第三章　スチューピッド・ネットワーク時代における通信傍受
――米国における法的枠組みと技術

土屋　大洋

１．対米同時多発テロと通信傍受

2001年の対米同時多発テロ（9.11）が、インテリジェンス・コミュニティの活動に大きく影響を与える事件であったことはいうまでもない。そして、その影響はインテリジェンス・コミュニティの主要な情報収集方法の一つである通信傍受にも及んでいる。というのは、テロリストたちがインターネットを使って連絡を取り合い、計画を練っていたことが明らかになり、インターネットのような新しいネットワークの通信傍受が重要な課題として広く認知されることになったからである。

テロリストたちは、アラビア語を使い、電話とは違って特定のデバイスや通信経路に依存しないインターネットを使った。さらに、公共図書館やキンコーズ（米国の事務サービス・チェーンの一つ）、ホテルのような公共の場所からインターネットにアクセスすることでアクセスそのものの証拠を残りにくくしている。膨大な情報の海に企みを沈めることで、米国のインテリジェンス・コミュニティの網をすりぬけた。無論、FBI（連邦捜査局）のローリー・メモやフェニックス・メモなどが明らかにしたように、その兆候はあったが、事前の警戒を十分に高めるに至るような情報をインテリジェンス・コミュニティに与えなかった。

いったいなぜ米国のインテリジェンス・コミュニティは、有用なインテリジェンスを精製することができなかったのだろうか。その一つの答えは、「ネットワークがスチューピッド（まぬけ）になったから」ではないだろうか。

本稿は、9.11が浮き彫りにした近年の通信傍受が抱える問題点について検討しようとするものである。ここでは、通信の世界における大きな変化を、「ネットワークのスチューピッド化」という視点から捉えなおし、特にインターネットに焦点を置いた通信傍受について考察することにしたい。

２．スチューピッド・ネットワークの台頭

（１）ネットワークの変化

現在、通信の世界で起きている変化は、デービッド・アイゼンバーグ（David Isenberg）によれば、「インテリジェント・ネットワーク（intelligent network）」から「スチューピッ

ド・ネットワーク（stupid network）」への移行である[1]。アイゼンバーグによると、伝統的な電話会社は、以下のような四つの仮定の上でインテリジェント（知的）なネットワークを構築してきた。

・高級なサービスの提供のために高価で稀少なインフラ設備が共有される
・音声がトラフィックの大部分を占めている
・回線交換による通話こそが重要な通信技術である
・電話会社がネットワークをコントロールする

しかし、これらがすべて崩れ去り始めているという。

・インフラ設備コストは過去20年間に最大数千分の１に低減している
・データ・トラフィックが音声トラフィックを抜きつつあり、多くの異なるタイプのデータが電話ネットワークを経由するようになっている
・イーサーネットなど多くの異なるタイプの通信技術が登場してきている
・通信のコントロールがエンドユーザに移っている

電話の時代には、一台数億円から十億円もするといわれた交換機が電話のネットワークの各所におかれ、ネットワークはピラミッド状に積み上げられ、全国網、国際網に接続された。国営電話会社が「ユニバーサル・サービス」義務を負わされ、全国一律料金を維持しながら、全国に電話網を普及させていった。日本では電電公社が電話加入者に7万円以上の加入権を買わせ、その加入権収入を新規投資に回すことで電話網を拡大させてきた。やがて全国網がほぼできあがると、交換機とネットワークを更新することで付加価値サービス（例えばキャッチホン）を提供していくことになった。

しかし、インターネットで使われるデータ中継機であるルーター（router）は、高いものでも数千万円、安いものなら数十万円である。電話交換機のようにすべて同じ仕様でないと接続できないというわけではなく、インターネット・プロトコル（IP）に対応している限りはすべて接続が可能である。ネットワークにコンピュータを接続するには、接続するコンピュータにIPアドレスと呼ばれる住所番号を割り当て、その割り当て表をドメイン・ネーム・サーバー（DNS）に書き込むだけでいい。ネットワーク上に数多くあるDNSは相互に割り当て表を参照しながら情報を交換し、最大48時間程度で新しいコンピュータが

ネットワークに認知されるようになる。つまり、電話会社が神経をとがらせながら管理する高価な交換機の時代は終わり、ユーザーが勝手に接続する格安のコンピュータがネットワークを構成するようになっている。

データの種類を見ると、すでに先進国ではデジタル・データのトラフィックが音声トラフィックを追い抜いてしまっている。通信と言えばアナログの電話だった時代は終わり、音声さえもデジタル化するデジタル・データ通信の時代になっている。デジタル・データはすべて0か1かのデジタル信号で表現されるが、それがソフトウェアで再生され、音声になったり、画像になったり、動画になったり、文字になったりする。

通信技術という点でも、回線交換のような無駄なネットワークの使い方はしない。電話網は、誰も話す人がいなければ使われないだけである。しかし、同じ電話線でもADSL（非対称加入者線）技術は電話線の使っていない帯域（band-width）を使ってデジタル・データの送信を可能にしている。回線交換では誰か他の人がそのネットワークを使っていれば別の人は使うことができなかったが、LAN（ローカル・エリア・ネットワーク）で使われるイーサーネットのケーブルでは、パケット化されたデータが細切れに送られ、ネットワークが混雑している時でも、混雑しているなりにデータを運ぶ。光ファイバーでは信号は電子でなく光に置き換えられ、高速でやりとりされている。いわゆるブロードバンドとは、一本で通信可能なデータ量を拡大させたネットワークで、ADSLならば20Mbps、光ファイバー1本ならば1Gbps（1000Mbps）程度のデータを送ることが可能になっている（普通は髪の毛ほどのファイバーを束ねて使うため、光ファイバーのケーブルで運べる容量はさらに大きくなる）。

そして、最大の変化は、ネットワークのコントロール権がユーザー側に移ったことである。電話のネットワークは、インテリジェントな交換機がネットワークの中にあって、ネットワーク自体の性能をコントロールしている。回した電話番号が正確に相手先につながるためには、エラーがあってはならない。電話会社は完璧なサービスを提供するために交換機とネットワークを改良し、すべて管理しようとしてきた。ネットワーク自体をインテリジェントに保つことでサービスの高度化を図ってきたのである。

ところが、インターネットのようなネットワークでは、ネットワーク自体をできるだけスチューピッドにしようとする。インターネットは「ネットワークのネットワーク」といわれるが、ネットワークを相互に接続していくためにはできるだけルールを緩やかで柔軟にしておかなくてはならない。そこで最低限IPを理解することが条件とされ、100%の完璧さを求めないことにした。その結果、「ベスト・エフォート」という「だいたいはつながる

