2　研究開発概要
2-1　サイバーセキュリティ技術の研究開発概要

井上大介

日々高度化するサイバー攻撃に対抗するため、サイバーセキュリティ研究室は 2011 年より、世界最先端のサイバー攻撃観測・分析・対策及び予防を可能にする技術基盤を構築し、実践的アプローチで社会課題の解決に貢献を目指し、サイバーセキュリティ技術に関する研究開発を実施してきた。2013 年には、それまでに研究実績を生かし、急増する標的型攻撃に対する根源的な防御戦術及びそれらの攻撃を安全に再現するための攻撃検証を研究するために、サイバー攻撃対策総合研究センターにサイバー防御戦術研究室及びサイバー攻撃検証研究室が設立された。本稿では、2011 年度から 5 年間の第 3 期中長期計画における、NICT で実施したサイバーセキュリティ技術の研究概要について述べる。

1　はじめに

インターネットは私たちの社会活動や経済活動に多大な恩恵をもたらし、インターネット普及以前の時代には、もはや逆戻りできない不可逆的変化を現代社会の隅々にまで及ぼしている。一方、その発展と同調するように、インターネットにおけるサイバー攻撃の脅威も拡大の一途をたどっている。サイバー攻撃は人間であるクラッカー（悪意を持ってハッキング行為を行う者）が引き起こすものだが、そのツールとして使われるのがマルウェアと呼ばれる不正なプログラムである。90 年代前半までマルウェアは愉快犯もしくは自己顕示を目的として作成・流布されることが多かったが、90 年代後半以降は金銭詐取を目的とした組織的な犯罪のツールとして利用され始め、高度化・巧妙化が急速に進んでいる。

このようにマルウェアに起因するサイバー攻撃に対抗するために、我々は、サイバー攻撃や標的型攻撃をリアルタイムで把握し適切な対応を実施するため観測・分析・対策技術、攻撃の前兆を捕えて予防を行うための基盤技術の開発を進めるとともに、得られたマルウェアや攻撃トラフィックのデータを、研究や人材育成に役立てるべく、防御技術についても研究を行っている。

本稿では、第 3 期中長期計画においてサイバーセキュリティ研究室で研究開発を行ってきた、世界最大規模のサイバー攻撃観測網の構築、サイバー攻撃分析・予防基盤技術、IPv6 セキュリティ検証と防御技術、サイバーセキュリティ研究基盤の 4 つの研究テーマについて紹介する。

2　サイバー攻撃観測網の構築

2.1　無差別型攻撃対策

我々は、無差別型攻撃対策として、インシデント分析センター NICTER*1（図 1）の研究開発を進め、外部組織及び海外へのセンサ展開により、平成 27 年度にはダークネット（未使用 IP アドレス）観測規模を倍化し世界最大規模の 30 万アドレスを達成した。観測網の拡大により、リフレクション型 DoS 攻撃*2（DRDoS）の準備活動や、IoT 機器の大規模感染等、新たな攻撃の兆候を迅速に発見可能なシステムを構築

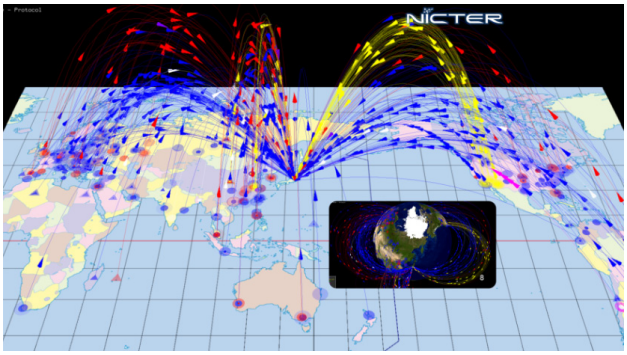

図 1　インシデント分析センター NICTER

*1　インシデント分析センター NICTER：Network Incident analysis Center for Tactical Emergency Response

*2　DNS リフレクション攻撃とは、リフレクション、つまり反射を用いた攻撃で、送信元の IP アドレスを偽装した DNS リクエストを DNS サーバに送ることによって、偽の送信元である攻撃対象に大量の DNS パケットを送り付ける攻撃のこと。

