

経済安全保障の観点からの技術流出対策について

2025年10月

貿易経済安全保障局

技術調査・流出対策室

本日のご説明

1. なぜ、今、技術流出対策が重要か
2. 技術流出の経路と事例
3. 技術流出対策のための各施策

1. なぜ、今、技術流出対策が重要か

2. 技術流出の経路と事例

3. 技術流出対策のための各施策

経済安全保障の観点からの技術流出対策の必要性

- グローバルな地政学リスクの高まりに伴い安全保障の概念が軍事・外交領域から経済領域へと拡大。経済施策を通じて安全保障を確保する「経済安全保障」の重要性が増大。
- AIや半導体等をはじめとする先端技術の確保が国家間の競争軸となっていることから、優れた技術を確保していくことが我が国の自律性・不可欠性を確保し、経済安全保障の確保に直結。

対処すべき課題

- 標的となる主体の拡大
 - 大企業、中堅・中小企業、大学、研究機関等の重要な技術を保有する全ての主体が技術獲得の標的となり得る時代に。
- 脅威の多様化
 - 産業スパイ活動やサイバー攻撃等の非合法の手段のみならず、生産拠点の海外移転、人材の引き抜きや企業買収等、合法の企業活動を通じても技術流出が生じる可能性あり。



- 安全保障上の機微技術は、外為法に基づく規制により、貨物・技術の国外への提供を規制。
- これに止まらず、優れた技術は他国の獲得の標的とされるため、技術流出対策を企業の将来への投資と位置づけ、技術流出対策に取り組む必要あり。

(参考：諸外国の動向＜米国＞) 技術管理の考え方 (トランプ政権下)



米国人は米国ファーストの貿易政策の恩恵を受けるべきであり、それに値する。従って、私は、投資と生産性を促進し、**我が国の産業及び技術の優位性を強化し、経済及び国家安全保障を守り**、何よりもアメリカの労働者、製造業者、農民、牧場主、起業家、及び企業に利益をもたらす**強力で再活性化された貿易政策を確立**する。

米国ファーストの貿易政策を検討する大統領指示
(2025年1月20日)

商務長官及び通商代表は、PRCとの恒久的正常貿易関係 (PNTR) に関する立法提案を評価し、これらの立法提案に対する推奨事項を作成する。

国務長官及び商務長官は、(略) 米国の**輸出管理システムをレビューし、戦略的対立国や地政学的ライバルに関する進展**、及びその他の関連する国家安全保障及びグローバルな考慮事項に照らして修正を助言する

財務長官は、(略) 大統領令14105 (**懸念国における特定の国家安全保障技術および製品に対する米国の投資に対処**する) を(略) をレビューし、連邦官報 (89 Fed. Reg. 90398) に掲載された「懸念国における**特定の国家安全保障技術及び製品に対する米国の投資**に関する規定」が国家安全保障上の脅威に対処するための十分な管理を含んでいるかどうかを評価する。

大統領への報告 (2025年4月3日)

2000年に米国が中国にPNTRを付与した後、中国は米国経済の開放性を最大限に活用し、国家主導の資本投資と補助金、**産業の過剰生産能力**、緩い労働・環境基準、**強制技術移転政策**、及び無数の保護主義的措置を利用した。(略) 対中貿易赤字は(略) 2024年には2954億ドルに膨らんだ。PNTRが付与されてから20年以上経過しても、**中国は依然として非市場経済システムを採用**している。通商代表はPNTRに関連する立法提案を慎重にレビューし、大統領に助言した。

米国は、**先進技術が敵対国に流出しないようにする必要**がある。輸出管理は、より簡素化され、厳格化され、より効果的であるべきであり、AIにおける**米国の優位性を促進**し、グローバルな**技術的リーダーシップを主張**する必要がある。

トランプ大統領の米国ファーストの投資政策は、政権が投資政策にどのようにアプローチするか的基础として機能し、海外投資制限を含む。米国ファーストの投資政策に基づき、国家安全保障会議及び財務省は、米企業が繁栄しながらも米国ファーストを掲げ、**米国の国家安全保障の利益を損なわないようにするためのオプション**を評価する。政権の評価予定事項の一つは、**技術の進展及び懸念国の戦略に対応**するために、**海外投資制限の範囲を拡大すべきかどうか**である。

(参考：諸外国の動向＜欧州＞) バステア欧州副委員長演説概要

・・・中国は、我々にとって同時にパートナーであり、経済的な競争相手であり、体制上のライバルでもあります。そして、この最後の2つの側面はますます収束しつつあります。

中国がソーラーパネル業界を支配するに至った経緯を私たちは見てきました。まず、通常は合併事業を必要とする国内の巨大市場への外国からの投資の誘致。次に、必ずしも合法的な手段ではない技術の獲得。3つ目に、国内の供給業者への巨額の補助金供与と、同時に段階的に国内市場を外国企業に対して閉鎖すること。そして4つ目として、余剰生産能力を低価格で世界中に輸出している。

その結果、現在ではEUで設置されたソーラーパネルの3%未満しかヨーロッパで生産されていません。この戦略は、今やクリーンテクノロジーのあらゆる分野、レガシー半導体、そしてそれ以外にも展開されています。中国は景気低迷に対処するために、供給面での支援戦略を倍加させています。

我々の経済はこれに対応できない。それは我々の競争力にとって危険であるだけでなく、経済の安定性をも脅かす。一方的な依存が我々にとって不利に働く可能性があることは、我々はすでに経験済みだ。だからこそ、米国と同様に、ヨーロッパも対応しているのだ。・・・

我々は、ケースバイケースのアプローチ以上のものを必要としている。我々は、体系的なアプローチを必要としている。そして、手遅れになる前に、それが必要なのだ。

(2024年4月9日) (邦訳)

