

推薦のことば

中央大学大学院法務研究科 教授
堀 部 政 男

法の世界では証拠が不可欠です。証拠は、大別して、人証と物証に分けることができます。人証とは、裁判で人の供述内容を証拠とするものであり、物証とは、物的証拠を意味します。裁判所では、例えば、詐欺罪を適用するためには、詐欺があったという事実を確定しなければなりません。詐欺の例としては、銀行の預金口座の残高を不正に動かして財産上の利益を得ることなどを挙げることができます。

その詐欺罪も情報技術の発展との関係で変化してきています。今となると、20年も前になりますが、詐欺罪について規定している刑法について、コンピュータに関連する不正行為であるコンピュータ犯罪にどのように対処するかが大きな問題になり、1987(昭和62)年5月に成立した改正刑法がコンピュータ犯罪として処罰すべき犯罪類型を設けるに至りました。その一つがコンピュータ利用による財産利得罪でした。

従来は、端末機を不正に操作して他人の預金口座から自分の預金口座に振り替えても、自分で引き出して使わないかぎり、詐欺罪にも窃盗罪にもなりませんでした。詐欺罪は機械ではなく人をだまして財物をせしめることであり、窃盗罪は財物を盗むことでありますが、この場合、いずれの行為もないからです。情報通信ネットワークを使えば、人を介さないばかりか、現金を動かさなくても決済することができます。現行刑法は、これらの行為を処罰するために窃盗罪や詐欺罪と同じ10年以下の懲役で処罰するとしています(246条の2)。警察庁によりますと、最近の検挙件数は、1999年98件、2000年33件、01年48件、02年18件、03年34件、04年42件、05年49件です。

このような事件では、電子的証拠が重要な役割を果たすことはいうまでもありません。

本書が対象としているデジタル・フォレンジックは、ここに掲げたような問題を解決するのに大いに役立ちます。デジタル・フォレンジックという新たな視点から問題を捉えることは今後ますます重要性を増してきます。電子社会システムにおける法的課題を研究している法学者として、本書を推薦します。

推薦のことば

中央大学 教授
日本学術会議 副会長
土 居 範 久

インターネット社会の進展に伴い、ほとんどすべてのデータはデジタル化して扱われるようになってきました。一方、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ました。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ています。

わが国でも、技術者や法律家がデジタル・フォレンジックの研究を開始し、関連製品もいろいろ出回り始めました。今後、多くの分野でデジタル・フォレンジックの考え方が必要とされ、関連製品が使われるようになっていくと思います。特に、内部統制の強化に伴い、企業のアカウントビリティ(説明責任)を問われるシーンがますます多くなっていくものと予想されます。すなわち、情報セキュリティ対策の視点からデジタル・フォレンジックを捉えるだけでなく、経営管理の視点からデジタル・フォレンジックを考えていくことも大切となります。

しかし、デジタル・フォレンジックは関連する分野が広く、その専門家であってもデジタル・フォレンジックの全体像を把握するのが困難な状況にありました。本書は、NPO法人デジタル・フォレンジック研究会の辻井重男会長が監修を行い、それぞれの分野の第一人者が、広く体系的に解説を行っており、全体像を的確に捉えるのに最適だと考えています。

日本国内だけでなく、海外においてもこのような事典はないと考えており、警察などの法執行機関や、企業、自治体などでデジタル・フォレンジック関連の実務を行っている人だけでなく、情報システム技術者や法律家などにも、本書を推薦いたします。

推薦のことば

慶應義塾大学医学部外科学 教授

万国外科学会 会長

日本学術会議 第19期・20期会員

北 島 政 樹

これまで病院における情報化はレセプト処理やオーダーリングを中心に進められてきたが、最近になり電子カルテという形で進展しつつある。医療における IT 環境の変貌は、単にペーパーレス、フィルムレスによる業務の効率化やコスト削減に留まらず、蓄積したデータの二次利用により、経営分析や医学的エビデンスの確立が可能となってきている。このような蓄積された診療情報は社会的に大きな意味をもつといえる。

一方で、手術患者の取り違い事故に端を発した医療過誤への国民の関心の高まりにともない、医療訴訟の件数が増加傾向にあるのも事実である。このような社会環境において、医療行為を事後的に検証可能な形で記録に残すことの重要性が増しており、医療における IT にデジタル・フォレンジックの技術を導入することは、今後必須となることが予想される。そのような観点から、本書のもつ意義は大きく、医療におけるデジタル・フォレンジックのバイブルとなる一冊であろう。

推薦のことば

株式会社 NTT データ 代表取締役社長
浜 口 友 一

近年、IT の進歩は目覚ましいものがあり、特にインターネットに代表されるネットワークを介した情報のやり取りは 10 年程前には想像もできなかった領域にまで到達しつつあると言えるでしょう。しかしながら、こうした利便性の飛躍的な向上の陰に、サイバー犯罪と言われる負の部分が存在するのも事実です。昨今はこうした犯罪の手口も年々巧妙化し、より深刻な事態を引き起こしつつあります。

こうした状況の中で、これらのサイバー犯罪に対応するための IT の仕組みもさまざまに工夫され、単にこうした犯罪からの被害を防ぐだけでなく、その犯罪を犯した根源をつきとめ、捕獲することを目的とした技術も開発されています。これらを総合して「デジタル・フォレンジック」と称せられる技術分野が注目を集めているのです。

私たち IT 業界でビジネスを展開する者にとって、利用者に真に役に立つシステム作りを常に追い求めていくことは言うまでもありませんが、一方でこうしたシステムを悪用されてしまえば、その価値は半減するどころか、マイナスの評価をされてしまうことにもなりかねません。常に利便性を追求すると同時に、その裏での悪用を防止する仕組みを両立させていくことが、今後ますます求められるのではないのでしょうか。

以上をふまえると、今、デジタル・フォレンジック分野の専門家によって、この新しい技術分野をより深いレベルまで学ぼうとする人々のための体系的な専門書が出版される意義はたいへん大きいと考えています。

ぜひ多くの方々に本書をお読みいただき、デジタル・フォレンジックの知識を深められ、ひいてはその後の IT の仕組みの構築に生かされていくことを願ってやみません。

推薦のことば

公認不正検査士協会日本事務局 (ACFE JAPAN)

