サイバー攻撃の解析・検知に関する研究開発
R&D of detective and analytical technology against advanced cyber-attack

代表研究責任者　津田 宏　　富士通株式会社

研究開発期間　平成 25 年度～平成 27 年度

【Abstract】

The cyber attack in recent years including the target type attack might pass through existing information security measures because it is repeated obstinately by making good use of the sleight of hand. This research is the one working on the achievement of technologies that detects behavior different from routine work and malicious access ,etc and understands damage situation and that network control technology that minimizes influence of attack and continues business by paying attention to the use of user's behavioral characteristics and environmental characteristics.

This research achieves the environment for which information can be safely used by applying appropriate measures approach responding to user's behavioral characteristics and continuing the business without the influence according to the status of damage even when damage occurs without pressing an excessive load and the limitation to the user.

1　研究開発体制

○ **代表研究責任者**　塩崎 哲夫（富士通株式会社）　平成 27 年 6 月 19 日まで
津田 宏（富士通株式会社）　平成 27 年 6 月 20 日から

○ **研究分担者**　塩崎 哲夫（富士通株式会社）　平成 27 年 6 月 19 日まで
津田 宏（富士通株式会社）　平成 27 年 6 月 20 日から
西田 助宏（エヌ・アール・アイ・セキュアテクノロジーズ株式会社）
高倉 弘喜（名古屋大学）　平成 25、26 年度
嶋田 創（名古屋大学）　平成 27 年度

○ **総合ビジネスプロデューサ**　冨田 高樹（みずほ情報総研）

○ **ビジネスプロデューサ**　太田 大州（富士通株式会社）
菅谷 光啓（エヌ・アール・アイ・セキュアテクノロジーズ株式会社）
高田 広章（名古屋大学）

○ **研究開発期間**　平成 25 年度～平成 27 年度

○ **研究開発予算**　総額　1,025 百万円

（内訳）

平成 25 年度	平成 26 年度	平成 27 年度
550 百万円	300 百万円	175 百万円

２　研究開発課題の目的および意義

近年、標的型攻撃をはじめとしてサイバー攻撃の高度化・複雑化が進展し、既存の情報セキュリティ対策ではネットワークへの侵入、マルウェアの感染等の情報セキュリティ上の脅威を完全に防ぐことが困難となっている。

こうした状況においてサイバー攻撃の被害を最小化するには、攻撃を早期に検知し迅速に対処することが重要である。そのため、本研究開発においては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及び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の研究開発を実施する。

（１）　政策目標（アウトカム目標）

2011年以降、国や国の安全に関する重要な情報を扱う企業等に対する標的型攻撃が相次いで明らかになる等、従前とは態様が異なる新たなサイバー攻撃の脅威が顕在化している。例えば、メールを利用した標的型攻撃では、攻撃対象となる利用者にあわせて時事情報等を組み込むなど、文面を巧妙化しメールを開封するよう仕向けるなど高度なソーシャルエンジニアリングの手法が用いられている。

そのため、本研究開発で得られた成果を実用化することで、利用者の行動特性に応じて適切な対策を適用するとともに、被害が発生した場合においても被害の進行状況に応じて影響のない業務を継続可能とし、利用者に過剰な負荷・制限を強いることなく安全に情報が活用できる社会の実現に貢献する。

（２）　研究開発目標（アウトプット目標）

標的型攻撃をはじめとする近年のサイバー攻撃は、巧妙な手口を駆使して執拗に繰り返されるため、既存の情報セキュリティ対策では対処することが困難である。

そのため、本研究開発では、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。

３　研究開発成果（アウトプット）

３．１　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

（１）　利用者の行動特性分析技術

標的型攻撃を受けやすい（受けにくい）利用者個人の差異、所属部署及び取り扱う情報等の差異を考慮し、標的型攻撃の検知及び被害との相関、利用者個人の行動特性に係る複数の因子を抽出する技術を確立する。

また、数百名規模の行動特性・プロファイル共有システムを実現し、課題Ⅰ．～ Ⅲ．と連携して、サイバー攻撃の迅速な検知並びに所属部署及び利用者個々人の行動特性を加味した柔軟かつ高効率な情報セキュリティ対策を実現する基盤技術を確立する。

（２）　利用者の行動特性分析に基づく不正意図の検知技術及び通信の制御技術

利用者の行動特性の分析によりプロファイリングされた情報、実際の利用者の行動との比較分析、類似の行動特性等を有する者との相関分析等を基に、ネットワーク及びサーバの負荷を抑えつつ迅速にマルウェア感染を検知する技術を確立する。

また、マルウェア感染が検知された場合に、影響の範囲及び影響度に応じた利用制限、監視強化等を実現するため、リアルタイムに経路制御を行う技術を確立する。なお、本経路制御技術は、複数の拠点からＷＡＮ経由で通信を誘導可能とする。

（３）　利用者の行動特性分析に基づくリアルタイム・アノマリ分析技術

時々刻々変化する利用者の状況を時系列データとしてリアルタイムに収集・学習し、利用者の行動特性・プロファイルと組み合わせて、リアルタイムなアノマリ分析を可能とし、定常でない状態（異常と疑われる状態）を検知し、アラーム通知を可能とする。

（４）　利用者のプロファイル情報を用いたゲートウェイ型のサイバー攻撃検知技術の研究開発

組織の特徴や利用者の特徴といった利用者のプロファイル情報を既存のゲートウェイにおける検知技術と組み合わせて標的型攻撃の検知を行う技術の研究開発を行う。これにより、従来の技術では検知することが困難であった高度な攻撃の検知や運用負荷を高めている誤検知を低減させ、標的型攻撃の検知性能を飛躍的に向上させる。

