

スパイ防止法推進の動きに反撃を！

井原 聰（東北大学名誉教授）

はじめに

この（2025年）7月14日松山市内で、「（公務員を対象に）極端な思想の人たちは辞めてもらわないといけない。これを洗い出すのがスパイ防止法です」という思想の自由、内心の自由、基本的人権を侵害する暴言が公党の、しかもスパイ防止法案を国会に提出した代表者によって語られていた、という^{注1)}。

また、スパイ防止法を推進しようとする自民・維新・国民・参政・保守の与野党グループ（以下、与野党G）は口をそろえて、スパイ防止法は、国家の安全保障に重要な情報の漏洩を防止し、外国その他の勢力による我が国の独立及び国民の安全に対する危険を未然に防止し、技術・産業・外交・防衛等の基幹的利益を保護し、もって国民の安全と国家の存立を確保することができる、という。そのうえで、「先進国でスパイ防止法がないのは日本だけ」「諸外国は普通にやっている。日本が異常だ」「国際標準に合わせないと国際協力ができない」「日本はスパイ天国」と「合唱」する^{注2)}。

与野党Gの衆議院議席数は263/465で過半数233議席を越え、参議院でも161/248で過半数129議席を超えており、議会制民主主義を破壊するいつもの強行採決の危険性がないわけではない。法案が出そろっていないからか、一部を除いてメディアも取り上げ方が低調であったが12月に入ってやや取り上げ方が増えた。最も法文がまとまるためには与野党G内での調整もかなりかかるだろう。しかし、高市首相の意気込みから2026年の通常国会での成立の見通しがないわけではない。審議が始まれば反対の声を上げないとまがないと見える。国会での30数議席程度の差なので、立憲民主党が動搖しなければ、反撃し、押し返すことも可能かもしれない。

そのためにも、提出されるであろうスパイ防止法案関連の特徴、問題点を予測し、明らかにしておかなければならぬ。筆者は法学者ではないが、この間、衆議院内閣経済合同委員会で「経済安全保障推進法案」に反対する陳述を、また参議院内閣経済合同委員会では「重要経済安保情報の保護及び活用に関する法律案」（経済秘密保護法案）に

反対する陳述を行いその後を見守ってきたかわりで、経済安保を語らって日米一体となった軍事同盟推進の日本側の総仕上げともいえるスパイ防止法の成り行きを憂慮してきたので、今なぜ、かつて廃案になったスパイ防止法案のようなものが登場するのかを考えたい。

1.かつてのスパイ防止法案に触れて

戦前、治安維持法（1925）、改正軍機保護法（1937）、軍用資源秘密保護法（1939）、国防保安法（1941）などで思想の自由、学問の自由、表現の自由、出版の自由、報道の自由などが奪われ、侵略戦争に国民を駆り立てた歴史を忘れてはならない。機密情報、技術の流出の防衛などは現行法の刑法をはじめ国家公務員法（1947）、外為法（1949）、入管法（1951）、自衛隊法（1954）、日米相互防衛援助協定に伴う秘密保護法（MSA協定、1954）、不正競争防止法（1993）、特定秘密保護法（2013）、共謀罪（改正組織的犯罪処罰法第6条の2「テロ等準備罪」）（2017）、GSOMIA（軍事情報包括保護協定（2019）、重要経済安保情報保護活用法（2023）などで十分対応できると考える（もっとも筆者は特定秘密保護法や共謀罪法、重要経済安保情報保護活用法などは廃案にすべきと考えているが）。政府は山本太郎議員の質問主意書に応えて『各国の諜報活動が非常にしやすいスパイ天国であり、スパイ活動は事実上野放しで抑止力が全くない国家である』とは考えていない。^{注3)}といっている。

ところで1985年に出されたスパイ防止法案については当時多くの批判的見解が示された。代表的なものに日弁連の声明がある^{注4)}。この声明では「国家秘密」の定義が曖昧、広範で恣意的運用が可能、死刑・無期懲役など重罰で処罰対象が広い、基本的人権・民主主義原則との抵触、言論・学問・取材の自由を脅かす恐れが厳しく指摘され、戦前の秘密保護法制との関連と懸念などが指摘された。今回登場している与野党Gの一部の案文にも、この指摘はズバリ当てはまっている。

