スマートフォン
セキュリティフォーラム

2012年5月24日

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

Information Security Laboratory
ISL

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

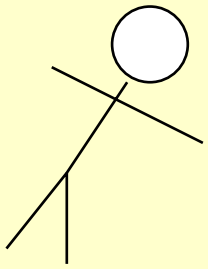
目次

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

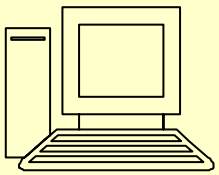
殺人事件



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

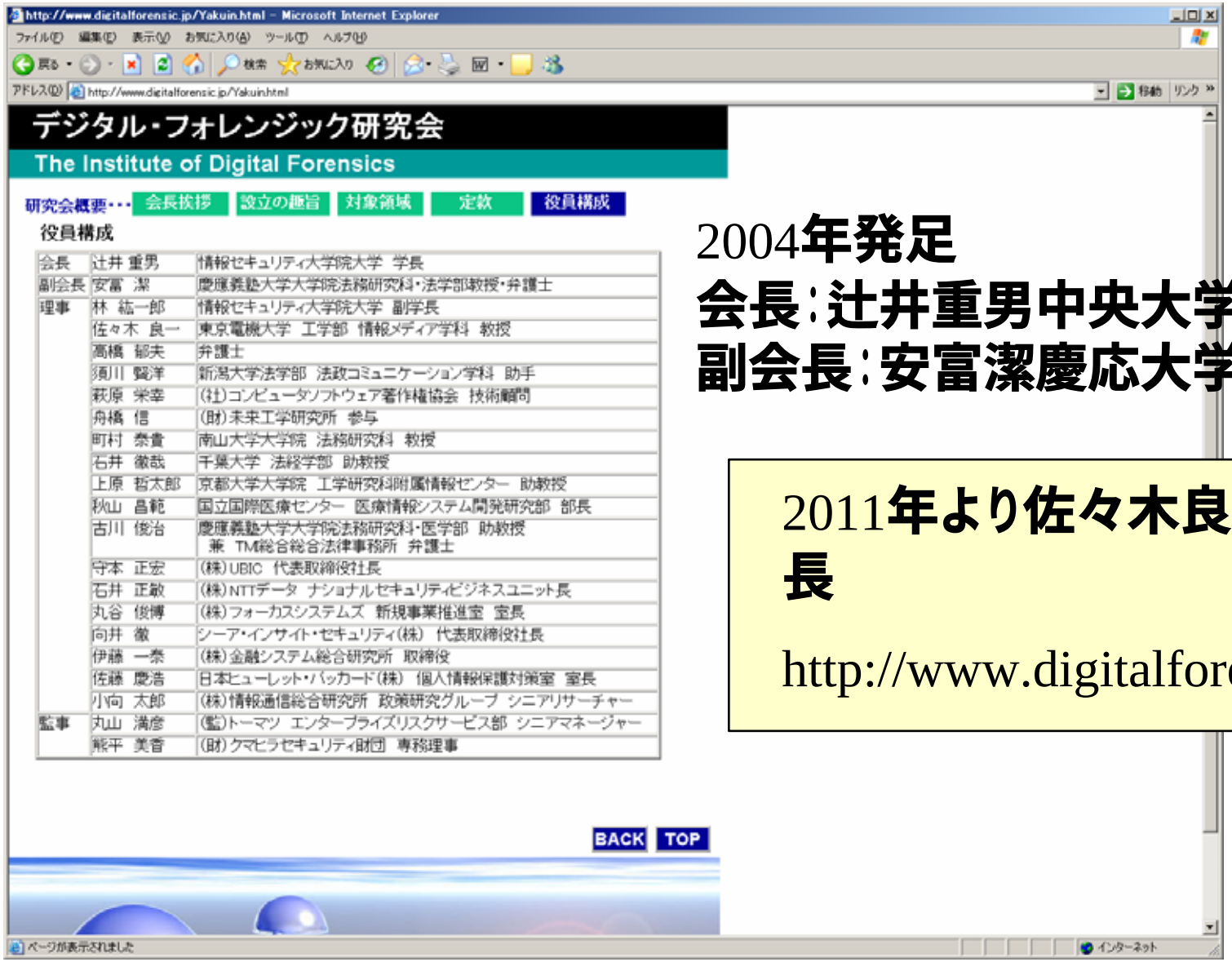
不正侵入



侵入手口は？

侵入経路は？

デジタル･フォレンジック研究会



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/

デジタル･フォレンジックのユーザは？

① 警察などの法執行機関

② PCユーザなどの個人

③ 企業などの組織

Information Security Laboratory
ISL

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

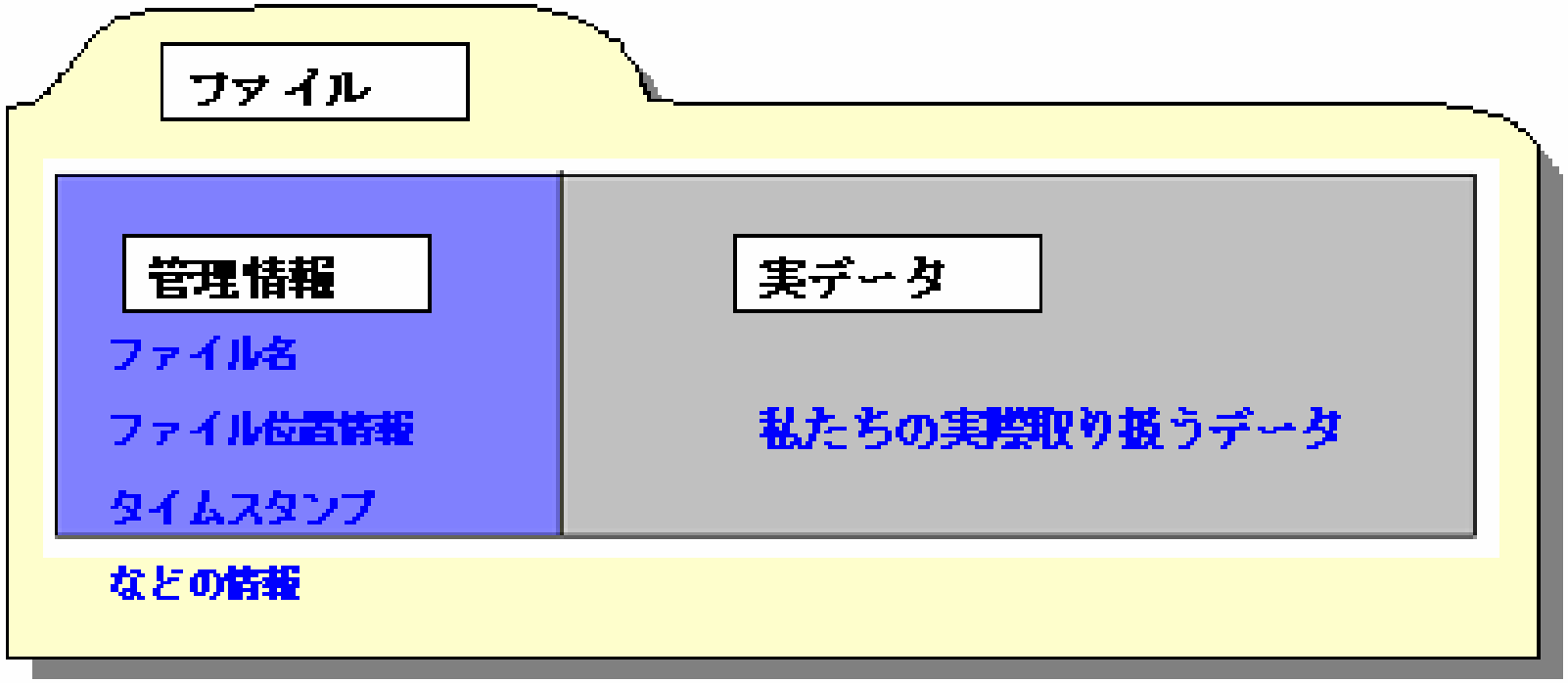
2011年に発覚した、日本相撲協会の現役の大相撲力士による大相撲本場所での取組での八百長への関与に関する問題

