

ブッシュ政権の令状なし通信傍受をめぐる課題：デジタル技術とネットワークがインテリジェンス・コミュニティにもたらした変化[†]

Policy Issues on Warrantless Wiretapping by the Bush Administration: Changes in Intelligence Community by Digital Technologies and Networks

土屋 大洋*

Motohiro Tsuchiya

2005年末、『ニューヨーク・タイムズ』紙のスクープ記事によって、米国のブッシュ政権が、法的に定められた手続きを取らずに大規模な通信傍受を行っていることが明らかになった。国際電話や電子メールなど、対象者は数千人に上ると見られている。ブッシュ大統領はテロ対策として正当化されると主張しているが、通信の秘密を損なうものとして批判されている。

通信傍受はインテリジェンス・コミュニティが行う活動のひとつであり、世界中の通信トラフィックが米国に集まっていることにブッシュ政権は注目し、通信会社に協力させている。これに対して訴訟が起こされ、政府が通信傍受活動そのものを止めるように求められるとともに、協力した通信事業者も集団訴訟を起こされている。

米国のこの事件は、日本の通信事業者にとって対岸の火事ではない。米国経由・日本発着の通信も傍受されている可能性が高く、日本の通信サービスの利用者の通信の秘密が守られていない。また、日本がテロの脅威に直接さらされたり、米国政府から要請を受けたりすれば、日本の通信事業者が同様の通信傍受活動に巻き込まれる可能性がある。テロに対する安全対策と、通信の秘密やプライバシーの保護との間のバランスを考え、そうした事態に備えておくことが必要である。

In December 2005, New York Times reported that the Bush administration of the United States was intercepting massive telephone communications and e-mail messages without court warrants required by a law. The number of people who were intercepted under this program is estimated over thousands. Although President Bush said the program should be justified to combat terrorism, it was widely criticized due to possible invasion of privacy and secrecy of communication.

Interception of communication is a part of activities of intelligence agencies. The Bush administration found that a large number of communications of the world could go through the land of the United States, and requested telephone and Internet operators to cooperate with this program. A few judicial challenges have been raised against this government program and a telephone company involved in it.

This case should not be fire on the other side of the ocean, because communication departing from and arriving Japan could be intercepted when it goes through the U.S. It could mean that secrecy of customers of Japanese operators is not protected. Moreover, as an ally of the U.S., Japanese government (and communication operators) could be requested by the U.S. government to cooperate with this program to fight against global terrorism. It is a possible and urgent policy issue for Japanese operators to prepare for this situation.

March 15, 2007

情報通信政策研究プログラム

[†] 本稿は「情報通信政策研究プログラム」の研究助成を得て行った研究の成果を総括したものである。

* 慶應義塾大学助教授 taiyo@sfc.keio.ac.jp

1. ニューヨーク・タイムズのスクープ

2005年12月16日、米『ニューヨーク・タイムズ』紙は、ジョージ・ブッシュ（George W. Bush）大統領が裁判所の許可なしで国家安全保障局（NSA : National Security Agency）に通信を傍受させているというスクープ記事を掲載した*。翌17日（土）、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ふたつある。第一に、外国情報活動監視法（FISA : Foreign Intelligence Surveillance Act）という法律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、米国民（米国の市民権を持つ人々）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、米国民の通信が傍受されていた可能性は高い。

9.11以降、さまざまな場面で安全保障とプライバシーのせめぎ合いがみられるようになってきている。空港でのセキュリティ・チェックや監視カメラの導入である。しかし、空港のセキュリティ・チェックは本人が認識しているなかで行われる。監視カメラも基本的には探せば分かるところに置いてある。隠しカメラと違って、監視カメラは監視されている人が行動を抑制することが目的だからである†。

しかし、通信の傍受は本人が気づかないところで行われていることが多い。自分の電話が誰かに聞かれていたり、電子メールが誰かに読まれていたりするという前提で使っていることは少ない。グーグル（Google）の無料電子メール・サービスであるGmailは、逆にグーグルのコンピュータがメールを読んでいることを売り物にしている。利用者のメールをコンピュータが読み込むことで（グーグルの従業員が読むことはない）、そのメールの内容に即した広告を表示することになっている。その代わりに、無料で大容量のメール・サービスを使うことができる。しかし、普通のISP（Internet Service Provider）や職場で提供されているメールが読まれている

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

† デイヴィッド・ライアン（河村一郎訳）『監視社会』青土社、2002年、13ページ。

とは、普通の人々は思っていない。

ブッシュ政権の令状なし傍受は、実は政府によって、それもコンピュータだけではなく人間によっても電子メールが読まれている可能性を示した。自分にやましいところがなければ、誰が通信を読もうと気にしないという人もいる。しかし、通信の秘密は、政治的な圧政から解放されるために確立された基本的な人権のひとつである。この問題をどう考えるかは、インターネットの自由を考えるうえで重要である。

また、米国の大手通信会社 AT&T は、NSA の通信傍受に協力したために集団訴訟を起こされることになった。通信会社のガバナンスという点でもこの通信傍受の問題は看過することができなくなってきている。

本稿では、2005 年末に発覚したブッシュ政権の令状なし通信傍受とはどのようなものであり、それが今後のインターネットにどのような影響を与えるのかについて考えることにしたい。

2. 米国における通信傍受

2.1. インテリジェンス・コミュニティ

ブッシュ政権は、9.11 から 1 年後の 2002 年 9 月に発表した「米国国家安全保障戦略」、いわゆる「ブッシュ・ドクトリン」の中で、潜在的な脅威に対しては先制攻撃（preemptive strike）も辞さないという方針を発表した[‡]。これに基づいて 2003 年 3 月には、大量破壊兵器を保有していると考えられていたイラクとの戦争を開始している。そのときに重要となったのが、「インテリジェンス（intelligence）」である。

ブッシュ・ドクトリンの中では、先制攻撃ばかりではなく、インテリジェンスの活用も重視されている。35 ページの文書の中で 16 回、「インテリジェンス」という言葉が出てくる。先制攻撃ができるということは、事前に米国にとっての脅威が察知されていなくてはならず、それを行うのがインテリジェンス・コミュニティの役割である。ブッシュ大統領による通信傍受の拡大は、こうした米国の安全保障戦略の延長のなかで出てきた事件であるといえるだろう。つまり、テロリズムを止めるためには何でもすると決意したブッシュ政権においては、人々のプライバシーをある程度侵害し、法律に抵触することをもいとわないということである。

そもそも、「インテリジェンス」という言葉は、一般的な辞書では、「(1) (人・動物などの) 知能、知力；理知；理解力、(人・行為・言葉などの) 聡明さ、利発さ。(2) 知性的 [理性的] 存在；天使；霊。(3) 情報、消息、情報収集、報道；諜報（機関）、情報部」といった意味が出

[‡] The White House, *The National Security Strategy of the United States of America* <<http://www.whitehouse.gov/nsc/nss.html>>.

