JPR&C Research&Consulting
JPR&C アナリスト・レポート
JPR&C Analyst Report
Vol. 11

2024 年 1 月 29 日

日本企業が直面する “スパイされるリスク”と“スパイにされるリスク”

はじめに

近年、国家が自らの戦略的目標を追求するために、軍事的な圧力ではなく経済的な手段によって他国に対して影響力を行使し、何らかの結果を導き出そうとする動きが顕著になってきました。こうした動きは「エコノミック・ステイトクラフト（economic statecraft／ES）と呼ばれます。米中間での貿易摩擦や技術覇権競争の激化、ロシアによるウクライナ侵攻、台湾情勢の緊迫化、イスラエル・ガザ戦争を含む中東情勢の不安定化などといった、最近の国際情勢を特徴づける各事象は、いずれも ES の要素が密接にからんでいます。戦後久しく“地政学”という言葉すらタブー視されてきた我が国においても、“地政学”と ES が結びついた“地経学（geoeconomics）”のうねりに対する現実的な対応は、政府はもちろんのこと、個々の企業にとっても、避けて通ることのできない重要課題であることは、疑いようのない事実といえるでしょう。

この“地経学”の時代にあって、各国は、自国の優位性を確保するために、機微技術の確保やサプライチェーンの強靭化といった「攻め」の動きと並行して、他国の ES がらみの動きに効果的に対応するべく、各種の規制や取り締まりなどの「守り」を強化する姿勢を強めています。このような ES をめぐる「攻め」と「守り」の体制づくりを、経済安全保障と呼ぶことができます。こうした動きを受けて、我が国でも、2022 年 4 月に経済安全保障推進法案の国会審議が始まり、同年 5 月 11 日に同法案が可決成立しました。現在、日本政府が同法運用指針の具体化を進めるなか、官民双方の立場で、経済安全保障の強化に向けた各種の取り組みが進められています。

周知のとおり、経済安全保障推進法は、以下の 4 つの柱からなります。

①サプライチェーン（供給網）の強化	**②基幹インフラの安全性・信頼性確保**
③先端技術開発支援（官民技術協力）	**④特許の非公開化**

これら 4 つの柱には経済安全保障をめぐる「守り」と「攻め」の要素の両方が盛り込まれ

ているといえますが、これらの柱に共通する前提としてすべての企業に注意喚起されていること、それは「企業の持つ“重要情報資産”の保護」です。これは裏を返せば、我が国のすべての企業が“重要情報資産”の漏洩あるいは窃取というリスクにさらされていることを意味します。

そこで本稿では、日本企業が抱える重要情報資産への最大の脅威というべき“産業スパイ”という古くて新しいリスクについて、その最新の状況と対応策についてご紹介したいと思います。

「国際化」する産業スパイ

ところで、上記でいう“地経学”あるいはESの状況が加速化した背景には、インターネットの普及、新型コロナウィルスの感染拡大がもたらした急速なDX化などを通じて、ヒト・モノ・カネが、国や地域を始めとしたあらゆる既存の枠組みから外れつつある――グローバル社会の成立が挙げられます。企業活動の国際化が急速に進み、また、今後も加速していくと考えられる昨今、“産業スパイ”も急速に国際化しつつあります。

我が国において、企業の情報資産を狙う“産業スパイ”とは、従来、国内の競合企業などが仕掛けるものとして、もっぱら国内的な問題とされておりました。しかし近年は、“地経学”的背景により、産業スパイの活動範囲も越境的になりつつあります。また、産業スパイの主体も、民間企業に留まらず、日本国外の特定国の政府の意向を受けるなど、従来の国家安全保障目的で行われたインテリジェンスオフィサー（諜報機関員）のスパイ活動との境界が不明確になってきています。もっとも日本には、いわゆる「スパイ防止法」はなく[1]、一部から「スパイ天国」との指摘を受ける状況にあります。

