

暗号規制の行方

ソフトウェア化する暗号技術

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)

謎の宮殿

ワシントンD.C.から北へ、ボルチモア・ワシントン・パークウェイを30分ほど走ったところに、『地球の歩き方』にも出ていない博物館がある。その名を「ナショナル・クリプトロジック・ミュージアム」という。直訳すれば「国家暗号学博物館」であろうか。

国家暗号学博物館は、9月11日以降しばらく閉鎖されていたが、12月になって再びオープンした。閉館間際の時間に滑り込んだのだが、ちょうど中からは制服を着た若い男女がぞろぞろと出てきた。士官学校の学生たちだろうか。口々に「すげえ、おもしろいなあ」と言いながら、入り口脇のパンフレットを持ち帰っていた。博物館の中には、スパイ事件に関する展示や暗号機などが置いてあり、現存が唯一確認されているという日本のパープル暗号機や、これも唯一という参謀本部陸軍暗号書四號と書かれた日本の暗号書もある。

この博物館は、実は国家安全保障局(NSA)の管轄である。NSAといえば泣く子も黙るGメンである。映画『メン・イン・ブラック(MIB)』に出てくる黒服の男たちは、NSAをモデルにしているといわれる。同じく映画『エネミー・オブ・アメリカ(原題はEnemy of the State)』(どちらの映画にもなぜかウィル・スミスが出演している)では、NSAが見事に悪役にされている。連邦捜査局(FBI)や中央情報局(CIA)は割と一般に広く知られているが、NSAはさらに高度な情報活動に携わっているとされ、あまり表に出てこない。FBIやCIAの長官の記者会見がテレビで流されることはあっても、NSAの人間が記者会見したことはないのではないだろうか。NSAは1952年に設立されたが、当初は存在そのものが秘

密にされ、NSAとは「No Such Agency(そんな組織は存在しない)」の略だと冗談に言われたほどである。

NSAについて書かれた本がいくつか出ているが、なかでもJames Bamfordの『謎の宮殿(The Puzzle Palace)』は、今でもこの分野の研究者にはよく読まれている^{*1}。同じ著者が最近出した『秘密の組織(Body of Secrets)』もベスト・セラーの棚に並んでいる^{*2}。表立って議論されることのないNSAだが、ワシントンアンに関心はひそかに高く、謎に満ちた政府機関である。

暗号をめぐる戦い

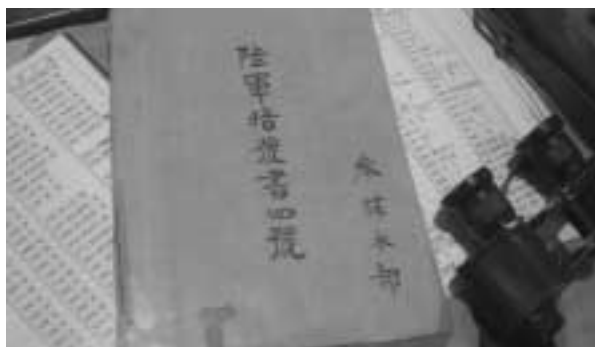
インターネットにおいてますます使われるようになっていく暗号と、この博物館の大半を占めている展示品とは大きく異なる。博物館の展示品の多くは、ハードウェアに依存した暗号である。第二次世界大戦中に使われたドイツのエニグマ暗号機、日本のパープル暗号機、アメリカのシガバ暗号機などは、ちょうどスーパーのレジのような大きさの機械である。それに対して、ソフトウェアとしての暗号はCD-ROMに簡単に収まり、インターネットでもどンドンやり取りされ、複製されている。

しかし、本質的に共通することは、暗号を制するものが勝利を収める、ということかもしれない。

1921～22年のワシントン会議において、英米は日本の海軍力を抑えるために、保有主力艦の総トン数比率を英・米5、日3、仏・伊1.75と定めた。しかし、その交渉過程において、日本側交渉団と東京の間の暗号通信は英米側に解読されていた。その結果、英米側は日本側がどこまで譲れるかをあらかじめ知っており、交渉を有利に進めることが



