

2006 年度卒業論文
山田正雄ゼミナール

デジタル・フォレンジックの可能性

日本大学法学部 法律学科 4年

学籍番号 : 0310290

鎗田かおる

はじめに

コンピュータ社会の進展に伴いインターネット、携帯電話、電子メールなどがコミュニケーションツールとして爆発的に普及し情報はデジタル化していった。しかし、利便性が飛躍的に向上している影でコンピュータやネットワークを利用した犯罪は劇的に増加している。これらの犯罪を捜査していく上で重要になってきたのが不可視であるデジタルデータである。従来の可視性のある書類等と違い、デジタルデータを確保・分析するためには専門知識・スキルが必要になってくる。このような状況から、デジタルデータの証拠性を確保し、訴訟などに備えるための技術、社会的仕組みである「デジタル・フォレンジック」が注目されてきている。

また、注目されたもう一つの要因として企業の内部統制強化が重要視されてきたことがあげられる。2002年に発生したエンロンの不正会計事件やワールドコムなどの粉飾決算が起こった際、電話の通話記録の解析などに「デジタル・フォレンジック」の技術が利用された。これらの事件により投資家などは企業の財務報告に対しきわめて高い不信感を持ったため、投資家の米国資本市場に対する信頼を取り戻すために上場企業に対して厳しいコンプライアンス体制の整備を求めたための SOX 法が作られた。ここでのデジタル・フォレンジックは証拠などに使用する“事後対応”だけでなく、事件発生の予兆発見や抑止効果など“事前対応”機能として活用しようとする試みである。またアメリカは訴訟社会であり訴訟が起こった場合に企業の潔白を証明するために普段から電子的な証拠を正確に、いつでも納得のいく説明ができるように、きちんと保全しておく方法として活用されている。

日本ではまだ「デジタル・フォレンジック」という言葉への馴染みは薄いですが、2005年に施行された個人情報保護法や、2008年度制定予定の日本版 SOX 法により企業は内部不正の防止、個人情報漏洩・管理対策をしていくためにより厳しい内部統制システムの構築を強いられることになる。これらの場合に有効な手段として日本でも「デジタル・フォレンジック」が注目されはじめています。捜査のためのデジタル・フォレンジックだけでなく、企業としてデジタル・フォレンジックを理解し導入していくことにより犯罪を未然に防いだり、事件が起こった場合にも迅速に対応できることができるであろう。この論文ではデジタル・フォレンジックを利用することにより捜査機関・企業・国がどのような利潤を得られるかについて述べていきたい。

- 目次 -

はじめに	1
1 デジタル・フォレンジック	3
1.1 証拠	3
1.2 デジタルデータ	3
1.2.1 デジタルデータとは	4
1.2.2 デジタルデータの特徴	5
1.2.3 デジタルデータの問題点	5
1.3 デジタル・フォレンジックとは	6
1.3.1 デジタル・フォレンジックの定義	7
1.3.2 デジタル・フォレンジックの歴史	8
1.3.3 デジタル・フォレンジックが注目された背景	9
1.3.4 デジタル・フォレンジックと法	10
1.3.5 デジタル・フォレンジックの分類	12
1.3.6 デジタル・フォレンジックに使用される技術	12
2 事件後のデジタル・フォレンジックの利用	14
2.1 デジタル・フォレンジック活用	14
2.2 利用する主体	14
2.3 手順	14
2.3.1 コンピュータ捜査の準備	14
2.3.1.1 法執行機関の捜査の準備	14
2.3.1.2 民間の捜査の準備	15
2.3.2 捜査の実行	15
2.4 事例	16
2.5 課題	17
3 事件前のデジタル・フォレンジック	18
3.1 活用	18
3.2 利用する主体	18
3.3 導入する利点	19
3.4 システム例	19
3.5 課題	20
4 デジタル・フォレンジックの普及対策	20
4.1 国のデジタル・フォレンジック普及への取り組み	20
5 デジタル・フォレンジックの今後の展望	21

参考文献

1 デジタル・フォレンジック

1.1 証拠

証拠とは真実・事実であることを明らかにするよりどころとなる事や物である。訴訟法上、判決の基礎たる事実の存否につき裁判官の判断の根拠となる資料のことをいう。証拠は大別して人証と物証に分けられる。人証は、裁判で人の供述内容を証拠とする物であり、物証とは、物的証拠を意味する。

日本の訴訟は民事訴訟と刑事訴訟の二つに分けられるがそれぞれにおいて証拠の位置づけ、証拠能力は異なる。日本では訴訟法上自由心証主義を採用しており、自由心証主義とは訴訟法上の概念で、事実認定・証拠評価について証拠方法を制限せず、証拠力も法定せず、裁判官の自由な判断に委ねることをいう。民事訴訟法では247条で、刑事訴訟法では318条においてこれを定めている。しかし刑事訴訟法では317条において事実の認定は証拠による旨の明文があり、厳格な証明の対象となる事実については、証拠能力を備えた証拠について法定の証拠調べ手続きを踏まなければならない。

また、刑事訴訟法では基本的に伝聞証拠は証拠とすることができないとする伝聞証拠禁止の原則と、どんなに価値のある証拠（証明力が高い証拠）でも、違法な手段で入手した証拠など、形式的に証拠能力のないものは事実認定の基礎とすることはできない違法収集証拠排除法則がある。

これに対し、民事訴訟では証拠能力を限定していない。

1.2 デジタルデータ

1.2.1 デジタルデータとは

デジタルデータとは「電子的方式、磁氣的方式その他人の知覚によっては認識することができない方式で作られる記録であって、電子計算機による情報処理の用に供されるもの」と定義する。

