

技術情報管理認証制度（TICS※）について

※Technology Information Control System

2024年

経済産業省 貿易経済安全保障局 技術調査室

1. 技術情報流出リスクの高まり

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
- ・ 経済安全保障上の課題への対応～ベストプラクティス集のご紹介～

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

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

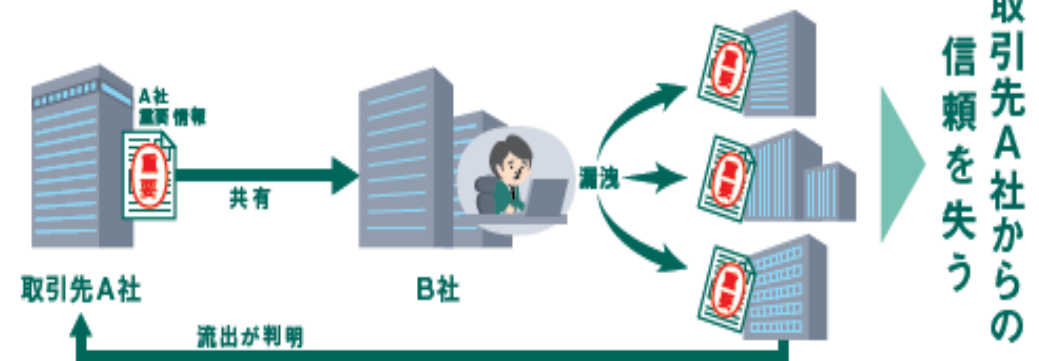
➤ 経済安全保障環境の変化

サイバー攻撃の巧妙化
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。

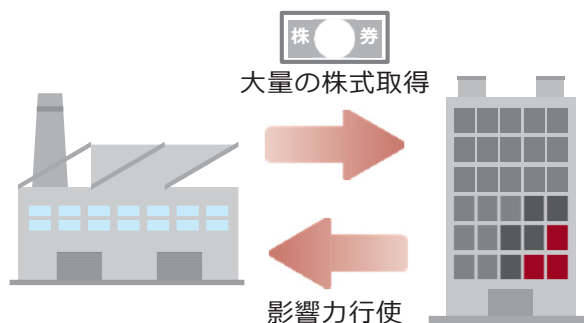
人材リクルート

～技術に精通している従業員の引抜き～



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

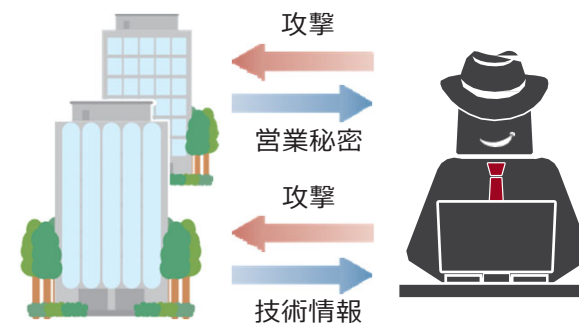
～留学生・研究者等の送り込み～

