TOKIO MARINE

リスクマネジメント最前線

2021 | No.6

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

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、サイバーセキュリティ
ビジネスリスク本部 兼 経営企画部 主席研究員 柴田 慎士
専門分野：リスクマネジメント、経営管理体制、リスク計測・事業性評価。米国公認会計士（USCPA）

激化する米中間の大国間競争を背景として、近年、日本で「経済安全保障」への関心が高まっている。こうした状況下で、民間企業は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整備が期待されている。一般的な意味での経済安全保障とは「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」と理解されるが、民間企業の側からすれば、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」といえる。

経済安全保障では貿易政策、投資政策、経済制裁等が主要な領域として指摘されているが、企業の観点・経営リソースとして整理した場合、経済安全保障上のリスクが懸念される領域として、①データ、②技術、③ヒト、④資本（投資）の４つに分類・整理できる。

データ・技術・ヒト・投資等の広範な領域で経済安全保障上のリスクが高まっていることを踏まえ、企業は例えば、①監督・執行の双方での経済安全保障を考慮した意思決定態勢の確保、②経済安全保障の観点での事業リスクの評価、③経済安全保障に関する情報収集・分析態勢の構築、④経済安全保障に関する記述情報（非財務情報）の対外開示等を通じて、ガバナンス・リスクマネジメント態勢を高度化していく必要がある。

1. 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

（1）経済安全保障とは何か

近年、日本や世界各国で「経済安全保障」への関心が高まっている。日本の法制度においても、外国政府の影響を極小化するため、2019 年改正外為法（外国人投資家による対内投資規制の強化）や安全保障上の重要な土地取引の規制に関する法律が成立し、2022 年には経済安全保障一括推進法が制定される見込みである。また政府から一部の民間企業に対して、経済安全保障担当役員を設置するように要請があったと報じられた[1]。財界でも、経済安全保障に関する提言を発信し、経済安全保障に関する団体を設置する動きがある[2]。

こうした状況を踏まえて、民間企業・組織で経済安全保障を考慮したガバナンス[3]・リスクマネジメント態勢構築の期待が著しく高まっている。

今日、経済安全保障とは「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」と理解されている（図表1）。経済安全保障は自国を「守る」ための手段でもあれば、外国に対する影響力行使、「攻め」の手段としても位置付けられる。他方、企業の側からすれば、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」といえる。ここでいう戦争行為とは軍隊同士の衝突や国際法上の戦争ではなく、「超限戦」[4]に代表される、あらゆる場所で、あらゆる手段による競争を指す。

■ 図表1 メディアや専門家が用いる「経済安全保障」および類似用語の一般的な意味

用語	概要
経済安全保障 economic security	• 経済的手段によって、自らの安全保障を維持すること。 • 1980 年代の「総合安全保障」のように、従来の経済安全保障は「security for economy」という安全保障の目的の側面が強調されていたが[5]、近年では「security by economy」という安全保障の手段の側面が強調されている。
エコノミックステートクラフト economic statecraft	• 貿易政策、投資政策、経済制裁、サイバー活動、経済援助、財政・金融政策、エネルギー政策の主要な領域で、「経済をテコに地政学的国益を追求すること」[6]
地経学 geo-economics	• エコノミックステートクラフトとほぼ同義。 • 「国家が、地政学的な目的のために、経済を手段として使うこと」「地政学的な利益を経済的手段で実現しようとする政治・外交手法のこと」[7]

出典：筆者作成。

[1] 「経済安保の担当役員設置、政府が主要企業に要請へ」日本経済新聞（2021 年 5 月 3 日）。

[2] 経済同友会提言「強靭な経済安全保障の確立に向けて：地経学の時代に日本が取るべき針路とは」（2021 年 4 月）；「〈独自〉経済安保協議の新組織発足へ 経団連企業が中心」産経新聞（2021 年 7 月 2 日）。

[3] 本稿でいうガバナンスとは、企業の持続的成長・企業価値向上に資する、業務執行（経営）の適切性を担保するための監督・執行双方における仕組みのこと。

[4] 「超限戦（unrestricted warfare）」とは中国人民解放軍将校が 1999 年に発表したアイデアで、戦場・非戦場、軍事・非軍事等のあらゆる境界・限度がない戦争を指す。喬良・王湘穂（坂井臣之助監修）『超限戦：21 世紀の「新しい戦争」』（共同通信社、2001 年）。

