警察政策学会資料　第147号
令和８（２０２６）年５月

スパイ防止に必要な制度と法律

警察政策学会

テロ・安保問題研究部会

まえがき

最近の報道によれば、「スパイ防止法」の制定を提言する政党も多く、また、2025 年 10 月に発足した高市自民党内閣の「日本維新の会」との連立政権合意書には「インテリジェンス・スパイ防止関連法制の策定」が記載されるなど、スパイ防止法制に対して関心が高まっている。

しかし、現時点で、スパイ防止法制として、各政党の議論の対象となっているのは、特定秘密保護法の罰則強化や外国代理人登録法の制定程度であり、スパイ防止に必要な制度や法律の総体について十分な理解が共有されているのか、疑問がある。スパイ防止には、多面的且つ多層的な対策が必要であり、一つや二つの法律でこれを実現するのは難しい。

そこで本稿では、多面的且つ多層的なスパイ対策とは何か、必要な要素を、純粋防御、積極防御、攻勢的防諜に分けて、主に米国と我が国の現状を対比して論述した。

第 1 に純粋防御面では、〇秘密指定制度、〇防諜・保全担当部署の整備、〇人的保全、〇物的保全又は施設保全、〇情報保全、〇内部脅威対策、〇民間企業の防御措置と政府の協力などの諸点である。

第 2 に、積極防御面では、脅威を探知解明し、或いは検挙摘発して脅威を排除するための、〇通信傍受を含む行政調査権限、〇司法捜査権限、〇必要な処罰規定、〇刑事司法の運用の課題などの諸点である。

第 3 に、攻勢的防諜では、脅威国の諜報組織の活動そのものを利用し無力化する対策についてである。

これらの議論を前提に、筆者の提言として、最も重要なことは、英米スパイ防止制度と実務の包括的な調査研究であると考えるが、また、当面の改革としては、〇政府関係省庁の防諜・保全専門部署の抜本強化、〇外国政府代理人届出義務違反罪と虚偽供述罪の制定、〇量刑委員会の創設を提言した。

本論考が、我が国のスパイ防止のための制度や法律についての議論において、何らかの貢献ができれば幸いである。

テロ・安保問題研究部会
部会長　茂田　忠良

スパイ防止に必要な制度と法律

茂　田　忠　良

＜目次＞

最近の報道によれば、「スパイ防止法」の制定を提言する政党も多く、また、2025 年 10 月に発足した高市自民党内閣の「日本維新の会」との連立政権合意書には「インテリジェンス・スパイ防止関連法制の策定」が記載されるなど、スパイ防止法制に対して関心が高まっている。

しかし、現時点で、スパイ防止法制として、各政党の議論の対象となっているのは、特定秘密保護法の罰則の強化と拡張、及び外国代理人登録法の制定程度であり、スパイ防止に必要な制度や法律の総体について十分に理解されているのか、疑問がある。

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、主として米国の制度との対比で、必要な視点と重要項目を説明したい。

【註】この分野の研究においては、関係する米政府文書が開示されていないことが多々ある。また、米政府の公式規則集やウェブサイトには既に廃止された規則類が有効なものとして掲示されていることも多い。本研究では、そのような不明瞭部分（現在、有効な規則類は何か）を相当解明できたと考えているが、なお誤りがあれば、御指摘いただけると幸いである。

1　スパイ防止は国民の自由と人権を守るため

（1）国際政治の現状とインテリジェンス（広義のスパイ活動）

そもそも、国際関係、そして国際政治の基本原理は何であろうか。

この点について、帝国主義華やかなりし 1848 年、英国で首相や外相を歴任したパーマストン卿が、下院議会で「我々には永遠の同盟国も不変の敵国もない。永遠かつ不変なのは我が国益である。国益追求こそが我々の義務である」旨の演説をしている。

このような国際政治観は 19 世紀の遺物と考える人がいるかも知れないが、米国の国家シギント機関 NSA は、現在でも同様の認識を持っている。即ち、1989 年の内部研究資料[1]に、「国家には友人も敵も存在しない、在るのは国家利益だけであると言われる」「今日の友人や同盟国も、いつまでも友人や同盟国である訳ではない」という記述がある。同資料は機密文書であるが、情報公開請求によって 2007 年に開示された。開示文書は、白塗りされた不開示部分が多くを占める文書であったが、当該部分は白塗りされずに開示されたのである。つまり、NSA はこの文言を開示しても差し支えのない、当然の認識であると考えているのである。筆者は現職の公務員時代にインテリジェンスに関わってきたが、この感覚こそ、世界のインテリジェンス業界の常識である。

現在の国際関係の実態を、虚心坦懐に観察すれば、各国が自国の国益の最大化を目指して鎬（しのぎ）を削る戦いの場であることが分かる。ロシアによるウクライナ侵略、イスラエルとイランやハマスとの戦い、中国共産党政権による強圧的な対外政策を見れば、明白であろう。また、米国は、第二次世界大戦後、その圧倒的な国力（経済力、軍事力、政治力）を背景にパックス・アメ

---

[1] NSA、"Third Party Nations: Partners and Targets," *Cryptologic Quarterly, Vol.7 No 4,* winter 1989, accessed 9 March 2020, https://www.nsa.gov/Portals/70/documents/news-features/declassified-documents/cryptologic-quarterly/third_part_nations.pdf.

リカーナと呼べる国際秩序を維持してきたが、国力の相対的低下の結果その余裕を失い、トランプ政権の「米国ファースト」政策となり、赤裸々な国益追及路線に転換した。残念ながら、国際関係は、助け合いの精神よりは、利己主義が蔓延する世界であり、各国が国益を賭けて鎬を削る場なのである。

このような国際関係において諸国の国益の対立を調整する手段としては、先ず外交交渉がある。外交交渉では両者の合意が必要であり、合意できない場合の手段としては戦争がある。しかし、戦争は負けた場合の損失は甚大であり、勝った場合でも大きな損害を被る虞がある。リスクが大きい手段なのである。そこで、外交以上、戦争未満の手段が必要となる。それが、インテリジェンスである。国際政治において、インテリジェンスは、外交交渉、戦争と並ぶ主要な手段なのである。

（ア）外交以上、戦争未満のインテリジェンス

外交以上、戦争未満のインテリジェンス（広義のスパイ活動）には、様々な活動があるが、先ず、科学技術スパイや産業スパイがある。要するに技術を盗むことによって、軍事力や経済力、国力を増進する活動である。有名な事例には、ソ連や中国による核兵器開発がある。ソ連の核兵器開発に、クラウス・フックス、セオドア・ホール、ローゼンバーグ夫妻などの在米スパイ網が大きな貢献をしたのは公知の事実である。また、中国の核兵器開発では、在米スパイのウェン・ホー・リーやグオ・バオ・ミンが貢献している。また、最近の産業スパイの一例を挙げると、中国の江蘇省国家安全庁第 6 局が、2010 年代に中国の国産ジェット旅客機開発支援のため、ヒューミントとシギントを駆使して、多数の欧米企業から技術情報を盗んでいた事例が解明されている[2]。このように科学技術スパイや産業スパイは、幾つかの国家にとっては、例外というよりは常態である。

また、国家の基本体制に対する転覆活動もある。冷戦華やかりし頃、米国 CIA は、多くの国でクーデタなどによって政権転覆に取り組み、イラン、グアテマラ、ブラジル、チリなどで成功を収めてきた。また、ソ連共産党や中国共産党は、暴力による共産主義革命を輸出していた。戦後日本でも、1950 年代に日本共産党はソ連や中国の共産党の指令と指導を受けて、暴力革命に取り組んだ。そして、現在イランは、イスラム革命を輸出しており、そのため、革命思想を輸出し、代理勢力（プロキシ）に対して資金援助、軍事訓練や活動技術の提供、武器供与などを行っている。更に、革命の輸出には、しばしば国際テロの輸出も随伴する。

また、積極工作（アクティブ・メジャーズ）や影響力作戦という分野もある。この分野には、宣伝やメディア操作などによる世論工作、偽情報工作、政治工作、選挙介入など様々手法がある。ソ連や中国が、我が国の政策に影響を与えるために、政治家や有力者に対して積極工作を行っていたのは公知のことであろう。最近は、新しい情報ツールである SNS を使った偽情報による世論工作や選挙干渉などが注目されている。近時、中国による対日取組が強化されている。

---

[2] 茂田忠良「江蘇省国家安全庁第 6 局による経済スパイ」『警察政策学会資料』137 号（2024 年 12 月）1-20 頁。

更に、暗殺という手法もある。ロシアはソ連時代から、好んで国内外で暗殺を行っている。米国 CIA は 21 世紀に入りドローンを使った「テロリスト」殺害（Targeted Killing）を多数実行している。また、暗殺未満の破壊活動もある。米国とイスラエルは 2010 年頃イラン・ナタンツの核燃料濃縮工場をスタックスネットというマルウェアを使用してサイバー攻撃をかけ、ウラン濃縮用の遠心分離器多数を破壊した。

このように、インテリジェンス活動には、「汚い仕事」（Dirty Job）も含めて、幅広いものがある。

（イ）外交支援

外交交渉は、関係国の合意による利害の調整であるといっても、インテリジェンス活動と無関係ではない。外交交渉とはポーカーゲーム的側面があり、自分の手札を秘匿しつつ相手の手札を知ることができれば、優位に交渉を進めることができる。そこで、インテリジェンス活動によって、相手側の手の内を探る活動が行われる。有名な事例では、第 1 次世界大戦後のワシントン軍縮会議がある。米国が日本の外交公電を解読して交渉を優位に進めたことはよく知られている。

インテリジェンスによる外交交渉支援はこれに限られない。2013 年にスノーデンが漏洩した NSA 機密資料によれば、2009 年の G20 ロンドン会合では、英国シギント機関 GCHQ は通信傍受によって各国代表団の状況について適時適切な情報を首相以下の関係者に提供して評価されている[3]。また、2007 年のアラスカでの国際捕鯨委員会総会では、米国 NSA は日本代表団の通信傍受により米国代表団を支援している[4]。要するに、外交交渉を支援するために、インテリジェンス活動を利用するのは普遍的な事象である。

（ウ）戦争遂行支援・戦争遂行の一形態

古来、戦争とインテリジェンスも不可分の関係にある。むしろ、インテリジェンスは軍事と共に発展してきたとも言える。戦争や軍事作戦にはインテリジェンスが不可欠である。「彼を知り、己を知れば、百戦危からず」という有名な孫子の言があるが、軍事作戦の前提として、敵国状況や敵軍の状況を知る必要がある。2026 年 2 月に始まった米・イスラエルによるイラン攻撃では、イランのハメネイ最高指導者を始め指導層の行動予定を把握して、攻撃初日に精密爆撃によって多数の指導者を殺害している。また、同年 1 月のベネズエラのマドゥロ大統領拉致作戦でも、マドゥロ大統領の動向と所在地の把握に米国の諜報力が発揮されている。

また、戦争では、敵国、敵軍に対する情報収集のみならず、戦争遂行支援、或いは戦争遂行の一形態としての様々なインテリジェンス活動が行われる。現在進行中のロシア・ウクライナ戦争でも、後方攪乱のための破壊活動や暗殺、SNS などを場とした欺瞞・宣伝などの情報作戦、更には、通信システムやインフラに対するサイバー攻撃も行われている。これらはインテリジェンス活動であり、インテリジェンスなしに戦争遂行は不可能である。

---

[3] 茂田忠良「米国国家安全保障庁の実態研究」『警察学会資料』82 号（2015 年 9 月）205-207 頁。
[4] 茂田ウェブサイト「外交交渉や国際会議におけるシギント活動（１）米国」（2025 年 5 月 4 日）、https://shigetatadayoshi.com/2025/05/04/us-sigint-activities-on-diplomatic-negotiations-and-summit-meetings/

（エ）政策決定支援

そして、インテリジェンスの重要な機能として、国家指導者による政策決定を支援するための、情報の提供がある。各国が国益を賭けて鎬を削る国際政治の場で、国家指導者が外交や安全保障に係わる政策を決定するに際しては、世界情勢や関係国について正しい情報を適時に入手する必要がある。

我が国で、インテリジェンスと言うと、この政策決定支援が想定されるようであるが、正に、これは「国家インテリジェンス」の中核的概念である。

（オ）防諜機能（セキュリティ・サービス）

上記のように、インテリジェンス活動は、国益を賭けて、様々な分野で攻勢をかけており、これに拱手傍観しているようでは、国益を損ねてしまう。そこで、各国とも、国家安全保障の観点からこれに対抗して主として国内で活動するインテリジェンス機関を設置している。これがセキュリティ・サービス[5]である。

欧米のセキュリティ・サービスは、警察・法執行組織の一部局として設置されている場合と、警察・法執行組織とは別組織であるが内務大臣など警察担当大臣の指揮下に置かれている場合がある。前者の例には、米国の FBI 国家安全保障部門やデンマーク PET やノルウェーPST があり、後者の例には、英国セキュリティ・サービス、フランス DGSI、ドイツ BfV、カナダ CSIS、豪州 ASIO などがある[6]。

セキュリティ・サービスによる対諜報活動は、平時においても重要であるが、特に戦時には死活的重要性を帯びる。現下のロシア・ウクナイナ戦争では、ウクライナのセキュリティ・サービス SBU の活躍が広く知られている。政府職員や政治家の対露協力者の摘発、ロシア諜報機関に SNS などでリクルートされた協力者による軍事・治安情報の収集やテロ・破壊活動の阻止、サイバー攻撃への対処、ロシアによる情報工作の暴露など、ロシアの諜報工作への対抗に大きく貢献している[7]。本稿執筆の時点（2026 年 4 月）でも、SBU のウェブサイトには殆ど連日検挙摘発の成果が掲載されている[8]。SBU の貢献がなければ、ウクライナの国土防衛戦は国内から崩壊していたであろう。セキュリティ・サービスは、国防のため必須の機能である。

上記はインテリジェンス諸活動の骨子を述べたに過ぎず、インテリジェンスにはその他の広汎な活動形態が存在する。

---

[5] セキュリティ・サービスは、主として国内において国家安全保障のためのインテリジェンス活動を行う組織である。歴史的に国家安全保障に対する主な脅威は、外国機関のインテリジェンス活動（Intelligence）、暴力的な政権転覆活動（Subversion）、テロ(Terrorism)であったので、セキュリティ・サービスの主任務は、防諜（C-I）、政府転覆活動の阻止（C-S）、テロ対策（C-T）の 3 つであった。21 世紀に入り、大量破壊兵器（WMD）の拡散防止対策の重要性が高まり、同対策（C-WMD）もセキュリティ・サービスの主要業務となっている。

[6] フランスやカナダのセキュリティ・サービスは、元は警察の一部門であったが、現在は、警察から分離されている。

[7] 茂田忠良「ウクライナ戦争の教訓～我が国インテリジェンス強化の方向性」『警察政策学会資料』125 号（2022 年 9 月）23-35 頁。

[8] https://ssu.gov.ua/en/novyny

以上を要約すると、国益を賭けて鎬を削る国際政治において、その闘いの主たる手段は、戦争（軍事力）と外交、そしてインテリジェンス（広義のスパイ活動）の３つであり、インテリジェンスの活動分野は広汎に及んでいる。インテリジェンスは、平時にも戦時にも、国益を賭けて闘っているのである。

なお、学説的には、インテリジェンスとは上記（オ）の政策決定支援機能（政策決定者への情報提供）のみを指し、政権転覆、破壊工作、暗殺、世論操作、選挙干渉、秘密政治工作などの各種の秘密工作は、本来のインテリジェンスではなく、インテリジェンス機関に付加的に与えられた任務であるとの立場（狭義説）[9]もある。しかし、筆者は、インテリジェンス機関やこれに準じる機関[10]が行う諸活動はすべてインテリジェンス活動であるという立場（広義説）に立っている。確かに、仮に我が国がインテリジェンス機関や体制を整備する場合、秘密工作に対しては慎重な立場となるであろう。我が国と同じく第二次世界大戦の敗戦国であるドイツの諜報機関 BND も抑制的である。しかし他方、我が国に脅威をもたらし得る諸国のインテリジェンス活動は上記のように広汎なものである。我が国に対する脅威を正しく認識し、これに対抗するためには、世界のインテリジェンス機関が行う活動全体を分析の対象とする必要があるのである[11]。

（2）スパイ防止は国民の自由と人権を守るため

国際政治の現状とインテリジェンスの実態を前提として、ここで確認しておくべき視点は、スパイ防止は何のためか、ということである。それは、直接的には国家安全保障の確保であるが、究極の目的は、それを通じて国民の自由と人権を守るためである。

現在の世界で、国民の自由と人権を侵害する脅威はどこから来るのであろうか。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、自国の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ある。確かに、政府権力が国民の人権の脅威となり得ることは、北朝鮮などの全体主義国家や専制主義国家の実態を見れば納得できる。

---

[9] 元 CIA 分析官のシャーマン・ケントの定義が有名である。

[10] 筆者は、インテリジェンス機関に準じる機関としては、共産党やイラン革命防衛隊を念頭に置いている。そもそもソ連共産党は共産主義革命のための工作機関として発足し、その組織原理や組織技術は 19 世紀ロシアの秘密の革命･テロ組織の伝統を継承している。そして、国内で権力を掌握した後も、対外的に工作機関としての性格を維持し、各種の非合法な工作活動を行ってきた。また、各国共産党はソ連共産党をモデルに組織されたのである。一方、イランの革命防衛隊（特にその対外部門であるアル・クッズ部隊＝エルサレム部隊）は、エルサレム解放を掲げ、イスラム革命の輸出、代理勢力（ハマス、フーシ派、ヒズボラ、イラク・シーア派民兵など）支援、反体制派の監視攻撃などの海外秘密工作、サイバー攻撃などに取り組んでいる。これらの組織は、欧米流のインテリジェンス機関とは言えないが、明らかにインテリジェンス機関としての性格も併せ持っていると言える。

