経済安全保障法の制定を

2020 年 3 月 11 日

技術安全保障研究会

《目　次》

経済安全保障法の制定を

2020 年 3 月 11 日
技術安全保障研究会

1. 経済安全保障法の必要性

(1) 安全保障と経済の一体化

もとより、経済力は国家安全保障に不可欠な要素である。同時に、安全保障の確保は、国民経済繁栄の大前提でもある。このような定理とも言える安全保障と経済の関係に、新たな現実が生まれた。それは、ハード、ソフトの両面で、競争力あるデジタル技術を持っていなければ、もはや安全保障も経済成長も議論すらできない、という現実である。

このため、当研究会では、わが国としての抜本的且つ包括的な取り組みを推進すべく、経済安全保障法の制定を提言する。同法は、経済安全保障に関する様々な重要テーマについて、わが国政府としての取り組みの方向性、具体的施策、ならびにその実施時期や工程を、それぞれについて示すものであり、いわゆる「プログラム法」として、経済安全保障への取り組みを大きく加速するものである。強力な政治のリーダーシップにより、一刻も早く、経済安全保障法が制定されることを求める。

2013 年に閣議決定された国家安全保障戦略で、その理念として、「国際政治経済の主要プレーヤーとして(中略)、国際社会の平和と安定及び繁栄の確保にこれまで以上に積極的に寄与していく」としている。経済安全保障法の制定と、具体的施策の実現に向けた取り組みは、国家安全保障戦略の重要な具現化努力の一環として、位置づけられるものである。

(2) 「DX」下でのサイバーセキュリティ確保の必要性

デジタル技術の先進的な活用が、競争力に重大な影響を与えるようになった。いわゆる「デジタル・トランスフォーメーション（DX)」は、全ての産業、組織、人々の行為・行動に根本的な変化をもたらし、全く新しい社会を創り上げようとしている。通信ネットワークの高速化や AI の発達・普及によって、この世界的トレンドがますます強固になることは、今や確実な未来である。

いかに優れた防衛装備品を保持していても、サイバー攻撃や電磁波攻撃に耐え切れなければ、電力、通信など、基本インフラが一瞬にして大打撃を被り、国内が混乱状態に陥る恐れがある。情報通信ネットワークなどを介した不正アクセスを許し、機密情報が流出すれば、国の安全が脅かされてしまう。高度なジャミングやハッキングによって、宇宙空間の「眼」とも言える衛星

ネットワークの機能が失われれば、自衛隊などの活動が実質的に停止に追い込まれる。民生市場においても、付加価値の源泉として、いわゆる「connected」の技術やサービスが、従来型の業界・業種の垣根を超えて、日に日に存在感を高めている。

この中で、サイバーセキュリティの確保は、まさに国家としての極めて重要な責務となった。今こそ、関係省庁が一体となり、適宜・適切に民間の協力を得ながら、潜在的リスクの顕在化回避を含め、自由・公正・安全なサイバー空間の創出・発展に向けて、能動的取り組みを推進すべきである。同時に、これを可能とする体制整備等を早急に実現する必要がある。

(3) 「技術力」こそ国力の基盤

各国はデジタル技術、新興技術(Emerging Technology)における優位性の維持・強化に躍起である。また、米国においては、新興・基盤技術を含め、安全保障上、重要となり得る技術の輸出管理を大幅に厳格化されている。わが国においても、昨年 11 月、外為法が改正され、安全保障上、重要な企業への外国企業による出資規制が強化された。しかし、欧米諸国が、企業や大学などの協力を得ながら経済安全保障への取り組みを進めていることに照らせば、まだまだ様々な課題が残されていると言わざるを得ない。先般、米財務省は、安全保障の観点からの対米直接投資の規制や審査を免除する国(「ホワイト国」)のリストを公表した。わが国がこの対象となっていないことは、日米経済がより一層のシナジーを発揮し、自由でオープンなグローバル経済を実現していく上でも、わが国として経済安全保障を確保し、同盟国・友好国との信頼関係を強化していくことが不可欠となっていることを示している。

経済安全保障を確保するためには、わが国の科学技術・イノベーション力を抜本的に立て直し、世界をリードする力を取り戻す必要があり、より積極的に新興技術の研究開発に投資を行っていかねばならない。DX が世界的に加速する中で、新たな国際ルールや標準作りにおいて主導的役割を担うことは、わが国としても、極めて重要であり、そのためにも、技術力の強化が不可欠である。また、技術や情報のセキュリティを確保し、グローバル経済との融合を安心して推進できる環境を整備することも死活的に重要であり、これには幅広い対策が必須である。

