

〈ネット・ポリティックス2001～2002 — 戦うインターネット・コミュニティ —〉
第10回

暗号戦争の10年

—インターネット・コミュニティの闘士たち—

土屋大洋

(GLOCOM主任研究員/ジョージ・ワシントン大学サイバースペース政策研究所訪問研究員)

ジョン・ナッシュの悪夢

今年のアカデミー賞で最優秀作品賞などを受賞した映画『A Beautiful Mind (邦題: ビューティフル・マインド)』では、主人公ジョン・ナッシュがアメリカ政府に協力して暗号解読を行っていた姿が描かれている。ナッシュ教授が本当にそうした役割を担ったのかどうかはよくわからない。しかし、実際に多くの数学者などが、政府の暗号解読に協力させられている。ある者は政府機関の職員として名前も知られることなく職務を果たし、別の者は大学教授などを務めながら機密の職務に従事している。

アメリカの暗号への取り組みは、第一次世界大戦ごろから本格化している。しかし、第一次世界大戦が終わると、いったん止まってしまう。フーバー政権の国務長官ヘンリー L. スティムソンが、外交文書を盗み見てはいけないとして、暗号局を閉鎖してしまったからだ。

これに反発したのがハーバート O. ヤードレーである。彼は1931年に『ザ・アメリカン・ブラック・チェインバー (The American Black Chamber)』という本を出版し、アメリカ暗号局の実態を暴露した。ヤードレーは、ブラック・チェインバーと呼ばれる暗号局の創設者であり、そのトップでもあった。第一次世界大戦での活躍にもかかわらず、評価されることなく閉鎖に追い込まれたのを不服とし、かつ他国も同じことをやっているのにアメリカだけやめてしまうのはナイーブではないか、とスティムソン長官を批判した。

しかし、第二次世界大戦の危機が迫ってくると、密かに暗号局は復活する。そこで活躍するのが、ウィリアム・フリードマンである。フリードマンは暗号の天才として数々の暗号の解読に成功し、アメリカの勝利に貢献した。彼の胸像が国家暗号学博物館に置かれている。

そして、フリードマンほど有名ではないが、その他、数多くの数学者やパズルの天才がアメリカ政府の下に集められた。それは第二次世界大戦後も、1952年に密かに設立されたNSA (国家安全保障局) に受け継がれ、

今日に至っている。映画『ビューティフル・マインド』の冒頭でも、数学者たちによる日本の暗号解読が戦争の勝利に貢献したと大学院の教授が新生に訓示するくだりがあるが、そうした時代背景がジョン・ナッシュにも影響したのだろう。

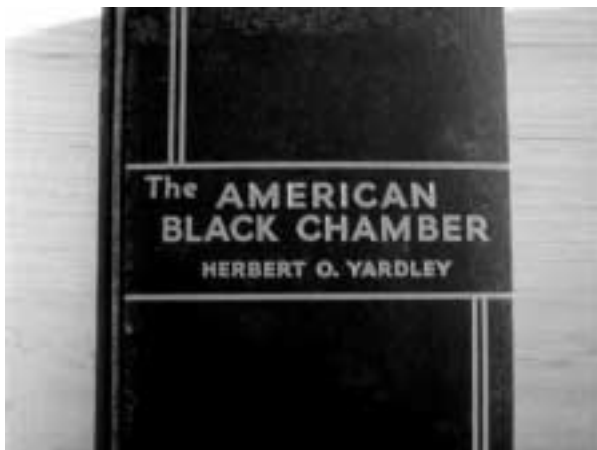
闘士ジーマン

冷戦時代の暗号はスパイが使うものであり、一般大衆にとっては好奇心の対象以外の何物でもなかった。しかし、1970年代に公開鍵暗号が発明され、暗号がソフトウェア化、汎用化することによって様相は変わってきた。国家対国家の暗号戦争に加えて、1990年代は政府とインターネット・コミュニティの間の戦争となった。

