特集にあたって

辻井　重男（中央大学）

サイバースペースは無色透明な世界です．インターネットで商取引を行うとき，取引相手は透明人間のように顔が見えません．電子商取引は先ず相手を確認すること，そして自分も相手に確認してもらうことから始めなければなりません．このとき，人間のもつ五感をフルに活用することはできず，一種の数理的な手法によって，互いに相手を確かめ合う必要があります．この数理的な手法が暗号であり，このような確認作業は，人に限らず，モノ，金，ソフト，情報サービス，時刻あるいは人々の権利などの真偽の識別に及びます．

例えば，電子マネーについて考えてみましょう．社会を根源的に変えていく情報システムの中で，最も先鋭的なものをひとつ挙げよと言われたら，筆者は躊躇なくそれは電子マネーだと答えることにしています．

現在，各所で実験中の電子マネーは，場所限定的であったり目的限定型，あるいは機能限定型であったりしており，これでは電子マネーの真価は発揮されません．しかし，今後，実用化される本格的な電子マネーは，国内はもとより，国際間の電子商取引にも使われるようになり，グローバル市場を一層活性化することとなるでしょう．反面，通貨の一元的な管理や徴税権の行使は近代国家の要件でしたが，こうしたことが電子マネーをはじめとする電子商取引によって崩されていく可能性も考えられます．

このような国家の枠組すら崩しかねないという潜在的影響力をもつ電子マネーも，暗号のもつ認証機能によって初めて実現されます．即ち，電子マネーとは，暗号のもつ認証機能によってその表示金額が保証された現金であり，暗号によって電子マネーの安全性が守られるというより，電子マネーは暗号によって作られるのです．

政治や行政あるいは種々の組織運営の分野に目を向けますと，暗号によってはじめて実現されるシステムとして電子選挙・電子投票があります．インターネットにより，人々がパソコンから投票を行うとき，本人確認とプライバー保護をあわせ行うことが不可欠です．この両立も公開鍵暗号の認証機能によって可能となります．勿論，誰が誰に投票したかを盗聴されるのを防ぐために暗号の秘匿機能も必要です．

また，インターネットなどの情報ネットワークを介した行政サービスの面でもプライバシーの保護とあわせて本人確認が基本的なことは，戸籍謄本などの証明書類の取得を考えてみれば明らかでしょう．

医療の面では，今後，その質の向上と，膨らむ一方の医療費の削減に，遠隔医療の普及や電子カルテの導入が不可欠ですが，人の生命にかかわるだけに，本人性や病名の確認が大事であることは言うまでもなく，ここでも公開鍵暗号技術の利用が不可欠です．

また，高速道路の料金収受所をノンストップで走り抜けることのできる自動料金収受システム（ETC, Electric Toll Collection）は，交通渋滞を3割減少させることができると言われていますが，このETCも暗号の認証機能を用いて課金を正しく行うことによって，初めて可能となるのです．今後，交通のみでなく，様々な物流の効率化にも暗号が活用されることとなるでしょう．

勿論，産業機密を守り，個人情報とプライバシーを保護するのも暗号の基本的な機能ですが，暗号の情報秘匿機能については暗号が歴史を舞台裏で動かした様々なエピソードによっても，良く知られています．現在，暗号に対して軍事・外交上の諜報しか連想しないなどという人は少なくなりましたが，暗号の重要性を守りの論理によって納得している人が多いように思われます．

本特集では，ORという分野にふさわしく，暗号のもつ認証（署名）技術を中心にして，攻めの面やゲーム的な話題を強調するような構成と致しました．

ネットワークの合理性と透明性に基くサイバー世界が開けつつあります．本特集が，このサイバー世界を健全に活性化させていく原動力である暗号技術を活用して頂くための一助となれば幸いに存じます．