情報の力で、国民を守る。

PSIA 公安調査庁
PUBLIC SECURITY INTELLIGENCE AGENCY

経済安全保障の確保に向けて

技術・データ・製品等の流出防止

公安調査庁

はじめに

　経済安全保障をめぐる動きが世界中で活発化する中、我が国の「強み」である技術・データ・製品等を不当に手に入れようとする国家や組織・個人等（以下「懸念主体」という。）が、通常の経済活動や学術活動を装い、技術・データ・製品等を流出させようとするケースが把握されています。

　我が国から意図しない形で技術・データ・製品等が流出した場合、我が国が有する国際的な競争力や研究の新規性が失われるおそれがあるほか、大量破壊兵器等の研究・開発等に転用され、国民・国家の安全が脅かされるおそれもあります。

　狙われる技術・データ・製品等は、最新・最先端のものとは限りません。例えば、高精度・高品質を誇る我が国の汎用製品が、意図せぬ形で悪用されるケースが確認されています。

　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強化し、これらの流出を未然に防止することが重要です。

　本パンフレットは、経済安全保障の確保に向けた観点から、技術・データ・製品等の流出防止のためのポイントを御理解いただくために作成したものであり、このような観点を必要とする方々の一助となれば幸いです。

目次

我が国を取り巻く現状

米中対立下の経済安全保障情勢

- 米国が中国に対する先端技術分野での輸出規制等を強める中、中国は経済的威圧等でこれに対抗
- 米中両国は、デカップリング（経済分断）を避けつつ、幅広い経済分野で対立を継続
- 対立の影響は、EUが経済安全保障戦略を公表するなど、世界の幅広い分野に波及。
  経済活動を行う上で、経済安全保障への対応は避けて通れない情勢に

米中対立をめぐる動向

中国人研究者・留学生の入国規制
— 2018年6月以降

「国防権限法2019」に基づき中国企業をエンティティ・リスト(※)に掲載
— 2019年5月以降

「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

半導体関連製品の輸出管理規制の強化
— 2022年10月以降

中国政府の量子技術の向上に関与したこと等を理由に37の中国企業等をエンティティ・リストに追加
— 2024年5月

「信頼できない実体リスト規定」の制定
— 2020年9月

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

「反外国制裁法」の制定
— 2021年6月

レアメタルに関する輸出規制の強化
— 2023年8月1日以降

国家安全法制の改正・運用強化を継続
— 2023年7月「改訂『反スパイ法』」施行
— 2024年9月「改訂『保守国家秘密法実施条例』」の施行

「レアアース管理条例」を施行
— 2024年10月

（※）大量破壊兵器プログラム、テロリズム又は米国の国家安全保障・外交政策上の利益に反する活動に従事した団体や個人を掲載。同リストに掲載された者への輸出等を規制

ロシアによるウクライナ侵略をめぐる経済安全保障情勢

- 西側諸国が厳格な対ロシア制裁を実施する中、ロシアは様々な対抗措置を講じつつ、
  第三国を介するなどして西側製品を調達
- 我が国を含む主要国は、ロシア軍の兵器に搭載されていた製品を調査・特定し、
  同品目の輸出について注意喚起

対ロ制裁をめぐる動向

- ▶ 政府高官・オリガルヒ等の資産凍結
- ▶ SWIFTから一部銀行を排除
- ▶ 原油、石油製品の上限価格の設定
- ▶ 奢侈品等の輸出禁止
- ▶ 新規投資の禁止・制限
- ▶ 輸入規制・禁止措置
- ▶ 重要技術・製品の輸出管理の強化　etc.

- ▶ 一部製品のロシアからの輸出禁止
- ▶ 船舶の入港制限
- ▶ リース航空機の国外への搬出禁止
- ▶ 特許使用に際しての補償金不払い
- ▶ 撤退する外国企業に寄付義務付け
- ▶ 共同事業運営母体の再編
- ▶ 第三国を介した製品のう回調達　etc.