無論、戦争といっても武力によるものではない。アイデアと技術と法律による戦いである。アメリカ政府は、二つのタイプの暗号規制を導入した。ひとつは「クリッパー・チップ」、「キー・エスクロー」、「キー・リカバリー」などと呼ばれるもので、アメリカ国内外で利用される暗号に、アメリカ政府がいざというときに復号できる裏鍵を作るというものである。クリッパー・チップは、電話やファクシミリ、コンピュータなどに埋め込まれる半導体集積回路のことで、このチップがあると裏鍵が自動で生成される。キー・エスクロー (鍵供託) は、裏鍵を政府機関に預けておくというものである。キー・リカバリー (鍵回復) は、キー・エスクローに対する批判を受けて変更されたもので、民間の機関に預けてある鍵をいくつか組み合わせることでソフトウェア的に復号するというシステムである。

もうひとつの規制は、強力な暗号製品を国外に輸出させないというものである。アメリカ国内ではどんな強力な暗号も使えるが、国際犯罪やテロを防止するために、一定強度以上の暗号は輸出させないというものである。

4月、サンフランシスコでCFP (Computers, Freedom & Privacy) という会議が開かれた。この会議には毎年、政府の暗号規制に反対する活動家やエンジニアたちが集まってくる。今年のテーマは9月11日のテロ以降、



『ザ・アメリカン・ブラック・チェインバー』の表紙

にわかに高まってきた政府によるネット規制にどう対処するかということであった。たくさん集まった人たちの中で、ひときわ注目を集めていたのがフィル・ジーマーマンである。

ジーマーマンは、政府対インターネット・コミュニティの暗号戦争におけるもっとも勇敢な闘士のひとりであろう。1980年代のレーガン政権の軍事志向に危機感を抱いたジーマーマンは、平和運動へのめりこむ。その過程で彼は、プライバシーを守ること、政府から情報を守ることの重要性に気づいた。たとえば、平和運動に献金をしてくれた人のリストが政府の手に渡らないようにすることは、運動の維持のために不可欠であった。そこから暗号技術への取り組みが始まる。

ジーマーマンは、ほぼ独学で暗号のプログラミングを始め、PGP (Pretty Good Privacy) という個人用の暗号ソフトウェアを書いていた。そこに、議会で暗号利用を規制する法案が審議されるとの情報が入り、彼は急ぎPGPを完成させた。彼は完成したソフトウェアを友人に渡し、友人を介してPGPはインターネット上にアップロードされ、世界中の人がそれをダウンロードし、あっという間に拡散してしまった。1991年のことである。

そこへ突然、アメリカ政府の税関担当官がやってきた。どうやってPGPが公開されたのかを調べ始めたのである。インターネットで公開するということは、海外からもアクセスできるようになるということであり、輸出に当たるとはならないかという嫌疑をかけてきた。当時の区分けでは、暗号は兵器であり、政府の許可なく輸出してはいけなかったのである。

ジーマーマンは政府にいやがらせをするためにPGPを作って公開したわけではない。アメリカ人には政府の干渉を受けることなくプライバシーを守る権利がある。さらに、抑圧的な政府を持つ国々で、政府の追及の手を逃

れながら反政府運動を組織するツールとしてもPGPは有効であると考えたのである(実際に、そうした人々からジーマーマンに対してPGP公開のお礼のメールが届くようになった)。

彼は政府の捜査に対抗するために、いくつかの手段を講じた。まず、マサチューセッツ工科大学(MIT)のFTPサイトでPGPを公開してもらった。その結果、MITとジーマーマンは同罪になったのである。ジーマーマンは、「MITと自分を同等に扱わなくてはならない」と主張した。MITを訴えるということになれば、人々の広範な関心を引きつけることになるにちがいがなかった。

次に彼は、PGPのソース・コードすべてを記載した本をMIT出版から発売した。本の出版は、表現の自由の保護という点から、アメリカでは聖域になっている。言論に政府が口を出すことはほとんど不可能である。出版された本の流通に規制をかけることもむずかしい。したがって、本は輸出可能である。MIT出版というプレステージの高い学術出版社の本の輸出を、政府は止められるだろうか。ジーマーマンたちは、政府が止められないことを知っていてあえてそうしたのである。

