コンピュータセキュリティ 10－9
(2000. 7. 25)

キーエスクロー以降の通信傍受: 歴史的分析

山根 信二† 相場 徹‡ 村山 優子†
s-yamane@soft.iwate-pu.ac.jp aiba@vacia.is.tohoku.ac.jp murayama@iwate-pu.ac.jp

†岩手県立大学ソフトウェア情報学部
‡東北大学大学院情報科学研究科

あらまし 暗号技術はナショナル・セキュリティを中心に位置づけられがちだが、それだけでは暗号の民間利用を正当に評価することができない。またキーエスクローをめぐる論争を政治的係争(「政府と産業界と市民の対立」や「プライバシーと法執行とのバランス」)として捉える見方ではIAB, IETFなど専門家集団による技術的分析を扱うことがきない。

日米のキーリカバリー提言は1998年に途絶えた。しかし通信傍受の要請がなくなったわけではない。IETFその他において争点となっている通信傍受の要請は、もはや1990年代に唱えられた暗号規制の枠組みでは説明できない。

キーワード キーエスクロー、RFC 1984、IAB、IETF

Surveillance after Key Escrow: Historical Analysis

Shinji Yamane† Tooru Aiba‡ Yuko Murayama†
s-yamane@soft.iwate-pu.ac.jp aiba@vacia.is.tohoku.ac.jp murayama@iwate-pu.ac.jp

†Faculty of Software and Information Science, Iwate Prefectural University
‡Graduate School of Information Sciences, Tohoku University

Abstract The status of cryptography is often offered as the national security issue. Such viewpoint fails to explain the status and history of private use of cryptography. The struggles over the key escrow in 1990s has been described as the political issue: the tradeoff between privacy and law enforcement, however, it fails to notice the risk analysis based on the technical review by professional organizations such as IAB statement.

Though the international key escrow lobbying was over, the needs for the electronic surveillance still remain. New surveillance scheme that is discussed at IETF is different from the key escrow scheme in 1990s anymore.

key words key escrow, RFC 1984, IAB, IETF

1 1990年代の暗号政策の枠組み

1990年代の暗号をめぐる議論はキーエスクロー(暗号鍵供託)を抜きにしては語ることができない。ここでいうキーエスクローとは、法的手続きによって暗号化された通信内容の電子的監視を行なうシステム[22, s.v. "key recovery."]のことを指している[1]。

日本の政策において、キーエスクロー構想はアメリカからの輸入というかたちをとってきた。たとえば1997年に郵政省審議会の「ネットワークを通じた認証業務の在り方に関する調査研究会報告書」[19]が、アメリカではキーエスクロー[1]の導入が決定され国際的にも採用が呼かけられていると報告している。この年には、警察庁外郭団体による情報セキュリティ調査研究委員会報告書[14]もキーエスクローが国際社会において「極めて高い関心を持って議論されている」ことを報告している。そして翌1998年には警察庁の情報セキュリティビジョン策定委員会の報告書[15]が、暗号化された情報へのアクセスの必要性、キーエスクローセンターおよび公証機関(certification authorities, CA)の適格性及び業務の適正性確保、日本国内にある暗号利用者が利用できる鍵回復機関を限定する方策を検討する必要、といった課題について報告を行なっている。

この動きは審議会レベルにとどまるものではない。1998年の警察白書[17]でも「暗号の不正利用を防止するための法制」の整備が提言され、そして政府の高度情報通信社会推進本部も「暗号技術の不正利用対策については、必要に応じた法的環境整備の検討を行う」ことを基本方針[18, II-7]の中で明言している。

こうした1998年までの動きはすでに「もう死んでしまった過去の話」[23]であり、それを解説するのは本稿の目的ではない。キーエスクロー構想が途絶えた後、今後の暗号政策はそれまでに唱えられた必要性とは異なる必要性によって推進されることが考えられる。そこで今後の争点を考えるために、1990年代の争点では捉えられない新しい問題を分析する。

