技術流出の防止に向けて

警察庁
National Police Agency

警備局外事情報部外事課経済安全保障室

（協力：経済産業省）

はじめに

近年、国際情勢の複雑化、AI、量子技術等の革新的技術の出現、宇宙・サイバー・電磁波といった安全保障における新たな領域の誕生等により、安全保障の裾野が経済・技術分野に拡大しています。

このような情勢の下、諸外国では、産業を強化するための支援、自国にとって大事な技術の流出防止、輸出管理の強化など、経済安全保障のための施策が推進されています。

我が国においても、安全保障の確保に関する経済施策として所要の制度を創設することを内容とする経済安全保障推進法の全ての規定が、令和6年5月までに施行されました。
また、重要経済安保情報の指定やその取扱者の制限、我が国の安全保障の確保に資する活動を行う事業者への重要経済安保情報の提供等について所要の制度（いわゆる経済安全保障分野におけるセキュリティ・クリアランス制度）を整備することなどを内容とする重要経済安保情報保護活用法の全ての規定が、令和7年5月までに施行され、経済構造の自律性の向上や技術の優位性・不可欠性の確保を進め、国民の安全・安心を守るという経済安全保障の取組が進められています。

こうした中、技術流出の防止も、経済安全保障上の重要な課題となっています。

我が国には、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。
これらの技術や研究成果の中には、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重大な影響が生じかねません。

警察ではこの課題に対し、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の情報を提供する活動（アウトリーチ活動）を推進しています。
身近に迫るリスクには警察だけでなく、皆さん自身による自主的な取組が必要です。

このパンフレットは、アウトリーチ活動の一環として、企業やアカデミアの管理者や社員・研究員などを対象に、技術流出のリスクのパターンや、一人ひとりが気を付けるべきポイントを示し、自主的な対策に生かしていただくことを目的としています。

皆さんの大事な技術をともに守っていくために、現在実施している様々な対策と合わせて、このパンフレットを参照していただければ幸いです。

目 次

技術流出を防止するために

技術流出を防止するためには、「情勢」「事例」「対策」を理解することが重要です。

情勢 今、何が起きているのか

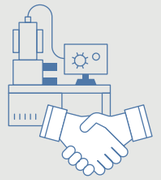
近年、地政学上のリスクがクローズアップされ、**国際的な産業競争が激化**しています。
日本には、規模の大小に問わず、先端技術を保有する企業やアカデミアが多数存在しますが、こうした技術を入手して**自国産業を強化**したり、**軍事技術に転用**したりしようとする**外国から狙われるようになっています。**

技術流出の防止は経済安全保障上の課題に

事例 どのようにして起きるのか

外国から企業やアカデミアの技術が狙われるリスクのパターンは、大きく**3つに分類**することができます。

技術流出リスクのパターン

サイバー攻撃による技術流出	スパイ工作による技術流出	経済・学術活動を通じた技術流出
		

技術流出はどのようにして起きるのか

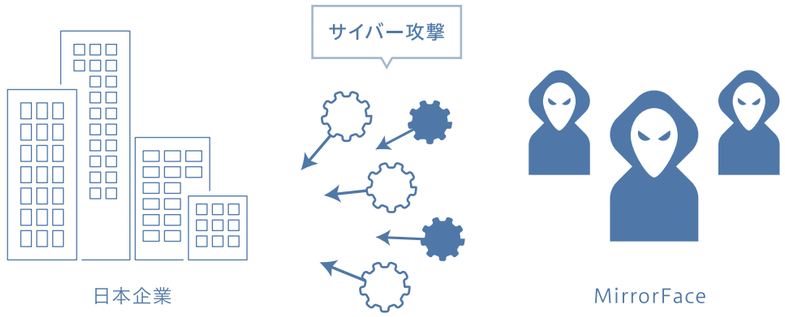
実際にあった技術流出の検挙事例や、
技術流出のリスクが高まるケースを見てみましょう。

サイバー攻撃による技術流出

国内外で政府機関や重要インフラ事業者などを標的としたサイバー攻撃が激しさを増しています。
あらゆる産業でDX（デジタルトランスフォーメーション）が進むにつれ、サイバー攻撃や不正アクセスによって、直接的に情報を窃取される危険性も増しています。

CASE 1

MirrorFace（ミラーフェイス）と呼称されるサイバー攻撃グループが、令和元年頃から国内の組織、事業者及び個人に対して、マルウェアを添付したメールやマルウェアをダウンロードさせるリンクを記載したメールを送信して感染させる標的型メール攻撃や、ネットワーク機器（特にVPN機器等）のぜい弱性を悪用した標的ネットワーク内への侵入により、情報窃取を目的としたサイバー攻撃を行っていることが確認されています。これらサイバー攻撃は、中国の関与が疑われる組織的なサイバー攻撃活動であると評価されています。

