

技術流出防止など経済安全保障上の重要政策に関する提言

令和6年9月3日
自由民主党政務調査会
経済安全保障推進本部

1. はじめに

安全保障の裾野が経済領域に拡大するのに伴って、外交力・防衛力・経済力・情報力の全てに資する技術力（以下、情報を含む）の重要性が益々拡大しており、その技術力を「育てる」のみならず「守る」こと、すなわち流出防止措置を講じることは、我が国の安全保障上、極めて重要な課題となっている。

例えば、米中間の激しい貿易摩擦の背景には、AIや半導体など先端技術の覇権争いが将来の軍事的優位性に直結するという現実があり、その技術流出は深刻な課題である。また、ロシアのウクライナ侵略やガザ地区での戦闘では、民生品を使ったドローン攻撃や迂回輸出が顕在化したが、いずれも既存の国際輸出管理レジームでは十分対応できていない。加えて、国際秩序の挑戦者である権威主義国家は、戦略的に必要な技術を他国企業から窃取することに何らの躊躇も罪悪感もないのではないかと警告するを得ず、我が国として適切に対応できていない。

かかる認識の下、我が党経済安全保障推進本部（以下、経済安保本部）は、昨年、第一歩として、技術情報を含む経済安全保障情報の保全を含む提言を行い（令和5年3月28日「経済安全保障上の重要政策に関する提言」）、それに基づき先の通常国会では、重要経済安保情報の保護及び活用に関する法律が成立（以下、重要経済安保情報保護活用法）、秘匿すべき政府保有の重要経済安保情報の保全制度が整備された。

一方で、民間が保有する重要な経済安全保障情報については、今後の検討課題となったが、我が国には世界最先端の技術を保有する企業やアカデミアが多数存在し、スパイ行為やサイバー攻撃等の不正行為のみならず、企業買収や共同研究など合法的な経済行為を隠れ蓑にした行為により、それらの機関から電子データを含めた技術や情報が搾取されるリスクが増大している。

当本部では、これに基づき、技術流出の防止措置として、

- ① 「不正行為規制」（不正行為による政府保有情報や民間保有営業秘密の漏洩防止等、特定秘密保護法、重要経済安保情報保護活用法、不正競争防止法、研究セキュリティ・イ

ンテグリティ等による措置)、

- ② 「経済・研究活動適正化」(投資審査、輸出管理、特許出願非公開化、強制技術移転防止、人材流出防止等、外国為替及び外国貿易法(外為法)、経済安全保障推進法、不正競争防止法、国際ルール、補助金・政府調達厳格化等による措置)、
- ③ 「サイバー活動適正化」(次期臨時国会提出予定のサイバー防御新法やサイバー基本法、不正競争防止法、標準化・国際ルール等による措置)、
- ④ 「基盤強化」(経済インテリジェンスや入出国管理厳格化等)、

の4つの領域に加えて、有事における経済安全保障について、本年2月より有識者等を交えて累次の議論を重ねてきた。この点、国家安全保障戦略では、「幅広い分野において有事の際の持続的な対応能力を確保する。そのために、エネルギーや食料等の確保、インフラの整備、安全保障に不可欠な部品等の安定的なサプライチェーンの構築等のための官民の連携を強化する。」とされている。

本提言は、その中で改めて特に急を要する課題について政府に対応を求めるものである。

2. 基本的な考え方

(多様な主体との連携及びリスク点検)

我が国の存立及び国民の安全に著しい影響を及ぼすことが無いよう、官民双方が主体的に技術流出を未然に防ぐ措置を一刻も早く講じるべきである。そのためには、官民双方による合理的かつ戦略的な連携と、同志国・有志国の連携が必須である。加えて、そうした多様な主体との情報共有とリスク点検を徹底し、問題が顕在化する前に未然に対処できる運用体制とガバナンスを国家として構築する必要がある。

(育てることで守る)

また、技術流出防止措置については、「育てる」ことで「守る」という考え方が重要である。ある程度の技術流出はやむを得ないものと割り切った上で、流出する頃にはさらに数歩先の技術開発を実現しているような、常に先を行く「Run faster 型」、「攻めの研究開発」を我が国は目指すべきである。