[5] 大平正芳首相が設置し、総合安全保障の検討を行った研究グループも「経済的安全保障」に言及している。具体的な定義を明示していないものの、「経済的安全保障」を（軍事的な意味での）「狭義の安全保障」と対置させ、経済を安全保障の目的および手段として言及している。政策研究会・総合安全保障研究グループ（議長：猪木正道）「総合安全保障研究グループ報告書」（1980 年 7 月）。データベース「世界と日本」（代表：田中明彦）【https://worldjpn.grips.ac.jp/documents/texts/JPSC/19800702.O1J.html】より。

[6] 詳細は、井形彬「『経済的国策』をめぐり激化する米中競争：エコノミック・ステイトクラフト（ES）にどう対処するか」『外交』No.54（2019 年 3-4 月号）、44-47 頁。

[7] 船橋洋一『地経学とは何か』（文藝春秋、2020 年）、9 頁；加藤洋一「なぜ今、地政学、地経学なのか」、日本再建イニシアティブ『現代日本の地政学 ：13 のリスクと地経学の時代』（中央公論社、2017 年）、4 頁。

企業にとっての経済安全保障問題の難しさは、①単に法令遵守に留まらない考慮が必要とされるが、経済安全保障は多義的でその内容や期待レベルが定まらないこと、②企業に期待される考慮内容や考慮レベルは、その時々の国際情勢や地政学的環境によって大きく変わること、であろう。

（2）背景：激化する米中対立

日本や世界で経済安全保障への関心が高まっている背景は、激化する米中対立である。現在、進行している米中対立は米国前トランプ（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[8]、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。佐橋亮（東京大学）によれば、米中対立の背景には、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[9]。こうした大方針の転換を前提とすると、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。

米中対立は当然、ビジネスにも影響を与える。例えば、鈴木一人（東京大学）は最悪のシナリオの一つとして、「米中デカップリング」が極限まで進展した結果、ビジネスは 3 つの世界（グローバル市場、米国を中心とする市場、中国市場）に分化していく可能性を指摘する。食料品や衣類等に代表されるコモディティは米中対立に関係なく、引き続きグローバルな市場を維持できる可能性が高い（新疆綿等の人権問題が懸念される品目は除く）。しかし、新興技術、機微情報・データ、重要インフラ等の国家の安全保障に関わる産業・事業等は米国市場か中国市場の選択を迫られる可能性がある。ここでいう米国市場とは、その同盟国やパートナー国家（欧州、日本、台湾等）を含む[10]。

他方、民間企業を中心に「米国か、中国かの選択を迫られることは現実的でもないし、不可能ではないか」との見方も強い。つまり、民間企業が「米中の二者択一を迫られる」ような状況はあり得ず、実際の問題は米中をはじめとする各国規制下でビジネスを最大化するかどうかであり、基本的にはこれまでの延長線上ではないか、との見方である。

米中対立の見通しについては、民間企業と安全保障関連の研究者・政府当局者の認識ギャップは決して小さくない。米中対立の将来・落としどころは不確実だが、民間企業は少なくとも、国家の安全保障に影響を与えるような事業等については、「米中の二者択一を迫られる」事態を想定する必要がある。ただし、選択は 100 か 0 かではなく、法人、事業、製品・サービス（およびそのスペック）ごとに、どちらの市場でビジネスを行うかの意思決定・判断が求められるだろう。加えて、何が経済安全保障上の機微かの線引きは相当ファジーであり、線引きはあくまで現状のもので、常に変わりうる。そのため、企業の意思決定も不断に検証し、見直す必要があるだろう。

---

[8] 国際政治学者らは、米中が「ツキディデスの罠」に陥るのではないかと懸念している。「ツキディデスの罠」とは、歴史家ツキディデスによる「アテネが台頭し、スパルタがこれを恐怖視したことにより、ペロポネソス戦争は不可避となった」との分析にちなみ、覇権国の衰退と新興国の台頭により国家間均衡が崩れ、戦争に至ることを意味する。ハーバード大学のアリソン教授らは、過去 500 年間の覇権争奪をめぐる 16 のケースのうち 12 ケース（75%）は戦争を伴うものであったと指摘する。グレアム・アリソン（藤原朝子訳）『米中戦争前夜：新旧大国を衝突させる歴史の法則と回避のシナリオ』（ダイヤモンド、2017 年）。

[9] 佐橋によれば、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。

[10] 鈴木一人氏へのインタビュー（2021 年 5 月 12 日）。

2. 経済安全保障をめぐる４つの領域

経済安全保障では、貿易政策、投資政策、経済制裁、サイバー活動、経済援助、財政・金融政策、エネルギー政策の７つが主要な領域と見なされている[11]。他方、企業の観点・経営リソースとして整理した場合、経済安全保障上のリスクが懸念される領域として、①データ、②技術、③ヒト、④資本（投資）の４つに分類・整理できる。

