

# 技術情報管理認証制度（TICS※）について

※Technology Information Control System

2026年2月

経済産業省

**1. 技術情報流出リスクの高まりと対策**

2. 技術情報管理認証制度（TICS）の概要

3. 技術情報管理認証（TICS）取得のメリット

（参考）技術情報管理 自己チェックリスト

# 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

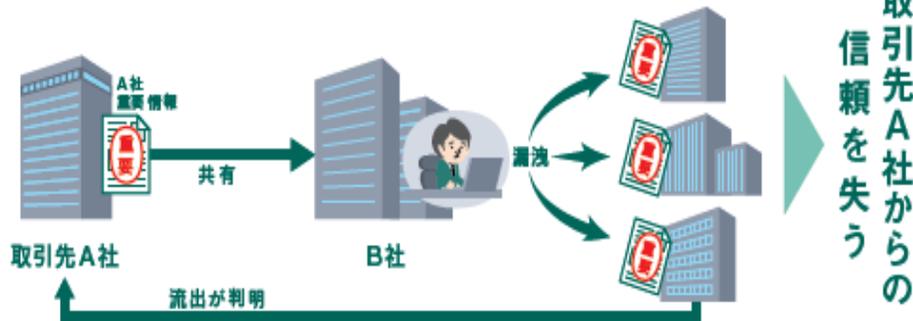
### ● 経済安全保障環境の変化

- 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＞



# 技術情報を狙う様々なアプローチ

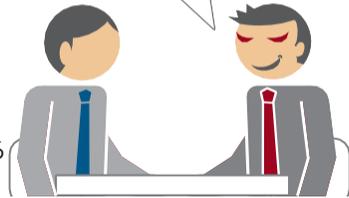
- 我が国企業が保有する優れた技術やデータは、常に悪意ある主体のターゲットとなることから、流出防止に向けてあらゆる対策を講じる必要。

