

技術流出対策ハンドブック

スタートアップ企業編

守るべき大切な技術
～企業の未来のために～



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

ステージに応じた技術流出対策で大切な技術を守り抜く

スタートアップ企業の先進的な技術は、多方面から狙われています。イノベーションを生み続ける攻めの姿勢こそが最大の技術流出対策ですが、研究活動を円滑に進めるためにも、守りとしての技術流出対策を講じることが大切です。

成長ステージ

成長ステージに応じた技術流出対策の考え方

シード～アーリー期

商用化段階になく製品の研究開発を実施している、又は製造・販売を開始したばかりの企業

ミドル期

本格的に商用化段階に入った企業

レイター期

黒字化・成長が見通され、IPOやM&A等の出口戦略の実行を目前に控えた段階の企業

シード～アーリー期

- 技術流出対策は「コスト」ではなく、成長を続けるための「投資」と考えましょう。
- 専門部署がなくても始められる対策から着手しましょう。

ミドル期

- 海外展開等も見据えて様々な取引先が増えてきます。
- 技術を提供する場合は、信頼できる取引先かを見極めましょう。

レイター期

- 組織としての情報管理の重要性が一層高まります。必要に応じて専門部署の設置等の組織体制整備も進めていきましょう。

時間

スタートアップ企業は、成長ステージに応じて組織体制の仕組みや成熟度が大きく異なります。本ハンドブックでは、ステージごとに注意すべき「人を通じた技術流出への対策」、「共同研究に伴う技術流出への対策」、「生産拠点の海外進出に伴う技術流出への対策」、「取引先との仕様調整等のすり合わせに伴う技術流出への対策」について記載しています。自社の状況に応じた対策を講じましょう。

また、次のステージを見据えた準備を進めることや、前のステージで出来ていなかった対策に取り組むことも重要です。

目 次

どのステージでも大切な対策

3
ページ

シード ～ アーリー期の企業に向けて

5
ページ

ミドル期の企業に向けて

9
ページ

レイター期の企業に向けて

13
ページ

関連する制度

17
ページ

どのステージでも大切な対策

STEP 1

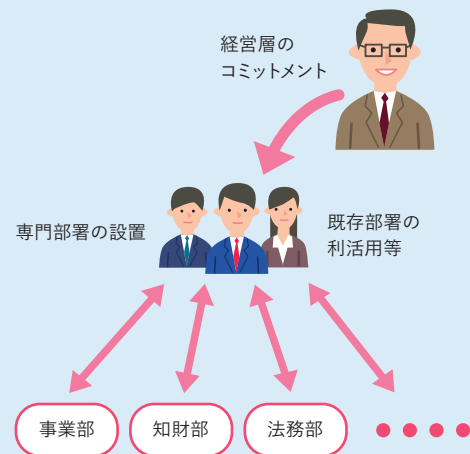
組織体制の構築

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。

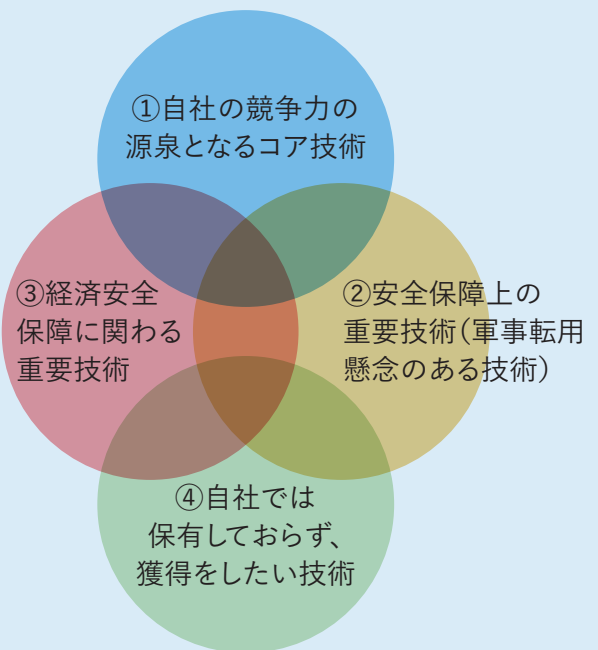
3 経済安全保障に関わる重要技術

- 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。

シード～アーリー期において特に注意すべきケース

シード～アーリー期に技術流出対策に取り組む重要性

Case 1 コアな製品開発に関与するメンバーから流出したケース

コアな製品開発に関与しているメンバーが、大切な技術情報を秘密管理することなく、自由に情報を持ち出していた。また、他社との兼業や技術コンサルも行っており、その状況を会社として把握できていなかった。