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

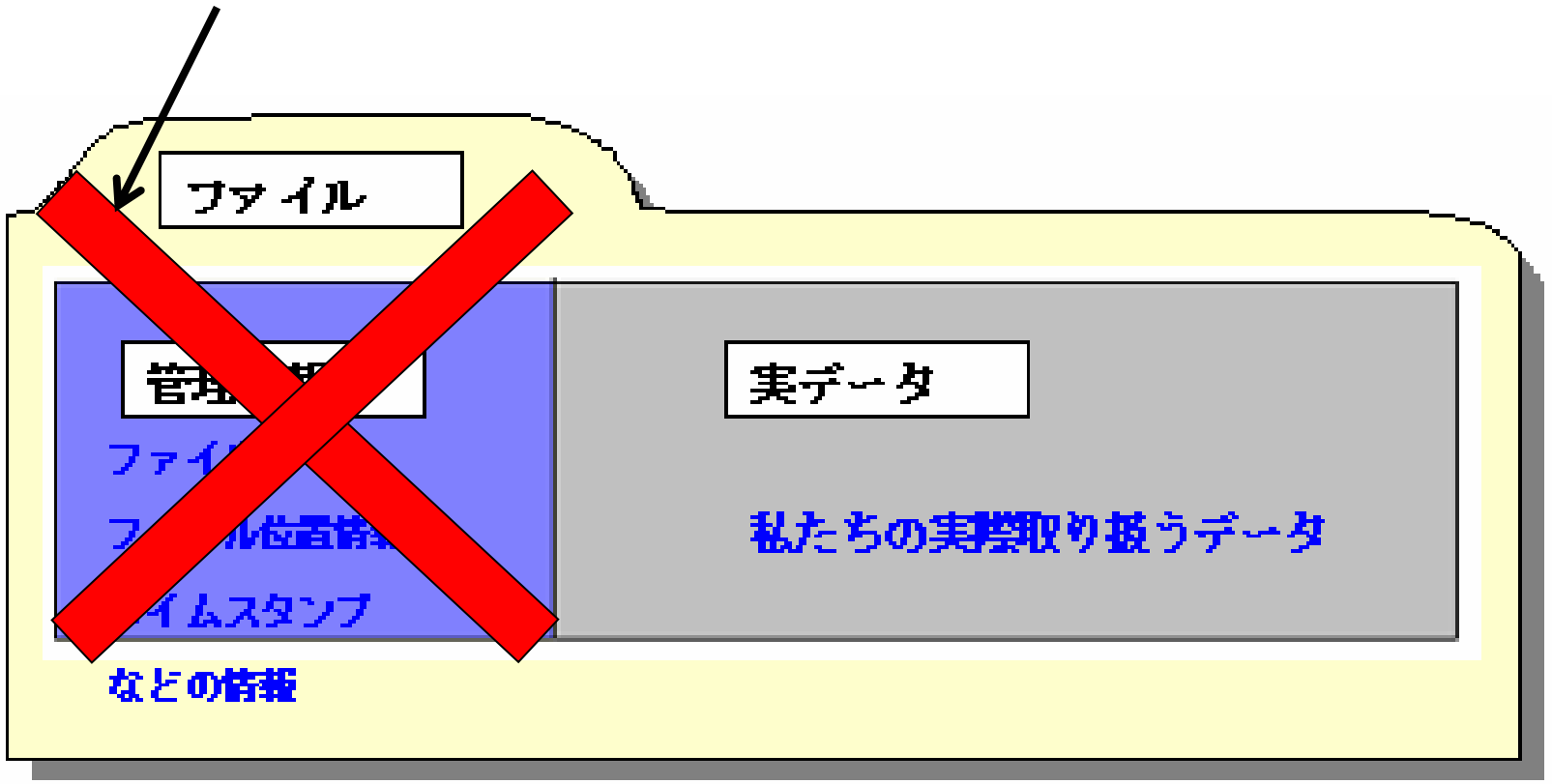
データ消去とは（1）

- 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



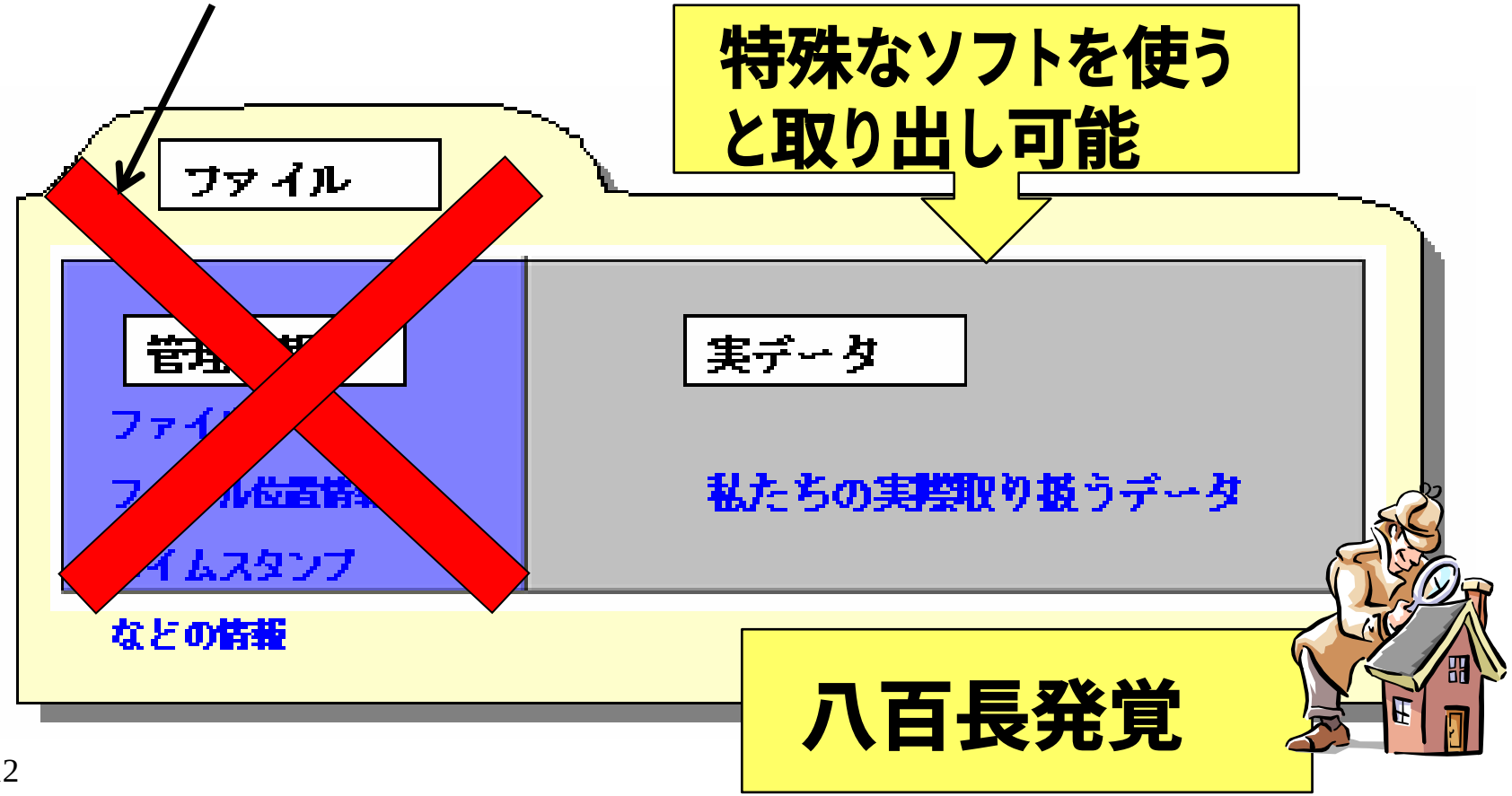
データ消去とは(2)