## 人材リクルート

～技術に精通している従業員の引抜き～

弊社に来ませんか？  
今の2倍の収入を約束します

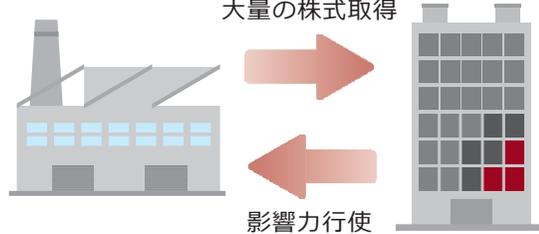
技術開発に  
携わっている  
従業員



## 投資・買収・合併

～影響力を行使して意思決定に関与～

株券  
大量の株式取得



## 不審なアプローチ

～従業員との1対1の関係構築～

今度外部で  
会いませんか？

出展企業の  
従業員

産業展示会会場



## 共同研究・事業

～技術・データの持ち出し～

一緒に  
頑張りましょう！

本当は…

技術・  
データ

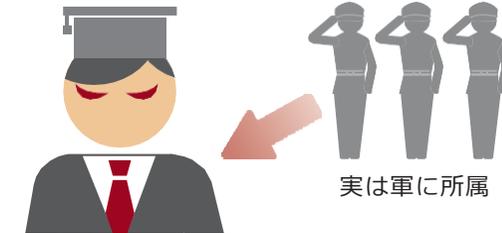


## 経歴偽装による在籍

～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

実は軍に所属



先端研究をしている  
大学・研究室等に応募

## サイバー攻撃

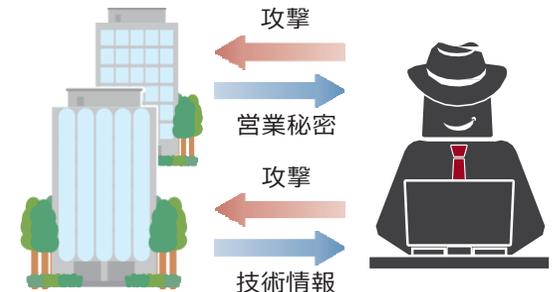
～企業や大学等が保有する秘密情報の窃取～

攻撃

営業秘密

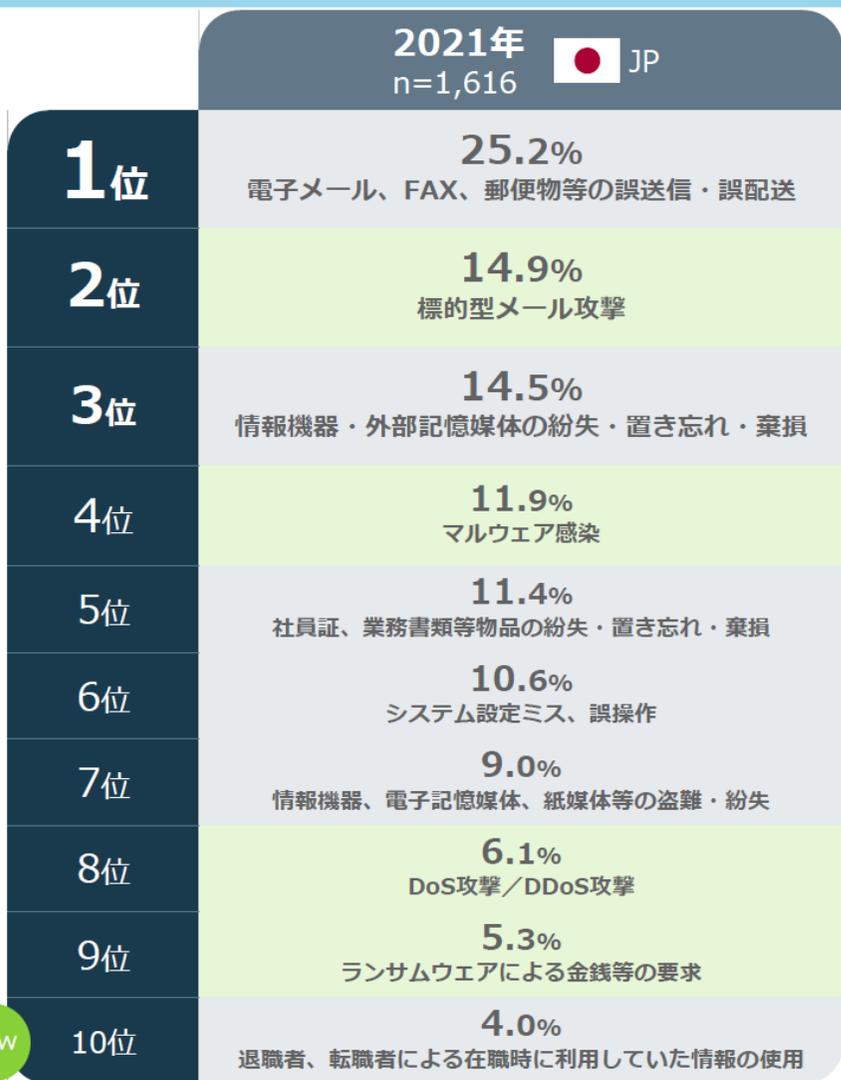
攻撃

技術情報



# 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經由した情報流出も発生。



## 【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。

new

# 報道された情報流出の事例

- 情報流出の事件・事故は後を絶たずに発生。

## 【大々的に報道された事例】

- 電機メーカーに対する**サイバー攻撃**により、防衛関連の情報が記録されたデータが約2万件（安全保障への影響を及ぼす可能性のあるデータ約60件）が流出した可能性がある（2019年）。
- 通信会社の元従業員が、**在日ロシア通商代表部・代表代理の要求**に応じ、会社のサーバーへ不正アクセスしデータを取得したとして、不正競争防止法違反の疑いで逮捕された（2020年）。
- 外国企業の従業員と**ビジネス用SNS**を通じて知り合い、自社の営業秘密を外国企業に流出され、不正競争防止法違反の疑いで逮捕された（2020年）。
- **国立研究開発法人の中国籍研究員**が中国にフッ素化合物に関する先端技術を漏洩して不正競争防止法違反の疑いで逮捕された（2023年）。
- Pマーク制度を運営する団体の審査員が**セキュリティ対策をしていなかった**ことで審査関連書類が漏洩した（2023年）。

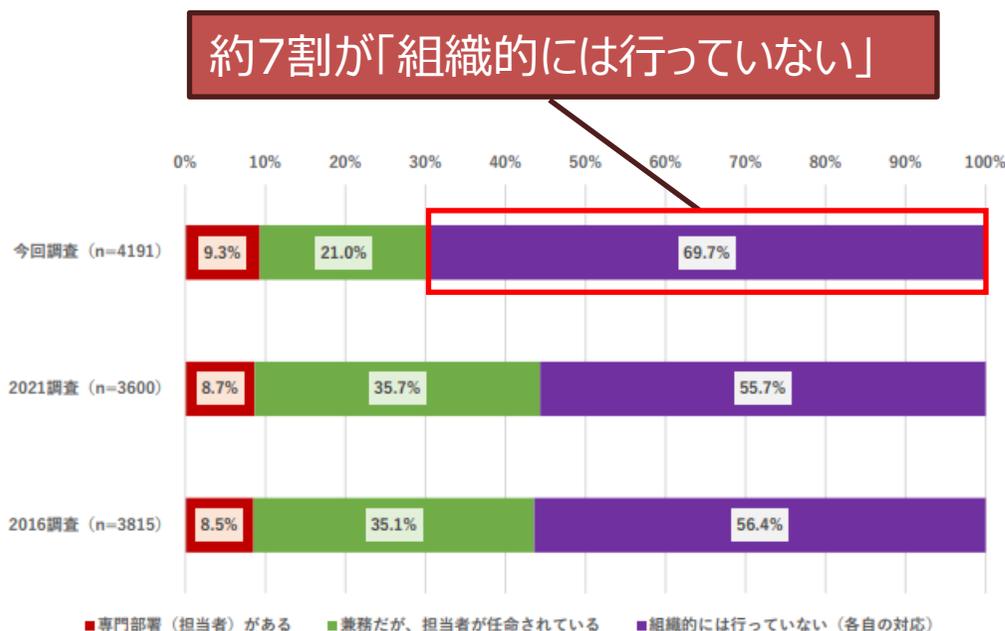
## 【中小企業等がターゲットになった事例】

- 徳島県の**町立病院**がランサムウェアの被害にあい、顧客情報約8.5万件が流出した（2021年）。
- **自動車部品メーカー**の社内システムに不正アクセスがあり、取引先の個人情報等が流出した（2023年）。