無防備きわまりないといえる、こうした我が国の現状には、良くも悪くも日本人の国民性、すなわち“相手を疑うことをよしとしない”、“まずは信用することから始める”、“自己主張が弱く、他者の意見に同調しやすい”といった性善説に基づく社会風土やビジネス慣習が関係しているのではないでしょうか。その結果、ひとたび悪意ある企業や個人によるから情報窃取への対応が後手に回るケースが、しばしば見受けられます。

そして、こうした日本人の国民性は、国を跨いだ産業スパイの活動に、大いに利用されて

[1] 1985年6月、「国家秘密に係るスパイ行為等の防止に関する法律案」が、議員立法として衆議院に提出されましたが、同年の臨時国会で審議未了廃案となりました。2014年12月に施行された「特定秘密の保護に関する法律」（通称：特定秘密保護法）は、我が国の安全保障に関する情報のうちとくに秘匿することが必要であるものの保護に関して必要な事項を定めたものであり、スパイ活動そのものを禁止または逮捕する法律ではありません。近年、日本国内で発生した同業者データを不正入手し、転職先で活用した事案については、不正競争防止法違反容疑での逮捕となっています。

いる面があるようです。

【参考情報】　一般的に言われる日本人の国民性

- 集団で行動することを好む。
- 統一性（皆と同じこと）を好み、人に意見を合わせる（自己主張が弱い）。
- 目立つことを嫌がる。
- 相手への配慮から、遠回しな言いまわしをすることが多い（意見の衝突を避けたい）。
- あまり感情を表に出さない。
- 比較的大人しい性格が多く、友人になるまでには時間がかかるが、懐に入ると無条件にすべてを信じてしまう。
- 何かを断る際に、理由を必要とする。
- マナーやルールを重んじる。
- 挨拶はほとんどの場合軽い会釈やお辞儀で、相手に求められた場合のみ握手を返す。
- 相手への敬意を示すために社交辞令を言うことが多い（嫌味ではなく思いやり、礼儀）。

※すべての日本人に当てはまるわけではありません。

知的財産権の重要性

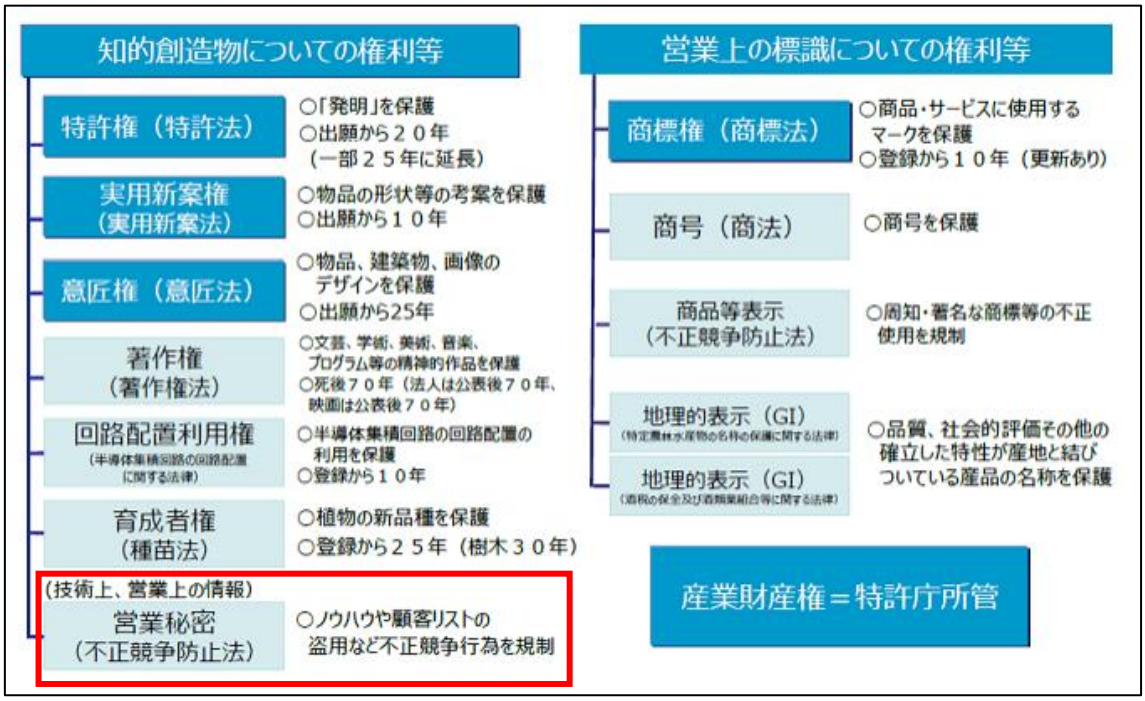
ところで我が国において、“産業スパイ”の主たるターゲットとなっているのが、いわゆる「ものづくり」（＝製造業）の現場です。近年、この業界にはソフト化の波が押し寄せており、それに伴い、知的財産が不可避的に付随し、その保護が求められるようになりました。

