3.7.1 サイバーセキュリティ研究室

室長　井上 大介　ほか29名

世界最先端のサイバー攻撃観測・分析・対策及び予防の基盤技術構築

■概要

1. 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、これまでに構築した世界最大規模のサイバー攻撃観測網において、機械学習等を応用した通信及びマルウェア等の分析支援技術を高度化するための研究開発を行う。
2. 急増しているルータやWebカメラなどのIoT[*1] 機器を踏み台にしたサイバー攻撃の脅威に対し、観測技術及び分析技術の研究開発を行うとともに、セキュリティ機器など複数の情報源からの情報を多角的に取り入れマルチモーダルなサイバー攻撃分析技術と可視化を駆使したセキュリティ・オペレーション技術を確立する。
3. サイバーセキュリティ研究及びセキュリティ・オペレーションの遂行に不可欠なマルウェアやインシデント情報等のサイバーセキュリティ関連情報を大規模集約し、安全かつ利便性の高いリモート情報共有を可能とするCURE[*2] の構築とこれに基づく自動対策技術を確立する。また、CUREを用いたセミオープン研究基盤を構築し、セキュリティ人材育成に貢献する。
4. 政府機関、地方公共団体、学術機関、企業、重要インフラ等におけるサイバー攻撃対処能力の向上を目指し、模擬環境及び模擬情報を用いたアトリビューション（原因特定）技術等の研究開発を行う。
5. 機能強化を図ったネットワークリアルタイム可視化システム NIRVANA[*3] 改について、政府機関、学術機関、企業など重要インフラ等における技術移転を行うとともに、対サイバー攻撃アラートシステムDAEDALUS[*4] の地方公共団体への展開など成果展開を推進する。

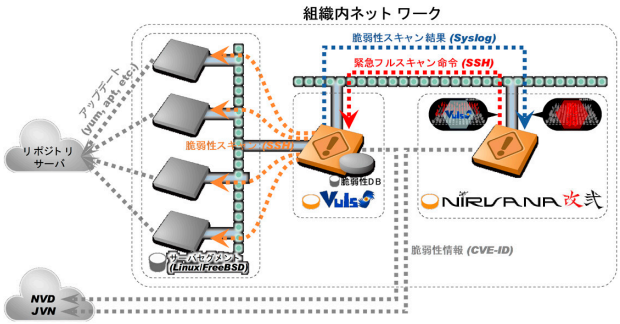

図1　NIRVANA改弐システム構成

■平成 30 年度の成果

1. 標的型攻撃等のサイバー攻撃に対抗するために、サイバー攻撃統合分析プラットフォーム「NIRVANA改」の高度化を進め、OS やソフトウェアの欠陥である脆弱性の迅速かつ効率的な管理を目指した脆弱性管理プラットフォーム「NIRVANA改弐」（図 1 ）を新たに開発した（6 月11日プレスリリース）。NIRVANA 改弐は、国産オープンソースソフトウェアの脆弱性スキャナVuls[*5] と連動することで、エージェントレスで組織内のサーバに定期的に接続して各サーバの脆弱性スキャンを行い、組織内の脆弱性の統合的な管理を可能にする。なお、この成果についてInterop Tokyo 2018で動態展示を実施した。
2. IoT機器向けセキュリティ技術として、マルウェア感染したIoT機器のユーザ通知実験をオランダのDelft工科大学、横浜国立大学との共同研究で実施した。この実験では欧州のISPと連携して、IoT機器のユーザに対して複数の手法で注意喚起を行った。その効果測定結果を国際会議NDSS2019において発表し、Distinguished Paper Awardsを受賞した。
3. CUREで大規模集約したセキュリティ関連情報の分析技術として、機械学習によるIoTマルウェアの自動分類技術を研究開発し、国際会議AsiaJCIS2018において、Best Paper Awardを受賞した。この手法では、マルウェアを構成する機械語を逆アセンブルして命令を抽出し、N-gram[*6] の組によって共通する命令列が多いほど類似度が高くなるように計算する。実際に、2,000個のマルウェア検体の類似度を計算し、2 次元平面上にマッピングした結果（図 2 ）、マルウェアの種類を明らかにすることができた。また、機械学習を用いたマルウェア大規模感染の早期検知手法として、ダークネット観測で収集される大量のパケットをテンソル分解[*7] することで、送信元IPアドレス群の協調動作を分析する手法

