暗号と社会のかかわり史(2)

（株）IT 企画　才所敏明

(1) はじめに

本稿は、第二次世界大戦終了までの古代・古典・近代暗号の時代を対象に記載した「暗号と社会のかかわり史」の第 2 稿である。第二次世界大戦終了後、暗号技術は飛躍的に発展し現代暗号の時代となった。本稿では、現代暗号の特徴・概要をまず紹介し、引き続き現代暗号を構成する共通鍵暗号方式の第 1 世代の暗号とその社会とのかかわりについて紹介する。なお、第 1 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) 現代暗号の概要（解説）

現代暗号は、第 1 稿で説明した古代・古典暗号で使用された操作である換字・転置の考えを踏襲しつつ、コンピュータを利用したはるかに複雑な操作に基づく共通鍵暗号方式と、数学的に難しい問題をベースに考案された公開鍵暗号方式の、大きくは二つのカテゴリに分類され、それぞれ発展を続けている。

現代暗号は、そもそも想定する利用者も従来とは異なっている。これまでの暗号利用者は、限られた仲間内での安全な情報伝達を目的とした国や組織等の紛争当事者であったのに対し、現代暗号の場合は、コンピュータ/ネットワーク社会の急伸に伴い、全ての組織・個人を利用者と想定し発展してきた。

また、従来の暗号がもっぱら情報の秘匿を目的とし利用されてきたのに対し、現代暗号では秘匿に加え、情報や情報作成者の認証（データが改ざんされていないかどうかの確認やデータ作成者の確認等）のためにも利用されており、用途も拡大してきた。

①現代暗号の特徴・・・暗号方式の暗号アルゴリズムと暗号鍵への分離

コンピュータ/ネットワークは組織・個人の日常的な活動・生活でも広範に使用されることになり、現代暗号も多様なサービスやシステム・機器に組み込まれる時代となった。その結果、多数の開発ベンダが暗号を組み込んだサービスやシステム・機器の開発を担うこととなり、現代暗号は多くの開発ベンダへの暗号方式の公開・周知が不可欠となった。“暗号方式を公開しない”ことで安全性を確保してきた従来の暗号とは異なる安全性を確保する仕組みが必要となった。そこで現代暗号では、暗号方式を暗号アルゴリズムと暗号鍵に分離し、暗号アルゴリズムを公開しても暗号鍵を公開しなければ安全性を確保できるよう、暗号アルゴリズムが設計されている。

暗号方式の暗号アルゴリズムと暗号鍵への分離をご理解いただくため、簡単な古代暗号を例に、現代暗号風に暗号アルゴリズムと暗号鍵に分離する具体例を示す。図１は第１稿で説明した古代暗号の一つシーザー暗号による暗号化の例であり、平文の一つ一つの文字を、アルファベット順に左へ３文字シフトすることにより、暗号化を行っている。

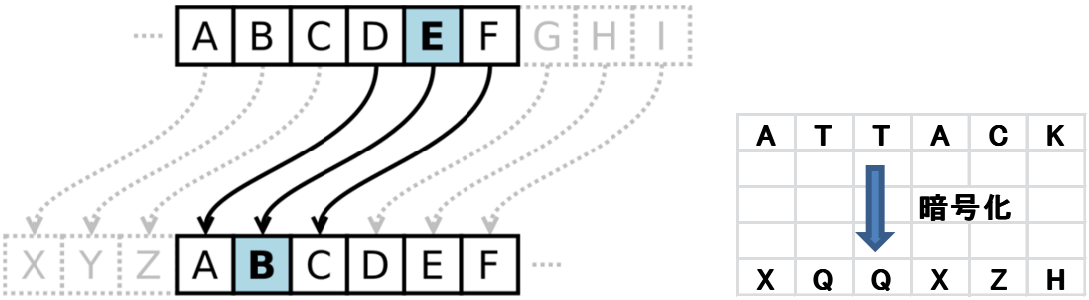

図１．シーザー暗号（3 文字左へシフト）による暗号化の例

https://commons.wikimedia.org/wiki/File:Caesar_cipher_left_shift_of_3.svg

この暗号方式を現代暗号風に暗号アルゴリズムと暗号鍵に分離した例を図２に示す。この例では、暗号アルゴリズムは“**アルファベット順に左へシフ**ト”、暗号鍵は“**3 文字**”、へ分離している。