たとえば、2005 年 11 月に経済産業省が発表した「ものづくり国家戦略ビジョン」[2]においては、環境問題の深刻化や少子高齢化、人口減少などの内外の情勢変化に伴い、従来の規格大量生産の製造業を中心としたパラダイムが限界にきていると指摘した上で、従来の製造業に加え、デザイン・ソフトウェア・コンテンツ・サービスといったものが我が国の経済発展の肝になると指摘しています。

こうした問題意識を背景として、日本では 2000 年以降、知的財産制度が拡充されてきました。近年の産業スパイ事件でターゲットとされた情報は、工業生産に係るアイデア、技術、プロセス、製法といった知的財産に関する情報、顧客情報、価格設定、研究調査、入札予定情報、企画・マーケティング情報、製品構成や生産工場といった企業が占有している情報や運営に係る情報など多岐にわたります（下記、日本における知的財産権の種類参照）。こうした情報を不当に入手するために、対象法人のネガティブ情報が交渉材料（脅しのネタ）として狙われるケースもあるようです。

[2] https://www8.cao.go.jp/cstp/project/bunyabetu/mono/3kai/siryo2-2.pdf

【日本における知的財産権の種類】



※特許庁 HP より（https://www.jpo.go.jp/system/patent/gaiyo/seidogaiyo/chizai02.html）

企業が“スパイされる”リスク

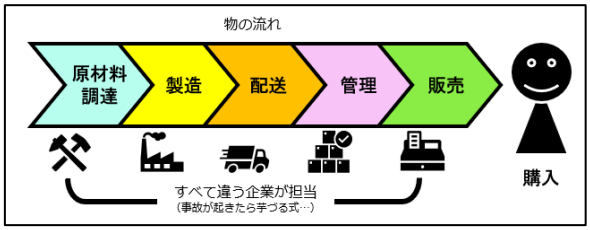
“産業スパイ”のリスクについて、本稿では、“スパイされるリスク”と“スパイにされるリスク”の二つの側面に整理して考えてみたいと思います。

まずは“スパイされるリスク”についてです。

経済安全保障推進法の第 1 の柱として、「サプライチェーン（供給網）の強化」が挙げられています。

現代社会で事業を営む企業の多くは、自社内で原材料の調達から販売まで全てを賄うことができるケースはほとんどなく、サプライチェーンを構成する複数の企業と関わりあいながら企業活動を展開しています。そのため、何かしら問題が発生した際には芋づる式に被害が拡大する可能性があり、サプライチェーン全体のリスクマネジメントが必要になってきます。

【サプライチェーン】



とくに、こうしたサプライチェーンを構成する企業の多くは、適時開示義務のある上場企業や世間の注目度が高い大手企業ではない中小企業であり、産業スパイに狙われ、インシデントが発生しても顕在化しにくい傾向があります。

