

## 刑事事件におけるデジタル・フォレンジックと証拠

安 富 潔

### 1 はじめに

情報通信技術の発達とともに、コンピュータ、タブレット端末、携帯電話、スマートフォンなどの普及により、サイバー犯罪に限らずさまざまな犯罪に電子機器が悪用される事態が生じている。

コンピュータや携帯電話などを利用した犯罪では、被疑者等により関連する情報が改ざん、削除されたり、通信内容が暗号化されていることがある。ときには、被疑者が携帯電話などそれ自体を破壊して証拠隠滅を図ることもある。

そして、接続経路の匿名化を行うソフトを利用したパソコン遠隔操作事件では、誤認逮捕という事案も生じたことは周知のところである。

今後、クラウドコンピューティングの進展とともに、さまざまなリスクも想定されるところであり、そこでの犯罪の証拠の収集・保全是喫緊の課題となろう。

ところで、電子機器等に保存されている犯罪の証拠となる電磁的記録を刑事裁判において証拠として用いるためには、対象となる電子機器等から電磁的記録を抽出し、解析をし、裁判官・裁判員がその知覚によって認識することができるようにしなければならない。

そこで、デジタル・フォレンジック技術を用いて、電子機器等やハードディスクなどの電磁的記録媒体に保存されていた電磁的記録を復元し、証拠となる情報を抽出・解析等することが行われる。

## 2 デジタル・フォレンジック

デジタル・フォレンジックとは、広義では、電子データ（電磁的記録）の保全と解析をいう。

刑事事件において、デジタル・フォレンジックは「犯罪の立証のための電磁的記録の解析技術及びその手続」<sup>(1)</sup>との定義が広く用いられている。

デジタル・フォレンジックは、さまざまな場面で利用されるが、<sup>(2)</sup>刑事手続との関連においては、犯罪の証拠としての電磁的記録の収集・保全及び解析という観点から、<sup>(3)</sup>用いられる。

もっとも、刑事裁判では捜査機関が強制処分として電子計算機に対する検索・差押えを行い（刑訴法 218 条 1 項・2 項）、情報技術解析の専門組織<sup>(4)</sup>によりデジタル・フォレンジック技術を用いて解析した結果をもとに、検察官が訴追することができるのに対し、被疑者・被告人側は自ら電磁的記録を解析して、証拠とするというより、捜査機関の成果を証拠開示という形で再利用するしかない立場におかれているので、被疑者・被告人側が積極的にデジタル・フォレンジック技術を活用するという局面は限られている。<sup>(5)</sup>

サイバー犯罪に限らず、およそさまざまな犯罪の実行にあたって、電磁的記録が証拠となることは決して少なくない。

サイバー犯罪における被疑者の特定や被害の実態把握、一般犯罪における犯人性立証のためのコンピュータや携帯端末での電子メールやインターネット検索・閲覧履歴等の解析、経済犯罪での帳簿類等の関係証拠の収集・保全などにデジタル・フォレンジック技術がしばしば利用されている。

デジタル・フォレンジックでは、電磁的記録媒体に記録されている電磁的記録について、その電磁的記録が意味している内容をそのまま過不足なく、何らかの恣意的な行為や解釈を差し挟むことなく証拠化することが求められる。<sup>(6)</sup>そのためには、「手続の正当性」「解釈の正確性」「第三者検証性」<sup>(7)</sup>が重要とされている。

例えば、ハードディスクを調査対象とする場合、① 調査対象コン

コンピュータのハードディスクの電磁的記録を全く書き換えることなく、複製を作成して証拠保全を行う（証拠保全）、② 証拠保全したハードディスクの電磁的記録を解析して、調査対象コンピュータの使用者が何をしていたのかを調査・特定する（電磁的記録の解析・抽出）、③ 刑事裁判において用いられることを想定して、解析した結果の報告書を作成する（報告書作成）ことがデジタル・フォレンジックを用いた証拠化の手順である。

もっとも、ハードディスクを調査対象とするにしても、電磁的記録がすべて暗号化されていたりすれば、暗号化された記録を解く鍵がないと内容を調査できないし、ハードディスクに痕跡が残らないように削除されていたときには完全な復元ができない。さらに、調査に用いるツールは解析できるファイルシステムや解析性能等が異なるので、ツールの性能的な限界が調査の限界ともなることがある。ときには、不正なアクセスをした際の通信ログを上書き改ざんしたり、不正なファイルを消去した際の記録をシステム上から消去したりするなどのアンチ・フォレンジック工作のためのツールを利用した妨害工作が行われることもある<sup>(8)</sup>。そして、調査対象コンピュータから物理的コピーの複製を行う証拠保全作業において、昨今のハードディスクは大容量化してきており、保全作業にかかる時間も相当かかる状況にある<sup>(9)</sup>。電磁的記録は、可視性・可読性がないということから、関連すると思われるハードディスクについて保全することとなるが、ハードディスクの数が多ければ、それだけ時間がかかることになって、迅速な捜査に支障を来すこともなくはない。

