

技術流出対策ハンドブック

中堅・中小企業編

今日から
はじめる技術流出対策



経済産業省

Ministry of Economy, Trade and Industry



技術流出対策ガイドス
本編はこちら

大切な技術、守れていますか？

技術流出は事業活動に大きなダメージを与えます

信頼の低下

大事な技術情報が漏えいすると、取引先や顧客、株主からの信頼が低下します。信頼の低下は、取引停止等にもつながります。



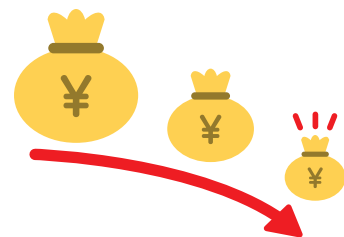
競争力の喪失

技術やノウハウが流出すると、自社の強みが失われ、他社製品と差別化できなくなります。その結果、市場での競争力を喪失し、顧客を失う可能性があります。



経済的損失

これまで技術開発に投下したコストの回収が困難となるほか、流出した技術を用いて他社が安価に類似品を作ってしまうことで、利益が減少してしまいます。



法的リスクの増加

取引先との契約に基づく管理や、法令で義務付けられる管理が行われていない場合、訴訟等のリスクが発生します。



目次

事例

人を通じた技術流出の事例 3~4ページ

- SNSを通じた接触をきっかけに技術流出したケース
- 競合他社による社員の引き抜きによって技術流出したケース
- 展示会への出展をきっかけに技術流出したケース
- 産業スパイの接触をきっかけに技術流出したケース

すり合わせに伴う技術流出の事例 5~6ページ

- 原料メーカー（仕入先）から技術流出したケース
- 製造装置メーカーから技術流出したケース
- 海外顧客へのサンプル提供をきっかけに技術流出したケース
- 製造委託先が無断で再委託し技術流出したケース

生産拠点の海外進出に伴う技術流出の事例 7ページ

- ライセンス契約先（海外企業）から技術流出したケース
- 撤退時の管理不足から技術流出したケース

共同研究に伴う技術流出の事例 8ページ

- 共同研究先の従業員から技術流出したケース
- 共同研究先の委託先から技術流出したケース

対策

まず最初にやるべき対策 9~10ページ

人を通じた技術流出への対策 11~12ページ

すり合わせに伴う技術流出への対策 13~14ページ

生産拠点の海外進出に伴う技術流出への対策 15ページ

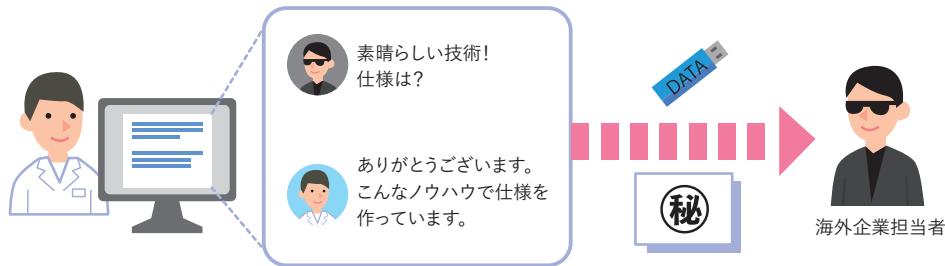
共同研究に伴う技術流出への対策 16ページ

技術流出対策チェックリスト 17~18ページ

人を通じた技術流出の事例

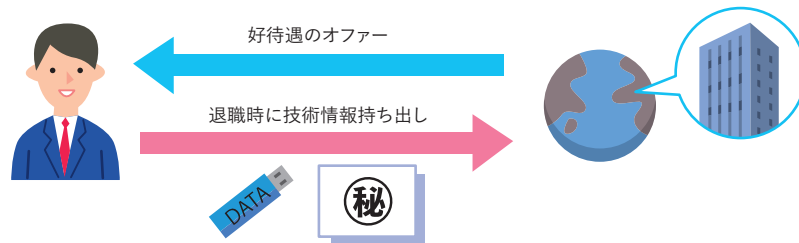
Case 1 SNSを通じた接触をきっかけに技術流出したケース

ビジネス用SNSを通じて、海外企業の担当者を名乗る者から、自身が関与した製品について質問を受けた。つい嬉しくなり、非公開の技術情報まで提供してしまった。



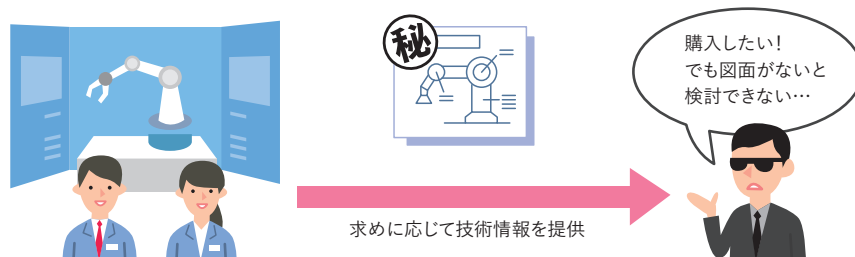
Case 2 競合他社による社員の引き抜きによって技術流出したケース

海外の競合他社から好待遇での採用を持ち掛けられ、転職を決意。退職時に、会社の技術情報をUSBメモリに保存して持ち出し、転職先で技術を提供した。しかし、転職後、数年で解雇されてしまった。



Case 3 展示会への出展をきっかけに技術流出したケース

展示会がきっかけで新しい引き合いがあった。何回か打合せを行った後、取引を進めるためと説明を受けて、求められるままに詳細な図面を提供した。その後、取引が進むことはなかった。



Case 4 産業スパイの接触をきっかけに技術流出したケース

プライベートで親しくなった知人から、ある日、勤務先のプロジェクトに関心を示された。最初は公開情報を提供していたが、徐々に重要な技術情報を求められた。それまでに金品を受け取っていたことから、技術情報の提供を断ることができなかった。



