デジタル・フォレンジックの原理・実際と証拠評価のあり方

吉峯耕平　弁護士

よしみね・こうへい
1977年、千葉県生まれ。2002年、東京大学経済学部卒業。司法研修所第58期修了。2005年、弁護士登録。田辺総合法律事務所所属。主な著作に「従業員が逮捕された場合には企業はどう対応すべきか」（共著、Lexis企業法務19号〔2007年〕69頁）、『病院・診療所経営の法律相談』（編集共著、青林書院、2013年）、「転嫁拒否の禁止に関する実務ポイントQ&A」（旬刊経理情報1362号〔2013年〕46頁）がある。

倉持孝一郎　弁護士

くらもち・こういちろう
1982年、神奈川県生まれ。2004年、東京大学卒業。司法研修所第60期修了。2007年、弁護士登録。田辺総合法律事務所所属。主な著作に『実践！営業秘密管理　企業秘密の漏えいを防止せよ！』（共著、中央経済社、2012年）、「法務担当者のための企業年金入門（第1回～第4回）」（共著、BUSINESS LAW JOURNAL 2013.7-10 No.64-67）がある。

藤本隆三　AOSリーガルテック株式会社フォレンジック調査員

ふじもと・たかみ
1957年、福岡県生まれ。1979年、防衛大学校卒業。

新井幸宏　AOSリーガルテック株式会社フォレンジック調査員

あらい・ゆきひろ
1956年、埼玉県生まれ。1989年、東京工業大学総合理工学研究科博士課程修了。

Ⅰ　はじめに

1　デジタルデータと刑事裁判

今日、われわれの日常生活のあらゆる側面は、不断にデジタルデータによって記録され続けている。日常的な取引の、そのほとんどがコンピュータにより処理され、記録される。コンビニのPOSデータ、クレジットカード、交通系ICカード、ETC、ビルの入退館記録、防犯カメラ、Nシステム……。また、近年著しく普及した携帯電話やスマートフォンには、かつては考えられなかったほどの密度の記録が、時々刻々と、長期間にわたって蓄積されている。

一方、刑事裁判に目を向けると、供述証拠偏重から脱する方向に舵を切りつつあるように見える。裁判員裁判の影響や捜査機関への協力意識の減衰など、様々な要因が理解できるが、技術的要因により客観的証拠が利用できる場面が増え、客観的証拠と供述証拠が矛盾すれば供述証拠が覆されるという、当たり前の現象が生じているに過ぎないとも考えられるのではないか。かつて捜査機関は、供述証拠という絵筆を自由に操り、白紙のキャンバスに好きな絵を描くことができた。今日、白紙部分は狭まりつつある。客観的証拠の密度が、供述証拠が覆される事例が目立ち始める程度に達したということであろう。

そうすると、不可逆的な趨勢として、客観的証拠を重視する傾向は進展していくものと予想される。デジタルデータも、客観的証拠の一種と理解できるところ、今後はさらに存在感を増していくことになろう。

2　デジタル・フォレンジックとは[1]

デジタル・フォレンジック（コンピュータ・フォレンジックとも呼ばれる）は、「コンピュータから有用な情報を抽出し、法的手続のために証拠化する技術」と定義できる[2]。

デジタル・フォレンジックの対象は広く、様々な応用分野にまで発展している。主な応用的分野を挙げると、以下のようなものがある。

①　モバイル・フォレンジック

携帯電話（いわゆるガラケー）、スマートフォン等の携帯端末を対象としたデジタル・フォレンジック。PCを対象とする場合と比べ、ハードウェアとソフトウェアの両面にわたって、解決しなければな

らない独自の問題が多い[3]。

② **eディスカバリー対応**[4]

米国訴訟における電子証拠の開示手続(e-Discovery)への対応。

③ **ネットワーク・フォレンジック**[5]

ネットワーク環境における通信データのログやサーバ上のデータの取得・分析により、サイバー攻撃の実態を解明する手法。

本稿では、単独で動作しているコンピュータ(PC)を念頭に置き、ハードディスクからデータを保全し、解析するという、いわば古典的なデジタル・フォレンジック[6]を対象に論を進める。なお、モバイル・フォレンジックについては、別稿を予定している。

3 捜査機関の対応と弁護人の能力

捜査機関は、近時、デジタル・フォレンジックに関する体制整備・人材育成を強力に推進している。

いわゆる厚労省FD改竄事件では、デジタル・フォレンジックの手法により、データ改竄が証明された[7]。「検察の在り方検討会議」の提言[8]を受け、最高検察庁は、デジタル・フォレンジックも扱う法科学専門委員会を設置した。もっとも、厚労省FD改竄事件は非違行為への対応という側面が強く、デジタル・フォレンジックの必要性が正面から問題になったものではない。

FD改竄事件以上のインパクトを与えたのが、PC遠隔操作事件といわれる、2012(平成24)年6～9月に発生した、4件の冤罪・誤認逮捕事件である[9]。PC遠隔操作事件の発覚以降、現場から上層部まで、捜査機関のデジタル・フォレンジックに関する意識は大きく変わってきたように思われる[10]。

捜査機関の姿勢の変化が、供述証拠偏重を排す方向に向かうのであれば、それ自体は積極的に評価されるべきことである。しかし、他方で、デジタルデータを理解し、処理する能力(それはパワーポイントで見栄えのよいスライドを作る能力とはイコールではない)において、捜査機関と弁護人に大きな格差が生じつつあるのではないかという危惧を感じざるをえない。

今日の刑事弁護において、客観的証拠――とりわけデジタルデータの収集・確保の重要性は、強調してもし過ぎることはない。また、日々の商取引に関するデータやモバイル機器に蓄積された情報が、事実認定にいかなる影響を与えるかを想像してみれば容易にわかるように、その影響のおよぶ範囲は、一部の特殊なサイバー犯罪に限られるものではない。冤罪であるという依頼者の主張を証明しようと考えたときに、利用可能なデジタルデータは様々なところに散在しているだろうし、その可能性を仔細に検討できない弁護人は、常に弁護過誤の危険を冒していると言っても過言ではない。

デジタル・フォレンジックは、デジタルデータの確保というテーマに対するひとつの回答であり、常にそれが必要になるとは限らない。データを保持する事業者に照会して回答を得れば足りるような事案も多いだろう。それなりにコストもかかることもあり、最大限の情報を、最も厳密な形で確保する必要があるか、事案により様々であろう。しかし、デジタル・フォレンジックを利用しない事案においても、コンピュータの動作原理とデジタルデータの処理についての基礎知識は、確保すべき証拠の「アタリ」をつけるためには重要である。

4 デジタル・フォレンジックと法律家の役割

デジタル・フォレンジックは、自律的で完結したひとつの技術体系となっており、局外者である法律家が口を挟む余地は比較的少ない。とはいえ、デジタル・フォレンジックの入口と出口において、法律の世界との接点があり、法律家の果たすべき役割もそこにある。

まず、フォレンジック調査の開始は、法律家の判断にかかっている場合が多い。FD改竄事件では、FDの解析は弁護人の判断を待って開始された。筆者(吉峯)が控訴審から関与した否認事件にも、原審弁護人の調査不足により有罪無罪を決する決定的なデータが保全されないまま消去され、復元できなかった事例がある。初動対応を失敗すると、データの喪失により取り返しのつかない事態となりかねない。法律家には、デジタル・フォレンジックの概要や、どのような結果が出る可能性があるのかについて理解し、調査の必要性とコストについて依頼者に助言する責務があるといえよう。

次に、デジタル・フォレンジック調査の結果は、最終的には裁判所の判断に供されるのだから、その証拠としての評価について、法律家が詰めた検討を行う必要がある。捜査機関がデジタル・フォレンジック

を使いこなすにつれ、「動かぬ証拠」によって事実認定を誤る事案が生じることが予想される。PC遠隔操作事件（とくに少年法上の保護処分にまで至った神奈川事件）は、「動かぬ証拠」を弁護人が弾劾できなかった事案でもあり、我々には重い課題を突きつけられていると言えよう。

5　本稿の目的と構成

本稿では、法律家と専門家の双方の視点を踏まえて、基本的なデジタル・フォレンジックを対象に、その枠組みを示したい。

まず、必ずしもコンピュータに詳しくない法律家を想定して、デジタル・フォレンジックの基礎を支える原理と実務の概要を解説する（Ⅱ・Ⅲ）。

そして、デジタル・フォレンジックの特質を踏まえて、証拠に対する法的な評価（証拠能力および証明力）のあり方を検討する（Ⅳ）。

デジタル・フォレンジックの実務では様々な専用機器や解析ソフトが利用されるが、本稿では、個別の商品の紹介までは立ち入らない。法律家が詳細を把握している必要は大きくないうえ、相当のスピードで情報が陳腐化するからである。

Ⅱ　デジタル・フォレンジックの原理

1　デジタル・フォレンジックの目的

デジタル・フォレンジックには、以下の2つの目的がある。後述する具体的な手順は、2つの目的を達成するために構成されているといえよう。

⑴　有用性確保

まず、調査対象のコンピュータから、可能な限り有用な情報を引き出すことが、第一の目的となる。

「有用な」というのは、情報を最大限引き出すだけでは十分ではなく、得られた情報を整理して絞り込むことも必要である。

⑵　証拠性確保

デジタル・フォレンジックの調査結果は、最終的には訴訟等の法的手続に、報告書等の証拠として提出されることを予定されている。したがって、その目的は調査結果が裁判所の事実認定に採用されることである。すなわち、当該証拠が、証拠能力と高い証明力を持つと評価されるように、調査を実施しなければならない。

この観点を、「証拠性の確保」と呼ぶことができる[11]。

2　デジタルデータ[12]

デジタル・フォレンジックは、コンピュータに記録されたデジタルデータを対象とするので、デジタルデータの特質をまず理解する必要がある。

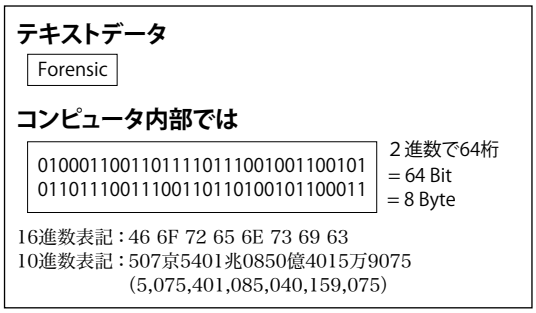
現在実用的に利用されているコンピュータは、デジタルデータ、すなわち2進数で表記される数字を処理する。2進数を読み取り、計算し、記録するのがコンピュータといえる。2進数とは何かというと、0と1を並べたものと理解すればよい。一例を挙げると「1101」である。

この2進数をわれわれが通常使う10進数の数字に変換するためには、各桁に1、2、4、8……と、2のn乗を乗じて合計すればよい。2進数の「1101」は、1×8＋1×4＋0×2＋1×1＝13なので、10進数で書けば「13」ということになる。

コンピュータは、文字、画像、音楽、動画、メール、ワープロ文書といった様々な情報を扱うことができるが、内部的にはすべて2進数の数字（＝デジタルデータ）を操作している。また、コンピュータの動作を指定したプログラムも、デジタルデータとして記録されている。

たとえば、「Forensic」という文字列は「0100011001101111011100100110010101101110011100110110100101100011」という数字として処理されている（図表1）[13]。

