

技術流出対策に係る支援施策

経済安全保障の観点からも重要な 技術流出対策

あなたの技術は狙われています！

- 日本の企業・大学が持つ優れた技術は、今日も、誰かに狙われています。
- 技術を守ることは、将来を守ること。コストではなく、未来への投資です！
- 以下を参考にさせていただくとともに、経済産業省まで気軽にご相談下さい。

【お問合せ先】経済産業省
貿易経済安全保障局 技術調査・流出対策室 E-mail : bzl-keizaianzen-gijutsuchousa@meti.go.jp
東北経済産業局 国際課 E-mail : bzl-thk-kokusai@meti.go.jp

< 参考 > 経済安全保障に関する産業・技術基盤の強化（基本的考え方）

1. 「経済安全保障」に係る社会的要請

- 現下の地政学的な変化、破壊的な技術革新の中、各国は国力増大のため、「経済安全保障」の切り口で施策強化
- 技術力をてこに、資源制約を乗り越え、経常収支バランスを確保してきた我が国において、今こそ取組強化が重要



2. 経済安全保障推進法の成立（2022年5月）

：平和と安全、経済的な繁栄等に向け、自律性の向上、優位性・不可欠性の確保に資する取組を法制化

① サプライチェーン強靱化

② 経済安全保障重要技術育成プログラム

③ 基幹インフラの事前届出制度

④ 特許出願非公開制度



3. 「産業・技術基盤強化アクションプラン」の策定（経産省）

2025年5月再改訂

- 産業支援策及び産業防衛策を有機的に組み合わせ（Run Faster戦略）ながら、同志国・地域とも協力し、官民連携で、具体的取組を実施するためにアクションプランを整理、提示。

1 産業支援策

- ◆ 設備投資支援
- ◆ 研究開発支援 等

2 産業防衛策

- ◆ 輸出管理（含む装備移転三原則）
- ◆ 投資管理（審査補強を検討中）等

3 国際枠組みの構築 産業界との対話

- ◆ 日米経済版「2 + 2」
- ◆ G 7 等

経産省においては、2024年7月に新たに「貿易経済安全保障局」を設置し、司令塔として、上記施策を総合的に推進
その基盤として、経済インテリジェンスと情報保全（セキュリティ・クリアランス）を強化

多様な技術流出の経路

- 技術流出は、非合法的な手法によってのみ生じるものではない。
- 技術流出の経路は多様化しており、その手法も巧妙化。日常的な経済活動を含め、注意が必要。

技術流出が生じうるケース（代表的な例）

※本省において、ヒアリングや相談等により把握した事案より

①生産拠点の海外進出

- ・ 海外拠点設置や海外企業との提携等により、ビジネス拡大を図るケース。
- ・ 技術移転後の漏洩などにより意図せざる技術流出をする場合がある。

②資金調達(投資買収)

- ・ 買収されるケース。財務基盤強化のために積極的に受け入れても、意図に反して、技術のみを獲得されてしまう場合もある。

③人を通じた技術流出

- ・ 従業員等から不正に技術流出するケース。営業秘密管理を適切に行っていない場合、発覚後の対応ができない場合もある。
- ・ また、優れた技術者を引き抜かれ、ノウハウを失う場合も。

④共同研究

- ・ 国内外の企業や大学と共同研究を行うケース。通常、相互に技術情報の交換するケースが多い。
- ・ 共同研究先が、不適切な意図をもっている場合や情報管理が不十分な場合には、技術が流出する場合がある。

⑤取引先との擦り合わせ

- ・ 部品メーカーや製造装置メーカーとの擦り合わせのために技術情報を交換するケース。
- ・ 取引先が、不適切な意図をもっている場合や情報管理が不十分な場合には、技術が流出する場合がある。

⑥システム管理（サイバー攻撃）

- ・ システム管理が不十分な場合、サイバー攻撃により技術が流出する場合がある。

◆技術流出対策って何をすればいいの？

⇒ 「技術流出対策ガイドンス」を活用しましょう！

- ✓ 海外生産や人材を通じた技術流出への対策をまとめています。
- ✓ 今後、「共同研究等の連携に伴う技術流出」など、継続的に改訂・拡充を図っていきます。

拡充・体系化

【技術流出対策ガイドンス】

【民間ベストプラクティス集】

想定されるリスク／事象	体制構築 リスクに対する戦略・体制等を整備する	特定 リスクの所在・大きさ等を理解・把握する	対処 リスクの顕在化に備えて影響を回避・軽減・移転する
技術流出のリスク	I 経済安全保障上の課題に対応するための組織体制の構築	II 技術流出の対策	
サプライチェーンのリスク	●意識醸成 ●体制整備	III サプライチェーンリスクへの対策	

