平成 28 年度事後事業評価書

政策所管部局課室名：情報流通行政局　情報流通振興課　情報セキュリティ対策室
評価年月：平成 28 年８月

１　政策（研究開発名称）

国際連携によるサイバー攻撃の予知技術の研究開発[1]

２　研究開発の概要等

（１）研究開発の概要

・実施期間

平成 23 年度～平成 27 年度（５か年）

・実施主体

民間企業、公益財団法人、大学

・事業費

1,049 百万円

平成 23 年度	平成 24 年度 （平成 23 年度補正）	平成 25 年度	平成 26 年度	平成 27 年度 （平成 26 年度補正）	総　額
225 百万円	236 百万円	230 百万円	198 百万円	160 百万円	1,049 百万円

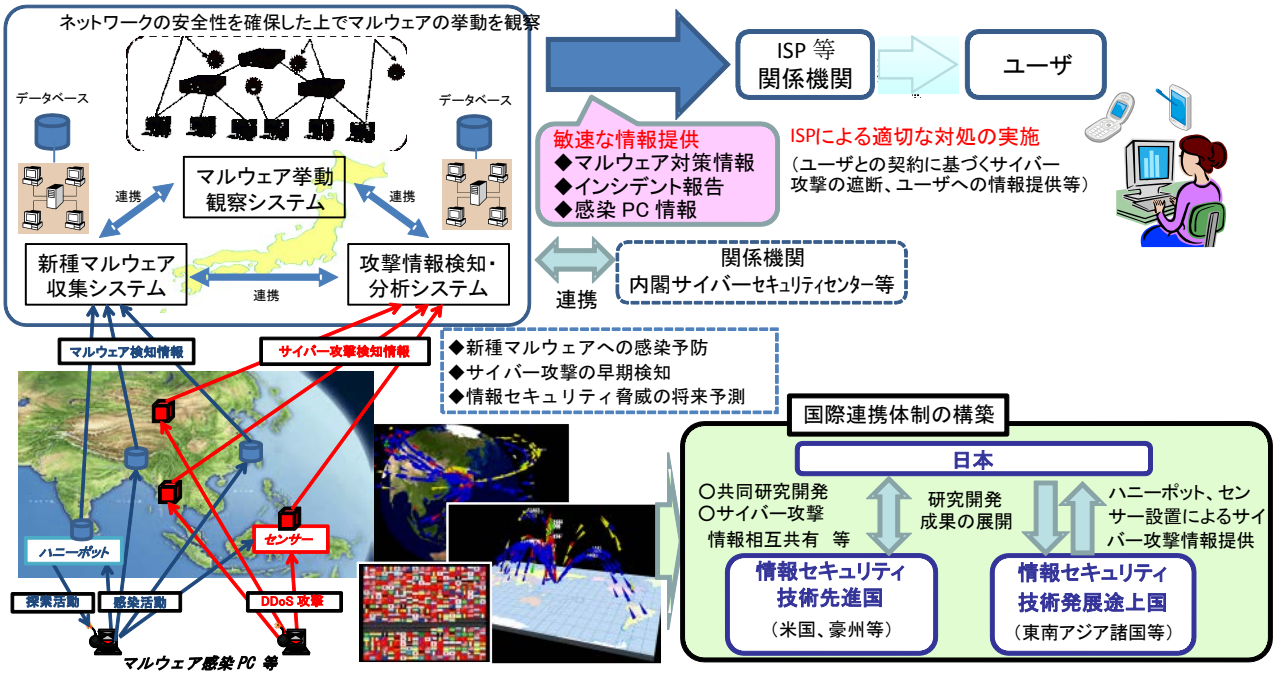
・概　要

近年、大規模なサイバー攻撃が世界各国で発生し、国際的な問題となっている。世界中に張り巡らされたサイバー攻撃基盤により、サイバー攻撃は一層巧妙化・大規模化する傾向にあり、国民の実生活や経済活動に甚大な影響を及ぼす可能性がある。今や公共のインフラとなっているインターネットの安全性、信頼性の向上を図り、利用者が安心・安全にインターネットを利用できる環境を実現するために、サイバー攻撃によるリスクを低減することの重要性はますます高まっている。

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。本研究開発では、サイバー攻撃に関する情報（ダークネット[2]観測により取得したスキャン等の攻撃パケット情報、Web 型も含めたマルウェア[3]感染活動情報等）収集ネットワーク及び連携体制を国際的に構築し、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する技術及び、将来のサイバー攻撃の脅威を速やかに把握する技術及び、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的とする。

