国家による暗号政策

―暗号の戦略性と輸出管理―

八田　善明

はじめに

「暗号（Cryptography）」とは、一般的に通信文などをなんらかの約束[1)]によって、通信の当事者以外の第三者にとり全く意味をなさない文に書き換えてしまう手段を指す。この意味での暗号の歴史はかなり古くまで遡り、人類史上において文字が使用され始めて間もない頃に既に萌芽を認め、シーザー暗号[2)]の様な置換型といった暗号の雛形も存在していた。更に時代は下って、英国のメアリー女王が牢獄から発出した暗号文が側近に解読された例[3)]や、近代暗号として第二次世界大戦中[4)]に活躍したドイツのUボートとの位置情報の暗号通信に用いられたエニグマ暗号[5)]が有名であるように、古代、中世、近代から現代へといつの時代にも暗号は使用され、発展を続けてきた。これらの例にも見られるように、これまでの「暗号」は、政治・軍事・外交・諜報の歴史とともに発展してきたと言えよう。

なお、「暗号」の本質が防御機能にあることに対し、コインの両面の如く攻撃的な「解読」機能が存在することや、解読に先立つ「傍受」・「盗聴」活動の存在も忘れてはならない。暗号の歴史は、情報を制する者による優位を実現するために、情報に対する攻撃と防御といった相反する両機能を高めるべく日々戦略が練られた歴史でもあったのである。

1）一定の約束・手順＝アルゴリズム

2）ジュリアス・シーザーのガリア戦記に記述がある。（Simon Singh, The Code Book, 1999, pp. 9–10）

3）ibid., pp. 36–44

4）日本でも大戦中独自に開発した「紫暗号」を使用していたが、後に米に解読されている。

5）アルトゥール・シェルビウス（Arthur　Scherbius）によって開発され、1918年には独海軍及び外交部に提供、1926年に正式採用されてUボートとの通信に使用された。後にポーランドや米等により解読される。（ibid., Chapter 4, Clacking the Enigma pp. 143–189.）

しかし、技術の進歩とともに情報の蓄積と伝達の手段が紙媒体から電子媒体へ、アナログ信号からデジタル信号へと変遷していく中、暗号自体もいち早くデジタル化への適応を進め[6]、その結果、暗号はもはや軍事・外交・諜報といった特定の使命に限られる性質のものではなくなった。このような一般化の現象は、我々の日常生活を見回してみることで十分にその度合いを確認できるであろう。銀行の現金引出機の暗証番号認証方式に始まり、テレビやビデオの画像処理に用いられる符号化技術[7]、各種放送技術、衛星放送におけるユーザー情報及び映画等のペイパービュー・システム、携帯電話等が混信しないで話せるスクランブル技術[8]、著作権保護のためのコピー・ガード、クレジットカード、インターネットの上の認証やデータ保護方式[9]を基盤とする電子商取引、流行りのｉ−モード等もはや暗号(符号)を使用しないで現代社会や現代経済・商業は成り立たないと言っても過言ではない。また、暗号方式自体も使用目的・環境に応じて様々なものが考案され[10]、実用化されてきており、今後も暗号に対する依存度が益々高くなるのは必至である。

このような背景の中、国家はどのように暗号を位置づけてきたか。ごく最近ま

6）コンピューター上で使用されるようになり、暗号の鍵も「0」と「1」の組み合わせで成り立つ。暗号鍵の長さはビットを単位として表される。

7） 画像を微細に分割して復元する技術自体が符号化技術。また、デジタル時代に入って、今後使用が更に拡大・発展されるパソコン上での画像記録（圧縮）アルゴリズムJPEGや、動画記録（圧縮）アルゴリズムMPEGも同様。

8）コードレス電話や、無線機も同様。今後利用の拡大が見込まれる電子・電気機器や家電間におけるデータ転送を目的とする短距離無線規格のブルー・トゥースも暗号技術の集大成。

9）米ネットスケープ社のセキュア・ソケット・レイヤー（SSL）等に始まりいわゆるブラウザ・ソフトや、メール・ソフトは電子認証や暗号化機能を備えているものが一般化されている。

10）暗号化と復号に全く同じ鍵を使用する「対称鍵暗号方式」や一方向の暗号化のみを行うone way hash暗号、鍵の受け渡しの問題を解決する非対称鍵暗号（＝公開鍵暗号）等。

で、多くの国々が暗号の戦略性に着目して国内規制や輸出上の制限などの政策をとってきたことは着目に価する。しかし、技術の進歩とともに大きな暗号市場が育ち、暗号が社会基盤に変貌した中、1990年代は戦略性のみに着目して厳格な輸出管理を行うことに限界の兆しが見えてきた時代であった。

本稿ではこのように多様化した「暗号」の国家における位置づけと、今後戦略面や経済・社会面において期待され得る役割を見極めることを目的としている。そのアプローチとして本稿においては、先ず、暗号先進国であるとともに安全保障面と経済・社会面の両面の対立から紆余曲折を経てきた米国を一つの柱とし、今後も課題となり続けるであろう戦略性とプライヴァシーのバランスの難しさを浮き彫りにしてみたい。また、その上で、米国や欧州を始めとする様々な暗号政策や国際環境をも併せて整理することによってその戦略性や輸出管理の意味、国内外の暗号政策のありかたについても考察してみる。

１．米国の暗号政策の推移

⑴　米国と暗号政策

米国は、暗号の効用と害悪につき明確な意識をもって国家政策上重要視し、独自の暗号政策を実施してきた希有な国である。このような暗号政策を持つに至ったのは、「情報」に対する認識の高さ、すなわち情報の有無における立場の優劣形成に敏感な政治や経済をもつ故の必然とも言えよう。米国は、自他共に認める暗号開発の先進国であり、使用国であると同時に最大級の輸出国である。

⑵　厳格な暗号管理

米国における暗号政策の最大の特徴は、国内における暗号の開発・使用については制限が無い一方で厳格な対外政策、すなわち輸出管理を行ってきていることにある。

その厳格性は、暗号が1996年に関連法令の改正が行われるまで国務省所掌下の

武器国際移転規則[11]（ITAR）の対象とされていたことからもうかがい知れる。これは、暗号が武器同様に国家安全保障上の重要事項に位置づけられていた証左であり、他の武器同様に輸出審査手続き上も、先ず国務省が審査を行った後、国防技術安全保障局（Defense Technology Security Agency）、エネルギー局、国家安全保障局（National Security Agency：NSA）等の順で行われ、国務省が最終決定を行うこととなっていた。

米国は、このような極めて厳格な暗号輸出管理の必要性の理由として、テロリストや組織的犯罪等の犯罪者の手に暗号が渡り、連邦捜査局（Federal Bureau of Investigation：FBI）等の捜索の障害[12]となることにより内外の米国民が侵害を受けることを防ぐことをあげている。なお、国家安全保障上においても暗号は諜報活動の阻害要因として位置づけられ、この観点からも輸出管理対象とされた。これは、暗号を輸出管理することによって、商業貨物レベルの暗号製品によって暗号化された国際通信の水準を米国の暗号解読能力以下の統制可能な水準に維持することを目指しているからである[13]。換言すれば、米国の諜報機関による暗号

11）ITAR（International Traffic in Arms Regulations）＝大統領からの委任により国務省が排他的な権限を有する武器輸出管理規則であり、米国軍需リスト（U.S. Munitions List）の策定と変更及び同リストに基づく輸出許可手続きを所掌する。同軍需リストは、国防総省と共同で作成され、その品目が性質上軍需品であるという点に着目してリストに加えられ、汎用性の有無は判断材料ではない。見直しの結果、軍需リストから除外されることとなった品目は、引き続き管理の要がある場合、商務省所掌下の輸出管理リストに移管されることとなる。「暗号」は、軍需リストCategory XIII (b)(1)に該当する。James Chandler, Diana Arrington, Lamarris Gill, Donna Berkelhammer：*Building Big Brother*, Springer-Verlag（New York）, 1995

12）通信傍受は、真に重要な犯罪捜査に際し用いられる手段であって、技術の進展とともに強力な暗号の使用が拡散した場合、新たな法律が施行されない限り、ただでさえオーバーロードのFBIは両手を後ろ手に縛られて捜査に立ち向かわなければならないような状況に陥るであろう。Louis J. Freeh FBI局長の上院司法委員会技術と法サブ・コミッティーにおける証言。1994年３月18日。

解析に耐えうる強度の戦略的能力を有する暗号システムのフォーリン・アヴェイラビリティー（第三者による入手可能性）を制限することであり、同時にトラフィック・セレクション（重要な情報か否かを区別する）に対する重大な障害になり得る強度の暗号システムの拡散使用を遅延させることと有識者は述べている[14)]。

