

技術等情報の管理に係る認証制度

令和元 9 月

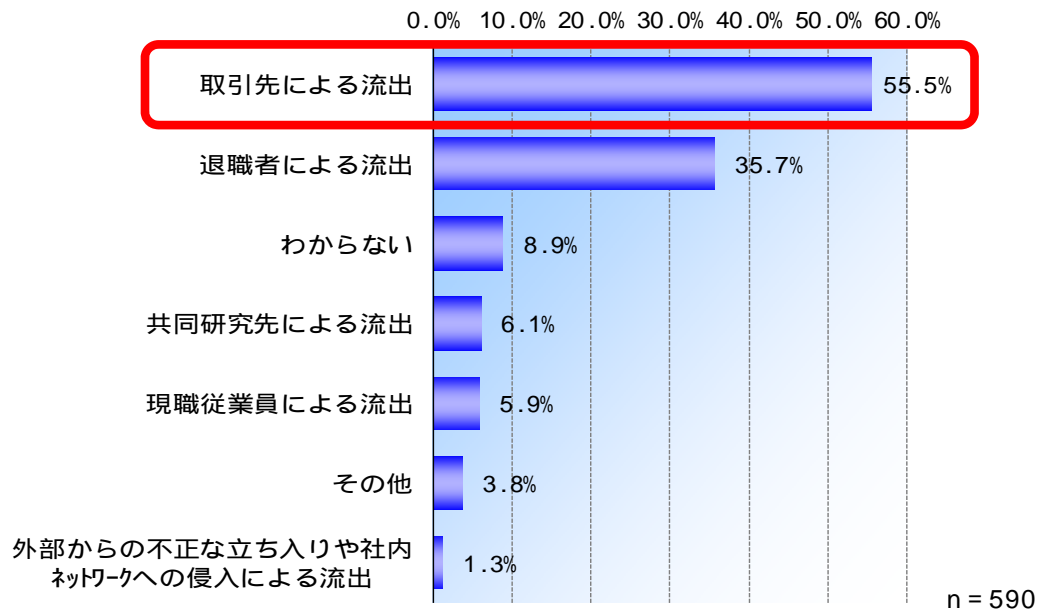
安全保障貿易管理課

1 . 企業における情報管理の現状

技術の流出経路・取引先への対策

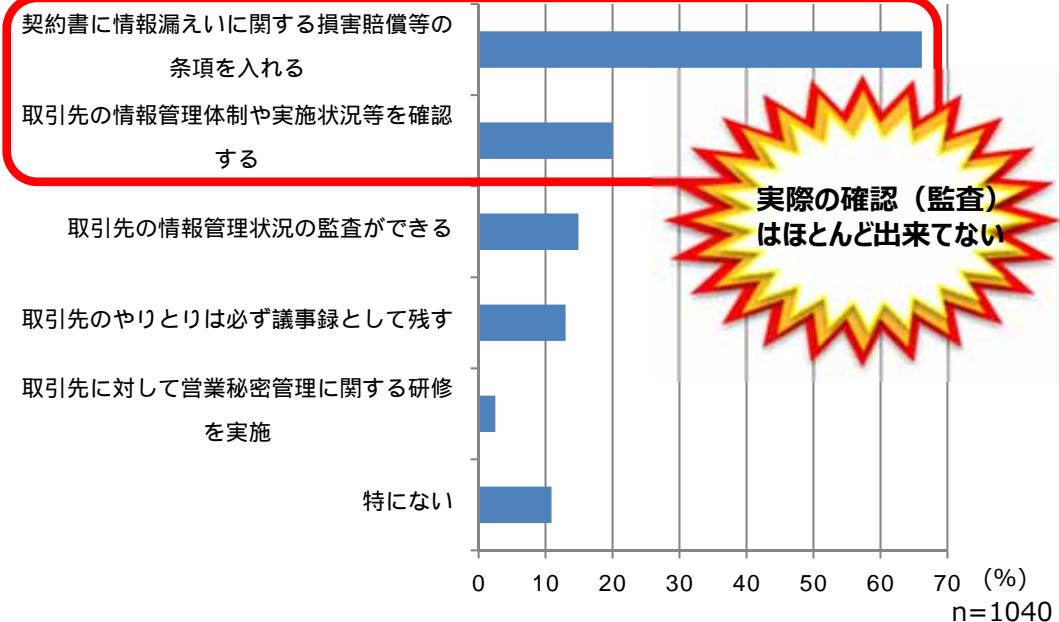
- 情報管理の現状について企業へのアンケート調査を実施したところ、「過去5年において技術が流出したと考える事例の流出経路」については「取引先による流出」が過半数を占めた（左図）。
- また「取引先に対する技術流出防止策」では、契約（秘密保持契約）の締結により担保している企業が60%以上、実際に取引先の情報管理体制等を確認している企業は、取引先の情報管理体制の確認にはコストがかかる、どのように確認をすればいいかわからない等の理由により、20%であった（右図）。

過去5年において技術が流出したと考える事例の流出経路



(出典) 経済産業省調べ (2018年12月)

