経済産業省

経済安全保障の観点からの技術流出対策について

２０２５年１１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施策の紹介

４．技術情報管理認証制度

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施策の紹介

４．技術情報管理認証制度

技術情報流出リスクの高まり

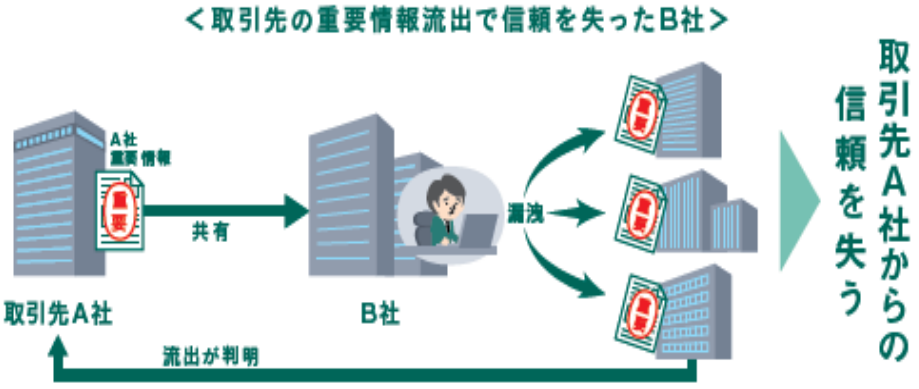
- **グローバル化の進展**等を背景に、国内外への**技術情報流出リスクが拡大**。
- 技術進歩に伴い、**民生技術を軍事転用する流れが拡大**し、**あらゆる先端技術の保有主体が技術獲得のターゲット**に。更に、大国間の対立の深刻化に伴い、技術を通じて自国の勢力を拡大しようとする事例も見受けられ、**サプライチェーンのカギとなる技術を保有する中小企業がターゲットとされるリスクも増大**。
- 技術情報はいったん**流出すると回収が難しく**、**経済的に大きな損失を負う**とともに、**取引先からの信頼を失い**、**事業者の競争力が大きく棄損**するおそれ。

技術情報流出リスクの高まり

- **グローバル化の進展**
  - 国際的な人材流動性の高まり
  - 国際競争の激化
- **IT技術の進展**
  - サイバー攻撃の巧妙化
  - 大容量データの持ち出しが容易に
  - テレワークによる情報流出リスク
- **経済安全保障環境の変化**
  - 民生技術の軍事転用拡大
  - 技術覇権を巡る対立

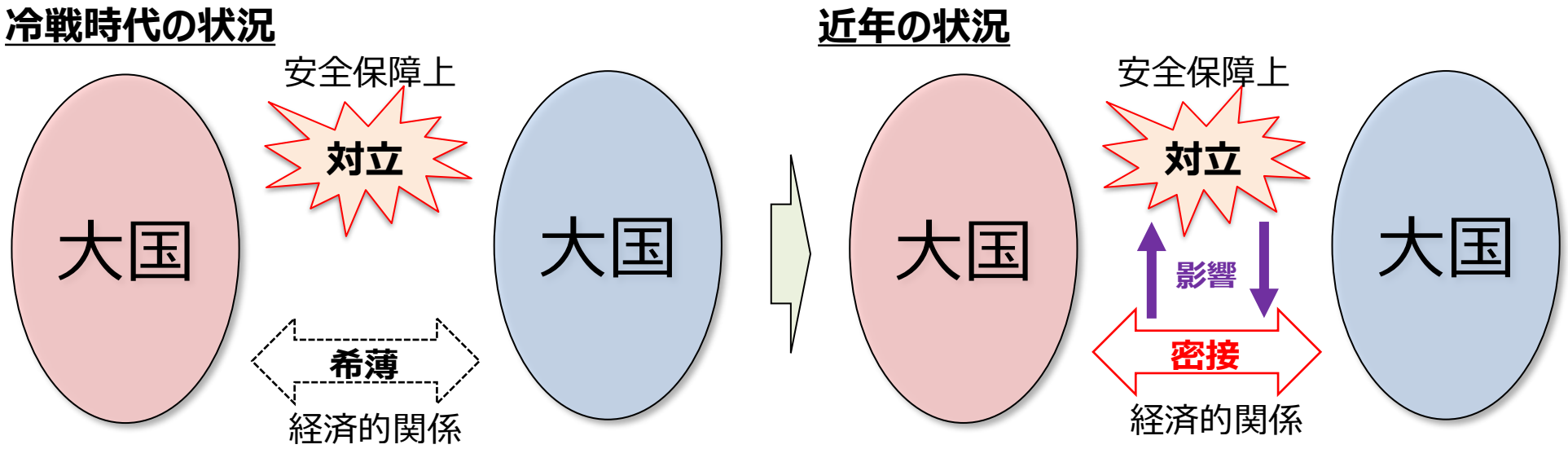
<関係者による技術流出で大きな損失を被ったC社>

<取引先の重要情報流出で信頼を失ったB社>



経済安全保障の重要性の高まり

- 冷戦時代、東西諸国は対立していたが、同時に**経済的な関係は希薄**。
- 近年、大国間の対立が顕在化する一方、既にグローバルなサプライチェーンが構築され、**経済的には相互に依存しあう複雑な関係**。
- このため、自国の勢力拡大を図るために経済的な威圧を加えるなど、**経済活動が手段として用いられるリスク**が拡大。経済の**自律性や不可欠性の確保が、国家の安全保障上の重要課題**に。
- 自律性や不可欠性のカギを握るのは**民間の技術力**。技術優位性の維持・獲得は、単なる**産業競争力強化の視点に留まらない各国の関心**に。