ことに、昨今、電磁的記録媒体が多様化し、コンピュータだけでなく、携帯電話、スマートフォンをはじめ、デジタルカメラ、防犯カメラ、ハードディスクドライブレコーダー、ゲーム機、PDA、デジタル複合機、ナビゲーションシステム、メモリーカード、ICカード、無線タグなどさまざまな電子機器に記録される情報に対して様々な手法のデジタル・フォレンジックが用いられている。また、フォレンジックも、これまでのようなデジタル・フォレンジックからネットワーク・フォレンジックへと展開されてきている<sup>(10)</sup>。

## 註

- (1) 平成 26 年警察白書 30 頁（警察白書では、2006 年から本文の定義が用いられている）。なお、デジタル・フォレンジックの定義については、「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及び調査・分析を行うとともに、電磁的記録の改ざん・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・技術をいう。」と利用目的と機能から定義することもある（デジタル・フォレンジック研究会編（舟橋信、安富潔編集責任）『改訂版デジタル・フォレンジック事典』（日科技連出版社、2014）5 頁参照）。

アメリカ合衆国での問題を簡潔に整理したものとして、Daniel B. Garrie and J. David Morrissey, Digital Forensic Evidence in the Courtroom: Understanding Content and Quality, 12 Nw. J. Tech. & Intell. Prop. 121 (2014), <http://scholarlycommons.law.northwestern.edu/njtip/vol12/iss2/5> がある。

- (2) 民事訴訟では、アメリカ合衆国において 2006 年に連邦民事訴訟規則が改正され、電子的に保存された文書を証拠として開示する e-Discovery 手続が規定されたが、e-Discovery に際して、コンピュータシステムや電磁的記録に残されたデータやログの調査やセキュリティ監査の手法として、デジタル・フォレンジックが活用されている。

e-Discovery については、守本正宏『日本企業のディスカバリ対策：世界と対等に戦うための e ディスカバリの正しい手順』（グローバルトライ、日本著作出版支援機構、2013）、土井悦生＝田邊政裕『米国ディスカバリの法と実務』（発明推進協会、2013）、守本正宏ほか『ディスカバリ～カルテル・PL 訴訟・特許訴訟～米国民事訴訟のディスカバリ対応から学ぶ国際的法律問題を有利に解決する” ディスカバリ” の正しい知識 eDiscovery』（起業家大学出版・2012）、町村泰貴＝小向太郎編著『実践的 e ディスカバリ 米国民事訴訟に備える』（NTT 出版・2010）などがある。

また、わが国においても、平成 22 年の金融商品取引法改正により、IT 技術を利用した内部統制が求められたことや国際会計基準の導入に際する証拠データの保全等の必要性に鑑み、デジタル・フォレンジックが利用されているほか、企業のリスク管理として、個人情報、企業情報等の管理と企業活動の健全性を証明する技術としてもデジタル・フォレンジックが用いられている。

- (3) 電子証拠の取扱いでは、本来的には、民事事件と刑事事件とで根本的に異なるわけではない。民事事件であれ刑事事件であれ、事実認定者（裁判官・裁判員）が、電磁的記録の内容を認識するためには、少なくともその内容を見聞きできる形態にしなければならず、デジタル情報それ自体では内容を見聞きすることができないので事実認定の資料にならない。従って、デジタル情報の原本性の確保、メタデータも含めた保全、その見読可能化、それぞれの

過程における正確さの確保は、民事事件・刑事事件を問わずに妥当する。町村泰貴「電子証拠の取扱と訴訟法の違い」<https://digitalforensic.jp/2014/07/14/column319/>

- (4) デジタル・フォレンジック技術を用いての解析にあたっては、解析過程の信頼性の確保とそのため技術者の技術水準・技量が重要である。

2014年に発生したいわゆる遠隔操作事件では、警視庁・大阪府警・神奈川県警・三重県警の解析担当者の技術力と解析作業における組織的管理が必ずしも十分であったとはいえなかったために、捜査部門との連携と情報の共有がなされなかったことから、誤認逮捕がなされてしまった。警視庁「インターネットを利用した犯行予告事件における警察捜査の問題点等について」<https://takagi-hiromitsu.jp/misc/misidentification2012/tokyo.pdf>「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」(季刊刑事弁護 73号 149頁以下、2013、<https://takagi-hiromitsu.jp/misc/misidentification2012/kanagawa.pdf>)、大阪府警察「インターネットを利用した犯行予告ウイルス供用事件の検証結果」<https://takagi-hiromitsu.jp/misc/misidentification2012/osaka.pdf>、三重県警察「インターネットを利用した犯行予告・ウイルス供用事件(伊勢神宮に対する威力業務妨害事件)の検証結果」<https://takagi-hiromitsu.jp/misc/misidentification2012/mie.pdf> 参照。これらの検証結果を受けて、警察庁は、刑事局長等の通達として「インターネットを利用した犯行予告・ウイルス供用事件の誤認逮捕事案を受けた今後のサイバー犯罪捜査の在り方について」<http://www.npa.go.jp/pdc/notification/keiji/keiki/keiki20121214.pdf> を発している。

