令和３年 12 月 13 日

令和3年度　追跡評価書

研究機関　　:KDDI(株)、(株)KDDI総合研究所、九州先端科学技術研究所、横浜国立大学、(株)セキュアブレイン、ジャパンデータコム(株)

研究開発課題　:国際連携によるサイバー攻撃の予知技術に関する研究開発

研究開発期間　:平成 23　～　平成 27 年度

代表研究責任者　:櫻井　幸一

■ 総合評価

（総論）

情報通信分野の技術発展は早く、「予知技術」というテーマは実現不可と思われたが、現在も研究開発を継続しており、その成果を学術的に論文化しているだけでなく、実運用でも応用していることから、研究開発の終了後において十分な成果を上げていると評価できる。今後は、https 通信など新たな通信形態への本研究成果の適用、社会変革をもたらすイノベーションの創出、国際的な技術連携の戦略的な方針の検討等が期待される。

（被評価者へのコメント）

- 本研究課題終了後も、研究開発で協力を継続していること、その成果を学術的に論文化していること、実運用で応用していることから、研究終了後も十分な成果を上げ続けていると考える。
- 情報通信分野の技術発展が早いこともあり「予知技術」という研究テーマは実現不可能な目標であったように思われるが、ある程度の成果を得たと評価できる。

- コロナ禍により https 通信、DNS over https、VPN といった新たな通信形態への移行及びランサムウェアの台頭など、サイバー空間の利用ケースの変化に伴って攻撃の傾向も大きく変化しているが、これらに対し本研究開発の成果をどのように適用していくのかについて記述が見当たらなかったのは惜しい。
- 学術的には、国際的に評価される内容のプロジェクトであり、実践面、すなわち、社会的にもセキュリティ技術の向上に寄与している。経済的な内容は、今後の課題となろう。
- 今後、グローバルにセキュリティを監視していく上で、我が国の高レベルな技術を、如何に他国へ提供するかも含め、戦略的な方針の検討も必要であろう。
- いくつかの事柄で顕著な成果を残した一方で、社会変革をもたらすイノベーション創出までは至っていない。

（1） 政策目標の達成状況等

（総論）

研究成果による観測データを国際的に研究者や開発者向けに共有している点は、社会的な効果を高め、我が国の国際競争力の強化やプレゼンスを示すために貢献している。AmpPot や IoTPOT の技術、機械学習手法を活用した Dark TRACER の開発は、他の研究開発や事業化、実用化につなげ、また観測結果は関係機関へ提供による活用が実施される等さらなる社会的効果が見込まれる。経済的効果については、研究成果を直接的な売上げにつなげることは難しいが、我が国のサイバー空間の安全確保の観点から、自社利用で留めず研究成果の製品化や一般化が期待される。特許や国際標準については、セキュリティと経済の両面での戦略的アプローチが必要となり、国益に供するための国際標準の取得等による社会還元が期待される。

（被評価者へのコメント）

- 研究活動の延長として、観測データを国際的に共有するようになっている点は我が国のプレゼンスを示すために貢献していると考える。
- AmpPot の利用や IoTPOT について優れた技術を開発しており、今後の国際競争の強化につながると考えられる。また、最新の観測結果の概況を研究者・開発者向けに提供しており、社会的な効果は充分ある。
- 機械学習手法を活用したDark TRACER の開発や他の総務省委託によるマルウェア無害化技術の研究における無害化対象検体の分類に利用でき、社会的効果がある。
- マルウェア長期観測システムを用いて、引き続き観測結果を ICT -ISAC に提供し、ISAC 等との連携により活用も期待されることから、今後、経済的、社会的な効果がでてくると予想される。
- 東京 2020 オリンピック・パラリンピック期間中に観測された DDoS 攻撃情報を ICT-ISAC を通じて国内 ISP 事業者にリアルタイムアラート配信している。
- 脅威を把握・捕捉する技術及び予兆現象をセキュリティ対応に活用する技術の確立という目的では、ハニーポットによる IoT 機器への攻撃観測など顕著な成果を得た。また、NICT において事業化や実用化が進められていることが評価できる。
- マルウェア分類・無害化に関して金融 ISAC に対してやホームページ上で情報提供をしている。
- サイバー攻撃対策ソリューションや情報提供サービスは圧倒的に海外製品が占めている現状に対し、我が国のサイバー空間の安全確保の観点から、研究成果の製品化や一般化といった改善が急がれる。
- 観測データからの攻撃のモデル化、運用者支援に関する研究開発（課題2－イ）から得られた知見をKDDI（株）の実通信サービスにおける DDoS 攻撃対策に活用中である。
- 本研究成果を利用した社内のセキュリティ監視運用品質の向上にもつながり、これがセキュリティ脅威下でビジネスを推進でき、経済的効果につながると考えられる。
- サイバーセキュリティに関する研究成果から直接的な売上げにつなぐことは難しいとはいえ、間接的な売上についても自社利用に留まっている点については更なる努力が求められると考える。
- KDDI（株）における社内事業と区別することが難しく、顕著な経済的な効果は認められない
- 特許や国際標準などの獲得が少ない印象が残る。「国際連携」の冠からすれば国際標準への提案が0件なのは残念である。国益に供するためには国際標準の獲得などによる社会還元が期待される。
- 本研究成果に基づく特許獲得が全くないので、今後、セキュリティと経済の両面での戦略的アプローチが必要であろう。

