RN-004

刑事訴訟におけるデジタル・フォレンジックツールの課題 ～アメリカの判例と動向を手がかりに～

Issues of Digital Forensic Tools in the Criminal Procedure - Based on Cases and Directions in the United States-

前田恭幸† 湯淺墾道‡
Yasuyuki Maeda Harumichi Yuasa

1. はじめに

近年、サイバー犯罪の件数が増加すると共に、技術的な手法も複雑化・高度化している。またコンピュータやスマートフォン、タブレット等の各種の電子機器が普及し、各種の犯罪に広く使用されるようになってきていることから、これらの機器から電磁的記録を抽出し、人が認識できるように文字や画像等に変換して犯罪捜査・刑事訴訟の証拠とするデジタル・フォレンジックの重要性が高まっている。しかし、デジタル・フォレンジックは、デジタル証拠にアクセスするのが難しいデバイスがあること[1]、スマートフォンのアプリ解析が困難であること[2]、膨大なデジタル証拠を処理する人員がおらず大量の未処理案件が生じておりトリアージが必要なこと[3]など、様々な課題を抱えるようになっている。このため、デジタル・フォレンジックにあたっては、さまざまなデジタル・フォレンジックツール（以下、「ツール」[4]という。）を使用することによって課題に対処することが多い。また、専門知識のない調査・解析者でも使用することができるように解析作業を自動化したツールも多く、解析現場におけるツールへの依存が高まっている[5]。

一方、国家公安委員会は、情報技術の解析の重要性が高まっていることから、平成 27 年 3 月に情報技術の解析に関する規則（平成 27 年国家公安委員会規則第 7 号）を制定した。同規則第 2 条は、「予断を排除し、先入観に影響されることがないようにし、微細な点に至るまで看過することのないように努めるとともに、情報技術の解析の対象が、公判審理において証明力を保持し得るように処置しておかなければならない。」と規定する。これは情報技術の解析の対象が、取扱いの過程における不適切な措置等によって公判審理において証明力を失うことのないように処置をしておくことを求めるものである[6]。このため、ツールを使用する際には、ツールによる解析結果も、公判審理において証明力を否定されることのないようにしなければならないが、日本では解析結果自体が争点になる判例がきわめて少ないのが現状であり、公判審理において証明力を失うことのないような処置として、具体的にはツールをどのように使用しなければならないのか、判例を通じて検討することが困難である。

これに対してアメリカにおいては、デジタル・フォレンジックのみならず、日本及び世界中で使用されているツールである EnCase を含めて、ツールに関係して多くの判例がある。このため本稿では、公判審理における証明力の確保という観点から、アメリカにおけるデジタル・フォレンジックツールに関する判例の動向を検討して、日本の将来の課題への示唆について考察した。

その結果、本稿では、日本の刑事訴訟におけるツールの具体的な課題として 3 点を明らかにした。

† 情報セキュリティ大学院大学
‡ 情報セキュリティ大学院大学

2. 刑事訴訟におけるデジタル・フォレンジック

2.1 電磁的記録の解析に関する現状

従来の、コンピュータのハードディスク等から物理コピーを行って当該コピーに対して解析を行うことで証拠の論理的同一性が証明されてきた手法は、レガシーフォレンジックとも呼ばれる。これに対して現在のデジタル・フォレンジックは第 2 世代デジタル・フォレンジックとも呼ばれ、レガシーフォレンジックと比較すると、証拠物が多様化していることなどの相違があり[7]。それに伴って、解析にあたりツールを使用することが必須となっている。

日本における電磁的記録の解析の現状とツールの利用状況について、国家公安委員会の統計データ[8]により説明する。それによれば、「スマフォに記録された内容の確認については、警察庁開発ツールの活用ができる場合等は都道府県警察で対応可能であり、情報技術解析部門は困難なものに注力」とある。ここでいう「困難なもの」とは、①スマホアプリのバージョンが上がるとツールのバージョンもそれに対応する必要があるアプリフォレンジックと、②不正プログラムの解析、の 2 点のことである。

同データによれば、解析件数及び解析する容量は近年急速に増加しているが、都道府県警から警察庁への解析依頼件数は増えていない。これは、ツールを用いて解析することによって都道府県警が対応することが可能となってきているためである。警察庁の情報技術解析部門の技術者は、都道府県警でツールによって解析することが困難な場合に注力して解析を行うとしており、日本でもツールへの依存が高まっていることを示している。

2.2 日本の判例

日本の刑事訴訟においては、デジタル・フォレンジックで使用したツールのエラー等について争われた判例や、ツール自体について争われた判例は、判例集や判例データベース等を参照するかぎりでは、まだ存在しないと思われる。

しかし、解析の結果について争われた事例などは存在している。たとえば、情況証拠による被告人と犯人との同一性の認定にインターネット検索履歴を用いる判例[9]や、写真データの EXIF にある位置情報についての改ざん（真正性）を争った判例[10]などがある。また、いわゆる村木さん裁判（厚労省事件）[11]においては、検察官によるデジタル証拠

の日付の改ざんがあった。さらに、解析結果が重要となった遠隔操作事件[12]があり、EnCase と X-ways というツールの名称等も鑑定人等により証言されている[13]。デジタル証拠は、改ざん・改変が容易なため、今後もこういった真正性が争われるケースが出てくるだろう。

2.3 日本とアメリカの刑事訴訟の類似点と違い

ツールに関するアメリカの判例を参照する上で、日米の刑事訴訟の類似点と違いを明らかにしておく必要がある。

青木は、日本の法体系及び法律実務は、憲法から個々の制度・運用に至るまでアメリカの多大な影響を受けており、刑事訴訟の分野に限ってみても連邦最高裁判所などが理論をリードしているという[14]。しかし、アメリカにおける議論をそのまま援用する上では、考慮しなければならない点もある。高橋は、日本とアメリカのデジタル・フォレンジックにおける法的な違いに関して、英米法の証拠法の考え方と日本の考え方の違い、民事と刑事における証拠法の現れ方の違い、アメリカにおける特徴的な制度の影響、証拠開示等についての考え方の違い、という 4 点を挙げている[15]。特に、証拠能力の観点が異なる。証拠となる資格を、日本では証拠能力といい、アメリカでは許容性という。アメリカでは、公判の前に裁判官のみで許容性の判断を行い、許容された証拠のみが公判で用いられる。それに対し日本では、公判で鑑定人等の証人尋問を行い、最終的に事実認定の資料に用いてよいかどうかの観点から議論が行われる。つまり、日本では、公判で事実認定者に示してよいかどうかの議論ではなく、審理後に最終的に有罪判断の基礎となる資料としてよいかどうかの議論である。