課題Ⅰ(1)利用者の行動特性分析技術では、被害に遭いやすい人の行動特性によるリスク判定技術を開発、人や組織に合せた対策手法を構築し、I(2),(3)との連携も考慮した組織リスク可視化により行動特性分析技術の有用性を評価した。

ICT 被害に遭いやすい人の行動特性に基づき開発した人の行動特性クラスに合わせた対策手法では、人の行動特性に基づくリスク判定ツールを開発し、国内外の展示会にて 500 名以上に対してトライアルを行った。その結果、職種においては営業、業種については金融や教育のリスクが高いなど、クラスによってリスクが異なることが分かった。

人に合わせたアラート画面の開発では、インターネットユーザ約 1500 名に対する Web アンケート調査を行い、周りの人の行動を適切に共有することは有効であり、例えば社給 PC と私物 PC 間での業務ファイルのやりとりが多い人や、PC 内のファイル整理をあまりしない人ほど、自身のメール操作の危険性を注意深い人のメール操作との数値比較をもって注意喚起する画面案を支持することなどを確認した。

行動特性分析による対策手法として、疫学の感染モデルも参考に、標的型メール攻撃を受信した場合に、よくメールをする人や当該ドメインとよくやりとりするなど、周りの関連する人のつながりから、類似の攻撃を受けそうな人に対してメールや Web のアクセスを制限するなどポリシーを強化するデモシステムを開発した。これを活用し、課題 I(2)(3)とも連携して被害リスク可視化システムを構築し、ICT リスク判定や匿名化ログをサーバで共有することで、個人や組織のリスクを可視化。標的メールなどの攻撃があった場合に、I(2)のネットワークセンサーの監視ポリシーを強化したり、I(1)で関連しそうな人のメール閲覧などの PC 操作をあらかじめポリシーで制限するなど、人や組織に合わせた、早期の事前対策につなげたりすることが可能であることを確認した。

課題Ⅰ(2)利用者の行動特性分析に基づく不正意図の検知技術及び通信の制御技術では、利用者の行動特性の分析により、利用者通信に紛れた不正意図を抽出し、踏み台となった端末を特定、通信を制御して対策を行う技術の実現を目指し研究開発を行った。

不正意図の検知技術の研究開発においては、組織内ネットワークを監視・解析し、その情報を統合サーバに収集・統合することで、利用者の通常通信に紛れた不正意図を抽出する技術の研究開発を実施し

た。単独のセンサー、もしくは複数のセンサー装置が連携してマルウェアの諜報活動を解析・検知し、踏み台を特定する技術を開発した。実験環境にて、入手したマルウェア(9 種類)を動作させた場合、すべて検知することができた（検知率 100%)。この中には、既存の Anti Virus ソフトや IDS では検知できないマルウェア活動(諜報活動)も含まれる。

検知技術の最適配置技術においては、本不正意図の検知技術を搭載した小型ネットワークセンサー装置を試作し、10～20 台程度の小規模ネットワークにおけるマルウェア活動が検知可能であることを確認した。また、本技術を搭載した大型ネットワークセンサー装置を試作し、数百台程度の PC が接続される基幹ネットワークでマルウェア活動が検知可能であることを確認した。さらに、課題 I(1)、(3)と連携することで、組織ごとのリスク状態の高低などに応じ、複数のネットワークセンサーを連携させ、監視精度・配置の自由度を調整できるようにした。

通信の制御技術の研究開発においては、感染が疑われる端末通信を誘導するスイッチ機能とトンネル GW 機能を、それぞれ SDN スイッチ装置とネットワークサーバ装置に搭載し試作した。さらに、トンネル GW 機能については、リモートへの誘導評価検証及び誘導に伴う影響検証を行い、フィードバック対応を実施した。また、SDN スイッチ装置と連動して制御可能なコントローラーの実現方式検討を実施した。結果として、問題と思われる端末が検知システムから通知された場合に、安全かつ確実に自動的に該当端末の通信のみを対策用仮想ネットワークに誘導するような制御を行う制御アプリケーションと、制御アプリケーションからの指示により各機器に設定を行うコントローラーの実現の目途がたった。

課題Ⅰ(3)利用者の行動特性分析に基づくリアルタイム・アノマリ分析技術では、これまでリアルタイムに検知することが難しかったサイバー攻撃を、利用者の行動特性に基づき、リアルタイムにアノマリ分析・検知する技術を開発し、実証実験でその有用性を確認した。

リアルタイム・アノマリ分析技術では、通信データ、メール操作、Web アクセスなどの個人/組織の行動ログに対して複数の検知処理を適用し、それらの結果を組み合わせてパターン化したものを普段の行動として学習し､その学習結果と現状の行動の違いをアノマリとして検知する複合判断機能を開発した。さらに、一つひとつの時系列データ（イベント）を高速に分析するとともに、長期間に及ぶデータをコンパクトに効率良く処理する高速化機能を開発した。これにより、マルウェアのような短時間でのアノマリに加え、長期間に渡るアノマリのリアルタイム検知も可能となった。

本技術に関し、実マルウェア 1 種類の動作データに対する検知実験を行い、少量の誤検知を含むものの、検知に成功した（498 プロセス中、5 プロセスをアノマリと判断。うち、1 つがマルウェア)。性能については、検知性能は 20 ノード構成で 17.0 万イベント/秒、複合イベント処理（データ前処理）は 20 ノード構成で 263 万イベント/秒を達成した。さらに、社内の実証実験環境にてやり取り型の標的型メール攻撃の模擬攻撃を実施し、メール受信を起点とする利用者の一連の操作を関連付けることで、マルウェア感染前の検知に成功した。従来技術（メール、Web アクセス、ファイルダウンロードごとの単体検知）と比べ、検知数を 10 分の 1 以下に抑制でき、さらに、検知向け照合データ量を 10 分の 1 以下に削減できた。