どうやって
対策すればいいの？

何よりも流出を防ぐための未然の対策が重要です。
また、大事な技術やノウハウを持っている技術者自身の社外流出を防ぐことも大切です。

未然の対策

■ ルールの整備

○ 技術情報の取扱いに関するルールを定めましょう。

■ ルールを浸透させる

○ 研修を実施し、ルールに基づく情報管理の重要性を社内に浸透させて、社員の理解を深めましょう。

■ 情報にアクセスする人を決める

○ 重要技術については、必要最小限の範囲でのみアクセス権限を設定しましょう。

○ 製造工程を細分化して、重要な技術を全て把握する社員を少数に絞りましょう。

事後の対策

■ 違反者への対応

○ 毅然と法的責任を追及することも大切です。

■ 再発防止策

○ 今後同じことが起こらないよう、ルールの見直しも重要です。

“人”の流出対策

■ 会社にロイヤリティを持ってもらう

○ 待遇向上や表彰制度等を通じて、「この会社で研究開発を続けたい」と思ってもらうことも、重要な技術流出対策です。また、退職者と優良な関係を構築することが重要です。

詳細は11、12ページへ▶

コラム

買収や資本提携等を通じた技術流出

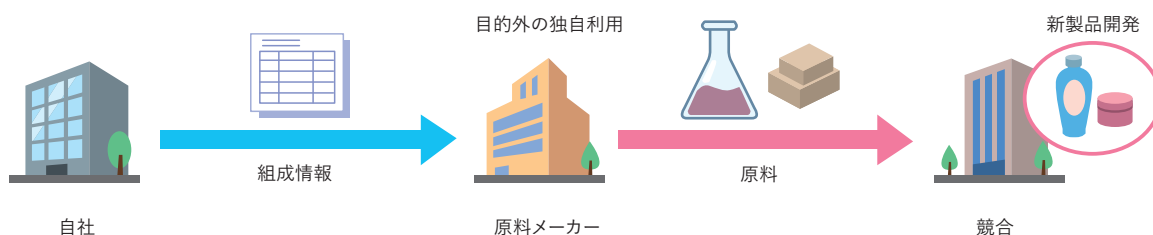
財務基盤の強化等を目的に、投資買収を受け入れるケースでは、意図に反して、技術のみを獲得されてしまう場合もあります。また、上場の是非を含め事業拡大等のための資本政策を検討する必要があります。



すり合わせに伴う技術流出の事例

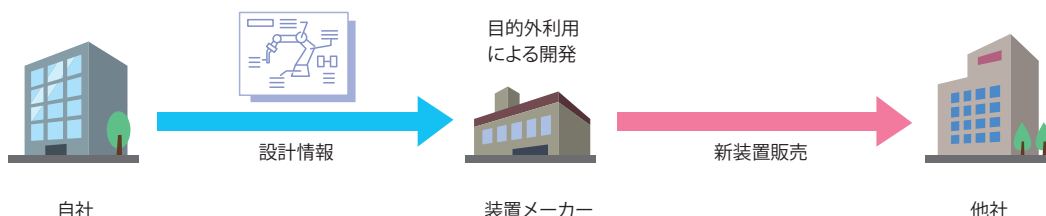
Case 1 原料メーカー（仕入先）から技術流出したケース

新製品開発のため、原料メーカーに開発方針を伝えた。原料メーカーはその情報を利用して、新たな原料を開発し、自社の競合にも提供し販路を拡大。その後、その原料を用いて、競合が新製品を開発・投入していることに気付いたが、証拠がなく法的責任を追及できなかった。



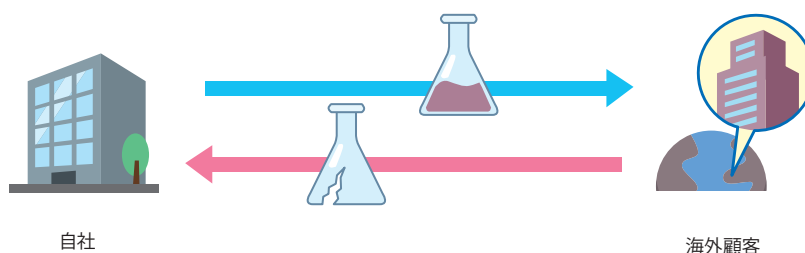
Case 2 製造装置メーカーから技術流出したケース

特注の製造装置の開発を委託し、装置メーカーに自社製品の設計情報を提供した。装置メーカーがその情報を目的外利用して、新たな装置を開発し、他社に販売した。



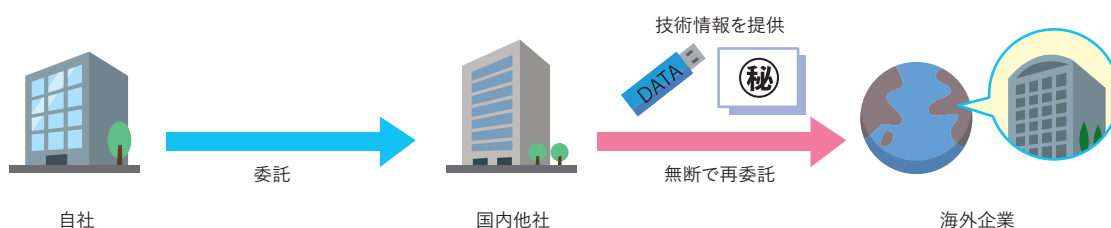
Case 3 海外顧客へのサンプル提供をきっかけに技術流出したケース

海外の新規顧客から引き合いがあり、サンプルを提供した。その後、期限を過ぎてもサンプルが返却されず、何度も連絡をしたところ、破損した状態で返却された。よく確認すると、リバースエンジニアリングの形跡があった。



