緩和される暗号輸出規制

米国の暗号政策をめぐる論争を考える

前川　徹
情報処理振興事業協会（IPA）セキュリティセンター

先進国の多くは強い暗号技術製品の輸出を規制している．米国政府は従来，鍵長が40ビットを超える暗号については厳しい輸出規制を行ってきたが，1995年以来，数度にわたり暗号技術製品輸出規制の緩和策を発表してきている．その過程で，連邦政府は輸出規制緩和の条件として，復号のための鍵を政府機関などに寄託する仕組みの実装を提案したが，産業界，暗号技術の専門家，市民団体はこれに強く反発し，現在は鍵回復機能の実現は規制緩和の条件ではなくなっている．一方，先進国の暗号輸出規制の基本となっているワッセナー・アレンジメントが1998年12月に改正され，世界的にも暗号輸出規制は緩和方向にある．暗号技術をとりまく状況を考えると，この規制はさらに緩和される方向にあると考えられる．

はじめに■

米国連邦政府は従来から暗号技術を利用した製品（ソフトウェアおよびそれを組み込んだチップなどのハードウェア）の輸出を厳しく規制してきた[1]．それは，強力な暗号技術の利用によって一部の連邦政府機関が行っている諜報活動が阻害され，国家安全保障に影響がでることを懸念しているからである．長期間にわたり連邦政府は，暗号製品は武器等の輸出を規制するITAR（International Traffic in Arms Regulation）に定められている軍需品に該当するという法的根拠に基づいて規制を行ってきた[2]．しかし，情報技術の発達とインターネットの普及によって，暗号技術は国防，外交，金融取引といった限定された世界で利用されるものではなくなってきている．

米国において暗号技術製品の輸出を実際に管理しているのは国務省と商務省であり，暗号技術製品は，証明や認証を目的としたもの，あるいは輸出向けに作られた弱い暗号方式の製品のみに限って輸出を許可する方針を堅持してきた．具体的には，1995年8月に第1回の規制緩和策が発表されるまで，原則として（共通鍵暗号の場合）鍵の長さが40ビットを超える暗号製品の輸出を禁止してきた．鍵の長さが40ビットの暗号であれば，最新のスーパーコンピュータを使えば，比較的短時間で暗号を解読できるからだといわれている．鍵の長さが56ビットのDES（Data Encryption Standard）と比べれば，約6万5000分の1の時間で十分だという計算になる．これが64ビットになると，40ビットに比べて約1600万倍の時間が必要になる．

ちなみにDESは，1977年に連邦政府によって正式に標準として認められた暗号であり，おそらく米国では最も広く利用されてきた暗号である．DESのアルゴリズムは最初，IBM社によって開発されたもので，暗号化と復号に同じ鍵を用いる共通鍵暗号（対称鍵暗号，秘密鍵暗号とも呼ばれる）である．

DESで用いられる鍵の長さは64ビットであるが，そのうち8ビットはエラー訂正用のチェックビットなので，実際の鍵の長さは56ビットである．暗号化された情報の発信者でもなく，受信者でもない第三者が暗号を解く，つまり「解読」する方法で最も一般的なものは，brute-force exhaustive searchと呼ばれる方法である．これは，可能性のあるビット列を順に試してみるという文字通り野蛮な方法であるが，これに優る現実的な方法はない（「線形解読法」や「差分解読法」では解読者が相当量の情報を持っていることが前提になっている）．この方法では最大「2の『鍵の長さ』乗」の試行が必要とされる．つまり，DESの場合，「2の56乗」回以内で解読できることになる．解読に必要な試行回数の平均（つまり期待値）はおよそ「2の55乗」回（約3.6京回）ということになる．1秒間に1回鍵を試みることができるとして，解読に10億年以上かかる計算になる．1秒間に10万回と仮定しても1万年である．しかし，現実にはDESは，1997年に約7万台

のコンピュータを用いて96日間で解読されているし[3]，1998年7月には25万ドル以下の費用で作成された暗号解読用コンピュータによって3日以内で[4]，1999年1月にはわずか22時間15分で解読されている[5]．