大橋充直「検証サイバー(ハイク)犯罪の捜査(第86回)遠隔操作真犯人事件の判決(その1)～(その2)」捜査研究 769号 76頁、同 770号 86頁参照。

- (5) 検察官から開示された電磁的記録の解析過程の正確性・信頼性をデジタル・フォレンジック技術専門家の協力で検討するとしても、時間と費用との制約があることは否めない。
- (6) 羽室英太郎＝國浦淳『デジタル・フォレンジック概論』177頁(東京法令出版、2015)。
- (7) 羽室＝國浦・前掲注(6) 22～24頁。

なお、電磁的記録媒体に記録された電磁的記録は、専用の物理的複製送致を用いて、原本となる電磁的記録と全く同じ物理コピーを作成することが可能であり、原本である電磁的記録との同一性は、ハッシュ値を計算することによって、その一致をもって確認できる。この点は、例えば、DNA型鑑定などで用いられる微細な細胞片を用いた鑑定では全量消費となることがあり、第三者による検証の可能性が担保されないが、デジタル・フォレンジックを

用いての電磁的記録の解析では、第三者検証性が担保される。

なお、不正プログラムの調査について、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17回不正プログラムの調査について」捜査研究 769号 102頁以下参照。

- (8) アンチ・フォレンジック・ツールが利用されることにより、偽装工作で調査が妨げられるとはいえ、フォイルとは異なる別の痕跡や不自然さは残るので、悪意による利用を推認することができる。

独立行政法人情報処理推進機構『情報セキュリティ白書』（2011年）65頁参照。

- (9) 例えば、高速なハードディスク複製装置の米国の Intelligent Computer Solutions Image MASter Solo-4 G3 Forensic Enterprise では、転送速度分速 32 ギガバイトとされているが、1 テラバイトのハードディスクであれば、保全処理に約 30 分程度の時間で済むが、容量の大きなハードディスクであればそれだけ時間がかかるし、多数のハードディスクを物理コピーするとなると、いっそう保全処理に時間がかかることになる。
- (10) デジタル・フォレンジックでは、電磁的記録を解析して証拠化することが主眼であるが、ネットワーク・フォレンジックでは、サイバー攻撃の実態解明を目的に、ログ等の解析を通して攻撃プロセスを特定していくことが求められる。デジタル・フォレンジック研究会・前掲注 (1) 61～62 頁。

### 3 デジタル・フォレンジックと刑事証拠法

刑事訴訟法第 317 条は「事実の認定は、証拠による。」として、犯罪事実については、証拠能力があり、適式な証拠調べを経た証拠によって認定しなければならないと定めている。

「証拠により認定される事実」と「事実に対する法的判断（意見・主張）」<sup>(11)</sup>とは、厳密に区分されることに留意することが必要である。

証拠は、事実認定の資料であるが、犯罪事実の認定にあたっては、証拠として用いることができ（証拠の許容性）、そして、その証拠に一定の証明力がなければならない。

証拠能力は、証拠として公判廷で取調べをすることができるという形式的な資格をいう。起訴状に記載された公訴事実を証明することができる証拠であっても、公判廷で取り調べることによって、裁判官に証明力の評価

を誤らせるおそれがあることもあるし、捜査手続に重大な違法があつて証拠とすることが正義に反するといえる場合には、証拠能力がないとされる。また、証明力は、証明しようとする事実の認定にその証拠がどの程度有用で裁判官が心証を形成することができるかという観点にたつての証拠の実質的な価値をいう。

ある証拠につき証拠能力が認められるには、その証拠が立証しようとする事実との間に関連性を有していなければならない。

関連性は、一般に、自然的関連性と法律的関連性に分けられる。

自然的関連性とは、証拠によって証明しなければならない犯罪の成否に関する事実を推認させるのに必要な最小限度の証明力がなければならないことをいう。自然的関連性のない証拠を取り調べてみても意味がないからである。また、自然的関連性がある証拠でも、裁判所に予断や偏見を抱かせたり、争点を混乱させたり、相手方、ことに被告人に不公正な不意打ちを与えるような証拠であつてはならない。これを法律的関連性という。

他方、証明力の判断は裁判官の自由な判断に任され、裁判官は法の拘束を受けずに経験則・論理則に従つて合理的に証明力の程度を判断する（刑訴318条）。

電磁的記録が証拠とされる場合には、まず証拠となる電磁的記録に証拠能力がなければ、公判廷で取り調べることができない。もっとも、電磁的記録は、「電子的方式、磁氣的方式その他人の知覚によつては認識することができない方式で作られる記録であつて、電子計算機による情報処理の用に供されるものをいう。」（刑7条の2）と定義されることから、電磁的記録媒体から出力・印刷し、又は複写された電磁的記録を印刷するなどして、可視性・可読性のある文書としてはじめて事実認定者にとってその内容を証拠とすることができる。ここでは、電磁的記録と出力された文書内容との同一性がまず問題となるが、これについては、保全された電磁的記録について印刷プログラムを用いて文書とした者が、その作成の真正を公判廷で証言すれば足りる。また、印刷された文書の原本性については、いくつもの立場が考えられようが、適正な手続で電磁的記録を保全している

場合に、その電磁的記録を可視性・可読性のある文書として印刷していれば印刷された文書を原本としてよい。<sup>(12)</sup>

さて、適法に差し押さえられた電磁的記録からデジタル・フォレンジックを用いて解析した結果が証拠として要証事実を証明することができることになるといえるためには、電磁的記録媒体に記録された電磁的記録と同一の保全記録とされ、その保全記録から証拠として意味がある記録が抽出され、抽出された記録を解釈することによって間接事実を認定することができる。<sup>(13)</sup>