てくる[§]。本稿でいう意味のインテリジェンスとはここでは (3) の意味である。

一般的に日本語で言う「情報」は「インフォメーション (information)」の訳語として使われているが、もともと情報は「インテリジェンス」の訳語であった^{**}。つまり、情報とは、「情勢報告」ないし「敵情報告」の略語として使われ始めたからである。情報社会が、中立的な意味でのインフォメーションがあふれる社会という意味ではなく、インテリジェンスが飛び交う社会という意味だったとしたら、その受け止められ方は違っていただろう。

しかし、現実には、「インフォメーション・ソサイエティ (情報社会)」は「インテリジェンス・ソサイエティ」にもなりつつある。1989年にベルリンの壁が壊れ、1991年にソビエト連邦が消滅して冷戦が終わると、インテリジェンス・コミュニティは不必要であるとされた。確かに、米国のインテリジェンス・コミュニティではリストラが行われ、多くの職員が民間に転出した。その結果、経済分野でのインテリジェンス的な活動が注目されることになる。たとえば、インテリジェンス・コミュニティからビジネス界へ転じた著者たちによる『CIA 株式会社』という本や^{††}、『プロファイリング・ビジネス—米国「諜報産業」の最強戦略—』という本も出ている^{‡‡}。ビジネスの世界にもインテリジェンスの考え方や手法が浸透してきている。

米国においては、1947年に作られ、その後改定され続けてきている国家安全保障法によって定められている複数の機関の集まりのことを「インテリジェンス・コミュニティ」と総称している。2007年1月現在、米国の安全保障体制におけるインテリジェンス・コミュニティとは以下の16機関である^{§§}。

- 中央情報局 (CIA : Central Intelligence Agency)
- 国防総省国防情報局 (DIA : Defense Intelligence Agency)
- 国家安全保障局 (NSA : National Security Agency)
- 国家偵察局 (NRO : National Reconnaissance Office)
- 国家地球空間情報局 (NGA : National Geospatial-Intelligence Agency)
- 国務省情報調査局 (INR : Bureau of Intelligence and Research) ^{***}

[§] ここではオンラインの辞書 (Yahoo! Japan) から引用した。

<http://dic.yahoo.co.jp/dsearch?enc=UTF-8&p=intelligence&dtype=1&dname=1na&stype=0&pagenum=1&index=03781400>

^{**} 仲本秀四郎「情報を考える」公文俊平編『リーディングズ 情報社会』NTT出版、2003年、14～25ページ。

^{††} F・W・ラストマン (朝倉和子訳) 『CIA 株式会社』毎日新聞社、2003年。

^{‡‡} ロバート・オハロー (中谷和男訳) 『プロファイリング・ビジネス—米国「諜報産業」の最強戦略—』日経BP社、2005年。

^{§§} <http://www.intelligence.gov/1-members.shtml>

^{***} 「INR」は「Bureau of Intelligence and Research」の略になっていないが、前組織の略称をそのまま使っている。

- 連邦捜査局 (FBI : Federal Bureau of Investigation)
- 空軍情報部 (US Air Force Intelligence)
- 陸軍情報部 (US Army Intelligence)
- 海軍情報部 (US Navy Intelligence)
- 海兵隊情報部 (US Marine Corps Intelligence)
- 国土安全保障省 (DHS : Department of Homeland Security)
- 沿岸警備隊情報部 (US Coast Guard Intelligence) ^{†††}
- エネルギー省情報部 (Department of Energy: Office of Intelligence) ^{†††}
- 財務省情報分析部 (Department of the Treasury: Office of Intelligence and Analysis)
- 麻薬取締局国家安全保障情報部 (Drug Enforcement Administration: Office of National Security Intelligence)

2.2. インテリジェンスと通信傍受

インテリジェンス・コミュニティの役割は、インフォメーションを集め、インテリジェンスを精製することである。それによって、外交・安全保障上の「突然の出来事 (サプライズ)」を回避し、テロなどの攻撃を防ぐことが目的である。インフォメーションは断片的な「材料」であり、それを収集し、分析することでインテリジェンスという「製品」を作る。そのインテリジェンスに基づいて、政府首脳は意思決定を行う。インテリジェンス・コミュニティの活動には以下の四つのカテゴリーが存在する。

- (1) 情報収集——情報機能
- (2) 敵の諜報活動および破壊工作に対する防御——保全機能
- (3) 対諜報活動 (敵の情報活動に対する積極的な解明)
- (4) 秘密活動 (破壊 [サボタージュ] 工作、欺瞞工作、転覆工作、奇襲攻撃、イデオロギー戦への支援)

こうした枠組みは 50 年近くがたった現在でも大きく変わることはない。しかし、それらの前提となる環境や技術が大きく変わってきている。本稿と関係するのは (1) 情報収集である。情報収集の手法としては、いくつか種類がある。代表的なのは以下の三つであろう。

^{†††} 沿岸警備隊は、組織上は国土安全保障省の一部だが、独立して数えられている。

^{†††} エネルギー省は核不拡散の点からインテリジェンス活動に参加している。

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

HUMINT（ヒューミント）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。映画や小説などで見られるいわゆる「スパイ」は、「エージェント」と呼ばれることが多い。それに対して、インテリジェンス機関の正規の職員は「ケース・オフィサー」と呼ばれ、外交官などの肩書きを持ちながらエージェントを使い、束ねる役割を担う。「情報工員」も通常はエージェントのことを指すことが多い。

IMINT（イミント）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。昔は人工衛星の写真はフィルムのカプセルにパラシュートを付けて投下し、これを軍用機で回収するという方法がとられていたが^{§§§}、さすがに現在ではリアルタイムでデジタル画像を入手できるようになっている。

SIGINT（シギント）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。

他にも、技術に力点を置いた TECHINT（Technology 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。

デジタル技術が強く影響するのは、SIGINT というまでもなく、TECHINT、COMINT、ELINT であろう。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とは、インテリジェンス・コミュニティを本質的に変えてしまうものである。

通信傍受は SIGINT に入れられる。「盗聴」といわれることの多い通信傍受だが、厳密には合法的な通信傍受と非合法的な通信傍受があり、非合法的な通信傍受のみを「盗聴」と呼ぶべきだろう。米国憲法には「通信の秘密」という言葉は使われていないが（日本国憲法では第 21 条で明記されている）、米国憲法修正第 4 条のプライバシー権によって通信の秘密は確認されている。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。いずれにせよ、合法的な通信傍受には「相当な

^{§§§} 斎藤彰『CIA』講談社現代新書、1985年、22～23ページ。

理由 (probable cause)」が必要になる。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。

通信傍受は、欧米では広く行われてきている。ドイツや英国では年間 1 万件ほど行われているという****。両国とも詳細な件数については発表していない。犯罪者やテロリストにヒントを与えることになるためである。ドイツではネオナチ勢力の監視の手段として通信傍受が使われており、英国では IRA (Irish Republican Army : アイルランド共和国軍) によるテロへの対策として用いられてきた。

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。ウォーターゲート事件の背景には、長引くベトナム戦争とニクソン政権の不人気があった。ニクソン大統領は再選を確実にするため、対立する民主党の党本部に盗聴器を設置するなど、合法性を疑われる活動を指示した。そうした疑惑が徐々に高まるなか、1974 年 12 月 22 日にセイモア・ハーシュ (Seymour Hersh) 記者が長文の記事を『ニューヨーク・タイムズ』紙に掲載した。その中で、いわゆる「家宝 (family jewels : 一家の恥という意味もある)」と呼ばれ、CIA が数年にわたって行ってきたオペレーションの詳細を述べた。それは外国の指導者の暗殺、外国政府の転覆、そして、米国市民の政治活動に関する情報収集も含まれていた。こうした活動は、完全に秘密裏に行われたわけではなく、一部の議員にも通知されていた。しかし、大々的に報じられたことで、議会はインテリジェンス活動を十分に監査できていないという批判が高まった。

こうしたニクソン事件を受けて 1975 年に組織されたのが「チャーチ委員会 (Church Committee)」である。これは「インテリジェンス活動に関する政府のオペレーションについての米国議会上院特別調査委員会 (United States Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities)」の通称で、委員長を務めたフランク・チャーチ (Frank Church) 上院議員 (民主党 : アイダホ州) の名前をとってチャーチ委員会と呼ばれている††††。

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。1974 年のニクソン辞任を受けて就任したジェラルド・フォード (Gerald Ford) 大統領は、大統領令 11905 を出し、外国の指導者の暗殺を禁止した (この大統領令は後に 1981 年にレーガン政権の大統領

