



企業に求められる技術流出対策：「面」と「点」によるリスク管理

Fortis Intelligence Advisory 株式会社 代表 稲村悠

東京海上ディーアール株式会社 ビジネスリスク本部 主任研究員 長村勇汰*

要約

- 地政学的な緊張や先端・新興技術の開発競争が激化する中、技術流出対策は企業経営にとって不可欠の要素となっている。技術流出対策を効果的に進めるためには、経済安全保障リスクの把握という「面」の視点と、個別の技術・人物・組織に関するリスクへの対応という「点」の視点を切り離さない体系的なアプローチが必要である。
 - 「面」としてのアプローチは、地政学的対立の構造を踏まえた経済安全保障リスクの把握と対応である。各国は国家の経済安全保障上重要な技術の保護や育成を強化している。この動向を継続的に把握することは、自社技術が置かれている構造的な位置づけと流出リスクの高まりを把握し、政策変更が事業に及ぼす影響の予見可能性を高めることが可能となる。
 - 「点」としてのアプローチは、守るべき技術・情報・人材、流出経路、人物・組織リスクの把握と対応である。自社が保護すべき技術の特定、流出シナリオに基づいた、自社の対応度の詳細な把握、「予防（抑制・制御）」、「検知」、「対応」の一連の運用設計、組織・人物による自社の重要技術に対するリスク評価プロセスを確立することが実効性のある技術流出対策につながる。
- 技術流出対策に必要なのは、重要技術・重要人材・重要取引を軸に、社内外のリスク情報と対策を横断的に俯瞰し、優先順位を付けて関係部門を動かす司令塔機能である。そうした機能を、「3つの防衛線」モデルを基に、経済安全保障上の動向モニタリングから技術流出対策までを組織横断的に担う体制に組み込むことが考えられる。

目次

1. 技術流出対策における「面」と「点」の一体的アプローチの必要性	2
2. 「面」としてのアプローチ：地政学的対立を踏まえた経済安全保障リスクの把握・対応	4
3. 「点」としてのアプローチ：守るべき技術・情報・人材、人物・組織リスクの把握・対応	6
4. 企業における体制整備	10
【補記】官民連携による予防型インテリジェンスと CIBC 構想	12

* 稲村が第3章および第1章・4章の一部を、長村が第1章、第2章、第4章を執筆。

1. 技術流出対策における「面」と「点」の一体的アプローチの必要性

(1) 「面」と「点」の2つのアプローチ

地政学的な緊張や先端・新興技術の開発競争等の国家間対立が激化する中、技術流出対策は企業経営にとっても不可欠の要素となっている。各国がどのような技術を重視し、獲得を目指しているかを把握することは、自社の技術が狙われる背景や、事業に影響する政策を理解する上で重要であり、実効性のある技術流出対策には、経済安全保障という構造的な視点が欠かせない。実際、2026年7月に改訂されたコーポレート・ガバナンス・コード（CGC）でも、地政学的な環境変化に伴うサプライチェーンの途絶リスクや重要技術の流出に対応する体制整備の必要性について言及されている。技術流出対策を効果的に進めるためには、**経済安全保障リスクの把握という「面」の視点と、個別の技術・人物・組織に関するリスクへの対応という「点」の視点を切り離さずに一体的に進めるアプローチが必要**である。

「面」としてのアプローチは、地政学的対立の構造を踏まえた経済安全保障リスクの把握・対応である。一方、「点」としてのアプローチは、守るべき技術・情報・人材、流出経路、人物・組織リスクの把握・対応である。各国の政治・軍事・経済安全保障政策の動向を把握するだけでは、「自社の何が、誰が、どこで狙われているか」という具体的なリスクの特定に至らず、企業実務への落とし込みが難しい。一方、個別の技術流出リスクの把握、人物・組織デューデリジェンスだけでは、「なぜその人物・組織がリスクなのか」という地政学的な意味付けを欠いたまま判断を迫られ、過剰反応や見逃し、場当たりの対応が生じる可能性がある。そのため、企業実務における技術流出対策では、「面」と「点」を接続したアプローチの組み合わせが効果的である。

(2) 政策・技術動向に応じて変化する自社技術の重要性

各国の経済安全保障関連の規制政策や重要技術、先端・新興技術の育成・支援政策の把握を通じて、戦略的重要性を持つ自社技術を特定することが重要となる。

規制政策の観点では、技術流出、移転、アクセス等について、各国がどのような制限や管理を求めているかを把握することで、各国が保護すべきと考える技術や、懸念される流出経路・利用形態を読み取る手掛かりとなる。

また、育成・支援政策の観点では、企業にとっての支援活用を把握すると同時に、自社の技術やノウハウが経済安全保障上、どのように位置付けられるかを検討する材料となる。例えば、日・米・EUにおいて、育成・支援対象とされる重要技術、先端・新興技術は次のとおりである（図表1）。