（2） 成果から生み出された科学的・技術的な効果

（総論）

本研究の成果を基に 3 件の後継研究開発があり、科学的な効果が認められる。技術的効果についても、東京オリンピック・パラリンピックでの活用に加えて、IoTPOT 等の国際レベルの技術が開発されていることは有益であったと評価できる。国際連携の観点では、11 拠点との連携について一定の効果は認められるが、今後は、より戦略的な国際協調の模索が求められる。本研究の普及状況及び影響力の評価には、論文発表数だけでなく、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。

（被評価者へのコメント）

- 本研究の最終年度の成果を基に他の研究費を活用して研究開発を継続しており、更なる成果を得ている点から科学的に効果があったと考える。
- 本研究成果が総務省や NICT の委託研究 3 件の後継プロジェクトに結びついた。
- 自社利用ではあるが、本研究成果を実運用で継続的に適用する、東京オリンピック・パラリンピックでも活用しており、技術的にも有益な研究であったと考える。できれば、どのような面で貢献したのかについても言及があった方が良いと思われる。
- IoTPOT 等、国際レベルの技術が開発されていることは評価できる。
- 国際連携では、11 拠点が知り合いベースのつながりであるが、一定の効果は認められる。ただし、今後はもう少し戦略的な国際協調も模索する必要があろう。例えば、中南米が抜けているとの説明があった。
- 本研究成果の普及状況の統計値（平成 28 年度以降、ほぼ全ての項目で数値が0件になっている）から、科学的・技術的な効果（新たな科学技術開発の誘因）に関する効果を確認することは難しい。
- 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。

（3） 副次的な波及効果

（総論）

サイバーセキュリティ研究分野の活性化のみでなく、ICT-ISAC を通じたアラートの発報やダークネットトラフィック解析、横浜国立大学での IoT マルウェア分類等、本研究成果を活用するだけでなく、終了後も協力体制を維持して、より発展させた研究へつなげたことは評価できる。また、本研究成果を基に機械学習をサイバー攻撃の分類に応用することで、機械学習とサイバーセキュリティの融合が進展しただけでなく、社会全体で希求される AI・データサイエンス人材の育成にも貢献した。今後、本研究開発に応じた費用に対する成果の数値化が望まれる。

（被評価者へのコメント）

- サイバーセキュリティ研究分野の活性化及び研究開発終了後も協力体制を維持しており、同研究分野の発展に大きく貢献したと考える。
- 自社利用ではあるものの、研究成果の一部が間接的な売上に寄与していることも副次的な波及効果があったと考える。
- ICT-ISAC 等を通じて多くの関係者にアラートとして提供され、サイバーセキュリティ対策に活用されていることは評価できる。
- ダークネットトラフィック解析や IoT マルウェア分類については、本研究開発の成果を、さらに発展させた研究につながっている。
- 横浜国大で情報提供サイトを公開し検体を研究者に向けて提供するなど、アカデミアにおける貢献は評価される。
- DOS 攻撃へのアラート配信について、アラート配信だけでは対策とは言えず、より効果的な方策が必要なのではないか。
- 機械学習をサイバー攻撃の分類に応用することで、社会全体で希求されている AI・データサイエンス人材の育成に貢献している。
- 本研究開発を通じ、サイバーセキュリティと機械学習の融合が進展した。
- サイバーセキュリティの場合、被害額 0 が目標となるため算出が難しいが、本研究開発に投じた費用に対するリターンがどの程度になったか、数字を示すことが望まれる。