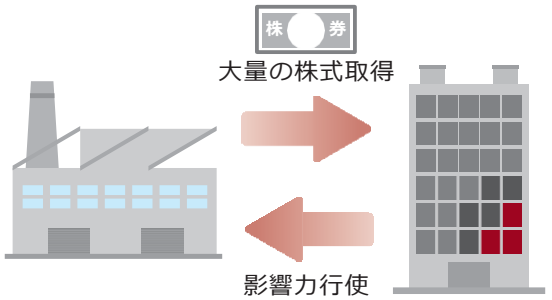
- **自律性、不可欠性の基盤は、民間の優れた技術。ゆえに狙われている。**

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～

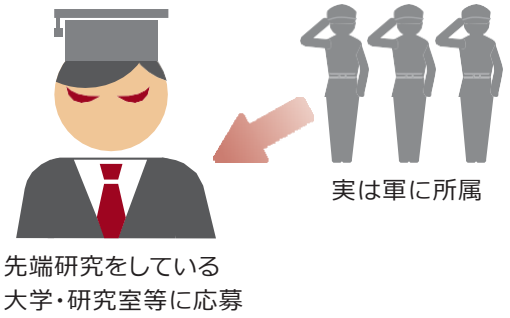
投資・買収・合併
～影響力を行使して意思決定に関与～



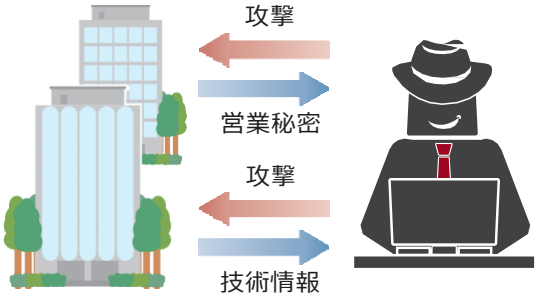
不審なアプローチ
～従業員との1対1の関係構築～

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～



サイバー攻撃
～企業や大学等が保有する秘密情報の窃取～



<出典>公安調査庁「経済安全保障の確保に向けて　～技術・データの流出防止～」（2021年版）

技術情報の流出理由

- 外部からの悪意ある**サイバー攻撃だけでなく**、**ヒューマンエラーや従業員を経由した情報流出も発生**。

	2021年 n=1,616 JP
1位	25.2% 電子メール、FAX、郵便物等の誤送信・誤配送
2位	14.9% 標的型メール攻撃
3位	14.5% 情報機器・外部記憶媒体の紛失・置き忘れ・棄損
4位	11.9% マルウェア感染
5位	11.4% 社員証、業務書類等物品の紛失・置き忘れ・棄損
6位	10.6% システム設定ミス、誤操作
7位	9.0% 情報機器、電子記憶媒体、紙媒体等の盗難・紛失
8位	6.1% DoS攻撃／DDoS攻撃
9位	5.3% ランサムウェアによる金銭等の要求
new 10位	4.0% 退職者、転職者による在職時に利用していた情報の使用

【事例①】サプライチェーンの弱点を悪用した攻撃

- 2022年3月、自動車製造企業の取引先において、子会社のリモート接続機器の脆弱性を利用したランサムウェア攻撃により一部のデータが暗号化され、その対応のため自動車製造企業の国内全工場が停止した。

【事例②】不注意による情報漏えい

- 2022年6月、市役所のシステムのデータ移管作業を請け負った事業者の従業員が、定められた手続きを踏まずに住民情報が保存されたUSBメモリーを持出したまま飲酒し、紛失した。

