経済産業省　御中

産業競争力強化法に基づく技術情報管理認証制度の普及促進に向けた調査分析及び専門家派遣等事業報告書

三菱総合研究所

デジタル・イノベーション本部
サイバーセキュリティ戦略グループ

2022年3月28日

目次

1. 調査の背景・目的

グローバルな競争が進む中、また、事業者の保有する無形資産が市場において重要な競争優位を形成する中で、事業者が無形資産たる技術情報を適切に管理することは、事業者同士の信頼構築を支え、事業者間での技術等の情報の共有を円滑にし、イノベーションを促進する重要な要素となっている。一方で、多くの事業者、特に中小事業者、にとっては自社の中で重要な技術情報の特定や当該技術情報の管理の整備については、知見・経験の不足や、ビジネスで直接の利益を生むわけではないものにリソースを割けない等もあり、十分に進んでいるわけではないのが実情である。

多数の事業者が技術情報を適切に管理している状況になると、管理ができていない事業者にとっては営業がしづらくなることや、そもそも管理の必要性への理解が進んでいることもあり、更に多くの事業者が管理することが見込まれる。しかしながら、現在のように、技術情報の管理が進んでいない事業者が多く、また、そうしたものを行う必要性への社会全体への理解が十分に進んでいない状況では、一部事業者にとって技術情報の管理が重要であることは理解しつつも、実際に進める上でのハードルが非常に大きい。

そこで、経済産業省としては、技術情報の管理として必要となる項目を国として基準で示し、当該項目を満たしたことを国が認定する第三者が認証する制度（産業競争力強化法に基づく技術情報管理認証制度。以下、「認証制度」という。）を創設し、認証制度の普及を進めていくことによって、事業者、特に中小事業者の技術情報の管理の理解醸成や、管理能力の底上げを図ることにより、もって我が国産業の競争力向上に資するイノベーション促進の環境を整えることを意図している。

本事業では、認証制度の普及促進に向けて必要となる認証制度の在り方についての調査分析、認証制度の取得を進めるための専門家派遣等の事業者への支援、普及のための広報等を行うことを目的とする。

2. 調査分析事業

2.1 国内外の類似の認証制度との比較・分析、比較表の作成

2.1.1 比較表

技術情報管理認証制度と国内外の類似した関連制度の調査を行った。調査対象は以下の通りである。

- Cybersecurity Maturity Model Certification（CMMC）
- 情報セキュリティマネジメントシステム（Information Security Management System ： ISMS）適合性評価制度
- SECURITY ACTION
- プライバシーマーク制度
- 業界ガイドライン （例）自動車産業サイバーセキュリティガイドライン

情報セキュリティ対策については、ISMS 適合性評価制度（マネジメントシステムの認証）やSECURITY ACTION（対策に取り組むことに対する自己宣言）といった制度がある。情報セキュリティに関しては、組織の情報の重要性に応じて、機密性・可用性・完全性を確保するための包括的な対策を要求するが、技術情報管理認証制度は、「守るべき情報を特定」し、重要情報の保護にフォーカスしている点で他の制度とは異なる。

技術情報管理認証制度と国内外の類似した認証制度の調査を行った。調査対象は以下の通りである。

- CMMC
- ISMS 適合性評価制度
- SECURITY ACTION
- プライバシーマーク制度
- エコアクション21 認証制度
- JAS 制度

認証制度における審査期間は主に数か月～半年程度である。更新期間は主に 2～3 年であり、制度によっては年に1度、維持審査や定期調査が行われる。主なインセンティブとしては入札要件が挙げられるが、特に中小企業向けの制度では補助金や融資の要件にもなっている。

比較表を次ページに示す。

表 2-1 技術情報管理認証制度と国内外の類似制度との制度概要比較

	技術情報管理 認証制度	CMMC	ISMS 適合性 評価制度	セキュリティ アクション	プライバシーマーク制度	業界ガイドライン （例）自動車産業 サイバーセキュリティ ガイドライン
制度の目的	中小企業等も含めた産業界全体における「技術をはじめとする重要な情報」の適切な管理を促進すること。	DIB（Defense Industrial Base:防衛産業基盤）企業による非機密扱いのネットワーク内の連邦契約情報（FCI）と管理された非機密扱い情報（CUI）の保護を促進すること。	企業・団体等の情報セキュリティ全体を向上させ、諸外国からも信頼を得られるようにすること。	中小企業の自発的な情報セキュリティ対策への取り組みを促し、安全・安心な IT 社会を実現すること。	適切な個人情報の取扱いを推進すること。 個人情報の保護に関する消費者の意識の向上を図ること。	自動車産業全体のサイバーセキュリティ対策のレベルアップや対策レベルの効率的な点検を推進すること。
制度主体	経済産業省、及び関係省庁	CMMC-AB	一般社団法人 情報マネジメントシステム 認定センター （ISMS-AC）	独立行政法人 情報処理推進機構（IPA）	一般財団法人 日本情報経済社会 推進協会（JIPDEC）	一般社団法人 日本自動車工業会・ 一般社団法人 日本自動車部品工業会
ターゲット	中小企業 （特に製造業）	DoD に製品やサービスを提供する全組織	企業・団体等	中小企業	企業・団体等	自動車産業に 関係する 全ての企業
対象とする情報	技術情報をはじめとする事業者の競争力の源泉となる情報（営業秘密情報）	FCI 及び CUI	情報資産全般	情報資産全般	個人情報	情報資産全般
認証対象	技術情報等の 管理方法	サイバーセキュリティ成熟度（プロセスとプラクティスが実装されているか）	情報セキュリティ マネジメントシステム	情報セキュリティ対策に 取り組むこと （自己宣言）	個人情報保護 マネジメントシステム	情報セキュリティ対策への 取組み （認証は行わない）
特徴	特に情報の秘匿性にフォーカスを当てている。	要件のベースとなっている NIST SP800-171 は特に CUI の秘匿性にフォーカスを当てている。	情報の CIA を保護することにフォーカスを当てている。	情報の CIA を保護することにフォーカスを当てている。	個人情報を対象としている。	自動車産業固有のサイバーセキュリティリスクを考慮した対策フレームワークや業界共通の自己評価基準を明示している。

出所）公開情報より三菱総合研究所作成

表 2-2 技術情報管理認証制度と国内外の類似制度における認証・評価手法に関する比較

	技術情報管理認証制度	CMMC	ISMS 適合性評価制度	SECURITY ACTION	プライバシーマーク制度	エコアクション 21 認証制度	JAS 制度
概要	事業者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認証する制度。	DIB 企業のサイバーセキュリティの成熟度レベルを評価する制度。	情報セキュリティマネジメントシステムに対して、国際基準への適合性を評価する制度。	中小企業自らが、情報セキュリティ対策に取り組むことを自己宣言する制度。	事業者が個人情報の取り扱いを適切に行う体制等を整備していることを評価する制度。	環境マネジメントシステムが環境省が策定したガイドラインに適合しているかを認証する制度。	食品・農林水産物の品質・仕様や事業者のサービス・マネジメントなどが、規格に適合しているかを認証する制度。
審査期間	認証機関によって異なる	半年(以上)	3～4 か月(以上)	1週間程度(自己宣言)	4か月(以上)	3～4 か月程度	2 か月～半年程度
更新期間	3 年を上限	3年	3年(年に1度の維持審査あり)	特になし	2 年	2年(1年後に中間審査あり)	特になし(年に1度の定期調査やマークの使用実績報告、不定期調査あり)
コスト	認証機関によって異なる	レベル1: $1,000 レベル2: $7,489 レベル3:$17,032 レベル4:$23,355 レベル5:$36,697 (小規模な事業者の平均評価コストの推定)	取得:約 90～100 万円 更新:約 70 万円 維持審査:約 50 万円 (従業員 50 名程度の場合、概算)	無料	約 31 万 4 千円 (小規模な事業者の場合, 消費税込み)	登録審査費: 12 万 5 千円 初回の中間審査費: 10 万円 更新審査費:10 万円 2 回目以降の中間審査費:5 万円 認証・登録料:10 万円 更新登録料:10 万円 (従業員 50 名程度の場合、消費税抜き)	認証(調査)申請手数料: 5 千円 書類審査(調査)手数料: 5 千円 実地審査(調査)手数料: 1 万 6 千円 判定業務手数料:5 千円 (特定非営利活動法人環境保全米ネットワークによる有機料理を提供する飲食店等の管理方法に係る取扱業者の認証の場合、消費税抜き)
インセンティブ	検討中	・DoD との取引が可能となる ・CMMC 規格の使用や、自国の規格や利害関係者との相互関係の実現に関心を持つ政府機関や米国の同盟国が多数存在。	・入札要件	・自己宣言事業者検索で検索可 ・補助金等の申請要件	・入札要件	・入札要件 ・自治体による支援や優遇制度 ・金融機関等による関連融資 ・環境省優良産廃処理業者認定制度との相互認証	・調達基準 ・JAS 適合を求める規制 ・優遇金利の適用 ・補助金

出所）公開情報より三菱総合研究所作成

2.1.1 各制度の審査・認証のスキーム

技術情報管理認証制度では、現地審査による認証と自己適合宣言の認証の2つの認証方法がある。

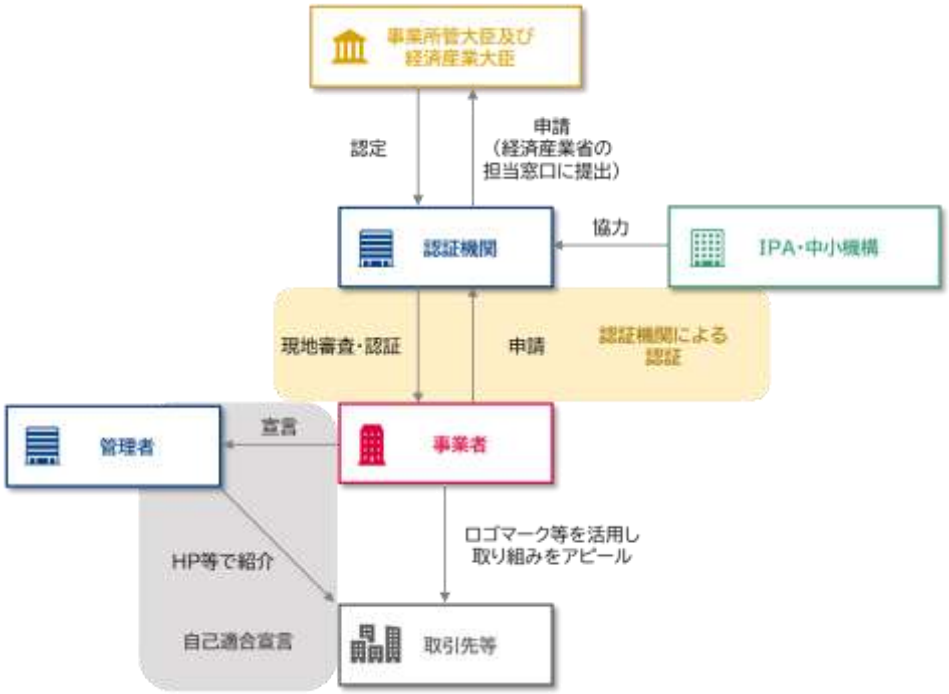


図 2-1 審査・認証スキーム（技術情報管理認証制度）

ISMS 適合性評価制度では、ISMS-AC により認定された認証機関が適合性を審査・認証している。

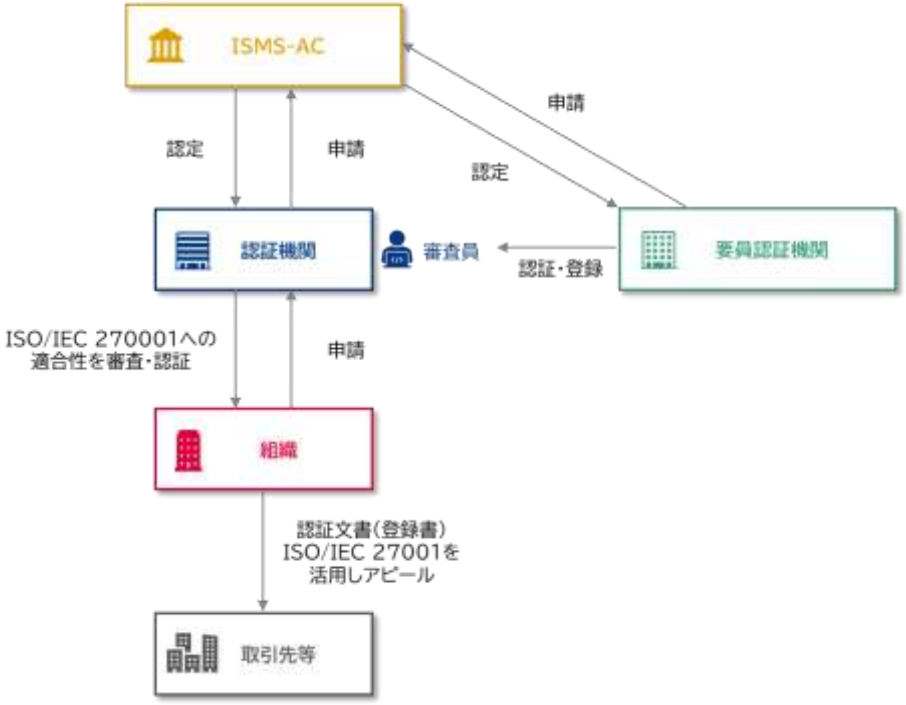


図 2-2 審査・認証スキーム（ISMS）

CMMC では、CMMC-AB により認定された C3PAO（Certified Third-Party Assessment Organizations：認定第三者評価機関）が評価・証明書発行を行っている。

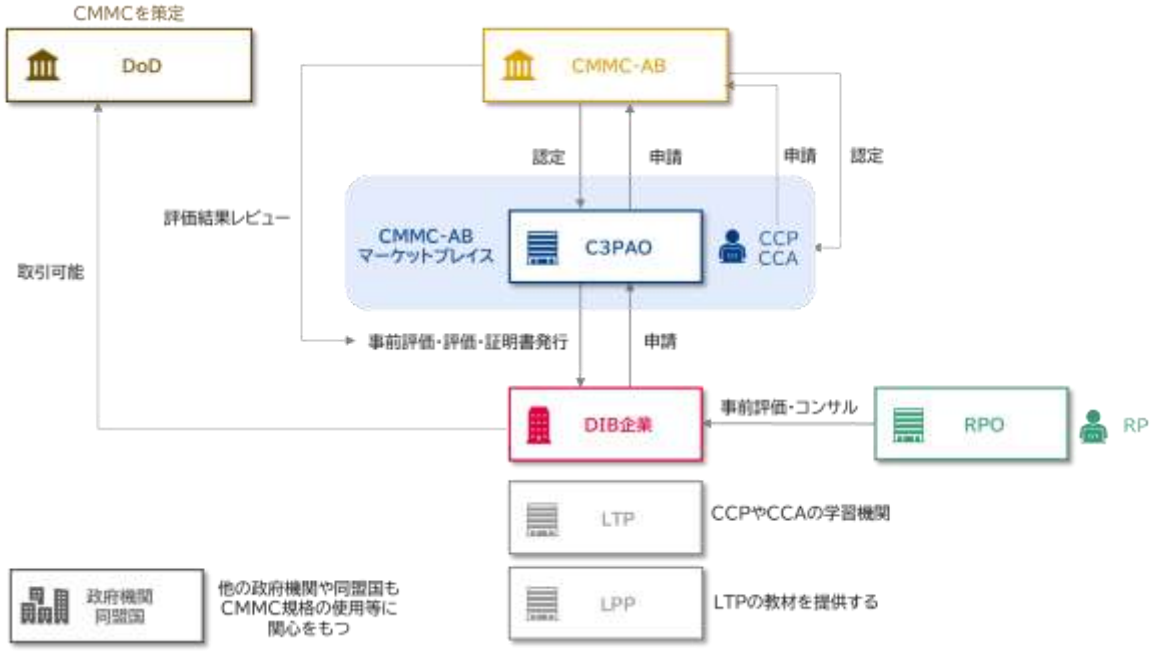


図 2-3 審査・認証スキーム（CMMC）

なお、2021 年 11 月 4 日に CMMC 2.0 が発表された。CMMC 1.0 からの主な変更点は、以下の通りである。

① 5 つから 3 つのコンプライアンスレベルへとモデルの合理化が推進された。
② 米国国立標準技術研究所（NIST）のサイバーセキュリティ基準が採用された。
③ レベル 1（Foundational）の全企業とレベル 2（Advanced）の一部の企業で、自己評価による適合性の証明が可能となる。
④ 第三者評価者の専門的基準と倫理的基準の監視が強化される。
⑤ 認証取得に向けた行動計画・マイルストーン（POA&Ms）の策定が特定の条件下で認められる。
⑥ 特定の条件下で CMMC 要件の免除が可能となる。
⑦ CMMC 1.0 と比較してコストが大幅に削減される予定である。

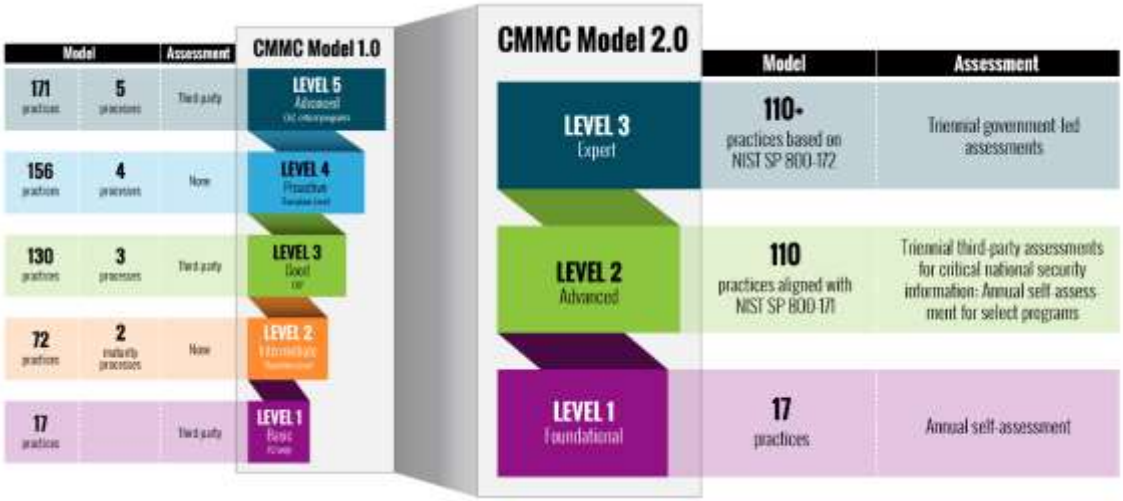


図 2-4 CMMC のモデル 1.0 とモデル 2.0 の違い

表 2-3 CMMC モデル 2.0 の概要

CMMC 2.0 のレベル	CMMC 1.0 との対応	ターゲット	セキュリティプラクティス数	NIST の要件との対応	評価
レベル3（Expert）	レベル 5 相当	CUI を扱う高優先度プログラム向け	110 以上	NIST SP 800-172 要件のサブセットに基づいている	3 年ごとの政府主導の評価
レベル2（Advanced）	レベル 3 相当	CUI を扱う企業向け	110	NIST SP 800-171 と同等	重要な国家安全保障情報に対する 3 年ごとの第三者評価 特定のプログラムに対する 1 年ごとの自己評価
レベル1（Fundamental）	レベル 1 相当	FCI を扱う企業向け	17		1 年ごとの自己評価

出所）ACQUISITION & SUSTAINMENT「ABOUT CMMC」https://www.acq.osd.mil/cmmc/about-us.html（最終閲覧日：2022 年 1 月 19 日）

