「スパイ天国」日本の実態…

インテリジェンス研究者
元警察庁政策評価審議官
茂田忠良

最近、「スパイ防止法」の制定を提言する政党も多く、スパイ防止法制に対して関心が高まっています。そこで、本稿では、スパイ防止に必要な制度や法律について議論する上で必要な視点と重要なポイントを説明します。

国民の自由と人権を守るため

国際関係の実態は、各国が自国の国益の最大化を目指して鎬(しのぎ)を削る戦いの場です。残念ながら、国際関係は、助け合いの精神よりは、利己主義が蔓延(はびこ)っているのが実態です。

このような世界で、国民の自由と人権を侵害する脅威はどこから来るのでしょうか。この点について、国内だけを見て政府と国民を対立の関係と捉えて「政府権力こそが国民に対する脅威であり、従って政府権力を憲法や法律で制約することこそが、国民の人権を守ることである」という考えがあります。確かに、政府権力が国民の人権の脅威となり得ることは、北朝鮮はじめ全体主義や専制主義国家の実態を見れば納得がいきます。

しかし、日本のように自由で豊かな民主主義国家においては、国民の人権に対する脅威の多くは国外からやってきます。オンラインのロマンス詐欺やサイバー攻撃の多くが国外から来ているのは常識ですが、重大なのは、外国政府や外国組織によるスパイ活動です。このような国外からの脅威を防止しなければ、結局は、国家制度が不安定となり、国民の自由と人権が損なわれてしまいます。

国外からのスパイの脅威を防止するには、政府に一定の権限を付与する必要があります。他方、このような権限は濫用されれば、国民の人権を侵害することとなるので、制度設計には慎重を期す必要があります。制度設計の議論で重要なことは、憲法上の人権規定を理念的に掲げて硬直的に文理解釈をするのではなく、その制度が国民の権利自由を侵害する具体的な可能性と、外国の脅威から国民の権利自由を守る効果とを比較考量することです。例えばスパイ対策のための行政通信傍受については憲法21条に通信の秘密があるから一切認めないという姿勢ではなく、具体的な制度が、国民の通信の秘密をどのような範囲で制限することになるのか、その制度によって阻止できるスパイによる脅威と比較して許容できるものであるか、などを具体的に議論することです。実際、米国の連邦裁判所の判決を読むと、そのような議論が展開されています。何れにしろ、スパイ対策の最終目的は国民の自由と人権を守ることです。

多面的重層的な対策が必要

スパイ防止法制というと、一般的には、米国の1917年スパイ防止法などを連想する方が多いようです。これらの法律には参考とすべき点はありますが、スパイ防止のための法律や制度は多面的かつ重層的であるべきで、我が国の弱点は単一の法律で解決できるほど簡単なものではありません。仮に、米国のスパイ防止法と同じ内容の法律を制定したとしても、我が国のスパイ対策の実効性が大幅に向上する訳ではありません。

それでは多面的かつ多層的なス

しげた・ただよし　昭和二十六年生まれ。東京大学法学部卒業後、警察庁に入り、在イスラエル日本大使館一等書記官、防衛庁陸幕調査部調査別室長、群馬・埼玉県警本部長などを歴任した。日本大学危機管理学部元教授。「警察公論」「治安フォーラム」「軍事研究」などへの寄稿多数。著書に『シギント　最強のインテリジェンス』(江崎道朗氏との共著、ワニブックス)。

パイ対策とは何か。必要な要素を純粋防御、積極防御、攻撃的防御の3つに分けて列挙してみましょう。先ず、純粋防御面では、①秘密指定制度②防諜・保全担当部署の整備③人的保全④施設保全⑤情報システム保全（サイバーセキュリティ）―などがあります。次に積極防御面では、脅威（スパイ行為）を探知し解明した上で、実害が生じないように関係者に秘密裡に警告するなど必要な対策を取る、或いは、検挙摘発して脅威を排除することです。更に、攻撃的防御面では、脅威国の諜報組織に浸透して、その中枢情報を使って対策を行うことです。