⑶　暗号の標準化

米国は、政治、金融等様々な観点から強力かつ耐用年数の高い暗号の標準化の必要性を意識し、1975年、データ暗号化標準（DES[15)]）を連邦政府標準として開発し、政府はもとより国家的な標準として使用されるに至った。当時最先端の水準として位置づけられたDES暗号は、国内及び海外における米国政府間の通信や米国市民の通信の安全のために用いられ、その一方で厳しい輸出管理の下に置かれた。1991年に、共産圏を対象とした輸出管理体制であるココム[16)]においてマスマーケット（一般的に市場で入手可能な部類の商品）のソフトウェアが規制から除外されるに至っても、米国内においては引き続き兵器と同様に厳しい管理は継続された。しかし、如何に輸出管理を実施しようとも1990年代初頭から世界的に暗号技術開発の進展と解読技術の進展が平行して進み、DESはもはや米国のみが所有する暗号ではなく世界標準に近いものとして成長していた[17)]。

13）Geoffrey W. Turnerの下院司法委員会経済及び商法サブ・コミッティーにおける発言から。1992年５月７日。

14）Whitfield Diffie, Susan Landau：*Privacy on the Line*, Massachusette Institute of Technology Press, 1998

15）DES（Data Encryption Standard）：NSAの協力によりIBM社が設計した対称鍵暗号で、56ビットの暗号鍵の長さ（鍵長）をもつ。

16）COCOM（Coordinating Committee）：冷戦期（1950年より活動を開始）における西側諸国による戦略物資・技術の輸出規制に関する非公式な合意に基づく多国間組織。本部はパリにあった。参加国はアイスランドを除くNATO諸国に日本、オーストラリアの17カ国。

商取引の多国籍化の進展や人・物の移動・移転の国際化及び大量化、そして電子通信技術の進歩によりインターネットが一般的に普及し始める等、米国内における経済的な環境にも大きな変化が起きてきた。この変化により米国は二つの大きな問題に直面することとなった。一つは、一般市場において流布・使用されている暗号の強度がその技術の進歩の速度によりNSAやFBIといった諜報機関や捜査当局の暗号解読レベルを越えてしまう事態が懸念されるに至ったことである。また、インターネットをはじめ、あらゆる分野において暗号や符号技術が使用されるに至ったことにより利用者が急速に一般の国民に広がり、同時にそれらを開発・利用するソフトウェア会社や関連業界の爆発的な拡大をもたらし、海外に販路を求める際に既存の輸出管理がその障害となってきたことがあげられる。

⑷ 暗号使用の経済・商業分野における重要性の増大

米国は、次第に国家として暗号による防御対象を軍事や外交面に限っていては不十分であり、早急に国内の暗号水準を高めて経済・商業面における防御力を高める必要性[18]を感じ始めた。それは、一般国民の理解と参加によるインターネット・インフラの構築に当たり、その前提として、プライヴァシー保護の必要性を

17）米Software Publishers Association（SPA）の1993年５月発表によると、アルゼンチン、オーストラリア、ベルギー、カナダ、デンマーク、フィンランド、フランス、ドイツ、香港、インド、アイルランド、イスラエル、日本、オランダ、ニュージーランド、ノールウェー、ロシア、南ア、スペイン、スウェーデン、スイス、英国の22カ国より340の暗号関連のハード又はソフトウェア若しくはそれらの複合製品を確認し、その内155はDESを使用していた。Stephen　T.　Walker上院司法委員会技術及び法サブコミッティー証言。1994年５月３日。

18）東西における諜報活動は、共産圏の崩壊の前後において、以前の軍事機密に関する諜報活動という性格から、後の経済的な諜報活動へとその性格を移行している。今日においては、経済自体が一国の安全保障上重要な位置を占めるようになってきている。Geoffrey W. Turnerの下院司法委員会経済及び商法サブ・コミッティーにおける発言から。1992年５月７日。

認識し始めたことが指摘できよう。

また、一方で米国暗号業界の暗号の国際市場における技術及びシェアの双方における優位性確保といったパラドックスにも挑まざるを得ない状況に陥った。

⑸　鍵預託イニシアティブ：EEI[19]

安全保障面と経済面の板挟みのパラドックスの解決策として政府が提示したのが、1993年４月15日の大統領令により施行されることとなった鍵預託イニシアティブ（EEI）である。このイニシアティブは、クリッパー・チップ[20]という政府設計による暗号通信用のチップ（集積回路）を用いた鍵預託方式[21]の採用により、国民の電話通信上の安全とプライヴァシーを確保しつつ、法執行の合法的な必要性にも応えようとしたものである。

同イニシアティブの発表に際し、政府は、高度な暗号が国外に輸出されると外

19）Escrowed Encryption Initiative（EEI）

20）Clipper　Chipは、NSAによって1985年に設計を開始し、1992年に評価を完了した。同チップは、SKIPJACKというアルゴリズムを採用しており、対称80ビット鍵の暗号／復号アルゴリズムであって、DESと同様の機能を持ち、一回の暗号／復号に32回の演算を行う。また、DES同様にFIPS81準拠の４つのオペレーティング・モードを有する。

⑴　ECB：Electronic Codebook：最も弱いモード

⑵　CBC：Cipher Block Chaining

⑶　OFB：64bit Output Feedback

⑷　CFB：１，８，16，32若しくは64 bit Cypher Feedback

回路設計は、MYKOTRONX社が担当し、VLSI社によってチップが製造された（MYK-78）。製造されたチップは、MYKOTRONX社がプログラムして、製品として消費者の手に渡る。他のクリッパー・チップと接続し、同調が確立した際の暗号化／復号化に要する時間は、コンスタントに15-20MB毎秒である（ECBモード）。クリッパー・チップのPCMCIAボード版としてCapstone Chipも用意されている。

21）キー・エスクロウ（Key Escrow）

22）1993年４月15日大統領令による。

国の諜報活動の強化に利用されるおそれがあるとの認識[22]を示しており、厳格な輸出管理の重要性を再確認した。

本イニシアティブの目玉である政府開発[23]による最先端の電子暗号チップのクリッパー・チップは、通常市販されている暗号製品よりも性能が高く[24]、かつ廉価であり、既存の電話に接続する簡便性の高い暗号製品として普及を期待されたものであり、このチップを内蔵した暗号機器により、企業の知的所有権や、個人の電話上での会話のプライヴァシー及び電子データの不正取得を防ぐことができる一方で、同時に連邦や国家、地方の法執行機関が合法的に犯罪者の電話通信を傍受することができるものとして政府の大きな期待を担って世に出された。その原理は、それぞれのクリッパー・チップに固有の暗号鍵の合い鍵を承認を受けた政府機関に委託し、捜査上の必要時に司法省からの令状に基づき合い鍵を用いて

23）NSAでクリッパー・チップ計画に関わったClinton Brooks氏によると、1989年、国家標準技術院（NIST：National Institute of Standards and Technology）と国家安全保障局（NSA：National Security Agency）からそれぞれ４人、合計８人の専門家で構成されるチームが結成された。その検討過程でウィーク・スポットを設計上組み込む「抜け穴（Trapdoor）」は連邦捜査官以外の侵入を許すことになるとして排除された。1990年の時点では、30人に膨れあがったNSA所属の暗号数理専門家がアルゴリズムの完成度と機能の確認作業に入り、1992年に確認を終えた。Bob Davis, The Wall Street Journal, Clipper Chip is Your Friend, NSA Contends NSA seeks to Dispel Misgivings of Public About Clipper Chip 1994年３月22日。

24）チップに採用されたSKIPJACKアルゴリズムは、政府評価チームの結論によると、18ヶ月毎にコンピューターの計算能力あたりの単価が半額になると仮定した場合、SKIPJACKを総当たり式（全ての鍵を片っ端から試みる鍵解読法）に解読する費用がDESの鍵の解読費用並になるまでには36年かかる見込みであり、従って向こう30～40年間は総当たり攻撃を持ってしてもSKIPJACKが破られることはない。なお、業界関係者は、コンピューターの性能向上のペースを半年から１年で倍増と見積もり、SKIPJACKの安全期間はおよそ12～18年とみている。Lance J. Hoffman, Faraz A. Ali, Steven L. Heckler, Ann Huybrechts, 暗号、政策及び技術傾向 1993年12月１日。

25）この２つの鍵がペアであって初めて機能する。

捜査当局が暗号を平文化することができるものである。鍵の預託は、チップが製造された時点で生成される２つの鍵[25]（数列）を司法長官が定める二つの鍵預託データベースにそれぞれ分けて厳重に保管される方法をとり、鍵預託機関として財務省のAutomated Systems Division及び国家標準技術院（National Institute of Standards and Technology：NIST）が指定された[26]。

しかし、クリッパー・チップは、発表直後より様々な問題点が指摘[27]され、政府の思惑とは全く正反対に茨の道を進むことになった。

まず、政府が傍受できるような暗号製品[28]の需要そのものに疑問が呈された。米国製品以外にいくらでも盗聴機能を有しない製品が出回っているので、テロリスト等が敢えてクリッパー・チップを使用するはずが無いという意見が表明されたのである[29]。この点についての政府の思惑は、FBI等が9000セットも発注して買い上げ、政府標準とすることによって、政府と通信しなければならない企業等はそのためにもクリッパーを導入せざるを得ないという前提に立ち、およそテロリストと言えども日常的に何らかの形で外界と連絡をとらねばならず、クリッパー・チップが標準化されていれば結果的にクリッパー・チップを使用してその痕跡を外界に残すことになるというものであった[30]。また、FBIの捜査における盗聴そのものの効用についても、情報が爆発的に増加した今日の時代においては

