KPMG

KPMG Newsletter

KPMG Insight

Sustainability

経済安全保障リスク対応の現在地
ーサステナビリティと交錯するリスクへの備え

Vol. 61

July 2023

Sustainability

経済安全保障リスク対応の現在地
― サステナビリティと交錯するリスクへの備え

KPMGコンサルティング
Sustainability Transformation
新堀 光城／シニアマネジャー

2023年5月、ウクライナのゼレンスキー大統領の電撃訪問など、注目を集めたG7サミットが広島で開催されました。そのアジェンダにも経済安全保障が取り上げられたように、いまや経済安全保障はサステナビリティと同様、各国政府における最重要課題の1つとなりました。企業における安全保障リスクは、従前より輸出管理や経済制裁対応のなかで検討されてきましたが、現在ではより広く捉えられ、重要物資のサプライチェーン戦略や中長期的な海外事業戦略など、事業戦略において検討する必要性が高まり、グローバルなサプライチェーンを有する企業を中心にその取組みが広がっています。

本稿では、日米の経済安全保障政策について、近時の動向を中心にその概要と影響を紹介するとともに、経済安全保障リスク対応の例として、シナリオ分析と体制検討の要点について解説します。

なお、本文中の意見に関する部分については、筆者の私見であることをあらかじめお断りします。

新堀 光城
Mitsushiro Niibori

POINT 1

経済安全保障とサステナビリティ

米国の国家安全保障戦略にサステナビリティ視点が取り込まれるなど、経済安全保障と人権などのサステナビリティが関連付けて議論されている。企業においても、双方の動向を踏まえたリスク管理施策を講じることが望ましい。

POINT 2

貿易と人権

輸出管理と人権イニシアチブなど、貿易管理において人権侵害防止の視点を考慮したルール形成に向けた議論が広がっている。今後は、サプライチェーン上の人権デュー・ディリジェンスを含む人権施策の重要性が一層高まることが予想される。

POINT 3

施策の基礎としてのリスク評価

関連リスクや対応事項が広汎かつ複雑になるなかで、自社のビジネスモデルに関連するリスク情報の収集・分析を施策の第一歩として進める企業が増加している。

POINT 4

サプライチェーンリスク

リスク評価においては、特定国・地域への依存関係が大きく、代替性の乏しい重要物資のサプライチェーンを特定することがポイントとなる。

I 経済安全保障の意義と背景

近時の国際情勢の不安定化、サプライチェーンの特定国依存への懸念、先端技術の軍事利用などを背景に、各国政府において経済安全保障政策および関連法制の策定が進展しています。こうした各国政府の動向などを受けて、グローバルなサプライチェーンを有する多くの企業にとって、経済安全保障リスクへの対応は不可欠な経営リスクに位置付けられています。

「経済安全保障」とは、国家の主権や独立、国民の生命・財産などの国益を経済面から確保することを言います。具体的には、半導体やエネルギーなどの重要な物資・資源の確保、先端技術の開発・保護といった経済活動を通じて、安全保障上の脅威からの、国家・国民の保護を目指す取組みのことです。類似の概念として、「エコノミック・ステイトクラフト」が挙げられますが、これは国家戦略上の目標実現のために経済的手段を用いて自らの政治的意思の反映を求めるものであり、その手段として経済制裁、輸出管理、通商の停止・障壁の設定、援助などがあります。双方とも経済的な手段を通じた取組みである点で共通するものの、脅威からの安全に重点を置いた守りの側面が強い経済安全保障に対して、エコノミック・ステイトクラフトは（他者に対して）政治的な意思の反映を重視する点で、プロアクティブな側面が強い概念であると言えるでしょう[1]。

II 日米の経済安全保障政策とその影響

1. 日本の経済安全保障政策

日本の経済安全保障政策では、①戦略的自律性の向上、②戦略的不可欠性の向上、③国際秩序の維持・強化が重視され、これを支える推進体制の強化が図られています。①戦略的自律性とは、「わが国の国民生活及び社会経済活動の維持に不可欠な基盤を強靭化することにより、いかなる状況の下でも他国に過度に依存することなく、国民生活と正常な経済運営というわが国の安全保障の目的を実現すること」、②戦略的不可欠性とは、「国際社会全体の中で、わが国の存在が国際社会にとって不可欠であるような分野を戦略的に拡大することにより、わが国の長期的・持続的な繁栄及び国家安全保障を確保すること」とされています[2]。