Case 2 大学との共同研究に伴い技術流出したケース

先進的な製品開発のため、大学の研究室と共同研究を行い、サンプルや非公開のデータを提供していた。しかし、自社のデータにアクセスできる研究室のメンバーを把握しておらず、学生が学会発表の論文にデータの一部を掲載してしまった。



Case 3 政府から情報管理が高く評価されたケース

資金調達をするにあたり、金融機関から将来有望な技術について適切な情報管理を行うよう、アドバイスを受けた。その後、政府の研究委託事業に申請した際に、情報管理をしっかり行っていることが高く評価され、採択された。



どんな事を
確認すればいいの？

技術流出対策の全体像を把握した上で、
まずは人を通じた技術流出対策を実施しましょう。

シード～アーリー期に取り組むべき技術流出対策の全体像

✓	チェック内容	ガイダンスの 該当箇所
共通事項		
<input type="checkbox"/>	組織体制の構築を検討する	11、12ページ
<input type="checkbox"/>	重点的に守るべき技術を特定・評価する	15、16ページ
<input type="checkbox"/>	コア技術・重要技術管理を徹底する	22、96ページ
人を通じた技術流出への対策		
<input type="checkbox"/>	重要な情報へのアクセスコントロールを実施する	85ページ
<input type="checkbox"/>	情報管理に関するルールを整備し、運用する	65、88、89ページ
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て、テーマを選定する	118、119ページ
<input type="checkbox"/>	公開情報や日々のコミュニケーションを基に、共同研究先のDDを実施する	120～128ページ
生産拠点の海外進出に伴う技術流出への対策		
<input type="checkbox"/>	契約において提供する技術内容を明確化する	39ページ
<input type="checkbox"/>	情報管理体制等に関する取引先のDDを行う	36ページ
すり合わせに伴う技術流出への対策		
<input type="checkbox"/>	取引開始前における情報提供範囲を明確化する	165ページ
<input type="checkbox"/>	契約において秘密保持義務・情報の取扱方法等を規定する	167ページ

※DD：デュー・ディリジェンス(Due Diligence)

詳細は7、8ページへ▶

コラム

経済安全保障の実践!!
経営ガイドラインで経営と現場をつなぐ

詳細はこちら▶



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の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。

経済安全保障経営ガイドラインでは、自社ビジネスを正確に把握してリスクシナリオを策定、経済安全保障への対応を“コスト”ではなく“投資”として捉える、マルチステークホルダーとの対話を**経営者等が認識すべき3つの原則**としています。

シード～アーリー期に取り組むべき技術流出対策

人を通じた技術流出への対策

アクセスコントロールの徹底

Need-to-Knowの原則に基づき、技術情報へのアクセス権限は必要な社員のみにも明確に設定し、人事異動や退職時には速やかに見直すことが重要です。



情報管理に関するルールの整備

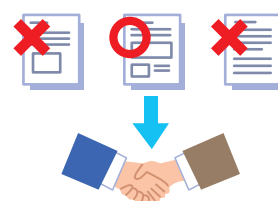
秘密情報の取扱い方や業務で利用するデバイス・ソフトウェアの利用方法等の情報管理ルールや、副業・兼業の手続を明確に整備するとともに、研修等によって社員の理解を進めることが重要です。



共同研究に伴う技術流出への対策

技術の重要性を踏まえたテーマ選定

研究テーマを選定する際には、そのテーマにおいて取り扱うこととなる技術の重要性を考慮し、流出時のリスクを評価しましょう。その上で、共同研究先の信頼度も踏まえて、適切なテーマを選定することが重要です。



公開情報や日々のコミュニケーションを通じた共同研究先のDD

研究テーマの重要性も踏まえつつ、共同研究先が信頼できるか確認することが大切です。以下も参考に、会社HPや登記情報等の公開情報や、日頃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



生産拠点の海外進出に伴う技術流出への対策

提供する技術内容等の明確化

提供する技術の範囲や内容、提供方法について、契約において、あらかじめ明確にしましょう。また、提供先が右記のようなリスクの高い行為を行わないように、契約において禁止したり、事前の承諾を必要とすることが大切です。