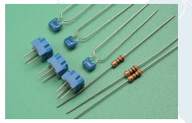
ロシア軍の兵器に使用された「Common High Priority Items」

我が国を含む主要国は、ウクライナで発見されたロシア軍の兵器に搭載されていた電子機器、機械部品等の製品を協力して調査・特定し、その結果を、「Common High Priority Items」と題する品目リストとして公表（2024年2月更新）。同品目の輸出に際し、最終需要者等を確認するよう注意喚起を実施。

集積回路

画像提供：Yotsuba/PIXTA（ピクスタ）

セラミックコンデンサ



画像提供：kj_port/PIXTA（ピクスタ）

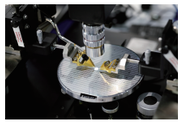
デジタルカメラ

画像提供：kuro3/PIXTA（ピクスタ）

玉軸受

画像提供：chormail/PIXTA（ピクスタ）

半導体製造装置



画像提供：genkur/PIXTA（ピクスタ）

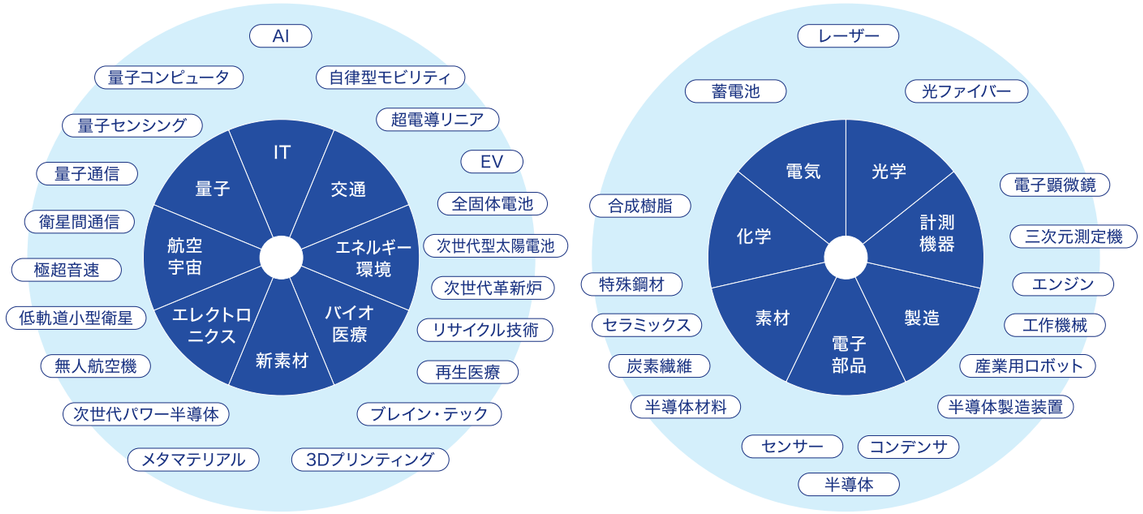
マシニングセンタ

画像提供：ivas76/PIXTA（ピクスタ）

注目される技術・製品等

近年、民生技術の発展が軍事分野に大きな影響を及ぼすようになったことなどを受け、安全保障の概念が、外交・防衛を中心とした伝統的な領域を超え、経済の領域まで拡大しています。

こうした情勢の中、主要各国では、AI、量子関連技術など、軍民両分野で“ゲームチェンジャー”となり得る新興技術や、その開発・製造に不可欠な基盤技術・汎用製品が、経済安全保障の観点から注目されています。



※この図は、公開情報を参考に技術分野を便宜的に分類し、イメージ化したものであり、技術全般について網羅的に記載したものではありません。

我が国では、従前から、技術・製品等が懸念主体による大量破壊兵器の開発等に転用されることを阻止するため、国際的な枠組み（国際輸出管理レジーム）や国内の関連法令に基づき、輸出管理措置等が実施されてきました。