暗号鍵を政府に預ける■というアイデア■

連邦政府の新しい暗号技術開発計画

情報技術の進歩によってDESの安全性が疑わしくなってきたという問題と，暗号技術が特殊な世界のものではなくなってきたという問題を抱えた連邦政府は，1993年に新しい暗号技術の開発計画を明らかにした[6]．これが悪名高い「クリッパーチップ計画」である．1993年4月16日にホワイトハウスから発表されたプレスリリースによれば，「電話におけるプライバシーとセキュリティの向上を目的にし，司法当局の合法的要求を満たす」ことが目的であり，クリッパーチップの民間企業における利用は任意であるとしている．

繰り返しになるが，米国連邦政府の最大の懸念は，「強力な暗号技術の利用によって国内外における諜報活動が阻害され，国家安全保障に影響がでること」である．そこで連邦政府は，検討の結果「鍵を政府に預けるというキー・エスクロー（Key Escrow）型の暗号を普及させる」という方針を採用することとした．つまり，連邦政府は，必要なときに（もちろん裁判所の許可を得て）第三者に預けられた鍵を取り出して暗号の復号ができる仕組みを構築する道を選択したのである．

連邦政府の新しい暗号関連計画は次の4つの要素からできていた．

1．暗号標準：EES（Escrowed Encryption Standard）
2．電子署名標準：DSS（Digital Signature Standard）
3．メッセージのダイジェスト化の標準：SHS（Secure Hash Standard）
4．暗号鍵の配送方式

この計画の中核となる暗号標準であるEESの鍵の長さは80ビットになっている．つまり鍵の長さが56ビットであるDESと比較すると，24ビット分だけ強力になっている．一般的に鍵が1ビット長くなれば，解読の難しさは2倍になる．つまりEESはDESより1600万倍以上強力であり，仮にDESを1時間で解読できるコンピュータでもEESなら1800年以上かかるという計算になる．したがって，EESは（アルゴリズムに欠陥さえなければ）当面は安全だと考えられる．

鍵寄託機能付きの暗号

EES（Escrowed Encryption Standard）は，1994年2月4日にNISTから発表された暗号標準で，スキップジャック（SKIPJACK）と呼ばれる80ビットの共通鍵暗号アルゴリズムを採用している[7]．このスキップジャックは，NISTの協力を得てNSAが開発したものである．このアルゴリズムを組み込んだ電話やFAX用のチップがクリッパーチップ（Clipper Chip）である．同様にコンピュータ用に開発されたデバイスは，キャップストーンチップ（Capstone Chip）と呼ばれ，これはPCMCIAタイプIIに適合したフォーテッザ（Fortezza）カードに組み込まれている[8]．ちなみにキャップストーンチップにはEESによる暗号化・復号機能だけではなく，電子署名機能，公開鍵暗号方式による鍵交換機能も組み込まれている．

このEESで使用されているスキップジャックのアルゴリズムの詳細は非公開であった（NSAは1998年6月23日にスキップジャックのアルゴリズムを公開した[9]）．連邦政府は，新しいアルゴリズムの安全性を保証するために，有識者からなる調査委員会を設け，1993年7月に「18カ月でコンピュータの能力が倍になるという仮定をおいても，安全性が現在のDES並になるまでに36年必要であり，またスキップジャックには簡単に暗号が解読できるような抜け道（バックドア）はない」という報告書をまとめている[10]．

クリッパーチップ（およびキャップストーンチップ）の特徴は，鍵を第三者に寄託する機能にある．連邦政府の当初計画によれば，デバイス・キーと呼ばれる暗号鍵を2つに分割してNISTと財務省に寄託する仕組みになっている．クリッパーチップを使って行われる通信には，必ずLEAF（Law Enforcement Access Field）と呼ばれる情報が付加される．このLEAFのある部分をデバイス・キーで復号すると，通信に用いられているセッション・キーが得られる．そのセッション・キーを使えば，暗号化された通信を復号できるという仕組みである．もちろん，連邦政府といえども，裁判所の許可なくしては勝手に鍵を取り出せないことになっている．デバイス・キーを分割して保管することになる機関は，デバイス・キーの半分を管理するだけなので，この機関が盗聴を行う心配はない．また，このデータベース自体も暗号化して保管されることになっている．つまり，第三者が悪意をもってクリッパーチップを用いた通信の盗聴を行おうとすると，2つの機関からデータファイルを盗み，そのデータを解読してデバイス・キーの合成を行う必要があることになる．

