サイバー攻撃の解析・検知に関する研究開発

実施研究機関：富士通(株)、NRIセキュア(株)、名古屋大学
研究開発期間：H25 年度～H27 年度
研究開発費：H25年5.2億円、H26年2.9億円、H27年1.7億円、・・・　計9.8億円
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

1. 目的
高度化・複雑化するサイバー攻撃からの脅威を防ぐため、利用者の行動特性等に応じて不正な通信の痕跡を発見し、ネットワークへの侵入及びマルウェアの感染等のサイバー攻撃による被害の程度並びに被害に至った経緯を明らかにする技術、及び当該情報に基づきサイバー攻撃への動的な防御を実現する技術を実現し、攻撃の早期検知と迅速な対処によりサイバー攻撃の被害を最小化することを目的とする。

2. 政策的位置付け
「情報セキュリティ2012」で定めた「我が国全体として対応能力を向上させるよう、サイバー攻撃に係る高度な検知技術等の研究開発を推進」を実行する。

3. 目標
利用者の行動特性及び環境特性の活用に着目することにより、組織内ネットワークにおける不正な通信等を検知する技術、サイバー攻撃の被害状況を把握する技術、及びサイバー攻撃の影響を最小化し業務を継続するネットワーク制御技術を確立する。

2. 研究開発成果概要

研究課題 I. 利用者の行動特性に基づくサイバー攻撃検知技術の研究開発

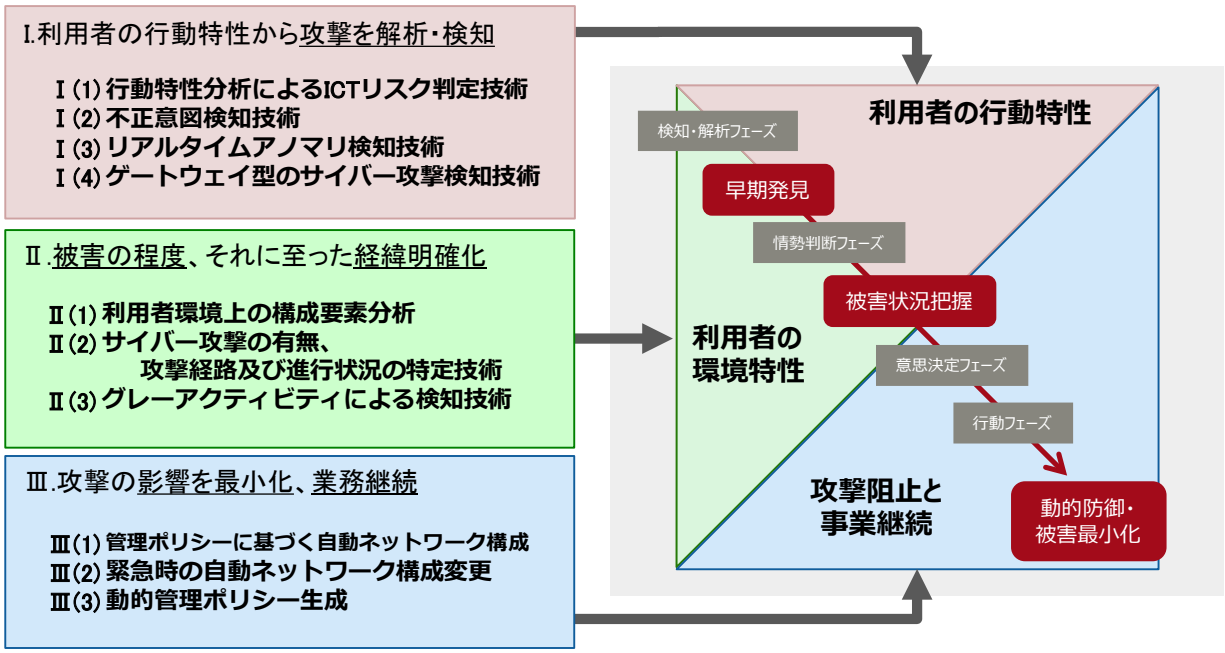
「利用者行動特性分析技術（富士通）」、「利用者の行動特性分析に基づく不正な意図の検知技術及び通信の制御技術（富士通）」「リアルタイムアノマリ検知技術（富士通）」「ゲートウェイ型のサイバー攻撃検知技術（NRIセキュアテクノロジーズ）」の開発により、利用者の行動特性からサイバー攻撃の検知を可能とした。