(人材育成及び意識醸成)

さらに、技術流出の経路は多岐にわたるため、その対応策も複合的なものが求められている。加えて、技術窃取の手法も対応策が講じられるとそれに対抗するために随時変化していく。このため、最新の技術流出に関する国内外の動向を深く理解し、相手の先を見越して対策を講じることが必要になる。それぞれの技術分野の専門知識を有し、技術開発の

現場の状況を理解し、かつ有効な技術流出対策の知見も有する専門人材が求められている。こうしたいわゆる技術流出対策のエキスパートを官民で育てるとともに、技術流出はすぐそばで起こっていることを自覚し、状況に応じた有効な対策を取ることができるよう、個々のアウェアネスを高め、国力の骨幹たる我が国の重要技術を守るという国民意識の底上げを図っていくべきである。

3. 技術流出防止（提言）

3-1. 「ヒト」による技術流出対策

（1）研究セキュリティ・インテグリティの強化（RS/RI¹）

（課題認識）

世界各国において、地政学的な要因を背景に、研究に対する他国からの不当な影響、干渉又は悪用、研究成果や知的財産の窃取といったリスクへの認識が高まり、RS/RIに関する具体的取り組みが急速に進んでいる。科学技術力の向上と技術の優位性確保のためには、国際共同研究等の国際化・オープン化は必須であるが、日本の研究現場でRS/RIの取り組みが遅れば、同志国最先端の外国研究機関から排除される恐れがある。従って、リスクを適切に管理し、自由で安心な研究環境を整備すること、即ちRS/RIの具体的取組を早急かつ徹底的に進める必要がある。その際、研究開発を実施する省庁、捜査・公安当局、法執行機関等も含めた政府内の関係機関の連携を推進するとともに、研究者との意見交換の機会を十分に設け、理解を得て丁寧に進めるなど、研究現場との密接なコミュニケーションを重視する。

（政府、研究機関等のリスク情報調査分析機能の強化）

まずは、技術優位性を確保する必要がある重要な研究分野・技術分野を、政府、研究機関等が適切に把握する必要がある。そのため、政府内におけるリスク情報の共有、関連政策の連携を推進する。また、研究機関等において公開情報等に基づきリスク情報の調査分析機能の強化をすることは必須である。民間調査会社の積極活用、研究資金に関する共有システムの有効活用など、研究機関等がRS/RIを強化するための支援等の具体的措置を講じること。

加えて研究機関は、研究開発を実施する上で関係する省庁・機関だけでなく、捜査・公安当局、法執行機関等も含めた関係機関との積極的な連携が重要であり、国はそのための具体的支援措置を講じること。

¹ Research Security (RS)/Research Integrity (RI)

（RS/RI の積極推進及び取組支援）

政府は、国立研究開発法人や大学等の研究機関が、機関の規模や実情に応じて RS/RI の取組を主体的に推進できるよう、ガイドラインを作成すること。また、当該ガイドラインは、同志国諸機関等から信頼されるよう、取り組みが理由とともに公表される、いわゆるガバナンスコードとすること。もしくは、当該ガイドラインと整合的な形で、大学等研究機関においては大学ガバナンスコード等への実装を目指すこと。特に経済安全保障上重要な技術については、国立研究開発法人と実質的に同等な対応が可能となる基準を設けること。各研究機関における RS/RI の取組実施・体制構築にあたって、政府は必要な支援を行うための具体的措置を講じること。

（留学生・外国人研究者の適切な受け入れ審査）

科学技術力の更なる発展を図る観点から、留学生・外国人研究者等を積極的に受け入れることは重要であるが、同時に、国際的にも機微技術流出防止の重要性が高まる中、技術流出防止のより実効的な水際管理を図るべきである。政府は、在留資格認定証明書や査証の申請・許可プロセスのデジタル化や体制整備を一層進めつつ、関係省庁が連携して、留学生や外国人研究者等の受け入れを適切に審査すること。

