No.	該当箇所			寄せられた御意見の概要	理由	提出意見に対する考え方
	該当文書	該当ページ又は項番	該当項目			
1	制度構築方針(案)	4	はじめに	目指す効果の1つ目に、制度の対象が『全てのサプライチェーン企業』とあるが、適用除外や猶予の判断基準が本文では不十分である。	現場ではOTや製品側の境界に関するグレーゾーンが多く、適用／非適用の線引きが曖昧だと負担や責任の過不足が生じるため。	本制度は、２社間の取引契約等において用いることを想定した任意の制度あり、その適用を強制するものではありません。
2	制度構築方針(案)	4	はじめに	制度趣旨に、再委託先の管理を明言しているが、★段階提示の想定において、再委託先管理の責任分界が具体性に欠け、曖昧である。	発注者が再委託先に直接の管理責任を持たない旨の注記が、サプライチェーンの深層までのリスク伝播管理を弱める可能性があるため。	再委託先への適用の範囲は、例えば制度構築方針(案)P.14に記載の考え方に基づき、直接の取引先(委託先)による判断で実施することが想定されます。
3	制度構築方針(案)	4	はじめに	蛇足かもしれませんが、「ここでいうサプライチェーンはISO27001:2022付属書Aの5.21のICTサプライチェーンと異なって、エンドユーザーからの注文を受けたサプライヤーが、原材料・部品の調達から、製造、在庫管理、配送、商品陳列などを連結させてお客の手元に商品を届けていく仕組みを対象としている」ことを明記したほうがよいと思います。 また、本評価制度は受注者が対応し、発注者が要求するものであることも、明確に記述したほうがよいと思います。 因みに、医療関係では医療機関は厚生労働省の作成したガイドライン、ベンダー側は総務省と経済産業省が作成したガイドラインに従うことになっています。	ISMS関係者が混乱しないため。	いただいた意見については、今後の検討の参考とさせていただきます。
4	制度構築方針(案)	6	制度の目的	制度目的の各効果欄にある、費用や低減に対する定量指標が欠落しているので、効果が不明である。	『可視化』や『コスト低減』が効果として記載されているが、実装負担に対する便益の測定枠組みが示されていないため。	いただいた意見については、詳細な制度設計等の検討に当たっての参考とさせていただきます。
5	制度構築方針(案)	6	制度の目的	「取引先に求めるセキュリティ対策の内容や水準の決定や、実施状況の把握が容易・適切になる」とありますが、本施策でも企業へのチェックリストでの運用が中心になると想定しております。チェックリストの各項目の回答に対してエビデンスの記載を明確にすべきではないかと考えます。これによって評価者の評価がより客観的になるメリットがあると考えます。		いただいた意見については、自己評価実施時の証跡の取り扱いの検討に当たっての参考とさせていただきます。
6	制度構築方針(案)	6	制度の目的	「セキュリティサービスの標準化」とは何を指すのかが不明確かと考えます。		ここでは、本制度の普及・浸透により、★を取得するために求められるセキュリティサービスの水準や機能等が標準化されていくことを指しています。
7	制度構築方針(案)	7	対象とするリスクの範囲	表中 最下行の影響を受けるサプライチェーン項目の ・「IT サービスサプライチェーン」 を ・「ビジネスサプライチェーン」に変更。	「マネージドサービス等の環境を踏み台とした、発注者側システム環境への不正侵入」については、運用サービスを提供するサプライチェーン企業が自社運用するマネージドサービス基盤が侵害された場合において自社基盤が侵害されていることから、ビジネスサプライチェーンと同等の整理になると考えます。	いただいた意見も参考にしつつ、制度構築方針における該当箇所の修正を検討させていただきます。
8	制度構築方針(案)	9	制度の対象範囲	★3 がサプライチェーンにおけるベースラインとして位置付けられる場合、発注側が受託側に達成を求める以上、発注側自身も同等水準を満たすことが前提となる運用が想定されます。このとき、発注側のグループ企業全体（子会社・関連会社等）への波及や、適用範囲の解釈による運用負荷の増大が懸念されます。評価単位を法人単位ではなく拠点単位等で運用可能とする方向性は合理的と考えますが、クラウド活用や共通基盤（認証、監視、運用等）がある場合、物理分離が可能でも実態として分離できない領域が残り得ます。拠点単位で評価する場合の分解点、除外要件、専門家判断の妥当性・統一性、OT（制御）システムの想定範囲等について、具体例を含め明確化し、過剰要求や形骸化を防ぐ指針を提示いただくことを要望します。		いただいた意見については、詳細な制度設計等の検討に当たっての参考とさせていただきます。
9	制度構築方針(案)	9	制度の対象範囲	「ネットワークに接続していない機器は除外」とあるが、物理的な持ち出しなどで 情報流出などが起こり得るのは、その様なスタンドアロン機器も同様だろう。 スタンドアロンであっても、パスワードや暗号化などの情報保護を行うよう、評価に含めるべきだ。 同様に、利用するクラウドに対する安全評価、外部からアクセスさせる情報への規制 (特に 最近問題になっている AI によるデータ収集" に対する 防御) も、規定すべきである。		本制度では、企業ごとの判断に応じて、スタンドアロン機器も適用範囲に含めることを許容しています。いただいた御意見も参考に、制度構築方針の該当箇所を修正を検討させていただきます。
10	制度構築方針(案)	9	制度の対象範囲	OT/製品を『直接の対象とはせず』とする除外条件が不明である。	IT/OTの融合が進む中で境界侵入経路としてOTが足掛かりになる事例が増加しているため。	ネットワークがファイアウォールやVLAN等により内外の通信が必要最小限になっていることを除外条件としています。 そのうえで、OTはITネットワークと論理または物理分離されていることを前提としています。 また、製品は、自社から顧客に販売等されるもので、自社IT基盤につながらないことを前提としています。
11	制度構築方針(案)	9	制度の対象範囲	インターネット公開サーバを『必ず含める』要件は妥当だが、CDN/WAF等の委託構成に触れていないため、 責任共有モデルの具体例にCDN/WAF/SaaS型メールを追加し、サービス側証跡（ログ取得、MFA、脆弱性管理）確認項目を明記する必要である。	現実の公開系はCDN・WAF・DDoS緩和サービスを介し、自社の責任範囲が不明確になりやすいため。	制度構築方針(案)P.9記載のとおり、クラウドサービスについては責任共有モデルに基づき、自社における対策実装又はサービス提供者等における対策状況の確認を行う必要があることとしています。
12	制度構築方針(案)	9	制度の対象範囲	[◆原則として適用範囲に含めるが、例外的に適用範囲に含めないことが許容され得るもの]の中に、サポート期限切れソフトがあり、判断を専門家に依存するため、例外は期限付き（90日）とし、仮想パッチ・隔離・アクセス制御の代替措置を義務化する必要がある。	例外が長期残存するリスクが潜み、評価判断を専門家に委ねる構造となるため、解決までに時間がかかる可能性があるため。	いただいた意見も参考にしつつ、制度構築方針における該当箇所の修正を検討させていただきます。
13	制度構築方針(案)	9	制度の対象範囲	Shared Responsibilityモデルに基づく責任分界の明確化を求めます。	クラウドやソフトウェアの利用が前提となる企業が、どのレイヤを自社で担い、どこをサービス提供者に求めるべきかを判断できれば、 過不足のない対策・契約設計が可能になります。責任分界が明瞭だと、インシデント時の初動も迅速化します。	クラウドサービス等の具体的な責任分界については、サービスごとの取り決めや他の制度・ガイドライン等に基づき対応を行うことを想定しています。
14	制度構築方針(案)	9	制度の対象範囲	また、ISMSとSCSの精度の比較の取得範囲で、SCSは「インターネットに接続している自社IT基盤」が対象となっているが、違和感を覚える。★３でもガバナンスの整備や取引先管理、リスクの特定やインシデントへの対応/復旧が要求事項に入っていて組織が対象外というのは、説明として苦しくないか。		大分類No.1「ガバナンスの整備」においては、No.1-1など、一部組織の状況等に係る要求事項・評価基準を規定しています。 いただいた意見については、今後の検討の参考とさせていただきます。
15	制度構築方針(案)	9	制度の対象範囲	原則として適用範囲に含めるが、例外的に適用範囲に含めないことが許容され得るものとして、「本制度の要求事項を満たすことが困難なIT機器やソフトウエア（例：サポート期限切れのソフトウェア等）」の記載があるが、、サポート期限切れのOSやブラウザーを狙っての攻撃はある一定ある現状の中で、例外にすべきではないのではないかと考えます。		いただいた意見も参考にしつつ、制度構築方針における該当箇所の修正を検討させていただきます。
16	制度構築方針(案)	9	制度の対象範囲	制度構築方針（案）資料スライドP.9に、「例外的に適用範囲に含めないことが許容され得るもの」の例として、「サポート期限切れのソフトウェア等」との記載があるが、脆弱な状況を許容すると解釈される恐れがある印象がある。サポート期限切れのソフトウェアはアップデートがなされないため脆弱性が放置されているケースが多く、むしろそれをどのようにセキュアに管理しているかを重点的に確認する必要があると考える。		いただいた意見も参考にしつつ、制度構築方針における該当箇所の修正を検討させていただきます。
17	制度構築方針(案)	9	制度の対象範囲	製造環境（OT）や発注元等に提供される製品・サービスを制度の直接対象外とする整理を再検討すべきである。	近年のサプライチェーン攻撃では、開発環境、CI/CD基盤、製造工程、ファームウェアやソフトウェア更新物そのものを起点とした侵害が多く確認されている。IT/OTで求められる対策が異なることは事実であるが、それは対象外とする理由にはならず、少なくとも別枠評価や最低限の統制要件を設けなければ実際の脅威モデルと乖離する。	製造環境（OT）や発注元等に提供される製品・サービスについては、他の制度やガイドラインなどにより対応することを想定しています。 また、本制度では、適用対象外とするネットワークや機器等については、ファイアウォール等によりネットワークを分離することとしています。