研究課題 II. 既存のログに依存しない利用者環境の特性を活用したサイバー攻撃の侵入経路及び進行状況を解析する技術の研究開発

「利用者環境上の構成要素分析技術（NRIセキュアテクノロジーズ）」、「利用者環境上の状態を用いたサイバー攻撃の有無、攻撃経路及び進行状況の特定技術（NRIセキュアテクノロジーズ）」「グレーアクティビティによる検知技術（NRIセキュアテクノロジーズ）」の開発により被害の程度、及び攻撃の経緯を明確化することを可能とした。

研究課題 III. サイバー攻撃の封込めと業務継続を可能とする組織内ネットワーク制御技術の研究開発

「管理ポリシーに基づく自動ネットワーク構成技術（名古屋大学）」、「緊急時の自動ネットワーク構成変更技術（名古屋大学）」、「動的管理ポリシー生成技術（名古屋大学）」の開発により、サイバー攻撃の影響を最小化し、業務継続を可能とした。



（続く）

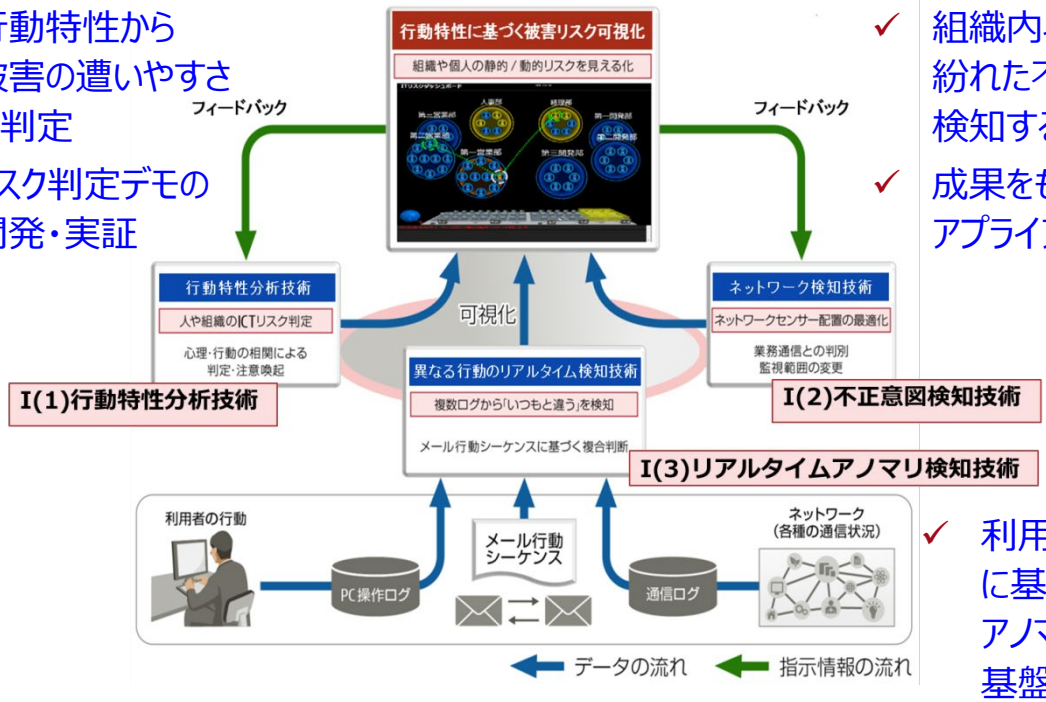
2. 研究開発成果概要（続き）

○ 攻撃の早期検知

「Ⅰ(1) 行動特性分析によるICTリスク判定技術」、「Ⅰ(2) リアルタイムアノマリ検知技術」と「Ⅰ(3) 不正意図検知技術」の連携により、利用者の行動特性から攻撃の解析、検知、及び早期対策を一連の流れとして実現した。