---

1 事前事業評価書時点では「国際連携によるサイバー攻撃の予知・即応技術の研究開発」
2 未使用の IP アドレス
3 コンピュータウイルス等の「悪意あるソフトウェア」の総称



技術の種類	技術の概要
サイバー攻撃情報の類似性・局所性・時系列性解析技術	国内外で収集された多種多様な観測データを用いて、各地の観測・統計データの類似性、局所性、及び時系列性を解析する技術の研究開発を実施する。 最終的には、サイバー攻撃情報の解析を 30 分以内に完了することを目標とする。
サイバー攻撃情報とマルウェア実体の突合分析技術	サイバー攻撃情報とマルウェア実体との相関性、連動性及び時系列性等の複合的な解析により、サイバー攻撃に関する直近の同行を把握するための高精度な突合分析技術を確立する。 最終的には、突合分析に要する時間を 30 秒以内とし、突合分析の精度（正解率）を 80%以上とすることを目標とする。
国際的なサイバー攻撃情報収集技術	国際的に分散配置されたセンサの運用・管理を遠隔化・自動化し、設置組織に応じて観測のためのフィルター設定やプライバシー設定を柔軟に変更（動的設定）することのできる技術を開発する。また、観測データから多くの評価指標に従って統計データを自動的に生成するとともに、可視化等の分析支援作業に資するための研究開発を実施する。 最終的には、動的設定に要する時間を 5 秒以内、統計データ抽出に要する時間を 10 秒以内にすることを目標とする。
サイバー攻撃情報共有基盤技術	国内外で収集した攻撃データ及びその分析情報（突合分析結果等）について、研究開発及び民間事業者等の関係機関と具体的に共有するための、情報共有基盤の構築技術を開発する。 最終的には、情報共有に関する処理が提供情報の発生から 10 分以内に完了することを目標とする。

（2）達成目標

感染手法が多様化するマルウェアを効果的・効率的に捕獲するシステム（ハニーポット [4]）と、攻撃手法が多様化するサイバー攻撃を広範囲に検知・分析するシステムを構築し、高度化・巧妙化を続ける情報セキュリティ脅威への迅速な対応実現に向けて、サイバー攻撃情報の類似性・局所性・時系列性解析技術、サイバー攻撃情報とマルウェア実体の突合分析技術、国際的なサイバー攻撃情報収集技術、サイバー攻撃情報共有基盤技術を確立し、新種マルウェアによる感染の予防、サイバー攻撃の早期検知・迅速な対応、情報セキュリティ脅威の将来予測に基づく予防的対処を可能とする技術的基盤を確立することにより 、安心・安全な ICT 利用環境を実現することに寄与する。

[4] マルウェアなどの検体を入手するために設置された機器やネットワークのこと

○　関連する主要な政策
　Ｖ．情報通信（ＩＣＴ政策）　政策９「情報通信技術の研究開発・標準化の推進」
○　閣議決定等の上位計画・全体計画等
・情報セキュリティ研究開発戦略（改訂版）（平成 26 年７月 10 日　情報セキュリティ政策会議決定）
　４（５）　国際連携による研究開発の強化等

・サイバーセキュリティ戦略（平成 27 年９月４日　閣議決定）
　５．４．１　研究開発の推進

・サイバーセキュリティ 2015（平成 27 年９月 25 日　サイバーセキュリティ戦略本部決定）
　４．１（４）　国際連携による研究開発の強化

（３）目標の達成状況

世界各国で発生しているサイバー攻撃に対し速やかな対処を行うために、その脅威を正確かつ速やかに察知することができる技術を以下のとおり確立し、新種マルウェアによる感染の予防、サイバー攻撃の早期検知・迅速な対応、情報セキュリティ脅威の将来予測に基づく予防的対処を可能とする技術的基盤を確立した。これらの技術により、サイバー攻撃を速やかに把握し、対応できるようになり、サイバー攻撃の被害の軽減に資することから、安心・安全な ICT 利用環境を実現に寄与し、所期の目標を達成した。

課題ア）サイバー攻撃情報の類似性・局所性・時系列性解析技術

課題に掲げている技術の確立、目標としていたサイバー攻撃情報の解析の 30 分以内の完了を達成した。これらに加え、大規模なマルウェアデータの分類技術と解析結果をわかりやすく表示する可視化技術の開発も実施した。マルウェアの分類について、従来手法では１万検体/24H のところを 10 万検体/24H まで高速化した。また、トラフィックデータの流れをよりわかりやすく可視化し、不正アクセス等の目視による検知が容易となった。