輸出された本をスキャナーで読みとれば、手間はかかるが、完全なソフトウェアの複製をアメリカ国外で作ることができる。ジーマーマンは筆者とのインタビューのなかで、「私たちは暗号の輸出規制の効果を台無しにしたのです。そして、輸出規制の継続を意味しないものになりました」と述べた。

結局、ジーマーマンは3年間捜査対象となったものの、1996年1月に突然、捜査打ち切りを宣言するファクシミリを受け取り、訴追されることなく、裁判も行われなかった。ただ、この3年間、彼は訴追されないようにするためにさまざまな法的対応をせねばならず、弁護士の助けを必要とした。しかし、弁護士たちの多くがボランティアで彼を支援した。彼の暗号輸出規制に対する挑戦を知ったインターネット・コミュニティの住人からも、支援の電子メールや資金援助が寄せられ、ジーマーマンは「たくさんの人が味方していると感じた」という。

本の出版は輸出か

アメリカでも、最近はずいぶん暗号に関する出版物が急激に増えてきているが、ブルース・シュナイアーの『応用暗号 (Applied Cryptography)』は10万部売れたそうである。758ページもある分厚い技術書なのだが、売れたのには訳がある。表紙の宣伝文句にもなっているように、「NSAが出版させたくなかった本」であり、人々の耳目を引く話題になったからである。NSAはアメリカ政府

の暗号政策の総元締めである。なぜNSAがこの本を問題にしたかという点、『応用暗号』には、アメリカ政府の標準暗号であるDES (Data Encryption Standard) やその他のソース・コード(プログラム)が印刷されていたからである。ジーマーマンのケースと同じく、アメリカ政府は本の出版と輸出を認めざるを得なかった。

そして、さらにこれに挑戦した人物がいる。クアルコム社のネットワーク・エンジニア、フィル・カーンが、暗号規制はばかげているとして、国務省を相手に訴訟を起こし、この本に印刷されているソース・コードを電子的に書き起こしたフロッピー・ディスクが輸出可能であることを認めさせようとしたのである。

カーンは、シュナイアーの依頼でこの訴訟を始めたわけではない。彼のウェブ・ページによれば、「私が『応用暗号』を選んだのは、広く普及しており、IDEAやDESといった強力な暗号のソース・コードを広範に載せているからである」*1とある。

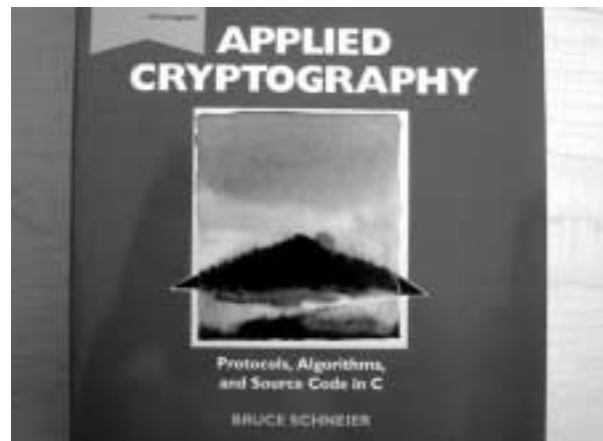
国務省と、その後暗号規制を引き継いだ商務省は、カーンのフロッピー・ディスクをアメリカの軍需品リストに分類した。つまり、輸出禁止にしたのである。カーンは、同じ内容が外国のウェブ・サイトにすでに何年も前から載せられており、アメリカ人だけがC言語のプログラムを書けると考えるのはばかげていると主張した。

彼は裁判に勝つことはできなかったが、アメリカ政府は2000年に暗号輸出規制を緩和し、結果的に彼の主張は認められることになった。カーンは「これが裁判での実際の勝利ほど満足のいくものではないことは確かだが、一切の現実的な目的からして、私が欲しかったものはすべて手に入れた」として、訴えが棄却されるのを容認した*2。