また、課題 I(1)、(2)と連携して、本技術でマルウェア感染前に攻撃行動を検知することにより、課題Ⅰ(1)、(2)における監視ポリシー強化等、早期の事前対策を実施できることを確認した。

課題Ⅰ(4)利用者のプロファイル情報を用いたゲートウェイ型のサイバー攻撃検知技術の研究開発では、企業毎の特性が出やすいと考える組織情報を活用した利用者プロファイル情報と既存のゲートウェ

イでの標的型攻撃対策システムを組み合わせた検知技術を試作してその性能を評価した。

はじめに、インターネット上に公開されているセキュリティ関連のニュースやセキュリティベンダー等のレポートをもとに利用者のプロファイル情報と標的型攻撃の関連性について調査を行い、国家活動や重要インフラに関わる情報等、機密性の高い情報を扱う組織が攻撃に狙われやすい傾向があったことから、利用者プロファイル情報となり得る情報として、機密情報又は重要情報の取り扱いの有無および公開窓口（外部とのやり取りが可能なメールアドレス）の有無を挙げた。そして、「機密情報又は重要情報の取り扱いの有無」については、機密情報を扱う場合には脅威を見逃さないために検知技術の検知感度を上げ、機密情報を扱わない場合には誤検知を低減させるために検知感度を下げるといった活用方法を検討した。また、「公開窓口か否か」も同様に検知感度の調整に活用できると考えた。

本研究開発技術では、脅威レベルとその重み付けによりポイントを積算し、アラート感度補正値によってポイントを最終調整する。そして、最終調整したポイントが指定された閾値以上の場合に攻撃と判断する。このアラート感度補正値と連動する脅威レベルは、検体の特徴や動作をもとに「高」、「中」、「低」の 3 種類が存在し、脅威レベルが高いほうが攻撃の可能性が高くなる。アラート感度補正値は、端末および脅威レベル毎に個別に設定可能なため、特定組織または特定端末といった粒度で脅威レベルに応じたアラート感度補正を適用することができる。

利用者プロファイルを活用し、脅威レベル「中」に対しアラート感度補正値を適用することで、誤検知率を約 23%低減しながらも検知率は約 7%の低下に抑えることができた。そのため、機密情報を取り扱う部署や公開窓口以外の攻撃されにくい部門等において、セキュリティを確保しながらも運用負荷を下げる目的で本技術を活用できることを確認した。

３．２　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

（１）利用者環境上の構成要素分析技術

サイバー攻撃の有無、攻撃経路及び攻撃の進行状況を特定するため、必要な状態を特定して既存ログとの有効性を比較するとともに、必要なデータを抽出する技術を確立する。また、各対象機器から必要なデータを最小限の頻度で抽出する技術及び組織内ネットワーク上に存在する機器を把握する識別技術を確立する。さらに、課題Ⅱ（２）の実施状況を踏まえ、検知精度の向上に必要な状態を追加・変更して抽出する技術を確立する。そして、これらの技術を基にマルウェア感染の有無を特定し、マルウェア感染の要因を根絶する技術を確立する。

以上の技術について、一般的な組織のネットワーク構成を踏まえ、本技術を大規模組織に適用した際のフィージビリティを、5 つ以上のブロードキャストドメインを持つネットワーク上で検証する。

（２）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

課題Ⅱ(1)の技術により抽出した状態を利用者環境の特性を踏まえて分析する技術、及びマルウェア感染が疑われる機器の活動を過去に遡り把握する技術を確立する。また、実際にマルウェア感染が疑われる機器の活動、抽出した情報、分析結果等を１箇所に集約して時系列で表示することにより、組織内ネットワーク上の端末、サーバ等の他の機器に同様のマルウェア感染が発生していないかを一括で特定可能な技術を確立する。

最終的には、課題Ⅱ(1)の開発と連携し、本技術を大規模組織に適用した際の有効性を確認するた

めに、100 台以上の機器で検証する。

（3）端末および、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の開発

端末および、ゲートウェイにおいて、マルウェア感染が発覚した場合、微妙であった判定結果や怪しい挙動のログである「グレーアクティビティ（怪しい挙動)」を効率的に蓄積、分析する技術の研究開発を行う。これにより、標的型攻撃の痕跡を発見した後に、迅速な攻撃経路の解析と被害範囲の特定を行う。

平成 25 年度には、1 セグメントに 60 台、2 セグメントで合計 120 台規模のクライアントから構成される検証環境を構築し、その環境を用いての検討及び検証を進めた。まず、基礎調査としてマルウェア等の攻撃手法を調査し、攻撃の有無、攻撃経路及び進行状況の特定技術の研究開発のための類似技術/製品の調査として、ハニーポット技術及びネットワークフォレンジック技術の調査を行った。特に攻撃手法の調査については、外部環境の変化に対応するためにも、平成 26 年度以降も継続して実施している。また、基礎調査を踏まえて、Windows 端末における攻撃検出を目的としたベースライン作成のため、及び攻撃経路や影響範囲等の調査のための Windows 端末上での具体的なモニタリング対象の選定を行った。選定した対象については、収集するための手段を整理し、収集の実現可否を見極めるための動作検証を実施した。ネットワーク構成把握技術の確立については、類似技術の調査/検証を完了し、特定技術の設計を進めた。