Case 4 製造委託先が無断で再委託し技術流出したケース

自社製品の製造工程の一部を、国内の他社に委託した。その際、契約書には、再委託に事前承諾が必要と定めていた。しかし、委託先が、無断で海外企業に再委託し、技術情報を提供してしまった。



どうやって 対策すればいいの？

取引先との仕様調整等のすり合わせに伴って、重要な技術情報を提供する場合があります。一步立ち止まって、信頼できる取引先か、しっかり確認しましょう。自社を守るためにも、契約には守秘義務条項をしっかり盛り込み、必要以上の技術情報を出さないように注意しましょう。

信頼できる取引先かどうか確認する

- まず最初に、信頼できる取引先か、情報管理が十分になされているか確認しましょう。



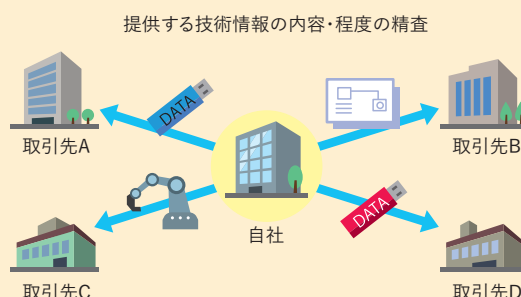
秘密保持契約を結ぶ

- 大切な技術情報を渡す場合には、既存の取引先でも、改めて秘密保持契約を結ぶことも大切です。



取引先に提供する技術情報の範囲を限定する

- 取引内容に応じて、どの技術情報を提供する必要があるか、あらかじめ明確にして、それ以上の情報を提供しないようにしましょう。
- 過度に情報を提供すると、技術流出のリスクが高くなります。情報を受領する企業としても、守秘義務を負う情報が増えてしまい、情報管理の負担が大きくなってしまいます。

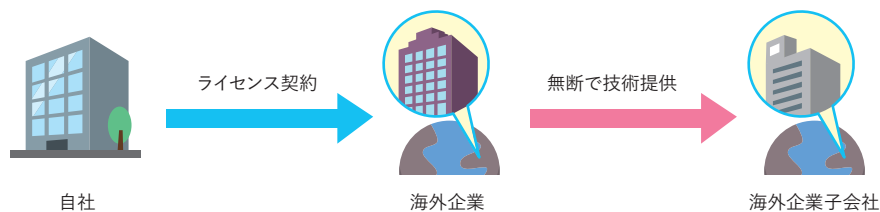


詳細は13、14ページへ▶

生産拠点の海外進出に伴う技術流出の事例

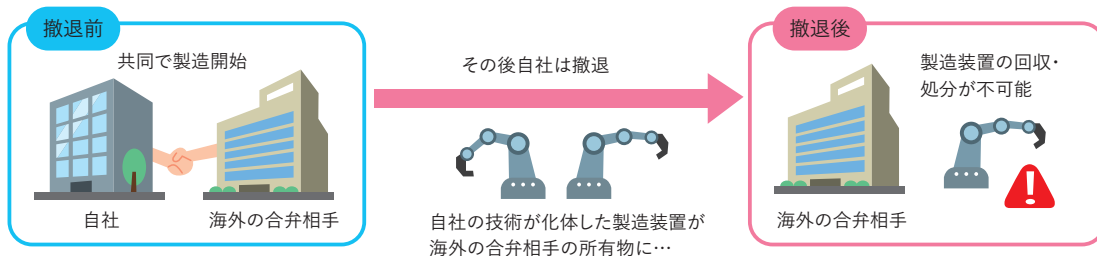
Case 1 ライセンス契約先(海外企業)から技術流出したケース

ライセンス契約先が説明した相手国の法制度や商慣行を鵜呑みにし、契約内容の精査を怠ったため、ライセンス契約先がその子会社に自社技術を流出させ、その子会社が類似製品を開発していることが発覚した。



Case 2 撤退時の管理不足から技術流出したケース

設備投資の費用を海外の合併相手に負担してもらい、生産を開始したものの、製品の製造装置が海外の合併相手の資産となっていたことから撤退時に廃棄することができず、結果として製造装置に含まれた技術情報が流出した。



どうやって
対策すればいいの?

日本とは異なる法令や慣習の影響により、技術流出リスクが高まります。まずは、大切な技術を安易に移転しないようにしましょう。

計画段階

進出先の国の法制度や、取引先(ライセンス契約先等)が信頼できるかを、事前に確認しましょう。

契約段階

提供する技術の範囲や、情報の取扱方法等について、明確にしておきましょう。

実施段階

大切な技術情報はブランクボックス化して、限られた社員のみが把握できるようにしましょう。

撤退段階

大切な技術情報は、他社任せにせず、責任をもって確実に返還・処分しましょう。

具体的な対策は15ページへ▶

共同研究に伴う技術流出の事例

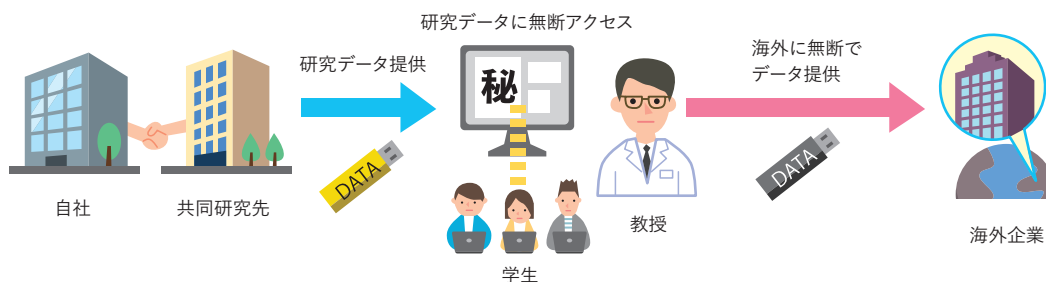
Case 1 共同研究先の従業員から技術流出したケース

共同研究の過程で提供した研究データを、共同研究先の従業員が無断でコピーし、海外の競合企業に転職し、研究データを流用した。



Case 2 共同研究先の委託先から技術流出したケース

共同研究先が研究の一部を委託していた大学の研究室内で、研究データが自由に閲覧可能となっており、実際に留学生がデータを閲覧していた。また、研究室の教授も、外国に無断でデータを提供していた。



