Vol.2016-EIP-72 No.9
2016/6/2

ケイシー事件を手がかりにした、デジタル証拠の証明力評価に関する考察

前田恭幸[†1]　湯淺墾道[†2]

概要：本稿では、デジタル・フォレンジックの失敗例と言われたケイシー事件の問題について、日本の事例と比較し、刑事訴訟におけるデジタル証拠の証明力評価の観点から検討を行う。ケイシー事件では、2つのツールによる解析結果の相違などが理由となり、陪審員の事件有罪への心証を形成できなかった。このことから、デジタル証拠の課題を指摘し、公判審理におけるデジタル証拠の証明力を高める方法について考察する。

キーワード：ケイシー事件、デジタル証拠、刑事訴訟、証明力

Study on Probative Evaluation of Digital Evidence - Examing Casey Trial and its Implications -

Yasuyuki Maeda[†1]　Harumichi Yuasa[†2]

Abstract: In this paper, the problem of failures and said the Casey case of digital forensics, compared with Japan's case, carry out the investigation from the point of view of probative force evaluation of digital evidence in criminal proceedings. In the Casey case, such as the analysis of the results the difference by the two tools is the reason, it was not able to form an impression to the jury of the case guilty. From this fact, it pointed out the challenges of digital evidence, consider how to increase the probative value of digital evidence in trial proceedings.

Keywords: Casey Trial、Digital Evidence、Criminal Procedure、Probative value

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、公判審理においてデジタル証拠の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、日本では解析過程の信用性が争点になる事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、事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・フォレンジックに関係して多くの事例がある。このため本稿では、

†1 情報セキュリティ大学院大学.
†2 情報セキュリティ大学院大学.

[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。

公判審理における証明力の確保という観点から、ケイシー事件を手がかりに検討して、日本の将来の課題への示唆について考察した。

2. ケイシー事件

2.1 ケイシー事件の概要

ケイシー事件は、事件当時 22 歳だった若い母親のケイシー・アンソニーがまもなく 3 歳になろうとしていた娘のケイリー・アンソニー(Caylee Anthony)を殺害したとして逮捕され、第 1 級殺人罪で起訴されたというものである。有力な物証がなく、フロリダ州オレンジ郡裁判所の陪審裁判において検察側は 23 人の専門家証人、弁護側は 14 人の専門家証人を繰り出した。このため公判は 1995 年の O.J.シンプソン裁判並みに全米の注目を集め、結局、2011 年に陪審によって殺人については無罪の評決が下された[7]。

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、書籍も出版されており、その中には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も含まれる[8]。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[9]、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[10]、陪審員の身元のインターネット上での公開[11]、有罪を予想した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[13]。当時この裁判所に在籍していた裁判官は、「国際的なメディアの報道の過熱によって、地方の問題である州の陪審制度に対する国民の関心がかき立てられた」と回想している[14]。また、事件をきっかけとして後述するように「ケイリー法(Calyee's Law)」を制定する州が現れるなど、本事件が刑事司法全体に与えた影響も大きい。

[7]State v. Anthony, No. 48-2008-CF-15606-O, 2011 WL 7463889 (Fla. Cir. Ct. Mar. 18, 2011).
[8]JEFF ASHTON, IMPERFECT JUSTICE: PROSECUTING CASEY ANTHONY (2011).
[9]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).
[10]陪審員のうち 5 人は男性（うち 1 人がアフリカ系）、7 人が女性（うち 1 人がアフリカ系）で、12 人のうち 10 人が被告人と同じ白人ということについて、偏向しているという批判も起きた。陪審員の一人のジェニファー・フォード(Jennifer Ford)という女性は、その後インタビューに応じている。フォードは当時 32 歳で、子どもを抱えながら看護学校に通う学生であった。フォードのインタビューは、陪審員は被告人は有罪という心証を形成しつつもそれを裏付ける物証が不十分と感じていたこと、検察側が殺人の動機を明確にすることができなかったこと等が無罪評決を下すに至った理由であることを示唆している。Marcia Clark, *Casey Jury Brainwash*, The Daily Beast, July 8, 2011, http://www.thedailybeast.com/articles/2011/07/08/casey-anthony-trail-the-sequestered-jury-fell-prey-to-idiotic-groupthink.html.
[11]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/.
[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。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).
[13]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.
[14]Antoinette Plogstedt, *Citizen Judges in Japan: A Report Card for The Initial Three Years*, 23:3 IND. INT'L. & COMP. L. REV. 371 (2013).