取引先に対する技術流出対策

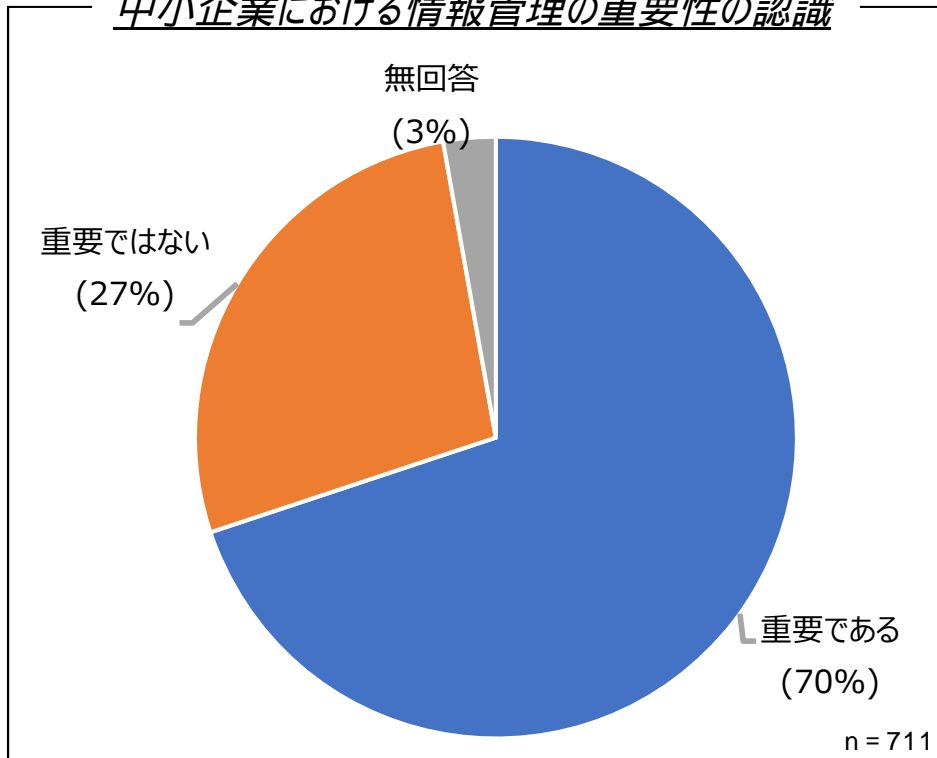


(出典) 経済産業省調べ (2018年12月)

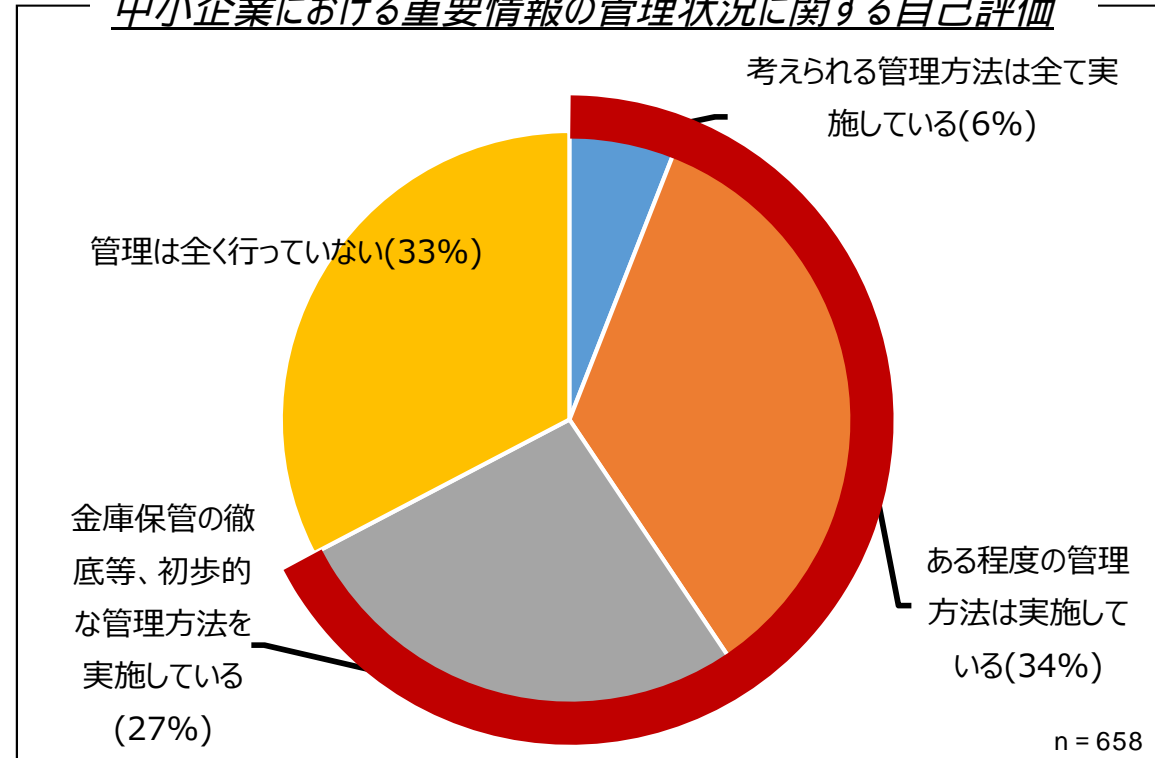
中小企業における情報管理の重要性の認識と対応状況

- 中小企業を対象に情報管理の重要性についてアンケート調査を実施したところ、情報管理が重要と認識する企業は70%を占める一方（左図）、情報管理の取組状況の自己評価結果は、管理を実施している企業が7割弱、また管理を全く行っていない企業は3割を超えた（右図）。
- 情報管理を行わない理由として、情報管理を実施するだけのリソースがない、どの情報が重要なのか分からない、重要情報をどのように管理すればいいか分からない等の意見があった。

