



企業における カウンターインテリジェンス

～諜報活動への防御と官民連携のあり方～

Fortis Intelligence Advisory 株式会社

株式会社エルテス

はじめに

国際的な技術競争や安全保障環境の変化を背景に、企業・研究機関等が保有する重要技術や営業秘密の保護は、競争力の維持にとどまらず、経済安全保障上の重要な課題となっている。技術情報が国外に流出する事件も相次いでおり、企業・研究機関にとって、技術流出は抽象的な懸念ではなく、現実にも備えるべきリスクである¹。

この技術流出の経路は、サイバー攻撃に限られない。経済安全保障の文脈で言えば、共同研究、技術提携、採用、通常取引など、日常の経済・学術活動を通じた技術流出に加え、国家アクターによる従業員や研究者への接近・働きかけといった伝統的な諜報活動が想定される。特に、諜報活動による技術流出は、これまで我が国で多くの被害を生み出し、依然として事件が相次ぎ、企業における対応が大きく出遅れている状況であり、諜報活動までも含む技術流出対策が強く要求される。

その諜報活動への対抗となる活動が防諜、すなわちカウンターインテリジェンスである。企業においては防諜については馴染みがないかもしれないが、諜報活動を含む技術流出における被害を未然に防ぐために、各種対策におけるカウンターインテリジェンスの視点が求められる。

本資料は、国家アクターが企業・組織へ向けて行う諜報活動に対して、「自助・共助・公助」の観点で、企業自身の対策から官民連携のあり方までを論じる。

要旨

企業・組織のカウンターインテリジェンスは、外部からの働きかけと組織内部の行為を一体として捉え、被害が生じる前に対処する必要がある。本稿は、諜報の歴史、現代の手口と事例を踏まえ、次の3層から実務上の枠組みを示す。

- ・**自助** 守るべき技術・人材と、脅威インテリジェンスから想定される相手・手法・関与経路を把握し、対策の重点を定める。予防・検知・対応の各施策を機能させ、連携させる。
- ・**共助** 各企業に埋没する不審な接触等の兆候、インシデント情報を、共有範囲と確度を管理しながら持ち寄る。個社だけでは不足する情報を統合・分析し、対策を見直すためのインテリジェンスに昇華させる。
- ・**公助** 官側が持つ脅威情報と企業・研究機関の現場情報を連携させ、具体的な対応につながる予防型インテリジェンスを共同で形成する。

¹ 警察庁「技術流出の防止に向けて」及び「令和6年版警察白書」より



全体の章構成

第 1 章 諜報の歴史	5
歴史を通じて変わらない諜報の本質	5
諜報の標的の変遷	6
日本の防諜の歴史的経緯	6
第 2 章 現代の諜報とトレンド	7
現代の諜報活動の主体と目的	7
接触手段の変化	7
主要な手口の整理	8
特に注目すべきトレンド	9
第 3 章 世界と日本の最新事例	10
海外の事例	10
日本の事例	10
事件から見える共通点	11
第 4 章 カウンターインテリジェンスのあり方	12
カウンターインテリジェンスとは何か	12
防御と攻撃（4つの CI 機能）	12
企業における CI の範囲	13
第 5 章 企業 CI の設計（自助）	14
企業におけるカウンターインテリジェンスの実装	14
保護対象の特定	14
非サイバー領域の脅威インテリジェンス	14
脅威分析の要点	15
脅威分析の運用	15
統制の全体像と要点	15
兆候の検知	16
対象者の属性分析	17
ソ連情報機関「KGB」の着目点	18
「MICE」と「MICELDS」による動機の分析	18
中国諜報における動機分析「BEWARE」	19
動機を生み出す外部接触	19
第 6 章 内部脅威検知の実装と防護の実装（自助）	20
カウンターインテリジェンスに基づく内部脅威の分析手法	20
内部脅威分析を構成する 3つの要素	20
要素の掛け合わせ（相関分析）とリスクスコアリング	21
内部者への働きかけと、行動変化による検知の限界	22
リスク・デューデリジェンスと継続的運用	22
オンラインへの対策	22



部門横断機能の重要性	23
運用の前提	23
第7章 予防型インテリジェンス（共助と公助）	24
官民連携のあり方	24
官民連携における3つの非対称性	24
企業間における共助	24
公助のあり方	25
官民連携インテリジェンス・サイクル	25
【特別寄稿】官民連携による防諜体制の構築に向けての提言	26
FBIによる検挙事例	26
官民連携の取組：米国と日本	27
米国の官民連携	27
日本の官民連携	28
提言	28
専門人材の確保	28
警察からの情報提供	29
第8章 おわりに	31
執筆者の紹介	32

本文書の利用はすべて自己責任でお願いいたします。

本文書の記述を利用した結果生じる、いかなる損失についても、Fortis Intelligence Advisory 株式会社および株式会社エルテスは責任を負いかねます。

本文書内の内容を転載いただく際には、出典元を必ず明記してください。

（例 出典：Fortis Intelligence Advisory 株式会社および株式会社エルテス共著【企業におけるカウンターインテリジェンス】）

また、本文書に関するお問い合わせはこちらまでお願いします。

- ・ Fortis Intelligence Advisory 株式会社 info@fortisintel.com
- ・ 株式会社エルテス マーケティング部 marketing@eltes.co.jp

第1章 諜報の歴史

上田 篤盛

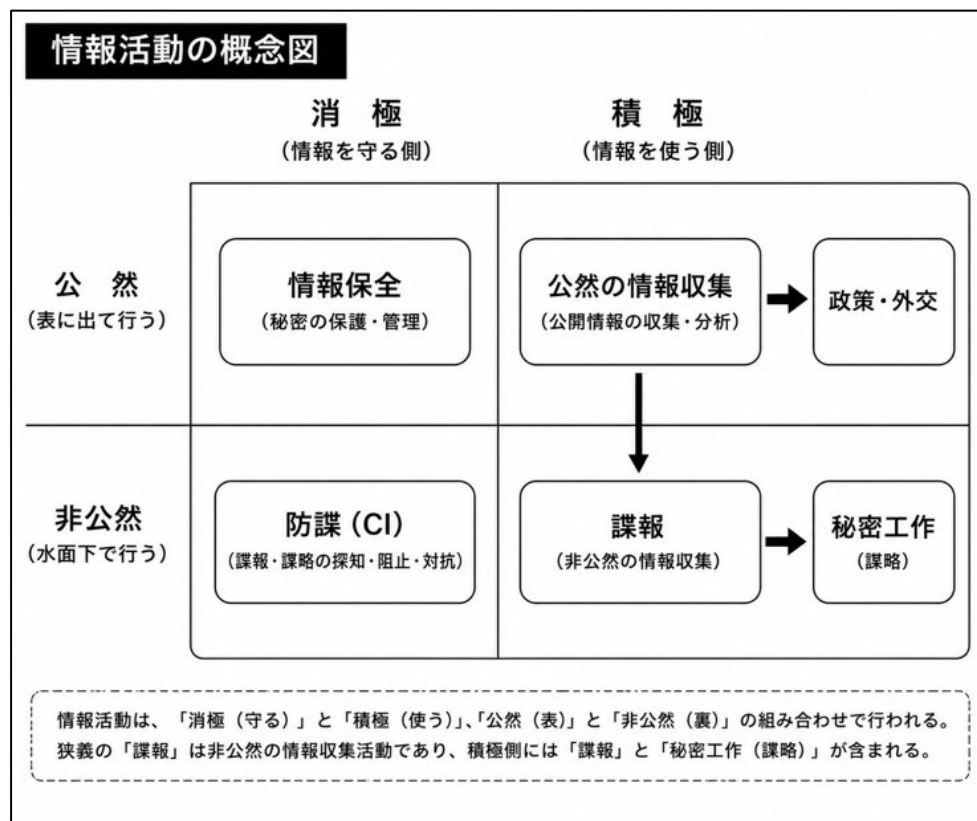
歴史を通じて変わらない諜報の本質

スパイは歴史上、第2番目に古い職業であるといわれている。その起源は紀元前13世紀の『旧約聖書』の「ラハブの物語」に由来する。紀元前5世紀には中国の『孫子』がスパイ（間）の運用を体系化した²。そんな古代の話を持ち出すまでもなく、自らの生存や利益のために相手を知ろうとすることは人間の本質であり、諜報は歴史が誕生して以来、必要不可欠とされてきた。

諜報は情報活動の1つである。情報活動は大きく「積極的な活動」と「消極的な活動」に分けられる（図表1参照）。積極的活動には、情報を収集・分析してインテリジェンスを作成し、政策や外交などに利用する活動と、相手に働きかける秘密工作（謀略）がある。一方、消極的な活動には、自らの情報を守る情報保全と、相手の諜報・謀略に対抗する防諜がある³。

情報収集には、報道、統計、研究成果などの公開情報を収集する公然活動と、相手が秘密にしている情報を秘密裏に入手する非公然活動がある。後者が狭義の「諜報（Espionage）」である。

「諜報」という言葉からはスパイ活動を連想しがちであるが、日本の旧軍では、目的を秘匿して行う情報収集活動を意味し、スパイに限定されない。また実際には、諜報による情報収集と、相手に働きかける謀略は密接に結びついてきた⁴。



² 孫武『孫子』用間篇。

³ 上田篤盛『戦略的インテリジェンス入門』並木書房、2016年。

⁴ 上田篤盛『情報分析官が見た陸軍中野学校——秘密戦士の孤独な戦い』並木書房、2021年。

諜報の標的の変遷

目的を秘匿して情報を収集するという諜報の本質は変わらないが、その標的と手段は時代とともに変化してきた。古くは人を敵地に送り込み、軍隊の規模や配置などを探る人的情報（HUMINT）が中心であった。20 世紀に入ると通信傍受や暗号解読などの信号情報（SIGINT）が重要となり、航空機による偵察、さらには偵察衛星などを利用した技術的な情報収集が発達した⁵。

同時に、標的も軍事や外交から、政治、経済、科学技術へと広がった。とりわけ科学技術や経済が国力を左右するようになると、政府機関だけでなく、先端技術や研究成果を保有する企業、大学、研究機関なども重要な標的となった。

インターネットの普及によって、諜報活動の舞台はサイバー空間へと拡大した。遠隔地から秘密情報を窃取できるだけでなく、SNS から対象人物の経歴、関心、人間関係などを把握し、直接接触することも可能となった。また、SNS は偽情報の流布や世論への働きかけなど、影響工作にも利用されている。

