解　説

ディジタル フォレンジック

～電磁的証拠の収集と分析の技術～

上原哲太郎　京都大学学術情報メディアセンター

ディジタルフォレンジックとは

情報通信技術（ICT）が社会を支える重要な技術となるにつれ，その社会基盤に安全と安心をもたらす情報セキュリティ技術もまたその重要性を増している．情報セキュリティに関してはこれまで，暗号・認証のような要素技術や，ファイアウォール・ウイルス検出などネットワークを悪意ある攻撃から守る技術をはじめ，さまざまな不正・犯罪行為や事故から情報システムを守る技術が盛んに研究され，実用に供されてきた．しかし現実にはいくらこれらの技術を用いても，事件事故の発生を完全に防ぐことはできない．現実に目を向けると，事件事故発生以降の対処，すなわち原因の究明や被害拡大の抑止，被害からの回復，再発防止といった事後対応にかかる課題もまた山積しており，これらに対応する技術の研究開発もまた重要である．この事後対応に焦点がある技術の１つに，ディジタルフォレンジック（Digital Forensics）がある☆1．

フォレンジック（Forensic）は一般に法科学とも訳され，Merriam-Webster Online Dictionary によると the application of scientific knowledge to legal problems; especially : scientific analysis of physical evidence（as from a crime scene）という意味を持つ語である．フォレンジックの中でも法医学（Medical Forensics），特に司法解剖にかかわる医学はよく知られているので，これを例にとるとディジタルフォレンジックの概念は理解しやすい．すなわち，事件や事故で人が亡くなった際に司法解剖を行い捜査や原因究明に役立てるように，情報システム上で事件事故が発生した際に，当該情報システム内のログなど電磁的な証拠を調べ，不正者・犯罪者の同定や事故原因・責任の究明を行おうというのがディジタルフォレンジックである（**図 -1**）．典型的な例としては，不正アクセスやウイルスなどにより攻撃・侵入を受けたサーバや端末において，再発防止のために原因究明を行う作業が従来から行われてきたが，このときに使われる一連の技術はまさにディジタルフォレンジックに含まれる．

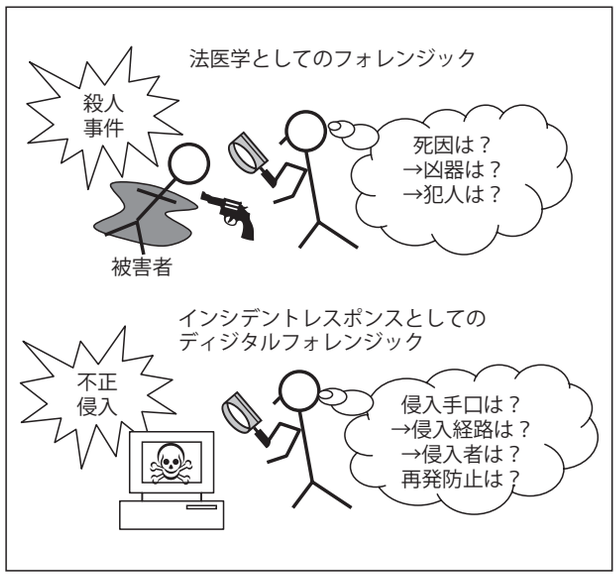

図 -1　（狭義の）ディジタルフォレンジックのイメージ

しかし，こういった情報システム上の事件事故や不正（ここではこれらをあわせてインシデントと呼ぶ）への単なる技術的対応，すなわち従来インシデントレスポンスといわれてきた作業のための技術は，ディジタルフォレンジックの一部に過ぎない．ディジタルフォレンジックでは，インシデントに対し単なる技術的な原因究明にとどまらず，一連の作業の結果を電磁的証拠として客観的に信頼し得るものに位置づけ，法的対応に備えることを強く意識する．これは情報システムが組織や社会にとっ

☆1　なお Forensics は英語としての正しい発音からフォレンシックスと表記すべきという意見もあるが，発音のしやすさなどからフォレンジックという表記が広まっているため，ここでもそれに従う．