中小企業における情報管理の重要性の認識



中小企業における重要情報の管理状況に関する自己評価



2 . 技術等情報の適切な管理に係る認証制度

技術等情報の適切な管理の促進に向けて

- 企業が保有する機微技術・情報（研究成果、事業活動に有用な情報等）について、国外への技術流出防止等、企業の適切な管理を担保するため、改正産業競争力強化法（平成30年5月成立）において技術等情報を適切に管理している企業を認証する制度を創設（平成30年9月25日施行）。
- 同制度は、企業の情報管理が国で示した「守り方」に即していれば、国が認定した「認定技術等情報漏えい防止措置認証機関（認証機関）」より認証を受けられる制度。

※日本検査キューエイ株式会社、一般財団法人日本品質保証機構を認証機関として認定（令和元年8月末時点）

事業所管大臣・経済産業大臣

国は、国が示す一定の方法（認証手法）により、認証業務を行うことができる体制を有しているか等を確認し、認定。

認定

- ➡国が認証機関をマネジメント（改善命令、認定取消等）
- ➡認定を受けた認証機関は国で公表

認定技術等情報漏えい防止措置認証機関（認証機関）

認証機関は、認証手法に従って、国が示す「守り方」（認証基準）に即して技術等の情報の管理が行われているかを確認し、認証。

認証

- ➡統一的な見方で、技術等の情報の管理の状況を評価
- ➡体制だけでなく、具体的な管理手法も評価

企業

- ➡企業は、大事な技術等の情報を特定、その情報の態様と価値等に応じて守り方を選択

技術等情報の適切な管理に係る認証制度（認証機関の認定）

- 産業競争力強化法第67条の定めにより、認定技術等情報漏えい防止措置認証業務を行う者は、事業所管大臣へ認証業務の範囲等を記載し申請し、認定を受けなければならない。
- 申請を受け付けた事業所管省庁は、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）」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」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

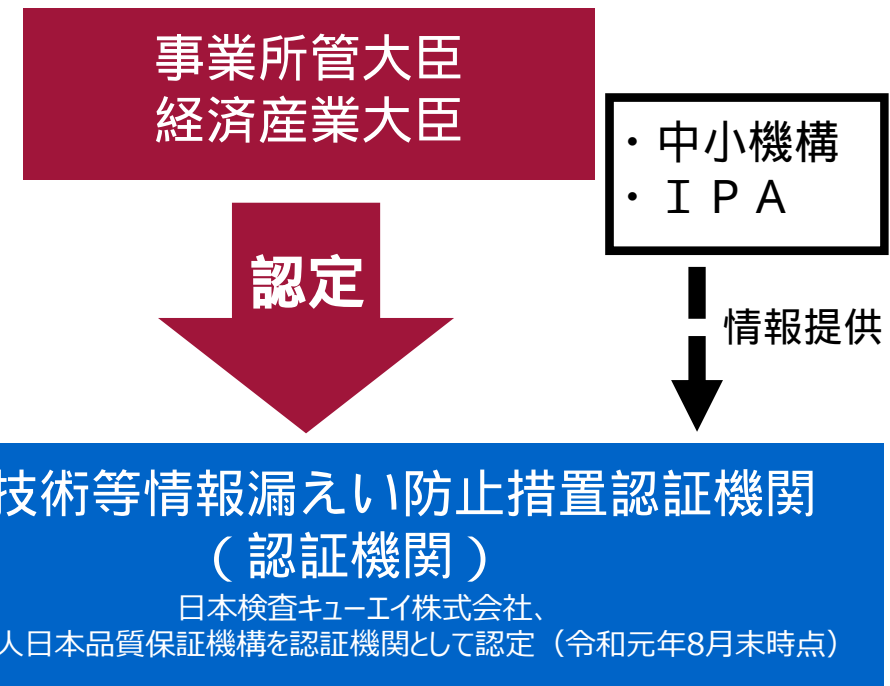
（関係省庁共同告示）

- **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管理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旨を定める。
- **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切に実施できる体制、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で収集し、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。

技術等情報漏えい防止措置認証業務の実施の方法

（関係省庁共同告示）

- **自己適合宣言確認型認証（シルバー認証）、現地審査を含む認証（ゴールド認証）の2段階の認証**の手法を定める。
- **公平な認証業務の実施**等を求める（認証機関の認定の国際基準とも整合性を確保。）。



技術等情報の適切な管理に係る認証制度（企業の認証）

- 技術等情報漏えい防止措置に係る認証を受けようとする企業は、自社で取り組む機微技術・情報（研究成果、事業活動に有用な情報等）の漏えい防止策等を踏まえ、認証機関に申請書を提出する。
- 認証機関は申請を受け、企業が取り組む機微技術・情報の漏えい防止策等が、国で示した守り方「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」に即しているかを審査し、認証を与える。
- 認証の種類は、最低限の管理を行っているかどうか書面で審査する「シルバー認証」と監査人による現地審査を含む「ゴールド認証」の2種類（2段階）。

