TOKIO MARINE

リスクマネジメント最前線

2023 | No.11

変化する経済安全保障環境と企業のリスク管理 *

ビジネスリスク本部　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

ビジネスリスク本部　研究員　　渡邉　彩恵香
　専門分野：　リスクマネジメント

要約

1. **【経済安全保障をめぐる国際環境】** 日本をはじめとする各国で経済安全保障に関する戦略・政策が策定され、二国間・多国間の枠組みでも経済安全保障協力が進展している。2023 年 5 月の G7 広島サミットでは、G7 各国は中国との「デカップリング」を求めず、内向き志向を回避した上で、経済的強靭性のための「デリスキング（de-risking、リスク低減）」と経済関係の多様化が必要だと強調した。しかし、実際には、国家安全保障に近い産業や先端技術分野での限定的な米中デカップリングがますます進行している。
2. **【進展する経済安全保障推進法の制度設計と運用】** 個別の経済安全保障上のテーマに目を向ければ、日本国内では 2022 年 5 月に成立した経済安全保障推進法の制度設計と運用が大きく進展している。具体的には、①サプライチェーン強靭化、②基幹インフラのサプライチェーン・サイバーセキュリティ、③官民技術協力、④特許出願の非公開の 4 制度の詳細が固まる。しかし、いずれの制度についても今後、対象となる物資・技術・業界等が見直し・追加される可能性があり、引き続き動向をモニタリングすることが不可欠だ。
3. **【拡大する経済安全保障上のリスクと課題】** 加えて、企業が対応すべき経済安全保障上のリスクや課題は経済安全保障推進法で明示されたものが全てではない。経済安全保障推進法審議時の衆参両院の附帯決議、政府の『国家安全保障戦略』、与党や財界の提言、G7 広島サミット等では多様なテーマや課題が指摘された。分類や特定の方法にもよるが、少なくとも 18 の経済安全保障上のテーマ（経済安全保障推進法関連の 4 分野を含む）が存在する。
4. **【企業に期待されるリスク管理】** 企業は、経済安全保障に関するリスクや課題が広範囲に渡り、かつ流動的で変化が激しいことを認識した上で、リスクマネジメント活動のサイクルをアジャイル化する必要がある。そのために、①最適な組織体制の構築、②経済安全保障動向の常時継続的モニタリングとリスク評価、③リスク対応に取り組むべきである。

＊ 本稿「１．経済安全保障をめぐる国際環境」、「３．拡大する経済安全保障上のリスクと課題」を川口、「２．進展する経済安全保障推進法の制度設計と運用」を渡邉、「４．企業に期待されるリスク管理」を川口・渡邉２名が担当した。

1．経済安全保障をめぐる国際環境

日本をはじめとする各国で経済安全保障に関する戦略・政策が策定され、二国間・多国間の枠組みでも経済安全保障協力が進展している。

日本では 2022 年 5 月に成立した経済安全保障推進法（以下、「推進法」と記載する場合がある）の制度の具体化や運用が進み【詳細は本稿２を参照】、2022 年 12 月に 10 年ぶりに改訂された『国家安全保障戦略』でも経済安全保障政策をさらに推進していくことが明言された。この『国家安全保障戦略』では、経済安全保障を「我が国の平和と安全や経済的な繁栄等の国益を経済上の措置を講じ確保すること」と幅広く定義している。実際に、経済安全保障上の政策課題は、経済安全保障推進法に限定されない広がりを持っている。

2023 年 5 月、広島市で開催された第 49 回先進国首脳会議、いわゆる「G7」では『経済的強靭性及び経済安全保障に関する G7 首脳声明』が採択される等、重要な成果を残した。具体的には、①サプライチェーン強靭化、②基幹インフラの強靭化、③非市場的政策、慣行への対応、④経済的威圧（economic coercion）への対処、⑤デジタル領域での有害な慣行への対応、⑥国際標準化における協力、⑦重要・新興技術の流出防止による国際的な平和および安全の保護といった経済安全保障上の政策課題と対応方針等が確認された。