- 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



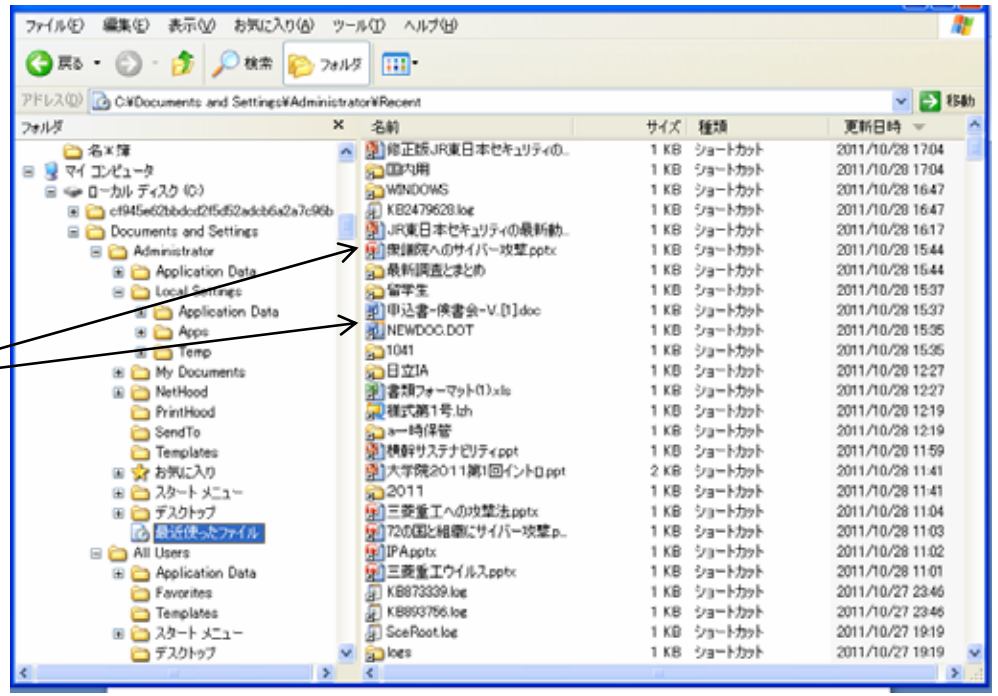
目次

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こんなことが分かる

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



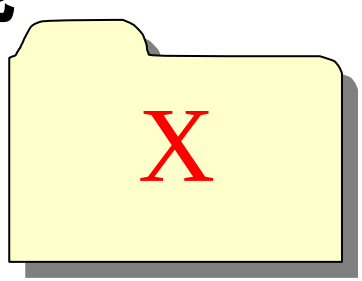
自分が最近使ってないファイルがあると、誰かがそのファイルを見た可能性やウイルスによって処理されている可能性がある。

