



第14回 のぞきの免許状  
——— フライバシーのないイギリス人

text : 土屋大洋 / [HP](#) / 「モードとしてのガバナンス」の[一覧へ](#) / [Text Only Version](#)

 イギリスのインテリジェンス・コミュニティ

映画の007でイギリス情報部員ジェームズ・ボンドは「殺しのライセンス (license to kill)」を持っていることになっているが、イギリスでは「のぞきの免許状 (snooper's charter)」というのもある。「snoop」という言葉は「かぎ回る、探る、コソコソ詮索する」といった意味である。殺しのライセンスが本当に存在するかは疑わしいが、実はのぞきの免許状は500以上の政府機関に与えられている。

もともとイギリスは政府による通信傍受が頻繁に行われてきた。言うまでもなく、イギリスの北部アイルランド統治に反対するアイルランド共和国軍 (IRA) のテロ防止のためである。年間数千件から1万件の通信傍受が行われているといわれ、日常化している。ネオナチ問題を抱えるドイツでも同じ状況で、テロが頻発する中東諸国では数え切れないぐらい行われているだろう。

アメリカでは9.11以降、パトリオット法が成立し、電話だけでなくインターネットも含めた通信傍受が簡単になった。アメリカでは「9.11がすべてを変えてしまった」とよくいわれるが、しかし、イギリスやドイツなどのヨーロッパ諸国は、9.11以前から通信傍受を頻繁に行っていたことになる。

政府による通信傍受はインテリジェンス活動の一環である。アメリカのインテリジェンス・コミュニティについては以前[この場で紹介した](#)が、イギリスはどうなっているの

だろうか。

本来インテリジェンス・コミュニティの活動は秘密主義のベールで覆われているが、イギリスのそれはきわめて秘密主義的である。第二次世界大戦当時、ウィンストン・チャーチル首相は早くからドイツ軍のエニグマ暗号を破って暗号を解読していたが、その事実を悟られないためにドイツ軍によるイギリスの町コベントリーへの空爆を黙認したといわれている。戦後もチャーチルは長らく暗号解読の事実を伏せていた。世界で初めてコンピュータを発明したのはアメリカということになっているが、それより先にイギリスが作っていた。この事実も長らく明かされなかった。



### ブレッチリー・パーク

イギリスが第二次世界大戦中に暗号解読部隊を置いていたのが**ブレッチリー・パーク**である。アメリカの暗号解読を行う国家安全保障局(NSA)が首都ワシントンDCから少し離れたフォート・ミードにあるように、ブレッチリー・パークも電車あるいはバスでロンドンから2時間ほどのところにある。もともとは金持ちの邸宅だったが、ロンドンからほどよく離れ、車の便も鉄道の便も良かったために軍によって購入された。しかし、暗号解読所だということが露見してしまえば空爆の対象になるため、付近の住民も暗号解読所だとは知らなかったようだ。

私と同僚が昨年秋に訪問したとき、季節外れのせいかあまり人はいなかったが、職員の人たちが妙にジロジロと私たちを見る。「どこから来たんだ」「日本から」「そうかあ、それはよく来たなあ。日本人がきたのは久しぶりだよ」という調子で、他の職員にも次々と私たちの来訪が伝えられていく(この歓待の理由は後で分かった)。

ガイド・ツアーに参加すると、いろいろなものが置いてある。ローリング・ストーンズのミック・ジャガーがプロデュースした映画『エニグマ』で使われたという潜水艦の巨大模型も置いてある。暗号解読を行っていた職員が使っていたという古いテニス・コートもある。ドイツ幹部が使っていた最小サイズのエニグマ暗号機は、マニアがよだれをたらすほど貴重なもので、一度盗難にも遭っている。現在は夕方の30分間しか公開されない。

ブレッチリー・パークにいた人でもっとも有名なのは、アラン・チューリングであろう。「チューリング・マシン」や「チューリング・テスト」という言葉で知られている。彼はイギリスの暗号解読に多大な貢献をしたにもかか

ならず、機密保持を優先する政府から同性愛を理由に追い詰められ、毒りんごをかじって自殺してしまう。

そのチューリングがドイツのエニグマ暗号解読に作ったのがボンブ (bombe) という巨大な解読機だ。しかし、これもイギリス政府は機密保持のために戦後に破壊してしまった(あるいはどこかに隠したのか)。ブレッチリー・パークに残っているのは安っぽいレプリカだけで、本物はアメリカのNSAの [国家暗号学博物館](#)に残っている。

日本人が歓迎されたのは、日本の暗号の解読に関する部屋が設けられているからだ。10名ほどのツアーのガイドは、「日本語は文字数が多くて大変なんだよね、そうでしょ」と聞いてくる。日本暗号の解読の実態をこうやって見せられると「ううむ」と唸るしかない。実際には、イギリスがドイツ暗号を担当し、アメリカが日本暗号を担当するという役割分担がある程度されていたようだが、現在の英米のインテリジェンス共有は第二次世界大戦までさかのぼる。

無論、ブレッチリー・パークの栄光は、インターネット時代には過去のものでしかない。しかし、イギリスのインテリジェンス・コミュニティは現在でも活発である。イラクの大量破壊兵器問題でブレア政権が窮地に陥ったことは記憶に新しいが、治安情報を担当する [MI5](#) や海外でのインテリジェンス活動をする [MI6](#) (正式名称は Secret Intelligence Service: SIS。いまだ公式ホームページはない) が存在する。中央情報長官が13機関を統括するアメリカのインテリジェンス・コミュニティとは違って、イギリスのインテリジェンス・コミュニティは各機関が緩やかに連携する形になっている。



