令和5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に関する調査分析及び普及促進等事業）
調査報告書

令和6年2月29日

目次

第1章　調査の背景・目的

グローバルな競争が進む中、事業者の競争力の源泉たる技術等の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とともに事業活動を効率化し、事業者の競争力を維持、強化していくために重要な要素となっている。一方で、多くの事業者、特に中小事業者では知見、経験やリソースの不足もあり、事業活動のために漏えいを防止すべき重要な技術等の情報の特定や当該情報の管理体制の整備については、十分に進んでいないのが実情である。

このような状況に対応するため、国は、事業者が取り組むべき技術等の情報の管理に必要となる項目を示し、当該項目を満たしたことを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。）を平成30年から開始した。認証制度は、その普及を進めることにより、事業者、特に中小事業者の技術等の情報管理の理解醸成や、管理能力の底上げを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目的としている。

認証制度は開始から4年が経過し、その間の新型コロナウイルスの流行によるテレワークの普及、雇用の流動化やサイバー犯罪の高度化等の事業環境の変化により、情報セキュリティの重要性がますます高くなっている。このことを踏まえ、認証取得に当たって満たすべき基準（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。以下、「基準」という。）を見直す必要が生じている。また、認証制度の目的を実現するため、さらなる普及に向けた取組も継続する必要がある。本事業では令和4年度に検討し、経済産業省Webページに公開している基準の改定方針（案）に沿って具体的な基準の改定案を検討するとともに、認証制度をさらに普及させるための取組を行うことを目的とする。

第2章　実施内容・方法

1. 漏えいを防止するために必要な措置に関する基準の改定案の検討

告示として定めているこの基準について、目的、内容等において類似する他の情報管理認証制度（ISO／IEC27001に基づくISMS認証等）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、かつ技術等の情報管理に一定の実効性を確保する観点で必要な修正を検討し、基準の改定案を作成した。基準の改定案作成に当たっては、以下の点に留意して実施した。

図表 2-1 基準改定案作成の際の留意点

・基準の改定案は情報セキュリティに関する専門知識を持たない中小企業の担当者であってもその求める内容について理解でき、かつ、認証取得に当たっての第三者審査の際に必要以上の解釈の余地がない表現とすること
・基準の改定案は、認証を取得するために最低限満たすべき事項について明示された形とすること
・基準の改定案は、製造業・サービス業等の特定の業種を前提としたものとせず、一般的な表現を用いること
・必要に応じて作業方針の詳細について経済産業省担当者と協議のうえ作業を進めること

（1）基準の改定案等に係るヒアリング

①ヒアリング対象

基準の改定案の検討に当たり、知的財産管理や技術等の情報管理に係る有識者・関係者を対象としたヒアリングを実施した。

・東京情報デザイン専門職大学 松井 俊浩 教授
・情報セキュリティ大学院大学 藤本 正代 教授
・ITコーディネータ協会 松下 正夫 氏

②ヒアリング項目

図表 2-2 基準の改定案等に係るヒアリング項目

I.近年の事業環境の変化を踏まえた基準のあり方について
1）認証制度の実効性を担保するため、基準改定にあたり考慮しなければならない新たな脅威の有無
2）技術情報管理のために必要な要件のうち、特に重視しなければならない要件・取組
3）対策の具体例を示す際に配慮すべき事項
Ⅱ.中小企業が活用しやすい基準や本制度のあり方について
1）幅広い業界に向けに取り組んでもらうため、基準設定にあたり工夫すべき点
2）認証を取得するために最低限満たすべき取組の検討にあたり、参考とすべき制度・基準
Ⅲ. 普及が見込まれる業界や企業規模について
1）当制度へのニーズ、親和性が高いと考えられる業界
2）当制度の現行基準及び今後改定する基準の水準を満たす取組を行える企業体力のある業種・企業規模
Ⅳ. その他

③ヒアリング結果概要

1）認証制度の実効性を担保するため、基準改定にあたり考慮しなければならない新たな脅威の有無

- 技術情報の流出は大きな脅威ではあるが、個人情報等と異なり事案が顕在化していない。実際にそれで損をしていても感じられていないのではないだろうか。
- 海外の情報保護の動きが厳しくなっている点に注目している経営者が多い。一方で、自社

の情報をどう守り、経済安全保障を確保するのかという観点は不足している印象がある。

- テレワークの普及は非常に重要であるので、業務文書のインターネット共有やVPN接続が一般的になっていることを踏まえた方がいい。
- クラウドに関しては、はじめから使うことを想定した基準とした方がいい。クラウドを使用する場合、データセンターが海外にあることを考慮しておく必要がある。
- クラウドを使うことの危険性という点以外にも、使用するクラウドが認証をきちんととっているかということの確認も重要である。ファイル転送サービスなど認証を取っていないものも多く、いい加減なものを選ばないようにしないといけない。
- パスワードをきちんと自分で管理することも重要。マイクロソフトや Google などパスワードを預けているような状態になっている。また、パスワードを忘れた際にはメールが最後の砦となるが、そのメールが外部から見られる状態になっているとパスワードが筒抜けになってしまう。
- パスワードに関しては、各種の記号を使うようにとしているものもあるが、それは間違いで、NIST のガイドラインでは長いパスワードを使うように推奨している。また、パスワードを業者に渡すケースや、共有しているケースも見受けられる。加えて、PPAP 方式でのパスワードのメール送信も禁じた方がいい。
- 新たな脅威としては、生成系 AI による情報の捏造のリスクが考えられる。
- 外資系企業や中国系企業についてもリスクである。また、サーバがどこにあり、誰が管理しているのかも気にしておく必要がある。

2)技術情報管理のために必要な要件のうち、特に重視しなければならない要件・取組

- 人物のセキュリティクリアランスをしっかりやってもらいたい。セキュリティクリアランスをきちんとしているという姿勢を見せないと誰でも入ってきてしまう。人事的な雇用関係は長期的なものなので、簡単に解雇することはできない。
- ISMS認証を推奨するべきだと思う。日本はPマークの取得率が多いという事だがPマークは法人全てに対して、ISMSは部署を限定できる。そう考えれば、Pマークよりも容易く、この認証制度を取れば、ISMSにも手が届くといった宣伝をするとよいのではないか。
- 外注と委託契約の見直しを行うべき。1990 年代に WTO と国際入札制度の整備で外国企業を差別できなくなっているが、外国は一律ではない。輸出管理では区別していると思うが、輸入側でも区別すべきである。
- 情報漏えいする前の段階でキャッチできるとよい。Honeypot など事前に怪しい動きを検知する施策を重視することも一案である。
- 諸外国では情報が流出しないような対策は徹底的に対策を打っている。重要な技術情報を特定するという点が非常に大事であり、企業の認識を改める入り口になるだろう。その

内容は今後も維持していくべきではないか。

3)対策の具体例を示す際に配慮すべき事項

- 近年の研究開発やイノベーションは、外部と実施することも増えていることにも注意するべきだろう。取引が長い企業でも契約では明文化することなどが重要で、逆にそれによりオープンイノベーション等も進むのではないか。
- E メールの使用を減らし、組織外から閲覧されるリスクを軽減できる Teams などグループウェアを使う方がよい。
- 紙の使用を減らすことも重要である。デジタルであればログも残るため、とりあえずデジタル化からはじめようと促すのがよいのではないか。
- 情報漏えいなどの事例を集めた後、国として対策を考える必要がある。警察に事例を出してしまうと事件となってしまい、対策を考えるべき組織に情報が共有されない。もう少し次の対策を考えるための組織に対して情報共有ができるような窓口を周知したほうがよいと思う。

4)幅広い業界に向けに取り組んでもらうため、基準設定にあたり工夫すべき点

- 壁の厚さなどの基準は変えていくべきだろう。
- 将来的に ISMS 認証の取得を目指すのであれば、文章の形式も基本方針、基本規定、実施要領という ISMS の構成に合わせた方がいい。
- 現状の内容は防衛産業に求めている基準に近いように感じるので、対象の情報を区分する等のような現実的な手法にすべきだろう。細かくレベル分けをするのは大変という印象を持った。
- 物理的な管理・対策が導入されると、従業員の目に見えるようになり、従業員の意識が変わる。決定的な打ち手ではないが、従業員の意識の改善には繋がる。
- 特別防衛機密のようなものではなくても、先端技術も守られるべきものである。同じような文脈で考える必要があることを意識させるべき。
- 制度の普及を考えると、中小企業団体等からのアプローチも考えられるが、商工会・商工会議所は個社に働きかけることが難しく、動きが鈍い印象もある。業界団体に働きかけて中小企業を動かしていかないと、普及は難しいのではないか。

5)認証を取得するために最低限満たすべき取組の検討にあたり、参考とすべき制度・基準

- ISO30000 がリスクマネジメント全般の基準である。また、CSMS などは ISMS よりも小さい企業を対象としており、製造業に向いていると思う。また、個人情報保護の観点であれば、GDPR や EU の AI 規制法も参考になるのではないか。

- セキュリティクリアランスの制度についてはアメリカ政府のものが参考になるのではないか。
- ISMS の周辺のガイドラインは参考になるが、分かりやすさという観点では中小企業に合ったレベルではないと思う。総務省の「国民のための情報セキュリティサイト」などは専門用語が使われておらず、分かりやすい。
- どういった企業規模をターゲットにするか次第だろう。数百人程度の規模であれば中小企業であっても IT セキュリティの話は一定数、分かる人がいるはずである。
- ターゲットは研究部門や開発部門の人を想定してはどうか。サイバーセキュリティの話を主に議論を進めてしまうと、制度の軸がぶれてしまう。

