平成 28 年 6 月 28 日

平成 28 年度　終了評価書

研究機関　：　KDDI 株式会社、九州先端科学技術研究所（ISIT）、株式会社セキュアブレイン、国立大学法人横浜国立大学、株式会社 KDDI 研究所、ジャパンデータコム株式会社

研究開発課題　：　国際連携によるサイバー攻撃の予知技術の研究開発

研究開発期間　：　平成　23　～　27 年度

代表研究責任者　：　中尾　康二

■　総合評価（5～1の5段階評価）　：　評価4

■　総合評価点　：　23点

（総論）

サイバー攻撃が巧妙化・悪質化するなか、国際連携の枠組も構築した上で十分な実用性を有し、他の研究のスプリングボードになりうる基盤技術を開発するなど、目標を上回る成果を達成したと言える。また、海外拠点における継続的な観測や国際連携の枠組みの活用により、我が国の今後のプレゼンスの向上が期待できる点について高く評価できる。

（コメント）

- ここで開発した技術は他の人が研究を行う上でのスプリングボードにもなりうる。
- 社会インフラとして成長したネットワークの安全性を担保することは極めて有用な課題である中で、不正アクセスの予兆を検出する本研究開発は重要である。
- 本研究で検討すべき課題は多岐にわたり、ネットワークの現状を的確に把握し、予兆に関わる情報を得られたことは有効であると言え、今後の研究開発、実利用に展開できるものと考えられる。
- 一部は見送りとなったが、実用性の高い技術については継続開発するだけでなく、海外観測拠点での観測も続けることにより、更なるサイバー攻撃の兆候把握の能力を獲得できると考えられる。

- 国際連携の枠組みを構築し、今後も連携することで我が国のサイバー攻撃対策技術のプレゼンスを高める事ができると期待できる。
- 巧妙化によりステルス化するサイバー攻撃に対して、その初期段階を捉える技術は世界的に見ても未解決の課題が数多く残っており、その一部とはいえ十分な実用性を有する技術を開発した点については高く評価できる。
- 重要なテーマを扱い、高い技術レベルで研究開発に取り組んでいる。国際展開はある程度できたが、国際連携と言えるまでには達していないのは、残念なところであるが、それを上回る予定以上の技術的成果をあげている。

（1） 研究開発の目的・政策的位置付けおよび目標

（5～1の5段階評価）： 評価4

（総論）

サイバー攻撃が巧妙化、悪質化している中、サイバー攻撃の予兆検出のための基盤技術の開発、国際規模での検出システムの構成及び実証実験を行う本研究開発はますます重要性が高まっており、情報通信社会にとって重要な課題に取り組んでいるものであると認められるとともに、今後の更なる進展が望まれる。

（コメント）

- サイバー攻撃はますます激しさを増しており、今後、2020 年東京オリンピック・パラリンピックに向けて巧妙化、悪質化が進むものと予想される。その対策の基本となる本研究開発はますます重要性が高まっていると考えられる。
- サイバー攻撃による被害は増加を続けており、企業や個人も金銭的な被害を被るようになっている。そのため、サイバー攻撃を初期段階で検知する技術を産官学共同で解決する意義は極めて高い。一方で、サイバー攻撃の特性上、後手に回らざるを得ない現状は続くと考えられ、予知という課題設定には若干の無理があったと考えられる。
- 「サイバー攻撃の予兆」といった難しい課題ではあるが、情報通信社会にとって重要な課題に取り組んでいる。
- 当該研究は今や社会基盤となったインターネットの安全性に支障をきたしているサイバー攻撃の予兆検出のための、基盤技術の開発、及び国際規模での検出システムの構成及び実証実験を行うものである。これらの研究課題は国が推進すべきであることは、研究開発開始時点と何ら変わりは無く、更なる進展が望まれる。

(2) 研究開発マネジメント(費用対効果分析を含む)

(5～1の5段階評価) : 評価4

(総論)

課題間の連携が十分に取られているとともに、NICT などの国内組織と連携している点について評価に値する。特に、データ共有の枠組、センサーの共有については相乗効果が得られたと考えられる。また、費用についても研究課題に応じて的確に利用されていると判断できる。

(コメント)