経済安保に関する G7 首脳声明は特定国に言及したものではないが、G7 全体の成果文書『G7 広島首脳コミュニケ』地域情勢パートとあわせて読めば、経済安全保障上の政策課題の大部分は中国を念頭においたものである。G7 各国は、中国との「デカップリング」を求めず、内向き志向を回避した上で、経済的強靭性のための「デリスキング（de-risking、リスク低減）」と経済関係の多様化が必要だと強調した。翌６月、デリスキングの「発案者」たる欧州で、初の『欧州経済安全保障戦略』が公開され、G7 と同様の経済安全保障上のリスクが指摘された[1]。

日米欧等で「デリスキング」が強調される一方で、実際には、国家安全保障に近い産業や先端技術分野での限定的な米中デカップリングがますます進行している。こうした動きは「領域を狭く限定し、高い壁を構築する」という意味で、「スモールヤード、ハイフェンス（small yard, high fence）」とも呼ばれる。典型例は先端的な半導体分野だ。2022 年 10 月、バイデン政権は従来の対中半導体輸出規制を拡大し、米国人が関連中国企業に勤務すること等も制限した。2023 年 8 月の米大統領令は、「懸念国」（中国）が「軍、インテリジェンス、監視、サイバー能力に不可欠な機密技術や製品の進歩を直接的に指揮、促進、その他の方法で支援する包括的・長期的な戦略を遂行している」との認識の下、米国から中国のスーパーコンピュータ等の開発に貢献する半導体等への新規投資を制限する。これにより先端半導体分野ではモノ、ヒト、カネのデカップリングが進む。

中国もまた対抗措置を講じる。中国の重要情報インフラ事業者が米マイクロン社の製品を調達することを禁じ、半導体素材に不可欠な希少金属であるガリウムとゲルマニウムの輸出管理を強化した。ドローン関連製品の輸出制限も対抗措置の一環の可能性がある。中国は 2015 年頃から輸出規制、データ、対外制裁、国家安全関連の法律を制定・改正し、経済安全保障上のツールを整備してきたが、最近の動きはツールの実運用段階とも評価できる。

こうした「デカップリング」ないし「スモールヤード、ハイフェンス」は半導体産業を超えて拡大するリスクがある。実際、8 月の米大統領令は量子関連技術、人工知能（AI）も対象としており、バイデン政権内では再生エネルギー関連やバイオ関連の技術も囲い込むべきだとの見方がある。

この他にも各国や様々な二国間・多国間枠組みで経済安全保障に関する戦略や協力の形成が進む。多国間枠組みという点では、米 EU 貿易技術評議会（TTC）、日米豪印（QUAD）、ファイブ・アイズ等の有志国・同志国での取組みは特に注視すべき動きだろう。

[1] 正確にいえば、EU が重視する（今後、評価を行う）経済安全保障上のリスクとして、①エネルギー安全保障を含むサプライチェーンの強靭性に対するリスク、②重要インフラの物理的およびサイバーリスク、③技術に関する安全保障や技術流出に関するリスク、④経済的依存関係の武器化または経済的威圧のリスクが指摘された。

2．進展する経済安全保障推進法の制度設計と運用

個別の経済安全保障上のテーマで重要なものは経済安全保障推進法である。同法は、激化する米中対立や、新型コロナウイルス感染症（COVID-19）を発端とする供給途絶といった背景の下、2022 年 5 月 11 日に成立、同 18 日に公布された。

国家・国民の安全を経済面から確保することを目的に、この法律において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「基幹インフラのサプライチェーン・サイバーセキュリティ強化」）、③特定重要技術の開発支援（いわゆる「官民技術協力」）、④特許出願の非公開、の 4 制度が創設された。

4 制度はそれぞれ段階を分けて施行済または施行予定で、内閣府が公開する 2023 年 9 月時点での施行・運用状況を簡潔に示すと図表 1 のとおりである。民間企業への“支援”の性格が強い①「サプライチェーン強靭化」および③「官民技術協力」では、それぞれの「基本指針」が先行して閣議決定され、2022 年時点で制度の対象となる物資や技術が指定されている。一方、民間企業への“規制”色の強い②「基幹インフラのサプライチェーン・サイバーセキュリティ」および④特許出願の非公開については 2023 年春以降、運用開始に向けた具体的な制度設計や進展が認められる。ただし、いずれの制度についても、今後、対象となる物資・技術・業界が見直し・追加される可能性があり、引き続き制度の動向をモニタリングすることが肝要である。