■ 図表1 経済安全保障の観点から日・米・EUで育成・支援対象とされる重要技術、先端・新興技術の例

分類	主な技術分野
1 半導体・マイクロエレクトロニクス	EUV露光・先端微細加工、先端ロジック半導体、集積フォトニクス、高周波半導体
2 AI・先端コンピューティング	基盤モデル（LLM・マルチモーダルモデル等）、画像認識・センサーデータ融合、高性能計算（HPC）
3 通信・ネットワーク	5G高度化・6G、低軌道衛星通信、光通信、ソフトウェア無線、インフラ非依存型メッシュネットワーク
4 先端センシング・測位・航法	LiDAR、合成開口レーダー（SAR）、高感度赤外線検出、磁場・重力勾配計測、慣性航法
5 サイバー・データセキュリティ	耐量子計算機暗号（PQC）、秘密計算、分散台帳によるデータ真正性・完全性の確保
6 宇宙技術	再使用型宇宙輸送、衛星群の協調運用、地球観測システム、宇宙状況把握、軌道上組立・燃料補給

分類	主な技術分野
7 量子技術	量子計算、量子通信・量子鍵配送（QKD）、量子センシング、量子計算等を支える制御・製造技術
8 ロボット・自律システム	無人航空機・無人水上艇・無人潜水機の自律制御、複数機の協調・群制御、外骨格の動作支援制御
9 先端材料・製造	高性能複合材料・接合技術、耐熱超合金、機能性ナノ材料、金属・セラミックス積層造形
10 先進推進・エンジン	ガスタービン高温部の製造・冷却技術、エンジン統合デジタル制御、宇宙機、先進ロケット推進
11 エネルギー変換・貯蔵・電力システム	高性能蓄電池・次世代電池、水素製造・貯蔵、先進核分裂炉、核融合、次世代太陽電池
12 バイオ・医療	遺伝子・ゲノム編集、合成生物学、核酸医薬の設計・製造、生体分子シーケンシング
13 脳・ヒトインターフェース	BMI／BCI、神経信号の計測・解読、神経接続型義肢制御
14 海洋観測・海中基盤技術	海中音響・光通信、海中音源の自動識別、深海探査・作業システム、海底ケーブル
15 極超音速	極超音速滑空体の空力・飛行制御、スクラムジェット低速化、極超音速飛行用の熱防護・耐熱構造
16 指向性エネルギー	高出力レーザー、高出力マイクロ波、ビーム制御・指向技術

出典：米国の“Critical and Emerging Technologies List Update,” (February 2024); “National Security Science & Technology Strategy,” (August 2026)、EUの“Commission Recommendation on critical technology areas for the EU's economic security for further risk assessment with Member States,” (October 2023)、日本の「特定重要技術の研究開発の促進及びその成果の適切な活用に関する基本方針」（2022 年 9 月）の特定技術領域を基に、筆者が技術分野を再構成し作成。

しかし、技術の進歩や融合、新たな用途の出現によって、図表 1 のような重要技術、先端・新興技術は今後も変化していくことを前提に[企業が技術流出対策上、重視すべき技術も絶えず見直していく必要がある。](#)

また、技術の重要性が変化すれば、その技術へのアクセスを認める共同研究先や取引先、当該技術を保有・取り扱う人材についても、従来と同じ管理を続けるだけでは十分とはいえない。例えば、自社が保有する技術が新たに経済安全保障上の重要性を増した場合、共同研究や取引を通じた外部への技術移転だけでなく、研究者・技術者の転職や兼業、外部組織との人的交流等を通じた技術・ノウハウの流出リスクも相対的に高まる可能性がある。このため、[「どの技術が重要か」という評価と、「誰がその技術にアクセスし、どのような経路で外部と接点を持つか」という評価を連動させることが重要となる。](#)

つまり、自社技術の重要性や外部からの関心を評価した上で、共同研究先、取引先、人材等のリスク評価に反映することが求められる。こうした継続的な見直しによって、「面」で把握した変化を、「点」における具体的な技術流出対策につなげることが可能となる。

企業における技術流出対応では、このように「面」で地政学的対立を踏まえた政策動向を把握し、「点」で把握した守るべき技術・情報・人材、流出経路、人物・組織のリスク情報と組み合わせながら、予防・検知・対応へつなげる組織横断的な司令塔機能を持つ体制を作る必要がある。

2. 「面」としてのアプローチ：地政学的対立を踏まえた経済安全保障リスクの把握・対応

「面」としてのアプローチは、政策情報の収集にとどまらず、自社技術を取り巻く脅威と事業環境の変化を捉え、具体的な技術流出対策や経営判断につなげるものである。以下では、技術流出対策との関係から、経済安全保障政策を①重要技術、先端・新興技術の保護を目的とする政策、②先端・新興技術の育成を目的とする政策の2つに分類し、把握しておくべき主な動向を示す。

(1) 重要技術、先端・新興技術の保護を目的とする政策

□ 輸出管理

輸出管理は、安全保障上の観点から、技術・製品の輸出を国家が規制する制度であり、「安全保障貿易管理」とも呼ばれる。技術流出の観点からは、輸出された技術が想定していない主体や用途に転用されるおそれがある点が重要となる。従来、輸出管理は懸念国・組織を明示したリスト規制による管理が中心であった。しかし、第三国を経由した迂回輸出等、様々な経路で技術が流出している現状に対して、規制の対象は拡大している。具体的には、リスト掲載企業との取引の有無に加え、企業の実質的支配者、最終用途・最終需要者、第三国を経由したサプライチェーン全体の確認までを求める制度へと変化している。