18	制度構築方針(案)	9	制度の対象範囲	外部ネットワーク境界を基点とした整理は、ゼロトラストやクラウド・SaaS前提の実環境を十分に反映していない。	現在の侵害事例の多くは、ID・認証情報の窃取、委託先アカウントの悪用、SaaS設定不備、APIトークンの漏洩等を起点としており、 ネットワーク境界機器の有無のみを重視すると実効的なリスク評価を誤る可能性がある。ID、認証、端末状態、委託関係を軸とした整理が必要である。	いただいた意見については、今後の検討の参考とさせていただきます。
19	制度構築方針(案)	9	制度の対象範囲	図の右下にあるクラウドサービスは、オンプレミスではないIT基盤（所謂Iaas、Paas）も対象範囲とすることを意味していると読み取ったが、クラウドサービスという言葉が広義であり、あたかもSaasなどIT基盤以外のクラウドサービスも含まれるように見えてしまう。Iaas、Paasなどの例示を頂きたい。若しくはp.9に記載の１．IT基盤の項の3点目について、p.8の図の「クラウドサービス」をさすものであることを明記いただきたい。	方針書であることは認識しているが、対象に関する誤認識を防ぐことが、事前準備の効率化の観点から重要であると考えるため。また、中小企業における課題については、明確な支援制度を記載することで、制度全体が推進しやすくなると考えるため。	本制度では、IaaS、PaaSのようなサーバー基盤を構成するものに加えて、SaaSについてもクラウドサービスに含めることを想定しています。
20	制度構築方針(案)	9	制度の対象範囲	本制度の対象範囲の基本的な考え方として、 IT 基盤および外部ネットワーク境界等は対象、製造環境等の制御（OT）システムは対象外とするものと理解している。他方、IT 基盤や外部ネットワークと接続している OT などは対象範囲になり得るか等（例示には一方向セキュ リティゲートウェイで外部ネットワークと区切られた製造拠点の制御システムと補足の記載もあった為）、ネットワーク環境次第では事業者側が判断に迷うケースもあろうかと思うため、「適用範囲外」と整理されるパターン・条件を含め、より具体的な指針などご教示いただきたい。	「適用範囲外」と整理され得る条件や代表的な構成例などが示されることで、事業者側における対象スコープ設定が明確になり、本制度の実効性向上にも資すると考えるため。	本制度では、制度構築方針(案)P.8記載のとおり、IT基盤を対象としOTについては対象外としています。一方で、取得希望組織においてOT領域を有する場合にあっては、OT領域は、ファイアウォール又はVLAN等によりIT基盤とネットワークを分離したうえで、適用範囲からは除外する必要があります。
21	制度構築方針(案)	9	制度の対象範囲	適用範囲を『適用範囲に含めないものに該当しないもの』と定義する構造は、制度として分かりにく、再整理が必要である。	否定形を多用した定義は、事業者ごとに解釈差を生み、評価結果の一貫性を損なう。攻撃者視点では適用範囲の曖昧さは防御の隙 となるため、典型的な対象・非対象の明示や具体例を含めた整理が望ましい。	いただいた意見については、詳細な制度設計等の検討に当たっての参考とさせていただきます。
22	制度構築方針(案)	9	制度の対象範囲	「原則として適用範囲に含めるが、例外的に適用範囲に含めないことが許容され得るもの」として、サポート期限切れのソフトウェアが例示されているが、やむを得ないと判断される場合の基本的な考え方やその他代表的な事例についてご教示いただきたい。	やむを得ないと判断される場合の考え方や代表的な事例がより具体的に示されれば、事業者と評価機関の双方が共通認識を持って 例外の適用可否を判断でき、本制度のと実効性の向上につながると考えるため。	いただいた意見も参考にしつつ、制度構築方針における該当箇所の修正を検討させていただきます。
23	制度構築方針(案)	9	制度の対象範囲	企業は個社/(国内又は海外を含む)企業グループ/事業部等と★の取得範囲を柔軟に定めることができる。 ●本企業評価制度の取得は、今後、政府調達や、様々な分野のガイドラインにおいても、取得が推奨あるいは勧告など求められることになると思慮するが、その際においても、取得する側が柔軟に取得範囲を決めることが出来るようにしていただきたい。	様々な事業分野を抱える大企業においては、取得が求められる分野毎に柔軟な対応が必要と考えるため。	いただいた意見については、詳細な制度設計等の検討に当たっての参考とさせていただきます。
24	制度構築方針(案)	9	制度の対象範囲	本制度における評価対象について、自社が直接契約していないクラウドサービスであっても、業務上利用しているクラウドサービスは評価対象に含まれるという想定であると理解している。 しかしながら、当該考え方が評価基準上、明確に読み取れる記載とはなっていないため、「自社契約の有無」「利用形態（直接利用／間接利用）」にかかわらず、業務利用しているクラウドサービスは評価対象に含まれることを、明示的に言及していただきたい。	契約主体のみを基準として評価対象を判断した場合、「シャドーITの見逃し」「実質的に重要な業務基盤が評価対象外となる」といったリスクが生じる。 制度の目的である「サプライチェーン全体のセキュリティ水準向上」を実現するためには、契約形態ではなく、業務利用の実態を基準とした評価対象の考え方を明確にすることが重要と考える。	制度構築方針P.8記載のとおり、本制度では、契約の有無にかかわらず「取得希望企業のIT基盤を構成するが、他社との間で対策に係る責任を共有するもの」について適用範囲に含める必要があることとしています。いただいた意見については、今後の検討の参考とさせていただきます。
25	制度構築方針(案)	9	制度の対象範囲	本制度において、親会社・子会社等を含む企業グループ単位での星獲得は現実的な運用として想定されているか確認したい。 また、その場合、技術監査（技術検証）は、「グループ共通基盤のみを対象とするのか」「事業会社ごとに個別実施が必要となるのか」について、どのような整理を想定しているか示していただきたい。	契約主体のみを基準として評価対象を判断した場合、「シャドーITの見逃し」「実質的に重要な業務基盤が評価対象外となる」といったリスクが生じる。 制度の目的である「サプライチェーン全体のセキュリティ水準向上」を実現するためには、契約形態ではなく、業務利用の実態を基準とした評価対象の考え方を明確にすることが重要と考える。	制度構築方針P.12記載のとおり、適用範囲の妥当性の確認がなされた場合には、グループ単位での取得も制度として否定はしていません。なお、技術検証の詳細なスキームについては、いただいた意見も参考に、今後検討してまいります。
26	制度構築方針(案)	9	制度の対象範囲	対象範囲の指定について、部門単位で取得する際に「NW分離」が必要条件とされている件について、条件が厳しく実効性が低いのではないか	大手企業で、一部の子会社のある特定部門とNWがつながっているケースを考える。その特定部門にのみ★４を求めたいが、そうすると子会社側にはその部門をNW分離するように構成変更してもらわないといけない	本制度においては、サイバー攻撃の被害拡大のリスクを低減しつつ、★を取得する範囲を明確化するために、適用範囲のネットワークについて、内外の通信を必要最小限とすることを求めています。いただいた意見については、今後の検討の参考とさせていただきます。
27	制度構築方針(案)	9	制度の対象範囲	2.2.2 制度の対象範囲「適用範囲に含めないもの」について、IT基盤以外の「外部ネットワーク境界」機器や「クラウドサービス」などを開始間接的に接続するIT基盤やクラウドサービスなどもあります。例えば社内ネットワーク機器がパブリッククラウド上のサービスと接続し管理者に様々な情報を提供するシステムなどについて、本制度の被監査範囲に含まれるかどうかご教授頂きたい		原則としては適用範囲に含まれると想定しています。
28	制度構築方針(案)	9	制度の対象範囲	「適用範囲とするIT基盤等に接続等するが適用範囲には含めないという判断をしたものについて、ネットワーク機器等(例：VLAN、ファイアウォール)により、適用範囲との境界を技術的に分離すること」とあるが、その例に「取得単位を国内の事業所とする場合～、海外事業所との間の通信をネットワーク機器等により必要最小限にする」とあり、「技術的に分離」と「必要最小限」の解釈に乖離がある（具体例になっていない）。リスク管理上は分離すべきと考えるため、分離の度合いを具体例として示すべき		いただいた意見も参考にしつつ、制度構築方針における該当箇所の修正を検討させていただきます。

No.	該当箇所			寄せられた御意見の概要	理由	提出意見に対する考え方
	該当文書	該当ページ又は項番	該当項目			
29	制度構築方針(案)	9	制度の対象範囲	制度運営に関する資料を拝見すると、法人はもちろん個人事業主も本制度の対象として想定されているように読み取れる。 確かに、法人格を有していなくとも、多数の人員を雇用し、法人に準ずる組織体制を有する事業者が存在することは事実である。一方で、本制度の案内のしかたによっては、一人会社や、少人数で運営されている個人事業主までもが本制度の対象であるかのように誤解される惧れがある。 現在の制度案はいずれも、一定の組織性や役割分担できる人員体制を前提とした設計となっており、いわゆる小規模法人や個人事業主は対象としづらい構造であると考える。 そのため、制度の入口条件として、法人格の有無にかかわらず、「一定以上の組織体制を有していること」を前提条件として明記することを提案したい。これにより、数人規模で運営されている小規模法人や個人事業主に、過度に重い制度負担を課すことを避けるとともに、本制度が本来想定する対象層を明確化できると考える。		いただいた意見については、詳細な制度設計等の検討に当たっての参考とさせていただきます。