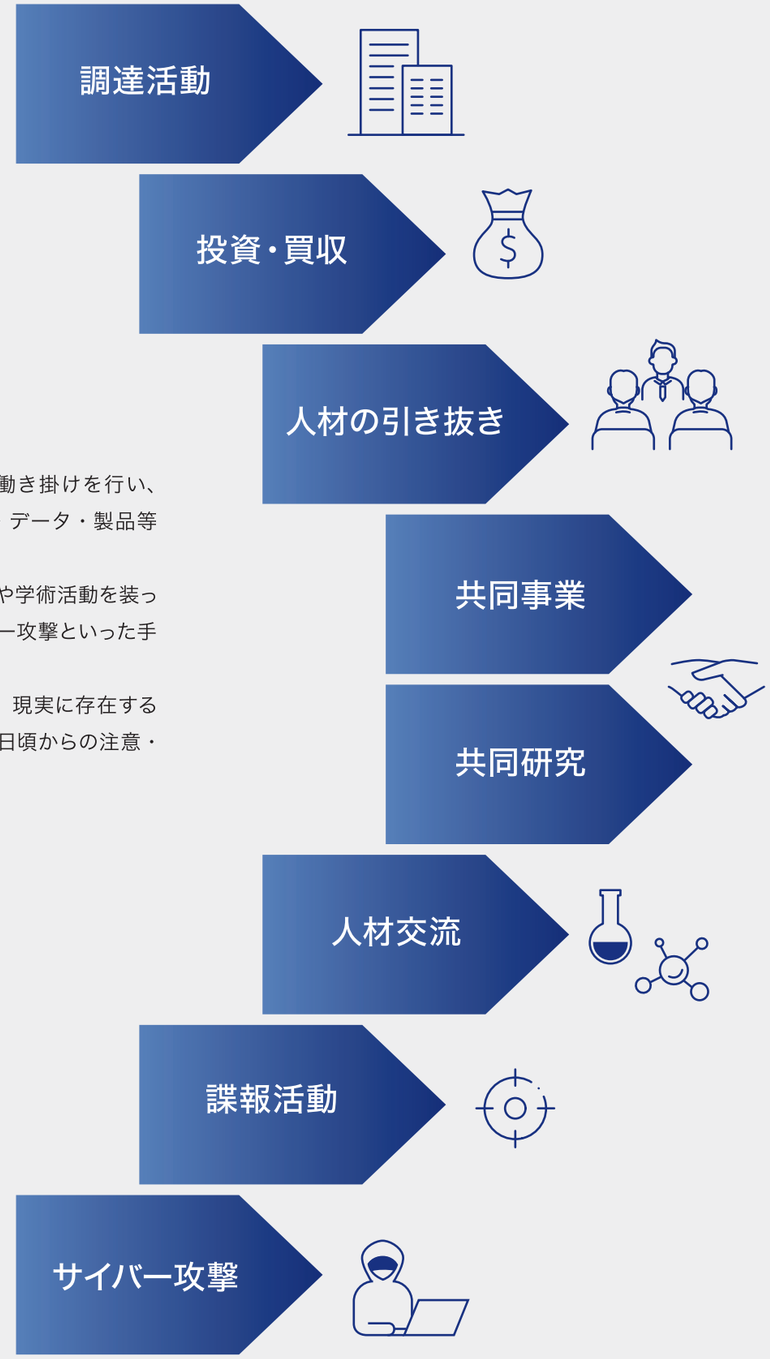
それに加え、今日では、我が国が他国に比して優位性（強み）を有する技術・製品の分野（又は、懸念主体側の“弱み”となっている分野）を把握した上で、それら技術・製品を意図しない形での流出から守るべく、輸出管理措置等の更なる強化のみならず、官民連携の推進や、大学・研究機関等における技術・データの適正な管理が必要とされています。

想定される流出経路

懸念主体は、様々な経路を通じた働き掛けを行い、我が国企業や大学等が取り扱う技術・データ・製品等を狙っています。

働き掛けの多くは、通常の経済活動や学術活動を装ったものであるほか、諜報活動やサイバー攻撃といった手法が用いられるケースもあります。

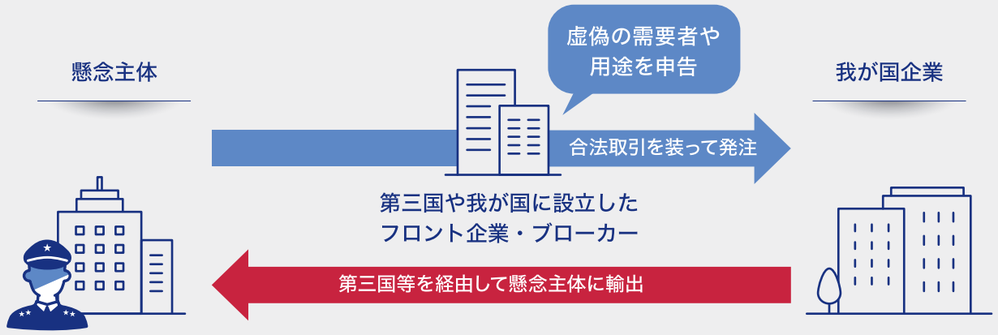
懸念主体によるこうした働き掛けは、現実に存在する脅威であり、流出の未然防止に向けた日頃からの注意・対応が必要です。



