情報処理学会論文誌 Vol.58 No.8 1364–1375 (Aug. 2017)

推薦論文

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

前田 恭幸[1,a)] 湯淺 墾道[1]

受付日 2017年3月7日, 採録日 2017年5月16日

概要：現在のデジタル・フォレンジックは様々な課題に対して，ツールを使用することで対処していることが多い．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自動化したツールもあり，ツールへの依存が高まっている．ツールに関連するアメリカの判例と動向を調査し，ツールの課題と証拠評価についてまとめた．結果，日本の将来の課題への示唆を得て，刑事訴訟におけるツールの課題として5点をあげた．課題を指摘し，公判審理におけるツールの証明力を保持する方法について考察する．

キーワード：デジタル・フォレンジック，刑事訴訟，自動化，証明力

Issues of Digital Forensic Tool in the Criminal Procedure —Based on Cases and Directions in the United States

Yasuyuki Maeda[1,a)] Harumichi Yuasa[1]

Received: March 7, 2017, Accepted: May 16, 2017

Abstract: Current digital forensics has various problems, and they are resolved by using the Digital Forensic Tool. There is also the Tool that automates the process of analysis. Such Tool can be used by the officials who are short of experiments of investigation and analysts. Reliance on the Tool has been increased. To investigate the American court cases and trends related to the Tool, we summarized the challenges to use of Tool. As the result, we conclude the implications for the future use of Tool and coming challenge of Japan. We suggest five points as the challenges to use of Tool in the criminal procedure. We point out the problem, discuss how to hold the probative value of the Tool in the trial procedure.

Keywords: digital forensic, criminal procedure, automated, probative value

1. はじめに

近年，情報通信技術を悪用するサイバー犯罪の件数が増加するとともに，その手法も複雑化・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．これらを利用した犯罪について捜査して被疑者を起訴し，有罪判決を得るためには，裁判所に証拠を提出する必要があるが，日本の刑事訴訟法はデータ（電磁的記録）をそのまま証拠とする制度・手続を欠く．このため，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必要があり，このような電磁的記録の抽出等を行うデジタル・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 [1]，スマートフォンのアプリ解析が困難である [2]，膨大なデジタル証拠を処理する人員不足で大量の未処理案件が生じておりトリアージが必要である [3] 等，様々な課題を抱えている．このため，様々なデジタル・フォレンジックツール（以下，「ツー

[1] 情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY, Yokohama, Kanagawa 221–0835, Japan
[a)] mgs14801@iisec.ac.jp

本稿の内容は 2016 年 9 月の FIT2016 第 15 回情報科学技術フォーラムにて報告され，プログラム委員長により情報処理学会論文誌ジャーナルへの掲載が推薦された論文である．

ル」[*1]という.）を使用することによってこれらの課題に対処することが増えてきた．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 [4].

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 [5]．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，日本およ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．さらに，人工知能（機械学習）を利用したツール[*2]や，自動化されたツールの需要が高まっており，こうした自動化による負の側面についても考察した．

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 5 点を明らかにした．

2. 刑事訴訟とデジタル・フォレンジック

2.1 電磁的記録の解析に関する現状

従来は，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．この手法はレガシー・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等の相違があり [6]．それにともなって，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 [2] 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．

同データによれば，解析件数およ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 日本の判例の現状

デジタル・フォレンジックで使用したツールについて争われた判例は，管見の限りでは公刊された判例集には登載されていない．しかし，解析の結果について争われた事例等は存在している．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 [7] 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 [8] 等がある．また，いわゆる村木さん裁判（厚労省事件）[9] 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 [10] 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[*3]．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であろう．

また，デジタル証拠の証拠能力が争われた事例の中には，検証許可状によるリモート・アクセスを利用した複写に関して，重大な違法があるとして証拠が排除された事例がある [11]．サイバー犯罪に使用される電子機器類とそのデータの保存方法が多様化し，必ずしも電子機器の内部にデータが保存されていない場合が生じているが，このような場合には機器類からデータを抽出・複写し，複写されたデータを分析するというレガシー・フォレンジックの手法では対応することができない．このため，ツール類を用いて電子機器類からデータの蔵置先（日本国外の場合もある）に遠隔的にアクセスすることが必要となるが，その是非と法

*1 アメリカの判例等においてデジタル・フォレンジックツールを示す際には，Software，Automated Software，Program 等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．

*2 例として，機械学習を用いて大量の文書ファイルから重要な文書ファイルを判断する Predictive Coding のツールがある．

*3 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．詳細は判例からは分からないため，江川氏のブログを参照．江川紹子【PC 遠隔操作事件】入手先 ⟨http://bylines.news.yahoo.co.jp/egawashoko/⟩（参照 2016-06）.

