TOKIO MARINE

リスクマネジメント最前線

2025 | No. 5

地政学リスク分野の公開情報分析と企業のインテリジェンス態勢構築

小原 凡司（一般社団法人 DEEP DIVE 代表理事）
笹川平和財団 上席フェロー。専門：現代中国政治（外交・安全保障）。
小泉 悠 （一般社団法人 DEEP DIVE 理事）
東京大学 先端科学技術研究センター 准教授。専門：ロシアの軍事・安全保障。
川口 貴久（東京海上ディーアール株式会社 ビジネスリスク本部 兼 経営企画部 主席研究員、マネージャー）
一橋大学 法学研究科 非常勤講師。専門：国際政治・安全保障、リスクマネジメント。*

要約

- 「インテリジェンス（intelligence）」と「インフォメーション（information）」はいずれも「情報」と訳されるが、両者は明確に区別される。インフォメーションが単なる事実や生の情報を指すのに対し、インテリジェンスとは、特定の目的や文脈のために加工（解釈・評価）された情報であり、意思決定や行動のためにある。
- 公開情報（open-source）であっても、複数の公開情報を組み合わせ、的確な関心領域・地域（Area of Interest: AOI）を選定することで、精度の高いインテリジェンスを生成することができる。ロシアによるウクライナ全面侵攻（2022 年 2 月～）や近年の中国人民解放軍の軍事演習を例にあげても、公開情報分析によって、民間企業の意思決定や行動に資する短期的動向・予兆や中長期の見通しを生成可能だ。
- 実際の民間企業・組織内でインテリジェンスを生成するための初期態勢構築に必要な要素は、①対象範囲の設定、②情報収集先・リソースのリストアップ、③必要な行動・選択肢の洗い出し、④組織体制構築である。

目次

* 小原が「1.公開情報分析（OSINT）とは」「2.（2）近年の中国の軍事演習とその意図」、小泉が「2.（1）ロシアによるウクライナ全面侵攻とその予兆」、川口が「はじめに」「3.企業におけるインテリジェンス態勢構築」を主に執筆した。

はじめに

第二期トランプ政権による政策転換、両岸（中台）の政治・軍事情勢、ウクライナや中東地域の武力紛争等、地政学リスクが顕在化する中、多くの企業が地政学リスクに関するインテリジェンス態勢を構築しようとしている。

インテリジェンス（intelligence）とは、特定の目的や文脈のために、インフォメーション（information）を加工（解釈・評価）したものである。インテリジェンスは、何らかの意思決定や判断のため、行動のため（もしくは行動しないため）に存在する。

身近な「明日の天気」で例えるならば、「ツバメが低く飛んでいる」という事実はインフォメーションである。しかし、「明日の外出予定をどうするか？」という目的・文脈を踏まえると、「明日は雨が降るかもしれない」というインテリジェンスが生成可能である（本稿はツバメと天気の相関・因果関係を主張するものではなく、あくまで例である）。このインテリジェンスの生成は口伝や経験則から導き出されるものだが、地政学リスクのインテリジェンス生成には当該分野における膨大な専門的知識の蓄積、妥当な因果推論といった「情報処理装置」「分析装置」[1]が必要である。

加えて、このインテリジェンス生成には「明日の外出予定をどうするか？」というインテリジェンス要求が先立ち、「明日は雨が降るかもしれない」というインテリジェンスを踏まえて、「傘を持参する」「カッパを着る」「予定を延期する」などの意思決定・判断と行動を伴う（表 1）。

つまり、企業のインテリジェンス態勢構築には、図 1 のように、①「インテリジェンスの活用者」側の態勢、すなわち、そもそもインテリジェンス生成の目的（インテリジェンス要求）やインテリジェンスを活用した意思決定・行動、②「インテリジェンスの生成者」側の態勢、つまりインフォメーションからインテリジェンスを生成するための体制・プロセス（公開情報の「情報処理装置」「分析装置」等）を整備する必要がある。

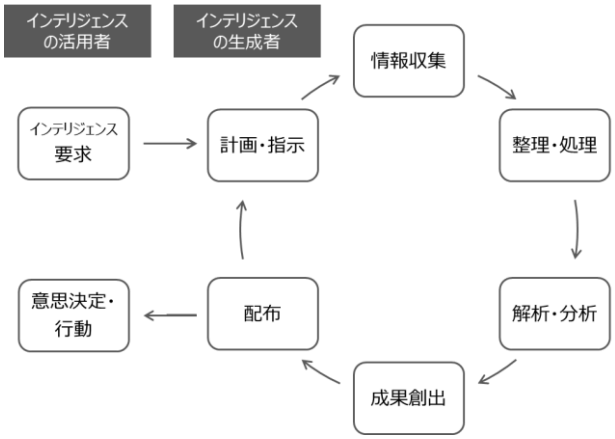
本稿では、地政学リスクに関する公開情報をベースとしたインテリジェンス、個別具体的な分析の例、企業における初期態勢構築のポイントを紹介する。