■ 図表 1　経済安全保障推進法の施行・運用状況（2023 年 9 月時点）

	① 特定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）	② 特定社会基盤役務の安定的な提供の確保（基幹インフラのサプライチェーン・サイバーセキュリティ強化）	③ 特定重要技術の開発支援（官民技術協力）	④ 特許出願の非公開
施行	2022年8月1日	（未）	2022年8月1日	（未）
「基本指針」の閣議決定	2022年9月30日	2023年4月28日	2022年9月30日	2023年4月28日
これまでの取組み	• 2022年12月20日 「特定重要物資」の指定 • 2022年12月以降　各特定重要物資の詳細な指定要件の公表 • 2023年4月以降 「認定供給確保事業者」の認定	• 2023年8月1日 「特定社会基盤事業」の指定	• 2022年9月16日 「K Program」第1弾対象技術27分野の指定 • 2023年8月28日 「K Program」第2弾対象技術23分野の指定 • 2023年3月30日以降 「K Program」における各研究開発構想の公募開始	• 2023年8月1日 「特定技術分野」および付加要件の指定
今後の流れ	• 認定供給確保事業者による「事業実施計画」の提出 • 安定供給確保支援法人による助成金の公布	• 2023年秋頃 「特定社会基盤事業者」および施策対象となる設備の指定 • 2024年春頃　制度運用開始	• 各研究開発構想の実施 • 対象技術の追加指定	• 2023年秋頃　審査手続き等の具体化 • 2024年春頃　制度運用開始
注：施策対象となる技術や物資、業界等の範囲に対し、今後見直しや追加が行われる可能性がある。				

出典：内閣府のウェブサイトをもとに筆者作成。

以下、4 制度それぞれの進展や制度設計について概要を述べる。

①　特定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」）

本制度は、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（＝特定重要物資）のサプライチェーンの強靭化を目的とし、これに資する「供給確保計画」を提出し、所管大臣から認定を受けた事業者に対して助成金やツーステップローンを通じた支援を行うものである。2022 年 12 月 20 日には、抗菌性物質製剤、肥料、永久磁石、工作機械・産業用ロボット、航空機の部品、半導体、蓄電池、クラウドプログラム、天然ガス、重要鉱物および船舶の部品の計 11 物資が特定重要物資に指定された。その後、各特定重要物資に関する「安定供給確保を図るための取組方針」において支援対象の詳細な要件等が示され、事業者からの申請受付が随時開始された。

2023 年以降、各特定重要物資における認定供給確保計画の概要が随時公開されている。例えば、経済産業省のウェブサイトによれば、特定重要物資の 1 つである半導体では 2023 年 4 月以降で計 16 件の供給確保計画が認定されており、判明している限りでも最大助成額は半導体分野で計 1,700 億円を超える。

②特定社会基盤役務の安定的な提供の確保（「基幹インフラのサプライチェーン・サイバーセキュリティ強化」）

本制度は特定社会基盤事業者、いわゆる「基幹インフラ」事業者の役務の安定提供に対する外国からの攻撃（「特定妨害行為」）を防止するために、各事業者における特定重要設備（ソフトウェア、クラウドサービス、委託先を含む）の導入や維持管理に際し、政府による事前審査を義務付けるものである。2023 年 8 月 1 日に閣議決定された推進法の施行令を改正する政令で、電気、ガス、石油、水道、鉄道、貨物自動車運送、外航貨物、航空、空港、電気通信、放送、郵便、金融、クレジットカードの計 14 業種における基幹インフラ事業が指定された。ただし、ほぼ同時期に「港湾」「医療」業種の追加指定の検討が始まり、継続的な注視が必要である。

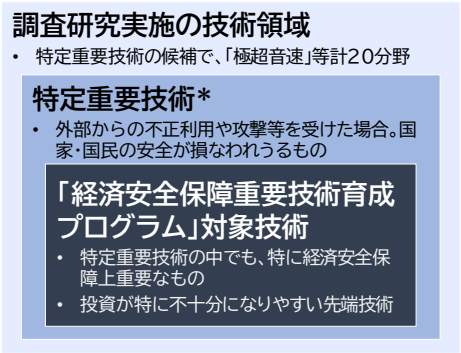
基幹インフラ「事業」の指定以降、主務省令によって各基幹インフラ「事業者」の具体的な指定基準や対象となる特定重要設備が公表され始めている（例えば、8 月 9 日には厚生労働省が「水道」事業に関する省令を公布）。審査にあたっては、対象設備の供給者が国外の主体から「強い影響」を受けているか、対象設備に関するリスク評価・対策を講じているか等の観点から「特定妨害行為」のリスクの程度が判定される。

