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

最近、ニュースや新聞で「経済安全保障」という言葉を見ない日はありません。
今、なぜ、この言葉が取り上げられるのでしょうか。

-国家間の競争が激しくなっていること
-AIや量子などの革新的な技術が現れたこと
-宇宙・サイバー・電磁波といった安全保障上の新たな領域が誕生したこと
-コロナ禍などにより、サプライチェーンの脆弱性が明らかになったこと

こうした様々な変化により、日本の安全保障を考えなくてはならない場面が、経済や技術の分野に広がりつつあります。

このような情勢を踏まえ、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。
日本でも、経済の自律性の確保、技術の優位性や不可欠性の獲得、国際秩序の維持・強化といったキーワードを柱とした施策が進められています。

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すことを目的としています。

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。

令和4年8月

目　次

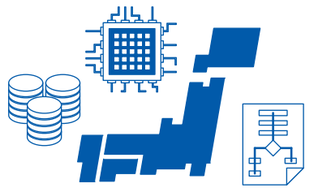
技術流出を防止するために

01 情勢を知る → 02 事例を知る → 03 対策を知る

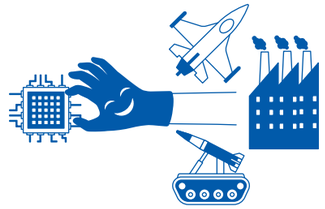
技術流出を防止するためには、「情勢」「事例」「対策」を理解することが重要です。

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



日本には、規模の大小を問わず、先端技術を保有する企業やアカデミアが多数存在



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

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

1 サイバー攻撃による技術流出

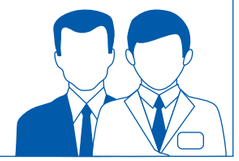
国内外で政府機関や重要インフラ事業者などを標的としたサイバー攻撃が激しさを増しています。
あらゆる産業でDX（デジタルトランスフォーメーション）が進むにつれ、サイバー攻撃や不正アクセスによって、直接的に情報を窃取される危険性も増しています。