想定される流出経路

1　調達活動

懸念主体は、様々な手段を用いて、技術・製品等の調達を試みています。



近年の指摘

米国当局は、2024年、米国製重機のイランへの不正輸出に関与したとして、米国籍の人物が拘禁刑の判決を受けたと発表。同人は、米国企業から重機を購入後、最終荷受人をUAE企業と偽って輸出し、イランにいる共謀者が重機をUAEからイランに輸送

ドイツ当局は、2024年、中国国家安全部のために軍事転用可能な技術を収集・提供したとして、ドイツ人3名を逮捕。同人らは、軍艦に使用可能な舶用エンジン関連技術を入手するため、自らが経営する会社とドイツの大学との間で技術移転に関する協定を結ぶなどしたほか、国家安全部が提供した資金で特殊なレーザー装置を購入し、無許可で中国に輸出

米国当局は、2023年、輸出規制対象の米国製電子部品をロシアに輸送したとして、ロシア・ドイツの二重国籍者を起訴。ロシア及びキプロスに居住していた同人は、ロシアの軍関係企業に納入するため、最終需要者や用途を偽って米国企業から電子部品を調達。共謀者らが第三国で運営する企業を経由して同部品をロシアに輸送

注意すべきポイント

- 国内にも、懸念主体の調達活動に協力する企業・個人が存在することに留意
- 不審な点があれば躊躇せず相手方に確認するほか、企業内部の輸出管理体制や社内教育に十分なリソースを割くことも重要
- 通常の経済活動を装った悪意ある調達活動に巻き込まれないよう、以下の点に注意が必要

こんな相手ではありませんか？

- 商号や所在地が制裁対象に似ている
- 引き合い対象の製品に関する知見に乏しい
- ウェブサイトが存在しないか、インターネット上に情報が少ない
- ウェブサイトの記載内容が言語によって異なる
- 「学術目的で使用する」と称して、リスト規制品の購入を図る
- 商品の輸送をハンドキャリーで行おうとする
- 役員、所在地、連絡先が同一の別会社が存在する

こんな特徴はありませんか？

- 最終需要者が明確ではない、取引の途中で変更される
- 取引に必要な情報が十分に明かされない
- 仕向地ではない場所からサポートの依頼がある
- 最終荷受人・最終需要者が運送業者となっている
- 輸送コストが高く、時間が掛かる不自然な輸送ルートが指定される
- 全く同じ製品の引き合いが頻発する
- 用途と製品のスペックが釣り合わない

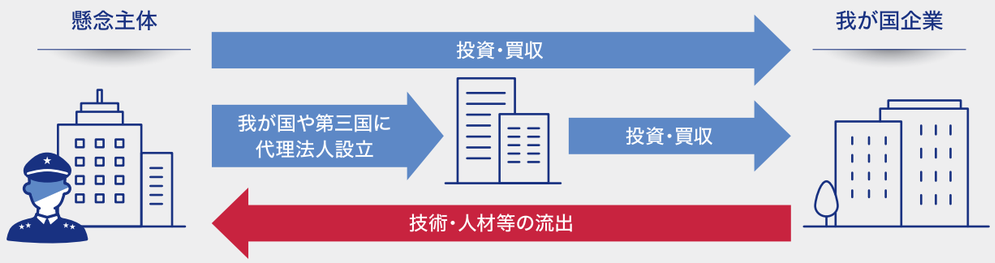
不自然な決済ではありませんか？

- 現金決済に固執する
- 法人口座ではなく、個人口座から支払おうとする
- 相場より異常に高い価格で買おうとする
- 第三者が取引代金を支払おうとする

想定される流出経路

2　投資・買収

経済安全保障上、重要な企業が懸念主体に買収された場合、
我が国の機微な技術・データ・製品等が流出するおそれがあります。



近年の指摘

ドイツ当局は、2024年、同国産業機械大手が手掛けるガスタービン事業の中国国有造船企業の子会社への売却について、安全保障を脅かすとして承認せず。ドイツメディアは、売却先の中国企業が駆逐艦のエンジンを製造しており、ドイツの技術が軍事利用される懸念がある旨指摘