[11] 世界の全ての国が、本文に述べたような広汎なインテリジェンス活動を行っている訳ではない。幅広い活動を行っている代表的な国としては、中国、ロシア、北朝鮮、イラン、米国、イスラエルで挙げられる。英仏は米国やイスラエルより限定的であり、ドイツは更に抑制的である。

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くる。オンラインの投資詐欺やロマンス詐欺、サイバー攻撃の多くが国外から来ているのは常識であるが、重大なのは、外国政府や外国組織によるインテリジェンス活動(スパイ活動)である。例えば、重要な政治情報を盗まれて国際関係で不利な立場に立たされる。影響力工作によって国の政策立案過程に干渉される。或いは選挙干渉によって公正な選挙が成り立たなくなる。国民の努力の結晶である科学技術や産業技術を盗まれて、国富を奪われてしまう。このような国外からの脅威を防止しなければ、国民の自由と人権を保障すべき国家制度が不安定となり、また時には、直接的にも国民の自由と人権が損なわれる。

そこで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る。先に述べた欧米のセキュリティ・サービスは皆そのための権限を付与されている。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る。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な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衡量することである。

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ある。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る。

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あり、この視点を忘れてはならない。

２　スパイ防止には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者が多い様である。また、最近は米国等の外国代理人登録法も注目されている。これらの法律には参考とすべき点はあるが、スパイ防止のための制度や法律は多面的且つ重層的であるべきで、我が国の弱点は一つ、二つの法律で解決できるほど簡単なものではない。仮に、米国 1917 年スパイ防止法や、米国の外国代理人登録法（FARA）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が大幅に向上する訳ではない。

それでは多面的且つ多層的なスパイ対策とは何か。必要な要素を、純粋防御、積極防御、攻勢的防諜に分けて列挙してみよう。

第 1 に純粋防御面では、①秘密指定制度、②防諜・保全担当部署の整備、③人的保全（Personnel Security、セキュリティクリアランスなど）、④物的保全又は施設保全（Physical Security）、⑤

情報保全（Information Security）などがある。

第 2 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防護対策を取る、或いは、検挙摘発して脅威を排除することである。

第 3 に、攻勢的防諜では、脅威国の諜報組織の活動そのものを利用し無力化する対策であり、例えば、脅威国組織に浸透して、その中枢情報（対日工作についての内部情報）を入手した上で対策を行うことが含まれる。

我が国のこれら各分野に対する取組を見ると、近時進展がある分野もあるが、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かと考える。以下、それぞれの分野について、米国との対比で我が国の課題を見ていくこととする。なお、米国と対比する理由は、第 1 に、米国は我が国が正式の条約で結ばれた唯一の同盟国であり、我が国のスパイ対策では、米国のスパイ対策の実態を認識し、調整を図る必要があること、第 2 に、米国の資料が相対的に多く開示されており、研究し易いためである。

3　純粋防御面

先ず、純粋防御面では、2013 年の特定秘密保護法の制定によって大きな進展が見られたが、実務経験者として見るとまだまだ改善を要する点が多い。立法に関与された方々は、残された課題を十分に理解しているものの、強い反対運動の中で漸く成立した法律であって改正には相当の困難が予想される。そこで、後は運用で頑張るしかないと、問題点については沈黙を守っていると推察する。しかし、それでは欧米諸国並みの水準には到底達し得ないので、ここでは、重要なポイントに絞って課題を指摘しておきたい。

3－1　秘密指定制度（Classification）

特定秘密保護法は、米国の制度と比較すると脆弱な点が多い。例えば、我が国では秘密とは「公になっていないもの」（非公知性）の要件があり、閣議決定の『運用基準』[12]によれば、報道機関等によって公表されている場合は非公知性を満たさないとされる。他方、米国では 2013 年に元 NSA 職員のスノーデンが機密情報を大量に漏洩し、その多くが報道され、現在でも閲覧できる状態に

---

12 閣議決定『特定秘密の指定及びその解除並びに適正評価の実施に関し統一的な運用を図るための基準』改訂版（2025 年 12 月 26 日）（以下、閣議決定『運用基準』と略称する。）

Ⅱ-1-（２）非公知性「当該情報と同一性を有する情報が報道機関、外国の政府その他の者により公表されていると認定する場合は、たとえ我が国の政府により公表されていなくても、本要件を満たさない。」

ある。しかし、米国では、権限無き開示によって秘密は解除されない[13]のであり、これら漏洩情報の殆ど（即ち、その後に政府が秘密指定を解除した情報を除き）は現在でも機密情報である。従って、米政府が、これらの漏洩情報自体について真正性を前提として公開の場で議論の対象とすることはない。また NSA などインテリジェンス機関の職員は、漏洩情報を真正なものとしてコメントすると、国防情報漏洩罪（スパイ防止法 793 条違反）に問われる。このようにして不用意なコメントによって、実質的に情報漏洩が拡大することを阻止しているのである。この違いは実務では極めて重要な点である。

また、米国には「機微区画情報」（Sensitive Compartmented Information: SCI）という制度がある[14]。これは、機密、極秘、秘密などの秘密区分とは異なる制度で、諜報源や諜報手段の違いによって情報を機微区画に区分し、その情報にアクセスするにはそれぞれの機微区画についてアクセス承認を必要とする制度である。区画は、大～中～小の 3 層構造となっており、大区画にはコミント（通信諜報）、ヒューミント、衛星情報などの幾つかの区分がある他、全体では 100 から 300 の中・小区画があるとされている。この制度は、国家諜報長官室の事務局（アクセス統制プログラム監督委員会：Controlled Access Program Oversight Committee）が管理する諜報コミュニティ共通の制度であり、諜報コミュニティ間の情報共有を進めるには不可欠な制度である。我が国でも、特定秘密の管理については、各関係省庁で更に区画化をして管理していると推定するが、重要なのは、米国 SCI 制度のように関係省庁横断の情報コミュニティ共通の公式制度として、それぞれの機微区画へのアクセス資格やそれぞれの機微区画の保全教育などを統一して、情報共有推進の基盤とすることが重要なのである。

13　大統領命令第 13526 号「秘密指定された国家安全保障情報」（EO13526 “Classified National Security Information”）は、米国政府の秘密情報についての基本命令であるが、その 1-1 条（ｃ）項は「権限無き開示によって秘密は解除されない」旨を明記している。そして、本条に関して、Information Security Oversight Office, *Classified Information Nondisclosure Agreement Briefing Booklet* (2001) p73.は、「新聞やテレビなど公開のメディアで報道されたからと言って、秘密指定は解除されない。権限ある職員に秘密指定の解除を確認せずに、当該情報を伝達したり或いはその正確性を確認したりすることは、秘密漏洩に該当する」旨を警告している。

スノーデン漏洩情報は、その多くがウェブ上で誰でも閲覧可能であるが、依然として秘密として取り扱われているのである。

この点で興味深い秘密指定の実例は、元 CIA 工作員 Valerie Plame の事例である。彼女の CIA 勤務開始時期については、連邦議会宛の秘密指定のない政府書簡に記載され、且つ、米国下院資料として誰でもウェブで閲覧可能な状態にある（即ち、公知の事実である）。にも拘わらず、秘密解除手続きが採られていない以上、秘密であるとして、彼女の回顧録に CIA 勤務開始時期を記載することが認められなかった。この解釈は連邦ニューヨーク南部地区裁判所で支持されている。Valerie Plame Wilson, *Fair Game*, (New York: Simon & Wilson, 2007), p.306。控訴審でも同旨（連邦第 2 巡回控訴裁判所 2009 年）。

14 米国シギント機関は、第二次世界大戦開始前に、日本の外交用 B 型暗号機を解読していた。解読外交文書は MAGIC と命名され、1941 年 1 月に、その配布先は、大統領、陸軍長官、海軍長官、国務長官、参謀総長、海軍作戦部長、陸海の戦争計画の長、陸海のインテリジェンスの長の合計 10 人に限定された。米国では、これが SCI 制度の始まりとされている。

3－2　防諜・保全担当部署の整備

スパイの脅威に対抗して秘密を保全するには、関係官庁にその専門部署と専門家集団が存在する必要がある。防諜・保全担当部署は、我が国でも一応設置され或いは指定されているが、米国と比較するとその態勢と専門性には大差がある。

中央官庁の防諜・保全担当部署を見ると、米国では局や部レベルの専門部署が設置され専門家が配置されているが、我が国では、せいぜい課内の補佐レベルで担当するにとどまっている。また、米国の担当部署は、人的保全（セキュリティクリアランス、保全教育）、施設保全、情報保全、内部脅威の発見探知など保全全般を担当しているが、我が国ではそのような官庁は存在しない。

さて、日米で代表的な官庁を幾つか選んで、その態勢を対比してみよう。なお、担当職員数は殆ど公表されていないので、多くは推定であるが、概ねの規模感は理解できるであろう。

（1）米国の防諜・保全部署の例[15]

米国を見てみると、政府の中央組織として、国家諜報長官室に国家防諜・保全センターNCSC[16]が設置されている。

主な省庁では、先ず国防総省では、本省には諜報・保全担当次官（Under Secretary）の下に局次長レベル[17]の防諜の専任者 DDI（CL&S）[18]が置かれ[19]、実働組織としては、国防防諜・保全庁DCSA[20]が置かれている。DCSA は契約職員を含めると 1 万 5 千の巨大官庁である[21]。

次に国務省には、本省の専門組織として外交保全局 Bureau of Diplomatic Security があり、更に全ての大使館や領事館には保全担当の専門職員が配置されている[22]。外交保全局は、セキュリティクリアランスなどの人的保全、サイバーセキュリティ対策、公館警備に加えて、要人警護など、

---

[15] 「Security」の訳語としては、「安全保障」と「保全」が考えられるが、本稿では、防諜・保全担当部署名の「Security」については、「保全」と訳している。

[16] National Counterintelligence and Security Center、政府の防諜・秘密保全の統括組織。

[17] 国防総省 DDI は Assistant Secretary より下位の Director、国務省の DS の長は Assistant Secretary、CIA の Office of Security の長は Assistant Director、FBI の Counterintelligence Division の長は Assistant Director。省のトップは Secretary であるが、CIA や FBI のトップは Director である。従って、CIA や FBI の Assistant Director の訳語を局長とすることも考えられるが、本稿では部長としておいた。

[18] Director for Defense Intelligence（Counterintelligence, Law enforcement & Security）の略称。

[19] Office of the Under Secretary of War for Intelligence & Security, website, accessed 6 September 2025, https://ousdi.defense.gov/About-Us/Organization/?

[20] Defense Counterintelligence and Security Agency

[21] DCSA, *Fact Sheet 2025*, https://www.dcsa.mil/Portals/128/Documents/about/err/DCSA-Fact%20Sheet_Jan2025_vFinal.pdf

[22] 在外公館の保全担当専門官は、大規模や中規模の公館には専門官（Regional Security Officer: RSO）が常駐しているが、小規模公館の場合は、同一 RSO が数カ所の公館の担当を兼任しているようである。在外の RSO は、防諜では CIA の Station Chief や FBI の在外アタッシェ（Legal Attache Offices）と密接に協力する。

任務が広汎に及ぶせいもあるが、人員規模は契約職員などを含む全職員数は 5 万人以上、プロパー職員だけでも 3500 人以上いる[23]。

次に CIA を見ると、作戦総局内の防諜任務センターCounterintelligence Mission Center（CIMC）が対外防諜作戦（攻勢作戦を含む）の中核的担当部署であり、また管理部門にはセキュリティクリアランスを含む人的保全、施設保全や情報保全など CIA 自体の防諜を担当する部レベルの保全室 Office of Security（OS）がある。在外の CIA Station にも OS 職員又は OS 連絡要員が常駐している。これら 2 つの組織の人員数は公表されていないが、CIMC で数百人以上、OS で千人以上が勤務しているとみられる。

最後に FBI は、国家安全保障部門の防諜部 Counterintelligence Division が米国内全体の防諜を担当しており、全米 56 の全支局には防諜課が置かれている。担当職員数は大雑把な推定ではあるが 2000 人程度はいると考えられる。また、FBI 自体の内部脅威については、管理部門の保全部 Security Division が、セキュリティクリアランスを含む人的保全、施設保全、情報保全を担当しており、職員数は 1000 人以上とみられる[24]。

つまり、これら米国の省庁では、局や部のレベルで防諜や秘密保全を担当する部署が設置されており、人員規模は数百から数千に及ぶ規模である。

更に、国家諜報長官室の NCSC と共に FBI が政府の防諜の中心官庁となっており、秘密情報の漏洩が疑われる場合には、即座に FBI に通報して対応は全て FBI と協議することが法律によって義務付けられている[25]。また各官庁の防諜部門では、FBI を中心として人事交流も行われており、担当者の専門性が担保されている。このように FBI を中心として防諜・情報保全のネットワークが政府全体に構築されているのである。

（2）我が国の防諜・保全部署の例

我が国で、上記米国の省庁に対応するとみられる防衛省、外務省、公安調査庁、警察庁の態勢を見るといずれも貧弱である。これら 4 省庁の組織令や組織規則を見ても、本省庁の政令職や省令（府令）職レベルに防諜や秘密保全を専門に担当する部署が存在しない。防諜や秘密保全を担

---

[23] 米政府資料によると、2017 年現在で、外交保全局のプロパー職員数は約 3500 人、他官庁職員（主として警備担当の海兵隊員）約 2000 人、現地職員などの契約職員と支援職員が 4 万 6000 人弱、合計 5 万 1 000 人以上で、増加傾向にあった。US Government Accountability Office, *Report to Congressional Addressees: Diplomatic Security Key Oversight Issues*, September 2017, https://www.gao.gov/assets/gao-17-681sp.pdf

[24] 公表資料によれば、Security Division の人員は 2006 年時点で 1250 人以上とされる。

[25] 合衆国法典 50 篇 45 章 3381 条（e）項。(1) 号「各省庁は、外国勢力又はその代理人に対する秘密情報の漏洩を示唆する如何なる情報も、即座に FBI に通報しなければならない。当該省庁が漏洩源の特定のため採る爾後の全ての対応措置について、FBI と協議しなければならない。また、FBI が漏洩源を特定するために調査を行う場合には、職員及び記録への時宜を得た完全なアクセスを与えなければならない。」他の規定がある。

当する部署自体は存在する[26]のであるが、担当としての専任部署は、官庁の組織単位として重要な政令職の課や省令（府令）職である室レベルには存在せず、課内の課長補佐レベルの担当となっている。なお外務省は、実行上の組織として大臣官房総務課の中に情報防護対策室[27]を設置しているが、省令職でもなく、課長補佐級の者が責任者を務める小さな組織と推定される[28]。防衛省は、実働組織として大臣直轄の部隊として自衛隊情報保全隊が設置されているが人員は千人規模と言われており、米国国防総省の DCSA の 1 万 5 千人とは比べるべくもない。こういう態勢であるから、防諜や秘密保全の専門家の関係省庁間の人事交流などは望むべくもない状況であろう。

（3）我が国の態勢が貧弱な背景

但し、防諜や秘密保全の担当部署の人員態勢が貧弱である責任は、これら省庁が全責任を負うべきものではない。我が国では 1981 年に第二次臨時行政調査会が「政府機構及び純増を抑制し、スクラップ・アンド・ビルドを徹底すること」を提言して以来、新組織の設置や増員に当たっては同規模の削減を行うスクラップ・アンド・ビルドの原則が「省庁単位で」適用されて来た。その結果、新たな行政需要が発生しても、スクラップすべき組織や人員の財源がない省庁は行政需要に応じた態勢強化が図れないのである[29]。本来、防諜や秘密保全の業務については、政治のリーダーシップの下、組織や人員を純増で手当して強化すべきものなのである[30]。残念ながら、我が国にはその政治的リーダーシップが不足している。

---

[26] それぞれの省庁の組織令などから判断すると、防諜や秘密保全の業務は、それぞれ防衛省防衛政策局調査課、外務省大臣官房総務課、公安調査庁長官官房総務課、警察庁警備局警備企画課の所掌となっていると考えられる。

[27] 外務省報道発表「『情報防護室』の設置について」（2007 年 8 月 10 日）、
https://www.mofa.go.jp/mofaj/press/release/h19/8/1174871_810.html

[28] 2004 年には在上海総領事館の電信官が自殺する痛ましい事件が起きた。彼は、中国公安部員に弱みを掴まれ協力を強要され、協力を回避するために自殺したのであるが、米国であれば、このような事案は起きなかったであろう。実際、ソ連時代の 1981 年に在モスクワ米大使館の駐在武官がハニートラップを仕掛けられたが、対象となった陸軍将校 2 人は即座に申告したため不利益処分も受けず保護されている。上海の事件後、外務省では総務課に情報防護室が設置され保全態勢は強化されてはいるが、果たして専門家集団が形成されたかどうか、疑問である。

[29] 1970 年代までに多数の組織や人員を純増で増やしてきた省庁は、スクラップ財源が見つけ易いが、そうして来なかった省庁はスクラップ財源に苦労することになったのである。

[30] 「政府全体」で、政府機構及び純増を抑制し、スクラップ・アンド・ビルドを徹底することは望ましいとしても、それを「省庁単位」で実施することは、如何にも我が国らしい横並びの措置である。しかし、これは副作用として、各省庁の組織人員の規模を 1980 年頃の状態に固定化することであり、行政のダイナミズムを自ら否定する効果を生んでいる。

3－3　人的保全（Personnel Security）[31]

人的保全には、セキュリティクリアランス（背景調査と適格性審査）や保全教育などの狭義の人的保全（Personnel Security）と、職員の不正行為・情報漏洩・外国勢力との不正接触などの内部脅威の発見探知を行う内部脅威監視（Insider Threat Program）の二つからなるが、ここでは、狭義の人的保全、セキュリティクリアランス制度を中心に、米国の仕組を我が国と対比して紹介したい。

先ずに、セキュリティクリアランスの大きな流れを確認しておこう。米国の場合には、本人がスポンサー省庁を経て申請をする。申請に基づき、背景調査が行われて、審査裁定されるという構造になっている。これに対して日本の場合には、本人が自分から申請するのではなく、特定秘密にアクセスする必要のある職務に就いた者に対して行政側が告知をし、本人の同意を得て、調査が行われ、そして、評価が行われるという構造になっている。