事務局長 甘 粕 潔

多くの日本人にとって、「デジタル」という言葉はすんなり耳に入るが、「フォレンジック」という言葉には馴染みがないであろう。辞書を引いてみると、英語の forensic には “relating to the methods for finding out about a crime”、つまり「犯罪について解明する方法に関する」という意味合いがある。

インターネットや電子メールの爆発的な普及によりコミュニケーションのデジタル化が進展するなかで、サイバーテロやフィッシングなどの新手の犯罪が横行し、また、それらの犯罪を立証する証拠は書類から電子データに移行しつつある。そのため、本書のテーマである「デジタル・フォレンジック」に関する知識・スキルは、企業が来るべき法化社会への対応力を高めるうえでその重要性を増してきている。遣われ始めた当時は違和感のあった「コンプライアンス」も、今や日本の企業経営を語るうえで欠かせない言葉として認知されているように、「フォレンジック」が日本語として定着する日もそう遠くないのではないか。

本書は、そのような時代の到来を見越した先見性に富むものであり、この分野に関する日本語の専門書としては、他に類を見ない包括的な内容となっている。米国に本部を置く当協会は、世界 120 カ国において不正リスク対策のエキスパートである「公認不正検査士 (CFE)」を認定・育成しているが、CFE の教育プログラムにおいても、デジタル・フォレンジックは、今最も注目されている分野のひとつである。当協会会員をはじめ、広く企業のリスクマネジメントに携わる方々に是非一読をお勧めしたい一冊である。

刊行にあたって

デジタル・フォレンジックとは何か。詳しい定義は本文に譲るとして、大よそのところ、企業等の業務情報に関する電子的証拠を漏れなく、かつ誤りなく保全し、そしてわかりやすく正確に開示するためのプロセスを法制度、経営管理、デジタル技術などの面から多角的に構築する手法および学術をデジタル・フォレンジックと呼んでいる。

なぜ、そのような手法や学術が必要とされるようになったのか。それは、1990年頃から、刑事、民事の裁判において、物的証拠と並んで、電子的証拠の重要性が増してきたからであり、より一般的には、2000年初頭、米国などにおいて多発した企業の不祥事をきっかけに、内部統制の強化が求められ、膨大な量の電子情報の保全と開示が不可欠となったからである。

契約・訴訟社会の米国に比べて、典型的な内部規範社会とみられる日本では、数年前までデジタル・フォレンジックは、情報セキュリティ分野でも話題になることは少なかった。しかし、インシデントレスポンスへの認識の深まりや、個人情報保護法の本格的施行、続いていわゆる日本版SOX法制定への動きなどを背景に、わが国でもデジタル・フォレンジックの研究・普及の必要性が高まってきた。こうした状況のなかで有志が集い、2004年8月23日、日本初の「デジタル・フォレンジック研究会」を旗揚げした。そして、2004年12月20日、21日の両日、「デジタル・フォレンジックの目指すもの」をテーマに「デジタル・フォレンジック・コミュニティ2004 in Tokyo」を開催し、情報セキュリティ技術、法制度、情報ガバナンスなどに携わる広い分野の人々の関心を集め、活発な議論を展開した。

これと並行して、当研究会は、2004年12月15日付けでNPO(特定非営利活動法人)として認可され、登記を完了した(URL <http://www.digitalforensic.jp/>)。その後1年間、技術、法務、監査等の分科会を編成して研究・啓発活動を続け、2005年12月19日、20日の2日間「デジタル・フォレンジックの新たな展開」と題して“コンプライアンス、内部統制、個人情報保護のための技術基盤”をテーマに第2回のシンポジウム「デジタル・フォレンジック・コミュニティ2005 in Tokyo」を開催し、広がりのある議論を展開することができた。さらに、2006年12月18日、19日の両日には、「J-SOX時代のデジタル・フォレンジック—信頼される企業・組織経営のために—」というテーマのもとに、第3回デジタル・フォレンジック・コミュニティ2006が開催される運びとなっている。

本書は、このようなデジタル・フォレンジック研究会の活動をふまえて、当研究会の総

力を挙げて、本分野を可能な限りわかりやすく体系化して解説したものである。

上にも述べたように、デジタル・フォレンジックは、個人情報漏洩対応や訴訟対応等のインシデントレスポンスの重要性やコンプライアンス等への関心の高まり、デジタルデータの取扱いに関する刑法の改正や国際間のサイバー犯罪関連条約等との関係からその必要性が急速に高まりつつある分野である。また、今後は携帯電話やPDA、USBメモリ、ユビキタス端末等々の各種の電磁的機器やメモリもフォレンジックの対象となっていくことなどから新しいセキュリティ手段としてさらに関心が高まってゆくものと見られる。

本書が、デジタル・フォレンジックに直接かかわられる専門家はもちろん、広くIT・情報セキュリティガバナンスに関心のある方々のための入門書・参考書として活用していただければ、そして、IT社会のセキュリティ基盤の確立に寄与することができれば幸いである。

2006年11月

情報セキュリティ大学院大学 学長

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

まえがき

21世紀に入り、ますます世界の情勢は混沌とし筆者が子供の頃に夢に描いていた『鉄腕アトム』などの世界は、筆者が生きているうちにはどうやら実現しそうにない。

ただし、コンピュータ(デジタル)の世界に限定すれば予想より遥かに先を行っている感がある。私事で恐縮だが25年以上も前、システムエンジニアの卵だった時代、使っていた大型コンピュータのメモリ量はたったの数メガバイト(ギガバイトではない)しかなかった。今では個人で使うパソコンですら1ギガバイトを超えるものが多い。ディスクにいたってはOSを格納する冷蔵庫並のディスクが数百メガバイト程度であった。このディスクを数台と数メガバイトから数十メガバイトのメモリでオンラインシステムを構築していたのである。本当に隔世の感がある。

こういう歴史の流れの中で「デジタル・フォレンジック」が大きな注目を浴びた有名な事件がいわゆる「SJG(Steve Jackson Games, Inc.)事件」である(事件の詳細は<http://www.comit.jp/sec/SJG.HTM>などに掲載されている)。

