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”

研究代表者

中尾 康二　ＫＤＤＩ株式会社

Koji Nakao　KDDI CORPORATION

研究分担者

竹内　純一[†]　櫻井 幸一[†]　山下　雅史[†]　村田　昇[†]　堀　良彰[†]　正代　隆義[†]　小野　廣隆[†]　高橋　規一[†]　岡田　義広[†]　来嶋　秀治[†]　笠原　義晃[†]　西出　隆志[†]　川本　淳平[†]　川喜田　雅則[†]　馮　尭楷[†]　高原　尚志[†]　松本　晋一[†]　穴田　啓晃[†]　田中　哲士[†]　岡田　晃市郎[††]　太刀川　剛[††]　中平　朋子[††]　岩本　一樹[††]　白石　訓裕[††]　奥村　吉生[††]　高田　一樹[††]　松本 勉[†††]　吉岡　克成[†††]　武笠　貴史[††††]　千賀　渉[††††]　蒲谷　武正[††††]　村上　洸介[††††]　木田　竜二[††††]　宮本　和生[††††]　石橋　寿幸[††††]　田中　暁[††††]　白石　哲郎[††††]　三浦　雄大[††††]　青木 智嗣[††††]　田中　康夫[††††]　藤本　浩二[††††]　浪岡　智朗[††††]　河野　健男[††††]　藤井　新吾[††††]　窪田　歩[†††††]　松中　隆志[†††††]　浦川　順平[†††††]　井沼　学[††††††]　四方　順司[††††††]　畑　太一[††††††]　今村　祐[††††††]

Junichi Takeuchi[†]　Kouichi Sakurai[†]　Masashi Yamashita[†]　Noboru Murata[†]　Yoshiaki Hori[†]　Takayoshi Shoudai[†]　Hirotaka Ono[†]　Norikazu Takahashi[†]　Yoshihiro Okada[†]　Shuji Kijima[†]　Yoshiaki Kasahara[†]　Takashi Nishide[†]　Junpei Kawamoto[†]　Masanori Kawakita[†]　Yaokai Feng[†]　Hisashi Takahara[†]　Shinichi Matsumoto[†]　Hiroaki Anada[†]　Satoshi Tanaka[†]　Kouichirou Okada[††]　Tsuyoshi Tachikawa[††]　Tomoko Nakadaira[††]　Kazuki Iwamoto[††]　Kunihiro Shiraishi[††]　Yoshio Okumura[††]　Kazuki Takada[††]　Tsutomu Matsumoto[†††]　Katsunari Yoshioka[†††]　Takashi Mukasa[††††]　Wataru Senga[††††]　Takemasa Kamatani[††††]　Kosuke Murakami[††††]　Ryuji Kida[††††]　Kazuo Miyamoto[††††]　Hisayuki Ishibashi[††††]　Akira Tanaka[††††]　Tetsuo Shiraishi[††††]　Yuta Miura[††††]　Tomotsugu Aoki[††††]　Yasuo Tanaka[††††]　Kouji Fujimoto[††††]　Tomoaki Namioka[††††]　Tatsuo Kouno[††††]　Shingo Fujii[††††]　Ayumu Kubota[†††††]　Takashi Matsunaka[†††††]　Junpei Urakawa[†††††]　Manabu Inuma[††††††]　Junji Shikata[††††††]　Taichi Hata[††††††]　Yu Imamura[††††††]

[†]公益財団法人九州先端科学技術研究所　[††]株式会社セキュアブレイン　[†††]国立大学法人横浜国立大学　[††††]ＫＤＤＩ株式会社　[†††††]株式会社ＫＤＤＩ研究所　[††††††]ジャパンデータコム株式会社

[†]Institute of Systems, Information Technologies and Nanotechnologies　[††]SecureBrain Corporation　[†††]Yokohama National University　[††††]KDDI CORPORATION　[†††††]KDDI R&D Laboratories, Inc.　[††††††]Japan Datacom

