国際連携によるサイバー攻撃の予知技術の研究開発
Research and Development on “Proactive response against cyber-attacks through international collaborative exchange”

代表研究責任者　中尾 康二　ＫＤＤＩ株式会社

研究開発期間　　平成 23 年度～平成 27 年度

【Abstract】

The "PRACTICE" (Proactive Response Against Cyber-attacks Through International Collaborative Exchange) project intended to effectively develop a world-wide threats monitoring & analysis environments among ISPs, Universities and related security companies in international basis in order to aim to develop feasible methods for detecting symptoms of cyber-attacks and for promptly responding against cyber-attacks.

To achieve the above objectives, we have conducted on several research subjects focusing on the following specific research topics：

- similarity, locality and time series analysis for cyber-attack information,
- correlation analysis of cyber-attack information and attacking entity,
- collection of international cyber-attack information and
- cyber-attack information sharing infrastructure.

In this report, several notable achievements of our researches including its continuity plans after the termination of the project are provided. For example, the following achievements can be highlighted：

1) A series of Honey-pots for DR-DoS and IoT has been successfully developed for the purpose of obtaining the online attack vectors to be used for early alert information. Dispatching the alert information to corresponding ISP has already been operated in Telecom-ISAC Japan；
2) A powerful sandbox environment including long-term analysis and taint analysis has been effectively implemented for getting C2 and malicious IP information to be used for the real-time alerting；

Deploying darknet sensors in 10 foregirn countries, the project has successfully conducted a correlation analysis among chaptured data from different countries to be utilized for acknowledging cyber-security information in each country. Furthermore, the project has completed to deploy « Web portal site » for each partner country to provide statistical data for all partners and specific data for each partner country.

1　研究開発体制

○　**代表研究責任者**　　中尾 康二（ＫＤＤＩ株式会社）

○　**研究分担者**　　櫻井 幸一（公益財団法人九州先端科学技術研究所）
山村 元昭（株式会社セキュアブレイン）
松本 勉（国立大学法人横浜国立大学）
田中 俊昭（株式会社ＫＤＤＩ研究所）
石田 祐子（ジャパンデータコム株式会社）

○　**研究開発期間**　平成 23 年度～平成 27 年度

○　**研究開発予算**　総額　1,056 百万円

（内訳）

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 （平成 26 年度補正）
230 百万円	238 百万円	230 百万円	199 百万円	160 百万円

2　研究開発課題の目的および意義

近年、大規模なサイバー攻撃（マルウェアの感染活動や DDoS 攻撃等）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危険性がある。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益々高まっている。

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）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状況の推移を予測する技術の確立を目的とする。

3　研究開発成果（アウトプット）

国内および海外のサイバー攻撃観測センサー及び、国内外から集めたデータを一元的に扱う統合管理部を構築し、「国内外の多様な情報に基づく攻撃予知技術に関する研究開発（課題１）」及び「国際的なサイバー攻撃情報収集・共有技術に関する研究開発（課題２）」を、図１に示す体制で実施した。

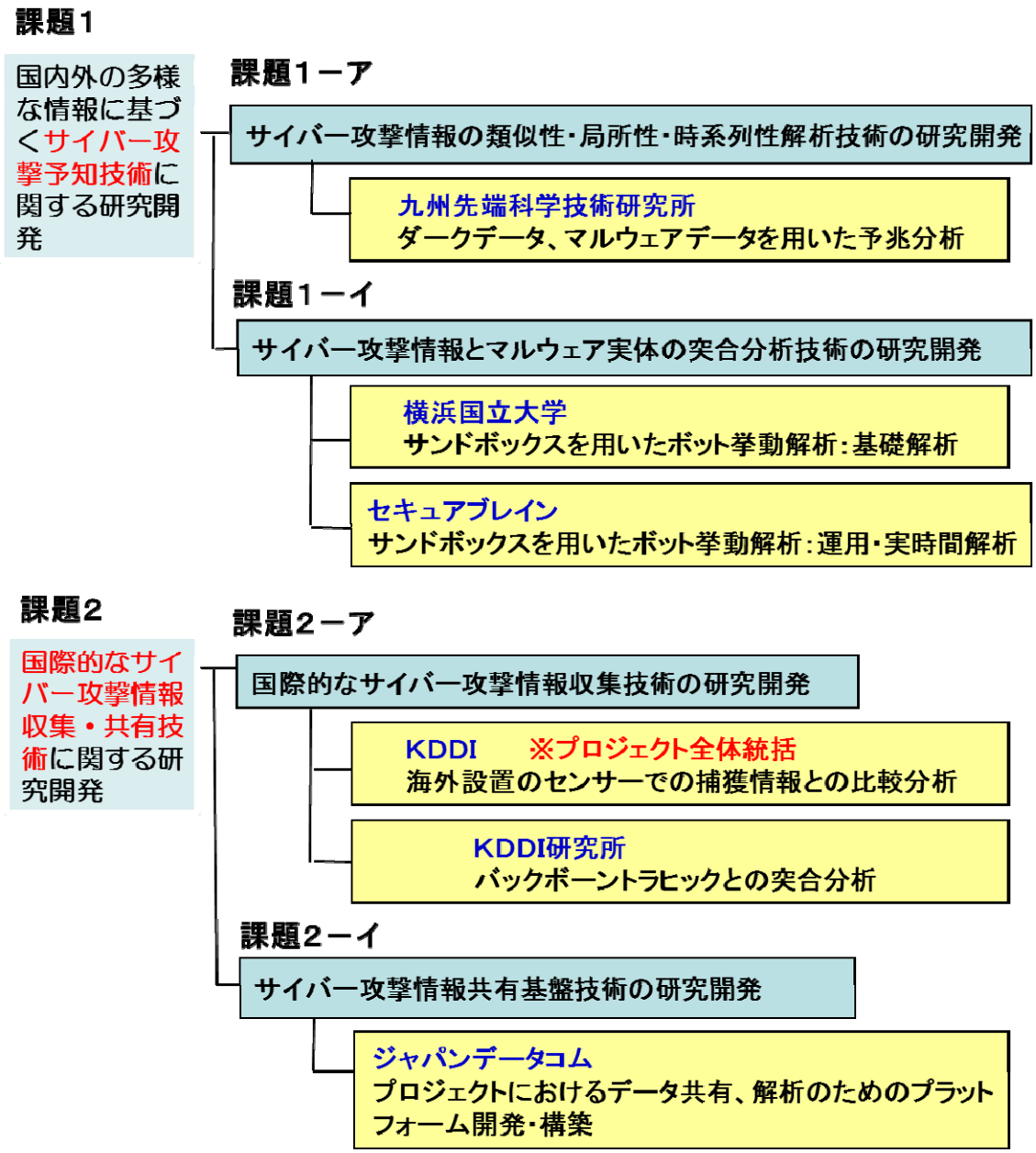

図 1. 研究開発体制

上記体制のもと各課題・研究機関が効果的な連携を行った。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。

本研究開発における主要な成果は、以下の通りである。

①予兆解析/早期攻撃把握からアラート導出

- ハニーポット（横浜国立大学）
  世界初で開発したハニーポット技術を早期攻撃把握に活用する技術をベースに、変遷を続ける脅威に対応した研究を展開し、サイバー攻撃の実態を明らかにすると共に、ISP の運用に資する即時アラート等、実用性の高い予知・即応技術を確立した。
- サンドボックス（セキュアブレイン）

マルウエアの時間軸での挙動変化を観測できるといった利点のある長期観測用マルウェア動的解析と Taint 解析を組み合わせた大規模なサンドボックス環境構築に成功し、C2, 悪性 IP 情報などのアラート発行を実現した。

- ダークネットデータ解析（九州先端科学技術研究所）
  調査系トラヒックが多く存在するダークネットにおいて、不要な雑音トラヒックを除去し、Morto 初期挙動や韓国内の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の開発に成功した。
- 通信事業者データ活用･運用技術（KDDI 研究所）
  公に観測したハニーポットなどの観測データとあわせ、通信事業者のデータをいかに活用し、実被害情報などとの突合を行うことで、アラート情報の精度・有効性の向上ができることを確認。

②海外拠点との国際連携による攻撃把握と技術連携（KDDI）

- 目標となる海外 11 拠点（＋国内１拠点）のセンサー展開を完了し、海外連携国から得られた観測データに基づく解析を実施した。結果、海外拠点における挙動の同期性に基づく、予兆分析/早期攻撃把握の有効性を確認した。
- 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、連携国との間でポータル情報を共有し、アラート情報やマルウェア感染 IP などを実時間で参照できる環境を構築した。

③情報共有基盤の活用開始（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データを共有しながら分析研究を行うためのプラットフォームを構築し、DNS データ等の機微情報の扱いも含め、連携研究のための基盤構築を実現した。
- 特に、これまで困難であった DNS などで扱う機微データを用いる解析のために、B-NONSTOP システムを開発・構築し、PRACTICE の解析における機微データとの相関分析に貢献した。

3.1 項及び 3.2 項で、各課題毎の具体的な成果及び達成事項について述べる。

３．１　国内外の多様な情報に基づくサイバー攻撃予知技術（課題１）

（概要）

国内外において観測・収集された多様な情報に基づき、サイバー攻撃挙動の詳細な分析を行い、攻撃の予知に資する技術の開発を実施する。

３．１．１　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１－ア）

国内外で収集された多種多様な観測データ及び統計データを用いて、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。

上記の目標のもと、ダークネットデータを用いて、主としてボットネットの活動を検知する技術を開発してきた。加えて、大規模なマルウェアデータの分類技術と、解析結果を分かりやすく表示する可視化技術の開発も行った。具体的な成果は以下の通りである。

（ア）スクリーニング技術：ダークネットデータに含まれる雑音の除去を行うスクリーニングエンジンを開発した。i) パケットの系列パタンの教師無し学習により、既知マルウェア由来のパケットを除去す

るエンジンと、ii)半教師付き学習を用いてスクリーニングルールを自動獲得するエンジンを開発した。i) は、文字列パタンを利用する手法と送信元ホスト群の連携構造を利用する手法を開発し、それらを連携して用いている。ii) で用いる半教師付き学習とは、少数の分類済みデータと多数の未分類データを用いて学習を行う手法である。さらに、大学等が調査のために行うスキャンパケットの除去を行う技術も開発した、これらの技術により、検知精度を高めつつ解析対象のデータを減らし、解析エンジンの負荷を大幅に減らすことに成功した。

（イ）グラフィカルモデルに基づく解析エンジン：glasso エンジンとグラフベース変化点検知エンジンを開発した。いずれもインターネット上の端末同士の協調動作をグラフの形で捉えて、ボットネットやマルウェアの拡散の様子を捉えるエンジンである。前者は glasso と呼ばれるスパース学習の手法によりグラフィカルガウシアンモデル(GGM)の時系列を作成し、その変化点においてアラートを生成するエンジンであり、後述の（ウ）のエンジンに組み込まれている。後者はグラフ的特徴量をデータから直接抽出して変化点を検出する仕組みである。前者は、マルウェアに大量感染した韓国内のホスト群の発見に成功した。これらホスト群はおよそ 1000 台から構成され、ダークネットセンサの広い範囲にわたり、23/TCP ポートと 20012/TCP ポート宛てのパケットを継続的に送信している。これについて課題 2-アにおいて検体を入手して分析を行った結果、新種のマルウェアであることが分かっている。この事例の通知を受けて、JPCERT が KRCERT に問い合わせを行っている(平成 28 年 2 月 22 日)。

(ウ)高リスクポート検知エンジン：本エンジンは、先述の「グラフベース変化点検知エンジン」と、多数のホストからの同時性を有する攻撃挙動の検知を行うエンジンである「分散型攻撃検知エンジン」を組み合わせ、攻撃リスクの高まっているポート群を検知する仕組みである。分散型攻撃検知エンジンは、各終点ポートに対して到達するパケットを集計し、単位時間あたりの始点数の分布を事前に学習しておき、それに基づいて新たなデータの異常検知を行う。前者でデータ全体のマクロ的な異常を検知し、後者によってその異常の原因となる現象を特定することができる。本エンジンは試験段階において、平成 23 年に発生したマルウェアである Morto を発生直後に検知することに成功した。また、平成 27 年 11 月後半に急増した 53473/udp 宛ての攻撃パケットを、11 月中旬の時点で実時間において検知した。このポートの脆弱性については平成 26 年 8 月 27 日にトレンドマイクロより報告があったため、平成 26 年のデータに遡って解析したところ、9 月 2 日の時点でこのポートに関するアラートを出力しており、本手法の有効性が確認できた。

（エ）信号源分解による高次元時系列解析：非負値行列因子分解（NMF）を応用した MNF エンジンについて、NICTER ダークネットデータを用いた検証実験により、DR-DoS ハニーポットで検知したアラートと関連したスキャンが検知可能なことを確認した。さらに、行列（2 階テンソル）を 3 階以上のテンソルに拡張したテンソル分解エンジンを開発し、実時間の運用を実現した。このエンジンは、平成 27 年 11 月に、33434/UDP(traceroute)に関するアラートを継続的に出力した。精査したところ、20 カ国に分布するホスト群が同期してパケットを送信する異常な事象であることが分かった。調査は継続中であるが、原因は分かっていない。これは単純なユニークホスト数の統計では捉えきれない事象であり、本手法の有用性を示している。

（オ）データ圧縮に基づくマルウェア分類：正規圧縮距離(NCD)を用いてマルウェアの系統樹を作成す

る手法である。これによりマルウェアの流行予測が可能になると期待される。NCD は、M. Li らがコルモゴロフ記述量の概念に基づいて考案したデータの類似尺度である。Cilibrasi と Vitanyi は NCD を木距離に近似することで系統樹を作成し、クラスタリングを行う手法を提案したが、大規模データに用いるには計算量に課題があった。本研究では、マルウェア検体に関する API ログファイル群を入力とし、10 万検体以上の分類を目標とする。現在、系統樹作成のアルゴリズムを工夫することで、5 万検体以上のデータの分類が可能であり、これにより新規のマルウェア分類が準リアルタイムに実現でき、これまで多くの処理時間をかけていた新規マルウェア解析の高速化が可能となる。