# 中小企業の情報セキュリティ対策状況

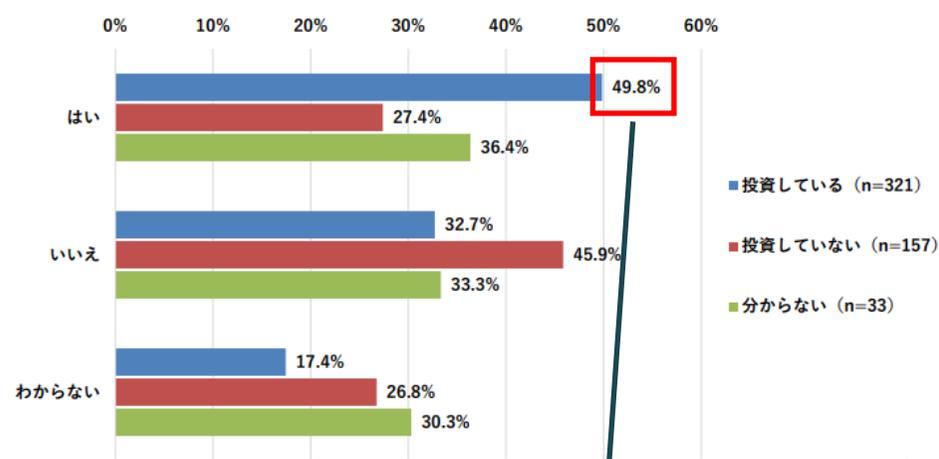
- 2024年度に実施された中小企業における情報セキュリティ対策に関する調査では、**約7割の企業で組織的なセキュリティ体制が整備されていない**ことが明らかになった。
- 一方で、**セキュリティ対策投資を行っている企業の約5割が、取引につながった**と回答。

## ◆ 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



## ◆ 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」

# 取引先への情報セキュリティの要求

- サプライチェーンの川下企業・業界団体による情報セキュリティの要求は強化される傾向。自工会・部工会をはじめ、業界ごとに情報セキュリティのガイドラインが整備されてきている。
- しかし、多くの業界団体のガイドラインは自己チェックであり、各企業がどこまで満たしているかは、必ずしも明らかでない。

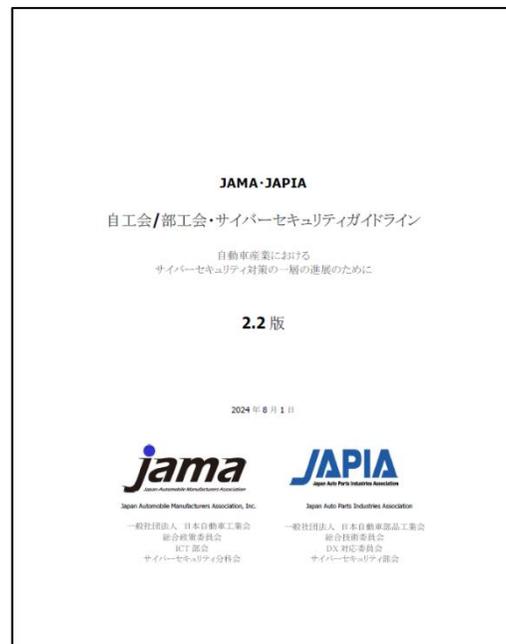
技術情報の提供を伴う発注をする際、  
・秘密保持契約の締結  
・情報セキュリティ体制の確認  
を依頼