さて、米国の情報関係のセキュリティクリアランスは、背景調査のレベルによって 2 つに分かれる。①Confidential（秘密）、Secret（極秘）情報にアクセスできる Tier3 又は NACLC、及び②Top Secret（機密）、SCI（Sensitive Compartmented Information: 機微区画情報）情報にアクセスできる Tier5 又は SSBI である[32]。①NACLC とは、National Agency Check with Local Agency Checks and Credit Check の略称であり、背景調査は主として国家機関（FBI、移民帰化局その他）の各種データベースへの照会、地方法執行機関への照会、金融信用調査からなり、不審点がある場合に更に追加調査が行われる。これに対して、②SSBI は、本人に加えて多数の関係者の面接インタビューが行われるなど、極めて詳細な調査である。そのため、調査や審査に日時を要し、平均①NACLC で数か月、②SSBI では半年以上かかったと言われる[33]。米国諜報機関で勤務するには、通常 Top Secret/SCI レベルのクリアランスを必要とする。

これに対して、日本のセキュリティクリアランス制度を見ると、最近まで国家機関への照会すら必須でないなど、そもそもセクリティクリアランス制度と呼べるのか疑問な程、脆弱なのものであった。後述するように、2025 年 12 月に運用基準が改正されて調査内容が強化され、漸く米国の①NACLC レベルに近付いたところである。しかし、米国でインテリジェンス機関員が通常必要とする②SSNI レベルとは依然として程遠いものがある。

それでは以下、セキュリティクリアランス制度の各項目について、詳細に見ていこう。

---

[31] 茂田忠良「警察政策学会第 25 回シンポジウム 経済安全保障 ショートスピーチ（2）米国のセキュリティ・クリアランスと背景調査」『警察政策』第 26 巻（2024 年）53-66 頁参照。
https://shigetatadayoshi.com/wp-content/uploads/2025/11/security-clearance-and-background-investigation2023symposium.pdf

[32] 後述するように、2022 年に調査方法の大改革があり、この結果、現在①NACLC の後継レベルは Moderate Tier（中位）、②SSBI の後継レベルは Higher Tier（高位）と呼ばれる。

[33] 2022 年に調査方法の大改革の結果、所要日数が短縮され、Moderate Tier（中位）で数週間、Higher Tier（高位）で数か月位になったと言われる。

（1）適格性の審査項目と審査指針

セキュリティクリアランスのための米国の審査項目や審査指針と、我が国の調査項目や評価の考え方などには、種々の違いがあるが、特に次の点が際立った違いである。

（ア）米国

先ず、米国の審査指針[34]で注目されるのは、「全人格的評価」（the whole-person concept）が打ち出されて、且つ、「適格性に関して少しでも疑念がある場合は、国家安全保障を優先して判断されるべきである（＝クリアランスを与えない）」とされていることである[35]。

「全人格的評価」とは、全人格、つまり全てが調査と審査の対象となるということである。「それはプライバシーだから言いたくない」というようなことは許されない。或る元 CIA 職員の回想によれば、CIA 入庁時にセキュリティクリアランスのための面接ではポリグラフを装着した上で諸々の質問を受けたが、その中で「貴方は奥さんに何か隠していませんか」と質問された。実は彼は過去に浮気をしたことがあり、それを奥さんに隠していたのである。彼は正直にその事実を述べた結果、セキュリティクリアランスを得て CIA に正式採用されたと回顧している[36]。私生活上の秘め事も弱点となり得るのであり、これを梃に脅迫を受ける可能性もある。従って、セキュリティクリアランスの面接では隠してはいけないのである。審査指針には「審査プロセスでの意図的な虚偽記載（供述）や非協力は如何なるものでも、重大な懸念事項である」[37]としている。

次に、審査項目で注目されるのは、最重要の審査項目として第 1 に「米国に対する忠誠心」を挙げていることである。且つ「前文」には、本人は「疑問の余地なく米国対して忠誠でなければならない。どのような監督も保全手続も個人の自己規律と尊厳には及ばない」と記載している。国家への忠誠心を重視しているのである。つまり、秘密漏洩は国家に対する背信行為であるから、国家に対する忠誠心が最大の抑止力なのである。

更に、過去のスパイ検挙事案を踏まえて、本人のみならず家族友人の外国との関係が、審査項目でも詳細に記述されている。これらを含め 13 の審査項目の記述は極めて具体的・詳細である。

（イ）日本

これに対して、我が国の特定秘密保護法の閣議決定『運用基準』Ⅰ-１-（１）では、「適性評価の実施に当たっては、プライバシーの保護に十分に配慮しなければならない」と記載し、且つ、適性評価のための調査については、閣議決定『運用基準』Ⅳ-１-（２）で特定秘密保護法 12 条 2 項に記載の調査事項以外の事項については調査してはならないと記載している（調査してはなら

---

34 政府保全責任者指令 4 号「国家安全保障審査指針」2017 年。政府保全責任者 Security Executive Agent とは、DNI 国家諜報長官である。
ODNI, *Security Executive Agent Directive 4: National Security Adjudicative Guidelines,* effective 8 June 2017.

35 同指針、 Appendix A “National Security Adjudicative Guidelines for Determining Eligibility for Access to Classified Information or Eligibility to Hold Sensitive Position,” 2(ａ)（ｂ）

36 なお、本人はこの CIA の採用面接を契機に、過去の浮気を妻に告白して謝罪し、他方、妻も夫に隠していた過去の出来事を告白し、夫婦仲が改善したそうである。

37 前掲、2（ｃ）。

ないのであるから、当然に評価してもいけないということであろう）。これらの規定から判断すれば、米国で行っているような「全人格的評価」を否定していると解釈せざるを得ない。

また、調査事項として、特定秘密保護法 12 条 2 項には国家に対する忠誠心が記載されていない。且つ、前記『運用基準』では、「評価対象者の思想、信条…については調査してはならない」と記載されており、これらから判断すると、我が国の秘密保護法制では、国家に対する忠誠心は、恰も秘密保持の意欲や能力とは関係がないかの如く扱われているのである。そもそも、全て国家というものは、国民の国家に対する忠誠を前提として存在している筈であるが、我が国にはこの常識が欠落しているのである。

更に、外国との関係については、『運用基準』の調査事項でも評価の考え方でも、これを重視する記載はない。秘密保護に関しては、外国との関係、接点の審査・評価が極めて大切なのは自明であるが、我が国の制度の枠組は、敢えてそれを目立たなくしているように見える。

その他、評価項目も、閣議決定『運用基準』Ⅳ-6 に記載があるが、特定秘密を漏らす虞がないなど抽象的な項目 7 項目が並んでいるに過ぎない。

（2）質問票

次に、セキュリティクリアランスの調査や審査の基本資料となる本人質問票を日米で対比してみる。

（ア）米国

セキュリティクリアランスのための米国の質問票は、SF86[38]という 136 頁にも及ぶもので、質問は広汎且つ詳細である。質問票の特色は先ず、虚偽供述や虚偽情報の提供は合衆国法典 18 篇 1001 条違反（虚偽供述罪）となり、刑事罰、免職その他の不利益処分の対象となることを、3 回以上に亘って記載し、最後の「確認」欄[39]ではそれを理解した旨の本人の署名を求めている点である。

また、質問項目は、背景調査や審査の実態と連動した内容になっており、調査員による実際の背景調査に役立つ情報の記載を求めている。例えば、過去 10 年間の住所と近隣の者の連絡先、過去 10 年間の職歴と上司の連絡先、過去 3 年以内の学校の教官や知人の連絡先、過去 7 年間本人を良く知る人 3 人の連絡先、離婚した配偶者全員の連絡先などの記述を求めている。また、外国関係の接点については詳細な記述を求めている。更に、同様の質問を微に入り細に入り繰り返し、性悪説に立つ質問構成となっている。つまり、記載漏れがあった場合に、過失による不記載という抗弁を許さず、即座に虚偽供述罪が成立する質問構成となっているのである。

（イ）日本

これに対して我が国の質問票は、閣議決定『運用基準』によれば、僅か 28 頁であり、米国と比較すると質量共に少ない。更に、質問票の虚偽記載については、「適性評価の結果に影響を及ぼすことがあります」と記載されているに過ぎない。質問票の記載には虚偽がないことが不可欠であ

---

[38] Standard Form 86 (Questionnaire for National Security Positions)（標準様式 86）、米国人事管理局が制定した様式。https://www.opm.gov/forms/pdf_fill/sf86.pdf

[39] SF86, p130.

るが、驚くことに、我が国では虚偽記載に対するペナルティが殆ど存在しないに等しいのである。

このように、セキュリティクリアランス制度を対比すると、米国では人間性悪説に基づき、不正にセキュリティクリアランスを得ようとする者がいる前提で制度を構築しているのに対して、我が国のセキュリティクリアランス制度はそのような者は存在しないという性善説に基づいているように見える。

（3）背景調査（人物調査）の具体的方法

具体的な調査方法は、日米で大きく異なるところである。

（ア）米国の新方式

米国は、2022 年に背景調査（人物調査）の方式を大変革して、「連邦職員ベッティング（適格性審査）調査基準」(Federal Personnel Vetting Investigative Standards)が導入された[40]。これは、従来とは全く異なる方式であり、時々の「調査」というよりも「継続的監視システム」への移行である。対象者に関する各種データ（犯罪、金融状態、海外渡航状態など）を常時継続的にコンピュータによって監視し、危惧すべき徴候が検知された際には徹底的に調査する方式である。また、面接インタビューは、従来の雇用主・近隣・知人に対する一律広汎な聞込みから、対象者本人に対する面接・インタビュー重視に移行し、本人面接の反復によりリスク要因を抽出してその部分の調査を深める方式に変更された。これによって、従来の一律フィールド調査による負荷を削減し、他方、コンピュータによる常時データ監視で、間断なき監視態勢の下においてセキュリティを向上させている。現時点、インテリジェンス機関職員については大部分が新方式に移行したようである。（なお、CIA や NSA は、従来から約 5 年毎に職員のポリグラフ検査を行っているが、これはこの制度改正後も変更がないと言われる。）

ところで、この新しい米国方式は、残念ながら、現時点で我が国の制度と比較することは適当でない。それは第 1 に、コンピュータによる常時監視の実態（監視データの種類や監視アルゴリズム）その他の、調査方式の詳細が開示されていないために、比較のしようがないからである。第 2 に、我が国の制度は、依然として従来型の時々の「調査」方式であり、この点でも比較の実益がないからである。

（イ）米国の旧方式

そこで、本稿では、2022 年以前の米国の背景調査制度を取り上げることとする。既述したように、米国では一律広汎な聞込みは廃止するなど調査方法の変更によって調査負荷の軽減は行われている。しかし、適格性審査の前提としての背景調査について、その実質的な精度が緩和された

---

[40] DNI and Director, Office of Personnel Management, *Federal Personnel Vetting Guidelines,* February 2022, accessed 17 March 2026, https://www.dni.gov/files/NCSC/documents/Regulations/Federal_Personnel_Vetting_Guidelines_10FEB2022-15Jul22.pdf
-- *Federal Personnel Vetting Investigative Standards Crosswalk Guide*, accessed 17 March 2026, https://www.cdse.edu/Portals/124/Documents/jobaids/personnel/FPV-Investigative-Standards-2022-Crosswalk.pdf

訳ではない。その意味で、改正前の方式であっても、米国の背景調査において求められる精度、そのための調査の広汎さが理解できるであろう。

それでは以下、米国の制度については、開示されている最新の指針で 2018 年まで使用された IC 政策指針 704.1 号「SCI その他のアクセス管理プログラム情報へのアクセスに関する人的保全の調査基準と手続」(2008 年)[41]に基づいて述べる。

米国で現実にインテリジェンスの職務に就くには、Tier 5 通称 SSBI[42]という機密（TS: Top Secret）や機微区画情報（SCI: Sensitive Compartmented Information）にアクセスできる最高位のクリアランスを得る必要があるので、SSBI レベルの背景調査について述べる。

SSBI で顕著なのは、本人提出の質問表に基づく面接調査の重視である。具体的には次の通りである。

○　教育歴：過去 3 年間の主たる活動が学業である場合は、本人の学業について直接的知識を持つ者（教員など）から事情聴取を行う。

○　職歴：過去 7 年間の全ての雇用歴を確認する。6 月以上勤務した職場については上司及び同僚から事情聴取を行う。

○　離婚した配偶者からの事情聴取：過去 10 年以内に離婚した配偶者全員から聴取する。

○　近隣：過去 3 年間の全ての居住地について、隣人 2 人以上からの事情聴取を行う。

○　人物評価(references)：本人の人物を評価できる者 4 人以上からの事情聴取。内 2 人以上は本

---

41 本稿の記述は、2008 年から 2018 年まで適用された①IC 政策指針 704.1 号「SCI その他のアクセス管理プログラム情報へのアクセスに関する人的保全の調査基準と手続」(2008 年) に基づいている。本 IC 政策指針 704.1 号は 2018 年 6 月に②指針によって③に改正された。改正後指針③では、2012 年に政府保全責任者（国家諜報長官）と政府適格性責任者（行政管理局長官）が共同で制定した the Federal Investigative Standards（FIS）に従うとしているが、同 FIS は開示されていないようで、ウェブで検索したが発見できなかった。一方、④連邦規則集 32 篇 147 部 B 節 Investigative Standards の規定がある。この規定は、連邦規則集に搭載されたのは 2021 年 7 月であるが、1998 年に the Federal Register で出版されたものと同一であり、2012 年の the Federal Investigative Standards（FIS）と同一か否か不明である。ただ、④の規定の内容も①の内容と大差がない(①の方がやや詳しい)。そこで、本稿では①の IC 政策指針 704.1 号に基づいて記述した。

① 2008 年指針：ODNI, *Intelligence Community Policy Guidance Number (ICPG) 704.1: Personnel Security Investigative Standards and Procedures Governing Eligibility for Access to Sensitive Compartmented Information and Other Controlled Access Program Information,* effective 2 October 2008.

②　改正指針：ODNI, *ICPG 704.1 Technical Amendment: Personal Security Investigative Standards, Personnel Security Investigative Standards for Access to Sensitive Compartmented Information*, 20 June 2018

③　改正後指針：ODNI, *ICPG 704.1: Personal Security Investigative Standards,　and Procedures for Access to Sensitive Compartmented Information.*

④　Code of Federal Regulations, Title 32 National Defense, Part 147 Adjudicative Guidelines for Determining Eligibility for Access to Classified Information, Subpart B Investigative Standards, Attachments A NACLC and B SSBI, accessed 17 March 2019, https://www.govinfo.gov/content/pkg/CFR-2025-title32-vol1/pdf/CFR-2025-title32-vol1.pdf, これは the Federal Register on 30 January 1998 (63 FR 4573)と同文である。

42 SSBI とは、Single Scope Background Investigation の略称。

人による推薦者でないこと（つまり、質問票に本人が記載した者以外の者）。2 人以上が本人の社会生活について知っていること。事情聴取は合わせて、対象者の過去 7 年間以上の期間をカバーできなければならない。

このように、背景調査では調査官が現地に赴いて、実に広汎な面接調査をするのである。

また、各種の関係機関照会も行われる。地方機関照会（過去 10 年間の居住地や学校勤務地の警察照会）、国家機関照会（FBI、CIA、国防総省、移民帰化局など国家機関の持つ各種データベースに対する照会）を行うが、配偶者や同居者についても、国家機関照会を行う。更に必要に応じて、各種金融情報のデータベースの照会も行う。各種の機関照会も多くは義務的で広汎である。

米国では、このような徹底した調査を、全ての SSBI レベルのセキュリティクリアランス申請者に対して行っているのである。従って、調査費用が掛かり、国防防諜・保全庁 DCSA の 2025 年度調査受託費用は、1 人当りの基本料金が 5355 ドルであり、不審点があって追加調査を依頼すれば更に追加料金が加算される[43]。

（ウ）日本

これに対して、我が国のセキュリティクリアランス（適性評価）のための調査は極めて簡略である。制定当初の 2014 年から 2025 年末まで適用されてきた閣議決定『運用基準』（Ⅳ-５）[44]によれば、先ず、本人提出の 28 頁程度の質問票に加えて、上司又は人事担当課の職員等（＝本人の職務遂行状況等について良く知ると認める者）が提出する調査票（適性評価）だけで、セキュリティクリアランスを与えることができた。上司等の提出する調査票は全部で 3 頁、実質的な記載頁は 2 頁と極めて簡略なものであり、且つ、その内容について上司等は本人に確認してはならないこととされている。

適性評価実施担当者は、本人質問票や上司等の調査票を基に疑問点が生じたときに初めて、上司、同僚その他の知人に質問したり、人事管理情報等を確認したり、本人面接をしたりすることができるとされていた。更に、これでも疑問が解消されない場合に初めて、公務所や公私の団体に対する照会を行うこととされていた。つまり、特に疑問が残った場合に初めて、公務所照会や公私の団体に対する照会をすることとなっていたのである。

つまり、この枠組では、公務所照会もせず、公私の団体照会もせず、米国に見られるような民間の幅広い関係者面接もせずに、本人質問票や上司等の調査票だけで、セキュリティクリアランスを付与できたのである。正に驚きの制度である。このような調査がそもそも背景調査（人物調査）の名に値するものなのか、疑問である。そもそもセキュリティクリアランス制度は、上司等による評価では不十分であるとの認識の基に構築されている制度なのである[45]。

---

[43] DCSA, *Federal Investigation Notice, No. 23-03: Subject: Products and Services Reimbursable Billing Rates for FY 2024 & FY 2025,* 13 September 2023, https://www.dcsa.mil/Portals/128/Documents/about/err/FIN%2023-03%20-%20FY24%20and%20FY25%20Products%20and%20Services%20Billing%20Rates.pdf

