

# デジタル時代の合法的通信傍受

## < アメリカ編 >

土屋大洋

( GLOCOM主任研究員 / メリーランド大学国際開発・紛争管理センター訪問研究員 )

パールハーバー以来？

9月11日のテロの直後、アメリカのテレビに出てくるコメンテーターたちは、「パールハーバー以来の出来事だ」と繰り返し言った。書店ではパールハーバーに関する本が特集コーナーに並んだ。こうしたパールハーバーとの比較に、長年ワシントンに住む日本人は二つの点から異を唱える。第一に、パールハーバーがアメリカ本土から離れたハワイにあるのに対し、今回のテロはワシントンD.C.とニューヨークという米国の心臓部がやられたという点である。これは1812年戦争(米英戦争)の最中、1814年にイギリス軍がホワイトハウスを焼き討ちして以来の出来事である。第二に、パールハーバーの攻撃対象があくまで軍事施設であったのに対し、ワールド・トレード・センターは民間施設だったという点である。

しかし、アメリカの諜報活動の大失敗という点では、やはりパールハーバー以来ということが言えるかもしれない。パールハーバー以前からアメリカは日本の暗号通信解読に成功していた。したがって、ルーズベルト大統領は日本のパールハーバー攻撃を事前に察知していながら、アメリカ参戦の世論作りのためにわざとやらせたのではないかと、いづルーズベルトの陰謀説」が根強くある。これに対して神戸大学の吉田一彦名誉教授は、1991年に公開されたアメリカ政府の文書に基づき、「暗号解読が遅れたのは解読要員が不足していたため」だったのではないかと指摘する<sup>\*1</sup>。いくら解読する術を持っていても、日本語でやりとりされる暗号の解読には、それなりの時間と手間がかかる。しかし、当時、日本の暗号の解読に携わっていたのは、たった8人だったというのである。

いずれにせよ、「二度とパールハーバーは許さない」という決意が、それ以後のアメリカに「膨大なスパイ網を張り巡らせ、スパイ機を飛行させ、スパイ衛星を打ち上げ、世界中の通信を傍受して警戒を厳に」させていた<sup>\*2</sup>。その網の目をくぐって大規模な同時多発テロが行われたということからすれば、やはりパールハーバー以来の、アメリカのインテリジェンス(諜報)コミュニティの大失態だったといえるだろう。

アメリカが何も気づいていなかったわけではない。具体的な内容は伴わないものの、「ビンラディンが何かをやりそうだ」ということは広く知られていた。例えば『NEWSWEEK』誌の2001年7月30日号6ページの記事は、「アラビア半島のアメリカ政府の前哨部隊<sup>\*3</sup>と企業は、変節したイスラムのリーダー、オサマ・ビンラディンに共感したテロリストたちの攻撃の可能性があることから、高度な警戒態勢にある」と書いている<sup>\*4</sup>。そのときすでに捕まっていたテロリストの一人は、ロサンゼルス空港を爆破する予定であったことを自供していた。いま思えば「やはり...」という思いが、関係者には強いであろう。断片的な情報を集め、それを意味ある情報へと整理・解釈することが、諜報戦の要といわれる所以である。

### 諜報活動と捜査活動

諜報活動と捜査活動はしばしば混同されるので、ここで整理しておこう。最も違う点は、捜査活動の目的がすでに起きた犯罪を処罰することにあるのに対し、諜報活動の目的は将来の危険に対処することだという点である<sup>\*5</sup>。

「諜報活動 = 非合法」という図式も正確ではない。諜報活動は秘密裏に行われなければ意味が

ないが、そのすべてが非合法的というわけではない。アメリカの法律では、タイトル50の「戦争と国防 (War and National Defense)」のチャプター36が「外国諜報監視 (Foreign Intelligence Surveillance)」になっている。この法律のもとでは、スパイ行為やテロ活動にかかわる外国勢力に対する諜報活動が認められている。つまり、アメリカ国内の外国勢力について、一定の条件のもとで諜報活動を行うことは合法とされているのである。

しかし、アメリカ国外においてアメリカ政府機関が行う諜報活動が、合法であるという保証はない。諜報活動を禁じる法律を持つ国では、そうした活動にかかわった外国人を逮捕するか、国外退去処分にするだろう。

