有事を見据えた経済安全保障の確保及び骨太方針に関する提言

令和７年５月 27 日
自由民主党政務調査会
経済安全保障推進本部

Ⅰ．一層厳しさを増す安全保障環境の中での経済安全保障政策

地政学的競争の激化やパワーバランスの変化に伴い、自由で開かれた、法の支配に基づく安定的な国際秩序は、ますます、重大な挑戦にさらされており、日本は国際社会の重要な一員として重い課題を負っている。日本が、自らの安全保障を確保するために守るべき対象は、一層、経済や技術分野に広がっている。同時に、AI・量子・バイオといったゲームチェンジャーとも言われる技術の登場を背景に、熾烈さを増す大国間の技術覇権競争は更に激化しており、安全保障を確保するための手段としての経済力と技術力、そしてそれらを支えるインテリジェンス能力もさらに一層意識されるようになっている。

これまで我が本部では、経済安全保障政策の概念的な整理として、有事を必ずしも前提とせず平時から取り組むべき課題を念頭に議論を重ねてきた。今後は明示的に有事を見据えた取り組み、すなわち有事を見据えた経済安全保障上の課題を整理し、必要な政策を措置すると共に、運用対応も念頭に置くこととしたい。

まずはその前提として、改めてリスク点検能力及び経済インテリジェンス能力の拡充強化を提言する。特にリスクシナリオの高度化は深刻な課題だと認識している。例えば米国の関税措置は政府のリスクシナリオには入っていなかったはずである。当然、米中合意による融和リスクシナリオもなければ、対立による有事リスクシナリオもないはずだ。こうしたリスクシナリオを所掌外扱いにせず、当事者意識と責任感を持って、管理できる体制整備を望む。

Ⅱ．有事を見据えた持続的な対応能力の確保

１．リスク点検の更なる深化・高度化

⑴有事をも見据えたリスク管理体制の構築

経済安全保障の観点から想定すべきリスクは様々なものが考えられるが、一層厳しさを

増す安全保障環境の中では、有事をも見据えたタブーなき議論を進めていく必要がある。特に有事を念頭に置いた場合に意識しなければならないのは、我が国の脆弱性に対する外部からの意図的な攻撃である。有事においては、こうした意図的な攻撃が予想されることを前提に、平時には到底想定しえないような深刻な被害が広範囲かつ長期間にわたって、しかも、時間がたつにつれ収まるよりもむしろ苛烈化する態様で、発生する恐れがある。

政府としての対応体制の整理を着実に進めるとともに、地方公共団体や重要インフラ事業者等との合同机上演習の実施も含め、関係者間の連携強化に努めること。業界毎に求めるべき対策水準を所管省庁が責任を持って示すとともに、事業者の対策状況の把握及び予算要求を含めた必要な取組を進めること。（少なくとも現状で既に認識されている非常用発電機や衛星電話などのバックアップ設備の整備は優先して進めること）。

⑵多様なリスクシナリオに基づく点検の定式化

刻々と変化する安全保障環境を前提とすれば、自身が知らないことを知らないという「未知の未知」（Unknown Unknowns）が存在することを常に疑い、不断のリスク点検を継続する必要がある。ＮＳＳや内閣府を中心に、あらゆる情報源を最大限活用してリスクの特定・評価・分析を行い、特に重点的な議論が必要なリスクシナリオを複数選定した上で、関係省庁や事業者等に提示し、脆弱性の洗い出しや必要な対策の検討のための議論を重ねること。また、こうしたリスク点検の取組を、経済安全保障政策における PDCA サイクルとして定式化していくこと。

⑶予防と対処の両面的な検討

リスク点検を進める上では、「リスクの発生の予防」と「リスクが発生した場合の対処」という観点の両面での議論が必要である。平時における議論は「予防」に力点が置かれがちであるが、限られた予算・人員の中で、あらゆるリスクについて予防を完全にすることは困難である。したがって、リスクが発生したときに、国民生活・経済活動への被害を可能な限り低減させるため、どのように「対処」すべきかという観点も十分考慮し優先順位をつけながら、必要な準備を確実に進めること。

⑷社会全体を包含したアプローチ

リスクの点検及び特定された脆弱性の克服という一連のプロセスを真に実効的なものとするためには、政府のみならず、地方公共団体、民間事業者、ひいては国民全体を巻き込んだ社会全体での取組が不可欠である。