課題イ）サイバー攻撃情報とマルウェア実体の突合分析技術

目標であった突合分析の所要時間 30 秒以内、突合精度 80%以上は平成 26 年度に 10,848 検体で達成した。さらに、最終年度には 16,236 検体となっても同様の性能を発揮している。加えて、IoT マルウェアといった新たな脅威を観測・分析する技術の開発も行った。

課題ウ）国際的なサイバー攻撃情報収集技術

各国に設置したセンサの観測データから多くの評価指標に従って統計データを自動生成するとともに、検索・分析を迅速、効率的に実施するための Web ポータルを構築した。本 Web ポータルは本研究開発でセンサを設置した各連携組織に対して公開しており、各国センサから収集したサイバー攻撃１次情報、各種解析エンジンにより得られる解析結果情報、及び国内サイバー攻撃観測網から得られる早期警戒アラート情報などを参照することが可能で、各情報源から情報を受け取った後、目標とする実時間で表示されることを確認しており、連携組織での迅速な活用が可能となった。

課題エ）サイバー攻撃情報共有基盤技術

最終目標は達成されており、最終年度にはダークネット予兆分析、DR-DoS[5]ハニーポット予兆分析、サンドボックス [6]のマルウェア挙動解析を行う各研究機関から、解析結果やアラートデータを情報共有基盤に自動で転送して蓄積し、その多種多様なサイバー攻撃情報を統合解析してサイバー攻撃対象に対してアラートを通知するシステムの構築を実現し、実運用を開始した。この実運用において、攻撃の発生から通知までの平均時間は、アラートデータ１件につき、１～２秒を達成している。

---

[5] Distributed Reflection Denial of Service:DDoS 攻撃の一種であり、インターネット上のサーバやネットワーク機器等を通信量の増幅器として用いて行う攻撃のこと

[6] 保護された領域でプログラムを動作させることによってプログラムが暴走したり、マルウェアを動作させようとしてもシステムが不正に操作されるのを防ぐセキュリティ機構のこと

３　政策効果の把握の手法及び政策評価の観点・分析等

研究開発の評価については、論文数や特許出願件数などの間接的な指標を用い、これらを基に専門家の意見を交えながら、必要性・効率性・有効性等を総合的に評価するという手法が多く用いられている。

上述の観点に基づき、「情報通信技術の研究開発の評価に関する会合」（平成 28 年６月）において、目標の達成状況等に関して外部評価を実施し、政策効果の把握に活用した。

また、外部発表や特許出願件数、国際標準提案件数等も調査し、必要性・有効性等を分析した。

○研究開発による特許・論文・研究発表・国際標準の実績

研究開発による特許・論文・研究発表の実績から、攻撃ホストの挙動解析装置・方法及びプログラムや不正処理解析装置、及び不正処理解析方法など多くの特許出願をするなど、標準化活動に貢献しており、本研究開発の必要性、有効性等が認められた。

主な指標	平成 23 年度	平成 24 年度	平成 25 年度	平成 26 年度	平成 27 年度	合計
査読付き誌上発表論文数	１件（　０件）	５件（　２件）	４件（　２件）	２件（　０件）	11 件（　５件）	23 件（　９件）
査読付き口頭発表論文数（印刷物を含む）	３件（　３件）	11 件（11 件）	６件（　６件）	３件（　３件）	７件（　７件）	30 件（ 30 件）
その他の誌上発表数	０件（　０件）	０件（　０件）	０件（　０件）	０件（　０件）	０件（　０件）	０件（　０件）
口頭発表数	26 件（　３件）	21 件（　２件）	24 件（　６件）	43 件（　６件）	49 件（　８件）	163 件（ 25 件）
特許出願数	２件（　０件）	１件（　０件）	０件（　０件）	０件（　０件）	１件（　０件）	４件（　０件）
特許取得数	０件（　０件）	０件（　０件）	０件（　０件）	０件（　０件）	０件（　０件）	０件（　０件）
国際標準提案数	０件（　０件）	０件（　０件）	０件（　０件）	０件（　０件）	０件（　０件）	０件（　０件）
国際標準獲得数	０件（　０件）	０件（　０件）	０件（　０件）	０件（　０件）	０件（　０件）	０件（　０件）
受賞数	０件（　０件）	１件（　０件）	２件（　１件）	２件（　０件）	２件（　０件）	７件（　０件）
報道発表数	１件（　０件）	０件（　０件）	０件（　０件）	０件（　０件）	２件（　０件）	２件（　０件）
報道掲載数	０件（　０件）	０件（　０件）	０件（　０件）	０件（　０件）	０件（　０件）	０件（　０件）

