小特集

暗号と社会の素敵な出会い

編集にあたって

松尾真一郎（国立研究開発法人 情報通信研究機構）
金岡　晃（東邦大学）

インターネットの登場を待つまでもなく，古来から情報の保護は社会の重要な課題であった．暗号技術は主に軍事用途で発達し，認証技術は，たとえば江戸時代の関所札のように，国や自治体におけるさまざまな権限管理に使われてきた．そして，インターネットの登場によって，そのような情報保護の必要性は一般市民の普段の生活にまでおりてくるようになった．つまり，一般市民がセキュリティ技術を意識して利用することが当たり前となった．そして，セキュリティ技術の中核の1つである暗号技術も，以前の軍事用途から，一般市民が当たり前に使うようになっている．

1970年代後半から現代暗号技術の研究が盛んに行われている．暗号技術には数学的な安全性証明が付けられ，我々が個々の暗号技術の安全性については心配しなくてもよいようになった．しかし，残念ながら，せっかく安全性の証明が付いた暗号技術を部品として使っていても，システムとして正しくくみ上げられなかったり，正しい運用がなされないことによって，セキュリティ事故を引き起こし，社会的な問題となるケースが出てきている．このような不幸をなくすためには，暗号技術の研究者・開発者が考える提供できるセキュリティ，制約条件などの設計意図と，暗号を情報システムに組み込んだり利用する人の期待が，合致する必要がある．まさに，暗号と社会が素敵な出会いをすることが，我々の社会生活を安全にするために重要になってきている．この思いから，今回の「暗号と社会の素敵な出会い」を企画するに至った．

本小特集では，暗号技術が今後の社会における信頼の基盤となる例として，まず最初に**「マイナンバーと電子署名・電子認証」**においてマイナンバーシステムへの認証技術の適用について示す．次に，我々がネットワーク上で利用するさまざまなプロトコルの安全性と暗号の安全性の関係性と，プロトコルのセキュリティを守るために必要な活動について，**「SSL/TLSと暗号プロトコルの安全性」**にて示す．続いて，社会に必要なトラスト（信頼）を，どのようにして暗号技術を用いて実現しようとしているかを**「トラストと暗号技術の関係性」**で示す．次に，暗号研究者が新たな暗号技術を開発するときの意図（キモチ）を**「楕円曲線暗号のキモチ」**にて解説する．最後に**「暗号技術でお金を実現する」**において暗号技術が新たな経済的基盤を作り出す例としてデジタル通貨の成り立ちを説明する．

本小特集によって，社会における安全や安心と暗号技術との結び付きに関する理解が深まり，暗号技術の研究と情報システムの開発の間で，より素敵な出会いがもたらされるようになることを願ってやまない．

（2015年9月8日）