的な手続きが問われたという事例である．

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うえで，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，日本の法体系および法律実務は，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等が理論をリードしているという [12]．しかし，アメリカにおける議論を参照するうえでは，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，証拠法の考え方，民事と刑事における証拠法の現れ方，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 点をあげている [13]．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が議論となる．

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 [14]．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，アメリカではディスカバリと陪審が多用されている．ディスカバリとは証拠開示手続を意味し，連邦刑事訴訟規則 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．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 [15]．

3. 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）等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 [16]．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 等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等，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 1 つであるともされている [17]．このほか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
Table 1 Classification of the tool.

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

ツールに関しては，デジタル・フォレンジック研究会が「証拠保全ガイドライン　第 5 版」[18] を公開しており，16 種類の代表的な収集およ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，本稿では，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[*4]．

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，ログ解析等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 [19]．

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 [20]．また，特殊な解析が必要な場合のツールには，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．判例では DNA 型鑑定等の科学的証拠にも専門性が必要であることが示されており[*5]，ツールを用いた証拠も同様と考えられる．

ツールを使用する時期は，犯罪捜査機関等が行っている捜査の一環としてネットワーク等を介して証拠の収集を行う証拠収集，保全作業，解析の 3 つに分けることができる．

[*4] ツールには，ソフトウェア・ハードウェアでの分類，収集・保全・解析等の用途での分類，データ復元・暗号解除・自動化等の機能面での分類等多岐にわたる．そのため，本論では，アメリカの判例に多く出てくるものが市販ツールであったため，ツールの開発者や流通経路を軸とした．

[*5] 最判平 12・7・17　判タ第 1044 号 79 頁．本件は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．

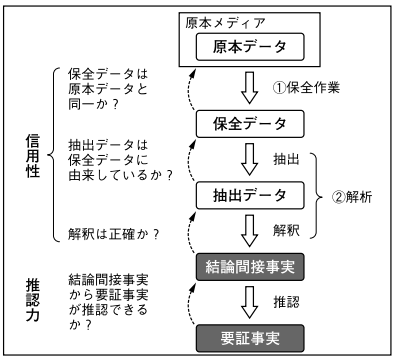

図 1 事実認定の構造 [22]
Fig. 1 Structure of the finding.

その中の，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 [21].

また，高橋らは，デジタルデータを証拠とするうえで，データそのものの性質に由来する問題として，原本性，完全性・真正性の立証，見読性（可視性）があるとしている [23]．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の問題がある．また安冨は，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する．これについては，電磁的記録を一定のプログラムに従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されている [24]．しかしこれらの問題につき，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[*6]，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．ところが，前述したように，日本ではこのような疑問が争点になった判例等は，判例集に登載されていないのが現状である．

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，**表 2** 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．

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，

[*6] ハードディスクの複写について，HPA（Host Protected Area）や DCO（Device configuration overlay）等の保護領域以外に，製品表示容量の約 0.4%のコピー不可能な外部領域があるため，全領域が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．

表 2 デジタル・フォレンジックにおける検察官側の課題 [25]
Table 2 Problem of the prosecutor side in Digital Forensic.

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．

CFTT[*7]がある．ほかにも，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分かる．

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

[*7] 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．

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の保護は及ばないとしてそれを退け [26]，控訴裁判所の判決でも原審の判断が支持された [27]．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 [28] 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 [29]．

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」[*8]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 [30] もある．

合衆国対バドジアック事件 [31] 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[*9]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 [32] 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 [33]，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 [34] 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 [35] 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 [36]．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 [37] 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 [38] 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等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

[*8] 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．

[*9] 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．

扱いについて規定する連邦法[*10]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および弁護人のみにアクセスおよ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 [39]．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自体の開示という 2 つがあることが分かる．

4.4 自動化ツールの許容性に関する判例

近年では，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，解析等が可能なツールが増加している．このため，そういったツールによる分析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 [40] 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てを行った．

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，令状な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 [41]．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 [42]，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 [43] 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 [44] 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

[*10] 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．

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 [45].

