TOKIO MARINE

リスクマネジメント最前線

2022 | No.8

経済安全保障推進法案の概要と今後の争点

ビジネスリスク本部 兼 戦略・政治リスク研究所 主席研究員 川口 貴久
専門分野：リスクマネジメント、国際政治・安全保障
慶應義塾大学グローバルリサーチインスティテュート（KGRI） 客員所員、一橋大学 非常勤講師

2022 年 5 月 11 日、第 208 回通常国会で「経済施策を一体的に講ずることによる安全保障の確保の推進に関する法律案（経済安全保障推進法案）」が成立した。法案は「安全保障の確保に関する経済施策」として 4 つの制度を創設する。具体的には、①特定重要物資の安定的な供給の確保（いわゆる「サプライチェーンの強靭化」）、②特定社会基盤役務の安定的な提供の確保（いわゆる「基幹インフラのサイバーセキュリティ」）、③特定重要技術の開発支援、④特許出願の非公開の 4 分野である。

しかし、経済安全保障推進法案が経済安全保障の全てをカバーしている訳ではなく、経済安全保障推進法案の成立は日本の経済安全保障政策の完了ではなく始まりだ。実際、経済安全保障に関する具体的な方針・指針は別途、策定されるものであり、制度の対象となる物資や事業者は今後、政省令で指定される。

経済安全保障推進法案以外で既に法改正等で対応済の分野としては、輸出管理の厳格化、研究インテグリティ（研究倫理）、出資規制、重要施設周辺の土地法整備等があげられる。また、今後の課題としては、データ、人権、機密情報を扱う適格性審査（セキュリティ・クリアランス）などが指摘される。年末までに、安全保障・防衛政策三文書（国家安全保障戦略・防衛計画の大綱・中期防衛力整備計画）の見直しが予定され、岸田文雄首相は国家安全保障戦略に「経済安全保障」を盛り込むと明言している。

企業は「経済安全保障は今後、継続的に対応が期待される課題」という認識の下、経営やリスクマネジメント活動に経済安全保障の要素を盛り込む必要がある。

1．経済安全保障推進法案の概要

（１）法案の概要：　経済施策で安全保障を確保するための４つの制度

経済安全保障とは一般に「国家が経済的な手段を用いて政治的目標を達成すること」、「経済的手段によって安全保障を確保すること」と定義される[1]。それゆえ、経済安全保障は自国の「守り」の手段でもあれば、外国に対する影響力拡大といった「攻め」の手段としても位置付けられる。「守り」と「攻め」はそれぞれ、経済安全保障推進法案に先立って設置された政府経済安全保障推進会議や経済安全保障法制に関する有識者会議で「自律性の向上」と「優位性ひいては不可欠性の確保」と表現される。

企業にしてみれば、「守り」の経済安全保障とは少なくとも「自社やその資産・事業が諸外国による戦争行為や影響力行使の媒介とならないこと、利用されないこと」であり、「攻め」とは海外を含む市場における優位性の確保であり、ビジネスそのものだろう。

2022年5月に成立した「経済施策を一体的に講ずることによる安全保障の確保の推進に関する法律案（経済安全保障推進法案）」はその名のとおり、「安全保障の確保に関する経済施策」を束ねた法案である。