目次

- 第0章 はじめに
 - 1 本ガイドンスの目的等
 - 2 意図せざる技術流出が生じうるケース
- 第1章 生産拠点の海外進出に伴う技術流出への対策
 - 0 技術流出事例
 - 1 計画前・計画段階において取り組むべき事項
 - 2 契約締結時に取り組むべき事項
 - 3 海外事業の実施段階において取り組むべき事項
 - 4 撤退・契約終了時に取り組むべき事項
 - 5 その他の取組事項
- 第2章 人を通じた技術流出への対策
 - 0 技術流出事例
 - 1 技術流出を防ぐために未然に取り組むべき事項
 - 2 技術流出した場合に取り組むべき事項
 - 3 技術者の流出に対して取り組むべき事項
 - 4 その他の取組事項

参考資料 技術流出対策チェックリスト



技術流出対策ガイドンス 第1版

経済産業省
貿易経済安全保障局 技術調査・流出対策室

第1章 生産拠点の海外進出に伴う技術流出への対策 1. 計画前・計画段階において取り組むべき事項

1. ① コア技術の特定

- 生産拠点の海外進出を検討する際に、どの範囲で技術提供するかは、経営戦略上の重要な判断。輸出管理の対象技術に留まらず、自社の重要技術（コア技術）を安易に海外に移転しない。経営戦略上、海外に移転すると判断する場合は、技術流出対策の一層の徹底が必要。流出対策に自信が持てないまま短期的な利益を追求すると、長期的には競争力を失うことに繋がりかねない。
- いずれの方針を取るにしても、正しくコア技術特定することが前提。これを誤れば、意図しない技術流出を招き、ビジネスを毀損してしまうおそれもある。

対応策の例

① 自社の競争力の源泉が何であるかを改めて確認する

- 自社の製品のどのような部分が市場において評価されているかを確認する。
- その上で、当該競争力は、どのような専業技術によって実現されているかを分析し、コア技術として特定する。
- 当該プロセスに、現場の技術者も関与させることで、組織全体の意識啓発に繋がることも期待できる。

② コア技術の優位性・重要性を確認する

- 輸出管理の対象であるかに関わらず、優位性や重要性が高いコア技術は、特に狙われやすいことを認識する。
- 特定されたコア技術が、他企業、特に進出先の国において容易に開発されうる技術であるか否かを確認する。併せて、市場における競争性やサプライチェーン上の重要性・不可欠性（ブレイクポイント）をまず第一にこの技術か）を確認する。また、自社が当該技術を開発するに至る経緯（投入した労力や費用、技術開発に至る研究開発活動の独創性など）の確認も有用である。

③ コア技術が、どの様に存在しているかを確認する

- コア技術が、どこに、どのような形態で存在するかにより、自ずと管理手法も変化していく。設計図面、配合比率データ、技術者の経験ノウハウ、カスタマイズした製造装置に化体しているかなどを把握する。また、コア技術の存在形態に応じて、当該技術に接する立場にある役職員の範囲や優位性も確認する。



◆ 技術流出対策ガイドンスの詳細はウェブページをご覧ください

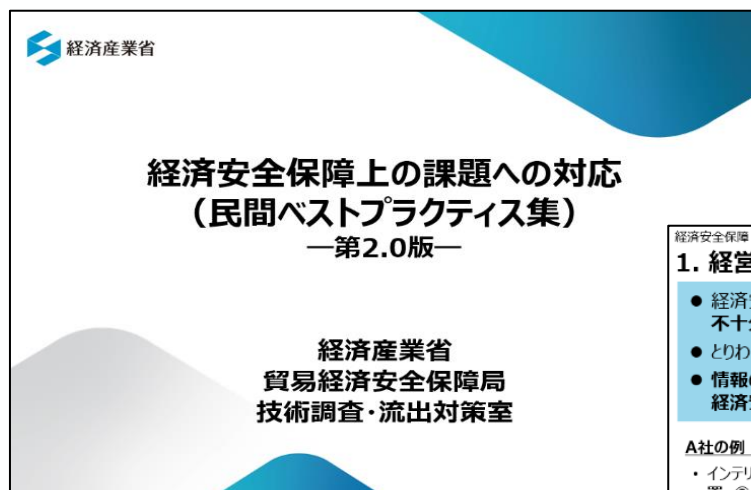
https://www.meti.go.jp/policy/economy/economic_security/index.html