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～



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。

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）。

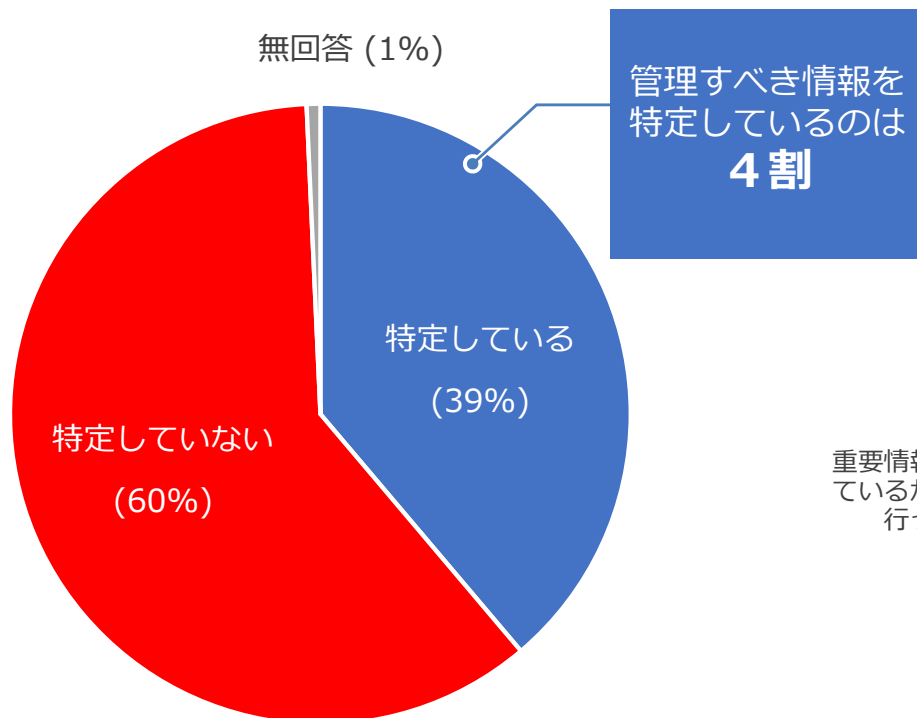
【中小企業等がターゲットになった事例】

- 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）。

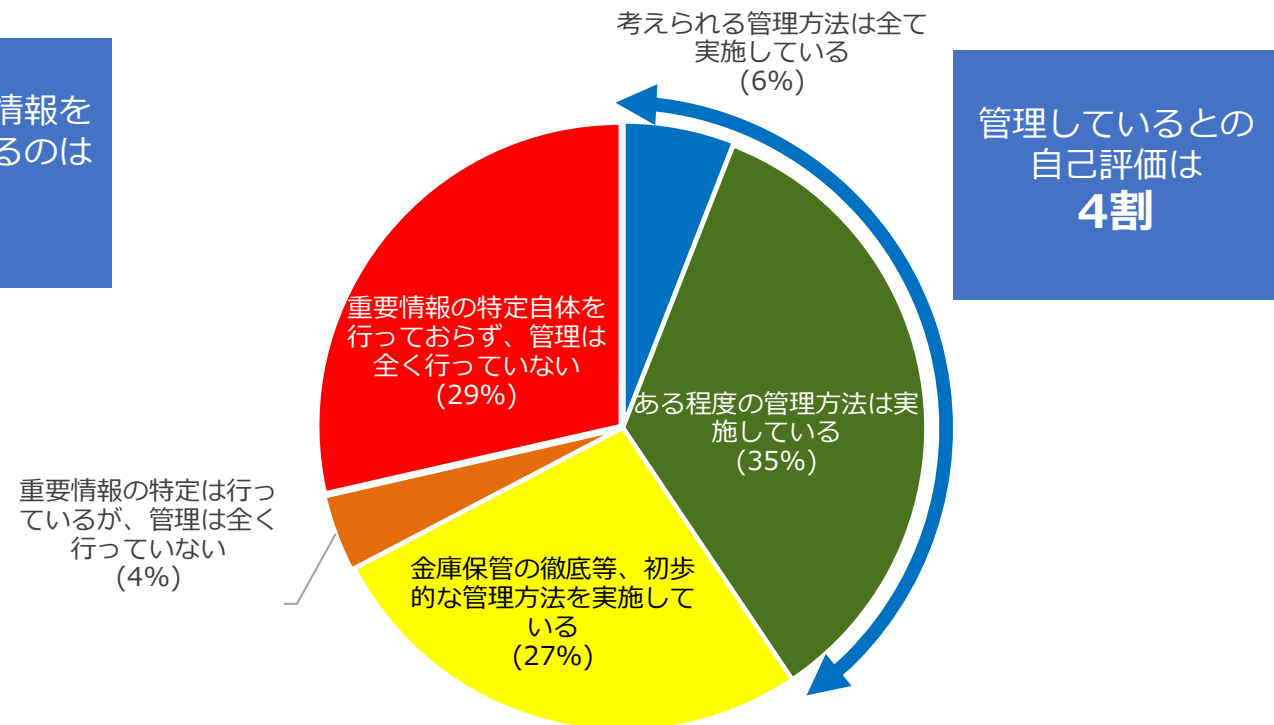
中小企業の情報セキュリティ対策状況

- 中小企業の約 6 割が管理すべき情報を特定していないなど、情報セキュリティの取組に遅れ。
- 個々の事業者がそれぞれの状況に応じて情報流出防止セキュリティ対策を適切に講ずることが重要。

<管理すべき情報の特定状況>



<情報セキュリティ自己評価>



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。

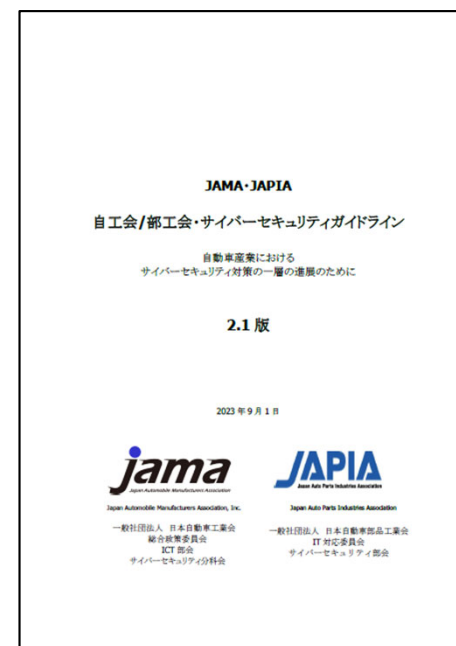
技術情報の提供を伴う発注をする際、
・秘密保持契約の締結
・情報セキュリティ体制の確認
を依頼