③特定重要技術の開発支援（「官民技術協力」）

本制度は、日本の安全保障において重要な先端的技術の研究開発を促進し、その成果を適切に活用するために指定基金（総額約 5,000 億円）を通じた事業者への助成、および官民連携のための協議会の設置等を行うものである。

推進法および基本指針では右記の分類で育成すべき技術領域を定めており、2022 年 7 月に「調査研究実施の技術領域」にあたる 20 分野が「特定重要技術」の候補分野として示された。これらの分野から、2022 年 9 月の「第一次研究開発ビジョン」では 27 点、2023 年 8 月の「第二次研究開発ビジョン」では 23 点の個別具体的な技術が「経済安全保障重要技術育成プログラム（K Program）」対象技術として指定された。

■ 図表 2　技術の集合関係



＊ 推進法および「基本指針」では特定重要技術の中から K Program 対象技術が指定されるとの整理だったが、現在これら 2 つの区分はほぼ同一のものとして扱われているとみられる。
各種公開資料を基に筆者作成。

研究開発促進のための指定基金は国立研究開発法人科学技術振興機構（JST）および国立研究開発法人新エネルギー・産業技術総合開発機構（NEDO）に造成され、これら 2 機構が上記の指定を受けた各技術に関する研究開発課題の公募を順次実施している。応募内容が採択されると、原則として複数年度にわたる助成金の交付がなされ、官民での協議会設置を通じた研究開発成果の適正利用が求められることとなる。

④特許出願の非公開

本制度は、安全保障上の機微度が高い発明の特許出願を「保全指定」（ならびに指定に際した「保全審査」）の対象とし、ごく限定された技術領域において発明内容の開示を制限することで、技術流出防止を図るものである。

保全指定の対象は、①安全保障上特に機微、または大量破壊兵器の開発に利用されうる 25 の「特定技術分野」から指定されるが、25 分野の発明全体を制度対象とすると民間企業の研究開発活動を過度に制約することとなる。そこで②3 つの「付加要件」を 25 分野のうち 10 分野に適用し、当該分野の中から機微性の高い発明のみを特許非公開の対象として抽出することで、イノベーションに与える影響の低減を図ることとなっている。

3．拡大する経済安全保障上のリスクと課題

このように日本では経済安全保障推進法の施行・運用に伴い、4 つの課題への対応が進展している。しかし、企業が対応すべき経済安全保障上のリスクや課題は推進法で明示されたものが全てではない。推進法審議時の衆参両院の附帯決議、『国家安全保障戦略』、与党や財界の提言、前述の G7 広島サミットでは多様なテーマや課題が指摘された。分類や特定の方法にもよるが、少なくとも 18 の経済安全保障上のテーマ（推進法関連を含む）が存在する。

■ 図表 3　企業が注目すべき経済安全保障上のテーマ

分類	No.	経済安全保障上のテーマ	提言・成果文書等での言及（年/月）				
			G7 23/5	政府 22/12	国会 22/5	与党 23/5	財界 22/9
推進法関連	1	サプライチェーン強靭化	●	●	●	●	●
	2	基幹インフラのサプライチェーン・サイバーセキュリティ強化	●	●	●	●	●
	3	先端技術開発に関する官民協力		●	●	●	●
	4	特許出願の非公開		●	●	●	●
	5	セキュリティ・クリアランス		●	●	●	●
推進法以外	6	サプライチェーン上の人権リスク対応			●		●
	7	産業スパイ・サイバーセキュリティ対策		●		●	
	8	データをめぐる安全保障	●			●	
	9	偽情報・ディスインフォメーション対策				●	
	10	研究インテグリティの見直し	△	●			
	11	安全保障貿易管理の強化	△	●		●	
	12	重要・新興技術管理	●	●		●	
	13	国際標準化	●				
	14	投資審査の取組・体制強化	△	●		●	
	15	非市場的政策、慣行への対応	●				
	16	経済的威圧への対処	●	●			
	17	業界ごとの「リスク点検」		●			
	18	経済インテリジェンスの強化			●	●	●