している。なお、サイバーセキュリティ分野における国際連携の一環として、同センサの米国、欧州機関等への海外展開を進めた。

特に、2014 年、2015 年の NICTER ダークネット観測統計では、1 つの IP アドレス当たりの年間の総観測パケット数が毎年倍化するなど、著しい増加傾向がみられるが、宛先ポート番号別にパケット数を見てみると、サービスとして 23 番ポート（TCP）上でのパケットが増加している傾向がみられ、横浜国立大学の吉岡研究室の調査結果では、実際に利用されている Web カメラやブロードバンドルータなどの IoT デバイスがマルウェアに感染し、これらの攻撃元となっていることが分かっている。この NICTER 観測結果の詳細については、「**3-1**　NICTER のダークネット長期分析」の資料を参照いただきたい。

さらに、NICTER による観測・分析情報は、JPCERT/CC、IPA、@Police、国内大学等が参画組織である SIGMON（定点観測友の会）、国内 ISP による DoS 攻撃への迅速な対応と協調対処を行うワーキンググループ及び総務省の ACTIVE プロジェクトに提供し情報共有を行っている。また平成 24 年度には、NICTER の技術を発展させ、プライベートアドレスから NICTER 観測網への通信をした際にアラートを出す仕組み（DAEDALUS[*3]）と実ネットワーク可視化・分析システム（NIRVANA[*4]）の開発を開始した。

災害時に、この観測結果から得られた観測情報をネットワーク障害の迅速な把握等に活用するための応用技術についても研究開発を行い、被災地のネットワークの死活状況推定（ACTIVATE）というシステムを構築している。

また、サイバー攻撃観測用センサの柔軟かつ動的な配置を実現する能動的サイバー攻撃観測網の構築に向け、複数組織に分散配置した仮想センサ群（仮想化技術を用いたトンネリングノード）と、センター側に設置した動作モードの異なる種々のセンサの動的スイッチングを組み合わせた能動的サイバー攻撃観測技術 GHOST[*5] Sensor について、研究開発を進め、平成 27 年度には、新たに約 1 万 6 千アドレスの大規模ダークネットで、長期運用試験（図 2）を実施し、マルウェア捕獲率の向上を実証した。

図 2　能動的サイバー攻撃観測技術
Ghost Sensor の長期運用試験

この NICTER の災害時応用の詳細及び NICTER のスピンオフ技術の無差別型攻撃対策のための対サイバー攻撃アラートシステム DAEDALUS については、**3** の関連資料を参照されたい。

2.2　無差別型攻撃対策

我々は、標的型攻撃対策として、マルウェアに感染したコンピュータからの情報流出に対処する技術についてのフレームワークデザインと、一部プロトタイプ開発を行っている。

標的型攻撃への対策技術の確立に向けて、これまでに進めてきた研究開発を発展させ、組織内ライブネット（実トラフィック）のリアルタイム観測及び分析と、各種セキュリティアプライアンス群からのアラート集約を行うとともに、リアルタイム可視化インターフェイスからアラート発生源へのドリルダウンを可能にするサイバー攻撃統合分析プラットフォーム “NIRVANA 改”（ニルヴァーナ・カイ）の開発を進め、複数種のアラートの横断的な分析を実現する相関分析エンジンの開発、エンドホスト連携機能及び自動防御機能の開発を行った。また、NIRVANA 改を Interop Tokyo に導入し、ShowNet（最先端のネットワーク機器で構築された展示会場ネットワーク）のライブネット観測・分析を行うとともに、国内外のセキュリティ関連企業複数社と連携して、多様なセキュリティアプライアンス群からのアラート集約の実証実験を実施した。直近の Interop Tokyo 2016 においても、多様なセキュリティアプライアンス群からのアラート集約の実証実験を実施した。

さらに、膨大なライブネットのリアルタイム分析を可能にするライブネット高速分析基盤の開発を進め、大容量オンメモリ処理により NICT のライブネットにおいて 20 万パケット毎秒のリアルタイム処理性能を実証した。また、本分析基盤上で動作する分析エンジンとして、ネットワーク境界侵害検出エンジンを開発するとともに、ブラックリスト方式、ホワイトリスト方式、スロースキャン検知といった、各種ライブネッ