法案は安全保障を確保するための経済施策として、具体的に以下の４つの制度を創設するものだ（詳細は本紙「２．経済安全保障推進法案の４つの制度」を参照）。

■ 図表１　経済安全保障推進法案の４本柱

分類	概要
①特定重要物資の安定的な供給の確保	国民の生存や、国民生活・経済活動に甚大な影響のある物資（半導体や医薬品等）の安定供給の確保のため、「特定重要物資」を指定し、民間事業者による供給確保計画の認定や財政支援、政府による特別対策（備蓄等）を講じるもの。
②特定社会基盤役務の安定的な提供の確保	14 の特定社会基盤事業（基幹インフラ事業）の重要設備（機器のみならずソフトウェア、クラウドサービス、委託先などを含む）が外国から行われる妨害行為の手段として使用されることを防止するため、重要設備の導入・維持管理等の委託先を事前に審査をして、勧告・命令等を可能とするもの。
③特定重要技術の開発支援	先端的な重要技術（安全保障上、重要なもの）の研究開発の促進とその成果の適切な活用のため、資金支援、官民伴走支援のための協議会設置、調査研究業務の委託（シンクタンク）等を講じるもの。
④特許出願の非公開	安全保障上機微な発明（当面は軍事転用可能なシングルユースに関する発明を想定）の技術流出を防止すると同時に、発明者が特許法上の権利を維持するため、出願時の審査で出願内容を非公開化し、外国出願を制限することを可能にするもの。

出典：　経済安全保障法制準備室「経済施策を一体的に講ずることによる安全保障の確保の推進に関する法律案」（2022年2月25日）の「概要」より抜粋・加筆修正。<https://www.cas.go.jp/jp/houan/208.html>

政府資料では、前者２つ（①②）を「守り」の経済安全保障施策、後者２つ（③④）を「攻め」の経済安全保障施策と位置付けていた。しかし、後者２つについても技術流出の防止が主眼であり、総じていえば「守り」の経済安全保障とみることもできる[2]。

[1] 詳細は、川口貴久、柴田慎士「経済安全保障を考慮したガバナンス・リスクマネジメント態勢の構築」『リスクマネジメント最前線』No.2021-6（2021年8月23日）、2頁。
<https://www.tokiorisk.co.jp/publication/report/riskmanagement/pdf/pdf-riskmanagement-355.pdf>

[2] 鈴木一人「岸田政権の経済安全保障戦略：まずは「守り」のツール整備か」Nippon.com（2022年1月12日）
<https://www.nippon.com/ja/in-depth/a07901/>

（2）法案の背景： 外国からの安全を害する行為への対処

米中をはじめ各国は貿易政策、投資政策、経済制裁、サイバー活動、経済支援、財政・金融政策、エネルギー・コモディティ政策を地政学的目標達成のために利用している[3]。日本では「経済安全保障」と呼ばれるが、諸外国では「エコノミック・ステイトクラフト」「地経学（geoeconomics）」とも呼ばれる[4]。

経済安全保障推進法案も同様の課題認識で、各国が安全保障上の目的のため経済政策を利用しているとみなす。法案は「国際情勢の複雑化、社会経済構造の変化等に伴い、**安全保障を確保するためには、経済活動に関して行われる国家及び国民の安全を害する行為**を未然に防止する重要性が増大していること」（法案第 1 条、下線強調は筆者）に鑑みて、制定されたものとする。法案中の 4 つの制度の目的として、「外部から行われる行為」を未然に防ぐことが度々指摘され、文脈上、「国家および国民の安全を害する行為」は潜在的に競争関係にある外国政府を念頭においたものといえる。

サプライチェーンの意図的寸断や基幹インフラへの破壊的活動は平時に大々的に行われるとは考えにくいが、新型コロナウイルス感染症（COVID-19）流行時や台湾有事などの戦時では、こうした行為が顕在化する恐れがある。軍事的覇権を左右する先端技術の獲得・開発をめぐる競争については、サイバー攻撃や産業スパイなどの非合法手段や公開情報分析を含めて平時から行われているとみるべきだろう。

これまで政府公式資料や国会答弁をみる限り、経済安全保障推進法案は特定国を念頭に置いたものではないとされる。しかし、各国で経済安全保障、エコノミック・ステイトクラフトへの関心が高まる背景には、中長期的には、技術覇権をめぐる米中対立がある[5]。

現在、進行している米中対立は米国の前トランプ（Donald J. Trump）政権の対中政策のみに起因するものではなく、米国に対して台頭する中国という中長期的な趨勢・構造、米国側では党派を超えた対中国観・対中競争戦略等に起因するものである。米中国交正常化（1979 年）以来の米国の対中国政策がオバマ（Barack H. Obama）政権後期からトランプ政権期にかけて否定、見直されてきたことにある[6]。他方、中国も建国 100 周年にあたる 2049 年（その中間目標として 2035 年）までに、国家・社会、軍事・安全保障、経済・産業などのあらゆる分野で米国を凌駕する中長期の戦略を打ち出してきた。こうした状況をふまえると、今日の米中対立の趨勢が短期的に大きく変わるとは考えにくい。

---

[3] Robert D. Blackwill & Jennifer M. Harris, “Today’s Leading Geoeconomic Instruments,” in *War by Other Means: Geoeconomics and Statecraft* (Cambridge: Harvard University Press, 2016), pp.49-92.