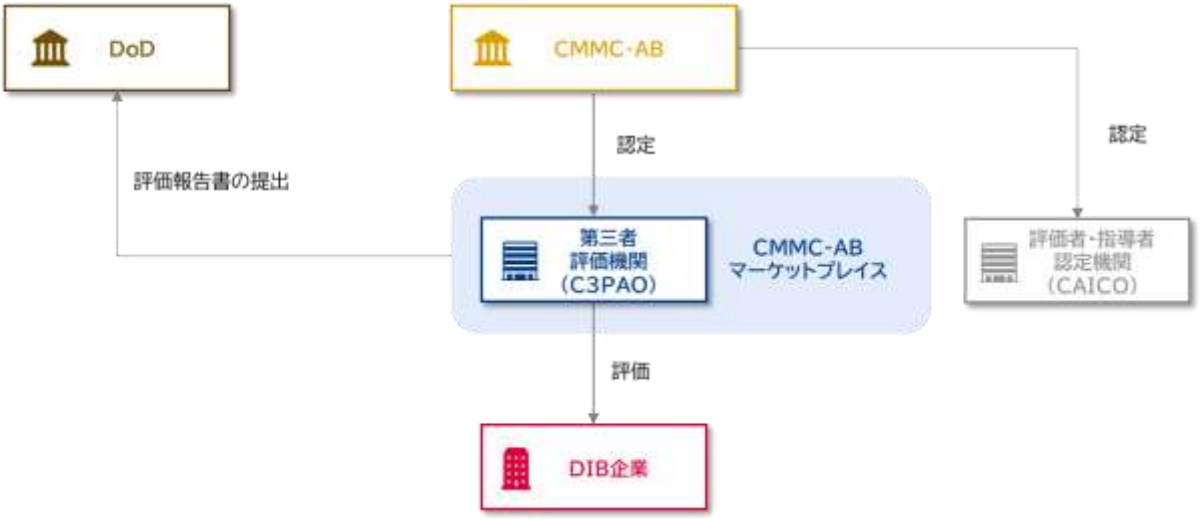


図 2-5 審査・認証スキーム（CMMC）

国家安全保障に不可欠な情報を含むプログラムか否かで自己評価か第三者評価かが変わる。CMMC 2.0 の行動計画及びマイルストーン（POA&M）としては、CMMC の要件を満たすための行動計画及びマイルストーン（POA&M）をもって、契約締結が行えるようなる。その際、契約締結前に達成すべき要求事項の基準値を設定し、残りの部分については明確に定義したスケジュールで POA&M に対応することが求められる。期限は 180 日を想定している。また DoD は、POA&M に含めることができない要件の一部を指定する予定である。

また、CMMC2.0 要件の免除については、特定のミッションクリティカルな要件の取得に関して、CMMC 要件を除外する限定的な免除プロセスが認められる。免除申請には DoD の上級幹部の承認が必要であり、期間も限定される。

エコアクション 21 では、中央事務局と地域事務局、審査員が連携して、審査・認証を行っている。

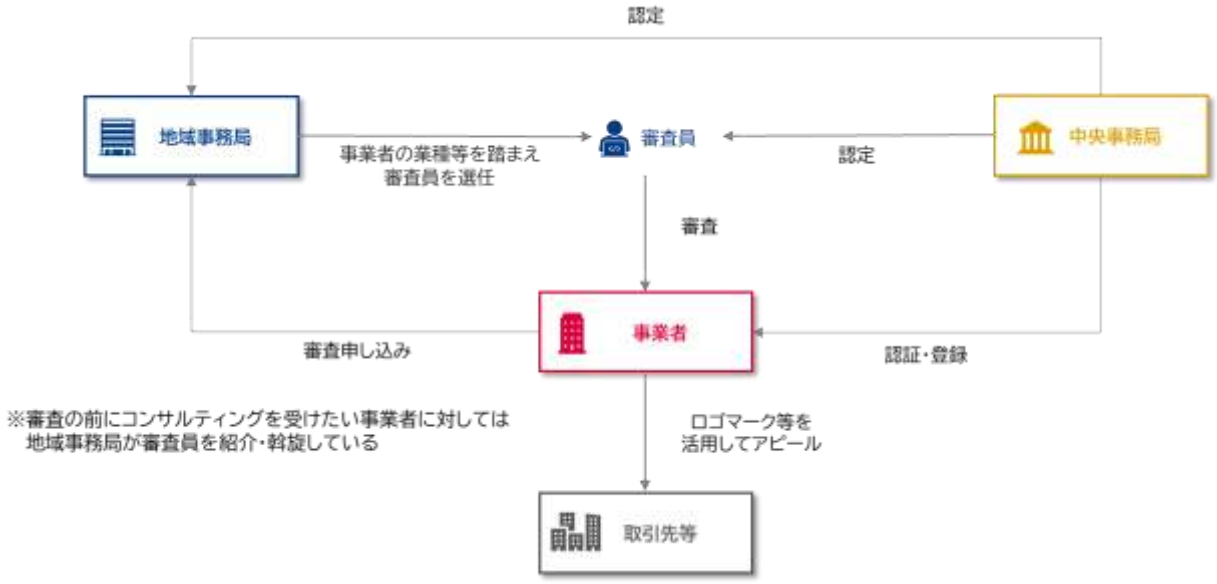


図 2-6 審査・認証スキーム（エコアクション 21）

JAS 制度では、農林水産大臣により登録された認証機関が、審査・認証を行っている。

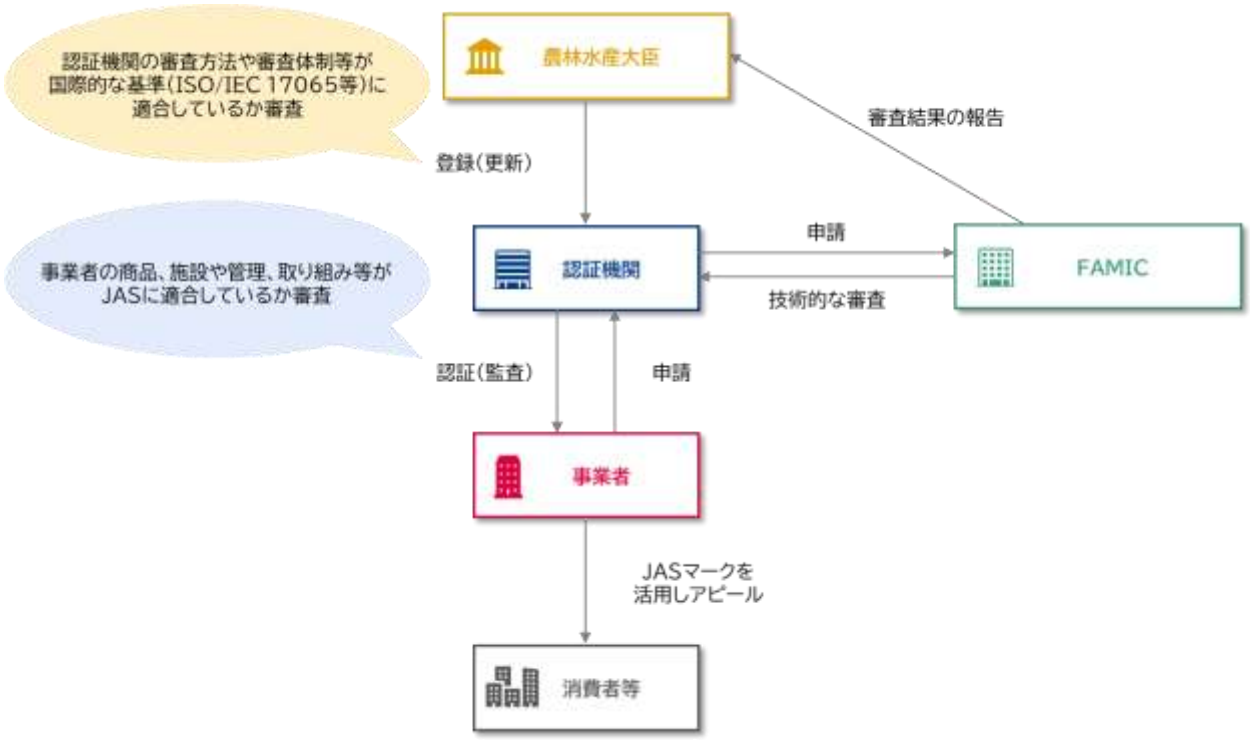


図 2-7 審査・認証スキーム(JAS)

表 2-4 JAS 制度の概要

	JAS 制度
概要	食品・農林水産物の品質・仕様や事業者のサービス・マネジメントなどが、規格に適合していることについて、国が認めた第三者機関(JAS 認証機関)が審査・認証を行う制度。
政策的位置づけ	日本農林規格等に関する法律(JAS 法)に基づく制度。 2017 年に制度の見直しが行われた。
対象	【産品】 ・特定の原材料、成分等の農林水産品・食品 ・特定の栽培法・西方で生産された農林水産品・食品 等 【事業者】 ・事業者による特定の栽培管理や飼養管理、品質・衛生管理、保管・輸送管理、販売管理、料理の調理や提供方法 等 ・官能評価員等の技量・力量 等 ・事業者による労務管理や社会貢献 等 【試験方法】 ・成分の測定方法や DNA 分析方法
規格・基準検査方法	規格や基準、検査方法は、製品や管理・試験方法の種類により異なる。 (https://www.maff.go.jp/j/jas/jas_kikaku/kikaku_itiran2.html)

2.1.2 各制度の審査・認証のプロセス

技術情報管理認証制度では、現状、申請ののち二段階の審査を経て認証を取得できる。

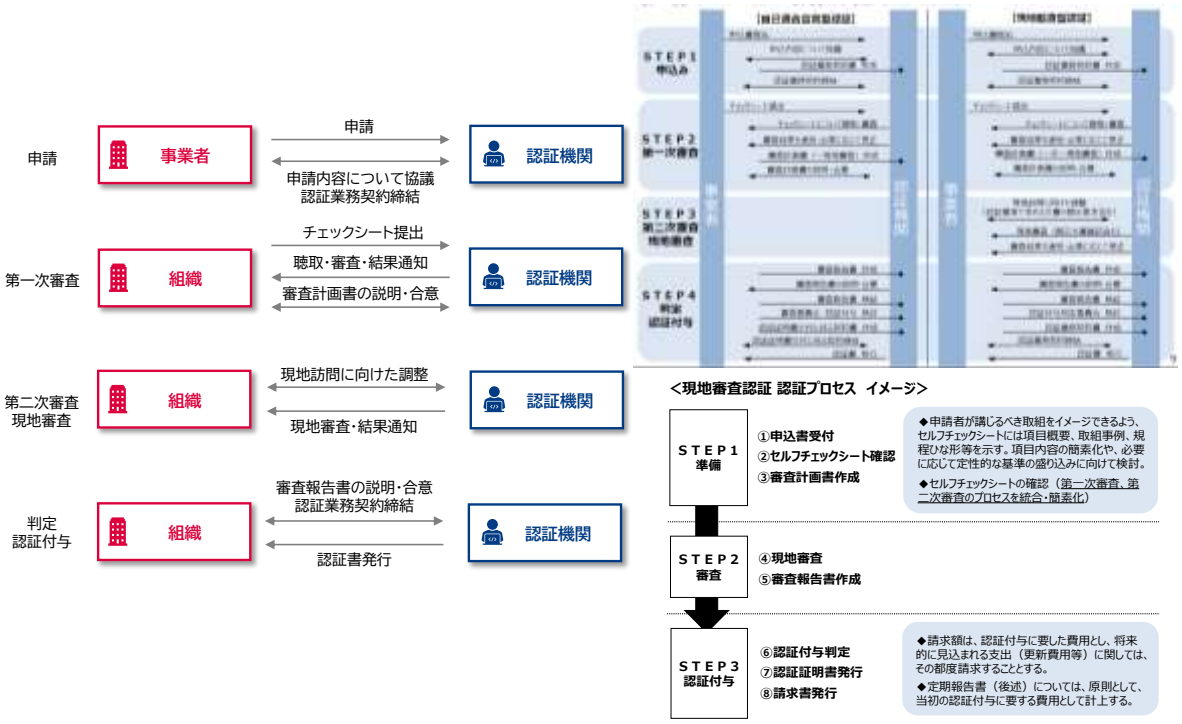


図 2-8 審査・認証プロセス（技術情報管理認証制度）

ISMS適合性評価制度では、申請ののち二段階の審査を経て認証登録が行われる。

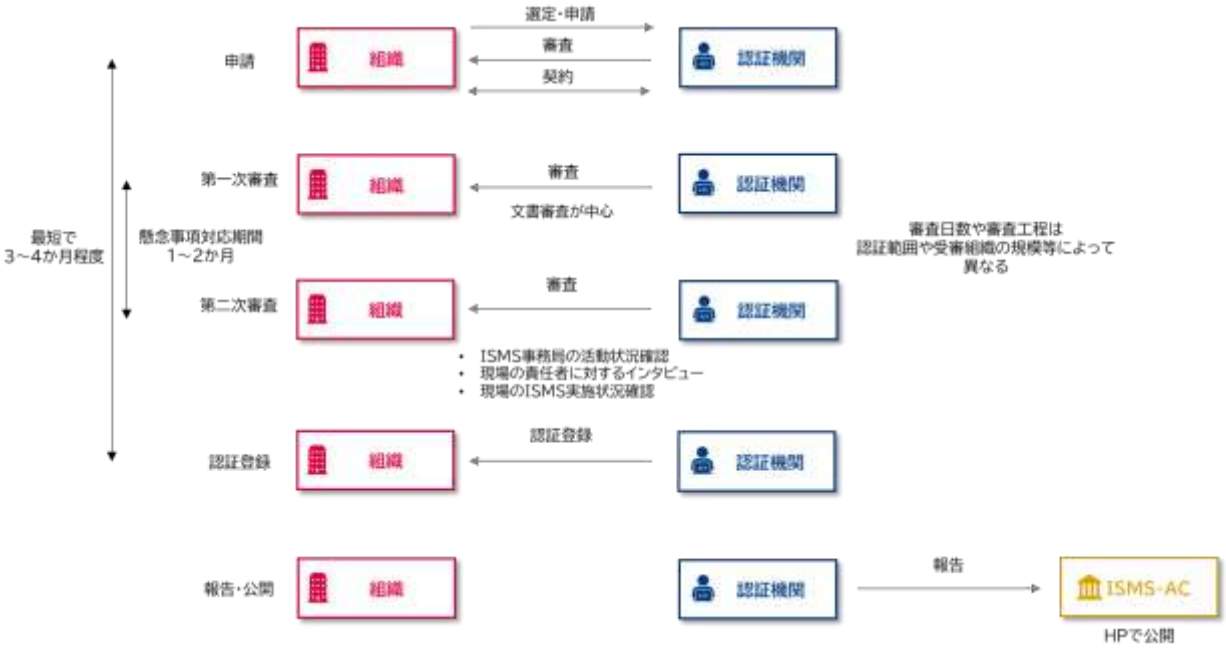


図 2-9 審査・認証プロセス（ISMS）

CMMC では、CSPAO による評価及び CMMC-AB による評価のレビューを経て認証される。

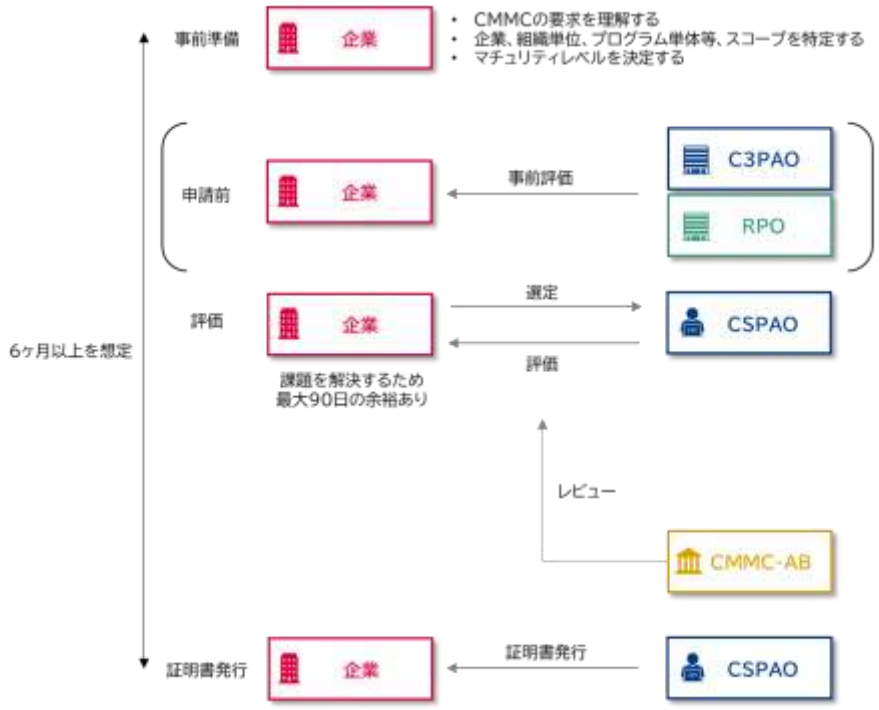


図 2-10 審査・認証プロセス（CMMC）

ISMS では 1 年ごとにサーベイランス審査が求められているのに対し、技術情報管理認証制度で定期報告書の提出を求めることとすると、以下のような流れとなる。

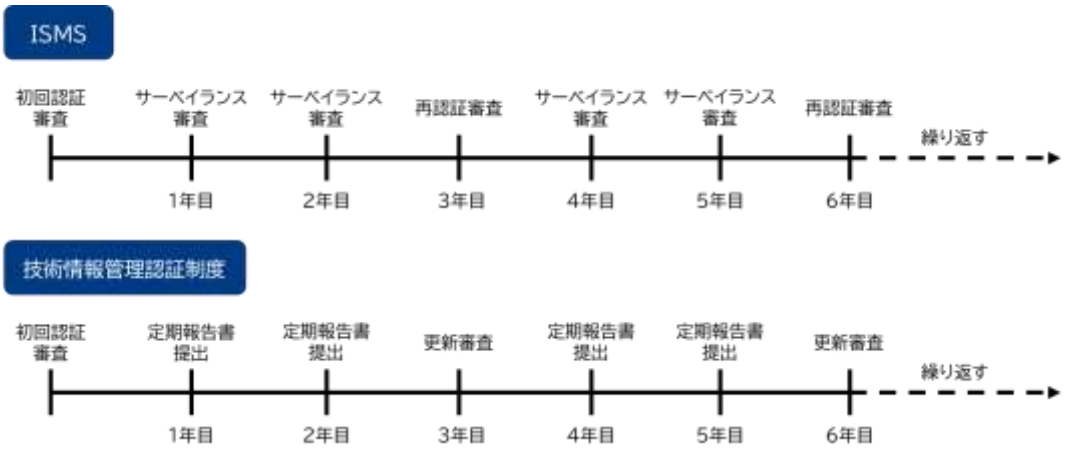


図 2-11 ISMS のサーベイランス及び技術情報管理認証制度の定期報告の仕組み

2.1.3 中小企業向け制度の普及に関する取組み

(1) インセンティブについて

セキュリティ関連の制度である「CMMC」「ISMS 適合性評価制度」「SECURITY ACTION」に加え、国内の認証制度である「エコアクション 21」「JAS」について、制度の概要等を調査した。そのうち、インセンティブについては、以下の調査を行った。

- 融資、補助金制度 (エコアクション 21)
- 優良産廃処理業者認定制度(エコアクション 21)

エコアクション 21 が要件となっている融資や補助金制度の具体例は以下の通り。

- 融資

  三菱 UFJ 銀行 ビジネスローン「融活力」

  エコアクション 21 の認証・登録を取得された企業は、ビジネスローン「融活力」において、審査結果に応じた所定の金利より、▲0.5%優遇される。

- 補助金制度

  東京都新宿区環境マネジメント規格認証取得費補助制度

  区内に事業所を有する法人が、環境マネジメントシステムの規格の認証を新たに取得する場合、更新する場合、又は適用範囲を拡大する場合の審査・登録費用が一部助成される。

  補助金額:対象経費の 2 分の 1 以内 上限 10 万円 ※1,000 円未満は切り捨て

  補助金総額:50 万円

表 2-5 エコアクション 21 の概要

	エコアクション 21
概要	組織や事業者等が環境への取り組みを自主的に行うための方法を定めたガイドラインに適合しているかを認証する制度。
政策的位置づけ	日本の環境政策における重要な施策の一つとして、国の法律や制度等に位置付けられている。 例:第五次 環境基本計画(平成 30 年 4 月 17 日 閣議決定) 「ISO14001 や中堅・中小企業向けエコアクション21など PDCA サイクルを備えた環境マネジメントシステムについてバリューチェーン全体で導入されることを促進する。」
地域事務局の役割	• 普及活動 • セミナーや個別相談会の実施 • コンサルタントの紹介 • サポート窓口の設置 • 審査申込書の受付 • 審査員の紹介 地域事務局としての認証登録の可否を判定(判定結果を中央事務局が精査・確認して登録が決まる)
インセンティブ	•建設等公共工事入札において、31 都道府県がエコアクション21を加点要素としている(2021 年 1 月時点) •20 の金融機関が 23 件のエコアクション21関連融資を提供している。 •24 の自治体等が補助金等制度を設けている。 優良産廃処理業者認定制度の認定において、エコアクション21は環境配慮基準の対象となっている。
その他	不動産投資法人は役員のみで従業員はいないため、委託先の資産運用会社が実質的な業務を行っている。そのため、認証登録事業者は不動産投資法人となるが、資産運用会社の事業活動が審査の対象となり、認証登録証にも資産運用会社として名称を記載する。

また、優良産廃処理業者認定制度は、通常の許可基準よりも厳しい基準に適合した優良な産廃処理業者を、都道府県・政令市が審査して認定する制度である。

認定を受けた産業廃棄物処理業者は、以下のメリットを受けられる。

- 許可証等を活用したPR
- 産業廃棄物処理業の許可の有効期間の延長
- 申請時の添付書類の一部省略(自治体の判断による。)
- 財政投融資における優遇
- 環境配慮契約法に基づき国等が行う産業廃棄物の処理に係る契約での有利な取扱い