図表1　デジタルデータの正体



3　デジタルデータの特質

デジタルデータには、物証や書面といった物理的実体を持った証拠（以下、「物理的証拠」という）と比べると、以下のような特質がある。

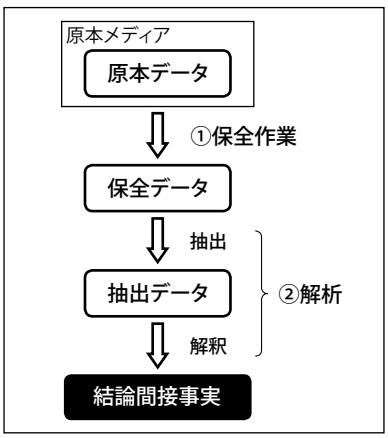
① 完全一致性――完全なコピーを作成することができ、完全に一致していることを容易に確認できる
② 改変可能性――容易に、かつ、痕跡を残さずに改変・消去[14]できる

もっとも、②については、あくまで原理的に妥当する性質である。現代のコンピュータは、巨大なシステムとして動作していることから、一部のデータを改変すると、他のデータとの一貫性が崩れる等、その痕跡が残ることが多い。また、データを消去しようとしても、あらゆる痕跡を全て消去することは、困難なことが多い[15]。

4 手順の概観

デジタル・フォレンジックのプロセスを理解するためには、①保全作業、②解析、の2つの段階に分けることが便宜である[16]。

図表2 手順の概観



(1) 保全作業

ある時点で調査対象コンピュータから、ハードディスク等の外部記憶装置(以下、「原本ディスク」という)のデータをコピーして、ハッシュ値を計算する。保全作業の結果、得られたすべてのデジタルデータを「保全データ」と呼ぶ。

(2) 解析

保全データを解析して意味のあるデータを抽出し(以下、得られたデジタルデータを「抽出データ」という)、抽出データを解釈することで、「特定内容のメールが受信された」、「ある操作が特定の時点に実行された」といった間接事実(以下、「結論間接事実」という)を認定する。

Ⅲ デジタル・フォレンジックの実際

1 保全作業[17]

デジタルデータは改変が可能であり、また、システムが動作するに従って時々刻々とデータは実際に書き換えられていく。情報を最大限に確保し、かつデータを改変していないことを立証できるようにするために、ある時点のコンピュータの状況を固定化する必要がある。そのために実施されるのが、保全作業である。

具体的な作業としては、対象となるコンピュータから、ハードディスクを取り出して、コピーするというのが、保全作業の概要である。対象となる外部記憶装置はハードディスクに限らず、SSDやUSBメモリ等も考えられるが、以下、とくに断らない限り、ハードディスクで代表させる。

保全作業自体はハードディスクのコピー作業であって、コンピュータや原本ディスクといった有体物の確保とは別の問題である。保全作業は、コンピュータの差押等の法的な証拠収集手続と密接に関連するが、これとは別に実施されることも多い。たとえば、典型的には以下のようなパターンが考えられる。

① コンピュータの捜索・差押の後、捜査機関において保全作業が実施される。
② コンピュータの任意提出・領置の後、捜査機関において保全作業が実施される。
③ 記録命令付差押(刑訴法99条の2、218条2項)により、対象ハードディスクをコピーし(保全作業)、コピーを差し押さえる。
④ 企業が従業員の使用させているコンピュータにつき保全作業を実施し、コンピュータは従前の通り利用を継続する。

保全作業の主なポイントは、ハードディスクを丸ごとコピーすること、ハッシュ値を計算すること、の2点であるが、前提として、ハードディスクがどのようにデジタルデータを記録するのか、という点から論を進める。

(2) ハードディスクの仕組み

(a) 物理ドライブ

ハードディスクは、莫大な数の記録素子を並べたものである。1個の記録素子は、0か1のどちらかの状態を取ることができ、すなわち、1ビットの情報を

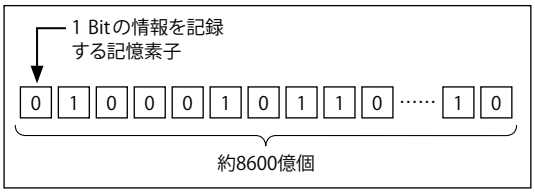
記録できる。

たとえば100ギガバイトのハードディスクは、約8600億個の記憶素子をまとめたものであり、2進数で約8600億桁（8600億ビット）を記録できる（10進数で約2600億桁相当）[18]。

ハードディスクの場合は、ディスク表面の極小の磁石を記憶素子として使っている。SSDは半導体を記憶素子として使う。

このように、ハードディスクは、莫大な桁数（たとえば8600億桁）の2進数を記録する方眼紙のようなものである。その方眼紙のマス（記憶素子）に1から8600億まで順番に番号を振って、必要に応じて書き変えて情報を蓄積することになる。

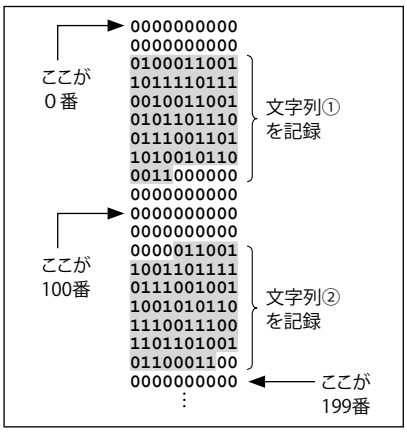
図表3　100GByteのハードディスクの概念図



⑹　ファイルシステム[19]

しかし、単に数字を並べて、読み書きすることができるというだけでは、非常に不便なので、ファイルシステムという仕組み（決まり）が用意されている。ファイルシステムには、Windowsで使われるFATやNTFS、Macで使われるHFS+など、様々なものがある。ファイルシステムの役割は、ファイルシステムがなければどうなるのかを考えればよく理解できる。

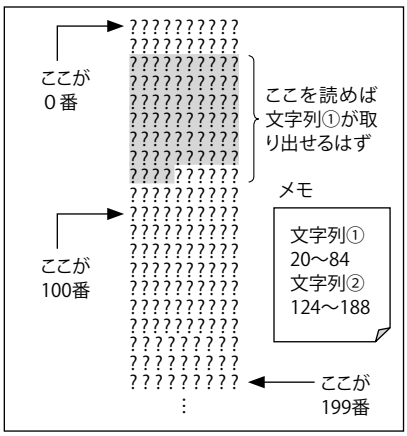
図表4　ハードディスクにデータを記録する



図表4は、ハードディスクの先頭から記憶素子が並んでいる状況を表している。実際のハードディスクは、膨大な数の記憶素子（たとえば約8600億個）が並んでいるが、そのごく一部200個だけを書いている。ここに0から始めて番号を振っていく。

「Forensic」という文字列をここに記録することを考えよう。この文字列（仮に、文字列①と呼ぶこととする）は、前述のとおり「01000110011011111011001001100101011011100111001101101001011000011」という64桁の数字として処理される。図表4では、文字列①を20番から84番の記憶素子に記録している。同様に、「forensic」という文字列（文字列②）を記録してみよう。文字列①との違いは先頭の「f」であり、ここが「01100110」に変わっている。図表4では、124～188番に文字列②が記録されている。

図表5　記録されたデータの読み出し



記録したデータを読み出すためには、そのデータがどこに記録されているかという情報が必要となる。たとえば、文字列①は20～84番、文字列②は124～188番、というメモを持っていれば、いつでも文字列①＝「Forensic」、文字列②＝「forensic」を取り出すことができる。逆にメモがなければどの場所を見ればよいのかわからない。

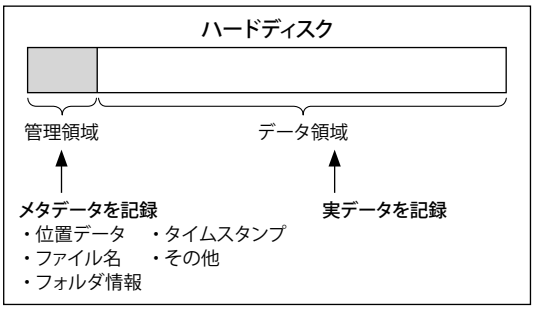
このように、ハードディスクを利用するためには、ハードディスクのどの位置に目的のデータが記録されているのかというデータ（以下、「位置データ」という）が必要になる。位置データを紙のメモで持っているのは不便なので、ハードディスクの特別な場所に記録しておくことになる。

また、位置データ以外にも、データを管理するために様々な情報を記録しておくことが便利である。そこで、ファイルシステムは、管理するデータ＝「ファイル」ごとに、「メタデータ」（データを管理するためのデータ）を記録することにしている。また、メタデータ

と対比して、管理の対象となるデータ（上記の例では「Forensic」というデータ）を「実データ」という。

ファイルシステムは、このようなメタデータを保存するための「特別な場所」をハードディスクに確保する、これを「管理領域」と呼んでいる。また管理領域以外の、実データを保存する領域は、「データ領域」と呼ばれる[20]。

図表６　管理領域とデータ領域に分ける



メタデータの種類はファイルシステムにより差異があるが、概ね以下のようなものである。

① 位置データ――ファイルが物理ディスクのどの箇所に記録されているかという情報[21]

② ファイル名――ファイルを利用者が認識するための情報

③フォルダ情報――ファイルのハードディスク上における物理的な位置は、位置データが記録しているが、それとは別に、抽象的な階層的フォルダ構造における位置を記録している。

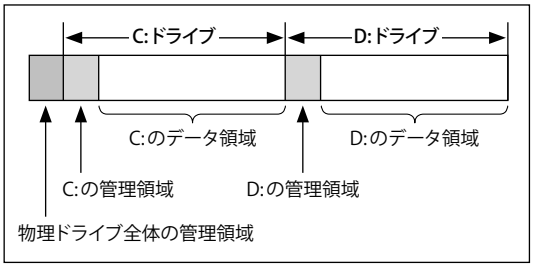
④ サイズ――ファイルの実データのサイズ。サイズによってハードディスク上の領域をどの程度確保しなければならないかが定まるので、位置データの一部とも考えられる。

⑤ タイムスタンプ――ファイルが作成された日時、更新された日時、最後に読まれた日時等の情報

(c) 論理ドライブ

さらに、１つのハードディスクを複数の領域（パーティション）に分けて使うことも可能である。たとえば、１つのハードディスクを２つの領域に分けると、Windows等のOSからは、あたかも２つのハードディスクがあるように表示される。この仮想的なハードディスクには、「C:」「D:」などと名前がついており[22]、それぞれを論理ドライブという。また、PCのメーカーが準備した初期化用のツールなどが使用する、ユーザーからは見えない隠し論理ドライブも存在する。