が、その保証はしない」という考え方が支持されるようになった。

インテリジェントになるべきは、ネットワークではなく端末（エンド）である。電話のネットワークではネットワークの末端に位置するユーザーが通信を行うには、電話会社とそのネットワークというインテリジェントな存在に対価を払うことでサービスを享受してきた。しかし、インターネットではエンドの利用者同士が直接やりとりする。ユーザーがインテリジェントなパソコンとソフトウェアを使って電子メールを作成し、宛先を付けてネットワークに放り込む。ネットワークにはただそのアドレスにより近い、隣のルーターにデータを渡すことしかできない、スチューピッドなルーターがいるだけである。

電話のネットワークでは誰でも使える黒電話というスチューピッドなエンドと、交換機で複雑に接続されたインテリジェントなネットワークで通信を成り立たせてきた。しかし、インテリジェントなネットワークは故障に弱い。ツリー型のネットワークの重要な結節点で故障が起これば、広範な地域で通信ができなくなる可能性が高い。それに対して、インターネットはそもそも完璧さを求めていない。ネットワークにつながる端末が故障した程度では通信には影響が出ない。ルーターが故障しても別のルートをパケットは通って目的地へ着くだけである[2]。電話のような同期通信には不向きだが（しかし、IPネットワーク上で同期通信を可能にするVoIP［ボイス・オーバーIP］技術も普及してきている）、「とにかくデジタル化されたメッセージが相手へ到着すればいい」という点では、インターネットはすぐれた耐故障性を持っている。さらに、それをグローバルな規模で、格安で行えるところが大きな利点である。

（2）困難になる通信傍受

しかし、通信傍受という点では、スチューピッド・ネットワークの台頭は大きな脅威となる。第一に、相手が同時に受話器を持って話さなくてはならない「同期型」の電話ではなく、相手がいつメッセージを受信するか分からない「非同期型」のインターネットが使われるようになったことで、通信に関わる人物の特定が難しくなった。電話を使って二者が話をしていれば、当事者が誰かを特定することは比較的簡単である。しかし、インターネットではメッセージの受取人が誰なのか分かりにくい。インターネット上を流れる電子メールが届く先の相手が本当に犯罪やテロの協力者であるかどうかを特定するのは困難である。極端な話をすれば、不特定多数が参加するメーリング・リストのメッセージの中に秘密のメッセージを潜り込ませたり、ウイルスに見せかけて送信されたメッセージに暗号を隠すことも可能である。

第二に、ネットワークの管理者があいまいになってきている。電話のネットワークは電話会社の完全な管理下にあった。国際電話の場合では市内通信網－長距離通信網－国際通信網などをつなぎ、それぞれには明確な管理者がいたために通信傍受も通信事業者の協力が得られれば実に簡単に行うことができた。しかし、インターネットになるとこうした形での管理は行われていない。個々のネットワークの所有者はいるとしても、どんなメッセージがそのネットワークを流れるかについて所有者はほとんど関知しない。回線交換のように一本につながった通話回線が一時的に確保されるわけではなく、メッセージはバラバラのパケットに分割されてネットワークに流される。すべてのパケットが別々のルートを通って目的地に着くことも理論上はありえる。仮に通信事業者の協力が得られても、目的のメッセージを100%捕捉できるかどうかは分からない。

第三に、情報技術の発達によってユーザー自らが、通信手段とメッセージを選べるようになってきている。電話口でいくらひそひそ話をしても意味はないが、電子メールの文章の暗号化（クリプトグラフィー）や画像にメッセージを埋め込む暗号化（ステガノグラフィー）といった技術を使えばメッセージの機密性を簡単に上げることができる。これがインテリジェンス・コミュニティには脅威となりつつある。テロリストや犯罪者たちがインターネット上で暗号通信を行う危険性については、クリントン政権が成立した1993年頃から2000年まで政治問題となった。クリントン政権はNSA（国家安全保障局）の意向を汲んで、政府が復号可能なクリッパー・チップと呼ばれる半導体チップの導入や、暗号製品の輸出規制を行おうとした。結局この規制は後にほとんど撤廃されることになるが、ユーザーがプライバシー保護のために情報管理を自ら行うようになればなるほど、インテリジェンス・コミュニティの通信傍受活動には支障をきたすことになるだろう。

第四に、ネットワークの要素技術そのものが、通信傍受になじまないものになりつつある。後述するように、これまで使われてきた銅線のネットワークは微弱な電磁波を発するために、それを捕捉することで容易にメッセージを復元できた。しかし、通信需要の増大に応えるために登場してきた光ファイバーは、そうした電磁波を出さないために、外部からメッセージを捕捉することがきわめて困難になっている。

こうした変化が実際にどのような問題を引き起こしているかを検討する前に、次節では簡単に米国の通信傍受の法的枠組みを振り返っておこう。

３．米国における通信傍受の法的枠組み

（１）通信の秘密

米国で通信傍受が注目を浴びたのは、アル・カポネ（Alfonso Capone）に対する捜査の過程である。1919年に米国憲法修正第18条によって禁酒法が作られた[3]。しかし、密造酒の製造は後を絶たなかった。密造で莫大な利益をあげていたマフィアの大物アル・カポネを捕まえるために、捜査当局は電話の傍受を行ったのである。

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「表現の自由」、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とされている。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[4]。

「通信傍受」と一言でいっても、いわゆる「盗聴」と同一視することはできない。「合法的な通信傍受」がある一方で、「非合法的な通信傍受（盗聴）」もある[5]。米国の法体系の中で合法的通信傍受と呼ばれるものには、犯罪捜査のためのものと、対外的な国家安全保障あるいはインテリジェンスのためのものとがある。国内の犯罪捜査については、米国法Title 18で「犯罪と刑事手続き」が規定されており、その中のChapter 119（Wire and Electronic Communications Interception and Interception of Oral Communications）とChapter 121（Stored Wire and Electronic Communications and Transactional Records Access）が関係している。対外インテリジェンスは、米国法Title 50「戦争と国防」のChapter 36（Foreign Intelligence Surveillance）において規定されている。

米国での合法的通信傍受には、四つの種類の法的な行動がある。第一に、傍受命令（interception order）である。これは裁判所が通信傍受を許可するものである。第二に、捜査令状（search warrant）である。これは物理的な建物や、帳簿のような有形のものの押収を許可するものである。第三に、「ペン・レジスター（pen register)」と「トラップ・アンド・トレース・デバイス（trap-and-trace device)」命令と呼ばれるもので、特定の通信デバイスがかけた電話番号、それにかかってきた電話番号の収集を認めるものである（通信内容の傍受はできない)。第四に、召喚令状（subpoena）で、これは記録のような有形のものの作成を求めることである。例えば、電磁的に記録されているサーバーの通信記録を印刷するなどして証拠にするのである。これらを使って捜査当局やインテリジェンス機関は通信傍受を行う。