各種資料を基に筆者作成。

※1 「経済安全保障上のテーマ」は相互に排他的・包括的な分類・整理ではない。ここでは、企業が対応すべき経済安全保障上の課題を洗い出すという点で、重複は許容している。また、上記のテーマは既に日本で法整備等が行われたもの、政策形成が進んでいるもの、国会・政府・財界から提言がなされているものをとりあげた（ただし、企業との関係が薄い「重要な土地取引の規制」等は除く）。

※2　セキュリティ・クリアランスについては 2024 年通常国会に改正経済安全保障推進法を提出し、制度を構築予定であるため、上記の通り表記している。

※3 「提言・成果文書等」の詳細は以下の通り。

- G7：「経済的強靭性及び経済安全保障に関する G7 首脳声明（仮訳）」（2023 年 5 月 20 日）
  ●は首脳声明の大項目・中項目のテーマ、△はそれ以外やその他関連文書で言及されたもの（ワンフレーズ程度の言及は除く）。
- 政府：『国家安全保障戦略』（2022 年 12 月 16 日閣議決定）
- 国会：　参議院内閣委員会　附帯決議（2022 年 5 月 10 日）
  衆議院内閣委員会でも附帯決議を採択しているが、参議院の方が内容・項目数が多いため、こちらを採用。
- 与党：　自由民主党政務調査会および経済安全保障推進本部「『経済財政運営と改革の基本方針 2023』に向けた提言」（2023 年 5 月 23 日）
- 財界：　一般社団法人日本経済団体連合会「経済安全保障法制に関する意見:有識者会議提言を踏まえて」（2022 年 2 月 9 日）

- **セキュリティ・クリアランス**とは、政府が指定した機密情報を取り扱う適格性審査のこと。主要国では制度が整備されているが、日本では未整備。内閣官房に設置された「経済安全保障分野におけるセキュリティ・クリアランス制度等に関する有識者会議」が 2023 年 6 月、「中間論点整理」を公表。「論点整理」によれば、特定秘密保護法の 4 分野に加え、経済安全保障上重要な情報（４分野と同等・準ずるもの）を保全対象に指定する。具体的には、①経済制裁関連の情報、②経済安保規制の審査に関する情報、③サイバー脅威情報、④宇宙・サイバー分野での政府共同開発に関わる重要技術情報等である。セキュリティ・クリアランス制度は民間人にも適用できる。現岸田政権は 2024 年通常国会で、改正経済安全保障推進法を提出し、セキュリティ・クリアランス制度を構築する予定。
- **サプライチェーン上の人権リスク対応**とは、サプライチェーン上の人権侵害リスクの有無の調査（人権デューディリジェンス）を含めた必要な対応を講じること。日本では法制化の議論もあったものの、企業向けガイドラインが公開された（経済産業省が 2022 年 9 月、「責任あるサプライチェーンにおける人権尊重のためのガイドライン」を公開）。純粋な人権問題対応の側面に加えて、中国新疆ウイグル自治区の人権状況をはじめ、米中対立の側面も否定できない。
- **産業スパイ・サイバーセキュリティ対策**とは、外国政府を背景とする、当該国の産業振興や強制的な技術移転のためのスパイ活動への対処を指す。特に国家機関の関与が疑われる「高度で持続的な脅威（APT）」によるサイバー攻撃と情報窃取への対処を含む。
- **データをめぐる安全保障**とは、民間企業が保有するデータが、国家安全保障等の名目で政府に不当にアクセスされないこと。G7 広島サミット等では、不当な「ガバメントアクセス」（民間企業が保有するデータへの政府の強制的なアクセス）への懸念が表明された。従来から、犯罪捜査の一環でガバメントアクセスは行われてきたが、近年では諜報活動や産業振興・技術移転の疑いのあるガバメントアクセスが懸念されている。ガバメントアクセスを担保する手段として、各国政府が外国企業等に対して、生成された個人・産業データを自国で保存することを義務付けたり、第三国への移転を禁止・制限する規制、いわゆる「データローカライゼーション」規制が進展している。
- **偽情報・ディスインフォメーション対策**とは、悪意ある偽情報（disinformation）への対応。厳密には、正しい情報であっても、悪意ある活用（その場合、malinformation、influence operation 等と呼ばれることが多い）への対処を含む。自民党や EU 米国貿易技術評議会（TTC）の経済安保関連提言・成果文書で言及された。一般的に、民間企業の対策の必要性は大きくないが、鉱物分野や製薬・医療分野では国家が関与する大規模なディスインフォメーションが確認されている。
- **研究インテグリティの見直し**とは、従来の研究倫理（研究不正、利益相反等）に加えて、新たな研究倫理（外国影響の防止、技術流出防止）を含む研究態勢を構築すること。2021 年 12 月、内閣府がチェックリスト等を見直し、研究者や研究機関・企業に新しい研究インテグリティに基づく対応を求める。
- **安全保障貿易管理の強化**とは、国際レジームで規制される物資・技術規制への対応。日本では、外為法および関連法規に基づく対応を指す。最近では、外為法第 25 条第 1 項の解釈運用を変更し、「みなし輸出」を見直すことで、軍事転用されうる機微技術の管理を厳格化した。
- **重要・新興技術管理**とは、既存の安全保障貿易管理で規制されない新興技術・基盤技術に関する管理・調整。特に同志国・有志国によるもの。自民党は既存の国際輸出管理レジームと、これに基づく外為法等の安全保障貿易管理に加えた新たな新興技術管理の枠組みを提唱。バイデン政権は半導体と同様に、AI、量子、バイオテクノロジー・バイオ製造、再生エネルギー関連技術を技術管理の強化対象にすることを検討。