例えば、米国の外国直接産品ルール（FDPR）は、米国技術・ソフトウェア等を直接利用して外国で生産された製品についても米国輸出規制（EAR）の対象とするもので、近年、運用が厳格化している。2026年6月には、ドイツの自動車部品製造大手 Bosch が、FDPR により EAR の対象となる外国製マイクロ・エレクトロ・メカニカル・システム（MEMS）センサー等を Huawei 関連企業に無許可で供給したとして課徴金が課された。さらに踏み込んだ規制としては、米商務省産業安全保障局（BIS）が2025年9月に導入した「Affiliates Rule」は、Entity List 等の掲載事業体が合計50%以上を所有する非掲載企業についても原則として同様の規制を及ぼすものである¹。これは、所有・支配関係を基準とした規制への拡大を示すものである。

□ 対内投資規制

外国企業・外国人による買収や投資を審査する対内投資審査は、外国資本が企業の所有・経営への参加を通じて機微技術、知的財産、データ、人材等にアクセスすることを防ぐ規制である。

米国の対米外国投資委員会（CFIUS）による審査はその代表例である。2026年1月には、中国の影響下にあるとされた中国系米国半導体企業 HieFo による米航空宇宙・防衛関連企業 EMCORE のリン化インジウムウエハー製造事業の取得について、トランプ米大統領が取引禁止を命じた。米政府は、EMCORE が保有する知的財産、独自のノウハウ・専門知識へのアクセスによる技術流出リスクを問題視した。

日本でも2026年6月5日に公布された改正外為法で、「対日外国投資委員会（JFIC）」が設けられ、投資審査が、個別省庁による業種審査から、より横断的な経済安全保障審査へ移行した。また、同法では、外国企業が保有する日本企業株式を別の外国企業が買収する「間接取得」が規制対象に追加され、間接取得者が外国政府等、特にリスクの高い外国投資家である場合の事前届出義務が課されるようになった。

□ 対外投資規制

最近では、対内投資規制に加えて、自国企業・投資家による海外企業への投資を規制する対外投資規制強化の動きがある。対外投資規制の目的は各国で様ではないが、例えば、米国の対外投資規制は、資金・技術が中国等の軍事力、先端・新興技術の向上に資することを防ぐことを主眼とし、該当する投資を禁止・届出対象として

¹ 同ルールは米中間の合意を受けて2025年11月10日から2026年11月9日まで1年間停止されており、2026年9月現在は適用されていない。

いる。他方、中国は第三国を経由した迂回的な技術流出への対応に焦点を当てながら、中国国内の企業、組織、居住者による海外投資規制を強化している。

□ 研究セキュリティ

外部機関との共同研究、研究者の兼業・兼職、人材交流等に伴うリスクを把握する研究セキュリティの重要性が高まっている。研究セキュリティの重要な点は、必ずしも「違法な技術移転」だけを対象としていないことである。法令上は許される共同研究であっても、将来的に戦略的重要性を持つ技術や研究者ネットワーク、研究データが懸念主体に蓄積されるリスクを事前に管理する取組みである。

日本では、内閣府が 2025 年 12 月に「研究セキュリティの確保に関する取組のための手順書」を策定し、重要技術に関係し、特に技術流出防止が必要な研究開発プログラムについて、資金配分機関がデューデリジェンスやリスク評価、フォローアップを実施する仕組みの整備を進めている。

□ 政府調達・市場流通規制

技術流出は、政府・企業が導入する通信機器やソフトウェアを通じても生じ得る。外国製の製品・ソフトウェアが国内に導入され、不正アクセスやデータの外部送信の経路となれば、研究開発情報、製造ノウハウ等が流出するおそれがある。そのため、安全保障上の懸念がある製品・サービスについて、政府調達からの排除や、輸入、販売、利用を規制する動きも強まっている。

日本でも技術流出防止の観点から国内市場でのデジタルアーキテクチャ、財・サービス等の公共調達要件への日本産業規格（JIS）等の活用による規制・認証制度の強化に向けた動きがみられる。

(2) 先端・新興技術の育成を目的とする政策

各国では、経済安全保障上の優位性や産業競争力を確保するため、先端・新興技術の研究開発支援が進められている。こうした政策で重視される技術は、経済的価値や軍事利用の可能性等から、他国にとっても獲得する意義が大きく、技術流出や意図しない技術移転への注意が必要となる。

日本では、先端的な技術のうち、特に国家・国民の安全に関わる技術として 20 領域²を「特定重要技術」として定め、「経済安全保障重要技術育成プログラム（K Program）」等による支援を行っている。また、総合的な防衛体制強化に資する重要な技術研究として 10 領域を「重要技術課題」として指定し、関係省庁の民生利用目的の研究と防衛上のニーズを結び付ける「マッチング事業」等が進められている。