（経済安全保障の視点を踏まえた人材育成のあり方の検討）

中長期的な科学技術力の発展の観点からは、技術流出防止とともに、経済安全保障上の重要な技術分野を特定し、その分野でどのような人材を育成していくべきなのかを検討する必要がある。また、経済安全保障上の重要技術分野において、我が国の優秀な人材を積極的に海外に派遣し最先端の研究に触れる機会を増進するとともに、海外からも多様な人材を受け入れ、その技術分野の特性に応じたバランスのとれた人材構成となるよう、戦略的に人材を育成・活用していくことが重要である。CSTI と NSS を中心に関係省庁が連携し、次期科学技術・イノベーション基本計画等において、経済安全保障の視点を踏まえた、国家としての人材育成の方向性を示していくこと。

（2）企業による営業秘密管理の強化

（課題認識）

民間が保有している技術の中にも、経済安全保障の観点から保護が必要な重要技術は多数存在する。このような重要技術は各企業において、営業秘密として適切に管理されていれば、不正競争防止法の対象となる。しかしながら、必ずしもこのような重要技術を有する全ての民間企業や大学において、高い問題意識に基づく営業秘密管理ができていない。さらに、実際には営業秘密漏洩が起きているにもかかわらず、それを検知する活動を十分に行っていない若しくはその能力がないために、自社の重要技術の漏洩に気づいていない企業も潜在的には多数あると思われる。また、漏洩を検知できてもレピュテー

ションリスクを恐れて放置するケースもある。

（我が国の経済安全保障上重要な情報の保護）

重要経済安保情報保護活用法に対する附帯決議にも示されているとおり、民間事業者等が保有している情報であって国として経済安全保障の観点から保護が必要と考えられる最先端技術情報等について、民間事業者が必要な対応を執れるよう、可及的速やかにその取り扱いについて検討を開始し、必要な措置を講じること。特に最先端技術を有するものの財政基盤が脆弱な中小企業やスタートアップはターゲットになりやすいため特段の配慮をすること。

（意識醸成と環境整備）

我が国の国際競争力の維持・発展に支障を及ぼすこととなる民間が保有する重要技術の国外流出を防ぐため、企業等が必要な対応をとるための環境整備について、政府として積極的に支援をすべきである。今回、経済安保本部で、企業に対してヒアリングを実施する中でも様々な営業秘密管理強化の取組が見られた。政府は、各企業で実施されている技術流出対策の好事例に関して、事例集として分かりやすい形でとりまとめて周知するなどして、民間における技術流出対策に関する意識醸成を官民一体となって進めること。また、そうした好事例を参考に、一般的に実施すべき取り組みをコーポレートガバナンスコードに実装する方向で検討すること。加えて経済安全保障に係る官民の戦略的人事交流や戦略対話を実施すること。

（国の研究開発プログラムにおける技術流出防止措置要件の追加）

政府機関からの委託、補助によって行われる経済安全保障上の重要技術に関する研究開発プログラムにおける交付要件に、所要の技術流出防止措置要件などを盛り込み、民間での営業秘密管理の強化を促進すること。

（3）企業による人材マネジメントの強化

（転職・退職を通じた技術流出の課題認識）

近年、最も企業を悩ましている技術流出のケースは、転職や退職等を通じた技術流出である。これまでは、企業で長年、技術開発に携わってきたベテラン技術者の定年退職後の転職等による「技術流出」リスクが多く語られてきた。しかしながら、昨今は、企業の機微技術に関わる技術者は、ベテランや若手を問わず、積極的な勧誘や引き抜きが行われており、我が国の国際競争力に直結する技術流出リスクが問題となっている。

（ベストプラクティスの横展開）

憲法で職業選択の自由が保障されている中で、企業は雇用契約や退職時の契約において、「競業避止義務」を規定するなどして機密秘密や顧客情報の漏洩を防ごうとしている。

政府は、様々な企業の取り組みや実態を調査した上で、モデルとなる労使間契約のひな型を作成するなど、人材マネジメント強化に関するベストプラクティスの横展開を図り、それを必要とする企業を後押しするべきである。

3-2. 「モノ」等による技術流出対策

(1) 安全保障貿易管理のさらなる強化

(新たな貿易管理のあり方の検討)