[4] 本稿では、「経済安全保障」と「エコノミック・ステイトクラフト」「地経学」を同じ意味で用いているが、学術的には異なるものという見方もある。

[5] 米中対立については、前掲「経済安全保障を考慮したガバナンス・リスクマネジメント態勢の構築」、川口貴久「経済安全保障 サイバーセキュリティ」『世界経済評論』（2022 年 5･6 月）、78-85 頁。

[6] 佐橋亮によれば、米中国交正常化以降の米国の対中政策の基調は支援と関与（engagement）政策であった。その背景には米中間の国力差に加えて、米国が中国に関与を続けることで、中国は①経済・市場改革を進め、②政治改革を行い、③既存の国際秩序を受け入れて国際社会で貢献を果たす、という将来に対する 3 つの期待があった。しかし、米国の対中政策の見直しは、米中間の国力差が縮小し、3 つの期待が裏切られたと認識したことに起因する。佐橋亮『米中対立：アメリカの戦略転換と分断される世界』（中央公論新社、2021 年）、162-163 頁。実際、トランプ政権の『国家安全保障戦略』（2017 年 12 月）では、関与政策の過ちを認め、「何十年もの間、米国の政策は、中国の台頭と戦後の国際秩序への統合を支援することが、中国を自由化するという信念に根ざしていた。しかし、我々の期待とは裏腹に、中国は他者の主権を犠牲にしてその力を拡大した」とする。バイデン（Joe Biden）政権の『暫定版の安全保障戦略指針』（2021 年 3 月）でも基本的には同様の認識を踏襲し、中国を「開放的な国際システムに持続的に挑戦が可能な唯一の競争相手」とみなす。

（3）法案の施行スケジュール

経済安全保障推進法案の施行日は、公布から 9 カ月以内（2023 年 2 月まで）の日で政令にて指定される。ただし、4 つの分野ごとに施行時期は微妙に異なる。また具体的な方針・指針は別途、策定されるものであり、また何が特定重要物資なのか、何が特定社会基盤事業者なのかは今後の政省令で指定される。今後の具体的スケジュールは図表 2 のとおりである。

■ 図表 2 経済安全保障推進法案の施行スケジュール

分類	施行時期		
	2022年	2023年	2024年
経済安全保障推進法案			
「基本方針」の策定	6ヵ月以内（～2022年11月）		
特定重要物資の安定的な供給の確保			
「安定供給確保基本指針」の策定	9ヵ月以内（～2023年2月）		
特定重要物資ごとの「安定供給確保取組方針」の策定	9ヵ月以内（～2023年2月）		
その他施策	9ヵ月以内（～2023年2月）		
特定社会基盤役務の安定的な提供の確保			
「特定社会基盤役務基本指針」の策定	1年以内（～2023年5月）		
特定社会基盤事業者の指定	1年6ヵ月以内（～2023年11月）		
その他施策	1年9ヵ月以内（～2024年2月）		
特定重要技術の開発支援			
「特定重要技術研究開発基本指針」の策定	9カ月以内（～2023年2月）		
その他施策	9カ月以内（～2023年2月）		
特許出願の非公開			
「特許出願非公開基本指針」の策定	1年以内（～2023年5月）		
その他施策	2年以内（～2024年5月）		

出典： 法律（案）より筆者作成。

また、年末までに、安全保障・防衛政策三文書（国家安全保障戦略・防衛計画の大綱・中期防衛力整備計画）の見直しが予定されている。岸田文雄首相は、国家安全保障戦略に「経済安全保障」を盛り込むと明言しており、安全保障戦略全体の中における経済安全保障の位置づけ、経済安全保障推進法案に限定されない経済安全保障政策が示されるものと考えられる。