また、中国では、新興産業として集積回路、航空宇宙、バイオ医薬等、未来産業として量子技術、バイオものづくり、具現化 AI 等を産業イノベーションプロジェクトとして実施していく方針を示している。

企業にとっては、こうした政策の対象分野や研究開発課題の動向を把握することが、自社の技術・ノウハウの戦略的価値と流出リスクを見極める手掛かりとなる。

² 特定重要技術領域は現行の 20 領域から 13 領域への変更が議論されている。

3. 「点」としてのアプローチ：守るべき技術・情報・人材、人物・組織リスクの把握・対応

(1) 技術流出は多面的に広がる

前節までに見たとおり、技術流出を防ぐための経済安全保障上の政策が相次いで整備・強化されている。しかし、「面」としてのアプローチで政策動向を把握し、規制に適合するのみでは、自社の技術を実際に守ることはできない。「点」として、守るべき技術・情報・人材、流出経路、人物・組織リスクを把握、自社の具体的なリスク対応につなげる必要がある。

技術流出という言葉からは、外部からのサイバー攻撃や、従業員による機密情報の持出しが想起されやすい。もちろん、これらは重大な流出経路である。

しかし、企業実務で把握すべき経路はさらに広い。公安調査庁は主要な経路として、投資・買収、不正調達、留学生・研究生の送り込み、共同研究・共同事業、人材リクルート、諜報活動、サイバー攻撃を示している。Fortis Intelligence Advisory 社（FIA 社）ではこれを企業側の管理単位に引き直し、内部不正、諜報・接触、リクルート、投資・買収、共同研究、通常取引という類型で整理している。

■ 図表 2 経済安保観点での漏洩類型

内部不正	①コミュニケーションツール、クラウド、通信関係等のIT関係、②記録媒体、撮影、紙媒体等の物理関係、③ヒトそのもの
諜報	①SNS接触、②展示会接触、③私的場面で直接接、④内部者の取り込み、⑤偽装採用
リクルート	①SNS経由、②転職エージェント経由、③競合他社の直接引抜、④退職者等の転職
投資買収	①SC経由全般、②供給元企業、③製造委託先企業、④周辺業務を担う企業、⑤技術協力関係を結んでいる下請企業
共同研究	①NDA・契約不備、②権利問題、③研究者派遣、④論文等での先行開示、⑤相手方アクセス経由で持出、⑥外国との共同研究
通常取引	工場見学、情報交換、契約締結前、サンプル交付時、契約時、契約期間中、契約期間終了後の各段階における各取引類型

出典：筆者作成。

この整理で重要なのは、外的脅威と内部不正を別々の問題として扱わないことである。国家やそれに紐づく懸念されるべき組織、競合企業等が、自社の研究者や技術者に接触し、金銭、転職機会、共同研究、講演依頼等を媒介として協力を求めた場合、最終的な持出し行為は、私用クラウドへのアップロード、メール送信、印刷、撮影、記録媒体の使用等、一般的な内部不正とほぼ同じ形をとる。すなわち、入口は外部からの働きかけであっても、出口では内部者の行為となる。諜報活動で考えると、外部からの接触を把握するカウンターインテリジェンス（防諜）から組織内のアクセス制御、ログ監視、持出し制御等の内部不正対策を接続しなければ、流出の全体像は見えない。

さらに難しいのは、合法的な活動に見える経路である。共同研究、技術提携、資本提携、取引前の情報交換、試作品の評価、工場見学等には、いずれも合理的な事業目的が存在する。そのため、違法行為を前提とした検知だけでは対応できず、相手方の実態、情報を求める理由、必要以上に広い情報要求がないか、契約後のアクセス範囲が妥当かといった文脈を評価する必要がある。

これら全てが接続され、その総体となるのが技術流出対策である。

(2) 「何を守るか」と「どう流出するか」を先に定義する

技術流出対策の出発点は、対策製品の導入ではなく、保護対象の特定である。まず、自社が保有する技術、情報、試作品、設備条件、研究データ、ソースコード、製造ノウハウ等を棚卸しする。そのうえで、市場・業界における重要性、国家戦略上の位置付け、代替可能性、流出時の事業・安全保障上の影響、第三者による再現容易性等から重要度を評価する必要がある。

保護対象は「データ」だけではない。設計図、仕様書、実験データのようにシステム上で管理できる情報に加え、紙資料、試作品、サンプル、設備設定、製造現場の掲示といった「モノ」、さらに、**製造ノウハウ、失敗知、工程理解、判断基準等を保有する「ヒト」も対象**となる。とりわけ暗黙知は、ファイルとして存在しないため、一般的な情報資産台帳から漏れやすい。重要技術を構成する情報を、データ・モノ・ヒトの三つに分解し、誰が全工程を理解しているか、誰に依存しているかまで把握することが重要である。

