令和３年 12 月 13 日

令和3年度　追跡評価書

研究機関　　：　富士通(株)、NRI セキュアテクノロジーズ(株)、
国立大学法人名古屋大学

研究開発課題　：　サイバー攻撃の解析・検知に関する研究開発

研究開発期間　：　平成　25　～　平成　27 年度

代表研究責任者　：　津田　宏

■　総合評価

（総論）

行動特性から攻撃を解析・予知する試み等、社会科学と連携する新たな分野の創出につながり、学術的な貢献として評価できる。また、本研究開発をきっかけにコミュニティが拡大した波及効果は高く評価できる。研究開発終了後においては対外発表を継続している点は評価できるが、セキュリティ対策技術が産業として拡大していないことも事実であり、国として継続した支援が必要と考える。今後、本研究によって創出された学術分野を継続展開し、さらなるイノベーション創出や、各課題の成果を結びつけたさらなる成果への発展が期待される。

（被評価者へのコメント）

- 研究計画について、当初の５年から３年に短縮されてはいるが、成果はあり、また、ビジネスプロデューサーの設置など、新たな試みも実施していることは評価できる。
- 人間の行動調査など、行動特性から攻撃を解析・検知する試みなど、リスクへの早期対応だけでなく、

社;会科学との連携する新たな分野の創出につながったことは学術的な貢献として評価できる。生み出された学術分野を継続展開して社会変革をもたらすイノベーション創出を目指してほしい。

- 追跡評価の結果として、本研究開発が国家プロジェクトとして遂行されたことは妥当であったと評価することができる。特に産学連携であった本研究開発が NICT など官における活動との連携につながっており、コミュニティが拡大した波及効果は高く評価して良いのではないか。
- 終了評価時に設定した目標を達成したうえで、終了後も対外発表を継続している点は評価できる。
- 人文科学系を含めた研究者のコミュニティづくりや若手研究者育成の観点でも貢献している。
- 本研究開発のような国家プロジェクトを経ても、まだセキュリティ対策技術が産業として拡大していないことも確かであるので、今後も継続した支援が求められるのではないか。
- 終了評価でも指摘されているが、各課題の成果はあるものの、それらが結びついたさらなる成果へとはつながっていない。

（1） 政策目標の達成状況等

（総論）

本研究成果を国内製品に適用し、性能向上を図り、継続的な売上げに寄与するだけでなく、研究成果の普及活動として、各種対外発表や Interop セキュリティ部門でのグランプリ受賞、研究期間終了後の特許取得など、様々な活動をしていることは評価できる。一方で、定量的な売上げなどの説明がなく、具体的な経済的な効果を確認することができなかった。また標準化については、国際競争力の強化につながる施策の提示がないため、国益に供するための国際標準の獲得等に向けた今後の検討が期待される。

（被評価者へのコメント）

- 本研究開発で得られた機械学習を用いたマルウェア実行検知機能のノウハウを、アライアンスを通じ既存の次世代エンドポイントセキュリティ製品に適用、性能向上を図り、国産製品の売上げに寄与したことは評価できる。
- 富士通においては、サービス移行の流れが顕著で製品市場の立ち上りは遅れ、リモートワーク普及からエンドポイント製品の需要は拡大したものの、内部ネットワーク対策製品の比率は低下した。
- 事業化にあたり、本研究の成果の活用がやや直接的ではなく間接的に留まっているのは、研究期間が短縮された事情を鑑みるとやむを得ないと評価する。一方、副次的な効果は十分得られていると見込まれる。

- 研究期間終了後も対外発表や事業化などが順調に行われており、おおむね期待通りの政策目標が達成できていると評価できる。
- 本研究課題で開発した不正意図検知技術をもとにした標的型サイバー攻撃・内部対策アプライアンスを製品化し、「Interop Tokyo 2015」の「Best of Show Award」セキュリティ部門グランプリを受賞するなど、本研究成果と製品の先進性が業界で評価された。
- 研究期間内に出願した特許が平成 28 年度以降に取得されており、本研究成果の普及に向けた活動の成果が出始めている。
- 「標準化は難しい」と標準化戦略などを一顧だにしない姿勢では、多額の国税を投入する事業としては適切ではないように感じた。特許取得と同様に標準化が難しいのであれば、国際競争力の強化につながる施策を検討して明示してほしかった。国益に供するためには国際標準の獲得などの国益に資する方策を十二分に検討すべきであり、検討が不十分であると感じる。
- 「セキュリティ運用サービスが国の機関や医療関連団体に採用」や「次世代エンドポイントセキュリティ製品のチューニングに適用、性能向上を図ることで国際製品の売上げに寄与」といった記載があるが、定量的な説明（売上げ、販売件数、採用数など）が示されておらず経済的な効果を確認することができない。