2. 経済安全保障推進法案の４つの制度

経済安全保障推進法案は４分野で新たな制度を構築するものだ。それぞれの制度の概要と評価は以下のとおり。

（１）重要物資の安定的な供給の確保： サプライチェーン強靭化

制度の概要

「重要物資の安定的な供給の確保」に関する制度は、国民の生存や、国民生活・経済活動に甚大な影響のある物資の安定供給、いわゆるサプライチェーンの強靭化を目的とする。制度が念頭におくのは、「外部に過度に依存し、又は依存するおそれがある場合において、外部から行われる行為により国家及び国民の安全を損なう事態」であり、特定国への供給依存を安全保障上のリスクとみなす。

施策としては、政令で「特定重要物資」を指定し、民間事業者による「供給確保計画」の認定や財政支援を行う。供給確保のための取組みは、生産基盤の整備、供給源の多様化、特定重要物資の代替物の開発などが想定されている。特定重要物資を所管する大臣は、こうした取組みにもかかわらず、安定供給が困難であると認めた場合、備蓄をはじめとする「特別の対策」を講じることができる。または所管大臣は、事業者に対して安定供給に関する調査を要請することができる。

評価と今後の争点

多くの事業者にとっての関心は、今後、**政令で指定される「特定重要物資」の範囲**であろう。経済安全保障法制に関する有識者会議、会議が参照した米欧の戦略・政策文書などでは、半導体、医薬品・原薬、大容量電池、重要鉱物、水素、クラウドエッジコンピューティングなどが例示されている。

こうした分野に加えて、ロシアによるウクライナ全面侵攻（2022 年 2 月 24 日～）をふまえて、食糧やエネルギー・重要鉱物などの戦略物資の重要性が再確認されている。COVID-19 流行以前、多くの国際政治・安全保障の専門家はマスクが戦略物資になるとは考えていなかったように、何らかの供給危機の結果、特定重要物資が追加指定されることもありえる。実際、有識者会議の提言によれば、特定重要物資の指定については、柔軟な追加と解除ができることを基本としている[7]。特定重要物資は、現時点の想定を超えて拡大する可能性も考慮しておく必要がある。

本制度は、特定国への過度な依存度をリスクとみなす。多くの業界で対中依存度が高い状況にあり[8]、供給源を中国から多角化できるかどうかが焦点となるだろう。仮に供給源の分散が可能な場合、**供給源の分散化の対象**として、いわゆる「有志国」があげられる。「有志国」の定義・範囲は明確ではなく、流動的な側面がある。一例として、林芳正外務大臣は経済安保分野での国際ルール形成、サプライチェーン、データのフリーフロー分野での「同盟国アメリカ、同志国（like-minded countries）のヨーロッパ諸国やクアッド（日米豪印）」のハーモナイゼーション（協調・連携）を提唱する。既に半導体などについては、有志国での供給連携が模索されている。加えて、米国バイデン政権が推進する「インド太平洋経済枠組み（IPEF）」でも、サプライチェーンの弾力性と安全性を重点分野に掲げる[9]。ただし、「有志国」のメンバーは、有事における連携やパートナーシップの観点で、相当なグラデーション（バラつき）があるため、特定重要物資ごとに妥当な分散先を考慮する必要がある。

---

[7] 経済安全保障法制に関する有識者会議「経済安全保障法制に関する提言」（2022 年 2 月 1 日）、12 頁。

[8] フランス国際経済研究所（French Research Center in International Economics, Centre D'Etudes Prospectives et D'Informations Internationales: CEPII)が公開するデータでは、単純な輸出面のみみても対中依存度が高いことが分かる。
<http://www.cepii.fr/CEPII/en/welcome.asp>

[9] The White House, Indo-Pacific Strategy of the United States, February 2022, p.15.
IPEF に関する分析は、「政権が打ち出すインド太平洋経済構想、国内議論が本格化（米国）」JETRO（2022 年 2 月 9 日）。

