

# デジタル時代の合法的通信傍受

## <ヨーロッパ編>

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)

### ホットピックになった暗号規制・通信傍受

9月11日のアメリカでの同時多発テロは、暗号利用規制、通信傍受問題を急速に政治問題化させている。いや、すでに政治問題化されて久しかったのだが、ホットピックとして論じられることがなかったのである。

ところが、アメリカ連邦議会は、これまでの議論をなし崩しにする形で、規制強化へと動き出している。特に「2001年テロ対策法案(Combating Terrorism Act of 2001)」が、ほとんど審議されないまま議会上院で採択されたことは、特筆に値するだろう<sup>1</sup>。この法案によって、捜査機関による通信傍受がより容易になるとされている(ただし、まだ上下両院の調整が済んでおらず10月7日現在、立法化は行われていない)。

これに対して、インターネット・コミュニティ側に立つEFF(Electronic Frontier Foundation)やEPIC(Electronic Privacy Information Center)、CDT(Center for Democracy Technology)といった団体は、規制強化に警告を出している<sup>2</sup>。今回の同時多発テロは、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であるとされているが、逆にそれを口実にプライバシーを侵害するような規制が拡大されると、サイバー・リバティ団体は懸念している。

アメリカ映画を見ていると、政府機関が市民の電話を傍受するシーンが出てくる。もともとアメリカでは、裁判所の許可を得て犯罪捜査のために通信を傍受することが認められていたし、1994年には「CALEA(法執行機関のための通信援助法)」という法律が制定されて、デジタル通信や無線通信の傍受に際して、通信事業者に設備変

更を含む協力を要請することができるようになった。犯罪捜査のために、ISR(インターネット・サービス・プロバイダ)の電子メールを全部読んでしまう「カーニボア(Carnivore)」というシステムも訴訟問題になっている。

アメリカは今、テロ直後の茫然自失の状態から、急速に愛国心を鼓舞する雰囲気になりつつある。これは即時報復、開戦という論調とは必ずしも結びつかないのだが、安全のためには、プライバシーが多少侵害されることもやむを得ないとする声があることは確かである。

例えば、連邦最高裁の判事のひとりで保守派とされるサンドラ・オコーナー判事は、「私たちの国で、これまでより先個人の自由が規制されることを、われわれは経験するかもしれません」と述べている<sup>3</sup>。

しかし、アメリカでの議論が落ち着くにはまだ時間がかかりそうだ。当面はどうやって国防を強化するか、テロの首謀者とされるビンラディン氏にどう対処するかという点が最優先である。

そこで今回は、今年3月に行った調査に基づき、ヨーロッパの通信傍受の動向について報告し、来月、アメリカの動向について報告することにしたい。ヨーロッパではプライバシーの保護に熱心である一方で、すでに合法的通信傍受という点では確立された制度を持っており、アメリカより先進んでいるからである。

### ニースの森の中

映画祭で有名なカンヌと、王国モナコに挟まれたフランスのバカンスの街ニース。ニースの市街地から車で20分ほど走り、山の中に分け入るとソフィア・アンティポリスがある。ここは知る人ぞ知るヨーロッパのハイテク集積地で、森の中にゆったりとハイテク企業や



青い海が広がるニース

コンソーシアムが散らばっている。

なかでも有名なのがETSI(エツィ)と略される、ヨーロッパ電気通信標準化機構である。ここは携帯電話などの移動体通信の標準化を活発に行っている。ヨーロッパの携帯電話といえばGSM(Global Standard for Mobile communications)と呼ばれる形式で、百数十カ国で使われる世界標準だ。日本では標準が違うので使えないが、GSMの国際ローミング・サービスは非常に便利だ。ヨーロッパでは、どこに行っても自分の携帯電話が使えるし、台湾の人が北京に行っても自分の携帯電話が使えるのだ。この標準化で中核的役割を担ったのがETSIである。

ETSIで出迎えてくれたのは、事務局を担当する巨漢のドイツ人、ローゼンブロック氏と、合法的通信傍受の標準化を担当する物静かなフィンランド人、ラシライネン氏である。