30	制度構築方針(案)	9	制度の対象範囲	本制度の対象範囲を正確に理解することは、企業における本制度への適切な対応を促すことに繋がる。「制度の対象範囲」の図において、取引先や再委託先の管理や制度適用要否など、「制度の対象とする組織」についても明確に記載することを望む。	情報システムの受託開発など多くの取引先／再委託先で構成させるビジネスにおいて、サプライチェーンのサイバーセキュリティを確保するには、取引先／再委託先を制度上どのように扱うかは非常に重要であるため。	いただいた意見については、詳細な制度設計等の検討に当たっての参考とさせていただきます。
31	制度構築方針(案)	9	制度の対象範囲	・企業は個社/(国内又は海外を含む)企業グループ/事業部等と★の取得範囲を柔軟に定めることができる。 ・適用範囲とするIT基盤等に接続等するが適用範囲には含めないという判断をしたものについて、ネットワーク機器等(例：VLAN、ファイアウォール)により、適用範囲との境界を技術的に 分離すること。(例：取得単位を国内の事業所とする場合、海外事業所との間の通信をネットワーク機器等により必要最小限にする) →「◆適用範囲に含むもの」の説明ではないと思いますので、「◆その他」として上に出してはいかがでしょうか。		いただいた意見も参考にしつつ、制度構築方針における該当箇所の修正を検討させていただきます。
32	制度構築方針(案)	11	制度の運用体制案	運用体制図に『スキームオーナーIPA（調整中）』とあるが、確定がいつになるのか不明である。	制度運営のガバナンス不確定は評価機関の中立性・紛争解決の設計に影響するため。	制度運用体制については、今後検討してまいります。
33	制度構築方針(案)	12	制度の対象とする組織	申請単位が『法人・グループ・事業部』と多様で、評価範囲外の弱点が残存する恐れがある。	柔軟性は利点だが、横断する共有基盤の責任が曖昧になり、評価範囲外の弱点が残存する恐れがあるため。	本制度において適用範囲を決定するに当たっては、ファイアウォール又はVLAN等により適用範囲内外の通信の制御等を行うことにより、適用範囲外に存在する脆弱性の影響を最小限にすることとしています。
34	制度構築方針(案)	12	制度の対象とする組織	再委託先の範疇には、中小企業もかなりの確率で入ってくるが、これはどのTier/レベルまでを対象にするのかを明確にしておかないと混乱が生じるのではないでしょうか。		本制度をどの範囲のサプライヤー企業にまで適用させるかについては、発注者側においてリスク等を判断の上決定することを想定しています。
35	制度構築方針(案)	12	制度の対象とする組織	右下注釈の「※取引先に対して、利用可能なセキュア環境を、発注者側から提供することなども考えられる。」についてどの部分の注釈かが分からない。 また、p.12では当該注釈が、制度が想定する対象事業者（赤枠）であることを示している様にみえるが、あくまでも発注者が管理する環境であり、受注者の「該当する★の対策範囲」の外であり、混乱を招く記載に見えるので、削除しては如何か。（p.8「制度の対象範囲」の図にも記載がない）	方針書であることは認識しているが、対象に関する誤認識を防ぐことが、事前準備の効率化の観点から重要であると考えるため。ま た、中小企業における課題については、明確な支援制度を記載することで、制度全体が推進しやすくなると考えるため。	いただいた意見も参考にしつつ、制度構築方針における該当箇所の修正を検討させていただきます。
36	制度構築方針(案)	12	制度の対象とする組織	評価取得の申請主体は、自社IT基盤を中心とした自社のセキュリティ対策の向上に責任を有する単位(基本的には法人単位、企業グループ単位又は事業部単位)とする。 ●本企業評価制度の取得は、今後、政府調達や、様々な分野のガイドラインにおいても、取得が推奨あるいは勧告など求められることになると思慮するが、その際においても、取得する側が柔軟に取得範囲を決めることが出来るようにしていただきたい。	様々な事業分野を抱える大企業においては、取得が求められる分野毎に柔軟な対応が必要と考えるため。	いただいた意見については、今後の検討の参考とさせていただきます。
37	制度構築方針(案)	13	制度において設ける段階	★３・★４間に★３． ５を置いてはどうでしょうか。 ★３． ５のレベルの評価は提出された「エビデンスの名称」、「エビデンスに基づく根拠」に対して適合基準を満たしているかを第三者評価をおこなうもので、★４のように、実地審査及び技術検証(脆弱性検査等)を伴わない評価法を提案します。	中小企業でセキュリティの専門家を持てない企業は自己適合宣言に２の足を踏んでしまいます。社外に依頼してもよいとしていますが、発注者の意向を配慮し、公正でなくなる可能性が高いと思います。すなわち、自己適合宣言では客観性がなく受注者側が自分に有利なように、または理解不足で判断してしまいがちです。また、第三者にエビデンスを提出することにより襟を正して自己チェックが行われるとも想定します。 ★４のように実地審査及び技術検証を実施しない分費用と時間の節約が期待されます。こうした提出エビデンスによる第三者評価は（一社）保健医療福祉情報安全管理適合性評価協会（ＨＩＳＰＲＯ）https://hispro.or.jp/index.html で実施されています。	いただいた意見については、今後の検討の参考とさせていただきます。
38	制度構築方針(案)	13	段階別評価の概要	３． ３． １段階別評価の概要において、★３、★４の定義が異なっているのは制度として整合性が取れていないのではないか。 ★３が「水準を目指す」と規定するのであれば★４も同様に規定すべきではないか。		いただいた意見も参考にしつつ、制度構築方針における該当箇所の修正を検討させていただきます。
39	制度構築方針(案)	13	段階別評価の概要	枠組みについて、以下のように出来ないか、ご検討をお願いしたいです ・現在の★4を★5とする ・ISMSを持っているかどうかを、★とは別に表す（★5I 等） ・★3の外部認証ありを、★4として新設 ・Pマークについて、上記の★4（外部認証あり★3）を前提とした枠組みにする（＝Pマーク所持は外部認証あり★3扱いとする） ・★3（または★3の外部認証あり）について、海外の会社（子会社など）も対象に出来るようにする →★3以上を、個人情報の保護に関する法律施行規則第十五条の対象として、個人情報の取り扱いを許可する		いただいた意見については、関連制度等との連携・整合の検討に当たっての参考とさせていただきます。
40	制度構築方針(案)	13	段階別評価の概要	実効性に関する技術的エビデンスの開示 ： 本制度の要求項目が、具体的にどのような攻撃手法をどの程度遮断できると想定しているのか、その技術的根拠を提示すべきである。		いただいた意見については、詳細な制度設計等の検討に当たっての参考とさせていただきます。
41	制度構築方針(案)	13	段階別評価の概要	★3/★4/★5の上下包含関係の説明に、移行・スキップ時の要件差分検証が不足ととらえるため、★4申請時に★3必須項目の達成証跡チェックリストを追加し、ギャップの是正計画の提出を義務づける必要がある。	★3を飛ばして★4取得するケースで、基礎項目の未達が隠れるリスクがあり、★3で求められる必須項目が確実に満たされているかを検証する仕組みが示されていないことが問題であるため。	★4を取得するためには、★4に区分された要求事項に加えて、★3に区分された要求事項についても、全て達成する必要があります。
42	制度構築方針(案)	13	段階別評価の概要	想定される脅威の分類が単純化されており、複合的・横断的なサプライチェーン攻撃を十分に捉えられていない。	実際の攻撃は、外部攻撃・内部不正・設定不備といった単一分類ではなく、正規アカウント侵害や委託先を踏み台とした横断的展開 として発生することが多い。脅威分類には侵害後の横展開や影響範囲の観点を含める必要がある。	いただいた意見については、詳細な制度設計等の検討に当たっての参考とさせていただきます。
43	制度構築方針(案)	13	段階別評価の概要	★による評価区分が示す意味（成熟度、運用実効性、リスク低減効果等）を明確に定義すべきである。	評価軸が曖昧なままでは、文書整備や形式的統制の達成が高評価につながり、実際の検知能力や侵害耐性を正しく反映できない。 攻撃検知、侵害後対応、委託先を含む横断的統制といった観点を評価に反映する必要がある。	いただいた意見については、詳細な制度設計等の検討に当たっての参考とさせていただきます。
44	制度構築方針(案)	13	段階別評価の概要	【想定される脅威】 ★3 『広く認知された脆弱性等を悪用する一般的なサイバー攻撃』とは具体的に何を指すのか。「広く認知された」とは単なる公開ではなく、悪用等が確認されて一般的な国民が認知するほどに知られた脆弱性を示すのか。その場合、等とは何を指すか。もしくは、広く認知された(脆弱性等を悪用する)一般的なサイバー攻撃を意味する場合、一般的なサイバー攻撃とは何か、非常に定義が不明確である。 ★4 供給停止等によりサプライチェーンに大きな影響をもたらす企業への攻撃及び機密情報等、情報漏えいにより大きな影響をもたらす資産への攻撃において、他の事項と異なり『サイバー攻撃』としていない理由はあるか。 ★5 未知の攻撃も含めた、高度なサイバー攻撃につき、未知の何を想定しているのか。未知の脆弱性か、未知の手法か、そもそも未知とは何か。		いただいた意見については、詳細な制度設計等の検討に当たっての参考とさせていただきます。 また、★5については、令和８年度以降に具体的に検討してまいります。