①中国市場への投資誘致

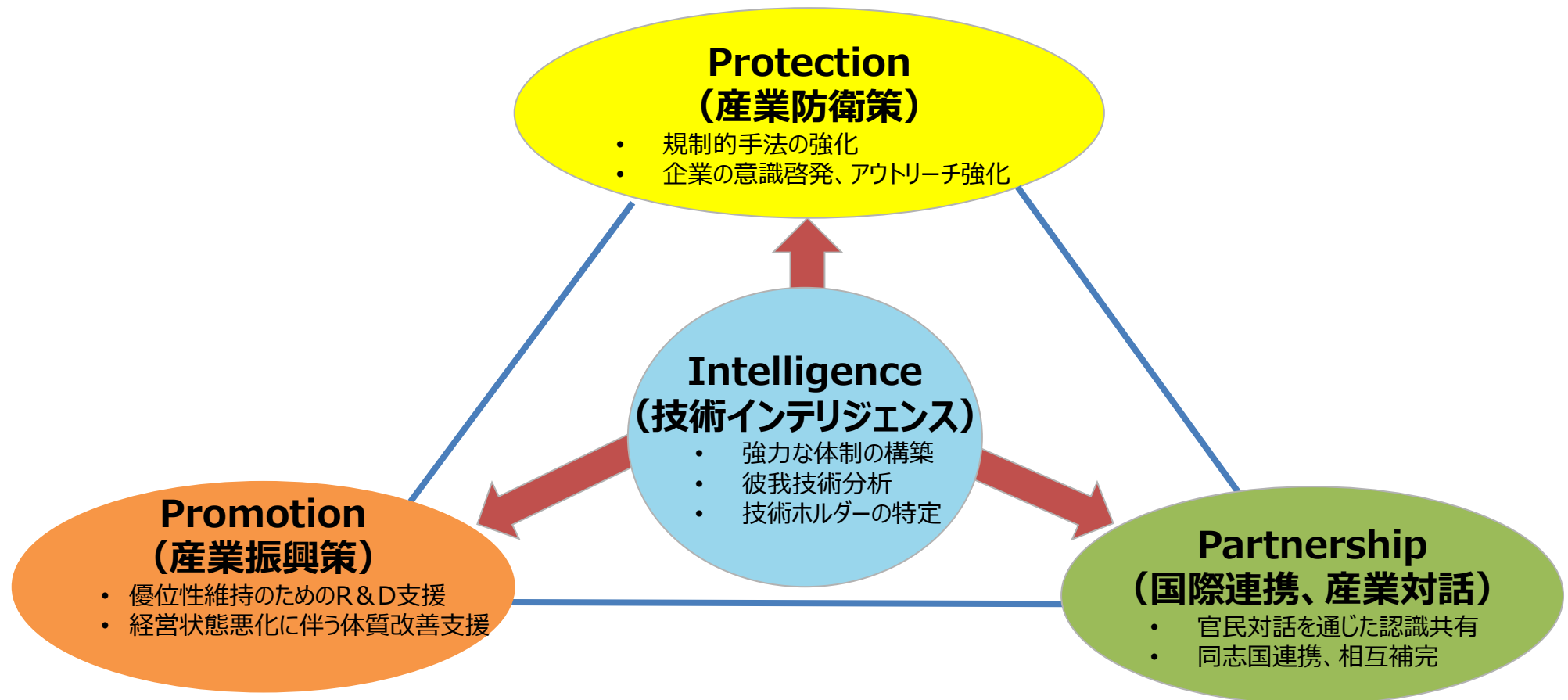
② (非合法手法を含む) 技術獲得

③国内企業への補助と外国企業の排斥

④過剰生産・供給

技術優位性の確保のための3つのP

- 技術流出を防止し、我が国の不可欠性を維持していくためには、産業防衛策（Protection）、国際・官民連携（Partnership）を推進しつつ、産業振興策（Promotion）を通じた技術革新を進めていくことが必要。これら「3つのP」を三位一体のものとして推進していくことが重要。
- これらの施策を推進していくための基盤となる、技術インテリジェンスを強化していくことが重要。

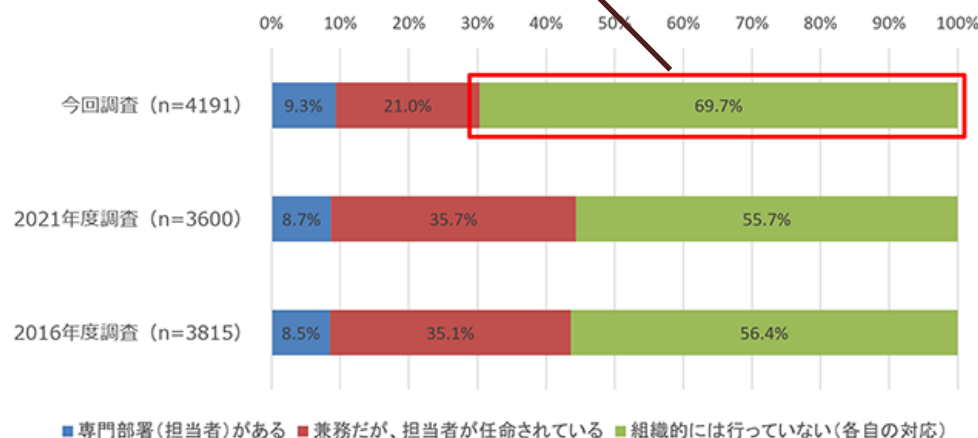


中小企業の情報セキュリティ対策状況

- 2024年度に実施された中小企業における情報セキュリティ対策に関する調査では、**約7割の企業で組織的なセキュリティ体制が整備されていない**ことが明らかになった。
- 一方で、**セキュリティ対策投資を行っている企業の約5割が、取引につながった**と回答。

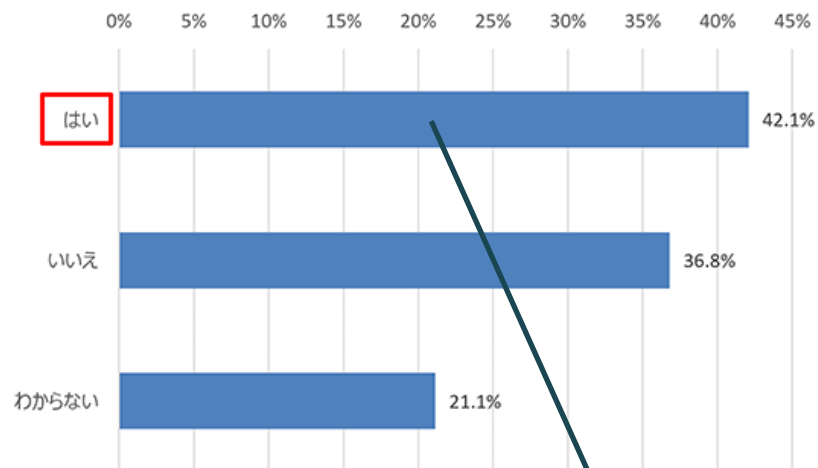
◆ 情報セキュリティ対策はどのような体制で行っているか

約7割が「組織的には行っていない」



◆ 取引先（発注元企業）から要請された情報セキュリティ対策を行ったことが取引先との取引につながった大きな要因か。

※取引先（発注元企業）から情報セキュリティ対策に関する要請を受けた経験がある企業に対しての質問



約5割が「取引につながった」

1. なぜ、今、技術流出対策が重要か

2. **技術流出の経路と事例**

3. 技術流出対策のための各施策

多様な技術流出経路

- 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。

技術流出経路の例

① 生産拠点の海外移転

- ・ 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 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。

(参考) 技術情報を狙う様々なアプローチ

- 我が国企業が保有する優れた技術やデータは、常に悪意ある主体のターゲットとなることから、流出防止に向けてあらゆる対策を講じる必要。

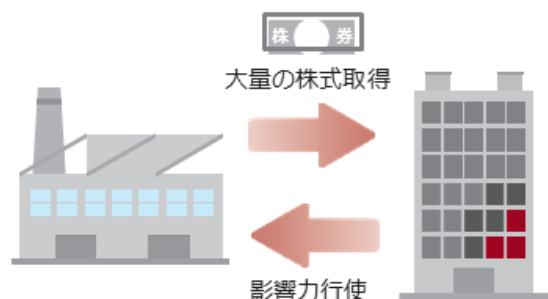
人材リクルート

～技術に精通している従業員の引抜き～



投資・買収・合併

～影響力を行使して意思決定に関与～



不審なアプローチ

～従業員との1対1の関係構築～



共同研究・事業

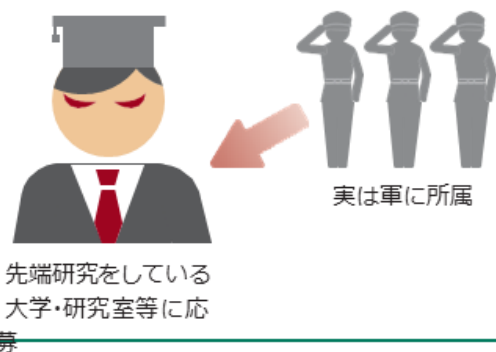
～技術・データの持ち出し～



経歴偽装による在籍

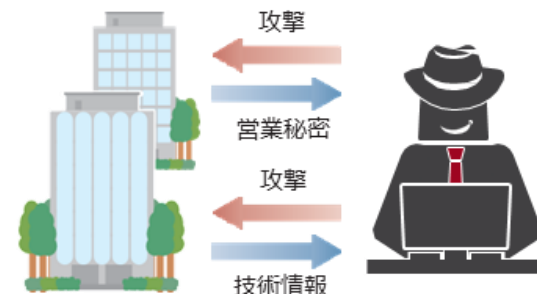
～留学生・研究者等の送り込み～

警戒心を持たれることを回避



サイバー攻撃

～企業や大学等が保有する秘密情報の窃取～



Case 1 : 生産拠点の海外移転に伴う技術流出

【事案の概要】

- 日本の装置メーカーX社は、海外企業Y社に対してライセンス生産を契約。品質確保のために、事前にY社従業員を招へいし、ノウハウなどを含めて技術指導を実施。
- Y社は、数台の生産を行った後、販売不振を理由に契約を終了。その後、別の現地企業が、極めて類似の製品を生産・販売するようになり、X社はシェアを喪失。
- 国内企業間での類似の商慣習に基づき、契約書も不十分であったことから、何も対処することができなかった。