1990年3月1日、米国シークレットサービス(法執行機関)は、連邦法上の令状に基づきテキサス州オースチンのSJG社において業務用のコンピュータ3台、外付HDD5台、FD300枚(そこにあったものすべて)、その他関係資料のほとんどを押収してしまった。その結果SJG社は業務の継続が不可能となり、完成間近のゲームソフトの出荷ができなくなった。しかも、SJG社の社長がハッカー行為の犯罪者扱いされ、信用がガタ落ちし、従業員の半数を解雇するに至った。ところが、その後の調査でハッカー行為とはまったく無関係であると判明したものの、シークレットサービスは3カ月後にやっと押収物を返還している。この事件後、いわゆる「写し(コピー)」の証拠能力が問題となり、原本主義に徹する限り現場で使用されているパソコンを押収されてしまい、その結果として企業の業務が停止し、最悪の場合倒産する可能性が出てきた。また、押収物を分析して「犯人」か否かの特定を行う捜査機関にとっても極めて重要な問題となっていたのである。その後、フォレンジックの考え方は急速に米国を中心に普及し始めている。しかし、日本国内をみればいまだに認知されているとは言い難い状況である。こうした状況に危機感を覚えた筆者らは、「デジタル・フォレンジック」という技術要素が今後の社会の中で必須となることを確信し、その啓蒙・普及を推進することで、健全なIT社会の実現に貢献するために特定非営利活動法人デジタル・フォレンジック研究会を2004年に設立した。

デジタル・フォレンジックが他の技術と異なる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、論理構造、ソフトウェアではネットワーク技術、OSの論理構造などがある、これらの集大成として、デジタル・フォレンジックという分野が成り立っているのである。

また、これらの学術的な要素に加え重要なことは、さまざまな犯罪行為に関する検知、防御、予防といった観点での論理的思考も必要としていることである。捜査機関で学ぶ犯罪心理学的要素も加味するのが望ましいだろう。このように多種多様な分野まで広がっていくのである。さらに、これらの要素を包含しながら医療や製造業、金融業といった業種別にその犯罪傾向が異なるので、その業種固有の問題も把握しておく必要がある。そこまで追求することでデジタル犯罪の抑制や検知、調査、発見という一連の作業の流れになってくる。

こうして書き並べるとうんざりするほどの問題点が出てくる感じを受けるが、同様に感じるのは筆者だけではないだろう。筆者らはまだまだ未熟であることを感じながらも、日本における当ジャンルの専門書がほとんどないことから、研究会の活動の一環として本を執筆することを決め、今回の刊行に漕ぎ着けたのである。

本書の出版にあたっては、当研究会の辻井重男会長、ならびに安富潔副会長から多大なご支援をいただきました。また、かつて『情報セキュリティ事典』で編者代表を務められた佐々木良一氏からは、ご経験を活かした編集上の数々のアドバイスをいただきました。編集会合や執筆者間の調整などにおいては、丸谷俊博事務局長と補佐の寺本真世さんを始めとした事務局メンバーの方々にさまざまな労を執っていただきました。本書の担当編集者である日科技連出版社の鈴木兄宏氏には夜遅くまで作業にお付き合いいただき、本当にお世話になりました。そして、何より執筆者の方々は、お互いが納得するまでメールでの議論など、今、思えば本当に大変な思いをされてご執筆をされておりました。この場をお借りして、皆様に心から厚く御礼申し上げます。

最後に、本書の出版にかかわったすべての関係者とそのご家族の皆様に重ねて感謝申し上げます。

2006年11月

社団法人コンピュータソフトウェア著作権協会 技術顧問

日本セキュリティ・マネジメント学会 理事

『デジタル・フォレンジック事典』編集責任者

萩原栄幸

執筆者一覧

(五十音順)

所属等は2006年11月1日現在。*は各章の主査を示す。

- | | |
|--------|---|
| 秋山 昌範* | マサチューセッツ工科大学 スローン経営大学院 客員教授、東京医科大学 客員教授 |
| 足立 正浩 | シーア・インサイト・セキュリティ株式会社 取締役サービス事業本部長 |
| 池上 成朝 | 株式会社 UBIC 取締役事業部長 |
| 石井 徹哉 | 千葉大学 法経学部 助教授 |
| 伊原 秀明 | ネットエージェント株式会社 取締役 |
| 上原哲太郎 | 京都大学 学術情報メディアセンター 助教授 |
| 大橋 充直 | 検察庁 検事 |
| 小向 太郎 | 株式会社情報通信総合研究所 法制度研究グループ 上席主任研究員 |
| 佐々木良一* | 東京電機大学 工学部 教授 |
| 佐藤 慶浩* | 日本ビューレット・パッカー株式会社 |
| 須川 賢洋* | 新潟大学 法学部 助手 |
| 高橋 郁夫 | I*T 法律事務所 弁護士 |
| 辻井 重男* | 情報セキュリティ大学院大学 学長 |
| 萩原 栄幸 | 社団法人コンピュータソフトウェア著作権協会 技術顧問、日本セキュリティ・マネジメント学会 理事 |
| 舟橋 信 | 財団法人未来工学研究所 技術・国際関係研究センター 参与 |
| 古川 俊治 | 慶應義塾大学 法務研究科・医学部外科 助教授、TMI 総合法律事務所 弁護士 |
| 町村 泰貴 | 南山大学大学院 法務研究科 教授 |
| 丸谷 俊博 | 株式会社フォーカスシステムズ 新規事業推進室 室長 |
| 丸山 満彦 | 監査法人トーマツ エンタープライズリスクサービス 公認会計士社員 |
| 宮坂 肇 | 株式会社 NTT データ 公共ビジネス推進部 部長 |
| 向井 徹 | シーア・インサイト・セキュリティ株式会社 代表取締役社長 |
| 守本 正宏* | 株式会社 UBIC 代表取締役社長 |
| 安富 潔* | 慶應義塾大学 法務研究科・法学部 教授、弁護士 |
| 和田 則仁 | 慶應義塾大学 医学部外科 助手 |

デジタル・フォレンジック事典 目次

推薦のことば	堀部政男	i
推薦のことば	土居範久	ii
推薦のことば	北島政樹	iii
推薦のことば	浜口友一	iv
推薦のことば	甘粕 潔	v
刊行にあたって	辻井重男	vii
まえがき	萩原栄幸	ix
執筆者一覧		xi

第1章 デジタル・フォレンジックの基本

(主査：佐々木良一)