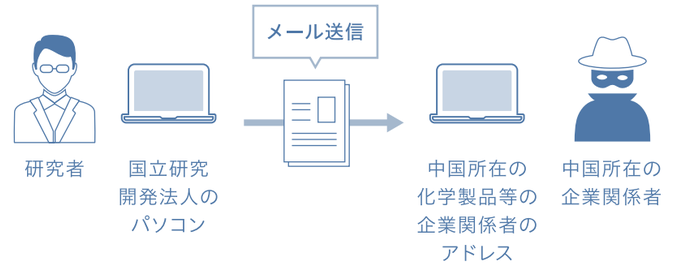


スパイ工作による技術流出

サイバー上のリスクだけではなく、人を通じた情報の窃取にも備えなければなりません。
こうしたパターンでは、外国が企業などの情報にアクセスしやすくなるよう、スパイとなる者を仕立てて情報を盗ませるといったケースに注意が必要です。

CASE 1

国立研究開発法人の外国人研究者が、平成30年４月に、中国に所在する企業が使用するメールアドレスに対して、同研究所の営業秘密であるフッ素化合物の合成技術情報の研究データを送信して開示したとして、令和５年６月に警視庁が同研究者を不正競争防止法違反の罪で逮捕しました。



CASE 2

大手化学メーカーの従業員は、平成30年から平成31年にかけて、同社の営業秘密である液晶技術に関する技術情報を不正に領得した上、中国に所在する企業に開示したとして、令和２年10月に大阪府警察が不正競争防止法違反の罪で検挙しました。
中国企業は、ビジネス用SNSを使用して従業員に接触したとされています。

経済・学術活動を通じた技術流出

経済活動がグローバル化し、また、研究活動のオープン化・国際化が進展する中で、合弁や企業の買収、共同研究など、それ自体は合法な経済・学術活動についても、これを隠れ蓑にすることにより情報が狙われるリスクが存在します。

CASE 1

宇宙関連研究開発のベンチャー企業の経営者が、事業関連のイベントに参加した際、米国政府機関職員で中華系アメリカ人と名乗る男が接近、連絡先等を交換しました。
後日、男は経営者に対して、「米日中露共同の宇宙開発計画があり、食事をしながら意見交換がしたい、あなた一人で来てほしい」等と１対１での接触を持ち掛けてきました。
しかし、経営者が確認したところ、男は同政府機関での在籍事実が無く、身分を偽って接近したものと判明しました。

CASE 2

国内の大学は、外国企業から、先端技術で作製した試験用細胞の提供を求められ、輸出許可を受けた上で手続きを進めていたところ、同国税関が輸出手続きの不備を主張し、本来必要のないはずの同細胞の作製方法、研究資料まで提出を要求されました。
大学側では、技術流出の危険性があるとして外国企業との取引を中止、「当該外国企業との取引を察知した税関が関連技術の獲得を目的として介入した」と受け止めています。

対策
何をすべきか

一人ひとりが、技術流出のリスクや手口を認識し、基本的な対策を講じることが重要です。
次ページ以降に、そのヒントやエッセンスをまとめました。「自分の身にも起こるかもしれない」という意識を持ち、日々の行動に役立ててください。

最初にすべきこと
秘密情報の指定と管理

技術流出を防ぐためには、
3つのステップを理解し、
実行していくことが重要になります。

Step 1

保有する情報の
把握・評価及び秘密情報の決定

[1] 企業が保有する情報の全体像を把握

自社の保有する情報を把握します。情報は紙、サーバーやPC内の電子データだけでなく、従業員が業務の中で記憶した製造ノウハウなど、文章化されず目に見えない形で存在する場合もあるので、漏れのないように注意しましょう。

[2] 保有する情報の評価

把握した情報を、経済的価値や漏えい時の損失の程度といった指標に基づいて評価します。

指標に基づく評価

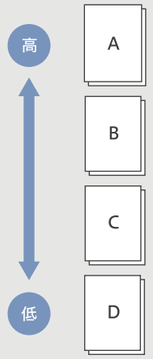
- 経済的価値
- 情報管理の必要性・程度
- 漏えい時の被害（経済的損害、競争力や社会的信用の低下等）
- 競合他社からみた有用性
- 契約等で他者から預かった情報か否か

[3] 秘密情報の決定

情報の評価の高低を基準に保護に値するかどうか判断します。
想定される管理コスト、訴訟コストのほか、漏えいによって被るおそれのある損失など総合的に判断をしましょう。

