暗号と社会のかかわり史(3)

（株）IT 企画　才所敏明

(1)はじめに

本稿は、現代暗号が芽生え始めた第二次世界対戦終了後から 2000 年頃までの第 1 世代共通鍵暗号の発展とその社会とのかかわりについて述べた第 2 稿に続く第 3 稿である。本稿では、現代暗号のもう一つの暗号方式、公開鍵暗号方式について、公開鍵暗号が芽生え始めた 1970 年中頃から 2000 年頃までの発展とその社会とのかかわりについて紹介する。なお、第 1 稿・第 2 稿と同様、本稿も多くの先人の成果と筆者自身の知見に基づいてまとめたものである。取り上げる技術やトピックは、筆者の個人的見解に基づき選定したことを、ご承知おき願いたい。

(2)現代暗号の二つの暗号方式による暗号化の仕組み（前稿のおさらい）

①共通鍵暗号方式による暗号化

共通鍵暗号は平文を暗号文に変換する際に使用される暗号鍵と、暗号文を平文に変換する際に使用される復号鍵が同一である暗号方式である。図 1 にその暗号化/復号の仕組みを示している。暗号鍵で生成した暗号文は、復号鍵を保有していない受信者は平文へ戻すことはできず、復号鍵を保有している受信者だけが平文へ復号できる。共通鍵暗号を利用し秘密の情報（平文）を特定の受信者へ安全に配信したい場合は、送信者とその受信者だけが暗号鍵（復号鍵）を事前に共有していることが大前提である（共通鍵暗号方式の鍵共有問題）。

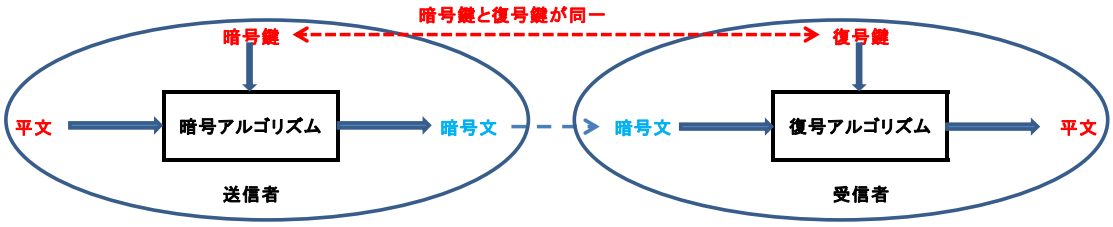


図 1. 共通鍵暗号方式による平文（秘密の情報）の暗号化/復号の仕組み

②公開鍵暗号方式による暗号化

公開鍵暗号方式は、平文を暗号文に変換する際に利用する暗号鍵（公開可能な鍵のため公開鍵と記載）と暗号文を平文に変換する際に利用する復号鍵（秘密裏に管理する必要がある鍵のため秘密鍵と記載）が異なる暗号方式である。図 2 にその暗号化/復号の仕組みを示している。公開鍵暗号方式では、公開鍵から秘密鍵（復号鍵）を導出するのが困難であるため、暗号鍵を公開鍵として公開できる。

なお、公開鍵暗号を利用し秘密の情報（平文）を特定の受信者へ安全に配信できるため

には、送信者がその受信者の正しい公開鍵を利用し暗号化することが大前提である（公開鍵暗号方式の公開鍵検証問題）。

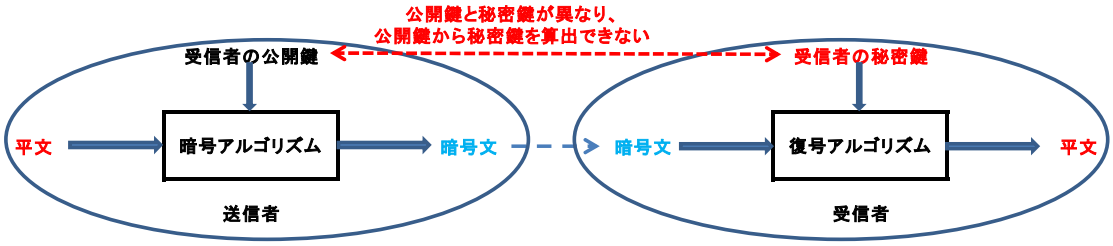


図 2. 公開鍵暗号方式による平文（秘密の情報）の暗号化/復号の仕組み

(3)主要な公開鍵暗号の発表の歴史とその概要

(3-1)Diffie-Hellman の鍵共有方式

1976 年、スタンフォード大学の教授であったマーティン・ヘルマンは 2 人の大学院生ホイットフィールド・ディフィーとラルフ・マークルとともに、共通鍵暗号方式の鍵共有問題を解決する方法を発表した。この方法は Diffie-Hellman の鍵共有方式と呼ばれ、共通鍵暗号を利用し暗号通信を行いたい場合に必要な鍵共有を安全に実現する方法として注目され、現在も多くのシステムで利用されている。

Diffie-Hellman の鍵共有方式は、公開できる配信鍵（公開鍵）と秘密裏に管理すべき秘密の情報（秘密鍵）を使用しており、マーティン・ヘルマン、ホイットフィールド・ディフィー、ラルフ・マークルの論文は、公開鍵暗号方式の概念を世界に先駆けて発表したものと高く評価されている。

①Diffie-Hellman 鍵共有の手順

以下、送信者 Alice と受信者 Bob 間の鍵共有手順を、具体例を交え説明する。

[1]送受信者間で二つの素数をあらかじめ共有

送信者 Alice と受信者 Bob は、generator と prime という二つの大きな素数をあらかじめ共有しておく。generator と prime という二つの素数は第三者に知られても構わない。