（２）特定社会基盤役務の安定的な提供の確保： 基幹インフラのサイバーセキュリティ

制度の概要

「特定社会基盤役務の安定的な提供の確保」に関する制度は、特定社会基盤事業（基幹インフラ事業）の重要設備が外国から行われる妨害行為の手段として使用されることを防止することを目的とする。本制度については、想定するリスクを単に「外部から行われる行為」ではなく、明確に「我が国の外部から行われる特定社会基盤役務の安定的な提供を妨害する行為」とする。

具体的な施策としては、重要設備の導入・維持管理等の委託を政府が事前審査し、結果によっては政府が勧告・命令等を行うことが想定されている。

「基幹インフラ事業」とは、電気、通信、放送、郵便、金融、クレジットカード、航空、空港、鉄道、貨物自動車運送、外航貨物、ガス、石油、電力、水道の 14 分野[10]を指し、具体的な事業者は今後、指定される。

「重要設備」とは、ハードウェアの設備・機器・部品のみならず、ソフトウェア、クラウドサービス、委託先などがあげられる。

評価と今後の争点

今後の争点は、まず、本制度の対象となるのは基幹インフラ事業者の指定である。しかし、**基幹インフラ事業（者）に指定されない事業（者）についても留意**が必要である。第一に、こうした基幹インフラ事業者に製品（電子製品、通信機器）やサービスを提供する事業者は、自らの製品・サービスが事前審査の対象となりうる。第二に、基幹インフラ事業（者）に指定されないとして、自社が調達する情報機器などの安全保障リスクを考慮しなくても良いということにはならない。指定されない場合は、事業者として主体的にリスクを評価し、対応することが求められる。制度の趣旨が、外国からの破壊的行為のリスクを低減することであれば、そうした事態が顕在化する状況（東アジア有事など）でも事業継続を期待される事業者（例えば、国民保護法制にいう指定公共機関）は、仮に基幹インフラ事業者に指定されなくても、同レベルのセキュリティが社会的に期待されると考えるべきだろう。

より悩ましい課題は、**どの国・地域の製品・サービスが安全保障上のリスクが高いと評価され、事前審査で指摘されうるか**という点である。本制度は、単にサイバーセキュリティの問題というよりも、外国政府による意図的な妨害といった国家安全保障リスクの問題と考えるべきである。安全保障リスクをもたらしうる具体的な国・地域は公式には開示されていないし、今後も明示されることはないだろう。しかし、経済安全保障法制に関する有識者会議で参考にされた資料から想定国を推察することもできる。例えば、有識者会議では、米国「情報通信技術・サービス（ICTS）サプライチェーンの安全確保」に関する大統領令 13873 号が参照された[11]。政治的配慮なのか、同会議資料では具体的な国・地域は明示されていないが、大統領令 13873 号の原文では香港を含む中国、キューバ、イラン、北朝鮮、ロシア、ベネズエラが示されている[12]。

---

[10] 経済安全保障推進法案でいう「基幹インフラ」14 業種は、サイバーセキュリティ基本法および関連計画にいう「重要インフラ」14 分野とは異なるため、留意する必要がある。例えば、「郵便」は基幹インフラだが、重要インフラではない。他方、「医療」「化学」は重要インフラだが、基幹インフラではない。

[11] 経済安全保障法制に関する有識者会議 基幹インフラに関する検討会合 第 1 回資料（2022 年 12 月 10 日）。

[12] 米国「情報通信技術・サービス（ICTS）サプライチェーンの安全確保」に関する大統領令 13873 号（2019 年 5 月 15 日）および商務省暫定最終規則（2021 年 1 月 19 日）は、ICTS サプライチェーンから香港を含む中国、キューバ、イラン、北朝鮮、ロシア、ベネズエラといった「外国の敵対者（foreign adversaries）」やその投資先・管理先等が設計、開発、製造、供給した ICTS を購入・利用等の取引のうち、「過度または容認できないリスクをもたらすもの」については、米商務長官の判断で取引中止やリスク軽減措置の履行を指示することができるとする。大統領令 13873 号の対象は、重要インフラ関連企業に加えて、大量個人データ保有企業、先端技術の開発企業等に及ぶ。