- **国際標準化**とは、次世代技術の開発・実装等に関する「開放的で、自主的で、コンセンサスに基づく標準」を策定すること　（G7 成果文書）。
- **投資審査の取組・体制強化**とは、外国による所有・支配・影響（FOCI）を通じた先端技術の漏洩・機密情報へのアクセスやその他悪影響を予防するもの。日本では外為法等に基づき、上場企業の約 56.5%（2,159 社）が指定業種（コア業種を含む）に指定され、一定の外資規制（事前届出制度等）がある。米国、英国、中国等でも安全保障上の理由から外資規制が強化される傾向にある。インバウンド投資のみならず、アウトバウンド投資の規制（例：米国の対中投資規制）にも留意。
- **非市場的政策、慣行への対応**とは、ルールベースの経済活動や予見可能性を損ねる恣意的な政策や慣行への対応。具体的な政策や慣行として、不透明かつ有害な産業補助金、国有企業による市場歪曲的慣行、強制技術移転（G7 広島サミット成果文書より）。
- **経済的威圧への対処**とは、政治的影響力行使のため、自国に対する経済的依存関係を武器に不当な経済的措置を講じることへの対処。「経済的威圧」の具体例として、不当な輸出入の規制（例：中国によるレアアースの対日輸出規制、日本の福島原子力発電所関連の処理水放出に関する水産物の対中輸入規制等）、許認可の見直し、対象国への自国民旅行客の制限等。中国による経済的威圧を念頭に、日米欧で政策協調されたテーマ。EU では、経済的威圧への対処のための対外ツールを整備中。
- **業界ごとの「リスク点検」**とは、重要な産業分野におけるリスクや課題の洗い出しのこと。過去（2021 年）、与党・自民党で実施したリスク点検を行政側で継続・定式化するもの。『国家安全保障戦略』では各産業等が抱えるリスクの継続的点検が盛り込まれた。なお、自民党が実施したリスク点検は①エネルギー、②情報通信、③交通・運輸、④医療（医薬含む）、⑤金融の 5 分野を「戦略基盤産業」として対象にした。
- **経済インテリジェンスの強化**とは、官民それぞれで経済安全保障に関するインフォメーションを収集し、特定の目的のために評価・解釈し、意思決定や判断に活用できるインテリジェンスに昇華させる態勢構築・強化を指す。

4．企業に期待されるリスク管理

以上のように、経済安全保障推進法の成立・公布から 1 年 4 か月あまりが経過した現在、推進法中の 4 制度の具体化が進む。しかし、制度・施策の対象となる技術・物資・業界は将来的に拡大・変化する可能性も示唆されており、政策動向の継続的なモニタリングは不可欠だ。加えて、推進法に限定されない幅広い経済安全保障上の新たなテーマ・課題が次々と指摘され、あるいは議論の俎上に上がりつつある。