2.2 デジタル・フォレンジックの意義と問題点

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ポンティアック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、デジタル・フォレンジックによる解析結果により、被告人宅のコンピュータを使ってサーチエンジンでクロロフォルムに関する検索を行っていたと判明したことが、第 1 級殺人罪成立の要件となる計画的殺人を行ったということを裏づける有力な証拠とされたのである[15]。

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。さらに、警察がアンソニ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証拠とされたのである。

警察の解析の際に利用されたのは、「NetAnalysis v1.37」というイギリス製のツールであり、このツールを使って、Mozilla Firefox の検索履歴データベース(Mork Database)を検索したところ、「クロロフォルム」というキーワードを入力して Google で 84 回検索したという証拠が得られたというのが、当初の検察側の主張であった。

ところが被告人側の証人であるコンピュータ・フォレンジックの専門家で、SiQuest 社[16]というフォレンジック・ツールの開発販売元の CEO であるジョン・ブラッドレー(John Bradley)が、それを覆す証言を行った。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 回だけであったという[17]。また検索した結果、実際に閲覧したのは「SCI-SPOT.COM」というサイト[18]であり、クロロフォルムに関する科学的な説明を淡々と記述しているにすぎないものであった。

検察側は、当初は全く検索履歴を復元できなかったもう 1 種類のツールの開発元に捜査官が依頼して、数晩かかって改良してもらったところ、改良版のツールによって 8557 記録を復元することができ、この記録の中から 84 回という検索回数の証拠が得られたという。ブラッドレーの証言によれば、このもう 1 種類のツールというのが SiQuest 社の CacheBack であった（現在は、CacheBack は Internet Examiner という名称に変更されている）。

[15]Goodison, Davis and Jackson, *supra* note 8,2.
[16]http://www.siquest.com/.
[17]Lizette Alvarez, *Software Designer Reports Error in Anthony Trial*, NY. TIMES, July 18, 2011, http://www.nytimes.com/2011/07/19/us/19casey.html.
[18]http://sci-spot.com/.

この間の事情について、上述の検察官の回想録は次のように釈明しており、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、事実のようである[19]。

トランクのサンプルの中からクロロフォルムが検出されたことは、我々全員にとっての驚きであった。クロロフォルムは、被害者の意識を失わせるための麻酔薬として使われることで知られており、そのあたりのドラッグストアで買えるようなものではない。それが実際に犯行に使用されたものではないにしても、メリッシュ(Melich)刑事は、何者かが[訳注：被告人らの家族が住んでいる]アンソニー宅のコンピュータを使ってオンラインでクロロフォルムを買おうと試みたかどうかを調べることは、実行に値すると考えた。

オレンジ郡保安官事務所のコンピュータ・フォレンジック捜査官であるサンドラ・ケイン(Sandra Cawn)は、すでにアンソニー宅のコンピュータを調査していた。少しでも[訳注：被告人が、被害者のベビーシッターとして雇ったとしていた]ザニーの行方に関する手がかりを得ようとしていたからである。メリッシュ刑事は、「クロロフォルム」という語で検索したかどうかも調べることができるかどうかをケイン捜査官に聞いた。ケイン捜査官は最初に、ケインが[訳注：被告人の男友達で、被害者が行方不明となっていた 31 日間、ほとんど一緒に過ごしていた]トニー(Tony)宅で使っていたラップトップ・コンピュータのハードディスクを検索したが、何も得られなかった。そこでケイン捜査官はアンソニー宅のデスクトップ・コンピュータに着目した。

捜査官は最初にアクティブなファイル類を検索したが、何も得られなかった。そこで捜査官は、ハードディスクの未割当領域に注目した。我々が説明されたところでは、コンピュータから何かを削除しても、デジタル情報はハードディスクの別の領域に移動し、新たな情報によって上書きされることが可能であるという。このコンピュータの特性は「未割当領域」と呼ばれている。コンピュータからファイルを削除したと思っても、実際にはファイルは存在する。その後、新たな情報がすべての領域を占めたとき、情報はやっと完全に消去される。そのときまでであれば、コンピュータ・フォレンジック捜査は、適切なソフトウェアを使って、データを掘り出すことができる。

ケイン捜査官がアンソニー一家のコンピュータを調査したとき、捜査官は「クロロフォルム」というキーワードが複数回参照されていることを発見したが、それがケイン捜査官のソフトウェアと捜査官自身の経験の限界であった。そこで捜査官は、上司や助言者、教師役であったケビン・スティンガー(Kevin Stenger)巡査に相談した。スティンガー巡査は、もっと洗練されたソフトウェア――それは開発途中のものであったが――を使って、3 月の日中 2 日間、何者かがクロロフォルムに関する情報の検索を行ったことを突き止めることができた。ある検索においては、何者かが実際に「クロロフォルムを作成する方法(how to make chloroform)」というクエリーを入力していた。