（カ）可視化技術：本課題では Parallel Coordinates 版 Time-tunnel(拡張版)等、いくつかの手法を開発してきた。これは、対話的な操作により時系列数値データを可視化するツールであり、多次元データの表示が可能である。本課題では、これに対して 2 属性対 2 属性の可視化を行えるように拡張を行った。これにより、トラヒックデータの流れをより分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になった。

３．１．２　サイバー攻撃情報と攻撃実体の相関分析技術（課題１－イ）

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動向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。

・類似判定に関する研究開発：

本テーマ総括　研究計画時に想定していたダークネットの分析に基づく突合分析技術だけでは多様化するサイバー攻撃に対応することは困難であるという判断から、下記の通り、サイバー攻撃に悪用されるマルウェアの様々な通信挙動に基づく突合を行うため、P2P ボットネット、反射型サービス妨害攻撃、IoT マルウェアといった新たな脅威を観測・分析する技術を開発した。

①パケットヘッダの特徴に基づく攻撃分類と突合技術

攻撃ホストからの通信をパッシブに観測するダークネット観測においては、観測可能であるのは攻撃試行の最初のパケットのみであり、攻撃の詳細を分析するのは困難であるが、一部のマルウェアや攻撃ツールにおいては、個々のパケット、特にそのプロトコルヘッダに特徴を有する場合がある。これに着目し、パケット単位で攻撃パケットの特徴を調べ、その送信元となり得るマルウェアや攻撃ツールを判別する手法を提案した。提案手法を攻撃通信検知ツール Tkiwa として公開すると共に、Tkiwa を情報通信研究機構が開発・運用するネットワーク攻撃観測システムである NICTER に導入し、NICTER が観測する攻撃通信をリアルタイム分析する組込みを行った。その分析結果は、総務省「官民連携による国民のマルウェア対策支援プロジェクト（ACTIVE プロジェクト）の枠組みによりテレコムアイザック推進会議（T-ISAC J）に提供され、ユーザへのマルウェア感染通知時の情報として利用されている。

②エクスプロイト攻撃の分析に基づく攻撃分類と突合技術

ハニーポットに届くエクスプロイト攻撃とマルウェア動的解析により観測されるエクスプロイト攻撃の突合を行う技術を提案した。具体的には、エクスプロイト攻撃を検出するため観測トラヒックを実行可能コードと解釈して CPU エミュレータ上で実行し、その挙動からシェルコード等の位置を突き止め、

送信内容のペイロードから攻撃の類似性を調べる方法を提案し、これによりハニーポットにより観測されるサイバー攻撃情報とマルウェア実体(マルウェア検体)の動的解析により観測される攻撃との突合を行った。既知の脆弱性を突いた攻撃を正解データとし、シグネチャ等の情報を用いずに上記方法で突合を行った結果、正しく分類が行われていることを確認した。

③ドメイン名前解決に基づく突合とマルウェア感染ホストの検出

15 種類以上のボット検体を動的解析システムで長期に動作させて、観測されるドメインの名前解決の挙動を観測した。その結果、多くのボットに関して周期的な名前解決が行われており、この特徴を用いて ISP 等のキャッシュ DNS サーバの通信と突合を行うことで当該ボットに感染したホストが検出できることを示した。特に Morto ワームから特徴的な名前解決パターンを抽出することで約 3 ヶ月の観測で 45.8 万 IP アドレスの感染疑いホスト群を検知した。

④P2P ボットネットの観測と感染ホストの検出

P2P ボットネットは同種のマルウェアに感染したホストの情報をリストとして内部に保持し、これを感染ホスト間で相互にやり取りし、リアルタイム更新することで攻撃者からの命令を伝達したり、機能更新を行う。自身はネットワークを介したエクスプロイト攻撃による感染拡大活動を行わない場合が多く、上述のダークネットや DNS ベースの観測機構ではその動向が把握できない。そこで、感染ホスト間で互いに通信を行うという特徴に着目し、P2P ボット検体を長期動的解析することで通信先すなわち感染ホストの特定を行った。特に ZeroAccess ボットネットは感染ホスト台数が 100 万台を超え、最大規模のボットネットであると言われていたため、ZeroAccess の観測に重点をおいた結果、ZeroAccess の感染ホストがボットネットの P2P ネットワークの中の重要ノードであるスーパーノードとして動作するためのネットワーク上の条件を突き止め、観測中の動的解析ホストをスーパーノードとして動作させることに成功した。その結果、平成 25 年 5 月下旬からの 2 ヶ月半の観測で 450 万 IP アドレスを超える感染疑いホストを検出することに成功した。

⑤反射型サービス妨害攻撃の観測と突合

近年、インターネット上のオープンサービスを踏み台として悪用した反射型サービス妨害攻撃が大きな脅威となっている。そこで、攻撃に悪用される踏み台を装った囮システムである DR-DOS ハニーポットを世界で初めて提案し、平成 25 年末より攻撃の観測を開始した。当初、ほとんど攻撃通信は観測されなかったものの、平成 26 年後半から攻撃が急増したため、平成 26 年 9 月より T-ISAC J を経由した国内 ISP への DoS 攻撃観測情報の提供を開始した。現在も、攻撃を検知した際の即時アラートを発行している。これに加えて、攻撃元となっている可能性のあるボットネットの解析を多数行い、攻撃元の特定を目指したが、攻撃通信の突合の結果、DR-DOS ハニーポットで観測される攻撃の多くはボットネット起源でないという結論に至った。その後の調査により、これらの通信の多くは Booter と呼ばれるサービス妨害攻撃代行サービスが起源となっている可能性が判明したものの、今後、より詳細な攻撃機構の解明が必要といえる。

⑥IoT マルウェアの観測と突合

平成 26 年の後半から非常に古い遠隔通信プロトコルである Telnet のデフォルト通信ポートへの攻撃が急増していることを検知した。さらにこれらの攻撃元が PC ではなく、組込み機器であることを Telnet

やWebのインタフェースから確認した。これは組込み機器のマルウェア感染を示唆するものであったため、これらの攻撃元を突き止めるため、多様な組込み機器のTelnetサービスを模擬した囮ハニーポットシステムIoTPOTを世界で初めて提案した。その結果、平成27年4月より4ヶ月で約15万IPアドレス、361種類の組込み機器から、90万回のマルウェアダウンロード試行が観測された。ハニーポットにより収集されたマルウェア検体は11種類の異なるCPUアーキテクチャで動作するものを含み、その9割はマルウェアデータベースVirusTotalにおいて未知であり、既知であるものについても、ウイルス対策ソフトの検知結果は著しく低く、従来のPC向けマルウェアとは異なる新規のマルウェア群が収集できたといえる。さらに、収集した検体の動的解析を行うため、多様なCPUアーキテクチャで動作する動的解析環境(サンドボックス)を構築しその挙動を観測した。その結果、多くのIoTのマルウェアはサービス妨害攻撃に加担すると共に、不正クリック、感染拡大活動、認証情報盗取といった様々なサイバー攻撃に悪用されていることを突き止めた。

・データエンリッチメントび大規模分散データベースに関する研究開発

基本計画で定めた計画に加えて、日本の金融機関を狙ったマルウェア(以降「金融系マルウェア」と呼ぶ)の解析も研究対象とした。これは、平成26年、金融系マルウェアが流行し、不正送金の被害が急増している背景を受けたものである。平成26年度上期に、「長期観測用マルウェア動的解析」にて、攻撃の実態の把握、有効なアラート情報の発信が可能である見通しを得た。平成26年度下期に、金融系マルウェア観測のシステム化を完了した。平成27年度、70検体以上の金融系マルウェアの長期観測を実施した。また、H27年度に自動化を完了した「潜在ネットワーク攻撃機能の抽出」(Taint解析)においても金融系マルウェアの解析を実施した。これらにより、Chthonic、Dyre、Rovnixといった主要なマルウェア含む観測マルウェアに対しアラート出力という先進的な成果を得た。
最終目標である突合分析の所用時間30秒以内、突合精度80%以上は昨年度10,848検体で本性能は達成している、今年度検体数が1,6236検体となっても昨年度と同様の性能を確認し30秒以内で検索できることを達成した。

①データエンリッチメントに関する研究開発

長期観測用マルウェア動的解析および、機能推定用動的解析への投入検体を自動で判別するようシステム化を行った。検体のDNSアクセスをネットワークに対する特徴的な振る舞いとみなし、大規模分散データベースに登録されていないDNSアクセスを行うものは、長期観測用マルウェア動的解析および、機能推定用動的解析対象とし、自動で投入を行うことによって、解析検体規模を拡大した。

①-1 長期観測用マルウェア動的解析

平成26年度に50検体、平成27年度に133検体の長期観測を実施した。検体に指示を行うC&Cサーリスト、検体が名前解決に利用するDNSサーバリスト、検体がSPAM送信に用いるSMTPサーバ等を取得することができ、攻撃情報として把握、アラートの発行を行った。また、検体が通信を行う頻度に着目し、検体の活動周期を明らかに、予兆把握の仕組み構築に貢献した。

①　-2 機能推定用動的解析(潜在ネットワーク攻撃機能の抽出)

潜在ネットワーク攻撃機能の抽出(Taint解析)の研究開発の過程で、本技術を用いた手動での解析を平成26年度から平成H27年度の間に、20検体の解析を行い、検体が通信を行うC&Cサーバリスト、C&C

から配信される攻撃対象リスト、攻撃コードを取得することができた。平成 27 年度に潜在ネットワーク攻撃機能の抽出(Taint 解析)の自動化を完了し、約 200 検体(うち金融系検体：10%)の解析を実施し、自動化の有効性を示した。なお、潜在ネットワーク攻撃機能の抽出においては過剰の処理負荷がかかることが判明したため、上記の研究アプローチを取ることとした。

②大規模分散データベース

観測データを蓄積するとともに、運用者や分析者等のデータベース利用者が使用できる Web インタフェースの開発を行った。最終年度、長期観測用マルウェア動的解析および潜在的ネットワーク攻撃機能の抽出(Taint 解析)で得られる情報をアラートとして自動発行機能を実装した。データベースへの検体情報蓄積量：1,6236 検体、蓄積した 1,6236 検体を次の項目で検索、全て 1 秒未満で検索結果を抽出
検索項目：ファイル HASH 値/アクセス HOST 名/アクセス PORT 番号/Mutex 名/API 名/アクセスファイル名/アクセスレジストリ名

３．２　国際的なサイバー攻撃情報収集・共有技術（課題２）

（概要）

サイバー攻撃を検知するセンサーについて、その分散運用・管理技術を含めた国際的なサイバー攻撃情報収集技術を確立するとともに、安全な利活用を可能とするサイバー攻撃情報共有基盤技術の研究開発を実施する。

３．２．１　国際的なサイバー攻撃情報収集技術（課題２－ア）

国際的に分散配置されたセンサーの運用・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 秒以内に、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。

・センサ分散運用・管理自動化技術、情報保護及び動的設定変更技術及び統計データ可視化技術に関する研究開発

①センサ分散運用・管理自動化技術

国際的に分散配置されたセンサーの運用・管理を人手に頼ることなく遠隔化・自動化し、センサーで収集したデータの解析に支障を生じることなく安定稼動可能な技術の研究開発を行った。

最終年度となる平成 27 年度までに、日本を含む 7 カ国 8 拠点のセンサを構築した。また、課題２－イの実施者と連携して、収集したサイバー攻撃情報を委託研究 6 者で共有する環境、及び、連携先に対して収集したデータを提供可能な環境を構築し、以下についての機能の確認・評価試験を行った。

Ⅰ．稼働状況の監視強化

センサの稼動状態をプロセスレベルに加え、ハードウェアレベルで的確に把握する手段の確保

Ⅱ．障害対応の迅速化、効率化。

センサが異常状態となった場合の復帰手段を確保するとともに、センサの電源 OFF/ON を遠隔から制御し、現地作業を機器交換作業等に最小限化。

Ⅲ．一元管理化

センサ OS の脆弱性修正、機能追加、ハードウェアの故障に伴うセンサ機器の交換による OS を含むソフトウェアの再インストールに対応。

ネットワークブート機能を使用することで、センサのソフトウェアイメージをネットワークからインストールする環境を構築。

また、海外拠点における観測センサの稼働停止時間、収集したサイバー攻撃情報の転送停止時間の短縮を図るため、センサ機能を構成するソフトウェア（OS、アプリ、プロセス群）の内、重要な構成要素についてハードウェア復旧後に自動で起動する設定・機能を導入した。

最終年度において、障害復旧の平均時間が 2 時間 57 分、稼働率の平均が 99.9%超となり、安定した解析環境を提供することができた。

②情報保護および動的設定変更技術

解析対象とする各国のダークネットデータおよび DNS データの匿名化技術の開発、および匿名化技術を利用して、解析目的に沿った、匿名化するデータの設定を動的に変更できるシステムの開発を行う。

成果の第一はダークネットを対象とし、各拠点が要求する匿名化を満足するために匿名化フィルタを設計し、システム開発を行った。これは予め用意した匿名化手法を各拠点側が選択し、匿名化を実現するシステムとなっている。第二に各国に設置されたセンサに関して DNS を想定し、DNS に対する匿名化システムを開発し、その匿名化フィルタの実装を行った。国内外拠点に分散配置されるセンサの中で、特に DNS サーバについて IP アドレス、ポート番号、URL などプライバシーに関わる情報の匿名化を行う。さらにこの匿名化において、各ノード、特に国内外拠点が要求する匿名化を原則、自由に選択出来るものとしている。同時に、各パラメータについての匿名化要求を Web での詳細なヒアリング、もしくはコマンドラインでの入力により分析し、必要かつ十分な匿名化手法を自動選択するシステムとなっている。さらに解析側から、解析に必要かつ十分な匿名化を要求し調整する機能も有する。また解析目的別に DNS の各抽出データにおいて必要十分なデータに対して匿名化を与える手法を提案した。第三に匿名化プログラムにおける出力のデータ構造から、推定できる（生）データの情報量を評価するために、時系列分析の一種である自己相関と相互相関を利用した複数のダークネットに対するパケット解析手法を提案し、実際に各国のダークネットトラフィックデータを用いて提案手法の検証を行った。次に公開される統計データと自国のダークネット観測データを利用したダークネット IP アドレスの推定手法を提案した。提案する推定手法により、公開する統計データの形態によっては他国のダークネット IP アドレスを推定することが可能であることを示し、さらにその対策法を与えた。

