5B-5

情報法科学（Information Forensics）体系化を目指して

向山　宏一†　　内田　勝也‡
情報セキュリティ大学院大学†‡　情報セキュリティ大学院大学†‡

１．はじめに

国内でも情報法科学の重要性が認識され始めてきたが、情報法科学は企業・組織における監査の延長としての観点から、裁判対応まで考えることが大切であろう。また、裁判証拠として考える場合、国内だけでなく、海外との連携も考慮する必要がある。

情報法科学の体系化を行うために、どの様なことを考慮する必要がある考察した。

２．情報法科学の定義

インターネットの進展と共に、企業・組織内のコンピュータネットワークは外部ネットワークにも繋がった。また、企業・組織内では一人一台のコンピュータ利用が当然になり、更にインターネットの普及により、外部から組織内のコンピュータへのアクセスも増大している。このようなネットワークユーザの増大や情報資産の重要性の増大により、企業・組織内の情報資産への不正アクセス、データの改竄等の問題も増大している。

情報法科学は、企業・組織の保有している情報資産に対する事故・事件が発生した際、そこに残された痕跡を探しだし、明確な証拠（Evidence）として報告することを目的とした、一連の活動を対象とする考え方である。

３．情報法科学の目的

情報法科学の目的は、企業・組織の保有するコンピュータシステムや情報資産に対して、なんらかの問題が発生した、もしくは発生する徴候が認められた場合に、その事象を明らかにするための証拠を収集・分析し、報告することにある。

情報法科学は、事象に対しての善・悪や公正・不正の判断を行うことはない。報告された証拠に対する判断は、決められたルールに則って下されるべきものであり、ルールには法律や企業・組織の規定・規則などがある。

報告された証拠には、その利用目的により以下のようなものが考えられる。

（１）刑事訴訟に使用される証拠
（２）民事訴訟に使用される証拠
（３）企業・組織の規定・規則違反の証拠
（４）企業間の契約条項違反などの証拠

一般的な企業・組織で、法的側面、特に刑事事件的な対応が必要と考えられる場合には、独自の対応を行うべきでなく、法執行機関へ連絡し、その指示に従う必要があり、これは殺人事件等への対応と同じである。

また、企業・組織では、就業規則やセキュリティポリシーなどを遵守させるために、従業員、取引先などに対して、それらをきちんと教育・周知させることが必要であり、教育・周知がされない状況で証拠収集等を行う場合には、企業・組織側が訴訟をおこされる場合もあることを認識すべきであろう。

４．情報法科学のライフサイクル

情報法科学における情報収集、分析、報告の過程は、以下の様なサイクルで活動を行うべきであろう。

（１）計画段階

証拠収集、分析、報告のポリシーや手順・手続きを定め、また情報法科学実施要員の確保、及び教育訓練を実施する。

要員確保には、以下の点を明確にする。

- 必要な技術・知識などは職務定義書で明確にする。
- 最低限の知識・キャリアパスなどを明確にする。
- チーム構成を明確にする。

また、情報法科学実施部門に対しては、

- 正規のソフトウェアライセンスの準備
- 必要十分な経費（機材・ソフトウェアライセンス・教育・各種更新費用）

が充分に確保されていることが重要である。

（２）証拠の収集

収集された証拠は完全でありかつ検証可能な状態で記録されていなければならない。そのため収集時には、その取扱に十分注意すべきである。

報告書には、機器の配置や位置関係なども必要になるので、証拠能力の有無を問わず写真などの記録を残しておくべきである。そのため付

「Systematizing of Information Forensics」
†「Kouichi Mukouyama・Institute of Information Security」
‡「Katsuya Uchida・Institute of Information Security」

箋紙に記述されたパスワードや、机上に置かれたメモなどのアナログ情報も注意して収集すべきである。
収集すべき証拠が保持されている媒体などは以下のようなものがあり、これらの操作方法、データの保持方法などに習熟しておく必要がある。

・ハードディスク（含可搬型 HDD）
・フロッピーディスク
・CD-ROM、DVD
・パームトップ、PDA、ポケット PC
・バックアップテープ
・ファイルサーバ、電子メールサーバ
・携帯電話
・デジタルカメラ
・メモリー（SD カード、コンパクトフラッシュ、USB メモリー）
・ボイスメール
・ＦＡＸ
・MP3 プレーヤ等
・コピー機など

（３）証拠の分析

収集された証拠を分析する手法には以下のものが考えられる。

① タイムフレーム分析

ファイルなどが作成・修正されたタイムスタンプや、セキュリティログ・アクセスログなどを分析することで、その時間に行われた行為を明らかにする分析手法。

イベントの発生時刻と個人の関係を明らかにする際に有用と考えられる。

② データ秘匿分析

パスワード設定やファイルの暗号化などの行為は、ある行為やその痕跡を秘匿しようとするものである。秘匿されたデータの検出・回復を行うことにより不正行為者の残した情報を明らかにできると考えられる。

③ アプリケーションとファイル分析

OS の種類や適用されているパッチ、導入されているアプリケーションの種類などを分析することにより、不正行為者が行った行為を特定することが可能であると考えられる。

（４）報告書の作成

報告書は、以下の要素を含んでいることが必要である。

・ 報告書は人が読め、包括的であること。
・ 修復、フォーマット変換、復号などの段階があれば明示する。
・ 信頼できるソフトウェアを利用していること。
・ 知識・技術を持った捜査者が対応していること。

５．情報法科学の裁判対応

インターネットを介して、犯罪行為を行った際には「サイバー犯罪条約」（Convention on Cyber-Crime）で取り締まれるが、犯罪行為はその行為が発生した国の法律によって罰せられる（属地主義という）。 しかしながら、この条約の批准国の中にも、国内立法が終わっていないものや、細部で整合が取れていないものもある。そのため情報法科学で収集した証拠も、各国の捜査・法執行当局に有用な情報を確認し、網羅しておく必要がある。

６．情報法科学の体系化

今までみてきたように情報法科学は広範な分野の知識・経験・技能をもった要員による対応が必要である。
そのため、以下の分野に関して体系的な知識の習得、経験が必要である。

・コンピュータ科学
・OS・アプリケーション
・ネットワーキングプロトコル
・各種ハードウェア
・周辺機器／オフィス機器
・インシデント・レスポンス対応
・情報セキュリティマネジメント
・法律
・規格・標準
・脆弱性情報
・ソーシャルエンジニアリング
・レポーティング能力
・業界情報
・業務知識 など

このような知識を、机上だけではなく実際に利用し、実務経験を積んでいくことが要員確保の道であり、情報法科学を体系化する際に必要な要素であると考える。

７．今後の課題

情報法科学に必要な分野について、更に詳細な内容に落とし込む必要があると考えている。

参考文献

(1) 「Forensic Examination of Digital Evidence: A Guide for Law Enforcement」（http://www.ojp.usdoj.gov/nij/pubs-sum/199408.htm）
(2) 「Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations」（http://www.cybercrime.gov/s&smanual2002.htm）