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、スマートフォンを狙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､今後さら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 24 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

- ブラックホールセンサ（無応答型センサ）とハイインタラクションハニーポット（高対話型センサ）の動的切替を実現するプロトタイプシステムを開発
- ドライブ・バイ・ダウンロード攻撃に対抗する技術として、複数種の Web ブラウザに対応したプラグイン型センサ等のプロトタイプを開発
- 標的型攻撃対策の技術として､組織内の異常通信及び組織内から組織外への異常通信を検出する分析エンジンのプロトタイプを開発
- IPv6 におけるセキュリティを検証するため、攻撃シナリオとそれらに対する防御策をまとめた報告書を作成
- 対サイバー攻撃アラートシステム「DAEDALUS」のアラート情報を外部利用する仕組みを整備し、国内企業が商用アラートサービスを開始

(2)　セキュリティアーキテクチャ研究室の活動

- セキュリティリスクを分析するセキュリティ知識ベース・分析エンジン「REGISTA」を構築
- 匿名認証と部分秘匿認証を同時に行える認証方式の高速化を行い、暗号ライブラリとして実装
- 省リソースデバイス向けの認証・プライバシ保護プロトコルを確立
- 大量のデバイスが接続する新世代ネットワークにおけるスケーラブルな認証方式を確立

（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の構築に向けた認証機能付き秘密分散方式の機能拡張と安全性検証を実施
- 格子暗号の安全性の根拠である最短ベクトル問題において 825 次元の問題を解き、世界記録を達成
- クラウド上で軽量暗号を高速復号処理する実装法を世界で初めて開発
- 次世代の公開鍵暗号であるペアリング暗号の安全性の根拠となる離散対数問題において 923 ビットの問題を解き、世界記録を達成
- 電子政府推奨暗号リストの改定に伴う暗号アルゴリズムの安全性評価を実施し、本年度のリスト改定に貢献

（4） 研究所共通の活動

- NICT 情報通信セキュリティシンポジウム 2013 の開催（図 1）
  平成 25 年 2 月 14 日に品川フロントビルにおいて「NICT 情報通信セキュリティシンポジウム 2013」を開催した。招待講演として、KDDI 研究所の田中執行役員からスマートフォンアプリの安全性評価やプライバシ保護における課題に関する講演を、また、九州大学の高木教授からペアリング暗号やポスト量子暗号等の次世代公開鍵暗号の特徴や課題に関する講演をいただいた。一方、当研究所からは、この 1 年間の研究活動の成果を中心に 4 名が講演した。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 170 名を超える参加をいただいた。
- Interop Tokyo 2012 への出展（図 2）
  平成 24 年 6 月 13 ～ 15 日に幕張メッセで開催された Interop Tokyo 2012 において、インシデント分析センター「nicter」及び「DAEDALUS」、「Risk Visualizer」を出展し、それぞれデモンストレーションを行った。
- 次世代安心・安全 ICT フォーラムにおける活動
  平成 24 年 6 月 19 日に開催した次世代安心・安全 ICT フォーラム総会における特別記念講演として、東京大学の松浦幹太准教授に「安心･安全のための暗号と認証技術の現状と今後」と題する講演をいただいた。また、平成 24 年 12 月 25 日に開催した企画部会・センシング技術部会合同会合において、当研究所から「災害時における情報通信セキュリティ技術」と題した講演を行い、災害時の重要情報を保証するセキュリティ技術等を紹介した。

図 1　NICT 情報通信セキュリティシンポジウム 2013 の会場模様

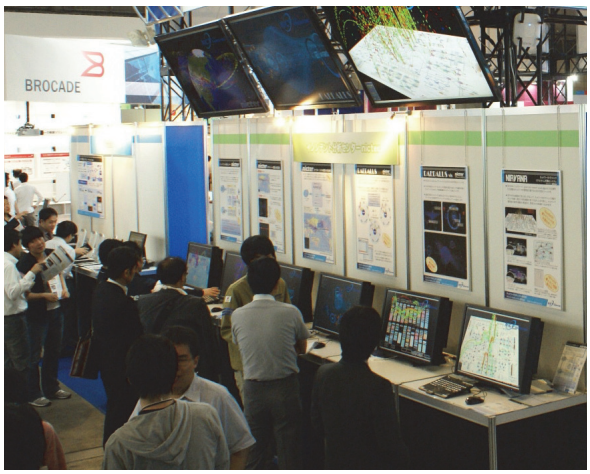

図 2　Interop Tokyo 2012 における出展模様