ところで、一般に、捜査において、科学的知見・技術・成果を利活用して得られた証拠を科学的証拠という。

デジタル・フォレンジック技術を用いて解析された結果の報告文書も、科学技術を用いていることから科学的証拠の一つである。

科学技術の進歩に伴い、捜査において、新規性のある科学技術を活用して客観的証拠の収集がなされ、その結果が犯罪現場の遺留物件についての同定（Identification）や同一性確認ないし異同識別という個別化・特定化（Individualization）のために用いられることがある。

科学的知見や技術を活用した捜査は、事実認定の精度を高めると同時に人権保障にも寄与する側面をもつ。しかし、「科学」への過信や偏見はかえって誤った事実認定をもたらすものとなる。そこで、科学的証拠について事実認定に用いることができるためにはどのような要件が必要かということが問題となる。<sup>(14)</sup>

科学的証拠は、その科学的理論と方法の合理性が一般的に承認されていること、及び結果の信頼性が認められる場合には、その証拠の証拠能力が認められる。具体的には、①専門の知識・技術を有し、経験のある資格者によって、②真正で鑑定に適した資料について、③性能・作動の面で誤りのない装置・器械を用いて、④適正な手法・手続によって実施され、⑤その経過と結果が正確に書面に記載されているかどうかを検討し、類型的・定型的に鑑定の正確性・確実性の保証が欠けているとまでいえないれば自然的関連性が認められると一般に解されている。<sup>(15)</sup>



刑事裁判の実務では、科学的証拠を唯一ないし決定的なものとして、有罪としたものはない。科学的証拠は、事実認定において、他の証拠との総合的判断において考慮されている<sup>(16)</sup>。

## 註

- (11) 人が体験した事実から推測したものでない、単なる評価・意見・主張は証拠とはならない。」(意見証拠)とされる(最大判昭和24年6月13日刑集3巻7号1039頁参照)。
- (12) 安富潔『ハイテク犯罪と刑事手続』261頁(慶應義塾大学出版会、2000)参照。なお、デジタル・フォレンジックを用いた解析結果の問題とは局面を異にする問題であることに留意する必要がある。
- (13) デジタル・フォレンジックと刑事手続での証拠の問題を周到に検討したものの、吉峯耕平「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」季刊刑事弁護77号134頁がある。同143～148頁では、フォレンジック報告書が証拠として用いられるにあたって、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を「証明力評価の3要素」とよび、これら进行评估することによって、証拠提出者が主張する要件事実の評価をなし得るとする。
- (14) アメリカ合衆国では、伝統的に専門分野での一般的承認を要するとの立場(Fryev. United States, 293 F. 2d 1013 (D.C. Cir. 1923))が採用されていたが、1975年アメリカ合衆国連邦証拠規則の制定に伴って、裁判官が「関連性(relevancy)」と「信頼性(reliability)」という基準に従って判断するという立場(Daubert v. Merrell Dow Pharmaceuticals, Inc., 509 U.S. 579 (1993))が判例によって採られることとなった。この裁判例は、アメリカ合衆国連邦証拠規則では、関連性のある証拠には許容性が認められ(同規則402条)、鑑定人は特定の分野において合理的情頼を置き得るようなものを基礎に鑑定意見又は推論を形成することができるとされている(同規則703条)ことを根拠とする。とはいえ、科学的知見をもたない裁判官が関連性と信用性という基準に基づいて科学的証拠の許容性を判断することになることから、その懸念も示されている(Renquist判事の一部反対意見)。

Daubert判決及びその後の議論について、成瀬剛「科学的証拠の許容性(2)」法学協会雑誌130巻2号161～183頁参照。

- (15) 科学的証拠の自然的関連性について、園原敏彦「証拠の関連性」松尾浩也＝岩瀬徹編『実例刑事訴訟法Ⅲ』121頁(青林書院、2012)は、科学的証拠の自然的関連性は、証拠採否の段階での科学的証拠が必要最小限の臨明力を

有する蓋然性があるかどうかの予測的判断であり、検査・判定の基礎にある科学的原理の実用化のための現論・技術を含め、その検査・判定方法信頼性に軍大な欠陥あるいは大きな疑問があるとはいえないことと理解できるという。

- (16) 家令和典「裁判員裁判における科学的証拠の取調べ」『新しい時代の刑事裁判』（原田國男判事退官記念論文集）211 頁（判例タイムズ社、2010）は「科学的法則を応用した技術に理論的妥当性があり、当該事案における用い方が相当なものであれば、証拠能力を肯定し、その証明力について詳細に検討するという手法をとってきたと考えられる」と指摘している。