26）1994年２月４日Janet　Reno司法長官の発表。なお、Jay　Levin, 1994年２月11日付New York　Unix誌によると、ゴア副大統領（当時）は、鍵預託機関が二つとも「行政機関」に属することはチェック＆バランスのシステムが欠如していると問題視し、変更の要があると述べた。

27）暗号の権威であるWhitfield　Diffie氏は公聴会において「クリッパー・チップの発表の後一月の間入手し得る全ての情報から判断するに、この提案は、良くとも時期尚早であり、最悪の場合、執行面での効果を期待できないばかりか、ビジネス上や権利上のダメージを被ることになる」と発言。下院エネルギー・商業委員会　通信及び金融サブコミッティーにおける公聴会　1993年５月11日。

28）本人は傍受の事実を知り得ない。

29）William Safire, ESSAY：“ *Sink the Clipper Chip* ”, New York Times,　1994年２月13日。

時代錯誤であるとの指摘とともに、もはや将来の法執行や諜報の世界においては、「暗号能力」は全ての「復号力（解読力）」を上回っているというパラダイム・シフトに直面しているとの指摘もなされた[31]。また、政府は、「政府の押しつけ」との懸念をもたれることを心配し、経済分野における強力な暗号の必要性を強調するとともに、あくまでも必要に応じた「任意」のものであると強調[32]し、国民のための措置であることを前面にだして抵抗感をなくそうと努めた。

しかし、要の鍵の預託システムそのものについても、権限の乱用等、捜査当局による適正な運用が完全に確保されるかどうかの点で信頼性を得られなかった[33]。

なお、決定的な問題点の指摘は技術面にも及んだ。1994年６月２日付のNew York Times, San Jose Mercury Newsは、AT&Tベル研究所の科学者マシュー・ブレイズ（Matthew Blaze）氏の報告書を紹介し、電子計算機の専門家

30）クリッパー・チップの評価チームに在籍したジョージア大学のDorothy Denning氏は、クリッパー・チップ・イニシアティブを国家の安全、効率的な法執行面と、プライヴァシーや産業の成功との関係において考えられる最もバランスのとれた案と評価。数々の盗聴による犯罪検挙例を挙げて盗聴の効用を説くとともに、当該チップを使用した機器のシェアが広がりさえすれば、他の機器を用いる可能性も小さくなるとの考えや、DESがより厳しい輸出管理対象であり続けるのに対し、クリッパーを組み込んだ製品は輸出が容易なので、業者としても採用するインセンティブになるだろうとの考えを表明。Dorothy Denning, *Encryption and Law Enforcement* 1994年２月21日。

31）William Safire, ESSAY：“*Sink the Clipper Chip*”, New York Times,：1994年２月13日。

32）NISTリリース 1994年５月３日

33）ニューヨークタイムズの社説もクリッパー電話が標準となることに疑義を呈し、政府がクリッパー・チップの奨励にとどまらず、電話会社に同技術の採用を義務づけることの懸念を示した。また、鍵預託システムの濫用を防ぐ観点から司法か民間がその管理を行う必要性に言及した。Editorial：“*A Closer Look on Wiretapping*”, New York Times, 1994年６月12日。

34）同記事によると、NSAのMicheal A. Smith政策局長は、法執行側のアクセスを回避するような者は、ブレイズ報告による複雑な手法を用いるよりは、他の簡便な方法をとるであろうとコメントした。

であれば、クリッパーの技術を逆手にとって、政府自身は解読できないような暗号化が可能であるとして、クリッパー・チップの根本的な欠陥を発見したと公表したのであった[34]。

政府は、クリッパー・チップを含めた暗号輸出管理に対する不評[35]に対応すべく、クリッパー・チップ・イニシアティブを施行して約一年後に規制緩和を盛り込んだ若干の改訂[36]を行ったが、DESを含めて強度の暗号を規制し続ける路線は変わらず、実質的な変更があったものではなかった。米暗号業界では、既に多数の国々で流通しているDES暗号を規制対象とし続けることに疑問が持たれ、他国の企業が世界市場を席巻し、米国企業が著しくそのシェアを失いかねないと危機感をつのらせた[37]。その危機感は経済・商業的な分野に限定的でなく、米暗号関連企業のハンディキャップは、結果的には米国の安全保障基盤を損ないかねな

35）輸出管理の厳しさのみならず、許可申請手続きにあたってNSAの製品審査を受けなければならないが、公式には通常１～６週間の審査期間を謳っているが実際には10ヶ月もかかる例もあり、月単位の技術進歩があるハイテク分野においてこの遅延は大量の市場を失いかねないとの不満もあった。Lance J. Hoffman, Faraz A. Ali, Steven L. Heckler, Ann Huybrechts, 暗号、政策及び技術傾向　1993年12月１日。

36）承認を受けた地域については個別許可申請（輸出許可申請を案件毎に行う方式）が不要となった。米国民は、一時的に持ち出す個人使用目的の暗号製品・ソフトウェアについて許可申請を免除されることとなった。鍵預託暗号製品については、最初の審査以降ほとんどの最終需要者（エンドユーザー）に向けて輸出が可能となる他、特別許可手続きの対象となった。マーサ・ハリス政治軍事担当国務次官補演説　1994年２月４日。

37）DES暗号はもとより、RSA方式の暗号を応用した製品を開発し、インターネット上に公開され米国内外の一般に流通することになったPretty Good Privacy（PGP：Phil Zimmermann氏が開発）の例等もある。PGP：1976年にWhitfield Diffie, Martin Hellman両氏によって開発された公開鍵暗号方式に引き続き1977年に実用化されたRSA公開鍵暗号方式（Rivest, Shamir, Adlemanの３人の米マサチューセッツ工科大学研究者の開発による。３者の頭文字から）を応用した暗号で対称鍵はIDEAを用いている。公開後、RSAとの関係でパテントの問題や、米国政府の暗号輸出規制との関係で問題となったことがあるが後にパテント問題、輸出規制問題とも解決している。

いとさえも思われるようになっていた。

その後数年間は政策の大きな変更がない状況下で、更に暗号業界にとって危機感をつのらせるだけの期間が続くことになる。輸出管理に縛られての競争力低下の懸念[38]だけでなく、自らのデータを守る手段としての暗号の強度自体がマイクロプロセッサーやコンピューターの飛躍的な進歩の前に次第に脆弱化してきている事態にも直面し始めたのである。例えば、政府が輸出許可対象としていた40ビット鍵の暗号については、1995年後半の時点で、総当たり攻撃（鍵解析）の前に殆ど防御性が無いことが示されてしまった[39]。この関連で、米暗号有識者は40ビット程度の暗号は安価かつそれなりの速度で解析する手段があることを指摘し、今後最低限耐用可能な暗号の鍵長は75ビットとの見解を示した[40]。業界全般の認識も40ビットを弱い暗号、64ビットを良い暗号、80以上を強い暗号とみているよ

38）米国暗号業界の国際的な競争力の低下については1996年１月11日の商務省報告書においても米国の輸出管理によって競争力が阻害されると述べていることから意識はされていた。Surprise, Surprise–Commerce Report Says Encyption Export Controls Hurt Industry：The Export Practitioner 1996年２月号。

39）フランス、パリの高等技術院（Ecole Polytechnique）の２名の大学院生がネットスケープ・ブラウザ（ネットスケープ社）のRC４アルゴリズムに対して総当たり解析を行ったところ数日で成功した。

40）通常のコンピューターではなく、フィールド・プログラマブル・ロジック・アレイ（FPLA）を用いた場合、安価かつ強力に鍵解析ができることを指摘している。400＄程度のFPLAで平均的な40ビット暗号解析所要時間は５時間程度、10000＄かけて25のFPLAを活用すればおよそ12分、また、ASIC（Application–Specific Integrated Circuits）を用いれば１秒間あたり２億鍵試験できる。Matthew Blaze, Whitfield Diffie, Ronald L. Rivest, Bruce Schneier, Tsutomu Shimomura, Eric Thompson, Michael Wiener, “*Minimal Key Lengths for Symmetric Ciphers to Provide Adequate Commercial Security*”1996年１月参照。

41）Encyption at a Crossroads–The First of Many：The Export Practitioner 1996年１月号。

うであったが、40ビット暗号の解読事実により40ビット暗号は「弱い」暗号とすらも認識されなくなった[41]。

⑹　鍵管理基盤：KMI[42]

このような状況下、DES暗号の輸出管理無意味論を含めた規制緩和要請が最高潮に達し、コンピューターのセキュリティ上の損害が無視できない状況になってきたこと[43]や、重要インフラ防衛委員会（Critical Infrastructure Defense Committee）の創設[44]等にみられるように政府も暗号による防御態勢の重要性を認識し始めたこと[45]等を背景として、1996年、政府は新たな政策を打ち出すに至った。10月１日に発表され、12月30日より施行された暗号規則の改定[46]は、政府に鍵を預託することへの不安や不満に対する対処として、鍵の管理先として政府以外の第三者による鍵管理システムを提唱する内容へと変更されたのである（キー・リカバリー方式）。改正規則の趣旨説明にも記述があるが、このイニシアティブのゴールは世界的な鍵管理基盤（KMI）の構築を意識したものであった。このよ

