

特集「実社会を支える暗号・セキュリティ・プライバシー技術」 の編集にあたって

須賀 祐治^{1,a)}

計算機とインターネットの普及により、計算機システムは身の回りにある家電や車載システムなどの組み込みシステムにも広く利用されている。また、個人情報をはじめとしたプライバシーに関わる様々なセンシティブ情報が個人デバイスだけでなく、高速なネットワークでつながれることによりクラウドといった外部サービスで管理・利用されることが一般的になりつつある。一方で、機密情報や個人情報などを目的としたサイバー攻撃もその手口が多様化・高度化しており、これらの情報を適切に、かつ安全に利用できることが必要不可欠になっている。このような環境の中、暗号技術やコンピュータセキュリティ技術、そしてプライバシー保護技術が実社会の安心・安全を支えるための技術としてその重要性を増している。

本特集号は、実社会を支える暗号・セキュリティ・プライバシー技術について、基礎理論だけでなく、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課題と解決策を広く深く議論することにより、社会インフラとしてのセキュリティ技術の進展に寄与することを目指して企画された。

本特集号では、40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22件の論文が採択された。採択率は55%であり、投稿数・採択率ともにおおむね当初予定どおりの結果になった。暗号の基礎理論からネットワーク解析、セキュリティ応用、IoT、ネットワークフォレンジックといった広範囲のコンピュータセキュリティに関する研究論文を集めることができ、その技術的発展に一定の寄与ができたと考える。これは、ひとえに本特集号の編集委員および査読者の皆様による適確な著者への助言と、著者の方々による真摯かつ適切な対応の賜物であり、この場を借りて深い感謝を申し上げたい。

さらに本特集号では招待論文として、セコムIS研究所の島岡政基氏、佐藤雅史氏、mercari R4Dの中島博敬氏に、暗号資産交換所の課題整理と適切な鍵管理について執筆していただいた。本論文の掲載が、今後同様のシステムが構

築される際の参照モデルとして活用され、安全なシステム運用に貢献できれば幸いである。

特集号の編集にあたり、コロナ禍という大きな制約の中、質の高い査読と編集作業を経て、予定どおり出版までたどりつくことができたのは、編集委員、査読者、招待論文執筆者、学会関係者の方々の多大なご尽力のおかげであり、厚く御礼を申し上げたい。特に、高橋健一幹事（鳥取大学）、沖野浩二幹事（富山大学）には、特集号編集委員会の中心として献身的にご尽力いただいた。心より感謝申し上げます。

「実社会を支える暗号・セキュリティ・プライバシー技術」特集号編集委員会

- 編集長
須賀祐治（インターネットイニシアティブ）

- 幹事
高橋健一（鳥取大学）、沖野浩二（富山大学）

- 編集委員
穴田啓晃（長崎県立大学）、五十嵐大（NTT セキュアプラットフォーム研究所）、井口 誠（Kii）、市野将嗣（電気通信大学）、大木哲史（静岡大学）、大東俊博（東海大学）、大山恵弘（筑波大学）、金井 遵（東芝）、金岡晃（東邦大学）、菊池浩明（明治大学）、國廣 昇（筑波大学）、佐々木良一（東京電機大学）、島岡政基（セコム）、嶋田 創（名古屋大学）、白勢政明（はこだて未来大学）、鄭 振牟（金沢大学）、寺田真敏（日立製作所）、寺田雅之（NTT ドコモ）、鳥居 悟（富士通研究所）、中西 透（広島大学）、西垣正勝（静岡大学）、橋本正樹（情報セキュリティ大学院大学）、濱田浩気（NTT セキュアプラットフォーム研究所）、林 卓也（デジタルガレージ）、藤田 彬（情報通信研究機構）、松浦幹太（東京大学）、水木敬明（東北大学）、南 和宏（統計数理研究所）、三村 守（防衛大学校）、毛利公一（立命館大学）、森 達哉（早稲田大学）、盛合志帆（情報通信研究機構）、八木 毅（NTT セキュリティ・ジャパン）、山内利宏（岡山大学）、山田 明（KDDI 総合研究所）、渡邊裕治（日本IBM）

¹ 株式会社インターネットイニシアティブ
Internet Initiative Japan Inc. (IIJ), Chiyoda, Tokyo 102-0071, Japan

^{a)} suga@ij.ad.jp