なお、例題では計算が簡単なように、g(enerator)は 2、p(rime)は 53、とする。

[2]送受信者はそれぞれの秘密の情報を作成し管理

送受信者は、乱数を利用し、それぞれの秘密の情報を作成し管理する。

例題では、送信者 A の秘密の情報 x は 9、受信者 Bob の秘密の情報 y は 3 、とする。

[3]送受信者はそれぞれの配送鍵を作成し相手へ送付

それぞれの配送鍵はそれぞれの秘密の情報を利用し、次式により計算し、相手へ送付する。この配送鍵は、途中で第三者に傍受されても構わない。

$$配送鍵 = g^{\{秘密の情報\}} \bmod p$$

例題の場合 g=2、x=9、p=53 であるから、Alice は次の計算式によって配送鍵 A を計算

し、これを Bob に送る。

$A = g^x \bmod p = 2^9 \bmod 53 = 512 \bmod 53 = (477+35) \bmod 53$

$= (53*9+35) \bmod 53 = 35$

例題の場合 g = 2、y = 3、p = 53 であるから、Bob は次の計算式によって配送鍵 B を計算し、これを Alice に送る。

$B = g^y \bmod p = 2^3 \bmod 53 = 8$

[4]送受信者はそれぞれ二人だけの共有情報を作成

送受信者それぞれによる、相手から受け取った配送鍵と自身の秘密の情報を利用した次式の計算結果は同一となり、これが送受信者の共有情報となる。この共有情報を利用し暗号鍵および復号鍵を生成することにより、共通鍵暗号方式の課題であった鍵共有が可能となる。

共有情報 $=$ (相手から受け取った配送鍵)$^{\{自身の秘密の情報\}} \bmod p$

例題の場合、B = 8、x = 9、p = 53 であるから、Alice は次の計算式によって共有情報計算する。

Alice の共有情報計算式 $= B^x \bmod p = 8^9 \bmod 53 = 51$

例題の場合、A = 35、y = 3、p = 53 であるから、Bob は次の計算式によって共有情報計算する。

Bob の共有情報計算式 $= A^y \bmod p = 35^3 \bmod 53 = 51$

このように、確かに Alice と Bob は共有情報を入手できることがわかる。

②Diffie-Hellman 鍵共有方式の安全性

安全性は、配送鍵は送受信者それぞれが保有する秘密の情報を使用し簡単に計算できるが、第三者が入手できる配送鍵から秘密の情報を計算するのは極めて難しい、という一方向性に基づいている。

つまり、次式による配送鍵の計算は容易だが、

配送鍵 $= g^{\{秘密の情報\}} \bmod p$

第三者が入手した配送鍵、g、p およびこの計算式を利用しても、秘密の情報を計算するのは難しいため、配送鍵、g、p を公開しても秘密の情報は第三者に知られることは無い。

このような、$\alpha = g^{\beta} \bmod p$ の式の、α、g、p から β を求める問題は離散対数問題と呼ばれ、g、p が大きな素数の場合、β を効率的に見出すアルゴリズムは発見されていないことが、Diffie-Hellman 鍵共有方式の安全性の根拠となっている。なお現在は、解読が困難なように、g、p として使用する素数は 2048 ビット程度の非常に大きな素数が使われている。

(3-2)RSA 暗号

1978 年、アメリカのマサチューセッツ工科大学のロナルド・リベスト(Rivest)、アディ・シャミア(Shamir)、レオナルド・エーデルマン(Adelman)は、ディフィー、ヘルマン、マークルによって発表されたばかりの公開鍵暗号という新しい概念に対し、秘匿や認証を実現

できる具体的な暗号アルゴリズムを考案した。この方法は、3 名の名前を繋ぎ RSA 暗号と呼ばれている。

①RSA 暗号の原理

RSA 暗号は、p,q を素数とすると、その積 （p＊q） を法とする世界では、

ある数の $n^{\{(p-1)と(q-1)の最小公倍数\}+1}$（n は任意の整数）は元の整数 n と一致、つまり、

ある整数 n を{(p-1)と(q-1)の最小公倍数}+1 回掛けると元の数 n に戻る

という性質を利用する。

②RSA 暗号による暗号化/復号の手順

以下、暗号化の手順を、具体例を交え説明する。

[1]鍵ペア（公開鍵、秘密鍵）の生成（受信者）

適当な正整数 e を選択する。

大きな二つの素数 {p,q} を生成し、それらの積 n (= pq) を求め、{e,n} を平文の暗号化に使用する鍵（公開鍵）とする。暗号化に使用する鍵は公開しておく。

次式より、暗号文の復号に使用する鍵（秘密鍵）d を生成し秘密裏に保管する。

$d = e^{-1} \bmod\{(p-1)(q-1)\}$

例題では計算が簡単なように、e = 3、p = 3、q = 11 という小さな値とすると、n = 33、d = 17 となり、公開鍵{e,n}は{3,33}、秘密鍵 d は 17 となる。

[2]暗号化（送信者）

秘匿したいメッセージを m とすると、公開されている受信者の公開鍵{e,n}により暗号化されたメッセージ c を以下の式で作成し、受信者へ送付する。なお、m<n とする。（もし、m≧n の場合は、m は複数のメッセージに分割され、それぞれに以下の式を適用し暗号化メッセージを作成するものとする。）

$c = m^e \bmod n$

例題では、秘匿したいメッセージとして m を整数 6 とすると、暗号化されたメッセージ（整数）c は以下の式で生成する。

$c = m^e \bmod n = 6^3 \bmod 33 = 216 \bmod 33 = 18$

[3]復号（受信者）

暗号化されたメッセージ c は秘密鍵 d を利用し以下の式で復号、秘匿されたメッセージ m を入手する。

$m = c^d \bmod n = (m^e)^d \bmod n = m \bmod n = m$

例題では、m は暗号化されたメッセージ（整数）c を以下の式で復号し入手する。

$m = c^d \bmod n = 18^{17} \bmod 33 = 21859115597387000000 \bmod 33 = 6$

このように、秘匿されたメッセージが正しく復号されることがわかる。

③RSA 暗号の安全性

安全性は、RSA 暗号における暗号化で必要な m^e の計算はべき乗演算であり容易に計算できるのに対して、暗号化されたメッセージ c から秘匿されたメッセージ m の計算（c の e