45	制度構築方針(案)	13	段階別評価の概要	脅威に対する達成水準(イメージ)】 ・ここでいう「取引先」とは、3.2に示す取引先であると定義されているならば、取引先の対策状況の把握は、受注者もまた発注者の対策状況を把握せよ、という理解でよいか。 ・取引先等への指導や共同での訓練の実施などは、発注者の優越的地位の乱用に繋がらないか。		事業継続リスクや情報管理リスクを考慮の上、必要に応じて受注者から発注者の対策状況を確認することも考えられますが、本制度は、基本的には発注者の立場で受注者の対策状況を確認することを主に想定しています。 いただいた意見については、今後の検討の参考とさせていただきます。
46	制度構築方針(案)	14	★3・★4適用の考え方(例)	制度の目的はサプライチェーン全体のセキュリティ強化ですが、 リスクが極小の企業に★3を要求することは本来の目的に合致せず、制度の実効性と現場負担の両面で問題が生じます。 そのため、★3未満でもよい企業の基準を明確に示し、 「注記ではなくフロー図に明記する」という形で制度に反映していただくことを要望いたします。		いただいた意見については、詳細な制度設計等の検討に当たっての参考とさせていただきます。
47	制度構築方針(案)	14	★3・★4適用の考え方(例)	★3・★4適用の判定フローの各リスクに関する部分で、例示(判断において考慮すべき観点の例)に、「同業他社からの調達可否」「在庫確保の困難さ」程度にとどまっており、代替可能性の評価が簡略化しているため、API連携依存度指標やRTO/RPO要求を判定に追加し、事業影響評価（BIA）との整合を図る必要がある。	『同業他社からの調達可否』『在庫確保の困難さ』のみでは連携APIや運用委託の依存度を反映し切れないため。	制度構築方針(案)P.15記載のフロー図はあくまで例示であり、発注企業ごとに★3・★4の適用に当たって具体的な指標を定めることは否定されるものではありません。
48	制度構築方針(案)	14	★3・★4適用の考え方(例)	意見：「情報管理リスク」や「事業継続リスク」の判断基準が発注者に委ねられているため、発注者のリスク回避志向によって、過剰に★4（第三者評価）を要求される懸念があります。 フロー図においては「重要な業務」や「重大な影響」といった定性的な判断基準が示されています。しかし、発注側企業が安全性を最優先して（安全側に倒して）判断した場合、本来は★3で十分なサプライヤーに対しても、コストのかかる★4が要求されてしまう可能性があります。 サプライヤーを保護する観点から、発注者が不当に高いレベルを要求しないようにするためのガイドラインや、牽制機能を設けるべきだと考えています。		いただいた意見については、詳細な制度設計等の検討に当たっての参考とさせていただきます。
49	制度構築方針(案)	14	★3・★4適用の考え方(例)	「事業継続リスク」「情報管理リスク」「要求する段階」に関して、発注者目線での要求事項が複数社からの要求で異なってしまうケースが出てきた場合、どのレベルに合わせるべきかが明確になっていなように見えます。サプライヤー側での混乱を招く要素になっているのではないでしょうか。		いただいた意見については、詳細な制度設計等の検討に当たっての参考とさせていただきます。
50	制度構築方針(案)	14	★3・★4適用の考え方(例)	■ 意見内容 中小企業は★3・★4 のいずれを取得すべきか判断に迷うと思われる。その基準や目安を、もう少し明確に示すべき	フローチャートで「★3・★4 適用の考え方（例） 」が示されているが、基準が曖昧であり、中小企業にとっては、いずれを選ぶべきか判断が困難と予想される。★4 はもとより★3 すら、取得が困難な場合も少なくないと思われるため、2025 年度および 2026 年度の実証結果を踏まえ、★3・★4 それぞれの取得対象企業例（業種、従業員数、その他条件等）を示すなど、より具体的かつ現実的な判断基準を示されたい。	制度構築方針(案)P.14記載のフローチャートについては、あくまで考え方の一例であり、★3・★4の適用については、当該ページも参考に、各組織のリスク判断等により決定されることを想定しています。
51	制度構築方針(案)	14	★3・★4適用の考え方(例)	本制度において、星獲得を求める取引先は「事業活動上、重要な業務の多くがIT基盤に依存している取引先」であり、全ての取引先に一律で要求するものではない、という理解で差し支えないか確認したい。 また、メールも本制度の対象となることから、契約書、設計書等の機密情報をメールでやり取りしている取引関係については、実質的に制度対象となり得る点を、より明確に示した方が制度理解が進むと考える。	制度の対象範囲が曖昧な場合、「過剰要求」「逆に重要取引先への要求漏れ」が発生する恐れがあるため、発注者側が判断しやすい説明が必要と考える。	御認識のとおり、本制度は全ての取引先に一律で要求することは想定していません。また、制度構築方針(案)P.14記載のフローチャートについては、あくまで考え方の一例であり、★3・★4の適用については、当該ページも参考に、各組織のリスク判断等により決定されることを想定しています。
52	制度構築方針(案)	14	★3・★4適用の考え方(例)	P.15で提示されている指標を参考に発注者が判断する方針には賛同する。 一方で、本制度の策定にあたり、経済産業省として想定している「重要な機密情報」の具体例を明示することが、制度の実務適用において有効と考える。 また、「アクセス可否」だけでなく、当該情報を保持（保管）している場合も同様にリスク判断の対象となると考えられるが、その観点が指標例に明確に記載されていないため、追記を検討していただきたい。	発注者・受注者双方で重要性判断の認識を揃えるためには、一定の共通理解が必要であるため。 （想定される機密情報例） 「個人情報」「契約・取引情報」「財務・経営情報」「技術・知的財産情報」「セキュリティ関連情報」「人事・労務情報」	いただいた意見については、詳細な制度設計等の検討に当たっての参考とさせていただきます。
53	制度構築方針(案)	14	★3・★4適用の考え方(例)	「必要に応じて適用段階や要求水準等を調整すること」や、「対策強度が不足している場合は（中略）、それぞれの要求事項へ必要な対策を上乗せすることも想定される」という内容に賛同する。運用開始にあたり、企業等の理解を深めるよう導入促進策の中で強調、周知いただくことを望む。	取引内容やリスク等に応じて、項目毎には★４以上のセキュリティ対策が必要となる可能性が十分に考えられるところ、★４を取ることで十分なセキュリティ対策を実施しているという誤解を与えない記載が必要なため。	いただいた意見については、詳細な制度設計等の検討に当たっての参考とさせていただきます。
54	制度構築方針(案)	14	★3・★4適用の考え方(例)	情報管理リスクが初出なので、「2.2.1 対象とするリスクの範囲」にあるデータ保護リスクと不正アクセスを指すことを注釈でいれてはいかがでしょうか。		いただいた意見も参考にしつつ、制度構築方針における該当箇所の修正を検討させていただきます。

No.	該当箇所			寄せられた御意見の概要	理由	提出意見に対する考え方
	該当文書	該当ページ又は項番	該当項目			
55	制度構築方針(案)	14	★3・★4適用の考え方(例)	★3か★4のどちらかが適用されるフローになっています。どちらも適用されない結果もあると思いますので、フローに追加していただきたいです。		[註]のとおり、重要度が高くない調達等については、本フローの対象とせず、★3・★4を適用しないことが想定されます。
56	制度構築方針(案)	14	再委託先への適用の考え方(例)	★4評価基準(案)にある、★4『重要な取引先の対策状況把握』の頻度が年1回以上と定めているが、把握頻度が最低1回となるリスクがあるため、重要度に応じた頻度テーブル（高：四半期、中：半期、低：年1回）を追加し、重大変更時の臨時確認を義務化するべきである。	高変化のクラウドやMSPでは年1回ではリスク把握が追いつかない可能性があるため。	今回の要求事項・評価基準では、取得希望組織が一律で満たすべきベースラインとしての基準であることを考慮し、最低限年1回重要な取引先の対策状況を確認することとしています。各取得希望組織の任意の取り組みとして、それ以上の頻度等で確認を行うことは否定されるものではありません。
57	制度構築方針(案)	14	再委託先への適用の考え方(例)	どの階層まで評価要求を適用するかの基準を明確にするとともに、再委託先の適用への対応状況を委託者が確認し、 その情報を基に委託判断を行う仕組みが望ましいです。	多層構造の取引において、適用範囲が明示されるとともに対応状況が確認できれば、過度な調査や過小な管理を避けつつ、 リスクの高い箇所に的確に対策を集中できます。結果として、利用企業は効率的にサプライチェーンの健全性を高めることが可能となります。	本制度をどの範囲のサプライヤー企業にまで適用させるかについては、発注者側においてリスク等を判断の上決定することを想定しています。
58	制度構築方針(案)	14	再委託先への適用の考え方(例)	本制度は、サプライチェーンにおける発注者・受注者の関係性を前提に整理されていると理解している。 一方で、事業形態上「自社が発注者となるが、他社から業務を受注する立場にない企業」の場合、本制度における星獲得は想定されていない、もしくは必須ではないとの理解で差し支えないか確認したい。	企業によっては、サプライチェーン上で情報を受領・保持する立場にあるものの、いわゆる「受注者」として業務委託を受ける形態ではないケースも存在するため、制度の想定範囲を明確にする必要があると考える。	本制度は主に受注者側での活用が想定されますが、サプライチェーン全体での★適用によるセキュリティ対策を企図して発注者側でも★を取得するなど、発注者側において★を取得することを妨げるものではありません。