しかしながら、例えば、リスクの特定・評価・分析を行う段階において、行政機関・民間事業者の双方において、自ら抱えるリスクや脆弱性を組織外と共有し議論することに消極的な傾向がある。しかし、官民が異なる脅威認識の下、異なる方向性で取組を進めていては、国家全体としてのレジリエンス向上には繋がらない。

想定されるリスクや脆弱性を官民で共有するために、相互信頼に基づく率直なコミュニケーションを可能とする官民連携の枠組みを構築すること。

さらに、特定された脆弱性を克服するための取組は、地方公共団体や民間事業者、国民の理解・協力が必要なケースものがほとんどである。社会全体の理解・協力を得るため、取組の必要性の前提となる政府のリスク認識を可能な範囲で対外的に発信すること。また、地方公共団体や民間事業者、国民に求めるべき対策・アクションについても、具体的に発信していくこと。

⑸既存の基本リスクシナリオとその取組推進

既存の基本的なリスクシナリオである自然災害やサイバー攻撃については、リスクシナリオの更なる高度化と深堀は当然としても、見えてきた課題や論点から必要な取り組みを順次進めること。（現状で既に認識されている非常用発電機や衛星電話などのバックアップ設備の整備は優先して進めること）。特に、万一サイバー攻撃による大規模インフラ障害が発生した場合に、国民生活・経済活動に及ぼす影響を可能な限り低減するための対応も並行して進める必要がある。

⑹データ等を活用した分析の高度化

リスク点検の議論をより高度なものにしていくためには、データの活用が不可欠である。関係省庁、ひいては地方公共団体や事業者等がそれぞれ保有しているデータを効果的に組み合わせることで、例えば、ある地域で特定のリスクが発生した場合の被害推定や、我が国のサプライチェーンの脆弱性の調査など、総合的かつ精緻な分析が可能になる。関係省庁等が連携しながら、データを活用した分析を高度化するとともに、特に、分野横断的な分析は特定の組織が一元的に実施することが効率的かつ効果的と考えられるところ、リスク点検に係るデータ分析体制を構築していくこと。

２．経済インテリジェンスの強化

⑴経済インテリジェンスの体制・基盤の強化

経済インテリジェンスの体制・基盤の強化については、2023 年に経済安保推進本部より提言を行い、NSS、内閣情報調査室やその他の各省庁にまたがる各種の課題について、問題提起を行った。こうした課題について、一定の進展が見られることは評価できるものの、政府としては、その進捗を確実にフォローアップし、更なる経済インテリジェンスの強化を図ること。なお、当本部としては、経済インテリジェンス強化の必要性を深刻に受け止めており、今後１～２年かけて集中的に議論を重ね、政府体制強化を図っていくものとする。

⑵総合的なシンクタンク機能の構築に向けて

2021 年３月、第６期科学技術・イノベーション基本計画にて、「安全・安心に係る科学技術戦略や重点的に開発すべき重要技術等の政策提言を行う安全・安心に関する新たなシンクタンク機能の体制の構築」が記載された。足下では、CSTI が主導する安全・安心シンクタンク（重要技術戦略研究所（仮称））の設立準備が進んでいる。また、経済産業省が主導する政府における外部専門家の受け入れ（官民交流）、経済安全保障センター（仮称）の設立（独立行政法人等による取組強化）、産業界における経済インテリジェンス投資強化（Trusted Thinktank Network、グローバルフォーラム）等についても検討が進んでいる。これらの動きも踏まえ、NSS が司令塔となり、政府全体の経済インテリジェンスの強化の取組を確実に前進させることが必要である。この観点から、重要物資サプライチェーンの把握・分析など経済インテリジェンスを有する独法の一層の体制整備を進めるべきである。

その上で、経済安全保障の裾野は、ますます、拡大の一途にあり、科学技術の発展が国家及び国民の安全や国際秩序にも甚大な影響を与えるに至っていることを考えると、経済と技術の観点のみならず Diplomacy：外交、Intelligence：情報、Military：防衛、Economy：経済、Technology：技術の専門知識を集結し、総合的に経済安全保障を推進していく観点から、政府に対して経済安全保障分野全般の政策提言を行うシンクタンク機能の構築が必要になってきている。以上を踏まえ、総合的な経済安全保障シンクタンク機能の体制や予算を含めた将来像について以下のような方向を目指していくこと。