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

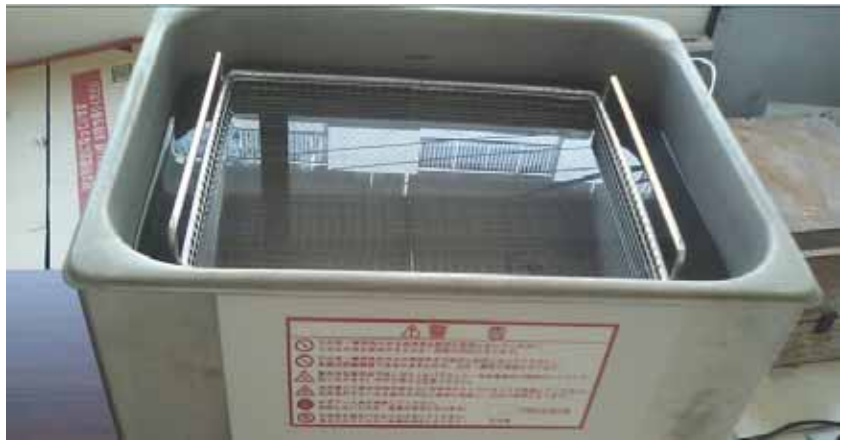
（ハードディスク部）

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

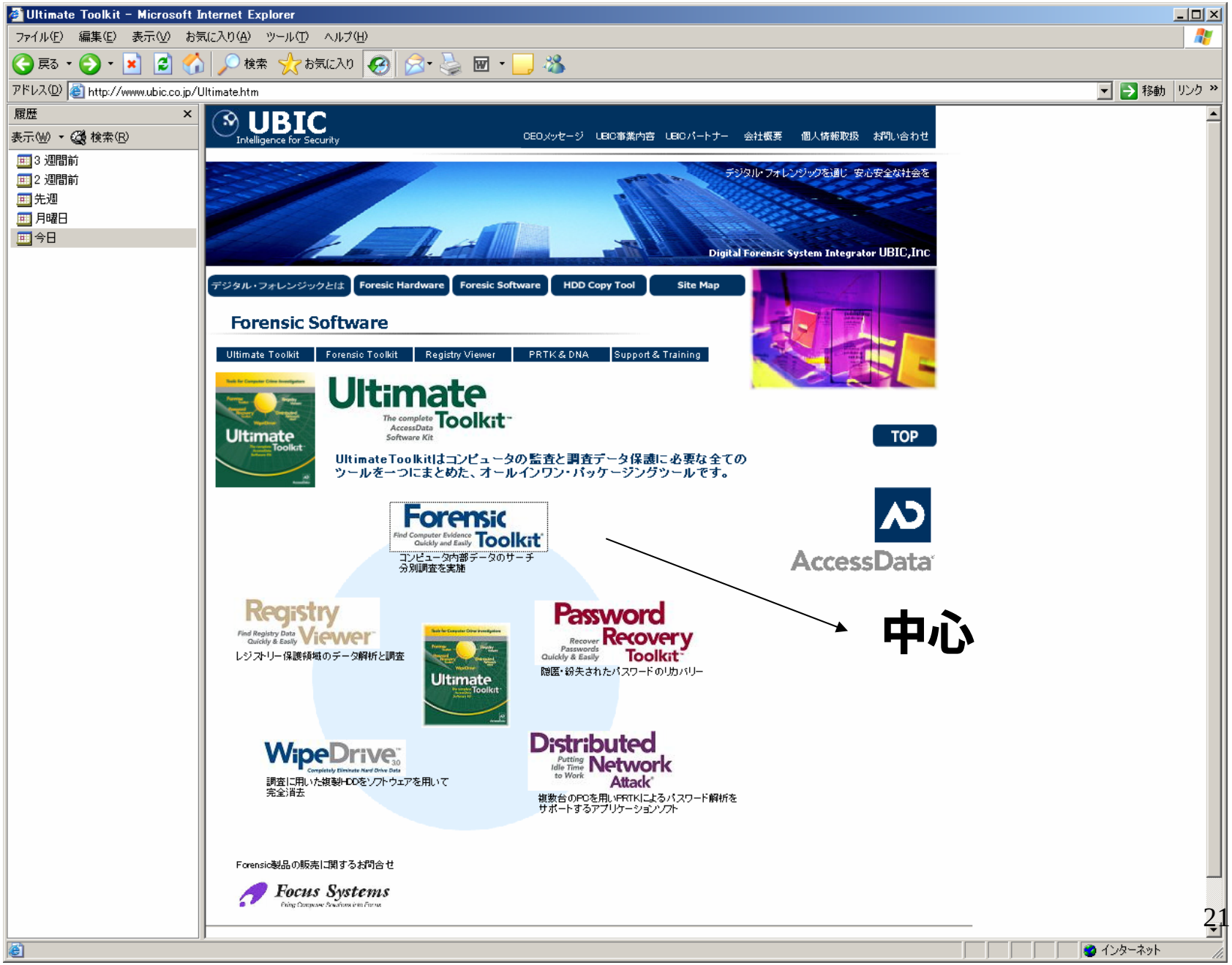