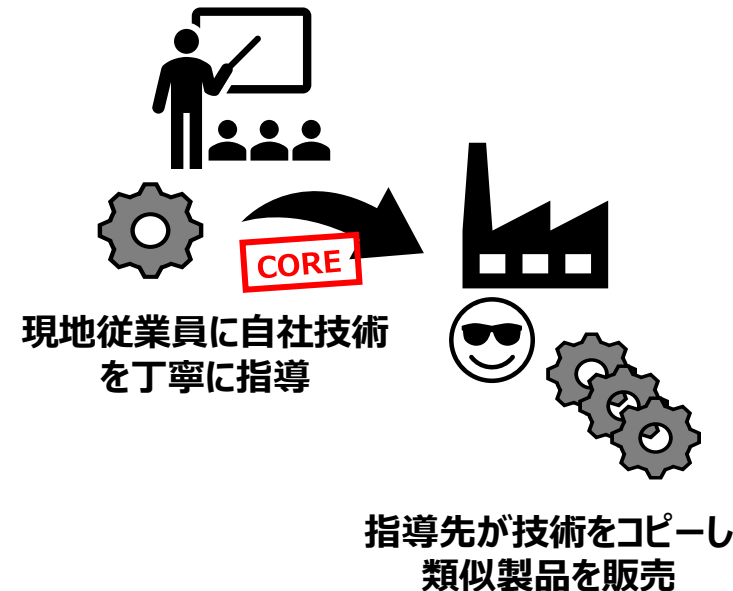
論点

- ・ 現地従業員に自社の技術を丁寧に指導した。
- ・ 同一品を製造されたが、対処できる契約条項がなかった。

本事案からの学びの点

- ・ 対策なしの海外進出・提携は技術流出を招く。
- ・ 全ての技術を提供するのではなく、コアとなる技術の秘匿や特定の素材、部品を日本から持ち込むなど完全にコピーをさせないことが重要。
- ・ トラブルに備えて契約条項は慎重な検討が必要。

関係図



Case 2 : 投資買収に伴う技術流出

- 日本企業のX社は、高い技術力を有していたが、資金難に直面。海外企業Y社からの**資金提供を受諾。その条件として、技術提供を要請される。**
- その後も、追加的な資金需要が生じる度に、Y社から資金提供が提案されるも、**追加的な技術供与や協力関係の深化を要求された。**

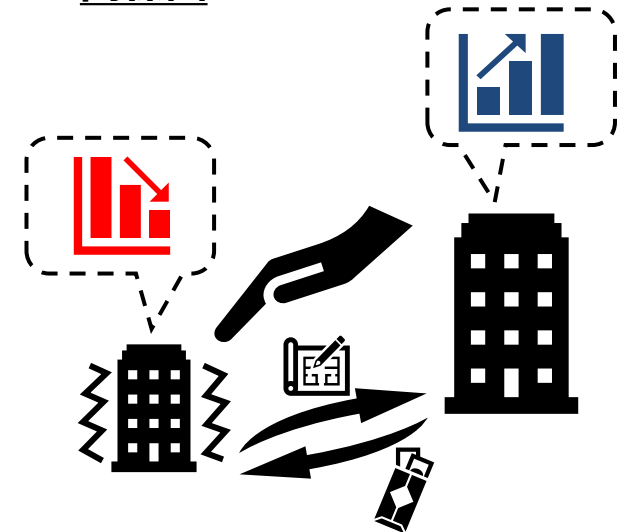
論点

- ・ 海外企業による資金提供の見返りとして、**技術協力**を行った。
- ・ 更なる資金提供の見返りとして、**技術の核心までアクセス可能とするような協力の深化**を条件とされた。

本事案からの学びの点

- ・ 一旦資金提供等での関係を構築すると、**関係の深化**を求められ、最後は**不平等な関係構築**まで求められる可能性がある。
- ・ 関係構築や資金を受け入れる段階で、法律家も交えた**条件の十分な精査**を行うとともに、**メインバンクなど他のステークホルダーとも十分な協議**が必要。

関係図



資金提供の交換条件として、技術提供や不利な条件の合意を迫られる

(参考)「企業価値向上に向けた海外資本活用ガイドブック」(経産省)

- 本年6月、海外プレイヤーとの協業連携やオープンイノベーションにおける、**海外資本活用の具体的検討に際し備えておくべき基礎知識や、有効性を高める上で経営層に期待される行動**を記載した「企業価値向上に向けた海外資本活用ガイドブック」を策定。
- 海外資本活用に際しての留意点・リスクとして、「**意図しない技術等の流出**」についても言及。

企業価値向上に向けた海外資本活用ガイドブック

2025年6月25日
経済産業省

<第1部3.「海外資本活用の留意点・リスク」より抜粋>

- ✓ **悪意のある出資者によって自社の技術・データ等が外部に流出したり、知的財産権に係る不当なライセンス契約によって自社が不利な立場になったりするおそれがある。**
- ✓ 出資者が自社の知的財産権等の活用を計画している場合には、**知的財産権等の出資者への権利付与の要否及びその範囲について、技術流出対策の観点から適切に判断する必要がある。**
- ✓ 出資者から知的財産権等（権利化されていないノウハウや技術を含む）を移転するよう要求されることもあるが、その際、その**価値が正当に評価されているかどうか、確認する必要がある。**
- ✓ 悪意のある出資者が、日本企業の有する知的財産の獲得を目的として、役員を派遣するケースもあるため、**役員指名権の有無やそのアクセス権の範囲等について精査すべきである。**
- ✓ 日本企業は、まず**出資者がパートナーとしてふさわしいかどうかを見極めることが重要**である。

Case 3 : 人を通じた技術流出

- 日本企業X社のA氏は、ある新製品の開発初期から携わっており、**ほぼ全ての行程に関する技術を把握**。
- A氏は、**外資系企業のY社に転職**。その後、**Y社が類似製品の開発を進めている**との情報あり。
- その過程で、A氏が、X社現役社員B氏（A氏の元部下）に対して、**Y社への転職を勧誘**していたことも発覚。

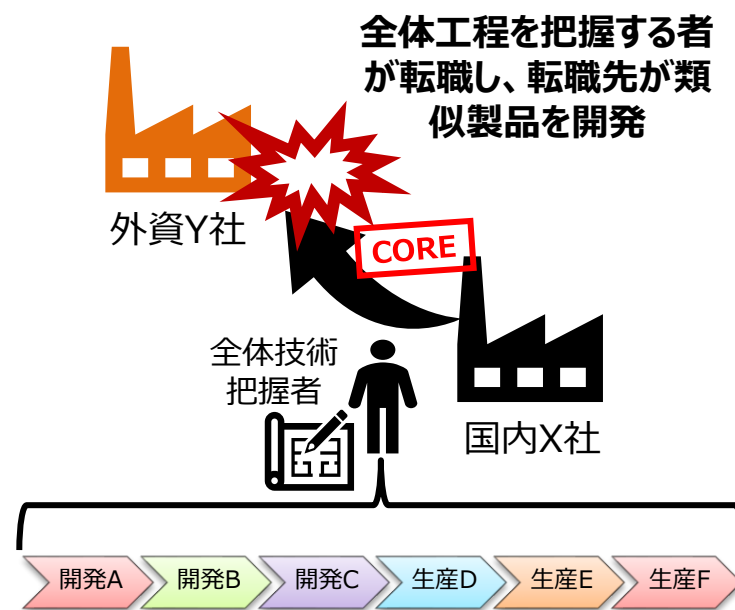
論点

- **全行程を知るキーパーソン**が存在する場合、1人引き抜かれただけで、他社が同様の製品を開発できてしまう。

本事案からの学びの点

- 全ての工程を把握するような重要社員が引き抜かれた場合、技術流出に伴うリスクが格段に増大する。
- **キーパーソンには相応の待遇を与えたり、情報を分割して担当させる**ような工夫を行うことが重要。
- 追加的な引き抜きへの警戒を高めるなども重要。

関係図



Case 4 : 在職する外国人派遣従業員が流出させたケース

- 日本企業X社に派遣職員として在籍していた外国人Aは、ユーザー企業の保守メンテナンス作業を担当。
- Aは、X社の派遣契約終了後に備え、同業他社への就職活動を開始。その際、**X社の内部資料が含まれるデータ一式を記録媒体にダウンロードし、持ち出した上で退職。**