## 4 デジタル・フォレンジックを用いた解析結果に関する裁判例

被告人の犯人性が争点となった事案で、インターネット閲覧・検索履歴の解析結果を間接事実を立証する証拠のひとつとして事実認定をしている裁判例がいくつかある。

### （１）裁判員裁判非対象事件

大阪地判平成 22 年 5 月 25 日（平成 21 年（わ）第 1420 号・傷害被告事件）判例タイムズ 1346 号 247 頁

#### 【事案の概要】

被告人は、平成 20 年 10 月 17 日午前 1 時 25 分ころ、大阪府茨木市 a 町 b 丁目 c 番 d 号付近の路上において、歩行中の A（当時 28 歳）に対し、自転車で追い抜きざまに、背後からその後頭部をハンマー様のもので 1 回殴打する暴行を加え、よって、同人に加療約 1 週間の頭部挫創の傷害を負わせたとして起訴された。

#### 【判決】

裁判所は、「被告人のみが使用していたパソコンのインターネット閲覧履歴の解析結果によれば、被告人は、本件に関する多数の検索を行う中で、10 月 23 日に、インターネットの検索サイトで、『茨木、ハンマー』の条件で検索を行っているが、この時点で、本件犯行の凶器を『ハンマー』とする報道はなかった。

パソコンの解析結果によれば、10月18日及び19日に、多数回に渡って、本件に関すると思われる条件での検索やサイトの閲覧がなされており、被告人自身も、公判廷において、本件に関するインターネットでの検索やウェブページの閲覧をした旨述べている。

以上のように、本件以後、被告人が本件に関して高い関心を抱いていたこと、本件について凶器である可能性のあるハンマーに限定した検索を行っていたことは、特異な行動といえ、被告人が犯人であることを疑わしめる事情ではある。」としつつ「しかし、被告人の前記のようなやや特異な行動は、必ずしも被告人が犯人であることにのみ結びつく事実とはいえないから、(中略)独立して犯人性を推認させる価値は低く、犯人性を判断する上で重要な事情とはなり得ない。(中略)したがって、被告人の犯人性を検討する上では除外するのが相当である。」と判示した。<sup>(17)</sup>

本件の事案は、路上を歩行中の被害者に対して、自転車で追い抜きざまに、背後からその後頭部をハンマー様のもので殴打して傷害を負わせたというものであるが、公判では、被告人の犯人性が争点となった。被害者は、犯行にあう5分ほど前にジョギング中にすれ違っためがねを掛けた自転車にまたがった状態の不審な男と、自転車に乗って逃げる犯人の後ろ姿を目撃し、そのすれ違った男と犯人とは同一人物であると思うが、そのすれ違った男は被告人であったなどと供述していたことから、この被害者供述や、その他の事実から、被告人が犯人であると認定できるかが問題となった。被告人の犯人性認定の間接事実のひとつとして、犯行後の被告人のインターネット閲覧履歴について、本件凶器である可能性の高いハンマーについて閲覧していることは、被告人の犯人性を肯定する積極事情といえるが、被告人の過去の行動からすると、そのような行動にでることは不自然ではなく、犯人性を検討する事情から除外するという判断をしていることが注目される。<sup>(18)</sup>

確かに、一般的には、被告人の特異な行動は、被告人の犯人性を肯定する積極事情ということはできようが、そのみで直ちに被告人が犯人であ

るとすることはできない。動機や目的を立証趣旨として、インターネット閲覧履歴が証拠請求されることがあるが、関連性や重要性の観点から慎重に判断されるべきである。

## (2) 裁判員裁判対象事件

裁判員対象事件においても、被告人と犯人との同一性が争点となった事件でパソコンのインターネット閲覧履歴や電子メールについて、犯人性を推認する間接事実のひとつとして証拠として検討した事案がいくつかある。  
ア 岐阜地判平成 23 年 1 月 28 日（平成 22 年(わ)第 276 号・現住建造物等放火被告事件<sup>(19)</sup>）

### 【事案の概要】

裁判所の認定した事実によれば、被告人は、岐阜県揖斐郡所在の A が現に住居として使用する□□神社に放火しようと企て、平成 22 年 4 月 23 日午後 7 時 30 分ころ、同神社社務所内において、同神社保管の軽油約 40 リットルを、寝室、台所及び廊下等に撒いた上、寝室のベッドの上にあった布団にマッチで点火して放火し、その火を同社務所の柱等に燃え移らせ、よって、木造瓦葺き平屋建ての同社務所、木造トタン葺き平屋建ての渡り廊下、木造瓦葺き平屋建ての斎館を全焼させるとともに、木造（梁が一部鉄骨）瓦葺き平屋建ての本殿の天井の一部を焼損させたものであるというものである。

弁護人は、真犯人は別人として放火の事実を争ったが、裁判所は、犯行前に被告人が犯行をほのめかすメールを送信していること、犯行後に診察した複数の医師に対して、犯行を認める供述をしていることなどから犯人であることが強く推認され、上申書、弁解録取書の内容が信用できることも併せ考慮すると、被告人が犯人であるとした。

### 【判決】

裁判所は、被告人には放火をする動機がないとの弁護人の主張について、被告人が使用していたパソコンのインターネット閲覧履歴等からは、被告人が健康状態に関心を有していたことが認められるし、また、被告人の携