図表７　パーティションを含んだ物理ドライブ全体の構成

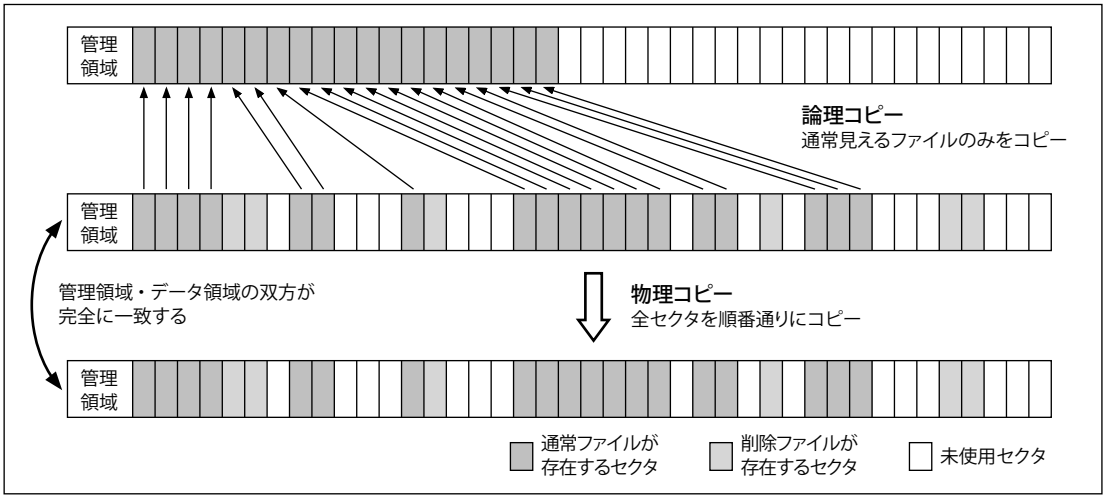


(2) 物理コピーと論理コピー

保全作業では、原本ディスク上のデータのコピーを作成するが、物理コピーと論理コピーという２つの方法がある。

物理コピーは、ハードディスク（物理ディスク）に記録されたデジタルデータ（以下、「原本データ」と

図表８　物理コピーと論理コピーの概念図



いう）を、先頭から末尾まで全てそのままコピーすることをいう。前述した100ギガバイトのハードディスクの例では、約8600億桁の0と1が原本データである。これをそのままコピーするのである。

これに対し、論理コピーは、通常のコピーであり、ファイルシステムによって管理されているファイルごとにコピーを実行する。

物理コピーは、「イメージコピー」、「フォレンジックコピー」とも呼ばれるが、原本ディスクに記録されていたすべての情報を保全することができるのに対し、論理コピーでは、情報の一部が失われてしまう。具体的には、論理コピーでは、**2**(2)で後述する削除ファイル復元ができなくなってしまうのである。

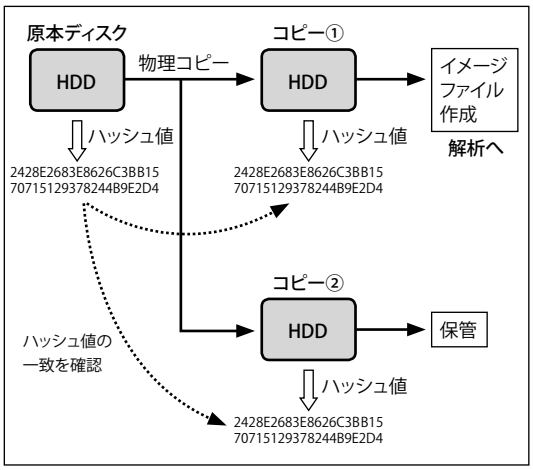
つまり、なるべく多くの情報を確保するという有用性確保の観点から、物理コピーを取得する必要があるといえる。

また、物理コピーは、原本データをそのままの形でコピーするものだから、証拠性確保の観点からも有利である[23]。

(3) 保全作業の具体的手順

(a) 電源が入っている場合

図表9 保全作業の具体的手順のイメージ



調査対象コンピュータの電源が入っている場合、ハードディスクだけでなく、メモリ上のデータ等を取得することがある。ただし、その操作によって、ハードディスクのデータが変更され、場合によっては消失するリスクもあるため、慎重な判断を要する。

(b) 物理コピーの取得

コンピュータを分解してハードディスクを取り出し、専用の物理複製装置（写真）に接続して、物理コピーを実施する。多くの場合、1個のハードディスクから2個のコピーを一度に作成する。また、ノートパソコンを分解してハードディスクを取り出すことが難しい場合などには、ソフトウェア方式で物理コピーを取得することもある[24]。

なお、原本データと関係のないデータが混入することを防止するため、コピー先のハードディスクは、あらかじめデータを完全に消去する措置をとる。

(c) ハッシュ値の計算・確認

物理複製装置を使用した物理コピー

正確に物理コピーが完了したことを確認し、証明するために、原本ディスク、コピー先についてハッシュ値を計算し、それぞれ一致することを確認する。ハッシュ値とは、デジタルデータの「指紋」となる短いデータで、これが一致すれば全く同じデータであることが確認できる（**IV2**(2)で後述する）。

フォレンジック用の物理複製装置は、ハッシュ値を自動的に計算して一致を確認し、ログを出力する機能がある。

(d) イメージファイルの作成

物理コピーしたハードディスクは、1個を解析用、1個を保管用とすることが多い。また、解析用のハードディスクについても、ハードディスクにアクセスしての対象とはせず、イメージファイル（ハードディスクに記録されたすべてのデータを記録したファイル）に変換して、解析の対象とすることが多い。イメージファイルを利用したほうが、誤ってデータを変更してしまう可能性が低く、また、解析用コンピュータに複数のイメージファイルを保存することができて、便利だからである。

(e) 記録

保全作業については十分な記録を残すことが、証

拠性確保の観点から、極めて重要である。実務上、①保全作業の全過程をビデオで撮影する、②CoCと呼ばれる書類[25]に作業内容等を逐一記録する、といった措置が取られている。

とくに、原本データのハッシュ値は、証拠性確保の起点となるので、確実に記録しておく必要がある。

2　解析

⑴　解析ソフト

保全作業により保全データが得られるが、ここから必要な抽出データを絞り込み、これを解釈するのが、「解析」の過程である。

実際の作業は、解析ソフトを利用することになり、可能な限り自動化されている。以下の説明の多くは、解析ソフトがどのような作業を実施しているのかという説明である。

⑵　削除ファイルの復元[26]

デジタルデータは、原理的には、痕跡を残さずに改変・消去できる（改変可能性）。しかし、Windows等の操作でファイルを「削除」しても、それだけではデジタルデータは消去されないことが多く、一定の操作で削除データを復元することができる。しばしば、削除したはずのデータから意外なほど大量の情報が得られることがあり[27]、削除データの復元は重要な位置を占める技術である。

ⓐ　ファイル削除≠データ消去

1⑵ⓑで前述したとおり、ハードディスクは管理領域（メタデータを記録）とデータ領域（実データを記録）に区分けされ、管理領域には、ファイルがデータ領域のどこに記録されているのかをあらわす位置データが記録されている（図表10①）。

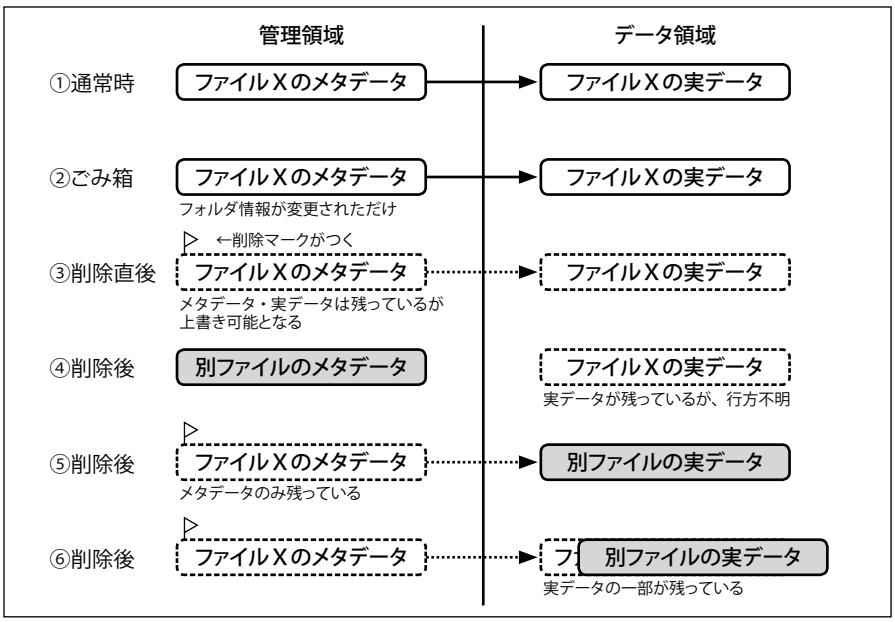
Windowsで、ファイルを「ごみ箱」に入れると、今まで「デスクトップ」となっていたメタデータ（フォルダ位置）が、「ごみ箱」に書き換えられる（②）。

そして「ごみ箱を空にする」を実行すると、Windowsはそのファイルを削除する。しかし、削除の具体的な動作は、ファイルのメタデータの先頭に「削除マーク」を記録するだけである。これにより、そのファイルはWindowsからは見えなくなり、当該ファイルの使っていた管理領域・データ領域は、未使用領域として、別のデータを書き込むことができるようになるが、メタデータ・実データは、消去されずに残っているのである（③）[28]。したがって、この段階であれば、「削除マーク」を元に戻すだけで、削除ファイルがそのまま復元できる。

ⓑ　データは上書きにより失われる

その後、管理領域・データ領域がそれぞれ再利用され、別のデータが上書きされていき、以前のファイルに関する情報は次第に消去されていく。データ消去の態様は、どの位置に新しいデータが書き込まれ

図表10　ファイルの削除とデータの消去



るのかという偶然に左右され、新しいデータが多く上書きされるほど、復元の可能性は低くなっていく。とくに、ハードディスクの高速化のために行われるデフラグ（データの再配置）が実行されると、復元が難しくなることが多い。

管理領域が先に上書きされた場合は、位置データが失われるので、実データがどこにあるのか、行方不明の状態となる（④）。この場合、データ領域からヘッダ情報や特定のテキストを検索することで、残存した実データを探し出し、復元することになる。

逆に、データ領域の実データが先に上書きされる場合もある。ファイル名、サイズ、タイムスタンプ等のメタデータを持つファイルが存在していたのはわかるが、その中身（実データ）はわからない（⑤）、あるいは一部しか残っていないという状態になる（⑥）。

解析ソフトは、ある程度の削除ファイルの復元は、自動的に実行する。④の実データの探索は、手動でキーワードを指定して検索することもある。

⑶　その他の情報収集手段

⒜　ログデータ

Windows等のOSや、アプリケーションソフトは、様々なログ（履歴）をハードディスクに記録している。

たとえば、Windowsでは、レジストリというデータベースで設定やシステムの状況を集中的に管理している。レジストリには例えば以下のような事項が記録されている。

- Explorerから起動したプログラム
- ログインユーザー名
- 最近使ったドキュメント
- USBに接続したUSBメモリやハードディスク等のデバイスの記録（日時やUSB機器を特定するシリアル番号）

また.pfファイルと呼ばれるファイルにも、実行したプログラムの履歴情報が含まれている。

以上は、Windows（OS）レベルで管理されている履歴だが、アプリケーションも様々なログを記録している。特に重要なのは、ウェブブラウザのログだろう。大きく分けると、アクセスログと、ウェブアクセスの高速化のための仕組みであるキャッシュデータ（Temporary Internet Files）がある[29]。

⒝　様々なファイル形式の解析

ハードディスクには様々な形式のファイルが保存されている。

一般に、アプリケーションソフトは、データファイルの中に、作成者情報、タイトル、タイムスタンプ等の管理情報を記録することが多い。これは、前述の管理領域に保存されているメタデータとは異なり、実データの中に、ファイルを管理するためのデータが記録されているのである（以下、「ファイル内メタデータ」という）。

たとえば、画像データに書き込まれているExif情報も、このようなファイル内メタデータの一種であり、撮影機材、カメラの設定、日時等の詳細な情報が記録されている。カメラによっては、GPSによる場所情報も記録されている[30]。

