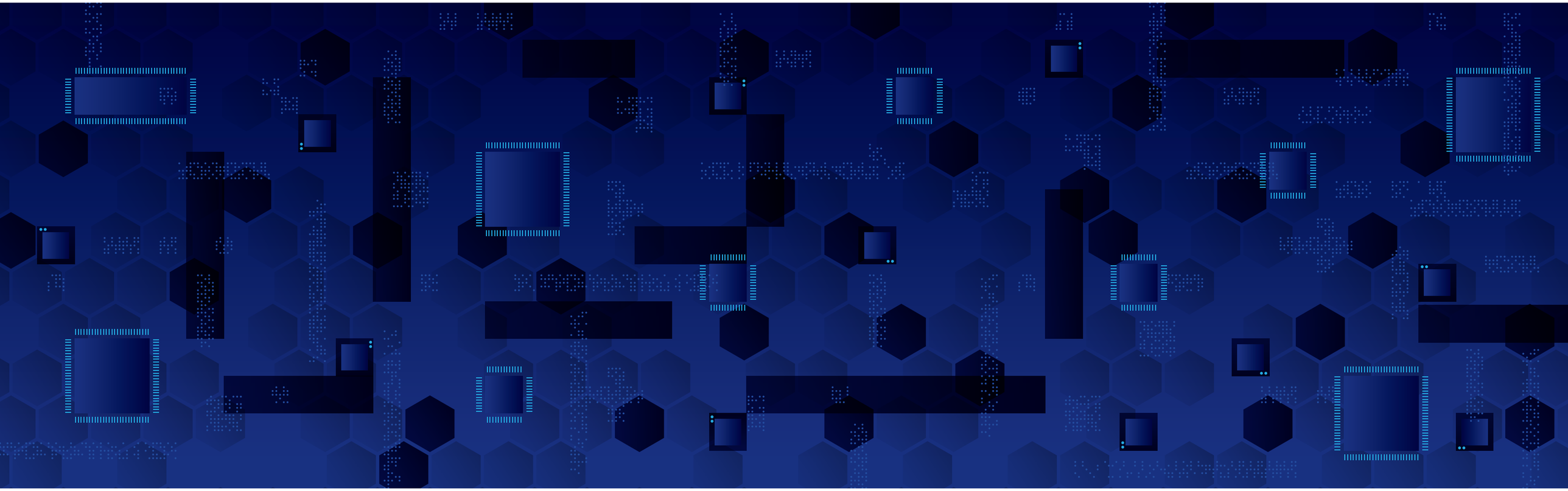
経済安全保障の確保に向けて2022

技術・データ・製品等の流出防止



情報の力で、国民を守る。

PSIA 公安調査庁
PUBLIC SECURITY INTELLIGENCE AGENCY

公安調査庁

2022.05

はじめに

国際社会において、現在、経済や先端技術をめぐる安全保障上の課題への対応が重要となっています。各国が、自国の製造能力や技術向上のため、技術・データ・製品等の獲得に向けた動きを活発化させる中、我が国においても、適正な経済活動や研究活動を装って標的となる企業や大学等に接近し、目的を達成する事案等が発生しています。

我が国から技術・データ・製品等が流出した場合、大量破壊兵器等の研究・開発等に転用されるおそれや我が国企業や大学等が有する技術上の優位性等が失われるおそれもあり、ひいては、国家及び国民の安全が脅かされたり、国際的な競争力が失われたりすることにもつながりかねません。そのため、こうしたリスクを正しく認識した上で、官民が連携して経済安全保障の確保に向けた取組を実施し、技術・データ・製品等の流出を未然に防止することが何よりも重要です。

本パンフレットは、経済安全保障の観点から留意すべき現状等について国民の皆様に知っていただくために作成いたしました。ご理解の一助となりましたら幸いです。

目次

公安調査庁の取組

我が国においては、平和を保ち、国民の安全・安心を確保することを目的として、脅威や脅威に対応する技術を「知る」、必要な技術を「育てる」、育てた技術を社会実装し「生かす」、これらの技術の流出を防ぎ「守る」ための取組が進められています。

