国際連携によるサイバー攻撃の予知技術の研究開発

実施研究機関：KDDI（株）、九州先端科学技術研究所、（株）セキュアブレイン、横浜国立大学、（株）KDDI総合研究所、ジャパンデータコム(株)
研究開発期間：H23年度～H27年度
研究開発費：H23年度 2.3億円、H24年度 2.4億円、H25年度 2.3億円、H26年2.0億円、H27年1.6億円　計10.6億円
担当課室名：サイバーセキュリティ統括官室

1. 研究開発概要

＜目的＞

サイバー攻撃に起因する脅威情報の収集ネットワークを国際的に構築し、収集した情報をISP、大学等と協力して分析することにより、サイバー攻撃の脅威を速やかに把握・捕捉する技術及び、早い段階で捕捉できるサイバー攻撃の予兆現象を実践的なセキュリティ対応に生かす技術を確立する。

＜政策的位置付け＞

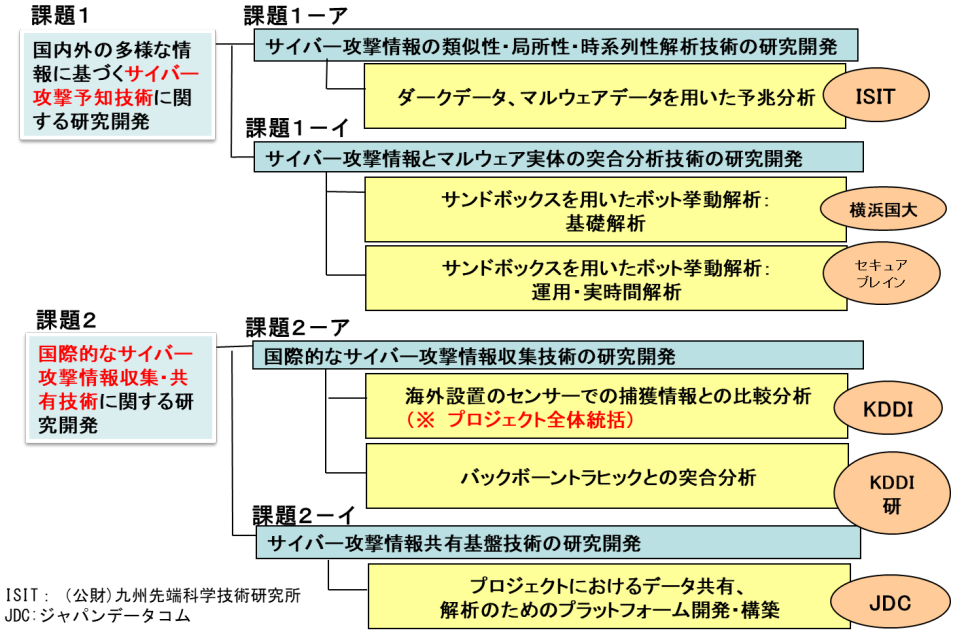
国民を守る情報セキュリティ戦略（平成22 年5月情報セキュリティ政策会議決定）では、「マルウェアへの感染対策等を強化するため、（中略）情報セキュリティ脅威の収集解析システム等の充実や、利用者・ISP 等への情報提供を通じたネットワーク等の情報セキュリティ対策を強化する。加えて、国際的な連携を推進する。」とされている。また、「情報セキュリティ2010」（平成22 年7月情報セキュリティ政策会議決定）では、総務省が「ISP と協力してサイバー攻撃に関わる情報収集ネットワークを構築し、サイバー攻撃の事前防止・早期対策に向けた枠組みの構築を検討する。」とされており、本研究開発はこれらの施策の一部を担う。

＜目標＞

近年、大規模なサイバー攻撃が世界各国で発生し、政府関係機関、金融機関等の主要機関のサービスが長期間に渡って停止するなど、国民生活や経済活動に甚大な影響を及ぼしている。国際的なサイバー攻撃への速やかな対処を行うためには、その脅威を正確かつ速やかに察知することが必要不可欠である。本研究開発は、国際連携により各地のサイバー攻撃情報(ダークネット観測により取得したスキャンやシェルコード等の攻撃パケット情報、Web 型も含めたマルウェア感染活動情報等)を収集し、それを即時に分析することにより、サイバー攻撃の脅威を速やかに把握する技術及びさらに分析を進め、将来のサイバー攻撃状況の推移を予測する技術の確立を目標とする。

2. 研究開発成果概要

以下の課題、体制にて研究開発を実施した。



本研究開発における主要な成果を、以下に示す。

課題1：予兆解析/早期攻撃把握からアラートを導出

（ISIT） マルウェアの初期挙動や大量感染などの不正挙動をダークネットから抽出することが可能となる解析エンジン群を開発した。

（セキュアブレイン） マルウェア動的解析とTaint解析を組合せた大規模なサンドボックスを構築、C2、悪性IP情報などのアラート発行を実現した。

（横浜国立大学） 開発したハニーポット技術をベースに、P2P型ボットネットの感染ホスト情報や反射型サービス妨害攻撃に対する即時アラート、IoTマルウェアの詳細挙動等、実用性の高い予知・即応技術を確立した。