[44] 閣議決定『運用基準』改訂版（2021 年 6 月 11 日）。

[45] 本来、本人質問票や上司等の調査票のみでは必ず疑問が残る筈であるので、実務上はマトモな組織は申請者全員について疑問が残るとして、次の段階の調査に移行していたのであろうか。そうとでもしなければ、セキュリティクリアランス制度とは到底呼べないものであった。

この『運用基準』は 2025 年 12 月に改訂された。改訂後の『運用基準』[46]によれば、本人の質問表と上司等の調査票に加えて、①人事管理情報等による確認（職歴、懲戒の経歴、情報の取扱いに係る非違の経歴その他人事管理業務等と通じて得られた情報）、②公務所又は公私の団体に対する照会（海外に居住し又は渡航した経歴、犯罪の経歴、信用状態その他の事項）、③適性評価実施担当者による本人面接も、実施されることとなった。そもそも、これら①②③の事項は当然に実施されるべき事項であって、これらの実施が選択的であった改訂前が異常だったのである。この改訂で漸く正常なクリアランス手続に前進したと評価できる。但し、『運用基準』によれば、③の本人面接は、「勤務地が遠隔地にあるなどの事情があるときは、評価対象者の負担軽減のため、通信の方法により実現して差し支えない。」とされている。つまり、ZOOM などのウェブ会議方式でも可とされており、まだまだ手続に甘さが見られる。

日本の現在の制度は、米国のセキュリティクリアランス制度と比較すると、漸く Secret（極秘）或いは Confidential（秘密）レベルに近付いたところであり、上記の米国の Top Secret/SCI（機密/機微区画情報）のための Tier5、SSBI レベルとは程遠いものである[47]。

（なお、既述のように、米国では 2022 年に背景調査の制度が大改革をされ、面接インタビューは、従来の一律広汎な関係者インタビューから、対象者本人の面接インタビュー重視に移行した。即ち、本人面接の反復によりリスク要因を抽出してその部分の調査を深める方式に変更された。同時に、対象者に関する各種データを常時継続的にコンピュータによって監視し、危惧すべき徴候が検知された際には徹底的に調査する「継続的監視システム」方式に移行している。しかし、この改正によって、適格性の審査や評価の前提としての背景調査の精度が実質的に緩和された訳ではない。その意味で、改正前の方式であっても、米国の背景調査において求められる精度、そのための調査の広汎さが理解できるであろう。）

（4）特に本人面接（インタビュー）

背景調査（人物調査）の方法でも、特に重要なのが本人面接である。米国のインテリジェンス機関は、機微なポストに就く職員については本人面接で専門家がポリグラフを使用して面接している。特に CIA や NSA（国家安全保障庁、国家シギント機関）では広汎に使用している[48]。

更に米国では、セキュリティクリアランスは 5 年毎に更新することになっており、その度に背

---

46 閣議決定『運用基準』改訂版（2025 年 12 月 26 日）。

47 我が国の調査票の簡略さと米国の質問票の精緻さ、虚偽記載に対するペナルティを比較すると、我が国の特定秘密保護法によるセキュリティクリアランスのレベルが、米国の Tier3・NACLC（Secret、Confidential）レベルと同一水準に達したのか、疑問が残る。

48 ポリグラフの使用について規定する行政命令は、政府保全責任者指令第 2 号修正版「秘密情報へのアクセス又は機微な職務の適格性判断のための人的保全決定支援のためのポリグラフ使用」、Office of the Director of National Intelligence, *Security Executive Agent Directive 2 (SEAD 2): Use of Polygraph in Support of Personnel Security Determinations for Initial or Continued Eligibility for Access to Classified Information or Eligibility to Hold a Sensitive Position* (originally issued 4 February 2016; revised version effective 1 September 2020).

景調査が繰り返されるが、本人面接も行われる[49]。元 CIA 工作員の Valerie Plame の回顧録[50]にはクリアランス更新のための本人面接と思しき記述があるが、彼女は、本人面接がたった 3 時間で終わり記録的な短さであったと自慢している。いかに通常の本人面接が厳しいものであるか分かるであろう。

ポリグラフを使用する本人面接は、単に非違行為の探知だけでなく、秘密漏洩や外国諜報機関への通謀に対する威嚇力としても機能しているのである[51]。

これに対して、我が国では、本人面接は義務化されたとはいえ、ZOOM を使用したリモート面接も可とされているなど、どれだけ厳しい面接ができるのか、疑問で残る。

（5）SNS 情報の収集分析

更に、背景調査では対象者ソーシャルメディア上の情報も調査対象とすることができる旨規定されており、行政命令（政府保全責任者指令第 5 号）「人的保全背景調査及び審査におけるソーシャルメディア情報の収集・使用・保持」[52]も発出されている。但し、ソーシャルメディア情報の調査は、現時点では各省庁の裁量に任されており、採用している省庁と採用していない省庁に分かれるようである。

（6）背景調査の調査態勢

以上のように、米国では背景調査が徹底しており、そのための態勢は充実している。国防総省や FBI、CIA、国務省、国土安全保障省などはそれぞれ調査の専門組織を持っている。この中で一番大きな調査機関は、国防防諜・保全庁 DCSA 傘下の「国家背景調査局 NBSB[53]」で 8500 人程の専従職員（内、5500 人は契約職員）がいる。同庁は、国防総省だけでなく、連邦政府の多くの省庁から背景調査を受託しており、連邦政府による全調査の 95％を実施している。また、FBI では FBI 本体の組織の他に「背景調査契約サービス BICS[54]」という契約職員の組織を設置し 1800 人

---

[49] 2022 年の制度改正によって、常時継続的な監視システムに移行したことにより、TS/SCI レベルの 5 年毎の背景調査は不要となったが、CIA や NSA では、依然として 5 年毎に保全検査としてポリグラフ検査を実施しているようである。

[50] Valerie Plame Wilson, ibid., p.53.

[51] 2010 年 10 月に、警視庁公安部外事第三課の国際テロ関係の極秘調査資料がウェブ上に大量に漏洩されたが、FBI であれば漏洩源を特定するために、同資料にアクセス可能な職員全員にポリグラフを掛けたであろう。また、通常からポリグラフを使用した面接が制度化されていれば、漏洩事件そのものの発生を防止できたのではないだろうか。

[52] *Security Executive Agent Directive 5（SEAD 5）, Collection, Use, and Retention of Public Available Social Media Information in Personnel Security Background Investigation and Adjudications*, 2016 年 5 月 5 日制定、5 月 12 日施行。

[53] National Background Investigation Bureau

[54] Background Investigation Contract Service。FBI は、大統領任命高官、大統領府職員、議会職員の一部、連邦裁判所職員、司法省幹部などの背景調査も担当している。

を雇用しているが、FBI の OB がなっていることが多い[55]。また、国務省は外交保全局が担当しており、そのため契約職員を雇用している。更に、背景調査受託企業も Omniplex や CACI など数社存在していて、背景調査業務自体が一つの産業となっている。

他方、我が国で調査態勢は公表されていないのでその規模は不明であるが、自衛隊情報保全隊を保持する防衛省でさえ、数百人が上限であろう。その他の省庁は、調査のための専従組織を保持していないと考えられる。警察は、警備公安部門の警察官を動員して調査することが可能であるが、その他の官庁ではそれも無理であろう。我が国の調査態勢が、米国と比べて大きく見劣りすることだけは確実である。

（7）保全教育

米国では、職場単位（例えば、大使館や支局毎）に防諜・秘密保全の専従担当者が配置され、職員は情報保全の必要性、秘密を漏洩した場合の帰結（刑事罰）、スパイ工作の手法などについて、毎年、定期的に保全教育を受けている[56]。職員は、保全教育の修了証明書がないと秘密情報にアクセスする業務を継続できない。また、リスク事象が発生した場合には、専従担当者は職員からの相談にも応じている。

他方、我が国では防諜・秘密保全の専任部署の態勢の貧弱さから判断しても、どれだけ充実した保全教育が行われているか、疑問がある。

（8）報告義務

秘密情報の取扱者の報告義務について、米国政府は行政命令（政府保全責任者[57]指令第 3 号）「秘密情報アクセス者の報告義務」[58]で統一基準を定め、諜報工作やテロの対象となり得るリスク事象やセキュリティクリアランス継続に悪影響を及ぼしかねない事象の報告を義務付けている。具体的には、私的な外国旅行、外国人との継続的交際、海外資産など外国関係の活動、更には結婚・同居人、相続や懸賞金などの臨時収入ほか個人的な事象を幅広く報告対象としている。そして、「事前に又は事後可及的速やかに」報告することを義務付け、上司には、国家安全保障に潜在的脅威が生じる場合は必要な行動をとることを義務付けている。結婚や同居、或いは相続や懸賞金による臨時収入は、プライバシーに係わることだから報告しないなどということは許されないのである。

---

[55] FBI・OB のインターネットの書込みを読むと、FBI 退職後の理想のパート仕事で、平均して年間数万ドルの収入になり、FBI とも繋がりを維持できる、と後輩に勧奨している。

[56] EO13526, *Classified National Security Information,* 29 December 2009.及び連邦行政規則集 32 篇 2001.70 条。https://www.law.cornell.edu/cfr/text/32/2001.70。秘密情報にアクセスするには、初期教育と毎年の定期教育の受講を義務付けられている。ISOO, *Agency Training Requirements*, https://www.archives.gov/isoo/training/agency-training-requirements 参照。

[57] 米国政府の政府保全責任者 Security Executive Agent は、国家諜報長官 DNI である。

[58] *Security Executive Agent Directive 3（SEAD 3）, Reporting Requirements for Personnel with Access to Classified Information or Who Hold Sensitive Position,* 2016 年 12 月 14 日制定。12 June 2017 施行

更に、報告義務事項には、他者による秘密保全基準不遵守、裕福な生活や過剰債務、その他セキュリティクリアランスの審査指針に抵触しかねない行為について報告義務を課している。つまり、同僚の不審動向に気が付いた場合は、即座に報告をせよということであり、職員に相互監視を義務付けているのである。

これに対して、我が国では、セキュリティクリアランス付与時に職員が提出する誓約書で、一定の事項[59]についての事後報告を誓約させているが、あくまで「事後」報告であり、且つ、報告事項も限定的である。流石に外国人との結婚は報告対象となっているが、外国旅行、外国人との接触、臨時収入、日本人との結婚や同居など重要な事象が報告対象とはなっていない。これらは各省庁における個別の対応に委ねるということかも知れないが、徹底を欠いていると言わざるを得ない[60]。

3－4　物的保全(Physical Security)

物的保全とは、機密情報等へ不正に物理的にアクセスすることを防止するための措置の総体である。つまり、施設防護（警備態勢など）、入退管理、施設構造基準、侵入検知と監視態勢、金庫などによる機密資料の保護である。米国では、これが大統領令以下の規則により体系的に整備されている。

特に有名なのが諜報コミュニティ指令（IC 指令）第 705 号「機微区画情報施設（SCIF）の物理的・技術的セキュリティ基準」[61]であり、この基準は、機微区画情報（SCI）を取り扱う全ての諜報機関が従う政府統一基準である。この基準と付随する技術仕様規則[62]によって、施設の建設基準（対侵入構造、強化ドア・壁・床・天井の基準など）、侵入検知システム、入退管理（認証付きアクセス制御と記録）、盗聴・電磁波漏洩対策、遮音対策、通信回線の施設基準など、包括的で厳格な基準が定められている。そして SCIF は、防諜・保全部署が、基準に合致しているか、設計段階で審査し、且つ完成後は現地確認をしなければ使用できないのである。このため、米国のインテリジェンス関係施設の多くは、外窓のない全てコンクリートで覆われた施設である[63]。米国のインテリジェンス機関を訪問したことのある者には良く知られた事実である。

このような政府統一基準があるからこそ、諜報コミュニティ間の機微情報の共有、それも電子的な情報共有が可能なのである。

---

59 閣議決定『運用基準』Ⅳ-9-（1）

60 かつて我が国では、某実力官庁の幹部（複数）が、私用旅券を保持して、組織に報告することなく懸念国への渡航を繰り返していた事実がある。このようなことは米国では到底許されず、懲戒処分やセキュリティクリアランスの取消事由になる。また、虚偽供述罪で刑事罰の対象にもなり得る。

61 ODNI, *Intelligence Community Directive 705: Intelligence Community Standard for Physical and Technical Security of Sensitive Compartmented Information Facilities (SCIFs),* 26 May 2010.

62 ODNI, *The Intelligence Community Technical Specifications for ICD 705* (通称 the IC Tech Spec)

63 因みに、米国の SCIF の建物設計では、外窓がなくでも圧迫感を減じる各種の工夫をしている。

これに対して、我が国は政府の統一的基準は存在せず、各官庁任せとなっているのが実態である。これでは、機微な情報の関係省庁間における共有にも支障が生じる筈である（他官庁の物的保全の基準が分からなければ、機微情報の共有はできないであろう）。

3－5　情報保全（Information Security：INFOSEC）

情報保全とは、情報の取扱いの観点からの保全の取組であり、秘密指定・管理、アクセス統制と Need-to-Know、秘密情報の取扱・保管・送達、情報システムのセキュリティなどからなっている。

① 秘密指定・管理。機密、極秘、秘密などの秘密指定と制度管理、機微区画情報（SCI）など特別アクセス統制の管理。秘密指定の解除[64]など。

② アクセス統制と Need-to-Know 原則。職員がアクセスする情報に対して適切なクリアランス・レベルを保持しているか確認し、秘密情報へのアクセスが公務上必要な範囲に限定されているか（Need-to-Know 原則）を管理する。

③ 秘密情報の取扱・保管・送信。秘密資料の適切な表示・取扱・保管手続を管理する。秘密情報の伝送が秘密区分に応じた通信経路、即ち、暗号化メール、JWICS（機密用）、SIPRNet（極秘用）他の適切な秘密通信ネットワークで行わるように管理する。

④ 情報システム・セキュリティ（Information Systems Security）。現在は殆どの情報は情報システム上にあるので、この情報システム・セキュリティの重要性が増している。この基本規則として、諜報コミュニティ（IC）指令第 503 号「諜報コミュニティ情報環境リスク管理」[65]が制定されている。同指令は、情報コミュニティで使用する情報システムのセキュリティリスクを統一的に管理するためのもので、情報システムの運用認可（セキュリティ審査）手続、運用開始後の継続的監視システムの導入[66]、「ゼロ・トラスト」原則の適用、諜報コミュニティの情報システム運用認可の相互承認などを指示している。更に、同指令実施のために具体的な技術マニュアル（未公表）も出されているようである。

情報システム・セキュリティ対策には、内部脅威対策とも重複するが、情報システムへのアクセス統制（多要素認証やアクセス履歴監査）や秘密情報へのアクセス状況監視（不正或いは不審な活動の検知）も含まれると考えられる。

---

64 秘密指定の解除に責任を持つ部署の存在は重要である。期限が来たからと一律に解除するのではなく、秘密指定を維持するかどうかを内容に即して判断する。他方、必要のない秘密指定は期限内であって秘密指定を解除する。こうして実質的に秘密を管理する部署がないと、秘密指定が形骸化してしまう。

65 ODNI, *Intelligence Community Directive 503（ICD 503）：Intelligence Community Information Environment Risk Managements,* 25 October 2024.

よりサイバー防衛に特化した指令としては次の指令も発出されている。ODNI, *Intelligence Community Directive 502（ICD 502）：Integrated Defense of the Intelligence Community Information Environment*, 11 March 2011.

66 Information Security Continuous Monitoring.

なお、本指令を一読した印象としては、情報システムに対する供給網工作、即ち、製品の製造段階や配送段階でマルウェアを仕込まれることへの警戒が看取できる。米国自体が諸外国に対して供給網工作を仕掛けており、供給網工作を警戒するのは当然であろう[67]。

3－6　内部脅威対策（Insider Threat Program）

防諜・秘密保全対策は、従来は、上記の人的保全、物的保全、情報保全など分野別の対策の集合体であったが、米国では 2012 年に、政府を挙げて内部脅威対策に取り組むこととし、政府中央機関を設置すると共に関係省庁にも専門家による専門部署の設置を義務付けて取り組んでいる。

基本となる根拠法令は、2011 年の大統領命令と 2012 年大統領覚書である。

（1）2011 年の大統領命令 13587 号（E.O.13587）[68]

先ず、大統領命令では、政府の中央機関として「国家内部脅威対策タスクフォース」（National Insider Threat Task Force: NITTF）を設置した。NITTF の共同議長は司法長官と国家諜報長官、委員は関係省庁の代表者である。事務局は FBI と国家防諜保全センターNCSC[69]などから派遣される職員によって構成するとしている。そして、NITTF は、秘密情報にアクセスできる全省庁に対して内部脅威対策の指針を示し、各省庁はこれに従って内部脅威対策を実施することとされた。

（2）2012 年大統領覚書[70]

次に、大統領覚書は、「内部脅威対策の方針」と「最低基準」を定めている。「内部脅威対策の方針」では、NITTF は、主として次の 4 点について実施すべき基準を示すこととされている。即ち、①対象者のネットワーク活動の監視、②対象者の人的保全情報の継続的評価（背景調査、クリアランス審査、外国旅行報告、外国接触報告、金融情報、ポリグラフ検査その他）、③職員の内部脅威の認識向上、懸念情報の報告手続と報告義務などの内部脅威対策の訓練、④懸念情報の分析と報告、そして具体的な対処態勢の整備である。

---

[67] 茂田忠良「サイバーセキュリティとシギント機関～NSA 他 UKUSA 諸機関の取組～」『情報セキュリティ総合科学』第 11 号（2019 年 11 月）、補論２　華為問題（中国による Supply Chain Operation）参照。

[68] Executive Order 13587（7 October 2011）, *Structural Reforms To Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information.* 「秘密ネットワークのセキュリティ、及び秘密情報の責任ある共有と保護の向上のための構造改革」、https://www.archives.gov/files/isoo/policy-documents/eo-13587.pdf

[69] National Counterintelligence and Security Center、政府の防諜・秘密保全の統括組織。国家諜報長官室の下部組織で 2014 年に設立。E.O.13587 発出時の担当組織「国家防諜監督官室」ONCIX（Office of the National Counterintelligence Executive）の後継組織。