ただし、こうした外国勢力の活動に明白にかかわっているとみなされない限り、アメリカ市民が諜報の対象になることは厳しく禁じられている。この点について、ネオナチ勢力を国内に抱えるドイツや、IRA (Irish Republican Army: アイルランド共和国軍) によるテロ活動を抱えるイギリスでは、アメリカより制限が緩められている。条件をクリアすれば、ドイツ市民、イギリス市民に対する諜報活動も認められている。

そして、何か事件が起きた後に行われるのが捜査活動である。言論の自由が保障されている国では、明白な脅威と認定されない限り、たとえ「テロ実行」という言葉を使ったとしても逮捕されることはない (そうでなければ小説は書けなくなる)。少なくともテロ未遂事件を起こすか、明白な計画の証拠がない限り、捜査対象とはならない。

しかし、正当な手続きを踏んで行われなければ、捜査活動も非合法になる可能性がある。この場合、裁判においては証拠として採用されなくなることがある。

一般的にいわれる「盗聴」とは、広くとらえれば通信の第三者取得全体のことと考えられるが、法執行機関の立場からすれば、彼らのやっていることは盗聴ではなく合法的な通信傍受であって、社会の秩序維持のために必要なことである。それに対して、非合法的な通信傍受こそが盗聴であり、両者は厳

密に区別されるべきだということになるだろう。

問題は、そうした区別が現実にはあいまいになっており、グレーゾーンが大きいということであろう。ケネディ元大統領やニクソン元大統領が、政治目的のために疑わしい通信傍受を行っていたことはよく知られている。CIA (中央情報局) が諸外国で行っている活動の一部は、それらの国々では非合法的なものになっている。NSA (国家安全保障局) が作り上げていると噂される「エッシュロン」という諜報ネットワークも、本来は安全保障上重要な合法的諜報活動とみなされるものだが、それが一般市民の通信にも広くかかわってくるものであるために、非合法盗聴ネットワークであるとの強い批判を受けている。

#### 通信傍受の手段

通信傍受を手段から考えてみると、交信分析、通信 (内容) 傍受、暗号解読という分類が考えられる。

交信分析とは、誰が誰にメッセージを送ったのかという事実を分析することである。伝えたいメッセージがあるからこそ通信は行われるのであり、仮にその内容がわからなくても、通信が行われたという事実が重要な示唆を与える場合がある。テロリストとして疑われている人たちの間で頻りにメッセージが交わされるようになれば、何かしら近日中に行われるテロがあると想定することができるだろう。

狭義の通信傍受とは、当事者に知られることなく通信の内容を聞いたり、読んだりすることである。古くは手紙の開封であったり、タッピングと呼ばれる電話線への接続であったりした。最近では、電子メールや携帯電話の傍受など、電子的な通信傍受の役割が増している。

しかし、通信内容の傍受では不十分な場合もある。手紙や電子メールが暗号化されていることがあるからだ。メッセージの内容が全く意味不明のこともあるが、一見して普通の文章なのに別の意味が隠されている場合もある。暗号化されたメッセージがやり取りされている場合、解読できなくても交

信分析で十分な成果をあげられることもあるだろう。しかし、暗号の解読が必要な場合もある。

近現代史において、最も熟達した暗号解読を行ってきたのはイギリスであろう。第一次世界大戦、第二次世界大戦、そしてそれ以後もイギリスは一貫して世界の通信の傍受を行っており、暗号解読も行ってきた。両大戦中におけるドイツとの戦いでは、いずれも最終的に暗号解読に成功した。特に第二次世界大戦では解読不可能といわれた「エニグマ」暗号の解読に成功し、少なくとも戦争の早期終結に貢献したと評価されている。しかし、イギリスの暗号解読は大っぴらに行われていたわけではなく、暗号解読の事実を同盟国にも隠し、戦後もしばらくは隠していた。

アメリカの通信傍受は、第一次世界大戦後、スティムソン国務長官の「紳士は他人の手紙を読むべきではない」という言葉によって後退を余儀なくされたが、第二次世界大戦になると、他国の暗号解読に力を入れるだけでなく、自らの暗号通信システムの開発にも邁進することになった。その結果、日本の「パープル」暗号の解読に成功しただけでなく、アメリカの暗号「シガバ」は、大戦中解読されなかった唯一の暗号とされている。