59	制度構築方針(案)	14	★3・★4適用の考え方(例)	本制度を実効性のあるものとするためには、発注側企業における★3の位置付けについても一定の考え方を示すことが重要であると考える。 例えば、発注側企業がサプライヤーに対して、すべての取引において一律に★4の取得を求めるのではなく、 取引内容やリスクに応じて、★3を一定水準のセキュリティ対策を実施している状態として評価・受容すること ★3を取得している事業者については、取引継続や段階的な高度化（将来的な★4取得）を前提とした関係構築を行うこと といった運用が想定されることを、制度上またはガイダンス等で示すことにより、★3が実務上も活用される段階として機能しやすくなると考える。 サプライチェーン全体のセキュリティ強化を実現するためには、取得要件の厳格さのみならず、発注側・受注側双方にとって現実的で分かりやすい制度設計が重要である。★3と★4の役割整理、評価方法の段階化、および発注側における活用イメージの明確化について、前向きに検討いただきたい。	本制度の目的であるサプライチェーン全体のセキュリティ対策水準の底上げを達成するためには、中小企業を含む幅広い事業者が参加可能な制度設計が不可欠である。★3を取得しやすい初期段階として明確に位置付け、発注側においても適切に評価・活用される仕組みとすることが、制度の普及および実効性向上につながると考えるため。	いただいた意見については、詳細な制度設計等の検討に当たっての参考とさせていただきます。
60	制度構築方針(案)	16	要求事項・評価基準	要求事項の一覧で大分類「インシデントへの対応」の★4の追加項目がないのが考慮不足である。	インシデント対応は★3よりも高度化が必要だが差分が示されていないため。	いただいた意見については、今後の検討の参考とさせていただきます。
61	制度構築方針(案)	16	要求事項・評価基準	メールセキュリティ（DMARC/SPF/DKIM）の明示がない。	ビジネスメール詐欺対策の実害が大きいため。	いただいた意見については、今後の検討の参考とさせていただきます。
62	制度構築方針(案)	16	要求事項・評価基準	大分類「攻撃等の防御」の★3「不正アクセスに対する基礎的な防御」、★4「多層防御による侵入リスクの低減」に、クラウドSaaSの監査ログの扱いが不明確のため、主要SaaSの監査ログ取得・保持期間・エクスポート要件を明記するべきである。	SaaS提供者が保持する監査ログの取り扱いが重要であるため。	いただいた意見については、今後の検討の参考とさせていただきます。
63	制度構築方針(案)	16	要求事項・評価基準	大分類「攻撃等の防御」の★3「不正アクセスに対する基礎的な防御」、★4「多層防御による侵入リスクの低減」に、MFA必須化の明確化が不足しているので、★3で管理者・外部、★4で全社SaaS/リモートに拡張するべきである。	初期侵入の主要経路であるため。	要求事項・評価基準においては、★3では重要な情報を取り扱うと考えられるクラウドサービスへのアクセスに(No.4-1-3-2)、★4ではそれに加えて、インターネット経由での管理者のアクセス及び機密区分が高い情報を扱うシステムへのユーザのアクセスに対して、多要素認証を使用することとしています。 また、制度構築方針(案)P.16に記載の表については、あくまで代表的な要求事項・評価基準を抽出したイメージとなっています。
64	制度構築方針(案)	16	要求事項・評価基準	大分類「攻撃等の防御」の★4「多層防御による侵入リスクの低減」に鍵管理の詳細が不足である。	鍵ライフサイクルが対策の要であるため。	いただいた意見については、今後の検討の参考とさせていただきます。
65	制度構築方針(案)	17	ガイダンス資料の整備	自己評価、外部審査、技術審査におけるガイダンスが作成される際、 ・要求事項を満足すると判断する水準 ・要求事項が満たせない場合の代替施策 について、明確に定義していただきたい。		いただいた意見については、ガイダンス資料の作成に当たっての参考とさせていただきます。
66	制度構築方針(案)	17	ガイダンス資料の整備	ガイダンス資料が『今後策定する予定』となっており、具体的な公開時期・版管理のスケジュールが明確になっていない。	評価の一貫性確保にはガイダンスの参照版管理が不可欠であるため。	いただいた意見を踏まえ、制度構築方針P.39におけるスケジュールの説明を修正しました。
67	制度構築方針(案)	17	ガイダンス資料の整備	要求事項の粒度・判断基準の明確化、項目間の整合性の精緻化を要望します。	企業が自社の現状を正確に自己評価し、過不足なく改善計画を立てられるよう、解釈のばらつきを減らすことが重要です。 インシデント対応体制の整備前提が要求に内在している箇所は、明示されている方が利用企業の混乱を避けられます。	制度構築方針(案)P.17記載のとおり、今後要求事項・評価基準に係る評価方法や取組み事例等を具体的に解説する各種ガイダンス資料等を整備する予定です。いただいた意見については、当該ガイダンス資料等の作成に当たっての参考とさせていただきます。
68	制度構築方針(案)	17	ガイダンス資料の整備	自己評価ガイドや第三者評価ガイド、技術検証ガイドの内容に、評価方法の他に代替案の例示や代替案の考え方を含めることで、★3-4の要求事項への達成手段の具体化と柔軟化を促進して欲しい。	IT環境は事業内容や企業体毎に異なり、評価ガイドの通りに要求事項に遵守できるとは限らない為。 ISMS（ISO/IEC 27001）やPCI DSSにおいて、代替コントロール（要求事項がそのまま満たすことが技術的/ビジネス的に困難な場合に、該当要件と同等のリスク軽減効果を持つ別の対策を導入し、要件を満たす）の概念が存在し、準拠審査の際に何らかの形で採用される。 特にPCI DSSでは、具体的な代替コントロールの考え方が規定化されている。 参照：https://pcireadycloud.com/blog/2019/04/04/2770/	本制度は大企業から中小企業まで一律で満たすべきベースラインを定めているところ、要求事項が求めるセキュリティ水準を多くの者が達成できるよう、実証事業での結果を取り得る手段の多様性に配慮して適宜代替策を追加の上、要求事項・評価基準(案)を作成したところです。制度構築方針(案)P.17記載のとおり、今後ガイダンス資料を整備する予定であり、当該資料において実装例等の拡充を図ってまいります。
69	制度構築方針(案)	17	ガイダンス資料の整備	「• ★３・★４要求事項・評価基準に加え（中略）※ 下記の図はあくまで本方針作成時点におけるイメージであり、完成後の文書とは異なる場合がある。」の下に、二つ目の「・」として以下を追加。 ・各種のガイダンス、ガイドラインについては、安全保障上のリスク担保についても説明する。	サプライチェーン全体でのセキュリティリスクの低減においては、安全保障リスクの考慮も不可欠であるため、安全保障リスクを担保する何かしらの仕組みが必要と考えます。 他方、当該制度は、サプライチェーン企業のセキュリティ対策を評価・可視化することによる対策水準向上の促進を目的としており、JC-STAR等国による評価制度とも趣旨が異なると理解しております。そこで、補完的に各業界向けセキュリティガイドライン等にて、安全保障上のリスク担保につき明記することを引き続き検討されることが重要と考えます。	いただいた意見については、今後の検討の参考とさせていただきます。
70	制度構築方針(案)	17	ガイダンス資料の整備	★４の取得にあたっては脆弱性テストを含む技術検証付きの第三者評価の実施を予定されていますが、技術検証ガイドの内容は示されていないところ、以下についてご教示いただきたい。 -技術検証ガイドの公表予定時期 -技術検証ガイドを策定する際に参照を予定しているベンチマーク -技術検証は、自社で実施している脆弱性診断の結果等の証跡を提出することによる代替等は可能か。	★４の取得を検討する事業者において、技術検証の具体的な内容や要求水準が不明確なままでは、制度対応への準備が困難と考えるため。	技術検証等の詳細については、ガイダンス資料に記載する予定です。ガイダンス資料の公開予定時期はスケジュールに記載いたします。 また、制度構築方針P.23記載のとおり、制度が定める条件を満たす場合は、別途実施した脆弱性診断の結果（証跡）を評価機関に提出し、確認を受けることで、技術検証の実施に代替することが可能となる予定です。
71	制度構築方針(案)	17	ガイダンス資料の整備	ガイダンス資料（★3・★4自己評価ガイド、第三者評価ガイド、技術検証ガイド等）について、今後の策定・公開スケジュールの目安があれば示していただきたい。 また、これらガイダンスを活用した人材育成・教育プログラムとの連携について、制度上どのように位置づける想定かを確認したい。	ガイダンス資料は制度の実効性を左右する重要な要素であり、「社内教育」「外部支援サービス」「セキュリティ専門家の育成」との連動が進むことで、制度の普及スピードと定着度が大きく向上すると考えられるため。	技術検証等の詳細については、ガイダンス資料に記載する予定です。ガイダンス資料の公開予定時期はスケジュールに記載いたします。
72	制度構築方針(案)	17	ガイダンス資料の整備	現状のアセスメントシートには、用語の使い方が項目によって異なるシーンが散見される。 この表現の差異を全項目で統一することは今後の改版を考慮すると望ましくない。むしろ、用語集のシートを別途作成し、正確な定義はそちらに記述することが望ましいと考える。 その上で、本シートには「用語」カラムを作成し、用語集シートに解説があることを明示する。これにより用語の誤解を避け、評価の公平性を担保できると考える。		制度構築方針(案)P.17記載のとおり、今後要求事項・評価基準を具体的に解説する各種ガイダンス資料等を整備する予定です。いただいた意見については、当該ガイダンス資料等の作成に当たっての参考とさせていただきます。