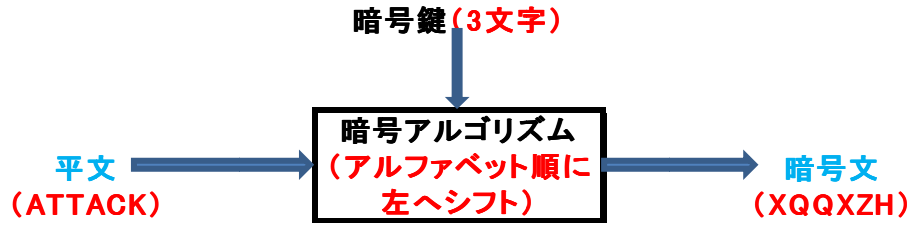

図２．シーザー暗号（3 文字左へシフト）の暗号アルゴリズムと暗号鍵への分離

シーザー暗号は簡単な暗号方式のため、暗号アルゴリズムを公開すると、暗号鍵としてはせいぜいアルファベットの数(26)しか有効では無いので試行錯誤で簡単に暗号鍵を見出すことができるし、平文とその暗号文の例があれば、その検査により暗号鍵を簡単に見出すこともできるが、現代暗号では複雑な暗号アルゴリズムを使用しているため、暗号アルゴリズムを公開しても、また、平文とその暗号文の例を多数入手できたとしても、暗号鍵を見出すことはできないように工夫されている。

②共通鍵暗号方式

現代暗号の内、共通鍵暗号方式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り、図３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は平文へ復号できる。

共通鍵暗号方式を利用し秘密の情報を伝えたい場合は、送信者と受信者が暗号鍵（復号鍵）を共有しており、その他の人は復号鍵を保有していない（知らない）ことが大前提で

ある。もし復号鍵が漏れると、暗号文が予期しない人に復号され、秘密の情報が漏れることになるし、秘密の情報を伝えたい受信者が復号鍵を保有していないと、伝えたい相手にも秘密の情報を伝えることはできない。

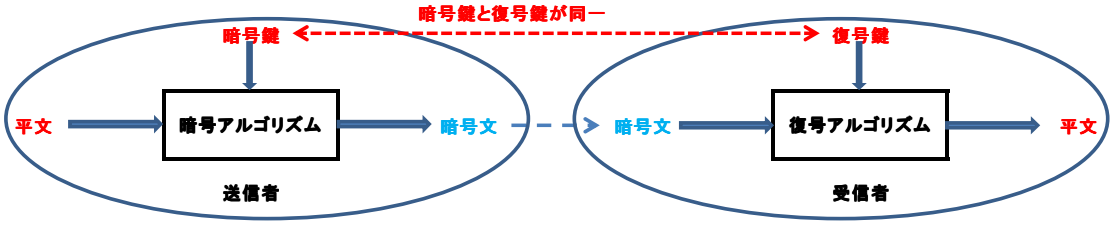

図３．共通鍵暗号方式による平文（秘密の情報）の暗号化/復号の仕組み

③公開鍵暗号方式

現代暗号の内、公開鍵暗号方式は、暗号鍵と復号鍵が異なり、暗号鍵から復号鍵を算出できないので暗号鍵を公開しても、復号鍵を持っている人しか暗号文を復号できないことが保証されている暗号方式である。図４にその暗号化/復号の仕組みを示している。受信者の暗号鍵（以下、公開鍵と表記）で生成した暗号文は、復号鍵（以下、秘密鍵と表記）を保有している受信者は平文へ復号でき、保有していない受信者は復号できない。

公開鍵暗号方式を利用し秘密の情報を伝えたい場合は、送信者は受信者の公開されている公開鍵で暗号化でき、復号に使用する秘密鍵（暗号化に使用した公開鍵に対応する秘密鍵）は受信者が保有していることが大前提なので、共通鍵暗号方式の場合のように鍵の共有は必要ない。一方、送信者が暗号化に使用する受信者の公開鍵が、本当に秘密の情報を伝えたい受信者の正しい公開鍵かどうかの確認ができる仕組みが必要となる。なぜなら、受信者の偽の公開鍵を使用し暗号化した場合、予期せぬ人に復号され秘密の情報が漏れることになる。そこで、公開鍵が秘密の情報を伝えたい受信者の正しい公開鍵かどうかを送信者が確認できる仕組み、公開鍵証明書の発行・検証の仕組みが別途必要となる。