まず、国内向けの通信傍受関連の法規として注目されるのは、1968年に成立した「通信傍受法（Wiretap Act)」である。通信傍受法では、(1）捜査機関が行う通信傍受に際して判事から傍受命令を取る必要があること、(2）命令を取る際には「信じるに足りる相当な理由（probable cause)」を判事に示さなくてはいけないこと、を規定した。しかしこれは事実上なし崩しになっている。つまり、ほとんどの通信傍受申請が受理され、判事が疑義を示して差し戻すことはまれだといわれている。

次に注目すべきは、1986年の「ECPA（Electronic Communications Privacy Act)」である。これは1968年の通信傍受法を修正し、電子通信にも拡大したもので、当時出てきていたパソコン通信に対応した。パソコン通信の掲示板などで児童ポルノが頒布されるという問題があり、電子メールの内容やパソコン通信会社などのログ（記録）を捜査対象とするためにこの法律が作られた。やはりこの場合も「信じるに足りる相当な理由」を示すことが必要である。

クリントン政権時代の1994年に成立した「CALEA（Communications Assistance for Law Enforcement Act)」は現在でも頻繁に議論の対象となる法律である。これは、捜査目的のための通信傍受における通信事業者の義務を明確化したものである。通信事業者は捜査当局から要求があった場合にはその要求に応じなくてはならない。そして、通信傍受を可能にする機器を通信事業者の設備の中に設置しなくてはならなくなった。そのための技術標準はFCC（連邦通信委員会）で設定されることになっている。

CALEAが注目されるのは、クリントン政権が情報スーパーハイウェー構想やNII（国家情報基盤）構想によって新しいデータ通信ネットワークを奨励した一方で、そうした新しい通信技術に対応する法的枠組みを用意したという点である。かつての単純な電話ネットワークの時代には捜査当局でも簡単に通信傍受を行うことができたが、新しいネットワーク技術に対応するためには通信事業者の協力が不可欠になってきたのである。

そして、対外インテリジェンスにおいて最も重要なのはFISA（Foreign Intelligence Surveillance Act）である。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。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。FISAの傍受命令申請やその妥当性の審査は非公開で行われているので、それが濫用されているのではないかという懸念が常につきまとっている。

（2）USAパトリオット法の成立

上述のような法律は、それぞれの時代の技術的な変化に対応しながらも、捜査当局による通信傍受の濫用を防ぐために司法によるチェックを課し、歯止めをかけようとするものであった。しかし、9.11の被害の大きさは、その枠組みの根本的見直しを迫ることになった。9.11後、さまざまなテロ対策法が連邦議会に提出されたが、最終的にその中から「USA法」と「パトリオット法」を合体させる形で成立したのが「USAパトリオット法（Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism）」である。この法律は、国内の犯罪捜査も、対外インテリジェンスも対象とし、それらを大幅に書き換え、緩和している。法律自体は通信傍受だけを扱っているものではなく、テロ防止を念頭に置いた包括的なものだが、特に通信傍受の緩和という点で大きな変化をもたらした[6]。

この法律成立以前は、捜査当局は傍受の対象とする電話一つ一つについて傍受申請をしていたが、USAパトリオット法は、対象者が使っている電話であれば、携帯・固定に限らず、すべて傍受できるようにした。また、電子メールの内容についてインターネット・サービス・プロバイダー（ISP）に記録を求めることができるようになった。通信事業者の協力はCALEAによっても決められていたが、USAパトリオット法では記録を一定期間必ず保存することが求められ、その内容にFBIを主とするインテリジェンス・コミュニティがアクセスできることになった。

この法律は4年間で失効するものとされている。時限の付与については審議時にかなり問題になり、ブッシュ政権側は永続的なものにしようとしていたが、一部上院議員や、インターネット・コミュニティ、プライバシー団体の強い反対があった。反対派は2年間にすべきだと主張したため、妥協案として4年間の時限付きとなった。

しかし、この法律の中には4年たっても失効しない条項がいくつかある。そのうちの第216節では、各州の検事総長がカーニボー（Carnivore）と呼ばれる通信傍受のための装置の設置を命令することができるとなっている。ここで検事総長が命令できるという点が非常に重要である。つまり、以前は司法府の裁判所へ行って申請することが必要だったが、同じ行政府の中で検事総長や連邦検事が命令を出せるようになった。これは大幅な緩和だといえるだろう。

USAパトリオット法によるこうした通信傍受規制の緩和は、9.11が米国社会に与えた精神的ダメージの大きさを物語っていると同時に、ある意味でインテリジェンスの失敗を取り戻そうとするインテリジェンス・コミュニティの並々ならぬ意欲のあらわれであるとも

いえるだろう。しかし、はたしてこうした規制緩和によって十分な情報が本当に取れるようになるのだろうか。次節では、通信傍受の技術的変化について検討する。

４．通信傍受の技術の変化

（１）非合法的通信傍受と合法的通信傍受の相違

通信傍受は実際どのような形で行われているのだろうか（図1参照）。非合法的な通信傍受を行う盗聴者にとって一番簡単なのは、例えば、コードレス電話や携帯電話の無線を傍受することである。現在の携帯電話は、かつてのアナログ無線のように丸裸の信号を送受信しているわけではなく、特定の通信形式を用いて簡単な暗号化を行っているので、ラジオの受信機で周波数を合わせればそのまま聞こえるという性質のものではない。しかし、通信標準そのものは機密ではないために、対応する機器を用意することができれば、その内容を聞くことも不可能ではない。あるいは、室内の会話を聞くために、屋内にマイク兼発信機を設置してその電波を傍受するということも行われている。