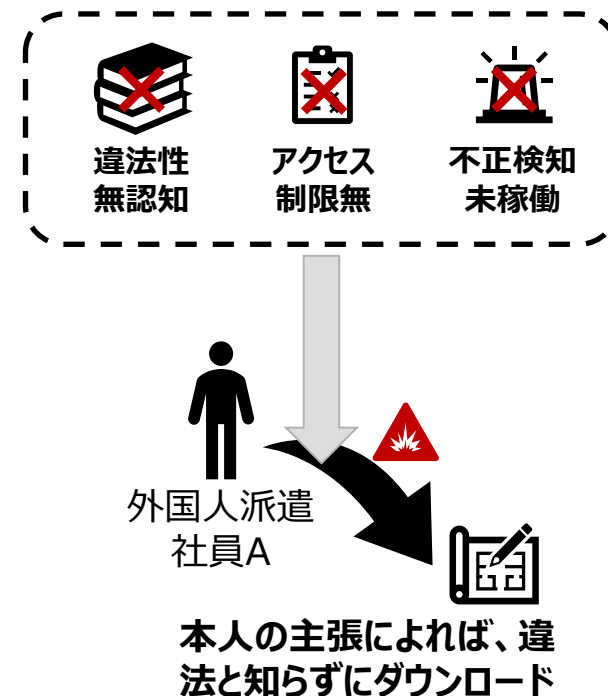
論点

- ・ Aの主張によると、**データ持ち出しが違法であるとは認識しておらず、データ持ち込みが転職先で歓迎されると考えていた。**
- ・ X社は、当該派遣社員に対しても、**内部資料にアクセスできる状態**にしていた。また、ダウンロード時の**不正検知も作用せず**、一旦は持ち出しを許すこととなった。

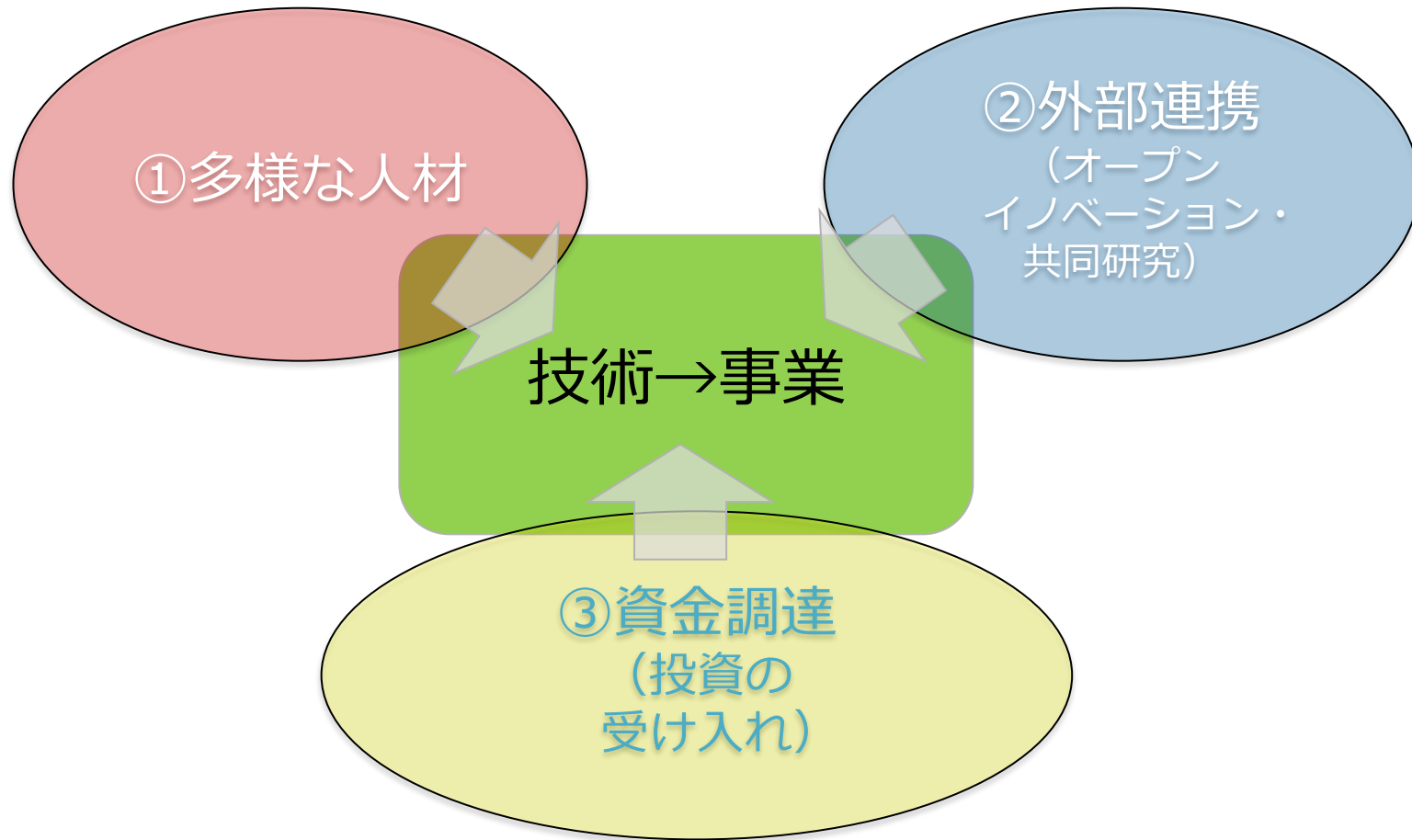
本事案からの学びの点

- ・ （派遣含む）従業員に対する教育の徹底。特に、外国人は異なる文化、法律に関する常識を有している可能性があり、**専用のカリキュラムを設ける必要**あり。
- ・ アクセス管理とアクセス権の設定を徹底し、**不必要な人員に機密データにアクセスさせないことが重要。**
- ・ データのダウンロードに際しての**検知・確認をシステム化**することが重要。

関係図



技術管理の出発点は、自社のコア技術（守るべき技術）を認識すること



1. ① コア技術の特定

- 企業活動において役職員が取り扱う情報は膨大であり、その重要度・機微度にも差がある。人を通じた技術流出については、**技術の重要度に応じたメリハリのある対策が肝要**。
- そのため、人を通じた技術流出対策を講じる前提としても、**企業の競争力の源泉たる重要技術（コア技術）を特定することが重要**である。
- 本章で記載する対策を含め、社内で技術流出対策を実施する際には、**コア技術か否かに応じて、より厳格な対策を講じる、対策の組合せ方を変えるといった工夫も有効**。

対応策の例

① 自社の競争力の源泉が何であることを改めて確認する

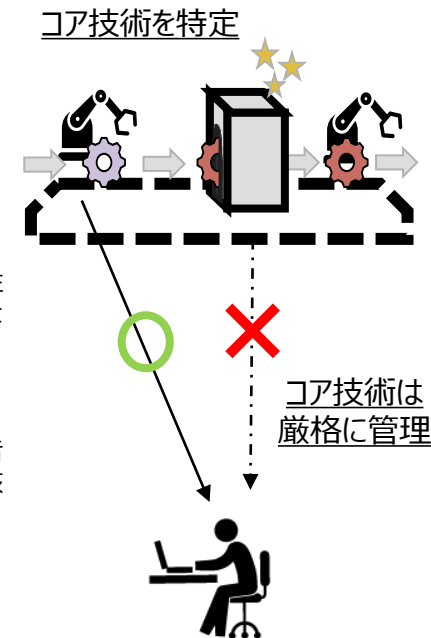
- 自社の製品のどのような点が市場において評価されているかを確認する。
- その上で、当該競争力は、どのような要素技術によって実現しているかを分析し、コア技術として特定する。
- 当該プロセスに、現場の技術者も関与させることで、組織全体の意識啓発につながることも期待できる。

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、他国の企業等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、市場における将来性やサプライチェーン上の重要性・不可欠性（チョークポイントをなす唯一無二の技術か）を確認する。また、自社が当該技術を有するに至る経緯（投下した労力や費用、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、どの様な形態で存在するかにより、自ずと管理手法も変化してくる。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、コア技術の存在する形態に応じて、当該技術に接する立場にある役職員の範囲や地位等も確認する。