4.5 陪審においてツールおよびツールを使用した解析結果が争点となった判例

4.1 節から 4.4 節までは許容性に関する判例であるが，証明力に関する判例として，陪審裁判でツールおよびツールを使用した解析結果への信頼性が問われ，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）[46] という判例がある．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，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 [47]．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[*11]，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 [48] や世論とは異なる評決をした陪審員への嫌がらせ等[*12]，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 [49].

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とともに，被告人の両親宅に同居していた．2008 年 7 月 15 日，オレンジ郡保安官事務所に被告人の娘が行方不明であるとの届けが出たが，警察の事情聴取に対して被告人は虚偽の陳述をした．被告人は，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，被告人の娘と確認された．2011 年 6 月，被告人は第 1 級殺人，児童虐待，激昂したうえでの児童故殺，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．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，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，公判では次のような検察側と被告人側の主張の対立があった．

> 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[*13]）：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が，SiQuest 社の「CacheBack」というツールを改良してもらい，その後，8,557 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ものである．
>
> 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と結果が相違することについても，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．

結果として，第 1 級殺人罪等について陪審は無罪と評決した．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，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 [50]．また, Microsoft OS 標準のブラウザである Internet Explorer（IE）と Fire Fox 双方の検索履歴を解析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等が事後に報道された [51].

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

[*11] 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，Bandes, S.: Fear Factor: The Role of Media in Covering and Shaping the Death Penalty, Oh. State. J. of Criminal L, Vol.1, pp.585–593 (2004).

[*12] 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．Battaglia, N.A.: *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).

[*13] 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．

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．④ EnCase 等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等においては，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，ツールおよ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

これまで，日本とアメリカの事例を紹介してきた．すでに述べたように，アメリカではツールを使用すること自体が争点となる判例も多くある．このため，アメリカの動向と判例を手がかりにしてツールを用いることにより得られた証拠の証拠能力と証明力の日本における課題について，次の 5 つの点から考察する．

5.1 ツールを用いた証拠収集と違法行為・証拠排除

ツールを用いて自動的にネットワーク上の情報を収集し証拠とする場合，収集した証拠が違法な行為により収集されたものとして排除される場合があるため，法的検討が必要であることはすでに示した．つまり，ツールを用いて技術的に収集可能であることと，収集した証拠が法的に証拠能力を有するかは別の問題である，ということである．

その一例として，法執行機関が標的のコンピュータに対してリモートで展開し，パソコンのカメラの起動，パスワードの収集，電話の傍受等を行うツールの総称であるリーガルマルウェアの使用の是非がある．高橋は，リーガルマルウェアの法的位置づけについて論じている [52]．こういったリーガルマルウェアを我が国でも使用すべきか，使用できるのかといった問題がある．

これらの点に関しては，法執行機関と犯罪者との不均衡が存在することを考慮すべきであると考える．犯罪者は，サイバー空間上で，TOR（The Onion Router：インターネットの接続経路の匿名化を行うツールであり，遠隔操作事件で被告人が使用していた．）に代表される匿名通信システム等を使用し，サイバー犯罪を行うためのツールの販売・購入を行い，いくつもの違法行為を積み重ねていることがある．例として，セキュリティの脆弱性を狙ったサイバー攻撃を行うことが可能なツールがダークウェブ上を中心に販売されており，専門性がなくても匿名で犯罪行為を行うことが可能となっている[*14]．それに対して，法執行機関側は，すでに述べたように，ツールを用いて技術的には情報収集・解析が可能であっても，それを法的観点から実施してよいかは別の問題であり，情報収集・解析に制約がともなうため，犯罪者の追跡や特定が困難な場合がある．

さらに，技術と法の観点から最近話題となっている課題として，iPhone のパスコード解除に関する事例がある．湯淺は，FBI が全令状法（All Writ Act）という連邦法に基づき，Apple 社に iPhone のロックを解除して，FBI の捜査を支援する命令を出すことを連邦裁判所に求めた問題について，ロック機能を解除する技術的支援命令に関して Apple 社がそれを拒否する法的な権利や根拠を有するかどうかについての議論を紹介し，Apple 社にそのような命令を出すことが憲法上は許容されるとしても，全令状法という法律レベルにおいて合法的であるかという別の問題もあると指摘している [53]．また，パスコード解除に関する事例は，デジタル・フォレンジックとプライバシの対立に発展する可能性もあるだろう．

