経済産業省　御中

令和4年度重要技術管理体制強化事業（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

2023年3月31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・経験やリソースの不足もあり、十分に進んでいないのが実情である。

事業者の多くが技術情報を適切に管理している状況であれば、情報管理の必要性の理解が進み、情報管理が不十分な事業者も情報管理に注力することが見込まれるが、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い状況では、事業者が技術情報管理に取り組むに当たってのハードルが非常に大きい。

そこで、経済産業省は、技術情報の管理に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。）を整備し、令和 4 年度には認証制度をより利用しやすくするために手続の簡素化等の制度改正を実施するなど、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の検討及び運用改善に向けた調査分析、認証制度の取得を進めるための事業者への支援、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 事業者自らが基準適合を確認するための自己チェックリスト及びガイドライン整備

2.1.1 自己チェックリスト及び活用ガイドに対する意見

自己チェックリスト及び活用ガイドの策定にあたり、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（WG）、ヒアリングを通じて意見をいただいた。いただいたご意見について、①記載内容、②形式、③対象、④活用方策の観点で整理した結果を以下に示す。

表 2-1 自己チェックリスト及び活用ガイドに対するご意見と対応案

No.	カテゴリ	ご意見	対応案
1	①記載内容	なぜ対策が必要なのかを記載し、説得力を持たせるべき。実施するメリットに加え、実施しないことによるデメリットを強調することも有効。	各項目について、対策が必要な理由を記載。
2	①記載内容	どれぐらいの規模の事業者かにもよるが、経営者が見て意識付けをするのか、担当者が見て対策を進めるのかによっても書きぶりは異なるだろう。	自己チェックリストは、経営者の指示を受けて担当者が現状確認・報告し、必要な対策を認識するものとして作成する。（活用ガイドは担当者が対策状況を確認するためのもの）
3	①記載内容	自己チェックリストは中小企業でも最低限実施すべき対策として見られるとよい。	最低限実施すべき項目として、「技術等情報漏えい防止措置の実施の促進に関する指針」記載の必要最低限の措置等の項目を踏まえて提示する。
4	①記載内容	自己チェックリストも、基準のここに該当する、だからここはクリアできた、という形で見える化できると、有効に使えると考える。	各項目について、該当する基準（項番）を自己チェックリストの中で示すのではなく、この自己チェックリストの項目はこの基準にあたるので、この基準は満たしているということがわかる説明資料を別途作成する。
5	①記載内容	対応基準に認証基準の番号を示しているが、結びつける意味がどこまであるのか。	
6	①記載内容	基準番号は自己チェックリストにある必要はないと思う。自己チェックリストをやって、認証に関心を持った人に対して対応表がどこかにあればよい。	
7	①記載内容	自己チェックリストに「技術情報管理認証」を示すと、認証に繋がっているように見えるので、自己チェックリストには「認証」という文字がない方がよい。	自己チェックリストにおいて、認証制度を説明する箇所以外は「認証」を使用しない。
8	①記載内容	○△×については、こういう場合は○、こういう場合は△という説明があるとよい。	凡例の形式で、○△×の記載の考え方について説明を加える。
9	②形式	サイバーセキュリティ経営ガイドラインでは、事業者の取組状況を評価するための可視化ツールがあり、レーダーチャートで評価概要が見られる。経営層向けには 10 項目程度に絞るのがよく、項目を人の管理、モノの管理、情報の管理など、分かりやすいキーワードで見せるとよい。	対策状況の評価が、項目数やキーワード等をわかりやすく見える形で提示する。
10	②形式	自己チェックリストは、認証の呼び水の位置付けとして、入門編と初級編で分けるとよいのではないか。入門編は技術情報を守る機運を作るもの（原案の 1～7）で、初級編（原案 8～）で何を取り上げるかは議論する。	自己チェックリストは、ファーストステップとセカンドステップを分けて作成する対応と、ファーストステップとセカンドステップも分けずに記載する案の両案を検討する。

11	②形式	自己チェックリストを分けるというより、ファーストステップ、セカンドステップを明記するということではないか。	
12	②形式	ファーストステップ入門編、セカンドステップ初級編と書かれているが、入門編、初級編という表現ではどちらのレベルが上なのかわかりにくい。入門、初級と書かずにファーストステップ、セカンドステップだけでもよいのではないか。	
13	②形式	入門と初級は一緒に並ぶものではなく、分ける必要もないかもしれない。	
14	②形式	ステップというよりは、基本事項の確認の質問項目、より具体的な対策の質問項目という、質問の種類という観点の分け方だけでもよいのではないか。	
15	②形式	自己チェックリストから興味を持っていただくのはよい。IPA「5 分でわかるセキュリティ自己診断」をイメージして作ると、馴染みのない事業者にも興味を持っていただきやすく、回答もしやすいと思われる。	IPA「5 分でわかるセキュリティ自己診断」を参考に、わかりやすさに配慮すると共に、自己診断・評価・対策実施の流れで構成する。
16	②形式	どの項目がどのカテゴリに対応しているかを示さないと、経営者がレーダーチャートを見てどう改善したらよいかがわからないので、項目とカテゴリのマッピングを示せるとよい。	自己チェックリストの項目と、レーダーチャートのカテゴリのマッピングを示す。
17	②形式	自己チェックリストの結果次第でこういうレベルになるので、ぜひ認証制度にチャレンジしましょうとなることが望ましい。点数を事業者に伝え、伝えたことによってどう認証取得に導くかが重要である。	自己チェックリストの最後のメッセージを、より認証取得に誘導できるものに修正する。
18	②形式	自己チェックリストの結果が低かった事業者が研修等を通じて対策を実施しレーダーチャートの面積が広がる、PDCA の活動を通じて運用面も向上する等、楽しみながら自社の取組を向上できるような連動した取組があるとよい。	事業者が楽しみながら取組の向上につなげられるよう、結果の見せ方について検討する。
19	③対象	自己チェックリストの内容は事業者の規模によって（担当者がいるかどうかによって）異なるのではないか。	専門の担当者が不在の小規模事業者も活用可能できるよう、入門編と初級編に分けて優先順位を分けて取り組めるようにする。
20	③対象	従業員 100 人以下の規模の事業者は対策ができていないこともある。より小規模の事業者をターゲットとして個社のレベルを上げていく方が、産業全体の底上げになるのではないか。	
21	③対象	担当者がいれば ISMS 認証を取りに行くので、そこまでいかない事業者をターゲットとし、ISMS 認証とは棲み分けをした方が良い。	
22	③対象	製造業だけではなく対象事業者を少しでも広げたいが、現在は工場を連想させるマークなので、認証制度の基本的な理解に至るまでが一苦労であるので、検討を進めていただきたい。	制度としては、これまで主に製造業を対象としつつ業種を限定したものではない。自己チェックリストは、この考え方に基づき、業種を限定せずに作成する。
23	③対象	ゆくゆくはあまねく事業者に広げることが望ましいが、まずは製造業中心でよい。	
24	③対象	業界毎に言葉を変えて自己チェックリストを作成している。業界毎の自己チェックリストを活用すれば、認証活動がしやすくなると思われる。	
25	③対象	医療業界や旅行業界においては、自身の業界で用いる言葉と合っていないとやらないと考える。ただし、汎用的な自己チェックリストから始	業種別の自己チェックリストは作成しない。

		めて、次の段階で言葉を換えていくことで考えている。	
26	④活用方策	技術情報管理がいかに重要かについて、制度があることによって周知をするということではないか。	認証制度にも触れ、技術情報管理の重要性について訴える内容とする。
27	④活用方策	技術情報管理認証制度というと一つのイメージに結び付かない。認証制度はブランド力が重要なので、制度の知名度を上げ、相手に容易にイメージしてもらえることが必要である。	イメージしやすい表現、用語を用いる。
28	④活用方策	自己チェックリストに基づく確認の結果、専門家の派遣を受けて対策を進める、派遣を受けて監査ができれば、認証に繋がる。専門家派遣等のインセンティブを紐付けながら制度の普及について検討していくとよい。	自己チェックリストをきっかけとして、他のコンテンツや専門家派遣事業も活かして認証取得につなげるような活用策とする。
29	④活用方策	審査機関と指導助言機関が同一で良いという特徴を活かし、自己チェックリストを認証制度の呼び水の位置づけとするなら意義がある。	
30	④活用方策	自己チェックリストは、認証制度に宣伝効果があるよう、認証制度に興味を持った事業者がまずやってみるのがよいのではないか。事業者の理解とアドバイスを通じて、認証取得に繋げることが重要である。	
31	④活用方策	自己チェックリストについては、事業者が取引先に対して対策状況を確認するために使えるようなものになるのがよい。	発注側の活用について、別途実施するヒアリング等を踏まえて検討する。
32	④活用方策	中小企業は顧客から自己チェックリストが送られて、回答次第で仕事をもらう立場としての優劣がつくのであれば、認証に申し込むきっかけとなる。その手段として自己チェックリストを使うということであればよい。	
33	④活用方策	自己チェックリストについては、自己宣言の代替ではなく、認証の準備段階とすべき。その場合、実施内容を簡単にするのではなく、活用ガイドで補足し、情報管理を実施できることを重視すべきである。	記載する対策水準を下げることはせず、対策を説明した活用ガイドをセットで示す。
34	④活用方策	認証制度は知らないがたまたま情報セキュリティ管理に関心があって経済産業省の WEB ページに来る人もいるはず。自己チェックリストで確認したら弱い点があり、WEB ページに認証制度のことも書いてあるからアドバイスを受けてみよう等、認証制度に興味を持ってもらうような誘導の仕方もある。	自己チェックリストや活用ガイドの作成にあたって考慮する。
35	④活用方策	自己チェックリストの利用者の情報について、保存しないというポリシーを明確化した方がよい。	自己チェックリストの提示の際に配慮する。

2.1.2 自己チェックリスト

事業者自らが、認証制度の基準の考え方をもとに自社の情報セキュリティの取組状況を確認できるよう、自己チェックリストを整備した。自己チェックリストは、技術等情報漏えい防止措置の実施の促進に関する指針（指針告示）において必要最低限とされている対策に加えて、第三者への情報預託時の対策を追加した19項目を、それぞれ簡潔に示した。19 項目はさらにファーストステップ（経営の視点から必要な事項を示したもの）とセカンドステップ（実務的な視点から、情報の守り方や形態等によって検討す

る事項を示したもの）に分けて整理した。

自己チェックリストは、WEB ページ上で Excel 形式としても提供し、A4 裏表 1 枚で印刷できる形式とした。事業者が Excel に情報管理の取組状況を入力すると、評価結果が取組分野ごとの達成状況を示したレーダーチャート及び総合評価点で、取組状況の評価を可視化できる機能を含めた。自己チェックリストを利用する事業者が、取組結果の評価コメントを通じて情報管理の取組を徐々にレベルアップすることを目指し、将来的には認証取得に繋げていけるよう、取組状況に対する講評コメントの内容を工夫するとともに、自己チェックリストの最後に認証制度へ誘導できる情報を記載した。

技術情報管理　自己チェックリスト

○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。判断に迷ったときは「活用ガイド」もご参照ください。

「○」実施している　　：全従業員が、全ての守るべき情報（※）についておおむね実施している
「△」一部実施している：一部の従業員・一部の守るべき情報で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で実施できていない
「－」該当しない　　：取引先から預けられた情報がない、情報を外部に預けていないなど、項目の条件に該当しない（一部の項目のみ）

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

確認者		チェック欄
情報セキュリティ責任者		
情報セキュリティ担当部門		

ファーストステップ（経営の視点）

1st ステップ

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、一目でほ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）情報漏えいが起きそうになっていないかをいつも確認し、漏えいが起きたら対応する。 （5）（2）～（4）の取組状況を記録する。	○
6	情報セキュリティの責任者が誰なのか、全従業員がしっかり分かるようにしている。	○
7	守るべき情報を作ってから廃棄するまでの全期間、しっかり管理するための取組を従業員が実践している。	○
8	全ての従業員に対して、情報セキュリティに関する意識を高めるためのトレーニング機会を設けている。	○
9	守るべき情報の漏えいや不正な取扱いに気づいた場合の報告先を決めて、全従業員に知らせている。	○
10	守るべき情報の漏えいや不正な取扱いが発生した場合の対応手順を定めている。	○

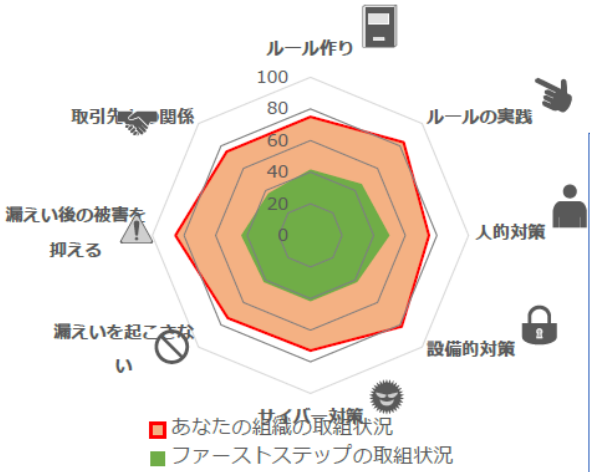
図 2-1　自己チェックリスト（表面）

セカンドステップ（実務の視点）

セカンドステップは情報の漏えいを防ぐための具体的な対策です。
実務に沿って守るべき情報の種類を確認し、それぞれ必要な対策を実施しましょう。

	内容	チェック欄
セカンドステップ（実務視点からの具体的対策）		
11	守るべき情報を外部委託先などに渡す場合には、守るべき情報の第三者への開示の禁止を含む秘密保持契約を結んでいる。	△
12	守るべき情報に接することができる人を定め、その人以外が守るべき情報に接することがないよう制限している。	△
守るべき情報が金庫などの保管容器に保管できる場合（例えば、書類・試作品など）		
13	守るべき情報を保管容器に施錠して保管している。	△
14	守るべき情報を書庫、金庫などから持ち出した場合に取り扱ってよい場所を定めている。	○
守るべき情報が金庫などの保管容器に保管できない場合（例えば、製造装置など）		
15	守るべき情報が置かれる場所を立入制限区域とし、守るべき情報に接することができる人以外が立ち入らないよう制限している。	○
16	守るべき情報を他社の事業所等で取り扱う場合に、秘密保持契約を結び、施錠、巡回監視などを依頼している。	△
守るべき情報が電子情報の場合		
17	守るべき情報が保存されたPCや記録媒体の持ち出しを管理するなど、守るべき情報に接することができる人以外に情報を見られないよう制限している。	○
18	電子ファイルにパスワードを設定するなど、守るべき情報に接することができる人以外に情報を見られないよう制限している。	△
19	守るべき情報をクラウドサービスなどに保存するときは、信頼性を確認して保存先を決め、秘密保持契約を結んでいる。	△

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。）



総合評価点 **77点**

お疲れ様でした。
あなたの組織は、このチェックリストで確認できる取組を半分以上達成しています。
活用ガイドや経済産業省の技術情報管理認証制度WEBページで提供している研修素材などを活用し、満点を目指して対策を進めましょう。
また、第三者から専門的な指導・助言を受けられる技術情報管理認証への挑戦もご検討ください。

情報セキュリティ対策に関する助言を受けたり、対策が十分かどうか第三者機関による審査が受けられる「技術情報管理認証」については、経済産業省WEBページをご確認ください。

技術情報管理認証制度　検索

【お問合せ先】経済産業省　安全保障貿易管理課　TEL：03－3501－2800
MAIL：bzl-technology_management@meti.go.jp

図 2-2 自己チェックリスト(裏面)

2.1.3 活用ガイド

活用ガイドについては、自己チェックリストに示した項目について、その対策を行う理由、対策例を示した。5 ページの構成としたが、1～4 ページ目は対策の解説を中心に記載し、そこだけを独立した 4 ページの見開きパンフレットとして活用できる形で構成した。内容は、対策の解説の他、認証制度の説明、項目と基準告示の番号との対比を示した。

技術情報管理　自己チェックリスト　活用ガイド

自己チェックリストにおいて、対策ができているか判断に迷ったときは、この活用ガイドをご確認ください。

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。

1	経営者とともに、守るべき情報を特定している。
	守るべき情報とは、その情報が漏えいした場合に、 ・自組織の競争力に大きな影響を与えるもの ・自組織の信用や顧客等との信頼関係に大きな影響を与えるもの（顧客等から預けられた情報など） のことを言います。
理由	守るべき情報を明確にしないと、組織において情報の管理ができません。経営者が関わり、自組織の経営の観点から、どの情報を守るべきかを決める必要があります。
対策例	金型・試作品、製造装置・製造プロセス情報、研究情報、製造設計図・CAD、顧客情報・仕入れ先情報、業務マニュアル・製造/業務ノウハウなど、自社が持つ情報を洗い出し、経営者がその価値を判断して、守るべきかどうかを決めます。

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。
理由	守るべき情報の形態に合った保管を行わないと、情報漏えいを起こす恐れがあります。また、保管場所を明らかにしないと、情報が盗み出された場合にすぐに気づくことができず、被害が拡大する恐れがあります。
対策例	紙情報の場合はキャビネット、電子情報の場合はサーバ・PC・クラウド、試作品など小さな物は保管庫・金庫、製造装置など大きな物は設置された拠点・工場に保管します。

3	守るべき情報には、一目でほかの情報と区別できるよう、目印をつけている。
理由	守るべき情報だと思われないと、適切に管理されません。
対策例	紙情報の場合：情報が記載された紙に管理対象情報であること（社外秘等の表示）を記載します。 電子情報の場合：ファイル名に管理対象情報であることを記録します。 試作品・製造装置などの物の場合：当該物そのもの又はその保管容器に表示します。

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。
理由	自社だけで対策方法を定めると、顧客が求める対策と異なることで、対策が行われていないと判断される恐れがあります。
対策例	取引先の意向で示された情報の取り扱いに関する条件に従って、対策を行います。

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)情報に触れる職員を制限・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)情報漏えいが起きそうになっていないかをいつも確認し、漏えいが起きたら対応する。 (5)(2)～(4)の取組状況を記録する。
理由	管理者を定めないと、役割や責任をもって情報管理を進められません。 また、組織における管理者の業務として正式に定めることで、管理者が情報管理に取り組む時間を確保するとともに、その成果を人事評価に反映することができます。
対策例	管理者として総務部門の責任者、情報システム部門の責任者、品質管理部門の責任者、製造部門の責任者などを定めます。

図 2-3　活用ガイド（P1）

6	情報セキュリティの責任者が誰なのか、全従業員がしっかり分かるようにしている。
理由	責任者が認識されないと、従業員が管理者の指示に従わない恐れがあります。 責任者が認識されることで、従業員が報告や相談をしやすくなります。
対策例	責任者を社内のイントラネットに掲載します。

7	守るべき情報を作ってから廃棄するまでの全期間、しっかり管理するための取組を従業員が実践している。
理由	情報の作成から廃棄まで一貫して対策を行わないと、対策が不十分なところから情報漏えいを起こす恐れがあります。
対策例	守るべき情報の管理簿を作成し、守るべき情報には、情報に接することができる人のみに伝えられる、閲覧できるような手順を定めます。また、守るべき情報の複製や廃棄の手順を定めます。

