特集

暗号世代交代と社会的インパクト

特集編集にあたって

編集チームリーダー　牧野光則

現代社会を支える主要技術に暗号が含まれることに異論を唱える者は多くなかろう．秘匿と認証を主な目的として，暗号技術は数多くかつ広範囲に現在の電子情報通信システムに利用され，日常生活に溶け込んでいる．一方，暗号技術の多くは計算量的な「解読しにくさ」でその安全を担保されている．このため，我々の生活の安全は日ごとに確実に低下している．

本特集は「暗号の危たい化（危殆化（きたいか），compromise）」を主たるキーワードとしている．危たい化とは一般に「徐々に危うくなる」状態を指す．暗号に関する危たい化としては，独立行政法人情報処理推進機構が2005年3月に公表した「暗号の危殆化に関する調査報告書」（http://www.ipa.go.jp/security/fy16/reports/crypt_compromize/index.html）で，以下の3種類に分けて定義している．

- 暗号アルゴリズムの危殆化とは，ある暗号アルゴリズムについて，当初想定したよりも低いコストで，そのセキュリティ上の性質を危うくすることが可能な状況を指すものとする．
- 暗号モジュールの危殆化とは，ある暗号モジュールについて，当初想定したより低い現実的なコストで，権限が与えられていないデータや資源にアクセス可能な状況を指すものとする．
- 暗号を利用するシステムの危殆化とは，あるシステムにおける暗号が関連する機能について，当初想定したよりも低い現実的なコストで，権限が与えられていないデータやシステム資源にアクセス可能な状況を指すものとする．

いずれも「当初想定したよりも低い現実的なコスト」で実現可能となることが中核となっている．情報処理の要素技術やシステム構成技術の日進月歩は我々の社会を豊かにする一方で，我々の社会を危険に陥らせつつある．専門家では「2010年問題」と呼ばれたこともあるこの暗号の危たい化とその対応は，まさしく現在進行中である．ただし，社会インフラとして一旦普及した技術を更新して新しい技術に基づく社会を構築することにはハードルが高い．そのため，社会影響が最小限度（理想的にはゼロで）となるよう，対応や技術・システム更新を計画的にかつ慎重に進める必要がある．このような状態に社会があることをICTシステムの運用者・管理者はもちろんのこと利用者も危たい化への意識を高めて正しい知識を得ることで，いらぬ混乱が起きないようにすべきであろう．しかも，情報セキュリティに関する意識の低さが原因で生じた事件・事故が絶えないこともあり，正しい知識の普及を本会としても図る必要があると考える．

そこで，本特集「暗号世代交代と社会的インパクト」では危たい化への対応に関して現状と対応計画を紹介し，当該分野に近い方が多い本会会員に情報をまとめて提供するものである．本特集は15件の解説で構成されている．最初の「IT基盤を支える暗号技術と日本の情報セキュリティ政策」は本特集を総括するものである．続く14件の解説の位置付けもここで示されているので，ぜひ初めに御一読頂きたい．続いて，暗号政策・方針に関する5件の解説で，我が国，欧米諸国，標準化機関などの状況を明らかにする．そして，危たい化状況に関する7件の解説で暗号技術の危たい化状況を示し，現在どの程度安全といえるのかについて述べられている．最後に，暗号技術を利用している業界の対応状況を例示することで，社会対応の実際を紹介している．

本特集を通じて，これまで安心していたものが安全ではなくなりつつあること，しかしながらその対応も着実に進んでいることを御理解頂ければ幸いである．

特集編集チーム　牧野　光則　須賀　祐治　毛利　公美　天野　一幸　一色　剛　今井　順一
岩城　護　大野　光平　久保田　彰　櫻田　英樹　土屋　隆生　早川　昭二
坂東　幸浩　比留間伸行　松永　裕介　宮永　喜一　湯川　正裕