【事例③】内部不正による情報漏えい

- 2022年9月、飲食店チェーンの役員が競合する別企業に転職したのち、元同僚に依頼して商品原価等の情報を持ち出し、転職先で利用した疑いで逮捕。

＜出典＞NRI Secure Insight 2021（NRIセキュアテクノロジーズ株式会社）

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施策の紹介

４．技術情報管理認証制度

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。

Case１：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。**

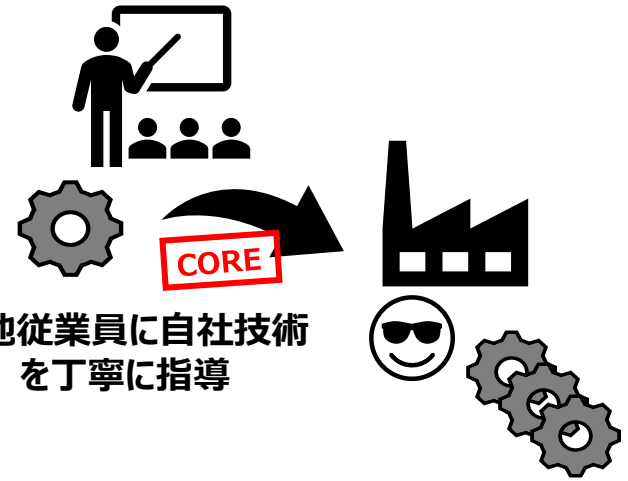
論点

- 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



Case２：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。

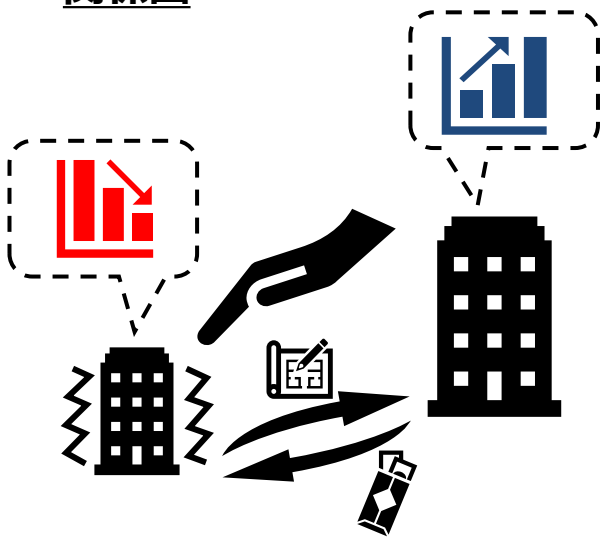
論点

- **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

Case３：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。

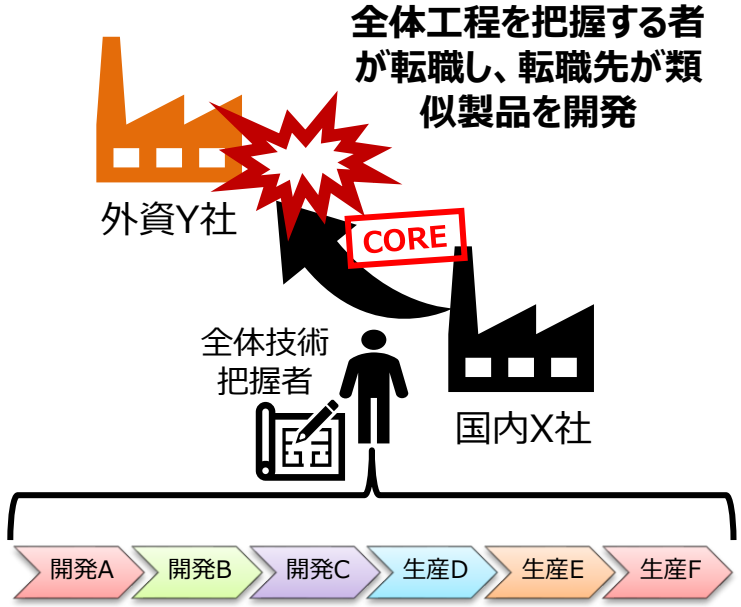
論点

- **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



Case４：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ー式を記録媒体にダウンロード**し、持ち出した上で退職。