1.1 デジタル・フォレンジックとは	佐々木良一	3
1.2 体系化の試み	佐々木良一	5
1.2.1 従来のデジタル・フォレンジックと最近の動向		5
1.2.2 デジタル・フォレンジックの分類軸と全体像		6
1.3 企業において訴訟を行うためのデジタル・フォレンジック	佐々木良一	9
1.3.1 不正侵入に対するデジタル・フォレンジック		9
1.3.2 不正侵入以外の不正に対するデジタル・フォレンジック		10
1.4 企業において訴訟に備えるためのデジタル・フォレンジック	佐々木良一	12
1.4.1 訴訟に備える側のデジタル・フォレンジックの分類		12
1.4.2 訴訟する側のデジタル・フォレンジックとの比較		13
1.5 法執行機関におけるデジタル・フォレンジック	佐々木良一	14
1.6 本章のまとめと関連技術	佐々木良一	15

第2章 デジタル・フォレンジックの現状

(主査：守本正宏)

2.1 欧米にみるデジタル・フォレンジックの運用状況	21
2.1.1 ハイテク犯罪対策(法執行機関)	守本正宏 21
2.1.2 企業等における内部統制等へのフォレンジックの活用	高橋郁夫 26
2.2 日本におけるデジタル・フォレンジックの運用状況	32
2.2.1 ハイテク犯罪対策(捜査機関)	守本正宏 32
2.2.2 わが国における内部統制等へのフォレンジックの活用	高橋郁夫 36

第3章 デジタル・フォレンジックの歴史

(主査：須川賢洋)

3.1 コンピュータの歴史	上原哲太郎 47
3.2 フォレンジックの歴史	53
3.2.1 技術側面の歴史	守本正宏 53
3.2.2 国内判例からみたデジタル・フォレンジックの歴史	須川賢洋 57

第4章 デジタル・フォレンジックの技術

(主査：佐々木良一)

4.1 デジタル・フォレンジック技術の概要	67
4.1.1 デジタル・フォレンジック技術の分類	佐々木良一 67
4.1.2 フォレンジックのためのコンピュータ技術入門	上原哲太郎 69
4.2 訴訟する側のデジタル・フォレンジック技術	佐々木良一 96
4.3 訴訟される側のデジタル・フォレンジック技術	100
4.3.1 正当性証明技術	足立正浩 100
4.3.2 e-Discovery 技術	守本正宏 105
4.4 パソコン以外の機器のデジタル・フォレンジック対応技術	112
4.4.1 モバイル・フォレンジック(PDA・携帯電話)	池上成朝 112
4.4.2 ネットワーク・フォレンジック技術	佐々木良一・向井 徹 117
4.5 デジタル・フォレンジックの要素技術	127

4.5.1	暗号・時刻認証とデジタル・フォレンジック	宮坂 肇	127
4.5.2	デジタル・フォレンジックと電子透かし	上原哲太郎	136
4.5.3	HDD(ハードディスクドライブ)内のデータの消去技術と復元技術	上原哲太郎	144
4.6	技術と法の対応	舟橋 信	162
4.6.1	科学技術の進展にともなう犯罪事象の変遷と法の対応等		163
4.6.2	技術者から見たデジタル・フォレンジックに係る法律の諸問題		168
4.7	システム設計とデジタル・フォレンジック	萩原栄幸	174
4.7.1	システム設計における前提条件		174
4.7.2	RASIS から見たデジタル・フォレンジック		174
4.7.3	デジタル・フォレンジック的な考慮点		175

第5章 デジタル・フォレンジックと法

(主査：安富 潔)

5.1	情報および情報セキュリティの法的保護		181
5.1.1	情報の法的保護	石井徹哉	181
5.1.2	情報セキュリティと刑法	石井徹哉	186
5.1.3	個人情報保護法	安富 潔	196
5.1.4	e-文書法	小向太郎	210
5.1.5	公益通報者保護法	町村泰貴	218
5.1.6	不正競争防止法による営業秘密の保護	須川賢洋	224
5.2	法運用とデジタル・フォレンジック		229
5.2.1	刑事手続とデジタル・フォレンジック	大橋充直	229
5.2.2	民事証拠法から見たデジタル・フォレンジックの効用	町村泰貴	239
5.2.3	デジタル時代の裁判——米国における e-Discovery の最近の動き	高橋郁夫	246
	第5章参照条文		250

第6章 企業におけるデジタル・フォレンジック

(主査：佐藤慶浩)

6.1	企業におけるデジタル・フォレンジックの基本的な考え方	佐藤慶浩	273
-----	----------------------------	------	-----

6.1.1	デジタル・フォレンジックの対象となるデータとしての違い	274
6.1.2	デジタル・フォレンジックを使う局面による違い	275
6.1.3	デジタル・フォレンジックの対象が誰のものかによる違い	277
6.1.4	デジタル・フォレンジックを選択することの妥当性	277
6.2	電気通信事業者におけるデジタル・フォレンジック	小向太郎 279
6.2.1	デジタル・フォレンジックと電気通信事業者	279
6.2.2	電気通信事業者と民事訴訟	281
6.2.3	電気通信事業者と刑事訴訟	282
6.3	公認会計士監査とデジタル・フォレンジック	丸山満彦 284
6.3.1	はじめに	284
6.3.2	監査と不正調査	284
6.3.3	財務諸表監査における監査意見形成	285
6.3.4	監査証拠	286
6.3.5	電子化された契約書等を監査証拠として利用する場合の留意点	288
6.3.6	米国公認会計士監査マニュアルにおけるデジタル・フォレンジックについての記述	290
6.3.7	電子的証拠を利用した監査の重要性の増加	291
6.3.8	サーベンス・オクスリー法の影響——監査の強化と管理の強化	292
6.3.9	今後の課題	293
6.4	金融機関におけるデジタル・フォレンジック	萩原栄幸 294
6.4.1	個人情報保護法と金融機関	294
6.4.2	金融機関と IT 犯罪	295
6.4.3	インターネットバンキングの拡大と不正アクセス	297
6.4.4	フィッシング詐欺	298
6.4.5	預金者保護法の制定と日本版 SOX 法	298
6.4.6	金融機関と CSIRT	300
6.4.7	金融機関におけるデジタル・フォレンジックの考え方	302

第7章 デジタル・フォレンジックと医療

(主査：秋山昌範)

