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。
- 対サイバー攻撃アラートシステム DAEDALUS[*2] 及びネットワークリアルタイム可視化システム NIRVANA[*3] について、技術移転を推進する。

【平成 25 年度の成果】

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と、センタに設置した各種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 GHOST[*4] Sensor の設計とプロトタイプ開発を行った。また、無応答型センサと高対話型センサをミリ秒オーダで切り替え、新規ホストからのサイバー攻撃を優先的に収集する機能を実現し、小規模実験運用により有効性を確認した。

図 1　24 万アドレスに拡大したダークネット観測網

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昨年度の約 21 万 IP アドレスから約 24 万アドレスに拡大するとともに、サイバーセキュリティ分野の国際連携の一環として、同センサの海外展開を進めた（図 1）。さらに、ダークネットの災害時応用技術の確立に向け、マルウェア感染ホストからのダークネット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推定を行うシステム ACTIVATE[*5] のプロトタイプ開発を実施した。

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について、複数種の Web ブラウザに対応したプラグイン型センサ及びセンタ機能のプロトタイプ開発を

[*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] GHOST: global, heterogeneous, and optimized sensing technology
[*5] ACTIVATE: active connection tracer for Internet vitality auto-estimation

完了した。さらに、センタ側の分析手法として、Web サイト間のリンク構造解析技術、収集した Web コンテンツの動的解析技術／静的解析技術を開発した。また、平成 26 年度より予定している小規模実証実験の実施に向け、ユーザ挙動ログ収集に関する法的検討及びユーザサポート体制構築を実施した。また、SNS における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を提案し、Facebook に対応したプロトタイプ実装及び小規模実証実験での運用を実施した。

サイバー攻撃分析・予防基盤技術の確立に向け、今年度新たに台頭した DNS amp 攻撃（DNS クエリの反射・増幅を用いた DDoS 攻撃）に関してダークネットと DNS ハニーポットのマルチモーダル分析を実施した。その結果、DNS amp 攻撃が始まる数日前から、その前兆である DNS オープンリゾルバ探索のスキャンがダークネットで観測されていることが判明した（図 2）。また、マルウェア解析の高度化に向けて、機械学習を用いたマルウェア難読化ツールの高精度な自動判別手法を開発した（国際会議 Asia JCIS 2013 において Best Paper Award を受賞）。また、サイバー攻撃予測を実現するため、ダークネットトラフィックからボットネット等の人為的・突発的な要素を除去した上でモデル構築を行う予測フレームワークの基礎設計を実施した。

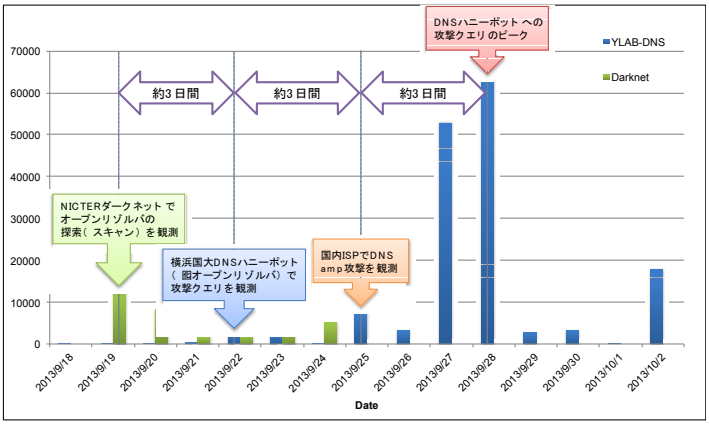

図 2　DNS amp 攻撃に関するマルチモーダル分析

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 2012 年に公開した IPv6 セキュリティに関するガイドラインを基に、ITU-T において国際勧告化を実施（2013 年 10 月 X.1037 として Approved）。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）を検討し、プロトタイプ開発を実施した。

サイバーセキュリティ研究基盤（NONSTOP）の管理機能を強化するとともに、スパムメール等の情報追加を実施した。また、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 2013（MWS2013）のデータセットとして、NONSTOP 経由でダークネットトラフィックを提供した。その結果、国内 14 組織が NICTER の提供データを研究利用し、6 件の論文発表が行われた。

DAEDALUS については、組織内のプライベート IP アドレス観測・分析機能を新規開発し、国内企業に技術移転を行った。また、海外の複数の政府機関及び教育機関に対し、アラートの送信を開始した。さらに、地方自治情報センター LASDEC（平成 26 年 4 月から地方公共団体情報システム機構）との連携の下、地方自治体へのアラート提供を開始した（図 3）。これら DAEDALUS の研究開発・社会還元活動が評価され、2013 年グッドデザイン賞を受賞した。NIRVANA は新たに国内企業への技術移転を完了するとともに、その他、国内外の組織への導入に向け、協議を進めた。

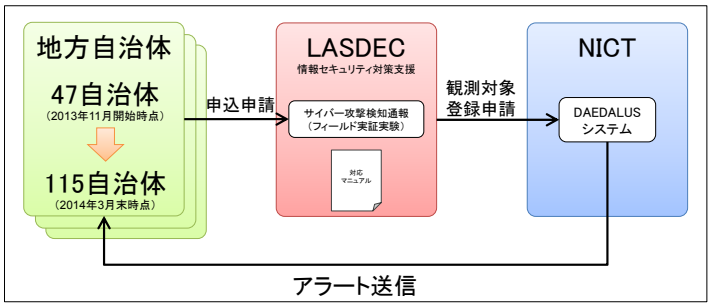

図 3　地方自治体への DAEDALUS アラート提供