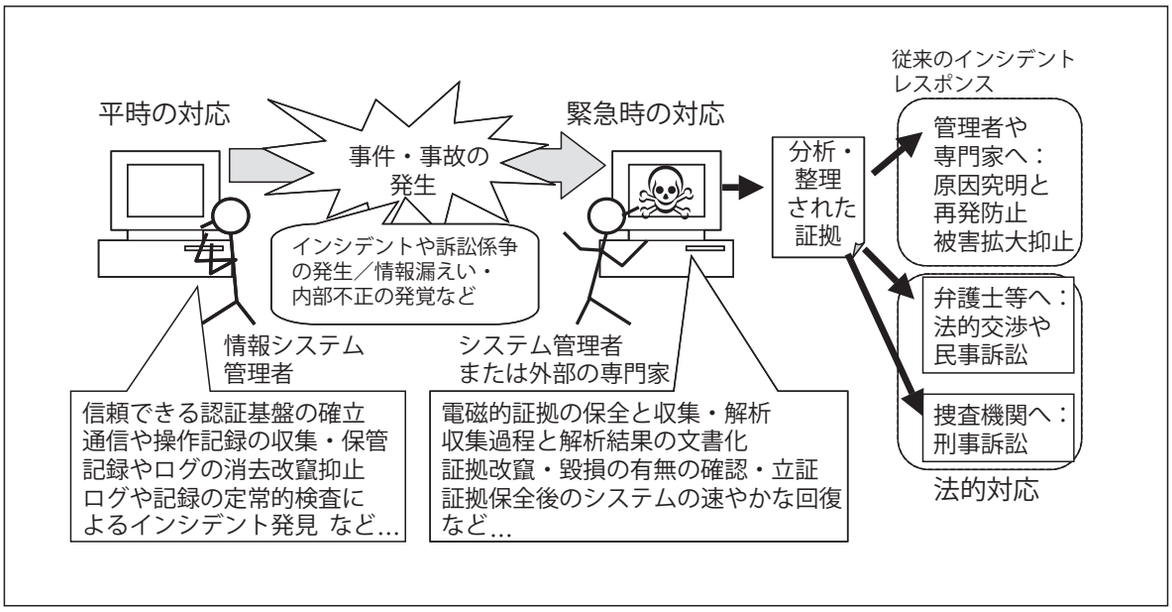

図 -2　情報システムから見たディジタルフォレンジック

ての重要な基盤となり，インシデントが各組織・社会に与える被害が大きくなるにつれて，「なぜインシデントが起きたのか」という技術的論点だけではなく「誰がそのインシデントの責任を負うのか」という法的論点がその重みを増したためといえる．そのため，ディジタルフォレンジックでは，インシデントレスポンスによる解析結果を訴訟や法的紛争の場で証拠性を持つものとするための技術や手続きが重要視される．また，インシデント発生前の平時においても，インシデントに備えて認証基盤の整備やログ管理プロセスの整備などの技術が必要になる．さらに，不正アクセスやシステム障害など技術的解析が必要な事件事故だけではなく，システムの正常な運用の中で起こった内部不正，情報漏えい，企業間取引における契約違反などに際して，民事的係争にかかる事案に対応するためシステム内の電子文書などを分析する技術もディジタルフォレンジックと呼ばれる(**図 -2**)．デジタルフォレンジック研究会では，「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および調査・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調査手法・技術」をディジタルフォレンジックと定義しており，記事・論文などでよく引用されている．

ディジタルフォレンジックが扱う技術的課題

ディジタルフォレンジックの応用分野は多岐に広がりつつあるため，各応用分野ごとに解決が求められる技術的課題は少しずつ異なっている．この応用分野の違いによる技術的課題の差を理解するために，まずディジタルフォレンジックの体系化が求められる．文献 5）は，電磁的証拠が訴訟の原告・被告どちら側に使われるか，および訴訟の種類と対象行為を軸にして**図 -3** のようにまとめており，それをもとにディジタルフォレンジックを**図 -4** のように体系化している．本稿でも，おおむねこの体系に沿って，ディジタルフォレンジックの応用分野を以下の 3 つに分けて整理する．

◎インシデントレスポンスとしてのディジタルフォレンジック

狭義のディジタルフォレンジック，またはコンピュータフォレンジックとも呼ばれるのは，図 -4 で言えば不正侵入に関するディジタルフォレンジックにあたる．情報システムが不正アクセスによる侵入を受けたり，ウイルス等のマルウェアを仕掛けられた場合に，そのシステムを解析してインシデントの原因を探り，被害拡大の防止とシステムの速やかな回復，再発防止を図るものである．さらに，法的措置に備えてその被害の状況や，解析によって判明した侵入経路，侵入者等の追跡の手がかりとなる証拠等を保全する．

この場合，必要になる技術としては，まず平時において認証を確実に行い，特に管理者権限を容易に奪えないように守る技術，システムログ等を確実に収集し，侵入者等による証拠の消去に対抗する技術が必要である．また被害時においては，迅速に証拠の保全を行うためシステムの状態を複製・保存する技術，システムを解析し侵入経路等を調査する作業を支援する技術，仕掛けられたマルウェアの発見やその解析を支援する技術，侵入者等による証拠の消去の痕跡を探し出し状況によっては復元

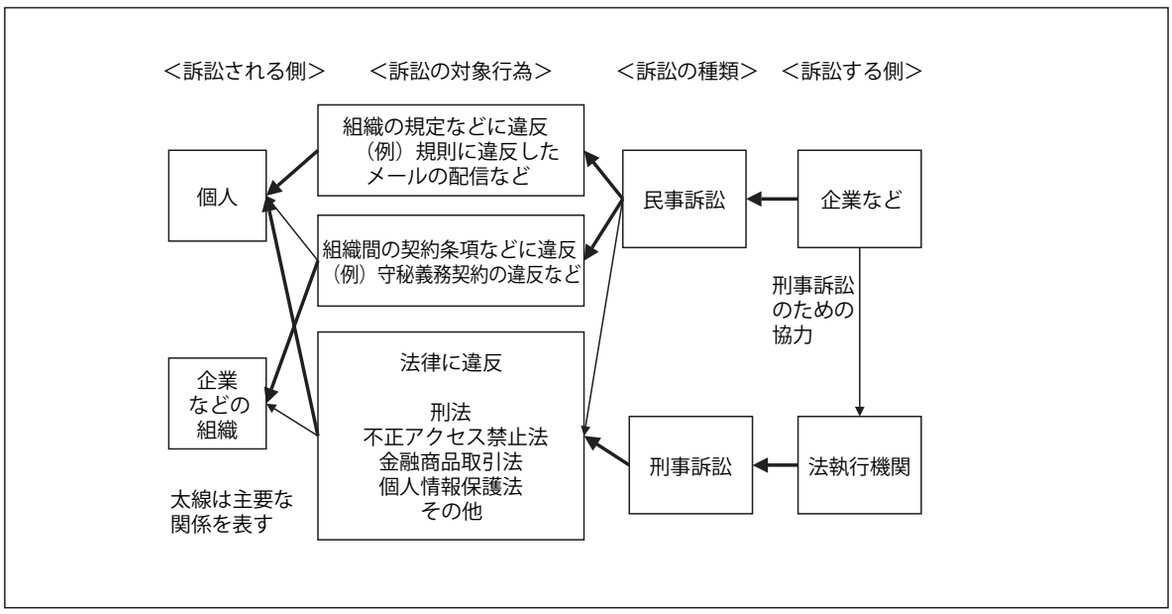

図 -3　電磁的証拠の使われ方 [5)]

する技術などがある．

そしてこれら電磁的証拠の解析経過および結果を文書化する作業を支援する技術も求められている．特に文書化にあたっては，この分野における電磁的証拠が技術的内容を多く含むため，法律関係者にどのようにその内容を伝え，判断材料にさせるかは大きな課題となる．

◎刑事事件におけるディジタルフォレンジック

刑事事件におけるディジタルフォレンジックとは，図 -4 では法執行機関によって運用されている部分にあたる．近年では企業から個人に至るまで，多くの活動がパーソナルコンピュータ（PC），携帯電話といった情報機器やインターネット上で行われるようになり，結果として多くの犯罪捜査にディジタルフォレンジックが必要となっている．警察庁「平成 18 年のサイバー犯罪の検挙及び相談状況について」によると，サイバー犯罪に関する検挙数は近年急増しているが（**図 -5**），平成 18 年度にサイバー犯罪として検挙数に挙げられているもののうち 81.2% は「ネットワーク利用犯罪」（犯罪の構成要件に該当する行為についてネットワークを利用した犯罪，または構成要件該当行為でないものの，犯罪の実行に必要不可欠な手段としてネットワークを利用した犯罪）である（**図 -6**）．サイバー犯罪に分類されていない犯罪に関しても情報機器が使われる例が少なくないことを併せると，ディジタルフォレンジックは不正アクセスなど情報科学技術そのものにおける犯罪だけではなく，一般の犯罪捜査においても必要な技術となっているといえる．