乗根の計算）は「二つの素数をかけ合わせた数を法とする世界」では難しい、という一方向性に基づいている。更に、秘密鍵 d を見出して秘匿されたメッセージ m を求めることも、十分大きな素数 p、q の合成数 n の素因数分解は困難なため p、q を見いだせず、秘密鍵 d の算出も困難である。現在、RSA 暗号では p、q として 2048 ビット程度の素数が使用されている。

(3-3)楕円曲線暗号

1985 年頃、 IBM トーマス・J・ワトソン研究所のビクタ・ミラー（Victor Miller）とワシントン大学のニール・コブリッツ（Neal Koblitz）が各々発明した暗号である。楕円曲線暗号（Elliptic Curve Cryptography : ECC）は、楕円曲線上の離散対数問題（EC-DLP）の困難性を安全性の根拠としている。

①楕円曲線暗号の原理

楕円曲線というのは、式 : $y^2 = x^3+ax+b$ で表現される曲線である。a、b の値によって曲線は変化する。

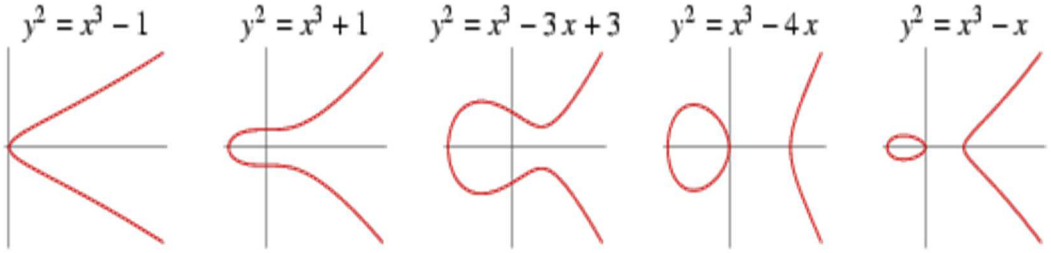
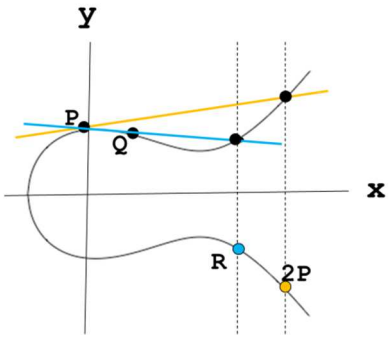


図 3. 楕円曲線の例（http://cse.iitkgp.ac.in/~debdeep/pres/TI/ecc.pdf より引用）

楕円曲線上で 2 点 $P(x_p,y_p)$、$Q(x_q,y_q)$の加算結果 $R(x_r,y_r)$、および P の 2 倍（P+P）の結果 2P を以下の図のように定義する。



説明：

[1]点 R は、2 点 P、Q を結ぶ直線と楕円曲線の交点の y 座標の符号を反転した点、とする。

[2]2P に対応する点は、点 P の楕円曲線の接線と楕円曲線の交点の y 座標の符号を反転した点、とする。

図 4. 楕円曲線上の演算

このように定義された楕円曲線上の演算は、任意の整数 n に対し nP に対応する点 S を容易に求めることができるが、整数 n が十分大きい場合、P および S がわかっていても、n

を求めることは困難、という性質を利用しているのが、楕円曲線暗号である。

②楕円曲線暗号による暗号化/復号の手順

[1]鍵ペア（公開鍵、秘密鍵）の生成（受信者）

まず、楕円曲線（次式）のパラメータ a、b、p を決める。

$$y^2 = x^3+ax+b \bmod p$$

また、使用する楕円曲線上に基準点 G を決める。

次に、大きな整数 n を決め、これを秘密鍵とし、nG を暗号化に使用する公開鍵に対応する点 P_n として公開する（$P_n = nG$）。

[2]暗号化（送信者）

秘匿したいメッセージを m とすると、m に対応する点 P_m（m を x 座標とする楕円曲線上の点）を求める。

任意の大きな整数 k を決め、公開されている受信者の公開鍵に対応する点 P_n を利用し暗号化されたメッセージ c（二つの点の組合せ）を以下の式で作成し、受信者へ送付する。

$$c = \{P_{c1},P_{c2}\} = \{kG,P_m+kP_n\}$$

[3]復号（受信者）

暗号化されたメッセージ c は秘密鍵 n を利用し以下の式で復号、秘匿されたメッセージ m に対応する点 P_m を特定し、メッセージ m を入手する。

$$P_m = P_{c2} - n\,P_{c1} = P_m + kP_n - n(kG) = P_m + kP_n - k(nG) = P_m + kP_n - kP_n = P_m$$

このように、第 2 項（P_{c2}）から第 1 項（P_{c1}）に秘密の鍵 n を乗じたものを差し引くと秘匿されたメッセージ m に対応する点 P_m が特定でき、秘匿されたメッセージ m を入手できる。

③楕円曲線暗号の安全性

さて、受信者の秘密鍵 n がわからなくとも、第 2 項の式 $P_{c2} = P_m + kP_n$ より、k がわかれば P_m の特定は可能である。そこで、楕円曲線暗号の安全性は、第 1 項の式 $P_{c1} = kG$ を利用した k の算出の困難さに依存することになる。n、k が大きな整数の場合、P_{c1}、G がともに既知であっても、第 1 項の式より k を算出する問題は楕円曲線上の離散対数問題と呼ばれ難しい問題である。このことが楕円曲線暗号の安全性の根拠である。現在、楕円曲線暗号では秘密鍵 n および k として、200 ビット程度の整数が使用されている。

(4)公開鍵暗号による電子署名と公開鍵証明書

秘密鍵と公開鍵の鍵ペアを使用する公開鍵暗号では、情報の秘匿を目的とした暗号化（図 2）のみではなく、図 5 に示すように、秘密鍵で暗号化した情報は対応する公開鍵でしか復号できない、という性質を利用し情報の送信者の確認や送信情報の改ざんの検知を目的とした送信者認証やデータ認証に使用されている。