ローゼンブロック氏はまず、「合法的通信傍受は、ヨーロッパでは全くノーマルな話になっている。すでに法令の一部である。セキュリティの危機がある場合には、国家はその権利を持っている」という。

もちろん、ヨーロッパ内にもいわゆる「盗聴」に関する懸念は根強くある。私と同僚がETSIを訪れる前の週に、ドイツの雑誌が「ETSIは通信傍受の手伝いをしている」という批判記事を出したそう。ローゼンブロック氏は「合法的(lawful)という言葉が抜けているんだよなあ」とぼやく。警察が犯罪捜査のために合法的通信傍受を行うといっても、それは政治的に歪められた意図の下に行われ、引いては一般市民のプライバシーまで奪われてしま

う。そういうイメージがあるのは事実だ。

ローゼンブロック氏は、ETSIとして記事に反論するかどうか迷ったが、やめることにした。合法的通信傍受を行うかどうかは各国の問題であり、各国の政府が説明すべき問題だと考えたからである。ETSIが作るのは標準であり、法律ではないのだ。

きっかけは携帯電話

ETSIが合法的通信傍受の問題にかかわるきっかけとなったのは、携帯電話の標準化である。実は、固定電話の合法的通信傍受については、あまり技術的に議論する余地がないそう。その気になればいくらでも方法はあるそうで、法律に基づいて、どうそれを実施するかが問題となるだけである。

携帯電話が問題になるのは、それが暗号化されているからだ。携帯電話は無線通信技術の一つだが、例えばラジオ放送は受信機があれば誰でも聞くことができる。暗号化されていないからだ。しかし、携帯電話の内容が暗号化されていないとしたらどうだろう。会話がそのままラジオに流されるようなものである。

携帯電話といっても、すべてのネットワークが無線でつながっているわけではない。手許の携帯電話は近くのアンテナにつながり、そこからは光ファイバーなどの有線でつながる。そこから固定電話のネットワークにも入っていくし、アンテナから別の人の携帯電話にもつながる。だから、会話が有線ネットワークを通る間に捕捉すれば、有線の通信傍受とさほど変わらない。

ヨーロッパの携帯電話方式であるGSMは、すでに述べたように国境を越えて使うことができる。そうすると、ある国の政府が法律に基づいて合法的通信傍受を行おうとしても無理な場合がある。政府当局が話し合っただけで協力することが必要になるが、こうした協力はえてして時間がかかり、迅速な犯罪捜査には不向きである。

さらに、各国で通信傍受のための技術標準が違っていたらどうなるだろう。犯罪者がどんどん移動する間に、暗号化された通信の解読に時間が

かかれば、犯罪者を取り逃がす可能性は高くなる。捜査協力の問題は別にして、せめて技術の標準化ができないかと考えたのが、ETSIでの標準化のきっかけであった。

### ETSIの標準

標準化をすと思わぬメリットがあることもわかってきた。ETSIは、標準化をする理由として以下の点を挙げている。

第一に、通信傍受に対応する機器メーカーが規模の利益を享受できる。各国で標準と仕様が異なっていれば、市場規模は細分化され、メーカーにとってはコストがかさむだけになる。標準が同じであれば、少なくともヨーロッパ域内のどこでも売れることになる。

第二に、通信事業者も運用がしやすくなる。通信事業者にとってみれば、合法的とはいえ通信傍受は厄介事以外の何物でもない。通信傍受に関する費用負担を事業者に求める国もある。さらに「あの電話会社の通話は全部聞かれているらしいよ」などという噂を立てられたらたまったものではない。すでにヨーロッパ各国では、通信事業のライセンスの条件として合法的通信傍受への対応が義務付けられているため、どうせやるならみんな同じ標準でやって欲しいのだ。ヨーロッパの通信事業者は、どんどん国境を越えたビジネスを展開している。各国で標準が違くと参入障壁にもなりかねない。