**** ドイツと英国における関係機関でのヒアリングによる。土屋大洋『ネット・ポリテックス-9.11 以降の世界の情報戦略-』岩波書店、2003 年、48-57 ページ。

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

令 12333 によって改定・更新されている^{††††}。

チャーチ委員会の提言は、外国インテリジェンス監視法 (FISA : Foreign Intelligence Surveillance Act) の成立と外国インテリジェンス監視裁判所 (FISC : Foreign Intelligence Surveillance Court) の設立へとつながった。FISA は、技術的にインフォメーションを集める場合、「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、そして最も重要な点は、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^{§§§§}。」また、この法律の下では、CIA は米国内では電子監視は一切できない。FISA に基づいて申請し、FBI に実施してもらいたいと要望できるだけである^{*****}。

FISC は、米国内にいる外国のスパイ容疑者の監視令状 (surveillance warrants) 請求を監査している。これによって、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^{††††}。ところが、今回の事件はそれが復活していることを示している。ブッシュ政権も本来であれば、この FISC から令状をとり、通信傍受を行うべきであった。しかし、なぜブッシュ政権はそうしなかったのだろうか。次節では、『ニューヨーク・タイムズ』紙で事件をスクープしたジェームズ・ライゼン (James Risen) の著書を元に追いかけてみよう。

3. テロの拡大と通信傍受

3.1. 令状なし通信傍受の背景

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。ホワイトハウスのカウンターテロリズム担当だったリチャード・クラーク (Richard A. Clarke) は、著書『爆弾証言』の中で、ロナルド・レーガン (Ronald W. Reagan)、ジョージ・H・W・ブッシュ (George H. W. Bush)、ビル・クリントン (William J. Clinton)、ジョージ・W・ブッシュ (George W. Bush) の四人の大統領の対テロリズム政策について分析しているが、一番熱心だったのはクリントン大統領で、息子のブッシュ大統領はほとんど聞く耳を持っていな

^{††††} 大統領令 12333 号は CIA に暗殺を禁じ、それ以降、新入りの CIA 局員は全員、それを読んで署名することが義務づけられていた。ロバート・ベア (佐々田雅子訳)『CIA は何をしていた?』新潮社、2003 年、20 ページ。

^{§§§§} 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 ページ。

^{*****} ターナー、前掲書、146 ページ。

^{††††} Risen, op.cit, p. 42.

かったという⁺⁺⁺⁺。

しかし、9.11によって危機に直面したジョージ・W・ブッシュ大統領はインテリジェンスへの依存を深めていく。そうした過程の延長として令状な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なしの通信傍受は、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、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とおり、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。裁判所のチェックは実は「ざる」になっている現状が浮かんでくるだろう。

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、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だろう。

しかし、単純にトラフィックを素通りさせるという状況に甘んじていることが許されなくなったのが9.11であった。ブッシュ政権はチャーチ委員会以来、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は令状なしで米国内の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るという。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から数ヶ月後の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^{§§§§}。新聞報道の翌日のラジオ演説で認めたとおり、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。

⁺⁺⁺⁺ リチャード・クラーク（楡井浩一訳）『爆弾証言-すべての敵に向かって-』徳間書店、2004年、288ページ。

^{§§§§} Risen, op.cit., pp. 44-45.

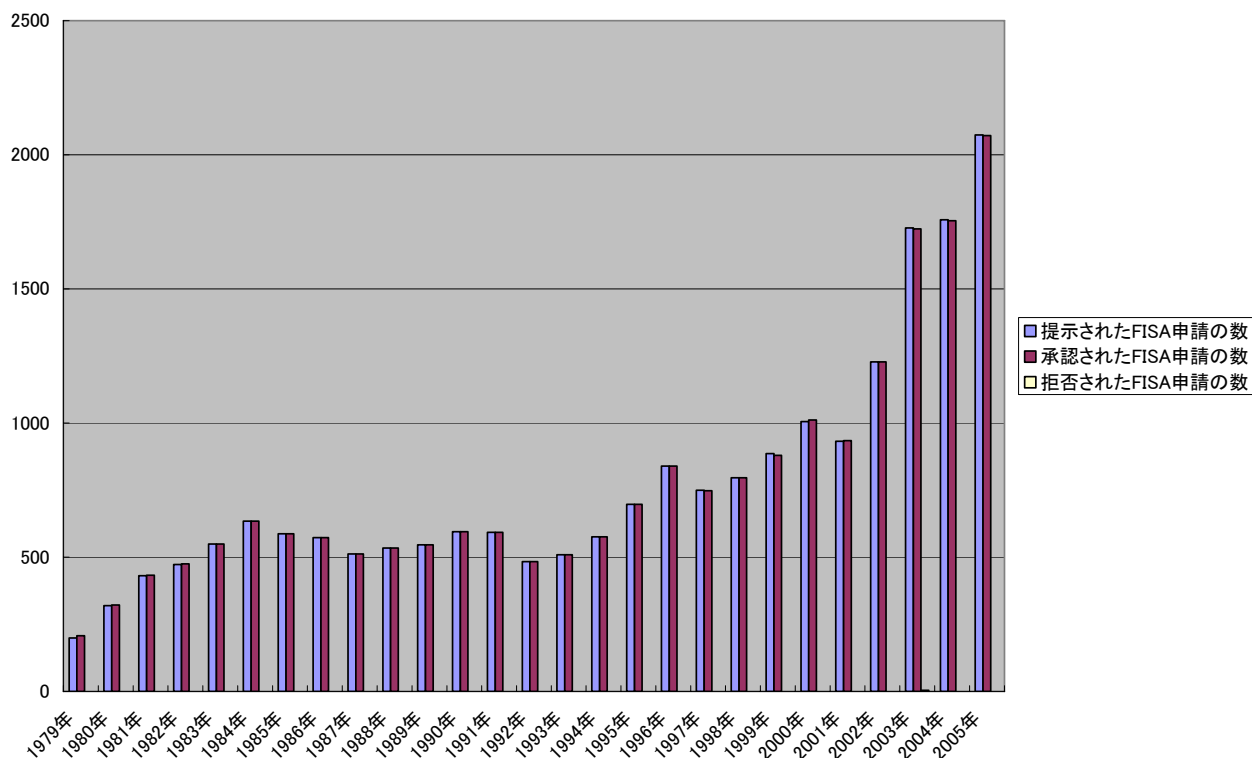


図 1：米国における国家安全保障目的の通信傍受件数の推移

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

<http://www.epic.org/privacy/wiretap/>

ブッシュ政権が裁判所の令状を回避した第一の理由は、通信量があまりに膨大だったため、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言われている。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*****。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。たとえば、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

***** Risen, op.cit., p. 48.

れない。

図 2 は、国際インターネット回線の接続状況を示したものである（国内回線は省略されている）。回線容量が大きいところほど太く示されている。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。米国とヨーロッパとの間を結ぶ大西洋回線が最も太い。米国とアジアを結ぶ太平洋回線もそれなりの太さがある。