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

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）

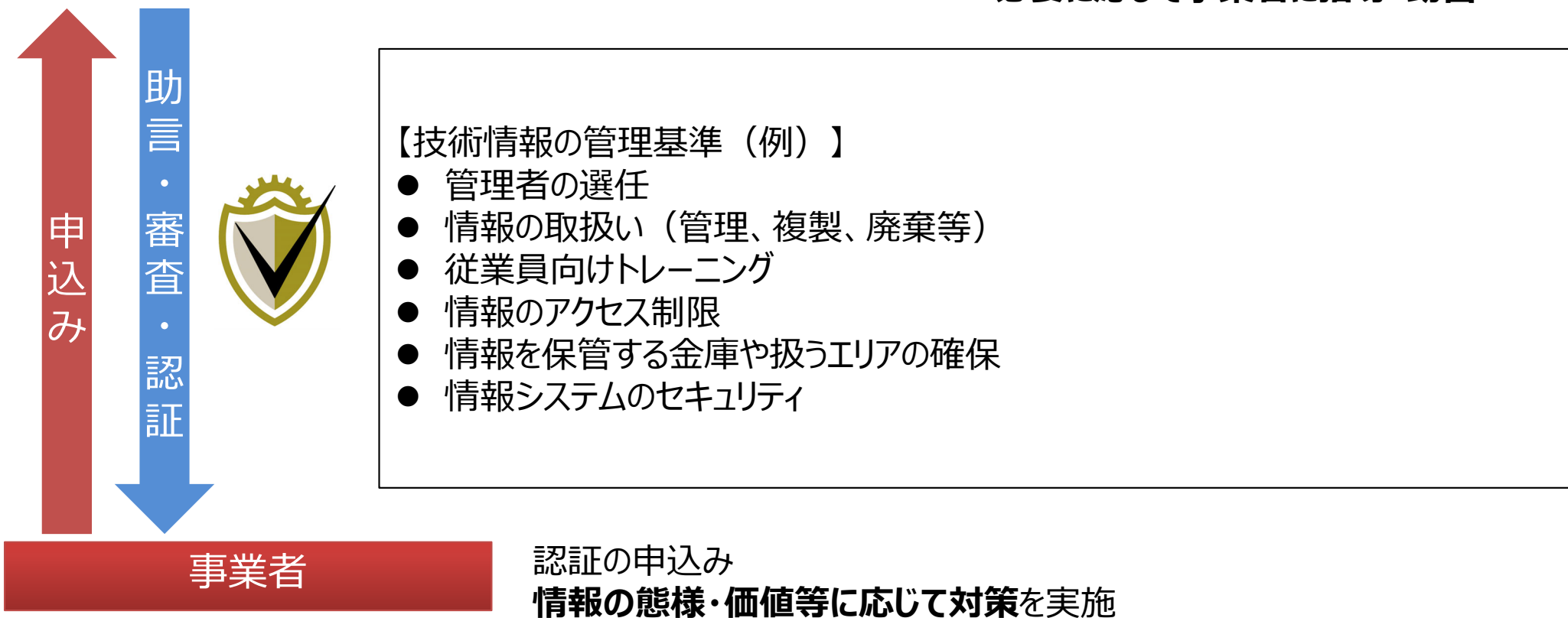
- ・ 技術情報管理 自己チェックリスト
- ・ 経済安全保障上の課題への対応～ベストプラクティス集のご紹介～

技術情報管理認証制度（TICS）の概要

- 国が認定した認証機関が、事業者の情報セキュリティ体制を客観的に審査・認証。（産業競争力強化法、2018年9月25日施行）
- 認証取得により、事業者は適切な情報セキュリティ体制について第三者が検証していることを示すことができ、取引先等の信頼獲得につなげることが可能。
- 中小企業の経営資源の状況等に配慮し、関係機関と連携する制度設計。