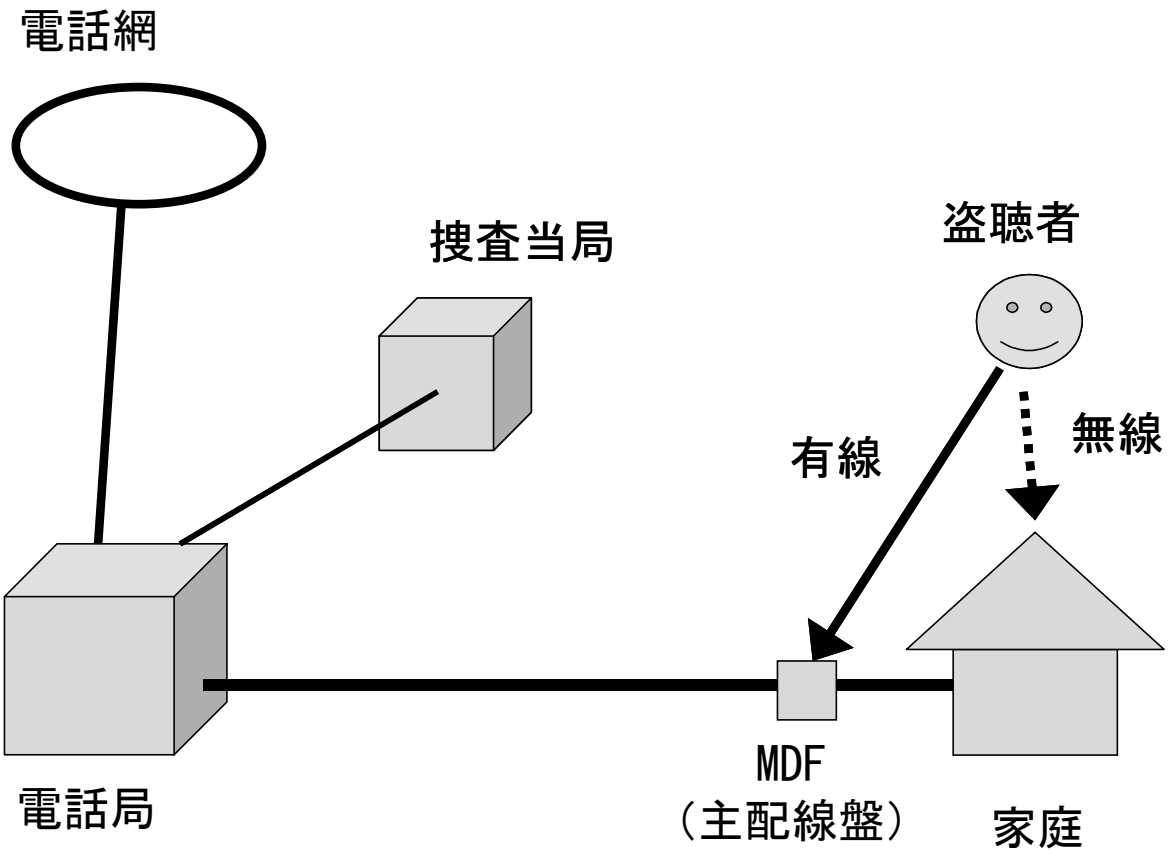

図1　電話の傍受

もう一つは、有線ネットワークにアクセスする方法である。電話線であれば、各家庭の

配線をひとまとめにした配線盤が電柱の上や建物の壁に置かれている。そこに対応する機器を接続することができれば簡単に通信内容を聞くことができる。例えば、家庭の電話が故障したときに電話会社に修理を依頼すると、担当者が来て配電盤を開け、電極を差し込むとそのまま通信内容を聞くことができるのと同じである。しかし、その配電盤にどうやってアクセスするかということが課題として残る。物理的にこじ開け、アクセスすることは可能だが、いずれそれは証拠が露呈することを意味するため、スマートなやり方とはいえない。

このやり方を実際に使ったのが、1986年の緒方靖夫・共産党国際部長宅を警察が盗聴した事件である。これは正式な手続きを踏んだ捜査ではなく、当時は通信傍受法も成立していなかったので、違法に行われたといえるだろう。このケースでは、警察官たちが緒方部長の自宅から100m離れたところにアパートを借り、緒方部長宅の電話線から自分たちのところまで別の線を引いて会話を録音していた。

しかし、実際の「合法的な」通信傍受は、電話会社と電話局の協力を得て特定の人の通話を記録している。携帯電話を傍受する必要があるときには基地局から傍受したり、有線電話の場合は電話局に直接繋いで傍受したりしている。したがって、合法的な通信傍受の枠組みでは、傍受されている側がその事実に技術的に気づくのは難しいということになる。

（2）インターネットの通信傍受

インターネットでの通信傍受はどのように行われているのだろうか。一つの方法は、ワールド・ワイド・ウェブ（WWW）の中をソフトウェアのロボットに巡回させ、疑わしい情報があったらコピーし、記録するというものである。しかし、これはGoogleやAlta Vistaのような検索エンジンと同じことをやっているに過ぎず、際だった効果が上がるわけではない。例えば、リンクが一切張られていないサイトにはソフトウェア・ロボットはたどりつくことができない。また、WWW自体が猛烈なスピードで自己増殖しているために、ロボットの活動が追いつかない。1999年の段階では、GoogleやAlta Vistaなどの検索エンジンがカバーする領域は、ウェブのおよそ40%にすぎないという調査結果が出ている[7]。つまり、WWWに限っても、インターネット上のあらゆる情報を蓄積するのは不可能なままであり、コンテンツが常に変化し続けていることを考えれば、WWWから情報を引き出すのは困難であるといえるだろう。

インターネットでの通信傍受の二つ目の方法として、目的のターゲットのところに行き、その通信を傍受することがある（図2参照）。ターゲットが家庭からダイヤルアップで電話

局に接続し、そこからISP（インターネット・サービス・プロバイダー）に接続している場合には、電話局やISPの協力を得ていれば簡単であろう。USAパトリオット法その他を用いて通信傍受装置をISPに付けることも可能であり、ISPはその義務を負わされている。あるいは、ダイヤルアップではなく、光ファイバーなどでIPネットワークに接続されている場合でもISPから情報を取ることができる。この方法は、ターゲットが明確に分かっている場合には非常に有効である。