どうやって
対策すればいいの？

共同研究は他の組織や研究者との技術の共有が想定され、技術流出リスクが高いため、テーマ・内容、パートナーの選定が重要です。

テーマ選定

研究領域や扱う技術の重要性を考えて、テーマを設定しましょう。

パートナー選定

信頼できる共同研究先か、情報管理が十分になされているか、国・組織・個人の観点から、確認しましょう。

契約・実施段階

研究に参加するメンバーは特定し、他の研究者や従業員が情報にアクセスしないようにしましょう。

具体的な対策は16ページへ▶

まず最初にやるべき対策

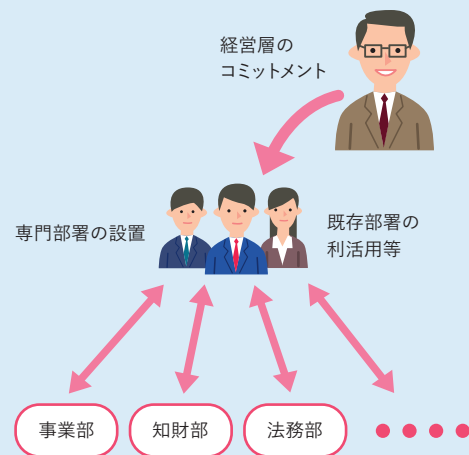
STEP 1 組織体制の構築

1 経営層のリーダーシップ

- 技術流出リスクへの対応は、短期的にはコストが先行しますが、中長期的には重大な損失を回避し、企業価値向上に資することを認識しましょう。
- 買収等を通じた技術流出リスクも考慮して、資本政策を検討することも大切です。

2 責任者の設置

- 技術流出対策は、各人の判断に任せきりにするのではなく、組織横断的な対応が不可欠です。対策を推進する責任者を任命し、部署間の連携や全社的な対策を講じることが重要です。



※経済産業省では、企業が経営戦略を考える上での経済安保対応に関する推奨事項をまとめた「経済安全保障経営ガイドライン」を公開しています。



詳細はこちら

STEP 2 重点的に守るべき技術の特定・評価

技術の重要度に応じたメリハリのある対策が重要です。

次のような観点を踏まえながら重点的に守るべき技術を特定・評価しましょう

1 競争力の源泉となるコア技術

- 自社の競争力に直結する技術を明確にしましょう。権利化・秘匿化を意識し、社内での情報管理に万全を期すことが大切です。
- 技術によっては、下記の2および3の重要技術に位置付けられるものもあります。その重要性について判断に迷う場合には、経済産業省や所管省庁へ相談することも有用です。

2 安全保障上の重要技術(軍事転用懸念のある技術)

- 外為法上のリスト規制に該当する技術等、安全保障に影響を与える可能性がある技術は特に慎重な対応が必要です。
- 外為法に違反することがないように、該非判定等の手続を確実に行いましょう。

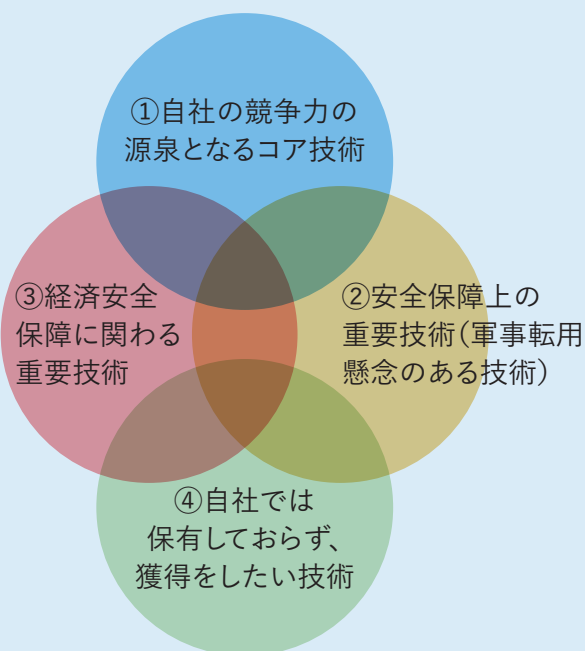
3 経済安全保障に関わる重要技術

- 経済活動の自律性や不可欠性を確保するために重要な技術があります。そうした技術は、他国の獲得関心の対象となっている場合もあり、注意が必要です。
- 一社の技術流出が産業・技術基盤、さらには国力に影響を及ぼす可能性があります。

4 自社では保有しておらず獲得をしたい技術

- 技術流出対策とオープンイノベーションのバランスをとりつつ、共同研究等で積極的に技術の創出・獲得に取り組むことが重要です。
- 共同研究のテーマや相手方によって、レピュテーションリスクや海外の法令抵触リスクにも十分配慮しましょう。

技術の重要性の評価



STEP 3 コア技術・重要技術管理

1 営業秘密管理

- 特許取得せず、オープンにしない重要技術については、営業秘密として徹底した管理が必要です。
- 営業秘密としての保護を受けるには、情報に接する人が、秘密情報として認識できるよう管理する必要があります。その他の条件も満たす必要があります。詳しくは経済産業省が公表している指針等で確認しましょう。



詳細はこちら

2 違反に対する毅然とした対応

- 技術流出時に不正競争防止法に基づく毅然とした対応を講じることは、取引先や株主等からの信頼向上につながります。
- また、社内においても、今後の技術流出への抑止や、社員の意識向上にもつながります。

