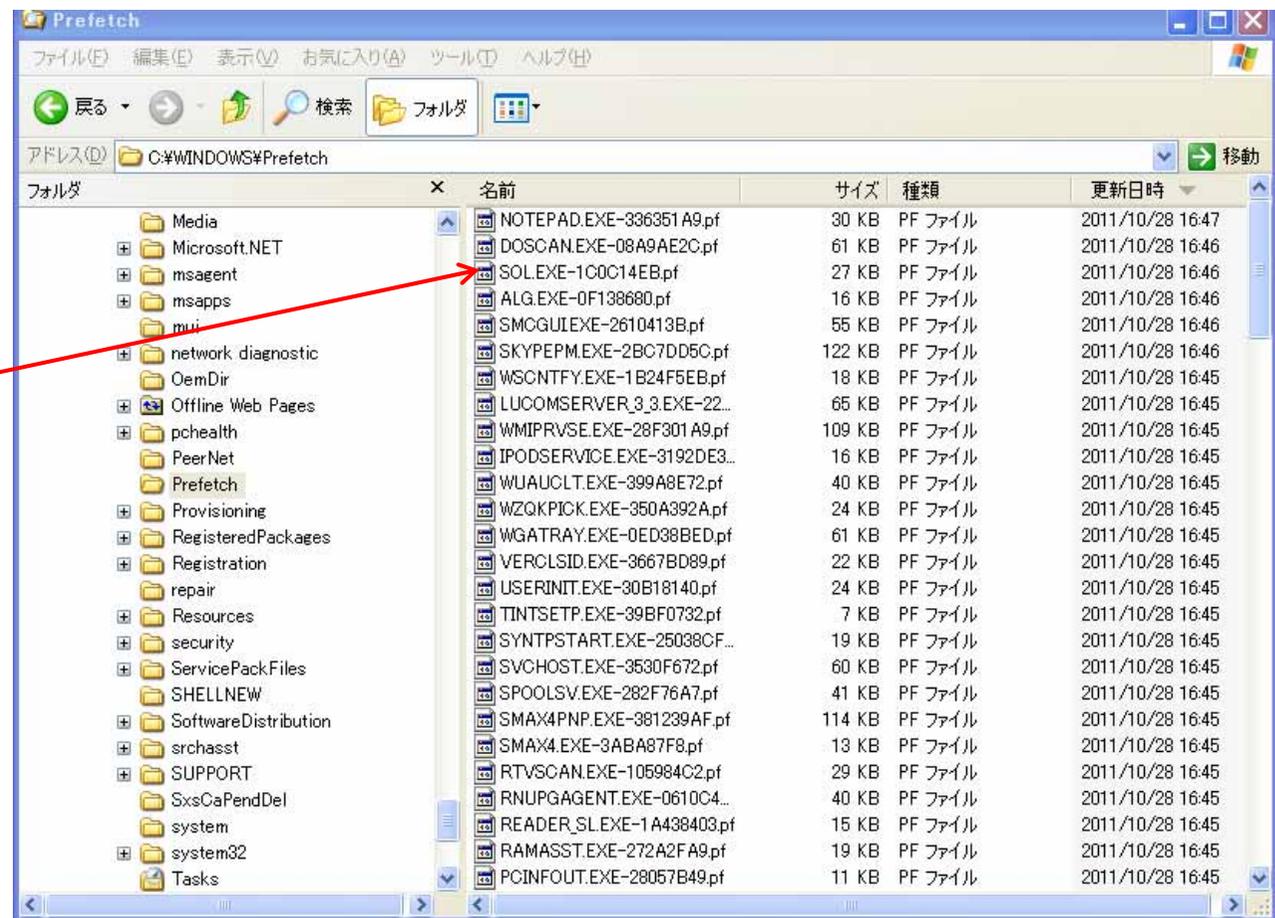
ツールを使わなくてもこんなことが分かる

プリフェッチ

C:\WINDOWS\prefetch
を調べると最近使ったプログラムがわかる。

この例だと、16:45に
sol.exeを実行したことが示
されている。

定時内にソリティアゲーム
をしたことが分かる



名前	サイズ	種類	更新日時
NOTEPAD.EXE-336351A9.pf	30 KB	PF ファイル	2011/10/28 16:47
DOSCAN.EXE-08A9AE2C.pf	61 KB	PF ファイル	2011/10/28 16:46
SOLE.EXE-1C0C14EB.pf	27 KB	PF ファイル	2011/10/28 16:46
ALG.EXE-0F139680.pf	16 KB	PF ファイル	2011/10/28 16:46
SMCGUI.EXE-2610413B.pf	55 KB	PF ファイル	2011/10/28 16:46
SKYPEPM.EXE-2BC7DD5C.pf	122 KB	PF ファイル	2011/10/28 16:46
WSCNTFY.EXE-1B24F5EB.pf	18 KB	PF ファイル	2011/10/28 16:45
LUCOMSERVER_3_3.EXE-22...	65 KB	PF ファイル	2011/10/28 16:45
WMIPRVSE.EXE-28F301A9.pf	109 KB	PF ファイル	2011/10/28 16:45
IPODSERVICE.EXE-3192DE3...	16 KB	PF ファイル	2011/10/28 16:45
WUAUCLT.EXE-399A8E72.pf	40 KB	PF ファイル	2011/10/28 16:45
WZQKPICK.EXE-350A392A.pf	24 KB	PF ファイル	2011/10/28 16:45
WGATRAY.EXE-0ED38BED.pf	61 KB	PF ファイル	2011/10/28 16:45
VERCLSID.EXE-3667BD89.pf	22 KB	PF ファイル	2011/10/28 16:45