利用者の行動特性から攻撃を解析・検知・早期対策

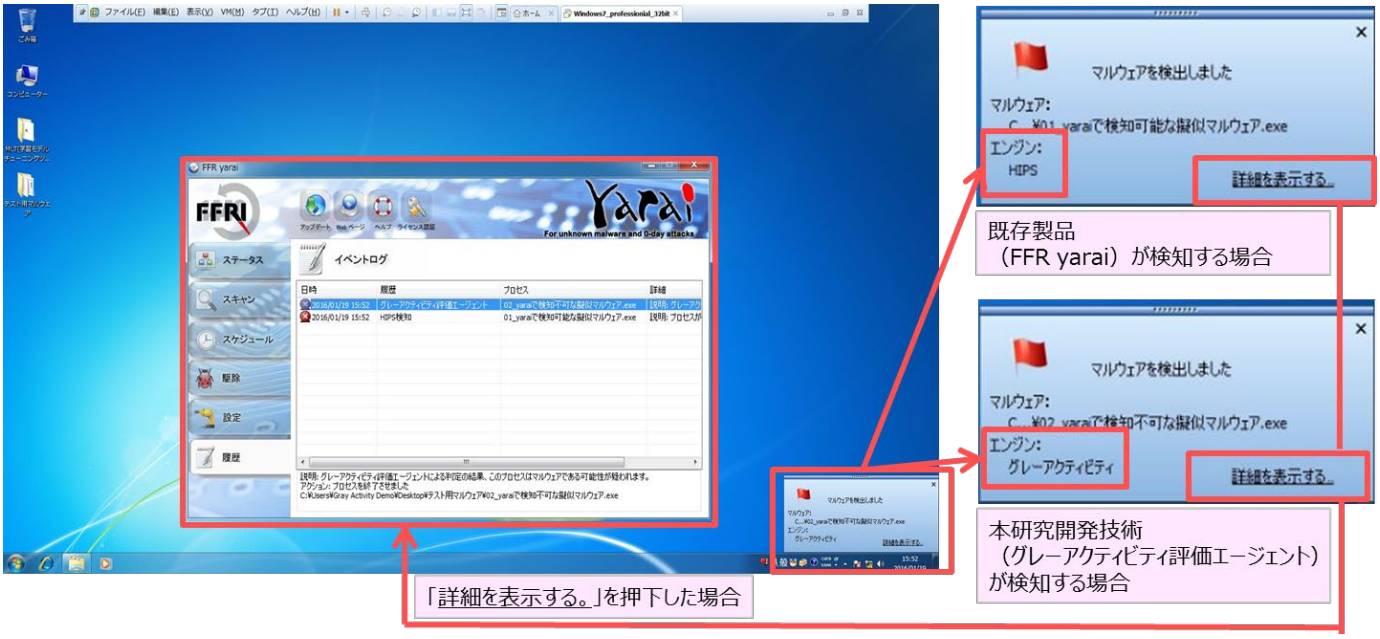
- ✓ 行動特性から被害の遭いやすさを判定
- ✓ リスク判定デモの開発・実証



- ✓ 組織内ネットワークに紛れた不正意図を検知する技術を開発
- ✓ 成果をもとにしたアプライアンスを製品化
- ✓ 利用者の行動特性に基づく、リアルタイムアノマリ分析・検知基盤を開発

○ 被害状況の把握

「Ⅱ(3) グレーアクティビティによる検知技術」を開発、既存製品との連携によりマルウェアの挙動検知を実現した。



- ✓ 端末及び、ゲートウェイにおける「グレーアクティビティ」の蓄積による攻撃経路の解析と被害範囲の特定技術 ⇒【マルウェア実行検知機能を開発】⇒【既存製品との連携】