既にこうした領域では、経済安全保障を考慮した法制度化が進んでいる。日本企業は当然、日本の法令の適用を受けるだけでなく、米国や中国で事業を展開する場合、現地の法令の影響を受ける。また外国の法令が域外適用されることもあるため、注意が必要である。

■ 図表２:経済安全保障をめぐる４つの領域（経営リソースの視点での分類）

分類	概要	顕在化した事例	関連する各国の政策・法制度
データ	外国政府等が**強制力をもって民間企業が保有するデータにアクセス**（いわゆるガバメントアクセス）し、（合法だが）不当に利用される恐れ。	• 日本のインターネット関連会社の国内データセンターに対する中国からのオペレーショナルアクセス	• 米国：対外諜報活動監視法、CLOUD 法 • 中国：国家情報法、インターネット安全法、暗号法、データセキュリティ法 • 豪州：反暗号化法 • ベトナム：サイバーセキュリティ法 • インドネシア:OEST 規制
技術	特定技術等（それらを含むモノ・サービス・ソフトウェア）の第三国移転・輸出や特定国技術の利用が、**貿易制裁・金融制裁・政府調達規制の対象**となる恐れ。	• 安全保障上の懸念がある特定企業の製品を自社製品に用いること、利用することによる政府調達・重要インフラ調達からの排除	• 米国：輸出管理改革法（ECRA）による新興技術・基盤技術の輸出規制、輸出管理規則（EAR）の対象拡大、連邦政府調達における特定の外国企業の規制 • 中国：輸出管理法、「信頼できないエンティティリスト（UEL）」
ヒト	従業員（特に、事業・リスク管理・IT 等の高次権限を持つ幹部等）が、**外国政府等にリクルーティング**され、機密情報等を漏洩する等、外国政府当局に不正に協力すること。	• 中国当局による米クラウドサービス大手・事業部門幹部、仏航空大手・IT マネージャのリクルーティング • ロシア当局による日本通信大手幹部のリクルーティング	• 米国：セキュリティクリアランス制度 • 中国：国家情報法
資本（投資）	外国人投資家が**企業の支配権・影響力**を得ることを通じて、国家安全保障に影響を及ぼすこと。マジョリティを得ずとも、取締役会への出席や機密情報へのアクセスを通じて影響を及ぼすこと。	• 中国インターネット関連会社から日本のインターネット関連会社への出資 • 米政府による、外資企業の半導体各社、アプリ開発会社の買収阻止・株式売却指示	• 日本：改正外為法 • 米国：外国投資リスク審査現代化法(FIRRMA)による対米投資委員会（CFIUS）の審査権限の強化 • 中国：外商投資法、外商投資安全審査弁法、証券法 • 英国：国家安全保障・投資法

出典：筆者作成。

[11] 井形、前掲「『経済的国策』をめぐり激化する米中競争」。

（1）データ：「ガバメントアクセス」への懸念

第一に、データ分野の経済安全保障リスクである。データは今日の経済安全保障や米中対立の最前線の一つである。背景にあるのは、（米中対立とも関係するが、基本的には別軸のテーマとして）各国政府機関が民間企業に対して、「ガバメントアクセス」や「データローカライゼーション」を要求していることである。

企業にとっては、自社が保有するデータが、外国政府によって不当にアクセスされ、諜報活動や不正競争に利用されるリスクである。重要なことは、こうしたアクセスはサイバー攻撃とは異なり、合法的に行われる点である。

通常、データをどこに置くか、すなわちクラウドサービスを含むデータセンターやサーバの物理的設置場所は、様々な要素（安価で安定的な電力、最終消費地からの物理的近接性、冷温な気候、オペレーションコスト、災害リスク等を勘案して決定される[12]。しかし、近年では、「個人データ保護[13]」「産業振興」「安全保障」を理由に、政府が国内外の企業に対して、データを保管する施設を物理的に当該国内に設置すること（データローカライゼーション）を義務付ける法制度化が進展している。

これにより、政府が民間企業の保有するデータ等に強制的にアクセスすること、すなわち「ガバメントアクセス」が可能・容易となる。もちろん、従来から司法捜査や刑事手続きの一環としてガバメントアクセスは行われてきた。しかし、近年では、情報機関が諜報活動の一環として行うガバメントアクセスが注目されている。