市民団体と産業界の反対運動

クリッパーチップに対する反対運動は，1993年4月にホワイトハウスがクリッパーチップに関する計画を発表したときから始まったが，1994年2月以降，市民団体や情報産業界を中心により激しい反対運動が繰り広げられた[11]．反対者が主張した主な問題点は以下の4点である．

- 政府による通信の監視への懸念
- スキップジャックのアルゴリズムの信頼性問題
- 実効性（犯罪者やテロリストはク

リッパーを利用しない）
• 暗号技術の進歩を阻害し，情報産業の競争力に悪影響

まず，政府が電話やコンピュータによる通信を監視するのではないかという指摘については，その仕組みから考えて，大部分は誤解に基づくものだと思われる．ただ，政府が合法的に盗聴を行う手続きを十分知っていながら，連邦政府による監視を心配する声があるところをみると，連邦政府はあまり信用されていないのかもしれない．確かに今の政府が説明している方法では，多少厄介な手順を踏まない限り合法的盗聴は不可能である．しかし，政府がこの手順を変えないという保証はない．すべての電話やモデムにクリッパーチップが搭載されてしまえば，政府が市民のすべての会話を監視することも不可能ではないというのが，反対派の意見である．

第2に，クリッパーチップのアルゴリズムの信頼性に問題があるのではないかという指摘がある．当時，NSAが開発したスキップジャックと呼ばれるアルゴリズムの詳細は秘密にされていた．何人かの暗号の専門家が信頼性を保証しても，どこかに欠陥がないとは断言できない．実際，1994年6月にはAT&T社のベル研究所のマシュー・ブレイズは，偽のLEAFを作り，合法的な盗聴を不可能にできる方法があることを指摘している．チップの設計者は「ブレイズが実験したのはプロトタイプで，すでにこの部分は改良されている」と回答している．しかし，ブレイズが指摘した欠陥は修復済みだとしても，もし，5年後に数千万，数億のチップが利用されているときに欠陥が発見されたら，あるいは誰かが簡単に解読できる方法（隠し扉）を発見したとしたら，大変な問題になる．ニコラス・バランは著書の中で，2000年に一人のハッカーがクリッパーチップの隠し扉を発見してEESによる暗号が解読されるという架空のエピソードを書いている[12]．

第3に，クリッパーチップは犯罪の摘発，防止に有用であると連邦政府は説明しているが，実際にはほとんど役に立たないだろうという指摘がある．つまり，連邦政府によって盗聴され解読される恐れのある暗号装置を使うような，間抜けな犯罪者はいないという意見である．また，国家安全保障を考えた場合，米国以外の国が進んでクリッパーチップを採用するとは思えない．とすれば，クリッパーチップは国家の安全保障にはなんら貢献しない．

第4の指摘は，暗号研究者や情報産業界からの意見であるが，クリッパーチップの採用によって，米国における暗号技術の研究のインセンティブが小さくなり，暗号技術の進歩を阻害し，強いては米国の競争力に悪影響を与えるというものである．

条件付きの輸出規制緩和■

こうしたクリッパーチップに対する批判が続く中，1995年8月に連邦政府は，暗号技術製品の輸出規制緩和策を発表した．これは，政府が定めたキー・エスクロー基準を満たせば鍵長64ビットまでの暗号技術製品の輸出が可能となるというものであった．実際に1996年1月には，ロータス社が暗号鍵の24ビット分をNSAに寄託することで64ビット暗号を組み込んだグループウェア製品（ロータス・ノーツ）の輸出許可を得ている．

さらに1996年3月，連邦政府は新しい暗号技術政策を提案した．この提案は，公開鍵インフラストラクチャ（PKI）確立の必要性を指摘するとともに，新しく「キー・リカバリー（Key Recovery）」という概念を打ち出した．この新しい政策案に沿って連邦政府は1996年10月，暗号技術を用いた製品の輸出規制を今後2年間かけて緩和するというガイドラインを発表し，翌11月には，ガイドラインに沿った大統領令が公布された．この輸出規制緩和策において連邦政府は「キー・エスクロー・システム」に代えて「キー・リカバリー・システム（KRS: Key Recovery System）」を提案している．KRSは復号に必要な鍵を紛失に備えて第三者に預けておく仕組みである．もちろん，当事者が復号のための鍵を紛失したときに，鍵を回復するために利用するシステムであるが，裁判所の許可を得た上で司法当局が合法的に復号のための鍵を入手できるようにするためでもある．また，連邦政府は，輸出管理法を改正し，暗号装置を武器の分類から汎用品の分類に移した．これによって暗号技術製品のうち民生用の製品については，商務省が輸出許可の権限を持つことになった．

