KPMG

KPMG Newsletter

KPMG Insight

Vol.
55
July
2022

Topic ①

地政学・経済安全保障リスクに向きあう日本企業の挑戦

地政学・経済安全保障リスクに向きあう日本企業の挑戦

KPMGコンサルティング
足立 桂輔／パートナー
新堀 光城／シニアマネジャー

昨今、ロシア・ウクライナ情勢に関する痛ましいニュースが連日報じられています。現在の情勢は企業のサプライチェーンへの直接的な影響のみならず、さまざまな業務活動にも影を落としはじめました。ロシア・ウクライナ情勢が象徴するように、昨今の地政学的変動の中で、各国において経済安全保障上の規制強化や制裁の執行が活発化しており、企業の貿易活動や技術情報の流出対策等にも見直しの必要性が高まっています。このような地政学・経済安全保障に関わるリスク対応は、複合的なリスク観点からの経営判断を要するものになるため、経営層を支える各部門、特に管理部門にとっても中長期的な取組みと体制整備が求められる課題です。

本稿では、地政学・経済安全保障リスクへの対応の参考にしていただくために、リスク顕在化時における事業判断の特徴、関連するリスクの概要、企業としての備え（体制整備等）を中心に紹介します。

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いたします。

POINT 1

地政学・経済安全保障リスクの視点

地政学・経済安全保障リスクの代表例として、貿易規制・制裁、投資規制、情報セキュリティ、人権、役職員等の安全、サプライチェーン等、多岐にわたるリスクが挙げられる。これらへの対応は単独部門によるものではなく、各主管部門、グループ会社等との連携が重要となる。

POINT 2

リスク顕在化時の事業判断の主な検討要素

地政学・経済安全保障リスク顕在化の際に事業を維持する場合の主な検討要素として、事業の公益性・公共性、規模等が挙げられる。一方で、事業を停止・縮小・撤退をする場合の主な検討要素には、サプライチェーンの混乱、各国の制裁、レピュテーション、役職員の安全等が挙げられる。

POINT 3

リスク顕在化時の事業判断の要諦

地政学・経済安全保障リスクに直面した際の事業判断は、最終的には自社の理念やパーパス、そして経営者の信念に沿ったものであるかで決断することになる。それを支えるためには、グローバル世論やステークホルダーの声を適時・適切に経営層に共有することと平時からの思考訓練が不可欠である。

POINT 4

地政学・経済安全保障リスク管理体制

地政学・経済安全保障リスク対応の統括部門を設置する場合、各関連リスク主管部門との円滑な施策の連携ができる体制にするために、統括部門の専任者の他に、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る。また、地政学・経済安全保障リスクを管掌するCROやCLO等は、平時においても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る。

足立 桂輔
Keisuke Adachi

新堀 光城
Mitsushiro Niibori

Ⅰ 地政学・経済安全保障リスクの考え方

1. 経営の基軸の1つとなった地政学

近年、地政学がビジネス上のバズワードになっています。当初は日中関係、ここ数年は米中新冷戦、そして現在はロシア・ウクライナ問題がその話題の中心になっていることは言うまでもありません。特に、ロシア・ウクライナ問題は、21世紀の現在において、まずは起こりえないと考えられていた先進国同士の戦争をきわめて深刻なレベルで想起させるものであり、欧米諸国のみならず世界の国々に大きな緊張をもたらしています。また、この問題の注目点の1つは、経済的な便益が軍事的目的に優るであろうという認識、言い換えれば経済関係の強化とグローバル化が軍事的紛争の回避につながる、という幻想をものの見事に壊してしまったことです。特に、日本企業においては、先の大戦への反省、そして日米安保の傘もあり、国家として軍事への関与が「控え目」であったこと、またその中で日本企業は高度経済成長の恩恵を大いに受けたことから、長らくの間、政経分離のビジネス文化が定着していました。もちろん、その時々の政治・軍事情勢による影響回避や規制対応等は行ってきてはいるものの、どちらかといえば対処的なものであり、個々の事業判断にかかる外部環境要因の1つとしてみていたことは否めません。今、求められることは、デジタル、サステナビリティと同様、乗りこなすべきメガトレンドそれそのものへの対処が企業価値を左右する命題の1つとして、常に「経営のテーブル上にのせるもの」として地政学を捉えていくことです。