クロロフォルムについての検索日時を知って、メリッシュ刑事は、誰がその午後にコンピュータを操作したのかを知りたいと考えた。メリッシュ刑事は、シンディとジョージはおそらく家にいなかったであろうと推察し、クロロフォルムに関する検索が行われた時間の彼らの勤務記録を取り寄せれば、それを証明できると考えた。シンディの勤務記録は、2 日間ともにその時間にはシンディは働いていたことを示していた。ジョージの勤務記録は、その月にはジョージは雇用されていなかったことを示していたが、ジョージは検索が行われた 2 日間のうち 1 日は 10 時間働いていた。

トランクの中と、コンピュータの検索記録の中からクロロフォルムを発見したことは、この事件の疑惑に新しいレイヤーを追加することになった。

これに対して弁護側は、検察側の主張では、最初に NetAnalysis を使用して解析作業を行った時点で 84 回の検索履歴が復元できたかのように説明していたのは、陪審員を意図的に誘導するものであると検察側を強く批判した。また弁護側は、Net Analysis の解析結果と別のツールである CacheBack 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とした[20]。

2.3 判決と事後の報道

結局、陪審は第 1 級殺人、児童虐待、激昂した上での児童故殺については無罪という評決を行い、4 件の警察官への虚偽陳述については有罪と評決したのである[21]。

その後、4 件の警察官への虚偽陳述についてフロリダ州刑法[22]違反で有罪と評決されたことについて、被告人側は不服として控訴した。これに対してフロリダ州第 5 地区控訴裁判所は、2013 年 1 月 25 日にオーフィンガー(Orfinger)首席裁判官、トーリー(Tory)裁判官及びエバンダー(Evander)裁判官が全員一致の判決を下し、二重の危険禁止の法理を適用して、4 件のうち 2 件を有罪とした[23]。

被告人が虚偽の陳述をしたとされている 4 件は、被告人の両親宅における尋問の際の陳述が虚偽であったことについて起訴されたものであるが、そのうち 2 件は後日に警察署における尋問の際にも繰り返して虚偽陳述を行っており、両親宅における尋問の際の虚偽陳述と警察署における尋問の際の虚偽陳述とは、別件の刑事事件を構成するとした。このため、アメリカ合衆国憲法及びフロリダ州憲法の二重の危険禁止の法理を適用して、4 件ではなく、2 件について虚偽陳述で有罪としたものである。

その後、地元のテレビ局は、警察が証拠を見落としていた可能性があることを報道した[24]。報道によれば、警察はアンソニー宅のコンピュータのインターネット・エクスプローラ(IE)の閲覧履歴を解析した。しかし、被告人は IE ではなく Mozilla の Firefox のほうを好んで使っていたといい、警察は Firefox の閲覧履歴も解析すべきであったのに、それをしていなかった。アンソニー宅のコンピュータで Firefox 上から Google を使って検索したキーワードの中には、「確実な窒息(foolproofsuffocation)」というものがあったと報じ

[19]Ashton, *supra* note 8, 115-116.

[20]この問題について、判決後、「Net Analysis」の開発・販売元の技術者は、CacheBack のツールによる結果が誤りであることを示している。Craig Wilson, *Digital Evidence Discrepancies – Casey Anthony Trial*, http://www.digital-detective.net/digital-evidence-discrepancies-casey-anthony-trial/.

[21]State v. Anthony, *supra* note 7.

[22]§ 837.055, Fla. Stat. (2008).

[23]Anthony v. State, 108 So. 3d 1111 (Fla. Dist. Ct. App. 5th Dist. 2013).

[24]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

られており、Firefox の閲覧履歴を解析していれば、それを証拠として法廷に提出できていた可能性は高いとされた。

警察がデジタル・フォレンジックを行った際のデータの保全が不適切であり、事後検証ができない状況となっていることも判明したと報道されている[25]。

3. 日本の刑事訴訟とデジタル証拠

アメリカの議論を日本の将来においての課題への示唆として考察するために、日本の刑事訴訟における証拠能力と証明力、デジタル証拠の特殊性、日本においての事例を述べる。

3.1 日本の刑事訴訟における証拠能力と証明力

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[26]。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、の 4 点を挙げている[27]。

アメリカでは、刑事訴訟における証拠と民事訴訟における証拠に分けて議論することがほとんどないが、日本においては民事訴訟と刑事訴訟に間で証拠の取扱いに関する考え方が異なり、さらには証拠能力と証明力の間で、証拠に対する議論が異なる。

