独立行政法人**情報処理推進機構**

〒113-6591
東京都文京区本駒込2-28-8　文京グリーンコートセンターオフィス16階
http://www.ipa.go.jp/

2011 情財第 0266 号

# 暗号鍵の適切な運用・管理に係る課題調査

# 調査報告書

**平成 25 年 2 月**

# 目　　次

# 1. はじめに

暗号鍵寄託（Key Escrow）・鍵回復（Key Recovery）政策は、米国クリントン政権が 1993 年に発表した Clipper 政策[1]に端を発する。当時、暗号技術は世界的にも軍事技術の範疇として扱われ、特に、1993 年 2 月に発生した世界貿易センター爆破事件を受け、テロ組織による暗号の利用を警戒する米国政府は、暗号技術の利用規制と輸出規制を暗号政策の両輪としていた。

一方、インターネットの一般利用が盛んになり始めた 1990 年代の産業界では、インターネットの商用利用に必要な安全策として暗号の利用が求められるようになるとともに、米国政府の打ち出した暗号鍵の強制的な寄託制度は個人のプライバシー保護に反するという人権擁護論者や、暗号鍵を集中管理することによりかえって危険性が増すという技術者などの反対意見が数多く出された。また、米国連邦議会においても共和党が Clipper 政策に対する反対法案を幾つか提出するとともに、連邦裁判所においても鍵寄託や暗号の輸出規制に対する違憲判決が出るなど、米国国内での Clipper 政策は 1995 年頃には行き詰まりの様相を呈した。

この状況を背景に、米国政府は、OECD などの国際機関に働きかけて、鍵寄託・鍵回復政策を国際的な枠組みの中で実現し、それによって米国国内においてもこの政策の実現を図ろうとした。この働きかけの一環として、米国政府は 1996 年から 1997 年にかけて、OECD 加盟各国に暗号特使を派遣し、鍵寄託・鍵回復政策への同調を依頼した。しかし、OECD においては、1997 年 3 月に「暗号政策ガイドライン」が勧告され、その中で米国が目指した政府による鍵寄託・鍵回復の強制は実現しなかった。更に、1998 年 12 月にワッセナー・アレンジメントにおいても鍵寄託・鍵回復政策は否定された。

他方、米国政府の暗号政策のもう一つの柱である輸出規制についても、1996 年 12 月に暗号技術が武器リストから商業統制リストでの扱いとなるとととともに、1997 年から 1999 年にかけて規制緩和が大幅に進んだ。

このような経緯から、2000 年の時点では、暗号利用規制や輸出規制は大幅に緩和され、鍵寄託・鍵回復政策自体も自然消滅の状況となり、国の安全保障政策の重点は、暗号規制対策から不正アクセス・サイバーテロ対策に移っていった。

一方、国が主導する鍵寄託・鍵回復政策とは別に、民間企業において暗号利用が盛んになるとともに、暗号鍵が紛失する「ロストキー」の問題も顕著になり、これに対する対策としての鍵回復システムの必要性は 1990 年代から指摘されていた。また、最近は、内部統制の観点から、第三者によるデジタル・フォレンジック実施の際にも鍵回復の必要性が新たに指摘されている。このように、民間部門における鍵回復システムの必要性は現代においても引き続き生きているといえる。

本調査は、米国や国際社会における鍵寄託・鍵回復に関する歴史的な動向を振り返るとともに、当時の日本政府の対応や、通産省・IPA が実施した鍵回復試作システムの内容を概観した上で、現代的な視点での鍵回復システムの必要性や課題などをまとめるものである。

尚、本調査にあたっては、中央大学の今井秀樹教授、辻井重男教授、東京電機大学の佐々木

[1] 暗号鍵を政府機関に登録（鍵寄託 Key Escrow）することを強制する米国政府の政策の総称。

良一教授、一般財団法人日本情報経済社会推進協会の木村道弘氏、東芝ソリューション株式会社の遠藤直樹氏、株式会社ＩＴ企画の才所敏明氏、日本電気株式会社の山崎正史氏、株式会社富士通研究所の鳥居直哉氏に対してインタビューを行い、ご協力をいただいた。ここに感謝の意を表する。

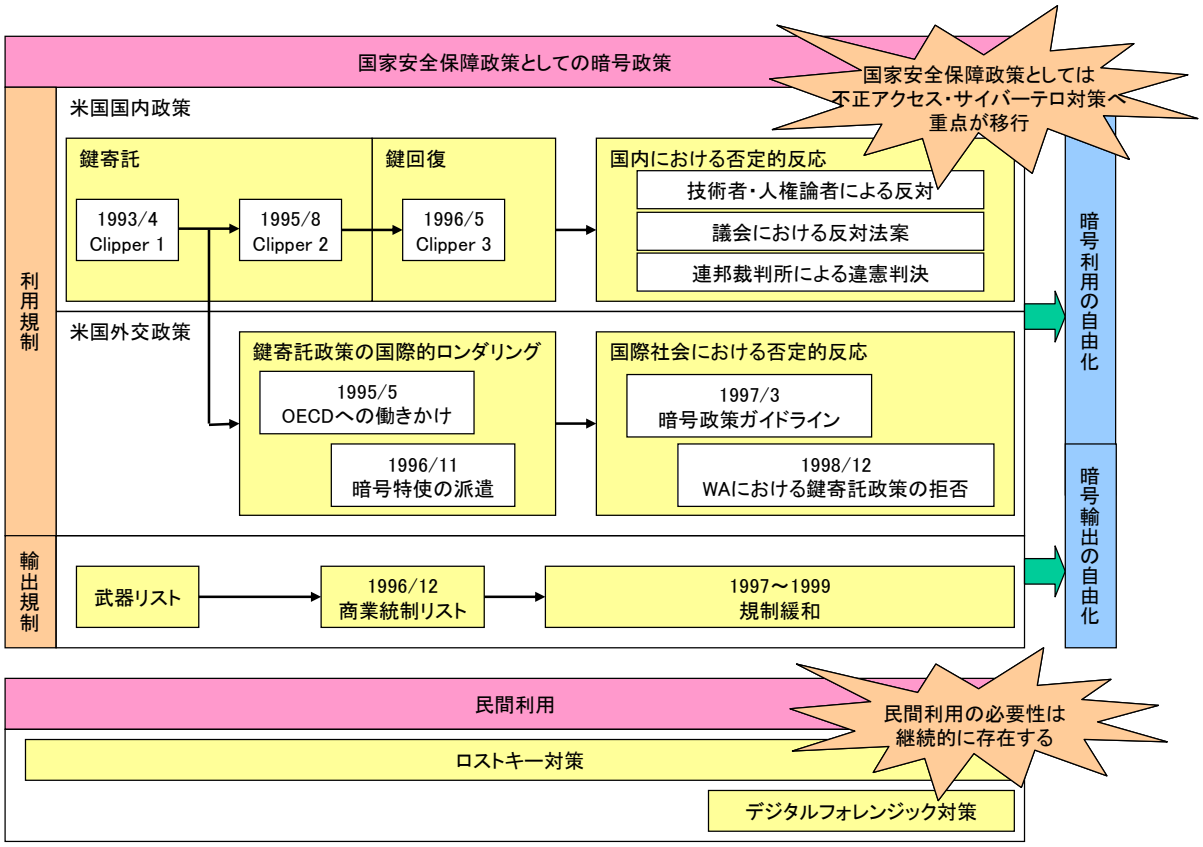


図１　鍵寄託・鍵回復政策の歴史的動向の概観

## 2. 米国の暗号政策

### 2.1 Clipper 政策以前

暗号技術は、世界的にみても、伝統的に軍事転用が可能な技術として、その利用や輸出にあたっては国が関与し、規制を加える対象と捉えられていた。米国においてもこの点は例外ではなく、暗号技術の標準策定と輸出にあたって国の関与は大きかった。[25]

#### (1)暗号技術の標準策定

1990 年代初頭において、米国における暗号技術は、NIST(National Institute of Standards and Technology)による米国連邦技術標準(FIPS:Federal Information Processing Standards)の認定を通じて、政府調達製品のみならず、民間における事実上の標準として利用されていた。例えば、共通鍵暗号アルゴリズムである DES は、商務省標準局（NBS：現在の NIST）が公募したプロジェクトに対して、IBM 社により開発され提案された暗号アルゴリズムである。IBM 社により提案された暗号アルゴリズムに対して、鍵長の変更、S-Box の入れ替えなどが行われ、1977 年に FIPS-46 として連邦政府機関が利用するべき暗号アルゴリズムとして制定されるとともに、民間においても幅広く活用され、事実上の国際標準として広く普及した。[7][16]

なお、DES に関しては、1984 年に ISO TC 97/SC 20（Data Cryptographic Techniques）で、DEA1 の名称で国際標準化が図られたが、IS 出版直前に米国より「暗号アルゴリズムの標準化は中止すべきである」とのコメントが寄せられ、実際の国際標準とはならなかった。[48]

#### (2)暗号技術の輸出規制

米国において、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、軍需リスト(United States Munitions List)が規定されている。他方、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、商業統制リスト(CCL:Commercial Control List)が規定されている。

このような中、暗号を利用した装置は軍事目的の技術・装置に該当するとされ、海外に輸出するためには国務省による個別審査が必要とされた。[25]

この当時の米国の暗号政策は、暗号技術の標準を国が規制することによる暗号の利用規制と暗号技術の輸出規制が車の両輪として機能していた。

### 2.2 Clipper 政策

1993 年 2 月に発生した世界貿易センター爆破事件は、テロ組織に対する米国政府の安全保障政策を見直すきっかけとなり、暗号政策についても、テロ組織が暗号を利用することに対する警戒感が強まった。そのような背景のもとで、暗号を利用するにあたりその鍵を政府の機関に登録（鍵寄託 Key Escrow）することを強制する Clipper 政策が打ち出された。

1993 年に Clipper 政策の第 1 弾（Clipper 1）が打ち出された後、米国国内の世論などの反応を踏まえて、その内容を見直した政策として、1995 年に第 2 弾（Clipper 2）、1996 年

に第 3 弾（Clipper 3）が打ち出され、この段階で鍵寄託ではなく鍵回復(Key Recovery)という用語が使われるようになった。

そのような中で、民間企業では、鍵回復システム開発のビジネスおよび技術面での検討を進める動きも見られ、キー・リカバリー・アライアンス(Key Recovery Alliance)などの国際的な組織も生まれた。

その一方で、暗号の自由な利用や輸出の自由化を求める産業界や人権擁護団体の意見も根強くあり、Clipper 政策の実現は困難を極めた。[2][3][6][7][14][15][19][20][21][37]

### (1)Clipper 1

Clipper 1 はクリントン政権により 1993 年 4 月に発表された Clipper 政策の第 1 弾で、アルゴリズム非公開（classified algorithm）の鍵長 80 ビットの共通鍵暗号 SKIPJACK[3] を組み込んだ Clipper Chip を通信端末に設置することを、政府・民間を問わず、暗号利用の条件とする米国政府の構想である。なお、当初はアルゴリズム非公開であった SKIPJACK の仕様は、1998 年 5 月に NIST から公開された。[50]

Clipper 1 の特徴や Clipper 1 をめぐる主な動きは、次の通りである。

- 暗号鍵を二つに分けて財務省と NIST が持ち、裁判所の令状により暗号解読が可能となっている。
- 1994 年 2 月、Clipper 1 のコンセプトが EES(Escrowed Encryption Standard)として FIPS に認定された。[14][49]
- 1994 年 10 月、米国政府は Clipper 1 構想を実現するための通信会社の設備改造に補助金を交付することを発表した。これを受けて AT&T は、この補助金を利用して、Clipper 1 を実装した電話機を開発した。

初期の EES に対する弱点として、法執行機関による合法的アクセスを忌避する手法が論文として公表され、それに対する対応策も公表されるという事例が頻発した。[15][19][21]

また、Clipper Chip に対する疑問が数多く出された。例えば、米国製品以外にも盗聴機能を有しない製品が出回っているため、テロリストが敢えて Clipper Chip を利用するはずがない、鍵寄託機関の権限の乱用や捜査当局による適正な運用が確保されるか等、数多くの疑問が提示された。[6]

### (2)Clipper 2

Clipper 2 は Clipper 1 に対する批判を踏まえ、1995 年 8 月に発表された暗号技術規制の緩和策である。尚、Clipper 2 という名称自体は米国政府の付けた正式な名称ではなく、EFF(Electronic Frontier Foundation)などの米国暗号政策ウォッチャーが名づけたものである。[25]

Clipper 2 の特徴は、①鍵寄託を前提として DES を使用した製品の輸出規制を緩和、②鍵寄託機関として民間機関も利用可能としたものである。

この構想に対しては、

- 鍵を寄託する民間機関の資格要件や寄託の方法が不明確

・輸出できる暗号強度に上限を設けることに対する産業界の反発

などの理由から、実施には至らなかった。[2]

### (3)Clipper 3

Clipper 政策が手詰まり感を深める中、米国政府は 1996 年 5 月にいわゆる Clipper 3 政策を発表した。この政策の特徴は、①公開鍵方式による暗号鍵管理インフラ（KMI:Key Management Infrastructure）の構築、②利用者が認証機関(CA)を利用するには、利用者の秘密鍵を鍵寄託機関へ寄託することが条件、③寄託された秘密鍵は、司法の要請により法執行機関に開示されて鍵回復に利用、④外国での法の執行手段を維持するための鍵寄託に関する政府間協定の締結、といった点である。この中で、寄託された秘密鍵は利用者の要請により鍵回復(Key Recovery)に利用される、とされ、評判の悪い鍵寄託という用語に代わって鍵回復という用語が使われ始めた。[2][25]

また、米国政府は、鍵回復政策と合わせて、暗号製品の輸出規制の緩和策も打ち出している。（暗号輸出の緩和策については後述する。）

しかし、Clipper 3 政策に対する批判も多く、鍵回復によるリスクとして、①鍵回復機能の不具合により情報の保全性自体が危うくなる可能性、②鍵回復機能自体が暗号機能に比べてはるかに複雑、③企画・施行・運用すべてにわたり膨大な費用の発生、④鍵寄託先の信頼性、⑤鍵寄託先の集合的な鍵管理に対する外部からの攻撃等、数多くの指摘がなされた。[6][8][17]

### (4)キー・リカバリー・アライアンス

Clipper 3 政策の発表を受け、鍵回復技術の開発を目指し、IBM、Apple、Atalla、Digital Equipment、Groupe Bull、Hewlett-Packard、NCR、RSA、Sun Microsystems、TIS、UPS の民間企業 11 社による Key Recovery Alliance (KRA)という企業連合が 1996 年 10 月に発足し、1997 年 5 月時点では加盟企業 70 社以上の国際的な連合に発展した。[2]