第三に、各国政府が余計な議論を回避することができる。仮に各国ごとに標準化をしたら、なぜその標準を採用するのか政府は説明せねばならず、長い議論に巻き込まれる可能性がある。しかし、電気通信に関するさまざまな標準化を手がけてきたETSIに委ねれば、そうした議論を避けることができる。

第四に、一般の人々にとっても、ETSIが標準化の議論をオープンに行い、標準そのものがオープンになることで、通信傍受に対する不安を少しでも解消することにつながる。これは犯罪者にとっても標準がオープンになるということなのだが、結果と

して犯罪が少なくなればいいという考え方だ。

では、どうやって標準化を進めるのだろうか。通信傍受だからといって特別なやり方をするのではない。あくまでもETSIのこれまでのやり方に従う。議論の過程は、ETSIのメンバー（通信事業者や機器メーカーなど）と各国の法執行担当機関にはオープンになる。電子メールやメンバー専用のホームページなども活用される。議論の結果はインターネットなどで公開され、標準の使用料などは一切取らない。誰でも使うことができる<sup>4</sup>。

七つのワーキング・グループがあり、それぞれ約6週間ごとに会合が開かれる。場所はETSIのほかにも提供してくれるところがあれば、そこでやることもある。議論を有益なものにするには、メンバーの間の信頼関係や個人的なつながりが必要だと、ローゼンブロック氏は指摘する。

ETSIは、ゆくゆくはETSIの標準を世界標準にしたいと考えている。通信分野の標準化は、長い間、ITU（国際電気通信連合）で行われてきたが、ETSIは、問題をITUに投げかけることはしなかった。問題の性質ゆえに、政治体制の異なる国が集まるITUでは結論が出ないと考えたのである。しかし、ETSIの標準が優れたものであり、誰でも無料で使えるようになっていけば、自然と採用されるだろうと考えている。機器製造業者の少ないヨーロッパにとっては、日本やアメリカの製造業者が標準を採用してくれることも重要なのだ。

### イギリスの場合

ETSIの合法的通信傍受のワーキング・グループで指導的な役割を果たしているのが、イギリスの通信事業者ブリティッシュ・テレコム（BT）のゲーブ氏だ。ゲーブ氏は、長身で、「鉄腕アトム」のお茶の水博士のようにもじゃもじゃとした髪の毛を持ち、眼鏡の奥の鋭い眼光が印象的だ。

イギリスでは、1984年にケーブル・アンド・ワイアレス社がローカル電話市場に参入し、通信市場の開放が行われた。これを受けて、翌年に合法的通信傍受を含む法律が制定された。ブリティッシュ・テレコムが国営電話会社であったときは、さして面



ブリティッシュ・テレコム  
の  
ゲープ氏

倒な手続きを踏まなくても合法的通信傍受が可能だったが、民営化され、他の事業者も入ってきたことで法制化が必要になったのである。同じく1995年には、EUレベルで通信傍受に関する決議が提出されたことも議論を後押しした。当初、この決議に対してフランスが強い懸念を表明したが、1996年1月に採択されたという。

ロンドンを見ると、携帯電話では4社から5社が激しい競争をしている。高価で柔軟性がない標準だと通信傍受が市場参入の障壁となってしまう。実際、すでに投資をして、顧客もいたのに、通信傍受への対応ができていないために参入をあきらめさせられた事業者もいた。標準は、例えば最大のシェアを握るブリティッシュ・テレコムに有利なものであってはならず、市場に中立的でなくては行けない。通信傍受の標準自体が、GSMのネットワークの一部になっていることが重要である。

ゲープ氏がワーキング・グループの中で苦労したのは、やはり各国の警察当局との意見の調整だったという。技術はどんどん進化するが警察はそれについていけず、また常に自国の観点から問題を考えようとする。しかし、市場がどんどんグローバルになっていることを、共通認識として持つように努力した。