表 1　日本における刑事訴訟と民事訴訟における証拠能力及び証明力の違い

	証拠能力（証拠となる資格）	証明力（証明の程度）
民事訴訟	証拠能力に制限はなく、伝聞証拠であっても証拠として採用される。※形式的証拠力が必要[28]　※違法収集証拠に関しては議論あり	事実認定に関して、裁判官の自由な心証により主張を採用するか判断できる（民事訴訟法 247 条、自由心証主義）
刑事訴訟	事実の認定は、証拠による（刑事訴訟法 317 条、証拠裁判主義）ため、厳格な証明の対象となる事実については、証拠能力が必要になる。	証拠の証明力は、裁判官の自由な判断に委ねる（刑事訴訟法 318 条、自由心証主義）　※例外として、自白の補強法則等[29]がある。

日本においては、証拠能力と証明力という 2 つの概念があり、前者は形式的に法定され、裁判官の自由な判断を許さない（ある程度の例外として、刑訴法 326 条 1 項がある）。庭山は、証拠能力制限について、関連性に基づくもの、証明政策に基づくもの、証拠禁止に基づくものと 3 種を考えることができるとしている[30]。これらは、自然的関連性、法律的関連性、証拠禁止とも呼ばれる。

アメリカは許容性に関する事例・議論が多く、この許容性の意味としては、日本の証拠能力に当たる場合もある。ケイシー事件は、陪審員の心証の問題であるため、日本における証明力の課題といえる。

3.2 デジタル証拠の特殊性と証明力評価

デジタル証拠とは、デジタル化された文書・メール、SNS の情報、写真、録音データなど、デジタルデータによって組成される証拠をいう[31]。また、アメリカのデジタル証拠科学作業部会では、Digital Evidence のことを「デジタル形式によって保存又は伝達される証明力を有する全ての情報」[32]と定義している。

高橋らは、デジタルデータの特殊性として、原本性に関する問題、完全性・真正性に関する問題、見読性（可視性）に関連する問題があると指摘している[33]。デジタル証拠の課題として、デジタルデータは、改変が容易であり、改変しても外形上痕跡が残らないという性質がある。そのため、デジタルデータを証拠として提出するに際しては、データが作成者によって作成されたもの（真正性）であり、それがそのまま改変されていないオリジナルの状態であること（完全性）を証明しなければならない。

吉峯らは、デジタル証拠の証明力判断のためには、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、の 3 つの要素があるとしている[34]。

保全データの同一性とは、ハードディスクの複写時にハッシュ値を取ることでデータを改変していないことの証明することなど、ある時点のコンピュータの状況を固定化するために実施する保全作業のデータが常に同じ状態を示すものである。保全作業は、コンピュータの差押などの法的な証拠収集手続と密接に関連するが、これとは別に実施されることも多く、以下のようなパターンがある。

・捜索・差押の後、捜査機関において保全作業を実施
・任意提出・領置の後、捜査機関において保全作業を実施
・記録命令付差押（刑訴法 99 条の 2、218 条の 2 項）により、保全作業を行い複写したものを差し押さえる

こういった保全作業では、十分な記録を残すことが証拠確保の観点から極めて重要である。また、原本ディスクのハッシュ値は、その後の手続において証明力を確保するための起点ともなる。

解析過程の信用性とは、ⅰ抽出データが保全データに由来し、かつ、ⅱ抽出データの解釈が正確なことである。このⅰ及びⅱに関してはツールの問題に帰着することが多い。また、解析過程は、保全データの同一性が保たれている限り、何度でも再現が可能である。これは、分析の対象とな

[25]Pipitone, *supra* note 24.
[26]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）　283 頁以下
[27]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 9 月　オンライン原稿　http://www.comit.jp/BLTJ/civilpro/LS/forensic2.htm 2016 年 3 月アクセス
[28]特に文書については、署名押印がなされた私文書について真正に成立したものと推定する規定（民訴法 228 条 4 項）
[29]自白補強法則：自白だけで不利益な処分をしてはならない。自白排除法則：強制された自白は証拠として採用してはいけない。どちらも、歴史の教訓から得られたものである。
[30]庭山英雄「刑事訴訟における証拠能力に関する一問題」中京法学 1 号（1966 年）143 頁以下。
[31]高橋、梶谷、吉峯、荒木、岡、永井、デジタル証拠の法律実務 Q&A（加除出版　2015 年）P.10 以下
[32]SWGDE（Scientific Working Group on Digital Evidence）、デジタル証拠の標準と原則、
https://www.fbi.gov/about-us/lab/forensic-science-communications/fsc/april2000/swgde.htm/　2016 年 4 月アクセス
[33]高橋ら、前注 31
[34]吉峯ら、前注 31、　P.143 頁以下