研究期間　平成 23 年度～平成 27 年度

概要

サイバー攻撃から受ける影響を軽減し、適切なセキュリティ対策を講じるためには、各種のサイバー攻撃に起因する様々な脅威を正確かつ速やかに察知・把握し、それら脅威を関連する組織間で迅速に共有することが必要不可欠である。本研究開発においては、国際連携による活動も含め、国内外にダークネットを始めとする様々なサイバー攻撃観測網を配備し、これらの観測網から得られる攻撃に起因する脅威情報を実時間で収集・分析する仕組みを構築した。本研究開発により、ボットネットを始めとする様々なサイバー攻撃に起因する脅威（予兆的挙動も含む）を早い段階で捕捉することができ、サイバーセキュリティ対策実施のための実践的な早期対応を可能とした。

１．まえがき

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。世界中に存在するサイバー攻撃のためのインフラにより、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。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。

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

２．研究開発内容及び成果

国内外のサイバー攻撃観測センサー及び、収集し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。

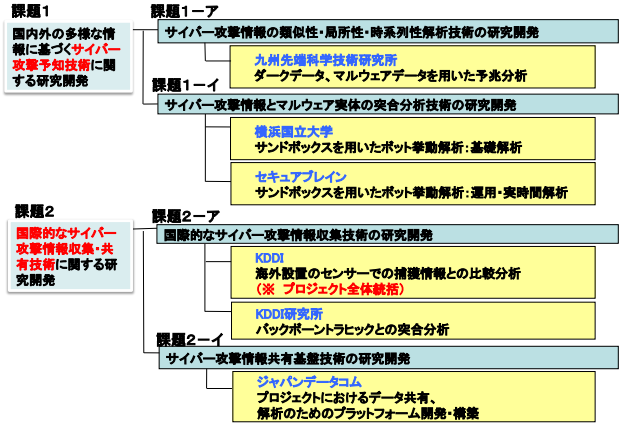

図 1．研究開発体制

図１に示した各課題別の詳細な研究開発内容は以下の通りである。

２．１．各課題別の研究開発内容

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）

【目標】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。

【実施内容】ダークネットより収集される攻撃データ（主にスキャン）を用いて、複数の攻撃における同期性、類似性などに視点を置いたマイニング解析を実施し、ボットネット等の活動を早い段階で検知する技術を開発した。詳細な研究開発内容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ー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。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。前者のエンジンを用いて、他の観測では検知できなかった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ー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。本エンジンによる検知の結果を JPCERT/CC に展開し、韓国の KRCERT への問い合わせを行った（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。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 NICT の NICTER より早く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すで検知しており、遡った形の確認ではあるが、本手法の早期検知における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。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。単純なユニークホスト数の統計では捉えきれないこのような事象を検知するなど、本手法の有用性について確認できた。

（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。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した。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において、本アルゴリズムによるマルウェア分類を用いることで、解析処理の高速化が期待できる。

（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。2 属性対 2 属性の可視化を行えるように拡張を行うことにより、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。

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）

【目標】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。

【実施内容－１】類似判定に関する研究開発：

研究計画時に想定していたダークネットの分析に基

づく相関分析に加え、より多くのサイバー攻撃に起因する脅威を捕捉し、それらの分析を行うために、P2P ボットネット、反射型サービス妨害攻撃、IoT マルウェア等といった新たな脅威を観測するためのハニーポット技術、及び収集結果を効率的／相関的に分析するサンドボックス技術を開発した。詳細な研究開発内容は以下の通りである。

(ア) パケットヘッダの特徴に基づく攻撃分類と突合技術

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 Japan）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現在利用されている。

(イ) 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。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。

(ウ) 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。

(エ) P2P ボットネットの観測と感染ホストの検出

P2P ボットネットが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。

(オ) 反射型サービス妨害攻撃（DR-DoS）の観測と突合

DR-DoS 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、平成 26 年 9 月より T-ISAC Japan 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。

(カ) IoT マルウェアの観測と突合

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 割以上はマルウェアデータベース VirusTotal において未知であり、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。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。