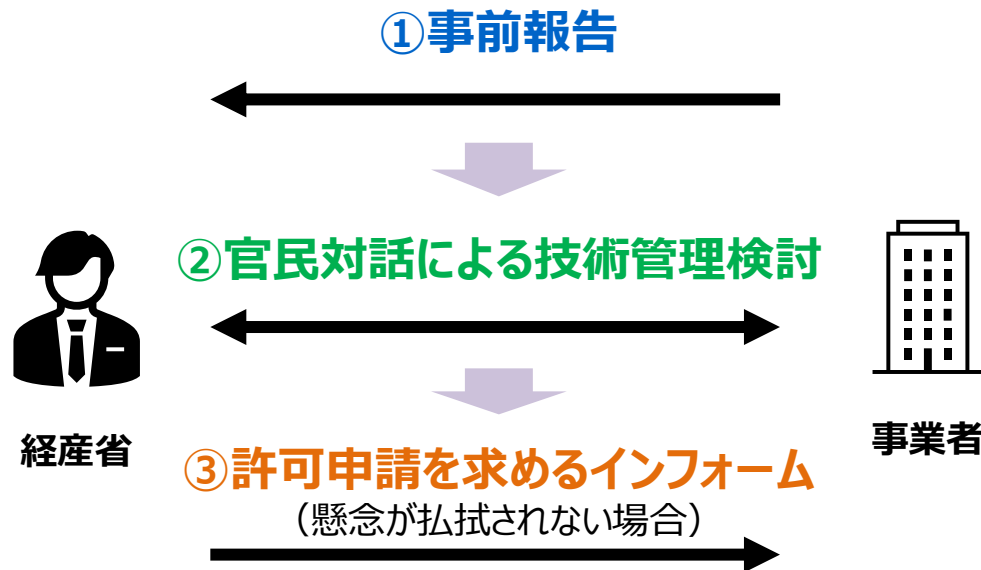


1. なぜ、今、技術流出対策が重要か
2. 技術流出の経路と事例
3. **技術流出対策のための各施策**

官民対話による技術管理対話スキーム

- 技術は、貨物に比して、一度移転すれば、管理の難易度が高くなる。また、移転後の時間的経過とともに主体や用途が変化し、当初想定できないような軍事転用に繋がる懸念がある。
- このため、安全保障上の観点から管理を強化すべき重要技術の移転に際して、外為法に基づく事前報告制度を設け、これを端緒として官民が確実に対話する。
- 技術移転を止めることが目的ではなく、適切な技術管理を徹底することが目的。技術流出の懸念が払拭されない場合に、許可申請を求めるインフォームを発出する場合もあるが、原則として、対話を通じた信頼関係の下での解決を目指す。
- 事前報告対象として、現在 15 技術を指定しており、今般、新たに 4 技術を追加するべく手続き中。

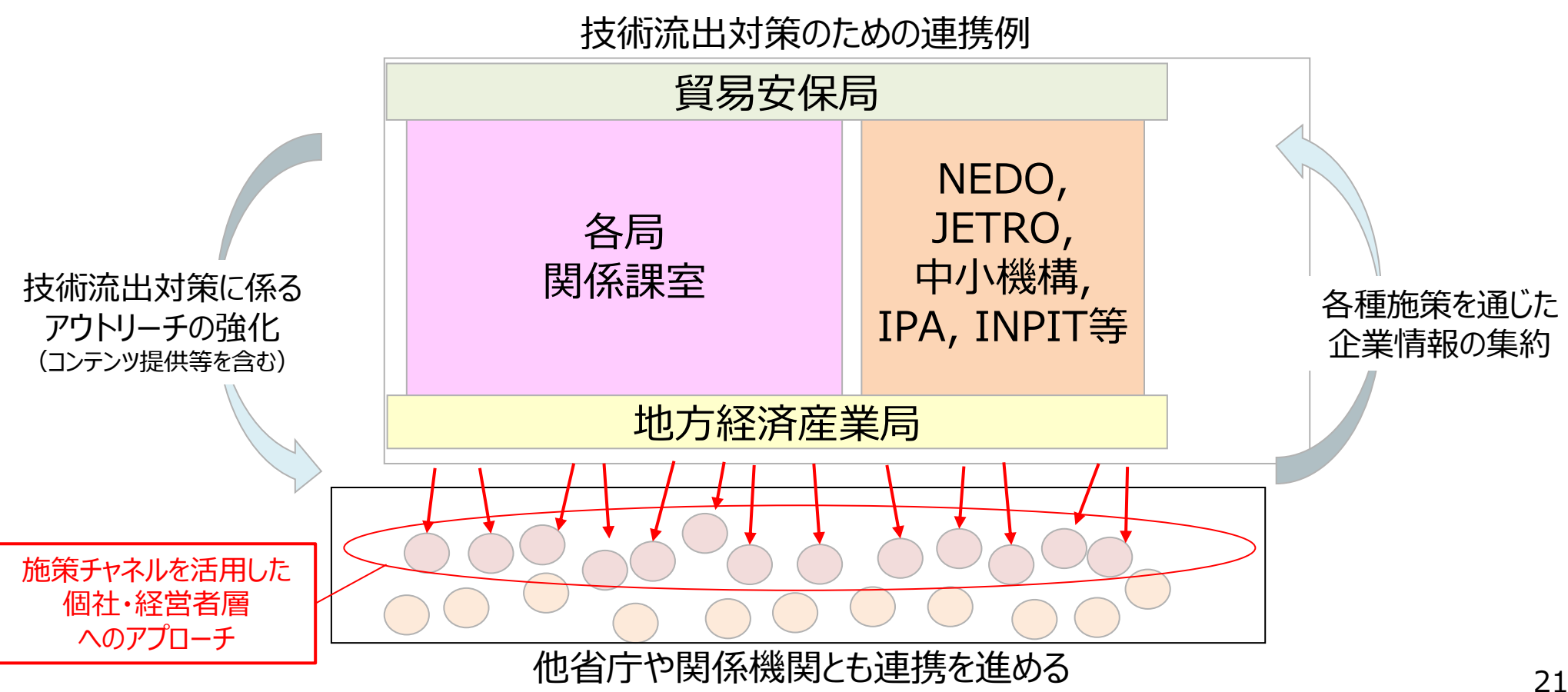
<スキーム概要>



事前報告の対象技術	
①積層セラミックコンデンサ (MLCC)	⑪磁気センサー
②SAW及びBAWフィルタ	⑫スポンジチタン
③電解銅箔	⑬正負極バインダ
④誘電体フィルム	⑭固体電解質
⑤チタン酸バリウム	⑮セパレータ製造装置
⑥炭素繊維	⑯量子ドット
⑦炭化ケイ素繊維	⑰TADF材料（有機EL次世代発光材料）
⑧フォトレジスト	⑱位相差フィルム
⑨非鉄金属ターゲット材	⑲軟性内視鏡
⑩走査型／透過型電子顕微鏡 (SEM／TEM)	
今般の追加	

技術流出対策の強化に向けたアウトリーチ活動の強化

- 技術流出対策は、各企業が、技術管理の重要性を理解し、主体的に取り組むことが必要。各企業の取組を促進するため、参考となるコンテンツの充実を図る。
- 産業界全般に対する広範な働きかけに留まらず、個社、特に中堅・中小企業の場合には経営者層へのきめ細かいアプローチが重要。
- 経済産業省の関係部局と連携しつつ、独立行政法人、関係団体、他省庁、他機関等が有するチャンネルも活用し、地域の中堅・中小企業に対するアウトリーチを強化する。



民間の好事例の横展開① 民間ベストプラクティス集

- 産業界の経済安全保障に対する意識は徐々に高まっているものの、大企業を含め、具体的に何をすればよいか分からないとの声。
- このため、民間の好事例の横展開を目指し、「民間ベストプラクティス集」を策定（令和5年10月）。
- 現在、民間ベストプラクティス集第2．0版を公開中。

【民間ベストプラクティス集】

経済産業省

経済安全保障上の課題への対応
(民間ベストプラクティス集)
—第2.0版—

経済産業省
貿易経済安全保障局
技術調査・流出対策室

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
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 ●技術の区分 ●人員配置の工夫 ●接触リスク分析 ●防止策（取引先等）
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）