さらに，鍵の長さが40ビット以内の製品は従来から包括許可の対象であるが，鍵の長さが41ビットから56ビットの製品も，ある条件をみたせば包括許可の対象になった．この条件が，KRSの整備である．KRSが整備されていない場合でも，KRSの開発計画を示し，2年後からはKRSの仕組みのない暗号製品は輸出しないことを約束し，さらに6カ月ごとにKRSの開発状況を報告するなら，包括許可の対象になり得る．また鍵の長さが56ビットを超える製品についても，KRSが整備されているものは個別許可の対象になることになった．

この1996年の一連の動きについて，連邦政府が公開鍵インフラストラクチャの重要性を指摘した点は評価されているが，新しく打ち出した「キー・リカバリー」という概念は従来の「キー・エスクロー」と本質は変わっていないとの批判を受けることになった．

輸出規制緩和法案の行方■

クリッパーチップ計画の発表，それに対する民間の反対運動，連邦政府の暗号技術製品の輸出規制緩和策

の発表といった動きに対応するように，議会でも暗号技術に関連する問題が取り上げられた．1996年3月に，“Encrypted Communications Privacy Act of 1996”が上院に，“Security and Freedom through Encryption Act of 1996”が下院に提出された．この2つの法案は類似点が多く，その主な内容は以下の通りであった．

- 米国民は自分自身の情報を守るために，暗号方式，鍵の長さ，暗号システムを自由に選ぶ権利を持っていることを確認すること
- 連邦政府が無制限に個人や企業の情報にアクセスすることを可能にする「鍵の第三者寄託」の強制を禁止すること
- 「鍵の第三者寄託」を選択した個人や企業の情報の安全を保証すること
- 犯罪の実行や犯罪の隠匿のために暗号技術を利用することを法的に禁止すること
- 海外の企業から入手可能な暗号技術製品と同程度（あるいは同程度以下）の暗号技術製品（ソフトウェアであるかハードウェアであるかを問わない）の輸出を認めること

この両法案は，第104回議会（1995～1996年）中に採決されることなく廃案になったが，第105回議会に再提出された．またこの他，新しく2つの暗号関連法案が議会に提出された．

まず，1997年2月にはBob Goodlatte下院議員（共，バージニア州）がSAFE法案（“Security and Freedom through Encryption Act of 1997”）（H.R.695）を下院に提出した．この法案は，1997年9月末までに5つの委員会（司法，国際関係，商業，安全保障，諜報）を通過したが，各委員会はそれぞれ異なる修正を施した法案を可決したため，下院裁定委員会で一本化の作業が行われることになった．しかし，結局この一本化の作業が完了する前に議会の会期末を迎え，法案は再度廃案となった．

Patrick Leahy上院議員（民，バーモント州）が1997年2月に再提出したECPA法案（“Encrypted Communications Privacy Act of 1997”）（S.376）およびConrad R. Burns上院議員（共，モンタナ州）が1997年2月に提出したPro-CODE法案（“Promotion of Commerce On-line in the Digital Era”）（S.377）はいずれも1997年秋の時点で廃案状態になっていた．

John McCain上院議員（共，アリゾナ州）とBob Kerrey上院議員（民，ネブラスカ州）が1997年6月に提出したSPNA法案（“Secure Public Networks Act of 1997”）（S.909）は，政府関係機関に対してKRSの導入を義務化する条項が入っている（民間での利用は任意としている）ことで注目を浴びた．この法案は，上院の商業委員会を通過したが，そのまま会期末を迎え他の法案と同様に廃案となった．

産業界，団体，研究者，欧米■に広がる波紋■

本当は大幅な規制緩和を望む産業界

1996年に発表された暗号技術製品の輸出規制緩和方針に呼応するように，IBMを含むコンピュータ関連企業11社は1996年10月，Key Recovery Alliance（KRA）を結成した．KRAの目標は，世界中で共通的に利用できるキー・リカバリー技術の開発と利用を促進すること，キー・リカバリー機能を持ったシステムとそうでないシステムとの相互運用を可能とするための要件を明らかにすること，暗号化された情報の復元を可能とする世界的なインフラストラクチャの構築を支援することなどである．1998年7月に公開された“1997 Year in Review Report”によれば，日本企業を含む71社がKRAに加盟している[13]．