2 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。

3 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。

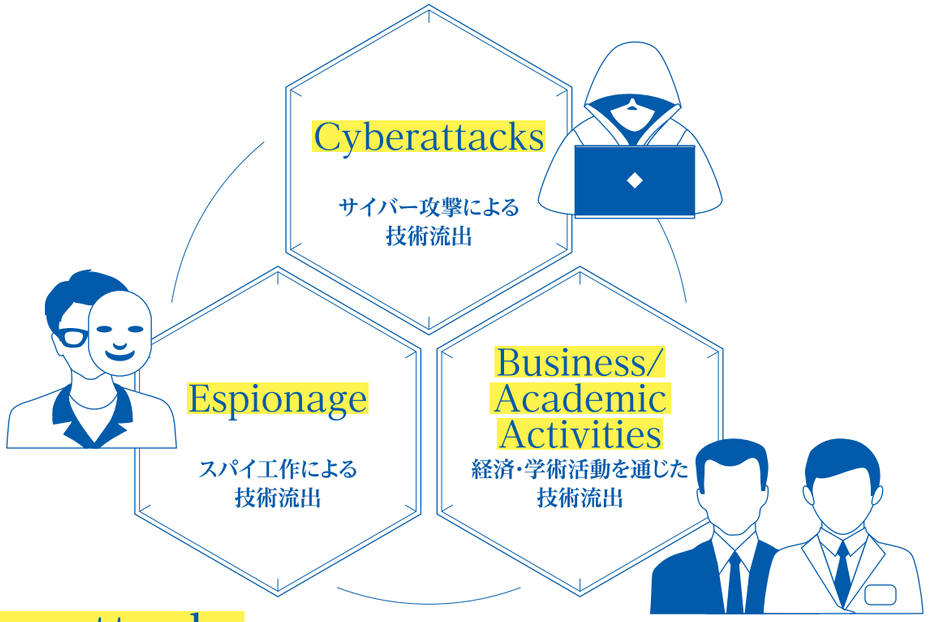


対策～何をすべきか

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。

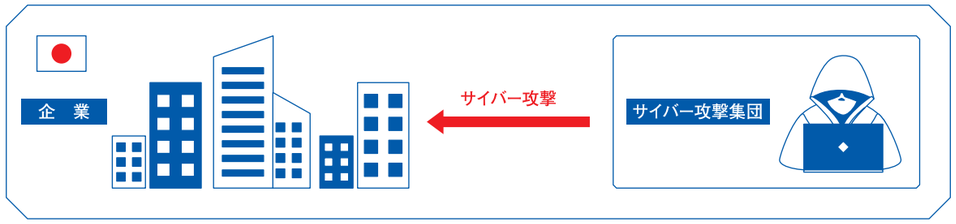
技術流出はどのようにして起きるのか

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。



Cyberattacks

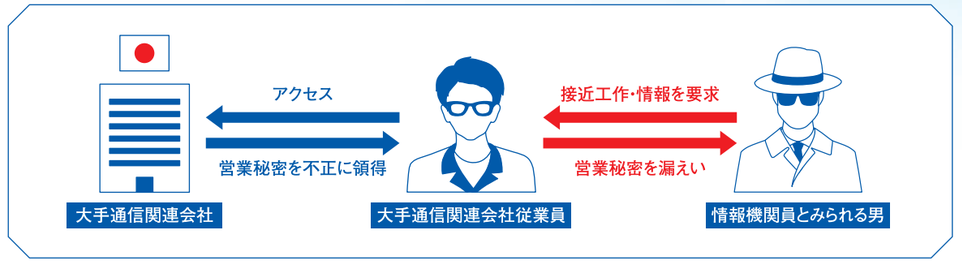
CASE1 平成28年から翌年にかけて、住所、氏名などを偽って日本のレンタルサーバの契約に必要な会員登録を行ったとして、令和3年、警視庁が中国共産党員の男を検挙しました。この事件の捜査を通じ、航空宇宙関連組織に対するサイバー攻撃が、中国人民解放軍を背景に持つ可能性が高いサイバー攻撃集団によって実行されたものと結論付けられました。他にも、同一の攻撃集団が関与している可能性が高いサイバー攻撃が、約200の国内企業などに対して実行されていたことが把握されました。



CASE2 外国に進出している日本企業が、現地の経済特区への移転について交渉していた際、外国当局から、技術情報などの提供・共有を要求されました。同社が、この要求を拒否したところ、その日からサイバー攻撃を受ける事態になりました。

Espionage

CASE1 大手通信関連会社の従業員が、平成31年2月から3月にかけて、同社の営業秘密である無線基地局の実証実験に関する情報を不正に領得し、ロシアの情報機関員とみられる者に渡したとして、警視庁が両人を不正競争防止法違反などの罪で検挙しました。



CASE2 外国政府機関職員は、日本の先端技術を有する企業の複数の職員に対し、帰宅途中を見計らって声を掛け、道を尋ねる口実で接近しました。後日個人的に会おうと酒席へ誘い出していました。

Business/Academic Activities

CASE1 国内のある大学では、情報の流出防止に関する“輸出管理条項”を盛り込んだ上で、外国の大学と人材交流プログラムを締結しました。その後、先方から既存の合意書を再作成したいとの要望があったことから内容を確認したところ、新しい案文では“輸出管理条項”が何の説明もなく削除されていました。

CASE2 外国企業が、日本の大学教授に共同研究を持ち掛けました。教授は、この外国企業が別の国の規制リストに掲載されていたことから申し出を断りましたが、「形式だけ別の企業の名前を使うのはどうか」と提案されました。

最初にすべきこと
～秘密情報の指定と管理

3つのステップ

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	STEP 2	STEP 3
保有する情報の把握・評価及び秘密情報の決定	秘密情報の分類	秘密情報の分類に応じた対策の選択

