政府機関によるインターネット傍受の課題

土　屋　大　洋　　慶應義塾大学大学院政策・メディア研究科准教授

1 はじめに

米国の「テロとの戦い[1]」は、通信傍受への依存を高めている。テロリストが拘束されるきっかけは、彼らの会話を米国や関係国のインテリジェンス機関が傍受したからだと報じられることが多い[2]。そして、従来からの電話の通信傍受だけではなく、インターネットや携帯電話といったデジタル通信の傍受も広く行われるようになってきている。

そうした中、2005 年 12 月末にニューヨーク・タイムズ紙のスクープ記事によって明らかになったのが、米国のジョージ・W・ブッシュ（George W. Bush）政権による大規模な令状無し通信傍受であった。米国法の下では、インテリジェンスに関わる通信傍受に際して裁判所からの令状取得が義務づけられている。しかし、ブッシュ大統領は密かに大統領令を出し、令状無しで通信傍受をできるようにした。

さらに問題になったのは、対象者が外国勢力に限定されているはずの外国インテリジェンス監視法（FISA）の枠組みを使って、米国内で通信傍受が行われ、多くの米国市民および永住権保持者が傍受の対象となった点である。1970 年代のニクソン政権下におけるウォーターゲート事件をきっかけに、米国内でのインテリジェンス活動には大きな歯止めがかけられてきたが、それが密かに崩されていたことに批判が高まった。それに対し、ブッシュ政権側は、テロとの戦いにおいては大規模な通信傍受は不可欠の措置であったと主張し[3]、2008 年夏には外国インテリジェンス監視法の改正を議会で可決させた。

本稿はなぜブッシュ政権が大規模な令状無し通信傍受を行うようになったのかという問題について、技術的および政治的な背景を探ることを目的としている。局地的な現象であったテロがグローバル化する一方で、インターネットをはじめとするデジタル通信技術もまたグローバル化している。この二つのグローバル化が密接に絡んだ事例としてこの問題を考えることができるだろう。

---

[1] 2009 年 3 月、オバマ政権は、ブッシュ政権が使ってきた「テロとの戦い」という言葉を使わないことにすると発表したが、本稿ではブッシュ政権下の問題について焦点を絞っているため、そのまま用いる。

[2] 2003 年 3 月 1 日、国際テロネットワークであるアルカイダのナンバー3 と呼ばれたハリド・シェイク・ムハンマド（Khalid Shaikh Mohammed）が拘束されたが、それにはパキスタンのインテリジェンス機関が集めた情報とともに米国の国家安全保障局（NSA）の通信傍受が貢献したとされている。モハメドの拘束については、例えば、以下を参照。Oliver Burkeman, "How Mobile Phones and an £18m Bribe Trapped 9/11 Mastermind," guardian.com <http://www.guardian.co.uk/world/2003/mar/11/alqaida.terrorism> March 11, 2003. NSA についての研究としては、ジェームズ・バンフォード（James Bamford）がよく知られている。James Bamford, *The Puzzle Palace: A Report on America's Most Secret Agency*, Harmondsworth: Boston: Houghton Mifflin, 1983. 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. James Bamford, *The Shadow Factory: The Ultra-Secret NSA from 9/11 to the Eavesdropping on America*, New York: Doubleday, 2008. また、法律家の視点としては、例えば、リチャード・ポズナー（Richard Posner）を参照。Richard A. Posner, *Uncertain Shield: the U.S. Intelligence System in the Throes of Reform*, Lanham, Md.: Rowman & Littlefield, 2006. また、歴史家の視点としては、アーサー・シュレジンガー（Arthur Schlesinger）を参照。アーサー・シュレジンガーJr.（藤田文子、藤田博司訳）『アメリカ大統領と戦争』岩波書店、2005 年。また近年の通信傍受の実態を明らかにしたものとして、以下を参照。パトリック・ラーデン・キーフ（冷泉彰彦訳）『チャター―全世界盗聴網が監視するテロと日常―』日本放送出版協会、2005 年。

[3] ブッシュ政権側を代表する見解としては、ホワイトハウスの法律顧問を務めたジョン・ユー（John Yoo）の著書を参照。John Yoo, *War by Other Means: An Insider's Account of the War on Terror,* New York: Atlantic Monthly Press, 2006.