例えば、豪州の反暗号化法（2018 年 12 月制定）は、暗号化されたデータや通信内容に警察や情報機関がアクセスできるように通信事業者等に支援を命じるもので、裁判所の令状がなくとも、行政傍受として通信傍受を可能としている[14]。中国の国家安全法（2015 年 7 月施行）、国家情報法（2017 年 6 月施行）、インターネット安全法（網絡安全法、2017 年 6 月施行）、データセキュリティ法（2021 年 9 月施行）も同様のガバメントアクセスを可能にしている。

問題は、日本企業が日本国法律に基づく政府要請に応えることは適切と考えられるが、米国政府や中国政府のガバメントアクセスに応えることが、企業の意思決定として（日本および現地法令に照らし合せて合法だとしても）適切かどうかということである。2021 年 8 月現在の日本の地政学的環境を考慮すると、自由民主主義国家、同盟国やパートナー国家によるアクセスは経済安全保障上、「許容」され、権威主義国家やライバル国家によるアクセスは経済安全保障上、「不適切」と判断されるだろう。またデータや通信分野では、「ファイブ・アイズ（Five Eyes）[15]」＋アルファ、「クアッド（Quad）[16]」、「T12（Techno-democracy 12）[17]」等の連携が提唱され、これらの構成国の多くは「許容」されやすいかもしれない。ただし、「適切」「不適切」の線引きは曖昧で、国際情勢や地政学的環境によって流動的なものであると考えた方が良い。

---

[12] 慶應グローバルリサーチインスティート（KGRI）・客員所員の小宮山功一朗氏へのインタビュー（2021 年 4 月 30 日）。
また、公開情報から推察される Amazon Web Services、Microsoft Azure、Google Platform、Alibaba Cloud 等の所在地は以下のとおり。Global Internet Map 2021. https://global-internet-map-2021.telegeography.com/

[13] 個人データ保護の文脈では、EU 一般データ保護規則（GDPR）、米カリフォルニア州消費者プライバシー法（CCPA）、ブラジル個人情報保護法(LGPD)、タイ個人情報保護法（PDPA）、インド個人情報保護法（PDPB）等も個人データの越境移転に規制を課し、企業に対して「データローカライゼーション」を要求しているといえる。

[14]湯淺墾道（明治大学教授）「データローカライゼーション法制の現状」サイバーセキュリティ法制学会第 12 回研究会（2021 年 5 月 29 日）より抜粋。当該学会はチャタムハウスルールのため、湯淺氏本人の許諾を得て記載。

[15] ファイブ・アイズは米国、英国、カナダ、豪州、NZ のアングロサクソン系諜報機関の協力スキームを指す。伝統的にはフランス、イスラエルも協力関係にあり、近年では、ファイブ・アイズと日本、ドイツ、オランダとの政策協調が確認されている。

[16] クアッドは日本、米国、豪州、インドによる協力スキームを指す。実質的には、中国を念頭においた安全保障協力との見方がある。2012 年 12 月、第二次安倍政権発足直後、安倍首相名義で公開された「セキュリティダイヤモンド構想」の流れを汲む。

[17] T12 は日本、米国、英国、仏、独、豪、カナダ、韓国、フィンランド、スウェーデン、インド、イスラエルによるデジタル問題・サイバーセキュリティ等に関する民主主義国家の協力スキームを指す。

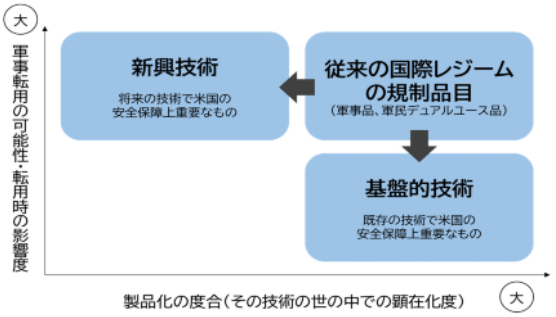
（2）技術： 特定技術等の輸出や利用に関する規制

第二に、技術分野の経済安全保障リスクである。企業にとっては、特定技術等（それを含むモノ・サービス・ソフトウェア等）の輸出・第三国移転や、特定企業の製品・技術を輸入・利用する行為が、各国の貿易制裁・金融制裁・政府調達規制の対象となるリスクである。

技術や製品の「出」の問題については、従来、安全保障貿易管理や輸出管理と呼ばれてきた。具体的には、大量破壊兵器および通常兵器そのもの、兵器開発に関するデュアルユース品を規制する国際条約・国際レジームに基づき、各国が立法化措置を講じることで、安全保障の観点から国境を超えた物資・技術の移転・取引を規制するものである。