②統計データ可視化技術

各国に設置したセンサー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、以降の検索・分析を迅速、効率的に実施する為の Web ポータルを構築した。本 Web ポータルは PRACTICE がセンサーを設置した各連携組織に対して公開しており、各国センサー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（マルウェアサンドボックス、DR-DoS ハニーポット等）から得られる早期警戒アラート情報などを参照する事が可能である。連携組織へ提供される情報については月次レポートを除き、各情報源からポータルが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

が可能となっている。

Web ポータルにおいて取り扱う情報、連携先へ提供される情報については、以下の図に示す通りである。

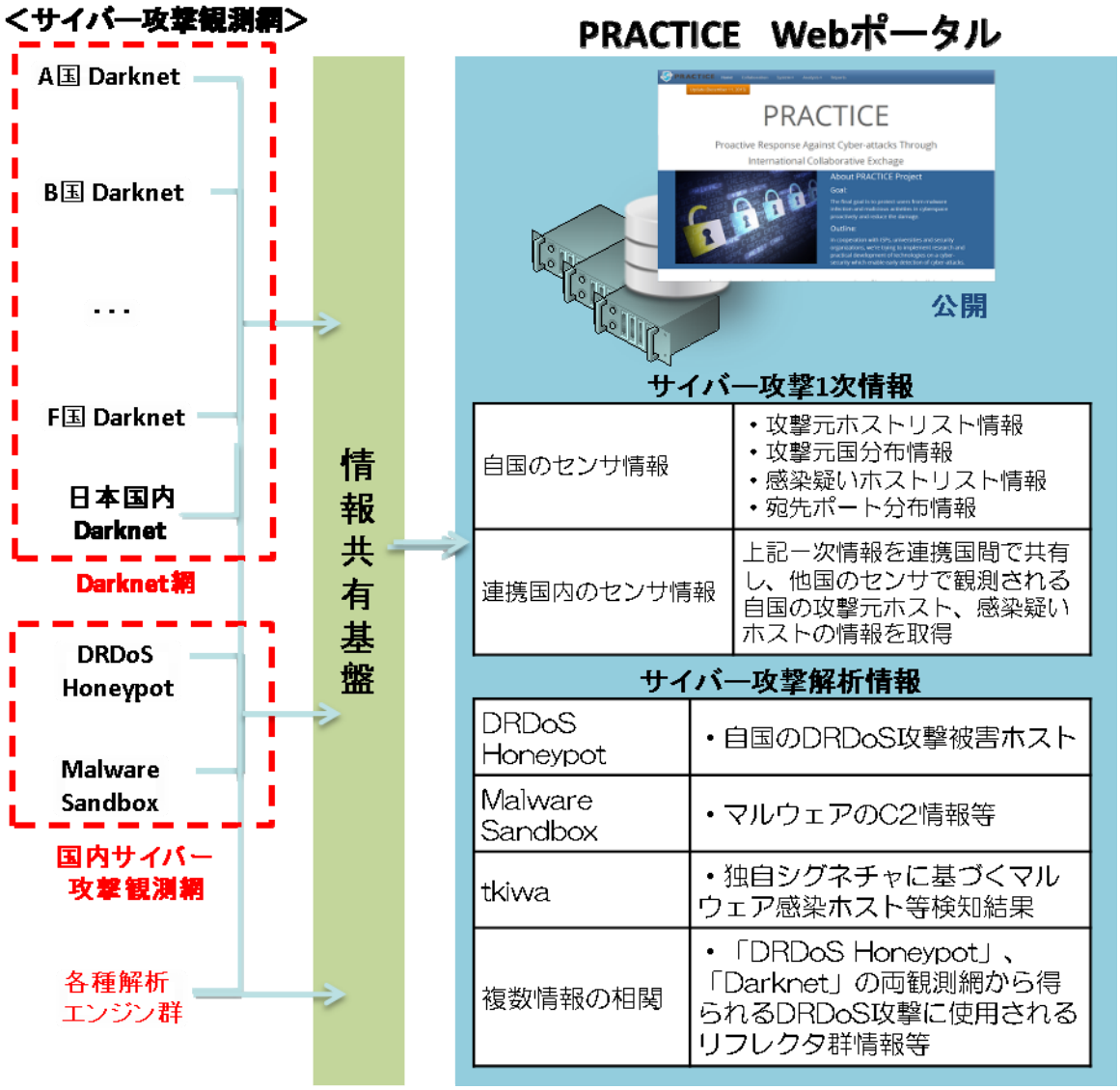

図 2. Web ポータル通じて連携組織へ提供される情報

「サイバー攻撃 1 次情報」として、自国に設置したセンサーから得られる自国宛の攻撃情報、及び、他の連携国に設置したセンサーから得られる自国の攻撃元ホスト情報や自国の感染疑いホスト情報がリアルタイムで処理されポータル上で情報提供されており、連携組織において「自国宛の攻撃傾向の把握」や「攻撃元ホスト情報の分析」の為これらのデータが有効活用されている事を確認した。

「サイバー攻撃解析情報」として、ダークネット以外のサイバー攻撃観測網や各種解析エンジンから得られる C2、DoS 攻撃元(リフレクタ)、DoS 攻撃被害ホスト、及び、サイバー攻撃 1 次情報の解析結果等の情報が含まれており、連携組織はこれらの情報を参照する事により自国内の DR-DoS 攻撃被害ホスト・攻撃種類等をリアルタイムで把握できると共に、「DR-DoS 攻撃」の攻撃元となっている「リフレクタ」や「C2」の自国内件数についても把握する事が可能となっている。国内において被害が拡大するリ

フレクション型の DoS 攻撃は連携国の多くにおいても観測されており、実際に連携先数カ国の官公庁・重要インフラ Web サイトに対する大規模攻撃（2015/9-10）等の早期警戒アラート情報が本 Web ポータルを通じてリアルタイムで連携組織へ共有された。

DR-DoS ハニーポットによる早期警戒アラート情報については、平成 25 年 10 月から本研究開発の姉妹プロジェクトである「国際連携によるサイバー攻撃予知・即応に関する実証実験」を通じて同プロジェクトの実施機関であるテレコムアイザック推進会議（T-ISAC J）の参加メンバーに対してメール形式で配信されている。本アラートについては攻撃の早期検知・情報提供だけに留まらず、ISP 運用の改善に役立てる事を実証しており、DoS 攻撃対策オペレーションの時間短縮等の効果について既に確認している。海外連携組織においても本アラートメール配信に対する要望があるため、実施体制を含めた今後の国際展開可能性について関係機関と検討を進めている。

さらに、連携各国に設置したダークネットセンサによって収集されたトラフィックの解析を行い、各センサに共通する特徴からインターネット全体に行われると想定される攻撃を検知し可視化するシステムを構築した。本システムでは、センサで観測されるトラフィックをプロトコル・ポート別に監視し、観測ホスト数の増加度合い（一定期間過去の時点での観測ホスト数と現在時点での観測ホスト数の比率により評価する値）が一定数以上のセンサ間で共通して閾値を超過する場合に検知を行う。実際に本システムを各連携国に設置したセンサにより収集されたトラフィックに適用した結果、各種注意喚起や脆弱性情報に対応した特定ポートへの攻撃を検知することが確認された。検知された事例としては例えば、特定の企業が製造した NAS の WEB 管理画面（5000/tcp）に存在する脆弱性を探索する挙動や、多くの Unix 系システムが影響を受けた Shellshock 脆弱性を含む WEB ベースのシステム管理ツール（10000/tcp）に対するスキャンなどが挙げられる。さらに 5000/tcp の事例では、各国で観測されるスキャンホスト数の増減に時間差があることから、スキャンホストの増加が遅く観測されるセンサでは事前に通知できる可能性がある。このような事例では本システムの検知結果の早期警戒への利用が期待される。

また、平成 27 年度では本検知手法のホスト数増加度合いの評価指標として ISIT の成果を適用した。具体的には分散型攻撃検知エンジンの手法を各国設置センサにより収集されるトラフィックに適用し、共通するポートで同時期にアラートが出力される場合にグローバルアラートとして検知を行うようにした。この結果、従来の手法では検知されていた調査目的の組織（SHODAN、ShadowServer 等）によるスキャンが関与していると思われるアラートの一部を削減することに成功した。

一部の事例ではダークネットにスキャンを行うマルウェア種別の特定を達成した。アンチウイルスソフトベンダの ESET が公開したレポートから Linux.Moose というマルウェアが 10073/tcp ポートへスキャンを行うという情報を得たために、本プロジェクトで観測しているダークネットアドレスレンジに当該ポートへスキャンを行うホストの調査を行った。本マルウェアは当該ポートへスキャンを行う他、Telnet(23/tcp)や 10073/tcp で待ち受けを行うことがレポートにより明らかにされておりそれらのポートへコネクトバックすることで調査を行った。この結果、スキャンを行うホストの一定数がこれらのポートを開放しており感染の疑いが強いこと、解析レポートに記載されていない機器からのスキャン等を確認した。

・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

① ミクロ解析結果利活用のための有効性検証

25 年度にハニーポットにて観測を開始した分散反射型サービス妨害（DR-DoS：Distributed Reflective

Denial of Service）攻撃を対象とし、ネットワーク運用者視点での攻撃判定精度、早期検知に関してハニーポットの有効性を実証した。検証は、2014/08/01-2014/11/30 に観測した DR-DoS 攻撃を対象に行い、ハニーポットのデータと ISP バックボーンの観測攻撃データの突合分析により実施した。結果、ハニーポット検知事例の約 58%が一定レベルの攻撃規模に発展し、攻撃に発展した事例のうちの約 86%において、ハニーポットの方が ISP バックボーン上に配置されている既存の DoS 攻撃対策システムよりも、平均約 30 秒早期に検知可能であることを確認できた（平成 26 年度実施）。

平成 27 年度は DR-DoS ハニーポットアラートにおける攻撃検知の網羅性と検知速度・精度を個別の ISP に最適化するための検知閾値に関する検証を実施した。検証は、DR-DoS ハニーポット観測データと ISP オペレータの攻撃対処ログを突合分析し、パケット集約時間および同一宛先に対する集約時間中のパケット数からなる閾値を調整し、早急なオペレータ対処が必要なアラート、対処が必要でないアラートの検知数を算出した。今後この結果を基に、運用中の DR-DoS ハニーポットアラートの通知設定を調整する予定。

② 攻撃の規模推定技術

運用者支援を目的とし、ハニーポットの初期観測データからその後予想される攻撃全体の規模を推定する手法の提案・検証を行った。本手法は、ハニーポットで観測された特徴量で攻撃事例をクラスタリングし、ハニーポット観測トラヒック量と ISP バックボーンで観測された攻撃全体のトラヒック量の相関の高いクラスタリングを抽出し、規模を推定する。平成 26 年 2 月 1 日～11 月 30 日に観測した DNS リフレクション攻撃を対象に検証を行い、アラート全体の 64%の攻撃規模を推定可能であり、特定のクラスタに属する攻撃の規模を最大誤差±35%以内で推定可能であることを確認した。この結果から、ハニーポットの監視により、攻撃を早期に検知できることに加え、早期検知時点で推定した攻撃規模情報をアラートに付与することにより、運用者による対処の優先順位付けを支援できると考えられる。

③ 高速フロー分析技術

攻撃観測データ、攻撃予測情報、悪性ホスト情報等のミクロ解析の成果を運用者支援に役立てるために、ISP バックボーンの膨大なフローデータとの高速な突合分析が可能なフローフィルタの開発を行った。本フィルタにより十数万 IP とのマッチング処理で従来方式（nfdump）の 1000 倍以上の高速化を実現した。また、本フィルタを利用し、ミクロ解析で観測した攻撃（DR-DoS ハニーポットで観測した攻撃、マルウェア感染ホスト群からの攻撃）を ISP バックボーンで長期間にわたり収集・保持するシステムの開発を行った。

④ 重要攻撃分類技術

ISP バックボーンでの大量通信検知アラートに DR-DoS ハニーポットアラートおよびネットワークトポロジ情報を付与したアラートからオペレータ対処を必要とする重要アラートを抽出する技術の開発・検証を行った。本手法は、上記アラート情報と ISP オペレータの過去の攻撃対応ログを用いて機械学習により重要アラートを抽出する。平成 27 年 1 月 1 日～3 月 31 日の大量通信検知アラートを対象に検証を行った結果、重要アラートを非重要アラートと判定する確率（False Negative）が最小になるよう閾値設定した場合、False Negative が 0%で、全大量通信アラートから 53%の非重要アラートを削減可能であることを確認した。また、非重要アラートを重要と判定する確率（False Positive）が最小になる閾値設定を行った場合、False Positive 0.1%（平均 1.4 件/20 秒）程度に抑えることが可能であることを確

認した。重要攻撃観測の網羅性と検知精度はトレードオフの関係であるが、利用 ISP やオペレータごとにパラメータ調整することで、より有益なアラートの通知が可能と考えられる。

⑤ ISP バックボーンでの攻撃観測

1. ボット（Morto）感染ホストの観測

ミクロ解析の結果に基づき収集された Morto ボット感染ホストの IP アドレス情報と、ISP バックボーン上での大量通信アラートの突合分析を行った。その結果、各攻撃事例の主な送信元（上位 3 ホスト）に含まれるボットを 1800 ホスト観測でき、ミクロ解析とバックボーンとの突合分析が、DDoS 攻撃の発生源の識別に有効であることを確認した。捕捉できるボットの種類、感染ホスト数が増えれば、ボットネット毎の DoS 攻撃活動状況を把握し、優先的にテイクダウンすべきボットネットの選別等に役立てられると期待できる。

