

## 退職者による情報漏洩

### ケース1 IDF コミュニティ 2007

## 内部からの通報

### メーカーA社の内部通報

「競合Y社から出されている特許情報及び関連論文等を確認してみると、弊社（A社）が研究中の未発表の特許技術に関する内容が多々含まれていた。」

「専門家の判断では、それは偶然の産物や類似特許の類ではなく明らかにA社から漏洩された情報である事は明白であるとの結論が出された。（試薬の混合比や分留機器という選択肢が多数有り得る部分までそっくりであるのは絶対に有り得ないという）」

## 社内調査

「外部からのアクセスとか侵入、その他の情報漏洩（紙での流出やUSBメモリの紛失、盗難など）などあらゆる可能性を徹底的に調査・分析を行った。その結果浮かび上がったのは内部の人間による故意の情報漏洩の可能性であった。よってこの部分を更に調べた結果、漏洩された情報を知りえる関係者がこの3年以内に5名辞めている事が判った。（内、研究員以上の者は3名）この数字はA社の規模、研究テーマのプロジェクト規模、A社平均離職率などから勘案すると統計学的に極めて突出した異常値であった。」

- A社内部の現社員による本件（特許）関連の情報漏洩か？  
退職者であるならば、誰か？

## 社内調査

更に絞って調査を継続した結果、下記の事実が判明した。

- (1) 漏洩したと思われる技術の主要部分はM主任研究員、I研究員、S研究員の3名のチームからなるプロジェクトの成果物であった
- (2) 半年前にM主任研究員が、そして3ヶ月前には研究員が退職しており、現在ではS研究員とサポートとして新人と入社2、3年目の社員3名の合計5名でプロジェクトを支えている状況で、実質はS研究員が頼りというぎりぎりの作業環境であった
- (3) M主任研究員と研究員は、退職後しばらく経ってからライバルのY社に就職していた

## 社内調査

情報漏洩防止システム（ネットワーク・フォレンジック製品等）を先月から導入し稼働しており、S氏及び周辺の現社員のアクセス・挙動に関しては分析の結果、システム導入前後で変化がない事が判り、現社員からの漏洩の可能性は低いと判断された。

## 社内調査

退職したM主任研究員、I研究員が使用していたPCは社内に残っていることが分かった。

M主任研究員のPCは既に後任者が使用していたが、OS等の再インストールはされていなかった。I研究員のPCは未だ次の使用者が決まっておらず、退職時のままであった。

- M主任研究員、I研究員の使用PCのHDDのフォレンジック調査
- 退職時のデータサルバージ
- 情報のメディアへのコピー持ち出しやメール等での送付の疑いの調査

## フォレンジックとは？

フォレンジック(ス) = 科学捜査、鑑識  
 コンピュータ・フォレンジック(ス) = デジタルデータに対する科学捜査、鑑識

高度な科学技術を用いて法的に問題を解決する手段 =

ハイテク技術を用いた訴訟支援

証拠保全

解析

報告書作成・報告



調査対象コンピュータのHDDのデータを全く書き換えることなく、複製を作成して証拠保全を行う。



証拠保全したHDDのデータを解析して、調査対象コンピュータの使用者が何をしていたのかを特定・推測する。



解析した結果の報告書を作成、それを用いて報告を行う。

The Institute of Digital Forensics

7

## HDDデータ複製技術



調査対象コンピュータよりHDDを取出す。調査対象のHDDのデータを書き換えることなく、HDDの全領域を複製する。

調査対象コンピュータからHDDの取出しが困難である場合、証拠保全のソフトウェアをCDブートで起動する。そのため、調査対象のHDDのデータを書き換えることなく、複製を行うことができる。