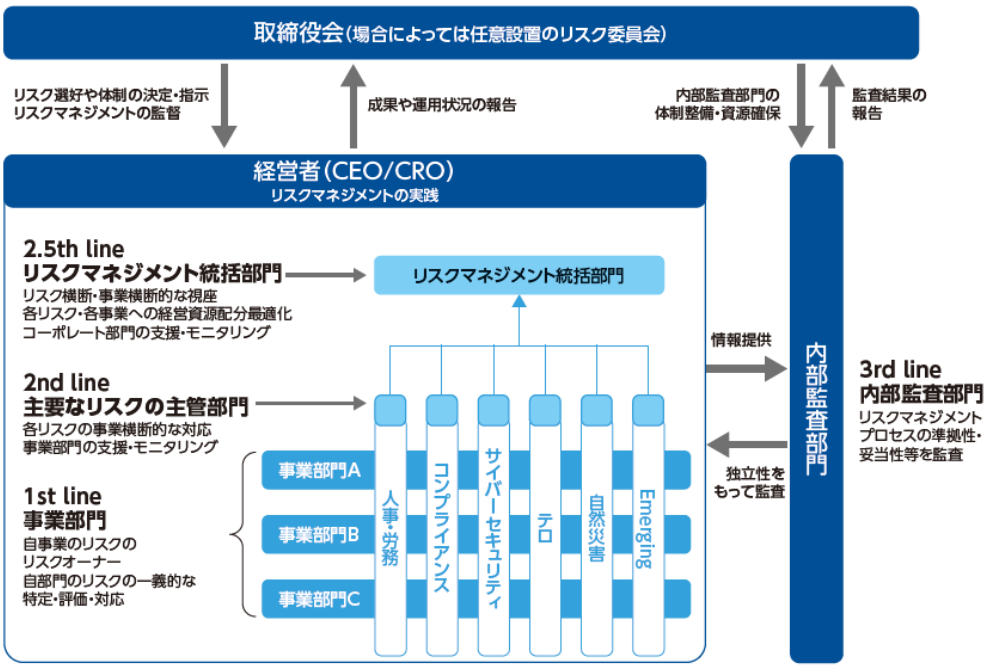
企業には、経済安全保障に関するリスクや課題は広範囲に渡り、かつ流動的で変化が激しいことを認識した上で、リスクマネジメント活動のサイクルをアジャイル化することが求められる。そのための①最適な組織体制の構築、②経済安全保障動向の常時継続的モニタリングとリスク評価、③リスク対応は以下の通りである。

◆ 組織体制の構築： 全社的な視点に立って、抜け・漏れをなくす

企業の執行サイドのリスクマネジメント体制は一般的に「3 つの防衛線（3 lines of defense）」モデルを基に設計されることが多い。「3 つの防衛線」とは、「第 1 線」としての事業部門、「第 2 線」としての主要なリスクの主管部門（例：人事部門、IT・サイバーセキュリティ部門等）、全社的なリスクマネジメントを推進する「第 2.5 線」としてのリスクマネジメント統括部門、「第 3 線」としての内部監査部門である。第 2.5 線は常設の組織・部門のみならず、委員会形式が併用されることも少なくない。

経済安全保障上の課題やリスクに効果的に対応できている企業・組織の特徴として、①安全保障貿易管理、サイバーセキュリティ対策、研究インテグリティ等の**個別の経済安全保障テーマ・リスクは第 1 線（事業部門）や第 2 線で対応**し、②**経済安全保障に関するテーマ・リスク全般や政策動向全般は、第 2.5 線のような立場や機能が担っている**ことが指摘できる。この「第 2.5 線のような立場や機能」は組織によって異なるが、常設部門であれば、リスク統括部門、経営企画部門、経済安全保障専任部門、政策渉外部門等であり、委員会形式であれば、リスクマネジメント委員会、経済安全保障委員会等といった会議体である。最適な組織形態は各社により異なるが、各企業がこれまで構築してきたリスクマネジメント体制を活用することも効果的・効率的であろう。

■ 図表 4 企業のリスクマネジメント体制



出典：柴田慎士「リスクマネジメント体制・プロセスの整備状況」、東京海上ディーアール株式会社『リスクマネジメント動向調査 2021』（東京海上日動火災保険株式会社、2022 年 1 月）、11 頁より抜粋。（The Institute of Internal Auditors "The IIA'S Three Lines Model: An update of the Three Lines of Defense," September 9, 2020 を参考に作成）