⒞　暗号化とパスワード解析[31]

ファイルの中には暗号化されているものもあり、パスワード解析によって暗号化を解除することがある。暗号化の強度は、暗号化の形式やパスワードの長さによって様々である。

⑷　情報の絞込み・整理

近年のハードディスクの大容量化やシステムの複雑化の影響で、大量の（数千件、数万件もの）データが抽出できることが多い。そこで、調査の目的から有用な情報をどのように絞り込み、整理するのかという観点が重要になる。

解析ソフトは、情報の整理、絞込みのために、検索機能[32]、フィルター機能（特定の日付やサイズ等の条件を設定し、これに該当するファイルを抽出する機能）、時系列での整理機能といった、多様な機能を用意している。大量の既知のファイルを排除して、現在調査中のシステム特有のファイル（それはユーザーが作成したファイルか、そのシステム特有の情報を含んでいるかもしれない）を抽出する機能もある[33]。

膨大な情報の中から、調査目的との関係で有用な情報をいかに絞り込んでいくのかということであり、解析ソフトの機能もさることながら、調査員の経験・技術に依存する部分も大きいといえる。

Ⅳ　証拠評価

1　総論

⑴　証拠能力と証明力

法的な観点から証拠を評価する場合、証拠能力と

証明力の2つの視点から検討する。

証拠能力は、証拠として用いることのできる法的許容性であり、証明力は、証拠が事実認定に役立ちうる実質的価値をいう（刑訴法318条、民訴法247条）[34]。

民事訴訟では、原則として証拠能力が否定されることはなく、証明力のみが問題となる[35]。

刑事訴訟では、証拠能力の要件が法律の明文上、または、解釈上、厳格に規制されている。証拠能力をクリアしてはじめて、証明力を評価することになる。

⑵　証拠の形態

フォレンジック調査は、裁判所の鑑定、捜査機関からの嘱託による嘱託鑑定、弁護人その他の私人の依頼による私的鑑定として実施される。その調査結果は、鑑定書、嘱託鑑定書や報告書等の書証（以下、あわせて「フォレンジック報告書」という）として裁判所に提出されるのが通例である。

保全データそのものを提出することは、ほとんど意味がない。裁判官が、保全データから直接、意味のある事実を認定することは不可能であり（たとえるなら、DNAのATCGの塩基配列をそのまま提出し、それ自体を事実認定の根拠とすることを求めるようなものである）、コンピュータを利用した解析を経ることが不可欠だからである。

したがって、デジタル・フォレンジックに関する証拠の証拠能力は、デジタルデータそのものについて議論するのではなく[36]、フォレンジック報告書の証拠能力を論じることになる。

⑶　科学的証拠としての観点

フォレンジック報告書は、犯罪事実（または民事上の紛争）に関する資料を対象に科学的分析を実施し、その結果を報告するものと考えることができるから、科学的証拠の一種と位置づけられる。科学的証拠については、足利事件や東電OL事件を契機にして、司法研究[37]が発表される等、議論が活発化している[38]。従前あまり意識されてこなかったところであるが[39]、フォレンジック証明書の評価も、科学的証拠の評価という視点を欠かすことはできない。

他方、フォレンジック報告書は、他の科学的証拠と比べて、かなり特殊な点がある。保全作業完了後は完全な再現可能性があること、立証対象が不定形であることの2点である。

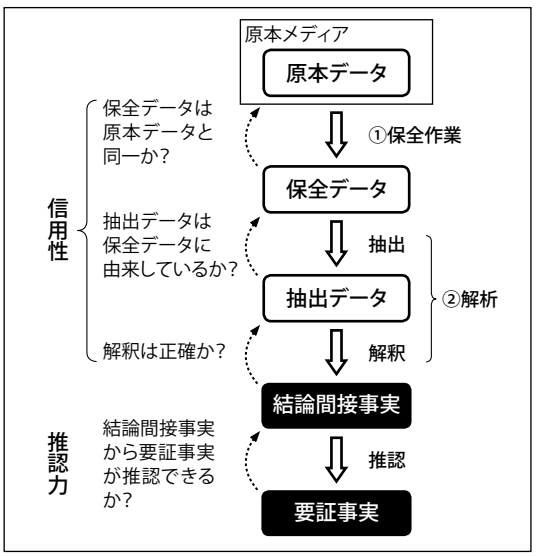
⑷　証拠構造と証明力の判断過程

II4で前述したとおり、フォレンジック報告書における証拠の構造は、原本データ→保全データ→抽出データという過程を経て、抽出データを解釈して、結論間接事実を認定することになる。

ここで「結論間接事実」[40]とは、フォレンジック解析の結果直接認定できる事実であって、たとえば、「当該コンピュータに、脅迫文と同じ文面、メールアドレス、パスワードが記載されたテキストファイルが保存された」というような事実である。結論間接事実から、さらに事案との関係で証明が必要な事実（要証事実）が推認される。たとえば「当該コンピュータの所有者Xが、脅迫文をメールで送信した」といった事実である。

このような、原本データを起点に、結論間接事実、要証事実に至る事実認定の構造は、DNA鑑定などの科学的証拠と共通する。司法研究は、結論間接事実を「i（スモールアイ）事実」、要証事実を「I（ラージアイ）事実」と呼び、それぞれの範囲を厳密に区別する必要性を指摘している[41]。

図表11　事実認定の構造



フォレンジック報告書の証明力については、この事実認定の構造を踏まえて、証拠提出者が主張する要証事実が、原本データまで遡ることができるのかを評価する必要がある。具体的には、後述するとおり、①保全データの同一性、②解析過程の信用性、③結論間接事実の推認力の3点を評価することになる。このうち、①②は、フォレンジック報告書の内容が正

確かという「信用性」の問題であり、③は、解析結果からどのような事実がどの程度の蓋然性をもってあると言えるかという「推認力」の問題である[42]。

上記①～③を、本稿では「証明力評価の３要素」と呼ぶこととする。

⑸　デジタル・フォレンジックに関する従前の議論

ⓐ　ガイドラインと証拠評価の関係

保全作業の手順については様々なガイドラインが策定されており[43]、実務的には、保全作業はこれらガイドラインに準拠して実施されている。

これらのガイドラインは、有効性確保と証拠性確保の両方の目的を達成するために構成されており、有効性確保の観点から定められたルールも多い。したがって、ガイドライン違反が直ちにフォレンジック報告書の証拠能力や証明力に影響するとは限らない。これらガイドラインはフォレンジック調査員にとっての行為規範であるが、事実認定者にとっての裁判規範ではないのである。

ⓑ　米国証拠法上の概念について

デジタル・フォレンジックの文献において、しばしば、証拠性の確保のために「保管の連続性」（Chain of Custody）が必要であるとされることがある[44]。

保管の連続性は、米国法に由来する概念である。物証の証拠能力について、同一性が必要とされているところ、物証に顕著な特徴があればそれだけで同一性が認定され、そうでない場合には、証拠物の保管の連続性を証明しなければならない、というものである[45]。

保管の連続性は、米国法の物証に関する規律であるから、日本法におけるデジタル・フォレンジックの規律においてこれを参照する必然性はまったくない[46]。有体物としてのハードディスクの保管が連続しているよりも、ハッシュ値の確実な記録によりデジタルデータとしての論理的同一性を立証することの方が、デジタルデータの証拠性確保のためには重要であることは論を俟たない。

また、デジタルデータ自体の証拠能力につき、最良証拠法則（Best Evidence Rule）を参照して原本性が議論されることがあるが、⑵で前述したとおり、デジタル・フォレンジックの手法が適用されている限り、実際に問題となることはないだろう。

デジタル・フォレンジックは主に米国で発展してきたものであり、これに附随して米国法の概念が直輸入的に紹介されたことはやむをえない面があるが、日本法にこれら米国法の概念を導入する必要性の検討が十分になされたとは言いがたいように思われる[47]。

⑹　小括

以下、まずは①保全データの同一性、②解析過程の信用性、③結論間接事実の推認力、という、証明力判断のための３要素について検討した上で（**2**～**4**）、司法研究で示された科学的証拠の評価基準との関係を確認する（**5**）。それを前提として、証拠能力についての個別論点に若干の検討を加える（**6**）。

2　保全データの同一性

⑴　保全データの同一性とは

デジタル・フォレンジックでは、保全データを対象に解析を実施する。解析の対象となった保全データは、保全作業時に原本ディスクに記録された原本データと、同一でなければならない。これを保全データと原本データの同一性ということができる[48]。

ここでいう「同一」とは、デジタルデータとしての同一性である。デジタルデータの特徴のひとつとして、完全なコピーを作ることができることが挙げられるが（完全一致性）、そのような「完全なコピー」であることが求められるのである。

より具体的に言うと、以下のとおりである。２個のデジタルデータについて、2進数の桁数が同じで、かつ、対応する桁の０と１がすべて同じである場合、これらは同一であるといえる。同一のデジタルデータは、コンピュータ処理において、まったく同じように振る舞い、区別ができない。このような意味のデジタルデータの同一性を、物証における同一性（物理的同一性）と区別するために、論理的同一性と呼ぶこととする。

たとえば「0100」と「0100」は論理的に同一である。どちらも４桁であり、すべての桁の０と１が一致するからである。大きな桁数（bit数）のデジタルデータも同様に考えることができる。

保全データは、原則として[49]、原本データと同一でなければならないし、証拠提出者は、同一性を証明する必要がある。

⑵　ハッシュ値

それでは、保全データの同一性は、どのように認識・

証明すればよいだろうか。ここで使われる技術が「ハッシュ値」である。ハッシュ値は、「フォレンジック技術の中核」[50]ともいうべき重要な概念である。

ハッシュ値[51]については、「ハッシュ値とは、電子ファイル等の電子データを一定の計算式（ハッシュ関数）により演算し、文字列に変換した値であり、電子データの一部でも変更されていると、異なるハッシュ値を示すため、電子ファイルの特定手法としても利用されるものである」と説明した裁判例がある（東京地判平16・6・8判タ1212号297頁）[52]。

(a)　具体例

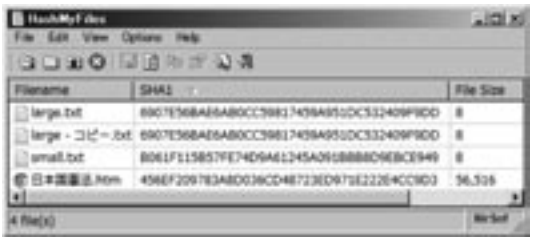
ハッシュ関数（ハッシュ値の計算の仕方）にはいろいろな種類があるが、有名なものとしてMD5やSHA-1がある。SHA-1を利用した論理的同一性の判断について、具体例を示す。

まず、テキストファイルを3つ用意する。それぞれのファイル名と実データは、以下のとおりとしよう。

	ファイル名	実データ
①	large.txt	Forensic
②	large - コピー.txt	Forensic
③	small.txt	forensic

この3つのファイルについて、フリーソフト[53]を利用してハッシュ値を計算した結果が、図表12である。「SHA1」と書いてある欄にハッシュ値が表示されている。

図表12　SHA-1ハッシュ値を計算した画面



このように、あるデータに対するSHA-1ハッシュ値を計算すると、それは元のデータ（これを「メッセージ」と呼ぶ）の大きさに関係なく、16進数で40桁（2進数で160桁＝160ビット）の数字が出てくる。図表12で、「日本国憲法.htm」は、大きなサイズのデジタルデータであっても、ハッシュ値は同じ長さとなることを示すために、あわせてハッシュ値を計算したものである。

