刑事手続におけるデジタル証拠の改ざん防止措置について

小坂谷聡 [1]　　上原哲太郎 [†1]

概要：個人の活動の痕跡として各種デジタルデバイスに記録されているデジタルデータは，裁判実務においてデジタル証拠として扱われる場面が増加している．しかし，デジタル証拠は，その性質上改ざんが可能かつ容易であるという特性を持つ．そのため，デジタル証拠が適切に利用されるためには，改ざんされていないことを客観的に確認できる仕組みが重要である．本研究では，デジタル証拠の改ざんが後から問われる例を減ずるべく，改ざん防止を客観的に確認するための具体的なシステム構築を提案する．

Anti-Tampering System for e-Evidence on Criminal Procedure

SATOSHI KOSAKATANI[1]　　TETSUTARO UEHARA [†1]

1. はじめに

個人の活動の痕跡としてパーソナルコンピュータ（以下，「PC」という.），デジタルカメラ，IC レコーダ，携帯電話などの各種デジタルデバイスに記録されるデジタルデータが裁判実務においても，民事事件・刑事事件を問わずデジタル証拠が扱われる場面が増えている．図 1 は，判例検索[a] を用いて，刑事裁判（児童ポルノ，公然わいせつ，リベンジポルノを除く.）に限定した上，4 つのデジタル機器 [b] の用語を含む条件で検索した結果を 3 年単位でグラフ化したものであるが，このグラフからもデジタルが扱われる裁判例が全体として増加傾向にあることが窺える．

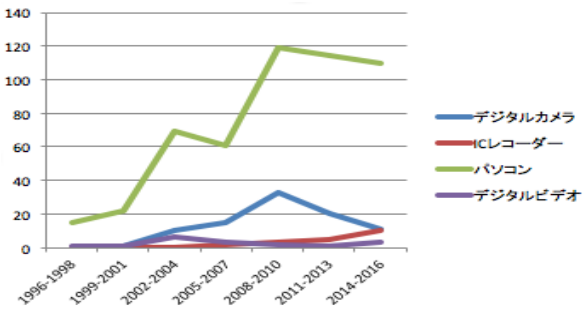


図 1 デジタル機器を示す語が判例文中に含まれる刑事裁判の年代別傾向

デジタル証拠は，機械的に記録されたデジタルデータを解析することによって得られる客観的・科学的証拠の一つとして，曖昧あるいは主観的な人の記憶に基づいた供述証拠に比べ，それ自体高い信頼性が認められている．特に，自白偏重の弊害が指摘されて久しい刑事裁判においては，今後もますます重要な役割を果たしていくと期待されている．

しかしながら，デジタル証拠は一般に改ざんが可能かつ容易であるという特性が認められる．その上，デジタル証拠が一旦改ざん等された場合，信頼性が大きいが故に，誤判の危険性は増大しその弊害も甚大である．他方，従前は，デジタル証拠の真正性が裁判において争点となった場合でも，特に刑事裁判においては，警察・検察が偽造するなどあり得ないという捜査機関に対する信頼感に依拠する判断がなされていたかもしれないが，厚労省 FD 改ざん事件（前田元検事事件）などがあり，今後は組織の信頼性のみに依拠することは難しくなるとも指摘されている[c].

この問題の解決のために，デジタル証拠が改ざんされていないことを客観的に確認できるシステムや制度が必要と考えられる．そこで本研究では，デジタルデータの改ざんの容易さについて実験し，また，デジタル証拠が裁判実務においてどのように扱われているかを概観した上で，改ざん防止の観点から，デジタル証拠が改ざんされていないことを客観的に確認できる具体的なシステム構築の方策等について考察した．

2. デジタル証拠の改ざん容易性の検証

2.1 改ざん容易性の予備調査

まず予備調査として，デジタル証拠となりうるようなデータの改ざんが一般的な PC の利用者にとってどの程度容易であるかを確かめるため，観察実験を実施した．

2.1.1 実験の被験者

被験者には，日常的に仕事上書類作成等の事務仕事でＰＣを使用しているが，画像加工や情報分野の専門的知識を有していない被験者として，弁護士４名，司法書士１名を選

1 立命館大学大学院情報理工学研究科博士後期課程，弁護士
†1 立命館大学情報理工学部

[a] 判例秘書 INTERNET によって，2017 年 2 月 27 日に検索した．
[b] ①「デジタルカメラ」(「デジカメを含む.」)，②「IC レコーダー」，③「パソコン」(「パーソナルコンピュータ」，「PC」を含む.)，④「デジタルビデオ」４つの機器について検索した．なお，デジタルカメラの件数が減少傾向にあるが，近年，スマートフォンの台頭によって，使用頻度自体が減少していることを反映していると考えられる．
[c] 吉峯耕平他「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 122 頁（2014）．

Copyright (c) 2017 by the Information Processing Society of Japan

んだ．被験者はいずれもデジタル証拠の改ざんについての予備知識は有さない．

表 1 被験者の属性

	年齢(代)	性別	職業	PC 使用歴	主な使用目的	主な使用ソフト
A	30 代後半	女	弁護士	15 年	仕事	ワープロ，表計算，メーラー，ブラウザ
B	30 代前半	女	弁護士	24 年	仕事	ワープロ，表計算，メーラー，ブラウザ
C	30 代後半	女	弁護士	20 年	仕事	ワープロ，表計算，メーラー，ブラウザ
D	30 代後半	男	弁護士	20 年	仕事	ワープロ，表計算，メーラー，ブラウザ
E	30 代前半	男	司法書士	15 年	仕事	ワープロ，表計算，メーラー，ブラウザ

2.1.2 実験環境

実験環境は以下を選んだ．

PC：Windows10 がプリインストールされたノート型 PC

インストール済みソフトウェア：

Adobe Photoshop CC 2015
Adobe Acrobat Pro DC
Adobe Acrobat Reader DC
Microsoft Word 2016
F6 Exif[d]

