3.7 サイバーセキュリティ研究所

研究所長　　宮崎 哲弥

■概要

我々の身の回りのモノ、そしてモノに搭載されているセンサーなどがネットワークにつながるIoT（Internet of Things）時代の利便性の陰で、IoT機器のセキュリティ対策が喫緊の課題となっている。さらに、IoT機器から集約されたビッグデータの利活用にあたって、情報漏えいやプライバシーの問題などサイバーセキュリティが扱う課題は日々拡大している。

サイバーセキュリティ研究所では、直近に迫っている危機から到来する近未来の情報社会課題に対処すべく、サイバー攻撃に実践的に対抗する最先端のサイバーセキュリティ技術や、社会の安心・安全を理論面から支える暗号技術などの以下に示すような研究開発を実施している。

1．サイバーセキュリティ技術

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、最先端の攻撃観測技術や分析技術等を研究開発する。また、サイバー攻撃に関連する情報を大規模に集約し、横断的分析や対策自動化等に向けた技術を確立し、研究開発成果の速やかな普及を目指す。

2．セキュリティ検証プラットフォーム構築活用技術

安全な環境下でのサイバー攻撃の再現や、新たに開発した防御技術の検証に不可欠な、セキュリティ検証プラットフォーム構築に関する技術の研究開発を行う。また、このプラットフォームを活用したサイバー演習等、セキュリティ分野の人材育成支援にも取り組む。

3．暗号技術

IoTの展開に伴って生じる新たな社会ニーズに対応するため、新たな機能を備えた機能性暗号技術の研究開発に取り組むほか、暗号技術の安全性評価を実施し、新たな暗号技術の普及・標準化及び安心・安全なICTシステムの維持・構築に貢献する。また、パーソナルデータの利活用を実現するためのプライバシー保護技術の研究開発や適切なプライバシー対策を技術支援する活動を推進する。

■主な記事

サイバーセキュリティ研究所における平成29年度の主なトピックスを以下に示す。なお、1.及び2.の詳細については、それぞれの研究室の報告において記す。

1．サイバーセキュリティ研究室の活動

（1）サイバー攻撃統合分析プラットフォーム（NIRVANA改：ニルヴァーナ・カイ）のより実践的なアラート・フィルタ機能やリプレイ機能を新規に開発するとともに、政府機関や学術機関、重要インフラ等におけるサイバーセキュリティ対策技術として導入を開始した。また、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を確立した。

（2）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サイバーセキュリティ・ユニバーサル・リポジトリ（CURE）のWeb用のアプリケーションプログラミング及びユーザインタフェースを開発し、異種間データベースの統合や自由度の高い開発環境の構築を行うとともに、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して、セキュリティ向けクラウド型遠隔開発環境（NONSTOP）によるデータ共有を行った。

（3）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、新たに利用申し入れのあった外部セキュリティ関連組織を加えて、分析結果の情報共有を行いサイバー攻撃対策技術研究開発の研究連携を拡大した。

（4）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）のサイバーセキュリティプロジェクトとして研究体制を構築し、研究データを活用したAIセキュリティ研究を推進している。

2．セキュリティ基盤研究室の活動

（1）世界初の高い安全性と相互接続性が可能な「群構造維持署名」を開発し、2017年７月に日本電信電話株式会社、カールスルーエ工科大と研究協力の成果としてプレスリリースを行うとともに、国際会議CRYPTO 2017において発表した。また、総務省、経済産業省及び独立行政法人情報処理推進機構（IPA）と連携して行っているCRYPTRECの活動として、IoT向け軽量暗号ガイドライン日英版を発行し公開を行った。

（2）実用化・国際標準化が進む格子暗号の安全性評価において、解析が不十分だったRandom Samplingアルゴリズムの再評価に成功し、国際会議Eurocrypt 2017で発表した。また、米国国立標準技術研究所（NIST）の耐量子計算機暗号標準化プロジェクトにおいて、量子コンピュータでも解読が困難な格子理論に基づく新公開鍵暗号方式LOTUS（ロータス）を提案した（2018年１月プレスリリース）。

（3）人工知能（AI）を活用したプライバシー保護データ解析技術として、複数の参加者が持つデータセットを互いに秘匿したままで深層学習を行うシステム（Deep Protect）を提案し、実用性検証を行い、AI連携・JST CREST研究「イノベーション創発に資する人工知能基盤技術の創出と統合化」を推進した。また、2017年５月30日より改正個人情報保護法が全面施行されたのを機に、仮名化によるプライバシーリスク評価ツールをシステム設計した。

3．研究所共通の活動

（1）Interop Tokyo 2017への出展

2017年６月７～９日に幕張メッセで開催されたInterop Tokyo 2017において、インシデント分析センター「NICTER」及び関連技術に関する出展として、組織内ネットワークで不審な振る舞いをするトラヒックをいち早く検知して防衛するサイバー攻撃統合分析プラットフォームNIRVANA改の新機能と、更に進化したネットワーク機器との連携及び標的型攻撃誘引基盤（STARDUST）をデモンストレーションとプレゼンにて紹介した（図１）。

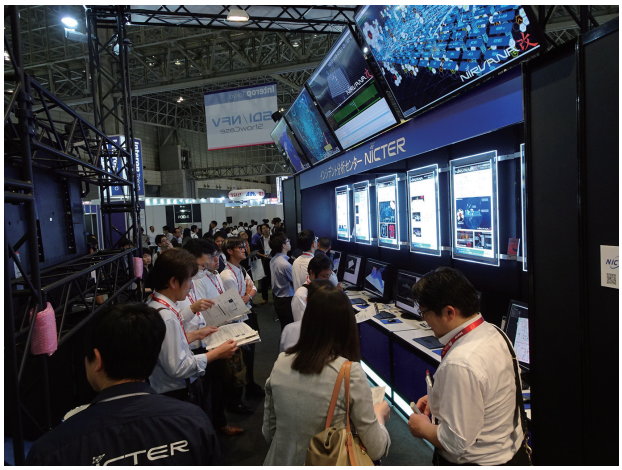

図1　Interop Tokyo 2017における展示

図2　「NICT サイバーセキュリティシンポジウム 2018」の模様

（2）「NICTサイバーセキュリティシンポジウム2018」において当研究所の研究成果を報告

2018年２月14日（水）「NICTサイバーセキュリティシンポジウム2018」にて、当研究所及びナショナルサイバートレーニングセンターの各研究室において実施する研究概要及びセキュリティ人材育成について紹介した。このシンポジウムでは、IoTにおけるサイバー攻撃の脅威とそのセキュリティ対策、プライバシーを保護したビックデータ利活用に関して当研究所と緊密な連携を行っている早稲田大学 森准教授、神戸大学 小澤教授及びPwCサイバーサービス合同会社 神薗所長から最先端の研究動向の講演を頂いた。当日は、民間企業や大学、官公庁等からサイバーセキュリティ関連業務に携わる方々を中心に190名を超える方々の参加があった（図２）。