事後評価報告書

１．　研究課題名：インシデント情報のモニターおよび分析技術

２．　研究代表者名：

２－１．日本側研究代表者：

中尾康二（(独）情報通信研究機構情報通信セキュリティ研究センター
インシデント対策グループグループリーダー)

２－２．米国側研究代表者：

Farnam Jahanian（ミシガン大学ＥＥＣＳ学部教授）

総合評価：　優

３．研究交流実施内容及び成果：

本研究交流では、セキュリティに関わるインシデントを的確なポイントで効果的にモニターする技術、およびモニターしたインシデントによる影響度、被害予測を求める分析を実施し、さらに将来に向けた起こり得るインシデントの予知を行うことを目指した。

■実施内容

平成１７年から平成２０年にかけて６度の研究会合(うち２回はワークショップ)を行い、ネットワークセキュリティインシデントの観測・分析に関する活発な議論と意見交換を行った。

■成果とその位置づけ

本研究交流を通じて、両研究チームがそれぞれ構築を進めるインシデント分析システムと要素技術の高度化を実現した。日本側は研究交流を通じて広域ネットワークにおける攻撃観測及び分析に関する多くの知見を得、その知見は日本側で独自に考案した統合的なインシデント分析のアーキテクチャ(マクローミクロ相関分析)の構想への重要な基礎入力となった。この研究構想は従来研究で見られる定点観測システムとは一線を画しており、広域ネットワークにおける攻撃観測とその原因となっていると思われるマルウェアの解析、さらには、観測されたネットワーク攻撃とマルウェアを突き合わせることで攻撃の原因特定を行うという内容である。その実現形態として開発中のインシデント分析センターnicterは、アジア最大級のネットワークコンピューティングイベントであるInteropにおける実証実験、国内外の学会での受賞、TVや雑誌等の報道で広く注目されるなど既に多くの成果を収めている。一方、米国側は当初よりネットワーク攻撃観測に重点をおいてIMSの構築を進めていたが、その後、日本側からの上記のような研究成果に大きく刺激され、マルウェア解析(ミクロ解析)をも視野に含めた研究を開始し、ボット解析を含めた多くの成果を収めている。

■目標の達成度

実施内容と成果共に当初の目標であるインシデント情報のモニター技術、および分析技術の高度化を十分に達成したといえる。

研究成果の今後期待される効果であるが、本研究交流によって得られたインシデント分析技術に関する知見は、今後、益々多様化・複雑化が予想されるセキュリティ脅威への対策を行う上で多くの示唆を与える重要なものである。また、インターネットのように国境が明確でない国際的な情報通信インフラにおいて、２つの国に属する異なる観測分析システムが協調的にインシデント情報を共有し、対策技術の検討を行うという研究活動のケーススタディとしての価値も大きく、今後、類似の活動を行う場合のモデルケースとして考えられる。

また、本研究交流を通じて得られた研究者間の人脈は貴重であり、第 6 回会議では、プロジェクト終了後も継続的な連携体制を保つことで日米の研究グループが同意しており、関連分野における更なる成果が期待できる。

４．事後評価結果

４－１．総合評価

極めて緊急な課題でありながら、学術的に扱い難い研究テーマに対して、日米の協力による顕著な成果を挙げている。即ち、ネットワークインシデントの分析に関する観測結果や傾向情報の共有、及び、観測・分析手法に関する日米の意見交換により、両国のシステムと分析技術の高度化を達成している。しかし、多くの研究業績を発表してはいるが、それらは日本側の成果であり、米国側の業績、あるいは共著論文は挙げられていない。

相手国に将来の研究交流を推進する人材が存在するのか、不明な点もあるが、本事業を端緒として、相手国における人脈の開拓も含めて、より活発な連携体制が維持・発展されることを期待したい。

４－２．研究交流の有効性

新しい知の創造に関しては、国内外での多くの学会発表と受賞、Interop における実証実験、ＴＶや雑誌等での報道などを通じて、科学技術の進展／新分野の開拓に成果を挙げている。

人材の育成に関しては、相手国研究者の状況、特に若手研究者の状況が不明であり、研究室訪問や意見交換などを超える共同研究まで発展する人材育成がなされたか否かは判断できない。

研究交流の今後に関しては、プロジェクト終了後も連携体制を継続することが日米間で合意されている。

４－３．当初目標の達成度

ワークショップの開催など計画通り実施された。