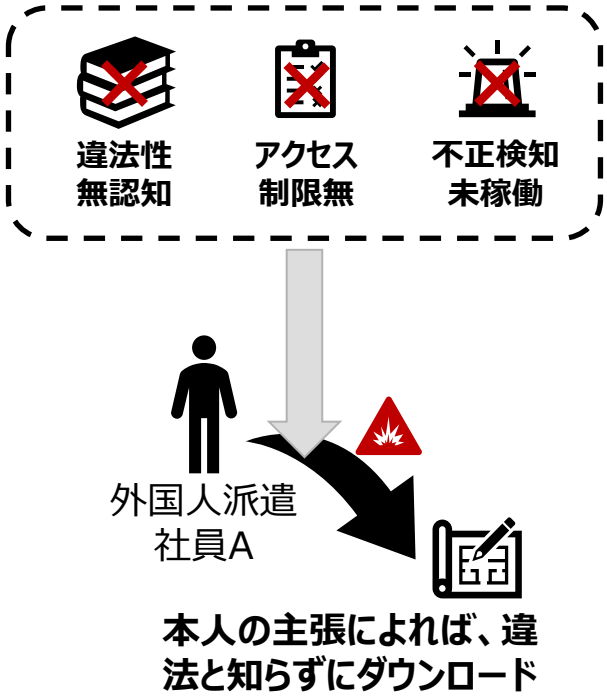
論点

- 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



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

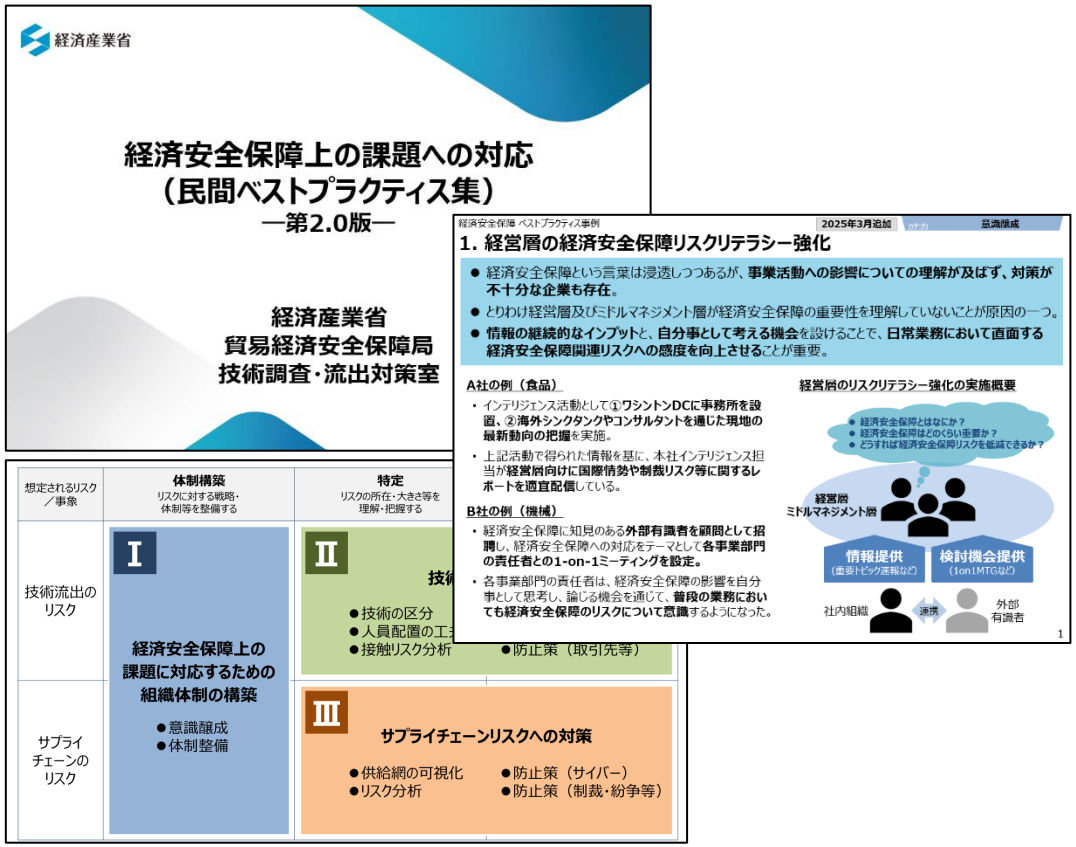
３．技術流出対策のための施策の紹介

４．技術情報管理認証制度

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】



◆ 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/best_practice2.0.pdf

技術流出対策ガイダンス

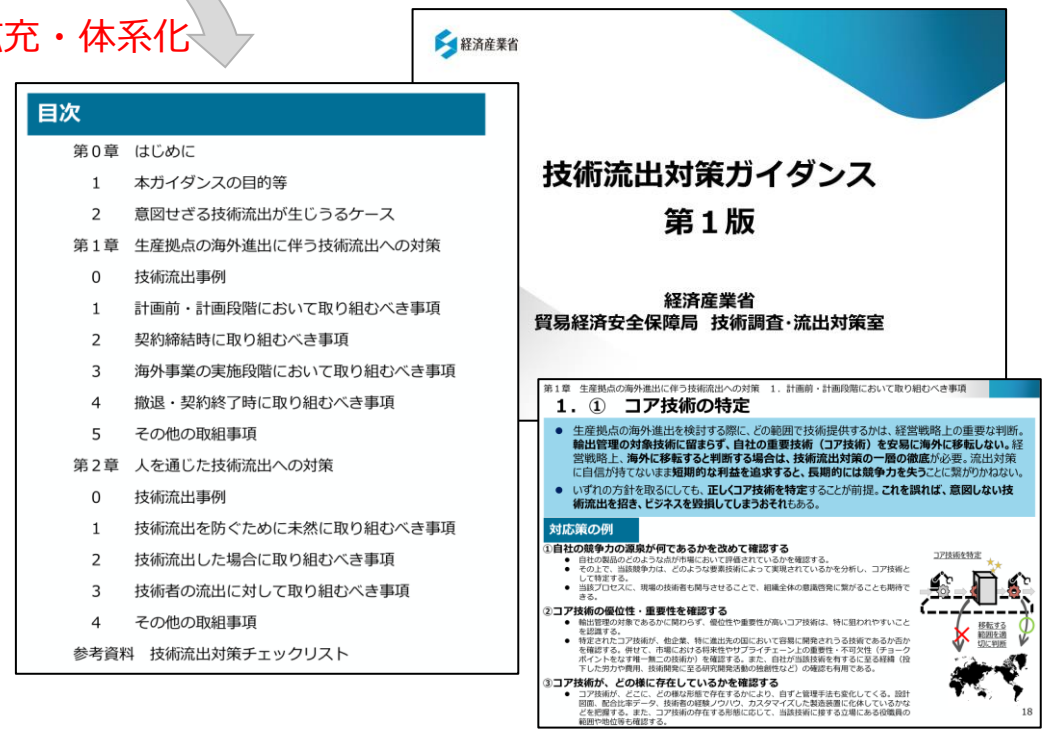
- ベストプラクティス集を部分的に発展させ、ビジネスシーンに応じた拡充・体系化を図るべく、企業ヒアリングや、産業界・労組・学識経験者等による研究会での議論を踏まえ、**「技術流出対策ガイダンス」**を策定（令和7年5月）。
- 本ガイダンスは、企業に**義務を課すものではなく、選択肢を示す**もの。完璧な対策はないことを前提に、最大限の努力を促す。今後、技術流出対策について**官民対話を行う際に活用**する。
- 第1版では、**「生産拠点の海外進出に伴う技術流出」**と、**「人を通じた技術流出」**に焦点を絞っている。今後、「共同研究等の連携に伴う技術流出」など、**継続的に改訂・拡充**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

【技術流出対策ガイダンス】

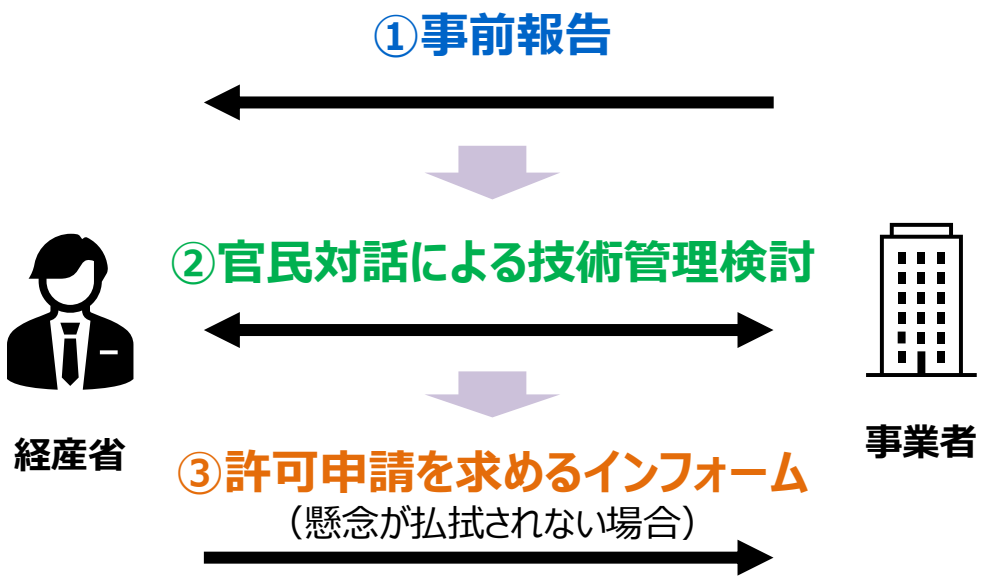


https://www.meti.go.jp/policy/economy/economic_security/guidance.pdf

外為法に基づく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、今般、**新たに４技術を追加（公布済み）**。