る試料が限られている DNA 型鑑定などの科学的証拠と顕著に異なる特徴である。

結論間接事実の推認力とは、解析の結果直接認定できる事実であり、この事実からさらに事案との関係で証明が必要な事実（要証事実）が推認されることである。この結論間接事実の推認力には、ⅰ現実世界との接点、ⅱ複数の結論間接事実による認定、の 2 点が必要である。ⅰ現実世界との接点に関しては、利用者の意思によってデータが作成されたものであること、潜在的な利用者特定、操作した者の識別であり、基本的に通常の事実認定の問題といえる。ただし、遠隔操作プログラムのような例外もあるので注意が必要である。ⅱ複数の結論間接事実による認定に関しては、単独の結論間接事実の推認力には限界があり、別の抽出デー・間接事実の存否を検討する必要がある。

この吉峯らの証明力評価の 3 要素から、デジタル証拠の証明力について考察する。

3.3 日本のデジタル証拠に関連する事例

日本において、ケイシー事件のように本格的に解析結果自体が争点になった事例はほとんどない。しかし、解析の結果から間接事実の推認について争われたもの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事例がある。また、解析結果の説明に警察庁技官の技術者が公判出廷する事例やフロッピーティスク改ざん事件などがあり、証明力に関連する事例といえる。

3.3.1 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た事例

大阪地判平 22・5・25 は、被告人と犯人の同一性が争われている傷害被告事件において、情況証拠を検討して犯人性が肯定されたと考えるには合理的疑いが残っているとして無罪を言い渡した事例である[35]。同一性の認定にあたって、インターネット検索によって被告人が本事件について凶器の可能性のあるハンマーに限定した検索を行っ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ったが、過去の事件においてもハンマーが使用されているため[36]、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言えず合理的な疑いが残るとして、無罪を言い渡された。この事例は、インターネット検索結果以外に、被害者がすれ違った男と被告人との同一性、すれ違った男と犯人の同一性、被告人と犯人との特徴の共通点など、複数の結論間接事実の推認力について検討されている。インターネット検索結果に関しては、特に現実世界との接点について、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とされた。むしろ、被告人の犯人性を考察する上で、不当な印象を与える危険な側面があるとされた。

金沢地判平 24・3・2 は、強盗殺人、死体遺棄の事案で、被告人が犯人であるか否かが争われた事例である[37]。犯行後間もない時期の被告人のインターネット検索に被害者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、アリバイ工作があることなどの情況証拠から、被告人は、被害者を殺害するのもやむを得ないとの意思を有していたとして、強盗殺人、死体遺棄の成立が認められ、有罪となった。自宅パソコンを用いてのインターネット検索語句には、被害者が殺害され、その死体が遺棄されている場所をうかがわせるものであることなど、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された。インターネット検索結果に関して、現実世界の接点を証明しており、証明力の評価として、結論間接事実が推認されることを示している。

奈良地判平 25・3・5 は、被告人が、死体損壊・遺棄、占有離脱物横領については認め、住居侵入、強盗殺人、窃盗・同未遂の成立を否認し、結果として無期懲役が言い渡された事例である[38]。インターネット検索と行動の関連により、被告人が被害者に対し殺人等の行為を行ったことが相当程度推認されるべきであるとされた。本件において、被告人は、インターネット検索履歴の語句に関して「覚えていない」と供述している。そのため、検察側の主張により、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た。また、被告人が、自殺の理由のない被害者の死亡に関し、殺人の時効に関する検索を、被害者が死亡した数日後の時期に行っていることなどからすれば、被告人が被害者に対し、死体損壊・遺棄以外の何らかの犯罪行為、とりわけ殺人等の行為を行ったことが相当程度推認されるというべきであると推認された。この事例も、証明力の評価として、結論間接事実の推認力について検討されている。特に現実世界との接点に関して、パソコンの所有者・使用時期などについては、要証事実を推認できる程度の証明をしている。

3 つの事案に共通しているのは、証明力の評価として、結論間接事実の推認力について検討されているが、保全データの同一性及び解析過程の信用性については検討されていない。また、インターネット検索履歴などの解析の過程については検討されていない。

3.3.2 技術者が公判出廷した判例

水戸地判平 23・5・20 は準強姦被告事件について、被告人は逮捕時から一貫して犯行を否認し、弁護人は犯行日時に別の人物と別の場所に居たとして無罪を主張して争われ、結果無罪となった事例である[39]。この事例は、本件写真に係る改ざんの可能性について争われ、技術者である警察庁技官が公判に出廷し写真データの EXIF[40]についての説明を公判で行った。結果、本件写真について、その撮影日時の情報が現実に人為的に改ざんされたものであることを推認させる具体的な事情は特には認められないというべきであり、少なくとも、検察官において、その旨の立証を十分なし得ているとは到底認めることができないとされた[41]。デジタル証拠が争点の一つになった事例といえる。