2. 地政学と経済安全保障リスクの意味

地政学という言葉は、さまざまな使われ方がされていますが、一般的には、国の地理的な条件に基づいて、他国との関係性や国際社会における行動を考察するアプローチ（学問）であり、国家における戦略論の側面を持っています。これを企業の視点で捉えると、たとえば、領土問題や国際的軍事同盟への加入を巡る国家間の緊張関係や紛争が発生したときに、当該国・地域での生産・販売等の企業活動への支障や原材料の高騰、サプライチェーンの混乱、役職員の生命・身体等への危険等のリスクへの対応が論じられます。

一方、経済安全保障とは、国家と国民の安全を経済面から確保することを意味します。半導体やエネルギー等の重要な物資・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国家や国民を保護する側面を持っているということです。企業の視点では、たとえば、インフラへのサイバー攻撃を通じた活動の停止、技術情報の流出、安全保障貿易規制の強化による輸出制限等のリスク対応が論じられます。

両者は異なる概念ですが、特に企業経営・事業活動の場面において、地政学リスクは経済安全保障という形で顕在化することが多く、同時に語られることが多くなります。

3. 地政学を巡る基本的視座

昨今の地政学において、基本的視座の1つとして、間違いなく専制主義vs民主主義の図式が挙げられます。米中問題に加え、今回のロシア・ウクライナ問題によって、その流れは決定づけられたとも言えます。実際、先般の国連人権理事会等での各国の国連投票行動をみても、ロシアへの制裁や非難において強く同調する国家の数は必ずしも“大多数”とは言えないのが実情です。中国やインド、ブラジルといった、BRICSと称される国々、また東南アジアやアフリカなどの新興国の多くが、G7を含む欧米先進国の動きとは一線を画しています。GDP、すなわち経済力による加重を行えば話は別ですが、少なくとも国の数、また人口比において、欧米先進国の価値観や振る舞いに、必ずしも同調し得ない国々が多数ある現実をしっかりと理解すべきです。

このような中で日本企業は、まさに国としての日本の置かれた地政学的な位置づけと同様に、バランスのジレンマに陥ることもあり得ます。実際に、人権問題といった地政学的ニュアンスを帯びた課題に対する発信やトップのコメント等においても、中国に大きなオペレーションを有する企業にとっては配慮を強いられるケースもあります。サプライチェーンのブロック化・コンパクト化モデルがしばし語られることが多いですが、法規制対応やコンプライアンスマネジメントにおいても、ブロック化が進む世界に適したガバナンスモデルが求められつつあります。

Ⅱ リスク顕在時の企業の対応方法／パターン

1. リスク顕在化時の事業判断パターン

実際に紛争などのリスクが顕在化した場合、企業は当該リスクが発生している国・地域における事業継続を早急に判断する必要があります。しかし、この判断は多くの企業にとって容易なことではありません。その事業判断は、おおむね①継続する、②一部事業の縮小・停止をする、③完全撤退する、といういずれかのパターンに分かれます。

事業を維持する場合の主な考慮要素として（①）、事業の公益性・公共性、規模等が挙げられます。たとえば、（国策の影響を受ける）資源・エネルギー関連の大規模開発プロジェクトや、公共性が非常に高い通信インフラ事業は、事業停止・撤退の判断をすることが困難な傾向にあります。

一方、事業を停止・縮小・撤退をする場合の主な考慮要素としては（②③）、製

造・販売活動等への支障を含むサプライチェーンの混乱、各国の制裁（取引禁止、SWIFTからの除外等）、レピュテーション、役職員の安全が挙げられます。特に、製造業においては、部品・原材料の調達が困難となり、生産拠点の機能の全部または一部が停止することで生産が滞り、それに伴い販売機能も損なわれる事態に陥りやすくなります（場合によっては、生産・販売拠点自体に損壊が生じるおそれもあります）。