6）当制度へのニーズ、親和性が高いと考えられる業界

- 重要な企業として半導体企業や電池企業などは狙われやすい。半導体関連の企業は大企業かもしれないが、材料や素材を提供している下請けの企業が重要であり、そのあたりの中小企業は注視する必要がある。
- 半導体の製造装置はリモート制御されている。制御システムのリモートメンテナンスなどの専用システムのセキュリティも気になるところである。
- 今回の対象とは異なるかもしれないが、公的機関の認証取得も重要である。
- 経営者は、親会社や主要取引先に言われたことを非常に気にするのでそういった観点から、サプライチェーン上の安全保障を気にしており、繋がりが強い業界が当面のターゲットになるのではないか。
- 自工会は、昨年度の研究成果として、「自動車産業サプライチェーンへのサイバーセキュリティ推進活動集計データ最終結果公表」を発表しているが、業界内でのセキュリティ対策実施のレベルも差が生じており、企業規模が小さい先への働きかけに特に苦慮していると聞いている。自工会と連携した活動も行えると望ましいだろう。自工会以外にも似たニーズを持つ業界団体はあると思われるため、そうした先の掘り起こしも検討してほしい。
- 業界ではないが、中小企業は、経営のキーマンが単独で意思決定できる。大企業ほど意思決定にロジックを必要としない中小企業の経営のキーマンに対し、講演等で説明しやすいような資料を作ることも重要だろう。
- 大きな事故や事件があると導入の契機になりやすいことから、営業秘密を売ってしまったといった判例などを参考に業界を検討するのも普及に向けては1つの視点となり得る。

7）当制度の現行基準及び今後改定する基準の水準を満たす取組を行える企業体力のある業種・企業規模

- ISMS は情報システム関係の部署がターゲットになるが、本制度に関しては、技術情報は研究部門や品質管理の部門が実際のターゲットになる。そういった部門が、保有する技術

が利益の源泉であると自覚・意識をする必要性があるだろう。

8)その他

- ISMS の導入時には、情報システム安全対策実施事業所認定制度(通称:安対制度)からの移行もあり一斉に導入に繋がった背景がある。他の普及している制度については、時期やタイミング等が恵まれたために普及したケースも多く、本制度のようなニーズ・必要性が高い一方で中小企業があまり取り組めていないのも仕方ない。
- 中小企業からすれば、お金を出すというのはハードルの高さに繋がりかねないのは間違いない。
- サイバーセキュリティに関してはISACのような組織により他社との情報共有がされている。
- セキュリティ全般に関して、関心を持ってもらうことにはみなさん苦労している。現場の人たちはセキュリティの重要性を理解しているが経営層が理解していないことが多い。
- 今は中国に抜かれてしまったが、日本も ISMS を取得する事業者数はとても多かった。日本人は認証における興味が強いと思うためやり方次第で普及するのではないか。
- 審査を通過するためには、情報管理に関する教育計画の体制が構築されていることが必要であるが、認証取得前の段階で中小企業がそこまで構築されていることはまれである。
- 研修等に関する運営委員会を、従業員 20～30 名程度の企業だと誰が取り仕切るのかという問題もある。
- ある大手企業が、取引先にセキュリティ対策の実施を求める際のチェックシートを作成し、配布していると聞いている。中小企業で複数の大手企業と取引を行っている際には、各社から異なるチェックシートが配布され、対応に苦慮するという話も聞いている。

（2）認証制度の在り方・活用の可能性等に係るヒアリング

①ヒアリング対象

認証制度の在り方・活用の可能性等を検討するため、認証制度の普及が期待される業界団体・業界に属する事業者等に対するヒアリングを実施した。

・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
・一般社団法人　電子情報技術産業協会　サイバー・フィジカル・セキュリティ専門委員会
・全国中小企業団体中央会
・独立行政法人中小企業基盤整備機構
・全国商工会連合会

②ヒアリング項目

図表 2-3　認証制度の在り方・活用の可能性等に係るヒアリング項目

Ⅰ.貴団体・貴団体の加盟企業における情報セキュリティ対策の取組状況について
1）貴団体の加盟企業の特徴や、貴団体における情報セキュリティ対策・普及啓発について特に力を入れて取り組んでいる施策
2）貴団体に加盟する企業間の取引、貴団体加盟企業の取引先企業から、情報セキュリティに対する要請の増加の有無
3）貴団体加盟企業における情報セキュリティに係る認証の取得状況
4）貴団体が策定している加盟企業向けのセキュリティガイドライン及び参考とした参考とした認証や他のガイドライン等の有無
5）会員企業が情報セキュリティ対策への投資を行う際、業界団体として支援する取組の有無
Ⅱ.貴団体が活用しやすい基準や本制度のあり方について
1）会員企業が本認証を取得するにあたって、障壁となる点
2）本制度の取得を会員企業に促すにあたって訴求が必要なメリット
Ⅲ. その他
1）貴団体において、重点的に普及を進める制度やお取り組み等決定方法
2）加盟団体・企業等へ制度の普及・案内を進める際に、特に喜ばれる支援メニュー
3）過去に補助金の加点要件になった・加点の点数が増えたことにより、普及した制度の有無

③ヒアリング結果概要

1）貴団体の加盟企業の特徴や、貴団体における情報セキュリティ対策・普及啓発について特に力を入れて取り組んでいる施策

（団体A）

・業界セキュリティガイドラインの普及啓発を軸として、加盟企業を含む産業全体を対象としてセキュリティ対策に取り組んでいる。ガイドラインの普及という観点では、業界の商流に沿って、サプライチェーンの上流から広めていって欲しいとお願いしている。多くの企業は自社にとって重要な部分から取組に着手しているようであるため、会社ごとに若干の個人差はある。

・ガイドラインの順守状況について、商流を経るにつれて普及効果は弱まっていると感じる。特に企業規模が小さくなると、自社のことで精一杯で、仕入れ先までアプローチするといったことはできていない印象である。

（団体B）

・取組状況の自己評価を実施している企業でも、個々の会社を見ていくと自己評価ほど実際は順守できていないといったケースはあるが、これらが一概に悪いとは認識しておらず、毎年取組のレベルを上げていけば良いと思っている。今年度はガイドラインの内容を説明し、自己評価に取り組むことを促す説明会を開始した。この他にも、ガイドライン読者の負担軽減のための「ガイドラインの解説書」の掲載やガイドラインに関する疑問を意見交換形式で解決することを目指す「よろず相談会」の実施、セキュリティ全般への啓蒙活動・意識啓発・基礎知識定着を目指したウェビナーの実施等行っている。

（団体C）

・経産省が公表しているガイドラインについて、中小企業が取り組めるように、物語や事例などを加えて分かりやすくしたガイドラインの作成を行っている。

・中小企業にはセキュリティの専門家、ネットワークの専門家が少ない、あるいはいないという状況であることを踏まえ、経産省のガイドラインだけでは分かりにくい点を補足しており、中小工場でセキュリティ構築を担当する者や、中小企業に製造委託する委託者、セキュリティ構築の委託を受けるコンサルタント等に使用いただきたいと考えている。

・具体的な内容としては、脅威の洗い出しやセキュリティの対策の具体的な方法や内容などが、専門家ではないと分からないような書きぶりであるため、具体的に何をすればよいか分かるような内容を加えている。

（団体D）

・業種にもよるが、自動車産業、航空部品産業、デジタル産業の企業は情報セキュリティについ

て重要と感じているが、中小企業の3割を占める食料品産業の企業はあまり関心がない。
・毎年、重点課題を設定し、その課題対応の一環として情報セキュリティ対策に取り組んでいただくようにお願いすることがある。情報セキュリティ対策をお願いする際は、業界の特性に応じて施策を広報することが一般的であるため、業種別にターゲットを絞り、その業界の言葉を使い、自分たちの業界にとって重要だとアプローチすることが必要となる。制度普及の際には、業界向けの用語でわかりやすく伝えるようにするといった工夫を行っている。力を入れたい業界に合わせてかみ砕いた案内を出すことができれば、情報を受け取る中小企業の心理的ハードルが下がると考え、業界毎に関係者が集まる会議などで自分たちの業界事として腑に落ちる事例を出して案内することを意識している。

（団体E）
・中小企業は絶対にやらなければいけないものでないと、後回しになる傾向があると認識している。そのため、中小企業はやった方がいいというレベル感では行動を促すインセンティブにならない。特に、認証取得に金銭の支払いが発生するとなると、なおさらその傾向が強くなる。
・中小企業におけるカーボンニュートラルの普及活動も行っているが、実例として取引を打ち切られた等の実害がなければ、なかなか取り組んでもらえない。カーボンニュートラルや情報セキュリティは、最終的にはどの中小企業も取り組まなければいけないものであり、早期に取り組めばメリットがあり、対応が遅れると義務的にやらされることになるため、どうせやらなければならないのならメリットが得られる早期に取り組んで欲しいと思っている。

（団体F）
・団体として情報セキュリティについて力を入れていることはない。事業所からの要望で助成金や補助金等の攻めの投資について補助しているが、守備面に使える補助金は少ないためである。
・情報セキュリティ分野でも積極的に活用できる補助金について施策として周知してほしいという要望はある。経営指導員がIT導入補助金を紹介して対応するが、対策ソフトを入れるくらいまでであり、マネジメント体制を整えたり、管理規定を作成したりするまではいかない。経営指導員に情報セキュリティ分野の情報や専門家派遣に繋げる知識が入っていれば、専門家への相談まで繋がる可能性はある。

2）貴団体に加盟する企業間の取引、貴団体加盟企業の取引先企業から、情報セキュリティに対する要請の増加の有無

（団体A）
・加盟企業の取引先を含め強化の要請はあまりない。この背景には、取引先の小規模企業が情

報セキュリティを徹底するのは難しいだろうと考え、声を上げていない側面もあると思う。
・取引先の要望については、商流に沿って普及させているがそれ以上の取組はない。

（団体C）
・取引先の要望については特にしていないが、サプライチェーン全体のセキュリティ構築が不可欠な時代でもあるので、各サプライヤーが自ら考えてセキュリティ向上に向けて行動を取れるよう、業界ガイドラインの作成に至った。

3）貴団体加盟企業における情報セキュリティに係る認証の取得状況

（団体A）
・「ISMS等の取得を行っていれば当団体のガイドラインは満たしているのか」といった質問を受けることはあるが、正確に各企業の認証等の取得状況を把握していない。また、その質問に対しては、他の認証に加えて当団体ガイドラインを遵守していただくようお願いしている。お願いの仕方として、他の認証とのダブルスタンダードになる部分が一部あるかもしれないが、業界全体としてのレベルアップや負荷低減を目指している取組であるため、是非ご協力いただけるようにとお願いをし、理解してもらうようにしている。

（団体B）
・ISMS、Pマークといった他のサイバーセキュリティに関する認証について、どんな認証をどの程度の企業が取得しているかは把握しておらず、調査も行っていない。

（団体C）
・ISMS、Pマークといった他のサイバーセキュリティに関する認証について、どんな認証をどの程度の企業が取得しているかは把握していない。ただし、総務部では何かアンケート等をしている可能性はゼロではない。