[70] Presidential Memorandum (21 November 2012), *National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Program*s. 「国家内部脅威対策政策、及び行政府内部脅威対策プログラム最低基準」https://sgp.fas.org/obama/insider.pdf

大統領覚書の「最低基準」は、各省庁の長には幹部職員を内部脅威対策の責任者に任命し[71]、同責任者が起案する省庁の内部脅威対策方針を制定することを義務付けている。次に同責任者には、毎年報告書を作成して、実施状況と改善勧告等を省庁の長に報告することを義務付けている。

「最低基準」が義務付けている内部脅威対策の具体策の骨子を例示すると、次の通り。

① 電子的及び人的な内部脅威の分析と対処能力を構築すること。防諜と保全の専門家を配置すること。

② 内部脅威対策部署に対して、必要な関係情報を関係部署が提供するようにすること。例えば、人的保全関係では、個人セキュリティ記録、ポリグラフ記録、施設入退記録、旅行記録[72]、外国接触報告、個人金融情報[73]その他。ネットワーク関係では、個人ユーザー名や別名、アクセス記録、印刷記録、外部記憶装置の使用その他。人事関係では、給与データを含む全ての人事記録。(註：このような各種の関係情報が、内部脅威の端緒情報があった場合の対象者の調査や分析に有用なのである。)

また、関係部署から内部脅威対策部署に対する懸念情報の自発的な報告基準と報告手続を定めること。(註・懸念情報とは、不審行動や、内部脅威の兆候となり得る行動の情報である。)

③ ネットワーク活動の監視。内部脅威の端緒を探知するため、対象者の全ての秘密情報ネットワークでの活動を監視すること。不審行動を特定する手法や内部脅威対策部署への報告手続を定める。更に、職員に対しては、(秘密以外を含む) 全てのネットワーク活動の監視に対する同意書を徴取し、且つ、ネットワークの端末にも監視対象であることを告知すること。

④ 秘密情報にアクセスできる職員全員には、内部脅威対策の訓練を施すこと (敵対国による接近・リクルートの手法や懸念情報の報告手続の教育を含む)。

以上は、最低基準の骨子の抜粋であり、最低基準が如何に包括的網羅的なものか理解できるであろう。

(3)「内部脅威対策指針」2024 年版[74]

更に、タスクフォース NITTF は、「内部脅威対策指針」と称して、上記大統領覚書の「最低基準」実施のベストプラクティス集を定期的に発行しており、最新版 (約 80 頁) が 2024 年に発行されている。

本指針では、実施すべきベストプラクティスが詳述されている。その中でも力を入れているの

---

71 米国各省庁の担当部署を見ると、内部脅威対策の専任部署は、前述した防諜・保全担当部署の一部門として設置されている例が多い様である。

72 出入国記録、航空機搭乗記録などは、無届外国旅行を探知し、また、届け出のあった外国旅行の実態を調査するのに有用であるとしている (2024 年「内部脅威対応指針」p. 49)。

73 信用格付け機構や財務省 FinCEN などの情報が有用であるとしている (2024 年「内部脅威対応指針」同上)。

74 NITTF, *INSIDER THREAT GUIDE – A Compendium of Best Practices to Accompany the National Insider Threat Minimum Standards,* 26 September 2024, 「内部脅威対策指針—国家内部脅威対策最低基準に伴うベストプラクティス集」
https://www.dni.gov/files/NCSC/documents/nittf/20240926_NITTF-Insider-Threat-Guide.pdf

が、ネットワーク活動を監視分析することによって、内部脅威の端緒情報を入手しようとするものである。具体的には、ログイン・ログアウト履歴、ファイル等のアクセス・作成・消去・修正等の履歴、データのダウンロードやエクスポート・インポート履歴、印刷履歴などのデータを分析して、端緒情報を得ようとするのである[75]。監視対象活動は、キーストローク、（メール、チャット、データ送受信などの）コンテンツ・データの把握、スクリーン画像の把握にまで及んでいる[76]。勿論、ネットワーク監視をゼロからマンパワーで行うのは現実的でないので、一定のアルゴリズムを構築して自動的に監視して、端緒となる不審行動を抽出探知するのである[77]。

このようなネットワーク監視活動によって、或いは職場の上司同僚からの報告によって、内部脅威対策部署が懸念情報を受理した場合の内部調査など具体的対処要領についても、本指針は示している[78]。ここで注目されるのは、各省庁の内部脅威対策部署は、対応する FBI の部局と普段から実質的な協力関係を樹立しておくように勧告していることである。既述の通り、合衆国法典 50 篇 45 章 3381 条 (e) 項によって、秘密情報の漏洩が疑われる場合には、関係省庁は即座に FBI に通報して、対応は全て FBI と協議することとなっており、そのための事前準備である。

なお、内部脅威対策に関連して、米国では退職後のインテリジェンス職員についても海外渡航などの監視態勢を敷いているようである。FBI による検挙事例を見ると、陸軍の諜報部隊に勤務した兵士が、報酬目的で中国に情報を提供しようとして、除隊後の 2020 年に香港に渡航したが、2023 年に帰国したところを空港で FBI に逮捕されている。この事例から、米国政府は元インテリジェンス職員の海外渡航を把握し、且つ、懸念国での行動について情報収集態勢を敷いていることが分かる[79]。

米国では内部脅威対策だけでも、これだけの専門の体制を構築しているのである。これに比較して我が国の態勢はどうであろうか。

---

[75] Ibid., p.46.

[76] Ibid., p.53.

[77] 2023 年春、マサチューセッツ州空軍州兵のジャック・テシェイラが膨大な機密情報を漏洩した。彼は、インテリジェンス IT システムの技術担当であったため、分析担当ではなかったものの、JWICS という米軍の機密情報システムへのアクセス権限を持っていた。彼はアクセス権限を濫用して、入手した機密情報を会員限定のソーシャルメディアで共有していたところ、会員がそれを他のソーシャルメディアに転載し、拡散したのである。FBI による事後捜査によれば、彼は、IT システムの技術者としては閲覧する必要のない、ロシア・ウクライナ戦争などの情報を JWICS で頻発に閲覧していた。従来、CIA や NSA と比べて、州兵の秘密保全は甘いとも言われてきたが、この事件を契機に、ネットワーク監視が強化されたと推定できる。拙稿「Texeira 漏洩情報に見る米国のインテリジェンス力」『警察学会資料』129 号（2023 年 8 月）1-6 頁参照。

[78] NITTF, ibid., pp.63-70.

[79] 茂田ウェブサイト「国外活動に対する FBI の捜査力～元米軍人の逮捕～」（2023 年 11 月 27 日）https://shigetatadayoshi.com/2023/11/27/arrest-of-a-former-army-intellgence-sergeant/。退職後の監視態勢に関する制度の実態は不明であるが、制度運用の効率性から考えて、渡航先やそこでの活動情報の収集は、元所属省庁毎ではなく、FBI を中心として政府一体として構築していると見られる。

3－7　民間企業による防御措置と政府の協力態勢

以上は政府機関の防御施策であるが、米国の民間企業も政府機関と同様な防御施策をとっている。先ず、民間企業にもしっかりした保全専門部署を設置しているが、ここには FBI の OB など関係政府機関からの転職者もいて、防諜・情報保全対策では FBI と端緒情報の相互通報など連携をとっている。また、企業自体は自らの情報システム・セキュリティに力を入れており、社員の不審動向の探知に力を入れている。

FBI による企業秘密漏洩の検挙事例を見ても、民間企業のセキュリティ対策と FBI との協力関係、そして FBI の調査能力が相まって、検挙に至った事例が多々見られる。例えば、GE 社のサイバーセキュリティ担当が、社内の情報システムにおける社員の不審な行動を探知し、これを企業の保全部署が FBI 支局に通報。FBI が通信傍受によって不審社員のインターネット上のメールや SNS 通信を調査し、中国に企業秘密を送信しているのを把握して検挙した事例がある[80]。或いは、逆に、先ず FBI が Honeywell 社のエンジニアが中国の軍系の中核大学である南京航空航天大学を訪問したのを探知して、これを同社の保全部署に通報。その後、同社の保全部署と FBI が協力して、エンジニアの中国における無届講演を明らかにして、これを端緒に中国国家公安部の工作員の逮捕にまで至った事例もある[81]。

このように防諜・秘密保全対策では、民間企業におけるセキュリティ対策の整備と政府防諜・捜査部門との協力関係が重要なのである。

3－8　情報のサニタイズ

直接のスパイ防止策ではないが、諜報コミュニティ内での情報共有を進めつつ、諜報源の秘匿を図る技法として、情報の所謂「サニタイズ」がある。「サニタイズ」とは、諜報源を秘匿しつつ、インテリジェンス顧客が必要とするインテリジェンス情報を情報価値を落とさずに提供する技法である。

この点について、嘗て中央諜報長官指令 DCID1/19[82]には、「情報漏洩やスパイ行為などによる諜報源と諜報手段に対する損害を避けるために、情報のサニタイズ（sanitization）を行う。全ての諜報報告作成部署は、SCI（機微区画情報）報告書から諜報源や諜報手段に関する情報を、削除し、サニタイズし、或いは一般化しなければならない」旨が記載されていた。つまり、一方で、報告書の情報価値は維持しつつ、他方、諜報源や諜報手段の記述を削除すると共に、情報内の特

---

80 茂田ウェブサイト「『海帰創業』：中国による経済スパイの一形態」（2024 年 12 月 10 日）、https://shigetatadayoshi.com/2024/12/10/returnee-entrepreneurship-as-a-form-of-economic-espionage/

81 茂田忠良「江蘇省国家安全庁第 6 局による経済スパイ」『警察政策学会資料』137 号（2024 年 12 月）1-20 頁。

82 *DCID1/19 Security Policy for Sensitive Compartmented Information and Security Policy Manual*（中央諜報長官指令「機微区画情報に関する保全政策及び同マニュアル」）(March　1995.), 3.0 Protection of Sources and Methods.

定の時刻や場所や人物などの記述から諜報源等が推定されないように、より一般的、或いは抽象的な表現に書き換えるのである。

その後、本指令 DCID1/19 は廃止され、現在その内容は各種の諜報コミュニティ指令（IC 指令）などに吸収されているが、現在のサニタイズの標準的な手法は、「ティアライン」[83]という手法で運用されているようである。その手法については、IC 指令 209 号「ティアライン作成及び配布」に規定されている[84]。各諜報機関は更に各自でティアライン方式を使用した報告書作成のマニュアルを作成している[85]。

我が国においても、実質的なサニタイズはそれぞれの機関でそれなりに行われているのであろう。しかし、諜報源の暴露を防止しつつ、諜報コミュニティにおける情報共有を進めるには、米国諜報コミュニティのように体系化された「サニタイズ」や「ティアライン報告書」などの制度を導入する必要がある。

４　積極防御面

次は積極防御について取り上げる。積極的にスパイを探知し解明した上で、対策を取ることである。関係者に内々に警告を発して防御を強化するなど必要な対策[86]を取ったり、或いは検挙摘発

---

[83] 筆者は「ティアライン」報告書の実物を見たことがないので、推測であるが、諜報源や諜報手段など特に秘匿すべき情報は報告書冒頭に集中して記載し、報告書本文からは諜報源や諜報手段を推定できる情報を極力削除しておく。そして、インテリジェンス顧客には諜報源関係部分を除去した報告書を配布する方式のようである。

[84] *ICD 209 Tearline Production and Dissemination*, 6 September 2012.
この他、関連する IC 指令には次のものがある。
—*ICD 208 Maximizing the Utility of Analytic Products,* 9 January 2017.
—*ICD 501 Discovery and Dissemination or Retrieval of Information within the Intelligence Community,* 21 January 2009.
—*ICD 710 Classification Management and Control Markings System,* 21 January 2013.

[85] ACLU による情報公開請求によって次の FBI の情報報告書マニュアルが開示されている。白塗り部分が多く、断片的な内容しか分からないが、ティアライン作成が標準化されているのが分かる。
FBI, *Intelligence Information Report Policy Implementation Guide,* 10 January 2010, accessed 19 March 2026, https://www.aclu.org/sites/default/files/field_document/ACLURM006050.pd

[86] 事件化以外の対策として最近注目されたのは、英国 MI5 による議会に対する警告である。MI 5 は 2025 年 11 月 18 日議会に対して次の警告を発している。即ち、中国国家安全部は、議会や政府の機微情報にアクセスできる個人をリクルートしようとして、両院議員、政府職員、政治コルサルタント、経済学者やシンクタンク職員を標的にしている。北京のアマンダ・チューと香港のシャーリー・シェンの 2 人は、民間の人材斡旋企業を仮装して、SNS の LinkedIn 経由或いは対面で、フリーランスのコンサルタントとして働かないかなどと接触してくる。これは、国家安全部の意を受けた接触で、後で国家安全部工作員に引き継ぐ積りであるなどと警告している。
実は、直前の同年 10 月に、英国の検察は、中国のために議員の情報収集活動をした英国人 2 人に対する起訴を取り止めており、上記警告は、これに代えて取られた対策ともみられる。

したりして脅威を排除するのである。

さて、我が国のスパイの探知解明能力はどの程度であろうか。スパイを探知して内々に必要な対策を取っても、公表されるものは多くないので、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方法が簡明である。

そこで、各国の摘発件数を比較してみる。米国については、FBI 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[87]で、韓国の産業技術の対外流出の摘発件数は年平均約 20 件だそうである[88]。これに対して、我が国警察によるスパイ事件や先端技術窃取、大量破壊兵器関連不正輸出の検挙摘発件数は、年 1 件から 2 件の間といったところであろう[89]。

この件数の格差はどうして生じるのであろうか。検挙摘発では、情報の収集能力と処罰規定と二つの側面があるが、より決定的なのは情報の収集能力である。

4－1　情報収集力の違い

筆者は前世紀に国際テロ対策に従事して、欧米のセキュリティ・サービス（治安情報機関）と付き合った経験があるが、印象的だったのは彼らの情報収集力の高さであった。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ある。その要因は、彼らの情報の収集手段が実に多様であったからである。

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、そして、協力者からの情報が少しある位であるが、欧米では、秘匿の通信傍受や信書開披、住居などの秘密

—Jennifer McKiernan, Frank Gardner, Kate Whannel, “UK will not tolerate Chinese spying, minister says after MI5 alert,” *BBC,* 19 November 2025.
—Michael D. Shear, “Chinese Spies Are Using LinkedIn to Target U.K. Lawmakers, MI5 Warns,” *The New York Times*, 18 November 2025.
—黒瀬悦成「英国情報機関 中国の議会工作を警告」『日本経済新聞』、2025 年 11 月 20 日。

87 宇生航「米司法省報道発表“Justice News”から見た先端技術窃取をはじめとする懸念国有害活動の摘発傾向と我が国の経済安全保障上の諸取組への含意」『警察政策』第 26 巻（2024 年）211-216 頁。本研究で集計対象とされたのは、先端技術窃取、不正輸出、カウンターインテリジェンスの 3 種の類型の摘発件数である。

88 流出対策委員会「韓国における対中国技術流出事案の特徴」『治安フォーラム』2025 年 1 月号、21－32 頁。

89 警察庁警備局『焦点（令和 7 年版）』によれば、ソ連・ロシアによる対日諜報事件の検挙数は、戦後から 2025 年末まで合計 30 件、1991 年から 2025 年末までの合計 11 件（年平均 0.3 件）である。本資料には、中国及び北朝鮮による対日諜報事件の検挙数については言及がない。『焦点～令和 7 年の治安の回顧と展望』（第 296 号・令和 7 年版、2026 年 3 月）32-49 頁。

また、警察庁警備局『治安の回顧と展望（令和 3 年版）』によれば、北朝鮮による対日諜報事件の検挙数は、戦後から 2021 年 11 月末まで合計 54 件（年平均 0.7 件）である。上記『焦点』の記述と対照してみると、令和に入ってからの検挙数は令和 2 年の 1 件だけの様である。また、大量破壊兵器関連物資等不正輸出事件の検挙数は、1966 年以降 2021 年 11 月末まで合計 40 件（年平均 0.7 件）である。『治安の回顧と展望（令和 3 年版）』（2021 年 12 月）資料 5-6 頁、12－14 頁。

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[90]などを活用していたのである。

警視庁公安部 OB の著作[91]によれば、公安部の尾行張込技術は世界一流であると FBI が評価したそうであるが、そもそも欧米諸国では我が国ほど尾行張込はしない。尾行張込は、人手が掛かる割に効率が悪い。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からである。

更に 21 世紀の今や、サイバー空間が主要な情報空間となっている。当然、スパイ活動もサイバー空間を主要な活動空間としている。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る[92]。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。こうなると尾行張込では対抗できない。サイバー空間を監視する必要があるのである。

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ってくる。重要な手法は広義の通信傍受である。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、というのが主な手段である。それで入手できる情報は広汎である。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る。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殆ど全て把握できるのである。

ところで、最近は「シグナル」などの暗号化通信アプリが普及し、データは自動消去が可能である。そこで、我が国の警察関係者の中には、FBI でも「シグナル」通信は情報収集できないと誤解している人がいる。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る[93]。

米国では、このような圧倒的な情報収集力を使って、スパイを検挙しているのであるが、我が国警察にはこのような情報収集力はない。この我が国警察の情報収集力の低さは、現場の警察官の能力や努力の不足ではなく、情報収集権限の違いから生じるものである[94]。

---

90 筆者が当時会った欧州某国セキュリティ・サービスの某幹部は、自分がセキュリティ・サービスの本部庁舎に初めて足を踏み入れたのは、採用後 10 年以上も経ってからであった（即ち、それまでの間は、アンダーカバー・エージェントとして対象組織に潜入していた）と回想していた。

91 勝丸円覚『諜・無法地帯　暗躍するスパイたち』（実業之日本社、2023 年）52 頁。

92 2025 年 9 月には、中国諜報機関に、オンラインでリクルートされ、オンラインで報酬を受け取っていた米国務省員マイケル・シェイナが国防情報漏洩罪で拘禁刑を宣告されている。茂田ウェブサイト「米国務省員が国防情報漏洩罪で有罪～中国によるオンライン・リクルート～」(2025 年 11 月 1 日) https://shigetatadayoshi.com/2025/11/01/dos-official-sentenced-for-selling-secrets-to-china/