証拠能力については、自然的関連性、法律的関連性、証拠禁止（証拠排除）の観点から判断される[16]。証拠能力が認められた証拠は、証明の価値を示す証明力が重要となる。

また、日本と大きく異なる制度として、アメリカではディスカバリと陪審が多用されている。日本の訴訟における証拠は原告・被告双方が独自に集めるのに対し、アメリカではお互いに自分の情報を相手方に開示しなければならず、原告・被告ともに、その相手方から提供を受けた情報の中から証拠を見つけ出すことが許されている、という点で大きく異なる[17]。

3. デジタル・フォレンジックツールの現状と課題

3.1 ツールの歴史と分類

デジタル・フォレンジックツールの歴史は、1980 年代に遡る。当時のツールは、アメリカの IRS（Internal Revenue Service）やオタワの RCMP（Royal Canadian Mounted Police）などの政府組織によって C 言語またはアセンブリ言語で開発され、一般人が利用することはなかった[18]。その後、司法機関のみで使用していたツールが民間にも広がり、米国 Guidance Software 社が開発・販売している EnCase などの市販ツールが多く普及していった。EnCase は、アメリカの FBI・CIA といった司法機関や民間企業など、世界中の多くの組織で利用されており、最も完全なフォレンジックセットの一つであるともされている[19]。この他にも多くのツール類が販売されている一方、オープンソースやフリーウェアのツール類も利用されるようになってきている。そこで、ツールの開発者や流通経路を基準として、ツールを 3 種類に分類した。製品例は、判例、レポート、海外カンファレンスや研修で出てくるものを例とした。

表 1　ツールの分類

ツールの分類	概要	製品例
フリーツール	オープンソース クローズドソース	Autopsy、FTK Imager、Volatility
市販ツール	有償・一部無償 購入・使用条件 資格・ライセンス	EnCase、X-ways、FTK、CPS
自作ツール	民間企業独自開発 司法機関独自開発	警察庁ツール、IRS ツール

ツールの例に関しては、上記の他、デジタル・フォレンジック研究会において「証拠保全ガイドライン　第 5 版」[20]を公開しており、16 種類の代表的な収集及び分析ツールについて説明している。このようにツール自体についても多くの種類があるが、本論では、市販ツールに関する判例を中心に取り上げ、考察を加えた。

3.2 ツールの使用目的・方法・時期

ツールの使用の目的について、羽室らは、データのトリアージ、マルウェア対策、暗号・パスワード解析、データの可視化、ログ解析などのためにツールを準備しておくことが求められるとしている[21]。

ツールの使用方法について、安冨は、解析能力のある技術者が信頼される方法で実施し、事後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としている[22]。また、特殊な解析が必要な場合のツールについては、理論的な正当性があることが求められるともしている。そこで問題となるのが、解析能力のない調査・解析者等がツールを用いて析出された証拠の証拠能力と証明力である。DNA 型鑑定等の科学的証拠についても専門性が必要であることが判例上示されており[23]、ツールを用いた証拠について調査した。

ツールを使用する時期は、証拠収集（ネットワーク捜査など）、保全作業、解析の 3 つに分けることができる。

証拠収集とは、P2P ファイル共有システム内の児童ポルノなどに関して犯罪捜査機関などが行っている捜査の一環であり、ネットワーク等を介して証拠の収集を行うものである。保全作業、解析において必要とされる要件については、吉峯らが図 1 のように整理している[24]。

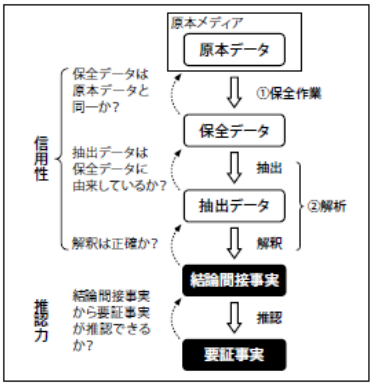

図 1　デジタルデータの信用性と事実推認力[25]

また、高橋らは、デジタルデータを証拠とする上での、データそのものの性質に由来する問題は、原本性、完全性・真正性の立証、見読性（可視性）に分けられるとしている[26]。原本性については、デジタルデータとプリントアウトの同一性や、HDD 複製時の論理的同一性がある。ここでの HDD 複製時の論理的同一性とは、デジタルデータの 0 と 1 の並びが最初から最後まで完全に一致することをいう。

安冨によると、電磁的記録と出力された文書との同一性については、可読的なハードコピーが証拠調べの対象たるデータを正確にプリントアウトしたものであることをどのようにして担保させるかという問題であるという。これについては、電磁的記録を一定のプログラムにしたがって出力した者がその成立の真正を公判廷で証言すれば足りると解する、とされている[27]。ここで、ハードディスクの物理コピーによる論理的同一性はないこと[28]と、専門性がない解析者等がツールによって析出された証拠を公判で証言することに疑問があることを指摘したい。しかし、日本ではツールが争点になった判例等は管見の限りないため、アメリカの判例と動向を調査した。

3.3 アメリカにおけるツールの課題

デジタル・フォレンジックの先進国であるアメリカでも、ツールに関する課題は少なくない。司法省、国立司法省研究所(NIJ：National Institute of Justice)、シンクタンクのランド社(Rand Corporation)、デンバー大学等からなる共同プロジェクトのレポートは、次の表のような課題と解消策を示している。レポートは主な課題として 30 項目を示しており、うち 15 項目はツールに関連するものであった。

表 2　デジタル・フォレンジックにおける検察側の課題[29]

問題または機会	関連付けられる要請
捜査機関には、どのようなツールを使うにしても、膨大なデジタル証拠を処理する十分な人員がおらず、大量の未処理案件がある。	事案と抽出するデータに関して、適切な優先判定、トリアージを行う方法またはツールを開発する（解析者と、現場で捜査官が使えるツール類の両方）。
車載システム（取り外せないデバイス）のデジタル証拠にアクセスすることが難しい。	物証保管の継続性を満たしつつ、分解または破壊することなく証拠にアクセスできるツールの開発。
分析するためのツールを警察が持っていない電子システムやデバイスがある。	ゲーム機、ネットワーク、ルーターなどを解析するためのデジタル証拠ツールを開発する。
刑事司法のために用いられる新しいデータ収集技術や解析技術の精度と受容性が不透明である。	確立された基準に基づき、時宜を得た技術評価、ならびに各製品及び技術ごとの分析を実施する。
裁判所の中には、情報の有効性及び物証保管の継続性と不確実性を理由として、デジタル証拠に対して懐疑的となっているところがある。	ドーバード基準を満たしていることを確認するため、デジタル証拠ツールの性能を組織的に認証するための取り組みが必要。