4）貴団体が策定している加盟企業向けのセキュリティガイドライン及び参考とした認証や他のガイドライン等の有無

（団体A）
・業界セキュリティガイドラインは「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（以下CPSF）」を中核に、「NIST Cybersecurity Framework v1.1」、「ISO 27001」、「IPA 中小企業の情報セキュリティ対策ガイドライン」等をベンチマークとして作成している。
・選定理由としては、当団体ガイドラインの作成がCPSFの策定直後に行われ、当時の最新のガイドラインであり、公的機関が国際標準を参照して作成していることもあり、中核のベンチ

マークとした。これに加えて、一般的に当該分野でメジャーなガイドライン・認証や、業界内で既に浸透しているガイドライン・認証をベンチマークに加えた。
・選定の段階で、特定の業界を意識したということはなく、CPSFを中心にガイドライン・認証等を参照し、その中で特に本産業にとって重要なもの抽出した。その当時の取組みのレベルを基準として、どこまで今後当てはめていけるかを想像しながらガイドラインを作成した。
・業界セキュリティガイドラインの各レベルに特定のガイドライン・認証の内容が対応しているという事は基本的にはない。一部、「IPA 中小企業の情報セキュリティ対策ガイドライン」の自社診断のための25項目を参考にしているといったところはあるが、正確に対応しているものがある訳ではない。

（団体C）
・CC（ISO/IEC 15408）等を参考にして作成した。

5）会員企業が情報セキュリティ対策への投資を行う際、業界団体として支援する取組の有無

（団体A）
・加盟企業の取り組み内容を正確に把握できている訳ではないが、当団体として支援している取組はない。基本的にはお願いベースの取組みであり、直接的な金銭支援というよりは、セミナー等の普及啓発に資する支援に力を入れている。

（団体B）
・当団体では金銭的・実務的な支援はほとんどないが、サイバーセキュリティ事故や情報漏洩に起因して発生する損害に対応するために、「団体サイバー保険制度」を2021年4月から導入している。本制度は、団体というスケールメリットを活かした割安な保険水準を設定するとともに、付帯サービスとして事故発生時の対応を専門家がワンストップで支援するサービスを利用できる。引受保険会社がセミナー等で会員に案内している。加入率は把握していない。

（団体C）
・金銭的、実務的な支援はほとんどない。

（団体D）
・当団体には相談窓口があり、相談内容により専門家派遣事業に登録し、専門家に対応をお願いしてもらっている。昨今多いITセキュリティ関連の相談についても、IPA（独立行政法人情報処理推進機構）の専門家に来てもらうこともある。また、毎年当団体の職員もIPAの講習を受けている。
・中小企業は認証取得というより、対応すべき内容が分からないので専門家に聞きたいという

ケースが多い。その際に専門家から優先順位をつけてもらい、必須で対応すべき事項に対応するというのが現状である。

（団体E）
・地域の支援機関や金融機関に周知して、そこを起点にハブとして普及に係る取組を広げてもらっているため、月1回程度で各地域本部がそれぞれの地域で、様々な研修会を行っている。また、本部で全国対象にした、オンライン勉強会も行っている。この研修会、勉強会の1枠として、情報セキュリティがテーマの会を実施したことがある。

（団体F）
・研修会、勉強会について、経産省の担当者が本制度に関するセミナーを実施するための枠を割くことは検討できる。どのようなセミナーを実施するのかのイメージが分かる資料があれば、担当者に繋ぎやすくなる。

6）会員企業が本認証を取得するにあたって、障壁となる点

（団体A）
・現状は基準の認知度が低いため障壁となる課題にたどり着いていないのではないか。実際に、当団体では本認証制度との関係を問われることはない。そのため、本認証制度に取り組みたいと思うきっかけがないことが課題と感じており、金銭的補助やインセンティブ等の検討が必要なのではないか。
・しかしインセンティブの問題よりも、ガイドライン・認証等と本認証制度で重複している部分が明確になっていないため、手間だけ増えるのではないかと思われている。その上で、特段のインセンティブもないとなると普及は難しいと思う。
・当団体ガイドラインも明確なインセンティブがある訳ではないが、業界で過去に起きたセキュリティインシデント事例を踏まえて具体的なリスクを提示することにより、優先順位の高い経営問題とであると認識してもらい普及を促進させた。そのため、インセンティブというよりはリスクの重大さをアピール材料とした。
・当団体会員企業でボトルネックとなるのは人的リソース、金銭的リソースである。

（団体C）
・サプライチェーン全体のセキュリティ水準を上げないといけない時代である一方で、サプライヤーの意識が低いというのが難点である。また、認証制度は国内企業を想定しているようだが、サプライヤーは海外にも多く存在している。その点も考慮すべきではないかと思う。
・IPAのサイバーセキュリティお助け隊が5万円であるにもかかわらず、その利用は不十分な状況である。本制度の取得にかかる数十万円をどの程度の中小企業が負担できるのか、必要な

負担として中小企業の経営者が意識できているのかは懸念がある。
・産業界において、工場のセキュリティ向上は大きな課題であるが、工場にはセキュリティやネットワークの専門家はほとんどいないと考える必要があるのではないか。

7）本制度の取得を会員企業に促すにあたって訴求が必要なメリット

（団体A）
・本認証と業界ガイドラインの対応関係が明確になり、片方の認証をクリアすれば、もう片方の特定項目をクリアできるという立付けになれば、認証取得におけるハードルが下がり、本認証制度を活用するメリットが提示しやすいのではないか。似たようなガイドラインの対応関係の整備はIPAとも行っている。
・本制度は補助金の加点要素になっているため、認証取得のハードルが下がれば、金銭的メリットも提示できると思う。サイバーセキュリティ対策をしたいが、金銭面がネックになって取り組めていない企業は多い。

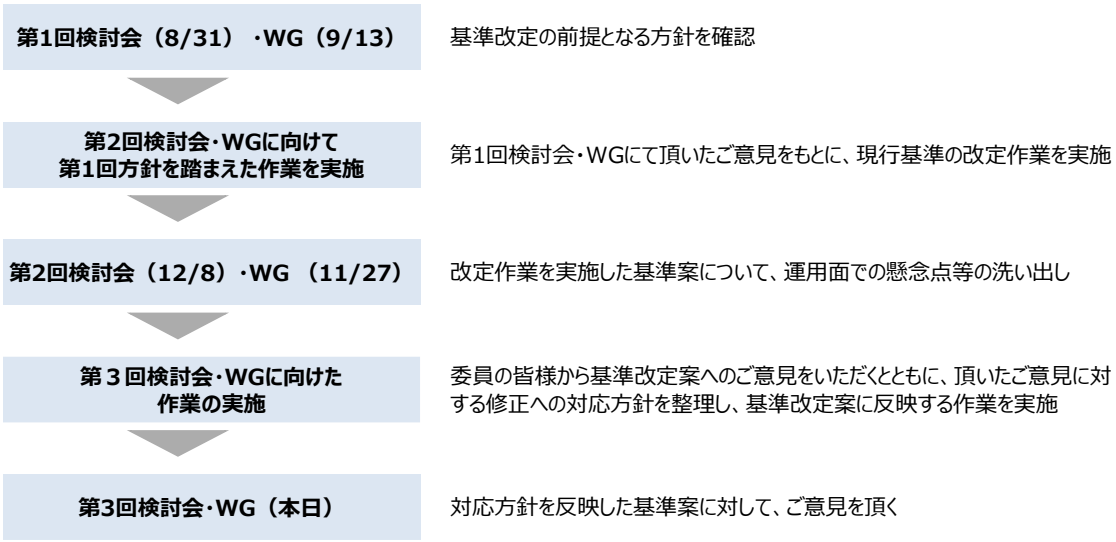
（団体B）
・よろず説明会、解説書等では「IPAのガイドラインのこの部分を使うと楽です」といった説明をしていることが多いため、本制度とガイドラインの対応関係が明確になれば、IPAのガイドラインと同様に業界で普及することはできると思う。
・本制度も段階分けして取得可能な立付けにすれば、業界としては使いやすいものとなる。

（団体C）
・第三者認定の国の制度という点は素晴らしい。こういった制度を構築するのは容易ではない。だからこそ、本当に制度を活用してほしいターゲットは誰なのか、いつまでに何件の認証を取得してほしいのか、といった活用全体の目標を整理していくことから始めるべきだろう。

④基準改定案作成の流れ

基準改定案の作成は以下のフローにより実施した。

図表 2-4 基準改定案作成フロー



⑤基準改定案

昨年度までの議論や、各業界団体・有識者へのヒアリングの結果も踏まえ、各章の柱書に加え、必ず達成することを求める「義務項目」と、「義務項目」を達成するための手段である「推奨項目」により構成する形で整理を行い、基準改定に向けた検討案（基準改定案）を作成した。次頁以降、本年度事業で作成した基準改定案を記載する。

第Ⅰ章 共通事項

項目番号	内容(案)
Ⅰ	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。)の漏えいを防止するために必要な措置を講ずる。

第1. 情報セキュリティ対応方針の策定及び組織内への周知

項目番号	内容(案)
第１	事業者は、自社の情報セキュリティ対応方針の策定・周知を実施する。
1	事業者は、自社の情報セキュリティ対応方針を策定し、文書化する。
2	事業者は、情報セキュリティ対応方針を社内で/組織内で容易に確認できる状態にする。
3	事業者は、定常的に、かつ、情報セキュリティ対応方針の改正時に周知する。
4	事業者は、自社の守秘義務のルールを規定し守らせるため、以下の事項を実施する。 *（1）自社の守秘義務を策定し、文書化すること* *（2）入社時あるいは社外要員の受け入れ時に守秘義務を説明すること* *（3）退職もしくは期間満了時に会社の機密情報を持ち出さないこと*
5	事業者は、業務で利用する情報機器について、個人所有機器(BYOD)を含めた利用ルールを規定し、周知する。
6	事業者は、情報セキュリティに関する法令を守るための社内ルールを策定し、教育・周知する。
7	事業者は、法令の変更、社会情勢の変化、契約上の要求事項や組織の状況変化等に伴い、情報セキュリティに関する社内ルールを適宜見直す。