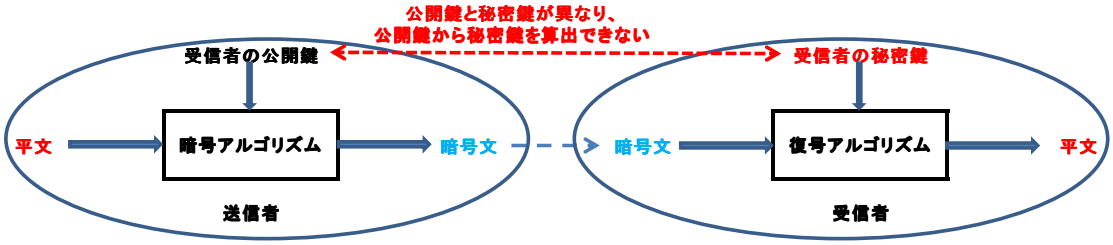

図４．公開鍵暗号方式による平文（秘密の情報）の暗号化/復号の仕組み

④本稿で対象とする現代暗号の範囲

本稿では、現代暗号の内、共通鍵暗号方式の第１世代の暗号出現から終焉、第２世代の暗号出現までの時期とし、同時期の公開鍵暗号方式の開発経緯や社会とのかかわりについては対象外とする。また、現代暗号は、従来の暗号と同じ秘匿目的の他、認証目的にも使用され始めるが、本稿では共通鍵暗号方式の主たる利用である秘匿目的に限定し社会とのかかわりについて紹介する。

（3）第 1 世代共通鍵暗号の代表　DES（Data Encryption Standard）

1977 年に米国初のデータ暗号化標準として採用された共通鍵暗号方式の暗号であり、世界で広範に利用された最初の現代暗号といえる。

①暗号方式（概要）

DES の暗号化処理フロー（概略）を図 5 に示している。大変複雑ではあるが、暗号化するデータ（平文）へ暗号鍵のビット列に応じ変化する転置や換字に類似した操作および排他的論理和（XOR）の操作などを繰り返すことにより暗号化する方式である。なお、この図では、鍵長は 64 ビットと記載されているが、8 ビットごとに 1 ビットのパリティビットが含まれているため、実質の鍵長は 56 ビットである。

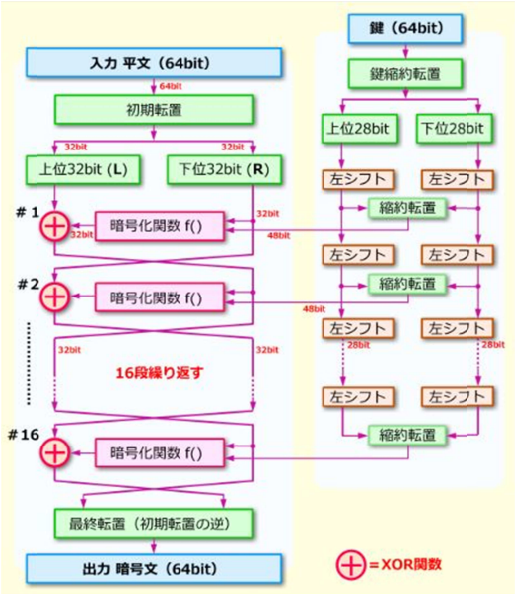

図 5．DES の暗号化処理

http://www.atmarkit.co.jp/ait/articles/1505/21/news030.html

②開発経緯

IBM は 1960 年代後半より暗号方式の研究に着手、英国のロイズ銀行の現金自動支払装置のデータ保護するために「Lucifer」という暗号方式を考案した。1971 年にロイズ銀行がこの Lucifer を採用すると、IBM は Lucifer を商用製品として提供を開始した。

一方、米国標準局（NBS：US National Bureau of Standards、現在の NIST）は 1968 年、コンピュータ・セキュリティについての需要調査を開始、統一された相互運用可能なデータを暗号化するための標準規格が必要との結論を得、その後 2 度（1973 年 5 月、1974 年 8 月）にわたって標準規格にふさわしい暗号方式の公募を実施した。

米国標準局の公募に応募された暗号方式の中で、最も有望な提案と評価されたのは IBM が提案した改良版 Lucifer であった。1975 年には標準案として改良版 Lucifer が公表され、その後、ワークショップが 2 度開催され、標準案について議論された。なお、標準案（改

良版 Lucifer）の更なる改良の過程で諜報機関である米国国家安全保障局（NSA：National Security Agency）の不適切な干渉によりアルゴリズムが弱められ、諜報機関だけが暗号化されたメッセージを容易に解読できるようにしたのではないかという疑いが持たれ、米国上院諜報特別委員会による調査が実施されたが、「そのような干渉は無かった」、というのが調査結果であった。紆余曲折はあったが、1976 年米国連邦標準（FIPS：Federal Information Processing Standardization）として承認された。その後、1981 年には米国国家標準協会（ANSI：American National Standards Institute）が定める標準として制定された。このような経緯で開発・改良・標準化されたのが、DES である。