なお、法執行機関のニーズに基づきツールの評価試験方法を確立するため、アメリカ商務省の標準技術研究所（NIST： National Institute of Standards and Technology ）が中立的な立場で実施しているプロジェクトとして、CFTT[30]がある。他にも、SWGDE（Scientific Working Group on Digital Evidence）や NIJ から、デジタル証拠やツール利用についての様々なレポートが公開されている。ツールに関連するプロジェクトや文献を調査するだけでも、日本よりも多くの議論があることがわかる。

4. アメリカの判例の検討

4.1 ツールを使用すること自体の是非に関する判例

アメリカにおいて、2010 年前後は、児童ポルノに関係する犯罪の立件にあたり証拠としてハッシュ値が用いられることが増えた時期であった。児童ポルノと判断される画像や動画像ファイルを収集してデータベース化し、ツール類を用いて P2P ネットワークで共有されているファイル類のハッシュ値（だけ）と被疑者のコンピュータの IP アドレスを取得して、データベースの画像や動画像ファイルのハッシュ値を比較することにより、被疑者が児童ポルノを提供・所持しているかどうかを判断するという手法である。

当初はこの作業に必要なクエリー送信等を捜査官の手作業で行っていたが、各種のツール類を利用して自動化するようになった。初期の判例では、このようなツール類を使用して証拠を抽出すること自体の適法性が争われている。

フォレンジック・ツール類の多くは、民間の企業によって開発・販売されるものであっても、警察や政府関係者だけに利用が許可されている場合がある。このため合衆国対ボロウィ事件において、弁護側は、警察のみが利用できるツールを利用すること自体が、不合理な捜索・押収を受けない権利（連邦憲法修正第 4 条）に違反すると主張した。これに対して、連邦地方裁判所は P2P ネットワークで共有されているファイル類にはプライバシーの保護は及ばないとしてそれを退け[31]、控訴裁判所の判決でも原審の判断が支持された[32]。これによって、刑事事件の捜査においてツール類を使用すること自体には違法性はないということも判例上確立した。

4.2 令状記載に関する判例

次に捜索令状の記載に関する判例である。合衆国対ガベル事件[33]では、警察が捜索令状請求書に警察関係者だけが利用できるツールについて記載しなかったのは違法であり、捜索令状は無効であるとして、被告人が証拠排除の申立を行った。しかし、連邦地方裁判所の判決では、警察関係者だけが利用できるツールを使用することを捜索令状請求書に記載する義務はないとして、申立は退けられている。その後の判例でも、本件を引用するものが多い[34]。

4.3 ディスカバリに関する判例

連邦刑事訴訟規則第 16 条は、被告人に対して、ディスカバリの権利を認めている。他方で、捜査や今後の捜査の支障となる場合には、検察側にはディスカバリに応じない免責が認められる。ディスカバリは、警察・検察側とは異なり起訴の前にツールを使ってデータを解析することができない弁護側にとっては、非常に有効な防御手段となる。

このため、被告人がディスカバリの権利を行使し、捜査に用いたツール類についての情報を明らかにするように求める場合が多い。

その際、ツール類が連邦刑事訴訟規則に定める「書籍、紙、書類、データ、写真、有形物、建築物、場所またはこれらのコピーもしくは部分」[35]に該当するかどうかが問題となる。またディスカバリの権利は、「弁護のために利用されるもの」であるから、当該の情報が弁護のために欠かせないものであるかどうかも争点となっている。さらに、ディスカバリの際、警察側が使用したツール自体のコピーについてもディスカバリの対象となるかどうかが争点となり、裁判所によって退けられた事例[36]もある。

合衆国対バドジアック事件[37]では、控訴審の判決において、被告人の主張の一部が認められ、捜査に使用したツールの情報に関するディスカバリの申立の一部が認容された。事実審の判決では、検察側のプロプライエタリ[38]の利益等の主張を認め、被告人の申し立てを棄却した。しかし、控訴裁判所[39]では、被告人側がツール類による解析結果にエラーが生じている可能性を証明できる場合には政府側が利用したプログラムにアクセスする機会を認めるべきであるとし、ディスカバリについては地裁判決を差し戻すとした。連邦最高裁は、本論に関し、被告人側の裁量上訴の訴えを特に理由は付さずに棄却する判決を下し[40]、控訴裁判所の判断が確定した。

また合衆国対チラディオ事件[41]においては、被告人側がツール類による解析結果にエラーが生じている可能性を証明できない場合は、政府側が利用したプログラムにアクセスする機会を認める必要はないとされた。

合衆国対ピロスコ事件においても、連邦控訴裁判所は検察側にディスカバリの義務の免責(privilege)を認めた。その際、捜査に用いた機器類の場所の秘匿を認めた先例[42]も引用しつつ、被告人側が、ツール類による解析結果にエラーが生じている可能性を証明できる場合には政府側が利用したプログラムにアクセスする機会を認め、挙証できない場合にはアクセスする機会を認める必要はないとしている[43]。ツール類による解析結果のエラーの可能性を被告人側が立証できる場合のみ、被告人側にツールに対するアクセスする機会を認めるという判断の枠組みは、前出の合衆国対バドジアック事件の控訴審判決[44]が採用されたものである。本件では被告人側がそれを引用しているが、合衆国対ピロスコ判決もバドジアック事件の控訴審判決の枠組み自体を否定しているわけではない。判決では、被告人は警察がツール類を利用して解析を行った際に設定を上書きしてしまった可能性があるという証拠を提出していないので、ツール類による解析結果のエラーの可能性を立証できていないという理由から、被告人の主張を退けている。したがって、被告人が本件で使用されたツール類の誤解析の可能性を挙証できれば、ツール類にアクセスする機会を認められていた可能性がある。

