国家安全保障戦略に基づく「情報力」の強化について

山本　達夫

戦後長い間、わが国の情報機能については、投入リソースの不足、情報機関同士の縦割り、政策部門との連携不足、秘密保全の不十分さ、中央情報機関の不在などの不備が論じられてきた。しかし、これらの問題の多くは、第二次安倍内閣の下で大幅に改善された。各省庁の情報は内閣情報官に集約され、NSC/NSS の創設により政策部門と情報部門との連携のパイプが確立し、特定秘密保護法の制定により各省庁をカバーする秘密保全体制が整備された。これらは安倍元総理の識見とリーダーシップ、北村滋前国家安全保障局長/内閣情報官を始めとする内閣官房・各省の行政官の努力によるものであり、高く評価されるべきであろう。

一方で、世界は今、歴史的な変革期を迎えている。国連の安保理常任理事国が国連憲章や国際人道法に明確に違反する武力侵略を行い、また別の安保理常任理事国は、「中華民族の復興」と称し国際法を無視した力による一方的な現状変更を進め、それを既成事実化しようとしている。

中国、北朝鮮、ロシアなど、軍事力を政策遂行の手段とする権威主義国家に囲まれた現在のわが国の安全保障環境は、わが国の歴史上という垂直軸で見ても、また現在の世界情勢という水平軸で見ても最も厳しい状況にあると言わざるを得ない。

その安全保障環境を受けて昨年の 12 月には、防衛力の抜本的な強化を目指し、いわゆる安全保障 3 文書が策定された。「国家安全保障戦略」においては、わが国の戦略的な目標を達成するための戦略的なアプローチとして、外交力、防衛力、経済力、技術力と並び情報力が挙げられ、国家戦略として情報の重視が明記された。厳しい安全保障環境の下でわが国の進むべき道を誤らないためには、国際社会での各国の動向、軍事・経済・技術面での世界の潮流、周辺諸国の軍事動向を迅速的確に把握することが不可欠であり、情報力の強化を戦略的アプローチの柱の一つを位置づけるのは至当な判断であろう。

「国家安全保障戦略」では、情報について、具体的には、

① 多様な情報源に関する情報収集能力を大幅に強化する、特に、人的情報についてはその収集のための体制の充実・強化を図る。

② 政策部門と情報部門の連携を強化し、情報部門についてはオール・ソース・アナリシスにより政策部門への高付加価値の分析結果の提供を行えるよう、情報分析能力を強化する。

③ 情報保全のための体制の更なる強化を図る。

④ 認知領域における情報戦への対応能力を強化するとともに、戦略的コミュニケーションを積極的に実施する。

ことなどが挙げられた。

今後、内閣官房を中心に情報力強化へ向けての取り組みが具体化されると思うが、その際に留意すべき視点を何点か指摘したい。

1　前提となる国民理解の重要性　：　国家の「生き様」の反映としての情報力の在り方

今日の世界各国の情報機能の在り方は、それぞれの国が置かれた戦略環境の下で、国家の生存を賭けての営みの歴史を通じて生み出されたものであり、まさに各国の「生き様」を反映したとも言うべきものである。

米国は、伝統的には孤立主義の傾向が強く、情報は必ずしも重視されてこなかったが、真珠湾攻撃など第二次世界大戦の教訓を踏まえ、また戦後の東西対立への対応の必要から、1947年には情報の分析及び対外秘密工作を担うCIAを設立し、CIAを中心にインテリジェンス・コミュニティーが形成され、ソ連を中心とする東側諸国との熾烈な情報戦を展開した。冷戦後には活動の見直しが迫られる中、2001年の9.11同時多発テロを契機にCIAによる情報の集約の不備等が指摘され、新設された国家情報官（DNI）が情報機関を統括することとなった。