＜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

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施策の紹介

４．技術情報管理認証制度

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、取引先等に示すことが可能となり、**取引先からの信頼性も向上**。

認証機関

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

申込み

助言・審査・認証

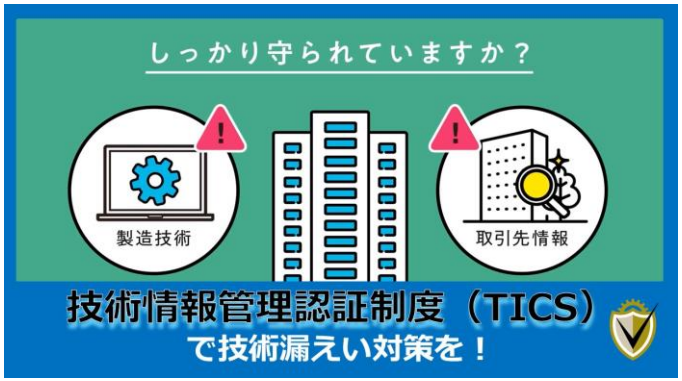
【技術情報の管理基準（例）】
- 管理者の選任
- 情報の取扱い（管理、複製、廃棄等）
- 従業員向けトレーニング
- 情報漏洩発生時の対応
- 情報のアクセス制限
- 情報を保管する金庫や扱うエリアの確保
- 情報システムのセキュリティ

※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

事業者

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！



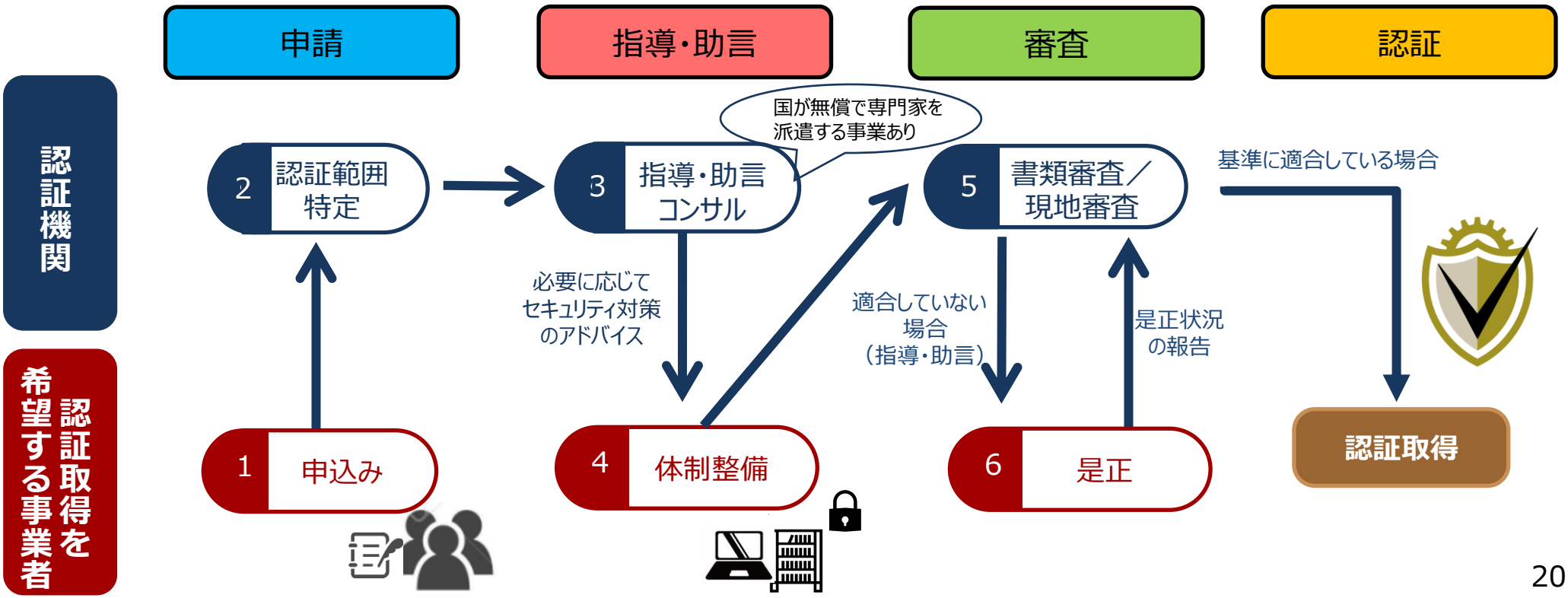
アクセスはこちら
https://www.youtube.com/watch?v=lPsdxU1jb2I

◆ 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

技術情報管理認証（TICS）取得プロセス

- 認証取得を希望する**事業者**は、認証機関に**審査を申込み**。必要に応じて認証機関の指導・助言を受け、**技術情報（研究成果など、技術に関する事業活動に有用な情報）のセキュリティ対策を整備、実施**。
- **認証機関**は、**必要に応じて指導・助言**しつつ、事業者の情報セキュリティ対策が**国が定めた基準を満たしているかを審査**し、適合していれば認証。
- 申込～認証取得まで早い場合で**１～２ヶ月**。