3.3.3 フロッピーディスクのデータが改ざんされた事例

大阪地判平 22・9・10 は、厚生労働省の課長が、虚偽有印公文書作成・同行使被告事件について、上記団体の会長

[35]大阪地判平 22・5・25　判タ 1346 号 247 頁

[36]被告人には、平成 16 年に、遊歩道にある公園で、桜の木をハンマーでたたいていたところを通行人に注意されたことが発端となってトラブルとなり、駆けつけた警察官に対し、趣旨不明な発言をしたことから保護され、結果として国家賠償請求事件にまで発展した経験がある。

[37]金沢地判平 24・3・2　（判例集未搭載）

[38]奈良地判平 25・3・5　（判例集未搭載）

[39]水戸地判平 23・5・20　（判例集未登載搭載）

[40]JPG 形式の画像ファイルには、ファイル自体に撮影日時、位置情報などのメタデータが保存されており、EXIF 情報と言われている。これとは別に、パソコンなども、ファイル作成日時・更新日時・アクセス日時などの日時情報をファイルシステムが管理している。

[41]被告人側が提出した資料である写真データは、デジタルカメラで撮影後、パソコンに複写又は移動し、その後外付けハードディスクに保存し、それをメール添付で送付されたものであった。このデジタルカメラとパソコンは既に紛失などで存在しないため、検察官側は、写真データと後から見つかった外付けハードディスクのみで改ざんを指摘した。

等その他関係者らの各供述は、客観的証拠に反するなどして信用できず、共謀は認められないとして、被告人を無罪とした事例である[42]。本件において、5 人の公判供述あるいは検察官調書には、フロッピーに保存されたデータや手帳、名刺その他の客観的証拠や証拠上明らかに認められる事実にそれぞれ符合しない点があり、それらの供述がいかに相互に符合しているとしても、信用性を高め合うものとはいえず、全体としてみても、十分な信用性があると認定することはできないとされた。

この事例は、村木さん裁判や厚労省事件とも言われており、検察官によるファイルの日付の改ざんを弁護側がデジタル・フォレンジックによって証明し、最終的に無罪を勝ち取ったという経緯があり、デジタル・フォレンジックが審理の上で効果を発揮した[43]。

その後の大阪地平 23・4・12 は、現職の検察官であった被告人が、主任として担当した事件の証拠であるフロッピーディスクに保存されていた文書のファイルの最終更新日時等を、検察官に有利な方向に改変したという証拠隠滅の事案について、懲役 1 年 6 月の実刑が言い渡された事例である[44]。前記、厚労省事件に関してデジタル証拠の改ざんを、デジタル・フォレンジックによって証明した。

解析過程の信用性について議論するときに、デジタルデータは改変が容易であるため、真正性が重要であることがこの事例からもわかる。

4. 考察

4.1 日本とアメリカの訴訟内容比較

2.2 及び 3.3.1～3 の事例である、被告人と犯人との同一性が争われた事例について、インターネット検索履歴が検討されたため、事例を表にまとめた。

表 2　日本とアメリカの事例比較

事例	デジタル証拠の課題	結果	証拠評価
ケイシー事件	解析結果の相違、ツールの信頼性	殺人罪については無罪評決	解析結果の信用性、間接事実の推認力ともに低い
平 22 大阪	なし	無罪	間接事実の推認力が低い、逆に不当な印象
平 24 金沢	なし	有罪	間接事実の推認力が高い
平 25 奈良	なし	有罪	間接事実の推認力が高い

4 つの事例を比較した結果、ケイシー事件のみ、デジタル証拠の課題が見えていること、解析結果の信用性についても争点となっていることがわかる。

ケイシー事件は、解析の手法や使用したツール名なども公表されており、解析結果に対しても争点になっている。それに対して、日本の事例は、結論間接事実の推認力について争われることは多いが、解析過程の信用性について争われることは少ないといえる。

4.2 ケイシー事件を手がかりにした証拠評価

ケイシー事件の検討結果をうけて、デジタル・フォレンジックの観点から見た証拠評価の課題を、証明力評価の 3 要素である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の 3 つの側面に即して分析する。

①保全データの同一性

データ保全が不適切であり、第三者による検証ができなく、評価できないことが課題である。

事後の報道により指摘されているデータ保全の不適切さであるが、カービングした Mork データベースだけは保全できていたようである。しかし、それ以外のデータ保全が不適切なことにより、デジタル証拠の特徴である第三者検証性がない。第三者検証性とは、「電磁的記録の解析に従事した者以外の解析担当者又は第三者が、正当な手続の下で、かつ正しい手順で、解析対象の電磁的記録について解析を行った場合には、同一の解析結果が再現可能であること」[45]とされている。

