IMES DISCUSSION PAPER SERIES

キーリカバリー構想を巡る最近の情勢について

岩下直行・宇根正志

Discussion Paper No. 97-J-8

IMES

INSTITUTE FOR MONETARY AND ECONOMIC STUDIES
BANK OF JAPAN

日本銀行金融研究所

〒100-91 東京中央郵便局私書箱 203 号

IMES Discussion Paper Series 97-J-8
1997 年 5 月

キーリカバリー構想を巡る最近の情勢について

岩下直行[*]・宇根正志[**]

要　旨

インターネットのようなオープンなネットワークを利用した情報通信や電子商取引においては、部外者から機密情報を保護したり、通信内容や通信相手の真正性を確認するために、暗号技術が積極的に利用されている。暗号技術の普及は、電子商取引を推進する立場や、利用者のプライバシー保護の観点からは望ましい反面、それが悪用されると、犯罪捜査等の法律執行における障害になるという問題が存在する。

こうした問題への対応策として提案されているのが、キーリカバリー構想である。この構想は、利用者が暗号化を行うための秘密の「鍵」を信頼できる機関に寄託しておき、法律執行上の必要が生じた場合は、一定の手続きに基づいて捜査当局がこの「鍵」を利用して暗号化された情報を解読できるようにする仕組みである。これが普及すれば、利用者のプライバシーを尊重しつつ、万一の場合は法律執行上の要請に応えることもできると主張されている。欧米主要国の当局者の間では、キーリカバリー構想を実現するための制度、システムを整備しようという動きが急速に具体化しつつある。

しかしながら、キーリカバリー構想については、社会的、技術的、経済的に、更に検討すべき様々な問題が存在することが指摘されている。インターネットの普及や電子商取引の実現のために暗号技術の重要性が増してきているため、こうした構想を含め、暗号技術を巡る諸外国の動向にも注意を払っていくことが必要となっていると考えられる。

キーワード：暗号、鍵管理、鍵寄託、鍵復元、キーリカバリー、キーエスクロー

JEL classification: L86

*　日本銀行金融研究所研究第２課副調査役（E-mail: iwashita@imes.boj.go.jp）
** 日本銀行金融研究所研究第２課（E-mail: une@imes.boj.go.jp）

本論文を作成するに当たっては、横浜国立大学の松本勉助教授、NTT 情報通信研究所の岡本龍明特別研究員および太田和夫主幹研究員から有益なコメントを頂戴した。

目　次

１．はじめに

(1)インターネットの普及と暗号技術利用の拡大

マイクロ・エレクトロニクス技術の発達、パーソナル・コンピューターの普及に伴い、様々な産業分野や人々の生活の中で、コンピューター・ネットワークを利用した情報通信を利用する機会が増えている。とりわけ、世界中を結んだオープンなネットワークであるインターネットの爆発的な拡大[1]に伴い、わが国でも、コンピューター・ネットワークを介する国際的な情報のやり取りが、ごく普通に行われるようになった。

インターネットのようなオープンなネットワークを利用した情報通信や電子商取引においては、従来とは異なり、部外者から機密情報を保護したり、通信内容や通信相手の真正性を確認すること――情報のセキュリティを確保すること――に対する強い要請が生じる。なぜなら、デジタル化された情報は、それを傍受したり改竄して悪用することが容易だからである。例えば、電話会社の回線と交換機しか経由しない電話やファックスと比べて、複数のプロバイダーや中継コンピューターを経由して情報が受け渡されるインターネット通信の場合は、その経路上で部外者に通信内容を傍受される可能性が高く、かつ得られた通信内容から特定の情報を選別すること（例えば、クレジットカード番号のみを抽出すること）も容易である。また、紙に書かれた手紙を改竄することに比べ、電子メールの内容を改竄することは簡単である。こうした問題に対応するため、インターネット上での情報通信や電子商取引においては、暗号技術が積極的に利用されている。多くの参加者が自由に利用できるインターネットのようなネットワークにおいて、情報セキュリティを確保する唯一の手段が、暗号技術を利用することだからである。

暗号技術を利用するためには大量の計算処理が必要であるため、コンピューターが高価であった時代には、暗号は特に高度なセキュリティが必要とされる業務分野（例えば巨額な資金移動に関する情報を電子的に送信する銀行業務[2]など）のみにおいて利用されてきた。しかし、マイクロ・エレクトロニクス技術の発達の結果、一般の利用者でも、高度な計算能力を持つパソコンを

[1] Network Wizard 社による 97 年 1 月時点でのインターネット接続台数調査によれば、日本は米国に次ぐ世界第２位のインターネット利用国となっている（世界に占めるウエイトは 4.5%）。

インターネットに接続されているホストコンピューター数の推移（単位 千台）

	Oct-92	Oct-93	Oct-94	Jan-95	Jul-95	Jan-96	Jul-96	Jan-97	年間伸率
全世界	1,136	2,056	3,898	4,852	6,642	9,472	12,880	16,146	70.5%
うち米国	622	943	2,044	3,178	3,653	6,053	8,224	10,111	67.0%
<ｳｴｲﾄ>	<54.8%>	<45.9%>	<52.4%>	<65.5%>	<55.0%>	<63.9%>	<63.9%>	<62.6%>	
うち日本	12	23	72	97	160	269	496	734	172.7%
<ｳｴｲﾄ>	< 1.1%>	< 1.1%>	< 1.8%>	< 2.0%>	< 2.4%>	< 2.8%>	< 3.9%>	< 4.5%>	
英国	－	－	－	241	291	452	579	592	31.0%
ドイツ	－	－	－	208	351	453	548	722	59.3%
カナダ	－	－	－	187	263	373	424	603	61.8%
フランス	－	－	－	93	114	137	190	246	78.9%
イタリア	－	－	－	31	46	73	114	150	103.9%
G7以外	－	－	－	817	1,764	1,661	2,303	2,988	79.9%

安価に利用することが可能となったため、最近では、インターネットでデータを送信したり、自分のパソコンに資料を保管する場合などに、暗号を利用して情報を秘匿することが珍しくなくなっている。例えば、インターネット上で WWW のホームページを閲覧するソフトである Netscape Navigator には、データの送信時に暗号化処理を行い、機密情報の漏洩を防ぐ機能が標準装備されている。また、インターネット上で機密性の高い情報を電子メール送信するためには、RIPEM（Riordan's Internet Privacy Enhanced Mail）、PGP（Pretty Good Privacy）等の暗号化電子メール用のフリーソフト（無償で配布されるソフトウェア）を利用したり、S/MIME（Secure / Multipurpose Internet Mail Extension）と呼ばれる暗号化フォーマットを組み込んだ市販ソフトを利用すればよい。このように、暗号技術に関する特別な知識を持たない一般のパソコン利用者であっても、暗号ソフトウェアを容易に利用することが可能となっている。

(2)キーリカバリー構想の提案と問題点

上記のような暗号技術の普及は、電子商取引を推進する立場や、利用者のプライバシー保護の観点からは望ましいものと評価できる反面、それが悪用されると、犯罪捜査等の法律執行（Law Enforcement）における障害になるという問題が存在する。例えば、テロリストがこうした暗号技術を利用して秘密裏に仲間と通信を取り合うとか、犯罪者が記録を暗号化して保存したため、それを捜査当局が押収しても、捜査資料や証拠として利用できなくなるといった懸念が指摘されている。

こうした暗号技術の悪用への対応策として、米国政府から提案されたのが、キーエスクロー（Key Escrow）あるいはキーリカバリー（Key Recovery）と呼ばれるスキームである[3]。これらは、簡単に言えば、利用者が暗号化を行うための秘密の「鍵」を信頼できる機関に寄託しておき、法律執行上の必要が生じた場合は、一定の手続きに基づいて捜査当局がこの「鍵」に合法的にアクセス（Lawful Access）して暗号化された情報を解読できるようにする仕組みのことである。この技術が普及すれば、利用者のプライバシーを尊重しつつ、万一の場合は法律執行上の要請に応えることもできると主張されている。こうした観点から、OECD/DSTI/ICCP/暗号専門家会合において審議された暗号政策ガイドライン[4]においても、「国家の暗号政策は、暗号化されたデータの平文又は暗号鍵への合法的アクセスを容認することができる（National cryptography policies may allow **lawful access** to plaintext, or cryptographic keys, of encrypted data.）」という規定が盛り込まれた。

しかしながら、キーリカバリー構想については、社会的、技術的、経済的に、更に検討すべき様々な問題が存在する。具体的には、次のような論点が指摘されている。

---

[2] 特に、米国では、財務省指令（Treasury Directive）により、電子資金移動（EFT）の取引データを DES を利用して暗号化することが規定されていることもあり、多くの金融機関が暗号技術を利用してきた。

[3] 米国政府は当初このスキームを「キーエスクロー」と呼んでいたが、1996 年 10 月のゴア副大統領の公式声明以降は「キーリカバリー」という表現に変更している。本論文では、歴史的な事実としての記述を除き、現在では一般的となった「キーリカバリー」という表現を利用している。この用語については、注 18 も参照。

[4] OECD 暗号政策ガイドライン: OECD の科学技術産業局(DSTI: Directorate for Science, Technology and Industry）の「情報、コンピューター及び通信政策委員会」（ICCP: Committee for Information, Computer and Communications Policy）の中に設けられたアドホックな暗号専門家会合において 1996 年の 5 月から 12 月にかけて起草され、1997 年 3 月 27 日に正式発表された各国の暗号政策に関するガイドライン。同ガイドラインは OECD のホームページ（http://www.oecd.org/dsti/iccp/crypto_e.html）に掲載されている。

① 犯罪捜査等を目的としているとはいえ、利用者が暗号化して秘匿しようとしている機密情報を、捜査当局が解析可能となってしまうことに対して反感を持つ人々が存在する。特に、米国では、インターネット上におけるプライバシーの保護を訴える市民団体等が、キーリカバリー構想に対して強く反発しているほか、これを擁護する政治家などを巻き込んで、活発な論争が展開されている。

② 技術的にみれば、キーリカバリーの具体的なスキームによっては、それを無効化する方法が存在する。すなわち、ある種のキーリカバリー技術に対して、その機能を組み込んだ暗号ソフトウェア等を特別な方法で利用することによって、「鍵」への合法的アクセスを行っても暗号を解読できなくすることが可能である。このため、法律執行におけるキーリカバリーの有効性については、実装面を含めた十分な検討が必要である。

③ 仮に理想的なキーリカバリー技術が開発され、かつ、それを採用することが望ましいという社会的コンセンサスが得られた場合でも、その技術をどのように普及させていくかという問題がある。犯罪捜査に利用することを想定するのであれば、全ての暗号通信システムにキーリカバリーが組み込まれていることが必要となる。なぜなら、仮にキーリカバリーをサポートするシステムとサポートしないシステムの両方が提供され、利用者が自由に選択できるならば、罪を犯そうとする者は、解読を恐れて、キーリカバリーをサポートしないシステムを使用すると考えられるからである。例えば、米国政府は、通信業者に補助金を与えたり、キーリカバリー機能を備えた暗号製品のみに海外への輸出を許可するといった優遇策によって、キーリカバリーが組み込まれた暗号製品を普及させる政策を進めようとしている。また、インターネット上で公開鍵暗号を活用するためのシステム基盤（KMI: Key Management Infrastructure）の構築と合わせて、キーリカバリーの導入を進めようとする動きも見られている。

わが国では、これまで国家が暗号技術を管理する度合いが低く、暗号を巡るオープンな議論もあまり行われてこなかった。しかし、インターネットの普及や電子商取引の実現のために暗号技術の重要性が増してきているため、こうした構想を含め、暗号技術を巡る諸外国の動向にも注意を払っていくことが必要となっていると考えられる。

(3)本論文の構成

本論文では、キーリカバリー構想を巡る米国等主要国の政策動向を整理するとともに、キーリカバリー技術の構造を概観する。本論文の構成は次の通りである。２．では、米国の暗号政策を整理する文脈の中で、キーリカバリーの歴史を概観する。３．では、欧州における最近の政策動向について、公表された情報を整理する。４．では、キーリカバリーの基本構造と実装技術について、これまでの公表資料を基に具体的な仕組みを解説し、その技術的な課題について説明する。

２．米国におけるキーリカバリー構想の推移

(1)米国の暗号政策の枠組み――技術標準と輸出規制

暗号技術は、伝統的には軍事・外交分野で機密情報の保護のために利用される技術であった。過去の戦争において、敵国の暗号技術解析の成否が戦局に大きな影響を与えた[5]といった事例を引き合いに出すまでもなく、現在でも多くの国において、暗号技術は「軍事転用可能な技術」として国家によって管理されている。とりわけ、現代暗号技術の最大の生産国/需要国である米国においては、国家の重要な政策として暗号技術の取り扱いが検討され、それに基づいて政府が厳格に暗号を管理している。キーリカバリー構想を巡る動きも、こうした文脈で理解することが必要である。

米国政府の暗号管理の具体的な手段は、①暗号技術の標準の策定と、②暗号技術の輸出規制の２つである。このうち、①の技術標準によるコントロールについては、具体的には、NIST[6]によるFIPS（米国連邦技術標準：Federal Information Processing Standards）の認定を通じて行われている。FIPS は、「機密ではないが取扱いに注意を要する情報」に関して、米国政府機関内での取扱標準を定めるものであり、直接的には政府機関が調達する暗号装置のみを対象としている。しかし、FIPS に認定された技術は民間にも開放されており、ある技術が FIPS として認定されると、いわば「政府のお墨付きを得た技術」と認識され、また、政府による調達の増加が価格の低下を招来するといった事情もあって、FIPS は民間においても事実上の標準として利用されることが多かった。例えば、DES（Data Encryption Standard）は、米国政府の公募に応えて 1970 年代前半に米国 IBM 社が開発し、1977 年に FIPS に採択された共通鍵暗号アルゴリズムであるが、その後、事実上の国際標準暗号として広く普及し、現在、世界中で最も多く利用される暗号となっている。

一方、②の暗号技術の輸出規制は、安全保障の観点から米国の暗号技術の海外への流出を政府が規制するものである。輸出規制には、国務省による規制と商務省による規制の２種類がある。すなわち、(a)軍事目的の技術・装置については国務省主導の輸出規制が行われており、Arms Export Control Act に基づいて定められた International Traffic in Arms Regulations が、輸出に際して認可を必要とする装置のリストである U.S. Munitions List を規定している。また、(b)軍事目的に転用可能な技術・装置については商務省主導の輸出規制が行われており、Export Administration Act に基づいて定められた Export Administration Regulations が、認可を必要とする装置を定めたリストである Commerce Control List を規定している。従来、暗号を利用した装置は (a)に該当するとされ、米国外に輸出するためには国務省による個別審査が必要であった。実際に個別審査で認可された例をみると、海外の政府機関や大手金融機関向けといった限られた先に対する輸出が殆どであった。

---

5 例えば、第二次世界大戦において、ドイツ軍が使用していたエニグマと呼ばれる暗号機の解析による暗号解読の成功は、連合軍の勝利に重要な役割を果たしたと言われている。

6 NIST（National Institute of Standards and Technology）：米国商務省の下部組織で、科学技術全般に関する標準を策定する役割を担っているほか、情報通信の分野では、1987 年に成立した Computer Security Act により、FIPS を制定する権限を有している。ただし、米国政府の情報セキュリティ政策を国防長官の管轄と定めた 1980 年の大統領令（Executive Order 12333）等により、実際の暗号政策の企画立案や標準策定は、国防総省の下部機関である NSA（National Security Agency）が強い影響力を持つと言われている。