公安調査庁では、このうち、「守る」に貢献するため、我が国の情報コミュニティの一員として、関係機関と連携しながら、我が国企業や大学等が保有する技術・データ・製品等を標的とした懸念動向に関する情報、経済活動を通じた影響力行使に係る情報などを収集・分析し、政府中枢を始めとする関係機関に情報提供しています。

日本経済団体連合会で行った経済安全保障についての講演

統合イノベーション戦略 2021
（2021年6月18日閣議決定）

（抜粋）

我が国の技術的優越を確保・維持するため、・・・適切な技術流出対策等を実施する。・・・
総合的な安全保障を確保することを両立しつつ、多様な技術流出の実態に応じて段階的かつ適切な技術流出対策を講ずべく、情報収集を進める・・・

公安調査庁は、インテリジェンス機関として、
●技術・データ・製品等を標的とした懸念動向
●懸念国による経済活動を通じた影響力行使動向
等に関する情報収集・分析を実施

経済安全保障に係る政策立案や
技術・データ・製品等流出の未然防止に寄与

我が国を取り巻く現状　激しさを増す米中対立

欧州連合（EU）

「対内直接投資審査（スクリーニング）に関する規則」— 2020年10月

- 機微技術や重要インフラに係る域外からの直接投資を審査

新産業戦略「開かれた戦略的自律性」— 2021年5月

- 輸入依存度が高くかつ調達先の多角化や域内代替が困難な品目を特定し、戦略的重要分野での連携を強化

「欧州半導体法」の草案公表— 2022年2月

- アジア製半導体への依存からの脱却及びEU域内の研究・開発や生産を強化

カナダ

「投資の国家安全保障審査に関するガイドライン」の改訂— 2021年3月

- 外国投資による国家安全保障上のリスクが懸念される分野を指定し、同分野における外国投資を審査

「研究協力に関する安全保障ガイドライン」の公表— 2021年7月

- 諜報活動などから国内の知的財産を保護

中国

「信頼できない実体リスト規定」の制定— 2020年9月

- 中国の主権や安全、利益を脅かす外国の組織・個人をリスト化し、輸出入や投資、入国などを制限・禁止

「外国の法律及び措置の不当な域外適用を阻止する規則」の制定— 2021年1月

- 外国の規制関連法規定が中国国内で適用されることを阻止

「反外国制裁法」の制定— 2021年6月

- 外国による「差別的な制限措置」に対して法律レベルで対抗措置を講じることが可能

アメリカ合衆国

中国人研究者・留学生の入国規制— 2018年6月以降

- 理工系の中国人学生等に対するビザの発給等を厳格化

「米国防権限法2019」に基づく中国企業のエンティティ・リスト掲載— 2019年5月以降

- エンティティ・リスト（輸出規制対象リスト）に多数の中国企業等を追加し、対中輸出管理を強化

（注）エンティティ・リストは、米国の制裁に該当する活動や米国の国家安全保障・外交政策上の利益を害する活動に従事した団体や個人を掲載。本リストに掲載された者への輸出等を規制。