↓

疑わしい従業員のPC（会社所有）の調査

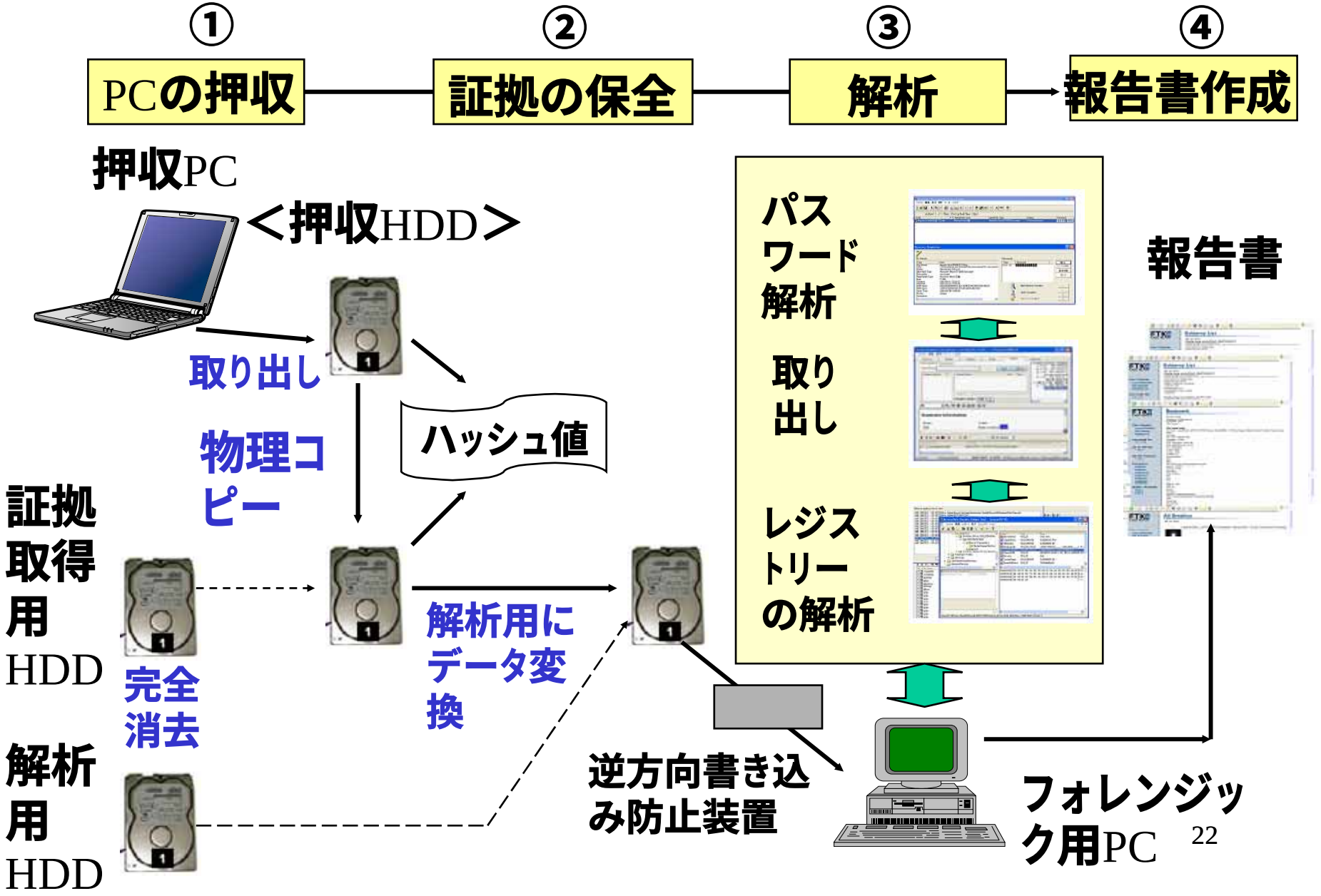
デジタル･フォレンジックツールの比較

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 メインメモリー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