[1]鍵供託、キーリカバリー(鍵回復)という表現もあるが、本論では引用を除いてキーエスクローという呼称で統一する。

2 キーエスクロー構想の再検討

1990年代のキーエスクロー構想をめぐる議論は単なる暗号インフラの選択にとどまらず、暗号問題の歴史的政治的位置づけが試みられていた。その枠組みにおいて捉えられなかった問題について検証を行なう。

2.1 歴史的枠組みの検証

キーリカバリーをめぐる議論において、シーザー暗号から暗号の歴史と意義を語り起こし、暗号技術の古典的用法は軍事や外交におけるものだという暗号史がしばしば語られてきた(最近のものでは郵政省研究会による「21世紀デジタル社会の暗号政策への提言」[2]がある)。また、近年のパーソナルコンピュータの普及によって、暗号技術がナショナルセキュリティの領域からプライベートな領域へと大衆化したという主張も珍しいものではない。

しかし、国家から民間へという暗号技術の位置づけは暗号の歴史を一面的に見ていると言わざるをえない。たとえばKahnの*Codebreakers*[16, pp. 74–75]では古代において単文字換字暗号の利用が推奨されていた事例として、インドのカーマスートラ(*Kāmasūtra*)の記述[21](暗号化手法についての記述はA.D.400以降ではないかと推測されている)を挙げている。軍事や外交といったナショナルセキュリティの視点ではこういった民間暗号の歴史を説明することができない。

2.2 政治的枠組みの検証

1990年代の暗号政策は、もっぱら政治的対立や利害の調整という枠組みから論じられてきた。その枠組みでは、キーリカバリーをめぐる議論はプライバシー保護と公共の安全確保とのバランスをどのようにとるかといったトレードオフや、市民と政府と産業界との要請の対立によって説明される。だが、その枠組みの中では暗号

技術の専門家を位置づけることができない。専門家は政治判断や利害調整を現場に反映させるだけなのだろうか?

キーエスクローをめぐる問題を単なる政治的決着として処理してしまわないためにも、ここで暗号技術の専門家の果たした役割について明らかにしておく必要がある。たとえばPGPの開発と配布においてCPSR(社会的責任を考えるコンピュータ専門家の会)やMIT Laborarory for Computer Scienceといった組織の専門家が果たした役割はすでに知られている[9]。それに対して、本稿では特定の国や暗号製品の問題ではなく国際的かつ原理的な問題を扱いたい。そのために、Internet技術における暗号について分析を行なう。

2.3 Internet技術標準と政府の暗号規制

RFC 1984の声明 公共の安全確保のためには法執行機関が公正な手続きにより暗号化された情報にアクセスできるべきである、というキーエスクロー提案に対して、1996年に出されたRFC文書がRFC 1984[2], "IAB and IESG Statement on Cryptographic Technology and the Internet"[13]である。この声明の中で、IABとIESGはすべての国のすべてのInternet利用者が強力な暗号技術にアクセスできる政策を支援することを表明している。そしてその根拠として、国際的な商業的トランザクションを保護しInternet利用者にプライバシーを提供することがあげられている[3]。

RFC 1984の特徴 RFC 1984は一見して産業界と政府、もしくは市民と政府との対立という図式で説明できるように思われるが、それだけでこの声明の特徴を説明できない。RFC 1984の特徴はその国際取引への志向以上に、技術評価に基づいたリスク分析にある。

RFC 1984は5ページという短い分量の中で、様々な暗号規制について技術的に困難であること、かえってリスクが高いことを論じている。この中で言及される政府の暗号規制は、輸出規制、暗号化に用いる鍵の長さの制限、キーエスクロー、暗号の使用禁止といった諸形態に及んでいる。中でも詳しいのはキーエスクローについての議論である。たとえばCAとエスクローセンターとを区別することで、暗号鍵を保証しなりすましを防ぐことと暗号鍵を預けることの区別を強調している。また、国際的なキーエスクローの抱える問題にも多くの分量を割いている。

