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. 8

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

本格化するフォレンジックツールの機能と操作性

広がるニーズに対応するソフトウェア開発の歩み

犯罪調査の現場で使われ続けてきた10年

前回の連載では、パソコンや携帯電話、スマートフォンの普及に伴い、こうしたデジタル機器が犯罪に悪用されるケースが急増していることを指摘しました。弊社への調査依頼も増加する一方。その際、もっとも重要なのが、デジタル機器に保存されているデータの解析です。

「ファイナルデータ」をリリースしたのは2000年1月。それまでは、データ復旧ソフトというカテゴリ自体が量販店の店頭にありませんでしたが、今では、大手の量販店に行くと、データ復元ソフトという棚があります。ファイナルデータは、このデータ復元ソフトの市場で12年連続して実売シェアNo．1（BCNランキングによる自社調べ）の実績を上げました。このファイナルデータにいち早く注目したのが警察などの捜査機関でした。警察向けには、市販のファイナルデータではなく、ファイナルデータプロフェッショナルという特別仕様のソフトを10年以上にわたって提供し、実際に、さまざまな犯罪捜査の調査で活用されてきました。

フォレンジックツールの機能の移り変わり

ファイナルデータは、いくつかの機能強化を行っています。そのなかで、もっとも要望が多かったのが、画像データの復元です。00年代後半になると、デジタルフォレンジックへの関心が一気に高まります。09年11月からは、東京地方検察庁を皮切りに検察庁への納入がスタート。現在、北は札幌から南は福岡まで、全国12の検察庁がデジタルフォレンジックのための専用復元・解析ソフトを使用しています。

11年12月には、金融庁（証券取引等監視委員会）に、デジタルデータ証拠開示ツールとして、「ヌイックス」をAOSが導入しました。ヌイックスは、オーストラリアで開発されたeディスカバリツールで、米国の政府機関などで使われています。

通常、証拠となるデジタルデータは容量が巨大で、すべてのデータを精査するには多大な時間と労力が必要になります。ヌイックスは、そうした課題を解決するために開発されたソフトウェアです。あらかじめ調査に必要とされるであろうデータの種類や作成・変更日時を指定しておくことで、重要なデータのみを収集することができるのです。ヌイックス自体は軽量で、USBメモリなどにインストールしておけば、パソコンに接続し、現場で直接、データを収集し、自動保全することも可能となります。

急速に広がるデジタルフォレンジックへの関心

警察庁から検察庁、そして金融庁へという流れは、まさにデジタルフォレンジック調査への関心が、急激に高まっていることを示しているでしょう。アメリカに比べると遅いスタートではあるものの、12年は、日本におけるeディスカバリ元年と呼ばれることになるかもしれません。

同時に、それは、たとえITに関する専門的な知識がない方々でも、簡単に扱えるものが求められるようになってきたということでもあるのです。聞くところによると、あるフォレンジックツールは、専門家向けのインターフェースを採用したため、非常に扱いづらく、導入した官公庁や企業ではほとんど使用されることもなく、眠ったままになっているとか……。その点、弊社は、もともとコンシューマー向けの製品を開発してきたという経緯もあり、ソフトウェアの操作性については、徹底的な検証を行っています。

官から民へ止められない流れ

デジタルフォレンジック調査への関心の高まりは、官公庁だけではありません。最近は、弁護士の方からの相談も増えてきました。というのも、現在、携帯電話などの調査は、警察が特化したノウハウを持っています（弊社も警察からの依頼で携帯電話の調査を行うことがほとんどです）。つまり、重大な証拠となり得る携帯電話などのデータが、警察側から提出されたものに偏ってしまっています。

こうした状況は不公平ですし、冤罪につながる危険性を指摘する方もいらっしゃいます。ただし、弊社の力不足もあり、世間一般には、まだまだデジタルフォレンジックの重要性が浸透していないというのが実情です。ある案件では、2年かけて、ようやく弊社の存在を知ったという方がいらっしゃいました。そのときは携帯電話から削除されたメールのやりとりを復元したのですが、「もっと早くデジタルフォレンジック調査のことを知っていたら、2年間、苦しむことはなかったかもしれません」とおっしゃっていたことが、いまでも印象に残っています。

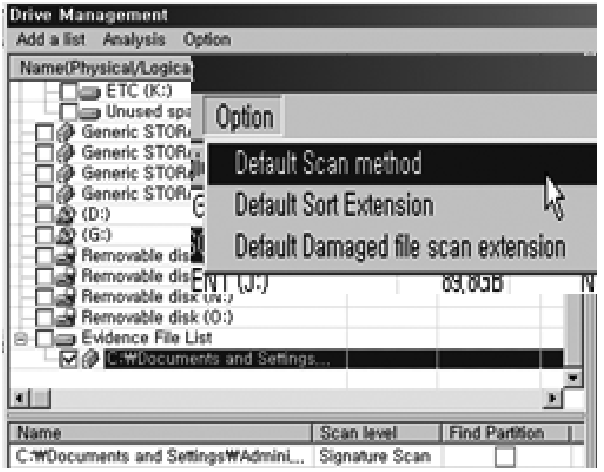
増え続ける内部不正調査

ここ最近は、企業内部の不正調査の依頼も非常に増えています。特徴的なのが、不正に手を染める人々も、それなりの対応策を練っているということ。

ある上場企業で、元役員のパソコンを調査したときは、専用のデータ抹消ソフトを利用した形跡がありました。つまり、復元することができないのです。このように調査対象の相手が専門的な知識を持っている場合の調査は困難を伴います。

別の企業では、役員のメールがすべて、外部のウェブメールに転送されるように設定されていました。さすがにこれはシステム管理者でなければできない芸当です。情報システム部門の人間が関わっていることは間違いありません。

残念ながら、技術が進歩すれば、それに合わせて悪知恵を働かせる者も出てくるということなのです。こうした憂うべき事態を招かないためにも、事後調査だけでなく、操作ログを自動的に記録するソフトの導入などの事前対策にも目を向けていただければと思います。



データ復元機能を持つ「FINALDATA」と、さらにデータの保全、偽装ファイルの検出、分析レポート機能を持つ「FINAL Forensics」は、捜査機関での利用実績を持っている。写真は、削除されたPC内のデータを復元する際の操作画面。