さらに今日では AI が加わり、大量の公開情報の収集・分析、対象人物の探索、文章・画像・映像の生成などを高速かつ大規模に行うことが可能になりつつある。

日本の防諜の歴史的経緯

日本で「防諜」という言葉が正式に採用されたのは 1936 年 7 月である。第 1 次世界大戦以降、総力戦の趨勢の中で各国の諜報・謀略活動が活発化すると、日本でもその対応を組織化するため、陸軍用語として防諜が生まれた。当時、防諜は「消極的防諜」と「積極的防諜」に分けられた。前者は秘密情報の漏えいを防ぐ活動、後者は外国による諜報・謀略を発見し、阻止・破砕する活動である⁶。すなわち、今日の欧米におけるカウンターインテリジェンス（CI）につながる概念がすでに存在していた。

敗戦によって旧軍や特高警察などの防諜組織は解体されたが、冷戦期には外国情報機関による諜報への対応が再び必要となった。以後、警察の外事部門や公安調査庁などが、それぞれの所掌で防諜を担ってきた。現在では、経済安全保障に関わる情報や重要技術も防諜の対象となっている。警察庁も、先端技術を保有する企業・研究機関への技術獲得の働き掛けを経済安全保障上の課題として位置付け、流出防止の取組を進めている⁷。

このように、諜報の本質は変わらないが、その標的と手段は時代とともに変化している。とりわけ今日では、国家機関だけでなく企業や研究機関もその標的となっている。

次章では、現代の諜報とその手口を見ていく。

⁵ Central Intelligence Agency, “Spy Speak Glossary.” CIA は HUMINT を「人的情報源から収集される情報」とし、20 世紀半ばの技術革命以前には主要な情報収集手段であったとしている。

⁶ 林武・和田朋幸・大八木敦裕「陸海軍の防諜——その組織と教育——」『防衛研究所紀要』第 14 巻第 2 号、防衛研究所。

⁷ 警察庁「技術流出の防止に向けて」および『令和 7 年版警察白書』。

第2章 現代の諜報とトレンド

藤谷 昌敏

現代の諜報活動の主体と目的

現代の諜報活動の主体には、まず「伝統的主体」とされる「国家情報機関」、「軍事情報組織」、「外交機関」、「治安機関」、「政府機関」がある。ここでいう「伝統的」とは、諜報活動の主体を基本的に国家機関として捉える古典的な見方である。

ただし、現代では、国家以外の「非伝統的収集者」である多様な主体が存在する。「民間企業」、「テック企業」、「サイバー企業」、「研究機関」、「ハッカー集団」、「犯罪集団」である。これら「国家主体以外の主体」も情報収集・分析・影響力工作に関与するため、国家のみが諜報活動の主体という従来の枠組みだけでは捉えられない。

伝統的主体の基本的目的が国家安全保障の確保、国家戦略の達成、外交政策の実現、軍事的優位維持、影響力の拡大、防諜の強化、サイバー空間の支配、経済安全保障の支援であるのに対し、非伝統的収集者の目的は、利益獲得、競争優位、政治的影響、理念の実現、情報公開、サイバー攻撃、テロ・犯罪の実行など多様化している。

接触手段の変化

ファイブアイズは、米国、英国、カナダ、オーストラリア、ニュージーランドによる機密情報共有の枠組みで、各国情報機関が高度な情報を共有し、国家安全保障上の脅威を共同で分析するインテリジェンス同盟である。2026年6月、ファイブアイズ加盟の情報機関が「Safeguarding Our Secrets」を公表し、中国の情報機関「国家安全部」(MSS)が職業関係のSNSやオンライン求人サービスを使った「非接触的手段」で、機密情報または特権的情報に接近できる人物を標的にしていると警告した⁸。

これまでは、学会、展示会、交流イベントなどで、「工作人員がターゲットに近づく」方式だったが、現在は、LinkedIn、IndeedなどのSNSで物理的接触なしで関係構築する、いわゆる「新型モデル」に転換している。

特徴的なのは、工作人員が接触するのではなく、ターゲットが応募してくる構造に変化したことである。具体的に言えば、「偽装企業が求人を出す」「転職希望者・研究者が応募する」「オンライン面接で内部情報を聞き出す」「暗号化アプリへ誘導し、より機密性の高い情報を要求する」などの流れで情報が漏えいする。

また、ターゲットが求職のためにSNSに公開した個人情報を利用してAIによる精密ターゲティングが行われている。こうした新型モデルへの転換に対応するためには、政府、企業、研究機関のより一層の緊密な連携が必要なことは言うまでもない⁹。

⁸ Five Eyes, Safeguarding Our Secrets, MI5/FBI/CSIS/ASIO/NZSIS, June 2026.、Five Eyes (FBI・MI5・CSIS・ASIO・NZSIS) が2026年6月に公表した共同勧告「Safeguarding Our Secrets」。

⁹ Defense News, “Five Eyes Issues Joint Alert on Chinese Targeting Government and Military Personnel Through LinkedIn and Job Platforms,” June 4, 2026.、勧告は、中国の軍事情報機関などが「偽装企業」「偽装コンサルタント」「偽装HR担当者」を用いて、オンライン面接を通じて非公開情報を引き出す手法を採用していると指摘。

主要な手口の整理

ここで中国、ロシア、北朝鮮の各情報機関による接触手段の手口について整理してみる。

国	主体	主な接触手口	対象	目的	特徴
中国	MSS PLA 民間企業	SNS 偽ヘッドハンティング 共同研究 企業提携	技術者 研究者 企業	技術情報・知財・ 軍民融合	組織化・制度化された産業スパイ 断片情報の一体化
ロシア	SVR GRU FSB	偶然接触 会食 外交官接触 犯罪組織利用	官僚 企業 研究者	政治・軍事情報 影響工作	HUMINT 伝統+犯罪組織のハイブリッド
北朝鮮	偵察総局	偽名就労 サイバー侵入 暗号資産窃取	IT 企業 金融機関	外貨獲得 軍事開発	非対面・潜伏型・サイバー中心

(参考)

中国

国家安全部（MSS）、人民解放軍（PLA）が諜報活動の主体であるが、その国の華僑組織や民間友好団体、民間企業を活用して情報ネットワークを拡大する手法を得意としている。先端技術情報の窃取を目的とするが、政財界に親中派を形成し、世論を動かすなどの影響力工作にも長けている¹⁰。

ロシア

SVR（対外情報庁）、GRU（軍参謀本部情報総局）、FSB（連邦保安庁）が諜報活動の主体である。海外で活動するのは、主に SVR と GRU であり、SVR の海外部署 Line X が先端技術・科学技術情報を担当するのに対し、GRU は軍事及び関連する科学技術情報を収集する。外交官の身分を利用して企業の展示会、学術研究会、飲食店、路上などで偶然を装って接触することがある。

北朝鮮

RGB（偵察総局）が海外で活動するほか、サイバーテログループ「ラザルス」「ブルーノロフ」「アンダリエル」「キムスキー」などが暗号資産窃取で世界中に莫大な被害を与えている。傘下の IT 技術者が LinkedIn や求人サイトで外国人技術者を装って入社し、企業のサーバーにマルウェアやバックドアを仕掛けるなどの手口が横行している。

¹⁰ 中国の工作は、華僑組織・民間友好団体・民間企業を活用した「社会的ネットワーク型情報収集」が特徴とされる（民間化・分散化の典型）。

特に注目すべきトレンド

トレンドとしては、ファイブアイズが指摘したような「非接触化」のほか、「分散化」、「民間化」、「デジタル化」が同時進行的に進められている。

分散化 (Distributed Intelligence)

情報源が国家機関から社会全体へ分散化し、従来は政府・軍・防衛産業が中心だったのが、現在では、研究者、ジャーナリスト、シンクタンク、民間企業、学生、技術者、SNS インフルエンサーなど社会全体が諜報の対象となった。

分散化した理由は、政策の温度感や専門の見通しが価値を持つこと、機密文書より「断片情報の組み合わせ」が重要であること、民間領域が巨大化（AI、半導体、量子、宇宙）したことなどである。

民間化 (Privatization of Intelligence)

現代の諜報では、国家情報機関だけがプレイヤーではなくなった。国家より民間の方が情報優位に立つ領域が増えており、民間サイバー企業、OSINT 企業、民間衛星企業、民間 AI 企業、民間軍事企業などの民間主体が積極的に関与する。

これにより、国家の情報独占が崩壊し、民間企業が国家級の情報収集能力を持ったことで、地政学上の重要なアクターとなったのである。

デジタル化 (Digital Intelligence)

サイバー空間が諜報の主戦場となったことで、APT 攻撃 (Advanced Persistent Threat : 高度で持続的な脅威)、サプライチェーン侵害、クラウド侵入、暗号化通信、デジタル監視、AI による自動分析などが主流となり、国家は「デジタル領域での情報優位」を争うようになった。特に AI は諜報の 3 領域（収集、分析、影響工作）を量的にも質的にも変えたといわれる¹¹。

次章では、世界と日本の最新事例について見ていく。

¹¹ APT 攻撃・クラウド侵入・暗号化通信・AI 分析などが諜報の主戦場となっていることは、Five Eyes の警告で示された「オンライン非接触型 HUMINT」「暗号化アプリへの誘導」などと整合する（デジタル化）。

第3章 世界と日本の最新事例

藤谷 昌敏

海外の事例

①中国国家安全部（MSS）による米国技術者リクルート事件

米国 FBI と司法省は、2026 年 6 月 10 日、中国国家安全部（MSS）と関係する偽コンサル会社 13 サイトを摘発したと発表した。報告によると、これら偽コンサル会社は、米国政府職員・軍関係者・防衛産業技術者から機密・非公開情報を引き出すリクルート工作を行うために設立され、LinkedIn などの求人プラットフォームを使って募集していた。

中国 MSS は、外資系コンサル会社、シンクタンク、採用担当者、防衛アナリスト求人などに偽装し、LinkedIn では、「あなたの経歴に興味がある」「専門性を評価している」と称賛した。応じた者には、高額な報酬付き「分析レポート」を依頼し、徐々に機密情報へ踏み込ませていた¹²。

②MI5 が警告した英国研究者への中国スパイ接触

英国 MI5 は、2025 年 11 月 17 日、英国議会へ「中国 MSS による LinkedIn を使ったスパイ活動」に関する警告文書を報告した。同文書では、偽ヘッドハンターが研究者を勧誘し、中国企業へ技術移転しているとして、「1 万人以上の英国人が LinkedIn で中国スパイに接触された」と発表している。