一方，マイクロソフトやロータス，アドビなどのパソコン用ソフトウェアメーカが参加しているBSA（Business Software Alliance）は1996年12月，声明を発表して連邦政府の発表した方針に反対を表明した．主な反対理由は，強制的なキー・リカバリーは事実上キー・エスクローと同じであること，ユーザが望んでいるのは単純な仕組みのキー・リカバリー技術であることなどである．一方で，BSAは暗号規制の大幅緩和を目指すSAFE法案やPro-CODE法案を支持することも明らかにしている．また，AT&Tやベル・アトランティックなどの通信事業者，ノキアやサン・マイクロシステムズなどの情報通信機器メーカがメンバであるCCIA（Computer and Communications Industry Association）も暗号規制の大幅緩和を目指すSAFE法案やPro-CODE法案を支持し，恣意的なKRSは無益であるとの立場を明らかにした．この他，主な情報技術関連企業が参加しているITAA（Information Technology Association of America）も，米国が輸出規制を行っている（強力な）暗号製品は海外で容易に入手可能なので，現在の輸出規制はあまり意味がないとの意見を明らかにしている[14]．

一方，デジタルメディア時代における個人の自由と民主的な価値を保護／推進するための公共政策の立案と実施を目的にした非営利団体であるCDT（Center for Democracy and Technology）や，サイバースペースにおける市民の権利を保護するために活動している非営利団体であるEFF（Electronic Frontier Foundation）などの非営利団体も連邦政府の暗号政策に強い反対を表明している[15]．

暗号研究者もKRSを批判

MITのHal Abelson教授他11名の暗号研究者は1997年5月，KRSを批判するレポートを発表した（このレポートは1998年に増補版が公表さ

れている[16]). このレポートが指摘している連邦政府のKRSの問題点は以下のとおりである.

• 安全性に疑問がある

実現されたキー・リカバリーの仕組みに欠陥があれば, その適正な運用は危機的になり, システムの信頼性も, 暗号の安全性も破綻をきたす. 具体的には, 鍵が適切な形で公開されない, 秘密になっているはずの鍵が盗まれる, 司法機関からの要求に対応できないなどの事態が考えられる.

• きわめて複雑で実現困難なシステムである

連邦政府が想定しているキー・リカバリー・システムを構築することは不可能ではないが, 非常に多くの機関や利用者を結ぶシステムになり, 相互の通信も, 鍵の数も, 運用上の必要条件も非常に多くなる. キー・リカバリー機能は, 本来の暗号機能よりはるかに複雑で実現の困難なものである.

• 多大なコストがかかる

連邦政府が想定しているキー・リカバリー・システムのコストについては, 試算はおろか, 検討すらされていない. しかし, こうしたきわめて複雑なシステムを設計, 実現, 導入, 運用するコストは, 最終的には許容できないほど高いものになる可能性がある.

欧州理事会も批判

欧州理事会 (European Commission) は1997年10月, "Ensuring Security and Trust in Electronic Communication" と題するレポートを発表した. このレポートは,「司法当局が暗号化された情報の平文にアクセスする必要がある」点には理解を示しているものの,「インターネット上にある強力な暗号ソフトへのアクセスを効果的に阻むことは不可能である」と指摘し,「暗号の利用を制限すれば, 法律を遵守している企業・市民から自衛手段を奪うことになりかねず, しかもそうした制限を行ったからといって, 犯罪者の (強力な) 暗号利用を完全に阻止できるわけでもない」と述べている. そしてさらに, KRSのような「暗号鍵にアクセスできるようにする仕組みは, (クラッカーに対して) 暗号解読の新しい方法を提供することになる」のでセキュリティを弱めることになりかねないと指摘している.

その後の動き■

1998年の輸出規制緩和

商務省は1998年7月, 別に定められた45カ国の銀行等の金融機関が電子取引のために利用する場合は, 鍵長や暗号方式, キー・リカバリー機能の有無にかかわらず, 技術審査を1回受けていれば, 以降はライセンスなしで輸出を認めるというガイドラインを発表した.