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（関係省庁共同告示）

- **適切な管理をする必要がある技術等情報の見極め（特定）**をすること、**選択制の措置のうち必要な措置を決定すること、責任者を置くこと、情報へのアクセス管理の実施等を基礎的な事項**として定める。
- **具体的な措置**（保管容器や立入制限区域の物理的強度、警備体制等のソフト面での対応、情報システムのセキュリティの確保等）は**選択制**。
- **基礎的なレベルのものからハイレベルなものまでを列挙し、基準を参照しつつ、ステップアップをしていくことが可能なように設計**する。

認定技術等情報漏えい防止措置認証機関
（認証機関）

認証

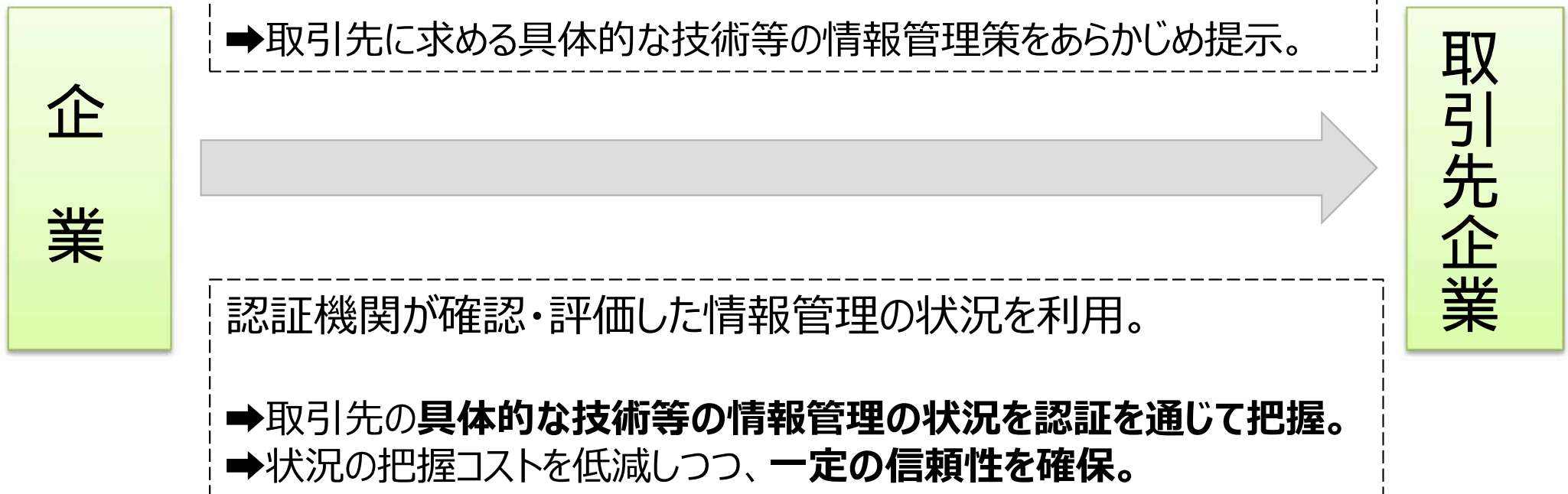
ITコーディネーター等

支援

事業者

技術等情報の管理の認証の活用に向けて

- 適切な管理を条件にビジネスパートナーに自社の大事な情報を渡す場合には、認証を活用し、具体的な情報管理の状況を知ってから渡すことが可能に。
- 企業は、実際の確認（監査）を行うことなく取引先の情報管理レベルを把握し、信頼性を確保できる。



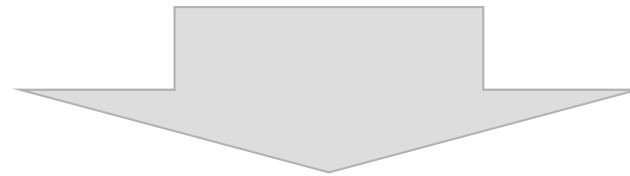
技術等情報の管理の流れ

①守るべき技術等の情報※を特定する

自らが保有している情報、他者から預けられた情報について、自社の競争力、自らの信用、事故があった場合の取引先等の信頼関係への影響等に鑑み、**経営層も関与**した上で、その**漏えいの防止措置を実施する対象を特定**する。

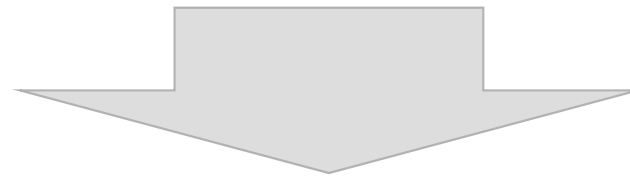
※「守るべき技術等の情報」:

