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 9 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 26 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（図 1）について、センサの切替ルールを Lua 言語によって記述可能なフレームワークを実装するとともに、中規模実験運用を実施した。

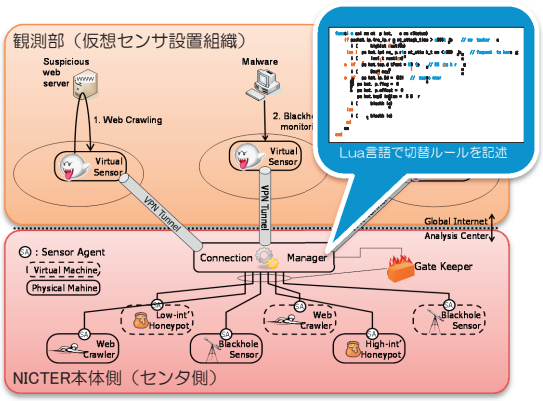

図 1　能動的サイバー攻撃観測技術
Ghost Sensor

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 28 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における国際連携の一環として、同センサの欧州機関等への海外展開を進めた。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[*5] について、プロトタイプ開発を実施し、有効性評価を行った。

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: **n**icter **o**pen **n**etwork **s**ecurity **t**est-**o**ut **p**latform
[*2] DAEDALUS: **d**irect **a**lert **e**nvironment for **d**arknet **a**nd **l**ivenet **u**nified **s**ecurity
[*3] NIRVANA: **ni**cter **r**eal-network **v**isual **ana**lyzer
[*4] GHOST: **g**lobal, **h**eterogeneous, and **o**ptimized **s**ensing **t**echnology
[*5] ACTIVATE: **a**ctive **c**onnection **t**racer for **I**nternet **v**itality **a**u**t**o-**e**stimation

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、小規模実証実験を実施した（図 2）。なお、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た。また、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を提案し、Facebook に対応したプロトタイプ実装を行い、小規模実証実験運用を継続し、有効性評価を行った。

図 2　DBD 攻撃対策フレームワーク実証実験サイト

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提案と評価を行った。また、サイバー攻撃分析・予防基盤技術の基盤となる NICTER 全データへの統一アクセスを実現する統合 API の設計・開発を開始した。さらに、サイバー攻撃予測を実現するため、サイバー攻撃予測フレームワークのプロトタイプ開発を実施した。

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、平成 24 年に国内公開した IPv6 セキュリティに関するガイドライン及び、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実施した。

サイバーセキュリティ研究基盤 NONSTOP について、国内 8 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 2014（MWS2014）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。

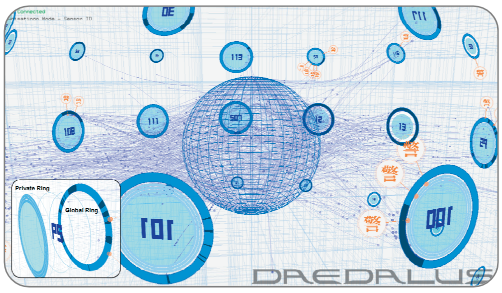

図 3　DAEDALUS-VIZ /* 2nd Evolution */

DAEDALUS は、プライベートアドレス観測・可視化機能を追加（図 3）するとともに、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 27 年 3 月末現在 223 の自治体が参画（図 4）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。

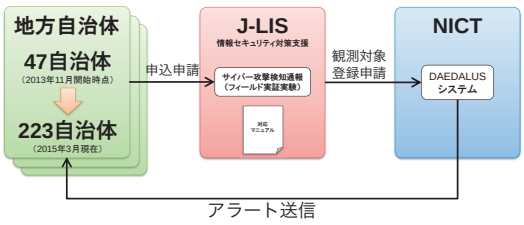

図 4　地方自治体への DAEDALUS アラート提供