端末および、ゲートウェイにおける攻撃経路の解析と被害範囲の特定技術について、クライアント端末からグレーアクティビティを記録する機能の開発及び検証を実施した。加えて、構築した検証環境に同機能をインストールし、収集、蓄積技術の設計を実施した。また、標的型攻撃のアクティビティを調査分析するための対象マルウェア検体を選定し、検証環境にて対象マルウェア検体のアクティビティを取得/分析した。

平成 26 年度には、平成 25 年度の研究結果を基に、組織内ネットワーク上に存在する機器を把握する識別技術、課題Ⅱ(1)の技術により抽出したグレーアクティビティと称する利用者環境の特性を踏まえてマルウェアを検知する技術を試作するとともに、平成 25 年度に構築した検証環境を用いての評価を行った。その結果、特に、グレーアクティビティを用いた標的型攻撃の攻撃経路と被害範囲を特定するマルウェア検知技術については、既存の振る舞い検知型の標的型攻撃対策ソフトウェアでは検知できないマルウェアに対して、検知率 69.16%、誤検知率 4.78% という実用化が望める評価結果を得ることができた。

そして、平成 27 年度には、グレーアクティビティを用いた新たな標的型攻撃検知技術と既存の振る舞い検知型の標的型攻撃対策ソフトウェアとを連携する開発を実施したことにより、本研究開発技術を同標的型攻撃対策ソフトウェアに組み込む形での製品化に一定のめどをつけた。

また、研究開発マネジメント上での工夫としては、基礎調査及び環境構築が完了した平成 26 年度から、技術の試作及び評価テストを円滑に進行するために製品開発の経験が豊富なメンバーを加え、コンサルティング分野及び製品開発分野に精通したメンバーを含む研究開発体制を構築した。そして、もっとも実用化が望める研究開発技術に対して重点的にリソースを割り振るなど、費用対効果が高まるようにめりはりをつけた開発を行った。

３．３　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

（1）管理ポリシーに基づく自動ネットワーク構成技術

管理ポリシーを表現するための記述法、当該ポリシーに基づいた論理ネットワークの構築及びネットワーク間のアクセス制御技術を確立する。また、設計された複数の候補について、組織外ネットワークとのアクセス性及びサイバー攻撃のリスクを自動的に評価する仕組みを確立する。

（2）緊急時における自動ネットワーク構成変更技術

標的型攻撃を検知し、被害が発生していると推定されるネットワークに対するアクセス制限及び組織ネットワークからの切離しを実行するとともに、今後の攻撃対象と推定されるネットワークの保護及び対象外となったネットワークでの業務を継続させるネットワーク構成技術を確立する。

（3）動的管理ポリシー生成技術

サイバー攻撃に関係せずかつ管理ポリシーに照らし合わせて、業務継続に不可欠と判断される通信を特定する技術を確立する。さらに、サイバー攻撃への対処完了後に、サイバー攻撃の侵入経路となった通信、被害拡大の要因となった通信及び業務継続に不可欠であった通信を明らかにし、新たな管理ポリシーの候補とこれを適用する際に必要となるネットワーク構成の組を複数生成し、可視化して提案する技術を確立する。

サイバー攻撃耐性の高い VLAN により細かなサブネットに分割された組織内ネットワークの構成を自動化する「管理ポリシーに基づく自動ネットワーク構成技術」の研究項目については、業務のポリシー記述や業務用サーバ情報から研究を実施した。この研究の成果により、対サイバー攻撃ネットワーク構成を、当初は業務のポリシー記述から生成した粗分割のネットワークから開始し、粗分割ネットワークにおける実トラフィックをもとに提示される細分割ネットワーク候補から細分割ネットワークを選択することで、ネットワーク管理者の負荷低減が可能となる。また、業務のポリシー記述については XML よりも簡潔に記述可能な JSON を用いて組織情報や業務サービス情報を記述時に既存の情報との関連を容易にするシステムを開発し、管理者の作業量を約 43%に削減した。さらに、業務のポリシー記述と通信量変化を連動させることにより、対サイバー攻撃時の緊急ネットワーク構成変更時の業務への予期せぬ副作用や対策により発生するマルウェアの挙動変化の発見にもつなげることができることを示した。マルウェアの早期発見を行う巡回監視についても本項目で実施し、感染レベルという変数を導入して巡回監視と検知システムの双方を制御するアルゴリズムについて提案を行った。

マルウェアを利用したサイバー攻撃を被った時に、マルウェアの封じ込めと業務継続の両立を実現する「緊急時における自動ネットワーク構成変更技術」については、管理者への対策ネットワーク提示システムを開発し、被験者を用いてその有用性を示した。本システムでは、マルウェアに侵入された細分割組織内ネットワークに対して、その VLAN 内の端末が新たにマルウェアに感染する可能性の定式化、段階を踏むサイバー攻撃の攻撃段階の影響度の定式化、業務影響算出の定式化、などの各種の定式化を行い、複数の対策ネットワーク提示と各対策ネットワーク選択時の危険度や業務影響を数値と可視化の複合によりネットワーク管理者に提示させ、対策ネットワークの選択を迅速化させる。このシステムはウェブサーバとウェブブラウザ上で動く Java アプレットで構成されており、OS やデバイス形態に依存しないという利点もある。被験者を用いた評価の結果、最短の対策ネットワーク選択は優れた管理者よりは劣るが、対策ネットワーク選択の最悪時間の大幅な短縮(約 37%)と平均時間の短縮(約 70%)を実現し、一般的な管理者のサイバー攻撃対応能力向上に効果があることを示した。また、システム実行に必要と