注１：各々の件数は国内分と海外分の合計値を記入。（括弧）内は、その内海外分のみを再掲。

注２：「査読付き誌上発表論文数」には、定期的に刊行される論文誌や学会誌等、査読（peer-review（論文投稿先の学会等で選出された当該分野の専門家である査読員により、当該論文の採録又は入選等の可否が新規性、信頼性、論理性等の観点より判定されたもの））のある出版物に掲載された論文等（Nature、Science、IEEE Transactions、電子情報通信学会論文誌等および査読のある小論文、研究速報、レター等を含む）を計上する。

注３：「査読付き口頭発表論文数（印刷物を含む）」には、学会の大会や研究会、国際会議等における口頭発表あるいはポスター発表のための査読のある資料集（電子媒体含む）に掲載された論文等（ICC、ECOC、OFC など、Conference、Workshop、Symposium 等での proceedings に掲載された論文形式のものなどとする。ただし、発表用のスライドなどは含まない。）を計上する。なお、口頭発表あるいはポスター発表のための査読のない資料集に掲載された論文等（電子情報通信学会技術研究報告など）は、「口頭発表数」に分類する。

注４：「その他の誌上発表数」には、専門誌、業界誌、機関誌等、査読のない出版物に掲載された記事等（査読の有無に関わらず企業、公的研究機関及び大学等における紀要論文や技報を含む）を計上する。

注５：PCT（特許協力条約）国際出願については出願を行った時点で、海外分１件として記入。（何カ国への出願でも１件として計上）。また、国内段階に移行した時点で、移行した国数分を計上。

注６：同一の論文等は複数項目に計上しない。例えば、同一の論文等を「査読付き口頭発表論文数（印刷物を含む）」および「口頭発表数」のそれぞれに計上しない。ただし、学会の大会や研究会、国際会議等で口頭発表を行ったのち、当該学会より推奨を受ける等により、改めて査読が行われて論文等に掲載された場合は除く。

○各観点からの分析

観点	分析
必要性	近年、DDoS 攻撃（Distributed Denial of Service attack：分散型サービス妨害）等の大規模なサイバー攻撃が世界各国で発生し、国際的な問題となっている。サイバーセキュリティインシデントは、一層巧妙化、大規模化するとともに、増加傾向にあり、今や公共のインフラとなっているインターネット

	の安心・安全な利用を阻害し、国民の実生活や経済活動に甚大な影響を及ぼす可能性がある。このため、諸外国と連携し、速やかにサイバーセキュリティインシデントに対処するための技術を確立し、サイバー攻撃の被害を軽減することにより、国民が安心・安全にインターネットを利用できるネットワーク環境を実現する必要がある。また、サイバーセキュリティの研究開発についてはサイバーセキュリティ戦略（平成 27 年９月４日閣議決定）や日本再興戦略 2016（平成 28 年６月２日閣議決定）などの政府戦略にも取り上げられている等、総務省だけでなく政府全体として積極的に推進すべきものとされている。 以上のことから、本研究開発には必要性があったと認められる。
効率性	サイバー攻撃に関する専門的知識や研究開発遂行能力を有する企業、研究者等のノウハウを積極的に活用することにより、各社がそれぞれ得意な分野を担当し、効率的に研究開発が進められた。さらに、課題間の連携が十分に取られているとともに、国立研究開発法人情報通信研究機構(NICT)などの国内組織と連携したことにより、効率的に研究開発が進められた。 また、委託経費の執行に当たっては、事前に予算計画書を確認するとともに、年度途中及び年度末に経費の執行に関する経理書類を提出させ、総務省担当職員が詳細な経理検査を行い、予算の効率的な執行に努めた。加えて、専門的知見を有した監査法人に経理検査の補助を依頼し、経費執行の適正性・効率性を確保している。 以上のことから、本研究開発には効率性があったと認められる。
有効性	サイバー攻撃情報の類似性・局所性・時系列性解析技術、サイバー攻撃情報とマルウェア実体の突合分析技術、国際的なサイバー攻撃情報収集技術、サイバー攻撃情報共有基盤技術を確立し、新種マルウェアによる感染の予防、サイバー攻撃の早期検知・迅速な対応、情報セキュリティ脅威の将来予測に基づく予防的対処を可能とする技術的基盤を確立したことにより、サイバー攻撃を速やかに把握し、対応できるようになり、サイバー攻撃の被害の軽減に資することから、安心・安全な ICT 利用環境の実現に寄与した。 本研究開発においては、国立研究開発法人　情報通信研究機構（NICT）が開発したネットワーク観測センサの技術提供を受け、海外 10 か国、11 拠点に展開された観測センサからデータの収集を行った。これらに加え、サイバー攻撃情報やマルウェア検体の解析情報を集約し、統合・解析を行い、サイバー攻撃予兆アラートを生成した。本アラート情報の一部は、ISP などの実運用環境における評価・検証に活用されている。特に、DDoS 攻撃予兆アラートは、平成 25 年 10 月からリアルタイムでメール配信を開始し、ISP のネットワーク運用において DoS 攻撃対策オペレーションの時間短縮等の効果を確認している。これらのことにより、サイバー攻撃を速やかに把握し、対応できるようになり、サイバー攻撃の被害を軽減することに資することができていると認められる。 以上のことから、本研究開発には有効性があったと認められる。
公平性	ICT の利活用が社会活動に広く浸透した現在では、多くの企業や一般ユーザがサイバーセキュリティの脅威にさらされており、誰もが被害者となり得る。そのため、サイバー攻撃やマルウェア等の情報通信におけるサイバーセキュリティ脅威の被害軽減に資する本研究開発の成果は、広く国民の利益になるものである。 また、支出先の選定に当たっては、実施希望者の公募を広く行い、研究提案について外部専門家から構成される評価会において最も優れた提案を採択する方式により、競争性を担保した。 以上のことから、本研究開発には公平性があったと認められる。
優先性	世界各国で大規模なサイバー攻撃が発生しており、新種のマルウェアにより、多くのウェブサイトが改ざんされるなど、国内外においてサイバーセキュリティインシデントによる被害が数多く発生している。また、サイバーセキュリティインシデントは、一層巧妙化、大規模化するとともに、増加傾向にあり、国民の実生活や経済活動に甚大な影響を及ぼす可能性がある。このような事態に一刻も早く対処し、公共のインフラとなっているインターネットの安全性、信頼性の向上を確保することは、喫緊の課題である。 以上のことから、本研究開発には優先性があったと認められる。