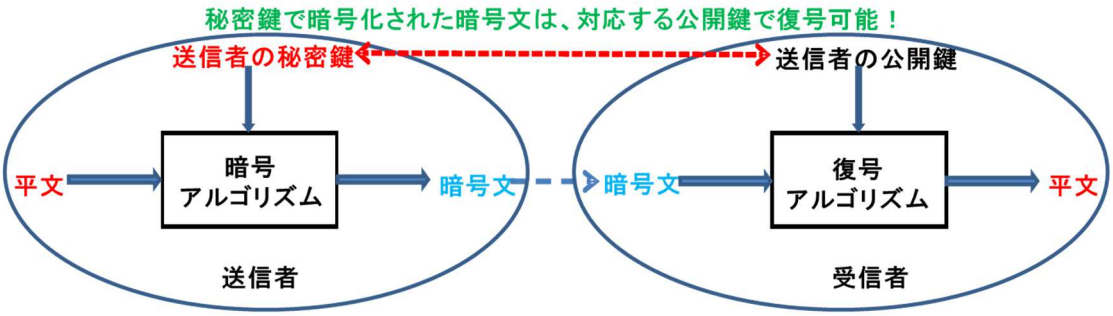


図 5. 秘密鍵による暗号化データは公開鍵により復号可能

(4-1)電子署名

図 5 の公開鍵暗号の性質を利用した、送信者の確認（送信者認証）や受信データの非改ざん性の確認（データ認証）には、電子署名が利用される。その仕組みを図 6 に示している。

ハッシュ値とは、元のデータを一定長の短いデータへ変換したものであり、元のデータが 1 ビットでも変われば異なるハッシュ値へ変換されるような関数を利用し生成する。電子署名は、ハッシュ値を送信者の秘密鍵で暗号化したものである。

送信者は、データそのものと作成した署名（電子署名）の二つを受信者へ送付する。受信者は、受信したデータから送信者と同じハッシュ関数を利用しハッシュ値を作成し、作成ハッシュ値（図 6 の㋐）を得る。受信者はまた、受信した署名を送信者の公開鍵で復号し復号ハッシュ値（図 6 の㋑）を得る。

この二つの値、作成ハッシュ値㋐と復号ハッシュ値㋑が同一であれば、受信者は、送信者が確かに想定した送信者であること、および、データが送信途中で改ざんされていないこと、の両方を確認することができる。

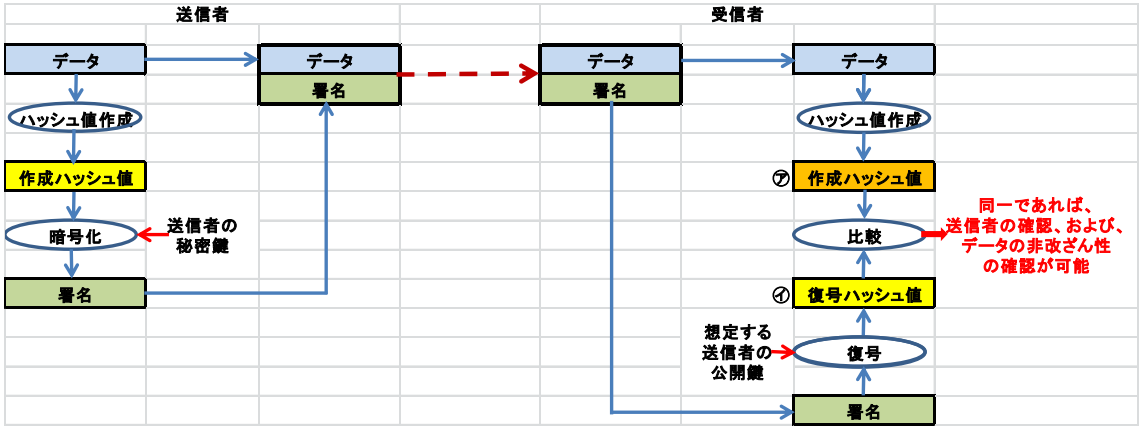


図 6. 電子署名による送信者認証およびデータ認証の仕組み

(4-2)公開鍵証明書

公開鍵暗号の利用は、受信者の公開鍵を使用しての情報の暗号化による秘匿、送信者の公開鍵を使用しての署名検証による送信者認証・データ認証の二通りが考えられるが、いずれも使用する公開鍵が受信者・送信者の正しい公開鍵であることが前提となっている。

そこで、秘匿のための暗号化に使用する公開鍵が本当に想定する受信者の公開鍵なのかどうか、また、送信者認証・データ認証に使用する公開鍵が本当に想定する送信者の公開鍵なのかどうか、の確認が必要となる。その確認のために用意されているのが公開鍵証明書である。

公開鍵証明書は、公開鍵とその所有者が関連付けられており、信頼できる第 3 者機関（認証局 : Certificate Authority）がその関連付けを確認の上で発行する証明書である。送信者・受信者が公開鍵を使用する場合は、信頼できる第 3 者機関より相手の公開鍵証明書を入手し公開鍵と公開鍵所有者との対応を確認し、更にその発行機関の信頼性とその証明書の有効性を確認の上、公開鍵を使用する必要がある。公開鍵証明書の形式は、ITU-T にて 1988 年に X.509 として規定され、その後、IETF にて改良・拡張が実施されている。

(5)公開鍵暗号の応用状況

(5-1)インターネットの発展と暗号応用の進展

現在、社会の様々の活動はインターネット上で展開され、インターネット無しでは日々の生活もままならない状況にあることはご承知の通りである。今後も社会のインターネット依存は強まることが想定されている。そのインターネットが生まれたのがこの時期であり、インターネットの普及を大きく支えたのが暗号技術である。

1961 年、アメリカのユタ州でテロにより 3 ヶ所の電話中継基地が破壊され、軍用回線も一時的に完全に停止してしまったことを契機に、アメリカの国防総省は、核戦争にも耐えうる新たな通信システムの研究を始め、分散型ネットワークによる通信ルートの複数化、情報のパケットへの分割・送信、というインターネットの基本的な仕組みが考案された。