The Institute of Digital Forensics

8

## 物理コピーの重要性

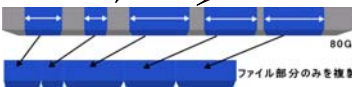
疑問

なぜ100%コピーが必要なの？

隠されたファイル

消去されたファイル

通常のコピーの場合



論理的に割り当てられている、ファイルやフォルダ情報などの部分のみコピーする

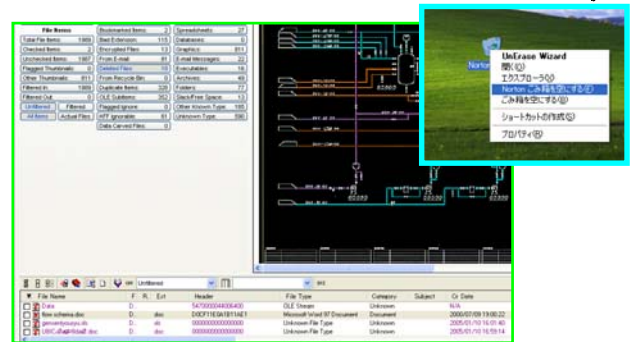
100%物理コピーの場合



全ての箇所を調査可能！

9

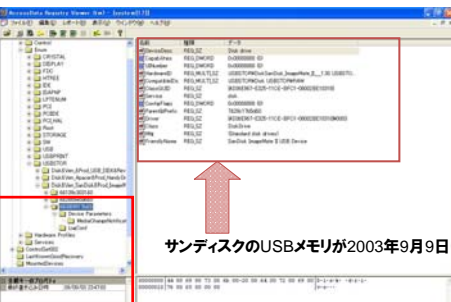
## 削除ファイルの復元



ゴミ箱から削除されたプラントの図面が復元された例

10

## 接続機器の履歴



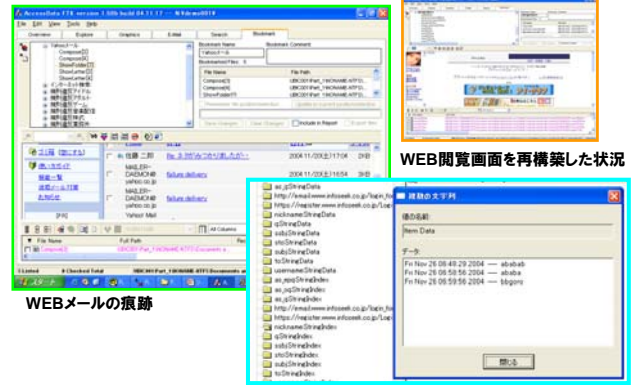
サンディスクのUSBメモリが2003年9月9日に接続された。

Windowsのレジストリファイル内に様々な接続機器の接続履歴が残っている

The Institute of Digital Forensics

11

## インターネット閲覧履歴



WEB閲覧画面を再構築した状況

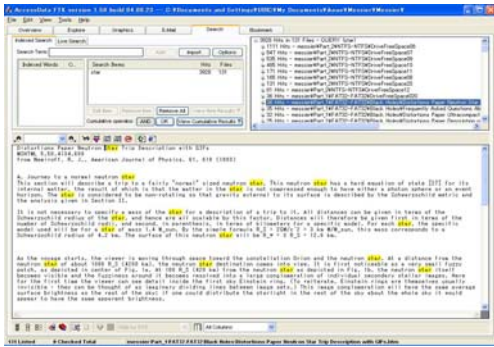
WEBメールの痕跡

ログインパスワード入力の痕跡<sub>2</sub>

The Institute of Digital Forensics

12

## キーワード検索



キーワードを含むデータを抽出 例(“まずい”・“極秘”・“秘”)

## 端末PCのコンピュータ フォレンジック調査

1. 退職したI研究員のPC内のデータを復旧したところ関連資料の形跡と外部機器へのLinkファイル等の履歴が、退職前1ヶ月の日付で見つかった。
2. レジストリに外付けDVD、HDDなどの会社から供与されていないデバイスの使用履歴見つかった。



## 端末PCのコンピュータ フォレンジック調査

3. 試薬名や混合比などの特徴的な文字列を用いた、キーワードサーチの結果、退職したI研究員のPC内のデータ内には、Web Mailの形跡あった。転職先の会社への情報提供内容と見られる文章が残されていた。
4. I研究員のPCに、パスワードを個人的に管理していた、ファイルが見つかった。その中にはM主任研究員が社内ネットワークのログオン時に使用していたパスワードが記載されていた。  
→ I研究員はM主任研究員のパスワード情報を知っていた。

## 調査結果

フォレンジック専門会社によるフォレンジック調査・解析の結果、該当情報は先に退職したM主任研究員が使用していたPCには無く、I研究員が退職前に研究データをサーバーよりコピーして外付けHDDに保存し、社外に持ち出した疑いが濃厚となった。  
また、それはM主任研究員のパスワードを研究員が知っており、M主任研究員のアカウントで必要情報を取得したことも判明した。

## 事後処理

- (1) 任意で(退職時の住所にまだ住んでいることの確認がとれたので、)I研究員に上記の調査結果を示してインタビューしたところ、証拠の列挙の前に言い繕うこともできず、重要情報を持ち出しそれをY社への再就職に活かしたことを話した。

## 事後処理

- (2) A社は、Y社に対して弁護士を通じて本件の処理に当たる旨を通知。  
事後、両社の法務部門を主体に、本件の処理が進められることとなった。
- (3) 社内においては、本件の調査結果を基に漏洩対策を強化することが決定された。