■ 表 1 ：身近なインテリジェンス

インテリジェンス要求（目的）	• 明日の予定と携行品を確認したい
インフォメーション	• ツバメが低く飛んでいる 等
インテリジェンス	• 明日は雨が降るだろう 等
意思決定・判断	• 傘を持参する • カッパを着る • 予定を延期する 等

出典：筆者作成。

■ 図 1 ：インテリジェンス・サイクル



出典： “The Intelligence Production Cycle,” Iowa Department of Public Safety を基に作成。

[1] 小泉悠『情報分析力』（祥伝社、2024 年）。

1．公開情報分析（OSINT）とは

一般に、民間の組織が情勢分析を行う際、政府機関が秘区分を付した情報を用いることはできない。そのため、民間の組織は公開情報分析（Open-source Intelligence: OSINT）を行うことになる。しかし、秘区分のない公開情報であっても、分析の精度を上げることは可能である。

ただし、例えば、1 枚の衛星画像にも多くの情報が含まれているが、そのような単一の公開情報だけを用いた分析結果の精度は十分に高いとは言えない。衛星画像に分析対象となる軍事施設や装備品が写っていたとしても、画像で確認できるのは、その時点での外観である。特徴的な外観であれば、その装備品の性能を推測することはできるだろう。しかし、その装備品の開発計画や進捗に係る政府や企業の発表、および報道等の内容を分析していれば、外観の特徴の分析と併せて、性能評価等の精度は上がる。

情報分析において、複数の種類の情報を用いることは、分析の精度を上げるために非常に重要である。異なる種類の情報やデータを統合して処理するシステムや手法を指す、「マルチモーダル」という言葉はインテリジェンスの世界だけでなく、自動運転等の交通システム、医療システム、製造業、さらには AI（人工知能）の分野でも盛んに用いられるようになっている。

米国国家情報長官室（Office of the Director of National Intelligence: ODNI）によれば、インテリジェンス・サイクルとは、インフォメーションを収集し、政策決定者や指揮官等が利用できるインテリジェンスに発展させるプロセスであり、指示・指向、収集、処理・分析、利用、拡散の段階があるとされる。また、インテリジェンスには表 2（次頁）の通り、主として以下の 6 つの種類があるとしている。

この他に、音響情報を示す ACINT（Acoustical Intelligence）という言葉もある。これらの分類は厳密に区分される訳ではない。例えば、IMINT に分類される衛星画像分析についても、民間企業が販売する衛星画像を用いれば OSINT に分類することができる。こうした情報は「市販情報（Commercially Available Information: CAI）」とも呼ばれる。

SIGINT は特に機微な内容を含み、また軍事装備品が発する電波の周波数帯と家電を含む民間で使用される電子装備品の周波数帯が似通っていることも多く、装備を特定するためには、電波情報を収集する以前に、対象となる装備品それぞれの詳細な電波諸元を得ていなければならない。

こうした特性から、SIGINT を OSINT 分析で使用することには限界がある。しかし、例えば、衝突防止のために船舶に搭載が義務付けられている自動船舶識別装置（Automatic Identification System: AIS）の情報は SIGINT に分類できるが、民間でも販売されており、OSINT として利用できる。AIS 情報を用いれば、外洋を航海する 300 トン以上の船舶、500 トン以上の全ての船舶の航跡や入港した情報を過去に遡って得ることができる。

一方で、軍艦および専ら漁業に従事する船舶等は適用除外とされており、AIS 情報から海軍艦艇の航跡等を得ることはできない。また、AIS 情報は、船舶の戸籍とも言われる IMO ナンバー（国際海事機関（IMO）が個々の船舶、船舶所有者、船舶管理者に与える番号）以外の情報を手動で書き換えることができ、位置情報等が正確である保証はない。

しかし、先述のように、AIS 情報と他の種類の情報を統合して分析を加えることにより、軍艦の位置情報に関する分析の精度や効率を上げることは可能である。例えば、合成開口レーダー搭載衛星（SATSAR）を用いて、特定の海域に占位する艦船を探知することは可能であり、全ての探知目標から AIS 信号を発信していない艦船を抽出すれば、それらは、海軍艦艇を含む、AIS 搭載の適用除外とされる艦船である。

一種類の情報に見られた兆候等は、他の情報によって裏付けされ、補完されることも多い。政府が保有する多くの情報とは異なり、自ら能動的に探知して取得するのではなく、すでに存在する情報を探して取得することが多い公開情報分析には、どこに必要とされる情報があるのかについての背景情報の理解が不可欠である。

公開情報は政府が保有する秘区分を付された情報と比較して精度に欠けることが多いが、単独の公開情報が詳細な内容を示していなくとも、他の種類の情報と統合して分析することによってその不完全性を補完でき、評価の精度を上げ、有効なインテリジェンスを導くことができる。さらに、同一の地点や対象物、イベントを継続して監視することにより、変化のパターンを特定できれば、将来の動きを予測することにもつながる。