実際に合衆国対タミンズ事件[45]では、被告人側が、捜査に使用したツール類の詳細な情報だけではなくツールなどに関してのディスカバリの申し立てを行った結果、申立の一部は認められ、一部は退けられた。HDD コピーの提出の申立に関して、検察側は、HDD のフォレンジック・コピーの提供は法廷に証拠として提出された児童ポルノの取扱いについて規定する連邦法[46]によって禁じられていると主張した。しかし裁判所は、EnCase のようなツールは解析に誤りを生じることがあるため、HDD のコピーに関して被告人側のフォレンジック専門家及び弁護人のみにアクセス及び検証することを許容した。

被告人側からのディスカバリの申立が退けられた合衆国対ピロスコ事件・合衆国対チラディオ事件等と、一部が認められた合衆国対タミンズ事件について検討してみる。

バドジアック事件の控訴審判決の枠組みの下では、被告人側は、ツール類による解析結果の誤りの可能性を客観的に示すことが必要である。しかし、有名なツール類であって誤解析が発生することが関係者の間で広く知られているか、NIST 等の公的機関による検証で解析に誤りが発生する可能性があることが確認されていないかぎり、弁護士がツール類の誤解析の可能性を挙証することは難しい。合衆国対タミンズ事件は、EnCase という世界中で使用され、解析のエラーが存在することについても広く知られたツールであったために、結果的にディスカバリの申立の一部が認められるに至ったといえる。

その意味で、弁護側から見たツールに関する課題は、検察側と弁護側の不均衡という点にある[47]。事実審裁判において、デジタル・フォレンジックを行うのは主として警察・検察側であり、弁護側が警察・検察側に対抗するために独自にフォレンジックを行うことができない。その場合、ディスカバリを最大限に利用することが弁護側の防御手段である。しかし、市販ツール類は通常は警察や政府関係者だけに利用が許可されているから（プロプライエタリ性）、弁護側にとっては、これらのツール類による解析の誤りを主張することは非常に難しいといえる。

これらの判例から、ディスカバリに関するツールの問題点として、HDD 自体を含めたデータの開示とツールの開示の 2 つがあることがわかる。

4.4 自動化ツールの許容性に関する判例

近年は、ボタンを押す（マウスでクリックする）だけで証拠の収集、保全、解析などが可能なツールが増加している。このため、そういったツールの自動化の許容性に関する判例が存在する。

合衆国対トーマス事件[48]は、被告人が、捜査員の使用した CPS という自動化ツールについて違法収集証拠排除の申立を行ったものの、棄却された判例である。被告人は、捜索令状発給請求書に(1)自動化されたソフトウェアと第三者のデータベースを利用することを適切に記載していなかった、(2)自動化されたソフトウェアは共有に供されないファイルも含めて、対象のファイル類に不完全にアクセスしたり消去・破損したりする可能性があると指摘されていたのに、それを明らかにしていなかった、(3)自動化されたソフトウェアのテストが不十分であることを明らかにしていなかった、等の理由で、違法収集証拠排除の申立を行った。

これに対して検察側は、自動化されたソフトウェアは、共有に供されない私的領域のファイル類にはアクセスできず、実際にアクセスしなかったので、令状無しの捜索は発生していないと主張した。また自動化されたソフトウェアについては適切に捜索令状発給請求書に記載しており、事実を意図的に隠蔽したり省略したりしたことはないとも主張した。

連邦地裁判決は、「警察が明らかにする義務を負うのは、児童ポルノであることを示すファイルを捜査する際のプロセスが、一般に公開されている情報の中から探査するソフ

トウェアを使うことで自動化されているという点であり、それ以上の詳細な情報は、逮捕相当理由を構成するためには要求されない」、「逮捕相当理由の認定にあたっては、捜査ツールのエラー率等の一定のレベルが要求されるわけではない」と判示した。

連邦地方裁判所判決を不服とした被告人は、第 2 巡回区連邦控訴裁判所に控訴した。しかし、控訴裁判所は地裁の判決を認容し、被告人の控訴を却下した[49]。控訴裁判所判決は、「ソフトウェアが第三者によって開発されたものであるという点に関して、当該ソフトウェアは、公知の事実を集める機能を有するに過ぎないから、蓋然性事由の認定にあたって何の影響も与えない。ソフトウェア開発者が公的機関ではない場合はそれを明らかにしなければならないと被告人は主張するが、それを裏づける判例や規則等は存在しない」、「被告人は、犯罪の証拠を得るために使用されたソフトウェアの商品名を明らかにしなければならないと主張するが、そのような判例や規則等も存在しない。連邦最高裁は、匿名市民の情報提供者による情報に基づく令状請求を認めており[50]、ソフトウェアの詳細や第三者のソフトウェアベンダーの名前までを明らかにすることを政府に要求することは、最高裁判決の趣旨に沿わない。」と判示した。また自動化機能について「CPS は、公知の情報を集積する作業を自動化するものであり、この作業は速度とペースの点で劣るとしても捜査官によって手動で実行しうる。」として、これを認容した。

州裁判所におけるツール類の利用に関する判例として、ウィルホード対テキサス州事件[51]は、EnCase が対象になった初期の事案である。新たな証拠として、EnCase によって作成された証拠の許容性に関して、新規の科学的証拠に対する DNA 型の証拠の判例[52]を参照し、EnCase の自動化機能を使用した結果の証拠への許容性を認めた。

またフロリダ州の裁判所において CPS を利用した証拠を排除すべきかどうかが争点となった際、上記の合衆国対トーマス事件を引用して CPS は捜査の過程を自動化するものにすぎないから CPS を利用した捜査は適法であるとする判決が 2015 年に下されている[53]。

4.5 陪審においてツール及びツールを使用した解析結果が争点となった判例

4.1 から 4.4 までは許容性に関する判例であるが、4.5 は証明力に関する判例である。

陪審裁判において、ツール及びツールを使用した解析結果への信頼性が問われる事件として、全米の注目を集めたケイシー事件（ケイシー対フロリダ州事件）[54]がある。この裁判をめぐっては多くのテレビ番組が製作・放映されたほか、事件を担当した検察官が回顧録を出版してベストセラーとなったものまである[55]。また科学的証拠に対する陪審員の理解・判断能力、過熱するマスメディアの報道による陪審評決への影響[56]、ソーシャル・メディア上での「炎上」に近い議論の過熱、陪審員選任の偏り、陪審員の身元のインターネット上での公開[57]や世論とは異なる評決をした陪審員への嫌がらせ等[58]、多くの問題を生み、『タイム』誌では「世紀のソーシャル・メディア裁判」とまで評された[59]。