- ✓ 目的外利用
- ✓ リバースエンジニアリング
- ✓ 図面等の複製
- ✓ 製造装置等の移設
- ✓ 再委託

取引先のDDの実施

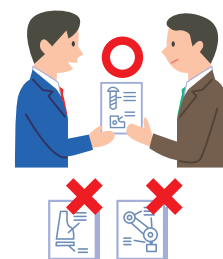
製造委託先やライセンス先が信頼できるか、情報管理体制の整備状況や財務状況を確認しましょう。自社の重要技術を提供する以上、取引先との企業規模の差に躊躇せず、情報管理状況等の説明を求めることが大切です。



すり合わせに伴う技術流出への対策

取引開始前の情報提供の範囲の限定

本格的な取引に入る前のフィージビリティ・スタディにおいて技術情報を提供する場合であっても、あらかじめ秘密保持契約を締結し、提供範囲を明確にすることが大切です。また、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

自社の大切な技術を取引先に提供する場合には、契約名称にとらわれず、秘密保持義務や情報の取扱いに関する規定を入れることが重要です。

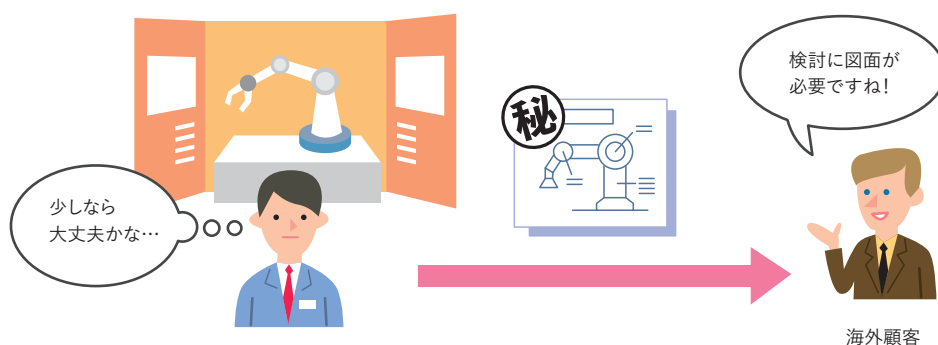


ミドル期において特に注意すべきケース

ミドル期に技術流出対策に取り組む重要性

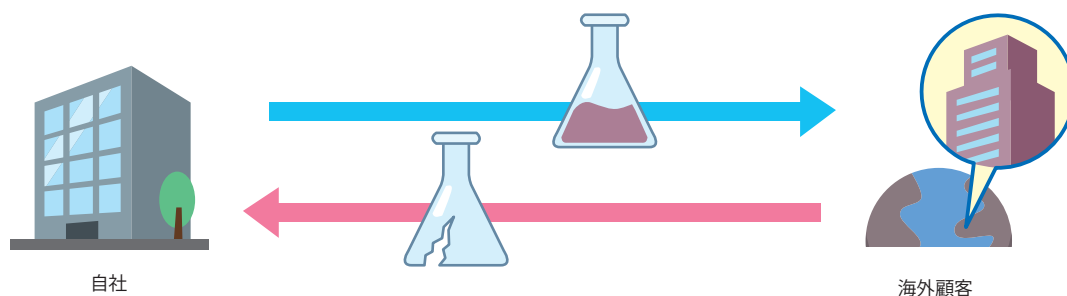
Case 1 展示会への出展をきっかけに技術流出したケース

国内での売上げも順調に伸びてきたため、海外へ販路を拡大するため、現地の展示会に出展。しかし、説明・公表可能な範囲を事前に社内で決めていなかったため、従業員が、興味を持った海外企業の従業員に対して、うっかり営業秘密を話してしまった。