日本からも、日立、NEC、富士通、東芝、三菱商事、三菱電機、NTT ソフトウェアなどの企業が参加した。

---

[2] 1997 年 5 月時点での加盟企業は次のとおり。America OnLine, American Express, Apple Computer, Atalla, Baltimore Technologies, Boeing, Candle Corporation, CertCo, Certicom, Compaq Computer, Compatible systems, Cryptomathic, CygnaCom Solutions, Cylink, DASCOM, Data Securities International, Deere & Company, Digital Equipment, Digital Signature trust, Entrust Technologies, First Data, Fort Knox Escrow Services, Fortress Technologies, Frontier Technologies, Fujitsu, GemPlus, Gradient technologies, Groupe Bull, Hewlett-Packard, Hitachi, IBM, ICL, Intel, IRE, Mitsubishi Corp. of Japan, Mitsubishi Electric America, Motorola, Mykotronx, Mytec Technologies, NCC Escrow, nCipher, NCR, NEC, Network Systems Group of StorageTek, Novell, NTT Software, Open Horizon, Portland Software, Price Waterhouse, Racal Data Group, Rainbow Technologies, RedCreek Communications, RPK, RSA, SafeNet Trusted Services, Santa Cruz Operation, Secant Network Technologies, Secure Computing Corporation, Siemens AG, Silicon Graphics, SourceFile, Spyrus, Sterling Commerce, Sun Microsystems, Tandem, Technical Communications, Toshiba, Trusted Information Systems, Unisys, UPS, Utimaco Safeware AG, VeriSign, VPNet Technologies

KRA は、

①国際的な電子商取引の活性化

②世界規模での市場主導かつ相互運用可能な鍵回復ソリューションの実装・展開・利用

③鍵回復技術のための商用基盤のビジネス及び技術面での要件の明確化

④暗号化情報の回復を支援する世界規模のインフラ開発への投資

などを目的として、3 ヶ月に一度の国際会議を開催するとともに、ビジネスシナリオ委員会、技術委員会、普及委員会、公的課題委員会、広報委員会の 5 つの委員会を組織して活動を展開した。

しかし、1999 年頃に Clipper 政策が衰退するとともに、活動は自然消滅した。

### (5) 鍵回復システムの実装例

#### (a)鍵回復システム製品[25]

この頃、Lotus 社、Trusted Information systems(TIS)社、IBM 社などが、鍵回復システム製品を発表している。

Lotus 社は Lotus Notes Release 4 において暗号技術を採用し、輸出版（International Edition）において、鍵回復技術を採用することにより輸出を可能とした。

TIS 社は RecoverKey という鍵寄託機能を有する製品を発表し、データ回復機関（Data Recovery Center）と呼ばれる鍵寄託機関と認証機関の両者の役割を果たす機関を利用する仕組みを提案した。

IBM 社は SecureWay Key Recovery Technology を発表し、暗号文を復号するための情報を Key Recovery Service Provider(KRSP)に保管する仕組みを提案した。

これらの製品では、一般的に、データの暗号化に利用した共通鍵を回復するための情報 KRF (Key Recovery Field)をデータ中に埋め込む方式が取られていた。

#### (b)合法的アクセスの無効化方法[25]

主な鍵回復方式に対して、その合法的アクセスを無効にする方法が公表されている。例えば、鍵回復の暗号アルゴリズム以外の暗号アルゴリズムを利用する、真正な KRF をデータに埋め込まない、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利用する、他者の KRF を使用して他者になりすます、などの合法的アクセスを無効化する方策が示されている。

### (6) Clipper 政策に対する米国内の反応

Clipper 政策に対する米国内の反応は、一般的には厳しいものであった。

ここでは、連邦議会、司法判断、民間の意見を紹介する。

#### (a)連邦議会の反応[2][5][6][37][41]

民主党のクリントン政権が打ち出した Clipper 政策に対し、共和党からそれに反対する法案が複数提出された。

例えば、1996 年には、共和党 Burns 上院議員が暗号の使用や販売の自由を保証し、暗

号規制の緩和を求める Pro-CODE（Promotion of Commerce Online in the Digital Era）法案を提出している。また、同じく 1996 年には、共和党 Goodlatte 下院議員が、暗号の使用と市場で一般的に入手可能な暗号製品の輸出の自由化、強制的な鍵の寄託の禁止を求めた SAFE 法案(The Security and Freedom Through Encryption Act)を提出している。これらの法案は、その後何度か再提出され、政府による鍵寄託・鍵回復の強制の禁止を盛り込んだ内容に変わってくる。

これらの法案の審議の過程でも、例えば、1996 年 6 月の上院商業委員会での Pro-CODE 法案に関する公聴会では、暗号の輸出規制や Clipper という規制では民間への対応は難しいことを議員が認識したとされている。[41]

(b)司法判断[37]

Clipper 政策や輸出規制に対する司法判断も幾つか出された。

例えば、1996 年 4 月、連邦裁判所は、D.J.Bernstein の暗号アルゴリズム Snuffle に対し、憲法修正第 1 条で保護される言論であると認定、同年 12 月には暗号輸出規制は違憲と決定した。更に、1997 年 8 月、商業統制リストによる規制も違憲との判決が出された。

(c)民間の意見[8][17][37]

Clipper 政策に対しては、政策公表の当初から、EFF(Electronic Frontier Foundation)、CDT(Center for Democracy and Technology)、EPIC(Electronic Privacy Information Center)などの技術者団体や人権擁護の非営利団体が反対意見を表明している。

Clipper 1 当時は、法執行機関による個人のプライバシーの侵害、採用される技術が非公開であることによる強度評価の困難さ、暗号政策の不透明さ、特定のメーカーが Chip 製造を独占していること等が批判の根拠として挙げられた。

また、Clipper 3 に対しても、EFF、CDT、EPIC は公開鍵インフラの整備と暗号鍵寄託をセットにしていることを批判した。

更に、米国研究評議会(NRC: National Research Council)は、1996 年 5 月、「情報社会の安全確保における暗号の役割(Cryptography's Role in Securing the Information Society(CRISIS))」を発表し、米国内での暗号の自由な使用と輸出規制の緩和を勧告した。

## 2.3 米国の対外政策と暗号輸出規制の緩和

国内での Clipper 政策の手詰まり感もあり、米国政府は、鍵寄託・鍵回復政策を国際的に認知させ、国際協調の枠組みの中で国内にも鍵寄託・鍵回復政策を普及させることができないかということを試み、OECD への働きかけや OECD 加盟諸国への暗号特使の派遣などを行ったが、大きな成果を挙げることはできなかった。

また、Clipper 政策とともに暗号政策の車の両輪の一つである暗号輸出規制は、国内世論の反発を受けて、徐々に緩和せざるを得なくなった。

### (1)OECD への働きかけと暗号政策ガイドラインの策定

米国は 1995 年に OECD に働きかけて暗号政策ガイドラインの策定を提案し、その中で、

鍵寄託制度の強制化を図ろうとした。[39][40][H6]

1995 年 12 月、パリにおいて暗号政策専門家アドホック会合が開催され、あわせて産業界との合同シンポジウムが開催された。日本からは、郵政省、通産省、警察庁などの省庁の代表、有識者、産業界代表の大派遣団が出席した。

1996 年には本格的な検討が開始され、米国は、司法省、FBI、NSA からなる派遣団を組織し、ロビー活動を展開した。後の暗号特使となる D. Aaron も参加していた。

このとき、米国が提案した鍵寄託政策に対して、フランスとイギリスは賛成の立場をとる一方で、カナダ、スペインは強く反対の立場をとり、ドイツ、オーストラリアなども反対の立場をとった。北欧諸国は鍵寄託が暗号に対する信頼を蝕む懸念を表明し、産業界代表はシステムを自由に選択する権利を望んだ。[40]日本では、警察庁が鍵寄託政策の推進に賛成の立場であったが、郵政省および通産省は慎重な立場をとった。[H5][H6]

1996 年に計 4 回の専門家グループの会合が持たれ、暗号政策ガイドラインの正式な勧告は 1997 年 3 月に出された。

暗号政策ガイドライン策定の過程において、議論のほとんどは、第 5 項「プライバシーと個人データの保護」と第 6 項「合法的アクセス」の部分に費やされた。[H6] 特に、第 6 項冒頭の「国の暗号政策は合法的アクセスを認めるべき（should allow)」とするか「認めてもよい（may allow)」とするかの大議論があり、最終的には may allow でまとまった。米国は、鍵寄託・鍵回復政策に結びつく should allow を希望したが、それは叶わなかった。

### (2) 暗号特使の派遣

米国政府は、OECD への働きかけを進める一方、鍵寄託・鍵回復政策への理解を求めるために、OECD 加盟諸国への特使を派遣した。この特使は暗号特使（Special Envoy for Cryptography）と呼ばれ、1996 年 11 月に D.Aaron が指名された。[6][46][47]

Aaron 特使は、1996 年 11 月から 1997 年 2 月にかけて、フランス、イギリス、ドイツ、ベルギー、カナダ、オーストラリア、日本等の OECD 加盟諸国を歴訪し、鍵寄託・鍵回復政策への支持を依頼した。

日本における D. Aaron 暗号特使との会合は、1997 年 2 月に政府機関との会合と有識者及び企業との会合が開催された。政府機関との会合としては、関係する郵政省、通産省、警察庁などの省庁を個別に訪問している。また、政府機関との会合の翌日には、米国大使公邸で有識者及び企業との会合が、1 時間程度行われた。米国大使公邸で開催された会合における日本側の出席者は、辻井重男教授、今井秀樹教授、NTT、東芝、日立、NEC、富士通、三菱電機の企業代表であった。

この会合において、Aaron 特使は鍵寄託・鍵回復の米国暗号政策を説明し、それに対する支持を訴えたが、その場では大した議論はなかった模様である。[H5][H6]

### (3) 米国の暗号輸出規制緩和

2.1 でも述べたように、Clipper 1 発表当時の米国の暗号政策は、暗号利用の制限と輸出

の制限を車の両輪としていたが、2.2 に示したような国内世論の反発から、暗号輸出の規制も徐々に緩和していった。[2][6][25][37][40]

まず、1996 年 10 月には、鍵回復システムの開発を条件に 1997 年 1 月から 2 年間を目途に暗号製品の輸出規制を緩和する方針（鍵回復イニシアチブ）が発表された。

更に、1996 年 11 月には暗号製品の輸出管理の管轄が国務省から商務省に移管され、同年 12 月には暗号製品を武器リストから商業統制リスト（CCL: Commercial Control List）へ移管すること、暗号化技術の国外輸出の段階的な解禁、暗号強度を 40 ビットから 56 ビットに拡大することが発表された。但し、この時点ではまだ鍵回復システムの採用が輸出の条件とされていた。

その後、1997 年 5 月には、金融取引にかかる使用目的のために特に設計された暗号製品については輸出を許可することが発表され、1998 年 9 月には 45 カ国の特定国向けの金融、保健・医療、社内内部情報の保護目的関連の輸出規制緩和が発表された。ここで、米国企業の本社・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無関係に輸出を許可することとされ、更に、DES 及び同等機能の暗号については一回の審査で輸出が可能となり、鍵回復計画書や途中経過の報告義務の提出要件も撤廃され、実質的に簡素化された鍵回復政策に移行した。

更に、1999 年 9 月には 45 カ国の輸出国リストが廃止され、テロ支援国 7 カ国以外の全地域に対し、技術審査及び分類の後に、他国政府ユーザ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。

これらの過程を経て、2000 年時点では、インターネットの普及と電子商取引の活発化に伴い、米国も含めた多くの国で暗号の規制は緩和された。[40]

## 3. 米国以外の国および国際機関の動き

### 3.1 欧州諸国の動き

#### (1) EU

EU においては、個人データ保護の重要性を早くから認識していた。EU 域外国への個人データ移転を規制し、個人データ保護が十分な第三国に限り個人データの移動を認める「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 1998 年 10 月 25 日に発効した。これにより、EU 加盟国の個人データ保護政策を調和させ、EU 域内における個人データの自由移動を確保することを狙いとし、結果として消費者の信頼の醸成、電子商取引の発展を見込んでいた。

同指令において、データ処理の安全確保についても規定しており、特にネットワーク上のデータ伝送を含みデータ保護措置を実施しなければならないとされ、データ保護の手段としての暗号利用の重要性が認識されていた。

暗号の輸出管理は、1994 年 12 月の EU 理事会において、汎用品輸出管理規則により管理対象とされ、2000 年 9 月時点でも暗号の管理は引き継がれているが、EU 域内については、2000 年末のワッセナー・アレンジメントの大幅な暗号管理水準緩和の決定を受けて緩和された。[6]

#### (2) フランス

フランスは EU 諸国の中でも暗号規制を厳しく行う国であり、1990 年 12 月の電気通信規制法において暗号の使用を規制したが、1990 年代項後半からは暗号政策の規制緩和を進めていた。

その一方で、1996 年 7 月の電気通信規正法の一部改正において、「情報の秘匿を目的とする暗号装置を利用する場合は、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」「暗号通信サービスを提供する事業者は、法律執行の枠組みに基づき、管理する秘密鍵を法執行機関に提出すること」が義務付けられた。更に、1998 年 3 月には「鍵寄託機関に暗号鍵を寄託したユーザは、それらの鍵で暗号スキームを自由に使うことが可能になること」「鍵寄託機関はある特定の状況下で法執行機関に鍵を渡すように要求されること」等を決めた法令が施行された。

しかし、1999 年 1 月に Jospin 首相は、国内の暗号利用の自由化を発表し、鍵寄託機関への義務的な鍵寄託を廃止する一方、法執行機関の要求に応じて暗号化文書の平文を司法局に提出するように要求できる仕組みを法制化する方針が示され、1999 年 3 月に法令として施行された。[5]

#### (3) イギリス

イギリスはフランス同様に暗号規制を行っていた。

1985 年に通信傍受法が制定され、国家安全保障や重大犯罪の予防・捜査における通信傍受について規定された。

暗号政策としては、1996 年 6 月、貿易産業省（DTI）が調査報告書を公表し、公衆ネットワーク上での暗号の使用に関する規制を発表し、鍵寄託に関しても、Trusted Third

Party(TTP)という考え方を示した。これを受けた政策として、1997 年 3 月に TTP の免許制が発表されたが、1998 年 4 月に発表された政策では、「TPP の認可は随意」「CA と鍵寄託機関は区別する」こととなった。更に、1999 年 3 月の DTI の報告書「電子商取引における信頼性の確立」という報告書では、「鍵寄託と鍵回復の使用は推奨されるが、強制されることはない」とされ、同年 7 月の電子商取引促進法案においては、TPP に対する暗号鍵保管の義務付けは見送られ、法執行機関に対する暗号鍵使用の権限が与えられた。[5]

### (4) ドイツ

ドイツでは、1996 年 12 月に電子署名法が制定され、その第 12 条において「法執行機関は必要に応じて認証機関の管理する個人情報が入手できる」という合法的アクセスの項目が明記された。[5]

他方、暗号政策に関しては、暗号の民間利用を促進しようという方針で政策を進めており、OECD における米国の鍵寄託・鍵回復政策に対しても反対を唱えた。[39]

