電子暗号の発展

—秘匿と認証—

伊藤和行

１　序

インターネットがＩＴ（Information Techonology ＝情報技術）の中核として論じられるようになって久しく，2001 年 3 月政府によって発表された「e-Japan 重点計画」においても超高速インターネット網の整備が重点項目の一つとされている(1)．インターネットが社会において果たす役割が大きなるにつれてより大きな問題となってきたのがセキュリティである．コンピュータ・ウィルスやサーバへの不正アクセスによる被害の増加は著しいものがある．また近年急速に発展してきているインターネットビジネスあるいは電子商取引（e-commerce）においては，情報の保護が大きな問題となっている，たとえばインターネット上でショッピングをする際にはクライアントのクレジット・カード情報を第三者から保護せねばならない．本来インターネットはごく限られた研究者間の情報伝達手段として開発されたシステムであって，セキュリティに関する対策は考えられていなかった(2)．カード情報のような個人情報や経済的に価値のある情報が伝達されることを前提としていないシステムだったのである．ケーブル上を伝わっている電気信号を盗聴することはいくらでも可能であり，改竄すら可能なのである．郵便でたとえるならば，ハガキだけで書留はもちろん封書すら存在しないと言えよう．このようなインターネットのシステム上で経済的活動を行う電子商取引では情報を保護する技術である暗号は不可欠なものとなっているといえよう．「e-Japan 戦略」の中でも，電子商取引の促進や行政の情報化（いわゆる「電子政府」）とともに，その基盤となるネットワークの安全性および信頼性の確保が挙げられており，ネットワーク・セキュリティの重要性は増すまず増大している．また 2001 年 4 月 1 日には，電子署名に対して法的効力を与える「電子署名及び認証業務に関する法律」が施行され，電子商取引が急速に普及していくと予想される(3)．このようなセキュリティ，電子証明および認証の技術的基盤となっているのが本稿で扱う電子暗号であり，以下では 970 年代以降の米国における電子暗号の発展を辿ることにする．

２　ＤＥＳ　電子商用暗号の誕生

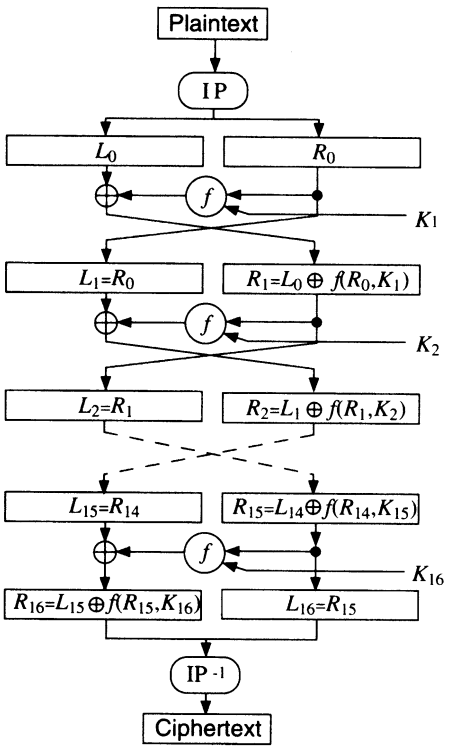
暗号といえばスパイが連想されるように，暗号がもっとも用いられてきたのは軍事・外交という市民の日常とはかけ離れた世界だった(4)．第２次世界大戦においては，各国が暗号解読戦争を繰り広げていたことが知られている．米軍は日本軍が用いた暗号「紫」を解読していたことによって戦況を有利に進めたと言われる．独軍が用いた「エニグマ」（Enigma）という暗号を解読するために，英軍が数学者らからなるチームを組織し，その解読の中心にチューリングがいたことはよく知られている．当時の暗号機は機械あるいは電動機械によっていたが，暗号解読のために Colossus と名づけられたコンピュータが開発されていた(5).

1950 年代以降コンピュータ技術が発展し，経済活動の中でコンピュータが用いられテイクに従って，暗号の商業的な用途が生じてきた．遠隔地にあるコンピュータ間のデータを電話回線等で伝達する際には，第三者からデータを守る必要があったのである．ＩＢＭ（International Buisiness Machine）は, 1960 年代後半から暗号の開発を New York の Yorktown Hieghts Research Laboratory で始めていた. そこで開発された暗号は"Lucifer"と呼ばれ, 1971 年に London の Lloyds に納入され，現金支払システムに用いられた(6).

1970 年代に入り, 国立標準局（NBS = National Bureau of Standards　後に連邦標準技術局 NIST = National Institute of Standards and Technology と改名）は，民事用の標準暗号の必要性を認め，そのアルゴリズムの公募を行った．1973 年 5 月 15 日の「連邦官報」（Federal Register）にアルゴリズムに必要な条件を公表したが，その概要は以下のとおりである(7).

・高いレベルのセキュリティを提供する
・完全に記述され，容易に理解できる
・そのセキュリティは鍵に属し，アルゴリズムの秘匿によるのではない
・すべてのユーザーに利用可能である
・様々なアプリケーションにおける利用に適応できる
・経済的に電子装置に実装可能である
・使用上効率的である
・確証可能である
・輸出可能である

この公募に対する候補が現れなかったので，NBS は翌年 1974 年 8 月 27 日に再公募を行った．これに対して，IBM は"Lucifer"に基づいたアルゴリズムを候補として提出した．NBS は，アルゴリズムの安全性を評価し，連邦標準としてふさわしいか否かを決定するために，国家安全保障局（NSA = National Security Agency）に援助を要請した．NSA は国務省の下にあり, 1952 年に当時の大統領 Harry Truman によって諜報活動に携わる機密機関として設立され，米国政府による通信の盗聴を防ぐとともに他国政府による通信を盗聴することを任務としている(8). NSA は暗号解読のために多くの数学者を雇い，つねに最速のコンピュータを用いており，おそらく世界で最も暗号解読に優れた機関であったと思われる．その意味では，NBS が NSA にアルゴリズムの評価を委ねたことは当然のことであった．そして NSA の指導の下に"Lucifer"に修正を施されたアルゴリズムが「データ暗号化規格」（DES: Data Encryption Standard）として公布された.