全てのソフトウェアはショートカットをデスクトップに置いており，インストールされていることにはすぐ気づくようにしてある．

2.1.3 実験課題

実験にあたっては，以下の 3 つの課題を用意し被験者にその作業を行わせるものとした．

実験 1　被験者に写真 1（jpg ファイル），およびその中央に写っている人物を消去した写真 2（例）を示し，そのように編集することを依頼する．

実験 2　被験者に上記写真の Exif 情報（撮影日，撮影場所）を変更することを依頼する．

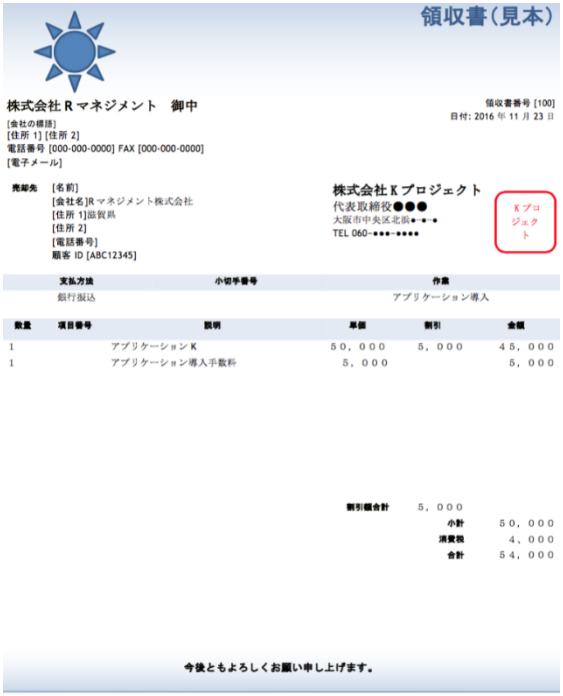
実験 3　被験者に領収書を模した PDF ファイル（図 2）の金額欄など記載内容の変更を依頼する．

実際の改ざんは，実験 1 については Photoshop の持つ「コンテンツに応じた塗り」機能，実験 2 については F6Exif の持つ機能，実験 3 については Word による PDF の読み込みと編集，書き出し，または Acrobat Pro による編集で行うことができるが，その手法自体は被験者には伝えず，インターネット検索などを通じて手法を自ら発見し，実際に作業が行えるかどうかを観察した．

写真 1

写真 2

図 2



d フリーソフトウェアとして http://www.ryouto.jp/f6exif/viewer01.html にて配付されている．Exif 編集ソフトウェアとして Google 検索の結果が最上位であるため，これを選んだ．

Copyright (c) 2017 by the Information Processing Society of Japan

2.1.4 実験手順

実験の手順は以下の通りである．

1. 実験環境として用意した PC 前に被験者を座らせ，PC が利用できることを確認させた上で，実験開始とともに実験１～３の課題を記述した文書を手渡す．
2. 制限時間として３０分以内に課題を行わせる．その間，インターネット検索は自由に行って良く，また使用するソフトウェアや方法については自由ということを示す．インストール済みのソフトウェア以外を使用することも自由だが，但し，インストール済みのソフトウェアだけでこれらの作業が可能であることは告知済みである．
3. この作業の様子を記録し，与えられた課題を実行する方法にいつ辿り着き，実際に作業を行えるかを観察する．作業の後には自由記述でアンケートを取る．

2.2 実験結果

実験の結果は以下の表１から表３の通りである．

なお，各実験については６つの評価ポイント（step1~step6）を設け，各 step ごとに達成度に応じて３段階で評価した．

【Step】

step1　課題の意味を理解する．
step2　インターネットで検索する際に，適切なキーワードを利用できる．
step3　想定していた対応可能なソフトウェアに辿り着く．
step4　上記ソフトウェアが PC 内にあることを発見する．
step5　対応可能なソフトウェアの適切な機能を見つけることができる．
step6　適切な機能を用いて，実際に課題を解決できる．

【評価】

○　：達成
△　：不十分ではあるが何らかの方法で部分的に処理した
×　：未達成
□　：想定と異なる方法をとるなどしたので未評価

表２　実験１の結果

	1	2	3	4	5	6	時間(分)	不成功の原因に繋がった行動
A	○	○	○	○	×	×		jpg ファイルが Photoshop に関連付けられておらず，ファイルの開き方が分からなかった
B	○	○	○	○	○	○	16	
C	○	○	□	×	□	□	(15)	標準ソフト（ペイント）のコピー＆ペースト機能で改ざんを行った．
D	○	○	○	○	×	×		Photoshop 内での適切な機能を発見出来なかった
E	○	○	○	○	○	○	7.5	

達成者の平均所要時間：　約１１分半

表３　実験２の結果

	1	2	3	4	5	6	時間(分)	不成功の原因に繋がった行動
A	○	○	×	×	×	×		Explorer におけるプロパティ表示に気を取られ，編集方法に気づけなかった．
B	○	○	○	○	×	×		F6Exif の操作方法が分からなかった
C	○	○	○	×	×	×		時間切れ
D	○	○	○	○	○	○	6	
E	○	○	○	□	□	□	(9)	Explorer のプロパティ機能から全て編集できると思い込み，その対応にこだわったため Exif 編集ソフトウェアの存在に気づくのが遅れた．

達成者の平均所要時間：　約６分

表４　実験３の結果

	1	2	3	4	5	6	時間(分)	不成功の原因に繋がった行動
A	○	○	○	○	×	□		アクロバットの使用方法が分からなかった
B	○	○	○	○	○	○	3.5	
C	○	○	○	○	○	○	12.5	
D	○	○	○	○	○	○	3	
E	○	○	○	○	○	○	7	