次に、保護対象ごとに流出シナリオを作る。「誰が狙うのか」「どのような目的を持つのか」「どの経路を使えるのか」「どの時点で情報に接触できるのか」「現在の統制はどこで機能し、どこで見逃すのか」を具体化する。例えば、共同研究先を経由した情報取得、退職予定者による大量ダウンロード、展示会で接触した人物からの継続的な勧誘、試作品の解析、再委託先からの流出等である。脅威主体の意図、能力、機会と、自社側の脆弱性を組み合わせることで、抽象的な「技術流出リスク」を、優先順位を付けられるシナリオへ変換できる。例えば、ログの取得・監視で言うと、通常のアセスメントでは、「ログは取得・監視しているか」という設問に対してほとんどの企業が Yes と答える。しかし、詳細を聞くとリアルタイムモニタリングではないため、後追いで追及はできるが、そのタイムラグは1ヵ月にも及び、持ち出し行為が検知できた時は既に流出後、という場合も非常に多い。また、そのログも断片的であり、印刷履歴やメール送付、勤務時間、入退館等が全てバラバラに検知され、統合・分析されていない場合が非常に多いのが実態だ。仮に統合・分析されていれば、予兆行為として不審行動傾向が捉えられる可能性がある。

技術流出のシナリオを描き、自社の対応度を詳細に把握した上で、**技術流出対策を「予防（抑止・制御）」、「検知」、「対応」の一連の運用として設計**する。例えば、内部不正対策では、誓約書による牽制、重要技術へのアクセス権の統制、印刷・撮影・メール・クラウドの制御、ログの統合分析、退職・異動等の変化点におけるレビュー、相談窓口、退職手続きの厳格化、退職申請時の持ち出し牽制（注意喚起）、証跡保全手順を接続する。

シナリオの妥当性は、机上で作成して終わりにせず、関係部門を交えた机上演習（TTX）等でも検証することが望ましい。実際の持出しや不審接触を想定し、どの部署が最初に兆候を認知するか、誰がアクセスを止めるか、本人への確認前に何を保全するか、どの段階で法務・経営・当局へエスカレーションするかを確認すると、規程上は存在していても実際には機能しない統制が明らかになる。全社員・全取引を一律に厳格化すれば、研究開発や営業活動を阻害する。重要度と流出シナリオに基づき、対象を絞って管理強度を上げるリスクベースの発想が不可欠である。

(3) 懸念される組織や合法的な接点を管理する「入口統制」としての DD

技術流出の経路が、諜報活動等の旧来の経路に加え、採用、共同研究、取引、投資等に広がるほど、相手方との関係開始前のデューデリジェンス（DD）が重要になる。いわゆる、「入り口」のデューデリジェンスだ。

ここでいうデューデリジェンスとは、相手方の財務健全性や法令違反歴を確認する従来型の調査にとどまらず、その組織・人物が、どのような資本、取引、研究、人的ネットワークの中に位置し、自社の重要技術へのアクセスによってどのようなリスクが生じ得るかを評価するプロセスである。

もっとも、あらゆる取引先・全社員を同じ深度で調査することは、コスト面でも、個人情報・労務管理の面でも現実的ではない。そこで、①相手に接触させる技術・情報の重要度、②付与するアクセス権限、③共同研究・製造委託・再委託等の関係類型、④相手方の所在国・活動地域や事業特性、⑤取引金額や関係期間、⑥外部との接点を持つ職務か、といった条件から対象と調査スコープを決める。採用内定前、共同研究・資本提携の審査時、重要情

報へのアクセス付与前、契約範囲の拡張時等を、明確な**実施トリガーとして業務フローに組み込むことが重要**である。

組織に対するデューデリジェンスでは、直接の契約当事者だけでなく、実質的な所有・支配関係、資金流入、役員・重要人物の兼任先、関連会社、再委託先、主要取引先、共同研究先、政府・軍・懸念組織との関係、制裁・輸出管理上の指定等を確認する。形式上は独立した民間企業であっても、役員、株主、資金、取引等を辿ると、別の組織や国家アクターとの接点が現れる場合がある。このため、対象企業を縦に深掘りする調査と、判明した人物・法人・研究機関を横に展開するネットワーク調査の双方が必要となる。特に、「ヒトの繋がり」はデューデリジェンス上非常に重要な示唆を持つ。

人的デューデリジェンスでは、経歴の整合性、過去・現在の所属、役職・兼業、共同研究者、論文・特許、関係法人、懸念組織との直接・間接の接点、公知の訴訟・不芳情報等を確認する。また、制裁リストやエンティティ・リストとの照合だけで、調査を完結させてはならない。公的リストは重要な起点であるが、指定前の組織、フロント企業、複雑な出資構造、間接的な人的接点等を十分に捕捉できない場合がある。

一方で、国籍や出身地といった属性そのものをリスクとみなしてはならない。また、単なる接点の存在をもって直ちに高リスクと判定することも適切ではない。接点が生じた時期、役割、目的、情報アクセス、相手方の行動、反証情報を含めて文脈を評価する必要がある。調査報告では、確認できた事実、合理的な分析・推論、未確認情報を明確に分け、出所、確認日、確度、残存する不確実性を示すことが、意思決定の質と対象者の公平性を担保する。