2 二つの情報コミュニティの衝突

2-1 ギークと技術フロンティア

ジョン・カッツ（Jon Katz）が『GEEKS』の中で描写したように、「コンピュータ・ギーク（geek)」たちはわれわれの社会になくてはならない存在になっており、かつてはネガティブな意味を持っていたギークという言葉も徐々にポジティブな意味合いを持つようになってきている[4]。ギークとはもともと「奇人、変人」を意味したが、徐々にポジティブな意味が加えられるようになり、過剰ともいえるほど特定の問題に精通している専門家という位置付けになりつつある。今日では、官庁でも企業でも学校でも、今日ではコンピュータとネットワークなしでは業務に差し支える。そうしたインフラストラクチャとしての情報技術（IT）を支えているのがギークたちである。

ギークたちの技術力は、最もハイテクであるはずの安全保障にも迫ってきている。その象徴的な例が、2005年に公開されたグーグル社の新サービス「グーグル・アース（Google Earth)」である。無料で配布されているソフトウェアをダウンロードすると、世界中の都市の衛星・航空写真を見ることができる。このサービスに対してインド、韓国、オランダといった政府がこれまで懸念を表明している[5]。今までこうした技術は軍事技術として、ごく一部の人にしかアクセスができなかった。しかし、コンピュータの普及は、より多くの人にアクセスの機会を提供するようになってきている。

注目すべきは、そうした技術を開発しているのは誰かという点である。ギークたちの間では政府や軍、大企業のようなピラミッド型の組織で働くことを嫌っている。そうした組織で働く人たちのことをギークたちは、「ガリ勉野郎」を表す単語の「ワンク（wonk)」、あるいはスーツを着ているという意味で「スーツ（suits)」と呼ぶ[6]。

ギークとワンクの間の、一種の文化的対立は深刻である。かつてギークたちは「われわれは王様も大統領も投票も拒否する。われわれが信じるのはラフ・コンセンサスと動くコードだ」という言葉が共有されている[7]。ワンクたちは、ギークたちの技術力を使わないわけにはいかない。しかし、安全保障を含めてわれわれの社会システムが技術に依存すればするほど、この文化的対立は深刻になるだろう。

2-2 インテリジェンス・コミュニティ

日本語で「情報機関」や「諜報機関」と呼ばれるインテリジェンス機関は、外交・安全保障政策における意思決定の判断材料となる情報を収集・処理・精製し、提供するための政府組織である。米国には、中央情報局（CIA）や国防情報局（DIA)、国家安全保障局（NSA)、連邦捜査局（FBI）など16のインテリジェンス機関があり、それらをまとめて「インテリジェンス・コミュニティ」と呼んでいる。

インテリジェンス機関の情報収集の手法として代表的なのは以下の三つである。

(1) HUMINT (Human Intelligence)
(2) IMINT (Imagery Intelligence)
(3) SIGINT (Signal Intelligence)

HUMINTとは、人間の活動による情報収集のことで、いわゆるスパイ活動もここに含まれる。IMINTとは、人工衛星や航空機による写真や各種画像の解析によるインテリジェンス活動である。SIGINTとは、電子的な通信の信号（シグナル）の傍受と解析によるインテリジェンス活動である。もともとは戦場で飛び交う電波の傍受とそこで使われている暗号文の解読から始まった。電波は誰でも受信できるが、それをそのままでは意味不明にする暗号も同時に発達した。他にも、技術に力点を置いたTECHINT（Technical Intelligence)、公開情報に力点を置いたOSINT（Open Source Intelligence)、コミュニケーション（通信）に力点を置いたCOMINT（Communication Intelligence)、電子情報に力点を置いたELINT（Electronic Intelligence）というような言い方もある。

---

[4] ジョン・カッツ（松田和也訳）『GEEKSギークス―ビル・ゲイツの子供たち―』飛鳥新社、2001年。
[5] Dinesh C. Sharma「『Google Earthは国防上の脅威』―インド大統領が警告」<http://japan.cnet.com/news/media/story/0,2000056023,20089041,00.htm>(2006年8月12日アクセス)。
[6] カッツ、前掲書。
[7] マサチューセッツ工科大学（MIT）教授のデービッド・クラーク（David Clark）の言葉である。ただし、クラークは無政府主義を唱道するために使ったわけではなく、インターネットの自由な活動の雰囲気を伝えるためにあえて誇張して使ったとしている。2008年7月21日、MITにおける筆者とのインタビュー。