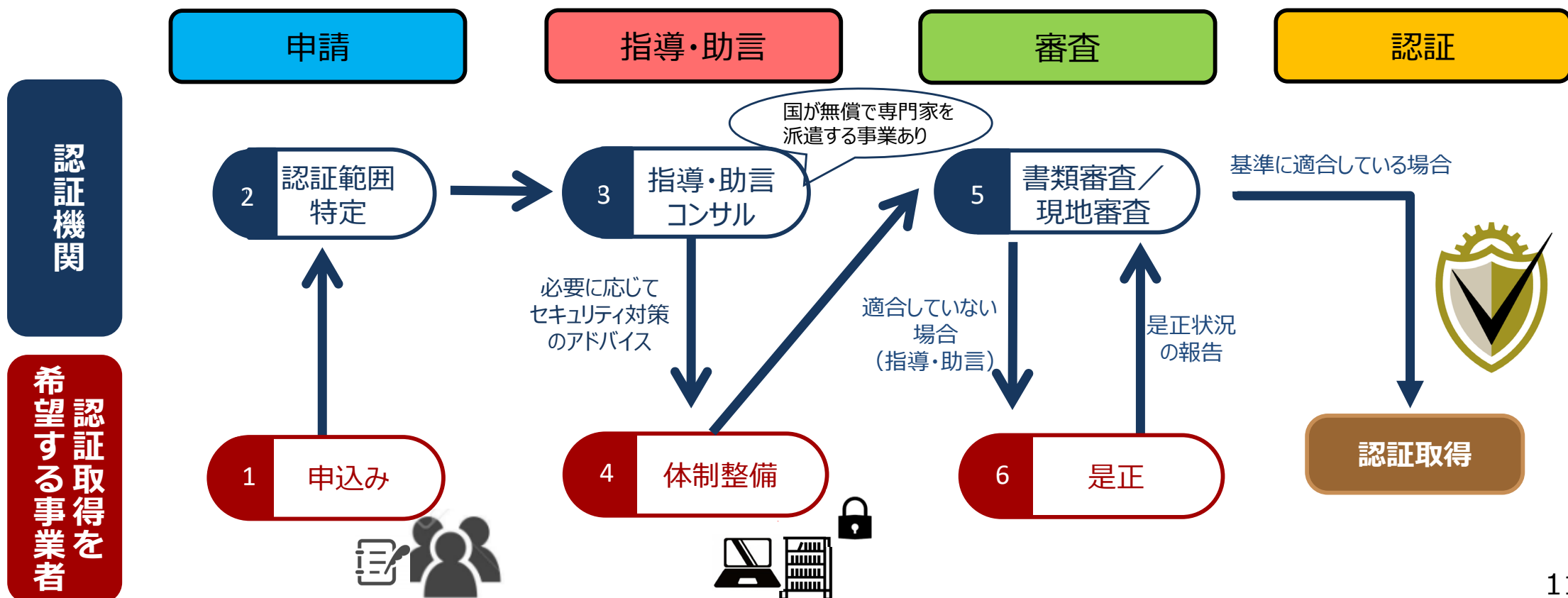
認証機関（認定技術等情報漏えい防止措置認証機関）

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



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**。

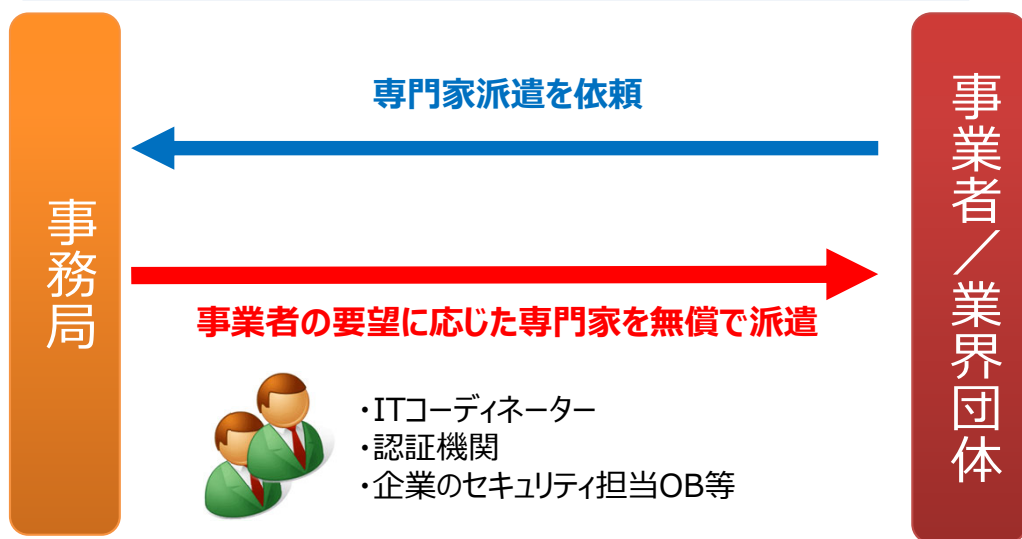


技術情報管理のための専門家派遣事業

- 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のアドバイスに加え、標準的な技術情報管理手法（モデル）の確立をサポート。