「米国のサプライチェーンに関する大統領令」に基づく重要技術・製品のサプライチェーンからの中国の排除— 2021年2月以降

- 中国企業製の情報通信機器等の調達・使用を制限

イギリス

「国家安全保障・投資法」— 2022年1月

- 外国からの投資等に対して政府が調査・介入する権限を付与

ドイツ

「対外経済法」の改正— 2020年7月

- EU域外企業による投資の通告義務の範囲を拡大

「ITセキュリティ法」の改正— 2021年5月

- 連邦情報セキュリティ庁の機能強化
- 重要インフラにおける部品が公共の安全を損なう場合、使用を禁止

フランス

「郵便・電子通信法典」の改正— 2019年8月

- 通信事業者に事前審査を義務付け

外資規制の特例措置を延長— 2021年11月

- 戦略分野の企業を外資による買収から守るための特例措置を延長（2022年12月末まで）

オーストラリア

「外資による取得及び買収に関する法律」の改正— 2021年1月

- 国家安全保障上機微な土地及び事業に対する外国投資は、投資額にかかわらず政府による審査を実施

「重要インフラ安全保障法」の改正— 2021年12月

- 外国投資審査の範囲を従来の4分野から11分野に拡大

投資・買収

不正調達

留学生・研究者の送り込み

共同研究・共同事業

人材リクルート

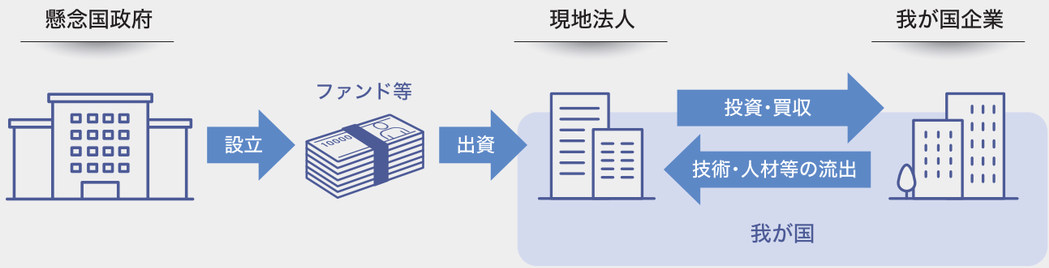
諜報活動

サイバー攻撃

想定される流出経路

我が国において、企業や大学等が取り扱う技術・データ・製品等は、様々な経路を通じて流出するおそれがあります。こうしたものの多くは、適正な経済活動や研究活動を装った働き掛け等を通じて流出しているとみられ、注意が必要です。

1 投資・買収



実際に発生したケース

Case 1:

中国企業が2020年、ドイツに子会社を設立し、同国の通信衛星中堅企業の買収を企図。ドイツ当局は安全保障を脅かすおそれがあるとして買収を阻止。

Case 2:

中国企業が2021年、韓国、フランス、台湾の半導体関連企業の買収を相次いで企図。中国経済を分析するオランダ企業によると、当該中国企業は、実質的に中国政府の支配下にあり、これまで買収した複数の海外企業の研究・製造拠点を中国に移転。

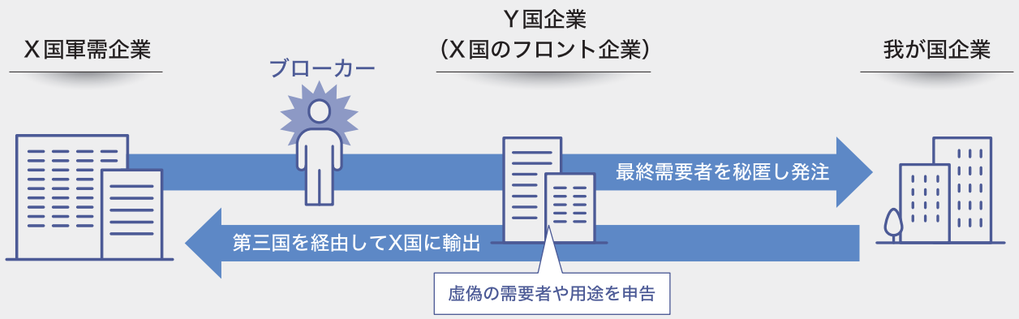
Case 3:

中国企業が2021年、ウクライナの航空エンジン大手企業の買収を企図。米国当局は、「中国の悪意ある投資」として懸念を表明。ウクライナ当局は、買収を阻止。

Point

- 懸念国の投資家が、我が国の重要技術を有する企業を買収することで、我が国の技術・データ・製品等が懸念国に流出するおそれ。
- 投資・買収を行う投資家が懸念国の投資家でなくとも、実質的に懸念国の影響下にあるとみられる可能性もあり、資本関係に注意が必要。
- 懸念国の投資家が我が国に新たに設立した法人等を通じて、企業の買収や高度人材の獲得を図る可能性も。

2 不正調達



実際に発生したケース

Case 1:

ドイツ当局は2021年、ロシアによる高性能機械の調達を支援した疑いのある人物Aを拘束したと発表。Aが経営する貿易会社は、ロシア情報機関とのつながりがあるとされ、同社を介して高性能な工作機械をロシア軍需企業に出荷していた模様。