設計図、顧客情報、納入者情報、試作品、試験データ、製造工程（製造ノウハウ、製造データ）、雇用/解雇計画、マーケティング戦略 等



②その守るべき情報の「態様」を把握する

紙媒体、もの（試作品、製造設備など）、電子媒体

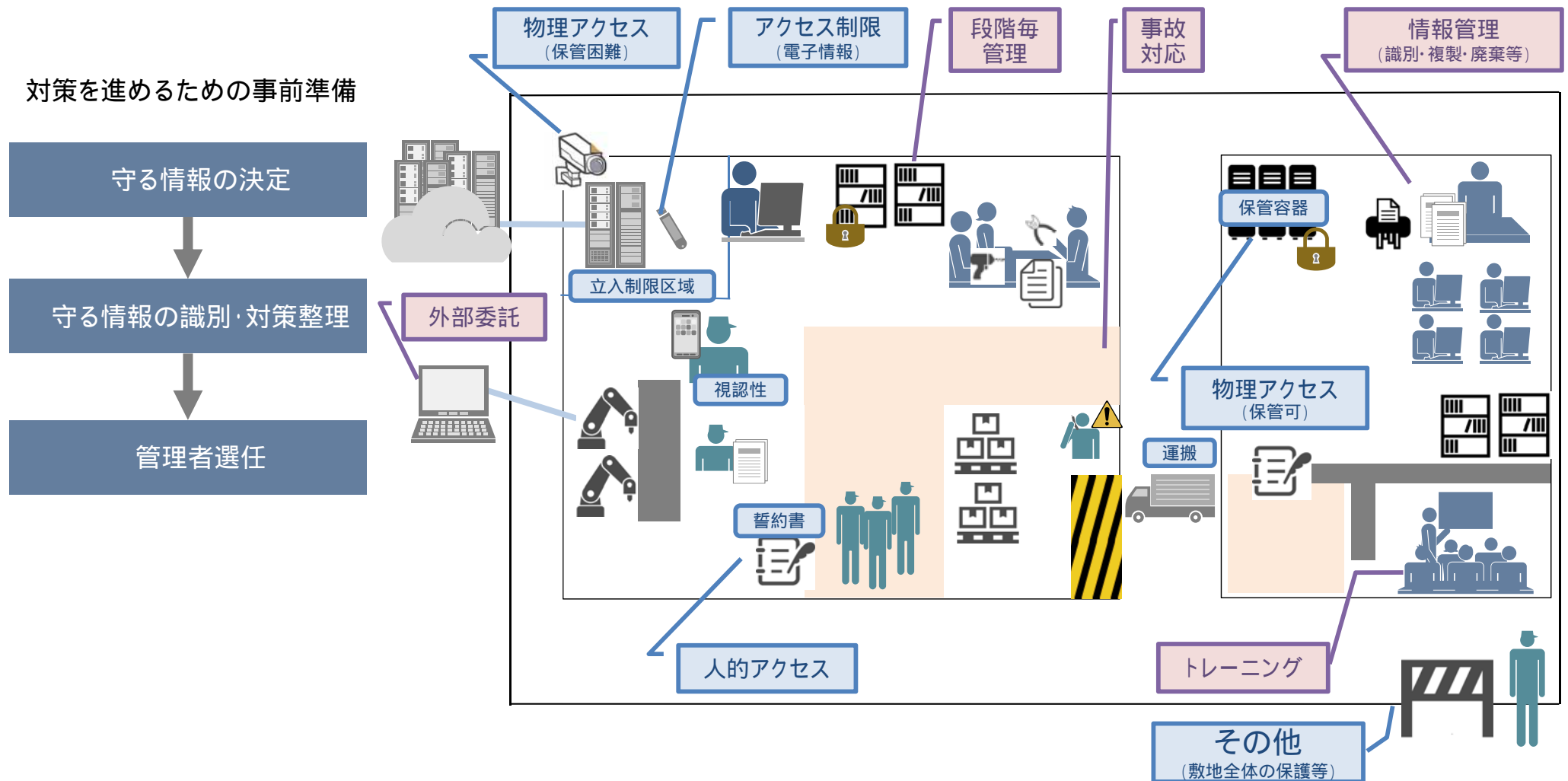


③守るべき情報の態様に応じて、適切な管理策を講じる

（参考）技術等情報管理に必要な対策例

技術等情報管理に必要な対策

- 技術等情報は、企業の重要な経営資源の1つであり、その技術等情報を適切に管理・活用することは、企業が事業活動を継続し、競争力を強化していくための第一歩です。
- また技術等情報管理については、情報の保管方法や従業員教育等の個別の対策があるが、これから対策を検討される方は必要最低限の取組を対策を進めるための事前準備から確認することをおすすめします。



対策を進めるための事前準備～ 守る情報の決定～

- 技術等情報管理の取組を進めるには、守る情報（管理対象情報）の特定が必要です。
- 守る情報を特定する際は経営層も関与し、以下のポイントを考慮しましょう。
ポイント1：その技術等情報が漏えいすると、自社の競争力に重大な影響を与えますか。
ポイント2：他社から契約等に基づき預けられた情報等で、その技術等情報が漏えいした場合、自社の信用や、他社との信頼関係等に重大な影響を与えますか。
- 特定した情報は、必要に応じて保管場所等を記録した目録を作成し、保管しましょう。

技術等情報の例



対策を進めるための事前準備～ 守る情報の識別・対策整理～

- 特定した守る情報（管理対象情報）は、他の技術等情報と区別して識別できるように表示しましょう。表示方法は以下のようなものがあります。
 - 紙の場合 : 「社外秘」等を表示し、守る情報であることを表示
 - 電子情報の場合 : ファイル名に記録し、守る情報であることを表示
 - 試作品・製造装置の場合 : 保管容器にラベルを貼る等、守る情報であることを表示
- 特定した守る情報（管理対象情報）については、情報の価値や種類等に応じて、必要な対策を決める必要があります。他社から預けられた情報の場合は、契約内容等他社が求める対策を考慮して、必要な対策を検討する必要があります。