我が国のこれら各分野に対する取り組みを見ると、進展がある分野もあるのですが、全般的には依然脆弱で、これが「スパイ天国」と呼ばれる所以ではないでしょうか。今回は、紙幅の関係から、積極防御面に絞って議論したいと思います。

日米探知解明能力の格差

我が国のスパイの探知解明能力はどの程度でしょうか。スパイを探知して内々に必要な対策を取っても、これは公表しないので、結局、各国の探知解明能力は、摘発して事件化したものを比較するしかありません。

米国については、ＦＢＩ（連邦捜査局）による先端技術窃取、不正輸出やスパイ事件の検挙摘発件数（テロ事件は除く）は年平均して約30件で、韓国の産業技術の対外流出の摘発件数は年平均約20件だそうです。これに対して、我が国警察の検挙摘発件数は、年間0件から2件の間といったところでしょうか。

この格差はどうして生じるのでしょうか。格差の要因としては、情報の収集能力と処罰規定と2つの側面がありますが、より決定的なのは情報の収集能力です。

（1）情報収集力の違い

私は前世紀に国際テロ対策に従事して、欧米の治安情報機関と付き合った経験がありますが、印象的だったのは彼らの情報収集力の高さです。過激派の動向について、実に詳しく正確に知っていたのです。何故かというと、彼らの情報の収集手段が実に多様であったからです。

我が国であれば、尾行張込をして情報を収集し、司法令状を得て捜索差押をする、それに協力者からの情報が少しある位ですが、欧米では、秘密の通信傍受や信書開披、住居などの秘密捜索やマイクなどの監視機材の設置、更に身分仮装による潜入調査などを活用していたのです。

警視庁公安部ＯＢの著作によれば、公安部の尾行張込技術は世界一流とＦＢＩが評価したそうですが、そもそも欧米諸国では我が国ほど尾行張込はしません。人手が掛かる割に効率が悪いからです。我が国では尾行張込の技術を磨くしかないのですが、欧米では他に情報収集手段があるので、尾行張込に頼る必要がないのです。

更に21世紀の今や、サイバー空間が主要な活動空間となっています。当然、スパイ活動もサイバー空間を主要空間としています。工作員と協力者の関係を見ても、サイバー空間を経由してリクルートし、サイバー空間で情報を遣り取りし、サイバー空間で報酬を支払うことが可能となっています。工作員は必ずしも物理的に協力者と会う必要がなくなっているのです。こうなると尾行張込では対抗できません。サイバー空間を監視する必要があります。

米国ＦＢＩがどういう手法を使っているかは、公表された起訴状やＦＢＩ捜査官の宣誓供述書を詳細に読み込むと浮かび上がります。重要な手法は広義の通信傍受です。通信回線から傍受する、データセンターから必要なデータを入手する、容疑者の携帯端末をハッキングする、というのが主な手法です。入手できる情報は広汎です。例えば、音声通話、メール、ＳＭＳなどのテキストメッセージ、音声ファイル、ｉＣｌｏｕｄなどクラウドデータも入手できます。加えて、ヤフーやグーグル検索、グーグルマップでの検索履歴、携帯電話の位置情報など、つまり、サイバー空間における活動をほとんど全て把握できるのです。

最近は「シグナル」などの暗号化通信アプリが普及しデータは自動消去できるので、ＦＢＩでも情報収集できないと誤解している人がいます。しかし、起訴事例を見ると、容疑者の携帯端末をハッキングして「シグナル」による通信をリアルタイムで監視していたと見られる事例があります。

米国では、このような圧倒的な情報収集力を使って、スパイを探知検挙しているのですが、我が国警察にはこのような情報収集力は

ありません。

（2）情報収集権限の違い

FBIの広汎な情報収集力は何に基づいているのでしょうか。代表的なものが1978年制定のFISA（対外諜報監視法）です。FISAは、スパイやテロの予防や抑止という国家安全保障目的の行政調査権限を規定した法律で、行政通信傍受は第1篇と第7篇に規定されています。

第1篇は、米国内にいる者に対する通信傍受であり、米国内において特定の外国勢力又はその代理人と信じる相当の理由のある場合に行うものです。FISC（対外諜報監視裁判所）の個別命令を得て行われます。但し、外国大使館や領事館の傍受、緊急時の7日間以内の傍受は、裁判所命令なしに行うことが出来ます。典型的な傍受対象は、大使館や領事館、外交官、スパイ容疑者、テロ容疑者です。