被告人ケイシーは 22 歳の若い母親で、19 歳のときに出産した娘のケイリーと共に、被告人の両親宅に同居していた。2008 年 6 月中旬、被告人ケイシーの母のシンディ(Cindy)・アンソニーは、被告人の母親としての適格性に疑問を持つようになった。被告人と被告人の両親との喧嘩の後、被告人は娘のケイリーを連れて家を飛び出した。その後数週間にわたって、被告人は男友達の家に泊まり、パーティー等に出歩いていた。この間、シンディはケイシーに電話をしてケイリーの様子を尋ねたが、そのたびにケイシーは、ケイリーはベビーシッターであるザニーと一緒にいると答えた。7 月 15 日、シンディはオレンジ郡保安官事務所に、ケイリーが行方不明であることを届け出た。警察の事情聴取に対して虚偽の陳述をした。ケイシーは、殺人の疑いで 7 月 16 日に逮捕された。2008 年 12 月 11 日、プラスチックのバッグに入った遺体が発見され、遺体はテープで鼻と口をふさがれており、ケイリーと確認された。2011 年 6 月、ケイシーは第 1 級殺人、児童虐待、激昂した上での児童故殺、警察官への虚偽陳述（合計 4 件）の計 7 件について起訴され、陪審裁判に付されることになった。

この事件においてデジタル・フォレンジックが注目されたのは、きわめて物証の少ない事件で、検察側にとって第 1 級殺人の要件となる母親の計画的殺人の立証が難しかったことが関係している。主な証拠は、ケイシーが乗っていた乗用車のトランクのカーペットからクロロフォルムが検出されたこと、トランクから発見された髪の毛はケイリーのものと一致すること、トランクから発見された髪の毛は腐乱した死体のものである可能性が高いこと、トランクには腐乱臭が充満していたこと、被害者の鼻と口はテープでふさがれていたこと等であった。しかし、被害者の死因を直接明らかにするような証拠はなく、被告人ケイシーの犯行と断定するには状況証拠にとどまった。

このため、検察側は、母親が娘の口をテープでふさぐ前にクロロフォルムを使用したと主張した。警察がケイシー宅のコンピュータを押収し、押収したコンピュータをツールを用いて解析した結果、「クロロフォルム(chloroform)」というキーワードで 84 回サーチエンジンを検索していたという証拠が得られたとした。これが法廷に提出され、母親がクロロフォルムを使用して娘の意識を失わせるということをあらかじめ計画し、娘を謀殺しようとしていた（第 1 級殺人罪成立の要件となる計画的殺人を行った）証拠とされたのである。このデジタル・フォレンジックの結果に対して、次のような検察側と被告人側の主張がある。

検察側：「NetAnalysis v1.37」というイギリス製のツールを使用した結果、「クロロフォルム(chloroform)」というキーワードで 84 回サーチエンジンを検索していたという証拠が得られた。

弁護側（SiQuest 社の証人[60]）：実は NetAnalysis で検索履歴データベースから検索履歴を復元することはできた記録の数は 320 以下であり、クロロフォルムというキーワードによって Google を使って検索した履歴についても、証拠が得られたのは 1 回だけである。

検察側：当初は履歴を復元できなった、SiQuest 社の「CacheBack」というツールを改良してもらい、その後、8557 記録を復元でき、この記録の中から 84 回という証拠が得られた。

弁護側：最初に NetAnalysis を使用して 84 回の履歴が復元できたかのように検察側が主張したのは、意図的な誘導である。別のツールを使用した解析結果の相違についても、デジタル・フォレンジックが適切でないことを示すものである。

結果、陪審員はツールによって得られた証拠に対して懐疑的になり、ツールの罪状についての心証を形成できなかったと思われる。実際に検察官の回想録では、最初の解析の際には 84 回という検索履歴が得られなかったのは事実としている[61]。また、事後において、Microsoft OS 標準のブラウザである Internet Explorer（以下、IE）と Fire Fox 双方の検索履歴を出していないため警察が証拠を見落としていた可能性がある点、デジタル・フォレンジックを行った際のデータ保全が不適切であり事後検証ができない点などが報道された[62]。

4.6 アメリカの判例のまとめ

アメリカの判例を、ツールを軸にして検討すると、次の 5 つの点が明らかとなった。

①ツールを使用すること自体の是非に関する判例では、ツールの使用については認められている。②ツールの令状記載に関する判例では、ツール自体の令状記載は必要ないが、捜査の種類によっては、概要を記載する必要があるとされている。③ツールのディスカバリに関する判例では、プロプライエタリとの兼ね合いが問題となっている。また、弁護側がツールによる解析のエラーの可能性を証明できる場合は、弁護側に、デジタル・フォレンジックによって解析したデータにアクセスする機会が与えられる場合がある。④EnCase などの自動化ツールに関しては、手動でも解析可能なことを自動化している場合、デジタル透明性（digital skeleton：この場合、ソースコードが表示されている）が担保されている場合などにおいては、自動化ツールを使用する捜査員の専門性は求められない。⑤陪審裁判においてツールを利用した結果が争点となった判例により、ツール及びツールによる解析結果について陪審員が懐疑的となり、証拠への信頼性が失われることがある。

特に、⑤は、日本でも裁判員裁判が始まっているところ、技術に関する知識を持たない陪審員がツール利用による証拠に懐疑的になり、被告人が有罪であるという心証を形成できなかったデジタル・フォレンジックの失敗例として、日本の裁判員裁判にも示唆を与えるものである。

5. ツールの課題と対応の考察

5.1 インターネット検索履歴に関する課題

前出のケイシー事件では、NetAnanlysis と CacheBack という 2 種類のツールの解析結果が異なったことから、データ復元等の特異な解析についてはより専門性が必要となる解析時の問題と、解析結果が異なった場合の公判での対応、という 2 つの側面の問題があることがわかった。前者は、ツールの性能強化と、鑑定者等の専門性の向上が求められる。後者は、起訴前と起訴後によって DNA 型鑑定等の結果が異なる科学的証拠でも起こりえることであり、異なった科学的証拠が出た場合の検察官側の対応が求められる。さらに、専門性の向上に向けた取り組みの一つとして、ケイシー事件のような 1 つの検索履歴のみの結果を出すのではなく、複数の解析結果を示すべきだろう。ケイシー事件では、捜査員は未使用領域から MORK データベースを復元し、そのデータベースからインターネット検索履歴を復元した。しかし、PC 内の他のブラウザや他の解析項目について触れていないことは、解析項目が不足しているといえる（IE と Fire Fox の両方を解析していないため証拠の見落としがある、と事後に報道されている）。