42）Key Management Infrastructure

43）13のコンピューター企業の代表より構成されるComputer Systems Policy Projectの報告書によると、1995年度のコンピューターのセキュリティ・システムの侵害による損害額は、20億～40億ドルの見積もりで、５年で倍増すると見積もられている。1996年６月16日米議会公聴会。

44）Commission on Critical Infrastructure Protection：CCIP。1996年６月15日に署名された大統領令13010号によりテロリスト及びその他の攻撃から国家の重要インフラを防御するための方策、法律、政策提言を任務とする目的で創設。1996年６月16日米議会公聴会。

45）国防総省においては、1995年度一年間におけるサイバー攻撃件数は25万件にものぼる。CIAもサイバーアタックの危機管理対象レベルをほぼトップレベルに位置づけることとした。NSAの報告によると世界中で約100カ国が情報戦技術に取り組んでいる。1996年６月16日米議会公聴会。

46）Federal Register/Vol. 61, No. 251/1996年12月30日参照

47）1996年７月25日の上院商務委員会における発言

うに鍵管理のシステムを一般化、国際化しようとするに至った背景は、言うまでもなく米国単独の鍵管理システムでは国際市場において需要を勝ち得ないとの懐疑的な世論によるものである。ウィリアム・ラインシュ商務次官は[47]、NSAと緊密に協力しつつ、各方面とも接触して情報収集[48]、意見交換をしてKMIアプローチを検討し、英国も同様のアプローチを採用していることを説明するとともに、米国は二国間交渉や経済協力開発機構（OECD：Organization for Economic Cooperation and Development）において精力的に国際的なKMIの整備にむけて働きかけていると述べている。実際に米国の暗号に対する立場への理解を求めるため、デイビッド・アーロン大使（暗号特命代表）を任命して交渉にあたらせた[49]。

なお、安全保障上の観点から特別扱いすることの限界により、それまで国務省所管のITARによる軍需リスト（USML：United States Munitions List）の下管理していたものを商務省所管下の輸出管理リスト（CCL：Commercial Control List）に移管することとなった。問題となっていたDESや同等の機能を有する56ビットまでの暗号については、キー・リカバリー機能を有していなくとも、暗号製造業者が移行期間として設定された２年間の間にキー・リカバリー機能を有する暗号製品を開発し、KMIの整備を支持すると約束することを条件に許可例外（License Exception）により輸出が可能となった。なお、若干の緩和が行われたように見受けられるが、その基本を貫いていたのは、11月15日の大統領メモランダムにあるとおり、暗号の国外使用は、米国の国外政策と国家安全保障を脅か

48）国際市場を把握するために、31の各地の米国大使館の商務部を活用して、各地の暗号需要及び米国製品のシェア、関連法制度を報告させた。また、外国の暗号製品の分析についても、28製品を購入してNSAにその強度や弱点を分析させた。

49）仏、英、独、ベルギー、カナダ、欧州委員会、OECDと接触。全ての政府が経済上暗号を重要と認識し、電子商取引の発展によりプライヴァシー保護の必要性を感じており、KMIと認証システムの国際協力が重要と認識されており、政府及び信頼機関による合法的なデータ等へのアクセスや、鍵預託が一つの可能性と認識していると報告。RSAデータ・セキュリティ会議におけるアーロン大使のステートメント　1997年１月28日。

し、暗号の国際犯罪組織による使用は、他国民も含め内外の米国市民の安全を脅かすものと位置づけており、相変わらず輸出管理の必要性を前面にだした性格のものであった。

いずれにしても、キー・リカバリーのイニシアティブも56ビットの暗号製品輸出の非規制の維持をちらつかせることにより、政府の各製造会社等への関与度を高めようという意識が見え隠れするようになったこともあり、長続きはしなかった[50]。

(7) 緩和法案

この頃には米国の両議会にも問題意識をもつ議員が様々な法案を提出し始め、議論を戦わせるようになった。

1997年２月には、ボブ・グッドラット（Bob Goodlatte）下院議員によるSAFE（The Security and Freedom Through Encryption Act）（H.R. 695）法案が提出された[51]。同法案の要点は、一般的に入手可能（Generally available）か、関心を有する一般人にとって一般的にアクセスが可能（Generally accessible to the interested public in any form）である「暗号機能」を有するものを含むソフトウェアは輸出許可を有しないことと、暗号を組み込んだハードウェアについては、軍需用途外であり、米国外において同様の製品が入手可能である場合には輸出が承認されるというものである。同法案についての公聴会[52]において、グッドラット議員は、輸出管理を撤廃する趣旨のものではなく、市場にて一般的に入手できる米国暗号製品の輸出を可能にするものであり、政府用の裏口（合い鍵）を個人

50）ケネット・フラム米ブルッキングス研究所外交政策研究プログラム・シニア・フェロー、政策ブリーフ“*Deciphering the Cryptography Debate*”1997年７月

51）1996年に一度法案を提出し（H.R. 3011）、H.R. 695は２度目の提出。1999年２月には三回目の法案を提出（H.R. 850）。グッドラット議員のホームページ参照。http://www.house.gov/goodlatte/encrypt.htm

52）1997年９月４日のSAFE法案（H.R. 695）にかかる公聴会

や会社用のコンピューターに設けることを禁止することを目指したと説明した。この公聴会だけを見ても賛否両論[53]に分かれたが、この法案は最終的には否決されている。

また、ほぼ時を同じくして上院においても緩和案が提出された。コンラッド・バーンズ（Conrad Burns）上院議員によるPro-Code（The Promotion of Commerce Online in the Digital Era Act of 1997）（S. 377）法案である。これも下院のSAFE法案のように、一般的に入手可能である類（マス・マーケット[54]）の暗号ソフト及び同ソフトウェアを内蔵するハードウェアについては、暗号鍵預託標準を課することなく、自由に輸出可能とするものであった。併せて、マスマーケット基準に合致しなくとも、軍事、テロ活動目的に転用されるおそれがあると商務省が判断しない限りにおいて外国銀行にも輸出できるという方向性を打ち出したが、上院商務委員会の投票によって12票中８票の反対により否決されるに至った[55]。

逆に、マッケイン（McCain）及びケリー（Kerrey）上院議員によって提出されたThe Secure Public Networks Act（S. 909）はかなりクリントン政権によるキー・リカバリーイニシアティブの内容を踏襲した内容となっていたため暗号規

53）Lofgren議員は、既存の輸出管理法令の見直しを行わないことは暗号産業自体の存続に関わると主張して法案を支持したが、ラインシュ商務省次官は既存のキー・リカバリー方式は機能しているとの認識により基本的に法案に反対であったし、Litt司法省犯罪局司法副次官補は、司法省としては、解読不可能な暗号の拡散と使用は、司法省の米国民保護能力を無力化するものとして憂慮しており、現状での法案には反対であった。

54）マス・マーケット（Mass Market）：米商務規則等においては、小売販売店の在庫より店頭販売、通信販売、電話注文により一般に入手可能な製品をさす。

55）“*Encryption Legislation Runs Short on Time, But still high on Agenda*”, The Export Practitioner 1996年10月号

“*Battle of the Bills*”, The Export Practitioner 1997年５月号

“*Secure Public Networks Act*”Positions itself as a Likely encryption candidate”, The Export Practitioner 1997年７月号

制派の支持を集めるとともに、SAFE等の緩和法案の内容も一部加味していたところから議論の中心は当法案に移行していってしまった。

このような中、商務省は必要に迫られて1997年５月、金融関係に対する規制緩和を発表した[56]。電子商取引の進展の中、米国の銀行関連会社については、その金融取引にかかる使用目的のために特に設計された上で顧客に提供される暗号製品については輸出が許可されるという内容であった。しかし、同時に政府はキー・リカバリーを継続するとも明言している。

なお、暗号の見識者は、純粋に技術的観点からキー・リカバリー・システムの評価を試みた報告書を発表した[57]。これは、様々なフォームのキー・リカバリー・システムについて個々に政策評価をすることを目的としたものではなかった。同報告書中、キー・リカバリー・システムは、同システムを有しない暗号機能と比べた場合、３つの側面における懸念があることが指摘されている。①危険性：キー・リカバリー機能の不具合等によって、情報の保全性自体が危うくなる可能性がある、②キー・リカバリー機能自体が暗号機能に比べて遙かに複雑な機能となってしまう、③企画、施行、運用の全てを見た場合の費用が多大になるおそれがあるとの評価である。また、その他にも、鍵の預託側等を含めた人的信頼性の問題（預託者の信頼性確保のための手法に始まり、例え政府機関であったとしても自国関係企業等の利益のために濫用する可能性もある）や、鍵預託先のデータベースといった集合的な鍵の管理・保管手段は、外部からの格好の攻撃対象を創設することになるといった問題が存在すること、そして政府から民間までを含めた極めて幅が広く、かつ緊密な連携のとれた体制を構築する類まれな規模