米国連邦標準となった DES はビジネス分野で広範に利用された。特にコンピュータ・ネットワークを利用して資金決済情報や顧客の秘密情報を送受信する際の情報の改ざんや不正侵入を防止したいという米国金融業界の強いニーズもあり、銀行の決済ネットワークには DES を利用したセキュリティ装置が次々と導入され、金融業界は DES の最大ユーザとなった。

（4）解読手法と DES 解読の歴史

現代暗号では、暗号文を平文に戻す（復号する）際に必要となる復号鍵を、復号鍵の保有者から受け取ったり、あるいは盗んだりするなど、復号鍵そのものを直接入手することなく、復号鍵を導出できる何らかの方法が見出された時、その暗号アルゴリズムは解読された、という。現代暗号の安全性は、復号の際に使用する復号鍵を秘密裏に保管しておけば、暗号アルゴリズムが公開されていても、その復号鍵を見出すことは非常に困難であることに依存しているが、復号鍵が容易に見出す方法が見つかった場合、意図しない（復号鍵を持っていない）人でも暗号文を平文へ戻し秘密の情報を得ることが可能となるため、その暗号はもはや安全ではなくなる。このような状態になった時、その暗号は解読された、という。

理論的な暗号解読手法として代表的なものに、差分解読法と線形解読法がある。
差分解読法は、解読者にとって都合の良い平文と暗号文のペアが入手可能である場合の解読手法である。平文とその暗号文、その平文の一部分を変更した暗号文など、入手した平文と暗号文の多数の組合せから平文間の差分、暗号文間の差分を利用し、秘密の鍵を推定する方法で、1989 年にイスラエルの Biham と Shamir によって考案された。なお、DES は、どうやら事前に対策がとられていたようで、この解読法は DES には有効では無かった。

線形解読法は、ある平文とそれを暗号化した暗号文がペアで入手できるが、攻撃者は平文を選ぶことができない場合を想定した解読法である。暗号化の関数を、より簡単な関数に近似（線形近似）させて置換え、この線形近似させた関数を解読することにより、少ない計算量で鍵を見つけようという方法で、1993 年に三菱電機の松井充氏によって考案された。松井氏はこの線形解読法により、2^{43} の平文と暗号文の組が必要であるが、DES 攻撃に成功した。

鍵の全数探索による解読（ブルートフォース解読）を目指す活動も、コンピュータの急速な高速化・廉価化に伴い、活発化してきた。DES の場合、鍵長は 56 ビットなので、2^{56} 種のビットパターンの中に鍵は必ずあるはずだから、その全てのビットパターンをチェックすることにより鍵を見出そうとする解読手法がブルートフォース解読である。DES については、米国の RSA Data Security 社が 1997 年より毎年、DES Challenge として、暗号解読コンテストを開催しており、その結果を表 1 に示している。このように、DES の安全性はコンピュータの高速化・廉価化により急速に低下しているのがわかる。

DES Challenge	DES Challenge の結果		
	解読年月	解読時間	解読に使用した機器
Ⅰ	1997年6月	140日	約7万台のPC
Ⅱ-1	1998年2月	40日	約5万台のPC
Ⅱ-2	1998年7月	56時間	約25万ドルで作成した解読専用マシン
Ⅲ	1999年1月	22時間15分	DES専用解読マシン＋ 約10万台のPC

表１．DES Challenge（DES 解読）の歴史

DES の延命策として、DES で 3 回暗号化することにより安全性を高めた暗号アルゴリズム TripleDES（鍵長 112 ビット）などが IBM により考案され、米国連邦標準にも加えられ利用されてきたが、2005 年には遂に DES が米国連邦標準から外された。

(5) 日本での第 1 世代共通鍵暗号の開発とその応用の状況

日本企業も米国連邦標準 DES を実装し、製品・機器への組込み等で利用してきたが、独自の共通鍵暗号の開発も進め、DES の開発から 10 年ほど遅れたが、NTT が 1985 年に鍵長が 64 ビットの FEAL を、1987 年には安全性を高めた FEAL-8 を開発した。IC カード等の 8 ビットマイクロプロセッサ上のソフトウェア向きに設計された暗号方式であった。1988 年には、鍵長が 64 ビットの MULTI2 を日立が開発した。また、鍵長の短さが DES の安全性を脅かしている状況から、NTT は 1990 年にはさらに安全性を高めた、鍵長が 128 ビットの FEAL-N(X)を開発した。一方、三菱電機は、DES 解読の経験を生かし、1995 年に鍵長が 128 ビットの MISTY を開発した。筆者が担当していた東芝のセキュリティ研究部隊も、DES/TripleDES との互換モードを有する TripleDES の改良版の Triplo（鍵長は 128 ビット）を 1999 年に発表した。このように、日本企業は各社が独自方式の開発を競って実施し、様々の製品・システム・サービスへの適用を推進した。