8	全ての従業員に対して、情報セキュリティに関する意識を高めるためのトレーニング機会を設けている。
	トレーニングにおいて以下のうち必要なものを含みます。 （1）技術等の情報と守るべき情報の違い （2）守るべき情報を適切に管理することの重要性、意識 （3）守るべき情報を含む技術等情報の漏えいとその結果の事例 （4）関係法令の内容 （5）マニュアル、重要情報の適切な管理に係る文書の内容 （6）関係法令等に違反した場合の処分等 （7）重要情報の漏えいの事故等発生時の報告手続 （8）標的型メール等の手口・ウィルス、感染防止の対策、感染した場合の対処の手順
理由	全ての従業員が情報セキュリティに対する意識を高めないと、従業員の対策の不備から情報漏えいを起こす恐れがあります。また、情報漏えいの兆候や事故が発生した際の従業員からの報告が遅れ、被害が拡大する恐れがあります。 情報セキュリティの意識が高い職場は、情報漏えいを起こしにくくなります。
対策例	全従業員に対して、情報の取扱いに関するe-learningを1年に1回実施します。週に1回、朝礼で情報の取扱いに関する注意喚起を行います。

9	守るべき情報の漏えいや不正な取扱いに気づいた場合の報告先を決めて、全従業員に知らせている。
理由	情報漏えい事故や不正な取扱いを見つけた場合の報告先がわからないと、報告が遅れ、情報漏えいの被害が拡大する恐れがあります。
対策例	情報漏えい事故や不正な取扱いに関する報告先を、e-learningで周知します。

10	守るべき情報の漏えいや不正な取扱いが発生した場合の対応手順を定めている。
理由	情報漏えい事故が発生した場合の対応手順を定めていないと、事故発生時に迅速に対応することができません。
対策例	責任者が情報漏えいの報告を受けた場合に、証拠を集めたり、事実を確認する手順や、対応を検討するための社内体制を定めます。

アイコンは、各項目がチェックリストで示されるレーダーチャートのどの項目に対応しているかを示しています。

ルール作り	ルールの実践	人的対策	設備的対策
サイバー対策	漏えいを起こさない	漏えい後の被害を抑える	取引先との関係

図 2-4 活用ガイド（P2）

セカンドステップ（実務の視点）

セカンドステップは情報の漏えいを防ぐための具体的な対策です。
実務に沿って守るべき情報の種類を確認し、それぞれ必要な対策を実施しましょう。

11	守るべき情報を外部委託先などに渡す場合には、守るべき情報の第三者への開示の禁止を含む、秘密保持契約を締結している。
理由	外部委託先の情報セキュリティを契約で定めていないと、外部委託先等が情報を適切に管理せず、情報漏えい事故を起こす恐れがあります。また、外部委託先等が情報漏えい事故を起こした際に、責任を問えなくなる恐れがあります。
対策例	外部委託先等が、自組織からの情報の取扱いに関する指示に対応できるかどうか事前に確認し、秘密保持契約を交わした後に、情報を引き渡します。

12	守るべき情報に接することができる人を定め、その人以外が守るべき情報に接することがないよう制限している。
理由	情報に接することができる人の制限がなされていないと、守るべき情報に接することができる人以外が情報を盗み出す恐れがあります。
対策例	守るべき情報に接することができる人のみが、その情報を扱えるような手順を定めます。 守るべき情報に接することができる人の範囲を、定期的に見直します。 退職等により必要がなくなった従業員については、守るべき情報に接することができる権利を直ちに失効させます。 守るべき情報に接することができる人との秘密保持契約を交わします。

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、書類・試作品等）

13	守るべき情報を保管容器に施錠して保管している。
理由	情報に接することができる人以外が、守るべき情報に近づきやすい、あるいは持ち出しやすいと、情報漏えいを起こす恐れがあります。
対策例	守るべき情報を保管する金庫などを、施錠して管理します。 保管容器は、近づく者を確認することができる場所（カメラや人感センサーの設置、視認できるレイアウト）に設置します。

14	守るべき情報を書庫、金庫などから持ち出した場合に取り扱ってよい場所を定めている。
理由	情報に接することができる人以外が、守るべき情報に近づき、情報漏えいを起こす恐れがあります。 持ち出した際の取扱い場所を明らかにしないと、情報が盗み出された場合に気づくことができず、また気づいた後も状況の把握や原因の調査が難しくなることで、漏えいの被害が拡大する恐れがあります。
対策例	守るべき情報に接することができる人が、情報を金庫から持ち出し、取扱いをする場所を限定する手順を定めます。 守るべき情報の運搬時の持ち出し、取り扱う場所への運搬、保管容器への保存について、情報に接することができる人に限るための手順を定めます。

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）

15	守るべき情報が置かれる場所を立入制限区域とし、守るべき情報に接することができる人以外が立ち入らないよう制限している。
理由	情報に接することができる人以外が、守るべき情報に近づきやすい、あるいは持ち出しやすいと、情報漏えいを起こす恐れがあります。
対策例	守るべき情報が管理される立入制限区域の入退室管理を行います。 守るべき情報が管理される立入制限区域に不正に侵入する者の監視（カメラやセンサーの設置）を行います。 守るべき情報が管理される立入制限区域に不正に侵入する者が検知された場合の警備員等の駆け付け体制を整備します。

16	守るべき情報を他社の事業所等で取り扱う場合に、秘密保持契約を結び、施錠、巡回監視などを依頼している。
理由	他社に求める情報管理の取組を契約で定めていないと、他社が情報を適切に管理せず、情報漏えい事故を起こす恐れがあります。 他社が情報漏えい事故を起こした際に、責任を問えなくなる恐れがあります。
対策例	守るべき情報を取り扱う他社が、建物の施錠・巡回監視を依頼し、契約を交わします。

図 2-5 活用ガイド（P3）

管理対象情報が電子情報の場合

17	守るべき情報が保存されたPCや記録媒体の持ち出しを管理するなど、守るべき情報に接することができる人以外に情報を見られないよう制限している。
理由	情報に接することができる人以外が、守るべき情報に近づきやすい、あるいは持ち出しやすいと、情報漏えいを起こす恐れがあります。
対策例	守るべき情報が保存されたPCや記録媒体の持ち出し手順を定めます。 守るべき情報を取り扱うデスクは常に整理整頓し、守るべき情報が万一持ち出されてもすぐに気づくようにします。
18	電子ファイルにパスワードを設定するなど、守るべき情報に接することができる人以外に情報を見られないよう制限している。
理由	情報に接することができる人以外が、守るべき情報に近づきやすい、あるいは持ち出しやすいと、情報漏えいを起こす恐れがあります。
対策例	PCにログインするために、1人に1つ、別々のIDを割り当てます。 IDを割り振られた人が、それぞれの業務に合わせて、電子ファイルを見られる範囲を定めます。
19	守るべき情報をクラウドサービスなどに保存するときは、信頼性を確認して保存先を決め、秘密保持契約を結んでいる。
理由	外部事業者に求める情報管理を契約で定めていないと、外部事業者が情報を適切に管理せず、情報漏えい事故を起こす恐れがあります。また、外部事業者が情報漏えい事故を起こした際に、責任を問えなくなる恐れがあります。
対策例	クラウド等を管理する者の信頼性を示す、ISO／IEC27017 の認証、日本セキュリティ監査協会クラウドセキュリティ推進協議会によるCSマークの取得の状況等を確認します。

情報セキュリティ対策に関する助言を受けたり、対策が十分かどうか第三者機関による審査が受けられる「技術情報管理認証」の取得もご検討ください。

技術情報管理認証制度

- 情報セキュリティの取組をマークで対外的に示せます
- 国が主導する制度のため、お客様や取引先の信頼につながります

取組手順

専門家の助言や第三者による認証を受けたい方 ▶ 国認定の認証機関に申込 ▶ 情報管理に関する専門家の助言※ ▶ 国の基準を満たすか審査 ▶ 認証（国の基準を満たせば）

国の基準に則った対策を自身で進めたい方 ▶ 自己チェックリストで自己点検 ▶ 研修素材を見ながら取組実施

※ 希望する場合のみ助言を受けられます。
助言を行わない認証機関もありますので、詳細は認証機関にお尋ねください。

技術情報管理認証制度　検索

【編集・お問合せ先】経済産業省　安全保障貿易管理課
ＴＥＬ：０３－３５０１－２８００
ＭＡＩＬ：bzl-technology_management@meti.go.jp

図 2-6 活用ガイド（P4）

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しています。
チェックリストの各項目について、対応する技術情報管理認証制度の基準は以下の通りです。

ファーストステップ（経営の視点）		
1	経営者とともに、守るべき情報を特定している。	Ⅰ 共通事項 第一
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。	Ⅰ 共通事項 第一
3	守るべき情報には、一目でほかの情報と区別できるよう、目印をつけている。	Ⅰ 共通事項 第二 1
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。	Ⅰ 共通事項 第二 3
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)情報漏えいが起きそうになっていないかをいつも確認し、漏えいが起きたら対応する。 (5)(2)～(4)の取組状況を記録する。	Ⅰ 第三1(1)
6	情報セキュリティの責任者が誰なのか、全従業員がしっかり分かるようにしている。	Ⅰ 第三1(2)
7	守るべき情報を作ってから廃棄するまでの全期間、しっかり管理するための取組を従業員が実践している。	Ⅰ 第四 柱書き
8	全ての従業員に対して、情報セキュリティに関する意識を高めるためのトレーニング機会を設けている。	Ⅰ 第五 柱書き
9	守るべき情報の漏えいや不正な取扱いに気づいた場合の報告先を決めて、全従業員に知らせている。	Ⅰ 第六 柱書き
10	守るべき情報の漏えいや不正な取扱いが発生した場合の対応手順を定めている。	Ⅰ 第六 柱書き
セカンドステップ（実務の視点）		
11	守るべき情報を外部委託先などに渡す場合には、守るべき情報の第三者への開示の禁止を含む、秘密保持契約を締結している。	Ⅵ 柱書き
12	守るべき情報に接することができる人を定め、その人以外が守るべき情報に接することがないよう制限している。	Ⅱ 柱書き
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）		
13	守るべき情報を保管容器に施錠して保管している。	Ⅲ 柱書き
14	守るべき情報を書庫、金庫などから持ち出した場合に取り扱ってよい場所を定めている。	Ⅲ 柱書き
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）		
15	守るべき情報が置かれる場所を立入制限区域とし、守るべき情報に接することができる人以外が立ち入らないよう制限している。	Ⅳ 柱書き
16	守るべき情報を他社の事業所等で取り扱う場合に、秘密保持契約を結び、施錠、巡回監視などを依頼している。	Ⅳ 柱書き
管理対象情報が電子情報の場合		
17	守るべき情報が保存されたPCや記録媒体の持ち出しを管理するなど、守るべき情報に接することができる人以外に情報を見られないよう制限している。	Ⅴ 柱書き
18	電子ファイルにパスワードを設定するなど、守るべき情報に接することができる人以外に情報を見られないよう制限している。	Ⅴ 柱書き
19	守るべき情報をクラウドサービスなどに保存するときは、信頼性を確認して保存先を決め、秘密保持契約を結んでいる。	Ⅴ 柱書き

図 2-7 活用ガイド（P5）

2.1.4 自己チェックリスト及び活用ガイドの活用方策

自己チェックリストは、産業界全体の情報セキュリティ対策の底上げに活用されることを目的としつつ、対応した事業者を認証取得へ誘導できる構成とした。自己チェックリストは、経済産業省の WEB ページに掲載し、事業者に自主的に活用いただくものとした。自己チェックリストのダウンロード時に企業名等を入力する、自己チェックリストの入力後の結果を送信する、あるいは経済産業省側にデータとして残す等、経済産業省に対する結果のフィードバックを求めることはせず、あくまでも事業者が自主的に入力し、結果を自社内で活用する利用方法を想定した。活用ガイドも同様に経済産業省の WEB ページに掲載し、自己チェックリストと共に活用いただく形を想定した。

自己チェックリストは、経営者が担当者に対策の指示を出し、担当者が自社の対策状況の確認を行うために利用できるものとするが、その事業者に情報管理を専門としている担当者がおらず、担当者が初めて情報管理に取り組む場合も理解しやすい内容・表現とするよう留意した。

以下に、認証制度において提供している各種ツールと、情報管理の「重要性の認識」「対策の認識」「対策の推進」の各フェーズにおける主に想定する対象者を整理する。

対象者		提供ツール	
経営者	**【重要性を認識するフェーズ】** 情報管理の重要性を知り、予算や体制を整備するフェーズ	自己チェックリスト	経営者が、担当者に対して自社の現状の確認と、対策を指示
担当者（※1）	**【重要性を認識するフェーズ】** 情報管理の重要性を知り、必要な対策を認識するフェーズ	自己チェックリスト	担当者が、（経営者の指示を受け）自社の現状確認と、必要な対策を理解
	【対策を認識するフェーズ】 情報管理の重要性は理解するも、具体的な対策方法を理解するフェーズ	自己チェックリスト	担当者が、取組状況を確認
		活用ガイド	担当者が、確認方法を理解しながら、取組状況を確認
		研修素材	担当者が、具体的な対策を理解し、自らが対策を実施
		専門家派遣	担当者が、専門家のアドバイスを受けながら、具体的な対策を実施
	【対策を進めるフェーズ】 情報管理の具体的な対策推進に取り組んでおり、認証取得が期待できるフェーズ	研修素材	担当者が、具体的な対策を理解し、認証取得に向けた取組を推進
		監査ガイドライン	担当者が、認証取得に向けた対策状況の内部監査を実施
		専門家派遣	担当者が、専門家のアドバイスを受けながら、認証取得のための対策を実施、あるいは内部監査を実施

（※1）担当者が不在の事業者においては、経営者自身である場合もある。

図 2-8 自己チェックリストと活用ガイドを含む、認証制度の各種ツールの活用方法

2.2 漏えいを防止するために必要な措置に関する基準の内容の検討

認証制度における基準について、認証制度の目的、内容等において類似する国内外の他の制度や情報管理制度、知財管理制度で求められる基準と比較し、より多くの事業者が認証制度を活用でき、かつ技術情報管理に一定の実効性を確保する観点から修正が必要なものを抽出し、具体的な修正案を作成した。修正案の作成に当たっては、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（基準告示）の改定を念頭に作業を行った。

修正が必要な点についての整理及び修正案の作成にあたり、検討会、WG、ヒアリングを通じて意見をいただいた。いただいたご意見について、①基準の示し方について、②基準の対象範囲について、③業種について、④環境変化への対応について、⑤その他・共通事項への対応について、5 つの項目で整理した。

2.2.1 基準告示の修正に当たっての検討

（1） 基準の示し方について

基準の示し方については、以下の方針で進めることが望ましいと考えられる。

- 必須として対応を求める事項を明確化する。
- 求める事項は達成目標として示す。
- 認証取得に当たっては、実施する具体的な対策方法を選択できるようにする。
- 求める水準別にレベル分けして示すことも検討する。

基準の示し方に関して、いただいたご意見と対応案を以下に示す。

表 2-2 基準の示し方に関するご意見と対応案

No.	カテゴリ	ご意見	対応案
1-1	① 基準の示し方	政府情報システムのためのセキュリティ評価制度（ISMAP）では、三桁管理策はマストで実施する事項、四桁管理策は提供サービスによって選択する事項となっている。このように、実施すべき項目が明確になっていた方がよい。	認証取得事業者に必ず対応することを求める達成目標を明確化する。
1-2	① 基準の示し方	現行基準は必須項目が抽象的な記載で記されており、残りの具体的な項目の選択は事業者の裁量に任されている。同じ認証制度の中で、差ができてしまう基準となっている。第三者から見て認証取得した事業者が必ず実施できている最低限の対策が明示されることが望ましい。	
1-3	① 基準の示し方	産業界の裾野での情報セキュリティの取組を広げるために認証制度があるのであれば、その目的を達成するために必要な基準が書かれるようにしていただきたい。	
1-4	① 基準の示し方	業界によって高度な対応を求められる要件は違う。製造業を中心にできるだけ広く参加していただくことを目指すのであれば、最低限満たすべき基準を示す方針でやった方が良いのではないか。	

1-5	① 基準の示し方	現行基準のⅢⅣⅤの柱書の下に例示的な項目から、最低限このレベルでしなければならないことを含んだ基準にすれば、この認証を取っている事業者であれば最低限こういうことはできているということが判断できる。	
1-6	① 基準の示し方	最低限実施すべき具体的対策を明示すべき。	
1-7	① 基準の示し方	最低限実施すべき具体的対策は制度の目的に照らして決定すべき。	
1-8	① 基準の示し方	ガイドラインとしては抽象度が高い記述にした方がよく、具体的に何をするのかをナビゲーションする方がよい。	
1-9	① 基準の示し方	求める最低限のものが書かれてあればよく、それ以上強くするには事業者がやればよい。意味のある認証とするには、最低限の対策が見えた方がよい。	
1-10	① 基準の示し方	必須をきちんと定めた方がよい。必須項目を順次実施していくことで、対策ができていけば、レベルアップすることにもなる。	
1-11	① 基準の示し方	ガイドラインとしては抽象度が高い記述にした方がよく、具体的に何をするのかをナビゲーションする方がよい。情報の重要度や漏えいした場合のリスクに応じて守り方が違うことを示すという整理の仕方はあり得る。	基準においては、達成すべき目標のみを必須項目とし、具体的な対策方法は事業者が選択できるようにする。
1-12	① 基準の示し方	必須項目の記載をもとに審査しており、具体的な対策は、事業者の状況に応じて個別に判断し、助言を行っている。	
1-13	① 基準の示し方	基準では達成すべき目的のみを示す方針に賛成である。実現するには例えばこういう方法があると示せればよく、実現方法は事業者の裁量に任せることが望ましい。	
1-14	① 基準の示し方	対策の目的を示し、対策の方法論は柔軟性を与えていただけるとよい。	
1-15	① 基準の示し方	基準は抽象的に表現されていればよい。	
1-16	① 基準の示し方	具体的な対策はあくまで例示として扱い、審査担当者に裁量を持たせるべき。	
1-17	① 基準の示し方	来年度以降で構わないので、もう少し具体化した基準にした上で、最低限のレベルを事業者自身が確認可能な自己チェックリストにした方がよいのではないか。踏み込んだ基準で、自社の状況を具体的にチェックできることが望ましい。	来年度以降の基準の見直しと合わせて検討する。
1-18	① 基準の示し方	ISMS 認証を意識する必要はなく、文章や言葉を現実的な表現やわかりやすい表現にして、より小規模な事業者でもわかるような表現とすべき。	基準の改定に当たって、分かりやすい表現となるよう留意する。
1-19	① 基準の示し方	自動車業界のサイバーセキュリティガイドラインはレベル分けされている。	求める水準別にレベル分けして示すことも検討する。