議会での攻防

議会でも繰り返し暗号規制に関する法案が提出され、公聴会も開かれてきた。たとえば、1997年3月19日、上院の商業・科学・運輸委員会で開かれた公聴会を見てみよう*3。FBIのルイス J. フリー長官、商務省輸出管理局のウィリアム A. ラインチ次席、ネットスケープ社CEOのジェームズ・バークスデール、NSAの副長官ウィリアム・クロウウェルが証言者として呼ばれた。FBI、商務省、NSAは、言うまでもなく政権を代表して暗号規制を推進する組織であり、ネットスケープは暗号技術の利用者として規制に反対する立場である。

公聴会の冒頭、委員長ジョン・マッケイン上院議員(共和党—アリゾナ州)は、「21世紀へ向かうにつれ、情報時代の仕事に必要な道具を、法執行機関や国家安



『応用暗号』の表紙

全保障に携わる人々に提供しなくてはいけない」としながらも、「暗号技術は非常に重大な商業上の懸念を見せ始めている」と問題提起している。またコンラド・バーンズ上院議員(共和党—モンタナ州)は、「外国の顧客は、他に選択肢があるなら、アメリカの法執行機関のための裏口がついた製品を買うわけがない」と指摘した。政府による規制に反対の立場をとるパトリック J. レイヒー上院議員(民主党—バーモント州)は、「アメリカ人はオンライン通信とコンピュータ・ファイルのプライバシーを守るために、もっとも適した暗号化方法を選ぶ自由を持つべきだ」と主張している。

最初に発言を求められた規制推進派のFBIのフリー長官は、「厳しい規制の下で復号された平文の情報にタイムリーにアクセスできるということが、公共の安全上必要であると強く感じる」と主張する。つまり、キー・エスクロー・システムが必要だというのである。次に、商務省のラインチは、「暗号を広範にコントロールしないことから生じる安全保障と法執行に対するリスクは、輸出規制の継続を正当化する」と主張する。さらに、NSAのクロウウェルは、「技術的な観点からして、鍵管理インフラの登場は必要でもあり、不可避でもあるとNSAは考えている」という。

これに対し、ネットスケープ社のバークスデールは、強力な暗号の輸出規制のために「私は世界中の顧客に製品を売りたいのだが、グローバル市場では競争できない」という。そして、「テロリストや犯罪者は、欲しければいつでも暗号を入手できる」として規制が無意味であると主張する。

こうした議論を受けて、バーンズ議員がラインチに質問する。

バーンズ議員:たとえばあなたと私が犯罪を考えている



暗号通信を使っていないサイト:
ブラウザ(この場合はネットスケープ)の左下の鍵が開いている



暗号通信を使っているサイト:
ブラウザ(この場合はネットスケープ)の左下の鍵が閉じている

とすると、私は出かけて行って124ビットのプログラムを買って、アメリカの中で使うことができる、こういうことですね。

ラインチ:そうです。

バーンズ議員:私は国内で買うことができます。

ラインチ:そうです。

バーンズ議員:では、われわれは海外に行っても使うことができます。われわれのうちどちらかが海外にいても使える。そういうことになりますか。

ラインチ:いいえ。それを海外に持っていったら、それを輸出していることになります。

バーンズ議員:ちょっと待ってください、待ってください。私とあなたの話です。私たち両方がフランスに行くとする…。

ラインチ:つまり、(暗号製品を)持って行くのですね。

バーンズ議員:そうです。一緒に持って行くのです。

ラインチ:では輸出することになります。

バーンズ議員:いや、私とあなたが使うだけで、それだけのことですよ。

ラインチ:一緒に持っていけば、輸出することになります。

バーンズ議員:私はそれをまだ所有しているんですよ。

クロウウェル:個人利用条項があるでしょう。

バーンズ議員:ええ、彼(バーンズ議員)が考えているのがそれだけならば、そうです。

クロウウェル:彼は個人利用のことを話しているのだと思います。

ラインチ:わかりました。

クロウウェル:しかし、フランスは彼がそれを持ち込むのを認めないでしょう(笑)。

バーンズ議員:別の国を挙げてください。イギリスはどうですか。

ラインチ:イギリスは大丈夫です(笑)。

(議会資料²⁴より引用)