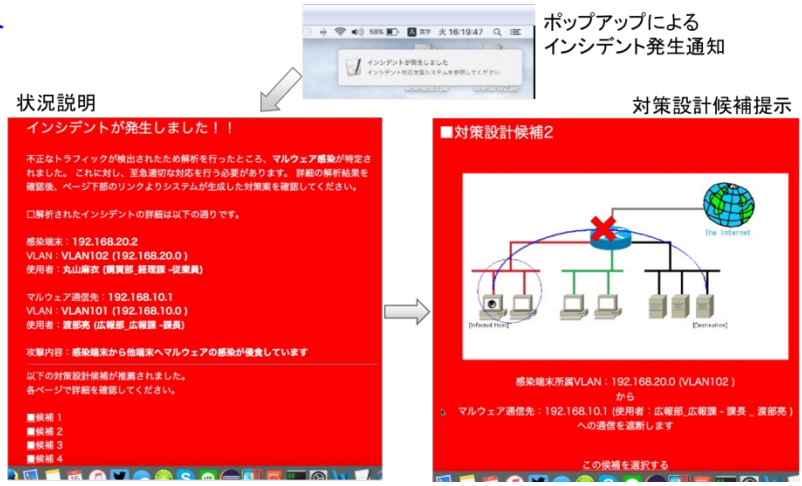
（続く）

2. 研究開発成果概要（続き）

○ 被害最小化

「Ⅲ(1) 管理ポリシーに基づく自動ネットワーク構成技術」、「Ⅲ(2) 緊急時の自動ネットワーク構成変更技術」、「Ⅲ(3) 動的管理ポリシー生成技術」の開発により、VLANによる被害対象の隔離を実現した。

- ✓ 感染経路遮断により通信(業務)継続を実現するインシデント対応補助システムを実装
- ✓ JSONによる組織/業務/サービス/機器の連携情報記述の提案
- ✓ ディレクトリサービスからの組織/権限情報の抽出の実現
- ✓ FPGA利用の高スループット通信特徴量抽出
- ✓ 軽量な動的/静的解析複合によるマルウェア分類
- ✓ 既知攻撃と未知攻撃を分類するアノマリ検知



ネットワーク管理者によるインシデント対応補助システム（IRSS）利用の様子

3. 政策目標の達成状況（経済的・社会的な効果）等

＜政策目標(アウトカム目標)の達成状況＞

○ 研究開発成果の社会展開に向けた主な取り組み

本研究成果をいち早く社会に還元し、アウトカムの効果を早期に発揮させるため、以下の取り組みを行った。

・成果物のうち、単独で社会的な有用性を発揮可能と判断される技術については、先行的に事業化(製品化・サービス提供)に取り組んだ。

・研究成果のうち、事業化や知財化を目指さないものについては、成果が得られ次第、速やかかつ積極的に学術発表や成果紹介を行った。これにより、事業のプレゼンスを高めるだけでなく、実証実験、成果の活用、成果の連携、及び発展課題に向けた取り組みにおける協力組織の確保が容易になる効果を得られた。

○ 終了評価用資料「今後の成果展開に向けた取組方針」に掲げた目標の達成状況

終了評価において以下のアウトカム指標(ベンチマーク)を定め、取り組んだ。(目標年度：平成30年)

① 社会的な有用性を発揮可能と判断される技術について自社グループ内やアライアンス先での製品を通じて事業化を推進した(指標：性能比、販売数量、売上高等)。終了条件を達成(「新たな市場の形成」を参照)

② 発展課題も含めて特許出願/取得及び学術発表や成果紹介を通じて事業プレゼンス向上に貢献した(指標：発表件数、特許出願件数等)。終了条件を達成(「知財や国際標準獲得等の推進」参照)

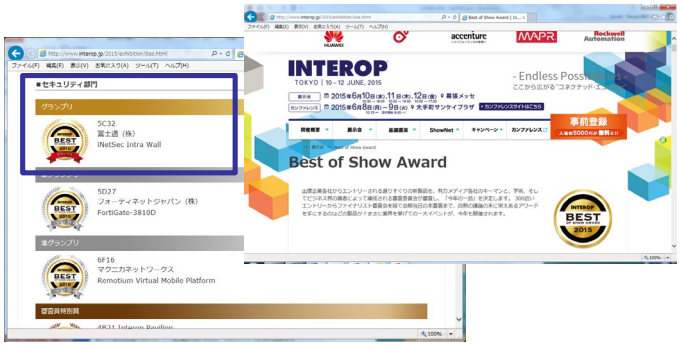
③ 実証実験等における共同研究機関相互及び他組織との協力体制を構築した(指標：協力体制に基づいて実施されるプロジェクト件数等)。終了条件を達成(「5項 副次的な波及効果」参照)