なぜRFC 1984がキーエスクローの具体的システムについて詳述しているのか、という理由は2000年現在の時点ですでにわかりにくくなっている。これを説明するには、1996年当時の国際情勢を理解しておく必要があるだろう。1995年12月からOECD(Organization for Economic Cooperation and Development)で開かれた暗号専門家による特別会合をはじめとする国際的な舞台で、アメリカの機関による国際的なキーエスクローシステムのロビイングが進められていた。この動きは政策の洗浄(laundering)だとも報じられる[20, pp. 321–324]。これは、当時のアメリカ国内ではキーエスクローは "The Bosnia of telecommunications" と呼ばれるほどの抵抗を呼んでおり、国内でのキーエスクローを進めるために国際的協調体制を利用していると考えられたためである。

RFC 1984が作成されたのはまさにこの時期であり、その分析は当時唱えられていたキーエスクローを強く意識したものになっている。つまり、RFC 1984がCAとエスクローセンターとの峻別や国際的キーエスクローに分量を割いているのは、各国が提示するであろうモデルを具体的に想定していたためである。たとえば、アメリカの動向が輸入された日本でも(冒頭に挙げたように)CAについての審議会報告でキーエスクローの紹介が行なわれたことがそれを物

[2]おそらくこのRFC番号は近未来小説 *1984* にちなんだものだろう。RFC EditorにはRFのCナンバリングについてある程度の裁量が認められてきた。たとえば、RFC EditorのJoyce K. Raynoldsは功労者Jon Postelを追悼する文書に対して特別に2468という番号を予約したことがある[6]。

[3]ここであげられている根拠は、1990年代のInternetの状況の変化を反映しているとも言えるだろう。すでにこの時期、国際的な民間業者の相互接続はInternetにおいて主要な位置を占めていた。RFC 1984が出る前年の1995年には、アメリカの主要なバックボーンネットワークはネットワークプロバイダーの相互接続によって運営されている。

語っている。

他の声明との比較　RFC 1984の特徴として、声明が技術的分析に基づいていることを挙げた。その他の特徴として、「プライバシー権と法執行のトレードオフ」といった議論を行なわないこと、そしてその作成プロセスがRFC独特のものだったことも挙げられる。

この声明が作成された経過は単純なものではない。それ以前は、IABでもキーエスクローについての評価は定まっていなかったからである。キーエスクロー構想が具体的に唱えられたのはアメリカのクリッパーチップ計画に遡ることができるが、IABはクリッパーチップ計画にははっきりとした態度をとっていなかった。RFC 1984が出る2年前に出されたIABワークショップの報告[5]では、クリッパーチップに対する様々な見方があることを示しているのみである。つまり、1994年の時点ではIABはクリッパーチップ問題について態度を決めることができなかったが、それから2年後にはクリッパーチップのみならず暗号規制についての包括的な原則をまとめたと言うことができる。

RFC 1984の作成は公開で行なわれており、その過程をみると作成には2年間どころか2,3ヵ月しかかかっていないことがわかる。その経過は以下のようなものだ。まず1996年6月11日にIABのオンライン会合で「クリッパーの後釜」について討議され、"This has been positioned by the government as primarily a political issue: the tradeoff between privacy and law enforcement."[24]という意見がでている。この時点から「プライバシー権対法規制のトレードオフ」という対立図式が疑われていたことは特筆に値する。そしてこのオンライン会合に続いて、6月26日にMontrealで開かれた36回IETF大会でのIAB公開ミーティングにおいて、この声明の作成が告知されている[25]。さらに翌月の7月には、IABの作成中の声明に対してIESGが共同声明に加わることに賛同する[8]。こうして声明は8月にRFC 1984として発行された。

OECDでの動向に呼応して、コンピュータ専門家の国際団体から政府による暗号利用の法的規制を憂慮する声明が幾つか出された。RFC 1984もその中の一つに数えることができるが、それらの声明を比べた時にその特徴をはっきりさせることができる。たとえば、IFIP (International Federation for Information Processing)による暗号普及を推進する声明は同じ時期に同じ問題意識で作成を開始している[10]。しかしそれが公示されるには1998年まで待たなくてはならなかった[11, 12]。それに比べてRFC 1984の作成は迅速だった。この速度差はアメリカの提言を持ち帰った各国政府の動きに対しても当てはまる。結局、各国政府はInternet専門家との間に大きな隔たりをつくることになる。

