3.3. デジタルフォレンジック

デジタルフォレンジックは、過去に起こったインシデントを科学的に立証するための証拠を保全・収集・分析することを意味する言葉です。この言葉が重要になって来た背景には最近の ICT 技術の進化とインターネット利用の目覚しい発展によって犯罪そのものが主として PC やサーバ等のコンピュータを介して行われるようになって来たためです。それで犯罪捜査においても ICT 技術を駆使して、その捜査能力の向上が必要と言えます。また情報内部統制や 2007 年 9 月 30 日までに完全施行された JSOX の存在もそれに大きく関連しています。

例えば、Web アクセスや E-mail のやり取りそのものが捜査対象になるということです。それらのやり取り、すなわち通信内容などを追跡するためには、サーバや PC 等の情報機器のログやシステムの状態が記録されたメディアを詳細に調査解析を行う技術が必要となります。大学が関係している事例としては、ネットワークストーカーの犯罪捜査への協力としてメール送信元に関するログを提出依頼されたケースや大学内のフィッシングサイトによって被害が発生したため Web サーバのログを提出し犯罪捜査へ協力、個人情報漏洩時のアクセスログの提出等が事例としてあがっています。

さてデジタルフォレンジックにスムーズに対応するためには、Web や E-mail などのメジャーな通信内容はすべてある一定期間保存するということになります。膨大なメールや Web アクセスを記録するとなるとそれなり資源が必要となります。例えば米国の企業においては、上記の E-mail などの保全収集とそのデータベース化「電子情報開示(e-Discovery)」に関連する規則が、2006 年 12 月 1 日に連邦民事訴訟規則（Fed. Ro Civil Proc.）発効したため、大きな負担となりつつあります。

大学でも恐らく例外なく、同様の事情が発生するかも知れません。あまり喜ばしくないシナリオとして、情報セキュリティに関する事件（セキュリティインシデント）が発生すれば、ICT 部門と総務部門などがその対応（証拠保全・解析・報告）を引き受けざるを得ない状況が発生し、そのような場合ログの部分提出が必要である、ということがありえそうです。しかしそれは、膨大なデータ処理や多様な文字コードへの対応が必要となります。たとえ 1 件でも大変なのに、同時多発的事態となれば恐らくほとんど対応できないと考えられます。

なにはともあれデジタルフォレンジックに対応するためには、情報機器の追跡可能性（トレーサビリティ）を維持しなければなりません。そうすると機関におけるログの保全は必須であり、その期間は判例から 3 年程度と言われています。またログの完全性(Integrity)をなんらかの形で維持する必要があります。例えばログの分散バックアップ保存などが挙げられます。またログを円滑に収集するために PC やサーバ等の情報機器にログエージェントを導入し、ログ収集サーバへログを集中保全管理させます。ログエージェントシステムが導入できない場合は、NIDS などのパケット収集に基づいたセキュリティアプライアンスの導入が考えられます。そして大量のストレージが必要です。

ログの保全技術としては、時系列データであるため時間認証局を使って時間の正当性を確保し、更にログは個人に関する情報やプライバシーを含むため機密性の高い情報資産と考えられるので、保存時に暗号化する必要があります。また既存のサーバや PC などの情報機器のログの完全性の保持も必要です。大学の ICT 部門では、組織全体のシスログ受信サービスも必要かと思われます。いずれにしても膨大なストレージを必要とするものと考えられます。

最後にセキュリティマネージメントの観点から、アウトソーシング化も選択肢の一つかも知れません。デジタルフォレンジックに耐えうるためには、外部評価の視点から大学でそのシステムを持たず、または大学のインフラ的施設の一部として考え、予算と人員を配置して施設部や設備課などにまかせる、ログデータの保全をアウトソーシング化する、解析のアウトソーシング化を念頭におきこれからの ICT 化や設備増強を施すことを考えなければいけません。セキュリティベンダーもアウトソーシングを受け入れる体制を確立すること、新しいビジネスモデルへの転換の必要に迫られていると思われます。