また、公開情報で懸念が見つからなかったことは、安全性が証明されたことを意味しない。情報が存在しないのか、公開されていないのか、同定が不十分なのかを区別し、調査の限界を明示する必要がある。リスクを「ある／ない」の二値で断定するのではなく、リスクの所在、判断の根拠、残る不確実性、推奨される管理措置を一体として提示することが重要である。

(4) 一度きりの審査から、継続的な変化点検知へ

入口で十分なデューデリジェンスを行っても、その時点の安全性が将来まで保証されるわけではない。企業の株主・役員・資金源・関連会社は変わり得る。共同研究では研究範囲、参加者、再委託先、成果公表の条件が変わる。人材についても、異動、昇進、兼業、プロジェクト変更、外部接触、退職申出等によって、保有知見やアクセス権、外部への露出が変化する。したがって、デューデリジェンスは、契約締結時や採用時だけの点検ではなく、**関係の重要度に応じた定期確認と、一定のイベントを契機とする再評価を含むべき**である。

人的リスクについては、採用時に候補者の経歴や接点を確認した後、在籍中は公開情報の差分、懸念組織・人物との新たな接点、役割・アクセス権の変更等を、適法かつ目的限定的な範囲で点検する。在籍社員では、特に人事イベントや重要技術を取り扱うプロジェクトへの従事等はイベントトリガーとして有効な機会となる。

また、取引先・共同研究先については、支配権変更、新規出資、役員交代、再委託先の追加、研究テーマの拡張、制裁・規制環境の変化等をトリガーとする。変化を検知したら、自社への影響を評価し、アクセス制限、モニタリング強化、契約条件の見直し、追加調査、関係停止等の早期手当てにつなげる。

この継続的な運用は、誰かが将来不正を行うと予測するものではない。接近、教唆、情報取得、持出しに至る兆候を、自社の重要技術・重要人材・外部接点と照合し、流出前に統制を変えるためのものである。デューデリジェンスは、相手方の「安全証明」でも、社内統制の代替でもない。入口と変化点でリスクを可視化し、どの統制をどの強度で適用するかを決める基盤である。

(5) デューデリジェンスで社員を守る

デューデリジェンスは、取引や採用の可否を判断するだけでなく、外部からの接触にさらされる社員を守る手段にもなる。例えば展示会では、名刺交換等で取得した来場者情報を集約し、所属・役職・関係組織・公知の懸念情報

を確認する。レッドフラグが認められた場合も、直ちに不正主体と断定するのではなく、当該社員に対し、追加面談や私的連絡、過度に具体的な技術質問、資料・サンプル要求があった場合の報告先と、開示可能な情報の範囲を個別に注意喚起する。社員個人に相手の見極めを委ねず、組織として接触後の警戒行動を支援する点が重要である。

対象は名刺交換者に限らない。自社が出展・登壇する展示会・学会の主催者、共催者、登壇者、主要参加組織、自社社員が外部カンファレンスへ参加する場合の主催・登壇者等も、テーマや重要技術・人材との接点に応じて事前又は事後に確認する。事前 DD は参加前ブリーフィングと情報開示範囲の設定に、事後 DD はその後のメール、面談、共同研究・講演依頼等への注意喚起に用いる。全件を同一深度で調査せず、重要技術を扱う部門・イベントを重点対象とし、その他は定期スクリーニングや接触トリガーで補完する。さらに、官側が把握する接触手口や類似事案と接続できれば、注意喚起の精度は高まる。このような積極的セキュリティにより、自社社員を保護するのである。

4. 企業における体制整備

求められる横断型対応と俯瞰力

企業における技術流出対応では、「面」で地政学的対立を踏まえた政策動向を把握し、「点」で把握した守るべき技術・情報・人材、流出経路、人物・組織のリスク情報と組み合わせながら、予防・検知・対応へつなげる必要がある。ただし、技術流出対応において把握しなければいけない情報や関係部門との調整は容易ではない。

実際、本稿で中心的に扱ったリスクは、人的・組織的デューデリジェンスのみで把握できるとは限らない。施設への物理的侵入に備える物理セキュリティ、サプライチェーン・マネジメント（SCM）上の脆弱性、納入される IT 機器・設備を介した侵害等、その手法と入口は多岐にわたる。

また、対策を担う部門も、総務、情報システム、調達・購買、人事・法務、R&D、営業、製造等に分散する。個々の部門が所掌範囲だけを見ていては、散在する小さな兆候を一つの技術流出シナリオとして結び付けることは難しい。

そこで必要となるのが、重要技術・重要人材・重要取引を軸に、社内外のリスク情報と対策を横断的に俯瞰し、優先順位を付けて関係部門を動かす司令塔機能である。経済安全保障室等の横断組織を設ける企業が増えてきた背景の一つも、この俯瞰・統合能力の確保にある。

具体的には、企業に期待されるリスク管理体制として、一般的に設計されることが多い「3つの防衛線（3 lines of defense）」モデルを基に経済安全保障上の動向モニタリングから技術流出対策までを担う、組織横断的な体制を構築することが考えられる（図表 3）。

