3.7.1 サイバーセキュリティ研究室

室長　　井上 大介　ほか23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28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」（図１）のアラート管理機能を更に強化し、アラートを自動分析して種類別統計を可能にするなど、ユーザビリティを大幅に向上させた。また、NIRVANA改と国産機器とのシステム連携を拡大し、アラクサラネットワークス株式会社のネットワーク機器及び株式会社PFUのセキュリティ機器による自動防御（図２）を可能にするなど、国産機器との連携強化を図った。なお、この成果をInterop Tokyo 2016にて展示を実施した。また、NIRVANA改の技術を応用し、「NIRVANA

＊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

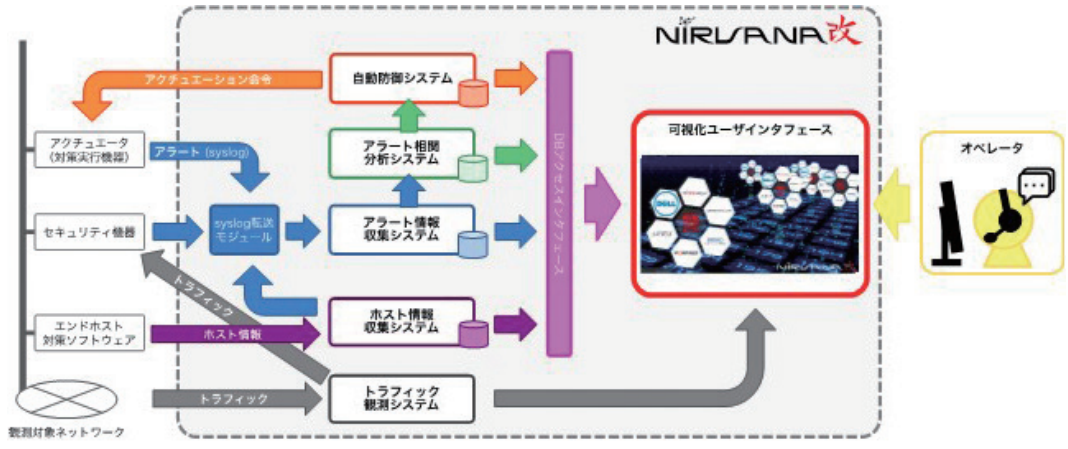

図1　NIRVANA改の機能構成

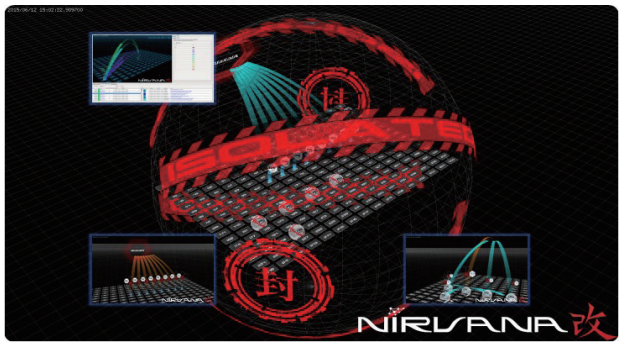

図2　バージョンアップしたNIRVANA改（通信の完全遮断）の可視化インターフェース

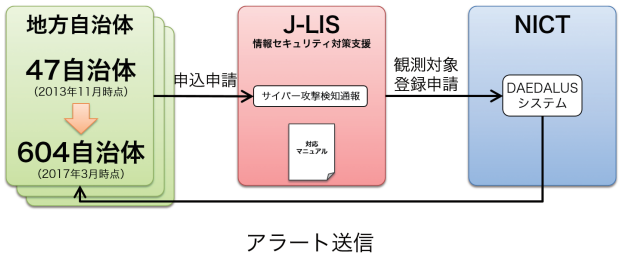

図3　地方自治体へのDAEDALUSアラート提供

改SECCONカスタムMk-III」を開発しサイバー模擬攻防戦（CTF）の様子のリアルタイムな視覚化に貢献した。NIRVANA改SECCONカスタムMk-IIIは、国内最大規模のCTFの大会であるSECCON2016決勝大会や総務省 サイバーコロッセオ×SECCON 2016に提供した。

2．対サイバー攻撃アラートシステム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ている。平成29年３月末現在604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への寄与が認められ、“「DAEDALUS」の開発に係る産学官連携”として産学官連携功労者表彰総務大臣賞を受賞した。これに加え、機構の分析センター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主要新聞各社を含む多数のメデイアで報道され、仮想環境を介して国内の研究機関にもデータ提供も行っており、さらにNICTER Webでの一般公開情報コンテンツも強化する等、国内セキュリティ強化・人材育成にも貢献した。

3．サイバー攻撃観測網の拡充と能動的なサイバー攻撃観測技術として、IoTマルウェア専用ハニーポットやリフレクション型DDoS攻撃観測用センサの開発を進め、The 19th International Symposium on Research in Attacks, Intrusions and Defenses（RAID 2016）に横浜国立大学、オランダのデルフト大学、ドイツのザールランド大学との共同研究として、リフレクション型

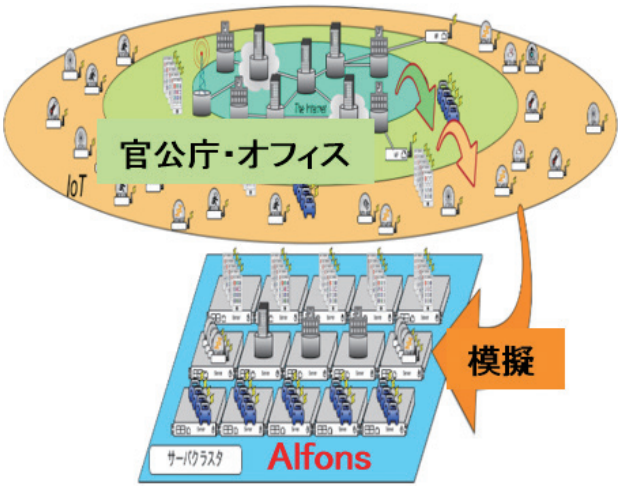

図4　模擬環境構築システム「Alfons」

図5　SecCap（実践セキュリティ人材育成コース）

DDoS攻撃の横断分析結果とマルウェアの解析回避技術の評価結果の２件が採録された。また、機械学習等を応用した通信分析技術、マルウェア自動分析技術、マルチモーダル分析技術の高度化に向けた基礎検討及びプロトタイプ開発を行い、攻撃通信をアソシエーション分析による新規攻撃を早期検知に成功するとともに、この分析支援技術の成果がIEEE Advanced and Trusted Computing 2016採録された。4．セキュリティ検証プラットフォーム構築活用技術について研究開発を進め、模擬環境及び模擬情報を用いたアトリビューション技術を確立するため、模擬環境を用いた攻撃者誘引の基礎実験を行うとともに、模擬情報を用いたアトリビューションについての基礎検討を行った。

さらに、セキュリティ・テストベッドの構築の研究開発を進め、模擬環境構築システム「Alfons」（図４）において、24ノード５サブネット環境を２時間以内に構築可能とするなどを実現し、その成果をSecCap（実践セキュリティ人材育成コース）（図５）とHardening Projectの２大会（Hardening 100 Value×Value, Hardening 100 Weakest Link）への環境支援として提供した。