デジタル技術が強く影響するのは、SIGINT はいうまでもなく、TECHINT、COMINT、ELINT であろう。それらに加えてインターネットが大量の情報を公開している点を考えれば、OSINT にも関係する。さらには、人と人とのつながりをインターネットが支援しているとすれば、HUMINT にも影響するし、グーグル・アースが示したように IMINT にも影響がある。つまり、デジタル技術の登場は、インテリジェンス活動を本質的に変えてしまうものである。

2-3 インターネット・コミュニティ

もともとは軍事的な背景を持っていたインターネットだが、1970 年代から 1990 年代初めまで、約 20 年にわたって、主として研究者たちによって運営されてきた。しかし、インターネットは、ネットワークのネットワークという意味であり、中心となる管理組織を持っていない。インテリジェンス・コミュニティが政府の法律によって作られ、税金によって支えられた組織であるのに対し、インターネット・コミュニティは、いわばボランティアによって支えられている組織である。

インターネット・コミュニティはまったくの空洞というわけではない。そこには複数の中心的役割を担う組織が存在する。しかし、どれも支配的な役割を担うことができず、「自律・分散・協調」的に運営されている。そうした組織としては、ISOC（Internet Society）、IETF（Internet Engineering Task Force）、ICANN（Internet Corporation for Assigned Names and Numbers）、W3C（World Wide Web Consortium）などがある[8]。無論、これらがインターネットに関連する組織のすべてではない。既存の外部の組織もインターネット・ガバナンスに関わるようになっている。

こうしたさまざまな組織、そしてそれに参加している個人を総称して「インターネット・コミュニティ」と呼んでいる。インターネット・コミュニティは、メンバーシップのはっきりとしたコミュニティではない。誰でもが参加できる代わりに、誰か特定の人が特殊な権限を持っているわけではない。

こうした方式は、多かれ少なかれ、他のインターネット関連の組織にも共有されている。つまり、重要な問題は誰かの恣意的な判断や権威によって決められるのではなく、情報の共有と熟議によって決められる。これは、インテリジェンス・コミュニティとはきわめて異なるシステムであるといえるだろう。

インテリジェンス・コミュニティは、自ら意思決定をすることはない。彼らは政策決定者が判断する際の素材を提供するに過ぎない。そして、その組織は法律と階層構造によって規定されている。それに対してインターネット・コミュニティはフラットでネットワーク型の組織構成をとっており、そこへの出入りも自由である。インテリジェンス・コミュニティに入るのは簡単ではない。厳密な背景調査と試験をくぐり抜けないとそのインサイダーにはなれない。まったく異なる組織原理で二つの組織は動いている。

3 ブッシュ政権の令状無し傍受

3-1 米国における通信傍受の法的枠組み

通信傍受とは情報の大海から有用な一滴を見つけ出すことに他ならない。情報社会といわれる今日、その作業はきわめて困難になる。また、その活動はプライバシーや言論の自由を侵害するおそれがあり、法的な規制もかけられている[9]。

米国憲法の中で「通信の秘密」は明示的に書かれてはいないが、憲法修正第 1 条の「言論の自由」、修正第 4 条の「プライバシーの保護」が援用されている。つまり、自由な表現をするためには自分の通信が盗聴されていないという保障がなければならない。また、自分の会話が正当な理由なく第三者に聞かれてしまうということはプライバシーの侵害にあたる。言論の自由とプライバシーを守るために通信の秘密が必要であるという論理である[10]。しかし、特定の条件を満たす場合には通信の傍受が認められることがある。

特定の条件とは犯罪捜査と国家安全保障上の危機である。犯罪が行われたことを証明するため、あるいはその疑いが強い場合に証拠集めとして行われるのが「司法傍受」である。まれには犯罪の予防のために行われることもある。司法傍受の実施者は主に警察である。これに対して、犯罪の予防的側面が強く、テロや組

---

[8] 土屋大洋「セルフ・ガバナンスの意義と変容」林紘一郎、池田信夫編『ブロードバンド時代の制度設計』東洋経済新報社、2002 年。

[9] 米国におけるインテリジェンス活動と通信傍受については以下も参照。土屋大洋『情報による安全保障―ネットワーク時代のインテリジェンス・コミュニティー』慶應義塾大学出版会、2007 年、第 7 章。

