3.4　ネットワークセキュリティ研究所

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 25 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を参照されたい。

(1)　サイバーセキュリティ研究室の活動

- 無応答型センサと高対話型センサ等の高速な動的切替え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および観測情報の集約を行うセンタ機能のプロトタイプを開発
- DNS amp 攻撃に対して、ダークネットと DNS ハニーポットのマルチモーダル分析を実施し、攻撃の前兆を観測
- 地方自治情報センター（LASDEC）と連携し、地方自治体へ DAEDALUS アラートの提供を開始
- DAEDALUS において、組織内のプライベート IP アドレス観測・分析機能を開発し、技術移転を完了
- サイバー攻撃統合分析プラットフォーム「NIRVANA 改」のプロトタイプを開発し、Interop Tokyo 2013 へ出展

(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」を用いて、企業ネットワークへのリモートアクセスのリスクを評価
- スマートフォンにインストールしているアプリケーションのリスクを即座に把握できる機能を

REGISTA に追加
- サーバ上の情報を暗号化したまま検索が可能な方式の設計において、プライバシ保護要件を緩和することにより、検索に必要なインデックスファイルの大きさを 1/7 に削減することを実現
- 「暗号プロトコル評価技術コンソーシアム（CELLOS）」を設立し、活動を開始

（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パスワード認証機能付き秘密分散方式の機能拡張と世界初の実装を実施
- 格子理論に基づく新たなプロキシ再暗号化方式を設計し、安全性を評価
- リソースの限られたデバイスに実装可能な「軽量暗号」の評価基盤の構築を開始
- 機密レベルに応じた処理が可能なセキュアストレージシステム PRINCESS を開発
- 離散対数問題をベースとした公開鍵暗号の安全性を評価
- SSL サーバ証明書に使用されている公開鍵の脆弱性を検証するシステム「XPIA（エクスピア）」を構築

（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 2014 の開催

  平成 26 年 2 月 13 日にコクヨホールにおいて、「NICT 情報通信セキュリティシンポジウム 2014」を開催した（図 1）。今回で 8 回目を迎える本シンポジウムは、政府が設定する「情報セキュリティ月間」である 2 月に毎年開催している。本年度のシンポジウムでは「情報セキュリティ技術の現状と今後」と題して、ネットワークセキュリティを取り巻く現状や課題を共有するとともに、当研究所の研究活動や成果を周知できた。招待講演として、中央大学の今井秀樹教授から暗号プロトコルに関するこれまでの研究動向について、東京工科大学の手塚悟教授から暗号プロトコル評価技術コンソーシアムの活動の紹介、カリフォルニア大学の Christopher Kruegel 教授から Web コンテンツ上に存在する悪意のあるコードの分析と検出に関する研究について、ソニー（株）の五十部孝典氏より RC4 の脆弱性とそれを用いた SSL/TLS への攻撃について、それぞれご講演をいただいた。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各研究室長が講演した。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 160 名を超えるご参加をいただいた。
- Interop Tokyo 2013 への出展

  平成 25 年 6 月 12 日から 14 日に幕張メッセで開催された Interop Tokyo 2013 において、インシデント分析センタ「nicter」およびサイバー攻撃統合分析プラットフォーム「NIRVANA 改」、セキュリティ知識ベース・分析エンジン「REGISTA」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　NICT 情報通信セキュリティシンポジウム 2014 の会場模様

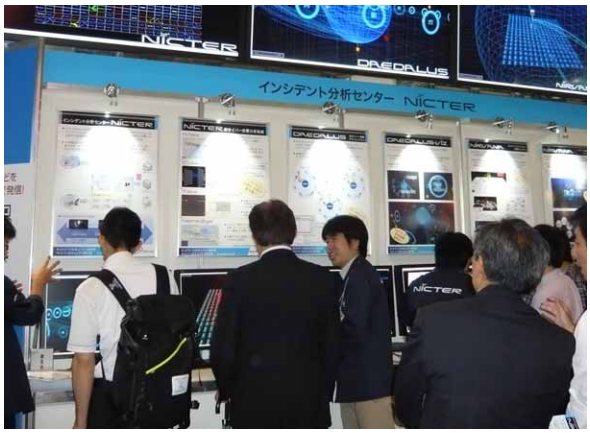

図 2　Interop Tokyo 2013 における出展模様