# キーリカバリ、キーエスクロウ、第三者信託方式による暗号のリスク 1998年増補版

# (The Risks of Key Recovery, Key Escrow, and Trusted Third-Party Encryption, 1998 Edition)


Hal Abelson [1] Ross Anderson [2] Steven M. Bellovin [3]

Josh Benaloh[4] Matt Blaze[5] Whitfield Diffie[6]

John Gilmore[7] Peter G. Neumann[8] Ronald L. Rivest[9]

Jeffrey I. Schiller[10] Bruce Schneier[11] 訳：山形浩生[12]



Final Report——27 May 1997, Revised 10 June 1998 [13]



[1]MIT Laboratory for Computer Science/Hewlett-Packard, <hal@mit.edu>

[2]University of Cambridge, <ross.anderson@cl.cam.ac.uk>

[3]AT&T Laboratories - Research, <smb@research.att.com>

[4]Microsoft Research, <benaloh@microsoft.com>

[5]AT& T Laboratories - Research, <mab@research.att.com>

[6]Sun Microsystems, <diffie@eng.sun.com>

[7]<gnu@toad.com>

[8]SRI International, <neumann@sri.com>

[9]MIT Laboratory for Computer Science, <rivest@lcs.mit.edu>

[10]MIT Information Systems, <jis@mit.edu>

[11]Counterpane Systems, <schneier@counterpane.com>

[12]Always On My Own, <hiyori13@mailhost.net>


[13]この文書の原文最新版は、World-Wide-Web 上では <http://www.cdt.org/crypto/risks98/> にある。また 1997 年のオリジナル版はhttp://www.crypto.com/key_study/、PostScript 形式では<ftp://research.att.com/dist/mab/key_study.ps>、ASCII テキスト形式では<ftp://research.att.com/dist/mab/key_study.txt>にある。

## 概 要

新技術がもたらした変化の中で隠密捜査を行おうとする政府機関によって、最近になってさまざまな「キーリカバリ」「キーエスクロウ」「第三者信託」方式の暗号システムに求められる各種条件が提案されてきている。本報告は、こうした要件がもつ基本的な性質について検討し、暗号化キーへの政府アクセスを可能とするシステム導入の技術的なリスク、コスト、およびそれがもたらす結果についてまとめる。[1]


[1] Reprinted and translated with permission from the authors and *World Wide Web Journal*, Vol.2 No.3. 

# 目 次

# はじめに

## 序

初版発表の 1997 年から 1 年たったが、本報告の基本的な知見はまったく変わっていないし、それを深刻に疑問視するような議論も提出されていない。その知見とはつまり、暗号化されたデータや通信に対して政府の隠密アクセスを可能にするようなキーリカバリ・システムの導入は、多大なリスクとコストを伴うものだ、ということである。このリスクやコストは、多くの暗号利用にとって適切でないと考えられ、したがって各種政府が広範なキーリカバリを推奨するような政策を検討する際には、これらの点についてもっと慎重かつ万全な検討を行うことが必要である。

われわれの 1997 年の「リスク」報告は、公開の技術的な議論と分析を奨励するように考えて書かれたものだった。そうした議論や分析は、大規模なキーリカバリ・システム導入につながるような、責任ある政策決定に先だって絶対に必要なものだとわれわれは判断する。キーリカバリから生じる問題には、経済的にも社会的に政治的にも重要なものがたくさんある。しかしこの報告の分析は、政府のアクセス仕様を満たすように設計されたキーリカバリ・システムの導入によって生じる、技術的な問題に限定されていた。1998 年半ば現在、こうした技術的な問題点をとりあげた本質的な反論は一つも提出されていない。

この 1 年間に、商業・業務目的のキーリカバリ・システムを設計しようという試みはあった。しかしそれらは、政府の要求仕様に応えるようなスケールと方法での導入から生じるような問題点を減らすものではない。安全性の高いキーリカバリ・システムの設計はいまだに技術的に見てもハードルが高く、キーリカバリ・システム導入のリスクやコストについてはほとんどわかっていない。いちばん大きな問題は、政府によるアクセスニーズのため、キーリカバリ・システムへの要求事項が増えてしまうということである。政府のアクセスニーズとは、たとえば隠密アクセス、あらゆる場面での採用、平文への迅速なアクセスなどである。多くの面から考えて、こうした追加の要求事項がキーリカバリのコストやリスクを大幅に増大させるであろう。

過去 1 年で、コンピュータや通信を守るための暗号の重要性に対する認識は、一般社会でも産業界でも高まってきた。現在導入されている暗号システムは、防犯や犯罪摘発の妨げとなるどころか、それを支援している。暗号は、防犯警報やキャッシュマシン、郵便仕訳計量装置や各種の自動販売機、チケット販売機などの悪用や不正利用を防ぐ役に立っているし、ネット上でクレジットカード取引を保護し、デジタルオーディオやデジタルビデオの不正コピーを防止することで電子商取引にも利用されている。しかしながら、暗号化（そしてその他の情報保護メカニズム）の導入はまだ部分的なものにとどまっている。キャッシュマシンの取引はほとんどが暗号化されて保護されているが、銀行職員が手で行う窓口取引（扱う金額は機械よりずっと大きいことも多い）は保護されていない場合がほとんどだ。インターネット上の電子メールのほとんどは、いまだに「すっぴん」状態で送られており、簡単に傍受できてしまう。アメリカでの携帯電話による通話のほとんどは、いまだに強力な暗号を使わないまま送信されている。この状況は、他分野でも似たり寄ったりである。

いまでも法執行機関や諜報関連分野で活動する人々は、エスクロウ（第三者預かり）なしの暗号

方式が広く普及してしまうことを懸念する声をあげ続けている。こうした人々は同時に、「重要性の高い（criticalな）インフラ」の脆弱性について、ますます懸念を表明するようになってきた。しかしながら、情報インフラに政府アクセス・キーリカバリシステムを大規模に挿入すれば、犯罪や情報テロの可能性は減少するどころか拡大するというリスクはきわめて大きい。重要性の高いインフラや事業上のデータへのアクセスを認められた人間の数を増やせば増やすほど、技術的にも、誤りを悪用するような手段でも、あるいは汚職などを通じても、攻撃の可能性は高まってしまう。さらに、キーリカバリの要件が暗号化を面倒で高価なものにしてしまったら、ますます脆弱になりつつあるコンピュータや通信ネットワークにおける暗号の導入を阻害したり、遅らせたりするといった影響も考えられる。

キーリカバリや第三者信託システムの技術的な問題点は、1998年になってもわれわれの1997年の分析からほとんど変わっていない。キーリカバリがどのようにして、なぜ法執行機関にとっては有用であり得るのか、そして同等かそれ以上のメリットをもたらすような、キーリカバリ以外の方式があるのかどうかについては、われわれは特に触れていない。しかしながら、キーリカバリで予想されるコストとリスクは、特に法執行機関が望むほどのスケールで導入された場合には、きわめて莫大なものとなる。それらの莫大なリスクやコストを上回るほどのメリットがあるということを論じるのは、キーリカバリ支持者たちの役目となる。

## 背景

暗号政策は、科学的、技術的、政治的、社会的、事業的、経済的な側面をもつ複雑な分野である。われわれの報告は、キーリカバリ問題の技術面と経済面に特化している。特に注力したのが、政府の仕様を満たす安全なキーリカバリシステムが技術的に可能か、そして可能であるなら、そうしたシステムがどの程度の追加コストやリスクを伴うものと期待されるか、という点であった。

この報告で扱う「キーリカバリ」システムは、暗号化されたトラヒックの平文に対し、例外的なアクセスを得るためのメカニズムが存在しているという点に特徴がある。キーリカバリは、広範なアクセス要件に対応できる、たとえばある企業がキーをなくしたときにも、自社の暗号化されたアーカイヴへのアクセスが妨げられないようにするためのバックアップ機構から、暗号化された電話での会話を盗聴した法執行機関が、その内容に隠密にアクセスできるようにするといった用途まで、用途は多い。キーリカバリ・システムの設計、実装、運用に内在するコストやリスク、複雑性の多くは、そのシステム設計時に根拠となったアクセス要件に左右される。

われわれが特に採りあげたのは、政府のアクセス仕様を満たすように設計されたキーリカバリ・システムである。政府のアクセス仕様は、いくつかの重要な点で民間業務上や個人レベルの暗号利用者のニーズとは大きくくいちがっている。

1. **エンドユーザに知られずに、同意を得ることもなくアクセス可能であること。**——民間ユーザで、自分の保護している平文データやキーを復元するときに隠密性を必要とする者はほとんどいない（かえっていやがる者が多い）。民間企業でのアクセス規則は通常は明確になって

いるし、濫用、誤用に対して監査が重要な安全弁となっている。政府の仕様は、この重要なセキュリティ慣行を阻害するようなメカニズムを必要とする。

2. **ほぼ全面的な採用。**——政府はあらゆる暗号化の利用について、キーリカバリを使わせようとしている。それがエンドユーザにとってメリットを持っているか、キーリカバリの使用にその状況で意味があるかといった点はまったく考慮されていない。実は、多くのアプリケーションやユーザにとって、キーリカバリはほとんど、あるいはまったく必要とされていないのである。たとえば、暗号化された通信のリカバリ需要は、民間企業はほとんど持っていない。そして一部の通信プロトコルに対するキーリカバリの設計と分析は、ことさら難しい。

3. **平文への迅速なパス。**——法執行機関は、高速な（ほとんどリアルタイムの）一日 24 時間、年 365 日にわたる平文アクセスを要求している。これは商業キーリカバリシステムに内在するリスクの一部を防止できるような、総合的な安全策の導入を不可能にしている。

こうした特殊な要件は、この報告で指摘したリスクやコストを大幅に増大させるものである。業務上のニーズに対応すべく設計されたキーリカバリシステムにも、それなりのコストとリスクが伴う。しかしわれわれは、これら政府アクセス・システムの特殊な要件——あらゆる暗号化データへの迅速かつ隠密なアクセス——から生じる影響に注力して議論を行っている。