2.先進国のスパイ防止法に問題はないのか？

「ないのは日本だけだ」とする与野党Gに、同じ言葉を返したい。民主主義を抑圧する制度に対する

表1 米英独仏各国のスパイ防止関連法等の特徴、問題点、監査・監察制度について

国名	スパイ防止法等関連法律	制度・組織等	監査・監視関連法	監査・監察制度
米国	・かつてスパイ防止法(1917) ・国家安全保障法(1947) ・経済スパイ法(1996) ・愛國者法(2001) ・営業秘密保護法(2016)	・CIA ・FBI ・NSC 国家安全保障会議など	・外国情報監視法 ・USA自由法 ・大統領令14086号 ・公益目的の内部告発も处罚対象	・FISC裁判所 ・議会情報委員会 ・監察官制度 ・プライバシー及び市民的自由監視委員会(PCLOB)により強力な監視が行われるが透明性を欠くことも
英国	・保安局法(1989) ・諜報活動法(1994) ・検査権限法(2016) ・国家安全保障法(2023)	・M15 軍事情報部第5課 ・M16 秘密情報部 ・GCHQ 政府通信本部 ・DI 国防情報局 ・JIC(合同情報委員会)など	・ダブル・ロック制度 ・公益目的の内部告発も处罚対象	・検査権限規制法(2000) ・監視権限が行政と司法から監視される ・関連する令状制度・監視制度を包括的に整備
独国	・刑法§94～ ・連邦情報庁法(BND法)1990 2016大幅改正 ・ドイツ連邦データ保護法(BDSG)： ・G10(2001)基本法10条	・連邦憲法擁護庁 ・連邦情報局 ・事務保安局 など	・ダブル・ロック制度 ・国外通信の大規模収集による恣意的運用や通信の機密性侵害 ・報道の自由への影響を懸念	・議会監視委員会 ・独立監視評議会 ・ドイツ連邦憲法裁判所は連邦情報局のグローバルで大規模な監視の実行を違憲とした ・G10審査会、データ保護監督官が強力に監視
仏国	・フランス諜報法(2015) ・外国エージェント登録法(Loi n° 2023-1358) ・軍事計画法(LPM 2024-2030)(2023)	・DGSE(対外治安総局) ・DGSI(国内治安総局) ・DRM(軍事情報局) ・DNRED(関税情報調査局)など	テロ対策名目で通信の過剰傍受が批判 ブラックボックスと通称される方法によるデータ収集	情報技術管理国家委員会(CNCTR)と憲法評議会による厳しい監視、国家情報自由委員会(市民の権利と自由を守るために十分保障がないと情報活動法に強い反対意見の表明)
日本	—	—	—	与野党Gが検討中の案の中には独立監視機関がなく、国会・司法の監視も限定的

る対抗措置関連の提起が「ないのは日本だけだ」と。表1に米英独仏のスパイ防止法と対抗措置についておおざっぱにまとめてみた^{注5)}。

アメリカはスパイ問題では話題がつきないが、「秘密の定義」が広く問題が多いとされる。また公益目的通報にも罰則があり、通信の秘密、言論・報道の自由の侵害が多く、加えて司法監視の弱さなどが長い間、問題とされつづけ、そのために対抗措置としての監査・監察も強化されてきたという。冒頭の「掛け声」の中には、この対抗措置としての監査・監察システムが全く抜け落ちている。米国では抑圧的な制限に対してFISA(外国情報監視法; 1978年成立)が外国の情報機関やスパイの活動を監視する手続きを定めている。そしてFISC裁判所は抑圧的となる監視や傍受の許可を検討するための特別裁判所となっているが、その裁判所ですら、通信の秘密、市民のプライバシー・自由の侵害、透明性など問題が多いとされているという。

イギリスの国家機密保護法・防諜法では内部告発の正当化が認められにくくされ、検査権限法2016が「秘密の通信傍受・監視・調査権」の使用を、独立して監督・承認するものとなっており、民主主義を抑圧する対抗措置として設置されている。

加えて検査権限規制法は「諜報機関・監視権限」の濫用を防ぎ、民主主義・法の支配を守るために制度となっている。しかし公益通報が处罚の対象となっており問題も大きいとされる。

ドイツの刑法§94は、国家の「対外安全保障」を害する「国家秘密の漏洩・不正伝達」の处罚条項で、G10通信秘密制限法を根拠とするG10審査会は情報機関による通信の秘密の制限措置(傍受・監視活動など)の必要性と合法性を審査・決定する独立した監視機関となっているが、透明性に問題があり、通信の秘密、言論・報道の自由の侵害が長らく問題となっているという。

フランスの諜報法(2015)は「諜報・国家安全保障/スパイ防止・秘密保護」関連の制度であり、CNCTR(情報収集技術に関する国家監督委員会)と憲法評議会による厳しい監視が行われているが、CNIL(情報処理および自由に関する全国委員会)は市民の権利と自由を守るために十分保障がないと情報活動法に強い反対意見を表明したという。CNCT(情報技術管理国家委員会)は情報機関による監視技術の使用が個人の自由を尊重しつつ適切に行われているかを監督する、フランスの独立した行政機関となっているが過剰監視が問題になっ