USERINIT.EXE-30B18140.pf	24 KB	PF ファイル	2011/10/28 16:45
TINTSETP.EXE-39BF0732.pf	7 KB	PF ファイル	2011/10/28 16:45
SYNTPSTART.EXE-25038CF...	19 KB	PF ファイル	2011/10/28 16:45
SVCHOST.EXE-3530F672.pf	60 KB	PF ファイル	2011/10/28 16:45
SPOOLSV.EXE-282F76A7.pf	41 KB	PF ファイル	2011/10/28 16:45
SMAX4PNP.EXE-381239AF.pf	114 KB	PF ファイル	2011/10/28 16:45
SMAX4.EXE-3ABA87F8.pf	13 KB	PF ファイル	2011/10/28 16:45
RTVSCAN.EXE-105984C2.pf	29 KB	PF ファイル	2011/10/28 16:45
RNUPGAGENT.EXE-0610C4...	40 KB	PF ファイル	2011/10/28 16:45
READER_SL.EXE-1A438403.pf	15 KB	PF ファイル	2011/10/28 16:45
RAMASST.EXE-272A2FA9.pf	19 KB	PF ファイル	2011/10/28 16:45
PCINFOUT.EXE-28057B49.pf	11 KB	PF ファイル	2011/10/28 16:45

< 禁止されているWinnyなどを使っていたことなどもわかりえる。 >

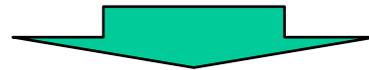
目次

- 1 . デジタル・フォレンジックとは
- 2 . 警察のためのデジタル・フォレンジック
- 3 . PCユーザのためのデジタル・フォレンジック
- 4 . 企業のためのデジタル・フォレンジック
- 5 . 今後の動向
 - 5 . 1 ネットワーク・フォレンジックの展開
 - 5 . 2 訴訟にそなえるためのDF
 - 5 . 3 スマホのDF