偽のヘッドハンターが「共同研究」「コンサル契約」を提案するが、実際は中国国家安全部のフロント企業であり、研究者が機密研究データを提供したケースも確認している。偽のヘッドハンターは、LinkedIn で「職務オファー風」のメッセージを議員スタッフや研究者に送り、「あなたの専門性に興味がある」「キャリアアップの機会を紹介したい」といった転職勧誘を装い、コンサル契約、共同研究、海外会議への招待などを提案して長期的な関係構築を図っていた¹³。

日本の事例

①日本企業 A 社における元研究員の技術流出事件

日本企業 A 社の元研究員は、2018 年 8 月～19 年 1 月に、電子材料の製造工程に関する機密情報を中国企業の社員にメールで 2 回送信したとされる。この元研究員は LinkedIn で中国企業から「共同研究・技術協力」のオファーを受け、機密情報を漏えいした。その後、元研究員は他国の企業に転職した¹⁴。

②国立研究関連法人における技術流出事件

2018 年、国立研究関連法人の中国籍の主任研究員は、以前からメールでやり取りしていた中国企業に自らが国立研究関連法人で研究に参加している研究データを送り、不正競争防止法違反で逮捕された。同研究

¹²Security Daily Review, “Five Eyes Warn Chinese Spies Use Fake Jobs to Target Clearances,” June 5, 2026.、Five Eyes の警告とも一致し、中国 MSS が LinkedIn を主要な人材獲得チャネルとして利用している典型例である。

¹³Oceania Cables, “Chinese Espionage Alert: Five Eyes Intelligence Agencies Warn of LinkedIn Threats,” June 4, 2026.、MI5 は、これらの偽プロフィールが「職務オファー風メッセージ」を送り、「キャリアアップ」「専門性への高評価」を強調する点を特に問題視している。

¹⁴高額報酬、転職斡旋を動機とする LinkedIn を使った「称賛 → 関係構築 → 機密情報要求」の典型パターンである。



員は中国の「国防七校」で博士号を取得したほか、北京理工大学でも兼職するなどしていた¹⁵。

事件から見える共通点

海外事件①、②及び日本の①の事件は、いずれもファイブアイズが指摘する LinkedIn の事例であり、非接触的手段で接触する「新型モデル」である。技術移転を狙って研究者をターゲットとしている点は4件とも共通であり、中国情報機関や企業の先端技術への関心の高さがうかがわれる。

また、協力の動機は、高額な報酬のほか、希望の就職先への斡旋などであるが、中国側が勧誘の中で「あなたの経歴に興味がある」「専門性を評価している」と称賛するなど、研究者の心理を突いた巧妙な罠が見て取れる。

次章では、「カウンターインテリジェンスのあり方」について見ていく。

¹⁵ 中国の軍民融合ネットワークと研究者の関係性が濃厚で、日本の研究機関が抱える「内部者リスク」の典型例である。

第4章 カウンターインテリジェンスのあり方

上田 篤盛

カウンターインテリジェンスとは何か

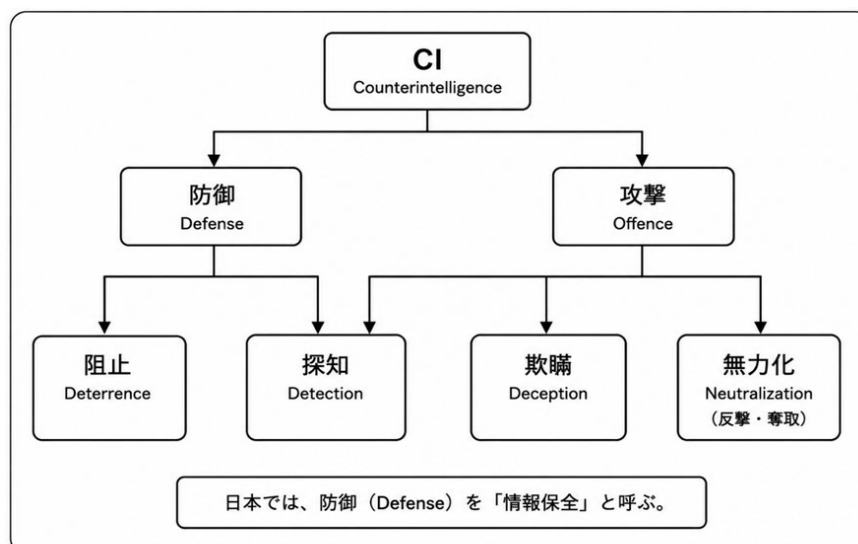
カウンターインテリジェンス（CI）は、一般に「防諜」と訳される。しかし、防諜を秘密情報の漏えいを防ぐ情報保全と同じものと捉えると、その意味を狭くしてしまう。CI とは、相手による諜報や謀略から自らを守るとともに、その活動を探知し、阻止し、必要に応じて対抗する活動である¹⁶。

第1章で述べたが、旧日本軍では、防諜は諜報、宣伝、謀略と並ぶ秘密戦の1つとされ、「消極的防諜」と「積極的防諜」に区分されていた。現在、米国ではCIを「防御（Defense）」と「攻撃（Offense）」の2つの側面から捉えている。名称は異なるものの、秘密を守るだけでなく、相手の諜報・謀略を探知し、これに対抗するという考え方は共通している¹⁷。

防御と攻撃（4つのCI機能）

CIの機能は「阻止」「探知」「欺瞞」「無力化」に整理できる。防御には「阻止」と「探知」がある。阻止とは、秘密保全、物理的保全、通信保全、人的保全などによって、相手による情報の取得や接近を困難にすることである。探知とは、自組織への不審な接触や行動などから、諜報・謀略の兆候を発見することである。

一方、攻撃には「探知」「欺瞞」「無力化」がある。ここでいう探知は防御の探知とは異なり、相手組織に浸透するなどして、その諜報・謀略活動を積極的に把握することまで含む。欺瞞は、偽情報などによって相手を欺き、その諜報・謀略の効果を無効化する活動である。無力化はさらに踏み込み、相手の要員やネットワークなどに働きかけ、諜報・謀略組織そのものを麻痺・破砕する活動である¹⁸。



資料：U.S. Marine Corps, Counterintelligence Field Manual, FMFM 2-22.3, 1997, Figure 2.3.

¹⁶ U.S. Army, Intelligence, FM 2-0, 2010, Chapter 6. 米陸軍はCIを、外国勢力等による諜報その他の情報活動に対し、識別、欺瞞、利用、妨害、防護等を行うための情報収集および活動と定義している。

¹⁷ U.S. Army, Counterintelligence, FM 34-60. 同マニュアルは、CI活動に攻撃的・防御的活動、調査、脆弱性分析等を含めている。

¹⁸ U.S. Marine Corps, Counterintelligence Field Manual, FMFM 2-22.3, 1997, Figure 2.3.



企業における CI の範囲

国家の CI 機関は、防御から攻撃まで幅広い機能を担う。一方、企業が外国情報機関に浸透したり、その諜報組織を欺瞞・無力化したりすることは、通常の企業活動の範囲を超える。したがって、企業 CI の中心は、自社の情報・技術・人材を守る「阻止」と、自社に向けられた諜報・謀略の兆候を把握する「探知」となる。

ただし、企業における探知は、スパイを特定し摘発することではない。不審な接触や情報要求、通常とは異なる情報へのアクセスなど、自社に対する諜報活動の兆候を捉えることである。外国情報機関などによる活動の実態解明や捜査、摘発、攻撃的 CI は、情報機関や司法警察機関などが担う領域となる。

企業に求められるのは、国家と同じ CI 機能を持つことなく、自らが担う「阻止」と「探知」を確実に機能させることである。

次章では、「自助」の観点から企業・組織がとるべき具体的な対策を見ていく。

第5章 企業 CI の設計（自助）



稲村 悠

企業におけるカウンターインテリジェンスの実装

前章で述べたとおり、企業における CI の中心は「阻止」と「探知」である。自社の何が狙われ得るのか、相手はどのような接点を利用できるのかを把握し、その働きかけや情報取得の兆候を捉え、被害を防ぐための措置を講じることである。

このとき、外的脅威と内部不正を別々の問題として扱ってはならない。外部の脅威主体が研究者や技術者に接触し、共同研究、転職、講演等の機会を通じて非公開情報の提供を求めた場合、最終的な情報の流出経路は、メール送信、印刷、撮影など、通常の内部不正と共通する経路をとり得る。入口は外部からの働きかけであっても、出口は内部者の行為となるのである。

したがって、社内の行為を捉える仕組みと、その背景にある人物・組織・接触を評価する仕組みを連携させる必要がある。これらを個別の対策を導入して終わらせず、1つの運用として設計すべきものである。

保護対象の特定

出発点の1つは、自社の何を守るかを明らかにすることである。自社が保有する技術、研究成果等について、自社の競争優位性の源泉としての価値、国家戦略上の位置付け、代替可能性、流出時の影響を評価する。第三者がその技術を再現するには何が必要か、どの情報や知見が当該技術を構成するのかまで掘り下げる必要がある。

保護対象は、設計図や実験データなどの「データ」、試作品、サンプルなどの「モノ」、そして失敗知、工程の知見を持つ「ヒト」に分けて把握する。特に、「ヒト」に関しては、誰がどの知見を持ち、誰が複数工程を横断して理解し、どの人材に技術が依存しているかを確認することが重要である。

ここでキーパーソンを特定する必要がある。キーパーソンとは、重要技術の知見、アクセス権、外部との接点を持つなど、防護上の重要性が高い人物である。これらは疑う対象を選ぶ作業ではなく、守るべき情報と、その情報を扱う人を明らかにする作業である。

非サイバー領域の脅威インテリジェンス

自社が備えるべき脅威は、企業ごとに異なる。同じ業種であっても、保有する技術、事業地域、取引関係などの外部との接点が異なれば、外的脅威が獲得したいものも、獲得のために利用し得る経路も変わる。したがって、保護対象の把握と並ぶ出発点として、外部の脅威を知る活動を位置付ける必要がある。