ここでの必要とされている技術は多岐にわたるが，ネットワーク利用犯罪をはじめ多くの犯罪の捜査において

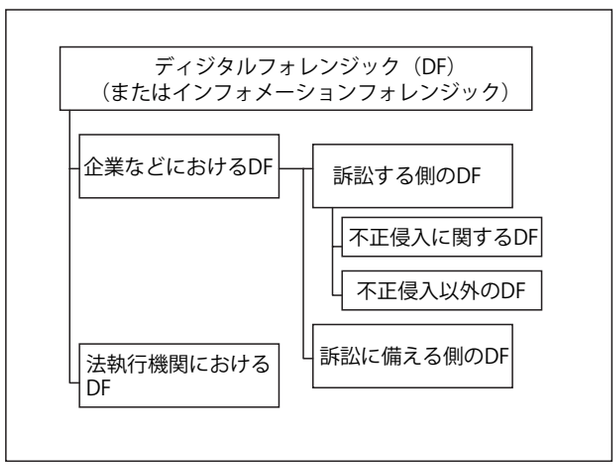

図 -4　ディジタルフォレンジックの体系 [5)]

は，被疑者の PC や携帯電話内にある Web のアクセス履歴やメール送受信履歴，ファイルなどから犯罪の証拠となり得るものを取り出す作業が必要である．しかしディジタルフォレンジックに関し高い技術を持つ専門の捜査員や鑑識員は十分確保できるとは限らないため，専門家でなくとも使用できるフォレンジックツールへの要求がある．また犯罪の場合は被疑者が証拠の隠滅や隠蔽を行う可能性が高いため，消去されたデータの復元，暗号化されたデータの解読，データの偽造の痕跡の発見，隠蔽されたデータの発見などの技術も重要である．

さらに，企業や団体による犯罪の捜査においては，古典的な書類押収と分析による捜査とともに，組織内の情報システム内の大量の電子文書やデータベース等の分析が必要である．たとえば 2001 ～ 2002 年に相次いだ米国企業の不正経理・粉飾会計の事件では，10TB 以上の