イギリスは、エリザベス1世の時代から秘密情報活動を行ってきたが、特に20世紀初頭以降、その覇権的な地位に陰りが見える中、今日の合同情報会議（JIC）、SIS（旧MI6）等につながる情報収集・分析の体制が整備された。同国では、「インテリジェンスは紳士のホビー」とも言われ、伝統的に情報業務への社会的評価は高く、情報と政策との安定的な関係が築かれてきたと言われている。

ドイツは、日本と同じ敗戦国であったが　東西対立の最前線に置かれ、ソ連、東独の脅威に対抗するために、第2次世界大戦中のドイツ国防軍の対ソ情報関係者を中心に、戦後、いわゆる「ゲーレン機関」が設置され、同機関をBNDという情報機関に発展させ、諜報活動を含む情報機能を強化してきた。

イスラエルは、建国以来、国家の生存に関わるアラブ諸国との戦いを続けており、「国家の安全保障が全てに優先する」という考えの下、情報収集、対テロ活動、暗殺を含む秘密工作を担う情報機関モサドが安全保障政策上重要な役割を担ってきた。

ソ連では、国内の反革命分子を摘発、弾圧するとともに国外の敵対勢力に対抗するために情報機関ＫＧＢが強大な権限を持ち、ソ連解体後のロシアでもＦＳＢがその任務・役割を引き継いでいる。

また、各国とも情報収集機能に加え、国外からの情報活動による自国への脅威に対処するための防諜（カウンターインテリジェンス）を重視している。アメリカの場合は、法執行機関であるFBIがその役割を担っているが、多くの国では、法執行機関とは別に、イギリスのMI5，ドイツのBfV、イスラエルのシャバクなどのカウンターインテリジェンス機関を設けている。

一方で、日本の場合、戦前の帝国陸海軍は、日露戦争までは、自国の国力・軍事力が他の列強よりも劣っているという認識もあり、日露戦争中の明石元二郎大佐の活躍（ロシアの反体制派を支援する謀略活動に従事）に代表されるように情報の収集、諜報活動などに力を入れていたが、その後は、自国の能力への過信、驕りも生まれ、組織面、人事面での作戦偏重、情報軽視が顕著となり、結果として無謀で悲惨な戦争に突入し、敗戦に至った。また、政府部内の分権的体質は根強く、各軍・省とは別の中央情報機関が置かれることはなかった。

戦後も過去の情報軽視についての反省がありながらも、国による情報活動は常に国民世論から警戒の目で見られてきた。これは、戦前の特高警察など国家機関による市民生活への監視・介入への国民の根強い不信が背景にある、現在の情報活動においても、例えば、通信傍受については、わが国では裁判所の判断に基づく司法的傍受に限定するなど、他国に比し極めて厳格な要件の下で行われている。特に、同時多発テロ以降、イスラム過激主義によるテロ等を経験した欧米諸国では治安対策のための情報活動への一定の理解が進む一方で、我が国の場合は、国民が「肌感覚」でテロの脅威は感じることが少なかったこともあり、情報活動への理解度の格差が広がっていることは否めない。

また、冷戦時の東西対立の下、米国との同盟を安全保障政策の基軸としていた日本としては、米国の対外政策に同調することに重点がおかれ、日本独自の政策が限られており、政策立案のための情報ニーズがそもそも低かったという事情もある。その間、情報部門の役割は、政策策定に寄与するというよりは、官邸にマスコミより早く情報を上げられるかどうかにあったとも言えよう。

しかしながら、冷戦構造の崩壊後、北朝鮮による核・ミサイル開発、9.11 同時多発テロ以降の国際テロの脅威の顕在化、中国の軍事力の増強及び力による一方的な現状変更の動きなどを受けて、わが国を取り巻く安全保障環境は厳しさを増し、わが国としての主体的な政策立案、それを支える情報機能の強化の必要性が高まり、縦割りの改善等の諸施策が具体化されてきたが、特に、先述した通り、第二次安倍政権における取り組みは、情報力強化に大きな前進をもたらした。