中国企業傘下のオランダ企業が、英国半導体メーカーを買収したことを受け、英国当局は、2022年、技術的・地理的な理由から安全保障上のリスクがあるとして、同オランダ企業に取得株式の売却を命令。同オランダ企業は、同株式を米国の半導体メーカーに売却することで合意

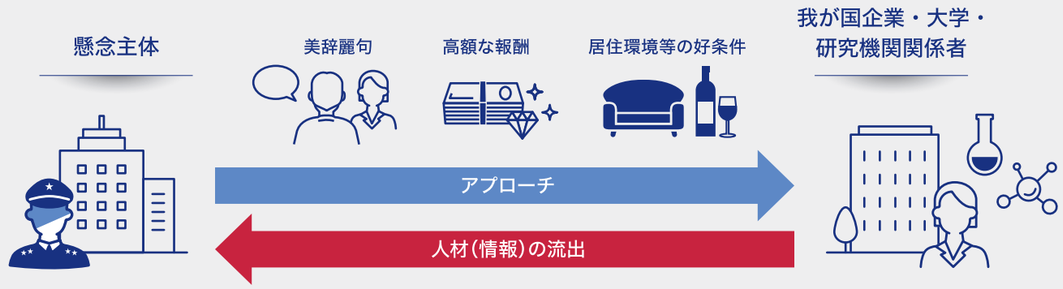
注意すべきポイント

- 懸念主体が重要技術を保有する我が国企業を買収したり、中小企業等の事業を継承したりすることで、技術・データ・製品等が流出するおそれ
- ベンチャー企業やスタートアップ企業による資金調達が、懸念主体による影響力行使に利用される懸念も
- 懸念主体が我が国や第三国に設立した代理法人等を通じて投資・買収を行うケースも
  投資・買収の主体が一見して懸念主体と無関係であったとしても、懸念主体の実質的な影響下にある場合もあり、資本関係に注意が必要

想定される流出経路

3　人材の引き抜き

懸念主体は、企業・大学・研究機関等の関係者が持つ知識や経験、
アクセス可能な情報等を狙い、様々な形でリクルート活動を行っています。



近年の指摘

台湾当局は、2024年、台湾企業から半導体を含むハイテク分野の人材を引き抜き、技術情報の窃取を試みたとして、複数の中国企業の拠点を捜査。この中には、台湾企業を装う形で企業を設立するとともに、100名近い人材を引き抜き、関連技術を持ち出そうとした中国企業も

韓国当局は、2024年、メモリ半導体の核心技術を中国に流出させ、不正使用した疑いで、韓国企業の元幹部2名を送致。元幹部の1人は、2020年、中国地方政府の資金で同国に半導体メーカーを設立し、韓国企業から約30名をリクルート。同メーカーは、リクルートに当たり、移籍前の2～3倍の年俸、中国滞在費、子供の教育費の支給等を提案

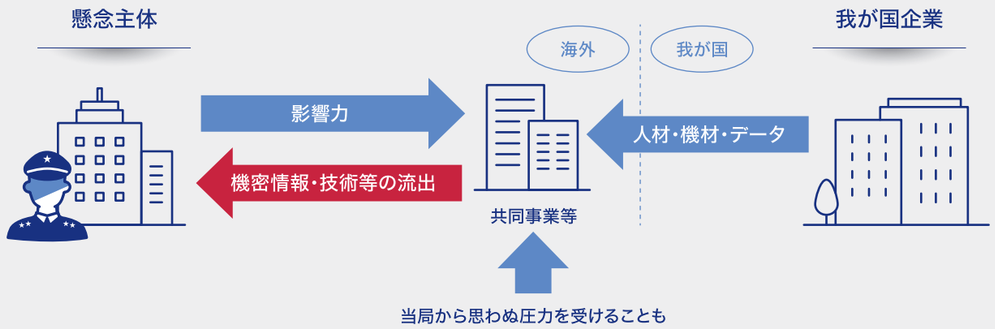
注意すべきポイント

- 懸念主体は、様々な手法を用いて引き抜きに向けたアプローチを実施。個人のSNSアカウントに対して接触が行われるケースも
- 高度な専門技能を有する人材のみならず、重要技術・データへのアクセス権限を有する人物も働き掛けの対象に
- 勧誘に当たっては、高額の報酬や住宅の提供、高位の役職といった条件が提示されることも。転職自体が違法行為に当たることはないが、社会通念を大きく上回るような好待遇・好条件の背後に潜む懸念主体の狙いに注意が必要