2. 経済安全保障確保に向けた 3 原則

経済安全保障の確保なくして、グローバルで自由な経済活動を発展させていくことはできない。このため、経済安全保障の取り組みを推進するに当たっては、下記の 3 原則が極めて重要である。

(1) 経済活動の自由化と安全保障の両立

第1は、国境を超えたイン＆アウト・バウンドの経済活動の自由化と、安全保障を両立させることである。即ち、グローバル経済のメリットを真に活用するために、国際的にも受け入れられている手法・施策を用いて、安全保障上の懸念を排除するということであり、安心してパートナー国との協力関係を深めていける環境を整備するということである。

(2) 同盟国・友好国の取り組みとの整合性確保と国際協力の推進

第2は、経済安全保障への取り組みを進めるにあたっては、同盟国・友好国と整合性のある水準で、わが国企業・大学等における新興・基盤技術情報の管理を確保するとともに、技術の保護・開発・活用等に関する国際秩序構築などの面で、協力を推進することである。

特に、現時点においても、技術情報管理水準の違いから、米国のハイテク・ベンチャーや大手企業等との共同研究が円滑に進展しないという事例がある。また、米国の規準に適合していない場合には、米国を含むグローバルサプライチェーンに参画できないという恐れもある。幅広い日米産業協力を強化する観点からも、上記整合性を確保すべきである。

(3) 官民一体となった取り組み推進

第3は、経済安全保障に関し、全ての府省庁が一貫し足並みの揃った取り組みを進めることである。同時に、経済人、有識者等が主体的に貢献する仕組みを設け、政府全体として、幅広い知見・情報の積極的活用を担保することである。また、必要な場合には、企業・団体は積極的に協力すべきである。

3. 具体的施策

(1) 「経済安全保障戦略」の策定・実施

国家安全保障戦略の下、政府一体となって経済安全保障戦略を策定し実施すべきである。特に、国家安全保障局は、必要な施策の企画・立案・実施、米国などの同盟国・友好国との連携強化に中心的な役割を果たすべきであり、そのための必要な体制を整備する必要がある。

また、諸施策を効率的に実施するとともに、内外に対する透明性を確保する観点から、経済安全保障確保に向けた政策ツールと、その優先順位を同戦略に明記することが肝要である。

(2) 新興技術への積極的な投資の実施

米欧ならびに中国においては、経済と安全保障の双方に資する新興技術力の強化に向けて、政府は精力的に施策を展開している[1]。わが国において

[1] 米国防総省は、2014年、防衛技術の強化に向けて、民間のＡＩ、ビッグデータ等の新興技術を活用する方針を提示。Defense Innovation Unit(DIU)を創設し、新興技術の防衛システ

は、国民の安全・安心に向けて新興技術の開発を加速する動きはあるものの、実際の研究開発投資（官民全体）は、過去 10 年、頭打ちとなっている。技術革新が日に日に加速する中、量子コンピュータや AI 等の特許出願数でみれば、中国や米国に大きく引き離され、国際的な技術競争力の低下は否めない状況である。

このため、新興技術への研究開発投資を抜本的に拡大すべきであり、経済安全保障新興技術補助金（仮称）を創設すべきである。加えて、かかる投資の戦略性を高める観点から、政府へ適切な助言を行うシンクタンク等を設置すべきである。

(3) 安全保障環境を変化させ得る新興技術情報の適切な把握・管理

経済安全保障戦略の基盤は、安全保障環境を変化させ得る新興技術を適切に把握し、技術情報の不当な流出を未然に防止することである。このためには、まず、政府において、当該技術をリスト化し、定期・不定期に更新していくべきである。

非同盟国・非友好国などへの輸出に際しては、そのリスクを個々の技術の特性と、具体的な輸出先（含：政府、軍、インテリジェンス機関との関係性）の両面から総合的に評価し、是非を判断しなければならない。輸出先として、懸念をどうしても拭いきれない企業や、注意喚起をせざるを得ない企業などが存在する場合には、政府としてこれらを予め明示し、わが国の企業や研究者などの自発的対応を可能とすべきである。