なぜETSIに協力したのかと聞くと、ETSIは標準化の工場であり、これまでもさまざまな技術標準の設定で成功してきたからだという。言い換えるならば、限られた時間の中で結論を得るという点においてETSIは効率がいい。また政府代表が議論す

るITUの世界では、民間が介入する余地がない。政府と民間と一緒に議論する場が必要なのだ。各国の政府にとっても、「ETSIで決まったんだから」と言えることは大きなメリットなのである。

### インターネットが問題だ

ゲープ氏のオフィスを辞したあと、ロンドン大学のコンピュータ関連犯罪センターのジョーンズ氏に会いに行った。彼は部屋に入るなり「日本ではお客さんが部屋の奥に座るんですよ。インターネットで調べたんだ」という。さすがに調べものは得意らしい。

彼はすでに白髪が生える歳なのだが、大学組織にいるにもかかわらず、肩書きは教授ではなくて「スペシャル・コンサルタント」である。彼は政府の手伝いでコンピュータ犯罪の捜査の手伝いをしたり、ヨーロッパの警察担当者を集めたセミナーで講師をしたりしている。彼の名前は「Robert S. Jones」なのだが、あまりにもよくありそうな名前、本名なのか怪しくなってくる。

彼は、警察官や裁判官が技術を理解していないのが問題だと言う。彼はある裁判に参考人として招かれたのだが、インターネットの仕組みなど、もろもろのことを法廷の人たちに理解させるのに丸一週間を費やした。さらには、押収された10ギガ（1.3メガのフロッピー・ディスクの7,692枚分）のハードディスクの中身を全部印刷してくれというような、無茶なことを捜査官は言うときく。

彼もまた、民間と政府がきちんとした対話の機会を持つことが重要だと言う。そのために、イギリスではフォーラムがいくつかあって定期的に話し合う機会を持っている。数年前、あるフォーラムの場で、両者の関係が悪くなったことがあった。警察側がギャンブルをインターネットから駆逐しようとしてISPに書簡をよこした。そこには、「ギャンブルを駆逐しないとんでもないことになるぞ」という強権的な書き方がされていた。これを見た技術屋たちは「何を言ってるんだ」と笑い、「そんなことを考えても無駄だ」と対立が深まってしまったのである。

さらにインターネットで問題なのは暗号通信だ。

インターネットのホームページを見るためのブラウザにはすでに暗号が組み込まれている。個人情報や安全に送りたいときに、情報の受信側がこれに対応していれば自動で(ほとんどの人がよくわからないままにOKのボタンをクリックして)暗号通信が行われている。

電子メールで暗号技術を使っている人はまだ少ないのだが、私は「PGP(Pretty Good Privacy: けっこうよくできたプライバシー)」という名のアメリカでよく使われているソフトウェアを使っていたことがある。確かにけっこう面白いのだが、相手も対応するソフトウェアを使っていないと意味がない。結局「読めないよ」と友人に言われて、使うのをやめてしまった。

しかし犯罪者にとって、暗号化されたメッセージの通信は非常に役立つ。暗号メールを使っているのは犯罪者だけであるといわれることもある。最近の、高度な数学を使った暗号ソフトウェアを解読するのは困難である。どんなに強力といわれた暗号でも破られてきたのが人類の歴史だが、3日後の犯行の打ち合わせに使われる暗号メッセージを解読するのに、1カ月かかるのでは意味がない(もちろん後の証拠にはなり得るが)。

最近の暗号ソフトウェアは、「暗号化する鍵」と「解読(復号)する鍵」を違うものに行うことができるようになっていて、解読を難しくしている。たとえ解読できたとしても、その内容が「今晚のおかずはカレーライスね」だったらどうなるだろう。これは文字通りの意味しかないかもしれないし、「今晚の銀行強盗のターゲットは 銀行だ」という意味かもしれない。

ただし、ジョーンズ氏は、必ずしも内容が解読される必要はないと指摘する。例えば、AからBへ暗号メッセージが送られ、それに対して、BからAへ返信が送られれば(特に、その返信も暗号メッセージであれば)、AとBが共謀関係にあると推定できる。他の証拠をつきつめていけば犯罪は証明できるかもしれない。