2. 最新の DR-DoS 攻撃の観測・分析

将来的に流行が予想される DDoS 攻撃への対策検討とし、海外で観測されている最新の DR-DoS 攻撃の日本での発生状況を調査した。対象プロトコルは NetBIOS、RPC Portmap、Sentinel、RIPv1 で、前者 3 プロトコルによる攻撃は日本国内では深刻化していないが、RIPv1 に関しては、海外での観測とほぼ同時期に国内でも急増していることを確認し、継続的に観察する必要がある。

上記に加え、近年増加している Booter(Stresser)サイトを使った DR-DoS 攻撃についても調査を行った。Booter は Web 経由で指定宛先に DDoS 攻撃を実施するサービスで、専門知識のない一般ユーザでも容易に攻撃が行えるため、今後当該サービスによる被害は増加すると考えられる。調査の結果、攻撃事例中の開始 10 秒間で当該事例中の全ユニークホストの約 90%を観測できており、1 攻撃中に利用される踏み台群は固定である可能性が極めて高いことが確認できた。そのため、当該攻撃への対策としては、攻撃継続期間中の全パケットの詳細分析は必要なく、一度詳細解析で攻撃判定されたものを一時ブラックリスト等に格納し、一定時間後は IP レベルでの低負荷マッチングを行うことでも大部分の攻撃トラヒックを規制できることが確認できた。

３．２．２　サイバー攻撃情報共有基盤技術（課題２－イ）

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、研究機関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。

初年度は、国内で攻撃情報を共有するため、情報共有基盤の基本設計を実施した。

情報共有基盤の基本設計方針は、①ダークネットデータ収集のためのセンサーが動作する仮想サーバ（VM）を管理する VM サーバと、その VM サーバを制御するファイルサーバを Local Edge Unit（LEU）として国内外拠点に配置し、国内外の LEU で得られたダークネットデータを国内にある統合管理部の共有ストレージに自動で転送して蓄積する、②共有ストレージに蓄積されたダークネットデータは、研究機関及び民間事業者等の各拠点ユーザがリモート接続して取得することにより、サイバー攻撃情報分析に利用することができる、③LEU－統合管理部間、ユーザ拠点－統合管理部間のデータ転送はセキュアな VPN 接続により行われる、とした。

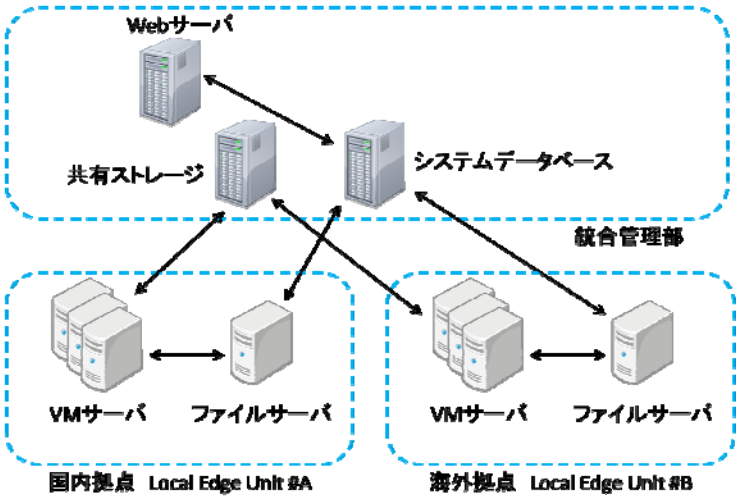

図 3．情報共有基盤

表 1．情報共有基盤における各ノード（サーバ）の役割

VM サーバ	センサー装置を含む情報収集用サーバ(収集拠点である各国や各地域に配置)
ファイルサーバ	システムデータベースからの制御のもと VM サーバを制御するサーバ
Web サーバ	システム維持管理・開発のために利用するユーザが接続する Web サーバ
共有ストレージ	本システムのサイバー攻撃情報を蓄積するデータサーバ
システムデータベース	本システムを維持管理するための情報を格納するデータベースサーバ

2 年目以降は、実用化に向けて、プロトタイプシステムを構築し、試験運用を通じて、利便性、性能面、機能面における個々の検証評価を行い、改良検討した。

2 年目には、必要な仕様・構成要素・リソース等を検討し、プロトタイプシステムを構築して統合管理部／各拠点 LEU のサーバ PC 起動試験、VM 移動・同期試験、サイバー攻撃情報収集試験、障害復旧試験等の機能試験、運用試験を行い、実用化に向けた試験運用を開始した。

3 年目には、研究機関のダークネットデータ解析エンジンのプロトタイプを情報共有基盤に組み込み、共有ストレージのダークネットデータを自動解析してその解析結果を共有ストレージに自動で転送する仕組みを確立したことにより、解析結果を効率的に共有できるようになった。また、機微データシステム（B-NONSTOP システム）を情報共有基盤に導入することにより、プライバシー保護、及び有害情報の無害化等を考慮した上で、各拠点ユーザのデータプロバイダへのリモート接続による機微データ解析の半自動化、高速化を実現した。

4 年目には、情報共有基盤に各研究機関が解析した結果（出力データ等）を共通化・正規化して蓄積する仕組み（解析データ管理システム）を追加した。これらの解析結果やアラートデータに適切なタグを付加、汎用フォーマットである JSON 形式で共通化して蓄積することにより、二次解析やアラート出力でどの拠点の解析データでも同じインターフェイスで検索・抽出できるため、関連性のある各拠点のデータや異なった研究機関の結果を枠組みを超えて利用・解析することが可能となった。さらに、各拠点のデータの突合解析を完全自動化し、高速化・汎用化を達成した。

最終年度には、ダークネット予兆分析、DR-DoS ハニーポット予兆分析、サンドボックス　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、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する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。

また、本研究で構築したシステムは、サイバー攻撃情報の統合解析により、多種多様なサイバー攻撃の予兆解析の高速化を可能にしている。例えば、研究機関 A のダークネット解析結果と研究機関 B の DR-DoS アラートの中から、送信元 IP アドレスと宛先ポートが一致するものを高速で検索・抽出することにより、攻撃者のスキャンと攻撃の相関関係（ルール）の発見、マルウェアの種類の特定をリアルタイムで行うことを可能にした。他にも、研究機関 A のダークネット解析結果で観測された増幅率の高いドメイン（応答サイズが一定サイズを超えるドメイン）を研究機関 B の DR-DoS アラートから検索・抽出することにより、ダークネットで観測されたそのドメインが、攻撃対象に対する DNS アンプ攻撃に使用されるまでの期間を瞬時に突合して、ダークネットの観測から DNS アンプ攻撃に至る相関関係（ルール）をリアルタイムで把握することも可能になった。

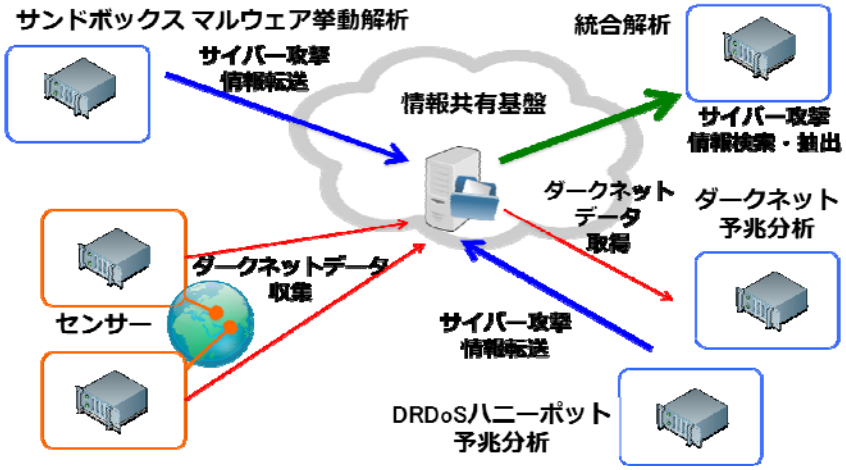

図 4. 情報共有基盤及び各システムの関係

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

本研究開発の政策目標は、「インターネットの利用における安全性、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」ことである。これを達成するため、国内外の多様な情報に基づく攻撃予知技術に関する研究開発（課題１）」及び「国際的なサイバー攻撃情報収集・共有技術に関する研究開発（課題２）」を行い、サイバー攻撃のリスクを軽減することを目的としている。

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 カ国 11 拠点に展開されたダークネット観測センサからデータの収集を行った。これらに加え、DR-DoS ハニーポットで収集したリフレクション攻撃情報やサンドボックスによるマルウェア検体の動的解析情報を、課題２のサイバー攻撃情報収集・共有技術により開発した基盤上で集約・統合解析を行い、サイバー攻撃予兆アラートを生成した。

アラート情報の一部は、本研究開発の姉妹プロジェクトである「国際連携によるサイバー攻撃予知・即応に関する実証実験」を通じて同プロジェクトの実施機関であるテレコムアイザック推進会議（T-ISAC J）の参加メンバーに提供され、ISP などの実運用環境における評価・検証に活用された。特に、DR-DoS ハニーポットにより生成された 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た。

また、マルウェアのサンドボックス解析の結果を、総務省の「官民連携による国民のマルウェア対策支援プロジェクト（通称 ACTIVE)」に提供し、マルウェア感染防止への利活用検討を行っている。

５　政策目標（アウトカム目標）の達成に向けた計画

海外連携機関に構築したダークネットセンサについては全て NICT へ移管し、プロジェクト終了後も NICT によりサイバー攻撃情報の収集及び、国際連携に関わる活動を継続する。（４月以降、順次が移管する予定である。）　課題１－ア（サイバー攻撃情報の類似性・局所性・時系列性解析技術）の成果である各種ダークネット解析エンジンについては、現時点で移管・継続方法は決まっていないが、NICT におけるダークネット分析に適用し活用することを想定している。

課題１－イ（サイバー攻撃情報と攻撃実体の相関分析技術）の成果である、DR-DoS ハニーポットについては引き続き横浜国立大学で運用を継続し、T-ISAC J を経由して各 ISP へのアラート配信を継続する。マルウェアサンドボックス解析については、ACTIVE との連携継続を軸に、今後の活用について調整を行っているところである。

課題２－アのサイバー攻撃情報収集技術については標準化や商品化などは想定していないが、サイバー攻撃情報の収集や統計可視化処理を円滑に行うためのシステムとして活用できるよう、導入のためのパッケージ化を進める予定である。

課題２－イのサイバー攻撃情報共有基盤技術については、上記のサイバー攻撃情報収集技術や、課題１の各種解析エンジンと連動することにより、研究開発分野での利活用が期待できる技術である。標準化や商品化などは想定していないが、NICT におけるデータ共有に利活用できるよう検討を進めている。

６　査読付き誌上発表論文リスト

[1] Ryo Takayanagi, Yoshihiro Okada, ``Visualization System by Combinatorial Use of Edge Bundling and Treemap for Network Traffic Data Analysis," Communications in Computer and Information Science" (CCIS), Springer, 投稿中, Feb. 2016

[2] Takayoshi Sboudai, Hikara Murai, ``A Semi-Supervised Data Screening for Network Traffic Data using Graph Min-CUTs,"情報処理学会論文誌「数理モデル化と応用(TOM)」, 投稿中, Jan. 2016

[3] Kensuke Koshijima, Hideitsu Hino, Noboru Murata, "Change-Point Detection in a Sequence of Bags-of-Data", IEEE Transactions on Knowledge & Data Engineering, vol.27, no. 10, pp. 2632-2644, Oct. 2015

[4] Norikazu Takahashi, Ryota Hibi, ``Global convergence of modified multiplicative updates for nonnegative matrix factorization," Computational Optimization and Applications, Vol.57, Issue 2, pp. 417-440, Aug., 2013

[5] Yaokai Feng, Yoshiaki Hori, Kouichi Sakurai, Junichi Takeuchi, ``A Behavior-Based Method for Detecting Distributed Scan Attacks in Darknets," Journal of Information Processing (JIP), Vol. 21, No.3 pp. 527-538, Information Processing Society of Japan (IPSJ), July, 2013.

[6] 溝口 誠一郎, 笠原 義晃, 堀 良彰, 櫻井 幸一, ``機械的通信挙動モデルに基づく階層型クラスタリングによるボット検知手法", 情報処理学会論文誌 Vol.54, No. 3, pp. 1087-1098, 情報処理学会, 3 月, 2013 年

[7] 千葉 一輝, 堀 良彰, 櫻井 幸一, ``機械的通信挙動モデルに基づく階層型クラスタリングによるボット検知手法", 情報処理学会論文誌 Vol.54, No. 3, pp. 1071-1076, 情報処理学会, 3 月, 2013 年

[8] 笠間貴弘, 織井達憲, 吉岡克成, 松本勉, "公開型マルウェア動的解析システムに対するデコイ挿入攻撃の脅威," Journal of Information Processing, Vol. 52, No. 9, pp. 2761 - 2774, 2011.

[9] T. Kasama, K. Yoshioka, T. Matsumoto, M. Yamagata, M. Eto, D. Inoue, K. Nakao, "Malware Sandbox Analysis with Efficient Observation of Herder's Behavior, " Journal of Information Processing, Vol. 20, No. 4, pp. 835 - 845, 2012.

[10] T. Kasama, K. Yoshioka, D. Inoue, T. Matsumoto, "Catching The Behavioral Differences between Multiple Executions for Malware Detection," IEICE Trans., Vol. E96-A No.1 pp. 225-232, 2013.

[11] 牧田大佑, 吉岡克成, 松本勉, "DNS ハニーポットによる DNS アンプ攻撃の観測," IPSJ Journal No. 55, Vol. 9, pp. 2021 - 2033, 2014.