1-20	① 基準の示し方	レベル分けをすることも考えてもよい。現状の必須項目だけだと少なすぎるので、基本はここまで、さらにこの事業者だと 50 項目、80 項目満たしているというような考え方がよいのではないか。業界によって選択肢は異なるかもしれないので、幅を持たせてもよいと考える。	
1-21	① 基準の示し方	どこにも通用して、誰もが当たり前と思う基準作りが重要である。審査員が大変になるかもしれないが、その業種に合わせた判断で助言や審査をする方が柔軟であり、本質を抑えられると思う。	基準の改定に当たって、特定の業種を前提としない表現となるよう留意する。
1-22	① 基準の示し方	管理対象情報の特定について、認証制度で明確に書けるとよいのではないか。	基準の改定に当たって、管理対象情報の特定についても、達成すべき目標を明記する。
1-23	① 基準の示し方	情報が漏えいした場合などに会社の経営が成り立たなくなるかもしれないケースはしっかり対応し、そうでないケースはもう少し緩くてもよい、という整理の仕方はあり得る。	基準の改定に当たって、管理対象情報に応じた管理策の選定を達成目標に加えることを検討する。
1-24	① 基準の示し方	絶対にやるべきこと、やった方が望ましいことを分けられると目標が明確化するが、分ける基準が明確になるかはかなり難しい。ISMS 認証の考え方と同様に、統制目標を明確にし、その統制目標に絶対必要な事項を挙げ、それ以外は実装しない理由を明らかにし、強制しないという方法もある。	基準の改定に当たって、選択すべき対策が分かりやすい表現となるよう留意する。
1-25	① 基準の示し方	他のガイドラインの項目を参照する場合、そのガイドラインを満たしていることは誰も保証できない。対応が説明しやすくなる、ということであれば問題ない。あくまでも認証制度の該当する項目を実施していれば、認証制度に対応するのは楽というレベル感であろう。「相当」「対応」というのが正しい言い方であろう。	基準策定時に他のガイドラインを参照した場合、該当するガイドラインを満たすという表現はせず、「参考になる」「対応する」等の表現を用いる。
1-26	① 基準の示し方	自動車セキュリティガイドラインのレベル 1 を満たすかどうか、同等性は別に証明しなければならないと考える。	
1-27	① 基準の示し方	技術水準は進化しており、具体的な目標値を記載するのは難しい。マネジメントサイクルの年 1 回等は書けるが、それ以上は難しいのではないか。	技術的な要件については数値はできるだけ記載せず、数値基準を満たす必要がある場合のみ数値基準を記載する。
1-28	① 基準の示し方	客観的な数値については、問題が生じない限り示さない方が良い。シュレッダーの場合は「できる限り復元が難しい」くらいの表現が良い。	
1-29	① 基準の示し方	数値に関しては、参考例を書くのは良いものの、基準にしてしまうと満たさなければいけない、となる。ある程度汎用的な表現をした後、参考事例が書いてあるならば良い。数値基準を満たさないといけないという特別なものがあれば、数値は書いても良い。	
1-30	① 基準の示し方	文言で同じようなものは同じように記してほしいというのはあるが、二重に掲載されるのに異論はない。異なるのであれば明確にすべきである。	同じ内容を要求する場合は同一表現とし、異なる内容である場合は明確に異なる表現とする。 必要な場合は重複して記載することも妨げない。
1-31	① 基準の示し方	重複する項目は、削除してなるべくシンプルにしていただきたい。事業者の方から、この項目は先ほどの項目と同じかどうか、質問が来るケースもある。	
1-32	① 基準の示し方	あくまでも上に示した項目が必須であり、下に記した項目を選択としてはどうか。例示的なものは推奨策としての例示にしてはどうか。文言	上が全般事項で、下が細部事項という関係として整理する。

		としては「・・・するとともに、次の例により、及びその他必要な措置を実施する。」ではないか。」	
1-33	① 基準の示し方	必須事項と選択事項ではなく、上が全般事項で、下が細部事項という関係にした方が良い。必須とすると、これだけでよいという誤った認識になる懸念も持つ。	

（2）基準の対象範囲について

基準の対象範囲については、以下の方針で進めることが望ましいと考えられる。

【新規追加する点】

- ISO/IEC 27001 の 2022 年改訂で導入されたサイバーセキュリティの要素を取り込む。（米国 NIST サイバーセキュリティフレームワーク（CSF）で示されたような検知・対処についても、中小事業者にとって無理のないレベルで含む。）
- ISO/IEC 27001 で要求される情報の完全性、可用性について、基準の分類を調整する。

【修正を行う点】

- ISMS 認証を参考にしつつ、組織におけるマネジメントシステムの確立を厳密に要求することはせず、中小企業が対応可能な基準とする。
- ヒューマンエラーや無知による情報漏えいへの対策については、必要な修正を加える。
- 自工会/部工会・サイバーセキュリティガイドラインとの整合を考慮する。

基準の対象範囲に関して、いただいたご意見と対応案を以下に示す。

表 2-3 基準の対象範囲に関するご意見と対応案

No.	カテゴリ	ご意見	対応案
2-1	②基準の対象範囲	ISO/IEC 27002 の改訂でもサイバーセキュリティの視点が入ってきており、米国のサイバーセキュリティフレームワーク（CSF）で示される検知や対処が重要になっている。中小企業に検知や対処を求めるのは厳しいので、他の施策の活用も含め、制度設計しても良いのではないか。	サイバーセキュリティの視点や、CSF の検知や対処を取り込む。 ただし、CSF の要求事項は難しいため、CSF の視点が取り込まれている ISO/IEC 27002 をベースにして基準を策定する。
2-2	②基準の対象範囲	サイバーセキュリティ上、難しいのは検知である。対象はサーバに重要な情報を保存しているような企業に限られるかもしれないが、それを基準にするのは厳しい。従来通り ISO/IEC 27002 をベースにして基準を作っていった方がよい。	
2-3	②基準の対象範囲	ヒューマンエラーや知識がないことで、インシデントとなるケースについて、認証制度のスコープに入れるか。営業秘密を持っている人に接触してくる人に対して対応できているかという観点もある。	ヒューマンエラーや無知による情報漏えいへの対策については、現行基準でも一定の配慮がなされているが、検討のうえ必要な修正を加える。
2-4	②基準の対象範囲	ISMS 認証をベースにして、簡易版という位置づけの方がわかりやすいのではないか。 ISO/IEC 27002 との整合性を取り、この項	ISMS 認証が情報の完全性、可用性も規定しているのに対し、認証制度はそれらと重複する部分もあるものの基本的には情報漏え

		番がこれということがわかればよいのではないか。	い防止に限っており、すべて整合させることは困難。 他方、基準改正に当たっては ISO/IEC 27002 でも同様の要求がある対策については、対応関係が複雑にならないよう、基準の分け方等を調整する。
2-5	②基準の対象範囲	認証取得は、お客様から信頼できる事業者と思われるひとつのカードになる。自動車業界のサイバーセキュリティガイドラインを意識すべきではないか。	見直しに当たって、自動車業界のサイバーセキュリティガイドラインとの整合を考慮する。
2-6	②基準の対象範囲	認証制度が信頼性を得るには、自動車業界のサプライチェーンにおいて利用されているサイバーセキュリティガイドラインがひとつの目安になるのではないか。	
2-7	②基準の対象範囲	ISO/IEC 27001 の 2022 年度版でサイバーセキュリティを網羅するように改変され、来年から施行されるので、NIST CSF の考え方ではなく ISO/IEC 27001 をベースに組み立てた方がわかりやすいのではないか。NIST CSF を勉強することは必要だが、中小企業に理解していただくのは非常に難しい。	ISO/IEC 27001 を参考にしつつ、マネジメントシステムは要求せず、本認証制度のターゲットを明確にした上で、中小企業が対応可能な基準として見直しを行う。
2-8	②基準の対象範囲	元々、ISO/IEC 27001 がある中で本認証制度を作ることになった。ISO/IEC 27001 に寄せていくのであれば、ISMS 認証を取ればよいという話になる。何のために本認証制度を作ったのか。世の中の変化に伴い認証制度も変化しなければならないが、寄せるというのは元々の趣旨と異なるのではないか。	
2-9	②基準の対象範囲	ISO/IEC 27001 と本認証制度は異なり、マネジメントがない。これは大きな違いで、中小企業にとっては ISMS 認証より取得しやすいはずである。NIST の要素を入れると高度になり、IT のみが対象となるので避けてほしい。	
2-10	②基準の対象範囲	基準にこだわる必要はなく、ISMS 認証もサイバーセキュリティは弱い。国際規格でも ISO/IEC 27100 シリーズというサイバーセキュリティを対象とした別の規格も作っているので、どれが万能ということはない。参考となるものはどれを使っても構わないと考える。	
2-11	②基準の対象範囲	この制度はそもそも ISMS 認証が取れない事業者を対象としたものであり、中小企業の競争力強化などが目的だったはずなので、そこはぶれないようにすべきである。関連するものを幅広く見ればよいのではないか。	
2-12	②基準の対象範囲	どの層をターゲットにしてこの仕組みを作るかを考え、他の規格を参考にしつつ検討するのがよいと思う。ISO/IEC 27001 は確かに網羅的ではあるが、PDCA を中小企業に要求するのは難しい。教育やハード面に重点を置いた仕組みになると思う。どの層をターゲットにするかをもう一度議論した方がよい。	
2-13	②基準の対象範囲	個人情報保護法等、最近の法改正を反映すべき。	基準の改定に当たって、その時点の法令と整合したものとする。
2-14	②基準の対象範囲	ヒューマンエラー対策をどこまで盛り込むか。	ヒューマンエラー対策については、現行基準でも一定の配慮がなされているが、検討のうえ必要な修正を加える。
2-15	②基準の対象範囲	知識不足対策をどこまで盛り込むか。	知識不足対策については、現行基準でも一定の配慮がなされているが、検討のうえ必要な修正を加える。

2-16	②基準の対象範囲	ルール実施不徹底対策をどこまで盛り込むか。	ルール実施不徹底対策については、現行基準でも一定の配慮がなされているが、検討のうえ必要な修正を加える。
2-17	②基準の対象範囲	システム設計不備対策をどこまで盛り込むか。	システム設計不備により事故が発生した場合の対策については、検討のうえ、必要な対策を加える。 システム設計不備を起こさないための対策については、現行基準でも一定の配慮がなされているが、検討のうえ必要な修正を加える。
2-18	②基準の対象範囲	社内の情報セキュリティ人材育成を盛り込むか。	社内の情報セキュリティ人材育成については、現行基準でも一定の配慮がなされているが、検討のうえ必要な修正を加える。
2-19	②基準の対象範囲	物理的な防護措置の項目を削除したとしても、防衛産業に対して影響はない。	防衛調達基準を参考とした、物理的な防護措置に関する具体的な基準については削除する。
2-20	②基準の対象範囲	可用性・完全性についても考慮していくことでよいのではないか。ユーザ要求にどの程度影響があるかで、機密性もあれば、完全性や可用性もある。	情報の機密性だけではなく、完全性、可用性について考慮する。
2-21	②基準の対象範囲	告示名は漏えい防止かもしれないが、漏えいだけではないので、完全性・可用性を考慮することで良いのではないか。	

（3）業種について

業種については、以下の方針で進めることが望ましいと考えられる。

【基準】

- どの業種でも通用する内容・表現とする。
- 業種毎のニーズに対応可能となるよう、具体的な実施方法は事業者が選択できるようにする。
- 幅広い業種に対応できるよう配慮しつつ、対策の選択肢を提示する。

【その他】

- 業界に属する事業者が有する情報を念頭にユースケースを設定し、基準の運用ができるようなガイドの作成について検討する。

業種に関して、いただいたご意見と対応案を以下に示す。

表 2-4 業種に関するご意見と対応案

No.	カテゴリ	ご意見	対応案
3-1	③業種	具体的な対象に向けたガイドとして、例えば製造業であれば CAD/CAM とサンプル等、典型的に業界に属する事業者が有する情報を念頭に基準の運用ができるようなガイドがあるとわかりやすいのではないか。	制度としては、主に製造業を対象としつつ業種を限定したものではないが、基準の改定に当たって、様々な業種の方にとって具体的に求められる対策が分かりやすくなるよう、表現に配慮する。
3-2	③業種	IT とプライバシーマークが包括するような対策を必要な項目としてチェックリストに追加している。業界毎のチェックリストを作らざるを得ない状況について課題と感じている。対策レベルを	

		高度にすると対象範囲が広がり、他の認証制度との差別化が難しくなる。	
3-3	③業種	基準を分野別などに拡張できるような形にしておくことも一案である。	具体的な実施方法は事業者が選択できる運用を維持するが、基準改正に当たっては幅広い業種に対応できるよう、配慮しつつ対策の選択肢を提示する。
3-4	③業種	基準を用いたユースケースを設定して、こういう業種だとこういうやり方が良いという実装の方法を解説する方が現実的ではないか。この基準を使った守り方のガイドを作成した方がよいのではないか。	認証機関による指導・助言の活用を促すとともに、必要に応じて典型的なユースケースを紹介することも引き続き検討する。

（4）環境変化への対応について

環境変化への対応については、以下の方針で進めることが望ましいと考えられる。

- テレワークの普及などの昨今の環境変化に対応し基準の改廃を行う。
- 基準の見直しについては、ISO/IEC や NIST 等の参照基準の変更を基に行う。

環境変化への対応に関して、いただいたご意見と対応案を以下に示す。

表 2-5 環境変化への対応に関するご意見と対応案

No.	カテゴリ	ご意見	対応案
4-1	④環境変化への対応	環境変化は製造業でも様々あると思うので、働き方改革などを背景とした変化を含めていくことは賛成である。	見直しに当たって、環境変化を考慮する。
4-2	④環境変化への対応	テレワーク対応を盛り込むべき。	
4-3	④環境変化への対応	セキュリティは時々刻々変わっていくので、基準の見直しは定期的に継続する必要がある。	今後も必要に応じた見直しを継続していく。
4-4	④環境変化への対応	環境変化への対応については、仮に基準を改訂するとなると、技術的な根拠を示すのが非常に難しい。明らかに修正が必要な点を、認証取得事業者などが共通して意見するようなきっかけがないと、何をどのように、どういう理由で変えるのか、明確にしないと混乱を招く可能性がある。参照基準である ISO/IEC や NIST の基準の変更に合わせて適宜改訂し、特に社会的に大きな問題が生じた場合に、その問題に対して手直ししていくことが現実的ではないか。	基準の見直しについては、参照基準の変更を基に行う。

（5）その他・共通事項への対応について

その他・共通事項への対応については、以下の方針で進めることが望ましいと考えられる。

- 基準の名称については、わかりやすい単語を用いて、内容がイメージしやすいものを検討する。

その他・共通事項への対応に関して、いただいたご意見と対応案を以下に示す。

表 2-6 その他・共通事項への対応に関するご意見と対応案

No.	カテゴリ	ご意見	対応案
5-1	⑤その他・共通	制度の内容が容易にイメージできるような名称を検討すべき。	基準の名称については、わかりやすい単語を用いて、内容がイメージしやすいものを検討する。
5-2	⑤その他・共通	情報セキュリティというのはよい言葉。本認証制度は「サイバーセキュリティ」にとどまらない範囲だと考える。わかりやすい言葉とすることで、皆が参照する形になっていく可能性はある。	
5-3	⑤その他・共通	制度設計は国がやってもよいが、別途認定機関を設けてセミナーやプロモーション、営業マーケティングも含めて ISMS-AC、JIPDEC にやってもらうのがよいのではないか。	普及の観点を含め、認定機関を設置する認証スキームについても検討する。
5-4	⑤その他・共通	管理責任者について、どのレベルの方が責任を持つかは、組織によって考え方が異なる。権限は委譲して良いが、最終責任は大元の責任者である。責任と権限を定め、運用がきちんとされているかを確認することになる。責任が曖昧になっていれば、運用上の指摘事項となる。管理者にはそれぞれの部下がいるので、厳密にする必要はないと考える。	管理責任者にどのような役職・立場の職員を選任するかは、組織の状況を踏まえて柔軟に判断できるような構成を維持する。
5-5	⑤その他・共通	「〇〇するための手順を確立する」という表現が多いが、行為そのものを基準とした方がよいのではないか。(「〇〇するための手順を確立する。」→「〇〇する。」 手順の確立は手段であり、〇〇することが管理策の目的である。)	適切な表現に統一する。
5-6	⑤その他・共通	「講じられることを確保する。」→「講じる。」とすべきではないか。	適切な表現に統一する。

2.2.2 基準告示の修正方針

前述の意見と対応方針の踏まえ、基準告示の修正方針は以下とする。

- 告示においては達成目標(技術情報管理のために必要な要件)を必須として記載する。
  - 対策例は基本的に 1 項目を 1 要件として記載する。(複数要件が 1 項目にまとめられている場合は分割する)
  - 達成するための手段としての対策例は選択式として告示の中に示す。
  - 事業者の状況や管理対象情報の態様等による場合分けも対策例として示す。
  - 現行の指針告示において示している「必要最低限の措置の部分」は削除し、必須とされている措置は基準の中で明確に記載する。
  - 技術情報管理のために、組織におけるマネジメントシステムの確立を厳密に要求することはせず、「取組が習慣化し、文書等に定めがなくてもその事業者の従業員等において行動が実践されている状態を確立する。」ことを要求する。
  - レベル別に求める水準については、その表現のあり方も含めて別途検討する。
- 用語は極力統一し、その項だけの定義を作らない。

- 必須として記載した達成目標でも、事業者の状況において当てはまらない項目については、理由を確認したうえで、達成しないことを認める運用とする。
- 情報の可用性、完全性の確保も、管理対象情報の特定に当たって考慮する運用とする。
- 必要な対策例は重複していてもそれぞれ記載する。
- 取組例の中で、具体的な数値要件を設けているものは、果たすべき機能に着目し、機能要件に書き換える。
- 自工会/部工会・サイバーセキュリティガイドラインについてはレベル 1 の要求事項を参照し、導入する。
- ISO/IEC 27001 については、検知・対応に関する管理策を参照し、導入する。

なお、定義を整理する用語及びその定義の案を以下に示す。

表 2-7 定義を整理する用語

用語	定義
技術等情報	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。
管理対象情報	告示に掲げる管理対象情報の漏えい防止に資する措置のうち必要と判断されるものの対象とする技術等情報。
情報システム	ハードウェア、ソフトウェア、ネットワーク又は電子記録媒体で構成されるものであって、業務処理を行うものをいい、パーソナルコンピュータ、スマートデバイス等を含む。
管理情報システム	管理対象情報を取り扱う情報システム。
管理責任者	管理対象情報の管理に関する責任を有する者。なお、管理責任者はその業務の一部の実施を他の者に委任することができる。
管理者	管理責任者又は管理責任者からその業務の一部の実施を委任された者。
情報システム管理者	管理者等管理情報システムの維持に責任を有する者であって、情報システムの管理を当該事業者以外の者に委託等をしている場合には、当該者を含む。
従業員等	事業者との間で雇用関係等のある者。
アクセス権者	Ⅱによりアクセス権を設定された者（認証取得事業者に所属する者に限る。）
可搬式記録媒体	USB記録媒体、光ディスク、外付けハードディスク等パーソナルコンピュータ等に挿入し、又は接続することでパーソナルコンピュータ等に記録されている情報を記録することが可能な電子記録媒体をいい、パーソナルコンピュータ、スマートデバイス等の持ち出しが可能な情報システムを構成する機器を含む。
紙情報	紙情報：管理対象情報が記載された紙。
電子情報	管理対象情報が電子的方式、磁気的方式その他人の知覚によっては認識することができない方式で作られた記録。