改善が図られたとは言え、ロシアのウクライナ侵攻など国際秩序を破壊する動きが顕在化し、また、デジタル技術の進歩により情報を巡る環境も劇的に変化する中、国家安全保障戦略で述べられたごとく、情報力の更なる強化が求められている。今後、人的・物的リソースの一層の充実、人的情報（ヒューミント）などの情報収集手法やカウンターインテリジェンス機能の充実などの施策を深掘りしていくためには、わが国の歴史的経緯も踏まえ、日本に求められる情報力の強化について国民へ丁寧な説明を行い、その理解を広める努力が不可欠である。

2　情報に内在する「限界」と「リスク」の認識と不断の改善努力

わが国の情報機能強化の一つのモデルとしているのは米国であり、いわゆる情報の専門

家と言われる人々は、よく「米国と比べて日本は・・・」と日本の情報軽視を嘆くことが多い。確かに、米国のインテリジェンス・コミュニティーは、膨大なリソースを獲得し、あらゆる情報機能を保有し、インテリジェンス・サイクルが整備され、カウンターインテリジェンス機能も具備している、しかし、米国の情報の歴史を見るに、それは失敗の連続とも呼ぶべきものである。さかのぼれば、1950 年の北朝鮮の侵攻、1962 年のソ連によるキューバへのミサイル配備、1979 年のイランの体制崩壊、ソ連のアフガン侵攻、最近でも 2001 年の同時多発テロなどの予測失敗、その後の 2003 年のイラク開戦における大量破壊兵器計画存在の判断の誤り、ウィキリークスや最近の機密情報流出などを含め、重大な失敗に枚挙のいとまがない。

これらの主たる原因は、将来予測を行う情報という仕事の「不可測性」に伴う「限界」にある。

その「限界」を更に増幅、悪化させる要因は、詰まるところ情報機関の分析能力の不備と、情報と政策の連携の問題にある（政策との関係については次項で論ずる）。分析において、専門家は、専門家であるがゆえに、予測を誤るともいわれる。その原因の例として指摘されるのは、

① 相手も自分と同じ思考をするであろうという思い込み（例えば、ロシアのウクライナ侵攻について、まさかプーチンがそんな不合理な判断をするはずがないと決めつけてしまう）、
② 相手に愛着を抱き過ぎ批判的な見方が困難（例えば、相手国への思想的、文化的な愛着のゆえに客観的なリスクから目を逸らせてしまう）、
③ 最初の分析官の見方を所与のものとし積み重ねる（例えば、イラクの大量破壊兵器問題で端緒となった情報源を無批判に前提としてしまう）、
④ 周りの見方に安易に同調してしまう（周囲がイラクの大量破壊兵器の存在を前提に議論しているので疑問を挟めない）などの問題である。

分析の不備は、分析官個人の資質の問題だけでなく、自由で建設的な意思疎通が行えないという組織の官僚化による弊害や、同時多発テロの際のように断片的な情報をつかみつつも、適切な形で総合化できないという、情報の共有・評価・報告のプロセスの不備によって生ずるものである。

また、情報活動においては、安全保障等の目的のための情報収集の必要性がある一方で、当然のことながら何をしても言い訳でなく、社会的妥当性・正当性とのバランスをとる必要がある。しかし、相手に手の内を知らせない、あるいは情報源を秘匿するという秘密の傘の下、第三者による検証機能が働かず、情報収集の対象、態様が拡大、肥大化し、社会的妥当性・正当性の限界を超える「リスク」をはらんでいる。例えば、ウィキリークスによって明らかにされた米国内、同盟国における幅広い監視活動の妥当性の問題や、1985 年のフランスの対外安全保障局（DGSE）による環境保護団体グリーンピース調査船の爆破事件など情

報機関の秘密工作活動における「暴走」とも呼ぶべき事案も生じてきた。

情報というものには、その不可測性に伴う分析の「限界」と秘密というベールに覆われたことによる暴走の「リスク」が内在している。しかし、失敗するから駄目だ、あるいは暴走のリスクがあるから危険だということで切り捨てるのではなく、「限界」と「リスク」を認識した上で、適切な監視機能を整備しつつ、失敗については、その原因を検証し、改善する営みを定着させることが重要である。