### テロリストの通信

今回のテロ事件の首謀者と目されるオサマ・ビンラディンが、暗号マニアであるということは長らくいわれてきた。彼は暗号つきの衛星携帯電話を使い、アメリカのインテリジェンス・コミュニティはそれを解読しようとしてきた。

テロの後、彼のビデオ・メッセージが公表されたときも、その映像には一種の暗号が秘められており、テレビ局はそれを流すべきではないという意見をアメリカ政府が発表し、テレビ局も独自の判断でそれに従うことになった。ビデオの中でビンラディンがなぜか米軍の迷彩服を着ていることが、いぶかしがられたのである。

サイモン・シンは、ベストセラー『暗号解読』の中で、「暗号をめぐる論争は、世界各地からひっきりなしに流れ込んでくる情報にたえず影響を受けて

いる」と指摘している<sup>\*6</sup>。まさに今回のテロ事件は暗号問題に大きな影響を与えることになった。

テロリストたちは暗号を使って通信を行っており、今後のテロを防ぐためには暗号を規制しなくては行けないという声も、さしたる証拠も出てこないうちに聞かれるようになった。ここでいう暗号とは、PGP(プリティ・グッド・プライバシー)のような、メッセージを意味不明の記号の羅列に変換するソフトウェアを使ったもので、対応する鍵がないとメッセージを復号できないというものである。

ところが、捜査が進むうちに、テロリストたちは暗号通信など行っておらず、公共施設のインターネットを使って、平文のメッセージをやりとりしていたということがわかってきた。ある者はホテルのインターネットを使い、別の者は街角にあるKinko'sや公共図書館のインターネット・サービスを使っていたというのである<sup>\*7</sup>。

実際にどのような内容のメッセージが交わされていたのかは、今のところ公表されていない。利用者のプライバシーに対する配慮もあって、図書館側も情報の提供に慎重な態度をとっている。仮にテロリスト・グループが残したメッセージが見つかったとしても、それがテロに直接結びつくような言説を残しているかどうかは疑わしい。そもそも彼らが英語で電子メールをやり取りしているとは限らない。アラビア語などの言葉を使ったうえに、何らかの秘密の合言葉が使われていて、意味不明の可能性もある。内容がわからなくても、交信分析でビンラディン宛のものが見つければ良いが、そんな可能性はほとんどないだろう。

テロ直後の混乱からやや落ち着いてくると、問題の本質が暗号解読だけにあるのではなく、通信傍受全体にあるとの見方が一般的になってきた。つまり、メッセージが暗号化されていようがまいが、テロリスト・グループがどのような通信を行っていたかが捜査の対象となり、次のテロを防ぐための諜報活動が必要だとの認識が強くなったのである。その結果が、テロから約1ヵ月半で成立したテロ対策法であった。

## テロ対策法の成立

9月11日にテロが起きる前にもたくさんのテロ対策法案が議会に提出されていたが、テロ直後から、よりいっそう多くの法案が提出された。9月19日にはブッシュ大統領と司法省が「対テロリズム動員法 (Mobilization Against Terrorism Act)」と題する法案を作成し、議会に対して22日までの成立を求めた。大統領は直接法案を提出する権限がないため、議会に対する要請という形でアシュクロフト司法長官が原案を発表した。

しかし、この法案は捜査当局の大幅な権限拡大を含むものであったため、EFF (Electronic Frontier Foundation) などのサイバー・リバティ団体が強い反対を示し、議会の中にも懐疑的な声が強かった。対テロリズム動員法は「反テロリズム法 (Anti-Terrorism Act)」に名前を変え、引き続き法案提出が検討されたが、結局そのままの形で提出することは見送られた。

議会は、大統領の要請に応える形で、ホワイトハウスとの協議を重ねながら、超党派の法案をまとめた。その結果、提出されたのが、下院の「H.R.2975パトリオット法 (PATRIOT: Provide Appropriate Tools Required to Intercept and Obstruct Terrorism Act)」と、上院の「S.1510 USA法 (Uniting and Strengthening America Act)」であった。パトリオット法は10月2日に提出され、10日後には下院で可決、USA法は10月4日に提出され、1週間後の11日に上院で可決した。