(4) 経済安全保障の観点を踏まえた政府調達の実施

経済安全保障に関する現下の情勢に鑑み、政府調達の一般競争入札に関する方針を見直すべきである。また、府省庁ならびに政府関連機関が情報機器等の調達を実施する際には、新興技術情報の漏洩を防ぐため、同盟国の政府やインテリジェンス機関の動向を踏まえ、経済安全保障の観点を加味し、調達産品やサービスを決定すべきである。

加えて、府省庁ならびに政府関連機関と情報共有等を行う企業に対しては、一定期間内に、セキュリティ上、課題のある機器を社内システムから撤去する等の対策を実施するよう、求めるべきである。

(5) 緊急対応策の準備

わが国の安全保障、外交政策、もしくは経済が、通常では考えにくい並外れた脅威にさらされた場合には、経済安全保障に関わる措置の発動が求められる。政府は、状況を内外にしっかりと説明した上で、国内の外国組織・個

ムなどへの活用を進めている。欧州も、欧州防衛庁(EDA)が、デュアルユース技術への投資を拡大するとともに、欧州投資銀行（EIB）は EDA との連携の下、デュアルユース技術、サイバーセキュリティ技術等への積極的な投資を行うこととしている。中国も、2017 年に習近平主席を委員長とする中央軍民融合発展委員会を設置し、軍事と経済を同時に強化する施策「軍民融合」「製造 2025」などを実施している。

人の資産の凍結や輸出規制などにより、その脅威に的確に対処しなければならない。これら緊急時の措置をあらかじめ明確化することは、国際社会への透明性を確保することとなる。

様々な緊急事態への対応には、わが国企業の積極的・柔軟な協力が不可欠である。これを確保する観点から、政府による重要技術保護に関する投融資の仕組みを整備する必要がある。また、情報セキュリティにも配慮しつつ、平時から適切なインセンティブを提供し、合理的なかたちで、人道支援等の面で民間企業の協力を得る工夫が求められる。例えば、米国政府においては、緊急時に民間航空会社の協力を得るためのインセンティブとして、平時において米系航空会社が優先的に使用されている。

(6) サイバーセキュリティの強化

サイバー攻撃を受けた時に、適時適切な政府の対応を可能とするため、サイバー攻撃を受けた企業が速やかに政府に報告し、政府が同種事例の予防策を講じる制度を導入すべきである。

またサイバー攻撃の実施者を特定するアトリビューションについては、わが国としても、これを引き続き積極的に行っていく必要がある。同時に、アトリビューションをより効果的に実施するために、制度面の検討を進めるべきである。かかる制度の導入は、サイバー攻撃に対する抑止力としても機能するものである。

(7) 対日直接投資適正化委員会(仮称)の設置

国際経済活動がますます複雑化し高度化している現状に照らせば、外国企業等による対日直接投資が安全保障上の脅威となるか否かについて、個々に審査を行い、判断する委員会を政府に設置すべきである。

同委員会は、直接投資が計画された時点、ならびに直接投資の実施後についてはその経過年数に拘らず、自らのイニシアチブで、もしくは当該外国企業等の届出に基づき、審査を開始できるものとすべきである。同委員会が、経済安全保障上、問題を有すると判断した場合には、上記の緊急対応策に基づき、政府は当該直接投資内容の修正もしくは差し止めを行えるものとすべきである。逆に、同委員会が問題なしと判断した場合には、当該外国企業等に対して、一種のセーフハーバーを与えるものとして機能させるべきである。

同委員会により、当該直接投資の修正等が求められる場合でも、手続きの完了には一定期間の猶予を設定する必要がある。その間、重要な技術情報や個人情報へのアクセスによって安全保障リスクが高まり続けないよう、重要情報へのアクセスを即時に停止できるルールを整備するとともに、これを担保する仕組みが求められる。

なお、投資協定のパートナー国に対しては、同委員会の設置等は、自由でオープンなグローバル経済を実現していくための措置であり、同盟国・友好国との足並みを揃えるためのものである旨、丁寧に説明し、理解を得

るべきである。

(8) 国家安全保障会議に対する民間評議会の設置

今日、技術革新が加速度的に進み、非連続の経済活動が展開されている。この中では経済安全保障についても、常に新たな課題が生じている。このため、経済安全保障戦略の立案・実施にあたっては、民間の知見を最大限活用することが不可欠であり、経済人、有識者による評議会を設置すべきである。