認定を受けるためには、「遵法性」「事業の透明性」「環境配慮の取組」「電子マニフェスト」「財務体質の健全性」の 5 つの基準に適合することが必要となる。

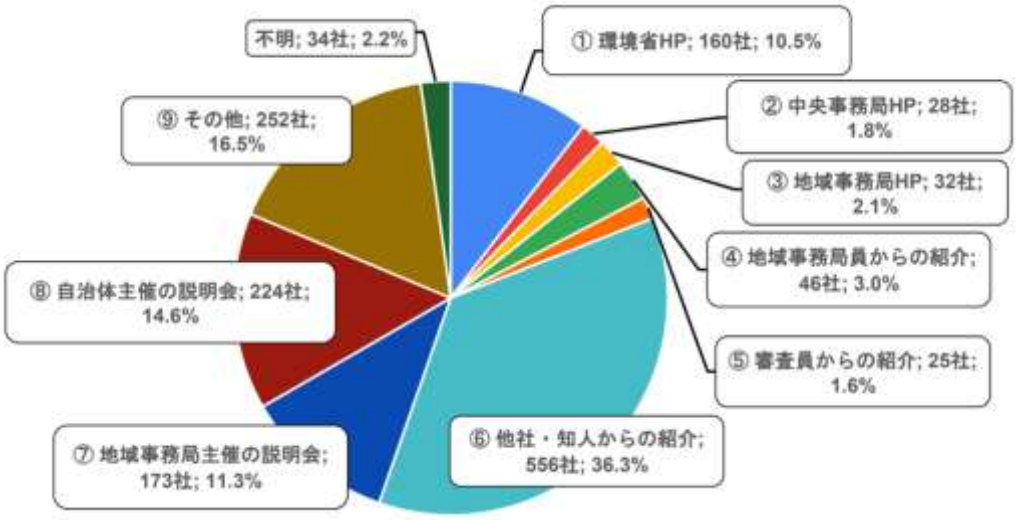
「環境配慮の取組」として、「ISO14001 又はエコアクション 21 若しくはこれと相互認証されている認証制度による認証を受けていること」が要件となっている。

（2）普及の方法について

普及の方法については、同じく中小企業向けの制度である「SECURITY ACTION」と「エコアクション 21」について、調査を行った。

- 普及賛同企業 （SECURITY ACTION）
- 関係企業グリーン化プログラム （エコアクション 21）
- 表彰制度 （エコアクション 21）

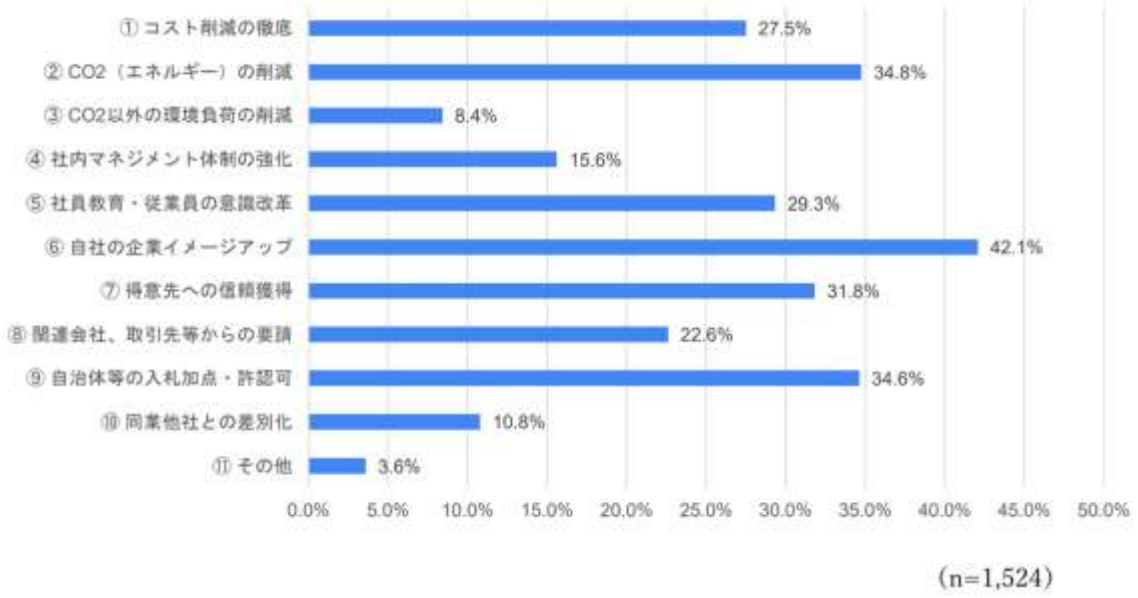
エコアクション21を知ったきっかけは、紹介（40.9%）、説明会（25.9%）、HP（14.4%）となっている。



出所）一般財団法人 持続性推進機構「エコアクション21と社会課題（SDGs）に関するアンケート調査（2021 年）」より引用

図 2-12 エコアクション 21 を知ったきっかけ

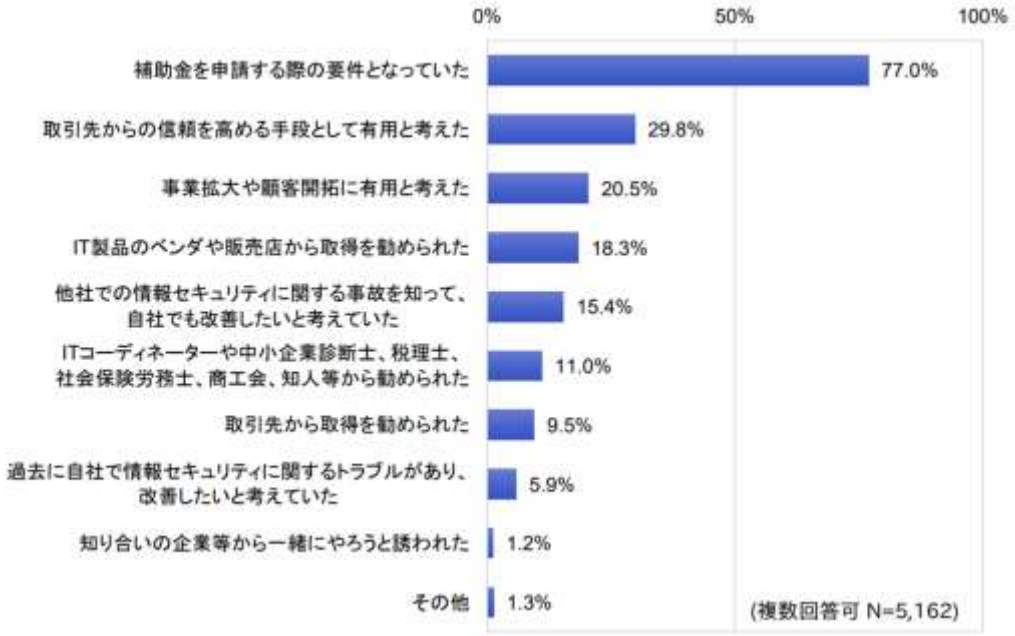
エコアクション21に取り組み始めた理由としては、「イメージアップ」「CO2 の削減」「入札加点・許認可」が挙げられている。



出所）一般財団法人 持続性推進機構「エコアクション21と社会課題（SDGs）に関するアンケート調査（2021 年）」より引用

図 2-13 エコアクション 21 に取り組み始めた理由（複数回答、最大3つ）

SECURITY ACTION 宣言を行おうとしたきっかけとしては、「補助金申請の要件」が大きな割合を占めている。

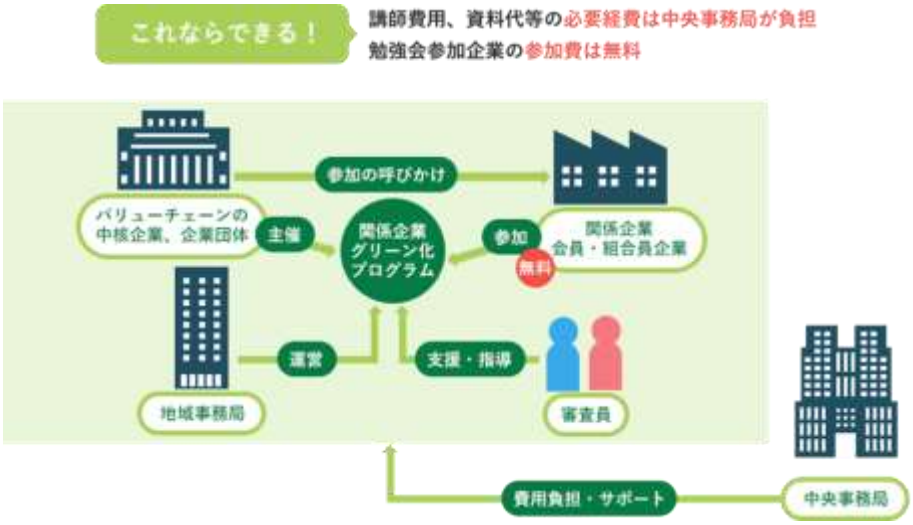


出所）独立行政法人 情報処理推進機構「2018 年度 SECURITY ACTION 宣言事業者における情報セキュリティ対策の実態調査 調査報告書」より引用

図 2-14 SECURITY ACTION 宣言を行おうとしたきっかけ

1） 普及に関する取り組み例①（エコアクション 21：関係企業グリーン化プログラム）

関係企業グリーン化プログラムは、バリューチェーンの中核企業等が関係企業等に参加を呼びかけ、エコアクション21の構築・運用方法を一から丁寧に指導し関係企業等のエコアクション21認証取得をサポートする「塾」を（4～5 回程度）開講する制度である。これまでにプログラムを実施した企業団体は 134団体に上る。関連会社等からの要請によりエコアクション21に取り組み始めた事業者が 22.6%存在することから、関係企業グリーン化プログラムには一定の効果があると考えられる。



出所）エコアクション21中央事務局「関係企業グリーン化プログラム」https://www.ea21.jp/kanren-initiative/（最終閲覧日：2021 年 9 月 8 日）より引用

図 2-15　エコアクション 21「関係企業グリーン化プログラム」

2） 普及に関する取り組み例②（エコアクション 21：環境コミュニケーション大賞）

環境コミュニケーション大賞 環境経営レポート部門では、エコアクション 21 認証事業者の優れた環境経営レポートの表彰を行っていた。令和2年度実施の第 24 回環境コミュニケーション大賞の環境経営レポート部門には、114 点の応募作品があった。令和2年度の開催をもって休止となったが、今後新たな表彰制度が公表される見込みである。

3） 普及に関する取り組み例③（SECURITY ACTION：普及賛同企業等）

SECURITY ACTION では、趣旨に賛同し、当制度の普及促進のための積極的な取り組みを実施する企業及び団体等の紹介を HP 上で行っている。取組みとしては、メールマガジンやセミナーを通じた情報提供やサイバー保険の割引、申請のサポート等が行われている。2022 年 1 月現在、普及賛同企業等は 182 団体に上る。

中小企業が制度を知るきっかけとして「他社や知人からの紹介」は一定数あると考えられるため、普及賛同企業の取り組みは一定の効果があると思われる。

出所）SECURITY ACTION「関普及賛同企業等について」https://www.ipa.go.jp/security/security-action/promotion/index.html（最終閲覧日：2022 年 3 月 28 日）より引用

図 2-16　SECURITY ACTION における普及賛同企業等の紹介状況

表 2-6 関連制度における普及に関する取組み

	関係企業グリーン化プログラム（エコアクション 21）	環境コミュニケーション大賞 環境経営レポート部門（エコアクション 21）	普及賛同企業（SECURITY ACTION）
ターゲット	・バリューチェーンでの環境への取組を推進したい大手企業 ・会員、組合員企業の環境対応力強化を図りたい企業団体	・既にエコアクション21認証を取得している事業者	・SECURITY ACTION 制度の活用を検討している事業者
取り組み内容	主体となる大手企業等が関係企業等に参加を呼びかけ、エコアクション21の構築・運用方法を一から丁寧に指導し関係企業等のエコアクション21認証取得をサポートする「エコアクション21の塾」を（4～5 回程度）開講する。参加費は無料。	エコアクション 21 認証事業者の優れた環境経営レポートを表彰する。（令和2年度の開催をもって休止となったが、新たな表彰制度が公表される見込み。）	SECURITY ACTION の趣旨に賛同し、当制度の普及促進のための積極的な取り組みを実施する企業及び団体等を HP で紹介する。
実績等	【過去のプログラム実施企業・団体】 企業：24 社 金融機関：6 機関 商工会・商工会議所・中央会：19 団体 組合：46 組合 協会：23 協会 その他：16 団体	令和2年度実施の第 24 回環境コミュニケーション大賞の環境経営レポート部門には 114 点の応募作品があった。	【取組み例】 ・メールマガジンを通じた情報提供（一般社団法人中小企業診断協会） ・セミナーを通じた情報提供（西武信用金庫） ・サイバー保険の割引（損害保険ジャパン日本興亜株式会社） ・申請のサポート（コニカミノルタジャパン株式会社）

出所）公開情報より三菱総合研究所作成

2.1.4 JIS Q 17050「適合性評価ー供給者適合宣言ー」の概要

自己適合宣言型認証の仕組みの検討にあたり、同じく自身が適合性を宣言する「JIS Q 17050「適合性評価－供給者適合宣言－」の概要」について調査を行った。

JIS Q 17050 の規格群は、供給者適合宣言に対する一般要求事項や宣言の裏付けに用いられる支援文書に対する一般要求事項を規定している。

- 適合性評価－供給者適合宣言－
- 第1部 一般要求事項 JIS Q 17050-1(2005), ISO/IEC 17050-1(2004)
  供給者適合宣言に対する一般要求事項を規定。
- 第2部 一般要求事項 JIS Q 17050-2(2005), ISO/IEC 17050-2(2004)
  供給者適合宣言の裏付けに用いられる支援文書に対する一般要求事項を規定。

適合宣言の目的は、「識別された対象が宣言書中の規定要求事項に適合しているという保証を与えること、並びにその適合及び宣言の責任者を明確にすること。」とされている。

また、供給者適合宣言に対する一般要求事項には必須項目と推奨項目がある。

【一般要求事項】

適合宣言の発行者は、適合宣言の発行、維持、拡大、縮小、一時停止または取り消し、及び対象の規定要求事項への適合に責任をもたなければならない。

適合宣言は、第一者、第二者、又は第三者の一つ以上が実施した適切な種類の適合性評価活動の結果に基づかなければならない。関与する適合性評価機関は、適用できる場合、該当する国際規格、ガイド及びその他の基準文書を参照することが望ましい。

適合宣言は、同類の製品群に対するものである場合、その製品群の個々の製品に適用されなければならない。適合宣言は、ある期間にわたって引き渡された同類の製品に対するものである場合、引き渡し時又は受領時の個々の製品に適用しなければならない。

適合性評価の適正実施基準として、適合性評価結果をレビューする要員は署名者と異なる者であることが望ましい。

出所）https://www.jisc.go.jp/index.html より引用

JIS Q 17050-1 では、適合宣言書に含むべき内容を規定している。

・適合宣言の発行者は、適合宣言の受領者が次の事項を識別するのに十分な情報を、適合宣言書が含んでいることを確実にしなければならない。

適合宣言の発行者
宣言の対象
適合を宣言する根拠とした規格又は代理署名者
適合宣言の発行者を代表する署名者又は代理署名者

・適合宣言書は、少なくとも次の事項を含まなければならない

適合宣言の固有の識別
適合宣言の発行者の名称及び連絡先住所　等々

・適合宣言の基礎とした適合性評価結果と宣言とを関係付けるため、例えば、次に示す追加の支援情報を提供してもよい

関与した適合性評価機関の名称及び住所
該当する適合性評価報告書の引用及びその報告書の日付　等々

出所）https://www.jisc.go.jp/index.html より引用

JIS Q 17050-1 文書には、規定の一部とはなっていないが、適合宣言書の様式例が示されている。適合宣言書の例については附属書 A を参照することとなっており、適合宣言は印刷物によるものでも、電子媒体又はその他の適切な媒体によるものでもよいとされている。


（この規格に従った）供給者適合宣言書

1) 番号：

2) 発行者の名称：
発行者の住所：

3) 宣言の対象：

4) 上記宣言の対象は、次の文書の要求事項に適合している：

	文書番号	表題	版数/発行日
5)			

追加情報：

6)

代表者又は代理者の署名：

（発行場所及び発行日）

7)

（氏名、役職名）　（発行者から権限を与えられた者の署名又は同等の印）

出所）https://www.jisc.go.jp/index.html より引用

図 2-17　供給者適合宣言書

JIS Q 17050-1 には、適合宣言書へのアクセス性や製品上へのマーク表示、宣言の有効性の継続に関する事項が記されている。

【アクセス性】

適合宣言書の写しを適合宣言の対象に関連する他の文書、例えば、声明書、カタログ、送付状、取り扱い説明書又はウェブサイトに含めてもよい。

【製品上へのマーク表示】

適合宣言の存在を示すために製品上に表示を行う場合、そのような表示は、他の何らかの認証マークと混同することのないような形式でなければならない。このような表示は、適合宣言へのトレーサビリティがなければならない。

【適合宣言の有効性の継続】

適合宣言の発行者は、引き渡し時又は受領時における対象が、適合宣言書に表明された要求事項に対して引き続いて適合することを確実にするための手段をもち、実施しなければならない。

適合宣言の発行者は、次に示す状況が生じた場合に適合宣言の有効性を再評価するための手順をもち、実施しなければならない

対象の設計又は仕様に重大な影響を与える変更

対象の適合を表明する根拠となる規格の変更

該当する場合、供給者の所有権又は経営構造の変更

対象がもはや規定要求事項に適合していない可能性を示す関連情報の存在

2.2 制度改正の改善に向けた資料作成

認証プロセスにおいては、3 年間の有効期間中は毎年定期報告を求めることを想定しているが、当該報告を効果的・効率的に行うためのフォーマットについて、他認証制度を参考にしつつ、認証機関や担当者と協議の上で定めた。

2.2.1 関連制度における定期報告・審査の状況

（1） ISMS におけるサーベイランス審査

ISMS におけるサーベイランス審査の概要は以下の通りとなっている。

- 目的：
  被認証組織の認証されたマネジメントシステムが、継続して要求事項に対して適合していること、及び有効性があることを確認すること。
- 審査間隔及び審査時期：
  「基準日」（通常は初回審査の際の認証日）を起算日として年 1 回以上、原則として 12 ヶ月毎に実施。顧客から要望がある場合には、6 ヶ月毎に実施可能。
  ただし、初回認証に続く最初のサーベイランス審査の期日は、初回審査の第二段階審査の最終日から 12 ヶ月を超えないものとする。
- サーベイランス審査の事前調査：
  認証機関は、前回の審査後の変更事項の有無の確認を含めた審査計画の調整を行う。
  変更事項のある場合、顧客に「認証内容変更申請書」の提出を求める。
- 審査計画書（サーベイランス審査）の作成：
  事前調査結果を基に、認証機関は審査計画書を作成する。
- 審査計画書（サーベイランス審査）の実施：
  審査計画書（サーベイランス審査）に基づいて実施する。次の事項についての評価を行う。
  - ア. 内部監査及びマネジメントレビューのプロセス
  - イ. 前回の審査で特定された不適合についてとられた処置の有効性のレビュー
  - ウ. 苦情の処理
  - エ. 顧客の目的達成に関するマネジメントシステムの有効性
  - オ. 継続的改善を狙いとする計画的活動の進捗状況
  - カ. 運用管理に関するマネジメントシステムの有効性
  - キ. 情報セキュリティマネジメントシステムの変更の有効性に影響を及ぼすか又は影響する恐れのある変更内容に関する情報
  - ク. 認定シンボル等の使用及び認証に関する引用

  不適合については、是正処置要求書（CAR）を発行する。不適合ではないが、審査中気づいた改善事項については、気付事項をあげる。
- サーベイランス審査報告書の作成：
  サーベイランス審査終了後、審査報告書（暫定版）を作成し、顧客に提出し、報告書に対する顧客の意見を求める。

- 不適合の修正及び是正処置：
  不適合がある場合、不適合の修正及び是正処置を検討いただき、不適合の修正及び是正処置の計画又は実施が完了したら、認証機関に連絡と次の資料の提出をいただく。
  - ア. 是正処置要求書
  - イ. 修正・是正処置回答書
  - ウ. 修正及び是正処置の証拠治しての文書又は記録の該当部分
  - エ. 情報セキュリティマネジメントシステム文書リスト（変更がある場合）