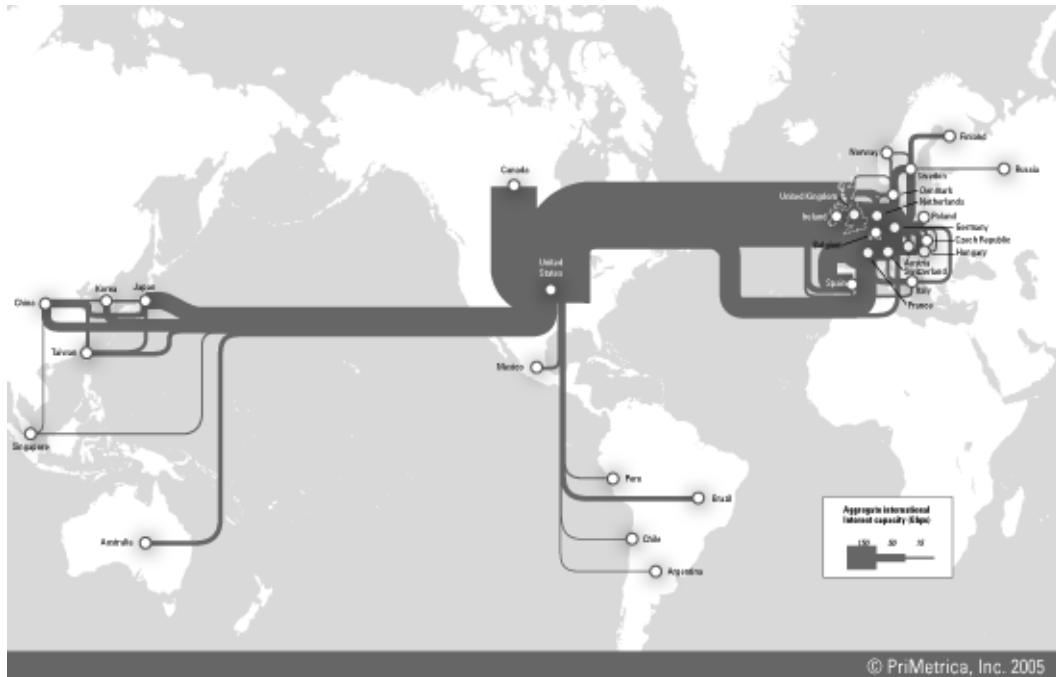
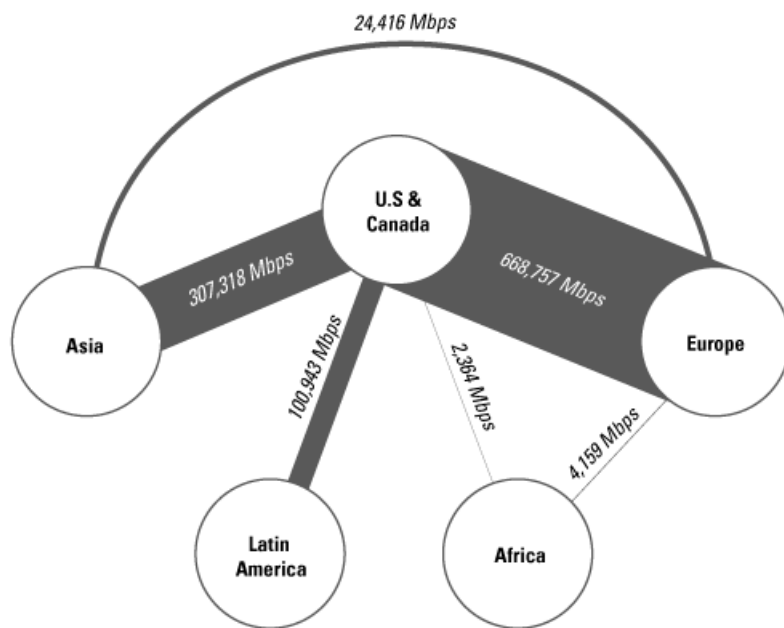


図 2 国際インターネット回線

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



© PriMetrica, Inc. 2005

図 3 国際インターネット回線の帯域

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

図 3 は、回線の帯域幅を図式化したものである。これを見ると、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考えたことであった。

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 Narus 社の「NarusInsight」という傍受用機器は、DSL (Digital Subscriber Line) 回線 39,000 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。

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なし傍受の要請に応じた通信会社は、AT&T、ベライゾン (Verizon)、ベルサウス (BellSouth)

の大手三社だったといわれている。図 4 は、NSA が行っている通信傍受のネットワークを推測して公表されたものである。2006 年 5 月 12 日、中堅通信事業者のクwest・コミュニケーションズ (Qwest Communications) 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るため、拒否したという⁺⁺⁺⁺⁺。

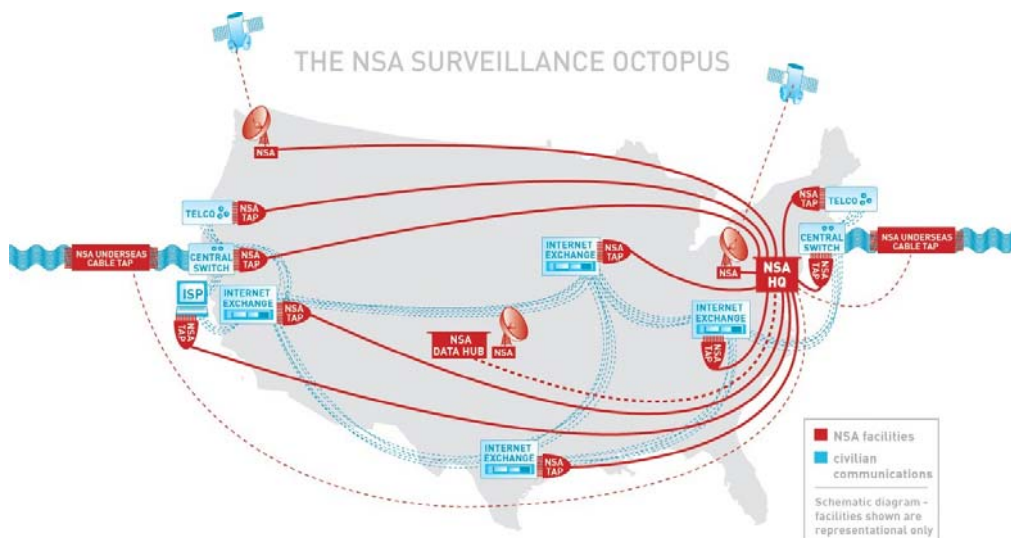


図 4 NSA による通信傍受の予想図

出所：<http://www.aclu.org/safefree/nsaspying/23989res20060131.html>

3.2. マイケル・ヘイデンと NSA

ブッシュ政権の令状なし通信傍受において重要な役割を果たしたのが、マイケル・ヘイデン (Michael Hayden) である。彼は 2007 年 1 月現在、CIA 長官を務めているが、かつて NSA の長官も務めており、彼が NSA の長官在任中に令状なし通信傍受が始まっている。彼は現在でも米空軍の現役将軍のまま CIA 長官を務めている。これまでの CIA 長官はほとんどが文官だったが、ヘイデンは制服を脱ぐことなく、CIA の長官になった。

ヘイデンは 1945 年に生まれ、1969 年、24 歳の時に軍に入隊している。空軍でのキャリアの後、1999 年 3 月、クリントン政権の時に 54 歳で NSA 長官に就任し、2005 年 4 月まで務めている。秘密の組織というイメージが強い NSA だが、ヘイデンは、そうした NSA の暗いイメージ

⁺⁺⁺⁺⁺ 「米通信中堅クwest 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。

を払拭するためにオープンな姿勢を取り、記者たちを自宅でのディナーに招くこともあった。

ヘイデンは、NSA 長官を辞めた後、新設の国家情報長官 (DNI: Director of National Intelligence) に就いたジョン・ネグロポンテ (John Negroponte) の下で、国家情報副長官 (Principal Deputy of National Intelligence) になった。ところが、この新設された国家情報長官と、かつて中央情報長官 (DCI : Director of Central Intelligence) の役割を兼務していた CIA 長官との間で権力闘争が起きる。国家情報長官のネグロポンテと CIA 長官のポーター・ゴス (Porter Goss) は旧友であったが、組織対組織の対立に巻き込まれることになった。その結果、2006 年 5 月 5 日にゴス前長官は辞任した。

これを受け、5 月 8 日にブッシュ大統領はヘイデンを CIA 長官に指名した。ネグロポンテは自分の副官を CIA 長官に付け、権力の基盤固めに成功したことになる⁺⁺⁺⁺⁺。5 月 23 日、上院のインテリジェンス委員会は 12 対 3 でヘイデンの長官就任を承認し、上院本会議も 5 月 26 日に 78 対 15 で承認した。制服を脱がず、問題となっている令状なし通信傍受の責任者であったヘイデンの承認には時間がかかるものと思われていたが、予想以上にあっさりと承認されたことになる。5 月 30 日、ヘイデンは CIA 長官としての宣誓を行い着任した。