ケイシー事件を参考としながら、インターネット検索履歴を解析する際の注意事項を考察すると、次が挙げられる。他のブラウザの解析、今回の MORK のデータベース以外にのジャンプリスト・キャッシュ等の解析項目、（OS が Windows Vista 以降の場合）初期から設定されている VSS 機能の使用等、多くの事実を利用すべきである。

5.2 ツールに依存しなければならない課題

バージョンアップの頻度が多いアプリフォレンジック（2.1 参照）、証拠物が多様化していく IoT フォレンジック[63]、解析データの容量増加のためのトリアージ（3.3 参照）などに対して、新たなツールを開発し、それらのツールを適切に使用することが求められる。NIJ のレポート（3.3 参照）からはデジタル・フォレンジックの課題の多くはツールの開発が求められていること、トーマス事件（4.4 参照）からは CPS のような証拠を収集する自動化ツールを使用することが犯罪捜査上有効であることなどが判明した。そして、ケイシー事件（4.5 参照）からは、解析結果の正確なツールが求められていることが判明した。今後のデジタル・フォレンジックには、ツール（特に自動化したもの）に依存しなければならない問題は多いということがいえる。

5.3 ツールだけでは解決が難しい課題

ツールだけでは解決が不可能、または解決が難しい課題も多い。ツールを適切に使用しても、エラーが起こる可能性もあることや、ツールには限界があることである。ツールの限界の例の一つに暗号解読がある。今回の事件には直接関係ないが、WindowsOS のログオンパスワード解析の例では、パスワードが 14 桁以内の LM ハッシュ（DES）であれば暗号解読が可能でありパスワードが判明する。しかし、パスワードが 15 桁以上、または NTLM ハッシュ（MD4）であれば暗号解読は困難であり、パスワード判明も困難となる[64]。こういった暗号や、解析対象物のバージョンアップなどにより、今までツールで解析できていたことが、急に解析できなくなる例も存在する。逆に、昨日まで解析できなかったことが、ツールにより今日は解析できるようになる例もある。このためツールの限界を認識し、最新の情報や知見を得ることが必要となる。

さらに注意が必要な点として、ツールを使用するリスクとして、誤った使用をすることで証拠物である電磁的記録物のデータが消去・改変される例があることである。

デジタル証拠の法的課題に関しては、同一性、真正性、完全性が求められるが、同一性について課題の一例として HDD 以外の対象物がある。例えば SSD には、ユーザーや OS がアクセスできない領域（Over Provisioned Capacity）が製品表示容量の 5～30%存在し、そこにデジタル・フォレンジックに活用できるデータが多く保存されている可能性が高いとされる反面、レガシーフォレンジックの手法では Over Provisioned Capacity を対象としておらず論理的同一性はない場合が多い[65]。また、共著者である湯淺が指摘している海外ツールへの依存[66]、ツールに対する情報公開請求時の対応、押収したツールの使用、リーガルマルウェア[67]の使用の是非、リモートストレージにおける課題などがある。

日本の刑事訴訟においては、専門性がない解析者などが自動化ツールで析出した全ての証拠は許容されるかどうか（特に、法律的関連性と証拠排除の観点）が課題である。前出のウィルホード対テキサス州事件では、EnCase を自動化ツールとして使用したが、そのときの解析者の専門性は問われなかった。日本では、違法収集等により証拠禁止に当たらず、証拠調べ手続において被告人側から不同意の意見がある場合、法律的関連性が課題となる。この点に関しては、証拠調べ手続において証人尋問で鑑定人等が公判期日において証人として尋問を受け、真正に作成されたものであることを供述すれば証拠能力は認められる（刑事訴訟法 321 条 3 項及び 4 項）。つまり、ツールによって析出された証拠に、違法性がなく、データの改ざんがないかなどの真正性が重要となる。さらには、自動化ツールを使用した場合について検討しなければならない。

証明力に関しては、デジタルデータはもともと可視的でなく、ツールもそれ自体は可視的でない中で、公判において特に証人出廷が求められた場合、どのようにそれを可視的に説明するかという課題がある。この公判における課題は、DNA 型鑑定などの科学的証拠でも同様である。鈴木は、科学鑑定の内容を非専門家（法曹三者や裁判員）が理解することが難しく、専門家と非専門家の齟齬があるため科学鑑定を裁判で有効利用できない場合があるとしており、その解決策を示している[68]。その解決策とは、専門家が鑑定能力を持ち公判において的確に表現すること、非専門家への教育、鑑定書を分かりやすいものに変えることとしている。また、吉峯らは、証明力評価の 3 要素として、保全データの同一性、解析過程の信用性、結論間接事実の推認力を挙げている[69]。今後、ツールによる証拠に対して証明力を保持するためには、具体的にどのような要件が考えられるかの検討が必要である。

自動化ツールの普及により現場では解析者等に専門性が求められなくなっていくことと、完全なツールは存在しないため解析者等に専門性が必要であるという矛盾をどのように解消するかも課題である。定型的な解析を行う時以外は専門的な知識と経験が必要になる場合があり、自動化ツールを使用して解析結果などを得た場合、それを公判で説明しなければならない場合があるためである。自動化ツールを用いても、解析者には依然として専門性が必要である。

6. 結論

ツールについてアメリカの判例を手がかりにして考察を加えた結果、日本の将来の刑事訴訟において次の 3 点が課題となることが明らかとなった。それぞれについて課題への対応の方向についても述べてみたい。

①専門性がない解析者などが自動化ツールで作成した全ての証拠は許容されるか。これは主に証拠能力の問題となり、証拠禁止に当たらないこと、証人尋問においてデータの改変がないか等の真正性について証言すること（法律的関連性）によって、証拠能力は認められると解する。問題は、自動化ツールの動作や原理を理解していない鑑定者等の場合であろう。

②デジタルデータやツールがブラックボックスである部分を、証人尋問においてどのように対応すべきか。これは主として証明力の問題であり、解析者が鑑定能力を持ち、保全データの同一性、解析過程の信用性、結論間接事実の推認力という観点から公判において的確に表現することが求められる。また、公判審理における証人尋問の留意点として、専門化が公判で供述する前の時点で具体的な争点を理解しておく必要がある。そのため、冒頭陳述や争いがない前提事実に関する証拠調べを通じて、裁判員が、どこが争いになっており、そこは争いになっていないのかを理解する必要がある。