自社

取引先

適切な情報セキュリティ体制を構築している  
ことを証明する必要

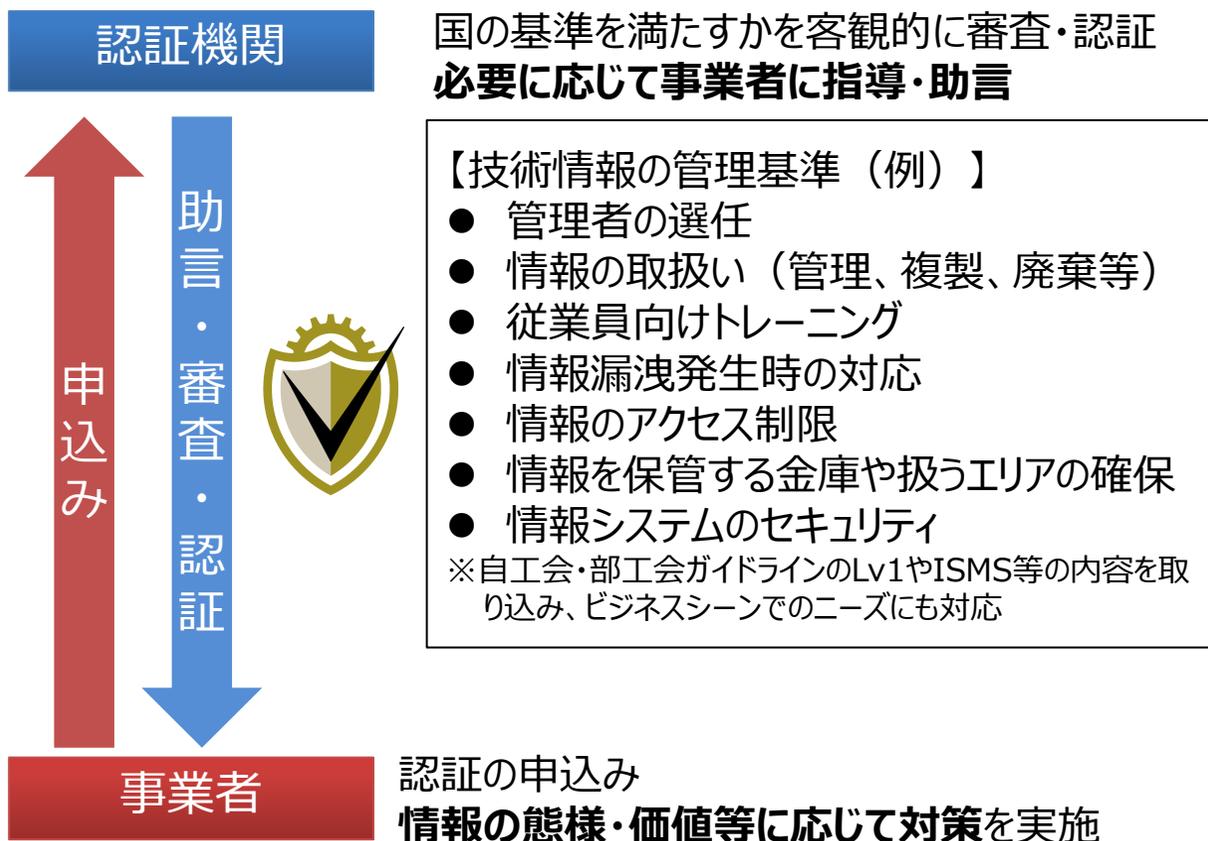
## 自工会/部工会サイバーセキュリティガイドライン



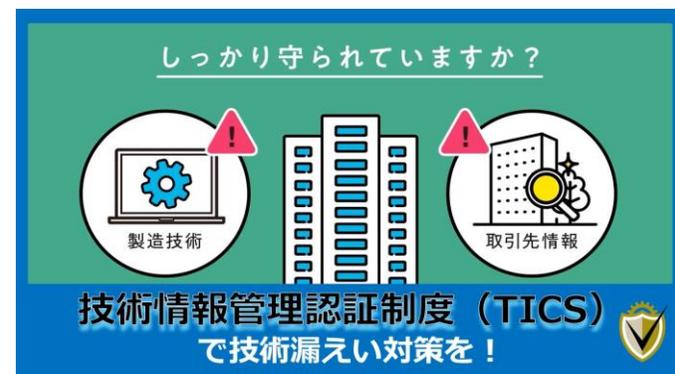
1. 技術情報流出リスクの高まりと対策
  - 2. 技術情報管理認証制度（TICS）の概要**
  3. 技術情報管理認証（TICS）取得のメリット
- （参考）技術情報管理 自己チェックリスト

# 技術情報管理認証制度（TICS）の概要

- 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。
- TICSは、産業競争力強化法に基づき政府が運用する制度。企業は認証機関の指導・助言を受けつつ、対策に取り組み、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。