いずれにしても、特に公開情報分析においては、的確な関心領域・地域（Area of Interest: AOI）の選定が重要である。世の中には膨大な量の情報が出回っており、何を見れば将来の事象を予測できるのかを理解していなければ、必要な情報に触れることも難しい。そして、的確な AOI を選定するためには、地域研究等によって当該地域に関する理解を深めておく必要がある。こうした準備を行い、適切な手法を用いれば、公開情報分析から得られる有益な情報は多い。

■ 表２：様々なインテリジェンス

分類	概要
SIGINT	Signals Intelligence。個別であれ組み合わせであれ、捉えた信号から導き出されるインテリジェンスであり、全ての COMINT、ELINT、FISINT を含む。
COMINT	Communications Intelligence。電話やメール、無線等の通信手段による会話や、オンラインでのやりとりから情報を収集する活動または通信内容に関わる情報。
ELINT	Electronic Intelligence。レーダー波やミサイル誘導電波等を含む電磁波を傍受・分析する活動およびその情報。
FISINT	Foreign Instrumentation Signals Intelligence。SIGINT、COMINT、MASINT のサブカテゴリー。航空宇宙、地上、地下システムの試験や運用配備に関連する海外からの電磁放射を傍受・分析する活動およびその技術情報。
IMINT	Imagery Intelligence。電子的または光学的手段によって画像を収集し分析する活動およびその情報。画像は、光学カメラ、レーダー・センサー、電気工学的手段によって得られ、フィルム、電子ディスプレイ、その他メディア上に再現。IMINT の中でも衛星画像分析は、光学衛星や SATSAR 等によって対象を撮像した画像を分析する。
MASINT	Measurement and Signature Intelligence。ターゲットおよびイベントの物理的属性を定量的および定性的に分析し、それらの特徴付け、位置特定、識別を行うことによって生成される情報。
HUMINT	Human Intelligence。人間の情報源から情報を取得する活動およびその情報。HUMINT にはスパイや秘密工作のイメージがあるが、その大半は、駐在武官等の報告や対象国への出張者からの聞き取り等、公然と行われている。HUMINT は最も古い情報収集方法であるが、現在でも、主要な情報源である。
OSINT	Open-Source Intelligence。ラジオ、テレビ、新聞、雑誌、インターネット、商用データベース、ビデオ、グラフィック、図面等、印刷物または電子的に公開されている情報を収集・分析する活動およびその情報。
GEOINT	Geospatial Intelligence。地球上の安全保障に関連する活動を分析し、視覚的に表現する情報活動および表現された情報を意味し、画像、画像情報、地理空間情報を統合して作成される。

出典："What is Intelligence?" Office of the Director of National Intelligence (2025 年 3 月 24 日アクセス)を基に筆者作成。

2．ケース･スタディ： 公開情報分析から何が分かるのか

本パートでは公開情報分析を用いた 2 つの具体的な事例を紹介する。1 つは多くの民間企業にとって大きなサプライズとなったロシアによるウクライナ全面侵攻（2022 年 2 月～）であり、もう 1 つは現在進行形で多くの日本企業が注視している中国人民解放軍による軍事演習である。

（1）ロシアによるウクライナ全面侵攻とその予兆

「意図」と「能力」

ロシア軍のウクライナ侵攻作戦はおよそ 1 年かけて準備された。2021 年初頭から春頃に掛けて、ロシア軍がウクライナ国境周辺に集結しているとの報道が見られるようになったものの、夏になって一時的に「撤退」と報じられた。しかし、この時点でロシア軍は一部の重装備を残置していたと見られる。その後、秋になるとロシア軍は再びウクライナ国境周辺への集結を開始し、「侵攻はあり得るか」という議論が盛り上がることになった。

ここで一般的に問題とされたのが、「意図」である。プーチン（Vladimir Putin）大統領は実際のところ何を考えているのか。合理的に考えれば多大な経済的損失をもたらす侵攻を決断することはあり得ないのではないか。侵攻の危険性を主張しているのは主に米国であるが、その見方はどこまで正しいのか。米国の反露プロパガンダに過ぎないのではないか。あるいは侵攻はあり得るとしても、ごく限定的なものとなるのではないか。大雑把にまとめれば、当時の争点はこのような形に集約されよう。

しかし、現実問題としてロシアは侵攻に踏み切った。ここから導き出される第一の教訓は、合理的選択を前提とする平時の論理は必ずしも常に妥当ではない、ということである。少なくとも「合理性」なるものは経済的な損得勘定とイコールに見做せるという保証は、軍事的危機事態においては存在しない。