認証機関の認定状況

- **認証機関として８機関**を認定。

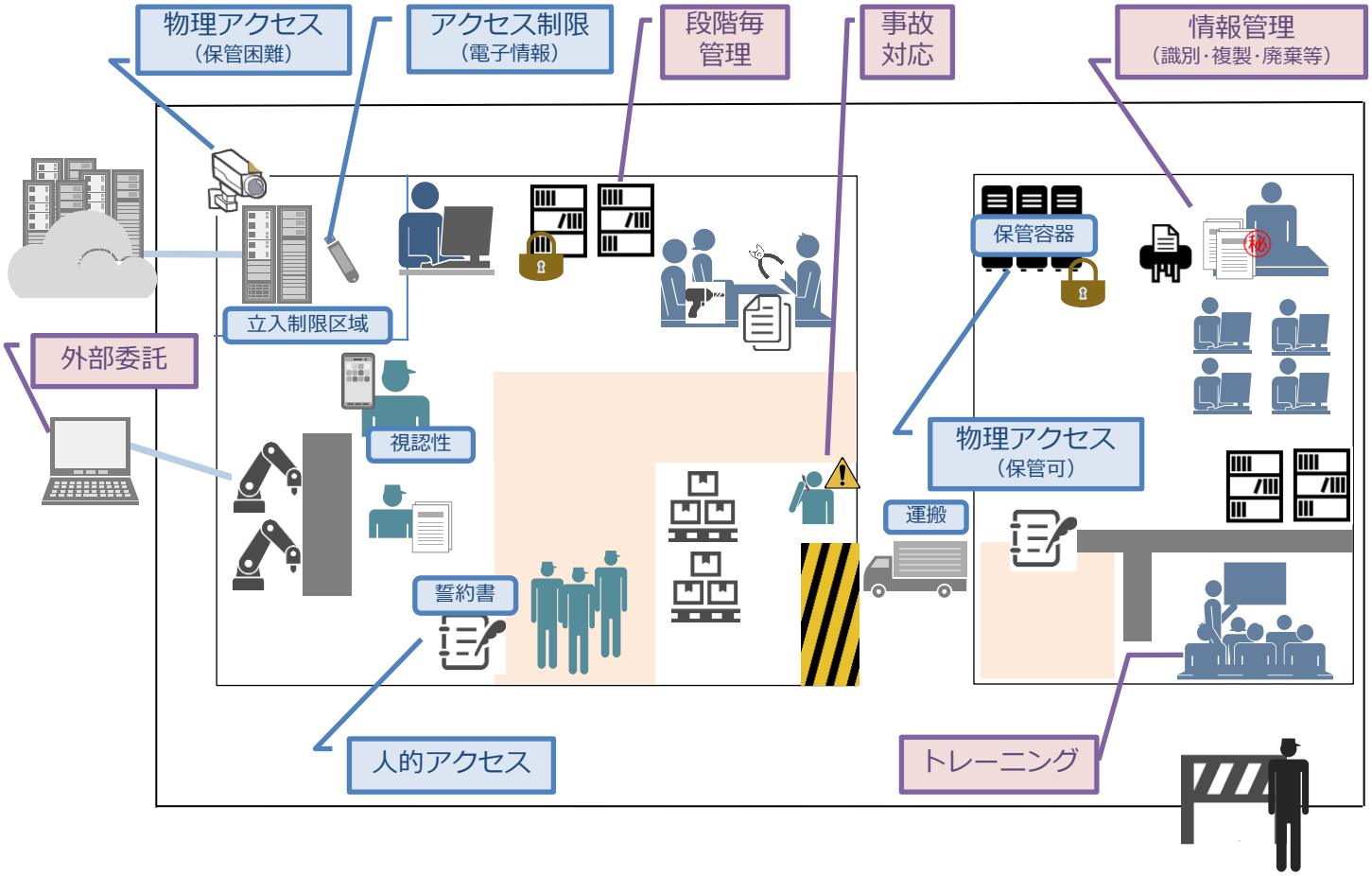
＜認定済みの認証機関＞ ※令和7年9月30日現在

機関名	連絡先	業務の範囲
（一財）日本品質保証機構	03-4560-5700	全て
（株）日本環境認証機構	03-5572-1745	全て
（公財）防衛基盤整備協会	03-3358-8704	電気機械器具製造業、情報通信機械器具製造業及び輸送用機械器具製造業のうち航空、 宇宙及び防衛分野に係るもの
（一社）情報セキュリティ関西研究所	06-6136-3925	全て
（一社）日本金型工業会	03-5816-5911	製造業
（一社）日本金属プレス工業協会	03-3433-3730	全て
ライド（株）	03-3237-1173	中小企業者
日本検査キューエイ（株）	03-5542-2752	全て

最新の認証機関情報は認証制度ホームページをご覧ください：
https://www.meti.go.jp/policy/mono_info_service/mono/technology_management/index.html

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）情報セキュリティに関する類似の認証制度との比較

- 国際標準に基づくISMS適合性評価などの類似制度も含め、**各社で求められる取組水準やリソースも踏まえ、最適な対応をご検討ください**。
- 認証を取得せず、自社内で取り組む場合も、**一度は第三者による監査、コンサルティングを受けることを推奨**します。

	TICS	ISMS適合性評価
制度の根拠	産業競争力強化法	ISO／IEC　27001（国際標準）
認証制度 運用主体	国（経済産業省、関係省庁）	基準策定：国際認証フォーラム 国内認証機関認定： (一社)情報マネジメントシステム認定センター・(公財)日本適合性認定協会
特長	● 法律に基づく唯一の認証制度 ● 認証機関が指導・助言を実施 ● 一部の補助金等で優遇	● 国際標準に基づく信頼性 ● 認証取得に向けたコンサルが充実 ● 海外企業にアピールしやすい
評価対象となる事項	技術情報の管理方法	情報セキュリティマネジメントシステム
主な対象企業	全ての法人 （中小企業・製造業系企業が多い）	全ての法人 （大企業・IT関連企業が多い）
認証取得までの期間	１カ月程度～	１２カ月程度～
継続コスト	３年ごとに更新審査 １年ごとに定期報告	３年ごとに更新審査 １年ごとに維持審査

技術情報管理認証（TICS）を取得した事業者の声

- 技術情報管理認証を取得した事業者の多くが、**技術情報の管理体制が整備できていることを取引先に示すことができる**ことに加え、**社内の情報セキュリティ意識の向上**につながることから認証取得の重要性・意義を強調。