## 1997 年版に対する批判

すでに述べたように、1997 年報告でわれわれが指摘した問題点について、本質的な反論はいまのところ一つも発表されていない。われわれが知る範囲でわずかながら批判は寄せられたものの、そのいずれも問題を技術的に掘り下げて議論することを回避しており、さらにわれわれの指摘した点も歪曲している。

1. **「この報告は、単一の巨大な中央集中型インフラを前提とした議論でしかない」**——キーリカバリの提案の一部は中央集中型ではある。しかしわれわれの報告はキーリカバリすべてを検討対象としている。それが単一の政府主導インフラであろうと、多数の分散化された民間システムだろうと成立する議論を展開したものである。報告で指摘したリスクやコストは、ほとんどがキーリカバリの機能的な要件（そして特に、政府がもとめるような規模）から生じるものであり、その実装方法から生じるものではない。

2. **「この報告は、キーリカバリは現実的ではないと主張するが、キーリカバリ連合（Key Recovery Alliance, KR**——確かに一部の企業はキーリカバリ製品を開発している。しかしそうした製品が、政府の求めるようなあらゆる場面での利用を達成できるかどうかは、まったくわからない。こうしたシステムの多くは狭い範囲での利用に向けたものである。

3. **「キーリカバリのメリットは、そのコストを上回るものだ」**——確かにキーリカバリは、一部のユーザや政府にとってはメリットがあるかもしれない。最終的にそうしたメリットをコスト

とはかりにかけるのは、市場と政策立案者の行うべきことであり、本報告の議論をはずれる。本報告では単に、そのコストが並々ならぬものになる理由を説明しようとしたにすぎない。

## キーリカバリ：1998 年時点の状況

1998 年半ば現在までに、政府、産業、学術分野で、政府仕様を満たすようなキーリカバリ・システムを仕様化し、プロトタイプをつくり、標準化しようという試みが広範に見られてきた。産業界の努力の一部は、将来製品にキーリカバリ機能を設計して導入することを約束した企業に対し、輸出の扱いを優遇するというアメリカ政府の政策に刺激されたものであり、さらにイギリス政府が、認証機関のライセンシングとキーリカバリ・ソフトの利用とを結びつけようとする動きを見せたことも手伝っている。

しかしこうしたインセンティブや、研究開発チームによる強い興味や努力にもかかわらず、産業界も政府も、政府の要求を完全に満たし、しかも暗号ユーザのセキュリティ要件やコスト要件も完全に満たすようなキーリカバリのアーキテクチャをいまだに生み出していない。

既存のキーリカバリ製品は、民間商業の要件と政府仕様との対立を解決するものではない。政府の圧力がなければ、市販キーリカバリ機能は、その利害の性質からして、おもに暗号化された形のみで保管されているデータに、絶えず確実にアクセスできるという保証に対し、かなりのマージンを支払う用意のある事業に向けたものとなる。キーリカバリ製品を必要とする機関の中にあってさえ、多くの暗号利用（たとえば通信トラヒックに対するもの）は、リカバーの必要がないと事前にわかるので、キーリカバリシステムを使うような設計はなされない。

別の問題として、安全で経済的なキーリカバリ・システムのほとんどは、政府が捜査のために必要としている、リアルタイムの第三者による隠密アクセスをサポートしていない、ということがある。特に、個人による「自己エスクロウ」は政府のアクセス要求にはマッチしていない。各種の政府の要求に含まれた、第三者によるグローバルに広がったアクセスという性格は、企業内部のオフライン・リカバリ設備に比べて、キーリカバリシステムをずっとむずかしく、高価で、リスキーな提案にしてしまっている。たとえば、ほとんどの組織はバックアップを平文のままで、磁気媒体に保存して物理的に保護された場所に保管している。同じように、暗号化されたデータを保管している組織は、バックアップ用のキーを銀行の金庫の保管箱に保存しておくのが、いちばんよいだろうと当然考えられる。しかしながらほとんどリアルタイムのアクセスが要求されるために、このようなアプローチはいかに適切でしっかりしたものであろうと、排除されてしまう。

アクセス時間上の要件は、すべて特別なリスクを伴う。特にそれは、ある種のネットワーク技術を必要とするのが普通である。こうしたネットワークは多数の法執行機関をさまざまなキーリカバリ・センタと結ばなくてはならず、安全なものにするのがきわめて難しい。アメリカでは現在、電話網や送電グリッド、銀行ネットワークや航空管制システムなど重要性の高いインフラの安全性の問題について関心が高まっている。これはまさに、キーリカバリでのリスク管理の問題を裏付けるものでもある。こうした重要性の高いインフラを支持するシステムは、ますますオープンネット

ワークや情報システムに頼るようになってきており、現在も将来も、暗号の利用においていちばん重要なアプリケーションとなる。キーリカバリによって導入される複雑さとリスクの増加は、暗号によって保護される重要なインフラを、こうしたシステムに対していちばん深刻な脅威となる高度な攻撃者に対し、ずっと脆弱なものにしてしまう。

この報告の 1997 年版では、政府アクセス式キーリカバリを安全に建設・運用するのを困難で高価にしてしまう複雑さやリスクやコストの多くが、まさに政府の要求仕様そのものから生じていることを見てきた。これは、個別システムの工学的な細部とはほとんど関係ない。なんらかのアクセス方針にしたがって、うまくキーや平文をリカバーするような小規模システムを設計・実装するのは難しいことではない。実際、多くの組織は自分たちのデータをずっとアクセス可能にしておくための、何らかの方式をすでに持っている。難しいのは、大規模なシステム、またはシステムのシステムが、うっかりまたは悪意によってデータをもらさないことを確実にすることなのである。

輸出規制緩和のためのキーリカバリシステム用につくられた政府仕様は、承認されたときにはキーが確実に回復できるという簡単な方の問題にだけ集中している。不正なデータ公開を確実に防ぐという、ずっと難しい問題については、とりあげていないし手法もあげていない。だから、輸出向けの政府仕様を満たすキーリカバリシステムのプロトタイプを設計・構築しても、そのシステムが安全に、経済的に、大規模に、受け入れがたい新たなリスクをもたらさずに運用できることを実証するには十分ではない。提案されたシステムを評価するなら、どんなものでも設計、実装、運用、政策上のさまざまな考慮事項を検討しなくてはならない。

1998 年半ば現在において、必要とされるような分析を経たキーリカバリ提案は、われわれの知るかぎりでは一つもない一方で、われわれの報告でも述べたように、暗号学と高安全システム工学の最先端の状況から見て、政府アクセス式キーリカバリは大規模で経済的で安全な暗号システムとは相容れないと考えるべき理由は、きわめて説得力が高いのである。

## Executive Summary

新技術がもたらした変化の中で隠密捜査を行おうとする政府機関によって、最近になってさまざまな「キーリカバリ」「キーエスクロウ」「第三者信託」方式の暗号システムに求められる各種条件が提案されてきている。本報告は、こうした要件がもつ基本的な性質について検討し、暗号化キーへの政府アクセスを可能とするシステム導入の技術的なリスク、コスト、およびその結果についてまとめる。

法強制機関の要求仕様にしたがった、キーリカバリに基づく暗号化インフラの導入は、エンドユーザにとってのセキュリティを大きく犠牲にするとともに、そのコストを増大させる結果となる。こうした仕様が要求するのに十分な技術的な裏付けを提供できる、セキュリティの高いコンピュータ通信インフラを整備するのは極度に複雑となり、現在のこの分野における経験や能力をはるかに上回るものである。こうしたインフラが仮に整備できたとしても、このような運用環境のリスクとコストは、最終的に容認しがたいほど高いものになってしまうかもしれない。さらに、これ

らのインフラは一般に、人間側の信頼水準が極端に高くなければ成立しえない。

こうした困難は、各種キーリカバリ式暗号化システムで提案されている、政府からの基本的なアクセス要件から派生するものである。これらの困難は、リカバリシステム自体のデザインがどうであっても存在する——それが個人キー暗号を使おうと、公開キー暗号を使おうとも：そのデータベースが秘密共有技術を用いて分割されていようと、単一の物理的に強固な高セキュリティ施設で維持管理されていようとも：リカバリサービスが個人キーやセッションキーを提供する場合でも、あるいはデータを必要に応じて解読するだけであっても：そして単一の集約化されたインフラを使おうと、多数の分散化されたインフラを使おうとも、あるいは複数の方式の集合を採用しようとも。

あらゆるキーリカバリシステムは、取り扱い要注意でありながら容易に入手可能な秘密キー、またはそうしたキーの束を必要とし、しかもそれは長期にわたってセキュリティの高い形で管理されなくてはならない。こうしたシステムは、キーの所有者への通知を一切行わずに、法執行機関が解読用情報を迅速にアクセスできるようにしなくてはならない。こうした基本的な要件のため、キーリカバリ一般が困難かつ効果になってしまう——そしておそらくは、多くの利用分野や多くのユーザにとってはあまりにセキュリティが低いか、または極度に高価についてしまう。

輸出規制、輸入や使用規制、国際標準などによってキーリカバリ暗号方式を広く使うように強制しようとするなら、こうした要因を考慮にいれて検討しなくてはならない。公共は、政府アクセスによるキーリカバリを導入する前に、コストと便益を十分に考える必要がある。グローバルなキーリカバリ用インフラを導入すれば、新しいセキュリテイ上のリスクを持ち込んだり、巨額の投資（直接的なものと間接的なものをあわせると、下手をすれば何十億ドル）をつぎ込むことが必要になるからである。

## グループの目的

この報告は、アメリカをはじめとする各国の政府から提出されている、第三者が解読キーをアクセスできるようにするための、議論の余地の大きい「キーリカバリ」システム導入案が持つ、技術的な意味合いについて研究してみようという共同作業から生まれたものである[2]。こうした政策のもつインパクトについて考察をおこなうにあたり、われわれは可能な限り、個々の暗号化スキームや特定の政府案をとりあげたりはしないようにした。むしろ、各政府から表明されている要求（これは暗号ユーザが求めるような条件とは別のものである）を満たすために必要となるキーリカバリの基本的な要素を広く見渡そうとしている。