1996 年 6 月には、連邦議会で、通信の秘密の憲法上の権利の範囲内で暗号の使用を自由に選択できる旨の決議が行われた。[37]

また、1998 年にドイツ議会の調査委員会で「利用者が自分を暗号によって守ることを法によって規制すべきでなく、このような技術の自由な使用を禁止すべきではない」という勧告を出した。[5]

## 3.2 OECD の動き

2.3(1)に記したとおり、米国は OECD に対して暗号政策ガイドラインの策定を働きかけ、その中で、鍵寄託制度の強制化を図ろうとした。[39][40][H6]

1995 年 12 月にパリにおいて暗号政策専門家アドホック会合と産業界との合同シンポジウムが開催された。本格的な検討は 1996 年に開始され、OECD は伝統的な 2 年間をかけたコンセンサスをとる手法を改め、コアグループにより 1 年間で決着を図ることとした。1996 年に計 4 回の専門家グループの会合が持たれ、暗号政策ガイドラインの正式な勧告は 1997 年 3 月に出された。

暗号政策ガイドラインでは、策定の背景を次のように述べている。[11][40]

- 世界規模の情報通信ネットワーク技術が進み、これらのシステムで伝送・蓄積されるデータの効果的な保護に対する要求が高まっている。暗号技術はデータセキュリティシステムにおける基本ツールであり、データの信頼性と整合性を確保し、電子商取引における認証と否認防止機構を提供する。
- 各国政府は、データ保全と商用アプリケーションのために暗号の利用を奨励するが、一方で、プライバシー、合法的アクセス、国家安全保障、技術や商業の発展などの様々な利益バランスをとる必要がある。本質的に国際的な性質を持つ情報通信ネットワークと新たな地球環境で法的な境界を定めることの難しさのため、国際的な協力により暗号政策を進めていかなければならない。
- ガイドラインは様々な商用アプリケーションを通して、電子商取引を発展させ、ネ

ットワークの信頼性を支え、データの安全性とプライバシーの保護を提供するために、暗号の利用を推進することを目指した。

・ いくつかの OECD 加盟国では既に暗号についての政策と法を整備しているが、多くの国ではまだその途上にある。これら国家政策の国際レベルでの協調に失敗すれば、地球規模の情報通信ネットワークの進化の障害を導き、国際貿易を阻害することになる。OECD 加盟諸国は国際協力の重要性を認識し、暗号やより広範な情報通信ネットワーク技術に係わる政策や規制の問題についてのコンセンサスを得ることに寄与してきた。

このような認識のもと、ガイドラインは次の 8 原則からなる。[11][36][37][40]

① 暗号手法に対する信頼

暗号手法は、情報通信システムの利用に対する信頼感を醸成するため、信頼に足るものであるべきである。

② 暗号手法の選択

ユーザは、適用される法に従い、いかなる暗号手法をも選択する権利を持つべきである。

③ 市場主導の暗号手法の開発

暗号手法は、個人、ビジネス及び政府の必要性、需要及び責任に対応して開発されるべきである。

④ 暗号手法に関する諸標準

暗号手法に関する技術的諸標準、諸基準及びプロトコルは、国内及び国際レベルで開発され、また、公表されるべきである。

⑤ プライバシー及び個人データの保護

通信の秘密及び個人データの保護を含むプライバシーに関する個人の基本的権利は、各国の暗号政策、暗号手法の実施及び利用に当って尊重されるべきである。

⑥ 合法的アクセス

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なアクセスを認めることができる。これらの政策は、最大限可能な範囲で、このガイドラインにある他の原則を尊重しなければならない。

⑦ 責任

暗号サービスを提供し又は暗号鍵を保持し若しくはアクセスする個人又は主体の責任は、契約又は立法のいずれかによって確立された場合であっても、明確に記述されるべきである。

⑧ 国際協力

各国政府は、暗号政策を調整するために協力すべきである。かかる努力の一環として、政府は正当化されない貿易障壁を除去し、又は暗号政策の名の下にそれを創出することを回避すべきである。

### 3.3 G8 の動き

G8 は 1975 年より毎年開催され、主要国のリーダが集まって諸問題を議論しており、暗号政策についても米国の強い提言により議論のテーマの一つとなっていた。[40]

1996 年のリヨンサミット（米国、イギリス、フランス、ドイツ、カナダ、イタリア、日本、ロシアが参加）において、「合法的な通信のプライバシーを保護しながら、必要に応じて、テロ行為の防止または捜査の目的で、データまたは通信に対する政府機関による合法的アクセスを認める暗号の使用に関して、二国間または多国間の協議を促進する」旨の決議がされた。[37][40]

更に、1997 年 6 月のデンバーサミットにおいて、OECD の暗号政策ガイドラインに沿って、暗号鍵管理や合法的な政府機関によるアクセスを規定した暗号政策を、各国が策定することを加速するとともに、これらの政策の国際協調の必要性が強調された。[40]

しかし、1998 年 5 月のバーミンガムサミットにおいては、暗号自体には特に触れず、適切なプライバシー保護を行いつつ、犯罪の証拠としての電子データの取得、提示、保護についての法的枠組みを作ることについて、産業界と緊密に協力していくことを呼びかけた。更に、これらが、インターネットを含む新しい技術の悪用による広範囲な犯罪との闘いに役立つことが強調された。[40]

この頃には、国際的には、暗号を規制することよりは、インターネット犯罪などの防止策に重心が移っていったとみられる。

### 3.4 ワッセナー・アレンジメントの動き

冷戦時代に、共産主義諸国に対する軍事目的の技術・装置や軍事目的に転用可能（dual use）な技術・装置の輸出を規制するための多国間協議を行っていた COCOM (Coordinate Committee on Multilateral Export Controls)は、冷戦の終結に伴い、1993 年の 11 月に終了した。その後、新たな枠組みとして、1995 年 12 月にワッセナー・アレンジメント（Wassenaar Arrangement。以後、WA）が成立し、現在 40 カ国が参加している。

WA では、規制対象国は明文化されておらず、罰則規定もない。輸出規制の目標となる WA 規制リストを定め、各国はこれを基に自国の規制リストを定めており、このリストは定期的に見直されている。

暗号技術は、軍事目的に転用可能な技術・装置として規制リスト（Dual-Use Control List）に掲載されているが、1998 年 12 月にこの見直しがなされ、一定強度の暗号の輸出規制緩和がなされた。共通鍵暗号に対しては、鍵長が 56 ビットを超えるハード／ソフト暗号製品（これには Web ブラウザー、e-mail アプリ、電子商取引サーバ、電話スクランブル装置等も含む）がリストに加えられた。また、これ以外の大量販売商品（PC の OS、ワープロ、データベース等）は 64 ビットを超える製品が 2 年間の期限付きでリストに加わった。尚、公開鍵暗号方式では、RSA 暗号のような素因数分解問題を安全性の根拠とする場合は 512 ビット、楕円曲線上の離散対数問題に安全性の根拠を置く楕円曲線暗号の場合は 112 ビットが閾値である。[24]

一方、DVD 等の知財関係の暗号製品はリスト対象外となった。更に、インターネットからダウンロードされる無形配布のソフトウェアも対象外となった。[40]

この合意で，56 ビット以下の共通鍵暗号，512 ビット以下の RSA 暗号，112 ビット以下の楕円曲線暗号の 3 種類の製品や技術については輸出審査を不要とし，自由に輸出できるようになった。また、日本においては、DVD 等の知財関係の暗号製品やインターネットからダウンロードされる無形配布のソフトウェアも規制対象外となった。

更に、1998 年 12 月の会合において、暗号鍵の寄託の強制は完全に否定された。[40]

## 3.5 ISO の動き

### (1)暗号の標準化

1997 年 3 月の暗号政策ガイドライン及びワッセナー・アレンジメントにおける暗号利用の見直しを契機として、ISO JTC1/SC27 において暗号アルゴリズム標準化が着手された。[39]

1997 年には楕円曲線ベース暗号の標準化に着手し始めた。更に、一般的な暗号標準として、４つのパートからなる ISO/IEC 18033 が作成され、2005 年から順次発行された。

### (2) 鍵管理に関する標準

ISO における暗号鍵に関連する標準化は、TC68（金融サービス）と ISO/IEC JTC1 SC27（情報セキュリティ）で標準化が行われている。それぞれの委員会で審議された標準には以下のようなものがあるが、鍵寄託・鍵回復に関する標準化は行われていない。

[ISO TC68/SC2 金融サービス　セキュリティ]

- ISO 13491：Banking-Secure cryptographic devices(retail) Part 1:Concepts, requirements and evaluation methods
- ISO 11568-1: Banking-Key management (retail)-Part1: Part1: Principles
- ISO 11568-2: Banking-Key management (retail)-Part2: Symmetric ciphers
- ISO 11568-4: Banking-Key Management (retail) -Part4:Asymmetric cryptosystem-Key management and life cycle

[ISO/IEC JTC1 SC27/WG2 情報セキュリティ　暗号とセキュリティメカニズム]

- ISO/IEC 11770-1 Key management - Part 1: Framework
- ISO/IEC 11770-2 Key management - Part 2: Mechanisms using symmetric techniques
- ISO/IEC 11770-3 Key management - Part 3: Mechanisms using asymmetric techniques
- ISO/IEC 11770-4 Key management - Part 4: Mechanisms based on weak secrets
- ISO/IEC 11770-5 Key management - Part 5: Group key management

## 4. 鍵寄託・鍵回復システムの民間利用

### 4.1 民間企業における鍵回復機能の必要性

これまで述べてきた鍵寄託政策は、基本的には利用者が暗号鍵を第三者機関に寄託し、法執行機関が何らかの条件のもとにその暗号鍵を入手して犯罪捜査等に利用できる制度であったが、Clipper3 の時点からは鍵紛失時の対応面を重視した「鍵回復」という名称に変えている。しかし、国が主導する「鍵寄託」の一面は否定できない。

他方、民間部門では、本来の意味での鍵紛失時対策として、鍵回復システムの必要性が認識されていた。民間企業における鍵回復機能の必要性については、1999 年当時のアンケート調査結果が報告されている。[9]

その結果によれば、調査した 363 社中、鍵回復機能を必要とする企業が 164 社（45.2%）、必要としない企業が 43 社（11.8%）、わからないとする企業が 151 社（41.6%）となっている。

また、鍵回復機能が必要とした 164 社中、「社員が急に退職・死亡したとき」が 105 社（64.0%）、「鍵を消失してしまったとき」が 104 社（63.4%）、「不正利用が行われたときにチェックするため」が 89 社（54.3%）、「情報の内容に問題がないかどうかを常にチェックするため」が 48 社（29.3%）等となっている。

これらの結果から、この当時から民間企業におけるロストキー対策や不正利用チェック（現代的な視点でのデジタル・フォレンジック対策）としての鍵回復機能の必要性は認識されていた。

### 4.2 鍵回復制御

暗号学者の B.Gladman は 1997 年の論文において、国が主導して進める法執行機関による合法的アクセス手段としての鍵回復と、民間のロストキー対策として利用する鍵回復を、蓄積データに関するものと通信に関するものに整理した上で、鍵回復は基本的には政府ではなく、企業を含めた民間に任せるべきと主張した。[22]

また、利用者が制御する鍵回復を

> 鍵回復は、情報の保護に使われる暗号鍵を一次手段(primary means)で得ることができない場合に、これらの鍵を復元する能力である。利用者が制御する鍵回復は、守るべきデータの所有者が暗号による保護力を変えることなくそれを使うか否かを選ぶことができるような形式でその能力を記述する。

と定義した上で、鍵回復の制御は、国でもなく、ましてやエンドユーザでもなく、データ所有者が行うべきとし、企業の現場においては企業側の判断で行い、個人の私人においては本人が判断すべき、としている。

更に、Gladman は、この定義に従った利用者が制御する鍵回復システム製品は、企業で利用されるコーポレート鍵回復（CKR）と個人ユースであるパーソナル鍵回復（PKR）の 2 種類に区分けされ、CKR と PKR が相互運用できることが必要とした。即ち、

- 企業と個人の両者は、データ交換の際に、互いに影響を与えることなく、鍵回復機能

を使うか否かが選べる

- 鍵回復機能を使うか否かの選択は、データ交換で可能な暗号による情報保護力や両者の暗号化／復号の能力にいかなる形によっても影響を与えない

という条件を満たすべきとした。

この当時の製品では、このような条件を満たすようなものはなく、強力な暗号化機能を持ち鍵寄託機能のオン／オフができる国内向け製品と、強力な暗号化機能を持たない海外向け製品しかないとしている。

# 5. 日本の暗号政策と鍵寄託・鍵回復システムへの対応

## 5.1 日本の暗号政策

### (1) 暗号特使派遣当時の日本の暗号政策

暗号特使が派遣された 1997 年当時は、日本において特段の暗号政策や不正アクセスを取り締まる法制度もなかった。

警察庁はこのような事態に危機感を持ち、犯罪等防止のための情報セキュリティビジョンの策定が急務であり、特に、国際的な整合性に配慮した暗号政策、情報セキュリティ施策の策定が喫緊の課題であるとの認識のもとに、不正アクセス禁止法・ネットワーク犯罪防止法制の整備の必要性等を訴えている。[1][2][45]

他方、民間技術者の間では、国家政策としての鍵寄託・鍵回復システムには懐疑的な意見が多かった。[42]

### (2) 暗号特使との会合

2.3(2)にも述べたように、D. Aaron 暗号特使との会合は、1997 年 2 月に米国大使公邸で行われた。この会合において Aaron 特使は、鍵寄託・鍵回復の米国暗号政策を説明し、それに対する支持を訴えたが、その場では大した議論はなかった模様である。[H5][H6]

### (3) 暗号特使以後の日本の暗号政策

1996 年以降、通産省や IPA による鍵回復システムの試作事業などの技術的な検証は行われた[S1][S2][S3][S4][S5]が、国家政策として鍵寄託・鍵回復政策がとられることはなかった。

一方、ハイテク犯罪や不正アクセスに対する対策として、1998 年 6 月に警察庁が「ハイテク犯罪対策重点推進プログラム」を発表し、あわせて 1999 年 4 月には警察庁にナショナルセンター（HITEC）が設置される。更に、1999 年 8 月には不正アクセス禁止法が公布され、日本における情報セキュリティ対策の制度は徐々に整っていった。

また、暗号に関する政策としては、2000 年度から客観的な評価により安全性及び実装性に優れると判断された暗号技術をリスト化する暗号技術評価プロジェクト CRYPTREC（Cryptography Research and Evaluation Committees）が始まった。CRYPTREC では、公募された暗号技術や業界で広く利用されている暗号技術を評価・検討するとともに、安全性及び実装性能に優れた暗号技術を評価・選択した。この結果を踏まえて、2003 年に総務省と経済産業省は「電子政府における調達のための推奨すべき暗号のリスト(電子政府推奨暗号リスト)」を公表した。