Case 2 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。



どんな事を
確認すればいいの？

企業規模・事業規模が大きくなっていく時期です。
組織体制を構築し、様々なビジネスシーンに応じて、できる限りの対策を講じましょう。

ミドル期に取り組むべき技術流出対策の全体像

✓	チェック内容	ガイダンスの 該当箇所
共通事項		
<input type="checkbox"/>	組織体制の構築を検討する	11、12ページ
<input type="checkbox"/>	重点的に守るべき技術を特定・評価する	15、16ページ
<input type="checkbox"/>	コア技術・重要技術管理を徹底する	22、96ページ
人を通じた技術流出への対策		
<input type="checkbox"/>	情報管理に関する定期的・階層的な研修を実施する	67ページ
<input type="checkbox"/>	展示会等を契機とする部外者との接触への対応方法を決める	94ページ
共同研究に伴う技術流出への対策		
<input type="checkbox"/>	共同研究先のDDを実施する	120～128ページ
生産拠点の海外進出に伴う技術流出への対策		
<input type="checkbox"/>	進出先国の制度や労働慣行を確認する	33、35ページ
<input type="checkbox"/>	段階的に技術提供を行う	45ページ
すり合わせに伴う技術流出への対策		
<input type="checkbox"/>	仕入先に対する情報提供範囲を限定する	170ページ
<input type="checkbox"/>	顧客との間での情報提供範囲を限定する	171ページ

※DD：デュー・ディリジェンス(Due Diligence)

詳細は11、12ページへ▶

コラム

スタートアップに潜む
「突然のリスク」に備えましょう!!

動画はこちら▶



スタートアップの成長は、ある日突然、加速します。しかし同時に、知的財産や技術情報をめぐるリスクも突然顕在化します。

INPITのショートドラマ「スタートアップは突然に…」では、大型契約、共同研究、海外展開、人材の移動といった場面で、一見チャンスに見える出来事が、技術流出や権利喪失につながる様子が描かれています。また、産業スパイの存在についても注意喚起しています。

これらは決してフィクションの世界だけの話ではありません。技術やノウハウを守る第一歩は、「自分たちにも起こり得る」事例として知ることです。

ミドル期に取り組むべき技術流出対策

人を通じた技術流出への対策

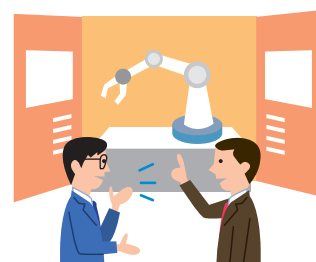
情報管理に関する定期的・階層的な研修の実施

社員が正確にルールを理解できるよう、定期的に研修を実施しましょう。また、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。



展示会等を契機とする部外者との接触への対応

展示会では来場者との会話や展示物を通じて技術が流出するおそれがあります。まずは、回答してもよい範囲をあらかじめ明確にしましょう。また、過度に技術的な質問をされる、プライベートの連絡先を求められるといった、実際の対応で迷う場合には、社内担当者を確認し、慎重に対応しましょう。



共同研究に伴う技術流出への対策

共同研究先のDDの実施

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、外国政府等による情報収集活動に協力する義務の有無、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等も確認しましょう。



※DD：デュー・ディリジェンス(Due Diligence)

生産拠点の海外進出に伴う技術流出への対策

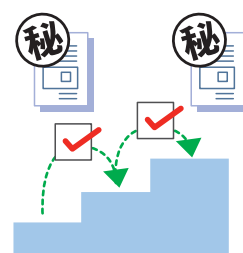
進出先国の法制度の確認

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、注意が必要です。また、転職率の高い国では現地スタッフの転職による技術流出のリスクも高まります。現地の制度や労働慣行等を事前に確認し、必要に応じて専門家の助言も得てトラブルを防ぎましょう。



段階的な技術提供

最初から広範な技術を提供すると、結果として必要のない技術情報まで提供してしまい、一気に模倣されるリスクが高まります。提供する技術の内容を事業段階ごとに絞り、各段階で、必要最小限の情報を提供しつつ、事業計画の進捗や信頼関係の構築を見極めながら、提供範囲を調整しましょう。