ただし、法律におけるデジタルデータとは媒体そのものを指しているのではなく、一般にいう電子データが一定の記録媒体上に情報として使用でき得る状態に記録・保存されたものをいう。従って、FD、CD-R、磁気テープ、DVD等の磁気媒体等に情報として使用できるように記録保存された状態にあるものを指す。

デジタル・フォレンジックにおけるデジタルデータは捜査の情報であり、証拠である。主に以下の情報処理機器から押収することが可能である。

- ① パソコン
- ② サーバ
- ③ ネットワーク機器
- ④ 携帯電話
- ① 情報家電

1.2.2 デジタルデータの特徴

【図 1-1】

	紙媒体、紙に書かれた情報	電子媒体、電子的な情報
複製	複製を繰り返すと劣化する	劣化せず複製可
修正	困難	容易
可視性	物理的に存在(確認が容易)	電子的に存在(確認にアプリケーション等が必要)
送受信	郵便物等を利用(電子的送受信に比べて少し面倒)	電子メール、その他のプロトコルを使用(簡単)
情報の蓄積・保存	紙の物理的容量分のスペースが必要(長期の保存が可)	小型の媒体に大量の情報を蓄積可(長期の保存は不明)

デジタルデータは紙記録と違い、デジタルデータはコンピュータを解してディスプレイに表示したりプリンタに出力しないと読むことができない。この人間が可視・可読できるかが証拠能力として重要な点である。そのため、デジタルデータはデジタル記録媒体に記録された有体物のものだけが証拠として認められる。デジタル記録媒体にあたるものが紙記録では「紙」であり、記録された状態にあるものを「文書」になる。

1.2.3 デジタルデータの問題

デジタルデータの問題の一つとしてデジタルデータの証拠能力の有無があげられる。日本では証拠は有体物（物理的存在）であることが前提とされている。それは、日本の主要な法律の大半が半世紀以上前に作られたものであり、電子記録を想定していなかったためである。そこで我が国では、カード等の犯罪増加から昭和 62 年の刑法一部改正により、コンピュータ犯罪に対する法的規制が図られた。その結果、電磁的記録を定義した 7 条の 2、電磁的記録不正作出及び供用罪(161 の 2)、電子計算機損壊等業務妨害罪(234 条の 2)、電子計算機使用詐欺罪(246 の 2)が新設された。

また、昭和 62 年の刑法一部改正の際に定められなかった不正アクセスについては、平成 11 年に不正アクセス禁止法が制定された。

様々な法律が制定され、判例でもログが証拠として認められるようになってきた。デジタルデータと言っても、アナログ社会の文書情報が性質や媒体からデジタル化したにすぎないからであるというのが総論だからである。実務では FD、CD、DVD やプリントアウトして証拠化しなければならない。

また民事訴訟法は平成八年に全面改正され、電子媒体記録を「準文書」として扱われるとともに、そのプリントアウトを「文書」として扱うことができる。

1.3 デジタル・フォレンジックとは

1.3.1 デジタル・フォレンジックの定義

デジタル・フォレンジックとは「デジタルデータの証拠性確保の技術と手順」と定義する。

フォレンジック (forensic) とは、一般的に「法廷の～」 「法医学の～」 といった言葉を指す形容詞で、フォレンジックスという名詞になると、「鑑識課」「科学捜査」などの意味を持つ。簡単にいえば、実際の事件現場で指紋採取などの物的証拠を集めるための鑑識の役割を果たすものである。つまりデジタル・フォレンジックとは、過去に発生した事象の証拠保全・不正アクセスの追跡を行う手段であり、事件が発生した後の「証拠保全」「解析」「証拠提出」の機能を持ち合わせているものである。(図 1-2)

【図 1-2】



デジタルフォレンジック基盤が、事件発生時の調査基盤と、
監査ログ取得による情報漏洩の抑止効果を提供。

出典：キーマンズネット

『デジタル・フォレンジックに必要な証拠保全・解析・証拠提出』

デジタル・フォレンジックは大きく二つに分類することができる。

(1) 犯罪や法的紛争が生じた際に、原因究明や捜査に必要な機器やデータ、電子的記録を 収集・分析しその法的な証拠性を明らかにする手段としてのデジタル・フォレンジック

(2) コピーや消去、改ざんが容易であるという電子データの性質に対応して、データが捏造されたものかどうかを検証する技術や、記録の段階でデータが改ざんできないよう工夫したりハッシュ値やデジタル署名などで同一性を保全する技術。定期的にフォレンジックを用いた監査を行う事により、不正行為の発生を抑制するとともに発生後の対応を迅速に行えるようにする。

コンピュータはネットワークハイジャック、アカウントハイジャック、ハッキング、クラッキング、スパイ活動、データ流出、ウイルス攻撃などの特別なハッカーにのみ使用されるツールであるだけではなく、窃盗、詐欺、横領、麻薬、婦女暴行、強盗、子どもの虐待、テロ及び殺人のような犯罪においても使用されている。

デジタル・フォレンジックが他の技術と異なり複雑な点は、その領域の広さにある。法学的な要素、会計学的な要素、そしてコンピュータ技術についてはハードウェアメーカー並のハードディスクやメモリの実装技術、理論構造、ソフトウェアではネットワーク技術、OSの理論構造などがあってこれらの集大成としてデジタル・フォレンジックが成り立っている。

似たような言葉としてコンピュータ・フォレンジックがある。コンピュータ・フォレンジックとは“Computer forensics is the application of science and application to the legal problem of digital evidence. It is a synthesis of science and Law.”とFBIのMarkPollittが定義している。「計算機科学などを利用して、デジタルの世界の証拠性(evidence)を確保し、法的問題の解決を図る手段。ログの改ざん、破壊等、これまでの手法では証拠を検出することが困難な被害を受けたコンピュータに対しても、高度なツールによってコンピュータ内のデータを調査・分析することにより、不正アクセスの追跡を行う手段を含む」コンピュータ・フォレンジックとデジタル・フォレンジックの違いはコンピュータ内のデータだけでなく、ネットワーク上や、携帯電話、情報家電内などのデータも積極的に扱おうというのが、デジタル・フォレンジックである。