■ 図表 3 「3つの防衛線」モデルでの技術流出対策

	第1線	第2線	第2.5線	第3線
部門	事業部門、生産部門 ・研究開発部門	リスク主管部門 人事部門、IT・サイバーセキュリティ部門、 海外事業部等	リスク管理統括部門／ 経済安保専任部門	内部監査部門
役割	現場でのリスク把握・対策の実行	専門的見地からの評価	リスク全体の統括	独立した検証
具体的な役割	- 重要技術・重要人材の把握 - 外部との接点把握 - 対策の実施	- 重要技術・重要人材の重要度評価 - 人的・組織的DDの実施 - 専門分野別の審査・調査	- 経済安保リスク把握 - 自社への影響評価・共有 - 対策の優先順位の決定	- リスク管理体制の検証 - 対策の実施状況の監査

第2.5線が司令塔となり社内外情報を統合し、横断的対策を実施

出典：筆者作成。

「第1線」：事業・生産・研究開発部門。自部門の保護すべき技術・人材等を「データ・モノ・ヒト」の観点で把握・重要度評価、外部との接点を把握、不審なアクセス・接触・勧誘等を認知した際の「第2線」「第2.5線」への情報共有。

「第2線」：リスクの主管部門（人事・IT・サイバーセキュリティ・海外事業部門等）。人物・組織 DD の実施（第1線が行う場合もある）、専門分野別の審査・調査、アクセス権限・ログ監視等の具体的対策の実施。

「第 2.5 線」：経済安全保障室やリスクマネジメント統括部門。司令塔機能を担う。経済安全保障リスクの把握および自社の保護すべき技術・人材等への影響評価、評価結果の共有、「第 1 線」「第 2 線」が保有する情報の統合、対策の優先順位付け、対策方針の調整。

「第 3 線」：内部監査部門。リスク管理体制が機能しているかの検証、個別の対策の実施状況、現場の兆候が統括部門へ共有されているか等を独立した立場で検証する。

司令塔機能を機能させるには、以下 3 点を実装することが望ましい。

- ① 重要技術・重要人材・重要取引の情報を横断的・一元的に管理する共通フォーマットを整備し、部門ごとに異なる粒度で保持される兆候・DD 結果等を同一の単位で統合する。
- ② 政策変更、相手方の支配権変更、研究範囲・アクセス権の変更、不審接触の発生等をトリガーとして、事象の重大度に応じた判断権限（第 2.5 線が単独で判断できる範囲、経営層の承認を要する範囲等）、対応期限をあらかじめ定める。
- ③ 突発的な事象への対応にとどまらず、第 1 線・第 2 線からの情報を定例的に吸い上げ、「面」の変化が自社のどの重要技術・取引に影響するかを突き合わせる統合レビューの場を設ける。

こうした体制により、「面」での変化を「点」の確認へ、「点」での兆候を全社的なリスク評価へと双方向に反映できる。企業単独では判断が難しい場合には、共有する情報の範囲を整理した上で、関係当局や外部専門家の知見も活用しながら、経営層の監督の下、「面」と「点」での把握、対策の実行、モニタリングを継続することで技術流出リスク対応の実効性を高めることが可能となる。

【補記】官民連携による予防型インテリジェンスと CIBC 構想

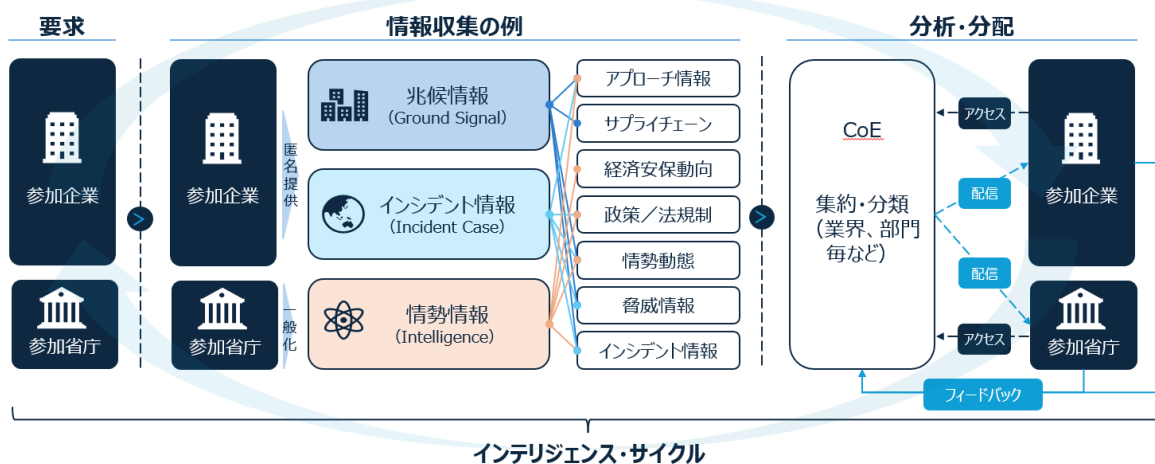
もともと、企業が自社の重要技術、人材、取引先、共同研究先を把握し、デューデリジェンスと内部統制を整備しても、企業単独で得られる情報には限界がある。警察等の官側は、脅威主体、接触手口、活動傾向といった秘匿性の高い知識や具体兆候を把握し得る。一方、企業側は、重要技術・重要人材、ヒヤリハット事案等、官側からは見えない現場で観測された“生”情報を持つ。技術流出を予防するには、双方の情報を接続し、企業が自社内で照合し、対策に変換する必要がある。これこそが「予防型インテリジェンス」であり、誰が不正を行うかを予測するものではなく、企業統制を最適化させる基盤となる。