携帯電話から送信されたメールの内容などからすると被告人に家族関係に関する悩みがなかったとはいえないとして、「被告人が以前から度々うつ症状や不安定な精神状態に陥ることがあったことを前提とすれば、このような健康状態に関する悩み及び家族関係に関する悩みは、自殺を企てる動機として十分ありうるものであると考えられる。犯行の動機がない旨の弁護人の主張には理由がない。」と斥けた。<sup>(20)</sup>

そして、「犯行前に被告人が犯行をほのめかすメールを送信していること、犯行後に、被告人が医師らに対して犯行にかかわったことを認める供述をしていることは、いずれも、被告人が本件犯行の犯人であることを推認させるものであり、このような犯人であることを推認させる事実が複数存在することにより、被告人が本件犯行の犯人であることは非常に強く推認されるといえる。」として被告人が犯人であるとした。

イ 金沢地判平成 24 年 3 月 2 日（平成 23 年(わ)第 70 号・強盗殺人、死体遺棄被告事件）<sup>(21)</sup>

#### 【事案の概要】

裁判所の認定した罪となるべき事実によれば、被告人は、(1) 平成 22 年 11 月 17 日ころ、知人の A から、従前から持ちかけていた株式投資のための資金名目で、現金 800 万円を受領したが、平成 23 年 1 月 19 日ころ以降、同女から、複数回にわたり、元金として受け取った 800 万円を含む運用益等の支払いを迫られていたところ、その支払いに窮し、同女に対する債務の支払いを免れるために、成り行きによっては、同女を殺害するのちやむを得ないなどと考え、同年 2 月 6 日午後 9 時ころ、同女を呼び出した上、同日午後 9 時 35 分ころから同月 7 日午前 2 時 16 分ころまでの間に、金沢市内又はその周辺に駐車した普通乗用自動車内において、前記運用益等の支払いを免れる目的で、同女（当時 27 歳）に対し、殺意をもって、所携の刃物でその左頸部を数回突き刺し、よって、そのころ、同女を頸部刺創に基づく出血性ショックにより死亡させて殺害し、もって同女に対する債務の支払いを免れて財産上不法な利益を得た、(2) 前記日時ころ、石川県河北郡内灘町字大根布地内砂浜にお+いて、前記 A の死体を埋め、

もって死体を遺棄したというものである。

裁判では、被告人が犯人であるか否かが争点となった。

裁判所は、被害者女性が被告人に会いに行く旨述べて外出してから遅くとも2時間以内に被告人車輦内で殺害されていること、犯行後間もない時期の被告人のインターネット検索に、同女が殺害され海岸に遺棄されていることをうかがわせるものがあること、アリバイ工作及び偽装工作があること、同女に支払う金員の用意ができないまま、金銭の用意ができたと虚偽の事実を伝えて、同人を呼び出したことがうかがわれることなどから、被告人は、債務の支払を免れるため、被害者を殺害するのやむを得ないとの意思を有していたとして、強盗殺人、死体遺棄の成立を認めた。

#### 【判決】

裁判所は、犯行当日後の被告人の行動等について、被告人方のパソコン（以下「自宅パソコン」という。）のインターネット検索履歴から、「被告人は、平成23年2月7日午前2時16分ころから同日午前3時27分ころにかけて、被告人方において、自宅パソコンを用いて、「血の臭い 消す」「殺人 懲役」「海岸 白骨」などといった語句を、インターネットで検索している事実が認められる。」とし、「このインターネット検索は、被害者が殺害された時点と極めて近接した時期においてなされたものであり、かつ、その検索語句には、被害者が殺害され、その死体が海岸に遺棄されていることをうかがわせるものが含まれていることから、この時点で、被告人は被害者がこうした状況にあることを把握していたことをうかがわせるものであり、被告人が犯人でなければ、説明することが極めて困難な事実であるといえる。」

強盗殺人の成否に関して、被告人による被害者の殺害行為が、被害者に対する債務の支払いを免れる目的でなされたかどうかについて、「〔パーソナルコンピュータの解析結果について〕と題する書面（甲113）等の関係証拠からすれば、被害者が、被告人に対し、平成22年11月17日ころ、株式投資資金の名目で現金800万円を交付した事実が認められる。また、被害者とFの間でなされた携帯電話のメール内容（甲119）等からも、被

害者が、被告人に対し、複数回にわたり、金銭の支払いを求めていたことが認められる」とする。

また、被告人が被害者の死体を遺棄した犯人であるかどうか等について、「被告人が、被害者を殺害した犯人である事実が推定されること、平成 23 年 2 月 7 日午前 2 時 16 分ころ以降の時点で、自宅パソコンを用いて、「白骨化」「海岸 白骨」などを含む語句をインターネットで検索していることなどからすれば、特段の事情がない限り、被告人が、被害者の殺害後間もない時間帯に、被害者の死体を遺棄現場に遺棄した犯人であることを認めることができる。」と認定し、被告人が強盗殺人、死体遺棄の犯人であると述べている。<sup>(22)</sup>

ウ 奈良地判平成 25 年 3 月 5 日（平成 23 年(わ)第 283 号、平成 23 年(わ)第 255 号、平成 23 年(わ)第 290 号・住居侵入、強盗殺人、死体損壊、死体遺棄、占有離脱物横領、窃盗、窃盗未遂被告事件<sup>(23)</sup>）