◆他の企業はどうしているの？具体例はないの？

⇒ 「民間ベストプラクティス集」を活用しましょう！

- ✓ 民間企業の先進的な取組事例をまとめています。
- ✓ 分かりやすい紹介動画も公開中！

【民間ベストプラクティス集】



想定されるリスク／事象	体制構築 リスクに対する戦略・体制等を整備する	特定 リスクの所在・大きさを理解・把握する	対応 リスクの所在に 影響を回避・軽減
技術流出のリスク	I 経済安全保障上の課題に対応するための組織体制の構築 ●意識醸成 ●体制整備	II 技術流出の対策 ●技術の区分 ●人員配置の工夫 ●接触リスク分析	●防止策（従業退職） ●防止策（取引先）
サプライチェーンのリスク		III サプライチェーンリスクへの対策 ●供給網の可視化 ●リスク分析	●防止策（サイバー） ●防止策（制裁・紛争等）

経済安全保障 ベストプラクティス事例 2025年3月追加 意識醸成

1. 経営層の経済安全保障リスクリテラシー強化

- 経済安全保障という言葉は浸透しつつあるが、事業活動への影響についての理解が及ばず、対策が不十分な企業も存在。
- とりわけ経営層及びミドルマネジメント層が経済安全保障の重要性を理解していないことが原因の一つ。
- 情報の継続的なインプットと、自分事として考える機会を設けることで、日常業務において直面する経済安全保障関連リスクへの感度を向上させることが重要。

A社の例（食品）

- インテリジェンス活動として①ワシントンDCに事務所を設置、②海外シンクタンクやコンサルタントを通じた現地の最新動向の把握を実施。
- 上記活動で得られた情報を基に、本社インテリジェンス担当が経営層向けに国際情勢や制裁リスク等に関するレポートを適宜配属している。

B社の例（機械）

- 経済安全保障に知見のある外部有識者を顧問として招聘し、経済安全保障への対応をテーマとして各事業部門の責任者との1-on-1ミーティングを設定。
- 各事業部門の責任者は、経済安全保障の影響を自分事として思考し、論じる機会を通じて、普段の業務においても経済安全保障のリスクについて意識するようになった。

経営層のリスクリテラシー強化の実施概要

- 経済安全保障とはなにか？
- 経済安全保障はどのくらい重要か？
- どうすれば経済安全保障リスクを軽減できるか？

経営層
ミドルマネジメント層
社内組織
外部有識者

情報提供（重要トピック連絡など）
検討機会提供（1on1MTGなど）

◆ YouTubeで紹介動画を公開中！



アクセスはこちら

<https://www.youtube.com/watch?v=pll5RygY0I8>



◆ 民間ベストプラクティス集の詳細はウェブページをご覧ください

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

◆ちゃんと対策できているか不安だし、誰かに確認してほしい

⇒ **技術情報管理認証制度（TICS：ティックス）を活用しましょう！**

- ✓ 技術管理体制に関する法律に基づく認証制度です。
- ✓ 認証は、政府の認定機関が行います。 体制づくりの支援もセットで行います。
- ✓ 企業の対策を、取引先等に出すことが可能となり、取引先からの信頼性も向上したとの声も。
- ✓ 分かりやすい紹介動画も公開中！



国の基準を満たすかを客観的に審査・認証
必要に応じて事業者に指導・助言

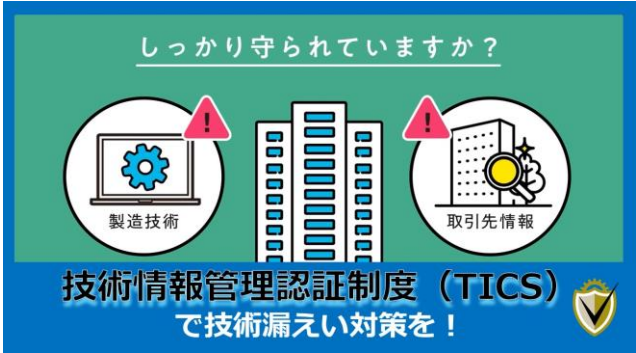
【技術情報の管理基準（例）】

- 管理者の選任
- 情報の取扱い（管理、複製、廃棄等）
- 従業員向けトレーニング
- 情報漏洩発生時の対応
- 情報のアクセス制限
- 情報を保管する金庫や扱うエリアの確保
- 情報システムのセキュリティ