紙の場合



【社外秘】設計図.doc



【関係者限り】試作品イメージ.ppt

電子情報の場合



モノの場合

対策を進めるための事前準備～ 管理者選任～

- 経営層は、管理対象情報を守るための対策推進に責任を持つ管理者を選任する必要があります。
- 従業員数が多い場合や管理対象情報が複数の事業部門に関係する場合は、誰が管理者か従業員等が認識できるように、社内規程や社内掲示で周知しましょう。
- 従業員数が少人数の場合は、経営層が管理者を兼務する等、組織の規模に応じて適切な管理者を選任しましょう。

管理者の役割

情報管理プロセスの確立

人的アクセスの制限・管理、従業員教育

情報を守るために必要な対策の実施と状況把握

情報漏えい等事故の把握や対応

各種対策について記録を取得・一定期間保管

個別の対策～情報管理プロセス～

- 管理対象情報を適切に管理するために、管理対象情報の作成から廃棄までの情報管理プロセスを作成する必要があります。
- 管理対象情報については、管理簿を作成し、情報の持出や複製・廃棄等の状況がわかるようにしましょう。
- さらに、情報管理プロセスは、従業員に周知し、情報管理の取組が習慣化するようにしましょう。

各プロセスで検討する内容の例

プロセス	検討内容例
作成	<ul style="list-style-type: none"> 作成された情報が管理対象情報の場合、識別できるようにする手順を検討
内容の伝達	<ul style="list-style-type: none"> 情報へのアクセスが認められている従業員から、アクセスが認められていない従業員へ情報を伝える際の手順等を検討
複製	<ul style="list-style-type: none"> 管理対象情報の複製を認める際の基準や承認手順等を検討
廃棄	<ul style="list-style-type: none"> 管理対象情報を復元不可能な方法(細断や焼却等)で廃棄するための手順等を検討



さらに取組を強化する場合・・・

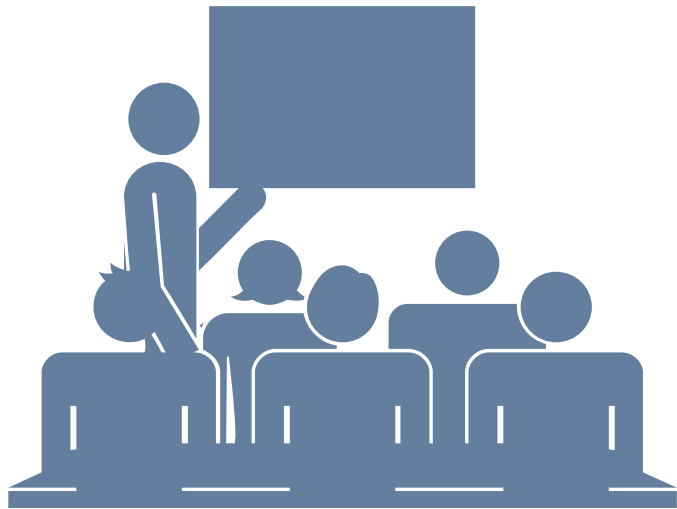
管理対象情報は段階別に管理しましょう。
(価値の高い情報は、アクセス者を限定、対策を組合せて強化 等)

敷地全体を保護しましょう。
(外周の金網、監視カメラ等の侵入防止、監視・駆けつけ体制 等)

外部委託先を管理しましょう。
(情報は全体像がわからないよう渡す、情報蓄積による漏えいを防止する契約)

個別の対策～従業員教育～

- 技術等情報の適切な管理の取組を進めるうえでは、**従業員等に対策を周知し情報管理に対する意識を高めるために、従業員教育を行うことが効果的**です。
- 従業員教育の方法としては、社内会議での実施やe-learning等があります。
- 従業員教育は、1回実施するだけでなく、**定期的に実施**しましょう。



以下の内容等の従業員教育を定期的に実施

- 管理対象情報を適切に管理することの重要性や意義
- 情報管理に関する社内規程やルール
- 情報漏えい等が発生したときの報告ルール 等

個別の対策～情報漏えい等事故発生時の報告ルール～

- 管理対象情報の漏えいが疑われるような事故が発生した際に、被害の未然防止や拡大を防ぐために、事故等発生時の報告ルールを策定し、従業員等に周知する必要があります。
- 報告ルールには、どのような事象を発見したときに報告してほしいか、報告先は誰か等を整理しましょう。

報告を求める事象の例



私有のUSB等への管理対象情報の複製・持出



競合他社等との頻繁な接触・情報提供

個別の対策～人的アクセス制限～

- 管理対象情報を適切に管理するために、必要な人のみが管理対象情報にアクセスできるように、適切なアクセス権の設定を行きましょう。
- アクセス権の設定状況は、定期的に確認・見直しを行う必要があります。特に、従業員の異動時や退職時等は気を付けましょう。
- また、従業員による情報漏えいを防ぐために、守秘義務の厳守や退職後に業務中に知り得た情報を不正に使用しないよう、秘密保持の誓約書を締結することも有効です。