[10] 日本国憲法では第 21 条の中で「通信の秘密」が明示されている。しかし、やはり犯罪捜査には必要であるとして、日本でも強い反対がある中、1999 年 8 月に通信傍受法が成立した。

織犯罪などを防ぐ目的として、インテリジェンス機関によって行われるのが「行政傍受」である[11]。いずれにせよ、合法的な通信傍受には「相当な理由（probable cause)」が必要になる。

米国の対外インテリジェンスにおいて最も重要なのは外国インテリジェンス監視法（FISA）である。米国では、欧州ほどではないが長い間、通信傍受が行われてきた。第二次世界大戦前はそれを規制する法律も明確には存在しなかったため、かなり広範に行われていた可能性がある。しかし、リチャード・ニクソン(Richard Nixon）政権のときにこの問題が注目され、強い批判を浴びることになった。いわゆるニクソン大統領によるウォーターゲート事件である[12]。この事件を調査したチャーチ委員会は、1975 年と 76 年に、合わせて 14 本の報告書と提言を発表した。チャーチ委員会の提言は、FISA の成立と外国インテリジェンス監視裁判所（FISC）の設立へとつながった。

FISA は、技術的に情報を集める場合、「最低の侵入技術に留めねばならないこと、求めるものは個人情報でなく、純粋な秘密情報ないしスパイ防止情報でなければならないこと、必要な情報は通常の調査技術によって合法的に入手しなければならないこと、そしてもっとも重要な点は、監視下におかれる米国人は外国勢力の機関員であると信じるべき理由がなければならないこと、を規定していた[13]。」

対外インテリジェンスが国内の犯罪捜査の場合と異なるのは、犯罪性が傍受命令取得の要件ではなく、対象が外国勢力であるかどうかが問われる点である。つまり、米国民に対する通信傍受は犯罪に関わっている「信じるに足りる相当な理由」がある場合を除いて認められていないが、外国人と外国勢力に関係する者に対しては実質的に無制限に行われる。

米国内での傍受については、ウォーターゲート事件によって、実質的に NSA による国内の傍受は終わりを告げたはずであった[14]。ところが、ブッシュ政権の令状無し傍受は、それが復活していたことを示している。

3-2 ニューヨーク・タイムズのスクープ

そもそもこの問題が発覚したのは、2005 年 12 月 16 日、米『ニューヨーク・タイムズ』紙によるスクープであった。記事を書いたジェームズ・ライゼン（James Risen）によれば、ブッシュ大統領は裁判所の許可なしで NSA に通信を傍受させていた[15]。記事が出た翌日の 17 日、ブッシュ大統領は定例のラジオ演説をテレビでも中継させ、その中でこの報道を認めた。大統領は、2001 年の対米同時多発テロ（9.11）以降、30 回以上にわたり、米国内と海外との間の国際電話や電子メールなどを、大統領令に基づいて傍受させていたと述べた。『ニューヨーク・タイムズ』の記事によれば、30 回といっても、実際に傍受されたメッセージは数百ないし数千にもなるという。ただし、大統領は事前に議会の指導者たちに通知しており、完全に秘密裏に行われていたわけではない。

この問題のポイントは二つある。第一に、前章で触れた FISA に基づいて裁判所で手続きをとれば同様の傍受ができたはずなのに、なぜ大統領令によってこれを簡略化しようとしたのかという点である。FISA の枠組みの中でも緊急傍受は可能で、数時間以内に傍受の許可を出すことも可能である。第二に、市民権を持つ米国市民がインテリジェンス活動の対象となった可能性があるという点である。かつてベトナム戦争時代に反戦運動をしている人物や市民団体がインテリジェンス活動の対象となってしまった反省から、明白な理由がない限り、米国市民に対してはインテリジェンス活動をすることは認められていない。外国との国際電話や電子メールが対象であったとはいえ、米国市民の通信が傍受されていた可能性は高い。ブッシュ政権の令状無し傍受は、政府によって電子メールが読まれている可能性を示した。

米国政府と同盟国による通信傍受活動としては、いわゆる「エシュロン」がよく知られている[16]。エシュロンは公式に存在が認められているわけではないが、そうした通信傍受活動が行われていたことは確かであ

---

[11] なお、わが国では行政傍受は認められていない。1998 年に成立した通信傍受法は司法傍受を認めるものである。

[12] James Risen, *State of War: The Secret History of the CIA and the Bush Administration*, New York: Free Press, 2006, pp. 41-42.