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

● 経済安全保障とは何か？
● 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把握できるか？

情報提供
(重要トピック定額版)

検討機会提供
(1on1MTG版)

社内組織
ミドルマネジメント層
外部有識者

◆ YouTubeで紹介動画を公開中！



アクセスはこちら

<https://www.youtube.com/watch?v=pll5RygY0l8>



◆ 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

民間の好事例の横展開② 技術流出対策ガイドンス

- ベストプラクティス集を部分的に発展させ、ビジネスシーンに応じた拡充・体系化を図るべく、企業ヒアリングや、産業界・労組・学識経験者等による研究会での議論を踏まえ、「**技術流出対策ガイドンス**」を策定（令和7年5月）。
- 本ガイドンスは、企業に**義務を課すものではなく、選択肢を示すもの**。完璧な対策はないことを前提に、最大限の努力を促す。今後、技術流出対策について**官民対話を行う際に活用**する。
- 第1版では、「**生産拠点の海外進出に伴う技術流出**」と、「**人を通じた技術流出**」に焦点を絞っている。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**を図る。

【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	●技術の区分 ●人員配置の工夫 ●接触リスク分析 ●防止策（従業員） ●防止策（退職者） ●防止策（取引先等）
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	●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）

拡充・体系化

【技術流出対策ガイドンス】

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をすることが前提。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や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、どのような要素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、特に取扱い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自獨に開発されうる技術であるか否かを確認する。併せて、市場における将来性やサプライチェーン上の重要性・不可欠性（「ジョーポイント」をなす技術＝二重特許の）を確認する。また、自社は当該技術を開発するに至る経路（限られた努力や費用、技術開発に至る研究開発活動の独創性など）の検証も有効である。

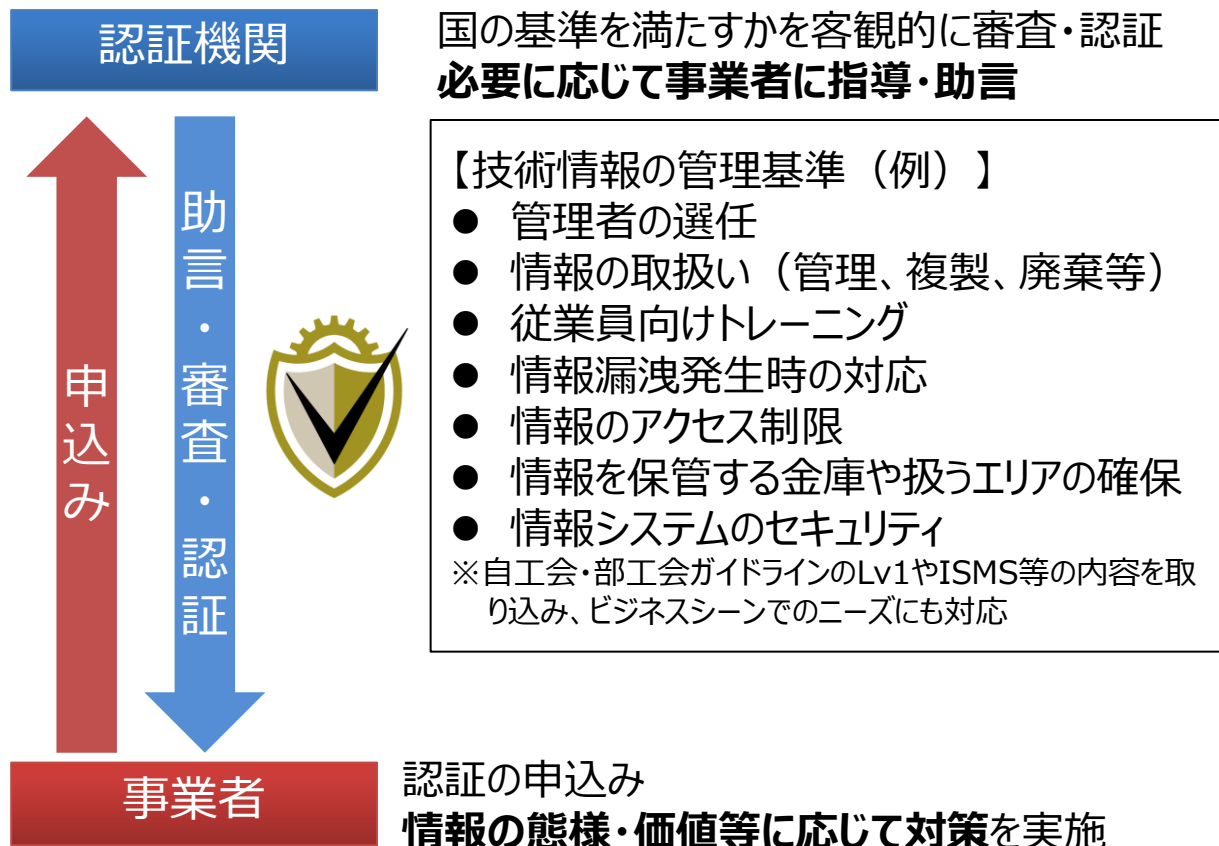
③コア技術が、どの様に存在しているかを確認する

- コア技術が、どこに、どのような形態で存在するかにより、自社の管理手法を定めていく。設計図面、製造工程データ、技術者の知見／ノウハウ、カスタマイズした製造装置に依存しているかなどを確認する。また、コア技術の存在する形態に応じて、当該技術に接する立場にある関係者の範囲や役割等を確認する。

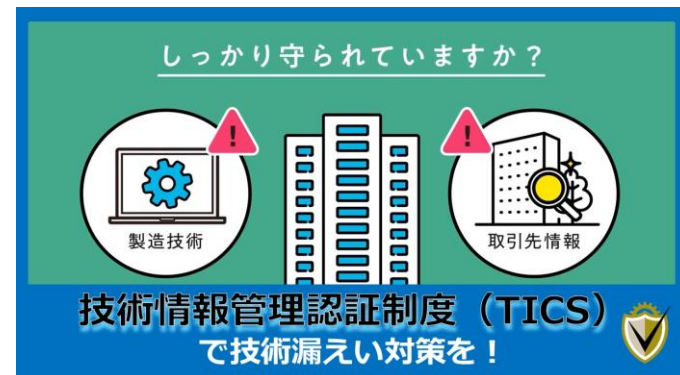


技術情報管理認証制度（TICS）

- 技術流出対策や情報管理を進めるには、社内ルールの策定や体制の構築、情報アクセス制限の付与など、包括的な対応が必要。他方、経営資源に限りがある中小企業には、自社のみで取組を進めることが難しいとの声も寄せられていた。
- 国が設けたTICSでは、企業は認証機関の指導・助言を受けつつ、体制整備等に取り組み、その状況が客観的に審査・認証される。企業の対策を、取引先等に表示することが可能となり、取引先からの信頼性も向上。