93 茂田忠良「韓国国情院による対米影響力工作」『警察学会資料』137 号（2024 年 12 月）21-35 頁。本事件では、容疑者はシグナルなどの暗号化メッセージアプリを使用し、且つデータは消去していたが、FBI はその通信内容を把握していた。

94 2026 年 5 月 6 日付け『産経新聞』は、「情報活動人員 3.3 万人従事～警察 6 割超～国内治安に偏る～政府初公表」という記事で、警察の警備部門（機動隊を除く）の人員が約 2 万 1 千人で、情報活動の人員が国内に偏っているという趣旨を述べている。しかし、警備部門には、（機動隊以外の）警備実施部門と公安部門（情報収集及び公安事件捜査）の両部門があり、2 万 1 千人全てが情報収集活動に携

4－2　情報収集権限の違い

FBI の高い情報収集力の基礎となっている情報収集権限とは何であろうか。代表的なものが1978 年制定の「外国諜報監視法」（Foreign Intelligence Surveillance Act: FISA）である。FISA は、スパイやテロの予防や抑止という国家安全保障のための行政調査権限を規定した法律であり、通信傍受や秘密捜索などの広汎な情報収集権限を認めている。また、米国の一般的な司法捜査権限も我が国と比べて遥かに広汎である。FBI による検挙事例を見ると、FISA による行政調査でスパイの端緒情報を得てある程度解明したところで、司法捜査権限による捜査に移って証拠化して検挙している実態が見て取れる。そこで、ここでは FISA 中の行政通信傍受と秘密捜索、一般司法捜査の司法通信傍受などの主な情報収集手段について見てみる。

（1）行政通信傍受

行政通信傍受は FISA（外国諜報監視法）第 1 篇と第 7 篇に規定されている。

第 1 篇（電子的監視）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ある。「外国諜報監視裁判所」（Foreign Intelligence Surveillance Court: FISC）の個別命令（court order）を得て行われるが、外国大使館や領事館などの純粋な外国施設の傍受、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できる。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、テロ容疑者である。本規定による通信傍受は、電気通信事業者の協力を得て行うもの（リアルタイムの通信傍受もあれば、データセンターに保存されたデータ収集もある）の他、スマートフォン端末のハッキング、或いは秘密裡に対象者住居や施設に傍受機器を仕掛けて行うものも含まれている。

これに対し第 7 篇（米国外の者に関する追加的手続）は、2008 年に制定された新しい通信傍受である。これは、通信事業者の協力を得て米国内の通信施設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[95]で、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ある。米国内のデータセンターには、G メール、ホットメール、ヤフーメールを初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ある。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ある。但し、付随的に、通信相手である米国人や米国内居住者の情報も収集してしまう。そこで、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る。この枠組は年に一度 FISC（外国諜報監視裁判所）の認証を受ける必要がある。

これらの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ある。司法傍受では特定の犯罪を疑う相当の理由が必要であるが、FISA 第 1 篇では外国勢力の代理人と

わっている訳ではない。また、本文で述べるように、我が国の警備警察部門は、情報収集権限が極めて限定され、人海戦術以外の有効な情報収集手段がなく、諸外国のセキュリティ・サービスと比べて多くの人員を必要とするのである。

95　米国外にいる者を標的にした通信傍受でも、通信事業者の協力を得ないで行うものの根拠法令は、FISA ではなく、大統領命令第 12333 号「合衆国諜報活動」である。

疑う相当の理由でよい（FISA 第 7 篇はそれすら不要）。第 2 に、FISC は秘密審理であり、傍受対象者には事後でも傍受の事実は通知されず、調査の事実は秘匿される（FISA 第 7 篇は個別審理自体が不在）。通信傍受を通知すれば、傍受能力を暴露し、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ある。第 3 に、傍受期間は、数年に及ぶような長期間の傍受が可能である[96]。第 4 に、本行政傍受の目的は、国家安全保障のためのインテリジェンス情報の収集であるが、同時に犯罪捜査目的があっても良いとされている。つまり、犯罪捜査での利用が可能である。第 5 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る[97]。但し、通常は、嫌疑の解明が進めば、司法令状を得て通信傍受を行い、裁判では司法傍受や司法捜査で得た情報のみを証拠として提示するのが常態である（parallel construction[98]という手法を使う）。政府としても行政通信傍受の詳細は秘匿しておきたいので、裁判での公開を極力回避しているのである。

なお、これらの行政通信傍受制度は、法律の制定以前から、大統領の行政権限に本来的に付随する権限として行われていた。しかし、政治問題化したために、連邦議会が大統領権限の行使の枠組を制定したものである。

（2）秘密捜索[99]

FISA（外国諜報監視法）には、1995 年に追加された第 3 編（物理的捜索）もある。これは、秘密捜索の規定であり、第 1 篇（電子的監視）の規定に準じて、FISC（外国諜報監視裁判所）の個別命令を得て行われる。第 1 篇同様に、外国大使館等の純粋な外国施設には FISC の命令を要せず、また、緊急時には FISC の裁判官一人に通告をした上で FISC の命令を得ずに秘密捜索ができる。この秘密捜索では、パソコンやスマホなどに保存されたデータを、コピーなどにより秘密裡に取得することも可能である。

スパイ事件ではなく有名なテロ未遂事件であるが、FBI は 2009 年にナジブラ・ザジによるニューヨーク地下鉄同時爆破テロを未然に阻止したが、その際、ザジの宿泊したホテルの部屋に対して秘密捜索が行われた。その根拠は本条によると推定されている[100]。

---

96 50 U.S.C. § 1805。第 1 篇による傍受期間は、米国人対象の場合は当初 90 日間で、延長（各 90 日間）が可能。米国内の外国勢力や非米国人を対象とする場合は、当初 1 年間又は 120 日で、延長（各 1 年間）が可能。延長の反復も可能であるので、必要があれば数年に及ぶような相当長期の傍受が可能である。他方、第 7 篇による傍受では、そもそも法律による傍受期間の設定が存在しない。

97 50 U.S.C. § 1806、50 U.S.C. § 1881e。

98 FBI など米国の法執行機関は、特に FISA 第 1 篇による通信傍受情報については、その収集手法を秘匿するために、parallel construction という手法を使っていると言われている。parallel construction とは、FISA などの機微な情報収集手法を裁判で開示しなくて済むように、同様の証拠を「裁判で提示可能な別の秘密でない捜査手段」を使って作り直すことを意味する。そのため、既に FISA による通信傍受で得た情報を、裁判呈示用に捜索令状を得て再度取得し直すことも行われているという。

99 米国には、司法捜査においても秘密捜索（通称、Sneak and Peek Search 忍込み捜索）が認められているが、30 日以内（裁判所の許可で延長可能）に対象者に通知する必要がある。18 U.S.C. §3103a と Rule 41(f)(3)。

100 茂田忠良「テロ対策に見る我が国の課題」『警察学会資料』113 号（2020 年 11 月）37-39 頁。

なお、本秘密捜索も、法律制定以前から大統領の行政権限に本来的に付随する権限として行われてきたものを、1995 年に FISA に追加規定したものである。

（3）司法通信傍受

米国では、司法通信傍受の一般法は 1968 年に制定された「通信傍受法」[101]である。この司法通信傍受は、FISA による行政傍受と比べて要件は厳しいものの、行政傍受などで端緒情報を把握した後に、司法通信傍受に移行して、スパイ活動の解明検挙に使用することが可能であり、スパイ対策でも貢献している。

司法傍受は裁判所の令状を得て行うのであるが、具体的な要件を見てみる[102]。第 1 に、特定の犯罪の遂行を疑う相当の理由が必要である[103]。第 2 に、他の捜査手法では目的を達成できない、或いは危険過ぎるなど、通信傍受の必要性(補充性要件)を説明する必要がある。第 3 に、傍受期間は 30 日以内であるが、期間延長の繰り返しは可能であり、傍受期間の合計は 1 年を超えることも可能である。第 4 に、傍受終了後 90 日以内に、傍受対象者に傍受の事実を告知することとされているが、裁判官に必要性を説明すれば、告知時期の延期が可能であり、この延期期間には法律上の制限はない[104]。更に、裁判所の令状を得る暇の無い時は、48 時間以内の通信傍受の緊急執行も認められている[105]。その上、米国では 1994 年通信傍受支援法[106]によって、電気通信事業者に迅

ザジが泊まったホテルの部屋を FBI が秘密捜索をして、爆破テロに関する資料を収集したが、裁判には証拠として提出されなかった。因みに、ザジが爆破テロを計画しているのを把握した端緒情報は、NSA による FISA 第 7 篇（702 条）による収集で、米国内のザジとパキスタン内のアルカイダ幹部が爆弾の製造方法について隠語を使って通信してしていたのを捕捉したことであるが、この通信も裁判には提出されなかった。

101 1968 年総合犯罪対策・街路安全法第 3 編（Title III of the Omnibus Crime Control and Safe Streets Act of 1968）。

102 18U.S.C. §2518。

103 18U.S.C. §2518(3)(a) 。個人が犯罪を遂行している、遂行した、又は遂行しようとしていると信じる相当な理由。なお、「相当の理由」の要件は、18U.S.C. §2518(3)(b) 「当該犯罪に関する通信が傍受できると信じる相当の理由」も必要であるが、これは通信傍受について当然の要件なので、本文での記述は省略した。

104 18U.S.C. §2518(8)(d)。

105 但し、傍受開始後 48 時間以内に、裁判所から通信傍受令状の発布を受けないと、傍受データは違法に収集されたものと看做される。18U.S.C. §2518（7）（ｂ）.

106 1994 年通信傍受支援法（Communications Assistance for Law Enforcement Act：CALEA）。本法は、通信事業者に対して法執行機関による通信傍受への協力を義務付ける法律である。主な内容は、迅速な通信傍受を可能とする能力（システム）の構築と、24 時間 365 日対応可能な連絡窓口（ワンストップサービス）の設置である（合衆国法典 47 篇 1002 条、連邦規則集 47 篇 1.20003 条）。この結果、大手通信キャリアでは傍受インターフェースが常に起動しており、FBI など法執行機関から適法な通信傍受の要請を受信次第、窓口担当者が即座に傍受対象番号を入力することで通信傍受が開始される。通信キャリアと FBI の間は専用回線が設置されているため、傍受結果は迅速に提供される。

このため AT&T や Verizon などの通信キャリアは、法執行支援センターなどという名称で、24 時間稼働する法執行機関との窓口を設置している。FBI など連邦機関の他に、州や自治体の法執行機関からの依頼もあるので、年間 10 万件を超える傍受を受付ているという。一方、米国に限らず、世界の多くの国では米国と同様の法制（例えば欧州では ETSI LI）があるため、Cisco、Nokia や Ericsson

速な通信傍受の協力を義務付け、FBI との間には専用回線が設置されおり、極めて迅速に通信傍受を実施することが可能となっている。

これに対して、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、確認しておこう。我が国の通信傍受法では、対象犯罪は、薬物犯罪、武器犯罪、殺人等の組織的な犯罪に限定されている。そもそも特定秘密保護法違反や公務員の守秘義務違反、或いは営業秘密の侵害など、秘密漏洩・秘密窃取関係の犯罪は、傍受対象犯罪ではないので、我が国の通信傍受法はスパイの探知摘発には使えない。仮に、特定秘密保護法違反等の犯罪を対象犯罪に加える法改正をしたとしても、次の理由から殆ど効果は見込めない。

第 1 に、組織的な犯罪ににについて、特定の犯罪の遂行を疑うに足りる「十分な理由」が必要であり、且つ、数人の共謀であると疑うに足りる状況が必要である。傍受開始の時点で「十分な理由」と「共謀性」を示す必要があり[107]、極めてハードルが高い。第 2 に、補充性の要件、即ち、他の捜査方法では当該犯罪の証拠収集が「著しく困難」であることと要件が加重されている[108]。第 3 に、傍受期間は 10 日以内であり、延長をしても最長 30 日を超えることはできない[109]。第 4 に、傍受対象者に傍受の事実を告知するのは、傍受終了後 30 日以内が原則であり、裁判官の許可を得ても最長 60 日以内である[110]。このように、我が国の通信傍受の要件は極めて厳しい。先ずスパイ捜査で、傍受開始のための「十分な理由」と「共謀性」などの要件を当初から満たすことは困難である。更に、傍受期間が短く、また、傍受開始後、遅くとも 90 日以内に対象者に傍受の事実を告知しなければならない。スパイ活動などの解明には長期間を要するが、これでは捜査途上で対象者に捜査していると警告する結果となる。スパイの探知解明には使えないのは明白である。

実際、我が国の通信傍受法による通信傍受の件数は極めて少ない[111]。現在の捜査実務では、捜査の終盤で既に逮捕相当の証拠を収集した段階で、共犯者などの犯罪組織の全体像を解明するために使用されており、捜査の初期乃至中期段階で捜査の突破口を開くためには使用できない。

（4）端末のハッキング

上記（3）の司法通信傍受の対象は、ライブの電話通話やインターネット通信を通信回線から傍受するものであるが、米国では、通信機器そのもの、典型的にはスマートフォン端末をハッキングして、端末に保存されたデータを収集したり、端末の位置情報を取得したり、端末のカメラや

などの世界的な通信機器メーカーは、その製品に最初から傍受機能・傍受管理機能を附置（built-in）した通信機器システムを販売している。また、Verint など傍受・傍受管理用の専用機器を販売する企業も存在している。

なお、本通信傍受支援法は、通信傍受の対象を司法通信傍受に限定していないため、FBI は FISA 第 1 篇による行政傍受にも本法のデータ収集システムを使用しているようである。

107 通信傍受法 3 条。

108 通信傍受法 3 条。

109 通信傍受法 7 条。

110 通信傍受法 30 条。

111 著者が某民間通信企業に聞いたところでは、我が国の通信システムには、米国の様な通信傍受のための専用設備は存在せず、その都度、技術者が対応しているという。

マイク機能を使用する（遠隔操作する）ことも可能である。

法律的根拠は、連邦刑事訴訟規則 41 条[112]の捜索差押の規定である。本条による令状発布の要件は「相当の理由」[113]であり、特別な加重要件はない。なお、行政通信傍受では、前述した FISA（外国諜報監視法）第 1 篇の規定によって、端末のハッキングが可能であり、且つ対象者に事後的にもハッキングの事実を告知する必要はない。これに対して司法手続（捜索差押）によるハッキングは、FISA と異なり、事後に対象者にその事実を告知する必要がある。告知は執行後 30 日以内に行う必要があるが、不告知期間は延長が可能であり、その必要性が説明できる限り、延長回数に制限はない[114]。

FBI の端末ハッキングの担当部署は、「作戦技術部（Operational Technology Division）」内の秘密部署「遠隔作戦ユニット（Remote Operation Unit）」[115]であり、ハッキング・ツールは民間から購入したり[116]、FBI で内製したりしている。

この端末ハッキングによって、スパイ協力者や（スパイの運用者である）外国工作員の使用端末をハッキングすることにより、重要な情報の入手が可能である。最近は、「シグナル」や「WhatsApp」など端末間暗号化アプリが普及して、通信回線の通信傍受では情報入手が困難な場合が増加しており、端末ハッキングは極めて重要な情報収集手段である。

なお我が国では、通信傍受法その他の法律に、端末のハッキングを可能とする規定は存在していない。

（5）データセンター情報の収集[117]

FBI のスパイの検挙事例を見ると、G メール、ホットメール、ヤフーメールなどのウェブメール、ボイス・メール、iCloud などのクラウドデータなど、IT 企業のデータセンターに保管された情報が重要な役割を果たしている。

これらの情報は、FISA 第 1 篇や第 7 篇による行政通信傍受で入手が可能であるが、司法捜査手続でも入手可能である。その根拠法は 1986 年保存通信法[118]である。この保存通信法 2703 条の規

---

112 Rule 41 of the Federal Rules of Criminal Procedure。スマートフォン端末のハッキングは、しばしば Remote Access Search（遠隔捜索）などと呼ばれている。

113 Rule 41(d)(1).

114 18 U.S.C. § 3103a(b)(3) and Rule 41(f)(3).

115 Lorenzo Franceschi-Bicchierai, “FBI Spies on Suspected Criminals by Hacking into Computers,” *Mashable com,* 3 August 2013, accessed 7 December 2025, https://mashable.com/archive/fbi-hacking-criminals.

116 イタリア企業 Hacking Team の RCS スパイウェアやイスラエル企業 NSO の Pegasus スパウェアを購入した事実が知られている。---Joseph Cox, “The FBI Spent $775K on Hacking Team's Spy Tools Since 2011,” *Wired,* 6 July 2015, accessed 7 December 2025, https://www.wired.com/2015/07/fbi-spent-775k-hacking-teams-spy-tools-since-2011
--- Mark Mazzetti and Ronen Bergman, “Internal Documents Show How Close the F.B.I. Came to Deploying Spyware,” *the New York Times*, updated 15 November 2025.