達成者の平均所要時間：　約６分半

表５　実験終了後のアンケート内容（自由記載）

A	方法については全然知らなかった 思っていたよりは少し正解に近づきそうになった気がした もう少し時間があれば何とかなったかもしれない 躍起になりすぎた もう少し柔軟に色々試せばよかった
B	画像消去と PDF ファイル編集はやったことはあったが，別のアプリなどでしたことがあった記憶がぼんやりあるだけ いざ方法を問われると明確に思い出せず，すべて Web で調べながらやった Exif 情報の改変は初めてやった 時間制限ありで難しかった できると面白くてはまりそうになった
C	写真ファイルの人物消去は時間をかけてもっと綺麗に消去したかった 時間があれば，インターネットで検索して調べれば大抵のことはできそうだと思った
D	方法については知らなかった デジタルデータの改ざんが思いの外簡単にできることを実際にやってみて理解できた
E	写真の人物を簡単に消せたことについてはビックリした やり方についてはほぼ知らなかった ネットで検索すれば意外と簡単にすぐに方法が出てくることにも驚いた

Copyright (c) 2017 by the Information Processing Society of Japan

2.3　考察

今回の実験では，PDF の編集を経験したことがある者が１名（B）いた．他は，実験１ないし３の全てについて事前に経験していた被験者はおらず，最終的にすべての実験課題を完成（step6）させた者はいなかった．もっとも，もう少し時間があればある程度は出来そうだと思ったという趣旨の感想を述べた被験者が３名（A，B，C）いた．いずれの被験者も日常的に業務で PC を使用し，PC の扱いについては十分慣れていたため，課題の意味を理解し（step1），検索エンジンを利用し方法等を検索すること（step2）については全く問題なかった．しかしながら，日常的な PC の使用方法については，全員が業務における事務作業に使用しており，趣味等で画像編集等を行っている者がいなかったことからも分かるように，各自不慣れな作業であったということに加え，制限時間の短さが影響したため，このような結果となったと考えられる．

実験別にみると，実験３（PDF ファイルの編集）の成功率が最も高く，４名（B，C，D，E）が成功した．これは，被験者の間でも PDF ファイルは馴染みがあり，Adobe Acrobat の編集機能についても認知されていたことによると考えられる．ただ１名成功しなかった A については，一旦は Adobe Acrobat の存在に気付いて立ち上げるまでに至ったものの当該ファイルを同ソフトで開くという使用方法が分からず，結局，当該ファイルをダブルクリックで開いてしまい（当該環境では PDF ファイルをダブルクリックすると AcrobatReader が起動し開くようになっていた.），そのまま同ソフトでの編集にこだわってしまったためと思われる．なお，A については，実験１及び２においても達成出来なかったが，ファイルを開く際，ダブルクリックで開いては閉じるという行動を繰り返しており，アプリケーションから開く方法について不知あるいは不慣れであることが伺えた．

これに対して，成功率が最も低かったのが実験２（Exif の編集）で，最終的に成功した者は１名（D）だけであった．F6 Exif のサイトを発見しながら，既に PC にインストールされていたことに気付かなかった者が２名（C，E），インストールされていたことに気付きながら操作の方法が分からず完成できなかった者が１名（B）いた．実験２は編集作業にはいわゆるフリーウェアを利用することが求められていたが，主に仕事上の事務作業でしか PC を使用しない層にとっては，フリーウェアの使用に馴染みがなく障害になったと推察される．なお，実験２については，全員がプロパティによって Exif 情報が読み取れることには比較的早い段階で確認することができ，うち１名（E）がプロパティの操作によってファイルのタイムスタンプの編集までは出来た．しかし，それが却ってプロパティを操作すれば全て達成出来るという誤解を助長して結果的に無駄に時間を掛けすぎてしまい時間不足を招いたと推測される．

最後に，実験１（写真上の人物の消去）については，Adobe Photoshop の標準機能を使用し完成させた者が２名（B，E），Windows 標準のペイントソフトのコピー&ペーストを利用して類似の編集を行った者が１名（B）という結果だった．残り２名（A，D）については，Adobe Photoshop の存在には気付いたものの，A はそもそも Adobe Photoshop で当該ファイルを開くことが出来ず，D は，Adobe Photoshop で当該ファイルを開くことは出来たが，機能の使用方法が分からなかった．制限時間の制約内でソフトの機能に気付き，実際に色々と試行したか否かが結果を分けたと考えられる．

今回の実験は，過去に一度でも同様の作業経験があれば容易に完成できる作業について，知識・経験がない場合にどの程度行えるかということを確認する目的で実施したものである．実験の結果からは，課題がいずれも被験者にとって未経験であるため試行錯誤が行われたが，その課程において情報科学的な知識の欠如により作業が困難になる様子が窺えた．特に，Exif 情報の改ざん作業は，写真や PDF の加工といった外見的な作業とは異なり，ファイルの内部情報に関する作業であって，情報科学の基礎知識を有しない被験者にとってはその意味を理解することが困難であったようである．また作業の観察においては，制限時間という制約や自身の作業内容が観察されるという実験環境内での緊張から作業が困難になったと思われる行動や言動も見られた．全ての被験者が実験後，デジタルデータの改ざんが簡単に出来るということを実感したとアンケートなどで述べており，そのことを理解した後，実験のように時間制約がなく観察による緊張もない状況ではより簡単にデジタルデータの改ざん作業が行えるようになったのではないかと考えられる．デジタルデータの改ざんや編集については，容易に実行出来る多くの定番ソフトウェアが有償無償を問わず存在し，それらの使用方法等や改ざんの方法を解説・説明するウェブサイトも多く存在する．少なくとも，今回の実験を通じて，動機付けさえあれば，容易にそれらの情報にアクセス可能であることも明らかになった．

これらのことから，デジタル証拠の改ざんが一般的 PC 利用者にとっても，事例さえ示されれば事前知識なく行える場合が少なからずあることが明らかになったと考えられる．

3.　刑事裁判においてデジタル証拠の真正性・完全性が問題となった事例と考察

3.1　真正性等以外の事例

デジタルデータの解析結果の意義が問題となった事例としては，改ざんそのものが争点となった訳ではないが，いわゆる厚労省フロッピーディスク改ざん事件として知られる一連の事例[e]がまずあげられる．この事件は，捜査主任の検察官によって証拠資料であるフロッピーディスクのファイルシステム上のメタデータ（最終保存日時）が改ざんされたという事例である．主任検事は，当該フロッピーディスクを改ざんした後，これを作成者の弁護人に返還したが，返還を受けた弁護人が日時等の記録されたプロパティ情報に不審を抱いたことから，専門業者によるデジタル・フォレンジック調査を依頼した．その結果，文書ファイルデータに記録されたメタデータとの矛盾が判明し改ざんの事実が発覚したというものである[f].