ここでは、その基礎的な法制度である経済安全保障推進法を説明するとともに、近時の動向として、先端半導体製造装置の輸出規制、G7サミットにおける経済安全保障に関する共同文書、人権施策への影響、セキュリティ・クリアランスについて紹介します。

(1) 経済安全保障推進法

経済安全保障政策の重要な法制度として、2022年5月、経済安全保障推進法が成立・公布されました（2年以内に段階的に施行。すでに一部施行）。同法では、①重要物資の安定的な供給の確保、②基幹インフラ役務の安定的な提供の確保、③先端的な重要技術の開発支援、④特許出願の非公開、この4つの制度の創設を趣旨としています。主に、①②が戦略的自律性に、③④が戦略的不可欠性に関する施策と見られます。特に、②基幹インフラ役務の安定的な提供の確保に関して、対象事業者とされる企業（に加えて、対象事業者に関連サービスを提供する企業）は、自社のバリューチェーン／サプライチェーンの見直しが必要となるケースが生じ得ることが想定されます（図表1参照）。

基幹インフラ役務の安定的な提供の確保に関する制度とは、エネルギー・輸送・金

図表1 経済安全保障推進法の概要

名称	概要	主な関連企業など	主な影響・対応事項例
重要物資の安定供給	半導体などの特定重要物資の安定供給の確保を図るため、民間事業者への財政支援を行うとともに、調達先などを国が把握	・半導体、重要鉱物、蓄電池、抗菌薬など、特定重要物資を製造する企業 ・上記物品のサプライチェーンを有する企業	・補助金、ツーステップローンなどの金融支援の活用
基幹インフラの安全確保	基幹インフラ14業種の特定社会基盤事業者において、特定重要設備を導入前に、事前届出を行い、サイバー攻撃などの危険について国が審査を実施	・金融、交通、エネルギーなど、特定社会基盤事業者とされた企業 ・上記事業者に機器・サービスを提供する企業	・届出などの事務 ・ベンダーの見直し ・委託先管理の強化
先端技術の開発促進	AIなどの特定重要技術の開発促進などのため、国による資金支援、官民伴走支援のための協議会などを設置	・民間の研究機関、大学 ・国立の研究開発機関	・研究開発の促進 ・情報管理の見直し
機微技術に係る特許の非公開	安全保障上機微な発明の特許出願の流出を防止するため、一定の特許について非公開化	・防衛、宇宙航空、原子力関連企業 ・大学、研究開発機関	・非公開対象特許の開示・実施制限への対応 ・特許戦略の見直し

出所：KPMG作成

融などの基幹インフラサービスの安全性・信頼性の確保のため、重要設備の導入・維持管理などの委託を国が事前審査する制度です。指定された基幹インフラサービス14業種に関して、対象事業者（特定社会基盤事業者）に重要設備（特定重要設備）の導入・維持管理などの委託に関する計画書を事前に届出をさせて、国による審査を受ける義務を課しています。審査においては、サイバー攻撃によるシステム障害や情報流出のリスクなどが検討され、審査の結果、リスク低減に必要な措置（設備の導入・維持管理の内容の変更・中止など）を勧告・命令される場合があります。

本制度に関して、2023年4月、「特定妨害行為の防止による特定社会基盤役務の安定的な提供の確保に関する基本指針」が閣議決定されましたが、対象設備などの詳細は主務省令で指定されます。対象事業者はその義務を履行するために、対象設備（設備・機器類、プログラムなど）、供給者・委託先などに関する届出事項の把握やデータマネジメント、リスク管理措置を実施し、場合によっては委託先などの見直しが必要となります（2023年6月、「経済安全保障法制に関する有識者会議」にて規制対象、届出事項等に関する検討状況を公表）。また、供給者・委託先においても取引継続のために、その対応協力が必要です。

（2）先端半導体製造装置の輸出規制

経済産業省は2023年5月、外為法に基づく貨物等省令の改正を公布し、先端半導体製造装置など23品目を輸出管理の規制対象に加えました（2023年7月施行予定）。これにより、追加される23品目は友好国など42ヵ国・地域向けを除いて個別許可が必要になります。この規制強化は、米国が2022年10月、先端半導体（14～16ナノメートル以下のロジック半導体）などに必要な装置や技術の輸出を米商務省の許可制にするなど、規制強化を図っていることが背景にあるとみられています。

