デジタル・フォレンジックによる情報漏えい調査

NPO デジタル・フォレンジック研究会　理事
株式会社 UBIC　代表取締役社長
守本　正宏

1. デジタル・フォレンジックの必要性

現代ではIT技術の発達によって情報がより高速に大量にかつ容易に保管･移送･書き換え･消去が可能になった。これに伴い、企業の業務形態も大きく変化している。設計・会計・各種管理簿から、プレゼン資料作成・業務連絡に至るまで、コンピュータを使用しないオフィス業務は考えられないと思えるほどに広くコンピュータが普及し、紙媒体で管理・運営してきた膨大な情報は、デジタルデータに変わり保管・管理しやすくなったほか、今まで郵送していた社内・社外への重要情報はインターネット環境を利用することにより、一瞬にして相手に送付できるようになり、効率良く且つスピーディーに業務ができるようになった。まさにIT社会の到来といえる。

一方、上記のような特徴に加えデジタルデータは目に見えない形で存在するため、そのリスク管理は容易ではなくなった。デジタルデータをどれほど正確にかつ安全に管理できるかが、その情報を持つ団体や個人にとっての重要課題になっている。そのため、デジタルデータを守るさまざまな情報セキュリティ技術が発達してきた。しかし、現実的にはデジタルデータを守ることは非常に困難であり、完全に情報を守ることは不可能であるといわざるを得ない。

その結果、情報の不正使用などは必ず発生するものであるという観点にたった対策が必要になってきた。これまで主流であった防御的なセキュリティ対策に加えて、情報漏えいなどのセキュリティインシデント発生後の対応策が必要になった。

また、IT社会においては発生する全ての犯罪は何らかの形でデジタル機器が関与しているといっても過言ではない。誹謗中傷や、不正会計、横領といったローテクな犯罪であっても、その証拠が何らかの形でコンピュータに残っている可能性が高くなっている。そのため、捜査機関ではコンピュータなどのデジタル機器は指紋と同様に優先的に取得すべき重要な証拠として位置づけされている。すなわち、デジタル機器が関与している犯罪はハッカーによるものだけでなく、さほどITの知識を有しない人々にまで広がっていった。

そのような中、ハイテク機器のデータを高度な技術を用いて証拠性を維持しつつ取得・解析を行い、法的問題を解決する手段であるデジタル･フォレンジックは危機管理という観点からにわかに脚光を浴びてきた。

また、同時に、サーベンスオクスリー法や新会社法など、企業コンプライアンスのための内部統制を義務づけた法律が出され、その具体的な手法としてのデジタル･フォレンジックの役割は重要である。

今回は、フィクションの情報漏えいの事件を例に取り、デジタル･フォレンジックの技術と運用方法を紹介する。

2. 今回の事例の背景（機密情報の漏えい）

対象者(鈴木一郎氏：仮名)はあるサービス業の大手企業Ａ社で､営業職に就いていた｡鈴木氏が退職して、同業他社Ｂ社に移った後に、Ａ社が所有する、ある地域の顧客情報がＢ社に漏れているらしいとのうわさが立った。不審に思ったＡ社は鈴木氏が使用していたコンピュータをデジタル・フォレンジック専門企業に依頼して調査することにした。Ａ社では退職者のうち、重要人物、および要注意人物のコンピュータデータを適時保全し、1年間保管することを規定していたので、迅速に調査を開始することが出来た。コンピュータのデータは使用時間とともに、記録が書き換わる可能性が高いので、対象者が使用していたという証明が困難になってしまう。そのため、事件が起きた場合、安易にコンピュータを操作したりせず、コンピュータ内のデータが書き換わらないように保つことが非常に重要である。

3. 証拠保全の重要性

法的証拠能力を持たせたまま、証拠データを確保

する作業を証拠保全という。具体的には対象者のコンピュータのHDD：ハードディスクドライブ(保全元)に保存されているデータを別に用意した保全用HDD(保全先)に複製(物理コピー)を行なう。そこで重要になるポイントは主に保全元のデータと保全先のデータが書き換えないように複製すること及びその同一性を証明することの2つに絞られる。

証拠保全時における複製は必ず物理的複製が必要となる。物理的複製とはデータが格納されている部分だけの複製ではなく、セクター毎にHDDの全領域に対して複製を実施する。表面的にはデータが格納されていない箇所に、故意に容疑者がデータを隠蔽している可能性や、消去されたデータ等が存在している可能性があり、証拠となる重要データがその部分に隠されている可能性が高いからである。(図1)

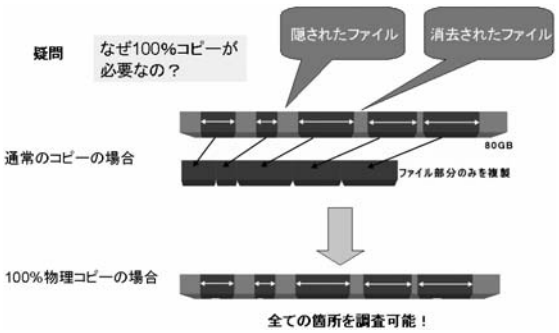


図1　物理的複製(コピー)の重要性

今回の作業では、A社では平時よりデジタル・フォレンジックの専門化により、物理コピーが実施されていたので、HDDの全ての領域に対して、退職時の状況が保存されたまま、調査を実施することが出来た。