（続く）

3. 政策目標の達成状況（経済的・社会的な効果）等（続き）

＜新たな市場の形成、売上げの発生（GDP等増大）、国民生活水準の向上＞

○ 本研究成果の一部を先行して実用化し市場に製品を投入することで、攻撃の早期検知と迅速な対処によるサイバー攻撃の被害最小化を実現する製品市場を形成した。
「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。さらに、本製品を含む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され、国民の情報保護に寄与した。



「Interop Tokyo 2015 Best of Show Award」
セキュリティ部門グランプリを受賞
（平成27年6月10日発表）

○ 本研究開発で得られ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て既存の次世代エンドポイントセキュリティ製品（FFRIセキュリティ社 FFRI yarai）のチューニングに適用、性能向上を図ることで国産製品の売り上げに寄与している。
研究開発で開発したソフトウェア等を直接的に販売するには至らなかったが、研究開発のノウハウを役立てることができた。特に機械学習を使ったエンドポイントにおけるマルウェア検知製品は、技術の流れが非常に早く、そのような激しい競争環境の中、機械学習を使った国産製品として性能を維持、向上し販売が継続されている意味は大きいと考える。（研究課題 Ⅱ）

＜知財や国際標準獲得等の推進＞

○ 知財戦略に基づく特許取得、論文発表等の実績

項　目	委託研究終了時※1	昨年度末※1	追加数※1
特許出願数	26件（9件）	36件（17件）	10件（8件）
特許取得数	0件（0件）	28件（15件）	28件（15件）
査読付き誌上発表論文数	3件（0件）	8件（1件）	5件（1件）
査読付き口頭発表論文数 ※2	11件（11件）	24件（20件）	13件（9件）
その他の誌上発表数	1件（0件）	8件（3件）	7件（3件）
口頭発表数	22件（3件）	42件（3件）	20件（0件）
受賞数	2件（0件）	3件（1件）	1件（1件）
報道発表数	2件（2件）	2件（2件）	0件（0件）
報道掲載数	10件（2件）	10件（2件）	0件（0件）

※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
※2　印刷物を含む

○ ICITST-2015における発表の様子

会議名：10th International Conference for Internet Technology and Secured Transactions

開催地：London, 英国
開催期間：平成27年12月14日から16日まで
発表：RAT-based Malicious Activities Detection
on Enterprise Internal Networks
不正意図の検知方式について、本方式の検討過程である攻撃分析(RAT、攻撃手法) から、方式の提案・評価までの成果をまとめ発表（研究課題 Ⅰ）

4. 研究開発成果（アウトプット目標）から生み出された科学的・技術的な効果

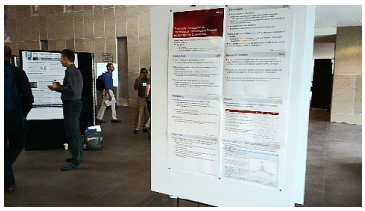
＜新たな科学技術開発の誘引＞

○ 本研究開発では、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、論文発表や国内外の展示会でデモ展示を行った。特に、ヒューマンインタフェース学会や人工知能学会など多様な学術分野で発表し、多くの論文から引用されている。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た。（研究課題 Ⅰ）