サプライチェーンにも関連しますが、各国の経済制裁・輸出管理規制の強化により、対象の団体・個人との取引が禁止され、事業が困難になる事態もあり得ます。また、消費者を中心として、人道的な観点からレピュテーションリスクが発生し、それによってエシカル消費に関する意識の高い欧米市場等で深刻な打撃を受けることもあり得ます。加えて、紛争地域や紛争の当事国における駐在員・ナショナルスタッフ等の生命・身体・自由への侵害も懸念されます。

なお、日本企業においては希少ではあるものの、昨今の情勢下においては、侵略国による活動に対する積極的な妨害や抑制、また被侵略国における防衛策への積極的な貢献を行う企業もあることにも注目すべきです。

このような考慮要素を踏まえて事業判断をするにあたって、（平時ではなく）リスク顕在化時においては、次項で説明する特徴にも留意する必要があります。

2. リスク顕在化時の事業判断の特徴

リスク顕在化時の事業判断の特徴としては、緊急性、流動性、不透明性、広汎性が挙げられます。紛争によりリスク状況が急速かつ継続的に変化し（緊急性、流動性）、事態の見通しを正確に把握しがたい中で（不透明性）、企業は役職員の安全、経済制裁・輸出規制、サプライチェーン、社内外のステークホルダーの意向、国内外世論の動向等、多くの考慮事項を踏まえて事業判断をしなければなりません（広汎性）。

このような事業判断を適切に行うためには、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・プロセスが望まれます。また、危機対応における実施事項、関係部門は多岐にわたるため、サイロ化した組織では機動的な対応を行うことが難しくなります。そのため経営陣、特に地政学・経済安全保障リスクを管掌するCRO（チーフ・リスク・オフィサー）やCLO（チーフ・リーガル・オフィサー）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、地政学・経済安全保障リスクが顕在化した場合、前述のとおり、事業の公益性・規模、サプライチェーン、金融・経済制裁、レピュテーション、役職員の安全等を勘案のうえ、事業継続・撤退の是非が検討されますが、収益性よりも倫理的な側面や公益的な側面がより強調されます。ただし、善悪の判断や「正義」の所在を巡っては、一般的に複数の見方があることも事実です。最終的には、自社の理念やパーパス、そして経営者の信念に沿った判断が求められますが、それが結果的に「独善的なもの」や「私益を優先したもの」にみえる事態は避けるべきです。そのためにグローバルな世論、そしてステークホルダーの声を適時・適切に経営層で共有すること、そして平時からの思考訓練が不可欠です。

なお、有事に備えた組織・体制設計のポイントはIV-1節で紹介します。

III 地政学・経済安全保障リスクの概要

前述のとおり、地政学・経済安全保障リスクの具体的な内容は多岐にわたり、各主管部門等との連携が必要です。特に、安全保障貿易規制・制裁、投資規制、情報セキュリティ、人権、役職員等の安全、サプライチェーンの視点は欠かせません（各リスク項目の内容、主管部門例は図表1を参照）。ここでは、主なリスクの概要や留意点について紹介します。

1. 安全保障貿易規制・制裁

安全保障上脅威となる国や個人・団体に対する取引規制等をするものです。代表例として、日本の外国為替及び外国貿易法（外為法）、米国輸出管理規則（EAR：Export Administration Regulations）、米国OFAC（Office of Foreign Assets Control）による規制、EU輸出管理規則、EU制裁が挙げられます。

上記の米国規制はいわゆる域外適用が問題となります。EARは米国原産品目等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が必要になる等の制限が課され、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等を要求します（違反すれば、米国企業との取引禁止等、厳しい制裁が課されます）。紛争等のリスク顕在化時には、輸出の要許可品目の拡大（電子・コンピュータ・通信・暗号等、広汎なカテゴリ）、許可方針の厳格化、Entityリスト（制限取引先）の拡大、SDNリストの拡大、直接製品規制の拡大（米国製機器・技術・ソフトを利用して製造した製品の輸出制限強化）等が行われ得ます。

