特集にあたって

神田　雅透（NTT情報流通プラットフォーム研究所）

平成19年度通信利用動向調査や電子商取引市場調査によれば，一昔前はFiber To The Home（FTTH）ともいわれた家庭への光ファイバによる高速通信も普及率が30%を超え，これにxDSLやCATVを含めたインターネット利用者におけるブロードバンド利用率は66%にもなった．この数字は日本国民全体のおよそ半数が高速インターネット通信を利用していることを示している．これだけの利用者規模となると，オンラインショッピング，ネットバンキング，ネットオークションなどに代表される消費者向け電子商取引の市場規模も大きく成長し，5.3兆円規模に達している．

このような情報化社会を健全に成り立たせるために，情報の秘匿や利用者の認証などを行う暗号技術が陰に陽に広く使われている．

しかし，暗号技術の必要性は理解できても，縁の下の力持ち的存在であり，表面的には可視化できないため，どのような動作をしているかを実際に理解することは簡単なことではない．そのため，暗号技術は専門家に任せておけばいい的風潮が無きにしもあらずだが，現実にはサービス提供者が暗号技術の使い方を誤ると大きな社会問題を引き起こしかねない．暗号化機能の有効期限切れによるシステム障害で全日空の利用者約7万人に影響が出るなどはその代表例といえる．

今後ますます情報化社会が進展すれば，より多くのシステムにおいてセキュリティ設計が重要になってくる．そうしたなか，暗号技術を理解しておくことがシステム設計やサービス提供者に求められるようになってくるであろう．

ただ，一言で暗号技術といってもその範囲は非常に広い．そこで，本特集では，引き続き「情報化社会における暗号技術の役割」として暗号技術の現状について概論的に紹介させていただいた後，様々な方面から暗号技術の概要や安全性などについて，第一線で活躍されている研究者の方々に解説をお願いした．

最初に，暗号を構成する数理理論について田中圭介氏に紹介していただいた．とりわけ公開鍵暗号を構成する基礎となる内容であり，以降の内容を理解する上で役に立つであろう．

次に，暗号技術のもっとも基礎となる公開鍵暗号と共通鍵暗号について，その仕組みがどのようになっており，また安全性とはいかなるものなのかについて，高木剛氏と松井充氏にそれぞれ解説していただいた．特に，日常生活でもよく使われる“安全”という言葉が，暗号の世界では，あいまい性のない，厳密な学術上の意味を持っていることに注目していただきたい．

単体としても機能する暗号技術であるが，それらをより複雑に組み合わせることによって，プライバシー保護といった別の要件を実現する手法が考えられており，それらを使って電子投票システムなどのセキュリティシステムを作り上げることができる．これらの手法は一般に暗号プロトコルといわれ，様々な応用目的を実現するうえでの必要な技術である．尾形わかは氏には，そのなかでもプライバシー保護を実現するうえで有効なΣプロトコルについて解説していただいた．

最近の動向として，従来のデファクト暗号技術の安全性低下に伴い，暗号技術が広く使われるようになって初めて，本格的な世代交代が求められている．しかし，そのための対策を実施しようとしても，関係者が想像以上に広範囲にわたる一方，動作の可視化ができないため，コスト負担やリスク判断一つを取ってみても，関係者間の利害が必ずしも一致するとは限らない．そこでは，OR的手法がもっとも発揮できる領域でもあると考えられるリスク評価・分析が重要な役割を果たす．佐々木良一氏には，デジタル署名の長期保存のための対策を題材にリスク評価・分析を紹介していただいた．

最後に，宮澤俊之氏には将来展望を見据え，量子計算機が実現した後の公開鍵暗号の将来像について解説していただいた．

本特集の話題は，OR手法と直接的な関係は薄いかもしれないが，例えばリスク評価などを通じて，読者に少しでも暗号技術に興味を持っていただけたならば，オーガナイザーとして大きな喜びである．