課題2：海外拠点との国際連携による攻撃把握と分析基盤の構築

（KDDI） 海外11拠点にセンサーを設置して観測データの解析を行い、予兆分析/早期攻撃把握の有効性を確認した。また、収集したデータや解析結果を閲覧できるWebポータルを構築し、アラートやマルウェア感染情報などを実時間で連携国と共有した。

（KDDI総合研究所） ハニーポットなどの観測データと通信事業者の実データとの突合分析により、アラート情報の精度・有効性の向上を行った。

（ジャパンデータコム） 異なる関連研究機関が観測収集した、機微情報を含むデータを共有して相関分析するため基盤構築を実現した。

3. 成果から生み出された経済的・社会的な効果

＜政策目標（アウトカム目標）の達成状況＞

ISITにおける学術的成果（課題1－ア）の応用について、NICTでの活用を念頭に九州大学、早稲田大学、横浜国立大学のグループで、サイバーセキュリティのための機械学習をテーマに共同研究を継続し、NICTの情報提供サービスでの活用を目指して開発を行っている。令和元年度 - 2年度には、NICT「サイバー攻撃ハイブリッド分析実現に向けたセキュリティ情報自動分析基盤技術の研究開発」で、令和2年度からは、総務省「電波の有効利用のためのIoTマルウェア無害化/無機能化技術等に関する研究開発」で継続して研究を行っている。これらの活動の中では、本委託研究で基礎研究を行った、「系統樹によるマルウェアクラスタリング技術」について、IoTマルウェアの分類を対象とした発展的研究を行っている。

セキュアブレインの開発したマルウェアサンドボックス解析アラート（課題1－イ）については、ICT-ISACにおいて活用を継続。平成28年度は、総務省「情報共有基盤の実証実験」での接続検証、及びICT-ISAC情報共有ワーキングでの脅威情報のコンテンツ検証でマルウェアの動的テイント解析技術を活用。平成29年度以降はマルウェアの長期観測環境を継続運用し、得られた情報をSTIX形式に変換しICT-ISACに配信している。

分散型サービス妨害攻撃観測システム（Amppot）（課題1－イ）は横浜国立大学にて継続的に運用しており、ICT-ISACに対して攻撃観測アラートを提供している。さらに、令和3年7月にはアラートの国際展開を開始し、Shadowserver Foundationを通じて130か国以上のCERTと6000超のネットワークオペレータへの配信を行っている。また、IoTサイバー攻撃観測システム(IoTPOT)（課題1－イ）は横浜国大にて継続的に運用しており、本委託研究終了後に本格化したIoTにおけるサイバー攻撃を詳細に観測・分析する先駆的技術として重要な役割を果たしている。

KDDIにより連携国に設置したダークネットセンサー（課題2－ア）は本委託研究終了後にNICTへ移管し、継続してダークネットデータの収集と、連携先との情報共有を行っている。また、KDDI総合研究所で実施した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の通信サービスにおけるDDoS攻撃対策の自動化・高度化に活用中である。

＜新たな市場の形成、売上げの発生、国民生活水準の向上＞

ダークネットデータの分析（課題1－ア）に基づくNICTからの情報提供は、令和4年度中に実施できる予定であり、インターネット利用におけるセキュリティを高め、国民生活水準の向上に資すると期待している。
マルウエアの長期観測環境から得られた情報（マルウェアサンドボックス解析アラート）（課題1ーイ）をICT-ISACへ配信することにより実用化。継続的に提供していくことでサイバー攻撃のリスクを軽減し、社会に貢献している。また、セキュアブレインが提供するネットバンキングの利用を支援する不正送金対策サービスに対して、長期観測環境から得られた情報の製品開発への活用や、社会還元活動としてICT-ISACへ情報提供をしていることによる対外的なPR活動への活用効果により、間接的に売り上げに寄与している。
IoTにおけるサイバー攻撃の深刻化は、テレビ、新聞、インターネットメディア等を通じて広く伝えられているところであり、IoTPOTの活用成果（課題1ーイ）は、多数のニュース報道、複数の特集番組などを通じて注意喚起やリテラシ向上に貢献している。
また、本研究開発成果の知見（観測データからの攻撃のモデル化、運用者支援（課題2－ア））は通信事業者の実ネットワークにおけるDDoS攻撃対策に活用されており、大規模なDDoS攻撃の自動的軽減、被害の未然防止が可能となり、安定した通信サービスの提供に貢献している。

＜知財や国際標準獲得等の推進＞

セキュリティ研究の性質上、技術そのものについては攻撃者への情報開示となるため知財としての展開は困難であるが、マルウェアの長期観測環境を継続運用し得られた情報（課題1－イ）について、今後の国際標準を視野に入れSTIX記述仕様に関し、攻撃をされている側（被害者側）の情報を配信するための記述仕様について改善提案を検討しており、学術シンポジウムにて発表する準備を進めている。