第2.　適切な管理をする必要がある技術等情報の特定・識別

項目番号	内容(案)
第２	事業者はその経営層が関与し、技術等情報のうちこの告示に掲げる措置の対象とする技術等情報(以下「管理対象情報」という。)のうち、以下の(1)に該当するものを「高い機密区分」の管理対象情報として、「高い機密区分」に準じる(2)に該当又は相当するものをその他の管理対象情報として特定する。 (1)「高い機密区分」の管理対象情報 一　それ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技術等情報 二　それ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技術等情報 三　それ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技術等情報 四　他者から契約等に基づき預けられたで情報あること等により、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技術等情報 (2)その他の管理対象情報 一「高い機密区分」の技術等情報への攻撃の手掛かりを与える情報 二　それが漏えい・改ざん・使用不可になった場合に、自らの競争力への影響が懸念されるため、保護することが望ましい技術等情報 また、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。
1	事業者は、高い機密区分の管理対象情報を一覧化し、特定した当該管理対象情報の態様、管理責任者名、部署名、保管場所、保管期限、開示先、連絡先等を記録する。
2	事業者は、管理対象情報が電子情報の場合、ファイル名、文書ヘッダー、文書の透かし、フォルダ名、ファイル属性情報等に管理対象情報であることを記録する。
3	事業者は、管理対象情報が試作品又は製造装置等の場合、当該物そのもの又はその保管容器に表示する。
4	事業者は、管理対象情報が紙情報の場合、表紙等の適切な場所に管理対象情報であることを表示する
5	事業者は、管理対象情報を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。

第3.　管理対象情報の適切な管理

項目番号	内容(案)
第 3	事業者は、管理対象情報の機密区分を設定・把握し、その機密区分に応じて情報を管理する。また、会社が保有する情報機器及び機器を構成する OS やソフトウェアといった IT 資産の情報(バージョン情報、管理責任者、管理部門、設置場所等)を適切に管理する。
1	事業者は、機密区分に応じた情報の管理ルールを定める。なお、その他の管理対象情報については必要に応じて更に区分することができる。
2	事業者は、管理対象情報を機密区分及び重要度に応じた管理ルールに沿って管理する。
3	事業者は、機密区分及び重要度に応じた IT 資産の管理ルールを定める。
4	事業者は、IT 資産の情報 (バージョン情報、管理責任者、管理部門、設置場所等)について、一覧を作成する。

第4.　管理対象情報の管理体制の整備

項目番号	内容(案)
第 4	事業者は、平時の情報セキュリティリスクを管理する体制を整備し、事故発生に至らないよう、情報収集と共有を行う。体制整備の一環として、管理対象情報の管理に関する責任を有する者(以下「管理責任者」という。)を選任する。 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。
1	事業者は、情報セキュリティを統括する役員(CISO 等)や情報セキュリティ担当部署を選任し、平時の管理体制と責任と役割を明確化する。
2	事業者は、社内での情報収集と共有のための連絡先リストを整備する。
3	事業者は、定期的又は必要に応じて、管理体制を見直す。
4	事業者は、サイバー攻撃や情報漏えいの新たな手口を知り、対策を社内部署へ共有し、サイバー攻撃や予兆を監視、分析をする体制を整備する。
5	事業者は、方針、対策又はマニュアルを適切、有効かつ妥当なものに維持する。
6	事業者は、あらかじめ、自らの事業継続計画、コンティンジェンシープラン等に管理対象情報の漏えいの事故等を位置付け、当該漏えいの事故等が発生した場合の影響の最小化と事業継続のための措置を決定する。
7	事業者は、管理対象情報の漏えい等の事故等に係る対応により得られた教訓を事業継続計画、コンティンジェンシープラン等に反映させ、継続的に見直す。
8	管理責任者は、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訓練を行う。
9	管理責任者は、保管容器若しく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。
10	管理責任者は、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を行う。
11	管理責任者は、その管理対象情報が複数の事業部門等にまたがるものである場合には、社内規則等への規定又は社内における掲示により、誰が管理責任者であり、どのような責任を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するための取組を行う。
12	管理責任者は、方針、対策又はマニュアルが作成(変更を含む。)された場合はその承認をすることや、管理対象情報の適切な管理の責任の明確化、自らの関与の明示等により、管理対象情報の適切な管理を確立するための取組を行う。

第5.　事故発生時(情報セキュリティ事件・事故)の対応体制の整備

項目番号	内容(案)
第 5	事業者は、情報セキュリティ事件・事故発生時の対応体制及び対応手順を整備し、その責任者を明確にする。
1	事業者は、情報セキュリティ事件・事故の基準や社内外組織との連絡先、連絡ルートを明確にする。
2	事業者は、情報セキュリティ事件・事故発生時の連絡体制と報告のための手順を明確にする。
3	事業者は、情報セキュリティ事象に関連する証拠を特定、収集、取得及び保存する。
4	事業者は、情報セキュリティ事件・事故発生時に、事故の概要、影響及び対応内容の記録を残す。
5	事業者は、定期的又は必要に応じて、事故発生時の体制を見直す。
6	事業者は、マルウェア感染時の対応手順を定める。
7	事業者は、1～6に掲げる事項を文書化した手順に沿って対応する。

第6.　従業員への教育

項目番号	内容(案)
第 6	事業者は、従業員として注意すべきこと及び情報セキュリティの基礎に関する社内教育を行う。
1	事業者は、電子メールのマルウェア感染に関する社内への教育を行う。
2	事業者は、インターネットへの接続に関する社内への教育を行う。
3	事業者は、機密区分に応じた情報の取り扱いに関する教育を行う。
4	事業者は、情報セキュリティ事件・事故発生時の対応について教育・訓練を実施する。
5	事業者は、教育・訓練の内容を必要に応じて見直す。

第7.　リスク対応

項目番号	内容(案)
第 7	事業者は、自社内及び業務委託先の情報セキュリティリスクへの対策を実施する。
1	事業者は、管理対象情報において「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影響や被害を特定する。
2	管理責任者は、必要に応じて経営層へ業務影響及び対策を報告し、セキュリティ業務に関与している社内部署と共有する。
3	事業者は、業務影響への対策を、策定された計画に沿って実施する。
4	事業者は、情報セキュリティの脅威に関連する情報を収集及び分析する。
5	事業者は、利用中の情報システムの技術的ぜい弱性に関する情報を継続的に収集する。

第8.　外部情報システムの利用における安全性と信頼性の確保

項目番号	内容(案)
第 8	事業者は、関係団体(サプライヤー等を含む。)との関係において、 自社の通信ネットワーク構成を把握し、他団体との連携状態やデータの流れを監視する。
1	事業者は、自社の機器が接続している外部情報システム(関係団体の情報システム・クラウドサービス・外部情報サービス等)の利用ルールを定める。
2	事業者は、利用している外部情報システムを一覧化する。
3	事業者は、外部情報システムの一覧を定期的又は必要に応じて見直す。

第9.　サプライチェーン上で発生する情報セキュリティ要件の明確化及び他者から預けられた管理対象情報の管理方針の策定

項目番号	内容(案)
第9	管理責任者は、取引先毎に、取引で取り交わされる技術等情報及び取引に利用している手段を把握し、サプライチェーン上で発生する情報セキュリティ要件を明確化する。また、他者から預けられた管理対象情報がある場合は、当該他者からの意見を聞いて必要なものを決定する。
1	管理責任者は、他者との間で、技術等情報の取り扱い方法を明確化する。
2	管理責任者は、情報セキュリティ事件・事故時の他者との役割と責任を明確化する。
3	管理責任者は、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)を一覧化する。
4	管理責任者は、管理対象情報の漏えい防止に資する措置の実施状況を記録し、当該記録の保管期間を定め、定期的に確認する。
5	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、当該他者からの意見に基づき適切な措置を講ずる。
6	管理責任者は、他者から預けられた管理対象情報の一覧を定期的又は必要に応じて見直す。

第10.　管理対象情報の管理簿の作成等及び保管

項目番号	内容(案)
第 10	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。
1	管理責任者は、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。
2	管理責任者は、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。
3	管理責任者は、他者から預けられた管理対象情報の状況を管理するため、他者毎に管理簿を作成し、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。

第11.　管理対象情報の内容の伝達及び複製の制限

項目番号	内容(案)
第 11	管理責任者は、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伝えること及び閲覧させることをいう。)及び複製の対象を、アクセス権限を付与した者(以下「アクセス権者」という。)に限る。
1	アクセス権者は、他の従業員等(管理対象情報の他のアクセス権者を除く。第十一2において同じ。)に対して管理対象情報の内容の伝達又は複製をしようとする場合には、管理責任者の承認を得る。
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又は複製についての承認を求められた場合には、真に必要なものか否かの確認を行い、伝達又は複製の範囲を可能な限り限定した上で、これを認める。
3	管理責任者は、管理対象情報の内容の伝達及び複製について、第十の管理簿に記録する。
4	管理責任者は、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、可搬式記録媒体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、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定める。
5	管理責任者は、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。

第12.　管理対象情報の適切な廃棄

項目番号	内容(案)
第 12	事業者は、管理対象情報の廃棄については、その管理対象情報の態様に応じ、復元不可能な方法により廃棄をする。
1	事業者は、紙情報又は試作品等である管理対象情報を廃棄する場合には、シュレッダーにより裁断する等、復元できない状態にする。
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、復元できない状態にする。
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、データを消去した上で、当該可搬式記録媒体を物理的に破壊する等、復元できない状態にする。

第Ⅱ章　管理対象情報への人的アクセスの制限

項目番号	内容(案)
Ⅱ	事業者は、管理対象情報への人的アクセスの制限を実施する。

第1.アクセス権の設定

項目番号	内容(案)
第１	事業者は、管理対象情報へのアクセス権の付与においては、権限の付与が見込まれる者についてのレビューをし、統一的な判断基準(考え方)の下で、以下の事項を考慮し行う。 (1)Need to Know の原則に照らし、グローバル競争が進む中での国外へ技術等情報の流出リスク等を考慮しつつ、必要最小限の範囲となっているか否か (2)事業者内部における情報の取扱いに係る社内規程への違反履歴 (3)その従業員等の退職、研修員の派遣元への復帰等近い将来において管理対象情報を保有する事業者の直接の管理の対象から外れる可能性
1	事業者は、全ての管理対象情報へのアクセス権の設定を一人の管理責任者が行っている場合には、当該アクセス権の設定に係るレビューを当該管理責任者の上司等の他の者に行わせる。
2	事業者は、管理責任者以外の者がアクセス権の設定を行っているときは、当該管理責任者以外の者に対し、管理責任者にアクセス権の設定をされた者の氏名等必要な事項を連絡させる。
3	管理責任者は、アクセス権者以外の者による管理対象情報へのアクセス(立入制限区域(壁その他の物理的な境界で他の区域と区分することができる区域であってその区域が他の区域と接触する全ての入退室口を施錠することができる区域。以下同じ。)にある管理対象情報である製造設備の見学のように一時的なアクセスを含む。)について、 Need to Know の原則を満たすものであるかを評価する。
4	事業者は、管理対象情報にアクセスするアクセス権者以外の者から、その訪問により得られた管理対象情報を第三者等に開示しないこと等を誓約する書面を得る。
5	事業者は、アクセス権者以外の者が管理対象情報へアクセスする際は、アクセス権者が立ち会う等、管理対象情報を保護するために適切な措置を講ずる。