56）1997年５月８日付商務省プレスリリース

57）Hal Abelson, Ross Anderson, Steven M. Bellovin, Josh Benaloh, Matthew Blaze, Whitfield Diffie, John Gilmore, Peter G. Neumann, Ronald L. Rivest, Jeffrey I. Schiller, Bruce Schneier. The Risks of Key Recovery, Key Escrow & Trusted Third Party Encryption：A Report by an Ad Hoc Group of Cryptographers and Computer Scientists：Digital Issues no. 3, 1998年６月

でのスキームを予定しなければならないが、暗号使用の状況は爆発的に拡大しているといった点を指摘した。

1998年９月には、暗号にかかる商務省規則の改正[58]を行い、上記1997年の５月の改正の流れを受けて、45カ国の特定の国向けの金融、保健・医療、社内内部情報の保護目的関連の輸出規制緩和を行った。また、米国企業の本社と支社間の通信に使われる場合は、鍵長や、リカバリー機能の有無とは無関係に輸出が許可されることとなった。DES及び同等の機能を有する暗号については、一回の技術審査の後、輸出が可能となり、キー・リカバリー計画書の提出要件は撤廃され、同時に途中経過の報告義務も撤廃され、簡素化されたキー・リカバリー政策へと移行した[59]。また、同年12月には更に同規則のアップデート（緩和）が施行された。

1998年の規則改正から一年後の1999年９月、クリントン政権はさらなる規則改正を発表した。なお、発表時点では同年12月15日を発効予定としていたが、その

58）1998年９月22日の改正。Federal Register/Vol. 63 No. 183/1998年９月22日

59）簡素化することによって、キー・リカバリー政策を推進しようとの考え。ホワイトハウス報道官発表。1998年９月16日

60）小売製品（Retail）

⑴ 以下のいずれかに該当することにより一般的に入手可能なもの。

㈠ 製造者から独立した小売店において有形にて販売されるもの

㈡ 個人消費者使用のために特に設計され、有形ないし無形の形態にて販売及び移転がなされるもの。

㈢ 電話取引、電子取引、郵送取引において制限無く、大量に販売されるものであって、

⑵ 次の全てに該当するもの

㈠ 暗号機能が利用者によって容易に改変できないもの

㈡ 設置及び利用にあたって、特に支援を必要としないもの

㈢ 暗号機能が変更されたり、消費者固有の改造がなされていないもの

㈣ 大量通信用に設計されたスイッチや高機能ルーターといったネットワーク基盤製品でないもの

後内容をめぐって暗号業界との調整がつかず、約一月ずれ込んだ2000年１月14日の発効となった。

この改正により、45カ国の輸出国リストは廃止されテロ支援国である７カ国以外の全地域を対象に、技術審査及び分類の後、他国政府ユーザー以外であれば、鍵長に無関係に輸出ないし再輸出が可能となった。また、小売暗号製品[60]については、技術審査と分類手続きにより「小売製品」とされた場合には、テロ支援７カ国[61]以外の全地域について、全ての使用者を対象として鍵長に無関係に輸出ないし再輸出が可能となった。この規制緩和により、一度技術審査を経て輸出許可対象となった暗号製品については、その後製品の設計変更等により鍵長が変更になっても追加的な技術審査を受ける必要が無くなり[62]、鍵長による規制概念が米国の暗号規制からなくなった[63]。

引き続き７月17日に１月14日の改正のアップデートが発表され、これに従い、10月19日に改正が施行[64]された。これは、最新の技術動向や、EUとの関係を意識した大幅な緩和措置を内容とするものになっている[65]。先ず、EU加盟15カ国に８カ国を足した23カ国については、暗号解析装置及び同技術以外は許可例外下で許可を要せず輸出が可能となった。手続き面でも申請と同時に輸出を開始してよいとされるなど簡素化が進んだ。また、ブルー・トゥースや類似技術の将来性に鑑み、短距離無線通信技術は許可を要せず輸出が可能となった[66]。その他にも、

61）米国政府の定めるテロ支援国家：北朝鮮、イラン、イラク、リビア、キューバ、スーダン、シリア。

62）暗号機能についての変更は再度技術審査を受けなければならない。

63）一部例外規定はあるが、64ビット以上の鍵暗号についての報告は義務づけられた。

64）Federal Register/Vol. 65, No. 203

65）Federal Register/Vol. 65, No. 203の背景説明中に、EUが６月に施行した23カ国向けの輸出規制緩和実施に際し、米国企業が不利にたたされず、効果的に競争するための政府決定との記述がある。

66）技術審査や報告義務も要しない。

オープン・クリプトグラフィック・インターフェースや、ベータテスト・ソフトウェア、ソースコード等についての緩和がみうけられる。

2．米以外の地域・国家による暗号政策

⑴ EUの暗号政策

1995年頃のEUは既に、グローバルな電子コミュニケーション時代における社会・経済的インパクトの観点から、暗号関連製品やサービスのビジネス、個人ユーザー、公的サービス分野において増大する重要性を認識しており、電子商取引や暗号、関連サービスの流通や使用の自由の確保の観点から、域内市場機能の保全の重要性を意識していた。また、同時に世界レベルでの暗号製品やサービスにかかる相互互換性のある枠組みの構築の必要性についても同様に重要と位置づけていた。その一方で、暗号による秘匿された通信は、加盟国が犯罪に対抗し、国家の安全を維持する上で懸念となることについても指摘されている。なお、EUは電子認証・保全製品とデータの秘匿のための製品の相違を区別してきている[67]。

このように、データ保護の重要性が認識される中、1995年10月24日付の「個人データ処理における個人保護および自由移動に係る指令」が３年間の国内実施期限を経て、1998年10月25日に発効した[68]。これは、経済活動または行政活動の一部として、または、それらの団体の活動に付随して、個人データを収集、保管ま

67）Conclusions of the“ *Telecommunications* ”Council on the Communication entitled “ *Security and Trust in Electronic Communication–towards a European framework for digital signatures and encryption* ”from EU official HomePage

68）Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ No L281, 23.11.95 p 31

69）庄司克宏　平成11年３月（資料）EUにおける「個人データ保護指令」個人データ保護と域外移転規則　横浜国際経済法学第７巻第２号

たは移転する者が遵守しなければならない共通規則を定立したものであり、EU域内における個人データ保護の水準が損なわれるのを防ぐために、EU域外国への個人データ移転を規制し、保護の十分な第三国に限り認めるものである[69]。これは、単一市場を背景として各EU加盟国の様々なデータ保護指令を調和させることによりEU域内における個人データの自由移動を確保することが狙いであり、これにより、消費者の信頼が醸成され、また加盟国間におけるデータ保護指令の相違が最小化され、その結果としての電子商取引の発展が見込まれている[70]。また、同指令第８部第17条はデータ処理の安全確保を規定しており、加盟国に対して特にネットワーク上のデータ伝送を含む場合のデータ保護措置を実施しなければならない旨規定していることから暗号によるデータ保護が視野に入っているものと思われる。なお、この指令は米国においても色々な憶測を呼ぶこととなった[71]。EUが米をデータ保護遵守国と認定するか否かによって、米国のEU域内におけるあらゆる活動に支障が生じてくる可能性があったからである。航空会社やホテルチェーンに始まる顧客名簿データや、製薬会社の臨床実験データ、保険、金融等多岐にわたるデータの移転がその管理下に置かれることになるということを懸念してのことであった。

更に時代は下って、1999年にベルリンで開催された「欧州における情報の安全に対する対処」会議のオープニング・スピーチ[72]でも、欧州におけるインター

70）Data Protection：Background Information（EU公式ホームページ参照。http://europa.eu.int/comm/internal market/en/media/dataprot/backinfo/info.htm）

71）The European Union Privacy Directive　1998年５月７日の米下院欧州連合に関する国際関係委員会における発言。Robert E. Litan Senior Fellow, Economic Studies The Brookings Institution（The Brookings Institution ホームページ参照）

72）“ *TRUST AND SECURITY IN ELECTRONIC COMMUNICATIONS*：*THE EUROPEAN APPROACH* ”Erkki Liikanen Commissioner for Enterprise and Information Society European Commission Information Security Solutions Europe（ISSE 99）Welcome Address Berlin, 4 October 1999

ネットの重要性とそれを支えることとなる電子認証や秘匿のための暗号の重要性について指摘されており、暗号によるプライヴァシーに対する懸念の払拭なしにインターネットや電子商取引の拡大はあり得ないとの意見が表明されている。また、域内市場の保全は、暗号市場や同業界にとって重要と述べている。

EUにおける暗号の輸出管理は、一般的には汎用品輸出管理規則によって実施されてきており、1994年12月のEU理事会規則No. 3381/94の下で汎用品を定めた中で管理対象としてきた。その後、輸出管理の体制強化と効率化をめざした2000年９月28日施行の新汎用品規則においても暗号の管理は同様に引き継がれている[73]。なお、それまでEU域内についても管理対象となっていた暗号については域内については大幅な規制緩和を実現した他、2000年末のワッセナー・アレンジメント（WA）の大幅な暗号の管理水準緩和の決定を受けて同様に緩和された。