(2)インターネットの普及による環境変化

こうした米国政府の暗号政策は、暗号技術が軍事・外交分野のほか、せいぜい金融分野までの限られた利用者にしか利用されないことを前提としたものであった。しかし、インターネットの普及により、一般の人々がコンピューターとネットワークを自由に利用できるようになり、また、ネットワーク上でのプライバシーやセキュリティ対策に関する関心が高まるとともに、（キーリカバリー構想の問題とは独立に）主に米国内から、米国政府の暗号政策に対する批判の声が高まってきた。主な批判者は、①暗号技術を自由に利用し、ネットワーク上でのプライバシーを保護することを主張するインターネット技術者と、②インターネット用情報機器メーカーやソフトウェア・ベンダーであった。その各々の主張とその背景は、次のとおりである。

①インターネット技術者による米国の暗号政策批判

インターネット技術者は、暗号技術を一般に普及させる運動の強力な推進者の役割を果たしてきた。インターネットの技術的な発展は、IETF[7]に代表されるような、大学や企業のコンピューター技術者によるボランティア・ベースの貢献に支えられてきた。「パーソナル・コンピューターの能力を一般大衆に開放し、コンピューター・ネットワークによって新しいコミュニティを形成すること」を目的とした様々な非営利のプロジェクトに身を投じてきたインターネット技術者からみれば、個人のプライバシーを保護するために使われるべき暗号技術が政府の厳しい統制下に置かれ、仮に米国外に暗号ソフトを頒布すると犯罪行為となってしまう、という事態は耐え難いものであったのだろう。

インターネット技術者達が、ネットワーク上のプライバシー保護等を議論し、政治的な活動に繋げていくために 1990 年に設立したのが、EFF[8]と呼ばれる団体である。この団体が設立された背景には、次のような事件があった。1990 年 1 月 15 日、AT&T の長距離電話交換機がダウンした事故について、米国捜査当局は「電話回線に侵入したハッカーの仕業ではないか」と疑い、大規模な犯罪捜査を行なった。大勢のインターネット技術者達が嫌疑をかけられ、システム機器等を押収された。本事件は、結局 AT&T 側の原因による事故との結論となったが、それでは収まらないインターネット技術者達が、自分達のプライバシーを守るために EFF を設立したという（古瀬・廣瀬[2]）。EFF や、同様の考え方に基づき各地で設立されたインターネット技術者を中心とする団体（CDT[9]、EPIC[10]等）は、その後発表されたキーリカバリー構想に対する最も有力な反対勢力となった。

こうしたインターネット技術者の中に、インターネット上で自分達が利用する暗号化メール用ソフトウェアを無償頒布する者が現れた。Phillip R. Zimmermann は 1991 年に PGP (Pretty Good Privacy)というソフトを発表した。Mark Riordan は 1993 年に RIPEM（Riordan’s Internet Privacy

---

[7] IETF（Internet Engineering Task Force）：インターネットを管理するための委員会（IAB：Internet Architecture Board）の下部組織で、インターネットの標準プロトコルを指定したり、インターネットで使用する規格を推薦する専門技術者の自主的な集まり。

[8] EFF（Electronic Frontier Foundation）：米国西海岸在住のインターネット技術者達が組織した非営利団体。本拠地はサンフランシスコ。コンピューター・ネットワークにおけるプライバシー、人権問題、知的財産権と自由な情報共有の両立等、サイバースペースにおける様々な問題について、幅広く議論を喚起し、政府に対して様々な要求を行うと同時に、それらに関連する様々な情報をインターネット上でリアルタイムに提供している（EFF[14]）。

[9] CDT（Center for Democracy and Technology)：EFF から派生したメンバーがワシントン D.C.を本拠地に設立した非営利団体。EFF と同様、ネットワーク社会におけるプライバシーと人権問題について活動を行っている（CDT[8]）。

[10] EPIC（Electronic Privacy Information Center）：人権問題とプライバシー問題に関する調査・広報活動を主目的とする市民団体。本拠地はワシントン D.C.。Fund for Constitutional Government（「合衆国憲法に則した政治」を求める非営利財団）が支援する事業として 1994 年に設立された。OECD 暗号専門家会合にも委員を派遣している（EPIC[15]）。

Enhanced Mail）というソフトを発表した。彼らは、インターネットにおける常識として、発表したソフトをインターネット上で公開し、誰でも自由にダウンロードできるようにした。インターネットは世界に対して開かれたネットワークであるため、結果として海外にも当該ソフトを頒布する形となってしまった。米国政府は、これを暗号輸出規制の脱法行為と捉え、彼らにソフトの公開を止めるよう圧力をかけ、また 1995 年には、国務省が Zimmermann を Arms Export Control Act 違反で起訴するという事件が起きた。この事件については、多くのインターネット技術者が国務省を非難し、インターネット上で「Zimmermann を救おう」というキャンペーンや募金活動が展開され、結局、国務省側が起訴を取り下げた。こうした経緯から、EFF メンバーを始めとするインターネット技術者の多くは、米国政府の暗号輸出規制を厳しく批判するようになった。

②情報機器メーカーによる米国の暗号政策批判

インターネットが普及するまでは、暗号技術の用途は政府機関や金融機関のネットワークに限られていたから、暗号技術の実装を担当するのは、大手のコンピューター・メーカーであった。このため、仮に暗号技術を組み込んだシステムを海外に輸出する必要が生じた場合も、金額の大きいプロジェクト単位であれば、個別に国務省の認可を取ることはさほど手間ではなかった。そのような時代には、メーカー側からは、暗号輸出規制についての表立った批判は聞かれなかった。

しかし、インターネットの普及に伴い、暗号技術を組み入れた一般利用者向けのパッケージ・ソフトが普及するようになると、事情が変わってくる。例えば、Netscape Navigator のような少額ソフトウェアの輸出についてまで、「軍事転用可能な技術」として１件毎の認可が必要となると、事実上輸出が不可能となってしまう。これ以外にも、ファイヤーウォール[11]装置、暗号化電子メール・ソフト、電子商取引用のソフトウェア等、暗号技術を応用したインターネット用の情報機器、ソフトウェアが多数開発・販売されるに伴い、「暗号輸出規制は、米国企業が世界の市場で競争する際の足枷となっている」との批判が聞かれるようになった。

こうした批判を受け、1994 年 9 月に国務省は、U.S. Munitions List で規定された暗号技術に関して、予め定められた地域に対する輸出については、１件毎の輸出認可の取得を省略することとした。具体的には、鍵長 40 bit までの「比較的弱い」共通鍵暗号[12]を組み込んだ装置やソフトウェアであれば、１件毎の認可なしに輸出が可能となり、また比較的強度の強い暗号であっても、それが電子商取引等の認証目的で組み込まれ、他に転用できないことが証明されれば、輸出が可能となった。こうしたルールに基づき、Netscape Navigator（但し、国内用の 128 bit の RC4 暗号を改造し、40 bit としたもの）や、CyberCash（電子商取引においてクレジットカード番号を暗号化するために 768 bit の RSA 暗号を利用）等のソフトウェアが輸出可能となった。また、1996 年 2 月からは、個人的な利用に限り、米国民が一時的に暗号装置を海外へ持ち出すことを許可することとした。しかし、こうした漸進的な輸出規制緩和策は、輸出規制対象となる技術、装置の見直し等の抜本的な緩和策を望んでいる情報機器メーカーの立場からは不十分との意見が大勢であった。

---

11 ファイヤーウォール：複数のネットワーク間でのアクセス制限を行い、不正なアクセス要求を通さずに各ネットワークを論理的に分離するための装置。例えば、高度なセキュリティの必要な社内 LAN とインターネットを接続する場合、両者をファイヤーウォール機器を介して接続すれば、社内 LAN のセキュリティを失うことなく、インターネットの各種機能を利用することができる。高セキュリティ領域の情報の秘匿や、正当なアクセス要求の認証に、暗号技術が利用されることが多い。

12 共通鍵暗号の強度は、一般にその鍵長に応じて変化する。すなわち、共通鍵暗号を全数探索法（考えられるすべての鍵で復号化処理を行ってみる攻撃法）によって解読する場合、鍵長が長いほど候補となる鍵の種類が多いので解読が困難になる。1997 年 1 月にカリフォルニア大学の大学院生が、40 bit 鍵長の RC5 共通鍵暗号を 250 台のワークステーションを利用して約 4 時間で解読したとの報告もあり、40 bit 程度の鍵長の共通鍵暗号は比較的弱いとの認識が一般的である。

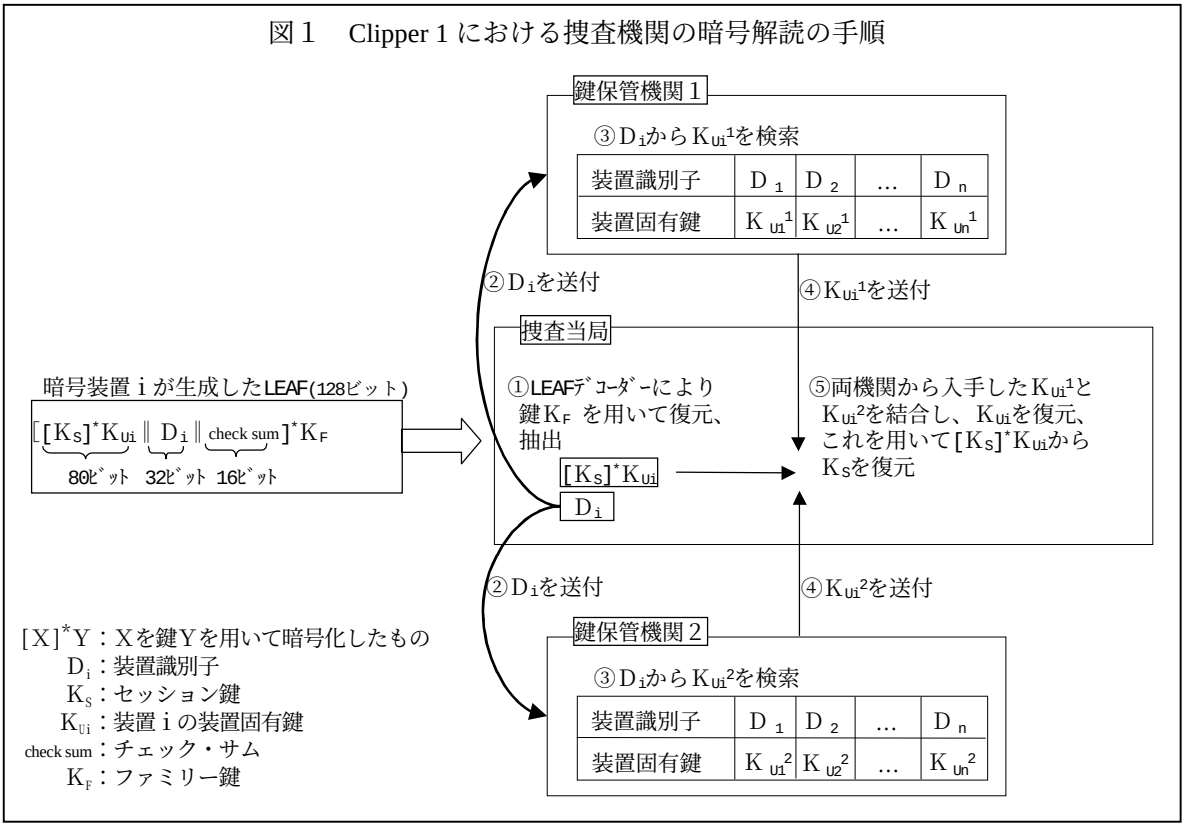
(3)キーエスクロー構想の始まり

①Clipper 1 の発表

米国政府は、1993 年 4 月、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（以下、Clipper 1 という。）を発表した。この構想は、政府が強度の高い暗号を民間に対して提供する一方、暗号鍵の第三者機関への寄託（escrow）を義務付けるもので、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通信内容を解読することが可能となる。これが、キーエスクロー構想の始まりである。

本構想の下では、利用者は、Clipper Chip[13]と Skipjack[14]を用いた通信の高度な暗号化が可能となる。具体的には、利用者は、暗号通信を行う都度、80 bit のセッション鍵をランダムに生成し、公開鍵暗号技術等を用いてそのセッション鍵を通信相手先と共有し、通信内容をこのセッション鍵で暗号化して相手に送信する。なお、その際、当該セッション鍵を「装置固有鍵」で暗号化し、これと装置識別子を並べた情報をファミリー鍵で暗号化した LEAF（法律執行アクセス・フィールド：Law Enforcement Access Field）と呼ばれる情報が、自動的に送信される。

図１　Clipper 1 における捜査機関の暗号解読の手順



---

13 Clipper Chip：Mykotronx 社が独占的に供給する MYK78 と呼ばれる専用チップ。暗号アルゴリズムである Skipjack、装置識別子、ファミリー鍵、装置固有鍵が格納されており、内部の情報を解析・変更できないような「耐タンパー性」を持つとされている。

14 Skipjack：NSA(National Security Agency)によって開発された DES タイプの共通鍵暗号アルゴリズム。80 bit の鍵をパラメータとして非線形変換を 32 回繰り返し、64 bit の平文ブロックを 64 bit の暗号文ブロックに変換する仕組み。なお、そのアルゴリズムや技術の詳細は開示されていない。

ユーザーが利用する Clipper Chip の「装置固有鍵」は、予め２つの鍵寄託機関に分割して寄託されている。この鍵は、通常は秘密に保管されているが、法律執行上の必要性から暗号の解読が必要と判断された場合には、捜査機関は、裁判所の許可を取得した上で、各鍵寄託機関に鍵の開示を求めることができる。捜査機関は各鍵寄託機関から入手した鍵を結合して当該ユーザーの「装置固有鍵」を求め、LEAF からセッション鍵を入手し、それで暗号化されたメッセージを復号化することにより、捜査対象が行う通信内容を解読することが可能となる（図１参照)。

本構想において、Skipjack のアルゴリズムを非公開とし、Clipper Chip という耐タンパー性を持つチップに格納したのは、真正の Skipjack 装置との交信が可能な偽造装置を製造したり、チップを改造して暗号化のプロセスに手を加えることにより、鍵の寄託や LEAF の生成を行わずに Skipjack による暗号通信が行われることを防ぐためであった。また、「装置固有鍵」を２つの鍵寄託機関に分割寄託したのは、鍵寄託機関が事故または故意に保管された鍵に関する情報を漏洩してしまい、それが悪用されるのを防ぐためであった[15]。

米国政府は、本構想の発表時点では「キーエスクローの使用はあくまで voluntary である」としていたが、その後、1994 年 2 月に Clipper 1 のコンセプトを「EES (Escrowed Encryption Standard)」として FIPS に認定した(NIST[25])。この対応は、これまで同様、FIPS を用いて民間で利用される暗号技術をコントロールすることを目指したものと考えられている。

また、1994 年 10 月には、政府が通信会社に対して補助金を与え、キーエスクロー構想を実現するために通信設備を改造する際の費用を政府が負担することを定めた法律が成立、施行されている。米国 AT&T 社では、この補助金を利用して Clipper 1 のコンセプトを実現した電話機（AT&T Surity Telephone Device 3600）を開発している。この電話機では、暗号通信用ボタンを押すことにより、80 bit のセッション鍵をランダムに生成し、その鍵を通信相手先と「Diffie-Hellman 方式による鍵共有」[16]を用いて共有し、Skipjack を利用した秘話通信を行う仕組みとなっているという（Office of Technology Assessment [32])。