さらに1998年9月16日, 連邦政府は輸出規制緩和を拡大する方針を明らかにした[17]. その内容は以下の通りである.

(1) 56ビットのDESおよび同等の暗号製品は, イラン, イラク, リビアなどの7カ国を除き, 技術審査を1回受けていれば, 以降はライセンスなしで輸出可能

(2) 鍵長や暗号方式, キー・リカバリー機能の有無にかかわらず, 以下のセクターについては輸出可能

• 米国企業の子会社：イラン, イラク, リビアなどの7カ国を除く

• 保険会社：銀行などの金融機関に対して認められている45カ国

• 保健および医療機関 (医薬品会社は含まない)：同上の45カ国

• オンライン通販企業：同上の45カ国

この規制緩和の詳細を定める実施規則は, 間もなく輸出管理局から発表されることになっている.

33カ国が新しい暗号規制で合意

米国と同様, 多くの先進国も暗号技術の輸出を規制している. その輸出規制の基本になっているのがワッセナー・アレンジメントであり, 日本の暗号輸出規制の内容もこれを基本としている. ワッセナー・アレンジメントは, 1996年7月に発足した輸出管理に関する国際的な枠組みで, 通常兵器とその関連製品の輸出管理を目的としており, 現在33カ国が参加している.

そのワッセナー・アレンジメントの総会が, 1998年12月2, 3日にウィーンにおいて開催され, 暗号技術製品については, 大幅な規制緩和を行う一方, 2年間の期限付きではあるものの, 64ビット超の大衆市場製品を新たに規制の対象とするという新しい合意が行われた. この合意によれば, まず56ビット以下の共通鍵暗号, 512ビット以下のRSA暗号, 112ビット以下の楕円暗号は規制の対象外となる一方, 従来は規制の対象外とされてきた「店頭等で入手可能な64ビット超の暗号ソフトウェア」が規制の対象とされることになった.

この新しい合意にいたる経緯や合意の詳細, それを踏まえた日本の新しい暗号輸出規制については, 通商産業省貿易局の近藤賢二安全保障貿易管理課長の寄稿を参照されたい.

米国の暗号政策の展望■

米国における暗号技術製品に対する輸出規制は, 徐々に緩和されつつあるものの, 米国産業界が期待しているようなスピードでは進んでいないし, 規制の現状は産業界や市民団体が望む水準にははるかに遠い.

米国連邦政府の最大の懸念は, いうまでもなく, 強力な暗号技術の利用によって国内外における自国の諜報活動が阻害され, 国家安全保障に影響がでることである. しかし, 国家安全保障のために強力な暗号技術の利用を制限する必要があるなら, 世界的なコンセンサスを得て, 高度な暗号技術を持つ (あるいは持つ可能性がある) 国々が協調して暗号技

術の輸出のみならず利用も規制しなければ意味をなさない．しかし，国際的な規制は，現実に可能なのだろうか．米国が危険視する国々において高度な暗号製品がつくられる可能性はあるし，多くの暗号アルゴリズムは公知のものとなっている．既知のアルゴリズムを利用したソフトウェアの開発には，天才的なプログラマーは必要としない．すでに米国外に流出してしまった十分に強力な暗号ソフトを入手するという手段もある．つまり欧州理事会が指摘するように，こうした規制を続けても「犯罪者の（強力な）暗号利用を完全に阻止できるわけでもない」．とすれば，連邦政府の輸出規制は，現実にはあまり意味がなく，単に米国の情報技術関連輸出の足を引っ張っているにすぎないという米国情報産業界の主張の方が正論に聞こえる．こうしたことを考えると，連邦政府はこの輸出規制をさらに緩和することになるのではないだろうか．