2.2.3 基準告示の修正案

基準告示の修正方針をもとに、現行の基準の一部を修正した案を以下に示す。

表 2-8 基準告示の項目別修正案（管理対象情報の特定）

項目番号		項目名	内容（案）	備考
Ⅰ	第一	適切な管理をする必要がある技術等情報の特定	事業者は、~~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（以下「技術等情報」という。）について、~~その技術等情報の~~価値~~重要度等に応じて選別し、~~第二以下に掲げる措置のうち必要と判断されるものの対象とする技術等情報（以下~~「管理対象情報」~~という。）~~を特定する。 その際、以下に掲げる措置その他この目標を達成するために有効な措置から必要な措置を選択して実施する。	必須目標 自工会/部工会・サイバーセキュリティガイドライン（No.54：レベル1）に対応 ISO/IEC 27002 5-1 に対応
	1		技術等情報のうち管理対象情報の特定に当たっては、事業者の経営層も関与した上で、以下の事項を考慮する。 *一 その技術等情報が漏えいした場合に、自らの競争力に重大な影響を与えるか否か。* *二 その技術等情報が改ざんされた場合に、自らの競争力に重大な影響を与えるか否か。* *三 その技術等情報が使えなくなった場合に、自らの競争力に重大な影響を与えるか否か。* *四 他者から契約等に基づき預けられた情報であること等により、その技術等情報が漏えいした場合に自らの信用、他者との信頼関係等に対して重大な影響を与えるか否か。*	ISO/IEC 27002 5-1 に対応
			~~情報資産において「機密性」「完全性」「可用性」の 3 要素が確保できなくなった場合のリスクを特定できている~~ ~~【規則】~~ ~~・対象の情報資産に情報セキュリティ事件・事故が発生した時の業務影響を影響範囲や発生頻度を踏まえ把握すること~~ ~~【対象】~~ ~~№ 26 で特定した情報資産~~ ~~【観点】~~ ~~外部の脅威~~ ~~自社の脆弱性~~ ~~※必要に応じて、パートナー企業起因の脅威、脆弱性を考慮すること~~ ~~情報資産の価値~~ ~~【方法】~~ ~~対象の情報、情報システムを定めること~~ ~~各観点の評価規則、およびそれらを考慮したリスクレベルの規則を定めること~~ ~~各情報、情報システムについて、各観点の評価からリスクレベルを決定すること~~ ~~【頻度】~~ ~~重要な情報 資産を見直した時、または、1回／年 以上~~	自工会/部工会・サイバーセキュリティガイドラインから追加 （No.66：レベル 1） ⇒上に追記
			~~事業者は、管理対象情報を特定した場合には、当該管理対象情報の態様が、紙情報（管理対象情報が記載された紙をいう。以下同じ。）、電子情報（管理対象情報が電子的方式、磁気的方式その他人の知~~	~~「識別」するを必須とし、「目録の作成」「目録の保管」を~~

			~~覚によっては認識することができない方式で作られた記録をいう。以下同じ。）又は試作品、製造装置等の物自体のいずれに当たるか識別し、必要に応じて保管場所等を記録した目録を作成し、合理的な期間保管する。~~	~~分割し選択とする。~~ ~~自工会/部工会-サイバーセキュリティガイドライン(No.56:レベル1)に対応~~

表 2-9 基準告示の項目別修正案(管理対象情報の分類)

項目番号		項目名	内容(案)	備考
Ⅰ	第二	適切な管理をする必要がある技術等の分類	事業者は、~~管理対象情報を~~特定した~~場合には、~~当該管理対象情報の態様が、紙情報~~(管理対象情報が記載された紙をいう。以下同じ。)~~、電子情報~~(管理対象情報が電子的方式、磁気的方式その他人の知覚によっては認識することができない方式で作られた記録をいう。以下同じ。)~~又は試作品、製造装置等の物自体のいずれに当たるか識別分類する。 その際、以下に掲げる措置その他この目標を達成するために有効な措置から必要な措置を選択して実施する。 ~~し、必要に応じて保管場所を記録した目録を作成し、合理的な期間保管する。~~	必須目標 「分類する」を必須とし、「目録の作成」「目録の保管」を分割し「管理対象情報の識別」の項に回す。 自工会/部工会・サイバーセキュリティガイドライン(No.56:レベル1)に対応 ISO/IEC27002 5-9 に対応
	1		事業者は、管理対象情報をその価値等に応じて段階を設けて管理し、当該段階に応じてこの告示のⅠの第三の管理者を選任(複数の段階の管理対象情報に係る管理責任者を一の者とすることを含む。)し、価値の高いものであればよりアクセス権者を限定し、物理的措置を複数組み合わせて強化する等の措置を講ずる。	現行基準Ⅶから移動 ISO/IEC 27002 5-12 に対応
	2		事業者は、管理対象情報をその価値等に応じて段階を設けて管理する場合であって、この告示のⅠの第四の１の⑴の管理簿を作成するときには、その段階に応じて、管理簿を分けて作成する。	現行基準Ⅶから移動
	3		事業者は、管理対象情報をその価値等に応じて段階を設けて管理する場合であって~~、~~当該管理対象情報が電子情報であるとき~~の~~は、その段階に応じて、管理情報システムが提供する機能について、アクセス権者に対し、提供する機能を制限する。	現行基準Ⅶから移動 ISO/IEC 27002 8-2 に対応
	4		事業者は、管理対象情報のうち特に価値の高いもの等を管理するために立入制限区域の内部で間仕切りする場合には、入退室口及び警報装置を間仕切りした区画ごとに独立して設置する。	現行基準Ⅶから移動 ISO/IEC 27002 7-8 に対応
	5		管理責任者は、他者から預けられた管理対象情報等他の技術等情報と明確に区別することが必要なものについて、当該管理対象情報の識別が容易になるよう体系的に管理する~~ための手順を確立する~~。	現行基準「管理対象情報の管理簿の作成等」から移動

表 2-10 基準告示の項目別修正案(管理対象情報の識別)

項目番号		項目名	内容(案)	備考
Ⅰ	第三	適切な管理をする必要がある技術等情報の識別	事業者は、管理対象情報であることを明らかにするために、表示等の方法により他の技術等情報と区別して識別できるよう必要な措置を講ずる~~ものとする~~。 その際、以下に掲げる措置その他この目標を達成するために有効な措置から必要な措置を選択して実施する。 ~~表示により識別できるようにする方法としては、例えば、紙情報の場合であればその情報が記載された紙に管理対象情報であること(社外秘等の表示)を記載し、電子情報の場合であればファイル名に管理対象情報であることを記録し、試作品、製造装置等の物の場合であれば当該物そのもの又はその保管容器に表示することが考えられ、その他の方法としては、例えば、第一の3の目録による管理や電子情報にアクセス可能な者を限定したフォルダにより管理する方法等が考えられる。~~	必須目標 自工会/部工会・サイバーセキュリティガイドライン(No.54:レベル1)に対応 ISO/IEC 27002 5-13に対応
	1		事業者は、~~管理対象情報を~~特定した~~場合には、~~当該管理対象情報の態様~~が、紙情報(管理対象情報が記載された紙をいう。以下同じ。)、電子情報(管理対象情報が電子的方式、磁気的方式その他人の知覚によっては認識することができない方式で作られた記録をいう。以下同じ。)又は試作品、製造装置等の物自体のいずれに当たるか識別し、必要に応じて、対象情報、管理責任者名、部署名、保管場所、保管期限、開示先、連絡先等を記録した目録を作成し、合理的な期間保管する。	自工会/部工会・サイバーセキュリティガイドライン(No.56:レベル1)に対応
	2		~~表示により識別できるようにする方法としては、例えば、~~管理対象情報が紙情報の場合~~であれば、~~その情報が記載された紙に管理対象情報であること(社外秘等の表示)を記載する。~~し、~~	必須項目から具体的な対策例を分離
	3		管理対象情報が電子情報の場合~~であれば、~~ファイル名に管理対象情報であることを記録する。~~し、~~	必須項目から具体的な対策例を分離
	4		管理対象情報が試作品、製造装置等の物の場合~~であれば、~~当該物そのもの又はその保管容器に表示する。~~ことが考えられ、その他の方法としては、例えば、第一の3の目録による管理や~~	必須項目から具体的な対策例を分離
	5		~~電子情報に~~アクセス可能な者を限定した書庫、フォルダ等により管理する~~方法等が考えられる~~。	必須項目から具体的な対策例を分離
	6		~~管理者は、~~作成~~又は取得~~した技術等情報が管理対象情報である場合について、その識別をするための手順を確立する。~~~~	自工会/部工会・サイバーセキュリティガイドライン(No.54:レベル1)に対応 ISO/IEC 27002 5-12に対応
	7		管理責任者は、(1)の手順に従って措置が講じられていることを実地に確認すること等その措置が速やかに講じられることを確保する~~ために必要な取組を行う~~。	
	8		管理責任者は、他者から預けられた管理対象情報が他の技術等情報と組み合わされている場合等において、当該他者から、当該管理対象情報が識別可能となるようにすることを求められたときは、当該他者の求めに応じ、下線を引く、枠囲いをする等管理対象情報が分かるよう適切な措置を講ずる。	

表 2-11 基準告示の項目別修正案(管理対象情報の管理方針の策定)

項目番号		項目名	内容(案)	備考
Ⅰ	第四	適切な管理をする必要がある技術等情報の管理方針の策定	事業者は、管理対象情報について、その~~価値、~~重要度及び態様等に応じて、この告示に掲げる管理対象情報の漏えい防止に資する措置のうち必要なものを決定する。	必須目標 自工会/部工会・サイバーセキュリティガイドライン (No.62:レベル 1)に対応
			~~情報資産機器は重要度に応じた管理ルールに沿って管理している~~ ~~【規則】~~ ~~・No59 に定義した管理ルールに沿って管理を実施すること。不備・違反があれば是正を行うこと~~ ~~【頻度】~~ ~~1 回/年 以上~~	自工会/部工会・サイバーセキュリティガイドラインから追加 (No.62:レベル 1) ⇒上に統合のうえ削除
	1		事業者は、管理対象情報の漏えい防止に資する措置のうち~~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		~~必要に応じて経営層へ業務影響及び策定した~~対策を経営層に報告し、~~セキュリティ業務~~管理対象情報に関与~~しそいす~~る社内部署と共有~~しそいる~~する。 ~~【規則】~~ ~~・№ 66 で把握した業務影響に対する対策方法及び計画を策定し、報告・共有すること~~ ~~・報告に際し役員からの指示があった場合、これを関係部門へ共有すること~~ ~~【対象】~~ ~~情報セキュリティの総括責任者、関係部門~~ ~~【頻度】~~ ~~1 回以上/年~~	自工会/部工会・サイバーセキュリティガイドラインから追加 (No.68:レベル 1)
	3		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。	
	4		事業者は、~~当該管理対象情報が~~他者から預けられた管理対象情報が~~ものの~~である場合は、当該他者からの意見を聞いてこの告示に掲げる措置その他有効な措置のうち必要なものを決定する。~~し、当該他者からの求めがあったときは、その状況を記録し、合理的な期間保管し、報告する。~~	
	5		事業者は、管理対象情報が他者から預けられた情報である場合であって、当該管理対象情報についてのマニュアルを当該他者からの求めに応じて作成するときは、当該他者に当該マニュアルの内容についての確認をとる。これを変更するときも、確認をとる。	
	6		事業者~~の取締役等の経営層~~は、~~第二の2により~~必要と決定した管理対象情報の漏えい防止に資する措置の実施の状況を管理~~責任~~者に記録をさせ、当該記録の保管期間を定め、定期的に確認する。	

表 2-12 基準告示の項目別修正案(管理責任者の選任)

項目番号		項目名	内容(案)	備考
Ⅰ	第五	管理責任者の選任	事業者の取締役等の経営層は、管理対象情報~~に~~の管理に関する~~し、以下に掲げる事項についての~~責任を有する者(以下「管理責任者」という。)を選任する。 その際、以下に掲げる事項その他管理に有効な事項から必要な事項を選択し、それぞれについて責任を持つ者を明らかにする。 ~~なお、~~管理責任者はその業務の一部の実施を他の者に委任することができる~~を妨げない~~。	必須目標 自工会/部工会・サイバーセキュリティガイドライン(No.13:レベル 1)に対応 ISO/IEC 27002 5-9に対応
	1		管理対象情報について、第~~四三の2~~により必要と決定した措置に係る必要な手順を確立させること。	ISO/IEC 27002 5-2に対応
	2		管理対象情報を取り扱う者の制限及び管理を行い、当該管理対象情報を取り扱う者に対するトレーニングを行うこと。	ISO/IEC 27002 6-3に対応
	3		保管容器又は立入制限区域の鍵の管理又は暗証番号の設定等の管理対象情報の漏えいの防止のために必要な措置を講じ、その状況を把握すること。	ISO/IEC 27002 7-3に対応
	4		管理対象情報の漏えいの兆候や漏えいの事実の把握に努め、その事象があった場合に必要な対応等の措置を講ずること。	ISO/IEC 27002 5-8に対応
	5		2から4~~三から四~~までに掲げる事項について、記録を取得し、合理的な期間保管すること。	ISO/IEC 27002 5-22に対応
	6		事業者は、当該事業者の従業員等~~(事業者との間で雇用関係等のある者をいう。以下同じ。)~~が多い場合、その管理対象情報が複数の事業部門にまたがるものである場合等には、社内規程に定めることや社内における掲示をすること等により、誰が管理責任者であり、何の~~(1)の各~~事項の責任を~~誰が~~有しているかを当該事業者の従業員等の全ての者が認識できるように措置を講ずる。	ISO/IEC 27002 5-3に対応
	7		~~1にかかわらず、~~事業者の従業員等が少人数の場合等には、当該事業者の取締役等の経営層の判断により、経営層の者が管理責任者を兼務することができる。 事業者の従業員等が少人数の場合等とは、例えば、取締役等の経営層が全ての従業員等を認識することが可能な程度の人数であり、当該取締役等の経営層が管理対象情報の取扱い状況をほぼ把握できるとともに、従業員等から当該取締役等の経営層に対して、管理対象情報に係る報告等が直接される取組が習慣化し、文書等に定めがなくてもその事業者の従業員等において行動が実践されている状態が確立している場合等が考えられる。	ISO/IEC 27002 5-3に対応

表 2-13 基準告示の項目別修正案(管理対象情報の管理簿の作成、保管)

項目番号		項目名	内容(案)	備考
Ⅰ	第六	管理対象情報の管理簿の作成等及び保管	管理責任者は、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し、保管する。 その際、以下に掲げる措置その他この目標を達成するために有効な措置から必要な措置を選択して実施する。	必須目標 自工会/部工会・サイバーセキュリティガイドライン(No.58:レベル 1)に対応
	1		管理責任者は、~~(1) 又は(2) の~~管理簿について、保管期間を定めた上、施錠したロッカー等において保管し、又は暗号技術を用いて情報システム~~サーバ又はパーソナルコンピュータ(以下「サーバ等」という。)~~に記録する等適切に管理(当該ロッカー等の鍵の管理を含む。)する。	
			~~管理者は、(2) の管理簿について(3)の保管期間を定める場合は、当該管理簿に係る管理対象情報を預けた他者の確認をとる。~~	下に統合
	2		管理責任者は、新たに作成または取得した管理対象情報が管理簿が適切に記録されていることを定期的に点検し、必要に応じて是正する。	新規追加 自工会/部工会・サイバーセキュリティガイドライン(No.58:レベル 1)に対応
	3		管理責任者は、~~(1) 又は(2) の~~管理簿が適切に管理されていることを定期的に点検し、必要に応じて是正する。	自工会/部工会・サイバーセキュリティガイドライン(No.58:レベル 1)に対応
	4		管理責任者は、~~(1)の~~管理簿について廃棄をしようとする場合は事業者の取締役等の経営層に、~~(2)の管理簿について廃棄をしようとする場合は当該管理簿に係る管理対象情報を預けた他者に、それぞれ~~確認をとる。	他者から預けられた情報については下に統合
	5		管理責任者は、~~(1) の管理簿について、~~他者から預けられた管理対象情報についてのみの状況を管理するため、自ら及び他の他者から預けられた~~の~~ものと別にして管理簿を作成し、当該他者に共有する。また、管理簿の保存期間を定める場合及び廃棄をする場合も当該他者の確認を取る。	自工会/部工会・サイバーセキュリティガイドライン(No.70:レベル 1)に対応

表 2-14 基準告示の項目別修正案(管理対象情報の内容の伝達の制限)

項目番号		項目名	内容(案)	備考
Ⅰ	第七	管理対象情報の内容の伝達の制限	管理責任者は、~~原則として、この告示のⅡによりアクセス権を設定された者(以下「アクセス権者」という。)に限り、~~管理対象情報の内容の伝達(管理対象情報である紙情報や電子情報に記録された事項を~~当該紙情報や当該電子情報を用いずに口頭等により~~伝えること及び閲覧させることをいう。)の対象をアクセス権者に限る~~がされるようにする~~ための手順を確立する。 その際、以下に掲げる措置その他この目標を達成するために有効な措置から必要な措置を選択して実施する。	必須目標 ISO/IEC 27002 5-10 に対応
	1		管理責任者は、アクセス権者が~~そのアクセス権者の属する事業者の~~他の従業員等(管理対象情報の他のアクセス権者を除く。~~以下この第四において「他の従業員等」という。~~)に対して管理対象情報の内容の伝達をしようとする場合には、当該アクセス権者から、管理責任者に対して承認を得るための手順を確立する。	ISO/IEC 27002 5-15 に対応
	2		管理責任者は、アクセス権者から他の従業員等に対する管理対象情報の内容の伝達についての承認を求められた場合には、当該伝達が真に必要なものか否かの確認を行い、伝達の範囲を可能な限り限定した上で、これを認める。	ISO/IEC 27002 5-15 に対応
	3		管理責任者は、管理対象情報の内容の伝達について、第六~~1の(1)又は(2)~~ の管理簿に記録する。	ISO/IEC 27002 5-15 に対応

表 2-15 基準告示の項目別修正案(管理対象情報の複製の制限)

項目番号		項目名	内容(案)	備考
Ⅰ	第八	管理対象情報の複製の制限	管理責任者は、管理対象情報の複製をアクセス権者のみが行うことができるようにするための手順を確立する。 その際、以下に掲げる措置その他この目標を達成するために有効な措置から必要な措置を選択して実施する。	必須目標
	1		管理責任者は、アクセス権者が、管理対象情報の複製をしようとする場合には、当該アクセス権者が~~から、~~管理責任者~~に対して~~から当該複製の承認を得るための手順を確立する。	
	2		管理責任者は、アクセス権者から管理対象情報の複製についての承認を求められた場合には、当該複製が真に必要なものか否かの確認を行い、複製の範囲を可能な限り限定した上で、これを認める。	
	3		管理責任者~~事業者~~は、電子情報である管理対象情報について、情報システム(ハードウェア、ソフトウェア(プログラムの集合体をいう。以下同じ。)、ネットワーク又は電子記録媒体で構成されるものであって、これら全体で業務処理を行うものをいう。)を構成する機器、~~及び~~可搬式記録媒体~~(USB記録媒体、光ディスク、外付けハードディスク等パーソナルコンピュータ等に挿入し、又は接続することでパーソナルコンピュータ等に記録されている情報を記録することが可能な電子記録媒体をいう。以下同じ。)~~又はネットワークを介して接続するストレージサービスであって、~~個人が管理する事業者の~~管理に属さないものへの複製をするための手順を確立する。	
	4		管理責任者~~事業者~~は、管理対象情報を複製した場合において、当該複製された情報を管理対象情報として適切に管理するための手順を確立する。	