◆ 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>



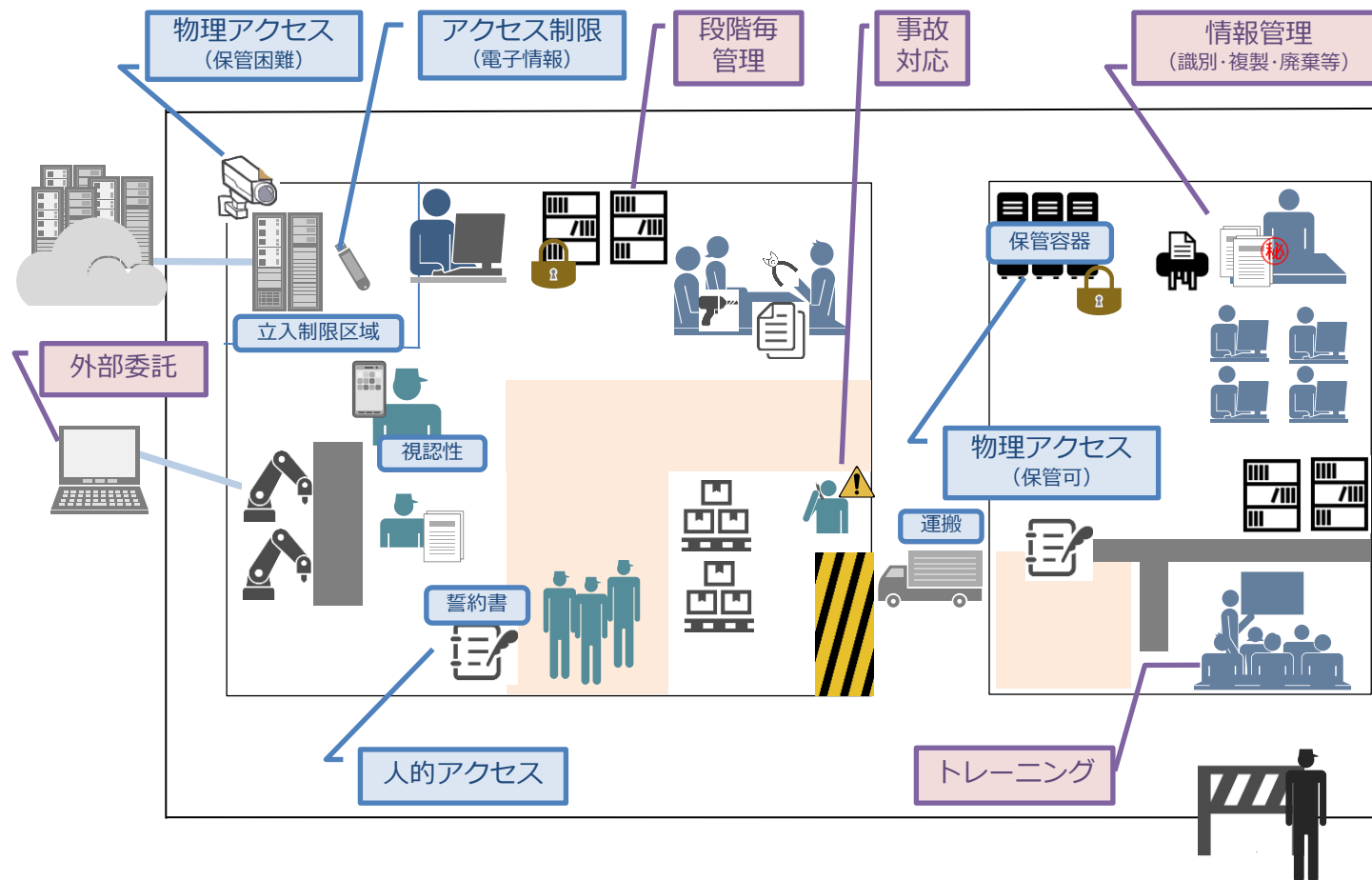
◆ 技術情報管理認証制度の詳細は ウェブページをご覧ください

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



(参考) 技術情報管理認証 (TICS) の取得に必要な取組 (例)

- 例えば、①守る情報の決定、②守る情報の識別・対策整理、③管理責任者選任、④情報管理プロセスの設定、⑤従業員への対策周知や教育、⑥情報漏えい等の事故発生時の報告ルールの設定、⑦管理対象情報へのアクセス権の設定、⑧金庫等による物理的情報の管理、⑨ID設定等による電子情報の管理、などが必要。
- サイバーセキュリティのほか物理的対策・人的対策も含め、**情報セキュリティ対策を総合的に審査**。



(参考)「ものづくり補助金」の採択審査時の優遇

- 中小企業等による革新的な新製品・新サービス開発や海外需要開拓を行う事業のために必要な設備投資等を補助する事業。
- 2024年度は2回の公募で、延べ約2,200者が採択。
- 認証取得事業者は、採択審査時に加点を受けられる。

現行の支援概要

※詳しい情報は最新の公募要領をご確認ください <https://portal.monodukuri-hojo.jp/>

補助対象経費	機械装置・システム構築費（必須）、技術導入費、専門家経費、運搬費、クラウドサービス利用費、原材料費、外注費、知的財産権等関連経費 （グローバル枠の内、海外市場開拓に関する事業のみ）海外旅費、通訳・翻訳費、広告宣伝・販売促進費
--------	---

申請類型	従業員規模	補助上限額	補助率
製品・サービス高付加価値化枠 革新的な新製品・新サービス開発の取組に必要な設備・システム投資等を支援	5人以下	750万円	中小企業1/2、小規模企業・小規模事業者及び再生事業者2/3
	6～20人	1,000万円	
	21～50人	1,500万円	
	51人以上	2,500万円	
グローバル枠 海外事業（①海外直接投資、②海外市場開拓（輸出）、③インバウンド対応、④海外事業者との共同事業）を実施し、国内の生産性を高める取組に必要な設備・システム投資等を支援	従業員規模毎の区切り無し	3,000万円	中小企業1/2、小規模企業・小規模事業者2/3

※特例措置として、大幅な賃上げに取り組む事業者には、補助上限額を100～1,000万円上乘せ。最低賃金の引き上げに取り組む事業者は、補助率を2/3に引上げ。

(参考)「中小企業新事業進出補助金」の優遇 (令和7年度開始)

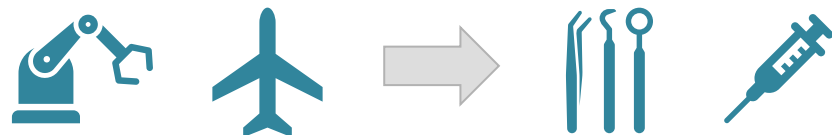
- 既存の事業とは異なる、新市場・高付加価値事業への進出にかかる設備投資等を支援
- 認証取得事業者は、採択審査時に加点が受けられる

現行の支援概要

項目	内容								
補助対象者	企業の成長・拡大に向けた新規事業への挑戦 を行う中小企業等								
補助金額	<table><tr><td>従業員数20人以下</td><td>750万円～2,500万円 (3,000万円)</td></tr><tr><td>従業員数21～50人</td><td>750万円～4,000万円 (5,000万円)</td></tr><tr><td>従業員数51～100人</td><td>750万円～5,500万円 (7,000万円)</td></tr><tr><td>従業員数101人以上</td><td>750万円～7,000万円 (9,000万円)</td></tr></table> ※賃上げ特例の適用による補助上限額の引上げを受ける事業者の場合、括弧内の補助上限額を適用	従業員数20人以下	750万円～2,500万円 (3,000万円)	従業員数21～50人	750万円～4,000万円 (5,000万円)	従業員数51～100人	750万円～5,500万円 (7,000万円)	従業員数101人以上	750万円～7,000万円 (9,000万円)
従業員数20人以下	750万円～2,500万円 (3,000万円)								
従業員数21～50人	750万円～4,000万円 (5,000万円)								
従業員数51～100人	750万円～5,500万円 (7,000万円)								
従業員数101人以上	750万円～7,000万円 (9,000万円)								
補助率	1 / 2								
補助対象経費	機械装置・システム構築費、建物費、運搬費、技術導入費、知的財産権等関連経費、外注費、専門家経費、クラウドサービス利用費、広告宣伝・販売促進費								

新事業となる例 (イメージ)

航空機用部品製造業者が技術を活かし、新たに医療機器部品の製造に着手



※詳しい情報は最新の公募要領をご確認ください
<https://shinjigyou-shinshutsu.smrj.go.jp/>

(参考)「Go-Tech事業」採択審査時の加点と認証取得経費補助

- 「成長型中小企業等研究開発支援事業（Go-Tech事業）」（旧サポイン・サビサポ事業）において、認証取得事業者による申請を優遇するとともに、すべての申請事業者に認証取得を推奨。
 - ✓ 認証取得事業者は採択審査時に加点
 - ✓ 申請時の技術情報の管理の実施状況の申告を認証取得済の事業者は免除
 - ✓ 認証未取得の事業者は認証取得費用も補助

成長型中小企業等研究開発支援事業（Go-Tech事業）とは

（補助率：原則 2 / 3 以内、補助上限額：2 年度で 7 5 0 0 万円 など）

- 中小企業等が大学・公設試等と連携して行う、ものづくり基盤技術及びサービスの高度化に向けた研究開発等を支援。
- 研究開発等に当たって事業者は、複数の企業や、大学・公設試等の研究機関等、及びアドバイザー等と連携し、共同体を構成。