EU制裁は、欧州連合条約に掲げられた共通外交・安全保障政策（CFSP：Common Foreign and Security Policy）の目標を達成するために、拘束力のある国連安全保障理事会決議を受け、または自主的に第三国政府や個人、企業等の組織、テロリスト集団等に制限措置を発動するものです。これは、EU域内で事業を行う法人、事業

体または団体に対しても適用されます。紛争等のリスク顕在化時には、制裁対象者に対する資産凍結、資金利用の禁止、EUへの渡航禁止（EU域内の移動禁止を含む）等が課され、企業においても制裁対象者への物品・技術の輸出を含む取引制限等が課され得ます。

国家間の緊張関係が高まっている場面（とりわけ、米国・欧州と他国・地域との緊張関係が高まる場面）では、安全保障貿易規制・制裁はEntityリストやSDNリスト等の各種リストの更新等が継続的かつ頻繁になされ、その主管部門やそのオペレーションを担当する事業部門の負担は大きくなります。輸出を含む取引可否に影響する重要事項であるため、平時より、その体制の充実化、オペレーションの効率化（特に該非判定・取引審査に関するSOPやスクリーニングシステムの活用等）に向けた準備をしておくことが肝要です。

また、これらの規制・制裁に加えて、紛争リスクの顕在化時には、侵攻国とその協力国の金融機関に対するSWIFT（国際銀行間通信協会＝銀行間国際送金ネットワーク）からの排除も問題となり得るため、制裁対象銀行を利用した決済が困難になること等にも留意が必要です。

2.情報セキュリティ

紛争等のリスク顕在時には、ランサムウェア等によるサイバー攻撃の脅威が高まります。実際、日本企業を含むグローバル企業が攻撃の標的となり、深刻な被害を受けるケースが見られます。一定の政治的思想・思想信条や国家機関との関係に基づいてサイバー攻撃を行うケースもあれば、単に混乱に乗じて攻撃を行うケースもあります。国家機関が関係する活動として、たとえば敵対国（とその協力国）の軍事・外交に関する機密情報の窃取や、相手国の技術開発の妨害が挙げられます。関連する技術開発を進める企業、製品・サービスを提供する企業は特に注意が必要です。

サイバー攻撃の対象には、大企業の拠点だけでなく、国内外の中小企業も含まれます。そのため、大企業においてもサプライチェーン上の企業における情報セキュリティ対策はビジネスの持続性において重要となります。特に、先端技術に関する機密情報や顧客情報の窃取を狙った事例が多数報告されています。

このようなサイバー攻撃により、機密情報等の漏えいはもちろんのこと、研究開発の停止・遅延、クライアントからの信用喪失・損害賠償、システムやデータ復旧のコストなどの影響が発生し得ます。紛争等のリスク顕在時には大規模なサイバー攻撃が発生しやすく、完全に防ぎきることは容易ではありません。そのため、ファイアウォールの設置といった予防策だけでなく、被害の発生を早期に発見し、是正対応を可能とする仕組みや報告体制を整備する等、ダメージコントロールを図ることも重要です。

なお、主に平時の管理活動に関するものですが、日本において2022年5月に成立した経済安全保障推進法（公布後2年間以内で段階的に施行）は、基幹インフラに安全保障上の脅威となりうる外国製品が導入されることを防ぐことを目的にして、指定された電気や金融、鉄道等の14業種に関して、事業者に重要設備の導入・維持管理等の委託に関する計画書を事前に届出させて、国による審査を受ける義務を課します。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等が検討され、審査の結果、妨害行為を防止するために必要な措置（重要設備の導入・維持管理等の内容の変更・中止等）を勧告・命令される場合があることから、今後、指定業種の企業においても留意する必要があります。