[e] 大阪地判平成２２年９月１０日判タ 1397 号 309 頁，大阪地判平成２４年１月 23 日判タ 1404 号 373 頁，大阪地判平成２３年４月 12 日判タ 1398 号 347 頁，大阪高判平成２５年９月２５日判タ 1408 号 293 号他.

[f] 鈴木一朗他「デジタルデータ（フロッピーディスク）分析　厚労省事件」季刊刑事弁護 71 号 60 頁（2012），高橋郁夫他「デジタル証拠の法律実務Ｑ＆Ａ」（日本加除出版株式会社 2015）284 頁

Copyright (c) 2017 by the Information Processing Society of Japan

また，４名の PC からそれぞれウェブサイトへの書き込みを通じて実行された各殺人予告事件等が，後に，一人の人物による PC の遠隔捜査等によって実行されたことが発覚した PC 遠隔捜査事件[g]が有名である．この事件では，遠隔捜査を実行した被告人も，当初は自分の PC も遠隔捜査されたとして無罪を主張しており（最終的には公判中に自白するに至っているが.），被告人が職場で利用していた PC のハードディスクに残った遠隔捜査ウィルスの痕跡の解析結果が争点となっていた[h]．これも改ざんの有無自体が争点となっていた訳ではないが，ハードディスク上に残されたデジタルデータの解析結果の重要性が指摘された事案である．

この他にも，いわゆる電磁的記録不正作出罪や児童ポルノ関係などデジタルデータを直接対象とする犯罪以外の一般的な犯罪において，被告人の犯人性が争点となった事例で，デジタルデータの解析結果等のデジタル証拠が事実認定のための間接証拠の一つとしてその推認力が問題となった事案についてもいくつか散見される[i]．もっとも，これらの事案についてもいずれもデータ自体の真正性等が争われたわけではない．

3.2 真正性・完全性（改ざん）が問題となった事例

⑴ 東京地判平成１７年３月２５日（ACCS 事件）[j]

検察官が提出したサーバのアクセスログ（履歴）について，その改ざんが弁護人によって争われた事例である．この事例では，裁判所は，アクセスログの記録が第三者によって不正に作出された「可能性をうかがわせる具体的な事情は何ら存在しない上，第三者が被告人のアクセス記録をことさらに作出する必要性もないことから，アクセスログは正確に被告人のアクセスを記録していると認められる.」と判断した．

⑵ さいたま地判平成２１年７月２８日[k]

被告人と共犯者間の PC ないし携帯メールの送受信に関して，共犯者が特殊なソフトウェアを使ってメールのヘッダ情報を書き換え，成り済ましメールを作成した事実があるとして被告人によって争われた事例である．しかし，裁判所は,「メールのヘッダー情報の書き換えが技術的に可能であるとしても」，共犯者において，「被告人との間のメールの送受信をわざわざ偽装する理由も必要性も見当たらない」として，被告人の主張を退けた．

⑶ 高松高判平成２４年４月２６日[l]

被告人が自らの主張を根拠付ける証拠として提出した IC レコーダに記録されたデジタル音声データについてその改ざんの有無が争われた事案である．これに対して，裁判所は，デジタルデータは痕跡を残さずに加除訂正することが容易であるとし，最終的に，やり取りの中には相当不自然な部分もあることを理由に，元の音声データに対し加除訂正が加えられたものであると認定した．

⑷ 水戸地判平成２３年５月２０日[m]

上記の事例に対して，これは，被告人から提出された写真データが保存されたハードディスクに関して，写真データの EXIF 情報が改ざんされた痕跡は特に見当たらないとする捜査機関が実施した鑑定が存在するにもかかわらず，検察官がその改ざんの可能性の有無を争った事例である．しかし，裁判所は，当該写真に記録された撮影日時の情報について，人為的に改ざんが行われたことを推認させる具体的事情は特に認められないと判断し，検察官の主張を退けた．この事例では，裁判所は，一般論として EXIF 情報を編集することは編集ソフト等を使用すれば比較的容易であることを認めながらも，当該事案においては，実際にかかる編集ソフト等が使用された形跡が明らかにされた事実がないことを指摘している．

3.3 考察

個人の活動履歴としてデジタルデータがパーソナルコンピュータ，デジタルカメラ，IC レコーダ，携帯電話などの各種デジタルデバイスに記録される機会が量的にも割合的にも多くなるにつれ，そのデジタルデータが，犯罪立証あるいは犯人性立証のための重要な間接事実となることは当然の帰結である．インターネットの検索履歴やパーソナルコンピュータの操作履歴（ログ）等が裁判例に度々登場するようになってきていることはその証左である．但し，これらのデジタルデータが犯罪性ないし犯人性立証の証拠となりうるのは,もとより真正性が認められてのことである．そうすると，デジタル証拠の真正性が争点となる事例も，我々が調査した限り現時点では多くなかったが，今後は増加するものと考えられる．

ここで，何故これまでデジタル証拠の改ざんが争点とされることが多くはなかったのかについて考察する．

従来，デジタルデータが裁判で証拠として申請ないし採用される際には，紙等の媒体に再現（印刷）された形で，あるいは印刷物等と合わせて提出されることが多かったと思われる．その場合，原本データと照らし合わせ正確に再現（印刷）されているか否の確認が重要であることは当然の前提となっているものの，当該原本データの真正性自体にまで踏み込んで検証されることは少なかったと考えられる[n]．

この点，これまでの裁判実務においては，デジタルデータに関する証拠を提出する法曹等に対する一定の信頼が暗黙の共通認識となっていたという指摘もなされているが[o]，その信頼には，デジタルデータ自体に対する信頼もあったと考えられる．つまり，デジタルデータは改変しやすい性質であるということを一般的な知識としては理解しつつも，それを現実的な問題としては十分に捉えられていない意識があると考えられる．実際，ACCS 事件においても，現に，

---

[g] 東京地判平成２７年２月４日（判例集未搭載）

[h] 前掲高橋他 298 頁以下.