現在、CRYPTREC は、総務省と経済産業省が共同運営する「暗号技術検討会」と、NICT 及び IPA が運営する「暗号技術監視委員会」「暗号モジュール委員会」「暗号運営委員会」で構成されている。

このうち、「暗号技術監視委員会」は電子政府推奨暗号リストに掲載された暗号の安全性の監視・調査、「暗号モジュール委員会」は暗号を実装した暗号モジュールの日本における評価基準を確立する活動、「暗号運用委員会」は電子政府における暗号技術の適切な運用を目的とした調査・検討を行っている。

## 5.2　鍵寄託・鍵回復システムの試作

1996 年度から 1998 年度にかけて、IPA 及び通産省の事業として実施された鍵寄託・鍵回復試作システムの概要を述べる。

### (1) 1996 年度試作システムの概要[S1][S2][S3]

**【開発者】**日立製作所、富士通、北陸先端科学技術大学院大学

**【システムの目的】**

企業におけるロストキー対策。特に、利用者の秘密鍵を紛失した際の対策。

**【システムのポイント】**

・全体のシステム構成は、利用者システム、鍵登録機関、データ回復機関及び複数の鍵保管機関 $KS_i(i=1,2,\cdots,k)$からなる。

・**（利用者の秘密鍵の分割保管）**利用者は、自身の秘密鍵 UPriKey を鍵保管機関数分 $UPriKey_i(i=1,2,\cdots,k)$に分割[3]した上で、任意の共通鍵 K で各 $UPriKey_i$ を暗号化し、使用した共通鍵 K を鍵保管機関の公開鍵 $KS_iPubKey$ によって暗号化したエンベロップ｛E[K](UPriKey$_i$), E[$KS_i$PubKey](K)｝[4]を作成し、鍵保管機関 $KS_i$ に預ける。

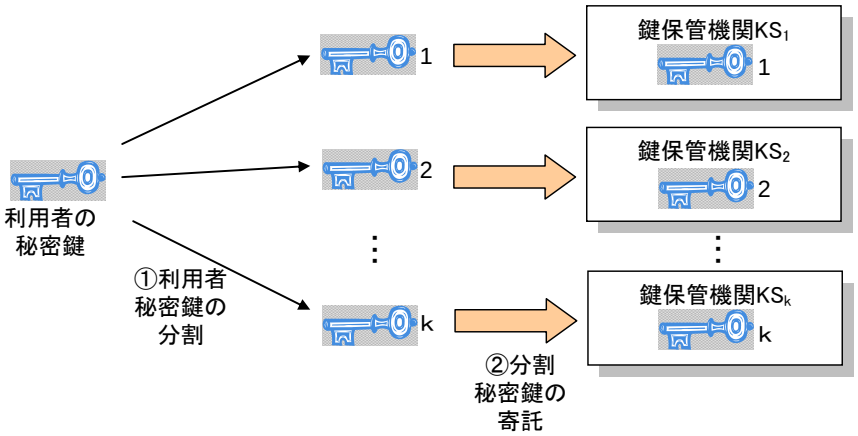


図 2　利用者秘密鍵の分割寄託（事前準備）

・**（暗号化データは PKCS#7 でエンベロップ化）**データ M の共通鍵 L による暗号化データは、｛E[L](M), E[UPubKey](L)｝というエンベロップ（PKCS#7）で保存されているとする。ここで、UPubKey は利用者の公開鍵を表す。尚、利用者 A から利用者 B に伝送されるデータの場合は UPubkey は利用者 B の公開鍵を表す。

---

[3] 例えば、RSA 法による公開鍵暗号の構成は、P、Q を異なる素数とし、A を(P-1)と(Q-1)の最小公倍数、e を A と互いに素な正の整数、d を ed≡1 mod.A となる正の整数としたとき、UPubKey=(e,PQ)、UPriKey=(d,PQ)のペアで表せる（脚注 4 も参照）。このとき、d を d=d1+d2+…+dk という正の整数の和で表したときの各(di,PQ)が $UPriKey_i$ に相当する。

[4] データ D の暗号鍵 K による暗号化データを E[K](D)と表す。特に、公開鍵暗号において K=(k,PQ)と表したとき（脚注 3 参照）、E[K](D)は $D^k$ mod.PQ を表す。

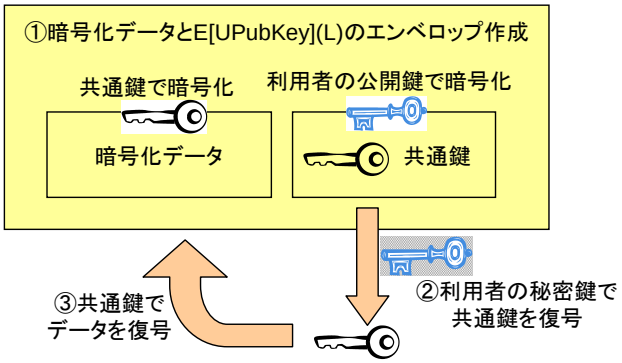


図 3　暗号化及び通常時の復号処理

・利用者が自身の秘密鍵 UPriKey を紛失した際の暗号化データ回復手順は、E[UPubKey](L)をすべての鍵保管機関に送り、$UPriKey_i$ により共通鍵 L の部分鍵 $L_i$ を回復し、データ回復機関に送る。データ回復機関では、各 $L_i$ を合成して共通鍵 L を回復し、データ M を回復する。[5]

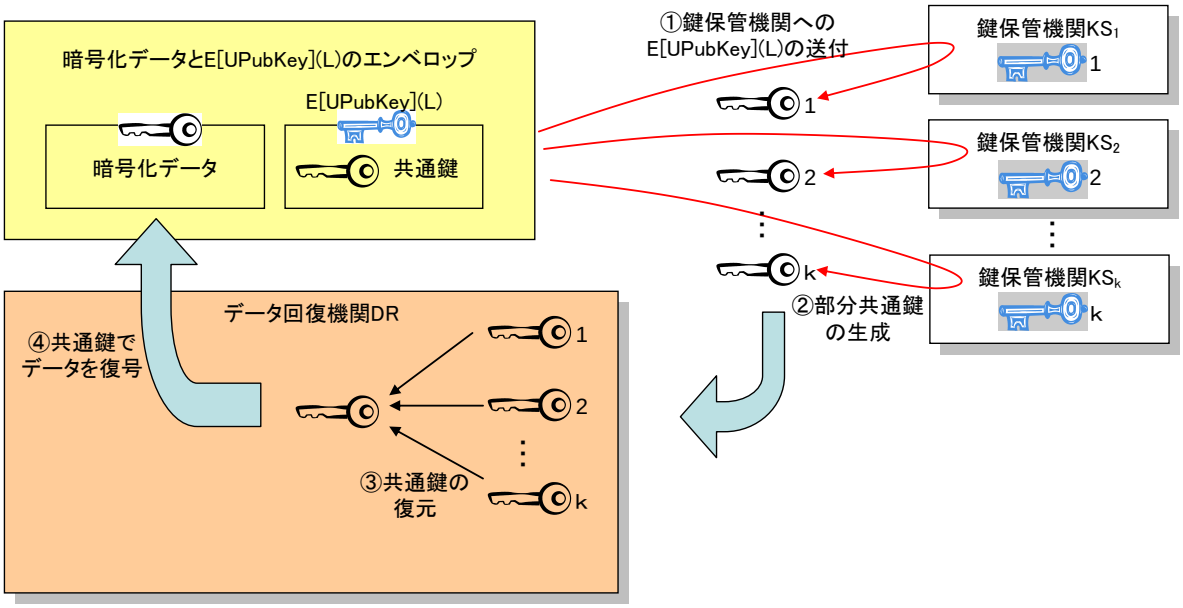


図 4　鍵回復処理

・この方法では、データ M の暗号化に利用した共通鍵 L は回復されるが、利用者の秘密鍵 UPriKey 自身はデータ回復機関及び鍵保管機関のいずれにおいても復元されないため、利用者が暗号化した他のデータの秘密は守られる。[6]

---

[5] P、Q、e、d を脚注 3 のとおりとすると、任意の正の整数 D に対して $D^{ed} \equiv D \bmod PQ$ が成り立つことが RSA 暗号の根拠となっている。脚注 4 で述べたように、$E[UpubKey](L)=L^e \bmod PQ$ であり、d= d1+d2+…+dk としたとき、$L^{ed}=L^{e(d1+d2+\cdots+dk)} = L^{ed1} \cdot L^{ed2} \cdot \cdots \cdot L^{edk}$ となる。本文に述べている「回復した部分鍵 $L_i$」とは $L^{edi} \bmod PQ$ のことであり、これらの mod.PQ における積をとると、$L^{ed} \bmod PQ \equiv L \bmod PQ$ となって、元の鍵 L が復元される。

[6] 脚注 5 の用語で言えば、分割した d1、d2、…、dk から d を直接求めるのではなく、先に $L^{ed1}$、$L^{ed2}$、…、$L^{edk}$ を求めておいて、これらの積をとることで L を復元するため、d 自体はどこにも現れず、利用者の秘密鍵自体は暴露されない。

**【本方式の特徴の考察】**

本方式において、他の方式との違いとなりうるポイントについてまとめる。

・利用者の秘密鍵を事前に第三者機関に分割寄託しておく。（**秘密鍵の分割寄託**）

・データの暗号化は共通鍵方式で行い、利用した共通鍵は利用者の公開鍵で暗号化して KRF(Key Recovery Field)を作成し、暗号化データに添付する。利用者の秘密鍵が利用できる状態においては、KRF から直接共通鍵を取り出してデータを復号する。

・利用者の秘密鍵が利用できない状態となった際には、KRF を分割寄託した第三者機関全てに送り、各第三者機関で共通鍵の部分鍵を復元する。これら部分鍵を全て掛け合わせて共通鍵を復元し、データを復号する。

・この方式の正当性は、前ページ脚注 5 の $L^{ed}=L^{e(d1+d2+\cdots+dk)}=L^{ed1}\cdot L^{ed2}\cdot\cdots\cdot L^{edk}$ という式が根拠となっている。従って、寄託した第三者機関全ての情報が必要になる。例えば、必ずしも全ての第三者機関の情報を必要としない秘密分散法[53]では必ずしもこの式が成立するとは言えないため、**本方式での利用者の秘密鍵の第三者機関への寄託において一般的には秘密分散法を使うことはできない**。[7]

・この方式の場合は、対象となるデータに添付された共通鍵のみが回復されるので、各データに異なる共通鍵を設定しておけば、鍵回復を行ったことによる他の暗号化データの秘密暴露の危険性はないが、強いて言えば、ビッグブラザーが第三者機関の部分秘密鍵全てを入手し、利用者の秘密鍵を復元する危険性がない訳ではない。（秘密鍵は利用者本人のみが持つべきであり、たとえ部分鍵といえども第三者に寄託した場合の危険性はある。）

[7] 強いて言えば、共通鍵の部分回復ではなく、利用者の秘密鍵を直接回復する方法をとれば秘密分散法が適用できるが、この場合、利用者の秘密鍵が暴露されるという重大なリスクがある。

### (2) 1997 年度試作システムの概要[S4]

**【開発者】**日本電気、日立製作所、富士通

**【システムの目的】**

企業におけるロストキー対策。特に、データの暗号化に利用した共通鍵を紛失した際の対策。

**【システムのポイント】**

・全体のシステム構成は、利用者システムと複数のデータ回復センター$DRC_i(i=1,2,\cdots,k)$からなる。

・**（暗号化データと暗号化共通鍵の DRC 公開鍵による暗号化のエンベロップ）**

データ M の共通鍵 L による暗号化データは、{E[L](M), L の DRC の公開鍵による暗号化} というエンベロップで保存されているとする。ここで、L の DRC の公開鍵による暗号化の部分は、①順次方式、②並列方式、③秘密鍵分散方式のいずれかの方式により、それぞれ①$E[DRC_1PubKey[DRC_2PubKey[\cdots]]](L)$、②$E[DRC_1PubKey](L_1)$, $E[DRC_2PubKey](L_2),\cdots$, $E[DRC_kPubKey][L_k]$, $L=L_1+L_2+\cdots+L_k$（+は排他的論理和を表す）、③一つの DRC と複数の鍵保管機関を利用した 5.2(1)と同様の方法、のいずれかとなる。

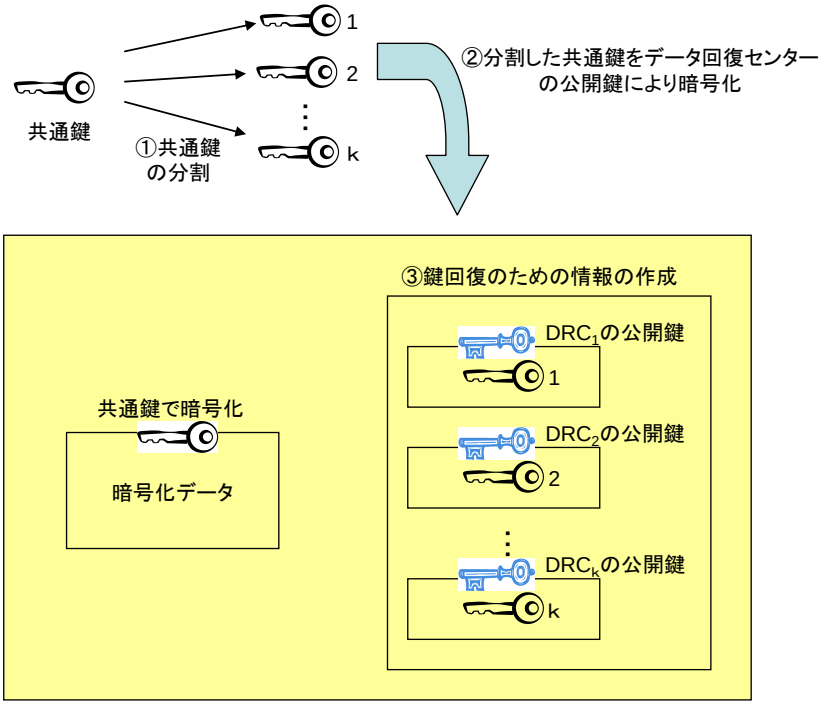


**図 5　共通鍵の分割と鍵回復情報の作成（並列方式の場合）**

・共通鍵 L を紛失した場合、①②③の場合に応じて、次の手順でデータ復元する。

①の場合：決められた順番により、各データ回復センターで共通鍵 L を順次回復し、最後の $DRC_k$ で L は完全に復元する。

②の場合：各データ回復センターで部分鍵 $L_i$ を復元し、それらを合成して共通鍵 L を復元する。

③の場合：5.2（1）と同様に、E[UPubKey](L)を各鍵保管機関におくり、それぞれの鍵保管機関で部分鍵 $L_i$ を復元し、それらをデータ回復センターで合成して共通鍵 L を復元する。