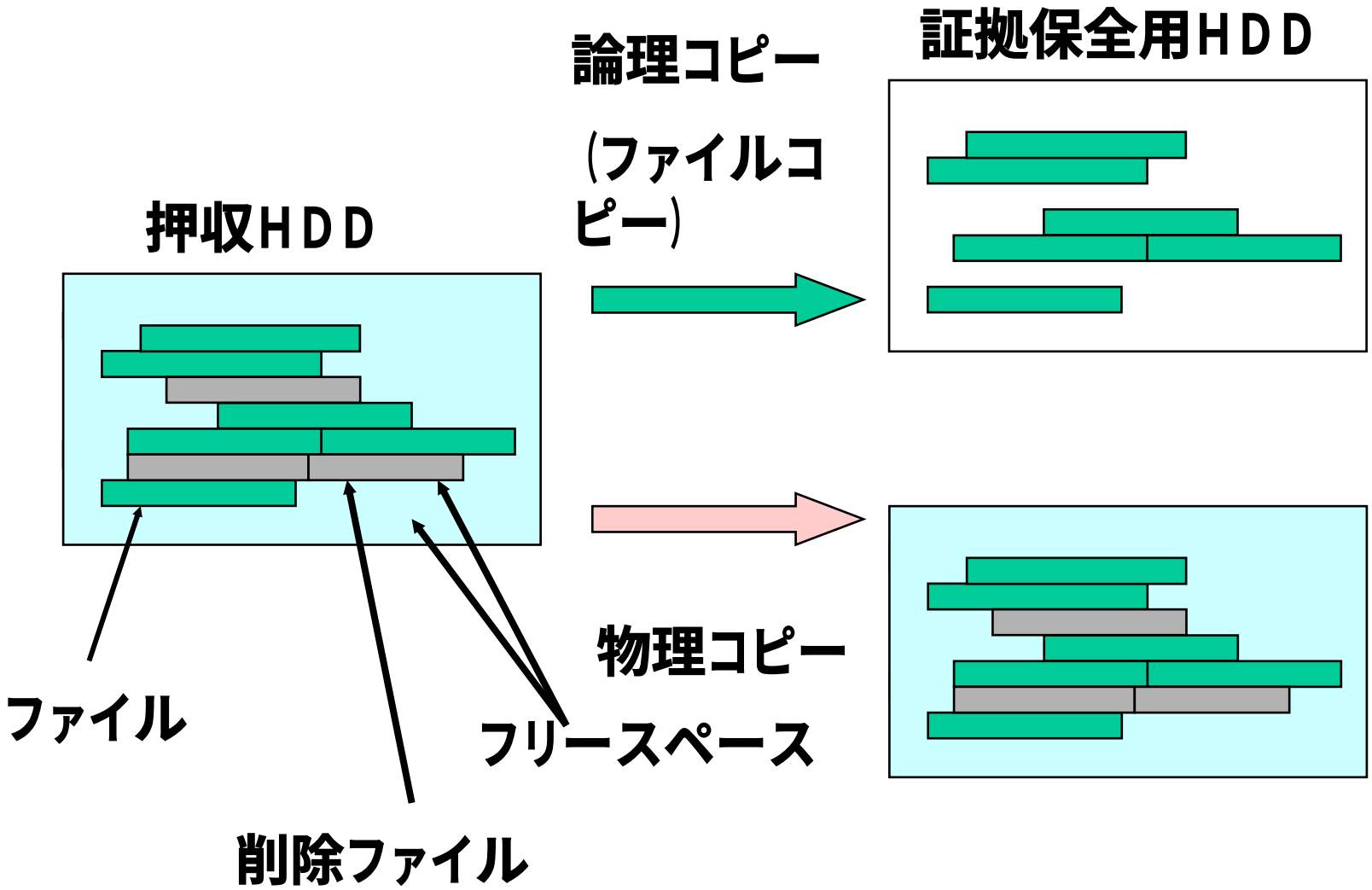
AccessData社の製品



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。

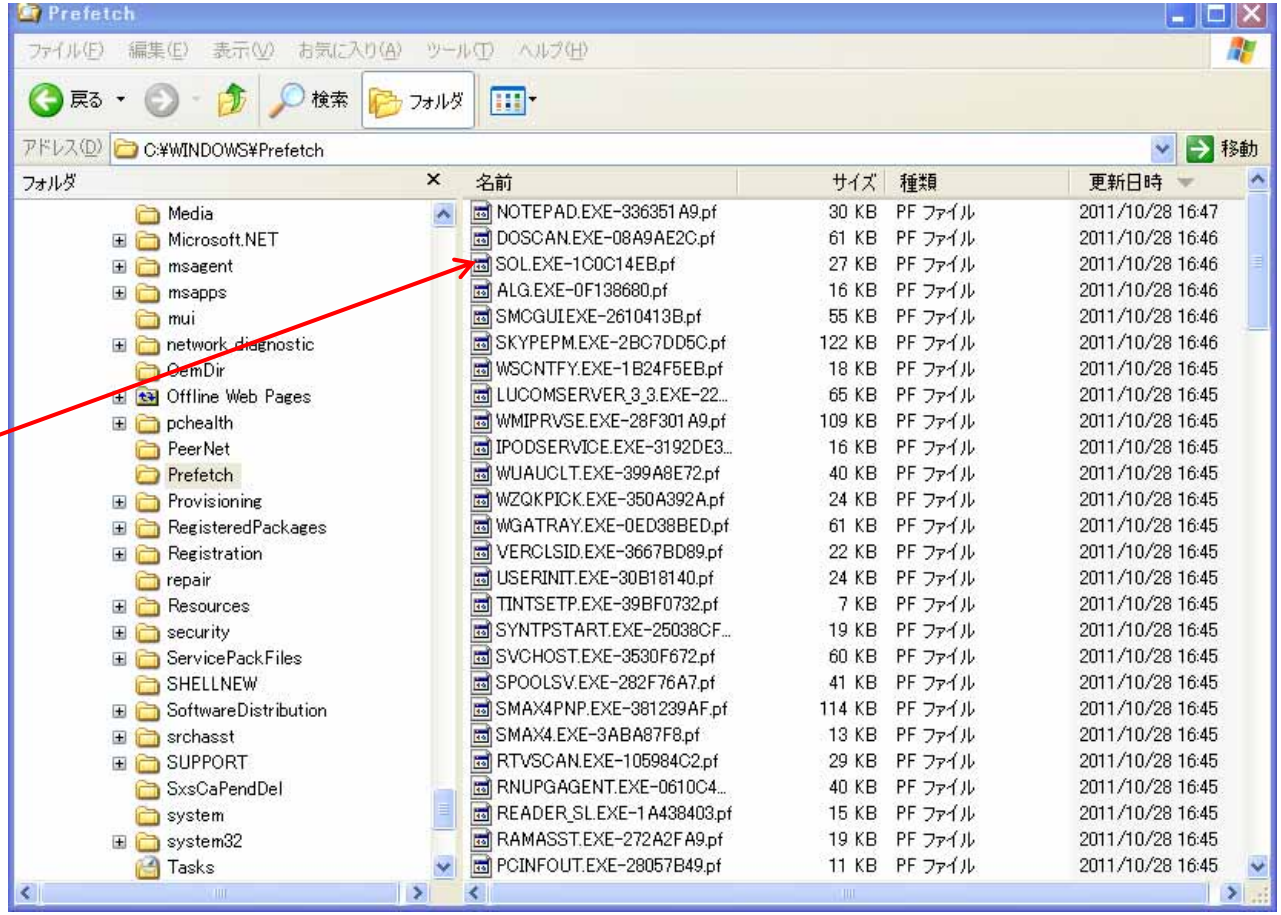