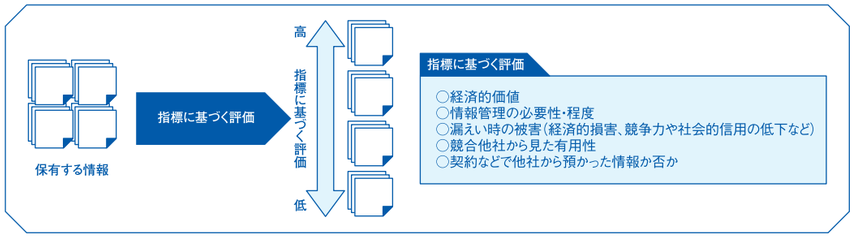
STEP 1 保有する情報の把握・評価及び秘密情報の決定

（1）企業が保有する情報の全体像の把握

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。

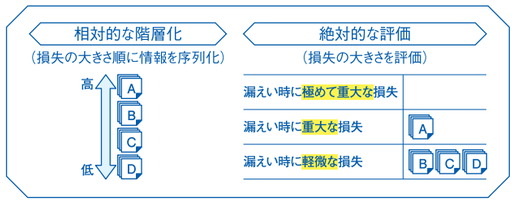
（2）保有する情報の評価

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。



（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。



STEP 2 秘密情報の分類

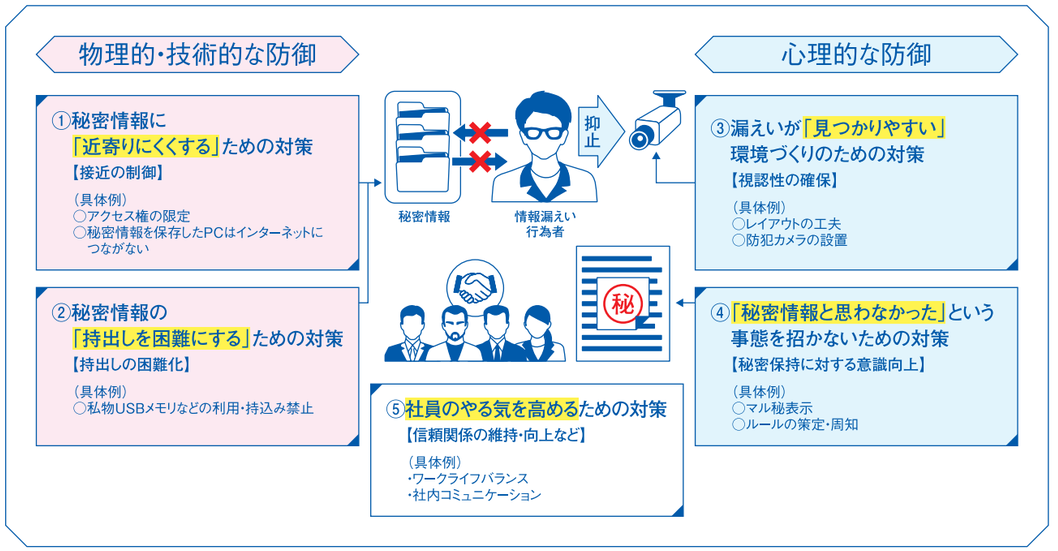
各企業で取り扱う秘密情報の内容・性質やその評価の高低、その利用態様、企業において採用することが可能な管理措置などの事情に応じ、秘密情報の管理水準を分類していきます。情報と保護の観点と日頃の業務で情報を使う場合の利便性の観点とのバランスをとることが重要です。

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。



【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。

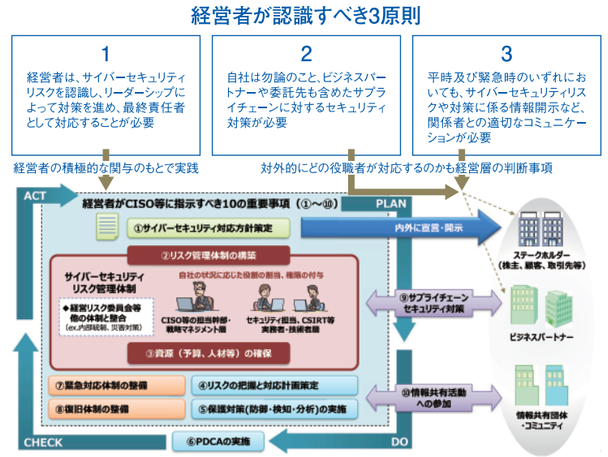
3 インシデント発生時の適切な対処・回復

- 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。

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」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Ver2.0実践のためのプラクティス集」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

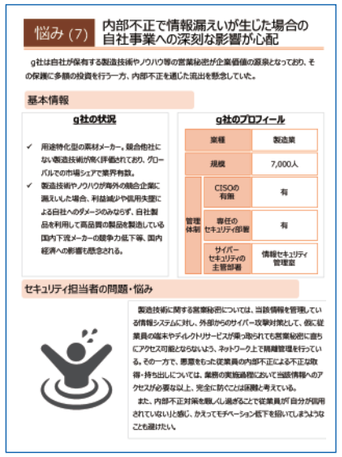
経営層の心構えとサイバー対策で重要な体制の構築が記載



【出典:経済産業省「サイバーセキュリティ経営ガイドラインVer2.0 付録F」】

具体的対策

悩みに対して取るべき対策が詳細にわかる



【出典:独立行政法人情報処理推進機構（IPA）「サイバーセキュリティ経営ガイドラインVer2.0実践のためのプラクティス集第3版】

対策②
～スパイ工作への備え

Espionage

一人ひとりに守ってほしい3つのS

1 **See** 相手を よく見る

2 **Stop** 立ち止まって 考える

3 **Share** 共有する・ 相談する

こんなことありませんでしたか?

- ☑ 個人のSNSに、接点のない外国企業からメッセージが送られてきた
- ☑ 道端で、見知らぬ外国の人に声を掛けられた
- ☑ 付き合いのある外国企業の人から、「お礼」としてプレゼントやご馳走をされた
- ☑ 外国企業の人から、アクセス制限のある情報の提供をお願いされた

これらは、スパイがあなたに
近付いてくるときのサインの一例です。
スパイ工作から身を守るため、
何に気を付ければいいでしょうか。

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。

対策③
～経済・学術活動における備え

Business/
Academic Activities

企業やアカデミアに守ってほしい3つのS

1 **See** 相手・書類をよく見る

2 **Stop** 立ち止まってリスクを把握する

3 **Share** 共有する・相談する

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、
意図・予測していなかった技術流出を招く
リスクも秘めています。
こうしたリスクが、日本の安全保障にも
影響を与えかねないといわれている昨今、
企業やアカデミアは何に気を付ければいいでしょうか。

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。

外国における技術流出防止に関する啓発動画

FBI

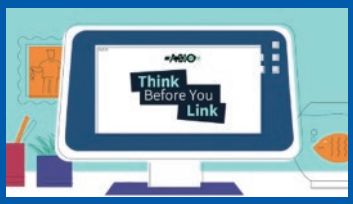
The Nevernight Connection

（日本語字幕あり）

FBI

The Company Man: Protecting America's Secrets

（日本語字幕あり）



ASIO

Jack's Story- Think Before You Link

FBI：Federal Bureau of Investigation（米国連邦捜査局）
ASIO：Australian Security Intelligence Organisation（オーストラリア保安情報機構）

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