表 2-16 基準告示の項目別修正案(管理対象情報の廃棄等の制限)

項目番号		項目名	内容(案)	備考
Ⅰ	第九	管理対象情報の廃棄等の制限	事業者は、管理対象情報の廃棄については、~~当該廃棄に係る管理対象情報を探知することができないよう、紙情報の場合におけるシュレッダーでの細断、電子情報の場合における完全消去や難読化等~~その管理対象情報の態様に応じ、~~焼却、粉砕、細断、溶解、破壊等の~~復元不可能な方法により廃棄をするための手順を確立する。 その際、以下に掲げる措置その他この目標を達成するために有効な措置から必要な措置を選択して実施する。	必須目標
	1		事業者は、紙情報又は試作品等である管理対象情報を~~シュレッダーにより細断を廃棄~~する場合には、~~以下に掲げるいずれかの性能を有する~~シュレッダーにより裁断する等、Ⅲで決定した情報を復元できない状態にするための措置を講ずる~~を用いる~~。	
			~~縦横細断方式のシュレッダーであって、一辺を3mm以内とし、細断された紙の面積が4.5平方mm以内に細断をすることができるもの~~	削除。必要に応じて、Ⅲ(管理対象情報が紙、試作品等の保管できるものの場合の対策)で記載
			~~縦横細断方式のシュレッダーであって、細断された紙の面積が10平方mm以内(一辺は1mm以内とするものに限る。)に細断をすることができるもの~~	削除。必要に応じて、Ⅲ(管理対象情報が紙、試作品等の保管できるものの場合の対策)で記載
			~~縦細断方式のシュレッダーであって、一辺を1mm以内に細断をすることができるもの~~	削除。必要に応じて、Ⅲ(管理対象情報が紙、試作品等の保管できるものの場合の対策)で記載
	2		事業者は、電子情報である管理対象情報を消去する場合には、上書き消去(データの完全消去)等、Ⅴで決定した情報を復元できない状態にするための措置を講ずる。	追加
	3		事業者は、電子情報である管理対象情報を記録した可搬式記録媒体を廃棄する場合には、当該可搬式記録媒体を物理的に破壊する等、Ⅴで決定した情報を復元できない状態にするための措置を講ずる。	追加

表 2-17 基準告示の項目別修正案(情報システム利用ルールの策定)

項目番号		項目名	内容(案)	備考
Ⅴ	第一	情報システム利用ルールの策定	事業者は、管理対象情報が電子情報である場合には、~~可搬式記録媒体(パーソナルコンピュータを含む。以下このⅤにおいて同じ。)の持ち出しを管理し、当該電子情報が事業者の内部のサーバ等で記録されている場合には、ID認証、パスワード等により~~当該電子情報へのアクセスをアクセス権者に制限する手順を定め、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。~~した上で、以下に掲げる事項のうちこの告示のⅠの第三の2により必要と決定した措置を実施して、管理対象情報へのアクセスの制限を実施する。~~ その際、以下に掲げる措置その他この目標を達成するために有効な措置から必要な措置を選択して実施する。	必須目標 ここではルールの策定のみを目的として明示する。 具体的な手段は別の項で規定。
			~~なお、当該電子情報がクラウド等当該事業者以外の者のサーバ等で記録されている場合には、そのクラウド等を管理する者の信頼性を確認(例えば、ISO/IEC27017 の認証の取得の状況、日本セキュリティ監査協会クラウドセキュリティ推進協議会によるCSマークの取得の状況等を確認)、又は当該事業者以外の者であるデータセンターに自らのサーバ等を設置している場合は、当該データセンターの信頼性を確認(例えば、日本データセンター協会のデータセンターファシリティスタンダードのティア1からティア4を取得しているデータセンターのうち自らの管理対象情報の価値等に応じてデータセンターのサービスを適切に提供し得ること等を確認)、し 当該クラウド等を管理する者又はデータセンターとの間でⅥの秘密保持契約を締結した上で、以下に掲げる事項のうち事業者自らが措置を実施することが可能なものについて、この告示のⅠの第三の2により必要と決定した措置を実施し、管理対象情報の適切な管理をする。~~	情報システムの構成の項に移動
	1		管理対象情報が可搬式記録媒体に記録されている場合には、当該可搬式記録媒体~~(パーソナルコンピュータを含む。以下このⅤにおいて同じ。)~~の持ち出しをⅢで規定する管理対象情報と同等の手段で管理する手順を確立する。~~し、~~	
	2		当該電子情報が事業者の内部のサーバ等で記録されている場合には、ID認証、パスワード等により当該電子情報へのアクセスをアクセス権者に制限する手順を確立する。	
	3		事業者(自らの情報システム(以下単に「情報システム」という。)の維持に責任を有する者を含む。以下 4 から 5 までにおいて同じ。)は、情報システムのセキュリティに配慮したログオン手順、電子メールで管理対象情報を送付する場合の手順等を含む操作手順書を作成する。~~し、常に利用者が利用可能な状態にする。~~	「利用可能な状態にする」は「情報システムの構成」に移動
	4		事業者は、業務で利用する情報システムを構成する機器(個人所有の物を含む)の利用開始時、利用終了時の手続き、利用中の遵守・禁止事項、紛失時の手続きを含む利用手順を確立する。~~ルールを規定し、周知している(個人所有機器含む)~~ ~~【規則】~~ ~~・情報機器(PC、サーバー、通信機器、記憶媒体、スマートデバイス等)の利用ルールを策定し、このルールには利用開始時、利用終了時の手続き、利用中の遵守・禁止事項、紛失時の手続きを含むこと~~ ~~・情報機器の利用ルールを容易に確認できる状態にすること~~ ~~【対象】~~ ~~・役員、従業員、社外要員(派遣社員等)~~ ~~【頻度】~~ ~~・定常的に、かつ、ルールの改正時に周知すること~~	自工会/部工会・サイバーセキュリティガイドラインから追加 (No.8:レベル 1)

	5		マルウェアを始めとする不正アクセスに対する保護のため、~~は、~~利用者に必要なトレーニングを実施する。~~の適切な認識によって実施及び支援することが望ましい。~~	ISO/IEC 27002 8-7 から追記

表 2-18 基準告示の項目別修正案(情報システムを構成する機器の条件)

項目番号		項目名	内容(案)	備考
Ⅴ	第二	情報システムを構成する機器の条件	事業者は自社が構築する情報システムを構成する機器の選定に当たって、信頼性を考慮したうえで機器を選定する。 その際、以下に掲げる措置その他この目標を達成するために有効な措置から必要な措置を選択して実施する。	必須目標を追記
	1		事業者は、情報システムを構成するハードウェア、ソフトウェア等について、サポート窓口が明確であり、当該サポート窓口に常時連絡がとれる事業者から導入する。	
	2		事業者は、管理情報システムを構成する機器について、無線でのネットワークへの接続をすることができるものを用いない。	
	3		事業者は、立入制限区域の内部のみで利用する管理情報システムを、有線により配線接続して構築し、当該立入制限区域の外部への通信を行わせないための手順を確立する。	
	4		~~なお、当該電子~~管理対象情報~~を~~が~~クラウド等~~当該~~事業者以外の者のサーバ等で保存す~~記録されてい~~る場合には、そのクラウド等を管理する者の信頼性を確認(例えば、ISO/IEC27017 の認証の取得の状況、日本セキュリティ監査協会クラウドセキュリティ推進協議会によるCSマークの取得の状況等を確認) する。~~し、~~	
	5		管理対象情報~~を又は~~当該事業者以外の者であるデータセンターに自らのサーバ等を設置して保存している場合は、当該データセンターの信頼性を確認(例えば、日本データセンター協会のデータセンターファシリティスタンダードのティア1からティア4を取得しているデータセンターのうち自らの管理対象情報の価値等に応じてデータセンターのサービスを適切に提供し得ること等を確認) する。~~し、~~	
			~~当該クラウド等を管理する者又はデータセンターとの間でⅥの秘密保持契約を締結した上で、以下に掲げる事項のうち事業者自らが措置を実施することが可能なものについて、この告示のⅠの第三の2により必要と決定した措置を実施し、管理対象情報の適切な管理をする。~~	⇒「情報システムを管理する第三者の制限」に移動
	6		事業者は、この告示のⅣの立入制限区域に管理情報システムを構成する機器のうちサーバ等一定のものを設置する。	
	7		~~この場合において、~~管理責任者等管理情報システムの維持の責任を有する者は、~~当該一定のもの~~管理情報システムを構成する機器以外のサーバ等の持込みを禁止し、及びサーバ等を新設する場合の内蔵ソフトウェアの状況を確認した上で、当該サーバ等が従業員等の個人の所有にかからないものに限り認める~~ための手順を確立する。~~	

表 2-19 基準告示の項目別修正案(不正アクセスの防止)

項目番号		項目名	内容(案)	備考
V	第三	不正アクセスの防止	事業者は自社が構築する情報システムの構成するネットワーク、システム及びアプリケーションについて異常な行動・動作がないか監視し、不正アクセスを防止するために必要な措置を講ずる。 その際、以下に掲げる措置その他この目標を達成するために有効な措置から必要な措置を選択して実施する。	必須目標を追記
	1		事業者は、情報システムとインターネットの間にファイアウォールを導入する。	
	2		~~事業者は、情報システムへのアクセスログ等を取得する~~。	第七に移動
	3		事業者は、IDS(Intrusion Detection System)等により、情報システムへの不正なアクセスを検知して、情報システムの維持に責任を有する者に通知するシステムを導入する。	
	4		事業者は、IPS(Intrusion Prevention System)等により、情報システムへの不正なアクセスを検知し、防御するシステムを導入する。	
	5		事業者は、ネットワークに接続するサーバについて、不要なポートを閉鎖すること、匿名でのネットワークへの接続(Anonymous 接続)を禁止すること等を実施する。	
	6		事業者は、管理情報システムにおいてオペレーティングシステム及びソフトウェアによる制御を無効にすることができるシステムユーティリティの使用を制限するための手順を確立する。	
	7		事業者は、管理情報システムにソフトウェアを導入する場合、管理責任者等管理情報システムの維持に責任を有する者によりソフトウェアの安全性が確認された場合を除き、認めないための手順を確立する。	
	8		事業者は、管理情報システムの共有ネットワーク(インターネット等)への接続については、その接続に伴うリスクから保護するため、アクセス権者の職務内容に応じて設定するアクセス制御の方針(定期的又は管理対象情報の漏えいの事故等があった場合に見直すことができるものに限る。)を定め、これに基づいて認めるための手順を確立する。	
	9		事業者は、情報システムから外部への通信についてログの取得等により監視する。	
			~~情報セキュリティインシデントの可能性がある事象を評価するために、ネットワーク、システム及びアプリケーションについて異常な行動・動作がないか監視し、適切な処置を講じることが望ましい~~。	ISO/IEC 27002 8-16 から追記 必須目標に統合
	10		事業者は、管理情報システムを構成する機器について、不要なネットワークポート、 USBポート、シリアルポートを物理的に閉塞すること等当該機器に可搬式記録媒体を接続することによる管理対象情報の流出を防止する措置を実施するための手順を確立する。	

表 2-20 基準告示の項目別修正案(情報システムの継続性)

項目番号		項目名	内容(案)	備考
V	第四	情報システムの継続性	事業者は、その事業を継続させるために情報システムが継続的に利用できるよう、必要な措置を講ずる。 その際、以下に掲げる措置その他この目標を達成するために有効な措置から必要な措置を選択して実施する。	必須目標を追記
	1		事業者は、管理対象情報について、定期的な保存(バックアップ)を実施し、当該保存された情報を管理対象情報として適切に管理する。	
	2		情報システムを置く処理施設はを、~~,~~サポートユーティリティの不具合による~~,~~停電、~~,~~その他の故障から保護するための措置を講ずる~~ことが望ましい。~~	ISO/IEC 27002 7－11から追記
	3		事業者は、必要に応じて情報システムを復元する ~~リストア~~ 手順を整備する。~~している~~ ~~【規則】~~ ~~バックアップ対象ごとにリストア手順書を整備すること~~	自工会/部工会・サイバーセキュリティガイドラインから追加 (No.149:レベル 1)
	4		情報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する。~~している~~ ~~【規則】~~ ~~・システム利用不可能時を想定した、実施可能な代替手法を整備すること~~ ~~対象~~ ~~高い可用性が求められる 稼働停止許容時間が短い システム~~ ~~※対象はリスクに応じて各社判断~~ ~~対策例~~ ~~アナログツールの利用 (FAX など~~ ~~クラウドサービスなどの外部情報システムの利用~~	自工会/部工会・サイバーセキュリティガイドラインから追加 (No.150:レベル 1)
	5		事業継続の目的及び ~~ICT~~ 情報システム継続の要求事項に基づいて~~,ICT~~ 情報システムの備えを計画, 実施, 維持及び試験する~~ことが望ましい~~。	ISO/IEC 27002 5－30 から追記
	6		情報システムの運用に当たって、現在の及び予測される容量・能力の要求事項に合わせて、~~,~~資源の利用を監視し調整する~~ことが望ましい。~~	ISO/IEC 27002 8－6 から追記

表 2-21 基準告示の項目別修正案(情報システム管理者の制限)

項目番号		項目名	内容(案)	備考
V	第五	情報システム管理者の制限	事業者は、情報システム管理者管理者等管理情報~~システムの維持に責任を有する者~~の利用権限を必要最低限にとどめ、当該利用権限が最低限であることを定期的に監査するための手順を確立する。その際、以下に掲げる措置その他この目標を達成するために有効な措置から必要な措置を選択して実施する。	必須目標
	1		事業者は、情報システム管理者管理者等管理情報~~システムの維持に責任を有する者~~について、その者による当該管理情報システムの設定変更や運用に関する作業ログを取得する。	
	2		事業者は、1 の作業ログについて、情報システム管理者管理者等管理情報~~システムの維持に責任を有する者~~の上司等により、又はデータ解析ツール(データマイニングツール)を活用すること等により、定期的に点検させる。	
	3		事業者は、管理情報システムの監査に用いるツールについて、悪用を防止するため必要最低限の使用にとどめる。	
	4		事業者又はアクセス権者は、管理情報システムが無人状態に置かれる場合、使用していない管理情報システムを構成する機器の電源を切り、又は機器の表示画面の表示停止と再表示時にパスワードが必要なよう設定すること等により、無人状態であっても管理対象情報が適切に保護されるよう必要な対応をする。	

表 2-22 基準告示の項目別修正案(情報システムの更新)

項目番号		項目名	内容(案)	備考
V	第六	情報システムの更新	事業者~~(管理者等管理対象情報を取り扱う情報システム(以下このVにおいて「管理情報システム」という。)の維持に責任を有する者を含む。22 から 24 までを除き、以下このV及びⅧの第一の3において同じ。)~~ は、管理情報システムを最新の状態に更新~~されたウィルス対策ソフトウェア等を用いて、少なくとも週1回以上フルスキャンを行い、パッチの更新を行うこと等により、当該管理情報システムが提供する機能を妨害するウィルス、スパイウェア等から保護~~し、適切に機能を提供するための取組を実施する。 その際、以下に掲げる措置その他この目標を達成するために有効な措置から必要な措置を選択して実施する。	必須目標を追記
	1		情報システム管理者は、当該管理情報システムが提供する機能を妨害するウィルス、スパイウェア等から保護するため、管理情報システムを構成する機器について、更新されたウィルス対策ソフトウェア等を用いて、少なくとも週1回以上フルスキャンを行い、パッチの更新等を行う。	自工会/部工会・サイバーセキュリティガイドライン(No.124:レベル 1)に対応
	2		業者は、一定期間(例えば、1週間)電源の切られた状態にある管理情報システムを構成する機器については、再度の電源投入時に 1 の取組を実施する。	
	3		事業者は、管理対象情報を記録するための可搬式記録媒体について、2 又は 3 の取組を実施する。この場合において、2 中「電源の切られた」とあるのは「使用されていない」、「電源投入時」とあるのは「使用の前」とする。	
	4		事業者は、管理情報システムに対するペネトレーションテストを定期的に実施する。	
	5		事業者は、情報システムを構成するソフトウェアの利用状況を確認し、利用がされていない場合には、当該ソフトウェアを消去する。	
	6		事業者は、管理情報システム及びネットワークを通じて管理情報システムにアクセス可能な情報システムの日付及び時刻を定期的に合わせる。	
			~~情報システム・情報機器、ソフトウェアへセキュリティパッチやアップデート適用を適切に行っている~~ ~~【規則】~~ ~~・セキュリティパッチやアップデート適用を、規則と期限を定め実施すること~~ ~~・やむを得ず適用できない場合は、適用対象外の理由を記録すること~~ ~~【対象】~~ ~~・パソコン、スマホ、タブレット、サーバー、ネットワーク機器、ソフトウェア等~~ ~~・会社支給のクライアント PC の OS、ブラウザ、Office ソフト~~ ~~・サーバーの OS、ミドルウェア~~ ~~・会社支給のスマートデバイスの OS、アプリ~~ ~~・インターネットとの境界に設置されているネットワーク機器の OS、ファームウェア~~	自工会/部工会・サイバーセキュリティガイドラインから追加 (No.124:レベル 1) ⇒上で統合

表 2-23 基準告示の項目別修正案(アクセスログ等の保管)

項目番号		項目名	内容(案)	備考
V	第七	アクセスログ等の保管	事業者は、情報システムへのアクセスログ等を取得する。 その際、以下に掲げる措置その他この目標を達成するために有効な措置から必要な措置を選択して実施する。	必須目標
	1		事業者は、3のアクセスログをその記録のあった日から合理的な期間以上保存し、情報システム管理者~~情報システムの維持に責任を有する者(情報システムの管理を当該事業者以外の者に委託等をしている場合には、当該者を含む。以下この第一において同じ。)~~により定期的に点検させる。	
	2		事業者は、当該アクセスログを改ざん又は不正なアクセスから保護するために適切な措置を講ずる。	
	3		事業者は、管理情報システムの利用の状況、管理情報システムにおける管理対象情報へのアクセス(アクセス権者が利用した管理情報システムを構成する機器並びに当該機器へのログオン又はログオフの日時及びその成否並びに使用されたプログラムを含む。)及び例外処理を記録した監査ログを取得する。	
	4		事業者は、3 の監査ログを記録のあった日から三月以上保存し、定期的に点検し、当該監査ログを改ざん又は不正なアクセスから保護するために適切な措置を講ずる。	

表 2-24 基準告示の項目別修正案(電子情報である管理対象情報の消去)

項目番号		項目名	内容(案)	備考
V	第八	電子情報である管理対象情報の消去	事業者は、可搬式記録媒体に記録された管理対象情報を確実に消去するために必要な措置を講ずる。 その際、以下に掲げる措置その他この目標を達成するために有効な措置から必要な措置を選択して実施する。	必須目標
	1		事業者は、可搬式記録媒体に記録した管理対象情報を消去する場合には、復元できないように上書き消去(データの完全消去)を速やかに行うための手順を確立する。	
	2		事業者は、~~5の~~手順に従い管理対象情報が消去された可搬式記録媒体に限り、その使用を認める。	
			~~事業者は、管理対象情報が記録されたサーバや可搬式記録媒体の廃棄を行う場合には、ハードディスクドライブ等全体に対して上書き消去(データの完全消去)を行い、その消去を確認した上で、物理的な破壊を行うための手順を確立する。~~	持ち出しの制限の項に重複項目があるのでここでは削除
			~~事業者は、管理情報システムを構成する機器の廃棄を行う場合には、データを消去すること等により読み取りができない状態にするための手順を確立する。~~	持ち出しの制限の項に重複項目があるのでここでは削除

