

事後評価報告書

1. 研究課題名：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－
2. 研究代表者名：
 - 2－1. 日本側研究代表者：
佐々木良一（東京電機大学未来科学部情報メディア学科教授）
 - 2－2. 米国側研究代表者：
Rayford B. Vaughn（ミシシッピ州立大学コンピューター科学学科教授）

総合評価： 優

3. 研究交流実施内容及び成果：

本研究交流は、日米双方のフォレンジック（科学捜査）手続の手順を把握し、法的な問題点、相互利用の際の問題、さらにフォレンジックに関する新しい技術を調査・研究するものである。実施内容及び成果については以下のとおりとなった。

(1) 実施内容

i 日本側研究者の米国訪問 3回

ミシシッピ州立大学との研究内容のすり合わせ、並びにデジタルフォレンジックの先進国である米国の研究状況の把握及び企業訪問による民間でのデジタルフォレンジックの活用状況等の現状調査も併せて実施した。

ii 米国側研究者の日本訪問 3回

相互に研究実施状況の確認を行うとともに、米国側研究者の来日に合わせて日米共同研究に関するワークショップを開催し、警察関係者、研究者及び実務家に対してデジタルフォレンジックに関する啓発を行うとともに、研究成果を還元した。

iii IFIP WG11. 9における活動 3回

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。

(2) 研究交流実施成果

i 成果の位置づけ及び類似研究

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。このようなことから、国内で公表されている限りにおいては、類似研究は行われていないものと推察される。

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。本交流研究を通じて、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、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。

ii デジタルフォレンジック体系化の試み

日米共同研究の成果も活かし、デジタルフォレンジック技術の体系化の試みを行い、それを、論文（佐々木良一他「デジタル・フォレンジックの体系化の試みと必要技術の提案」日本セキュリティ・マネジメント学会論文誌、20 巻第 2 号、pp49-61、2006. 9）として纏め上げた。

iii 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

米国側の協力を得て、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、日本の警察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。

【例：デジタル証拠複製時の同一性証明へのハッシュ関数の導入等】

iv 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。

v 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いるという評価されるべきは、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。

vi デジタル証拠の確保のための次世代技術の研究開発

スタンドアロン環境下でパソコンの使用者が不正を行おうとしても証拠性の保持が可能となる技術の研究・開発を行い、3 件の海外講演を行うとともに、論文として纏め上げた（芦野佑樹、佐々木良一「セキュリティデバイスとヒステリシス署名を用いたデジタルフォレンジックシステムの提案と評価」情報処理学会論文誌、Vol. 49、

No. 2、 pp999-1009 (2008年2月号))。また、学生の発表が情報処理学会のセキュリティに関するシンポジウムであるCSS2007において学生論文賞に選定された。

デジタルフォレンジックで重要性が増してきている E-Discovery (電子情報開示) を必要十分に効率よく実施するための研究を行い国際学会で1件発表を行った。

vii 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。

まず実際に店舗で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か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かがえられる。

研究成果の今後期待される効果であるが、

(1) 成果の今後の展開

- i 今後も、得られた知見等を、国内の関係者に還元し、ボーダレスなインターネットを介する犯罪の取り締まり等に寄与する。
- ii 研究開発された成果は、実用化を目指し、官民の情報セキュリティの推進に寄与する。
- iii ネットワーク管理・情報共有・攻撃対応などの観点からするネットワークフォレンジックや悪意あるプログラムに対する脅威測定・対応プログラム作成などに関するソフトウェア・フォレンジックなどの重要性がましているものと思慮される。これらの観点をも踏まえた広義のデジタルフォレンジックへの注目は、重要インフラ防衛の観点から重要なものといえるであろう。
- iv 米国の状況については継続して情報交換を行うとともに、EUについても、状況調査や情報交換を行う。

(2) 社会への波及効果

- i デジタルフォレンジックに係る啓発や成果発表を通じて、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。
- ii 情報処理学会等、学会や各種研究会において講演し、研究者等の啓発に寄与した。
- iii 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。

4. 事後評価結果

4-1. 総合評価

デジタル・フォレンジックは、刑事訴訟、民事訴訟のみならず、最近、企業における内部統制・ITガバナンスにおいても、基盤的役割を担うようになってきた技術的・法的・監査的システムであり、グローバル化が進む中で、日米の間に、情報に対する刑法の相違があることもあって、両国間の交流が不可欠な分野である。代表者の佐々木教授は、早くからデジタル・フォレンジックに対して、総合的な研究を推進してきた研究者であり、本推進事業において、技術と法制度の観点から、米国と交流を重ねたことは、フォレンジック手続きガイドラインの作成に向けて、有意義であった。

しかし、発表論文の殆どの著者は日本人であり、相手国の研究者と共著論文が少ないのが惜しまれる。

4-2. 研究交流の有効性

新しい知の創造に関しては、日米双方のフォレンジック手続き、利用されているフォレンジックツール、電子的証拠の法的な側面等の差異を明らかにすると共に、パソコン使用者の不正行為に対する証拠保存技術の研究開発を行い、多くの論文を発表している。

人材の育成に関しては、平成20年1月に、京都において開催したIFIP WG11.9の国際会議において、日本人研究者7人が発表し、また、情報処理学会コンピュータセキュリティシンポジウム2007論文集で、学生が受賞する等、研究者の育成に大きく貢献した。

研究交流の今後に関しては、IFIPに引き続き参加すると共に、ミシシッピ州立大学を始め、米国との幅広い交流が期待できる。

4-3. 当初目標の達成度

研究交流実施体制は適切につくられ、研究交流は計画以上に積極的に行われた。