②キーエスクロー構想への反発と米国政府の軌道修正

キーエスクロー構想に対しては、その発表直後から、多くの批判的な発言が噴出した。特に、EFF、CDT、EPIC 等のインターネット技術者、プライバシー保護論者が、インターネット上でネガティブ・キャンペーンを繰り広げたため、一時期、若いインターネット利用者の間では、キーエスクロー構想に反対の立場を表明することが一種のファッションとなった感があった。NII 構想[17]を進めるクリントン－ゴア政権にとっては、こうしたインターネット利用者層は有力な支持基盤のひとつであったから、その批判を真摯に受け止めざるを得なかったと言われている。

彼らが主張したのは、①捜査機関が個人のプライバシーを侵害するのではないかという懸念、②採用されている Skipjack アルゴリズムや Clipper 1 の技術面でのフレームワークの非公開に伴う

---

15 鍵寄託機関の役割を誰が担うか、という問題については、米国政府は、当初、政府内の機関に任せることを想定しており、1994 年 2 月に司法長官が示した案では、NIST と財務省が担当するとしていたが、その後、ゴア副大統領は、「２つの鍵寄託機関をともに政府内に置くと、政府の権限濫用を懸念する意見を説得できない」として、一方は民間団体に委ねる考えを表明した。

16 Diffie-Hellman 方式による鍵共有：離散対数問題（$y \equiv a^x \pmod p$を満たす x を求める問題）の困難性に基づく鍵共有方式。暗号通信者は予め a と p を定め、各々秘密の乱数 x_1,x_2 を生成し、$y_i \equiv a^{x_i} \pmod p$を生成する。暗号通信者は互いに相手に y_i を送付し、相手の y_i に自分の秘密の乱数 x_j を乗じて、$y_1^{x_2} \equiv y_2^{x_1} \equiv a^{(x_1 x_2)}$を計算する。これが共通の暗号鍵となる。このようにして、暗号通信者は秘密の暗号鍵をネットワークで配送せずに共有することができる。

17 NII 構想（National Information Infrastructure、情報スーパーハイウェー構想）：アメリカのゴア副大統領が提唱した、全米を光ファイバーで結ぶ次世代通信網構想。1992 年にクリントン・ゴアの選挙公約として発表され、クリントン政権の主要施策として推進されている。2015 年を目標として全国規模の通信情報基盤を構築することにより、国際競争力の強化、雇用機会の増大、教育・医療サービスの向上等の社会経済的効果を実現することが提唱されている。

強度評価の困難さ、③政府機関の役割分担の問題を含む暗号政策の不透明さ、④特定のメーカー（Mykotronx 社）が独占的に提供している専用チップ（Clipper Chip）への依存、等に対する批判であった。

こうした批判を受け、キーエスクロー構想そのものは事実上頓挫し、米国政府は、その実施方法の見直しを余儀なくされた。すなわち、1994 年 7 月に、ゴア副大統領が、下院議員 Maria Cantwell に宛てた書簡において、暗号政策における政府、企業、プライバシー保護論者の３者間の協力体制の強化を図る姿勢を表明し、Clipper 1 の代替案の検討を民間部門と共同で行っていくことを表明した。また、キーエスクロー構想を見直すに当っては、アルゴリズムの公開、ソフトウェアによる実現、民間の鍵寄託機関の設置等を検討対象とすることを約束した。

(4)新しい暗号政策への転換

米国政府は、Clipper 1 発表から約２年間、暗号政策に関する目立った動きを見せていなかったが、1995 年末から、新しい暗号政策に基づく施策を次々に発表し始めた。以下では、その発表内容を時系列で概観し、米国の新しい暗号政策のコンセプトを整理する。

①Clipper 2 の発表――暗号輸出規制見直しへの動き

Clipper 2 は、NIST が 1995 年 12 月に発表した、米国政府による暗号技術の輸出規制の緩和案である（NIST [26,27,28]）。なお、Clipper 2 という名称は、本措置が Clipper 1 の流れを汲むものであることから、EFF を始めとする米国暗号政策ウォッチャーが名付けた通称であり、正式な名称ではない。

その基本的な内容は、「鍵の寄託された暗号ソフトウェア」について、米国から海外への輸出を認めるという内容である。これは、キーエスクローを採用さえすれば、従来の厳格な暗号輸出管理を緩めてもよいという意味で、それまでの暗号政策から一歩踏み出したものと言える。

具体的に言うと、Clipper 2 では、以下の条件に適合する暗号関連ソフトウェアについては、当該装置に対する国務省による review を経たうえで、その輸出認可を商務省の所管とし、原則的に輸出を許可することが表明されている。

①装置の暗号鍵が、正規の手段で入手しようとした際に、入手可能な状態になっていること。

②装置の鍵寄託機能は、以下の方法に沿って寄託されるまでは作動しない状態になっていること。

③装置の暗号鍵が、米国政府あるいは米国の法律執行および安全保障上の要件を満たす政府間協定を米国と締結している国の政府により認可された鍵寄託機関に寄託されていること。

④当該装置の暗号鍵が寄託されている鍵寄託機関の名前および該当する鍵を特定できるだけの情報が、アクセス可能な状態となっており、かつ十分な頻度で記載されていること。

⑤当該装置が、暗号文を作成した場合と受信した場合のどちらの場合でも、暗号文を解読することが出来るような仕様となっていること。

⑥正当に認可された期間中は、いつでも鍵を入手できる仕様になっていること。

⑦装置で使用されるアルゴリズムが公開されており、かつその鍵長が 64 bit 以下であること。

⑧使用される暗号アルゴリズムが、triple-DES の様な組合せ暗号ではないこと。

⑨当該装置は、本規定を満たす装置とのみ互換性をもつこと。また、鍵寄託機能が改造されたり、機能しない状態となっている装置とは通信を行わないような仕様となっていること。

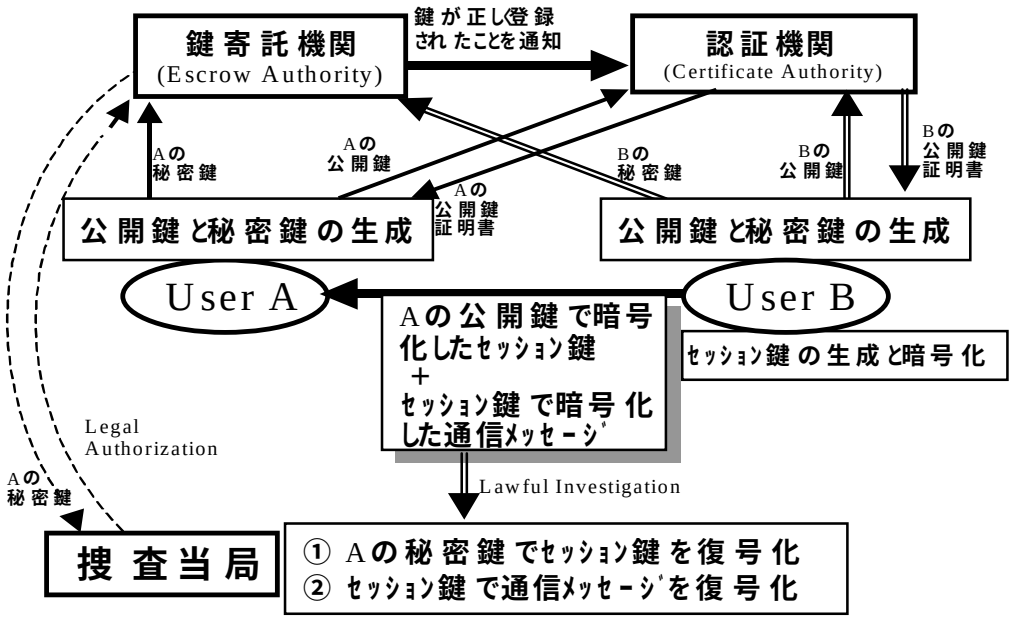
⑩装置が、上記①から⑨に示された仕様を毀損したり迂回したりするような作用に対して耐久性を備えていること。

②Clipper 3 の発表――公開鍵インフラ構築の提案

続いて米国政府は、1996 年 5 月に、公開鍵暗号の情報インフラ(Key Management Infrastructure、以下、KMI) の構築を唱える“Enabling Privacy, Commerce, Security and Public Safety in the Global Information Infrastructure ”と題する論文を発表した（Office of Management and Budget[31]）。この構想も、公開鍵暗号方式における秘密鍵を寄託させ、法律執行における暗号鍵への合法的アクセスを認めるという意味で、Clipper 1 の流れを汲むものであることから、通称 Clipper 3 と呼ばれている。

本構想は、公開鍵暗号を利用することによりネットワーク上での認証および鍵配送機能を実現する一方で、秘密鍵を鍵寄託機関に寄託することにより法律執行の手段を維持する仕組みを構築しようとするものである。KMI への参加自体は voluntary ではあるが、認証機関による公開鍵の証明を受けるためには秘密鍵の鍵寄託機関への寄託を義務付けると定められているほか、外国での法律執行の手段を維持するために、鍵寄託に関する政府間協定を締結することも提案されている。なお、本構想においては、使用される暗号アルゴリズム、鍵長、実装方法等は、今後民間部門と協力して選定する、としていることや、民間企業による秘密鍵の「自己寄託」を認めるとされていることなど、Clipper 1 に対する批判をある程度織込んで改良を加えたものとなっている。

図２　Clipper 3 における暗号通信と捜査機関による復号化の手順



- 認証（デジタル署名）および守秘（鍵交換）の目的に利用可能な公開鍵暗号のための情報インフラ (Key Management Infrastructure)を構築。
- 利用者の秘密鍵を鍵寄託機関 (Escrow Authority) に寄託し、鍵が寄託されたことを確認の上、公開鍵を認証機関(Certificate Authority) が認証する。
- 寄託された秘密鍵は、利用者の要請により鍵復元 (Key Recovery)のために利用される他、法律執行上の要請がある場合は捜査当局に開示される。

Clipper 3 の中では、メッセージの守秘を行うために、メッセージ自体の暗号化を行った暗号鍵（以下、セッション鍵）を公開鍵で暗号化し、メッセージと一緒に保管する方法が示されている。法律執行の際には、捜査機関は、まず鍵寄託機関から捜査対象の秘密鍵を開示させ、それを用いてセッション鍵を復号化し、復号化されたセッション鍵によりメッセージを復号化して内容を解読する（図２参照）。

Clipper 3 において提案された内容は多岐にわたっているが、比較的重要と思われる項目を整理すれば次の通り。

① KMI への参加は強制されないが、利用者が認証機関から認証書を得るためには、暗号鍵を鍵寄託機関に提出する必要がある。寄託された鍵は、法律執行上の要請があった場合には、捜査当局に開示される。

② 鍵寄託機関および認証機関は、民間による運営も可能とする。また、信用力のある企業については、鍵を自己で保管する自己寄託を許可する。ただし、当該企業は、捜査当局より要請された際には鍵の開示を行う義務を負う。

③ 暗号アルゴリズム、鍵長、プロトコル、実装方法等については、政府が特定のものを強制することはせず、今後民間主導で決定する。米国政府は、民間企業や既存の標準化団体と協力し、暗号アルゴリズム、技術的なプロトコル、鍵配送、デジタル署名の詳細な仕様を検討し、FIPS 等の技術標準を策定し、その技術標準に従って政府内の情報基盤を構築する。KMI 上で用いられるアプリケーションの安全基準に関して、民間部門と協力して基準の策定を行う政府機関を決定する。

④ 米国政府は、諸外国の政府と協力し、寄託された鍵へのアクセスに関して、各国の国家主権、国家の安全、国防の観点に沿う方式を検討する。その上で、外国での暗号装置の使用については、米国あるいは当該国のどちらかに鍵を寄託することを義務づける政府間協定を締結する。なお、この政府間協定の基本方針は、以下のとおりとする。

a. 法律執行上の必要性からアクセスが許可された際に、速やかに秘密情報を得ることができること。
b. 政府間協定により暗号技術の開発動向に影響が出ることのないようにすること。
c. 第三者あるいは自己寄託による鍵の提出の手順は米国内の方式と整合的なものとすること。

⑤ 上記の協定が多国間で締結される以前については、暗号装置の輸出に関して、以下の経過措置を講じる。

a. 鍵寄託に関する正式な政府間協定の締結以前であっても、欧州諸国など、今後、鍵寄託が採用される可能性の高い国に対しては、KMI 対応の装置の輸出を許可する。
b. 今後、鍵の寄託に関して２国間で協定を締結した国に対しては、個別に検討したうえで KMI 対応装置の輸出を許可する。また、こうした国に対しては、暗号輸出規制の一層の緩和を進める。

⑥ 民間部門との協力により、(a)無権限での鍵の漏洩に対する罰則、(b)不正行為に対する被害者の損害賠償請求、(c)鍵寄託機関により秘密鍵が開示されるための条件、(d)鍵寄託機関の免責条項、等に関する法制度を整備するほか、認証機関や鍵寄託機関の行動規程の策定を行う Policy Approving Authority を設置する。

③ゴア副大統領の公式声明――キーリカバリー構想への転換

米国政府は、1996 年 10 月 1 日に、ゴア副大統領の公式声明として、NIST が Clipper 2 および Clipper 3 で提案した暗号政策の転換を正式に発表した。その内容は、Clipper 2 および Clipper 3 と大きく変るものではなく、米国暗号政策ウォッチャー達からは、「Clipper 3.1.1」（つまり、Clipper 3 のマイナーチェンジ）と呼ばれている。ただし、本発表において、評判の悪かったキーエスクローという言葉に代えて、キーリカバリーという言葉を前面に出し、「犯罪捜査のための暗号解読」というコンセプトから、「正当な利用者が鍵を紛失した時のための備え」というコンセプトに切り替えた点が重要である[18]。これ以降、キーエスクローという言葉はほとんど使われなくなり、一般にもキーリカバリーという表現が用いられるようになった。本発表の関連部分を訳出すると次の通りである。

> キーリカバリーの下では、暗号通信利用者の秘密鍵を復元（recover）することができる鍵復元機関が設置される。この鍵復元機関は、その暗号利用者の所属する民間組織の内部に設立することも可能である。鍵復元機関が管理する秘密鍵へのアクセスは、各利用者が自分の秘密鍵を失念してしまったときにそれを復元する場合、または、法律執行機関が、犯罪捜査等に際して通信内容の解読が必要となり、裁判所等正当な機関の承認を得ることができた場合に限定される。なお、国内で使用される暗号装置にキーリカバリーを採用するかどうかは自由である。

また、Clipper 2 および Clipper 3 では、キーエスクロー技術が確立するまでの移行措置について明確な規定が置かれていなかったが、本発表では、「２年以内に暗号装置へのキーリカバリー機能の搭載が可能となるように、技術開発、製造、販売等の詳細な計画を作成して、監督当局（商務省）から承認を受け、さらに６ヶ月毎に事前に承認された計画の進捗状況がチェックされる」という条件で、キーリカバリー技術が確立する前から、暗号装置のメーカーに暗号輸出のライセンスを付与する制度を導入することが明らかになった。これに関連する規定の詳細は、次の通り。

> 従来、暗号装置の輸出に関しては、輸出可能な暗号装置の鍵長の上限を 40 bit に限定していたが、２年間に限り、鍵長が 56 bit 以下の暗号装置についても輸出を許可する。ただし、輸出業者は、輸出ライセンスを取得するために、以下の２つの要件を満たす必要がある。
>
> ① 輸出ライセンス取得後２年以内に、40 bit より長い鍵長をもつ輸出用の暗号装置すべてに、キーリカバリーを搭載しなければならない。
>
> ② 輸出ライセンス取得後２年以内に暗号装置へのキーリカバリー搭載が可能となるように、技術開発、製造、販売等の詳細な計画を作成して、監督当局（商務省）から承認を得なければならない。さらに、キーリカバリー搭載が可能となるまでは、輸出ライセンスの更新が６ヶ月ごとに行われ、その際に事前に承認された計画の進捗状況がチェックされる。