我が国は、ワッセナー・アレンジメント等の国際輸出管理レジームの合意を踏まえ、外為法に基づき、国際的な平和及び安全の維持の観点から、安全保障貿易管理として、製品の輸出と技術の提供を管理しており、これまで一定の役割を果たしてきた。しかし、そもそも軍事転用のおそれがある場合に技術管理を行うものであることから、昨今の先端技術輸出や迂回輸出などの課題に適切に対応できているとは言い難い。政府は、先端技術を保有する民主主義国家による責任ある技術管理の動向も踏まえ、新たな貿易管理のあり方を検討すること（将来的には外為法以外の新たな管理措置の創設も考え得る）。

(現行制度に基づく柔軟かつ迅速な対応)

我が国を取り巻く国際情勢の変化に速やかに対応するため、現行の安全保障貿易管理の限界を認識しつつも、現行制度に基づき必要な制度や運用の見直しを積極的に行うこと。国際社会に働きかけるとともに外為法の柔軟な運用に注力することで、新たな課題の出現にも柔軟かつ迅速に対応すること。

(少数国コンセンサスによる迅速な技術管理等)

国際輸出管理レジームは、参加国のコンセンサス（全会一致）により意思決定するため、仮に、我が国として管理対象とすべき技術を特定しても、参加国間の認識を揃えることが困難になっていることから、合意形成に時間を要する状況にある。このため、国際輸出管理レジームにおいて、コンセンサスに至らない場合であっても、技術的議論が成熟した製品や技術は、同志国とともに管理すべきである。特に、新興技術は、懸念や緊急性について参加国間の認識の一致には時間を要することから、我が国と同様な技術を保有する国と連携して先行して管理するべきである。そのための具体的取組を検討すること。

(民生分野に由来する技術の管理)

民生分野に由来する技術が、軍事分野に転用される懸念が高まっている。当初、民生技術であったとしても、想定と異なる軍事転用に繋がる可能性がある。技術は、製品と異なり、一度流出した場合に管理することが難しいことから、一定の性能のものを管理するだけでなく、より広範な技術を管理する必要がある。あらゆる技術を管理することは現実的ではないことから、我が国から外国への流出懸念がある重要技術を特定し、官民で連携し

て、技術管理を強化すること。その為の具体的措置を検討すること。

(迂回輸出への対応)

国際輸出管理レジームに参加していない技術保有国が台頭する中、懸念国による調達活動は巧妙化しており、第三国を経由した懸念国への迂回が想定される。政府は、国際輸出管理レジームの非参加国であっても、連携を強化するべきである。一方で、迂回輸出が原因で我が国の安全保障環境及び国際秩序が著しく劣化する事態となる場合には、一時的に輸出停止が可能となる措置を講じること。

(2) サプライチェーン・マネジメントの強化

(政府調達・補助金支援制度の再構築)

懸念国による「サプライチェーンの武器化」の動きが強まっており、我が国も経済的威圧の対象となることがしばしば発生している。重要鉱物などの安定調達に支障が出れば、我が国の産業に多大な影響が出るのみならず、国民の生活に直接支障が出る恐れがある。

資源や食料等の多くを海外からの輸入に依存する我が国にとって、このサプライチェーンの強靱化は急務であるものの、一朝一夕に実現するものでもないのもまた事実である。このため、サプライチェーンの武器化に対しては、同志国を含む国際連携で対応していく一方で、我が国としてもその「防御策」の構築を急ぐべきである。

具体的には、我が国のサプライチェーンの強靱化及び持続可能性を強化する観点から、重要物資に係る政府調達や補助金支援制度を再度、見直すこと。すなわち、これまでのように調達時点での価格のみで判断するのではなく、価格以外の「強靱化」や「持続可能性」といった要素も考慮すること。

3-3. 「カネ」による技術流出対策等

(1) 対内投資審査の強化

(技術流出懸念及び課題)

外国投資家による日本企業への投資は歓迎すべきである。一方で、先端技術を有する企業や、技術力はあるも経営不安に陥った企業に対する買収や出資によって、我が国の経済安全保障上の重要な技術流出が懸念されている。

外国投資家による企業への影響力行使を通じた技術流出懸念に対しては、主に外為法に基づく投資審査制度により対応してきた。財務省及び事業所管省庁は、関係省庁とも連携しつつモニタリング等の強化に取り組んできたが、事前届出の審査件数が膨大になっている現状においては、事前届出審査への対応が中心とならざるを得ず、将来的には、投資実行後の誓約や基準の遵守に係るモニタリング対応に支障を来す可能性がある。