すり合わせに伴う技術流出への対策

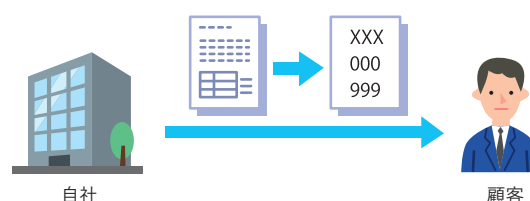
仕入先に対する情報提供範囲の限定

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。



顧客との間での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。

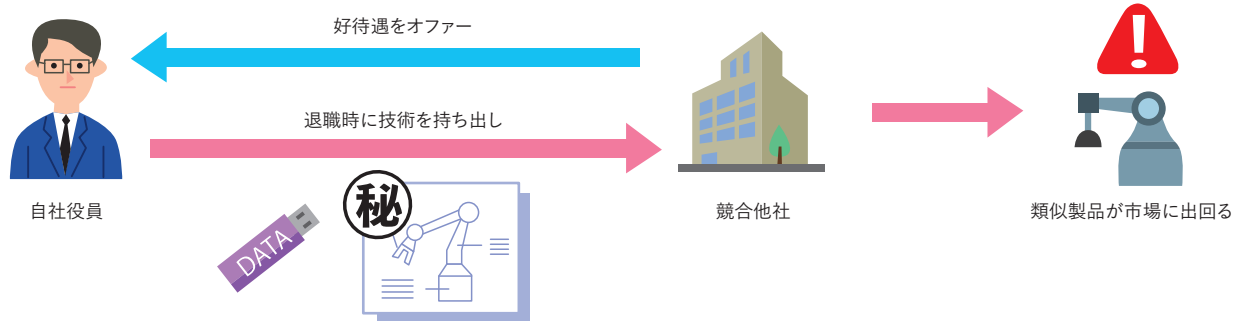


レイター期において特に注意すべきケース

レイター期に技術流出対策に取り組む重要性

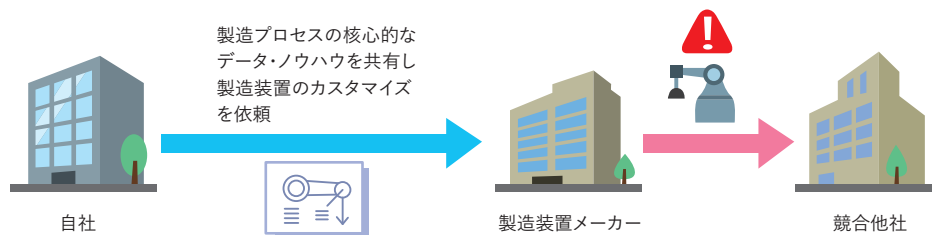
Case 1 元役員が情報を持ち出し不正に利用したケース

競合他社から好待遇で引き抜かれた元役員が、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、転職先で開発に利用。数ヶ月後、類似製品が市場に出回るようになった。



Case 2 製造装置メーカーがデータやノウハウを目的外に使用したケース

製造装置メーカーと秘密保持契約を締結した上で、装置のカスタマイズを目的に、運転条件等のデータやノウハウを共有した。ところが、製造装置メーカーがこれらの情報を目的外利用して、独自に特許を出願し、カスタマイズされた製造装置を競合他社にも販売した。その結果、自社の優位性を失い、競争力が大きく低下した。



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。



どんな事を
確認すればいいの？

上場等を見据えた際には、技術情報管理も含めた適切なガバナンス体制を構築することが、投資家等が重視する要素の1つになりえます。

レイトー期に取り組むべき技術流出対策の全体像

✓	チェック内容	ガイダンスの 該当箇所
共通事項		
<input type="checkbox"/>	組織体制の構築を検討する	11、12ページ
<input type="checkbox"/>	重点的に守るべき技術を特定・評価する	15、16ページ
<input type="checkbox"/>	コア技術・重要技術管理を徹底する	22、96ページ
人を通じた技術流出への対策		
<input type="checkbox"/>	工程の細分化や全体工程を知る社員を限定する	92ページ
<input type="checkbox"/>	ノウハウを持つ技術者の流出防止のための取組を行う	100ページ
共同研究に伴う技術流出への対策		
<input type="checkbox"/>	組織的なセキュリティ管理と防御態勢を強化する	149ページ
<input type="checkbox"/>	共同研究先の資本変動等に備えた契約内容とする	139ページ
生産拠点の海外進出に伴う技術流出への対策		
<input type="checkbox"/>	技術情報をブラックボックス化する	46ページ
<input type="checkbox"/>	海外における研究開発拠点の情報管理を徹底する	54ページ
すり合わせに伴う技術流出への対策		
<input type="checkbox"/>	サプライチェーン外との連携時の情報提供を制限する	173ページ

詳細は15、16ページへ▶

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!!

