3.4.2　ネットワークセキュリティ研究所　セキュリティアーキテクチャ研究室

室長（事務取扱）　平　和昌　ほか５名

ネットワークの安全性を最適にする技術を構築し、将来のネットワークにおける安全性の確保に貢献

【概　要】

本研究室では、進化が著しいネットワークの安全性を最適に確立するための、リスク評価、認証・プライバシー保護、その安全性評価のための技術を構築し、将来のネットワークにおけるセキュリティ確保の実現に貢献することを目指しており、今年度は以下の３つの研究テーマを中心に研究開発を行った。

●知識ベースを活用したセキュリティリスク分析・リスク評価技術

知識ベースを活用することにより、スマートフォン等のアプリケーション利用におけるセキュリティリスクを分析する技術の開発や、情報システムにおけるIT資産に存在するセキュリティ面の脆弱性を管理するシステムの開発、組織間でセキュリティ情報を交換する際に必要となる技術などを研究開発

●省リソースデバイス向け認証・プライバシー保護技術

IoT時代における大規模ネットワーク上で多種多様の利用が想定される「RFIDタグ」を省リソースデバイスの対象として、認証とプライバシー保護の両立に向けたセキュリティ技術などを研究開発

●暗号プロトコルの安全性評価技術

ネットワークを利用した通信の安全を保つ目的から、暗号を利用する通信の手順を規定した「暗号プロトコル」について、理論的に網羅性をもった安全性評価技術を研究開発するとともに、代表的な暗号プロトコルの安全性情報を発信

【平成27年度の成果】

（１）　知識ベースを活用したセキュリティリスク分析・リスク評価技術

ネットワークを用いたサービスを一般ユーザが利用する際、当該サービスの利用によりユーザが直面するセキュリティリスクを分析し、ユーザの端末にその分析結果及び推奨される対策方法を提示するシステムの構築を行っている。今年度は、以下の３項目を中心に研究開発を実施した。

①スマートフォン向けのセキュリティリスク評価技術について、昨年度に構築したAndroidアプリケーション（以下、Androidアプリ）のリスク分析フレームワークにおける「脆弱性」の評価に対して、Androidアプリのコーディング上の不備を発見することによりリスクを提示する機能を実装した（図1）。昨年度から行ってきた同フレームワークの一連の開発により、Androidアプリに対する「脅威」及び「脆弱性」の両面からリスクを評価できる技術を確立した。

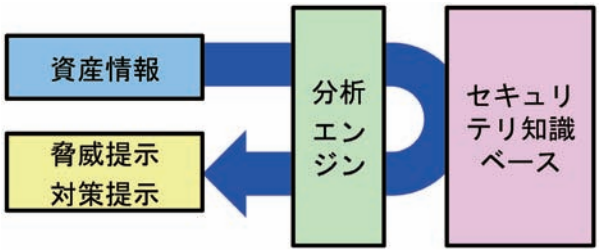

図１　知識ベースを活用したセキュリティリスク分析のフレームワーク

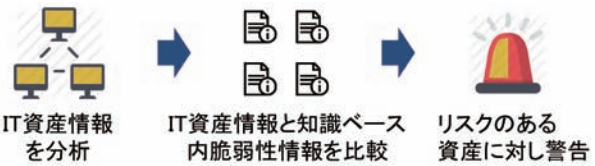

図２　情報システム内のIT資産に存在する脆弱生管理システムの構成

②知識ベースを活用して、情報システムにおけるIT資産に存在するセキュリティ面の脆弱性を管理するシステムのプロトタイプを構築した（図2）。このプロトタイプでは、ネットワーク上のIT資産に関する情報を自動的に収集し、それらをID化する技術及びそのIDを用いて知識ベース内の脆弱性情報を検索して関連する脆弱性情報を管理者にリアルタイムで通知・警告する機能を有する。本システムの構築検討にあたっては、複数の地方公共団体に対して脆弱性管理の実態をヒアリングし、本技術へのニーズを把握した。本プロトタイプは、いくつかの地方公共団体の情報システム上にインストールされ、実証実験を開始した。

③各組織で得られたリスク分析結果など、組織間で何らかのセキュリティ情報を交換する際、その情報構造を合意しておく必要がある。これまで当研究室では、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、昨年度に RFC 7203 として発行されることが決まったが、本年度は当該 RFC に対するツールを構築し、情報の交換に関する評価を実施した。

（2） 省リソースデバイス向け認証・プライバシー保護技術

IoT 時代における大規模ネットワーク上で多種多様の利用が想定される「RFID タグ」を省リソースデバイスの対象として、RFID タグの利用における認証・プライバシー保護技術の研究開発を実施している。今年度は、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た。また、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得た（図 3）。さらに、RFID のセキュアな通信環境を評価するため、無線通信環境下での暗号プロトコル開発に有益となる RFID 暗号評価ボードを試作開発した。今後、当該分野における内外のハードウェア実装開発者と連携し、当該ボードを次世代 RFID 開発に供していく。

図 3　100 台の FPGA を用いた RFID 認証プロトコルの実装実験

（3） 暗号プロトコルの安全性評価技術

ネットワークを利用した通信の安全を保つ目的から、暗号を利用する通信の手順を規定した「暗号プロトコル」の安全性を評価する手法の研究開発を実施している。今年度は、以下の 3 項目を中心に研究開発を実施した。

①認証プロトコルをはじめとする 58 個の標準化された暗号プロトコルについて、脆弱性の有無を評価し、それらを使用する際の問題点や技術的に信頼性のある情報を付した上で集約した「AKE Protocol Zoo」を整備し、機構ホームページ上の「暗号プロトコル評価ポータルサイト（CPVP）」において公開（図 4）し、併せて報道発表した。その結果、1 面記事を含む新聞 4 紙への掲載に加え、数多くの Web サイトにも掲載された。ポータルサイトへのアクセスは、発表後 1 週間で約 9,200 アクセス、3 月末までに約 35,000 アクセスに達した。

図 4　標準暗号プロトコルの安全性評価結果をリスト化し NICT Web サイトにて公開

②インターネットにおける代表的な暗号プロトコルである SSL/TLS（Secure Sockets Layer/Transport Layer Security）において認められる新たな攻撃に対する安全性の評価手法として、今年度に発見された Logjam 攻撃の自動検出を可能とする形式手法を確立した。当該手法を用いることで SSL/TLS の最新バージョンである TLS1.2 で脆弱性を抽出した。その結果に基づき、TLS1.2 のプロトコルへの改良案を提示し、Logjam 攻撃への脆弱性が解消されていることを確認した。

図 5　暗号プロトコル評価技術コンソーシアム（CELLOS）による安全性情報の発信
（出典：CELLOS ホームページ）

③ Logjam 攻撃を始め、今年度、SSL/TLS において認められた新たな攻撃について、脆弱性の技術的正しさと実システムへの影響を評価し、暗号プロトコル評価技術コンソーシアム（CELLOS）に評価結果を提供し、CELLOS の迅速な技術速報の公開に寄与した（図 5）。これにより、暗号を活用したネットワーク利用の安全性向上に技術的な側面から貢献した。