しかし、こうした国際条約・国際レジームでは、安全保障上の機微な技術や物資を特定しても、実際に規制するまでに時間がかかる（数年を要する）こと、最先端の技術や物資等をカバーできていないことが課題として認識されてきた[18]。そのため、新たな技術の開発が国家間競争を決定付ける「ゲームチェンジャー」になりうるとの認識の下、機微度の高い技術全般の第三国移転を制限する動きもある。例えば、米国では 2018 年に輸出管理改革法（ECRA）が成立し、米国の安全保障上、重要な技術を「新興技術（emerging technologies）」「基盤的技術（foundational technologies）」とし、輸出規制の対象としている（図表 3）。「新興技術」は、現時点で実用化されていないものも含めて、これまで米商務省産業安全保障局（Bureau of Industry and Security: BIS）より複数回にわたって、例示されている。

■図表 3 従来の輸出規制品目と新興技術・基盤的技術



出典：中野雅之「米国の輸出管理の新展開」（脚注 18）、123 頁から抜粋（一部筆者修正）。

また中国政府や欧州連合も新興技術を特定・指定し、輸出管理の対象としている。米中欧に共通する新興技術として、ロボティクス・3D プリンタ、量子技術（演算、暗号、センシング）、半導体・集積回路、宇宙・航空、機械学習、ネットワーク・サイバーセキュリティ、バイオテクノロジー等があげられる。

日本国内では新興技術・基盤的技術全般の輸出管理を対象とする法制度はないものの、外国法の域外適用により、日本企業も「再輸出」「見なし輸出」として適用される場合があるので、研究・開発拠点に適用される法令や情報管理の在り方（社内ネットワークの構成やアクセス権等）に注意が必要である。

新興技術等の第三国移転とは逆の動きとして、「入」のリスクも指摘されている。具体的には、自国の政府調達や重要インフラ調達に外国政府の影響が懸念される製品・技術を規制する動きである。2018 年米国防授権法では、連邦政府調達規制において、中国の特定企業 5 社の規制（部品・製品としてのみならず、調達事業者の利用も禁止される）が決定した。

ここで問題となっているのは、特定外国企業の技術的脆弱性の有無というよりも、外国政府の「意図」であり、特定企業と外国政府の関係性である。つまり、外国政府が平時における不正競争や諜報活動、有事における破壊活動を意図して、特定企業に情報提供や不正行為を命じ、特定企業が本社所在国政府の指示に応じざるを得ないリスクである。例えば、豪州政府は 2018 年 8 月、第 5 世代移動通信システム（5G）調達について、「オーストラリアの法律に違反するような外国政府からの指示に従う可能性のあるベンダーの関与」はリスクであると発表した。

[18] 中野雅之「米国の輸出管理の新展開」、村山裕三編著『米中の経済安全保障戦略：新興技術をめぐる新たな競争』（芙蓉書房出版、2021 年）、119－121 頁。

（３）ヒト： 外国政府・情報機関のリクルーティング

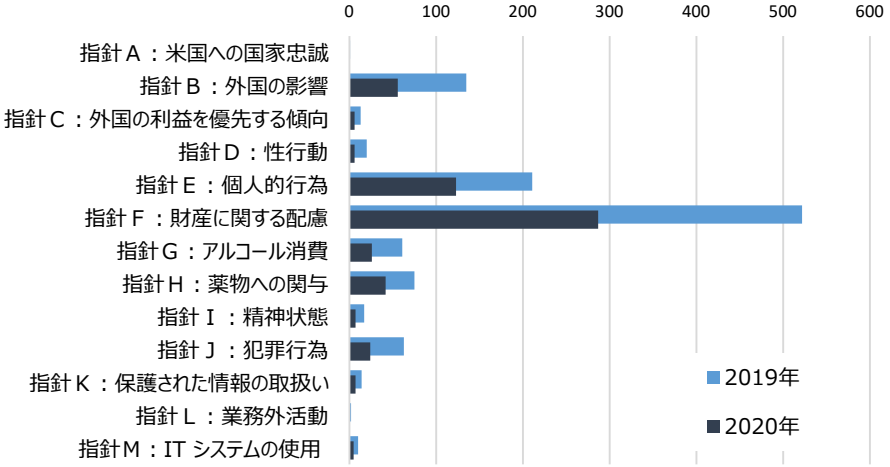
第三に、ヒトの経済安全保障リスクである。自社の役職員・関係者が外国政府・情報機関にリクルートされ、（産業）スパイとして利用される恐れである。実際、日米の司法当局の公式発表によれば、フランスの航空会社の IT マネージャ、米国のクラウドサービス大手や日本の大手通信キャリアの幹部が外国諜報機関の標的となり、これら機関の指示に従って、機密情報の提供等の不正行為に従事していることが判明している。