DES の暗号化は 56 ビットの鍵を用いて，平文（plain text）を 64 ビットごとのブロックに区切り，非線形処理を行っている．以下では概略を示すことにする(9).

１．各ブロックのデータに対して初期転置 IP を行う．たとえば第 58 ビットは第 1 ビットに，第 50 ビットは第 2 ビットに，第 42 ビットは第 3 ビットに置き換えられる．
２．64 ビットの鍵のうち，56 ビットは鍵の生成に，8 ビットはチェックに用いられる．48 ビットの大きさの鍵が 16 個生成される．
３．最初の 64 ビットのデータ・ブロックを 32 ビットずつに２分し，左側のブロックを L_0，右側のブロックを R_0 とする．
４．第１段階では，掻き混ぜ関数（mangler function）f(R, K)は 32 ビットの R_0 と最初の 48 ビットの鍵 K_1 から 32 ビットの新しいデータ $f(R_0, K_1)$を生成する．この $f(R_0, K_1)$は L_0 に加えられ，次の段階の左側のブロック L_1 となる．一方 R_0 は，そのまま第２段階の左側のブロック L_1 となる．すなわち

$$R_1=L_0 + f(R_0, K_1) \qquad L_1=R_0$$

５．第１段階で行われた処理が 16 回繰り返される．第 n 段階における操作は

$$R_n=L_{n-1} + f(R_{n-1}, K_n) \qquad L_n=R_{n-1}$$

６．16 段階の処理によって生成した L_{16}，R_{16} を置き換えて合成したものに，行程１で行われた初期転置とは逆の最終転置 IP^{-1} が行われる．

アルゴリズムの中心となっているのは掻き混ぜ関数 f(R, K)である．DES の仕組みは基本的には線形であり，DES の強度はこの関数が非線形であることによって高められている．
32 ビットの R は拡大転置という操作によって，48 ビットに拡張され，さらに 48 ビットの鍵と排他的論理和の演算を加えられる．その結果は 6 ビットずつ 8 つのブロックに分割され，各ブロックは 8 つある S-box（換字表）によって変換されるようになっている．復号化は暗号化の過程を逆にすることによってなされる．

NSA がアルゴリズムの開発に関与していたことは，アルゴリズムの中に NSA だけがアクセスできる秘密の仕組んだのではないかという疑惑を招いた．たしかに"Lucifer"では 128 ビットだった鍵の長さが DES では 56 ビットに短くされ，また暗号化を行う S-box（換字表）の仕組みが一部変更されていた．さらに S-box の設計方法が公表されず秘密にされていた．

DES は 1976 年 11 月 23 日に連邦標準として採用され，さらに米国規格協会（ANSI = American National Standards Institute）は，1981 年に DES を民間部門の標準として認可し，"Data Encription Algorithm" (= DEA)と命名した．こうして DES は米国内外において商用暗号の標準として認められ，現在まで経済活動においてもっとも広く用いられてきた．

３　公開鍵暗号の誕生

DES は，商用暗号の時代の到来を知らせるものとして，また最初の本格的な電子暗号であり，またアルゴリズムの公開という点において画期的だった．しかし過去のすべての暗号と同様に情報の送り手と受け手の間で事前に鍵の受け渡しをせねばならないという原理的な制限を持っていた．商業活動で広く使われるためには，それまで情報の交換をしていないような者同士で暗号を用いる際にどのようにして鍵の受け渡しをすればよいのかという問題を解決せねばならなかった．この鍵配布問題は，公開鍵暗号（Public key encryption）というまったく新しい暗号概念によって解決された．

公開鍵暗号は，従来の暗号が暗号化と復号化において同じ鍵（共通鍵）を用いていたのに対し

て，暗号化の際と複合化の際に異なる鍵を用い，さらに暗号化に用いた鍵によっても暗号を復号化すなわち解読できないというものである．すなわち一つの暗号の処理に際して，セットになった二つの異なる鍵を用いるのである．受信者はまず自分の暗号化鍵を公開し，送信者はその公開鍵を用いて送りたい情報を暗合化する．そして暗号を受け取った受信者は，もう一つの鍵である公開していない秘密鍵を用いて元の情報に変換することができるが，他の者は暗号化鍵しか持っていないので，暗号を解読することはできないのである．

3.1 Diffie-Hellman 鍵交換方式

この公開鍵のアイデアを最初に提示したのは，スタンフォード大学の研究員だった Whitfield Diffie と Martin Hellman だった．彼らは 1976 年に発表した論文「暗号学の新方向」(10)において，誰かに盗聴される可能性のある通信手段によって，メッセージを暗号化するために用いる共通鍵を共有する方法を論じた．彼らの方法は Diffie-Hellman の鍵交換方式と呼ばれている(11).