4. 解析(コンピュータ端末調査作業)の実施

解析を実施する場合には、証拠保全して得た証拠データを直接解析することは禁じられている。それは直接解析することによって誤ってデータを破壊することを防ぐためである。

解析実施時はまず、証拠保全したデータを解析専用データ形式に変換する。変換後に専用ソフトウェアにてデータの解析を行なう。専用ソフトを使用することによってデータ領域を分けている部分へのアクセスや、消去されたデータあるいは、レジストリ保護領域へのアクセス等、通常Windows上で制限がかかっている領域での作業が可能となる。また、コンピュータ内の全ファイルを形式ごとに分類し、調査を容易に出来るようにしている。(図2参照)

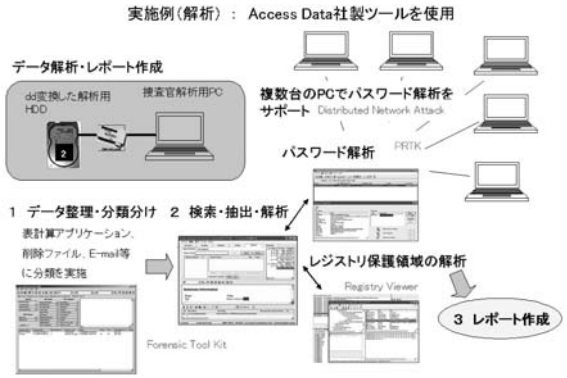


図2　解析工程

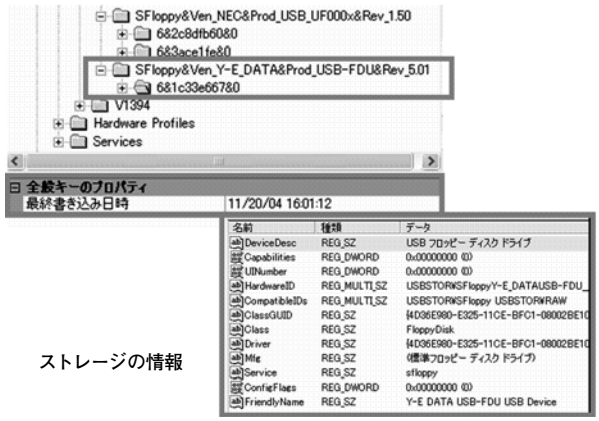
今回、機密情報の漏えいが考えられたので、ファイルのダウンロードが行われたかをレジストリ領域を調査したところ、実際の業務には必要のない地域の顧客情報ファイルを退職直前にダウンロードしていることを突き止めた。

最終書き込み日時	11/29/04 10:48:18
クラス名	Shell

名前	種類	データ
MRUList	REG_SZ	dcbajihgfe
d	REG_SZ	\\File-server\SEER\玉川店顧客情報\顧客名簿世田谷区.xls
c	REG_SZ	C:\Documents and Settings\Administrator\My Documents\SecurityADatabase\inous_waka_05.jpg
b	REG_SZ	C:\Documents and Settings\Administrator\My Documents\SecurityADatabase\images.jpg
a	REG_SZ	C:\Documents and Settings\Administrator\My Documents\SecurityADatabase\00040170.jpg
j	REG_SZ	C:\Documents and Settings\Administrator\My Documents\SecurityADatabase\480_663.jpg
i	REG_SZ	C:\Documents and Settings\Administrator\My Documents\SecurityADatabase\kasuma_530_02.jpg
h	REG_SZ	C:\download\総務資料\顧客名簿世田谷区.xls
g	REG_SZ	C:\download\総務資料\わか\.jpg
f	REG_SZ	C:\download\総務資料\item_4.jpg
e	REG_SZ	C:\CCIS\db\create.sql

図3　NTUSER.DAT ／ OpenSaveMRU レジストリ

次に情報が漏えいした経路の調査を行った。まず、USBメモリ等の外部接続機器の履歴を確認した。(図4)　比較的多い情報の持ち出し手法はこういった外部メディアを使用したものである。しかし、今回は外部メディアへデータをコピーした形跡は発見できなかった。



ストレージの情報

図4　外部メディア接続情報の表示

次に、HDDに残るEメールデータの調査を行った結果、WEBメール(Yahooメール)にて社内の機密情報を売買する内容のやりとりを行っている事が判明した。送信相手は　“佐藤二郎＜sato_jiro@yahoo.co.jp>（仮名）で、11月20日から26日の間にかけて複数回データの売買に関する連絡をとっていた。社内サーバーからダウンロードした「顧客情報世田谷区.xls」ファイルをメールに添付し、11月22日の10:08に佐藤二郎宛てに送信していたことが判明した。このように、デジタル・フォレンジック解析ソフトウェアにより、Internetの閲覧画面の再構成や復元が容易に可能になる。