【実施内容－２】データエンリッチメント及び大規模分散データベースに関する研究開発：

他研究分担などにより捕獲したマルウェアを長期的に動作させ、その活動を詳細に把握・分析するためのサンドボックス環境を構築した。また、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)の解析についても研究対象とし、70 検体以上の金融系マルウェアの長期観測を実施した。これらにより、Chthonic、Dyre、Rovnix といった主要な金融系マルウェア含む観測マルウェアに対し、C2 情報や不正送金先情報等を含むアラート出力という先進的な成果を得た。さらに、「潜在ネットワーク攻撃機能の抽出」(Taint 解析)の開発実装を行い、通常のマルウェア解析では達成できなかった攻撃機能の抽出を高速化、高精度化することに成功した。詳細な研究開発内容は以下の通りである。

(ア) 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。

(イ) 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 C２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。

(ウ) 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、これまで容易に抽出できなかった C２サーバリスト、C２から配信される攻撃

対象リスト、攻撃コードなどを取得することができた。

（エ）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うと共に、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。具体的には、データベースへの検体情報蓄積量 : 16,236 検体、蓄積した 16,236 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　などである。

③　国際的なサイバー攻撃情報収集・共有技術（課題２）

【目標】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。

【実施内容－１】センサー分散運用・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：

国内外に分散設置したセンサー群の運用・管理の自動化を行うことにより、効率的なセンサー分散運用・管理を実現した。

また、分散されたセンサーにて収集される情報の共有において、情報の保護技術、及び Web を用いた共有技術について研究開発を実施した。詳細な研究開発内容は以下の通りである。

（ア）センサー分散運用・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。

日本を含む 7 カ国 8 拠点のセンサーを構築し、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。

（イ）情報保護および動的設定変更技術

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。

（ウ）統計データ可視化技術

本研究開発の成果を連携組織へ展開するための Web ポータルを構築した。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、図 2 に示す通りである。