7.1	医療の進歩と IT 化	秋山昌範・古川俊治・和田則仁 307
7.2	医療における個人情報の意義	秋山昌範・古川俊治・和田則仁 308
7.2.1	伝統的な職業倫理的・法的守秘義務	308

7.2.2	現代医療における患者のプライバシー権	308
7.2.3	医療情報における要保護性の差異	310
7.3	プライバシー保護におけるインフォームド・コンセントの問題	
	秋山昌範・古川俊治・和田則仁	311
7.3.1	インフォームド・コンセントの概要	311
7.3.2	特殊疾患における問題	311
7.3.3	遺伝子解析における「インフォームド・コンセント」の新しい意義	312
7.3.4	プライバシー保護における診療記録開示の問題	313
7.4	公益目的の医療情報の活用とプライバシー保護	
	秋山昌範・古川俊治・和田則仁	315
7.4.1	プライバシーと公共性	315
7.4.2	医療の場合に特有の問題が存在	316
7.4.3	データの二次利用におけるセキュリティ要件	317
7.4.4	プライバシー保護に関する社会的、心理学的要因の検討	318
7.4.5	患者から見た安心のレベル	319
7.4.6	医療情報の研究利用におけるプライバシー保護	321
7.5	2つのガイドライン	秋山昌範・古川俊治・和田則仁 324
7.5.1	医療・介護関係事業者における個人情報の適切な取扱いのためのガイド ラインの概要	324
7.5.2	医療情報システムの安全管理に関するガイドラインの概要	333
7.6	医療事故とデジタル・フォレンジック	秋山昌範・古川俊治・和田則仁 359
7.6.1	医療安全対策における医療事故情報の活用とデジタル・フォレンジック	359
7.6.2	医事訴訟における立証活動とデジタル・フォレンジック	361
7.6.3	手術映像の保存	362
7.7	遠隔医療とデジタル・フォレンジック	秋山昌範・古川俊治・和田則仁 363
7.7.1	遠隔医療と患者のプライバシー保護	363
7.7.2	遠隔医療の歴史	363
7.7.3	動画伝送時のセキュリティの研究	364
7.7.4	遠隔手術指導	366
7.7.5	遠隔カンファレンス	367
7.7.6	遠隔共同手術	368
第7章参考資料「医療情報システムの安全管理に関するガイドライン」(平成17年3 月、厚生労働省)の解説		
		371

第8章 デジタル・フォレンジックの実際

(主査：守本正宏)

8.1	9.11 テロ事件後のフォレンジック調査	守本正宏	405
8.1.1	調査に必要なデジタル・フォレンジック技術		405
8.1.2	テロ対策におけるデジタル・フォレンジック調査の役割		407
8.2	e-Discovery 作業	池上成朝	409
8.2.1	はじめに		409
8.2.2	De-Duplication(重複の除外)および証拠データ統合		409
8.2.3	不要データに対する防御策		410
8.2.4	多言語の壁		411
8.2.5	オンライン管理と提出用データフォーマット		411
8.2.6	ネットワークを用いた e-Discovery		412
8.2.7	おわりに		412
8.3	米国における法執行機関の事例	守本正宏	414
8.3.1	はじめに		414
8.3.2	犯罪捜査におけるデジタル・フォレンジック		414
8.3.3	フォレンジックトレーニング		414
8.3.4	フォレンジックラボラトリ		415
8.3.5	ハイテク犯罪捜査部隊		415
8.3.6	産官学の連携		416
8.3.7	証拠を形成する重要な要素		416
8.3.8	デジタル・フォレンジック捜査の実例		417

第9章 デジタル・フォレンジックツールの紹介

(主査：守本正宏)

9.1	ネットワーク・フォレンジックツール(シーア・インサイト・セキュリティ社)		
		向井 徹	421
9.1.1	電子メール関連		421
9.1.2	ログ関連情報(サーバ向け)		422
9.1.3	クライアント PC ログ管理ツール		424
9.1.4	ログ保全・解析ツール		425

9.1.5	ログ管理・監査支援ツール	427
9.2	証拠保全用ハードウェア	守本正宏 428
9.2.1	ハードディスク消去ツール	428
9.2.2	データ複製ツール	429
9.2.3	書込み防止装置	432
9.3	調査・解析用ツール(Guidance Software 社)	伊原秀明 434
9.3.1	概要	434
9.3.2	EnCase の取得機能	435
9.3.3	EnCase の解析機能	439
9.3.4	EnCase のレポート機能	447
9.4	調査・解析用ツール(AccessData 社)	守本正宏 449
9.4.1	ファイル形式の変換とデータベース作成ツール	449
9.4.2	パスワード解析	450
9.4.3	レジストリ保護領域の調査	452
9.5	解析専用コンピュータ	守本正宏 453

第 10 章 デジタル・フォレンジックの今後と課題

(主査・執筆担当：辻井重男)

(1)	IT の浸透による社会構造の変化	457
(2)	技術開発の方向性——情報システムの信頼性向上へ向けて	457
(3)	情報セキュリティ法制度・ガイドライン等の統合的整合性	459
(4)	証拠捕捉の困難性への対策	459
(5)	デジタル・フォレンジック人材の育成	460
(6)	デジタル・フォレンジックによる日本の精神的土壌の変容	461

卷末資料	1.「特定非営利活動法人デジタル・フォレンジック研究会」の紹介	丸谷俊博 463
	2. デジタル・フォレンジックの研究団体・組織一覧	丸谷俊博 467
索引		469

4.5 デジタル・フォレンジックの要素技術

4.5.1 暗号・時刻認証とデジタル・フォレンジック

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、第1章で述べたように、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、「利用者がある個人・機密情報に対してどのような利用をしたかを履歴保存」といった行為で証拠保全が考えられ、そのため履歴のなかに個人・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変更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ざんすることは容易である。デジタル・フォレンジックにおいては、証拠能力が要求されるため、この証拠データ自体が変更されていないこと、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ととなる。別の視点においては、第三者(特に不正者)が証拠としてどのような情報が残っているのかを把握できることは、その証拠保全としての抜け道を探す(フォレンジックシステムのセキュリティホールを解析する)ことに相当する。こ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、証拠データの暗号化技術が必要となる。

ただし、事案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をとらずに復号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(Key Recovery)技術も重要となる。