ここまで1996年のRFCの暗号セキュリティについての声明を分析した。技術的分析に基づいた声明がいちはやく出された重要性は無視することのできないものである。また、プライバシー保護と法規制とのバランス図式だけではInternet技術の専門家による声明を読み解くことができないことも強調したい。

3　今後の通信傍受政策

キーリカバリー提言が途絶した現在、暗号規制の動きは新たな視点から捉え直す必要があるだろう。最後に、今後問題になるであろう通信傍受政策について論じる。

すでに現在、1990年代の暗号規制を焦点とした争点では捉える事ができない通信傍受の要請が進行している。1990年代末に登場したアメリカの捜査機関からの新たな提案として、FIDNET構想[1]やgateway-based encryption (あるいは"private doorbell" sheme)の提案を挙げることができる。

前者のFIDNETは、集中監視センターによって全米の連邦政府ネットワークの侵入を検知するという構想である。これについてはACM[1]がパネルを開いている。後者はend-to-endの暗号化ではないgateway間による暗号化において、gatewayに通信傍受機能を組み込むことを提案したものだ。これは電話における交換機での通信傍受措置をVoice over IPなどのMedia

Gatewayに適用するという考えにもとづいている。この二つの提言は、アメリカの国内政策とInternet技術標準という違いはあるが、どちらもネットワーク設計への法執行機関の介入として理解することができる。暗号鍵を誰が管理するのかといった視点ではこれらのネットワークモデルに関わる問題に対処できない。セキュリティについてのより技術的原則が問われなければならない。

gatewayに通信傍受機能を付加する要請に対し、IABは即座に声明を出している[26, 3]。それに加えて、やはりここでも公開討議による技術的分析が行なわれたことを見逃すわけにはいかない。この討議はIETF大会やInternet-Draft[7]の作成を通じて行なわれ、その成果はRFC 2808, "IETF Policy on Wiretapping"[4]として2000年5月にRFCとして出されている。RFC 2808では、gatewayの問題に限定されない通信傍受についての原理的な議論がなされている。さらに、セキュアなネットワークはいかにあるべきかという原則としてRFC 1984の声明が再確認されている。技術的分析にもとづいたRFC 1984の原則はキーエスクロー後も継続されている。

4 まとめ

1990年代のキーエスクローをめぐる議論では、プライベートな暗号利用や、技術的な分析にもとづくコストやリスクの評価が正当に位置づけられなかった。そして暗号をめぐる問題は政治的な問題として扱われてきたために、それらとは直接つながりのない専門家集団が打ち出した原則がみえにくくなっている。キーエスクローとは異なる通信傍受の要請が起こりつつある現在、技術的な分析にもとづく原理的な考察を再確認する必要がある。

参考文献

[1] FIDNet and the Government's Role in Computer Surveillance, http://www.acm.org/fidnet/ (1999).

[2] 暗号通信の在り方に関する研究会21世紀デジタル社会の暗号政策への提言, 郵政省 (June 1999), http://www.mpt.go.jp/policyreports/-japanese/group/internet/ninshou/.

[3] BOARD, I. A. IAB statement on "private doorbell" encryption, http://www.iab.org/iab/121898.txt (Oct. 1998).

[4] BOARD, I. A. and GROUP, I. E. S. IETF Policy on Wiretapping, *Request For Comments* (May 2000), RFC 2804 (Status: Informational).

[5] BRADEN, B., CLARK, D., CROCKER, S. and HUITEMA, C. Report of IAB Workshop on Security in the Internet Architecture - February 8-10, 1994, *Request For Comments* (June 1994), RFC 1636 (Status: Informational).

