小特集

ハードウェアセキュリティの課題と展望

小特集編集にあたって

編集チームリーダー　高木一義

社会や産業を脅かす情報セキュリティインシデントが日々発生している．情報通信技術が社会の有様を変えるほど普及した現代において，情報セキュリティは重要なトピックであり，今後も重要性が増していくことは疑いない．そのため，通信技術及び暗号技術を基盤とした，情報セキュリティを守るための基礎技術については，古くから研究され発展が続いている．一方，情報システムを構築しているハードウェアに焦点を当てたセキュリティ技術に関して，分野横断的な新しい研究課題が展開されつつある．

本小特集では，セキュリティ技術のハードウェア面に関する最先端の話題について，5名の研究者の方々に執筆頂いた．本小特集は，当該分野を担うために設立された，基礎・境界ソサイエティのハードウェアセキュリティ研究専門委員会の協力により実現した．

ハードウェアセキュリティの研究分野では，システム設計の埒外からの新種の脅威，ハードウェアによる新しい機能の提供，新しい保護の枠組み，等々，様々な方向性の研究課題が生まれてきている．課題は多彩かつ流動的であり，現時点で体系的，網羅的な解説は難しいと考えられる．強いて課題を分類するならば，1章の松本勉氏の用語をお借りして，ハードウェア「の」セキュリティ，及び，ハードウェア「で」セキュリティ，の二つの面を考えると分かりやすい．ハードウェア「の」セキュリティとは，ハードウェアのためのセキュリティの課題であり，システムを構成するハードウェアに対する攻撃にいかに対処するかという課題である．ハードウェア「で」セキュリティとは，セキュリティのためのハードウェアの課題であり，ハードウェア実現による高効率処理，また，ハードウェアならではのセキュリティ機能に関する課題である．

まず1章では，サイバーフィジカルシステムの捉え方に基づき，当該研究分野を展望する．2章では，暗号処理の専用ハードウェア向きのアルゴリズムを紹介する．3章は，暗号処理システムの内部情報を物理的手段で取得しようとする，サイドチャネル攻撃に関する解説である．4章では，耐タンパ性，セキュリティ認証，及びその周辺の話題を取り上げる．5章では，ハードウェアの真贋判定に利用可能である，物理複製困難関数に関する話題を紹介する．2章は主にハードウェア「で」セキュリティ，3，4章は主にハードウェア「の」セキュリティ，5章は両方の面に関わる話題と捉えられる．

ハードウェアセキュリティ研究分野は，従来の分野の枠組みを超えた新しい融合領域であり，今後の更なる広がりが期待される．また，基礎理論から製品開発に至る幅広いステージに属する研究者，技術者の協働のキーワードにもなると考えられる．本小特集が，当該分野の周知と発展の一助になれば幸いである．

最後に，御多用の中，原稿を御執筆頂いた皆様，記事内容を御検討頂いたハードウェアセキュリティ研専の皆様，殊に研専幹事団の皆様，また，御協力頂いた編集チームの皆様，学会事務局の皆様に深くお礼を申し上げる．

小特集編集チーム　高木　一義　堀山　貴史　北　直樹　熊木　武志
白木　善史　土屋　健伸　平井　経太