### 【事案の概要】

交際相手の母親である被害者に対して行なった住居侵入、強盗殺人、死体損壊・遺棄、占有離脱物横領、窃盗、同未遂の事案で、被告人は、①住居侵入、②強盗殺人、③窃盗・同未遂の成立を否認した。裁判所は、被告人の供述や死体を異常なほど徹底的に損壊した上で処分したり埋めたりするなどの間接事実等から、被告人が被害者を故意行為により死亡させた犯人でないとすれば合理的に説明することが著しく困難であるとして、強盗殺人などを認めた上で、当初から強盗や殺人を計画していたとまでは認めがたいとした。

### 【判決】

裁判所は、インターネット閲覧履歴について被告人が否定しているのを斥けた、「被告人は、公判廷において、前記検索については覚えていない旨供述するが、6 月 25 日から 7 月 7 日までの期間、何者かが被告人のノートパソコンを使用して、これらの検索の一部でも行い得る状況にあったとは考えられず、被告人が自ら前記検索を行ったものと認められる。」「被害者に自殺を窺わせる理由や兆候はなく、事故死、第三者による他殺

の可能性が完全に否定される。一方、生前の被害者と最後に接触したのも被害者の死体に最初に接触したのも被告人である。その被告人が、被害者の死体に対し徹底的な損壊・遺棄行為をした理由は、被告人が被害者を故意行為により死亡させた犯人でないとすれば合理的に説明することが著しく困難である。(その他の事情を併せれば)被告人が被害者を殺害した犯人であると合理的に推認することができ、後述するように、本件立入りが金品窃取目的であったと認められることも併せ考えれば、被告人が被害者を殺害したものと優に認められる。」と、犯人性を肯定した。

これらの判決では、いずれもインターネット閲覧履歴等について、被告人が犯人であることを推認する間接事実として、積極的に評価している。

岐阜地判平成 23 年 1 月 28 日では、弁護人の被告人には放火をする動機がないとの主張について、「被告人が使用していたパソコンのインターネット閲覧履歴等からは、4 月 23 日に至るまでに、被告人が甲状腺の病気や更年期障害、うつ病等について関心を有していたことが認められるし、被告人の携帯電話から送信されたメールの内容などからすると、被告人と夫との夫婦関係は、必ずしも良好ではなかったことが認められる」として被告人の健康状態に関する悩み及び家族関係に関する悩みは、自殺を企てる動機として十分ありうるものであると考えられると弁護人の主張を斥けている。

また、金沢地判平成 24 年 3 月 2 日では、被告人が被害者の死体を遺棄した犯人であるかどうか等について、犯行後間もない平成 23 年 2 月 7 日午前 2 時 16 分ころ以降の時点で、自宅パソコンを用いて、「白骨化」「海岸 白骨」などを含む語句をインターネットで検索していることなどからすれば、特段の事情がない限り、被告人が、被害者の殺害後間もない時間帯に、被害者の死体を遺棄現場に遺棄した犯人であることを認めることができるとしている。また、奈良地判平成 25 年 3 月 5 日でも、被告人が犯行後に閲覧したインターネット検索履歴について、被告人が覚えていないと供述したのについて、何者かが被告人のノートパソコンを使用して、こ



これらの検索の一部でも行い得る状況にあったとは考えられず、被告人が自ら前記検索を行ったものと認められるとして被告人の犯人性を肯定する間接事実のひとつとしている。これらについては、他の間接事実との総合的評価としてはありえなくもないが、犯行間がない時点での、インターネット閲覧が、被告人の犯人性についての関連性を推認する事情として十分とまではいえないと考えられる。

なお、奈良地判平成 25 年 3 月 5 日では、メールの解析結果について、「検察官は、被告人が C や G、被害者の友人らに被害者の生存を装うメールを送信したことも、死体損壊・遺棄や国外への脱出を図るための時間を稼ぐためであり、仮に本件が発覚した場合も自分の関与が疑われないように偽装工作するものであるとして、被告人が被害者を殺害した犯人でなければ合理的に説明できない行為だと主張する。この点、被告人の当該メールが被害者の生存を装い、被害者死亡の発覚を遅らせるための時間稼ぎであるとの点は当裁判所も疑わない。しかし、このメール送信のみをみると、被告人が、被害者が死亡したことから、被害者の財産〔車やカード等〕をより長い時間使用するためにそのようなメールを送信した可能性も考えられるから、メール等の偽装工作の事実のみをみると、被告人が被害者殺害犯人でないとしても一応説明することができる。」と検察官の主張に慎重な判断をしている。

#### 註

- (17) 本件では、間接事実を総合しても被告人が犯人とするには未だ合理的な疑いが残っているというべきであると無罪にした。
- (18) 最判平成 22 年 4 月 27 日刑集 64 卷 3 号 233 頁は、刑事裁判における有罪の認定に当たっては、合理的な疑いを差し挟む余地のない程度の立証が必要であるところ、情況証拠によって事実認定をすべき場合であっても、直接証拠によって事実認定をする場合と比べて立証の程度に差があるわけではないが（最高裁平成 19 年（あ）第 398 号同年 10 月 16 日第一小法廷決定・刑集 61 卷 7 号 677 頁参照）、直接証拠がないのであるから、情況証拠によって認められる間接事実中に、被告人が犯人でないとしたならば合理的に説明することができない（あるいは、少なくとも説明が極めて困難である）事実関係