【2023年度利用実績：延べ87回】

専門家派遣事業の流れ

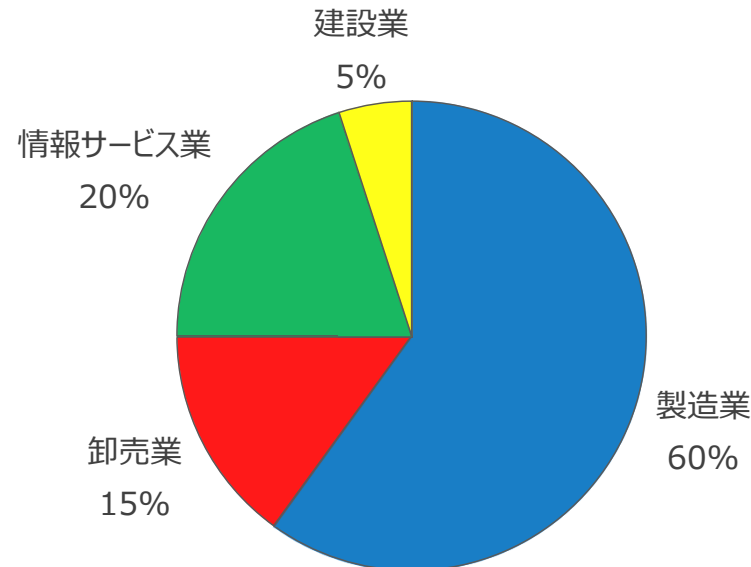


<支援内容例>

- (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
- (3) 業界毎のモデル確立支援

ほか

2023年度の派遣先事業者等の業種



認証機関の認定状況

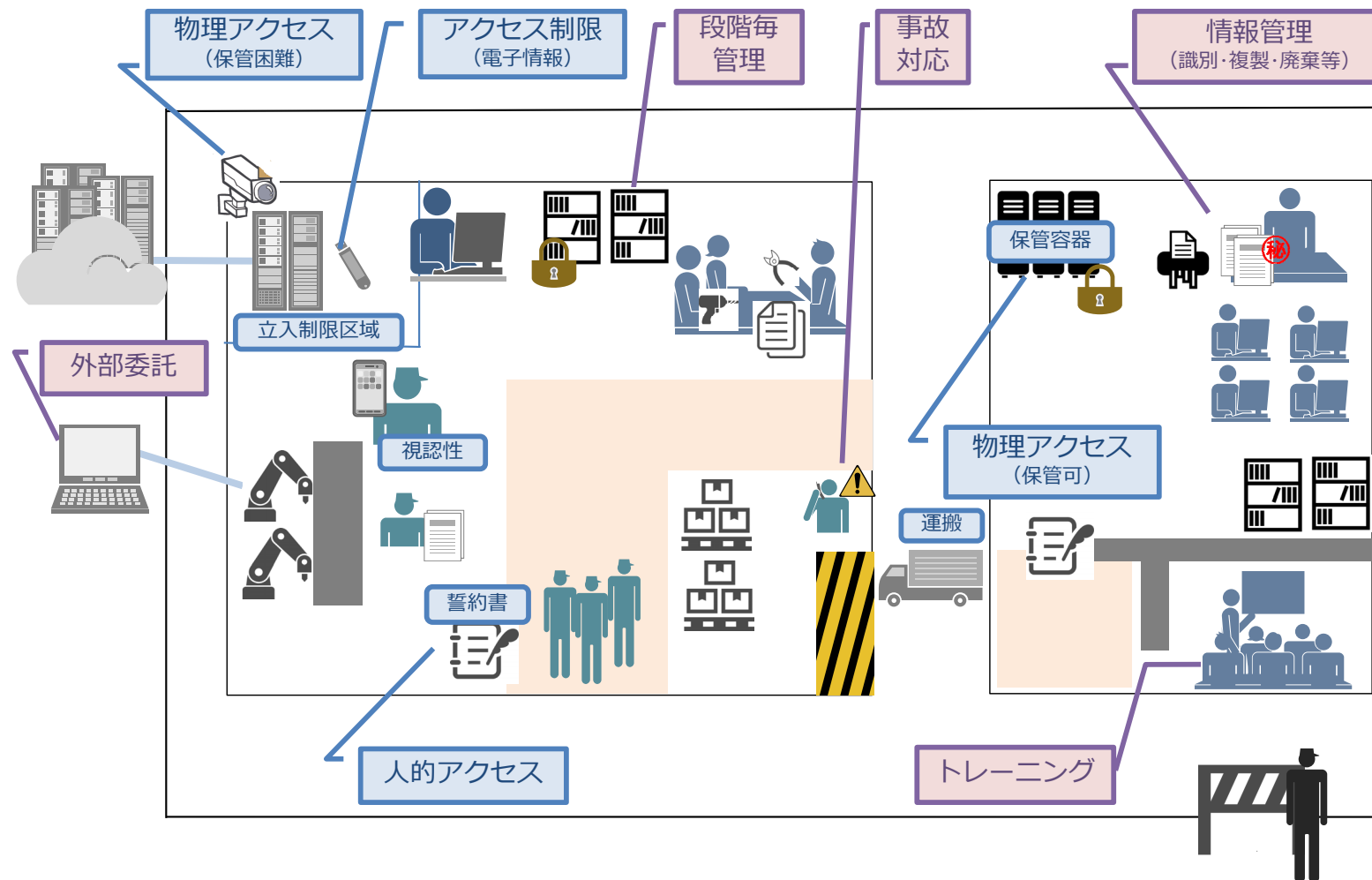
- 認証機関として8機関を認定。

＜認定済みの認証機関＞ ※認定日順

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
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
(一社) 日本金属プレス工業協会	03-3433-3730	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**。