⑵ フランスの暗号政策

仏は、欧州はもとより世界でも希有な暗号管理国家であった[74]。

仏は1990年の法により、国内外の安全保障上の利益を守るため、暗号の供給、輸出、使用の規制を定めており、国内をも対象にした最も厳格な暗号管理を行っている国の一つであった[75]。

なお、1990年の法によれば、伝達する情報の内容の完全性を証明するための署名（電子署名）については事前登録するのみで良いが、情報の秘匿を目的とする

73）汎用品の輸出管理リストはワッセナー・アレンジメントをはじめとする国際輸出管理レジームの管理品目リストを踏襲している。なお、域内については、2000年の規則によりかなり緩和された。

74）ロシアも厳格な政策をとっていた希有な国である。エリツィン大統領は、承認されていない暗号の開発、輸入、販売及び使用や、情報の保管、加工、伝達に対する技術的な保護手段を禁止した。Michael Froomkin, 1996 U. Chi. L. Forum 15

75）露も同様に国内管理を行っている。一方で米国は国内への輸入や使用については自由。

76）Service central de la sécurité des systèmes informatiques

暗号使用については事前の許可申請を要した。この法の下で、年間およそ100件ほどある許可申請は、情報システム中央局[76]に送られ、暗号システムの審査に6カ月を要したといわれる[77]。

しかし、フランスでもインターネットの普及とともに暗号の使用が広まり、その結果として1998年には、通信上の暗号使用について規制緩和を発表するに至った[78]。これは、政府が容易に解読できる程度の40ビットまでの弱い暗号については自由化[79]することとし、それ以上の強度の暗号については第三者（機関[80]）に鍵を預託するものであった[81]。

フランスも米国と同様に、暗号の一般的な使用は組織犯罪やテロリズムを助長するとして理由付け、その使用を制限し、鍵の預託を求める等、暗号を諜報、外交、軍事分野における使用に限定的な政策をとってきており、第三者への預託システムはその延長にあるものである。

しかしながら、1999年1月に開催された情報社会のための閣僚委員会においてリオネル・ジョスパン首相は、国外の電子的スパイ手段の開発の前に、情報交換の秘匿性の保護と私人の生活の保護の観点から暗号は必須の手段であるとの見解を示し、これまでのフランスの暗号政策に対して180度の方向転換を示したので

77）“ L ‘ *Exception* ”cryptographique française ”, Le Monde（Paris）, 1995年9月30日

78）1998年3月25日付官報

79）リオネル・ジョスパン首相は56ビットまで緩和することを約したが、クリスチャン・ピエレ産業大臣は、技術的な観点及び解読費用の観点から保留した結果40ビットとなっている。

80）第三者機関として承認を受けるには、政府より承認された最低6人の管理者を置かねばならず、その内2人は、鍵の必要時に備え24時間体制を確保しなければならない。Les apports des décrets du 25 février et 23 mars 1998 en matière de cryptographie, Alexandre Menais, Juriscom.net ホームページ、1998年4月

81）Herve Morin,“ *La France redifinit sa réglementation en matière de cryptologie* ”, Le Monde（Paris）, 1998年3月28日

あった。早速、この方向転換によりそれまで使用が許されていた40ビットの暗号に代わり、128ビットの暗号までその使用が自由化された。なお、同時に政府の暗号解読能力の引き上げを強化することも決定されている[82]。

⑶ OECDにおける暗号の位置づけ

OECDにおいてもインターネットの普及と併せてデータ保護の重要性について認識し、1990年に情報、コンピューター、コミュニケーション政策委員会[83]を設置して専門家による情報システムのセキュリティに係る指針の策定作業を行った[84]。

様々な議論の中で特筆すべきは、仏、米、英によって推奨された第三者預託方式であるが、他の加盟国の反対を呼び、1997年３月27日に発表されたOECDの原則では暗号の自由化を推奨する内容となり、第三者預託方式の全面的な採択とはならなかった[85]。

３．暗号の戦略性

⑴ 暗号の防御性

暗号は通常、通信やデータの保存の際にその情報を閲覧されたり、奪取された場合に、第三者に知られたくない情報を秘匿するための防御手段として使用される。その秘匿度は通常の国家においては、国家の存続に関係する国家機密レベル、すなわち軍事機密や外交機密が最も高く位置づけられており、それらの傍受は、

82）Henri Morin,“ *La France mise sur la cryptologie pour se proteger* ”, Le Monde（Paris）, 2000年２月22日

83）Information, Computer and Communications Policy（ICCP）

84）Guidelines for the security of information systems/OECD

85）Annie Kahn,“ *L ’OCDE préconise de liberaliser le cryptage* ”, Le Monde（Paris）, 1997年４月７日

国家の安全保障上や外交上不利に働くばかりでなく、最悪の場合には国家の存亡にも関わる重大さを持っている。当然のことながら、これらの情報は絶対に対外的に漏れてはならない性質のものであり、暗号は最大の防御手段である。

⑵　情報の戦略性

国家の保有する機密情報には程度の差はあるにしてもそれを守る当事国や同盟国等とそれを知られてはならない第三国という関係が存在する。知られてはならない情報とは、第三国にとって有益な情報であったり当事国や同盟国にとって不利な情報であり、なんらかの形で第三国に有利に働く情報といえる。従って、この情報をとりまき防御する側と入手しようと（奪取・傍受）する攻撃側が存在することになる。このように、国家戦略上、相対的な有利や不利をもつことを情報の戦略性といえ、その度合いにより情報価値の高低が決まってくる。

⑶　情報収集の戦略性

秘匿されているか否かに関わらず、自国の軍事・外交・経済・その他の観点から、様々なレベル・分野で情報収集が日夜行われている。特に国防、安全保障、外交、経済面においては必ずしも公開情報に限らず、秘匿された情報についてもその情報価値の高さから積極的に情報収集が行われているはずである。とりわけ重要な機密や時間的に緊迫した事項に関する情報については、その最も攻撃的な情報収集手段としての盗聴・傍受が行われることもある。また、傍受した情報が暗号によって防御されていた場合には、この暗号を解読してでも情報の内容取得に努めるのは必然であろう。実際に、戦争中にはこれにより自国軍を有利に導いている例が多々ある。米国の暗号解読の機密室は、1921年のワシントンでの海軍軍縮会議中の日本側の暗号電報、全権本部への秘密訓電も含めて、およそ5000通

86）H.O.ヤードレー著　平塚柾緒訳、1999年「ブラック・チェンバー」米国はいかにして外交暗号を盗んだか、第12章　日本の外交暗号はいかに解読されたか、荒地出版社

を解読して合衆国政府へ送っていたと解読者が手記を書いているくらいである[86]。

⑷ 諜報機関や盗聴網

特定の情報を入手する目的で個別に諜報活動を行う等、多くの国が独自に盗聴機関や諜報機関[87]を有していること自体はもはや驚くに価しない。なお、2000年初頭に欧州委員会において米国を中心とした盗聴網「エシュロン[88]」の存在が白日の下にさらされ、大きな問題となった。これは、米国、カナダ、オーストラリア、英国、ニュージーランドの間で協定により成立し、米国のCIA（Central

87）例えば、米国のNSA（National Security Agency：国家安全保障局）。Peter Kornbluh（NSAの専門家：80年代にチリ、ニカラグア、キューバ問題担当）がFreedom of Information Actにより入手した書類によりNSAの存在が初めて明らかにされた。彼が入手した書類は、1991年９月３日付のSugar Glove（West Virginia）におけるNSAと544e諜報部隊の合同の電子傍受活動を記したものと、1995年６月15日付でエシュロンに付随するユニットとして、Elmendorf（Alaska）, Yakima（Washington州）, Puerto Rico, Guamの複数の米国空軍基地における活動を記している。Jacques Isnard,“ *Des documents americains confirment l èxistence d Echelon* ”, Le Monde（Paris）, 2000年２月22日

88）Echelon：ヴァール県UDF党のArthur Paecht議員によって2000年10月11日に公開された報告書によると、英国Menwith Hillに設置されたエシュロンの英国の盗聴基地には600人の英国人と1200人の米国人が従事していた。Jacques Isnard,“ *L ’Europe《Piégée》par le réseau d èspionnage* ”, Le Monde（Paris）, 2000年10月12日

89）伝統的な衛星による傍受方法だけでなく、安全だと思われていた海底ケーブルについてもケーブルの発する磁場を確保することにより傍受が可能であった。光ファイバーについても困難ではあるが、不可能ではない。Michel Alberganti/Herve Morin,“ *L ’Espionnage s ’adapte aux nouvelles technologies* ”, Le Monde（Paris）, 2000年２月24日

90）例えば武器販売契約（ブラジル向けレーダー納入に際し、米レイセオン社により仏トムソン社は140万ドル相当を失ったと思われる）や、民間契約（サウディ・アラビアにおける航空機契約でエアバス社がボーイング・マクドネル・ダグラス社に負けた）において不利益が生じた他、WTOにおける米国の優位を確保するためにも利用された。Laurent Zecchini,“ *Comment les Etats-Unis espionnent l ’Europe* ”, Le Monde（Paris）, 2000年２月22日