＊3　DAEDALUS: direct alert environment for darknet and livenet unified security
＊4　NIRVANA: nicter real-network visual analyzer
＊5　GHOST: global, heterogeneous, and optimized sensing technology
＊6　NIDS: Network-based Intrusion Detection System
＊7　HIDS: Host-based Intrusion Detection System

ト分析エンジンを開発した。

アンチウイルスソフトを含む、エンドホストソフト（ホストベースの侵入検知）とライブネット分析（ネットワークベースの侵入検知）を協働させるNIDS[*6] HIDS[*7]連携システムの開発を行い、エンドホストのプロセス状態監視やセキュリティレベルの変更等を一元的に行う機構、エンドホストからの収集情報及びエンドホスト連携機能及び自動防御機能を開発した（図3）。

サイバー攻撃検証研究室と共同で、StarBED上に組織内ネットワークを簡易的に模擬した模擬ネットワーク環境を構築するとともに、攻撃者が使用する指令サーバ（C&Cサーバ）やRAT（リモートアクセスツール）を整備し、本環境内で標的型攻撃の一連の流れを実際に再現する模擬攻防実験を実施し、防御側の攻撃観測・分析技術の検証や、標的型攻撃時に生成される各種ログの検証を行った。

NIRVANA改をベースに、サイバー攻撃の対処能力の強化を目的とした競技“CTF”（Capture The Flag）の攻防戦をリアルタイムに視覚化する専用エンジン“NIRVANA改 SECCONカスタム”や“NIRVANA改 SECCON カスタム Mk-II”、“AMATERAS”を、毎年のCTFの実施に併せて開発し、情報セキュリティのコンテストイベントであるSECCON全国大会においてCTF決勝戦の世界各地から集まったCTFのトップチームによる攻防戦をリアルタイムに視覚化した。

3　サイバー攻撃分析・予防基盤技術

我々は、WebやSNS等を利用した新たな脅威に対する観測技術及び分析技術の研究開発を行い、各種センサからの多角的入力やデータマイニング手法等を用いたサイバー攻撃分析・予防基盤技術を研究開発している。

Webを利用したドライブ・バイ・ダウンロード（DBD）攻撃に対抗するための研究開発として、Webブラウザにプラグインする形式のセンサをユーザに大規模展開し、ユーザ群の巨視的な挙動をセンター側で観測・分析することで、マルウェアダウンロードサイト等の不正サイトを検出するとともに、ユーザの不正サイトへのWebアクセスを直接的にブロックし、Webを利用した攻撃への対抗を可能にするDBD攻撃対策技術を開発した。平成26年度には小規模な実験を、平成27年度には約1,600名のユーザ参加型大規模実証実験を実施し（図4）、有効性評価を行うとともに、実証実験に先立ち、外部有識者を含めた実証実験実施内容検討会を開催し、個人情報の適切な管理等についての法的・技術的な検討を行っている。

また、SNSセキュリティ技術の基礎研究として、SNSをユーザアカウント間及びそれらアカウントに関連したリソース間のリンク構造でモデル化し、そのモデル上でスパムメッセージの拡散やマルウェア感染等を把握する手法の検討やSNS観測技術及び分析技術のプロトタイプ開発、SNSにおけるなりすまし等の不正ユーザ対策として、SNSユーザ同士が連携協力する不正ユーザ検出手法の提案と実証実験、有効性評価を実施した。

サイバー攻撃分析・予防基盤技術の確立に向け、ブラックホールセンサや各種ハニーポット、Webクローラ、スパムメール、マルウェア動的解析結果等からの多角的入力情報を用いて各種のサイバー攻撃間の相関性を明らかにするためのマルチモーダル分析について研究開発を行い、これまで個別に分析されていた各種のサイバー攻撃間の相関性を明らかにした。また、サイバー攻撃予測の実現に向け、ダークネットトラフィックからボットによる人為的・突発的なトラ

