



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 MI 5 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。MI 5 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に、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】

FIVE PRINCIPLES TO SECURE INNOVATION

- 1. KNOW THE THREATS**
We want to support you to innovate and collaborate in a way that keeps your organization safe and secure.
There are many ways a state-backed or hostile actor could try to get hold of innovations or technologies:
 - Insider
 - Cyber
 - Physical
 - International Travel
 - Investment
 - Overseas jurisdictions
 - Supply chain
- 2. SECURE YOUR BUSINESS ENVIRONMENT**
Effective protective security requires management of the security risks a business faces.
 - Ownership: Appoint a board-level security lead who factors security into business decisions and initiates a security dialogue within the business.
 - Identification: Identify your business-critical assets and the threats to them.
 - Assessment: Assess security risks alongside other risks to your business.
 - Mitigation: Protect your critical assets using physical and virtual barriers, access controls and detection and plan your response should something go wrong.
- 3. SECURE YOUR PRODUCTS**
You should ensure the products and services your business is developing are secure, and that you are actively protecting and managing your intellectual assets and expertise.
 - Secure by default: Embed security in your products and services to keep your customers safe and develop a more secure society.
 - IP management: Identifying and actively managing intellectual assets, property and your business's expertise will help maintain the novelty and commercial value of your business's innovation.
- 4. SECURE YOUR PARTNERSHIPS**
To operate securely, your company should manage the risks that partnerships with investors, suppliers and collaborators bring.
 - Background checks: Your business should know who you are working with.
 - Share with intent: Take a strategic approach to what you are sharing with partners, investors and potential investors.
 - Legal protections: Include protections for assets and data within contracts.
- 5. SECURE YOUR GROWTH**
As your company grows, additional security risks arise which need to be managed.
 - Entering new markets: As you enter international markets, you will need to consider export controls, jurisdiction risk and travel security.
 - Expanding workforce: Growing companies will need to introduce pre-employment screening and security training, and work on developing or maintaining your security culture as your organization changes.

英国国家保護セキュリティ当局 (NPSA²) ウェブサイトより

² 国家保護セキュリティ当局は、MI 5 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室(ODNI³)の下にある国家防諜保全センター(NCSC⁴)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月末時点で、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くと幸いです。

(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い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くと幸甚です。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
National Police Agency

情勢 | 事例 | 対策 | コンテンツ | 関連サイト

検索

技術流出の防止に向けて

PROTECT YOUR FUTURE

動画公開中!

ABOUT

はじめに

日本には、先端技術を保有する企業やアカデミアが多数存在しています。これらの技術には、軍事転用が可能なものもあり、その情報が国外に流出した場合、企業などの国際競争力が低下するだけでなく、我が国の安全保障上も重大な影響が生じかねません。

いまや、技術流出の防止は、経済安全保障上の重要な課題となっているのです。

警察では、この課題に取り組むため、企業やアカデミアにおける技術流出の防止対策を支援するため、具体的な手口やその対策などを情報提供する活動（アウトリーチ活動）を推進しています。

このサイトでは、技術流出を防止する上で理解すべき「情勢」「事例」「対策」のほか、動画、パンフレットを掲載していますので、現在実施している様々な対策と合わせてご覧ください。



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>