1969 年には、その成果として世界初のパケット通信のネットワーク、インターネットの先駆けである「ARPANET (Advanced Research Projects Agency NETwork)」がスタートした。なお、同年には、ベル研究所（Bell Laboratories）が、現在の主要なコンピュータ OS の一つである UNIX を発表している。

現在のインターネットで使用されている通信プロトコル TCP/IP（Transmission Control Protocol/Internet Protocol）の原案は米国の計算機科学者 Vinton Gray Cerf および Robert Elliot Kahn により 1974 年に発表され、ここで初めてインターネット（Internet）という単語が使用された。1983 年には ARPANET がそれまでの通信プロトコル NCP（Network Control Program）から TCP/IP へ移行し、現在のインターネットが立ち上がった。

日本では、1984 年、慶応大、東工大、東大で UUCP（Unix to Unix Copy Protocol）をベースにした JUNET（Japan University Network）が創設され、日本での研究用インタ

ーネットがスタートした。1987 年には、産業界でのインターネット利用の研究・実証のための Inet Club が創設され、筆者も東芝の代表として参加、企業活動での試用が始まった。1992 年には日本でも商用インターネット接続サービスが開始され、こうして日本のインターネット時代が始まった。

インターネットでは、利用者が他の利用者を攻撃することを想定していなかったため、セキュリティ機能は装備されていない。インターネットの利用が広がるにつれ、様々のセキュリティ課題が発生し、その都度、対応に追われているのが実情である。そのような状況下でも、暗号技術はインターネットのセキュリティ課題を克服する有力な技術として活用されてきた。

①電子メール

インターネット開始当初から利用され続けているのが電子メールである。電子メールはインターネット普及を支えたキラーアプリケーションの一つであり、現在も電子メールは産業界の活動はもちろん、国民の日々の生活に欠かせない電子的情報伝達手段であることはご承知の通りである。

そもそも電子メールは、インターネットに先駆けて開発された。1960 年代には、メインフレーム上のタイムシェアリングシステムの複数の利用者が相互に通信する方法として使われ始めたのが電子メールの起源とも言われているが、BBN（Bolt Beranek and Newman）社のレイ・トムリンソン（Ray Tomlinson）が 1971 年に ARPANET 上の電子メールシステムを開発し、ARPANET 上で初めての電子メールが送信され話題となった。@を使って利用者名と機器とを指定できるようにした最初の電子メールシステムであった。ARPANET 上では電子メール利用者が急激に増大したようである。

一方、1969 年に開発された UNIX 上で、UNIX メールが 1971 年には使用されていたようである。UNIX メールの異なる UNIX システム間の通信に UUCP が使用されていたが、1976 年に UNIX 上に TCP/IP が組み込まれ、ARPANET が 1984 年に TCP/IP へ移行後、UNIX メールも UUCP から TCP/IP の利用へ移行した。

さて、一般の人向けの電子メールとしては、1979 年に米国で CompuServe が開始したパソコン通信サービスでも提供されていたが、インターネットのサービスが開始・拡大するにつれ、他のシステムとの相互接続が可能なインターネットの電子メールが広範に利用されるようになった。

電子メールのセキュリティ課題の一つは、メール情報の漏洩問題である。電子メールは、送信者が使用するメールサーバから、インターネットを経由し、受信者が使用するメールサーバへ転送される。その過程で、電子メール内の情報が漏洩するリスクが存在する。また、電子メールの情報が改ざんされるリスク、電子メール送信者をなりすましされるリスクも存在する。

このような電子メールのリスクを回避するため、セキュリティ機能を有した電子メール S/MIME（Secure Multipurpose Internet Mail Extensions）が提案されている。S/MIME

は当初、米国の RSA Data Security Inc.（RSA 暗号製品の開発・販売会社）が 1995 年に開発したが、S/MIME ver.2 が発表された 1998 年よりインターネットの技術の標準を推進する IETF（Internet Engineering Task Force）にて仕様の拡張や変更が議論されている。

S/MIME Ver.2 では、電子メール内の情報保護のために DES や RC2 などの共通鍵暗号による暗号化と、受信者が復号するのに必要な復号鍵の安全な配送（共有）のために公開鍵暗号 RSA による暗号化、が規定されている。（このように、情報そのものの暗号化には処理効率の良い共通鍵暗号を使用し、その鍵共有のためには処理効率は悪いが事前の鍵共有が不要な公開鍵暗号を使用する方式はハイブリッド暗号方式と呼ばれ、現在も幅広く利用されている。）

また S/MIME Ver.2 では、電子メールの情報が改ざんされるリスク、電子メール送信者をなりすましされるリスクへの対策として、公開鍵暗号 RSA による電子署名の仕様が規定されている。

S/MIME はその後も拡張・改良が IETF にて行われ、現在は共通鍵暗号として TripleDES や AES が規定されている S/MIME Ver.3.2 へと改訂されているが、暗号化の仕様が企業や組織のセキュリティポリシーと整合が取れず残念ながらあまり利用されていない。（現在、筆者は S/MIME を更に改良・拡張した、企業・組織を含め社会全体で活用可能な安心・安全な電子メール利用基盤 SSMAX（Secure and Safe MAil eXchange framework）、の必要性を提唱しているところである。）

②ホームページ（World Wide Web サイト）

現在、多くの企業がホームページを保有し、個人でもホームページを開設している人は多く、全世界で約 12.5 億のホームページが存在すると言われている。

WWW（World Wide Web）は、1989 年、CERN（欧州原子核研究機構：European Organization for Nuclear Research）の Tim Berners-Lee が基本的な枠組みを考案、その中で転送プロトコル HTTP（HyperText Transfer Protocol）、リソース識別名 URL（Uniform Resource Locator）、ページ記述言語 HTML（HyperText Markup Language）などが開発された。1991 年には、CERN がインターネット上での WWW のサービスを開始した。