117 データセンター情報の収集は、我が国でも、司法手続の捜索差押によって一定程度行われている。

118 18U.S.C. §2703

定により、ウェブメール、クラウドデータの内容や携帯端末の位置情報履歴は、連邦刑事訴訟規則 41 条の捜索差押の手続によって入手可能である[119]。対象者に対する事後告知も、原則 30 日以内であるが、不告知期間の延長が可能である[120]。

捜査実務では、parallel construction のために、FISA 第 1 篇や第 7 篇による行政調査で得た情報と同一の情報を、刑事裁判用に、この司法手続（捜索差押令状）によって、再度収集することが行われているようであり、データセンターに保管された情報を収集できる 1986 年保存通信法の価値は高い。

（6）位置情報やクレジットカード使用情報

先に、我が国のスパイ捜査では、尾行張込が多用されるのに対して、欧米では多用されないと述べた。通信傍受など他の調査・捜査手段があるためであり、例えば、対象者の携帯端末をハッキングすれば、対象者の位置情報を含め多くの情報を得ることができる。とは言え、対象者の行動確認・動向の把握が不要な訳ではない。ところが米国では、尾行張込の替わりに、或いは尾行張込の補助として、対象者の携帯端末や自動車情報を使ってリアルタイムの所在確認が可能である。

即ち、対象者が携帯端末を持っていたり、自動車を運転したりしている場合には、携帯端末の GPS 情報や自動車のテレマティックス情報[121]から、ほぼリアルタイムで位置情報を把握することができる。FBI は、これらの情報を FISA 第 1 篇の規定により FISC（外国諜報監視裁判所）命令を得て、或いは司法捜査手続による捜索差押状[122]を得て、通信事業会社や自動車サービス企業から入手できるのである[123]。また、緊急時には、FISA 第 1 篇の規定による令状なしの執行も認められている[124]。

また、クレジットカードの使用情報についても、連邦刑事訴訟規則 41 条の捜索差押でリアルタイムの把握が可能である[125]。

---

119 位置情報以外のメタデータは、2073 条（d）項の規定により、捜索差押の要件よりも緩い要件で入手可能である。

120 18 U.S.C. § 3103a(b)(3) and Rule 41(f)(3).

121 自動車のテレマティックス情報とは、自動車の位置や走行状態に関する情報を常時送受信するもので、自動車メーカーがサービス向上のため導入し、2000 年代に普及が始まり 2010 年代以降は標準化している。OnStar (GM), Hyundai Blue Link , Uconnect (Chrysler), BMW ConnectedDrive , SYNC(Ford), T-Connect(トヨタ), NissanConnect, Honda CONNECT, SUZUKI CONNECT, ダイハツコネクトなど各社が導入している。

122 法律的根拠は、連邦刑事訴訟規則 41 条の捜索差押の規定である。

123 位置情報のリアルタイム取得には、通信事業会社に関しては、脚注 106 で既述した 1994 年通信傍受支援法のための制度が使用されている。自動車のテレマティックス情報に関しては、各企業が法執行機関と 24 時間対応可能な窓口を設置している。

124 法律的根拠は、外国諜報監視法 FISA1805（e）。人の生命や重傷を惹起する可能性がある場合は保存通信法 18USC2702(b)(8)及び(c)(4)による緊急執行も可能である。

125 VISA、マスターカード、アメックスなどのカード発行金融機関やカード企業については、発行金融機関は、通信事業者同様に、法執行支援センターなどの連絡窓口を設置しており、そこを経由してリアルタイム又はニアリアルタイムでの情報入手が可能である。なお、過去のクレジットカードの使用記録は、保存通信法 18USC2703 により取得可能である。

これに対して、我が国では、筆者が現場の警察官に聞いた限りでは、このようなリアルタイムでの位置情報等の取得は行われていない。

以上、米国における FBI の情報収集権限を見てきたが、我が国とは大きな違いがあることが分かるであろう[126]。

4－3　処罰規定の違い

次にスパイ防止に有効な処罰規定を見てみよう。最近のスパイ防止法制の議論では、米国のスパイ防止法と外国代理人登録法に言及されることが多いようである。そこで、両者について論ずると共に、両者よりも重要な処罰規定について述べる。

（1）米国 1917 年スパイ防止法

米国には 1917 年スパイ防止法があるが、我が国でも 2013 年に特定秘密保護法が制定されており、米国同様、一定の情報漏洩やスパイ行為には罰則がかかるようになっている。

但し、異なる点がある。第 1 に罰則の軽重である。米国では、最高刑は死刑や終身刑まであるが、我が国では 10 年の拘禁刑が最高刑である。第 2 に犯罪の構成要件の違いである。特定秘密保護法 23 条では、業務従事者が特定秘密を漏洩すると処罰されるが、スパイ防止法 793 条(e)(d)項では、国防情報の不正伝達或いは不正所持だけで、業務従事者か否かに関係なく、且つ外部に漏洩しなくても可罰的となる[127]・[128]。第 3 に外国工作員に適用されるべき構成要件と罰則の軽重の問題である。特定秘密保護法では、外国工作員が我が国のインテリジェンス機関職員に特定秘密の提供を働き掛けても、それ以外に特定の違法行為を犯さなければ[129]、情報漏洩の教唆扇動罪（25 条）で最高刑は 5 年の拘禁刑に過ぎない。更に第 4 は、併合罪制度の不存在である。これはスパイ防止法に限った話ではないが、米国には我が国の様な併合罪の制度がないので、量刑は罪数の

---

126 この他にも、スパイ調査・捜査に使用できる情報ツールとしては、監視カメラがある。例えば、ニューヨーク市には市警察とマイクロソフト社が共同運営する数万台の監視カメラがあり、ニューヨーク市警の協力を得てリアルタイム監視が可能である。ロンドン市にも、ロンドン警視庁がリアルタイム監視に使用できる監視カメラが数万台設置されていると言われる。ニューヨーク市内やロンドン市内では、これらの監視カメラシステムや携帯端末の位置諜報を使用して、人的尾行を代替する行動監視が可能であると推定できる。

これに対して、我が国の警視庁では、事件発生後に民間防犯カメラ等の映像を利用した所謂「リレー捜査」は有名であるが、筆者が知る限り、人的尾行を代替してリアルタイム監視に使用できるような公的カメラシステムは設置されていない。

127　更に 793 条(f)項は、重過失による不正伝達・不正所持も可罰的としており、故意の不存在を理由とする抗弁を許さない仕組となってい。また、同僚による不正伝達・不正所持を知りながら報告しない行為も可罰的とされているなど、秘密漏洩防止のため実践的な規定となっている。

128 法 794 条（c）項では共謀行為自体が可罰的となっている。共謀罪では、国防情報を実際に外国政府に伝達したことを立証する必要がないので、FBI は 794 条では（c）項の共謀罪を好んで適用している。

129　特定秘密保護法 24 条によれば、暴行脅迫、窃取損壊、不正アクセスなど特定秘密保有者の管理を害する行為によって特定秘密を取得した場合に、漸く 10 年以下の拘禁刑となる。

数だけ積み上がり重い科刑となり易いのである。過去の裁判例では、中国スパイのラリー・ウータイ・チン（CIA 職員）、ロシアの協力者であったオルドリッジ・エイムズ（CIA 職員）、同ロバート・ハンセン（FBI 職員）などは終身刑が宣告されている[130]。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[131]には拘禁刑 35 年が宣告された。

米国の 1917 年スパイ防止法と我が国の特定秘密保護法には、上記のような違いがあるので、構成要件の拡張や外国工作員による情報漏洩の教唆扇動罪の重罰化などは、有意義であるが、それをしても、スパイ防止のための処罰規定が整備されたとは言い難い。1917 年スパイ防止法は、米国でスパイ検挙に使用される処罰規定の一部にしか過ぎないからである。

（2）外国代理人登録法と外国政府代理人届出義務違反罪[132]

現在、外国代理人登録法も議論の俎上に上っている。しかし、米国の外国代理人登録法（合衆国法典 22 篇 611～621 条）と外国政府代理人届出義務違反罪（同 18 篇 951 条）の混同が危惧される。スパイ摘発で活用されているのは、後者なのである。

外国代理人登録法（FARA: Foreign Agents Registration Act of 1938）は、外国主体(foreign principal)の利益のために行うロビー活動や世論形成活動の「透明化」を目的とする行政規制法である。米国司法省は、違反者に対しては、従来は検挙よりも警告を発し登録を促す運用をしてきた。近時、司法省も取締りの道具として再評価し適用に積極的になっているものの、「故意」の立証が難しく、有罪事例はそれ程多くない状況である。

勿論、外国代理人登録法は、無秩序なロビー活動の規制には効果があるので、立法自体は望ましい。但し、秘密裡に活動する外国のスパイやその協力者の取締りには、米国では主に外国政府代理人届出義務違反罪（合衆国法典 18 篇 951 条）という刑法の規定を適用しており、検挙件数も多数に及ぶ。

外国政府代理人届出義務違反罪は 1948 年制定の刑罰法規である。スパイ対策としては、1917 年制定のスパイ防止法が既に存在していたのであるが、国防情報に係わらない諜報工作は対象外であり、また、国防情報もその立証を要するなど、必ずしもスパイ防止に活用し易い罰則規定ではなかった。そこで、スパイ防止法による処罰行為の前段階や周辺領域の行為を取り締まる罰則規定として制定されたのである。そのため、本条は「準スパイ罪」や「防諜法」とも呼ばれている。

規定の内容は、（外交官や領事館員以外の者が）「外国政府の代理人」(an agent of a foreign government)として活動する場合に、司法長官への届出をせずに活動すると 10 年以下の拘禁刑に処せられる。外国の工作員は、外国政府の代理人であるが、当然のことながら届出はしない。そ

---

130 厳密に言えば、ラリー・ウータイ・チンは、終身刑 2 つ相当の有罪判決を受けたが、科刑宣告の前に自殺した。オルドリッジ・エイムズは、司法取引をして、仮釈放なしの終身刑 1 つの科刑宣告を受けた。ロバート・ハンセンは、仮釈放なしの終身刑 15 個の科刑宣告を受けた。

131 ブラッドレイ・マニングは、スパイ防止法 793 条違反 6 件、政府財産の窃盗（データ不正取得）5 件、コンピュータ不正使用 2 件、軍法違反などで有罪を認定されている。

132 より詳しくは、茂田ウェブサイト「米国の外国代理人登録法と外国政府代理人届出義務違反罪の違い」（2026 年 3 月 9 日）、https://shigetatadayoshi.com/2026/03/09/fara-and-18-u-s-c-951/

こで、外国政府或いは外国政府職員の指揮下で活動していること（活動内容は問わない）さえ立証すれば、本条違反が成立する。このように、立証が容易で、刑罰も重いので、最近の FBI による外国工作員や協力者の摘発では、本罰則が活用されている。

有名な事例としては、2010 年のロシアの在米スパイ 10 人の一斉逮捕がある。アンナ・チャップマンら 10 人は、ロシア諜報機関 SVR の工作員であることを秘匿して米国社会に入り込み、米国社会の中枢に着々と接近していた。20 年以上も米国で生活していた工作員もいれば、息子を名門大学に入学させて米国エリート社会への潜入を画策していた工作員もいた。発覚の端緒はロシア SVR 内に米国が獲得した協力者からの情報であるが、FBI は通信傍受（居宅への傍受機器の設置を含む）などによって、10 人が SVR の担当者から指揮命令を受けて活動していることを立証して、外国政府代理人登録義務違反罪で逮捕したのである。

この他にも、外国政府代理人届出義務違反罪による検挙は多数に上る。同違反罪の適用が増加している背景には、冷戦期にはウータイ・チンやエイムズやハンセンのように政府中枢に潜伏する古典的なスパイ活動が注目されたが、21 世紀になると、学術研究者、企業技術者、シンクタンク研究員、政治ロビイスト、地方政治家など幅広い層を利用した非伝統的なスパイ活動（科学技術窃取、産業スパイ、影響力工作など）が注目されるようになったことが挙げられる。非伝統的なスパイ活動には、スパイ防止法では対処できないのである。

ところで、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る。現在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ことが最も効率的である。但し、通信傍受ができなくても、携帯電話などの捜索差押によってある程度の立証は可能であろう。

（3）虚偽供述罪（合衆国法典 18 篇 1001 条）他の処罰規定

外国政府代理人届出義務違反罪の他にも、FBI が活用している刑罰法規は種々あるが、最も重要な処罰規定は、虚偽供述罪である。

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、5 年以下の拘禁刑に処せられる。FBI 捜査官や入国審査官の事情聴取に対して嘘の供述をすると本条違反になる。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な規定である[133]。外国工作員や協力者は FBI による面接インタビューの際は、黙秘しても良いのであるが、大体疚（やま）しいことを隠して嘘を付くことが多い。そこで、本条違反が成立するのである。FBI は、スパイ防止対策で、本条単独で検挙する場合もあれば、より悪質な事案の入口事件としても適用している。

本条適用の実例を見てみよう。例えば、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た。彼はロシア大使館の工作員と 8 年間に亘って付合い、その間、飲食の接待を受

---

[133] 「3—3 人的保全（Personnel Security）（３）質問票」で述べたように、本条は、政府の行政手続において、虚偽の申請や申告を防止するために極めて重要な規定でもある。

けたり現金を受領したりしていたのであるが、結局、不起訴となった。秘密資料の提供などが立証できなかったためであろう。他方、米国の類似の事例としては、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る。彼女は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ていなかった。そこで、秘密情報の提供は立証できなかったものの、中国人との関係の不申告が違法とされたのである。結局、彼女は司法取引で虚偽供述罪などを認めて拘禁刑 40 ヵ月の判決を受けた。行為自体の悪性はクレイボーンの方が軽いと思われるが、それでも実刑となったのである。日米の処罰規定の違いが現れている。

その他にも、政府財産の窃盗（同 18 篇 641 条：情報窃盗を含む）[134]、通信詐欺（同 1343 条）[135]、査証詐欺（同 1546 条）[136]、マネロン違反（同 1956 条）[137]など多彩な罰条がスパイ対策では適用されている。

1917 年スパイ防止法や外国代理人登録法（FARA）だけでは、スパイ防止のための罰則規定としては不十分であり、幅広い刑罰規定の整備が必要なことが理解できるであろう。

4－4　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であるが、刑事司法の運用でも問題がある。特にスパイの抑止力を弱めているのが、「寛刑主義」である。「寛刑主義」とは、我が国の刑事司法の量刑の特徴を、東京大学名誉教授・先端科学技術研究センター特任教授の玉井克哉氏が形容した言葉である[138]。

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る。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ある。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る。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。

しかし、外国のスパイやサイバー攻撃を仕掛けてくる外国の犯罪者はどうであろうか。彼らはそもそも日本社会の一員になりたいなどとは考えない人々である。或いは、トクリュウなど犯罪企業的な集団も増加している。彼らに対しては「寛刑主義」は意味をなさない。

---

134 10 年以下の拘禁刑。

135 電子メールで虚偽申請、オンライン申請で助成金詐欺、研究資金の虚偽申請、電子通信を使った企業秘密窃取など、州際通信を使用して詐欺行為（虚偽申請、虚偽説明など）をすると成立する。20 年以下の拘禁刑。

136 外国政府の工作員が、外国政府との関係を隠して米国査証を取得すると違反となる。10 年以下の拘禁刑。

137 違法行為のために米国の内と外の間で資金を移動させると本条違反となる。外国工作員の活動資金は、使途を隠して送金されることが通常であるから、外国政府代理人届出義務違反の工作員が国内外間で活動資金の移動に関与すると、本条違反となる。罰則は 20 年以下の拘禁刑。

138 玉井克哉「警察政策学会第 25 回シンポジウム 経済安全保障 基調講演（2）技術流出問題にどう対処するか～経済安保とインテリジェンス機関の役割～」『警察政策』第 26 巻（2024 年）33 頁。

これで想起されるのは、北朝鮮の工作員に対する量刑である。彼らは対日工作のために海から工作船を使って密入出国を繰り返していた。前世紀には警察は海岸線を警戒して多くの工作員を逮捕してきたが、裁判所の量刑の相場は、極めて軽い。警察 OB で外事警察の専門家であった佐々淳行氏は、北朝鮮の工作員を検挙しても、懲役 1 年執行猶予 4 年が量刑相場であったと嘆いている[139]。実際の量刑を警察庁資料[140]で見ると、米軍占領時代の 1950 年に警視庁が検挙した北朝鮮スパイ事件では、占領目的阻害行為処罰令違反で懲役 10 年の刑が宣告されているが、占領終結・主権回復後は、スパイ工作員自体に対する処罰法令がないため、密入国を捉えて出入国管理令違反や外国人登録法違反を適用しているものの、科刑は懲役 1 年程度であった[141]。且つ、それも執行猶予が付くのが常態となってきた。1966 年以降の出入国管理令や外国人登録法違反事件の検挙事例を見ると[142]、量刑の平均は懲役 1 年であり、大半に執行猶予（平均期間は 3 年）が付き、実刑を科されたのは約 2 割強に過ぎない。

このような状況であるから、北朝鮮の工作員は、逮捕されても直に帰国できたのである。つまり、執行猶予が付けば、裁判が終われば北朝鮮に帰国できたのである。北朝鮮では工作員に対して「逮捕されても 6 ヵ月で帰国できるぞ」と言って送り出していたと言う。他方、これでは、刑罰の抑止力は全くない。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か。

また、最近の事例では、2018 年に産業技術研究所の中国人研究者が、研究データ（フッ素化合物の合成技術データ）を中国に不正に送信して、中国で妻の経営する企業が特許登録をする事案があった。不正競争防止法（営業秘密侵害）違反[143]で起訴されたが、2025 年 2 月の第 1 審判決では、懲役 2 年 6 月執行猶予 4 年、罰金 200 万円で、実刑判決は免れている。驚くほど、軽い量刑である[144]。

これが我が国の裁判所の量刑の相場、常識であるが、我が国の裁判所の「寛刑主義」は時代の要請に応えられなくなっている。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。且つ、その実態を国民が知り得ない、著しく透明性を欠く慣行である。

---

139 佐々淳行『金日成閣下の無線機』（読売新聞社、1992 年）18-19 頁。入国管理令の密入国に対する刑罰は 3 年以下の懲役であったが、通信機、暗号表など工作員であることを明白に示す物的証拠があっても、科刑の平均は 1 年の懲役なのであった。

140 警察庁警備局『治安の回顧と展望（令和 3 年版）』（2021 年 12 月）資料 5-6 頁、「北朝鮮関係諜報事件一覧表」

141 1953 年に検挙した第二次朝鮮スパイ事件では、懲役 1 年である。

142 前掲の警察庁資料で、1966 年～2021 年 11 月までに、出入国管理令違反や外国人登録法違反で検挙された 35 人の処罰を見ると、内、起訴猶予が 4 人、実刑判決が 8 人、執行猶予付き懲役刑が 23 人である。刑期は 6 月から 1 年 6 月が多く、平均は約 1 年。執行猶予の期間は、2 年から 4 年が多く、平均は約 3 年である。