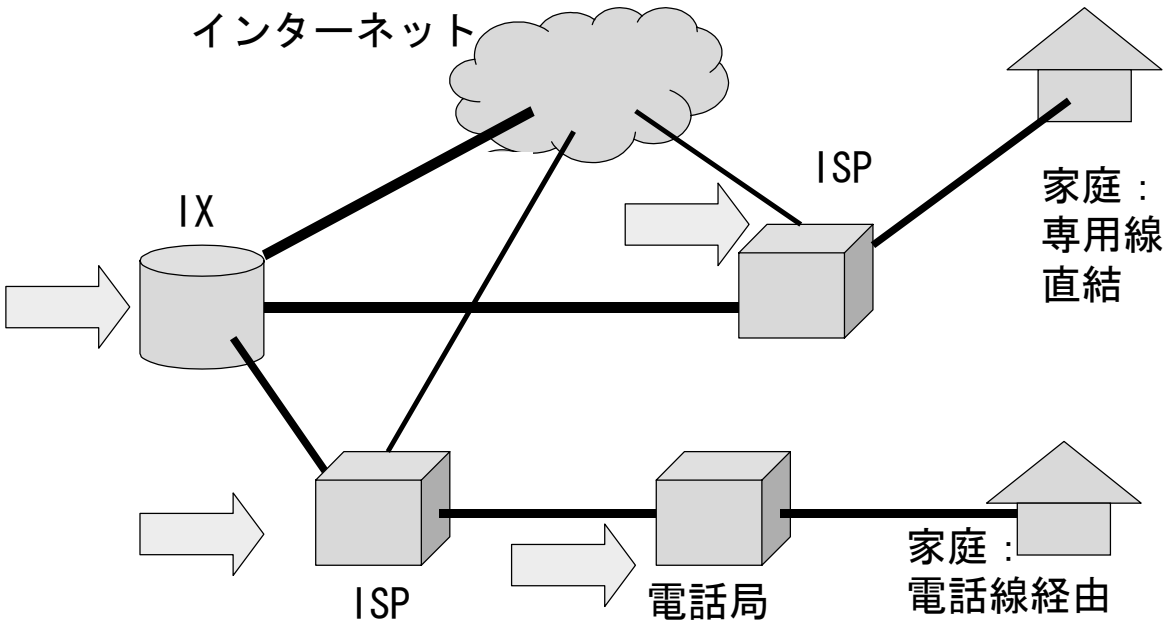

図２　インターネットの傍受

インターネット通信を捕捉するもう一つの可能性は、IX（インターネット・エクスチェンジ）である。「ネットワークのネットワーク」の結節点となるのがIXで、そこにはISPやインターネットの基幹網を持つバックボーン・プロバイダーのネットワークなどが集中している。IXが扱うトラフィック量は膨大になるために、そこから該当する情報を抜き出すのは簡単ではない。

しかし、まったく不可能というわけではない。インターネットを通るすべてのパケットには、少なくとも「受取人」を示すIPアドレスがついている。同時に、通常は「差出人」が使っているコンピュータなどの端末のIPアドレスも書かれている。実際には人間一人一人とIPアドレスが一対一で対応しているわけではないから、仮にIPアドレスが分かったとしても、即容疑者の特定につながるわけではない。しかし、誰がそのIPアドレスを持つ端末にアクセス可能であったかを特定することはできる。9.11のテロリストたちは、自分のパ

ソコンは使わず、公共図書館やインターネット・カフェなどのパソコンを使った。それは不特定多数の人が使うパソコンのほうが彼らにとっては安全だったからである。FBIはテロリストたちの電子メールを割り出すと同時に、すぐに彼らが使っていた公共図書館やインターネット・カフェ、ホテル、事務サービス・チェーンの端末を割り出し、捜査に向かっている。

しかし、ある程度の技術を学べば、そうした発信記録を削除したり、改ざんしたりすることができる。例えば、スパムと呼ばれる未承諾広告メールの多くが虚偽の発信アドレスを使っている。仮に発信者のアドレスが不正であったり、削除されていたとしても、そのパケットが通過したサーバーにログ（記録）が残っていれば、それを逆にたどって差出人にたどりつくことができる可能性も、わずかながら残されている。

FBIのサイトでは前述のカーニボーの仕組みが説明されている（図3参照）。これは、通信ネットワークの中にウィンドウズのパソコンを改良したデバイス装置を入れると、データの中から特定のキーワードなどに合致するものをフィルタリングし、引っ掛かったものを記録するという仕組みである。

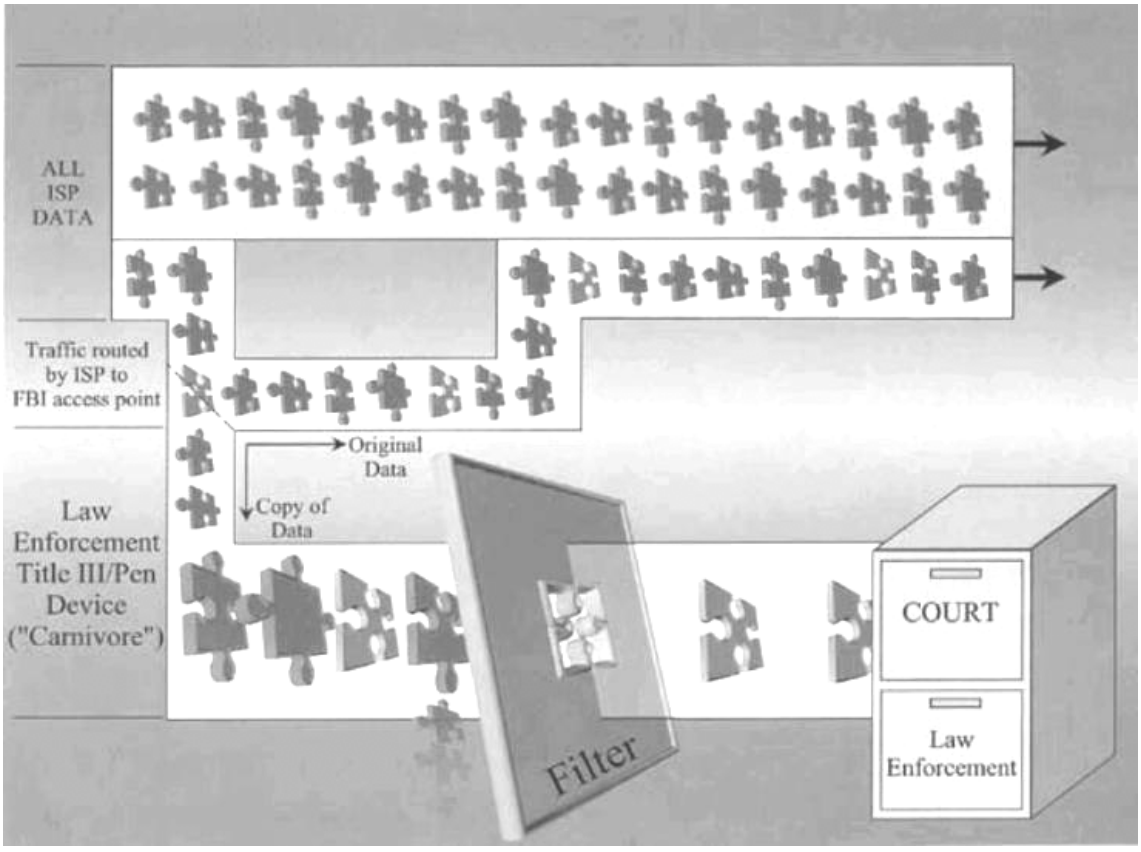

図３　カーニボーの仕組み

出所：http://www.fbi.gov/

しかし、その実行性には疑問の声もある。実際に9.11に関連する通信傍受を行ったときにもカーニボーが設置されていたが、関係ない市民の通信まで多数捕捉してしまっていたために、FBI担当者はそれを全部削除してしまったことがある[8]。もしそのときに適切な措置が取られていたり、「他の一般市民のものもあるが、仕方がない」と記録が残されていたりしたら、捜査の展開は違ったものになったかもしれない。同時に、カーニボーが現実にプライバシーの懸念を引き起こすデバイスであることもこの事件は示している。

いずれにせよ、通信傍受のターゲットがはっきりしている場合には比較的簡単だが、そうでない場合には通信傍受はますます難しくなってきている。インターネットを流れる膨大な情報の中から目的のものを探し出すのは至難のわざとなるだろう。

