経済安全保障とインテリジェンス

公安調査庁長官
和田雅樹（わだ まさき）

安全保障の裾野が経済や技術分野に広がる中、情報機関が注視すべき対象も大幅に拡大してきている。それは、大量破壊兵器の拡散防止（counter-proliferation）や外国情報機関からの防諜（counter-intelligence）などの伝統的な課題だけでなく、軍事的な優劣をも左右する先端技術の防護、サプライチェーンにおける脆弱性の分析、技術やデータを標的としたサイバー攻撃の解明など、より広範な事象への対応を意味する。我が国でも、外為法の改正や経済安全保障推進法の制定など、経済安全保障の確保に向けた政策面での取り組みが進む中、政策立案、法執行、技術等の流出やサイバー攻撃の未然防止に資するインテリジェンスが求められている。

技術、データ、製品等の流出防止

特に重要な課題の1つとして挙げられるのが、技術、データ、製品等の流出防止である。近年、懸念国が通常の経済活動や研究活動を装って企業や大学等に接近する事例が見られるところ、欧米を中心に各国情報機関も懸念を強めており、自国の政策・法執行機関と連携した取り組みを強化している。

例えば、投資や企業買収、共同事業に伴う技術・データの流出について、多くの国で対内直接投資に係る審査制度を設けているが、経済安全保障の観点からは、特定企業の実質支配者や軍・政府との関係、保有する技術の機微度や軍事転用の可能性、自国のサプライチェーンに与える影響など、様々なインテリジェンスが必要となる。この点、米国では、対米外国投資委員会（CFIUS）の審査において、情報機関が国家安全保障に係る脅威を評価している。

次に、個人からの技術・データの流出については、リクルート活動や共同研究を通じたものだけでなく、我が国でも懸念国の情報機関員等が路上や展示会、SNSを通じて企業関係者に接触する事案が発生しており、注視する必要がある。また、各国では留学生・研究者の査証審査を強化する動きも見られ、マッカラム英保安局（MI5）長官は、英国における学術技術承認スキーム（ATAS）の規制強化による成果を強調している。このほか、企業やアカデミアに対するアウトリーチについては、米国家防諜安全保障センター（NCSC）が、内部脅威（insider threat）の探知や対応について、カナダ安全情報局（CSIS）が、標的となる研究分野や外国の影響から研究を守るための方法等について啓発している。

さらに、機微な製品等の不正調達については、各国の輸出管理を回避するために、複数のフロント企業やブローカーを介した調達活動の事例が見られるところ、政府として適切な対応をとるためには、真の最終需要者や標的とされている製品、調達背景、迂回ルートなどに関するインテリジェンスを把握する必要がある。米国においては、これらインテリジェンスを把握するため、法執行機関と情報機関との協働の場として輸出執行調整センター（E2C2）が設けられている。

最後に、サイバー空間上での技術・データの

窃取については、攻撃者への制裁や起訴など、各種措置をとる前提となるアトリビューションの観点からもインテリジェンスは不可欠である。また、サイバー攻撃を支援する外部協力者の有無や、通信機器・ソフトウエア等を通じた情報流出、サイバー空間上での外国情報機関・当該機関と連携するハッカー等による働き掛けにも注意を払う必要がある。この点、米連邦捜査局（ＦＢＩ）や独連邦憲法擁護庁（BfV）は、特定のスパイウエアによる流出リスクやＳＮＳ上での外国情報機関による情報収集等について警告を発している。

公安調査庁の取り組み

上記を踏まえつつ、公安調査庁としても関連の情報収集・分析を強化している。経済安全保障に関しては、技術流出だけでなく、懸念国による様々な形での経済的な影響力の行使につながる動向も注視している。また、サイバー分野では、国家の関与が疑われるサイバー攻撃の主体解明、攻撃の対象や時期等の予兆把握、事案の分析等に注力している。２０２２年４月には、経済安全保障特別調査室およびサイバー特別調査室を新設し、調査体制を強化したところではあるが、各国情報機関の取り組みも踏まえ、調査・分析能力のさらなる向上に努めている。この点、米中央情報局（ＣＩＡ）は、２０２１年10月、新興技術や経済安全保障を含む地球規模の課題に取り組むため、越境・技術ミッションセンターの設置を発表している。また、同年11月に、ムーア英秘密情報局（ＭＩ６）長官が「デジタル時代におけるヒューマン・インテリジェンス」と題して実施したスピーチは、新たな脅威に対応して情報機関が外部の知見も取り入れつつ現代化する必要性に言及しており、当庁にとっても示唆に富んだ内容となっている。

関係機関・企業等との協力

当然、経済安全保障への対応は一組織でなし得るものではなく、関係機関との協力が不可欠である。まずは、政策立案や法執行を担う他省庁と緊密に連携したうえで、施策上の判断に資するインテリジェンスを提供していく所存である。次に、外国機関との連携については、ファイブアイズや欧州など多くの国で我が国と同様の問題意識を有しているところ、情報機関同士のインテリジェンス分野での連携をさらに強めていくことが肝要と考える。２０２２年７月に、マッカラム英ＭＩ５長官とレイ米ＦＢＩ長官が、外国による技術窃取やサイバー攻撃への対応強化について合同演説で強調したことは象徴的である。

最後に、技術流出の未然防止のためには、企業・大学等との官民連携が重要である。公安調査庁では、講演や個別の意見交換を通じて、具体的な技術流出の事例や働き掛けの手口、不審なアプローチを受けた場合の対応等の知見を共有している。２０２２年６月には、経団連と共同でシンポジウムを開催し、古川禎久法務大臣およびエマニュエル駐日米国大使からメッセージをいただくとともに、ＦＢＩの特別捜査官から米国の取り組みについて発表していただいた。当庁ホームページでは、経済安全保障やサイバーに関するパンフレットを公表しているほか、関連の相談・講演依頼等の窓口を設けている。経済団体や企業、大学の皆さまからは、さらなる知見・情報の共有について強い要望をいただいているところ、民間との連携や人材交流を進めている外国機関の事例も参照しつつ、当庁としてもアウトリーチ活動をより強化し、企業・大学側の取り組みに最大限貢献していきたいと考えている。

公表資料

経済安全保障の確保に向けて

技術・データ・製品等の想定される流出経路や事例等

サイバー空間における脅威の概況

サイバー攻撃の脅威の態様や脅威主体、その手法や対策等

相談・講演依頼等窓口

HP上に経済安全保障に関する相談・講演依頼等窓口を設置

提供：公安調査庁