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することに。
 - 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）、シュレッダーの仕様（細断の細かさ等）

(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。

	技術情報管理認証 (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～	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

1. 技術情報流出リスクの高まり

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
- ・ 経済安全保障上の課題への対応～ベストプラクティス集のご紹介～

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

- 中小企業等による新商品・サービス開発、生産プロセス改善のための設備投資等を補助する事業。
- 2023年度は3回の公募で、延べ約8000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

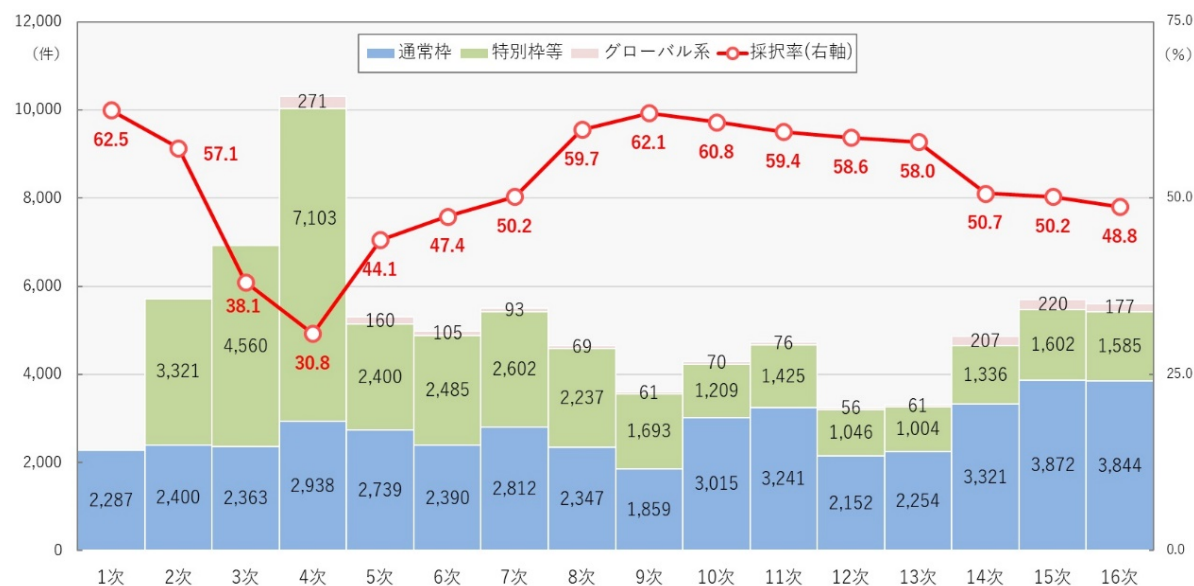
※詳しい情報は最新の公募要領をご確認ください

予算額	2,000億円の内数（2023年度補正）			
補助対象事業者	中小企業、個人事業主、企業組合、商工組合 等			
補助対象経費	機械装置・システム構築費、技術導入費、外部専門家経費 等			
補助上限額・補助率	申請類型		補助上限額	補助率
	一般型	通常枠	従業員 5人以下 ：750万円 6～20人 ：1,000万円 21人以上：1,250万円	1/2 (※小規模事業者・再生事業者は2/3)
		回復型賃上げ・雇用拡大枠 業況が厳しい事業者に対して、賃上げ・雇用拡大に取り組むための生産性向上を支援。		2/3
		デジタル枠 DXに資する革新的製品・サービス開発、デジタル技術を活用した生産プロセス改善等を支援。		
		グリーン枠 温室効果ガス排出削減に資する革新的製品・サービス開発、炭素生産性向上を伴う生産プロセス改善等を支援。		
	グローバル展開型 ①海外直接投資、②海外市場開拓、③インバウンド市場開拓、④海外事業者との共同事業のいずれかに合致するものを支援		3,000万円	1/2 (※小規模事業者・再生事業者は2/3)