同じメッセージから計算したSHA-1ハッシュ値は、必ず同じ数字となる。逆に、異なるメッセージでSHA-1を計算すると、たとえそれが1bitの違いであっても、違うハッシュ値が計算される。厳密には、異なるメッセージから同じハッシュ値が計算されることが、極めて小さな可能性で起こりうるが、適切なハッシュ関数を利用している限り、(3)(a)で後述する性質から、そのような可能性は事実上無視して差支えない。

したがって、以下のように判断できる。

①ハッシュ値が同一→メッセージが同一

②ハッシュ値が異なる→メッセージは同一ではない

上記の例では、データ①とデータ②で、同じハッシュ値が計算されているので、実データを見なくとも、実データは同一であると判断できる。なお、ファイルのハッシュ値を計算する場合、実データを対象とするので、ファイル名やタイムスタンプ等のメタデータはハッシュ値に影響しない。データ①とデータ②で、ファイル名は異なるが、ハッシュ値は変わらない。

また、データ①とデータ③は、ファイル冒頭の「F」と「f」の一文字が違うだけだが、まったく異なるハッシュ値となっており、論理的同一性がないこと（違うデジタルデータであること）が、実データを見なくとも判断できるのである。

(b)　ハードディスクのハッシュ値

保全作業でハッシュ値を計算するときは、前述の例とは異なり、ファイルではなく、ハードディスク全体に対するハッシュ値を計算する。ハードディスクには、膨大な桁数のデジタルデータ――たとえば100GByteのハードディスクであれば、約8600億桁の2進数――が記録されているのは、**Ⅲ1(2)**(a)で前述したとおりだが、その約8600億桁の2進数をメッセージとして、ハッシュ値を計算するのである。

ハードディスク上の全データであっても、ファイルの実データであっても、有限桁数の2進数という点では変わらないので、同じようにハッシュ値が計算できるのである。

(c)　ハッシュ関数の種類

ハッシュ関数には様々な種類があり、MD5とSHA-1が有名である。しかし、MD5は安全性に疑問が生じてきており（(3)(a)参照）、SHA-1もそれほど遠くない将来に同様の問題が起こると考えられている。

今後は主に、電子政府推奨暗号リスト[54]で推奨されている、SHA-2[55]と呼ばれる、より強い安全性を

持つハッシュ関数への移行が進むものと思われる[56]。

(d) ファイル・コンペア

2つのデジタルデータの最初から最後まで、0と1が同じように並んでいるのかを一桁ずつ確認していくという方法があり、ファイル・コンペア(比較)と呼ばれている[57]。

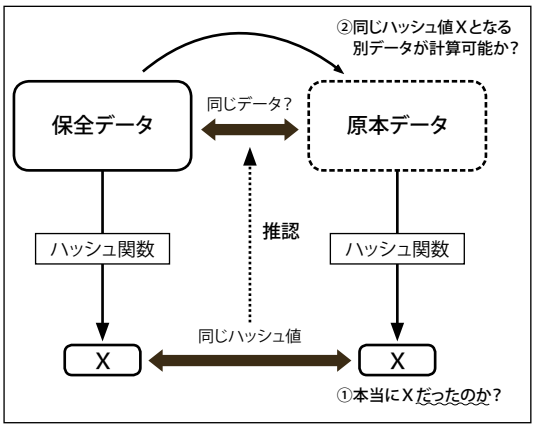
コンペアはわかりやすい手法だが、ハッシュ値と比べると2つの欠点がある。同時に存在するデジタルデータ同士についてしか論理的同一性を判断できないことと、コンペア結果を偽ることが容易であり、虚偽の可能性を完全には排除できないことである。ハッシュ値に代えてコンペアを利用することに、合理的な理由はないと考えられる[58]。

(3) 保全データの同一性の認定と弁護人の対応

保全データの同一性を主張する検察官としては、ⓐ保全作業時、原本データのハッシュ値はXだった、ⓑ解析の対象とした保全データのハッシュ値はXだった、という2つの事実を主張し、これが認められると、原本データと保全データの論理的同一性が極めて強く推定されることになる。

これに対して考えられる反論は、①ⓐの事実を否認するか、②上記事実上の推定を覆すかである。

図表13 保全データの同一性と弁護人の主張



(a) ハッシュ関数の脆弱性

まず、推定を覆す事実について検討する。

仮に捜査機関側が解析結果を偽造することを考えると、偽造保全データを作成し、これを対象に解析を実施して、フォレンジック報告書を作成することになる。

原本データのハッシュ値(=真実の保全データのハッシュ値)がXであるとすると、論理的同一性のない偽造保全データのハッシュ値はこれとは異なるYになることが一般的である(このようにハッシュ値が異なる場合、保全データの同一性が証明できない)。しかし、原本データと異なるが、同一のハッシュ値を有する別のメッセージ(データ)は存在し、これを計算することは、時間が無尽蔵にあれば可能である。ただ、あまりに膨大な時間がかかるので、現在利用できる技術では、そのような別メッセージを計算することは事実上不可能なのである。これはハッシュ関数の「弱衝突困難性」という性質である[59]。

逆に、弱衝突困難性を満たさないハッシュ関数は、同一のハッシュ値であるからといって、メッセージが同一であるとは限らない。たとえば、偽造保全データのある領域をランダムに書き換えてハッシュ値を計算していき、原本データのハッシュ値Xと同じハッシュ値を持つ偽造保全データを得るという方法が考えられる[60]。

したがって、ハッシュ関数に脆弱性が存在し、現実的な方法で弱衝突困難性を突破できるのであれば、上記推定を覆す事情となる可能性がある。捜査機関側としては、このような主張への予防策として、十分な安全性のあるハッシュ関数を利用する必要がある。

(b) ハッシュ値は保全作業時に計算されたものか

証拠偽造を達成する手段として、上記の弱衝突困難性の突破より簡単なのは、偽造保全データのハッシュ値を計算して、事後的に、原本データのハッシュ値とすり替えることである。たとえば、保全作業経緯を記載した捜査報告書を、日付を遡及して事後的に作成し、後日計算した偽造保全データのハッシュ値を記載する、といった方法が考えられる。

したがって、弁護人としては、保全作業の当日に計算されたハッシュ値が適切に記録化されていたかどうかを検討する必要があり、場合によってはこれを否認することになるだろう。

捜査機関としては、そのような争点が生じないように、確実な方法で(捜査機関がその気になっても偽造が不可能だったと証明できる方法で)ハッシュ値を証拠化しておく必要がある。フォレンジック業者の保全作業では、その全過程をビデオ撮影することが多く、そこにハッシュ値が撮影されていれば、これを後日偽造することは事実上不可能であろう。また、被

疑者・弁護人（民事訴訟の場合は対立当事者）にハッシュ値を通知しておくことも考えられる[61]。

⑷　改変可能性の評価

このように、保全データの同一性に疑義が生じないようにするためには、捜査機関（あるいはフォレンジック業者）がハッシュ値を確実な手段で証拠化しておき、保全データのハッシュ値と照合すればよい。

この点について必要な措置が取られなかった場合――たとえば、①MD5によるハッシュ値しか取得していない、②原本データのハッシュ値について改変可能な信用性の低い証拠（捜査報告書等）しか存在しない、③保全データが開示されない（保全データが消滅した場合を含む）といった場合には、デジタルデータは改変可能だったということになり、少なくとも抽象的には改竄の疑義が生じる。そして、具体的に改竄が行われた証拠までは存在しない場合、裁判所は困難な判断を迫られることになる[62]。

これは、デジタル・フォレンジック特有の問題ではなく、デジタルデータのプリントアウトを証拠として提出するような場合と共通する問題で、要はデジタルデータの改変可能性を、証拠評価においてどの程度考慮するかということに帰着する。

従前の考え方としては、改竄の抽象的な疑念が生じたに過ぎない場合に、デジタルデータが改変可能だからといって証拠能力や証明力を否定するという判断がなされることはなかったと思われる[63]。このような判断は、デジタルデータに関する証拠を提出する弁護士や企業が、そのようなデータの改竄に及ぶことはないだろう――ましてや捜査機関の客観的証拠の偽造などありえない――という、一定の信頼感に基づく判断だったといえよう。

とすると、現時点においては、厚労省FD改竄事件という、検察官の客観的証拠偽造が明白に立証された事例が出現したとしても、なお、この信頼感が維持できるのかということが検討される必要があるだろう。これを、ごく例外的な、個人的な非違行為でしかないと評価すれば、改竄の可能性を無視することになろうし、今後類似の事例が起きる可能性が否定できないと考えるのであれば、安易に信用性を認めるべきではないことになる。

また、フォレンジック報告書の特殊性として、上記の改変可能性の観点のほか、改竄された場合の弊害の大きさも留意されるべきである。

他の科学的証拠は、その証明の対象が一定の事項に限られるが（たとえば、DNA検査は、個人の識別・同定のみを対象とする）、デジタル・フォレンジックは、コンピュータに記録されている事項はすべて証明の対象となりうる。したがって、万が一恣意的な介入がなされた場合は、極めて重要かつ広範な影響を与えうるのである。

3　解析過程の信用性

解析過程においては、保全データから意味のあるデータ（抽出データ）を抽出し、これに解釈を加えることで、結論間接事実（i事実）を認定する。

ここで必要な条件は、①抽出データが保全データに由来し、かつ、②抽出データの解釈が正確なことの2点である。

⑴　抽出データと保全データの関連性

抽出データは、保全データに何らかの論理的操作を加えてその結果得られたものでなければならない。これを、抽出データと保全データの関連性と呼ぶことができる。

たとえば、削除データの復元は、削除ファイルの実データが保全データのどの領域に存在するのかを（可能な限り）特定して、並び変える作業である。多くの場合、保全データに加えられる操作は、保全データのうち特定領域の抽出であり、抽出された断片データの結合ということになろう。また、圧縮ファイルや暗号化されたデータのように、一定の計算式に従って変換を実施している場合もある。

保全データの関連性を示すためには、一般的な、恣意的ではない操作によって抽出データが生成されていることを示せば足りる。これは、一般的な解析ソフトを利用している限り、容易に立証できることが通常であろう。

⑵　解釈の正確性

抽出データの解釈は、様々なデータ形式で記録された抽出データの意味するところを、明らかにする作業である。PCで利用されるデータ形式は、多くの場合、一般的な形式であり、かつ、仕様が公開されているので、解釈の正否が問題になることは少ないと考えられる。ソフトによっては仕様の公開されていない独自の形式でデータを保存することがあり、データ

形式の解析が必要になる場合もある。

解釈の正確性についても、保全データの関連性と同様に、解析ソフトの問題に帰着することが多い。

⑶　弁護人の対応

解析過程は、保全データがそのまま（原本データとの同一性を保ったまま）記録されている限り、何度でも再現可能である。これは、分析の対象となる試料が限られている他の科学的証拠と顕著に異なる特徴である。

また、抽出データの抽出と解釈という実際の作業は、解析ソフトが自動的に実行する。したがって、通常、⑴および⑵の評価は、適正な解析ソフトが正しく用いられているかという点に帰着する。

以上から、解析過程の信用性について検討するには、保全データ（ハッシュ値で特定される）の開示を受け、解析ソフトで、解析過程が再現できるかどうかを確認することが最も直截な方法ということになろう。