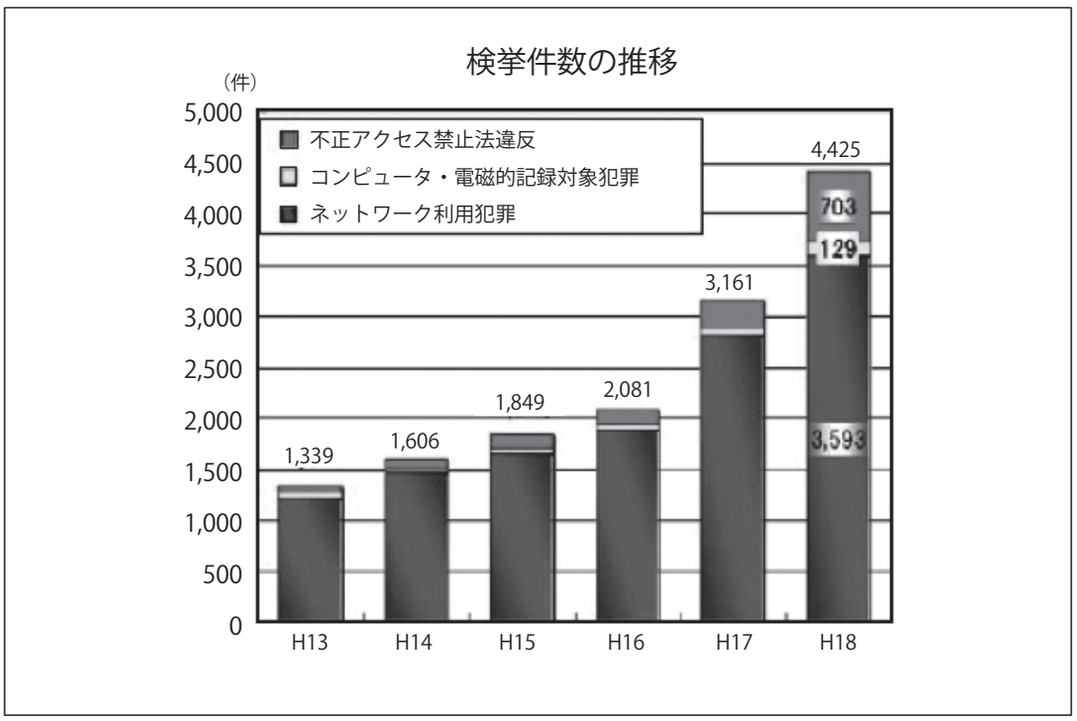

図 -5　サイバー犯罪検挙数の推移（警察庁「平成 18 年のサイバー犯罪の検挙及び相談状況について」）より

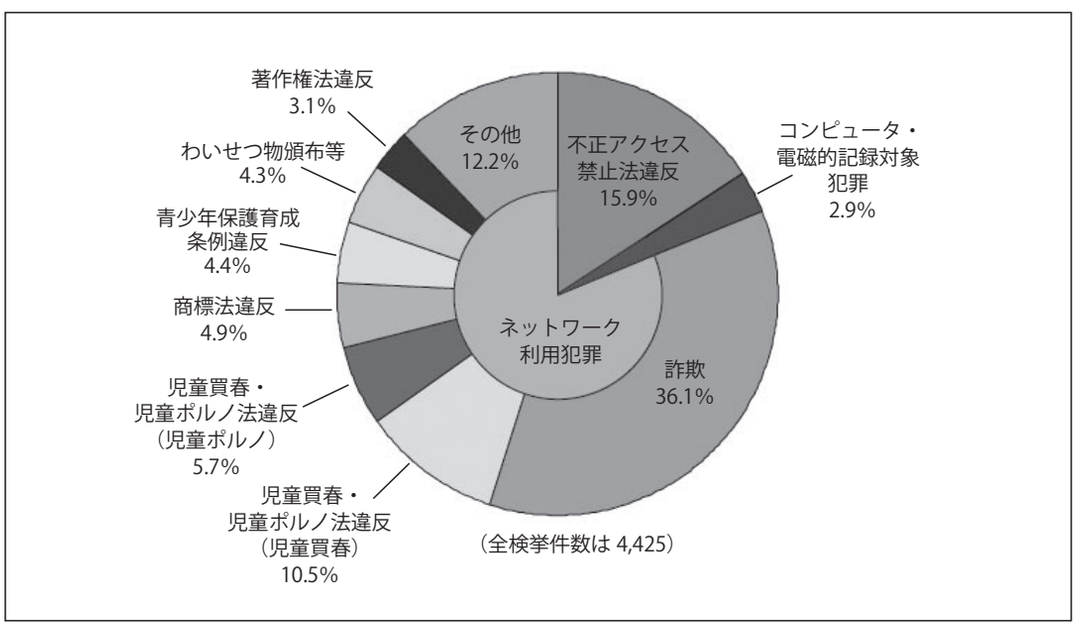

図 -6　平成 18 年度サイバー犯罪検挙数の内訳
（警察庁「平成 18 年のサイバー犯罪の検挙及び相談状況について」）より

ディジタルデータが捜査対象になったといわれており [2]，このような大量のデータの解析を支援するデータマイニングなどの技術も必要とされている．

◎企業活動等におけるディジタルフォレンジック

企業や個人の活動，特に経済活動において情報機器やシステムの果たす役割が大きくなるにつれて，そこで発生する法的紛争においてディジタルフォレンジックが必要とされてきている．図 -4 の，企業などにおける不正侵入以外のディジタルフォレンジックおよび訴訟される側のディジタルフォレンジックは，こういった企業活動等における不正や契約違反，内規違反などによる民事訴訟や，個人情報保護法，e- 文書法，公益通報者保護法，プロバイダ責任制限法などが関係する民事または刑事訴訟への対応が求められた際に必要となる技術である．とりわけ企業にとっては，企業会計不正事件を受けて設けられた米国企業改革法（SOX 法）や，その日本版といわれる金融商品取引法，新会社法への対応が近年話題に

なっている．これらの法律はいずれも，企業活動に関して特に会計監査結果の適正性を確保するため内部統制の確保，すなわち法令順守違反となる事項の発生の未然抑止・発生時の発見修正が合理的に行えることが可能な組織的体制の構築を求めている．これは企業内情報システムにとっては，企業活動にかかる電磁的記録の保全をきちんと行い，監査や法的係争の際には改竄や消去がないことを合理的に説明できる形で証拠として提出できなくてはならないことを示す．情報通信事業者や医療機関，金融機関，公団体など，個別の法令順守を求められる団体においても，それらの関連する団体活動に関する電磁的記録の保全がしっかりとなされ，必要に応じて電磁的証拠を提出した際にその真正性が合理的に示せる情報システムを構築する必要がある．よってこれらに対応するため，認証技術や，電子署名・タイムスタンプ等の技術が必要になってくる．

また国際的に活動する企業や団体においては，海外における民事訴訟に備えて電磁的記録の保全が重要になる場合がある．特に米国では，日本の民事訴訟と異なり，訴訟当事者間において原則として相手方の保持している証拠の開示を請求できる証拠開示（Discovery）という手続きが存在する[4]．この際，自方に不利な証拠を意図的に非開示にする等，適正な開示が行われていないと裁判所が認識すると，種々の制裁が課せられる．この証拠開示を電磁的証拠で行うのが e-Discovery と呼ばれる手続きであり，これに基づき企業内の大量の電磁的記録中から特定のキーワードや事項にかかる記録を抽出して提出することが求められることがある．よって，この e-Discovery を支援するデータマイニング技術や，開示した電磁的証拠の適正性を示すための技術，たとえば証拠作成の手続きの透明性を確保するためその仔細な記録をとる技術や，非開示とした情報の中に開示が請求されているキーワードが含まれていないことを示す技術などが求められる．

ディジタルフォレンジックの技術

これらディジタルフォレンジックの各分野の技術的要求に対し，シーズとなる情報科学の要素技術を組み合わせ，ソリューションとして提供するのが情報科学に携わる研究者の役割であろう．シーズとなり得る技術を，いくつかの分類軸で整理しながら挙げてゆくと次のようになる．

- **電磁的証拠が残る機器に関する分類軸**
  サーバ，クライアント PC，ゲーム機などの他のネットワーククライアント機器，ルータなどネットワーク機器，携帯電話や PDA，ディジタルカメラ・ビデオ，ナビゲーションなど GPS 機器，その他の情報家電機器などそれぞれに対する電磁的証拠の収集と解析技術．
- **電磁的証拠の物理的格納メディアや位置による分類軸**
  主記憶，ハードディスク，各種光ディスク，フラッシュメモリ，磁気テープ，パソコン上の BIOS の設定領域（いわゆる CMOS メモリ）などそれぞれに残る電磁的証拠の収集と解析の技術，内容の複製を高速に得る技術．さらに，ネットワーク経路上で電磁的証拠を収集・解析する技術（ネットワークフォレンジック）．
- **電磁的証拠の論理的格納位置による分類軸**
  ファイルシステム上のファイルおよびメタデータ，データベースおよびメタデータなどの解析技術．特にメタデータからは，ファイル／レコードの参照記録や削除記録が得られ，消去されたファイル／レコードの一部または全部を復元することが可能な場合もある．
- **電磁的証拠の種類による分類軸**
  テキストデータ，プログラムバイナリ，Office などアプリケーション固有のデータ，画像・映像データ，音声データ，電子メール，プログラムソース，操作ログ，認証ログ，送受信ログなどの解析技術．たとえばテキストデータは検索が容易であるが，アプリケーション固有の形式を持つデータファイルが大量にあった場合，そこからの内容の検索を行うにはデータフォーマットを解析する作業が必要になる場合がある．
- **訴訟以前と以降による時間的分類軸**
  訴訟以前の電磁的記録の自動保存とその保証のためのマネジメント負荷軽減技術，訴訟以降の適正な公開のためのデータマイニング技術など．
- **電磁的証拠の消去・改竄（アンチフォレンジック）とそれに対抗する分類軸**
  ファイルの削除と復元技術，メディアの物理的破壊・消去と修復・復元技術など．
- **符号理論や暗号応用から見た分類軸**
  暗号とその解読，電子透かしやステガノグラフィの利用とその検出，データ複製の同一性保証のためのハッシュ関数の利用，真正性保証のためのタイムスタンプや電子署名の利用など．