暗号システムは暗号化変換と復号化変換という二つの部分から構成され，さらにそれらは，一方が与えられても対応する他方を見いだすことはできないようなものでなければならない．各利用者は一組の逆変換を E と D を生成して，復号化変換 D を秘密にし，暗号化変換 E を公開すればよいのである．このような性質をもつ関数は一般に「一方方向の落とし戸関数」（one way trapdoor function）と呼ばれ，その性質をわかりやすく述べると次のようになる

１．y = f(x)を計算して y を計算することは容易である．

２．y = f(x)であるような y に対して，$x=f^{-1}(y)$を計算して x を求めるのは，関数 f に組み込まれたある情報すなわち「鍵」を知っていれば容易であるが，知らなければ計算量の点から困難である．

彼らが「落とし戸一方向関数」として提案したのは，剰余体で累乗計算を行う離散対数である(12)．任意の素数 q と α，そして X (1≦X≦q-1)を選び，Y を次のように定義する．

$Y = \alpha^X \bmod q$（ただし N mod q は N を q で割ったときの余りを意味する）

このとき X は，α を底とする離散対数によって，法 q において次のように表される．

$X = \log_\alpha Y \bmod q \ (1 \leqq X \leqq q-1)$

X から Y を求めることは比較的容易であるが，反対に Y から X を求めることは非常に困難でなのである．この点を利用したのが彼らの方法である．

実際には，各ユーザーは自然数の組｛1, 2,…, q-1｝から任意の数 X_i を選び，各 X_i に対して $Y_i = \alpha^{Xi} \bmod q$ を求め，それらを公開ファイルに置いておく．ユーザー i と j が秘密裏に通信を行いたいときには，$K_{ij} = \alpha^{XiXj} \bmod q$ を鍵として用いればよい．このときユーザー i は公開ファイルから Y_j を得ることによって K_{ij} を知ることができる．またユーザー j も公開ファイルから Y_i を得ることによって K_{ij} を知ることができる．しかし他のユーザーは X_i も X_j も知らないので，Y_i と Y_j から K_{ij} を求めねばならないが，これは上で述べた離散対数の性質から非常に困難である．したがってユーザーi とユーザーj は容易に鍵 K_{ij} を知ることはできるが，他の誰かが回線を盗聴したとしても鍵 K_{ij} を見いだすことはできないのである．

二人のユーザーは共通鍵を共有した後は，共通鍵暗号を用いてメッセージの交換を秘密裏に行うことができる．

この方法はユーザーがオンラインで情報を交換することが必要であったし，次節で紹介する RSA 暗号のように，メッセージ自体を暗号化するものではなく，またメッセージに電子的に署

名することもできなかった．しかしながら，第三者によって情報を盗聴される可能性のある通信手段において秘密裏に共通鍵を共有するという限定された機能の点では RSA 暗号よりも効率がよく，インターネットにおける鍵交換の手段として良く用いられている．

3.2 RSA 公開鍵暗号

実用されることになった最初の公開鍵暗号を考案したのは，MIT の R. L. Rivest, A. Shamir, L. Adleman だった．彼らは Diffie-Hellman の論文に刺激を受け，論文「デジタル署名を得る方法と公開鍵暗号システム」(13)において，前もって情報を交換することなく鍵情報を安全に送り仕組みを考案し，またシステムを逆にすることによって署名の確認も可能なことを示した．

公開鍵システムでは，各ユーザーは暗号化の手続き E を公開するが，対応する復号化の手続き D は非公開にする．その手続きは以下の四つの条件を満たしている．

１．暗号化した形態のメッセージMを復号化することによってMに戻る．すなわち D(E(M))= M

２．E と D は容易に計算可能である．

３．ユーザーは E を公開することによって，D を計算する容易な方法を公開するのではない．すなわちそのユーザーしか E あるいは D によって暗号化されたメッセージを復号化できない．

４．もしメッセージMが最初に復号化され，次いで暗号化されるならば，その結果は M である．すなわち E(D(M))=M

条件１，２，３を満たすとき関数 E は「一方向落とし戸関数」と呼ばれ，さらに４の条件をも満たすものは 「一方向落とし戸置換」（trap-door one-way permutation）と呼ばれる．公開鍵暗号では，各ユーザーは公開の暗号化手続き E（公開鍵）と非公開の復号化手続き D（秘密鍵）を持っている．たとえばアリスの鍵を E_A，D_A，ボブの鍵を E_B，D_B とすると，ボブがアリスにメッセージを送る過程は次のようになる．

１．ボブは公開ファイルからアリスの公開鍵 E_A を取り出す．

ボブはそれによって暗号化したメッセージ $E_A(M)$をアリスに送る．

２．アリスは $D_A(E_A(M))=M$ を計算することによってメッセージを復号化する．

性質３によって暗号 $E_A(M)$を復号化できるのはアリスだけである．また逆にアリスがボブにメッセージを送るためには，ボブの公開鍵 E_B を用いればよい．彼らが安全な情報伝達を行うために前もって情報の交換する必要はなく，公開ファイルに暗号化に必要な公開鍵を置くだけでよいのである（実際には公開ファイルにある公開鍵が本当に当人のものであることを保証する機関が必要となる）．

また４の条件を満たすことによってデジタル署名が可能になる．すなわちあるメッセージを受け取った受信者がそのメッセージが特定の送信者から送られてきたことを確認できるのである．ボブがアリスに「署名した」メッセージを送る過程は次のようになる．

１．ボブは D_B を用いてメッセージ M に対する彼の署名 $S=D_B(M)$を計算し，署名 S を E_A を用いて暗号化してアリスに $E_A(S)$を送る．

２．アリスは受け取った暗号 $E_A(S)$を D_A によって復号化し，S を得る．

ついで公開ファイルにある E_B を用いて，$M=E_B(S)$を得る．こうしてアリスは一組のメッセージと署名(M, S)を得る．

ボブは後でこのメッセージ S をアリスに送ったことを否定できない．というのは，彼以外誰も

$S=D_B(M)$を作ることはできないからである．またアリスはメッセージ M を M'に改変することができない．なぜなら，彼女は対応する署名 $S'=D'_B(M)$を作ることができないからである．こうしてこのメッセージ S がボブのものに他ならないことが確認されるのである．

