特集
Special Feature

［最新のデジタル・フォレンジック事情］

2 最新のデジタル・フォレンジックにおける技術的課題

応
般

上原哲太郎　立命館大学情報理工学部

デジタル・フォレンジック（以下，DF）の歴史と技術

コンピュータ上で行われる不正や犯罪行為は，パソコンの普及が始まった 1980 年代にはすでに社会問題化していた．日本において銀行員がオンライン端末の操作により巨額の横領をして社会問題になったのは 1981 年のことであり，米軍のコンピュータに侵入してゲームを楽しんだばかりに核戦争を引き起こしそうになる高校生を描いた映画『ウォー・ゲーム』が公開されたのは 1983 年である．パソコン上で動作するコンピュータウィルスが新聞紙面を賑わすようになったのは 1980 年代後半であり，1990 年には当時の通商産業省の告示に伴い，（独）情報処理推進機構がコンピュータウィルスや不正アクセスに関する被害の届出制度の運用を開始している．このような不正や犯罪行為の証拠となるデータの取扱いを，鑑識学のような学問として位置づけて体系的に整理しようという動きが始まったのは 1990 年代に入ってからである．1992 年にはこの分野に Computer Forensics という用語を充てようという提案が行われ [1]，90 年代後半になると FBI や Interpol の文書内でも使われるようになった．しかし 2000 年代に入って，PDA やスマートフォンなどパソコン以外の電子機器の存在感が増すにつれ，Computer Forensics は Digital Forensics として再定義されることになった．2001 年には Digital Forensic Research Workshop （DFRWS）が開催され，以降現在に至るまで毎年開催されている．IFIP は 2004 年に WG11.9 Digital Forensics を設け，2005 年より毎年国際学会を開催している．我が国においては 2004 年に特定非営利法人デジタル・フォレンジック研究会（IDF）が設立され，産学連携による普及啓蒙活動を続けている．IDF が定めた DF の定義である「インシデントレスポンスや法的紛争・訴訟に際し，電磁的記録の証拠保全及び調査・分析を行うとともに，電磁的記録の改ざん・毀損等についての分析・情報収集等を行う一連の科学的調査手法・技術」は，現在広く引用されるに至っている．

情報科学分野における技術の進化は速いため，DF も新技術への対応を常に求められている．特に，証拠の発見と分析の対象となってきた二次記憶装置においては，その急速な容量の増加と，ハードディスクからフラッシュメモリへの置換えという 2 つの大きな変化への対応が迫られてきた．さらに，DF の対象となる機器の広がりや，クラウド技術への対応も大きな課題である．加えてサイバー攻撃や不正の手法が進化してきたことや，対象となるディジタル証拠が単なるログや文書データから，画像や音声，映像といったものも含むマルチメディアデータに広がってきたことへの対応の課題もある．本稿では，最新の DF の技術が直面しているさまざまな課題について述べる．

特集
Special Feature

二次記憶装置の技術進化への対応

パソコンに内蔵される二次記憶装置の容量は，2005 年ごろには 60 ～ 200GB 程度だった．それが 2010 年ごろには最大で 1TB 程度の容量に達している．その後，市販パソコンに内蔵される二次記憶装置の容量はさほど増えていないものの，ハードディスクドライブ（HDD）の容量増加は続き，2021 年現在 3.5 インチ HDD の最大容量は 20TB に達している．しかしこの急激な容量増大に対し，HDD プラッタの回転速度はほとんど向上していないため，データ転送速度の向上も緩やかである☆1．HDD と外部を接続するインタフェースにおける速度も，2008 年に SATA-3 によって 600MB/s が達成されて以来，向上していない．DF においては HDD の解析前に，ファイルが記録されていない領域も含めた全セクタデータの複製による証拠保全が求められるが，この作業には HDD の容量にほぼ比例した時間がかかるため，大きな課題となっている．実際の証拠保全装置における複製の実効速度は使用する装置や HDD の状態によって変わるが，たとえば 100MB/s とすると容量 18TB の HDD の証拠保全に 50 時間程度を要する．HDD の容量向上は今後も続き，近く 3.5 インチ HDD の容量は 80TB 程度まで増大することが予想されているので[2]，遠からず HDD の証拠保全が現実的な時間では終わらなくなることが予想される．本来，このような証拠保全は HDD 内の解析の際に削除ファイルの復元を行うなどの作業が元データの破壊につながらないようにする目的で行われているので，証拠となる HDD 上での直接の作業においてもデータ書き込みを抑止する技術や，そのような作業が行われた場合であってもデータの破壊や改ざんに繋がっていないことが客観的に確認できる技術が今後求められてくると思われる．