- ◆ 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>



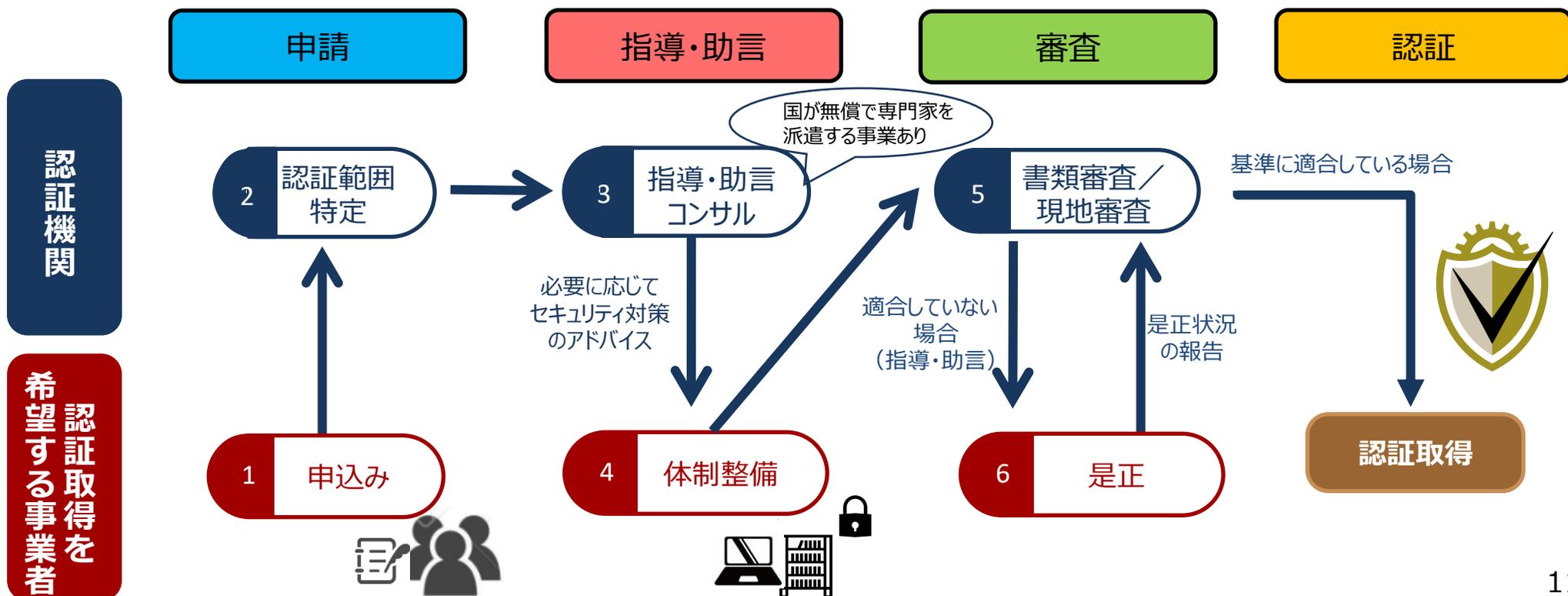
- ◆ 技術情報管理認証制度の詳細は ウェブページをご覧ください

[https://www.meti.go.jp/policy/mono\\_info\\_service/mono/technology\\_management/index.html](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**。

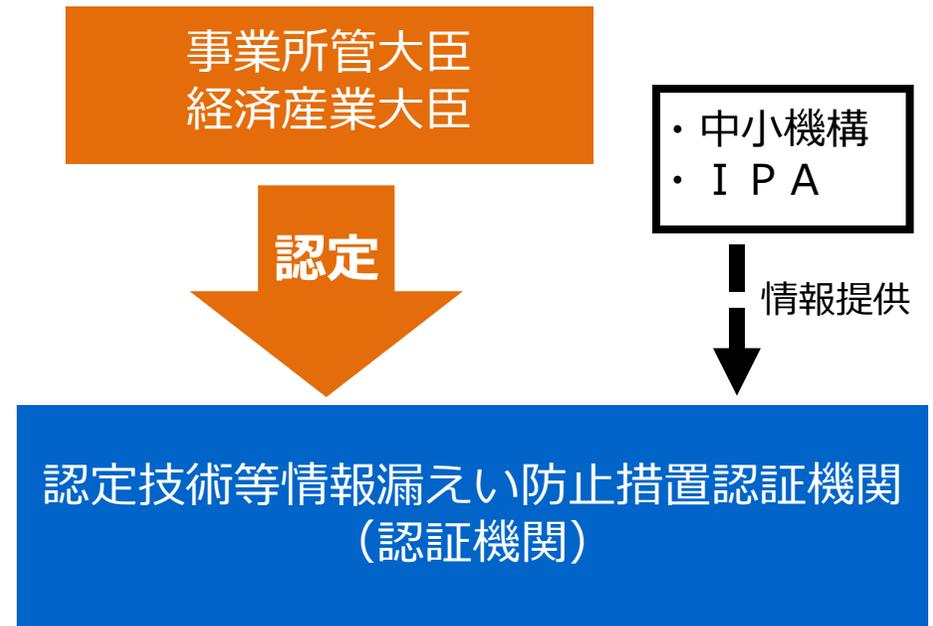


# 認証機関の認定

- 認証機関の業務を行う者は、認証業務の範囲等を記載・申請し、国の認定を受けなければならない。
- 申請を受けた国は、その申請内容が「技術等情報漏えい防止措置の実施の促進に関する指針（促進指針告示）」に適合しているかどうか、また「技術等情報漏えい防止措置認証業務の実施の方法（実施方法告示）」に即した認証業務を行えるかどうかを審査し認定を行う。

## 技術等情報漏えい防止措置の実施の促進に関する指針 (関係省庁共同告示)

- **基本的な方向**として、オープンイノベーション等の面からの **情報セキュリティの重要性等を示す**とともに、関係省庁ではWeb等での広報、説明会の開催に努める。
- **認定基準**となるべき事項として、認証業務の実施の方法を適確に実施できる **体制、経理的基礎**及び認証業務のリスクに備えるための保険等の対応を求める。
- **中小企業への配慮事項**として、**過度なコスト求めないこと**、中小企業認証取得の状況等の必要な情報を経産省が収集し、その評価結果に基づき、必要な対応を検討すること等を示す。