まず、経済安全保障に関する官民連携のプラットフォーム及び関連するシンクタンクネットワークの中核として経済安全保障のシンクタンク機能を担う機関を設置し、民間保有情報やオープンソースを含めた、経済インテリジェンス機能を強化すること。「官民協議会」を通じて、官民の情報共有を活性化させること。同時に、政府のインハウス分析機能を強化すること。その上で、同機関と政府内のインハウス機能を連携させ、セキュリティ・クリアランス制度も活用した上で、政府保有データの分析・調査等との連携を通じて、より機微度の高い政策提言を行うこと。さらに、政府内外で活躍できる経済安全保障

政策に関わる優秀な人材を育成・集結・循環させる仕組みを構築すること。そして、NSSが司令塔となり、政府全体のガバナンスを利かせ、経済安全保障の関連省庁と協力し、政府のニーズに即応し、効果的な政策提言を行うこと。

Ⅲ．経済安全保障上のその他の主な課題

１．経済安保推進法及び重要経済安保情報保護活用法の着実な施行と不断の見直し

⑴経済安保推進法の着実な施行と３年後見直し

経済安保推進法については、2022 年の成立・施行以降、特定重要物資の追加や、2023 年の名古屋港へのサイバー攻撃を契機とした基幹インフラ事業への一般港湾運送事業の追加等、所要の見直しを不断に講じてきたところであるが、附則第４条では、「政府は、この法律の施行後三年を目途として、この法律の施行の状況について検討を加え、必要があると認めるときは、その結果に基づいて必要な措置を講ずるものとする。」と規定されている。これを踏まえて、更なる経済安全保障の確保のために、新たな施策の追加を含め、早急に見直しの方向性を定めるべきである。

重要物資の安定供給確保については、これまで民間事業者の生産基盤強化等を強力に進めてきたところだが、例えば、国内の海底ケーブル敷設船が不足して敷設役務を過度に外部依存すれば海底ケーブル機能の安定供給が脅かされ得るといった課題に対応できていない。他にも海運・造船などで日本企業は人材不足や立地制約により、船舶建造や修繕での競争力を失いつつある。こうした課題を踏まえ、重要物資の対象拡充や物資の安定供給確保に不可欠な役務について必要な対応を実施すべきであることや国主導による GOCO（Government-Owned, Contractor-Operated）の活用による設備投資の拡充などが有効である。また、重要物資の生産能力の喪失や技術流出が懸念される中、生産者のみならず金融機関を含めて幅広い関係者から迅速かつ的確に情報収集を行い、対処することができているのか。さらに、現行の「物資」の確保に着目した枠組みでは拾いきれないような、国内向けの措置だけではない港湾・建造修繕ドックをはじめとする海外事業、特にグローバルサウス諸国との協働を通じた経済安全保障上の重要な海外事業展開は十分に実施できているか。こうした観点から十分な対応策を講じることができるよう、制度整備を行うこと。また 、国内における重要な事業に着目し、物資のみならず、それを支える物流、金融、データなどのサービスを含む産業バリューチェーン全体を捉えた自律性・不可欠性確保に必要な対応や、人材不足を補う AI・ロボット化やデータ連携を促進する施策を含む DX や GX による高付加価値化、サービス化の流れを踏まえた「新たな製造業」の創出に必要な対応を進めること。

基幹インフラ役務の安定的な提供の確保に関する制度については、医療の安定的な提供を確保するため、対象分野に医療を追加するとともに、特定社会基盤事業者として、医療DX 推進の中心的役割を果たし電子カルテ情報共有サービス等の開発・運用主体となる社会保険診療報酬支払基金や、高度な医療提供能力を有し地域で重要な役割を果たす主要な医療機関を指定すること。医療機関の指定に当たっては、事業者の規模や地域分布に加え、救急医療や災害医療の拠点としての役割を考慮し、空白地域が生じないようにすること。

経済安全保障上の重要技術について、政府全体で研究開発を更に推進するためには、関係省庁等の多様な主体が、自ら実施する研究開発を経済安全保障の観点から捉え直して推進する、いわゆる「経済安全保障トランスフォーメーション（ES-X）」の促進が重要である。このため、内閣官房・内閣府においては、後述する経済安全保障上の重要技術領域を整理したリストを作成し、技術育成に向けて多様な主体の参画を促すとともに、経済安全保障推進法における指定基金の指定についても、現行法で指定基金として指定できる基金にとどまらないその他の多様な主体も含めて、機動的な対応を可能とすること。