表 2-25 基準告示の項目別修正案(電子情報である管理対象情報の送信)

項目番号		項目名	内容(案)	備考
V	第九	電子情報である管理対象情報の送信	事業者は、管理対象情報を外部に送信することによる管理対象情報の流出を防止するために必要な措置を講ずる。 その際、以下に掲げる措置その他この目標を達成するために有効な措置から必要な措置を選択して実施する。	必須目標を追記
	1		事業者は、管理対象情報を電子メール等の電子情報をネットワークを経由して送信できる手段で外部に送信する場合は、送信する管理対象情報又は電子メールそのものについて暗号化すること等の適切な措置を講ずるための手順を確立する。	
	2		事業者は、管理対象情報を電子メール等の電子データをネットワークを経由して送信できる手段で外部に送信する場合~~又は受信する場合に~~、その~~送受信の~~ログを合理的な期間保存する。	

表 2-26 基準告示の項目別修正案(可搬式記録媒体への記録の制限)

項目番号		項目名	内容(案)	備考
V	第十	可搬式記録媒体への記録の制限	事業者は、管理対象情報を可搬式記録媒体に記録することによる管理対象情報の流出を防止するために必要な措置を講ずる。 その際、以下に掲げる措置その他この目標を達成するために有効な措置から必要な措置を選択して実施する。	必須目標を追記
	1		事業者は、電子情報である管理対象情報を可搬式記録媒体に記録する場合は、暗号技術を用いる。	
	2		事業者は、管理情報システムを構成する機器及び可搬式記録媒体であって、個人が所有するもので、管理対象情報を、取り扱わせないための手順を確立する。	

表 2-27 基準告示の項目別修正案(情報システムを構成する機器の持ち出しの制限)

項目番号		項目名	内容(案)	備考
V	第十一	情報システムを構成する機器の持ち出しの制限	事業者は、管理情報システムを構成する機器の持ち出しを制限する。 その際、以下に掲げる措置その他この目標を達成するために有効な措置から必要な措置を選択して実施する。	必須目標を追記
	1		情報システム~~管理の維持に責任を有する~~者は、情報システムを構成するハードウェア、ソフトウェア等の管理簿~~(保守(修理を含む。以下同じ。)及び点検の記録、持ち出した場合の持ち出しの記録、廃棄した場合の廃棄方法及びデータの消去の記録、セキュリティパッチの状況等そのハードウェア、ソフトウェア等が適切に機能を提供するための対応の記録を含む。)~~を作成し、合理的な期間保管する。	
	2		管理簿には、~~(~~保守(修理を含む。以下同じ。)及び点検の記録、持ち出した場合の持ち出しの記録、廃棄した場合の廃棄方法及びデータの消去の記録、セキュリティパッチの状況等そのハードウェア、ソフトウェア等が適切に機能を提供するための対応~~のを~~記録~~するを含む。)~~	
	3		事業者は、情報システム管理者~~管理者等管理情報システムの維持に責任を有する者~~が、当該管理情報システムを構成する機器の持ち出しに伴うリスクを回避することができると判断し、その承認をした場合を除き、当該機器を持ち出させないための手順(持ち出しをする場合の記録を含む。)を確立する。	
	4		事業者は、管理情報システムを構成する機器を再利用又は譲渡する場合は、管理対象情報が復元できない状態であることを点検した後で再利用する。	
	5		事業者は、管理情報システムを構成する機器を廃棄する場合には、当該機器に記録された管理対象情報が復元できない状態であることを確認し、当該機器を物理的に破壊し、廃棄する。	

表 2-28 基準告示の項目別修正案(情報システムを管理する第三者の制限)

項目番号		項目名	内容(案)	備考
V	第十二	情報システムを管理する第三者の制限	事業者は、管理情報システムの保守及び点検を第三者に行わせる場合、当該第三者が管理対象情報を漏えいさせないよう必要な措置を講ずる。 その際、以下に掲げる措置その他この目標を達成するために有効な措置から必要な措置を選択して実施する。	必須目標を追記
	1		事業者は、管理情報システムに係るサービス、システム、機器の保守及び点検をサプライヤーを含む外部の第三者に行わせる場合であって、当該第三者が管理対象情報に関わるときは、情報システム管理者~~管理者等管理情報システムの維持に責任を有する者~~の指示の下で、管理対象情報を他の記録媒体に移した上で、管理対象情報を復元できないように消去する等の措置を実施する。~~し、又は~~	
	2		事業者は、管理情報システムに係るサービス、システム、機器の保守及び点検をサプライヤーを含む外部の第三者に行わせる場合であって、当該第三者が管理対象情報に関わるときは、事業者の従業員等が~~保守及び点検業務に~~立ち会い、若しくは作業ログを取得し、若しくはカメラを設置すること等により、保守及び点検業務~~作業~~を監視することができる状況で行わせる~~手順を確立する。~~	
	3		事業者は、管理情報システムに係るサービス、システム、機器の第三者による情報システムの保守及び点検に当たって、当該第三者の作業者にIDを付与することが必要な場合には、一時的なIDを付与することとし、作業終了後は、その権限を無効化する~~ための手順を確立する。~~	
	4		事業者は、管理情報システムを構成する機器をこの告示のⅣの立入制限区域に設置する場合であって、当該管理情報システムを構成する機器の保守及び点検をサプライヤーを含む第三者に行わせるときは、~~Ⅵの~~秘密保持契約を締結した上で行わせる。	
	5		この場合において、~~情報システム管理者管理者等管理情報システムの維持に責任を有する者~~は、当該第三者の作業者についてこの告示のⅣの第二の6の手順を確立しているときは当該手順に従い、若しくは当該手順を確立していないときは作業者を確認し、当該作業者の立入りを認め、並びに当該立入制限区域内の保守及び点検の対象となる機器以外の機器~~(当該立入制限区域内に保守及び点検の対象となる機器に記録された管理対象情報以外の管理対象情報が置かれている場合には当該管理対象情報を含む。)~~を撤去すること等により作業者~~が~~の当該保守及び点検の対象となる機器以外の機器への接触を防止するための措置を講じた上で、作業者が作業を実施している間は~~管理者等管理情報システムの維持に責任を有する者が常時立ち会うようにし、又はその指定する者~~事業者の従業員等に立ち会わせ、~~当該指定する者からの~~作業の状況の報告を受けるものとする。	
	6		事業者は、クラウド等を管理する者又はデータセンターのサーバ等で管理対象情報を管理している場合~~における、~~その従業員等が、当該サーバ等の保守及び点検を行うときは、■■に掲げる措置に相当する対応を実施することをクラウド等を管理する者又はデータセンターのサーバ等を管理する者に確認~~以下のいずれかの措置を実施~~する。 ~~一 その保守及び点検を行う者がクラウド等を管理する者又はデータセンターの従業員等である場合 当該保守及び点検を行う従業員等を確認する等の措置~~ ~~二 その保守及び点検を行う者がクラウド等を管理する者又はデータセンターの従業員等以外である場合 当該クラウド等を管理する者又はデータセンターにおいて 25、26 に掲げる措置等適切な措置を講ずることを確認する等の措置~~	

表 2-29 基準告示の項目別修正案(情報システム上の管理対象情報へのアクセスの制限)

項目番号		項目名	内容(案)	備考
V	第十三	情報システム上の管理対象情報へのアクセスの制限	事業者は、情報システムに管理対象情報を保存する場合、当該管理対象情報へアクセスすることによる管理対象情報の流出を防止するために必要な措置を講ずる。 その際、以下に掲げる措置その他この目標を達成するために有効な措置から必要な措置を選択して実施する。	必須目標を追記
	1		事業者は、アクセス権設定等の特別な権限を持つ情報システム管理者~~管理者等管理情報システムの維持に責任を有する者~~の管理情報システムへのログインに対して、二つの認証機能(パスワー ド、生体認証、電子証明書等)を組み合わせた二要素認証を導入する。	
	2		事業者は、アクセス権者によるテレワーク等外部からの管理情報システムの管理対象情報へのアクセスについて、利用者の認証を行うための手順(情報システム管理者~~管理者等管理情報システムの維持に責任を有する者~~は、あらかじめ、認めた範囲でのみ認証をするためのものを含む。)を確立する。	
	3		~~とともに、~~事業者は、アクセス権者によるテレワーク等外部からの管理情報システムの管理対象情報へのアクセスについて、可能な限り暗号化された通信路を用いさせる。	
	4		情報システム管理者~~管理者等管理情報システムの維持に責任を有する者~~は、電子政府推奨暗号を用いて暗号化する等の措置を講じる。~~た上で管理情報システムにおいて管理対象情報を適切に管理するための手順を確立する。~~	

表 2-30 基準告示の項目別修正案(情報システム上の管理対象情報へのアクセス権者の限定)

項目番号		項目名	内容(案)	備考
V	第十四	情報システム上の管理対象情報へのアクセス権者の限定	事業者は、情報システムに管理対象情報を保存する場合、当該管理対象情報へのアクセスを行う者を必要最低限に限るために必要な措置を講ずる。 その際、以下に掲げる措置その他この目標を達成するために有効な措置から必要な措置を選択して実施する。	必須目標を追記
	1		事業者は、管理情報システムの利用者の職務内容に応じて、利用できる管理情報システムの機能を制限した上で、これを提供する。	
	2		事業者は、アクセス権者による管理情報システムへのアクセスを許可し、適切なアクセス権を付与するため、管理情報システムの利用者としての登録及び人事異動等に伴い速やかに登録の削除をする~~ための手順(定期的な見直しを含む。)を確立する~~。	

表 2-31 基準告示の項目別修正案(ログイン ID・パスワードの管理)

項目番号		項目名	内容(案)	備考
V	第十五	ログイン ID・パスワードの管理	事業者は、情報システムにアクセス権を設定した管理対象情報を保存する場合、当該管理対象情報へのアクセスを行う際のログインIDおよびパスワードについて、適切に管理されるための必要な措置を講ずる。 その際、以下に掲げる措置その他この目標を達成するために有効な措置から必要な措置を選択して実施する。	必須目標を追記
	1		事業者は、管理情報システムの利用者に対して、初期又は仮のパスワードを発行する場合には、容易に推測されないパスワードを発行する等その適切な管理に配慮した方法で発行する。	
	2		事業者は、アクセス権者に~~おいて~~パスワードを自ら設定させ、パスワードを設定する場合には、当人の関連情報(例えば、名前、電話番号、誕生日等)に基づかないこと、辞書攻撃に脆弱でないこと(辞書に含まれる語~~から~~だけで成り立っていないこと)、~~同一文字を連ねただけ、~~数字だけ、又はアルファベットだけの文字列ではないことを求めること等アクセス権者以外の者から容易に類推されないような設定とするようアクセス権者に周知~~し、又は管理情報システムでパスワードを設定する者に対してその要求をするように~~する。	
	3		事業者は、管理情報システムそのものに、必要に応じてパスワードの変更を利用者に促す機能やパスワードの再利用を防止する機能等を持つようにする。	
	4		~~情報システム管理者管理者等管理情報システムの維持に責任を有する者~~は、アクセス権者等に対して、管理情報システムにログオンするためのパスワードを記載した紙を目に見えるところに置かないこと等を周知する。	
	5		事業者は、管理情報システムへのアクセスについては、複数者間で同じパスワード(共通パスワード)を使用しないための手順を確立する。	

表 2-32 基準告示の項目別修正案(情報システム上の管理対象情報への取扱いルール策定)

項目番号		項目名	内容(案)	備考
V	第十六	情報システム上の管理対象情報への取扱いルール策定	事業者は、管理対象情報が電子情報である場合の当該管理対象情報の取扱いについて、必要な手順を確立する。 その際、以下に掲げる措置その他この目標を達成するために有効な措置から必要な措置を選択して実施する。	必須目標を追記
	1		事業者は、可搬式記録媒体に管理対象情報が記録されている場合には、当該可搬式記録媒体を管理対象情報そのものとして取り扱うための手順(可搬式記録媒体の使用を事業者が承認し、当該可搬式記録媒体を他の技術等情報が記録された可搬式記録媒体と容易に区別することができるよう措置するための手順を含む。)を確立する。	
	2		事業者は、管理対象情報を可搬式記録媒体に保存した上で管理情報システムからの消去を行うこと、他者から預けられた管理対象情報であって可搬式記録媒体に記録されたものを事業者の可搬式記録媒体にのみ保存し、利用すること等により、当該管理対象情報を、必要最小限の範囲で取り扱うための手順を確立する。	

表 2-33 基準告示の項目別修正案(可搬式記録媒体の保管)

項目番号		項目名	内容(案)	備考
V	第十七	可搬式記録媒体の保管	事業者は、管理対象情報を記録した可搬式記録媒体が適切に取り扱われるために必要な措置を講ずる。 その際、以下に掲げる措置その他この目標を達成するために有効な措置から必要な措置を選択して実施する。	必須目標を追記
	1		情報システム管理者~~管理者等管理情報システムの維持に責任を有する者~~は、管理対象情報を記録し、又は記録のために用いる可搬式記録媒体の管理簿(保守及び点検の記録、持ち出した場合の持ち出しの記録、データの消去の記録、廃棄した場合の廃棄方法及びデータの消去の記録、セキュリティパッチの状況等の記録を含む。)を作成し、合理的な期間保管する。	
	2		事業者は、管理情報システムを構成する機器及び立入制限区域等の特定の場所でのみ使用する可搬式記録媒体について、施錠できるラック等への設置、セキュリティワイヤでの固定等不正な持ち出し、盗難等から保護するための措置(ラック等の鍵について、情報システム管理者~~管理者等管理情報システムの維持に責任を有する者~~による管理を含む。)を講ずる。	
	3		事業者は、管理対象情報を記録した可搬式記録媒体を施錠することができるロッカー等に集中的に保管し、その鍵等を適切に管理する。	

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、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

認証制度の普及を促進し、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、調査分析事業について、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」を設置した。

（2） 設置期間

2022 年 10 月 14 日～2023 年 3 月31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　専門委員
	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
	小暮 亮	全国商工会連合会　産業政策部　産業政策課　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

（2022/3/3 時点、委員五十音順、敬称略）

（4）開催概要

1）第 1 回

表 2-34 技術情報管理認証制度に係る検討会 第 1 回会合

日時	2022 年 10 月 14 日(金) 15:00 ～ 17:00
場所	株式会社三菱総合研究所 4 階大会議室 C ／ 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 2-35 技術情報管理認証制度に係る検討会 第 2 回会合

日時	2022 年 12 月 22 日(木) 13:00 ～ 15:00
場所	株式会社三菱総合研究所 4 階 CR-B 会議室 ／ オンライン開催(WebEX)
議題	(1) 開会 (2) 自己チェックリスト及び活用ガイドについて (3) 基準の在り方について (4) 今後のスケジュールについて

3）第 3 回

表 2-36 技術情報管理認証制度に係る検討会 第 3 回会合

日時	2023 年 3 月 3 日(金) 17:00 ～ 19:00
場所	オンライン開催(WebEX)
議題	(1) 開会 (2) 自己チェックリスト及び活用ガイドについて (3) 基準の在り方について (4) 今後のスケジュールについて

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

認証制度の普及を促進し、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、認証制度の在り方を検討し、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検討するために、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」を設置した。

（2） 設置期間

2022 年 10 月 26 日～2023 年 3 月 31 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
	小谷野 裕司	ライド株式会社クラウド事業部・インフラ事業部・認証事業部長
	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 事業開発グループ長
	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 ISMS 技師長
	光守 健	日本検査キューエイ株式会社 執行役員
	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

（2023/2/20 時点、委員五十音順、敬称略）

（4） 開催概要

1）第１回

表 2-37 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	2022 年 10 月 26 日(水) 13:00 ～ 15:00
場所	株式会社三菱総合研究所 4 階大会議室 A ／ オンライン開催(WebEX)
議題	(1) 開会 (2) 経済産業省 挨拶 (3) 委員挨拶及び今年度の認証取得見込み、取組状況について (4) 運用ワーキンググループの趣旨について (5) 運用ワーキンググループの取り扱いについて (6) 今年度の事業について (7) 今後のスケジュールについて

2）第２回

表 2-38 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	2022 年 12 月 6 日(火) 15:00 ～ 17:00
場所	株式会社三菱総合研究所 4 階 CR-D 会議室 ／ オンライン開催(WebEX)
議題	(1) 開会 (2) 自己チェックリスト及び活用ガイドについて (3) 基準の在り方について (4) 今後のスケジュールについて

3）第３回

表 2-39 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	2023 年 2 月 20 日(月) 15:00 ～ 17:00
場所	株式会社三菱総合研究所 4 階 CR-E 会議室 ／ オンライン開催(WebEX)
議題	(1) 開会 (2) 自己チェックリスト及び活用ガイドについて (3) 基準の在り方について (4) 今後のスケジュールについて

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（3 者）

2）ヒアリング項目

(1)情報管理に関わる昨今の動向について
(2)類似制度や昨今の状況を踏まえた認証制度に求められる修正について
(3)情報管理に関する認証制度の在り方について

3）結果概要

a. 情報管理に関わる昨今の動向について

- 「組織における内部不正防止ガイドライン」が、2021 年度改訂され第 5 版として発行された。改訂の基本的な考え方として、トップの関与が明確化された。5 つの基本対策（①アクセス権管理、②持ち出し困難化、③ログの記録、④ルール化と周知徹底、⑤職場環境の整備）は、サイバーセキュリティ対策とほぼ一緒であるが、内部不正対策で特徴的なのは⑤職場環境の整備と考えられる。昨今は、個人情報保護に加え、営業秘密保護がリスクとして大きくなっているため、第 5 版の改訂では営業秘密保護が重視されている。
- 基準は、業界毎に細かく定めている場合もあるし、全く定められていない場合もある。規制がある業界はやっている。電機業界は、かつては自動車業界に近い形のサプライチェーンだったと思うが、現在はグローバルも含めて協力会社の統制が弱くなっているのではないか。製品自体の競争力が下がっているので、認証コストを製品価格に転嫁しづらい可能性もある。
- 防衛産業ではサイバーセキュリティ基準が作られており、来年度契約から適用となっている。各企業の理解は、大企業は担当者はいるのでともかく、中小企業は進んでいないのではないか。

b. 類似制度や昨今の状況を踏まえた認証制度に求められる修正について

- 内部不正ガイドラインでは、テレワーク、雇用の流動化、法改正等 7 つの課題と 3 つの重要対策ポイントとして以下を示している。
  ① テレワーク・クラウドの普及に伴う対策：セキュリティ対策
  ② 退職者関連対策：退職者のアカウント管理・モニタリングに関する施策。一定程度持ち出す人はいるが、抑止が重要
  ③ ふるまい検知等の新技術対策：AI 等による行動監視・検知技術導入におけるプライバシー・コンプライアンス等に関する注意事項