人を通じた技術流出への対策

技術流出を未然に防ぐために取り組むべき事項

- 多くの企業では、日常的に、多数の社員が様々な技術情報に触れています。企業の規模や業種にかかわらず、人を通じた技術流出対策を考えることは、重要です。
- まずは、できる対策から確実に実行していく等、メリハリを付けて対応することも大切です。

社内ルールは定めていますか？

ルールがないと、従業員任せの管理になってしまいます。

- ▶技術情報の保管方法や取扱いの手順、業務デバイスの利用方法、SNS利用時の注意点等について、社内規程を作りましょう。
- ▶社内規程の内容は、現場の意見や最新の情報も踏まえて、アップデートしていきましょう。

ルールをしっかり周知していますか？

ルールは、社員が内容を理解し、遵守してこそ意味があります。

- ▶ルールの内容について、社内研修を実施しましょう(対策例1)。

大切な技術情報に誰がアクセスできるか、把握できていますか？

大切な技術情報は、それを知る必要がある社員しかアクセスできないようにしましょう。

- ▶技術情報の内容に応じて、入退室管理やアクセス権限を実施しましょう(対策例2)。
- ▶重要な工程は担当者を分けて、全体工程を知る社員は限定しましょう(対策例3)。

技術者の流出に対して取り組むべき事項

- 大切な技術やノウハウを持っている優秀な技術者が他社に転職してしまうと、自社の競争優位性が損なわれてしまいます。

自社へのロイヤリティを高めましょう(対策例4)

自社で研究開発に携わることに魅力を感じてもらうことが何より大切です。

- ▶ふさわしい職位や給与等により待遇を向上させましょう。
- ▶大切なノウハウを身につけた技術者とは、定年後も持続的な関係を構築することも一案です。

退職者との良好かつ適切な関係を構築することも大切です。

- ▶OB・OG会等を通じて定期的にコミュニケーションを図りましょう。
- ▶就業規則や退職時の誓約書において、社員が退職後に競合他社で業務を行うことを制限する規定(競業禁止義務条項)を導入することも重要です。

対策例 1 情報管理に関する定期的・階層的な研修の実施

社員がルールを十分理解できるように、定期的に研修を実施しましょう。業務の内容や部署ごとに注意するポイントが異なる場合もあります。対象者の立場に応じて、研修メニューを変えることも大切です。展示会への参加や海外出張等、不審な接触を受けやすいケースに備えた研修内容も用意しましょう。



対策例 2 技術保有者の特定とアクセスコントロールの徹底

重要な技術を身につけた人や、その技術情報にアクセスする人を特定することが重要です。その上で、重要な技術情報については、それを知る必要のある社員を限定し、アクセス権限や入室権限を設定しましょう。極めて重要な技術情報については、外国政府の情報収集活動に協力する義務を負っている社員かどうか等、技術情報を漏らすおそれがないかを確認することも考えられます。また、重要技術を扱う職種に従事する労働者の採用選考にあたり、応募者の採用選考時に、技術流出防止に関連した確認の一環として、国籍を確認する場合については、厚生労働省のHPを参照。



対策例 3 工程の細分化・全体工程を知る社員の限定

コア技術の全容を知る社員から流出が起きると被害が甚大となるため、製造工程を細分化し、担当者が知る情報を限定しましょう。全体工程を把握する社員は必要最小限に限定し、組織的に管理・把握しましょう。



対策例 4 ノウハウを持つ技術者の流出防止

大切な技術やノウハウを持っている技術者については、給与等の待遇を向上させることが大切です。また、定年退職後に競合他社に転職してしまうケースもあります。顧問やコンサルタント等の立場で持続的な関係を構築したり、OB・OG会を通じて定期的にコミュニケーションを図ることも大切です。また、社内表彰制度の導入や、短期的利益に直結しない研究開発を重んじる企業風土を築くことも大切な取組です。



すり合わせに伴う技術流出への対策

契約締結前の対策

信頼できる取引先かどうかの確認

サプライヤーや顧客との間では、商品の引き渡しだけでなく、仕様の調整や、保守・メンテナンス、トラブル対応等様々な場面で、自社の技術情報を提供することがあります。特に新規取引先や、重要な情報を提供する可能性がある取引先については、信頼できる取引先か確認することが大切です。以下のポイントも参考に、会社HPや登記情報等の公開情報や、取引先との日々のコミュニケーションを通じてチェックしましょう。

- ✓ 過去の法令違反や情報インシデントの有無
- ✓ 情報管理体制の状況(社内規程や責任者の有無、社内研修の状況等)
- ✓ 資本構成
- ✓ 設立時期、事業・研究開発実績



契約締結時の対策

取引開始前の情報提供の範囲の限定

商談や設備導入の検討段階では、フェージビリティ・スタディのために技術情報を提供することがあります。あらかじめ秘密保持契約を確実に締結した上で、提供範囲を明確にし、提供する情報も必要最小限の範囲にとどめることが重要です。

秘密保持義務・情報の取扱方法等の規定

新規の取引先はもちろん、既存の取引先であっても、仕様調整やカスタマイズに伴って技術情報を提供する場合には、秘密保持義務を契約に定めることが大切です。また、自社の技術が、意図しない主体や方法で利用されないよう、技術情報の取扱方法や、第三者への委託の制限等を定めることも大切です。

※経済産業省HPでは、秘密保持契約書等各種契約書の参考例を公開していますので、ご参考にしてください。

<https://www.meti.go.jp/policy/economy/chizai/chiteki/trade-secret.html>

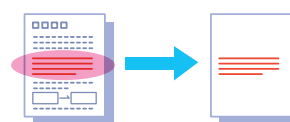


詳細はこちら

サプライチェーン内外との連携時の対策

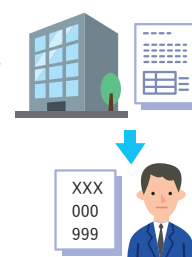
仕入先に対する情報提供範囲の限定

原料や素材を調達する際に、自社の技術情報を提供するケースもあります。提供する情報は必要最小限の範囲に限定することや、具体的な用途について言及しないことが大切です。