第2.アクセス権の管理

項目番号	内容(案)
第 2	管理責任者は、アクセス権者の管理を行う。
1	管理責任者は、アクセス権者のみが管理対象情報を取り扱い得ることを明らかにする。
2	管理責任者は、アクセス権者の従事する管理対象情報に係る業務の内容等に応じ、当該アクセス権者のアクセスの範囲を限定し、その責任を明確にする。
3	管理責任者は、人の異動に伴うアクセス権の管理ルールを定める。
4	管理責任者は、アクセス権の管理を確実なものとするため、アクセス権者の氏名、役職、アクセス権の設定年月日、訓練の受講の状況等アクセス権の範囲及びアクセス権者の状況を記録した管理簿を作成し、合理的な期間保管する。
5	管理責任者は、管理ルールに沿ってアクセス権の発行、変更、無効化及び削除を実施する。
6	管理責任者は、アクセス権の見直しを定期的又は必要に応じて実施する。
7	事業者は、アクセス権者に対し、訓練による周知並びにその後の定期的な上司からの説明等により、アクセス権者としての責任を明確に認識させる。
8	事業者は、アクセス権者が定められた手順を守らない場合、アクセス権者のアクセス権を失効させる。

第3.アクセス権者に対する秘密保持等に関する担保

項目番号	内容(案)
第 3	事業者は、アクセス権者としての責任を明確にするため、アクセス権者から、以下の事項のうち必要なものを確保し、秘密保持に係る誓約書の取得又は秘密保持契約を締結する等の措置を取る。 (1) 第三者に対する守秘義務を厳守すること。 (2) アクセス権の設定の解除の後(退職後も含む。)も、当該アクセス権が設定されている間に知り得た管理対象情報について、公知になったものを除き、不正に開示し、又は使用しないこと。 (3) マニュアルその他の事業者内部における情報の取扱いに係る社内規程を遵守すること。 (4) 管理対象情報の漏えいにつがなり得る事象等を発見した場合に管理責任者等事業者が指定した者に報告を行うとともに、管理対象情報の漏えいの事故等が発生した場合に措置を講ずること。 (5) 管理対象情報へのアクセスのログ等をアクセス権の設定を行った者等から確認されること。 (6) 管理対象情報に接する必要がなくなった場合は、速やかに、返却すること等所要の対応が求められること。
1	事業者又は管理責任者は、誓約書等の記載事項の定期的な確認を実施する。
2	事業者又は管理責任者は、情報の適切な管理に係る状況の変化、管理対象情報の漏えいの事故等が発生した場合は、その都度、誓約書等の内容の見直しを実施し、必要に応じて、変更した誓約書等によりアクセス権者の責任を確認する。
3	事業者は、第三に掲げる事項のうち誓約書等の記載事項として含まれていないものについて、アクセス権者に理解させるため、定期的に上司からの説明等の取組を行う。
4	事業者は、アクセス権者を含めた従業員等がマニュアルに違反し、管理対象情報を漏えいさせ、又は目的外に利用する等事業者内部において情報の取扱いに係る不正をした場合、当該従業員等を解雇等の懲戒処分とすることについて就業規則等に定めるとともに、刑事告発や民事訴訟の法的手続に関する規程を社内規程に定める。
5	事業者は、アクセス権者を含めた従業員等が管理対象情報を漏えいさせ、又は目的外に利用する等事業者内部において情報の取扱いに係る不正をした場合には、当該不正の事例及びその処分の内容を全ての従業員等に周知する。

第Ⅲ章　管理対象情報が物である場合のアクセス制限等

項目番号	内容（案）
Ⅲ	事業者は、管理対象情報が物である場合には、管理対象情報への物理的アクセスを制限する。

第1.管理対象情報を保管・持ち出す場所の設定並びに保管容器及び立入制限区域の鍵等の管理

項目番号	内容(案)
第１	管理責任者は、保管容器及び立入制限区域の鍵、警備の体制を適切に管理する。また、事業者は、管理対象情報及び管理対象情報が保管された保管容器を、立入制限区域に設置するとともに、持ち出す場所についても制限する。
1	管理責任者は、鍵の貸出、共有を管理するための管理簿を作成し、合理的な期間保管する。
2	管理責任者は、施錠することができる保管容器を用いている場合にあっては、当該保管容器の解錠手段を、以下のような事象が生じた都度、変更する。 （1）保管容器の購入後、使用する場所に備え付け、又は使用する場所を変更した場合 （2）管理者又は管理者の委任を受けたアクセス権者が替わった場合 （3）鍵番号がアクセス権者以外の者に漏えいし、又はそのおそれがあると管理者又はアクセス権者が認めた場合
3	管理責任者は、立入制限区域に係る入退室口を、業務時間中のみ開錠する。
4	管理責任者は、立入制限区域へのアクセス権者を含む全ての者の立入りの状況(立入者の所属、氏名及び立入りの目的等)を記録し、事後的に確認可能とするため以下のような適切な措置を講ずる。 （1）鍵の貸し出しに係る管理簿の作成 （2）受付の設置による受付簿の管理 （3）IDによる認証の導入 （4）作業をしている者以外の者による同行と確認の実施
5	管理責任者は、立入制限区域の全ての鍵の解錠が可能なマスターキーの製作、共通パスワードの設定等がされている場合には、そのマスターキー等を管理する。
6	管理責任者は、立入制限区域内に保管容器や製造設備等の管理対象情報を設置した場合において、ワイヤで固定すること等により保管容器を物理的に持ち出せないよう適切な措置を講ずる。
7	管理責任者は、管理対象情報を持ち出す際に、持ち出し先となりうる場所について以下の事項等を事前に指定する。 （1）住所 （2）建物・施設名 （3）部屋番号 （4）持出先部屋の配置 （5）保管場所

第2.管理対象情報の運搬

項目番号	内容(案)
第 2	管理責任者は、管理対象情報を保管容器から持ち出し、運搬するための手順を定める。
1	管理責任者は、管理対象情報の運搬の際に、外部から当該管理対象情報を視認できないようにする。
2	管理責任者が指定した者は、当該管理対象情報を取り扱うための場所等においてアクセス権者に引き渡したときに、当該アクセス権者から受領証を受け取り、管理責任者に提出する。
3	管理責任者は、管理対象情報の運搬を信頼できる輸送機関又は運搬事業者に行わせる。
4	管理責任者は、当該管理責任者の属する事業者以外の者に管理対象情報を運搬させる必要がある場合には、当該者の情報の管理について評価し、及び当該者と秘密保持契約を締結しているかを確認する。管理対象情報を当該者以外の者から当該者に運搬する場合も同様とする。
5	管理責任者は、管理対象情報を持ち出す際に、持ち出しを行う持出人を最小限とし、その持出人を記録する。
6	管理責任者は、管理対象情報を持ち出す際に、持ち出しを行う目的を可能な限り限定し、その目的を記録する。

第3.立入制限区域への侵入の視認性の向上

項目番号	内容(案)
第 3	事業者は、立入制限区域への不審者の侵入に係る視認性を高める。
1	事業者は、立入制限区域に赤外線警報装置、セキュリティカメラ等の警備システムを導入する。
2	事業者は、警備員等がモニターにより立入制限区域及びその周辺を常時監視する体制を確保する。
3	事業者は、立入禁止区域の周辺に立入が禁止されていることを視覚的に認識できるようにする。
4	事業者は、立入制限区域への全ての立入者について、他の者から視認できるよう、当該立入制限区域に立ち入ることが許されていることがわかる標識の着用を求めるものとする。

第Ⅳ章（旧第Ⅴ章） 管理対象情報が電子情報である場合のアクセスの制限等

項目番号	内容（案）
Ⅳ	事業者は、管理対象情報が電子情報である場合には、管理対象情報への電子的なアクセスを制限する。

第1.サーバ等に記録される電子情報の管理手順の確立

項目番号	内容(案)
第１	事業者は、管理対象情報が電子情報である場合には、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予定の者に周知し、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。
１	事業者は、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手順等の操作手順書を作成する。
２	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定める。

第2.　サーバ等の重要機器への不正操作による情報漏洩、改ざん、システム停止の防止

項目番号	内容(案)
第 2	事業者は、サーバ等の設置エリアには、物理的セキュリティ対策を行う。
1	事業者は、管理者等管理対象情報を取り扱う情報システム(以下「管理情報システム」という。)を構成する機器のうちサーバ等は立入制限区域に設置する。
2	事業者は、サーバ等の設置エリアに入場可能な者を定める。
3	事業者は、サーバ等の設置エリアを施錠等で入場を制限する。

第3.情報システムを構成する機器の条件

項目番号	内容(案)
第 3	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、信頼性を考慮した上で機器を選定する。
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、管理対象情報をクラウド等自社以外の者のサーバ等で保存する場合には、そのクラウド等を管理する者の信頼性を確認(例えば、ISO／IEC 27017 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。
3	事業者は、管理対象情報を自社以外の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、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。
4	管理責任者は、サーバ等を設置する立入制限区域への管理情報システムの構成機器以外のサーバ等の持込みを禁止する。管理責任者は、管理情報システムの構成機器を新設する場合には、内蔵ソフトウェアの状況を確認した上で、当該構成機器が従業員等個人の所有物ではないものに限り認める。