第二に、かかる事態において「意図」を外形的に把握することはまず不可能であると考えなければならない。プーチン大統領が何を考えているのかを高い確度で知ることができるのはおそらくロシア政治指導部の限られたインナーサークルだけであり、大国の情報機関ならばまだしも、民間の意思決定においてはまず不可能であると想定しておかねばならない。さらに言えば、ロシアのような権威主義国家においてはインナーサークル内部でさえ指導者の本当の意思が共有されているとは限らないし、指導者自身も最後の瞬間まで決断を保留している可能性もある。

したがって、第三に、軍事的危機事態においては「能力」が問題になる。相手の意図を察知することは困難であるとしても、軍事侵略のような大規模な作戦を行うには大掛かりな準備が必要であって、その規模を知ることができれば「可能行動」、すなわち「決断すればできることの上限」はある程度まで推し量ることが可能である。言い換えるなら、「プーチンは戦争に踏み切るのかどうか」ではなく「もしもプーチンが戦争を命令した場合、ロシア軍はどこまで戦争ができるのか」を基準にものを考えるということである。以下、ロシアのウクライナ侵略に先立って観察された「能力」とその分析手法について紹介してみたい。

ウクライナ侵略に先立って察知された兆候

前述のように、ロシア軍のウクライナ侵攻は約 1 年をかけて準備されていた。しかも、商用衛星サービスの普及によって、その兆候はマスコミや研究機関等の民間セクターによってもかなり幅広く把握されていた。

ロシア軍は約 15 万人から 18 万人程度の兵力で侵攻したと見られるが、平時のロシア陸軍は 28 万人程度に過ぎない。海軍歩兵部隊や空挺部隊を加えてもロシア軍の地上兵力は 36 万人程度であったから、15-18 万人という兵力は、徴兵主体の低練度部隊を除いた常時即応部隊のほぼ全てであったと思われる。それゆえ、ロシアは欧州正面の部隊だけでなく、シベリアや極東からも広範に部隊をかき集める必要があった。この結果、ロシア西部の駐屯地では、域外から展開した部隊のテントや装備品が敷地外にまで溢れ、衛星画像によって明瞭に把握することが可能であ

った。これらの展開地域の多くはウクライナとの国境（または 2014-15 年の紛争によって生まれたウクライナ東部の停戦ライン）から 150-250km 程度の距離に位置していた。

また、これらの地域においては、航空機の集結も確認された。特徴的だったのは、平時から運用されている主要軍用飛行場のみならず、普段使用されていない予備飛行場（特にウクライナ国境に近いベラルーシの予備飛行場）においてもこの現象が見られたことである。予備飛行場に展開したのは Su-25 攻撃機等の戦術航空機であり、おそらくは航続距離の短さを補うための措置であったと思われる。加えてヘリコプターについては予備飛行場だけでなく平原に設けられた臨時飛行場も使用した。

他方、シベリアや極東の駐屯地からは多くの装備品が姿を消したことがやはり衛星画像によって観測されていた。ウクライナ正面へと転用されたと見られるが、それらを運ぶ貨物列車は沿線住民のスマートフォンによって撮影され、やはり重要な手がかりとなった。特に 2022 年に入ってからは東部軍管区の部隊が大挙してベラルーシへと展開し、東部軍管区司令官も現地入りするなど、過去の演習では見られなかったほどの大規模な戦域間機動が実施されているとの未確認報道が見られるようになった。ロシアが通常の演習を超えた大規模軍事作戦を企図していることがほぼ確実と考えられるようになったのはこの時期である。

このように、「能力」を基礎とする分析は、ロシア側の「意図」が不明瞭な中でも一定の役割を果たした。すなわち、ロシアは当時の保有軍事力によって想定される中でほぼ最大規模の軍事作戦を準備していたことが外形的に把握されていたのであり、実際の展開は可能行動のほぼ上限一杯に相当するものであった。

限界と今後の展望

他方、「能力」に基づく分析には限界も多かった。

最大の問題は天候である。2 月の欧州は厚い雲に覆われる日が多く、光学衛星のみによってはロシア軍の展開状況を継続的に観測することが難しかった。また、当時の商用衛星画像サービスでは運用衛星の数が限られており、撮像頻度も高かったとは言えない。したがって、衛星画像分析はリアルタイムの追跡とはならず、時期の異なる観測結果を繋ぎ合わせたパッチワーク的なものとならざるを得なかった。ただ、この点は、天候に左右されにくい合成開口レーダー（SAR）衛星の普及とそのコンステレーション化、商用光学衛星の増勢によってある程度緩和されつつある。

第二に、開戦直前になると、ロシア軍の動きを衛星画像分析で把握することがさらに困難になった。ロシア軍の多くが集結地点を出て国境付近の攻撃発起位置に展開すると、入念な偽装と分散措置を施すようになったためであると考えられる。電波発信源を人工衛星搭載センサーによって把握する電波インテリジェンス（ELINT）が商用化され始めたことにより、偽装・分散した部隊を観測できる可能性はあるが、軍事作戦開始前の部隊は電波封鎖を行うのが一般的であり、あまり多くを期待すべきではない。ここまで述べたアプローチで可能なのは「軍事的危機事態に向けてどれだけの能力が蓄積されているか」を把握することまでであり、作戦・戦術レベルでの部隊展開や具体的な開戦タイミングまで把握するのは依然として簡単ではないと考えておくべきであろう。