4　結論間接事実の推認力

⑴　現実世界との接点

抽出データから解釈される結論間接事実は、すべて当該コンピュータ内の出来事であり、これと現実世界の事実を区別する必要がある。

たとえば、特定のデータが保存されていた場合、原則として、そのデータはコンピュータの利用者の操作によって作成されたものと考えられるだろう（ただし、遠隔操作プログラムのような例外もある）。次に問題となるのは、潜在的な利用者の特定と、操作した者の識別であり、この点は基本的に通常の事実認定の問題である[64]。

⑵　複数の結論間接事実による認定

図表13は、事実認定のあり方としては、やや単純化しており、実際には、多数の抽出データから多数の結論間接事実が認定され、複数の結論間接事実（○○の痕跡がないという消極的事実も含む）や、コンピュータ外の間接事実をも総合して要証事実が認定される。

そもそも保全作業が実施されておらず（したがって、保全データの同一性が担保されておらず）、改竄が介入した例であるが、厚労省FD改竄事件では、管理領域に記録されたメタデータと、データ領域に記録されたファイル内メタデータの双方にタイムスタンプが記録されており、ファイル内メタデータに改変の痕跡が残っていたとされている[65]。フロッピーディスクという、容量の小さい原始的な記録メディアにおいても、データの一貫性を保ちながら一部のデータを改変することは困難を伴うことがわかる。

PC遠隔操作事件のうち、神奈川県警の事例[66]では、対象PCから、神奈川県のウェブサイトにアクセスしたキャッシュが発見されており、その結論間接事実のみを考慮すると、PC所有者が脅迫文を送ったという要証事実が推認されうる状況だった。しかし、ⓐキャッシュによるとメール送信フォーム画面と送信メール確認画面のキャッシュのタイムスタンプの差が１秒である、ⓑ前述のキャッシュは残っているが、同内容のアクセス履歴は残っていなかった、ⓒ直前に内容不明のURLにアクセスしたアクセス履歴が存在する、といった結論間接事実を考慮すると、要証事実の推認に疑いを入れる余地があったといえよう[67]。

デジタルデータは、ごく狭い範囲のみを考えると、痕跡を残さずに容易に改変が可能であるが（改変可能性）、システム全体（あるいは、ネットワークで接続されるサーバ等に残るデータ）の整合性を保ち、改変の痕跡も残さないことは容易ではない。これを、証拠評価の観点から見ると、単独の結論間接事実の推認力には限界があり、別の抽出データ（結論間接事実）・間接事実の存否を検討する必要があるということになるのである。

5　科学的証拠としての信頼性（６段階・８項目）

司法研究では、科学的証拠の証明力評価の一般的枠組みとして、「６段階・８項目」を挙げている[68]。ここまで本稿で検討した証明力評価の３要素が、この司法研究の枠組みにおいてどの項目に相当するのかにつき、簡単に検討する。

⑴　基礎となる科学的原理・知見の信頼性

デジタル・フォレンジックの基礎となっている原理ないし知見としては、①デジタルデータの特質やコンピュータの仕組みに関する知見、②ハッシュ関数に関する数学的知見の２点が挙げられるだろう。いずれも確度は高く、この項目について問題が生じることはないと言ってよいだろう。

⑵　科学的原理・知見を実用化する理論・技術の信頼性

⑴①の原理・知見の実用化に関しては、主に解析ソフトの信頼性が問題となり、これは⑶⒝と重なる。また、⑴②に関しては、ハッシュ関数の種類が問題となりうるだろう。

⑶　具体的な検査に関する信頼性

⒜　試料化の信頼性

ＤＮＡ鑑定や薬理鑑定等の科学的証拠と異なり、前処理の過程は存在しないと言ってよいだろう[69]。

⒝　具体的検査方法、過程の適格性

証明力評価の３要素のうち、「解析過程の信用性」に相当し、現実的には、解析ソフトの信頼性に帰着することが多い。解析ソフトの信頼性は⑵の問題と捉えられることは、前述したとおりである。

なお、有益な情報が得られる可能性のある解析項目がもれなく実施されているか、という点が問題となるが、これは後記⑸の問題と把握するべきであろう。

⑷　検査者の技術水準、技量[70]

有用性確保の観点からは、フォレンジック調査員の技術水準は極めて重要である。保全作業の手順を誤れば、得られるべき情報が失われることも多いし、解析においても、どの程度の情報が取得できるかは、調査員の技術（および解析ソフトの機能）によるところが大きい。これに対し、証拠評価の観点からは、フォレンジック調査の結果が正しいかどうかは、調査員の技術とは関係なく検証することができるので、調査員の技術水準を問題とする場面は限られる。

調査員の技術水準が問題になる場合として考えられるのは、後記⑸の結論間接事実の推認力を評価する場面である。経験豊富で、技術水準の高い調査員であれば、当該事案で調査すべき項目について調査していない可能性は低いと評価される可能性がある。

もっとも、デジタル・フォレンジックの歴史が浅いこともあり、専門知識の体系化や人材育成の制度化は不十分な段階にとどまっており[71]、裁判所が調査員の技術水準を正しく評価することは極めて困難と思われる。

⑸　検査結果の評価に関する信頼性

「結論間接事実の推認力」として論じたところが、本項目に相当する。

なお、司法研究では、⑸⒜評価に関する原理・基準の信頼性、⑸⒝当該ケースへの当てはめの信頼性の２項目に分けて論じている。

⑹　検査資料の適正（資料の収集、移動、保管過程の適切さ）

デジタル・フォレンジックで「検査資料」に相当するのは、原本データからコピーされた保全データである。したがって、この項目は、「保全データの同一性」の問題である。物理的な資料では、「資料の管理過程」[72]が問題になるが、デジタル・フォレンジックでハッシュ値による論理的同一性の確保・立証がこれに対応する。

６　証拠能力

まず、刑事訴訟法においても、弁護人・被告人が同意をすれば、証拠能力が肯定される（刑訴法326条）。証明力の３要素について検察官から十分な開示と説明がなされるのであれば、同意によって証拠能力が付与されることがほとんどであろう。

同意がない場合、以下のような観点から証拠能力の有無が問題になるが[73]、概ね、証明力の３要素の立証に帰着すると言えよう。

⑴　伝聞法則

フォレンジック報告書は、伝聞証拠であるから、原則として証拠能力がない。伝聞例外と呼ばれる証拠能力を取得する特別の条件を満たす必要があるが、刑訴法321条４項により、書面作成者が「真正に作成されたもの」であることを証言することが必要になる[74]。これは①名義の真正および②記載の真正の両者を含むとされている。①は、当該書面を証人が作成したことであり、②は、鑑定した内容を正しく記載したことを指し、この両方を、フォレンジック報告書の作成者が証言することになる。

②記載の真正について、作成者は、フォレンジック調査の作業内容を、そのまま正確に書面化したという点について証言し、反対尋問を受ける。この証人尋問の手続は、実質的には、証明力の３要素の審理とほぼ重なると思われる。しかし、書面作成者の証人尋問は、保全データの事前開示や解析過程の再現といった、法廷外での事実確認と比べると、３要素を解明する手段としては迂遠であり、補助的な役割にとどまると考えられる。

(2) 科学的証拠の許容性（関連性）

証拠能力の要件として、関連性が必要と解釈されているところ、科学的証拠については、関連性を認めるためには特別の要件が必要となるという見解がある[75]。

たとえば、成瀬論文は、科学的証拠の関連性を認めるために、図表14左欄の項目が必要とする[76]。これは、項目としては、司法研究の「6段階・8項目」にほぼ対応していることは明らかだろう（図表14右欄）。

図表14　成瀬論文と司法研究の判断枠組み

成瀬論文	司法研究
(1) 原理・方法の信頼性	(1) 基礎となる科学的原理・知見 (2) (1)を実用化する理論・技術
(2) 当該事案における検査過程 a 専門家の知識・経験 b 検査機器の正確性 c 具体的な検査方法の適切性 d 検査資料の真正性・同一性	(4) 検査者の技術水準、技量 (3) 具体的な検査に関する信頼性 (6) 検査資料の適正
(3) 導出された結論の評価	(5) 検査結果の評価に関する信頼性

成瀬説と司法研究の違いは、司法研究が原則として証明力の問題とするのに対し[77]、成瀬説は証拠能力（関連性）の問題と把握するところにある。つまり、成瀬説に従うと、フォレンジック報告書の証明力の3要素に問題がある場合、証明力を低く評価されるに留まらず、証拠能力を欠く場合もあるということになろう[78]。

証拠能力の問題として把握することの当否について、本稿は立ち入らない。この問題は、証拠評価を証明力と証拠能力でどのように切り分けるかという大きな問題の一場面であると言えるが、**7**(2)で後述する点は、デジタル・フォレンジック独自の着眼点として、検討の余地があろう。

7　まとめ

(1) 証拠評価のポイント

前述した証明力の3要素のうち、①保全データの同一性と②解析過程の信用性の立証までは、結論間接事実（司法研究の「i事実」）の認定にかかる部分であり、③結論間接事実の推認力は、要証事実（司法研究の「I事実」）の認定に関する。この2つの段階に応じて、証拠評価で考慮すべき事項の性質に大きな違いがあるように思われる。

(a)　結論間接事実の認定

結論間接事実の立証（上記①②）は比較的容易であり、紛れが少ないと言えよう。①は、適切なハッシュ関数によるハッシュ値を確実に記録するということに尽きるし、②は、一般的なの解析ソフトを用いる限り、問題が生じることは稀であろう。

この段階における課題は、まず、捜査機関（あるいはフォレンジック業者）がやるべきことをやるということである。そして、捜査機関の手続に問題があった場合にのみ、裁判所がそれをどう評価するかという問題が生じることになる（①保全データの同一性については、**2**(4)で前述した）。

(b)　要証事実の認定

これに対し、要証事実の認定、すなわち③結論間接事実の推認力の評価は、困難な作業となる可能性がある。

解析の結果、ある結論間接事実が得られ、そこから要証事実を容易に推認できるように見えても、保全データの中に、かかる仮説を否定するデータが埋もれていたり、仮説が成立するのであれば当然あるべき痕跡が存在しないということがあり、その確認を怠ると、誤判を招く危険性がある。このような観点から間接事実の推認力を評価するためには、コンピュータのシステム全体の挙動について広範な知識が必要となる。

保全データの持つ情報は膨大であり、千差万別でありうる。したがって、結論間接事実の推認力評価の段階においては、具体的なデータのありように応じて様々な問題が生じうるが、現時点においてはその輪郭を明らかにすることさえ困難である[79]。PC遠隔操作事件は、いくつかの検討素材を提供したものであるが、それで問題が尽きていると考える理由はない。

もし、刑事弁護において、デジタル・フォレンジックにより決定的な証拠があると捜査機関が主張しているが、被疑者はまったく身に覚えがないとしている事案があったとする。弁護人は、まず、保全作業や解析過程に問題がないかを確認する必要があるのはもちろんであるが、結論間接事実の推認力評価として、いかなる仮説が成り立ちうるのか、専門家の助力を得ながら幅広く検討しなければならないだろう。

仮に被疑者が嘘をついていないのであれば、そこに活路があるはずである。

⑵　証拠開示の重要性

司法研究は、科学的証拠の証拠開示を重視し、開示の範囲として「鑑定経過を含め、科学的証拠に関する再現可能性の検討が可能な程度のデータが開示されるべきである」としている[80]。