[12] 牧田大佑, 吉岡克成, 松本勉, 中里純二, 島村隼平, 井上大介,"DNS アンプ攻撃の事前対策へ向けた DNS ハニーポットとダークネットの相関分析," 情報処理学会論文誌, Vol. 56, No. 3, pp. 921-931, 2015. (情報処理学会特選論文)

[13] Yinmin Papa, Katsunari Yoshioka, Tsutomu Matsumoto, "Detecting Malicious Domains and Authoritative Name Servers Based on Their Distinct Mappings to IP Addresses," Journal of Information Processing, Vol. 23, No. 5, pp. 623-632, 2015.

[14] 金井 文宏, 庄田 祐樹, 橋田 啓佑, 吉岡 克成, 松本 勉, "Android アプリケーションの自動リパッケージに対する耐性評価,"" 情報処理学会論文誌, 2015.

[15] 庄田 祐樹, 金井 文宏, 橋田 啓佑, 吉岡 克成, 松本 勉, "メソッドの呼び出し関係のグラフを用いた

Android マルウェア検知手法の改良," 情報処理学会論文誌, 2015.

[16] 田辺 瑠偉, 笠間 貴弘, 吉岡 克成, 松本 勉 "重要情報へのファイルアクセス失敗挙動に基づく情報探索型マルウェア検知手法," 情報処理学会論文誌, 2016.

[17] Yin Minn Pa Pa, Suzuki Shogo, Katsunari Yoshioka, Tsutomu Matsumoto, Takahiro Kasama, Christian Rossow "IoTPOT: A Novel Honeypot for Revealing Current IoT Threats," Journal of Information Processing, Japan, 2016.

[18] T. Kasama, K. Yoshioka, D. Inoue, and T. Matsumoto, "Malware Detection Method by Catching Their Random Behavior in Multiple Executions," 2012 IEEE/IPSJ 12th International Symposium on Applications and the Internet, pp. 262 - 266, 2012.

[19] T. Fujii, K. Yoshioka, J.Shikata, and T. Matsumoto, "An Efficient Dynamic Detection Method for Various x86 Shellcodes," 2012 IEEE/IPSJ 12th International Symposium on Applications and the Internet, pp. 284 - 289, 2012.

[20] Yinminpapa, K. Yoshioka, T. Matsumoto, "Search Engine Based Investigation on Misconfiguration of Zone Transfer," AsiaJCIS2013, 2013 (AsiaJCIS2013 Best Paper Award).

[21] Yin Minn Pa Pa, Shogo Suzuki, Katsunari Yoshioka, and Tsutomu Matsumoto, Takahiro Kasama, Christian Rossow, "IoTPOT: Analysing the Rise of IoT Compromises," 9th USENIX Workshop on Offensive Technologies (USENIX WOOT 2015), 2015.

[22] Lukas Kramer, Johannes Krupp, Daisuke Makita, Tomomi Nishizoe, Takashi Koide, Katsunari Yoshioka, Christian Rossow, "AmpPot: Monitoring and Defending Amplification DDoS Attacks," Proc. Research in Attacks, Intrusions, and Defenses (RAID15), Lecture Notes in Computer Science, Vol. 9404, pp. 615-636, 2015.

[23] Jiawei Su, Katsunari Yoshioka, Junji Shikata, Tsutomu Matsumoto, "Detecting obfuscated suspicious JavaScript based on information-theoretic measures and novelty detection," 18th Annual International Conference on Information Security and Cryptology, 2015.

7 査読付き口頭発表論文（印刷物を含む）リスト

[1] Takumi Kimura, Norikazu Takahashi, ``Global Convergence of Modified HALS Algorithm for Nonnegative Matrix Factorization", The Sixth IEEE International Workshop on Computational Advances in Multi-Sensor Adaptive Processing, Cancun, Mexico, Dec., 2015.

[2] Ryo Takayanagi, Yoshihiro Okada, ``Visualization System by Combinatorial Use of Edge Bundling and Treemap for Network Traffic Data Analysis", The 10th International Workshop on Information Search, Integration, and Personalization (ISIP 2015), North Dakota, America, Oct., 2015.

[3] Yaokai Feng, Yoshiaki Hori, Kouichi Sakurai, ``A Proposal for Detecting Distributed Cyber-Attacks Using Automatic Thresholdin", The 10th Asia Joint Conference on Information Security (AsiaJCIS 2015), Kaohsiung, Taiwan, May., 2015.

[4] Masato Seki, Norikazu Takahashi, ``New Update Rules based on Kullback-Leibler, Gamma, and Renyi Divergences for Nonnegative Matrix Factorization," 2014 International Symposium on Nonlinear Theory and its Applications (NOLTA2014), Luzern, Switzerland, Sep., 2014.

[5] Norikazu Takahashi, Jiro Katayama, Junichi Takeuchi, ``A Generalized Sufficient Condition for Global Convergence of Modified Multiplicative Updates for NMF,'' 2014 International Symposium on Nonlinear Theory and its Applications (NOLTA2014), Luzern, Switzerland, Sep., 2014.

[6] Can Wang, Yao-Kai Feng, Junpei Kawamoto, Yoshiaki Hori, Kouichi Sakurai, ``A Parameterless Learning Algorithm for Behavior-Based Detection,'' 9th Asia Joint Conference on Information Security (AsiaJCIS2014), Wuhan, China, Sep., 2014.

[7] Kazumasa Yamauchi, Junpei Kawamoto, Yoshiaki Hori, Kouichi Sakurai, ``Extracting C&c;C Traffic by Session Classification Using Machine Learning,'' The 7th Workshop among Asian Information Security Labs (WAIS2014), Shanghai, China, Jan., 2014.

[8] Jiro Katayama, Norikazu Takahashi, Junichi Takeuchi, ``Boundness of modified multiplicative updates for nonnegative matrix factorization,'' The fifth IEEE international workshop on computational advances in multi-sensor adaptive processing (CAMSAP2013), Saint Martin, Dec., 2013.

[9] Hisashi Tsuruta, Takayoshi Shoudai, ``Structure-based Data Mining and Screening for Network Traffic Data,'' IIAI-AAI, ESKM2013, Special Session on Machine Learning and Data Mining, Shimane, Japan, Aug., 2013.

[10] Heejae Yim, Norikazu Takahashi, Yukiko Yamauchi, Shuji Kijima, Masashi Yamashita, ``Finding Items Associated with Varied Members in a Pairwise Data Stream,'' The 16th Korea-Japan Joint Workshop on Algorithms and Computation (WAAC2013), Suwon, Korea, Jul., 2013.

[11] Kouhei Kubo, Yukiko Yamauchi, Shuji Kijima, Masashi Yamauchi, ``On Approximation of Normalized Compression Distance by Tree Metric for Clustering,'' The 16th Korea-Japan Joint Workshop on Algorithms and Computation (WAAC2013), Suwon, Korean, Jul., 2013.

[12] Kazumasa Yamauchi, Yoshiaki Hori, Kouichi Sakurai, ``Detecting HTTP-based Botnet based on Characteristic of the C&C session using by SVM,'' The 8th Asia Joing Conference in Information Security (AsiaJCIS2013), Seoul, Korea, Jul., 2013.

[13] Yoshihiro Okada, ``Network Data Visualization Using Parallel Coordinates Version of Time-tunnel with 2Dto2D Visualization for Intrusion Detection,'' The Ninth International Symposium on Frontiers of Information Systems and Network Applications (FINA 2013), Barcelona, Spain, Mar., 2013

[14] Atsushi Okamoto, Takayoshi Shoudai, ``MINING FIRST-COME-FIRST-SERVED FREQUENT TIME SEQUENCE PATTERNS IN STREAMING DATA,'' IADIS International Conference e-Society 2013 (ES2013), Lisbon, Portugal, Mar., 2013.

[15] Sayaka Yamauchi, Masanori Kawakita, Junici Takeuchi, ``Botnet Detection Based on Non-negative Matrix Factorization and the MDL Principle,'' The 5th International Workshop on Data Mining and Cyber Security (ICONIP2012), Doha, Qatar, Nov., 2012.

[16] Satoru Akimoto, Yoshiaki Hori, Kouichi Sakurai, ``Collabrative Behavior Visualization and its Detection by Observing Darknet Traffic,'' The 4th International Workshop on Security (CSS2012), Melbourne, Australia, Dec., 2012.

[17] Kazuki Chiba, Yoshiaki Hori, Kouichi Sakurai, ``Detection of abnormal HTTP communication

based on the edit distance," poster, The 7th International Workshop on Security (IWSEC2012), Fukuoka, Japan, Nov., 2012.

[18] Satoru Akimoto, Yoshiaki Kasahara, Yoshiaki Hori, Kouichi Sakurai, ``Analysis of DNS Traffic to Resolve the Same Domain for Botnet Detection," poster, The 7th International Workshop on Security (IWSEC2012), Fukuoka, Japan, Nov., 2012.

[19] Yaokai Feng, Yoshiaki Hori, Kouichi Sakurai, Junichi Takeuchi, ``A Behavior-based Detection Method for Outbreaks of Low-rate Attacks," The 12th IEEE/IPSJ International Symposium on Applications and the Internet (SAINT2012), Izmir, Turkey, Jul., 2012.

[20] Kazuki Chiba, Yoshiaki Hori, Kouichi Sakurai, ``Reviewing the Way to Quantifying Information Leeks on HTTP Requests and Proposing the Detection System," Fifth Workshop among Asian Information (WAIS2012), Pohang, Korea, Jan., 2012.

[21] Satoru Akimoto, Yoshiaki Kasahara, Yoshiaki Hori, Kouichi Sakurai, ``A Study of Collaborative behavior Detection and Investigating change of Attack using 3D-visualization on Observing the Darknet Traffic," Fifth Workshop among Asian Information Security Labs (WAIS2012), Pohang, Korea, Jan., 2012.

[22] Ryota Hibi, Norikazu Takahashi, ``A Modified Multiplicative Update Algorithm for Euclidian Distance-Based Nonnegative Matrix Factorization and its Global Convergence," 2011 International Conference on Neural Information Processing, Shanghai, China, Nov., 2011.

[23] Yoshiro Fukushima, Yoshiaki Hori and Kouichi Sakurai, ``Proactive Blacklisting for Malisious Web Sites by Reputation Evaluation Based on Domain and IP Address Registration," IEEE TrustCom 2011, Changsha, China, Nov., 2011.

[24] Seiichiro Mizoguchi, Yoshiaki Hori, Kouichi Sakurai, ``Network-based Malware Detection by focusing on distributions of data transmission intervals," Informational Workshop on Security (IWSEC) 2011, Nov., 2011.

[25] 澤谷　雪子、窪田　歩、山田　明、“Understanding the Time-series Behavioral Characteristics of Evolutionally Advanced Email Spammers”、AISec’12 ACM 978-1-4503-1664-4/12/10（2012 年 10 月 19 日）

[26] H. Mori, K. Yoshioka, T. Matsumoto, “Proposal of Visualization Method and User Interface for Analyzing Traffic Observed by Long-term Malware Sandbox Analysis,” IWSEC2012, Poster Session, 2012.

[27] YinminPapa, K. Yoshioka, T. Matsumoto, “Search Engine Based Investigation on Misconfiguration of Zone Transfer,” IWSEC2012, Poster Session, 2012.

[28] K. Yoshioka, "PRACTICE: botnet tracking for detecting emerging threats," Work-In-Progress Session, AsiaJCIS2013, 2013.

[29] R. Tanabe, K. Yoshioka, and T. Matsumoto, "Detecting Intrusion using Dummy Credentials," Work-In-Progress Session, AsiaJCIS2013, 2013.

[30] Takashi Koide, Daisuke Makita, Katsunari Yoshioka, Tsutomu Matsumoto, "Observation and Analysis of TCP-based Reflection DDoS Attacks Using Honeypot," Research in Attacks, Intrusions, and Defenses (RAID15), Poster session, 2015.

８　その他の誌上発表リスト

９　口頭発表リスト

[1] 米巧，山内由紀子，来嶋秀治，山下雅史、``大規模マルウェアデータ群に対する系統樹推定," OR 学会 2016 年春季研究発表会、神奈川県横浜市、3 月、2016 年

[2] 田中翔真，川喜田雅則，竹内純一, ``非負値行列因子分解を用いたボットネット検出手法の実証実験," 電子情報通信学会総合大会、福岡県福岡市、3 月、2016 年

[3] 竹内純一, 櫻井幸一 ``サイバーセキュリティにおけるデータ解析," 電子情報通信学会総合大会、福岡県福岡市、3 月、2016 年

[4] 穴田啓晃, ``国際会議 S&P2015 参加報告", 第 71 回コンピュータセキュリティ研究発表会, 神奈川県, 12 月, 2015 年

[5] 木村匠，高橋規一, ``非負値行列因子分解のための階層的交互最小二乗法の大域収束性解析", 第 38 回情報理論とその応用シンポジウム, 岡山県, 11 月, 2015 年

[6] 関真慧，高橋規一, ``非負値行列因子分解に関連する制約付き最適化問題に対する乗法型更新式の導出とその大域収束性の解析", 電子情報通信学会非線形問題研究会, 広島県, 10 月, 2015 年

[7] 高原尚志，櫻井幸一, ``KDD CUP 99 Data Set を用いた異なる学習データによる機械学習アルゴリズムの評価", コンピュータセキュリティシンポジウム 2015, 長崎県, 10 月, 2015 年

[8] フォン ヤオカイ，　櫻井幸一, ``挙動に基づくポートスキャン検知の自動化に向けた学習アルゴリズムの提案とその性能評価", 第 68 回電気 ・情報関係学会九州支部連合大会, 福岡県, 9 月, 2015 年

[9] 穴田啓晃, 川古谷裕平, 須崎有康, ``国際会議 NDSS2015 参加報告", IEICE 信学技報, 福岡県, 6 月, 2015 年

[10] 木村匠, 高橋規一, ``非負値行列因子分解のための階層的交互最小二乗法の修正とその大域収束性", 電子情報通信学会 2015 年総合大会, 京都府, 3 月, 2015 年