3　政策と情報との適切な「間合い」の確保

「国家安全保障戦略」では、政策部門と情報部門との緊密な連携の必要性が謳われている。もとより、情報の目的は、その成果を政策の立案に活用することにあり、その観点から、政策部門の情報要求を明確化し、その要求に沿った形で情報を収集、分析し、成果を政策部門にフィードバックするインテリジェンス・サイクルが重要である。わが国においては、従来、政策部門からの情報要求が明確でなく、同サイクルが整備されていないことが大きな問題とされてきたが、NSC/NSS の創設、内閣情報官による情報集約の強化などにより、問題は大幅に改善された。

しかし、問題がこれで解決したわけではなく、常に政策と情報の適切な「間合い」を取る努力を継続する必要がある。

まず、政策部門に情報へのニーズがあることが何よりの前提である。冷戦期のわが国のように、独自の政策が限られていた場合には、情報の役割は、時の指導者の「俺は早く知っていた」「俺しか知らない」といった、ある種の虚栄心を満足させるだけのものとなってしまう。情報を生かすも殺すも、政策決定に携わる人々、特に政治指導者の意識次第であることに留意する必要がある。

逆に、政策部門に主体的な政策があるとしても、政策の正当化のために、情報部門に圧力をかけ、政策に都合のいい客観性に欠けるプロダクトを求めることが大きなリスクを生む。例えば、2003 年の米国のイラク侵攻に先立ち、イラク攻撃を主張する急先鋒であった当時のチェイニー副大統領がたびたび CIA を訪問し、何等かの「圧力」を加えたのではないかと言われている。

また、特に注意すべきは、情報機関の「政治化」である。情報機関の職員も役人である。人事権者である権力者に評価されたいし、出世したいと思うのが人情であろう。しかし、情報に携わる職業人としての責任を忘れて、政策決定者におもねるために、政策決定者の好むオプションを支持する内容にプロダクトを歪曲した場合には、悲劇的な結果を生むことになりかねない。米国のイラク侵攻の理由とされたイラクの大量破壊兵器開発疑惑について、事後の検証により意図的な「歪曲」はなかったとはされたが、当時のテネット CIA 長官らにホワイトハウスへの「忖度」があった可能性は否定できない。また、昨年のロシアのウク

ライナ侵攻に際して、FSBがウクライナ軍の士気・能力、国民の抗戦意思について楽観的な情報をプーチン大統領に報告していたと言われているが、大統領の意向を考慮しての何らかの「忖度」が行われた可能性がある。

政策と情報の関係性は、両者が疎遠であることが問題である一方で、過剰な「連携」もリスクであり、情報部門がニーズを踏まえた客観的な成果をフィードバックできるよう、政策と情報との適切な「間合い」を確保する努力を続けることが必要である。

4　機能強化の中身の具体化の必要性　：　総論から具体論へ

これまで、多くの論者が、情報機能強化、中央情報組織の創設などを論じてきたが、往々にして、外交、軍事、治安のいずれのバックグラウンドがあるかにより、念頭に置くイメージが異なったまま、一括りに「情報」強化として議論されてきた嫌いがある。情報機能強化についてこれまでに一定の成果が見られる今日、そろそろ総論としての情報強化論だけでなく、情報の中身、性格に応じた具体論を問うべき時期が来たと思われる。

情報といっても、目的等に応じて様々な性格のものがある。例えば、

・国の進路を決める上で必要となる戦略的な情報
・対象国の軍事能力を的確に評価するために必要となる情報
・軍事作戦の遂行を迅速的確に行うために必要となる情報
・対象国の外交、軍事面での意図を把握するために必要となる情報
・対象国の謀略等の情報活動を阻止するため、あるいは犯罪行為を取り締まるための情報
・経済安全保障に関わる産業・技術に関わる情報