第4.不正アクセスの防止

項目番号	内容(案)
第 4	事業者は自社が構築する情報システムを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不正アクセスを防止するために、必要な措置を講ずる。
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、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、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。
3	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。
4	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し、匿名でのネットワークへの接続(Anonymous 接続)を禁止する。
5	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。
6	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、情報システム管理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、導入を認めない。
7	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。
8	事業者は、インターネットへの接続に関する社内への教育を行う。
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。
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で、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。
11	事業者は、ユーザーID を個人毎に割り当てる。
12	事業者は、ユーザーID とシステム管理者 ID の権限を分離する。
13	事業者は、パスワード設定に関するルールを定め、周知する。

14	事業者は、ユーザーID 及びシステム管理者 ID は定期的、又は必要に応じて見直しを行い、不要な ID を削除する。
15	事業者は、情報システム、情報機器及び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う。
16	事業者は、パソコン及びサーバに、マルウェア感染を検知・通報するソフトウエア（ウイルス対策ソフト）を導入する。
17	事業者は、ウイルス対策ソフトのパターンファイルを常に最新化する。
18	事業者は、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る。

第5.情報システムの継続性

項目番号	内容(案)
第 5	事業者は、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。
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	事業者は、情報システムを置く施設を、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取組を行う。
3	事業者は、必要に応じて情報システムを復元する手順を整備する。
4	事業者は、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。
5	事業者は、事業継続の目的及び情報システム継続の要求事項に基づいて情報システムの備えを計画、実施、維持及び試験する。
6	事業者は、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。

第6.情報システム管理者の制限

項目番号	内容(案)
第 6	事業者は、情報システム管理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。
1	事業者は、情報システム管理者について、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、定期的に点検する。
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、情報システム管理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に設定することにより、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。

第7.情報システムの更新

項目番号	内容(案)
第 7	事業者は、管理情報システムを最新の状態に更新し、適切に機能を提供するための取組を実施する。
1	事業者は、当該管理情報システムが提供する機能を妨害するウイルス、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、更新されたウイ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。
2	事業者は、管理情報システムに対する脆弱性診断を定期的に実施する。
3	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。
4	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、利用されていない場合には、当該ソフトウェアを消去する。
5	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。

第8.アクセスログ等の保管

項目番号	内容(案)
第 8	事業者は、管理情報システムへのアクセスログを保管する。
1	事業者は、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により定期的に点検させる。
2	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。
3	事業者は、法令や契約上の要求事項及びリスクを考慮し、監査ログの合理的保存期間を決定した上で、2 の監査ログを当該期間保存し、定期的に点検する。

第9.電子情報である管理対象情報の送信

項目番号	内容(案)
第 9	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。
1	事業者は、管理対象情報を電子メール等によりネットワークを経由して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を暗号化する。
2	事業者は、管理対象情報を電子メール等によりネットワークを経由して外部に送信する場合は、そのログを合理的な期間保存する。

第10.　可搬式記録媒体の管理

項目番号	内容(案)
第 10	事業者は、管理対象情報を記録した可搬式記録媒体を適切に管理し、管理対象情報の流出を防止する。
1	情報システム管理者は、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(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、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。
3	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、暗号化する。
4	事業者は、従業員等個人が所有する情報システムを構成する機器及び可搬式記録媒体で、管理対象情報を取り扱わせない。

第11.　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	内容(案)
第 11	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。
1	情報システム管理者は、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を作成し、合理的な期間保管する。
2	事業者は、保守及び点検の記録、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を管理簿に記録する。
3	事業者は、情報システム管理者が、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。
4	事業者は、管理情報システムを構成する機器を譲渡する場合は、管理対象情報が復元できない状態であることを確認させる。

第12.　情報システムを管理する第三者の制限

項目番号	内容(案)
第 12	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にする。
1	事業者は、第三者が管理情報システムの保守及び点検を行うときは、情報システム管理者の指示の下で、管理対象情報を他の記録媒体に移した上で、管理情報システム内の管理対象情報を復元できないように消去する。
2	事業者は、第三者が管理情報システムの保守及び点検を行うときは、事業者の従業員等が立ち会い、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、保守及び点検業務を監視することができる状況で行わせる。
3	事業者は、第三者による管理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IDを無効化する。
4	事業者は、管理情報システムの保守及び点検を含む第三者に行わせるときは、秘密保持契約を締結した上で行わせる。
5	情報システム管理者は、第三者が管理情報システムの保守及び点検を行うときは、当該第三者の作業者を確認し、作業者の立入りを管理し、並びに立入制限区域内の保守及び点検の対象外の機器を撤去すること等により作業者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事業者の従業員等に立ち会わせ、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は、当該サーバ等を管理する事業者が第十二に掲げる措置に相当する措置を講ずることを確認する。

第13.　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	内容(案)
第 13	事業者は、管理情報システムへのアクセスを通じた管理対象情報の流出を防止する。
1	事業者は、管理情報システムに保存した管理対象情報へアクセスする者を必要最低限に限る。
2	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。
3	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の登録を適切に管理し、人事異動等に伴いアクセス権者に変更が生じた際は速やかに登録内容を変更する。
4	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の管理情報システムへのログインについて、2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。
5	事業者は、テレワーク等外部から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。
6	事業者は、テレワーク等外部から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。
7	事業者は、管理対象情報を電子政府推奨暗号を用いて暗号化する。

第14.　ログイン ID･パスワードの管理

項目番号	内容(案)
第 14	事業者は、アクセス権を設定した管理対象情報を管理情報システムに保存する場合、当該管理対象情報へのアクセスを行う際のログインID及びパスワードを適切に管理する。
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、管理情報システムそのものに、漏洩、なりすましが疑われる事態になった際に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。
3	事業者は、アクセス権者等に対して、管理情報システムにログイ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。
4	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)を使用させない。
5	事業者は、ユーザーID を個人毎に割り当てる。
6	事業者は、ユーザーID とシステム管理者 ID の権限を分離する。
7	事業者は、パスワード設定に関するルールを定め、周知する。
8	事業者は、ユーザーID 及びシステム管理者 ID を定期的、又は必要に応じて見直しを行い、不要な ID を削除する。

第Ⅴ章(旧第Ⅵ章) 管理対象情報をその管理対象情報を保有する事業者以外の者に渡す場合の措置

項目番号	内容(案)
Ⅴ	事業者は、管理対象情報を当該事業者の管理に属する従業員等以外の者(以下「外部委託先等」という。)に渡し、取り扱わせる場合には、当該管理対象情報の第三者への開示の禁止等を含む秘密保持契約を締結した後で引き渡すこととし、外部委託先等の情報管理の体制等の確認を通じて、管理対象情報の外部委託先等における適切な管理を確保する。

第1.外部委託先等に管理対象情報を取り扱わせる前の確認

項目番号	内容(案)
第１	事業者は、外部委託先等に管理対象情報を取り扱わせる前に、外部委託先等の情報管理の体制等を確認する。
1	事業者は、当該外部委託先等からの情報の流出等のリスクを考慮し、真に必要な取引であるかを検討した上で行う。
2	事業者は、当該外部委託先等が、管理対象情報を適切に管理し、かつ、当該事業者自らの情報の管理の要請に適切に対応できる能力を有するか否かについて事前に確認する。この確認は、基本的には、自らが講じている管理対象情報の適切な管理に係る取組と同等以上の取組が外部委託先等において行われているか否かを確認し、特に、外部委託先等が海外企業である場合等には、物理的に管理が行き届かないことや、法律や商慣行の違い等により漏えいリスクが高まる可能性も考えられるため、より確実に行う。
3	事業者は、管理対象情報を外部委託先等と共有する際に、情報セキュリティ事件及び事故発生時の、関係者ごとの役割と責任を明確化する。
4	事業者は、外部委託先等のサービスも含めた外部情報システムの一覧を作成し、定期的又は必要に応じて見直す。
5	事業者は、外部委託先等に管理対象情報を提供する場合には、可能な限り分割して引き渡すことにより、管理対象情報の全体が外部委託先等から見てわからないようにする。
6	事業者は、製造設備のリモートメンテナンス等、管理対象情報そのものを渡すことにはならない一方で、長期にわたり徐々に技術等情報がリモートメンテナンス等を行う事業者に蓄積され、管理対象情報を構成することができるような事例にも対応するため、外部委託先等が技術等情報を適切に管理し、かつ、自らの要請に適切に対応できる能力を有するか否かについて事前に確認し、蓄積された管理対象情報の目的外利用の禁止、第三者への開示の禁止を契約で明記し、条件違反等契約に違反した場合に損害賠償請求等の法的措置をとる旨の記載を行う等の取組を行う。
7	事業者は、管理対象情報に関連する物(例えば、製造委託をした場合の製造設備)のメンテナンス等を外部委託先等に委託し、更に当該外部委託先等が当該メンテナンス等を第三者に再委託する場合には、事前に当該管理対象情報を提供する者の承認を得ることを条件とする。

第2.秘密保持契約

項目番号	内容(案)
第 2	事業者は、管理対象情報を外部委託先等に提供する場合は、適切な管理を行うために必要な条項を含む秘密保持契約又はこれに準ずる法的拘束力のある取決めを締結する。
1	事業者は、管理対象情報を外部委託先等に提供する前に、以下の事項のうち必要なものを含む秘密保持契約又はこれに準ずる法的拘束力のある取決めを締結する。 (1) 外部委託先等は、提供された管理対象情報の取扱者を限定すること。 (2) 外部委託先等は、提供された管理対象情報の取扱者の氏名等を明らかにすること。 (3) 外部委託先等における提供された管理対象情報の取扱者の範囲が Need to Know の原則に照らして必要最小限であることを、当該管理対象情報を提供する者が確認すること。 (4) 外部委託先等は、外部委託先等における提供された管理対象情報の取扱者による管理対象情報へのアクセスを記録し、管理すること。 (5) 外部委託先等は、提供された管理対象情報の複製、廃棄等をした場合の管理簿を作成し、合理的な期間保管すること。 (6) 外部委託先等は、管理対象情報を提供する者から求められている場合には、当該管理対象情報を提供する者に対して、当該管理対象情報の複製、廃棄等をした旨の通知を行うこと。 (7) 外部委託先等は、提供された管理対象情報に係る契約の満了時又は解除時において、当該管理対象情報を速やかに廃棄又は返還等をすること。 (8) 外部委託先等は、管理対象情報を提供する者に対して、当該管理対象情報の管理の状況について、定期的に報告をすること。 (9) 外部委託先等において、定期的又は不定期に管理対象情報を提供する者からの監査を受け入れること。 (10)外部委託先等の管理対象情報の管理責任者が管理簿を廃棄する場合は、事前に事業者の取締役等の経営層に確認すること。
2	事業者は、秘密保持契約又はこれに準ずる取決めのひな形を定める。

