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 27 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で約 30 万アドレスを達成するとともに、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、初の米国、欧州へのセンサ設置を実現。
- 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」を WIDE プロジェクトの大規模ダークネットにて長期運用試験を実施。
- 総務省の PRACTICE プロジェクト（国際連携によるサイバー攻撃予知・即応プロジェクト）と連携し、リフレクション型 DoS 攻撃（DRDoS）の攻撃指令を検知可能な「DRDoS ハニーポット」を運用し、アラートを発する仕組みを開発。
- 地方公共団体情報システム機構（J-LIS）と連携し、地方自治体への DAEDALUS アラートを提供。また、NIRVANA をベースにしたセキュリティサービスが重要インフラで稼動。

(2)　セキュリティアーキテクチャ研究室の活動

- 知識ベースを活用し、ネットワークシステム上に存在する IT 資産の脆弱性を監視し、警告を自動生成する技術・プロトタイプを構築。複数の地方公共団体の情報システムの上で本システムの有効性評価実験を開始。
- 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 の挙動を分析し、構築した認証プロトコルの回路規模及び演算時間を実装により検証。

- 標準化されている 50 個以上の暗号プロトコルの安全性評価結果（脆弱性の有無）を集約し、技術的に信頼性のある情報の参照をつけた「AKE Protocol Zoo」を整備して NICT の Web サイトにて公開。

（3） セキュリティ基盤研究室の活動

- ビッグデータ解析で多用されているロジスティック回帰分析に対して、データを暗号化したままロジスティック回帰計算を可能にする技術を開発し、暗号化された 1 億件のデータを 30 分以内で複数グループに分類できることをシミュレーションで確認。
- 路車間通信においてプライバシー保護を実現する軽量グループ署名を提案し、シミュレーション解析を実施。同じ車でも異なる期間に作成されたものであればリンク不可能となる「期間に依存した匿名性」をもつ軽量グループ署名を提案。
- 今後のプライバシーに関する諸問題を検討する場として、有識者を交えた「プライバシー検討ワーキンググループ」を機構内に立ち上げ、適切な同意取得やプライバシーリスク評価に関する議論を開始。

（4） 研究所共通の活動

- 「NICT サイバーセキュリティシンポジウム 2016」において当研究所の研究成果を報告

  平成 28 年 3 月 9 日に開催された「NICT サイバーセキュリティシンポジウム 2016」にて、当研究所が第 3 期中長期計画において実施してきたネットワークセキュリティ技術の研究開発の成果をまとめて報告するとともに、第 4 期中長期計画において実施予定の研究開発課題について紹介した。このシンポジウムでは、3 人の研究室長からそれぞれの研究室で実施してきた技術に関して「研究開発成果と今後の課題」と題したプレゼンテーションを行った後、特別講演として、明治大学総合数理学部先端メディアサイエンス学科の菊池浩明教授から「サイバーセキュリティ分野における研究開発への期待」と題して、サイバーセキュリティ分野の現状と課題や「NICT への期待」と題する提言をいただいた。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連業務に携わる方々を中心に 150 名を超える方々にご参加をいただいた（図 1 ）。
- Interop Tokyo 2015 への出展

  平成 27 年 6 月 10 ～ 12 日に幕張メッセで開催された Interop Tokyo 2015 において、インシデント分析センタ「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、デモンストレーションを行った（図 2）。

図 1　NICT サイバーセキュリティシンポジウム 2016 の模様

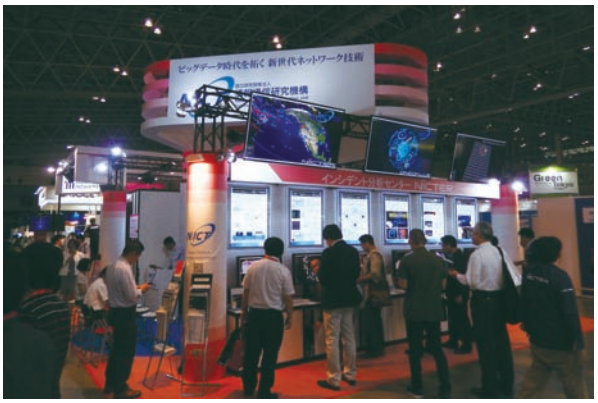

図 2　Interop Tokyo 2015 における出展模様