相対的な階層化

損失の大きさ順に情報を序列化



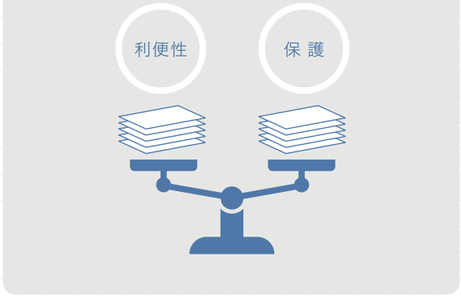
相対的な評価

損失の大きさを評価

漏えい時に極めて重大な損失	
漏えい時に重大な損失	A
漏えい時に軽微な損失	B C D

Step 2

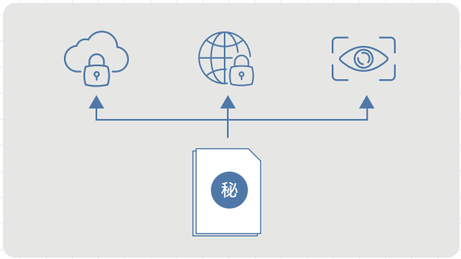
秘密情報の
分類



各企業で取り扱う秘密情報の内容・性質やその評価の高低、その利用態様、企業において採用することが可能な管理措置などの事情に応じ、秘密情報の管理水準を分類していきます。
情報と保護の観点と日頃の業務で情報を使う場合の利便性の観点とのバランスをとることが重要です。

Step 3

秘密情報の分類に応じた
対策の選択



秘密情報の分類ごとに、具体的にどのような情報漏えい対策を講ずるのかを選択します。
誰に対して対策を行うのか、どのような形で秘密情報が存在しているのか、漏えいの手口やその動機がどんなものかといった状況によって効果的な対策は異なります。
テレワークの有無などによっても判断が変わるので、各社に応じた対応をしましょう。

5つの漏えい対策

漏えい対策には、大きく5つの対策があります。
それぞれの対策と目的を理解し、社内への浸透を目指しましょう。

物理的・技術的な防御

1 秘密情報に「近寄りにくくする」ための対策

接近の制御

［具体例］
- アクセス権の限定
- 秘密情報を保存したPCはインターネットにつながない

2 秘密情報の「持出しを困難にする」ための対策

持出し困難化

［具体例］
- 私物USBメモリ等の利用・持込み禁止

心理的な抑止

3 漏えいが「見つかりやすい」環境づくりのための対策

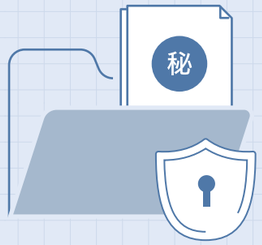
視認性の確保

［具体例］
- レイアウトの工夫
- 防犯カメラの設置

4 「秘密情報と思わなかった」という事態を招かないための対策

秘密情報に対する認識向上

［具体例］
- マル秘表示
- ルールの策定・周知



5 社員のやる気を高めるための対策

信頼関係の維持・向上等

［具体例］
- ワークライフバランス
- 社内コミュニケーション

出典：経済産業省「秘密情報の保護ハンドブック」

対策①

サイバー攻撃への備え

Cyberattacks

3つの基本的対策

1 リスク低減のための措置

- パスワードが単純でないかの確認、アクセス権限の確認、多要素認証の利用、不要なアカウントの削除などにより、本人認証を強化する。
- IoT機器を含む情報資産の保有状況を把握する。特にVPN装置やゲートウェイなど、インターネットとの接続を制御する装置の脆弱性は、攻撃に悪用されることが多いことから、セキュリティパッチ（最新のファームウェアや更新プログラムなど）を迅速に適用する。
- メールの添付ファイルを不用意に開かない、URLを不用意にクリックしない、連絡・相談を迅速に行うことなどについて、組織内に周知する。

2 インシデントの早期検知

- サーバなどにおける各種ログを確認する。
- 通信の監視・分析やアクセスコントロールを再点検する。

3 インシデント発生時の適切な対処・回復

- データ消失などに備えて、データのバックアップの実施及び復旧手順を確認する。
- インシデント発生時に備えて、インシデントを認知した際の対処手順を確認し、対外応答や社内連絡体制を準備する。

「サイバーセキュリティ経営ガイドライン」の活用

経済産業省が作成している「サイバーセキュリティ経営ガイドラインVer3.0」では、経営者が認識すべき原則や指示すべき事項（リスク管理体制の構築など）について記載されています。
また、独立行政法人情報処理推進機構（IPA）が作成した「サイバーセキュリティ経営ガイドラインVer3.0実践のためのプラクティス集 第４版」では、各セキュリティ担当者の悩みと、具体的な実践事例が記載されています。
サイバーセキュリティ対策を講じる上で参考となります。3つの基本的対策と合わせ、是非ご活用ください。

