特集
Special Feature

［最新のデジタル・フォレンジック事情］

3 サイバー犯罪とデジタル・フォレンジックの課題
―企業や組織における事前対策の備え―

応用

北條孝佳　西村あさひ法律事務所

ディジタル社会と電磁的記録

電磁的記録の特徴

ディジタル社会の浸透によって，ディジタルデータである電磁的記録が至るところに存在する．そのため，サイバー犯罪が発生した場合だけではなく，通常の犯罪捜査においても，この電磁的記録が証拠として取り扱われるようになってきており，電磁的記録なくして犯罪捜査はできないといっても過言ではない状況である．

電磁的記録は，「電子的方式，磁気的方式その他人の近くによっては認識することができない方式で作られる記録であって，電子計算機による情報処理の用に供されるもの」（刑法７条の２，民事訴訟法３条の７第３項カッコ書）を指し，いわゆるディジタルデータを意味するが，この電磁的記録は，誰でも容易に作成や削除，修正，改変，複写等ができる上，容量も膨大になる．そのため，電磁的記録を用いた犯罪捜査は，さまざまな技術を駆使しなければ適正かつ効率的な捜査ができない．

電磁的記録が犯罪捜査に必要不可欠な現状に鑑みると，常に犯罪の立証のためというデジタル・フォレンジック（以下「DF」という）を意識しておく必要がある．もっとも，DF は犯罪捜査のためのみならず，サイバー犯罪の被害に遭った状況把握にも用いられることもあるし，企業や組織が適切な調査を実施したことの証左にもなり得る．

DF の大きな流れとしては，電磁的記録が保存されている電子計算機等の端末の収集または特定および電磁的記録の保全，当該電磁的記録の検査・分析（解析），解析結果報告書の作成がある（図 -1 参照）．

企業や組織がサイバー犯罪の被害に遭った場合

企業や組織がサイバー犯罪の被害に遭えば，被害状況を特定することが必要になる．しかし，企業によっては，事業継続を優先するあまり，被害に遭った端末を元に戻そうと，証拠となり得る電磁的記録を保全せず，バックアップデータから被害前の状態に戻したり，購入時の状態にするためクリーンインストールしたりすることもある．このような対応後に，セキュリティ事業者に連絡したり，警察に通報したりする企業もあるが，このような状況下では，被害実態が判明しないおそれがあるのは想像にかたくない．ネットワーク機器や重要なファイルを保存しているファイル共有サーバ等には痕跡データがわずかながら残存している場合もあるが，被害に遭った端末等の痕跡データがほとんど残っていない状況においては，被害経路，

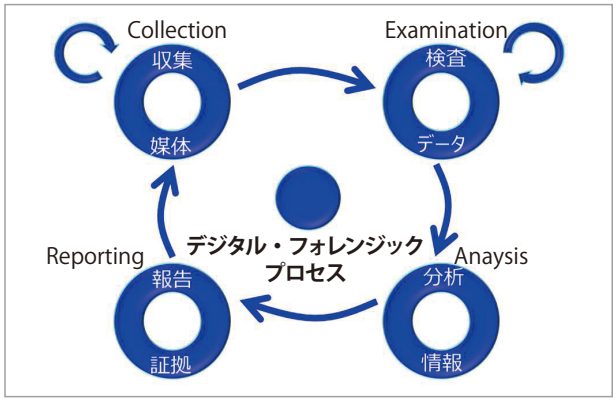

図 -1　デジタル・フォレンジックの流れ

被害日時，流出の被害対象となった電磁的記録等が判明しない可能性がある．このような場合，いつから犯罪者に侵入を許していたのか，どこから犯罪者が侵入したのか，第三者から預かっている電磁的記録等が漏えいした可能性があるのか，といったことが不明になるおそれがある．そうすると，外部に対して被害状況を説明することができず，漏えいした可能性のある電磁的記録の主体である第三者に何が漏えいしたのかを説明することもできなくなる．また，再発防止策を検討することもできなくなる．