1.3.2 デジタル・フォレンジックの歴史

デジタル・フォレンジックの歴史はコンピュータの歴史とともに変遷してきた。ここでは、コンピュータの歴史とともに、日本だけでなく世界のデジタル・フォレンジックの歴史について書いていきたい。

コンピュータの歴史は1940年までさかのぼり、最初は大学や軍関係などごく限定されていたが、1950年代になると商用化がなされ、1960年代の終わりごろにはコンピュータは現在求められているような機能を備えるようになった。すなわち

- ・複数の人間が一台のコンピュータを使う際に互いが競合しないようにする技術
- ・コンピュータの設定変更をともなう操作を管理者以外ができないようにする技術

この2つは資源保護技術と呼ばれ、現在のアクセス制御技術の基礎になっている。しかしセキュリティに関する認識は低く、重要視されていなかった。

1970年代に入ると汎用大型コンピュータが普及して多くのコンピュータは高等教育を受けた専門家の独占的なグループによって利用された。利用者は、銀行、工学技術、大学部門で働く人々であった。そして同時に電子犯罪も金融部門において増え始めた。これらの産業でコンピュータデータを操作することによりお金を稼ぐ方法が明らかになったときから、ホワイトカラーの犯罪が発生したのである。しかし、犯罪が行われても法執行機関のほとんどは、コンピュータについて、裁判で適切な答弁を行ったり、証拠を保存するための十分な知識を持たなかった。そこで、法執行機関を対象にデジタルデータの復旧の訓練を目的で設立されたアメリカのFLETC (Federal Law Enforcement Training Center) に多くが参加した。

1980年代に入ると汎用大型機から中型機、小型機へと移行していった。1981年にIBMによるIBM-PCが発売される。これは現在のWindowsの原型と言われ他にも数多くのOSが誕生した。またUNIXワークステーションの普及とともに組織内でネットワークを構成するLANという考え方が広まり、1つのコンピュータを多数のユーザが使う集中型から、多数のコンピュータをLANで接続して互いに通信しあう分散型に変化していった。1983年にTCP/IPが開発され、インターネットに採用され、コンピュータ通信のオープン化が実現した。このころからコンピュータ犯罪が次第に認知されるようになった。1980年代半ばに、X-Tree Goldという新しいツールが誕生した。これはファイルの種類を認識して、失われたり削除されたファイルを取得するツールであった。また、Norton Disk Editがこれに続き、削除されたファイルを検索するいちばんのツールとなった。この頃のフォレンジックツールは、DOSベースのものが主流である。コンピュータのファイル数も一万ファイル以下のものが多く、現在と比較して調査・解析が容易であり、暗号読解も同様に容易であった。1989年には、北テキサス大学にてコンピュータ・フォレンジックスペシャリストのプログラムがスタートした。このプログラムは後に連邦法執行機関訓練センターIACIS (International Association of Computer Investigative Specialists) に移行された。

1990年代初頭にインターネットの商用化がはじまるとともに、WWW技術が確立し、爆発的に普及し始めインターネットを介して感染するコンピュータウイルスが目立つようになった。1990年までのコンピュータ記憶容量は非常に限られており、デジタルデータの主な保存場所は3.5インチや5インチのフロッピーディスクであり、ハードディスクの容量も100MB以下の非常に小さいものであった。ほとんどのフォレンジック調査は一つの捜査案件の中で1台のパソコンの調査をすれば結果は得られた。また、この頃からフォレンジック調査の必要性がさらに高まり、FBI、FLETC、IACISによる米国の各法執行機関においてコンピュータ・フォレンジックスペシャリストの育成をするためのトレーニングが行われるようになった。1991年にはIACISがオレゴン州のポートランドにて最初のデジタル・フォレンジックに関する会合が開かれた。

1990年の半ばから急速にハードディスクの容量が増大していった。そして OS は Windows95 や Windows98 が主流になっていった。大容量ハードディスクの導入により、デジタル・フォレンジックの捜査において新たな問題が発生する。当時の DOS ベースのソフトウェアの多くは 8GB 以上のハードディスクを認識しなかったのである。多くの場合、1つのケースで複数台のパソコン調査が必要になり、平均の調査対象ファイル数は最高 10 万ファイル以上になった。この頃になるとコンピュータ・フォレンジックツールやコンピュータ・フォレンジックトレーニングに対する関心が国際的に高まりだしていった。

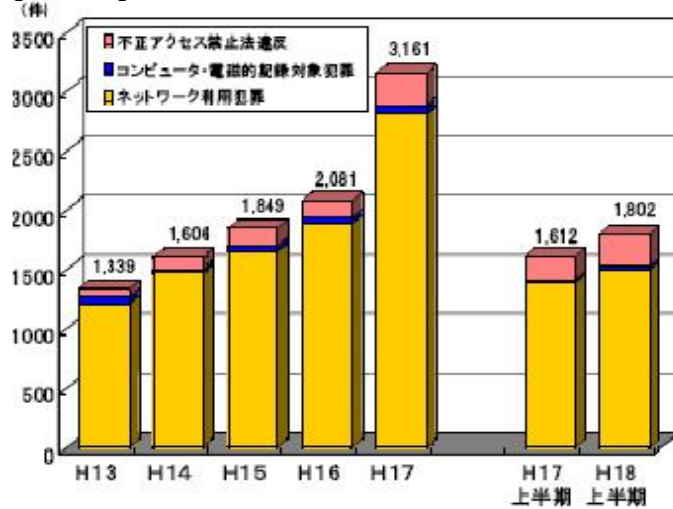
また、マイクロソフトがオフィス製品に 40 ビットの暗号化機能を付加させたものを市場に投入したため、1つのファイルの読解に数ヶ月も費やす場合が出てきた。そのため暗号読解に使用されたのが分散コンピューティングを利用した読解方法である。分散コンピューティングを利用した解読ツールを使用することによって、56 ビットの暗号も解読することが可能となった。このようなツールはインターネットに接続された 150 万台のアイドル中の CPU の力を利用した分散コンピューティングを採用している。