本項においては、デジタル・フォレンジックと暗号について解説を行う。

(1) データの暗号化

データの暗号化において証拠性、つまり法的な対応までを考慮した際には、政府で求められている要件に近いことが想定される。暗号アルゴリズムの選択にあたっては、それ自体が公開され、CRYPTREC⁹⁾で定めている共通鍵、特に128ビットブロック暗号を前提

9) CRYPTREC(Cryptography Research and Evaluation Committees, <http://www.cryptrec.jp/>)の略で、総務省および経済産業省が共同で開催する暗号技術検討会と(独)情報通信研究機構(National Institute of Information and Communications Technology: NICT)および(独)情報処理推進機構(Information-Technology Promotion Agency: IPA)が共同で開催する暗号技術監視委員会で構成され、特に電子政府推奨暗号の安全性を評価・監視し、暗号モジュール評価基準等の策定を検討するプロジェクトである。

表 4.5.1 CRYPTREC で推奨されている守秘暗号アルゴリズム (2005 年 11 月 30 日時点)

方 式	アルゴリズム
公開鍵暗号(守秘)	RSA-OAEP
	RSAES-PKCS1-v1_5 注1)
64 ビットブロック暗号 注2)	CIPHERUNICORN-E
	Hierocrypt-L1
	MISTY1
	3-key Triple DES 注3)
128 ビットブロック暗号	AES
	Camellia
	CIPHERUNICORN-A
	Hierocrypt-3
	SC2000
ストリーム暗号	MUGI
	MULTI-S01
	128-bit RC4 注4)

注 1) SSL 3.0/TLS 1.0 で使用実績があることから当面の使用を認めている。

注 2) 新たな電子政府用システムを構築する場合、より長いブロック長の暗号が使用できるのであれば、128 ビットブロック暗号を選択することを推奨している。

注 3) 3-key Triple DES は、以下の条件を考慮し、当面の使用を認めている。

①NIST SP 800-67 として規定されていること

②デファクトスタンダードとしての位置を保っていること

注 4) 128-bit RC4は、SSL 3.0/TLS 1.0 以上に限定して利用することを想定している。なお、リストに掲載されている別の暗号が利用できるのであれば、そちらを使用することを推奨している。

出典) CRYPTREC 電子政府推奨暗号アルゴリズムリストより一部引用。

とすることが望ましいと考える。しかし、今現在は表 4.5.1 で示しているようなアルゴリズム、および鍵長が求められているが、暗号技術の危殆化動向は日進月歩であるため、その時点で利用するアルゴリズムについて、外部の評価団体の指針を把握して選定する必要がある。特に、暗号を使用する場合には、暗号の用いられる環境や暗号の安全性を適切に監視することが必要となり、CRYPTREC の活動において、暗号の専門家による評価、実装面での評価・認証を常に行っており、使用する暗号の安全性を確保するには、本団体の活動などを常に把握し、適切に対応することが必要となる。暗号の危殆化が予測される場合には、より強い暗号方式に変更する、暗号鍵長を変更する、などやこれらにより署名などを行い、暗号化されたデータの安全性を確保する対策を早急に行う必要がある。

(a) 暗号の危殆化

暗号の安全性は、時間が経過するとともに変化し、その安全性は損なわれていく。暗号

5.2 法運用とデジタル・フォレンジック

5.2.1 刑事手続とデジタル・フォレンジック

(1) はじめに

刑事手続は、魔女裁判や拷問に代表される人権侵害を防ぐため、憲法や刑事訴訟法で厳格な手続が定められている⁵⁹⁾。デジタルデータ等を対象とするデジタル・フォレンジックに基づき、証拠の収集、犯人の特定、犯罪の立証、刑罰権の執行(犯行供用物件の没収を含む)を行う場合も、その厳格な手続にしたがう必要がある。

ところで、刑事実体法はデジタルデータやその処理に関する刑事罰を設けるようになったが⁶⁰⁾、本稿執筆時点では、刑事手続法令は、証拠を有体物に限る法制のままであり、無形物・無体物であるデジタルデータ(電子ファイル等)の取扱いは解釈に委ねられているのが現状である⁶¹⁾。

刑事手続は、捜査、公訴(起訴)、公判手続(証拠調べ)、判決、刑罰の執行という順序で進むが、いずれの段階においても、デジタルデータに関して、実務上でこれをどう取り扱うかが問題となる。

(2) 捜査

(a) デジタルデータの証拠化

前記のとおり、デジタルデータそのものは、そのままでは証拠とすることができないので、目に見える有体物として証拠化する必要がある。その場合は

- ① デジタルデータが記録された記録媒体(メディア)ごと証拠物として押収する、
- ② デジタルデータを紙媒体に印刷したもの(プリントアウト)を押収する、
- ③ デジタルデータの HDD 等の内容を別の HDD や CD-ROM や DVD にコピーして、そのコピーした HDD 等を押収する⁶²⁾

59) 憲法 31 条(適正手続の保証)、32 条(裁判を受ける権利)、33 条(逮捕の要件)、34 条(抑留拘禁の要件)、35 条(住居の不可侵、搜索押収の要件)、36 条(拷問の禁止)、37 条(刑事被告人の諸権利)、38 条(不利益供述拒否権、自白の証拠能力、自白の証明力)、39 条(罪刑法定主義、一事不再理)、40 条(刑事補償)。

60) 不正アクセス罪(不正アクセス禁止法 3 条違反)、電子計算機損壊等業務妨害罪(刑法 234 条の 2)、電磁的記録不正作出及び供用罪(刑法 161 条の 2 ほか)、電子計算機使用詐欺罪(刑法 246 条の 2)、支払用カード電磁的記録に関する罪(刑法 236 条の 2~5)、公用文書等毀棄罪(刑法 258 条)、私用文書等毀棄罪(刑法 259 条)。

61) わが国も「欧州評議会サイバー犯罪に関する条約」の締結に基づき、デジタルデータに関する捜査手続等を定める刑事訴訟法の改正案ができたが、本稿執筆時点では、この案は国会で審議される段階にとどまっている。

などの方法で、デジタルデータを証拠化しているのが現状である。

なお、証拠の管理者が任意に証拠物件を捜査機関に提出する手続を「任意提出」といい、捜査機関が任意提出を受けた証拠物件を受領する手続を「領置」という。捜査機関が令状等に基づき強制的に押収することを「差押え」という。「押収」は、この「領置」と「差押え」の双方を含む概念である。

