2-2　セキュリティアーキテクチャ技術の研究開発概要

平　和昌

NICT では、平成 23 年度から 27 年度に至る第 3 期中長期目標期間において、次世代のネットワークをセキュアに構築するためのセキュリティアーキテクチャ技術の研究開発を実施した。本稿では、当該研究開発の概要をまとめる。

1　まえがき

情報通信ネットワークを誰もが安心・安全に利用でき、かつそれを支えるセキュリティ技術の存在を利用者に意識させない世の中を実現するために、ネットワーク自身のセキュリティを高め、攻撃に強いネットワークの実現を目指した研究開発を中長期的な視点に立って実施する必要がある。そのなかでも、様々な条件下で存在するネットワーク機器やあらゆるユーザのセキュリティを確保するために、過不足のないセキュリティ対策を適宜適切に提供するなど、新たなセキュリティ技術を導入したネットワークアーキテクチャを構築していくことが重要である。

NICT では、平成 23 年度から 27 年度に至る第 3 期中長期目標期間において、ネットワークの安全性を確立するためのリスク評価技術や、IoT 等で利用される省リソースデバイスにおける認証・プライバシー保護技術、ネットワークを利用した通信の安全を保つ暗号プロトコルの安全性評価技術など、次世代のネットワークをセキュアに構築するためのセキュリティアーキテクチャ技術の研究開発を実施した。本稿では、当該研究開発の概要を述べる。それらは、大きく以下の 4 つの研究開発課題に集約できる。

- セキュリティ知識ベース・分析エンジンの研究開発
  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の研究開発などを実施
- 大規模認証・プライバシー保護技術の研究開発
  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の研究開発などを実施
- 新世代ネットワーク向けセキュリティアーキテクチャの研究開発
  10 兆個規模のデバイスがネットワークに接続され、莫大なユーザ数が想定される「新世代ネットワーク」におけるセキュリティ確保やプライバシー保護の観点での研究開発を実施
- 暗号プロトコルの安全性評価技術の研究開発
  ネットワークを利用した通信の安全性確保を目的として、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の発信などを実施

2　各研究開発課題の概要

上述の各研究開発課題で実施した内容及び得られた成果について、以下に概要を示す。なお、各研究開発課題の詳細については、**6** の各節を参照されたい。

(1) セキュリティ知識ベース・分析エンジンの研究開発

本研究開発では、ネットワークを通じてサービスを受ける際に被るリスクを分析して自動的に提示する技術を構築することを目的としている。その際、リスク等を判断する根拠となる情報を蓄積する仕組みとして「知識ベース」を用いる。

まず、様々なセキュリティ情報を蓄積し、あらゆるセキュリティ対策に活用していくための「セキュリティ知識ベース」を構築するために、セキュリティ情報収集／交換のための形式記述手法の検討を実施した。また、セキュリティリスクを分析する「セキュリティ分析エンジン」を構築するため、分析手法の検討を実施した。このセキュリティ分析エンジンが行う技術的な分析に対して、システム利用者が要求するセキュリティ要件を明示して合意させるため、セキュリティ

SLA（Service Level Agreement：サービスレベル合意書）を定義するが、当該セキュリティ要件の記述方法や、システム利用者とサービス提供者の間でセキュリティレベルを合意するためのプロトコルを構築した。

本研究開発では、近年、社会的にも大きな問題となっているスマートフォンアプリケーションを利用する際の脅威に対して、リスクを自動的に評価してユーザに提示する仕組みを構築することに注力してきた。Android アプリケーション（以下、Android アプリ）を対象とし、リスク分析フレームワークにおける「脅威」及び「脆弱性」の評価に対して、独自の手法を提案して実装した。「脅威」の評価では、ある Android アプリがマルウェアである可能性を統計及び機械学習に基づき定量化するが、その際、インターネット上から取得した Android アプリのコンテクストに応じて判定を行った。「脆弱性」の評価では、コーディングの不備を発見することによりリスクを表示した。Android アプリのリスク分析に資するため、約 20 万件の Android アプリの分析結果及びメタ情報をセキュリティ知識ベースに格納した。格納する際の情報構造についても定義し評価した。

これらのフレームワークにおけるインシデント情報の交換に必要なスキーマ技術について、IETF（The Internet Engineering Task Force）において国際標準化を先導し、RFC 7203 として発行された。本技術を用いたエンタープライズネットワークの脆弱性アラートの自動交換ツールについて、プロトタイプを構築した。

本研究開発においては、知識ベースを活用して情報システムにおける IT 資産に存在する脆弱性を管理するシステムのプロトタイプを構築した。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。本プロトタイプ構築の検討においては、地方公共団体情報システム機構（J-LIS）のご協力のもと、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上で構築の検討を行った。