ネットワーク・フォレンジックの必要性

三菱重工や衆議院への攻撃で重要な情報が漏えいの可能性



従来のサーバでのログの収集だけでは、情報漏洩の有無や漏洩ルートがわからないことが多く、パケットログの収集の必要性が増大

データ流出事実・流出経路の確認

- ネットワーク・フォレンジックのためのログの保存の強化
- (a) 内部から外部へのパケットの保存 (Firewall,IDSなど)
 - (b) 全通信パケットの保存 (Net- Detectorの利用 など)

ログ間の相関の把握

- (a) ホスト側のログとパケットログの相関分析の実施
- (b) 全ログ (入退室のログ等を含む) 間の相関分析システムの導入 (ArcSightなど)



NISCとデジタル・フォレンジック研究会が協力して検討会を実施し、調査報告書を作成

目次

- 1 . デジタル・フォレンジックとは
- 2 . 警察のためのデジタル・フォレンジック
- 3 . PCユーザのためのデジタル・フォレンジック
- 4 . 企業のためのデジタル・フォレンジック
- 5 . 今後の動向
 - 5 . 1 ネットワーク・フォレンジックの展開
 - 5 . 2 訴訟にそなえるためのDF
 - 5 . 3 スマフォのDF



企業が訴訟を受けることが増加



(1) 企業が企業を訴訟する場合

業務依頼を受けたビジネスの相手から、守秘義務の違反や、不誠実な業務であったとして契約違反で、訴えられる可能性がある。

(2) 国などが企業を訴訟する場合

SOX法(米国企業改革法)や商法(証券取引法など)などの違反で、訴えられる可能性がある。

(3) 個人が企業を訴訟する場合

企業の不正の告発や、組合活動などのために、会社から不当な扱いを受けたということで従業員が、企業を訴訟する場合が考えられる。

望ましくない結果(損害)の例

情報漏洩事件の加害者として相手から訴えられ、自分の無過失または軽過失を証明できず、有罪または重過失と判断されて、過大な損害賠償をせざるを得なくなる

【濡れ衣、そこまではやってない】



不正を行っていないことの証明の準備

(1) 企業のシステムが不正を行えないようになってきていることの規則作り => ポリシー作成

(2) 従業員が不正を行っていないことの監視と証拠の確保 => 基本的には従来と同じ

(3) 管理者であっても不正を行えないことの仕組みづくり

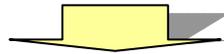
=> 技術で対応

例えばTrusted OSや専用ハード

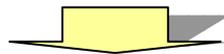


PC内での不正を防止するために

ICカード(スマートカード)のような耐タンパー装置の中
なら装置の持ち主であっても不正はできない



PCの持ち主がPC内でログデータの改ざんを行うのは
比較的容易



PC全体を耐タンパー化できないか(研究1)



研究1 耐タンパー高速処理装置

耐タンパ性を持ち高速処理を行える
PCベースのハード・ソフト

High Grade Anti-Tamper Equipment

HiGATE

を試作した



目次

- 1 . デジタル・フォレンジックとは
- 2 . 警察のためのデジタル・フォレンジック
- 3 . PCユーザのためのデジタル・フォレンジック
- 4 . 企業のためのデジタル・フォレンジック
- 5 . 今後の動向
 - 5 . 1 ネットワーク・フォレンジックの展開
 - 5 . 2 訴訟にそなえるためのDF
 - 5 . 3 スマホのDF



スマホのデジタル・フォレンジック

1. 基本的部分はPCなどのデジタル・フォレンジックと同じ
<フォレンジックツール>

Oxygen Forensic Suite (Oxygen Software社・ロシア)

iPhone及びAndroid、他に対応

Lantern (Katana Forensics社・米国) iPhoneに対応

2. 位置情報や大量の写真なども入っているのでデータを復元することにより見えてくるものも多い

3. ハードディスクではなくフラッシュメモリーを使っており、同じところを何回も書き変えないようにしているので、特別の処理をしなければ時間がたってもデータの復元が容易か



詳細検討必要