(i) メディアごとの押収

これは犯人が犯行に供用したデジタルデータを押収するときに多く用いられている。この場合は、FD、HDD、MD、CD、DVDなどが証拠物として押収されることはもちろん、内蔵HDDごとパソコンやサーバを押収する場合もある。それは、犯人が犯行に供用したパソコン等は犯罪供用物件といってパソコンごと没収の対象となるので、むしろ押収が必須となる場合が多く、また、被害者のサーバと異なり、犯人のパソコンを押収しても、被害が少ないからである。被害者や第三者のパソコンやメディア原本そのものは、これを押収すると被害者らのサーバ利用に支障が生じる場合が多いので、後述③のデジタルデータをコピーしたものを押収する場合が多い。

(ii) 紙媒体にプリントアウトしたものの押収

この方法は、テキストファイルである簡易なログの証拠品化としてよく用いられる。典型例は、電話の通信履歴やアクセスログ、携帯電話の電子メール履歴等である。また、容易な視覚化を確保するため(法執行機関は目で証拠を調べる)、バイナリファイルの場合はASCIIダンプでプリントアウトすべきであろうし、各種画像ファイルなら画像状態でプリントアウト(紙媒体に印刷したもの)すべきである。ただし、印刷したら数万ページとなる膨大なログや多数の画像ファイルは、この方法では不適であるし、動画ファイルはそもそもそのまま全部を印刷するのに不適であるから、これらのものは、③のデジタルデータをコピーしたものを押収する方法がよい。なお、動画の場合は、その要旨を視覚化するため、前記デジタルデータをコピーしたものを押収した上、主要部分をコマ撮りしたものを抜粋して印刷する方法がとられている。

(iii) コピーしたデジタルデータの証拠化

プロバイダなどで、HDD内に証拠となる電子ファイルを発見したが、HDDを差し押さえると業務に支障がある場合には、前記のとおり、デジタルデータを他の媒体にコピーして証拠化することになる。その具体的方法は、①(捜査官媒体・捜査官コピー)捜査官が、

62) 理想論でいえば、削除ファイルの痕跡を捜査する必要がある場合が多いので、可能な限り、イメージコピーでダビングすべきである。

7.7 遠隔医療とデジタル・フォレンジック

7.7.1 遠隔医療と患者のプライバシー保護

近年の情報通信機器の開発・普及にともない、情報通信機器を応用し診療の支援に用いる、いわゆる遠隔診療が徐々に実際の臨床の場でも実用化されつつある。遠隔診療には、①医療の地域格差・施設間格差の解消と医療の質の向上、②医療の効率化、費用の削減、③患者サービスの向上、④診療困難な場に対する診療機会の提供、⑤国際医療協力、など多様な効用が期待される。

しかし、患者情報はいったん漏洩してしまうと回復しがたい被害を及ぼすことがあるため、医療施設間で、情報通信システムを用いて患者情報を利用する場合には、堅牢なセキュリティを確保することが求められる。

米国では、家庭医と専門医が電子メールで患者情報を交換して質の高い医療を供給しようという試みがなされてきたが、医師の多くは患者のプライバシー保護について適切な措置がとられるかどうかを案じて消極的であったとされている。また、不正な患者情報へのアクセスが既に社会問題化し、議会は患者情報への機密性保持のための立法措置をとった。わが国においても個人情報保護法と、これを受けた適正な取扱いの確保および安全性確保のためのガイドラインが制定されており、遠隔診療では、セキュリティ技術の採用により不正なアクセスを可及的に防止することが不可欠である。

遠隔医療実施によって、患者のプライバシーが侵害された場合、医師は、患者から損害賠償責任を問われ得る。この場合、問題となるのは、患者に対してプライバシー侵害の危険について告知がなされていたか、適切なセキュリティ対策が採られていたか、などの点である。異なる施設間で情報の交換を行う場合には、契約等によりセキュリティに関する責任範囲を明確にし、管理の責任の所在を明らかにする必要がある。

このように、遠隔医療における患者の情報セキュリティ対策の重要性は強調されてきているが、完全無欠のセキュリティはあり得ないため、遠隔医療の分野においてはデジタル・フォレンジックの概念が今後重要性を増してくると考えられる。ここでは、これまで慶應義塾大学医学部外科における遠隔医療の研究において取り組んできた情報セキュリティの実例を紹介し、今後のデジタル・フォレンジックへの展望を概説する。

7.7.2 遠隔医療の歴史

わが国の遠隔医療の歴史(表 7.7.1)は、1971 年、和歌山県での CCTV (closed circuit television) 回線および電話線による実験に端を発する。200 km の心電図伝送実験が行われ、遠隔医療の技術的可能性が示された。その後、1980 年代に入り通信衛星や ISDN など、

表 7.7.1 遠隔医療の歴史

年	主な出来事
1971	和歌山県山間へき地での実験(CCTVと電話)
1982	東京都三鷹市での実験(INS64、56~128 Kbps)
1985	長野県諏訪市で在宅医療実験(CATV)
1996	慶大、AESOP2000のライブデモ(日本内視鏡外科学会)
1999	慶大、遠隔手術指導(ISDN×3回線、384 Kbps)
2000	慶大・京大、施設間ドミノ肝移植(ISDN×3回線) 慶大、ロボット手術と遠隔手術指導のライブデモ(日本外科学会)(ISDN×3回線)
2001	米仏間、Lindbergh手術(ATM、10 Mbps)
2002	慶大・東京医療センター、インターネットを利用した遠隔手術支援(ADSL、1~2 Mbps)
2004	慶大・東京医療センター、遠隔共同手術(DVTS、70 Mbps)

その時代の通信技術を利用した試みが研究されてきたが、画像の質やコストの面などで制約があり普及するには至らなかった。

慶應義塾大学医学部外科では1990年代半ばより外科領域における遠隔医療の研究を進めてきた。1996年の日本内視鏡外科学会総会のライブデモでは、学会会場から慶應義塾大学病院手術室のAESOP2000を音声でコントロールし、遠隔地から手術に参画し得ることを実証した。その後、遠隔手術指導や、遠隔カンファレンスの技術を用いた研究を進めてきたが、もっぱら専用回線を利用してきたことと、セキュリティに対する社会的要請が低かったため、当時は情報セキュリティに関してことさら配慮することはなかった。