（3）G7サミットにおける経済安全保障に関する共同文書

2023年5月、G7広島サミットにおいて、経済安全保障は重要アジェンダとして取り上げられ、経済安全保障に関する共同文書が公表されました。そのなかで、日本の経済安全保障政策でも重視する、重要物資に関するサプライチェーンの強化や基幹インフラの安全性、重要・新興技術の流出防止などに向けた国際連携の強化が確認されました。同文書の内容が、今後、関連する経済連携枠組みの形成や各国の政策・規制にどのように反映されていくかを注視する必要があります[3]。

G7広島サミット・経済安全保障に関する共同文書の要点

- **強靭な供給網の構築**
  全ての国に「強靭で信頼性のあるサプライチェーンに関する原則」への支持を促進するとともに、重要物資のサプライチェーンを強化
- **強靭な基幹インフラ構築**
  デジタル領域などの基幹インフラの安全性を強化するため、ベストプラクティスの共有などを通じた協力関係を強化
- **非市場的政策への対応**
  不透明な産業補助金、強制的な技術移転などへの懸念を表明し、WTOにおける取組みを強化
- **経済的威圧への対処**
  経済的威圧への懸念を表明し、「経済的威圧に対する調整プラットフォーム」を通じたパートナー間の協力を促進
- **デジタル領域の有害な慣行への対抗**
  企業へのデータ管理規制（政府によるアクセス許可など）への懸念を表明し、慣行への対抗に向けた戦略的対話を進展
- **国際標準化における協力**
  「デジタル技術標準に関するG7連携のための枠組み」を通じた協力を再確認
- **重要・新興技術の流出防止のための連携・取組強化**
  先端技術の軍事力強化への利用防止に向けた連携や、輸出管理における多国間取組みを強化

（4）人権施策への影響

日本では、欧州で策定が進む人権デュー・ディリジェンスを義務付ける法制（ドイツのサプライチェーン・デューディリジェンス法など）や、米国の貿易円滑化・貿易執行法のような人権侵害被疑物品の輸入規制が策定されていません。一方で、日本でも、人権デュー・ディリジェンスを義務付ける法整備の議論や、デュアルユース製品・技術（民生と軍事の両目的に使用できる製品・技術）の人権侵害への利用防止を目的とした有志国連携枠組みの「輸出管理と人権イニシアチブ（ECHRI）」に参加するなどの動きは見られます。

また、ガイドラインレベルであるものの、2022年9月に「責任あるサプライチェーン等における人権尊重のためのガイドライン」（日本政府）が、その企業実務を後押しするため、2023年4月に「責任あるサプライチェーン等における人権尊重のための実務参照資料」（経済産業省）が公表されました。このような動きのなか、今後、企業の輸出管理・通商においても、人権デュー・ディリジェンスを含む人権侵害防止の取組み要請が強化されることが予想されます（ECHRIについては後述）。

（5）セキュリティ・クリアランス

日本でも、セキュリティ・クリアランス制度の導入に関する議論が進んでいます。セキュリティ・クリアランス制度とは、国家における情報保全措置の一環として、政府が保有する安全保障上重要な情報として指定された情報にアクセスする必要がある者に対して政府による調査を実施し、当該者の信頼性を確認したうえでアクセスを認める制度のことです（内閣官房「中間論点整理」）。米国、英国などでは導入されており、次世代技術の国際共同開発の機会を拡充することなどを理由に、その必要性が議論されています。

2023年6月、制度導入に関する中間論点整理が公表され、その指定対象の範囲について、経済制裁に関する情報、サイバー攻撃への防御策、宇宙・サイバー分野

などでの国際共同開発に関する情報が挙げられました。制度が導入された場合、情報保全を適切に実施するための体制整備などの負担が生じ得るため、その動向を注視する必要があります。

2.米国の経済安全保障政策

米国の現政権の政策では、インド太平洋地域の重視や、国内労働者の保護と通商政策の連携を重視する前政権の方針を踏襲しつつも、サステナビリティに関する広範なテーマをも安全保障上の問題として捉え、同盟国・友好国などとの協調を通じて解決を図ろうとする姿勢が見られます。

2022年10月に公表された国家安全保障戦略では、軍事面だけでなく、基幹インフラの保護、重要物資のサプライチェーン、気候変動・エネルギー問題、食料不安、人権など、広範な分野を安全保障上の重要課題として挙げています。また、民主主義の強化を強調する一方、たとえ民主的ではない国であっても、ルールに基づく国際秩序を支持する国であれば協力していく旨が示唆されている点も注目されます[4]。