想定される流出経路

4　共同事業

海外での合弁会社の設立や現地工場の設置といった共同事業を通じて、
懸念主体に技術やデータ等が流出する事態が発生しています。



近年の指摘

英国当局は、2019年、外国と共同事業を行う上でのリスク軽減策を公表。外国と共同事業を検討する企業は、直面し得るリスクの特定と評価を行った上で、アクセス制限を始めとする物理的なセキュリティの強化、従業員の採用に伴うスクリーニングの実施、問題発生時の対応に関する事前検討などの対策が重要と指摘

中国当局は、2021年、重要データの保護に関する「データ安全法」を施行。中国国内で収集・生成された重要データは、中国国内で管理し、国外移転には当局の許可が必要。米国当局は、同法を含む中国の動向について、各国政府や企業の間で深刻な懸念が生じていると指摘

注意すべきポイント

- 共同事業で取り扱う技術・データ・製品等の範囲の明確化や、技術流出につながり得る契約項目の有無に関する事前確認が必要
- 共同事業等の相手が所在する国の法令等によっては、設備やデータの持ち出しに困難が生じるおそれも
- 外国企業に製造委託を行う際は、コア技術の流出防止等に向けた対策が重要

想定される流出経路

5　共同研究

懸念主体が持ち掛ける共同研究の中には、懸念主体側のみを利するものや、
研究成果が目的外利用されるおそれがあるものも存在します。

近年の指摘

カナダ当局は、2024年、同国の研究を保護するための新たな政策を発表。注意を要する研究分野及び懸念ある研究機関のリストを公表し、機微技術に関する共同研究を行う研究者に対し、リスク軽減のための事前審査を奨励。同国の特徴である開放的な研究環境が外国の標的となり、共同研究の枠組が国家安全保障を損なう形で悪用されることを懸念

米国の大学は、2024年、エンティティ・リストに掲載されている中国の大学との研究・教育連携の解消を発表。両大学は、中国国内における教育施設の設立、軍事転用可能な最先端半導体技術に関する共同研究等の連携を進めていたが、米国議会が、同共同研究について、中国人民解放軍の関連企業が関与していることなどの懸念を指摘

注意すべきポイント

- 共同研究の相手が懸念主体と接点を有している場合、研究成果が意図せぬ形で悪用されるおそれがあるほか、技術流出等が発生することでレピュテーションリスクを招く懸念も
- 共同研究の提案を受けた際には、相手方から提供された情報や公開されている情報を基にリスク評価を行い、受入れの可否の判断を行う必要。意図せぬ情報流出を防ぐため、必要なデータにのみアクセスを許可するといった管理も重要

想定される流出経路

6　人材交流

留学生・研究者の中には、懸念主体との関係性を秘匿するなど、
経歴を偽って来日する者が含まれている可能性があります。

近年の指摘

中国人民解放軍の現役の軍人が、所属を秘匿して米国に留学し、研究活動に従事。留学中、米国の文書や情報を中国に送るなど、同軍からの任務遂行を続けていた疑い。米国当局は、2020年、ビザの不正取得、外国政府の代理人としての活動の罪等で起訴

中国の軍系大学出身の研究者が、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。同研究者が論文に記載した肩書き（研究機関）は、中国軍系大学の複数の研究者が、留学時に使用した架空とされるもの

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を複数確認

注意すべきポイント

- 留学生・研究者を装った懸念主体関係者が入国し、我が国での研究等を通じて入手した技術・データ等を、自国の兵器開発や性能向上に利用するおそれ
- 研究の信頼・公正の確保に加え、留学生・研究者自身を守る観点からも、受入前の審査や、研究室等における受入後の指導・情報管理が重要