そして、残念ながら下記のような考え方から、十分な対策を行わない企業経営者も少なくありません。

- **「当社には、（産業スパイが）狙うような重要情報はない」**
- 「当社には、情報セキュリティ担当がいるから大丈夫！」
- 「当社の社員や取引先に、そんなことをする人はいない」
- 「取引先は、長年お付き合いしている先しかないから大丈夫」

とくに、「(産業スパイが) 狙うような重要情報はない」との考え方は、取引先をも巻き込む最も危険なものといえるでしょう。自社情報を重要情報として認識していない企業は、情報管理が杜撰になり、守るべき情報の「秘密管理性」を失ってしまうことになります。

前述の通り、日本にはスパイ防止法がありませんが、機密情報の侵害や産地偽装、コピー販売行為などについては、「不正競争防止法」での取り締まりは可能です。ただし、同法で保護されるためには、対象の情報が“営業秘密”であると認定される必要性があり、1）秘密として管理されていること、2）役立つ情報であること、3）一般に知られていない情報であることの 3 条件を満たすことが求められます。中でも、1) 秘密として管理されていること、すなわち「秘密管理性」[3]が満たされていない場合、産業スパイの被害にあったとしても立証できず、泣き寝入りすることになるでしょう。

「そうはいっても、うちの情報が何かの役に立つとは思えないよ…」と考える向きもあるかもしれません。例えば、産業スパイの背後に特定国家の政府の存在があった場合、また、さらにその国では軍や政府と企業の距離が近かった場合、産業スパイが持ち寄ったバラバラの情報は、その国の軍や政府によって統合・分析されることになります（こうした国では、いわば国民総スパイの様相をなしているのが常であり、各個人には必ずしもスパイの自覚はないことが多いです）。こうした場合、重要情報であるか否かを決めるのは、被害を受けた企業ではなく産業スパイを仕掛ける側であるということが重要です。

一口に、セキュリティリスクといってもその具体的な内容はさまざまです。そうしたリスクを語る際、サイバー攻撃が想定されていることが多いですが、従業員や取引先関係者に直

[3] 情報管理において、▼パスワードがない（もしくはいい加減）、▼パスワードが全社員で共通（パスワードの意味をなさない）、▼秘密情報として扱っていない、といった状況は、営業秘密情報と認められません。

接、接触を図るケースも多く見受けられます。

例えば、サイバー攻撃を仕掛けて入手した取引先の顧客リストから、取引窓口となっている人物を特定し、その人物の SNS などから個人情報を集めて接触を図り、相手を信用させたところで情報を取得する、あるいは、取引先に近づき、取引先の紹介で従業員として入社し、内部から情報を抜き出すといったケースもあります。

これらのケースは、既述した日本人の国民性、「懐に入ると無条件にすべてを信じてしまう」、「人に意見を合わせる（紹介者の存在が信用のきっかけ）」といった特性も大いに関係しているといえるでしょう。

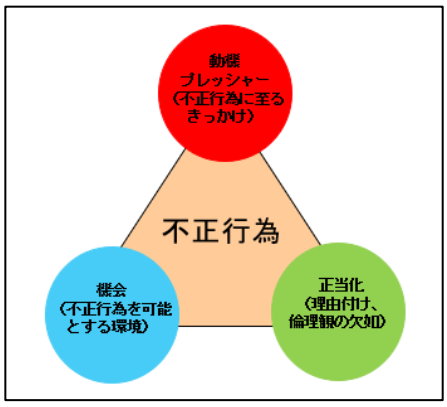
こうした産業スパイへの対策として必要なことは、主に下記 4 項目と考えられます。

1. **従業員管理に留意する。**
2. **同業他社への転職者、同業他社からの転職者に注意する。**
3. 情報管理者は必ず複数人設置する。
4. ID・パスワードの設定。セキュリティアップデートは常に最新版にする。