また、同法（経済安全保障推進法）では、軍事転用のおそれがある技術の漏えいを防ぐために、一部の特許情報を非公開とする制度も導入されます。対象発明を出願する企業は開示の禁止や、情報の適正管理等の義務が課せられることになるため、今後、知的財産部門と連携した情報セキュリティ対策が一層重要となります。

3.人権／役職員等の安全

武力行使は、最悪な形態の人権侵害行為であり、企業としても役職員（役職員のご家族、取引先・ビジネスパートナー・活動所在地の地域住民等）の生命・身体等の各種人権への侵害が懸念されるところです。国家間の緊張が高まった際、当事国でのビジネスを有する企業は、外務省・現地大使館等の公的情報、大手メディアの報道情報等に注視しつつ、役職員の退避を含む安全施策を速やかに検討・実行する必要があります。また、当事国内では、プロパガンダに反する言動への規制強化が行われうるため、情報発信の内容・方法にも注意を要します（企業としての理念・信条を堅持しつつも、役職員等の安全に配慮した対応が必要になります）。

企業の取引の観点からは、米国・EU等では、人権侵害に対して制裁対象者の渡航禁止や資産凍結を課す制裁法を策定・運用していることから（たとえば、米国のグローバル・マグニツキー人権問責法）、企業では取引関係に制裁対象者が含まれているか否かの確認等が必要となります。また、人権侵害被疑物品の貿易を制限する規制もあり（たとえば、米国の貿易円滑化・貿易執行法）、サプライチェーンにおける人権侵害被疑物品の有無の確認も重要となります。

人権侵害への対応を検討する際に重要なのは、人自体への負の影響に対する低減策を第一に重視することです（ビジネスへの影響に関する判断に優先します）。また、自社だけではなく、製造委託先等のサプライチェーン上の人々の人権への配慮を要します。平時における取引・投資、リスク顕在化時の撤退に関しては、判断を

図表1　地政学・経済安全保障リスク例

リスク項目例		リスク主管部門例	連携部門例（2線）
安全保障 貿易・制裁	□ 外為法（輸出規制） □ 米国輸出規制/OFAC規制 □ EU輸出管理規則/制裁 □ SWIFTからの排除 □ 中国輸出管理法等、各国輸出管理規制	・経済安全保障 部門（or輸出管理部門）	■ 規制面： ・法務・コンプライアンス部門 ■ 送金・決済面： ・財務部門
投資規制	□ 外為法（対内直接投資規制） □ 外国における外資規制（米国FIRRMA等）	・経営企画部門	■ 規制面： ・経済安全保障部門（or輸出管理部門） ・法務・コンプライアンス部門
情報・ セキュリティ	□ 技術情報等、営業秘密の漏えい（共同研究における情報のコンタミネーション等） □ 個人情報の漏えい □ 特許の非公開対応（秘密保持義務） □ 海外製IT機器・サーバ・クラウドの利用 □ 委託先の情報セキュリティ □ 自社への各種サイバー攻撃	・情報セキュリティ部門	■ 特許面： ・知財部門 ■ IT機器等の利用： ・総務部門
人権	□ 政情不安に伴う人権侵害 （例：不当な身体拘束、言論弾圧、プライバシー侵害） □ 人権侵害に関する制裁法 （例：米国グローバル・マグニツキー人権問責法） □ 人権侵害被疑物品の輸出入規制 （例：米国貿易円滑化・貿易執行法）	■ グループ内対応： ・人事部門 ■ サプライヤー対応： ・物流・調達部門	■ 開示等のコミュニケーション： ・経営企画・IR ・サステナビリティ部門 ■ 規制面： ・経済安全保障部門（or輸出管理部門） ・法務・コンプライアンス部門
安全	□ 有事における役職員等の安全	・リスク管理部門	■ 海外拠点対応： ・海外事業管理部門 ■ 事務・手続： ・総務部門 ・人事部門
サプライ チェーン	□ 禁輸措置等に伴う原材料の高騰 □ 有事に伴う調達先の業務停止 □ 懸念取引先との取引によるレピュテーションリスク □ サプライチェーン見直しに伴う移転価格税制	・物流・調達部門	■ 取引判断プロセス： ・経済安全保障部門（or輸出管理部門） ■ 税務面： ・税務部門