⑵重要経済安保情報保護活用法の着実な施行

重要経済安保情報保護活用法が、今月（2025 年５月）、施行を迎えたことは、我が国の経済安全保障のための重要な一歩である。引き続き、内閣府を中心に、同法の円滑な施行及び制度普及のための対応を進めること。適切な情報指定や情報保全など、同法の的確な運用のため、各省庁は内閣府と随時連携すること。

２．既存の取組の更なる強化と実効性確保

⑴技術流出防止対策等の重要政策の強化

技術流出防止対策等の重要政策の強化については、2024 年秋に経済安保推進本部より提言を行い、包括的な問題意識を政府に提示した。政府はこの提言を含めた過去の提言を着実にフォローアップすること。特に、機微技術を有する日本企業に対する合法的な買収行為や研究機関等へのサイバー攻撃によって技術流出が懸念される事案が新たに積みあがっていることも踏まえ、これらに対しても NSS を中心に関係省庁が連携して着実に対応していくこと。また、偽情報対策についても、情報収集分析や正確な情報の対外発信を含む対処能力を引き続き強化すべきである。個別課題の進捗と課題については、以下の通り改めて提言する。

⑵経済安全保障上の重要技術領域リストの作成と研究開発の推進

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、・バイオなどがあげられているが、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、産学官民の力を総動員して世界に先駆けて投資を行い、これらの分野における技術を育成・獲得するとともに、技術流出防止策を徹底すべきである。政府は、このような観点から経済安全保障上の重要技術領域リストを作成すること。また、経済安全保障に係る研究開発の在り方を検討する際、当該リストも参考にすること。こうした方針について、上記の推進法３年後見直しにおいて必要な対応を実施するとともに、次期科学技術・イノベーション基本計画にも反映していくこと。

⑶経済安全保障の視点を踏まえた一貫し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、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、海外から多様な優秀な人材を積極的に受け入れることが重要であるが、同時に技術流出防止対策を徹底し、より実効的な水際管理を図るべきである。こうした観点から、大学等研究機関におけるRS/RIの取組を引き続き強化するとともに、政府においても、水際管理に関する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。この際、政府全体の経済インテリジェンス強化の取組とも連携し、審査の実効性を向上させること。また、航空、金属、素材、造船といった基盤技術を担う人材不足へ対応するためにも、中核となる大学と産業界が連携し、人材育成にも取り組むべきである。さらに、我が国の国力、とりわけ、科学技術力を強化するために、上述した経済安全保障上の重要技術領域リストも参考にして、それぞれの技術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し、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、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。

⑷輸出管理の強化

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、実効性を向上するため、制度や運用の見直しを積極的に行うこと。具体的には、重要・新興技術に関する潮流も踏まえつつ、官民の対話や、地方も含めた体制の強化を通じて、企業・大学等における適切な輸出管理を徹底すること。特に、経済安全保障の観点から重要な技術分野については、アウトリーチを強化し、技術流出のリスク

を踏まえた必要な措置を実施すること。この際、国際共同開発研究を含め、同志国の企業等との連携は、優位性の確保に資するものでもあることから、企業・大学等の負担を考慮し、許可申請等の手続の合理化を図ること。

⑸対内直接投資審査制度の見直しの検討

本年４月、政府は、国の安全等を損なうリスクが高いと認められる一定の外国投資について、事前届出免除制度の対象外とするよう制度改正を行ったが、本制度は、投資後のモニタリングや関係省庁間の連携によって、その実効性を担保することが重要であり、引き続き、地方も含めた体制の強化や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、投資の実態を踏まえた運用改善に取り組むべきである。また、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ところ、投資促進と投資審査強化のバランスは大前提としつつ、これまでの施行状況も勘案の上、政府を挙げて制度の実効性の確保に向けて必要な見直しの検討を進めるべきである。

⑹研究セキュリティと研究インテグリティ（RS/RI）の強化

政府は、大学等研究機関が、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、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、政府は大学等研究機関からの相談に対応する体制を充実するなど、必要な支援を行うための具体的措置を講じること。さらに、国際共同研究のより一層の推進に向け、我が国の RS/RI の取組の発信を強化し国際的なプレゼンスを高めること。

⑺地方公共団体への対応

地方公共団体は、住民の生活を支える行政サービスや水道・医療などのインフラ役務の提供を行うとともに、自然災害をはじめとする危機対応を担う中心的な存在であることを踏まえれば、地方公共団体においても安全保障の観点から適切な対応を行うことが必要である。

