

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 27 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（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能動的サイバー攻撃観測技術 GHOST*4 Sensor について、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 1）を実施し、マルウェア捕獲率の向上を実証した。



図 1 能動的サイバー攻撃観測技術 GHOST Sensor の長期運用試験

外部組織への NICTER センサの展開を進め、ダークネット観測範囲 30 万アドレスを達成するとともに、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、同センサの米国、欧州機関等への海外展開を進めた。また、大規模ダークネット観測により、リフレクション型 DoS 攻撃 (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することが可能となった。

上記の研究開発に加え、ダークネット観測・分析結果の実社会での利活用の一環として、総務省の ACTIVE プロジェクト（国民のマルウェア対策支援プロジェクト）にマルウェア感染が疑われる IP アドレスの情報を提供し、国内 ISP を経由して個別の ISP ユーザへの注意喚起が行われ、国民生活の安全性向上に貢献した。

*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

Webを利用したドライブ・バイ・ダウンロード(以下、DBD)攻撃に対する根源的な対策技術を確立するため、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DBD攻撃対策フレームワークについて、約1,600名のユーザ参加型大規模実証実験を実施した(図2)。

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、マルウェアの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おいて、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ハニーポットを連動させるシステムの基盤技術を確立した。また、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。

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、ITU-Tにおいて国際勧告化を実施(平成25年10月X.1037として承認)したガイドラインに基づき、NDP(近隣探索プロトコル)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継続した。

サイバーセキュリティ研究基盤NONSTOPについて、国内10大学等との連携の下で試験運用を継続した。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2015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、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。

DAEDALUSは、地方公共団体情報システム機構(J-LIS)との連携の下、地方自治体へのDAEDALUSアラート提供を進め、平成28年3月末現在553の自治体が参画(図3)するなど、我が国のセキュリティ向上に寄与した。また、総務省JASPERプロジェクトへの一環としてASEAN諸国へのDAEDALUSアラート提供を行った。また、NIRVANAについては制御システムベンダ等への技術移転を行い、実社会への研究開発成果の展開を進めた。

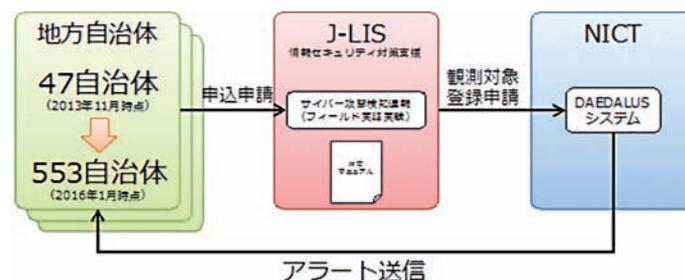


図3 地方自治体へのDAEDALUSアラート提供



図2 DBD攻撃対策フレームワーク実証実験サイト