なる情報の一部を組織内で使われるディレクトリサービスから自動収集する方法についても研究を行い、システム導入の負担を下げる試みも行っている。

サイバー攻撃を検出し自動ネットワーク構成変更のトリガとなる「動的ポリシー生成技術」については、対外接続部と比較して格段に通信量の多い組織内ネットワークからアノマリ検知用情報を抽出するFPGA を利用した HW/SW 複合型アノマリ検知、ドライブバイダウンロード系列を安全に解析可能なトラフィックのリダイレクトを伴う悪性通信解析システム、トラフィックシーケンス単独によるマルウェア分類、マルウェアバイナリとトラフィックの複合によるマルウェア分類、SVM や DBSCAN を用いてセッションデータのクラスタリングを行うことによる未知攻撃の検出、組織内ネットワークでの拡散を画策する標的型攻撃に利用されるマルウェアに特化した動的解析環境、などの様々な攻撃手法に対応すべく多数の研究を実施した。これらの研究成果の複合により、ソフトウェア等の未知の脆弱性を突く攻撃、亜種マルウェアを利用して既存のセキュリティ対策をすり抜ける攻撃、ドライブバイダウンロードにより本命マルウェアを隠す攻撃、などの近年のサイバー攻撃の手法に対して自動ネットワーク構成変更を適用するトリガを生成することが可能となった。

４　政策目標（アウトカム目標）の達成に向けた取組みの実施状況

平成 25 年度から 27 年度までの 3 年間に渡り、毎年 3 回のビジネスプロデューサ会議を開催し、研究開発期間中の事業化に向けた取り組み状況の共有及び課題の解決に取り組んだ。また、総合ビジネスプロデューサは各実施機関における事業化計画状況を随時把握し、当初設定したアウトカム指標の達成に向けて必要な調整を行った。こうした取り組みと並行して、市場調査活動として競合製品や標準化動向の把握を行うとともに、国内外でのウェブアンケート調査の実施を通じて、研究開発成果の市場での受容可能性や関心など、事業化計画立案に資する情報の収集を行い、調査結果を実施機関に提供した。

５　政策目標（アウトカム目標）の達成に向けた計画

本研究開発の成果は、各実施機関によりまず実施機関単独での製品・サービス化への取り組みが行われた後、連携による事業化についても検討が行われる方向となっている。一方、富士通と名古屋大学の研究開発成果については、各種学会・国際会議等での発表、プレスリリース等により、社会的な認知度を高めるための取り組みが実施されている。

こうした取り組みを通じて、本研究開発の成果が社会的に活用されることで、サイバー攻撃下におけるシステムの可用性の向上、損失額の減少、利用者が要するサイバー攻撃対応の時間の減少といったアウトカムの達成が見込まれるだけでなく、その派生効果として、こうした本研究開発成果を活用した ICT 環境による高いレジリエンスを備えた社会の実現が期待される。

６　査読付き誌上発表論文リスト

[1]大平健司，山口由紀子，八槇博史，高倉弘喜，星野寛，中野博樹，″インシデント対応を考慮した IPv6 ノード情報収集システムの設計と試作″，電子情報通信学会論文誌 D，Vol.J96-D，No.6， pp.1483-1492 (2013 年 6 月).

[2]北川直哉，高倉弘喜，鈴木常彦，″通信挙動の特異性を利用した spam 送信ホスト検出システムの開発″，電子情報通信学会論文誌，Vol. J97-D，No.5，pp.987-1000 (2014 年 5 月)：

[3]長谷川皓一，山口由紀子，嶋田創，高倉弘喜，″標的型攻撃に対するインシデント対応支援システム″，情報処理学会論文誌 Journal of Information Processing，Vol. 57，No. 3，pp. 836-848 (2016 年 3 月)：

７　査読付き口頭発表論文（印刷物を含む）リスト

[1]Yang Zhong，Hirofumi Yamaki，Yukiko Yamaguchi，Hiroki Takakura，“ARIGUMA Code Analyzer: Efficient Variant Detection by Identifying Common Instruction Sequences in Malware Families”，The 37th Annual International Computers，Software and Applications Conference (COMPSAC2013)，pp.11-20，DOI：10.1109/COMPSAC.2013.(2013 年 7 月)：

[2]Hajime Shimada，Yukiko Yamaguchi，Hiroki Takakura，“Capability of Anomaly Detection Enhancement with FPGA plus Large Capacity CAM”，International Workshop on Innovative Architecture for Future Generation High-Performance Processors and Systems (IWIA) 2014，pp.1-3 (2014 年 3 月)：

[3]Soshi Hirono，Yukiko Yamaguchi，Hajime Shimada，Hiroki Takakura，“Development of a Secure Traffic Analysis System to Trace Malicious Activities on Internal Networks”，The 38th Annual International Computers，Software and Applications Conference (COMPSAC2014)，pp.305-310，10.1109/COMPSAC.2014.41 (2014 年 7 月)：

[4]Hirokazu Hasegawa，Yukiko Yamaguchi，Hajime Shimada，Hiroki Takakura，“A Countermeasure Recommendation System against Targeted Attacks with Preserving Continuity of Internal Networks”，The 38th Annual International Computers，Software and Applications Conference (COMPSAC2014)，pp.400-405，10.1109/COMPSAC.2014.63 (2014 年 7 月)：

[5]Shohei Araki，Yukiko Yamaguchi，Hajime Shimada and Hiroki Takakura，“Unknown Attack Detection by Multistage One-Class SVM Focusing on Communication Interval”，The 2014 Cybersecurity Data Mining Competition and Workshop，Neural Information Processing Lecture Notes in Computer Science，Vol.8836，pp.325-332 (2014 年 10 月)：