そこで、非サイバー領域の脅威インテリジェンスが重要となる。非サイバー領域、すなわちカウンターインテリジェンスの観点で自社を狙う脅威アクターの意図・能力・機会を分析することである。単なる事件の紹介や情勢の解説にとどまらず、脅威主体は誰か、その目的は何か、標的の傾向や用いられる手法とその変化を、自社との関係性を踏まえて分析し、継続的にキャッチアップしていくことに重点を置く。

ここでいう「非サイバー」とは、物理的空間での活動にとどまらず、SNS やメールを介した勧誘・情報要求も、人的接近や技術獲得の手法として扱う。通常、サイバー領域における脅威インテリジェンスは普及し

ているが、非サイバー領域の脅威インテリジェンスは普及しているとは言い難い。

脅威分析の要点

脅威の分析では、意図・能力・機会の三つの観点を用いる。意図とは、相手が何を獲得し、又は何を実現しようとしているかである。関心を向ける技術や人材まで、過去の活動等からその目的を評価する。

能力とは、その目的を実行するための資源と手段である。資金、人員、協力者や関係組織に加え、所属を偽った接近、研究・取引上の依頼を利用した情報獲得、内部者への働きかけなど、用いられる手法も分析する。ただし、ある手法を用いる能力があることと、自社に対してその手法を用いる可能性があることは、別の評価である。

機会とは、相手が自社の保護対象に接近し、目的を実行し得る条件や接点である。オンライン空間、展示会・学会、共同研究等について、誰が、いつ、自社の保護対象に接することができるかを照合する。

三つの観点を組み合わせることで、「どのような主体が、何を狙い、どの関係者や組織を経由し、自社の誰に接触して、どこから情報を得ようとするのか」を具体化する。自社への直接の接触に加え、取引先、共同研究先、委託先、元社員等を介する間接的な経路も検討する。主体を特定し尽くしてから対策を始めるのではなく、確認できた情報と仮説を区別しながら、想定すべき主体の類型と手法を整理するのである。

脅威分析の運用

分析の成果は、主体名や手口の一覧に加え、自社のどの技術・人材・業務に関係するか、どの接点を重点的に確認するか、どの兆候を捉えるか、どの部門が何を判断するかまで整理する。その評価を、外部接触時の確認事項、ログ分析の重点など各施策へとつなげることに、実務上の意味がある。

脅威インテリジェンスを持つことは、公開情報、専門家・専門機関の分析、官民の情報共有等を活用しながら、自社として何を知る必要があるかを定め、得られた分析を業務に適用できる体制を持つことである。情報の量ではなく、警戒や対策に関する判断に利用できるかを基準とする。

この分析は、単発的な取り組みではなく、定期的な評価に加え、脅威主体の標的や手法の変化、自社の新技術の公表、事業地域の拡大、共同研究の開始等を契機に、関与経路と対策の重点を見直す。外部の脅威動向と自社の実態を継続的に照合する。

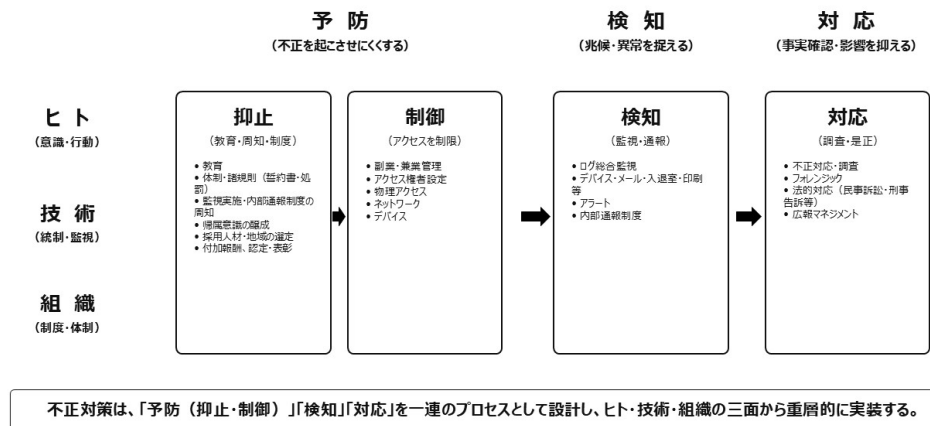
脅威を知る活動は、当初の対策の出発点であると同時に、その後の運用を更新し続ける基盤でもある。

統制の全体像と要点

保護対象の把握と脅威インテリジェンスを踏まえ、流出シナリオごとに現状の統制を点検する。共同研究を通じた必要以上の情報要求、展示会での接触後に続く個人的な面談依頼、委託先を経由した持出しなど、情報の所在から外部への流出までを経路として描く。そこには、外部からの働きかけだけでなく、退職を控えた担当者による情報の集約など、内部者を起点とする内部不正経路も検討する。

現状の対策は、その経路上に配置した上で不正対策モデルに当てはめて評価する。不正対策モデルは、予防（抑止・制御）～検知～対応の各フェーズにおいて、自社がどこで統制できているかを確認する。

不正対策の全体像



また、全ての情報、全ての人材、全ての取引を同じ強度で管理する必要はない。まずは重要技術を扱う部門やプロジェクトを重点対象とし、既存の業務・管理の仕組みを生かして不足部分を補う。営業、研究開発、海外活動の実態を理解せずに制御を強めれば、保護すべき事業そのものを阻害するため、抑止策や検知策を強化するなど統制のバランスを見極めることが、対策の実効性と継続性の前提となる。

兆候の検知

ここまでの脅威評価を検知につなげるには、「行為」「人」「接触」の三つの視点から情報を観測し、照合する必要がある。

「行為」は、情報の検索・閲覧・送信等の振る舞いであり、ファイル操作、メール、クラウド、印刷、入退館等の記録から捉える。

「人」は、保有知見、担当業務、アクセス権、所属や役割の変化である。

「接触」は、社外の誰と、どのような関係を持ち、何を求められているかという文脈である。

例えば、重要技術を扱う社員が、学会で知り合った相手から非公開の情報について繰り返し質問を受け、その後、担当外の研究資料を閲覧し始めたとする。このケースにおいて、接触の機会と社内ログが別々に扱われれば見過ごされるかもしれない。両者を結び付けることで、外的脅威による接触可能性と閲覧の業務上の必要性を確認する理由が生まれる。ただし、この段階で本人の不正や相手の諜報活動を断定することはできない。

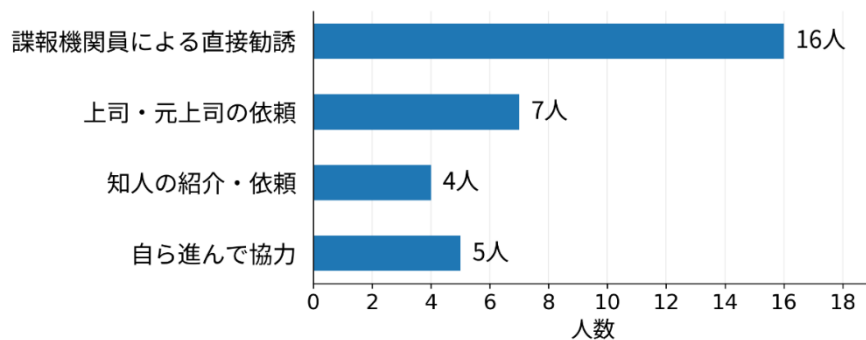
分析では、前述のキーパーソンとイベントトリガーを組み合わせる。イベントトリガーとは、退職の申出、異動、重要プロジェクトへの参加・離脱、役職の変更等を契機に、対象情報へのアクセス権の変動と環境の変化を検知と接続させる。

ただし、当初から情報取得を目的として組織に入り込んだ者や、正当な職務権限の範囲で情報を取得する者については、過去の本人の行動から大きな変化が現れない場合がある。本人の平常時との差分だけでなく、担当業務と閲覧対象の整合性、重要情報を横断して収集する継続的な行動、採用・契約時の確認内容等を併せて評価する必要がある。

対象者の属性分析

対象者の分析では、「なぜその人が狙われるのか」と「なぜ働きかけに応じるのか」を分けて考える必要がある。前者は、保有知見、アクセス権等の属性に関わり、後者は、動機、置かれた環境、相手との関係性に関わる。

大上渉氏が2017年に公表した研究¹⁹では、1952～2015年に日本でロシア・旧ソ連の諜報機関に協力した情報提供者32人を分析している。検挙時の年齢は40代が10人、50代が12人であり、職業には自衛官等、国家公務員、メーカー社員、自営業者等が含まれた。注目すべきは協力に至る経緯である。上司・元上司からの依頼が7人、知人の紹介・依頼が4人であり、計11人が既存の人的関係を介して情報提供に至っている。外国情報機関から本人への直接勧誘だけを想定しては、この経路を見落とす。



※対象：1952～2015年の日本のロシア・旧ソ連諜報関連事例。上司・元上司、知人を介した経路は計11人。接触を受けた全対象者の分布や勧誘成功率を示すものではない²⁰。

中国関連の米国公表事例でも、情報を提供した者の年齢や立場は一樣ではない。米海軍の Wenheng Zhao は2024年の判決時に26歳であった一方、退役後に防衛企業で勤務した Shapour Moinian は2022年の判決時に67歳であった。若年の実務担当者であっても情報へのアクセスを持ち、退職・退役後も知識や人脈、再就職先でのアクセスを通じて情報取得に関与し得ることが分かる²¹。

ただし、これらは摘発や司法手続を通じて公表された事例であり、接触を受けた全対象者の分布ではないことには注意が必要である。

企業で把握すべき属性は、本人がどの情報にアクセスできるか、どの知見を持つか、誰に依頼すれば情報を得られるか、どの業務を通じて外部と接するかを確認する。重要技術に従事する者に加え、その上司・元上司、退職者等も、情報流出の直接・間接の経路として検討する必要がある。これは疑人物を把握しにくく作業ではなく、守るべき人と接点を明らかにする作業である。

¹⁹ 大上渉（2017）「日本においてロシア諜報機関に協力した情報提供者の類型化」『犯罪心理学研究』

²⁰ 大上渉（2017）「日本においてロシア諜報機関に協力した情報提供者の類型化」『犯罪心理学研究』を再図示。

²¹ 米国司法省、Wenheng Zhao 事件の判決に関する公表資料（2024年1月8日）及び Shapour Moinian 事件の判決に関する公表資料（2022年11月7日）。年齢はいずれも判決時。