- モニタリングで雇用者のモチベーションを下げない施策が重要である。経営者は、従業員を守るために監視を行っていることや、人事評価には使わない点を従業員に伝える必要がある。
- 多くの企業においては、重要情報が特定され分けられていない。重要情報を特定する点を、認証制度で明確に書けるとよいのではないか。
- 認証制度の現行基準については、ある部分については非常に細かく定められており、非常にアンバランスである。個々の管理策は、ISMS 認証では定めているが、具体的な内容までは規定していない。逆に、NIST の規格や、FISC や PCIDSS も細かく基準が定められている。認証制度において、どこまで細かく示すかは要検討である。
- 基準においては、強度の高い考え方も含め、様々なレベルの項目が数多く書かれているが、求める最低限のものが書かれていればよく、それ以上対策を強くするには事業者がやればよいと考える。物理的防御を高めることもよいが、多くの項目は必要ないとは考える。
- 基準においては、最低限実施すべき項目はあった方がよい。現行基準は、総論的に書かれた項目以外は事業者が選ぶこととなっている。例えば、誓約書を書いてもらう、というのが選択肢の 1 つにあるが、経営者が要らないといえばそれでよいのか。あるいは、物理的防御も、壁何メートルは要らないまでも中が見えないようにする程度の基礎的な対応は要らないのか。本認証制度は、経営者が決めたレベルでやっていることを認証するものなので、意味のある認証とするからには、また認証取得を宣言してリストに載るからには、意味のある項目で取得しているかが懸念される。それを考えると、最低限の対策が見えた方がよい。

c. 情報管理に関する認証制度の在り方について

ア） マーケティングについて

- 製造業や技術情報という観点で、目に見える資産、図面などへの対策を強化しているという特徴付けまで PR できていない。様々な業界で使っていただけるのはよいが、マーケティングとしては業界を絞った方がわかりやすい。
- 制度設計は国が行ってもよいが、セミナーやプロモーション、営業マーケティングは認定機関等、他の機関にやってもらうのがよいのではないか。その点で、認定制度も含めた形で強化することも検討してよいのではないか。
- プロモーションについては、業界を決め、具体的なアプローチを考えていくべきである。例えば、ISMS 認証は入札要件に定められているため取得している事業者も多く、公共の仕事をしている部門や防衛系の部門が、部門単位で取得している。自治体でも、この認証を取っていればISMS 認証と同等とするなど、入札要件に定めていけば認証取得は増えるだろう。
- 認証制度は、自主的にセキュリティを高める、そのための指標として推進されていると理解しており、それが、認証や自己チェックリストといった策に繋がっていると思う。そのため、契約条件に含めることは一挙には行かないだろうが、普及のためには何らかの強制力というのも必要である。情報管理は重要であるが、所管省庁やプライムから言われなければ対策が進まないのが実態なので、国として入札の要件に入れるなどを検討いただくとよいのではないか。

イ） 制度の位置づけについて

・ 認証制度が、マネジメントシステム系か、そうでないのかという観点がある。管理策に近づくと、できている／できていないが判断しやすくなりチェック可能となる。マネジメントシステム系は汎用的なルール作りで自由度がある。汎用型とするならば、ISMS 認証の簡易版という位置づけがわかりやすいのではないか。

ウ） 認証機関のインセンティブについて

・ 認証機関は一回制度を始めるとやめられない。それなりにニーズがあることが見込めないと、積極策をとれない状況なのではないか。
・ 認証機関にとっては、現在の制度では 3 年に 1 回しか収入がなく、収支のバランスから言うと、収入が大幅に上回るということではない。審査をしてもコンサルができるというのは大きな特徴であり、コンサルを収益につなげることも可能であるが、コンサルができない認証機関にとってのメリットも考慮する必要がある。例えば、1 件あたりの金額は小さくても、次のステップで ISMS 認証を取得することとなれば、認証機関としてはビジネスになる。また、ISMS 認証のようにセクター毎の拡張版のような形で広げる考え方もある。情報管理に関する認証は一度やったら終わりではなく、深めていくということが本質なので、そこをうまく活用できればよい。

（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（6者[1]）

2） ヒアリング項目

(1)業界の状況について
(2)自己チェックリストや活用ガイドに求められる役割と、作成に当たって必要な事項について
(3)認証制度の活用可能性について

3） 結果概要

a. 業界の状況について

ア） 業界 A

・ 取引先からの情報管理の要求は一部あるが、ほとんど求められていないのが実態である。欧州は厳しくなってきて、この 2、3 年で情報管理を求めるようになってきた。

[1] 一部ヒアリング対象者は、(1)認証制度の在り方に関するヒアリング調査の対象者と重複している。

- 企業の現場を実際に見ると、対策ができていないところも多い。システム的に制限をかけていないので、厳密な運用はできていない。グローバルカンパニーの場合は厳しく管理されるが、日本企業はまだ従業員に対して甘いところがある。
- 情報管理は NDA 締結ぐらいが実態。何かあった場合の責任を明確化することが目的。NDA を結んだからといって、対策は万全かというとそうではない。
- 発注元が委託先までチェックしているのは皆無と言ってもよい。監査に行っても厳しくは見ていない。契約は、長年の信頼関係に基づき、性善説で対応していることが多い。
- 社内でも従業員を信用していて、基礎教育ができていない。
- 担当者が情報管理の必要性を社内で訴えても、上司からは金のかかることをやらなくていいと言われる。情報管理については、団体からの周知を行っても手応えがない状態である。
- 情報管理については、従業員 100 人ぐらいの規模でも難しく、50 人未満だと IT 担当も不在であることから、ほとんど対策はできない。従業員 200 人程度の規模では部長クラスで問題意識を持ち、社長も巻き込んだ対策を進めることもできるので、担当の部長クラスを通じて経営者に伝える流れを作るとよいのではないか。従業員 50 人程度の企業は対策の責任をトップが担っているので、社長に問題意識を持たせる必要がある。

イ） 業界 B

- 今まで、具体的な管理手法を求められることはなく、秘密保持契約で締結するのが一般的であった。
- 最近は、取引先から情報セキュリティ対策に関する取引先業界のチェックリストの記載を求められるケースはある。取引先独自の基準を示され、準拠を求められた事例もある。

ウ） 業界 C

- 目に見えない技術が強みであり、信用で取引関係を築いている。取引先とは一度契約を行うと、他社で同じ製品を作ることができるわけではないので、簡単に他社に契約を変えられることはない。取引先からも技術について情報開示の要求はなく、技術情報は自社に閉じている。
- 技術そのものより、どの会社がどういう技術を用いて何を作っているか自体、会社の名前すらも秘匿したい。
- 重要なノウハウを持っていれば情報管理について神経を尖らすだろうが、小規模な企業で、情報について秘匿が要求されていない取引であれば、厳密な管理にならない企業もあるだろう。各社ともなんらかの重要な情報は持っており、個社毎に情報管理をしているが、レベル感は様々であろう。
- 10 名程度の会社であっても、IoT、BCP、脱炭素、担当が 1 人で情報を入手し、取組を進めている企業もある。小規模であっても、何事にもしっかりと取り組む企業はある。

エ） 業界 D

- 情報管理は秘密度に応じて求められ、管理方法は各社様々である。

- 再委託先まで直接管理できていないのが実態である。委託先に情報管理を要求し、再委託先も管理するよう伝えている。製品種別によっては厳しく要求している場合もある。
- 目指してほしいレベルは取引先にも伝えるが、必ずしもそれを満たさなければ取引をしないということではなく、自分事として捉えて対策を進めてほしいという位置づけである。
- 自己チェックの場合、厳しく見る会社もそうでない会社も様々あるのが実態である。数字化に意味はあるが、絶対値での企業の比較を行うものではなく、各企業の経年変化を見ることなどに使えるとよいのかもしれない。
- 取引先に対してどこまで要求できるかは課題である。自分事として取り組んでもらうことが本来の姿で、どれぐらい強くお願いしていくのかは配慮しなければならない。

オ） 業界 E

- 企業秘密のような重要な情報を取り扱っている企業は ISMS 認証なども取得している。
- 取引先との契約において定められない限り、対策はなかなか進んでいないのが実態である。

カ） 業界 F

- 周知のためにメルマガを出してきたが、イメージしづらい・難しそうという受け止め方をされている。直接リアルな話をして説明した方が良い。案内の後に少しでも刺さりそうな人に手を打っていかないと、周知だけだと難しいと思われる。色んな段階でのリーチが必要だと思われる。
- セミナーは地道に続けていけば効果が出てくる。最初のころは反応が悪いこともあるが、ある日突然向こうから問い合わせが来たりすることがある。継続して実施すると良い。

b. 自己チェックリストや活用ガイドに求められる役割と、作成に当たって必要な事項について

ア） 記載の内容について

- 自己チェックリストに委託先への要求事項を入れたのはよい。認証の審査でも重要な項目と考える。
- 専門的な用語は正しく使って、注釈をつけるなどしてはどうか。わかりやすさのために言葉を変えることで、本来の意味が伝わらなくなることも懸念する。
- 自己チェックリストは、項目が網羅されているものよりは、自社の対策で不足していることがわかり、それを実施すると次に進めるなどのしかけがあると、見る人が増えるのではないか。
- わかりやすい解説がないといけない。絵を入れ図示して、よりわかりやすいものが必要と考える。

イ） 記載の分量について

- 13 項目＋αと、必要な項目が絞られているので見やすいと考える。
- 活用ガイドは対策が全て書いてあるよりは、現状の素案のような量でないと読む気にはならないだろう。
- 基本的には項目数は少なく、きちんと内容が示されているのであれば有効であろう。

- 量が少なければ少ないほど目は通すだろう。現状の量であれば取り組みやすいだろう。
- 記載の分量については、年商か従業員数の規模で分ける方法もあるのではないか。

ウ）見やすさについて

- 視覚的に見やすいものがよい。情報管理は継続することが重要なので、一度自己チェックリストをベースに対策を確認した後、疲れ果ててしまうようなものではなく、来年もやりたいと思えることが重要であり、継続して取り組みやすいものがよい。
- 漢字の密度が詰まっているとイメージが沸きにくいので、漢字を少し減らすと、頭に入りやすく、取り組みやすくなるのではないか。

エ）活用方法について

- 小規模企業が多いので、自己チェックリストや活用ガイドが活用できると考える。
- 平素の業務に追われており、複雑なことは後回しになるので、情報管理は大事だと思っても後回しになりがち。簡単に平素の状態をチェックできるとよい。そういったものがあると、意識改革に繋がる。
- 経営者などが考えるきっかけとなるのであればよいのではないか。情報管理の重要性は皆わかっており、進めたいと思っているので、そのきっかけになるとよい。
- 自己チェックリストを作るだけでは、認証制度の普及を進めるという観点では効果的ではない。Web ページに載せるのであれば Web ページに来てもらうために努力すべきである。
- 業種毎の平均達成レベルと回答企業を比較できる可視化ツールのようなものがあるとよいのではないか。
- 自己チェックリストの目的は 1 つではないだろうが、認証取得の準備のものとするのか、認証取るまでではないが自分で情報管理対策の確認をやるという企業に使ってもらうかで必要な内容が異なるだろう。認証取得の準備とするのであれば詳しい内容が必要である。認証取得のために 100 程度の要求項目があるのを、10 項目だけのリストで大丈夫とすると、誰も認証を受けるとはならないだろう。

c. 認証制度の活用可能性について

ア）業界としての活用可能性について

- セキュリティ対策に関しては、双方に知識がないと確認に時間がかかるが、「認証を取っている」の一言で説明を省略できることが認証取得の魅力である。
- ロゴマークはよい。一般的に取引を行う際に、上場企業を優先して取引したいというような安心感・信頼感と同様、信用度を増すというステータスを持てれば、ビジネスチャンスにつながるため認証取得も増えるのではないか。
- ものづくり補助金、省エネ補助金の審査などで加点されれば、情報管理に取り組み、認証を取ろ

うという企業が増えるのではないか。比較的よく使う補助金であることが望ましい。会員企業の事業に少しでも役に立つ情報を提供するのが業界団体の業務でもあり、補助金などとセットで案内できれば、会員に対してアピールしやすい。

- 競合他社に加点があると優位性をもたれるので、事業者にとっては同時にリスクにもなる。補助金はメリットがわかりやすい。
- 仮に事故が起こったとしても、対策を行っていれば、ここまでやったけど事故が起こってしまったと説明できることが望ましい。
- 認証を受けたことによるメリットが何になるか。認証を受けて、どうアピールできるか。情報管理体制を持っていることを公表できるのであれば、うちも取ろうとなるだろう。

イ） 普及の対象について

- 普及を働きかけるには経営層の方がよい。理解している人は言われなくても情報管理は行っており、愛社心あるいは危機感からやっていることもあれば、IT に強い人がやっている場合もあるだろう。認証取得によって、そのような情報管理を行う人も評価し、給与を払うということが必要である。
- 企業規模毎にアプローチを変えるのではなく、企業規模にかかわらず経営者に働きかけるのがよいのではないか。

ウ） 認証機関について

- 認証機関においても、この認証制度は単体で商売ができる商品ではなく、二次的な価値で事業が成り立っている。業界団体としても、会員満足度を高めるためにやっている。本来は、認証を取得することで認証機関・事業者とも満足することが必要である。
- 認証機関も増やした方がよい。

エ） 業界の取組との関連について

- 業界で定められている基準とこの認証制度については直接の関係はないため、このままでは関わりを持たせづらいと考える。
- 業界のガイドラインも取り込んでいかないと、企業側の混乱が生じると思う。カバーしている範囲が若干違う部分については、説明で対象の違いを示せるとよい。業界のガイドラインと揃えていかないと浸透しない。
- 第三者認証に対するニーズについては、外から見たときに間違いないという意味もあるが、現状はそこまで求めていない。他方、自分がチェックすると甘くなってしまうということもあり、何ができたら〇にしてよいかの判断も難しい。それを第三者に指摘してもらうことによって、不十分だったことがわかる、気づかないところを見てもらうという点は意味があると考える。第三者により自己チェックのサポートができる、改善ができるという点ではよいと考える。

オ） 普及策について

- 認証取得は、動機付け、メリット、強制力がないと進まないだろう。
- 認証のハードル次第で普及が進むのではないか。
- 日本では過去 ISO 9000 の流行があった。皆が取得するという状況が、認証取得に向かうこともある。
- 認証取得した企業が、次の更新タイミングの 3 年で脱落する可能性がある。普及のためには、更新に繋がる取組も必要である。
- 営業秘密の問題は、コンプライアンス面でも経営において重要なテーマである。SDGs は、これまでも地球温暖化などの課題としてあったが、現在は言葉を変えて推進している。カーボンニュートラルは具体的な数値目標があり定量的に把握できるということが、サイバーセキュリティより進めやすい理由かもしれないが、DX などデジタルとの関係で訴求できる可能性がある。

（3）ヒアリング結果からの考察

1） 事業者に対するインセンティブの必要性

業界団体からは、情報管理の取組を示すマークが取引先の安心感や信頼感につながるという点を評価する意見が得られた。また、補助金の審査における加点などのメリットは、事業者にとってもわかりやすく、業界団体としても会員企業に周知しやすいとの意見があった。

事業者における制度活用を促進するためには、認証を受けたことによるメリットを創出し、これらを明確に事業者にアピールしていくことが有効である。認証取得した事業者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、事業者において情報管理を進める担当者に対しても、その業務を評価し、適切な処遇を行うべきとの意見もあった。認証取得によって担当者が評価されるきっかけとなった事例もあることから、組織として情報管理を推進する役割を果たす担当者が事業者において評価されるような、組織体制、人事制度等を構築していく点についても、経営者に対してその必要性を訴えていくことや、良事例として示していくことが必要であると考えられる。

2）認証機関が魅力を感じる制度設計

認証取得を増やすためには、審査を行う認証機関を増やすことも必要である。認証機関を増やす取組と、認証取得事業者を増やす取組は、平行して検討する必要がある。まずは認証機関を増やすために、想定する業界団体等に対して、業界団体として認証制度に取り組むメリット・業界における効果等について認知を進めることが必要である。

また、認証制度は、ISO の認定を受けた認証機関や業界団体等、様々な立場の組織が認証機関となることが可能な制度であるが、認証取得の対象や審査内容等を考慮すると、認証機関が認証業務自体で事業化を行うにはまだマーケットサイズが小さいのが現状であり、認証機関にとっては付帯する業務によって価値を得ているというのが実態である。ヒアリングにおいても、認証事業自体で、認証機関・事業者とも満足することが必要であるとの意見があった。

3）業界団体における既存の活動との連携

業界によっては、業界独自の情報管理に関するガイドライン等を策定している事例も見られた。しかし、情報管理に取り組む事業者にとっては、複数の基準や類似した制度が乱立することで、混乱が生じるおそれがある。業界としての取組も本制度に取り込んでいくべきではないか、との意見もあった。

各業界で定める基準や制度の目的や対象範囲、要求する事項はそれぞれ異なるものであろうが、整合性を図るところは揃える、違いがあるならばその違いを事業者にわかりやすく示す、その上で本制度の特徴を明確にして打ち出すことで、双方の取組みが活性化されることが望ましい。

4）自己チェックリストや活用ガイドを通じた効果的な普及

自己チェックリスト素案は項目を絞って作成したが、ボリュームは多くない方が取り組みやすいという意見が多かった。また、簡単に情報管理の取組をチェックできるとよく、経営者が考えるきっかけとなる、事業者の意識改革に繋がることが期待できるとの意見もあった。

制度の普及を進めるためには、自己チェックリストそのものを充実させると共に、自己チェックリストを掲載した Web ページへの誘導策も合わせて検討する等のプロモーション策も合わせて検討する必要がある。また、今後は自己チェックリストを通じて業界標準との比較ができるといった、さらなる活用策についても検討していくことが有効である。

3. 業界等と連携した技術情報管理認証制度の普及活動

3.1 特定の業界・団体と連携した普及啓発活動

認証制度の認証基準について、制度の活用が見込まれる業界・団体を選定し、その実情を踏まえた適切な運用となるよう、認証制度の認証付与の方法を含めた活用方法の説明等の普及に向けた活動を、当該業界・団体に対して行った。

3.1.1 業界団体への制度説明、活用可能性の検討

（1） 説明対象

認証制度の活用が見込まれる業界団体（2 者）

（2） 説明内容

(1)制度の概要について
(2)業界における技術情報管理認証制度の活用可能性について

（3） 結果概要

制度説明及び質疑応答の後、業界における制度の活用可能性について以下の意見が得られた。

- 会員企業が、どんな印象を持つかは分からないが、日本金型工業会のように会員企業のレベルアップに有効との声が多ければ、活用検討の対象になると思う。
- 制度自体を知らない企業が多いと思うので、セミナー等での周知が必要と思う。
- 当協会の会員には大企業が多く、既に別の認証を取得していることも多いと思われるので、自らがこの認証を取得するというよりは、サプライチェーンに関係する中小企業に取得を依頼するケースが想定される。その場合、下請法などとの関係でどこまで強く要求できるかという懸念はある。
- 対策のレベルの差が分かるように、認証マークを複数にしてもらえると、企業側が個別に状況を確認する負荷が減り、管理レベルを判断しやすい。

3.2 認証制度取得事業者又は技術情報管理に取り組む事業者の声の収集

すでに認証制度による認証を受けた事業者又は技術情報管理に積極的に取り組んでいる事業者にヒアリングを実施し、技術情報管理に取り組むことによって得られた成果等の事例情報を収集し、認証制度の普及に向けて対外的に発信できるよう整理した。