[13] スタン・ターナー（佐藤紀久夫訳）『CIA の内幕―ターナー元長官の告発―』時事通信社、1986 年、143 頁。

[14] Risen, op.cit, p. 42.

[15] James Risen and Eric Lichtblau, "Bush Lets U.S. Spy on Callers Without Courts," *New York Times*, available at <http://www.nytimes.com/2005/12/16/politics/16program.html> (publish: December 16, 2005).

[16] 例えば以下を参照。産経新聞特別取材班『エシュロン―アメリカの世界支配と情報戦略―』角川書店、2001 年。鍛冶俊樹『エシュロンと情報戦争』文藝春秋、2002 年。小倉利丸編『エシュロン―暴かれた全世界盗聴網―』七つ森書館、2002 年。

る。しかし、エシュロンが得意とする傍受はアナログの無線通信であり、衛星電話やマイクロ波による通信、同軸ケーブルによる有線通信が対象となってきた。それに対して現在ではデジタル通信が主流になり、光ファイバーが多用されている。アナログ時代の傍受がエシュロンであるのに対し、デジタル時代の傍受がブッシュ政権による通称「プログラム」である。

3-3 テロの拡大と通信傍受

ブッシュ大統領は、9.11 以前はインテリジェンスの活動にほとんど関心を示さなかったといわれている。しかし、9.11 以降、2001 年 11 月頃には、ブッシュ大統領は、世界中の電話やその他の通信を傍受する NSA の能力に魅了されるようになっていた。重要な電話の会話を盗聴できれば、今後のテロを防げるかもしれないし、少なくとも減らすことは可能だろう。「あらゆる電話を盗聴して、やつらを追いつめ、無辜の人々を守る」と述べたという[17]。そうした過程の延長として令状無し傍受は行われるようになった。

図 1は、国家安全保障を目的として行われた通信傍受の件数を示している。クリントン大統領が再選される 1996 年から件数が増え始め、9.11 の翌年の 2002 年からは急増していることが分かる。ブッシュ政権が行った令状無しの通信傍受は、このグラフの中には含まれていない。このグラフに含まれているのは、令状が出され、FISC（裁判所）が認めたものだけである。また、このグラフを見て分かる通り、拒否された FISA 申請はほとんどない。元データを見ると 2003 年に 4 件拒否されているだけである。他の年で提示数と承認数にずれが生じているのは、政府側が自主的に申請を取り下げているからである。FISC のチェックは実は「ざる」になっている現状が浮かんでくる[18]。

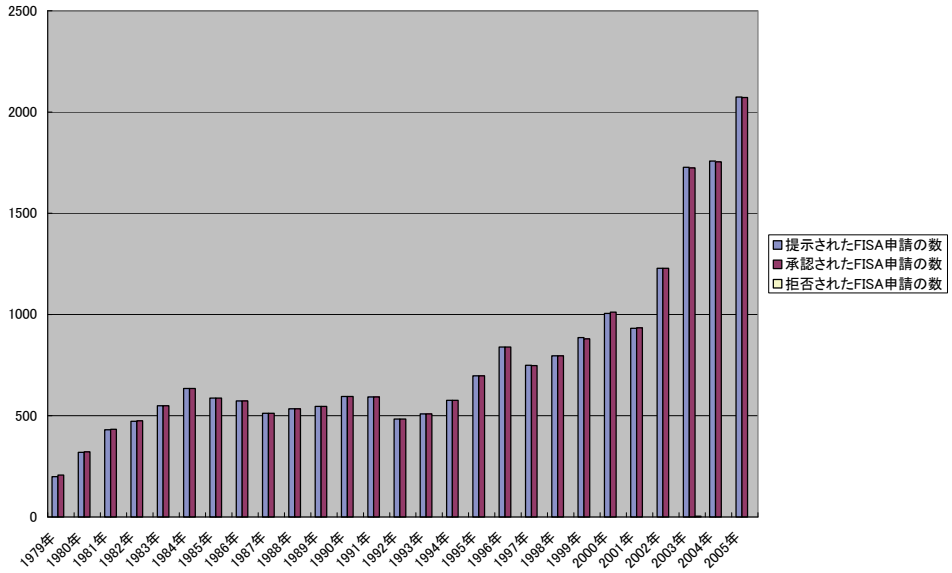

図 1　米国における国家安全保障目的の通信傍受件数の推移

出所：http://www.epic.org/privacy/wiretap/stats/fisa_stats.html
http://www.epic.org/privacy/wiretap/