ソ連情報機関「KGB」の着目点

ここで、情報機関がどのような対象に着目しているかについて紹介する。Free Russia Foundation が「The Lubyanka Files」で公開した KGB（ソ連国家保安委員会）の教材がある。ここでは、1985 年の外国人への心理的働きかけに向けた工作担当者の訓練に関する教材を取り上げる²²。

同教材の記述では、自分の職位が能力等に見合わないと感じる者、上司の評価を不公平だと考える者、他の職員に比べて昇進が遅いと感じる者、職位の不安定さに不満を持つ者が、着目すべき対象として扱われている。肩書や経済状態だけでなく、本人が自分の置かれた状況をどのように受け止めているかが、評価の対象なのである。

年齢と職位を組み合わせた記述もある。36～45 歳で低い職位にある職員を、特に働きかけを受けやすい層として位置付けている。その説明として、仕事への意欲の低下、家庭の問題、子どもの教育費や住宅ローン等の負担、上司に対する不満などを挙げ、新たな提案＝諜報活動への協力を受け入れやすくなるという見方を示している。

本稿が企業実務に引き付けて読むべきと考えるのは、特定の年代そのものではなく、本人の期待と職務上の処遇との間に生じる隔たり、すなわち不満である。組織から見れば通常の配置転換や研究方針の変更であっても、本人には、自分の専門性や貢献が認められなくなった出来事として受け止められるかもしれない。そこに外部から評価や機会が提示されたとき、その提案が本人にとって持つ意味を理解する必要がある。

この読み替えでは、従業員の不満や負担を探し出して危険人物を選ぶのではなく、組織として支援を要する変化点と、情報へのアクセスや外部との接点を確認する。例えば、重要技術を扱う担当者の役割が変わる時点には、権限を整理するだけでなく、外部から届く不審なアプローチをどこへ相談できるかを伝えておく。本人が既に応答した後でも相談できることが、接触を個人だけの問題にしないために重要となる。

次に述べる動機に関するフレームワーク「MICE」や「MICELDS」と照合すれば、金銭的な事情、承認への期待、処遇への不満、生活上の負担等を、複数の要素から検討できる。

このように、KGB の教材が示す対象者の評価は、今日の企業にとって、そのまま活用すべき人物のリスク判定基準ではなく、外部の働きかけを理解するための材料となる。

「MICE」と「MICELDS」による動機の分析

諜報員が協力者を獲得する際の動機を整理する代表的な枠組みに、Money（金銭）、Ideology（思想・信念・信条）、Compromise（名声や信用の危機）、Ego（欲求）の四つからなる MICE がある。Money は金銭的な困窮だけでなく、報酬や利益を得たいという期待を含む。Ideology は、自らの価値観や信念に合うと考えて協力する動機である。Compromise は、知られたくない事柄を暴露され、名声や信用を失うことへの恐れに関わる。Ego では、特に承認欲求や自己顕示欲に着目し、自分の専門性や貢献を認めてほしいという感情を捉える。

また、筆者が提唱する MICELDS（マイセルズ）は、この MICE に Love、Disgruntlement、Stress、Secret を加えた拡張的な枠組みである²³。最後の S には Stress と Secret の 2 つの要素を置く。個人の協力

²² Free Russia Foundation 「The Lubyanka Files」の公開目録では 1985 年資料としている。英訳題名：Some Aspects of Training the Operative for Psychological Influence of Foreigners During Cultivation。

²³ 稲村悠『謀略の技術』中央公論新社、2025 年

可能性を数値で予測するものではなく、MICE だけでは捉えにくい感情や環境、関係性を分析するための視点である。

Love（愛）は、恋愛に限らず、家族愛、友情、組織愛を含む。例えば、「家族を守りたい」という感情は、強い動機になり得る。

Disgruntlement（不満）は、組織や上司への不満だけでなく、自分が正当に評価されていないという不満感や、人生・キャリアへの失望も含む。

Stress（ストレス）は、仕事、家庭、経済事情等に伴う負担や、複数の問題が重なる状況に着目する。

一方、Secret（秘密）は、秘密を暴露すると脅す Compromise とは区別する。秘密や悩みを理解し、共有・保護してくれる相手への安心感や仲間意識が、関係の維持を支えるという観点である。ただし、その関係が後に秘密の暴露を恐れる関係へ変わる場合には、Secret と Compromise が重なり得る。

これらの要素は、相互に関連する。承認欲求と職場への不満、家族への思いと経済的負担などが重なり、関係の進展とともに協力の理由が変わることもある。動機分析は、何が協力の入口となるかを読み解くものである。

中国諜報における動機分析「BEWARE」

ニコラス・エフティミディアスが中国の諜報活動を分析して提唱した BEWARE も参考になる。Business opportunities（ビジネス機会）、Ethno-nationalism（国家・民族への帰属意識）、Wealth（金銭等の直接的利益）、Academic advancement（学術的評価・研究機会の拡大）、Repression（脅迫・圧力）、Emotional bonds（感情的つながり）という 6 つの観点から、協力の背景を整理するものである²⁴。

MICELDS で本人の不満や承認欲求を捉え、BEWARE で相手から提示される事業・研究上の機会に着目すれば、本人の事情と働きかけを結び付けて検討できる。

動機を生み出す外部接触

2020 年の Jun Wei Yeo 事件の米司法省公表資料では、中国情報機関側の指示に基づき、情報へのアクセスを持つ人物を探すとともに、仕事への不満や経済的な問題を確認していたことが記載されている。Yeo は報告書の作成に報酬を支払い、最終的には中国政府へ渡ることを対象者に明かしていなかった。情報に接近できる立場と、依頼に応じる理由の双方に着目していた事例である²⁵。

このような関係を理解するには、脅迫による「強制」だけでなく、本人が協力を合理的だと感じる「納得」の形成を見る必要がある。筆者はその働きかけを、「理解」「支援」「救済」「承認／評価」「依存」「共鳴」「正当化」の 7 つに整理している²⁶。相手が悩みを理解し、専門性を評価し、本人の目標に合う機会を提示することで、協力への心理的な抵抗が小さくなる過程を捉えるためである。

このような過程では、例えば、開発プロジェクトの中止によって不満や失望を抱えた技術者に、外部から開発継続の機会が提示され、その検討の名目で非公開資料を求められる場面が想定できるだろう。不満や転職の検討自体を問題とするのではなく、その変化点で誰が接触し、どのような行動の変化が生まれたかが重要な要素となる。

²⁴ Nicholas Eftimiades 『CHINA'S ESPIONAGE RECRUITMENT MOTIVATIONS』(2023)

²⁵ 米国司法省（2020 年 7 月 24 日）、Jun Wei Yeo 事件の有罪答弁に関する公表資料

²⁶ 稲村悠『謀略の技術』中央公論新社、2025 年

第6章 内部脅威検知の実装と防護の実装（自助）

川下 巧
稲村 悠

前章では、行動を解釈するための属性・動機・接触の文脈を整理した。本章では、その文脈を社内で得られる記録と連携させ、内部脅威の兆候を捉える方法と、防護の実装・継続運用を述べる。

カウンターインテリジェンスに基づく内部脅威の分析手法

CIを現代のIT環境に応用し、組織内の人物の振る舞いから「内部脅威リスク」を分析・検知するには、「動機」「情報接触」「情報出口」という3つの要素（アクション）を軸にログデータを集約し、それらを相関分析することでリスクをスコアリングし、脅威の兆候を探ることが重要だ。

この手法は、諜報活動に利用された人物が、特異な行動やこれまでと異なる行動をしたことを可視化する面で効果を発揮するが、当初から情報取得を目的としているなど、行動の変化が表れにくい場合には、後述する検知の限界を踏まえた対応が重要となる。

内部脅威分析を構成する3つの要素

調査・監視においては、ユーザーの挙動を以下の3つの分析観点から多角的に把握する必要がある。

① 動機（Why：不正や持ち出しの背景・要因）

従業員が外部から指示・教唆を受けることで脅威主体（スパイや情報持ち出し者）へ変わる隙がある心理的・環境的要因を示す兆候。

前述したMICELDSフレームワークやBEWAREフレームワークに紐づく動機は、時に社内で収集できるログと紐づくものであり、労務管理ログやWebアクセスログ等から以下を分析する。ただし、以下の記録は動機そのものの証明ではなく、業務・接触の文脈と照合するための手掛かりとして扱う。

- ・ **離職リスク**：転職サイトへのアクセスや退職規定の閲覧。
- ・ **不就労**：業務無関係なWeb閲覧や、他ユーザーに比べて著しく低いPC操作回数。
- ・ **ハラスメント／メンタルヘルス**：相談サイトへのアクセスや関連キーワードの検索・閲覧。
- ・ **金銭問題／超過勤務**：消費者金融やトラブル関連サイトの検索、勤怠データとPC操作（アクティブウィンドウ等）の乖離。

② 情報接触（What & How：情報資産へのアプローチ・準備）

機密情報に触れる挙動を示す。

- ・ **情報入手・閲覧・検索**：機密性の高い情報や大量データの入手・検索・閲覧行動。
- ・ **情報削除**：証拠隠滅や妨害を目的とした大量データ・ログの削除行動。
- ・ **アカウント運用・接続**：なりすましログイン、権限外アクセス、社外環境からのネットワーク接続。
- ・ **ルール遵守**：セキュリティポリシーから大きく乖離した違反行動。

③ 情報出口（Where：情報資産の外部持ち出しチャンネル）

実際に外部へ情報を流出させる経路を示す。

- ・ **オンラインチャンネル**：クラウドストレージ、社用メール、Web メール、ファイル転送アプリ、グループチャット、SNS へのファイルアップロード・送信。
- ・ **生成 AI**：許可外の生成 AI サービスへのファイル書き込み・アップロード。
- ・ **物理チャンネル**：USB 等の外部記憶媒体へのファイル書き出し、紙媒体での印刷。

要素の掛け合わせ（相関分析）とリスクスコアリング

印刷を行った、転職サイトを見たという個別の行動だけで不正と断定すると誤った判断につながる。このログ分析手法における要点は、「要素（動機×情報接触×情報出口）の掛け合わせによるスコアリング」をいかに判断するかにある。

分析のシナリオ例①（内部不正型）：

- ・ **【動機】** 転職サイトを頻繁に閲覧し、退職規定を確認（離職兆候）
- ・ **【情報接触】** 深夜帯に通常業務ではアクセスしない営業秘密関連のフォルダを大量検索・閲覧
- ・ **【情報出口】** 許可外のクラウドストレージや Web メール、あるいは USB メモリへ連続して書き出し