認証取得による効果（認証取得事業者ヒアリング結果）

- 情報セキュリティに関する**取引先の要望に対応**できるようになった
- 取引先の情報、自社の技術情報の管理に対して**従業員の意識が向上**した
- **経済産業省のWEBページに社名**が掲載され、士気が上がった
- 営業部門が**名刺の認証マークを見せて取引先に説明**すると、納得を得られやすい
- 情報セキュリティに関する**取引先のヒアリングで合格**の評価を得られた
- 情報セキュリティの取組を**対外的にアピール**できるようになった

株式会社山本金属製作所

高度なものづくりを支援する事業を行っており、お客様のビジネスに関わる情報を扱うにあたり、情報管理は非常に重要と考える。認証取得は、リテラシーの底上げにも効果的であり、今後も、生産性を阻害することなく、自社の強みを活かした情報管理の仕組みを構築していきたい。

日本金型工業会（株式会社小出製作所）

認証取得をきっかけに、情報管理の取組の一歩を進められた意義は大きい。業界として認証に一足早く取り組むことで、社員1人1人が情報を守る意識を高めていき、近い将来、お客様から情報管理を求められた時にも、その期待に十分に応えていきたい。

「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

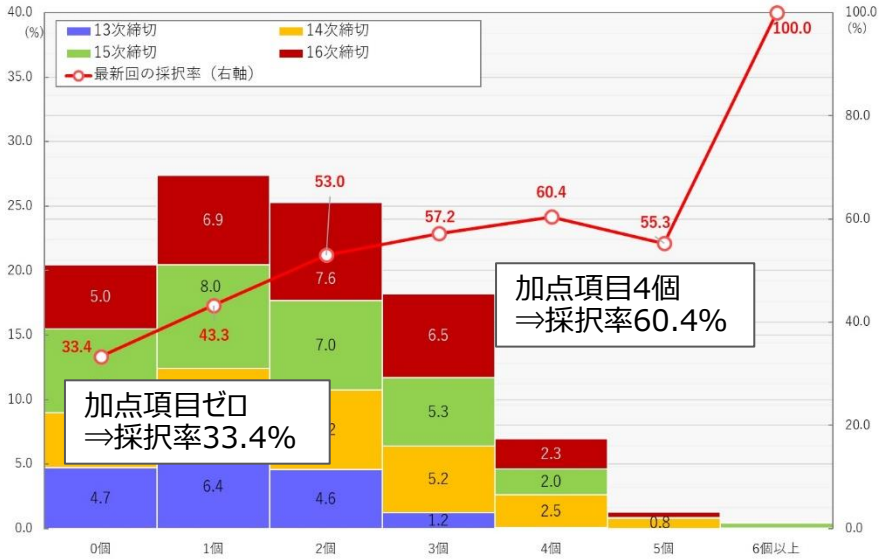
※特例措置として、大幅な賃上げに取り組む事業者には、補助上限額を100～1,000万円上乗せ。最低賃金の引き上げに取り組む事業者は、補助率を2/3に引上げ。

「ものづくり補助金」の採択審査時の優遇（加点の効果）

- ものづくり補助金の**採択率は５割前後**で推移（令和3年度）。
- **加点項目が１点増えるごとに採択率が１０%程度向上**。

採択率の推移

加点項目数と採択率の関係



技術情報管理認証以外の加点項目

- 有効な期間の経営革新計画の承認
- パートナーシップ構築宣言
- 再生事業者
- DX認定
- 健康経営優良法人の認定
- J-Startup、J-Startup地域版の認定
- 賃上げ
- ワーク・ライフ・バランス等の推進の取組

ほか

※詳しい情報は最新の公募要領をご確認ください

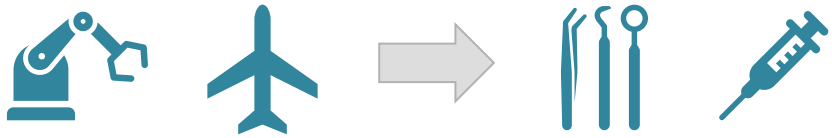
「中小企業新事業進出補助金」の優遇（令和7年度開始）

- 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	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） ※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
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



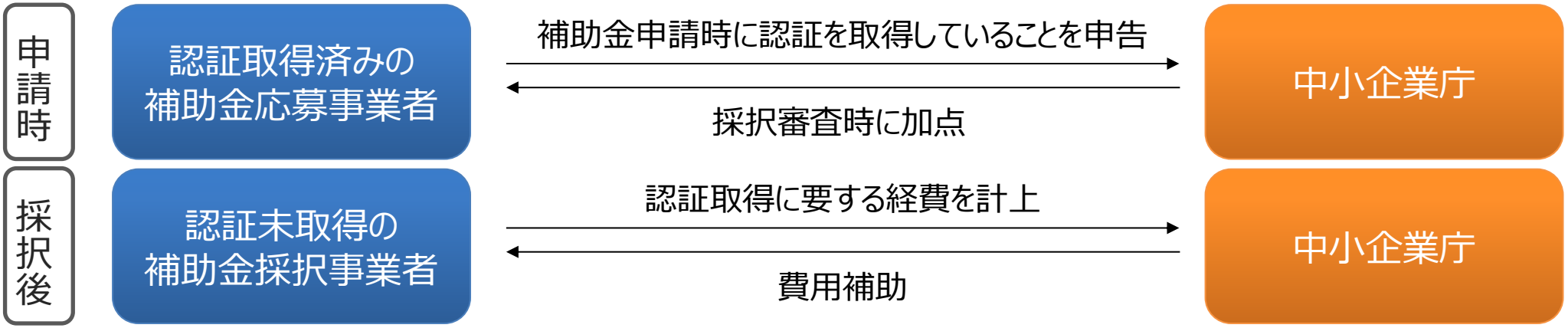
※詳しい情報は最新の公募要領をご確認ください
https://shinjigyou-shinshutsu.smrj.go.jp/