1993 年には、米国・イリノイ大学の NCSA（米国立スーパーコンピュータ応用研究所：National Center for Supercomputing Applications）の Mark Andreessen が、NCSA Mosaic 1.0 をリリースした。WWW は文字情報だけを扱うものであったが、Mosaic は画像も扱える画期的なブラウザであった。Mosaic はすぐに無料でソースコードが公開された。東芝でスーパーコンピュータの応用を推進する職にあった筆者も当時 NCSA を訪問、Mosaic の大きな可能性を感じたものであった。

1994 年には、Mark Andreessen らは Mosaic Communications Corporation（後の、Netscape 社：Netscape Communications Corporation）を設立し、Netscape Navigator 1.0 をリリースした。このブラウザは世界中で利用され、一時期ブラウザの 9 割程度のシェアを占めた。

Netscape 社は、サーバ上の WWW（ホームページ）とクライアント上のブラウザ間のインターネットを利用した通信のセキュリティ（通信の秘匿、通信の改ざん検知、エンティティ認証）を確保するため、SSL（Secure Socket Layer）を開発し、1995 年にリリースした Netscape Navigator 1.1 に SSL2.0 を組込み、セキュアな転送プロトコル HTTPS（HyperText Transfer Protocol Secure）のサポートを開始した。

SSL の通信手順（概要）を図 7 に示している。まず、ブラウザが動作するクライアントと WWW が動作するサーバの双方で使用可能な共通鍵暗号の中から使用する共通鍵暗号を決め、次にクライアントにて共通鍵暗号で使用する暗号鍵（=復号鍵）を生成し、サーバから受けとったサーバの公開鍵証明書から公開鍵を抽出し、そのサーバの公開鍵を使用し生成した共通鍵暗号の暗号鍵を暗号化し安全にサーバへ送信する。サーバは自身の秘密鍵で共通鍵暗号の暗号鍵を復号し、こうしてクライアントとサーバが暗号鍵（=復号鍵）を共有することができる。以降は、クライアントもサーバも共有した暗号鍵（=復号鍵）を使用し情報を暗号化したデータとして送信するので、インターネットを経由しても情報の漏洩が無く改ざんされる心配も無い。なお、クライアントは受け取ったサーバの公開鍵証明書の正当性（正しい公開鍵証明書か、現在も有効な公開鍵証明書か）の検証を行う必要がある。

SSL の標準化は、1996 年以降、Netscape 社からインターネットの技術の標準を推進する IETF（Internet Engineering Task Force）に移管され、名称も TLS（Transport Layer Security）へ変更され、新たに顕在化する様々のセキュリティ課題へ対応しつつ仕様の拡張や変更が実施されている。2018 年に IETF にて承認された TLS の最新版 TLS1.3 では、共通鍵暗号として AES、公開鍵暗号として RSA 暗号や楕円暗号が推奨されている。

TLS は、現在も重要なセキュリティプロトコルの一つとして、インターネット上の様々のサービスにおいて、パスワードや個人名・住所等の個人情報、商品・サービスの購入・利用履歴等のプライバシー情報の漏洩・改ざんからの保護に利用されている。

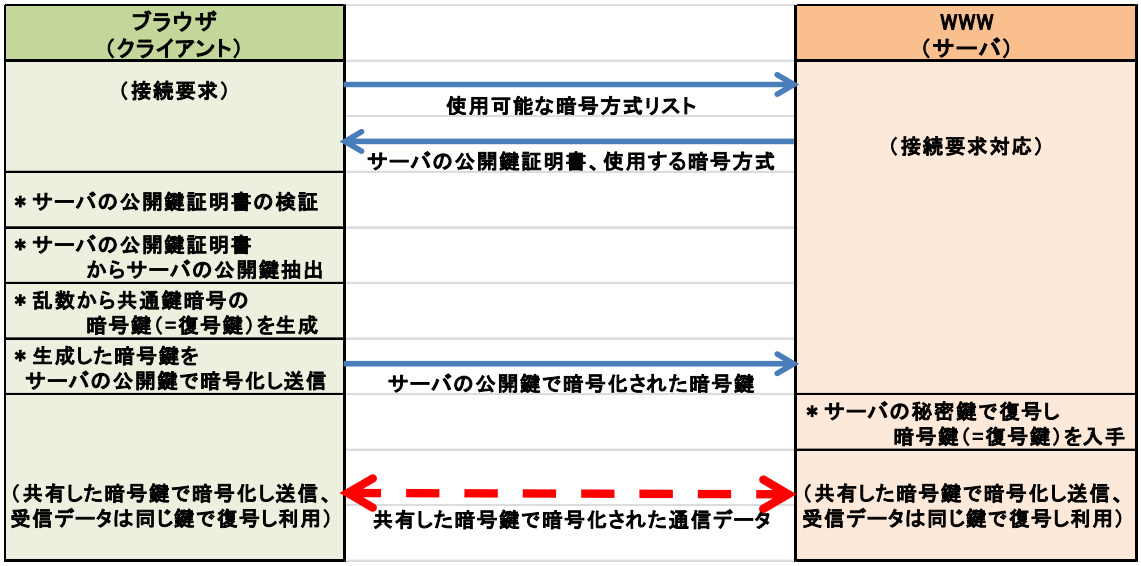


図 7　SSL の通信手順（概要）

(5-2)IC カードの発展と暗号応用の進展

私たちの快適な日常生活(特にフィジカル空間における生活)を支えている IC カードも、発明されたのはこの時期である。暗号技術およびその実装技術の研究開発の進展に応じ、応用分野も広がり発展してきた。

カードとしては、1960 年に IBM が発明した磁気ストライプカードが長年利用されてきたが、ドイツでは 1968 年、日本では有村國孝氏が 1970 年、フランスでは 1974 年、と各国で並行し IC カードが考案・発明された。1970 年代後半には、ブルとモトローラにより開発された CPU を搭載して単体で演算能力を持つ IC カードが登場、IC カード時代の幕開けとなった。日本では、1983 年に大日本印刷や凸版印刷が IC チップインカード、1984 年には東芝が IC カード、1985 年には日立も IC カードを開発した。ソニーは 1988 年に非接触 IC カード（FeliCa 方式）の開発に着手した。