国立暗号学博物館



日本軍の暗号書



第二次世界大戦中に日本軍が使っていたパープル暗号機



第二次世界大戦中にドイツ軍が使っていたエニグマ暗号機

できた。1943年に山本五十六海軍大将がブーゲンビル島上空で撃墜された事件も、日本海軍の暗号がすでに解読されていたために可能となったのは有名な話だ。

ドイツが使っていたエニグマ(「謎」という意味)は、仕掛けを満載した暗号機である。あまりにも複雑なために、これは破られないとドイツは考え、この暗号機に依存した。しかし、ドイツの脅威にさらされたポーランドが、この暗号の解読のきっかけを作った。ポーランドはドイツとロシアの間に位置するため、ドイツとロシアが開戦することになればポーランドは戦場となり、どちらかに占領される可能性があった。ポーランドはどうしてもエニグマを解読しなくてはならなかったのだ。

エニグマが作り出す暗号は、同じ暗号機が手元になければ解読不能と考えられており、イギリスもアメリカもエニグマの解読にはお手上げ状態だった。しかし、そこにポーランドから解読の手がかりが持ち込まれ、驚嘆した英米は一気に暗号解読

へと突き進み、エニグマが作り出す可能性がある暗号の解読の鍵をすべて試すという方法で、成果を挙げるようになった。

こうした試みが成功した要因の一つには、ドイツ軍人の生真面目さもあった。というのは、各地のドイツ軍の前線基地は、本国に対して定時に報告を行う習慣があった。その報告には、たいてい「～から、～へ」という文字が含まれているはずであり、メッセージが短い場合には「異常なし」と書かれていることが多い。エニグマで暗号化されると、同じ「異常なし」という言葉も毎回全く違った言葉に置き換えられる。したがって、それを解読するのは難しいのだが、それでも手がかりになった。

日本のパープル暗号も同様のやり方で解読された。日本の暗号文の元になる文章はカタカナで書かれており、アルファベットより文字数が増えるため、日本の暗号解読はドイツの暗号解読より面倒ではあったが、結局は成功した。大島浩駐独大使の東京宛暗号文は英米に解読されていた。大



第二次世界大戦中にアメリカ軍が使っていたシガバ暗号機



NSAの初期のコンピュータRISSMAN

島は優秀な外交官であり、ドイツのヒトラーに首尾よく接近し、高度な機密情報に接することができた。彼はヒトラーから得た情報を東京へ送ったのだが、それが英米の手に渡り、戦局を左右することになったのである。

通常の歴史の教科書には、暗号解読が戦争において重要な役割を果たしたということは、ほとんど記述されていないのではないだろうか。しかし、暗号に携わった者たちから見ると、戦局はすべて暗号解読に左右されていたということになる。アメリカがイギリスから独立する際、事実上の決戦となった1781年のヨークタウンの戦いでも、トーマス・ジェファーソンらがイギリス軍の暗号解読に成功し、それをジョージ・ワシントン将軍に伝えたことで、勝利へとつながったそうである。

デジタル暗号の時代

現在のソフトウェア暗号発明の前史ともいえるのが、音声通話のデジタル暗号化である。これについて暗号学博物館で配布されているパンフレットを基に概略を追ってみよう³。第二次世界大戦前、英米両国の高官は、大西洋をまたぐ無線通信に、「A-3」と呼ばれる秘密音声通信システムを使っていた。しかし、これは脆弱なシステムで、ドイツはリアルタイムで解読に成功していることがわかった。

そこで1939年ごろ、ベル電話研究所が「ヴォイス・コーダー（音声暗号化装置）」、略して「ヴォコーダー（vocoder）」というシステムを開発した。1942年にアメリカ軍はこれを採用することにし、SIGSALYと呼ばれるようになった。SIGSALYとは何かの略

ではなく、一種の合言葉として使われた。SIGSALYは、1943年7月にロンドンとワシントンのペンタゴンとの間で最初に導入され、1946年まで使われた。

驚くべきことは、1942年にシステムは開発され、その年に特許が出願されたが、実に1976年までその特許は公開されなかったということだ。これはアメリカ特有のサブマリン特許の一例である。サブマリン特許とは、アメリカ特有の特許制度で、(1)特許が成立するまで出願内容が公開されず(早期公開制度の欠如)かつ(2)特許成立日を特許権起算日とする(権利期間のシーリングの欠如)先のである⁴。

SIGSALYの運用には部屋いっぱいの機材と熟練した要員が必要で、大変なコストがかかるものだったが、現代の暗号は、よりコンピュータの能力に依存するものになりつつある。

NSAがコンピュータを使い始めたのは、コンピュータの歴史とともにあるといい。国家暗号学博物館には「第二次世界大戦によってNSAは、自分の仕事に精を出すのにコンピュータが価値あることがわかった。NSAは発足時からコンピュータの開発と利用において世界のリーダーであると書かれたプレートが飾られている。