４　政策評価の結果（総合評価）

本研究開発において、サイバー攻撃情報の類似性・局所性・時系列性解析技術、サイバー攻撃情報とマルウェア実体の突合分析技術、国際的なサイバー攻撃情報収集技術、サイバー攻撃情報共有基盤技術を確立し、新種マルウェアによる感染の予防、サイバー攻撃の早期検知・迅速な対応、情報セキ

ュリティ脅威の将来予測に基づく予防的対処を可能とする技術的基盤を確立した。これらの技術により、サイバー攻撃を速やかに把握し、対応できるようになり、サイバー攻撃の被害を軽減に資することから、安心・安全な ICT 利用環境の実現に寄与した。
以上のことから、本研究開発の有効性、効率性等が認められた。

＜今後の課題及び取組の方向性＞
本研究開発終了後は、本研究開発の委託先及び国立研究開発法人情報通信研究機構（NICT）が研究を引き継いで実施しており、今後も巧妙化・悪質化するサイバー攻撃に対応するため、本研究開発で確立した技術を高度化する取組を進めており、総務省も追跡調査等でフォローアップを行っていく。

５　学識経験を有する者の知見の活用

「情報通信技術の研究開発の評価に関する会合」（平成 28 年６月）において、目標の達成状況や得られた成果等について、研究開発の目的・政策的位置づけ及び目標、研究開発マネジメント、研究開発成果の目標達成状況、研究開発成果の社会展開のための活動実績並びに研究開発成果の社会展開のための計画等の観点から、外部評価を実施し、以下に示す御意見などをいただいたため、本研究開発の評価に活用した。

・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。
・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。
・いくつかの研究成果について、レベルの高い国際学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。
・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。

６　評価に使用した資料等

○情報セキュリティ研究開発戦略（改訂版）（平成 26 年７月 10 日　情報セキュリティ政策会議決定）
http://www.nisc.go.jp/active/kihon/pdf/kenkyu2014.pdf

○サイバーセキュリティ戦略（平成 27 年９月４日　閣議決定）
http://www.nisc.go.jp/active/kihon/pdf/cs-senryaku.pdf

○サイバーセキュリティ 2015（平成 27 年９月 25 日　サイバーセキュリティ戦略本部決定）
http://www.nisc.go.jp/active/kihon/pdf/cs2015.pdf

○総務省　平成 23 年度開始の研究開発プロジェクト一覧
http://www.soumu.go.jp/menu_seisaku/ictseisaku/ictR-D/itiran23.html