Intelligence　Agency）とNSAが運営を担い、120の衛星[89]を擁して全世界の電話、FAX、電子データ通信の全てを対象に傍受活動を展開していたというものである。冷戦期に対ソ目的で構築されたこの世界規模の電子的盗聴機関は、麻薬取引や組織犯罪、テロに対しても利用されたという。なお、その後米国の企業のために流用されたという憶測も流れた[90]が、米国はこれを否定している[91]。EUにおけるエシュロンの問題がより感情的に大きく取り上げられたのは、英国がEUの中にあってただ一国エシュロンの恩恵を受けていたところにあった[92][93]ようである。

91）米国国務省報道官は、米国諜報機関は米国企業の利益のために商業的機密を入手したり、産業スパイをすることを任務とするものでない。NSAは私企業に情報を提供する権限を与えられておらず、米国法に厳密に従ってのみ活動をしている。Laurent　Zecchini,“*Les Etat-Unis se Defendent d'utiliser le réseau d'èspionnage Echelon a des fins industrielles*”, Le Monde(Paris),　2000年２月22日

92）Herve Morin,“《*Echelon*》*nous écoute*”, Le Monde(Paris), 2000年２月22日

93）ワシントンのFree Congress Research and Education Foundationによると、エシュロンから情報の提供を受けている第三国として、ドイツ、日本、ノールウェー、韓国、トルコがある。Jacques Isnard,“*Des documents americains confirmet l'èxistence d'Echelon*”, Le Monde(Paris), 2000年３月９日

94）米国のNSAとCIAは共同機関としてSpecial　Collection　Serviceという公式には認知されていない機関を創設し、その活動も秘密下に置かれており、NSAとCIAの暗号解読の専門家によって構成されるチームであることしか解っていない。なお、その目的は、目下世界中における通信防御や暗号の進歩による傍受の困難性や秘密の解読のための手段を米国諜報部に提供することにある。Jacques Isnard,“*Une Alliance secrete entre la NSA et la CIA*”, Le Monde(Paris)

95）Jacques Isnard,“*Groupement des controles radioélectriques*：*GCR. Le Royaume-Uni au coeur du dispositif en Europe*”, Le Monde(Paris), 2000年２月22日

96）Alluets-Feucherolles（Yvelines), Agde（Herault), Domme（Dordogne), Mutzig（Bas-Rhin), Solenzara（南コルシカ), Saint-Barthelemy（Antilles), Reunion, Djibouti, Mayotteにおいて傍受を行っている。Jacques Isnard,“*Le Royaume-Uni au coeur du dispositif en Europe*”, Le Monde(Paris), 2000年２月22日

なお、この盗聴活動の主体が、単なる盗聴・傍受に限らず、暗号により秘匿されたものも対象であったことは想像に難くない[94]。

なお、世界的盗聴網は、エシュロンに限られたものではなく、フランスも独自に世界的な盗聴網を有しており、電波管理部[95]によって各地の都市、海外県等[96]において衛星やその他の傍受活動を行っている。この主体は、対外安全保障総局[97]の別組織から始まった諜報部であり、商業的傍受の疑いをもたれたこともあるという[98]。

４．国際輸出管理体制（ワッセナー・アレンジメント）

冷戦構造の瓦解とともにその役割を終えたココムに代わり、「紛争予防」の観点にその目的を一般化した通常兵器及び関連汎用品・技術の国際的輸出管理レジームとして、ワッセナー・アレンジメント（WA）が発足した[99]。ワッセナー・アレンジメントは、武器（通常兵器）とその関連汎用品及び技術の移転と過剰な蓄積を防止することによって地域の不安定化を防ごうとするものであり（＝紛争予防）、参加国が非参加国に対して行った移転を参加国間において通報し合う制度によって確保されるグローバルな移転の透明性の拡大と輸出管理を主な手段と位置づけている。実質的に移転を防ぐ手段としての「輸出管理」に当たっては、各参加国が遵守する輸出管理品目リストを協議の上作成しており、各々の参加国が自国の輸出管理制度によって実施している。同管理品目については、ほぼココムのものを引き継ぎ、カテゴリー５パート２に管理されている「暗号」規制も引

97）Direction générale de la sécurité exterieure：DGSE. Jacques Isnard,“ *Le Royaume-Uni au coeur du dispositif en Europe* ”, Le Monde（Paris）, 2000年２月22日

98）Jacques Isnard, “ *Le Royaume-Uni au coeur du dispositif en Europe* ”, Le Monde（Paris）, 2000年２月22日

99）Wassenaar Arrangement：事務局をウィーンにおき、33の参加国より構成されている。日本も発足時からの参加国である。

き継いだ。その中で米国をはじめとして、暗号の管理を重視している国々は、国内規制の方向性もあり、ワッセナー・アレンジメントにおいても規制緩和については慎重派であり続けた。なお、WAは経済情勢や技術動向等にも照らしつつ毎年一度の管理品目リストの改訂を行っており、1999年以降は、米も経済的利益の観点や暗号の普及・一般化と合わせる方向で大幅な規制緩和を行い、続いて2000年にも大幅な規制緩和が行われた。その結果、今や鍵長による制限なくマスマーケット製品については輸出が可能となり、かなり時代の要請に応える形に近づいた管理となっている。なお、現在のところは注文生産で特殊な場合等、マスマーケットと認定されない製品については、未だ56ビット（対称鍵）水準を管理水準の基準としている。

5．暗号技術の今後

⑴　高度化する暗号（AES）

米国商務省下の国家標準技術院（NIST：National Institute of Standards and Technology）は、これまで連邦情報保護標準（FIPS：Federal Information Proc-

100）選考過程及び技術的詳細については、NIST （National Institute of Standards and Technology）/Computer Security Divisionの作成したレポートを参照されたい。James Nechvatel, Elaine Barker, Lawrence Bassham, William Burr, Morris Dworkin, James Foti, Edward Roback：NIST：Report on the Development of the Advanced Encryption Standard（AES）

101）ベルギーの暗号専門家であるDr. Joan Daemen（Proton World International）とDr. Vincent Rijmen（ルーヴァン・カトリック大学電子工学部）の２名の共作。

102）AESアルゴリズムの技術的条件は、対称鍵暗号であって、ブロックサイズは128ビット、鍵長は、128, 192, 256ビットの三種類であること。Rijndaelが採用されたのは、安全であり、性能、効率、施行の容易さ、柔軟性の全てを考慮した結果である。とりわけ、ハード及びソフトの双方において良好な性能を示すほか、鍵のセット・アップ時間がすばらしく、メモリー消費もわずかで、限られた環境下における使用にも適している。

essing Standards）として定められたDESアルゴリズムでは不十分との認識にたち、1997年に次世代を担う対称鍵暗号として、AES（Advanced Encryption Standard）を開発することとし、世界中より暗号アルゴリズムを募集し、選定作業を開始した[100]。NISTは、応募のあった暗号を選考にかけ、1998年には15候補まで絞り込み、更に審査を続けMARS, RC6TM, Rijndael, Serpent, Twofishを最終選考に残し、最終的にRijndael（レインダール）[101]をAES候補として推薦することを決定した[102]。このアルゴリズムは、新たなFIPSとして定められることとなる。AESは、DES同様に米国政府が機密以外の重要情報の保護を目的として使用することを予定しており、米国政府以外にも任意で広く広がることが期待されている。AESは、様々な意見聴取等の手続き期間を経た後の2001年春以降に新FIPSとして正式決定される予定となっており[103]、妥当性を常にチェックする意味において採用後も５年毎に見直しの審査を受けることとなっている。

このように、強度の暗号が、国家主導で開発・導入されていく例からも、今後も益々強度暗号の重要性が増していく傾向がうかがえよう。

103）AESファクトシート、NIST/Computer Security Divisionホームページ、2000年10月12日

104）Shoniti Systemが製造したCentury Tapを用いて10Base-T Ethernetに接続される。100 Mbpsの環境下において１ビットの遅延しかないので、ネットワークのパフォーマンス自体には影響を与えない。

105）Carnivoreは、TCP, UDP, ICMPレイヤーのみを対象としており、その他レイヤーのプロトコルの復元には、Carnivore以外に「Packeteer」と「CoolMiner」の２つのデータ・プロセスソフト（２つを併せてDragonwareという）が用意されている。「Packeteer」ソフトは、傍受した全てのパケットから関連パケットのみを合わせて一セッションを復元することを目的とする。「CoolMiner」は、「Packeteer」によって纏められたパケット群を分析するためのWEBブラウザ・ソフトウェア。