などである。

また、情報の収集分析の観点からは、①ヒューミント(HUMINT: human intelligence　人的情報)、②シギント(SIGINT：signals intelligence　通信情報)、③イミント(IMINT：imagery intelligence　画像情報)、④オシント(OSINT open-source intelligence　公開情報)などという分類がなされている。

当然のことながら、情報の目的、種類によって、収集、分析、利用の在り方も異なり、それぞれの特性に応じた強化策を講じていく必要がある。

国家安全保障戦略においても「多様な情報源に関する情報収集能力を大幅に強化する、特に、人的情報についてはその収集のための体制の充実・強化を図る」とされているが、例えば、そこでいう「人的情報」の充実・強化とは、具体的に何を目指すのかが明確でない。人的情報、いわゆるヒューミントは、相手の意図を知り得るということで極めて効果的な情報手段である。ヒューミントが有効なのは確かであるが、その強化を論じるに際しては、念頭におくヒューミントとは何かを明確にした上で、強化策を論じることが必要である。

ある論者は、「外交交渉で相手国の目的を事前に知ることができて、効果的な交渉ができた。やはりヒューミントは重要だ。」という主張をされている。ここでいうヒューミントと

は、外交官が日々の本来業務を真面目にやった結果として得られた対象国の意図に関する情報である。ヒューミントには、その他にも、海外で活動する商社・報道関係者などの民間人からの聞き取りによる情報、更には、対象国に潜入した自国の諜報員による情報や相手国の協力者・亡命者から得られる情報などがある。

一般的にイメージされるヒューミントとは、対象国に潜入した諜報員による相手国政府の意図を入手する活動であろう。その典型的な成功例は、第二次世界大戦中のソ連の諜報員であったリヒャルト・ゾルゲの活動である。ドイツのジャーナリストとして日本に滞在していたゾルゲが、在日ドイツ大使館を拠点として「日本が南方進出を決定、ソ連攻撃の意図なし」とする情報を入手し、ソ連に報告した結果、独ソ戦の渦中にあったソ連は、戦力をヨーロッパ正面に集中させ、ドイツの攻撃を凌ぐことが可能となった。ゾルゲ自身は、その後、特高警察に逮捕され処刑されたが、戦後、ソ連から「ソ連邦英雄」の称号が授与された。

一方で、ヒューミントは、誤情報、相手国の謀略である可能性も高く、情報の価値を見極める眼力、そして相手の謀略に対抗するカウンターインテリジェンス機能を持つことが必要となる。米国は、イラク侵攻の理由としてイラクによる大量破壊兵器の開発を挙げ、その具体的な根拠として、パウエル国務長官が国連安保理の発言でも引用した「移動式の生物兵器製造車」の存在を指摘した。この情報は、暗号名「カーブボール」と呼ばれた亡命イラク人技術者が提供した情報であり、根拠のないガセネタであることが後に判明したが、CIA はその情報を真に受け世界に大恥を晒すこととなった。一方、ドイツの BND は同じ情報を一次情報として入手していたが、情報に「信憑性なし」と判断し、ドイツのイラク開戦反対の論拠の一つとなったとも言われている。

ヒューミントといっても、大きな幅があり、「人的情報」で何を目指すのか、「外交官はもっと真面目に働け」というレベルから、「諜報員の養成・カウンターインテリジェンス機能の充実」、「対外諜報庁創設」というレベルまである中、何を念頭に置くのかを明確して具体論を議論することが必要である。

5　テクノロジーの進歩による劇的環境変化への対応

テクノロジーの進歩により情報を巡る環境が劇的に変化した。何よりも、コンピューターと通信手段の連接により生まれたデジタル空間の誕生は世界を一変させた。

第一に、デジタル空間により、流通するオープンソースの情報量が飛躍的に増大し、また、AI の発達・活用により膨大な情報の処理が技術的に可能となった。第二に、デジタル空間においては、情報は、瞬時に世界を駆け巡り、誰もが即座に世界に向けて情報を発信し、同時に、情報を入手することができることとなった。第三に、デジタル、AI などの最先端技術の発展は、民間が主導しており、また、従来は国家が優位にあった宇宙などのドメインでも民間の参入が進んでおり、民間部門の果たす役割が飛躍的に拡大した。