○ 人工知能学会第29回大会

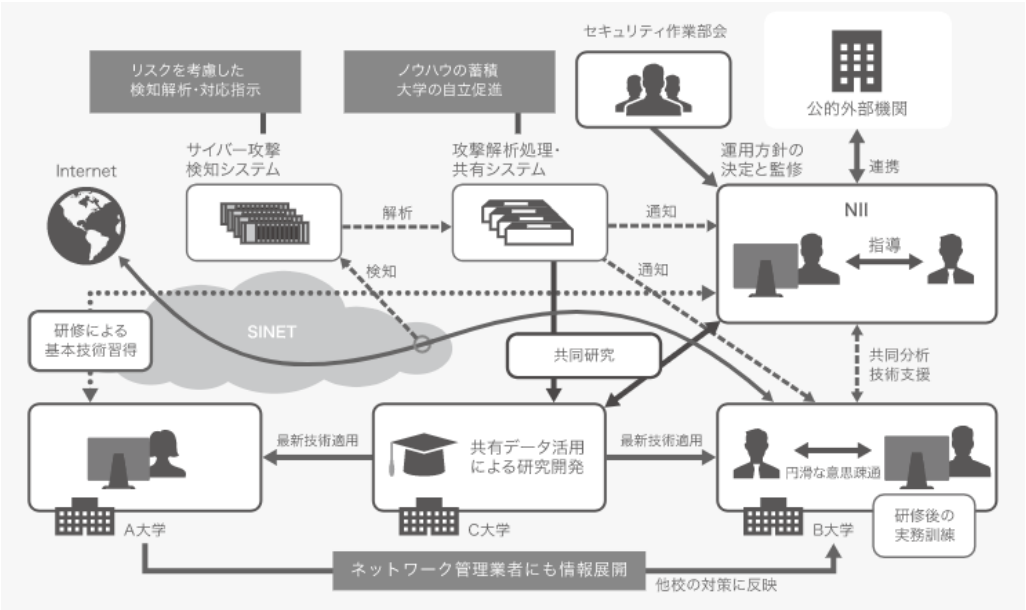
開催地：公立はこだて未来大学（北海道函館市）
開催期間：平成27年5月30日から6月2日まで
参加者数：1,200名 以上（発表648件）
発表：AI応用「産業・社会システムにおけるAI」セッションで発表
「利用者の行動特性分析に基づくセキュリティリスク判定技術の試作」
大学や企業の研究者などと情報交換を行った。

○ 国際会議 SOUPS(Symposium On Usable Privacy and Security) における発表の様子



開催地：オタワ市 カールトン大学（カナダ）
開催期間：平成27年7月22日から24日まで
参加者数：約180名
主催：CUPS（CyLab Usable Privacy and Security Laboratory, カーネギーメロン大学の関係団体）

○ 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、本研究課題であるインシデント・レスポンスの成果を組み込んでサイバー攻撃分析を実施している。（研究課題 Ⅲ）



図：情報セキュリティ運用連携サービス（NII-SOCS）の概要

（引用元: https://www.nii.ac.jp/service/nii-socs/）

○ マルウェアの挙動を機械学習により分析する技術を獲得した。これにより、アライアンスを通じて既存の次世代エンドポイントセキュリティ製品（FFRI yarai）におけるマルウェア検出エンジンの性能向上を実現した。（研究課題 Ⅱ）

5. 副次的な波及効果

＜副次的な波及効果＞

○ 国立研究開発法人情報通信研究機構(NICT)と連携し、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「Interop Tokyo 2016」(2016年6月に幕張メッセで開催)で動態展示され、Made in Japanによる多層防御の実現可能性を社会にアピールした。（研究課題 Ⅰ）

（出典:「NIRVANA改が更にバージョンアップ！ ～アラート管理機能の強化と国産機器連携でユーザビリティを大幅向上～」(平成28年6月7日、国立研究開発法人情報通信研究機構)

○ 本研究を契機として、学会、イベント、政府の主催する委員会・検討会、政府や関連組織（IPA）が委託する調査において本研究関係者（研究実施者、研究開発運営委員、ビジネスプロデューサ）との継続的な情報交換及び技術 交流を推進した。また、新たな企業や学術機関など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、産官学による研究コミュニティの拡大に寄与した。

6. アウトカム目標の達成に向けた取組計画の達成状況等

＜アウトカム目標の達成に向けた取組計画の達成状況＞

○ 本研究開発では、共同研究を担う3機関に研究者とは別に1名ずつ「ビジネスプロデューサ」を設置した。さらに、研究開発全般にわたり取組みの進捗状況について総括する「総合ビジネスプロデューサ」を設置してアウトカム目標の達成に向けて取り組んだ。