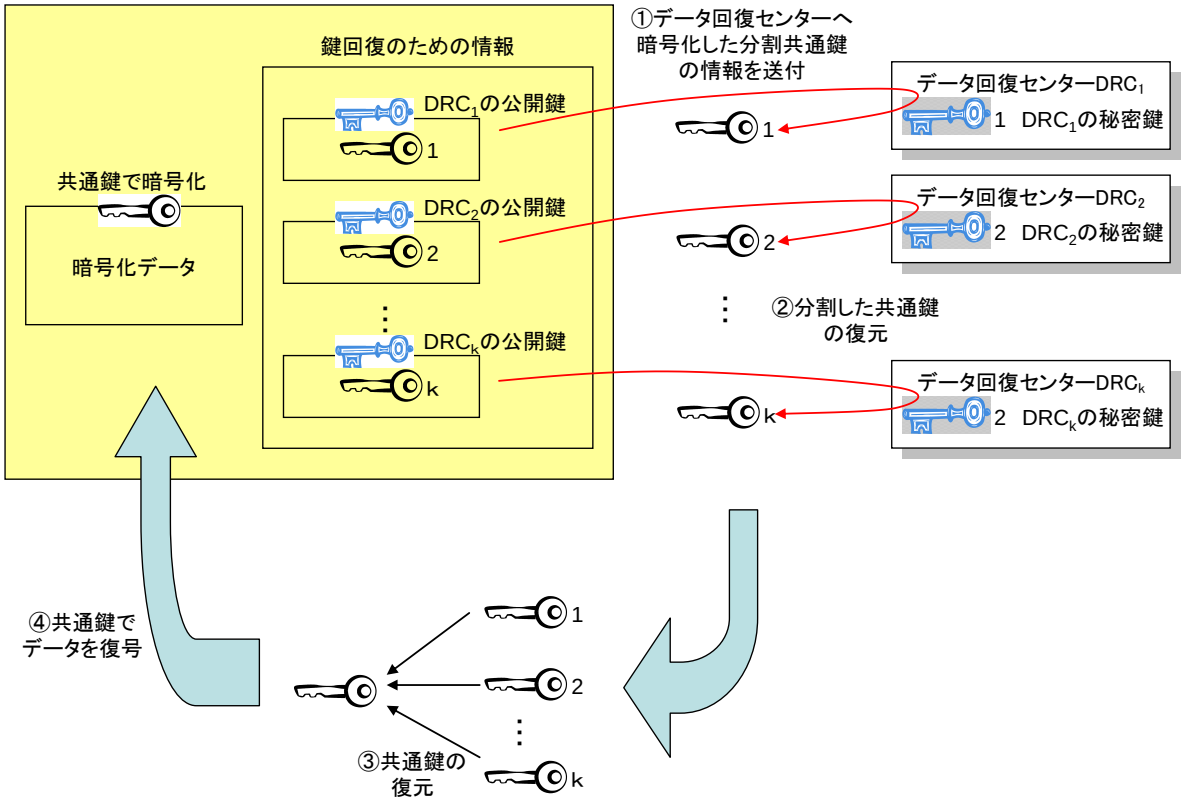


図 6　鍵回復処理（並列方式の場合）

**【本方式の特徴の考察】**

本方式の②の場合について、他方式との違いとなりうる点についてまとめる。

- **事前に鍵の寄託は行わない**。（事前に鍵の寄託を行わない点は(1)との大きな違い。）
- データの暗号化は共通鍵方式で行うとともに、利用した共通鍵 L を部分鍵 $L_i$ により $L= L_1+L_2+\cdots+L_k$（+は排他的論理和を表す）と分割する。各 $L_i$ を複数のデータ回復センターの公開鍵で暗号化したもの $E[DRC_1PubKey](L_1)$, $E[DRC_2PubKey](L_2),\cdots$, $E[DRC_kPubKey][L_k]$をとりまとめて KRF とする。データ暗号化の時点で L の部分鍵を作成しておく点は(1)との大きな違い。また、L の分割に排他的論理和を用いているため、基本的には**全ての部分鍵が揃わないと元の共通鍵は復元できない**。（この点は次に述べる(3)の方式との違い。）
- 本方式の場合、(1)の方式とは異なり、共通鍵 L の利用者の公開鍵による暗号化データは添付されていないため、**共通鍵 L は別途利用者間で共有されている前提**と思われる。従って、(1)のように**データ毎に暗号化鍵 L を変えられる方式ではない**と思われる。（もし、データ毎に暗号化鍵 L を変えるとすると、暗号化データの復号のたびに鍵回復の手順を踏まなければならなくなる。）
- 共通鍵 L が利用できない状態となった際には、KRF の中の暗号化された部分鍵

E[DRC$_i$PubKey][L$_i$]を各データ回復センターに送り、部分鍵 L$_i$ を復元した後、それらを全て排他的論理和で合成して共通鍵 L を復元する。

・上に述べたとおり、共通鍵 L は利用者間で事前に共有されていると考えられ、鍵回復の対象となったデータ以外のデータの暗号化にも使われている可能性がある。従って、鍵回復処理を行った後に、この共通鍵 L を使って暗号化された他のデータについても秘密が暴露される危険性（**バックワードセキュリティの観点での脅威**）がある。また、鍵回復後は、同じ L を使った暗号化データはやはり秘密が暴露される危険性（**フォワードセキュリティの観点での脅威**）がある。

・まとめると、利用者の秘密鍵を事前に寄託する必要のない点は利用者にとっては長所であるが、データ毎に共通鍵を変えることができない点はバックワードセキュリティやフォワードセキュリティの観点では短所である。

### (3) 1998 年度試作システムの概要[S5]

**【開発者】** 東芝

**【システムの目的】**

企業におけるロストキー対策。特に、データの暗号化に利用した共通鍵を紛失した際の対策。

**【システムのポイント】**

・全体のシステム構成は、利用者システムと複数の鍵回復エージェント $KRA_i(i=1,2,\cdots,k)$、認証局からなる。

・**（暗号化データと暗号化共通鍵の KRA 公開鍵による暗号化のエンベロップ）**

データ M の共通鍵 L による暗号化データは、{E[L](M), L の KRA の公開鍵による暗号化(KRF:Key Recovery Field)} というエンベロップで保存されているとする。ここで、「L の KRA の公開鍵による暗号化」の部分は、共通鍵 L を秘密分散法[53]により鍵回復エージェント数分 $L_1, L_2, \cdots, L_k$ に分割した上で、$E[KRA_1PubKey](L_1)$, $E[KRA_2PubKey](L_2),\cdots, E[KRA_kPubKey][L_k]$をエンベロップとして埋め込む。この秘密分散法を用いた点が 5.2(2)②の並列方式と異なる。

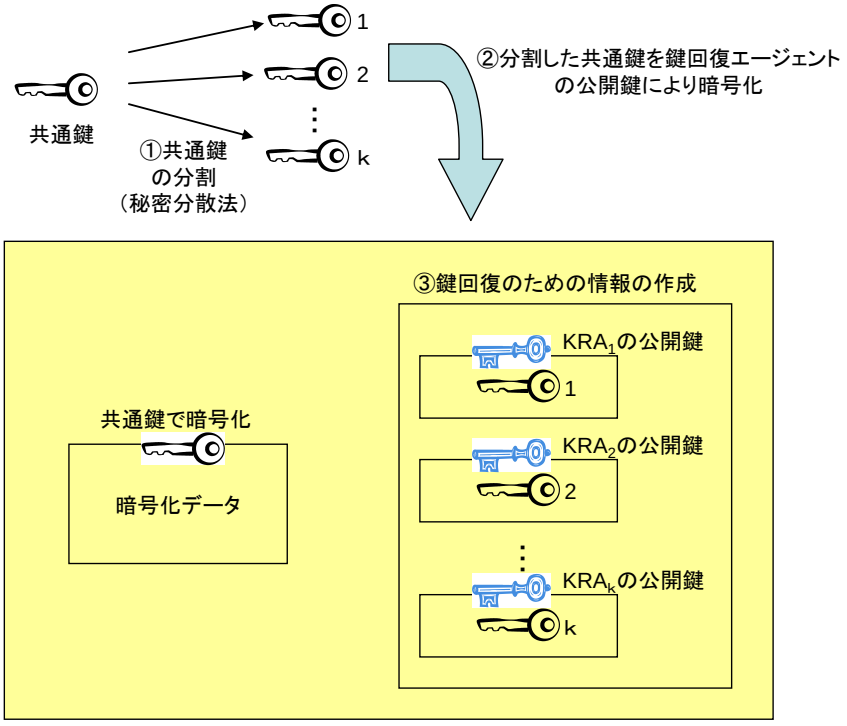


**図 5　共通鍵の分割と鍵回復情報の作成**

・共通鍵 L を紛失した場合、各 $KRA_i$ で部分鍵 $L_i$ を復元し、それらを合成して共通鍵 L を復元する。尚、秘密分散法の構成より、全ての部分鍵が揃わなくても、一定の数が揃えば L を復元できる。

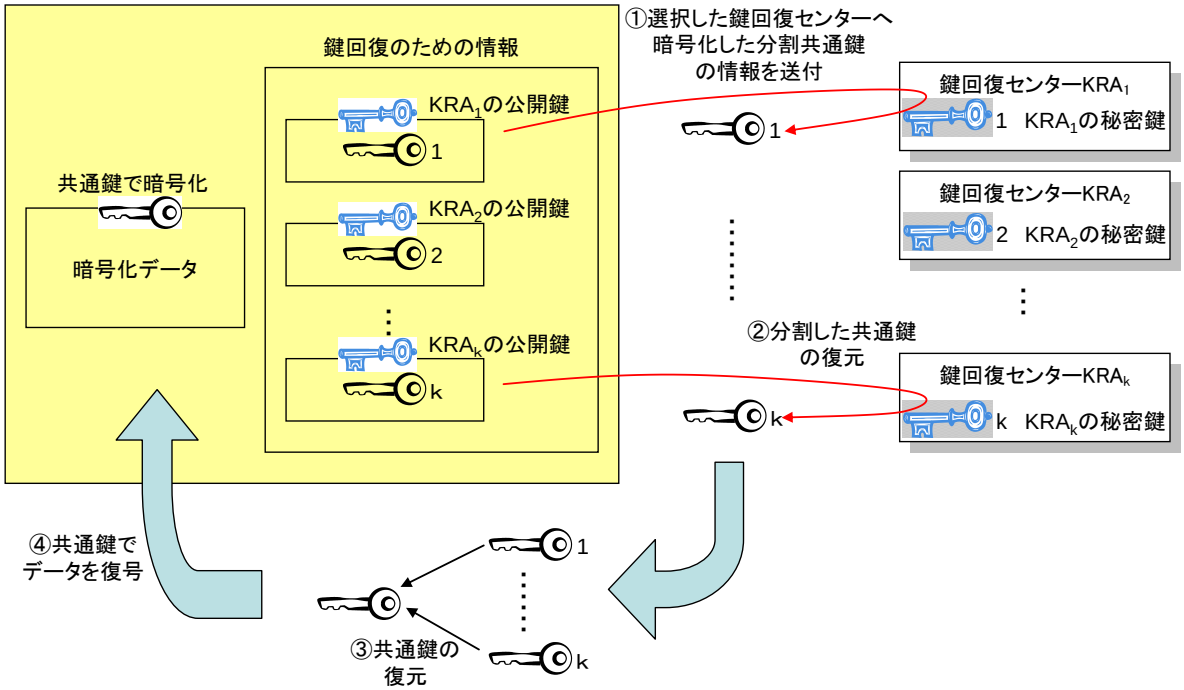


図 6　鍵回復処理（並列方式の場合）

**【本方式の特徴の考察】**

本方式において、他の方式との違いとなりうるポイントについてまとめる。

- **事前に鍵の寄託は行わない**。((2)と同様に、事前に鍵の寄託を行わない点は(1)との大きな違い。)
- データの暗号化は共通鍵方式で行うとともに、利用した共通鍵 L を秘密分散法[53]により部分鍵 $L_i$ に分割する。各 $L_i$ を複数の鍵回復エージェントの公開鍵で暗号化したもの $E[KRA_1PubKey](L_1)$, $E[KRA_2PubKey](L_2)$,…, $E[KRA_kPubKey][L_k]$をとりまとめて KRF とする。秘密分散法を用いているため、**必ずしも全ての部分鍵が揃わなくても一定数の部分鍵があれば元の共通鍵を復元できる**。((2)との違い)
- (2)と同様、本方式の場合も(1)の方式とは異なり、共通鍵 L の利用者の公開鍵による暗号化データは添付されていないため、**共通鍵 L は別途利用者間で共有されている前提**と思われる。従って、(1)のように**データ毎に暗号化鍵 L を変えられる方式ではない**と思われる。(もし、データ毎に暗号化鍵 L を変えるとすると、暗号化データの復号のたびに鍵回復の手順を踏まなければならなくなる。)
- 共通鍵 L が利用できない状態となった際には、KRF の中の暗号化された部分鍵 $E[KRA_iPubKey][L_i]$の中から一定数のものを選び対応する鍵回復エージェントに送り、部分鍵 $L_i$ を復元した後、合成して共通鍵 L を復元する。秘密分散法で部分鍵が作られているため、必ずしも全ての部分鍵がなくても L を復元できる。
- (2)と同様に、共通鍵 L は利用者間で事前に共有されていると考えられ、鍵回復の対象となったデータ以外のデータの暗号化にも使われている可能性がある。従って、鍵回復処理を行った後に、この共通鍵 L を使って暗号化された他のデータについても秘密が暴露される危険性（**バックワードセキュリティの観点での脅威**）がある。また、鍵

回復後は、同じ L を使った暗号化データはやはり秘密が暴露される危険性（**フォワードセキュリティの観点での脅威**）がある。

・まとめると、利用者の秘密鍵を事前に寄託する必要のない点や、一定数の部分鍵から元の共通鍵を復元できる点は利用者にとっては長所であるが、データ毎に共通鍵を変えることができない点はバックワードセキュリティやフォワードセキュリティの観点では短所である。

# 6. 現代的視点での鍵回復システム

## 6.1　現代的視点での鍵回復システムの目的と要件

### (1) 現代的視点での鍵回復システムの目的

2.及び 3.で見たように、国の安全保障政策としての鍵寄託・鍵回復システムは、現代的な視点では完全に否定されている。その一方で、4.で見たように、民間部門における鍵回復システムは、1990 年代からその必要性は十分に認識されているとともに、現代においてもその必要性は変わらない。

現代的な視点で鍵回復システムが必要となる理由は、企業内での職員の退職等による鍵紛失というクラシカルなもの以外に、最近のクラウド利用におけるデータの暗号化及び鍵管理の必要性や、犯罪捜査の目的でのデジタル・フォレンジックにおける第三者による暗号化データの復号の必要性等、新たな理由も現れている。