[6]Hyoyoung Lim，Yukiko Yamaguchi，Hajime Shimada，Hiroki Takakura，“Malware Classification Method Based on Sequence of Traffic Flow”，1st International Conference on Informaiton Systems Security and Privacy (2015 年 2 月)：

[7]Shohei Hiruta，Yukiko Yamaguchi，Hajime Shimada，and Hiroki Takakura，“Evaluation on Malware Classification by Combining Traffic Analysis and Fuzzy Hashing of Malware Binary”，In Proceedings of the 2015 International Conference on Security and Management (SAM’15)，pp. 89-95，(2015 年 7 月)：

[8]Satoshi Fuchigami，Hajime Shimada，Yukiko Yamaguchi，and Hiroki Takakura，“FPGA Base TCP Session Features Extraction Utilizing Off-Chip Memories”， In Proceedings of the 7th International

Conference on Evolving Internet (INTERNET 2015), pp. 38-42, (2015年10月):
[9]Hirokazu Hasegawa, Yukiko Yamaguchi, Hajime Shimada, Hiroki Takakura, “An Incident Response Support System Based on Seriousness of Infection”, The 30th International Conference on In Proceedings of the 30th International Conference on Information Networking (ICOIN2016), pp. 69-74, (2016年1月):
[10]Takeaki Terada, Yoshinori Katayama, Satoru Torii, Hiroshi Tsuda, ″Preliminary Investigation on Psychological Traits of Users Prone to be damaged by Cyber-attack″, Poster, The 11th Symposium on Usable Privacy and Security (SOUPS) 2015 (2015年7月)
[11]Masahiro Yamada, Masanobu Morinaga, Yuki Unno, Satoru Torii, Masahiko Takenaka, “RAT-based Malicious Activities Detection on Enterprise Internal Networks”, ICITST-2015(The 10th International Conference for Internet Technology and Secured Transactions) (2015年12月)

８　その他の誌上発表リスト

[1]寺田 剛陽, 鳥居 悟, 津田 宏, ″人の行動特性からのセキュリティ対策″, ヒューマンインタフェース学会誌 Vol.17, No.3, pp.21-27 (2015年8月)
[2]森永 正信、野村 祐士、古川 和快、天満 尚二、”組織内通信・ログ分析によるサイバー攻撃対策技術”、雑誌FUJITSU、Vol.67、No.1、pp.63-68 (2016年1月)
[3]寺田 剛陽, 片山 佳則, 鳥居 悟, 津田 宏, ″人の行動特性の基づくセキュリティ対策″, 雑誌FUJITSU, Vol.67, No.1, pp.76-82 (2016年1月)

９　口頭発表リスト

[1]山田正弘、森永正信、海野由紀、鳥居悟、武仲正彦、“組織内ネットワークにおける標的型攻撃の諜報活動検知方式”、2014年 暗号と情報セキュリティシンポジウム（鹿児島県鹿児島市）(2014年1月23日)
[2]片山 佳則、寺田 剛陽、津田 宏、“利用者の行動特性を用いたサイバー攻撃における成りすまし対策技術”、第28回人工知能学会全国大会（愛媛県松山市道後）(2014年5月15日)
[3]寺田 剛陽、津田 宏、片山 佳則、鳥居 悟、“IT 被害に遭いやすい心理的・行動特性に関る調査”、マルチメディア、分散、協調とモバイル(DICOMO2014)シンポジウム（新潟県新発田市月岡温泉）(2014 年 7月10日)
[4]片山 佳則、寺田 剛陽、鳥居 悟、津田 宏、“ユーザ行動特性分析による個人と組織の IT リスク見える化の試み”、2015年暗号と情報セキュリティシンポジウム(SCIS2015)(北九州小倉)(2015年1月23日)
[5]小柳佑介、小林賢司、今岡干城、松原正純、坂本喜則、“リアルタイム検知基盤の動的負荷分散機能の開発”、2014年並列／分散／協調処理に関する『新潟』サマー・ワークショップ (SWoPP新潟2014)（新潟県新潟市） (2014年7月30日)
[6]津田宏、“人間系からのセキュリティ対策アプローチ”、富士通SS研（東京）(2014年8月25日)
[7]Takeaki Terada, Yoshinori Katayama, Satoru Torii, Hiroshi Tsuda. “Survey on Psychological and Behavioral Characteristics of Users Prone to be Damaged by Cyber Attack”、Cyberspace2014 (Brno, CZ) (2014年11月28日)
[8]山田正弘、森永正信、海野由紀、鳥居悟、武仲正彦、“組織内ネットワークにおける標的型攻撃の振る

