特集「量子時代をみすえたコンピュータセキュリティ技術」の編集にあたって

國廣 昇[1,a)]

大規模な量子計算機が実現すると，RSA 暗号などの現在広く利用されている公開鍵暗号は解読されることが広く知られている．そのような時代が来ると，暗号，セキュリティ，プライバシ技術は一変することが予想される．実際，量子計算機到来後にも，機密情報や個人情報などの守るべき情報を安全に通信・保管・利活用するための研究開発や標準化などが，世界中で活発に行われている．このような環境の中，耐量子計算機暗号の研究開発だけでなく，それらへの安全な移行や計算量仮定によらないコンピュータセキュリティ技術，プライバシ保護技術など，解決すべき課題は山積みである．

本特集号では，量子時代をみすえたコンピュータセキュリティ技術について，基礎理論，プロトコル，アーキテクチャ，ソフトウェアシステムの研究，およびそのアプリケーション，実装例，管理運用，さらには行動科学や社会科学的考察をも含めた広範囲のセキュリティ技術を議論することにより量子時代に対応したセキュリティの実現に貢献することを目指して企画された．

本特集号には 16 件の論文が投稿され，特集号編集委員会による慎重な審議を経て英文論文 7 件を含む 12 件の論文が採択された．

特集号の編集にあたり，限られた時間の中で，多様な分野の論文について慎重な査読をいただき，計画どおりに出版に至ることができたのは編集委員，査読者，招待論文執筆者，学会関係者の方々のご尽力によるものであり，厚く御礼を申し上げたい．特に山田明幹事（KDDI 総合研究所），葛野弘樹幹事（神戸大学）には本特集号の企画から査読，編集，出版準備に至るまで全般的にご尽力いただき，心から感謝する次第です．

[1] 筑波大学
University of Tsukuba
[a)] kunihiro@cs.tsukuba.ac.jp