今後，高機能なツールが開発された場合には，それを使用して証拠を収集・解析してよいかどうか，収集・解析が正当な業務行為（刑法 35 条）に該当するか等の議論が必要になるものと考えられる．

5.2 ツールの使用に関する検察官側と被告人側の不均衡

前述のようにアメリカにおける弁護人のデジタル・フォレンジックの課題の 1 つとして，検査官側と被告人側の不均衡があった．ケイシー事件では，法執行機関のみが使用できるツールは許容された．さらに，合衆国対バドジアック事件では，検察官側のプロプライエタリという条件付きであるツールがディスカバリの対象となるのは，被告人側が解析結果のエラーについて立証できる場合に限られるとされた．このように，検察官側のみ使用できるツールがあることや，被告人側はそれらのツールを使用することが困難であるため，検察官側と被告人側の不均衡が存在する．

しかし，合衆国対タミンズ事件では，被告人側に対して，解析前のハードディスク（証拠物であるハードディスクを複写したもの）に対してはディスカバリが認められた．また日本でも，遠隔操作事件において，検察官側の証拠であるハードディスクが被告人側に開示された．このように，データが保全されている場合，検察官側の証拠物を複写したものに関して証拠が開示されることが，被告人側の最大の防御策であろう．また，検察官側の科学的証拠に関するデータが，被告人側から開示請求があったにもかかわらず開示されない場合，科学的証拠の信頼性を低下させる可能

[*14] ここでの攻撃ツールは，デジタル・フォレンジックツールを示しているわけではない．デジタル・フォレンジックの技術やペネトレーションの技術等が悪用され，犯罪に利用されるツールがあることを示している．

性があるため，証明力の問題にもなりうる．この点は，デジタル証拠に第三者検証性があるため，他の科学的証拠よりも開示が容易である場合が多いことも影響する．

したがって，ツールの使用に関する検察官側と被告人側の不均衡については，解析前のハードディスクを複写したものおよび元のデータに関しては開示を認めることで，検察官側と被告人側の不均衡に対応できると考えられる．

5.3 自動化ツール使用者に求められる専門性の不透明さ

現状では，自動化ツールを使用する解析者等に求める専門性が不透明なため，専門性のない解析者等による証拠の見落としが起こり，証明力が減殺される可能性がある．ケイシー事件では，専門性が不足する捜査員の証拠の見落としがあったことで証明力の減殺があったものと予想される．

しかし，コンピュータ・アーキテクチャ，カーネル，メモリ，ファイルシステム，データベース，ネットワーク等，広範囲で深い知識が必要であるデジタル・フォレンジックに関して，専門性を定義することは困難である．また，すべての解析者等に，技術者と同等の専門性を求めるのは，予算・時間・人数の観点から非常に困難であり現実的でない．そのため，ツールを使用するすべての解析者等が，ツールの限界とリスクを知ること，収集・保全・解析の記録を取ることが重要である．

ツールの限界とは，パソコンの保全作業の場合，ハードディスクを物理コピーですべて複写した場合は未使用領域からのデータ復元が可能であるが，ハードディスクを論理コピーで複写した場合は未使用領域からのデータ復元は不可能で，論理コピーによる複写後は，ツールを用いても未使用領域からはデータ復元できないという問題である．ツールのリスクは，ツールを使用することで，証拠物のデジタルデータが改変・消去される場合があることである[*15]．そのため，デジタル・フォレンジックの目的と状況に応じて，使用するツールとツールの使い方を変える必要がある．捜査員がツールの限界とリスクを知ることで，デジタルデータの証拠の見落としが減少し，結果として証明力の保持にもつながる．

専門性のある技術者が使用したツールやその解析結果について争われた場合，当該技術者が証人尋問で証言することで，証明力保持に向けた議論が可能になる．しかし，専門性のない捜査員等がツールを使用した解析結果や，使用したツールの信頼性が争われた場合，専門性のない捜査員が証言をするのは困難な場合がある．その場合，ツールの開発・検査者の証人尋問による証言，鑑定，鑑定嘱託等の対応によって，証明力保持に向けた議論が可能となる．そのため，ツールを使用する解析者等は，ツールの名称・バージョン・開発元・使用日時・使用手順・解析対象物等の記録を残し，事後においても再解析できる状況にするべきである．