この時代、日本でも社会を支える様々の暗号応用製品・システム・サービスやビジネスが出現した。1991 年に始まった有料放送、多様なコンテンツが少額の費用負担で自宅の TV で楽しめる現在があるのも、暗号化された放送コンテンツの復号が可能なのは契約者のみに限定することができる限定受信システム（CAS：Conditional Access System）が開発さ

れたからである。CAS の仕組みを下図に示す。このように、映像および映像情報などは暗号化され放送されるが、契約ごとに異なる共通鍵 $_{M}$ と適切な契約情報を保有する受信機のみが復号でき、視聴できるような仕組みとなっている。CAS では共通鍵暗号が利用されている。

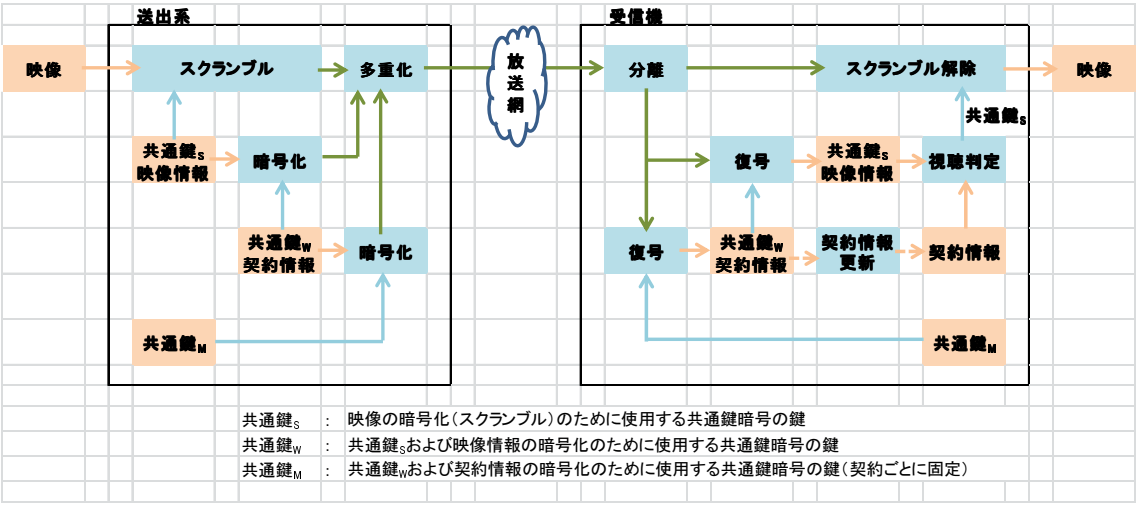

図 6．限定受信システム（CAS）の仕組み

また、それまでは専用の機器でしか視聴できなかった映画等の DVD が、現在のように PC で視聴できるようになったのも、1995 年頃から東芝、インテルが中心になって暗号技術を利用し映画等のコンテンツの不正コピーを防止する仕組み DTCP（Digital Transmission Content Protection）の策定を進め、1998 年に事実上の国際標準とすることができたためである。DTCP では、公開鍵暗号、共通鍵暗号の両方が利用されている。

更に、自動車が料金所で停車する必要も無く高速道路を快適に走行できるのも、1997 年に試験運用が始まった高速道路料金収受システム（ETC：Electronic Toll Collection System）、その ETC に組み込まれた暗号技術による自動車の認証や課金情報の改ざん防止の仕組みのおかげである。詳細は非公開だが、共通鍵暗号が利用されている。

（6）暗号技術に関する規制

暗号の民間利用が始まり、コンピュータやネットワークの急速な発展とも重なり、様々の分野での製品・システム・サービスでの応用が展開された時代であったが、現代暗号も従来の暗号と同様、国や組織間の争いを有利に進める道具（武器）としても利用されるため、暗号技術や暗号製品の輸出は規制されていた。

1950 年に活動を開始した対共産圏輸出統制委員会（ココム）は、冷戦期に日本を含む資本主義諸国を中心に構成され、共産主義諸国への軍事技術・戦略物資の輸出規制（あるいは禁輸）を目的としたものであるが、暗号技術、暗号製品も対象と認定され、鍵長が 40 ビットを超える暗号を組み込んだ製品の輸出は規制されていた。