第7篇は、2008年に制定された新しい通信傍受です。これは、米国内において米国外にいる者を標的にして通信傍受をするものです。有名なのは米国内のグーグルやアマゾンその他のデータセンターからデータを収集するものです。米国内のデータセンターには、Gメール、ホットメール、ヤフーメールをはじめ世界中の膨大な情報が蓄積されているため、極めて有効な手段です。米国外の非米国人を標的にして収集するため、裁判所の個別命令は不要です。但し、付随的に、米国人や米国内居住者の情報も収集してしまうので、傍受計画の枠組（標的決定手順、最小化手順、検索手順）を定め、米国人情報の使用や配布を極力限定しています。この枠組はFISCの認証を受ける必要があります。

行政通信傍受の特色は第1に、司法傍受よりも要件が緩和されていることです。司法傍受では重大な犯罪を疑う相当の理由が必要ですが、FISAでは外国勢力の代理人と疑う相当の理由でよいのです。第2に、FISCは秘密審理であり、傍受対象者には傍受の事実は事後でも通知されず、調査の事実は秘匿されます。通信傍受を通知すれば、国際関係を悪化させ、或いはスパイ容疑者に警告情報を与えることになるからです。第3に、本行政傍受の目的は、国家安全保障目的のインテリジェンス情報の収集ですが、同時に犯罪捜査目的があっても良いとされています。犯罪捜査での利用が可能なのです。第4に、本傍受で得た情報を裁判で犯罪の証拠として提出する際の裁判上の手続も法定されています。但し、通常は、容疑の解明が進めば、司法令状を得て司法通信傍受を行い、裁判では司法傍受で得た情報を証拠として提示するのが常態のようです。政府としても行政通信傍受の詳細は秘匿しておきたい情報ですので、裁判での公開は極力回避しているのです。

最後に、我が国の司法通信傍受制度がスパイの防止摘発に使えるか、確認しておきましょう。我が国の通信傍受法では、傍受令状の発布には「組織的重大犯罪」かつ「他の方法では証拠収集が著しく困難」という厳しい要件が課されています。そして捜査実務では、捜査の終盤で逮捕できるような証拠がある場合に、共犯者などの犯罪組織の全体像を把握するために使用されており、捜査の初期段階で捜査の突破口を開くためには使用できません。更に、傍受期間が最長30日と短く、スパイ取締りで使える制度ではありません。一方、諸外国の司法通信傍受制度は傍受要件が我が国よりも緩やかで、捜査の初期・中期段階でも通信傍受が可能なので、スパイ対策でも使えるのです。

米国との処罰規定の違い

次にスパイ防止に必要な処罰規定を見ていきます。2013年に制定された我が国の特定秘密保護法と米国の1917年スパイ防止法を比較してみましょう。我が国でも、米国同様に情報漏洩やスパイ行為には罰則が掛かるようになっています。但し、異なる点があります。第1に罰則の重さです。最高刑は、米国では死刑や終身刑までありますが、我が国では10年の拘禁刑が最高です。第2に犯罪の構成要件が微妙に異なっています。米国では犯罪の実態を基に立証を考慮した構成要件となっており、言い逃れを許さない仕組みになっています。第3は、併合罪規定の不存在です。米国では併合罪の規定がありませんので、量刑は罪数の数だけ積み上がり重い科刑となり易いのです。過去の裁判例では、中国やロシアのスパイ又は協力者であったラリー・ウータイ・チン（CIA職員）、オルドリッジ・エイムズ（同）、ロバー

ト・ハンセン（ＦＢＩ職員）などは終身刑を宣告されています。また、２０１０年にウィキリークスに情報を漏洩したブラッドレイ・マニングには情報漏洩で拘禁刑35年が宣告されました。