[*15] 証拠物であるパソコンを操作して一部のログ等が消去される場合，同じく証拠物であるパソコンのメモリフォレンジックを行う手順が良くないため一部のログが消去される場合，スマートフォンの解析時に対象の証拠物にエージェントを入れること等が例としてある．

5.4 ツールのエラーの可能性

合衆国対タミンズ事件では，EnCase という世界中で使用され CFTT において評価を受けているツールであっても，解析結果にエラーが存在するため，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．また，ケイシー事件から，ツールを用いることで必ず正しい解析結果を得るとは限らないことも分かる．

ツールによる解析の誤りの可能性を増大させている要因として，様々な技術の進化に対応しなければならないこと，「アンチ・フォレンジックツール」の存在がある．

技術の進化の例として，スマートフォンの無料通話アプリ等があり，それらは犯罪インフラとして悪用されることが多い．それらのアプリの解析のためには，1 つの OS のみを考えても，おおよそ月に一度のアップデートがあり，そのつど，ツールの更新について検討する必要がある．

また，デジタル・フォレンジックを回避するアンチ・フォレンジックの手法が存在する．その例として，携帯電話機等を解析する UFED というツールに対して，携帯電話機にアンチ・フォレンジックツールをインストールすることで，解析機能を回避することが可能とした研究がある [54]．その反面，アンチ・フォレンジックツールの痕跡を検出することで，デジタル・フォレンジックに一定の効果があることを示す研究 [55] もある．

このようにアンチ・フォレンジックという手法の出現によって，ツールが使用できない，またはツールを使用しても効果がない場合が生じている．アンチ・フォレンジックの対策のためのツール開発が求められる等，ツールの開発はつねに新しい課題とも向き合いながら，精度を高めていかなければならない．さらには，ツールによって解析結果が異なる場合もあり，その証拠評価の在り方が問われる．

ツールを用いることで必ず正しい解析結果を得るとは限らない．このため，ツールの精度向上や，確実な保全作業・証拠収集，解析手法・公判での対応を変えることといった対策が必要となると考える．

5.5 公判におけるツールに対する評価の困難性

公判において解析過程等について証明力が争われた場合，裁判官や裁判員が認識，評価することが困難となる場合がある．裁判官および裁判員から見ると，デジタルデータのみならず，ツールも「ブラックボックス」であるため，認識・評価が困難である．そのため，証人や鑑定人の公判廷における証言が重要となる．

解析過程の信用性が争点となった場合，証拠書類を作成

した者，あるいはツールを開発・検査した専門家が証人出廷し，尋問を受けることで証明力が争われることになる．また，デジタル証拠の改ざんがないかの真正性が争われた2章の判例では，鑑定人の作成した鑑定書および公判廷における鑑定人の証言により，証明力が争われた．したがって，捜査員が自動化ツールを用いて解析したものの，ツールの動作・原理について不明な場合には，専門家が公判廷で尋問を受けることが考えられる．

デジタル証拠の信頼性が争われる場合，科学的証拠の信頼性の前提である「収集，移動，保管の過程の適切な管理」についてはもちろんのこと，デジタル証拠の特殊性であるデジタル証拠の改変・改ざんがない（真正性）ことはいうまでもなく必要である．さらに，解析結果の正確性等が争われた場合，公判の証人尋問における証言が重要となり，公判で証明力を争うための尋問については，証言の信用性と証人の信用性の問題がある[*16]．

証人の信用性に関し，遠隔操作事件の第4回公判において検察官側証人は，被告人側の質問に「覚えていない」「記憶にない」を繰り返し，明らかに鑑定と関連する事項についての問いにも証言を渋ったといわれている．それらに対し江川は，被告人側の尋問に対してのみ証言を渋る態度や，鑑定に至る経緯等をいっさい証言しないという態度を続ければ，この証人の証言全体についての信頼度が損なわれかねない，と意見を述べている [56]．そのため，検察官側の証人であろうと被告人側の証人であろうと，主尋問，反対尋問ともに変わりなく証言すべきである．

証言の信用性について，日本の公判において解析過程やツールの信用性が争われた場合には，検査方法を評価する項目に沿って説明するという方法が有効的であると考える．そこで，以下の項目について証言することを提案する．

- ツール開発の原理や知見が信頼できること
- ツール動作の具体的理論や技術が信頼できること
- ハードディスク等の解析対象である証拠の前処理が適切であること
- 解析用パソコンを含めた機器が正しく作動し手法が適切であること