企業では、不正競争防止法や内部犯対策として取り組んできた分野であるが、その背景に外国政府があることに留意する必要がある。企業は全世界から多様で優秀な人財を確保しつつ、内部犯や人的諜報活動（Human Intelligence: HUMINT）の脅威から組織を守ることが必要とされる。

しかし当然ながら、多様性や競争力の確保等の観点から、国籍のみを以って採用・配置を判断することはできない。従って、企業は業務や部署の機微度に応じた機密適性要件を設定し、個々人のバックグラウンドチェック、普段の業務から機密適性を測る運用が必要とされる。

こうした考え方は、米国等では「セキュリティクリアランス」（秘密情報にアクセスするための適格性審査）[19]と呼ばれ、日本や日本企業でもセキュリティクリアランス制度を導入することが提案されている[20]。仮に日本が米国のセキュリティクリアランス制度を参照するのであれば、136 頁に及ぶ「標準フォーム 86（Standard Form 86）[21]」への記入・自己申告を基本とするものが考えられる。なお、米国における機密適性が拒否される推定要因は図表 4 のとおり、「財産に関する配慮」（一般的にいえば、多額の借金等）が最も多い。

図表 4 判断指針毎の推定される機密適性認定の拒否件数（米国）



出典：Marko Hakamaa, Top Reasons for Security Clearance Denial in 2020, *ClearanceJobs*, Jan 6, 2021.
https://news.clearancejobs.com/2021/01/06/top-reasons-for-security-clearance-denial-in-2020/
邦訳は、脚注 19 の永野「米国における科学者・技術者に対するセキュリティクリアランス」より抜粋。

---

[19] 米国のセキュリティクリアランス制度の詳細は、永野秀雄「米国における科学者・技術者に対するセキュリティクリアランス：量子情報科学を中心に（上）」『CISTEC Journal』No.192（2021 年 3 月）、148-166 頁。

[20] 例えば、与党の提言を参照。自由民主党政務調査会新国際秩序創造戦略本部「『経済安全保障戦略策定』に向けて」（2020 年 12 月 22 日）、16 頁；自由民主党政務調査会新国際秩序創造戦略本部「中間とりまとめ：『経済財政運営と改革の基本方針 2021』に向けた提言」（2021 年 5 月 27 日）、20-21 頁。ただし、実際に実効的な制度が構築・運用されるかは不明である。米国のセキュリティクリアランス制度の前提は、政権交代に伴い、民間企業の幹部が連邦政府機関に政治任用され、クリアランス取得済みの連邦政府機関幹部が民間企業に転職するというサイクル、軍や情報機関でクリアランスを取得した人物が退官後、民間企業に転職するサイクル等の存在である。

[21] これまでの学校、職場、健康・メンタルヘルス状態、借金、逮捕歴、飲酒・ドラッグ使用、交際関係等に関する質問票。U.S. Office of Personnel Management, Questionnaire for National Security Positions, Standard Form 86, Revised November 2016. https://www.opm.gov/forms/pdf_fill/sf86.pdf

（４）資本： 投資を通じた支配・影響力行使と出資規制

第四に、外国人投資家が自国企業に対する支配権・影響力を得ることを通じて、国家安全保障に影響を及ぼすリスクである。そのため、多くの国では特定の業種や企業には外資規制（事前審査制度を含む）が制定されている。

日本企業が外国企業に投資する際、当該国の外資規制に抵触すること、外国からの出資を受ける際、日本の関連規制に準拠する必要がある。

対内投資の観点で、日本では外為法が改正（2019 年 11 月成立、2020 年 6 月施行）され、外国人投資家が安全保障上重要な日本企業の株式を取得する際に必要な事前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う。日本国内の上場企業約 3,800 社のうち、約 56%（右記の区分②および③）が事前届け出を要する。

■図表 5 本邦上場会社の外為法における対内直接投資等事前届出該当性リスト

区分	社数	対全体比
区分①：指定業種以外（事後報告業種）の事業のみを営んでいる会社	1,663	43.5%
区分②：指定業種のうち、コア業種以外の事業のみを営んでいる会社	1,504	39.4%
区分③：指定業種のうち、コア業種に属する事業を営んでいる会社	655	17.1%
②+③	2,159	56.5%
合計	3,822	100.0%