これら 4 項目のうち、3 と 4 は、主として情報セキュリティ分野であり、本稿の論じる射程から外れますので、詳細言及は避けたいと思います。

1.「従業員管理に留意する」

これは自社から産業スパイを生まないために必須の行動といえます。機密情報にアクセス権を持つ社員と定期的に面談等を行うこと、つまり従業員の状況把握をすることにより、経済的に不満を持つ、重要業務を一人で行っている、誰にも迷惑が掛からないといった意識を持つなど、不正行為を発生させる環境（いわゆる不正のトライアングル）を作らせないことが重要といえます。



【不正のトライアングル】

2.「同業他社への転職者、同業他社からの転職者に注意する」

これは同業他社への転職者が産業スパイにならない様に、同業他社からの転職者は自社が産業スパイを招き入れない様にすることが目的です。同業他社への転職者については前項の通りです。同業他社からの転職者は、前職のデータを持ち込んでいる可能性があり、本人に自覚がなくとも、前職企業から産業スパイとの指摘を受ける可能性があります。同業他社から疑われないための施策が必要です。

企業の社員が“スパイにされる”リスク

前項では、日本企業が“スパイされるリスク”をご紹介しました。しかしながら近時、日本企業はもう一つのリスクを負っています。それは、本人が知らないうちに“スパイにされるリスク”、すなわち「自覚なきスパイ」が発生する問題です。

産業スパイは、“営業秘密に明るく、守秘義務に関する意識が低い人”に狙いを定めています。したがって、ビジネス用 SNS に経歴や研究内容、趣味やプライベート情報を掲載している人は、とくに狙われやすいとされます。たとえば、ある対象人物にヘッドハンティングを装って接近し、接待や情報交換を重ねていく内に情報を引き出し、その人物が途中で情報漏洩に気付いたとしても、すでに引き返すことができない状況に陥っていた____、というケースも少なくありません。「口には戸を立てられない」、「知識には境界線を引くことができない」といった理由で対策が非常に難しい問題ですが、まずは営業秘密の秘密管理性を保護すること、そして保護されていることを社員に自覚させることで、ある程度は防御できるでしょう。

そして、近年、深刻度を増している事態がもう一つあります。これは事業の国際化に伴い日本国外に事業拠点を持つ企業で発生しているものです。中国は、2014 年に中華人民共和国反間諜法（以下、反スパイ法）を制定しました。同法は、反スパイ活動の強化およびスパイ行為の防止や阻止、処罰によって中国国家の安全を維持することを目的とした法律です。中国は、2023 年 7 月に同法を改正し、スパイ行為とする行動の適用範囲を拡大したほか[4]、国家安全保障機関（当局）が国民を動員しスパイ行為を阻止すること、また国民が当局に協力・支援することを制度化（義務化）[5]ました。

2023 年 10 月、日本のある製薬会社の現地法人幹部（日本人男性）が逮捕されたことは、記憶に新しいところです。2023 年 11 月時点で、中国に拘束された日本人は 17 人に上り、うち 12 人は起訴されるなどし、5 人は現在も服役もしくは拘束中です。反スパイ法で拘束された場合、容疑自体が公表されず、どういった行為が問題視されたかすらも確認できない状況であるため、政府関係者も具体的に交渉することができずにいます。

このように合理的な予見可能性も回避可能性も成り立たない状況下で、中国の日本人駐在員らは企業活動のために正確かつ詳細な情報を得ようとしても、必要と考えられる現地業界関係者や地方政府関係者へのアクセスも、それ自体が当局による拘束リスクを孕む危険極まりない状況に置かれています。

---

[4] 改正・反スパイ法では、国家機密だけでなく、国家の安全と利益に関わる文書、データ、資料、物品の窃取、偵察、買収、不法提供や、中国国家職員を唆す活動、国家機関、秘密に関わる機関若しくは重要情報インフラ等に対するサイバー攻撃、侵入、妨害、制御、破壊等の活動、敵に攻撃目標を指示すること、などもスパイ行為に該当するとされています。