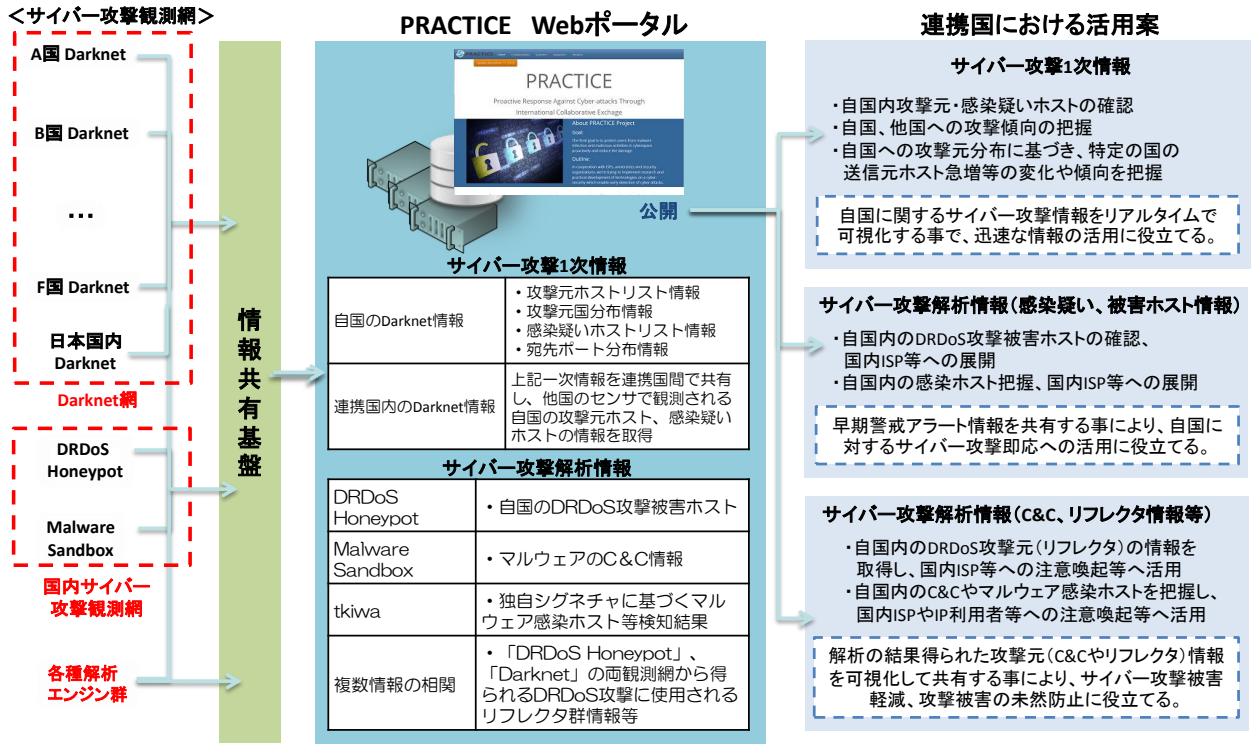

図 2.　Web ポータル通じて連携組織へ提供される情報

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提供されており、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。

さらに、連携各国に設置したダークネットセンサーによって収集されたトラヒックの解析を行い、各センサー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。本システムを各連携国に設置したセンサーにより収集されたトラヒックに適用した結果、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）に対するスキャン等、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した。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、各国に設置したセンサーから得られる解析結果情報を早期警戒情報として利用することが期待される。

また、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（課題１－ア）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ーにより収集されるトラヒックに適用し、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。

【実施内容－２】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：

ハニーポットやダークネットで収集される観測データに基づき、実際のターゲットへの攻撃がネットワーク運用の視点からどのような形で現れ、運用者にとってどのような具体的なアクションが有効となるかを解明するための研究開発を実施した。詳細な研究開発内容は以下の通りである。

（ア）ミクロ解析（ハニーポットや長期観測用マルウェア動的解析等）結果利活用のための有効性検証

分散反射型サービス妨害攻撃を対象とし、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。

また、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、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。

（イ）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 DRDoS に関連する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。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。

（ウ）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。

（エ）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。

（オ）ISP バックボーンでの攻撃観測

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 となっており、RIPv1 に関して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たため、今後も継続的に観察を行っていく。

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。当該攻撃への対策として、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。

④　サイバー攻撃情報共有基盤技術（課題２－イ）

【目標】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。

【実施内容】図３に示す通り、各研究機関から解析結果やアラートデータを情報共有基盤に自動で転送して蓄積し、その多種多様なサイバー攻撃情報を統合解析してサイバー攻撃対象に対するアラートを通知するシステムを構築し、実運用を行った。実運用において、攻撃の発生から状況把握までアラートデータ１件につき、平均 1～2 秒の処理時間を達成した。

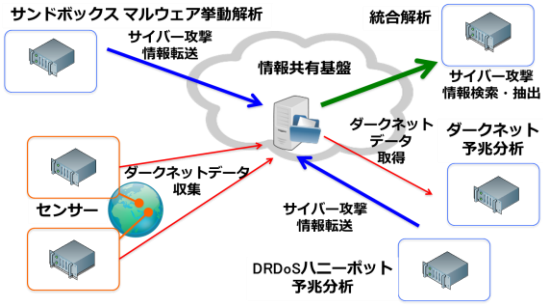

図 3.　情報共有基盤及び各システムの関係

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 C 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 D 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ており、かくて情報共有基盤の構築により、本プロジェクトへの参加組織が各種の統合分析を円滑に実施可能となっており、本研究成果の導出に資する事が出来た。

２．２．研究開発全体成果

図１に示した体制のもと、各課題を有効に達成するために各担当研究機関が効果的な連携を行った。主な成果としては、ハニーポットで捕捉した攻撃をアラートとして具体的な ISP 運用の改善に役立てたほか、新たな観測手法や分析手法による新規研究課題の導出を行うことができた。また、研究開発メンバー間で密な研弓連携を行い、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た。本研究開発により達成した主な成果概要を以下に示す。