彼らがこのアイデアをアルゴリズムとして具体化するために用いたのは，大きな素数の積を因数分解することが非常に困難であることだった．すなわち公開鍵として二つの自然数の組(e, n)を用いるのである．あるメッセージ M を暗号化するためには，その数を e 乗し，Me を n で割ったときの余り（法 mod n）を暗号文 C とする．暗号文を復号化するためには，他の自然数 d によって d 乗して再び n で割って余りを調べればよい．暗号化と復号化のアルゴリズム E と D は次のようになる．

メッセージ M に対して，C = E(M) = Me (mod n)

暗号文 C に対して，D(C) = Cd (mod n)

ここで暗号鍵（公開鍵）は一組の自然数(e, n)であり，復号鍵（秘密鍵）ももう一組の自然数(d, n)である．これらの数は次のようにして決められる．

１．二つの非常に大きな素数 p と q を選び，その積を n=p*q とする．n は公開されるのが，n を因数分解するのはきわめて困難なので，p と q は実際的には他の誰にもわからない．

２．(p-1)*(q-1)に対して互いに素であるような大きな自然数 d を取ると，d は次の式を満たす．

gcd (d, (p-1)*(q-1)) = 1

３．自然数 e は，法(p-1)*(q-1)における d の積に関する逆元として求められる．

e*d =(d, (p-1)*(q-1)) = 1

このようにして定義された二つの自然数の組(e, n)，(d, n)は各々公開鍵，復号鍵となる．この暗号システムの安全性は大きな数の因数分解が困難なことによっているので，実際に用いるためには当時のシステムでは 80 桁の数であれば安全であり，200 桁の数であれば将来も安全だろうと彼らは推測している．しかし 1000 桁の整数演算を行うためには当時としては膨大な演算能力が必要であり，実用化されるには 1980 年代後半を待たねばならなかった．考案者の Rivest, Shamir, Adleman はこのアルゴリズムに対して特許を取り，1982 年に RSA Data Security 社という会社を設立したが，経営が軌道に乗るのはインターネットが普及した 90 年代に入ってからだった(14)．現在では，公開鍵暗号システムとして RSA 暗号の他に，離散対数を用いた ElGamal 暗号，楕円曲線上の離散対数問題に基づく楕円曲線暗号などが考案され実用化されている．

４．Clipper 論争

NSA は，DES の制定におけるように 1970 年代までは米国内における暗号に関するすべての活動をその制御下に置くことに成功していた．それゆえ，彼らのコントロール外の暗号や暗号研究者が現れることは NSA にとっては大きな衝撃であり，また許されないことでもあった．公開鍵暗号の誕生はまさにそうような事態の発生を意味していた．Rivest は公開鍵暗号を発表した際に，その論文のコピーを，MIT に返信用の切手を貼った封筒を送った者には誰にでも提供すると発表した．それに対して NSA の Joseph Meyer が，暗号システムを公表することは国家保安法違反になるという警告を述べた手紙を，当時計画されていた暗号学の研究会の主催者に送ったのである．その結果，最終的にコピーの発送が再会されるまでにはほぼ１年を要した(15)．

しかし 1980 年代に入り，コンピュータ研究者の中から多くの暗号の研究者が現れて来るにつ

れ，彼らのコントロールには限界が見え始めていた．さらに 1991 年には，Phil Zimmermann が PGP（Pretty Good Privacy）という RSA 公開鍵暗号を用いた暗号ソフトをフリーウェアとしてインターネット上で配布し，一気にこの暗号ソフトは世界中に広まった．米国政府は国際武器流通規定（ITAR = International Traffic in Arms Regulations ）によって PGP が国外に出ることを阻止しようとしたが，ときはすでに遅かった．この政府の規制に対して，インターネット上で世界中のプログラマーが集まってチームを構成し，PGP の開発が進められ，新しいヴァージョンは国外でリリースされ，米国に逆輸入されたのである．Zimmermann は 1993 年 2 月に武器輸出規制違反の疑いで召喚されたが，最終的に不起訴に終わっている(16).

米国政府とくに NSA と暗号研究者の関係をさらに悪化させたのは，1993 年 4 月に発表された新しい暗号政策「鍵寄託構想」（Escrowed Encryption Initiative）である(17)．その考えは，民間に対して通信を安全なものとする強力な暗号システムを提供する一方で，捜査が脅かされないようにするというものである．そのために暗号鍵を第三者機関に寄託することを義務づけ，捜査当局は裁判所の許可の下で，この暗号鍵を用いて通信内容の暗号解読を行うのである．このための秘密鍵暗号アルゴリズム Skipjack が NBA によって開発され，耐ジャンパー機能を備えた Clipper Chip というハードウェアに実装されることになっていた．"Skipjack"は通信ごとに 80 ビットの鍵を生成し，送信者と受信者は公開鍵暗号を用いてこの鍵を共有し，メッセージを暗号化する．その際に，そのチップを同定する情報を含むフィールド Law Enforcement Access Field が同時に送られる．捜査の際には，二つの鍵寄託機関に分割されてある二つの master key を入手して結合し，LEAF によって，その通信の際の鍵を求めて暗号の復号化を行うのである．

この Clipper 構想には，情報技術に携わる技術者・研究者や個人のプライバシー擁護論者などから多くの批判が集まり，社会的に大きな問題となった．批判の理由は，捜査機関が個人のプライバシーを侵するのではないかという懸念の他，Skipjack のアルゴリズムが非公開であるために安全性を評価できないこと，Clipper チップが特定のメーカー（Mykotronx）によって独占的に提供される点などがあった．多くの批判の中，1994 年に２月に，鍵寄託は任意的なものであるとしつつも，NIST が Clipper を「寄託鍵標準」（Escrowed Encryption Standard）として「連邦情報処理標準」（FIPS = Federal Information Processing Standard）に認定し，実質的な暗号標準にすることを目指した(18)．しかし 7 月には，ベル研究所の研究者 Matt Blaze が，LEAF のデータを変更して捜査機関がメッセージの復号化を妨げる方法を発見した(19)．こうしてこの年の中頃には，政府はこの構想の再検討を余儀なくされ，その代替案を民間との協力の下で検討していくことを表明した．