（4） その他研究開発終了後に実施した事項等

（総論）

本研究開発後も研究及び協力体制を維持し、研究成果を基に新たな研究活動や実運用での活用につなげており、AmpPot で検知した情報を ICT-ISAC 会員企業へアラートとして配信している点や、研究成果から得られた攻撃情報を関連サイトに情報提供する等、十分な活動を行っており、研究成果の普及活動を行っている。

（被評価者へのコメント）

- 研究開発終了後も研究及び協力体制を維持し、継続的に学術的な研究発表を行っているだけでなく、実運用でも活用する等、十分な活動を行っていると考える。
- 本研究開発の成果を基に新たな研究活動へつないでいる点も、本研究課題の重要性が高かったことを示している。
- 本研究開発終了後の継続的な観測結果公開は、研究成果の普及活動とみなせる。
- ICT-ISAC では、AmpPot から提供される情報を会員企業の ISP 各社に対してアラートとして配信している。
- IoT マルウェア攻撃の情報提供サイトや DoS 攻撃情報提供サイトで最新の観測結果を公開しており、今後は、攻撃検知シグネチャや攻撃者サーバリストも提供予定である。
- 平成 28 年度以降に「自己実施件数」、「実施許諾件数」、「報道発表数」などの件数が0件であり、終了後の活動が活発とは言えない。

（5） 政策へのフィードバック

（総論）

サイバー空間の安全確保は国家的な課題であり、国家主導のプロジェクトとして疑う余地はなく、国際連携、東京オリンピック・パラリンピックに係る行事等で成果を発揮していることから十分な効果があったと言える。本研究開発終了後、研究を継承した体制が構築され、本成果を承継しているのは評価できるが、商品化の観点では、依然として諸外国が先行しており、研究成果の十分な活用が望まれる。今後、特許や経済効果、学術論文以外の社会貢献については国、企業、研究機関が連携し、戦略的に考える必要がある。本研究開発における課題の整理を行いつつ、政策へのフィードバックとして PDCA を回して全体の振り返りや政策への提言が必要と考える。

（被評価者へのコメント）

- 課題設定では、サイバー攻撃の予兆検出という成果が得られるか確証が得にくい問題であり、研究成果の応用範囲も限定的とならざるを得ないが、サイバー空間の安全確保は国家的な課題であり、国が行うべきプロジェクトであることは疑いの余地はない。その観点で、本研究開発は、国際連携、東京オリンピック・パラリンピック、ネットバンキングなどで成果を発揮しており、十分な効果があったと考える。
- 本研究開発の初期段階から NICT や ICT-ISAC との連携を強く意識した実施体制を構築しており、プロジェクト終了後も本成果をスムーズに承継し、多くの関係者が継続して活用できている。
- サイバーセキュリティ技術の商品化は依然として米国、イスラエル、台湾等の諸外国が先行しており、本研究課題で得られた成果が十分に活用できていないと考える。
- サイバー空間の安全確保は安全保障上も重要な課題であり、本研究課題及びその後の継続研究の成果を実用化する支援が必要と考える。
- 本研究開発は国際連携の観点から、国家主導で行うべき内容である。
- 今後、特許や経済的効果について国、企業、研究機関が連携し、戦略的に考える必要がある。
- 国が主導するプロジェクトとして、海外の政府やセキュリティ機関、大学等との連携ができた。
- 論文発表で当該技術の優位性が損なわれ市場での競争性を失う可能性やサイバー攻撃が助長される可能性があるため学術的な成果を強く求めないことから、学術論文以外の社会貢献が強く期待される。
- 本研究開発の対象外としても、社会問題化した Emotet 感染に対し効果がなかったことは多額の国税を投入している事業として社会貢献に関する説得力が欠け、「予知技術」というテーマは難しすぎたのかもしれない。

- 政策へのフィードバックとして、PDCAを回して当該事業の全体の振り返りやサイバーセキュリティに関連する政策への提言が必要である。