## 非合法的通信傍受

通信の秘密が守られていないと議論する人たちが、よく口にするのがエシュロンだ。これは、アメリカとイギリスが手を組んだ秘密プロジェクトで、詳細は不明だが、衛星を使って世界中の通信を傍受し、あらゆる秘密を探っているというものだ。

私がヨーロッパで会った人たちは、「あれは非合法的通信傍受であり、諜報活動のようなもので、われわれがやっていることとは別物だ」という。

エシュロンの真偽は確かめようもないが、「そんなものがうちのネットワークでやられていたら断固阻止する」と言うのはドイツ・テレコム(T-Com)のツェルジツヒ氏だ。彼は、自分の部屋に貼ってある世界地図を指差しながら、「ここやここ、それにここでもエシュロンはやっている」と教えてくれる。日本にも傍受のための施設があるらしい。

しかし、全世界の通信を記録するには膨大なハードディスクが必要で、さらにそれを解析するのは無駄といっている作業だ。エシュロンは自動的にキーワード検索をすることで重要な情報を割り出すといわれているが、わざわざ「一週間後に大統領を暗殺する」と書く人はいないだろう。

コストに見合うとともに、プライバシーに配慮した捜査の仕方をするには、こうした網掛け方式ではなく、ピンポイントの通信傍受しかない。

## ドイツの場合

ツェルジツヒ氏の同僚で、イギリスのゲープ氏とともにETSIの標準化を進めてきたアダムズ氏が、「日本ではどのくらいの電話に関する通信傍受が行われているんだい?」と聞くので、「今のところ数件」と答えると、どっと笑い声が上がった(2000年8月の通信傍受法施行以前も、実は日本で合法的な形で通信傍受がわずかに行われていた)。

ドイツでは年間1万件以上の合法的通信傍受が行われている。そのほとんどがドイツ・テレコムで行われるので、ドイツ・テレコムにとっては大きな負担になっている。実際に通信傍受の命令が裁判所から出るのは3,000件ぐらいで、そのうち実施されるのは1,500から2,000件ぐらいである。それぞ

れの傍受において複数回行われるのが普通なので、年間1万件ぐらいになるのだそうだ。

イギリスでも同じくらいの規模で行われているといわれるが、正確な数は公表されていない。というのは、イギリスでは通信傍受で集められた記録は、法廷での証拠として使われないことになっているからだ。あくまでも捜査当局の補助的なツールとなっていて、その内容が公表されることはない。捜査当局は別の証拠で犯罪を立証しなくてはならない。通信傍受の数を公表すると犯罪者にヒントを与えることになるため、一般には公表せず、特別の委員会が監視のためにチェックしているという。

ドイツでは法律的に通信傍受は合憲とされ、1968年10月に法律ができた。その法律は何回も改正され、技術変化、市場変化に応じて犯罪のリスト(リスト)に載っていること以外には通信傍受が認められない形に変更されている。

ドイツ・テレコムのアダムズ氏は、「一番の誤解は、通信事業者のネットワークが警察に直結していると思われていることだ。われわれは正式な書面の手続きを踏んでからではないと、ネットワークを警察の設備につなげることは決してない。期限が来たらすぐに切断する」と指摘する。顧客の信頼を維持するために、通信事業者は公正な運用を行わなくてはならない。

ただし、ヨーロッパでも完全に問題が解決されたわけではない。特にインターネットに関しては模索中の段階である。例えば、オランダでは政府がISPに対して通信傍受のための特別な要求を求め、そのコストの高さのためにISPが悲鳴を上げている。まだ誰も満足のいきやり方を知らないのだ。

議論と標準化はオープンに

プライバシーと公共の秩序の両方を完全に満たす技術は、難しいのかもしれない。重要なのは、制度が適正に運用されているかどうかという点で、政府と国民との間に信頼関係があるかどうかだろう。民主主義が根付いていると思われる国でも、「人権派」とレッテルを貼られてしまうような人たちが、いざ自分が被害者になると逆のことを求めてく