こうしたこととは別に、大きな社会変化が生まれていた。つまり、デジタル通信技術の普及と、通信量の大幅な拡大である。つまり、ギークたちが作りだしたインターネットや携帯電話、携帯通信端末、さらにはインターネットを使った音声通話（VoIP：Voice over IP）などが普及し、デジタル化された信号が大量に通信ネットワーク回線の中を通るようになった。アジアとヨーロッパのとの間の通信は、米国を経由して行われることが予想される。

しかし、この状況に甘んじていることを許さなくしたのが 9.11 であった。ブッシュ政権はチャーチ委員会

[17] ボブ・ウッドワード（伏見威蕃訳）『ブッシュの戦争』日本経済新聞社、2003 年、401 頁。
[18] 正式な申請の前に裁判所との間で申請をめぐる調整が行われており、不適切な申請、却下される可能性が高い申請については事前に修正されたり、取り下げられたりすることが多いため、却下されるものが結果的に少なくなるという。2009 年 2 月、匿名の元 FBI 職員とのインタビュー。

以来、約 30 年にわたって守られてきたルールを脇に追いやり、NSA に大規模な国内の通信傍受を命じることにした。

ライゼンによれば、NSA は令状無しで米国内の 500 人の電話を傍受し、潜在的には数百万人の携帯電話や電子メールにアクセスしていたという。ブッシュ大統領は、テロ活動の兆候をつかむためにこうした活動を秘密裏に承認した。これを可能にしたのは、9.11 から数カ月後の 2002 年初めに大統領が署名した秘密の大統領令である。また、ホワイトハウス、CIA、NSA、司法省の弁護士たちもこれを可能にするための一連の意見書をしたためた[19]。新聞報道の翌日のラジオ演説で認めた通り、大統領は責任逃れをすることなく、大統領の権限で承認したと述べている。

ブッシュ政権が裁判所の令状を回避した第一の理由は、通信量があまりに厖大だったため、そのすべてについて裁判所から迅速な承認を得ることが難しかったからだとライゼンは指摘している。FISA が作られた 1970 年代、傍受の対象となる通信量がこれほど拡大すると考えていた人はいなかった。2006 年には、年間で約 9 兆通の電子メールが米国で送信され、毎日 10 億回の携帯電話の通話、そして 10 億回を軽く超える固定電話の通話が行われていると見積もられている[20]。いわば制度が現実に追いついていないため、ブッシュ政権は制度を回避することを考えたことになる。

第二の、そして主たる理由は、そこに有用なインフォメーションが大量にあると考えられたことである。つまり、米国の通信基盤が世界で最も進んでおり、通信回線のネットワークのハブが米国になっている。米国が本来関与しない通信も米国を経由して行われることがある。例えば、中東の国とアジアとの間で行われる通信も、物理的には米国内の通信設備を経由して行われることがある。これにアクセスできれば、有益なインフォメーションが得られるかもしれない。

図 2は、国際的なインターネット回線の帯域幅を図式化したものである。これを見ると、米国を中心にネットワークが敷設されていることが分かる。アフリカはいまだに細い回線しか引かれておらず、孤立している。また、アジアとヨーロッパとの間を直結する回線も実は細いことが分かる。アジアとヨーロッパとの間の通信は米国を経由して行われることが予想されるだろう。

そうすると、本来は傍受することができないアジアとヨーロッパとの間の通信にアクセスできれば、テロに関する有益な情報を得られるかもしれない。これがブッシュ政権の狙いであった。

この政策転換によって、通信傍受のやり方も大きく変わった。もともと米国の通信事業者は法律によって政府に協力することが求められているが、ブッシュ政権の下で NSA はこれまでにない規模で通信会社の協力を仰ぐことになった。つまり、NSA の傍受ネットワークが各通信会社の設備と直結され、大量のデータが NSA に流れることになった。NSA が使っているとされるナルス (Narus) 社の「ナルスインサイト (NarusInsight)」という傍受用機器は、DSL 回線 3 万 9000 本にあたる OC-192 のネットワーク回線をリアルタイムでモニターする能力がある。