6. 終わりに

同じ解析対象物に，同じ解析者が，異なるツールを使用したところ，解析結果が異なったという事例は，日本だけではなく世界中どこでも起こりうる問題である．また多様な電子機器に様々なアプリがインストールされ，利用の態様が広範化・複雑化していることを考えると，デジタル・フォレンジックにおける自動化等のツールの重要性は，増加する一方であると思われる．しかしツールの自動化による負の側面として，自動化によりだれにでも解析作業を行うことができるため解析者等に専門知識や技能が要求されなくなるという点がある．その反面で，刑事訴訟において要求される専門性が不透明であることや，自動で解析されている過程がブラックボックスであるため証拠の評価が困難であることが問題点として表面化してきている．

本稿ではアメリカの動向と判例の検討を通じて，日本の将来における課題に対して様々な示唆を得ることができた．アメリカの判例からは，法執行機関のみが使用できるCPSというツールの動作，使用するための研修およびライセンスが必要であること，P2Pファイル共有ソフトウェア上の証拠の収集方法が問題となること，評価が高く世界中で使用されているEnCaseというツールであってもツールの信頼性が争われること等，多くの問題が存在することが明らかとなり，それらの論点について考察を行った．

本稿ではアメリカの事例の考察を通じて，自動化ツールを使用する解析者等の専門性や公判におけるツールの評価のあり方について検討を加え，このような事例が発生した場合の対処方法についての提言を行った．本稿で提言した対処方法により，日本の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）および「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．

[*16] 証明力を争うための尋問は，「証人の観察，記憶又は表現の正確性等証言の信用性に関する事項及び証人の利害関係，偏見，予断等証人の信用性に関する事項について行う．」とある（刑事訴訟規則199条6項）．

参考文献

[1] Goodison, S.E., Davis, R.C. and Jackson, B.A.: Digital Evidence and the U.S. Criminal Justice System: Identifying Technology and Other Needs to More Effectively Acquire and Utilize Digital Evidence (2015), available from ⟨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，入手先⟨https://www.npsc.go.jp/report27/03-26.pdf⟩.
[3] Goodison, *supra* note 1, at 23.
[4] James, J.I. and Gladyshev, P.: Challenges with Automation in Digital Forensic Investigations, *Computers and Society* (2013).
[5] 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，Vol.68, No.4, p.89 (2015).
[6] Murphy, E.: *The New Forensics: Criminal Justice, False Certainty, and the Second Generation of Scientific Evidence*, Vol.95, No.3, pp.721–729 (2007).
[7] 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）．
[8] 水戸地判平23・5・20（判例集未登載）．
[9] 大阪地判平22・5・26（判例集未登載）．
[10] 東京地判平27・2・4（判例集未登載）．
[11] 横浜地判平28・3・17 LEX/DB 25542385.