さらに、インターネットの通信傍受で問題になるのが、個人の暗号利用の増加である。暗号はこれまでは政府機関やインテリジェンス・コミュニティにユーザーが限定されていたが、インターネットは暗号を汎用技術にしてしまった。例えば、ネットスケープ・ナビゲーターやインターネット・エクスプローラーのようなブラウザーにも暗号技術が組み込まれており、電子商取引の基盤技術となっている。

加えて、電子メールや保存ファイルの暗号化ツールも一般に市販されるようになってきているため、犯罪者やテロリストの情報にもアクセスするのが困難になってきている。暗号の是非に関しては1990年代に激しい論争が行われた。PGP（Pretty Good Privacy）という個人向け暗号を開発したフィル・ジマーマン（Philip Zimmermann）は、1980年代、レーガン政権でミサイル構想が出てきたときに、「これでは我々は死んでしまう」という懸念から平和運動に身を投じ、その平和運動に寄付をしてくれる人たちのリストを守るために暗号技術開発を始めた。彼は、インテリジェンスの意義を認めながらも、人々は最低限のプライバシーを守るために暗号技術利用の自由を持つべきだと主張している[9]。

クリントン政権時代、米国の暗号通信を担うNSA（国家安全保障局）が強い暗号規制を求めたが、現在では表だった主張は行われていない。おそらくは、法的に暗号を押さえ込むよりも、技術的な暗号解読能力の向上に努めるという選択をしたのではないかと思われる。NSAの国家暗号学博物館（National Cryptologic Museum）では、すでに引退した暗号解読のためのコンピュータが展示されている。2000年まで使われていたという「ZIEGLER」の回路基盤は、メモリが32ギガ、ハードディスクが142ギガで、8個の並列プロセッサを使っていた（図4参照）。現在のコンピュータと比較しても非常に高い能力を持つコンピュータである。こうした高性能のコンピュータを導入することで暗号の普及に対応しようということではないだろうか。

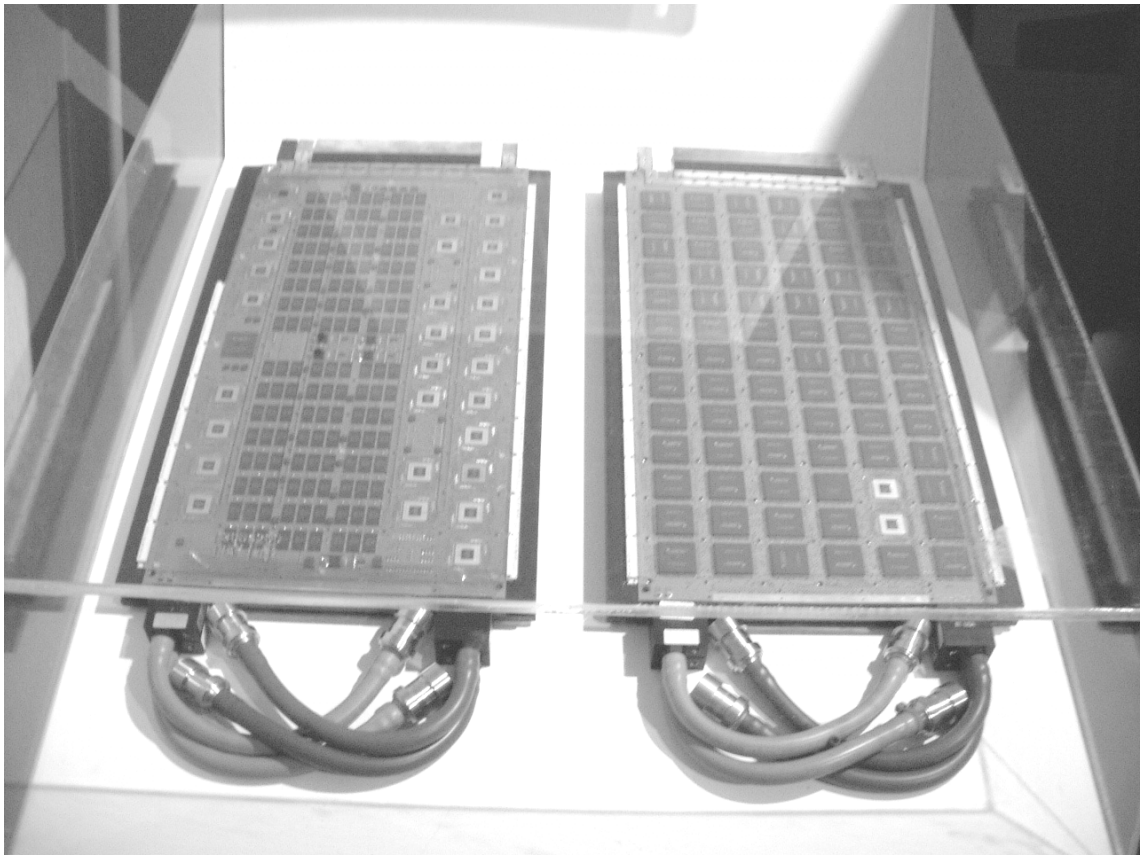

図４　ZIEGLERの回路基盤

出所：国家暗号学博物館展示物（筆者撮影）

（３）国際的な通信傍受活動

国際的な通信傍受に関する事例として、ソ連に対する米国の「アイビー・ベル（Ivy Bells）作戦」がある[10]。1970年代後半、米軍はオホーツク海に沈んでいたソ連の海底ケーブルを見付けるために兵士を海に潜らせ、水深400フィート地点で直径たった5インチのケーブルを見付け出した。銅線は非常に微弱な電磁波を周りに出してしまう。それを記録・解析することによってそこに流されたメッセージをおおよそ復元することができる。そこで、米軍は電磁波を捕捉して記録する装置を水深400フィートにある海底ケーブルに取り付け、一定期間が経過して記録がいっぱいになると取りに行って交換する、という作業をしていた。ところが、1981年になって問題の場所にソ連の艦隊が集合してきた。米国は人工衛星でその様子を見ていたが、ソ連の艦隊が引き上げた後に現場に行って点検してみると、やはり装置はなくなっていた。現在、その装置はモスクワのKGB博物館に展示中である（図5参照）。発見の原因は、NSAの職員の賄賂による情報漏洩であるといわれている。