人的アクセス制限・管理する際のポイント

管理対象情報にアクセスできる人が必要最小限の範囲となっているか

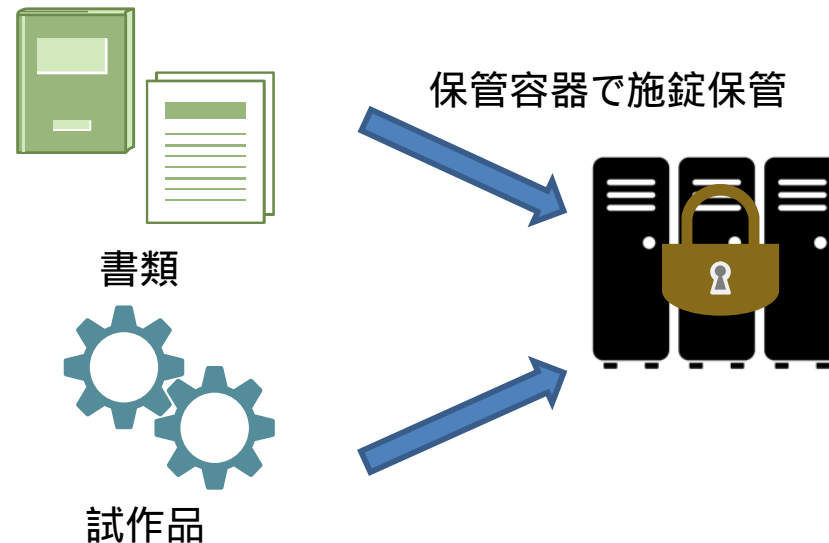
アクセス権の定期的な見直しの実施(プロジェクトの終了時や、異動・退職時等)

管理対象情報へのアクセス権を設定した人への責任明確化(秘密保持の制約等)

一時的な訪問者(見学者等)を受け入れる場合のルール(誓約書面の取得、立ち会い等)

個別の対策～情報の物理的保管～

- 管理対象情報が保管容器（金庫等）で保管できる（紙情報や試作品等）の場合、施錠して保管できる保管容器を用いて保管し、物理的アクセスを制限しましょう。
 - ・ 鍵の適切な管理（鍵の貸出し管理簿作成、文字盤鍵の鍵番号の年1回以上変更 等）
- 保管容器から情報を持ち出して取扱う場合や運搬する場合は、取扱のルールを決めて、運用しましょう。
 - ・ 運搬時の封筒の封印、受領証の受け取り、外部事業者との秘密保持契約締結 等
- 製造装置等保管容器に保管できない場合は、製造装置等を設置している場所の立ち入り制限区域にする等、物理的アクセスを制限しましょう。
 - ・ 入退口の施錠管理、受付簿による立入状況の記録、立入者として視認可能な標識の着用 等



個別の対策～情報の電子的保管～

- 管理対象情報が電子情報の場合は、パソコン等の可搬式記録媒体の持出を管理しましょう。
- 電子情報を自社のサーバ等で保管する場合は、IDやパスワード等による認証を行い、適切なアクセス制限を行い、必要な対策を実施し、管理対象情報を適切に管理しましょう。
- 自社サーバではなくクラウドやデータセンターに保管している場合は、委託先事業者と秘密保持契約を締結した上で、自社で行える対策を実施し、管理対象情報を適切に管理しましょう。

情報システムの管理対策の例

パソコン等へのウイルス対策ソフトをインストールし、定期的に更新・スキャンする

OS等を最新の状態に更新する

ファイヤーウォールやIDS/IPS等を導入する

アクセスログを取得し定期的に確認する

不要なネットワークポートやUSBポート等を使用不能にする

3. 企業の情報管理の促進に向けて

経済産業省による支援

- 経産省としては、経営リソースに限界のある中小企業における適切な技術等情報の適切な管理を促していくため、**研修素材の提供、専門家の派遣等による支援を実施。**

◇ 企業担当者向けの研修素材の提供

企業（特に中小企業）からの技術等の情報の管理として何をしたらよいか分からない、従業員向けの教育の重要性はわかってても何を教育したら良いかわからない等の声に応え、研修資料を経産省HPに用意。

経産省 重要技術マネジメント



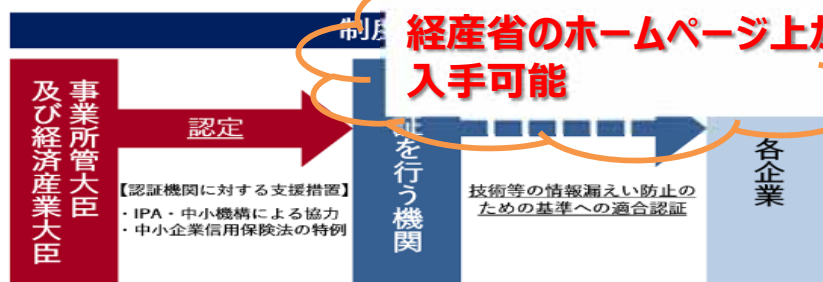
(https://www.meti.go.jp/policy/mono_info_service/mono/technology_management/index.html)

<研修資料内容>

- ✓ 技術等情報漏えいの事例、漏えい等による事業への影響を紹介。
- ✓ 技術等情報を守るために必要な対策について具体例を説明。
- ✓ 自社の技術等情報管理の対策状況をクイズ形式で確認可能。
- ✓ 研修資料の最終ページには、セルフチェックシートを用意。実際に自社の情報管理状況の把握に活用。