出典：財務省「本邦上場会社の外為法における対内直接投資等事前届出該当性リスト」（2020 年 7 月 10 日更新）より作成。

米国では、2019 年国防授権法および外国投資リスク審査現代化法（Foreign Investment Risk Review Modernization Act: FIRRMA）により、対米投資委員会（Committee on Foreign Investment in the United States: CFIUS）の審査権限が強化された。これにより、「支配を伴わない」投資の一部も審査対象となった。

これまで、CFIUS の審査・調査に基づく大統領決定（presidential decision）による介入事例は少なくとも 6 件が確認されており、その内、3 件は半導体関連企業の買収等に関するものである。最近では、米国政府は 2019 年、ある中国のオンラインゲーム大手企業に対して、同性愛者向けのマッチングアプリを運営する米国企業の株式を売却するように指示した[22]。大統領決定に至る経緯・根拠は不明だが、中国政府当局が中国企業を通じて、性自認・性的指向に関する米国人データにアクセスし、何らかの形で悪用することが懸念されたため、と考えられる。

包括的な外資規制に加えて、業界・産業ごとの外資規制制度が存在することもある。例えば、米国通信分野では、CFIUS 以外にも、米司法省が主導する「チーム・テレコム」等が、外国資本の参入を審査・介入する権限がある[23]。

日米以外でも、中国では外商投資法・外商投資安全審査弁法・証券法、英国では国家安全保障・投資法等が存在し、各国の出資規制の概要や実施の運用状況を確認する必要がある。

[22] CFIUS の審査・調査に基づく大統領決定による介入例は、藤井麻理「米国による対中国措置の背景と動向」JETRO 米中通商問題セミナー（2019 年 7 月 23 日）より。

[23] 土屋大洋「通信網に影落とす米中対立」『日本経済新聞』（2020 年 3 月 25 日）。

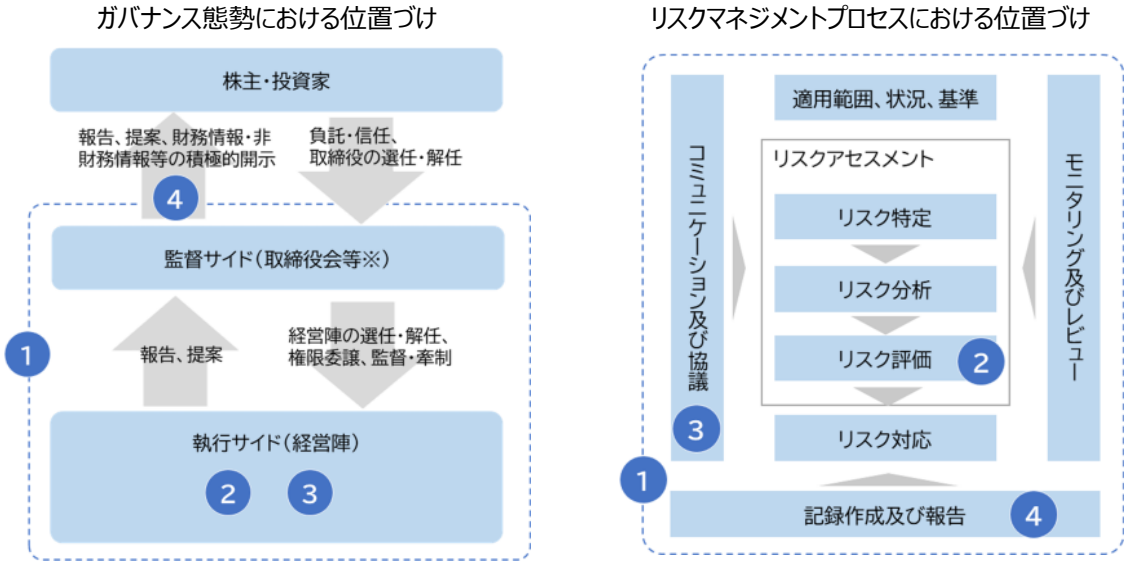
3．経済安全保障を考慮したガバナンス・リスクマネジメント態勢の構築

データ・技術・ヒト・投資等の広範な領域で経済安全保障上のリスクが高まっていることを踏まえ、企業は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整備を進める必要がある。データ管理や安全保障貿易管理等の個別の対応に加えて、全般的な態勢整備としては図表 6 で示した取組みが必要であろう。こうした取組みが、ガバナンス態勢やリスクマネジメントプロセスのどこに位置付けられるかを示したものが図表 7 である。