最後に、衛星画像分析は大国の政治的思惑に対して完全に中立ではいられないという点を指摘したい。これまでの商用衛星画像は米国企業によって提供されることが多かったが、それゆえに米国政府にとって都合が悪いと見做された地点・時期には意図的に衛星画像が利用できなくなることがままあった。将来の東アジア情勢を踏まえると、今後、同盟国を含む他国の思惑に左右されにくい、我が国発の商用衛星画像サービスの更なる発展が期待される。

（２）近年の中国の軍事演習とその意図

近年、中国人民解放軍が軍事演習の方法を変えている。あるいは、中国が軍事戦略を変えたと言った方が良いかも知れない。中国が、軍事演習の戦略的コミュニケーションとしての意義付けを変化させたように見受けられるのだ。

台湾政府やシンクタンク等の分析によれば、2023 年から 2024 年にかけて、中国の軍事力を用いた情報影響工作の目的は、台湾社会の「戦争に対する不安・恐怖」を煽ることにあった。中国は、自らの軍事力の強大さをイメージとして誇示することを重視していたのである。

中国は機会を捉えて、台湾に対して軍事的圧力をかけてきた。2023 年の台湾総統選挙期間中、中国は民進党候補の頼清徳氏の当選を阻止するために圧力をかけた。中国は、中国と台湾の中間線を越えて多数の戦闘機、爆撃機、無人機を飛行させるだけでなく、「中国が台湾に軍事侵攻すれば米軍は逃げ出す」などの「疑米論」を含むディスインフォメーションを流布するなどして、中国軍の強大さをアピールした。

2024 年、頼清徳氏が台湾総統に就任すると、中国は同氏に「台湾独立主義者」のレッテルを貼り、同氏の言動を捉えては軍事演習を繰り返した。例えば、2024 年 5 月、頼清徳氏の台湾総統就任演説に反応して、「聯合利剣 2024A」を行った。また、同年 10 月には、双十節（台湾の国慶節）に行われた頼清徳総統の演説の内容を不服として、「聯合利剣 2024B」演習を行った。頼清徳氏の両方の演説は、蔡英文前総統が述べた内容を踏襲したにも関わらず、である。

これら 2024 年に行われた演習では、大規模な部隊展開は見られない。また、公表された演習海空域に緯度経度は示されず、航行警報も発出されていないことから、実弾射撃も実施されていないと考えられる。一方で、これら演習の際、中国人民解放軍東部戦区司令部は、演習海空域のイメージ図を公表し、中国の軍事力が台湾を取り囲むという印象を与えようとした。

さらに、同司令部の統合メディアセンターが動画を作成し、中国の軍事力が台湾を締め上げ、最後には血の海に沈めるというメッセージを伝えた。公式発表、報道、動画等で軍事力を誇示する手法は、情報影響工作の性格が強いと言える。もう一つ、中国は、台湾以外の国々に過度の緊張をさせないよう、軍事行動の説明を積極的に行ってきたという側面もある。

しかし、2024 年末から中国はイメージを用いた情報影響工作を止めたように見受けられる。中国国防部は、2024 年 12 月 10 日、事前通告なく、同月 9 日から 11 日の間、浙江省や福建省の東部空域に 7 か所の「保留区」を設定したと発表し、台湾政府関係者によれば、90 隻にも上る中国艦艇が第一列島線に展開された。

さらに、同月 13 日、中国国防部報道官は、記者会見において、「演習を行うかどうかは、自身の必要性と闘争の形勢に基づき自主的に決定する」と述べ、軍事行動の目的を演習だと明言しなかった。中国は、「自分たちが演習するかどうか、あなた方には関係ない」と言ったに等しい。こうした態度は、これまで、動画まで用いて演習の実施を大々的にアピールしてきたのとは大きく異なる。

この一回だけであれば、中国が軍事力を用いる目的や戦略を変えたかどうかは判断できない。特異な背景があって、軍事演習をアピールしなかったとも考えられるからだ。しかし、この軍事行動は特異点ではなかった。

中国海軍の 055 型駆逐艦、054A 型フリゲートおよび 903A 型補給艦の 3 隻が、事前通告なしに、オーストラリア、ニュージーランドおよびタスマニアに囲まれたタスマン海において実弾射撃訓練を行ったのである。報道によれば、少なくとも 49 の民航機が航路変更を余儀なくされた。

さらに中国艦隊は、タスマン海での実弾射撃の後、南西進してメルボルンやタスマニアの南方に達し、オーストラリアの南側を西進して中国に帰投した。055 型駆逐艦は射程 1500km の対艦・対地ミサイルを搭載しており、周回航行することによってオーストラリアの主要都市を全て攻撃できることを示し、威嚇したとも言われる。