この報告は、政府の**要求仕様**を満足させることによる一般的なインパクトを検討しており、それを満たす特定のキーリカバリシステムや提案の長所について検討するものではない。われわれの分

[2]この報告は、1997 年 1 月末にカリフォルニア州メンロパークのサン・マイクロシステムズにおいて行われたグループ会議から生まれたものである。この会議には著者の多くと共に、Ken Bass、Alan Davidson、Michael Froomkin、Shabbir Safdar、David Sobel、Daniel Weitzner も参加していた。著者一同は、これらの参加者の貢献に感謝するとともに、この会議を主催して本最終報告の執筆を支援してくれた Center for Democracy and Technology にも感謝したい。

析は、そのキーリカバリのインフラが中央に集約されているか、あるいは広く分散していてるかとは関係なく成立するものである。

われわれは特に、特定の規制・法制上の提案や商業製品について、肯定したり否定したり、何らかの結論を導き出したりはしないようにしている。むしろ、政策立案者たちが情報時代におけるもっとも野心的で影響の大きい技術的な導入を行おうとするにあたり、本論の検討結果がキーリカバリに関する議論にもっと貢献し、キーリカバリのコストについて、ながいこと待ち望まれていた基本的な分析を提供できればというのがわれわれの希望である。

自由社会における暗号とキーリカバリの正しい役割についての議論には、さまざまな側面があるが、われわれはこの問題の純粋に技術面だけに注力し、もっと一般的な政治的・社会的問題は扱わなかった。たしかに、政府による広範なキーリカバリ用インフラという考え方そのものが民主主義における自由とプライバシーの考え方に反すると主張する人も多い。こうした考え方は、そのキーリカバリインフラが中央に集約されていようと、広く分散していようと関係なく成立する。われわれの分析が技術的な性格のものだからといって、それが政府によるキーリカバリの社会的なメリットについては認めているのだと解釈してはならない。それどころかわれわれは、この問題についての活発で広範な公開議論を大いに奨めるものである。

# 1 背景

## 1.1 暗号とグローバル情報基盤（GII）

グローバル情報基盤（GII）は、電子商取引を革命的に発展させ、政府を再活性化し、情報化社会に対する新しいオープンなアクセスを提供すると約束している。しかしこの約束は、情報セキュリティとプライバシーなしには実現不可能である。セキュリティが高く、信頼性の高いインフラがなくては、企業も個人も民間事業や個人情報をオンラインに移行するのを、だんだんいやがるようになる。

情報セキュリティの必要性は広範で、情報技術のユーザであろうとなかろうと、われわれみんなに関わってくる。さまざまな種類の機密情報が、ますます電子化されるようになってきているからだ。例としては:

- 民間の個人同士や取引上のやりとり、たとえば電話の会話、ファックス、電子メール
- 電子送金などの金銭取引
- 機密性の高い事業の情報や商売上の秘密
- 航空管制、電話網、送電網など重要性の高いインフラシステム運用に使われるデータ。
- 診療記録、人事ファイルなどの個人情報

電子的に管理された情報は、現代社会では日常生活のほとんどあらゆる面にかかわってくる。このような、重要だがセキュリティの整っていないデータの増大のため、好奇心のつよい身近な人々

や産業スパイ、敵対国、組織犯罪、テロ組織などに対し、われわれの社会はますます脆い存在となってきている。

矛盾しているようだが、電子情報を管理してやりとりするための技術はすさまじい勢いで向上しているにもかかわらず、この進歩は一般に内在するセキュリティを犠牲にすることで成立している。一般に、情報技術が向上して高速、安価、便利になるにつれて、機密情報がどこを流れるか、ドキュメント類の出所がどこか、あるいは電話の向こう側にいるのがだれか、といったことをコントロールする（あるいはそれ以前にはっきり同定する）ことがだんだんむずかしくなってくる。現代社会の基幹通信インフラのセキュリティは低下してきているのに、われわれはそれをますます重要性の高い用途に使うようになってきているのである。こうしたトレンドが続くにともない、暗号技術は今後もっと頻繁に、プライバシーと機密情報の安全を確保する唯一の手段となってくるであろう。

暗号は、情報時代におけるセキュリティをもたらす不可欠なツールである。暗号はデータをスクランブルして、承認された受け手でなければオリジナルの「平文」を回復するのがきわめて困難——できればほぼ不可能——にするための、数学的手続きの利用に基づいている。きちんと実装されれば、暗号は機密情報をセキュリティの低いコンピュータに保存したり、それをセキュリティの低いネットワークで送ったりすることを可能にする。しかるべき解読「キー」を持った者だけが平文情報を回復できる。

非常にセキュリティの高い暗号化方式は、比較的安価に導入できるし、価値の高そうなデータを扱う通信製品やアプリケーションには、まちがいなく暗号が採用されて組み込まれるようになるものと広く考えられている[3]。暗号のアプリケーションとしては、ファイルを盗難や無許可アクセスから保護したり、通信が傍受されないよう保護したり、高セキュリティの商取引を可能としたりするようなものがある。別の暗号技術を使えば、ファイルやメッセージの内容が変更されていないことを保証したり（整合性、integrity）、先方のアイデンティティを検証したり（認証、authentication）、法的な効力を持たせたり（否認不可能性、non-repudiation）することができる。

情報を、招かれざる傍受や横取り、窃盗から安全に守る強力暗号（strong encryption）には副作用があった。法強制執行機関が犯罪の容疑者に対してある種の隠密電子捜査（特に盗聴）を行おうとしても、それをターゲットに知られて協力を得られない限りそれがやりにくくなってしまう。この困難が、キーリカバリに関する論争の核心となっている。

## 1.2 「キーリカバリ」：その必要条件と各種提案

アメリカ合州国をはじめとする各国政府は、法執行機関が平文にアクセスできることを保証するような「キーリカバリ」機構が組み込まれていない限り、暗号の広範な利用を阻止しようとしてきた。こうした政府主導のキーリカバリシステムの要件は、暗号ユーザが求める機能とはちがってお

[3] National Research Council が 1996 年に出した、暗号についての総合的な報告では、暗号の重要性が増していることについて詳細な検討が行われている。National Research Council, ***Cryptography's Role in Securing the Information Society*** (1996)

り、最終的には深刻な新しいリスクやコストをもたらすことになる。

キーリカバリ暗号システムは、通常の暗号化と解読のチャンネルの外で、なんらかの形で平文にアクセスを可能にしなくてはならない。キーリカバリは「キーエスクロウ」と呼ばれることもある。「エスクロウ」という用語は、アメリカ政府のクリッパーチップ計画との関連で有名になった。この計画では、各暗号化装置のマスターキーが「エスクロウ」（第三者預かり）状態で保持され、これが法執行機関に提供されることになる。今日では、「キーリカバリ」という用語がこうしたシステムを指す一般用語としてつかわれ、近年導入された「キーエスクロウ」「第三者信託」「例外的アクセス」「データリカバリ」「キーリカバリ」などの暗号化システムすべてを含むものとなっている。これらのシステムはそれぞれ異なっているが、ここでの目的を大きく歪めるような差はない。本報告では、「キーリカバリ」という一般用語は広い意味で使われており、第三者（政府）が暗号化データに確実にアクセスできるようなシステムすべてを指すものとする。

キーリカバリ暗号システムには、いろいろな方式がある。初期の「キーエスクロウ」提案では、個人キーをアメリカ政府が保管することになっていた。もっと最近では、それを指定の民間組織にゆだねるとされている。別のシステムでは「エスクロウ・エージェント」や「キーリカバリエージェント」が設置され、かれらは指定の暗号化された通信セッションや保存されたファイルについて、キーを取得できる能力を持つことになる。こうしたシステムでは、そうした「セッションキー」がリカバリ・エージェントの知っているキーを使って暗号化され、データに含められることが必要になる。一部のシステムでは、キー取得能力を複数のエージェントが分割して持つこととしている。

多くの利害関係団体は、さまざまなキーリカバリ提案をそれぞれ明確に区別しようとしてきた。確かに、新しいキーリカバリシステムが登場してきており、それはキーの保管と取得方法の面で、オリジナルの「クリッパー」提案とは異なっているのは事実である。しかしながら、われわれの議論はどれか個別方式の詳細を扱うのではなく、問題の基本的な要件についての、もっと高レベルでの見方をしている。したがって、「キーリカバリ」「キーエスクロウ」「第三者信託」を区別する必要はない。これらのシステムはすべて、この報告の中で検討される基本要素を共有しているのである。その要素とは以下の通り：

- 暗号化およびその解読の主要な手段の外部にあって、それを使って第三者が暗号化されたデータの平文に秘密裏にアクセスできるような機構。
- 非常に高い機密性を必要とする秘密キー（あるいはその集合）が存在し、それが長期にわたって維持されていること。

この 2 つの要素をあわせることで、これは法執行機関の要求仕様を満足するように設計された「あらゆる場面で利用されるキーリカバリ」を含むものとなる。個別の詳細は変わっても、この基本的な要件はまず変わらないと考えてよい。これらは暗号化された通信トラヒックの平文に対し、法執行機関がユーザに通知する必要なしに、迅速にアクセスできることを保証するという、表明されている目的を満足するようなどんなシステムにおいても、必須要件なのである。