73	制度構築方針(案)	17	ガイダンス資料の整備	現行の評価制度の基準は、達成すべき状態（アウトカム）や達成条件が明確な基準というよりも、実施すべきセキュリティ管理策の列挙として整理されているように見受けられます。この場合、発注側・受託側の双方において同一の管理策を参照しても解釈が分かれやすく、取引実務における共通理解の形成が困難となる懸念があります。 ついては、要求事項の記述にあたり、管理策の列挙にとどまらず、達成すべき状態や確認観点等を可能な範囲で明確化し、実務上の判断が一致しやすい形で整理いただくことを要望します。あわせて、攻撃手法の変化を踏まえ、管理策・評価内容の定期的な見直し（改善）を前提とした制度設計とすることが重要と考えます。		制度構築方針(案)P.17記載のとおり、今後要求事項・評価基準に係る評価方法や取組み事例等を具体的に解説する各種ガイダンス資料等を整備する予定です。いただいた意見については、当該ガイダンス資料等の作成に当たっての参考とさせていただきます。 また、制度構築方針(案)P.16記載のとおり、要求事項・評価基準についてはサイバーセキュリティの動向等を生前、今後定期的に見直しを実施することを想定しています。
74	制度構築方針(案)	18	各段階の評価スキームの概要	自己評価結果に関して、使用したツールやサービスの明記を必須にして、第3者の客観的なデータをベースにしたことを明解にすべきでは。さらに言うと、エビデンスの提出を求めるべきで、それによって誰が見ても納得できる評価になると考えます。		いただいた意見については、自己評価実施時の証跡の取り扱いの検討に当たっての参考とさせていただきます。
75	制度構築方針(案)	18	各段階の評価スキームの概要 - ★3	星3の評価プロセスにおいて、適用範囲外とのネットワーク分離（VLANやFW設定等）が適切に行われているかを、文書確認だけでなく、より実効性のある方法で確認する仕組み（または専門家による現地視察の必須化など）を明確にしていただきたい。	資料3の実証結果では、適用範囲外を設けた企業の多くがファイアウォール等で分離していると回答しているが、その設定が「実際に侵入を防げる設定」になっているかどうかの技術的有効性までは検証されていない懸念がある 。星3は「自己評価＋専門家の文書確認」が主となるスキームだが 、専門家が現地を見ずにネットワーク図や設定書の文書だけで「論理的な分離の有効性」を担保するのは困難である。 分離が不十分なまま認証が付与されると、そこがサプライチェーン全体のセキュリティホールになり得るためである。	本制度では、★4の評価スキームにおいて、取得希望組織がインターネットに公開している機器のうち、脆弱性を悪用等された場合に組織内部に侵入されるリスクが高い機器(例：VPN装置、ルータ)を対象とした技術検証の実施を行うことにより、取得希望組織における技術的対策の信頼性を担保を図ることとしています。 また、★3においては、セキュリティ専門家による確認・助言を受けることで、取得希望組織における自己評価結果の信頼性の担保を図ることとしています。
76	制度構築方針(案)	18	各段階の評価スキームの概要 - ★3	★3については、より参加しやすい初期段階としての位置付けを明確化し、★4において第三者評価による客観性・信頼性を担保するという段階的な整理が望ましい。具体的には、★3について以下のような運用・制度設計を検討いただきたい。 ・制度で定める要求事項に基づく、標準化されたチェックリスト形式による自己点検を基本とすること ・組織代表者等による**自己宣誓（セルフアテステーション）**により、評価結果を確定すること ・セキュリティ専門家による確認や助言については、必須ではなく任意又は段階的な選択肢とすること これにより、中小企業にとっての初期的な参入障壁を下げつつ、制度への参加を促進し、将来的に★4へのステップアップを目指す導線を明確にすることが可能になると考える。	本制度の目的であるサプライチェーン全体のセキュリティ対策水準の底上げを達成するためには、中小企業を含む幅広い事業者が参加可能な制度設計が不可欠である。★3を取得しやすい初期段階として明確に位置付け、発注側においても適切に評価・活用される仕組みとすることが、制度の普及および実効性向上につながると考えるため。	いただいた意見については、詳細な制度設計等の検討に当たっての参考とさせていただきます。 なお、★3における評価スキームでは、制度構築方針(案)P.18記載のとおり、取得希望組織の自己評価を前提に評価結果について各取得希望組織が責任を有することとしており、その点を明確にするために、★3取得に当たっては経営層による自己適合宣誓を実施することを想定しています。 そのうえで、★3においても自己評価結果についてセキュリティ専門家の助言・確認を受けることで、評価の有効性・信頼性を確保するとともに、中小企業の継続的なセキュリテレベルの向上を図ることとしています。
77	制度構築方針(案)	18	各段階の評価スキームの概要 - ★3	以前は自己確認のみであった★3の認定プロセスに、突然取って付けたかの如く専門家確認"が追加された経緯を明確にしていただきたい。		令和7年4月公表の「サプライチェーン強化に向けたセキュリティ対策評価制度構築に向けた中間取りまとめ」においても★3の評価スキームにおいてセキュリティ専門家による確認等を必須としていましたが、今回の制度構築方針(案)では、その点を明確にするために、★3の評価スキームを「専門家確認付き自己評価」としています。

No.	該当箇所			寄せられた御意見の概要	理由	提出意見に対する考え方
	該当文書	該当ページ又は項番	該当項目			
78	制度構築方針(案)	18	各段階の評価スキームの概要 - ★3	「3.5.1 各段階の評価スキームの概要-★3」では、組織内(企業グループ内含む)の情報処理安全確保支援士（以下、支援士）による「確認・助言」を実施する旨、記載されている。 専門人材の活用という観点から組織内支援士の活用は、適切であると考えられる。 しかしながら、「確認」時において、組織の利益と支援士の法的義務（情報処理の促進に関する法律(以下、情促法)第二十一条：信用失墜行為の禁止）が対立する恐れがあるという 構造的な問題が生じる。対立した場合の支援士保護が記載されていない点、深く憂慮する。 支援士は、情促法により「サイバーセキュリティの確保を支援する(第三条)」と規定された業務に関し「信用失墜行為の禁止(第二十一条)」という義務を負う。同時に情報処理安全確保支援士倫理綱領を遵守し、公正・誠実に行動することを求 められる。 したがって、支援士は本制度の「確認」において、制度事務局へ提出する内容について不正を覚知・確認した場合に是正を要求すること、制度事務局へ提出する内容に関して組織 が支援士に対して署名を強制する等の不当な業務を命令した場合に署名を拒否することも義務付けられると考えられる。 一方、方針(案)では、法や倫理綱領に沿って正当な業務を実施した支援士の保護が明文化されていない。「確認」を実施する支援士が保護されない場合、本制度の運用が形骸化し、結果として経済・社会全体でのサイバーレジリエンスの強化という目的が達成できない恐れがある。ひいては、情促法で規定された国家資格である支援士の信頼性も毀損しかねない。これは容易に予見される。 以上のことから、本制度において「正当な職務を遂行した支援士に対し、解雇、降格、減給、配置転換その他一切の不利益な取扱いを禁ずる」規定の明文化と不正を覚知した場合や不当な業務命令があった場合の対処をガイダンスに明記することを提案する。 当該提案の実現により、支援士が公正かつ誠実に「確認」業務を遂行できる環境が整備され、本制度が目指す「サプライチェーン全体のサイバーレジリエンス強化」に真に寄与するものと確信する。	支援士の法的義務と組織利益の対立に関して未検討のまま放置された場合、国が普及を目指している支援士制度自体の衰退を招く恐れがある。結果として本制度も形骸化する恐れがあるため、意見する	いただいた意見については、詳細な制度設計等の検討に当たっての参考とさせていただきます。
79	制度構築方針(案)	18	各段階の評価スキームの概要 - ★3	「3.5.3 評価の考え方 – 評価の有効期間等」では、「★の取消し等」について「内部通報等により、取得組織において虚偽報告、情報隠蔽等の不正行為が確認された場合、評価機関又は制度事務局から★の一時停止又は取消しを行う場合がある」と記載されている。本制度の信頼性担保のため、当該記載は適切であると考えられる。 しかしながら「内部通報等」という記載は、「不正行為の通報」が公益通報者保護法上の「公益通報」に該当するか否か、詳細判然としない。これを踏まえ、以下の点について明らかにすべきである。 ➢ 不正行為の通報は、公益通報に該当するのか否かを明記すること。 公益通報に該当しない場合は、通報者は公益通報者保護法で保護されないこと、および他の法律等によって、通報者が法的に保護されるか否かを明記すること。 ➢ 情報処理安全確保支援士(以下、支援士)は、情報処理の促進に関する法律(以下、情促法)「信用失墜行為の禁止(第二十一条)」および「情報処理安全確保支援士 倫理綱領」を遵守しなければならない。これに基づき、不正等を覚知・確認した支援士は、実質的に通報義務を負う旨を明記すること。 ➢ 不正行為を通報した支援士は、組織から情促法「秘密保持義務(第二十二条、第七十六条第二項に基づく親告罪)」違反で告訴される場合がある旨を明記すること。 併せて、不正行為の通報が正当な理由に該当せず、情促法で規定された秘密保持義務違反であると司法が認定した場合、通報を実施した支援士は刑事罰に処されることがあり得ることを明記すること。 以上のことから、本制度「★3」のセキュリティ専門家における支援士と民間資格者それぞれの法的取扱い、および「内部通報等」の目的、通報者保護、通報方法に関して、ガイダンスに明記することを提案する。 尚、上述の通り国家資格である支援士とその他民間資格者の間で心理的、経済的負担に差が生じていると考えられる。この差は、本制度の確認・助言業務において、支援士に対してのみ合理的な根拠のない差別的取扱いを生じることになりかねず、法的安定性の観点から深く憂慮する。	内部通報等における通報者保護や支援士の法的リスクが未検討で明文化されないまま放置されると、内部通報等が形骸化する恐れがある。結果として本制度も形骸化する恐れがあるため、意見する。	いただいた意見については、詳細な制度設計等の検討に当たっての参考とさせていただきます。