このような状況は決して望ましいものではなく，企業によっては，株主らステークホルダへの説明責任を果たせなくなるおそれすらある．

そこで，次章ではサイバー犯罪の被害に遭った端末を証拠保全しておくために必要な事項およびその課題について説明する．

証拠保全

端末の特定および収集

端末やサービスの特定

サイバー犯罪が発生した場合に，どの端末やサービスがサイバー犯罪に使用されたか，あるいは被害に遭ったかを特定し，証拠保全のための準備をする必要がある．

たとえば，サイバー犯罪にマルウェアが使用され，電子メールに添付されたマルウェアに感染した端末を経由してファイル共有サーバからデータが盗まれた事例を仮定する．このような場合，①マルウェアを特定して抽出し，マルウェアの解析を行うこと，②マルウェアに感染した端末からファイル共有サーバに接続した履歴を収集すること，③ファイル共有サーバから盗まれたデータを特定すること，④ファイル共有サーバからマルウェアに感染した端末に盗まれたデータがコピーされ圧縮された痕跡がないかを調査すること，⑤マルウェアに感染した端末から外部に送信された接続履歴を収集すること，などが求められる．そのためには，マルウェアに感染した端末の証拠保全，ファイル共有サーバの証拠保全，ネットワーク履歴の証拠保全を実施し，解析することが考えられる．

ただし，近年のマルウェアはファイルレスマルウェアとしてファイル自体が存在しないものも多く，①のマルウェア自体を抽出することができないこともある．また，②マルウェアに感染した端末からファイル共有サーバに接続した履歴を保存していない環境であれば，接続履歴が存在しない．ファイル共有サーバにおいてファイルへのアクセス履歴すべてを取得していなければ，③ファイル共有サーバから盗まれたデータを特定することもできない可能性がある．さらに，近年，企業が用いる端末は SSD（Solid State Drive）が内蔵され，SSD 全体が暗号化されているものが多いことも痕跡データが失われる原因の 1 つになる．この理由は次のとおりである．犯罪者は，マルウェアに感染した端末を介してファイル共有サーバに接続し，当該サーバから電磁的記録をマルウェアに感染した端末にコピーし圧縮した上で外部に転送する．その後，犯罪者は，当該圧縮データを削除するといった手法を用いることが多い．この後に，SSD のガベージコレクション（SSD はブロック全体でなければ消去できないため，ブロック内の有効なデータを別のブロックにコピーして，不要となったブロック全体を消去することを自動で実施する機能）が実施されると，④削除された圧縮データの痕跡を抽出できなくなる．ほかにもプロキシサーバを経由して外部ネットワークに接続する構成ではなく，各端末が直接外部に接続可能な環境であれば，⑤マルウェアに感染した端末から外部に送信された接続履歴が保存されていないこともある．

このように被害実態を解明するために証拠保全を実施したとしても，被害実態を直接解明することが可能な痕跡データがほとんど残っておらず，被害実態を解明するには他の痕跡データから推定しなければならないといった事態も多々存在する．

近年，スマートフォン端末は，電子メールや画像データ，バックアップデータなど，ほぼすべての電磁的記録がクラウドサービスに保存されるようになってきて

いるため，サイバー犯罪に関係するスマートフォン端末を特定し，当該端末を使用してどのようなサービスが使用され，クラウドサービスに保存されているかが重要になることもある．

企業や組織の端末に対する事前準備

端末がサイバー犯罪の被害に遭った場合，被害申告のあった端末だけではなく，当該端末を経由して，他の端末がサイバー攻撃の被害を受けている可能性もある．そのため，迅速にすべての被害端末を特定し，被害全体を把握する作業が必要になる．

端末の操作ログをすべて保存するような EDR（Endpoint Detection and Response）等のシステムを導入していない企業や組織では，各端末から簡易的な情報を収集できるツール等を活用して，被害端末を特定することになるため，見逃しがあったり，重要な情報を収集できなかったりすることもある．

このような作業は，非常に非効率的であり，時間だけが膨大に消費されてしまうため，特定非営利活動法人デジタル・フォレンジック研究会（IDF）が作成している「証拠保全ガイドライン第 8 版」では，ファストフォレンジックの実施を推奨している．

ここで，ファストフォレンジックとは，早急な原因究明，侵入経路や不正な挙動を把握するため，必要最低限のデータを抽出およびコピーし，解析することをいう．ファストフォレンジックを実施するには前述した EDR の導入等，事前の環境構築や専用ツールの動作検証等の準備が重要になるが，ファストフォレンジックを実施することによって，企業や組織のセキュリティ担当者の作業量が少なくて済む場合がある．また，被害端末を早期に特定しなければ，犯罪者によってインストールされたマルウェアがシステムやネットワーク内に潜伏し，気づかぬうちに被害を拡大させている可能性もあるため，ファストフォレンジックによる早期解明が重要になる．

ほかにも犯罪者が感染端末を遠隔操作するために，感染端末が C2（Command and Control）サーバと呼ばれるサーバと定期的に通信を行う場合がある．しかし，この C2 サーバは短期間で消滅することもあるため，被害端末を特定した後すぐに，C2 サーバを調査することで，接続元 IP アドレスや通信内容を把握できる可能性もある．