ているといわれる。

米英独仏いずれの国もスパイ関連の法律による抑圧的措置に対して、対抗措置と制度がビルトインされているが、民主主義をまもる制度や組織になっているのか否かが現在も問題とされているといつてよい。

与野党 G は「スパイ先進国」のどこの国でもその運用に大きな問題を長く抱えてきていることは目をつぶり防諜・諜報法のみの検討でこれらの國の後を追おうとしている。

3. 与野党 G 及び自民・維新合意書のスパイ防止法案等について

そこで与野党 G が提出している「スパイ防止法」関連法案や各党のスタンスの主な特徴を表 2 にまとめてみた。さらに自民党・維新の党連携による政策合意したインテリジェンス政策を表 3 にまとめた。

与野党 G に共通する大きな特徴は上に述べたように、民主主義を抑圧するスパイ防止制度の提案にもかかわらず、民主主義を保証する措置として先進各国が取り入れてきた制度や組織を全く考慮していないことである。なかには人権や報道の自由を尊重するという表現があるが、その実現を担保する仕組みは欠けていて、多少踏み込んだものでも国会の情報監視審査会に触れる程度で、政治権力の暴走を止める仕掛けがなくきわめて危険な法案といえる。

スパイ防止にあたって設置すべき組織として「国家情報局」と「国家情報局長」を創設し、「国

家安全保障局」「国家安全保障局長」と同格とする「インテリジェンス部門」の圧倒的強化も、いま一つの大きな特徴といえる。

またどれもが防諜制度の確立 (FBI 型) を念頭に置いているが、仮想身分（他人に成りますことを合法化すること）による情報収集を可能とする法改正や対外情報庁創設のように CIA 型の諜報活動をも射程に入れていることに警戒しなければならない。欧米の「軍事国家」と肩を並べようとしてこの分野からも憲法改正を不可欠としている。

国民民主党のインテリジェンスに係る体制の整備、参政党の外国勢力の支持を受けた者の届け出義務及び報告義務も自民党・維新の党連立の合意内容と調整が可能で与野党 G の調整も案外早く進むかもしれない。参政党のあげている「特定秘密の保護に関する法律及び重要経済安保情報の保護及び活用に関する法律の一部を改正する法律案」では罰則の強化がうたわれているが、この点ではかつてこの法律に賛成した立憲民主党が動搖する可能性も考えられる。

外国勢力による活動への罰則強化や対象者にはセキュリティ・クリアランス（以下、SC と略す。関係者の家族、職場の同僚、友人までが調査対象）の義務化を強制し、その監視を強化する。維新の党の省庁横断的情報要員の養成機関（戦前の中野学校を髪髄とさせる！）の設置、参政党の情報リテラシーの強化により、市民を監視下に置く体制と翼賛会的市民の育成が危惧される。

表3の自民党・維新の党の合意書によれば2027年度までに段階的にシステムを作り上げていく

表2 「スパイ防止法」をめぐる各党の提出法案、主な動き、特徴など

項目	法案提出もしくは準備状況	法案名もしくは主な特徴	事前届出	適性評価	教育的側面
自民	「「治安力」の強化に関する提言～安全・安心な日本を取り戻すために～」	■偽情報等の収集・分析・集約や偽情報等に対する対外発信等の対策を強化政策決定を支える情報収集・分析能力の強化 ■諸外国と同水準のスパイ防止法の導入に向けた検討 ■仮想身分による情報収集		すでに導入	
維新	■外国代理人登録法	■内閣情報調査室を「国家情報局」に格上げ ■内閣情報官を「国家情報局長」へ格上げ ■軍事情報部長は自衛官 ■独立した対外情報庁の創設	あり		省庁横断的な情報要員養成機関
国民	■インテリジェンスに係る態勢の整備の推進に関する法律案（インテリジェンス態勢整備推進法案）	■インテリジェンス態勢整備推進本部を設置す	外国による不当な影響力の行使の防止のための措置等	インテリジェンスに係る職務に從事する者等の安全及び適切な待遇の確保	国民の理解の増進及び信頼の向上
参政	■防諜施策推進法案 ■特定秘密の保護に関する法律及び重要経済安保情報の保護及び活用に関する法律の一部を改正する法律案		外国勢力の指示を受けた者の届出義務および報告義務	公益目的の漏洩も原則違法 報道の自由への萎縮効果あり	情報リテラシーの強化（広報・教育）