申請時

認証取得済みの
補助金応募事業者

補助金申請時に認証を取得していることを申告

中小企業庁

採択審査時に加点

採択後

認証未取得の
補助金採択事業者

認証取得に要する経費を計上

中小企業庁

費用補助

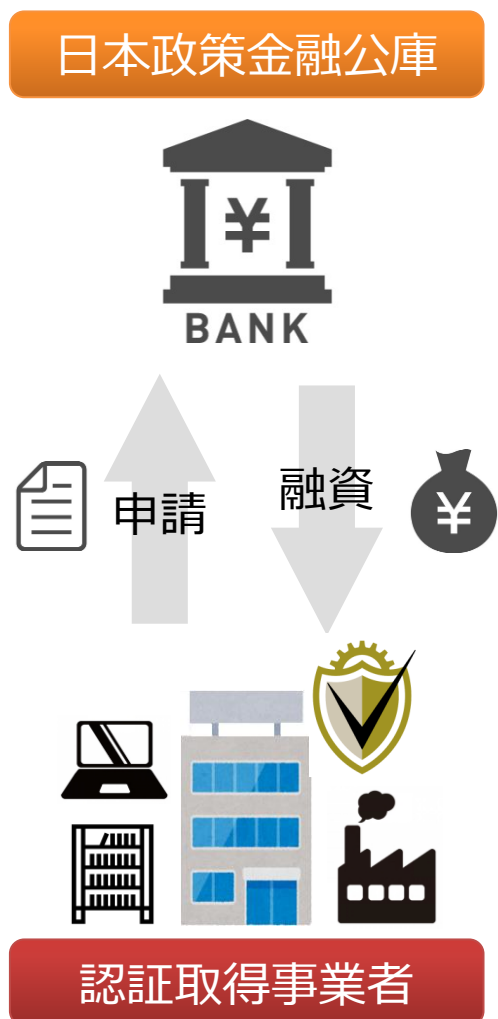
※詳しい情報は最新の公募要領をご確認ください

<https://www.chusho.meti.go.jp/support/innovation/2025/250217kobo.html>

(参考) 認証取得事業者への低利融資制度

- 日本政策金融公庫の「IT活用促進資金」は、情報技術の活用の促進を図る中小企業を支援。
- 技術情報管理認証を取得した中小企業に対し、I T 関連設備を取得するための設備資金及び運転資金を特別利率で融資。

IT活用促進資金の概要（技術情報管理認証関連部分）



貸付対象	1. 電子計算機（ソフトウェアを含む） ※ 2. 周辺装置（モデムなどの通信装置など） 3. 端末装置（多機能情報端末など） 4. 被制御設備（高度数値制御加工装置（CNC）や自動搬送装置など） 5. 関連設備（LANケーブルや電源設備など） 6. 関連建物・構築物（上記装置および設備の導入に併せてその取得に必要不可欠なもの） ※ 2～6 の他の設備等と組み合わせて導入する場合のみ対象
利 率	基準利率。ただし、技術情報管理認証の取得事業者は、2 億 7 千万円を限度とし設備資金について特別利率①（基準利率より0.4%低い利率※）を適用。 <u>（無担保でも適用）</u> ※令和 7 年 4 月時点の利率
融資限度額	7 億 2 千万円
貸付期間	設備資金：20 年以内 運転資金：7 年以内

詳しい情報は日本政策金融公庫のHPをご確認ください。

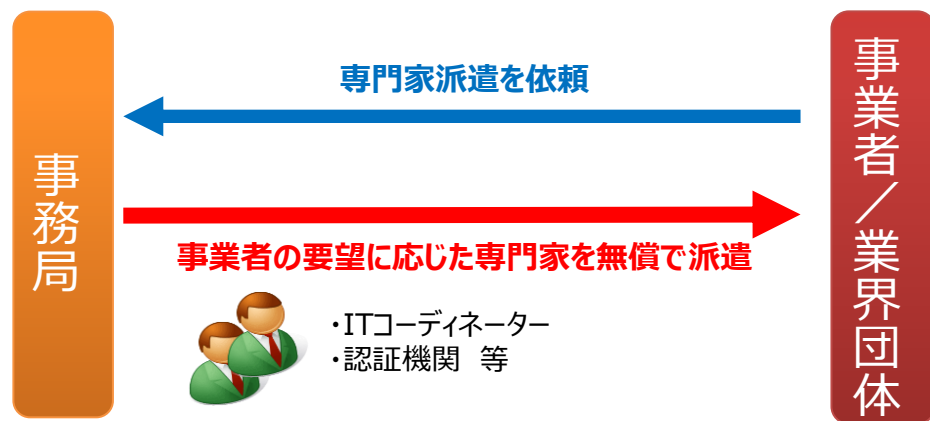
https://www.jfc.go.jp/n/finance/search/11_itsikin_m_t.html

(参考) 技術情報管理のための専門家派遣事業

- 適切な技術情報管理を促進するため、認証機関及び事業者への支援等を実施。
- 認証取得を検討する事業者等への支援として、情報セキュリティの専門家を無償で派遣し、守るべき情報の見極めや具体的な情報セキュリティ手法をアドバイス。

【2024年度利用実績：延べ90回】

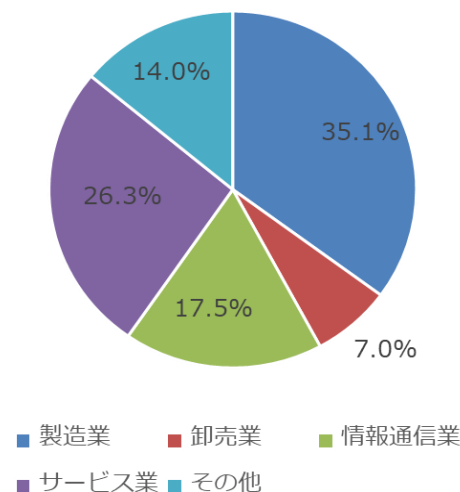
専門家派遣事業の流れ



<支援内容例>

- (1) 守るべき情報の特定
- (2) 情報セキュリティ、認証取得に係るアドバイス ほか

2024年度の派遣先事業者等の業種



2025年度専門家派遣事業は2025年8月18日より開始しています。

以下の認証制度HPよりお申込みいただけます（上限に達した場合、締め切られる可能性があります）

https://www.meti.go.jp/policy/mono_info_service/mono/technology_management/page04.html

関心を持っていたら：まずはチェックリストをお試ください

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？	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く、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はなく、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 <table><thead><tr><th colspan="2">確認者</th><th>チェック欄</th></tr></thead><tbody><tr><td>情報セキュリティ責任者</td><td></td><td></td></tr><tr><td>情報セキュリティ担当部門</td><td></td><td></td></tr></tbody></table>	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		
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											
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説明しているか？										

1 内容

2 ページ

I 共通項目		チェック欄
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冒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。	

[guidance.pdf](#)

個別の相談にご関心の方：INPIT知財戦略エキスパートのご紹介

実践感覚を持った企業出身の「知財戦略エキスパート」が、「教科書」には載っていない知財活動のリアルな現場で培った豊富な専門知識・ノウハウを活かして、知財を活用した海外展開や営業秘密管理、大学・スタートアップにおける知財経営戦略策定や産学連携推進など、皆様の課題解決をサポートします！

営業秘密支援窓口

✓相談無料！ ✓全国各地へ訪問可能！

中小企業等の皆様に対し、技術ノウハウ、商品アイデア、顧客情報といった秘密情報の抽出や管理ルールの整備、社内セミナーの実施等の支援サービスを提供する専門窓口です。

（海外展開知財支援窓口/アカデミア知財支援窓口/スタートアップ知財支援窓口もINPIT本部に設置）

相談例

- 営業秘密に関する**管理体制を構築したい**
- 営業秘密の**漏えい・流出事案への対処方法を知りたい**
（要望に応じて警察庁と連携可能）
- **情報セキュリティ対策を強化したい**
（要望に応じて情報処理推進機構（IPA）と連携可能）
- **権利化／秘匿化の判断や、それらを組み合わせた知財戦略を知りたい**



営業秘密支援窓口

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

支援依頼Webフォーム

https://www.inpit.go.jp/form/gippd_inquiries.html



本日のまとめ：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。