このようにスパイ防止法自体を見ても違いがあるのですが、より重要な違いはその他の処罰法令です。米国ではスパイ摘発に使用できるその他の処罰規定が多数存在し、これがスパイ摘発の実務を支えています。特に重要なものを２つ挙げます。ＦＢＩによる検挙事例を見ると、これらをスパイ摘発の「入口事件」として使い、或いは、これらの罰則違反だけで立件している事例が沢山あります。

第１は、外国代理人届出義務違反罪（合衆国法典18篇９５１条）です。これは、（外交官や領事館員以外の者が）外国政府の代理人として活動する場合に予め司法長官への届出を義務付けたもので、届出をせずに活動すると懲役10年以下に処せられます。外国の工作員は、外国政府の代理人ですが、当然のことながら届出はしないので、本条違反となるのです。但し、本条違反を立証するには、工作員が外国政府の指揮を受けて活動していることを立証する必要があります。現在では指揮連絡はサイバー空間で行われることが通常なので、指揮連絡の内容を通信傍受によって証拠化する必要があります。

第２は、虚偽供述罪（同18篇１００１条）です。これは連邦政府の業務に関して、虚偽の供述や虚偽の書類提出をすると違反となるもので、懲役５年以下に処せられます。ＦＢＩ捜査官や入国管理職員に対して嘘の供述をすると本条違反になります。また、セキュリティクリアランスの申請書にも適用されるので、申請書内容の真正を担保するのに重要です。スパイ協力者はＦＢＩに面接される際、黙秘しても良いのですが、大体やましいことを隠して嘘を付くことが多いので、本条違反が成立し、検挙に至ることが多くあります。

これらがどのように適用されるか、実例を見てみます。両事件とも秘密情報の漏洩は立証できなかったとみられる事案です。２００７年、内閣情報調査室の勤務員が警視庁公安部によって逮捕されました。彼はロシア大使館の工作員と８年間に亘って付き合い、その間、飲食の接待を受けたり現金を受領したりしていたのですが、結局、不起訴となりました。

米国では類似の事例で２０１７年に起訴された国務省職員キャンディス・クレイボーンの事件があります。彼女も中国の国家安全部の協力者と付き合い様々な利益供与を受けていたのですが、セキュリティクリアランスその他の手続における様々な報告で、中国人との関係を申告しなかったことが違法とされたのです。結局、司法取引で虚偽供述罪などを認めて拘禁刑40カ月の判決を受けました。行為の悪質性はクレイボーンの方が軽いと思いますが、それでも実刑となったのです。日米の処罰規定の違いです。

刑事司法の運用「寛刑主義」

我が国ではスパイ行為に対する探知解明能力や処罰規定も不十分なのですが、刑事司法の運用でもいろいろ問題があります。特に問題なのが「寛刑主義」です。「寛刑主義」とは、我が国の刑事裁判における量刑の特徴を、東京大学先端科学技術研究センター教授の玉井克哉氏が形容した言葉です。

我が国の刑事司法は、「善良な犯罪者」を前提として制度が運用されています。その前提は、犯罪者は根っからの悪人ではなく、悔い改めて日本社会に復帰したい人々であるという思い込みです。ここでは重罰を科すのではなく、社会復帰を促すのが基本となります。これは多分、大多数の日本人犯罪者については正しい運用であろうと思います。また、この「寛刑主義」は、失職などの社会的制裁で補完されていたのです。

しかし、外国のスパイやサイバー攻撃を仕掛けてくる人々はどうでしょうか。彼らはそもそも日本社会に復帰したいなどとは考えない人々です。或いは、トクリュウなど犯罪企業的な集団も増加しています。彼らに対しては「寛刑主義」は意味をなしません。

これで思い出すのは、北朝鮮の工作員に対する量刑です。彼らは対日工作のために工作船を使って海から密入出国を繰り返していました。前世紀に警察は海岸を警戒して多くの工作員を逮捕してきましたが、裁判所の量刑の相場は、出入国管理令違反や外国人登録法違反で、懲役１年執行猶予３～４年でした。裁判確定後は国外退去処分です。裁判が終われば北朝鮮に帰国できたのです。北朝鮮では工作員に対して「逮捕されても６