2006 年 1 月 23 日、国家情報副長官だったヘイデンは、ワシントン DC のナショナル・プレス・クラブで記者会見を行ったが、そこでの発言が物議を醸した。そこでの質疑応答のやりとりを記録に基づいて振り返ってみよう。質問者はナイト・リッダー (Knight Ridder) 社のジョナサン・ランデイ (Jonathan Landay) 記者である^{§§§§§§}。

ランデイ：同じ問題についてうかがいたいのですが、あなたが傍受のターゲットとする際の基準についてです。私は弁護士ではありませんが、私の理解では、憲法の修正第 4 条は、不法な搜索や拘束に対する米国民の権利を侵害しないような搜索を可能にするためには相当な理由 (probable cause) がなくてはならないと規定しています。あなたが使っているのは……

ヘイデン：いや、実際には……修正第 4 条は、実際には不当な搜索や拘束に対してわれわれすべてを保護しているのだ。

ランデイ：しかし……

ヘイデン：それがその条項が言っていることだ。

⁺⁺⁺⁺⁺ 2007 年 1 月 5 日、ブッシュ大統領はネグロポンテを空席だった國務副長官に任命すると発表した。国家情報長官 (DNI) には、マイク・マコネル (Mike McConnell) 元国家安全保障局 (NSA) 局長を指名した。

^{§§§§§§} "What American Intelligence and Especially the NSA Have been Doing to Defend the Nation: Remarks by General Michael V. Hayden, Principal Deputy Director of National Intelligence And Former Director of the National Security Agency," Address To The National Press Club, Washington, D.C., January 23, 2006

<<http://www.globalsecurity.org/intell/library/news/2006/intell-060123-dni01.htm>>.

ランデイ：しかし、目安は相当な理由だと思えますが。
ヘイデン：修正条項は不当な捜索と拘束とっている。
ランデイ：しかし、それは相当なとっているのでは……
ヘイデン：違う。修正条項が言っているのは……
ランデイ：裁判所の基準、法的な基準の話です……
ヘイデン：不当な捜索と拘束だ。

このやりとりに対して、メディアはヘイデンが「相当な理由」を無視しているのではないかと報じた。つまり、結果的に不当でなければ令状なし通信傍受は正当化されると考えているのではないかと、ヘイデンに対する批判が高まった。

4. 司法と立法の対応

4.1. ACLU の訴訟

ブッシュ政権の令状なし通信傍受で争点とされたのはどのような点だったのだろうか。本節と次節では、このプログラムをめぐって起こされたふたつの訴訟を見てみよう。

ブッシュ政権内でもこの通信傍受活動について知っていた人は限られており、この活動は単に「プログラム (the Program)」とだけ述べられていた。このプログラムを知っていた政府関係者の中にもこのプログラムが憲法の修正第 4 条に違反するのではという懸念があった^{*****}。

先述のように、ブッシュ大統領はこのプログラムを実施するために秘密の大統領令を出し、政権の弁護士たちが法的意見書を書いて法的な基盤を固めようとした。これらの文書は 2007 年 1 月現在公開されていない。こうした文書が依拠するのは、米国憲法第 2 条の広い解釈だといわれている。第 2 条は、軍隊の最高司令官としての権限を大統領に与えている。実際の文言は下記のようになっており、ここから直接、国内の通信傍受を認める権限を見出すことはできない。

第 2 条 第 2 節 (1) 大統領は、合衆国の陸海軍および合衆国の軍務に実際に就くため召集された各州の民兵の最高司令官である。大統領は行政各部の長官から、それぞれの部の職務に関するいかなる事項についても、文書による意見を求めることができる。大統領はまた合衆国に対する犯罪につき、弾劾の場合を除いて、刑の

***** Risen, op.cit., p. 44.

執行延期および恩赦を行う権限を有する^{††††††}。

もうひとつ、政権側が法的根拠としたのが、9.11の一週間後に議会が可決した決議である^{††††††}。この決議は、テロに対するグローバルな戦争を遂行する権限を大統領に与えるというものであり、政権側の弁護士たちは、この決議がNSAの傍受活動を支持する基盤になったと論じている。

9.11の後に議会が可決した「パトリオット（PATRIOT : Provide Appropriate Tools Required to Intercept and Obstruct Terrorism Act）法」は、FBIが行う通信傍受を容易にしている。しかし、この法律でもFISAの令状は必要とされているため、パトリオット法は令状なし通信傍受の根拠とはならない。令状を取得するには傍受対象がテロに関係していると疑われる理由がなくてはならない。パトリオット法はNSAにとって何ら新しい権限を与えていない^{§§§§§§}。

広く自由に関連する問題に取り組み、オンラインの問題にも取り組んでいるACLU（American Civil Liberties Union）は、2006年1月17日、ミシガン州の東地区（デトロイト）の連邦地方裁判所で訴訟を起こした^{*****}。ブッシュ政権のプログラムを即時、恒久的に止めることを求めたACLUの訴訟には、ジャーナリストや非営利組織、テロ専門家なども加わった。こうした人々は中東との間で行われる通信の秘密が仕事をするうえで重要だからである。この中にはNSAに関する一連の著作で知られるジェームズ・バンフォード（James Bamford）も含まれている。ACLU側は、大統領が法を破る権限を持っているわけではないと論じ、米国人対象の通信傍受は民主主義に反するもので、即時に停止されなければならないとした。そして、そうしたプログラムは言論の自由とプライバシーを侵害しているとも主張した。

訴える側が憲法問題の持ち込むのは戦略的な側面がある。かつて1996年に成立した通信品位法（CDA : Communications Decency Act）が問題になったとき、やはり憲法修正第1条の言論の自由が持ち出された。憲法に違反していると訴えることで耳目を集めることができるとともに、法律のテクニカルな解釈ではなく、原理原則論に持ち込むことができる。誰も憲法の条項を否定することは難しいため、訴える側が勝ちやすくなる。実際、通信品位法は訴訟によって違憲判決が出されている^{††††††††}。

^{††††††††} 在日米大使館のウェブ・サイトにある翻訳

<<http://tokyo.usembassy.gov/j/amc/tamcj-071.html>>から引用。

^{††††††††} 9月14日に提出され、18日に成立したS.J.RES.23（Public Law No: 107-40）のこと。そのタイトルは、「米国に対する直近の攻撃に責任ある者に対して米国の軍事力の使用を承認する合同決議（A joint resolution to authorize the use of United States Armed Forces against those responsible for the recent attacks launched against the United States）」である。

^{§§§§§§} Risen, op.cit., p. 47.

^{*****} ACLU, "ACLU Sues to Stop Illegal Spying on Americans, Saying President Is Not Above the Law," <<http://www.aclu.org/safefree/nsaspying/23486prs20060117.html>> (January 17, 2006).