ることがある。議論の落ち着くところ、多くの人たちが納得するところを見つけるのは難しい。議論の場には、人権派であろうと、マスコミであろうと、一般の人々であろうと、オープンに入れていかないと、どんどん話がこじれる。

少なくとも、技術的な標準化においては、ETSIにおける携帯電話の通信傍受標準化に学ぶところがあるだろう。ETSIの議論の場に一般の人が参加できるわけではないが、どこで議論がされているかということは見えてくるし、議論の結果は公表される。通信事業者にとっても機器のメーカーにとってもメリットがある。日本の法執行機関、通信事業者、メーカーがETSIに参加することも可能である。

次世代携帯電話が普及すれば、日本の携帯電話サービスでも国際ローミングができるようになる見込みだ。無論、インターネットのメッセージに国境はない。しかし、法律体系は、いまだきわめてナショナルなものである。インターネットの世界でも国家の役割というのは、しぶとく残らざるを得ないだろう。

ヨーロッパでは、インターネットが普及する以前から、合法的な通信傍受が国民に受け入れられてきた。そのため、現在のアメリカで見られるような激しい抵抗はない。インターネット・コミュニティの活発な動きも見られない。

暗号規制問題を研究してメリーランド大学から博士号を授与されたランディ・ベゼット氏は、「フランスではアメリカよりずっと高いレベルの国民監視が行われているが、ほとんどの国民は『自分は何も悪いことをしていないから問題ない』という態度だ」と指摘する。同じ自由を愛する国民でも、フランスとアメリカでは大きな差が見られるということである。

9月11日のテロ以降、アメリカの司法省、FBI、そして議会は一気に通信傍受推進へと動いている。それに対抗するアメリカのインターネット・コミュニティもまた、大きな声を上げはじめている。

しかし、そもそもこの議論は、「テロリストたちが暗号通信を使っていた」、「ビンラディンは暗号マニアだ」という不確かな情報が発端で、その真相

究明はあまり行われていない。次号では、アメリカの状況をさらに詳しく紹介することにしたい。

\*1 Declan McCullagh「米上院、ネット監視を強化する新テロ対策法を採択(上)」<<http://www.hotwired.co.jp/news/news/culture/story/20010917201.html>>(2001年9月14日)

Declan McCullagh「米議会で高まる暗号規制への動き(上)」<<http://www.hotwired.co.jp/news/news/culture/story/20010917203.html>>(2001年9月13日)

ここでいう2001年テロ対策法(Combating Terrorism Act of 2001)とは、下院の予算関連法案H.R. 2500( Departments of Commerce, Justice, and State, the Judiciary, and Related Agencies Appropriations Act, 2002 )に対する修正法案S.AMDT.1562のことである。

\*2 下記のウェブページを参照。

Electronic Frontier Foundation, "ALERT: Hackers Could Get Life in Prison, No Parole, Under 'Anti-Terrorism' Bill," <[http://www.eff.org/alerts/20010927\\_eff\\_wiretap\\_alert.html](http://www.eff.org/alerts/20010927_eff_wiretap_alert.html)> (Access: October 7, 2001).

Center for Democracy and Technology, "Response to September 11, 2001 Terrorist Attacks," <<http://www.cdt.org/security/010911response.shtml>> (Access: October 7, 2001).

American Civil Liberties Union, "ACLU Calls New Senate Terrorism Bill Significantly Worse; Says Long-Term Impact on Freedom Cannot Be Justified," <<http://www.aclu.org/safeandfree/>> (Access: October 7, 2001).

\*3 LINDA GREENHOUSE, "O'Connor Foresees Limits on Freedom," New York Times <<http://www.nytimes.com/2001/09/29/national/29SCOT.html>> (September 29, 2001).

\*4 すべて<<http://www.etsi.org/>>で入手可能。無料だが登録が必要。ちなみに合法的通信傍受は英語で「lawful interception」である。

「智場」記事一覧