


- 3 . フォレンジック手続ガイドラインの作成のための基礎的研究

日米において証拠の相互利用を可能とするために

Basic Research on Digital Forensic Procedure Guideline for mutual recognition of digital evidence

 キーワード	デジタルフォレンジック、サイバー犯罪、デジタル証拠
Key Word	Digital Forensics、Cyber Crime、Digital Evidence

1. 調査研究の目的

インターネットの特質の一つは、ボーダレスであることであり、インターネット上の犯罪や、インターネットを介して重要インフラに対して行われる攻撃、すなわちサイバーテロについてもボーダレスに生起することから、EU諸国を中心として、これら行為のサイバー犯罪としての犯罪化が求められ、サイバー犯罪条約が策定された。我が国もサイバー犯罪条約の策定に参加するとともに、同条約に署名し、既に発効したところである。現在、それに係る刑法、刑事訴訟法及び国際捜査共助法の改正案が国会に提出され、継続審議中である。

このような状況下において、サイバー犯罪等をなした人間を識別し、そのなした行為を把握し、分析し、証拠を収集し、裁判において適切な処罰がなされなければならない。しかしながら、そのための証拠収集手続き等に関し各国に基本的な差異があれば、証拠が国際的に利用し得ないことも起こりうる。その上、技術の進展に伴い、証拠収集等についても困難性が増すことが予測され、それに対する技術的対応の必要性もますます増加している。そのような観点からの新しい技術の研究・開発も欠かせないものと考えられる。そこで、日米双方のフォレンジック手続の標準的な手順を把握し、その過程で起きる法的な問題点、相互利用の際に問題になる点さらにフォレンジックに関する新しい技術を調査・研究しようというのが、本研究の目的である。

本研究は、独立行政法人科学技術振興機構の戦略的国際科学技術推進事業の一環として、日本側研究者5名((財)未来工学研究所、東京電機大学、千葉大学、京都大学、IT法律事務所)、米国側研究者3名(ミシシッピ州立大学)が共同して実施したものである。

2. 調査研究成果概要

(1) 調査研究項目

日米の法執行機関におけるデジタルフォレンジック実施手法に関する研究

デジタル証拠の日米における証拠法上の位置づけに関する研究

外国で取得された証拠の位置づけに関する研究

デジタル証拠の確保のための次世代技術の研究開発(東京電機大学にて実施)

オークションサイトなどのパソコンデータの消去状況の研究(東京電機大学と共同して実施)

(2) 主な成果

我が国では、法執行機関を除いて、デジタルフォレンジックに関する研究や教育は、大学や大学院、研究機関等においても行われてこなかったのが実情である。また、関連する学会等においても研究発表件数が極めて少なく、この分野の研究者の層の薄さは明らかとなっている。

欧米諸国では、大学等においても盛んに研究が行われている他、ベンダー企業は、世界市場を視野にいれたフォレンジックツールの開発を行っている。また、米国では商務省標準技術局(NIST)や司法省等が評価チームを構成して、ツールの技術的評価を実施しているところである。本調査研究を通じて、警察関係者、研究者及び実務家に対して、米国におけるデジタルフォレンジック研究等の実態を伝えるとともに、過去3回、日米共同研究ワークショップを開催し研究成果を発表し、我が国のこの分野

の研究への取り組みに寄与したところである。

また、日米両国のメンバーは、IFIP(国際情報処理連合)WG11.9(デジタルフォレンジックに関するワーキンググループ)に参加し、海外の研究者との交流を図りながら、先端的な研究状況を把握するとともに、平成20年1月には、日本側研究者が実行委員となり、京都において、WG11.9の国際会議を開催し、この分野における国際的な評価を得た。

本調査研究の主な成果は、以下の通りである。

日米法執行機関におけるデジタルフォレンジック実施手法に関する調査

米国の法執行機関におけるデジタルフォレンジックに係る実施手法、使用されているフォレンジックツール及び警察官に対する教育訓練等の実態を把握し、その状況を、日本の関係者に紹介してきたところ、この3年余りの間に、我が国においても米国製のフォレンジックツールが導入されるなど、デジタルフォレンジックの実施手法の側面では、日米間の差が見られなくなってきた。

デジタル証拠の日米における証拠法上の位置づけに関する調査

米国においては、デジタルデータを証拠として取り扱うために必要な法整備がなされており、デジタルフォレンジックに関する法的な裏付けがなされているといえる。デジタルフォレンジックの技術的展開が法的準則に適合する形で、展開されてきたようである。これに対して、日本では、証拠を有体物に限るため、米国と同様の技術的手法を投入した場合であっても、その法的な裏付けが明確にあるとはいえない。そのため、現在の情報通信技術に適合した刑事訴訟法の改正がまたれるところであり、それによって、デジタルフォレンジックのより適切な展開がなしうものと思料される。

外国で取得された証拠の位置づけに関する調査

デジタルフォレンジックについては、法執行機関における実務において、日米の相違がほとんどなくなってきたと評価されるべきは、上述したが、日本においては、かかるコンピューターから取得されたデータの証拠能力・証明力について法廷において現実に議論されたことはなく、日米間において証拠の相互流用性についての法的な問題としては、不明といわざるをえない。また、日米において専門家証人・鑑定人の利用等についての相違の影響があることも認識された。

オークションサイトなどのパソコンデータの消去状況の調査

フォレンジック技術の一つである消去ファイルの復元技術により、中古のハードディスクの内容が情報漏洩につながる可能性について、中古ハードディスクの購入及びオークションに出品している業者に対するアンケートによって調査した。

店舗で販売されている中古ハードディスクを数台購入し、その内容を調査した結果、これらのハードディスクが消去ツールによって正しく消去されており、昨今の個人情報保護意識の高まりを反映して少なくとも中古パソコンショップ等においては適切な処理がなされている場合が多いことが判明した。一方、オークションにおいては多くの業者が正しく処理をしていると答えるものの、実際のヒアリングや報告書の内容を見る限りファイルの復活可能性に関して誤解が多く、必ずしも正しい削除が行われていない様子がわかった。今後は中古ハードディスク販売に関する一定のガイドラインなどの設置が求められると考えられる。

3. まとめ

情報処理学会等、学会や各種研究会における講演、成果発表を通じて、研究者及び実務家の関心を高め研究者等の増加に寄与した。

前述の国際会議を日本で開催したことにより、デジタルフォレンジックに関する国際交流に寄与するとともに、国際交流の人的ネットワークを構築することができ、今後の持続的な研究交流に貢献することができた。

SOX法、J-SOX法に係るIT統制基盤を構成する手法として、今後、その重要性が認識される契機を作った。