②解析過程の信用性

本件では、2 つのツールを用いた解析過程について争点になっている。検察官側の供述が誘導するかのように誤っていたことも問題ではあるが、特に、ツールによる解析結果の相違が陪審に与えた影響は大きいといえる。

次に、解析の中身について検討する。解析過程に、InternetExplorer が出てきたこと、使用されていたツールである NetAnalysis は Windows OS ベースのものであることから、解析対象パソコンの OS は Windows であると判明する。解析者は、未使用領域からカービングにより Mork データベースを復元している[46]。そして、復元したデータベースからインターネット検索履歴を抽出し、可視化しているが、2 つのツールでの解析結果が異なった。判決後、今回使用されたツールの開発元が、ツールによる解析結果の相違に関するレポートを公開している。

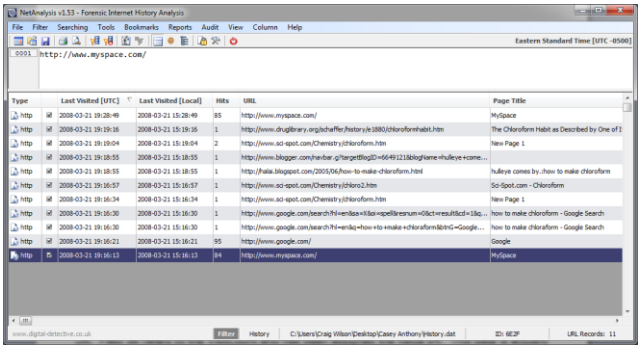

図 1　判決後のツール検証結果[47]

[42]大阪地判平 22・9・10　（判例集未登載）
[43]鈴木一郎　「デジタルデータ分析　厚労省事件　」季刊刑事弁護 No.71 号　（2012 年 7 月　）60 頁以下
[44]大阪地平 23・4・12　（判例集未登載）
[45]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）24 頁以下
[46]Windows OS の場合、データ復元を行う一般的な方法は、$MFT と $Bitmap の管理テーブルから復元する方法と、ヘッダー・フッター・データ構造などのデータが持つ特徴的な痕跡をとらえて復元するデータカービングの 2 つである。
[47]Craig Wilson 、前注 20

図 1 は、開発ツールである NetAnalysis を開発した会社が判決後に出したレポートで取り上げられた、ツール検証結果のスクリーンショットである。このレポートでは、クロロフォルムの検索回数が、ツールによって異なっていたことの詳細を技術的に説明しており、専門家証言においての誤りなどを指摘している。これは、判決後において 2 つのツールの検証や、データベースの分析が可能であったものであり、解析時に時間・人・予算の制限があるとき、その場で正確な解析結果を得ることが難しいケースが存在することがわかる。こういったパソコンのインターネット検索履歴の復元などの項目について、常に完全なツールは存在しないといえる。解析過程の信用性についてはツールに依存している部分が多いため、この点はデジタル証拠の大きな課題である。

③結論間接事実の推認力

解析過程の信用性、捜索・差押のデジタル証拠に対する対応などから、結論間接事実を推認するにあたり、陪審員の心証を形成できなかった。

クロロフォルムの物証とインターネット検索履歴について、ケイシーのみがパソコンを使用したことは、現実世界との接点があり 1 つの結論間接事実として推認できるであろう。しかし、インターネット検索履歴の解析結果に関しては、解析に関する単独の結論間接事実の限界ともいえる。そのため、解析に関する複数の結論間接事実による認定が必要になるだろう。

4.3 デジタル証拠の課題と対策

この事例からわかるデジタル証拠の課題は 3 点ある。

4.3.1 完全な解析ツールは存在しない

解析を行う際、時間・人・予算の制限があるため、常にすべてを解析可能な完全なツールは存在しない。これは、ツールにより解析結果が異なったため、証明力においての課題となる。

ケイシー事件は、ツールに依存してしまったため解析者などの専門性が不足していた点が課題としてある。しかし、すべての解析者などが、解析に関する全ての知識と経験を有することは大変困難であり、多くは自動化したツールによって対処しているのが現状である。例えば、アメリカ司法省のレポートでは、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、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などの、デジタル・フォレンジックの課題を 30 項目挙げている。しかし、そのうちの半分はツールを開発・使用することで対処することを示している[48]。

4.3.2 解析者などに専門性が求められる

いくつかのボタンを押すだけで解析が可能な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が課題である。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、それを公判において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。