106）記録されるパケットは、IPアドレス、プロトコルや電子メールの場合は使用者名によって選別して記録することができ、特別のケースには内容によっても選別できる。

⑵　高度化する傍受技術（Carnivore）

米国では、FBIが電子通信データ傍受用として次世代ソフトの開発を行っている。「Carnivore」の名をつけられたそのシステムは、令状に基づき電子通信の監視を実施する際に使用されることを目的としており、ISP（インターネット・サービス・プロヴァイダ）等が捜査上必要な情報の提供ができない場合等にのみ使用されることとされている。原理的には、イーサネット（Ethernet）上[104]を流れるIPパケット[105]をチェックし、必要なパラメーターに合致するIPパケット若しくはセグメントのみを記録[106]するソフトウェア・ベースのシステムであって、キーワードを基に電子メール等を傍受できるものである[107]。Carnivoreは、ISP等のイーサネットに接続され、キーワードや通信者名、アドレス等を指定することにより、関連の情報を傍受することができるため、従来パケット・スイッチ通信上困難とされていたインターネット上の傍受が可能となる。

この技術の開発は、傍受面の問題の拡大をも提示している。一つは、インターネットの情報伝達方式には国境概念が無いに等しいことに起因する。これは傍受地点が国内に限定されて他国の領域を侵犯しなくとも、パケット通信の性質上ルート指定をしていない限りにおいてはパケット自身が傍受地点を通過する可能性が排除されないため、場合によっては結果的とはいえ領域外における傍受があり得る。また、令状主義等の運用上の制約はあっても傍受の技術的可能性が存在するということは、第三者による類似機能の開発やその不正使用等、合法、非合法の様々な傍受・盗聴問題を内包しているのである。

107）Stephen P. Smith Henry Perrit Jr, Harold Krent Stephen Mencik, J. Allen Crider, Mengfen Shyong, Larry L. Reynolds, 2000年11月17日, IITRI：Independent Review of the Carnivore System, Draft Report、Inside Risks 124, October 2000, Mathew Blaze, Steven M. Bellovin

おわりに

⑴ パラドックスの追求

際限なき暗号の高度化を前に、実効的なレベルでデータを保護しようとする方向性と、例え暗号化されていようとも、それらを傍受し解読しようとする方向性が、様々な局面を経験した米国のような暗号先進国においてもなお存在し、諦めるどころかさらに暗号政策を継続、発展させようとしているところが興味深い。

米国国内のおけるクリッパー・チップや、フランスの第三者預託システムに示されたとおり、ここ10年間の暗号の開発能力と解読能力におけるバランスの推移は、開発力が解読力を圧倒的に凌駕してしまい、合い鍵を用意しない限り、実効的な時間内の解読が不可能であることが露呈された歴史であった。しかし、ある時点で安全と思われた暗号が時間の経過、すなわち技術の進歩にともなってパーソナル・コンピューター程度の計算機を用いた学生に解読されるようになるのもまた一方で事実である。この現代版の「矛盾」の逸話をどこまで続けることになるのか、決定的な方法が見つからない現在は、これまでの姿勢となんら変わることがなく、相対的に強度な暗号力[108]をもって国民の社会・経済活動の安全を確保しつつ、国外からの諜報活動に防御壁を構築していく一方で、必要に応じ、いかなる防御壁をも壊して傍受することができる解読力を身につける競争を続けていくといったアプローチの継続となろう。ただし、素因数分解等をその原理とし、

108）例えば、米国のAESは、DESの鍵を１秒で割り出す（２の55乗の数の鍵の総当たり）ことのできる計算機があったと仮定しても、AES 128ビットの鍵を割り出すためには149兆年を要する。

109）Artur Ekert, CQC Introductions：Quantum Cryptography, Centre for Quantum Computation/Oxford Univ. March 20, 1995

110）同上、他（矢野寿彦：Emerging Technology，日経産業新聞 2000年１月15日）。また、４月16日付の日本経済新聞１面には総務省が産官学共同で2010年を目途に量子情報通信を実用化に向けて研究すると報じている。

実用的な時間内における解読は不可能と言われている現代暗号をもってしても、遅くとも20年後には実現可能と言われている量子コンピュータの前には、脆弱そのものとなってしまう可能性がある[109]。では、来る量子コンピュータ時代には暗号はまた傍受と解読能力のもとにひれ伏すことになるのかというと、一方でその量子を用いた「量子暗号」の研究も進んでいる。微弱な光子の粒子に鍵情報を載せ伝送するというもので、第三者が中途でのぞき見をすると、量子力学的に光子の状態が変化し、解読が不能となるというものである[110]。このように、ある技術が開発されると、ほぼ同水準の対抗法が考案されることが今後も続くとみられ、どちらかの機能が絶対的に他方を上回るような原理が発見されれば初めて両機能の競争から解放されることとなるが、この量子暗号がそのような決め手になるかについても今のところ定かではない。

⑵　国内の治安維持の観点からの暗号政策のあり方

国内における治安一般についての暗号の功罪、すなわち組織的犯罪やテロの捜査・逮捕上暗号の使用が大きな障害になるといった議論も様々な場所で行われてきているが、現代の社会生活上では、起きるかも知れない犯罪に使われる暗号と暗号によって守らなくてはならない人々の日常生活上の利益の比率からしても圧倒的に後者の方が高いことに着目する必要がある。犯罪に関係した通信や情報隠蔽に使われるかも知れないといった可能性だけの恐れから、守るべき国民の自衛する手段や権利を奪うことは、結果的により大規模な損害を生じることになろう[111]。テロリスト等の手口も益々電子世界における攻撃（サイバーアタック）等へとその手法を変更し得る環境が整いつつあり、暗号等の自衛手段の構築がより重要性を増しているのは明らかである。個人を対象とした場合には、個人情報の不正奪取や改竄による、個人の尊厳・名誉の毀損、財政上の損失、個人情報をた

111）Whitfield Diffie, Susan Landau, Privacy on the Line/The Politics of Wiretapping and Encryption, The MIT Press, 1998, pp 240-245

てにした脅迫の可能性等が考えられ、国家や各種機関、企業に対しては、重要な社会インフラ、社内ネットワークの制御機能の奪取や機能停止による実質的な損害や、脅迫の可能性などが想定され得る。このように、国内外から個人やインフラを人質に取ることが可能となっていく中、これらの対象とならない様、個人レベルからの防御力の確立が急務となっている。

犯罪捜査上の問題については、暗号で交わされる通信の傍受・解読のみが主要な手がかりとは到底言えず、暗号通信以外に外界との接触なしに犯罪を遂行できる類の犯罪は極めて希であることも考慮に入れる必要がある。犯罪者とて日常の生活は営まなければならず、宿舎、食事、移動、通信、犯罪準備、犯罪行為のいずれかにおいて犯人は外界となんらかの接触を行うはずであり、情報収集の手段と機会は与えられている。

このような内政上の安定と安全の問題は日本にのみあてはまる事項ではなく、世界的に言えることであり、全ての国の、個人、社会活動の安定があって我が国の安定も享受できるとの観点に立脚した場合、必ずしも暗号製品を厳格な輸出管理対象とすることだけが安全への最短距離とはいえないと思われる。

⑶ 戦略的暗号規制の今後の方向性

上述のとおり、国内の治安維持の観点にたった場合、暗号の使用を規制することは今後、必ずしも得策となり得ない。このような暗号の大衆化時代を迎えた中、暗号の使用や拡散を最も恐れるのは傍受や盗聴を行う主体であるかもしれない。その主体は、会社組織等の産業レベルである場合もあるし、諜報機関といった国家政府レベルのこともある。しかし、強度に暗号化されたものが全て重要な情報

112）インターネット上のソフトウェアの移転等の移転形態を無形移転（intangible transfer of technology/software）というが、無形移転は現在各種国際輸出管理レジームでも問題になっているトピックでもあり、FAX、電話、電子情報移転又は人の移動に付随するので、技術的、法的（人権）問題との兼ね合いもあり難しい問題となっている。法的側面はともかく、執行面（実効的な移転管理）は非常に困難である。

であった時代とは異なり、暗号の大衆化は、とるに足らない情報をも強度に暗号化することが一般化されていく。つまり、暗号化されているという事実をもって、重要な情報であるとのメルクマールにはならなくなってきている。このような現状は、多大な暗号解読努力の末、全く情報価値の得られない状況へと移行してきているとも言えよう。国家的なレベルで暗号を戦略的に位置づけた場合、暗号規制政策の代表として暗号輸出規制が存在してきた。しかし、諜報活動の妨げとなるような暗号を輸出することによって、自らの諜報活動が思うようにできないことを理由に高度な暗号を輸出管理の対象とすることは、先述のとおり、暗号使用の大衆化の環境の中、ソフトウェアとしての移転を妨げることがほぼ不可能であるといった性質や[112]、自己開発が可能である等の理由を勘案するとほとんど意味をなさない時代に入ってきている。商業的や政治的目的に日常使用される標準化された暗号アルゴリズムには暗号の強度のみならず、その暗号化や復号化の速度等の利便性が求められるが、単に情報や通信を隠蔽するために利便性を犠牲にできる人々（＝犯罪者、テロリスト）には現在でも既に無限の可能性が与えられていると言えよう。

いずれにしても、防御手段の拡散によって社会や国家の安全保障が受けるであろう損失の可能性と得られる安全とを衡量した場合、これからはより「安全確保」を追求すべき時代に来ているのではないであろうか。

（筆者は兵器関連物資等不拡散室事務官）