4．成果から生み出された科学的・技術的な効果

＜新たな科学技術開発の誘引＞

本研究開発の成果の一部または、発展させた研究開発として、NICT委託研究「Web媒介型攻撃対策技術の実用化に向けた研究開発」（平成28年度-令和2年度）、NICT委託研究「サイバー攻撃ハイブリッド分析実現に向けたセキュリティ情報自動分析基盤技術の研究開発」（令和元年度-2年度）、総務省「電波の有効利用のためのIoTマルウェア無害化/無機能化技術等に関する研究開発」（令和2年度-）などが実施されている。
このように、本研究開発の成果が次の技術に継承され、さらに高度化されて多くの研究成果の基盤となっている。

5．副次的な波及効果

＜副次的な波及効果＞

本研究開発のうちISIT担当部分は、ISIT本務の研究者と、九州大学および早稲田大学の教員および大学院生が担当した。九州大学と早稲田大学の参加者は、主として機械学習を専門とする研究者であり当初はサイバーセキュリティは一つの応用と捉えていた。本研究開発を通じ、サイバーセキュリティと機械学習を融合した研究サークルが構成され、NICTを中心に活動を発展させている。
IoTPOTの観測結果は累計35か国150に及ぶ研究組織、個人へと提供され、IoTマルウェア対策研究において世界的な成果を生んだ。平成27年, 28年に発表した当該技術に関する論文は令和3年9月時点で学術論文による参照件数が450件を超えており、当該分野に大きな影響を与えている。また、この観測結果に基づくIoTマルウェア対策に関する研究がサイバーセキュリティ分野の最高峰国際会議において論文賞を受賞するなど、学術的にも大きな成果をあげている。
セキュアブレインと横浜国立大学とはハニーポット技術やマルウェア解析技術において交流を継続しており、最新のマルウェア検体および解析情報の共有を行っている。令和2年度からの総務省「電波の有効利用のためのIoTマルウェア無害化／無機能化技術等に関する研究開発」においても受託者として連携しており研究の推進だけでなく研究者育成への効果も期待できる。
令和3年に行われた東京2020オリンピック・パラリンピック大会においても、ICT-ISACを通じて国内ISP事業者にAmppotのアラートをリアルタイムに共有。ISP各社が大会中のサイバーセキュリティ監視体制を強化する中、DDoSなどのサイバー攻撃傾向の把握などに活用された。

6．その他研究開発終了後に実施した事項等

＜周知広報活動の実績＞

本研究開発テーマに関わる技術や実証の内容について、継続して論文等で発表している。
IoTにおけるサイバー攻撃の深刻化は、テレビ、新聞、インターネットメディア等を通じて広く伝えられ、多数のニュース報道、複数の特集番組などを通じて注意喚起やリテラシ向上に貢献している。
九州大学と早稲田大学では，研究開発終了後も本テーマに関わる論文発表を継続して行った。

＜その他の特記事項に係る履行状況＞（研究開発終了後も行うべきものについて）

本研究開発と並行して実施された総務省「国際連携によるサイバー攻撃の予知・即応技術の実証実験」と密に連携を行い、その内容はICT-ISACのサイバー攻撃即応WGにおいてISP間で共有・活用された。研究開発終了後も、ICT-ISACのDoS-WGおよびオリパラSiGにおいて同実証実験及び本研究開発によって得られた知見が承継され、東京2020オリンピック・パラリンピック大会等において攻撃予兆データが活用された。
マルウェアサンドボックス解析アラートに関しては、令和元年度からの総務省「ソフトウェア脆弱性を狙ったサイバー攻撃の防御に向けた情報共有基盤に関する実証実験」において、STIX情報配信のUse Caseとしての活用、STIX情報配信の環境やバージョン移行での活用が行われている。
海外機関との関係においても、例えばドイツECOの会議（平成29年）で本研究成果の共有が要請されており、継続的な研究連携が行われている。

7．政策へのフィードバック

＜国家プロジェクトとしての妥当性、プロジェクト設定の妥当性＞

各課題・研究機関が効果的な連携を行った結果、ハニーポットのアラートをISP運用の改善に役立てたほか、新規研究の導出、研究開発メンバ間の相関性の高い研究推進など、研究開発マネジメントの点からも効率的にプロジェクトを推進し、先進的な成果をあげることができた。また、海外の10か国の政府やセキュリティ機関、大学等と連携し、研究成果の提供や情報共有を実施できたことは、国が主導するプロジェクトとして極めて妥当であった。

＜プロジェクトの企画立案、実施支援、成果展開への取組み等に関する今後の政策へのフィードバック＞

IoTPOTやダークネットを用いた収集と分析に関する研究については、引き続き横浜国立大学やNICTにおいて進めており、本成果が新たなICT-ISACプロジェクトやNISCの活動に生かされている。また、Amppotについても、横浜国立大学において運用と監視、ICT-ISACやShadowserver Foundationへのアラート配信が継続すると共に、NICTにおいても同様の観測システムを別途構築しており、東京オリパラCSIRT等へのアラート配信を行っている。
本研究開発では、研究の初期段階から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することができた。