ｉ）予兆解析/早期攻撃把握からアラート導出

・ハニーポット技術（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。

・サンドボックス技術（セキュアブレイン）

マルウェ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した。

ii）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拠点を含む）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。

iii）情報共有基盤の構築とその活用（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．今後の研究開発成果の展開及び波及効果創出への取り組み

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、2 章に示した各個別課題への取り組みを通じ、サイバー攻撃に起因する脅威を早い段階で把握･捕捉することによりリスク軽減に繋がる研究開発を推進することができた。今後の成果展開及びその波及効果創出に向けた取り組みについては、以下の通りである。

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、NICT における NICTER システムのダークネット分析エンジンのを補完する解析エンジンとしてすでに動作させており、今後 NICT のサイバーセキュリティ研究基盤の一部として活用される予定である。

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については、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 Japan）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できた。DR-DoS ハニーポットについては NICT と連携して引き続き横浜国立大学で運用を継続し、T-ISAC Japan を経由して各 ISP へのアラート配信を継続しており、本研究開発プロジェクト終了後も継続した技術展開、効果継続を実施できている。また、マルウェアの長期サンドボックス解析については、その解析結果（C2 情報や悪性 URL など）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、具体的なマルウェア感染防止への利活用に貢献することができた。本サンドボックス解析についても、本プロジェクト終了後、セキュアブレインにて運用を継続し、結果の ACTIVE への提供を推進しており、達成した成果の継続活用を行っている。

課題２－アのサイバー攻撃情報収集技術においては、海外 10 カ国 11 拠点に展開したダークネット観測センサーの全てを NICT におけるダークネット観測網に移管することとなり、現在、すべての海外センサーは NICT に移管済みである。従って、プロジェクト終了後においても、本プロジェクトで達成した海外観測環境は、すべて NICT におけるサイバー攻撃情報の収集、及び、国際連携に関わる活動に引き継ぐことができ、継続した成果展開を達成している。

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り、具体的な技術成果展開としては、NICT におけるデータ共有技術である NON-STOP 環境における Live データ解析機能として利活用する方向で検討を進めている。

４．むすび

NISC などの戦略や行動計画において、「予兆情報の共有」「国際連携の重要性」などが明に述べられているように、本研究開発のテーマ設定には非常に重要な内容を含んでおり、その達成は容易ではない。５年間における本研究開発の取り組みにおいては、時系列的に多様化する攻撃に迅速に対応し、これまでのボット型攻撃に加え、たとえば、P2P マルウェア、リフレクション型の DDoS 攻撃や、金融系のマルウェア等、新たな攻撃に対応した研究開発を実施することができた。特に、世界初で開発したハニーポット技術や Taint 解析等を含めた長期サンドボックス解析技術などを用いて早期に攻撃を把握するための技術基盤を確立でき、なかなか達成が難しいとされた実用性の高い予知・即応技術（攻撃予兆把握、分析技術）、およびその基盤技術を確立することができたことは大きな成果であると言える。これらの成果は、2013 年ころから欧州の EU プロジェクトでも認識され、その一環でオランダの大学との研究連携を達成することができた。本プロジェクトの成果は、すでに継続的な活用及び社会展開を進めているところであるが、2020 年の東京オリンピック・パラリンピックを含めた近未来における高度な脅威（攻撃）観測基盤、及び分析基盤の構築において有効的に利活用され、本成果が今後の日本の安心安全に向けて大きく貢献できることを期待したい。

【査読付発表論文リスト】

[1]Y. Feng, Y. Hori, K. Sakurai, & J. Takeuchi: “A Behavior-based Method for Detecting Distributed Scan Attacks in Darknets”, Journal of Information Processing Vol.21 No.3 pp527-538 July 2013

[2]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 pp615-636 2015

[3]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

【受賞リスト】

[1]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

[2]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

[3]牧田大佑、吉岡克成、松本勉、中里純二、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

【報道掲載リスト】

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

【本研究開発課題を掲載したホームページ】

[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