○ 総合ビジネスプロデューサは、研究開発に資する市場動向等の調査を行い、ビジネスプロデューサに提供した。これを踏まえ、商品化やプロモーション、産学連携の権限を持つビジネスプロデューサが周知広報や事業化、実用化戦略を立案し、研究者及び事業部門がこれを実行した。

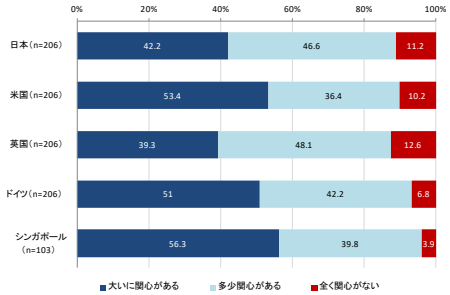


図: 海外アンケート結果 例1
本成果に基づく製品への関心

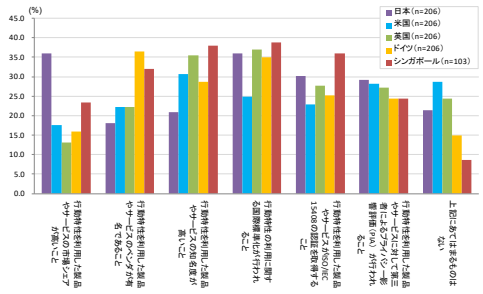


図: 海外アンケート結果 例2
懸念を解消するための対策として重要な要素

＜周知広報活動の実績＞

○ 誌上論文発表、口頭論文発表、口頭発表、その他市場発表、報道発表、報道掲載、展示会については、3項及び4項を参照。

○ 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という発展的なセキュリティ課題の研究を推進し成果を論文発表、口頭発表で継続的に発信。