※自工会・部工会ガイドラインのLv1やISMS等の内容を取り込み、ビジネスシーンでのニーズにも対応

認証の申込み
情報の態様・価値等に応じて対策を実施

◆ YouTubeで概要動画を公開中！



アクセスはこちら
<https://www.youtube.com/watch?v=IPsdxU1jb2I>



◆ 技術情報管理認証制度の詳細は
ウェブページをご覧ください

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



◆企業が関心をお持ちの場合：まずはチェックリストをご利用ください

- ✓ 「技術情報管理認証制度」（TICS）の基準をもとに、自社の情報セキュリティ対策の状況を自ら確認し、必要な対策を把握するためのツールも用意しています。

参考資料 技術流出対策チェックリスト（第1章）

チェック項目		チェック
1 計画前・計画段階において取り組むべき事項		
①	コア技術の特定 ☞ 自社の競争力や技術優位性などを考慮して、コア技術を特定・分析しているか？ ☞ コア技術がどのように存在しているか確認しているか？	
②	日本社内の情報管理体制の整備 ☞ 情報管理規程を整備し、社内研修を実施しているか？ ☞ 最新情報を規程や研修の内容に反映しているか？	
③	相手国の制度の確認 ☞ 技術流出対策の観点から、相手国の制度の確認・リスク分析を行っているか？ ☞ 現地情勢や法制度以外のルール・慣行も確認しているか？	
④	相手国の技術的関心の確認 ☞ 社内横断的な情報収集・分析体制を整備しているか？ ☞ 公的機関等との連携等を通じて、相手国の技術的関心を確認しているか？	
⑤	相手国の労働法制・慣習・雇用情勢等の確認 ☞ 法令遵守の観点から、相手国の労働法制を把握・理解しているか？ ☞ 労働法制に限らず、労働慣習等も確認し、社内規程や研修等に反映しているか？ ☞ 相手国の雇用情勢も考慮して、移転する技術の範囲を見極めているか？	
⑥	情報管理体制等に関する取引先DDの実施 ☞ ヒアリングや現地確認等によって、取引先の情報管理に関するデューデリジェンスを実施しているか？ ☞ 財務健全性やコンプライアンス遵守状況に関するデューデリジェンスも実施しているか？ ☞ 情報管理が自社の水準に達していない場合、必要な情報管理体制の整備が完了してから契約しているか？	
⑦	ステークホルダーに対する事前説明 ☞ 契約内容を確認した上で、海外技術移転の規模等も考慮し、技術流出リスクと対策状況を丁寧に説明しているか？	

[guidance.pdf](#)



出典：技術流出対策ガイダンス第1版（P80）より

技術情報管理 自己チェックリスト 改正基準に対応！

○この自己チェックリストは、国が推進する技術情報管理認証制度の基準をもとに作成しており、あなたの組織の情報セキュリティの取組状況のチェックにご活用いただくものです。

○各項目のチェック欄に回答を入力すると、あなたの組織の情報セキュリティの達成度を確認できます。

以下を参考に、あなたの組織の取組を評価してください。

「○」実施している：全ての従業員、全ての守るべき情報（※）、全ての取組においておおむね実施できている

「△」一部実施している：一部の従業員、一部の守るべき情報、一部の取組において実施できていないことがある

「×」実施していない：ほとんどの従業員、ほとんどの守るべき情報、ほとんどの取組において実施できていない

「-」該当しない：取引先から預けられた情報がない、情報を外部に預けていないなど、項目の条件に該当しない（一部の項目のみ）

？

※「守るべき情報」とは？

- ・もし漏えいしたら自組織の競争力、信用などを大きく損なう可能性がある情報を示します。
- ・書類や電子ファイルだけでなく、試作品、製造装置など、あらゆる形態の情報が該当します。

各項目に表示しているアイコンは、その項目がレーダーチャートのどの分野に対応しているかを示しています。

ルール作り

ルールの実践

人的対策

設備的対策

サイバー対策

漏えいを起こさない

漏えい後の被害を抑える

取引先との関係

確認者		チェック欄
情報セキュリティ責任者		
情報セキュリティ担当部門		

1 ページ

I 共通項目

1	自社の情報セキュリティ対応方針の策定及び周知を実施している。		
2	守るべき情報を特定し、ファイル名の一部や文書の罫頭にマル秘マークやラベルを付する等により、他の情報と識別ができるようにしている。		
3	守るべき情報や情報機器の機密性に応じた管理方法を規則に定め、それに従って管理している。		
4	情報セキュリティの責任者を選任し、情報セキュリティ事件・事故時の対応を行う体制や手順を整備している。		