[18] 米国 IBM 社は、ゴア副大統領の公式声明と同時期に、”The need for a global cryptographic policy framework”と題する論文（IBM[17]）を発表しているが、この中で、キーエスクローとキーリカバリーとの違いについて説明している。それによると、両者の違いは秘密鍵に関する情報を第三者機関がどのような形態で管理するかにあり、「キーエスクローの場合には、第三者機関は秘密鍵そのものを管理するが、キーリカバリーの場合には、第三者機関は、秘密鍵そのものではなく秘密鍵を生成するために必要な情報（Key Recovery Information）のみを管理し、必要に応じてこの情報から秘密鍵を復元する」としている。ただし、後で述べるように、キーリカバリーを実現するための技術には様々なバリエーションが存在するため、本論文では、より広い意味でキーリカバリーという用語を使用している（注 3 を参照）。

④新しい暗号政策の実施

米国の新しい暗号政策は、1996 年 12 月 30 日の米国商務省による輸出管理規制（Export Administration Regulations）の一部改正によりその詳細が規定され、1997 年 1 月 1 日から発効している。その主な改正点を整理すれば次の通り。

(a) 暗号輸出規制の所管が国務省から商務省に移され、商務省の規制に暗号装置の分類、輸出ライセンスの審査手順等に関する規定が置かれた。
(b) キーリカバリー機能を搭載した暗号装置は輸出規制の対象から外される一方、キーリカバリー機能を搭載していない暗号装置は 1998 年末までにキーリカバリー機能を搭載することを条件に 56 bit 以下の鍵長であれば輸出が許可されることが規定された。
(c) 輸出を許可する条件であるキーリカバリー機能の技術的要件等に関する規定が置かれた。すなわち、(i) 合法的な法律執行手続きによって、ユーザーの協力がなくても政府が暗号文を解読するための情報（以下、鍵情報）を入手することが可能となること、(ii) 当該暗号装置によって生成された暗号文だけでなく、受信した暗号文の鍵情報にもアクセスが可能となること、(iii) 鍵情報は、商務省輸出管理局（Bureau of Export Administration）によって認可された鍵復元機関（Key Recovery Agent）のみによって保管されること、等が規定された。
(d) 鍵復元機関の組織およびそれに属する職員がこれまで国家治安上問題を起こしていないかどうか、また情報管理上セキュリティ対策に問題がないかどうかを厳密にチェックすることが定められた。

また、こうした輸出用暗号装置へのキーリカバリー構想の適用に続いて、1997 年 3 月 12 日、米国内におけるキーリカバリー構想の推進を唱えた Electronic Data Security Act of 1997 と呼ばれる法案が米国政府により発表された。同法案では、インターネット上における電子商取引の推進等のために KMI の構築が提案され、その中で米国国民にキーリカバリー構想に参加することを呼びかける内容となっている。

⑤暗号装置製造業者の対応

こうした米国政府の動きを踏まえ、コンピューター・メーカー、ソフト・ベンダー等、暗号装置の製造業者の多くは、政府に積極的に協力する姿勢を示している。IBM 社など 11 社[19]の米国企業は、1996 年 10 月 1 日のゴア副大統領による新政策発表後、共同でキーリカバリー技術の開発・普及に取り組むために Key Recovery Alliance という企業連合を結成すると発表した。Key Recovery Alliance では、政府と協調してキーリカバリー構想に利用される暗号通信技術の標準化を進めるための技術提携を行うことを目的としている。その上で、強力な暗号技術に対するニーズが高まる中、キーリカバリー構想に協力し、これまでよりも強力な暗号装置の輸出ライセンスを取得することを最終的な目的としていると考えられる。その後、この Key Recovery Alliance に参加する企業は更に増加し、1996 年 12 日時点で 40 社に達している。

なお、IBM 社は、ゴア副大統領の公式声明と同時期に発表した論文 “The need for a global cryptographic policy framework” において、「通信利用者の強力な暗号技術へのニーズと、犯罪捜査等における当局の諜報活動に対するサポートとを両立させるために、世界規模でのキーリカバリーを構築する必要があるため、キーリカバリー技術の標準化および実際の運用方法を規定すべく早急に行動しなければならない」と表明している。

1997 年入り後、個別企業にも、キーリカバリー技術の開発に関する具体的な動きがみられ始めている。まず、1997 年 2 月には、IBM、DEC、Cylink の各社が 56 bit 鍵長の暗号輸出許可を得た。これらの 3 社は、現時点でキーリカバリー技術について米国政府から承認を得たわけではなく、今後のキーリカバリー技術の開発計画が承認されたものである。また 1997 年 3 月には、TIS 社の

[19] Key Recovery Alliance に参加した企業は、Apple Computer、Atalla、Digital Equipment、Groupe Bull、Hewlett-Packard、IBM、NCR、RSA Data Security、Sun Microsystems、Trusted Information Systems、UPS の 11 社。

キーリカバリー製品 RecoverKey が、初めてキーリカバリー技術を搭載した暗号装置として承認され輸出を許可された。この製品は他の暗号ベンダーからも注目されており、TIS 社は、本製品について IBM 社とライセンス契約を締結したことや、Hewlett-Packard 社の暗号製品の開発について技術提携を行ったことなどを発表している。

こうした動きがある一方、キーリカバリー構想と輸出規制緩和措置を組み合わせた米国の新しい暗号政策に対して懐疑的な意見を表明する企業もある。例えば、米国 RSA Data Security 社[20]の Jim Bidzos 社長は、1997 年 3 月 21 日の東京での記者会見において、「キーリカバリー構想に協力して、56 bit 以下の暗号装置に関する 1998 年末までの輸出ライセンスを取得する考えはない」ことを表明している。その理由として、「56 bit でも暗号としては不十分で、半年もすれば簡単に破られる恐れがある」ことと、「輸出ライセンスの期限である 1998 年末に、米国政府が追加規制をかけてくる可能性がある」ことの 2 点を挙げ、「こうした状況では、誰も米国製の暗号装置を買いたいと思わないだろう」と発言している。

⑥インターネット技術者の意見

米国政府のキーエスクロー構想（Clipper 1）を事実上頓挫させることに大きな役割を果たした EFF、CDT、EPIC といったインターネット技術者、プライバシー保護論者は、新しい暗号政策、キーリカバリー構想に対しても、引き続き批判を続けている。インターネット上で発表されているキーリカバリー構想に対する彼らのコメントをみると、公開鍵暗号を使用するためのインフラである KMI の構築自体には賛同の意を表しているが、キーリカバリー機能についてはプライバシー侵害に繋がることを懸念する声が引き続き強く、キーリカバリー構想が鍵の寄託と公開鍵インフラの構築を事実上ワンセットにしていることを強く批判している。

EFF は、1996 年 5 月 22 日、キーリカバリー構想に対して以下のとおりコメントしている。

- キーリカバリー構想は、公開鍵の認証に関する民衆の無知につけ込み、KMI には鍵寄託が必要であるかのような誤解を起こさせている。
- 認証と鍵寄託をセットにすることにより、政府から認可を受けた認証機関は、鍵寄託を行わないユーザーの認証を拒絶する可能性がある。
- KMI は、多くの外国政府が同様の政策を採用しないと機能しないが、外国が KMI を受け入れるかどうかは不明である。

また、CDT は、1996 年 5 月 21 日に発表された “Preliminary Analysis of “Clipper III” Encryption Propose”において、以下のとおりコメントしている。

- KMI において安全な通信を行うためには鍵の認証が必要であるが、キーリカバリー構想では、鍵寄託が認証を得るための前提条件となっており、鍵の寄託が事実上強制されている。
- キーリカバリー構想では、鍵寄託の必要性の根拠をデータのバックアップに求めているが、これは公開鍵インフラとは無関係に実現することが可能であり、政府主導で鍵寄託を行う理由にはならない。
- 国際的な鍵の交換に関して、具体的な手順が定められていない。
- 鍵寄託機関に秘密鍵を集中することは、ネットワーク全体のセキュリティを著しく低下させる。
- これまでの企業やプライバシー保護論者の意見が全く反映されていない。現在の米国の暗号政策からはこうした視点が抜け落ちており、国防や法律執行のみが重視されている。

[20] RSA Data Security 社は Key Recovery Alliance の創立メンバーに加わってはいるが、当初からキーリカバリー構想に対して積極的に取り組む姿勢を示していた訳ではなかった。

３．欧州における TTP/鍵寄託制度を巡る動向

米国におけるキーリカバリー構想を巡る議論は、欧州諸国にも波及し、同様の構想を実現しようとする動きがみられている。欧州諸国においても、伝統的に暗号技術は国家が管理してきたため、米国同様、インターネットの普及に伴う暗号技術の一般化が暗号政策に大きな影響を与えている。ただ、欧州諸国の場合、公開鍵インフラにおける鍵寄託機関、鍵復元機関、認証機関の機能を果たす機関である TTP（Trusted Third Party）という概念を用いて、これに対する規制を導入することで、暗号鍵への合法的アクセスを可能とする方針を採っている。欧州諸国では、従来から厳格に暗号技術を規制していたこともあって、TTP 構想においても、それを取り締まるための法制化を先行させるなど、比較的統制色の強い政策を進めていると言われている。

なお、欧州連合では、1995 年 9 月に閣僚理事会において「情報技術に関連する刑事訴訟法の問題に関する勧告（95）13」を採択している（ Committee of Ministers, Council of Europe [36]）が、その中で、①犯罪捜査のための技術的手段を確保すべく、一定の条件の下で情報通信データの傍受を可能にする法案を準備すべきである、②こうした通信傍受等に関する国際的な法的基盤を構築する必要がある、と提言している。

(1)フランスの動向

フランス政府は、1996 年 7 月に電気通信法の一部改正法案を策定しており、その中で、情報の秘匿を目的とする暗号装置を利用する場合には、その暗号鍵を政府によって承認された組織に寄託することを義務付けている（Steptoe & Johnson LLP[35]）。この改正法案はすでに議会を通過しており、現在は具体的な行政立法の策定作業が進められている。該当する条文（電気通信法の一部改正法案の第 12 条）の主な内容は以下の通り。

①情報秘匿のための暗号通信サービス提供者

- 情報の秘匿を目的とした暗号通信サービスを提供する組織は、その事業を行うためには総理大臣による承認が必要である。
- この組織は予め提供するサービス内容を特定する必要があるほか、法律執行の枠組みに基づいて、管理する秘密鍵を法律執行機関に提供しなければならない。
- この組織の承認や法律執行手続きについては、国事院（Council of State）の政令によって規定される。

②暗号装置の利用

- 認証および情報の完全性を確保するための暗号装置については利用が自由であるが、情報の秘匿に用いる暗号装置は総理大臣により承認された組織によって管理される場合にのみ利用することができる。

(2)ドイツの動向

ドイツでは、1996 年 12 月に「情報・通信業務の条件の規制に関する連邦法」が作成され、議会で審議されているが、その第 3 款「電子署名法」の第 12 条（データ保護）において、「法律執行機関は必要に応じて認証機関の管理する個人情報を入手することができる」という条文が置かれている（Kuner[21]）。また、1996 年 10 月に設置された暗号政策に関する省庁間タスクフォースにおいて、ユーザーによる暗号装置の選択の自由と犯罪捜査のための規制との間のバランスをいか

にとるかといった観点から、情報秘匿のための暗号装置の規制や鍵寄託制度の新設が検討されている（辻井・石崎[1]）。

一方、ドイツ産業界では、国際商工会議所ドイツ支部（The German chapter of the International Chamber of Commerce）、ドイツ産業連盟（Bundesverband der Deutschen Industrie e.V.）やドイツ電気通信企業組合（Teletrust e.V.）等がドイツ政府の暗号規制や鍵寄託制度に反対の意を表明している。特に、国際商工会議所ドイツ支部は、政府の規制導入に対して以下の４点を指摘し、「規制導入によるコストに見合う便益を得ることは困難」としている（Kuner[22,23]）。

① 政府が暗号ソフトの利用を法律で制限したとしても、いくつかの暗号ソフトはインターネットを利用することで当局に知られることなく容易に入手可能であり、暗号規制は実質的に無効である。

② 今後の技術革新の方向性は不確実であり、現時点で有効である通信傍受の手段が将来にわたって有効であるとは必ずしもいえない。したがって、現時点での技術を前提とした規制を導入するのは好ましくない。

③ ドイツ政府は暗号通信に利用される暗号鍵を trust center と呼ばれる機関に寄託する仕組みを検討しているが、そうした仕組みは膨大な管理コストを生じさせる。

④ 暗号通信のユーザーの暗号鍵全てを寄託すると、外国の諜報組織等の格好のターゲットとなる可能性があり、そうした組織による不正利用につながりかねない。

(3)イギリスの動向

イギリス政府（貿易産業省：Department of Trade and Industry、以下、DTI）は、1997 年 3 月 21 日に、TTP に関する提言を発表した（DTI[12,13]）。本提言では、イギリス国内で守秘目的の暗号サービスを提供する事業者は、本提言内容に基づいて行われる DTI による審査に合格し、TTP の免許を取得しなければならないとされている。

ただし、銀行のホームバンキングサービス、クレジットカードのオーソリゼーションやペイ TV といった「暗号化される情報が厳格に限定される商業サービス」での暗号の利用や、一組織内に限定された情報通信に暗号を利用する場合には、この規制は適用されない扱いとなっている。

提言の主な内容は、①TTP としての適格性に関する基準、②法律執行手続き、に関するもの。TTP の適格性に関しては、その組織の構成・所有形態、職員や管理者の属性、セキュリティ方針や経営計画等に関する基準が設定されている。また、法律執行については、政府内に法律執行のための単一の中央情報管理機関 (a central repository)を設置することが示されているほか、TTP は、法律執行要請がある場合にはこの法律執行機関に対して秘密の暗号鍵等を提供しなけらばならない、と明記されている。

本提言については、5 月 30 日まで一般からコメントを募集し、それをもとに提言内容の修正等を行う予定。特に、以下の点についてコメントを求める旨が示されている。

① 本提言が想定しているあらゆる前提が妥当かどうか、また、文書の完全性や署名の正当性確認等は取引当事者間の合意だけで十分なのかどうか。

② TTP としての適格性に関する基準の妥当性と、TTP の免許が不要と考えられる暗号サービスの範囲。

③ 海外の利用者を対象に暗号サービスを提供する業者にも TTP の免許を義務づけるべきかどうか。

④ 法律執行に伴う TTP との情報のやり取りを電子的手段によって行うことの是非、法律執行時に裁判所による許可が必要かどうか。

４．キーリカバリー技術――その原理と実装

Clipper 1 の発表後、キーリカバリーの必要性、妥当性を巡って政治的、法律的な観点から様々な議論が行われたが、同時に情報通信技術の分野からも、多くの技術的貢献がなされた。その貢献は、①Clipper 1 のようなハードウェアと非公開の共通鍵暗号アルゴリズムの組み合わせではなく、公開鍵暗号等を利用した新しいキーリカバリー技術の提案、②キーリカバリー技術に対するアタック（例えば、キーリカバリー技術が実装されたシステムを利用しつつ、合法的アクセスを回避する方法）とその対策の研究、などである。以下では、こうした技術面について整理する。

(1)様々なキーリカバリースキーム

キーリカバリーを実現するスキームは、1993 年の Clipper 1 を嚆矢として様々なアイデアが考案されてきた。キーリカバリー構想を推進してきた暗号学者である Dorothy Denning の文献等を基に整理すると、これまで発表された主要なキーリカバリースキームには以下のようなものがある。