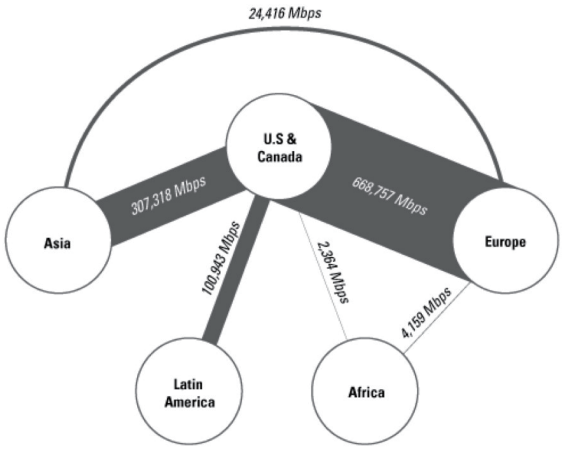

図 2　国際インターネット回線の帯域

出所：Telegeography.com (c) PriMetrica, Inc. 2005

[19] Risen, op.cit., pp. 44-45.
[20] Risen, op.cit., p. 48.

しかし、こうした大規模な通信傍受は、業界の協力がなくてはできない。ブッシュ政権の令状無し傍受の要請に応じた通信会社は、AT&T、ベライゾン、ベルサウスの大手三社だったといわれている。2006 年 5 月 12 日、中堅通信事業者のクエスト・コミュニケーションズ前最高経営責任者(CEO)のジョセフ・ナッチオ(Joseph Nacchio) は、「当局から記録提出要請があったが拒否した」との声明を出した。ナッチオ前 CEO は、インテリジェンス・コミュニティ側が捜査令状を持たず、連邦通信法に抵触するおそれがあったため、拒否したという[21]。

ブッシュ政権の令状無し傍受は、その後、複数の訴訟に直面することになる。そのうち一つはブッシュ政権の決定自体が違法であると訴えるものであり、別のものは、ブッシュ政権のプログラムに荷担した AT&T を集団訴訟で訴えるものである。

ブッシュ政権は批判をかわすため、いったんは令状無しの傍受を中止すると発表するとともに、FISA の改正によって改めて合法性を確保することにした。2008 年の大統領選挙の時期と重なる中で議論が行われ、2008 年 7 月に FISA 改正法は成立した (Public Law No: 110-261)。この改正ではテロ対策としての傍受が認められるとともに、政府に協力する通信会社に対する免責も認められることになった。民主党のバラック・オバマ (Barack Obama) 大統領候補は、当初改正に反対したが、途中で改正賛成に回り、支持者を失望させる一幕があったが、ヒラリー・クリントン (Hillary Clinton) 候補は終始反対だった。

4 おわりに

インテリジェンス・コミュニティの活動と通信傍受は切っても切れないものになってきている。ブッシュ政権の令状無し通信傍受は、それを如実に示した事例だといえるだろう。一方、ギークたちは、政府が処理しきれないほどの通信を生み出すシステムを作り出し、発展させてきた。電話の時代ならば政府が対応すべきはせいぜい郵便と電話、特に国際電話を傍受していれば良かった。しかし、インターネットをはじめとするデジタル技術はいとも簡単に国境をすり抜けていく。

9.11 でも明らかなように、テロリストたちはインターネットや携帯電話をフル活用している。今でも世界中のテロリストたちは、そうした新しいデジタル技術を使って、資金を集め、人材をリクルートし、支持を集めるためのメッセージを発信し、眠れる潜在的テロリストたちを呼び覚まし、テロ実行のための作戦計画をオンラインで練っている。電子メールはいうまでもなく、暗号を使ったメッセージがウェブの掲示板などに貼り付けられている。テロリストたちのウェブ・サイトは短期間で転々と所在を変え、つかみ所がない。逆に政府機関のコンピュータに侵入し、欲しい情報を奪うこともしているかもしれない。サイバースペースでは実に安価にテロ関連行為ができる。

ギークたちのインターネット・コミュニティと、政府のインテリジェンス・コミュニティは、全く質の異なる二つの情報共同体である。インターネット・コミュニティは誰にでもオープンで、情報の共有に最大の価値を置き、公益性と自発性に基づいて形成されてきた。それに対してインテリジェンス・コミュニティは、クオリファイされた人々による閉ざされたコミュニティであり、情報の統合的所有に力点を置き、政府組織の中の権限と秩序の維持という使命に基づいて形成されてきた。交わることの無かった二つの情報共同体が、テロリストたちによってつながり、衝突するようになってきている。