IC カードの携帯性、高セキュリティ性、多様な機能の実装可能性等の特徴により、IC カードは徐々に社会で利用されるようになり、安心・安全な利用のための更に高いセキュリティ機能が求められるようになり、暗号技術の IC カードへの搭載が進められた。当初は IC カードに内蔵された汎用 CPU のソフトウェアとして実現されたが、暗号処理ニーズの拡大や高速処理へのニーズの高まりと共に、汎用 CPU とは別に暗号処理専用回路（コプロセッサ）を搭載する IC カードが開発された。東芝は 1980 年代後半にソフト＋補助ハードウェアにより世界に先駆けて DES を IC カードに実装した。現在では、共通鍵暗号方式である TripleDES/AES のコプロセッサを搭載した IC カードも利用されている。公開鍵暗号方式については、1990 年代後半、東芝は DES と共に RSA 暗号のためのコプロセッサを搭載した IC カードを開発、他社もほぼ同時期に開発した模様。その後、楕円曲線暗号の IC カードへの実装も進められた。

IC カードは発明されて未だ半世紀ではあるが、暗号技術およびその実装技術に関する研究・技術開発の進展、社会の IT 化の進展に伴い、IC カードの応用分野は急速に拡大し、今や国民の毎日の生活、様々の社会活動に不可欠な存在となっている。

①交通分野

[乗車カード]

1985 年、当時の日本国有鉄道（国鉄）がプリペイドカードであるオレンジカードを発売した。オレンジカードは自動券売機に投入して乗車券と引き換えるカード（間接式）で、カードをそのまま自動改札機に投入することはできず、乗車カードとは言えなかった。

1991 年には、東日本旅客鉄道（JR 東日本）が SF（Stored Fare）方式のイオカードを山手線内の一部の駅で利用開始し、その後、首都圏各駅に導入を進めていった。イオカードは、自動改札機に直接投入することが出来る磁気ストライプ方式のプリペイド乗車カードであった。

ソニーは 1987 年に FeliCa の研究開発をスタートした。当初は、物流分野における RFID（Radio Frequency IDentification）の市場向けに開発を目指したようであるが、1990 年

代に入ってからは、乗車 IC カード市場向けの FeliCa の開発に力を入れ、1995 年に香港の乗車 IC カードへの採用が決定し、3 年後の 1997 年に「オクトパスカード」が本格稼働した。このオクトパスカードが、世界初のプリペイド乗車 IC カードであった。日本では、2001 年に FeliCa 方式を採用した JR 東日本の「Suica」の利用が始まり、また私鉄を含む様々な鉄道・バス各社でプリペイド乗車 IC カードの導入が進むと共に、2010 年頃から交通系 IC カード全国相互利用サービスが全国に拡大し、乗車 IC カードの時代が到来した。

なお、乗車 IC カードで採用されている FeliCa 方式では、通信する IC カードとリーダ/ライタやリーダ/ライタとコントローラ間での相互認証（お互いに適切な機器であることの確認）のためや、機器間の通信路を流れる情報の暗号化（情報の漏洩・改ざんからの保護）のために共通鍵暗号 DES/TripleDES/AES が利用されている。

②金融分野

[クレジットカード]

紙製のクレジットカードが出現したのは 19 世紀後半の米国と言われている。プラスチックカードの普及は米国で 1950 年頃からで、他国では 1960 年代に入って普及した。世界で最初のクレジットカード専門の会社は 1950 年に設立された米国のダイナースクラブである。現在の主要なクレジットカードブランドの一つ AMEX が発行されたのも 1958 年であり、バンクオブアメリカカード（VISA の前身）も同年に発行され、1966 年にはマスターチャージカード（MasterCard の前身）が発行された。

日本で最初のクレジットカードを発行したのは丸井で 1960 年のことであった。1961 年には日本クレジットビューロー（JCB の前身）が設立され JCB カードの発行を開始、1960 年に設立された日本ダイナースクラブも 1961 年にダイナースクラブカードの発行を開始した。日本でも 1964 年の東京オリンピックがきっかけとなりクレジットカードが広く使われるようになり、銀行業界もクレジットカード発行に積極的に取り組み、また 1970 年頃から海外のクレジットカードブランドとの提携が進み、現在の様な海外でも使える国際カードの時代が到来した。

以上のようにクレジットカードの歴史は長いが、クレジットカードの機能や形態は時代時代のニーズに応じ大きく異なっていた。当初は紙製であったが、1950 年頃からプラスチックカードが発行され、そのプラスチックカードの裏面に磁気ストライプが付けられるようになったのは 1972 年頃であり、それまでは、暗証番号も無かった時代である。

1993 年、Visa と MasterCard が「IC チップ搭載クレジットカードの統一規格」を策定した。両社の頭文字である「M」と「V」に、規格策定当時ヨーロッパで MasterCard ブランドを運営していた Europay International の「E」を加えて「EMV 仕様」と呼ばれている。EMV 仕様の維持・管理は 3 社の出資で 1998 年に設立された EMVCo,LLC が行っている。EMV 仕様の IC クレジットカードは世界各国で実用化され始め、イギリスやフランスをはじめヨーロッパ諸国では広く普及が進み、現在ではほぼすべてのクレジットカードが

EMV 仕様に対応している。日本でも 2001 年に導入され、現在では多くのクレジットカードが EMV 仕様に対応している。

EMV 仕様では、セキュリティを高めるため暗号技術が駆使されているが、使用する共通鍵暗号アルゴリズムとしては DES/TripleDES の他、2011 年には AES の使用もオプションとして加えられている。公開鍵暗号アルゴリズムとしては RSA 暗号が指定されている。

[キャッシュカード]

銀行のキャッシュカードは、長年、磁気ストライプ式のキャッシュカードが使用されており、磁性体の塗布や磁気カードリーダ／ライタを使って磁気情報を読み取る「スキミング」が容易で、偽造カードによる被害が多く発生していた。IC カードの出現、応用が進展する中、キャッシュカードも偽造カード対策として IC カード化、IC キャッシュカードの実現・普及が期待されていた。