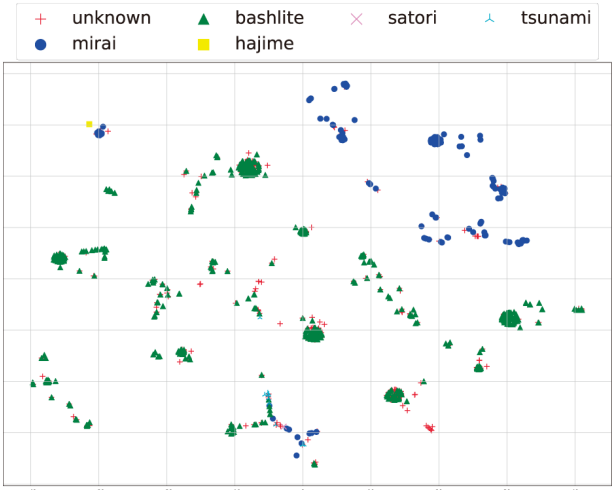

図2　類似度に基づいてマルウェアを分類した結果

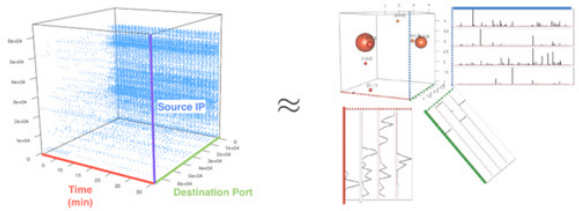

図3　テンソル分布によるマルウェア協調動作検出

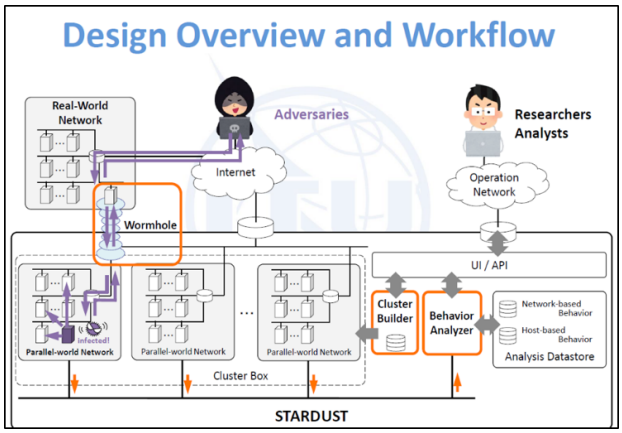

図4　STARDUSTのシステム詳細

を開発し、IoTマルウェア等の感染活動を自動検知することに成功（図３）した。この分析結果を国際会議ACM SAC 2019にて発表した。

4. 標的型攻撃の攻撃者を模擬環境に誘い込み、長期挙動分析を可能にする標的型攻撃誘引基盤STARDUST（図４）について、外部組織によるSTARDUSTの利活用を拡大し、外部連携の強化を行った。また、STARDUSTの高度化のための研究開発として、STARDUSTにより収集された各種データセットについて、観測対象環境、データの意味と構造、データの書式といった３つの要素からなるモデル化を実施し、動的データセット生成システムを実現した。なお、STARDUSTで培ったセキュリティ・テストベッド技術を活用し、ニュージーランドの ワイカト大学や台湾のAIS３など、海外機関におけるサイバー演習の技術支援を行った。

5. このほか、NICT委託研究「Web媒介型攻撃対策技術の実用化に向けた研究開発」（WarpDrive[*8]）において、攻殻機動隊 REALIZE PROJECT[*9] との連携の下、ブラウザプラグイン型センサーを開発し、６月にユーザ参加型の実証実験開始を開始した（６月１日プレスリリース）。その結果、平成31年３月末に延べ7,700ユーザを達成し、Web媒介型攻撃対策のための観測網を確立した。また、知能科学融合研究開発推進センター（AIS）とのCybersecurity連携プロジェクトとして、アラートのふるい分けと優先順位付け技術、上述のIoTマルウェアの機械学習による分類技術、テンソル分解によるマルウェアの協調動作検出技術などを開発した。さらに、サイバーセキュリティに関する情報発信として、通年のダークネット観測・分析結果をNICTER観測レポート2018で公表するとともに、NICTER Blog及びNICTER Webでの情報発信を行った。

---

*1 IoT: Internet of Things
*2 CURE: Cybersecurity Universal REpository
*3 NIRVANA: Nicter Real-network Visual ANAlyzer
*4 DAEDALUS: Direct Alert Environment for Darknet And Livenet Unified Security
*5 Vuls:フューチャー株式会社により開発された国産OSS脆弱性スキャナ
*6 N-gram: N文字単位で文字列を分解・解析する方法
*7 テンソル分解: テンソル（３軸以上のデータ）をより階数の少ないテンソル（含む行列やベクトル）の積和で表現する数学的な手法
*8 WarpDrive: Web-based Attack Response with Practical and Deployable Research InitiatiVE
*9 攻殻機動隊REALIZE PROJECT: 産学官と製作委員会が連携し「攻殻機動隊」に描かれている近未来テクノロジーの実現可能性を追求するプロジェクト