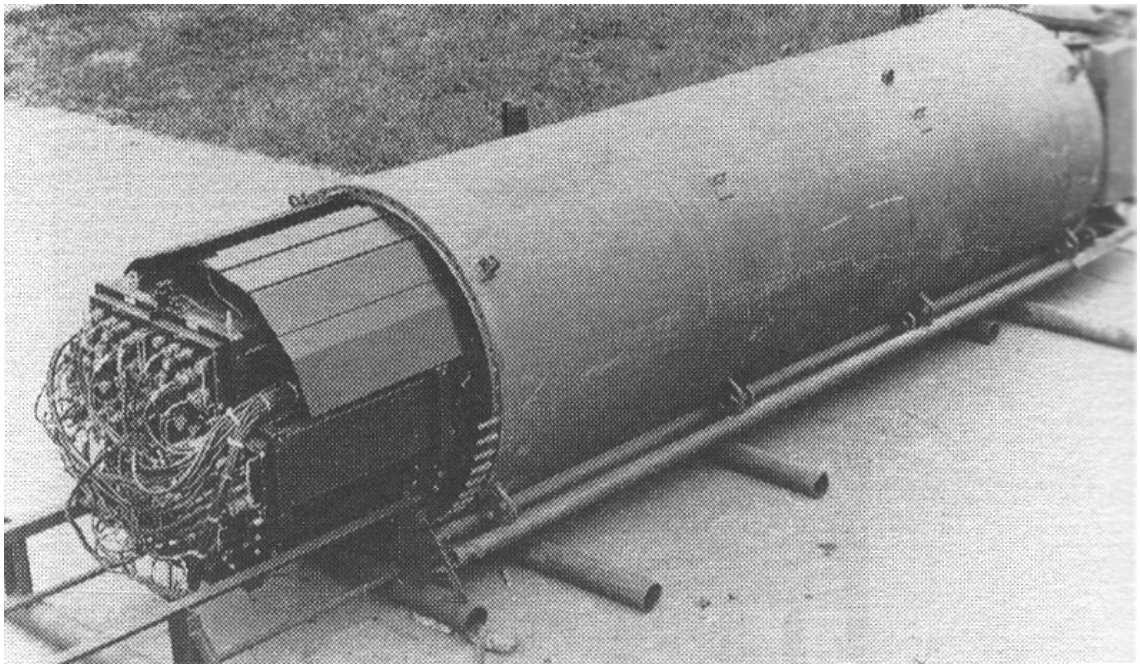

図５　アイビー・ベル作戦で使用された通信傍受装置

出所：Sherry Sontag, and Christopher Drew, with Annette Lawrence Drew, *Blind Man's Bluff: The Untold Story of American Submarine Espionage*, New York: Public Affairs, 1998, 挿絵。

近年、「あらゆる情報を傍受している」と喧伝される「盗聴」ネットワークのエシュロンが注目されている。エシュロンは、主に人工衛星を使って、電話・ファクス・電子メールなどの通信を傍受するシステムで、いちいち各国で正式な許可を取っているとは思えず、一般的な認識では非合法活動である。しかし、国家安全保障上の問題については、米国法は対外インテリジェンスを認めているので、対象が米国外である限りにおいて、米国では合法であるとも解釈できる（しかし、この米国の行為が対象とされる国々で合法であるということには無論ならない）。

エシュロンはもともと存在が隠されていたが、ニュージーランドの政府が漏らしたことから発覚した。その背景には、フランスの反発があったといわれる[11]。かねてから米英のインテリジェンス活動に不満を持っていたフランスがEUに調査させ、その活動の一部が世に知られるようになった。

エシュロンの全容はいまだ明らかにされていないが、技術的に考えれば、エシュロンが世界中のあらゆる情報を集めていると考えるのには無理がある。エシュロンにとって簡単な情報とは、無線通信・衛星通信である。携帯電話会社は無線の端末から基地局までは無線で繋ぎ、基地局から基地局に飛ばす際にはマイクロ・ウェーブ無線を使っている場合があるが、エシュロンはそのような無線通信を主に傍受しているといわれている。アイビー・

ベル作戦で見たように、同軸の海底ケーブルも傍受しやすい通信の一つである。

しかし、エシュロンは新しい技術に関しては困難に直面している。同軸ケーブルは電磁波を発してしまうので、そこにデバイスを設置することである程度傍受できる。しかし、光ファイバーはそのような電磁波を全く発しない。極めて微弱な電磁波を発することもあってエシュロンはそれを取っているという主張もあるが[12]、技術的には証明されていない。一つ可能性があるとすると、光をいったん電子に置き換え、それをまた光に変換するための増幅装置が一定の間隔で置かれており、この増幅装置が狙われるということである。しかし、現在はそれも電子に変換しない光スイッチになってきているので、エシュロンにとってますます難しくなるだろう。

仮にエシュロンがあらゆる通信を傍受できたとしても、そうした情報を蓄積・分析するだけの能力は膨大なものになる。情報の洪水から、危険な活動につながる情報だけを選び出すコストは計り知れない。「ディクショナリー」といわれるデータベースを使って該当する言葉を選び出しているといわれるが（カーニボーと同じ発想である）、犯罪者やテロリストが一見して分かるような言葉を使う可能性はきわめて低いだろう。

５．結論

米国のインテリジェンス・コミュニティは、9.11を契機として、それ以前の法的枠組みを強化（規制を緩和）するUSAパトリオット法を成立させ、インターネットを視野に入れた通信傍受活動を拡大した。しかし、スチューピッド・ネットワークの登場によって通信傍受は技術的にますます難しくなっている。あらためて整理すれば、次のような問題が指摘できるだろう。

・同期通信から非同期通信へ：容疑者の特定が困難に

　電話のような同期通信では当該通信の発信者と受信者が特定しやすかったが、インターネットのような同期通信ではそれが困難になる。情報の洪水の中から特定の情報をつかみとれる可能性は小さくなりつつある。

・ネットワーク管理の縮小：さまざまな協力体制の確立が必要に

　回線交換の電話網では、その管理者が明確に規定されており、通信傍受の制度的・技術的インターフェースは安定していた。しかし、ネットワークのネットワークであるインターネットでは管理者は分散しており、さまざまな組織の協力を得る必要性が出てきている。

・通信形態とコンテンツのコントロール権がユーザーに：柔軟な対処が必要に

電話時代の通信形態とは音声通信に他ならず、コンテンツは人間の声による会話であった。しかし、インターネットでは音声、画像、動画、文章などさまざまなコンテンツがデジタル化され、さまざまな種類のデータ・パケットとして送信されるため、画一的な対応ができなくなっている。また、個人が手軽に暗号通信を行うこともできるようになってきている。

・傍受しにくい技術の登場：上回る能力の模索

通信傍受を困難にする光ファイバーのような技術の登場は、インテリジェンス・コミュニティにそれを克服する技術の開発、能力の育成を迫っている。

今後の通信傍受はどうなっていくのだろうか。例えば、たくさんの人たちが自分独自の暗号を使うといったように、情報技術によって個人がエンパワーされていくと、通信傍受はますます難しくなっていくだろう。そうした変化に対応するために、インテリジェンス・コミュニティは通信事業者やISPとの協力関係を拡大せざるを得ない。ただ、その際に暗号化された内容そのものを解読することはそれほど重要ではなく、誰と誰が暗号通信をやっているという事実が重要になる。暗号の内容を解読するのに3000年かかるとしても、特定の人物の間で暗号通信が行われていれば、その人たちに関する情報をヒューミント、イミントから得て、それらを総合的に判断すれば、十分なインテリジェンスとなるかもしれない。