## 2　キーの取得：政府の要件 VS エンドユーザの要件

キーリカバリシステムがとりあげられるようになったのは、政府の諜報機関や法執行機関が、暗号ユーザの同意を得たり、あるいはかれらに知られたりすることなしに、確実に暗号化された情報にアクセスしたいと考えているためである。きちんと設計された暗号システムでは、正しいキーを知らずに暗号化データを復元することはほぼ不可能に近い。ときにはこれが、暗号ユーザ自身にとっても問題をつくりだす可能性がある。同意なしの第三者を除外するコストとしては、もし必要時点でキーをなくしたり、あるいはそれが手元になかったりした場合に、暗号利用者が自分の情報を利用できなくなってしまうというものがあげられる。これを根拠にして、産業界もキーリカバリを必要とし、求めているのだ、政府の提唱するようなキーリカバリは自分自身の暗号化データを確実に回復できるようにするという産業界のニーズにも応えるものなのだ、といった議論がされることがある。最近の政府提案のいくつか (および政府の要件を満たすように設計された商業製品やサービスなど) は、政府のアクセスと同時に「所有者」のアクセスも保証するという二重の役割を果たすものとして宣伝されている。しかしながら、この点での産業界や個人ユーザが求める条件と政府の求める条件とはあまりにかけはなれており、実はそれぞれの問題に応えるシステムの間に、重なる部分はほとんどないのである。

政府主導のキーリカバリ暗号の最終的な目標は、アメリカ商務省の最近の暗号規制にも述べられているように、「キーエスクロウとキーリカバリ暗号方式を使った全世界的なキー管理インフラを目指す」ものである[4]。このような全世界的なキーリカバリシステムに対する法執行機関の要求に応えるようなインフラの必要とする条件としては、以下のようなものが挙げられる：

**ユーザへの通知やその同意なしに、第三者/政府がアクセスできること。**企業が自分自身のキーを保管するような、いわゆる「自己エスクロウ（self-escrow）」システムでさえ、リカバリ・エージェントとキーの持ち主との間を十分に遮断することで、解読情報がいつリリースされたかわからないようにする必要がある。

**キーリカバリのあらゆる場面における国際的採用。**キーリカバリが法執行機関の役に立つためには、エンドユーザ側でリカバリ機能の需要があろうとなかろうと、その方式がきわめて普及していて、暗号化された保存情報や通信のほとんどに使われていなくてはならない。

**常時利用可能。どんな運用条件下でも 24 時間の平文アクセスが可能なこと。**法執行機関は、解読キーの迅速な入手を求める— アメリカなどで提案されている規制では、2 時間以内とされている[5]。 民間の暗号ユーザでは、なくしたキーを 24 時間いつでも回復できるようなニーズや、これほど短時間で回復しなければならないようなニーズはほとんどない。

---

[4] Dept. of Commerce, "Interim Rule on Encryption Items," ***Federal Register***, Vol. 61, p. 68572 (Dec. 30, 1996)

[5] たとえば、最近のイギリスにおける「第三者信託（Trusted Third-Party）」システムは、似たような法執行機関側の要求条件を挙げているが、そこでは TTP リカバリ・エージェントの要求対応時間は**1 時間以内**でなくてはならないとされている。イギリス通産省（U.K. Department of Trade and Industry）"LICENSING OF TRUSTED THIRD-PARTIES FOR THE PROVISION OF ENCRYPTION SERVICES,"（1997/03）（Public Consultation Paper）参照のこと。

**保存された暗号データだけでなく、暗号化された通信トラヒックへのアクセス。**キーリカバリに対して産業界からの需要があるにしても、それは保存されたデータに限られており、通信トラヒック解読に対する需要はない。

実のところ、政府によるキーリカバリに必要とされる条件は、ほとんど完全に、商業暗号ユーザのニーズと相容れないものなのである。両者の食い違いがもっとも顕著なのは、以下の 4 点である：

- リカバリを必要とするデータの種類
- リカバリ用キーの種類
- リカバリ用キーの管理方法
- キー認証とキーリカバリの関係

政府のキーリカバリは、民間ユーザやビジネスユーザに対しては特にメリットはないのである。同じように、ビジネス界で自然発生的に生まれつつあるキーの管理とリカバリシステムは、政府の利用にはあまり適していない。

## 2.1 通信トラヒック VS 蓄積データ

キーの「リカバー可能性」が一部のデータ保存システムでは付加価値として重要になる可能性はあるものの、暗号のほかの応用では、この機能に対する需要もニーズもほとんどない。特に、暗号ユーザが電話やファックス、インターネットリンクのような通信セッションを守るのに使われてたキーを取得したがるような事態はほとんどあり得ないと言っていい。このようなキーがなくなったり、こわれたり、あるいは使用できなくなったら、すぐに問題が生じるので新しいキーが協議されてつくりだされるだろう。また、第三者にそうしたキーを預けるべき理由も、民間ユーザ側にはまったくない。キーのリカバー可能性は、万が一民間でなんらかの使い道があったとしても、せいぜい復元不可能な保存データの保護くらいである。これ以外の利用には、基本的にまったくビジネスモデルが存在しないのである。これについては以下に述べる。

保存データへの応用を考えてみると、ビジネス上で重要な情報の継続的な利用を保証する手段として、キーリカバリは決して唯一の手段ではない。ほかのオプションとしては、数名でキーを共有する（たとえば秘密共有技術を用いるなど）、バックアップを管理するローカルなキー登録機関からキーを入手する、暗号化されたデータの平文バックアップを慎重に管理する、などがある。こうした選択肢のどれがいちばんいいかは、個別のアプリケーションやユーザによる。

暗号化された電子メールは、通信の面と保存の面の両方をあわせもった、特殊な例として興味深い。キーリカバリが高セキュリティ電子メールの利用者にとって役にたつものかどうかは、その個別システムの設計にもよる。

一方の政府は、ほとんど**あらゆる**暗号キーに適用されるようなキーリカバリインフラを提案している。これは（なかでも特に）通信セッションを保護するためのキーも含む。

## 2.2 認証 VS 秘密鍵

暗号はこれまで機密保持のためのものとされてきたが、認証コードやデジタル署名といったほかの暗号メカニズムは、メッセージが細工されていないか、偽造されていないかを確認するものとして使われる。一部のシステムは、手書きのサインと同じような性質を提供し、これには「否認不可能性（Non-repudiation）」も含まれる。これによって受信者は、そのメッセージがある特定の個人によって署名されたものであることを証明できる。

電子商取引の約束する成果のほとんどは、法的拘束力のある関係を確立するための暗号技術が使用できるかどうかにかかっている。しかしながら、一部のキーリカバリ方式は、認証キーと署名キーを機密保持キーといっしょに保存しておく設計になっている。このような方式は、法的拘束力ある関係を確立するのに必要となる、絶対的否認不可能性という性質を破壊してしまう。さらに、認証キーや署名キーのリカバリをしても、まともな使い道はまったくない。民間セクターはあらゆる署名者に対して別々のキーを必要とする。これは、あるメッセージを送る権限を与えられた人物が 2 人以上いたとしてもである。これがなければ、やりとりを事後監査する能力が失われてしまう。政府の捜査も署名キーのリカバリは必要としない。

しかし、政府から提案されているようなキーリカバリ・インフラでは、認証キーや署名キーを除外するのはむずかしい。なぜなら一部のキーは、署名と暗号化の両方に使われているからである[6]また、リカバリ・システムのキーの中から、金銭的な取引を守るためだけに使われているキーを除くだけでは不十分である。多くの電子商取引方式は、使用範囲が限定されないキーを使うからである。たとえばあるキーをつかって個人の電子メールを暗号化し、同時にそのキーで契約に電子的に署名したり、送金を認証したりするかもしれない。

署名キーが回復できなくなったら、その持ち主はもうメッセージに署名できなくなるので非常に困るだろうという議論がなされている。しかしながら、一般的な慣行からみて、なくしたキーは無効にすることができるし、古いものと同じ権利や特権を持った新しいキーを発行することもできる。つまりなくした署名キーや認証キーを回復するなどという事態は、絶対に起きないのである。

## 2.3 インフラ：ローカル VS 第三者管理

暗号ユーザにとってキーリカバリ方式が価値を持つためには、キーの登録、取得、保管について厳重なコントロールが行われている必要がある。一般に、個別キーを取得する能力を必要とするのは、ごく少数の人々にすぎない。これらの人々は、通常は同じ場所でお互いに顔見知りとなって働いていることが多い。実際にキーの回復が必要となったら、これはその現地の問題であることが多

[6]それどころか、安全な通信を行うために、通信の両サイドが自分たちの認証キーを使って暗号化キーを合議してきめるというのは、技術的にもまわりくどくない手段である。信頼に基づく認証キーを配布するシステムは、すべて *ipso facto*（まさにそれ自体が）政府の捜査の手が及ばない私的通信のためのインフラとして機能してしまう。

い。これはオフィスの鍵をなくしたり、コンピュータファイルをバックアップから復元したりするのと同じことである。キーリカバリが行われる時間や、個別のキーに対するアクセス権が認められている個人の同定、キーがいつの段階で回復されるべきかという方針、その他基本的な運営手続きは、単一の企業内部ですらユーザごとに大きく異なる。なかでも特に重要なのは、「回復可能」なキーを使い終わったときに、それがいつ、どのようにして破棄されるかということである。これは特に、機密性の高い個人的な記録や企業の記録に関わるキーの場合に重要となる。

同様に、企業ではキーの回復が秘密である必要はないし、利用者の協力なしでキーを入手可能にする必要もないのがふつうである。キーリカバリが企業環境で使用される場合、それはその企業における総合的なデータ管理方針の一部であるのが通例だろう。ユーザは通常、自分自身のキー回復を確実にするため、その場に立ち会えるだけの信用は与えられており、それが経営慣行や監督によって支援されているはずである。キーが回復されなくてはならない場合というのは、ユーザ自身が正しいキーを持っていないことに気づいたり、あるいはキーを持つ人物がすでにいなかったりする場合である。よく持ち出される仮説的な例として、不満をいだく職員が重要なファイルの解読を拒否する場合にはどうするのか、といったものがあるが、こうした例はおそらくは、ビジネス上のデータ管理慣行（たとえば上司による監督や、企業にとって不可欠なデータを平文としてバックアップしておく、など）によっていちばん有効かつ経済的に対処できるものであり、中央化された標準キーリカバリ機構などは必要ない。そしてこの（いささか考えにくい）ケースにおいてすら、キーが回復されたという事実をユーザから隠す必要はまったくない。