Case 2:

米国当局は2018年、中国籍の人物を、中国人民解放軍と密接な関係にある中国の大学からの依頼に基づき、対潜水艦戦に転用可能な米国製の水中聴音装置を同大学に不正輸出した容疑で逮捕。

Case 3:

2021年、アラブ首長国連邦（UAE）に在住するイラン人Bは、核兵器、ミサイル誘導システム等に転用可能な米国製部品をイランに不正輸出した容疑で米国において有罪判決。

Case 4:

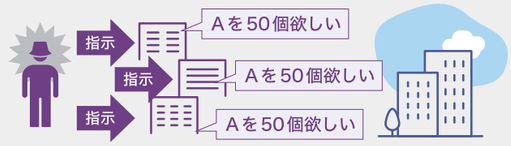
2021年、我が国機械製造会社社長を、軍用ドローンに転用可能な高性能モーターを無許可で中国企業に輸出しようとしたとして、外為法違反（無許可輸出未遂）の容疑で検察官送致。

Point

- 各国の輸出管理を回避するために、複数の企業やブローカーを介することで最終需要者を秘匿しようとする手口が散見。
- 国内にも、外国の不正調達に協力する企業・個人が存在するおそれがあることに留意。
- 発注元の事業内容と販売製品が合致するか、発注数量、用途、最終需要者等に不審な点がないか確認することが重要。

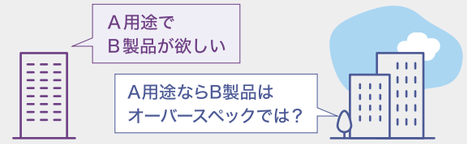
その他考えられる例

同一製品について同時期に複数の引き合い



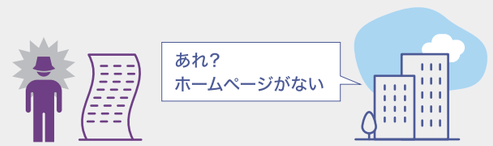
最終需要者が同一である可能性？

用途と製品スペックの不釣り合い



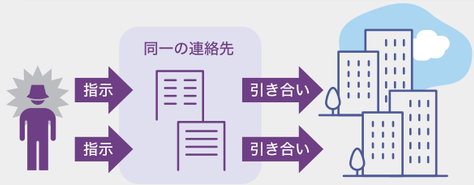
用途の秘匿？

発注元のホームページが存在しない



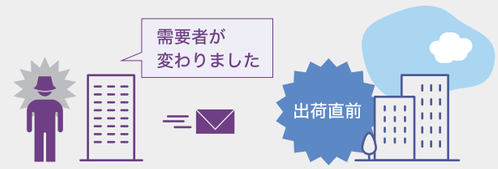
発注元に実体がない可能性？

異なる企業の連絡先が同一



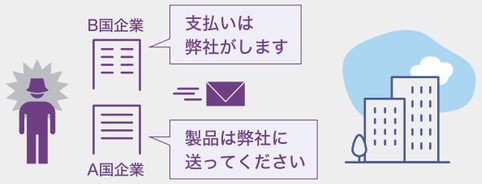
規制措置の回避？

突然の最終需要者変更



最終需要者の秘匿？

発注元と支払人の不一致



用途の秘匿？

3 留学生・研究者の送り込み

実際に発生したケース

Case 1:

中国の軍系大学に在籍する元留学生は2020年、現役の軍人であることを隠蔽して不正に米国の査証を取得したなどとして、起訴。同人は、米国の大学で物理学等の研究に従事しながら、同国の軍のプロジェクト等に係る情報収集を行っていた模様。

Case 2:

中国の軍系大学出身で、同国において複数の軍事研究に従事する研究者は、ノルウェーの大学に在籍中、新エネルギー研究の名目で同国政府から研究補助金を受け、極超音速関連の研究に従事。なお、当該研究者は、論文に架空の研究機関の肩書を記載。

Case 3:

我が国大学・研究機関に在籍後、外国において軍事研究に従事する研究者が複数存在。

Point

- 海外の研究者・学生が研究意図や一部の経歴を秘匿して入国を企図するおそれ。
- 研究室等において重要技術を扱う場合は、研究データ等の管理も重要。
- 留学生・研究者に提供した技術が、ミサイル、戦闘機といった外国の兵器等の開発や性能向上に利用されるおそれも。

4 共同研究・共同事業

実際に発生したケース

Case 1:

米国当局は 2019年、中国においてスーパーコンピュータの開発を行う企業の関連企業と米国企業との合弁企業等をエンティティ・リストに掲載。

Case 2:

米国の米中経済安全保障調査委員会（USCC）は 2019年、「中国は、特に米国とその同盟国やパートナー国との共同研究などの手段を用いて、技術を積極的に獲得してきた」などと指摘。

（注）米中経済安全保障調査委員会（The U.S.-China Economic and Security Review Commission）は、米国議会により設立され、米中間の経済関係が国家の安全保障に与える影響の監視・調査を行い、議会に報告する委員会。

Case 3:

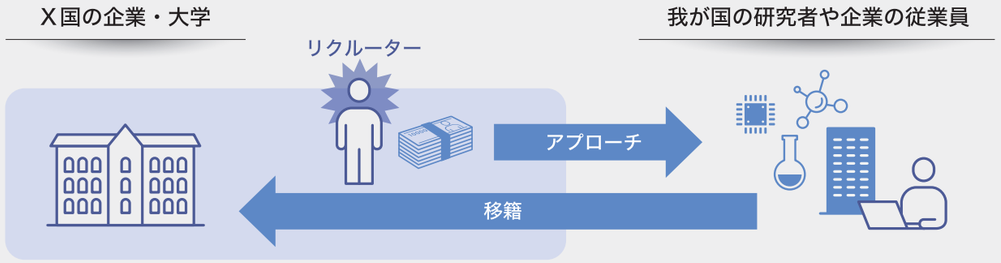
米国のシンクタンク「C4ADS」は 2021年、報告書の中で、「中国の大学研究者の中には、大学と国防関連企業が設立した合弁企業に所属する者がいる」とした上で、中国の大学研究者との交流には想定外のリスクが存在すると示唆。

（注）C4ADS（The Center for Advanced Defense Studies）は、ワシントン所在の安全保障等について分析を行う非営利組織。

Point

- 共同研究又は共同事業の相手が懸念国の軍需産業と接点を有している場合、研究・事業の成果が軍事転用されるおそれ。
- 共同研究・共同事業を通じて、当該研究・事業に関与した技術者等がリクルートの対象となるおそれも。
- 外部との共同研究・共同事業に関しては、我が国企業や大学等において研究資金の出所を確認したり、リスク評価を実施したりすることが重要。

5 人材リクルート



実際に発生したケース

Case 1:

我が国の研究者Aは2013年、中国の人材招へいの計画に参加し、中国人民解放軍と関わりの深い大学の研究センターに移籍。当該研究センターの幹部には、我が国を含む海外の著名研究者が多数在籍。

Case 2:

韓国当局は2015年、自動車変速機の検査装置の生産技術を中国企業に流出させたとして、自動車関連企業の幹部Aを起訴。Aは、中国企業から「年収2倍」「マンション提供」などの条件を提示され、技術関連資料を持ち出し、移籍。その後も、元同僚に対して、最新の図面の提供を依頼し、受領。

Case 3:

米国当局は2020年、化学生物学分野での権威である研究者Aが中国人民解放軍の影響力を受ける大学から毎月数万ドルの給料や生活費を受け取っていたにもかかわらず、それを秘匿して米国から研究費を受領し、研究を継続したとして、Aを逮捕。

Point

- 高度な専門技能を有する人材が幅広い分野でリクルートの対象に。
- リクルートの対象として、研究者以外にも重要技術にアクセス権のある人物が選ばれる場合も。
- 勧誘に当たっては、高額の報酬や住宅、役職など魅力的な条件が提示されることも。
- 懸念国を一方的に利する契約が結ばれることも。