同評議会には、経団連会長、日商会頭など、民間部門のリーダーが参加し、経済安全保障に関わる諸課題につき、積極的・能動的に調査・検討し、国家安全保障会議に対して提言や報告を行うものとすべきである。専門家によるタスクフォースをタイムリーに設置し、米ホワイトハウス、国務省、国防総省の諮問機関(Defense Science Board や Defense Policy Board など)に匹敵する建設的役割を果たすものとすべきである。

(9) 経済安全保障に関する企業の意識向上に向けた情報センターの設置

わが国においては、従来、ポスト・ココム規制などの輸出管理は、実務家の問題として受け取られる傾向があったが、今や、経済安全保障は企業価値に関する善管注意義務に関わるものとなっている。経営トップは、率先して経済安全保障に取り組むべきである。

このため、経済安全保障に関する国際的情勢や企業として求められる対応等につき、広く先端・基盤的技術の安全保障リスクを啓蒙するとともに、経営者が効果的・効率的に情報を得、活用できる専門の情報センターを設置すべきである。

(10) 情報セキュリティに関する技術規格の拡充

米国は 2019 年 8 月、AI、遺伝子工学、顔認証、音声動画操作などの新興技術情報を活用する場合には、NIST SP800-171 という技術規格からなる情報システムでの管理を義務付けた。この技術規格は、広く民間における調達行動にも影響を及ぼし、いわば国際ビジネスのデファクト・スタンダードになると見込まれている。NIST SP800-171 同等の技術規格のわが国政府調達に関する導入は、現時点で防衛分野に止まるが、他の政府調達分野においても、同基準に合わせた技術規格の導入を急ぐべきである。

特に、SP800-171 においては、政府機関ならびに大学や企業などにおいて、一定水準以上の重要技術情報に対するアクセス権付与や共有の方法、ならびに保存のあり方等についての基準が示されている。わが国において、かかる取り扱いを確保することは、国全体の情報セキュリティ水準の向上に大きく貢献するものであり、早急な取り組みが必要である。

(11) 電子証拠保全制度の導入

IoT 製品や関連サービスを提供する企業にとっては、当該産品やサービスがセキュアであることが不可欠な価値である。このため、万が一、民事訴訟

の対象となった場合でも、意図的なバックドアの組み込みやゼロデイ情報のリークなどの疑念を払拭し、当該企業に対する信頼を強固なものとできるよう、米国の状況を参考に、わが国においても、電子証拠保全制度を導入し、企業における電子証拠の保全能力を確保すべきである。

(12)上場外国企業の財務情報に関する透明性確保

安全保障環境に影響を及ぼす可能性があると判断された企業に対し、資金調達面で支援をしてしまう事態を回避するため、日本国内の証券取引所に上場している外国企業に対し、国際会計基準に準拠した情報開示を義務付けるべきである。

(13)機関投資家に対する安全保障を踏まえた投資基準の整備

機関投資家は資金調達面で安全保障環境の悪化に肩入れしてしまうリスクを回避すべきである。よって資産運用先の選定に際し、日本政府、同盟国、友好国において安全保障の観点から懸念が示された外国企業をポートフォリオに組み入れることを禁じ、保有後にリスクが判明した場合は適切なタイミングで売却すべきである。

また、機関投資家はESG（Environment 環境、Social 社会、Governance 企業統治）のG（ガバナンス）の重要な要素として各国の安全保障政策情報の収集体制や予見可能な政策に対する能動的な準拠計画など、組織的な即応体制が整備されているかどうかを評価基準に加えるべきである。

(14)安全保障上、重要技術の非公開制度の整備

安全保障上、極めて重要な技術の特許出願を非公開とし、政府がこれを管理するとともに、当該技術を開発した企業等に対して必要な経済的利益を補填する制度を導入すべきである。かかる制度は、広く国際的に認知されたものであり、G20 で関連制度を有しないのは、わが国とメキシコのみである。同時に、政府における審査体制を整備すべきである。

なお、上記の制度については、経済活動への悪影響を懸念する向きも存在する。しかし、米国において、国防総省の研究開発プロジェクトなどから無数の企業が誕生し、今日のデジタル社会をリードし、莫大な経済的効用を世界に提供していることを考えれば、適切な運用を確保することによって、企業活動への悪影響は十分、排除し得る。