③自動化により解析者などの専門性がなくなっていくことと、完全なツールは存在しないため解析者に専門性が必要であるという矛盾をどう解消するか。これは証明力の問題であるが、自動化ツールを使用しても調査・解析者の専門性は不要となるわけではなく、解析者の専門性が不足する場合、専門性のある技術者との連携が求められる。これらは組織に求めるものであるが、自動化ツールを使用する専門性がない個人において、ツールの限界とリスクを認識する必要があると考える。

これらの対応によって、公判審理における証明力の保持が可能となると考えられる。

謝辞

本研究は、科学研究費「行政におけるデータの取扱いに関する法的規制の比較研究（研究課題番号：26380153）及び「適応的セキュリティ制御とプライバシー保護支援を可能とするビッグデータ流通基盤」（研究課題番号：15H02696）の研究成果の一部である。

参考文献

[1]Sean E. Goodison, Robert C. Davis, and Brian A. Jackson, Digital Evidence and the U.S. Criminal Justice System: Identifying Technology and Other Needs to More Effectively Acquire and Utilize Digital Evidence, *available at* http://www.rand.org/content/dam/rand/pubs/research_reports/RR800/RR890/RAND_RR890.pdf.

[2]国家公安委員会「国家公安委員会説明資料 No.9　平成 26 年における情報技術解析の実施状況について」https://www.npsc.go.jp/report27/03-26.pdf

[3]Goodison, *supra* note 1, at 23.

[4]アメリカの判例などにおいてデジタル・フォレンジックツールを示す際には、Software、Automated Software、Program などとも表記されている。本稿では、「ツール」とは、それらを含めた広い意味でのデジタル・フォレンジックツールを示す。

[5]Joshua I.James and PavelGladyshev, *Challenges with Automation in Digital Forensic Investigations*, Computers and Society (2013), 17.

[6]宮西健至・島田義孝「『情報技術の解析に関する規則』の制定について」警察学論集 68 巻 4 号（2015 年）89 頁。

[7]Erin Murphy, *The New Forensics: Criminal Justice, False Certainty, and the Second Generation of Scientific Evidence*, 95 CAL. L. REV. 721, 729(2007).

[8]国家公安委員会、前掲注 2。

[9]大阪地判平 22・5・25　判タ 1346 号 247 頁、金沢地判平 24・3・2　（判例集未登載）、奈良地判平 25・3・5（判例集未登載）。

[10]水戸地判平 23・5・20　（判例集未登載）。

[11]大阪地判平 22・5・26　（判例集未登載）。

[12]東京地判平 27・2・4　（判例集未登載）。

[13]遠隔操作事件は、多くの被告人側反対尋問を残したまま、被告人の自白により、（解析結果等による）被告人と犯人の同一性の争いに関しての結末を迎えた。詳細は判例からはわからないため、江川氏のブログを参照。江川紹子【PC 遠隔操作事件】http://bylines.news.yahoo.co.jp/egawashoko/　2016 年 6 月アクセス。