以下、関連政策のうち、輸出・投資などに関する規制強化、重要物資のサプライチェーン政策、輸出管理と人権イニシアチブについて紹介します。

(1) 輸出・投資などに関する規制強化

輸出規制・取引規制の代表例としては、米国輸出管理規則（EAR：Export Administration Regulations）と米国OFAC（Office of Foreign Assets Control：財務省外国資産管理室）規制が挙げられます。EARは米国原産品目などの対象品目の再輸出（米国外から第三国への輸出）について米国商務省の許可を要求するなどの制限を、OFAC規制は米国内外においてSDNリスト（Specially Designated Nationals and Blocked Persons List）の掲載者との取引禁止などを定めるもので、域外適用に注意が必要となります。

近年、米国は対中輸出規制の強化を継続しており、2022年10月、EARの改正により、AI技術に利用する先端半導体やその製造装置、スーパーコンピュータの対中輸出規制を大幅に強化しました。これにより、米国などの半導体メーカーが中国向けの輸出を縮小するなどの動きが見られます。また2018年には、新興技術（AIなど14分野）、基盤技術（半導体製造装置など）の輸出規制に関する輸出管理改革法（ECRA）が成立しています。

対米投資においては、米国ではCFIUS（対米外国投資委員会）による審査を通じて、安全保障上懸念のある対米投資を制限しています。近時、外国投資リスク審査現代化法（FIRRMA）およびその下位規則によって、CFIUSの審査対象となる取引の範囲が大幅に拡大されました（外国企業などによる重要技術・インフラ、機微な個人データに関する事業投資、不動産取得など）。企業は、投資案件の審査基準・プロセスがこれに対応したものかを確認し、必要に応じて見直す必要があります。

(2) 重要物資のサプライチェーン政策

2022年2月、米国は国内製造業の活性化と重要製品のサプライチェーン強化に向けた計画を発表、「CHIPSおよび科学法」（2022年8月成立）などを通じて、半導体などの重要物資のサプライチェーンについて国内回帰や友好国での形成を後押しする政策を打ち出しました。

また、米国主導のもと、IPEF（インド太平洋経済枠組み）では、①貿易、②サプライチェーン、③クリーン経済、④公正な経済の4つの柱について交渉目標が設定され、インド太平洋地域での連携を強化する政策が議論されています。2023年5月には、その柱の1つである、重要物資のサプライチェーンの強化に関する協定が合意されています。関連物資のサプライチェーンを有する企業は、その具体的なルール形成の動向を注視する必要があります。

サプライチェーンに関する協定の要点

- 途絶リスクの高い物資についての参加国間の情報共有
- 重要物資について、参加国同士での調達先の拡大
- 重要物資が不足した国・地域へのサポート
- サプライチェーン上の労働者の権利を尊重する企業への積極的な投資

(3) 輸出管理と人権イニシアチブ

米国は2023年3月、「輸出管理と人権イニシアチブ（ECHRI）」に関する行動規範を、日本を含む有志国とともに策定しました（Export Controls and Human Rights Initiative Code of Conduct Released at the Summit for Democracy - United States Department of State）。ECHRIは米国主催の第1回民主主義サミット（2021年12月開催）で提案された、有志国間の連携枠組みです。軍事用・民生用のデュアルユース製品・技術の人権侵害への利用防止を目的とし、日本を含む24ヵ国が参加しています。

上記行動規範は、非拘束的なものであるものの、参加国にデュアルユース製品・技術の人権侵害への利用防止に向けたルール・取組みの推進や、企業などにおける人権デュー・ディリジェンスの促進を求めています。輸出管理・通商の側面においても、人権デュー・ディリジェンスを含む人権尊重に向けた取組みの要請が高まることが想定されます。

ECHRI行動規範の要点

- デュアルユース製品・技術の人権侵害への利用防止に向けたルール・取組みの推進
- 人権問題や輸出管理法令の執行に関する、産官学、市民との協議・連携
- 技術進歩がもたらす人権への脅威やリスクに関する情報に対する有志国間の継続的な共有
- 人権侵害防止に向けた輸出管理に関するベストプラクティスの共有
- 企業などにおける人権デュー・ディリジェンスの促進
- 非参加国のキャパシティビルディングおよび行動規範に沿った行動の促進