中国海軍はまた、タスマン海における実弾射撃と同日にベトナム沖のトンキン湾で射撃訓練を行い、26 日には、やはり事前通告なしに台湾南西海域に演習海域を設定し、実弾射撃を行った。中国は、突然、他国の眼前に軍事力を展開して、それらの国々を驚かせ、震え上がらせようとしているようだ。

こうした中国海軍の行動は米国の同盟国等に対する威嚇であるが、中国メディアは、タスマン海等における行動には他の目的もあるという。こうした軍の行動は、中国が海洋強国になるという主張であり、海洋の秩序形成における支配的プレイヤーであることを示すものだというのである。

軍隊の行動は様々な戦略的コミュニケーションに使用される。説明によって、あるいは説明しないことにより、他国の認識に影響を与えることができるのだ。中国が、自らが世界秩序を形成するアクターであることを主張するために、ターゲットとした国々を驚かせ、大きな反響を引き起こすことを企図するのであれば、今後も、大々的に軍事演習等をアピールし、事前通告しないことが予想される。

そうなれば、中国の軍事行動を早期に予測することは、より困難になる。どの地域で演習を行うかさえ予測することは難しく、また、予測できたとしても監視すべき地域は広大である。中国の軍事行動を予測するためには、大規模な軍事行動の前に軍事基地等に見られる、戦力の集中や補給活動等、戦略的兆候を検知することが現実的である。例えば、中国が台湾周辺で軍事行動を起こす際には、東部戦区海軍の基地に所在する艦艇に増減が見えるだろう。航空基地にも動きが見えるかも知れない。

図 2 は、中国人民解放軍東部戦区海軍の舟山保障基地の衛星画像である。画像を見ると、一部の桟橋の色が異なることが分かる。より白い桟橋は、新たに建設されたか改修されたことを意味する。同基地の衛星画像を継続的に見てきた結果、2021 年 3 月には、同基地に 2 本の桟橋を新設する工事が行われていることが確認されている。これらから、中国海軍は同時期から、少なくとも舟山保障基地における水上艦艇の増強を想定していた。

■ 図 2：中国東部戦区海軍舟山保障基地

出典：Google Earth。詳細な分析結果は本文を参照。

しかし、中国人民解放軍の基地は数多く存在する。中国海軍は他の海軍基地でも桟橋等の施設の増設や改修を行っており、その全てを継続して監視するためには、高額な費用と多数の分析員が必要になる。さらに、地域研究等に基づく背景情報を得た上で、監視すべき基地や施設を絞り込む必要もある。1 枚の衛星画像は、その時点のその地域の状況を切り取るに過ぎない。将来の状況を正確に予測するためには、他の情報を統合して分析する必要がある。

3．企業におけるインテリジェンス態勢構築

2 つのケース・スタディからは、2 種類のインテリジェンスが生成可能であることが示唆される。一つはケース（１）に代表されるような、対象となる地政学リスクの**短期的動向・予兆**である。これは企業の危機管理や事業継続に必要なものである。もう一つはケース（２）の通り、対象の地政学リスクに関する**中長期の見通し**である。中長期の軍事能力の向上は地域の武力紛争の可能性を高め、特定の国・地域や領域における投資判断やバリューチェーンの見直しに資する可能性がある。

本パートでは、こうしたインテリジェンスを民間企業・組織内で実際に生成するための初期態勢構築について紹介する。インテリジェンスは企業の意思決定・行動に用いられるものであるため、検証可能性や説明可能性を重視したインテリジェンス態勢が構築されなければならない。「誰も知らない秘密情報」だけで判断・意思決定を下すことは企業に期待されるインテリジェンスではない。初期態勢の構築に最低限必要な要素は、①対象範囲の設定、②情報収集先・リソースのリストアップ、③必要な行動・選択肢の洗い出し、④組織体制構築・ネットワーキングである。

■ 図３：企業内でのリスク・インテリジェンスの初期態勢構築に必要な要素

対象範囲の設定	情報収集先・リソースのリストアップ	必要な行動・選択肢の洗い出し	組織体制構築
• インテリジェンスに関する経営層からの要求・指示の実現可能な形での（再）設計、的確な関心領域・地域（AOI）の選定 • 「分かること」「分からないこと」の見極めが重要 • インテリジェンスの対象事象に関連する事象の洗い出し・構造化	• 市販情報（CAI）を含む公開情報および非公開情報の整理 • メディア、行政機関、シンクタンク等のリソースに加えて、領域ごとの専門家リストも有用 • 非公開情報は、政治家・政策当局者、同業他社・業界団体、外部専門家 等	• インテリジェンスをふまえての行動・選択肢の洗い出し • 実際の行動・選択肢の決定とインテリジェンス生成は分離されるべき、とされる	• 企業内の情報収集・分析を一元化する組織体制の構築 • 専門知識やスキルを獲得・維持するための「内製化」と「外製化」