フォレンジック報告書に関しては、①保全作業の過程の記録、②解析の対象となった保全データ自体、③解析過程の記録の３点が開示の対象となる[81]。

そして、一般的に上記のような事項を開示することは、容易であり、少なくとも公判段階においては、開示の支障となる事情はほとんど考えられないであろう[82]。一般的な科学的証拠においては、分析の対象となった試料（たとえばＤＮＡ鑑定における細胞片）そのものを開示することは困難な場合が多いが、デジタル・フォレンジックでは容易である[83]。保全作業が完了した後の解析過程については、完全に再現可能であることが、デジタルデータを対象とするデジタル・フォレンジックの大きな強みである。

したがって、デジタル・フォレンジックでは、他の科学的証拠と比べても、証拠開示の必要性は高く、その障碍もほとんどないと言える。そして、証拠開示がなされなかった場合には、証明力の３要素の立証が困難となり、証明力に影響することはもちろんであるが[84]、さらに、証拠能力についても検討の余地があると考えるべきであろう。

1　デジタル・フォレンジックについて詳細に論じた邦語文献としては、マイケル・Ｇ・ソロモンほか（AOS法務IT推進会訳、佐々木隆仁ほか監修）『コンピュータ・フォレンジック完全辞典』（幻冬舎ルネッサンス、2012年。以下、「辞典」という）と辻井重男監修『デジタル・フォレンジック事典』（日科技連、2006年。以下、「事典」という）が挙げられる。また、佐々木隆仁『デジタルデータは消えない』（幻冬舎ルネッサンス新書、2011年）は、入門書として好適であり、技術的な側面についてわかりやすく解説した文献として大徳達也「捜査官のためのデジタル・フォレンジック入門　第１回～第６回」捜査研究744～749号（2013年）がある。

2　Mark Pollitt “Computer Forensics: an approach to evidence in cyberspace” (http://www.digitalevidencepro.com/Resources/Approach.pdf)は、「デジタル証拠に関する法的問題への科学と技術の適用」（日本語訳は筆者による）と定義している。また、広く引用される定義として、「インシデント・レスポンスや法的紛争・訴訟に対し、電磁的記録の証拠保全及び調査・分析を行うとともに、電磁的記録の改竄・毀損等についての分析・情報収集等を行う一連の科学的手法・技術」という、デジタル・フォレンジック研究会の定義がある（事典４頁）。なお、「インシデント・レスポンス」とは、コンピュータ・セキュリティ分野の用語で、不正アクセス等のセキュリティ上の脅威への対応を指す。

3　白石陽ほか「フォレンジック技術を利用した携帯端末のための証拠保全手法」情報処理学会論文誌54巻１号（2013年）91頁が、概略を説明している。また、問題点を指摘し、メーカーとの協力等の方針を概説した文献として、野本靖之「ネットワーク利用形態の多様化とデジタルフォレンジックの課題」警察政策12巻（2010年）227頁を参照。

4　町村泰貴ほか編著『実践的ｅディスカバリ――米国民事訴訟に備える』（ＮＴＴ出版、2010年）。

5　特定非営利活動法人デジタル・フォレンジック研究会「証拠保全ガイドライン〔第３版〕」（http://www.digitalforensic.jp/eximgs/20130930gijutsu.pdf）（以下、「ＩＤＦガイドライン」という）60頁参照。同ガイドラインは、主にネットワークフォレンジックに対応するために改訂された。

6　IDFガイドライン60頁参照。

7　鈴木一郎＝岩井博樹「事例報告⑨デジタルデータ（フロッピーディスク）分析　厚労省事件」本誌71号（2012年）60頁、朝日新聞取材班『証拠改竄　特捜検事の犯罪』（朝日新聞出版、2011年）。

8　平成23年3月31日「検察の再生に向けて　検察の在り方検討会議提言」（http://www.moj.go.jp/kentou/jimu/kentou01_00001.html）。

9　2013（平成25）年２月には、これら事件の遠隔操作の実行犯とされる被疑者が逮捕され、現在、公判整理手続が続行中である。

10　たとえば、「科学的捜査への取組」法律のひろば66巻５号（2013年）２頁、吉田久「研修の現場から」研修782号（2013年）91頁参照。

11　デジタル・フォレンジックに関する文献において、「証拠性の確保」（たとえば事典５、24、110頁）、「証拠性保持」（守本正宏「危機管理とデジタル・フォレンジック」警察政策８巻（2006年）57頁〔68頁〕）といった言葉が、明確な定義が与えられないまま使われることがある。おおよそ、本文に述べたような意味で用いられているようである。

12　法律上は、電磁的記録（刑法７条の２、電子署名法２条等）という概念が用いられるが、「電磁的記録とは、一定の記録媒体上に情報あるいはデータが記録、保存されている状態を表す概念であって、情報あるいはデータそれ自体や記録（記憶）媒体そのものを意味するものではない」（米澤慶治編『刑法等一部改正法の解説』〔立花書房、1988年〕61頁。傍点は引用者）とされており、デジタルデータとは一応区別された概念である。

13　２進数でデジタルデータを表記すると長くなるので、短縮のために16進数で表記することが多い。16進数は、０～９、Ａ～Ｆまでの合計16個の数字を使う。16進数は、あくまで桁数を減らすために２進数の代用として用いられるもので、16進数の

数字が出てきたら、これは2進数、0と1の羅列を縮めて書いているのだと理解するとよい。文字とデジタルデータの対応を確認しておくと、2進数で冒頭の8桁「01000110」、16進数で「46」という数字に、「F」という文字が割り振られている。以下、16進数で「6F」が「o」、「72」が「r」というように続く。

14 権限のない者による、あるいは不当な改変を指して「改竄」という場合が多い。本稿では権限の有無を区別する必要のない場合は「改変」との用語を使う。なお、一般に、デジタルデータの改変には、消去も含まれる。

15 佐々木・前掲注1書14〜21頁参照。

16 守本・前掲注10論文は、⑴証拠保全、⑵解析、⑶報告、としている。⑶については、独立した項目として検討するに足るデジタル・フォレンジック独自の問題がないことから、本稿では省略した。IDFガイドライン2頁では、⑴収集、⑵検査、⑶分析、⑷報告、という4段階モデルを紹介している。本稿の立場と比べると、⑴が①保全作業、⑵⑶が②解析に対応する。⑵⑶を区別する実益はあまりないように思われる。

17 辞典178〜218頁、大徳達也「捜査官のためのデジタル・フォレンジック入門　第6回　証拠保全の基礎知識」捜査研究749号（2013年）44頁。なお、しばしば用いられる「証拠保全」という用語は（たとえば、IDFガイドライン）、刑事訴訟法及び民事訴訟法上の証拠保全手続（刑訴法179条、180条、民訴法234〜242条）と区別するためには、望ましくないといえよう。

18 1ギガバイトは、1024^3=1,073,741,824バイトであり、ビットに換算すると約86億ビット（2進数で約86億桁）ということになる。

19 事典88〜95、144〜156頁、辞典82〜87頁。

20 厳密には不正確で、たとえば、FATでは、データ領域に位置データの一部が記録される。事典144〜156頁参照。

21 ここまでの説明では割愛しているが、実際のファイルシステムでは、「セクタ」や「クラスタ」という単位でデータの位置が指定される。セクタは通常512バイトであり、クラスタは複数のセクタから構成される。

22 ドライブレターという。なお、Cから始まっているのは、フロッピーディスクに「A:」「B:」が使われていた名残である。

23 ただし、論理コピーの際にも、個々のファイルごとにハッシュ値を取得することで、原本ディスクに記録された情報（削除ファイルの情報を除く）がそのまま保存されていることを証明することはできる。

24 CD-ROMやUSBメモリを利用して対象コンピュータを専用のOSで起動し、USB等でコンピュータに接続したハードディスクにデータをコピーする方式。専用OSを利用することで、ハードディスクに追加の書き込みが生じないような仕組みとなっている。

25 保全ガイドライン49頁。「CoC」は「証拠保管の連続性（Chain of Custody）」に由来する。後述**Ⅳ1(5)**(b)を参照。

26 事典144〜161頁、佐々木・前掲注1書21〜26頁、大徳達也「捜査官のためのデジタル・フォレンジック入門　第1回　削除ファイルの復元」捜査研究744号（2013年）20頁。

27 たとえば、加藤新太郎編『民事事実認定と立証活動』（判例タイムズ社、2009年）175頁［山浦善樹発言］。

28 Windowsで使われているファイルシステムFATの場合、メタデータの先頭（ファイル名が記録されている）にE5（16進数）を書き込むことになっている。したがって、ファイル名の先頭の文字が失われる場合もある。

29 大徳達也「捜査官のためのデジタル・フォレンジック入門　第4回　ウェブの仕組みとアクセス記録」捜査研究747号（2013年）49頁。

30 これらの情報が事実認定に大きな影響を及ぼしうることは明らかである。他方、Exif情報は容易に改変できるので、デジタル・フォレンジックの手法を用いない場合には、裁判所の判断を誤らせる危険性もあり、注意が必要である。

31 辞典264〜304頁。

32 検索の種類としては、事前にインデックス（目次）を作成して高速に検索を実行するインデックスサーチと、データをすべて確認していくライブサーチがある（事典55頁）。

33 ハードディスク中のファイルごとのハッシュ値を計算し、解析ソフトのメーカが提供している既知のファイルのハッシュ値のリストと一致するものを排除する、という仕組みである。

34 松本時夫ほか『条解　刑事訴訟法〔第4版〕』（弘文堂、2009年）809頁、819頁、門口正人ほか編『民事証拠法大系第1巻』（青林書院、2007年）218頁。

35 当事者が依頼した私的鑑定の証拠能力を否定する見解があるが、実務上は採用されていない。秋山幹男ほか『コンメンタール民事訴訟法Ⅳ』（日本評論社、2010年）289頁参照。

36 デジタルデータやこれを出力した書面の証拠能力や原本性が議論されることがあるが（たとえば、事典236頁、安冨潔『ハイテク犯罪と刑事手続』〔慶應義塾大学法学研究会、2000年〕261頁、平野龍一ほか編『続刑事訴訟法』〔青林書院、1980年〕317頁「磁気テープの証拠能力」［原田國男執筆］、石井夏生利「電磁的記録の法的地位」InfoCom REVIEW Vol.39〔2006年〕86頁）、デジタル・フォレンジックの手法が利用されている場合は、問題にならない。

37 司法研究所編『科学的証拠とこれを用いた裁判の在り方』（法曹会、2013年。以下、「司法研究」とする）。

38 本稿では、とくに、英米法の詳細緻密な分析に基づき科学的証拠の許容性基準を示した成瀬剛「科学的証拠の許容性㈠〜㈤」法協130巻1号〔2013年〕1頁、2号〔2013年〕386頁、3号〔2013年〕573頁、4号〔2013年〕801頁、5号〔2013年〕1025頁（以下、「成瀬論文」という）を参照した。

39 たとえば、司法研究4頁は科学的証拠の具体例を列挙しているが、デジタル・フォレンジックは挙げられていない。また、デジタル・フォレンジック関係の文献でも、従前の「科学的証拠の許容性」の議論を意識した論述はあまり見られないようである。これは、現実問題として、フォレンジック報告書の証拠能力が争われる例が少なかったことを反映していると考えられる。

40 成瀬論文⑸1036頁では、結論間接事実を指して、「間接事実」と呼んでいる。しかし、これと対比される要証事実は、主要事実に限られず間接事実の場合もあることから、ここで「間接事実」と「要証事実」という用語を用いると、一般的な間接事