（制度及び運用の改善）

対内投資審査について、技術流出防止と投資促進のバランスに留意しつつ、国の安全等を損なうリスクが高いと典型的に認められる外国投資について、①投資家の属性、②投資先日本企業の事業の属性の両側面から、事前届出免除制度の利用制限を検討すべきである。その際、国の安全等を損なうリスクが高いとは典型的に認められない外国投資が阻害されないよう、マーケットを含む関係者の意見等も十分に勘案しながら検討を進めるべきである。早急に手当てを行う必要性に鑑み、2024年度中に、必要な政省令改正を含めて見直しを行うこと。

運用面においても、投資後のモニタリングや関係省庁間の連携によって投資審査に係る制度の実効性を担保することが重要である。引き続き、地方も含めた体制の強化に加え、特に典型的にリスクが高いと認められる外国投資についての厳格な事前審査の実施や免除基準の遵守状況を含めたモニタリングの強化などにより、リスクに応じたメリハリのある運用改善に取り組むべきである。

（2020年改正外為法施行後5年の見直しに向けて）

他国の動向や市場への影響も踏まえつつ、国の安全保障に支障を及ぼすおそれのある投資について適切に対応ができるよう、早急に検討を行い、速やかに制度改正を行い、審査を補強すること。特に、2020年の改正外為法では、改正法施行後5年を経過した状況において、必要があると認めるときは、必要な措置を講ずることを附則で規定している。このため、検討の方向が定まった上記免除制度利用制限については先んじて見直しを進める一方で、同附則に沿って、投資促進と投資管理強化のバランスは大前提としつつ、政府を挙げて必要な見直しの検討を進めるべきである。

（2）国が自ら実施する措置による流出防止措置

経済安全保障上の重要物資について、機微技術を有する企業や、重要な供給能力を持つ企業が、懸念国企業に買収されたり、輸出規制等の経済的威圧による経営悪化で倒産したりすることによる安定供給上のリスクに対して、安定供給確保のため、必要に応じて、国自らが措置を講じることができないか、検討を進めること。

（3）対外投資審査の不断の確認

我が国企業の対外投資による海外 M&A 等に起因して、我が国企業から重要技術が流出している可能性は否定できない。現行の外為法では、国際的な平和及び安全を損なう等のおそれに対応する観点から、武器の製造業や漁業等一定の業種に係る対外直接投資について、事前届出を求めているが、例えば、米国では、同国の安全保障にリスクをもたらす機微技術や製品の流出防止を目的として、半導体、量子、AI など、対象技術を絞った厳しい規制を導入しようとする動きがみられる。対内投資と同様、経済活動の自由とのバランス

は必要であるが、技術流出防止の観点から見たときに、現行の対策で十分かどうか、不断の確認を行うことが必要である。

3-4. 「サイバー」等による技術流出対策等

(1) サイバー・セキュリティの制度及び体制の着実な整備

サイバー攻撃による被害は年々拡大しており、サイバー空間を利用した技術流出を防止することは焦眉の急を告ぐ課題である。昨年、我が本部は、重要経済安全保障情報の保護に関する提言を行うと同時に、サイバー・セキュリティに関する提言を行った。政府は、関連法律案を確実に次期臨時国会に提出すること。また、必要な体制整備に万全を期すこと。

(2) データセキュリティの確保

近年、諸外国の一部において、自国内のデータに対するガバナンスを強化するため、個人情報や産業データ等の越境移転を規制し、自国内の保管義務等を課す「データローカライゼーション」や、懸念国（懸念国の民間企業含む）から機微な個人データや政府保有データへのアクセスの禁止・制限にかかる措置、政府等の公的機関から民間保有データへのアクセスを可能とする「ガバメントアクセス」といった規律を設ける動きがある。

