3.4　ネットワークセキュリティ研究所

研究所長　　平　和昌

【研究所概要】

情報通信は、我々の知的な活動や経済的な活動を支える基盤であり、現代ではインターネットがその中核的な役割を果たしている。その一方で、我々は情報セキュリティに関係する不安を抱えてインターネットを利用している。企業などのネットワークシステムに対する不正侵入や、スマートフォンをねらったウイルスによる犯罪などは日を追うごとに増加しており、ネットワーク環境におけるセキュリティ対策なくしては安心・安全に情報通信サービスを受けられない状況になっている。

ネットワークセキュリティ研究所では、誰もが安心・安全にネットワークを利用できる技術の開発を目標として、以下に示すような理論と実践を融合させたセキュリティ技術の研究開発を実施している。

① サイバーセキュリティ技術の研究開発

高度化・巧妙化が進むサイバー攻撃に対し能動的に対抗するために、サイバー攻撃の世界的な観測網を構築して、サイバー攻撃の観測、分析、対策、予防の研究開発を行う。また、NICT の中立性を活かして、収集したサイバー攻撃に関連する情報の安全な利活用を促進するための研究開発を行う。これらの研究開発は、主としてサイバーセキュリティ研究室が実施する。

② セキュリティアーキテクチャ技術の研究開発

ネットワークを用いたサービスを受ける際、それぞれの状況に最適なセキュリティ環境を自動的に構築し、利活用できる技術の研究開発を行う。また、今後更なる発展が見込まれるモバイル機器やクラウドサービスにおいて新たに必要となるセキュリティ技術の研究開発を行う。これらの研究開発は、主としてセキュリティアーキテクチャ研究室が実施する。

③ セキュリティ基盤技術の研究開発

量子 ICT 技術と現代暗号技術を活用し、情報理論的に安全なネットワークを構築する技術の研究開発を行う。また、長期にわたって利用が可能となる暗号技術や、最先端の解読技術を用いた暗号の安全性の評価を行う。これらの研究開発は、主としてセキュリティ基盤研究室が実施する。

【主な記事】

ネットワークセキュリティ研究所における平成 26 年度の主なトピックスを以下に示す。なお、(1) から (3) 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

- ダークネット観測規模を約 28 万アドレスに拡大するとともに、サイバーセキュリティ分野における国際連携の一環として、同センサの欧州機関等への設置を展開
- 能動的サイバー攻撃観測網の構築に向け、複数組織に分散配置した仮想センサ群と、センタ側に設置した各種センサの動的スイッチングを組み合わせた観測技術「GHOST Sensor」の中規模実験運用を実施
- ドライブ・バイ・ダウンロード攻撃対策フレームワークにおいて、Web ブラウザにプラグインする形式のセンサをユーザに展開し、実証実験を実施
- DNS amp 攻撃に関して、ダークネットと DNS ハニーポットを連動させるシステムの提案と評価を実施
- DAEDALUS にプライベートアドレス観測・可視化機能を追加するとともに、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 アラート提供、総務省 JASPER プロジェクトと連携した ASEAN 諸国への DAEDALUS アラート提供を実施

(2) セキュリティアーキテクチャ研究室の活動

- 個々の Android のアプリケーションが有するリスクの定量評価手法を提案し実装
- IETF（The Internet Engineering Task Force）において、セキュリティ情報に対する構造の国際標準化を先導し、RFC 7203 として発行が決定
- PUF（Physical Unclonable Function：物理的複製困難関数）を利用することにより物理的な安全性が確

保されている RFID 認証プロトコルを構築し、100 台の FPGA を用いて SRAM PUF の挙動を分析
- 暗号プロトコルの安全性評価について、あらゆる実行環境における安全性評価が可能な形式手法を確立し、様々な攻撃の過程を可視化するシステムを試作
- 暗号プロトコル評価技術コンソーシアム（CELLOS）と連携し、暗号プロトコルの安全性情報を迅速に発信

（3） セキュリティ基盤研究室の活動

- 量子セキュリティネットワーク構築に向けて、量子ネットワーク上でパスワード認証機能付き秘密分散機能を備えたセキュアな外部ストレージシステムを試作
- 格子理論に基づくプロキシ再暗号化技術を活用して、暗号化したまま暗号強度が変更でき、さらに暗号化したまま加算と乗算が可能な準同型暗号方式「SPHERE」を世界で初めて開発
- 高度道路交通システム（ITS）におけるビッグデータの利活用を促進させる基盤技術として、セキュアストレージシステム「PRINCESS」を応用し、クラウドを介したセキュアな自動車情報共有システムを試作
- パーソナルデータに関するプライバシー問題の解決に向けた研究開発を開始
- 公開鍵の安全性検証システム「XPIA」を一般財団法人日本情報経済社会推進協会（JIPDEC）に技術移転

（4） 研究所共通の活動

- 「情報セキュリティシンポジウム道後 2015」において当研究所企画の講演セッションを開催
  愛媛県松山市にて 3 月 12・13 日に開催された「情報セキュリティシンポジウム道後 2015」は、『「ネクスト ICT」に求められる安心・安全』をテーマに掲げ、国の情報セキュリティ政策をはじめ、技術面、法制度面、対策事例など様々な側面から講演やパネル討論が行われた。このシンポジウムのプログラム検討に当研究所も加わり、多くの関係者が集まる同シンポジウムにおいて当研究所の研究成果を紹介するセッションを企画し、招待講演を含む 4 件の講演及び NICTER/DAEDALUS/NIRVANA 改のデモ展示を行った。招待講演として（株）FFRI 代表取締役社長の鵜飼裕司氏から、IoT におけるセキュリティの課題に関するこれまでの各種の国際会議やセキュリティイベントでの発表事例をご紹介いただきながら、引き続き研究開発が重要性である旨の講演をいただいた。一方、当研究所からは 3 名の研究者がこれまでの研究活動の成果を中心に講演した。当日は、民間企業や大学、官公庁等から情報セキュリティ関係に携わる方々を中心に 300 名を越える関係者にご参加をいただいた（図 1）。
- Interop Tokyo 2014 への出展
  平成 26 年 6 月 11～ 13 日に幕張メッセで開催された Interop Tokyo 2014 において、インシデント分析センター「NICTER」及び対サイバー攻撃アラートシステム「DAEDALUS」、ネットワークリアルタイム可視化システム「NIRVANA」、サイバー攻撃統合分析プラットフォーム「NIRVANA 改」を出展し、それぞれデモンストレーションを行った（図 2）。

図 1　「情報セキュリティシンポジウム道後 2015」における講演セッションの模様

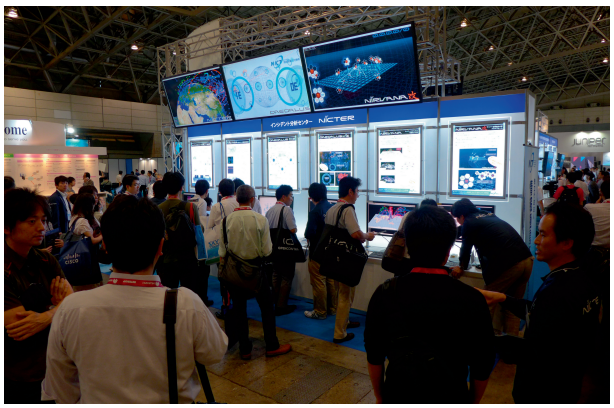

図 2　Interop Tokyo 2014 における出展模様