最後のフランスが持ち込みを認めないというくだりは、当時、フランスが暗号の国内利用も禁じていたという背景がある。いずれにせよ、輸出規制には明らかな問題があった。当時、アメリカ国内で使われていたWWWのブラウザには、輸出規制にひっかかる暗号が組み込まれており、それをインストールしたまま、多くのビジネスマンが海外出張に出かけていたのである。アメリカから出国するビジネスマンのラップトップを全部空港でチェックするのはばかげているし、彼が個人利用に限定するかどうかを確認できるとは思えない。

ジョン・ケリー上院議員(民主党—マサチューセッツ州)が、国際的な流れについて、「他の国では(テロや犯罪に対する)懸念が増えており、こうした(暗号を規制する)方向に進んでいるとっていいのだろうか」と質問した。これに対し、ラインチとクロウウェルはイエスと答えた。しかし、パークスデールは、テロに対する懸念が高まっているのはその通りだが、だからといってアメリカ政府の規制に彼らが従うと考えるのは間違いだと反論した。

1999年3月18日の下院国際関係委員会国際経済・貿易小委員会の公聴会では、ワシントンに本拠を置く代表的なプライバシー団体であるCDT(Center for Democracy and Technology)のアラン・デービッドソンが証言している。彼は、「アメリカの暗号政策は国際的な場では失敗しています。2年前にすでに、世界の国々はキー・リカバリーと輸出規制をすぐにも採用するはずだと(アメリカ政府は)いっていましたが、実際には、市場は輸出規制もキー・リカバリーも歓迎しませんでした。(中略)アメリカの暗号政策は裁判所でも失敗しています。今月はじめ、第9巡回控訴審は暗号ソース・コードに関する輸出規制は、(表現の自由を定めた)憲法修正第一条に違反するという判断を出しています」と主張した²⁵。

産業界の支援を受けたプライバシー団体であるACP(Americans for Computer Privacy)の代表エドワード・ギレスピーは、1999年3月4日、下院司法委員会で開かれた公聴会で、「現実的な政策を持たなくてはならない」と証言した²⁶。「もし、われわれアメリカが指導的な地位を失ったらどうなるでしょうか。国家安全保障を担う機関は、アメリカ企業ではなく、外国企業が作った暗号が蔓延するという事態に直面するでしょう。もし、もともと洗練された暗号技術の専門家と製造業者が外国に住んでいたとしたら、国家安全保障を担う機関は、技術的な手助けをどこに求めればいいのでしょうか」と訴えた。

規制緩和の要因

上記のようなさまざまな取り組みと議論の末、1998年以降、暗号規制は段階的に緩和されていったのだが、アメリカ政府が規制緩和に踏み切った本当の理由は何だったのだろうか。私はこの点について三つの仮説を立ててみた。

第一の仮説は、インターネット上で暗号ソフトウェアがどんどん手に入るようになり、暗号規制そのものの意味がなくなってしまったというものである。

第二の仮説は、ネットスケープのような民間企業が政府に圧力をかけ、国際競争力の点から規制緩和に踏み切らせたというものである。

第三の仮説は、CDTのようなプライバシー団体、インターネット・コミュニティの圧力が高まり、規制緩和が進んだというものである。

この三つの仮説を、当時、商務省で実際の政策過程に携わっていた二人におつけてみた。

ひとりにはエリオット・マックスウェルである。彼はクリントン政権時代、商務省で電子商取引にかかわる政策を担当し、一時的にホワイトハウスの担当になったこともある。彼は直接暗号規制に携わったわけではないが、電子商取引という暗号と密接な分野を担当していた。彼は、アメリカにおけるプライバシー団体の影響力というのはあなどりがたいものがあるとしながらも、暗号規制問題においては、それほど重要ではなかったという。ただし、民間企業の影響力は多少あったかもしれないという。ゴア副大統領の支持基盤のひとつはハイテク産業であり、2000年の大統領選挙を考えれば、ハイテク産業の声を無視するわけにはいかなかった。しかし、もっとも重要だったのは、政策の有効性が失われているという判断だったという。名目だけ続けていても意味はなく、実際に機能しない規制はやめるべきだという判断があったのだという。