表3 自由民主党・日本維新の会連立合意書（2025年10月20日）

(五、インテリジェンス政策)

2025年検討開始
○インテリジェンス・スパイ防止関連法制（基本法、外国人代理人登録法及びロビー活動公開法等）
2026年通常国会
○内閣情報調査室・内閣情報官格上げ→「国家情報局」「国家情報局長」創設＝国家安全保障局、国家安全保障局長と同格
○「内閣情報会議」（閣議決定事項）→「国家情報会議」創設
2027年までに
○対外情報庁（仮称）創設
○情報要員（インテリジェンス・オフィサー）養成機関創設

ことが合意されているので、これに乗れる他の与野党Gは来年の通常国会で合意の手を打つことになるかもしれない。

4. スパイ防止法と研究者・技術者

スパイ防止法関連の法案が成立するとまっさきにその網にかけられるのが、国家公務員はもとより、先端科学・技術分野の研究者達、基幹インフラ事業者、サプライチェーンの事業者である。

1) 安全保障技術推進制度と K Program にかけられる SC と守秘義務と監視の目

安全保障技術研究推進制度（以下推進制度と略）（約100億円前後）の目的が装備開発（兵器開発）にあることが明らかにもかかわらず、先進分野の研究者たちの応募が減少するどころか増加している。基礎研究だから、いや民生用研究だから、いやデュアルだからと種々の言い訳を考えて応募し、これを認める大学当局が増え始めている。

また競争的研究費の配分機関でもある新エネルギー・産業技術総合開発機構（NEDO）と科学技術振興機構（JST）が各2500億円計5000億円もの基金を用意して公募するK Programでは、防衛省とはことなり応募に敷居がない。しかし、このK Programも装備開発（兵器開発）に誘導する仕掛けになっている。というのも、先日（6月13日）設置が決まった「重要技術戦略研究所（仮称）」－シンクタンク機能の創設で、「（科学・技術分野の）脅威の動向の監視・観測・予測・分析、国内外の研究開発動向把握^{注6)}」というまるで諜報機関のような研究所が内閣府に設置され、先端分野で優位性を確保するための研究課題K Programの研究課題としてJSTとNEDOに提起し、装備開発につなげるというのである^{注7)}。

この二つの競争的研究費が装備開発（兵器開発）にねらいがあることを実際に示しておく。

各省庁が年度ごとに作成する行政レビュー

トがある。まだ2023年度版までしか公表されていないが、各省庁の事業がどのように進展しているのかをレビューするものである。推進制度についてみると2020年度の総合評価に「防衛分野での将来の研究開発に資する基礎研究の発掘・育成により優れた先進技術を効果的・効率的に防衛省の研究に応用することは、技術的優越確保のために重

要」であるという。2023年度の外部有識者所見では「学術・産業分野への波及効果を想定した研究テーマを選定し、さらに応募者の研究を防衛のニーズにマッチングさせるため、研究期間中も一定のコミュニケーションをとり、ニーズ側のインプットを十分なものにすべき」とある。研究には防衛省の介入は一切ないとは表むきだけのことなのであろうか。

次はK ProgramだがNEDOの募集要項に「高感度小型多波長赤外線センサ技術の開発」6年間で50億円という課題であるが「その熱源探知能力から弾道ミサイルや高速飛翔体の発射検知及び追尾、また暗視センサとして安全保障用途で使用することができます」とある。またJSTの課題「無人機技術を用いた効率的かつ機動的な自律型無人探査機（AUV）による海洋観測・調査システムの構築」（5年間80億円）では「海洋における脅威・リスクをはじめとする海洋状況の早期把握が肝要である」と述べている。

以上からもわかるように推進制度とK Programは軍事研究が狙いであり、SCがしっかり守られているかをスパイ防止法の防諜システムによって監視し得る仕組みが必要だというのである。

2) 研究者・技術者等の監視

経済安保推進法、経済秘密保護法では特定秘密として先端の特定重要技術20分野の科学・技術指定がしきりに話題となった。次ページの図を参照（「読売新聞」電子版、2022/07/18 05:00）。

この分野で特定技術に選定されれば、研究成果、ソフト、プログラム、磁気記録、書画、設計図、研究データ、その他物的対象、研究開発環境施設・設備の各種届け出と守秘義務のみならず、人的対象