（３）先端的な重要技術の開発支援

制度の概要

「先端的な重要技術の開発支援」に関する制度は、先端的な重要技術の研究開発の促進とその成果の適切な活用を目的とする。正確にいえば、制度の対象となるのは、「先端的技術」のうち、技術が不当に流出した場合等に国家安全保障（国家及び国民の安全）に損害を与えうる「特定重要技術」である[13]。

具体的な施策として、政府資金による支援、官民伴走支援のための協議会設置、「特定重要技術」を見極める調査研究業務の委託（シンクタンク）等である。「科学技術・イノベーション創出の活性化に関する法律（科技イノベ活性化法）」に資金を拠出する大臣らは、協議会を組織することができ、政府内外の必要な人員を協議会構成員に加えて、特定重要技術に関する情報収集、促進・活用方法、情報保全の在り方を検討する。

協議会の構成員（民間企業の研究者等を含む）、シンクタンク業務を委託される者は、共有される機微情報に関して守秘義務を負う。

評価と今後の争点

本制度は、経済安全保障４施策のうち、最も「攻め」の要素が強い施策である。報道によれば、研究資金は将来的に 5,000 億円規模を目指すという。

本制度の今後の争点は、**「特定重要技術」の具体的内容**である。有識者会議提言では、「支援対象となる先端的な重要技術」として「宇宙・海洋・量子・AI・バイオ等」が例示されたが[14]、現時点で具体的に指定されたものはない。

諸外国の取り組みに鑑みると、こうした技術分野の指定は広範なものに及ぶと考えられる。例えば、米国で「特定重要技術」に相当するものは、米国「輸出管理改革法（ECRA）」（2018 年 8 月）にいう「新興技術（emerging technologies）」14 分野、「基盤技術（fundamental technologies）」（分野指定なし）、「重要新興技術（critical and emerging technology: CET）に関する国家戦略」の 17 分野などで示された幅広い技術である。

「特定重要技術」は、その技術が不当に流出したり、外部に依存する場合、「国家及び国民の安全を損なう事態を生ずるおそれ」をもたらす安全保障上の重要技術である。しかし、安全保障上の重要性はいくつかの階層があると考えられる。例えば、①軍事的覇権を左右する機微技術（核、極超音速、指向性エネルギー、量子など）、②軍事転用可能な機微技術（宇宙、海洋、サイバー、ドローン、AI など）、③経済・産業力全般に関わる技術（半導体、バイオなど）といった階層が考えられ、自社の先端技術がどのような安全保障上のインパクトを持ちうるのかを評価・分析する必要がある。

---

[13] 「先端的技術」とは「将来の国民生活及び経済活動の維持にとって重要なものとなり得る先端的な技術」を指し、「特定重要技術」とは「先端的技術のうち、当該技術若しくは当該技術の研究開発に用いられる情報が外部に不当に利用された場合又は当該技術を用いた物資若しくは役務を外部に依存することで外部から行われる行為によってこれらを安定的に利用できなくなった場合において、国家及び国民の安全を損なう事態を生ずるおそれがあるもの」を指す（法案 61 条）。

[14] 経済安全保障法制に関する有識者会議「経済安全保障法制に関する提言」（2022 年 2 月 1 日）、35-36 頁。

（４）特許出願の非公開化

制度の概要

「特許出願の非公開化」に関する制度は、安全保障上機微な発明の技術流出を防止すると同時に、発明者が特許法上の権利を維持するための制度である。本制度は、前項の「先端的な重要技術の開発支援」の対象技術よりもはるかに限定したものである。法案も「国家及び国民の安全を損なう事態を生ずる**おそれが大きい**発明に係る情報の流出を防止」（下線強調は筆者）することを念頭におく。

日本の現行特許制度下では、出願から１年６カ月後、もしくは第三者からの出願公開請求に基づき、出願内容が公開特許公報に掲載され、ウェブサイトで誰でも閲覧可能な状態となる。米国や欧州を含むＧ20 の多くは、安全保障上機微な発明が諸外国に利用されないようにするため、特許出願の非公開化、秘密保持義務、外国出願制限、罰則規定などの制度が整備されているが、日本では未整備なままである。