被害対象の電磁的記録がクラウド上に保存されている場合は，当該クラウドサーバからどのような電磁的記録が収集できるかを把握しておく必要がある．当該クラウドサーバへのアクセス履歴や認証履歴，削除されたデータの復元などの機能が存在するかの把握である．特に，クラウドサービス提供事業者が提供するサービスが利用金額によって区分けされている場合，認証履歴しか保存されない安価なサービスも存在するため，契約しているクラウドサービスがどのレベルの履歴等を提供しているかを事前に把握しておくことが望ましい．

証拠保全の実施

これまでは，痕跡データが残存している可能性が少ない点について述べてきたが，ここでは，マルウェアに感染した被害端末を証拠保全する際の手続きについて解説する．

証拠保全は簡単にいえば HDD/SSD の物理コピーであり，この物理コピーを実施するまでの準備が必要になる．証拠保全において，保全対象物の状態によってはより多くの情報を保全できる可能性があるが，不用意な手順によって有意義な証拠が散逸しないように留意する必要がある．

たとえば，保全対象物が，起動中のパソコンであった場合，パソコン内で起動中のプロセスや接続中のネットワーク構成等，証拠価値のある情報が存在している可能性が高いが，これらは電源をオフにした時点で失われる揮発性情報である．したがって，電源をオフにする前に，揮発性情報を取得するコマンドの入力やメモリ・ダンプを実施するかどうかなど，必要な措置を検討すべきである．ただし，コマンドの入力やメモリ・ダンプを実施したことにより，保全すべき状態が変更されることには留意すべきであり，変更されることを把握した上で，それでもコマンド入力やメモリ・ダンプを実施した方がより被害実態の解明に寄与するかを判断して行う．

無線 LAN や Bluetooth を含むネットワーク情報や起動中のプロセス一覧を画面表示させて写真撮影するなどして保全する手法も有効である．

その他，注意すべき基本的事項としては以下のようなものが挙げられるため，これらのメリットやデメリットを考慮して実施する必要がある．

①起動している状態を強制的に電源オフにすることで，プログラムやファイルが破損し，読み取れなくなる可能性がある
②強制的に電源をオフにせず，通常の終了処理をする場合，終了作業によって HDD/SSD 内の各電磁的記録が書き変わったり，起動時に動作していたアプリケーションに関する情報が取得できなくなったりする
③通常の終了処理をする場合，主記憶装置（メモリ）の不足分を補うために使用されるページファイルまたはスワップファイルと呼ばれる仮想メモリが解放される可能性がある
④OS の機能等により HDD/SSD 内の電磁的記録が暗号化される設定になっている場合には，電源をオフにしてしまうと，復号されている状態を維持できない（暗号化状態を復号できなくなる）可能性がある
⑤ノートパソコンの場合，完全に電源をオフにするには，電源コードを抜くだけではなく，バッテリーパックを外す必要がある
⑥スマートフォン等のモバイル機器では，常に外部とネットワーク接続されていることにより，遠隔操作で情報を改変または消去されるおそれがあるため，機内モードに設定する等，ネットワークから遮断する

このほかにも犯罪者による証拠隠滅のため，特定の操作をしないで端末を操作した場合には自動的に端末内の電磁的記録を消去するようなプログラムが組み込まれている場合も想定される．

証拠保全の準備が整えば，物理コピーを実施する．複写（コピー）先に用いる HDD/SSD は，あらかじめ書込みや読込みに不具合がないかを確認し，データが存在しない状態にしておくために一定の値(E5 など)やランダムな値を書き込んでおくことは当然として，コピー元の HDD/SSD に対しては，複写作業により動作記録等の追加書込みや書換えが行われないように書込防止装置等を用いて実施する．

コピーが終了した後は，コピー元とコピー先のハッシュ値を確認するが，このハッシュ値が一致せず，同一性を担保できない場合には，確認時の状況の写真撮影等を行い，同一性を担保する．

作業の実施者は，作業の管理者，所属先，取扱案件名や案件番号，作業に用いた機器のシリアルナンバ，ソフトウェアやファームウェアのバージョン番号等を記録し，作業時には，各デバイスのラベル表示（メーカ，型番，モデル名，シリアルナンバ，セクタサイズ，総セクタ数，記憶容量），作業内容および詳細設定情報などを作業状況メモなどとして残しておく．