(15)安全保障上、重要な技術情報を扱う資格制度の導入

安全保障に関係する技術情報、サイバーセキュリティ情報等を扱う企業人、大学研究者等について、一種の資格制度(セキュリティ・クリアランス制度)を導入し、重要情報を扱う権利と責任を付与すべきである(罰則規定を含む)。この資格は、関連組織の求めに応じて、審査を経て対象となる個人に付与されるもので、同盟国・友好国との制度の同等性にも配慮したものとすべきである。また、扱い得る情報の重要度に応じて、いくつかの水準を設ける必要

がある。

(16) 大学・研究機関における先端技術情報管理の強化

他国の大学との共同研究、外国人教授、留学生や外国人研究者を通じた先端技術の流出により大量破壊兵器の拡散や、安全保障環境への変化を引き起こさないために、大学は研究者全てに対して、バックグラウンドチェックを厳格化し、研究情報、研究室へのアクセスを適切なものとすべきであり、出入国管理やビザ発給を、このための手段として活用すべきである。

また、研究に用いる設備や材料、それらの構造の推測に役立つ発注情報や見積情報なども、アクセス制限の対象に含めるべきである。加えて、米国同様、安全保障上、重要な研究に関しては、上記のセキュリティ・クリアランス制度の対象とすべきである。

研究プロジェクト資金の拠出元如何に拘らず、先端技術情報を適切に管理することは、大学・研究機関の社会的責務である。この適切な実施を確保すべく、上記の技術情報管理の状況の報告制度の導入を検討すべきである。

(17) インフルエンス・オペレーションへの対応力強化

健全な自由民主主義を維持するために、外国政府の悪意を持った経済活動、汚職、教育などを通じた政策への直接的、間接的な影響力の発揮を阻止するために、情報収集活動を強化することは同盟国、友好国との連携において重要性が高まっている。特に、これを実現する手段として多用され始めているディープフェイクに関する情報の報告制度についても検討すべきである。

(18) 経済安全保障人材の育成強化

経済安全保障に精通し、世界の政策コミュニティとのネットワークを有する人材を確保することは、わが国の将来の国際競争力を確保する上で不可欠である。このため、かかる人材の育成プログラムや人的ネットワーク構築に向けた場を創設すべきである。

(19) 競争政策のあり方の再検討

わが国においては、今後、数十年に亘り人口減少が避けられず、国内市場規模の頭打ちもしくは縮小が想定される。一方、経済活動のグローバル化、デジタル化の中で、様々な産業分野で、海外のグローバル企業との国際競争が、国内における市場競争と表裏一体のものとなりつつある。このような新しい状況においても、わが国企業がイノベーションを通じた国際競争を積極的に展開する能力を確保することは、経済安全保障上、不可欠である。このため、国内企業の合併・統合に関する指針などを含め、競争政策のあり方につき、経済安全保障強化の観点から根本的な検討を行うべきである。

以　上

（参考）技術安全保障研究会について

座長　玉井克哉　東京大学教授・信州大学教授

委員　油木清明　BGA Japan 代表、戦略国際問題研究所(CSIS)ｼﾆｱｱｿｼｴｲﾄ
荒井寿光　知財評論家、元通商産業審議官
岩瀬充明　元警察庁生活安全局長
國分俊史　多摩大学大学院教授・ルール形成戦略研究所所長
坂本吉弘　安全保障貿易情報センター理事長、元通商産業審議官
長瀬正人　グローバルインサイト代表取締役社長、元三菱商事
西　正典　元防衛事務次官
西山淳一　未来工学研究所研究参与、元三菱重工業
頓宮裕貴　サイバーセキュリティ有識者、元情報処理推進機構理事
森口泰孝　JAEA シニアアドバイザー、元文部科学事務次官
渡辺秀明　元防衛装備庁長官

事務局長　國分俊史　多摩大学大学院教授・ルール形成戦略研究所所長

幹事役　利光　尚　安全保障貿易情報センター参与、元三菱商事

技術安全保障研究会は、日本の技術・経済・安全保障に関する学界・官界・経済界の有識者により、２０１７年に設立され、内外の情勢分析や提言活動を行っている。

２０１８年１０月１０日　提言
「諸外国並みの技術安全保障体制の構築を
～技術保護とサイバーセキュリティが急務～」
https://crs-japan.org/publications