（2） 成果から生み出された科学的・技術的な効果

（総論）

利用者の行動特性に着目した ICT リスク判定という視点を提起し、各種学会や国際会議での発表等を行っているだけでなく、NII との連携によるサイバー攻撃の分析の実施などは評価できるが、事業化に至っていない点については引き続き技術開発への取組が望まれる。学術的には、本研究開発が心理学や行動経済学などの人文系分野との連携により新しい学術分野を切り開く先駆けとして貢献した可能性があり、今後の研究集会の継続的な主催等が期待される。マルウェア対策として、機械学習や AI 技術を用いた自動化は重要課題であり、これに関連する学会発表が充分に行われていることは評価できるが、誌上発表数は少なく、学術的な効果は限定的に思われるため、継続した普及活動が期待される。

（被評価者へのコメント）

- 当初目標である「リスクの高い行動を行う人の特定」については一定の技術的成果は得られているものの、事業化につなげる開発に至っていないのが残念である。課題は多いものの重要な研究と思われるので、何らかの形で引き続き技術開発が進められることを期待する。
- 利用者の行動特性に着目した ICT リスク判定という視点を提起し、ヒューマンインタフェース学会や人工知能学会などでの論文発表や国内外の展示会でデモ展示を行った。当該分野の著名な国際会議 SOUPS（Symposium On Usable Privacy and Security）でポスター発表も行った。
- 国立情報学研究所(NII)が運用する、大学間連携に基づく情報セキュリティ体制の基盤(NII-SOCS)において、インシデント・レスポンスの研究成果を組み込んでサイバー攻撃分析を実施している。
- 行動特性から攻撃を解析・検知する試みが新しい研究分野を切り拓く先駆けに役立った可能性があり、心理学や行動経済学などの人文系分野との連携で新しい学術分野を創出する一つの要因となったことは、学術的な貢献として評価される。研究集会を創設したのであるならば、その内容やその後の研究動向を報告してほしかった。この分野の研究集会を主催することなどが今後も期待される。
- 情報セキュリティ対策の向上に利用者の行動特性を利用することに関して、社会的な受容性の拡大、並びに心理学や行動経済学など異分野と連携した研究活動の活性化に寄与している。
- ますます増加するマルウェア対策に対して、機械学習や AI 技術を用いて自動化を進めることは非常に重要な課題であり、既存セキュリティ製品のマルウェア検出の性能向上だけでなく、これに関連する学会発表等が十分に行われていることは高く評価できる。事業の研究の影響力を評価するためには、論文発表数ではなく、当該事業の関連論文等のサイテーションインデックスを調べる必要がある。社会実装が重視されるとしても、誌上発表数が8件であるのは少ない印象がある。誌上発表が8件では学術的な効果は限定的に思われる。

（3） 副次的な波及効果

（総論）

心理学や行動経済学などの人文系分野との連携促進は特筆され、機械学習の取り込み等に加え、NICT との連携によりセキュリティ脅威の検知・可視化技術とマルウェア感染拡大の自動防御を実現することができ、国内製による多層防御の実現可能性を社会に示したことは評価できる。産学官による研究コミュニティの拡大への寄与についての評価は難しいが、我が国のセキュリティ対策技術が産業として拡大するような波及効果につながることを期待する。

（被評価者へのコメント）

- 心理学や行動経済学などの人文系分野の研究者との連携が促進されたことは特筆され、機械学習などを取り入れていることも時代の要請に合致している。
- 研究コミュニティの拡大に寄与した効果は評価できる。ここから我が国のセキュリティ対策技術が産業として拡大するような波及効果にさらにつながることを期待する。
- 「産学官による研究コミュニティの拡大に寄与」の記載があるが、定量的に説明がなく評価が難しい。
- 人文社会科学系を含めた多方面の研究分野が連携するとともに、NICT のセンサーの高度化等による観測機能強化の研究との連携も行い、国内の研究者や研究機関との連携を促進するだけでなく、本研究成果であるセキュリティ脅威の検知・可視化技術とマルウェア感染拡大の自動防御を実現した。本成果は「InteropTokyo2016」で動態展示され、国内製による多層防御の実現可能性を社会に示したことは評価できる。
- 本研究開発を契機に、研究関係者（研究実施者、研究開発運営委員、ビジネスプロデューサー）と継続的な情報交換及び技術交流を推進した結果、企業や学術機関と共に新規プロジェクト（戦略的イノベーション創造プログラム）に参画している。
- 本研究開発を通じ、機械学習に強い技術者の育成も行っている。