「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７５００万円　など）

- 中小企業者等が大学・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。



※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

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、ＩＴ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。**（無担保でも適用）** ※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

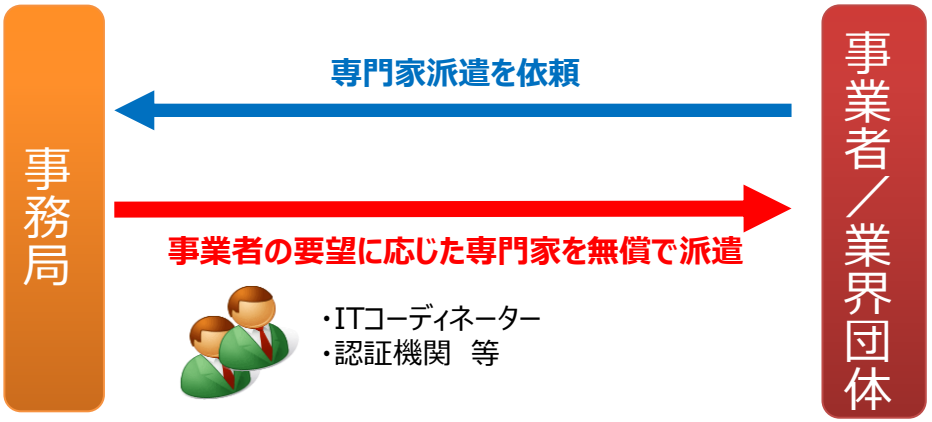
詳しい情報は日本政策金融公庫のHPをご確認ください。
https://www.jfc.go.jp/n/finance/search/11_itsikin_m_t.html

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**。

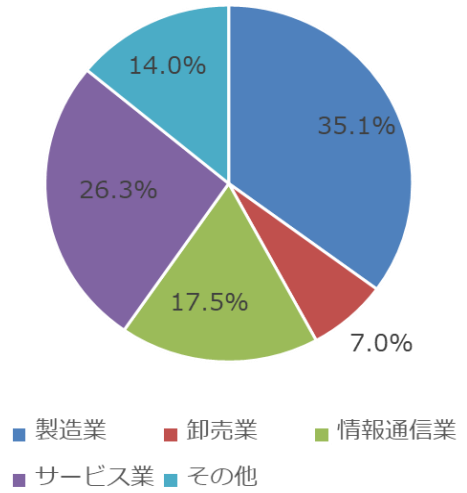
【2024年度利用実績：延べ90回】

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

技術情報管理 自己チェックリスト

- 技術情報管理認証の取得には第三者の審査が必要となるため、**「とりあえずやってみる」には、ハードルが高い**。
- このため、技術情報管理認証の**基準に沿って自組織の情報セキュリティ体制を確認**する自己チェックリストを公開。
- 自組織内で完結するため、**手軽に情報セキュリティのチェック**が可能。

項目ごとに自組織の対応状況を選択式でチェック！

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）

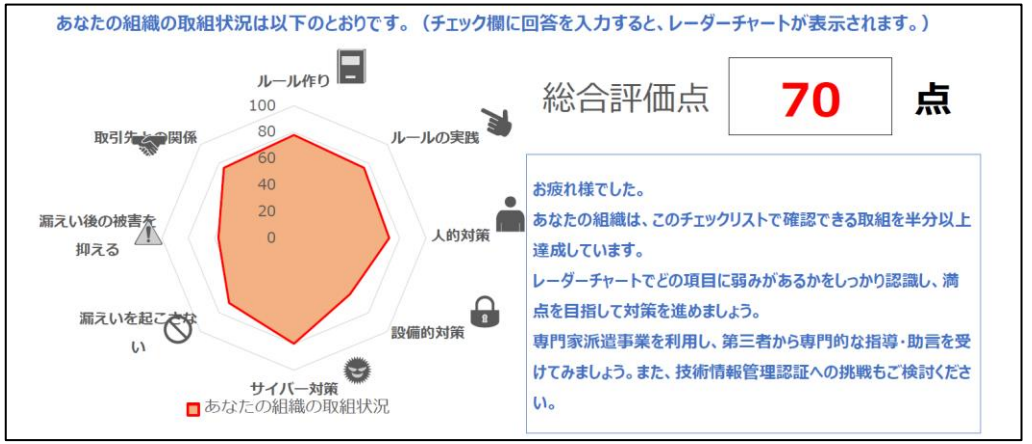
※「守るべき情報」とは？
・もし漏えいしたら自組織の競争力、信用などを大きく損なう可能性がある情報を示します。
・書類や電子ファイルだけではなく、試作品、製造装置など、あらゆる形態の情報が該当します。

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

	内容	チェック欄
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。	

自組織の得意分野・苦手分野を採点し レーダーチャートで表示



あなたの組織の取組状況は以下のとおりです。（チェック欄に回答を入力すると、レーダーチャートが表示されます。）

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

100　80　60　40　20　0

あなたの組織の取組状況

総合評価点　70　点

お疲れ様でした。
あなたの組織は、このチェックリストで確認できる取組を半分以上達成しています。
レーダーチャートでどの項目に弱みがあるかをしっかり認識し、満点を目指して対策を進めましょう。
専門家派遣事業を利用し、第三者から専門的な指導・助言を受けてみましょう。また、技術情報管理認証への挑戦もご検討ください。

「技術情報管理 自己チェックリスト」は
経済産業省ＷＥＢページからダウンロード可能
（企業名、担当者連絡先などの登録は一切不要）
https://www.meti.go.jp/policy/mono_info_service/mono/technology_management/pdf/checklist_kaitei.xlsx