  提出書類を確認し、十分であれば、確認結果を記入した「是正処置要求書」及び「修正・是正処置回答書」をつけて「審査報告書」を作成し、認証の維持の可否の判定に進む。
- 認証維持の可否の判定及び通知：
  認証維持の可否の判定は、審査報告書にも基づき行われる。
  変更審査を兼ねて実施した場合は、マネジメントシステム判定委員会において判定が行われる。
- 審査費用の請求と納付：
  認証の維持の可否の判定が行われた後に、顧客にサーベイランス審査料を請求する。

なお、サーベイランス審査時に確認される項目は以下の通りである。

- 組織の現状把握
- 情報セキュリティリスクアセスメント
- リスク対応計画
- 目標の管理
- 教育
- 内部監査
- マネジメントレビュー
- 是正処置とインシデント対応報告

（2）プライバシーマーク更新審査

プライバシーマークの更新審査に必要な書類は以下の通りである。

＜必須＞

No.	申請書類
0	【申請様式 0 更新】プライバシーマーク付与適格性審査申請チェック表
1	【申請様式 1 更新】プライバシーマーク付与適格性審査申請書（代表者印の捺印必須）
2	【申請様式 2 更新】事業者概要
3	【申請様式 3 更新】個人情報を取扱う業務の概要
4	【申請様式 4 更新】すべての事業所の所在地及び業務内容
5	【申請様式 5 更新】個人情報保護体制
6	【申請様式 6 更新】個人情報保護マネジメントシステム文書の一覧
7	【申請様式 7 更新】JIS Q 15001 との対応表
8	【申請様式 8 更新】教育実施サマリー（全ての従業者に実施した教育実施状況）
9	【申請様式 9 更新】内部監査実施サマリー（全ての部門に実施した内部監査実施状況）
10	【申請様式 10 更新】マネジメントレビュー（事業者の代表者による見直し）実施サマリー
11	【申請様式 11 更新】前回付与適格決定時から変更のあった事業の報告
12	最新の個人情報保護マネジメントシステム文書一式の写し （【申請様式 6 更新】、及び【申請様式 7 更新】に記載の内部規程・様式の全て。 なお、様式は未記入で空欄のままの見本。）
13	個人情報を特定した台帳、いわゆる「個人情報管理台帳」の運用記録（様式ではない）の冒頭 1 ページの写し
14	上記 13 に対応する、いわゆる「リスク分析結果」の写し

＜該当する場合＞

15	登記事項証明書（「履歴事項全部証明書」または「現在事項全部証明書」）等申請事業者（法人）の実在を証す公的文書の写し
16	定款、その他これに準ずる規程類の写し
17	変更報告書（前回の付与適格決定後に「事業者名、本店所在地」に変更があったが変更報告書を提出していない場合は必須）

＜任意＞

18	教育を実施したことが確認可能な記録一式（「教育計画書」「教育実施報告書」等の運用記録や教材の写し、「理解度確認テスト」等の雛形） ※注 1 ※注 2
19	内部監査を実施したことが確認可能な記録一式（「内部監査計画書」「内部監査実施報告書」「内部監査チェックリスト」等の写し） ※注 1 ※注 2
20	マネジメントレビュー（代表者による見直し）を実施したことが確認可能な記録一式（「マネジメントレビュー議事録」の写し） ※注 1
21	会社パンフレット等

注 1：これらの書類を事前に提出すると、現地審査当日の審査がより効率・効果的となり、審査の所要時間の短縮化につながる。

注 2：教育や監査の記録については、実施したことが確認できればよく、それぞれ数ページ分の写しを提出する。

（3）主な法定点検

各種法律に基づき、法定点検が求められる設備がある。多くは、専門の資格を有する者によって点検を実施することが求められている。

◆主な法定点検一覧表

区分	点検対象物	点検周期	内　容	点検資格者	対象の詳細
建築基準法	・敷地関係 ・構造関係 ・防火・避難関係	3年に1回（一定規模以上の劇場・ホテル等は毎年〔各自治体条例による〕）	敷地・構造・建築設備に関する定期調査	建築士（1、2級）または特殊建築物調査資格者、昇降機検査資格者等	階数5以上、延べ面積1000㎡以上の建物で特定行政庁が指定する建築物等
	・換気設備（火気使用室・無窓居室） ・排煙設備 ・非常用照明装置 ・給排水衛生設備（ビル管理法・水道法で指定する給排水設備を除く）	1年に1回	定期検査		
	昇降機：・エスカレーター ・小荷物昇降機 ・エレベータ	1年に1回（毎月自主点検）	昇降機の定期検査		特定行政庁が指定する昇降機等（労安法で指定するものを除く）
労働安全衛生法等	昇降機：・エスカレーター ・小荷物昇降機 ・エレベータ	1年に1回（毎月自主点検）	昇降機の性能検査	昇降機検査資格者等	工場等のもっぱら生産過程のエレベータで積載荷重1トン以上のもの
	・照明設備	半年に1回	照度の測定	—	労働者を常時就業させる場所・事務所
	・機械換気設備	2ヶ月に1回	点検	—	—
	空調設備：・中央管理方式の空調設備	2ヶ月に1回	一酸化炭素含有率等の検査	—	事務所の用に供される部屋
ビル管理法	空調設備：・空調用設備（冷却塔、冷却水管、加湿装置）	毎月1回	点検	—	延面積3000㎡以上の事務所・店舗・百貨店・集会所・興業場・図書館等、および延面積8000㎡以上の学校
		1年に1回	清掃	—	
	・衛生環境	2ヶ月に1回	空気環境の測定	—	
		半年に1回	建物内の定期清掃	—	
			鼠・昆虫等の防除	—	
	・給排水設備	半年に1回	水質検査	水道技術管理者等	
		1週間に1回（一部は2ヶ月に1回）	有利残留塩素等の測定		
		1年に1回	貯水槽の清掃		
		半年に1回	排水設備の清掃		
消防法	消防設備：・消火設備 ・警報設備 ・避難設備 ・非常用電源	半年に1回	外観・機能の作動点検	政令指定のものは消防設備士または消防設備点検資格者、それ以外のものは自主点検	防火対象物に設置されている設備
		1年に1回	総合点検		

区分	点検対象物	点検周期	内　容	点検資格者	対象の詳細
水道法	・給排水設備	1年に1回	貯水槽の清掃	各自治体または厚生労働大臣の指定する者（水道技術管理者等）	受水槽の有効貯水用が10立方メートルを超えるもの
		1年に1回	貯水槽設備点検		
		異常を認めたとき	水質検査		
水質汚濁防止法	・厨房施設 ・洗浄入浴施設	日平均排水量により異なる	排出水の測定	—	300床以上の病院の洗浄入浴施設、および厨房施設、業務に供する総床面積420㎡以上の飲食店の厨房施設等
浄化槽法	し尿処理設備 ・浄化槽	日平均排水量により異なる	水質検査	登録業者または浄化槽管理士等	処理対象人数が500人を超えるし尿浄化槽、および指定地域特定施設の浄化槽
		使用開始後6か月時点、以後1年に1回	水質検査		—
	・単独処理槽 ・合併処理槽	処理対象人数および処理方式により異なる	保守点検		
		全ばっ気方式はおおむね半年に1回、それ以外の方式は1年に1回	清掃		
ガス事業法	・ガス設備	3年に1回（通産大臣の許可を受けた場合はこの限りではない）	消火機器の技術上の基準適合性の調査（大口排気を除く）	ガス事業者	ガス湯沸器とガス風呂釜、およびその排気筒・排気扇（例外あり）
電気事業法	・自家用電気工作物	毎月1回	定期点検	電力会社、電気技術主任者等	電力会社から6kV以上の高電圧で電気を受け、自前で変電設備を設けている施設
		1年に1回	年次点検（停電を伴う）		

※このほか、ボイラー施設、焼却炉、圧力施設、危険物の貯蔵槽などを施設内に設置する場合には、大気汚染防止法、ダイオキシン類対策特別措置法、消防法、高圧ガス保安法などが規定する法定点検の義務が生じます。
※点検実施にあたっては、最新の法令をよく確認し、各専門業者のアドバイスを受けてください。

出所）http://www.subarusya-linkage.jp/img/b-template/jisha/download/p309.pdf

図 2-18　主な法定点検一覧表

定期検査報告に関連する法令は、建築基準法、建築基準法施行令、建築基準法施行規則、昇降機に係る告示等、東京都建築安全条例（東京都の場合）、東京都建築基準法施行細則（東京都の場合）などがある。

建築基準法では、建築物の所有者又は管理者の義務として、法第8条において「建築物の所有者、管理者等は常時適法な状態に維持するよう努めなければならない。」と定められている。

同様に、建築基準法第 12 条 3 項により所有者は、当該建築設備について国土交通省令で定めるところにより、定期に、一級建築士若しくは二級建築士又は昇降機等検査員資格者証の交付を受けてい

る者に検査をさせて、その結果を特定行政庁に報告するよう定められている。

また、昇降機や遊戯施設の安全性の確保のため、法に基づく定期検査を行っていることを明らかにするとともに、利用者に「安心」、「安全」を提供することを目的として、利用する昇降機等の見えやすい位置に、「定期検査報告済証」を掲示することとされている。

● 対象となる昇降機等

1. 建築物に設けた昇降機(年1回)
- エレベーター
- エスカレーター
- 小荷物専用昇降機(テーブルタイプは除く)
- 段差解消機
- いす式階段昇降機乗用エレベーター又はエスカレーターで観光のためのもの(一般交通用に供するものを除く)

2. 遊戯施設(年2回)
- 観覧車
- ジェットコースター
- ウォータースライド
- メリーゴーランド
- その他の遊戯施設

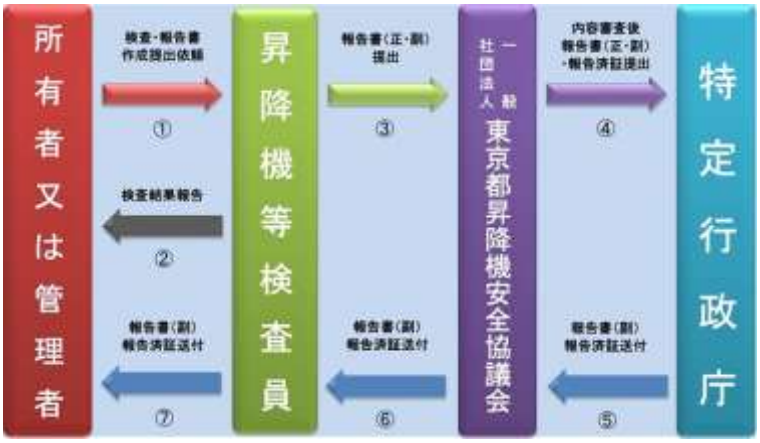
● 報告者
- 報告義務者は、報告を行わければならない昇降機等の所有者又は管理者(所有者からその昇降機等について維持管理上の権限を委任された方)の方

※ ホームエレベーター等個人住宅内に設置された昇降機については報告を要しない。
※ 労働安全衛生法に基づく性能検査を受けている昇降機については報告を要しない。

出所)https://www.beec.or.jp/report/about/
http://www.tsak.jp/report/

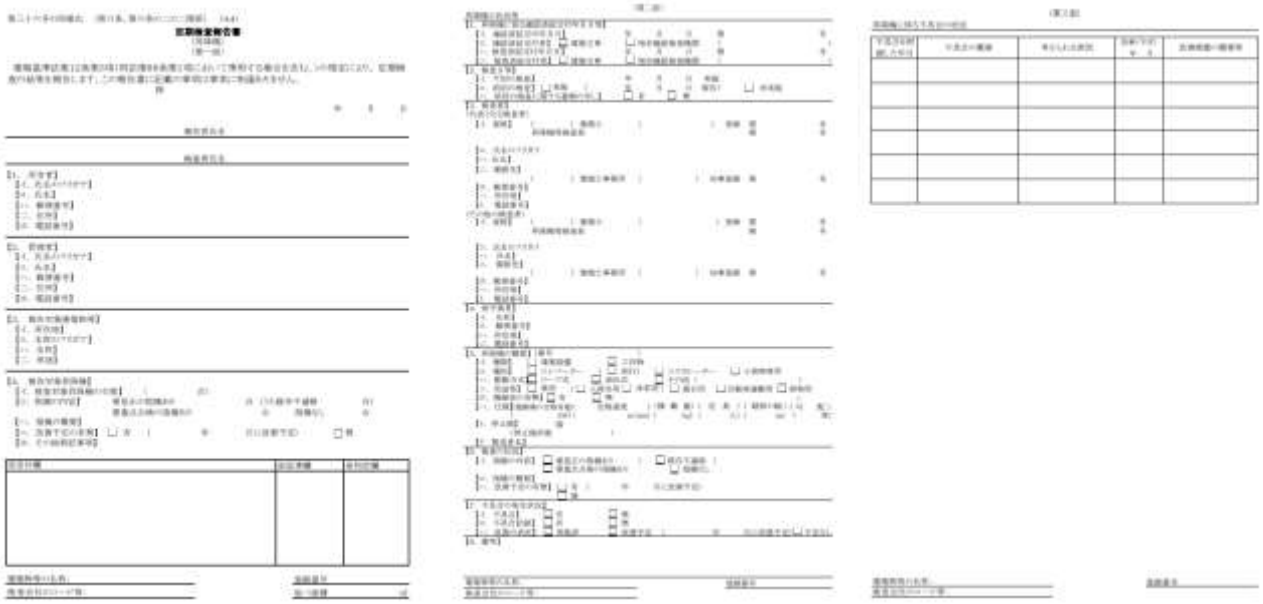
図 2-19　法定点検(昇降機等)における対象と報告者

東京都昇降機安全協議会では、東京都内の35特定行政庁から業務委託を受け、定期検査報告書の受付、予備審査等の業務を行っている。



出所)http://www.tsak.jp/report/ (東京都昇降機安全協議会)

図 2-20　定期検査報告の流れ(昇降機の場合)



出所）http://www.tsak.jp/publication/index.html#01

図 2-21 定期検査報告書様式（昇降機） 第一面から第三面

- 昇降機定期検査報告書は「昇降機・遊戯施設定期検査報告業務基準書（2017年版）（一財）日本建築設備・昇降機センター発行」に基づき作成される。
- 「東京都昇降機等定期検査報告実務マニュアル2020年版」では、昇降機検査結果表を作成する際の留意事項をわかりやすくまとめている。

出所）http://www.tsak.jp/publication/index.html#01

図 2-22 定期検査報告概要書様式（昇降機） 第一面・第二面

2.2.2 定期報告様式の検討

（1） 関連制度の調査結果

技術情報管理認証制度における定期報告様式を検討するにあたり、関連制度における定期報告の有無とその位置づけ・内容について確認した。

調査の結果、ISMS はマネジメントシステムの認証であることから、次の更新までにサーベイランス審査（毎年の審査）があり、継続して要求事項に対して適合していること、及び有効性があることを認証機関が確認・審査を行う。そのため、企業では、審査に必要な情報として、内部監査報告書を含む、各種規約・文書・記録等を提出する。各項目への対応状況は監査結果として一覧化される。

プライバシーマークでは、2 年に一度の更新時に審査に必要な書類を提出する。毎年の報告はないが、更新時の審査に必要な書類に、内部監査実施サマリー、教育実施サマリー、マネジメントレビュー実施サマリー（及びこれらを実施したことが確認可能な記録一式）が含まれる。これらは、実質的に毎年実施する必要があるため、毎年の報告はないものの、実施記録を毎年自身で作成することが必要となる。

その他、法令に基づく設備の定期点検状況について定期報告する制度がある。設備の定期点検では、検査状況や是正の指摘の有無・内容、不具合の有無・内容、改善状況・予定等について報告書に記載する。

（2） 定期報告内容策定にあたっての方針

技術情報管理認証制度が毎年求めるのは、審査（適合性の評価）ではなく、実施状況の報告である。

プライバシーマークは、更新審査の際に（更新までの）実施状況を提出しており、技術情報管理認証制度で求める内容は、プライバシーマークの報告内容が近いと考えられる。

プライバシーマークでは、2 年毎の更新時に内部監査実施サマリー、教育実施サマリー、マネジメントレビュー実施サマリー（及びこれらを実施したことが確認可能な記録一式）を提出することから、実質的に毎年の内部監査・教育・マネジメントレビューの実施記録作成が必要となっている。

そこで、技術情報管理認証制度における定期報告時に必要な項目として、関連制度の審査・報告項目を踏まえつつ、主としてプライバシーマークにおける毎年の実施事項における記録項目を参照することとした。技術情報管理認証制度では、マネジメントレビューは要求しておらず、教育は監査項目に含まれることから、主として内部監査における記録内容が参考にできると考えられる。一方、事業者及び認証機関に対して、告示で求める事項以外の対応を必須として求めることはできないこと、また、認証制度をスムーズに運用継続することを考慮し、可能な限り制度運用上の柔軟性を持ちつつ、既存の書類を活用した様式とすることとした。

結果的に、定期報告時の提出書類は、認証取得・更新時に作成する「チェックシート」の更新版とすることとした。

	ISMS	Pマーク	法定点検
審査時の確認項目	● 組織の現状把握 ● 情報セキュリティリスクアセスメント ● リスク対応計画 ● 目標の管理 ● 教育 ● 内部監査 ● マネジメントレビュー ● 是正処置とインシデント対応報告	● 個人情報保護体制 ● 個人情報保護マネジメントシステム文書の一覧 ● JIS Q 15001対応表 ● 教育実施サマリー ● 内部監査実施サマリー ● マネジメントレビュー ● 変更のあった事業の報告 ● 個人情報保護マネジメントシステム文書一式(写) ● 個人情報管理台帳の運用記録(写) ● リスク分析結果(写)	● 定期検査報告
うち、監査や検査関連書式の記載事項	● 内部監査計画(監査対象(部門等)、スケジュール、監査員、監査項目) ● 内部監査チェックリスト(監査項目、確認内容、監査結果) ● 内部監査報告書(監査対象、監査員、実施日時、監査内容、結果(指摘事項や改善提案事項等))	● 内部監査実施サマリー(監査実施日、監査員、指摘事項、改善指示事項)	● 定期検査報告(報告者、点検者、検査対象、指摘内容、改善予定の有無)

図 2-23 関連制度における定期審査・報告時の記載事項

技術情報管理認証制度に係る検討会及び運用ワーキンググループの議論を踏まえ、技術情報管理認証制度における定期報告様式については、認証取得・更新時に作成する「チェックシート」の項目を更新する形式とした。チェックシートは認証機関ごとに異なることから、「チェックシート」とほぼ同等の様式である「監査の指針」に記載した「監査記録例」を参照し、「報告様式ひな形」を定めた。ただし、告示として「報告様式ひな形」を一律に定めるのではなく、技術情報管理認証制度のホームページ等の告示以外で「報告様式ひな形」を示し、ひな形を元に、各認証機関が様式を定められるものとした。

告示の修正案においては、認証取得事業者には、認証の有効期間内においても、定期報告の周期又はその認証に係る苦情等に対応するために必要な時期において、認証機関による技術情報漏えい防止措置基準に定められた措置に適合していることの確認を受けることを求めた。また、告示には、認証機関は、その確認を受けることを認証取得事業者が拒否した場合や然るべき報告がなされない場合、対応を求め、その対応が行われない場合には、認証取得事業者に対し、認証証明書の認証機関への返納、認証を取得したことを他者に知らしめる文書からの掲載の撤廃等を求めることがあると記載した。定期報告を行わない認証取得事業者に対して、報告が行われない場合には認証を取り消すことを伝え、提出を促すこと等は可能となる。

そのため、認証取得事業者からは、正しい記載がなされた報告が提出されることを前提に、報告において基準を満たしていることが示されていることを確認すればよいという前提で報告様式ひな形を定めた。

ただし、認証取得事業者が確認事項について責任をもって正しく記載することを促すために、各項目において確認者の氏名・確認日を記載することを求めるものとした。事業者が定期的に自己確認を行い、自主的に対策の見直し・改善を継続するためには、内部監査を行うことが有効であるため、事業者において内部監査が可能な体制を整え、内部監査人を育成することが望ましい。ただし、本制度の自己確認における確認者は、監査人か否か、内部のものか外部の者か等、定めることはしない。

その他、検討会及び WG の議論においては、以下のような意見があった。

- 認証取得事業者自身による確認の結果、課題が見つかった場合には、それに対してどのように対応したかまで定期報告の資料に記載した方がよい。そうすれば、認証機関も報告に対して信頼を持つことができ、更新の際に、記載された対応が実施されているかについて確認を行い、更新を認めることができる。
- 認証取得事業者及び認証機関の確認の負荷を軽減することが目的ではないが、審査時からの「変更無し」等の記載も認めることでよい。
- 毎年全ての項目についての報告を求めるのではなく、3 ヵ年で少しずつ確認していくことや、経営者が確認しなくても良いと判断した項目は理由を記載すれば対象外とする等も含め、報告対象とする項目に関しては柔軟性を持たせるべきである。
- 確認日と確認者については別紙にまとめて記載する等、記載方法に関しても、柔軟に定めてもよい。
- 企業規模によっては内部監査員を自社で保持することが難しい場合もあるため、一律に内部監査を要求するのは厳しいだろうが、内部監査と同等の内容が報告されるよう、確認方法や報告の書き方について記載された定期報告のガイドラインを作成するとよい。