グローバル化したサプライチェーンの現状に鑑み、データの国境を越えた共有・利活用を前提としたセキュリティの在り方を早急に検討する必要がある。我が国では、信頼性が確保された自由なデータ流通の促進を通じたグローバルなデジタル経済の発展に向けて、DFFT（Data Free Flow with Trust）を提唱し、G7をはじめとする国際場裡における議論を主導してきた。今後も、DFFTの提唱国として、IAP（Institutional Arrangement for Partnership）および二国間・多国間の様々な機会をとらえ、データの越境移転を前提としたデータガバナンスにおける国際協調を図りつつ、日本企業のニーズを踏まえた上で、今後のデータセキュリティに関する国際的な議論を主導すべきである。このため、産学官連携による検討の場を設け、我が国のデータセキュリティに関する推進方策の方向性を示すべきである。

また、近年、個人情報保護や知財確保の観点からのデータ保護と流通のバランスを図る議論に加え、国家安全保障の観点から、インフラの稼働データ、モビリティ関連のデータ、国家機密に関するデータが懸念国に流出・活用されてはならない、との議論も活性化している。さらに、データ処理に必要なデータセンター・スパコン等の計算能力が懸念用途に活用されないようにすべき、との議論も見られる。

我が国においても漏えいすることで国の安全等を損なうおそれがある機微なデータについては、DFFTの考え方との整合性を確保した上で、適切な保護を行うことが必要である。このため、安全保障の観点から保護すべき機微データやデジタルインフラを特定する

作業を進めるとともに、そうした機微データに対する保護措置の在り方・方策等について検討すること。

(3) IoT セキュリティ適合性評価制度の構築

IoT 製品の脆弱性を狙ったサイバー脅威が高まっている中、政府は、IoT 製品に対するサプライチェーンリスク対応も含めた IoT セキュリティ適合性評価制度の早期構築を目指している。地方自治体や民間事業者では製造者の信頼性までは判断できないことから、政府も関与した適合性評価制度を構築するとともに、政府機関や重要インフラ事業者に加えて地方自治体等の調達においても、本制度が活用されるよう、積極的に関係省庁や関係業界、地方自治体等に働きかけていくこと。

4. 技術流出防止を支える重要事項

(1) 官民戦略対話を通じた経済インテリジェンスの強化

技術の進展と共に産業構造や国際情勢が複雑さを増す中、我が国が直面するリスクを的確に把握するため、我が国全体の経済インテリジェンス能力を強化する必要がある。そのためには、有志国政府のみならず、シンクタンク、産業界、アカデミアとの連携を通じて、リスク情報の共有と分析、政策調整、共同対処などが実施できるよう、国際的な官民コミュニティの構築（経済安保戦略対話グローバルコミュニティ構想（仮称））を進めるべきである。また、経済安保専門人材の育成に本格的に取り組むとともに、官民での戦略対話に加え戦略人事交流等（リボルビングドア型）も進めること。

さらに、経済安全保障推進法に基づき整備されつつあるシンクタンクについては、本格的に独立した機関として運用を開始すること。また、そのシンクタンクや新設セキュリティ・クリアランス制度を積極的に活用し、民間が本格的にコミットした経済安全保障シンクタンク設立の取組を活性化させること。

(2) 技術優位性のある分野の特定と投資強化

主要国は、国家安全保障の観点から技術的優位性を確保するための取組を本格化させている。現在、注力すべき技術領域として AI・量子技術、半導体やバイオテクノロジーなどが設定されているが、前述のシンクタンク機能も活用しつつ、流出インパクトの大きい研究分野・技術分野、技術開発に遅れることが致命的となる研究分野・技術分野、世界経済や秩序をけん引できる研究分野・技術分野を、政府をあげて恒常的に分析して特定し、世界に先駆けて投資を行うべきである。

(3) 経済安全保障上のリスク点検の深化

経済安全保障の推進に当たっては、国際情勢の変化や技術の進展等、我が国をとりまく

状況がめまぐるしく変化していく中で、自律性の向上、優位性・不可欠性の獲得の観点から、我が国の重要な産業が直面する経済安全保障上のリスクを網羅的に、不断に点検していくことが重要である。特に、昨今相次ぐ重要インフラへのサイバー攻撃や技術流出事案の発生、懸念国による重要物資の輸出管理措置の強化などをはじめとして、経済安全保障上のリスクが日々顕在化している状況を踏まえれば、政府が従来実施してきた点検をより一層効果的・高度なものとしていく必要がある。