本稿では，この各分類軸に応じた技術すべてを解説することはできないが，いくつかの部分についてどのような技術課題があるかを挙げる．

◎ PC からの電磁的証拠の収集

ディジタルフォレンジックにおいては，電磁的証拠の収集の際の手続きが適正であることは重要である．PC からの電磁的証拠の収集の手続きは比較的標準的なもの

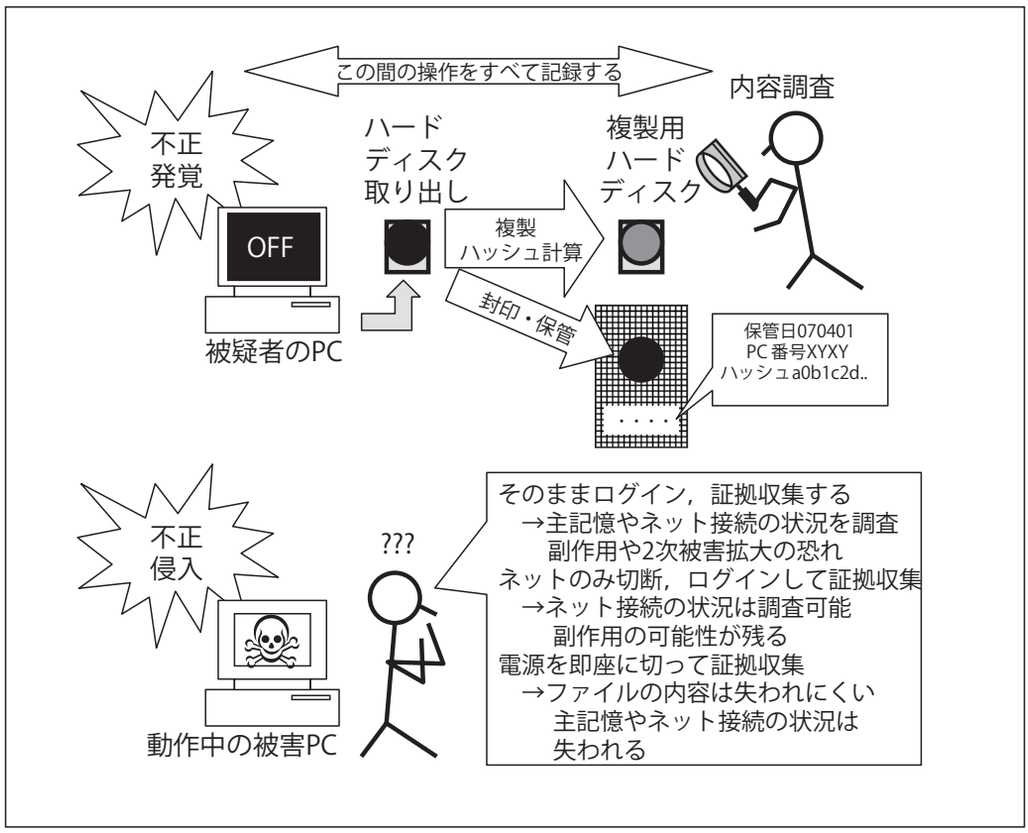

図 -7　非動作／動作中の PC からの電磁的証拠収集

が知られている．たとえば，調査に入ったときに電源が入っていなかった PC では，まず 2 次記憶装置（多くの場合ハードディスク）を物理的に取り外し，その内容を別のハードディスクなどに複製する，あるいは全セクタデータのデータ（イメージ）を抽出するなどの作業を専用の機器で行った後，証拠の同一性を後で確認できるようにデータのハッシュ値を計算して記録し，そのハッシュ値や証拠の出所，時刻などの情報とともに元のハードディスク等を封印して保管する（Tag&Bag と呼ばれる）．この間の作業経過は詳細に文書化しておくほか，可能であれば，この作業風景をビデオなどに記録しておく．収集した電磁的複製の証拠性を確保するために広く行われている手続きである．実際の電磁的証拠の分析はこの作業で作成した複製の上で行うことにより，手違いなどで証拠が失われたり，書き換えられたりすることを未然に防ぐことができる．

ところが，不正アクセスが発覚した情報システムの調査など，動作中の PC からの電磁的証拠の収集をどのような手続きで行うべきかは，いまだに課題が多い．たとえば RFC3227 などいくつかの知られたガイドラインは，主記憶など失われやすい（揮発性の高い）電磁的証拠から順に収集するべきとの原則から，まずログイン等して証拠収集用ツールを外部記憶装置から導入，電磁的証拠をメモリ上のものから 2 次記憶装置上のものの順に収集しつつその手続きを作業時刻とともに文書に記録することを勧めている．しかし実際には，この手続きには収集作業の影響でいくつかの電磁的証拠が失われてしまう（たとえば最終ログイン時間などの情報が書き換わる）副作用や，作業終了までの間の被害拡大の懸念がある．2 次被害を防ぐために当該 PC をネットワークから物理的に切断してから作業に臨む考え方もあるが，これだと失われる情報（たとえば TCP のセッション情報）とのトレードオフとなるほか，ネットワーク切断を検知して証拠の隠滅やシステム破壊行為といった副作用を行うマルウェアが仕掛けられている恐れもある．証拠である当該 PC の電源を即座に切断すればハードディスクなど 2 次記憶装置上の電磁的証拠の確保は確実になるが，メモリ上などの電磁的証拠は失われてしまう（**図 -7**）．確実に副作用なくメモリ上の証拠を収集するには，事前にメモリの内容やシステムの状態を随時保全できるツールを当該 PC に導入しておく必要があり，一部のフォレンジックツールや端末管理ソリューションにはこのような機能が設けられている．しかし，こういったツールが PC 使用者の監視ツールとしても利用できるため普及には抵抗があるほか，侵入者によってさらなる悪用がなされる危険性も否定できない．いずれにせよ，動作中の情報システムからの電磁的証拠の収集には，情報システムの性質や被害の状況に応じた対応が必要であり，その手続きを支援す

るような技術開発が求められている．

◎携帯電話からの電磁的証拠の収集

携帯電話は，犯罪や不正にかかわる通信に使われる場合がPC等よりも多く，特に刑事訴訟の場では重要な捜査対象である．携帯電話網上の通信にかかる記録は携帯キャリア側に多くが残るが，何らかの事情でどうしても端末内に残る証拠が必要であり，かつ被疑者が証拠の消去や破壊を行った場合にはその収集が困難になる場合がある．たとえば携帯電話のメールを端末内で削除された場合，携帯電話はPCと違って2次記憶（通常はフラッシュメモリが使われる）に直接アクセスする手段が提供されていないため，その復元は容易ではない．どうしてもその内容が必要となる場合には，携帯電話を分解した上，マイクロプロセッサのデバッグ機能を利用して内部を読み出したり，あるいはフラッシュメモリ素子を基板から引き剥がして直接端子からデータを読み出すなどの手法が必要であるが，これには高度な技術が必要である．