ところが、二つの法案にはいくつかの違いがあったため、調整が必要になった。その調整を行っているさなか、10月5日にフロリダの男性が肺炎で死亡し、徐々に炭疽菌による新たなテロが問題となりはじめた。そして、15日には上院のダシユル院内総務の事務所にも炭疽菌が入った郵便が届き、炭疽菌問題が急速に深刻になった。議会は審議を一時停止し、議会内にいた人すべてが検査を受けることになった。こうした事態のために法案審議は進まなくなった。

審議が再開されると、上下両院は法案の違いを

調整したうえで、あらためて23日に「H.R.3162 USAパトリオット法」として新たな法案を提出した。この法案は提出の翌日の24日には下院で可決され、さらに翌日の25日には上院でも可決された。議会を通過した法案はブッシュ大統領のもとに送られ、大統領はすぐに署名し、26日に成立した。

法案の概略は以下のようになる<sup>\*8</sup>。

- ・承知のうえでテロリストをかくまうことを犯罪とする。
- ・テロリストと疑われる外国人を、犯罪で告発あるいは国外退去処分を開始する前に、7日間まで拘留する権限を司法長官に与える。
- ・単一の電話だけでなく、外国人テロリスト容疑者が使うすべての電話を傍受可能にする「ローピング傍受」の裁判所命令を連邦当局が取得することを許す。
- ・連邦政府の犯罪捜査機関と諜報機関の捜査員が、大陪審と傍受内容その他の情報を、より容易に共有できるようにする。
- ・マネー・ロンダリングの脅威があると見られる外国や銀行を特定する権限を財務省に与える。
- ・北の国境に配備される国境警備員の数を3倍にする予算と、北の国境沿いにある入国管理事務所の職員を3倍にする予算を承認する。
- ・テロ容疑者の電子メール通信についてインターネット・サービス・プロバイダ (ISP) から記録を求める召喚状取得を法執行機関に認める。
- ・多くのテロ犯罪の処罰を増やすとともに出訴期限法を増やす。
- ・ほとんどの通信傍受・諜報規定を4年で無効にする。

最後の点について、ブッシュ政権は期限を設定する「サンセット方式」に反対し、無期限の法制化を求めていた。しかし、下院の法案は2年を限度としていた。議会での審議の結果、妥協が図られ、4年に収まった。

## インターネット・コミュニティの対応

こうした議会の動きに対して、EFF、CDT (Center for Democracy and Technology)、EPIQ (Electronic

Privacy Information Center といったサイバー・リバティ諸団体は、猛烈ともいえる反対運動を展開した。

それぞれの団体は、メール・マガジン形式の情報提供・啓蒙ニュースレターを発行している。行政府、司法院、立法府で起きているさまざまなネット・ポリティクス関連の話題を取り上げ、情報提供するとともに、購読者がとるべき行動を具体的に記述している。

テロ発生後から10月26日のテロ対策法成立までの間に、CDTは「CDT POLICY POST」というニュースレターを4回出した(うち1回は法案に関する記述なし)。EPICは「EPIC Alert」というニュースレターを5回出している(うち2回は法案に関する直接の記述なし)。最も活発に法案を追いかけたのはEFFで、「EFFector」というニュースレターを10回出し、そのすべてで法案に触れている。

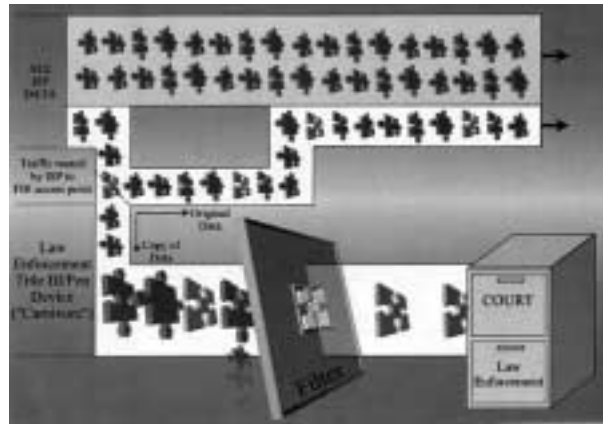
EFFの分析によれば、新法の問題点は以下の三つである。第一に、監視の増大はチェック・アンド・バランスの低下につながる。第二に、テロだけに焦点を当てているわけではなく、広く他の捜査にも適用される可能性があること。第三に、アメリカの諜報機関の権限拡大が、アメリカ市民に対するスパイ活動につながる。こと、である。