[i] 例えば，大阪地判平成２２年５月２５日判タ 1346 号 247 頁は，事件の凶器に関連する「ハンマー」という単語が検索されたという間接事実の推認力だけでは犯人性の立証には不十分であると判断された．また，金沢地判平成２４年３月２日（LEX/DB 25480441）や奈良地判平成２５年３月５日（LLI/DB 判例秘書 L06850138）などは，検索ログを間接事実の一つとして犯人性を推定している．

[j] 東京地判平成１７年３月２５日判タ 1213 号 314 頁（ACCS 事件）

[k] さいたま地判平成２１年７月２８日（LLI/DB 判例秘書 L06450468）

[l] 判例集未搭載.

[m] 水戸地裁土浦支部判決平成２３年５月２０日（LLI/DB 判例秘書 L06650285）

[n] この点，前掲高橋他 272 頁では，特に供述証拠についてではあるが，伝聞法則が厳しい要件を課していることから，従来，真正性が問題になることは少なかったに過ぎないが，デジタルデータの改変可能性を考慮すると，今後は真正性についての議論がより必要になってくる旨指摘されている．

[o] 前掲吉峯他 122 頁（2014）.

Copyright (c) 2017 by the Information Processing Society of Japan

改ざんの主張が認められるためにはその可能性を疑わせる具体的な事情が必要であるとされており，抽象的に改変・改ざんの疑念が主張されたに過ぎない場合では，たとえデジタルデータが改変可能だからといっても証拠能力や証明力を否定するという判断がなされることは，少なくとも従前の考え方からすれば考え難いということになろう[p].

しかし，先の実験結果においても明らかになったように，デジタルデータの改ざんは，現実問題としても，今や限られた専門家による高度な知識・技術がなければ不可能であるという状況ではない．専門的知識・技術のない素人であっても，デジタルデータの改ざん・改変を行うための情報やそれを可能にするツール等の環境はインターネット上に溢れており，少しの時間の間にその手法にまで簡単にたどり着けることが先の実験結果で示された．このことは，捜査機関においても同じであって，専門的組織的対応のみならず，一捜査官の個人的対応によっても容易にデジタル証拠の改ざんは実行されうる状況にあると考えられる．従って，証拠の収集保全段階において，仮に必要な改ざん防止の措置が取られていなければ，収集されたデジタル証拠は常に改ざんされた可能性が残ると見るべきである[q]. デジタル証拠に関する必要な改変防止の措置がとられていない場合，相手方に開示されるまでの間改変する十分な機会があり，かつ改変・改ざんについても極めて容易であることは否定出来ないため，既に改ざん行為の類型的な危険が認められる状況にあると考えられる[r]．従って，デジタル証拠の収集過程にはこのような危険が存在する現状を鑑み，その危険が現実化することを防止するためのシステムを構築することが必要かつ重要となる．そこで，次章では，捜査機関がデジタル証拠の任意提出を受けた際，あるいは押収した際に，客観的に真正性を担保することが出来，かつ弁護人からも容易かつ安全に改ざんの有無を確認出来るシステムの構築を検討する．

4. 改ざん防止の具体策

4.1 改ざん防止の前提

捜査機関がデジタルデータを証拠として収集・保全する際，保全されたデータが改ざんされることを防止するために必要な防止策としては，オリジナル媒体のデジタルデータと同一であることをハッシュ値によって確認することが最も効果的である[s]．捜査機関等がハッシュ値を確実な手段で証拠化しておき，保全データのハッシュ値と照合することによって，保全データの同一性あるいは改ざんの有無を確認することができる[t]．従って，弁護人としては，捜査機関が捜索押収したデジタル証拠に関して，ハッシュ値が記録されているかどうかを確認し，仮にこれが同一でなかった場合には，提出されたデジタル証拠の証拠能力や証明力を争えばよいことになる[u].

しかし，問題はそのハッシュ値の確認手段ないし方法である．保全の際にハッシュ値を記録することが改ざん防止のために効果的であり，ハッシュ値を記録することが推奨されていたとしても，ハッシュ値を記録・確認するための客観的かつ統一的なシステムが確立している状況にはなく，捜査機関の運用に委ねられているのが現状である．しかし，そもそも改ざんに関しての疑義が問題となっている場面で，捜査機関の運用に依存する状況は望ましいとは言えない．また，我が国の捜査機関では，ハッシュ値を捜査書類に記録すること自体に消極的であるという指摘も存在する[v].

そこで，捜査機関による恣意的な運用に頼ることなく，被告人・弁護人側にとっても納得出来る客観的な防止システム（ハッシュ値登録システム）の構築が求められる．

4.2 ハッシュ値登録システムの提案

4.2.1 システムの概要

１　アップロードシステム

起動可能な USB メモリ上に構成したソフトウェアを用いて，これを用いて PC を起動すれば USB メモリ上の OS およびソフトウェアが起動し，内蔵ハードディスク全体のハッシュ値が計算され，その計算結果及び当該ハッシュ値のアップロード先の URL 等の情報を QR コードとして PC 上の画面にするためのプログラム（以下,「本プログラム」という.）を作成する．

上記ハッシュ値のアップロード先のハッシュ値登録用サーバを，中立的な第三者機関に構築しておく．このサーバは登録されたハッシュ値にタイムスタンプ署名を施した上で，その値を広く Web サーバとして公開する．

２　システムの実行段階

捜査機関がデジタルデータの格納された PC, あるいは PC に内蔵されたハードディスク等の記録媒体を差押え等する際に，PC 等の所有者（管理者）は，上記 USB メモリを挿入し，本プログラムを起動させる．そして，画面上に表示された QR コード（上記ハッシュ値の情報）をスマートフォン等で読み取り，その値およびアップロード先を捜査機関

---

[p] 前掲高橋他 272 頁，同上.