[11] 米巧, 山内由紀子, 来嶋秀治, 山下雅史, ``大規模データ群分類のための木距離近似計算法", OR 学会, 東京都, 3 月, 2015 年

[12] 向井脩, 川村勇気, 川喜田雅則, 竹内純一, ``スパース構造学習を用いた異常検知によるボットネット検出実験 ", 情報セキュリティ研究会（ISEC）, 福岡県, 3 月, 2015 年

[13] 高柳涼, 岡田義広, ``Treemap と Edge Bundling を利用したダークネットデータの可視化システムの提案", 火の国情報シンポジウム 2015, 佐賀県, 3 月, 2015 年

[14] 村井光, 正代隆義, ``効果的なネットワークインシデント検知のための半教師ありデータスクリーニング", 火の国情報シンポジウム 2015, 佐賀県, 3 月, 2015 年

[15] 村井光, 正代隆義, ``グラフベースの半教師あり学習によるデータスクリーニングソフトウェア", Software in Mathmatics Demonstration Track in Hakata Workshop 2015, 福岡県, 2 月, 2015 年

[16] 向井 修, 川村 勇気, 川喜田 雅則, 竹内 純一, ``スパース構造学習をボットネット検出法の性能評価", 2015 年暗号と情報セキュリティシンポジウム (SCIS2015), 福岡県, 1 月, 2015 年

[17] Yaokai Feng, Yoshiaki Hori, Kouichi Sakurai, ``A Behavior-based Engine for Detecting Distributed Internet Attacks and its Performance Investigation", 2015 年暗号と情報セキュリティシンポジウム (SCIS2015), 福岡県, 1 月, 2015 年

[18] 川村 勇気, 川喜田 雅則, 村田 昇, 竹内 純一, ``非負値行列因子分解における MDL 原理について", 第 37 回情報理論とその応用シンポジウム (SITA2014), 富山県, 12 月, 2014 年

[19] 穴田 啓晃, 佐藤 将也, 山内 利宏, 堀 良彰, 盛合 志帆, 櫻井 幸一, ``ASIACCS2014 参加報告", コンピュータセキュリティシンポジウム 2014 (CSS2014), 北海道, 10 月, 2014 年

[20] 川本 順平, 須賀 祐治, ``IEEE Symposium on Security and Privacy 2014 参加報告", コンピュータセキュリティシンポジウム 2014 (CSS2014), 北海道, 10 月, 2014 年

[21] 王 サン, フォン ヤオカイ, 川本 淳平, 堀 良彰, 櫻井 幸一, ``挙動に基づく検知手法に向けてパラメータなしの学習アルゴリズムの提案と検証", 平成 26 年度（第 67 回）電気情報関係学会九州支部連合大会（JCEEE2014）, 鹿児島県, 9 月, 2014 年

[22] 山内 一将, 川本 淳平, 堀 良彰, 櫻井 幸一, ``機械学習を用いたセッション分類による C&C トラフィック抽出", 第 31 回暗号と情報セキュリティシンポジウム (SCIS2014), 鹿児島県, 1 月, 2014

[23] 王 サン, フォン ヤオカイ, 川本 淳平, 堀 良彰, 櫻井 幸一, ``ポートのアクセス数分布によるポートスキャン検知", 第 31 回暗号と情報セキュリティシンポジウム (SCIS2014), 鹿児島県, 1 月, 2014

[24] フォン ヤオカイ, 堀 良彰, 櫻井 幸一, ``Reconsidering the Behavior-based Method for Detecting Distributed Scan Attacks in Darknets", 第 31 回暗号と情報セキュリティシンポジウム (SCIS 2014), 鹿児島県, 1 月, 2014

[25] 川村 勇気, 島村 隼平, 中里 純二, 吉岡 克成, 衛藤 将史, 井上 大介, 竹内 純一, 中尾 康二, ``非負値行列分解を用いたボットネット検出実験", 情報通信システムセキュリティ研究会, 福岡県, 11 月, 2013 年

[26] 松本 晋一, 松浦 幹太, 井家 敦, 岡本 学, ``IEEE Symposium on Security & Privacy 2013 参加報告", コンピュータセキュリティシンポジウム 2013 (CSS2013), 香川県, 10 月 2013

[27] 山内 一将, 堀 良彰, 櫻井 幸一, ``Detecting HTTP-based Botnet based on Characteristic of the Access Behavior to the C&C Server Using by Support Vector Machine", 第 66 回電気関係学会吸収支部連合大会 (JCEEE2013), 熊本県, 9 月, 2013

[28] 片山 慈朗, 高橋 規一, 竹内 純一, ``非負値行列因子分解のための各種乗法型更新式の修正と有界性解析", 第 23 回インテリジェント・システム・シンポジウム (FAN2013), 福岡県, 9 月, 2013

[29] 片山 慈朗, 高橋 規一, ``非負値行列因子分解のための修正乗法型更新式の有界性", 電子情報通信学会 2013 年総合大会, 岐阜県, 3 月, 2013

[30] 岡本 敦, 正代 隆義, ``ストリーム上の頻出時系列とその近似発見アルゴリズムについて", 情報処理学会第 75 回全国大会, 宮城県, 3 月, 2013

[31] Sayaka Yamauchi, Masanori Kawakita, Junichi Takeuchi, ``Botnet Detection using NMF and the MDL criterion," poster, 2013 International Symposium on Information Science and Electrical Engineering (ISEE2013), Fukuoka, Japan, Jan., 2013.

[32] 山内 さやか, 川喜田 雅則, 竹内 純一, ``MDL 規準による非負値行列分解のモデル選択とボットネット検出への応用", 第 35 回情報理論とその応用シンポジウム（SITA2012）, 大分県, 12 月, 2012

[33] Junichi Takeuchi, ``High Dimensional Data Analysis for Botnet Detection," invited talk, The 5th Workshop on Data Mining for Cyber Security (ICONIP2012), Doha, Qatar, Nov., 2012.

[34] 秋本 智, 笠原 義晃, 堀 良彰, 櫻井 幸一, ``同一ドメインの問い合わせに着目したボットネット検出の為の DNS トラヒック解析", 第 65 回電気関係学会九州支部連合大会（JCEEE2012）, 長崎, 9 月,

2012

[35] 千葉 一輝, 堀 良彰, 櫻井 幸一, ``HTTP リクエストの編集距離に基づく Web アクセスの異常検知", 第 65 回電気関係学会九州支部連合大会（JCEEE2012）, 長崎, 9 月, 2012

[36] 溝口 誠一郎, 須崎 有康, 吉岡 克成, 松浦 幹太, ``NDSS2012 会議参加報告", 第 57 回コンピュータセキュリティ研究発表会, 秋田, 5 月, 2012

[37] 衛藤 公希, 小野 廣隆, 山下 雅史, 竹内 純一, ``文字列圧縮を用いたネットワークセキュリティにおけるインシデント検出", 情報科学技術フォーラム（FIT2012）, 東京, 9 月, 2012

[38] フォン ヤオカイ, 堀 良彰, 櫻井 幸一, 竹内 純一, ``挙動に基づく同時多発低レート攻撃の検知案および実験検証", 情報通信システムセキュリティ研究会（ICSS2012）, 3 月, 2012

[39] 千葉 一輝, 堀 良彰, 櫻井 幸一, ``HTTP リクエストにおける情報量の外れ値検出を用いた漏洩検知", 2012 年 電子情報通信学会総合大会, 岡山, 3 月, 2012

[40] 溝口 誠一郎, 堀 良彰, 櫻井 幸一, ``送信間隔のエントロピーに着目した機械的挙動の数値化ならびに実トラフィックを用いた評価", 暗号と情報セキュリティシンポジウム（SCIS2012）, 石川, 1-2 月, 2012

[41] 秋本 智, 堀 良彰, 櫻井 幸一, ``ダークネットトラヒック観測による 3 次元可視化を用いた攻撃変遷調査と協調型攻撃検知", 暗号と情報セキュリティシンポジウム（SCIS2012）, 石川, 1-2 月, 2012

[42] 山内 さやか, 川喜田 雅則, 竹内 純一, ``非負値行列分解と MDL 規準によるボットネットの活動パターン", 暗号と情報セキュリティシンポジウム（SCIS2012）, 石川, 1-2 月, 2012

[43] 日比 亮太, 高橋 規一, ``Nonnegative Matrix Factorization のための修正乗法型更新アルゴリズムとその大域的収束性～ダイバージェンス最小化の場合～", 回路と研究会, 福岡, 1 月, 2012

[44] 溝口 誠一郎, 堀 良彰, 櫻井 幸一, ``DIMVA 2011 会議参加報告", コンピュータセキュリティシンポジウム（CSS）2011, 新潟, 10 月, 2011

[45] 千葉 一輝, 堀 良彰, 櫻井 幸一, ``HTTP リクエストにおける情報漏洩量の数値化手法の検討と検知システムの提案", コンピュータセキュリティシンポジウム（CSS）2011, 新潟, 10 月, 2011

[46] 日比 亮太, 高橋 規一, ``NMF に対する終了条件付き修正乗法型更新アルゴリズム", 平成 23 年度（第 64 回）電気関係学会九州支部連合大会, 佐賀, 9 月, 2011

[47] 溝口 誠一郎, 堀 良彰, 櫻井 幸一, ``エントロピーを用いた機械的特徴のスコアリングとボット検知への応用", 平成 23 年度（第 64 回）電気関係学会九州支部連合大会, 佐賀, 9 月, 2011

[48] 千葉 一輝, 堀 良彰, 櫻井 幸一, ``履歴情報に基づく HTTP リクエストにおける情報漏洩量の数値化手法の検討", 平成 23 年度（第 64 回）電気関係学会九州支部連合大会, 佐賀, 9 月, 2011

[49] 竹久達也、野川裕記、森井昌克、“仮想マシンモニタを改変することでリアルタイムに仮想マシン上の AES 鍵を奪い取る手法”、CSS2011（新潟市）（2011 年 10 月 19 日）

[50] Tatsuya Takehisa、Hiroki Nogawa、Masakatu Morii、“AES Flow Interception: Key Snooping Method on Virtual Machine - Exception Handling Attack for AES-NI -”、JWIS 2011（Kaohsiung, Taiwan）（2011 年 10 月 5 日）

[51] 竹久達也、野川裕記、“AES-NI に対する Exception Handling Attack について”、SCIS2012（金沢市）（2012 年 2 月 2 日）

[52] 畑太一、井沼学、四方順司、竹内新、中尾康二、″サイバー攻撃情報の相関分析のためのタグ付加による効率化に関する一考察″、ICSS2014（名護市）（2015 年 3 月 3 日）

[53] 畑太一、井沼学、四方順司、今村祐、竹内新、″PRACTICEにおける情報共有基盤の構築″、IEICE2016（福岡市）（2016 年 3 月 18 日）

[54] 澤谷　雪子、山田　明、窪田　歩、“トポロジ解析に基づく DoS 攻撃発生時の影響推定に関する一検討”、電子情報通信学会ネットワークシステム研究会（山口大学）（2011 年 12 月 16 日）

[55] 澤谷　雪子、山田　明、窪田　歩、“トラフィックの統計解析による DoS 攻撃事例モデル化の検討”、電子情報通信学会総合大会（岡山大学）（2012 年 3 月 20 日）

[56] 浦川　順平、窪田　歩、牧田　大祐、吉岡　克成、　松本　勉、“DNS アンプ攻撃の早期検知と規模推定に関する一考察”、電子情報通信学会総合大会（富山大学）（2014 年 3 月 18 日）

[57] 浦川　順平、澤谷　雪子、山田　明、窪田　歩、牧田　大祐、吉岡　克成、　松本　勉、“ハニーポット監視による DR-DoS 攻撃の早期規模推定”、SCIS2015（北九州市）（2015 年 1 月 21 日）

[58] 山田　明、浦川　順平、澤谷　雪子、窪田　歩、“ISP のサイバーセキュリティ確保における OODA ループ適用に関する一考察”、SCIS2016（熊本市）（2016 年 1 月 20 日）

[59] 浦川　順平、澤谷　雪子、山田　明、窪田　歩、牧田　大祐、吉岡　克成、　松本　勉、“ISP 運用におけるハニーポットセンサ観測データを用いたサイバー攻撃予測の評価”、電子情報通信学会総合大会（九州大学）（2016 年 3 月 18 日）

[60] 神薗 雅紀、岡田 晃市郎、星澤 裕二、吉岡 克成、“ボットを対象としたマルウェア動的解析手法の提案”、2013 年電子情報通信学会総合大会（岐阜市）（2013 年 3 月 22 日）

[61] 星澤 裕二、神薗 雅紀、“マルウェア動的解析結果の可視化の一手法”、第 66 回コンピュータセキュリティ研究会（CSEC）（函館市市）（2014 年 7 月 3 日）

[62] 西田 雅太、太刀川 剛、岩本 一樹、遠藤 基、奥村 吉生、星澤 裕二、“静的解析と挙動観測による金融系マルウェアの攻撃手法の調査”、マルウェア対策研究人材育成ワークショップ 2014（MWS2014）（札幌市）（2014 年 10 月 24 日）

[63] “マルウェア長期観測・テイント解析の解析手法と観測結果”、2016 年電子情報通信学会総合大会（福岡市）（2016 年 3 月 18 日）

[64] Makoto Nakamura, " New project on International Collaboration for Cyber Security ", Internet Security Days 2011, 2011.

[65] Wataru Senga, " An Approach toward Trend Forecasting Technologies against Cyber-attacks ", 3rd APT Cybersecurity Forum, 2012.

[66] Takemasa Kamatani, " An Approach toward Trend Forecasting Technologies against Cyber-attacks ", Japan-ASEAN Information Security Workshop, 2013.

[67] Takemasa Kamatani, “Introduction of R&D activities Cyber attack trend detected by Darknet sensor, ” Japan-ASEAN Information Security Workshop, 2013.

