巻頭論文

暗号技術の現状と将来展望

松井　充*

Technology Trends and Future of Cryptographic Algorithms

Mitsuru Matsui

要　旨

暗号技術は，個人のプライバシー保護や企業機密保護に欠かせない要素技術として，幅広くIT製品やITシステムに利用されている。直接的に見えることは少ないものの，今では暗号をまったく使わずにわれわれが一日を過ごすことが困難とすら言える時代になった。

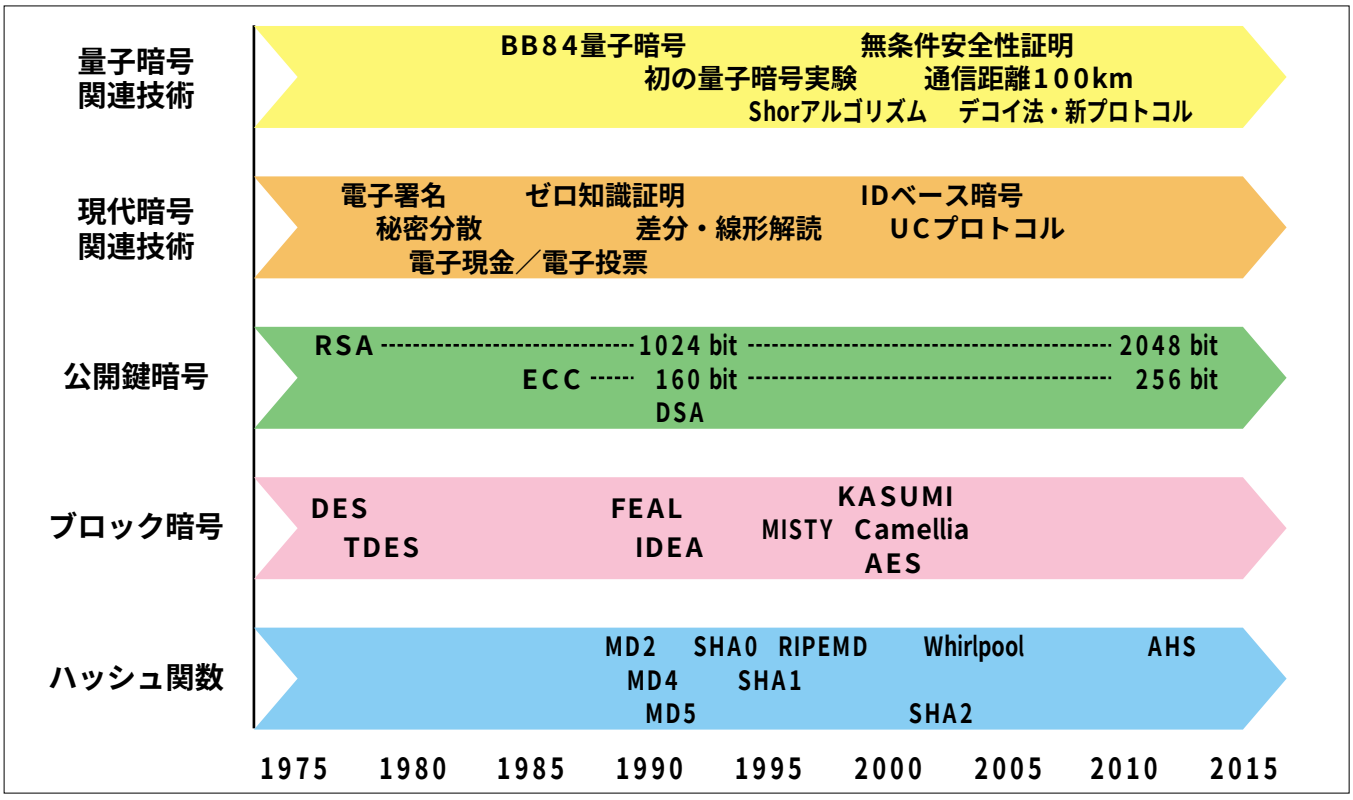
暗号技術を支える暗号アルゴリズムは，その機能に応じて共通鍵(かぎ)ブロック暗号，ハッシュ関数，公開鍵暗号など様々なタイプに分類されるが，それぞれのアルゴリズムはシステムの中で役割分担を行いながら有機的に結合され，情報通信の安全性を支えている。

三菱電機では，1995年以降“MISTY”や“Camellia(NTTとの共同開発)”に代表される共通鍵ブロック暗号を設計し，その仕様を公開するとともに，国内外の標準化に提案する活動を推進した結果，現在ではこれらの暗号アルゴリズムはISO(国際標準化機構)で世界標準に採用されるに至っている。

一方で，暗号アルゴリズムの安全性評価を目的とする解読研究の進歩もめざましい。最近ではハッシュ関数など，現在広く利用されている暗号方式の一部に将来的な安全性の懸念が示され，このため世界的に現方式から新方式への移行が進みつつあるのもまた事実である。

このような背景のもと，本稿では暗号アルゴリズムの安全性の最新状況を，実用的な観点からまとめるとともに，暗号利用に対する将来への指針を与えることを最初の目標とする。またIDベース暗号や量子暗号など最近特に注目を集めている新しい暗号技術の潮流についても概観する。

暗号は数学的安全性だけでなく，そのソフトウェアやハードウェアへの実装上の安全性も実システムでは考慮されなければならない。この点で暗号技術と物理学との接点が広がってきたと言えるであろう。



暗号技術と暗号アルゴリズムの歴史

1970年代半ばに発明されたDES(Data Encryption Standard)暗号とRSA(Rivest，Shamir，Adleman)暗号が現代暗号の幕開けであった。この図はそれ以降の主要な暗号アルゴリズムや暗号関連技術に関する発展を示したものである。公開鍵暗号については鍵長で変遷を示している。RSA暗号の鍵長は2010年以降徐々に2048ビットが主流になると考えられている。またハッシュ関数については現行のSHA(Secure Hash Algorithm)シリーズにかわる新標準AHS(Advanced Hash Standard)が2012年ごろ米国で制定される見通しである。

*情報技術総合研究所 情報セキュリティ技術部長(情報理工学博士)