具体例に学ぶ

e法務ソリューション

デジタル訴訟社会を生き抜くために

vol.6

text by
佐々木隆仁
AOS Technologies 代表取締役社長
▶eLaw.jp

強固なセキュリティで守られたフォレンジックラボで行われる証拠調査。データ復旧のパイオニアとして、10年以上に渡って培われた高度な復旧技術が駆使されるフォレンジック調査の心臓部。

訴訟に強いデジタル証拠開示とは

情報漏洩問題とデジタルフォレンジックの今

大きな注目を集める情報漏洩問題

2011年2月、NHKのドキュメンタリー番組「追跡！AtoZ」で、情報流出の問題が大きく取り扱われました。放映タイトルは「メガリーク～情報流出の闇を追え」。内容は、高度情報化社会に潜む情報流出の危険性を指摘するとともに、情報流出を防ぐための防衛策を紹介するというものです。

番組制作には弊社も全面的に協力。デジタルデータ特有の「外部へ持ち出しやすく、流出させやすい」という特性が、企業の存続に関わるほどの打撃を与え得るという事実に、視聴者の方々は衝撃を受けられたようです。

放映からおよそ2か月後。プレイステーション3とプレイステーション・ポータブルのネットワークである「プレイステーションネットワーク（PSN）」に何者かが不正にアクセスし、7700万件（最終的には1億件）にもおよぶ個人情報が流出したとソニーが記者会見を行い、被害者に謝罪しました。流出したと思われる個人情報は、住所、氏名、性別、生年月日、メールアドレス、PSNのログインパスワードやオンラインID。さらに、過去の買い物履歴や請求先の住所を含むプロフィールデータ、クレジットカード番号、パスワードの照合質問なども含まれた可能性が高く、史上最悪の情報流出事件と呼ばれました。

元役員による顧客情報漏洩事件の顛末

私たちの暮らしは、PCや携帯電話、スマートフォン、タブレット型端末といったデジタルデバイスに囲まれ、幸か不幸か、かつてはハッキング技術がなければできなかったようなことも、たやすく行うことが可能となりました。「外部へ持ち出しやすく、流出させやすい」というデジタルデータの特性を利用すれば、機密情報のファイルをメールに添付したり、USBメモリへコピーしたりするだけで、「いつでも」「誰でも」「簡単に」情報をリークすることができるのです。

弊社が扱った事例をご紹介しましょう。元役員による顧客情報漏洩事件です。これは、A社を退職した役員Yが、退職前に顧客情報を持ち出し、退職後にA社の顧客を次々と奪い、その結果、A社の売上が大幅に減少してしまったという事件です。

A社は、Yが使用していたパソコンを調べ、顧客情報を持ち出した痕跡を探したのですが、当然、既にデータは削除されていました。そこでA社は、弊社にデジタルフォレンジック調査を依頼。調査員が復元したデータからは、会社からYの個人アドレスに、顧客情報が転送されていたことが分かり、A社はYを提訴。デジタルフォレンジック調査によって検出されたデータが決定的な証拠となり、A社は勝訴したのです。

フォレンジック調査の手順とは？

デジタルフォレンジックは、証拠保全、解析、報告という三つの手順で構成されています。最初に行うのが、調査の対象となるハードディスクや携帯電話などの保全。ハードディスクや携帯電話のデータが改変されないように専用機器で保全したうえで、同じ内容を複製し、複製されたデータを対象に解析を行います。

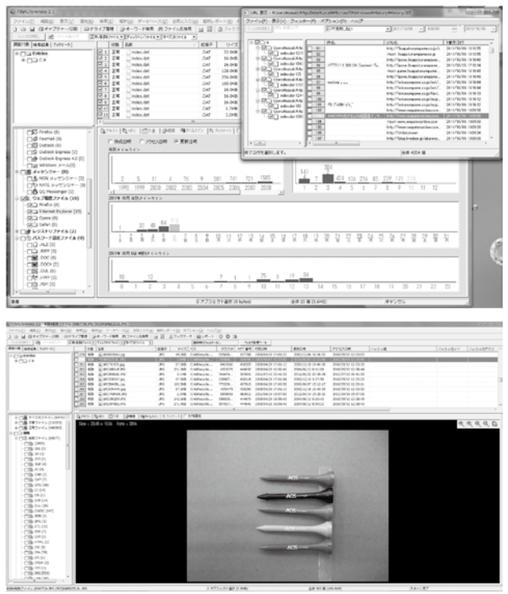
オリジナルデータの保全は、最重要事項のひとつと言ってよいでしょう。デジタルデータは変質しやすく改変が容易です。つまり、保全を行わないとデータがオリジナルのままなのか、改変されたものなのかが不明瞭になってしまいます。その結果、法的な信頼性が低く、証拠として採用されなくなってしまうケースが多々あるのです。

次に保全が終了すると、証拠となり得る情報を抽出・解析する作業に取りかかります。このとき重要なのが、削除されたデータの復元。とはいえ、一口に復元といっても、大きく分けて「浅い復元」と「深い復元」があります。前者は、削除ファイルの復元で終わってしまうケースがほとんど。技術的にはUndeleteと呼ばれるもので、意外と簡単にできてしまいます。

弊社が行っているのは後者。さらに深いレベルでの復元を実施しています。まず、データ修復のために復元すべきファイルを探し出します。それら回収ファイルには、Word書類を示す「.doc」「Excel書類を示す「.xls」、画像ファイルを示す「.jpg」などといった拡張子が組み込まれています。それを丁寧に読み込み、証拠となるデータをじっくり探っていくやり方です。同じハードディスクや携帯電話を対象にしたとしても、専門家としての高度なスキルを持っているかどうかで、証拠の出方は違ってくるのです。

削除されたデータこそ重要な証拠

弊社が提供しているパソコン用フォレンジックソフトが「ファイナルフォレンジックス」です。前述の「元役員による顧客情報漏洩事件」においても大いにその機能を発揮してくれました。データ復元はもちろん、データベース復元、保全機能、偽装されたファイルの検出、分析レポート機能など、デジタルフォレンジックに必要な機能がひと通り組み込まれているのが特徴です。例えば、復元されたファイルを日付別・時間別、拡張子別に分析したり、場合によっては過去5年間のウェブ閲覧の履歴を復元することも可能です。係争中の裁判で、重要な証拠となり得るようなデータが出て一気に和解へ進むというパターンが増えてきました。その一方、社内で独自にパソコンや携帯電話を調査し、「証拠が見つからない」とあきらめるケースも多いように見受けられます。デジタル証拠を開示できるかどうかは、企業や各種組織にとって運命の分かれ道。専門家によるデジタルフォレンジックをおすすめするゆえんです。



（上）ウェブ閲覧履歴。たとえブラウザ上の履歴が削除されても、保存されたログから履歴を復元することができる。（下）画像復元機能。削除された画像も、高度なログ解析技術で復元することが可能。