ところがアメリカ政府が提案しているキーリカバリ方式は、その性格上、現場でのコントロールを許さない。迅速に、だれにも知られず、しかもキーの所有者に通知することなくキーを回復できるという政府の要求は、ほとんどその定義からして、第三者によって実装されなくてはならず、しかもその手続きはユーザとは完全に分離したものでなくてはならない。政府がある組織に自分自身のキー管理を認めたとしても、キーリカバリ・エージェントはかなり中央集中し、実際のユーザから離れた存在でなくてはならない。この必要条件によって、キーリカバリの濫用に対する最初の防衛ライン——キーの所有者——が排除されてしまう。

## 2.4 インフラ：キー認証と配布 VS キーリカバリ

電子商取引と暗号の利用が普及するにつれて、暗号の利用者を同定するため、なんらかの「認証機関（Certification Authorities、略して CA）が一部のアプリケーションでは必要となってくる。CA は信頼された第三者であって、暗号利用者のアイデンティティ（またはその他の性質）を保証する存在である。高セキュリティで信頼できる電子的なやりとりのためには、認証機関の発展と利用が不可欠であると広く考えられている。そしていずれは結果的に、電子商取引やオンライン通信においてはこうした認証機関の存在が前提となるようになるだろうと考えられている[7]。

[7]CA の監督において政府が果たすべき役割については、激しい議論が行われている。CA は最終的には巨大で中央集権化された、ひょっとして政府の承認をうけた機関となるかも知れないが、逆に小さくて地域ごとに信用をうけた機関となるかもしれない。いまはまだ発展段階のごく初期にあるため、政府の役割として何が適切かについては、合意は得られていない。CA 規制監督の議論に関する見事なまとめについては Michael Froomkin, “The Essential Role of Trusted

キーリカバリとキー認証は、どちらもキー管理に関わるという点で一見似ているように思える。しかし、キーリカバリの性格は、キー認証とはまったく異なる。認証機関のもっとも重要な機能は、デジタル署名に使用されている公開キーを認証することである。ところがキーリカバリは、機密保持に使われるキーを扱うものである。もっと重要な点として、認証機関の運用にあたっては、機密性の高いユーザ情報を扱う必要はない。CA は一般に、ユーザの公開キーだけを扱い、それと対応する秘密キーはまったく知らされない。もし CA の秘密キーが侵害されたり暴露されたりしても、そこから生じる直接の被害としては、その機関からの認定が偽造できるようになるというだけである。一方、もしキーリカバリ・エージェントの秘密キーが侵害されれば、被害はずっと大きく、ずっと直接的なものとなる。そのリカバリ・エージェントの利用者すべてが、秘密を侵害される危険性が生じるからである。

認証は、キーリカバリなしでも存在しうる（そして現に存在している）。逆に、キーリカバリインフラは、キー認証インフラとはまったく関係なしに存在しうる。

最近の政府提案のいくつかは、キーリカバリをキー認証と関連づけようとしている。それらで提案されている CA とキーリカバリとのリンクは、技術的にはまったくのナンセンスである。それどころか、そのようなリンクは重大な欠陥を持っている。そんなシステムが機能するかどうかさえはっきりしていない。署名や身分証明に使われるキーの登録が必要とされかねないという点で、こうしたシステムはセキュリティ上のリスクを増やすものである。第三者が署名用のキーにアクセスできるようにする正当な理由など存在しない（政府の法執行上の必要性を考慮しても）。署名用のキーは、もし侵害されてしまったら、他人になりすましたり、かれらのデジタル署名を偽造したりするのに使われてしまう。そしてさらに、認証インフラを通じてキーリカバリを実現しようという試みは、おそらくは法執行機関の目標達成には貢献しないであろう。多くの（それどころかほとんどの）暗号化キーは、直接的には認証されていない。つまり認証ベースのリカバリシステムの手の届かない存在だということになる。

## 3　キーリカバリのリスクとコスト

キーリカバリシステムは、リカバリ機能のない類似システムに比べて本質的にセキュリティが低く、高コストで、使いにくいものとなる。キーリカバリは暗号化によって得られる多くの安全装置、たとえばデータ解読方法についてのユーザの絶対的なコントロールなどを骨抜きにしてしまう。さらに、全地球的なキーリカバリ・インフラは、とてつもなく複雑で高価なものとなるのはまちがいない。

キーリカバリのインパクトは、少なくとも 3 つの側面から考えることができる：

**リスク** ——キーリカバリ機構が破綻した場合、暗号システムのまともな運用、その根拠となる秘密性、そして最終的なセキュリティまでが脅かされる。脅威としては、キーの不適切な公開、

Third-Parties in Electronic Commerce,” 75 Oregon L. Rev. 49 （1996）を参照のこと。

貴重なキー情報の盗難、あるいは法執行機関の要求に応えられなくなること、などが挙げられる。

**複雑さ** ——暗号のエンドユーザにキーリカバリをある程度意識されないようにすることは可能だが、完全に機能するキーリカバリインフラはとてつもなく複雑なシステムであり、無数の新しい関係機関や運用上の必要条件とやりとりを必要とする。多くの場合、システムのキーリカバリの面は、基本的な暗号機能自体よりもずっと複雑で実装のむずかしい部分となる。

**経済的なコスト** ——キーリカバリの真のコストを示す信頼に足る経済モデルについては、だれもいまだに実証はおろか、概略を述べてすらいない。しかしながら、あらゆるキーリカバリ方式に共通する基本的なシステム要素について堅実な定性的判断を下すことは可能である。それらの要素は、設計コスト、実装コスト、導入コスト、運用コストにそれぞれ大きなインパクトをもたらす。

## 3.1 新たな弱点とリスク

あらゆるキーリカバリ・インフラは、まさにその性格上、これまで存在しなかった部分に無許可のデータ取得を可能にする新たな弱点を付け加えてしまう。これは最低でも 2 つの悪影響をもたらす：

- キーリカバリ機能のないシステムに存在するセキュリティ保証を破棄してしまう。リカバリ機能のないシステムは、機密の平文を取得するためのユーザのコントロールのきかない代替パスを持たない。
- 犯罪者やその他攻撃者にとって価値の高い標的となる、解読情報の新たな集中地点をつくりだす。

こうしたリスクは、通信や保存に使われる暗号でも生じるが、一番集中して生じるのは認証に用いられる暗号であろう（もしキーのどれかがこうした目的の複数にまたがって使用されていた場合、問題はさらに拡大する）。

### 3.1.1 平文取得の新しい手段

どんな実装方式をとろうとも、もしキーリカバリシステムがキー全体か平文への迅速なアクセスを法執行機関に提供しなくてはならないのであれば、それはこれまでなかったような、データ取得の新しく高速な道を提供するものである。

キー取得アクセスの道筋は、完全にユーザのコントロールの外にある。実のところ、こうした例外的アクセスへの道は、暗号ユーザからは見えないものになるように、意図的に設計されているのである。これにより、誤用やニセのキーのリリースなどの事態にたいする根本的な安全弁の一つが取り除かれてしまう。

これと対照的に、キーリカバリのないシステムは、通常はセキュリティの高い形で、裏口などなしに設計できる。多くのユーザの多くの使用においては、裏口アクセスは必要とされていないし、それが通常の運用でもないし、望ましいものでもない。

### 3.1.2 インサイダーによる濫用

人間がからむすべてのセキュリティシステムと同様、キーリカバリ・システムは正式な権限を持つ個人の職権濫用には非常に弱い。キーリカバリシステムのユーザは、キーリカバリの設計、実装、立ち上げを行い、さらにはそれを運用している人々を信用しなくてはならない。イデオロギーやどん欲さ、脅迫などに動かされた個人やその集団は、自分らに与えられた権力を濫用するかもしれない。こうした濫用は個人や特定企業の秘密、あるいは国家機密まで脅かす恐れがある。近年、重要な地位にある個人が、与えられた信用を裏切った例は数多く見られる[8]。キーリカバリシステムだけが特にうまく運営管理されると考えるべき理由はまったくない。

「インサイダーによる濫用」のリスクは、国際的なスコープのキーリカバリ方式を設計しようとしてみれば一層明らかになる。こうした濫用は、敵対企業や敵対政府によって組織的に行うこともできる。たとえばある国の法執行機関が、自分たちのキーリカバリ権限を濫用して自国企業に有利なようにすることもあり得る。

### 3.1.3 新たに生じる攻撃目標

キーリカバリの性質上、暗号システムを攻撃する際に価値の高い新たな攻撃目標ができてしまう。キーリカバリ・エージェントは、その顧客がきわめて大事にしている情報や通信へのキーを、集約化されたかたちで保存しているデータベースを維持管理することになる。多くのキーリカバリシステムでは、リカバリ・エージェントの持つ秘密キーを 1 つ（ないし少数）盗めば、ある個人や企業に関するデータをほとんどすべて取り出すことができるようになる。リカバリ・エージェント自身の秘密キーを盗めば、もっと広範な通信にアクセスが可能となるし、また暗号輸出規制への適合性を保証するためのヘッダ情報を簡単に書き換えてしまうことも可能となるかもしれない。キーリカバリインフラは、攻撃のコストとリスクに十分見合うほど価値の高い目標をつくりだすことになりかねない。

こうした新しい有望な攻撃目標の所在やアイデンディディは、キーリカバリシステムそのものによってきわめて明確にされてしまう。あらゆる暗号化された通信や保存ファイルは、そのキー取得情報の所在についての情報を含むことが必要とされる。この「ポインタ」は、法執行機関に平文取得の方法を示す地図だが、一方で権限のない攻撃者に対し、どこに注力すればいいかを示すものでもある。さらに、こうしたリスクを低下できるシステム（たとえば分割キーシステムなど）は、かわりにコストを大幅に増大させることになってしまう。たとえばキーを 2 つに分割すれば、リカバ