政府にとってはいかにしてギークたちを取り込むかが重要な課題の一つになる。米国の NSA の優位は、圧倒的な技術と優秀な職員によって支えられている。それを上回る勢力の登場があるとしたら、政府にとっては大きな脅威となるだろう。現にグーグルは、世界政府があったとして、そのための情報システムを作ろうという思想を持っている[22]。

テロリストたちがギークたちの技術を最大限活用しようとするならば、インテリジェンス機関もまたそうしなければならない。技術過信だという批判もありえよう。しかし、技術変化のスピードは圧倒的である。インターネットは世界中に新技術に関する情報をばらまいている。ギークたちを理解できなければインテリジェンス・コミュニティは失敗するだろう。もはや技術を止めることはできないからである。最先端の技術に追いついていけなければ、テロリストたちに遅れをとることになる。

---

[21]「米通信中堅クエスト　記録提出を拒否　情報機関からの要請に」『日本経済新聞』2006 年 5 月 13 日夕刊。
[22] 梅田望夫『ウェブ進化論―本当の大変化はこれから始まる―』ちくま新書、2006 年、14～15 頁。

【参考文献】

James Bamford, *The Puzzle Palace: A Report on America's Most Secret Agency*, Harmondsworth: Boston: Houghton Mifflin, 1983.

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.

James Bamford, *The Shadow Factory: The Ultra-Secret NSA from 9/11 to the Eavesdropping on America*, New York: Doubleday, 2008.

Edward C. Liu, "Amendments to the Foreign Intelligence Surveillance Act Set to Expire in 2009," CRS Report for Congress, R40138, Congressional Research Service, March 16, 2009.

Richard A. Posner, *Uncertain Shield: the U.S. Intelligence System in the Throes of Reform*, Lanham, Md.: Rowman & Littlefield, 2006.

James Risen and Eric Lichtblau, "Bush Lets U.S. Spy on Callers Without Courts," *New York Times*, available at <http://www.nytimes.com/2005/12/16/politics/16program.html> (publish: December 16, 2005).

James Risen, *State of War: The Secret History of the CIA and the Bush Administration*, New York: Free Press, 2006.

John Yoo, *War by Other Means: An Insider's Account of the War on Terror*, New York: Atlantic Monthly Press, 2006.

ボブ・ウッドワード(伏見威蕃訳)『ブッシュの戦争』日本経済新聞社、2003 年。

梅田望夫『ウェブ進化論―本当の大変化はこれから始まる―』ちくま新書、2006 年。

大津留(北川)智恵子「大統領像と戦争権限」『アメリカ研究』第 43 号、2009 年、59～75 ページ。

小倉利丸編『エシュロン―暴かれた全世界盗聴網―』七つ森書館、2002 年。

鍛冶俊樹『エシュロンと情報戦争』文藝春秋、2002 年。

ジョン・カッツ(松田和也訳)『GEEKS ギークス―ビル・ゲイツの子供たち―』飛鳥新社、2001 年。

パトリック・ラーデン・キーフ(冷泉彰彦訳)『チャター―全世界盗聴網が監視するテロと日常―』日本放送出版協会、2005 年。

産経新聞特別取材班『エシュロン―アメリカの世界支配と情報戦略―』角川書店、2001 年。

アーサー・シュレジンガーJr.(藤田文子、藤田博司訳)『アメリカ大統領と戦争』岩波書店、2005 年。

スタン・ターナー(佐藤紀久夫訳)『CIA の内幕―ターナー元長官の告発―』時事通信社、1986 年。

土屋大洋「セルフ・ガバナンスの意義と変容」林紘一郎、池田信夫編『ブロードバンド時代の制度設計』東洋経済新報社、2002 年。

土屋大洋『情報による安全保障―ネットワーク時代のインテリジェンス・コミュニティ―』慶應義塾大学出版会、2007 年。

〈発　表　資　料〉

題　　名	掲載誌・学会名等	発表年月
サイバーセキュリティーが米新政権の課題に	NIKKEI NET	2008 年 8 月
Defense against Cyber Terrorism: Head War and Body War	International Studies Association Annual Convention 2009	2009 年 2 月
インターネットにおけるテロとの戦い―米国における FISA（外国情報監視法）を事例に―	日本公共政策学会 2009 年度研究大会	2009 年 6 月