一方で、負の側面としては、デジタル空間を攪乱させるサイバー攻撃が、平時から有事に

わたり、民間企業から社会インフラ、政府機関・軍というあらゆるアクターに対する攻撃手段として常態化し、同時に、ＳＮＳ等の情報伝播の即時性、広範性を利用し、個々人そして社会全体の状況認識を混乱させる偽情報の拡散等による認知戦・情報戦の重要度が増している。

これらの変化は、各国の情報機関の在り方にも大きな変化を促している。かつては、安全保障にかかわる重要な情報の収集・分析は国家機関の仕事であった。例えば、画像情報では国が打ち上げた偵察衛星のみが高解像度の写真を撮ることが可能であり、それを長年の経験を有する分析官の「職人芸」で解析していた。しかし、今では、民間企業が高精度の画像衛星を打ち上げ、得られた画像をＡＩ等の活用により短期間で分析して成果を公表できることとなった。北朝鮮の核開発やロシアによるウクライナ侵攻の戦況分析において、今や、民間のシンクタンクが大きな役割を果たしている。

このような変化の中で、国の情報機関が効果的な活動を行うためには、情報機関自らがAI等を活用してオープンソースの情報処理能力を高めるとともに、民間の情報分析成果を的確に取り込み活用することが必要である。民間が大きな役割を果たすとは言え、その情報分析には、誰も責任を問われないという民間の特性ゆえに、玉石混交となるリスクがあり、国の機関による適切な評価、活用が求められる。

また、インターネット、SNSの普及により、瞬時に情報が世界を駆け巡る今日、これからの情報戦に求められるのは、スピードである。ロシアのウクライナ侵攻の当初、ロシアは、「大統領は国外に出た。武器を捨て、家に帰れ」という偽情報を拡散させたが、ゼレンスキー大統領は、即座に大統領府前で自撮りした映像をネットに投稿し、偽情報を否定してロシアの思惑を打ち砕いた。今や、相手の偽情報を即座に否定し、対抗する情報を発信する戦略的コミュニケーション能力が不可欠となった。

これらの劇的環境変化に対応するためには、従来の情報部門の手法の延長、改善ではなく、既成概念にとらわれない「非連続的な」改革を行うことが求められている。

６　ドグマからの脱却

日々の業務を続けていると当然の前提と思われていることが、業務を離れ距離を置いて見ると「何か変」と感じることが間々ある。情報の世界にも、当然の前提としていることに、ある意味でドグマ化している慣行や常識があるのではないか。

「秘密至上主義」のドグマ

情報機関は当然のことながら秘密保全を重視する。戦略的にも、我の手の内を知られてしまえば、相手に対抗措置をとられ、こちらが不利な立場におかれてしまう可能性がある。情報収集手段の確保という面でも、非公然な手法により入手した情報が明らかとなると、対象

国に情報源が特定され、その後の情報入手が不可能となる、あるいは情報源が人（ヒト）である場合には情報提供者の命に危険が及ぶことになる。また、自ら収集した情報でなく、他国の情報機関から提供された情報を、相手の了解を得ずにリークした場合には、情報機関同士の信頼関係が崩壊し、その後情報の提供を受けられなくなる。

例えば、1983 年のソ連による大韓航空機撃墜事件に際しては、わが国の情報部隊がソ連戦闘機のパイロットと地上との平文の交信を傍受していた。わが国としては、ソ連軍内の通信を傍受していることが明らかとなれば、その後の情報収集が不可能になるとして公表は望ましくないと考えていたが、情報を共有していた米国政府の政治的判断により国連安全保障理事会でソ連による撃墜の決定的な証拠として公表された。わが国が懸念したとおり、その後のソ連の航空機の通信は暗号化され、情報の収集に支障をきたした。しかし、総合的に見れば、情報部門のロジックにより秘密を重視するよりは、ソ連の蛮行の証拠を国際社会に突き付けたという政治的メリットが大きかったと言うべきであろう。