[5] 外国企業の現地法人が保有する電子機器や手荷物まで、強制捜査できることも明文化されました。

当社スタッフと個人的なコネクションを持つある日本企業の現地駐在員は、改正・反スパイ法施行直前に「今後は、中国国内から日本に国際電話もできない。また、こちらへ電話することも控えて欲しい。何をスパイ行為といわれるか、誰に通報されるか分からない」との連絡を最後に、現在に至るまで音沙汰がなく、安否が案じられています。

2021 年以降、新型コロナウィルス禍による交流中断、処理水放出に対する水産物禁輸措置、改正反スパイ法の施行などの一連の流れの中で、日中関係は対中投資も含めて冷え込んでいます。そうした中、改正・反スパイ法をめぐっては、当局による恣意的運用の可能性が指摘されており、中国国内に事業拠点を置く日本企業としても、中国の対外姿勢の動向（日中のみならず米中関係を含む）の把握が必須であり、さらに世界の主要国の経済安全保障の関連法の執行状況について注視する必要があります（本稿末尾の参考情報を参照）。

むすびにかえて

本稿では、日本企業が晒されている産業スパイに関するリスクをご紹介しました。

日本は 1945 年の敗戦以降、東西冷戦を経て現在に至るまで、いわゆる国家間紛争の当事者となることはありませんでしたが、その間、国家間紛争の「作法」は着実に進化を遂げてきています。従来の正規戦（交戦資格を有する軍隊による戦い）に加えて、非正規戦（民兵によるゲリラ戦、大衆蜂起など）、サイバー戦、情報戦、心理戦、そして本稿で取り扱った ES の一環としての産業スパイなども国家レベルで体系的に展開される状況が現実化しつつあります。

とりわけ企業にとっては、自社の重要情報資産をターゲットとする産業スパイは、しかける主体に関わらず、その効果的な防御が死活的に重要となります。そうした個々の企業による、産業スパイ・リスクに対する意識の向上、またその上での効果的な防御策の徹底こそが、物理的な損害の回避につながり、またその会社の非財務的な企業価値の向上につながることはいうまでもありません。

当社は、日系インテリジェンスカンパニーとして、地政学・経済安全保障の視点を含め、国内外の公開情報や人的情報ネットワークを活用した情報収集、産業スパイ等の社内不正関連調査（行動調査含む）等、企業のみなさまのためのオーダーメイドによるリスクマネジメントのサポートおよび経営判断の一助となる各種インテリジェンスサービスをご提供しています。

（JPR&C 調査部）

参考情報

■　各国の経済安全保障関連法・規則一覧

国	関連法・規則等	要点
中国	「信頼できない実体リスト規定」（中国版エンティティ・リスト）の制定（2020.9）	中国の主権・安全・利益を脅かす外国の組織・個人をリスト化、輸出入や投資、入国などを制限・禁止する。
	「外国の法律および措置の不当な域外適用を阻止する規則」の制定（2021.1）	外国の規制関連法規定が、中国国内で適用されることを阻止する。
	「反外国制裁法」の制定（2021.6）	外国による「差別的な制裁措置」に対して、法律レベルで対抗措置を講じることが可能。
	中国サイバーセキュリティ法（2017.6）	中国がサイバーセキュリティを強化するために制定した法律。 国家安全保障のためのサイバーセキュリティ確保を目的に、対象は中国域内のネットワーク運営者、重要インフラ施設運営者、インターネットサービス提供者など、サイバーセキュリティ等級保護の実施義務、権利義務の明確化、適切なネットワーク運営方法の確立、サイバーイノベーションの奨励、セキュリティリスクの識別、コンプライアンスの遵守などを定めている。
	中国データセキュリティ法（2021.9）	データセキュリティにおけるリスクや脅威に焦点を当て、政府によるデータセキュリティの強化、データセキュリティの審査、リスク評価などを定めた法律。
	中国個人情報保護法（2021.11）	中国国内で個人情報を処理する活動に適用される法律。中国国内に拠点を持たない外国企業へも適用される。
	改正「中華人民共和国反間諜法」（2023.7）	スパイ行為を防ぎ、制止し、それに懲罰を与え、国家の安全を守る。2023.7 の改正で摘発対象が大幅に拡大された。
ロシア	大統領令「2030 年までの経済安全保障戦略」（2017.5）	ロシア連邦に対する具体的な経済安全保障上のリスクおよび脅威（25 項目）を挙げ、ロシア政府の施策（目標、課題、優先分野）がまとめられている。
日本	「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（経済安全	安全保障確保に関する経済施策を総合的かつ効果的に推進するため、安全保障確保の推進に関する基本方針を策定するととも