（研究課題 Ⅲ）

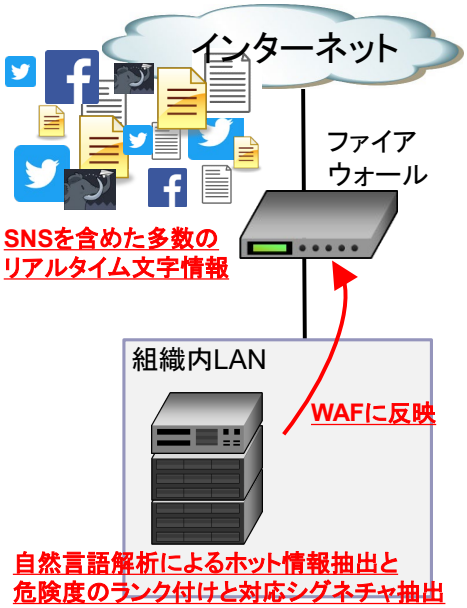


図: オープンアクセス情報からの
WAFシグネチャ生成

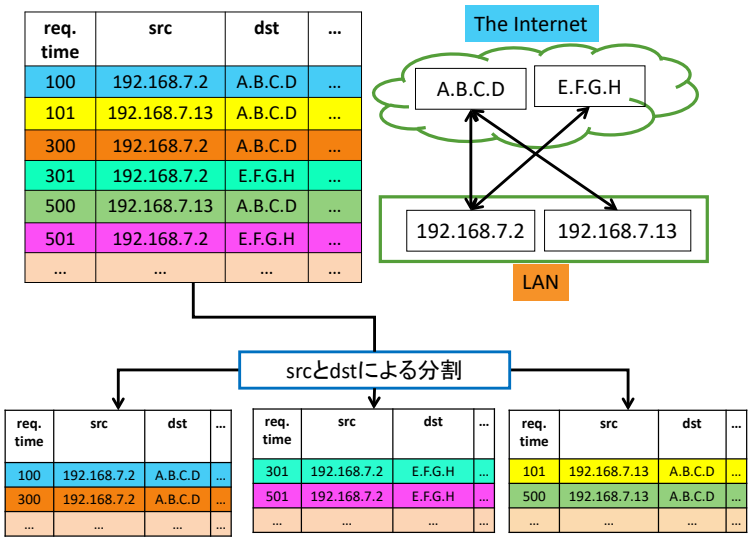


図: HTTPリクエスト/レスポンスペアによるC2検知

（続く）

6. アウトカム目標の達成に向けた取組計画の達成状況等（続き）

＜周知広報活動の実績（続き）＞

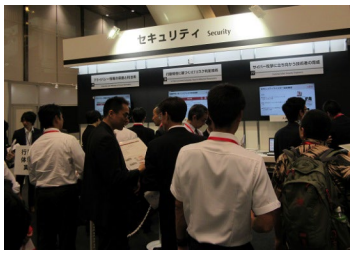
○ 総務省が主催するICTイノベーションフォーラム2016での発表とポスターセッション、及び富士通が主催する展示会である富士通フォーラム（有楽町）とFujitsu Forum 2015 Munich（ドイツ）での研究成果のデモ展示をはじめ、多くの成果発表を実施、積極的に研究成果の普及を行った。
具体件数は「知財や国際標準獲得等の推進」参照。（研究課題 Ⅰ、Ⅲ）

○ ICTイノベーションフォーラム2016の概要

開催期間：平成28年10月4日、会場：幕張メッセ 国際会議場
発表：ICT重点技術の研究開発 オーラルセッション「サイバー攻撃の解析・検知に関する研究開発」
ポスターセッション：「サイバー攻撃の解析・検知に関する研究開発」

○ 富士通フォーラム 2015の概要

開催期間：平成27年5月13日より15日まで、会場：東京国際フォーラム
総来場者数：約20,000人
展示タイトル：行動特性に基づくICTリスク判定技術、展示デモ体験者：約560名



実際のデモ風景：
アンケート入力により行動特性を取得し、ICTリスクを判定

○ Fujitsu Forum Munich 2015の概要

開催期間：平成27年11月18日から19日まで
開催地：独 International Congress Center Munich （ICM）
来場者数：14,000人以上

＜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）

○研究開発成果の情報発信：
基本計画書「6. その他」に、本研究開発終了後に成果を論文発表、プレス発表、製品化、ウェブサイト掲載等を行う際には「本技術は、総務省の『サイバー攻撃の解析・検知に関する研究開発』による委託を受けて実施した研究開発による成果である。」という内容の注記を発表資料等に都度付すことと記載されている。
これに従い、研究開発終了後も査読付き誌上発表論文、印刷物を含む査読付き口頭発表論文、技術紙への誌上発表、口頭発表、報道発表、社外展示会、社内展示会において、所定の内容を記し、外部発表投稿の手続きに従って確認、及び報告を行った。

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＞

○ 本プロジェクトは、サイバーセキュリティ2015で掲げた「国民が安全で安心して暮らせる社会の実現」を目指し、高度化・巧妙化するマルウェアの被害防止に向けた総務省の取り組みの一部である。サイバー攻撃の解析・検知技術の課題である攻撃の早期検知、被害状況把握、動的ポリシー管理を活用した被害最小化技術の開発により基礎技術の獲得に貢献した。特に、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まさに始まっていた時期であり、各国において国のバックアップのもとで研究が行われていたと考えられる。国内でそのような最先端の研究促進を行い、また具体的な事業に繋げた意味は大きい。ノウハウなどが活用された点、機械学習に強い技術者の育成といった副次的な効果も大きい。
さらに、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、NICTが取り組んでいるセンサーの高度化による観測機能強化の研究との連携を実現したという日本の研究者や研究機関との連携促進という副次的な波及効果が得られた。これらの点から、当該プロジェクトとそのテーマ設定は、国家プロジェクトとして妥当であった。

＜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＞

○ 基本計画書に従って外部の学識経験者、有識者等で構成される研究開発運営委員会を設置したことが、研究成果の有効性向上に大きく寄与した。関連する要素技術間の調整、成果の取りまとめ方、研究開発全体の方針について幅広い観点から助言いただいた。

○ 研究開発運営委員に、サイバーセキュリティの学識経験者と有識者に加えて、人文社会科学系の若手研究者が参加し、行動心理学や疫学における感染モデルの知見という視点で助言をいただいたことは本プロジェクトの成功点であると言える。