そのため、本制度は特定の技術分野のスクリーニング（一次審査）、保全審査（二次審査）、非公開化を含む保全指定、外国出願制限などを整備するものである。

評価と今後の争点

本制度は、民間企業のイノベーション・研究開発への影響が大きいこともあり、施行時期が最も遅い。民間企業にとっての関心は、**特許出願の非公開化の審査対象となる技術分野**である。

有識者会議提言は、「具体的な対象発明のイメージ」として、核兵器開発等につながるシングルユース（軍用）技術のうち国家安全保障上、極めて機微な発明を基本としている。シングルユース技術については、発明者・関係者もその機微性を認識しているため、運用上の支障は少ないのではないかと考えられる。しかし、軍事利用可能な技術の多くは、デュアルユース（軍民両用）である。提言は、デュアルユース技術は民間のイノベーションに支障が少ないケースに限定するものとしている。具体的には、国費による委託事業の成果である技術、防衛等の用途で開発された技術、出願人自身が了解している場合などである[15]。

[15] 経済安全保障法制に関する有識者会議「経済安全保障法制に関する提言」（2022 年 2 月 1 日）、47-48 頁。

3．法案以外の経済安全保障上の課題

以上のように、経済安全保障推進法案は 4 つの分野で新たな制度を創設し、安全保障を高めようとするものだ。しかし、経済安全保障推進法案が経済安全保障の全てをカバーしている訳ではなく、経済安全保障推進法案の成立は日本の経済安全保障政策の完了ではなく始まりとみるべきだ。

経済安全保障推進法案以外で既に法改正等が講じられた分野として、輸出管理の厳格化、研究インテグリティ（研究倫理）、出資規制、重要施設周辺の土地法整備などがあげられる（図表 3）。

■ 図表 3 法案以外の経済安全保障上のテーマ（直近で法改正等があったもの）

テーマ	概要
輸出管理の厳格化	• 「みなし輸出」の見直しを通じて、軍事転用されうる機微技術の管理を厳格化する。具体的には、「居住者」（国籍問わず）に技術を提供する場合、この「居住者」が特定 3 類型（①外国との雇用関係・指揮命令、②金銭・利益の享受、③指示などの影響）に該当し、「非居住者」の強い影響下にある場合、機微技術の提供にあたっては経済産業省への届け出を必要とするもの[16]。 • 外為法第 25 条第 1 項の解釈運用変更（2022 年 5 月 1 日開始）
研究インテグリティ（研究倫理）の見直し	• 研究開発にあたっては、従来の研究インテグリティ（剽窃・改竄等の不正防止、利益相反、法令順守等）に加えて、研究の国際化・オープン化に伴う新たなリスク（外国の影響、技術流出、信頼低下等）への対応を考慮することを期待するもの[17]。 • 研究者や研究者所属機関に対して、具体的なガイドラインの公開。 • 内閣府所管「競争的研究費の適正な執行に関する指針」の改訂（2021 年 12 月 17 日公開）
対内投資規制の強化	• 外国人投資家が安全保障上重要な日本企業（2020 年 7 月時点で上場企業の約 55%が該当）の株式を取得する際に必要な届出の基準が持分比率 10%以上から 1%以上に引き下げとなった。届け出に基づき、政府は出資の審査を行い、出資後の動向（非公開技術へのアクセス等）のモニタリングを実施。 • 改正外為法（2020 年 6 月施行）

出典： 筆者作成。

また、今後重要性が高まるテーマとしては、**データ、人権、機密情報を扱う適格性審査（セキュリティ・クリアランス）**などがあげられる。データは経済安全保障推進法案で明示的に扱われない分野であり、外国政府による強制力をもった民間企業データへのアクセス（いわゆる「ガバメントアクセス」）に伴うリスクが懸念される。