カ月で帰国できるぞ」と言って送り出していたと言います。これでは、刑罰の抑止力は全くありません。日本人拉致問題は、我が国の裁判所の「寛刑主義」にも責任の一端があったのではないでしょうか。

また、最近の事例では、産業技術総合研究所の中国人研究者が研究データを中国に不正に送信して、中国で特許登録をする事案がありました。2025年2月に第1審判決がありましたが、これも懲役2年6月執行猶予4年で、実刑判決は免れています。

これが我が国の裁判所の量刑の相場なのです。時代遅れとしか言いようがありません。しかし、この「寛刑主義」は、「裁判官村」が慣行として形成してきた量刑相場であるために、個々の裁判官では変えることができず、他方、誰も責任を負わないのです。犯罪の実態を直視して、特に我が国に帰属意識のない外国工作員や協力者などスパイ活動をする者に対しては、量刑相場を再考する必要があるのではないでしょうか。

何を今後なすべきか

このようにスパイ防止のための積極防御面をみても、スパイの探知解明能力（通信傍受を含む行政調査権限）、処罰規定、刑事司法の運用の各分野で、我が国は米国をはじめとする先進民主主義諸国と大きく異なっています。効果的な対策を行うには、通信傍受を含む国家安全保障行政調査権限の創設、処罰規定の整備、刑事司法の運用、各分野での抜本的改革が必要です。

それでは、そのような抜本的な改革が現在の我が国で可能かというと、それは極めて困難です。国民の支持が得られないからです。

国民の支持が得られない最大の理由は、国民が世界標準である諸外国のスパイ防止のための法律制度やその運用実態を知らないからです。そもそも、我が国の法学者や行政学者のほとんどは、諸外国の国家安全保障のための法律制度を研究していません。無知なのです。我が国の行政法学の大家である塩野宏東大名誉教授は、教え子の北村滋氏（元国家安全保障局長）に対して「安全保障のことはよく分からない」と自認しています。また、政府事務当局も研究していません。昨年、サイバー安全保障の能力向上に向け政府有識者会議が開催されましたが、事務局

提出資料には米国の行政通信傍受法制について基本的な誤解がありました。このような状態で、行政通信傍受制度の創設を議論しても、憲法の「通信の秘密」の理念闘争や政治闘争に陥る可能性が高く、人権に配意しつつ、同時に真に機能する効果的な法律を制定するのは困難でしょう。

他方、先進民主主義国家は全て「通信の秘密」を重要な人権としていますが、同時に国家安全保障のための行政傍受を認めています。従って、政府が取り組むべきなのは、専門部署を設置して、特に米英両国の国家安全保障のための行政調査に関する法律と実務を徹底的に研究することです。勿論、この分野は法律や一冊の教科書を読んで分かるようなものではありません。各国とも実務の実態はなるべく秘匿しています。全て開示してしまえば、スパイ対策に支障が生じるからです。従って、政府開示文書を丹念に読み解く作業が必要で、研究には時間と労力が掛かります。しかし、これが効果的な行政調査権限法を制定する最短・最良の方策であると考えます。研究成果は国会はじめ関係者で共有して、議論の資料とすべきです。なお、江崎道朗氏が本誌先月号で、このような調査研究を「国家安全保障戦略」（2027年「中間見直し」予定）で義務付けるよう提唱されています。

次に、処罰規定についても研究対象とするべきですが、今すぐにでも立法可能な処罰規定は、米国の外国代理人届出義務違反罪と虚偽供述罪です。これらは、行政通信傍受ができないと効力は半減するのですが、それでも一定の効果はあるので、この2罪は早期に制定すべきでしょう。まさか、この2罪創設について、憲法違反を主張する学者はいないでしょう。憲法38条の黙秘権は、虚偽供述の権利ではありません。

最後に、寛刑主義については、「量刑ガイドライン」を制定すべきでしょう。米国では1984年量刑改革法に基づき、「合衆国量刑委員会」が設置されました。「量刑委員会」は法律家や有識者で構成され、「量刑ガイドライン」を制定して、定期的に見直しています。同時に、全米の連邦犯罪の量刑データを収集して年次報告書を作成しています。我が国も量刑委員会を設置して、量刑の過程を可視化する必要があると考えます。