舞い検知に向けた複数センサ連携手法”、2015 年 暗号と情報セキュリティシンポジウム（福岡県北九州市）（2015 年 1 月 21 日）
[9]武仲正彦、”サイバー社会の安心安全を支えるセキュリティ研究最前線”、富士通フォーラム 2015(東京国際フォーラム・有楽町)（2015 年 5 月 14 日）
[10]片山 佳則、寺田 剛陽、鳥居　悟、津田 宏、“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”、第 29 回人工知能学会全国大会（はこだて未来大学（函館））(2015 年 6 月 2 日)
[11]Hiroki Takakura, “New Detection Technologies to Mitigate Damage of Targeted Attacks”, The 6th International Workshop on Data Mining and Cybersercurity, Invited Talk (Daegu) (2013 年 11 月)
[12]佐藤正明, 山口由紀子, 嶋田創, 高倉弘喜, セッションデータのシーケンスに着目した異常な通信パターンの検出, 暗号と情報セキュリティシンポジウム(SCIS2014), No. 2C1-3, pp. 1-8（鹿児島）(2014 年 1 月)
[13]林孝英、山口由紀子、嶋田創、高倉弘喜, トラフィックの出現パターンの類似度に着目したマルウェア分類手法の提案, 電子情報通信学会, 情報システムセキュリティ研究会, 信学技報, vol. 113, no. 502, ICSS2013-83, pp. 149-154（名護）(2014 年 3 月)
[14]塩田実里, 山口由紀子, 嶋田創, 高倉弘喜, 自動ネットワーク構成システムにおける管理ポリシー記述手法の実装, 信学技報, vol. 114, no. 70, IA2014-10, pp. 49-54（神戸）(2014 年 6 月)
[15]柳瀬駿, 嶋田創, 山口由紀子, 高倉弘喜, HW/SW 協調によるアノマリ検知の高速化のための FPGA 部実装, 信学技報, 2014-CSEC-66(11), pp.1-6（函館）(2014 年 7 月)
[16]林孝英、山口由紀子、嶋田創、高倉弘喜, ネットワークトラフィックフローにおけるシーケンスパターンに基づくマルウェア分類手法, 2D1-1, Computer Security Symposium 2014（札幌）(2014 年 10 月)
[17]Shun Yanase, Hajime Shimada, Yukiko Yamaguchi, Hiroki Takakura, Network Access Control by FPGA-Based Network Switch using HW/SW Cooperated IDS, IEICE Tech. Rep., vol. 114, no. 286, IA2014-52, pp. 91-96 (Chiang Mai) (2014 年 11 月)
[18]深尾　篤、“情報セキュリティマネジメントセミナー2014 における展示”、情報セキュリティマネジメントセミナー2014（東京）(2014 年 11 月 6 日)
[19]荒木翔平, 山口由紀子, 嶋田創, 高倉弘喜, ″通信のクラスタ間遷移に基づくサイバー攻撃検知手法″, コンピュータセキュリティシンポジウム 2015(CSS 2015), 3E2-1, pp. 1066-1072（長崎県長崎市）(2016 年 10 月)
[20]長谷川皓一, 山口由紀子, 嶋田創, 高倉弘喜, ″ディレクトリサービス情報とネットワークトラフィックを用いた内部分離ネットワーク構築手法″, コンピュータセキュリティシンポジウム 2015(CSS 2015), 3E3-3, pp. 1221-1228（長崎県長崎市）(2016 年 10 月)
[21]塩田実里, 山口由紀子, 嶋田創, 高倉弘喜, ″インシデント対応時における通信量解析に基づく業務支障検知″, 電子情報通信学会技術報告, Vol. 115, No. 334, ICSS2015-36, pp. 7-12（福島県郡山市）(2015 年 11 月)
[22]淵上智史, 長谷川皓一, 山口由紀子, 嶋田創, 高倉弘喜, “マルウェア感染拡大抑止に向けたネットワーク型動的解析システム”, 電子情報通信学会技術報告, Vol. xx, No. xx, IA2015-xx, pp. xx-xx（佐賀県唐津市）(2016 年 3 月)

１０　出願特許リスト

[1]片山　佳則、津田　宏、メッセージ送信装置、メッセージ受信装置、メッセージ送信プログラム、メッセージ受信プログラムおよびメッセージチェック方法、日本、2014 年 3 月 14 日、特願 2014-052557

[2]寺田 剛陽、片山　佳則、森永正信、武仲　正彦、管理方法、管理装置および管理プログラム、日本、2014 年 3 月 14 日、特願 2014-052693

[3]小柳　佑介、小林　賢司、松原　正純、坂本　喜則、監視プログラム、監視方法および監視装置、日本、2014 年 2 月 28 日、特願 2014-039339

[4]山田正弘、海野由紀、森永正信、ネットワーク監視装置、監視方法及びプログラム、日本、2014 年 1 月 9 日、特願 2014-002693

[5]小林　賢司、小柳　佑介、今岡　干城、松原　正純、坂本　喜則、分散処理プログラム、分散処理管理装置及び分散処理方法、日本、2014 年 7 月 16 日、特願 2014-146170

[6]小柳　佑介、小林　賢司、今岡　干城、松原　正純、坂本　喜則、″MONITORING METHOD AND MONITORING APPARATUS″、米国、14/605437（2015/01/26）

[7]山田正弘、森永正信、ネットワーク監視システム及び方法、日本、2014 年 12 月 26 日、特願 2014-265798

[8]牛田 芽生恵、片山 佳則、寺田 剛陽、津田 宏、アラート発信方法、プログラム、及び装置、日本、2014 年 12 月 24 日、特願 2014-260785

[9]片山　佳則、津田　宏、ユーザ判定装置、方法、及びプログラム、日本、2015 年 1 月 8 日、特願 2015-002377

[10]片山　佳則、津田　宏、端末判定装置、方法、及びプログラム、日本、2015 年 1 月 15 日、特願 2015-006059

[11]山田　正弘,海野　由紀,森永　正信、ネットワーク監視装置、監視方法及びプログラム、米国、2014/12/16、14/571532

[12]片山佳則、他、″MESSAGE SENDING DEVICE, MESSAGE RECEIVING DEVICE, MESSAGE CHECKING METHOD, AND RECORDING MEDIUM″、米国、14/615166（2015/02/05）