	保障推進法）」（2020.5）	に、経済施策として、所要の制度を創設する。
	「重要土地等調査規制法」（2021.6）	重要施設または国境離島等の機能阻害を防止するため、重要土地を指定・調査・規制する。重要施設とは、自衛隊の施設、米軍基地、海上保安庁の施設のほか、機能が失われると国民の生命、身体、財産に重大な被害が生じる恐れのある政令で指定される生活関連施設など。
アメリカ	「中国人研究者・留学生の入国規制」（2018.6～）	理工系中国人学生等に対するビザの発給を厳格化。
	「米国防権法 2019」に基づく中国企業のエンティティ・リスト掲載（2019.5～）	エンティティ・リスト（輸出規制対象リスト）に多数の中国企業等を追加し、対中輸出管理を強化。 ※エンティティ・リストには、米国の制裁に該当する活動や米国の国家安全保障・外交政策上の利益を害する活動に従事した団体や個人が掲載されており、輸出等が規制されている。
	「米国のサプライチェーンに関する大統領令」に基づく重要技術・製品のサプライチェーンからの中国排除（2021.2～）	中国企業製の情報通信機器等の調達・使用を制限。
EU	対内直接投資審査（スクリーニング）に関する規則（2020.10）	機微技術や重要インフラに係る域外からの直接投資を審査する。
	新産業戦略 「開かれた戦略的自立性」（2021.5）	輸入依存度が高く且つ調達先の多角化や域外代替が困難な品目を特定し、戦略的重要分野での連携を強化する。
	欧州半導体法の採択（2023.7）	アジア製半導体依存からの脱却、EU 域内の研究・開発・生産強化を目指す。
イギリス	「国家安全保障・投資法」（2022.1）	外国からの投資等に対し、政府が調査・介入する権限を付与。
ドイツ	改正「対外経済法」（2020.7）	EU 域外企業による投資について、通告義務の範囲を拡大。
	改正「IT セキュリティ法」（2021.5）	連邦情報セキュリティ庁の機能強化。重要インフラにおける部品が公共の安全を損なう場合、使用を禁止。
フランス	「外資規制を強化する政令」（2024.1）	戦略分野の企業を外資による買収から防衛する特例措置（事前届け出の基準となる議決権を 25％から 10％に引き下げ）を恒久化。

	改正「郵便・電子通信法典」（2019.8）	通信事業者に事前審査を義務付け。
カナダ	投資の国家安全保障審査に関するガイドライン」改定（2021.3）	外国投資による国家安全保障上のリスクが懸念される分野を指定し、同分野における外国投資を審査。
	「研究協力に関する安全保障ガイドライン」の公表（2021.7）	諜報活動などから国内の知的財産を保護。
豪州	改正「外資による取得および買収に関する法律」（2021.1）	国家安全保障上、機微な土地および事業に対する外国投資は、投資額にかかわらず政府による審査を実施。
	改正「重要インフラ安全保障法」（2021.12）	外国投資審査の範囲を従来の 4 分野から 11 分野に拡大。

※2024 年 1 月時点の情報

この原稿は 2024 年 1 月 25 日時点の情報に基づいて執筆されています。