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 12 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

【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。
- 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・予防基盤技術を確立する。
- 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。
- 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するため、サイバーセキュリティ研究基盤（NONSTOP[1]）を構築し、産学との連携の下で実運用を行う。
- nicter アラートシステム（DAEDALUS[2]）と実ネットワーク可視化・分析システム（NIRVANA[3]）について、平成 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 24 年度の成果】

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、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システムのプロトタイプ開発を行い、ブラックホールセンサ（無応答型センサ）とハイインタラクションハニーポット（高対話型センサ）の動的切り替えの動作検証を行った。また、外部組織への nicter センサの展開を進め、ダークネット観測規模を約 21 万アドレスに拡大（前年度比 2 万アドレス増）するとともに、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、同センサの海外展開（図 1）を進めた。また、ダークネットで観測される DDoS 攻撃の跳ね返りであるバックスキャッタの分析を進め、バックスキャッタの分類手法の提案を行った。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、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[4] の基礎検討を進め、ダークネットトラフィックから送信元ホストが所属する AS（自律システム）を特定するための技術検討及び、複数の送信元ホストからの情報を統合してネットワーク広域の死活状況を把握するための技術検討を行った。

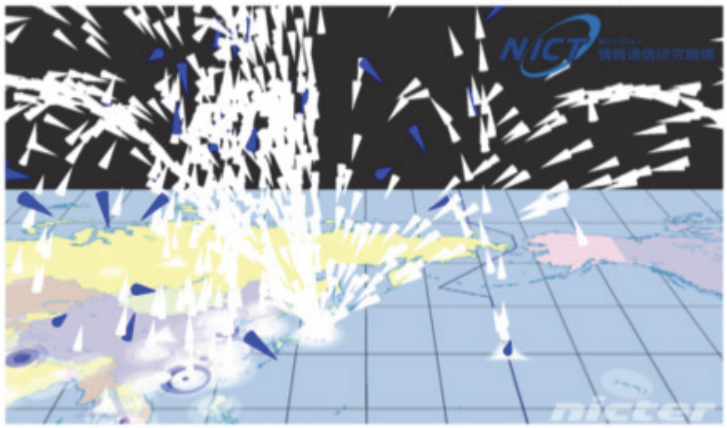

図 1　海外センサで観測した攻撃（青い口ケット）

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

[1] NONSTOP: nicter open network security test-out platform
[2] DAEDALUS: direct alert environment for darknet and livenet unified security
[3] NIRVANA: nicter real-network visual analyzer
[4] ACTIVATE: active connection tracer for Internet vitality auto-estimation

サイトへの Web アクセスの先行的なブロックを可能にするドライブ・バイ・ダウンロード攻撃対策フレームワークの技術検証及び、複数種の Web ブラウザに対応したプラグイン型センサ等のプロトタイプ開発を進めた。また、平成 26 年度より予定している実証実験内容の具体化や、ユーザからの収集情報に関する法的問題の検討を行った。さらに、ブラウザプラグイン型センサと組織内に設置されたゲートウェイ型センサの収集情報を突合することで、組織内のマルウェア感染ホストを検出する手法を新たに提案した。また、SNS におけるセキュリティ技術を確立するため、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によって表現するモデル化手法を提案するとともに、SNS のプライバシー問題に関する基礎検討を行った。さらに、SNS 観測技術及び分析技術のプロトタイプ開発を行った。

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など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、情報ソースとして FTP ハニーポットを追加するとともに、これら実データを用いた分析を実施した。また、サイバー攻撃予測の基礎検討を進め、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新たに開発した。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開発を行い、NICT 内ネットワークで実証実験を実施した。

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、IPv6 セキュリティ検証環境下で実施した 40 通りの攻撃シナリオと、それらの攻撃シナリオに対する 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 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。また、防御策の一部についてプロトタイプ開発を行った。

サイバーセキュリティ研究基盤 NONSTOP の機能強化を行い、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し、共用のマルウェア解析機能として利用可能とした。また、国内 3 大学と連携し、NONSTOP の試験運用を行い、ネットワークセキュリティを研究する学生を中心に、nicter が収集したセキュリティ情報の利活用を進めた。

研究開発成果の社会還元を進め、実ネットワーク可視化・分析システム NIRVANA を国内のシステムインテグレータ経由で一般販売し、国内の複数の企業等への導入を進めた。また、nicter アラートシステム DAEDALUS の可視化エンジン DAEDALUS-VIZ を新規開発（図 2）し、サイバーセキュリティの可視化技術に関する国際会議 VizSec 2012 に採録された。DAEDALUS のアラート情報を外部利用する仕組みを整備し、国内企業が nicter の大規模ダークネット観測結果を利活用した商用アラートサービスを開始した。nicter の観測結果を広く公開する nicterWeb を安定稼働させるとともに、センサ設置組織向けに機能強化版の nicterWeb premium を開発し、限定公開を開始した。

図 2　DAEDALUS-VIZ