出所：KPMG作成

するにあたって、可及的に人権デューデリジェンスの結果を斟酌することが重要となります。これらは、国連のビジネスと人権に関する指導原則等からも企業に期待されるところです。そして、企業がそうした視点に欠けた対応をするとブランド毀損や不買運動につながり、結局はビジネス自体にも悪影響を与えることになります。

4. サプライチェーン

前述のとおり、安全保障貿易規制・制裁、情報セキュリティ、人権／役職員等の安全等は、いずれもサプライチェーン上のリスクの側面も持っています。また、自社や調達先における製造・販売拠点が損壊することにより、活動を停止せざるを得ない場合もあり得ますし、侵攻の当事国への社会的な非難の声を受けて、調達先等の取引先が活動を停止する場合もあります。近時は、特に世界的な半導体不足に拍車がかかる状況も看過できません（ロシアによるウクライナ軍事侵攻により、半導体製造に使われるネオン等の原料供給に影響があり、中長期的には影響が生じ得ることが指摘されています）。今後に向けて、BCP（事業継続計画）の策定や、地政学的な視点を踏まえた供給源の多角化、代替供給先の確保、製造設備への投資等の検討が欠かせません。

なお、日本では2022年3月、ロシア・ウクライナ情勢を受けて、石油・石炭・天然ガスのエネルギーや半導体等のサプライチェーン強化を目的として、経済産業省内に戦略物資・エネルギーサプライチェーン対策本部が設置され、日米を中心とした同盟国・有志国間での半導体・デジタルサプライチェーン協力枠組みや半導体原材料の供給確保等に向けた取組みが検討されています。

また、前述の経済安全保障推進法においても、重要物資の安定供給の確保に向けた施策が含まれています。今後、企業においてサプライチェーンの見直しを検討するにあたっては、国内外の経済安全保障

政策・規制の動向を踏まえることの重要性が一層高まっています（国内外のサプライチェーン・技術開発の強化政策の概要についてはⅤ節を参照のこと）。

Ⅳ 地政学・経済安全保障リスクに対する事前の備え

ここでは、地政学・経済安全保障リスクへの事前の備えに関して（個別リスク対応ではなく）、共通基盤となるリスク管理の体制面・取組み面から、施策上のポイントを紹介します。

1. 地政学・経済安全保障リスク管理体制

地政学・経済安全保障リスクにおいても、他のリスク同様に、自社に想定される各リスク（リスクカテゴリとその具体的なリスクシナリオ）、各リスクの主管部門・連携部門を整理し、リスク低減策の策定・展開についての責任を明確化することが重要です（図表1は、リスク項目、リスク主管部門、連携部門の参考例）。

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地政学・経済安全保障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）が挙げられます（図表2参照）。

統括部門の設置は、委員会の活用よりもリソース確保等の負担が大きいため、まずは委員会を活用しながら、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／重要インフラ業種等）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等です。

統括部門を設置する場合、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は、統括部門の専任者の他に、関連する主要なリスク主管部門を兼任し、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（設計例について図表3を参照）。また、経営陣、特に地政学・経済安全保障リスクを管掌するCRO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。

2. 危機シナリオ分析と対応策

平時においては、過去の紛争時における企業への影響等を参考に、自社のビジネス・サプライチェーンに対応した危機シナリオを事前に複数検討し、事業継続計画（以下、「BCP」という）の作成や危機対応マニュアル等の文書化を進め、関係部署間と認識共有をしておくことが望まれます。

危機シナリオの検討において、たとえば役職員の安全、安全保障貿易・制裁、投資規制、情報セキュリティ、サプライチェーン、役職員や委託先従業員の人権といった視点から、自社ビジネスではどのようなケース・影響があり得るのかを特定・分析し、関連する統制の有無・課題、主管部門・担当者などを整理します（検討対象のリスク項目と主管部門については図表1を参照）。