2. 業界等と連携した技術情報管理認証制度の普及活動

(1)当事業における普及活動実施の狙い

当事業における業界等と連携した技術情報管理認証制度の普及活動は、大きく3点の課題認識をもとに実施した。3点の課題、課題への対処の方向性、当事業における打ち手は以下のとおりである。

図表 2-5 普及に係る課題、課題への対応の方向性、当事業における打ち手

【課題】	【課題への対応の方向性】	【当事業における打ち手】
①当制度の認知度が低い	当事業の普及活動を通じ、より多くの方に認証制度を知っていただく。	特定の団体に向けたセミナー・説明実施ではなく、不特定向けのオンラインセミナーを開催し、制度の認知を高める。
②当制度の存在を認知していたとしても、関心・認証取得につながるアクションをとってもらえない	当制度への関心・認証取得につなげていただくためのファーストステップとして、なぜ情報管理が必要なのか、何から始めるといいのか、認証取得後にどういった展開があり得るのかを理解してもらう。	情報セキュリティに係る最新の動向や、まず取り組むべきセキュリティ対策に関する説明、自己チェックリスト活用に関する説明パートを設ける。また、認証取得によるインセンティブについても経産省より説明を行う。
③認証取得に興味を持つような企業のニーズを把握しきれていない。	参加者からのアンケート等を通じ、当制度への認知度の正確な把握や、今後の制度や普及へのニーズを把握する。	セミナー事後アンケートを通じた対応を実施する。

（2）実施概要

実施概要は以下のとおりである。

①セミナータイトル

「信頼確保のための情報管理の重要性～情報管理の高度化に向け求められる取組と活用すべき認証とは～」

②開催日時

・第1日程：2023年12月6日14:00～
・第2日程：2023年12月13日13:30～

③会場

・WebEXによるオンライン開催にて実施

④対象

・これから自社の技術等の情報の管理に取り組もうとお考えの方
・自社の技術情報の管理体制について情報収集中の方
・情報管理・セキュリティに関する認証を取得して対外的にアピールしたい企業のご担当者の方

⑤登壇者

当制度への関心・認証取得につなげていただくためのファーストステップとして、なぜ情報管理が必要なのかを訴求するため、情報管理に精通している外部弁護士（弁護士法人NEX渡邉遼太郎先生）に講演をいただいた。

また、技術情報管理認証制度概要やインセンティブ等については、経済産業省担当者より説明を行うとともに、昨年度公表された「技術情報管理　自己チェックリスト」について、三菱UFJリサーチ＆コンサルティングより説明を行った。

⑥セミナー周知

経済産業省ウェブサイト、中小企業基盤整備機構ウェブサイト（J-Net21）、三菱UFJリサーチ＆コンサルティングウェブサイト等を通じた周知を行うとともに、一部業界団体向けにセミナー実施の周知を実施した。セミナー周知にあたっては、以下のようなセミナーチラシを作成した。

図表 2-6 セミナー周知チラシ

参加費
無料

12/6(水)・12/13(水) 開催セミナー

信頼確保のための情報管理の重要性
～情報管理の高度化に向け求められる取組と活用すべき認証とは～

企業経営の重要な資源である「技術をはじめとする大事な情報」を適切に管理する重要性は高まり続けており、情報管理が不十分で情報漏えい・紛失を起こすと、取引停止になったり業務や売上に大きな損害を被る可能性があります。また、最近では、企業間の取引の条件として適切な情報管理・情報セキュリティ対策の実施が求められることも増えています。

本セミナーでは、情報管理の重要性について有識者よりご説明をいただきつつ、国の基準に基づき、国の認定を受けた機関が、組織の情報セキュリティ体制を審査・認証する制度(技術情報管理認証制度)について、経済産業省ご担当者様より紹介します。

●2023年12月6日(水)　14:00～15:30 (終了予定)

●2023年12月13日(水) 13:30～15:00 (終了予定)

(1)情報管理の重要性/情報管理上重要となる取組

【講師】 渡邊 遼太郎 弁護士

(2)情報管理体制強化に向けた初めの一歩(自己チェックリストを活用したセルフチェックのご紹介)

(3)技術情報管理認証制度のご案内

【ご説明者】 経済産業省ご担当者様

※事前参加登録はコチラ
https://www.murc.jp/cam/tech-manegement2023/

セミナー	信頼確保のための情報管理の重要性 ～情報管理の高度化に向け求められる取組と活用すべき認証とは～
開催日時	(1)2023年12月6 日(水) 14:00～15:30(終了予定) (2)2023年12月13日 (水) 13:30～15:00(終了予定)
開催形式	オンライン (WebEXウェビナー)
参加費	無料
参加申込	事前参加登録制
プログラム(予定)	・ 情報管理の重要性/情報管理上重要となる取組(講師による講演) ・ 情報管理体制強化に向けた初めの一歩(自己チェックリストを活用したセルフチェックのご紹介) ・ 技術情報管理認証制度のご案内(認証取得のための支援・取得によるメリット等)

令和5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に関する調査分析及び普及促進等事業)(受託事業者:三菱UFJリサーチ&コンサルティング株式会社)
【お問合せ先】E-mail:tech-manegement2023@murc.jp

⑦プログラム

オンラインセミナーは以下のプログラムに沿って進行した。以下に、12月6日開催の進行表を記載する。

図表 2-7 プログラム進行表(12月6日開催分)

13:00～13:20	事務局会議設定準備	事務局
13:20～13:30	発表者接続テストの実施 ※音声接続のテスト、投影資料の共有確認	経産省様 外部弁護士
13:45～14:00	開場	
14:00～14:05	開会ご挨拶	事務局もしくは経産省様
14:05～14:45	「情報資産管理の重要性と必要な取組み」 ※最後の5～10分程度は質疑も含む	外部弁護士 ※質疑の司会は事務局
14:45～15:05	技術情報管理 自己チェックリストの活用 ※最後の5分程度は質疑も含む	事務局
15:05～15:20	技術情報管理認証制度の概要 ※制度概要・インセンティブ等について説明 ※最後の5分程度は質疑も含む	経産省 ※質疑の司会は事務局
15:15～15:20	まとめ	事務局
15:20～15:25	閉会ご挨拶	事務局もしくは経産省
15:25～30頃	閉会	

⑧参加者

オンラインセミナーには、2日程合わせて58名の方にご参加をいただいた。

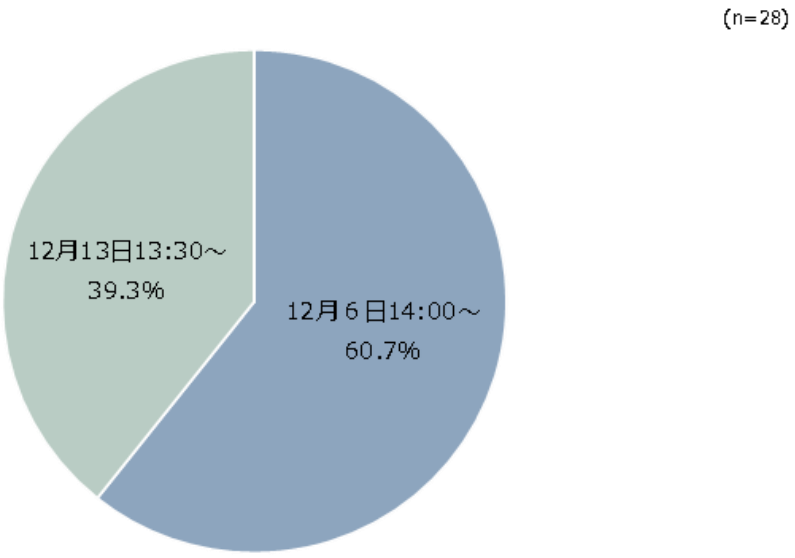
(3)実施後アンケート結果

セミナー実施後に、セミナーの満足度や要望を聴取するためのオンラインアンケートを実施し、28名の参加者から回答をいただいた。

①問1. 参加いただいた日程について教えてください。参加できなかった場合には、申込いただいた日程をご回答ください。

「12月6日14:00～」の割合が最も高く60.7%となっている。次いで、「12月13日13:30～(39.3%)」となっている。

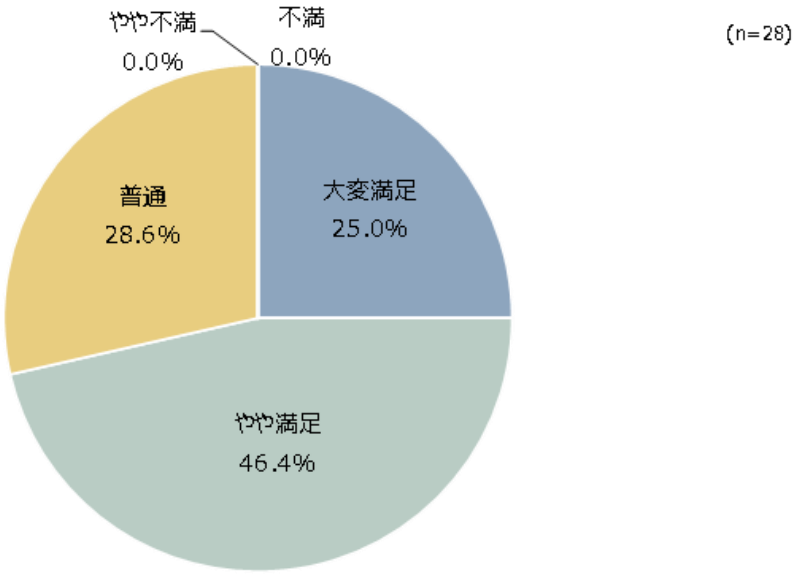
図表 2-8 参加いただいた日程について教えてください。参加できなかった場合には、申込いただいた日程をご回答ください。