一方、監視の存在を認識している者は、閾値を避けるために挙動を平準化させる。

分析のシナリオ例②（高度持出し型）：

- ・ **【動機】** 転職や独立の兆候は実行の数か月前に現れ、直前期にはむしろ平常化する
- ・ **【情報接触】** 深夜帯を避け、通常業務時間内に日々少量ずつ閲覧し、ローカルに集約する
- ・ **【情報出口】** 単一経路に依存せず、少量のメール送信、クラウドの共有設定変更を経た社外からのダウンロード、私物端末での撮影などに分散させる

このように 3 要素が単一の人物・時間軸上で重なった際に高リスクスコアを算出・発報することで、真に危険度の高い内部脅威や防諜上のリスクを早期に洗い出し、決定的な被害が発生する前に先手を打つことが可能となる。

種別	視点	分析内容	必要データ種別													
			資産情報 (ハードウェア)	アクティ ブフウ ド	WEB アクセス	ファイル 操作	メール	印刷	ログオン ログオフ	ドライ ブ追加	アプリ ケーション 稼働	通信 デバイス	未登録 端末	勤怠管理	施設 入退館	CRM
情報 セキュ ディ	情報持ち出し (情報持ち出しの兆候 や持ち出し有無を調査 するもの)	Webブラウザ経由のファイル持 ち出し	推奨	推奨	必須	-	-	-	-	-	-	-	-	推奨	推奨	-
		Webサイトへの書き込み行動	推奨	推奨	必須	-	-	-	-	-	-	-	-	推奨	推奨	-
		アプリケーション経由の情報持 ち出し	推奨	必須	推奨	必須	-	-	-	-	推奨	-	-	推奨	推奨	-
		社用メール経由の情報持ち出し	推奨	-	-	-	必須	-	-	-	-	-	-	推奨	推奨	-
		外部記憶媒体へのファイル書き 込み	推奨	-	-	必須	-	-	-	推奨	-	-	-	推奨	推奨	-
		印刷	推奨	-	-	-	-	必須	-	-	-	-	-	推奨	推奨	-
	情報接触 (情報持ち出しのため の準備)	機密情報などの入手・加工	推奨	推奨	-	必須	-	-	-	-	-	-	-	推奨	推奨	推奨
		なりすまし/不正ログイン	推奨	-	-	-	-	-	必須	-	-	-	-	推奨	推奨	推奨
	セキュリティポリシー 違反	セキュリティポリシーが適切に運 用されているか調査するもの	推奨	必須	必須	必須	必須	必須	推奨	必須	推奨	推奨	推奨	推奨	推奨	推奨
		pc操作状況から勤務実態を把握 勤怠実績との乖離があるか調査 を行うもの	推奨	必須	推奨	推奨	推奨	推奨	推奨	-	-	-	-	必須	推奨	-
労務管理	不就業	勤務時間中に不就業（ネット サーフィンやゲームなど）に該 当する行動を行っているないか 調査するもの	推奨	必須	必須	-	-	-	推奨	-	-	-	-	必須	推奨	-
		人材流出/ハラスメン ト/メンタルヘルス	推奨	必須	必須	推奨	推奨	-	-	-	-	-	-	推奨	推奨	-
		ハラスメントへの悩みや転職を 示唆する行動/ハラスメント行動 を調査するもの	推奨	必須	必須	推奨	推奨	-	-	-	-	-	-	推奨	推奨	-

分析に必要なログデータ種別

内部者への働きかけと、行動変化による検知の限界

諜報活動を行う者は、すでに組織に所属する従業員を教唆するなどして取り込み、目的を達成するよう行動させることが考えられる。こうして教唆された従業員の行動に変容が生じた場合には、内部脅威検知のアーノマリー分析で発見できる可能性がある。情報の所在やアクセス権限を確かめる過程で生じる、重要情報の保存先に対するアクセス拒否や、権限の範囲内でありながら担当外の情報を横断的に閲覧する行動は、その兆候となり得る。いずれも単発では判別がつかないため、継続性の観点から評価することが求められる。

一方、採用・受入れの時点から情報取得への協力を目的としている者については、情報へのアクセスが職務上正当なものとして現れ、本人の平常時との差分が生じない場合がある。これは情報機関員自身の潜入を一般的なモデルとするものではなく、情報取得の目的がいつ形成されたかによって、検知できる変化が異なるという問題である。

そのため、当初から目的を持つ場合も、後から取り込まれる場合も、本人の過去の行動との比較だけでなく、担当業務と閲覧対象の整合性、付与された権限と実際の利用、重要情報を横断して取得する継続的な行動を確認する。

ただし、これらは組織の内側で観測できる事象に限られる。リスクの発生源が採用・受入れ前や組織外の接触にある場合も想定し、重要情報へのアクセスを伴う人材については、採用・契約時のリスク・デューデリジェンスと、その後の適格性の継続的な確認を制度として組み込む必要がある。

以下では、その入口統制と外部接触管理を、継続的な防護の運用として具体化する。

リスク・デューデリジェンスと継続的運用

リスク・デューデリジェンスは、採用候補者や取引先について、コンプライアンス上の問題に加え、相手が懸念される組織・人物と接点を持つかを把握し、必要な管理措置を決める入口統制である。活用局面には、重要情報を扱う人材の採用・受入れ、共同研究、新規取引等を含め、接触する技術情報の重要度と付与する権限に応じて実施要件を変える。

組織については、当事者、実質的な支配関係、役員の兼任、関連会社、研究協力先等を確認する。人物については、経歴の整合性、過去・現在の所属、兼業・兼職、論文・特許、研究者ネットワーク、関係法人等を手掛かりにしながら、経済安全保障上懸念される組織や人物との接点を検知する。

ただし、国籍や出身地をもってリスクを判断したり、ある組織との接点があるだけで不正主体とみなすことは絶対にあってはならない。接点の時期、役割等の文脈を確認し、判断する。

また、入り口のリスク・デューデリジェンスに加え、継続的な実施・運用も想定される。その対象である社員・組織には、兼業の開始、役員・株主の変更等の変動事項が生じうる。そこで、その実施頻度を技術情報への関与度合い・重要性に応じて定める。リスク・デューデリジェンスは、相手の「安全であることの証明」ではなく、対策の内容と強度を決めるための基盤なのである。

オンラインへの対策

昨今のトレンドであるオンライン上の接触については、接触相手が健全な存在か＝「相手が誰か」にまず着目する。例えば、社用メールであれば、ネガティブリストから紐づくドメインをアラート対象とし、当該ドメインからの連絡受信に対してアラートを鳴らすことは可能であるが、その網目は十分ではない。また、自社社員の SNS から、新たな繋がりを持った人物が懸念される主体かを判別することは一定可能だが、個

人の SNS アカウントを監視することは許容されない。

そこで、「相手が誰か」だけに注力するのではなく、相手が「どのような手法をとってくるか」について、脅威インテリジェンスから導かれる手法を整理して社員に教育し、組織を介さないやり取りへの誘導や具体的な情報の要求等が重なる場合には、速やかに組織に報告・相談する教育を徹底し、相談窓口の間口を広げておく必要がある。

これら対策は、脅威インテリジェンスによって詳細に分析され、その分析結果と一致した場合には一定の注意喚起を行う仕組みを導入することと連携される。早期相談によって社員を保護するという姿勢を、制度と現場の対応の両方で示す必要がある。

部門横断機能の重要性

企業 CI を機能させるには、誰がその脅威や問題を把握し、誰が決めるかを定めなければならない。人事は役職等の変化を知り、情報システム部門はログを持ち、研究開発部門は情報の重要性を理解し、総務や施設管理部門は入退館や物理的セキュリティを扱う。これらを横断的に把握・管理する機能が必要である。

経済安全保障室等の専門部門はその担い手となり得る。俯瞰して全体像を把握し、対処方針を設計したのち、法務、人事、情報セキュリティ等の部門と連携し、対策の実装を進めることが推奨される。

運用の前提

企業 CI は、社員に対する管理がどうしても重たくなる。ただし、その管理は、監視・制限だけを念頭に置かず、不安や不満、外部からの圧力等を相談できる環境、適切な評価やキャリア支援も重要な対策となる。特に、不審な接触については、一般の内部通報とは異なる専門的な判断を要するため、CI の知見を備えた専用の相談窓口を設け、既存の人事・法務・内部通報の機能と連携させることが望ましい。

ログや人的情報の取扱いについては、目的、取得範囲等の手順を定め、法務・人事の確認を経て運用する。社員の支援のために得た情報を無制限に監視へ転用せず、必要性和相当性を個別に検討する。重要技術を守るための取組が、根拠のない人物評価や不利益取扱いを生む仕組みになっては本末転倒である。

これらの企業 CI の各施策は、社員を保護するための施策なのである。

以上が企業内で担う「自助」の基本である。ただし、自社のログや接触記録だけでは、相手が他社でも同様の働きかけをしているか、特定の技術分野に接近が集中しているかまでは分からない。自社に合った脅威インテリジェンスを維持するうえでも、社外の知見との接続が欠かせない。自助の限界を補い、自社の経験を他者の防護にも生かすために必要となるのが、次章で述べる共助と公助である。

第7章 予防型インテリジェンス（共助と公助）

稲村 悠

官民連携のあり方

企業が自社の重要技術を把握し、各対策を整備しても、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、未公開事案など、企業が独力では得にくい知識や具体的な兆候を把握し得る。企業における CI を実現させるためには、事件として全容が解明されるのを待つのではなく、双方の情報を連携させ、企業が自社内で打ち手を検討できる具体的な警告へ変換する必要がある。

この連携を実現させ、官民が協力して未然防止を図る仕組みが「予防型インテリジェンス」である。兆候を早期に可視化し、被害が生じる前に企業の統制を改善させる基盤となる。第5章・第6章で述べた脅威インテリジェンスと企業内の検知を、官民双方の情報によって補い、具体的な対処につなげることに意味がある。

官民連携における3つの非対称性

ただし、官民連携を単なる「情報共有の場」として設計しても、継続的な協力にはつながりにくい。筆者は、その設計に当たり、次の3つの非対称性を小さくする必要があると考える。

第1は、情報の非対称性である。企業が具体的な自社情報を提供しても、官側から返る内容が一般的な注意喚起にとどまれば、自社の防護にどう役立つのかが見えない。官側の情報を全て開示することは不可能であるが、企業が官側から得た情報をどう対処事項に落とし込めるか、すなわち、官側は企業に寄り添った情報を提供できるかが課題となる。