冷戦の終結により、ココムも役割を終え 1994 年に終了したが、その 2 年余り後の 1996 年には、地域の安定を損なうおそれのある通常兵器の過度の移転と蓄積を防止すること、ならびにテロリストに通常兵器や関連技術が渡る事を防ぐのを目的としたワッセナー・アレンジメントが日本を含む 33 か国にて締結され、通常兵器及び関連汎用品・技術の責任ある輸出管理が参加各国に求められた。暗号技術もその規制対象であったが、徐々に規制が緩和された。日本では、1999 年には欧米等の先進国向けの輸出については鍵長が 64 ビット以下は許可不要となり、2000 年には鍵長が 64 ビット以下という鍵長の制限も撤廃された。

なお、ワッセナー・アレンジメントは現在も有効であり、参加国は 41 か国。現在は、テロ支援国として 7 か国が指定され、それ以外の国へは鍵長に関係なく輸出可能となっている。

（7）キーエスクロー（Key Escrow）/キーリカバリー（Key Recovery）構想

前節で述べたように暗号に関して長年厳しい輸出規制が行われてきた。その目的は、暗号が武器として使われる可能性があるため、高度な暗号技術や暗号製品が敵対勢力、冷戦時の共産主義の国々や、その後はテロ支援国へ渡ることを防ぐためである。

米国では輸出規制に留まらず、国内でもテロリストや組織的犯罪等の犯罪者の手に暗号が渡ると連邦捜査局（FBI：Federal Bureau of Investigation）等の捜査の障害となることを理由に、1993 年にキーエスクロー構想を発表した。具体的には、Clipper Chip と呼ばれるハードウェアと Skipjack と呼ばれる非公開の暗号アルゴリズムを採用した暗号通信技術を導入する構想で、政府が強度の高い暗号を民間に提供する一方で、復号鍵の第三者機関への寄託（escrow）を義務付けるものであった。これが実現すると、捜査当局が裁判所の許可の下で捜査対象の暗号化された通信内容を解読することが可能となる。

このキーエスクロー構想は、多くの批判を受けた。捜査機関による個人のプライバシー侵害への不安・不信、非公開の暗号アルゴリズムへの不安・不信、特定のメーカが独占的に提供する専用チップ（Clipper Chip）への依存、などに対する批判であった。このような批判を受けたクリントン－ゴア政権は、Clipper 2、Clipper 3 とキーエスクロー構想の内容を見直したが、批判をかわすことはできなかった。

1996 年、ゴア副大統領は、キーエスクロー構想からキーリカバリー構想への転換を発表した。基本的には、ほとんど同じ内容の構想ではあったが、犯罪捜査のための暗号解読を目指した構想では無く、正当な利用者が復号鍵を紛失した時の備えを目指した構想であることを訴えた。そして、復号鍵の復元を可能とする鍵復元機関は、捜査機関が犯罪捜査等で通信内容の復号が必要となった場合には裁判所の許可を得れば復号鍵にアクセス（合法的アクセス）が可能なことを前提に、民間組織としても設立可能とした。

米国政府は、このキーリカバリー構想を世界規模で実現すべく、OECD（Organisation for Economic Co-operation and Development：経済協力開発機構）へ暗号政策ガイドラインの策定を提案した。このガイドラインにおいて、「国の暗号政策は合法的アクセスを認めるべき」という内容を織り込むよう米国は主張したが反対も多く、結局「認めても良い」という強制しない表現となった。暗号政策ガイドラインの正式な勧告は 1997 年に出された。なお、日本では、警察庁は米国の鍵寄託政策に賛成の立場だったが、郵政省（現在の総務省）や通商産業省（現在の経済産業省）は慎重な立場であった模様。

米国はまた、キーリカバリー技術の標準化や実際の運用方法の規定が必要であることを、各国に働きかけた。日本でもキーリカバリー技術の研究開発が注目され、キーリカバリー・システムの試作が通商産業省の支援を受け実施された。1996 年には日立・富士通・北陸先端科学技術大学院大学のグループ、1997 年には NEC・日立・富士通のグループ、1998 年には東芝（筆者が担当する東芝のセキュリティ研究部隊）が単独で、それぞれキーリカバリー・システムを試作した。