[q] 前掲吉峯他 122 頁では，改変防止の必要な措置が取られなかった場合，捜査機関によるデジタルデータ改変の機会は否定出来ず，少なくとも抽象的には改ざんの疑義が存在すると言えるが，その場合，厚労省 FD 改ざん事件という，検察官の証拠偽造事件が立証された事例が出現したことを考慮しても，なお抽象的な疑義だけでは足りないという判断が妥当するのか検討する必要がある旨指摘されている.

[r] なお，民事事件についてではあるが，大阪高判平成２１年5月１５日（判タ 1313 号 271 頁）は，電子メールの真正性が争われた事案に関して,「電子記録はその性質上改ざんしやすいものであるから，これを証拠として採用するためには，その記録が作成者本人によって作成され，かつ，作成後に改ざんされていないことを確認する必要がある.」と指摘している.

[s] 同じく民事事件についてではあるが，東京高判平成２１年３月２７日（判タ 308 号 95 頁）では，IC レコーダーに記録された音声データについて一部削除の有無が争われ,「一般にデジタル方式で録音された音声データは削除，結合等による編集を行ってもその形跡が残らないと認められるから，本件音声データに編集改ざんの痕跡が認められないからというだけでは，本件音声データについて録音後に編集改ざんが行われなかったと断定することはできない.」と判示されている．また，東京地判平成２８年３月２３日（LLI/DB 判例秘秘書 L07130728）では，ファイルの不正コピーに関して，事件発覚後相当期間経過後に民事証拠保全手続きが行われたが，不正行為時の PC 及びネットワークの操作ログについての改ざんに関して争われた事案である．最終的に改ざんした事実は認められないとさているが，事件発覚後の早期の保全手続きの重要性が示唆された事案と言える.

[t] 前掲高橋等 281 頁以下，前掲吉峯他 122 頁.

[u] 前掲高橋等 282 頁参照.

[v] 同上.

Copyright (c) 2017 by the Information Processing Society of Japan

に確認させた上で，上記サーバにアップロードする．サーバは計算されたハッシュ値にタイムスタンプ付き電子署名を付して Web 上に公開する．

３　ハッシュ値の確認段階

後日，デジタルデータが証拠開示された際に，同時にイメージファイルについても開示させ，ハッシュ値を計算して公開サーバ上の値と比較することによって，改ざんの可能性の有無を確認することが可能となる．

4.3 想定される利用場面

4.3.1 刑事事件の場合

捜査機関がデジタル証拠を収集するには，任意処分による方法と裁判所の発布する令状によって実行される強制処分による方法が存在するが，いずれの方法によるにせよ，①目的となるデジタルデータが記録されている PC（電子的計算機），ハードディスクあるいはフラッシュメモリー等のオリジナルの記録媒体そのものを差押えるか（任意提出の場合であれば，領置する），②別途記録媒体を用意させ，そこにデジタルデータを記録させ，それを差押える（あるいは任意提出してもらう）という方法によることになる[w]．

本システムは，前述の通り，PC に USB メモリを挿入し，PC 画面上に計算されたハッシュ値等の QR コードを表示させる仕組みであることから，ここでは，PC の差押えに限定して考える．

そうすると，②の場合であれば，差押え手続きの一環として記録媒体にデジタルデータを記録する際に，捜査機関によってもハッシュ値の計算を行うことが予想されることから，差押え手続きに先立ち，本システムにおけるハッシュ値の保全作業（以下，「本作業」という．）を実施することが望ましい．他方，①の場合では，捜査機関は，PC を差押えた際，その現場でハッシュ値を計算する作業を行うことはなく，そのまま持ち帰ることが通常であろう．しかし，PC を警察署等に持ち帰った後，捜査機関自身によって本システムが利用されることが期待出来れば良いが，それが期待出来ないのであれば，差押え前に，同その現場で本作業を実施することが望ましい．本システムは，改ざんが可能かつ容易なデジタル証拠の改ざん防止を確保するために構築されたシステムである以上，捜査機関による差押えと同時に実施されることがその趣旨に適うと言える．

4.3.2　民事事件における応用

なお，本システムは，直接的には刑事事件での利用を想定して提案したものであるが，もとより民事事件においても利用可能である．確かに，本システムは，証拠の保全作業の過程において，証拠が改ざんされるリスクを防止するために考案されたシステムであり，保全作業以前の改ざんを検知するようなシステムではない．従って，デジタル証拠自体の真正性･完全性を担保するものではない．しかし，デジタル証拠を法廷に証拠として提出しようとする場合，当該デジタル証拠を入手した後直ちに本システムを利用して，タイムスタンプ付き電子署名を付しておけば，その時点以降の改ざんの有無が争われるリスクは事実上なくなり，デジタル証拠の真正性・完全性に関する争いは格段に減少することが期待出来る．また，本システムの普及が進めば，容易に改善防止の措置が取れたにもかかわらずその措置を取らなかった事実自体が立証責任の観点から不利に扱われる事由にもなると考えられる．

5.　システムの評価

5.1 フォルトツリー分析

ハッシュ値を計算しサーバ上にアップロードしてもその過程で，不正な手段や過誤が介入し正しくないハッシュ値がアップされるリスクが高いのであれば，本システムに対する信頼は得られない．そこで，ここでは，刑事事件についてこのようなリスクが果たして高いと言えるのかについてフォルトツリー分析（FTA:Fault Tree Analysis）及びイベントツリー分析（ETA:Event Tree Analysis）により評価する．なお，今回は，捜査機関が本システムの利用については同意していることを前提としている．また，本システムの使用する場面を想定した場合，捜査機関自身が利用する場合，被疑者・被告人が利用する場合，そして第三者が利用する場合が想定されるが，被疑者等の被差押対象者が主導的に行うことは現実的には想定しづらいことから，捜査機関自身が行う場合以外の場面については，そもそも想定しないものとして考える．