◆ リスクアセスメント： 常時継続的なモニタリングで変化を捉える

全社的な対応体制が構築された後、2.5 線部門（または、経済安全保障を専任とする部門等）が経済安全保障の観点からの「リスクアセスメント」を実施することが望ましい。ここでいうリスクアセスメントは、一般的なリスクマネジメントのプロセスと同様に、経済安全保障に関わるリスクを特定・洗い出し、自社の経営・事業への影響を評価し、優先的に対応すべき課題・リスクを決定するプロセスである。

しかし、経済安全保障を考慮したリスクアセスメントは、**常時継続的な政策動向等に関する情報収集とこれに基づく影響評価**が期待される。というのは、前述の通り、①既に特定・評価した個別テーマであっても、その内容が流動的であり、自社への影響も変わりうる、②既に洗い出された個別テーマに加えて、新たな個別テーマが形成されうる、からである。一般的なリスクアセスメントは年単位（もしくは隔年）で実施されることが多いが、こうした経済安全保障観点での情報収集とアセスメントはより高頻度で、または政治イベントをふまえて不定期（法案審議時、新たな政策・成果文書の公開時等）に行われるべきである。

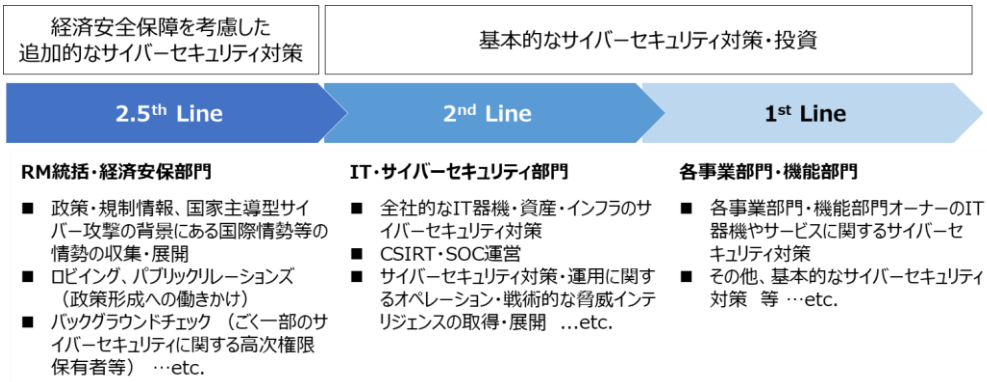
また、個別テーマを分析・評価する場合、**自社への適用可否や蓋然性よりも影響度（インパクト）を重視**すべきである。なぜなら、①政策の実現可否や法律の適用可否は政治状況や政治判断によって変化しうるし、②法律関連の個別テーマについて、仮に自社が法律や政策の直接の適用対象ではなくとも、法律や政策の趣旨や背景をふまえた判断や行動が期待される場合があるからである。

◆ リスク対応： 第 1 線、第 2 線のリスク対応を支える

自社にとって影響度が高いと判断されたリスクや課題に対しては、対応方針を策定し、リスク対応活動を行うことが不可欠である。個別リスクの低減や回避といったものもあれば、課題・リスクによっては個社企業や業界団体・経済団体による政策形成（ロビイング）やパブリック・リレーションズも有効な対応の一つとなるであろう。

個別の経済安全保障上の課題やリスクへの対応では、前述の「第 2.5 線のような立場や機能・部門」の活動が重要となる。例えば、個別テーマとしての「サイバーセキュリティ」をあげれば、（第 1 線や第 2 線が）基本的なサイバーセキュリティ対策・投資を行った上で、（第 2.5 線が）経済安全保障を考慮したサイバーセキュリティ対策を追加的に実施する必要がある。実際には、以下でいう第 2 線部門（IT・サイバーセキュリティ部門等）と第 2.5 線（リスクマネジメント統括部門、経済安全保障部門等）の共同・連携といった形になるだろう。

■ 図表 5 個別テーマへの対応例



To Be a Good Company

[2023 年 9 月 4 日脱稿、2023 年 9 月 20 日発行]

東京海上ディーアール株式会社

ビジネスリスク本部 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）
ビジネスリスク本部 研究員 渡邉 彩恵香（専門分野：リスクマネジメント）
〒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 https://www.tokio-dr.jp/