日経ＢＰ社『日経ＢＰデジタル大事典 2001-2002**年版』**

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

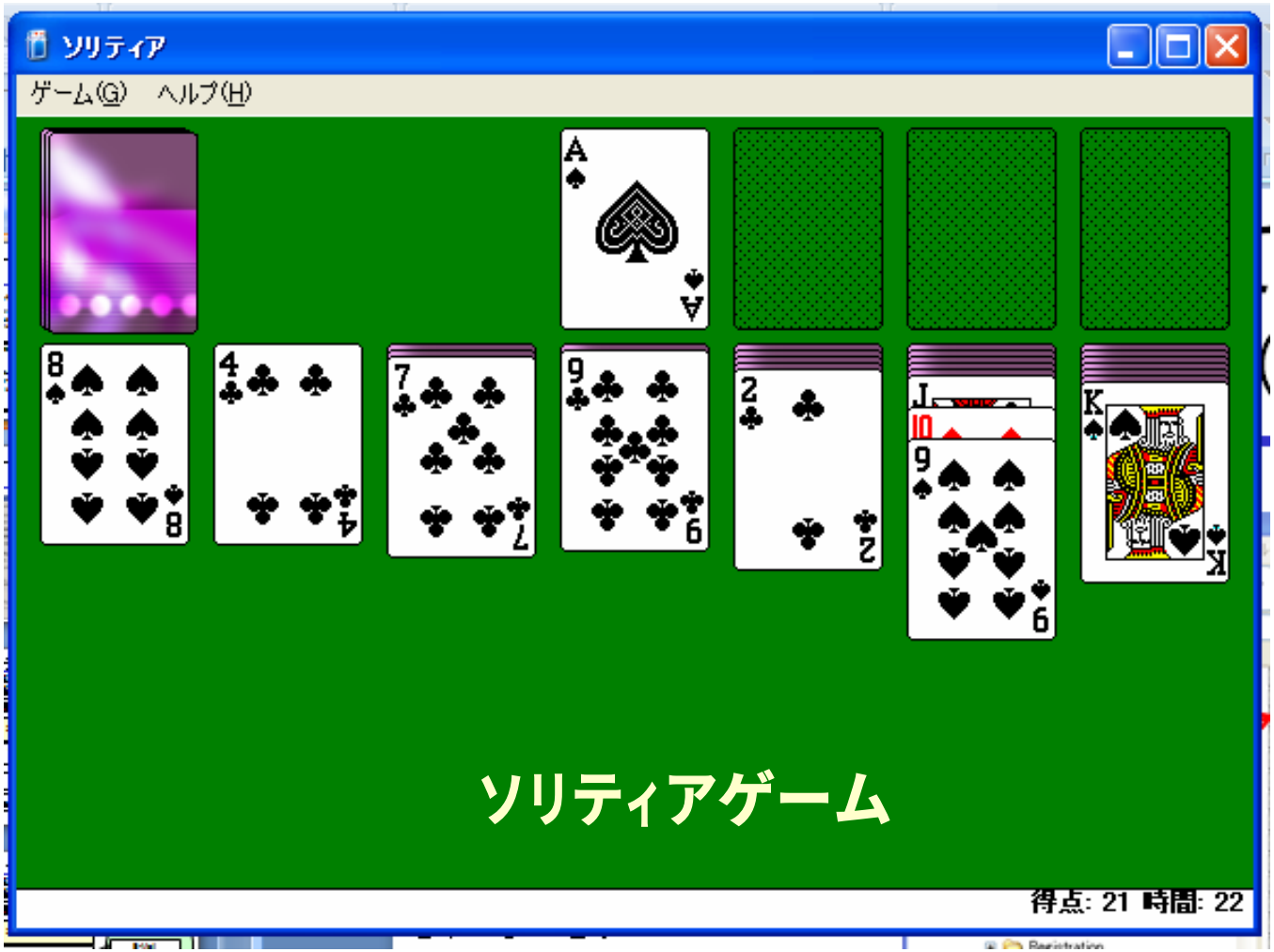
C:¥WINDOWS¥prefetch
を調べると最近使ったプログラムがわかる。