[68] Takemasa Kamatani, “An approach toward the detection of early stage of cyber attacks, ” 4rd APT Cybersecurity Forum, 2013

[69] Takemasa Kamatani, “ Cyber-attack monitoring and visualization by utilizing darknet, ” Brainstorming Workshop on 5G Standardization: WISDOM(Wireless Innovative System for Dynamic Operating Mega communications) at the occasion of GISFI Five Years Anniversary Celebrations, 2014.

[70] Wataru Senga, "Overview of PRACTICE," Singapore-Japan Symposium on Cyber Security, 2014.

[71] Kosuke Murakami, "International data analysis based on PRACTICE sensors," Singapore-Japan Symposium on Cyber Security, 2014.

[72] 村上, 蒲谷, 千賀, 鈴木, 小出, 島村, 牧田, 笠間, 衛藤, 吉岡, 井上, 中尾, “複数のダークネット観測拠点で同時期に急増する攻撃を検知する手法の提案,” 情報処理学会コンピュータセキュリティシンポジウム 2014, 2014

[73] Takemasa Kamatani, “ Introduction of PRACTICE Project ? Research：Recent activities toward an early detection & response against cyber-attacks, ” 5th ASEAN-Japan Information Security Workshop, 2014

[74] 村井健祥, 古本啓祐, 村上洸介, 中尾康二, 森井昌克, "複数のダークネットに対するトラフィックデータ解析とその応用," 2015-06-ICSS, 2015

[75] 村井健祥, 古本啓祐, 村上洸介, 中尾康二, 森井昌克, "複数のダークネットに対するトラフィックデータ解析とそこからの情報漏えいについて," FIT2015, 2015

[76] 村井健祥, 古本啓祐, 村上洸介, 中尾康二, 森井昌克, "ダークネットトラフィックへの時系列解析と攻撃手法の特徴分析," 暗号と情報セキュリティシンポジウム 2016, 2016

[77] 村井健祥, 古本啓祐, 村上洸介, 中尾康二, 森井昌克, "PRACTICE ダークネットトラヒックへの時系列解析とスキャン特徴量によるスキャンツール等の分類," 2016 年電子情報通信学会総合大会, 2016

[78] 村上洸介, 浦川順平, 山田明, 中尾康二, "NTP リフレクション攻撃における monlist 応答を用いた潜在被害ホスト群の推定," 暗号と情報セキュリティシンポジウム 2016, 2016

[79] Wataru Senga, "Activities of PRACTICE project in Japan," 6th APT Cybersecurity Forum, Bangkok, Thailand, 20-22 October, 2015

[80] 千賀渉，蒲谷武正，村上洸介，中尾康二，“PRACTICE ―国際連携によるサイバー攻撃の予知・即応プロジェクト―”，2016 年電子情報通信学会総合大会, 2016

[81] Takemasa Kamatani, " An Approach toward Proactive Response against Cyber-attacks through international collaboration", Workshop on Cyber Security: The Lifeline of Information and Communication Technology (ICT), 3 June 2015, New Delhi, India,2015

[82] Takemasa Kamatani, "Cyber Security joint Activity with Japan PRACTICE Deliverables with Demo," 22st GISFI Standardization Series Meeting (GSSM#22), 2 September 2015, Navi Mumbai, India, 2015

[83] K. Yoshioka, "Fighting malware with sandbox analysis," Joint Workshop on Information Security, Taiwan, 2011.

[84] 吉岡克成, "PRACTICE - 国際連携によるサイバー攻撃予知・即応技術の研究開発" 信学技報, Vol. 112, No. 499, ICSS2012-66, pp. 55 - 55, 2013.

[85] Katsunari Yoshioka, "PRACTICE project or proactive countermeasure against Cyber-Attacks," Joint workshop between III and NICT, Taiwan, 2013.

[86] Katsunari Yoshioka, "Detailed research results on PRACTICE," Joint Workshop on Cyber Security through JASPER between Indonesia and Japan, Indonesia

[87] Katsunari Yoshioka, "Case study for DR-DOS monitoring," 2nd Joint workshop between III and NICT, Taiwan, 2014.

[88] Katsunari Yoshioka, "Current detail PRACTICE activities," 18th GISFI Standardisation Series

Meeting & Brainstorming Workshop on 5G Standardization: WISDOM atthe occasion of GISFI Five Years Anniversary Celebrations in India", India, 2014.

[89] Katsunari Yoshioka, "Updates from PRACTICE Project: Case study for DR-DOS monitoring," Joint Meeting between TU Delft, PRACTICE and NICT, Netherlands, 2014.

[90] Katsunari Yoshioka, "Technical output from PRACTICE (1)- Case Studies: Monitoring huge P2P botnet and DR-DOS," Singapore-Japan Symposium on Cyber Security, 2014.

[91] Daisuke Makita, Correlation Analysis between DNS Honeypot and Darknet for Proactive Countermeasures of DNS Amplification Attacks, IWSEC2014, invited talk session, 2014.

[92] Katsunari Yoshioka, "Efforts for DDoS Monitoring and Alerting,", The First IAS-YNU Symposium on Information and Physical Security, 2015.

[93] Katsunari Yoshioka, "Detailed research results of the PRACTICE project," The Second Joint workshop between TU Delft, PRACTICE project and NICT: INNOVATING BOTNET MITIGATION, Tokyo, 2015.

[94] Katsunari Yoshioka, "Efforts for DDoS Monitoring and Alerting," Cyber Security French-Japanese Workshop, Tokyo, 2015.

[95] Katsunari Yoshioka, "IoTPOT：Analysing the Rise of IoT Compromises," 3rd Joint workshop between III and NICT, Hokkaido, 2015.

[96] Katsunari Yoshioka, "IoTPOT: Analysing the Rise of IoT Compromises," Workshop on "Impact of ICT on Green Environment" jointly with 22nd GISFI Standardisation Series Meeting (GSSM), India, 2015.

[97] 吉岡克成, "ネットワーク観測からみる IoT の衝撃的現状とその打開策," IoT セキュリティフォーラム, 2015.

[98] Katsunari Yoshioka, "Understanding IoT Security Issues by Active and Passive Monitoring," ジャパンデータコム IOT フォーラム, 2015.

[99] 吉岡克成, "インターネット接続された IoT デバイスのマルウェア感染状況," 電子情報通信学会情報システムセキュリティ研究会, 招待講演, 2015.

[100] 吉岡克成, "ネットワーク観測から見る IoT 機器の大量マルウェア感染の現状," 日経 BP サイバーテロ対策フォーラム, 2015.

[101] 吉岡克成, "サイバー攻撃の実態把握と対策について," 北陸先端科学技術大学院大学 SCHOOL OF INFORMATION SCIENCE SEMINAR 2015, 2015.

[102] 吉岡克成, "ハニーポットによる IoT 機器の感染状況の観測と IoT マルウェアの解析," Security Day 2015, 2015.

[103] 吉岡克成, "IoT 機器の脆弱性が金融機関へ与えるインパクト," 日本銀行金融研究所 情報セキュリティ・セミナー, 2015.

[104] Katsunari Yoshioka, "Detection and Warning of Emerging Cyber Threats-Latest Results from PRACTICE Project-," ASEAN-JAPAN Security Workshop for ISPs, 2015.

[105] 吉岡克成, "IoT 機器のマルウェア大量感染の現状把握とその対策," 情報セキュリティ Summit 2016, 2016.

[106] 吉岡克成, 牧田大佑, 西添友美, 井上大介, 中尾康二, 松本勉, "DR-DoS 攻撃のリアルタイム検知

と即時警報システム," 電子情報通信学会総合大会　特別企画「国際連携によるサイバー攻撃の予知・即応」, 2016.

[107] 吉岡克成, "ハニーポットによるIoTデバイスのマルウェア感染状況の観測と対策に向けて," 電子情報通信学会総合大会 特別企画「サイバーセキュリティを支える情報セキュリティ基盤技術」, 2016.

[108] 村上洸介, 藤井孝好, 吉岡克成, 松本勉, "リモートエクスプロイト攻撃を効率的に観測可能なマルウェア動的解析手法の提案," 情報処理学会コンピュータセキュリティシンポジウム(CSS2011) 論文集 CD-ROM, セッション 3B3-3, 2011.

[109] 笠間貴弘, 吉岡克成, 井上大介, 松本勉, "実行毎の挙動の差異に基づくマルウェア検知手法の提案," 情報処理学会コンピュータセキュリティシンポジウム(CSS2011) 論文集 CD-ROM, セッション 3B3-4, 2011.

[110] 神保千晶, 村上洸介, 藤井孝好, 吉岡克成, 四方順司, 松本　勉, "マルウェアが内包するゼロデイ攻撃機能の検出可能性について," 電子情報通信学会技術報告 ICSS2011-32, pp.1-6, 2011.

[111] 神保千晶, 藤井孝好, 村上洸介, 吉岡克成, 四方順司, 松本勉, 衛藤将史, 井上大介, 中尾康二, "ハニーポット・トラフィック分析によるゼロデイ・リモート・エクスプロイト攻撃検出," 電子情報通信学会暗号と情報セキュリティシンポジウム 2012 CD-ROM 論文集, セッション 2E2-3, 2012.

[112] 藤井孝好, 吉岡克成, 四方順司, 松本勉, "シェルコード動的検知手法の定量的評価" 電子情報通信学会暗号と情報セキュリティシンポジウム 2012 CD-ROM 論文集, セッション 2E2-5, 2012.

[113] 村上洸介, 吉岡克成, 松本勉, "悪性Webサイトを見逃さないリモートセキュリティ検査法," 電子情報通信学会暗号と情報セキュリティシンポジウム 2012 CD-ROM 論文集, セッション 2E3-3, 2012.

[114] 田辺瑠偉, 村上洸介, 吉岡克成, 四方順司, 松本勉, "マルウェア感染ホストへのリモート侵入の可能性," 電子情報通信学会暗号と情報セキュリティシンポジウム 2012 CD-ROM 論文集, セッション 1E1-3, 2012.

[115] 橋本遼太, 吉岡克成, 松本勉, "未検知マルウェアへの対応に基づくアンチウイルスソフトウェアの評価," 情報処理学会研究報告 Vol.2012-CSEC-056, 2012.

[116] 森博志, 吉岡克成, 松本勉, "長期間のマルウェア動的解析を支援する通信可視化手法とユーザインタフェースの提案," 情報処理学会研究報告 Vol. 2012-CSEC-58, No. 38, pp. 1 - 8, 2012.

[117] 塩谷正治, 森博志, 吉岡克成, 松本勉, "マルウェアの自己書換え動作をメモリアクセスに着目して可視化する方法," 情報処理学会コンピュータセキュリティシンポジウム CSS2012, 3B1-3, 2012.

[118] 田辺瑠偉, 鉄穎, 水戸慎, 牧田大佑, 神薗雅紀, 星澤裕二, 吉岡克成, 松本勉,"長期動的解析によるマルウェアの特徴な DNS 通信の抽出," 情報処理学会コンピュータセキュリティシンポジウム CSS2012, 3B1-1, 2012.

[119] 鉄穎, 田辺瑠偉, 水戸慎, 神薗雅紀, 星澤裕二, 吉岡克成, 松本勉, "多数のマルウェア検体を並列解析可能な動的解析システムの提案," 情報処理学会コンピュータセキュリティシンポジウム CSS2012, 3B1-2, 2012.

[120] 塩谷正治, 森博志, 吉岡克成, 松本勉, "マルウェアの多段にわたる自己書換え動作が表現可能な可視化方法," 電子情報通信学会暗号と情報セキュリティシンポジウム 2013, CD-ROM 論文集, セッション 3C4-4, 2013.

[121] 牧田大佑, Yin Minn Pa Pa, 吉岡克成, 松本勉, "名前解決動作の類似性に基づくマルウェア感染ホストの特定," 電子情報通信学会暗号と情報セキュリティシンポジウム 2013, CD-ROM 論文集, セッ

ション 3D4-2, 2013.

[122] 庄田祐樹, 金井文宏, 森博志, 吉岡克成, 松本勉, "Android 用アンチウイルスソフトは簡易な変更が施された既知の不正アプリを検知できるか？," 電子情報通信学会暗号と情報セキュリティシンポジウム 2013, CD-ROM 論文集, セッション 4C1-2, 2013.

[123] 米持一樹, 田辺瑠偉, 吉岡克成, 松本勉, "ダミーの認証情報を用いて不正侵入を事後検知する方法," 電子情報通信学会暗号と情報セキュリティシンポジウム 2013, CD-ROM 論文集, セッション 4C2-5, 2013.

[124] Yin Minn Pa Pa, Daisuke Makita, Katsunari Yoshioka, Tsutomu Matsumoto, "Finding Malicious Authoritative DNS Servers," 信学技報, vol. 112, no. 499, ICSS2012-61, pp. 25-30, 2013. (電子情報通信学会 情報システムセキュリティ研究賞)

[125] ファムアンフォン, 吉岡克成, 松本勉, "入出力プログラムの実行トレース差分によるパッカー特定手法," 信学技報, vol. 112, no. 499, ICSS2012-63, pp. 37-42, 2013.

[126] 金井文宏, 吉岡克成, 松本勉, "動的解析による Android マルウェアの DNS 通信の観測," 信学技報, vol. 112, no. 499, ICSS2012-62, pp. 31-36, 2013.

[127] 森博志, 金井文宏, 庄田祐樹, 吉岡克成, 松本勉, "Android 携帯によるリモートエクスプロイト攻撃の可能性," 信学技報, vol. 112, no. 499, ICSS2012-64, pp. 43-48, 2013.

[128] 高橋佑典, 神薗雅紀, 星澤裕二, 吉岡克成, 松本勉, "UUID に着目したリモートエクスプロイト攻撃のネットワークベースの分類," 信学技報, vol. 112, no. 499, ICSS2012-65, pp. 49-54, 2013.