1995 年 12 月に，政府は鍵寄託構想を暗号の輸出規制緩和に絡めて押し進めることを試みた．鍵の長さが 64 ビット以下の暗号に関しては，鍵寄託システムが実装されているならば輸出を認めるという，この措置は Clipper 構想の姿を変えたものとして，Clipper II あるいは Son of Clipper と呼ばれた．

また 1996 年 5 月には, 政府は, 草案"Enabling Privacy, Commerce, Security and Public Safety in Global Information Infrastructure"を発表し，「鍵管理インフラストラクチャ」（Key Maganement Infrastructure）の確立を提唱した．これは，公開鍵暗号における秘密鍵を鍵寄託機関に寄託させるというものであり，そのことから Clipper III と呼ばれている．ただし鍵の寄託が任意であり，暗号アルゴリズムの選択も自由とされていることは，それまでの批判を考慮したものだった．

さらに 1996 年 10 月 1 日に政府は，ゴア副大統領の公式声明の形で，それまでの暗号政策の転換を発表した．それでは，不評だった「鍵寄託」（key escrow）を「鍵復元」（key recovery）に置き換え，捜査のための「鍵寄託」から紛失した鍵の復元へと視点を変えることをねらっている．さらに key recovery 技術の確立以前でも，許可から 2 年以内で実装することを条件として，56 ビット以下の暗号の輸出を認めた．この政策は，1996 年 12 月に，商務省による「輸出管理規制」（Export Administration Regulation）の改訂により具体化され，それまで暗号は武器として国務省の管轄下にあったのが，商務省に管轄が移された．

1997 年以降も政府は政府主導の「鍵管理インフラストラクチャ」構想の実現を産業界に働き続けたが，ほとんど実現を見ずに頓挫してしまった．一方米国の暗号ソフトを開発利用していた企業は，国内ではより強力な暗号を用いながらも，輸出の際にはより弱い暗号を用いねばならないことによる国際的な競争力の低下を政府に訴え，様々な形で働きかけを行っていった．この結果，1998 年以降政府は暗号輸出規制を次のように徐々に緩めていった(20).

・1998 年 9 月 22 日施行規則

銀行および金融機関に対しては，一回の審査の後，データ復元要件を満たさなくとも，45 ヶ国に対して輸出が認められた．

・1998 年 12 月 31 日施行規則

一回の審査の後，すべての鍵長 56 ビット以下の暗号の輸出が認められた（テロリスト支援国：キューバ，イラン，イラク，リビア，北朝鮮，スーダン，シリアを除く）．

・2000 年 1 月 12 日施行規則

技術審査の後，任意の長さの鍵を用いる暗号の輸出が認められた(21).

・2000 年 10 月 19 日施行規則

15 の EU 諸国および 8 ヶ国（オーストラリア，チェコ，ハンガリー，日本，ニュージーランド，ノルウェイ，ポーランド，スイス）に対しては，申請後，技術審査の結果を待たずにすぐに製品の輸出が可能になった．

こうして米国政府による暗号輸出規制は実質上撤廃されてしまったのである．また Clipper もほとんど普及することなくその指名を終えてしまったようである．そのチップを組み込んだ電話機は ATT によって製品化されたが，政府関係で購入されただけでほとんど民間では私用されたなかった．また NSA は Clipper を用いた PCMCIA カード Fortezza を開発したが，これもあまり使用されずに終わっている．Clipper 問題は，1990 年代に起こったインターネットを中心とする情報技術の急速な進展に米国政府が対応しきれなかったことを示していると言えよう．

５．DES から AES へ

DES は，1977 年以降，米国内だけでなく，世界中において，経済活動とくに金融分野において事実上の標準暗号として用いられてきた．しかし 1990 年代に入り，「差分解読法」や「線形解読法」といった解読方法が発見され，また鍵の長さが 56 ビットと短いために，コンピュータの技術的発展の結果，「鍵の全数探索」（Exhaustive Key Search）が現実的なものとなり，その安全性の保証が困難となってきた．実際 RSA Security 社が，DES 暗号の安全性の低下を実証することを目的として行った第三回 DES 暗号解読コンテスト（DES Challenge，1999 年 1 月）では，インターネット上で約 10.000 台のコンピュータを用いて 22 時間 15 分で解読されてしまっ

た(22)．現在一部では，DES を補強したトリプル DES（Triple DES）が用いられている．これはその名の通り，二つないし三つの暗号鍵を用いて DES の暗号化過程を三回繰り返すことによって，DES の鍵長を長くするものである．

このような状況を踏まえ，NIST は 1997 年 1 月 2 日に DES 代わる新しい標準暗号 AES（Advanced Encryption Standard）を公募すると発表し，アルゴリズムの必要条件（Minimum Acceptability Requirements），評価基準，選定過程などについてコメントを募集した(23)．その要件と評価基準は，(1)公開で決定される，(2)共通鍵ブロック暗号，(3)鍵長は可変，(4)ハードウェアにもソフトウェアにも実装可能，(5)自由に利用可能，あるいは米国規格協会（ANSIAmerican National Standards Institute）の特許権方針に従って利用可能である．また評価基準としては，(1)安全性，(2)計算効率，(3)必要なメモリー量，(4)ハードウェアおおびソフトウェアの適応性，(5)単純性，(6)柔軟性，(7)ライセンス要件が挙げられている．さらにこの選定にあたっては，Clipper 論争での失敗を踏まえ，公募されたアルゴリズムを公開し，研究者からの評価を仰ぎ，それを踏まえて選考を進めていくとした．