2000 年台になるとハードディスクの容量はさらに増大し、平均的にその容量は 40GB から 100GB になる。この頃になると、多くのケースにおいて複数のパソコンを調査することが普通になり、ときには 50 万台以上のパソコンで合計数 TB のデータを調査する場合もあった。大容量データの調査に対応するため、一旦データにインデックスを付けてデータベースを作成する方式のフォレンジックツールが開発された。この場合、ハードディスク内の大量のデータにいったんインデックスを付けてデータベース化しているため、表計算アプリケーションやワープロ用アプリケーションなどのファイル形式毎の分類や削除ファイルや暗号化されたファイルなどのカテゴリ毎の分類、および語句に対する分類が可能になった。このようにインデックスを付けてデータベースを作成してから行うキーワード検索をインデックスサーチと呼ぶ。

2000 年にはアメリカ政府が暗号化技術を非軍事目的に転用することを許可し、128 ビットの暗号化技術を利用した製品が多くの技術で開発された。そのため、総当たり攻撃による暗号読解は現実劇には不可能となったのである。結果として暗号読解には辞書攻撃に加え高度なプロファイリングを利用した解読手法が使用されるようになった。同時に分散コンピューティングは必要不可欠な技術となる。

1.3.3 デジタル・フォレンジックが注目された背景

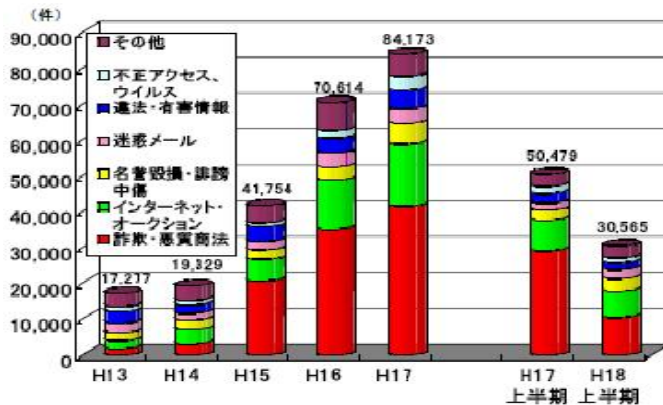
【図 1-3】



出典：統計調査データ

『サイバー犯罪の検挙件数』

【図 1-4】



出典：統計調査データ

『サイバー犯罪等に関する相談状況』

1960年代後半からパソコンが利用されはじめ、文書帳簿をフロッピーでつけるようになり、パソコン通信が一般家庭に浸透して行くにつれてデジタルデータを利用した犯罪は増えていった。それに合わせデジタル・フォレンジックが重要になっていった。ただし、殺人など一見関係ないように思える犯罪でもデジタル・フォレンジックは行われている。携帯電話やパソコンから証拠を探すためである。日本ではここ10年ぐらい捜査機関において普及していたが、海外では特にヨーロッパでは80年代から進んでデジタル・フォレンジックが行われてきた。これはスパイ技術が応用されていたためである。

②企業におけるコンプライアンスの重要性（訴訟の増加）

刑事の分野では1990年代の半ば頃からデジタル・フォレンジックは始まって

いたが、内部統制や民事訴訟の分野でその重要性が認識され始めたのは、この分野の先進国アメリカでも 2000 年以降である。発端としては冒頭で述べたようにエンロン、ワールドコムの不祥事である。現在のアメリカの大企業や監査法人はフォレンジック専門のチームが編成されているほどで、裁判においてもデジタル・フォレンジックで作成された証拠資料が実際に使われている。

これらの波が数年遅れであるが日本にやってくる。日本においても、従来は考えられなかったような場合にも訴訟が行われるようになってきた。また、個人情報保護法の施行や、企業に対するコンプライアンスや財務の信頼性向上の要求を高める日本版 SOX 法、内部統制システム構築の義務化を明言している新会社法（2006 年 5 月施行）の状況から、デジタルデータの証拠性を確保し、訴訟などに備えるための技術や社会的仕組みであるデジタル・フォレンジックが重要性を増してきた。

1.3.4 デジタル・フォレンジックと法

法律や裁判の世界においてデジタル・フォレンジックという言葉が使われだしたのはつい最近であり、様々な問題があった。ここでは、事件の判例からどのように法が新たな技術・事件に対応するために解釈、改正されていったか、また情報の法的保護のために制定されたいくつかの法律についてまとめていきたい。