2001年からは、遠隔医療の普及のためにはインターネットなどの広域ネットワークの利用が不可欠と考え、その臨床応用の可能性を検討してきた。しかしながら広域ネットワークにおいては、典型的に要保護性の高い医療情報を扱う上で、高度にセキュリティを確保することが要求される。また情報漏洩やハッキングなどの事例が報道されるようになり、セキュリティに関して社会的な関心が高まりつつあるのもこの時期であった。外科領域における遠隔医療では高画質な動画像がリアルタイムで伝送されることが必須の条件となるが、このような大容量の情報を強固に防御するには、従来、高性能のコンピュータを必要としたため実用化が困難であった。そこで筆者らは2002年に、暗号強度と通信速度が両立可能なカオス信号を応用した新しい暗号技術を利用することで高いセキュリティを確保しつつ、インターネットを介してリアルタイムに動画像を転送し得るシステムを構築した。さらに2004年には遠隔地の指導医がリアルタイムに高画質画像を見ながら、手術用内視鏡をコントロールして手術を指導する遠隔共同手術システムを臨床応用するに至った。

7.7.3 動画伝送時のセキュリティの研究

筆者らは、遠隔医療における暗号化の強度と能率の検討を行った。暗号強度と通信速度が両立可能なストリーム系共通鍵暗号であるC4S暗号技術を用いて情報伝送のシステム

9.3 調査・解析用ツール(Guidance Software 社)

9.3.1 概要

EnCase は、米国ガイダンスソフトウェア社(Guidance Software, Inc)が開発・販売している商用のコンピュータ・フォレンジックツールの一つであり、米国の司法機関(FBI、CIA)、民間企業などで多くの利用者をもつ。

EnCase は Windows 上で動作する GUI アプリケーションであり、主にハードディスクおよびファイルシステム(イメージファイル)を対象とした調査・解析用ツールである。機能として大きく①取得、②解析、③報告の3つをもっている。EnCase を利用することで、ハードディスクのイメージファイルの作成(取得)、取得したイメージファイルに含まれているファイルやデータの調査(解析)、調査した結果レポートの作成(報告)までを一通り実現することができる。

EnCase 製品のラインナップとしては、スタンドアロン環境で利用する EnCase Forensic 版(FE)と、3千台以上の PC を所有する大規模環境での利用を想定した EnCase Enterprise 版(EE)に分けることができる。

本節で解説している EnCase は、基本的にスタンドアロン版の EnCase FE を対象としている。EnCase EE は、EnCase FE の機能をネットワーク経由で利用できるようにしたものであり、主に大規模環境向けの製品となっている。

FE 版が保全したハードディスク(電源を落としてから複製したもの、デッドコピーと呼ばれる場合もある)を解析対象とするのに対し、EE ではサブレットと呼ばれるエージェントプログラムを調査対象システムへインストールし、実行しておく必要がある。調査員は EE のサブレットに TCP/IP ネットワーク経由で接続し、該当システムの調査を実施することができる。TCP/IP で通信できる環境であれば、遠距離にあるシステムの調査も即時に開始できることから、現地まで移動してから複製し調査を開始するといったタイムラグが発生しない。EE は TCP/IP ネットワークを経由して操作すること以外は、基本的に FE と同等の機能をもち、スタンドアロン版で可能なことがネットワーク経由ですべて可能となる。スタンドアロン版との最大の違いは、EE では調査対象のシステムを稼働させたまま調査することが可能な点にある。これにより、重要なサーバシステムなどを停止することなく調査することが可能になり、従来の電源を落としてから調査する場合に発生していたシステム停止時間の発生問題を解決することが可能となっている。

捜査機関が稼働中システムを停止することなく捜査できるようにする EnCase Field Intelligence Model(FIM)も EnCase EE と同じ技術で構成されており、稼働中のシステムに対する調査機能(揮発性情報の取得など)が特徴となっている。FE と EE それぞれの製品

詳細については EnCase の Web サイトを参照していただきたい(<http://www.encase.jp/>)。

9.3.2 EnCase の取得機能

EnCase はハードディスクや USB ドライブなどのビットストリームイメージ⁵⁾を取得(複製)する機能をもっている。EnCase の取得機能を利用することで、ハードディスクドライブ(物理ディスク)の内容を論理的な証拠ファイル(イメージファイル)として複製・保存することが可能になる。作成された証拠ファイルは、EnCase へロードすることで、イメージファイルに含まれているファイルやデータにアクセスできるようになる⁶⁾。

(1) イメージファイルの取得方法

EnCase はビットストリームイメージを取得する方法として、①MS-DOS ベースの FD や CD-ROM から起動する EN.EXE プログラムを利用して取得する方法と、②Windows 上の EnCase プログラムから取得する方法の2つを用意している。

(a) EN.EXE を利用して証拠イメージを作成

EnCase には、DOS 環境で実行することができる EN.EXE が付属している。EN.EXE は Windows 付属のコマンドプロンプトではなく、純粋な MS-DOS 環境で実行する必要がある。

EN.EXE を利用することで、FD または CD-ROM から起動した MS-DOS 環境からハードディスクのプレビュー(後述)や、証拠イメージ(E01 形式ファイル)の取得を実行することができる。

EN.EXE は EnCase のパッケージに付属しているが、起動ディスクはガイダンスソフトウェア社の Web からダウンロードすることができる。ここでは FD のイメージと CD-ROM の ISO イメージが提供されている。

起動ディスクには、①スタンドアロン環境で利用する EnCase Barebones Boot Floppy Image と、②クロスケーブル接続で利用する EnCase Network Boot Disk (ENBD) の2つのタイプがある。クロスケーブル接続を利用する ENBD の起動ディスクには、ネットワークインタフェースカード(NIC)のドライバが組み込まれており、対応する NIC を利用することで、クロスケーブル経由で別の PC 上の EnCase から、調査対象 PC のハードディスクへアクセスできるようになる。なお、ENBD での接続はクロスケーブルを利用した1対1での接続となる。

ガイダンスソフトウェア社の Web から入手できる MS-DOS 起動ディスクは、証拠イ

5) ハードディスクなどの内容をセクタ単位で読み取りファイル化したもの。

6) EnCase は証拠ファイルを読取り専用でアクセスするのでデータ内容が変化することはない。