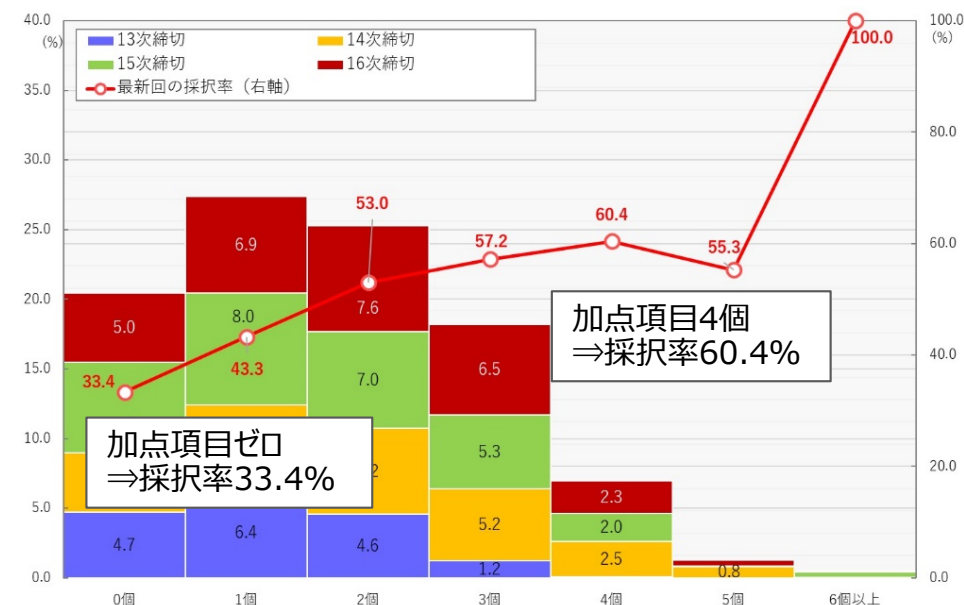
ものづくり補助金の採択審査時の優遇（加点の効果）

- ものづくり補助金の採択率は5割前後で推移（直近3回）。
- 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
- 創業・第二創業後5年以内
- パートナーシップ構築宣言
- 再生事業者
- 健康経営優良法人の認定
- J-Startup、J-Startup地域版の認定
- 事業継続力強化計画の認定
- 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

事業再構築補助金の採択審査時の優遇

- ポストコロナに対応した事業再構築をこれから行う事業者への支援を行う事業。
- 認証取得事業者は、成長分野進出枠（通常類型）、成長分野進出枠（GX進出類型）、サプライチェーン強靱化枠の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

予算額	既存基金の内数		
補助対象事業者	中小企業者等、中堅企業等		
補助対象経費	建物費、機械装置・システム構築費、技術導入費、外注費・専門家経費、広告宣伝費・販売促進費、研修費、廃業費等		
補助上限額・補助率	事業類型	補助上限額	補助率
	成長分野進出枠（通常類型）	3,000万円（※4,000万円） （一部廃業を伴う場合2,000万円上乗せ） ※短期に大規模な賃上げを行う場合	中小1/2（※2/3） 中堅1/3（※1/2） ※短期に大規模な賃上げを行う場合
	成長分野進出枠（GX進出類型）	中小：5,000万円（※6,000円） 中堅：1億円（※1.5億円） ※短期に大規模な賃上げを行う場合	中小1/2（※2/3） 中堅1/3（※1/2） ※短期に大規模な賃上げを行う場合
	コロナ回復加速化枠（通常類型）	2,000万円	中小2/3 中堅1/2
	コロナ回復加速化枠（最低賃金類型）	1,500万円	中小3/4（※2/3） 中堅2/3（※1/2） ※コロナで抱えた債務の借り換えを行っていない者の場合
	サプライチェーン強靱化枠	3億円（※5億円） ※建物費を含む場合	中小1/2 中堅1/3

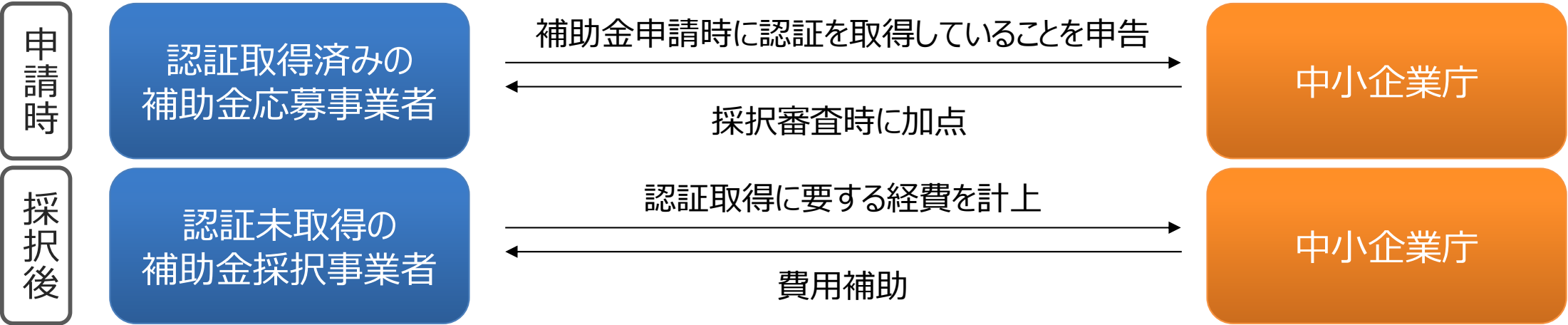
Go-Tech事業採択審査時の加点と認証取得経費補助

- 「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。

<https://www.chusho.meti.go.jp/keiei/sapoin/2023/230222kobo.html>



※詳しい情報は最新の公募要領をご確認ください

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5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