2002年9月に発表されたブッシュ・ドクトリン（米国国家安全保障戦略）では、インテリジェンスの強化が謳われているが、スチューピッド・ネットワーク時代の通信傍受に関していえば、ますます断片化する情報を総合する能力が問われることになるだろう。NSAは9.11前日に攻撃を示唆するメッセージを傍受していたものの、そのアラビア語の翻訳はテロ後に行われたという[13]。結果論から言えば、断片化されたメッセージをつなぎ合わせる感覚の鋭さがますます求められるようになったといえるだろう。

――注――

1　David Isenberg, "Rise of the Stupid Network," *Computer Telephony*, August 1997. pp. 16-26.

2　インターネットに接続されている普通のサイトがつながらなくてもインターネット全体のパフォーマンスにはほとんど影響がない。それは9.11の際にニューヨークの一部がつながらなくなったものの、インターネットにはほとんど影響がなかったことでも分かる。ただし、9.11直後はCNN.comやNYTimes.com、ABCNews.comなどのサイトでアクセスが殺到したため1時間ほどつながらなくなった。これはインターネットがつながらなくなったということではなく、当該サイトの能力がアクセスに耐えられなかったということである。しかし、YahooやGoogleなど、インターネット上にはいくつかのハブ・サイトが存在する。一般的なサイトがどれだけ故障してもインターネット全体には大差ないが、こうしたハブ・サイトは同時に落ちてしまうことになると、多大な影響が出る。インターネットの住所機能を担うDNS（ドメイン・ネーム・サーバー）のうち、ルート・サーバーと呼ばれる最上位のものは世界13カ所に設置されている。それぞれAからMまでのアルファベットが振られており、中でももっとも重要なルートAサーバーは米国商務省の管理下に置かれている。13のうち、半分程度が攻撃を受けて使えなくなると、インターネットは分断されるといわれている。インターネットは故障には強いが攻撃には弱いといわれる理由である。アルバート＝ラズロ・バラバシ（青木薫訳）『新ネットワーク思考－世界のしくみを読み解く』（日本放送出版協会、2002年）を参照。

3　結局、禁酒法はなし崩しになり、その後、ルーズベルト大統領が憲法修正第21条によって解除した。

4　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。

5　一義的には法律で認められているものが合法で、認められていないものが非合法だが、そのボーダーラインは各国の政治体制などによって大きく異なる。例えば、権威主義体制の国では、通信傍受が合法化されているわけではないが日常的に政府によって行われている場合が多い。こうした現状が、すべての通信傍受を「盗聴」と呼ばせ

ることになっている。言うまでもなく、非合法的な通信傍受は、日常的に行われており、その多くが処罰の対象となっていない。例えば、恋人の動向調査が目的で私的な盗聴が行われることもあるし、あるいは政府が何らかの意図を持って盗聴をすることもある。しかし、そうした盗聴行為の明白な証拠があり、裁判の結果、プライバシーの侵害などの有罪判決が出れば罰せられることには変わりない。

6　法律の解釈については、例えば、以下を参照。Electronic Frontier Foundation, "EFF Analysis of the Provisions of the USA Patriot Act that Relate to Online Activities," <http://www.eff.org/Privacy/Surveillance/Terrorism_militias/20011031_eff_usa_patriot_analysis.html> (October 31, 2001).

7　バラバシ、前掲書。

8　AP通信「FBIの大失態 —— テロ関連電子メールを誤って破棄」Wired News（2002年5月29日）<http://www.hotwired.co.jp/news/news/20020530201.html>。

9　「フィル・ジマーマン・インタビュー：われわれはプライバシーを捨てるべきではない」HotWired <http://www.hotwired.co.jp/bitliteracy/interview/020709/>。

10　Sherry Sontag and Christopher Drew, with Annette Lawrence Drew, *Blind Man's Bluff: The Untold Story of American Submarine Espionage*, New York: Public Affairs, 1998.

11　鍛冶俊樹『エシュロンと情報戦争』（文藝春秋、2002年）。

12　同書。

13　Walter Pincus and Dana Priest, "NSA Intercepts On Eve of 9/11 Sent a Warning Messages Translated After Attacks," *Washington Post*, June 20, 2002; Page A01.

参考文献

・Bamford, James, *Body of Secrets: Anatomy of the Ultra-Secret National Security Agency*, New York: Doubleday, 2001.

・Berkowitz, Bruce D., *Best Truth: Intelligence in the Information Age*, New Haven: Yale University Press, 2000.

・Denning, Dorothy E., *Information Warfare and Security*, Boston: Addison-Wesley, 1999.
・Isenberg, David, "Rise of the Stupid Network," *Computer Telephony*, August 1997. pp. 16-26.
・Kahn, David, *The Codebreakers: The Story of Secret Writing*, New York: Scribner, 1967.
・Ludlow, Peter, *Crypto Anarchy, Cyberstates, and Pirate Utopias*, Cambridge: The MIT Press, 2001.
・Lyon, David, *Surveillance Society: Monitoring Everyday Life*, Buckingham: Open University Press, 2001.
・Richelson, Jeffrey T., *The U.S. Intelligence Community, Fourth Edition*, Boulder: Westview Press, 1999.
・Schneier, Bruce, *Secrets and Lies: Digital Security in a Network World*, New York: John Wiley and Sons, 2000.
・Smith, Michael, *The Emperor's Codes: The Breaking of Japan's Secret Ciphers*, New York: Arcade Publishing, 2000.
・Sontag, Sherry, and Christopher Drew, with Annette Lawrence Drew, *Blind Man's Bluff: The Untold Story of American Submarine Espionage*, New York: Public Affairs, 1998.
・Thomas, Douglas, and Brian D. Loader, eds., *Cybercrime: Law Enforcement, Security and Surveillance in the Information Age*, New York: Routledge, 2000.
・Treverton, Gregory F., *Reshaping National Intelligence for an Age of Information*, New York: Cambridge University Press, 2001.
・青木冨貴子『FBIはなぜテロリストに敗北したのか』（新潮社、2002年）。
・鍛冶俊樹『エシュロンと情報戦争』（文藝春秋、2002年）。
・アルバート＝ラズロ・バラバシ（青木薫訳）『新ネットワーク思考－世界のしくみを読み解く』（日本放送出版協会、2002年）。
・春名幹男『スパイはなんでも知っている』（新潮社、2001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）。