

1 緒言 情報通信セキュリティ研究センターの研究

1 Introduction: The Research of the Information Security Research Center

高橋幸雄

TAKAHASHI Yukio

インターネットが普及及び情報通信を用いた新しい社会変革がおき始めている現在社会において、いまや情報通信はライフラインのひとつになってきている。一方、クラウドやスマートフォン等新しい情報通信技術が登場し、情報社会の急速な変化に対し、情報通信に対応できて使いこなせる人とそうでない人の情報格差が拡大している。また、情報通信によって、本当に生活は便利に、豊かになったかという、多くの課題はまだ山積し、真の豊かで安心な情報通信社会の実現に至っていない。特に、情報セキュリティの脅威は日増しに増加し、それに費やす労力と経費は増加の一途をたどり、被害も多様かつ甚大になってきている。安全性と利便性の間で、情報セキュリティは、情報通信社会の中で大きなウエイトを占めている。

独立行政法人情報通信研究機構 (NICT) の情報通信セキュリティ研究センターでは、「安心・安全な社会の実現」「真に豊かなコミュニケーションの実現」のため、ネットワークのセキュリティ、その基盤となる暗号や認証技術、そして情報通信による非常時・防災対応など、主に次の4つの課題について実施してきた。

- 1) サイバー攻撃等のネットワーク上で発生している悪意のある人為的なイベント (インシデント) をネットワーク全体でおきている状況を捉え、インシデントの観測、分析、対応技術に関する研究開発
- 2) インシデントの発信元のアドレスの追尾やパケットの推移を解明する時空間の追跡・再現技術の研究開発
- 3) 暗号・認証技術、アルゴリズム、暗号プロトコル、及び漏洩電磁波セキュリティの技術等の研

究開発、暗号評価に関する研究・支援

- 4) 非常時におけるネットワーク技術、ネットワークを用いた防災・減災のための技術の研究開発

この研究課題を推進するため、第二期中期計画スタートの平成18年4月に、インシデント対策グループ、トレーサブルネットワークグループ、セキュリティ基盤グループ、防災・減災基盤技術グループの4研究グループと研究支援を推進する推進室の体制で情報通信セキュリティ研究センターが組織された。

この特集号は、第二期中期計画の5年間を通じて、情報通信セキュリティ研究センターが実施してきた研究のうちネットワークセキュリティに関する成果をまとめて報告し、どのような技術がありその利活用に資する参考として考えている。第二期中期計画で実現してきた多くの成果の中で主な技術の内容と意義と貢献について、トピック的に紹介した。各章で記述しているように、第二期中期計画を達成できていると考える。また、防災・減災基盤技術に関する成果は、情報通信研究機構季報「防災・減災基盤技術特集」(Vol. 57 Nos. 1/2, 2011) で紹介する。

これらの成果を踏まえて、平成23年4月から、新しく第三期中期計画においてネットワークセキュリティ研究所として、ネットワークセキュリティ研究を実施している。サイバー攻撃をリアルタイムで把握し適切な対策を実施するため観測・分析・対策・予防を行うサイバーセキュリティ技術、多様化したネットワーク環境や利用環境の多様化に対応した柔軟で、安全かつ進化持続性を有するセキュリティアーキテクチャ技術、現在暗号と量子通信を融合した量子セキュリティ技術や新しい暗号技術を

確立するセキュリティ基盤技術の3研究課題を、三位一体として進め、国民誰もが安心・安全に情報通信を行うことができるように研究開発を進めている。

防災・減災に関する研究に関しては、これまでの研究で目的とした成果や、開発した技術が実際の現場に技術移転できたこともあり、NICT全体で見直しを行い検討していくこととして、第二中期計画で防災・減災基盤技術グループの研究は終了とした。

この特集号が、情報セキュリティの研究開発に従事する方やこの分野に関心のある方の今後の活動に役立つものになれば幸いである。今後とも、新しくスタートしたネットワークセキュリティ研究所において、日々対応を行う観点と先端的な研究を進

め、それらが社会の安全、そして真の安心に役立てるようにしていきたいと考えている。これからも皆様からのご支援やご協力をいただければと考えております。

最後に、平成22年7月まで情報通信セキュリティ研究センター長をされてこられた現NICTのR&Dアドバイザーである国立大学法人北陸先端科学技術大学院大学の篠田陽一教授、大矢浩氏、関口博久氏、安井哲也氏、米子房伸元副研究センター長、研究センターの研究を支援してきた推進室やNICTの皆様、さらに、研究センターの研究に協力いただきました多くの関係機関の皆様のおかげで、多くの研究成果をあげることができ、深く感謝いたします。



たかはし ゆきお
高橋幸雄

ネットワークセキュリティ研究所
研究所長 博士(情報学)
宇宙測位技術、位置天文学、時空認
証、時空情報利活用