[6] BRADEN, R., REYNOLDS, J. K., CROCKER, S., CERF, V., FEINLER, J. and ANDERSON, C. 30 Years of RFCs, *Request For Comments* (7 April 1999), RFC 2555 (Status: Informational).

[7] CARPENTER, B. and BAKER, F. IETF Policy on Wiretapping, *Internet Draft* (February 2000), draft-iab-raven-01.txt. Expires in August 2000.

[8] COYA, S. Internet Engineering Steering Group (IESG) July 11, 1996, IESG meeting report, ftp://ftp.ietf.org/iesg/iesg.96-07-11 (July 1996).

[9] GARFINKEL, S. *PGP: Pretty Good Privacy*, O'Reilly & Associates (Dec. 1994), chapter 4 & 5.

[10] TC11 Strives for International awareness of Cryptographic Policies, *IFIP Newsletter*, **13**, 3 (Sept. 1996), 4,

http://www.ifip.or.at/newsletters/nl3q96.-htm.

[11] IFIP Policy on Cryptography Is Proposed, *IFIP Newsletter*, **15**, 1 (Mar. 1998), http://www.ifip.or.at/newsletters/nl1q98.-htm.

[12] INTERNATIONAL FEDERATION FOR INFORMATION PROCESSING, The IFIP Position on Cryptopolicies, http://www.ifip.or.at/statements.htm (1999).

[13] INTERNET ARCHITECTURE BOARD AND INTERNET ENGINEERING STEERING GROUP, IAB and IESG Statement on Cryptographic Technology and the Internet, *Request For Comments* (Aug. 1996), RFC 1984 (Status: Informational).

[14] 情報セキュリティ調査研究委員会 情報セキュリティ調査研究報告書, 日本実務出版 (Apr. 1997).

[15] 情報セキュリティビジョン策定委員会 情報セキュリティビジョン策定委員会報告書: 安全なネットワーク社会の実現を目指して (Feb. 1998), http://www.npa.go.jp/hightech/secv_repo/ (オンライン版, 1998.3.20 公開).

[16] KAHN, D. *The Codebreakers: The Story of Secret Writing*, Scribner, Revised edition (1996), chapter 2, Originally appeared in 1967.

[17] 警察庁 平成 10 年警察白書: ハイテク犯罪の現状と警察の取組み (1998).

[18] 高度情報通信社会推進本部 高度情報通信社会推進に向けた基本方針 (Nov. 1998), http://www.kantei.go.jp/jp/it/981110kihon.-html.

[19] ネットワークを通じた認証業務の在り方に関する調査研究会 報告書, 郵政省 (1997), http://www.mpt.go.jp/policyreports/-japanese/group/internet/index-net-n.html.

[20] SCHNEIER, B. and BANISAR, D. eds. *The Electronic Privacy Papers: Documents on the Battle for Privacy in the Age of Surveillance*, John Wiley & Sons, New York (Aug. 1997).

[21] SHASTRI, G. D. *Kāmasūtra by SrīVātsyāyana Muni, with the commentary Jayamangala of Yashodhar*, No. 29 in Kāshi Sanskrit Series, Benares (1929).

[22] SHIREY, R. W. Internet Security Glossary, *Request For Comments* (May 2000), RFC 2828 (Also FYI 36) (Status: Informational).

[23] 鈴木裕信 時代遅れな「キーエスクロー」, *Internet Magazine*, 56 (Sept. 1999), 330–331.

[24] WEINRIB, A. Minutes for June 11, 1996 IAB Teleconference, Online minutes (July 1996), http://info.internet.isi.edu/IAB/IABmins.960611.

[25] WEINRIB, A. Minutes for Open IAB Meeting at Montreal IETF Meeting–June 26, 1996, Online minutes. ftp://ftp.ietf.org/ietf/96jun/iab-minutes-96jun.txt (1996).

[26] WEINRIB, A. Minutes for July 14, 1998 IAB Teleconference (Final), Online minutes (July 1998), http://info.internet.isi.edu/IAB/IABmins.980714.

(URL は 2000 年 7 月 1 日時点のもの)