80	制度構築方針(案)	18	各段階の評価スキームの概要 - ★3	18 ページの図中におけるセキュリティ専門家(以下、専門家)の役割は「取得希望組織の自己評価結果の確認・助言を実施する」と記載されている。本制度の信頼性を担保する観点から専門家による確認・助言といった「支援」を行うことは、適切であると考えられる。 しかしながら、以下の点が不明確であり、経営層の誤認を招いて制度自体の信頼性を低下させ得る制度設計となっていると推察される点、深く憂慮する。 ➢ 制度上、★3 の評価結果提出内容の最終責任は評価主体である取得希望組織が負う。 一方、18 ページのスキーム説明では「最終的に制度事務局へ提出する内容に関して了承した場合に署名を実施」とあり、専門家の署名が提出の必須条件である。 したがって、実質的な最終責任は「署名した専門家」にあると言わざるを得ない。万一の不正等発覚時に制度事務局は「署名した専門家」を調査対象とし、追及することは容易に予見される。この点は、実質的な責任の所在が「署名した専門家」にあるという推察を補強するものである。 ➢ 制度上の★3 における「最終的に制度事務局へ提出する内容に関して了承し署名」する程度の「確認」とは、一般的に規定された要求事項(評価基準)をガイダンスに沿って、独立した立場で主体的に聴取や収集した証跡などを基にして「確かめる行為(Verification)」を指すと考えられる。一方、23 ページの評価の実施内容では、「1-2 日程度(想定)の所要期間」を以て「主に記載内容に矛盾がないか、評価基準から見て十分な事項が記されているかの確認」を行うことが記載されており「提出内容の表面的な点検・照合をする行為(Check)」に相当する内容が制度上の想定と見受けられる。「提出内容の表面的な点検・照合をする行為(Check)」の結果に関して、実質的な最終責任を有する専門家が了承し署名する行為自体の目的が不明確である。 ➢ 制度上★3 は登録機関へ提出する評価結果(セキュリティ専門家による署名を含むもの)を根拠に「経営層による自己適合宣誓」が行われるものと解される。その際、経営層が「提出内容の表面的な点検・照合をする行為(Check)」の結果を「確かめる行為(Verification)」と誤認し、専門家による署名を信頼(Trust)して、自己適合宣誓することが容易に予見される。これは、制度設計上の瑕疵になりうると考えられる。 以上のことから、専門家の目的、役割、および責任の明確化を提案する。具体的には「取得希望組織が実施した自己評価を経営層が自己適合宣誓」した結果を登録するという本制度の趣旨に沿って、★3 における専門家による署名は「確認」ではなく、「助言(Advisory)」を実施した証跡として、署名させることを提案する。 明確化を行うことで、役割の誤認を防ぎ、本制度が目指す「サプライチェーン全体のサイバーレジリエンス強化」に真に寄与するものと確信する。	★3 において経営層が「提出内容の表面的な点検・照合をする行為(Check)」の結果を「確かめる行為(Verification)」と誤認し、専門家による署名を信頼(Trust)して、自己適合宣誓することが容易に予見される。制度設計上の瑕疵になりうることから、意見する	いただいた意見については、詳細な制度設計等の検討に当たっての参考とさせていただきます。
81	制度構築方針(案)	18	各段階の評価スキームの概要 - ★3	しかしながら専門家の要件において、法的責任を負う支援士と法的責任を負わない民間資格者の混在は、以下の構造的問題が生じ制度設計上の瑕疵となりうる点、深く憂慮する。 ➢ 18 ページでは「確認・助言」を業務として想定している一方で、20 ページの「専門家及び作業従事者を対象とした研修」の「目的」には、「★3 の評価者として・・・」との記載がある。これは誤記ではなく「最終的に制度事務局へ提出する内容に関して了承した場合に署名を実施」させ、「専門家が★3 の実質的な評価主体として業務に当たらせ、その責任を負わせる」という制度側の意図が反映されたものと解される。 専門家の責任は「明示的には確認・助言に係る責任」であるが、「実質的には評価主体としての責任」を負う点、構造的に不整合が生じている。 ➢ 23 ページでは、★3 における専門家の「確認」は、「1-2 日程度(想定)の所要期間」を以て「主に記載内容に矛盾がないか、評価基準から見て十分な事項が記されている かの確認」を行うと記載されており、実態は「提出内容の表面的な点検・照合する行為(Check)」に相当する。前項にて述べた専門家の実質的な責任と業務内容に乖離があり、看過し難い構造的問題を内包している。 ➢ 上述の構造的な問題を放置した場合、制度設計上「提出内容の表面的な点検・照合を行ったことを以て、実質的に評価した」ことを「最終的に制度事務局へ提出する内容 に関して了承した場合に署名を実施」させることに関して、「支援士のみに法的義務を以て本制度を超える信頼性担保を強制される一方、民間資格者には法的義務はないことから強制しない」という著しい不均衡が生じる恐れがある。この構造的問題は 制度側が支援士に対して合理的な根拠のない差別的取扱いを生じさせるものであり、法の下の平等の観点から、慎重な検討を要する。 以上のことから、本制度の信頼性担保、支援士の差別的取扱い解消を目的として★3 の実質的な評価主体となるセキュリティ専門家は「法的責任を負う国家資格保有者である支援士のみ」に限定することを提案する。 併せて、不足しているセキュリティ専門家数については一定の基準を満たす民間資格保有者を支援士として登録させることで、セキュリティ専門家に対して一律の法的責任を課し、法的安定性の担保、セキュリティ専門家数の確保を目指すことを提案する。 法的安定性の担保やセキュリティ専門家の確保を実現することで本制度の円滑な運用を可能とするのみならず、2030年までに情報処理安全確保支援士を5万人まで増加させるという政府目標の達成手段となり得る。結果として、本制度が目指す「サプライチェーン全体のサイバーレジリエンス強化」に真に寄与するものと確信する。	法的責任を負う支援士と法的責任を負わない民間資格者の混在は、構造的問題が生じ制度設計上の瑕疵となりうる恐れがあるため、意見する	いただいた意見については、詳細な制度設計等の検討に当たっての参考とさせていただきます。
82	制度構築方針(案)	18	各段階の評価スキームの概要 - ★3	★3の専門家確認付き自己評価の手順③で『経営層による自己適合宣誓』の具体要件は、どの程度の粒度で責任を明確化するかが不明確のため、宣誓書に『適用範囲、未達項目、是正期限、予算配分』の必須記載欄を追加し、虚偽時のペナルティを明文化する必要がある。	宣誓の粒度が低いと形式的なチェックになり、是正力が弱まるため。	いただいた意見については、詳細な制度設計等の検討に当たっての参考とさせていただきます。
83	制度構築方針(案)	18	各段階の評価スキームの概要 - ★3	★3は「専門家確認付き自己評価」として、実地審査や技術検証を要求していない（P18の★3フロー参照）。このため証跡の信頼性確保が弱くなる恐れがある。最低限のリモート実機確認（画面共有等）を要件化し、重大な不一致が判明した場合は臨時のオンサイト確認へ引き上げる基準を明記すべきである。	証跡の信頼性確保に課題があるため。	いただいた意見については、詳細な制度設計等の検討に当たっての参考とさせていただきます。
84	制度構築方針(案)	18	各段階の評価スキームの概要 - ★3	制度では、自己評価結果に虚偽やその他の不正が発覚した場合のペナルティが「★の取り消しのみ」とされている。しかし、この措置だけではペナルティが軽く、制度を悪用する主体が出現する恐れがある。制度の信頼性を確保するため、★取り消しに加え、一定期間の再申請禁止や公表など、より厳格な措置を検討すべき。	ペナルティが軽い場合、制度を悪用する主体が出現する恐れがあり、制度の信頼性が損なわれる。厳格な措置により、抑止力を高める必要があるため。	いただいた意見については、詳細な制度設計等の検討に当たっての参考とさせていただきます。
85	制度構築方針(案)	18	各段階の評価スキームの概要 - ★3	★3取得時に制度事務局へ提出するシートの内容について、事務局が妥当性を確認しない場合、虚偽申請のリスクが高まり、制度の信用性が損なわれる可能性がある。最低限のチェック体制や、ランダム監査の導入を検討すべき。	事務局が確認を行わない場合、虚偽申請のリスクが高まり、制度の信用性が低下する。最低限のチェック体制を整えることで、制度の信頼性を担保する必要があるため。	いただいた意見については、詳細な制度設計等の検討に当たっての参考とさせていただきます。
86	制度構築方針(案)	18	各段階の評価スキームの概要 - ★3	【意見内容】 「経営層による自己適合宣言を経た取得希望組織として実施する評価のことを指し、組織内のセキュリティを担当する担当者や部門が独自に実施する評価は含まれない。」とありますが、以下のいずれの意味であるか分かりづらく、誤解を招くことが懸念されます。 １．経営層が関与しない、現場部門の専行による評価は不可である ２．★３・★４要求事項・評価基準ではない独自の基準を用いた評価は不可である		ここでは、1.の経営層が関与しない評価を排除する趣旨を想定しています。
87	制度構築方針(案)	18	各段階の評価スキームの概要 - ★3	「経営層による自己適合宣誓」とは、経営層が内容を確認・承認したうえで提出された自己評価結果であることが求められる、という理解で差し支えないか確認したい。	経営層の関与レベルが不明確な場合、形式的な宣誓に留まるリスクがあるため、求められる関与の水準を明確にする必要があると考える。	御認識のとおりです。
88	制度構築方針(案)	18	各段階の評価スキームの概要 - ★3	星獲得後の「公開」および「証書の発行」を「必要に応じて」としている理由について、制度設計上の考え方を確認したい。	「対外的な信頼性の確保」「取引先への説明」の観点から、公開・証書の位置づけは制度普及に影響を与える要素であるため。	「公開」について、表記を見直します。「証書の発行」について、具体な内容は今後検討してまいります。