想定される流出経路

7　諜報活動

外国機関員等は、外交官や民間人に成りすましたり、様々な協力者を利用したりしながら、
我が国の企業、大学、研究機関等が保有する機微な情報の入手を試みています。

近年の指摘

2020年、我が国通信会社元社員が、同社のサーバ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。同社員は、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

オーストラリア当局は、2024年、年次脅威評価において、外国の情報機関員がビジネス特化型サイトを利用して標的を探している旨報告。外国の情報機関員は、機密情報へのアクセス権限を有するオーストラリア人を探した上で、様々な偽装身分を用いて標的に接触し、金銭を対価に政治、経済、外交、安全保障等に関するレポートの作成を依頼

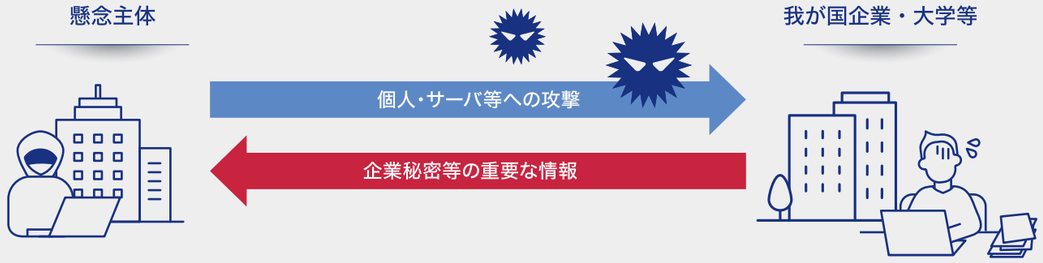
注意すべきポイント

- 外国機関員等は基本的に目立つことを嫌うため、標的となる人物と個別に接触しようとする傾向。不審な人物からの働き掛けに対しては、個人ではなく組織で対応することが必要
- ビジネス特化型サイトや転職サイト、SNSを通じた接触にも注意

想定される流出経路

8 サイバー攻撃

懸念主体によるサイバー攻撃も、技術やデータの流出経路となり得ます。
特に、国家等が関与・支援する高度なサイバー攻撃には、
コスト度外視で執ような攻撃が継続される傾向があり、警戒を要します。



近年の指摘

韓国のサイバー関連当局は、2024年、北朝鮮のサイバー攻撃主体が2023年後半以降、韓国の半導体業界を標的としたサイバー攻撃を行い、関連企業のサーバから製品の設計図面等を窃取したと発表。マルウェア(※)の使用を最小限に抑え、正規プログラムを使用した手法であるため、攻撃の検出が困難との指摘 (※不正なプログラム)

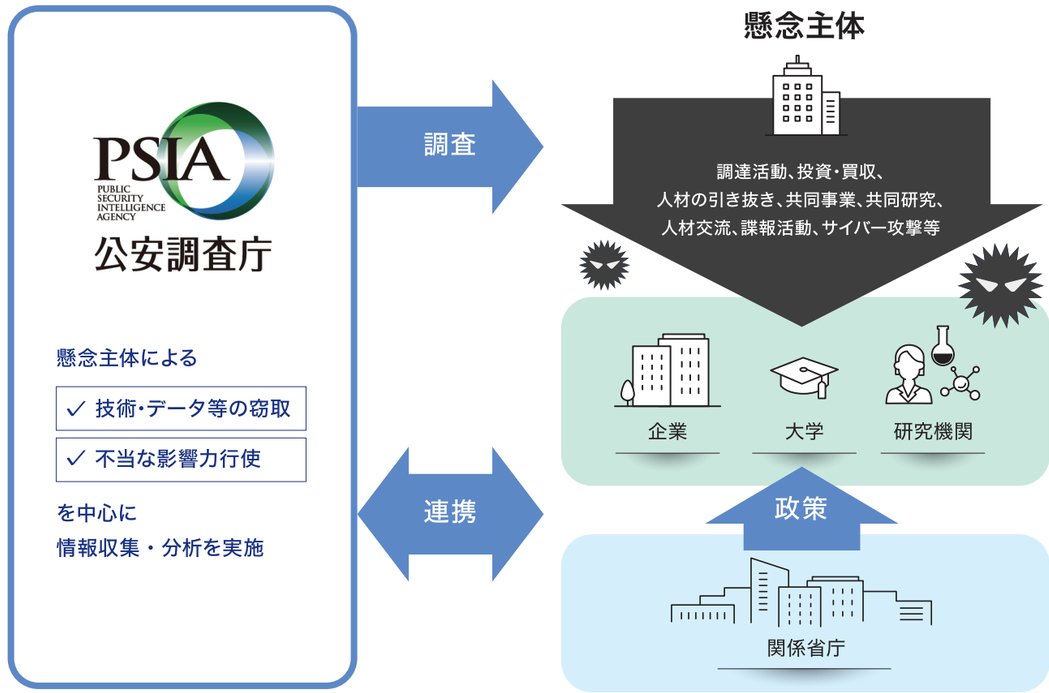
米国、英国及びポーランドのサイバー関連当局は、2023年、ロシア情報機関傘下のサイバー攻撃主体が2023年9月以降、チェコのソフトウェア企業が提供する製品のぜい弱性を悪用し、米国、欧州、アジア及びオーストラリアの幅広い業種の企業数十社のネットワークに侵入していたと発表