この事例において、解析過程の信用性のためには、他の結論間接事実による認定を求めるべきである。本件の解析において、Mork データベースだけに依存して解析を行うこと自体が不適切でもある場合もある。証拠評価の観点から見るときに、単独の結論間接事実の推認力には限界があることを述べたが、本件においても他の解析結果との存否を検討すること、他の解析結果から結論間接事実の推認力を高めることが求められる。ケイシー事件の場合、インターネット検索履歴の解析結果が課題の 1 つになっているが、検索履歴に該当、または類似項目として、ジャンプリストの解析、キャッシュの解析などが挙げられる。また、他の解析手法として、VSS（Volume Shadow Copy Service）[49]などを利用することや、メモリフォレンジック[50]、Firewall ログの利用などがある。

4.4 デジタル証拠に対する解析者などに求められるもの

この事例において、完全なツールは存在しないことがわかった。そのため、自動化したツールを使用する解析者などは、ツールの限界・エラー、ツールのリスクの 2 点を理解し、常に最新の情報・知見を収集するべきである。

4.4.1 ツールの限界・エラー

ツールを適切に使用しても、エラー（例外的な状態）・バグ（不具合）が起こる可能性もある。また、検証してあるツールであっても、エラー・バグが起こる場合がある。最も多いのは、ハードウェアやソフトウェアのバージョンアップによるエラーであるが、それ以外にも、件数や容量の多い DB やファイル（例えば、10 万件の履歴や、3 万件の画像処理など）を解析するとエラーが生じることがある。他にも、検証時には使用していなかった機能などが使用されることで、ツールの作動中にエラーで止まることもある。

また、ツールで全ての収集・保全・解析ができるわけではなく、ツールには限界がある。そ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[51]。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。

4.4.2 ツールのリスク

技術的に完全なツールは存在しないため、現在解析した結果が全てではない場合がある。ツールを過大評価、ツールに依存しすぎると、この事例のように証拠の見落としが生じる可能性がある。

[48]Goodison, *supra* note 1, at 22-24.

[49]Windows Vista 以降のバックアップ機能であり、誤って削除したデータの復元などにも活用可能である。Windows Vista は 2006 年に販売されたため、事件当時（2008 年）のパソコンは、OS が Vista の可能性があり、VSS の機能を使用できた可能性がある。

[50]RAM のデータを解析するメモリフォレンジックについては、捜索・差押時の現場でのみ保全可能なデータであるが、ハードディスク内にも pagefile.sys などのメモリデータが存在する。当該データに関しては捜索・差押時でなくともハードディスクやイメージファイルがあれば解析可能である。

[51]暗号解読が困難な場合でも、Pass-the-hash 攻撃など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。

さらに注意が必要な点として、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。例えば、ある特定のスマートフォンを解析する際に、ある特定のツールを使用すると、証拠物であるスマートフォンのデータが消去・改変される。こういった誤った使い方などをしないためにもツールのリスクを認識する必要がある。

4.5 その他のデジタル証拠の法的課題

日本におけ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ことを述べたが、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残存し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 を解析対象としておらず論理的同一性はない場合が多い[52]。また、湯淺から指摘されている海外ツールへの依存[53]、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[54]の使用の是非、リモートストレージにおけるデータ収集の課題などがある。

5. 結論

今回､デジタル証拠の課題と証拠評価について考察した。ケイシー事件などを手がかりにした結果、デジタル証拠の課題として、データを解析する完全なツールは存在しないこと、解析者などに専門性が求められること、その他法的課題があることを指摘した。

また、日本の事例では、結論間接事実について争われる判例が多い反面、解析過程の信用性などについては検討される事例は少なかった。解析過程の信用性は、ツールに依存しているとの指摘もある。しかし、完全なツールは存在しないため、解析過程の信用性の問題は日本においても同様の課題であるといえる。

ケイシー事件を手がかりにした、デジタル証拠の証拠評価向上のためには、

・データ保全が重要であること

・解析過程の信用性のために、一つの結論間接事実で推認力がない場合は、複数の結論間接事実を使用すること

が重要であることを指摘した。

また、自動化したツールを使用する解析者などは、ツールの限界・エラーやツールのリスクなどを理解し、常に最新の情報・知見を収集することを提案したい。これらによって、公判審理における証明力を高めることが可能となると考えられる。

[52]前田恭幸　SSD の Over Provisioned Capacity からのデータ抽出手法 CSEC　2015 年 12 月

[53]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。http://janet.jw.jiji.com/apps2/do/contents/view/142c97d93639c5bf1f187498f5437ae3/20160224/322/viewtemplate1/jncolumn005　2016 年 3 月アクセス

[54]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。