NSAにとって最初の本格的なコンピュータは、1969年に導入されたTELLMANだという。これはパンチカードと呼ばれる穴の空いたカードを差し込んで入力するもので、当時としては膨大ともいえる512キロバイトのメモリと、6メガバイトのハード・ディスク・ドライブを備えていた(後には48メガバイトに



コードが張り巡らされたクレイ社の初期のスーパー・コンピュータ



2000年まで使われていたZIEGLERの集積回路

拡張)

1970年代末から使われたのが、RISSMANというコンピュータで、インテル社の8086というプロセッサを三つ搭載していた。これは16メガバイトのメモリと300メガバイトのディスク・スペースを持っていた。しかし、現代のパソコンと比べると巨大なもので、部屋の壁一面を覆う大きさだったようだ。

1980年代半ばになると、いわゆるスーパー・コンピュータの時代がやってくる。クレイ社のXMP-94というコンピュータは、1983年から1993年までNSAで使われた。このコンピュータの中にはびっしりとコードが張り巡らされており、その総延長は47マイルにもなるらしい。

しかし、そうした長いコードは、半導体技術の進歩によって半導体集積回路の中に組み込まれ、格段にスピードがアップした。1993年8月から2000年4月まで使われていたというクレイ社製の愛称ZIEGLER(YMP M90)は、巨大な回路を組み込んでいる。メモリのサイズはなんと32ギガ(3万2,000メガ)バイトで、142ギガバイトのディスク・スペースを持っており、8個の並列プロセッサを内蔵していた。われわれが今使っているパソコンで、32ギガのメモリを搭載したマシンなど、そう簡単にお目にかかれるものではない。しかし、ZIEGLERはすでに博物館の展示品になってしまっている。NSAは現在どれくらいのコンピュータを使っているのだろう。NSAは時代の超最先端技術を使い、暗号処理を行ってきた。世の中で普及しているコンピュータより確実に性能が上でなければ意味がない。

しかし、それでも暗号解読にかかる処理はまず



スーパー・コンピュータZIEGLERの巨体

まず時間がかかるようになっている。思い切って簡略化していえば、現代のソフトウェア暗号の解読とは、膨大な桁の数字の素因数分解とっていいそうだ。素数とは、2、3、5、7、11など1より大きい整数のうち、1とそれ自身以外に約数を持たないものである。素数は無限に多く存在する。そして、その分布は不規則になっている。素数と素数の掛け算というのは比較的簡単だ。たとえば、131という素数と47という素数を掛け合わせれば、6157という数字が簡単に出てくる。しかし、6157という数字だけを与えられて、これを素因数分解せよ、と言われたら、2、3、5、7、11...というように順次試して行って、47で割り切れるまで、続けていかななくてはならない。与えられる素数が膨大な桁数になってしまえば、これを素因数分解するには膨大な時間がかかる。その結果、「この暗号を解読するには、現在のコンピュータの性能で数十年かかる」といった言い方で、暗号の強度が説明されることになる。実際にはもっと複雑なアルゴリズム(計算の手続き形式)に基づいて、計算が行われることになる。

暗号の汎用化

ソフトウェア化された暗号技術がもたらした最大の変化は、利用者の拡大である。いやむしろ、それと知らずに暗号を使っている人の増加である。オンライン・ショッピングとはつまり、暗号を使うことにほかならない。インターネットでクレジットカード番号を送信するのは危ないとよくいわれる。確かに、電子メールで暗号化せずに送るのは危険だ。ISPはもちろん、相手先に届くまでに経由するコンピュータで、その情報はいつでも簡単に読むことができるだろう（読むことができるからといって即、犯罪につながるわけではない）。

現在、普通に行われているオンライン・ショッピングやオンライン・バンキングでは、暗号が使われている。一般的なウェブ・ページは「http://」から始まるが、暗号化されているウェブ・ページは「https://」となっていたりする（「Secure」の意味の「s」が入る）。

ここでたいてい使われているのは、RSAセキュリティ社が開発した暗号である^{*5}。たとえば、アメリカの大手銀行のオンライン・バンキングのページでは、RSAセキュリティ社の「RC4」という暗号を使っている。この暗号は金融取引によく使われるもののようだ^{*6}。ブラウザの「ページ情報」というメニューで確かめてみると、「表示中のページは、インターネット上に送信される前に暗号化されました。ネットワーク上で移動する情報を暗号化することによって、非認可のユーザはそれらの情報を表示しにくくなります。そのため、ネットワーク内で誰かがこのページを読んだ可能性はほとんどありません」と表示される。この暗号を使うためには、ユーザのブラウザにも対応するソフトウェアが組み込まれていなくてはならないが、ネットスケープ社のナビゲータにも、マイクロソフト社のインターネット・エクスプローラにも、対応するものが最初から組み込まれている。