■ 図表 6 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を確保するための取組み（例）

分類		概要
①	監督・執行の双方での経済安全保障を考慮した意思決定態勢の整備	経済安全保障を考慮するための必要な役職・組織を設置・見直し、取締役会・経営会議等における決裁・報告プロセスに経済安全保障が考慮されるよう設計する。
②	経済安全保障の観点での事業リスクの評価	新規および既存の事業が経済安全保障上のリスクがないかを定期的に点検・評価できる態勢を確保する。
③	経済安全保障に関する情報収集・分析態勢の構築	自社の意思決定を支えるため、外部の専門家・研究者の知見を含めて、経済安全保障に関する情報を収集・評価できる態勢を確保する。
④	経済安全保障に関する記述情報（非財務情報）の対外開示	投資家やその他ステークホルダーとの間で経済安全保障に関する建設的対話を促すため、有価証券報告書を始めとする開示文書や自社ウェブサイト等で、経済安全保障に関するリスク認識・対応、意思決定プロセスにおける議論に関する記述情報（非財務情報）を拡充・開示する。

■ 図表 7 ガバナンス態勢およびリスクマネジメントプロセスにおける各取組みの位置づけ



出典：（左）筆者作成。図はコーポレート・ガバナンス・コード等から示唆されるガバナンス態勢の簡略図である。※会社の機関設計（監査役会設置会社、監査等委員設置会社、指名委員会等設置会社）および各社の裁量により、取締役会以外の組織体・会議体は異なる。
（右）ISO31000（2018）で明示されたリスクマネジメントのプロセスを基に筆者作成。

① 監督・執行の双方での経済安全保障を考慮した意思決定態勢の整備

第一に、企業は経済安全保障を考慮するための必要な役職・組織を設置・見直し、取締役会・経営会議等における決済・報告プロセスに経済安全保障が考慮されるよう設計する必要がある。どのような役職・組織が必要かは企業によって異なるが、一例は以下のとおりである。

- 監督・執行サイドにおける機関・会議体の設置
- 取締役のスキルマトリックスの一要素としての「経済安全保障」の明示
- 執行サイドにおける担当役員・専門機関の設置
- 社外取締役や外部有識者としての専門家の招聘

また、取締役会・経営会議等における決裁・報告プロセスに経済安全保障が考慮されるよう設計すべきである。

② 経済安全保障の観点での事業リスクの評価

第二に、新規および既存の事業で経済安全保障上のリスクがないかを定期的に点検・評価できる態勢を確保する。データ、技術、ヒト、投資といった分野で、現状・将来の国内外情勢を踏まえて、経済安全保障上のリスクがどの程度懸念されるのかを評価する必要がある。

③ 経済安全保障に関する情報収集・分析態勢の構築

第三に、企業の意思決定を支える経済安全保障関連の情報収集・分析の態勢・プロセスを整備することである。（経済）安全保障問題は複雑で流動的な面があり、企業・組織内部で完結することが難しく、外部の専門家・研究者の知見が必要となるだろう。また大学・シンクタンク・政府機関等であっても、1 人の専門家がこの問題を全てカバーすることは極めて困難であるため、企業・組織としては自社に必要な個別具体的な問題領域やテーマ毎の専門家を把握しておくことが現実的である。外部の知見も含めて、必要な経済安全保障関連情報を収集・分析するインテリジェンス態勢を構築する必要がある。

④ 経済安全保障に関する記述情報（非財務情報）の対外開示

第四に、企業は投資家やその他ステークホルダーとの間で経済安全保障に関する建設的対話を促すため、有価証券報告書を始めとする開示文書や自社ウェブサイト等で、経済安全保障に関するリスク認識・対応、各種機関・会議体における経済安全保障の議論の状況等に関する記述情報（非財務情報）を拡充・開示する必要がある。有価証券報告書を例にとれば、「事業の状況」中の「経営方針、経営環境及び対処すべき課題等」「事業等のリスク」、「提出会社の状況」中の「コーポレート・ガバナンスの状況等」等の箇所で記述情報を充実させるべきである。

[2021 年 8 月 23 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、サイバーセキュリティ）
ビジネスリスク本部 兼 経営企画部 主席研究員 柴田 慎士（専門分野：リスクマネジメント、経営管理体制、リスク計測・事業性評価。米国公認会計士（USCPA）

〒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