# 認証機関の認定状況

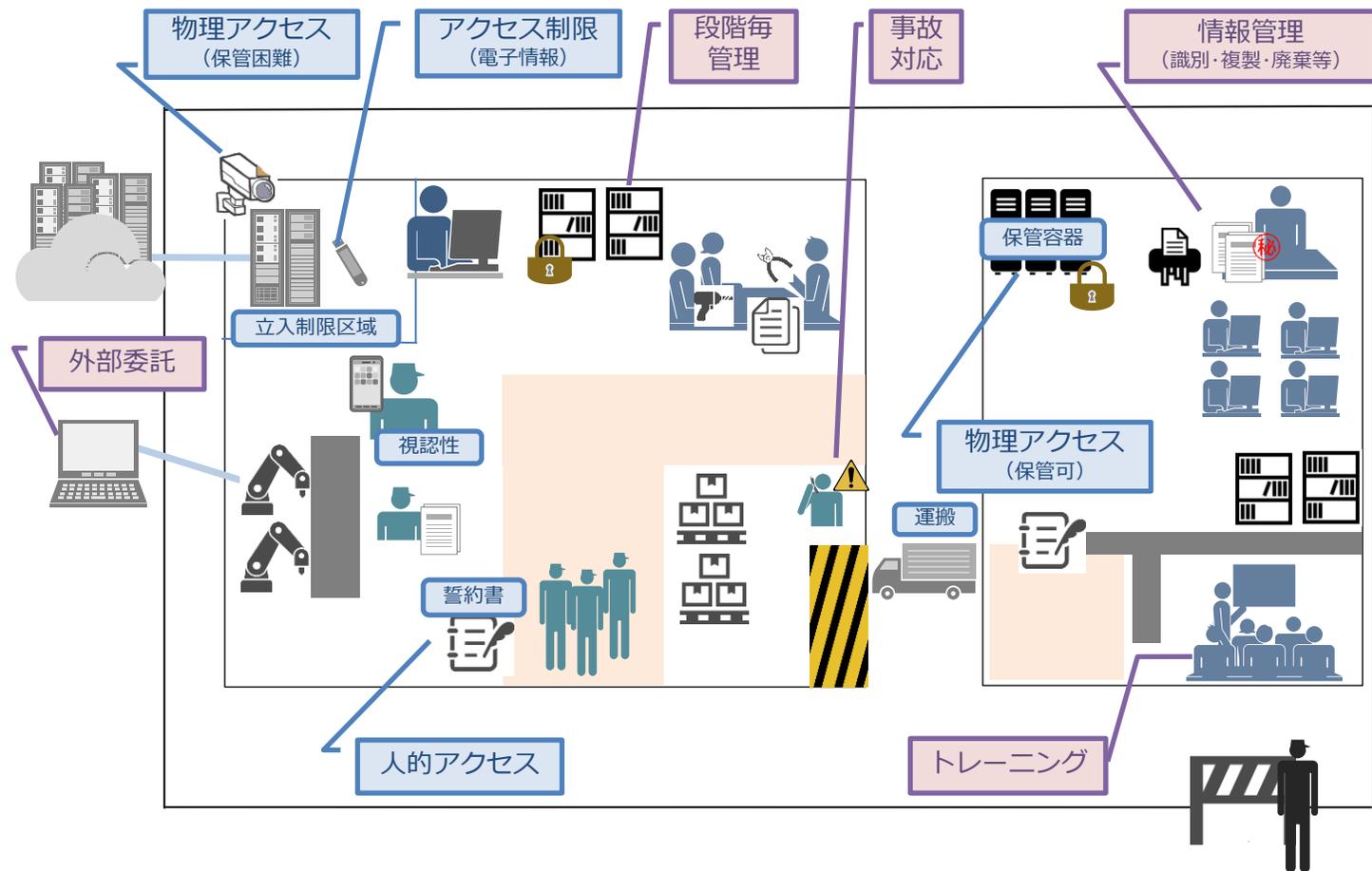
- 認証機関として7機関を認定。

<認定済みの認証機関> ※令和8年2月24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
(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

# 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	<ul style="list-style-type: none"> <li>● 法律に基づく唯一の認証制度</li> <li>● 認証機関が指導・助言を実施</li> <li>● 一部の補助金等で優遇</li> </ul>	<ul style="list-style-type: none"> <li>● 国際標準に基づく信頼性</li> <li>● 認証取得に向けたコンサルが充実</li> <li>● 海外企業にアピールしやすい</li> </ul>
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～	1 2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

# 認証基準の改正

- TICSは**2018年9月の施行から6年が経過**し、その間、テレワークの普及、サイバー犯罪の高度化、雇用の流動化など**社会情勢も変化**。
- これまでの基準は「複雑で難解」「最低限何を満たせばよいのか分かりにくい」など、**認証機関や事業者から改善を求める声**が上がっていた。
- そのため、以下の方針で認証を取得するための基準告示を改正（2024年8月16日施行）
  - 企業が具体的に**取り組む内容をわかりやすく**する
  - 業界団体の問題意識やニーズを踏まえ、**自工会/部工会ガイドラインのレベル1**の項目をカバー
  - 経済社会環境の変化に対応するために、**ISO27001の「検知・対応」**に関する項目を取り入れる
  - 現下のセキュリティに関する状況にそぐわない**数値要件を削除**する

## ★追加された項目の例

事故発生時の対応（ISOの「検知・対応」）、情報の機密区分の設定、社内教育の実施、外部情報システムの利用のルール、取引先との協力、情報システムの継続性の確保

## ★削除された項目の例

保管容器の仕様（材質、厚さ、耐火性等）、鍵の仕様（回転盤の目盛りの数等）、立入制限区域の施設の仕様（金網の設置、鉄格子の仕様、壁の厚さ・高さ等）、シュレッターの仕様（細断の細かさ等）

技術及びこれに関する研究開発の成果、生産方法その他の事業活動に有用な情報の漏えいを防止するために必要な措置に関する基準：[https://www.meti.go.jp/policy/mono\\_info\\_service/mono/technology\\_management/pdf/08.pdf](https://www.meti.go.jp/policy/mono_info_service/mono/technology_management/pdf/08.pdf)

1. 技術情報流出リスクの高まりと対策
  2. 技術情報管理認証制度（TICS）の概要
  - 3. 技術情報管理認証（TICS）取得のメリット**
- （参考）技術情報管理 自己チェックリスト

# 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步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、その期待に十分に答えていきたい。



