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、サイバーセキュリティ技術として、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30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項を参照いただきたい。

1．サイバーセキュリティ研究室の活動

（1）国産オープンソースソフトウェアの脆弱性スキャナと連動する、脆弱性管理プラットフォーム「NIRVANA[*1]改弐」を開発し、サイバーセキュリティ対策技術としてInterop Tokyo 2018にて紹介するとともに、NICTのCSIRT[*2]に導入を開始した。また、IoT機器に対するマルウェアを自動で分析・分類する機械学習による研究開発を継続し、マルウェアに感染したIoT機器のユーザ通知実験を実施している。

（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・リポジトリ技術として、CURE[*3]の試験運用を開始するとともに、機関学習によるIoTマルウェアの種類を分類する自動対策技術の研究開発と、テンソル分解によるマルウェア協調動作検出による攻撃の検知・脅威予測手法の研究開発を行った。

（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、外部組織による利活用を拡大し、外部連携の強化を行っている。また継続的な研究開発として、STARDUSTにより集められた各種情報のデータセットをモデル化し、より利用者が望むデータセットの取得が可能なようにシステムを改良した。

（4）Web媒介型攻撃対策フレームワーク（WarpDrive）のブラウザプラグイン型センサーを開発し、６月に実証実験開始を開始し平成31年３月末に7,700ユーザを達成した。また、知能科学融合研究開発推進センター（AIS）のCybersecurityプロジェクトの攻撃の検知・脅威予測手法として、アラートのふるい分けと優先順位付け、IoTマルウェアの種類の機械学習による分類、テンソル分解によるダークネット観測で検知されたアラートの協調動作検出などを

開発している。

2．セキュリティ基盤研究室の活動

（1）暗号化した医療データの中身を見ることなく、解析対象外データの混入を防ぐ解析手法の実証実験を、国立大学法人筑波大学と共に行った（7月プレスリリース）。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、耐量子計算機暗号の安全性評価に関する動向調査報告書をCRYPTREC Report として発行する予定である。

（2）NICTで開発した、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）は、アメリカ国立標準技術研究所（NIST）の耐量子暗号（PQC：Post-Quantum Cryptography）標準化プロジェクトの69方式の中の1候補として取り上げられ、その技術について、NIST PQC標準化ワークショップにて発表した。さらに、LOTUSなど格子暗号の安全性評価に用いる格子点探索アルゴリズムの計算量について、量子版の厳密な評価を行った。この評価を古典版探索アルゴリズムの計算量の下限評価と組み合わせることで、長期的な運用に向けたパラメータ設定が可能になった。

（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の深層学習を行うシステム（Deep Protect）の研究開発を継続して行っており、銀行の実取引データを用いた不正取引検知の実証実験を神戸大学、株式会社エルテスと共に開始した（平成31年2月プレスリリース）。これは、実社会の膨大なデータを統合して利活用する際のプライバシー保護やデータ機密性の確保のため、暗号技術や人工知能技術を活用し、プライバシーを保護した状態で高速にデータ分析や異常検知を行う技術の応用として実施している。

3．研究所共通の活動

（1）Interop Tokyo 2018への出展

6月13～15日に幕張メッセで開催されたInterop Tokyo 2018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、脆弱性管理プラットフォーム「NIRVANA改弐」をデモンストレーションとプレゼンテーションにて紹介した。（図1）。

（2）「NICT サイバーセキュリティシンポジウム 2019」において当研究所の研究成果を報告

平成31年2月7日（木）「NICTサイバーセキュリティシンポジウム2019」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、当研究所と緊密な連携を行っている東京大学の國廣准教授から量子計算機と暗号技術の関係と将来動向を、日立製作所の寺田主管研究員からサイバー攻撃誘引基盤（STARDUST）における観測事例の紹介に関する講演を頂いた。さらに、井上室長をモデレータとした若手研究者3名によるパネルディスカッションを実施し、セキュリティ分野における「数字」の見方・伝え方やNICTに今後期待する研究課題に関する議論を行った。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220名超の参加があった。（図2）。

*1　NIRVANA: Nicter Real-network Visual ANAlyzer
*2　CSIRT: Computer Security Incident Response Team、組織内の情報セキュリティ問題を専門に扱うチーム
*3　CURE: Cybersecurity Universal Repository

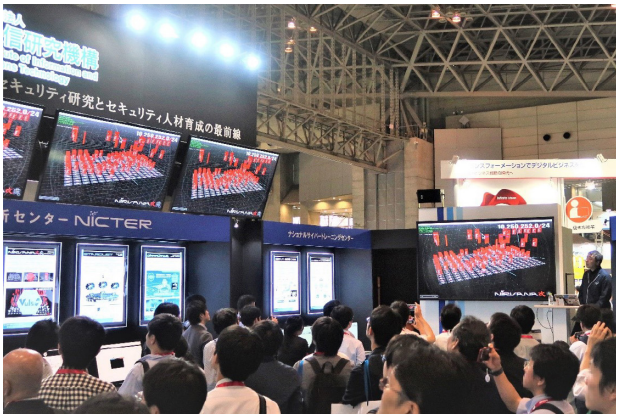

図1　Interop Tokyo 2018における展示


図2　「NICT サイバーセキュリティシンポジウム 2019」の模様