NIST は専門家からのコメントを踏まえて，同年 9 月 12 日には最終的な公募要項を発表し，満たすべき用件，評価基準，評価日程が提示された．

それによれば，アルゴリズムの用件とは，

(1)共通鍵暗号であること

(2)ブロック暗号であること

(3)鍵長は 128 ビット，192 ビット，256 ビットが利用可能，またブロック長は 128 ビットが利用可能であること．

評価基準としては，

(1)安全性（解読に必要な労力）

(2)コスト

(i)ライセンス要件　特許使用料が無料であること

(ii)計算効率

(iii)必要なメモリー量

(3)アルゴリズムと実装上の特徴

(i)柔軟性

(ii)ハードウェアやソフトウェアへの適用性

(iii)単純性

選定のスケジュールとしては，二回の技術評価を行って候補を絞り最終選定を行うが，その際には評価会議を公開で行い，さらに最終選定の後にも期間を定めて一般からのコメントを求めることとなっていた．

以下時系列に従って最終選定までの過程を追っていこう．

(1)アルゴリズムの募集（1998 年 6 月 15 日締め切り）

(2)第一回選考会議（First AES Candidate Conference (AES1), 1998 年 8 月 20-22 日）

15 の候補を発表：CAST-256, CRYPTON, DEAL, DFC, E2, FROG, HPC, LOKI97, MAGENTA,

MARS, RC6, RIJNDAEL, SAFER+, SERPENT, TWOFISH(24)

(3)第二回選考会議（Second AES Candidate Conference (AES2), 1999 年 3 月 22-23 日）

(4)最終候補の選定（1999 年 4 月 15 日）

MARS, RC6, RIJNDAEL, SERPENT, TWOFISH(25)

(5)第三回技術評価会議（20009 年 4 月 23-14 日）

(6)最終選定（2000 年 10 月 2 日）

RIJNDAEL（２人のベルギー人 Joan Daemen (Proton World International)と Vincent Rijmen (Katholieke Universiteit Leuven)による）

(7)AES に関する「連邦情報処理標準」（Federal Information Processing Standard (FIPS) ）草稿を公表（2001 年 2 月 28 日）(26)

90 日間（2001 年 5 月 29 日まで）にわたり，一般からのコメントを募集した後，それらを検討した上で夏には AES を標準として制定する予定となっている．このように各段階において研究者のコメントを広く求めて選定を進めていく姿勢は Clipper 論争という苦い経験から学んだものだろう.我が国においてもこれに倣った形で,2002 年度までの暗号技術の標準化を目指し,2000 年 6 月に「国電子政府システムに適用可能な暗号技術」を情報処理振興事業協会（IPA）が公募し,「暗号技術評価委員会」によって技術評価の途中にある(27).

６．公開鍵インフラストラクチャ

1990 年代にインターネット上での経済活動が大きく普及する一方で，その基盤としての公開鍵の利用を可能にする「公開鍵インフラストラクチャ」（PKI = Public Key Ingrastructure）の確立が進められてきた．公開鍵暗号は，不特定多数がアクセスするインターネット上で安全な情報通信を可能にするものであるが，広く用いられるためには，その発行，配布，保持，認証，廃棄等を行う認証機関（Cetification Authority）の設立とその業務を行うための技術の確立が不可欠だったのである．

公開鍵暗号の普及を目指した RSA Security 社は,1991 年に公開鍵インフラとして PKCS（Public Key Cryptography Standard）を発表した(28)．さらに 1995 年には，認証と電子認証証明書の発行管理を行う専門機関を独立させ，AT&T，Microsoft，Visa などの多くの企業の協力によって Verisign 社を設立している(29)．ほぼ同時期に Netscape 社は，暗号通信や認証機能を備えた通信プロトコル SSL（Secure Socket Layer）を発表し，ウェブ・ブラウザーNavigater に実装した．これは公開鍵暗号を用いて，セッション鍵を生成し，その鍵によってデータを共通鍵暗号化して通信するものである(30)．この通信を利用して電子商取引を行うウェブサイトの大部分は，Verisighn 社から認証を受けており，その電子認証証明書は業界標準となっていると言えよう．

NIST は「連邦情報処理標準」（FIPS）として, PKI に関して FIPS140-1（1997 年）と FIPS186-1（1998 年に）を制定している．前者（Security Reguirement for Cryptographic Modules）は秘密鍵を保管するためのモデュールが満たすべき条件を４つの安全レベルにおいて定めており，後者（Degital Signature Standard）は電子認証に用いる暗号アルゴリズムを定めている(31)．さらに NIST は米国連邦政府が利用する PKI である「連邦公開鍵インフラストラクチャ」（FPKI = Federal Public Key Infrastructure）の策定作業に入っており，認証関連技術に関する検討を行っている(32).
我が国でも「電子署名及び認証業務に関する法律」の施行に伴い，国は民間認証機関を「認定」

する業務を「日本品質保証機構」に委託し，同機構では調査機関として「電子署名・認証調査センター」を発足している(33).

このように我が国でも本格的な電子署名に基づく電子商取引や電子行政の時代を迎えようとしているが，しかし電子技術に伴う大きな危険も潜んでいることもわすれてはならない．実際 2000 年 3 月 2 日に VeriSign 社は，1 月 29 日と 30 日に Microsoft 社の社員になりすました何者かに２件の証明書を発行したことを発表した(34)．すぐに同社は証明書を無効にし，証明書廃棄リスト（CRL）に追加したということである．しかしこの証明書はプログラムやマクロの署名に用いられるのものであり，これを悪用すれば，Microsoft 社の名を語って，ソフト利用者にコンピュータウィルスなどを送ることもでき，非常に大きな被害を引き起こす可能性もある(35).