図3　NIRVANA改の自動防御機能

図4　DBD攻撃対策フレームワーク
実証実験サイト

フィック増の影響を除外し、ワーム型マルウェアによる感染活動のトレンドのみを抽出するため、データマイニングを用いたボットトラフィックの検出手法を開発した。平成 24 年度には、この開発した結果を標的型攻撃対策技術として、組織内の通信から異常を検出する分析エンジンと、組織内から組織外への通信から異常を検出する分析エンジンのプロトタイプとして、NICT 内ネットワークで実証実験を実施した。また、マルチモーダル分析として、DNS amp 攻撃（DNS クエリの反射を用いた DDoS 攻撃）に関してダークネットと DNS ハニーポットでの分析を実施し、DNS オープンリゾルバ探索のスキャンがその前兆であることが判明するなど、サイバー撃分析・予防基盤技術の基盤となる技術を確立している。

さらに、DRDoS ハニーポットを総務省の PRACTICE プロジェクト（国際連携によるサイバー攻撃予知・即応プロジェクト）と共同で運用するとともに、DRDoS のアラート発報機構を開発し、国内組織への DRDoS 攻撃を高精度で検知することに成功した。

4　IPv6 セキュリティ検証と防御技術

IPv6 等の新たなネットワークインフラのセキュリティ確保に向けて、IPv6 環境等のセキュリティ検証及び防御技術の研究開発を行っている。

NICT と OS ベンダ、通信事業者、ネットワーク機器ベンダ等とで設立した IPv6 技術検証協議会において、企業ネットワークを想定した IPv6 セキュリティ検証環境を設計・構築し、その環境下で 40 通りの攻撃シナリオを実行して攻撃の成否や原因等の検証を実施した。

また、それらの攻撃シナリオに対する防御策について防御策を協議会内で検討し、平成 23 年度には、100 通りの防御策について最終報告書としてまとめ、一般公開を行った。検証結果や防御策については、ITU-T 国際勧告化を実施（平成 25 年 10 月 X.1037 として承認）した。また、40 種類の攻撃シナリオのうち、24 種類は NDP（近隣探索プロトコル）を要因とした攻撃であることから、NDP の不正使用に対する防御技術（NDP Guard）を開発し、実験環境での有効性評価を実施した。

5　サイバーセキュリティ研究基盤

我々は、機構の中立性・公共性を活かして収集した攻撃トラフィックやマルウェア検体等のセキュリティ情報の安全な利活用を促進し、我が国のネットワークセキュリティ研究の向上に資するため、セキュリティ情報の外部漏洩を防止するフィルタリング技術やサニタイジング技術等を研究開発するとともに、それらの技術を組み込んだサイバーセキュリティ研究基盤（NONSTOP[*8]）を構築し、産学との連携の下で実運用を行っている。

平成 23 年度には、NONSTOP のフィルタリング技術として、マルウェア検出や PCAP（パケットデータ）検出、圧縮ファイル検出、FIPS140 -2 の乱数検定に基づく暗号文検出及び通信量制限等の機能を導入するとともに、攻撃トラフィックに対してはセンサの IP アドレスに対するリアルタムサニタイジング技術を導入し、セキュリティ情報の安全な利活用の基盤を整備した。またその後、マルウェア検体を扱う仮想マシン内にデバッグ機能を追加、スパムメール等の情報追加などの機能強化を行ってきた。

さらに、最初は国内 3 大学、その後は国内 8 大学等と連携し、NONSTOP の試験運用を行ったり、国内最大のマルウェア対策研究専門のワークショップであるマルウェア対策研究人材育成ワークショップのデータセットとして 2013 年から、NONSTOP 経由でダークネットトラフィックを提供するなどして、NICTER が収集したセキュリティ情報の利活用を進め、国内の複数の組織が研究利用するなど、喫緊の課題となっているセキュリティ人材の育成に貢献した。

井上大介　（いのうえ　だいすけ）
サイバーセキュリティ研究所
サイバーセキュリティ研究室
室長
博士（工学）
サイバーセキュリティ、ネットワークセキュリティ、情報セキュリティ

＊8　NONSTOP：nicter open network security test-out platform