キーリカバリースキーム	論文執筆者／開発企業	発表時期	主な用途
1. Clipper Chip (Clipper 1)	米国政府	1993	電話通信
2. Leighton/Micali	Leighton & Micali	1993	
3. Threshold Decryption	Desmedt et al.	1993	情報通信、ﾌｧｲﾙ
4. Leiberich TB-Clipper	Otto Leiberich	June 1994	電話通信
5. Blaze File Crypto	Matt Blaze	June 1994	ﾌｧｲﾙ
6. Micali Fair Crypto	Silvio Micali	Aug. 1994	情報通信、ﾌｧｲﾙ
7. TIS Software Clipper	Trusted Information Systems 社	Aug. 1994	
8. TIS Software Master Key	Trusted Information Systems 社	Aug. 1994	
9. Nortel Entrust	Nortel Secure Network 社	Oct. 1994	電子ﾒｰﾙ、ﾌｧｲﾙ
10. Diffie Time-Bounded Clipper	Beth et al.	1994	電話通信
11. Fortress KISS	Fortress U&T 社	1994	情報通信、ﾌｧｲﾙ
12. TESS with Key Escrow	Beth et al.	1994	情報通信
13. Desmedt Traceable	Yvo Desmedt	May 1995	
14. National CAKE	National Semiconductor 社	June 1995	
15. Cylink Key Escrow	Cylink 社	Sept. 1995	情報通信、ﾌｧｲﾙ
16. Shamir Partial Key Escrow	Adi Shamir	Sept. 1995	情報通信、ﾌｧｲﾙ
17. PC Security Stoplock KE	PC Security 社	Nov. 1995	情報通信、ﾌｧｲﾙ
18. Bankers Trust SecureKEES	Bankers Trust 社	1995	情報通信
19. Kilian/Leighton F-safe	Kilian & Leighton	1995	
20. Lenstra/Winkler/Yacobi	Lenstra et al.	1995	
21. Micali Partial Escrow	Silvio Micali	1995	情報通信、ﾌｧｲﾙ
22. Micali/Sidney Esc.	Micali & Sidney	1995	
23. Royal Holloway TTPs	Jefferies et al.	1995	情報通信
24. Lotus Notes International	Lotus 社	Jan. 1996	情報通信
25. TIS Commercial Key Escrow	Trusted Information Systems 社	Mar. 1996	情報通信、ﾌｧｲﾙ
26. AT&T Crypto Backup	AT&T 社	Mar. 1996	ﾌｧｲﾙ､ﾒｯｾｰｼﾞ音声
27. Bell Atlantic Yaksha	Bell Atlantic 社	Mar. 1996	情報通信、ﾌｧｲﾙ
28. Nechvatal Public-Key	James Nechvatal	Oct. 1996	情報通信
29. Bellare-Goldwasser VPKE	Bellare & Goldwasser	1996	情報通信
30. Bellare-Goldwasser TDKE	Bellare & Goldwasser	1996	情報通信
31. Binding ElGamal	Verheul et al.	Jan. 1997	情報通信、ﾌｧｲﾙ
32. IBM SecureWay	IBM 社	Feb. 1997	情報通信
33. Fortezza Card	Rainbow Technologies 社	―	電子ﾒｰﾙ、ﾌｧｲﾙ
34. RSA Secure	RSA Data Security 社	―	ﾌｧｲﾙ
35. TECSEC VEIL	TECSEC 社	―	ﾌｧｲﾙ

資料：Dorothy E. Denning, "Descriptions of Key Escrow Systems"（Denning[10]）ほか

(2)キーリカバリー技術のモデル化と主要構成要素

キーリカバリー機能を実現するスキームには様々なものがあるため、それらを分類・整理するために、Denning [10]に従って、キーリカバリーの基本機能をモデル化する。その上で、各スキームをそのモデルに当てはめることによって、その特徴点を整理する。

キーリカバリーの基本機能を極めて単純化して記述すれば図３のようになり、キーリカバリーの基本構成要素は、次の３つに分類できる。

①User Security Component (USC)

各ユーザーが暗号化を行う際に、データの暗号化・復号化を実施するとともに、キーリカバリーをサポートする部分。ハードウェア装置又はソフトウェア・プログラムによって実現される。通常、暗号文に **Data Recovery Field (DRF)**を添付する機能を持つ。

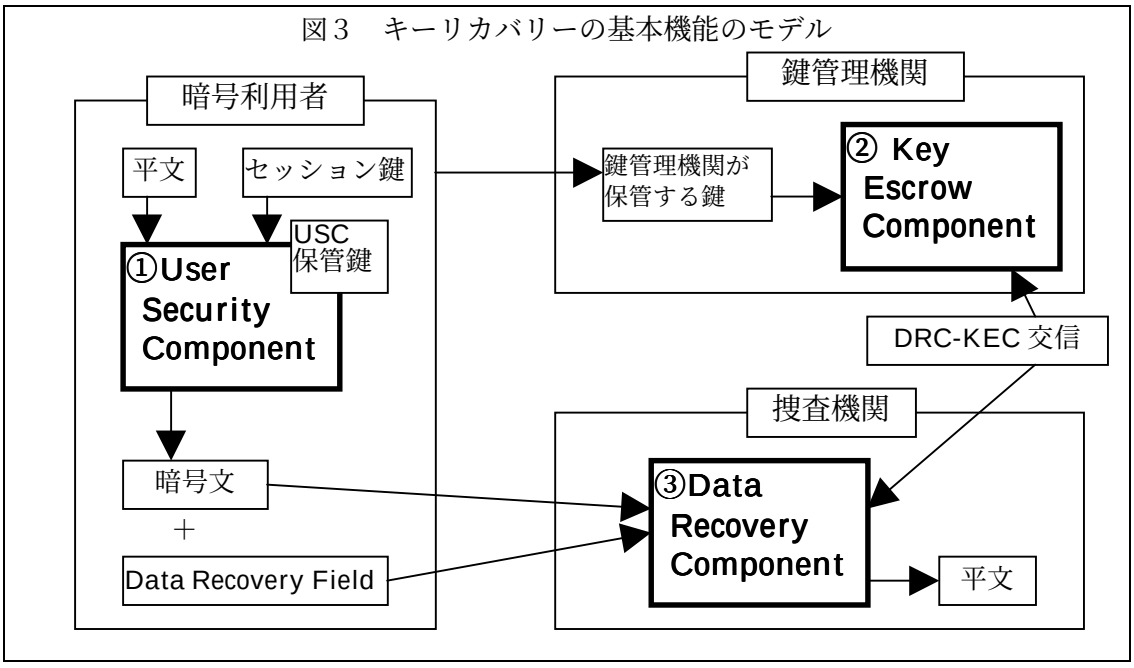
②Key Escrow Component (KEC)

鍵管理機関が操作する部分。事前に装置固有鍵、ユーザー秘密鍵等を受け入れ、これを安全に保管するとともに、必要に応じて鍵情報の提示または暗号化情報の復元サービス等を行う。公開鍵の認証機関または一般的な鍵管理インフラの一部として提供されることもある。

③Data Recovery Component (DRC)

捜査機関等が操作する部分。DRF 内に存在する情報及び KEC により提供される情報に基づいて、解読の対象となる暗号文から平文を復元する。ただし、法的な承認がなければ、鍵復元／データ復元を実行できない仕組みとなっていることが必要。

図３　キーリカバリーの基本機能のモデル



(3)各キーリカバリースキームの評価

前掲のキーリカバリースキームのうち、既に製品化されているものを中心に、前記モデルに基づいてそれらの特徴点を整理すると次のとおり。

キーリカバリースキーム (*は製品化されているもの)	①User Security Component (USC)				②Key Escrow Component (KEC)			③Data Recovery Component (DRC)	
	暗号ｱﾙｺﾞﾘｽﾞﾑ	USC保管鍵	DRF暗号化鍵	実装方法	鍵管理機関が保管する鍵	鍵管理機関数	DRCに提供されるｻｰﾋﾞｽ	復元対象鍵	DRC-KEC交信頻度
①Lotus Notes*	公開	公開鍵	公開	Soft	Master鍵の一部	―	ｾｯｼｮﾝ鍵の一部復号化	送信	ｾｯｼｮﾝ毎に交信
②TIS RecoverKey*	公開	秘密鍵	公開配送	Soft	Master鍵	1	ｾｯｼｮﾝ鍵の復号化	送受信	送受信者毎に交信
③IBM SecureWay Key Recovery Technology	公開	秘密鍵	公開	Soft	Master鍵	複数	ｾｯｼｮﾝ鍵暗号化情報の提示	送受信	ｾｯｼｮﾝ毎に交信
④Micali Partial Escrow	―	―	―	―	User秘密鍵の一部	―	―	―	―
⑤Micali Fair Crypto	公開	秘密鍵	公開配送	―	User秘密鍵	複数	user秘密鍵の提示	受信	受信者毎に交信
⑥Royal Holloway TTPs	公開	秘密鍵	秘密配送	―	User秘密鍵	―	user秘密鍵の提示	送受信	送受信者毎に交信
⑦Bankers Secure KEES*	公開	秘密鍵	公開配送	Hard	User秘密鍵	複数	user秘密鍵の提示	送受信	送受信者毎に交信
⑧Nortel Entrust*	一部公開	秘密鍵	公開配送	Hard Soft	User秘密鍵	1	user秘密鍵の提示	送受信	送受信者毎に交信
⑨Fortezza Card*	非公開	秘密鍵	秘密	Hard	User秘密鍵 装置固有鍵	1 2	装置固有鍵の提示	受信	送受信者毎に交信
⑩Clipper Chip (Clipper 1)*	非公開	秘密鍵	秘密	Hard	装置固有鍵	2	装置固有鍵の提示	送信	送信者毎に交信
⑪Leighton/Micali	公開	秘密鍵	―	―	装置固有鍵	―	装置固有鍵の提示	送受信	―
⑫Shamir Partial Escrow	―	秘密鍵	―	―	ｾｯｼｮﾝ鍵の一部	―	ｾｯｼｮﾝ鍵の一部提示	―	―
⑬PC Sec. Stoplock KE*	一部公開	秘密鍵	―	Soft	ｾｯｼｮﾝ鍵	―	―	―	―
⑭Bell Atlantic Yaksha	公開	秘密鍵	―	―	ｾｯｼｮﾝ鍵	1	ｾｯｼｮﾝ鍵の提示	―	ｾｯｼｮﾝ毎に交信

①USC (User Security Component)の特徴点

- 暗号アルゴリズム（**Data Recovery Field** 等を暗号化するアルゴリズムの公開／非公開）
  ――Clipper 1 は非公開としていたが、その後のスキームでは公開アルゴリズムの暗号を利用する例が多い。
- USC 保管鍵（USC に常時保管され、キーリカバリー機能のために利用される鍵）
  ――通常は共通鍵方式の鍵や公開鍵暗号の秘密鍵が利用される。
- DRF 暗号化鍵（**Data Recovery Field** を計算するために用いられる暗号鍵）
  ――Clipper 1 では共通鍵方式の鍵が利用されていたが、その後のスキームでは、KEC の公開鍵を利用したり、鍵配送のデータを DRF として利用するスキームが増えている。
- 実装方法
  ――Clipper 1 では特別なハードウェアが必要とされていたが、その後、ソフトウェアのみで実装可能なスキームが登場している。

②KEC (Key Escrow Component) の特徴点

- 鍵管理機関が保管する鍵
  ――Clipper 1 では装置固有鍵を保管していたが、マスター鍵（鍵管理機関の秘密鍵）、各ユーザーのセッション鍵、各ユーザーの秘密鍵などを保管するスキームが登場している。
- 鍵管理機関数
  ――Clipper 1 では複数の鍵管理機関に装置固有鍵を分けて保管する構想であったが、その後考案されたスキームには、1 機関のみとしているもの（鍵保管機関の情報濫用については割り切る考え方）、複数機関を想定し全機関の鍵情報が必要なもの、複数機関を想定し n 機関のうち k 機関の鍵情報が必要なもの、がある。
- DRC に提供されるサービス
  ――Clipper 1 では、装置固有鍵の提示を受ける作りであったが、特定の取引のセッション鍵等を提示、復元したり、鍵の部分情報のみを提示したり、特定の盗聴対象時間や有効期限付きの鍵が提示されるといったバリエーションが提案されている。これは、一旦装置固有鍵を入手してしまうと、捜査機関が過去から将来に亘る全暗号化情報を復号化できてしまうという批判に応えたもの。

③DRC (Data Recovery Component) の特徴点

- 復元対象鍵
  ――Clipper 1 では送信者の暗号情報を復号化する鍵を入手するスキームであったが、その後は受信者側の鍵を入手できたり、送信者と受信者の両方の暗号情報を復号できる鍵を入手するスキームが提案されている。この項目は、特に国際的な暗号通信において、送信者または受信者の居住する国の捜査機関が、送信電文も受信電文も復号化できるか否かという問題に関連している。
- DRC-KEC 交信頻度（DRC が鍵を得るために KEC と交信しなければならない頻度）
  ――セッションの都度、異なる鍵を入手する必要がある場合、DRC と KEC との交信頻度は高くなるが、送信者毎、受信者毎に１種類の鍵で復号化ができれば、交信頻度は少なくなる。

(4)各キーリカバリースキームの概要

(3)で特徴点を整理した 14 種類のキーリカバリースキームの概要は次の通り。

① Lotus Notes（Release 4 International Edition）

利用者は、機密情報を 64 bit のセッション鍵によって暗号化し、そのセッション鍵を 512 bit の RSA 暗号によって暗号化する。また 64 bit のうち 24 bit が米国政府の RSA 公開鍵で暗号化されて、DRF として暗号データとともに保存される。

法律執行時には、法律執行機関が米国政府の秘密鍵を用いて DRF からセッション鍵の 24 bit 部分を復号化するとともに、残りの 40 bit については全数探索法によって復元することで、セッション鍵全体を復元し、機密情報を解読する。

② TIS RecoverKey

送信者は、まずセッション鍵（通常は 56 bit の DES 鍵）を生成し、a.機密情報をセッション鍵を用いて DES 暗号で暗号化し、b.受信者の RSA 公開鍵でセッション鍵を暗号化する。そして、c.セッション鍵に 32 bit の識別子（ARI：Access Rules Index）を添付したものを鍵管理機関の RSA 公開鍵によって暗号化し、これに鍵管理機関の ID を添付して DRF を作成する。送信者は、このようにして作成したデータ a.、b.、c.を一緒にして受信者に送信する。

受信者は、自分の RSA 秘密鍵と b.のデータから、RSA 暗号を復号化してセッション鍵を入手し、そのセッション鍵を用いて a.のデータを DES 暗号で復号化して機密情報を入手する。

法律執行時には、法律執行機関は、鍵管理機関に法律執行対象者が送信者となる暗号文の DRF（c.）を送付し、セッション鍵の復元を依頼する。鍵管理機関は、DRF を自分の RSA 秘密鍵で復号化した後、DRF に含まれる ARI が確かに法律執行対象者のものであることを確認して、法律執行機関にセッション鍵を提供する。このセッション鍵を用いて、法律執行機関は機密情報を復号化することができる(TIS[37])。