が含まれていることを要するものというべきであるとして、原判決及び第一審判決を破棄し、一審裁判所に差し戻している。

また、鹿児島地判平成 22 年 12 月 10 日（LLI/DB 判例秘書登載 L06550725）では、被告人が公判廷で『被害者方に行ったことは一度もない』と述べているが、被害者方から指掌紋と DNA が発見され、これらは偽装工作により付着したものではないのであるから、この点に関する被告人の供述が嘘であることは明らかである。また、被告人は、平成 21 年 6 月 15 日朝から 17 日夜までの 3 日間入浴も着替えもしていないと述べたり、古い靴を捨てた時期について捜査段階と供述内容を変えるなど、供述内容に不自然な点がある上、逮捕前に携帯電話の発着信履歴等のデータをすべて消去するという不可解な行動に出ている。しかし、嘘をついた理由が、本件犯行と関係するのかどうかすら説明できていない以上、嘘をついている一事をもって、直ちに被告人を犯人であると認めることはできない。」として、上記最高裁判決と同様に、犯人性が争われた住居侵入、強盗殺人事件において、情況証拠によって認められる間接事実の中に、被告人が犯人でなければ合理的に説明することができない（あるいは、少なくとも説明が極めて困難である）事実関係が含まれていないというほかないから、本件程度の情況証拠をもって被告人を犯人と認定することは、刑事裁判の鉄則である「疑わしきは被告人の利益に」という原則に照らして許されないというべきであって、結局、犯罪の証明がないとして、被告人を無罪としている。

- (19) LLI/DB 判例秘書登載 L06650033（懲役 6 年（求刑、懲役 8 年））
- (20) 判決では、証拠の標目として、明示的にインターネット閲覧履歴に関する解析結果報告書があげられているわけではないが、捜査報告書として証拠採用されているものと推察される。
- (21) LLI/DB 判例秘書登載 L06750102（無期懲役）
- (22) この事案では、証拠の標目として、「携帯電話の解析結果について」と題する書面や「パーソナルコンピュータの解析結果について」と題する書面があげられている。
- (23) LLI/DB 判例秘書登載 L06850138（無期懲役）

## 5 おわりに

デジタル・フォレンジックによる証拠の解析において、重要なことは、適正かつ適切な手順によって解析が行われることであるということ<sup>(24)</sup>はすでに述べたところである。

デジタル・フォレンジックによる証拠の解析の手順は、汎用性のあるソフトウェアを用いて実施することができるものもあるが、特殊なオペレーティングシステムなどではそれに対応するソフトウェアを用いる必要がある。前者の場合には、デジタル・フォレンジックの分野における基礎原理には科学的根拠があり、かつ、その手段、方法が妥当で、定型的に信頼性のあるといえるソフトウェアを用いて実施されるが、後者の場合には、必ずしもそのようにはいえないので、解析のソフトウェアについて理論的な正当性があることが証明される必要があろう。その上で、いずれの場合も、解析能力のある技術者が、信頼される方法で実施し、事後の検証が可能な手順の記録を残しておくことが求められる。そして、他の科学的証拠とは異なり、電磁的記録媒体からハッシュ値が一致する物理コピーされた電磁的記録の解析過程については、デジタル・フォレンジックによる再現が可能であるだけに、これについて証拠開示の対象とされるべきである。

ところで、デジタル・フォレンジックを用いた解析結果から要証事実の認定するにあたっては、保全された電磁的記録媒体には膨大な電磁的記録が記録されているのが通常であり、どのような電磁的記録を用いて要証事実を認定するかは慎重な検討を要する。インターネット閲覧履歴についていえば、被告人が犯罪に関連するサイトを閲覧していたからといって、それが直ちに被告人の犯行を推認することにはならない。デジタル・フォレンジックによる解析結果は、さまざまな事項の立証対象となりうるだけに、最良証拠として用いるにあたって、要証事実をふまえた十分な吟味が必要である。<sup>(25)</sup>

## 註

- (24) デジタル・フォレンジックに関しては、国際標準化も進められており、2012年にISO/IEC27037「デジタル証拠の特定、収集、取得及び保全に関する指針（Guidelines for identification, collection, acquisition and preservation of digital evidence）」が制定され、また、ISO/IEC27041「調査手法の適合性及び妥当性を保証するためのガイダンス（Guidance on assuring suitability and adequacy of incident investigation methods）」やISO/IEC17042「デジタル

証拠の解析及び解釈に関するガイドライン (Guidelines for the analysis and interpretation of digital evidence)」、ISO/IEC27043「インシデント調査の原則及びプロセス (Incident investigation Principles and Processes)」、ISO/IEC2705-1「電磁情報開示」(Electronic discovery)」等が、審議されている。

- (25) デジタル・フォレンジックを用いた解析結果としての証拠評価は、厳密に検討する必要がある。すなわち、捜査機関から証拠開示された解析結果が証拠として用いることができ、証拠として信頼性があり、要証事実を立証できるかということを法的な観点から慎重に吟味する必要がある。