ただし、官民連携を単なる「情報提供の要請」として設計しても機能しにくい。企業が具体的な自社情報を出しても、官側から返る情報が一般論に見えるという情報の非対称性、情報公開、取引先への説明、再発防止策の検討等のリスクを主に企業が負うというリスク負担の非対称性、官側の助言が抽象的なものにとどまり、企業のアクセス制御やログ監視等の具体的措置に落とし込むことが困難であるという実装可能性の非対称性があるからである。企業が早期に官側と連携するためには、提供情報の取扱範囲、匿名化の可否、事件対応へ移行する条件、企業へ還流される示唆をあらかじめ明確にする必要がある。

この接続基盤として筆者（稲村悠）が構想しているのが、官民連携の防諜コンソーシアム（Counter Intelligence Bureau Consortium : CIBC）である。CIBC は、各企業の内部に埋没している不審接触、共同研究上の違和感、過去のインシデント等の「埋没した経験値・情報資産」を、匿名化した上で共有する相互防衛の仕組みである。

■ 図表 4 官民連携コンソーシアム：「CIBC」構想

CIBCは、企業内部に眠る「埋没した情報」を、経済安全保障の盾に変える仕組みである。官民連携および企業同士の相互防衛モデルを構築し、インテリジェンス・コミュニティの形成を図る。



出典：筆者作成。

参加企業から寄せられた兆候や事例を匿名化・分類し、業界別の脅威傾向、共通手口、相談基準等、実務上の対策へ変換する。さらに、分科会等で課題を検討し、得られた知見を再び共有基盤へ戻すことで、単なる情報交換にとどまらない民間カウンターインテリジェンス・コミュニティを形成する。

そして、官側との情報共有の場を CIBC で持ち、相互の情報関心に基づく“生の情報”を生きた状態で共有するのである。

CIBC が担うべき役割は、**企業の現場から得られる兆候を集約し、官側の警告や政策動向を企業実務へ翻訳し、情報を「行動」に変えること**である。警察が企業に脅威を教えるだけでも、企業が警察に情報を出すだけでも、技

術流出は止まらない。必要なのは、官側が持つ脅威情報・具体兆候と企業の現場を接続し、予防型インテリジェンスを共同生成する官民連携サイクルなのである。

<略歴>

稲村悠：Fortis Intelligence Advisory 株式会社代表。1984 年生まれ。東京都出身。大卒後、警視庁に入庁。刑事課勤務を経て公安部捜査官として諜報活動の捜査や情報収集に従事した経験を持つ。警視庁退職後は、不正調査業界で活躍後、大手コンサルティングファームにて経済安全保障・地政学リスク対応に従事した。その後、Fortis Intelligence Advisory 株式会社を設立。経済安全保障対応や技術情報管理、企業におけるインテリジェンス機能構築等のアドバイザーを行う。

著書に『謀略の技術』（中央公論新社）、『企業インテリジェンス』（講談社）ほか

Fortis Intelligence Advisory 株式会社：官民双方の経験を持つ専門家で構成されたインテリジェンス・セキュリティファーム。内部不正から外部脅威のフィジカル／オンラインでのアプローチを検知、適切な対応を導くカウンターインテリジェンス（対諜報）・ソリューション「CISENTRA」、非サイバー領域のカウンターインテリジェンスに関する脅威インテリジェンスを提供する「CISENTRA-Intelligence Watch」、採用・共同研究・新規取引等の文脈で人的・企業リスクを検知する DD ツール「Signal DD」、技術流出対策の戦略立案・実装まで支援するコンサルティングを提供。

長村勇汰：東京海上ディーアール株式会社 ビジネスリスク本部 主任研究員。外務省入省後、在外公館において情報収集、分析、邦人保護等に従事したのち、2024 年東京海上ディーアール入社。現在は、官公庁・民間向けの災害・政変リスクの評価・洗い出し、リスクマネジメント態勢構築、経済安全保障インテリジェンス等のソリューションを提供。主な執筆に「米国・イスラエルによるイラン攻撃」（海外リスクセンサー、2026 年 3 月）、「2026 年のグローバルリスク」（リスクマネジメント最前線、2026 年 1 月）、「セキュリティ・クリアランス制度の民間適用拡大と企業に求められる対応」（リスクマネジメント最前線、2025 年 3 月）、「偽情報拡散の影響と企業に求められる対策」（海外リスクセンサー、2024 年 9 月）ほか

[2026 年 10 月 9 日発行]



〒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 ウェストタワー23F
Tel. 03-5288-6594 Fax. 03-5288-6626 <https://www.tokio-dr.jp/>