もうひとりには、ジェームズ・ルイスである。彼は商務省の輸出管理局で、まさに暗号規制を担当していた。彼は、民間企業の影響力については、多少はあったと認める。しかし、プライバシー団体、インターネット・コミュニティの影響力については、ほとんどなかったという。彼らはワシントン政治がどう動くかをまだよく理解しておらず、洗練された影響力の行使の仕方を身につけていなかったというのである。無論、インターネット・コミュニティにいる人たちに聞けば、彼らは「100%影響力があった」と主張するだろうとはいうものの、実際の政策決定の理由は別のところにあったという。

その理由とは何だったのだろうか。アメリカの安全保障政策を最終的に決定するのは、ホワイトハウスのスタッフと関係閣僚から構成されるNSC(国家安全保障会議)である。暗号の規制緩和を決定したのは、NSCの下に設置されていた次官委員会(Deputy Committee)だったという。ここにはホワイトハウスの担当者のほか、国防総省や国務省の次官クラスが参加しており、暗号問題に関連する商務省のメンバーも加わった。この委員会で暗号にかかわる政策が練られ、その後、NSC、副大統領、大統領へと上げられていくことになる。

この委員会での結論は、「安全なネットワークを持つことは、アメリカの利益になる」というものだったとルイスはいう。これからの時代はサイバー・セキュリティに対する懸念が増大していく。そうした現実を考えたとき、政府、民間企業、個人のそれぞれが強力な暗号を使うことによって、分散的にセキュリティの向上を図ることが重要だと委員会は考え、テロ支援国家などへの輸出規制は続けるものの、それ以外は緩和すべきだという結論に達したのである。

ルイスは、今後インターネット・コミュニティは政治的に洗練されてくるにしても、今のところはそれほど影響力を持っていないという。政権がもっとも影響を受けるのは議会と議員からの圧力で、インターネット・コミュニティの代表が政府にロビーイングにいつて何かを訴えてもそれほど影響力はないが、議員が会いに行けば大きな影響力があるという。

つまり、インターネット・コミュニティは、ワシントン政治のルールに従って伝統的なロビーイングをしなくてはならないということである。一番効率的なのは、有権者による議会への圧力である。議会の公聴会は、企業や諸団体が議会に意見をインプットするまたとないチャンスである。

インターネット・コミュニティが政治勢力として台頭するには、今のところこうした伝統的なやり方に従うしかない。1996年にインターネット・コミュニティが大反対した通信品位法が議会であっさり成立したのも、当時のインターネット・コミュニティがワシントン政治を理解していなかったからだといえよう。その後裁判により通信品位法は違憲との判決を受けたが、議会で止めることができたなら、裁判にエネルギーを費やす必要はなかった。

インターネット・コミュニティが政治化することによって、現実政治における影響力を拡大させることができるかどうか、あるいは全く別の方法で政治を変えていくことができるのかが、今後問われることになるだろう。

インターネット・コミュニティは暗号戦争に勝利したと

考えている。一方、政府は戦う必要がなくなったから戦うのをやめたのだという。立場によって結論は異なるが、われわれが暗号を使う自由を手に入れたことには変わらない。

*1 Phil Karn, "The Applied Cryptography Case: Only Americans Can Type!" <<http://people.qualcomm.com/karn/export/>> (Access: April 28, 2002).

*2 同上。

*3 "Encryption: Hearing before the Committee on Commerce, Science, and Transportation, United States Senate, One Hundred Fifth Congress, First Session, March 19, 1997," Washington: U.S. Government Printing Office, 1998.

*4 同上。

*5 "Encryption Security in a High Tech Era: Hearing before the Subcommittee on International Economic Policy and Trade of the Committee on International Relations House of Representatives, One Hundred Sixth Congress, First Session, May 18, 1999," Washington: U.S. Government Printing Office, 2000.

*6 Edward Gillespie, "The United States Needs a Clear and Realistic Encryption Policy," <<http://www.house.gov/judiciary/106-29.htm>> (Access: May 3, 2002).

「智場」記事一覧