RSAセキュリティ社は、Ronald Rivest、Adi Shamir、Leonard Adlemanという3人の暗号研究者の名前をとって設立された会社である。マサチューセッツ州に本部を置き、2001年の収益は2億

8,270万ドル（約367億円）である。コンピュータ・ソフトウェアで断然トップのマイクロソフトが252億9,600万ドル、第二位のオラクルが108億6,000万ドルだから、RSAの規模はそれほど大きくない。しかし、その市場支配力は、会社の規模以上に大きかった。RSA社が握る公開鍵暗号の特許が事実上の標準となり、インターネットのあらゆるところで使われていたからだ。ところが、その特許は2000年9月20日に期限切れを迎えた。RSAセキュリティ社はその特許をいち早く、9月6日にはパブリック・ドメインにし、自由に使えるようにした。

アメリカの暗号規制

特許は自由になったものの、アメリカ政府ははまだ暗号に関する規制を残している。強力な暗号を犯罪者やテロリストが使うようになると、アメリカの安全保障が脅かされるというのである。クリントン政権は、暗号に関して二つの規制をとろうとしていた。ひとつは、国内利用におけるキー・エスクロー（鍵供託）システムであり、もうひとつは輸出規制である。

キー・エスクロー・システムとは、暗号化されたメッセージの復号に必要な鍵（鍵といってもデジタル化された情報にすぎない）を第三者機関に預け（供託）、犯罪捜査など必要なときに、その鍵を捜査当局が使えるようにするというものである。しかし、この政策は民間からの強い反対にあった。プライバシー団体は、政府が人々の通信を読むことができるようになるのはプライバシーの侵害だと反発した。プライバシー関連製品を作っている業界も、これでは売れなくなると反対した。これに関連して大統領令が出されるなどしたが、結局、キー・エスクロー・システムは有効に機能しないまま、クリントン政権は任期を終えた。

一方、輸出規制については、強度の高い暗号に関する輸出許可制がまだ続けられているが、一般的にインターネットで使われる64ビット以下の暗号については1999年に規制が撤廃され、自由に輸出できるようになった。64ビット以上の暗号製品についても、テロリストを匿っていると疑われる7

カ国以外には許可されるようになっている^{*7}。

ここで「ビット」とは暗号鍵の長さを表しており、数字が大きくなるほど暗号は解読されにくくなる。現状のコンピュータの性能では、128ビット程度ならほぼ安全な暗号強度といわれており、逆に勘ぐれば、128ビットの暗号ならばNSAは破ろうと思えば破れるということなのだろう。一般的な利用上の安全性と、国家安全保障上の安全性とのバランスがとれたところが、今のところ128ビットなのかもしれない。しかし、コンピュータの性能が向上していけば、いずれこの数字は大きくならざるをえないだろう。

128ビットの暗号が輸出許可になる前は、アメリカ国内では128ビットの暗号を搭載したウェブ・ブラウザを使うことができたが、日本のユーザは64ビットまでのものしか使えなかった。当時のネットスケープ社のサイトでは、アメリカ国内居住者用のダウンロード・サイトとそれ以外の国々の居住者用のサイトが別々にしてあるという事態になっていた。

アルカイダのコンピュータ解読

しかし、このアメリカの輸出規制が現実に役に立った事件が起きた。オサマ・ビンラディンのテロ・ネットワーク、アルカイダが使っていたコンピュータのハード・ディスクをアメリカの新聞記者が入手し、それを解読することに成功したのである。

『ウォール・ストリート・ジャーナル』紙の Alan Cullison 記者のノート・コンピュータは、北部同盟のトラックに乗っていたときひっくり返って壊れてしまった。そこで、アフガニスタンの首都、カブールで交換部品を探した。すると、アルカイダが放棄した家から見つかったというコンピュータが出てきた。Cullison 記者は、もうひとつあるという売人から、二つあわせて1,100ドルで購入した。

中に入っていたOSはマイクロソフトのウィンドウズ2000で、暗号ソフトウェアで内容が保護されていた。つまり、そのままでは内容を読むことはできなかったのである。しかし、その暗号の強度は40ビットでしかなかった。アメリカ政府の輸出規制により、アフガニスタンには強い暗号を輸出できな