一方、米国政府のキーリカバリー構想の発表を受け、1996 年に米国の民間企業 11 社によるキーリカバリー・アライアンス（KRA：Key Recovery Alliance）が発足、キーリカバリー技術の開発・標準化を目指した。この KRA は、欧州や日本企業も参加し、1997 年には 70 社以上の国際的な連合に発展した。日本からは、日立、NEC、富士通、東芝、日本 IBM、三菱電機、三菱商事、NTT ソフトウェアなどの企業が参加した。筆者も東芝の代表として 3 か月ごとの国際会議に参加したが、キーリカバリーの仕組みの有無に関係なく暗号技術・暗号製品の輸出規制の緩和が進んだため、1999 年に入り KRA は自然消滅した。KRA の最後の国際会議は、日本企業団（NEC、東芝、三菱電機、日本 IBM、富士通）主催で、1998 年 11 月、ハワイで開催した。本来は日本での開催が筋であったが、鍵寄託は微妙な問題であったため、日本での開催は避けハワイ開催となった。

（8）第 1 世代共通鍵暗号の終焉・・・第 2 世代へ

①米国の動き　新たな米国連邦標準暗号 AES の策定

鍵長が 56 ビットの DES は(4)で示したように、コンピュータの高速化・廉価化により 1990 年代後半には明らかに安全性が不十分な状況となった。その後も、DES を 3 回使用し、鍵長を 112 ビットとした TripleDES が米国連邦標準として利用されてきたが、もともと単独で動作することを前提で設計された DES のアルゴリズムを繰り返し実行しているため処理効率は良くなかった。そこで、米国国立標準技術研究所（NIST：National Institute of Standards and Technology、従来の NBS）が 1997 年 1 月に新たな米国連邦標準暗号 AES（Advanced Encryption Standard）を選定するプロジェクト開始を宣言、AES ワークショップによる議論を踏まえ選定方法や選定基準を検討し、1997 年 9 月に NIST が、安全性、処理性能、実装性に優れた新たな暗号方式 AES の公

募を開始した。公募に対し 1998 年 6 月に締め切った時点では 21 件の応募があり、書類選考（公募条件等のチェック）により 15 件に絞り込まれ、第 1 回 AES 候補会議で発表された。その 15 件の中には、日本の NTT からの提案である E2 も含まれていた。その後の約 9 ヶ月の第 1 次評価の結果を踏まえ第 2 回 AES 候補会議にて 5 件に絞り込まれ、その後の約 1 年の第 2 次評価の結果が第 3 回 AES 候補会議で議論され、最終的には 2000 年 10 月に NIST は AES 候補としてベルギーの暗号学者が提案した Rijndael を選定したことを発表した。そして、2001 年 11 月、Rijndael は AES として米国連邦標準に登録された。

このように 5 年をかけて米国連邦標準に選定された AES は、鍵長が 128 ビット、196 ビット、256 ビットを選択できる共通鍵暗号で、第 2 世代共通鍵暗号を代表する暗号として世界各国で使用されることになる。

②欧州の動き　暗号技術推奨リスト策定活動　NESSIE

欧州連合（EU）は米国の AES プロジェクトに対抗し、2000 年 1 月から 3 年の予定で、NESSIE(New European Schemes for Signature, Integrity, and Encryption)プロジェクトを開始した。AES では共通鍵暗号のみが公募の対象であったのに対し、NESSIE では共通鍵暗号、公開鍵暗号を含め 7 つのカテゴリの幅広い暗号技術を対象に、2000 年 3 月に公募を開始、第 1 回の NESSIE 会議（2000 年 11 月）では 35 件の応募暗号技術の発表があった。また、AES では「一つ」だけを選定するとしたのに対し、NESSIE では暗号技術推奨リストの作成を目標とし、カテゴリごとに三個を選定することとした。AES プロジェクトと同様、NESSIE プロジェクトでも何度かの評価作業、国際会議開催の結果を踏まえ、2003 年 3 月に暗号技術推奨リストを含む最終報告書が公表された。AES が属する共通鍵暗号のカテゴリでは、MISTY1（鍵長は 64 ビット）、Camellia（鍵長は 128 ビット）、SHACAL-2（鍵長は 256 ビット）の三つ、それに AES が推奨された。NESSIE で推奨された新たな共通鍵暗号三つの中の二つ、MISTY1（三菱電機）、Camellia（NTT と三菱電機）が日本からの提案であった。日本企業の暗号技術のレベルの高さがうかがえる。