5.2 フォルトツリーの作成

まず，頂上事象として，捜査機関によって正しくないハッシュ値がサーバにアップされるという事象を設定する．次に，その原因であるが，まず第１に，本システムによって正しくハッシュ値が計算されたものの，サーバにアップする段階で偽の QR コードにすり替えアップした場合，第２に，そもそも正しくない QR コードが作成される場合の二つの要因事象が想定出来る．そして，後者については，さらに，捜査機関の故意による不正の場合，捜査ミス等人的過誤（ヒューマン・エラー）による場合，または，機器の故障やソフトウェアのバグ等システム自体のエラーの場合が基本事象として想定される．そして，これらの各事象間は OR ゲートの関係（下位事象うち１つでも起きれば上位事象が成立する．）が成り立つ．

このようにして，作成したフォルトツリーを図３に示す．

---

[w] 強制処分の場合，従来，オリジナルの記録媒体以外を差押えるという方法は認められていなかった．しかし，デジタルデータそのものだけが必要な場合やデジタルデータが記録されたオリジナルの記録媒体を差押える必要がない，あるいは差押えることが不都合もしくは困難な状況も存在することから，平成２３年，情報処理の高度化等に対処するための刑法等の一部を改正する法律（平成２３年法律第７４号）により刑事訴訟法が改正され，次の３つの場合に限り，押収すべきデジタルデータに関し，記録媒体へ記録させ，その記録媒体を差押えることが可能となった．

i記録命令付差押え（刑訴法 99 条の 2，218 条 1 項）

裁判所が令状発布の際に，電磁的記録を保管する者等に命じて必要な電磁的記録のみを記録媒体に記録等させた上，当該記録媒体を差し押える方法．

ii電磁的記録の複写等（刑訴法 110 条の２，123 条 3 項，222 条 1 項）

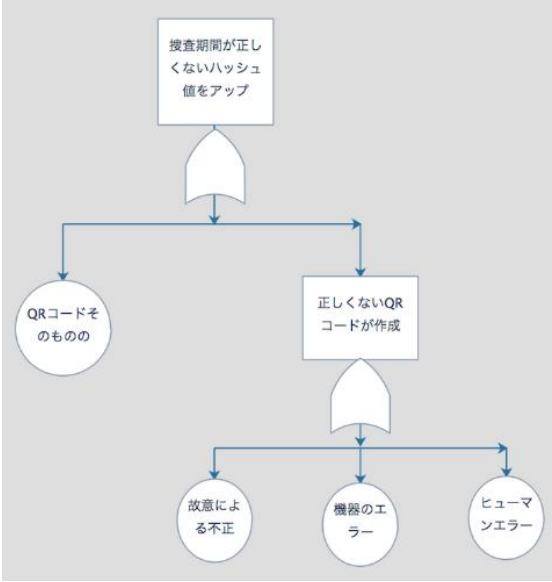
差押状の執行をする者が，その差押えの際にその差押えに代えて，差し押さえるべき記録媒体に記録された電磁的記録を他の記録媒体に複写等した（あるいは差押えを受ける者に複写等させた）上，当該他の記録媒体を差し押える方法．

iii電気通信回線接続記録の複写（刑訴法 99 条 2 項，218 条 2 項）

差し押えるべき物が電子計算機であるときは，当該電子計算機に電気通信回線で接続している記録媒体に保管されており，当該電子計算機で作成・変更・消去することができる電磁的記録については，当該電子計算機等に複写した上，当該電子計算機等を差し押える方法．

Copyright (c) 2017 by the Information Processing Society of Japan

図３　不正なハッシュ値がアップされるフォルトツリー



5.3 フォルトツリーの評価

このフォルトツリーを用いて各事象の発生確率を検討する．

ところで，本システムは，ハッシュ値の計算・表示，サーバへのアップについてはほぼ自動化されており，人の手が介在するのはハッシュ値の読み取りのためにスマートフォン等をかざす行為程度であり，ヒューマン・エラーが生じるリスクはそもそも極めて低く設定されている．少なくとも，捜査機関が独自にハッシュ値を計算し記録しておく通常の過程に比べれば，ヒューマン・エラーの発生確率は格段に低いと言える．また，機器の不具合やソフトウェアのバグ等のシステム自体のエラーについても，リリースまでに通常想定できる程度の適切なテスト等を経ていれば，捜査機関による通常の作業過程に比べてリスク発生確率が高くなることは想定出来ない．

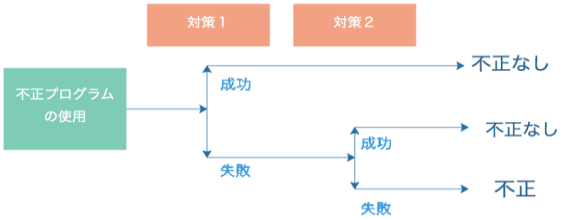
とすると，本システム利用によるリスク発生の確率を検討する場合，捜査機関による不正行為が介在するリスクを検討すれば足りると言える．

5.4 イベントツリー分析

そこで、次に，捜査機関による不正行為が介在する二つの各事象について，そこから正しくないハッシュ値がアップされる発生確率を検討する．ここでは，各事象を起因事象として，そこから生じるリスクに対する対策を検討することによって最終状態の発生確率を求めるイベントツリー分析を用いる。

まず，起因事象１として，捜査機関が偽の QR コードを作成しすり替える場合を想定したイベントツリーを図４に示す．

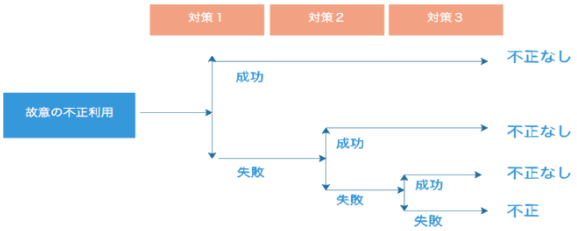
図４　偽の QR コードの作成に対応するイベントツリー



この場合，捜査機関が偽の QR コードを作成しても，被差押者が，本システムによって実際に作成された QR コードを確認すれば（対策 1），捜査機関の不正は防げる．また，その場で確認出来なかった場合でも，本システムによって作成された QR コードをログとして保存するようにしておけば（対策 2），実際にアップされた偽 QR コードと比較することは可能である．とすれば，これからの対策が奏功せず，正しくないハッシュ値がアップされるリスクは，相当程度限られた局面に限定されるだろう．