(1) 1980 年代

1980 年代に入ると業務用ネットワーク関連の事件が起ころはじめた。その中心は金融機関の内部者のオンライン不正使用事件とカード不正使用事件であった。

1981(昭和 56)年に「三和銀行オンライン詐欺事件」が起きた。銀行の女子行員が、同行の他支店に架空人名義の普通預金口座を開設の上、オンラインシステム端末機を操作して右預金通帳お預り欄に振替入金があり、これを同支店が代受けしたように偽りの記帳をし、同時に入金データを入力して、預金払戻請求書と偽りの記帳をした預金通帳を窓口係員に提出し、払戻請求の金額が実際に入金されているものと誤信させ、預金払戻の名目で現金等を騙取した事案である。この事件のような架空入金データの入力行為自体は、人を欺罔するものではないので詐欺罪の対象とならない。刑法は従来有体物を基礎に体系化されており、そのまま適用することが困難な局面が生じたのである。このような事件がいくつか起ころ、1987(昭和 62)年に刑法が一部改正され、コンピュータ犯罪に関する条項がいくつか追加された。これは国際的に見てもかなり早いほうであった。「電磁的記録不正作出罪」(刑法 161 条の 2)「電子計算機損壊等業務妨害」(同 234 条の 2)「電子計算機使用詐欺罪」(同 246 条の 2)そして、公文書・私文書の毀棄罪へ

の電磁的記録の追加(同 258 条、同 259 条)である。電子計算機損壊等業務妨害罪は、高度情報化社会の到来に伴い、業務処理におけるコンピュータへの依存が飛躍的に増大したため、コンピュータシステムの損壊等が業務の遂行を阻害する度合いが深刻になり、コンピュータに対する対物的加害行為を類型化したものである。したがって本罪の保護法益は、電子計算機による業務の円滑な遂行であって、情報処理それ自体、情報処理の対象となるデータや情報セキュリティではない。

(2) 1990 年～2000 年

不正アクセスによる web ページ改竄事件が 1990 年代半ばに起こる。しかし、事件判決時にはまだ「不正アクセス禁止法」は制定されておらず、電子計算機損壊等業務妨害罪のみの成立となっている。しかし、Web ページの改竄に電子計算機損壊等業務妨害罪の適用を認めた判例はこれ以前には存在せず、その点では意味のある判例である。

1998 (平成 18) 年、日本のインターネットに関する差し押さえ事件判例として有名な「ベッコアメ顧客データ差押え準抗告事件」が起こる。1982 年に福岡簡易裁判所より出された捜査差押許可上に基づいて警察庁によって都内で差し押さえられた顧客データの入ったフロッピーディスクに関して、インターネット接続業者 (ISP) 側から差押え取消の求め(準抗告)がなされ、裁判所が取消しを認めたという事例である。裁判所は、「本件会社は、本件被疑事実の被疑者ではない上、利用者のプライバシー保護が強く要求される電気通信事業法上の特別第二種電気通信事業者であるから、本件会社に対する捜査差押の適法性を判断するに当たっては、捜査差押の必要性と並んで利用者のプライバシー保護を十分に考慮する必要がある」として、全員分丸ごとの差押えの必要は認められないとした。この事件は、まだ ISP の業務やネットワークやサービス提供のためのサーバというものがどのようなものか捜査機関にもほとんど知られていない商用インターネット黎明期に起きた事件である。その捜査や証拠差押えなどの手法も通常の刑事事件と同じ方法で行おうとして混乱を来した事例である。また、コンピュータのデータのように可視性のないものに対しては、通常の有体物の顧客名簿などと同様に扱うわけにはいかないことを示したものである。

さらに、磁気データの押収時における一つの判断基準を示した判例としては、「浦和フロッピーディスク差押え事件抗告審決定」がある。1990 年代の終わり頃という時代から、差押え時の媒体が大量のフロッピーディスクとなっている。大容量記憶メディアが主体となる現在とでは多少状況が異なるかもしれないが、「情報を損壊させる危険がある場合には、内容確認をすることなく差押えが可能」との最高裁判断により、フロッピーディスクであるかハードディスクであるかを問わず通用するものと思われる。

(2000年以降)

2000年、高度情報通信ネットワーク社会形成基本法が制定され「高度情報通信ネットワーク社会」の基本政策が定められた。2000年代になると、コンピュータがより一層身近になり、それと同時にコンピュータ犯罪も増えていき、それに対応するようにたくさんの法律が制定・改正された。

ネットワークないしコンピュータシステムに対する危害をもたらす犯罪で重要なもののなかで不正アクセス禁止法が制定された。また、情報社会の進展にともない個人情報漏洩やプライバシー侵害の危険が増大してきた。これにより個人情報保護法が制定される。

1.3.5 デジタル・フォレンジックの分類

- ・ デジタル・フォレンジックを利用する主体
 - (1) 法執行機関
 - (2) 企業などの一般組織
- ・ 訴訟の対象となる行為
 - (1) 法律に違反
 - (例) 刑法、不正アクセス禁止法、個人情報保護法、商法など
 - (2) 組織の規定などに違反
 - (例) 規則に違反したメールの配信など
 - (3) 企業間の契約条項などに違反
 - (例) 守秘義務契約の違反など
- ・ 訴訟の種類
 - (1) 刑事訴訟
 - (2) 民事訴訟

1.3.6 デジタル・フォレンジックに使用される技術

デジタル・フォレンジックの主たる機能は証拠保全であるが、個人情報や企業の機密情報を扱うケースもあるため、その証拠データ自体も個人情報や機密情報になりえる。例えば、コンピュータ操作ログであれば「操作者がある個人・機密情報に対してどのような処理を行ったかを履歴保存」、ネットワークアクセスログであれば、「利用者が個人・機密情報に対してどのような利用をしたかを履歴保存」というように証拠保全が考えられ、そのため履歴の中に個人・機密情報が含まれることになる。