③ IBM SecureWay Key Recovery Technology

暗号通信を行う際、セッション鍵は予め配送される。次に、送信者および受信者は、自分が登録している鍵管理機関（複数化可能）に対して、DRF を作成するために必要な情報の送付を依頼する。鍵管理機関は、固有の乱数を自分の公開鍵で暗号化したものと、その乱数から生成したユニークなパラメータとを返送する。以上の情報を入手した送信者および受信者は、各鍵管理機関が生成したパラメータで順次セッション鍵を暗号化する。受信者は、a. 自分の ID 情報、b. 鍵管理機関の公開鍵により暗号化された乱数（鍵管理機関の数だけ存在）、および c. 各鍵管理機関のパラメータにより暗号化されたセッション鍵を送信者に送信する。これらを受け取った送信者は、自分と受信者に関する以上の a., b., c. から構成される DRF を作成する。この DRF は、セッション鍵により暗号化された通信データに添付され、受信者に送付される。

法律執行時には、法律執行機関は DRF を入手し、その中から法律執行対象者の鍵管理機関によって暗号化された乱数を抽出して、該当する鍵管理機関に提出する。鍵管理機関は乱数を復号化し、その乱数からセッション鍵を暗号化するのに用いたパラメータを復元して法律執行機関に提供する。法律執行機関は、各鍵管理機関から入手したパラメータを使ってセッション鍵を復号化する(IBM[18])。

④ Micali Partial Escrow

利用者は、公開鍵暗号（RSA 等）における自分の秘密鍵の一部を複数の鍵管理機関に分割して寄託する。秘密鍵のうち鍵管理機関に寄託されない残りの部分の鍵長は、法律執行機関が素因数分解問題や離散対数問題の求解計算によって復元可能なように設定する。送信者は、セッション鍵を受信者の公開鍵によって暗号化し、鍵配送を兼ねた DRF として配信する。

法律執行時には、法律執行機関は、各鍵管理機関から受信者の秘密鍵の一部を入手して秘密鍵を復元する。秘密鍵の残りの部分は上記計算によって求める。

⑤ Micali Fair Crypto

鍵管理機関は各利用者の公開鍵と秘密鍵を保管しておく（分散保有可能）。暗号通信に際し送信者は生成したセッション鍵を受信者の公開鍵で暗号化するが、同データが DRF となる。

法律執行時には、法律執行機関は、鍵管理機関から捜査対象通信路における受信者の秘密鍵を入手し、傍受した DRF からセッション鍵を復元する(Micali[24])。

⑥ Royal Holloway TTPs

ユーザーは送信用および受信用の２種類の公開鍵・秘密鍵のペアを所有する。このうち、送信用の秘密鍵が鍵管理機関に寄託される。また、受信用の秘密鍵は、通信を行うユーザーの２つの鍵管理機関が共有する数値と、各ユーザーの ID を使って生成される。

暗号通信を行う場合、まず、送信者は自分の鍵管理機関から、受信者の受信用公開鍵を入手する（鍵管理機関は、受信用秘密鍵および公開鍵を、各ユーザー ID と、受信するユーザーの鍵管理機関との共有情報によって計算可能)。送信者は、受信者の受信用公開鍵と自分の送信用秘密鍵を利用してセッション鍵を作成し、それを用いて通信データの暗号化を行う（Diffie-Hellman の鍵交換方式)。さらに、送信者は、DRF として、自分の送信用公開鍵と、受信者の受信用公開鍵を暗号文に添付する。

法律執行時においては、法律執行機関は、鍵管理機関から法律執行対象者の送信用または受信用秘密鍵を入手する。法律執行の対象者が送信者の場合、そのユーザーの送信用秘密鍵を入手し、受信者の受信用公開鍵を使ってセッション鍵を復元する。一方、法律執行の対象者が受信者の場合は、受信用秘密鍵を入手し、送信者の送信用公開鍵を使ってセッション鍵を復元する(Laurie[23])。

⑦ Bankers Secure KEES

利用者は、鍵配送のための公開鍵および秘密鍵が封入されている IC ｶｰﾄﾞを利用する。このうち、秘密鍵は鍵管理機関に寄託され、同時に寄託証明書が発行される。暗号通信を行う場合、暗号文に Message Control Header（MCH）と呼ばれる DRF が添付される。MCH には、暗号文送信者の公開鍵で暗号化されたセッション鍵、受信者の公開鍵で暗号化されたセッション鍵、そしてそれぞれの寄託証明書が含まれる。

法律執行時には、法律執行機関は、入手した MCH の寄託証明書によって鍵管理機関を特定して秘密鍵を取得し、セッション鍵を復号化する。

⑧ Nortel Entrust

鍵管理機関である Entrust Key Manager がセッション鍵配送のための公開鍵および秘密鍵を生成・保管するとともに、各ユーザーにそれらのコピーを送付する。暗号文送信者は、DES 等のセッション鍵を生成して暗号文を作成したのち、受信者の公開鍵で暗号化したセッション鍵等をもとにして DRF を作成する。DRF は暗号文に添付されて送付される。

法律執行時には、法律執行機関は鍵管理機関から受信者の秘密鍵を入手して DRF を復号化し、セッション鍵を入手する。

⑨ Fortezza Card

Fortezza Card は、Capstone Chip を実装する PCMCIA card であり、共通鍵方式のアルゴリズムとして Skipjack を利用する。Capstone Chip には Skipjack の秘密鍵のほか、鍵配送（Diffie-Hellman 方式）に利用される公開鍵・秘密鍵が保管される。鍵管理機関に対しては Skipjack の秘密鍵が寄託されるほか、鍵配送に用いる秘密鍵も公開鍵の認証機関に対して寄託される。セッション鍵は暗号通信を行う前に配送されるが、これが DRF として機能する。

法律執行時には、法律執行機関は認証機関から受信者の秘密鍵を入手してセッション鍵を復元できるほか、鍵管理機関から Skipjack の秘密鍵を入手して復元することも可能である(National Semiconductor[30])。

⑩ Clipper Chip (Clipper 1)

セッション鍵が Diffie-Hellman 鍵交換方式等により共有された後、送信者の保有する装置固有鍵により暗号化されたセッション鍵が、DRF として暗号文に添付される。装置固有鍵は２つの鍵管理機関により分割保有されている。

法律執行に際しては、法律執行機関は２つの鍵管理機関から得たパーツを合成、装置固有鍵を復元し、傍受した DRF からセッション鍵を復元する。

⑪ Leighton/Micali

鍵管理機関は、各ユーザーにユニークな ID と秘密鍵を生成して、各ユーザーにそれらのコピーを送付する。ユーザー間の暗号通信に利用されるセッション鍵は、各ユーザーの秘密鍵と通信相手の ID を使って生成され、自動的にユーザー間での共有が可能となる（ID に基づく予備通信不要な鍵共有方式）。同時に、鍵管理機関も各セッション鍵は計算可能である。

法律執行時には、法律執行機関は、鍵管理機関からセッション鍵または受信者の秘密鍵を入手することによって暗号文の復号化が可能となる。

⑫ Shamir Partial Escrow

利用者は、セッション鍵のもととなる 256 bit の数値のうち、固定されている 208 bit 分を鍵管理機関に寄託し、残り 48 bit を暗号通信の度に生成する。データの暗号化を行う際には、利用する共通鍵方式の鍵長に合わせて 256 bit の数値を圧縮する。

法律執行時には、法律執行機関は各鍵管理機関から 208 bit 分の鍵を入手するとともに、全数探索によって残りの 48 bit の部分を復元する。

⑬ PC Security Stoplock KE

最初に鍵管理機関がすべてのユーザーのセッション鍵を作成し、そのコピーをユーザーに送付する。各ユーザーはこのセッション鍵を利用して暗号通信を行う。DRF は利用しない。法律執行機関は、鍵管理機関からセッション鍵を入手して暗号文の復号化を行う（詳細は不明）。

⑭ Bell Atlantic Yaksha

ユーザーは、鍵配送に利用する秘密鍵および公開鍵を生成しておく。暗号通信を開始するに際し、セッション鍵生成を鍵管理機関に依頼し、自分の秘密鍵の部分情報を鍵管理機関に送付する。鍵管理機関は、生成したセッション鍵をこの秘密鍵の部分情報で暗号化して各ユーザーに送付する。各ユーザー側では、残りの秘密鍵の部分情報と公開鍵によってセッション鍵を復号化して利用する。

法律執行時には、鍵管理機関はセッション鍵を法律執行機関に提供する。

(5)具体的な実装製品の例

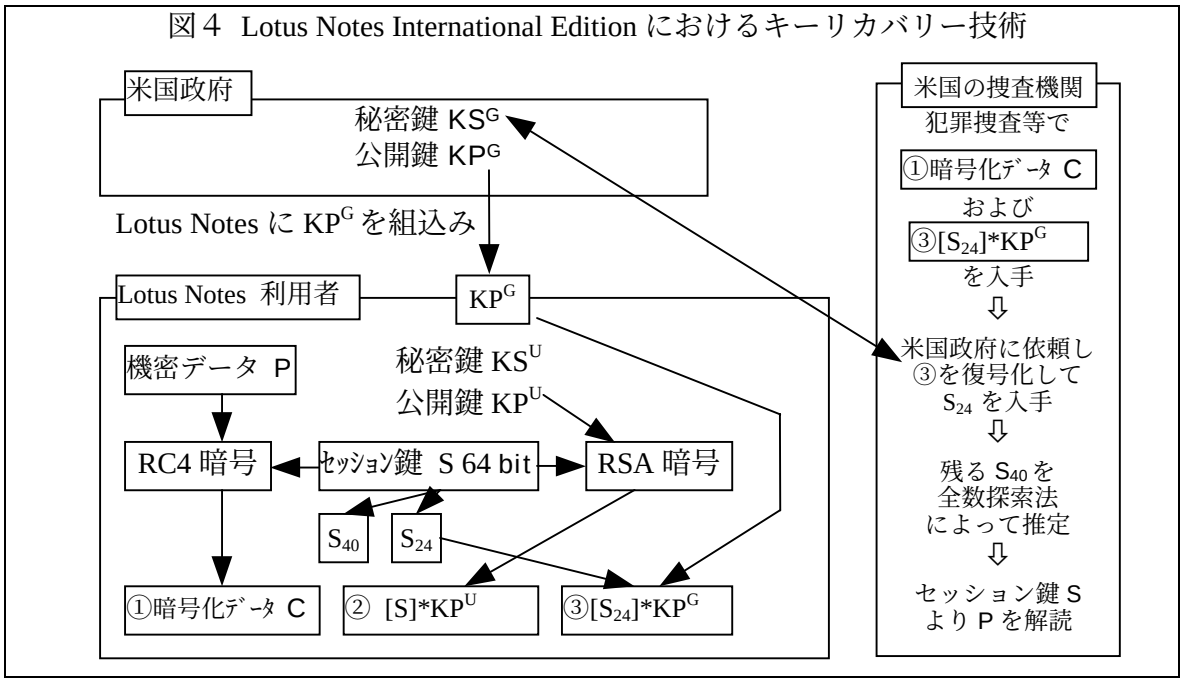
以下では、キーリカバリー技術を実装した製品の構造をみるために、①Lotus Notes、②TIS RecoverKey、③IBM SecureWay Key Recovery Technology について、やや詳しく紹介する。

① Lotus Notes（Release 4 International Edition）

Lotus Notes は米国 Lotus 社が開発したグループウェア製品で、LAN を利用した企業の情報システムの構築において、社内における各種決裁事務を機械化する場合などに多く利用される。グループウェア製品としては世界中で最も広く普及している製品であり、事実上の業界標準の地位を獲得しているとされている[21]。

1996 年に発売された Lotus Notes Release 4 では、決裁書類にデジタル署名を付与したり、機密情報を含む電子メール、ファイルを暗号化して保管する場合などに、暗号技術を採用した。具体的には、ファイルの暗号化には鍵長 64 bit の RC4 共通鍵暗号を、RC4 で利用するセッション鍵の暗号化には鍵長 512 bit の RSA 公開鍵暗号を、各々利用している。このソフトウェアを米国から海外に輸出する場合、そのままでは暗号輸出規制に抵触するため、その International Edition（輸出版）においては、次のようなキーリカバリー技術を採用することにより、事実上の鍵長を 40 bit として輸出許可を取得している（図４参照）。

図４ Lotus Notes International Edition におけるキーリカバリー技術



利用者が機密情報（P）を暗号化しようとすると、64 bit のセッション鍵（S）がランダムに生成され、RC4 によって暗号化が行われる（C）。セッション鍵は、その利用者のみが秘密鍵を知っている 512 bit の RSA 暗号によって暗号化される([S]*KP^U)。また 64 bit のうち 24 bit（S_{24}）が米国政府の RSA 公開鍵（KP^G）で暗号化されて、DRF として暗号データとともに保存される([S_{24}]*KP^G)。法律執行においては、米国政府は自分の秘密鍵を用いて DRF からセッション鍵の 24 bit 部分を復号化するとともに、残りの 40 bit（S_{40}）については全数探索法によって復元することで、セッション鍵全体（$S=S_{24}+S_{40}$）を復元し、機密情報（P）を解読する。

[21] Lotus 社の資料によれば、1996 年末時点で、Lotus Notes のユーザーは全世界で 950 万人、日本国内で 122 万人に達している。国内での大規模ユーザーは、官庁、金融機関、電機・自動車等の大手メーカー、通信業者等、あらゆる業種に亘っている。

② TIS RecoverKey[22]

TIS RecoverKey は、Trusted Information Systems 社[23]が開発したキーリカバリー技術である。同社の資料 “TIS announces encryption Key Recovery Technology – Technical Description” (TIS[37])によれば、同社が提供する暗号開発ツールキットを利用してユーザーのシステムに CSP（Cryptographic Service Provider）と呼ばれるプログラムを組み込むことにより、Clipper 2 に定められている Key Escrow 機能を具備する暗号機能の提供を可能にすると謳われている。なお、同社は 1996 年 9 月に本技術に関する特許を取得している。

RecoverKey では、Key Escrow 機能を実現するために、データ復元センター（DRC：Data Recovery Center）と呼ばれる鍵寄託機関と認証機関の機能を果たす機関を利用する。DRC は、ユーザー登録時に自分の公開鍵が含まれている認証証明書を各ユーザーの CSP に発行し、法律執行や秘密鍵の失念等が生じた場合には、DRF からセッション鍵を復号化する役割を担っている。CSP は、DRC が発行した認証証明書から DRC の公開鍵を入手してセッション鍵を暗号化し、それを DRF の一部として暗号文に添付する。RecoverKey のキーリカバリー技術の主な特徴は次の通り。

① ユーザーは、暗号通信に利用する秘密鍵やセッション鍵を第三者に寄託する必要がない。
② DRC は DRF からセッション鍵を入手するため、法律執行対象者が受信者であっても発信者であってもその暗号文は復号化可能である。
③ セッション鍵は通信の度に変更されるので、法律執行機関による通信傍受が可能な期間を限定することが可能である。

暗号アルゴリズムとしては、通信データの暗号化には RC2、RC4（以上、鍵長 128 bit まで可能）、DES または Triple-DES といった共通鍵暗号が利用され、セッション鍵の交換、デジタル署名や DRF の作成には RSA（鍵長 1,024 bit まで可能）公開鍵暗号が利用される(TIS[38])。

（RecoverKey における暗号通信―ﾕｰｻﾞｰ A がﾕｰｻﾞｰ B に暗号文を送付する場合、図５参照）

① 各ユーザーは DRC に登録し、DRC から Access Rule Index（ARI、32 bit のデータ）と呼ばれる ID と、ユーザーの公開鍵に関する DRC の認証証明書を取得する。
② ユーザー A は、ランダムにセッション鍵を生成し、それを用いて平文を暗号化した後、セッション鍵をユーザー B の公開鍵で暗号化する。セッション鍵は暗号通信の度変更する。
③ ユーザー A は、暗号文に添付するデータとして、DRF と DRC Verification String（DVS）を作成する。
・ DRF は、セッション鍵と ARI を連結したものを DRC の公開鍵で暗号化したもの。
・ DVS は、DRC の公開鍵と ARI を連結したものをセッション鍵で暗号化したもの。