経営者の認識と体制構築

経営層の心構えとサイバー対策で重要な体制の構築が記載

経済産業省「サイバーセキュリティ経営ガイドライン Ver3.0」

具体的対策

悩みに対して取るべき対策が詳細にわかる

IPA「サイバーセキュリティ経営ガイドラインVer3.0実践のためのプラクティス集 第４版」

対策②

スパイ工作への備え

Espionage

見知らぬ外国人からのメッセージや外国企業からのプレゼントなど
普段とは異なる相手との接触には、スパイ工作の危険性が潜んでいます。

See：相手をよく見る

プライベートやSNSなど、普段のビジネスシーンとは異なる場面で
出会った相手については、所属や連絡先などの情報を確認しましょう。

- 悪意ある者が近付いてくるリスクは誰にでもあります。
- あなたのことを調べた上で、偶然を装って近付き、食事に誘い出すなどして情報を引き出そうとするケースもあります。
- 相手の会話内容とプロフィールに矛盾がないか、相手の会社は実在するかなどもチェックポイントです。

Stop：立ち止まって考える

SNSなど、不特定多数の人の目に触れる場所に個人情報を記載する時は
立ち止まって慎重になりましょう。

SNSは便利なツールですが、悪意ある者は、ターゲットの個人情報を調べ上げ、接近する際の口実や脅迫などに利用する可能性もあります。

相手からの贈り物には、一度立ち止まって慎重になりましょう。

相手からのプレゼントやご馳走は、あなたを「断りづらい状況」に追い込み、後からあなたに情報提供を要求するきっかけとなる可能性があります。
なぜ個人的に贈り物をするのか、その意味を冷静に考えましょう。

Share：共有する・相談する

ささいなことでも上司や同僚に共有・相談しましょう。
不審に思うことがあれば、警察にも相談してください。

- 悪意ある者はひそかにターゲットに狙いを定めます。見知らぬ人からのコンタクトや不審な働き掛けがあった場合、相談することで冷静になり、共有することで周りの人がターゲットにされることも防げます。
- 情報の提供を依頼された場合に、「これくらいの情報なら」「相手はいい人だから」と軽く考えると、大切な技術が流出してしまうだけでなく、あなたが法律違反に問われる可能性もあります。

一人ひとりに守ってほしい 3つのS

- See　相手・書類をよく見る
- Stop　立ち止まって考える／リスクを把握する
- Share　共有する／相談する

対策③

経済・学術活動における備え

Business/Academic Activities

合弁企業の設立、共同研究の実施など外国企業とのコラボレーションは、
企業価値を高めるチャンスとなる一方で、技術流出を招くリスクも秘めています。

See：相手・書類をよく見る

取引などの相手方となる外国企業をよく確認して下さい。

- 外国企業との合弁や買収、共同研究を抑制することではなく、背景に存在するかもしれない技術流出のリスクを認識することが重要です。
- 専門家により、相手方の実態をチェックすることも有効です。

技術流出のリスクを認識しましょう。

- 契約書などの記載内容もよく確認して下さい。
- 相手を信頼して確認を怠ると、“輸出管理条項”などの重要な項目が、説明なく削除される可能性もあります。担当部署や専門家などによる確認も有効です。

Stop：立ち止まってリスクを把握する

外国への技術の提供につながる行為や活動については、
一度立ち止まり、リスクを踏まえた検討を行って下さい。

- 外国企業から契約成立直前に機器の不備を指摘され、設計図の閲覧や機器の試作品の提供を要求されたというケースがありました。
  こうしたケースで相手側に渡してしまった機器などから技術が盗まれる可能性もあります。
- 例えば、外国への進出や合弁企業の設立に伴うリスクだけではなく、外国からの撤退や合弁の解消などに伴うリスクもチェックポイントです。
- その国の法律や、リスクのある事例を確認するための業界内での情報交換も有効です。

Share：共有する・相談する

機微な技術の提供を含む取引については、
関係部署などに情報共有・事前相談をしてください。

取引の成立に向けて集中していると、輸出管理や営業秘密管理などがおろそかになり、対応を誤って関係法令に抵触してしまう可能性もあります。

不審な動向があれば関係機関や警察に相談してください。

- 一度技術情報が流出してしまったら、取り戻すことはできません。
- 未然防止のためにも、外国への技術の提供をめぐって不審に感じることがあれば、関係機関や警察に相談してください。

警察庁webサイト 技術流出の防止に向けて
https://www.npa.go.jp/bureau/security/economic-security/index.html

警備局外事情報部外事課経済安全保障室
keizaianpo110@npa.go.jp