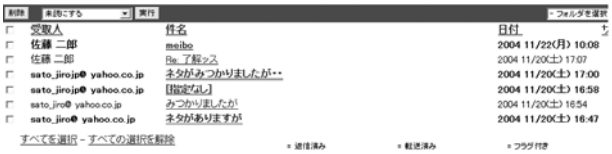


図5　Webメール:送信済みフォルダ(再構成)

図6　Webメール:メールの画面(再構成)

図7　Webメール:名簿の送信画面(再構成)

次に、鈴木氏の就業中の態度を調査する為に、Internetの閲覧履歴を確認したところ、オンライントレードサイトにアクセスしており、業務とは関係ないホームページを閲覧していたことが判明した。
◆11月25日にアクセスした履歴があった。

File Name	Full Path	Acc Date
ad[1].htm	M:¥NONAME-NTFS¥Documents and Settings¥Administrator¥Local Settings¥Temporary Internet Files¥Content.IE5¥QLMN61KL¥ad[1].htm	2004/11/25 15:05

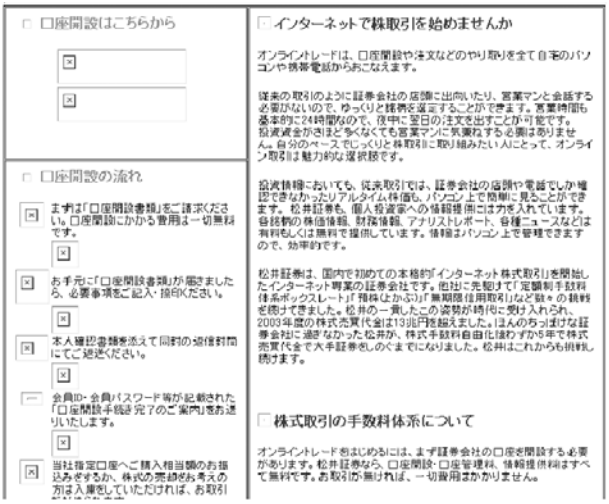


図8　オンライントレードサイト

5. 結論

対象者(鈴木一郎氏)は、退職前に社内の機密情報をダウンロードし、不正に外部へ持ち出しており、更には、就業時間中に業務とは関係ないホームページにアクセスしていたことも判明した。

ここでは、データを不正に流出させた証拠だけでなく、就業時間中に業務外のホームページの閲覧記録なども証拠としてあげている。これらの記録は、あまり問題にはならないように思えるが、実は訴訟になった場合は、裁判官の心証に与える影響は大きく、実際の事件においては貴重な証拠として採用されることがあるので軽視できない。

このように今まで困難であったコンピュータを利用した不正の証明を法廷でも利用できるような技術的手法(デジタル・フォレンジック)を用いて行うことが可能になった。

この事件ではInternetの閲覧履歴の調査を中心に記述したが、その他にも数多くのデジタル・フォレンジック調査技術・手法があり、さまざまなケースの調査を可能にしている。

現在、企業においてはその書類の90%以上がデジタル化されていると言われている。デジタル・フォレンジック調査体制の整備が、企業の危機管理体制における重要な鍵となることは疑い得ない。

6. おわりに

今回はデジタル・フォレンジックを不正調査で利用した例を紹介したが、デジタル・フォレンジックの最も記すべき特色は、開示する情報に関して訴訟にまで耐えうるほどのIntegrity（正当性)を維持していることである。ここ数年、わが国において企業コンプライアンスの重要性が叫ばれ、内部統制がキーワードになってきている。金融商品取引法(日本版SOX法)や会社法などの法整備も進んできている。時代はまさに企業や組織の信頼性を求めている。信頼性は正しい情報開示から生まれるといっても過言ではないだろう。そのためにデジタル・フォレンジックの重要性はますます高まっており、いまや普及・啓蒙からすでに実用化のフェーズに移行しているといえる。NPOデジタル・フォレンジック研究会では、そのような時代の要請に応え、“J-SOX時代のデジタル・フォレンジック”と題して第3回デジタル・フォレンジックコミュニティ 2006を12月18日、19日の2日間にわたり、グランドヒル市ヶ谷で開催した。そこでは各方面の専門家を招き、技術、法律、経営・監査の各分野から企業・組織における信頼性確保のためのデジタル・フォレンジックの実用化に関して提言している。J-SOX法対応に関して、企業・組織に具体的な指針を示す貴重な機会になったのではないかと考える。この場をお借りして紹介させていただきたい。もしご興味があり、レジュメ集(有料)をご希望される方は、NPOデジタルフォレンジック研究会事務局(ウェブサイト www.digitalforensic.jp)にお問い合わせ願いたい。