結局のところ、サイバー・リバティ諸団体の反対運動は、法案の成立そのものを阻止することはできなかった。しかし、すぐにもこの法案の違憲訴訟が起こされるのではないかと見られている。

## カーニボー

今回の通信傍受権限拡大の中で幾度となく紹介されたのが、FBI(連邦捜査局)の電子メール傍受システムである「カーニボー」である。FBIはテレビ・ドラマ『Xファイル』で有名になったが、アメリカ全体に及ぶ犯罪、州をまたぐ犯罪の捜査を行っている。

カーニボーの存在は、2000年7月にメディアによって報じられた。FBIはある程度の情報をウェブで公開しているが<sup>9</sup>、その詳細ははっきりせず、さまざまな憶測とともに批判がなされた。カーニボー



カーニボーのシステム

は、FBIの説明によれば、法的に取得が認められた通信データの packets を、ISPの通信トラフィックの中からフィルターを使って抜き出すというものである(図参照)。

行動派で知られるEPICは、すぐにFBIに対して情報公開請求を行ったが、FBIは法定期限までに情報を公開しなかった。EPICは連邦地方裁判所に訴えを起こし、さらに情報公開を求めた。2001年1月、ようやくFBIは1,756ページの関連文書のうち、1,502ページを公開した。

すでにテロ直後から、複数のISPがカーニボーの設置に関してFBIに協力を始めていたといわれるが<sup>10</sup>、こうした動きが新法によって拡大することを、サイバー・リバティ団体は強く懸念している。

## 自由を奪われたアメリカ

テロはさまざまな形でアメリカに影響を与えているが、つまるところ、アメリカ人が最も我慢ならないのは、多くの人の命が奪われたことと同時に、アメリカン・ウェイ・オブ・ライフの根幹的な価値である自由が奪われたということなのではないだろうか。

空港の安全強化などは、ようやく日本並みになったようにしか見えない。例えば、日本は国内線でも搭乗者以外が登場ゲート前まで行くことはできなかったが、アメリカではそれがテロ以前は可能だった。日本では国際線に乗る場合、3時間前までに空港に行くようにと旅行代理店に言われるが、テロ以前のアメリカでは1時間ぐらいと考えている



テロ対策に躍起になっているFBI本部



FBIの脇で売られるビンラディンのTシャツ

人が多かった。

こうした不便さの増大が、アメリカ人には不満の種になっているようだ。匿名での通信が特徴だったインターネットにも、監視の目がいっそう厳しくなっている。インターネットにおける自由というものを、アメリカは考え直しは始めている。

\*1 吉田一彦『暗号戦争』小学館、1998年、72ページ。

\*2 吉田、前掲書、130ページ。

\*3 前哨部隊とは、休止する部隊が、敵情探索、奇襲防止などのため、その前面に配置する部隊のこと。

\*4 Mark Hosenball, "The Secret Reasons for the Alert," NEWSWEEK, July 30, 2001, p. 6.

\*5 Philip B. Heymann, *Terrorism and America: A Commonsense Strategy for a Democratic Society*, Cambridge: The MIT Press, 1998, p. 129.

\*6 詳しくは、サイモン・シン(青木薫訳)『暗号解読 ロゼッタストーンから量子暗号まで』新潮社、2001年、57ページを参照。

\*7 シン、前掲書、413ページ。

\*8 Kevin Johnson, "Hijackers' e-mails sifted for clues Computer messages were sent uncoded," USA TODAY, October 1, 2001.

Ariana Eunjung Cha and Jonathan Krim, "Terrorists' Online Methods Elusive: U.S. Agencies Seek Experts' Help in Tracing Encrypted Messages," Washington Post, September 19, 2001.

\*9 Dave Boyer, "Senate OKs Bill for Nation's War on Terrorism: Feingold Alone on 98-1 Vote," Washington Times, October 26, 2001, A1 and A14.

\*10 FBIのウェブ・ページ<<http://www.fbi.gov/hq/lab/carnivore/carnivore.htm>>を参照。

\*10 Declan McCullagh「米国同時テロ:米政府、カーニボアによるネット監視を強化か」<<http://www.hotwired.co.jp/news/news/culture/story/20010913202.html>>(2001年9月12日)