一方、コンピュータのデジタルデータは容易に改変することができるため、証拠保全のために残されたログ等を不正に改竄することは容易である。デジタル・フォレンジック

クにおいては、証拠能力が要求されるため、この証拠データ自体が改変されていないこと、つまり証拠の真正性の確保と、アクセスログや文書履歴などの各種記録には正確性の確保が要求される。これらのような状況においては、デジタル・フォレンジックの機能としての機密性を保全することも重要な位置づけとなる。これらのように、証拠データの真正性、正確性、機密性を確保する手段とし、証拠データの暗号技術が必要となる。ただし、事件が発生した時点では、暗号化された証拠データ自体を正規の手続きをとらずに複合することもデジタル・フォレンジックでは要求されることになり、キーリカバリ技術も重要となる。キーリカバリ技術とは暗号化されたデータを、緊急時に正規の手順を踏まずに復号することである。復号用の暗号鍵を紛失したり、鍵を持っている者と連絡がとれなくなったなどの場合にも暗号を平文に戻すことができる。キーリカバリにはいくつかの手法があるが、信頼できる第三者に、復号用の鍵かそれに準ずる物を預けておくという方法が広く知られている。キーリカバリ方式は暗号利用者の利便性が高まるとして期待される一方で、暗号の安全性が失われるとして、これを忌避する姿勢も根強い。特にアメリカでは、犯罪発生時に国家機関がキーリカバリを行える暗号システムを開発・採用するよう政府がコンピュータ業界に働きかける計画が明らかになり、大きな議論に発展した。

2 事件後のデジタル・フォレンジック

2.1 デジタル・フォレンジックの活用

コンピュータ犯罪・刑法犯罪においてパソコンが多用されるようになりパソコンやサーバー等に残されたデータを抽出することにより、犯罪の証拠として活用するデジタル・フォレンジックが導入された。10年前のデジタル・フォレンジックでは捜査にパソコンが1台あればよく、ファイル数もせいぜい1万ファイルくらいで十分であった。しかし急激なコンピュータの発展によりデータは複雑化し、1つの事件で扱うデータ量が数テラバイトである場合や、ファイル数が1億を超える事件も出てくるようになった。この章では事案が起こった場合にどのように利用し、手順で行い、どのような問題点があるかについて述べていきたい。

2.2 利用する主体

訴訟する側
法執行機関（犯罪捜査）、企業などにおける訴訟（法廷証拠提出）
訴訟される側
側

2.3 事件後のデジタル・フォレンジック捜査の手順

2.3.1 コンピュータ捜査の準備

デジタル・フォレンジックの捜査は、法執行機関の捜査と民間または企業の捜査二つに分かれる。捜査官の役割は、容疑者のコンピュータなどから証拠を集め、犯罪または企業規定の違反が行われたかどうかを判断することである。容疑者による犯罪または規定違反をほのめかすような証拠が上がった場合、事件の準備、つまり法廷や企業の審問に備えて証拠の収集を始めることになる。デジタル・フォレンジック事件において証拠を集めるには、容疑者のコンピュータを調べ、それを別のコンピュータに保存する。捜査を始める前に、事件の準備を行うために認定された手順に従う必要がある。それぞれの事件に系統的に取り組むことにより、証拠を徹底的に評価し、証拠の連鎖を詳細に記録することができる。また、捜査の計画を立て、証拠の保護をし準備をする。

2.3.1.1 法執行機関の捜査の準備

法執行機関による捜査では、政府機関が犯罪の捜査や起訴を担当する。容疑は殺人、強盗、いたずら行為などの刑事犯として捜査し、刑事訴訟法、刑法、憲法などの法に基づいた捜査を行わなければならない。犯罪の実行に使われたツ-

ルが何かを聞き出す。

2.3.1.2 民間の捜査の準備

民間の捜査の準備は、弁護士、企業などによって行われ、不当解雇や企業規定違反などの調査を行う。民間の捜査は通常は民事事件において行われるが、民事事件が刑事事件に発展したり、同様に刑事事件が民事事件に発展する場合もある。民間企業においてコンピュータ捜査を実施する場合には、捜査による事業の中断を最小限にとどめなければならない。また、訴訟はコストがかかるので訴訟を最小限に、あるいは行われぬよう努力している。企業のコンピュータ犯罪としては、電子メールなどによるハラスメント、データの偽造、横領、サボタージュ、産業スパイなどがあげられる。

2.3.2 捜査の実行

① 証拠の収集

証拠を収集する際には、忘れずに静電気防止袋とリストストラップ付きの静電気防止パッドを用意して、壊れやすい電子証拠を静電気により破損しないようにする。また出来る限り性格に証拠のコピーを作成し、証拠をきちんと保管する

(1) HDD などオリジナルの証拠を入手する

(1) 証拠用 HDD(コピー先)へ 100%物理コピーのビットストリームコピーを行う

(2) 対象 HDD(コピー先)と証拠 HDD のデータ同一性を比較するため捜査ログ上の ハッシュ値を確認する

(3) 物理コピーされたデータを解析ソフトウェアに適したイメージファイルへ変換

② デジタル証拠の分析

デジタル証拠の分析では、作業としてデータリカバリを行うことになる。ユーザーがディスク上のファイルの削除や上書きを行っている場合、ディスクには削除されたファイルとファイルのフラグメントが含まれており、元のファイルが占めていた空間はフリースペースになり、ユーザーが新しいファイルを保存するとこの空間が使われる。ファイルを削除しても、同じ位置にファイルが保存され、その領域の内容が上書きされない限り、削除されたファイルはディスク上に残る。その間には削除されたファイルでも元に戻すことができる。フォレンジックツールのほとんどは、証拠として使用するために削除されたファイルでも元に戻すことができる。

(1) 解析用ファイル形式に変換された証拠用データを解析用ソフトで認識させる

- (2) ファイルデータの分別⇒データベース作成
- (3) ビュワーを用いて様々なファイル解析ソフト一つで閲覧⇒フィルタリング
- (4) 必要に応じてパスワードリカバリーを実施したりレジストリーエリアを閲覧⇒データ抽出
- (5) レポート化

