3.4.1　ネットワークセキュリティ研究所　サイバーセキュリティ研究室

室長　　井上大介　ほか 11 名

日々高度化・巧妙化するサイバー攻撃に対抗するため、世界最先端のサイバー攻撃観測・分析・対策およ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

【概　要】

- 進化を続けるサイバー攻撃やマルウェアに能動的・先行的に対抗するため、観測範囲を 30 万アドレス程度に倍加させた世界最大規模のサイバー攻撃観測網を構築するとともに、災害時には当該観測網によって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研究開発を行う。本年度は、サイバー攻撃の能動的な観測・分析・対策を実現するための基盤技術として、センタからの指令によりセンサの動作モード（応答の可否や OS バージョン等）を柔軟に変更可能な新型センサのメカニズムを設計・開発する。また、外部機関との連携を促進し、ダークネット（未使用 IPv4 アドレス）の観測規模を現状の約 14 万から約 18 万程度に拡大する。さらに、災害時にダークネットの観測結果をネットワーク障害の把握に活用するための基礎検討を行う。
- 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、サイバー攻撃を観測する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・予防基盤技術を確立する。本年度は、Web を利用したドライブ・バイ・ダウンロード攻撃に対抗するため、ユーザの Web ブラウザ上の挙動の観測・分析技術と、Web ブラウザに直接作用する対策技術の基礎検討及びプロトタイプ開発を行う。また、SNS の観測技術の基礎検討とプロトタイプ開発を行う。また、サイバー攻撃分析・予防基盤技術の確立に向けて、マクロ－ミクロ相関分析の高度化（入力情報の多角化）を行うとともに、サイバー攻撃予測アルゴリズムの基礎検討を行い、数時間オーダの予測について技術的な見通しを立てる。
- 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う。本年度は、民間企業等との連携の下、IPv6 セキュリティ検証環境の構築を進めるとともに、30 種類以上の攻撃シナリオを実行し、その結果得られた知見をガイドライン等として公開することで社会還元を図る。また、それら攻撃に対する防御技術について基礎検討とプロトタイプ開発を行う。
- NICT 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）を構築し、産学との連携の下で実運用を行う。本年度は、NONSTOP に組み込むフィルタリング技術やサニタイジング技術の基礎検討及びプロトタイプ開発を行うとともに、大学等との連携の下で試験運用を行う。
- nicter アラートシステム（DAEDALUS）と実ネットワーク可視化・分析システム（NIRVANA）について、H23 ～ 24 年度中の運用外部化や技術移転等を目指して民間企業等との調整を進める。

【平成 23 年度の成果】

- 能動的サイバー攻撃観測網の基本設計を行い、複数組織に分散配置した仮想センサ群と、センタ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観測アーキテクチャを提案し、基礎評価を実施した。また、外部組織へのセンサ展開を進め、ダークネット観測規模を約 19 万アドレスに拡大した（図 1）。さらに、大規模ダークネット観測の災害時応用技術の確立に向けた基礎検討を行い、マルウェア感染ホスト群からのダークネットへのアクセスを逆用して、被災地周辺のネットワークの死活状況の推定を行うシステム ACTIVATE（Active Connection Tracer for Internet Vitality AuTo-Estimation）を提案し、

図 1　拡大した nicter のダークネット観測網

ダークネットの災害時応用の可能性を示すとともに、ダークネットトラフィックを都道府県ごとに集計する統計機能の開発を行った。

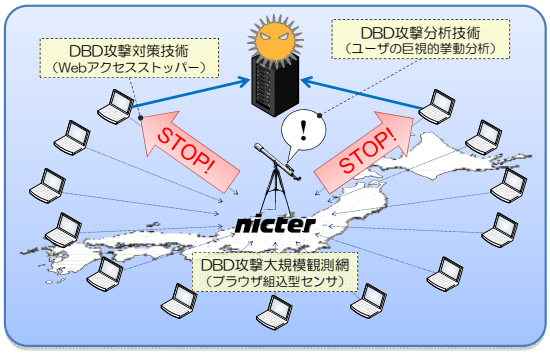

図 2　DBD 攻撃対策フレームワーク

- 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ドライブ・バイ・ダウンロード（DBD）攻撃対策フレームワークの提案とプロトタイプ開発を行った（図 2）。また、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、SNS セキュリティ技術の基礎検討を行った。
- 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（無応答型ダークネットセンサ）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たマルチモーダル分析を提案し、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するための第 1 弾検証を行った。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の前処理方法や各種データマイニングアルゴリズムの適用についての基礎検討及び基礎実験を実施し、数時間オーダの予測についての技術的見通しを立てた。
- 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を協議会内で検討し､その中から 16 の防御技術についてプロトタイプ開発を行った。検証結果や防御策については、中間報告書を作成して協議会メンバに展開するとともに、ITU-T SG17 Q2（X.ipv6-secguide）の寄与文書として国際ガイドラインへの入力を行った。
- サイバーセキュリティ研究基盤（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イ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。さらに、国内 3 大学と連携し、NONSTOP の試験運用を行い、nicter が収集したセキュリティ情報の利活用を進めた。

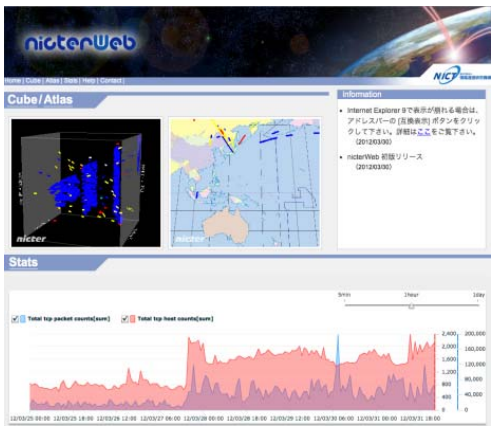

図 3　nicterWeb（http://www.nicter.jp/）

- 研究開発成果の社会還元を進め、NIRVANA（レイヤ 2 観測バージョン）を国内大手企業に導入した。また､NIRVANA（レイヤ 3 観測バージョン）を国内システムインテグレータに技術移転し､一般販売を開始した。DAEDALUS についても、技術移転に向けた国内企業との調整を開始し、サービスイメージの検討を進めた。さらに、nicter の観測結果の一部について、Web サイト（nicterWeb）での外部公開を開始した（図 3）。
- 政府機関や国内企業を狙った標的型攻撃が新たな脅威として社会問題化したことを踏まえ、標的型攻撃対策技術の確立に向けた取り組みを開始し、標的型攻撃に用いられたマルウェア検体の解析及び NIRVANA とデータマイニング技術を組み合わせた検出技術の基礎検討を行った。
- 国民の安心・安全なネットワーク利用に向けたネットワークセキュリティ技術の研究開発能力の向上及び研究開発成果の社会展開の促進のため、通信事業者、セキュリティベンダ、メーカ及び学識経験者等とともに、ネットワークセキュリティ研究フォーラムを設立した。
- サイバーセキュリティに関する国際的な情報共有や研究協力を促進するため、米国、欧州、アジア・太平洋地域の諸国との国際連携を推進するとともに、nicter センサの海外展開を行った。