3.2.1 調査概要

（1） 調査対象

認証制度による認証を受けた事業者又は技術情報管理に積極的に取り組んでいる事業者 5 社について、認証機関からの紹介等により選定した。

表 3-1 認証制度取得事業者又は技術情報管理に取り組む事業者 ヒアリング対象

	業種	従業員数	地域	設立
A 社	製造業（金属）	201-300 名	近畿地方	2000-2009 年
B 社	製造業（自動車部品）	101-200 名	中部地方	1950-1959 年
C 社	製造業（精密機械）	51-100 名	近畿地方	1970-1979 年
D 社	製造業（金型）	201-300 名	近畿地方	1960-1969 年
E 社	製造業（金型）	201-300 名	関東地方	1950 年以前

（2） 調査手法

オンラインによるヒアリング調査によって、事例情報を収集した。

ヒアリング調査により得られた内容については、対外的に発信する際に活用しやすいよう表形式で整理し、記載内容については調査対象企業の確認を行った。また、企業名については非公開とした。

（3） 調査項目

調査項目は以下の通りである。

- 技術情報の管理に関する現状
  - 管理対象となる技術情報
  - 管理に関する課題
- 技術情報管理の取組
- 技術情報管理認証の取得理由／情報管理の取組理由
  - 認証制度の認知媒体
  - 認証取得／
  - 情報管理の取組のきっかけ・理由

・　技術情報管理の取組や認証取得による効果

3.2.2 調査結果

調査結果を次ページ以降に示す。

A 社		
業種	製造業 （金属）	**＜対策のポイント＞** ・取引先からの要請に応えるために、情報管理の取組を推進。守るべき情報を真に重要なものに絞り、業務への影響を抑えつつ、現場の理解を促しながら、クラウド移行や可搬式記録媒体の管理等の対策を進めている。
従業員数	201-300 名	
地域	近畿地方	
設立	2000-2009 年	

■技術情報の管理に関する現状	
管理対象となる技術情報	● 特定のお客様から預かった情報、自社の技術情報を管理対象とした。
管理に関する課題	● 紙が中心の管理であり、持ち出しや利用状況の把握が困難であった。
■技術情報管理の取組	
技術情報管理の取組	● ここ 5 年間で、重要な情報を徐々にクラウドに移行した。キャビネット 1 台分の紙文書を廃棄した。重要な情報は工場の壁への掲示も止めた。 ● 重要な情報としてクラウド化する情報は、まず一部の事業に限った。監督職以上にアクセス権を持たせ、対象者に対して理解を進めた。一般職は、監督職の許可が必要になったので、手間を感じている可能性はある。 ● 可搬式記録媒体（PC,USB メモリ等）は、重要情報に限らず全社一律で同じ管理とし、持出しを許可制にした。帰宅時は PC を施錠管理するようにした。 ● 試作品については、業務上社員の立ち入りがあり、入室制限を行える場所で保管することが難しい状況だった。できるだけお金をかけず、監視カメラを新たにつけることから始めた。
■技術情報管理認証の取得理由／情報管理の取組理由	
認証制度の認知媒体	● 認証機関のパンフレットによって技術情報管理認証制度を知った。
認証取得／情報管理の取組のきっかけ・理由	● 中小企業庁の補助事業に申請する際、管理団体から情報管理の状況について質問を受けた。チェックシートの対策項目がほとんどできていなかったことに危機感を感じた。 ● 取引先から情報管理に関する要請が再三あり、どうしてよいのかわからなかったところ、情報管理認証制度のパンフレットを見て、取り組むことにした。 ● ISMS（情報セキュリティマネジメントシステム）認証はハードルが高かったため、技術情報管理認証を取得することにした。
■技術情報管理の取組や認証取得による効果	
技術情報管理の取組や認証取得による効果	● 取引先からの情報管理の要望に対して対応できる状況となった。 ● 情報管理はこれで終わりということはないので、継続して取り組んでいきたい。 ● 現在は、事業継続計画（BCP）策定の取組を始めたところであり、災害対応を主に考えているが、情報漏えいの観点も取り込むことで、対外的にいいアピールができるかもしれないと考えている。

B 社		
業種	製造業 （自動車部品）	**＜対策のポイント＞** ・お客様から業界のセキュリティチェックリストの対策が要請されていることから、ハード的な対策と共に、社員の意識を高めながら運用面の対策を進めている。自社独自のわかりやすい啓発資料を用いて教育を行い、DX 推進とともに、その情報を守る重要性も意識付けている。
従業員数	101-200 名	
地域	中部地方	
設立	1950-1959 年	

■技術情報の管理に関する現状	
管理対象となる技術情報	● 取引先から預かった図面データ、それを元にどのように作るかという情報が最も重要である。 ● 自社のノウハウ、現場のデータ（手順書、IoT で収集した現場のデータ：品質や生産性向上、設備を止めないための設備情報等）が重要な情報である。 ● 最近は電子データが多いが、今でも紙の情報はある。取引先とはモノでのやりとりもある。
管理に関する課題	● 情報の取り扱いに関する社内の認識に、上と下とでギャップがある。社内で制度化し、対策を練っても、現場が思うように動かないところが課題である。 ● 他社事例を見ると、トップダウンで会社として取り組むと、教育の頻度も高く、うまくいっているように見える。逆にリーダーシップがなく、情報管理の取り組みを行う宣言ができていないと、現場に意識の高い人間がいても、トップはそう言っていないからと受け流されてしまう。
■技術情報管理の取組	
技術情報管理の取組	● 自動車産業サイバーセキュリティガイドラインのチェックリストが回ってきて、お客様から、期間内で評価点を満たす対策を要請されているため、それに沿って対策に取り組んでいる。 ● ハード的な対策はわかりやすく、チェックリストの評価に反映されやすいため、ファイアウォールの導入等から実施し、社員の意識を高めつつ、運用面も合わせて対策を進めている。 ● 社内のセキュリティに関する意識を高めるために、IPA「5 分でできる！情報セキュリティ自社診断」を参考に、自社向けに社内事例を交えてわかりやすくした資料を作成し、社員が集まる機会を活用し、5～10 分で説明している。 ● データ活用を促しながら、合わせてセキュリティに関しても教育をしようと考えている。 ● 社内だけでは情報も限られ、進め方もわからないので、支援機関からの専門家派遣を受け、DX と合わせてセキュリティの取組を進めている。
■技術情報管理認証の取得理由／情報管理の取組理由	
認証制度の認知媒体	● 中小企業団体中央会から案内を受けた。
認証取得／情報管理の取組のきっかけ・理由	● きっかけは、自動車産業でセキュリティインシデントがあり、業界団体から具体的な対策実施の通達が回ってきたことである。顧客からの強い要望は取組を始めるきっかけとなった。 ● 認証取得により情報を守る姿勢をお客様に見せていくということは重要。しかし、固定客である場合は、強みを見せて新たにアピールする必要性が薄い。新規顧客開拓に取り組む企業にとっては、積極的に活用できると考える。
■技術情報管理の取組や認証取得による効果	
技術情報管理の取組や認証取得による効果	● 社内の情報を見直し、その価値を再認識できることはメリットである。新たな事業展開に繋げることができると感じる。対策には費用がかかるので、投資としていくらまでできるか、事業に対する効果を考えていくのは重要である。情報資産をどう捉え、どう活用していくかは、中小企業の生き残りや活性化のために必要である。

C 社		
業種	製造業 （精密機械）	**＜対策のポイント＞** ・重要な技術情報を適切に管理し流出漏洩を防止し守ることで自社の事業活動の継続及び競争力を強化する。
従業員数	51-100 名	
地域	近畿地方	
設立	1970-1979 年	
■技術情報の管理に関する現状		
管理対象となる技術情報	● お客様からお預かりした技術情報、自社製品の開発情報、お客様へ納入した製品の技術情報	
管理に関する課題	● 可搬式記憶媒体（外部メモリ、NAS（ネットワークに接続可能なハードディスク））の取扱いについて規程で定め、会社から支給されたもののみを使用、使用都度のチェックや万一紛失時の措置等も含めているが、取り扱いの維持継続を懸念している。	
■技術情報管理の取組		
技術情報管理の取組	● 制度を知ってすぐ認証に向けて取り組んだわけでは無く、中期経営計画で取得を計画した。重要技術の特定（守る情報の決定）、重要技術の識別・措置方法や管理プロセスについて規程として策定した。策定及び運用にあたり、以下に工夫し取り組んだ。 ➢ 技術情報管理認証制度のチェックリストを基に、わかりやすい用語を用いて、自社で実施していた事項も含めルール化した。 ➢ 技術情報の特定に時間を要したが約 300 項目のチェックリストの理解とそれを考慮し重要技術情報を守る為に何に取り組むべきか検討した。 ➢ INPIT（独立行政法人　工業所有権情報・研修館）や経済産業省主催のセミナー受講等により知識習得や従業員の意識向上に取り組んだ。 ➢ 内部監査は ISO9001、14001、技術情報管理認証の 3 つのマネジメントシステムを同時に実施。該当プロセスを総合的に監査し改善につなげることと、現場の負担軽減にもなっている。	
■技術情報管理認証の取得理由／情報管理の取組理由		
認証制度の認知媒体	● 日本経済新聞（2017 年に掲載された記事を見て）	
認証取得／情報管理の取組のきっかけ・理由	● 兼ねてからお客様からお預かりする技術情報の保護、自社技術情報の管理に取り組む必要があると認識していたことと、取り組みのお墨付きをいただけるものであるため。	
■技術情報管理の取組や認証取得による効果		
技術情報管理の取組や認証取得による効果	● お客様情報の保護、自社技術情報の管理に対しての従業員意識の向上がみられる。 ● 経済産業省のホームページにも掲載いただき士気が上がるが、活動を継続し改善を繰り返すことで認証にふさわしいよう努力している。	

D 社		
業種	製造業 （金型）	**＜対策のポイント＞** ・情報管理を進めるにあたって、製造業で馴染みのある 3S 活動（整理・整頓・清掃）を活用し、現場の納得を得ながら段階的に取組を進めた。定期的な教育により現場の意識付けを行い、利便性と管理のバランスを取りながら対策を進めている。
従業員数	201-300 名	
地域	近畿地方	
設立	1960-1969 年	
■技術情報の管理に関する現状		
管理対象となる技術情報	● 情報資産の特定から始めた。重要情報はお客様からお預かりした情報で、主に製品図面である。共同で技術開発を行う場合は、技術的な仕様書を共有することもある。 ● 9 割以上は電子データで取引先とやりとりを行っているが、印刷した紙を使うこともある。	
管理に関する課題	● 情報管理の運用を徹底することは難しい。定期的に情報管理の教育、リマインドを行うことが課題と考えている。人の出入りがあるので、どういうトレーニングをしていくか規程を作り、最初に説明会を実施している。1 年に 1 回など、定期的な実施が必要と考えている。 ● どんどん便利なサービスが出てきており、利便性と管理のバランスが難しいと感じている。	
■技術情報管理の取組		
技術情報管理の取組	● 情報は極力一元管理している。最近は、社内の情報共有のために、営業部門の情報管理ツールを技術部門にも展開し、扱う情報に「重要」マークをつけて取り扱おうとしている。 ● 印刷物が綴じられたファイルにはお客様図面も含まれるので、ファイルを保管したキャビネットを入退室管理が可能な部屋に設置し、古い情報は倉庫の施錠可能な場所に置いた。 ● 最初は、経験が長いエンジニアほど、情報を傍に置きたいという要望があった。認証取得活動の一環として、期間を区切って対策を進めたところ、手間が増えたという声はなかった。 ● 現場の納得を得るために、段階を踏んで取組を進めた。スペースを確保するために一時的な置き場所を作った。100 冊～150 冊のファイルが入るキャビネットで、使ったり参照したりしたらシールを貼る取組を行い、1 ヶ月経ってシールを貼られていたらその場所に置く、2 ヶ月経ってシールが貼られていなかったら倉庫に行くなど、利用状況に応じた整理を行った。 ● 元々、徹底 3S 活動（整理・整頓・清掃）という製造業の基本的な取組を行っており、要るものと要らないものを分ける、道具箱の中身で利用頻度の高いものはここに入れる、といった活動をこれまでも実施していたので、馴染みやすかったのではないか。 ● 強制的なアプローチではあったが、情報セキュリティの担当が、重要情報を持つ部門の出身で、現場に対する理解が深かったことから、話が通りやすかった。	
■技術情報管理認証の取得理由／情報管理の取組理由		
認証制度の認知媒体	● 業界団体から案内を受けた。	
認証取得／情報管理の取組のきっかけ・理由	● 業界団体からの推奨がきっかけとなったが、取引先からも確認を受けることが増えてきたため、認証を取得することを決めた。	
■技術情報管理の取組や認証取得による効果		
技術情報管理の取組や認証取得による効果	● 営業部門が名刺の認証マークを見せながら情報管理の取組をお客様に説明すると、安心だと納得される様子である。 ● 取引先から情報管理の取組状況について確認される際、認証取得していることで対策状況を説明できることも効果の 1 つである。	

E 社		
業種	製造業 （金型）	**＜対策のポイント＞** ・在宅勤務の増加等も背景にクラウド化を推進。お客様のデータもクラウドに載せることで、一元管理を行うと共に、スペースの問題やデータ消失リスクへも対応。認証取得をきっかけに対策が進み、取引先が求める対策レベルをクリア。
従業員数	201-300 名	
地域	関東地方	
設立	1950 年以前	
■技術情報の管理に関する現状		
管理対象となる技術情報	● お客様のデータ、CAD/CAM が重要な情報である。	
管理に関する課題	● 認証を取る際に、各工場からのインターネット接続は直接では無く、閉域網にして本社経由にした方が良いというアドバイスがあり、ネットワークに関して精査を行っている。コロナで在宅勤務も増え、境界で守るやり方から、ゼロトラストを前提に考え方を変えている。	
■技術情報管理の取組		
技術情報管理の取組	● 以前は、社内サーバに保存していたが、現在はクラウドストレージに保存して管理を行っている。ファイル名も、製造番号と紐付く形で関連性をつけて付番している。 ● クラウドストレージは容量無制限のもので契約している。買い足す心配がなく、スペースの問題や、故障してデータを消失するリスクもない。 ● CAD データは容量が大きいので、ネットワークを介すことでレスポンスが悪くなる懸念もあったが、読出・書込を全てクラウド上で実施してもレスポンスは問題にならなかった。フォルダもメールアカウントと紐付いており、アクセス権の設定や退職者が出たらアカウントを外すなども容易にできる。 ● 各事業部に管理者を設け、フォルダのアクセス管理は各事業部の担当者が専任で実施している。 ● 製造部門に限らず、あらゆるアプリケーションについて徐々にクラウドに移行している。 ● USB メモリは基本的には私物は使わない、持ち出し可能な機器はセキュリティワイヤーをつける、外出時は盗難に注意するなど、管理規程を設けている。情報の持出がないよう、USB ポートに物理的に栓をするなどの対策も行っている。	
■技術情報管理認証の取得理由／情報管理の取組理由		
認証制度の認知媒体	● 業界団体から案内を受けた。	
認証取得／情報管理の取組のきっかけ・理由	● 自動車メーカーのセキュリティ事案をきっかけに、お客様に迷惑をかけてはいけないという意識が高まり、認証を取るべきと考えた。	
■技術情報管理の取組や認証取得による効果		
技術情報管理の取組や認証取得による効果	● 社員のセキュリティに対する意識が高まった。社員の中で、この情報をインターネットに上げてよいのか、といった情報セキュリティに関する話が出るようになった。 ● 自動車産業サイバーセキュリティガイドラインのチェックシートが、いろいろなお客様から届いている。また、とある家電メーカーからも情報セキュリティに関するヒアリングを受け、合格の点数をいただいた。認証取得に際し、助言を受けたことで情報管理の取組が進み、対外的にもアピールできるようになったことは、非常によかったと考える。	

4. 今後の方向性

2～3 章の調査結果を踏まえ、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） 自己チェックリスト及び活用ガイドを活用した普及

今年度は、事業者が自身で情報管理の取組を行うための自己チェックリスト及び活用ガイドを策定した。これらのドキュメントは経済産業省の WEB ページに掲載され、情報管理に取り組む事業者がファイルをダウンロードして利用することになる。自己チェックリスト及び活用ガイドを広く事業者に認知いただくために、認証制度のパンフレットや資料等への掲載、認証制度に関連する各種説明会や講演会における周知、具体的な対策方法を学ぶためのセミナー等における活用等、事業者における情報管理の取組段階に応じて、関心を持つようなアプローチを体系的に行うことが必要である。また、周知の際には、自己チェックリストや認証制度において準備している研修素材等の他のコンテンツを組み合わせた効果的な普及策を検討することが有効である。

（2） 基準の見直しに関する方針策定

認証制度の基準は、策定時に参照された関連基準の項目が古くなっている場合や、サイバー攻撃等の脅威の変化により必要な項目も変化していることから、見直しの方向性について検討を行った。

今後は、実際に基準告示の見直しを行っていくことになるが、修正に関しては、認証制度の元々の目的に照らして、必要な項目がカバーできているか、認証制度の主なターゲットとなる中小事業者が目指すべき情報管理のレベルとして妥当な水準かといった観点を考慮しながら進めるべきである。また、認証制度の適切な運用のためには、認証審査の際に認証機関及び認証取得しようとする事業者が、新たな基準告示によって、双方の認識の相違なく公平性を持った審査ができるか、という観点も踏まえて、見直しを進めていく必要がある。

（3） 情報管理に取り組む事業者に対するインセンティブの創出

認証によって得られるマークが取引先の安心感や信頼感につながる点や、認証取得が補助金の審査における加点となる点は、事業者にとってもわかりやすいメリットとなる。

事業者における認証制度の活用を促進するためには、認証を受けたことによるメリットを明確にするとともに、取引先等となる主に大企業や業界に対しても認証制度の認知や活用を進めていくことで、事業者が認証取得をアピールできることにもつながる。認証を取得した事業者におけるインセンティブについては、引き続き検討を行い、関係する制度の運営主体や業界団体等との連携を進めることが有効である。

（4） 認証機関を増やすための環境整備

認証取得数を増やすためには、認証機関を増やすことも必要である。認証機関となることが期待できる業界団体等に対して、業界団体として認証制度に取り組むメリット・業界における効果等について認知

を進めることが必要である。さらには、業界団体が認証機関となる場合の標準的な事業モデルの提示や、専門人材を派遣する仕組み等、認証業務に知見やノウハウを持たない業界団体においても、認証業務に取り組みやすい環境整備が有効と考えられる。

併せて、認証機関が認証業務に魅力を感じるような制度設計を検討することが必要である。認証業務に取り組もうとする団体が安心して認証事業に参入でき、その後も持続的に認証事業を行い認証制度に関わり続けられることが重要であり、それが将来的に認証制度の普及・発展につながると考えられる。

（5）業界団体の活動との連携推進

業界によっては、業界独自の情報管理に関するガイドライン等を策定している事例も見られ、業界としての取組も認証制度に取り込んでいくことで、認証制度の活用が進むと考えられる。

今後、各業界団体との活動の連携をさらに進め、各々の基準や制度の目的、対象範囲、要求する事項等について、整合性を図る、あるいは違いをわかりやすく示す等行いつつ、本制度の特徴を明確にして打ち出すことで、双方の制度や仕組みが活用されることが望ましい。

令和4年度重要技術管理体制強化事業（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事業）
報告書

2023 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