6 諜報活動

実際に発生したケース

Case 1:

米国当局は2018年、米国の航空宇宙関連企業の情報を窃取することを企てたとして、中国の情報機関員Aを起訴。Aは、標的とした人物に対して、大学における講演を依頼するなどの名目で訪中を促し、渡航費用や報酬を支払っていた模様。

Case 2:

米国当局は 2019年、中国の情報機関員に情報を渡したとして、中国系米国市民Bを逮捕。Bは、2015年から2018年までの間、情報源から入手した米国の安全保障に関連する情報を中国の情報機関員に渡した模様。

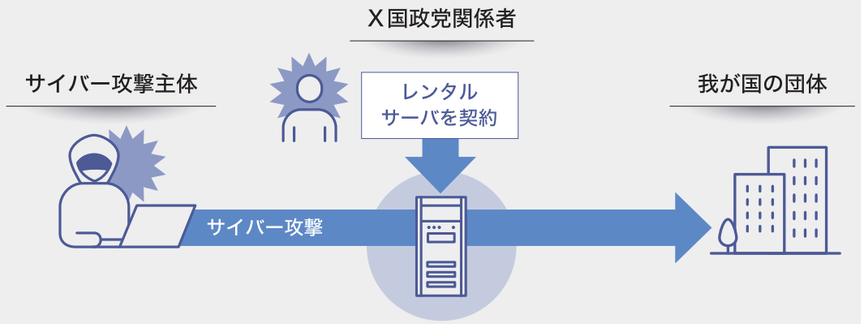
Case 3

2020年、我が国通信会社元社員Cを、同社のサーバーにアクセスして不正にデータを取得したとして、不正競争防止法違反の容疑で逮捕。Cは、在日ロシア通商代表部元代表代理と面談を重ねる中で、同人の要求に応じるようになり、最終的に不正取得に至った模様。

Point

- 情報機関員等は、産業展示会や講演会といった場を利用し、重要な情報・技術や人材を見定めた上で、標的とする人物を選定。
- 情報機関員等は、公私の場を問わず偶然を装って接触し、その後も様々な口実を設けて「1対1」での面談を図るなど、標的とする人物との関係構築に注力。
- 情報機関員等は、要求内容を徐々にエスカレートさせ、最終的に圧力をかけるなどして重要な情報の入手を企図。

7 サイバー攻撃



実際に発生したケース

Case 1:

我が国団体の職員が2015年、メールに添付されたマルウェア付きファイルを開封した結果、PC端末が外部から遠隔操作され、加入者の個人情報約125万件が流出。

Case 2:

我が国大手電機メーカーに対するサイバー攻撃（2019年）について、同攻撃により外部に流出した可能性のある防衛関連の情報が記録されているデータファイル約2万件のうち、安全保障への影響を及ぼすおそれのあるデータファイルが約60件あったことが判明。

Case 3:

2021年、当時我が国に滞在していた中国共産党員の男を、我が国団体等に対するサイバー攻撃に使用されたレンタルサーバを偽名で契約したとして、私電磁的記録不正作出及び同供用の疑いで検察官送致。同事案には、中国人民解放軍第61419部隊を背景に持つ中国のサイバー脅威主体「Tick」が関与している可能性が高いことが判明したと指摘。

Point

- サイバー攻撃では、コンピュータシステムなどの“ぜい弱性”（欠陥・弱点）が悪用されており、その中には“ゼロデイぜい弱性”と呼ばれる未知のものも用いられるほか、人間の心の隙を突き、だましたり誤解させたりすることで、システムへ不正アクセス。
- 使用しているPC・スマートフォンなど機器の状態やソフトウェア・アプリのバージョンを把握し、最新版に更新することが重要。
- 不審なメール・SMS・SNSなどの添付ファイルやURLのクリックは厳禁。

Column

懸念国による「経済的威嚇」

懸念国は、「経済的手法、または威嚇を用いて、他国政府の政策やその実行の変更を迫る」（出典：「オックスフォード・パブリック・インターナショナルロー」※1）行為を行っているとされ、こうした行為は「経済的威嚇（Economic Coercion）」と呼ばれている。