# 「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
<b>製品・サービス高付加価値化枠</b> 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	
<b>グローバル枠</b> 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。

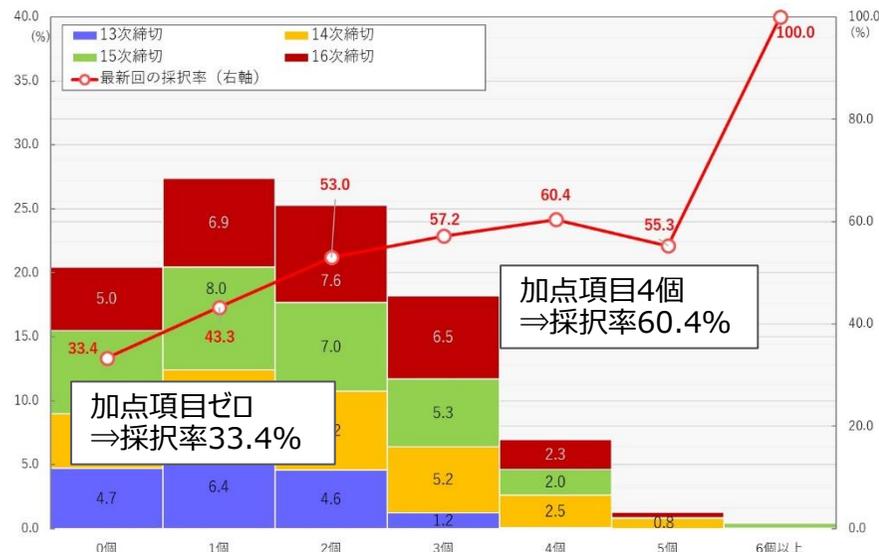
# 「ものづくり補助金」の採択審査時の優遇（加点の効果）

- 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）

# 「中小企業新事業進出補助金」の優遇（令和7年度開始）

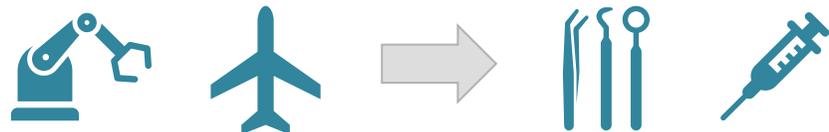
- 既存の事業とは異なる、新市場・高付加価値事業への進出にかかる設備投資等を支援
- 認証取得事業者は、採択審査時に加点が受けられる

## 現行の支援概要

項目	内容	
補助対象者	<b>企業の成長・拡大に向けた新規事業への挑戦</b> 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/>

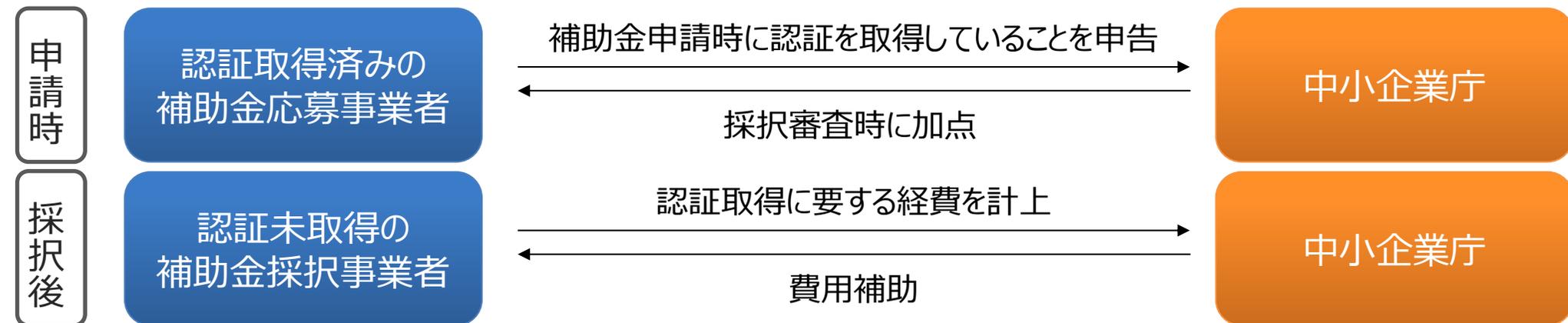
# 「Go-Tech事業」採択審査時の加点と認証取得経費補助

- 「**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/koukai/hojyokin/kobo/2026/260216001.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、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	<ol style="list-style-type: none"> <li>1. 電子計算機 (ソフトウェアを含む) ※</li> <li>2. 周辺装置 (モデムなどの通信装置など)</li> <li>3. 端末装置 (多機能情報端末など)</li> <li>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)</li> <li>5. 関連設備 (LANケーブルや電源設備など)</li> <li>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)</li> </ol> <p>※ 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</p>
利率	<p>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></p> <p>※令和7年4月時点の利率</p>
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](https://www.jfc.go.jp/n/finance/search/11_itsikin_m_t.html)

