1　緒言　ネットワークセキュリティ研究所における研究開発について

平　和昌

情報通信は、私たちの知的な活動や経済的な活動を支える基盤であり、中でもインターネットはその中核的な役割を果たしている。最近では、パソコンからネットワークを経由して情報通信サービスを利用することに加え、スマートフォンの爆発的な普及により、いつでもどこでもネットワークを利用して情報通信サービスを受けられる時代へと、その利用形態も大きく変化している。

その一方で、インターネットを利用している世帯の多くが「コンピュータウイルスの感染が心配」や「どこまでセキュリティ対策を行えばよいか不明」と感じているとの調査結果があることからも、私たち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ということが言える。実際、企業などのネットワークシステムに対する不正侵入による情報漏洩や、スマートフォンをねらったウイルスが原因となった犯罪などが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。

国立研究開発法人情報通信研究機構（NICT）では、平成23年度から27年度に至る5年間の第3期中長期目標期間において、ネットワークセキュリティ技術に関する研究開発を実施してきた。実施に際して主務大臣（総務大臣）から指示された「中長期目標」は以下のとおりである。また、中長期目標に対し、NICTが作成し主務大臣から認可された「中長期計画」は以下のとおりである。

【中長期目標】

世界最先端のサイバー攻撃観測・分析・対策・予防技術、セキュアネットワークの設計・評価と最適構成技術、次世代暗号基盤技術等、理論と実践を高度に融合させたネットワークセキュリティ技術の研究開発を行う。

【中長期計画】

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の実現を目指し、現在志向の研究と未来志向の研究を両輪で推進する。現在志向の研究では、日々高度化・巧妙化を続けるサイバー攻撃を日本全国レベルの大局的な視点で捉え対抗するための研究開発に取り組み、即効性のある成果展開を行う。未来志向の研究では、中長期的な視点に立ち、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て、セキュリティ設計を根本から見直し、あらゆる人やネットワーク機器に最適なセキュリティ機能を自動選択・自動配備する等のセキュリティアーキテクチャの研究開発や、計算機能力の向上や解読手法の進歩による暗号アルゴリズムの危殆化から脱却し、長期に渡り高度な安全性を担保可能な次世代の暗号・認証技術の研究開発を行う。また、大規模災害等の社会的危機に際しても、迅速な情報収集や情報の信頼性の確保、柔軟かつ簡便な個人認証等を実現するセキュリティ技術の研究開発を行う。なお、研究開発課題の設定に際しては、中長期計画の策定時点で可能な限り普遍的な課題設定を行うとともに、中長期目標期間中に新たに生じる世の中の状況変化（例えば、新たなサイバー攻撃手法の出現等）に対しても、柔軟に研究開発課題に取り込む。

この計画を実施するにあたって、NICTでは以下の実施方針を掲げた。

誰もが安心・安全にコミュニケーションできる社会を実現するために、理論と実践の両面からネットワークセキュリティ技術の研究開発を推進し、NICTが公的機関であることの中立性を最大限に活用することにより、中核的な研究開発拠点となることを目指す。

この実施方針のもと、以下に示す3本の研究開発を大きな柱として5年間実施した。

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、予防の研究開発を実施。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実施。

②セキュリティアーキテクチャ技術の研究開発

様々な状況でネットワークを用いたサービスを受ける際、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実施。また、今後更に発展す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実施。

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実施。また、長期にわたる利用が可能な暗号技術や、最先端の解読技術による暗号の安全性の評価を実施。

上記の各研究開発を推進する体制として、第3期中長期目標期間において「ネットワークセキュリティ研究所」を組織した。さらに、同研究所の中に「サイバーセキュリティ研究室」、「セキュリティアーキテクチャ研究室」、「セキュリティ基盤研究室」の3つの研究室を組織し、それぞれの技術の研究開発を実施した。

5年間にわたる研究開発の結果、中長期目標を大きく上回る複数の成果が得られたと自己評価するとともに、主務大臣から「中長期計画における所期の目標を上回る成果が得られている」と認められた。主務大臣が当該評定に至った理由は以下のとおりである。*

【主務大臣による評価（評定に至った理由）】

ネットワークセキュリティ技術は、第3期中長期計画において、サイバー攻撃分析・予防基盤技術の確立等のサイバーセキュリティ技術等の研究開発を行うこととしており、適正、効果的かつ効率的な業務運営の下で「研究開発成果の最大化」に向けて顕著な成果の創出や将来的な成果の創出の期待等が認められることからA とする。主な成果は以下のとおり。

- 30万IP アドレスを超える世界最大規模のサイバー攻撃観測網を構築するとともに、大規模拡散型マルウェアと標的型攻撃という全く性質の異なるサイバー攻撃それぞれに対して、最先端の観測技術、分析技術、可視化技術群を開発したことは顕著な成果の創出と認められる。
- 研究開発成果（DAEDALUS 、NIRVANA 等）を積極的に技術移転し、DAEDALUS に関しては全国558（平成28年3月末現在）自治体へ提供するなど、我が国のセキュリティ向上に大きく寄与した。
- 暗号プロトコルの評価技術に関する国際的なコンソーシアム「暗号プロトコル評価技術コンソーシアム（CELLOS）」を設立して活動の中心的な役割（事務局運営を含む）を果たし、国際的な連携体制を主導した。
- 秘匿・認証ともに情報理論的安全性が保証された世界初の実装として、量子ネットワーク上でパスワード認証機能付き秘密分散機能を備えたセキュアな外部ストレージシステムを実現し、本方式の国際標準化に向けて積極的な活動を行った。

本特集号では、第3期中長期目標期間において実施した上記①から③の各研究開発について、実施した内容及び得られた成果について詳細に記述してまとめる。①については**3**から**5**で、②については**6**で、③については**7**で、各節において詳細を報告する。第3期中長期目標期間終了時に「情報通信研究機構研究報告」の特集号としてまとめることにより、後世において参考とされる文献として残すことを目的とした。本特集号が、ネットワークセキュリティに関する研究開発や実務に従事なさる方々や、当該分野にご関心をお持ちの方々の参考になれば幸いである。

本年4月より開始された第4期中長期計画では、当該分野は「サイバーセキュリティ技術」と名称を改め、研究開発を推進している。今後ともNICT のサイバーセキュリティ技術分野の活動にご支援とご協力を賜りたくお願いする次第である。

最後に、平成24年9月まで研究所長であった高橋幸雄氏（現ソーシャルイノベーションユニット耐災害ICT 研究センター副研究センター長）及び研究所企画室の各位、当研究所の活動にご協力いただいた多くの企業研究者、大学等研究者、関係者のみなさま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
博士（工学）
電波伝搬、電磁環境、通信方式

＊ 参考：www.nict.go.jp/disclosure/s3-hyouka.pdf