人権は、事実上、国家の外交政策ツールと化している面が否定できない。欧州連合（EU）はこの分野でのルールメイキングを進め（EU サスティナビリティ・デューデリジェンス指令案）、米欧も人権起因の制裁ツールを整備する。日本では、経済産業省がサプライチェーン上の人権尊重に関するガイドラインを公開する予定だ。

セキュリティ・クリアランスは経済安全保障推進法案の審議過程で、与党内部・野党や経済団体から、その必要性が指摘されてきた。セキュリティ・クリアランス制度は基本的に国が設計・運用するものだが、制度を民間人に拡大した場合、対象者と企業の責務などが課題となるかもしれない。

---

[16] 大川信太郎（経済産業省貿易経済協力局貿易管理部安全保障貿易管理政策課兼大臣官房経済安全保障室 課長補佐）「経済安全保障と外為法に基づくみなし輸出管理の明確化について」『経団連タイムス』No.3524（2021 年 12 月 2 日）
<https://www.keidanren.or.jp/journal/times/2021/1202_06.html>

[17] 研究インテグリティの詳細は、国立研究開発法人科学技術振興機構 研究開発戦略センター『オープン化、国際化する研究におけるインテグリティ』2020 年 10 月。<https://www.jst.go.jp/crds/report/CRDS-FY2020-RR-04.html>

4．企業の対応状況

企業は「経済安全保障は今後、継続的に対応が期待される課題」という認識の下、経営やリスクマネジメント活動に経済安全保障の要素を盛り込む必要がある（詳細は脚注 1 を参照）。

既に、経済安全保障に対応している事業者では以下のような取組み例がある。

■ 図表 4 経済安全保障に関する企業の取組み例

分類		概要
組織体制	統括部門	経済安全保障は広範囲に及び、リスクマネジメントの範囲に近いため、リスクマネジメント統括部門が経済安全保障リスクの統括部門を担う。 ただし政策動向を含めた情報収集も重要となるため、リスクマネジメント統括部門と渉外・経営企画部門が密に連携。
	業務執行側の責任者	経済安全保障を統括する執行役員を設置。またはリスクマネジメントや渉外・経営企画を所掌する執行役員が明示的に経済安全保障を所掌。
	監督側	取締役のスキル・マトリックスの１つとしての考慮（「法務・規制政策」「渉外・公共政策」などのスキル中での考慮など）。
プロセス・施策	リスク評価	一般的なリスクアセスメント（特定・分析・評価）と同様に、経済安全保障の要素を考慮したリスクアセスメントを実施。経済安全保障推進法案の直接的影響、各国法制の影響、その他の影響等を考慮。
	情報収集・分析	組織内部で、経済安全保障動向を収集・分析し、経営・関係部門に定期的に発信する体制を構築・運用。
	シナリオ分析	中長期の国際関係・政策動向をシナリオプランニングの手法で分析し、自社へのリスクシナリオ（特に最悪シナリオ）を想定。
	教育・研修	全従業員／関係部門向けに経済安全保障に関する教育・研修を実施。
	個別対応	個別の経済安全保障上の課題については、統括部門と事業部門・機能部門（単一製品事業者では研究開発、生産、物流、営業を含む）、純粋コーポレート部門（人事、法務、広報、IT）が連携して対応。
ツール	公開情報調査	サプライチェーンや資本関係を可視化し、各国の制裁対象エンティティや特定国政府の支配下・影響下にある企業を抽出・分析するツールを利用。
	外部情報	経済安全保障動向、個別の法規制、政治・政策動向に関する外部情報サービスやコンサルティングを利用。

出典： 約 15 社の経済安全保障対応の取組みから作成。

[2022 年 5 月 11 日脱稿、2022 年 5 月 13 日発行]

To Be a Good Company

東京海上ディーアール株式会社

ビジネスリスク本部 兼 戦略・政治リスク研究所 主席研究員 川口 貴久（専門分野：リスクマネジメント、国際政治・安全保障）

〒100-0004 東京都千代田区大手町 1-5-1 大手町ファーストスクエア ウエストタワー23F
Tel. 03-5288-6594 Fax. 03-5288-6626 www.tokiorisk.co.jp