フランスでは、1990 年から 1993 年にかけて IC キャッシュカードが普及し、おかげでカード偽造による被害額が 1989 年と比較して、1998 年にはおよそ 10 分の 1 に減少したとのことである。

日本では、2001 年 3 月に旧・全国銀行協会が「IC キャッシュカード標準仕様」を制定、2002 年頃から導入検討や実証実験などが行われ、2004 年頃から実際に導入が始まり、我が国も急速に IC キャッシュカードへと移行した。「IC キャッシュカード標準仕様」は公開されておらず詳細は不明だが、カード内の口座情報等の保護や ATM/銀行センターとの通信の秘匿やカード認証等のため、共通鍵暗号 TripleDES/AES や公開鍵暗号 RSA が利用されている模様。

[電子マネーカード]

1990 年に英国で世界初の電子マネーMondex が Mondex International によって開発され、1995 年、英国で実証実験が行われた。VISA International が開発した電子マネーVISA Cash については、1996 年のアトランタオリンピックでデモンストレーション（実証実験）が実施された。

日本でも、1997 年~98 年には東芝も参加し SCJ（Smart Commerce Japan）コンソーシアムによる神戸での VISA Cash 実証実験、1998 年～99 年に SSS（渋谷スマートカードソサイエティ）による渋谷での VISA Cash 実証実験が行われた。

しかし、これまでの実証実験で使用された電子マネーIC カードはいずれも接触型であり、IC カードを端末に差し込んで使う使用時の操作の煩わしさが障害となり、普及には至らなかった。

日本の電子マネー時代を切り開いたのは、非接触 IC カード、FeliCa であり、日本で普及した最初の電子マネーは、Edy である。1999 年頃から FeliCa を用いた電子マネーの実証実験をソニー、ソニーファイナンスが中心に展開、2000 年には FeliCa チップを搭載した「Edy カード」を発行、2001 年には電子マネーEdy の運営会社ビットワレット（後に楽天が買収し楽天 Edy 株式会社へ）が設立され、実用サービスを開始した。

2001 年には、FeliCa チップを搭載した乗車 IC カード「Suica カード」が発行され、2004 年にはショッピングにも使える電子マネーとしてのサービスを開始した。

なお、以降に発行されたプリペイド型電子マネーIC カードも含め、全て FeliCa 方式が採用されており、暗号技術としては共通鍵暗号が使用されている。

③行政分野

[住民基本台帳カード、個人番号カード]

IC カードの高セキュリティ性や利便性に着目し、地方自治体は独自に市民カード、図書館カードや施設予約カードなどに IC カードを導入していたが、2003 年以降は統一的に「住民基本台帳カード」を発行し、本カードを利用した公的個人認証サービスがスタートした。住民基本台帳カードは、行政機関の窓口での本人確認に使用されるだけでなく、ネットを通した様々の行政サービスでの本人確認やネットを経由した送信データの秘匿や改ざん検知ができるよう、暗号技術が搭載されている。具体的には、共通鍵暗号である AES および公開鍵暗号である RSA が搭載されており、また自治体が発行した公開鍵証明書が格納されている。住民基本台帳カードの発行は 2015 年末で終了し、以降は民間での活用を含め、国民の生活活動・社会活動の基盤で活用されることを目指し、更に機能が強化された個人番号カードが発行されることになった。

(6)おわりに

本稿では、現代暗号の時代の内、公開鍵暗号が芽生え始めた 1970 年中頃から 2000 年頃までの、主要な公開鍵暗号アルゴリズムの開発状況・概要、およびその活用が社会に与えた影響など、暗号と社会のかかわりについて述べた。

前稿で紹介した共通鍵暗号を含め、現代暗号の主要なものは 2000 年頃までに開発され、高度情報化が進む社会の安心・安全の維持・向上に大きく貢献し、また、暗号技術の発展が新たな産業の創成・発展を促進してきた。

次の稿では、現代暗号に支えられた高度情報化社会、インターネット依存社会における暗号技術の役割の全体像を整理すると共に、高度化する暗号の悪用問題および対策状況の紹介、現代暗号の限界と次世代暗号の見通しなどについて言及する予定である。

以上

参考資料

①インターネット歴史年表（JPNIC：日本ネットワークインフォメーションセンター）
https://www.nic.ad.jp/timeline/
②電子メール（ウィキペディア）
https://ja.wikipedia.org/wiki/電子メール
③S/MIME（ウィキペディア）
https://ja.wikipedia.org/wiki/S/MIME
④World Wide Web（ウィキペディア）

https://ja.wikipedia.org/wiki/World_Wide_Web
⑤ウェブブラウザ（ウィキペディア）
https://ja.wikipedia.org/wiki/ウェブブラウザ
⑥SSL/TLS 20 年の歩みと動向（JPNIC：日本ネットワークインフォメーションセンター）
https://www.nic.ad.jp/ja/newsletter/No59/0800.html
⑦SSL/TLS 暗号設定ガイドライン
https://www.ipa.go.jp/security/ipg/documents/ipa-cryptrec-gl-3001-2.0.pdf
⑧IC カード（ウィキペディア）
https://ja.wikipedia.org/wiki/IC カード
⑨乗車カード（ウィキペディア）
https://ja.wikipedia.org/wiki/乗車カード
⑩クレジットカード（ウィキペディア）
https://ja.wikipedia.org/wiki/クレジットカード
⑪EMV Integrated Circuit Card Specifications for Payment Systems
Book 2 Security and Key Management
https://www.emvco.com/wp-content/uploads/2017/05/EMV_v4.3_Book_2_Security_and_Key_Management_20120607061923900.pdf
⑫住民基本台帳カード（ウィキペディア）
https://ja.wikipedia.org/wiki/住民基本台帳カード
⑬個人番号カード（ウィキペディア）
https://ja.wikipedia.org/wiki/個人番号カード