動画はこちら▶



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。

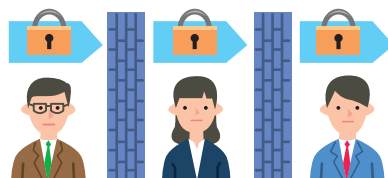
認証取得や取得に向けて対策を進めることにより、取引先からの信頼獲得や、技術流出リスクの軽減といったメリットが得られるだけでなく、認証取得者向けには補助金等での優遇措置も用意されています。

レイター期に取り組むべき技術流出対策

人を通じた技術流出への対策

工程の細分化・全体工程を知る社員の限定

重要な技術の全容を知る社員から技術流出が生じると被害は甚大です。製造工程を細分化し、個々の担当者が知る情報を限定するとともに、全体工程を把握する社員を必要最小限の範囲に限定し、会社側で把握しましょう。



ノウハウを持つ技術者の流出防止

重要なノウハウを持つ技術者の転職が、技術流出につながる場合もあります。給与等の待遇面で改善を図ったり、社内表彰制度や定年後に競合他社に転職することを防ぐため、顧問等として関係を継続することも一案です。社内表彰制度や、研究開発を評価する企業風土を築くことも大切な取組です。また、退職者との良好な関係を構築することも大切であり、OB・OG会等を通じて定期的にコミュニケーションを図ることや定年後に競合他社に転職することを防ぐため、顧問等として関係を継続することも一案です。



社内表彰制度



インセンティブ報酬

共同研究に伴う技術流出への対策

組織的なセキュリティ管理と防御態勢の強化

アクセス管理の甘さや設備の脆弱性により技術情報が漏えいするおそれがあります。情報へのアクセス権限管理と物理的セキュリティを強化しましょう。また、セキュリティ担当者を配置しサイバー防御態勢を整えることも大切です。



セキュリティ体制の強化

共同研究先の資本変動等に備えた契約内容

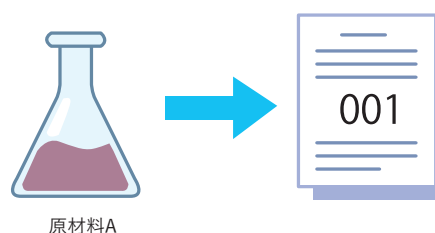
共同研究先の業績が悪化したり、資本構成に大きな変動があった場合、その内容によっては技術流出リスクが高まる場合があります。DDの段階で確認した事項が大きく変化する場合には、事前の承諾や通知を義務付けることや、契約が解除できるようにしておくことが考えられます。

※DD：デュー・ディリジェンス(Due Diligence)

生産拠点の海外進出に伴う技術流出への対策

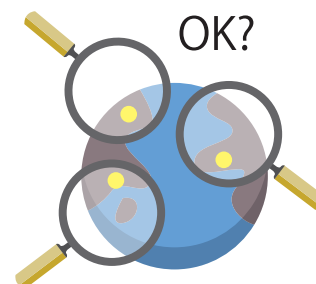
技術情報のブラックボックス化

必要以上に詳細な技術情報を提供すると、結果として、重要な技術が流出する危険性が高まります。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、提供方法も工夫することも大切です。



海外における研究開発拠点の情報管理を徹底する

海外拠点では管理水準や慣行の違いにより技術情報が流出するおそれがあります。拠点ごとに情報管理体制を点検し、アクセス制限等を徹底し、重要技術を扱う部門には厳格な基準と継続的な監査を行いましょう。



すり合わせに伴う技術流出への対策

サプライチェーン外(製造装置メーカー等)との連携時の情報提供制限

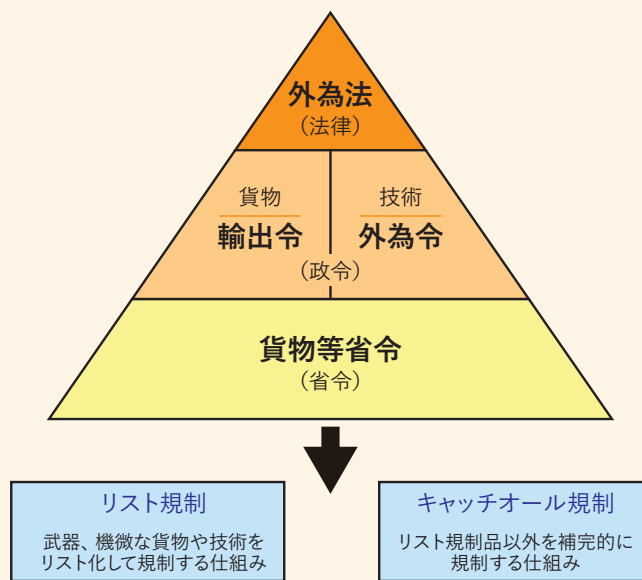
製造装置メーカーやシステム会社等のサプライチェーン外での連携においては、秘密保持条項の設定や提供する情報の範囲の限定、場合によっては製造装置等の内製化等で技術流出リスクに備えることが重要です。製造装置については、自社で独自にカスタマイズをしているケースがあり、それ自体が重要なノウハウである場合には、メンテナンスや修理に出す際に、購入時の状態に戻す等の対策も大切です。

