特別寄稿

経済安全保障の確保に向けた日本警察の取組

警察庁警備局外事情報部外事課経済安全保障室長　**山田　雅史**

1　はじめに

令和７年の新春を迎え、謹んでお慶び申し上げます。

最初に、一般財団法人安全保障貿易情報センター及び会員の皆様には、平素より警察行政各般にわたって御理解と御協力を賜っておりますことにつきまして、厚く御礼を申し上げます。

さて、警察では、令和４年４月に警察庁外事課に経済安全保障室を設置し、その後も必要な体制の整備等を進めて、経済安全保障の確保に向けた取組を強化しているところです。本稿では、米国、英国を中心に海外における関連の動向を紹介した上で、経済安全保障分野において日本警察が進める諸活動について概要を御説明させていただきます。本稿により、会員の皆様に警察の取組の意義を御理解いただく上で御参考になれば幸いに存じます。

2　海外における最近の動向

昨今の国際情勢の複雑化を踏まえ、経済安全保障に関する関心が高まっています。安全保障の裾野が経済領域に拡大し、人工知能（AI）、量子技術、半導体といった先端技術分野における研究で他国を凌駕することは経済的な側面に加え、軍事的優位性の獲得・確保に資するなど安全保障に影響力を及ぼすとともに国際社会での支配的地位を生み出すことにつながっており、こうした分野における各国間の熾烈な競争が展開されています。各国における技術流出に対する強い危機感を反映するように、特に米国や英国では、治安情報機関等により積極的に情報発信を行っている状況が確認されています。この章では最近の動向を幾つか紹介させていただきます。

（１）「ファイブ・アイズ」による対談

2022 年７月には米国の連邦捜査局（FBI）のクリストファー・レイ長官と英国の保安庁（MI５）のケン・マッカラム長官がロンドンで企業や大学の関係者に対して、初めて共同会見を行い、中国の産業スパイの脅威について警戒を呼び掛けたのに続き、2023 年 10 月には「ファイブ･アイズ」[1] と呼ばれる、米国、英国、カナダ、オーストラリア及びニュージーランドの治安情報機関のトップが、シリコンバレーの民間企業関係者を集めた会合（「Emerging Technology and Securing Innovation Security Summit」）に参加して対談を行い、その中で中国による知的財産の窃取の脅威について訴えました。同対談において、米国 FBI のレイ長官は「中国政府は、長い間、

[1] 米国と英国に加え、第二次世界大戦後、米国と英国間で締結された 1946 年 BRUSA 協定（後に UKUSA 協定に名称変更）にその後加盟したカナダ、オーストラリア及びニュージーランドから構成される、情報共有や安全保障に関する連携のパートナーシップを指します。