出典：筆者作成。

第一に必要な要素はリスク・インテリジェンスの**対象範囲の設定**である。インテリジェンスに関する標準的な教科書では、インテリジェンス生成・サイクルに先立って、①カスタマーによるインテリジェンス要求があり、②インテリジェンスの活用者と生成者は明確に分離されるべき、と考えられている。民間企業でおきかえれば、まず経営層からのインテリジェンス要求・指示があり、その上で、要求者とは異なる組織がインテリジェンス活動を行う、という意味である。しかし、経営層からの要求・指示は曖昧・抽象的な場合やそもそも不可能なものである場合があるから、妥当な形でインテリジェンスの対象範囲を（再）設計する必要がある。的確な関心領域・地域（AOI）の選定なしに、意味のあるインテリジェンスの生成は難しい。

単なる情報収集対象としては、全世界の主要な地政学リスクを網羅的にとりあげることも可能だが、意思決定のために必要なインテリジェンスの対象事象は慎重に限定する必要がある。対象事象を「○○有事」等のいくつかに絞ったとしても、適切な設計が必要である。例えば、インテリジェンスの目的に「A 国が B 国を侵攻するのはいつか」といったものを設定することは困難である。ケース・スタディ（１）で指摘された通り、ロシア軍が最終的にウクライナに全面侵攻するか否かは、プーチン大統領自身しか分からなかった。確かにバイデン政権はあらゆる情報収集手段を動員して、ロシアによるウクライナ侵攻タイミングを評価し、機密相当の分析結果を公開したが、その正否はプーチン大統領しか分からなかった。

経営層から「A 国が B 国に侵攻するのはいつか？」との旨の要求があった場合、「A 国が B 国に対して、着上陸・首都占領を含む全面侵攻の準備が整ったと外形的に判断できるのはどのような状況か？」（例）といった再設定が必要だろう。あるいは、「X 国は Y 国、Z 国に対する核攻撃を行うのか？」といったインテリジェンス要求は、「現時点で、X 国は Y 国、Z 国に対して弾道ミサイルでの核攻撃能力（大気圏への再突入能力、弾頭部分に積載可能な

核物質量等）を有し、それはＹ国、Ｚ国の防空能力を凌駕しているか？」（例）と再設計すべきであろう。こうしたインテリジェンスの対象範囲を踏まえて、関連する事象を洗い出し・構造化することが重要である。

第二に、**情報収集先・リソースの特定**である。端的にいえば、これは市販情報（CAI）を含む公開情報と非公開情報に大別される。インテリジェンスというと、如何に機密情報にアクセスするかが重要だ、という印象を持つかもしれないが、これは実態とは異なる。確かに機密情報・非公開情報は重要だが、多くの外交官や研究者が指摘している通り、冷戦下の米国の対ソ連インテリジェンスでさえ、その約 80-95%以上は公開情報であったとされる[2]。

公開情報は「１．公開情報分析とは」で述べたように、伝統的には、新聞、テレビ、ラジオ、雑誌（業界紙、学会誌等のアクセスしにくいものも含む）や行政・議会・司法等の公式発表等である。加えて、デジタル化とオープンソース化が進展した現代では、民間企業が比較的アクセスしやすく、インテリジェンス活動に有益な情報・データとその収集・解析プラットフォーム（CAI を含む）として以下があげられる。

- ソーシャルメディア上のユーザ生成コンテンツ（User-generated Content: UGC）データ
- 衛星画像データ
- 船舶自動識別装置（Automatic Identification System: AIS）データ
- サイバー脅威インテリジェンス（※これは生のデータや情報ではなく、一定の加工がなされたもの）等

より網羅的なオンラインでの調査ツールやリソースは、非営利の OSINT 団体「ベリングキャット（Bellingcat）」が「オンライン調査ツールキット」として公開している[3]。

非公開情報とは、そのアクセス・収集手段がもっぱら「ヒューミント（HUMINT）」と呼ばれるものである。ヒューミントとは一般に諜報活動・スパイ活動が想起されることが少なくないが、政治家・政策当局者や同業他社・業界団体への情報収集、外部専門家へのインタビュー等も含まれる。これは企業と対象者の相互にとってリスクのない関係性で行われることが望ましい。

しかし、こうした公開情報・非公開情報、一次情報・二次情報を収集しても、企業内で専門的知見に基づく解釈・評価を下すことは容易ではないため、平時から有益な情報源、具体的には**分野ごとに専門家・ジャーナリストや専門機関を把握しておく**ことが望ましい。その際、領域・分野と専門家・機関を適切にマッチさせることが重要である。「Ｘ国」の専門家ではなく（そういった存在もいなくはないが、基本的には少ない）、「Ｘ国」の内政、特に支配政党の統治・行動原理の専門家、「Ｘ国」の軍事・安全保障政策の専門家等、必要な領域に適切な粒度を設定することが重要である。こうした専門家評価には、対象の実績や業界内の評価等一定の知見や経験を要する。