そのため、今後、定期報告に関するガイドラインを定め、確認方法や報告の記載方法について指針を示すことで、適切な定期報告が行われることを促していくことが有効と考えられる。

なお、定期報告の際、各認証機関において追加的なサービスを行うことを妨げるものではない。すなわち、制度の中で定期的なサーベイランス（審査）を行うことを妨げるものではなく、また、定期報告のタイミングに合わせて指導助言を行うことは、審査と指導助言を切り離すことが前提であれば問題ない。

表 2-7 定期報告様式ひな形

										審査	定期報告		
章	節	項	番		内容					確認内容	確認内容	確認日	確認者
I	第四	1	(1)		共通事項	管理対象情報の管理等	管理対象情報の管理簿の作成等	管理者は、持ち出し、複製、廃業等の管理対象情報の状況を管理するための管理簿を作成する。					
		6	(1)				管理対象情報の適切な管理についての文書の作成等	事業者は、1から5までに定める手順のほか、第二の2により必要と決定した措置を実施するため、管理対象情報の適切な管理についての具体的な実現手法を記載した文書（以下「マニュアル」という。）を作成する。					
			(2)					事業者の取締役等の経営層（管理対象情報を活用し、事業を実施する部門の長を含む。）は、マニュアルを、当該管理対象情報を取り扱う可能性のある全ての者に周知する。					
	第六	1				管理対象情報の漏えいの事故等の発生時等の報告		事業者は、アクセス権者を含む全ての従業員等に対して、管理対象情報へのアクセス権を有さない者がアクセス権者の近傍にいない状態で管理対象情報を取り扱っていることを発見した場合等当該管理対象情報の漏えいが発生し、又はその疑いがあると従業員等が認める場合に、直ちに、管理者等当該事業者が報告先として指定した者に報告をさせるための手順を確立する。					

2.3 有識者会議・ヒアリング等の運営・実施

認証制度に関係の深い有識者を集めた会議を設置し、認証制度の現状・課題の分析や本事業の実施内容・手法等の有効性や改善点等について議論した上で、当該議論の結果を踏まえた事業とした。また、認証機関等実務者から構成されるWGを設置し、当該WGでの議論を取りまとめた。

また、有識者会議に加え、知的財産管理や技術管理に係る有識者に対して認証制度の在り方についてのヒアリングや、認証制度の普及が望ましい業界団体・業界に属する事業者に対して認証制度の在り方についてのヒアリングを実施した。

2.3.1 技術情報管理認証制度に係る検討会

（1） 設置目的

グローバルな競争が進む中、技術情報を適切に管理することは、事業者間での技術等の情報の共有を円滑にし、イノベーションを促進する重要な要素となっている。一方で、多くの事業者、特に中小事業者にとっては、重要な技術情報の特定や当該技術情報の管理の整備については、十分に進んでいるわけではないのが実情である。

経済産業省では、技術情報の管理として必要となる項目を国として基準で示し、当該項目を満たしたことを国が認定する第三者が認証する制度（産業競争力強化法に基づく技術情報管理認証制度。以下、「認証制度」という。）を創設し、認証制度の普及を進めていくことによって、事業者、特に中小事業者の技術情報の管理の理解醸成や、管理能力の底上げを図ることにより、もって我が国産業の競争力向上に資するイノベーション促進の環境を整えることを意図している。

この普及を進めていくため、今年度は、認証制度の普及促進に向けて必要となる認証制度の在り方についての調査分析、認証制度の取得を進めるための専門家派遣等の事業者への支援、普及のための広報等を行う「産業競争力強化法に基づく技術情報管理認証制度の普及促進に向けた調査分析及び専門家派遣等事業」（以下、「本事業」という。）を実施するところ、本事業を適切に実施していくためには、産業界、有識者、関係機関からの意見を踏まえて進める必要がある。

上記の背景を踏まえ、認証制度の現状・課題の分析や本事業の実施内容・手法等の有効性や改善点等について議論し、普及に向けた取組みの方向性について取りまとめるために、経済産業省から本事業の委託を受けた株式会社三菱総合研究所において、産業界、有識者、関係機関等を委員として意見を聴く場として「技術情報管理認証制度に係る検討会」を設置する。

（2） 設置期間

2021 年 7 月 20 日～2022 年 3 月 28 日

（3）委員

座長	田中 芳夫	一般社団法人ものこと双発推進　代表理事
委員	及川 勝	全国中小企業団体中央会 常務理事 兼 事務局長
	小川　隆一	独立行政法人情報処理推進機構　セキュリティセンター セキュリティ対策推進部　シニアエキスパート
	押田 誠一郎	独立行政法人中小企業基盤整備機構　経営支援部　部長
	土井 和雄	全国商工会連合会　政策推進部　事業環境課　課長
	永宮 直史	特定非営利活動法人日本セキュリティ監査協会 エグゼクティブフェロー
	比留間 貴士	特定非営利活動法人 IT コーディネータ協会　常務理事
	山内 清行	日本商工会議所　産業政策第一部　部長

（2022/3/28 時点、委員五十音順、敬称略）

（4）開催概要

1）第 1 回

表 2-8 技術情報管理認証制度に係る検討会 第 1 回会合

日時	2021 年 7 月 20 日(火) 10:00 ～ 12:00
場所	オンライン開催(WebEX)
議題	(1) 開会 (2) 経済産業省 挨拶 (3) 検討会の趣旨について (4) 検討会の取り扱いについて (5) 座長の互選 (6) 座長の挨拶 (7) 今年度の事業について (8) 今後のスケジュールについて

2）第 2 回

表 2-9 技術情報管理認証制度に係る検討会 第 2 回会合

日時	2021 年 10 月 4 日(月) 15:00 ～ 17:00
場所	オンライン開催(WebEX)
議題	(1) 開会 (2) 事業状況の中間報告について (3) 告示修正内容案について (4) 今後のスケジュールについて

3）第３回

表 2-10 技術情報管理認証制度に係る検討会 第 3 回会合

日時	2022 年 2 月 25 日(金) 15:00 ～ 17:00
場所	オンライン開催(WebEX)
議題	(1) 開会 (2) 事業状況の中間報告について (3) 告示修正内容案について (4) 今後のスケジュールについて

4）第４回

表 2-11 技術情報管理認証制度に係る検討会 第 4 回会合

日時	2022 年 3 月 24 日(木) 11:00 ～ 12:00
場所	オンライン開催(WebEX)
議題	(1) 開会 (2) 調査報告書(案)について

2.3.2 技術情報管理認証制度に係る検討会運用ワーキンググループ

（1） 設置目的

グローバルな競争が進む中、技術情報を適切に管理することは、事業者間での技術等の情報の共有を円滑にし、イノベーションを促進する重要な要素となっている。一方で、多くの事業者、特に中小事業者にとっては、重要な技術情報の特定や当該技術情報の管理の整備については、十分に進んでいるわけではないのが実情である。

経済産業省では、技術情報の管理として必要となる項目を国として基準で示し、当該項目を満たしたことを国が認定する第三者が認証する制度（産業競争力強化法に基づく技術情報管理認証制度。以下、「認証制度」という。）を創設し、認証制度の普及を進めていくことによって、事業者、特に中小事業者の技術情報の管理の理解醸成や、管理能力の底上げを図ることにより、もって我が国産業の競争力向上に資するイノベーション促進の環境を整えることを意図している。

この普及を進めていくため、今年度は、認証制度の普及促進に向けて必要となる認証制度の在り方についての調査分析、認証制度の取得を進めるための専門家派遣等の事業者への支援、普及のための広報等を行う「産業競争力強化法に基づく技術情報管理認証制度の普及促進に向けた調査分析及び専門家派遣等事業」（以下、「本事業」という。）を実施するところ、事業者等の認証取得を促すためには、認証制度の円滑な運用や認証機関の活動の充実が必要であり、関係機関からの意見を踏まえて進める必要がある。

上記の背景を踏まえ、技術情報管理認証制度の在り方の検討や普及に向け、制度運用に関わる課題

の洗い出しや改善の方向性について取りまとめるために、経済産業省から本事業の委託を受けた株式会社三菱総合研究所において、認証機関等を委員として意見を聴く場として「技術情報管理認証制度に係る検討会運用ワーキンググループ」を設置する。

（2）設置期間

2021 年 7 月 26 日～2022 年 3 月 28 日

（3）委員

委員	金森 喜久男	一般社団法人情報セキュリティ関西研究所　代表理事
	小橋 弘政	日本検査キューエイ株式会社　取締役
	高村 博紀	一般財団法人日本品質保証機構　認証制度開発普及室　主幹
	中里 栄	一般社団法人日本金型工業会　専務理事
	羽田野 尚登	株式会社日本環境認証機構 IS ビジネスユニット審査グループ長
	六畑 方之	公益財団法人防衛基盤整備協会　情報セキュリティ部長

（2022/3/28 時点、委員五十音順、敬称略）

（4）開催概要

1）第 1 回

表 2-12 技術情報管理認証制度に係る検討会運用ワーキンググループ 第 1 回会合

日時	2021 年 7 月 26 日(月) 17:00 ～ 19:00
場所	オンライン開催(WebEX)
議題	(1) 開会 (2) 経済産業省 挨拶 (3) 運用ワーキンググループの趣旨について (4) 運用ワーキンググループの取り扱いについて (5) 今年度の事業について (6) 今後のスケジュールについて

2）第２回

表 2-13 技術情報管理認証制度に係る検討会運用ワーキンググループ 第 2 回会合

日時	2021 年 9 月 28 日(火) 17:00 ～ 19:00
場所	オンライン開催(WebEX)
議題	(1) 開会 (2) 事業状況の中間報告について (3) 告示修正内容案について (4) 今後のスケジュールについて

3）第３回

表 2-14 技術情報管理認証制度に係る検討会運用ワーキンググループ 第 3 回会合

日時	2022 年 2 月 22 日(火) 13:00 ～ 15:00
場所	オンライン開催(WebEX)
議題	(1) 開会 (2) 事業状況の中間報告について (3) 告示改正案について (4) 今後のスケジュールについて

4）第４回

表 2-15 技術情報管理認証制度に係る検討会運用ワーキンググループ 第 4 回会合

日時	2022 年 3 月 23 日(水) 11:00 ～ 12:00
場所	オンライン開催(WebEX)
議題	(1) 開会 (2) 調査報告書(案)について

2.3.3 ヒアリング調査

（1） 認証制度の在り方に関するヒアリング調査

1）ヒアリング対象

知的財産管理や技術管理に係る有識者（4 名）

2）ヒアリング項目

(1)我が国の事業者における知財・技術情報管理に関する現状・意識について
(2)情報管理に関する認証制度の在り方、普及促進について
(3)知財・技術情報管理に関して必要な管理策について

3）結果概要

a. 我が国の事業者における知財・技術情報管理に関する現状・意識について

- 取引先にスペックを渡さなければならない場合など、技術情報管理はセンシティブにやっている。直接海外とやりとりをするのではなく、国内に渡して制作・納入してもらう場合に含まれている海外の管理が難しい。
- 大企業では、知財を見ている部署は社内の技術情報を把握しているが、管理は事業部毎に異なる。研究開発も事業部とは異なる。
- 知財関係部署とセキュリティ関係部署が連携するとよい。セキュリティ関係部署はセキュリティに特化しているので、技術そのものを見ている訳ではなく、何がクローズで何がオープンでよいのかどうかの判断はしない。
- 企業にとっては、どんな情報が重要で、何が秘密で何がオープンかの線引きが難しい。そのアドバイスができる専門家が必要である。知財がわかり、どういう技術が大事で、どこを秘密にした上で特許として公開するか、そういう訓練をしているような、弁理士を含めて、技術情報について詳しい方の支援が有効である。それが理解できた上で、どう管理するかはセキュリティ系の人が担当することになる。
- 企業において、NDA を結び、秘密保持義務は課すが、監査まで行っている企業はわずかである。情報漏洩があれば損害賠償請求を行うことになるが、対策の実態は見えず、漏洩リスクは下がっていないのではないか。監査の条項を入れることになかなか合意ができない。監査で見られても困るし、その場面では協業できたとしても、違う場面ではライバルになる場合もあり、当事者同士で見ていくことは難しい。そこで第三者認証のニーズはあるはず。
- 知財に関しては、問題意識を持っていても、契約の訴状に上がってこない。知財部は、特許、訴訟、商標等が業務範囲であり、営業秘密はあまり積極的ではなさそうである。契約交渉はどの部署が行うかも各企業でまちまちで、調達が自ら交渉する場合もあれば、事業部、法務部の場合もある。
- 知財部と法務部は仲が悪い場合もあり、セキュリティ関連部署は立場が弱いことも多いので、企

業においてこのテーマを発案をする人がそもそもいないのではないか。経営層から実施しないと取り組みが進まない。

- コーポレートガバナンスコードに知的財産が入ったため、経営層の目に入ると現場に指示が入る。現場の担当がやらざるを得ないとなると、契約交渉の必須項目になっていく。経営層も、善管注意義務違反に問われると必死になって対応しようとするため、うまく刺さる形で説明することが重要。
- 認証制度を取ろうと思っても、現場の担当者にインセンティブがない。面倒なことをやらなければならない。営業秘密でなくなってほしいのが本音だろう。担当者が評価されないことが普及しない原因にもなるのではないか。担当者がやれば報われるようなガバナンス、組織体制なども検討すべき。
- 知財戦略という形で、特許と営業秘密を使い分けるということを言われている。特許は権利化するのでわかりやすいが、外に出さない判断をした後、情報の特定がなされ、営業秘密保護のプロセスに乗るかというとそうではないのではないか。知財部の中で閉じて、関係部門への連携がなされていない可能性がある。営業秘密に関しては、関係部門と連携し、管理体制に乗せていくことが大事ではないか。
- 中小企業の製造業は仕事が属人的であり情報管理も属人的であるのが現状。専任された管理者しか知らないこともある。経営者の立場からしても、守るべき情報というより、その人の持っているノウハウが文書化されておらず、その人を守ることの方が大事になっている。危機感があるのは、外資系企業がお金を積んで引き抜いてしまうことだったりする。
- サプライチェーンにおいては、取引先から言われて対策を進めているのが実態。自動車産業もガイドラインを策定したので情報管理を進めているが、サプライチェーンの末端は伝言ゲームのようで、趣旨や実施事項が伝わっていない場合もある。
- 認証は取引先へのアピールとなるので、中小企業にとって取り組みやすいのではないか。
- 大企業では、情報管理・セキュリティ対策に関して、取引先への対策推奨を行っていることも多い。中小企業の情報管理の取組みを支援することで、レベルアップした中小企業は自信が持てている。
- 中小企業では、自社において何が営業秘密か、何が重要な情報かは意識されていないのではないか。

b. 情報管理に関する認証制度の在り方、普及促進について

- 企業において本制度の必要性を認識いただくために、機微情報の例示をしたり、中小企業と取引先との関係性を整理することが必要ではないか。分野、技術毎の例示、ヒヤリハットなどを作るとよい。狙いがサプライチェーン観点での底上げであれば、意識した上で、制度説明・セミナー、具体的なケース（例示）等が必要である。
- セキュリティや営業秘密はガイドラインができているので、逐一反映していかないと基準が古くなってしまう。意図して盗みに来た人をどう防ぐかと、一般的な営業秘密管理は対応が異なる。本制度で全てカバーするとなると、範囲も広くわかりにくいため敬遠されることになる。入口は軽くしておいて、ガイドラインがある領域は、受け渡すことにした方がよいのではないか。
- 制度が知られていないのが現状であり、認知がまず課題である。

- 当事者が認証制度を知っていないと使われないため、情報開示する大企業側から中小企業・スタートアップに対して求めれば使われるようになるのではないか。
- 時間がかかるようであれば取引が成り立たないので、必要な時に速やかに認証取得できることも必要。
- 認証制度が使われるようになると、不正競争防止法において、認証結果が証拠として出てくることになるだろう。裁判所が認めたという事例が出れば、認証取得企業は、勇気を持って権利行使できるようになるだろう。
- これをやれば事業が拡大する、という形でないと普及は難しいのではないか。製造業では、ISO9000 や 14000 などは認証取得が企業価値の向上につながったが、情報管理は難しいかもしれない。
- P マークは自治体中心に調達時に活用され、大企業も使うようになった。同じような流れを作ることが有効。
- 制度設計、すなわちインセンティブ設計すべきである。
- この制度は認識していなかった、まずは、認知度を高めることが望ましい。
- 商工会議所などとも連携することが望ましい。
- 取引先に対して情報管理に関するチェックリストを統一化していく方向性はあると思う。段階を付けるのであれば、格付けの発想となる。民間が独自に基準を作るより、国が基準を策定した方が信頼がある。調達側の理解とセットで考える必要がある。最も川下の業界ニーズに応えられるとよいのではないか。
- SECURITY ACTION と類似しているように見える。制度が乱立するのは望ましくないため、ISMS 等、類似した制度との違いなど、整理してわかりやすくすべき。
- IPA 中小企業セキュリティガイドラインとの整合性や、SECURITY ACTION、お助け隊サービス等との連携も考慮すべき。セキュリティから入ってきた中小企業と、TICS で営業秘密から入ってきた中小企業が、関連するテーマに対して意識を高め、双方の制度で取組みが活性化することが望ましい。

c. 知財・技術情報管理に関して必要な管理策について

- 人の管理は現場で行う必要があり、本制度に入れた方がよいだろう。営業秘密で議論するのは人の管理であり退職者からの漏洩をどう防ぐかや、立入禁止エリアに入れない等の基礎的なことを定めることが望ましい。逆に、人を管理しないセキュリティの高度な対策は別途とするとよい。
- IPA 秘密情報保護ガイドブックの改訂が進んでおり、間もなく公表されるので参照されるとよいだろう。
- H27 営業秘密指針が全面改訂されており、必須項目が古い印象を与える。アクセス制限と言う言葉が目立つが、昔の管理指針には結構出てきていたものの、現在アクセス制限は必須ではない。物理的なものの施錠が望ましいことはわかるが、よく使うものであればあるほど、保管する際に施錠するのが適切かどうかという課題はある。
- 共通事項の 1・2 項目目ができていれば、秘密管理性としては満たされる。3 以降については漏洩ができないようにという観点での取り組みであると考える。イコール営業秘密として保護されるものではない。ただし、必須項目として、取り組むべきことを定めた方がよいことは理解できるの

で、項目自体があることはよい。

- フォーカスが広いと取り組みにくい。ISMS・P マーク・営業秘密パンフレット等、様々な関連文書があるので、要件が漏れていないかより、矛盾がないかを確認した方がよい。
- チェックリストを埋めたときに、ISMS のチェックリスト上でも同じようなチェックが入り、P マークも同じように入るといった形で対応できるとよい。重要情報は追加されたチェックリストが発生するが、機密性が高い情報に対するルールと一致している等、営業秘密にフォーカスした方がよい。
- 告示への記載は、定める事項の大枠を決めて、施行規則のような文書は別参照するのがよいのではないか。
- 内部犯行にも対応していることはよい。想定する脅威と、それに対して何を要求しているかが整理され、わかりやすくなっているとよい。

（2） 認証制度の普及に関するヒアリング調査（業界団体）

1） ヒアリング対象

認証制度の普及が望ましい業界団体・業界に属する事業者（8者）

2） ヒアリング項目

(1)技術情報・知財管理に関わる現状、課題について
(2)情報管理に必要な項目について
(3)情報管理に関する認証制度の在り方、普及促進について

3） 結果概要

a. 技術情報・知財管理に関わる現状、課題について

- 業界として、鉄工系製造業と IT・ソフトウェア系企業があり、鉄工系は IT 系の知識がなく対策推進が難しい。中小企業が多く、IT 人材・セキュリティ人材が置けない。
- 顧客のセキュリティ意識は高い方。業界としてセキュリティへの理解がある企業も多く、ガイドに従って社内で対策する企業も増えたが、認証取得まではいかない。
- 情報管理/セキュリティに対するモチベーションが働かない。P マークのように顧客に PR できるとよいが、本認証制度はまだ認知度が低く、ブランドバリューがない。
- 多くの中小企業では、自社にとってその情報が重要なのかそうでないのか、把握して切れておらず、情報管理の取組みには積極的でない。
- 技術力でビジネスをするのではなく、ある商品と異なる売り方・マーケティング手法でオリジナリティを出すことが強みの企業にとっては、スピード感が大事であり、情報管理がなじまない。
- 文書管理の観点では、欧米ではレコードマネージャーという役割の人がコントロールするは、日本は文書管理というとサーバに入れて終わりであり、管理がなされていない。
- 業界団体として業界の情報管理を進めるような取組みはなく、個社で取り組んでいるのが実態。

