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当たって、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28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）のアラート管理及び可視化機能を強化し、国産セキュリティ機器との連携を拡充するとともに、民間への技術移転や政府機関、学術機関への導入を実施した。なお、このNIRVANA改のデモンストレーションをInterop Tokyo 2016にて実施し、この機能に対しBest of ShowNet Awardを受賞した。

（2）リフレクション型DDoS攻撃の解析を横浜国立大学、オランダのDelft大学との共同研究で、マルウェアの解析回避技術の評価を横浜国立大学、ドイツのSaarland大学との共同研究で実施し、いずれの成果も国際会議RAID2016（The 19th International Symposium on Research in Attacks, Intrusions and Defenses）にて採録されるなど、高く評価された。

（3）サイバー攻撃の観測・分析・対策を行うインシデント分析センター（NICTER）が観測した情報を公開するNICTERWEB（http://www.nicter.jp/）において、情報セキュリティ関連組織や企業・大学の情報セキュリティ管理部門からの要望に応え、機能強化を行うとともにデータの公開範囲を拡大した。

（4）地方公共団体情報システム機構（J-LIS）と連携した、地方自治体へのDAEDALUSアラートの提供については継続し実施を行い、この成果展開に対し産学官連携功労者表彰 総務大臣賞を受賞した。

2．セキュリティ基盤研究室の活動

（1）パーソナルデータの利活用に対応した、暗号化したまま演算が行える「準同型暗号」の演算を制御する方式を提案し、コンピュータセキュリティシンポジウム（CSS）2016において、最優秀論文賞を受賞した。また、モジュラー設計を可能にしつ

図1　Interop Tokyo 2016におけるプレゼン

つ、安全で利便性の高い機能性暗号技術を実現する群構造維持暗号系の研究について、市村学術賞（功績賞）を受賞した。

（2）実用化・国際標準化が急務となっている格子暗号の安全性評価において、より正確な評価手法を提案し、暗号分野でトップレベルの国際会議Eurocrypt 2016にて採録された。また、格子暗号の安全性評価の国際評価コンテストにおいて世界記録を更新した。

（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、科学技術振興機構のCRESTプログラム「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」に「複数組織データ利活用を促進するプライバシー保護データマイニング」の提案が採択され研究代表としてプロジェクトに着手した。また平成28年度は、総務省、文部科学省、経済産業省の３省による人工知能（AI）研究開発のための「人工知能技術戦略会議」が立ち上げられ、専門家として参画した。

３．研究所共通の活動

（1）Interop Tokyo 2016への出展

平成28年６月８～10日に幕張メッセで開催されたInterop Tokyo 2016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逸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改のネットワーク機器との連携を含む機能についてデモンストレーションとプレゼンにて紹介した（図１）。

図2　「NICTサイバーセキュリティシンポジウム 2017」の模様

（2）「NICTサイバーセキュリティシンポジウム 2017」において当研究所の研究成果を報告

平成29年３月10日「NICTサイバーセキュリティシンポジウム2017」にて、当研究所が今中長期計画において実施する研究開発課題について紹介した。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横浜国立大学 吉岡准教授及び筑波大学 佐久間教授から最先端の研究動向の講演を頂くとともに、今年から開始したサイバーセキュリティ人材育成について園田センター長が取組状況について講演を行った。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150名を超える方々の参加があった（図２）。