（4） アウトカム目標の達成に向けた取組計画の達成状況等

（総論）

ビジネスプロデューサーの設置は、研究開発を自己目的化せず、ビジネス戦略上の判断や顧客目線での産学連携を実現したことは評価できるが、研究開発終了後の国際競争力の強化、学術分野の創出や国民への啓発などについては、総合ビジネスプロデューサーとしての役割が機能していないように思われる。研究成果の普及や啓発活動については、各種学会での発表やイベントへの参加を研究開発終了後も積極的に実施しており、若手人材の育成の観点などでも評価できる。今後、道半ばとなっている事業化や産業への拡大について、継続した取組が望まれる。

（被評価者へのコメント）

- 研究者とは別にビジネスプロデューサーを設置し、政策目標の達成に向け取り組んだことで、研究者の科学的知識と能力に加え、ビジネス戦略上の判断や顧客目線で産学連携を実現しただけでなく、研究開発を自己目的化させないために極めて重要であり、高く評価できる。
- アウトカム目標に向けた体制として総合ビジネスプロデューサーが十分に機能していなかったことが、追跡調査でもうかがえる。メタなアウトカム目標として国際競争力を高め、学術分野の創出や国民への啓発など、本事業終了後も総合ビジネスプロデューサーの役割であると思われるが、機能していないように思われる。事業全体の統一した方向性も明確でなかった。
- 本研究開発に関する活動は、終了評価時に「今後の成果展開に向けた取組方針」に掲げた目標が達成したことを踏まえ完了している。
- 平成 28 年度以降も ICT イノベーションフォーラム 2016 や富士通フォーラム（有楽町）、Fujitsu Forum 2015 Munich で啓発活動を行い、名古屋大学と富士通が研究成果の学会発表や誌上発表を行っているだけでなく、特許出願 10 件、査読付き論文 5 件、査読付き口頭発表 13 件の実績を残しており、研究成果の普及を積極的に実施していることは評価される。
- インシデント・レスポンスに関する継続課題に加え、セキュリティ・ナレッジ構築、機械学習/深層学習システムへの攻撃対策の研究を推進し、成果を学会等で継続的に発信した。
- イノベーションキャンパス in つくば 2015 において、高校生を対象に講義と研究成果を含む展示デモを実施するなど若手の人材育成に努めた結果、本研究開発に携わった人材（研究員、学生）が、国際会議や学会において受賞するなど活躍している。
- 実際の事業化や産業としての拡大については道半ばであるので、継続した取組が望まれる。

（5） 政策へのフィードバック

（総論）

機械学習を用いたマルウェア検知の研究が世界的に始まり出した時期に、国内で最先端の研究に取組、行動心理学や疫学の知見という新たな視点を取入れる等、国家プロジェクトとして妥当な計画と評価できる。メールを利用した Emotet 等の標的型攻撃に対しての有効性や、当初目指していた総合対策基盤の構築に必要な事柄など、当該研究開発から得られた知見については、今後の成果の展開が望まれる。今後、当該分野が産業として国際展開が可能なレベルまで発展することが期待される。

（被評価者へのコメント）

- 本研究開発は国家プロジェクトとして妥当な計画として遂行されたと評価される。
- 研究開発期間当時は世界的に機械学習を用いたマルウェア検知の研究が正に始まっていた時期であり、国の支援の下、各国が研究を進めていたところ、国内で最先端の研究促進を行い、具体的な事業につなげた意味は大きい。
- 外部の学識経験者、有識者で構成される研究開発運営委員会を設置し、委員に、人文社会科学系の若手研究者が参加し、行動心理学や疫学の知見という新たな視点から助言を得たことも評価できる。
- セキュリティ研究者だけでなく、人文社会科学系を含めた多方面の研究分野が連携したプロジェクトに発展した。
- 大学における事例などを示すことができないのかもしれないが、メールを利用した標的型攻撃である Emotet 感染に対する有効性を示すことができれば、本事業の価値を説得力を持って説明できたであろう。利用者の行動特性に応じた適切な対策がアウトカム目標であるならば Emotet などの現実の社会問題への有効性と、その限界について説明してほしかった。
- 政策へのフィードバックとして、当初目指していた総合対策基盤の構築に必要な事柄など当該事業から得られた知見を示してほしかった。
- 今後も同様の研究開発が国から支援されることによって、この分野が産業として発展し国際的にも展開できるレベルになることを期待する。