---

[22] TIS 社が発表したキーリカバリー対応製品は複数存在するが、ここではその基本技術を紹介している。なお、TIS 社の技術文献のうち、TIS[37]では Commercial Key Escrow、Commercial Key Recovery、TIS[38]では RecoverKey-International、RecoverKey という名称が使われているが、これらの違いを整理すれば、下表のとおり。

TIS 社のキーリカバリー技術のタイプ別・時期別による分類

	1996 年 1 月の資料･TIS[37]	1996 年 11 月の資料･TIS[38]
米国内向け技術 (Key Recovery はオプション)	Commercial Key Recovery	RecoverKey
輸出向け技術 (強制的に Key Recovery を行う)	Commercial Key Escrow	RecoverKey-International

[23] Trusted Information Systems 社：米国 Maryland 州 Glenwood を本拠,とする情報セキュリティ製品の有力なベンダー。暗号ソフトウエアの開発サポート、ファイヤーウォール製品の製造・販売やコンサルタント業務を行っている。

なお、ユーザー A は、同時にユーザー B の ARI を利用してユーザー B の DRF および DVS も作成する。

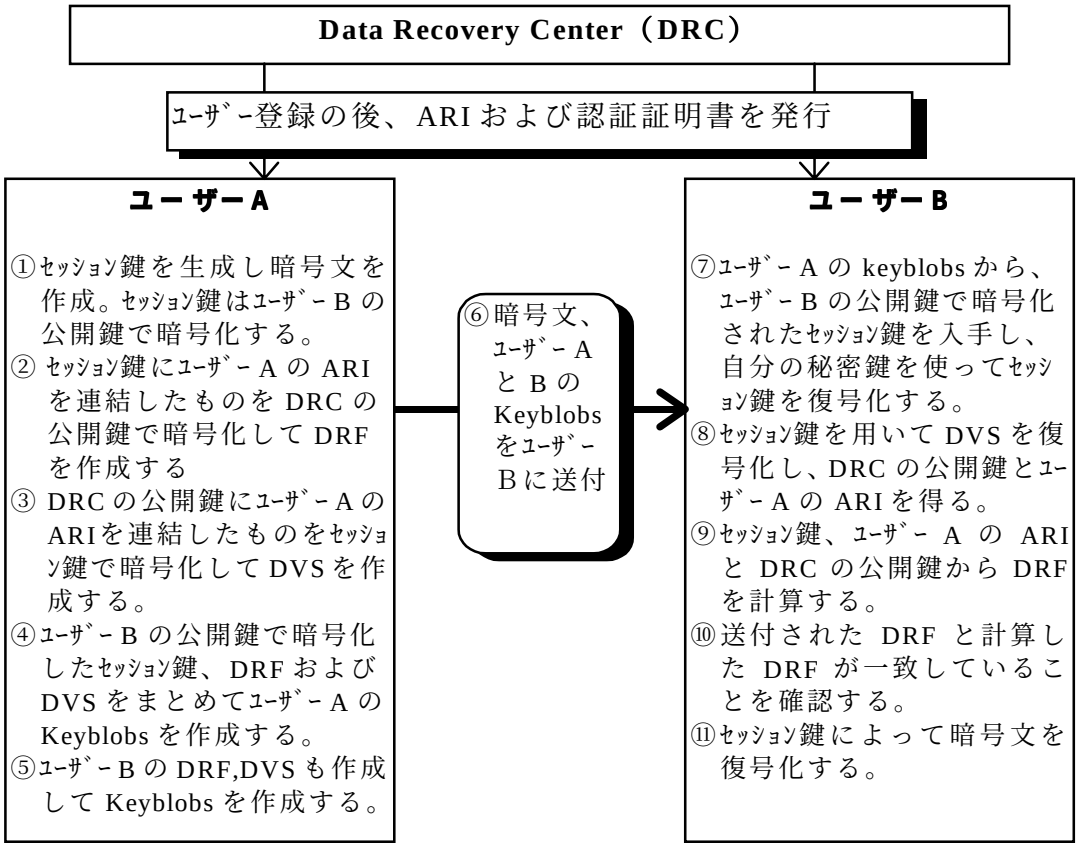
④　ユーザー A は、DRF、DVS、通信相手の公開鍵で暗号化されたセッション鍵を組み合わせて Keyblobs（これら３つの鍵情報を束ねた「鍵束」の意味）を作成する。ユーザー A は、ユーザー B の Keyblobs も作成し、２つの Keyblobs を暗号文とともにユーザー B に送付する。

⑤　ユーザー B は、ユーザー A の Keyblobs の中から、自分の公開鍵で暗号化されているセッション鍵を取り出し、自分の秘密鍵を使ってセッション鍵を復号化する。次に、復号化されたセッション鍵を利用して DVS を復号化し、DRC の公開鍵と ARI を得る。

⑥　ユーザー B は、セッション鍵と ARI を連結したものを DRC の公開鍵で暗号化し、DRF を作成する（ユーザー A とユーザー B の２つを作成)。作成した２つの DRF と、ユーザー A から送付された２つの DRF がそれぞれ一致することを確認する。

⑦　ユーザー B は、セッション鍵によって暗号文を復号化する。

図５　RecoverKey における暗号通信方法
（ﾕｰｻﾞｰ A からﾕｰｻﾞｰ B に暗号文を送信する場合）



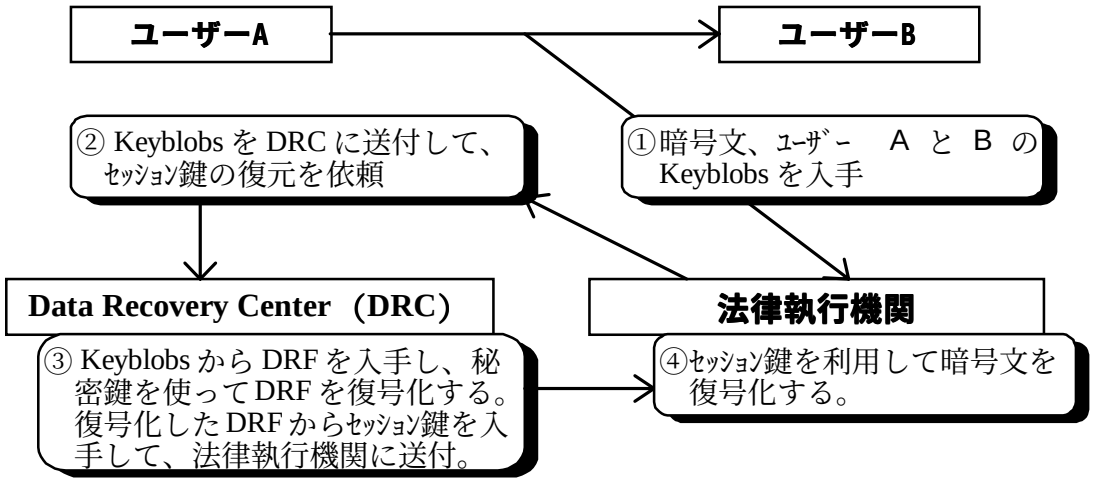
（セッション鍵の復元手順、図６参照）

①　法律執行機関は、復号化したい暗号文と、それに添付されている Keyblobs を入手し、Keyblobs の中から DRF を DRC に送付する。

② DRC は、自分の秘密鍵で DRF を復号化して ARI とセッション鍵を得る。DRC は、法律執行機関が通信を傍受しようとしている者が合法的に許可された対象者に間違いないことを ARI によって確認する。確認後、法律執行機関にセッション鍵を提供する。

③ 法律執行機関は、入手したセッション鍵で暗号文を復号化する。

図６　RecoverKey における キーリカバリーの方法



③IBM SecureWay Key Recovery Technology

IBM SecureWay Key Recovery Technology（以下、SecureWay）は、IBM 社が開発したキーリカバリー技術である。同社の資料”Key management framework and key recovery technology”（IBM[18]）によれば、SecureWay の主な特徴は次の通り。

① 暗号文を復元するための情報は、Key Recovery Service Provider（以下、KRSP）と呼ばれる機関によって保管される。KRSP については、鍵寄託機関のような独立した機関、あるいは民間企業が社員の KRSP となる等のフレキシブルな運用を想定している。しかし、保管される情報はユーザーの秘密鍵やセッション鍵ではなく、DRF に含まれる暗号化されたセッション鍵を復号化するための情報である。

② 法律執行上の要請からセッション鍵を復号化する場合、KRSP はセッション鍵を復号化するための情報を法律執行機関に提供するのみであり、セッション鍵自体を知ることはできない。セッション鍵は、法律執行機関自らが復号化する。

③ セッション鍵は各暗号通信ごとに変更されるほか、KRSP が法律執行機関に提供するセッション鍵復号化のための情報も各暗号通信ごとに生成されるため、法律執行機関が傍受できる暗号文を制限することが可能である。

④ 法律執行機関は、ある特定のユーザーについて、そのユーザーが受信した暗号文だけでなく送信した暗号文についても傍受可能である。

（暗号通信―ﾕｰｻﾞｰ A からﾕｰｻﾞｰ B に送信する場合、図７参照）

① ユーザー A は、暗号通信開始前に、利用する KRSP を複数選択し（利用する KRSP の数は任意）、登録する。

② ユーザー A は、通信相手との間で相互認証およびセッション鍵の交換を行う。

③ ユーザー A は、通信文をセッション鍵によって暗号化した後、セッション鍵を復号化するための情報 Key Recovery Information（以下、KRI）を作成する。KRI の内容および作成方法は次の通り。

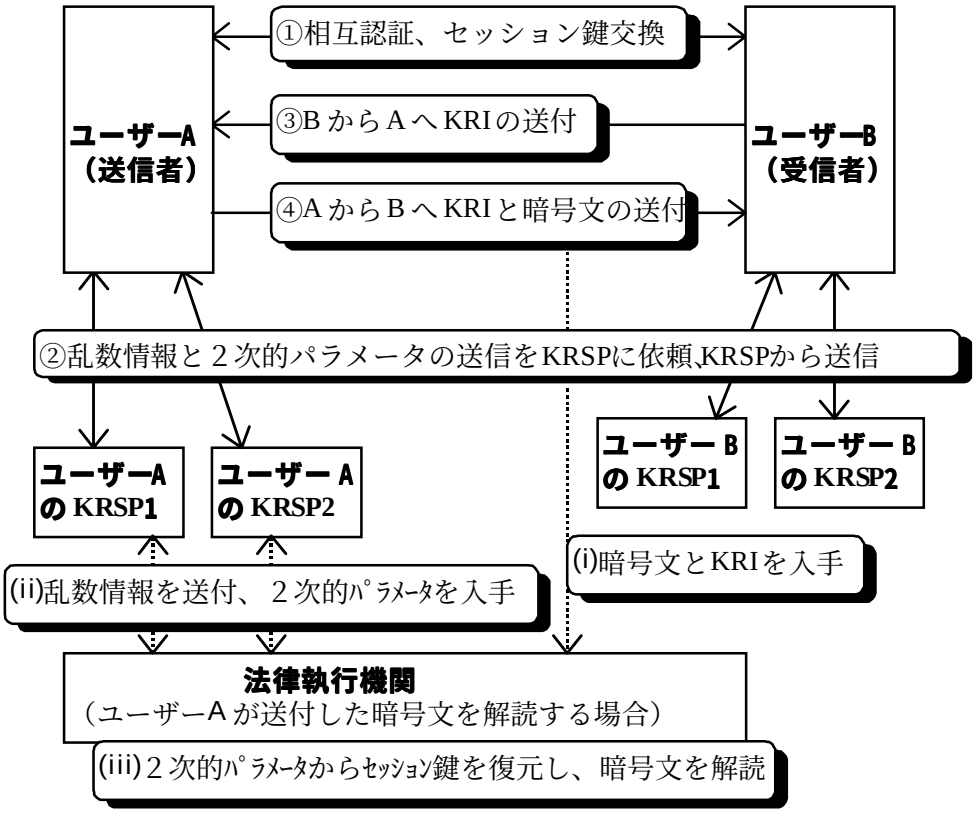
- KRI は、管理情報、乱数情報、セッション鍵情報から成る。
- 管理情報は、暗号文の送受信者の ID、KRSP の ID、セッション鍵の有効期間、暗号文送信時刻等によって構成される。
- 乱数情報は、各 KRSP が秘密に所有している乱数を、各 KRSP の公開鍵によって暗号化したものである。KRI には、この乱数情報が KRSP の数だけ含まれる。
- セッション鍵情報は次の手順で生成される。まず、各 KRSP は自分の乱数からある特定の方法で２次的パラメータ（Secondary Parameter）を生成する。次に、ユーザー側のサーバーが、各 KRSP の２次的パラメータを利用して順次セッション鍵を暗号化する。この暗号化されたセッション鍵がセッション鍵情報となる。

④ ユーザー B は、自分の KRI を同様に作成し、ユーザー A に送付する。

⑤ ユーザー A は、２つの KRI を暗号文に添付して送信する。

⑥ ユーザー B は、暗号文を受信すると、あらかじめ交換しておいたセッション鍵によって暗号文を復号化する。通常の暗号通信では KRI は利用されない。

図７　SecureWay を利用した暗号通信およびキーリカバリーの全体図



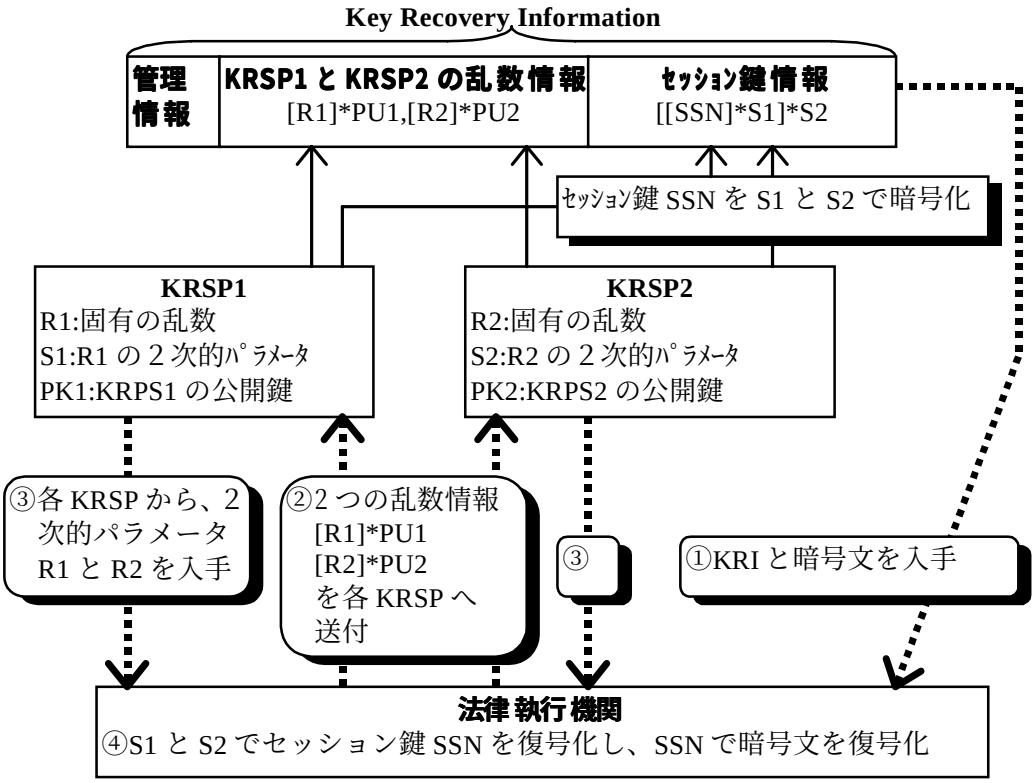
（セッション鍵の復元手順、図８参照）

① 法律執行機関は、復号化したい暗号文に添付されている法律執行対象者の KRI を入手し、そのうちの乱数情報を対応する各 KRSP に送付する。

② 各 KRSP は、まず乱数情報を自分の秘密鍵で復号化して乱数を得た後、その乱数から２次的パラメータを生成し、それを法律執行機関に提出する。

③ 法律執行機関は、各 KRSP から入手した２次的パラメータを利用してセッション鍵情報を復号化し、セッション鍵を得る。

図８ KRI の内容とセッション鍵復号化の手順（KRSP が２つの場合）



(6)合法的アクセスを回避する技術とその対策

以下では、キーリカバリー技術に対する攻撃法、特に当該キーリカバリースキームを利用しつつ、合法的アクセスのみを無効化する方法とその対策の研究動向について、簡単に紹介する。