- 業界は大手から数名の企業まで幅広いため、一律に情報管理に取り組むのは難しい。
- 取引先におけるセキュリティ担保は機密保持契約だけであり、本当に守れているのかはわからない。具体的な守り方までは見られていない。認証が活用できるならばよい。
- 委託先に対して情報セキュリティの要求は出していかなければならないとは考えている。NIST SP800-171 をベースに進めようとしている。
- 防衛系のお客様がいる企業では、厳しいレベルで社内規定を作り、情報管理を行っている。お客様毎に管理できる体制が整っているが、全社としては厳しいお客様にレベルを合わせてしまうことが課題。
- 純粋な紙の時代は管理できていた面もあった（発出時、受入時に捺印して確認）が、電子化により管理が難しくなっているのではないか。分類した後の扱いがコントロールできておらず、保存の仕方が徹底されていない。

b. 情報管理に必要な項目について

- 貿易管理規定を網羅しているので特に違和感はない。
- 人的、物理的は対策の考え方は ISO 15408 の環境セキュリティの考え方とも一緒であるし、担保する教育・ルールの支えがあればこのような項目であろう。
- 情報は社内に散在しており、管理は個人のリテラシーに依存するので、末端まで教育することが重要である。
- トレーニングはより具体的に定義した方がよい。情報管理だけ抜き出してやった方が効果があると考える。
- 怪しい兆候を見つけること、ログのチェック等が必要ではないか。
- 基準がカタログ的に使えて、どんな脅威があって、守るべきは何、それに対してどういう対策を取るというときに、カタログから選んでチェックするとすれば、使えるだろう。汎用的に使う場合は、ある程度の項目をカバーしていないと厳しいだろう。
- ある程度コントロールできる組織は抽象度の高い項目でもよいが、わからない組織には細かいレベルで選択できるとよい。実施事項がこれしかないとなると使いづらいが、難易度があって重要度によって変えることができる等であるとよい。例示や、その特徴・解説があるとわかりやすいと考える。

c. 情報管理に関する認証制度の在り方、普及促進について

- セキュリティはコストとしか見られていないが、重要ということを示すには、トップダウンで進めることが必要。
- 委託先に要求するのであれば、委託元がこれを使う必要があり、委託元にもメリットがあるかどうかが重要。
- 制度のブランド化により、取引において活用される仕組みとなっていくことが望ましい。いかにビジネスにつなげるかが重要である。
- 認証取得により、設備投資等で優遇されるのは望ましい。
- 他の業界のインシデントに関する情報共有など、企業が興味を示すような取組みを進めてはどう

か。

- ISMS に取り組む企業もいるが、そこまでではない企業がほとんど。過年度の事業で構築した業界モデルは、自社が取り組んでいない箇所を確認し、対策を進めるために活用している。業界としてのガイドラインはない。
- 業界団体が認証を進められるかどうかは、マーケットサイズ次第ではないか。専属スタッフを 2 名置くなら 2,000 万円ぐらいの市場規模が必要。一度始めたら簡単にはやめられないことも躊躇する理由。十分な人材を置いている業界団体は少なく、自主事業で収入を得ている団体はまれである。機械製造業はどの業界団体もよく似ているので、どこかの組織が束ねてやるという方向性はあるのではないか。

（3） 認証制度の普及に関するヒアリング調査（制度運用事業者）

1） ヒアリング対象

認証制度や類似制度の運用事業者（2者）

2） ヒアリング項目

(1)制度設計において普及のために考慮した点
(2)普及のための各種取組と効果、普及のポイント
(3)普及における課題と解決方法
(4)本制度に対するご意見

3） 結果概要

a. 制度設計において普及のために考慮した点

- 第三者認証の信頼性確保のために、コンサルティングを担った場合の審査に関するルールを定めている。
- 利用者のインセンティブを意識し、NISC の政府統一基準に載せた。大きな転機になったのは、無料で登録できていた情報セキュリティ監査企業台帳の廃止である。情報セキュリティサービス審査登録には費用がかかるため、本気でサービスを提供する意志のある企業しか登録しなかったことで、品質に対する信頼性が高まった。
- 制度を作る際、関係団体の代表を審議の場に迎え入れ、どのような要件にすればよいか、相談しながら策定した。また、基準ができ次第、各団体に向けて説明会を行い、制度の認知度を高めた。
- 地方公共団体の情報セキュリティ戦略の整備の基本方針が 2019 年 2 月に改訂されたが、そこで情報セキュリティサービス基準適合サービスリストを参照するよう記された。

b. 普及のための各種取組と効果、普及のポイント

- 審査員に対しては、筆記試験と審査（実地訓練）がある。試験内容は、制度に関する知識、関連

法規等である。研修会において審査員を育成している。地域事務局における普及プログラムは複数ある。

- 当初は登録料と審査料をまとめていたが、審査を受けたものの登録は辞退した企業や審査に落ちてしまった企業に配慮し、分けることにした。このように、企業にかかる負荷をできる限り小さくしようと努めた。
- 毎年、本制度に関する検討会において、要件の見直しや地方に対する振興策等、普及に関する検討を行っている。制度に関するユーザーアンケートや事業者アンケートを実施しており、それ自体も普及策の一つと言える。
- 政府情報システムのためのセキュリティ評価制度（ISMAP）の監査機関に対する要求事項に、情報セキュリティサービス基準適合サービスへの登録が含まれたことも、普及の観点で大きな要素だった。

c. 普及における課題と解決方法

- 制度開始から二十年近くが経過しているため、若い世代の審査員を増やしたい。より広い中小企業に対するメリットが重要と考える。
- 本当に重要な制度であれば、我慢をして地道な活動を行うフェーズが必要であり、芽が出るまでの 5 年間を乗り越えられる体制を作ることが求められる。また、その体制の中心となる人材を探すことも大切である。国の支援がある間に、持続的に回る組織や制度を作り上げなければならない。

d. 本制度に対するご意見

- カーボンニュートラルの流れもあり、環境保護の取組みが義務化される動きもある。時代背景や社会の要請が変わると、情報管理における認証取得の意向も変わってくると考えられる。
- 情報セキュリティ監査制度においては、登録料を監査人の方にお支払いいただいている。専門家派遣についても、そういった資格によるビジネスを考えれば良いのではないか。
- 認証制度に合わせて中小企業が技術的に困っていることを支援するのはどうか。例えば、技術情報は全てクラウドで管理すれば、審査では ID や現物の管理のみを評価することとなる。そのため、審査をする側とされる側、どちらの負担も軽減できると考えられる。
- 基準は 3～5 年に 1 回は見直しが必要であるため、内規として持つ方がやりやすいのではないか。
- 経営者が自分事として捉えられるよう、事例を集めると良いのではないか。
- 技術情報管理認証制度において、次のターゲットとなる業界のイメージを持つべきである。技術情報管理や経済安全保障の観点で、脅威に晒されて特に困る産業や日本として守るべき分野について、検討を行った方が良い。

（4） 認証制度の普及に関するヒアリング調査（中小企業）

1） ヒアリング対象

情報管理に積極的に取り組む中小企業（3 社）

2） ヒアリング項目

（1）知財・技術管理に関わる意識、状況、課題
（2）知財や技術情報管理に必要な項目
（3）情報管理（情報セキュリティ）対策に関わる大凡の費用感
　（認証取得事業者様の場合）認証取得前後で費用面の変化
（4）技術情報管理認証制度の在り方に対するご意見、普及に向けて必要な事項

3） 結果概要

a. 知財・技術管理に関わる意識、状況、課題

- 2017 年頃、日経新聞で経済産業省の記事を読み、情報管理に取り組んでみようと考えた。お客様の情報である情報も自社の情報も流出させてはいけないということを、営業秘密の観点で認識した。お客様に信頼を得ていただく方法として認証取得した。認証取得の効果はこれから出てくると思うが、お客様の開発サンプル等を扱う際に、機密保持契約を交わす等、情報を守るという意識は出てきている。従業員浸透が課題であり、各部署で遵守確認を実施した。継続していけるかどうかは遵守確認次第と考える。大手企業は年 1 回アンケートの形で取引先の調査を行う。ある程度、質問に回答できるレベルになってきた。
- 元々、セキュリティを積極的にやっていこうと考えていた訳ではないが、サポインに採択され、補助金を受けて進めていく際に、県から情報管理に関する質問状があり、管理状況の改善を勧められた。どこから手をつけてよいかわからなかったが、認証機関からパンフレットをみせてもらい、専門家派遣があるということで、活用することとなった。取引先とも NDA を結んだりするが、会社としての仕組みはできておらず、社内の様々な技術情報管理もそれぞれに任せていた。現状の情報の棚卸しから始まった。このきっかけがなければ何も変わらなかった。
- 何がノウハウ、情報資産として管理すべきなのか、特定できない。保護すべき情報の線引き・識別がスタートとなる。意識と知識が第一ステップ。情報の特定にあたって、民間のコンサル会社に簡単に情報開示は難しい。政府や行政からお墨付きをもらっている業者、政府系の外郭団体等が主導権を持って責任を持っていただくことが重要。

b. 知財や技術情報管理に必要な項目

- 可搬式記録媒体（USB）がお客様で必要になって、個人が量販店で買って使っていたケースがあった。USB 管理については、自社で認証にかけたもののみ使用することとした。従業員に周知して運用に至っている。お客様の販売前の製品情報の保管についてバラツキがあったため、統一する取り組みを行った。

- 取り組みは始まったばかりで成果はまだわからないが、取り組み方やレベルの整理がわからないところから、安心して手順に沿って進められる段階になった。
- サーバ等の物理的なハード面は課題。製造業であれば、製造物そのものが秘密の対象である。どう保管するのか、それに対する設備、施錠管理にコストがかかる。中小の製造業でものを製造するとなると図面を見ながら加工していく。図面全てを対象とするのか、どこまでを対象とするかで対策が変わる。小さいものに対してどこまで守るのか。事例などがあるとよい。

c. 情報管理(情報セキュリティ)対策に関わる大凡の費用感

- ハード面では、警備会社と契約し、監視カメラを 24～25 台つけた。元々予算を取っていたので、負担感はない。親会社の指導もあり入れ替えた。ハード面では 15%費用が上昇。ソフト面では、自社の教育、規程作り等。4 名程度が参画して半年かけた。各部門と話し合い、すりあわせながら策定した。
- コンサル費用の補助は助かる。専門の方がいる企業はよいだろうが、ない場合は専門の方がほしい。実費はかかるが、決まったらやらざるを得ない。
- サーバ複数を立てて、バックアップのための施設も整備すると、建築で100～200 万の規模となる。主に上記の物理的な対策費用負担となるが、サイバーセキュリティ、ネットワークの費用ももちろんある。

d. 技術情報管理認証制度の在り方に対するご意見、普及に向けて必要な事項

- 取り組み自体が継続されていくことで知名度も上がると思う。
- 周知媒体としては、日経新聞や技術系の人であればイプロス。ビジネス全般の雑誌を見る。リスク管理という文脈での周知媒体もあろう。
- 認証取得を目指すことによって、社内の情報が整理される、不要な情報が捨てられることが期待できる。ISO はあまり効果を実感できていないままなんとなく更新しているので、そうなってほしくない。
- 取引先への PR は、より普及が進んできてからではないか。
- 既存の仕事をしながら、＋αの仕事をすることになるので、トップがやると決めないと進まないだろう。
- 認証を取ったからといって事業成長と関わりがない。ある事業をやるには認証取得企業が優先される等メリットが必要。
- 取引先とは、基本的には取引基本契約書を取り交わす。NDA の主な項目を含む。情報管理に関して厳しくチェックリストを設けて、運営面でチェックするというプロジェクトもあるが多くはない。
- IoT 化の流れに沿って、製造業においても、インテグレーターの役割を果たす企業が増えていくが、インテグレーターから情報が漏れるということは大問題。今後、新しいビジネスに取り組むインテグレーターに本認証制度をフィットさせていくのではないか。

（5）ヒアリング結果からの考察

1） 持続可能な制度・仕組みの構築

制度の普及まで継続可能な体制をいかに構築するかを検討する必要がある。現場で中心となる運営組織や、中心人物を育てていくことが必要である。認証制度がビジネスとなるためには、社会的なニーズの高まりと制度側の取組みが合致することが重要である。社会的ニーズが生まれたときに、制度として機能する仕組みを整えておく必要がある。

持続可能な仕組みとするために、例えば、専門家に対する資格（登録料）による事業等、関係する事業者において事業が成り立つ仕組みも検討に値する。

なお、技術情報管理認証制度の第三者認証という信頼性を特徴とするならば、別の制度に対して、信頼性を担保する制度としてビルトインすることで、別の制度が一定のクオリティが担保されるものとして認められるという方向性もある。

2） 審査員/専門家の育成、柔軟にアサインする仕組みの検討

審査員と専門家を柔軟にアサインすることで、人材の有効活用が可能となり、審査及び指導助言の拡大が期待できる。審査と指導助言の切り分けは厳しく行う必要があるが、派遣可能な審査員/専門家の規模拡大や育成機会の提供の観点から、ある程度の審査員/専門家を登録・プールし、認証機関や専門家として状況に応じて柔軟に派遣していく仕組みが、制度をスケールする上で有効と考えられる。

3） 認証機関への支援の実施

業界団体が認証機関となる可能性については、業界団体において十分な人材を置くことは難しく、また自主事業で収入を得ている団体はあまりないことから、障壁は高いと考えられる。また、業界団体が認証事業を進められるかどうかは、マーケットサイズが重要となる。そこで、業界団体が認証機関を担う際の、事業として成立するモデルや認証機関を支援する仕組みを構築・提示することが有効と考えられる。また、認証機関における人材不足を解決するためには、審査員や専門家等を派遣・融通する仕組みも効果的であると考えられる。また、認証機関に対して、制度普及のための各種支援を制度運営側で実施していくことも有効である。

認証機関となる団体については、類似した業界団体をまとめている団体が担うという方向性も考えられる。

4） 情報管理に積極的な事業者に対するインセンティブ

中小企業からは、認証取得事業者が優先される等のメリットが必要との意見が多かった。取引元となる大手企業の情報管理に関する要望に応え、取引に繋がり、ビジネスが拡大することが、中小企業における積極的な認証取得に対するインセンティブの 1 つとなる。お客様からの信頼を得ることを期待して認証取得した中小企業や、大手企業からの取引先の状況確認に対して認証取得したことで回答可能なレベルになった中小企業も見られたことから、中小企業においては認証取得により取引におけるメリットを期待し、実感している。認証取得した中小企業におけるインセンティブについては、継続的に検討する必要がある。

また、IoT 化を背景にものづくりからインテグレーターに役割が変化する等、新しいビジネスに取り組む中小企業もある。このような事業者に対して、新規ビジネスの後押しをするような形で、情報管理の必要性を訴え、市場にアピールすることで、本認証制度の活用を促せるとよいのではないか。

なお、事業者に対するインセンティブももちろんであるが、事業者において情報管理を進める担当者にとっても、メリットがないという意見もあった。個人単位でのインセンティブ、例えば人事として評価されるような組織としてのガバナンスや体制、制度等についても、検討を進めるべきである。

5）知財・情報管理における課題への対応

営業秘密の保護や情報管理については、具体的な対策が契約に折り込まれている訳ではなく、情報漏洩リスクは下がっていないという指摘があった。事業者間の取引において、二者監査ではその場面では協業できたとしても、違う場面では競合する場合もあることから、情報管理の実効的な対策を確認する第三者認証のニーズはあると考えられる。

事業者にとっては、どんな情報が重要なものとして保護すべきであるか、また、どの情報を秘密としてどの情報をオープンとするかの線引きが難しいため、そのアドバイスができる専門家が必要である。

さらに、営業秘密に関しては、事業者内で知財の担当者、情報管理やサイバーセキュリティの担当者が連携し、管理体制を構築していくことが必要となることから、管理体制の構築について事業者における課題やニーズを把握し、解決策を提示していく等の検討も必要である。

6）効果的な普及・啓発

事業者において情報管理を進めるにあたり、その必要性が十分に認識されていない現状がある。産業分野や技術情報の例示、実際に起こった事故やヒヤリハット等を提示することにより、情報管理の必要性を認識してもらうことが重要である。特に昨今、サプライチェーンの観点が重要となっていることから、取引における機微情報や中小企業と取引先との関係性を整理し、実態を捉えた上で、認証制度をどのように活用できるか検討を行うべきである。

事業者において必要性の認識を促すためには、特に経営層に対する啓発が重要である。現在、コーポレートガバナンスコードに知的財産が入ったため、経営層の目にも止まりやすい状況である。善管注意義務などのリスク等を訴えるなど、経営者が危機感を認識する形で説明することが有効と考えられる。

さらに、類似制度との違いを整理した上で、事業者にとってわかりやすく説明することが求められる。情報管理やサイバーセキュリティ等、取り組みのきっかけとなった課題意識は異なる場合でも、類似・関連した制度が認識されることで、双方の取組みが活性化することが望ましい。

7）告示基準、セルフチェックシートに含めるべき項目や活用方法

サイバーセキュリティや営業秘密は既にガイドラインがあり、告示基準にすべてを含めてしまうと逐一反映する必要があるため、ガイドラインがある領域については、受け渡すことにした方がよいという意見があった。例えば、営業秘密指針が全面改訂されている中、「アクセス制限」という用語を使わない、具体的な対策としてアクセス制限を必須としないなど、守り方に関する考え方の変化についても考慮する必要がある。そのため、関連した領域におけるガイドラインや指針等の対策について、どこまでを告示基準に折り込み、どのように整合性を取って運用していくかは検討する必要がある。

一方、ISMS・P マーク・秘密情報の保護ハンドブック等、類似したテーマで様々な関連文書があるので、要件が漏れていないかより、矛盾がないかを確認した方がよい。

技術情報管理認証制度においては、内部犯行にも対応していることは特徴的であると言える。想定脅威と要求が整理されると、どんな目的で対策を実施しているのかが事業者にとってもわかりやすく腹落ちもしやすいため、脅威と対策を整理することも有効である。

また、現在、取引先に対して似て非なる情報管理にかかわるチェックリストが提示されている状況にある。これらを統一化していく方向性はありうるという意見もある。取引先に対する情報管理の要求レベルが段階的である場合もあり、格付けを行っていくという考え方もある。取引先に対する要求事項や要求にあたっての課題等については、サプライチェーンの最終顧客となる業界のニーズを把握し、これらのニーズに技術情報管理認証制度が応えることで普及が進むと考えられる。

3. 専門家派遣事業

適切な技術情報管理の構築等に向けたアドバイスや技術情報管理の内部監査を希望する事業者、認証機関になることを目指しており内部手続・能力構築を求めている事業者等（以下、「依頼者」という。）に対して、専門家の派遣を実施した。

また、専門家派遣の結果分析、特に派遣内容等を踏まえた技術情報管理の課題（認証制度の課題、事業者の技術情報管理の課題の両方）分析を行った。

3.1 専門家派遣による技術管理の構築、認証取得に向けた支援、フォローアップ等支援

3.1.1 派遣概要

専門家派遣については、以下のニーズに対応して実施した。

① 適切な技術情報管理の構築や認証取得に向けた支援

適切な管理をすべき技術等の情報の特定や、認証制度に沿った具体的な技術情報管理の実施方法が課題となっている事業者に対して、改善点の提案・アドバイスを実施。

② 技術情報管理に係る内部監査、認証取得後のフォローアップ支援

認証を取得した事業者が実施している技術情報管理が、認証制度に沿って適切に行われているかについての内部監査を実施。改善点がある場合においては、提案・アドバイスを実施。

③ 認証機関の申請に向けた支援

認証機関を目指す事業者等に対し、一般的な体制構築や書類作成に係る提案・アドバイス等を実施。

3.1.2 派遣募集

2021 年 8 月 5 日より、委託機関（株式会社三菱総合研究所）のホームページにおいて専門家派遣の募集を開始した。

公募情報

「産業競争力強化法に基づく技術情報管理認証制度の普及促進に向けた調査分析及び専門家派遣等事業」（経済産業省事業）において専門家の派遣を希望する事業者の公募のご案内について

シェア　ツイート

2021.8.5
株式会社三菱総合研究所

三菱総合研究所（MRI）では、経済産業省からの受託事業「産業競争力強化法に基づく技術情報管理認証制度の普及促進に向けた調査分析及び専門家派遣等事業」の一環として、技術情報管理を進めようとする事業者の皆さまに、情報管理の具体的な方法のアドバイスや、認証取得申請の支援を行う専門家を派遣いたします。

参考：技術情報管理認証制度について（経済産業省）

技術情報管理認証制度に係る指導支援等の専門家派遣　ご案内

募集期間

2021年8月～2022年2月28日（月）
※定員に達し次第締め切ります。お早めにお申し込みください。

派遣時期

2021年8月中旬～2022年3月11日（金）

対象者

技術情報管理認証取得を希望する事業者
重要な情報に関して、情報管理のレベルアップを希望する事業者
（技術情報に限らず、顧客情報や研究情報等、事業者の強みとなる情報全てが対象です）
技術情報管理認証取得後のフォローアップを希望する事業者