[129] 牧田大佑, 吉岡克成, 松本勉, "マルウェア感染ホストの特定を目的とした DNS 通信の可視化," 研究報告コンピュータセキュリティ（CSEC）, 2013-CSEC-61, no. 7, pp. 1-6, 2013.(情報処理学会コンピュータセキュリティ研究会推薦論文)

[130] 瀬川達也, 神薗雅紀, 星澤裕二, 吉岡克成, 松本勉, "Man-in-the-Browser 攻撃を行うマルウェアの安全な動的解析手法," 研究報告コンピュータセキュリティ（CSEC）, 2013-CSEC-61, no. 8, pp. 1- 8, 2013.

[131] 牧田大佑, 吉岡克成, 松本勉, " DNS ハニーポットによる不正活動観測," 研究報告セキュリティ心理学とトラスト（SPT）, 2013-SPT-6, no. 54, pp. 1-8, 2013.

[132] 鉄穎, 吉岡克成, 松本勉, "マルウェアのポート待ち受け状態を考慮した並列動的解析環境のネットワーク制御," 情報処理学会コンピュータセキュリティシンポジウム(CSS2013)・マルウェア対策研究人材育成ワークショップ(MWS2013), No. 4, pp. 761 - 768, 2013.

[133] 牧田大佑, 吉岡克成, 松本勉, 中里純二, 島村隼平, 井上大介,"DNS アンプ攻撃の早期対策を目的とした DNS ハニーポットとダークネットの突合分析," 電子情報通信学会暗号と情報セキュリティシンポジウム 2014, 論文集, 2014 (SCIS 論文賞).

[134] 水戸慎, 鉄穎, 田辺瑠偉, 吉岡克成, 松本勉, "ZeroAccess ボットネットにおける新規プラグイン拡散のリアルタイム検知," 電子情報通信学会暗号と情報セキュリティシンポジウム 2014, 論文集, 2014.

[135] 柴原健一, 笠間貴弘, 神薗雅紀, 吉岡克成, 松本勉 "Exploit Kit 検知用シグネチャの動的解析に基づく自動作成," 情報処理学会研究報告. CSEC, 2014-CSEC-64(35), 1-7, 2014.

[136] 筒見 拓也, 野々垣 嘉晃, 田辺 瑠偉, 牧田 大佑, 吉岡 克成, 松本 勉, "複数種類のハニーポットによる DR-DoS 攻撃の観測," IPSJ SIG Notes 2014-CSEC-65(16), 1-6, 2014.

[137] 金井文宏, 庄田祐樹, 吉岡克成, 松本　勉, "Android アプリケーションの自動リパッケージに対する耐性評価," IPSJ SIG technical reports 2014-SPT-10(46), 1-7, 2014.

[138] 陳悦庭, 吉岡克成, 松本勉, "Evaluation of Anti-virus Software on Capability of Behavior-based Malware Detection," 情報処理学会コンピュータセキュリティシンポジウム 2014, 論文集, 2014.

[139] 牧田大佑, 吉岡克成, 松本勉, 島村隼平, 井上大介, 中尾康二, "DNS ハニーポットによる DNS Water Torture の観測," 情報処理学会コンピュータセキュリティシンポジウム 2014, 論文集, 2014.

[140] 鈴木, 小出, 村上, 牧田, 笠間, 島村, 衛藤, 吉岡, 松本, 井上, "複数国ダークネット観測による攻撃の局地性分析," 情報処理学会コンピュータセキュリティシンポジウム 2014, 論文集, 2014.

[141] 小出, 鈴木, 牧田, 村上, 笠間, 島村, 衛藤, 井上, 吉岡, 松本, "TCP/IP ヘッダの特徴に基づく不正通信の検知・分類手法," 情報処理学会コンピュータセキュリティシンポジウム 2014, 論文集, 2014. (CSS2014 学生論文賞)

[142] 森, 吉岡, 松本, "通信可視化システム MACIVISY(MAlware Communication Interactive VIsualization SYstem)によるマルウェア動的解析の支援," 情報処理学会コンピュータセキュリティシンポジウム 2014, 論文集, 2014.

[143] 名執邦彦, 高橋佑典, 吉岡克成, 松本勉, "キャプチャ通信のセキュリティアプライアンスによる事後検査の精度評価," 情報処理学会コンピュータセキュリティシンポジウム 2014, 論文集, 2014.

[144] 田辺, 筒見, 小出, 牧田, 吉岡, 松本, "Linux 上で動作するマルウェアを安全に観測可能なマルウェア動的解析手法の提案," 情報処理学会コンピュータセキュリティシンポジウム 2014, 論文集, 2014.

[145] 橋田啓佑, 金井文宏, 吉岡克成, 松本勉, "Android の実機を利用した動的解析環境の提案," 情報処理学会コンピュータセキュリティシンポジウム 2014, 論文集, 2014.

[146] 牧田大佑, 西添友美, 小出駿, 筒見拓也, 金井文宏, 森博志, 吉岡克成, 松本勉, 井上大介, 中尾康二, "早期対応を目的とした統合型 DR-DoS 攻撃観測システムの構築," SCIS2015, 2015.

[147] 西添友美, 牧田大佑, 吉岡克成, 松本勉, "プロトコル非準拠のハニーポットによる DR-DoS 攻撃の観測," 電子情報通信学会暗号と情報セキュリティシンポジウム SCIS2015, 論文集, 2015.

[148] 庄田祐樹, 金井文宏, 吉岡克成, 松本勉, "悪性コード挿入時の特徴に着目した Android マルウェア検知手法の提案," 電子情報通信学会暗号と情報セキュリティシンポジウム SCIS2015, 論文集, 2015.

[149] 森島周太, 筒見拓也, 田辺瑠偉, 高橋佑典, 小林大朗, 吉川亮太, 吉岡克成, 松本　勉, "動的解析と統合型マルウェア検査サービスの活用によるサイバー攻撃情報収集手法," 信学技報, vol. 114, no. 489, ICSS2014-81, pp. 109-114, 2015.

[150] 筒見拓也, 森島周太, 鈴木将吾, 柴原健一, 吉岡克成, 松本　勉, "サイバー攻撃に集中的に利用されるネットワークアドレスブロックの特定方法," 信学技報, vol. 114, no. 489, ICSS2014-83, pp. 121-126, 2015.

[151] 森　博志, 吉岡克成, 松本　勉, "マルウェア動的解析で観測される様々な DoS 攻撃の可視化," 信学技法 ICSS2014-90, pp.163-168, 2015.

[152] 蘇 佳偉, 吉岡 克成, 四方 順司, 松本 勉, "A new approach for detecting obfuscated malicious JavaScript based on information theory and semi-supervised learning," 情報処理学会コンピュータセキュリティシンポジウム CSS2015, 論文集, 2015. (CSS2015 学生論文賞)

[153] 小出 駿, 牧田 大佑, 吉岡 克成, 松本 勉, "ハニーポットによる TCP リフレクション攻撃の観測と分析," 情報処理学会コンピュータセキュリティシンポジウム CSS2015, 論文集, 2015.

[154] 牧田 大佑, 西添 友美, 吉岡 克成, 松本 勉, 井上 大介, 中尾 康二, "DR-DoS ハニーポットが観測した攻撃の履歴を用いた攻撃対象の傾向分析," 情報処理学会コンピュータセキュリティシンポジウム CSS2015, 論文集, 2015.

[155] 小出 駿, 牧田 大佑, 笠間 貴弘, 鈴木 未央, 井上 大介, 中尾 康二, 吉岡 克成, 松本 勉, "通信プロトコルのヘッダの特徴に基づくパケット検知ツール tkiwa の実装と NICTER への導入," 信学技報, ICSS, 2015.

[156] 菊地 陽介, 吉岡 克成, 松本 勉, "登録アプリの悪性度と影響度に基づく Android マーケットの評価について," 信学技報, ICSS, 2015.

[157] 柴原 健一、筒見 拓也、小出 駿、森 博志、村上 洸介、中尾 康二、吉岡 克成、松本 勉, "DR-DoS 攻撃を観測可能なダークネットを用いたリフレクタの分析," SCIS2016, 2016.

[158] 小山 大良、森 博志、髙橋 佑典、吉岡 克成、松本 勉, "遠隔操作される RAT サーバの動作を観測用ホスト上で再現する手法," SCIS2016, 2016.

[159] 横山日明、石井攻、田辺瑠偉、笠間貴弘、吉岡克成、松本勉, "サンドボックス情報収集ツール SandPrint によるマルウェア動的解析環境の実態調査," SCIS2016, 2016.

[160] 鉄穎, 吉岡克成, 松本勉”ビル管理システムへのサイバー攻撃のハニーポットによる実態調査,” 電子情報通信学会情報システムセキュリティ研究会, 2016.

[161] 鈴木将吾, インミンパパ, 江澤優太, 鉄穎, 中山颯, 吉岡克成, 松本勉, “組込み機器への攻撃を観測するハニーポット IoTPOT の機能拡張,” 電子情報通信学会情報システムセキュリティ研究会, 2016.

[162] 川上奈津子, 吉川亮太, 鉄穎, 田辺瑠偉, 吉岡克成, 松本勉, “囮文書の内容に着目した標的型攻撃の分析,” 電子情報通信学会情報システムセキュリティ研究会, 2016.

[163] Jiawei Su, Katsunari Yoshioka, Junji Shikata, Tsutomu Matsumoto, “A fast detecting method for obfuscated malicious JavaScript based on text pattern analysis,” 電子情報通信学会情報システムセキュリティ研究会, 2016.

１０　出願特許リスト

[1] 澤谷　雪子、窪田　歩、攻撃対策装置、攻撃対策方法及び攻撃対策プログラム、日本、2011 年 12 月 6 日、2013 年 6 月 17 日、特開２０１３－１２１００８（Ｐ２０１３－１２１００８Ａ）

[2] 澤谷　雪子、窪田　歩、攻撃対策装置、攻撃対策方法及び攻撃対策プログラム、日本、2011 年 12 月 6 日、2013 年 6 月 17 日、特開２０１３－１２１００９（Ｐ２０１３－１２１００９Ａ）

[3] 澤谷　雪子、窪田　歩、攻撃ホストの挙動解析装置、方法及びプログラム、日本、2012 年 9 月 21 日、2014 年 4 月 10 日、特開２０１４－６４２１６（Ｐ２０１４－６４２１６Ａ）

[4] 岡田 晃市郎、藤原 信代、髙田、一樹、白石 訓裕、マルウェア解析システム、2016 年 2 月 29 日(予定)

１１　取得特許リスト

１２　国際標準提案・獲得リスト

１３　参加国際標準会議リスト

１４　受賞リスト

[1] 牧田大佑, 吉岡克成, 松本勉, 中里純二, 島村隼平, 井上大介, 情報処理学会特選論文, "DNS アンプ攻撃の事前対策へ向けた DNS ハニーポットとダークネットの相関分析,”　2015.

[2] Yinminpapa, K. Yoshioka, T. Matsumoto, AsiaJCIS2013 Best Paper Award, "Search Engine Based Investigation on Misconfiguration of Zone Transfer," AsiaJCIS2013, 2013.

[3] Yin Minn Pa Pa, Daisuke Makita, Katsunari Yoshioka, Tsutomu Matsumoto, 電子情報通信学会 情報システムセキュリティ研究賞, "Finding Malicious Authoritative DNS Servers," 2013.

[4] 牧田大佑, 吉岡克成, 松本勉, 情報処理学会コンピュータセキュリティ研究会推薦論文, "マルウェア感染ホストの特定を目的とした DNS 通信の可視化," 2013.

[5] 牧田大佑, 吉岡克成, 松本勉, 中里純二, 島村隼平, 井上大介, 電子情報通信学会暗号と情報セキュリティシンポジウム論文賞, "DNS アンプ攻撃の早期対策を目的とした DNS ハニーポットとダークネットの突合分析," 2014.

[6] 小出，鈴木，牧田，村上，笠間，島村，衛藤，井上，吉岡，松本, 情報処理学会コンピュータセキュリティシンポジウム学生論文賞, "TCP/IP ヘッダの特徴に基づく不正通信の検知・分類手法," 2014.

[7] 蘇 佳偉, 吉岡 克成, 四方 順司, 松本 勉, 情報処理学会コンピュータセキュリティシンポジウム学生論文賞, "A new approach for detecting obfuscated malicious JavaScript based on information theory and semi-supervised learning," 2015.

１５　報道発表リスト

（１）報道発表実績

[1] "100%感染防止のソフトなし," NHK ニュース おはよう日本, 2012 年 2 月 29 日, 2012.

[2] "防衛関連団体にサイバー攻撃 文書の外部流出も," NHK ニュース 7, 2016 年 2 月 4 日, 2016.

[3] "サイバー攻撃　狙われる防衛分野," NHK ニュース 9, 2016 年 2 月 4 日, 2016.

（２）報道掲載実績

[1] "IoT デバイスのマルウェア感染の現状を知る," IoTNews.jp, 2015.

１６　ホームページによる情報提供

[1] 特徴的な TCP/IP ヘッダによるパケット検知ツール tkiwa
http://ipsr.ynu.ac.jp/tkiwa/index.html

[2] IoTPOT - Analysing the Rise of IoT Compromises
http://ipsr.ynu.ac.jp/iot/index.html

[3] 通信可視化システム MACIVISY
http://ipsr.ynu.ac.jp/macivisy/index.html

研究開発による成果数

	平成 23 年度	平成 24 年度	平成 25 年度
査読付き誌上発表論文数	１件（　０件）	５件（　２件）	４件（　２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）
その他の誌上発表数	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）
特許出願数	２件（　０件）	１件（　０件）	０件（　０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）	２件（　１件）
報道発表数	１件（　０件）	０件（　０件）	０件（　０件）
報道掲載数	０件（　０件）	０件（　０件）	０件（　０件）

	平成 26 年度	平成 27 年度	合計
査読付き誌上発表論文数	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）	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）
口頭発表数	４３件（　６件）	４９件（　８件）	１６３件（２５件）
特許出願数	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）
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	２件（　０件）	２件（　０件）	７件（　０件）
報道発表数	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）

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。