3.7.1 サイバーセキュリティ研究室

室長　　井上 大介　ほか27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。

■平成29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」のアラートフィルタ機能とリプレイ機能（図１）を新規に開発するなど、更にユーザビリティを向上させた。また、NIRVANA改と国産機器とのシステム連携を拡大し、セキュリティ機器による自動防御機能を追加した。なお、この成果はInterop Tokyo 2017にて展示を実施した。また、NIRVANA改について、国内サイバーセキュリティ企業へ開発した機能の技術移転を進めるとともに、政府機関や学術機関、重要インフラ等における導入を進めた.

2　サイバー攻撃トラフィックの攻撃元IPアドレスに対して能動的にアクセスし、応答データを自動分類してIoT機器の判定を機械学習で行うといった、IoT機器に対する能動的なアクセス及び機器からの応答を自動で分析・分類する機械学習による手法（図２）を確立し有効性を実証した。また、この成果を電子情報通信学会の情報通信システムセキュリティ研究会（ICSS）研究会において発表し研究賞を受賞した。

3　対サイバー攻撃アラートシステムDAEDALUSは、従前より地方公共団体情報システム機構（J-LIS）と連携して地方自治体へのDAEDALUSアラート提供を進めてきたが、新たに国立研究開発法人協議

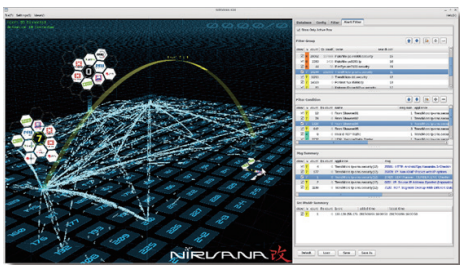

図1　2017年に追加したNIRVANA改の新機能

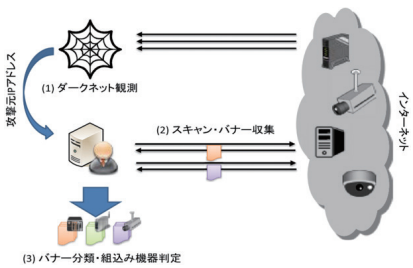

図2　能動的サイバー攻撃観測によるIoT機器分類

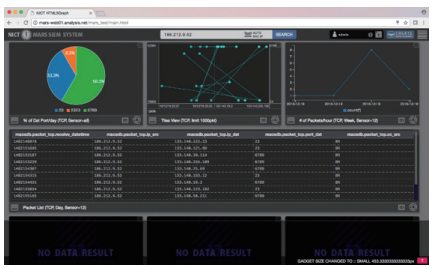

図3　CUREプロトタイプ

会（国研協）からの協力要請に基づき、国研協複数機関へのアラート提供及び提供準備を進めた。また、機構のインシデント分析センターNICTER[*5]で運用している大規模サイバー攻撃観測網の観測結果は、仮想環境を介して国内の研究機関へデータ提供も行っており、さらにNICTER Webや NICTERレポート（2018年２月 プレスリリース）、NICTER Blogでの情報公開を行うなど、国内セキュリティ強化・人材育成に貢献した。

4　CUREのプロトタイプ（図３）として、Web用のアプリケーションプログラミングインターフェース（API）を整備し、異種のデータベースの統合環境を整えた。また、自由度の高いWebユーザインタフェース（UI）を開発した。セキュリティ人材育成のためのセミオープン研究基盤となるセキュリティ向けクラウド型遠隔開発環境（NONSTOP）によるデータ共有の利用登録において、学術機関や企業など100組織を突破するとともに、若手セキュリティイノベーター育成プログラム（SeckHack365）においても活用された。

5　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）について、2017年５月にプレスリリースにより公開した。このSTARDUSTによる攻撃者誘引実験は継続され、累計20件以上の誘引に成功するとともに、模擬情報を用いたアトリビューション（原因特定）技術の基礎実験（図４）を開始した。この技術の外部組織による利用を促進するとともに、その成果をマルウェア対策研究人材育成ワークショップ（MWS2017）において発表し、ベストプラクティカル研究賞を受賞した。さらに、STARDUSTのWeb機能の強化や並行ネットワーク内のWindowsカーネル観測技術（Preserver）の開発を行った。なお、これら開発した模擬環境は、サイバー演習支援技術として、堅牢化技術競技（Hardening）に提供した。

6　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」として、Web媒介型攻撃対策フレームワーク（WarpDrive）のセンサーとセンター基盤技術を開発するなど、本格的にプロジェクトを始動させた。また、知能科学融合研究開発推進センター（AIS）のCybersecurityプロジェクトとの研究連携も開始し、研究データを活用したAIセキュリティ研究に関する研究体制の構築と３つの重点課題（図５）のとりまとめを行った。

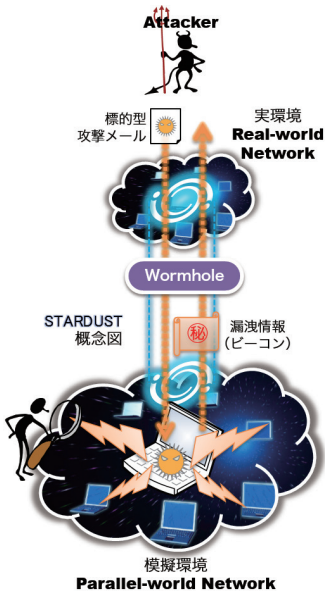

図4　STARDUSTによるアトリビューション技術の実験の概要

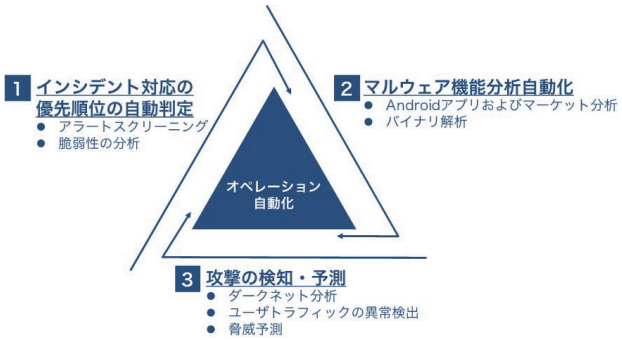

図5　AIS Cybersecurityプロジェクトにおける3つの重点課題

*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　NICTER：Network Incident analysis Center for Tactical Emergency Response