^{††††††††} 木村忠正、土屋大洋『ネットワーク時代の合意形成』NTT出版、1998年。

6月12日、連邦地裁は最初の審理を行った⁺⁺⁺⁺⁺。ACLUの議論に対して政府側は、ACLUの憲法擁護と大統領の権限に関するチェックは「行き過ぎ (extreme)」だと論じた。

第二回目公判は、7月10日に行われた⁺⁺⁺⁺⁺。ここでACLU側は、別の裁判の判決を引用した。つまり、2004年の「ハムダン対ラムズフェルド (Hamdan v. Rumsfeld)」訴訟において、テロとの戦争の間においても大統領は議会の承認なしに無限の権限を行使することはできないと判断された。この裁判で裁判所は、テロとの戦争によってグアンタナモ収容所に入れられた米国市民に対する法的なアクセスを差し止めたり禁じたりするような「無制限の権限 (blank check)」はないと判断した。これは、ブッシュ政権がテロを理由に法の制限を超えることはできないということを意味した。

これに対して政府側は、このプログラムは国家安全保障の秘密を伴うものであり、公判を中止すべきだと主張した。しかし、ACLU側は、すでにプログラムの存在と内容は公知の事実になっていると論じた。

この訴訟の判決は2006年8月17日に出された⁺⁺⁺⁺⁺。デトロイトの連邦地裁は、ブッシュ政権の令状なし通信傍受プログラムは違憲であり、停止されなければならないと判断した。アンナ・ディグス・テイラー (Anna Diggs Taylor) 判事は、NSAのプログラムは憲法修正第1条と第4条の言論の自由とプライバシーを侵害しており、また、FISAとも矛盾すると述べた。また、政府側はこのプログラムの機密性を理由に審理の差し止めを求めていたが、この要求も退けた。テイラー判事は、「米国には世襲の王はおらず、憲法が作る以外の法は存在しない。したがって、[大統領が主張する]『固有の権限』は憲法から引き出されなければならない」と書いている。

4.2. EFFの訴訟

オンラインの自由やプライバシーに関する問題に取り組んでいるEFF (Electronic Frontier Foundation) は、2006年1月31日、ブッシュ政権の令状なし通信傍受は違法であるとして、それに加担したAT&T社に対して集団訴訟 (class action lawsuit) を起こした⁺⁺⁺⁺⁺。つまり、NSA

⁺⁺⁺⁺⁺ ACLU, "Court Hears Arguments on Legality of NSA Spying Program for the First Time Ever," <<http://www.aclu.org/safefree/spying/25833prs20060612.html>> (June 12, 2006). また、ACLU側は別の論点も提起している。つまり、2006年3月に通信大手のAT&Tとベルサウスが合併を発表したが、両者が顧客情報をNSAに提供したのは違法であるというのである。

⁺⁺⁺⁺⁺ ACLU, "Government Abusing State Secrets Claim in NSA Case, ACLU Tells Court," <<http://www.aclu.org/safefree/nsaspying/26098prs20060710.html>> (July 10, 2006).

⁺⁺⁺⁺⁺ ACLU, "Federal Court Strikes Down NSA Warrantless Surveillance Program," <<http://www.aclu.org/safefree/nsaspying/26489prs20060817.html>> (August 17, 2006).

⁺⁺⁺⁺⁺ EFF, "EFF Sues AT&T to Stop Illegal Surveillance," <http://www.eff.org/news/archives/2006_01.php#004369> (January 31, 2006).

に協力して AT&T が大規模な非合法スパイ・プログラムを行っていることは、FISC から令状を取ることにしに通信は傍受されないという FISA の条項に違反するというのである。

NSA の通信傍受に協力する際、AT&T その他の通信会社は、それらの通信記録のデータベースに直接アクセスさせているという。AT&T は、通信記録のために世界で最大級の 300 テラバイトのデータベースを持っているが、政府はそれに自由にアクセスできるようになっている。AT&T は顧客のプライバシーを守るという企業責任を果たしていないと EFF は主張する。しかし、そうした活動にも関わらず、本来のテロ対策という点ではほとんど成果があがっていない。したがって、EFF は AT&T の通信傍受の差し止め命令とともに、プライバシー侵害の損害賠償を求めた。EFF は政府を直接訴えるのではなく、政府に協力する企業を訴えることで、人々のプライバシーを守ろうと考えた。

しかし、この訴訟に政府が介入してきた。EFF が訴えたのは政府ではなく AT&T である。ところが、この訴訟で EFF が提出した資料が政府の機密に関わるとして、司法省が資料を非公開とするように求めてきたのである⁺⁺⁺⁺⁺。それに対し EFF は、資料を公開にすべきだと裁判所に求めた。

司法省が非公開を求めてきた資料には、AT&T の元従業員であるマーク・クライン (Mark Klein) の資料が含まれている⁺⁺⁺⁺⁺。クラインは自分が関わった業務について内部告発するとともに、いくつかの資料を持ち出していた。この資料は、連邦政府の連邦通信委員会 (FCC : Federal Communications Commission) でインターネット技術に関する上級アドバイザーを 2001 年 7 月から 2005 年 7 月まで務めた J・スコット・マーカス (J. Scott Marcus) によって支持され、説明が加えられている。

2006 年 5 月 15 日、政府は、今度は EFF の訴訟を棄却するように求める手続きをとった^{*****}。政府は、AT&T に対する訴訟は、「AT&T が法律を破ったかどうかについての法的な調査は国家機密を暴露し、国家安全保障を傷つけることになるため、AT&T に対する訴訟は、すぐに終了させられなければならない」と主張した。その主張は非公開とされたため、EFF も全文を読むことは認められなかった。EFF は、国家機密の下に隠してしまうことは不当だとこれに反発し

+++++ EFF, "EFF Motion in AT&T Surveillance Case Draws Government's Eye,"

<http://www.eff.org/news/archives/2006_03.php#004514> (March 31, 2006).

+++++ EFF, "EFF Files Evidence in Motion to Stop AT&T's Dragnet Surveillance,"

<http://www.eff.org/news/archives/2006_04.php#004538> (April 06, 2006). EFF, "Government Moves to Intervene in AT&T Surveillance Case,"

<http://www.eff.org/news/archives/2006_04.php#004613> (April 28, 2006).

***** EFF, "Government Files Secret Motion to Dismiss AT&T Surveillance Case"

<http://www.eff.org/news/archives/2006_05.php#004662> (May 15, 2006). EFF, "AT&T Wants Closed Courtroom in Tomorrow's Hearing in Surveillance Case,"

<http://www.eff.org/news/archives/2006_05.php#004671> (May 16, 2006). EFF, "Judge Denies AT&T Request to Discuss Closing Courtroom,"

<http://www.eff.org/news/archives/2006_05.php#004678> (May 16, 2006).

た。翌 16 日、AT&T もまた EFF に対して資料を公開せず、裁判を中止するように求めたが、EFF はこれを拒否した。

5 月 17 日、サンフランシスコの連邦地裁は、EFF が提出した資料を非公開にするかどうかを判断する審理を行った^{††††††††††}。ヴァーン・ウォーカー (Vaughn Walker) 判事は、EFF が資料を裁判において使うことは認めたが、しかし、当面公開することは認めなかった。そして判事は、AT&T は EFF と協力して EFF の資料から機密情報を削除し、公開できるようにするよう命じた。

AT&T は裁判所の命令に従い、EFF の資料が部分的に公開された^{††††††††††}。それによると、AT&T は NSA による傍受のために同社の設備内に秘密の安全な部屋をひとつ用意していた。明らかにされたクラインの証言によれば、その中で AT&T は、顧客の電子メールやその他のインターネット通信をまとめて大量に迂回させていた。令状やその他の法的監視もなく、光ファイバに直接アクセスさせていたのである。

6 月 23 日、この裁判の中止を求める政府の訴えに関して公判が開かれた^{§§§§§§§§§§}。ここで EFF は、AT&T に対する集団訴訟で「国家機密特権 (state secrets privilege)」を持ち出すことは認められるべきではないと主張した。これに対して司法省の弁護士は、NSA プログラムが仮に違法だったとしても、この裁判を進めることは国家機密をさらすことになるかと反論した。また、AT&T もこの訴訟は棄却されるべきだと主張した。

7 月 20 日、裁判所は、政府の主張を退け、訴訟を続ける判断を下した^{*****}。ウォーカー判事は、「自由と安全の間の妥協は難しいままである。しかし、この訴訟を最初の時点で棄却するということは、安全を何ら明確に促進することなく自由を犠牲にすることになるだろう」と述べて政府の訴えを退けた。この判断に対して EFF は、「これは、非合法監視を止めさせ、こうしたプライバシーの侵害に関して AT&T に説明責任を確保するために重要なステップである」としている。

7 月の決定を受けて、政府と AT&T は裁判の棄却を求めて控訴した。11 月 7 日、第九連邦控訴裁判所は、控訴を審議すると判断した^{††††††††††}。

^{††††††††††} EFF, "EFF Can Use Critical AT&T Documents in Surveillance Lawsuit," <http://www.eff.org/news/archives/2006_05.php#004681> (May 17, 2006).