また、鍵紛失の卑近な例として、データのやり取りをメールの添付ファイルで行う際の添付ファイルの暗号化が挙げられる。この場合、復号のためのパスワードは別メールの本文に記入される場合が多いが、この添付ファイルをダウンロードして保管する際にパスワードの管理を忘れると、後々このファイルは開けない可能性が大きい。これは、復号の手順がシステム化されておらず、人手や記憶に頼るアドホックな手順になっているからである。このように、従業員が退職するか否かに関わらず身近に鍵紛失の危険性は潜在しており、簡易な暗号の利用が進めば、今後このような鍵紛失が大きな問題となりかねない。

更に、行政分野の例を挙げれば、職員の判断で行政文書を暗号化した場合、国民からの情報公開請求に対して、鍵紛失を理由に情報公開ができない事態も想定される。

このように、現在、暗号の利用は個人の判断で自由に行えるが、その反面、暗号化データの取扱いの原則は必ずしも明確ではない。

このような状況を鑑みたとき、鍵回復システムを鍵紛失時の単なる対症療法として捉えるのではなく、むしろ視点を広げて、暗号利用管理システムと捉えるのが現代的ではないか。この視点から、暗号利用管理システムとしての鍵回復システムは、次の 3 つの基本機能を備えるべきと考える。

① データを暗号化する者（データ所有者）は、その暗号化データを復号できる者（データ利用者）を明示的に指定できる。

② ①で指定されたデータ利用者は、その暗号化データ自体から復号に必要な情報（共通鍵）をシステム的に入手し、暗号化データの復号を行うことができる。

③ ①に関わらず、法令の規程、組織ポリシーの規程、事故・災害時等の緊急対応方針等に準じて、①で指定された者以外の者が暗号化データを復号する手段を提供する。このとき、対象となる暗号化データと復号できる者を限定できる。

### (2) 現代的視点での鍵回復システムの要件

5.2 に示した試作システムの方式も参考として、(1)の 3 つの基本機能を備えた現代的な視点での鍵回復システムに求められる要件をまとめる。

要件１　暗号化データには、そのデータを復号できる者（複数も可）を示す情報（Data Decryption Field 以下、DDF）が含まれる。DDF に記された者は、復号に必要な共通鍵をシステム的に入手し、暗号化データを復号することができる。

要件 2　暗号化データには、DDF に記された者以外の者が暗号化データを復号するための情報（Key Recovery Field 以下、KRF）が含まれる。KRF を利用することで、暗号化データの暗号鍵（共通鍵）を入手することができる。これを鍵回復と呼ぶ。

要件 3　鍵回復にあたっては第三者機関（原則複数）が関与し、第三者機関が設定する運用ポリシーに準じた認証・認可を受けた者のみが鍵回復を行うことができる。また、対象となる暗号化データも運用ポリシーに準じたものに限定される。

要件 4　第三者機関の運用ポリシーは、法令、組織ポリシー、事故・災害時等の緊急対応方針等に整合したものでなければならない。また、複数の第三者機関が関与する場合は、その運用ポリシーは互いに協調的なものでなければならない。

これらの要件は、(1)の 3 つの基本機能を技術面及び運用面で担保するために必要なものである。

また、次の要件は、2.及び 3.で示した古くから指摘されている鍵寄託・鍵回復に対するリスクの観点から、暗号利用の信頼性を担保するために必要なものである。

要件 5　鍵回復の対象となる「鍵」は、データの暗号化に用いられる共通鍵であり、データ利用者の秘密鍵ではない。

データ利用者の秘密鍵を回復することは、第三者にデータ利用者の秘密鍵を暴露することにもつながり、データ利用者の秘密保護の面で重大なリスクとなる可能性がある。

要件 6　鍵回復によって回復対象となったデータ以外のデータの秘密が暴露されることはない。

鍵回復によって、回復対象となったデータ以外のデータに対して、時間的ないし空間的なリスクが発生する可能性がある。

時間的なリスクとは、鍵回復を行った時点以前に暗号化したデータの秘密が暴露されるバックワードセキュリティの観点からのリスクと、鍵回復を行った時点以降の暗号化処理に影響を与えるフォワードセキュリティの観点からのリスクである。

また、空間的なリスクとは、鍵回復の対象となった暗号化データ以外に、本来関係のない暗号化データの秘密暴露につながるリスクである。

鍵回復は、このようなリスクが発生しないような仕組みにする必要がある。

要件 7　暗号化に用いる共通鍵及びデータ利用者の秘密鍵は第三者に寄託しない。

暗号化に用いる共通鍵やデータ利用者の秘密鍵を第三者に寄託することは、新たな攻撃のターゲットを生むことにつながるという指摘は古くからある。[8][17]

### (3) 鍵回復システムの方式

(2)で示した鍵回復システムの要件を満足する鍵回復システムの方式は、5.2 で見た試作システムの内容も踏まえると、次のようなものが考えられる。

まず、要件 1 及び 2 より、DDF 及び KRF を暗号化データ自体に添付しておくことが必要である。DDF と KRF は、5.2 で見た試作システムの方式も考慮すると、5.2(1)の方式と 5.2(2)及び(3)の方式のハイブリッド型がよいことが判る。即ち、

① （DDF の作成）データの暗号化に用いた共通鍵を、指定するデータ利用者（複数可）の公開鍵で暗号化し、暗号化オリジナルデータに添付する。これを DDF とする。

② （KRF の作成）データの暗号化に用いた共通鍵を、鍵回復で利用する第三者機関数分に分割する[8]。これらの分割した共通鍵を、それぞれ対応する第三者機関の公開鍵で暗号化し、それらを暗号化オリジナルデータに添付する。これを KRF とする。尚、この第三者機関は複数設定し、いずれも(2)の要件 3 及び要件 4 を満たすものとする。[9]

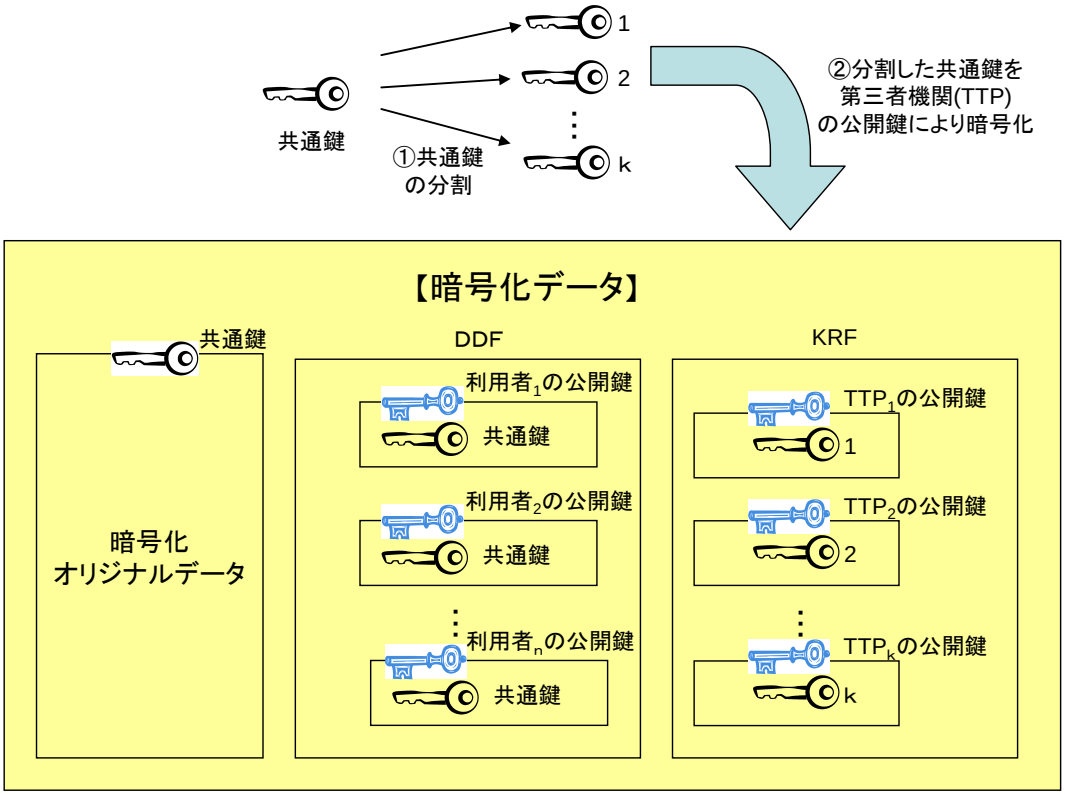


図 7　暗号化データ・DDF・KRF

③ （通常の復号処理）①に指定したデータ利用者の秘密鍵が安全かつ有効に保持されている場合は、DDF 内のデータ利用者の公開鍵で暗号化された共通鍵を、データ利用者の秘密鍵で復号し、その共通鍵で暗号化オリジナルデータ自体を復号する。

---

[8] この分割方法には、5.2(2)の排他的論理和を用いる方法や 5.2(3)の秘密分散法を用いる方法がある。

[9] 第三者機関は原則として複数設けるべきである。何故なら、もし第三者機関が一つしかないとすると、KRF はその第三者機関のデータだけとなり、共通鍵そのものをその第三者機関が復号できることになるので、あらゆる暗号化データを復号できる潜在能力を持つことになる。

④ （鍵回復時の処理）DDF による復号ができない場合は、KRF による鍵回復を行う。鍵回復処理を要求する者は、各第三者機関の認証・認可を得た上で、KRF 内の暗号化した分割共通鍵を対応する第三者機関に送る[10]。各第三者機関は、自身の秘密鍵で分割共通鍵を復号したものを要求者に送り返す。要求者は、送られた分割共通鍵を合成して暗号化に利用した共通鍵を復元し、その共通鍵で暗号化オリジナルデータ自体を復号する。

①は 5.2(1)の PKCS#7 に複数のデータ利用者を記したものに相当し、これに KRF を追加したものが上記方式である。これらのデータを、データ作成時にデータ暗号化処理とともに作成しておくというのがこの方式のポイントである。また、第三者機関の役割は、鍵の寄託先ではなく、鍵回復処理の支援という位置づけである。

この方式が(2)の要件 1～7 を満たすことは、容易に確認できる。

### (4) 鍵回復が必要となる場合

鍵回復が必要となる場合として、次のようなものが例として考えられる。

① DDF に指定した利用者の秘密鍵が使えなくなった場合に、当該利用者が申請して鍵回復を行う。

② 企業が所有するデータで、従業員が個人の秘密鍵で暗号化したデータについて従業員の秘密鍵が使えなくなった場合に、企業が申請して鍵回復を行う。

③ 企業の不正行為や、企業の従業員の犯罪行為の証拠として、法執行機関による捜査に必要なデータに対して、令状を持った法執行機関が申請して鍵回復を行う。（デジタル・フォレンジック）

④ 個人が自らの財産等に係わる電子文書を暗号化し、その個人が亡くなった場合に、法定相続人が申請して鍵回復を行う。

### (5) 第三者機関の要件

(3)に記した第三者機関に求められる要件として、次のものが挙げられる。

① 第三者機関は、申請者から KRF のデータのみを受領し、暗号化オリジナルデータの復号に必要な共通鍵の断片（部分共通鍵）を申請者に返す。

② 第三者機関は、DDF を用いた暗号化オリジナルデータの復号には一切関与しない。

③ 第三者機関は、暗号化オリジナルデータにはアクセスできない。

④ 第三者機関を利用する可能性のある者は、事前に本人認証用の認証局電子署名付きの公開鍵認証書を第三者機関に届けておく。

⑤ 第三者機関への登録候補者としては次の者が想定される。

・暗号化オリジナルデータ作成者
・DDF に記された利用者
・企業ないしは企業の特定部門
・国の機関

---

[10] 共通鍵の分割で秘密分散法を用いた場合は、共通鍵復元に必要な数の第三者機関を選択した上で、それらの第三者機関に暗号化した分割共通鍵を送る。

・自治体
・法執行機関　等

⑥　鍵回復を依頼する際には、申請者の電子署名付きの申請書で申請する。申請書には、鍵回復理由と対象データを記す。

⑦　鍵回復においては、部分鍵の合成による共通鍵の復元と暗号化オリジナルデータの復号は申請者自身が行い、第三者機関は関与しない。

### (6) 個人利用と企業利用の運用面での留意点

4.2 で示した B.Gladman の分類による鍵回復システムは、大別すると個人利用と企業利用に分けられる。

個人利用の場合は、データ所有者=利用者=本人であり、秘密鍵は本人のみが持つ。

他方、企業利用の場合は、データ所有者=企業、利用者=従業員であり、また部門でデータ共有が必要な点を考慮すると、同じ秘密鍵を複数人が共同利用する必要が出てくる。この場合の秘密鍵の持ち方は、通常の個人の秘密鍵の持ち方ではなく、例えば部門専用の耐タンパー性の媒体に部門従業員が同一の部門用秘密鍵を持ち、従業員の異動に伴い確実に媒体自体をメンバー間で引継ぎする等、鍵管理の運用面での考慮が必要である。

## 6.2　今後の課題

6.1 で示した鍵回復システムと、現在一般的な暗号の利用形態とのギャップはかなり大きい。6.1(1)で示した潜在的な鍵紛失リスクをベンダー及び利用者に知らしめて、暗号データの取扱い原則の明確化やアドホックでないシステム的な復号方法の必要性を認識させる必要があろう。