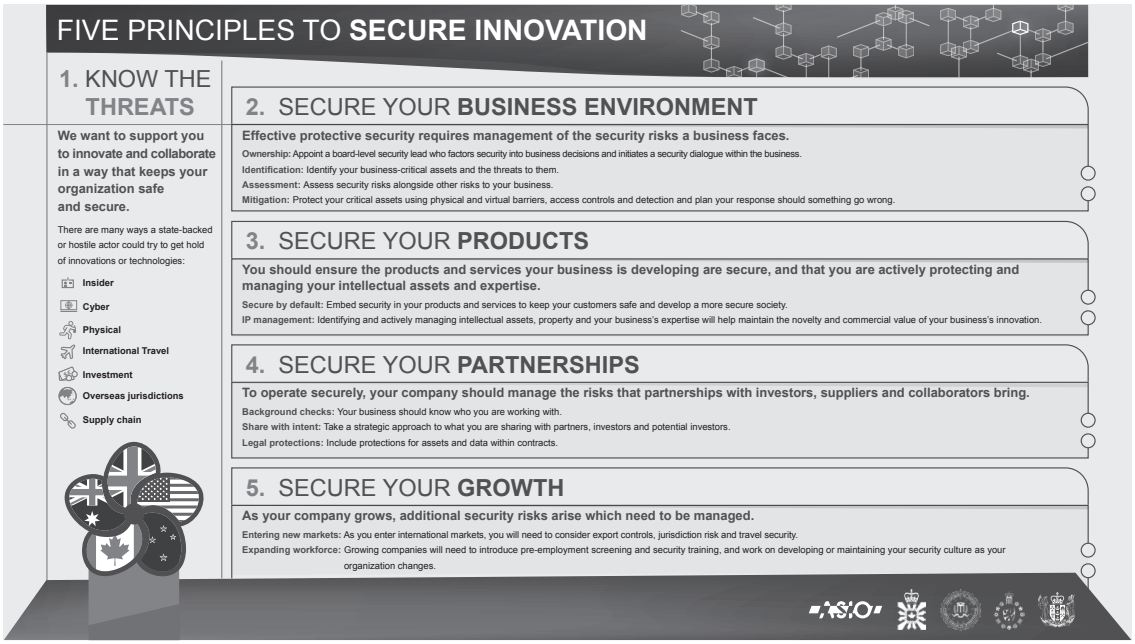
サイバー攻撃、人的諜報活動から、一見無害に見える企業取引まで、様々な手段を同時に使って、企業を標的にしてきた」と述べ、中国政府が大規模な情報の窃取を行うための手段として、サイバー攻撃、協力者を使った人的要因による技術獲得、投資や業務提携等の様々な手段を、時には複数の手段を組み合わせていることを指摘しています。また、英国 MI５のマッカラム長官は同対談において、「（技術獲得に向けた攻撃的試みが）特に新興技術について先鋭化している。AI、量子コンピューティング、合成生物学といった分野で先を行く国家が将来の世界を形作る力を持つ。」と述べたほか、英国では２万人の英国人が企業秘密を入手する目的で中国政府から SNS を通じた接触を受け、推定１万社の英国企業がリスクに晒されている旨も同時期の報道によるインタビューにおいて明らかにしています。そもそも「ファイブ・アイズ」の治安情報機関のトップが一堂に会すること自体が非常に珍しいことであり、中国政府による技術窃取に対する強い危機感を参加国各国が共有している証左と言えます。他方で、両長官は、発言に当たって中国共産党や中国政府の一定の部門が関与する活動を論じており、中国国民一般について論じているのではないと述べていることにも留意する必要があります。

（２）「イノベーション保護のための５原則」

(1) で取り上げた対談においては、企業やアカデミアが自らの知的財産や技術を産業スパイから保護するための「イノベーション保護のための５原則（Five Principles to secure innovation）」が示されました。

その内容は、①国家による脅威や技術窃取の手段について理解を促す「脅威の認識」、②効果的なセキュリティのリスクマネジメント体制の構築を促す「ビジネス環境の保護」、③製品の開発初期段階からセキュリティ保護の仕組みを構築し、知的財産の適切な管理を促す「製品の保護」、④投資家、サプライチェーンの提供者等とのパートナーシップがもたらし得るリスクの管理を促す「パートナーシップの保護」、⑤新たな市場開拓等に伴うセキュリティリスクの管理を促す「成長の保護」の計５項目から構成されています。MI５のマッカラム長官は、「これらの原則は、実用的で、実行可能で、まずもって守ろうとしている開放性やイノベーションを阻害しないことを目的に関係部門と共同で作成した」と説明しているとおり、広く通用性があり、我が国においても参考になるものと考えられます。

【イノベーション保護のための５原則】



英国国家保護セキュリティ当局（NPSA[2]）ウェブサイトより

[2] 国家保護セキュリティ当局は、MI５の一部としてアウトリーチ活動等を実施しており、NPSA は National Protective Security Authority の略称です。