③ 証拠提出

事件が完了し、報告書を作成し終えたら、自分の部署や同僚の捜査官とミーティングを行い、事件に対して批評を行う。

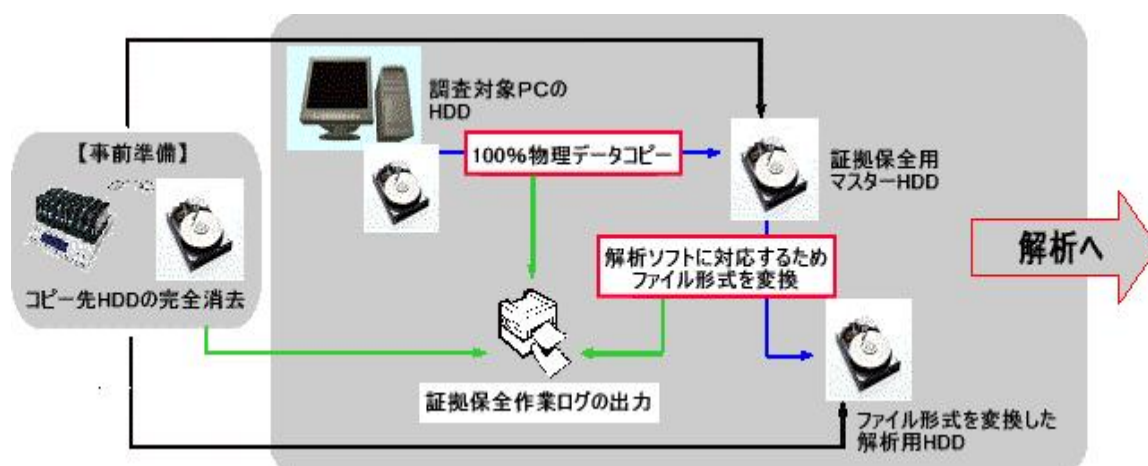
- ・ 事件の取り組み方をどのように改善できたか
- ・ 予測通りの結果を得られたか。あるいは、事件が全く予測しない方向に進展したか
- ・ 出来る限り完全な書類を作成したか
- ・ 新しい問題は発生したか。その場合問題は何か
- ・ 事件または調査において、新しいテクニックを利用したか

作業記録に次回以降の捜査において改善すべき、または取り組むべきテクニックや作業手順についてメモを残しておくが良い。また、作業記録は安全な場所に保管する。

2.4 事例

不正アクセスが起きた場合

既存のセキュリティツールだけでは、そのシステムで犯罪が行われたことを立証することは困難である。たとえ、不正アクセスの痕跡がアクセスログに残されていたとしても、それが法廷で証拠として認められ、容疑者の特定にまで至るかどうかは別問題である。また、自分たちの都合のいいようにアクセスログが改ざんされる可能性がある。こういった状況に対処するためにコンピュータ・フォレンジックに役立つ専用ツールがあり、これを使えばどんなに被害を受けたデータでも不正アクセスの様子を追跡して、法廷での証拠能力を保持した分析レポートを作成することができる。



【図 2-1】

2.5 課題

捜査する点における課題

- ・ システム技術
- ・ 超大容量のデータ
- ・ 指導者の養成・・・CFCE
- ・ Caseに関連する多種のデジタルデバイス
- ・ ASCII 以外の文字

データを出す側の課題

不適切な情報開示

デジタルデータは非常に膨大な情報が含まれており、場合によっては訴訟に直接関係ないが不利になるような情報が含まれている場合もある。

例・誤操作によるデータ消去

- ・ 安易に対象コンピュータに電源をいれたりデータにアクセスすることによるタイムスタンプの変更
- ・ フォレンジックイメージの作成方法を知らないが故の改変かつ原本証明の欠如

証拠作成能力がないとみなされる（意図的・組織的な隠蔽工作とみなされる）

↓

全てのコンピュータやメディアをそのまま提出するよう要求される

⇒訴訟に直接関係のない知的財産のような重要機密事項の流出

3 事件前のデジタル・フォレンジックの利用

3.1 事件前にデジタル・フォレンジックを活用

デジタル・フォレンジックは、企業において法的問題が発生したときにデータの解析を行い、証拠を保全するためのツールである。もともと企業間の訴訟が多いアメリカでは、不祥事の原因究明のためにデジタル・フォレンジックが積極的に取り入れられている。しかし日本では法曹界、企業におけるデジタル・フォレンジックの認知度は高くなく日本でデジタル・フォレンジックが積極的に活用されるのはこれからと見られている。ここでは企業が会社のシステムにデジタル・フォレンジックの技術を導入することによりどのような利点があり、課題があるかについて述べていく。

3.2 利用する主体

企業などの一般組織

3.3 導入する利点

企業が導入する利点として以下4つ考えられる

- ①何かがあったときの備えとしてのフォレンジック
- ②アカウントビリティ確保のためのフォレンジック
- ③サービスレベルの維持
- ④見えにくい物の可視化～信頼性の確保

①の何かがあったときの備えとしてのフォレンジックとは、民事訴訟で訴えられた場合でも証拠を提出する能力を保持し、犯罪捜査のための証拠をいつでも出せる状態にしておけるシステムを作ることである。②のアカウントビリティ確保のためのフォレンジックとは個人情報保護法やSOX法などの法律により、企業は世間に対し内部統制、安全管理措置ができなければならない。そのためにフォレンジックのシステムを作ることにより③サービスレベルの維持とは、内部統制のシステムを整えることにより監視システムが作用し、緊張感を持って仕事ができる。