例えば、地方公共団体の IT システムの開発等の適切性が、外国の法的環境等によって影響を受けることで、地方公共団体が保有する住民データが流出したり、システムの機能が停止したりする事態は、安全保障の観点からも重大な問題となる。このため、地方公共団体の IT システム等に対する懸念国からの不正な影響を排除し、地方公共団体が保有する重要なデータの防護や地方公共団体が実施する重要な業務の継続をより確実なものとするた

め、政府情報システムのためのセキュリティ評価制度であるISMAPを地方公共団体が使用するITシステムにも活用することや、法制度も含めた新たな仕組みを講じること。その際、地方公共団体における国家安全保障に対する意識を高める取組を推進するとともに、これまでのガイドライン等による地方公共団体の自主的な取組を推奨する対応ではなく、地方公共団体に安全保障に関する取組を確実に実施させるための新たな仕組みについて、総務省を中心に講じること。

併せて、地方公共団体のサイバーセキュリティに関する方針の策定、基幹業務システムの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、必要な対策を多角的に実施すること。

３．新たな課題への対応

⑴重要なデータの防護及びデータセンター等の安定的運用の確保

デジタル時代において、機微なデータの窃取などから重要なデータを保護するデータセキュリティの必要性が飛躍的に高まっている。懸念国に流出することで国家及国民の安全が損なわれる重要なデータを確実に保護するとともに、重要なデータの多くの保存・処理等に用いられ、社会経済活動を支える基盤であるデータセンターやクラウドサービスについて、経済安全保障の観点からも安定した運用を確保することが必要である。

基幹インフラの安定的な役務提供に必要なデータや特定重要物資の安定的な供給に必要となるデータは、安全保障の観点から防護が必要なデータと考えられる。基幹インフラや特定重要物資の供給網に関するデータについては、経済安全保障推進法等の既存制度の運用改善等で対応すべきである。

個人に関するゲノムデータ・医療情報・金融情報や、戸籍、地方税といった地方公共団体が保有するデータ等も懸念国に流出することにより、影響力行使等を通じて、国家安全保障上の不利益が生ずる恐れがある重要なデータと考えられる。このため、安全保障上のリスクとなり得るデータを整理した上で、懸念国へのデータ流出を防ぐ観点からデータ保有者に対する必要な対応について、法制度も含めて実施すべきである。

また、データセンターやクラウドサービスは、重要なデータを含む様々なデータの保存・処理先となっており、デジタルサービスの提供に不可欠な基盤であることから、懸念国へのデータ流出だけでなく、データセンターやクラウドサービスの機能停止による社会経済活動の混乱といったリスクに対応することが必要である。

データセンターやクラウドサービスを規律する法律がないため、政府において国内におけるこれらの事業実態を把握できておらず、問題発生時に政府として必要な対応を取ることができないのは対応すべき重要な課題である。国内における事業実態の把握は、大規模

なサイバー攻撃の発生等において、事業者との連携に基づき、安定的な役務提供を維持する上で不可欠である。このため、データセンターやクラウドサービスの機能停止や懸念国へのデータ流出を防ぐ観点から、データセンターやクラウドサービスに対する必要な対応について、法制度も含めて実施すべきである。

その際、規律の対象となるデータ及び対象者が広範に及び得ることを踏まえ、民間事業者側による自主的な取組を含め、官民が連携して対応可能かつ実効的な制度を講じるべきである。

⑵情報セキュリティサービスの対応強化

サイバー攻撃による被害は年々拡大しており、サイバー対処能力強化法及び同整備法が今般の通常国会で成立したことで、政府の対応力が強化される点は評価できる。一方、情報セキュリティサービスについては、日本国内に法制度がなく、懸念国企業を含め様々な主体が参入している実態がある。情報セキュリティサービスは、いわばサイバー空間における警備業であり、当該サービスを提供する事業者は、技術的な知見だけでなく、懸念国企業から影響を受けないかなど事業者自身の信頼性を確保することが必要である。民間事業者が外国の法的環境や外部からの指示により影響を受けることや、その環境も変わりうること等を勘案し、情報セキュリティサービスの提供主体の信頼性を確保するための取組を進めるべきである。