情報の世界の秘密優先の論理を見直すという考え方は、ロシアのウクライナ侵攻が噂される時期での米国の積極的な情報開示においても示された。世界の多くの専門家がウクライナへの軍事進攻という不合理な選択をプーチンがするはずがないと見ていた中、米国政府は、ロシア軍のウクライナ周辺への集結状況、ロシア政府内の政策決定に関する情報等を逐次開示し、軍事侵攻が切迫しているという警告を世界に発信し、ロシアを牽制するとともに、ロシアに対抗する国際社会の連携強化を図った。ある意味で自らの情報収集の手の内を晒すということは、今後の情報活動に支障を生むリスクはあったが、米国としては危機的状況を公表することにより、「情報開示による抑止」の道を探ったものと考えられる。結果的には、バイデン大統領の「軍事的なオプションは考えていない」という不用意な発言等により、抑止は成功しなかったが、今後も、紛争抑止の一つの手法として情報の積極的開示が活用されることとなろう。

また、情報関係者は、そもそも秘密が「大好き」であり、何でも秘密にしたがる傾向がある。秘密にしておけば様々なリスクを回避できるし、秘密の「塀」の中で部外の検証を受けることなく安住していられる。しかし、健全な業務遂行のためには、情報のロジックで安易に秘密にするのではなく、秘密にすることが本当に合理的な必要性に基づくものなのか、常に検証することが求められる。例えば、情報機関での人材の育成という観点からも「秘密」との関わりの在り方を検討すべきであろう。情報機関の分析能力の向上の必要性は、国家安全保障戦略でも謳われているが、真の能力向上のためには、情報の分析官に「秘密」の世界に閉じこもるのではなく、幅広い専門家との交流、研鑽など、言わば「他流試合」の経験を積ませることが必要なはずである、「秘密」という殻に閉じこもり、自己満足に陥っていないのか、人材の育成に欠けることはないかの検証、反省が必要であろう。

守るべき秘密を守るのは当然であるが、一方で情報という閉ざされた部門のロジックが、

必ずしも全体の合理性にはつながらないという現実を直視して、従来型の「秘密至上主義」のドグマを再考すべき時にある。

「外交一元化」というドグマ

情報機能強化を議論する際に必ず立ちはだかるのが外務省による「外交一元化」というドグマである。外務省は、各省関係者が海外のカウンターパートとのやり取りで入手した情報を本省に直接送る行為を「外交一元化」に反するとして容認していない。その理由は、戦前、陸軍が外務省を通さずに独伊との外交交渉を行い、三国同盟締結に至ったという反省から、「外交一元化」、すなわち、外国とのやり取りの情報は全て外務省の公電によらなければならない、各省庁が直接海外駐在の職員とやりとりを行うのは、再び国を誤らせるという理屈である。

外交交渉は外務省を通して行うべきことは当然としても、日々の情報の取り扱いは、情報の性格に応じて柔軟に対応すべきであろう。わが国において民主主義に基づく政治体制が定着した今日、海外情報のやり取りを全て外務省の公電を通さないと「国の誤らせる」というロジックは余りにも時代錯誤であり、湾岸戦争後の PKO 法案の審議の際に、当時の社会党が「自衛隊を海外に出せば再び戦前の軍隊のように暴走する」として反対したロジックを彷彿させる。

世界の情報機関にはサードパーティー・ルール(third party rule)という暗黙の約束があり、相手から提供された情報については、承諾なく情報機関以外の第三者には提供しないことが慣習化されており、これを守れない組織との間では機微にわたる情報のやり取りは行わないとされている。そのため各国の情報機関は在外公館においって、通常の外交電報とは別に独自の通信手段を保有している。一方で、わが国においては、「外交一元化」という建前の下で、外交電報以外の通信・連絡手段が否定されてきた結果、在外公館や外務省本省における電報処理の過程で情報関係者以外の者が関与することとなり、世界の常識であるサードパーティー・ルールを守れない状況が続いてきた。