顧客に対する情報提供範囲の限定

顧客に技術情報を求められても、必要最小限にとどめ、ノウハウや製造条件は秘匿し、固有名詞はコードネーム化して提供しましょう。情報管理は営業担当者任せにせず、事前に社内の方針を整理し周知しておきましょう。



製造装置メーカー等に対する情報提供範囲の限定

製造装置メーカーやシステム会社等とのサプライチェーン外での連携においては、秘密保持条項の設定や提供する情報の範囲の限定、場合によっては製造装置等の内製化等で技術流出リスクに備えることが重要です。製造装置については、自社で独自にカスタマイズをしているケースがあり、それ自体が重要なノウハウである場合には、メンテナンスや修理に出す際に、購入時の状態に戻す等の対策も大切です。

外国政府等の要請に基づく情報開示要求への適切な対応

原材料の仕入れ先等から、外国政府からの要請等を背景に、技術のサプライチェーン等の情報開示を求められる場合には、その要求の合理性を確認しましょう。不当な内容と思われる場合には、安易に応じず、経済産業省にご相談ください。

コラム

**技術情報の管理体制を認証するための
政府が運用する制度があります!!**



認証マーク



制度概要はこちら

経済産業省では、情報管理にお悩みの事業者や研究機関の皆様に向けて、国が認定した機関が、情報セキュリティ体制を審査・認証する**技術情報管理認証制度(TICS)**を設けています。

認証取得や取得に向けて対策を進めることにより、取引先からの信頼獲得や、技術流出リスクの軽減といったメリットが得られるだけでなく、認証取得者向けの補助金等での優遇措置も用意されています。

生産拠点の海外進出に伴う技術流出への対策

海外に生産拠点を設ける際には、国内とは異なるリスクがあります。生産拠点を海外に設ける際は、計画段階から海外特有のリスクを認識しながら、技術流出の懸念が顕在化しないよう、慎重に取り組む必要があります。

計画段階

進出先の国の法制度の確認

進出先の国によっては、技術流出につながる制度があるケースもあります。専門家に相談して、海外の制度を確認しましょう。

提供先の情報管理体制の確認

技術提供先について、社内規程や責任部門の整備状況、過去の情報漏えいの有無等を確認しましょう。株主構成や財務状況の確認も大切です。

ステークホルダーへの事前説明

外国企業が技術獲得の目的を秘して、現地生産を持ちかけるケースがあります。技術流出は甚大な損失につながるため、ステークホルダーに相談・説明をしましょう。

契約段階

提供する技術の内容等の明確化

「提供する技術」と「提供しない技術」を明確に区別し、提供方法や、技術情報を取り扱うことができる社員を限定しましょう。目的外利用や無断での再委託の禁止を定めることも大切です。

契約終了後の情報返還・廃棄

契約を締結する時点で、あらかじめ、契約終了後のデータの返却や廃棄について明確に合意しておきましょう。廃棄を認める場合には、廃棄証明書の提出を義務付けることも大切です。

実施段階

技術情報のブラックボックス化

提供する技術情報は必要最小限にしましょう。特に、原材料名等の重要な固有名詞はコードネーム化する、部品の調達元を秘匿化する、といった提供方法の工夫も大切です。

製造設備メンテナンス時の管理

製造設備には独自のカスタマイズによるノウハウが多く含まれます。自社では当たり前の情報も狙われていることを認識し、メンテナンスはできる限り自社や設備メーカーで対応しましょう。

撤退段階

撤退計画時の情報管理

現地従業員の転職を通じた技術流出リスクを意識した対策が大切です。たとえば、重要情報へのアクセス権限の再設定や、不自然なデータのダウンロードのチェックを強化しましょう。

製造設備の管理・処分

ノウハウが詰まった製造設備を現地に残すことがないよう、契約で確実に返却・廃棄を実施させましょう。廃棄する場合は自社立ち会いのもと確実に処分しましょう。

共同研究に伴う技術流出への対策

イノベーションの実現には、他の企業や大学等のパートナーとの共同研究を推進することも大切です。一方で、共同研究では、他者と技術が共有されるため、技術流出リスクへの対応も必要となります。共同研究の価値を最大化するためにも、研究テーマ・内容や、パートナーに応じて、適切なマネジメントが重要です。

テーマ選定

技術の重要性を踏まえたテーマ選定

研究テーマの選定は、その研究で提供することになる技術の重要性(P10参照)や、共同研究先のDDの結果も踏まえて行いましょう。

※DD: デュー・ディリジェンス(Due Diligence)

パートナー選定

相手国の観点でのDD

海外で実施する共同研究の場合は、技術流出につながるおそれのある法制度がないかを確認しておきましょう。

組織の観点でのDD

相手方が企業・大学いずれの場合でも、過去の法令違反の有無や、情報管理体制の整備状況等を確認し、信頼できる相手かどうかを見極めましょう。

個人の観点でのDD

実際に情報を扱うのは共同研究に参加する個人であるため、共同研究に参加するメンバーの経歴や外国政府等による情報収集活動に協力する義務の有無等も確認しましょう。

契約段階

研究参加メンバーの明確化

契約書や計画書で参加メンバーを特定し、委託を含め、無断で第三者に情報を扱わせないようにしましょう。メンバーに学生が含まれる場合も秘密保持の誓約書を提出してもらいましょう。

提供する技術の範囲の明確化

共同研究契約以前から保有している技術情報を特定し、研究により創出される技術と明確に区分しましょう。共同研究の過程で提供する技術の内容・範囲を明記することも大切です。