HDD の容量増大はほかの問題も引き起こしている．HDD では，メディア上のセクタの一部が磁性体不良などによりエラーになることが避けがたいため，余剰のセクタをあらかじめ用意しておいてエラーが生じたセクタと入替える代替処理が行われている．この余剰セクタの容量が HDD 容量増大に比例して増加しているため，この余剰セクタを利用してデータを隠蔽するような処理が行われるリスクが指摘されている[3]．このようなデータ隠蔽を行うためには HDD のコントローラに対する特殊な命令の発行などが必要であるため，現状ではそのリスクは必ずしも高くはないが，このような隠蔽を簡単に行うことができるツールが将来流通した場合に一気にリスクが高まる恐れもあるため，注意が必要になるだろう．

また，二次記憶装置において HDD からフラッシュメモリを用いた SSD への移行が続いていることも大きな問題となっている．DF においては，削除されたファイルの復元は証拠隠滅の可能性を分析するための重要な手続きである．HDD においては，ファイルの消去はファイルシステム上でのメタデータの書き換えで行われるため，データ本体はメディア上に残存しており，その領域へのデータ上書きが行われない限りはファイルの復元が可能である．しかし SSD においてはフラッシュメモリのメディア特性上，データの上書き前に消去が必要であり，これに処理時間を要することから，削除されたファイルのデータが記録されたセクタについても OS と SSD コントローラが協調してバックグラウンドで先行消去することにより，書き込みを高速化する処理が一般化している．このため一般に SSD における削除ファイルの復元処理は困難であり，メタデータに残存する情報の分析など削除ファイル復元に拠らない分析技術が求められている．

☆1 HDD の容量は記録媒体であるプラッタの枚数と記録密度それぞれに比例して増加するが，回転速度が一定の場合，記録密度の増加のみが転送速度の向上に寄与する．しかも記録密度が 2 倍になっても転送速度は$\sqrt{2}$倍にしかならない．プラッタの各記録面に用いられる読み取りヘッドを独立に制御できれば理論上は転送速度がプラッタ枚数に比例して向上するが，2021 年現在はヘッドを 2 組に分けてそれぞれ制御するデュアルアクチュエータ技術がようやく実用化されたところである．

フォレンジックの対象となる機器やシステムの多様化への対応

情報通信技術の発展によりさまざまな機器や情報システムが生活の基盤として用いられるようになればなるほど，DF が対象とする機器やシステムも多様化している．

この 10 年ほどで急速に普及したスマートフォンは，現在では DF の重要な対象デバイスとなった．ほとんどのスマートフォンは iOS または Android をベースとした OS が搭載されているが，いずれもパソコンやサーバ向けの OS とは異なり，アプリケーションはそれぞれサンドボックスモデル[☆2]に基づいて隔離された環境で動作するため，OS やほかのアプリケーションにアクセスする手段が限られており，マルウェアとして作成されたアプリケーションが OS やほかのアプリケーションのデータ改ざんなどを行うのが難しい．さらに，アプリケーションも Apple や Google が悪意ある挙動がないか確認した上で，App Store や Google Play Store などのいわゆる公式ストアを経由して提供することを基本としているため，マルウェアの配布手段に乏しい．特に iOS に関しては App Store 経由以外でアプリケーションの提供ができないため，より安全に利用できるとされる．さらにアプリケーションが OS の脆弱性を突く手段も限られるため，パソコンに比してマルウェアリスクがきわめて少ないとされる．

しかしこのことは DF において証拠保全手続きに必要となるファイルシステムへの直接アクセスを困難にしている．実際スマートフォンにおいては，OS の脆弱性を突いてサンドボックスモデルを回避する Jailbreak（iOS の場合）や root 化（Android の場合）と呼ばれる手段を用いてファイルシステムへの直接アクセス手段を確保することがあるが，このことによって削除ファイルの復元などフォレンジックに必要な技術が適用可能になる一方，この手順の間に予期せぬデータの破壊が起きたり，また得られた証拠の真正性に疑義を生じさせたりするリスクがある．そもそも特にいずれの OS においても脆弱性の改修は進み，JailBreak や root 化が年々難しくなってきていることもフォレンジック作業の障害となっている．一方で一部のアプリケーションデータについては，iOS では iTunes を用いたバックアップファイルの解析，Android ではデバッグ機能として提供されている ADB コマンドを用いた解析によって一定の情報が得られる場合があり，利用されている．このほかに，刑事事件の被疑者や不正調査の対象者が個人所有するスマートフォンの解析において，対象者が暗証番号や生体認証によるロック解除に同意しなかった場合に，強制的にロック解除する方法についてもニーズが高いが，これは OS の基本的なセキュリティ機能であるだけに脆弱性やバックドアを発見する以外には実現が難しい．