第三に、インテリジェンスを生成・配布した結果の**行動・選択肢の洗い出し**である。これは対象範囲の設定と不可分であり、実際にはより早い段階で検討されるだろう。

「はじめに」で述べた「明日の予定」の例では、「ツバメが低く飛んでいる」というインフォメーションから、「明日は雨が降るだろう」というインテリジェンスを生成したとしても、明日の予定をどうするか（意思決定・行動）は自明ではない。「傘を持参する」「カッパを着る」「予定をキャンセルする」などの様々な選択肢が存在する。

インテリジェンスを踏まえた判断事項・行動、例えば、投資判断、駐在員の退避、事業継続計画の発動、現地への権限委譲等の行動・選択を予め洗い出しおくことが重要である。それは、**中期経営計画・事業計画、緊急時対応**

[2] 例えば、George F. Kennan, "Spy and Counterspy," *New York Times* (May 18, 1997); マーク・Ｍ・ローエンタール（茂田宏他訳）『インテリジェンス：機密から政策へ』（慶應義塾大学出版会、2011 年）、129 頁；元外交官・宮家邦彦氏（キヤノングローバル戦略研究所・外交安全保障グループ研究主幹（当時））へのインタビュー（2016 年 7 月 12 日）。他方、近年では SIGINT の重要性が高まっている。ある報道によれば、米情報機関が行う大統領日報の少なくとも 60%は国家安全保障局（NSA）が収集した SIGINT が基盤となっている。 Warren P. Strobel and Ellen Nakashima, "CIA chief faces stiff test in bid to revitalize human spying," *The Washington Post* (May 28, 2025).

[3] Bellingcat's Online Investigation Toolkit や"Bellingcat's Online Investigation Toolkit CSV Export," GitHub.

計画、事業継続計画という形で明文化されることが一般的である。また、インテリジェンスの要求者と生成者の分離原則に従えば、実際の行動・選択肢の決定（≠洗い出し）とインテリジェンス生成は分離されるべき、とされる。

第四に、これらを踏まえて組織内でインテリジェンス・サイクルを活用する**組織体制構築**である。地政学リスク分野では、多くの関連組織・部署が関わる。例えば、リスク管理部門、経営企画部門、海外事業部門、政策渉外部門等である。専任組織、ワーキンググループ、委員会等、様々な形態の組織体制が想定されるが、企業内の情報収集・分析を一元化する組織体制が望ましい。

「ツバメが低く飛んでいる」ことは誰でも観察できるかもしれないが、「明日は雨が降るだろう」という解釈・評価を得るためには専門的知識やスキルが必要になる。例えば、分かりやすいものでは、外交的・官僚的修辞や専門用語、メディア等の政治的立ち位置等の知識である。そして多くの場合、継続的な観察や情報収集が必要である。この点が企業にとって最も悩ましい課題である。こうした**専門知識やスキルを獲得・維持するための方向性として、内製化と外製化の 2 つがある**。政治リスクといっても、その領域や範囲は膨大で、一人の専門家がカバーできる範囲は限られる。一定規模のリスクマネジメント先進企業であれば、企業にとって重要な領域には少数の要員をあて、それ以外の領域では外部ネットワークを用いること――企業や事業にとって必要な領域・分野に複数の信頼できる専門家や情報源を確保すること――が現実的である。この他にも、「成果物」としてインテリジェンスそのものを購入する、「プロセス」としてのインテリジェンスとして解析・分析ツールを利用する、「体制」としてのインテリジェンスに外部専門家やコンサルタントを起用する、という選択肢もあり得るだろう。

以上（2025 年 5 月 30 日脱稿）

一般社団法人 DEEP DIVE について

- 一般社団法人 DEEP DIVE はデジタル領域をはじめとする公開情報分析（open-source intelligence: OSINT）と衛星情報分析を組み合わせたマルチモーダルなインテリジェンスを提供する非営利の民間組織であり、小原凡司氏（代表理事）と小泉悠氏（理事）により 2024 年に設立されました。
- DEEP DIVE と東京海上ディーアール株式会社は、地政学リスク・インテリジェンス関連ソリューションの高度化・拡充を目的とした業務提携を開始したことを公表（PDF 公表資料）しています。

東京海上ディーアール株式会社

小原 凡司（一般社団法人 DEEP DIVE 代表理事）
笹川平和財団 上席フェロー。専門：現代中国政治（外交・安全保障）。
小泉 悠 （一般社団法人 DEEP DIVE 理事）
東京大学 先端科学技術研究センター 准教授。専門：ロシアの軍事・安全保障。
川口 貴久（東京海上ディーアール株式会社 ビジネスリスク本部 兼 経営企画部 主席研究員、マネージャー）
一橋大学 法学研究科 非常勤講師。専門：国際政治・安全保障、リスクマネジメント。

〒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 https://www.tokio-dr.jp/