③日本の動き　電子政府推奨暗号リスト策定活動　CRYPTREC

日本政府は 1999 年 12 月にミレニアムプロジェクトを決定し、その中で 2003 年度までに行政手続きがインターネットを利用してペーパレスで行える電子政府基盤を構築する方針を示し、そのために通商産業省を主管としてセキュリティ技術開発を推進することとした。これに基づいて通商産業省が 2000 年 4 月に、情報処理振興事業協会（IPA: Information-technology Promotion Agency）を事務局とした暗号技術評価委員会を設置、電子政府において利用され得る暗号アルゴリズムの性能等を技術的・専門的見地から客観的に評価する、などの具体策を掲げた。そこで、IPA は 2000 年 5 月に暗号技術評価委員会（CRYPTREC ：Cryptography Research & Evaluation Committee）を設置、活動を開始した。

政府は 2000 年 11 月には IT 基本法（高度情報通信ネットワーク社会形成基本法）を成立させ、一方、2001 年 1 月には、縦割り行政による弊害をなくし、内閣機能の強化、事務および事業の減量、効率化することなどを目的とし、それまで 1 府 22 省庁で構成されていた中央省庁は 1 府 12 省庁に再編統合された。IT 基本法に基づき、また中央省庁の新体制のもと、翌年 1 月には e-Japan 戦略、3 月には e-Japan 重点計画を決定した。この重点計画には「高度情報通信ネットワークの安全性及び信頼性の確保」の実施施策の一つとして、「2002 年度までに暗号技術の標準化」が掲げられた。

CRYPTREC は 2001 年度から総務省と経済産業省の共管となり、IPA と通信・放送機構（TAO：Telecommunications Advancement Organization、現在の NICT）が共同事務局を務めることになった。CRYPTREC では、e-Japan 重点計画で掲げられた実施施策「2002 年度までに暗号技術の標準化」に呼応し、電子政府システムでの利用に資するかどうかの観点から評価を実施し、「電子政府推奨暗号リスト」の策定を 2002 年度末までに作成することとした。

CRYPTREC では、2000 年度、2001 年度の 2 度にわたり、暗号技術の公募（4 つのカテゴリ）、スクリーニング評価・詳細評価の実施、および暗号技術検討会やワークショップを開催し、最終的には 2003 年 2 月に「電子政府推奨暗号リスト」を決定した。AES のように暗号技術を一つに絞らず、また NESSIE のようにカテゴリごとに「三個」という制限を設けず、安全性の観点からの電子政府システムでの利用に資するかどうかの評価結果に基づき、「電子政府推奨暗号リスト」が策定された。共通鍵暗号の中の 128 ビットブロック暗号のカテゴリで電子政府推奨暗号として推奨されているのは、Camellia（NTT、三菱電機）、CIPHERUNICORN-A（NEC）、Hierocrypt-3（東芝）、SC2000（富士通）、それに AES であった。

(9) おわりに

本稿では、現代暗号の時代の内、第 1 世代共通鍵暗号の出現（1970 年頃）から第 2 世代共通鍵暗号が選定される（2000 年頃）までの時期について、共通鍵暗号に限って、日米欧の暗号アルゴリズムの開発状況、民間での利用状況、輸出規制や利用規制の動きなど、暗号と社会のかかわりについて述べた。

現代暗号のもう一つのカテゴリである公開鍵暗号の開発の歴史やその社会とのかかわりや、第 2 世代共通鍵暗号が活用される時代の暗号と社会とのかかわりについては、別途紹介させていただくこととしたい。

以上

参考資料

①IBM100 IBM 100 年の軌跡　世界をつなぐ暗号化技術

http://www-03.ibm.com/ibm/history/ibm100/jp/ja/icons/cryptography/

②Data Encryption Standard

https://ja.wikipedia.org/wiki/Data_Encryption_Standard

③情報セキュリティ調査研究報告書（平成 9 年　警察庁）

https://www.npa.go.jp/cyber/research/h9/secrepo/abstract.htm

④キーリカバリー構想を巡る最近の情勢について（平成 9 年　日本銀行金融研究所）

http://www.mofa.go.jp/mofaj/press/pr/pub/geppo/pdfs/01_1_2.pdf

⑤国家による暗号政策（平成 13 年　外務省）

http://www.mofa.go.jp/mofaj/press/pr/pub/geppo/pdfs/01_1_2.pdf

⑥日米欧の暗号技術標準化・評価プロジェクトを終えて

－ 3 プロジェクトの実績と今後への展望 －

（平成 15 年　NTT 情報流通プラットフォーム研究所）

http://www.jnsa.org/nsf2003/award/2003/J005-P0902.pdf

⑦暗号鍵の適切な運用・管理に係る課題調査（平成 25 年　情報処理推進機構）

https://www.ipa.go.jp/files/000027254.pdf