（３）スタートアップ企業からの技術流出のリスク

2024 年７月、米国の国家情報長官（ODNI[3]）の下にある国家防諜保全センター（NCSC[4]）等の機関は合同で、スタートアップ企業に対して技術流出の脅威について警戒を促す内容のパンフレットを公表しました。同パンフレットでは、スタートアップ企業が外国懸念主体の関与するベンチャー・キャピタルやプライベート・エクイティ等の投資を受けることに伴うリスクとして、米国政府との契約機会の喪失、外国からの不当な影響、データや技術の流出が挙げられています。また、不審な投資活動にみられる主な特徴として、複雑な投資構造スキームを構築することや投資実行前における知的財産や機微な情報の提供が要求されることなどが指摘されており、特に前者については投資審査を回避するためとされています。同パンフレットでは、スタートアップ企業が自らの重要資産を特定・保護すること、投資主体を知ること（投資者の正体を確認し、制裁対象者でないかなどを調査すること）、情報の共有範囲を制限すること、米国連邦機関や同業者と脅威や対策に関する情報を共有することといったリスクを低減させるための取組も紹介されています。

（４）米国における技術流出防止に向けた省庁間を跨ぐ取組

後述する日本警察の取組とも関係しますが、米国では、2023 年２月、複数の政府機関から構成される創造的技術攻撃部隊（DTSF：Disruptive Technology Strike Force）が立ち上げられました。

同部隊は、米国司法省国家安全保障局と米国商務省産業安全保障局が主導し、連邦捜査局、国土安全保障省に加え、全米 12 大都市圏の 14 の連邦検事事務所も参加して発足したもので、その後も関係機関や規模を拡大させています[5]。同部隊は、権威主義的な敵対的外国勢力が機微な技術を不法に取得し、それを軍事能力の開発や大衆の監視等の民主主義的な価値観に抵触する用途に利用することを防ぐことを目的とした省庁横断的な取組であり、対象技術にはAI、量子コンピューティング、バイオ科学等が含まれるとされています。

2023 年２月の発足以降、同部隊は 2024 年 10 月末時点で輸出規制違反や営業秘密の窃取を含む 24 件の刑事事件に着手し、その内訳は、ロシア関係 12 件（半導体、電子機器の違法輸出等）、中国関係９件（営業秘密の窃取等）、イラン関係６件（制裁違反の物資調達）となっています（複数の国に関係する３件を重複で計上しているため、内訳の合計は全体の件数と一致しません。）。ロシアによるウクライナ侵略を受け、同部隊の幹部がウクライナのキーウを訪問したほか、これまでの検挙件数でもロシアに関する事例が多く含まれているなど、米国が対露制裁関連の輸出管理の強化にも取り組んでいる状況が分かります。

３　日本警察における取組

日本においては、公共の安全と秩序の維持に当たる責務を有する警察が、経済安全保障に関連する各種情報収集や分析を行い、その中で把握した違法な事案の取締りに当たるとともに、アウトリーチ活動による企業・アカデミアへの情報提供を行っています。以下では、違法な事案の取締りやアウトリーチ活動の具体的な事例に加え、警察庁が国内や国外の関係機関と連携して進めている取組についても御説明します。

（１）最近の検挙事例

ア　SNS を通じた接近事例

大手化学メーカーの社員が、平成 30 年８月から平成 31 年（2019 年）１月にかけて、勤務先の営業秘密であるタッチパネル等に使用される素材に関する技術情報を不正に領得するなどした上、SNS を介して接触してきた中国所在の企業の社員に開示した事例について、令和２年 10 月、大阪府警察は、同人を

[3] 国家情報長官（DNI）は、米国のインテリジェンス・コミュニティの長として、米国大統領への主要なインテリジェンス・アドバイザー(primary intelligence advisor) として位置付けられており、ODNI は Office of the Director of National Intelligence の略称です。
[4] 国家防諜保全センターは、政府内の関係機関や民間セクターと協力し、内部脅威、サプライチェーン・リスク管理等の分野でアドバイスを提供しており、NCSC は National Counterintelligence and Security Center の略称です。
[5] 同部隊には、2024 年 10 月末時点、５つの連邦組織（司法省、商務省、連邦捜査局、国土安全保障省に加え、国防総省国防犯罪捜査当局（Defense Criminal Investigative Service））と全米 15 大都市圏の 17 の連邦検察事務所が参加しています。