3.4 システム例

・パケットキャプチャ機能—ネットワーク上に流れるすべてのパケットを取得する機能。

メールの送受信やWebページの閲覧履歴などそのままの状態でも再現できる。ただしパケットを取得するため、取得するデータ量に応じたストレージ領域を確保した製品を選ぶ必要がある

- ・解析機能－取得したパケットを解析する機能。全文検索、日付や時間、IP アドレス、ファイルサイズなどで絞込みが可能
- ・レポート作成機能－解析した結果をレポート出力する機能
- ・証拠保全機能－証拠保全にはテープメディアを使う。リピータハブもしくはミラーハブを使うことによりバックアップ構成をとる
- ・管理者通知機能－キーワードやファイルサイズなどをあらかじめ設定しておくことで、アラート情報を管理者にメールで通知することができる機能

他システムとの違いはログ解析による捜査の再現性と改ざん防止の機能の付加。また、取得したログをテープメディアに落とし、ログそのものをハッシュ値を計算することで、改ざんの防止を実現、証拠提出のためのフォーマットを持った点も通常のログ監視機能を持った製品との違い

3.5 課題

守るべき情報や、アクセス制限の遵守など社内の規律は、明確な基準と違反行為に対する厳正な処分担保されるといえる。情報管理の視点から適切な社内規定を整備し、これを担保するためのフォレンジックの活用や社員の調査への協力義務などを盛り込むことが有効である。そのために現在のシステム環境をきちんと見直しマニュアルを作り、導入するにあたって、コストはどうか、運用に合致しているか、会社の体制にあっているかどうかを見なければならぬ。

また技術者不足から証拠保全ができないことがある。そのようなことがないよう研修を行い、きちんとした管理体制をとっていく必要がある。

もうひとつの問題として、日本ではまだ導入事例が少ないため費用対効果が明確でないのも問題である

4 デジタルフォレンジックの普及対策

4.1 国のデジタルフォレンジック普及への取り組み

(1) 政府

2000年1月の省庁のHP改竄事件がきっかけに情報セキュリティポリシーに関するガイドラインなどを作っている。法務省では、セキュリティ関係の法律の整備、文部科学省では、セキュリティ関係の研究開発にお金を出すと共に、各大学にセキュリティの教育拠点を作ろうとしている。総務省とLASDEC(財団法人 地方自治情報センター)では、自治体のセキュリティ研修の実施や、監査の普及を推進しており、技術の話だけではなく、どう運用するかということを含めた教育もしている。

また、情報セキュリティ早期警戒パートナーシップでソフトウェア等の問題箇所(脆弱性)について、関係機関・ベンダーを通じて秘密裏に対策を講じ公開していくことによって企業へセキュリティの警告、情報の提供を行っている。

(2) 警察機関

日本の法執行機関におけるフォレンジックは以前から行われており、警察庁科学警察研究所では法科学部という部門が4つ存在している。警察庁では研究・開発を行い、さまざまなデバイスに対する証拠保全技術及び解析技術を培っている。また、諸外国の捜査機関とセミナーを行ったり、交流を図り技術などの情報交換を行っている。

警察庁は2004年の「警察庁情報セキュリティ政策大系-2004」、2005年「警察庁情報セキュリティ重点施策プログラム-2005」においてコンピュータ・フォレンジックに係る取り組みを強化していくと記述している。

警察機関においてデジタル・フォレンジックを所掌している部署は、警察庁情報技術解析課、管区警察局情報技術解析課および府県情報通信部情報技術解析課等である。フォレンジックに関する教育は、警察情報通信学校や管区警察学校等において行われ人材を育成している。複雑になっていく犯罪に対応するために産学界とより一層強力連携していくことが重要である。

5 デジタル・フォレンジックの今後の展望

法執行機関と法曹のコンピュータへの苦手意識、技術者の法律への苦手意識を少なくしていくこと、デジタル捜査法などの法整備、一般企業における問題意識の浸透、国際間協力、高度な技術への対応があげられる。デジタル・フォレンジックに携わる日本の人材は、米国に比べて一桁少ないといわれている。デジタル化の波は高まる一方であり、電子的証拠を的確に評価できる e-Discovery 等に造詣の深い裁判官や法曹関係者の養成、内部統制の分野においても、デジタル・フォレンジックや IT の知識を持つ財務監査人を数多く育てることが求められている。

<<参考文献・URL>>

<書籍>

デジタル・フォレンジック協会, 2006年, 『デジタル・フォレンジック事典』日科技連.
Bill Nelson, Ameria Phillips, Frank Enfinger and Cgris Steuart, 2005, *Guide to Computer Forensics and Investigation*. (=2000, SITEJ1 訳『コンピュータ・フォレンジック入門ー不正アクセス、情報漏洩に対する調査と分析ー』トムソンラーニング.)
上原敏夫, 2004年, 『民事訴訟法』有斐閣 S シリーズ.
2006年, 『コンパクト六法』岩波書店.

<URL>

『有限責任中間法人 JPCERT コーディネーションセンター』 <http://www.jpccert.or.jp/>
『経済産業省』 http://www.meti.go.jp/policy/it_policy/index.html
『特定非営利活動法人 デジタル・フォレンジック研究会』
<http://www.digitalforensic.jp/index.html>
『独立行政法人情報処理推進機構 (IPA)』 <http://www.ipa.go.jp/>
『IT用語辞典 e-words』 <http://e-words.jp/>
『@police』 <http://www.cyberpolice.go.jp/index.html>
『株式会社 UBIC』 <http://www.ubic.co.jp/>
『岡村久道 HOMEPAGE』 <http://www.law.co.jp/okamura/index.html>
『キーマンズネット』 <http://www.keyman.or.jp/>
『IT政策リンク集』 <http://japan.internet.com/public/link/>