3.経済安全保障リスクの視点

前述のような経済安全保障政策・関連規制は、企業の貿易、投資、サプライチェーン施策など、さまざまな面で影響を及ぼし、その対応範囲は従来からイメージされる安全保障リスクよりも広範囲に及びます。特に、サプライチェーン・事業戦略に直結するリスクや人権などのサステナビリティリスクは重要な経営課題となり得ます。「対象となる重要物資のサプライチェーンを有するか」、「対象となる基幹インフラ事業者やその供給者に該当し得るか」、「規制対象品目を輸出しているか」、「政府調達に伴う調達基準の順守の適用対象となり得るか」などについて、自社のビジネスモデルと照らして整理をし、自社に影響を及ぼし得る経済安全保障リスクの特定と、リスク対応の主管部門・連携部門を整理・認識共有を図ることが大切です（図表2参照）。

III リスク管理に係る施策と体制整備

リスク対応の基本は、リスクを特定・評価すること、リスクの程度に合わせて各種施策を策定・導入すること、これらの施策を支える体制を整備することにあります。以下、①リスク評価と対応策の策定、②体制整備という側面から、企業の施策のポイントを紹介します。

1.リスク評価と対応策の要点

リスク評価にはさまざまな具体的なアプローチがあり、目的によって進め方や着眼点は異なります。ここでは、代表的なシナリオ分析アプローチについて紹介します（他にも、政治（P）・経済（E）・社会（S）・技術（T）・法律（L）・環境（E）に着目するPESTLE分析に基づく事業環境分析などの外部環境分析があります）。

（1）シナリオ分析の各ステップ

シナリオ分析アプローチは、自社のビジネス・サプライチェーンに対する具体的な危機シナリオと自社ビジネスへの影響を分析し、その対応策を策定する手法です。特に、ビジネスモデル・サプライチェーン上の脆弱性を把握し、サプライチェーン戦略やリスク管理などの施策に活用することに適しています。（図表3参照）。

STEP1　対象事象の選定

危機シナリオの検討では、自社グループに大きな影響を与えることが想定されるリスク事象を特定します。その際には、国内外の政治（国家間対立、軍事同盟、領土問題など）、規制環境、先端技術開発等の動向を踏まえ、中長期的な視点で自社ビジネスに影響がある事象を選定します。

図表2　経済安全保障リスクの整理例

視点	日本・関連法制度例	米国・関連法制度例	企業への影響例	関連部門例
安全保障貿易・経済制裁	・外為法	・EAR・ECRA ・OFAC規制	輸出管理規制の改正・リスト更新への対応	・輸出管理 ・法務
投資規制	・外為法	・FIRRMA	各国における投資規制対応	・経営企画 ・法務
情報セキュリティ	・IT調達に係る政府調達ルール ・防衛調達サイバーセキュリティ基準	・2019年度国防権限法889条 ・大統領令13873号 ・NIST SP800-171	各事業プロセスにおける情報漏洩・セキュリティリスクへの対応	・情報セキュリティ
セキュリティ・クリアランス	（特定秘密保護法）	・大統領令13526号、12968号、12829号	対象となる機密情報へのアクセス制限への対応	・情報セキュリティ ・研究・開発
人権	（責任あるサプライチェーンなどにおける人権尊重のためのガイドライン）	・グローバル・マグニツキー人権問責法 ・貿易円滑化及び貿易執行法	自社およびサプライチェーン上の人権侵害防止	・経営企画 ・サステナビリティ推進 ・法務
サプライチェーン強靭化	・経済安全保障推進法	・CHIPSおよび科学法	重要物資の安定供給確保に係る補助政策の活用	・経営企画 ・調達・物流
基幹インフラの安定		・FIRRMA ・国防権限法	基幹インフラ事業者における重要設備の導入審査への対応	・情報セキュリティ ・調達・物流
技術開発		・CHIPSおよび科学法 ・国防権限法	先端技術の開発における国による支援の活用	・経営企画 ・研究・開発
特許の一部非公開		・特許法	安全保障上機微な発明に関する公開制限への対応	・研究・開発 ・知的財産