(2) 大規模認証・プライバシー保護技術の研究開発

今後ますます進展するであろう IoT 時代においては、センサなどのリソースが少ないデバイスからも多くのデータが発信されることになる。あらゆるものに付随して社会にばらまかれていくことにより、大規模ネットワーク上で多数の利用が想定される「RFID タグ」は、現在はリソースの制約から通信に暗号が用いられていないため、認証やプライバシー等の観点で課題が大きい。本研究開発では、RFID タグ等の省リソース向けの安全な暗号プロトコルを構築し、通信の安全性を確保するとともに、認証やプライバシーの課題も克服することを目指した。

まず、RFID タグにおけるセキュリティ・プライバシー要件の理論的な枠組みを構築した。証明可能安全性を有する RFID 認証プロトコルを構築するとともに、安全に所有権の譲渡を行うことが可能なプロトコルを開発した。その後、RFID タグ利用における認証・プライバシー保護技術において、高速に複数のタグへの読み込みが行われたことに対して証拠を残すプロトコルの構築を行い、中間者攻撃に対する高い安全性を証明可能とするプロトコルを提案した。

また、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。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。暗号プロトコルと PUF を融合することにより、省リソース端末における物理的な安全性を確保する仕組みを確立するため、安全性証明を行う上で必要な PUF に対する様々な安全性要件を定義した。

プライバシー保護型の RFID 認証プロトコルを実際の RFID タグの製造プロセスに載せることにより、回路規模や動作性能、通信可能距離等、実用面での性能評価を委託研究により行った。RFID タグ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 タグ開発に供していく。

一方、大規模プラットフォームにおける様々なアプリケーション・サービスに求められる異なるセキュリティ要件・異なるプライバシー要件に対し、要件ごとに柔軟な実現を可能とする暗号基盤技術も開発した。これまでにないフレームワークや概念を提唱し、それらを実現する具体的な基盤技術を提案した。また、プライバシー保護を実現する技術として、双線形写像を前提とした暗号技術は有力なツールであるが、あるタイプの双線形写像上を前提とした暗号方式群については、その安全性が危ぶまれ始めており、当該方式群を、より安全な環境で利用可能な暗号方式群へと変換する手法を提案した。この提案は、既存方式の救済という意義のほか、新しい方式を創出する際にも効率的な方式を構成するための指標とすることができる。

(3) 新世代ネットワーク向けセキュリティアーキテクチャの研究開発

新世代ネットワークにおいては、10 兆個規模のデ

バイスがネットワークに接続されるといわれており、莫大なユーザ数が想定される。このような状況では、ユーザ追加時の鍵発行のみならず、ユーザの削除や鍵紛失に対応するための鍵失効機能も必要になる。本研究開発では、新世代ネットワークにおけるセキュリティ確保やプライバシー保護に資する技術の構築を実施した。

スケーラビリティの観点では、利用しないデバイスの認証の無効化処理について、デバイス数に関して従来の log オーダーの時間で処理が可能な「Revocable ID ベース署名」方式を開発し、新世代ネットワークでの実装に向けたライブラリ実装を行った。上記の成果は、特に使えなくなるデバイスが多数発生する災害発生時に、認証に必要な運用コストを低下させる効果が大きい技術である。一方、暗号をシステムに組み込んで長期間使用する際、システム離脱時・鍵紛失時等に対応するための鍵失効機能が必要であるが、これまで考慮されていない安全性を達成する鍵失効機能付き ID ベース暗号を提案した。また、暗号文長が階層の深さに依存せず、かつ内部攻撃者を考慮した階層的鍵失効可能 ID ベース暗号を提案した。さらに、ユーザ削除時に公開するトークンサイズが削除ユーザ数に非依存なグループ署名方式を提案した。

プライバシー保護の観点では、暗号技術（ID ベース暗号／グループ署名）と通信技術（Tor）を組み合わせることで、サービスプロバイダがユーザを匿名で認証しつつサービス内容を暗号化することが可能なシステムを提案した。また、プライバシー保護と情報利活用との両立に向けて、購入履歴等のログの漏洩時には一切の個人情報が漏れることなく、一方で万が一の事態が起こった場合におけるユーザの追跡時には当該ユーザを特定することが可能なシステムを提案した。さらに、中間者と呼ばれるエンティティを導入することで、既存方式と比較して非常に効率的な匿名データ収集方式を提案した。本方式により、中間者には暗号化されたデータがある範囲に入っていることのみの検証を許すため、復号することなしに暗号化データの整理が可能となる。さらに、利便性を失うことなく強い安全性を持つ暗号システムの構築を目指して、時間に依存した匿名性を利用した路車間通信システムを提案した。その際、廃車にする場合や鍵漏洩なども想定して署名鍵の失効も実現した。また、検索トークンの漏洩対策としてトークンを削除可能な検索機能暗号を提案した。