1. 技術情報流出リスクの高まり

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
- ・ 経済安全保障上の課題への対応～ベストプラクティス集のご紹介～

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

ファーストステップ[®]（経営の視点）

ファーストステップは、情報漏えいを防ぐための基礎的な確認事項です。

経営上も重要な情報漏えいを防ぐための取組の方針ですので、全ての事項を確認しましょう。



内容		チェック欄
ファーストステップ（経営視点からの基礎的な確認事項）		
1	経営者とともに、守るべき情報を特定している。 	☐
2	守るべき情報が、紙情報、電子情報、試作品・製造装置などの物自体のどれに当たるかを分け、保管場所を記録している。 	☐
3	守るべき情報には、一目ではかの情報と区別できるよう、目印をつけている。 	☐
4	取引先などから預けられた情報は、その取引先などの意向を聞いて、対策方法を定めている。 	☐
5	経営層が、以下の取組に責任を持つ管理者を定めている。 (1) 情報セキュリティのルールを作る。 (2) 情報に触れる従業員を制限・管理して、トレーニングする。 (3) 情報セキュリティのルールを実行する。 (4) 情報漏えいがあったときにどう対応するかを事前に確認し、漏えいがあったら対応する。 	☐

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。）



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）



経済安全保障上の課題への対応～ベストプラクティス集のご紹介～

- 経済産業省では、各企業が、経済安全保障上、どのような課題に直面しているかヒアリングを実施。その結果、多くの企業が「**技術流出**」や「**ビジネスの予見性低下**」を挙げ、**具体的な対応に苦慮**している現状が明らかに。
- そういった中でも、**自主的に様々な工夫を行っている企業が存在**。本資料は、こういった事例を**ベストプラクティス**としてまとめ、他の企業にも参考としてもらうことを狙いとしている。
- 今後の**追加・充実**のため、各社で取り組まれている事例があれば、**是非、共有いただきたい**。

ベストプラクティス事例	1-1	1-2	1-3	1-4	1-5	2-1	2-2	2-3	2-4
① 重点的に守るべき技術の特定	○		○	○					
② 従業員の情報管理意識の醸成	○								
③ 従業員の副業からの技術流出防止	○								
④ 重要な技術を持つ従業員の流出抑制	○								
⑤ 守るべき情報へのアクセス権の設定	○								
⑥ 原材料等のコードネーム化	○		○	○					
⑦ 従業員に対する重要技術の秘匿	○			○					
⑧ 重要なノウハウを持つ技術者の雇用延長		○							
⑨ 製造設備の調達先分散			○	○					
⑩ 取引先企業の情報管理			○	○					
⑪ 海外工場で扱う技術・工程の制限			○		○				
⑫ 自社ノウハウ類似技術の他社による特許化対策				○		○			
⑬ 海外での事業撤退時のノウハウを含む製造設備の廃棄				○					○
⑭ 経済安全保障の観点から経営判断する体制整備						○	○	○	○
⑮ サプライチェーン構造・原料調達先の可視化						○			
⑯ 調達先との資本関係形成による安定供給確保						○			
⑰ 調達先の多元化・安定化						○	○	○	
⑱ 軍事転用防止							○		
⑲ レピュテーションリスクへの対策							○		
⑳ 契約において盛り込むべき条項							○	○	○
㉑ 適切な契約期間の設定							○		○

※目次の1-1～2-4は、これまでのヒアリングで明らかになった課題のいずれに対応するものであるかを示している。

<ヒアリングで明らかになった課題>

①技術流出リスク

- 1-1. 人（現役従業員）
- 1-2. 人（退職者・OB）
- 1-3. 取引先からの要求
- 1-4. 共同事業等
- 1-5. 相手国の政策・制度

②ビジネス環境の予見性低下

- 2-1. 原料・部品の供給途絶
- 2-2. 諸外国の規制・政策
- 2-3. 紛争などによる経済活動混乱
- 2-4. 契約内容が不十分

**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、以下の連絡先にご連絡ください。**

経済産業省 貿易経済安全保障局

経済安全保障政策課 技術調査室（認証制度担当）

電話：03 - 3501 - 1511 (内線) 3267

MAIL：bzl-technology_management@meti.go.jp

技術情報管理認証制度

検索