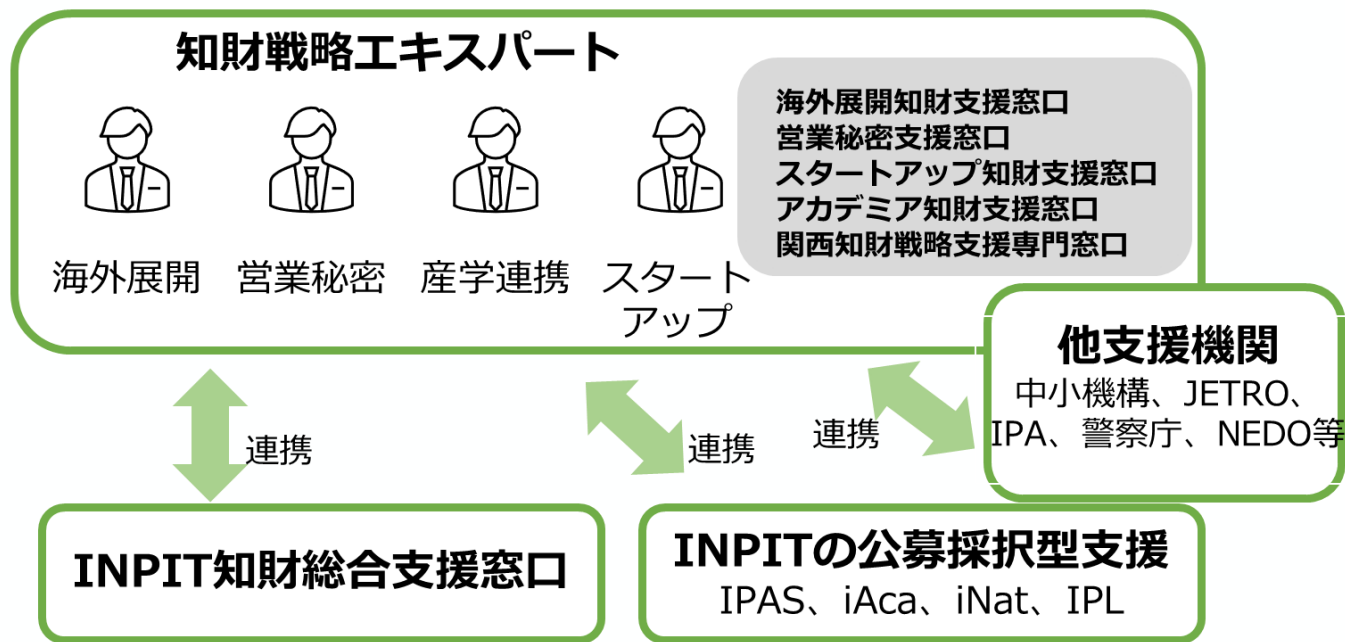
◆気軽に相談できる窓口はないの？

⇒**INPIT（インピット）知財戦略エキスパートに、ご相談ください。相談無料！**

- ✓ 技術流出対策のはじめの一步、営業秘密の管理等について、ご相談いただけます。
- ✓ その他、海外展開や産学連携、スタートアップなど、他の支援機関とも連携して支援します。

【INPIT（(独)工業所有権情報・研修館）知財戦略エキスパート】

- 知財戦略に関する高度な専門知識、企業等における豊富な実務経験を有する**知財戦略エキスパート**が支援する**5つの専門相談窓口**を設置（**無料、全国各地へ訪問可能**）。
- INPITの知財総合支援窓口や公募採択型支援、他支援機関とも連携して、円滑に支援を提供。
- セミナー・シンポジウム等への知財戦略エキスパートの**講師派遣**も可能（**無料**）。



知財戦略エキスパートへの相談はこちら

◆ 詳細はウェブページを
ご覧ください

https://www.inpit.go.jp/katsuyo/ip_strategyexp/



◆ お問い合わせ先はこちら

■ メール

INPIT 知財戦略部 エキスパート支援担当
メールアドレス：ip-sr01@inpit.go.jp

■ 電話

03-3581-1101（内線3823）

まとめ：ご理解いただきたい点



当社は軍事技術を持っていないから関係ないですよね？

いいえ、違います。

軍事技術と民生技術の垣根はありません。あらゆる優れた技術が狙われています。



海外進出せず、海外企業と付き合いなければ安心ですね。

いいえ、違います。

厳しい競争に勝ち抜く上で、海外展開を進めることに躊躇してはいけません。
グローバルに挑戦する前提として、技術流出対策により足元を固めましょう。



要するに、外為法を守っていればいいんですよね？

いいえ、違います。

外為法は、軍事転用のおそれが高い一部の技術のみが対象です。
技術を守るのは、規制があるからではなく、自社にとって大切だからです。



一人じゃ難しい！助けてくれるの？

はい、その通りです。

経済産業省では「官民対話」を通じて、できる限りのサポートをしていきます。
また、技術流出対策ガイダンスの整備など、役立つツールの整備も進めます。