さらに最近大きな問題となっているのはクラウド上に保存されたデータに対する分析への対応である．対象となるシステムが IaaS におけるストレージであった場合には従来のフォレンジック技術が適用可能である場合が多いが，SaaS や PaaS であった場合には，システム上の全データの取得や削除されたデータの復元はシステムがそのような機能を提供していなければ困難である．前者についてはデータのバックアップ機能等で代替できることが多いが，後者については削除データを復元できる機能が元々備えられているシステムでのみ実施可能となる．ただし特に米国企業に提供されるシステムについては，主に民事裁判におけるディスカバリーに対応するために，利用者に関する詳細なログの保管，広範なデータ検索や削除データの一定期間の保管などの機能提供がなされている場合があるが，これらは直接裁判に拠らないフォレンジック調査のためにも有用である．利用者のプライバシー保護と不正調査や犯罪捜

☆2 ここでは，各アプリケーションを互いに分離し影響しあわないようにするとともに，OS へのアクセスも最低限にするアーキテクチャのこと．

査からの要求とのバランスから，どのような機能をクラウドサービスが提供するべきかの議論は今後も続くと考えられる．

フォレンジックの対象となるデータの多様化への対応

かつて犯罪捜査や不正調査における DF では，情報システム上の各種ログ，ネットワークへのアクセス履歴や検索履歴，メール送受信履歴とその内容，そして特に多様なデータの中でも文書データがその主な対象だった．しかし最近はあらゆるメディアがディジタル化されるに伴い，画像や音声，動画といったマルチメディアデータが分析対象となる機会が増加している．この際に問題になるのは，その内容の真贋である．

すでに静止画像については，きわめて容易にその画像内の特定の人物や物体を消去したり，人の顔の表情を改変できる各種ツールが広まっているため，SNS を中心にいわゆるフェイク画像が多く出回るようになり，画像に対する信頼性が揺らいでいる．動画像についても，深層学習の技術を用いて動画像中の人の顔を他人と入れ替える，いわゆる DeepFake と呼ばれる技術が知られるようになり，これを実現するスマートフォンアプリケーションなどもすでに存在するため，偽造された動画像が出回るリスクが高くなっている．音声についても，元々ディジタルデータにおける一部削除などの編集は容易である上に，音声合成技術の向上も相まって，偽造された音声データが流通するリスクは高まりつつあると言える．

これら画像，音声および動画は，それを視聴・聴取した人に残る印象がきわめて強いため，偽造されたものが証拠として法的係争の場に持ち込まれた場合の弊害は大きい．よってマルチメディアデータの真贋を自動的に判定する技術への要求は高いが，これはまたそれらの自動判定技術を回避してより自然な改ざん画像等の生成を行う技術とのいたちごっことなっている．たとえば DeepFake については，その検出について多くの研究が発表されてきており，初期においては生成された顔が滅多に瞬きをしないことを利用した検出などが提案されたが，現在のツールは自然な瞬きを実現するようになってきており，真贋判定技術としてはもはや有効となっていない．静止画像の改ざん検出については，筆者らはさまざまな研究をサーベイしたが[4]，いずれも完全な自動判定は難しく，また改ざん側のツールの進化によって無効になるような技術が多いと結論づけている．今後はこれらのツールにおいて生成された画像等に電子透かし技術などで改ざんされたことをマークしておくなど，社会的な対応が求められてくると考えられるが，このようなマーキングを行わない，真に悪意ある改ざんへの対応はいつまでも課題として残ると考えられる．

以上見てきたように，DF の対象が広がるにつれてその技術的課題はむしろ増大している．本稿が，より多くの研究者がこの分野に参入することの一助になればと願っている．

参考文献

1）Collier, P. A., Spaul, B. J. : A Forensic Methodology for Countering Computer Crime. Artif Intell Rev 6, pp.203–215 (1992).
2）HDD の次世代記録技術 HAMR 対応 HD メディアの製造技術を開発，昭和電工（株）ニュースリリース，2020 年 2 月 6 日．
3）下垣内太：Exotic Data Recovery & PARADAIS, CodeBlue 2016.
4）Teerakanok, S. and Uehara, T. : Copy-move Forgery Detection : A State-of-the-art Technical Review and Analysis, IEEE Access, Vol.7, pp.40550-40568 (2019).

（2021 年 6 月 23 日受付）

■上原哲太郎（正会員） t-uehara@fc.ritsumei.ac.jp

1995 年京都大学大学院工学研究科情報工学専攻博士後期課程研究指導認定退学．京都大学助手，和歌山大学講師，京都大学助教授を経て 2011 年総務省通信規格課標準化推進官．2013 年より現職．京都大学博士（工学），特定非営利法人デジタル・フォレンジック研究会会長．和歌山県，京都府，滋賀県各警察本部のサイバー犯罪対策アドバイザーを務める．