[12] 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，Vol.24, No.1-2 (2010).
[13] 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), 入手先 ⟨http://www.comit.jp/BLTJ/civilpro/LS/forensic2.htm⟩ （参照 2016-03）.
[14] 安冨 潔：刑事訴訟法，第 2 版 (2013).
[15] 守本正弘：ディスカバリ，起業家大学出版 (2012).
[16] Nelson, B., Enfinger, F., Phillips, A. and Steuart, C. (Eds.), SITE J1（訳）：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).
[17] Solomon, M.G., Rudolph, K., Tittel, E., Broom, N. and Barrett, D.: 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).
[18] 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).
[19] 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).
[20] 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，Vol.49, No.1-2，産大法学 (2015).
[21] 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，No.77 (2014).
[22] 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，No.77, p.137 (2014).
[23] 高橋郁夫，梶谷 篤，吉峯耕平，荒木哲郎，岡 徹哉，永井徳人：デジタル証拠の法律実務，日本加除出版 (2015).
[24] 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).
[25] Goodison, *supra* note 1, at 22-24.
[26] United States v. Borowy, 577 F. Supp. 2d 1133.
[27] United States v. Borowy, 595 F.3d 1045, 1048 (9th Cir. Nov. 2010).
[28] United States v. Gabel, 2010 U.S. Dist. LEXIS 107131 (S.D. Fla. Sep. 16, 2010).
[29] 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).
[30] United States v. Pirosko, 2013 U.S. Dist. LEXIS 146754 (N.D. Ohio Oct. 10, 2013).
[31] United States v. Budziak, 2009 U.S. Dist. LEXIS 56199, 1-4 (N.D. Cal. May 14, 2009).
[32] United States v. Budziak, 697 F.3d 1105 (9th Cir. 2012).
[33] 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).
[34] United States v. Chiaradio, 684 F.3d 265, 278 (1st Cir. 2012).
[35] United States v. Gazie, 786 F.2d 1166, 1986 WL 16498, at *8-*9 (6th Cir. 1986).
[36] United States v. Pirosko, 787 F.3d 358, 365 (6th Cir. Ohio 2015).
[37] United States v. Budziak, 697 F.3d 1105 (9th Cir. 2012).
[38] United States v. Tummins, 2011 U.S. Dist. LEXIS 57656 (M.D. Tenn. May 26, 2011).
[39] Mercuri, R.: *CourttoomConsidarations in Digital Image Forensics*, Sencar, H.T. and Momen, N. (Eds.), Digital Image Forensics, 314 (2013).
[40] United States v. Thomas, 2012 U.S. Dist. LEXIS 147981, United States v. Thomas, 2013 U.S. Dist. LEXIS 159914.
[41] United States v. Thomas, No. 14-1083 (2d Cir. 2015).
[42] Illinois v. Gates, 462 U.S. 213, 238 (1983).
[43] Williford v. State, 127 S.W.3d 309 (Tex. App. Eastland 2004).
[44] Kelly v. State, 792 S.W.2d 579 (1990).
[45] Frazier v. State, 2015 Fla. App. LEXIS 17420 (Fla. Dist. Ct. App. 5th Dist. Nov. 20, 2015).
[46] State v. Anthony, No. 48-2008-CF-15606-O, 2011 WL 7463889 (Fla. Cir. Ct. Mar. 18, 2011).
[47] Ashton, J.: Imperfect Justice: Prosecuting Casey Anthony (2011).
[48] Spencer, T. and Kay, J.: *CaseyAnthonyJjurors Lay Low after Names Revealed* (Oct. 2011), AP, available from ⟨http://tampa.cbslocal.com/2011/10/25/casey-anthony-jurors-lay-low-after-names-revealed/⟩.
[49] Cloud, J.: *How the Casey Anthony Murder Case Became the Social-Media Trial of the Century*, Time (June 2011), available from ⟨http://www.time.com/time/nation/article/0,8599,2077969,00.html⟩.
[50] Ashton, *supra* note 58, 115-116.
[51] Pipitone, T.: *Cops, prosecutors botched Casey Anthony evidence: Computer search for 'foolproof suffocation' never found*, WKMG TV Station (Nov. 2012), available from ⟨http://www.clickorlando.com/news/cops-prosecutors-botched-casey-anthony-evidence⟩.
[52] 高橋郁夫：リーガルマルウェアの法律問題，InfoCom REVIEW, Vol.66 (2016).
[53] 湯淺墾道：全令状法と iPhone 問題に関する若干の考察，電子情報通信学会技術研究報告，Vol.116, No.71 (2016).
[54] Karlsson, K.-J. and Glisson, W.B.: *Android Anti-forensics: Modifying CyanogenMod*, *47th Hawaii International Conference on System Science* (2014).
[55] 浦野 晃，橋本正樹，辻 秀典，田中英彦：アンチ・フォレンジックツールの痕跡検出方式に関する初期的検討，コンピュータセキュリティシンポジウム 2013 論文集 (2013).
[56] 江川紹子：【PC 遠隔操作事件】コンピュータ・フォレンジクスで HDD を徹底 "解剖" する（第 4 回公判メモ 2），入手先 ⟨http://bylines.news.yahoo.co.jp/egawashoko/20140323-00033814/⟩ （参照 2016-06）.

推薦文

デジタル・フォレンジックツールという新規性の高い分野について，日米にわたって裁判例を分析し果敢に議論を展開している．科学的証拠の重要性や情報技術の進展と相俟って，今後，実務上も問題となる点についての分析と評価でき，論文誌への掲載を推薦できる．

（FIT2016 第 15 回情報科学技術フォーラムプログラム委員長 大場みち子）

前田 恭幸 （正会員）

情報セキュリティ大学院大学大学院情報セキュリティ研究科博士前期課程修了．

湯淺 墾道 （正会員）

情報セキュリティ大学院大学情報セキュリティ研究科教授.