[14]青木孝之「アメリカの刑事手続素描(1)-ミシガン州ウエィン郡の実務を題材に-」駿河台法学第 24 巻第 1･2 合併号（2010 年）283 頁以下。

[15]高橋郁夫「デジタル・フォレンジックスの外延・有用性・留意

点」（2011 年） http://www.comit.jp/BLTJ/civilpro/LS/forensic2.htm 2016 年 3 月アクセス
[16]安冨潔『刑事訴訟法 第 2 版』（2013 年）446 頁
[17]守本正弘『ディスカバリ』（起業家大学出版、2012 年）59 頁。
[18]Bill, Frank, America, Cgris, SITE J1『コンピュータフォレンジック入門 －不正アクセス、情報漏えいに対する調査と分析－』（BNN 新社、2005 年）5 頁。
[19]Michael G.Solomon,KRudolph,EdTittel,NeilBroom,Diane Barrett,『デジタル訴訟の最先端から学ぶコンピュータ・フォレンジック完全辞典』（幻冬舎ルネッサンス、2012 年）312 頁以下。
[20]特定非営利活動法人デジタル・フォレンジック『証拠保全ガイドライン 第 5 版』（2016 年）
[21]羽室英太郎、國浦淳編『デジタル・フォレンジック概論～フォレンジックの基礎と活用ガイド～』（東京法令出版、2015 年）200 頁以下
[22]安冨潔「刑事事件におけるデジタル・フォレンジックと証拠」産大法学 49 巻 1・2 号（2015 年）49 頁以下。
[23]最判平 12・7・17 判タ第 1044 号 79 頁 初めて最高裁で科学的証拠の証拠能力が争われ、証拠能力が認められた判例である。ここで、「DNA 型鑑定は、技術を習得した者により科学的に信頼される方法で実施された場合には証拠として用いることが許される。」とされた。
[24]吉峯耕平・倉持孝一郎・藤本隆三・新井幸宏「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」刑事弁護 77 号（2014 年）134 頁以下。
[25]吉峯ほか、前注 24、137 頁。
[26]高橋、梶谷、吉峯、荒木、岡、永井『デジタル証拠の法律実務』（日本加除出版、2015 年）10 頁以下。
[27]安冨潔『刑事手続とコンピュータ犯罪』（慶應義塾大学出版会、1992 年）227 頁。
[28]ハードディスクには、製品表示容量の約 0.4%のコピー不可能な領域があるため、全領域を完全一致するというのは矛盾が生じる。また、SSD にあっては、さらに多くの外部領域が存在する。
[29]Goodison, *supra* note 1, at 22-24.
[30]Computer Forensics Tool Testing Program の略であり、EnCase や FTK 等のツール動作の評価を行っている。この汎用的な基準は、「General Test Methodology for Computer Forensic Tools」にあり、「www.cftt.nist.gov/testdocs.html」から入手可能である。
[31]United States v. Borowy, 577 F. Supp. 2d 1133 .
[32]United States v. Borowy, 595 F.3d 1045, 1048 (9th Cir. Nev. 2010).
[33]United States v. Gabel、2010 U.S. Dist. LEXIS 107131 (S.D. Fla. Sept. 16, 2010).
[34] United States v. Carroll, 2015 U.S. Dist. LEXIS 166251 (N.D. Ga. Nov. 3, 2015), United States v. Brooks, 2013 U.S. Dist. LEXIS 184252 (M.D. Fla. Oct. 18, 2013).
[35]連邦刑事手続規則 16 条(a)(1)(E)は、ディスカバリ対象を次のように定めている。(E)文書及び物 書籍、紙、書類、データ、写真、有形物、建築物、場所またはこれらのコピーもしくは部分につき、政府が所持、押収または占有している場合は、被告人に調査またはコピーすることを認めなければならない。ただし、以下のいずれかに場合に限るものとする。(i)対象物が弁護のために利用されるものであること(ii)政府が対象物を公判のために利用する企図があること(iii)対象物が被告の所有または専有物であったこと
[36]United States v. Pirosko, 2013 U.S. Dist. LEXIS 146754 (N.D. Ohio Oct. 10, 2013).
[37]United States v. Budziak、2009 U.S. Dist. LEXIS 56199、 1-4 (N.D. Cal. May 14、 2009).
[38]専属的・再利用不可能性。ソフトウェアの仕様や規格、構造、技術を開発者等が独占的に保持し、情報を公開しないこと。本件では、検察側は、ツールの詳細情報を公開しないというプロプライエタリの条件の下で警察関係者だけが使用することができるツールであると主張した。
[39]United States v. Budziak、 697 F.3d 1105 (9th Cir. 2012).
[40]Budziak v. United States、 133 S. Ct. 1621、 185 L. Ed. 2d 605、 2013 U.S. LEXIS 2065、 81 U.S.L.W. 3513 (U.S. 2013).
[41]United States v. Chiaradio, 684 F.3d 265, 278 (1st Cir. 2012).
[42]United States v. Gazie, 786 F.2d 1166, 1986 WL 16498, at *8-*9 (6th Cir. 1986).
[43]United States v. Pirosko, 787 F.3d 358, 365 (6th Cir. Ohio 2015).
[44]United States v. Budziak, 697 F.3d 1105 (9th Cir. 2012).
[45]United States v. Tummins、 2011 U.S. Dist. LEXIS 57656 (M.D. Tenn. May 26、 2011).
[46]18 U.S.C. § 3509(m)は、「いかなる刑事訴訟においても、児童ポルノに該当する財産または物は、政府及び裁判所の管理、監督及び所持の下におかれなければならない」と規定する。
[47] Rebecca Mercuri,*CourttoomConsidarations in Digital Image Forensics,* in H.T. SENCAR AND N. MOMEN EDS., DIGITAL IMAGE FORENSICS, 314 (2013).
[48]United States v. Thomas、 2012 U.S. Dist. LEXIS 147981、United States v. Thomas、 2013 U.S. Dist. LEXIS 159914.
[49]United States v. Thomas, No. 14-1083 (2d Cir. 2015).
[50] Illinois v. Gates, 462 U.S. 213, 238 (1983).
[51]Williford v. State、 127 S.W.3d 309 (Tex. App. Eastland 2004).
[52] Kelly v. State, 792 S.W.2d 579 (1990).
[53]Frazier v. State, 2015 Fla. App. LEXIS 17420 (Fla. Dist. Ct. App. 5th Dist. Nov. 20, 2015).
[54]State v. Anthony、 No. 48-2008-CF-15606-O、 2011 WL 7463889 (Fla. Cir. Ct. Mar. 18、 2011).
[55]JEFF ASHTON, IMPERFECT JUSTICE: PROSECUTING CASEY ANTHONY (2011).
[56]この事件が、マスメディアの報道によって世論が過熱し、刑事裁判における真実発見に歪みが生じる「ヒーター事件」の典型例であるとするものとして、Susan Bandes, *Fear Factor: The Role of Media in Covering and Shaping the Death Penalty*, 1 OH. STATE. J. OF CRIMINAL L. 585, 593 (2004).
[57]Terry Spencer and Jennifer Kay,*CaseyAnthonyJjurors Lay Low after Names Revealed*, October 25, 2011, AP, http://tampa.cbslocal.com/2011/10/25/casey-anthony-jurors-lay-low-after-names-revealed/.
[58]陪審員の氏名がインターネット上で晒された結果、事件後、仕事を辞めたりフロリダ州から他州に転出したりすることを余儀なくされた陪審員もいた。Nicholas A. Battaglia, *The Casey Anthony Trial and Wrongful Exonerations: How "Trial by Media" Cases Diminish Public Confidence in the Criminal Justice System*, 75 ALB. L. REV. 1579, 1605 (2012).
[59]John Cloud, *How the Casey Anthony Murder Case Became the Social-Media Trial of the Century,*TIME, June 16, 2011,http://www.time.com/time/nation/article/0,8599,2077969,00.html.
[60]SiQuest 社というツールの開発販売元の CEO である John Bradley が、検察側の主張を覆す証言を行った。
[61]Ashton, *supra* note 55, 115-116.
[62]Tony Pipitone、*Cops*、 *prosecutors botched Casey Anthony evidence: Computer search for 'foolproof suffocation' never found*、 WKMG TV Station、 November 28、 2012. http://www.clickorlando.com/news/cops-prosecutors-botched-casey-anthony-evidence
[63]Jigang Liu, *IoT Forensics Issues,Strategies, and Challenges*，デジタル・フォレンジック研究会、第 12 回デジタル・フォレンジックコミュニティ 2015 in TOKYO
[64]暗号解読が困難な場合でも、Pass-the-hash 攻撃等の秘密情報のライブ抽出方法や、ブルートフォースアタック、レイボーテーブルの利用、サイドチャネルアタックなどでパスワード解読を試みることが可能である。しかし、果てしない時間が必要であったり、特定の条件が必要であったり、証拠物の破壊が伴ったりする。
[65]前田恭幸「SSD の Over Provisioned Capacity からのデータ抽出手法」CSEC 2015 年 12 月
[66]湯淺墾道「海外依存せざるを得ないサイバー犯罪捜査－解析ツール、販売拒否されたらお手上げ」e-World Premium 26 号（2016 年）59 頁。
[67]高橋郁夫「リーガルマルウェアの法律問題」InfoCom REVIEW66 号(2016 年) 90 頁以下。
[68]鈴木舞「裁判での科学鑑定の効果的な利用に関する実証的研究」日工組社会安全財団 2013 年度若手研究助成最終報告書
[69]吉峯ほか、前注 24、143 頁以下。