^{††††††††††} EFF, "Key Portions of Critical Documents Unsealed in AT&T Surveillance Case," <http://www.eff.org/news/archives/2006_05.php#004697> (May 25, 2006).

^{§§§§§§§§§§} EFF, "EFF Battles Government's Motion to Dismiss AT&T Surveillance Case," <http://www.eff.org/news/archives/2006_06.php#004761> (June 23, 2006).

^{*****} EFF, "EFF's Spying Case Moves Forward - Judge Denies Government's Motion to Dismiss AT&T Case," <http://www.eff.org/news/archives/2006_07.php#004832> (July 20, 2006). EFF, "Judge's Refusal to Dismiss EFF's Spying Case Sets Stage for Congressional Showdown," <http://www.eff.org/news/archives/2006_07.php#004843> (July 21, 2006).

^{††††††††††} EFF, "Court Grants Appeal in AT&T Spying Case," <http://www.eff.org/news/archives/2006_11.php#004990> (November 7, 2006).

2007年1月現在、EFFによるAT&Tに対する集団訴訟は、その本題に入ることができていない。政府とAT&Tが裁判そのものの取り下げを求めているため、AT&Tが何をし、それが違法なのかどうかという審理には入れていない。

しかし、AT&Tが実際に違法行為に加担しているかどうかを問わず、こうした問題に民間企業が巻き込まれること自体がダメージであるといえるだろう。決着がつくまではAT&Tは無罪とはいえ、「違法な」通信傍受に加担していると疑われ続けることになる。少なくとも、AT&Tの態度は、違法かどうかを問わず、NSAに協力しているということを顧客に印象づけるには十分である。そのことにより、AT&Tが失うものは少なくないだろう。

4.3. 議会の対応

『ニューヨーク・タイムズ』のスクープは、議会の法案審議にも大きな影響を与えることになった。このスクープのタイミングは、2001年に成立したパトリオット法の延長・改正の審議に重なったからである。

パトリオット法とは、9.11直後の2001年10月26日に成立した法律で、議会上院で98対1、下院では357対66で可決されている。法案のねらいは米国の内外のテロリズムに対処するために法執行権限を拡大することであった。通信傍受もこの法律によって大幅に容易になった
*****。

同法のいくつかの項目はサンセット条項と呼ばれ、2005年12月末で失効することになっていた。その多くは通信傍受関連の項目である*****。ブッシュ政権はこうした条項が引き続きテロとの戦争には必要であるとして延長を求めた。こうしたタイミングで『ニューヨーク・

***** パトリオット法をめぐる議論については以下を参照。城所岩生「テロで様変わりの米国通信傍受法 [1] ~ [6]」『国際商事法務』第30巻11号~12号、第31巻1号~2号、同4号、同7号(2002~2003年)。Cynthia Brown, ed., *Lost Liberties: Ashcroft and the Assault on Personal Freedom*, New York: The New Press, 2003. Amitai Etzioni, *How Patriotic is the Patriot Act?: Freedom Versus Security in the Age of Terrorism*, New York: Routledge, 2004. Richard A. Posner, *Preventing Surprise Attacks: Intelligence Reform in the Wake of 9/11*, Lanham, MD: Rowman and Littlefield Publishers, 2005. Richard A. Posner, *Uncertain Shield: The U.S. Intelligence System in the Throes of Reform*, Lanham, MD: Rowman and Littlefield Publishers, 2006.

***** サンセットの対象となった項目には以下のものが含まれる。§201 (テロリズムに関する電話、口頭および電子通信を傍受する権限)、§202 (コンピュータ詐欺・悪用法違反行為に関する電話、口頭、電子通信を傍受する権限)、§206 (1978年外国インテリジェンス監視法に基づく追跡傍受の権限)、§207 (外国勢力の代理人である非米国市民のFISA監視期間)、§209 (令状に基づくボイスメール・メッセージの押収)、§212 (生命・身体を守るための電子通信の緊急開示)、§214 (FISAに基づくペン・レジスターおよびトラップ・アンド・トレース権限)、§215 (FISAの下での記録およびその他の物品へのアクセス)、§217 (コンピュータ侵入通信の傍受)、§218 (外国インテリジェンス・インフォメーション)、§220 (電子的な証拠のための捜索令状の全米規模サービス)。

タイムズ』のスcoop記事は発表されたため、議会の論議に影響を与えることになった。議会は延長問題に決着をつけることができず、失効期限を年明けの2006年2月3日まで延長することにした。しかし、年明けに再開された審議でもこの問題は決着がつかず、再び3月10日まで延長された。

議会上院は、2006年3月2日、パトリオット法の更新を認めた。下院も3月7日に更新を可決した。しかし、旧法をそのまま認めたわけではなく、ふたつの条項を恒久化から除外した。そのうちのひとつはFISAに基づく「追跡」監視 (§ 206) である。追跡監視が認められると、容疑者が固定電話、携帯電話、電子メール、PDA (Personal Digital Assistant : 携帯情報端末) などを使う場合、それぞれいちいち令状をとらなくて済むようになる。もうひとつはFISAの下でのビジネス記録の作成を要求する権限 (§ 215) である。このふたつの条項は4年で失効する。しかし、ブッシュ大統領は、法改正の署名の後の声明で、同法のいくつかの条項には従う気がないことを示唆した*****。

その後、前節で見たように、ギークたちの団体は司法の場でブッシュ政権の通信傍受を争うようになった。同時に、議会の共和党タカ派は、違法の疑いの強いこの令状なし通信傍受を明確に合法にするべく法案を提出した。

2006年9月13日、議会上院の司法委員会は、NSAによる通信傍受を可能にする三つの法案を可決した+++++。そのうちふたつは共和党議員が提出したもので、ブッシュ政権に有利になるものであり、もうひとつは民主党議員が提出したもので、ブッシュ政権の活動に法的な規制をかけながらも、手続きを簡素化しようとするものである。

第一の法案はS.2453 (National Security Surveillance Act of 2006 : 2006年国家安全保障監視法) で、3月16日にチャック・ヘーゲル (Chuck Hagel) 上院議員 (共和党 : ネブラスカ州) によって提出されている。しかし、実際に法案を書いたのは、ディック・チェイニー (Dick Cheney) 副大統領と司法委員会委員長のアーレン・スペクター (Arlen Specter) 上院議員 (共和党 : ペンシルベニア州) だといわれている。法案は提出されるとすぐに司法委員会に付託され、7月26日と8月2日に公聴会が開かれている。そして9月13日に10対8で委員会を通過し、上院本会議に回された。この法案は、すべての国際電話の会話や電子メールを検査し、米国民の会話の令状なしの監視をルール化し、家の物理的搜索をする権限を拡大するものである。

同じく3月16日にマイク・デワイン (Mike DeWine) 上院議員 (共和党 : オハイオ州) によって提出された第二の法案S.2455 (Terrorist Surveillance Act of 2006 : 2006年テロリスト監視法) もまた、同じ日に10対8で司法委員会を通過した。この法案は、米国内の人々を捜査する際の

***** White House, "President's Statement on H.R. 199, the 'USA PATRIOT Improvement and Reauthorization Act of 2005,'" <<http://www.whitehouse.gov/news/releases/2006/03/20060309-8.html>> March 9, 2006.