次に，起因事象２として，故意によって不正を図る場面を想定したイベントツリーとして，捜査機関が偽のプログラムを使用する場合を例にして図５に示す．

図５　偽のプログラムの使用に対応するイベントツリー



捜査機関が，本プログラムを改ざんする等して偽のプログラムを用意し偽のハッシュ値を作成・アップしようとした場合，それに対する防止策として，まず，本システムを利用するためにはその都度特定のサーバから本プログラムをダウンロードする運用を確立することが考えられる（対策 1）．そして，この対策によっても不正プログラムへのすり替え等のリスクが避けられなかったとしても，次の対策として､本プログラムのハッシュ値を予め計算しておけば，当該偽プログラムのハッシュ値と比較することで防止出来る（対策 2）。さらに，仮に，この対策でも防げなかった場合でも，被差押者側でも差押証拠のハッシュ値を取ることによって，捜査機関によって計算されたハッシュ値と突合した上でアップロードする対策を取ることで不正の介在は防止出来る（対策 3）。そうすると，捜査機関が偽のプログラムを事前に準備していたとしても，偽の QR コードがアップロードされるリスクは，これらの対策が全て失敗するような極めて限られた場面に限定されると言えるだろう．

いずれにしても，以上の分析結果から考えれば，本システムによって正しくない QR コードがサーバにアップロードされるリスクは極めて低いものと評価出来る．

6. 考察とまとめ

本研究では，デジタル証拠の改ざんが容易であることを示し，改ざん防止の措置を取ることが重要であり，そのためのシステムとして本システムの有効性を示した．ところで，本システムでは，アップロードされる情報の中核は当該差押えされた PC のハードディスクのハッシュ値であり，それは Web ページ上に公開されることが前提となっている．これは，本システムが，当事者の合意のもとにサーバにアップロードすることによって，否認可能性を排除することが可能となるからである．この点，プライバシーの観点から，情報の公開について問題がないのかという批判もあるかもしれない．しかし，否認可能性の排除には，情報の公開が最も効果的であることに加え，ここで，公開されている情報は，あくまでもハッシュ値という数字であり，その数字自体には何の価値も意味もないことから，それを

Copyright (c) 2017 by the Information Processing Society of Japan

公開しても何ら問題は生じず許容性も認められる．

但し，ここで，一つ問題が生ずるとすれば，公開されている情報がハードディスクのハッシュ値だけであるとすると，そのハッシュ値が，当該差押えにかかる PC のハードディスクについてのハッシュ値であるということを確認する方法が存在しないということである．即ち，この識別の問題をクリアしておかなければ，捜査機関から開示された証拠のハッシュ値がもし一致しない事態が生じたとしても，そもそも証拠が異なっている等の言い訳（言い逃れ）を許す余地があるからである．プライバシーの問題に抵触しない範囲で，かつ事件ないし被差押え物件を識別出来る情報についても合わせて登録することが必要となる．例えば，差押え日時，場所，被差押対象者，被差押物件を登録すれば識別の観点からは十分であるが，当然，プライバシー上の問題が生じる．仮に，上記識別情報を暗号化することも考えられるが，そうするとシステム自体複雑になりすぎるという問題も生じる．事件等識別性を保持しつつ，それ自体を入手しても当事者以外の第三者にとっては被差押対象者を特定出来ない番号であることが望ましい．そうすると，差押時に作成される差押調書や任意提出の際に作成される領置調書に添付される押収品目録や領置品目録に記載される記号・符合・番号が相応しい．あるいは，差押え手続きの年月日及び開始時間並びに実施担当者の所属警察署及び氏名階級の記載でも被差押対象者のプライバシー上の問題は生ぜず，手続きの識別は可能である．

他方，民事事件の場合，本システムを利用してハッシュ値を登録する当事者は，デジタル証拠を管理し提出する当事者と一致することから，登録ハッシュ値と開示証拠のハッシュ値が一致しない以上，改ざんを疑われても，証拠が異なるという弁解は通用せず，識別性の問題は生じにくい．

なお，本システムは，民事事件，及び刑事事件の場合であれば，特に，任意処分の場合には，その任意提出者自身の判断によって実行することが可能であることから，より利用されやすいと言える．しかし，強制処分の場合，USB の挿入を伴う本システムの性質上，被差押者による操作を許せば，本システムの実行と見せかけてデータを破損させられるリスク等も否定出来ず，実務上，捜査機関が本システムの使用を許容することは難しいかもしれない．しかし，本システムは，単に PC（に内蔵されたハードディスク等）のハッシュ値を計算し，画面上に QR コードとして表示するだけの比較的単純なシステムである以上，実行前に捜査機関に USB を検証させる仕組みを合わせて構築する等して捜査機関にとっても安心できるシステムにすることが課題となろう．あるいは，差押えと同時にハッシュ値を計算し，それを保全することが最も重要な要素であることを考えれば，ハッシュ値の計算自体は捜査機関によって実行・開示させ，その開示されたハッシュ値をハッシュ値保管用サーバにアップロードするような運用上の工夫を加えることも検討に値するだろう．

参考文献

[1] 吉峯耕平他「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 122 頁（2014）

[2] 鈴木一朗他「デジタルデータ（フロッピーディスク）分析　厚労省事件」季刊刑事弁護 71 号 60 頁（2012）

[3] 前田恭幸他「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」情報処理学会研究報告 vol.2016-EIP-72 No.9

[4] 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（2015.10）

[5] 野上紘他「公判対応を前提としたメモリ・フォレンジック有用性の考察」SCIS2016

[6] 高橋郁夫他「デジタル証拠の法律実務 Q&A」（日本加除出版株式会社 2015）

[7] 町村泰貴他「電子証拠の理論と実務」（民事法研究会 2016）

[8] 後藤伸寿他「フォルトツリー解析及びイベントツリー解析によるリスク評価の事例」

Copyright (c) 2017 by the Information Processing Society of Japan