行政文書の暗号化や企業内の暗号文書に対するデジタル・フォレンジック対応などについては、法整備の必要性もあろう。

鍵回復に関与する第三者機関の法的な位置づけ、運用ポリシー、具体的なオペレーションなど、第三者機関についての検討課題は多い。

また、暗号技術については、最近、ID ベース暗号やペアリング暗号などの新技術が現れている[54]。これらの新技術と鍵回復システムとの整合性の確認も必要である。

更に、6.1(6)で触れた企業利用における鍵回復システムの運用面での考慮点は、一段と深い議論が必要と思われる。これについても今後の課題としたい。

## 参考１　　鍵寄託・鍵回復関係年表

| 年 | 月 | 国際的な動向 | 米国の動向 | | 欧州の動向 | 日本の動向 |
|---|---|---|---|---|---|---|
| | | | 推進派 | 慎重派 | | |
| 1993 | 4 | | ・米国政府が Clipper Chip、SKIPJACK を導入する構想 EEI(Escrowed Encryption Initiative)（Clipper 1）を発表(※データ鍵の寄託) | | | |
| 1994 | 2 | | ・NIST が Clipper 1 のコンセプトを EES(Escrowed Encryption Standard)として FIPS に認定 | ・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 Clipper 1 に対するネガティブ・キャンペーンを展開 | | |
| | 9 | | ・暗号技術の輸出について、予め定められた地域への輸出について、1件ごとの輸出許可取得を省略するように変更 | | | |
| | 10 | | ・通信会社が、鍵寄託構想を実現するための通信設備を改造する際の費用を政府が負担する法律が成立→AT&T は Clipper1 のコンセプトを実現した電話機を開発 | | | |

| 年 | 月 | 国際的な動向 | 米国の動向 | | 欧州の動向 | 日本の動向 |
|---|---|---|---|---|---|---|
| 1995 | 2 | ・米国 ITI、カナダ ITAC、欧州 EUROBIT、日本 JEITA が「グローバルな暗号政策の提言」を発表し、政府の合法的アクセスを容認する一方、民間にも暗号利用の権利があることを主張 | | | | |
| | 8 | | ・ 暗号技術の輸出規制緩和策（Clipper 2）が発表される | | | |
| | 9 | | | | ・EU 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」を採択<br>－ 犯罪捜査のための情報通信データの傍受を可能とする | |
| | | | ・国務省が Zimmermann（PGP の開発者）を武器輸出管理法違反で起訴 | ・Zimmermann 救済キャンペーンが起こり、政府は起訴を取り下げ | | |
| | 12 | ・新たな輸出貿易管理体制であるワッセナー・アレンジメントが成立（現参加国 40 カ国） | | | | |
| 1996 | 2 | | ・個人的な利用に限り、米国民が一時的に暗号装置を海外に持ち出すことを許可 | | | |

| 年 | 月 | 国際的な動向 | 米国の動向 | | 欧州の動向 | 日本の動向 |
|---|---|---|---|---|---|---|
| | 5 | ・BIACとICCが「暗号は電子的情報の機密性、完全性及び可用性を保護する重要な道具である」とする合同文書を発表 | ・米国政府が KMI(Key management Infrastructure)構想（Clipper 3)を発表(※秘密鍵の寄託） | ・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は KMI 構想自体は評価するも、KMI と鍵回復構想が一体化していることを批判 | | |
| | 7 | | | | ・フランス政府が電気通信法を一部改正<br>－ 秘匿目的での暗号技術の利用者に対する鍵回復機関への秘密鍵の預託の義務付け<br>－ 鍵回復機関の承認制を導入 | |
| | 9 | | | ・EPIC 主催のシンポジウムで 15 の市民団体が「暗号政策の基礎を個人がプライベートな通信を行う基本的権利に置くことを OECD に強く促す」という共同決議を採択 | | |
| | 10 | | ・ゴア副大統領が、暗号政策を鍵寄託から鍵回復に転換した旨を発表（以降、鍵寄託という言葉は使われず、鍵回復に変わる） | | | |
| | 11 | | ・D. Aaron が暗号特使（Special Envoy for Cryptography)に任命される | | | |

| 年 | 月 | 国際的な動向 | 米国の動向 | | 欧州の動向 | 日本の動向 |
|---|---|---|---|---|---|---|
| | 12 | | | | ・ドイツにおいて電子署名法が成立 | |
| 1997 | 1 | | ・輸出管理規制の一部改正<br>– 暗号輸出規制の所管が国務省から商務省に移行<br>– 鍵回復機能のついた暗号装置は輸出規制対象外となる<br>– 鍵回復機能のついていない暗号装置は、1998 年末までに鍵回復機能を搭載することを条件に、56bit 以下の鍵長であれば輸出を許可<br>– 鍵情報は商務省認可の鍵復元機関のみが保管する | | | |
| | 2 | | ・IBM、DEC、Cylink が 56bit 鍵長の暗号輸出許可を受ける | | | ・暗号特使 D. Aaron が来日し、政府関係者、有識者、企業代表と会談 |
| | 3 | ・OECD が暗号政策ガイドラインを発表 | ・電子情報安全法（Electronic Data security Act of 1997)が成立<br>・TISが鍵回復技術搭載の暗号装置の輸出許可を得る | ・RSA 社社長が 56bit 鍵長以下の暗号装置の輸出ライセンスを得るつもりがないことを表明 | ・イギリス政府が TTP(Trusted Third Party)の提言を発表 | |

| 年 | 月 | 国際的な動向 | 米国の動向 | | 欧州の動向 | 日本の動向 |
|---|---|---|---|---|---|---|
| | 6 | | | | | ・警察庁が「ハイテク犯罪対策重点推進プログラム」を発表<br>－ サイバーポリスの体制確立<br>－ 不正アクセス対策の法整備<br>－ 産業界との連携強化<br>－ 国際捜査協力のルール作成 |
| 1998 | 9 | | ・暗号の輸出規制の緩和策を発表<br>－ 56 ビット DES 相当以下の暗号の包括輸出認可<br>－ 56 ビットを超える強度の暗号についてもケースバイケースで規制を緩和<br>－ 鍵回復政策の簡素化 | | | |
| | 10 | ・Directive 95/46/EC 「個人情報処理における個人保護及び自由移動に係る指令」が発効 | | | | |
| | 12 | ・ワッセナー・アレンジメント総会において、56 ビット以下の共通鍵暗号及び 512 ビット以下の公開鍵暗号の輸出を自由化 | | | | |
| 1999 | 1 | | | | ・フランス政府が国内における暗号法の自由化に関する発表を行い、TTP への鍵寄託義務を廃止 | |

| 年 | 月 | 国際的な動向 | 米国の動向 | | 欧州の動向 | 日本の動向 |
|---|---|---|---|---|---|---|
| | 4 | | | | | ・警察庁がナショナルセンター(HITEC)を設置 |
| | 8 | | | | | ・不正アクセス禁止法公布 |
| | 9 | | ・45 カ国の輸出国リストが廃止され、テロ支援国7カ国以外の全地域に対し、鍵長に無関係に輸出ないし再輸出が可能となる | | | |
| | 10 | ・ISO/IEC SC27 が暗号の本格的な標準化着手を提案 | | | ・暗号標準化プロジェクト NESSIE 立ち上げ | |
| 2000 | 4 | | | | | ・CRYPTOREC が活動を開始 |
| | 10 | | ・EU加盟 15 カ国+8 カ国に対し、暗号解析装置及び同技術以外は許可を要せず輸出が可能となる | | | |
| 2001 | 4 | | ・AES 標準が発表される | | | |
| 2002 | 12 | | ・電子政府法が成立 | | | |
| 2005 | 2 | ・ISO/IEC18033 が順次発行される | | | | |

## 参考文献

参考文献の URL は、2011 年 10 月 30 日現在アクセス可能なものを記述している。また、オンラインでアクセスできない文献については、一般の人がアクセスできる所在場所を記述している。


[1]警視庁「情報セキュリティビジョン策定委員会報告書概要」,1998

URL：http://www.npa.go.jp/cyber/research/h10/secvision/index.htm

本格的なネットワーク社会の到来を間近に控え、犯罪等防止のための情報セキュリティビジョンの策定が急務であり、特に、国際的な整合性に配慮した暗号政策、情報セキュリティ施策の策定が喫緊の課題であるとの認識のもとに、暗号技術に係るセキュリティ上の課題の明確化、諸外国における暗号技術不正利用対策の動向を明らかにし、不正アクセス禁止法・ネットワーク犯罪防止法制の整備の必要性等を提言している。特に、鍵回復制度の整備を唱えている。

[2]警視庁「情報セキュリティ調査報告書」,1997

URL：http://www.npa.go.jp/cyber/research/h9/secrepo/contents.htm

1996 年末の時点での米国の Clipper 政策及び欧州諸国における暗号政策の動向をまとめている。特に Clipper1,2,3 について詳しい。

[3]NIST「SKIPJACK Validation List」,2009

URL：http://csrc.nist.gov/groups/STM/cavp/documents/des/skipval.htm

NISTにより認定されたSKIPJACKアルゴリズム実装製品リスト。2009年5月7日現在、13 製品が登録されている。

[4]NICT「国家と暗号の関わり方に関する海外調査報告書」,2006

URL：http://www2.nict.go.jp/y/y213/cryptrec_publicity/rep_ID0505.pdf

IPA 及び NICT が共同で行っている CRYPTREC（電子政府推奨暗号の安全性評価・監視事業）に資するため、米国、カナダ、イギリス、フランス、ドイツ、オーストラリア、韓国における推奨・標準暗号アルゴリズム及び暗号製品政府調達方針等を調査した。

[5]IPA「暗号技術に係わる政策動向調査（付録 C)」,1999

URL：http://www.ipa.go.jp/security/fy11/report/contents/crypto/crypto/report
/CryptogrphyPolicy/CryptographyPolicyReport.pdf

1999 年 9 月時点で、鍵寄託・鍵回復制度に関する各国の動向をまとめている。調査対象は米国、フランス、ドイツ、イギリス、オランダ、韓国、シンガポール、マレーシアの 8 ヶ国。

[6]外務省「国家による暗号政策」, 外務省調査月報 2001/No.1, 2001

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

1999 年末時点での米国及び EU、フランス、OECD の暗号政策について概説。

[7]NIST「Key Recovery Public Comments Sought on TAC Report」,1999

URL：http://csrc.nist.gov/keyrecovery/

Technical Advisory Committee での作業レポートに対するパブリックコメントを求めたもの。

[8]B.Schneier「The Risks of Key Recovery」,1998

URL：http://www.schneier.com/paper-key-escrow.html

鍵寄託・鍵回復政策におけるリスクを挙げ、慎重な対応を求めた論文。リスクとして、新たな脆弱性（平文に対する新たなパス、内部の不正、新たな攻撃ターゲット、フォワード・シークレシー）、新たな複雑性（規模、運用面での複雑性、鍵回復の正当性）、新たなコスト、鍵回復の粒度と範囲のトレードオフを挙げている。

[9]社会安全研究財団「暗号技術調査研究委員会報告書」,1999

URL：http://www.syaanken.or.jp/02_goannai/08_cyber/cyber_f.htm

民間企業におけるネットワーク利用状況やセキュリティ対策（暗号化、認証機関の利用等）についてアンケート調査を行い、国に対する暗号技術の普及のための施策や認証機関の利用普及方策の提言を行っている。

[10]日本防犯設備協会「情報セキュリティにおける不正行為に関する調査研究報告」,1998

**所在場所：国立国会図書館**

ネットワークの不正アクセスやコンピュータウィルス等、情報セキュリティにおける不正行為を細かく分類し、多くの事例を紹介している。

[11]OECD「Guidelines for Cryptography Policy」,1997

URL：http://www.oecd.org/document/11/0,3343,en_2649_34255_1814731_1_1_1_1,00.html

OECD 暗号政策ガイドライン・アド・ホック専門家会合の副議長を務められた堀部政男教授監訳の日本語訳は次の URL からアクセスできる。

URL：http://www.isc.meiji.ac.jp/~sumwel_h/doc/intnl/recm_crypt.htm

1997 年 3 月に正式勧告された暗号政策ガイドライン。①暗号手法に対する信頼、②暗号手法の選択、③市場主導の暗号手法の開発、④暗号手法に関する諸標準、⑤プライバシー及び個人データの保護、⑥合法的アクセス、⑦責任、⑧国際協力の 8 原則からなる。

[12]「U.S. Electronic Data Security Act of 1997」,1997

URL：http://epic.org/crypto/legislation/edsa_397draft.html

クリントン政権が、鍵回復及び公開鍵証明を行う機関の登録制、暗号製品に鍵回復方式を使用しているかのラベルの貼付、鍵回復機関の他国との相互承認の取り決め締結の交渉を行うこと、などをうたった法案の草案。

[13]富士通「富士通規準セキュリティポリシー 2007」,2007
URL：http://jp.fujitsu.com/solutions/safety/secure/concept/esa/files/ESA1011P.pdf
富士通が ISO/IEC 及び国内標準をもとに規定した情報セキュリティポリシー。セキュリティ統制、不正アクセス対策、情報漏洩対策、ウィルス対策、コンテンツセキュリティ対策、フィジカルセキュリティ、電子認証基盤、電子文書保証、Web アプリケーションセキュリティについて規定している。

[14]U.S.A. White House「Clipper Chip White House Statement」,1994
URL：http://epic.org/crypto/clipper/white_house_statement_2_94.html
1994 年 2 月 4 日に NIST が Clipper1 のコンセプトを EES(Escrowed Encryption Standard)として認定した旨の米国連邦政府からの発表文。

[15]J.He, E.Dawson「A New Key Escrow Cryptosystem」, Lecture Notes in Computer Science, Volume 1029/1996, pp.105-114, 1996
所在場所：国立国会図書館
初期の EES(Escrowed Encryption Standard)の弱点として指摘された点に対する対応策を記す。

[16]S.J.D.Phoenix「Cryptography, trusted third parties and escrow」, BT Technology Journal archive Volume 15 Issue 2, April 1997, pp.45-62, 1997
所在場所：国立国会図書館
共通鍵暗号（特に DES）、公開鍵暗号、デジタル署名、TTP、鍵寄託システムについて、技術的観点から詳説。

[17]P.G.Neumann「Security Risks in Key Recovery」,1997
URL：http://www.csl.sri.com/users/neumann/judiciary.html
鍵回復システムを導入することによる潜在的な技術的リスクを列挙し、国として世界規模の鍵回復基盤を構築する下地はできておらず、拙速に進めるべきではないことを記した論文。

[18]「The Economic Impact of the Regulation of Investigatory Powers Bill」, An independent report prepared for the British Chambers of Commerce, 2000
URL：http://is2.lse.ac.uk/research/BCC_RIPA.pdf
英国政府が 1999 年 11 月に法案提出した Regulation of Investigatory Powers (RIP)法案に対して、英国の産業、司法、国民生活に多大な負の影響を与えることを警告した学者達の論文。

[19]T.Beth etc「Towards Acceptable Key Escrow Systems」, Proceedings of the 2nd ACM Conference on Computer and Communications Security, pp.51-58, 1994

URL：http://delivery.acm.org/10.1145/200000/191191/p51-beth.pdf?ip=164.71.1.222
&CFID=42071470&CFTOKEN=98571158&_acm_=1315984417_
559ea640e20b1d9d00eeda24f2d98c59
No.21 で示された Clipper Chip の弱点を補強した鍵寄託方式を示す。

[20]D.E.Denning「The US Key Escrow Encryption Technology」, Computer Communications, Vol.17, No.7, July 1994, pp.453-457, 1994
所在場所：国立国会図書館
Clipper Chip と SKIPJACK アルゴリズムの概要について記した論文。

[21]Matt Blaze「Protocol Failure in the Escrowed Encryption Standard」,1994
URL：http://www.windowsecurity.com/uplarticle/2/eesproto.pdf
Clipper Chip の LEAF の部分を改造することにより、法執行機関による合法的アクセスができないような暗号通信が可能であることを示す。

[22]B.Gladman「Meeting the Needs of Users or Key Escrow in Disguise?」,1997
URL：http://web.archive.org/web/20060218165438/http://jya.com/bg/key_escrow.pdf
国が主導して進める法執行機関による合法的アクセス手段としての鍵回復と、民間のロストキー対策として利用する鍵回復を、蓄積データに関するものと通信に関するものに整理した上で、鍵回復は基本的には政府ではなく、企業を含めた民間に任せるべきと主張した論文。

[23]F.Piper「Trusted Third Parties for Secure Electronic Commerce - Are They Needed?」, Proceeding ACISP '97 Proceedings of the Second Australasian Conference on Information Security and Privacy, Lecture Notes in Computer Science, 1997, Volume 1270/1997 p.1, 1997
所在場所：国立国会図書館
信頼される第三者機関の必要性を説き、安全な電子商取引における TTP 利用の役割について述べる。