上記のような証拠保全は，前述したように保全対象となる HDD/SDD を丸ごとコピーする作業である．この作業は物理コピーとも呼ばれ，対象となる端末の HDD/SSD にインストールされた OS やプログラム等も丸ごとコピーすることになる．この際，著作権との関係が問題になり得るが，マルウェア等の被害に遭った HDD/SSD の OS やプログラム等について，被害当時の状況を保全するためにコピーし，第三者に調査解析を行わせるなどの場合，プログラムの実行等によってその機能を享受することに向けられた利用行為ではないと評価できるため，著作権法 30 条の 4（著作物に表現された思想または感情の享受を目的としない利用）に該当し，著作権侵害には該当しないと考えられる．

解析の実施と犯罪者特定の困難性

被害に遭った端末を特定し，証拠収集および証拠保全を行い，各種履歴等，痕跡データを解析して得られた結果から，サイバー犯罪に用いられた IP アド

レスや接続されていた端末，悪用されたサービスのアカウント等を特定する作業を実施する．

近年のサイバー犯罪では，スマートフォンやパソコン等の端末を用いて作成したドキュメントファイルや画像・動画データのほか，さまざまなイベントデータが電磁的記録として保存されているため，これらの解析を実施して被害実態を把握する場合もある．また，多くの機器が，他の機器と連携するためにネットワークに接続されるようになってきており，リモートで接続可能な監視カメラやインターネットに接続可能なテレビ，あるいは HDD レコーダ機器など，IoT（Internet of Things）機器に記録された電磁的記録も解析対象に含まれる場合がある．

さらに，新型コロナウイルスの影響も相まって各種のコミュニケーションツールの導入が加速度的に進んでおり，いまや多くの Web 会議ツール，SNS ツール等が多様化している．

このような実態に鑑みると，まずは，証拠として保全するのは，サイバー犯罪の被害に遭った端末を対象として実施することになるが，当該端末に残存する痕跡データはサイバー犯罪全体の一部である．そのため，痕跡データを解析して得られた結果から被害実態を解明するための電磁的記録を収集する必要があるが，この作業がいかに困難であるかを理解していただけたかもしれない．

サイバー犯罪の被害を受けた端末の解析から，仮に接続元 IP アドレスが特定できたとしても，犯罪者に辿り着くためのその後の証拠収集に支障を来す場面も多々存在する．たとえば，接続元 IP アドレスが Tor（The onion router の略称）の Exit（出口）ノードであった場合，Exit ノードにアクセス履歴等が保存されるような機能が付加されていなければ，攻撃元を辿ることがきわめて困難となる．接続元 IP アドレスが発展途上国のホスティングサーバであった場合，当該国の捜査機関と連携できない可能性があり，また，海外の匿名プロキシサーバが接続元 IP アドレスであった場合には，当該プロキシサーバを利用した本来の接続元に関するアクセス履歴が存在しないため，攻撃元を辿ることはできなくなる．

日本国内であっても，公衆 Wi-Fi や他人の居宅内に設置された無線 LAN のアクセスポイントから接続されていた場合には，攻撃元を辿ることが非常に困難になる．

ほかにも，端末に痕跡が残らない海外のコミュニケーションサービスが使用されていれば，当該サービス提供事業者から接続元に関する履歴の提供を受けられなければ攻撃者を特定することが困難であるし，Telegram のような秘匿性が高いメッセージアプリが使用されていた場合も同様である．

技術革新の功罪

ICT 技術の革新によって，便利な世の中になるが，人々の行動履歴がデータ化され，これを悪用されればプライバシー侵害にもつながることから，セキュリティの向上が図られ，痕跡データが残らなくなっている．スマートフォンなどの端末はパスコードや指紋認証が必須になり，一定回数間違うと初期化され，端末内の電磁的記録を抽出できなくなる．端末内の電磁的記録全体に暗号化が施されていれば，削除された電磁的記録の復元すらできなくなる．このような状況下はプライバシー保護のためには有益であるが，犯罪被害の実態解明を困難にすることにもつながる．

サイバー犯罪の犯罪者を捕まえて起訴するためには，DF を意識した証拠収集，証拠保全が必要になるが，そもそも証拠として収集できない電磁的記録が数多く存在し，泣き寝入りとなっている事件も多数に上る．これはセキュリティと犯罪捜査のジレンマともいえるかもしれないが，技術革新によって犯罪者を野放しになってしまう状況について今一度再考してみてもよいのではないだろうか．

（2021 年 5 月 30 日受付）

■北條孝佳　ta.hojo@nishimura.com

弁護士．元警察庁技官．企業の危機管理，サイバーセキュリティ対策の専門家．政府の各種委員を歴任，都道府県警察や経営者向けの講演，書籍の執筆，SeckHack365 のトレーナーやセキュリティキャンプ講師等，幅広い活動を行っている．