出所：KPMG作成

STEP2　シナリオ分析

当該事象の具体的なシナリオを分析します。分析に当たっては、時系列での事象分析と関連リスクテーマごとの分析が有効です。

時系列分析では、たとえば、グレーゾーン事態（国家間において、領土・経済権益などについて主張の対立があり、少なくとも一方の当事者が、武力行使に当たらない範囲で、実力組織などを用いて問題に係る地域にて頻繁にプレゼンスを示している状態）で想定される事象や、軍事衝突事態で想定される事象を局面ごとに分けて、自社ビジネスに影響し得るシナリオを具体的に分析します（例：海峡封鎖、大規模なサイバー攻撃、軍事施設などへの武力行使、経済制裁とその対抗措置など）。一方、リスクテーマごとの分析では、役職員の安全・人権、情報セキュリティ、会社資産などの視点から、想定されるリスク事象を整理し、影響分析や主管部門検討の基礎資料とします。

STEP3　企業への影響分析

シナリオ分析で検討した具体的なシナリオに基づいて自社への影響を分析し、重要な影響を生じ得る脆弱性を明確にします。その際には、伝統的な手法である経営資源を構成する4つの視点（ヒト・モノ・カネ・情報）から自社への影響を定量／定性の両側面から把握することが重要です。定量的な側面では、たとえば、予想される生産数、販売数の減少数、原材料の高騰などに基づき収益への影響を、定性的な側面では危険に晒される役職員などの安全、人権や情報資産への影響を把握することが考えられます。

その際に、自社ビジネスのバリューチェーン／サプライチェーンで大きな影響を受けるプロセスはどこか（例：某国・地域のグループ会社の重要生産拠点が停止する）、複数ある自社ビジネスのうち影響の大きいビジネスは何か（例：半導体が調達できなくなり、半導体利用製品の製造・販売が不可能となる）を検討することが有用となります。そして、これらの分析を通じて、自社に重大な影響を与える事項（脆弱性）を把握し、対応策の検討につなげます（たとえば、重要な部品・資材について、特定国・地域の特定のサプライヤーに依存し、有事においてその調達に支障をきたす恐れがあるにもかかわらず、代替的な調達先が確保できていないもの）。

STEP4　対応策の策定

上記影響分析を踏まえて、自社ビジネスのバリューチェーン／サプライチェーン上の脆弱性への対応を中心に、対応策を策定します。

（2）対応策策定の要点

（i）平時の取組みの見直し

まず、サプライチェーン戦略、BCP（事業継続計画）の見直しが重要です。有事では、製品・原材料の輸送手段・ルートの制限、各国制裁による取引制限、生産工場のオペレーションの停止、原材料の高騰などにより、サプライチェーンに多大な支障をきたす恐れがあります。そのため、リスクの高い国・地域との取引に依存する原材料・部品を中心にサプライチェーンの多元

図表3　シナリオ分析のステップ例

出所：KPMG作成

化、製造設備への投資、備蓄確保などについて、その可否や課題も含めて、具体化しておくことが望ましいです。現実的には、すぐに解決できない事項が多いですが、まずは中長期的な経営課題として認識共有を図っておき、施策を展開する土壌を形成します。

また、新規投資判断や既存事業のモニタリングについても、リスクを踏まえた経営判断ができるプロセスや基準になっているか、人権デュー・ディリジェンスなどサステナビリティ視点も加味されたものとなっているかを見直すことは、各ステークホルダーへの説明責任の観点からも欠かせません。関連して、万が一の場合に備えて、事業撤退に関する方針・手続きについても事前に整理しておくことも望ましいです。

（ii）有事における対応事項の見直し

役職員の安全確保に向けた退避行動、関係部門や政府機関などとの連携についてあらかじめ危機対応マニュアルを用意し、シミュレーションなどを通じて認識共有を図っておきます（センシティブなテーマについては、まずは関係者を必要最小限に絞って対応することも一案です）。また、リスクの予兆となる事象を事前に整理し、その予兆が見られたときに警戒レベルを上げ、速やかに危機対応体制への移行やリスク対応策の実行などをできるようにしておくことも有効です。

有事においては、サプライチェーンの混乱、各国経済制裁に基づく取引制限、国際的な世論などを踏まえて、既存／新規ビジネスに関する維持・縮小・撤退に関する経営判断を迫られる場面に直面するかもしれません。どのようなプロセス・考慮要素で判断をするのかを事前に整理しておくことが望ましいです。