実施段階

情報の利用ルールの明確化

データやサンプルの取扱方法等を定めた研究計画を作成し、研究参加メンバーにしっかりと説明しましょう。

情報アクセスの制限

大切な技術情報を提供する場合は、共同研究先のデバイスにコピーされないよう、自社管理のプラットフォーム上で共有し、閲覧・ダウンロード権限を適切に設定しましょう。

技術流出対策チェックリスト

優先度の高い技術流出対策をチェックリストにまとめています。
自社の実施状況の確認に活用ください。

※ 各項目に対応する技術流出対策ガイダンスの該当ページを、かっこ内に記載しています。

✓	まず最初にやるべき対策
<input type="checkbox"/>	組織体制の構築 (P11,12) 技術流出リスクへの対応は、コストではなく投資と考えましょう。組織横断的な対応を取るため、対策を推進する責任者を任命し、部署間の連携や全社的な対策を講じることが重要です。
<input type="checkbox"/>	重点的に守るべき技術の特定・評価 (P15,16) 技術の重要度に応じたメリハリのある対策が重要です。重点的に守るべき技術を特定・評価しましょう。
<input type="checkbox"/>	コア技術・重要技術管理 (P22,96) 特許取得せず、オープンにしない重要技術については、営業秘密として管理しましょう。
✓	人を通じた技術流出への対策
<input type="checkbox"/>	社内規程の整備 (P65) 技術情報の保管や取扱いの手順、業務デバイスの利用方法、SNS利用時の注意点等に関する社内規程を整備しましょう。
<input type="checkbox"/>	情報管理に関する定期的・階層的な研修の実施 (P67) 業務の内容や部署等、対象者の立場に応じた研修メニューを用意しましょう。展示会への参加や海外出張等、不審な接触を受けやすいケースに備えた研修内容も大切です。
<input type="checkbox"/>	アクセスコントロールの徹底 (P85) 技術情報ごとに、知る必要のある社員を限定してアクセス権限を設定しましょう。
<input type="checkbox"/>	工程の細分化・全体工程を知る社員の限定 (P92) 生産工程を細分化し、各担当者が知る情報を限定しましょう。全体工程を知る社員は必要最小限に限定し、組織的に把握・管理しましょう。
<input type="checkbox"/>	ノウハウを持つ技術者の流出防止 (P100) 給与等の待遇向上や社内表彰制度等を通じて技術者のロイヤリティを高めることも大切です。熟練技術者については、定年により社外流出しないよう、定年後も持続的な関係を構築することも一案です。
✓	すり合わせに伴う技術流出への対策
<input type="checkbox"/>	信頼できる取引先かどうかの確認 (P164) 重要技術を提供する可能性がある場合は、信頼できる取引先か確認しましょう。過去の情報インシデントの有無、情報管理体制、資本構成、事業実績等を、会社HP等の公開情報や日々のやり取りを通じてチェックしましょう。
<input type="checkbox"/>	取引開始前の情報提供の範囲の限定 (P165) 商談や設備導入の検討段階では、フィージビリティ・スタディのために技術情報を提供する場合があります。秘密保持契約を確実に締結した上で、提供してもよい必要最小限の範囲をあらかじめ明確にすることが大切です。
<input type="checkbox"/>	秘密保持義務・情報の取扱方法等の規定 (P167) 仕様調整やカスタマイズに伴い技術情報を提供する場合、契約に秘密保持条項を定めることが大切です。第三者への委託の制限や、情報の取扱方法等を定めることも大切です。
<input type="checkbox"/>	仕入先に対する情報提供範囲の限定 (P170) 原料や素材を調達する際に、自社の技術情報を提供するケースもあります。提供する情報は必要最小限の範囲に限定することや、具体的な用途について言及しないことが大切です。
<input type="checkbox"/>	顧客に対する情報提供範囲の限定 (P171) 製品の改善等のために技術情報を共有する場合でも、必要以上の情報は提供せず、ノウハウや重要な固有名詞は秘匿しましょう。営業担当者任せにせず、事前に社内でルール化することが大切です。
<input type="checkbox"/>	製造装置メーカー等に対する情報提供範囲の限定 (P173) サプライチェーン外の関係者と連携する際は、秘密保持条項の設定や提供する情報の範囲の限定、場合によっては製造装置の内製化等で技術流出リスクに備えることが重要です。
<input type="checkbox"/>	外国政府等の要請に基づく情報開示要求への適切な対応 (P170,171) 原材料の仕入れ先等から、外国政府からの要請等を背景に、情報開示を求められた場合は要求の合理性を確認し、不当な内容であれば、安易に応じず、経済産業省への相談も検討しましょう。