注

(1) 首相官邸ＨＰ「e-Japan 重点計画概要」（http://www.kantei.go.jp/jp/it/network/dai3/jyuten/）を参照．項目としては，「世界最高水準の高度情報通信ネットワークの形成」，「教育及び学習の振興並びに人材の育成」，「電子商取引等の促進」，「行政の情報化及び公共分野における情報通信技術の活用の推進」，「高度情報通信ネットワークの安全性及び信頼性の確保」が挙げられている．

(2) インターネットの仕組みに関しては，『岩波講座インターネット１インターネット入門』，岩波書店，2001．インターネットの歴史に関しては，Hafner and Lyon『インターネットの起源』,加地永都子･道田豪訳, アスキー, 2000；Abbate, J., *Inventing the Internet*, Cambridge, Mass., 1999. セキュリティに関しては，佐々木 良一『インターネットセキュリティ入門』，岩波新書，1999；山口英・鈴木裕信編『情報セキュリティ』（bit 別冊），共立出版，2000 などを参照．また現状に関しては，情報処理振興事業協会(IPA)セキュリティセンター のＨＰ（http://www.ipa.go.jp/security/）を参照.

(3) 経済産業省のＨＰ（http://www.meti.go.jp/policy/netsecurity/）参照．なお国に代わってその認定を行う機関として「日本品質保証機構」が「調査機関」として認定されている（http://www.jqa.or.jp/j/other/esac.html）. また米国では 2000 年 10 月 1 日に電子署名法（Electronic Signatures in Global and National Commerce (E-Sign) Act）が施行された（http://thomas.loc.gov/cgi-bin/query/z?c106:S.761:）.

(4) 暗号の歴史に関しては，Kahn, D., *The Codebreakers. The Story of Seceret Writing*, New York, 1967［部分訳は，カーン『暗号戦争』，秦郁彦・関野秀夫訳，早川文庫，1968］；キッペンハーン『暗号攻防史』，赤根洋子訳，文春文庫，2001.

(5) チューリングに関しては，Hodges, A., *Alan Turing: the Enigma*, New York, 1983. コンピュータの歴史については，キャンベル-ケリー・アスプレイ『コンピューター200 年史―情報マシーン開発物語―』，山本菊男訳，海文堂，1999.

(6) 電子暗号の歴史に関しては，Garfinkel 『ＰＧＰ暗号と電子署名』，山本和彦監訳，オライリー・ジャパン，1996；『デジタル・ウォーズ　暗号～日米ビジネス戦略』，日本放送出版協会，1997；Diffie, W. and Landau, S., *Privacy on the Line: The Politics of Wiretapping and Encryption*, Cambridge, Mass., 1998; Levy, S., *Crypto: How the Code Rebels Beat the Government – Saving Privacy in the Digital Age*, New York, 2000. 暗号理論の概説書としては，

辻井重男『暗号―ポストモダンの情報セキュリティ』，講談社，1996；今井秀樹『暗号のおはなし』，日本規格協会，1993；一松信『暗号の数理―作り方と解読の原理』，講談社，1980；長田順行『暗号―原理とその世界』，ダイヤモンド社，1971；『現代暗号とマジックプロトコル』（臨時別冊・数理科学），サイエンス社，2000，

(7) Schneier, B., *Applied Cryptography: Protocols, Algorithms, and Source Code in C*, 2nd ed., New York, 1995. p.266. 暗号理論に関しては，池野真一・小山謙二『現代暗号理論』，コロナ社，1986；岡本龍明・山元博資『現代暗号』，産業図書，1997；Stinson『暗号理論の基礎』，櫻井幸一訳，共立出版，1996；カウフマン・パールマン・スペシナー『ネットワークセキュリティ』，石橋啓一郎他訳，プレンティスホール，1997；

(８) NSA に関しては，Bamford, J.: *The Puzzle Palace: A Report on America's Most Secret Agency*, New York, 1983．また NSA のＨＰ（http://www.nsa.gov/）を参照．

(9) 図は，Schneier, *Applied Cryptography*, p.271 による．

(10) Diffie, W. and Hellman, M., "New Directions in Cryptography," *IEEE Transactions of Information Theory*, November, 1976, pp. 644-654.）また注(7)の文献および伊藤和行「暗号の革命―公開鍵暗号の誕生―」，『情報倫理学資料集 II』，日本学術振興会未来開拓学術研究推進事業電子社会システム「情報倫理の構築」プロジェクト，2000，pp. 37-49.

(11) 彼らは前年の 1975 年に「マルチユーザ暗号方式」（''Multi-User Cryptographic Techniques''）という論文を National Computer Conference で発表している．そこでは，複数のユーザ間で暗号の鍵を交換する考えが提示されていたが，具体的なシステムについては何も述べられていなかった．またカリフォルニア大学バークレー校の学生だった Ralph Merkle は，独自に鍵交換の問題に取り組んでいたことが知られている．Cf. Merkle, R. C., ''Secure Communications Over Insecure Channels,'' *Communications of the ACM*, 21, April 1978, pp. 294-299.

(12) 剰余体とは，自然数をある自然数で割ったときの余りの集合のことで，n を p で割ったときの余りは n mod n と表される．たとえば 45 を 7 で割ったときのときの余りは 3 であるから，3 = 45 mod 7 となる．通常 p の剰余類は mod(=modulo) p，法 p と呼ばれる．

(13) Rivest, R. L., Shamir, A., and Adleman, L., "A Method for Obtainin Digital Signatures and Public-Key Cryptosystems," *MIT Laboratory for Computer Science*, Technical Memo 82 April 1977, reprinted in *Communications of the Association for Computing Machinery*, Vol. 21, February, 1958, pp. 120-126.

(14) 現在の RSA Security 社（http://www.rsasecurity.com/）.