143 罰則は、10 年以下の懲役又は 2000 万円以下の罰金。不正競争防止法 21 条。

144 仮に同種事件が米国で摘発されれば、合衆国法典 18 篇（刑法）の 1831 条（経済スパイ）、1832 条（営業秘密窃取）、1343 条（通信詐欺）などの罰条が適用され、最低でも、数年間の拘禁刑の実刑と多額の懲罰的罰金刑が科され、執行猶予が付くことは先ずあり得ないであろう。

我が国に帰属意識のない外国工作員やその協力者、或いは産業スパイなど、広義のスパイ活動に対しては、犯罪の実態を直視して、量刑相場を再考する必要があるだろう。

5　攻勢的防諜

攻勢的防諜とは、スパイを摘発検挙するなどして防御するのではなく、それ以上の活動、即ち、脅威国諜報機関の活動そのものを利用したり、攪乱し無力化したりする攻勢的な作戦である。幾つかの主要な手法がある。

例えば、脅威国のスパイや協力者を発見探知した場合にも、摘発せずに泳がせる。そして、これに意図的に偽情報を掴ませて、本国に報告させて、敵を欺瞞する手法がある。或いは、二重スパイの運用がある。脅威国のスパイや協力者を転向させて自国のエージェントとして運用する手法である。そうすることによって、脅威国の情報関心を把握したり、偽情報を流して脅威国の諜報機関を攪乱したりするのである。このような活動は、セキュリティ・サービスが担当することが多く、米国では FBI の国家安全保障部門が取り組んでいる[145]。

この手法で歴史的に有名なのは、英国セキュリティ・サービス（MI5）が第二次世界大戦中に実施したダブル・クロス作戦である。英国は、ドイツが潜入させたスパイを捕まえて、英国側の二重スパイとして運用し、ドイツに偽情報を送り続けたのである。特に大きな成果が、ノルマンディー上陸作戦の欺瞞である。米英軍による上陸作戦の地点はより東のカレー地方との偽情報を流してドイツに信じこませ、上陸作戦を成功に導いたことが挙げられる[146]。

また、スパイ工作の策源地となっている脅威国の諜報機関の中枢に浸透して、脅威国の諜報組織中枢からの情報を基に対策を行う手法もある。ヒューミントとシギントの実例を示す。

ヒューミントの例では、既述したように 2010 年の夏、FBI はロシアの工作員 10 人を一斉に逮捕した。10 人はロシアの対外諜報機関 SVR が米国に派遣したイリーガル（秘密諜報員）だった。彼らの多くはロシア出身を隠して、偽名で米国の上流社会に溶け込み、将来の工作活動のための地歩を築いていたのである。正に江戸時代の隠密「草」のような存在である。

探知解明の端緒は、実はロシアの諜報機関 SVR の幹部アレクサンダー・ポテフ大佐を米国 CIA が協力者として獲得したことである。ポテフ大佐は SVR の S 局（イリーガル担当）副局長であったが、彼からの情報を端緒に FBI が 10 人を監視し、通信傍受などによって指揮連絡状況を解明

---

145 但し、二重スパイの運用は難しい。米国で失敗例として有名な事例に、中国出身のスパイ、カトレーナ・レオン（カリフォルニア在住）の例がある。FBI は、1984 年以降レオンを二重スパイとして運用して、中国情報を収集している積りであったが、彼女は、実は中国国家安全部の指示に従う三重スパイであった。漸くそれが判明したのは 2002 年であった。この間、FBI はレオンから中国の「韜光養晦」戦略に沿った偽情報を掴まされていたのである。

146 ノルマンディー上陸作戦時の欺瞞作戦としては、このヒューミント作戦のほか、軍がカレー上陸作戦を指向していることを示す偽装無線通信も行われている。

して、SVR 工作員である証拠を収集したのである[147]。逮捕時の罪名は、外国政府代理人届出義務違反（合衆国法典 18 篇 951 条）とマネロン違反（同 1956 条）であった。マネロン違反は活動資金を秘密裡に本国から受領していたからである。彼らの多くはスリーパー状態で、違法な情報収集活動は未着手であったので、こういう罪名になったのである。

シギントの例は、2013 年の NSA 職員スノーデンの漏洩情報で判明している。当時、米国の国家シギント機関 NSA（国家安全保障庁）は、米国を標的とするハッカー集団のサーバーや端末を逆にハッキングして、マルウェアなどの攻撃手法、攻撃の標的や時期、或いは既に窃取されたデータなどを解明していた。漏洩情報によれば、当時世界の 28 のハッカー集団のシステムに侵入して、対抗措置を取っていたそうである。中国については、12 の集団を解明対象としていて、その内 7 又は 8 のグループに対してはハッキングに成功していた[148]。

このように工作の策源地となっている脅威国の諜報組織に浸透して、その中枢から情報を得られれば、スパイ対策は大きく進展する。但し、このような攻勢的防諜に我が国が取り組むには、インテリジェンスに対する発想の転換など、越えなければならない多くの課題がある。

6　提言

以上、スパイ防止に必要な制度や法律を、純粋防御、積極防御、攻勢的防諜の三つの面に分けて見て来た。スパイ対策には、多面的且つ多層的な対策が必要であり、各分野で着実に取り組んでいく必要があること、一つや二つの法律制定で措置できるような単純なものではないことが明らかになったと考える。

純粋防御面では、秘密指定制度、防諜・保全担当部署の整備、人的保全（セキュリティクリアランス等）、物的保全、情報保全、内部脅威対策、民間企業による防御措置と政府の協力態勢、情報の「サニタイズ」など、各分野とも対策の強化が必要である。

また、積極防御面でも、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、我が国のスパイ対策は米国と対比して著しく弱体であることが明らかになった。効果的な対策を行うには、通信傍受を含む国家安全保障のための行政調査権限の創設、司法捜査権限の強化、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ある。

---

147 ポテフ大佐は、FBI によるイリーガル 10 人の逮捕直前に、ロシアを脱出した。2011 年には、欠席裁判で国家反逆罪で 25 年の懲役刑を宣告されている。

148 茂田忠良「米国国家安全保障庁の実態研究」『警察学会資料』82 号（2015 年 9 月）95-96 頁。

同「サイバーセキュリティとシギント機関～NSA 他 UKUSA 諸機関の取組～」原本は情報セキュリティ総合科学第 11 号（2019 年 11 月）、【修正版】（2025 年 11 月）42-44 頁。https://shigetatadayoshi.com/wp-content/uploads/2025/11/cybersecurity-and-NSAUKUSA-revised.pdf。シギントでは、このような活動を C-CNE（Counter Computer Network Operation）と呼ぶが、攻勢的防諜の一類型と言えよう。

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あろう。特に行政通信傍受などは、現状では国民の支持が得られないであろう。

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制度や法律、その運用実態を知らないからである。そもそも、我が国の法学者や行政学者の殆どは、諸外国の国家安全保障のための法律制度を体系的に研究していない。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」と自認している。また、政府事務当局も研究が不足している。2024 年、サイバー対処能力強化法等の制定に向け政府有識者会議が開催されたが、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った[149]。このような状態で、行政通信傍受制度の創設など、スパイ防止のための制度や法律を議論しても、憲法の人権擁護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制度や法律を整備するのは困難であろう。現状で制定可能な法律を一つ、二つ制定しても、真に必要なスパイ防止のための包括的な制度や法律を構築できるとは思えない。

（1）英米スパイ防止制度と実務の包括的な調査研究

そこで、政府が現在取り組むべき最重要事は何であろうか。

それは、調査研究の専門組織を設置して、欧米、特に米英両国の国家安全保障のための法律制度と実務を徹底的に研究することである。情報史学研究家の江崎道朗氏は、「国際標準、具体的には英米諸国のインテリジェンス活動に関するスパイ防止法などの法律と運用、組織、予算などについて徹底的に調査し、国会に報告させよ」と提言している[150]。正にその通りである。国家情報会議や国家情報局、或いはカウンターインテリジェンス・センターに、専門の調査研究組織を設置して取り組むべきであろう。

その際重要なのは拙速に陥らないことである。この分野は、法律や数冊の著書を読んで全貌を理解できるようなものではく、また、数か月の研究で全貌を把握できる訳でもない。各国とも実務の実態は成るべく秘匿している。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ある。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る。また、関係国政府の協力を得て調査団を派遣するとしても、調査団は反復派遣する必要がある。十分な基礎知識や背景智識を持たない者が、一度の調査で全体を理解できるようなものではないからである。時間をかけて実務の実態を含む全体像を正しく理解して、研究成果をまとめるべきである。

---

149 事務局資料を読むと、「国外に所在する非米国人に対する行政傍受の一般的な根拠法令は対外諜報監視法である」「米国では行政通信傍受で取得した資料は裁判で使用できない」と解釈しているようであるが、何れも誤解である。詳しくは、茂田忠良ウェブサイト「サイバー安全保障・政府有識者会議の事務局資料の重大な誤り　（行政通信傍受資料の捜査利用等に関して）」（2024 年 9 月 2 日）、https://shigetatadayoshi.com/2024/09/02/errors-in-reference-materials-of-a-government-advisory-board/

150 江崎道朗「インテリジェンス諜報の世界 No.8　スパイ防止法は人権抑圧法に非ず」『正論』2025 年 11 月号、193 頁。

研究成果は国会はじめ関係者で共有して、議論の基礎資料とすべきである。迂遠なようにも見えるが、これが、包括的で効果的なスパイ防止の制度と法律を構築するに至る最短最良の方策であると考える。

（2）今すぐにでも出来る改革

そうは言っても、当面、調査研究以外に実行可能で効果的な施策はないであろうか。筆者は次の2点を提案したい。

（ア）防諜・保全専門部署の設置・強化

政府の防諜・保全態勢を強化するために、直ぐにでも実行可能なのは、防諜・保全専門部署の設置・強化である。既述のように、我が国では、防衛省・外務省・警察庁・公安調査庁などインテリジェンス関係省庁にも、その本省庁の防諜・保全の担当者は課長補佐レベルであり、課（政令職）レベル以上の専門部署が存在しない。政治のリーダーシップを以て、これら4省庁に課（政令職）レベルの防諜・保全専門部署を設置し、相当数の人員を配置する必要がある。その上で、米国同様に防諜・保全に関する幅広い任務と権限を付与すべきである。また、国家情報局のカウンターインテリジェンス・センターの態勢強化も必要であろう。重要なことは、この強化を「スクラップ・アンド・ビルド」の原則ではなく、政治決断によって「純増で」措置することである。

その上で、国家情報局のカウンターインテリジェンス・センターと4省庁課長の定例会合を設定して、これを情報共有と経験交流の場とするべきである。更に、4省庁の関係部署間の人事交流も行う必要があろう。必要に応じて、現場で外国の工作員や協力者の容疑者の監視活動を行っている、従って実情を熟知している警視庁公安部員も人事交流の対象に含めるべきであろう。

（イ）最も効果的な処罰規定の制定

最も効果的で、今でも立法可能な処罰規定は、米国の外国政府代理人届出義務違反罪と虚偽供述罪である。これらは、行政通信傍受権限がないと効果は半減するが、それでも一定の効果は見込める。当面この2罪の制定に取り組むべきである。但し、米国のような刑法典への記載は、現状では不可能であろうから、特別法で対処するべきである。

○　外国政府代理人届出義務違反罪：現在、複数の政党が提案している外国代理人登録法を立法する際に、外国主体の利益のために行うロビー活動や世論形成活動の「透明化」を目的とする行政規制法（米国 FARA）とするだけでなく、ここに米国刑法の外国政府代理人届出義務違反罪（法典18篇951条）、即ち、外国政府の代理人として無届で活動する工作員・協力者に対する罰則規定を書き込むべきである。

○　虚偽供述罪：米国の虚偽供述罪（法典18篇1001条）のように、政府の業務に関連して幅広く虚偽供述や虚偽記載を処罰する規定は、今直ちに国民の理解を得ることは困難であろう[151]。従

---

151 我が国には、現在、行政手続に関して虚偽申請や虚偽供述を処罰する一般的罰則規定は存在しない。個別の行政規制法で個別に虚偽申請や虚偽供述を可罰的とする法律は存在する。

って先ず、特定秘密保護法の適性評価の手続に関して虚偽供述や虚偽記載に対する処罰規定を加えるべきであろう。現在のようにセキュリティクリアランスを得るための質問表に虚偽記載をしたり、面接で虚偽供述をしたりしても、罰則が適用されない状態は異常である。適性評価の有効性を著しく阻害している。この異常状態は早期に解消する必要があり、特定秘密保護法の改正で可能である。

（3）量刑委員会の創設を

本稿で見たように、我が国警察の（産業スパイを含む）広義のスパイを探知検挙する能力は高くない。それは第 1 に我が国の処罰法令が不十分であり、第 2 に警察にはそのための行政調査権限がなく、司法捜査権限も極めて限定されているからである。そのような不利な条件の中で、警察官の大量動員と昼夜を分かたぬ努力によって漸くスパイを検挙起訴しても、宣告刑が犯罪の悪質性に見合わず、執行猶予付きであったり、軽かったりでは、検挙によるスパイ防止効果は望めない。

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。この状況を改善し、量刑相場の透明性を高めるためには、「量刑指針」の制定と公開が必要である。

米国では 1984 年量刑改革法に基づき、司法府に「合衆国量刑委員会」[152]が設置された。量刑委員会は「量刑ガイドライン」[153]を制定して定期的に見直しているが、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る。

我が国も、例えば最高裁事務総局に量刑委員会を設置して、「裁判官村」が形成してきた量刑相場を「量刑指針」[154]の形で開示し可視化するべきではないか。その上で、その「量刑指針」が、国民感覚から遊離していないか、衆参両議院の法務委員会で説明を求めるべきであろう。

---

[152] 委員は投票権のある委員が 7 人。大統領が上院の承認を得て任命する。その内裁判官は 3 人以上とされている。裁判官以外では、検事、弁護士、有識者から選ばれる。他に投票権の無い委員が 2 人、司法長官と米国仮釈放委員会会長である。委員会事務局には 90～100 人の専門家が勤務している。

[153] US Sentencing Commission, *2025 Guidelines Manual,* effective 1 November 2025, https://www.ussc.gov/guidelines/2025-guidelines-manual.
--US Congress, *How the Federal Sentencing Guidelines Work: An Abridged Overview* (CRS Report R41697, 2 July 2015)
https://www.congress.gov/crs_external_products/R/HTML/R41697.web.html

[154] 米国の量刑ガイドラインは、ポイント制を取り犯罪類型ごとに極めて精緻なものであるが、我が国ではそこまで詳しいものは必要ないと考える。

7　最後に：日本国憲法の特質に合わせた柔軟な憲法解釈の必要性

ところで最後に、我が国の憲法解釈の在るべき姿について述べてみたい。スパイ対策で必要な改革を行おうとすると、憲法解釈問題に到達せざるを得ないからである。例えば、国家安全保障のための行政通信傍受について議論すれば、我が国では、日本国憲法 21 条 2 項の「通信の秘密」に反するという主張が行われるであろう。

ところで、憲法解釈において重要なのは、我が国の現行憲法の特質を正しく理解することである。

そもそも日本国憲法は占領下に占領軍によって起草されたものである[155]。当時の米国の起草者の世界観は、第二次世界大戦は（現代風に言えば）「悪の枢軸」である日独伊三国の侵略によって惹き起こされた。従って、アジアにおいては、日本を非武装化して軍隊を持たせなければ二度と戦争は起きない筈である。こうして、憲法 9 条を定めて日本に戦力の保持を禁じた訳である。では、非武装化した日本はどうやって国の安全を守るのかというと、それは憲法前文にあるように「平和を愛する諸国民の公正と信義に信頼」するということになる。侵略国日本が軍隊を持たないのであるから、アジアは平和になる筈だったのである。日本国憲法は全体がこのような世界観に基づいており、主権国家の国益のぶつかり合いの世界、そのような世界に置かれた独立国家日本国による国家安全保障政策を想定していないのである[156]。

しかし、現実の世界は、憲法が予定した世界とは大きく異なっている。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を削る戦いの場である。従って、そのような実態を認識した上で、日本国の国家安全保障と国益が守られるように、憲法解釈も柔軟に行うべきであろう。

即ち、国家安全保障という視点が欠落している日本国憲法を解釈運用するに当たっては、単なる文理解釈ではなく、世界各国の比較憲法学或いは比較行政法学の知識を基礎に置いて、日本国憲法を独立国家の憲法として合理的に解釈する必要がある。例えば、筆者の知る限り、欧州諸国で国家安全保障のための行政通信傍受制度がない国は存在しないが、その故に欧州諸国は非民主的であると批判する我が国の憲法学者や行政法学者はいないであろう。要は、国民の人権保障と（国民の人権と自由を保障する）国家の安全保障の両者を如何にして節調するかという制度設計の問題であろう。

（以上）

155　日本国政府によるポツダム宣言の受諾に際し、連合国は（1945 年 8 月 11 日、バーンズ米国務長官名回答）は、「日本国の最終的な政体の形態は、自由に表明された日本国民の意思によって決定される。」と回答しているが、日本国の政体を定める日本国憲法が「自由に表明された日本国民の意思によって決定」されたものでないのは、その制定過程を見れば明白である。

156 これらの事情は、次の占領軍による初期の占領政策の総括文書を読めば明らかである。Supreme Commander for the Allied Powers, *Political Reorientation of Japan: September 1945 to September 1948*, Vols I, II, (Washington, D.C.: U.S. Government Printing Office, 1949), reprinted (Literary Licensing, LLC, April 2013).

警察政策学会資料　第147号

スパイ防止に必要な制度と法律

令和8（2026）年5月

編集　警察政策学会
テロ・安保問題研究部会

発行　警察政策学会

〒102-0093
東京都千代田区平河町1-5-5　後藤ビル2階
電話（03）3230-2918・(03-3230-7520)
FAX（03）3230-7007