政府は、本年5月、リスク点検のプロセスを深化させるための新たな試みとして、関係省庁において各業界の実態も踏まえつつ分析したリスクシナリオを、重要インフラ事業者や地方公共団体等に対して提示し、シナリオ下での対応を検証する机上演習を実施した。こうした官民連携型の演習は、重要インフラ事業者や地方公共団体等のリスク認識強化・対応能力向上に繋がるのみならず、政府として対処すべき課題・教訓の洗い出しにも資するものである。今後とも、単一のシナリオや特定の地域での実施にとどまることなく、更なる演習のアップデート・横展開を検討するなど、我が国の脅威となり得るあらゆるリスク・事象を想定し、点検をさらに発展させていくこと。

(4) 地方公共団体における情報流出対策

地方公共団体は、住民への身近な行政サービス提供の担い手として、大量かつ多種多様な情報を保有している。その中でも、例えば、住民の個人情報や企業の経営情報、健康・介護・医療データ、地域のインフラ整備・維持管理に関する情報等については、それらが窃取・悪用されることで、我が国の国民生活・社会経済活動に著しい混乱をもたらしかねない。地方においても、行政のデジタル化の進展により、サイバー攻撃等の脅威がこれまで以上に高まっている現状を踏まえれば、地方公共団体における情報流出対策の徹底は急務である。

このため、まずは、地方公共団体に対する普及啓発を通じて危機意識の醸成に努めるとともに、地方公共団体の基幹業務システム標準化やガバメントクラウドへの移行、IoTセキュリティ適合性評価制度の構築等の動きも踏まえながら、地方自治体においても対応が可能な真に実効性のある対策の在り方を検討すること。

(5) 技術を有する中堅中小企業からの技術流出対策

我が国の経済・産業を支える重要な技術の中には、大企業ではなく、地方の中堅・中小企業が有しているものも多い。しかしながら、それらの中堅・中小企業の中には、資本力の制約から必ずしも社内での技術流出対策への備えが整っていない企業や経営者の意識がそこまで高まっていない企業もある。懸念国も、自国の産業競争力強化や不可欠性向上の観点から、このような機微技術を有する中堅・中小企業をターゲットに、資金提供や買収、合併・事業提携、市場・顧客提供など様々な手法を通じて、技術獲得の取り組みを進めていると言われている。

このような「合法的」な技術獲得の取り組みに対しては、不正競争防止法や外為法では対処できないことから、経営者との密接なコミュニケーションを通じて問題意識を伝えていくことが必要。このため、政府は、関係省庁や捜査機関等とも連携を取りながら、地方の中堅・中小企業の経営者に対して、丁寧な説明と問題意識の共有を進めること。

(6) 外国勢力による不正行為としての探知収集防止について

政府保有の情報について、特定秘密保護法及び重要経済安保情報保護活用法では、探知収集側の不正行為に関し、独立教唆が処罰の対象とされているものの、いわゆる探知収集罪として広く処罰する内容にはなっておらず、構成要件は「不正手段」及び「図利加害目的」とされ、正当業務行為と認められるならば不問とされている。これにつき、一定程度のスパイ行為は処罰の対象とされるが、巧妙な手段を駆使して教唆を試みる外国勢力の協力者に対処するには十分とは言い難い。そのため、スパイ防止法の制定を求める声が日に日に高くなっており、スパイ防止措置の強化に向けた検討を進めるべきである。

なお、重要経済安保情報保護活用法については、特定秘密保護法等我が国の既存の情報保全制度とシームレスに運用されるよう、必要な措置を講じるべきである。

(7) 不正競争防止法及び外為法の制度及び運用の不断の見直し等

民間保有の技術や情報の流出防止について、不正競争防止法及び外為法は主要な法的担保であり、これまでも技術の高度化と商取引の複雑化により累次の改正が行われてきたが、顕在化し立件に至った流出事件の裏側で潜在的なリスクは計り知れない。引き続き潜在リスクを低減するため不断の見直しを行うとともに、運用各当局は、運用上、十分な能力とガバナンスを構築するべきである。