なお，フラッシュメモリの各記憶素子には，その特性上書き換え回数に上限がある．このため，実使用時には各素子の書き換え回数ができるだけ平均化するようにソフトウェアまたはコントローラによって分散が図られている．よってあるデータが削除されたり，他のデータによって論理的に上書きされても，物理的には同一の素子上は上書きがなされず他の素子で代替されているため，物理素子上はデータが残存している可能性が高い．しかしこのデータを読み出すことは通常は困難であるため，やはり携帯電話本体の分解が必要になる．

このような機器の分解等によるデータの読み出しを用いると，電磁的証拠と無関係の本体内のプログラムやデータ，著作権保護がなされた着信音楽データなども読み取れてしまう可能性があり，携帯電話キャリアやメーカにとって好ましいことではない．理想的には，携帯電話内に残存するデータのうち電磁的証拠を携帯電話キャリアや法執行機関など限られた者にのみ読み出せる機能が最初から端末に備えられているとよいが，このようなフレームワークの実現には社会的なコンセンサスと携帯端末メーカの協力が不可欠であろう．

◎ファイルシステムからの電磁的証拠収集技術

現代の情報システムでは，電磁的証拠の多くはハードディスク上に構成されたファイルシステム中のファイルから得られる．ファイルそのものはたとえば文書やメール，データベースなど多くの証拠を含むものだが，ファイルシステムの機能によりそれ以上の証拠が得られることもある．

たとえば，ファイルのタイムスタンプは重要な証拠である．近年のPC用OSが備えるファイルシステムは，通常ユーザが参照する各ファイルの最終更新時刻以外に，最終参照時刻やファイル作成時刻，ファイル属性の最終変更時刻などを持つものが多い．特に最終参照時刻が有効になっているファイルシステムでは，認証ログ，監査ログなどと照らし合わせることにより，どのユーザがどのファイルを参照したかについて仔細な記録が得られることがある．

また，ファイルシステムによっては通常ユーザが目にすることのない場所にデータが残っており，ここから証拠となり得る情報が得られることがある．たとえばWindows系OSで現在主流のファイルシステムであるNTFSには，代替データストリーム（ADS）と呼ばれる機能があり，ファイルの本来のデータとは別に付加的なデータを格納することができる．これは現在，ファイルシステム本来の機能では格納しきれないメタデータ的な情報をファイルに付加するために使われている．たとえばWindows XP SP2以降のWindowsでは，インターネットからダウンロードした実行ファイルにADSを用いて特別なマークを付加し，実行時にマルウェアの可能性を警告するメッセージを表示する機能がある．よって実行ファイルのADSを調べることで，そのファイルがダウンロードされたものか否か判定することができる．このほか，ADSの機能を使ってデータを隠したりするマルウェアの存在も知られているため，特にインシデントレスポンス時はADSの調査も必要である．

削除されたファイルの痕跡の発見や復元もディジタルフォレンジックにとって大きなテーマである．ファイルシステムの構造にもよるが，一般には削除されたファイルはその直後であればデータ内容は残存しているため，メタデータの修復によりファイルとして復元できる．メタデータの修復が不可能な場合でも，データ領域内のデータ種別固有のデータ列を発見したり，内容を統計的に分析したりして種別の同定や，内容の復元を行う技術が研究されている．また，近年のファイルシステムは不意の電源断によってメタデータ内の構造に矛盾を生じないよう，ジャーナリングなどの手法を用いている場合が多い．この種のファイルシステムでは，メタデータの書き換えが生じるようなファイルシステムへの変更が一度ジャーナルに記録されるため，ジャーナルを解析すればメタデータの変更履歴などの情報が得られることがあり，ここから削除されたファイルの痕跡を発見する技術が開発されている．

なお，削除データの復元はファイルシステムだけではなくデータベースにおいても大きな課題である．データベース技術はサーバ型のデータベースシステムだけではなく，メールクライアントソフトウェアなどにおいても使われており，たとえば削除されたメールの復元に必

要になることがある．データベースファイル内では通常，レコードの削除直後であればその内容の復元は可能と期待できるが，データベースファイル自体の構造に依存する上，その内容は解析によってしか得られないことも多く，技術的な課題になっている．

◎ファイルのデータ種別に応じた電磁的証拠収集技術

古典的なフォレンジックでは，その証拠の種類に応じた鑑定，たとえば手書き文書に関しては筆跡鑑定や，使われている紙やペンの種類の鑑定などが行われてきた．これと同様の証拠の鑑定技術が，電磁的証拠に関しても求められてきており，研究や技術開発が行われている．

たとえばメールなどの文書において，使われる単語やフレーズの癖を何らかの手段で解析してその著者を鑑定しようというものがあり（Authorship Attribution），特に英文に関してはこの研究が進んでいる．同様にキーボードのタイピングの癖やマウスの操作の癖などから使用者の鑑定を行う研究もなされている．

さらに，ファイルの種別によっては，内容の分析によってファイルの作成に使われたアプリケーションプログラムや機器が鑑定できる場合があり，そのような研究も進められている．簡単な例では，メールのヘッダやHTMLファイルのMETAタグ，PDFファイルのヘッダなどには作成したツールなどの名称が残されているため証拠として利用できる．より高度な技術としては，JPEGやMPEGファイルといったマルチメディアファイルは，作成に用いたプログラムによってファイルの内容に特徴が出る場合があり，その鑑定を行う研究が考えられるほか，ステガノグラフィによってデータが埋め込まれていた場合にそれを検出する研究も行われている．さらに，ディジタルカメラの画像を解析して，CCDやCMOSといった撮像素子の特徴および機種ごとの画像生成のアルゴリズムの特徴から撮影された機種の判定を行うなどの研究もある．また，これはファイルではないが，ファイルの消去後に残されるファイルシステム内の痕跡から，証拠の隠滅に使われたファイルの「完全消去」プログラムの種類を鑑定する研究も発表されている．