+++++ ACLU, "ACLU Slams Senate Judiciary Committee's Approval of NSA Spying Bills," <<http://www.aclu.org/safefree/nsaspying/26722prs20060913.html>> (September 13, 2006).

要件を下げるものである。

第三の法案は、ダイアン・ファインスタイン (Dianne Feinstein) 上院議員 (民主党：カリフォルニア州) が提出した S.3001 (Foreign Intelligence Surveillance Improvement and Enhancement Act of 2006 : 2006 年外国インテリジェンス監視改善・促進法) である。9 月 7 日に提出されたばかりで、すぐに 13 日に 10 対 8 で委員会を通過した。この法案は、米国民を傍受する際には議会の決める手続きを踏まなければいけないとするものだが、FISA の令状取得を簡素化する。

下院でも同様に法案の審議が行われた^{*****}。下院では、ヘザー・ウィルソン (Heather Wilson) 下院議員 (共和党：ニューメキシコ州) が提出した H.R.5825 (Electronic Surveillance Modernization Act : 電子監視現代化法) が審議された。この法案は大統領に大幅な権限を与え、NSA が行う令状なし監視プログラムを承認するものである。2006 年 7 月 18 日に提出された法案は、9 月 20 日に下院司法委員会を通過した。しかし、インテリジェンスに関する常設特別委員会で修正され、さまざまな議論がなされた後、11 月 13 日に再び司法委員会に戻された。

上院の三つの法案と下院の法案が議会上院に回された後、11 月に米国の中間選挙が行われた。ここでブッシュ大統領の共和党は民主党に敗れることになった。下院では民主党が上回り、主導権を握った。上院でも僅差で民主党が上回った。11 月の中間選挙が終わってから 12 月のクリスマスまで、いわゆる「レームダック (lame duck) 議会 (落選した議員などが残り、法案や決議案などの議題もなく単に日程を消化するだけの議会)」が開かれたが、この間、三つの法案は可決されることなく終わった。

2007 年 1 月 17 日、ブッシュ政権は、突然、令状なし通信傍受をやめ、今後は FISC から令状をとって傍受を行うという声明を、司法省を通じて発表した。司法省は、FISC と協議し、「必要なスピードと機動性」を提供することに合意したという。

こうした転換の背景には、新しい議会が開会し、民主党主導の議会がこの問題について調査を行うと声明していたことがある。特に 18 日には司法長官のアルバート・ゴンザレス (Alberto R. Gonzales) が乗員の司法委員会でこのプログラムに関して議員たちから質問を受けることになっていた。引き続いて行われている訴訟を意味のないものにしようという意図もあったと報じられている^{*****}。

***** ACLU, "ACLU Slams House Panels' Approval of Wilson NSA Spying Bill, Says Measure Undermines Constitution, Condone Abuse of Power,"

<<http://www.aclu.org/safefree/nsaspying/26802prs20060920.html>> (September 20, 2006).

***** Eric Lichtblau and Dabid Johnston, "Court to Oversee U.S. Wiretapping in Terror Cases," *New York Times* <<http://www.nytimes.com/2007/01/18/washington/18intel.html>> January 18, 2007.

Dan Eggen, "Court Will Oversee Wiretap Program: Change Does Not Settle Qualms About Privacy," *Washington Post*

<<http://www.washingtonpost.com/wp-dyn/content/article/2007/01/17/AR2007011701256.html>> January 18, 2007.

5. 通信の秘密と安全保障

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なし通信傍受は、それを如実に示したものだといえるだろう。

本来、行政の行き過ぎを止めるのは司法と立法の役割である。EFF や ACLU は司法の場でブッシュ政権の活動に歯止めをかけようとしている。しかし、立法府はむしろブッシュ政権の活動を認める方向での立法化の動きを示している。立法府が国民の世論を代弁しているとするならば、それは米国民が求めていることかもしれない。

日本国憲法には通信の秘密が明記されている。日本では行政傍受は行われず、司法傍受がわずかに行われているだけである。しかし、この問題は対岸の火事ではない。第一に、本文中で述べたように、通信トラフィックの多くは米国を経由している。日本の ISP の顧客が送受信するメッセージの多くも NSA によって傍受されている。国際的な通信の問題とはいえ、通信の秘密が確保されず、顧客のプライバシーが守られていないという現実には通信事業者は直面している。これまでのベスト・エフォートのインターネットではこうした事態は技術的に避けられなかった。しかし、NTT をはじめ世界中の通信事業者が取り組み始めた NGN (Next Generation Network) において、プライバシーはどう確保されるのだろうか。

第二に、日本がテロの脅威に直接さらされた場合、あるいは米国政府から日本政府に対して日米同盟の点から協力が求められた場合、日本の通信事業者はこれに対応する準備ができていだろうか。「すべて法的な手続きに従うだけ」だと突っぱねることができるだろうか。AT&T に対する集団訴訟の結果はまだ出ていないが、こうしたダメージ・コントロールにも備えておかななくてはならない。

通信傍受は万能ではないし、望ましい技術でもないだろう。しかし、命の危機に直面したとき、通信の秘密はどこまで厳格に守られるべきだろうか。そのバランスを探る考察を始めておく必要があるだろう。

参考文献

- Cynthia Brown, ed., *Lost Liberties: Ashcroft and the Assault on Personal Freedom*, New York: The New Press, 2003.
- Amitai Etzioni, *How Patriotic is the Patriot Act?: Freedom Versus Security in the Age of Terrorism*, New York: Routledge, 2004.

- Richard A. Posner, *Preventing Surprise Attacks: Intelligence Reform in the Wake of 9/11*, Lanham, MD: Rowman and Littlefield Publishers, 2005.
- Richard A. Posner, *Uncertain Shield: The U.S. Intelligence System in the Throes of Reform*, Lanham, MD: Rowman and Littlefield Publishers, 2006.
- James Risen and Eric Lichtblau, " Bush Lets U.S. Spy on Callers Without Courts," New York Times, December 16, 2005 <<http://www.nytimes.com/2005/12/16/politics/16program.html>>.
- James Risen, *State of War: The Secret History of the CIA and the Bush Administration*, New York: Free Press, 2006.
- 大森義夫『日本のインテリジェンス機関』文春新書、2005年。
- 岡崎久彦『日本外交の情報戦略』PHP新書、2003年。
- ロバート・オハロー（中谷和男訳）『プロファイリング・ビジネス—米国「諜報産業」の最強戦略—』日経BP社、2005年。
- 北岡元『インテリジェンスの歴史—水晶玉を覗こうとする者たち—』慶應義塾大学出版会、2006年。
- 城所岩生「テロで様変わりの米国通信傍受法 [1] ～ [6]」『国際商事法務』第30巻11号～12号、第31巻1号～2号、同4号、同7号（2002～2003年）。
- 木村忠正、土屋大洋『ネットワーク時代の合意形成』NTT出版、1998年。
- リチャード・クラーク（楡井浩一訳）『爆弾証言—すべての敵に向かって—』徳間書店、2004年。
- 小谷賢『イギリスの情報外交—インテリジェンスとは何か—』PHP新書、2004年。
- 斎藤彰『CIA』講談社現代新書、1985年。
- 産経新聞特別取材班『エシユロン—アメリカの世界支配と情報戦略—』角川書店、2001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『ネット・ポリティックス—9.11以降の世界の情報戦略—』岩波書店、2003年。
- 仲本秀四郎「情報を考える」公文俊平編『リーディングズ 情報社会』NTT出版、2003年。
- ロバート・ベア（佐々田雅子訳）『CIAは何をしていた？』新潮社、2003年。
- デイヴィッド・ライアン（河村一郎訳）『監視社会』青土社、2002年。
- F・W・ラストマン（朝倉和子訳）『CIA株式会社』毎日新聞社、2003年。