本来、戦前のような誤りを繰り返さないという趣旨は、一部の行政機関が独走して国の政策を誤らせることのないよう、内閣に情報を集約して一元的な政策判断を行うべきということのはずである。それがいつの間にか「外交一元化」という名のもとに外務省の省益維持の手段に矮小化されてしまってきたと言うべきであろう。

この問題も、2010 年以降海外で邦人がテロに巻き込まれる中、第二次安倍政権の下で、2015 年に国際テロ情報を収集するための組織として CTU－J（国際テロ情報収集ユニット）が外務省内に設置され、通常の外交電報とは別に独立した通信・連絡手段を確保したといわれており、「外交一元化」というドグマを脱却する第一歩を踏み出したものとして評価されるべきであろう。CTU—J は、これまでに存在しなかったわが国の中央情報機関の嚆矢と見ることもでき、国としての情報力強化という観点からその充実を検討していくこ

とが求められる。

「情報の要（かなめ）は警察」というドグマ

わが国に、いわゆる中央情報機関が存在してこなかった中、政府における情報機能の取り仕切りを実質的にリードしてきたのは警察庁である。政府としての情報集約の要である内閣情報調査室長・内閣情報官のポストは警察庁出身者の指定席であり、内閣情報調査室は警察庁の出先とも言われてきた。これまでの警察庁関係者の政府の情報業務への貢献は高く評価されるべきであろう。一方で、安全保障環境が変化し、軍事面、外交面、技術面での情報収集・分析の重要性が高まる中、政府としての情報力強化の要の組織・ポストの在り方も見直すべきであろう。個々人の能力、識見はともかく、警察という組織は、治安を所掌する部署であり、その組織が、外交、軍事、経済を含む国全体の情報集約の責任を「組織として」実質的に担い続けることには大きな疑問を感じざるを得ない。少なくとも内閣情報官のポストを警察庁の指定席とするのではなく、適材適所で有為な人材を任用するなどの柔軟性を持たせるべきであろう。

なお、警察＝情報（防諜）機関という見方も必ずしも世界の常識ではない点も指摘したい。警察という法執行機関の情報収集は、犯罪実行者の逮捕、公判における犯罪の立証を目的とするのに対し、情報（防諜）機関の目的は、対象の活動実態の解明や対象の諜報員を利用しての情報収集にあり、必ずしも犯罪者の逮捕自体を目的とするものではない。先述した通り、アメリカを除き（アメリカでは 37 年間にわたりその職を務めたフーヴァーＦＢＩ長官の存在という特殊要因あり）、多くの国で法執行機関とは別に防諜機関を設けているのが世界の通例である。

おわりに

情報を巡る環境は劇的に変化している。オープンソースの情報の膨大化、先端技術を活用した情報処理技術の進化、SNS 等の普及による情報伝搬の即時化、偽情報を用いた認知戦の一般化、サイバー空間への攻撃の脅威の増大など、ハード面でもソフト面でも従来の情報業務の枠を超えた態勢の「抜本的な強化」が必要である。

また、「インテリジェンスは科学ではなくアートである」とも言われる。１００％確実なハードエビデンスは基本的には存在せず、最終的に評価判断を行うのは人であり、また、その成果を使うのも人である。金と物を投入し「立派な」組織を作っても、インテリジェンス・サイクルや秘密保全についての「完璧な」制度を整備しても、うまく機能する保証はない。米国、ロシアなど情報大国の数々の失敗がその限界を実証している。我が国の情報力強化の検討に当たっては、諸外国の情報機関の体制、制度を単に真似るのではなく、各国の数々の失敗に学び、わが国独自の情報機能のあり方を不断に探究していくことが求められている。