[13]小柳佑介、他、″検知プログラム、検知方法及び検知装置″、日本、特願 2015-036897（2015/02/26）

[14]寺田 剛陽、片山 佳則、森永 正信、武仲　正彦、管理方法、管理装置および管理プログラム、米国、14/631359（2015/02/25）

[15]寺田 剛陽、片山 佳則、津田 宏、評価方法、評価プログラム、及び評価装置、日本、特願 2015-063803（2015/03/26）

[16]山田正弘、森永正信、”ネットワーク監視装置、ネットワーク監視方法及びネットワーク監視プログラム”、日本、特願 2015-182298（2015/09/15）

[17]山田正弘、森永正信、”ネットワーク監視システム及び方法”、米国、14/950096（2015/11/24）

[18]寺田 剛陽、津田 宏、鳥居 悟、片山 佳則、リスク算定方法、リスク算定プログラムおよびリスク算定装置、日本、特願 2015-242682（2015/12/11）

[19]片山 佳則、寺田 剛陽、鳥居 悟、津田 宏、安全性判定装置、安全性判定プログラムおよび安全性判定方法、日本、特願 2016-020299（2016/02/04）

[20]片山佳則、他、″端末判定装置、方法、及びプログラム″、独国、1523072.5（2015/12/30）

[21]片山佳則、他、″端末判定装置、方法、及びプログラム″、米国、14/979155（2015/12/22）

[22]片山佳則、他、″ユーザ判定装置、方法、及びプログラム″、米国、14/977002（2015/12/21）

[23]牛田芽生恵、他、″アラート発信方法、プログラム、及び装置″、米国、14/977311（2015/12/21）

[24]小林賢司、他、″RECORDING MEDIUM STORING DISTRIBUTION PROCESSING PROGRAM, DISTRIBUTION PROCESSING

MANAGEMENT APPARATUS AND DISTRIBUTION PROCESSING METHOD″、米国、14/735218 (2015/06/10)
[25]坂本喜則、他、″検知プログラム、検知方法および検知装置″、日本、特願 2016-006453 (2016/01/15)
[26]坂本喜則、他、″検知プログラム、検知方法および検知装置″、日本、特願 2016-006455 (2016/01/15)

１１　取得特許リスト

特に無し

１２　国際標準提案・獲得リスト

特に無し

１３　参加国際標準会議リスト

特に無し

１４　受賞リスト

[1]片山佳則､DICOMO2014 シニアリサーチャー賞､“IT 被害に遭いやすい心理的･行動的特性に関する調査”、2015 年 7 月 11 日
[2]富士通株式会社、Interop Tokyo 2015 「Best of Show Award」、iNetSec Intra Wall 、2015 年 6 月 10 日

１５　報道発表リスト

（１） 報道発表実績
[1]“業界初！サイバー攻撃に遭いやすいユーザーを心理・行動特性で判定する技術を開発　ユーザーや組織に合わせたきめ細かいセキュリティ対策が可能に”、2015 年 1 月 19 日
[2]"やり取り型の標的型メール攻撃をリアルタイムに検知する技術を開発", 2016 年 1 月 21 日

（２）報道掲載実績
[1]″業界初！心理・行動特性でサイバー攻撃に遭うリスクを判定する技術を開発″, 日刊工業新聞, 2015/01/19
[2]″攻撃リスク個人別評価　サイバー被害 PC 操作の癖分析″, 日経産業新聞, 2015/1/20
[3]″セキュリティ対策で新技術　サイバー攻撃あいやすい人心理・行動で判定″, 電波新聞, 2015/1/20
[4]” Fujitsu psychology tool profiles users at risk of cyberattacks”, IDG news, 2015/1/21
[5]″サイバー攻撃を受けやすいか判定する技術″, テレビ東京　ワールドビジネスサテライト, 2015/02/04
[6]″止まらぬネット不正送金被害　金融機関、対策イタチごっこ″, 日経ヴェリタス, 2015/2/15
[7]″業界初！心理･行動特性でセキュリティ被害に遭いやすいユーザーを判定する技術を開発″, ニュースシブ 5 時　NHK 総合テレビ, 2015/04/01
[8]″標的型メール攻撃　富士通などＡＩで即検知″, 日経産業新聞, 2016 年 1 月 22 日
[9]″標的型メール攻撃 先回り警告発信″, 日刊工業新聞, 2016 年 1 月 22 日
[10]″Fujitsu fights targeted email attacks with AI″, ITProPortal, 2016 年 1 月 21 日

研究開発による成果数

	平成 25 年度	平成 26 年度	平成 27 年度
査読付き誌上発表論文数	１件（　０件）	１件（　０件）	１件（　０件）
査読付き口頭発表論文数（印刷物を含む）	２件（　２件）	４件（　４件）	５件（　５件）
その他の誌上発表数	０件（　０件）	０件（　０件）	３件（　０件）
口頭発表数	４件（　１件）	12 件（　２件）	６件（　０件）
特許出願数	４件（　０件）	11 件（　３件）	11 件（　６件）
特許取得数	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）
国際標準獲得数	０件（　０件）	０件（　０件）	０件（　０件）
受賞数	０件（　０件）	１件（　０件）	１件（　０件）
報道発表数	０件（　０件）	１件（　１件）	１件（　１件）
報道掲載数	０件（　０件）	７件（　１件）	３件（　１件）

	合計
査読付き誌上発表論文数	３件（　０件）
査読付き口頭発表論文数（印刷物を含む）	11 件（　11 件）
その他の誌上発表数	３件（　０件）
口頭発表数	22 件（　３件）
特許出願数	26 件（　９件）
特許取得数	０件（　０件）
国際標準提案数	０件（　０件）
国際標準獲得数	０件（　０件）
受賞数	２件（　０件）
報道発表数	２件（　２件）
報道掲載数	10 件（　２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 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こと。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こと。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。