①主要なキーリカバリースキームの分類

これまで提案されてきた主要なキーリカバリースキームをごく大まかに分類すると、次のような整理が可能である。

(**方式Ａ**) 各利用者に固有の秘密鍵（共通鍵方式）を鍵管理機関に登録させておき、セッション鍵を同秘密鍵により復元可能なデータ（KRF：Key Recovery Field）として通信文に埋め込ませる方式（Clipper 1）

(**方式Ｂ**) 各利用者に各自の公開鍵セット或はその部分情報を鍵管理機関に登録させておき、同公開鍵方式によりセッション鍵を配送させる方式（Micali の Fair Public-Key Cryptosystems（Micali[24]）、Kilian & Leighton の Failsafe Key Escrow Approach（Kilian and Leighton[20]））

(**方式Ｃ**) セッション鍵を鍵管理機関のマスター鍵（公開鍵暗号における秘密鍵）から算出可能なデータとして通信文に埋め込ませる方式（TIS 社の RecoverKey、IBM 社の SecureWay Key Recovery Technology）

②主要なキーリカバリースキームに対する攻撃法と対抗措置

①で挙げた主要なキーリカバリースキームに対して、これまでに提案されている合法アクセス無効化法と対抗措置は以下の通り。

(ア) 別の暗号アルゴリズムを用いる方法

これはキーリカバリーの暗号アルゴリズムの入力前後に別の暗号アルゴリズム（鍵は登録しているものと同じで良い）を用いて暗号化する方法である。これは最も原始的な合法アクセス無効化法であるが、どのようなシステムに対しても有効でかつ対抗策が講じ難い方法と考えられる。但し、こうした無効化法が行われていること自体は法律執行機関により検出され得る。

(イ) 真正な KRF を通信文に埋め込まない方法――方式Ａ、方式Ｃの攻撃法

プログラムに手を加えることにより真正な KRF を通信文に埋め込まないようにする方法が Blaze によって示されている（Blaze[5]）。真正性確認に合格するような偽造 KRF を作成する方法（Clipper Chip の場合、check sum が 16 bit なので、高々 2^{16} 回の暗号化と同等の操作で偽造 KRF を作成できる）と KRF 自体を送信しないで済ませる方法である。前者は送信者のみが不正を企図している場合に実行可能な攻撃（方式Ａに対し有効）であり、後者は送・受信者双方が不正を企図している場合に実行可能な攻撃（方式Ａ、方式Ｃに対し有効）である。但し、同無効化法が行われていることを法律執行機関は検出できる。

―― これらの攻撃法への対抗措置として、方式Ｂの Fair Public-Key Cryptosystems では真正な鍵が配送されていることを保証する一実現方式が示されている。しかしながら、同方式は処理に時間が掛かり過ぎ実用的ではない。

(ウ) Subliminal Channel Attack――方式Ｂの攻撃法

Subliminal Channel Attack とは、ユーザー側で鍵管理機関に登録した公開鍵セットとは異なる公開鍵セットを生成し、これを用いて暗号通信を行う攻撃である。特に、Micali の Fair Public-Key Cryptosystems の場合はユーザー側で鍵を生成する仕組みであるため同攻撃が容易に実行可能と思われる。Kilian & Leighton の Failsafe Key Escrow Approach は同攻撃を防止するため公開鍵セットをユーザー側と鍵管理機関側で半分ずつ生成し合成する仕組みとしているが、本質的な解決方法とはなっていないと考えられる。但し、こうした合法アクセス無効化法が行われていることを法律執行機関は検出できる。

(エ) Squeezing Attack―方式Ａの攻撃法

Squeezing Attack とは、他者の KRF を使用することにより他者に成りすます方法である（Frankel and Yung[16]）。Clipper Chip の場合、KRF を生成する際に送信者 a の IVa（Initialization Vector）を使って KRFa を作成する。暗号化モードでは、IV はその装置固有の IV に自動的に設定されるが、復号化モードの場合には、IV は手入力によって設定される。したがって、他者 b になりすまそうする暗号文送信者は、復号化モードにおいて他者の IVb を入力し、その IVb で KRFb を作成することができる。但し、同無効化法が行われていることを法律執行機関は検出できる。

―― 同攻撃法への対抗措置としては、(i)セッション鍵を送受信者の ID の関数とすること、すなわち ID に基づく鍵配送方式の利用や、(ii)セッション鍵を鍵管理機関のマスター鍵から算出可能なデータにより暗号化したデータを送信する方式が考えられる。

(オ) Spoofing Attacks―方式Ａ、方式Ｂの攻撃法

Spoofing Attacks とは、本人確認が未実現な通信システムにおいて成りすましにより他者の通信路を無断借用し鍵配送と暗号通信を実現する方法である（Frankel and Yung[16]）。この場合、真正なセッション鍵情報が含まれた KRF が送信されている訳であるが利用されている通信路の利用者は法律執行対象ではないため同 KRF が法律執行当局に盗聴されることはなく、従って検出もされない。

―― 同攻撃法に対抗するためには、ディジタル署名の導入により成りすましを不可能にすれば良い。

(カ) 合法アクセスより深い層での暗号通信

上記攻撃は、(オ)を除けば、何れも法律執行機関が合法アクセスを行おうとした時に暗号文の復号化自体はできないが、合法アクセス無効化法が講じられていることは検出可能である。本攻撃法は、こうした法律執行機関による検出自体も不可能にする方法である（松本・糸山[3]）。同攻撃法は大別して２種類ある。

・乱数部置換法
　キーリカバリープログラムを改造し、本来乱数を用いるべきところ（鍵等）を、一段深い層における暗号文で置き換えるという方法。

・多重暗号化法
　一段深い層における暗号文を合法アクセス対象メッセージに変換する方法。この場合、変換及び逆変換手続きは通信当事者間で秘密に共有されていなければならない。

両方法の具体的な実現例は以下の通り。

a.乱数部置換法

① 送信者は自分の装置或はソフトウェアを外部からセッション鍵或はメッセージ・パディング用のデータ等の乱数を入力できるように改造し、受信者は自分の装置或はソフトウェアを外部に上記乱数を出力できるように改造しておく。

② 送信者は真に送りたいメッセージ m'を予め受信者と示し合わせておいた何らかの方法で暗号化し、これを上記乱数とする。
③ 送信者は同乱数を改造された装置或はソフトウェアに入力し、受信者に送信する。
④ 受信者は改造された装置或はソフトウェアから同乱数を取出し、これを復号化して m'を得る。

b.多重暗号化

① まず、真に送りたいメッセージ m'を予め受信者と示し合わせておいた何らかの方法で暗号化し y を作る。
② y を「意味のある情報」m に翻訳する変換 T とその逆変換 T-1 を用意しておく。
③ Key Recovery 方式を用いて送信者から受信者に文書 m を送信する。
④ 受信者は上記逆変換 T-1 を用いて文書 m から y を復元する。
⑤ y を復号化して m'を取出す。

５．おわりに

２．および３．でみたように、欧米主要国の当局者の間では、キーリカバリー構想のための制度、システムを整備・構築しようという動きが急速に具体化しつつある。また、一部の暗号製品については、米国の輸出規制回避の観点から、既にキーリカバリー機能を組み込んだものが販売され普及しつつある。しかしながら、４．でみたとおり、キーリカバリー機能を実現するための技術は、最近急速に発展してきてはいるものの、現時点ではまだ完成したものとは言い難く、特に、合法的アクセスの回避策への対策や、具体的な実装技術とそのコスト等について、更なる研究が必要と言われている。

わが国では、これまで国家が暗号技術を管理する度合いが低く、暗号を巡るオープンな議論もあまり行われてこなかった。しかし、インターネットの普及や電子商取引の実現のために暗号技術の重要性が増してきているため、キーリカバリー構想を含め、暗号技術を巡る諸外国の動向にも注意を払っていくことが必要となっていると考えられる。

以　上

【参考文献】

[1] 辻井重男・石崎靖敏、「OECD 暗号政策ガイドラインとその背景」、 暗号と情報セキュリティシンポジウム、SCIS'97-1A、電子情報通信学会、1997 年 1 月 29 日.

[2] 古瀬幸広・廣瀬克哉、『インターネットが変える世界』、岩波新書、1996 年 2 月.

[3] 松本勉、糸山大志、「Lawful Access の無効化を狙う暗号通信の検出は容易か？」、電子情報通信学会技術研究報告 ISEC97-79、1997 年.

[4] 力武健次、『インターネットコミュニティ―国際ネットワーク最前線―』、オーム社、1994 年 11 月.

[5] Blaze, M., "Protocol Failure in the Escrowed Encryption Standard," *Proc. of The second ACM Conference on Computer and Communication Security*, pp. 59-67, ACM Inc., November 1994.

[6] Brickell, E. F., D. E. Denning, S. T. Kent, D. P. Maher, and W. Tuchman, "SKIPJACK Review: The SKIPJACK Algorithm," July 28, 1993.

[7] Bureau of Export Administration, Department of Commerce, "Department of Commerce Encryption Export Regulation," December 30, 1996.

[8] Center for Democracy and Technology, "CDT Cryptography Policy Issues Page," (URL: http://www.cdt.org /crypto/).

[9] Denning, D. E., "International Key Escrow Encryption: Proposed Objectives and Options," International Cryptography Institute 1994, August 2, 1994.

[10] Denning, D. E., and D. K. Branstad, "A Taxonomy for Key Escrow Encryption Systems, " *Communication of the ACM*, Vol. 39, No. 3, ACM Inc., March 1996.

[11] Denning, D. E., and M. Smid, "Key Escrowing Today," *IEEE Communications*, September 1994.

[12] Department of Trade and Industry, "Paper on Regulatory Intent Concerning Use of Encryption on Public Network," June 10, 1996.

[13] Department of Trade and Industry, "Licensing of Trusted Third Parties for the Provision of Encryption Services: Public Consultation Paper on Detailed Proposals for Legislation," March 21, 1997.

[14] Electronic Frontier Foundation, "Privacy, Security, Crypto, and Surveillance," (URL: http://www.eff.org /pub/Privacy/).

[15] Electronic Privacy Information Center, "Cryptography Policy," (URL: http://www.epic.org/ crypto/).

[16] Frankel, Y. and M. Yung, "Escrow Encryption Systems Visited: Attacks, Analysis and Designs," *Proc. CRYPTO '95, Lecture Note in Computer Science*, Vol. 963, pp. 222-235, Springer-Verlag, 1995.

[17] IBM Corp., "The need for a global cryptographic policy framework," October 1996.

[18] IBM Corp., "Key management framework and key recovery technology," IBM White Paper, February 1997.

[19] Kandau, S., S. Kent, C. Brooks, S. Charney, D. E. Denning, W. Diffie, A. Lauck, D. Miller, P. Neumann, and D. Sobel, "Crypto Policy Perspective," *Communications of the ACM*, Vol. 37, No. 8, pp. 115-121, ACM Inc., August 1994.

[20] Kilian, K., and T. Leighton, "Fair Cryptosystems, Revisited," *Proc. CRYPTO '95*, pp. 208-221, 1995, Springer-Verlag,.

[21] Kuner, C., "German ICC Draft Working Paper on Crypto Policy," (URL: http://ourworld.compuserve.com/homepages/chuner/icc01.htm#ICC Draft), March 3, 1997.

[22] Kuner, C., "Statements by German Business against Crypto Regulation," (URL: http://ourworld.compuserve.com/homepages/chuner/gmindst1.htm#gmindst), March 3, 1997.

[23] Laurie, B., "A Supplementary Analysis of the Royal Holloway TTP-based Key Escrow Scheme," (URL: http://www.algroup.co.uk/crypto/rh.html), November 16, 1996.

[24] Micali, S., "Fair Public-Key Cryptosystems, " *Technical Report 579*, MIT Lab. For Computer Science, August 1993.

[25] National Institute of Standards and Technology, "Escrowed Encryption Standard (EES)," Federal Information Processing Standards Publication (FIPS PUB) 185, 1994.

[26] National Institute of Standards and Technology, "Issues - Export of Software Key Escrowed Encryption," Discussion Paper #1, Key Escrow Issues Meeting, September 6, 1995.

[27] National Institute of Standards and Technology, "Discussion Issues: Desirable Characteristics for Key Escrow Agents," Discussion Paper #2, Key Escrow Issues Meeting, September 6, 1995.

[28] National Institute of Standards and Technology, "Export Criteria Discussion Draft - 64 bit Software Key Escrow Encryption," Discussion Paper #3, Key Escrow Issues Meeting, September 6, 1995.

[29] National Research Council, *Cryptography's Role in Securing the Information Society*, National Academy Press, Washington, D. C., May 30, 1996.

[30] National Semiconductor, "The National Fortezza Crypto Card," (URL: http://www.ipsecure.com/htm/fortezza.html), 1994.

[31] Office of Management and Budget, Executive Office of the President, " Enabling Privacy, Commerce, Security and Public Safety in the Global Information Infrastructure," May 17, 1996.

[32] Office of Technology Assessment, Congress of the United States, "Information Security and Privacy in Network Environments," U. S. Government Printing Office, September 1994.

[33] OECD, "Recommendation of the Council concerning Guidelines for Cryptography Policy," （URL: http://www.oecd.org/dsti/iccp/crypto_e.html）, March 27, 1997.

[34] Schneier, B., *E-MAIL SECURITY*, John Wiley & Sons, Inc., 1995.（Bruce Schneier 著、力武健次 監訳、道下宣博 訳、『E-Mail セキュリティ』、オーム社、1995 年 5 月.）

[35] Steptoe & Johnson LLP, "France's Proposed Statutory Trusted Third Party Rules for Encryption," (URL: http://www.steptoe.com/france.htm), 1996.

[36] Committee of Ministers, Council of Europe, "Recommendation No. R(95) 13 of the Committee of Ministers to Member States," September 11, 1995.

[37] Trusted Information Systems, Inc., "TIS announces encryption Key Recovery Technology – Technical Description," RSA Data Security Conference, San Francisco, California, January 18, 1996.

[38] Trusted Information Systems, Inc., "Exportable Strong Encryption: RecoverKey™ CSPs," (URL: http://www.tis.com/docs/products/recoverkey/rkey3.html), November 1996.

[39] VeriSign, Inc., *VeriSign™ CPS, VeriSign Certification Practice Statement Version 1.1*, 1996.（日本ベリサイン株式会社、『ベリサイン サーテイフィケーション プラクテイス ステートメント』、 1997 年 2 月 5 日.）