（iii）体制の見直し

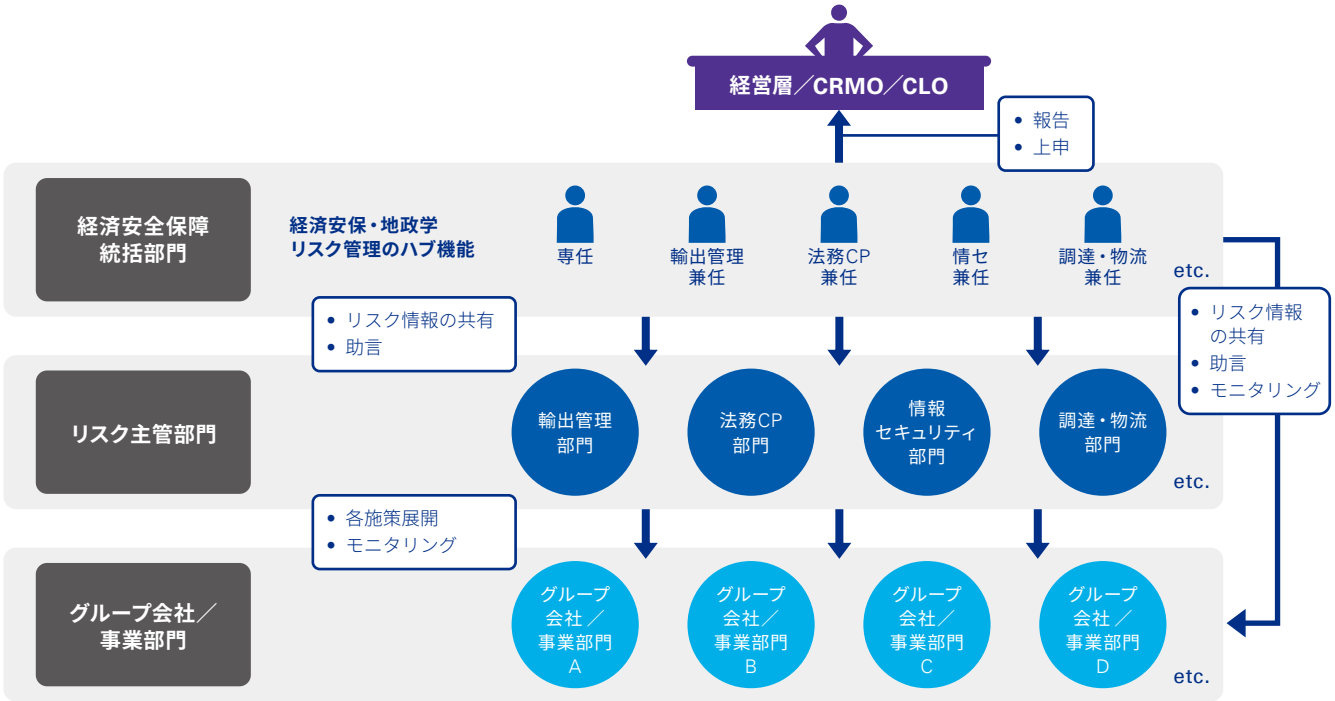
特定したリスクを踏まえて、各リスク対応策を実施する機関・部門の明確化や、有事の際の危機対応体制を明確化します。前者については、情報セキュリティ、サプライチェーン、役職員の安全・人権などに関連する対応の主管部門を明確にし、効率的な連携を可能とする組織設計となっているかを検証します。有事においては不祥事同様、初動対応が特に重要となります。そのため、後者はあらかじめ対応チームの構成、政府機関や外部専門家などとの連携体制、エスカレーションプロセスを明確にし、実施事項・プロセスと役割を文書化のうえ、認識共有を図っておくことが望ましいです。

2. リスク管理体制の整備

（1）リスク管理体制設計の考え方

経済安全保障や地政学リスクに対応するには、国内外の情勢変化のビジネスへの影響を適切に見極めなければなりません。そのためには、安全保障、情報セキュリティ、サプライチェーンなどの各リスクの主管部門が連携する必要があります。紛争などの危機状況への対応や、中長期的な事業戦略において適切に経営判断を行

図表4 経済安全保障統括部門の設計例



出所：KPMG作成

うには、リスク情報を可及的に正確かつ多面的に入手でき、適時かつ果断な意思決定を可能とする体制・プロセスが必要です。

経営陣、特に経済安全保障リスクを管掌するCRMO（チーフ・リスク・マネジメント・オフィサー）やCLO（チーフ・リーガル・オフィサー）には関係部門を取りまとめ、経営者による迅速な意思決定を支える司令塔としての役割が期待されます。また、関係部門が日頃から、情報共有や施策策定の連携などをしやすい仕組みを整備しておくことも必要です。