(8) 経済安全保障推進法の着実な推進

既に2024年7月末時点計90件の「供給確保計画」を認定している「サプライチェーンの強靱化」に関する制度や、支援対象として計50の重要技術を選定し計5,000億円の予算を確保している「経済安全保障重要技術育成プログラム(K Program)」に加え、2024年5月に新たに制度運用が開始された経済安全保障推進法に基づく「基幹インフラ役務の安定提供確保」に関する制度及び「特許出願の非公開」制度について、着実に施行を進めるべきである。特にK Programに関しては、着実に研究開発を行いつつ、最新の技術動向や産業動向等も踏まえながら研究開発ビジョン等を必要に応じて見直し、切れ目なく強力な支援を実現すること。

(9) 重要経済安保情報保護活用法の着実な推進

内閣府中心に、重要経済安保情報保護活用法の施行に必要な体制整備に全力を尽くすこと、対象となる情報の指定に不断かつ万全を尽くすこと、付帯決議で示された項目のう

ち、特に技術管理、経済インテル等については、その趣旨を十分に理解し、実装に全力を尽くすこと、その他、各省庁は内閣府に協力すること。

(10) 行政運営上の会合における外国勢力等の不当な影響の防止について

我が国には、優れた能力を有する民間有識者が多数存在し、政府の政策立案過程においてその知見を活用することは極めて重要である。一方で、外国勢力の影響を受けた者が政府の有識者会議のメンバーとして参加し、仮に政策誘導に至れば生じる影響は計り知れない。この点、今夏に内閣府は、有識者会議を設置する際の基本的考え方をまとめたが、実効的な運用がなされるよう努めること。

5. 有事の際の持続的な対応能力確保のための経済安全保障

現行の経済安全保障推進法では、基幹インフラ役務の安定提供確保及びサプライチェーン強靱化を図るための規定が置かれているが、原則としては平時における対応が念頭に置かれている。一方で、有事に際しては平時とは前提が全く異なる。その点、国家安全保障戦略では、「幅広い分野において有事の際の持続的な対応能力を確保する。そのために、エネルギーや食料等の確保、インフラの整備、安全保障に不可欠な部品等の安定的なサプライチェーンの構築等のための官民の連携を強化する。」とされた。政府において、いかなる事態が生じて、我が国が必要な対応をとれるよう、早急に論点整理を行い、必要な措置の創設を検討すべきである。

6. おわりに

我が国では、2020年6月には自民党政務調査会に新国際秩序創造戦略本部が設立され、2021年10月に経済安全保障対策本部（現・経済安全保障推進本部）へと改組される中で、幾度も政府に提言を行い、世界に先駆けて経済安全保障の問題を議論してきた。欧州委員会がEUの経済安全保障戦略を公表した2023年6月よりも早く、2022年5月には、このような党での議論を受けて、経済安全保障推進法が制定され、今般、2024年5月には重要経済安保情報保護活用法が制定された。政府によれば、欧米諸国のみならず、ASEANの国々からも日本の経済安全保障政策に対して高い関心が寄せられているという。まさに、日本は経済安全保障という分野において、世界から注目を集めていると言っても過言ではない。

このような状況であるからこそ、政府は、日本の経済安全保障政策の理念や考え方、具体的な政策について、体系的かつ包括的に示すべきではないか。経済安保推進本部は、過去5回全ての提言において国家安全保障戦略の付随文書として経済安保戦略の策定を求めてきた。改めてその策定の必要性を下記に示す。政府は、可及的速やかに経済安保戦略

(仮称)の策定に着手するべきである。

- (ア) 個別の具体的措置論に陥りがちな経済安保政策を、技術政策・産業政策・エネルギー資源政策等の関連政策を中心とした地政学的な戦略論として再構築し、国家として戦略的・整合的に推進する必要。
- (イ) 官民双方が主体となる経済安全保障政策を、官民の戦略的対話を通じて、双方の役割を明らかにしつつ、官民で戦略的・整合的に推進する必要。
- (ウ) 我が国のみでは対処できない課題が増える中、経済安全保障政策を、有志国と連携して推進し、加えて新しい国際ルール形成と国際秩序形成に繋げていく必要。