✓	生産拠点の海外進出に伴う技術流出への対策
<input type="checkbox"/>	進出先の国の法制度の確認 (P33) 進出先の国によっては、技術流出につながる制度があるケースもあります。専門家に相談して、海外の制度を確認しましょう。
<input type="checkbox"/>	提供先の情報管理体制の確認 (P36) 技術提供先について、社内規程や責任部門の整備状況、過去の情報漏えいの有無等を確認しましょう。株主構成や財務状況の確認も大切です。
<input type="checkbox"/>	ステークホルダーへの事前説明 (P37) 外国企業が、技術獲得の目的を秘して、現地生産を持ちかけるケースもあります。技術流出は甚大な損失につながるため、ステークホルダーに相談・説明することも大切です。
<input type="checkbox"/>	提供する技術の内容等の明確化 (P39) 「提供する技術」と「提供しない技術」を明確に区別し、提供方法や、技術情報を取り扱うことができる社員を限定しましょう。目的外利用や無断での再委託の禁止を定めることも大切です。
<input type="checkbox"/>	契約終了後の情報返還・廃棄 (P42) 契約を締結する時点で、あらかじめ、契約終了後のデータの返却や廃棄について明確に合意しておきましょう。廃棄を認める場合には、廃棄証明書の提出を義務付けることも大切です。
<input type="checkbox"/>	技術情報のブラックボックス化 (P46) 提供する技術情報は必要最小限にしましょう。特に、原材料名等の重要な固有名詞はコードネーム化する、部品の調達元を秘匿化する等、提供方法を工夫することも大切です。
<input type="checkbox"/>	製造設備メンテナンス時の管理 (P48) 製造設備には独自のカスタマイズによるノウハウが多く含まれます。自社では当たり前情報も狙われていることを認識し、メンテナンスはできる限り自社や設備メーカーで対応しましょう。
<input type="checkbox"/>	撤退計画時の情報管理 (P50) 現地従業員の転職を通じた技術流出リスクを意識した対策が大切です。たとえば、重要情報へのアクセス権限の再設定や、不自然なデータのダウンロードのチェックを強化しましょう。
<input type="checkbox"/>	製造設備の管理・処分 (P51) ノウハウがつまっている設備を現地に残すことがないよう、契約で確実に返却・廃棄を実施させましょう。廃棄する場合は、自社立ち会いのもと確実に処分しましょう。
✓	共同研究に伴う技術流出への対策
<input type="checkbox"/>	技術の重要性を踏まえたテーマ選定 (P118,119) 研究テーマの選定は、その研究で提供することになる技術の重要性(P10参照)や、共同研究先のDDの結果も踏まえて行いましょう。
<input type="checkbox"/>	相手国の観点でのDD (P120,121) 海外で実施する共同研究の場合は、技術流出につながるおそれのある法制度がないかを確認しておきましょう。
<input type="checkbox"/>	組織の観点でのDD (P122-126) 相手方が企業・大学いずれの場合でも、過去の法令違反の有無や情報管理体制の整備状況等を確認し、信頼できる相手かどうかを見極めましょう。
<input type="checkbox"/>	個人の観点でのDD (P127,128) 実際に情報を扱うのは共同研究に参加する個人であるため、共同研究に参加するメンバーの経歴や外国政府等による情報収集活動に協力する義務の有無等も確認しましょう。
<input type="checkbox"/>	研究参加メンバーの明確化 (P133) 契約書や計画書で参加メンバーを特定し、委託を含め、意図せず第三者が情報を扱わないようにしましょう。メンバーに学生が含まれる場合も秘密保持の誓約書を提出してもらいましょう。
<input type="checkbox"/>	提供する技術の範囲の明確化 (P134) 共同研究契約以前から保有している技術情報を特定し、研究により創出される技術と明確に区分しましょう。共同研究の過程で提供する技術の内容・範囲を明記することも大切です。
<input type="checkbox"/>	情報の利用ルールの明確化 (P144) データやサンプルの取扱方法等を定めた研究計画を作成し、研究参加メンバーにしっかりと説明しましょう。
<input type="checkbox"/>	情報アクセスの制限 (P146) 大切な技術情報を提供する場合は、共同研究先のデバイスにコピーされないよう、自社管理のプラットフォーム上で共有し、閲覧・ダウンロード権限を適切に設定しましょう。

あなたの大切な技術は、狙われています。

おかしいな?と思ったときには、勤務先に相談しましょう
もし対策に悩むことがあれば、迷わず、外部機関にご連絡ください

どこに相談するか迷ったら、
お近くの経済産業局にご相談ください

経済産業局連絡先リスト

北海道経済産業局 総務企画部 国際課

TEL 011-709-1752 メール bzl-hokkaido-kokusai@meti.go.jp

東北経済産業局 総務企画部 国際課

TEL 022-221-4907 メール bzl-thk-kokusai@meti.go.jp

関東経済産業局 総務企画部 国際課

TEL 048-600-0262 メール bzl-kanto-kaigai@meti.go.jp

中部経済産業局 地域経済部 国際課

TEL 052-951-4091 メール bzl-qchbnt@meti.go.jp

近畿経済産業局 国際部 通商課 経済安全保障室

TEL 06-6966-6039 メール bzl-kinki-keizaianpo@meti.go.jp

中国経済産業局 産業部 国際課

TEL 082-224-5659 メール bzl-qchgix@meti.go.jp

四国経済産業局 産業部 産業振興課

TEL 087-811-8525 メール bzl-qsikik@meti.go.jp

九州経済産業局 国際部 国際課

TEL 092-482-5423 メール bzl-kyukokusai@meti.go.jp

沖縄総合事務局 経済産業部 商務通商課

TEL 098-866-1731 メール bzl-oki-syomu@meti.go.jp

営業秘密、知財管理にお困りの場合

INPIT ((独)工業所有権情報・研修館)

営業秘密支援窓口 **無料**

TEL 03-3581-1101 (内線 3823) メール ip-sr01@inpit.go.jp

URL <https://www.inpit.go.jp/katsuyo/tradesecret/madoguchi.html>



技術流出対策について
もっと詳しく知りたい方はこちら

技術流出対策 ポータルサイト

https://www.meti.go.jp/policy/economy/tech_leakage_prevention/index.html



技術流出対策 ガイダンス第2版

https://www.meti.go.jp/policy/economy/tech_leakage_prevention/pdf/guidance2.0.pdf



技術情報管理認証制度 (TICS)

https://www.meti.go.jp/policy/mono_info_service/mono/technology_management/



経済安全保障 経営ガイドライン

https://www.meti.go.jp/policy/economy/economic_security/260123_guideline.pdf



警察庁 技術流出の防止に向けて

<https://www.npa.go.jp/bureau/security/economic-security/index.html>



[発行] 2026(令和8)年4月

経済産業省 貿易経済安全保障局 技術調査・流出対策室

〒100-8901 東京都千代田区霞が関1-3-1

電話 03-3501-1511(代)

<https://www.meti.go.jp/>