米シンクタンク「ジャーマン・マーシャル・ファンド（GMF）※2」は、中国及びロシアによる「経済的威嚇」に該当する主要な事例をデータベース化しており、その数は130件（中国70件、ロシア60件）に達する（2022年3月28日現在）。

ノルウェー

2010年、中国の人権活動家・劉暁波氏（故）に「中国における基本的人権改善のために、長年、非暴力的な戦いをした」としてノーベル平和賞を授与。

中国

ノルウェー産サーモンの検疫を強化し事実上輸入を制限。ノルウェー産サーモンの中国市場のシェアが92%から29%に。

「ノーベル賞・空席に置かれた劉暁波氏に贈られた賞状とメダル」（2010年12月10日）（写真提供：AFP＝時事）

モルドバ

EUと「深化した包括的自由貿易協定（DCFTA）を含む連合協定」を締結（2014年）後、EUとの政治、経済、安全保障上の結びつきを強化。

ロシア

モルドバに輸出する天然ガスの価格を（1㎥当たり）550ドルから790ドルに値上げするとともに、一部供給を停止。

ロシアからの天然ガスパイプライン（画像提供：共同通信社）

我が国の企業等が「経済的威嚇」の対象となるおそれも

※1 Barry E Cartert. “Economic Coercion”. Oxford Public International Law. http://opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-9780199231690-e1518?prd=EPIL#:~:text=As%20a%20starting%20point%2C%20the,structure'%20(Lowenfeld%20698). (2022-04-05)

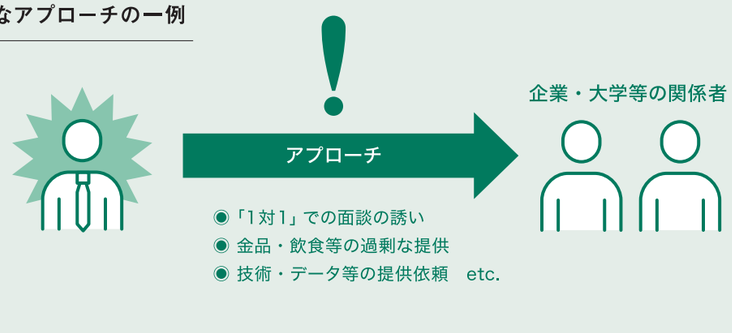
※2 “Tool: Economic Coercion”. Alliance for securing democracy, The German Marshall Fund of the United States. http://securingdemocracy.gmfus.org/asd_tools/strategic-economic-coercion/. (2022-04-05)

不審なアプローチへの対応

通常の経済活動や研究活動を行う中で、相手方から公私を問わず、例えば1対1での面談を執ように求められたり、金品・飲食等の提供など過剰な便宜供与の見返りとして、技術・データ・製品等の提供を求められたりする、といったアプローチを受けるおそれがあります。

このような場合、少しでも不審な点を確認したら、決して「個人」で対応することなく、「組織」で対応するよう心がけることが重要です。

不審なアプローチの一例



不審なアプローチを受けた場合の対応における主なポイント

- 所属の上司・同僚又は担当部署に対して、報告・相談を行うようにする。
- 私用の携帯電話やメールアドレスなどの個人の連絡先を教えない。
- 自身や同僚の担当業務について、詳細な言及は避ける。
- 個人の親切心（例：道に迷っている外国人に対する道案内）等を利用する接触があることにも留意する。
- 個人で面会の約束をすることは避けて、必ず上司又は担当部署に相談した上で、複数人で面会する。
- 可能な範囲で、相手方の担当の業務内容や目的について、具体的に聴取するよう努める。

適切な情報管理

組織内の情報管理の不徹底から、技術・データ・製品等が意図せず外部に流出するおそれがあり、適切な情報管理に向けた取組が求められます。

組織としての対策の一例

個人としての対策の一例

組織内の情報管理を行う場合の主なポイント

- 情報の取扱いに関するルールを定めて、遵守する事項を明確にする。
- 情報を取り扱う機器やファイルを適切に管理し、紛失や持ち出しを防止する。
- 情報にアクセス可能な者を制限し、部外者による閲覧や窃取を防止する。
- 外部からの不審なアクセスを受けた際には、部内で速やかに報告を行う体制を整備し、他でも類似案件が発生しないよう案件を公表する。
- 情報管理に関する研修など組織内教育を定期的に行い、情報を取り扱う者の意識向上を図る。