この危機シナリオの検討を踏まえて、BCPを作成するとともに、統制上の不備・脆弱性の改善に向けたアクションプランも併せて検討します。これらの危機シナリオ・BCPの策定において、特にサプライチェーンへの影響に関する検討は重要です。

紛争発生時には、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おそれがあります。そのため、地政学リスクの高い国・地域との取引に依存する原材料・部品を中心に、平時より、供給源の多角化、代替供給先の確保、製造設備への投資等の対応を具体化する必要があります。

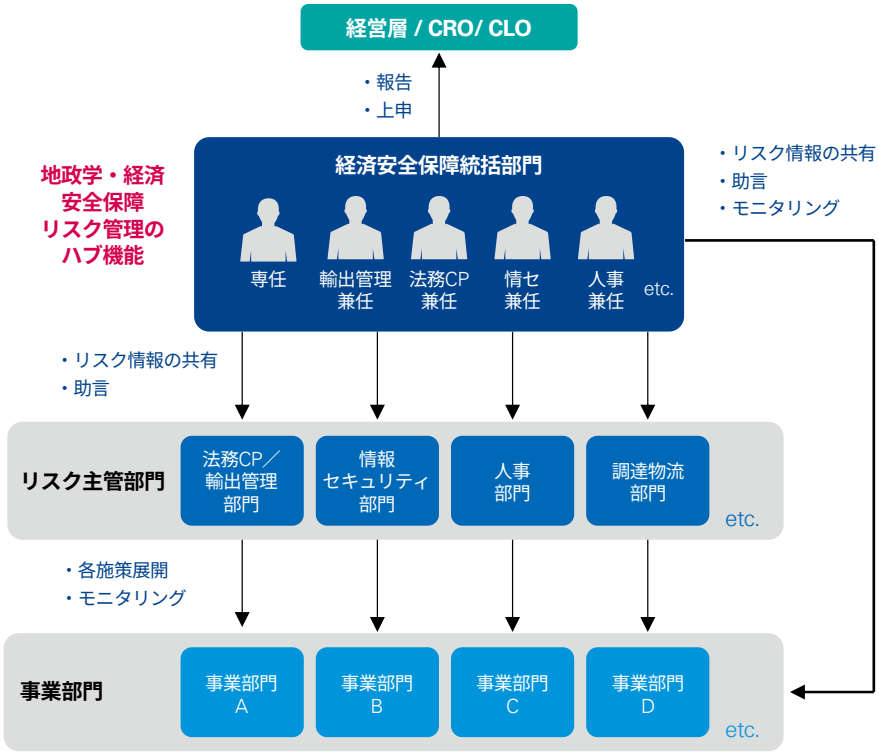
加えて、策定したBCPや危機管理マニュアルが機能し得るものかを確認することも重要です。自社にとって重要な影響のある典型的なリスクシナリオをもとに、シミュレーション訓練を実施し、マニュアル所定の対応手順どおりに行動できるか、対応の不備がないか等を関係者間で確認し、必要に応じて、マニュアルを含む文書を改訂しておくことが有効です（たとえば、サイバー攻撃関連はシミュレーション訓練に馴染みやすい）。

図表2　地政学・経済安全保障リスク管理体制の比較

視点	委員会設置型	統括部門設置型
委員会／統括部門の主な機能	情報連携	施策の策定・展開（ハブ機能）
機動性	低	高
必要リソース・負担	小	大
設置に適する企業例	右記程度に至らないものの、一定のリスク・要連携業務を有する	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／重要インフラ業種等）に属し、日常的に連携すべき業務が多い

出所：KPMG作成

図表3　経済安全保障リスク体制の設計例



出所：KPMG作成

3.インテリジェンス機能

米国等では、企業における技術情報の窃取への対策（産業スパイ対策）が進んでいますが、日本政府はセキュリティクリアランス制度（国家の機密情報を取扱う者の適格性を審査する制度）の導入検討を含め、議論の途上にあります。日本企業においても、米国企業等と同様に、技術情報の漏えい・窃取等の事例は問題とされており、その対応策の一環としてインテリジェンス機関経験者（米国で言えばFBI出身者等）と連携したリスク対応が注目されています。特に、海外拠点では調査が難しいため、インテリジェンス機関経験者等の専門家と連携した社内外の動向把握等を実施することが有効となり得ます。