(15) この事件が大きな話題になったのは，雑誌 Scientific American で「数学ゲーム」を担当しているマーチン・ガードナーが Rivest らの論文を誌上で取り上げたことによるところが大きい．ガードナー「落とし戸暗号」，「落とし戸暗号その後」，一松信訳，『落とし戸暗号の謎解き』［ガードナー数学ギャラリー］，丸善，1992 参照．

(16) 詳しくは，Garfinkel 『ＰＧＰ暗号と電子署名』を見よ．なおこの際にプログラムをプリントアウトしたものは著作物とみなされ，輸出の規制外とみなされたことから，ヨーロッパのエンジニアはそれを利用して PGP のプログラムを入手した．Zimmermann はソース・コードを本として出版している（PGP : Source Code and Internals, MIT Press, 1995）．Zimmermann は

1996 年に PGP 社（http://www.pgp.com/）を設立したが，1997 年に Network Associates 社（http://www.nai.com/）に買収された．

(17) NIST のＨＰ（http://csrc.nist.gov/keyrecovery/clipper.txt）参照．Cf. 岩下直行・宇根正志「キーリカバリー構想を巡る最近の情勢について」，IMES Discussion Paper No. 97-J-8，日本銀行金融研究所，1997（http://www.imes.boj.or.jp/jdps/97-J-08.html）；Bert-Japp Koops, “Crypto Law Sruvey,” (http://cwis.kub.nl/~frw/people/koops/cls2.htm); Schneier, B. and Banisar, D., The Electric Privacy Papers, New York, 1977（この著作には 1995 年までの米国政府の発表を含む関係する資料が収められている）．

(18) http://www.itl.nist.gov/fipspubs/fip185.htm.

(19) M. Blaze, “Protocol Failure in the Escrowed Encryption Standard.” *Proceedings of Second ACM Conference on Computer and Communications Security*, Fairfax, VA, November 1994 (http://www.crypto.com/papers/eesproto.pdf).

(20) 輸出管理局（Bureau of Export Administration = BXA）のＨＰ（http://www.bxa.doc.gov/Encryption/）を参照．

(21) それまでは各メーカーは国内向けと国外向けという二つの version を用意していた．Netscape Navigater を例に取れば，Netscape 社の Web Site には米国内向けの 128 ビットの暗号を用いたものと，国外向けの 40 ビットの暗号を用いたものがあった．

(22) RSA Security 社のＨＰ（http://www.rsasecurity.com/rsalabs/des3/index.html）参照．なお第１回目のコンテスト（1997 年 1 月）の結果は 140 日，２回目のコンテスト（98 年 1 月）の結果は 40 日だった．

(23) NIST の Home Page に詳しい資料が掲載されてるいる（http://csrc.nist.gov/encryption/aes/）．宇根正志「AES（Advanced Encryption Standard）について」，IMES Discussion Paper No. 97-J-16，日本銀行金融研究所，1997 (http://www.imes.boj.or.jp/jdps/97-J-16.html)；太田和夫「暗号解読法の進歩と時期米国標準暗号(AES)制定の動き」，『現代暗号とマジックプロトコル』，pp.25-37.

(24) 各暗号のアルゴリズムに関しては，宇根正志「最近の AES を巡る動向について」，IMES Discussion Paper No. 98-J-21，日本銀行金融研究所，1998 (http://www.imes.boj.or.jp/jdps/98-J-21.html)；宇根正志・太田和夫「共通鍵暗号を取り巻く現状と課題―DES から AES へ―」，IMES Discussion Paper No. 98-J-27，日本銀行金融研究所，1998 (http://www.imes.boj.or.jp/jdps/98-J-27.html).

(25) 第一回技術評価に関しては，杉田誠・今井秀樹「暗号の評価技術：AES 暗号を例として」，『現代暗号とマジックプロトコル』，pp.13-24.

(26) http://csrc.nist.gov/publications/drafts/dfips-AES.pdf.

(27) 情報処理振興事業協会（IPA）のＨＰ（http://www.ipa.go.jp/security/enc/CRYPTREC/index.html#kobo）参照．

(28) 現在は Ver.2 である（http://www.rsasecurity.com/rsalabs/pkcs/index.html）．

(29) http://www.verisign.com．もう一つの主要な認証会社として CyberTrust 社があるが，2000 年に Baltimore 社に買収された（http://www.baltimore.com）．我が国では，他に日本認証サービス社が認証業務を行っている（http://www.jcsinc.co.jp/）．

(30)　現在は Ver.3 となっている(http://home.netscape.com/eng/ssl3/)．SSL を用いている場合には URL が https で始まっている（通常の場合は http）．

(31)　http://csrc.nist/gov/publications/fips140-1/fips140-1.html; http://csrc.nist/gov/encruption/dss/fr981215.htm. なお 2000 年 2 月に新しい 186-2 が施行されている（ttp://csrc.nist/gov/publications/fips186-2/fips186-2.pdf）．谷口文一「金融業界における PKI・電子認証について―技術面，標準化に関する最近の動向を中心に―」，『金融研究』，日本銀行金融研究所，2000，4，pp.15-54；アダムス・ロイド『ＰＫＩ公開鍵インフラストラクチャの概念，標準，展開』，鈴木優一訳，ピアソン・エデュケーション，2000.

(32)　NIST のＨＰ（http://csrc.nist/gov/pki/）参照．PKI に関する国際的標準としては，国際通信連合下の通信標準セクターが作成した ITU-T Recommendation X.509 があり，公開鍵証明書や公開鍵証明書廃棄リスト（CRL = Certificate Revocation List）の使用を規定している．現在施行されているものは 1996 年に制定されたもので，公開鍵証明書については Ver.3，公開鍵証明書廃棄リストについては Ver.2 となっている．

(33)　http://www.jqa.or.jp/j/other/esac.html.

(34)　http://www.verisign.co.jp/press/alert/security_alertert20010321.html.

(35)　Microsoft 社はこの問題に対応した修正プログラムを配布している（http://www.microsoft.com/japan/technet/security/prekb.asp?sec_cd=MS01-017）．

(京都大学)