- いろいろな形で技術的成果を挙げており、コスト・効率良く研究を進められたと考えられる。
- NICT など、国内組織との連携についても評価でき、サイバー攻撃への対応として適切だと思われる。
- 一つの仕組みとしては完成していないが、それぞれの研究分担者が他者によって開発された技術を参考にする連携は十分であったと言える。特に、データ共有の枠組み、センサーの共有については相乗効果が得られたと判断できる。
- 課題間の十分な連携がとられ、目標は達成されており、また費用も研究課題に応じて的確に利用されていると判断できる。これらの観点から研究計画、研究体制は十分であったと考えられる。

(3) 研究開発成果の目標達成状況

(5～1の5段階評価) : 評価4

(総論)

ハニーポットを用いて早期攻撃の予兆を捉える有用な手法を開発し、それらの有効性を実ネットワークで示すなど、十分な実用性を有する基盤技術を確立しており、目標を上回る成果を達成していると言える。また、当初の予定にはなかったIoTセキュリティについても取り組んでおり、一定の成果を得たことも評価に値する。

(コメント)

- 国際連携について、一部予定通りでないところもあったが、それを上回る予定以上の技術的成果(ハニーポットの改良による P2P ボットや IoT ボットへの対応など)を挙げている。
- 予知とは言えないが、サイバー攻撃を初期段階で察知するための検知アルゴリズムの開発、データ共有の仕組みなど現在考えられうる成果として十二分のものであった。
- 当初予定にはなかった IoT セキュリティに取り組み、一定の成果を得たことも評価に値する。
- ポータルを構築し、評価試験を実施しており、不正アクセス予兆の検出の実例を示している点も評価できる。
- 「サイバー攻撃の予兆」という難しい課題に対し、一定の知見を得ており限定的ではあるが、高いレベルの成果が得られていると考えられる。
- いくつかの研究成果についてはレベルの高い国際研究集会で発表されており、非常に高いレベルにあると評価できる。
- 対象とすべき膨大な情報を取り扱わざるを得ない状況で、アタックの予兆を捉える有用な方法を開発し、それらの有効性を実ネットワークで示すことで、基盤技術として確立している。

(4) 研究開発成果の社会展開のための活動実績

(5～1の5段階評価) : 評価4

(総論)

国際的な学術論文誌に採録されるなど、研究成果としては十分であると言える。また、検出された予兆情報を関連機関に提供し、社会展開のための活動は十分であると言える。

(コメント)

- 海外発表、論文発表などは非常に精力的に行っており、レベルの高い学会での論文採択を達成している。一方、特許化、成果の社会への展開は今一歩である。
- いくつかの研究成果については、レベルの高い国際学会にて発表されており、非常に高いレベルにあると評価できる。
- 実環境で検証を行ったり、国際的な学術論文誌に採録されるなど研究成果としては十分であると言える。
- 国際連携について、他国との調整に予想以上の時間を要し、社会展開が十分ではなかった点は悔やまれる。
- 研究成果は学会誌論文及びシンポジウム(査読付き)として公表されている。
- 成果の社会公開なども計画通りに実施されている。
- 検出された予兆情報を関連機関に提供し、社会展開のための活動は十分である。
- サイバー攻撃予兆情報のシステムは、現状ではある程度成功しているが、十分機能しているとは思えない。

（5） 研究開発成果の社会展開のための計画

（5～1の5段階評価）： 評価3

（総論）

本研究開発の一部の機能はNICTに引き継がれ、各研究項目について継続研究が実施できる体制が検討されており、今後も引き続き研究が行われることにより、本研究開発において得られた知見が実用レベルになりうるものと期待できる。

（コメント）

- NICTのプロジェクトとのリンク等社会への次の展開を検討している。
- 今回開発した一部の機能がNICTに引き継がれたり、本研究課題に取り組んだ者が自己資金により継続して研究開発を続けることにより、本研究開発において得られた知見が実用的なものとなりうるレベルになると期待できる。
- 本研究開発のポータルサイトについて、研究開発の終了と共に閉鎖してしまった点は残念である。
- プロジェクト終了後の計画が十分に考察されていない印象を持った。
- 各研究項目において継続研究が実施できる体制、組織づくりが検討されており、この体制のもと研究が行われるものと考えられ、期待できる。