[8]訳注　蛇足ながら、日本においてはこれが一層顕著なのは言うまでもない。

リ・エージェントのコストは少なくとも倍以上にはなる[9]。こうしたシステムは、複数のエージェントを必要とし、さらに高価な協調メカニズムも追加で必要となり、さらに平文への迅速なアクセスを提供し続けるには、分割したキーを復元する手間を考えると応答時間をもっと短くしなくてはならない。キーがどれだけ分割されたかに関わらず、法執行機関は迅速なアクセスを要求するため、部分キー取得のための高速システムの開発が必要となる。部分キーの復元システムと、法執行機関用に復元された全体キーの両方が、新しい弱点として浮かび上がってくる。

### 3.1.4 将来的な秘密性（Forward Secrecy）

キーリカバリは暗号化された携帯電話など、通信システムにおいて特に大きな問題となる。なぜならそれは、将来的な秘密性（forward secrecy）という性質を破壊してしまうからだ。将来的な秘密性を持つシステムというのは、ある通信を解読するためのキーを入手しても、それがほかの通信のセキュリティに影響しないようなシステムをさす。たとえば、暗号化された電話の通話では、その通話を暗号化するためのキーは通話が確立されている間にその場で決めることができる。通話が終わったときにこのキーが破壊されてしまえば、通話を行った両者は、だれもその会話を後から解読することができないと確信できる——たとえその後の通話に使われたキーがどこかから入手されてしまった場合でも。結果として、通話が終わってしまえば、それを解読するのに必要な情報は、もはや存在しなくなる。これにより、セキュリティの高い処理や保存のコストやリスクが必要となるのは、その通話の期間だけに限られる。

将来的な秘密性は、2 つの理由で望ましく重要である。まず、高セキュリティシステムの設計と分析が簡単になり、設計そのものやその実装が本当に高セキュリティであることを保証するのがずっと容易になる。第二のもっと重要な理由として、将来的な秘密性はシステムのセキュリティを大幅に向上させ、そのコストを大きく下がる。なぜならキーは、その通信が実際に行われている間だけ維持して保護すればすむからだ。

キーリカバリは、この将来的な秘密性という性質を破壊する。そのトラヒックを復元する可能性は、もとの通話が起こってからずっと将来にわたって残ることになるからだ。後に政府が平文を要求したらそれに応じられるように、関連キーは破壊されずに保管されなくてはならない。もしキーが保管されているなら、それを暴くこともできる。キーが破壊されていれば、それが暴かれる危険性もその瞬間になくなるのである。

## 3.2 新たに生じる複雑さ

過去の経験が示すとおり、高セキュリティの暗号システムをきちんと設計して構築するのは想像を絶するほど困難である。きわめて簡単な暗号アルゴリズムや暗号プロトコルや暗号装置の設計と実装でさえ、複雑で細心の注意が必要となるプロセスとなる。ほんのちょっとした変更でさえ、し

[9] キーの一部を保存するコストは、キー全体を保存するコストより低いわけではなく、さらにキー分割手法として一般的なものがつくりだす分割キーは、それぞれがもとのキー全体と同じくらいのサイズになるのが通例である。

ばしば致命的なセキュリティ上の欠陥をもたらしてしまう。キーリカバリ機能のないシステムは、要求仕様の面ではかなり単純なのに、それでも実配備されているシステムにはしばしば悪用され得る欠陥が見つかっている。

著者一同は、暗号システムの設計、分析、実装で多くの経験をつんできている。その経験に基づいてわれわれは、キーリカバリ機能を加えることでそうしたシステムが期待通りに機能すると保証するのは一層困難になると断言できる。どんなキーリカバリシステムにも、設計上、実装上、あるいは運用上の弱点が必ずいくつか潜んでいて、それが無許可の第三者によるデータ取得を可能にしてしまうであろう。これは可能性として否定できないどころか、ほぼ確実と言っていい。産業界も学会も、キーリカバリから生じるような複雑なシステムをきちんと分析したり設計したりするだけのツールや力量は、端的に言って持っていないのである。

これは抽象的な留意事項などではない。今日までに行われてきたキーリカバリやキーエスクロウの提案は、国家安全保障機関（NSA）の設計したものを含めて、初期の実装後に弱点が見つかっている。たとえば、アメリカのエスクロウ式暗号規格（Escrowed Encryption Standard）は、1993年に発表されて以来、いくつかの欠陥が見つかっている。これは「クリッパーチップ」のもとになったシステムである。こうした問題は、システム設計者の能力不足で生じたものではない。それどころか、アメリカの国家安全保障機関は、世界の最先端をゆく暗号組織であり、アメリカ政府の軍や国家に関わる最高機密を安全に守る暗号システムの開発を任されている。エスクロウ式暗号規格に欠陥があったのは、そもそもきちんとしたセキュリティというのが技術的にきわめてむずかしい問題だからなのである。キーリカバリはそこに、これまでだれも直面したことのないような要求仕様を追加することで、さらにものすごい煩雑さを加えようとしているのである。

### 3.2.1 システムと運用のスケール

法強制執行機関が構想しているようなキーリカバリは、世界中の何千もの企業、リカバリ・エージェント、監督省庁や機関、法執行機関を結ぶ、高セキュリティインフラの導入を必要とする。そしてこれらの主体は、かつてないスケールでやりとりを行い、協力体制をとることになる。

ひとたび普及してしまえば、ネットワーク上の通信や機密ファイル保存の大半には暗号が使われる見込みが高い。2000年（まだ情報技術導入においてはごく初期である）までに、法執行機関が構想しているような、あらゆる場面で使われるキーリカバリシステムを実配備するには、以下のような要素を射程に入れて考えなくてはならない：

**何千という製品。**世界中の暗号商品はすでに800点以上におよび、この数は今後劇的に増加するであろう。提案されているシステムは、アメリカ国内だけでも多数のキーリカバリ・エージェントを想定している。ほかの国も独自のキーリカバリ・エージェントを置きたがるであろう。大企業は自分自身のキーリカバリ・エージェントとして機能したいと考えるだろう。こうしたエージェントのそれぞれがアメリカと、おそらくは諸外国の認証を獲得しなくてはならなくなる。

**何万にもおよぶ法強制執行機関。**アメリカだけでも、地方、州、連邦をあさせて 1,700 以上の法執行機関が存在しており、これらがすべて、許可された傍受用や押収データ用にキー情報を要求することになる[10]。世界中の国家および地方エージェンシーも、キーにアクセスを求めるであろう。

**何百万人ものユーザ。**今日、何百万人もの Web ユーザたちは、Web ブラウザが Secure ページ（クレジットカードを使った取引用ページなどでは多用されている）に出会うたびに、暗号化通信を使っている。2000 年までに、インターネットのユーザは 1 億人にものぼると予測されており、そのほとんどは次世代標準インターネットプロトコルの一部として、日常的に通信を暗号化することになる可能性が高い。その他何百万もの企業や過程におけるコンピュータ利用者も、情報を保存したり、イントラネット上の通信を日常的に暗号化することになる。

**何千万（あるいはそれ以上）の公開キー・秘密キーのペア。**ほとんどのユーザは、さまざまな目的に応じていくつかの公開キーのペアを持つことになる。一部のアプリケーションでは、キーのペアを利用のたびに「その場で」つくりだす。

**取得が要求される何十億ものセッションキー。**暗号化された電話の通話すべて、暗号化された保存ファイルすべて、電子メールすべて、secure web セッションすべてが、セッションキーを作り出し、それが取得要求を出されることになる（一部のキーリカバリ方式は、リカバリセンターが個別のセッションキーを処理しなくてすむようにしているが、こうした「きめ細かさのシフト（granularity shift）」は別のリスク要因を導入する——この点については、以下の第 3.4.1 節（25 ページ）を参照。）

最終的には、これらの数はさらに増えるであろう。情報時代の技術向上によって、もっと多くの人々やもっと多くのデータがオンライン上に押しやられるからである。

このシステムを導入して管理運営するのに必要な総合的インフラは、莫大なものになる。政府機関は製品を認定しなくてはならない。アメリカ内外のほかの機関は、きわめて機密性の高いリカバリ・エージェントの運用とセキュリティを監督しなくてはならない——その一方で、法強制執行機関が望み通りに迅速かつ隠密裏にアクセスできるようにもしなくてはならない。こうした複雑なやりとりのどこか一カ所ででもセキュリティが崩れれば、キーの秘密が冒され、不正利用やまちがった情報の公開の可能性が増大することになる。

いくつかの理由から、高セキュリティのキーリカバリシステムは、そう簡単にスケーラブル[11]ではないと考えられる。依頼を出してくる法執行機関や、製品開発者、監督官庁の監督機関、暗号のエンドユーザなどが幾何級数的に増大するため、キーリカバリシステム内のさまざまな関係者の職務は、単に増大するだけでなく、ずっと煩雑なものとなる。くわえて、さまざまな主体が関わってくる国際的なキーリカバリ体系の協調にともなう通信コストもきわめて高くなってくる。

[10] U.S. Department of Justice, Bureau of Justice Statistics, *Sourcebook of Criminal Justice Statistics 1995* (1996), p. 39

[11] 訳注　用途の規模にあわせてシステムの規模が変えられること。

暗号学、オペレーティングシステム、ネットワーク、システム管理といった分野は、これほどの規模と複雑さを持つ高セキュリティシステムの導入と運用にあたり、比べものになるような経験はまったくない。われわれは端的に言って、このような規模の集合的なキー管理インフラをどう構築していいのかわからないし、ましてどう運営すればいいのか見当もつかないのである。これはそのキーリカバリ・インフラが中央化されていようと、広く分散していようと変わらない。

### 3.2.2 運用上の煩雑さ

政府アクセス用のキーリカバリ・インフラに必要とされる運用規模のため、キーリカバリに伴うセキュリティ上の問題の多くは増幅されてしまう。法執行機関の要求として出されているものは、きわめて複雑なキーリカバリ・システムの構築を必要とする。キー取得の速度や手続き面で出されている要求は、キー取得情報を託されているエージェントらの職務の煩雑さをきわめて大きくしてしまう。全世界的にあらゆる場面で使われるようなキーリカバリの採用に対する要求は、これに関わる主体の複雑さとその数を莫大に増やしてしまう。そしてそのそれぞれが、こんどは逆にキーリカバリシステム自身のセキュリティやコストにきわめて大きな影響を与えるようになる。