⑶AI・AGI

大国間競争時代において、国際連携の中で、「経済の武器化を押さえる国際経済秩序の再構築」や、「透明、強靱で持続可能なサプライチェーン構築」等を目指していくことに加え、破壊的技術革新が進む領域では、同志国・地域と共にイノベーションを加速させ続け、技術優位性を維持することが経済安全保障上も重要。特に、各国で激しい研究開発競争が進められているAI・先端コンピューティング、量子、バイオ、宇宙分野は、安全保障の観点から大きなインパクトをもたらす分野であり、「Run Faster」戦略の重点分野に位置付けられるべきである。具体的には、データセンターと電力・通信インフラの一体的な整備や、次世代半導体、コンピューティング技術等の開発、更には国内のAI開発力の強化、AI活用の促進、データ連携を含めたデータの利活用の促進、国際連携や、データセンターの利用や海外も含めた人材戦略を進めるべきである。

他方、DeepSeek等の懸念国企業が開発したAI基盤モデルについて、特に懸念国企業が直接サービス提供を行う場合は、外国の法的環境による情報窃取等のリスクがあることに十分に留意することが必要である。政府においては、懸念国企業が提供するAIを利用す

る場合のリスクについて、広く認識の共有を図るとともに、政府職員によるＢＹＯＤ端末での取扱いを見直すだけでなく、地方公共団体や基幹インフラ事業者における情報窃取リスクのある AI の利用について、必要な対応を実施すべきである。

⑷経済安全保障に関するリテラシーの向上

IoT 機器の日常生活への浸透を含め、社会全体のデジタル化が進展する中、IT の安全に関する国民のリテラシーを高める必要がある。特に、製造や供給を行う企業が置かれる法的環境等から信頼性に懸念の残る製品・サービスが、価格優位などを背景に様々な分野で広がりを見せており、こうした製品・サービスには、アップデート等を通じてバックドアを仕掛けること等が可能である点を十分に認識する必要がある。こうした企業の製品やサービスが、民間企業だけでなく、地方公共団体や教育機関で寄贈等を通じて無警戒に使用されている例が散見されており、地方公共団体や教育機関の関係者に対する経済安全保障の意識を高めることが必要となっている。このため、政府は、経済安全保障上のリスクについて、政府機関だけでなく、地方公共団体や教育機関を含む国民全体に周知・公表することにより、リテラシーを高めるとともに、既存の施策について経済安全保障の観点での対応が必要かどうか、施策の見直しを進めるべきである。これを踏まえ、立法府内や我が党でも、自ら対応するべき施策がないかどうか検討をする。

Ⅳ．経済安全保障戦略の策定及び経済安全保障政策推進のための体制強化

以上で述べた全ての経済安保政策は、同盟国・同志国等及び産官学民での密なコミュニケーションなしには実効性を確保できない。特に、諸外国に対しては、我が国の経済安保政策を、より明確かつ体系的に説明して、さらなる連携強化を求めていくとともに、産官学民においては、「経済安保政策は政府のみのものではなく各主体の自主的な取り組みがなければ完成しないものである」という共通認識を醸成する必要がある。こうした趣旨から、経済安保推進本部は、過去６回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。政府は、複雑な国際環境においてますます必要性が高まっている経済安全保障戦略（仮称）の策定に可及的速やかに着手するべきである。

加えて、経済安全保障に関する取組は、引き続き広範かつ複雑であり、また、取組が効果的に行われるためには政府全体の更なる体制強化が必要である。こうした観点から、経済安全保障分野におけるセキュリティ・クリアランス制度や経済インテリジェンス等に関する体制整備について一定の成果を見たものの、リスク点検の更なる深化・高度化、総合的な経済安全保障に関するシンクタンク機能の構築を含む経済インテリジェンスの強化を

はじめとした上記の経済安全保障上のさらなる課題への対応についても、引き続き万全を期すこと。とりわけ、上記のシンクタンク機能の構築に関しては、その実現に向けてNSSを司令塔として政府を挙げて対応し、新たな部門の創設を含めた体制の抜本的な強化を実施するとともに、関係省庁においても人員・財源の拠出を含めた全面的な協力を行うこと。

今年度は「国の行政機関の機構・定員管理に関する方針」における新たな定員合理化目標数の下における予算編成の初年度にあたるが、経済安全保障に係る政策部門及び情報部門の体制については、機械的な合理化をせず、内閣の重要政策として、各省庁の定員枠とは別に「内閣の重要課題を推進するための体制整備及び人件費予算の配分の方針」における緊急重点分野（別枠）と位置づけ、戦略的かつ計画的に整備すべきである。