Ⅴ 各国で進むサプライチェーン・技術開発の強化政策を受けて

近時、国内外において、経済安全保障の観点を踏まえたサプライチェーン・技術開発の強化に向けた政策策定に向けた動きが活発化しています。米国では、2021年6月、半導体等の重要な製品・物資や重要な産業のサプライチェーンを検証する報告書が公表され、2022年2月に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が発表されました。サプライチェーン強化のための官民協力体制の推進、同盟・友好国との協力強化等が打ち出されています。ドイツやフランス等の海外各国においても、経済安全保障の観点を踏まえて、重要物資の安定供給や重要技術の開発強化に向けた政策が策定されています。

日本においても、前述のとおり、戦略物資・エネルギーサプライチェーン対策本部の設置や、経済安全保障推進法の成立等の動きがみられます。同法では、①重要物資の安定供給の確保、②基幹インフラの安全確保、③先端技術の官民研究、④安全保障上機微な発明に関する特許の非公開に向けた取組みを促進します（②④については、Ⅲ節を参照）。

重要物資の安定供給の確保（①）に関しては、半導体など戦略的に重要性が増す物資（戦略物資）の調達を海外に依存するリスクを減らすため、国が半導体、レアアース（希土類）等の重要鉱物、蓄電池、医薬品等を「特定重要物資」に指定し、関連産業向けの財政支援を厚くします（安定供給確保支援法人等による助成等）。また、先端技術の官民研究（③）に関しては、今後、各国における開発競争が激化している先端技術（人工知能、量子等）について、官民で研究・開発する環境を整備、テーマごとの官民協議会の設置促進や、企業や大学への資金支援が行われる予定です（一方で、当該研究に従事する役職員等は守秘義務を課せられます）。

このような各国政府の政策的支援・規制を踏まえて、日本企業も地政学・経済安全保障の視点から、グローバルサプライチェーン・開発戦略の見直し、それらを支える管理体制の見直しを進めることが期待されます。

Ⅵ まとめ

ロシア・ウクライナ情勢から伝えられる非情かつ不合理な武力の行使を鑑みるに、誰もが心情的にも「正義」という言葉を強く意識をせざるを得ません。企業の社会性、社会そして世界に対する責任がますます強まる中で、日本企業は国家、そして政治に対する覚悟もまた求められています。それは決して「倫理」や「徳」にとどまることのない、まさに（国家による）「正義」と「正義」の衝突への関与でもありま

す。地政学、そして経済安全保障は「善良なグローバル企業市民」を是としてきた日本企業に対して、誰のためのビジネスなのか？　日本企業とは何か？　という踏み絵を改めて迫るものとも言えます。

今回紹介したように、企業は地政学と経済安全保障からもたらされる個々のリスクに丁寧に対応しつつも、上記のような戦略思考の変化と、それらを継続的にまわすための組織・機能作りが求められています。

関連情報

ウェブサイトでは、法務コンプライアンス関連の情報を紹介しています。

https://home.kpmg/jp/ja/home/insights/2020/12/risk-legal-compliance.html

KPMGは、日本企業の海外事業展開をこまやかに支援するため、世界の主要34ヵ国88都市に、約760名の日本人および日本語対応が可能なプロフェッショナルを配しています。

各国の最新情報については、下記をご覧ください。
海外進出支援窓口
https://home.kpmg/jp/ja/home/services/global-support.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
足立桂輔／パートナー
keisuke.adachi@jp.kpmg.com

新堀光城／シニアマネジャー
mitsushiro.niibori@jp.kpmg.com

KPMGジャパン
home.kpmg/jp

home.kpmg/jp/socialmedia