ある通信や保存ファイルのためのセッションキーを、ある法執行機関が求めてきた場合、それに対応するため平均的なキーリカバリ・センターが行わなくてはならない作業を考えてみよう：

- 信頼できる形で、要求を出してきている法執行機関を同定し、認証する（アメリカ国内の法執行機関は 17,000 以上存在している）。
- 信頼できる形で、令状などの文書を認証する。
- 信頼できる形で、ターゲットとなるユーザとデータを認証する。
- 認定されている有効期限をチェックする。
- セッションキーや平文データなどの解読情報を回復する。
- 回復されたデータを指定の形式にする。
- 安全な形で回復されたデータを送信。ただし相手はその権限を認められたものに限る。
- 信頼できる形で監査用の記録を残す。

政府の要求仕様に応えるためには、これらの業務のそれぞれがきわめて短時間のうちに高いセキュリティを維持して行われなくてはならない。たとえば、リカバリ・エージェントに関する直近のアメリカ商務省規定では、昼夜を問わず政府の依頼には 2 時間以内に対応しなくてはならないとされている。この仕事は世界中のエージェントが行わなくてはならず、それが何百万もの顧客の要望に応えており、そうした顧客と無数の法執行機関双方からの依頼に応えることになるのである。

このような規模で、しかもここまできつい制約条件下で有効かつ経済的に運用されているような高セキュリティシステムは、ほとんどどころかまったく存在しないと言っても過言ではない。これ

はこの要求仕様が相当緩和されたとしても変わらない（たとえば応答時間を 2 時間ではなく 1 日以内にしたとしても）。こうした非常に短い取得時間が強いる焦りと性急さは、こうしたシステムに含まれるべき慎重な精査にとっては天敵とも言えるものだ。もしこの取得プロセスのどこかの段階で不確実な点がでてきたとしても、取得依頼が正式なものか、正確なものかどうかを確認するだけの時間がないかもしれない。

全地球的なキーリカバリ・インフラは、どうしても不正なキー要求に対してさらに弱いものになってしまうし、まちがったキーを出したりするなど、セキュリティを脅かすようなミスを多発させるようになる。職員配備をきちんと行い、技術的なコントロールに気を配り、十分に考慮を加えた設計を行えば、こうしたリスクはある程度までは減らせるだろうが、キーリカバリに伴う運用上のリスクを完全になくすのは不可能である。

### 3.2.3 キーリカバリーのための認証

キーリカバリ運用のための必要条件の一つは、それが保存されているキーを要求してきている個人を認証しなくてはならないということである。これを信頼できる形で行うのは非常にむずかしい。

身元確認の「人間的」な手段——パスポートや出生証明書など—— は簡単に偽造されることが多い。マスコミは、「身元の窃盗（identity theft）」問題が増大して深刻化していると報じている。電子的 ID は暗号化されていなくてはならない。しかしこの場合、キーリカバリ・システムが自分自身の攻撃に使われる可能性がある。つまり、法執行係官か、企業職員の署名キーを盗んだ（あるいは取得した）人物は、そのキーを使って、ほかの多数のキーに対する正式な取得依頼を偽造できてしまうのである。もっと言えば、もし機密性の高いキーを盗んだり保管庫から入手したりすれば、ほかのキー取得通信を傍受するのにそれが使えてしまうかも知れない。

これに対して、企業の現場での日常的なキーリカバリ・プロセスは、個人的な身元確認に頼ることができる。システム管理者や上司は、だれがどのキーを使う権利を持っているか把握しているはずだ。もっと怪しげな依頼、たとえば電話ごしの依頼なども、適切に対処できるであろう。責任者は、要求された情報の機密性や、その要求が論理的に考えてどの程度緊急のものか、そしてさらに、共通の体験への言及など、非公式の本人確認なども使ってさまざまな条件を総合的に判断できる。しかしながら、こうした手法のいずれも、現場の外の環境から行われる依頼に対してはうまく機能するようにスケーリングできないのであり、したがってキーの保管者が個人的に知らない人物や機関から依頼がやってくるような、もっと大規模な運用に導入するには不適切なものとなる。

## 3.3 新たなコスト

キーリカバリ、特に政府アクセスのために要求されているようなスケールでのものは、非常に高価になる。さまざまな主体のレベルと、リカバー可能なキーを使うシステムの寿命を通じて、新しいコストが発生する。

法執行機関によって提出された要求仕様は、あらゆる場面で使われるキーリカバリ・システムの設計、導入、運用の各段階で、新しいコストを発生させる。こうしたコストの代表的なものとしては：

**リカバリ・エージェントの運用コスト**　——機密性と価値の高いキー情報を、長期にわたって保管・コントロールするコスト、法執行機関や、正当な民間からのキー取得依頼に対応するコスト、ユーザやベンダとの通信コスト。

**製品設計とエンジニアリングのコスト**　——キーリカバリの厳格な要件に準拠した、高セキュリティ製品の設計に伴う新たな支出。

**政府の監督コスト**　——キーリカバリ製品を検査・認定し、認定されたリカバリ・エージェントを認証・監査し、さらに法執行機関からくるキー情報取得と使用の依頼を裏付けるために、政府、法執行機関、民間認証機関は大規模な新規予算を必要とすることになる。

**ユーザのコスト**　——キーリカバリシステムを選び、使用し、管理運営するコスト、および低下したセキュリティや、機密情報の誤った（あるいは悪意の）公開からくる損害。

### 3.3.1　運用コスト

キーリカバリのいちばん明白な問題は、それを実現するようなインフラをセキュリティの高い形で運用するコストであろう。一般的にいえば、暗号は原理上安価な技術なのである。高いセキュリティで通信を確立したり、データを保管したりするときには、外的に運用される「インフラ」などほとんど必要ない（一部のアプリケーションでキー認証があるくらい）。一方、キーリカバリは、複雑で十分に理解されていない—— したがって高価でセキュリティの低い——インフラを必要とする。

前章で述べた運用上の煩雑さは、キーリカバリ・センタごとに多額の運用コストを発生させることになる。こうしたコストは、かなり高価になる公算が強い。特に民間のキーリカバリ・システムで期待されるはずの通常の運用コストに比べれば相当なものになるだろう。たとえば政府のキーリカバリは、もし政府の要求仕様を高セキュリティをもって満足しようとすれば、多数の職員雇用（週に 7 日、1 日 24 時間）を必要とし、しかもその職員は高度な訓練を受けたきわめて信頼のおける人物でなくてはならず、使用するハードとソフトも高度な保証つきのものでなくてはならない。こうしたコストはすべての暗号アプリケーションが負うものである。これにはキーリカバリが、ユーザはおろか法執行機関にとってすら無意味なアプリケーションも含まれる。

リスクが高く、トラブル時の損害賠償も高額なキーリカバリ・センターの運用は、いまのところ消費者からの需要もほとんどない状態であり、経済的に引き合うものかどうかさえいまだにはっきりしないのである。

### 3.3.2　製品デザインコスト

キーリカバリはまた、ユーザレベルの暗号ソフトやハードを設計するうえで、むずかしさとコストを増大させる。こうしたコストは個別のアプリケーションや、リカバリ・システムの細かい性格によって変わってくるが、場合によっては相当なものになってくる可能性がある。キーリカバリを含めようとすれば（特にセキュリティの高い形で含めようとすれば）ソフトウェアのリリースはかなり遅くなる。今日のハードやソフトの市場は、きわめて競争が激しく、製品のライフサイクルも短い。こうした遅れがあると、ベンダーはそもそもそうした機能を導入したがらないだろう。あるいはもっと困った事態として、いい加減でまともな検証を経ない設計が氾濫する結果になるかもしれない。旧製品との互換性も、特殊な問題を引き起こしてさらにこうしたコストを増大させることになる。

### 3.3.3　エンドユーザのコスト

政府主導のキーリカバリがなければ、暗号システムをユーザに意識されないような形で実配備するのはたやすい。高セキュリティ通信やデータ保管がしたければ、市場で十分にテストされた強い暗号化機能を備えた定評ある市販製品を購入すればすむ。その暗号機能の利用も、オプション設定をしたり、アイコンをクリックしたり、ハードウェアのカードを挿したりするだけのこと。なんの規制もない市場では、多くのアプリケーションがこうした質の高いユーザに意識されない暗号化機能を組み込んで出荷されるであろう。これについては著者一同、まったく疑問の余地はないと考える。これはすでに起きており、ユーザへのコストはほとんどとるに足らないものである。

これに対して、高セキュリティのキーリカバリ・システムを使用するには、少なくとも多少のユーザ努力や辛抱強さ、あるいはコストが必要になる。暗号化商品の購入に加えて、キーリカバリ・エージェントを少なくとも一つ選ばなくてはならない。ユーザはこのエージェントと（かならずしも明示的でないにせよ）重要な契約関係を結ばなくてはならない。この契約関係は、いまも今後何年間にもわたって、きわめて機密性の高いキー情報の提供可能性を左右する。多くの場合、ユーザとリカバリ・エージェントとの間で、何らかのキー情報のやりとりが必要となる（一部の製品はキー組み込み済みで出荷されるかもしれないが、慎重なユーザであればキーを定期的に変えたいと思うだろう。また、ソフトウェア、なかでも大量販売される「シュリンクラップ」ソフト（箱入りソフト）は、それぞれ個別のキーを一本ごとに組み込んだ形で経済的に流通させるのは通常不可能である）。

キーリカバリユーザへの負担は、データが暗号化された後もずっと続く。キーリカバリ・エージェントは、何年にもわたり情報解読能力を持ち続ける。その間、エージェントはそのセキュリティ方針を緩めたり、倒産したり、あるいは競合他社に買収されるかもしれない——しかしながら、解読する能力は維持されるし、維持されなくてはならない。まじめで真剣な暗号利用者は、自分のキーリカバリ・エージェントの動向を、暗号を使って何年たっても見守り続けなくてはならないことになる。