（研究者・共同研究者・助手・技師・学生・事務員等）の口をも封じなければならない。研究施設も

◆特定重要技術の選定に向け、 調査研究を進める20分野

	極超音速・輸送
	人工知能・機械学習・先端コンピューティング・マイクロプロセッサー・半導体・量子情報科学
	医療・公衆衛生(ゲノム学含む)・脳コンピューター・インターフェース
	宇宙関連・海洋関連
	バイオ・先端エンジニアリング・製造・ロボット・先端材料科学
	先端監視・測位・センサー・データ科学・分析・蓄積・運用・高度情報通信・ネットワーク・サイバーセキュリティー
	先端エネルギー・蓄エネルギー・化学・生物・放射性物質及び核

対象となり大学・研究機関への監視が強化され、外国人共同研究者の事前届出などが進行し、学会発表の萎縮が始まると考えられる。

これを可能にし、実行たらしめるのがスパイ防止法による監視なのである。もっとも仮にスパイ防止法が成立するようなことがあっても監視する人材や設備が直ちに揃うわけではない。とりわけ予算措置、人材投入がどこまで出来るのかこれも国会論戦の一つでもあるが、先端分野の研究者の監視が先行するものと考える。

5. 基幹インフラ事業者・特定重要物質を扱うサプライチェーン業者の監視

基幹インフラ事業者の数は電気(49社以下同じ)、ガス(25)、石油(18)、水道(23)、鉄道(5)、貨物自動車運送(5)、外航海運(3)、港湾運送(32)、航空(2)、空港(6)、電気通信(10)、放送(6)、郵便(1)、金融(64)、クレジット(9)の15業種、258社(2025年12月12日現在)であるが、この事業者が運用している重要電子計算機が厳しい監視対象となり、届け出が必要となる。機器装置類、プログラム、ソフト類の届出が義務付けられ、変更のたびに変更届が必要となる。時には企業秘密にかかわる内容の開示が求められるかもしれない。企業によっては重要電子計算機の設置は多様であり、258か所とは限らない。このような調査が各省庁によって実施され始めている。この業務に関わる担当者はSCの取得が義務付けられる。

特定重要物資を扱うサプライチェーン業者も政府の各種届出と必要に応じてSC取得が義務化されるものと考えられる、一方、特定重要物資を扱う研究者にも網がかけられる。対象物質種は膨大である。抗菌性物質製剤、肥料、永久磁石、工作機

隔離する必要が出てくる。対象者にはSCを取らせ、漏洩はないかを常時監視するシステムが喫緊に必要というのである。従来からの監視対象はもとより、ついで推進制度やK Program関係者が監視

械・産業用ロボット、航空機の部品、鉱物資源など13種で、鉱物資源にあっては実際に35種類の鉱物が現在のところ指定されている。これらを取り扱う事業者が届け出の対象となりSC取得や国際協調主義による商取引の慣例、経営秘密を破ることが強制される恐れが大きい。

これだけ膨大な事業者に秘密を守らせるにはSCだけではなく防諜体制が必要なのである。自由貿易主義、国際協調主義による平和的取引を破棄すれば緊張関係が生まれ防諜・諜報せざるを得なくなる。そういう道に高市政権は踏み込もうとしている。

おわりに

詳細な営業秘密、研究秘密、技術秘密、重要電子計算機、プログラム、ソフト類、SCによる人的情報等の吸い上げとそのデータの一極集中による情報支配に対抗する強力な組織や制度の検討なしに、政権に抑圧的権限を明け渡す危険を深く理解しておかなければなるまい。それこそ冒頭に述べた欧米の問題事例をしつかり教訓とすべきである。詳細はふれなかつたが、情報集中による目的外使用の危険、情報の散逸、漏洩リスクの増大など防諜制度(例えば米国のFBI)を持つ国でさえ発生している。

「戦争をする国」の制度として作られた諜報制度は、声を大にしてその危険性を強調しておきたい。

いうまでもなくこの制度は一朝一夕にできあがるわけではないが、走りだしたら止まらない制度作りで、小さく生んで大きく育てる典型的の制度といえる。まずは多くの対象組織(企業、大学、研究所等)の情報提供に係る業務増大と業務の非効率化、SC取得義務による人事の流れの目詰まり、国際交流・情報交換・連携の停滞、情報秘匿による発表の自由の萎縮、特許非公開による技術発展の阻害、やがて経済活動の停滞が起きるものと危惧する。政府が知られたくないとする情報が恣意的に秘匿され、市民の知る権利が奪われ、戦前に回帰するこの法律の成立を許してはならない。

軍学共同反対連絡会としても反対声明や反対の行動に出ようではありませんか。

注1) 「毎日新聞」7月17日

<https://mainichi.jp/articles/20250717/k00/00m/010/308000c>

注2) スパイ防止推進の専用HP参照

Spyboshi <https://www.spyboshi.jp/booklet-05/>