②問2. セミナー全体の満足度について教えてください。

「やや満足」の割合が最も高く46.4%となっている。次いで、「普通(28.6%)」、「大変満足(25.0%)」となっている。

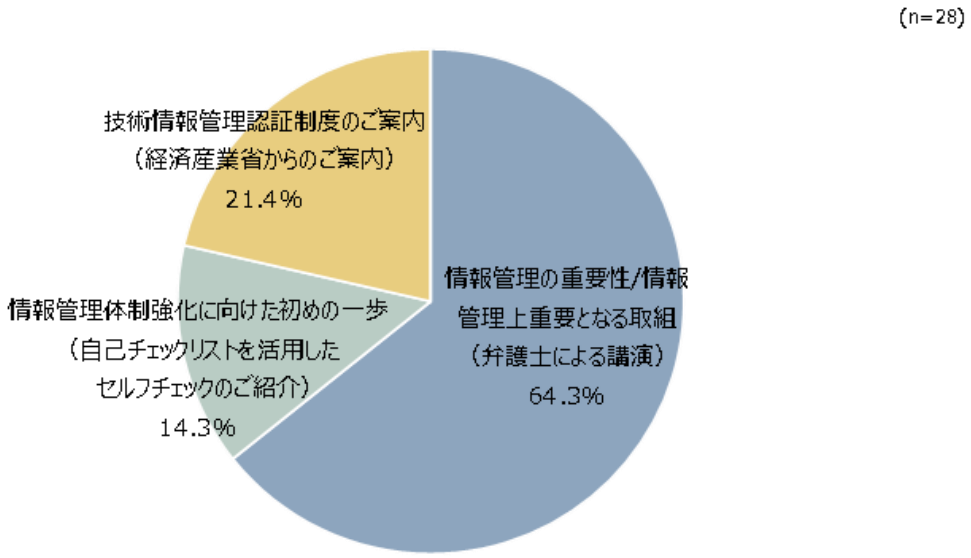
図表 2-9 セミナー全体の満足度について教えてください。



③問3. 各プログラムのうち最も満足度が高かったプログラムを教えてください。

「情報管理の重要性/情報管理上重要となる取組(弁護士による講演)」の割合が最も高く64.3%となっている。次いで、「技術情報管理認証制度のご案内(経済産業省からのご案内)(21.4%)」、「情報管理体制強化に向けた初めの一歩(自己チェックリストを活用したセルフチェックのご紹介)(14.3%)」となっている。

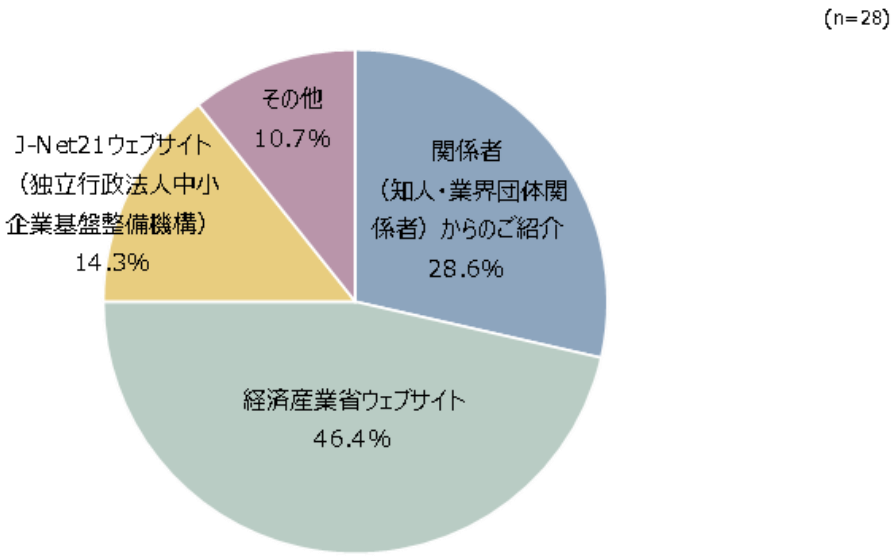
図表 2-10 各プログラムのうち最も満足度が高かったプログラムを教えてください。



④問4. 本セミナーを知った経緯について教えてください。

「経済産業省ウェブサイト」の割合が最も高く46.4%となっている。次いで、「関係者(知人・業界団体関係者)からのご紹介(28.6%)」、「J-Net21ウェブサイト(独立行政法人中小企業基盤整備機構)(14.3%)」となっている。

図表 2-11 本セミナーを知った経緯について教えてください。



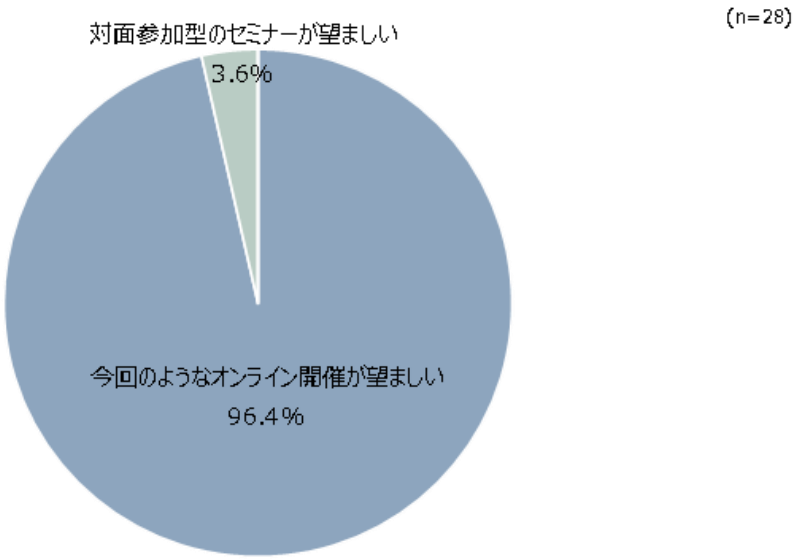
(その他自由回答)

- 経済産業省 新着情報配信サービス
- SQUET
- 経済産業省のメールニュース

⑤問5. 今回のようなセミナーの開催方法についてご意見をお知らせください。

「今回のようなオンライン開催が望ましい」の割合が最も高く96.4%となっている。次いで、「対面参加型のセミナーが望ましい(3.6%)」となっている。

図表 2-12 今回のようなセミナーの開催方法についてご意見をお知らせください。



⑥問6. 今回のセミナー全体に対するご意見やご感想、ご要望等があれば、お聞かせください。

図表 2-13 今回のセミナー全体に対するご意見やご感想、ご要望等があれば、お聞かせください（自由回答）

- 大変勉強になりました。情報管理は多岐にわたる法令やプロセスが関係してくるので非常に複雑で、弊社でもなかなか悩んでいるところです。
- 情報資産管理の重要性、必要な取組み、認証制度に関して、コンパクトにポイントを絞って説明いただき、非常に分かりやすかったと思います。
- 情報資産を適切に管理することが思わぬセキュリティリスクを防止又は低減することを再認識することができました。
- 出張の移動車内での受講だったため、通信遮断による聞き逃しがあった
- 期間限定で良いので「再放送」が視聴できるとありがたい
- 事前に資料をいただけるとより効果的かと思いました。
- 各方面から貴重なご講演をありがとうございました。
- 情報管理の重要性と企業の強みに変え得る仕組みについて学べました。

第3章　有識者会議・ワーキンググループの運営・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・課題の分析や基準改定案の内容・方向性について議論した上で、当該議論の結果を踏まえたとりまとめを実施した。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。

1. 技術情報管理認証制度に係る検討会

(1)設置目的

調査分析事業、業界等と連携した技術情報管理認証制度の普及活動について、経済産業省から本事業の委託を受けた三菱UFJリサーチ&コンサルティング株式会社において、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

2023年8月31日～2024年2月29日

(3)委員

及川　勝	全国中小企業団体中央会　事務局長/総務企画部長/人材育成部長
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
加藤　正敏	日本商工会議所　産業政策第一部長
川治　恒紀	独立行政法人中小企業基盤整備機構　経営支援部 経営支援企画課　課長
小暮　亮	全国商工会連合会　産業政策部　産業政策課　課長
田中　芳夫	一般社団法人ものこと双発推進　代表理事
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
藤本　正代	情報セキュリティ大学院大学　教授
松井　俊浩	学校法人滋慶学園　東京情報デザイン専門職大学　教授

（2023/8/31 時点、委員五十音順、敬称略）

(4)開催概要

①第1回

図表 3-1 技術情報管理認証制度に係る検討会 第1回会合

日時	2023 年 8 月 31 日(金) 13:00 ～ 15:00
場所	経済産業省別館 2 階 235 会議室 ／ 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

図表 3-2 技術情報管理認証制度に係る検討会 第2回会合

日時	2023 年 12 月 8 日(金) 13:00 ～ 15:00
場所	経済産業省別館 2 階 235 会議室 ／ オンライン開催(WebEX)
議題	(1)開会 (2)基準改定作業について

③第3回

図表 3-3 技術情報管理認証制度に係る検討会 第3回会合

日時	2024 年 2 月 13 日(火) 13:00 ～ 15:00
場所	経済産業省別館 11 階 1111 会議室 ／ オンライン開催(WebEX)
議題	(1)開会 (2)基準改定作業について

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

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三菱UFJリサーチ&コンサルティング株式会社において、認証機関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。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は促進指針第2の4の連絡会として開催する。

(2)設置期間

2023年9月13日～2024年2月29日

(3)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　認証事業部　部長
髙村　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
茨田　学	一般社団法人日本金属プレス工業協会　専務理事
光守　健	日本検査キューエイ株式会社　執行役員営業部長
六畑　方之	公益財団法人防衛基盤整備協会　第2事業部長

（2023/8/31 時点、委員五十音順、敬称略）

(4)開催概要

①第1回

図表 3-4 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	2023 年 9 月 13 日(水) 15:00 ～ 17:00
場所	経済産業省別館 3 階 302 会議室／ オンライン開催(WebEX)
議題	(1)開会 (2)経済産業省 挨拶 (3)ワーキング委員ご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

図表 3-5 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	2023 年 11 月 27 日(月) 13:00 ～ 15:00
場所	経済産業省別館 2 階 238 会議室 ／ オンライン開催(WebEX)
議題	(1)開会 (2)基準改定作業について

③第3回

図表 3-6 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	2024 年 2 月 7 日(水) 13:00 ～ 15:00
場所	経済産業省別館 238 会議室 ／ オンライン開催(WebEX)
議題	(1)開会 (2)基準改定作業について