費用

無し（認証取得申請には別途費用がかかります）

専門家実施内容、所要時間

(1) 情報管理方法のアドバイス：半日～最大3日程度
管理が必要な技術等の重要な情報の特定や、具体的な情報漏えい防止対策等について、それぞれの事業者の状況に合わせた提案・アドバイスを実施

(2) 認証取得のための内部監査：半日～最大3日程度
認証基準に沿った情報漏えい防止対策が行われているかを、第三者の立場で評価し、監査記録を作成

※所要時間は認証対象とする情報の種類・量や拠点規模、対策数等によって異なります
※派遣は (1)のみ、(2)のみ、(1)(2)両方、のいずれも可

事業案内・申込用紙

事業案内 [499.7KB]
技術情報管理認証制度に係る専門家派遣事業　申込書 [41.7KB]

ニュースカテゴリー
ニュースリリース
公募情報
お知らせ
RSS
グループ企業ニュース

年別一覧
2022年のニュース
2021年のニュース
2020年のニュース
2019年のニュース
2018年のニュース
2016年のニュース

図 3-1 専門家派遣募集ホーム-ページ

技術情報管理認証制度

専門家派遣事業のご案内

～ 技術など重要な情報・ノウハウの守り方を専門家がアドバイスします ～

平成 30 年 9 月 25 日、産業競争力強化法に基づき、技術等の情報の管理について、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。

この認証取得を目指して、自社の技術等の情報管理を進めようとする事業者の皆様に、情報管理の具体的な方法のアドバイスや、認証取得申請の支援を行う専門家を派遣いたします。

派遣する専門家
（1） 情報管理方法のアドバイス（ITコーディネータ、中小企業診断士 等）
（2） 認証取得のための内部監査（情報セキュリティ監査人 等）

募集期間	2021 年 8 月～ 2022 年 2 月 28 日（月） ※ 定員に達し次第締め切ります。お早めにお申し込みください。
対象者	技術情報管理認証取得を希望する事業者、技術情報管理のレベルアップを希望する事業者 技術情報管理認証取得後のフォローアップを希望する事業者
費用	無し （認証取得申請には別途費用がかかります）
専門家の実施内容、所要時間	（1） 情報管理方法のアドバイス ： 半日～最大 3 日程度 管理が必要な技術等の重要な情報の特定や、具体的な情報漏えい防止対策等について、それぞれの事業者の状況に合わせた提案・アドバイスを実施 （2） 認証取得のための内部監査 ： 半日～最大 3 日程度 認証基準に沿った情報漏えい防止対策が行われているかを、第三者の立場で評価し、「自己宣言認証」（第一次審査のみによる認証）で利用できる監査記録を作成 ※ 所要時間は認証対象とする情報の種類・量や拠点規模、対策数等によって異なります ※ 派遣は（1）のみ、（2）のみ、（1）（2）両方、のいずれも可
派遣時期	2021 年 8 月中旬 ～ 2022 年 3 月 11 日（金）

■ 専門家派遣の流れ

利用申込	派遣決定	派遣開始	派遣終了
・申込用紙に必要事項を記載の上、事務局、または本紙「お申込方法」に記載の認証機関・業界団体に送付	・申込内容を確認後、派遣可否を事務局より連絡 ・派遣に関する契約を事務局と締結	・日程調整の上、事務局より専門家を派遣	・派遣結果についてアンケートを事務局に提出

■ お申込方法

別紙「申込書」にご記入の上、**事務局、以下の認定技術等情報漏えい防止措置認証機関、またはご所属の業界団体**にお送りください。（申込先によって申込書の種類が異なりますのでご注意ください）

【認定技術等情報漏えい防止措置認証機関】
- 日本検査キューエイ株式会社（JICQA）
- 一般財団法人日本品質保証機構（JQA）
- 株式会社日本環境認証機構（JACO）
- 公益財団法人防衛基盤整備協会
- 一般社団法人情報セキュリティ関西研究所
- 一般社団法人日本金型工業会

■ お問合せ先（事務局）

株式会社三菱総合研究所 サイバーセキュリティ戦略グループ 技術情報管理専門家派遣担当
TEL：080-2281-6450 ／ E-Mail：tics-haken@ml.mri.co.jp

令和３年度 経済産業省委託事業「産業競争力強化法に基づく技術情報管理認証制度の普及促進に向けた調査分析及び専門家派遣等事業」

図 3-2 専門家派遣事業の案内

3.2 専門家の確保やその管理

3.2.1 派遣募集

専門家派遣にあたり、中小企業・製造業の情報管理や IT 活用に通じており、情報セキュリティ監査の知見を有する専門家を抱える特定非営利活動法人 IT コーディネータ協会及び一般社団法人情報セキュリティ関西研究所と連携し、円滑な派遣体制を構築した。

事業者向けの派遣については、主に両組織を通じて行った。専門家の秘密保持については、連携した 2 組織と専門家の間の守秘義務、及び連携した 2 つの各組織と委託機関（株式会社三菱総合研究所）との守秘義務において確保した。

また、応募事業者の希望により、認証機関（一般財団法人日本品質保証機構）からの派遣も実施した。

3.3 専門家への研修

3.3.1 研修の実施

本事業において派遣する専門家として、技術情報管理認証制度全般及び認証制度中の認証基準の十分な理解をいただくために、専門家に対して派遣前に研修を実施した。研修会における動画配信については、特定非営利活動法人 IT コーディネータ協会の協力を得て実施した。

また、助言・指導の標準化を図る上で、技術管理認証制度の専門家として適切な、知財管理、情報セキュリティ、認証枠組み等の本制度を理解するためのカリキュラム及び研修素材を作成した。

表 3-1 専門家研修(1 回目)

日時	2021 年 6 月 23 日(水) 14:00 ～ 17:00
場所	オンライン会議(zoom)
議題	(1) 技術等情報管理認証制度、専門家派遣制度 (株式会社三菱総合研究所) (2) 技術等情報管理認証制度 基準等 (情報システム監査株式会社 監査・コンサルティング部 ※ 録画 小河 裕一 氏)
参加者	3 名

表 3-2 専門家研修(2 回目)

日時	2021 年 7 月 13 日(火) 13:30 ～ 16:30
場所	オンライン会議(zoom) ※ 配信協力:特定非営利活動法人 IT コーディネータ協会
議題	(1) 技術等情報管理認証制度、専門家派遣制度 (株式会社三菱総合研究所) (2) 技術等情報管理認証制度 基準等 (情報システム監査株式会社 監査・コンサルティング部 小河 裕一 氏) (3) 今後の手続等
参加者	62 名

3.3.2 カリキュラムの策定

研修の実施にあたり、本制度における専門家に求められるスキルとして以下を整理した。

- 認証制度に関する知識
- 認証基準に対する判断基準
- 審査、内部監査に関する知識(≒ISMS 審査員、情報セキュリティ監査人)

- 企業(特に中小企業)の IT 活用やセキュリティに関する知識(≒IT コーディネータ)

検討方法としては、マネジメントシステム審査員 評価登録センター(JRCA)が規定する ISMS 審査員研修コース要求事項を参考に、技術情報管理認証制度の専門家において必要な知識を整理し、カリキュラムの案とした。

なお、全ての知識やスキルに対して本制度において研修を行うのではなく、既存の別の資格や研修制度において獲得できる知識・スキルがある場合は、他者が提供する資格や研修制度を活用することも効率的である。

表 3-3 ISMS 審査員研修コースにおける要求事項を元にした
技術情報管理認証制度で必要な知識と対応する研修素材

		座学研修 【凡例】赤字は変更・追加部分、青字は要検討、 a)b)・・は要求事項のNo.(本認証制度に関係のない項目は削除) (*)は座学・実技の研修で使用	実技研修 【凡例】赤字は変更・追加部分、(*)は座学・実技の研修で使用
カリキュラム	専門家(審査)において、ISMS審査員と類似する事項	a)技術情報管理認証制度の概要 b)認定機関、審査登録機関、審査員評価登録機関、研修機関の役割及び責任 c)第一者審査、第二者審査及び第三者審査の機能、その類似点および相違点 d)審査登録プロセスにおける審査員及び審査チームリーダーの役割及び責任 e)適合性審査と有効性の向上につながる審査の方式 f)審査中に記録された不適合に対して受審組織が作成した是正処置の提案の評価、また、是正処置の実施状況及び有効性の評価。 h)審査員は、地域の習慣に配慮することの必要性、及び受審組織の規則・規制がある場合、特に、安全・衛生に係わるものについては、それら規則・規制を遵守することの必要性 k)監査の指針、及び監査ガイドライン l)METIが定める専門家倫理綱領 m)専門家(審査)登録方法及び要件等の概要	a)文書化した情報のレビューの実施 b)監査計画の策定 c)監査のための文書化した情報の作成 d)初回会議の開催 e)監査の実施中の文書化した情報レビュー並びに情報の収集及び検証 f)監査所見の作成 g)監査結論の決定 h)最終会議の実施 i)監査報告書の作成 j)監査のフォローアップの実施 k) 組織が実施した不適合の原因分析と修正及び是正処置の検証 l) 審査報告書に記載する事項
	本制度の専門家(審査)に固有の事項	a)技術情報管理認証制度審査の目的と特徴 c)技術情報管理認証基準の各条項の意図及び要求事項 d)情報セキュリティやISMS審査との関連性、技術情報管理固有事項 g)技術情報管理認証基準の用語(あれば) h)技術情報管理認証基準の解釈(仮) i)技術情報管理認証基準に関連する法規制に関する知識 j)受審組織の技術情報管理認証審査登録プロセス	―
主な研修素材		技術情報管理認証制度概要(含む審査プロセス、認証機関に関する命令) 専門家倫理綱領 監査の指針(審査について追加が必要) 監査ガイドライン(*) 技術情報管理認証基準 技術情報管理認証基準の解釈(仮)	監査ガイドライン(*) 技術情報管理認証基準チェックリスト 審査報告書

3.3.3 研修素材の作成

検討したカリキュラムを念頭に、専門家研修における研修素材を作成した。構成は以下の通りとした。

1. 技術情報管理認証制度概要
   ① 技術情報管理の必要性、ポイント
   ② 認証制度概要(背景、目的)
   ③ 認証機関に関する命令
   ④ 審査プロセス
2. 専門家倫理綱領
3. 監査の指針、監査ガイドライン
4. 技術情報管理認証基準、解釈
   ① 重要情報の特定
   ② 重要情報の識別
   ③ 管理者の選任
   ④ 情報管理プロセス

⑤　従業員教育
⑥　情報漏えい等事故発生時の報告ルール
⑦　人的アクセス制限
⑧　情報の物理的保管
⑨　情報の電子的保管

3.4 専門家派遣の方法

専門家派遣については、以下の方法で実施した。依頼者からオンラインを希望された場合においてはオンラインでの実施も可とした。

- 依頼者からの申請については、受託者への直接申請だけではなく、認証機関、依頼者が会員となっている業界団体等を通じた申請も受付可能とした。
- 依頼者の依頼内容や意向を踏まえ、適切な専門家を派遣した。
- 派遣した専門家には、実施した業務の報告書を作成・提出いただいた。
- 依頼者には、派遣の内容に関するアンケートを実施した。

3.5 派遣結果

3.5.1 派遣実績

専門家派遣事業の派遣実績は、一般事業者への派遣が 28 回（22 件）、日本金型工業会と連携して実施した会員企業への派遣が新規 24 回（8 件）、フォローアップ 30 回（14 件）の合計 54 回（22 件）で、令和3年度の派遣実績は82回（44件）。であった。派遣形態は直接の訪問及びオンラインのいずれかとした。

今年度も、認証取得を希望する事業者に対する複数回の派遣を可能としたが、多くの事業者において複数回の派遣を実施することができ、認証取得を目的とした手厚い支援が可能であったと言える。今年度、専門家派遣を受けた事業者のうち、認証取得は 9 社である（予定を含む）。また、昨年度、専門家派遣を受けずに認証取得した事業者（1 社）が、今年度自己適合宣言型認証から第三者認証に変更しており、昨年度、専門家派遣を受けた事業者で認証を取得した 23 社（専門家派遣を受けずに認証取得した事業者（1 社（結果的に自己適合宣言型から第三者認証に変更）は含まない）を加えると、今年度終了時点での認証取得は 33 社の見込みである。

また、認定取得を希望する機関への派遣も準備していたが、希望がなかったため、認定取得を希望する機関への派遣実績はなかった。

3.5.2 派遣結果

事業者向け専門家派遣により、専門家から得られた主な意見として、事業者における成果と今後の技術等情報管理・認証取得に向けた見通し、困難だった点は以下の通りである。

なお、今回、認証取得後のフォローアップを実施したが、情報管理は一度行ったら終わりではなく、継続的に運用、改善が必要であることから、専門家派遣により、改めての運用に関する事業者の意識付けと対策のレベルアップに効果があったと考えられる。

1） 支援による成果、事業者が得たメリット

a. 情報管理の重要性の認識、課題の明確化

＜新規派遣＞

- 情報管理や情報セキュリティの重要性について理解できた。
- 管理対象情報の明確化と守り方の必要性、推進体制の必要性を理解できた。
- 自社の技術情報をはじめとする重要情報の整理がなく、守るべき秘匿情報の整理と重要情報の重み付けが大事であるとの認識が得られた。
- 全社社員の教育を通じ、社員一人一人が理解し行動することが重要であるとの認識が得られた。
- 全社一丸になって情報セキュリティ対策を進めることを考えるきっかけとなり、情報の洗い出しや対応について幹部の議論が進んだ。
- 情報セキュリティ基本方針における、経営者の責任や法令及び契約上の要求事項の遵守及び違反及び事故への対応など、情報セキュリティにおける企業のあり方や自社のガバナンスへの理解が深まった。
- 情報システム等を統轄する工場長が情報セキュリティに関心を示し、アクセス制限やハード機器からの情報漏えいについての問題意識を高めた。
- 認証に必要となる文書・手順書整備について理解した。情報セキュリティに関して必要であることは認識されていたが、今回具体的にどうすればよいかの道筋を理解した。
- 全項目を実施するのは困難であるため、まずは必須項目の課題整理と実施計画の策定を優先的に実施し、情報管理の強化を図ることを理解した。

＜フォローアップ派遣＞

- 認証後の実態について、フォローアップチェックシートを元にして、現状における課題の抽出ができた。
- 情報管理委員会を開催することで、担当者にも問題意識が生まれるとともに、各部署の情報管理責任者にも問題意識が醸成され、具体的にどのように運用するかが協議されるようになった。
- 情報セキュリティマネジメントシステムの体系、重要情報（極秘・秘）の識別、情報セキュリティ基本方針、情報管理規程の必要性と従業員への教育の必要性について理解できた。

b. 情報管理の推進

＜新規派遣＞

- 認証取得に向け重要情報の特定方針を整理できた。
- 規定類整備の方向性を定めることができた。
- 様式を整理するなど、何を記録すべきか理解できた。
- 帳票様式に対して修正点などをアドバイスし改善が図られた。規程の完成イメージについて事例などを示して説明することで取組みを推進した。
- ノート PC の取扱いについて、規程を整備した。実際の運用を始めるにあたってその手順等について確認した。また、規程の見直しの時期や方法について説明した。
- 組織体制に関して、少人数のため兼務となる組織図案を元に議論をした結果、適材適所において情報管理を行う点について、全社で推進するための理解を得た。
- 重要情報の管理についても「極秘」情報を明確に特定し、物理的な管理方法も含め具体的に対策が進展した。
- 重要情報を管理・運用する上での方針、規程、手順などを策定した。また実際に運用を行うに際して、全社社員への教育が重要であることの再認識が得られた。
- 情報管理に関する運用継続、改善の基盤が構築できた。

＜フォローアップ派遣＞

- 営業・設計・製造・品質・委託先までの重要情報のフローを明確にし、情報漏えいの課題と対策の助言を行った。
- 電子情報のアクセス制御等の対応作業が情報システム管理者に集中していたことから、管理部含めた作業手順の再検討を助言した。手順や記録が未整備の部分について、情報システム管理者および管理部の主体的な検討及び提案を助言することで、作業分担見直しを含めて明確化し、対応の方向性を定めることができた。
- 受注先からの見積依頼に添付される重要情報について、各グループが共有する重要情報を保管するファイルサーバのアクセス管理等について助言を行った。
- ベンダーに頼っていた部分から、自社運用可能なものを明確にした。

c. 認証取得に向けた意識向上

＜新規派遣＞

- 今回の専門家指導をきっかけに認証取得を目指し、全社的な展開と意識改革を図っていく。
- まずは課題解決に重点的に取り組み、認証取得については、今後、検討する。

2）事業者における今後の対策、認証取得の見通し

a. 今後実施する対策

＜新規派遣＞

・ 管理規程、運用手順書に従って、対象となる情報の仕分け、従業員への周知等、管理運用を行う。

＜フォローアップ派遣＞

・ 運用方法と体制の見直しを行っていく。
・ アクセス制限などのルール化などの改善が必要である。
・ 実物の管理の方針が明確になり、企業としての合意を得ることができた。重要情報（極秘・秘）の識別、情報セキュリティ基本方針、情報管理規程の策定と従業員への教育について指導・助言を行った。
・ 社長、情報管理責任者、情報システム担当者による建設的なディスカッションを通じて、是正案に沿った対応を実施いただけることが期待できる。

b. 認証取得の見通し

＜新規派遣＞

・ 今回、必要最小限の対策を講じて初回認証取得に挑戦し、3 年後の更新時期までに、それらの管理を強化していく。
・ 認証取得は 1 年後の意向であるが、取組の意欲を維持できる3～6ヶ月の間で受審する方がよいことを提言した。

3）支援において困難だった点（実施が困難な対策、支援時に企業に不足していた情報　等）

a. 事業者における対策状況

＜新規派遣＞

・ 情報管理について、自社で取組んだことがないため、情報セキュリティに関してはウィルスソフトなどの簡単な対応策しかなく、従業員のセキュリティ意識も低かった。
・ 小規模企業であることから、情報管理に携わる人数が限られることが、情報管理を進めるにあたり大きな課題であった。
・ 情報セキュリティは手間がかかり「面倒くさい」との意識があり、全社的に取り組むことは難しい状況であった。
・ 認証のための改善点が現行の業務に影響を与える場合があり、改善と業務影響の最小化との妥協点の合意が難しかった。
・ 敷地内及び工場は夜間等に施錠がなく、警備もおいていない。また、サーバ室の物理的対策措置が急務であるが、経費の兼ね合いもあり、直ちに対策することは困難と考えられる。

＜フォローアップ派遣＞

・ 経営幹部の情報セキュリティに対する意識はあるが、推進体制や役割分担が不明確であり、運用に関しての推進意識が低い。
・ 担当者（リーダーとスタッフ）が兼務であり、平行する他業務もあり、情報管理に関してうまく対応するのが難しそうであった。
・ 認証後には、規程や手順に記載された内容で運用しなければならならいが、運用があまりできていなかった。
・ 認証に関しては担当者も良く分からない点があり、基本的な点から指導助言をする必要があった。
・ 是正が必要な項目が多く、実際に対応いただけるような是正方法とすることが必要だった。また、自動車分野のサイバーセキュリティガイドラインに関わる項目について、どう対応すれば良いかの検討に時間がかかった。

b. 支援時に必要な情報

＜新規派遣＞

・ この制度の意義や、取得することのメリット（特に公共事業受注時の官公庁がこの認証をどの程度認めるのか）について明確な資料があると良い。

＜フォローアップ派遣＞

・ オンラインの場合、実物の確認ができなかったため、聞き取りが中心となってしまった。

4）事業者からの意見

派遣を受けた事業者から得られた主な意見は以下の通り。

＜良かった点＞

・ 情報管理の規定が一通り過不足なく整備することができた。
・ 現在の弊社に足りない所や今後目指すべきところについてご指摘をいただけた。
・ こちらの理解度に合わせて寄り添ったご案内をいただいた。
・ 今後、情報セキュリティの強化、対策をする上での一つの指針ができた。
・ 次回は認証に向けての取り組みをしっかりと行えるよう意識できた。
・ 不明点や疑問点などの的確なアドバイスをいただいた。
・ 例示や図を用いての説明などでイメージがしやすかった。
・ 図面、データ等誰でも見られる状態にあったが、管理できるようになった。また、従業員への情報管理およびセキュリティ教育ができた。
・ 技術情報の重要度と管理について基礎知識を得た。次のアクションとして教育やインシデント対応が必要であり、これらも認証制度に含め、ステップアップとなるような形を希望する。