技術等情報の適切な管理に向けて

平成30年9月25日、産業競争力強化法に基づき、企業の技術等の情報の管理について、国で示した「守り方」に即して守られているかどうかを、国の認定を受けた機関による認証を受けられる制度がスタートしました。(概要)



各企業の皆様（認定技術等情報漏えい防止措置認証機関から認証を受けたい方）へ

- ・ 各企業の情報管理担当者の皆様へ
- ・ 技術等の情報の管理について、具体的な管理方法を分かりやすく解説しており、クイズ形式で学ぶことができます。

技術等情報管理認証制度の概要

技術等情報管理認証制度は、企業の技術等情報の管理について、国で示した「守り方」に即して守られているかどうかを、国の認定を受けた機関による認証を受けられる制度がスタートしました。(概要)

技術等情報管理認証制度の詳細について

経済産業省「重要技術マネジメント」

<http://www.meti.go.jp/policy/>

また、技術等情報管理認証制度は、認証取得を希望する企業向けに以下のサポートコンテンツがあります。

セルフチェックシート

- 自社の情報管理状況を自身で把握できるチェックシートです。告示の各項目について、確認時のポイント等をまとめてあります。

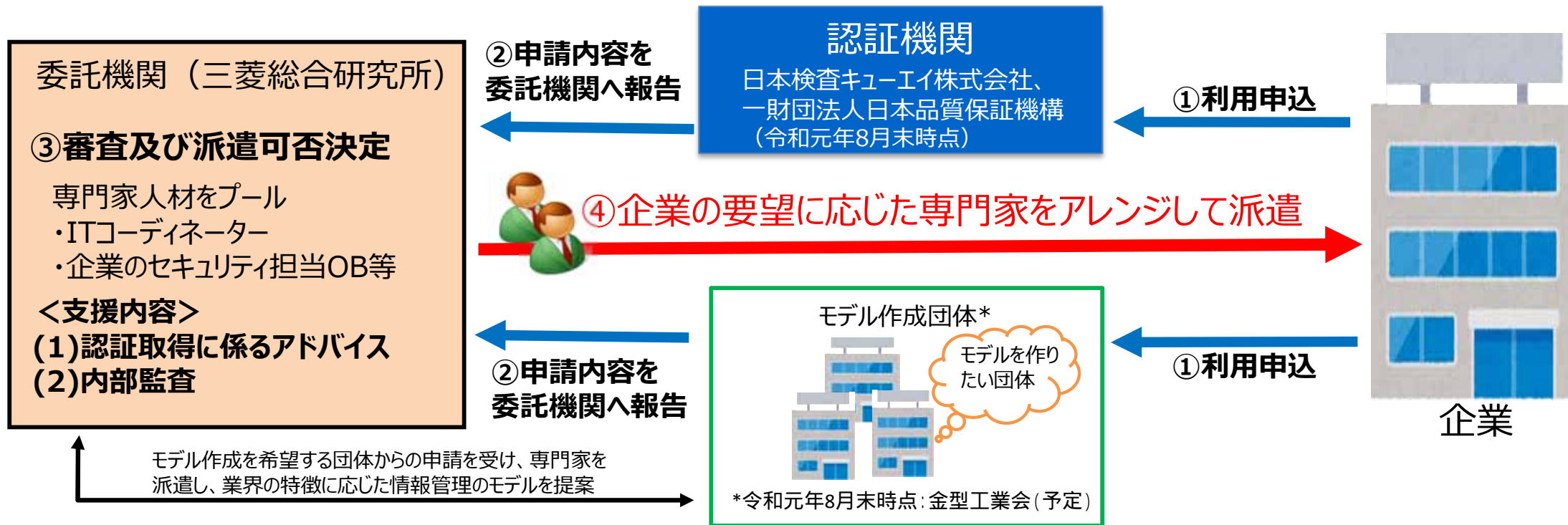
セルフチェックシートのイメージ
及びURLを追加

監査ガイドライン

- 告示の各項目について、基準を満たしているかどうかを確認する際のガイドラインです。
- 主に認証機関の利用を想定したのですが、企業の方が認証取得に向けた準備や自己監査をする際に活用できます。

専門家派遣事業（令和元年度経産省委託事業）

- 経済産業省では、企業の適切な情報管理を促進するため、個別企業に対して専門家を派遣し、守るべき技術の見極めや具体的な情報管理等のアドバイスを行う委託事業を実施。専門家の派遣希望者は、認証機関又はモデル作成団体へ申請。
- また本事業では、個別企業だけでなく団体（業界、複数企業の集合体等）に対しても専門家を派遣し、業界毎の標準的な技術等の情報管理手法（モデル）の確立を支援。



モデルとは

- 業界により守るべき技術等の情報は異なるが、**同じ業界であれば、どの技術等の情報を守るべきかある程度共通**している。
- 個々の企業のみならず関連する企業間において、技術等の情報の**適切な管理手法に係る共通認識**を醸成。
- 業界における業務の特性と守るべき技術等の情報の性質、業界等における情報管理にプラクティス等に合わせたモデルを構築することにより、**企業間における高度な技術等の情報の共有を円滑化**。

お問い合わせ先

経済産業省貿易経済協力局貿易管理部 安全保障貿易管理課

電話 03-3501-2800

技術等情報管理認証制度 担当あて

詳細についてはウェブサイトへ。
パンフレット、研修素材はこちらからダウンロードいただけます。

経産省 重要技術マネジメント **検索**



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