参考文献

1）前川　徹: サイバースペースと米国情報産業, 株式会社スパイク, pp.152-154（1997）.
2）Code of Federal Regulations: Title 22, Chapter I, Subchapter M, Parts 121.
3）Government Encryption Standard DES Takes A Fall, RSA Data Security, http://www.rsa.com/des/
4）EFF Builds DES Cracker that Proves that Data Encryption Standard is Insecure, Electronic Frontier Foundation, http://www.eff.org/descracker.html
5）RSA '99 Rress Release－RSA Code-Breaking Contest Again Won by Distributed.Net and Electronic Frontier Foundation, http://www.rsa.com/pressbox/html/990119-1.html
6）Press Release on "Clipper Chip" Encryption Initiative（Apr. 16, 1993）, The White House Office of the Press Secretary, http://www.pub.whitehouse.gov/uri-res/I2R?urn:pdi://oma.eop.gov.us/1993/4/19/6.text.1
7）NIST Announces Voluntary Escrowed Encryption Standard to Promote Secure Telecommunications, NIST, http://www.nist.gov/public_affairs/releases/n94-08.htm
8）MISSI Brochure, pp.4-5（June 1996）, http://www.nsa.gov:8080/programs/missi/pg4-5.html,（製品一覧）NSA Catalog-PCMCIA Crypto Cards, http://www.nsa.gov:8080/programs/missi/cat_pcc.html
9）DefenseLINK News: Encryption Formulas Declassified, Office of Assistant Secretary of Defence（June 23, 1998）, http://www.defenselink.mil/news/Jun1998/b06231998_bt316-98.html
10）Brickell, E. F., Denning, D. E., Kent, S. T. and Maher, D. P.: SKIPJACK Review Interim Report（July 28, 1993）, http://www.eff.org/pub/Privacy/Key_escrow/Clipper/skipjack_interim.report
11）"Privacy－Crypto－Key Escrow 1993-4（US）: Clipper/EES/Capstone/Tessera/Skipjack" Archive, Electronic Frontier Foundation, http://www.eff.org/pub/Privacy/Clipper/
12）Baran, N.: Inside the Information Superhighway Revolution（1995）,（邦題:「情報スーパーハイウェイの衝撃」, 勝又美智雄訳, 日本経済新聞社）.
13）1997 Year in Review Report, Key Recovery Alliance（July 1998）, http://www.kra.org/whitepapers/KRA_1997_rpt_w7.pdf
14）BSA－http://www.bsa.org/, CCIA－http://www.ccianet.org/, ITAA－http://www.itaa.org/
15）CDT－http://www.cdt.org/, EFF－http://www.eff.org/
16）Abelson, H., Anderson, R., Bellovin, S. M., Benaloh, J., Blaze, M., Diffie, W., Gilmore, J., Neumann, P. G., Rivest, R. L., Schiller, J. I. and Schneier, B.: The Risk of Key Recovery, Key Escrow, and Trusted Third-Party Encryption（June 1998）, http://www.cdt.org/crypto/risks98/
17）Administration Updates Encryption Policy, Office of the Press Secretary, White House（Sep. 16, 1998）, http://www.pub.whitehouse.gov/uri-res/I2R?urn:pdi://oma.eop.gov.us/1998/9/17/3.text.1

（平成11年5月10日受付）

1977年　7月	DESが連邦政府の暗号標準となる
1993年　4月	連邦政府が「クリッパーチップ計画」を発表
1993年　7月	連邦政府がSKIPJACKが安全であるという報告書を公表
1994年　2月	クリッパーチップ計画に基づく新暗号EESがNISTから発表
1995年　8月	連邦政府が最初の暗号輸出規制緩和策を発表
1996年　3月	連邦政府が新暗号政策案を発表,「キー・リカバリー」を提案
1996年　3月	議会に輸出規制緩和法案（SAFE法案（下院）とECPA法案（上院））が提出
1996年　7月	ワッセナー・アレンジメント発足
1996年10月	連邦政府が輸出規制緩和のガイドラインを発表
1996年10月	IBMを含む11社がKey Recovery Alliance（KRA）を結成
1996年12月	BSA（Business Software Alliance）が政府の方針に反対を表明
1997年　2月	SAFE法案とECPA 法案が議会に再提出
1997年　5月	暗号研究者11名がKRSを批判するレポートを発表
1997年　6月	DESが初めて解読される（約7万台のコンピュータで96日間）
1997年10月	欧州理事会が米国の暗号政策を批判するレポートを発表
1998年　6月	SKIPJACKのアルゴリズムをNSAが公開
1998年　7月	暗号解読用コンピュータによってDESが解読される（3日以内）
1998年　7月	連邦政府が金融機関向けの輸出規制緩和ガイドラインを発表
1998年　9月	連邦政府が輸出規制緩和策の拡大を発表
1998年12月	ワッセナー・アレンジメント総会において暗号輸出規制緩和を決定
1999年　1月	DESがわずか22時間15分で解読される

米国の暗号政策論争に関する年表