こうした負担は、暗号の全ユーザに適用される。各暗号の使用、ごとに、第三者キーリカバリ・エージェントとの契約締結を必要とするかもしれない。あらゆるまともなビジネスモデルでは、こうした例は多少なりとも追加コストを発生させるものである。

## 3.4 トレード オフ

キーリカバリのある側面は、高コストと高リスクの間で簡単にシフトできる。比較的セキュリティの高いかたちであるキーエスクロウシステムを実配備することは可能かも知れないが、これはユーザ側にとんでもないコストを要求する結果となることが多い。比較的単純で安価なキーエスクロウシステムは存在するものの、これらはセキュリティを犠牲にすることが多い。たとえば技能の低い低賃金の職員を雇い、物理的なセキュリティも低く、損害保険もかけていないような、劣悪な運営のキーリカバリ・エージェントなら、運営が高度なセンタよりは安くあがるはずだ。

おもしろいことに、セキュリティとコストは設計の段階でもトレード オフの関係にある。つまり、一番簡単な設計、一番わかりやすく、一番確認も簡単な設計は、おおむねその運用と環境について、もっとも法外な前提を必要とするか、あるいはちょっとでも崩れると全滅するといった最悪の誤動作特性を持っていたりする。たとえば、セッションキーをリカバリ・センタに送る際に、それをそのセンタの広く知られた公開キーで暗号化して送るような設計を考えてみよう。こうしたシステムを設計・実装するのは比較的簡単だし、これがある条件の下で正しく運用されている限りは安全であると証明することもできるかもしれない。しかしながら、システムとしての頑強さから見ると、これは最低最悪の設計の一つなのである。ここが崩れるとすべてが崩壊するようなポイント（リカバリ・エージェントのキー）があって、それを使ってあらゆるキーが暗号化されている。このキーが侵害されれば（あるいは細工されたキーがでまわれば）システム内のリカバー用のキーすべてが危険にさらされてしまう。（ちなみに、いくつかの市販システムは、ほとんどまさにこの設計で構築されていることを付記しておく）。

### 3.4.1 キーリカバリのきめ細かさ（Granularity）と影響範囲（Scope）

キーリカバリのコストとセキュリティに影響を与える最大の要因の一つが、キーリカバリシステムによって管理されるキーのきめ細かさ（granularity）と影響範囲（scope）である。特に、次の2点をよく理解しておくことが必要である：

**きめ細かさ（Granularity）**：リカバー可能なキーの種類（ユーザ、デバイス、セッションその他）

**影響範囲（Scope）**：リカバリ・エージェントのキーに問題があったときの影響がどこまで及ぶか

きめ細かさが重要なのは、あるエージェントによって回復可能なキーがどこまで詳細に指定できるかということ、そして必要とされるリカバリ・エージェントとの（ユーザや、法執行機関との）接触の頻度が、これで決まってくるからである。リカバリ・エージェントが「マスターキー」をつ

くり、それを使えば個別ユーザやハード装置が送受信するすべてのトラヒックが解読できる、というようなさまざまなシステムが提案されている。ほかのシステムでは、特定セッションのキーだけが回復される。きめが粗ければ（たとえば対象となるユーザのマスターキー）、回復できる内容は限られてしまう（たとえば特定の個人の全データに限るなど）が、法執行機関とリカバリ・センタとの間のやりとりは少なくてすむ。きめを細かくすれば（たとえば個別セッションのキー）、融通はきくが（たとえば特定のファイルやセッション、あるいは一定の時間内に起こったセッションだけ、など）、リカバリ・センターとのやりとり回数はふえてしまう（そしてデザイン上の複雑さも増す）。

さらに重要なのは、リカバリ・エージェント自身の秘密の影響範囲である。ほとんどのキーリカバリシステムは、ユーザのソフトやハードがリカバリエージェントの公開キーを使って自分のキーを暗号化し、リカバリエージェントに送ることを要求している。もしリカバリエージェントがそうしたキーを一つしか持っていなかったら、そのキーはとてつもなく貴重で、全地球的意義を持つ、システム全体の最大の急所となるであろう。もっとまずいことに、リカバリエージェントは自分に送られてくるキーを解読するのに自分の秘密キーを毎回使わなくてはならない（これは送られてきた時点でも、その後の解読時点でもいいが）ため、それが複製・攻撃されたり悪用されたりする可能性もまた増大する。こうしたもろさに対応するため、リカバリ・エージェントとしてはそうしたキーを、ユーザごとに一つ以上といった具合に複数用意することもできる。しかしながら、こうしたキーをユーザと協議して決め、さらにそれを配布することで、またもやシステムが複雑となり、新たな弱点も生じてしまう。

# 4　結論

キーリカバリシステムは、リカバリ機能のない同様のシステムに比べ、本質的にセキュリティが低く、高価につき、維持管理もむずかしい。法の強制執行側からの要求仕様に見合うような形での、キーリカバリに基づくインフラの大規模な導入は、セキュリティを大きく低下させ、利便性も低下し、暗号の全ユーザにとってコストを著しく押し上げることは避けられない。さらに、このようなスキームに必要とされるはずの、とてつもない規模と複雑さをもった高セキュリティ・インフラの構築は、経験的にも能力的にも、現在のこの分野の手に負えるものではなく、最終的には受け入れがたいほどの危険性とコストをもたらしてしまうおそれがある。

輸出規制、輸入や国内利用規制、国際標準を通じてキーリカバリを広範に採用するように強制しようとするにあたっては、こうした条件を考慮にいれたうえでの検討が必要である。こうしたシステムが導入されるに先だって、政府アクセスのキーリカバリのコストや便益を慎重に比較検討するような公の議論が行われることを強く要望するものである。

# 著者紹介

**Harold (Hal) Abelson** はMITのEECS学部教授であり、IEEEフェロー。共著書に教科書***Structure and Interpretation of Computer Programs***。1995年にはIEEEコンピュータ協会の教育賞を受賞。現在はMITを休職し、ヒューレット・パッカード社で同社のインターネット技術部門の科学顧問を勤める。

**Ross Anderson** はイギリスのケンブリッジ大学で、コンピュータセキュリティ、暗号学、ソフトウェア工学を教え、研究を行っている。高セキュリティシステムのエンジニアリング、その弱点と強靱性の高め方についての専門家である。商業暗号システムにおける経験が豊富であり、最近ではイギリス政府のキーエスクロウプロトコルに欠陥を発見している。

**Steven M. Bellovin** はAT&T研究所所属の暗号学、ネットワークとセキュリティ研究者である。共著書に***Firewalls and Internet Security: Repelling the Wily Hacker*** [12]がある。1995年には、Netnews創設に貢献した功績により、Usenix功労賞（Lifetime Achievement Award）を授与される。インターネット・アーキテクチャ委員会の委員でもある。

**Josh Benaloh** はマイクロソフト研究所の暗号学者であり、10年以上にわたって暗号学の研究者として活躍。秘密投票や秘密共有手法およびその応用の分野に数々の貢献を行ってきている。マイクロソフトに移る前は、トロント大学ポストドクター・フェローであり、クラークソン大学で準教授を勤めた。

**Matt Blaze** は、ニュージャージー州フローラムのAT&T研究所の研究科学者。1994年にはかれの研究がもとになってアメリカ政府の「クリッパー」キーエスクロウシステムの弱点が発見されている。暗号学分野でも活躍しており、信頼管理、リモートキー方式暗号、プロクシ暗号、IP層セキュリティプロトコルやファイルシステム層セキュリティプロトコルなど、数々の暗号上の概念やシステムに携わっている。1996年にはコンピュータとネットワークセキュリティへの貢献により、EFFのパイオニア賞を受賞。

**Whitfield Diffie** は、サン・マイクロシステムズの特別エンジニアで、セキュリティを専門としている。1998年には***Privacy on the Line***（MIT Press）をSusan Landauと共著。1976年にDiffieと Martin Hellmanは公開キー方式暗号を開発。これは、初めて連絡をとりあう者同士が符号化された情報をやりとりする際の問題を解決した方式であり、デジタル情報時代における暗号普及の基盤となった。

**John Gilmore** は事業家であり、民間リバータリアンである。初期のサン・マイクロシステムズに勤務、Cygnus SolutionsやElectronic Frontier Foundation、サイファーパンク、インターネットの「alt」ニュースグループを共同創設。コンピュータ産業で20年の経験を持ち、プログラミング、ハードウェアとソフトウェアのデザイン、マネジメントなどを行ってきた。

[12]『ファイアーウォールとインターネットセキュリティ』、ソフトバンク

**Peter G. Neumann** はSRIのコンピュータ科学研究所の主任科学者。リスクフォーラム（comp.risks）のモデレータであり、著書に ***Computer-Related Risks*** (Addison-Wesley)、共著書に National Research Council 調査報告 ***Cryptography's Role in Securing the Information Society*** （National Academy Press）がある。AAAS、ACM、 IEEE のフェロー。

**Ronald L. Rivest** は MIT の EECS 学部における、電気工学とコンピュータ科学の Webster 教授である。MIT コンピュータ科学研究所の副所長でもある。おそらく RSA 公開キー式暗号システムの共同発明者および RSA Data Securities 社の共同創設者としてもっとも有名であろう。

**Jeffrey I. Schiller** は MIT のネットワーク・マネージャであり、1984 年の開設以来、MIT の構内コンピュータネットワークを管理運営してきた。Schiller は Kerberos 認証システムの作者であり、Internet Engineering Steering Group のセキュリティ部門責任者をつとめ、インターネット工学タスクフォース（IETF）のセキュリティ関連ワーキンググループ統括を行っている。

**Bruce Schneier** は Counterpane Systems 社社長である。同社はミネアポリスのコンサルティング会社であり、暗号とコンピュータセキュリティを専門としている。Schneier は ***Applied Cryptography*** の著者であり、Blowfish と Twofish 暗号アルゴリズムの考案者でもある。