不正競争防止法違反（営業秘密侵害）で検挙しました。

英国MI５のマッカラム長官のスピーチで具体的な数値が取り上げられていたように、SNSで作成された偽アカウントが技術獲得のための接近工作に利用されるリスクは欧米諸国等で指摘されていました。同事例によって、日本においても同様の手法が行われていることが明らかになっており、現実空間だけでなくサイバー空間を通じた不審なアプローチがあり得ることは企業やアカデミアにおいて技術流出防止対策を講じる上で認識しておくべきリスクと言えます。

イ　国立研究開発法人からの情報流出事例

国立研究開発法人の研究員が、平成30年４月、同法人の営業秘密であるフッ素化合物に関する技術情報が記載されたファイルデータを中国所在企業のメールアドレスに送信して開示した事例について、令和５年６月、警視庁が同人を不正競争防止法違反（営業秘密の開示）で検挙しました。

同事例は、我が国の科学技術力の強化にとって重要な役割が期待される研究機関である国立研究開発法人からの情報流出が確認されたものですが、同事例は、アカデミアにおける技術情報流出の脅威を明らかにし、また、アカデミアにおける研究インテグリティの確保に向けた取組の強化につながることとなりました。

（２）アウトリーチ活動

ア　アウトリーチ活動と官民ネットワークの役割

日本警察では、警察署等のインフラを有し、地域住民の生活に密着して犯罪の予防等に当たる我が国の警察の特性を生かしてアウトリーチ活動を行っており、概して言えば、都道府県警察では各管内に所在する企業を、警察庁では大企業や経済団体を、それぞれ主な対象として実施し、企業やアカデミアに対して技術情報等の流出防止のための自主的な対策の強化を促しています。

多くの都道府県警察では、経済産業省、経済団体等とも連携して経済安全保障に関する官民ネットワークを設置するなどし、会議等においてこれらの関係機関・団体が所管している安全保障貿易管理に関する制度や現に講じられている営業秘密の流出防止対策等についての情報提供を行っています。令和６年10月末時点で、24の都道府県警察においてこうした官民ネットワークが構築されています。

【「愛知ものづくりTOPネットワーク」第４回総会の開催状況】

イ　京都府警察における新たな取組

京都府警察では、アで言及した官民ネットワークとして、他の府県警察に先んじて、平成26年（2014年）、「モノづくり・プリザーブ」を立ち上げ、京都府、京都市、産業団体等30団体、先端技術保有企業等約1,100社が参加し（令和６年10月末時点）、京都府警察から必要な情報提供、注意喚起等を進めてきました。

それに加え、令和６年11月からは、京都府南部の「関西文化学術研究都市（けいはんな学研都市）」に経済安全保障対策に特化した新たな警察拠点を設置し、運用を開始しています。同都市の京都府域には、先端技術を保有する約230の企業等が集中することに加え、今後データセンターの設置や更なる企業の進出が見込まれており、同都市の経済安全保障上の重要性が高まりつつあることに鑑みて、同府警察では、同拠点に配置した外事部門とサイバー部門の職員が、同都市の企業等に対してアウトリーチ活動を行うとともに、これらの企業等からの相談を受けやすい環境を整備し、企業等の技術流出防止意識の向上等を目指すこととしています。

（３）北朝鮮IT労働者のリスクに関する注意喚起

また、警察庁が関係省庁と連携して取り組んでいるサプライチェーン・リスクの１つとして、北朝鮮のIT労働者によるものがあります。北朝鮮のIT労働者によるリスクに関しては、2022年５月、米国国務省、財務省、FBIが連名で発出したガイダンスを

皮切りとして注意喚起がなされてきました。その中では、北朝鮮が世界中に高度な技術を持つ多くのIT労働者を送り込んで、契約を得るためにフリーランス労働のプラットフォームを悪用するなどして契約業者としてプログラムの構築に関与し、それにより、米国や国連によって課された各種制裁措置に違反して外貨獲得を行っていることが指摘されています。簡潔に言えば、再委託の形であれ、プログラムやアプリの開発等に北朝鮮のIT労働者が関与した場合には、それによる対価としての報酬がその後北朝鮮当局に還元され、兵器プログラム等の軍事強化に流用されるおそれがあることに加え、当該IT労働者がサイバー攻撃に日頃から従事していない場合でもその納入されたプログラムに脆弱性を抱えることになり、それを悪用したサイバー攻撃の被害に遭うリスクを負うこととなります。