第2は、リスク負担の非対称性である。企業は、事件化や報道に伴う影響に加え、社員への対応、労務上の調整、取引先への説明等を担うことになる。情報を提供した後に何が起こき、どのような負担が生じるのかが不明確であれば、早期相談をためらう要因となり得る。

第3は、実装可能性の非対称性である。官側が脅威や手口を説明しても、それだけでは企業の具体的な措置には結び付かない。官側には企業業務に沿ったアウトリーチ活動が求められる。

官民それぞれの権限と守秘上の制約を踏まえ、共有できる情報と対応できる範囲を明確にし、相互の実務を理解することが、継続的な信頼の前提となる。

企業間における共助

官民連携や共助基盤として準備しているのが、CIBC（Counter Intelligence Bureau Consortium）である。CIBCは、各企業の内部に埋没している不審接触などのヒヤリハット事案、過去のインシデント等の「埋没した経験・情報資産」を、匿名化した上で業界ごとに共有し、相互防衛に生かす仕組みである。

自社では通常の業務上の出来事に見えた事案も、複数の企業で共有された懸念ケースに紐づくことで、危険な兆候として捉え直せる。参加企業から寄せられた兆候や事例を匿名化・分類し、共有した上で対策へ変換する。情報を蓄積するだけでなく、他社が行動を起こすための材料にするのである。

さらに、業界やテーマごとの分科会で、接触を見逃しやすい場面、確認すべき情報、統制の有効性等を検

話し、得られた知見を再び共有基盤へ戻す。大学・研究機関も、重要技術と人材を守る当事者であると同時に、技術分野の特性や研究活動の実態に関する高度な知見を、この検討に生かすことができるだろう。こうした産官学の情報流通を通じて、単なる情報交換会ではなく、現場の対策を改善し続ける民間カウンターインテリジェンス・コミュニティの形成を目指すのである。

公助のあり方

CIBC では、企業間の共有に加え、官側との継続的な情報共有の場を設けることを想定している。官側が把握したい兆候と、企業側が防護のために知りたい事項をすり合わせ、相互の情報関心に基づく「生の情報」を、対処に間に合う段階で共有する。公表済みの事件の説明や一般的な注意喚起だけではなく、今起きている接触や情報要求を、具体的な確認と対処に結び付ける場である。

ここでいう「生の情報」とは、接触の経緯、要求された情報、現場で感じた違和感等を、判断に必要な文脈とともに匿名化して共有するという意味である。秘匿性の高い情報についても、その全てを共有することを前提とせず、共有可能な範囲で具体性を保ち、企業が自社の記録と照合できる形にすることを目指す。

企業が必要な情報を安心して提供でき、受け取った側がその限界を理解して利用できることが、この基盤を支える。

官民連携インテリジェンス・サイクル

官民連携の場で求められることは、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。官と民がそれぞれ何を知る必要があるかを共有し、関連する情報を持ち寄り、分析した上で、企業が自社内で確認できる警告を形成する。各社は、その警告を社内の各種懸念兆候と照合し、追加確認、証拠保全、当局への相談へつなげる。

対処した後は、確認できたこと、実際に機能した対策、判断に不足していた情報を、共有可能な範囲で官側へ戻す。その結果を次の情報要求、脅威評価、対策の改善に反映する。これにより、企業の経験が他社の防護を支え、官側の情報も現場の反応によって評価を更新できる循環をつくる。

官側が企業に脅威を教えるだけでも、企業が官側に情報を出すだけでも、十分ではない。必要なのは、官側の脅威情報・具体兆候と企業の実装現場を接続し、予防型インテリジェンスを共同生成する官民連携のインテリジェンス・サイクルである。

企業内の自助、企業間の共助、官の情報と対応を通じた公助を、一連の防護行動として機能させることが肝要である。

【特別寄稿】

官民連携による防諜体制の構築に向けての提言

茂田 忠良

国家間の経済大競争の現在、我が国の民間部門の持つ企業秘密等の機微情報を外国勢力から如何に守っていくかは国家的課題であり、そのためには官民連携が不可欠である。官民連携を有効に機能させるためには、何が必要か。米国 FBI による取組と対比して、我が国の課題を述べてみたい。

FBI による検挙事例

先ず、米国における FBI と民間企業の連携関係の実態を見るため、中国による経済スパイの検挙例を2つ例示する。

第1の事案は、2018年8月の鄭小清（ジェン・シャオチン）の摘発である。鄭は、中国の大学を卒業後に、渡米して MIT で学位を取り、米国で就職しやがて米国に帰化していた。鄭は2008年から GE パワー社でタービン・エンジンの技術者として働いていたが、2016年中国に親戚と共にタービン部品の会社を設立し、2018年の検挙に至るまで GE 社の企業秘密を持ち出して中国に送信していたのである。この間、鄭は遼寧省の最高幹部と親交を結び、補助金交付の手続が進んでおり、また「千人計画」にも選ばれていた。

発覚の端緒は、GE 社による社内システムの監視である。GE 社は、2017年末に鄭が使用する業務用コンピュータに大量の暗号化ファイルを発見した。暗号方式が GE 社が使用していない方式だったので、社内監視を強めると共に、FBI 支局に通報したものと見られる。そして社内監視と FBI によるデジタル捜査によって、犯行が解明されたのである。

鄭は、GE 社の企業秘密を暗号化して社内の業務用コンピュータに一時保管し、次にこれを自己の執務室のデスクトップ・コンピュータに送信した。更にステガノグラフィ技術を使って風景写真などに暗号化データを隠匿して、GE 社の自己メールアドレスから自己の Hotmail アドレスへ送信して GE 社外に持ち出し、これを中国の親戚の QQ（中国テンセント社）メールアドレスに送信していたのである。

GE 社のサイバーセキュリティ担当と保全担当、そして FBI 支局の間の密接な連携が印象的である。

第2の事案は、2018年春の江蘇省国家安全庁第6局の徐延軍（シー・ヤンジュン）の囲捜査による逮捕である。江蘇省国安庁第6局は、「国防七子」の1つである南京航空航天大学を場として、国産ジェット旅客機の開発支援のための情報収集工作をしていた。その一環で、GE アビエーション社のジェット・エンジン複合材の研究員デビッド・ジェン（中国出身）は、LinkedIn で勧誘を受け、2017年5月南京航空航天大学で講演をした。ところが、GE 社は企業秘密の漏えいを怖れて外部講演を殆ど許可しないので、ジェンは無許可で講演をしたのである。

FBI は、何らかの方法（シギント活動と推定）によりジェンの南京航空航天大学の訪問を探知して、GE 社の「内部脅威」特別班に連絡を取り対策を協議した。その結果、ジェンは同年11月に GE 社の保全担当官、続いて FBI 捜査官の事情聴取を受けたが、その際に上記大学訪問の事実を隠したのである。このため

に、虚偽供述罪が成立してしまう。連邦職員による事情聴取に対して嘘を吐くのは犯罪（合衆国法典第 18 篇 1001 条）なのである。ジェンは、不起訴を条件に捜査への協力を約束する。この後、ジェンは徐延軍に、一見企業秘密と見える情報（実は GE 社が作成して提供）を送信して信用させて、大量の企業秘密の提供を餌に 2018 年 4 月ベルギーに誘致し、現地当局が身柄を拘束し、同年 10 月に米国への送還を受けたのである。

徐延軍の逮捕は、FBI にとって中国による「対米経済スパイ活動」の実態を立証する画期的な事件であり、GE 社の積極的な協力、そして同社の保全部門と FBI の密接な協力関係が印象的な事件であった。

官民連携の取組：米国と日本

上記の FBI による事件検挙の背景には、一方で、我が国警察とは比較にならない FBI の強力な行政調査権限や司法捜査権限があるが、他方、同時に密接な官民連携が存在する。

米国の官民連携

米国では、外国勢力による企業秘密の窃取は、経済スパイ行為であり、米国経済と米国の経済安全保障に対する脅威と位置付けられている。そして、この脅威に対して、FBI と民間企業が密接に連携する仕組みが構築されている。

この官民連携は、FBI と企業等民間との「戦略的パートナーシップ」であり、協力は双方向である。先ず、FBI は、脅威情報を企業、大学、研究機関、業界団体などに提供する。この情報提供は、一般的な脅威情報や対処方法の助言（公開情報）のレベルと、機微情報（sensitive）や秘密情報（classified）のレベルが存在し、秘密の脅威情報の提供には、企業担当者がセキュリティクリアランスを保持し、且つ need to know があることが前提である。

他方、企業等民間に対して、犯罪の既遂には至らない不審情報の FBI に対する提供を積極的に呼び掛けている。例えば、中国人社員の突然の転職、退職直前の技術資料の大量コピー、海外研究機関からの不自然な共同研究の提案、外国政府関係者からの不自然な接触などである。こうして、「FBI の防諜・捜査能力」と「企業等の保全体制」を接続して、官民共同型の経済安全保障体制を構築しようとしているのである。

実際、FBI の広報動画²⁷では、外国企業やその代理人が社員に対して企業秘密を求めて接触した情報を、いち早く FBI に通報し、それを端緒に捜査により摘発に至る事例が紹介されている。本動画では、民間企業を外国勢力の不当な活動を探知するセンサー（触角）として位置付けており、正に官民共同の防諜エコシステムの構築を目指しているといえよう。また本動画では、企業秘密を守ることが、当該企業の競争力を維持し、地域の雇用を守り、ひいては国家の経済安全保障に繋がることが強調されている。

官民連携のための組織としては、FBI は民間企業との恒常的な統合連絡窓口として、2015 年頃、本部に「民間部門室」（Office of Private Sector : OPS）を設置すると共に、続いて 2016 年頃には全米の 56 支局に「民間部門連絡官」（Private Sector Coordinator : PSC）を設置している²⁸。

²⁷ FBI, "The Company Man: Protecting America's Secrets."