このような観点から、体制強化の方法例としては、(1) 従来のリスク主管部門を維持したまま、主要な関係部門のメンバーで構成する委員会を設置し、情報の連携を強化するケース（委員会設置型）、(2) 経済安全保障・地政学リスクに関する統括部門を設置し、日常的に各リスク主管部門のハブ機能を持たせるケース（統括部門設置型）、(3) 双方を組み合わせるケースなどが考えられます。

ただ、統括部門の設置は、委員会の活用よりもリソース確保などの負担が大きくなります。そのため、まずは委員会などの会議体を活用しながら、必要に応じて統括部門の設置を検討することが現実的と思われます。統括部門の設置が適するケースとしては、たとえば、高リスク業種（規制対象品目の輸出や重要技術の取扱いが多い／重要インフラ業種など）に属し、日常的に連携すべき業務が多く、常時、各部門の担当者をアサインすることが効率的である場合です。

なお、統括部門を設置する場合には、各リスク主管部門と円滑な施策の連携ができる体制とするために、統括部門の専任者のほかに、関連する主要なリスク主管部門を兼任して部門間の橋渡しをする担当者を設置することが考えられます。また、経営陣、特に経済安全保障リスクを管掌するCRMOやCLOは、平時においても種々の関連リスクを踏まえた施策展開を推進する司令塔としての役割を担うことが期待されます（図表4参照）。

(2) 経営判断を支えるインテリジェンス機能

各施策・取組みの前提として、意思決定に必要な情報が適切に収集・分析され、経営者・事業部門などの関係者間で必要十分に共有されていること、すなわちインテリジェンス機能の整備が重要となります（ここでいうインテリジェンスとは、諜報活動・スパイ活動という意味ではなく、情報の収集・分析により情報の利用者（経営者など）にとって有意義な情報連携を可能にする活動という意味で使っています）。インテリジェンス機能のポイントは、無数にある情報のなかから、意思決定に重要な影響を与え得る情報を適切に取捨選択して共有できるか否かです。経営者は不確実な状況下、多数のステークホルダーの利害を勘案しつつ経営判断を下す必要がありますが、ノイズ情報はその判断を一層困難にします。必要十分な情報を共有するには、リスク管理部門が事業部門のニーズを把握したうえで、そのニーズに応える情報収集・分析の計画を策定・実行し、フィードバックを受けて、取組みを改善すること、すなわち情報収集・分析におけるPDCAサイクルを回すことが必要です。また、リスク管理部門だけではなく、事業部門においても主体的にリスク情報を収集・分析を行う仕組みを浸透させます。このように、事業機会とリスクの両面を踏まえて事業判断ができるようにすることが大切です。

IV 結びに

本稿で紹介した経済安全保障リスクやその対応例は一側面に過ぎず、また継続的に変化しています。したがって、社内外の動向の変化に継続的に対応できる仕組みづくりとその運用が不可欠となります。本稿がその検討の一助になれば幸甚です。

1 「エコノミック・ステイトクラフトと国際社会」『米中の経済安全保障戦略 - 新興技術をめぐる新たな競争』(2021)、著：鈴木一人ほか、芙蓉書房出版

2 「提言『経済安全保障戦略策定』に向けて」2020年12月、自由民主党政務調査会

3 経済的強靭性及び経済安全性保障に関するG7首脳声明（2023年5月20日）外務省
https://www.mofa.go.jp/mofaj/fp/es/page1_001694.html

4 THE WHITE HOUSE, NATIONAL SECURITY STRATEGY OCTOBER 2022
https://www.whitehouse.gov/wp-content/uploads/2022/10/Biden-Harris-Administrations-National-Security-Strategy-10.2022.pdf

関連コンテンツ

ウェブサイトでは、経済安全保障・地政学リスクに関する動向やサービス等を紹介しています。

https://kpmg.com/jp/ja/home/services/advisory/risk-consulting/legal-compliance/economicsecurity-geopolitics-risk.html

本稿に関するご質問等は、
以下の担当者までお願いいたします。

KPMGコンサルティング株式会社
新堀 光城／シニアマネジャー

☎ 03-3548-5111
✉ mitsushiro.niibori@jp.kpmg.com

KPMGジャパン
home.kpmg/jp

home.kpmg/jp/socialmedia