かったのである。記者たちはその暗号解読に専門家たちとともに取り組み、成功したのである。

そこから出てきた内容は、9月11日のテロ事件に直接関連するものはなかったものの、アルカイダの活動についてさまざまな情報を提供した。あるファイルには170人もアルカイダのメンバーの名前が書かれていた。さらには、Abdul Ra'uff なる人物の行動記録が書かれていた。この人物の行動は、靴に仕掛けた爆弾を爆発させようとして捕まった Richard Reid、いわゆる「シュー・ボマー」の行動と酷似していた。Ra'uff は、Reid の別名を使って世界を渡り歩き、アルカイダの活動をしていたのではないかと推測されるのである。

イギリスの『インディペンデント』紙は、この一件について、アメリカ最大の企業のひとつが作った製品を、アメリカに対するテロ計画を保護するためにテロリストたちが使っていたというのは皮肉だと指摘し、暗号に関する、より厳しい規制が当然の結果として行われるだろうと述べている^{*8}。

暗号政策は必要か

日本では、暗号はどうしてもネガティブなイメージでとらえられているが、日本ほどではないにしろ、アメリカでも状況は同じようだ。アメリカ人の暗号研究者に聞いてみると、「暗号に関する研究をしている」というだけで、うさんくさい目で見られることがあるそうだ。

しかし、暗号はもはや戦争の道具であるだけでなく、プライバシーを守るための道具、商取引のための道具にもなっている。プライバシーやセキュリティに関する懸念と、公共安全や秩序との間のバランスをどこでとるかが政治的な課題である。暗号技術の普及と利用を政府の規制に閉じ込めておくのではなく、民間の手に委ねておくこともひとつの選択であろう。その選択の前に、本当にそこで適切なバランスがとれているかを議論する必要はあるだろう。日本の近代史を見る限りは、日本の情報戦略は甘かったといわれても仕方がない。

アメリカでも暗号をめぐる問題は人気のある話題ではないが、少なからぬ議論が行われているこ

とも確かだ。議会にはここ数年、必ず何本かの暗号関連法案が提出されるようになっていく。4月にはサンフランシスコでCFPという有名な会議が開かれるので(<http://www.cfp2002.com/>)、本連載の6月号ではその様子を交えながら、インターネット・コミュニティの暗号規制に対する反応を紹介することにしたい。来月(5月)号では、「人類の暗号」ともいえる遺伝子解読をめぐる生物学とITの協働関係について見ていくことにする。

- *1 James Bamford, *The Puzzle Palace: A Report on America's Most Secret Agency*, Reprint Edition, New York, Viking Press, 1983.
- *2 James Bamford, *Body of Secrets: Anatomy of the Ultra-Secret National Security Agency from the Cold War Through the Dawn of a New Century*, New York, Doubleday, 2001.
- *3 J. V. Boone and R. R. Peterson, *The Start of the Digital Revolution: SIGSALY Secure Digital Voice Communications in World War II*, Fort George G. Meade, Maryland, Center for Cryptologic History, National Security Agency, July 2000.
- *4 特許庁「サブマリン特許と早期公開制度」<<http://www.jpo.go.jp/tousi/pdf/sanko12.pdf>>(2002年3月5日アクセス)
- *5 RSAセキュリティ社の技術は、1976年にWhitfield DiffieとMartin Hellmanが開発した公開鍵暗号方式を実用化したものである。公開鍵暗号は、それ以前の秘密鍵(共通鍵)暗号からの画期的な技術革新であり、これなくしてはインターネットでの取引は困難である。
- *6 RSA Security, "What is RC4?" <<http://www.rsasecurity.com/rsalabs/faq/3-6-3.html>> (Access: March 6, 2002).
- *7 Declan McCullagh(酒井成美、合原亮一訳)「クリントン政権、暗号製品の輸出規制を緩和」HOTWIRED JAPAN <<http://www.hotwired.co.jp/news/news/Business/story/3072.html>>(2002年3月7日アクセス)
- *8 Alan Cullison and Andrew Higgins, "Account of Spy Trip on Kabul PC Matches Travels of Richard Reid," *The Wall Street Journal*, January 16, 2002. David Osborne, "Has an Old Computer Revealed that Reid Toured World Searching out New Targets for al-Qa'ida?" *The Independent*, January 17, 2002. Felicity Barringer, "Why Reporters' Discovery was Shared with Officials," *The New York Times*, January 21, 2002.

「智場」記事一覧