我が国に関しても、北朝鮮IT労働者が日本人になりすまして日本企業が提供する業務の受発注のためのオンラインのプラットフォームを利用して業務を受注し、収入を得ている疑いがあり、実際に、令和６年３月に詐欺罪等で検挙された事例では、被疑者らがクラウドソーシング企業のアカウント等を通じて日本企業からソフトウェア開発業務を受注し、その業務の一部に中国に在住するとみられる北朝鮮IT労働者を従事させていた実態が判明しています。こうした情勢を踏まえ、同月には、警察庁、外務省、財務省及び経済産業省の共同により「北朝鮮IT労働者に関する企業等に対する注意喚起」を発表しました。同発表においては、プラットフォームを運営する企業と業務を発注する企業のそれぞれに注意していただきたい特徴点について紹介しています[6]ので、是非その内容について会員の皆様に参照いただけると幸いです。

（４）日米韓における連携枠組み

米国の取組の一環として創造的技術攻撃部隊（DTSF）について言及しましたが、2023年８月にキャンプ・デービッドで行われた日米韓首脳会合の共同声明において、米国のDTSFと日本、韓国のカウンターパート間で情報共有や連携強化を進めることについて合意がなされました。これを受けて、2024年４月には、日米韓関係当局の第１回ハイレベル会合が開催され、日本からは警察庁、経済産業省、財務省が参加しました。同会合では、不正な技術移転に対処することが国家及び経済安全保障上の重要な課題であるという認識の共有、三カ国の執行機関間における情報共有及び更なる連携強化について合意がなされました。各国で展開される技術獲得に向けた工作手口や輸出管理の迂回に関与する主体等について情報共有・連携を強化することは経済安全保障の確保において重要であり、こうしたネットワークも利用して、警察庁では外国治安情報機関との連携を更に深化させることとしています。

４　おわりに

本稿では、米国・英国において、経済安全保障の推進のために治安情報機関が積極的に情報発信を行い、企業やアカデミアと連携した上で各種対策を進めている状況を取り上げましたが、警察庁としても、国内外の事例等を踏まえて技術獲得に向けた工作手口等をまとめたパンフレットや動画を作成し、活用できるよう、警察庁ホームページ上に経済安全保障特設サイトを設けて公開しています。例えば、「技術流出の防止に向けて」と題するパンフレットにおいて、技術情報等の獲得に向けた外国からの働き掛けに対する有効な対策として、「See（相手・書類をよく見る）」、「Stop（立ち止まってリスクを把握する）」、「Share（共有する・相談する）」を「企業やアカデミアに守ってほしい３つのＳ」として紹介しています。また、令和６年度中にも新たな動画を作成しているところであり、引き続き最新の情報を提供するように努めて行きたいと考えています。

企業やアカデミアの方には技術情報の流出に関する脅威（リスク）について把握し、それを踏まえた判断をしていただくことが重要であり、一般財団法人安全保障貿易情報センターから提供されている各国における輸出管理の制度や運用をはじめとする関連の最新動向に加えて、警察庁が公開するこうした素材も御活用いただけると幸甚です。また、一度技

[6] 警察庁ホームページ「北朝鮮IT労働者に関する企業等に対する注意喚起について」
https://www.npa.go.jp/bureau/security/NK_it.pdf

術情報が外部へ流出してしまえば、取り返すことは困難となることに鑑みれば早めに対策を講じることが重要ですので、被害を認知した場合だけでなく、その懸念を感じた場合にも、早い段階で警察へ御相談いただきますようお願いいたします。

【警察庁ホームページにおける情報発信】

警察庁特設ページ「技術流出の防止に向けて」
https://www.npa.go.jp/bureau/security/economic-security/index.html