米国当局は、2021年、知的財産及び営業秘密の窃取を目的とした世界規模のサイバー攻撃キャンペーンに関与したとして、コンピューター詐欺罪及び経済スパイの共謀の容疑で、中国海南省国家安全庁の職員3名を含む関係者4名を起訴

注意すべきポイント

- 企業や大学・研究機関等で使用しているPCやサーバ等の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、速やかに最新版に更新するとともに、多要素認証の導入、パスワードの使い回しの禁止といった対応が重要
- システム上のセキュリティに加え、「人の心の隙」への対策も。少しでも不審点を感じた場合は、添付ファイルを開かない、URLをクリックしないなどの対応を
- 趣味や仕事内容、友人関係等に関するSNS投稿が、サイバー攻撃の端緒となる可能性にも留意が必要

公安調査庁の取組



安全・安心な環境作りに貢献

我が国は、経済安全保障の確保に向けた取組を進めており、2022年12月16日に閣議決定した「国家安全保障戦略」においても、「経済的手段を通じた様々な脅威が存在していることを踏まえ、我が国の自律性の向上、技術等に関する我が国の優位性、不可欠性の確保等に向けた必要な経済施策に関する考え方を整理し、総合的、効果的かつ集中的に措置を講じていく」としています。

公安調査庁は、所管法令に基づき必要な調査を行っており、懸念主体による

- **我が国の技術・データ・製品等の窃取**
- **経済活動を通じた不当な影響力行使**

等に関する情報収集・分析を行い、我が国情報コミュニティのコアメンバーとして、関係機関への情報提供や、企業・大学・研究機関等との官民連携の推進に活用することで、経済安全保障に係る政策立案及び技術・データ・製品等の流出防止に寄与しています。

官民連携の重要性・情報発信

技術・データ・製品等の流出防止のためには、標的となり得る企業・大学・研究機関等において、適切にリスクを把握し、懸念主体による技術窃取等に巻き込まれないようにしていただくことが重要です。

公安調査庁では、企業・大学・研究機関等との個別の意見交換や講演会等を通じ、具体的な技術流出等の事例や懸念主体による働き掛けの手口、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ます。

外部講演の模様

また、ホームページ内に経済安全保障特集ページを開設し、本パンフレットや経済安全保障に関する啓発動画、過去に実施した主な講演の概要等を公表しています。

経済安全保障特集ページ

技術・データ・製品等の流出に関する個別の御相談や講演依頼、企業等内でのパンフレットや動画の活用等を希望される場合は、下記「経済安全保障に関する御相談・講演依頼等窓口」まで御連絡願います。

経済安全保障に関する御相談・講演依頼等窓口

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

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、業務内容等について紹介しており、「経済安全保障関連動向」に加え、「オウム真理教特集ページ」、「世界のテロ等発生状況」等国内外の諸情勢に関する各種情報も発信しています。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、是非御覧ください。

公安調査庁ホームページ（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Ｘ（旧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御覧ください。

公安調査庁公式Ｘ（旧Twitter）アカウント
@MOJ_PSIA

公安調査庁公式Ｘ（旧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

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/

令和7年3月発行