ディジタルフォレンジックの現状

◎ディジタルフォレンジックのツールやサービス

PCのハードディスク内解析などに使われるディジタルフォレンジック製品としては，ハードディスクのイメージ作成，そのイメージ内のファイルの検索や内容調査，削除ファイルの痕跡の発見と復元，暗号化された証拠の管理とレポートの作成といった一連の基本的なディジタルフォレンジックの手続きの多くの部分をサポートする統合ソフトウェアが最も使いやすいため普及している．特にGuidanceSoftware社のEnCaseおよびAccessData社のForensic Toolkit（FTK）は広く支持されており，捜査機関を含め広く使われている．このほか，ハードディスクの複製やイメージの取得，削除ファイルの復元，ファイルシステム内のメタデータの読み取り，ファイルのバイナリレベルでの表示・検索・編集などの機能については単機能ツールも多く，フォレンジックのために広く使われている．また，フリーやオープンソースのフォレンジック用ツールもいくつか出回っており，特にUNIX系OSではBrian Carrier氏が作成したThe Sleuth Kit（TSK）が有名である☆2．

ディジタルフォレンジック製品としてはほかに，組織内の情報システムでの操作の記録を保存するためのツールも出回っているが，ユーザの使用する情報機器すべてに操作記録を取ることはシステム管理の負担が大きい．それに比べ，ネットワーク経路上で通信記録を取ることにより結果的に各ユーザの操作の多くを記録すると，比較的低いコストで大きな効果が得られるため，よく使われる．この種の製品はネットワークフォレンジック製品と呼ばれる．ネットワークフォレンジック製品には，特定経路上（一般には各種サーバへの通信がすべて集中する個所および組織の内外の通信がすべて集中する個所）の通信トラフィックをすべて記録し，事件・事故の発生時にその内容を解析するものである．このほか，特定のアプリケーション（たとえば電子メールやWeb閲覧記録）にのみ絞ってすべての通信記録を保存するものもネットワークフォレンジックツールと呼ばれることがある．

ディジタルフォレンジックはその電磁的証拠の取得のプロセスが最も重要であることもあり，特に事件・事故発生時の対応を受託するサービスを提供している企業も多い．不正アクセスのインシデントレスポンス，内部不正や情報漏えい発覚時の調査，米国企業との訴訟や係争発生時のe-Discovery作業などのサービスを国内でも提供する会社が現れている．

◎ディジタルフォレンジックに関する研究活動

ディジタルフォレンジックは社会的な要請で生まれてきた技術分野であるため，実運用者である法執行機関自身や専門家団体によるノウハウの共有や教育活動が社会的活動として先行しており，それに比べて研究活動はこれまで活発であったとは言い難い．ディジタル

☆2　このほか米国の法執行機関や軍関係でのみ利用可能なフリーソフトウェアとしてILook Investigatorが知られている．これは，一般には公開されていないがその機能の概要は公開されており，EnCaseやFTKと同様の統合されたディジタルフォレンジックツールと思われる．

Alternative Routes for Data Acquisition and System Compromise
ICMAP : An Information-Centric Modeling Tool for Insider Threat Analysis
An Insider Threat Detection Digital Forensics System
In-Place File Carving
File System Journal Forensics
Legal Issues Related to the Collection and Analysis of Telephone Call Records
Role of Calibration in Establishing the Foundation for Expert Testimony
Perceptions of Prosecutors' and Judges' Knowledge and Willingness to Deal with Digital Evidence : A Survey
GooSweep : Mining Search Engines to Acquire Network Forensic Evidence
Forensic Analysis of Modbus-Based Distributed Control Systems
Investigating Railroad Accidents Using Digital Forensics
Forensic Logging System Using a Secure OS and Network Processor
A Law Enforcement Challenge to the Digital Forensics Research Community
Factors Affecting Cryptographic One-Way Hashes of CD-R Media
Disk Drive I/O Commands and Write Blocking
Using Tokens for Redacting Digital Information from Electronic Devices
A New Text String Search Process for Digital Forensic Investigations
Steganography Detection Using Multi-Class Classification
Future Trends in Authorship Attribution
The Keyboard Dilemma and Forensic Authorship Identification
Specializing CRISP-DM for Evidence Mining
Applying the Biba Integrity Model within a Forensic Evidence Management System
A Systematic Approach for Forensic Investigations of Computer Attacks Using Attack Trees
Attack Patterns : A New Forensic and Design Tool
An Analysis of Forensic Tools in Detecting Rootkits and Hidden Processes
A Method for Detecting Linux Kernel Module Rootkits
Parametrizing Super-Resolution Analysis of Video for Forensic Applications
A Framework for Analyzing Volatile Data Stores
Forensic Analysis of Xbox Consoles
Forensic Analysis of Credit Card Skimmers

表 -1　3rd Annual IFIP WG 11.9 International Conference on Digital Forensics での発表タイトル一覧（Keynote 含む）

フォレンジックに必要な技術に対するソリューションも，実運用者たち自身が既存の技術の中からシーズを拾い出して見つけ出してきた感がある．しかしディジタルフォレンジックの社会的重要性が増すに従って，特に米国を中心に学術研究活動も盛んになってきた．たとえば 2001 年から毎年米国で開かれている Digital Forensic Research Workshop（DFRWS）は，学術色を持つものとしては最も歴史がある学会である．ここ数年は International Workshop on Systematic Approaches to Digital Forensic Engineering（2005 年台北，2007 年シアトル），Workshop on Digital Forensics & Incident Analysis（2006 年イギリス，2007 年ギリシャ）など，ディジタルフォレンジックをテーマにした国際会議やワークショップが増加してきた．IFIP では，2004 年に TC 11（Security）に 9 番目の WG として Digital Forensics が設けられ，2005 年以来例年 1 月に国際学会を開いている．2007 年 1 月に開かれたこの学会での発表の表題をいくつか**表 -1** に示すが，これを見ても分かるとおり，情報セキュリティ分野だけではなく，あらゆる分野の研究者や実務担当者が参加している（端的な例としては，鉄道事故の調査におけるディジタルフォレンジックという発表があった）．ここでの発表は論文化され，Springer から Advances in Digital Forensics シリーズとして出版されている．このほか，定期発行される関連論文誌としては，Elsevier の Digital Investigation や，Taylor & Francis の Journal of Digital Forensic Practice，ADFSL の The Journal of Digital Forensics, Security and Law などがあるほか，IEEE Signal Processing Society から Transactions on Information Forensics and Security が刊行されている（いずれも年 4 回刊）．