²⁸ FBI, "Office of Private Sector," News, 2 February 2017, <https://www.fbi.gov/news/stories/office-of-private-sector>. 20 世紀においては、FBI と民間企業との連絡窓口は、スパイ対策、サイバーセキュリティ対策、テロ対策、一般犯罪対策など、FBI の現場の専門部署がそれぞれ設定していたが、1 社に対して複数の連絡窓口を設定するのは合理的でないで、全ての窓口を 1 つに統合したのが FBI 本部の OPS、支局の PSC である。同時に、より高位の企業幹部との連携機能を図るものでもある。それ以前、2000 年代後半から、FBI

また、FBI 本部では全国組織として「国内安全保障連携協議会」（Domestic Security Alliance Council : DSAC）を 2005 年に設置している。これには現在、FBI、国土安全保障省、重要大企業 800 社以上が参加しており、企業のセキュリティ担当最高幹部に FBI へのアクセスの場と共に、企業同士の経験交流・情報共有の場を提供している。

なお、このような FBI による官民連携、官民「戦略的パートナーシップ」構築の背景には、米国 ODNI（国家諜報長官室）の策定した「国家防諜戦略」（National Counterintelligence Strategy 2024）もあり、同戦略は、連邦・州・地方政府機関、民間企業、学术界、一般国民等の社会全体による協調したカウンターインテリジェンスの取組（whole-of-society approach）を呼び掛けている。

日本の官民連携

警察庁は、警備局外事課に経済安全保障室を設置して、FBI など諸外国の例も参考にして、官民連携「アウトリーチ活動」に取り組んでおり、その目指すところは FBI と同様ではないかと推定する。

但し、警察庁の公式文書を見ると、2025 年 5 月に警察庁外事課長通達「経済安全保障に係るアウトリーチ活動の推進について」が発出されているが、内容は開示されていない。そこで、警察庁の警察白書や警備局の「焦点」などの公刊資料を見ると、「アウトリーチ活動」とは、先ず「技術情報等を扱う企業等の自主的な対策が欠かせない」とした上で「捜査等を通じて把握した外国からの働き掛けの手口に関する情報やその対策に資する情報を提供する」活動（＝情報提供活動）と定義しており、米国の様な「戦略的パートナーシップ」の構築までは公式には打ち出していない。

提言

以上で述べた米国の状況を前提に、経済安全保障のための官民連携を進めて行く上で、特に重要と考える点を 2 点述べたい。専門人材の確保と警察からの提供情報である。

専門人材の確保

上記の米国における 2 つの検挙事例で分かるのは、企業等民間側に保全の専門部署があり保全の専門家がいて、FBI と緊密な連携が取れている点である。先ず、民間企業等が秘密保全の重要性を認識して、経営者に直結する保全専門部署を設置することが重要であるが、仮に設置したとしても、そこ専門人材がいなくては機能しない。ところが、我が国では専門人材は圧倒的に不足している。

そこで、警察（警察庁・都道府県警察）としては次の 3 つ方法で、企業等民間側に人材の供給に努めるべきであろう。

- ① 派遣・出向の推進～国公立大学や一般官庁で、保全責任者（security officer）の派遣・出向を希望する組織に対しては、積極的に職員の派遣・出向を行うべきである。実際、米国では、FBI 出身者が他官庁の保全部署で勤務している例も多いようである。

の counter-intelligence 部門は、民間協力の窓口として Strategic Partnership Coordinator（SPC）を設置していた。現実の人事を見ると、SPC を基にして PSC に発展させた例が多い様である。

- ② 退職者の再就職～現職時に外事警察など経済安全保障の知見がある者に対して、企業の保全責任者への再就職を奨励すべきである。但し、現職時の経験者と言っても、警備警察部門の業務は秘密保全のための著しく縦割りであるので、民間企業に必要な知見を全て有している場合は少ないであろう。従って、再就職前に一定の教育を提供する必要がある、そのような再教育の仕組を組織として責任を持って構築するべきである。また、その際、官側の論理を押付けずに、企業ニーズや課題への認識を深めるためには、民間経験者による講義も必要であろう。これは上記①の場合も同様である。
- ③ 途中退職者の支援～警察の現場の業務は夜間休日の活動が多く、家族などの事情から退職する者もいる。実際、FBI でも同様の理由で退職して民間企業の保全責任者に再就職する事例は相当にあると見られる。警察は途中退職者と疎遠になる傾向があるが、民間企業に再就職した途中退職者もアルムナイ（OB・OG、同窓）と位置付けて適切な関係を維持するべきである。

次に、警察の官民連携担当者の人事についても、検討を要する。

先ず、民間連携担当部署については、単に担当部署を定めるのではなく、連携担当官を定め、長期の在任期間を確保すべきである。民間とは顔の見える関係を構築する必要がある、また、民間側の立場にも十分に理解を深める必要がある。そのためには、相当長期の在任期間が必要である。また、「官民間の人材循環」（いわゆる「revolving door」）も検討すべきである。実際、FBI の初代「民間部門室」長に就任した Brad Brekke 氏は、元々FBI の特別捜査官(special agent)であったが途中退職して、巨大小売企業 Target の保全部門に再就職し、同社の最高保全責任者を 10 年以上務めた人物である。同氏が選ばれたのは、FBI と民間企業の双方での勤務経験を有し、双方のニーズと関心を熟知しているため、適任者と評価されたためである。このような柔軟な人事を、見習うべきであろう。

警察からの情報提供

次に、警察からの情報提供の質の向上も必要であろう。

先ず第 1 に、公開情報（一般的な脅威情報や対処方法の助言）の向上である。大府県警察は脅威情報や対処方法に関する情報も、自ら十分保持していると思われるが、地方の中小県警は自らの情報では不足があり、警察庁が発信する情報に頼らざるを得ないと思われる。FBI のウェブサイトを見ると、その情報量の豊富なことには驚くほどである。警察庁も、より一層の努力が期待される。

第 2 に、機微情報や秘密情報の提供である。民間の方の話を伺うと、一般的な脅威情報や対処方法はもう十分であって、当該企業に関係し対策に役立つ情報（relevant & actionable information）を欲しいという声を聞く。既述したように、米国では、FBI は、機微情報（sensitive）や秘密情報(classified)も一定の枠組の中で、民間部門にも提供している。

警備警察における経済安全保障の取組の目的は、企業秘密等の機微情報の国外流出の阻止であって、事件検挙はそのための有効な手段ではあるが、事件検挙自体が目的ではない筈である。従って、警備情報活動によって入手した情報を、適切な形で個別の企業や民間組織と共有して、民間側の対策を促進して企業秘密などの機微情報の国外流出を未然に防止することは、警察法第 2 条の警察の責務に適う活動である。

一部の県警では、企業や民間組織に機微情報を提供している事例があるかもしれないが、重要なのは、機微情報や秘密情報の提供の制度・枠組を定めて、全国的に斉一の制度として実施することである。FBI はこ



の点において、相当の取組をしており、我が国も米国の例に学ぶべきであろう。なお、秘密情報の提供に際しては、旧公務員について現職時に特定秘密保護法上のセキュリティクリアランスを保持していた者に限定するなど、秘密保持についての工夫も求められよう。

第8章 おわりに



本稿では、諜報の歴史と現代の手口・事例を踏まえ、企業・組織が担う CI のあり方を検討してきた。技術進展により手段が変化しても、人や組織への働きかけを通じて情報を得ようとする活動への備えは欠かさない。

企業に求められるのは、国家の情報機関と同じ活動を行うことではなく、自社が担う CI 上の「阻止」と「探知」を機能させることである。同時に、自社だけでは意味を捉えきれない兆候を、他社の経験と官側の情報によって評価し直すことが重要である。

自助・共助・公助は、互いに責任を委ねるための区分ではない。それぞれが持つ情報と機能を補い合い、被害を未然に防ぐ行動につなげるための枠組みである。

CI の目的は、重要な技術とそれを担う人材を守ることである。

『何を守り、どのような働きかけに備え、兆候を捉えたときにどう動くのか』

本稿が、この問いを社会で共有し、具体的な対策へ踏み出す契機となることを期待する。

以上

執筆者の紹介

茂田忠良

1951 年生まれ。1975 年東京大学法学部卒。1980 年米デューク大学大学院修士。1975 年警察庁入庁。警察庁では警備企画課長、政策評価審議官など主として警備・国際部門で勤務。群馬県と埼玉県で警察本部長、四国管区警察局長など。警察外では、在イスラエル日本大使館一等書記官、防衛庁陸幕調査部調査別室長・情報本部電波部長、内閣衛星情報センター次長を歴任。ヒューミント、シギント、イミントのインテリジェンス主要三分野を現場で経験した実務家。退官後にインテリジェンス研究（特にシギントとセキュリティサービス）に従事。2016～22 年日本大学危機管理学部教授。江崎道朗氏との共著に『シギント』。その他論文や月刊誌への寄稿多数。

上田篤盛

Fortis Intelligence Advisory 株式会社 シニアフェロー

元防衛省情報分析官

1984 年、防衛大学校卒業。同年、陸上自衛隊入隊。1987 年以降、情報関係職に約 30 年従事し、2015 年退官。退官後は民間企業でコンサルタント、研究員として勤務。著書に『戦略的インテリジェンス入門』『未来予測入門』『武器になる情報分析力』『台湾有事 日本企業が「戦場」になる』など多数。官公庁や民間企業を対象に、情報分析、インテリジェンス、シナリオプランニングなどをテーマとした講演・研修も行っている。

藤谷昌敏

Fortis Intelligence Advisory 株式会社 シニアフェロー

元公安調査庁 金沢事務所所長

学習院大学法学部、北陸先端科学技術大学院大学卒、知識科学修士。元公安調査庁職員として、中国、北朝鮮、ロシア、国際テロ等に関する情報収集・調査分析に長年従事し、金沢公安調査事務所所長で退官。現在、金沢工業大学産学連携室主任研究員・明倫館教授、日本戦略研究フォーラム政策提言委員。経済安全保障をめぐる国際情勢、経済依存と国家間競争、技術流出・技術安全保障、情報戦・認知戦、企業・研究機関の危機管理などを幅広く扱い、実務経験に基づいた執筆・講演を行っている。著書『経済安全保障と「経済インテリジェンス」』芙蓉書房出版（2026）など論文多数。

稲村悠

Fortis Intelligence Advisory 株式会社 代表取締役

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謀報事件捜査に従事した経験を持つ。警視庁退職後は、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。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など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）、『防諜論』（育鵬社）ほか

川下巧

株式会社エルテス 執行役員 IRI 事業本部 本部長

経済産業省認定資格 情報セキュリティスペシャリスト保有（現情報処理安全確保支援士）。新卒にてエルテスに入社し、IRI の立ち上げメンバーに選抜。多数の企業に対して、内部不正のリスクマネジメント支援を行い、IRI 事業の責任者を務める。