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**

sol.exeプログラムの実行



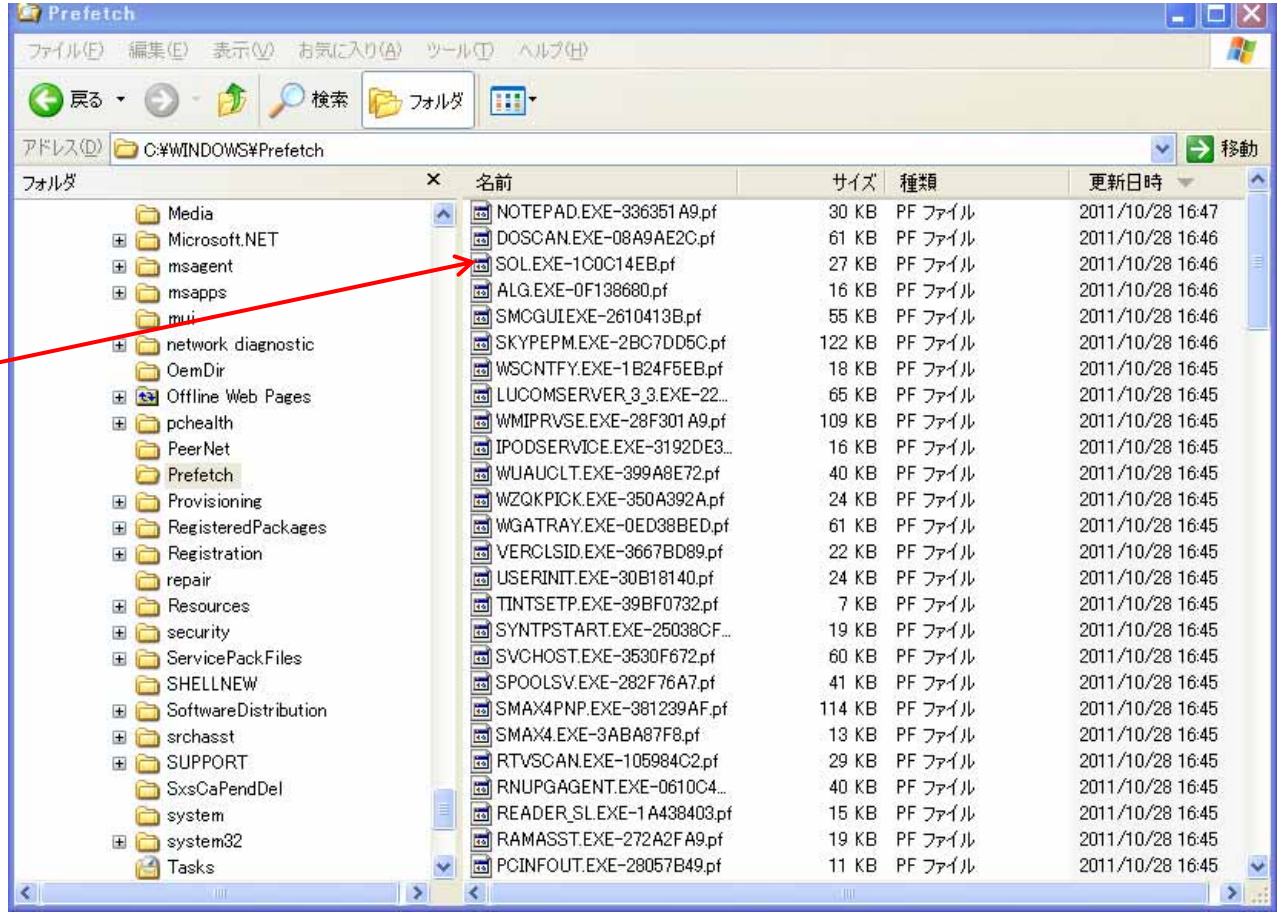
ツールを使わなくてもこんなことが分かる

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

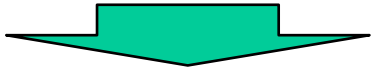


＜禁止されているWinnyなどを使っていたことなどもわかりえる。＞

目次

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

①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)

②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

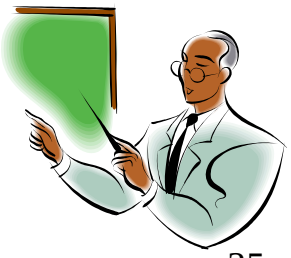
(1) 企業のシステムが不正を行えないようになっていることの規則作り　＝＞ポリシー作成

(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

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


END