官民連携・情報発信

官民連携の重要性

技術・データ・製品等の流出防止に向けて、企業・大学等や官公庁において懸念動向を把握し、適切に対応することが必要です。

公安調査庁では、技術・データ・製品等の流出防止には官民連携の強化が不可欠であるとの認識の下、経済安全保障に係る相談・連絡窓口を設置しているほか、各種情報発信を通じて不審なアプローチ等についての様々な知見を共有することで、企業・大学等からの技術等の流出防止に寄与しています。

情報発信

経済安全保障関連

公安調査庁ではホームページ内に経済安全保障特集ページを開設し、啓発動画やパンフレット等を公表しています。本パンフレットの掲載内容や経済安全保障について講演等を希望される企業・大学等のご担当者の方は、公安調査庁・渉外広報調整室（連絡先は下記参照）までお問い合わせください。

■啓発動画の公開

技術流出の危険性等についてまとめた動画を公開しています。

■経済安全保障関連動向

特集ページにて、関連する海外動向を年月別に公表しています。

■経済安全保障の確保に向けて

当パンフレットはホームページでも公表しています。

■講演の実施

ご依頼に応じて技術・データ・製品等の流出防止などをテーマとした講演を行っています。

経済安全保障に係る相談・連絡窓口

https://www.moj.go.jp/psia/kouan_mail_keizaianpo.html

E-mail **psia-es@i.moj.go.jp**

公安調査庁ホームページ

公安調査庁ホームページでは、公安調査庁の所管法令、沿革、業務内容などについて紹介しているほか、「経済安全保障特集ページ」「オウム真理教特集ページ」「世界のテロ等発生状況」など国内外の諸情勢に関する各種情報を発信しています。また、職員の採用情報や全国各地で実施している業務説明会の開催情報なども随時お知らせしていますので、是非ご覧ください。

https://www.moj.go.jp/psia/　公安調査庁　検索

公安調査庁ＳＮＳ公式アカウント

公安調査庁公式TwitterやYouTube公安調査庁公式チャンネルでは、公安調査庁の施策や取組、お知らせしたい情報等を発信していますので、ホームページと併せてご覧ください。

公安調査庁 Twitterアカウント　@MOJ_PSIA

公安調査庁 Twitterアカウント（採用担当）　@PSIA_recruit

YouTube 公安調査庁公式チャンネル　PSIAchannel

公表資料

内外情勢の回顧と展望

前年の公共の安全に関わる我が国内外の諸情勢について回顧し、今後を展望したものです。

内外情勢の回顧と展望
（令和4年（2022年）1月）

国際テロリズム要覧

国際テロリズムの潮流や国際テロ組織の概要・動向、地域別のテロ情勢等について、取りまとめたものです。

国際テロリズム要覧2021

サイバー空間における脅威の概況

近年のサイバー攻撃の脅威の態様や脅威主体、その手法や対策等について、取りまとめたものです。

サイバー空間における脅威の概況2022

全国ネットワーク

公安調査庁の組織は、内部部局、施設等機関及び地方支分部局からなり、内部部局として総務部、調査第一部及び調査第二部の３部、施設等機関として公安調査庁研修所があります。また、地方支分部局として全国に公安調査局と公安調査事務所があります。

1. 公安調査庁（本庁）
2. 公安調査庁研修所
3. 北海道公安調査局
4. 東北公安調査局
5. 関東公安調査局
6. 中部公安調査局
7. 近畿公安調査局
8. 中国公安調査局
9. 四国公安調査局
10. 九州公安調査局

●…公安調査事務所

公安調査庁

〒100-0013　東京都千代田区霞が関1-1-1 中央合同庁舎6号館　TEL：03-3592-5711（代表）　https://www.moj.go.jp/psia/