[24]前川徹「米国の暗号技術輸出規制の変遷と展望」, 情報処理学会研究報告. EIP, [電子化知的財産・社会基盤] 99(11) pp.139-146, 1999
URL：http://ci.nii.ac.jp/els/110002675688.pdf?id=ART0002947546&type=pdf&lang=jp&host=cinii
&order_no=&ppv_type=0&lang_sw=&no=1320038228&cp=
米国の暗号技術輸出規制の変遷について、Clipper 政策とも絡ませながら、1998 年 12 月のワッセナー・アレンジメントにおける輸出緩和の決定までを記している。

[25]岩下直行、宇根正志「キーリカバリー構想を巡る最近の情勢について」,1997
URL：http://www.imes.boj.or.jp/research/abstracts/japanese/97-J-08.html
1997 年 5 月時点で、鍵回復構想の歴史、各国の動向、鍵回復システムの方式、法執行機

関による合法的アクセスの回避策について記述。特に、Clipper 1, 2, 3、鍵回復システムの方式、合法的アクセスの回避策について詳しい。

[26]NIST「Issues:Export of Software Key Escrowed Encryption」, Discussin Paper #1 ,Key Escrow Issues Meeting, August 24 ,1995
URL：http://csrc.nist.gov/keyrecovery/september_issues_mtg/paper1.html
1995 年 8 月の Clipper 2 の発表に伴い、鍵寄託システムで想定される課題をまとめ、解決策を求めた。

[27]NIST「Discussion Issues:Desirable Characteristics for Key Escrow」, Discussin Paper #1 ,Key Escrow Issues Meeting, August 24 ,1995
URL：http://csrc.nist.gov/keyrecovery/september_issues_mtg/paper2.html
1995 年 8 月の Clipper 2 の発表に伴い、鍵寄託機関のあり方について想定される課題をまとめ、解決策を求めた。

[28]郵政省「21 世紀デジタル社会の暗号政策への提言」, 暗号通信のあり方に関する研究会　報告書, 1999
URL：http://warp.ndl.go.jp/info:ndljp/pid/258151/www.soumu.go.jp/joho_tsusin
/policyreports/japanese/group/internet/ninshou/index.html
デジタル社会において、電子商取引にとどまらず、行政、交通・物流、医療、電子文化などの様々な分野で暗号が重要な役割を担うことを示し、この時点での技術的な動向や海外の政策的な動向をまとめている。鍵寄託・鍵回復制度や電子署名・電子認証についても述べ、特に電子署名の法的位置づけや認証機関に対する資格制度などの法整備を提言している。

[29]IT 推進本部「高度情報通信社会推進に向けた基本方針」, 高度情報通信社会推進本部決定, 1998 年 11 月 9 日, 1998
URL：http://www.kantei.go.jp/jp/it/981110kihon.html
高度情報通信社会の推進に向け、「民間主導」「政府による環境整備」「国際的な合意形成に向けたイニシアティブの発揮」の行動原則のもとに、電子商取引等推進のための環境整備や公共分野の情報化等の 10 項目の課題と対応方針を示した。

[30]横山恭三「米国のサイバー・カウンターインテリジェンスについて」, 防衛取得研究（第四巻第四号）（2011 年 3 月号）, 2011
URL：http://www.bsk-z.or.jp/kakusyu/pdf/110328kenkyureport_23_03.pdf
ハッカーやテロリストなどがコンピュータ・ネットワークを利用して侵入しようとする行為の探知、敵対活動の防止、法執行機関との協力のもとでの敵対者の逮捕を行う活動であるサイバー・カウンターインテリジェンスにおける主要な情報収集手段である通信傍受について、米国の状況を紹介した。

[31]警察庁「諸外国における産業界等との連携手段の法的側面」, 情報セキュリティ対策会議報告書　資料編１, 2001
URL：http://www.npa.go.jp/cyber/csmeeting/h13/pdf/pdf13b.pdf
米国、イギリス、ドイツ、フランスにおける情報セキュリティに対する取り組み、法執行機関との連携状況、産業界における連携状況、人材育成、国・官公庁の取り組みに対する評価を調査した。

[32]社会安全研究財団「アメリカにおけるハイテク犯罪に対する捜査手段の法的側面報告書」,2004
URL：http://www.syaanken.or.jp/02_goannai/08_cyber/cyber1603_01/pdf/1603_01all.pdf
米国司法省のコンピュータ犯罪及び知的財産部刑事課の作成した「犯罪捜査におけるコンピュータ捜索・差押及び電子的証拠の獲得」と題するマニュアルを翻訳したもの。

[33]Caryn Mlden「カナダにおけるプライバシー」, 電子政府・電子自治体のプライバシーに関する調査研究報告書, 2003
URL：http://joi.ito.com/privacyreport/Contents_Distilled/JapaneseSection
/Canada_J_p06-72.pdf
カナダにおける法体系、プライバシー技術の状況、民間部門や公的部門における活動状況などを詳細にまとめたもの。

[34]IT 戦略本部「電子商取引等の推進に向けた日本の取り組み」, 電子商取引等検討部会報告書, 1998 年 6 月, 1998
URL：http://www.kantei.go.jp/jp/it/commerce/980622honbun.html
電子商取引等の推進に向けて、電子認証、プライバシー保護、違法・有害コンテンツ対策、消費者保護、セキュリティ・犯罪対策、電子決済・電子マネー、知的財産権、ドメインネーム、税、関税などの観点で課題を挙げ、対応策を提案している。

[35]警察庁「ハイテク犯罪の現状と警察の取組み」, 平成 10 年警察白書 第 1 章, 1998
URL：http://www.npa.go.jp/hakusyo/h10/h10index01.html
世界的なハイテク犯罪の状況と各国の取組みを紹介した上で、法や組織の整備を提言している。特に、認証機関や鍵回復機関の適格性及び業務の適正を確保する仕組みの導入について、法制面を含めた検討を行っているとしている。

[36]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 SCIS97－１A 電子情報通信学会 1997 年 1 月 29 日, 1997

[37]石崎靖敏「諸外国及び国際機関の暗号政策動向」, 電気通信 60（通巻 609）pp.17-21, 1997 年 9 月 1 日号, 1997
**所在場所：国立国会図書館**

米国における暗号政策、議会及び司法の状況、欧州諸国における暗号政策の状況などを詳説している。

[38]山根信二、村山優子「暗号技術を位置づける社会的枠組みについての考察」, 情報処理学会論文誌 Vol.42 No.8, pp.1975-1982, 2001
URL：http://ci.nii.ac.jp/els/110002725953.pdf?id=ART0003014413&type=pdf&lang=jp&host=cinii&order_no=&ppv_type=0&lang_sw=&no=1316149984&cp=
2001 年時点で、鍵寄託・鍵回復の枠組みは既に「死んでしまった過去の話」と認識した上で、暗号技術の議論の新たな枠組みとして、DVD プロテクト破りに象徴される暗号解析や著作権法との関係について論じている。

[39]須田祐子「暗号アルゴリズムの国際標準化」, 国際政治 第 156 号, 2009
URL：http://www.jstage.jst.go.jp/article/kokusaiseiji/2009/156/156_107/_pdf/-char/ja
1990 年代の米国及び OECD、欧州における暗号政策の動向を整理した上で、ISO における暗号アルゴリズムの標準化の動向について論じている。

[40]EPIC「Cryptography and Liberty 2000」,2000
URL：http://www.stanford.edu/class/msande91si/www-spr04/readings/week6/epic.htm
2000 年時点における米国の鍵寄託・鍵回復政策の動向や OECD、ワッセナー・アレンジメントの動きを整理するとともに、人権擁護団体である EPIC の立場から、主要国の暗号政策を「赤（危険）」「黄（注意）」「青（良好）」の 3 段階で評価している。

[41]土屋大洋「情報通信分野における国家モデルに基づいた情報化政策に関する研究」, 学位請求論文, 1999
URL：http://web.sfc.keio.ac.jp/~taiyo/hakuron/dissertation_tsuchiya.pdf
筆者の博士論文。欧米諸国の暗号政策について詳しく論じている。

[42]すずきひろのぶ「時代遅れなキーエスクロー」, インターネットマガジン 1999 年 9 月号, pp.330-331, 1999
URL：http://webcache.googleusercontent.com/search?q=cache:MCv4ytM930sJ:www.pp.iij4u.or.jp/~h2np/docs/KeyEscrow.html+%E3%82%AD%E3%83%BC%E3%83%AA%E3%82%AB%E3%83%90%E3%83%AA%E3%83%BC&cd=28&hl=ja&ct=clnk&gl=jp&lr=lang_ja&source=www.google.co.jp
鍵寄託・鍵回復制度に対する日本の技術者からの否定的な意見。

[43]アメリカ自由人権協会「通信回線の中のビッグブラザー」,1998
URL：http://www.jca.apc.org/privacy/19990813/brother.html
アメリカ自由人権協会(ACLU)が発表した鍵寄託・鍵回復制度に対する反対意見。

[44]「ブルース・シュナイアー、インタビュー」,2003
URL：http://metamemos.typepad.com/gt/2003/08/post.html
著名な暗号技術者である B.Shneier が暗号技術や暗号政策に対する率直な意見を述べたもの。

[45]本間雅雄「暗号政策の議論を深めよう」, オペレーションズ・リサーチ Vol.579, 1997 年 9 月号, 1997
URL：http://www.orsj.or.jp/~archive/pdf/bul/Vol.42_09_578.pdf
日本において暗号関係の法整備が遅れていることを危惧し、早期の法整備をもとめたもの。

[46]N.Wanchek「Who is a New Special Envoy for Cryptography?」, WIRED 1996 年 11 月 19 日, 1996
URL：http://www.wired.com/politics/law/news/1996/11/521
暗号特使に指名された D.Aaron について紹介している WIRED 誌の記事。

[47]BIS「Comments by Ambassador David Aaron Special Envoy for Cryptography」, RSA Data Security Conference in San Francisco, 1997 年 1 月 28 日, 1997
URL：https://www.bis.doc.gov/encryption/aaron.htm
暗号特使に指名された D.Aaron が、1997 年 1 月 28 日に San Francisco で行われた RSA Data Security Conference での講演。

[48] 情報処理学会「IT Security の最近の動向と標準化の課題」, 情報規格調査会 標準化活動トピックス, 1996
URL：http://www.itscj.ipsj.or.jp/topics/tp32.html
SC27 専門委員会苗村委員長（当時）による情報セキュリティに関わる ISO/IEC JTC1 SC27 委員会の活動内容の紹介。

[49] FIPS「FIPS-185 ESCROWED ENCRYPTION STANDARD」,1994
URL：http://csrc.nist.gov/publications/fips/fips185/fips185.txt
SKIPJACK を用いた鍵寄託に関する連邦情報処理標準規格。

[50] NIST「SKIPJACK and KEA Algorithm Specifications」, 1998
URL：http://csrc.nist.gov/groups/STM/cavp/documents/skipjack/skipjack.pdf
SKIPJACK と鍵寄託に関する仕様書。

[51]米国連邦議会上院司法委員会「Encryption, Key Recovery, and Privacy Protection in the Information Age」, 1997
URL：http://www.loc.gov/law/find/hearings/pdf/00140120273.pdf
米国連邦議会（第 105 回）上院司法委員会の暗号、鍵回復、プライバシー保護に関するヒ

アリングの資料。キー・リカバリー・アライアンスの活動についての資料が添付されている。

[52]NIST「Encryption Key Recovery ： Off the Launch Pad」, 1998
URL：http://csrc.nist.gov/nissc/1998/proceedings/panelG2.pdf
1998 年 10 月に米国バージニア州で行われた NIST 主催の第 21 回 NISSC（National Information Systems Security Conference）のパネル資料。キー・リカバリー・アライアンスの活動についての資料が添付されている。

[53]A.Shamir「How to Share a Secret」, Communications of ACM, Vol.22 Number 11, 1979
URL：http://securespeech.cs.cmu.edu/reports/shamirturing.pdf
(k,n)しきい値秘密分散法について記した歴史的論文。

[54]CRYPTREC「ID ベース暗号に関する調査報告書」, CRYPTREC ID ベース暗号調査 WG, 2009
URL：http://www.cryptrec.go.jp/report/c08_idb2008.pdf
ID ベース暗号及びペアリング暗号の技術概要、安全性評価、実装動向をまとめた報告書。

[S1]谷田 武、土屋 宏嘉、道明 誠一、鳥居 直哉、満保 雅浩、岡本 栄司「鍵回復システムの設計と実装」(1996 年度 IPA 事業関係），情報処理学会　全国大会講演論文集 第 55 回平成 9 年後期(3), 645-646, 1997-09-24, 1997
URL：http://ci.nii.ac.jp/els/110002896679.pdf?id=ART0003226266&type=pdf&lang=jp&host=cinii&order_no=&ppv_type=0&lang_sw=&no=1317194666&cp=

[S2]田渕治樹、谷田武、土屋宏嘉、道明誠一、鳥居直哉、満保雅浩、岡本栄司「プライバシー保護に適した鍵回復方式の研究開発」(1996 年度 IPA 事業関係），創造的ソフトウエア育成事業編，情報処理振興事業協会, 1998
URL：http://web.archive.org/web/20010612204431/http://www.ipa.go.jp/NBP/CREC/Data/2-066/2-066.pdf

[S3]道明誠一、梅木久志、土屋宏嘉、川井亨、谷田武、鳥居直哉、満保雅浩、岡本栄司「商用目的に適した鍵回復システムの開発」(1996 年度 IPA 事業関係），情報処理学会　全国大会講演論文集 第 56 回平成 10 年前期(3), 398-399, 1998-03-17, 1998
URL：http://ci.nii.ac.jp/els/110002896991.pdf?id=ART0003226583&type=pdf&lang=jp&host=cinii&order_no=&ppv_type=0&lang_sw=&no=1317195294&cp=

[S4]奥村悌二、山崎正史、大竹洋一、木村和人、西村崇「暗号データ回復システム」(1997 年度 IPA 事業関係），NEC 技報 Vol.51 No.9, 1998
**所在場所：国立国会図書館**

[S5]新保淳、佐野文彦、丹羽朗人「暗号技術と鍵回復システム」」(1998 年度通産省事業関係)，東芝レビュー Vol.54 No.7, 1999
**所在場所:国立国会図書館**

[H1]鳥居直哉氏ヒアリングメモ,2011
[H2]木村道弘氏ヒアリングメモ,2011
[H3]遠藤直樹氏ヒアリングメモ,2011
[H4]佐々木良一教授ヒアリングメモ,2011
[H5]今井秀樹教授ヒアリングメモ,2011
[H6]辻井重男教授ヒアリングメモ,2011
[H7]才所敏明氏ヒアリングメモ,2011
[H8]山崎正史氏ヒアリングメモ,2011