関連する制度について

参考

安全保障貿易管理について

武器や軍事転用可能な貨物や技術が、我が国を含む国際的な平和及び安全を脅かすおそれのある国家やテロリスト等、懸念活動を行うおそれのある者に渡ることを防ぐため、先進国を中心とした国際的な枠組(国際輸出管理レジーム)を作り、安全保障貿易管理を推進しています。我が国の安全保障貿易管理制度は、国際輸出管理レジームでの合意を受けて、外為法に基づき実施しています。外為法に基づく規制は、「リスト規制」と「キャッチオール規制」から構成されており、これらの規制に該当する貨物の輸出や技術の提供は、経済産業大臣の許可が必要になります。



詳細はこちら <https://www.meti.go.jp/policy/anpo/guidance.html>



参考

対内直接投資審査制度について

外国投資家は、一定の事業を営む日本の企業に一定の投資を行う場合等には、事前届出書を提出する必要があります。外国投資家から出資を受ける場合は、外国投資家はその旨をお伝えください。(対内直接投資審査の制度・手続一般については、財務省HPをご覧ください)



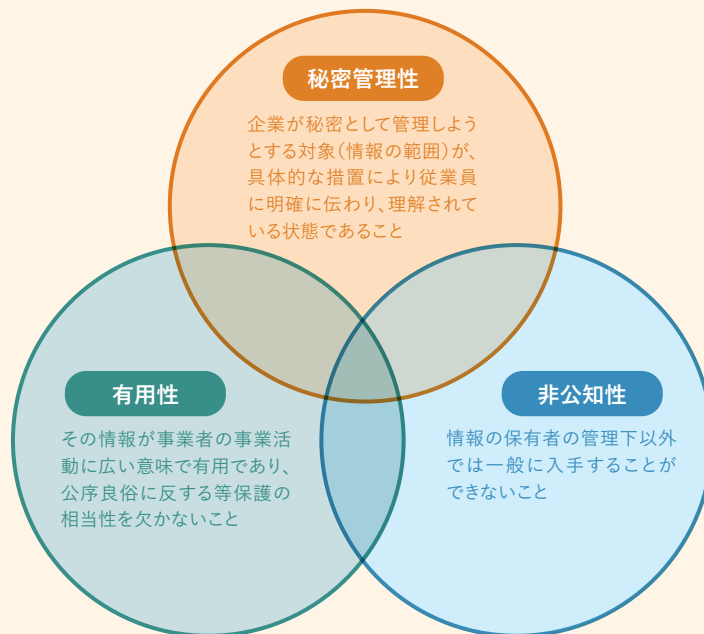
詳細はこちら https://www.mof.go.jp/policy/international_policy/gaitame_kawase/fdi/index.htm



参考

営業秘密管理について

企業が持つ秘密情報が不正に持ち出される等の被害にあった場合に、不正競争防止法で民事上・刑事上の措置をとることができます。そのためには、その秘密情報が、不正競争防止法上の「営業秘密」として管理されていることが必要です。具体的には、「有用性」「秘密管理性」「非公知性」の3つの要件を満たす必要があります。



詳細はこちら

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



参考

技術情報管理認証制度(TICS)について

経済産業省では、企業の情報セキュリティ対策を、国の認定を受けた認証機関が国が策定した基準に基づいて審査・認証する「技術情報管理認証制度(TICS)」を設けています。認証を取得することで、情報管理強化や取引先からの信頼獲得につながります。認証取得に向けては専門家派遣事業もご活用ください。



認証マーク



詳細はこちら

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



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-keizaijanpo@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](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](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/](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](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](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/>