(4) 暗号プロトコルの安全性評価技術の研究開発

近年、SSL（Secure Sockets Layer）/TLS（Transport Layer Security）などの暗号を用いた通信プロトコルの深刻な脆弱性がいくつも発見され、SSL/TLS などを利用してインターネットサービスを提供する組織ではその対応に苦慮している。このような状況から、現在使われている通信プロトコルにおいても、今後更に脆弱性が発見される可能性がある。本研究開発では、暗号を用いた通信プロトコルにおける脆弱性の評価と、その結果の社会への展開を実施した。

ISO/IEC 11770 -2,3 において規定されている「鍵管理プロトコル」におけるプロトコル上の脆弱性と修正方法を発見し、ISO/IEC に対して修正提案を行った。その結果、ISO/IEC で規定する鍵管理プロトコルにおける安全性定義の修正を行う議論が開始された。また、暗号プロトコルに対する理論的に網羅性をもった安全性評価手法として、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た。当該手法を用いて、著名な国際会議で他者が提案した新規の暗号プロトコルを評価したところ、国際会議への提案時には発見できていなかった攻撃を検出できた。さらに、形式手法による暗号プロトコルの安全性評価の過程を可視化するシステムを試作し、安全性評価における理論的な網羅性及び攻撃の詳細、脆弱性の直観的理解を可能とした。

暗号プロトコルの安全性評価について、国際的な議論を行って評価結果を社会還元するための「暗号プロトコル評価技術コンソーシアム（CELLOS）」の設立の発起人となり、さらに、事務局を担うことによりコンソーシアム活動に貢献した。また、複数の暗号プロトコル評価ツールを使い、多角的な暗号プロトコル評価を行う「暗号プロトコル評価ポータルシステム」を開発し、CELLOS に提供した。さらに、SSL/TLS において新たに発見された脆弱性の技術的正しさと実システムへの影響を評価し CELLOS に評価結果を入力することで、CELLOS が行う安全性情報の迅速な発信及び通信システムにおける暗号の安全な利用の促進に貢献した。

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、平成 27 年 10 月 NICT 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、朝日新聞出版の「dot.」や TECH Ascii、Impress Watch など、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、平成 28 年 3 月末までに約 35,000 アクセスに達した。

(5) 組織間機密通信のための公開鍵システムの研究開発

組織間の通信における秘匿性確保において、送信先

組織での復号権限を必要に応じて柔軟に変更できる「組織暗号」の検討を委託研究により実施した。組織暗号の具体的な利用シーンを想定して運用面等も含めた実利用に向けた構成方法の検討を進め、複数の方法を提案した。また、組織暗号を利用したシステムを地方自治体等で運用する際の課題を抽出するため、複数の自治体で説明会やシステムの技術紹介等を行った。さらに、そのうちのいくつかの自治体において実際に実証実験を実施することにより、技術面での課題のみならず、ユーザインターフェースや操作性、マニュアルの記述等、運用面を含め実導入に向けた課題の抽出を行った。また、組織暗号の適切かつ有効な実装のための実践規範（ガイドライン）を作成した。

3　むすび

本稿では、第３期中長期目標期間において実施してきた「セキュリティアーキテクチャ技術の研究開発」の概要を述べた。現在のネットワークは、ユーザに対する性善説を基盤として構築されているアーキテクチャであることから、特にセキュリティ確保やプライバシー保護の観点においては、対策が後追いになっていることが否めない。我々は、リスク評価技術や暗号プロトコルの安全性評価技術など、現状のネットワークのセキュリティを確保するための検討・提案を行うと同時に、今後のIoT時代におけるプライバシー保護等を確保する技術を検討・提案してきた。NICTでは、平成28年度より開始された第４期中長期目標期間において、本稿で述べた成果を更に発展させ、セキュリティ自動対策技術の確立やIoTシステムのセキュリティ・プライバシー保護技術の構築に向けて研究開発を推進していく所存である。

謝辞

本プロジェクトにおいて、研究及び研究室運営に真摯に取り組んでいただいた研究員及び技術員各位、金岡晃教授（東邦大学）、側高孝治様（日本電気株式会社）に敬意を表するとともに、研究室の日頃の活動を支えていただいた山口修平様、八代祐子様、高橋尚子様、山口美佐子様、村井千夏子様、戸塚幸様に、本稿の場を借りて感謝の意を表します。

平　和昌　（たいら　かずまさ）
電磁波研究所
研究所長
前ネットワークセキュリティ研究所長
前セキュリティアーキテクチャ研究室長事務取扱
博士（工学）
電波伝搬、電磁環境、通信方式