## 調査権限規定法

インターネットが普及する前からイギリスで通信傍受が頻繁に行われていたことはすでに述べた。それを可能にしていたのは1985年通信傍受法、1994年情報機関法、1997年警察法、1998年人権法などだという。そして、2000年7月28日に成立した2000年調査権限規定法(Regulation of Investigatory Powers Act 2000:RIPA)は、イギリスの通信傍受をインターネットに対応させるもので、MI5を管轄する内務省によって提案された。

この法律は、われわれが使っている暗号を復号するために鍵の提供を義務付ける。例えば、機密情報を暗号化してラップトップ・パソコンに入れている人が空港で検査を受け、暗号を復号するよう求められたとする。これを拒否すると、最高2年の懲役刑が科せられる可能性がある。

アメリカのパトリオット法が求めているような通信傍受も、この調査権限規定法の下では国務大臣(つまり、内務大臣だけではない)が署名するだけで可能である。5章83カ条からなる法律は、政府が調査・捜査目的で行う電話、電子メール、無線の傍受を合法化している(『外国の立法』第214号、2002年11月号に法律の解説と翻訳が掲載されている)。

何とも不思議なのは、イギリス人がこうした政府規制とあまり戦わないことである。日本人がプライバシー問題でどれだけ真剣に戦っているかという問題は棚上げするにしても、市民革命を通じて専制君主から民主制を勝ち取った人々とは思えない。無論、まったく反対運動がなかったわけではないのだが、9.11後の「仕方がない」という雰囲気の中で成立したアメリカのパトリオット法に対する反対運動と比べても、9.11前に成立した調査権限規定法に対する反対運動は目立たない。この問題に詳しいLSE(ロンドン大学政治経済学院)のサイモン・デイビーズは、「われわれには007の伝統があるからね」と笑い飛ばす。

イギリス訪問中、偶然、ケンブリッジ大学でこの問題に

関するセミナーが開かれると聞きつけた。ケンブリッジ大学といえば古色蒼然とした静かな大学町を想像するが、そうした古い区画とは離れたところにウィリアム・ゲーツ・ビルディングが立っている。マイクロソフトのビル・ゲイツ夫妻の財団が2000万ポンド(約40億円)を寄付してできたコンピュータ・サイエンスのためのビルである。ここに内務省の役人が呼ばれて調査権限規定法に関する講演をした。

アメリカでこうしたセミナーが開かれたら、激しいやり取りが当然行われるだろう。しかし、ゲストの内務省の役人は、机に腰掛けながら、会談教室に座るケンブリッジに学生たちに穏やかに話しかける。学生たちからの質問も、感情的にはならず、穏やかなものだ。



### 通信の秘密を守る

セミナーの後、司会をしていたケンブリッジ大学の **ロス・アンダーソン** にいろいろ質問してみた。すると、どうやらアメリカの **EFF (Electronic Frontier Foundation)**、**CDT (Center for Democracy and Technology)**、**EPIC (Electronic Privacy Information Center)** にあたるようなアドボカシー・グループがヨーロッパにはあまり存在しないらしい。つまり、そうした規制強化、監視強化に対する反対運動の核となるグループが存在しないのだ。

アンダーソン自身がかかわっている組織に **FIPR (Foundation for Information Policy Research)** というのがあるが、とても小さいという。比較的大きなところでは **Privacy International** があるが、その他の **Liberty Human Rights**、**State Watch**、**STAND** などの活動はいずれもそれほど大きくない。

ヨーロッパとひとくくりにしてしまうのはよくないかもしれない。ヨーロッパはよく知られているようにプライバシーの侵害に厳しい規制を施している。日米はヨーロッパでのビジネスを失わないために対応する法規制を求められており、日本の個人情報保護法成立の伏線ともなっている。実はイギリスの調査権限規定法も、政府の説明によれば欧州人権条約を批准するためのものということになっている。裏を返せば、それまで通信傍受法を根拠に野放しに近かった通信傍受に対していっそうの法的根拠を与えようということである。やはりヨーロッパの中でもイギリスは特殊なのかもしれない。

「確かに気分は悪いが、通信傍受にそれほど目くじらを立てる必要はない」という声もある。テロの取り締まりに役

に立つとともに、自分が悪いことを考えていなければ気にすることは無いというのだ。

しかし、十分に意識してわれわれはインターネットを使っているだろうか。電話にしろ、電子メールにしろ、ネットワークの管理者が協力すれば、あまりにも簡単にその内容を読むことができる。従業員が悪口を言っていないかチェックするために、従業員全員の電子メールを密かにチェックしていた社長の話を聞いたことがある。あるいは、特定のキーワードで従業員のメールをチェックしている会社も多い。会社のパソコンやネットワーク設備は会社の資産だから、そうされても法的には文句をいえない。一般のプロバイダーについても、アメリカのパトリオット法やイギリスの調査権限規定法では、プロバイダーが通信傍受に協力している事実を漏らしてはいけないことになっているから、ユーザがその事実に気づくのはきわめて難しい。

電子メールやその他のインターネット・アプリケーションは、一見するとプライベートだが、実はそうでないということも意識されていいのではないだろうか。そして、もっと厄介なのは、ユーザの秘密意識である。「秘密にしておいてくれ」と言ったところで、いったん受信された電子メールは転々と転送されていってしまう。しまったと思ったときには手遅れになりかねない。秘密は守られていると過信していると痛い目に遭うことになりかねない。通信の秘密は、技術的には簡単に破られるものだからだ。