＜改善点＞

・　雛形や業種毎の注意点や参考例があるとスムーズに話を進めやすい。

＜その他のご意見＞

・　コロナ過により WEB 認証審査などがあると助かる。

・　今後、自動車工業会の指針等の変化に応じて必要基準の追加や見直しが必要になる可能性があるように思うため、都度、情報やフォローがあると助かる。

4. 業界等と連携した技術情報管理認証制度の普及活動

4.1 特定の業界・団体に特化した技術情報管理認証制度の活用方法の検討及び技術情報管理のモデルの構築

技術情報管理認証制度にある認証基準について、特定の業界・団体の実情を踏まえた適切な運用となるよう、技術情報管理認証制度の認証付与の方法を含めた活用方法、当該業界・団体に属する事業者に適用される標準的な技術情報管理のモデルの検討を行った。

4.1.1 自動車産業

自動車産業においては、日本自動車工業会及び日本自動車部品工業会において、「自動車産業サイバーセキュリティガイドライン」が公表されている。本ガイドラインの目的は、自動車メーカーやサプライチェーンを構成する各社に求められる自動車産業固有のサイバーセキュリティリスクを考慮した、向こう 3 年の対策フレームワークや業界共通の自己評価基準を明示することで、自動車産業全体のサイバーセキュリティ対策のレベルアップや対策レベルの効率的な点検を推進することとされている。

本ガイドラインの初版は、特定の業務領域（工場、販売、コネクティッド領域）によらず、全体の業務に共通するエンタープライズ領域（業務基盤となる OA 環境）を対象範囲としている。そのため、技術情報管理認証制度が対象とする領域と合致しているが、自動車産業のガイドラインでは主に電子情報が対象となっている。

今年度の専門家派遣においては、日本金型工業会では本制度のチェックシート（必須項目）と自動車産業サイバーセキュリティガイドラインの全ての項目との対比をつけて、事業者への助言を実施している。必須項目は概要レベルでの項目を示しているが、今後、対比づけた項目については求めるレベルや表現等を含めて見直しの必要性について検討の必要がある。

表 4-1 自動車産業サイバーセキュリティガイドラインとチェックシートの対応（例）

項目番号	項目	内容	自工会・部工会ガイドライン項目
共通事項			
1	重要情報の特定	技術等の管理対象情報(以下、「重要情報」という)の特定は、規程等の決められた手順や方法により、適切に行われている。	【自No.25】機密区分に応じた情報の管理ルールを定めている 【自No.26】高い機密区分の情報資産(情報)を一覧化している
2	重要情報の識別	重要情報であることを明らかにするために、「関係者外秘」などの表示等を行っている。	
3		他者から預けられた重要情報は、当該他者からの意見に基づき管理方法を決定している。	【自No.20】他社との間で、機密情報の取り扱い方法が明確になっている 【自No.34】会社毎に取り交わす情報・手段(受発注の手段等、情報のやり取り)を一覧化している
4	管理者の選任	経営層は、以下の重要情報の管理に関わる責任者を定める。 (1)情報管理の手順を確立する。 (2)情報を取り扱う者の制限・管理、トレーニングを行う。 (3)情報漏洩防止対策を実施し、その実施状況を把握する。 (4)情報漏えいの兆候・事実の把握に努め、事象発生時に必要な対応を行う。 (5)(2)-(4)の記録を取得し、保管する。	【自No.7】情報セキュリティ責任者を含む、平時の体制と責任と役割を明確化している
5		従業員が多い場合や、重要情報が複数部門に跨がっている場合は、全従業員が責任者を明確に認識させるようにしている。	
6		従業員が少なく、経営層が管理者を兼務できる場合、当該経営層が従業員や重要情報の取り扱いについて十分把握できており、重要情報についての従業員の報告や行動が習慣化できている。	
7	管理の基本的な考え方	重要情報の作成から廃棄までのプロセスを通じて、情報管理を適切に実施している。	【自No.1】自社の情報セキュリティ対応方針(ポリシー)を策定している 【自No.4】業務で利用する情報機器の利用ルールを規定し、周知している(個人所有機器(BYOD)含む) 【自No.28】重要度に応じた情報機器、OS、ソフトウェアの管理ルールを定めている 【自No.49】復元(リストア)手順を整備している 【自No.50】システムが停止した際も業務が遂行できる代替手段を用意している
8	重要情報の管理をするためのトレーニング	全従業員に対して、重要情報の適切な管理に関する意識の啓発を図るためのトレーニングを実施している。	
9	重要情報の事故等の発生時の対応	従業員が重要情報の漏えいや不正利用を発見した際の必要な措置について、従業員が認識できる方法で明示し、迅速な対応を講じている。	【自No.10】情報セキュリティ事件・事故発生時の対応体制と責任と役割を明確化している 【自No.13】情報セキュリティ事件・事故時の対応手順(初動、システム復旧等)を定めている 【自No.14】ウイルス感染時の対応手順を定めている 【自No.21】情報セキュリティ事件・事故時の他社との役割と責任が明確になっている
10	人的アクセスの制限	アクセス権を有する者のみが重要情報を取り扱う事ができるようにしている。	【自No.22※】人の異動に伴うアクセス権(入室権限やシステムのアクセス権)の管理ルールを定めている
管理対象情報が金庫等の保管容器に保管できる場合（例えば、紙情報等）			
11	保管容器に保管できるものの物理的アクセスの制限	重要情報を保管容器に施錠して保管するとともに、持ち出して取り扱う場所についても限定している。	
管理対象情報が金庫等の保管容器に保管できない場合（例えば、製造装置等）			
12	保管容器に保管が困難な場合等の物理的アクセスの制限	重要情報が立入制限区域で管理されており、権限を有する者のみが取り扱うことができるようにしている。	【自No.39】サーバ等の設置エリアは、入場可能な人を定めている 【自No.40】サーバ等の設置エリアは、施錠等で入場を制限している
13		重要情報を外部で保管する場合には、秘密保持、施錠、巡回監視等の適切な管理を行うための契約を締結している。	
管理対象情報が電子情報の場合			
14	電子情報の場合のアクセスの制限等	重要情報の入ったPCや記録媒体の持ち出しの管理や、ID、パスワード等の認証によるアクセス制限を適切に行っている。 重要情報を外部のデータセンター等で管理する場合には、その信頼性を確認した上で秘密保持契約を締結している。	【自No.22※】人の異動に伴うアクセス権(入室権限やシステムのアクセス権)の管理ルールを定めている 【自No.35※】自組織の資産が接続している外部情報システムの利用ルールを定めている 【自No.38】業務で利用する情報機器の自社ネットワークへの接続ルールを定めている 【自No.43】パスワード設定に関するルールを定めている
重要情報を他者に渡す場合			
15	外部委託先等に重要情報を取り扱わせる場合の確認	秘密保持契約書を締結するとともに、適切な管理についての要求事項を事前に明確に提示し、管理状況を確認している。	【自No.35※】自組織の資産が接続している外部情報システムの利用ルールを定めている

【備考】自工会・部工会ガイドラインNo.に※がついているものは、複数の審査項目（2項目）に掲載がある。

4.1.2 情報通信機器産業

電子通信機器産業においては、企業における情報管理に関するガイドライン等を定めていることはなく、個別の分野（スマートホーム等）においてセキュリティガイドラインを定めている。この「スマートホームの安心・安全に向けたサイバー・フィジカル・セキュリティ対策ガイドライン」は、経済産業省「サイバー・フィジカル・セキュリティ対策フレームワーク」を元に、スマートホームに必要となるサイバーセキュリティ上の技術的な対策及び管理項目の明確化を行っている。そのため、技術情報管理認証制度が対象とする情報管理の領域とは異なる。

4.1.3 防衛産業

防衛産業においては、防衛調達において、米国の NIST SP800-171 を参照した新しい情報セキュリティ基準が策定され、2023 年度の契約から適用される見込みである。技術情報管理認証制度では、防衛調達基準も参考として告示基準が策定されていることから、新たな基準が判明次第、告示基準の見直しの必要について検討する必要がある。

4.2 普及のための広報

メールマガジンによる配信等を実施し、本認証制度及び専門家派遣事業の周知を行った。また、認証制度の理解促進のため、経済産業省における HP の改善提案を行った。

4.2.1 メールマガジンによる配信等

技術情報管理認証制度に係る検討会に参加いただいている中小企業関連の団体において、メールマガジンでの配信・HP への掲載を行った。

また、ヒアリングで話を伺った業界団体に対して、技術情報管理認証制度の案内を依頼した。

4.2.2 HP の改善提案

（1） 現状サイトの課題

現状の技術情報管理認証制度ホームページの課題に対して、以下のような方針で対応した。

（1）文字情報のみのため、一目でイメージが伝わりづらい。

＜対応策＞アイコンやテキストを整理して提示する。

（2）行間が狭く、アイコンやラベルなども無いため、読みにくい。

＜対応策＞アイコンやラベルを付与し、行間を整理する。

（3）認証取得を受けたい企業、認証機関になりたい企業への情報が並列で並んでいるため、閲覧者がどちらの情報対象か、わかりにくい。

＜対応策＞想定訪問者毎にタブからリンクを張り情報を整理する。

表 4-2 HP コンテンツの修正案

トップページ	制度概要 新着情報 制度の特徴・メリット パンフレット 認証機関一覧 認証取得事業者一覧 認証を受けた企業からの声／認証機関からの声 FAQ（認証制度に関する様々な事項をカテゴリ化して掲載） お問い合わせ　（フォーム掲載、または連絡先記載。ライトな質問も受け付ける体裁）
認証取得を目指す事業者向け	認証取得のメリット 審査方法、申請方法 （認証取得の際の流れ、所要期間等） 研修素材 セルフチェックシート 監査の指針・監査ガイドライン
認証機関を目指す組織向け	認証機関の役割 申請書式
参考情報	法令、告示 関連リンク　等

図 4-1 ホームページ修正案イメージ

4.3 事業者による自己確認について

告示の改正により、認証機関による「自己適合型認証」は告示から削除となることが決定したが、制度の普及という観点から、事業者が自社の技術情報管理の取組状況を確認する「自己確認」を導入することが有効であると考えられる。今後、各業界の取引時における情報管理のチェック方法なども参考に、自己確認のためのガイドラインやチェックリストを策定することが望ましい。

製造業の業界団体等へのヒアリングから得られた意見は以下の通り。

＜情報保護の実態について＞

情報保護の実態については、業界毎に様々であったが、業界団体として情報管理の取組みを行っている団体はなかった。

- 「安全保障貿易管理」と「営業秘密管理」の両輪で情報管理に取り組んでおり、サイバーセキュリティというよりは、スパイ行為等についての視点を中心に考えている。営業秘密をどう守るかは、個社それぞれでの対応に任せているが、スパイ行為の手口が変わる中で、今後もこれまで通りのやり方で良いかは気になっている。
- 大企業が半数程度あり、情報管理対策の取組みはできている。一方で中小企業の会員は、何をすればよいのか理解できていない面があり、取り組みは進んでいない。特に、自社の技術に対しての意識が高くない。
- 業界に所属する企業の事業としては、特許切れの技術に自社ユニークなものを付加して、オリジナリティを持たせた独自製品として製造・販売するケースが多い。自社技術を守ることより、マーケティングで独自性を打ち出す戦略の方に関心が高いため、情報保護という意識になりづらい。
- 事業内容から、機密度の高い情報が多く、個々の顧客ごとに、情報の取り扱いが詳細に決められている。顧客の事業分野によって要求レベルが異なる。

＜必要な項目について＞

チェックシートに必要な項目については、概ね現状でカバーされているという回答であった。

- 技術情報管理のチェックシートは、網羅性は十分あるように思える。営業秘密管理と合わせて活用していけるかは分からないが、管理レベルとしては厳しい方に合わせることになる。
- 文書管理の面よりは、ウイルス対策などの IT 技術面でのセキュリティ意識や関心が高い。
- 情報管理は、担当者だけでなく、全従業員それぞれが認識して、各自のリテラシーを向上させていくことが必須なので、研修の重要性は高い。

＜チェックシートの示し方について＞

チェックシートをどのような形で提示していくかについては、様々な意見が聞かれた。

- 必要な対策がカタログ的に提示されており、その中から選択できるとよいのではないか。
- ある程度必要な対策が理解できる組織は大枠の項目を示した方がよいが、対策がわからない組織には細かく具体的なレベルで対策を選択できるとよい。
- 対策に難易度があり、重要度によって変更できる方が使いやすいのではないか。
- 対策の例示があるとわかりやすいのではないか。

項目について特に追加すべきという意見はなかったが、項目の示し方に関して、自己確認の目的や、想定するターゲット（レベル感、求める項目等）となる中小企業や以下の観点を踏まえて検討していくことが必要である。

・　対策を具体的に示すか、大枠を示すか
・　選択式とするか、全件必須とするか
・　難易度を設定するか、しないか

5. 今後の方向性

2～4章の調査及び専門家派遣の結果を踏まえ、技術情報管理認証制度の在り方や普及等について検討を行った。以下に今後の方向性について示す。

（1） 事業者による技術情報管理の自己確認に関する仕組みの具体化及び普及啓発

今年度においては、告示の見直しについて検討を行い、自己適合宣言型認証は告示から除外するとともに、その代わりとして普及啓発を目的とした自己確認を設けることで検討を行った。今後、技術情報管理認証制度と共に、自己確認の仕組みを採り入れることに伴い、自己確認のために必要なチェックシートや自己確認を行うためのガイドライン等を定めていく必要がある。また、自己確認の制度を活用し、認証取得事業者を増やすとともに、事業者における情報管理のレベルアップを目指すにおいて、その普及のための方策について改めて検討していく必要がある。

（2） 認証制度の目的に沿った位置づけの明確化

今年度は、技術情報管理認証制度と類似した制度に関する調査を行い、本制度は守るべき情報に特化し、その守り方を提示しているという点で特徴的である点が示された。一方、関連するガイドラインや制度との関係や整合性を整理した上で、改めて本制度の立ち位置を明確に示し、事業者にとってわかりやすく示していくことが必要である。

（3） 告示基準改訂の必要性、及び改訂にかかる運用方法の見直しに関する方針策定

告示基準においては、策定時に参照された関連基準の項目や表現が古くなっているケースがあり、見直しについて検討する必要がある。特に、情報通信分野やサイバーセキュリティにおいては技術の変化が早く、告示という形で定めるべきか、運用の中で参照すべく告示外で定める方がよいのか、告示基準で示す項目やその位置付けについても、周辺で整備すべきドキュメントと合わせて検討する必要がある。特に、本制度においては重要な情報を保護する目的で、情報漏えいの脅威への対応が主となっているが、昨今のサイバーセキュリティ上の脅威として、マルウェア等の不正なプログラムが企業における情報資産に影響を与え、事業継続を脅かすリスクが増大している。このような脅威と対策について、制度の中でどのように扱っていくのか検討し、方針として定めていく必要がある。

また、情報管理に必要な項目を全て告示に含めるのか、難易度や成熟度を考慮した項目にすべきか等、項目の内容は当然のことながら、認証の対象となる項目は選択式になっていることから、事業者自らが選択する形でよいのか、保護対象となる情報のリスク分析結果や関連するガイドラインや基準等に基づき選択すべきなのか等、告示基準と認証方法については関係が深いため、併せて検討することが望ましい。

（4） 審査員や専門家の育成、登録制度の検討

審査員や専門家については、継続的に認証制度に関わり、スキルや知見を高めていくために、一元的に管理し、登録する仕組みについて検討することが、制度の拡大において有効と考えられる。登録制とすることで、専門家・審査員に必要なスキルの明確化と、適切な育成機会の提供を行うことが可能となる。また、登録制とすることで、認証機関の審査員、あるいは専門家として状況に応じて柔軟に派遣していく仕組みを構築することが可能であると考えられる。

（5） 認証機関となることを希望する組織の発掘、認証機関への支援

技術情報管理認証制度を普及するためには、認証機関を増やしていくことも必要となる。近年、認証機関が増えていないことから、認証機関となることを希望する組織の発掘が必要である。このために、公的機関・企業問わず、認証機関となりうる可能性がある対象を明確化していくことが有効と考えられる。これらの認証機関となりうる組織に対しては、審査員派遣や価格の設定等運営方法・支援策を含めた事業モデルの提示などを行い、専門家派遣制度を活用することで、スムーズに認証機関になることを促すことが望ましい。

また、認証機関に対しては、認証制度を普及するためのプログラム（パンフレット、セミナー等の機会）を提供することや、認証機関が相互に情報共有する場を構築し、制度や運営に関する経済産業省からの情報提供、課題やプラクティスの共有を行うなど、認証機関としての事業運営を円滑に行うための支援を行うことも有効と考えられる。

付録１　定期報告ひな形

定期報告ひな形、及び記載例は以下の通り。

表 付-1　定期報告ひな形

									審査	定期報告		
章	節	項	番					内容	確認内容	確認内容	確認日	確認者
1	第四	1	(1)		共通事項	管理対象情報の管理等	管理対象情報の管理簿の作成等	管理者は、持ち出し、複製、廃棄等の管理対象情報の状況を管理するための管理簿を作成する。				
		6	(1)				管理対象情報の適切な管理についての文書の作成等	事業者は、1から5までに定める手順のほか、第二の2により必要と決定した措置を実施するため、管理対象情報の適切な管理についての具体的な実現手法を記載した文書（以下「マニュアル」という。）を作成する。				
			(2)					事業者の取締役等の経営層（管理対象情報を活用し、事業を実施する部門の長を含む。）は、マニュアルを、当該管理対象情報を取り扱う可能性のある全ての者に周知する。				
	第六	1				管理対象情報の漏えいの事故等の発生時等の報告		事業者は、アクセス権者を含む全ての従業員等に対して、管理対象情報へのアクセス権を有さない者がアクセス権者の近傍にいない状態で管理対象情報を取り扱っていることを発見した場合等当該管理対象情報の漏えいが発生し、又はその疑いがあると従業員等が認める場合に、直ちに、管理者等当該事業者が報告先として指定した者に報告をさせるための手順を確立する。				

表 付-2　定期報告ひな形　記載例

									審査	定期報告		
章	節	項	番					内容	確認内容	確認内容	確認日	確認者
1	第四	1	(1)		共通事項	管理対象情報の管理等	管理対象情報の管理簿の作成等	管理者は、持ち出し、複製、廃棄等の管理対象情報の状況を管理するための管理簿を作成する。	管理対象情報管理簿（XX年XX月XX日～XX月XX日記録）を閲覧し、管理対象情報の持ち出し、複製、廃棄等の記録が示されていることを確認した。	管理対象情報管理簿（XX年XX月XX日～XX月XX日記録）を閲覧し、管理対象情報の持ち出し、複製、廃棄等の記録が示されていることを確認した。	20xx/xx/xx	●●
		6	(1)				管理対象情報の適切な管理についての文書の作成等	事業者は、1から5までに定める手順のほか、第二の2により必要と決定した措置を実施するため、管理対象情報の適切な管理についての具体的な実現手法を記載した文書（以下「マニュアル」という。）を作成する。	管理対象情報の管理手法を示したマニュアル（XX年XX月XX日策定、第2版）を閲覧し、管理対象情報の適切な管理についての具体的な実現手法が記載されていることを確認した。	変更無し	20xx/xx/xx	●●
			(2)					事業者の取締役等の経営層（管理対象情報を活用し、事業を実施する部門の長を含む。）は、マニュアルを、当該管理対象情報を取り扱う可能性のある全ての者に周知する。	管理対象情報の管理手法を示したマニュアルの周知記録（XX年度）を閲覧し、経営層がマニュアルを、管理対象情報を取り扱う可能性のある全ての者に周知していることを確認した。 管理対象情報を取り扱う製造部門の従業員へのインタビューにより、マニュアルを認識していることを確認した。	管理対象情報の管理手法を示したマニュアルの周知記録（XX年度）を閲覧し、経営層がマニュアルを、管理対象情報を取り扱う可能性のある全ての者に周知していることを確認した。	20xx/xx/xx	●●
	第六	1				管理対象情報の漏えいの事故等の発生時等の報告		事業者は、アクセス権者を含む全ての従業員等に対して、管理対象情報へのアクセス権を有さない者がアクセス権者の近傍にいない状態で管理対象情報を取り扱っていることを発見した場合等当該管理対象情報の漏えいが発生し、又はその疑いがあると従業員等が認める場合に、直ちに、管理者等当該事業者が報告先として指定した者に報告をさせるための手順を確立する。	管理対象情報の漏えい事故を発見、または疑いがあると認めた場合、報告先として定められた技術等情報管理責任者に対して、報告をするように指示された文書（XX年XX月XX日）を確認した。 本文書が、密週の各部門の朝礼で周知されたことを各部門からの週次報告で確認した。	変更無し	20xx/xx/xx	●●

産業競争力強化法に基づく技術情報管理認証制度の普及促進に向けた調査分析及び専門家派遣等事業
報告書

2022 年 3 月

株式会社三菱総合研究所
デジタル・イノベーション本部
サイバーセキュリティ戦略グループ
TEL 03-6858-3578