我が国では，ディジタルフォレンジックに関する学術研究はまだ盛んとは言い難いが，サイバー犯罪対策全般にかかる産官学連携活動としては，1997 年以来毎年初夏に開かれるサイバー犯罪に関する白浜シンポジウムや，2000 年以来毎年秋に行われるネットワークセキュリティワークショップ in 越後湯沢などがある．ディジタルフォレンジックに特化したものとしては，2004 年以来やはり産官学連携活動としてデジタル・フォレンジック・コミュニティが毎年 12 月に東京で開かれている．また，このコミュニティの運営主体である特定非営利活動法人デジタルフォレンジック研究会（会長：辻井重男情報セキュリティ大学院大学学長）は，情報科学・医学・法学各分野の研究者と弁護士・医師・関連企業の研究者等が数多く参加しており，講演会や分科会活動などを通じてディジタルフォレンジックの啓蒙活動を展開している．このほか，科学技術振興機構（JST）の支援により，東京電機大学工学部の佐々木良一教授を中心に日米共同でディジタルフォレンジックの運用状況に関する比較研究が

行われており，このメンバを中心にこれまで2回のワークショップが開かれている．

前述のIFIP WG 11.9に対しては，同じく東京電機大学工学部の佐々木良一教授を中心に筆者も含め数名の研究者が参加しているが，日本からの参加者は同WGの参加人数（60名前後）の1割にも満たないのが現状である．次回，第4回のIFIP WG 11.9 International Conference on Digital Forensics（ICDF2008）は2008年1月27日から30日にかけて，京都大学で開かれるので（投稿締切は9月15日），国内でもこの分野に興味ある研究者はぜひ参加していただきたい．

◎ディジタルフォレンジックの抱える問題

ディジタルフォレンジックに関する技術は，元来は事件事故といった非常時に強権的に発動されるものであった．しかしその応用が広がり，平時においてもより多くの証拠を残していこうという動きが広がるに従って，その運用上の問題は大きくなりつつある．たとえばすでに情報漏えい抑止のためメールやWebアクセスの記録を従業員ごとに仔細に取っている企業において，その記録が労務管理の過度の強化に使われたり，プライバシーを侵すような行為につながっているのではないかという懸念が従業員側から持ち上がって問題化する例が出てきている．今後フォレンジックツールの普及に伴い，各PCのキーボード・マウス入力をはじめとする細かい操作のすべてが記録されるようになると，この種の問題はさらに拡大する懸念がある．監視の対象とされる従業員等と監視を行う経営側や情報システム管理者との間で，どのような記録をどの程度残すか，事件・事故発生時以外にはみだりに記録内容が閲覧できないことをいかに担保するか，記録そのものの漏えいをいかに抑止するかなどの運用上の合意と相互監視が行われる必要がある．

またディジタルフォレンジックは特に情報漏えい防止に関する情報セキュリティ技術との間で運用に際し矛盾を生じかねないことも問題である．たとえば情報漏えい防止のため各ユーザの情報を暗号化し，各ユーザ固有の暗号鍵でないと復号できないようなシステムを導入した場合，事件事故発生時に証拠収集の障害となりかねない．そこで各ユーザの暗号鍵の複製を情報システム管理者に集めるなど，情報システム管理者等が非常時には復号できるシステムを構成すると，セキュリティ上脆弱になる問題を生じる．同様にネットワークフォレンジック上の要請からLAN内で暗号化された通信を禁止するような運用を行っているような組織では，LAN内での盗聴に対する物理セキュリティ上の対策などが必須になるだろう．

さらに，ディジタルフォレンジックそのものが，悪用された場合に非常に大きな脅威を与えかねない技術であることも問題である．たとえば暗号解読や消去データの復元などの技術，OSなどにおける非常時の特権回避などの技術は，ディジタルフォレンジックとして重要な技術であると同時に悪用も容易であるので，その技術の取り扱いには注意する必要がある．

ディジタルフォレンジックの今後

情報科学技術の進展が社会に与えたインパクトは革命にも例えられるほどであり，確かに現在，我々の生活は豊かで便利になった．この分野，特にインターネットの発展において学術研究者が非常に大きな役割を果たしてきたことも間違いない．だがその一方で，情報科学技術は悪用を企む者にも大きな可能性と力を与えてしまったのも事実であり，その弊害は次第に大きくなっているように感じられる．その状況に対し，情報科学技術の研究者の存在感が，サイバー犯罪対策の分野でそれほど大きくないことは個人的に残念に感じている．中でも，犯罪対策以外の応用分野が広く，情報システム運営管理に従事する技術者にとっても実務上重要度が増しているディジタルフォレンジックの研究に，今後ますます多くの研究者が参加してくれることを願ってやまない．

確かに，ディジタルフォレンジックは実学に近いため研究が難しいように感じられる．しかし，単なるデータを電磁的証拠と視点を変えて扱うことで，データを扱うあらゆる技術はディジタルフォレンジックとなる．また情報科学技術の各応用分野において，それが悪用された場合や事故が発生した場合にどのような対応が必要か考えれば，それもインシデントレスポンスとしてのディジタルフォレンジックとなる．このようにディジタルフォレンジックの応用分野はきわめて広い．社会に情報科学技術が広がれば広がるほど，より広い応用分野の研究者がディジタルフォレンジックに興味を持っていただけることを期待している．

参考文献

1）須川賢洋：国内判例から見たデジタル・フォレンジックの歴史，デジタル・フォレンジック事典，第3章2節2，日科技連(2006)．
2）守本正宏：9.11テロ事件後のフォレンジック調査，デジタル・フォレンジック事典，第8章1節，日科技連(2006)．
3）羽室英太郎：サイバー犯罪・サイバーテロの攻撃手法と対策，立花書房(2007)．
4）高橋郁夫：デジタル時代の裁判－米国におけるe-Discoveryの最近の動き，デジタル・フォレンジック事典，第5章2節2，日科技連(2006)．
5）佐々木良一：デジタル・フォレンジックの分類軸と全体像，デジタル・フォレンジック事典，第1章2節2，日科技連(2006)．

（平成19年6月29日受付）

上原哲太郎（正会員）uehara@media.kyoto-u.ac.jp

京都大学学術情報メディアセンター准教授．教育用コンピュータシステムの管理に従事．NPO情報セキュリティ研究所副代表理事，デジタル・フォレンジック研究会理事，和歌山県警サイバー犯罪対策アドバイザー．