実の用法と齟齬が生じうること、また、要証事実に間接事実が含まれることと整合しないと考えられることから、「結論間接事実」という言葉を用いることとした。

41 司法研究19～20頁。また、成瀬論文⑸1036、1043頁を参照。

42 石井一正『刑事実務証拠法〔第５版〕』(判例タイムズ社、2011年) 444頁、司法研究55、57頁、成瀬論文⑸1067頁脚注⑿参照。石井および司法研究は、推認力を「狭義の証明力」と呼ぶが、刑訴法318条の用語である「証明力」との混同を避けるため、成瀬論文の用語法に従った。

43 邦文のものとしてIDFガイドライン (前掲注１) がある。また、英文のガイドラインについては、関根廣行「警察におけるデジタルフォレンジック」警察政策10巻 (2008年) 242頁を参照。以下に、邦訳があるものを挙げておく。「証拠収集とアーカイビングのためのガイドライン」(http://www.ipa.go.jp/security/rfc/RFC3227JA.html)、「インシデント対応へのフォレンジック技法の統合に関するガイド」(http://www.ipa.go.jp/files/000025351.pdf)。

44 IDFガイドライン27頁、辞典121、131頁、事典110頁。

45 成瀬論文⑵403頁。ほかに証拠保管の連続性について詳しく述べた文献として、野々村宣弘「刑事訴訟における証拠の真正性に関する一考察」法と政治43巻３号 (1992年) 173頁、光藤景皎「証拠の関連性について」法学雑誌38号３・４号 (1992年) 762頁 (『刑事証拠法の新展開』〔成文堂、2001年〕所収１頁以下)。

46 物証 (有体物) について「保管の連続性」を参照することは、別論である。司法研究61頁は、検査試料 (物証) の「資料の管理過程」を検討している。

47 民事・刑事を問わず、証拠法は、書証・物証といった物理的証拠を前提に発展してきた。デジタルデータを証拠法上どのように扱うかという問題は、従前の証拠法と整合性を可能な限り保ちながら、デジタルデータの特質を踏まえた解決を採用するという、困難な課題である。安易に米国法概念を援用することは、さらなる混乱の原因を持ち込むことにもなりかねず、避けるべきであろう。

48 守本・前掲注10論文62頁は、Target Drive (TD) のデータとEvidence Drive (ED) のデータの同一性の確保と証明が重要であるとしている。TDは、本稿のいう原本ディスクを指し、本稿とほぼ同旨である。その他に、「同一性」という用語を使用している例として、事典111頁、IDFガイドライン37頁。一般的に、デジタルデータに改変がないことを「完全性」という (総務庁 (現総務省) 共通課題研究会「インターネットによる行政手続の実現のために」〔平成12年３月〕)。したがって、保全データと原本データの同一性を指して、「保全データの完全性」と言うことができる。

49 例外的な事例として、保全作業時に、不良セクタの影響等により、原本データのハッシュ値と保全データのハッシュ値が一致しないことはありうる。この場合も、少なくとも、保全作業時の保全データと、解析の対象とした保全データの同一性は、ハッシュ値により立証可能であるし、保全作業の状況が証拠化されていれば、それで十分であろう。IDFガイドライン24頁参照。

50 町村ほか・前掲注４書92頁。

51 ハッシュ値およびハッシュ関数については、結城浩『新版暗号技術入門――秘密の国のアリス』(ソフトバンククリエイティブ、2008年) 176頁、盛合志帆「ハッシュ関数の安全性に関する技術調査報告書」(http://www.cryptrec.go.jp/estimation/rep_ID0213.pdf) 参照。

52 ファイル共有ソフト「WinMx」に関して、公開されたファイルと被告が主張する個人情報が含まれたファイルの同一性を肯定した事例。東京地判平16・１・14判タ1152号134頁も参照。

53 様々なソフトが利用可能だが、HashMyFiles v1.95 (http://www.nirsoft.net) を利用した。

54 「電子政府における調達のために参照すべき暗号のリスト (CRYPTREC暗号リスト)」の公表 (http://www.soumu.go.jp/menu_news/s-news/01ryutsu03_02000038.html)。

55 SHA-256、SHA-384、SHA-512の３つのハッシュ関数をSHA-2と総称する。これらは、SHA-1と同じ構造で、ハッシュ値の桁数を増やすことで安全性を高くしたハッシュ関数である。

56 IDFガイドライン23頁脚注22。

57 事典232頁。

58 ハッシュ値と併用することは、有害ではない。実務上も用いられることがあるが、ハッシュ値が法曹関係者に理解されない場合の保険としての意味合いが強い (事典232頁参照)。

59 弱衝突困難性 (別原像計算困難性) とは、あるメッセージとハッシュ値が与えられた場合、同じハッシュ値を持つ別のメッセージを計算することが計算量的に困難なことをいう (結城・前掲注51書170頁、盛合・前掲注51報告書８頁)。「計算量的に困難」とは、現在の技術では天文学的な時間がかかり、事実上計算を完了させるのが不可能な状況を指す。

60 一般に広く使われていたMD5ハッシュ関数については、そのような攻撃が実際に可能であるとの報告もある。暗号技術検討会「2009年度報告書」(http://www.cryptrec.go.jp/report/c09_kentou_final.pdf) 19頁。

61 捜索差押時に保全作業を実施した場合は、押収物目録交付書に、物件特定事項としてハッシュ値を記載すればよい。また、捜索差押後に保全作業を実施した場合も、ハッシュ値を記載した文書を被疑者または弁護人に交付することが考えられるだろう。ハッシュ値からメッセージを復元することはできないため (不可逆性)、これによって捜査の秘密が害されることはありえない。そのほかに、民間事業者が提供するタイムスタンプサービス (電子計算機を使用して作成する国税関係帳簿書類の保存方法等の特例に関する法律施行規則３条５項２号ハ参照) や電子公証制度 (公証人法62条ノ６～62条ノ８。ただし、捜査機関は利用できない) を利用すること等が考えられる。

62 成瀬論文⑸1062頁は、科学的証拠の証拠能力の要件として、「検査資料の真正性・同一性」を挙げている。この見解によると、保全データの同一性に疑義が生じた以上、証拠能力を否定することになる可能性がある。ただし、成瀬論文のいう「同一性」は、物理的同一性のことであり、本稿の保全データの同一性 (論理的同一性) とは概念が異なる。

63　たとえば、東京地判平17・3・25判タ1213号314頁（ACCS事件）では、検察官が提出したサーバのアクセス履歴の信用性を被告人および弁護人が争ったが、裁判所は（第三者によるログの不正作出の）「可能性をうかがわせる具体的な事情は何ら存在しない上、第三者が被告人のアクセス記録をことさらに作出する必要性もないことから、アクセスログは正確に被告人のアクセスを記録していると認められる」と判断している。

64　ログイン履歴などのコンピュータ内の記録が手がかりになることもあるが、それでも当該IDを誰が使ったのかは別途認定する必要がある。

65　岩井・前掲注7論文65頁。

66　神奈川県警察「横浜市立小学校に対する威力業務妨害被疑事件における警察捜査の問題点等の検証結果」（2012年12月）。なお、本検証結果は、当初神奈川県警のウェブサイトで公表されたが、すぐに削除されてしまった。現在は季刊刑事弁護73号（2013年）149頁に転載されているほか、高木浩光（セキュリティ研究者）の個人ウェブサイトで入手できる（http://takagi-hiromitsu.jp/diary/20130119.html）。なお、PC遠隔操作事件に関する事実認定を論じた文献として、森拓也ほか「遠隔操作ウイルス事件が裁判実務に与える影響について」情報ネットワーク・ローレビュー12巻（2013年）52頁があるが、CSRFを用いた神奈川県警の事例とトロイを用いた他の3件を区別しないで論じていること、個別の事件でコンピュータにいかなる痕跡が残っていたのかを検討していない等、概括的な検討にとどまると言わざるをえない。

67　神奈川県警察・前掲注63検証報告3頁②、4頁イ。詳論する紙幅がないので割愛するが、同様の構造は、他の3件の事例においても見出せる。

68　司法研究14頁。田淵浩二「『在り方』の意義と限界――証明論・冤罪防止の観点から」本誌76号（2013年）90頁は、「6段階・8項目」を「科学的証拠の信用性のチェック項目を網羅するものと言ってよかろう」と評価している。

69　イメージファイルの作成や、解析ソフトが自動的に実行する前処理（削除ファイルの復活、検索用インデックス作成等）がこれに該当するようにも見えなくはないが、その適否によって信用性が損なわれる性格の作業ではない。

70　民事訴訟における鑑定について、鑑定人の専門知識、中立性および独立性を検討する間接的検討と鑑定内容についての直接的検討の2つの検討手段があるとされている（中野貞一郎「鑑定の現在問題」『民事手続の現在問題』〔判例タイムズ社、1989年〕163頁）。加藤新太郎ほか「鑑定結果の証拠価値」『新裁判実務大系　不動産鑑定訴訟法Ⅰ』（青林書院、2002年）22頁も参照。

71　現在、一般財団法人保安通信協会において、「デジタル・フォレンジック分科会」を設置し、民間業者の参画を得て、人材育成カリキュラムの研究を進めているところであり、今後の進展が期待される（http://tech.hotsukyo.or.jp/seminar/list/004/pdf/20130402_h24_digital_forensic.pdf）。

72　司法研究61頁。

73　原本性を問題にする必要がないことについては、前掲注33を参照。

74　裁判所が依頼した鑑定人の場合の規定であるが、捜査機関の嘱託を受けた鑑定嘱託者や、それ以外の私鑑定の場合も刑訴法321条4項が準用ないし類推適用されると考えるのが一般的である。石井・前掲注42書201頁、安冨・前掲注36書269頁。

75　司法研究23頁。

76　成瀬論文(5)1043、1065頁。ただし、(3)導出された結論の評価は、(1)原理・方法の信頼性に吸収されるとしているが（同1046頁）、ここでは別項目として記載した。

77　司法研究36～40頁。証拠調べの必要性によって規律する立場を取るが、成瀬論文(1)60頁は、裁判所の自由裁量に委ねる危険性は大きいとして、このような立場を批判する。

78　前掲注59参照。

79　たとえばDNA鑑定では、推認力の評価は、検出されたの特定のパターンの出現頻度の評価にほぼ収斂する。デジタル・フォレンジックでは、様々な事項が立証の対象となりうることから、そのような定形的なパターンは期待できない。

80　司法研究45頁。

81　①③は、通常、フォレンジック報告書に記載されていることが多い。

82　ただし、対象となるコンピュータが第三者の所有物であり、保全データに秘密情報が含まれるため、そのまま保全データを開示することが難しいというケースはありうる。この場合、何らかの守秘義務を負わせて開示する、開示はしないで第三者機関の鑑定に委ねるといった対処が考えられるが、被告人の防御権確保や相手方当事者の手続保証に意を尽くす必要がある。民事訴訟における秘密保護に関し、新堂幸司監修『実務民事訴訟講座〔第3期〕第3巻――民事訴訟の審理・裁判』（日本評論社、2013年）151頁以下［田邊誠執筆］参照。

83　すなわち、通常の科学的証拠では、再鑑定の問題として論じられる点が（司法研究47頁以下参照）、フォレンジック報告書では、証拠開示の問題に吸収されると言える。

84　司法研究45頁は、一般の科学的証拠に関して「科学的証拠の再現可能性に関する疑問が十分解消されなかったという意味において、その事情を科学的証拠の信頼性を低下させる事情として考慮することは可能」としている。