# 技術情報管理認証マークの活用

- 技術情報管理認証を取得した企業等は国が定めた認証マークを利用可能
- 認証マークはパンフレット、ウェブサイト、封筒、名刺などで表示可能

## 認証マークの表示ルール（抜粋）

### 認証マークの表示対象範囲

- 各社にて取得した認証マークは以下の媒体で表示可能。
  - ✓ 新聞、ポスター、パンフレット、カタログ、雑誌、看板、ウェブサイト 等のコミュニケーション媒体
  - ✓ 封筒、便箋、文房具、見積書、注文書、納品書、FAX 用紙 等の物品
  - ✓ 名刺、カレンダー 等の広告媒体
- 認証取得範囲の業務に関連しない内容のみを記載している媒体については表示不可。



# 経済産業省WEBページでの認証取得事業者紹介

- 認証取得事業者の対外発信の一助となるよう、掲載を希望する認証取得事業者については経済産業省WEBページで事業者名等を公開。

経済産業省  
Ministry of Economy, Trade and Industry

申請・お問合せ English サイトマップ 本文へ 文字サイズ変更 小 中 大 アクセシビリティ 閲覧支援ツール

ニュースリリース 会見・談話 審議会・研究会 統計 政策について 経済産業省について

ホーム ▶ 政策について ▶ 政策一覧 ▶ ものづくり/情報/流通・サービス ▶ 技術情報管理認証制度

## 技術情報管理認証制度

### 技術情報管理認証制度 認証取得事業者一覧

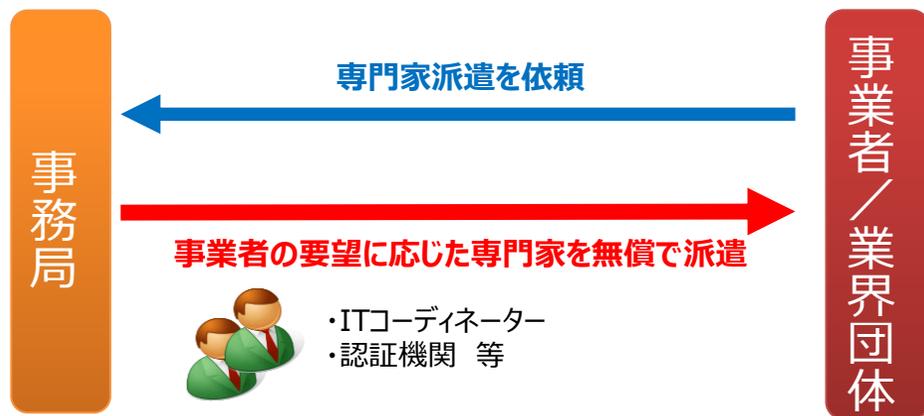
※認証取得事業者のうち、掲載に同意いただいた事業者のみを掲載しています。  
※事業者全体ではなく事業部等の単位で認証を取得している場合があります。

事業者の名称等	所在地	認証取得日
▶ <a href="#">株式会社アヤハエンジニアリング</a>	滋賀県東近江市	2021年 3月19日
▶ <a href="#">株式会社アサヒダイテック</a>	三重県員弁郡東員町	2021年 3月29日
▶ <a href="#">株式会社伊吹機械</a>	滋賀県長浜市	2021年 3月29日
▶ <a href="#">株式会社打田製作所</a>	茨城県稲敷郡阿見町	2021年 3月29日
▶ <a href="#">株式会社岡崎製作所</a>	福岡県北九州市	2021年 3月29日
▶ <a href="#">株式会社小出製作所</a>	静岡県磐田市	2021年 3月29日
▶ <a href="#">株式会社狭山金型製作所</a>	埼玉県入間市	2021年 3月29日
▶ <a href="#">昭和精工株式会社</a>	神奈川県横浜市	2021年 3月29日
▶ <a href="#">株式会社鈴木</a>	長野県須坂市	2021年 3月29日

# 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】

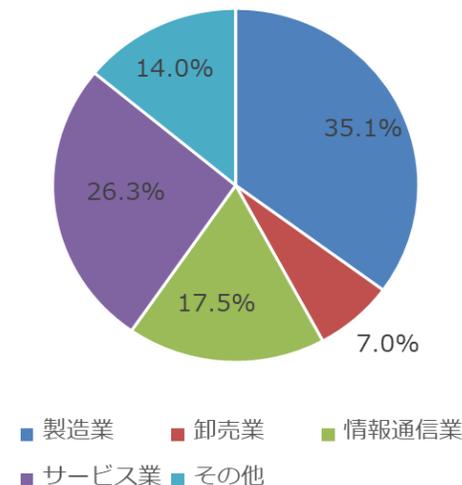
## 専門家派遣事業の流れ



<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日より開始いたしました。

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

1. 技術情報流出リスクの高まりと対策
2. 技術情報管理認証制度（TICS）の概要
3. 技術情報管理認証（TICS）取得のメリット

**（参考）技術情報管理 自己チェックリスト**

# 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！

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

## 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 : 取組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。



内容		チェック欄
<b>I 共通項目</b>		
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確保し、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。	

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。）



「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](https://www.meti.go.jp/policy/mono_info_service/mono/technology_management/pdf/checklist_kaitei.xlsx)



**技術情報管理認証制度（TICS）の詳細について  
ご質問などがあれば、以下の連絡先からご連絡ください。**

ご質問窓口：

経済産業省 貿易経済安全保障局

技術調査・流出対策室（認証制度担当窓口）

電話：03 - 3501 - 1511

MAIL：bzl-technology\_management@meti.go.jp

技術情報管理認証制度

検索