89	制度構築方針(案)	18	各段階の評価スキームの概要 - ★3	★3の評価を社内の専門家が行う場合、人事評価などを背景にした上司による不当な圧力が発生しうると考えられます。 情報処理安全確保支援士の倫理規定および年次のオンライン講習ではそれに対抗するように教育しているものの、抗いきれない場合も十分に想定されるものと思います。 導入促進策の１つとして、内部通報制度の案内などをわかりやすく明示的に行い、不当な圧力をかけることにはリスクがあると示していただけるとありがたいです。		いただいた意見については、詳細な制度設計等の検討に当たっての参考とさせていただきます。
90	制度構築方針(案)	19	各段階の評価スキームの概要 - ★4	★4の技術検証について、内製か外部委託かの選択基準（対象規模・機密区分・専門性）や、利益相反管理（評価チームと検証チームの職務分離、クロスレビュー、関与制限）が規定されていない。内製時のSoD（職務分掌）・品質二重化、委託時の選定基準（実績・認定・SLA・秘密保持水準）と監督手順を評価要件として明文化すべきである。	品質や独立性の観点で、評価機関が技術検証を内製する場合の利益相反管理に課題があるため。	いただいた意見については、詳細な制度設計等の検討に当たっての参考とさせていただきます。

No.	該当箇所			寄せられた御意見の概要	理由	提出意見に対する考え方
	該当文書	該当ページ又は項番	該当項目			
91	制度構築方針(案)	19	各段階の評価スキームの概要 - ★4	制度事務局が「不合格」を出した場合に評価機関が知る術がないため、評価機関は制度事務局に対して評価結果を提出後、制度事務局から結果に対する回答を得られるスキームにしなければならないのではないか。		いただいた意見については、評価スキーム詳細の検討に当たっての参考とさせていただきます。
92	制度構築方針(案)	19	各段階の評価スキームの概要 - ★4	⑦で予定されている評価機関から発行する証書は評価した事実を証明するものとなるのか。評価結果との違いが確認できない。		「証書の発行」について、具体な内容は今後検討してまいります。
93	制度構築方針(案)	20	セキュリティ専門家、評価機関及び技術検証事業者の要件 - セキュリティ専門家の要件	今回のスキームの中で、 ・サイバーセキュリティお助け隊サービス（新類型） ・中小企業向けサイバーセキュリティ対策支援者リスト の対象が中小企業となっていますが、 中小企業の定義はございますでしょうか？ 今回のスキームで必要となる【情報処理安全確保支援士】が所属する企業は 一般的な大企業の目安である ・資本金5億円以上、または従業員1,000人以上 に該当する企業であってもほぼ存在しないと考えられます。 このような、大企業であっても上記のサービスは受けられるようになるのでしょうか？		これらのサービスにおける中小企業の定義は、中小企業基本法にて定義される中小企業者を参照しています。 サイバーセキュリティお助け隊サービス（新類型）については、当該中小企業と同程度の規模の企業が利用することを前提としたサービスとなっています。 また、中小企業向けサイバーセキュリティ対策支援者リストについても、利用企業の制限はありませんが、概ね中小企業が活用することを想定したものとなっています。
94	制度構築方針(案)	20	セキュリティ専門家、評価機関及び技術検証事業者の要件 - セキュリティ専門家の要件	セキュリティ専門家（星3）や評価機関（星4）について、単なる資格要件だけでなく、「実地での判断能力」や「中小企業の業務実態への理解」を担保する選定基準・研修を厳格化していただきたい。また、専門家の供給不足により制度利用が滞らないよう、具体的な確保策を示していただきたい。	実証報告書（資料3）では、中小企業が自己評価を行う際、独力では回答が困難であり、専門家による手厚い伴走支援（2～3日程度）が不可欠であったとされている 。今後、数万社規模となるサプライチェーン企業に対し、実務的な支援まで行える質の高い専門家が十分に確保できるのか懸念が残る。質が低い専門家が形式的な確認だけを行う制度にならないよう、担保が必要である。また、要件に含まれている「ISMS主任審査員」は、ISO規格（マネジメントシステム）に対する審査力量を持つものであり、本制度が求める「具体的な技術的対策の強度」や「リスクへの耐性」を判断する専門性とは必ずしも一致しないため、専門家要件として適切か再考いただきたい 。	制度構築方針(案)P.20記載のとおり、セキュリティ専門家において円滑に助言・確認できるよう、本制度においてセキュリティ専門家及びセキュリティ専門家の下で作業に従事する者になる際には、制度で定めた研修の受講を求める予定です。 いただいた意見については、詳細な制度設計等の検討に当たっての参考とさせていただきます。
95	制度構築方針(案)	20	セキュリティ専門家、評価機関及び技術検証事業者の要件 - セキュリティ専門家の要件	制度案で示された専門家要件（情報処理安全確保支援士、公認情報セキュリティ監査人、CISSP等）は、それぞれ「技術」「監査」「マネジメント」と専門領域が異なり、保有する知見や判断基準（常識）にバラつきが生じる懸念があります。また、ITSSレベル4相当の資格保有が、必ずしも本制度の実務スキルを保証するものではありません。専門家の質を担保するためには追加研修が不可欠ですが、研修費用が自己負担となればなり手の確保が困難になります。質の高い専門家を確保するため、制度固有の研修については自己負担なし（国費負担等）で受講できる仕組みを実現していただきたいです。		いただいた意見については、詳細な制度設計等の検討に当たっての参考とさせていただきます。
96	制度構築方針(案)	20	セキュリティ専門家、評価機関及び技術検証事業者の要件 - セキュリティ専門家の要件	専門家資格が列挙型で、国際資格の同等性マッピング（例：GIAC群、ISO/IEC 27006に準ずる審査員資格）や実務経験年数・CPE/CPDによる代替可否の方針が無い。同等性審査手続と代替条件（例：実務5年＋近3年のCPE/CPD基準達成）を規定し、外資系・国際案件でも参画可能な条件整備を求める。	国際調達や外資系企業の参加を想定すると、資格要件の相互承認が必要であるため。	いただいた意見については、詳細な制度設計等の検討に当たっての参考とさせていただきます。
97	制度構築方針(案)	20	セキュリティ専門家、評価機関及び技術検証事業者の要件 - セキュリティ専門家の要件	★３の評価者である「セキュリティ専門家」について。IPA公認の「システム監査技術者」を入れるべきだと考えます。当該資格は、「情報処理安全確保支援士」と比較しても、取得難易度や対応範囲、意見表明に必要なスキル等、今回の制度実現に必要な要素は十分満たしていると考えます。監査系の資格として方針（案）には「公認情報セキュリティ監査人」の記載がありますが、「システム監査技術者」はスキームオーナーとして想定されているIPAの認定資格であり、本制度に関わる研修を受講した者であれば十分「セキュリティ専門家」としての活動ができると考えます。本制度への対応に迫られる中小企業が多数想定される中、市場のIT人材は（特にセキュリティ専門家）はまだまだ不足している状況かと思います。本制度を支える専門家の不足という事態を避けるためにも、IPAの「システム監査技術者」に専門家の裾野を広げることが望ましいと考えます。ご検討下さい。		本制度では、制度普及の観点も踏まえ、セキュリティ専門家として適切な力量を保有することに加え、力量を継続的に維持することまでを求めているかという観点も含めて対象資格を選定しています。いただいた意見については、今後のの検討の参考とさせていただきます。
98	制度構築方針(案)	20	セキュリティ専門家、評価機関及び技術検証事業者の要件 - セキュリティ専門家の要件	★３取得に関して、セキュリティ専門家の要件で「情報処理安全確保支援士」以降の資格を要する。となっているが、一案として経過期間を設け、社内で取得しやすい資格（セキュリティプレゼンター・ＩＴコーディネーター等）を有する者に導入当初は評価・検証できるようにし、経過期間の間に支援士等の資格を取得させるようにしていく。	現状の該当資格の保有者の総数および今後の合格率と合格者を鑑みるに、企業内での取得者の確保は困難であり、現実的には★４と同等の外部の専門コンサルタントに依頼することになる。 ★３取得のためにサプライチェーンを担う中小企業においては、物理的技術的な新規投資（多要素認証・バックアップ・ネットワーク監視等）が必要であり、さらに取得および毎年の更新に対してコンサル料もかかるとなると、費用が高んで取得の弊害になる惧れがある。 評価制度自体は素晴らしい制度であるが、取得のための費用を懸念して取得が進まないことは、セキュリティ対策の意識向上と実施を推進する障害とならぬよう、一定の経過措置を取ることが★３取得の拡大となると思われる。	いただいた意見については、今後の検討の参考とさせていただきます。
99	制度構築方針(案)	20	セキュリティ専門家、評価機関及び技術検証事業者の要件 - セキュリティ専門家の要件	セキュリティ専門家、評価機関及び技術検証事業者の要件について、ISO27001主任審査員とありますが、審査員は認めないのでしょうか？（審査員補は認める必要はないと思いますが） ISO審査員は主任審査員/審査員/審査員補というレベルがあります。さらにエキスパート審査員（JRCA）、プリンシパル審査員（IRCA）のレベルもあります。 また、審査員資格は、JRCAやIRCAへの登録・未登録で区別が必要かもしれません。今のISOの審査員はJRCAやIRCAへの登録は必須ではありません。審査員の力量は審査機関が担保する要求なため。 この資料にあるISO27001主任審査員の力量維持の「審査実績提出、15時間のCPD」の基準はJRCAです。 公認情報セキュリティ監査人も ・公認情報セキュリティ主任監査人 ・公認情報セキュリティ監査人 ・情報セキュリティ監査人補 ・情報セキュリティ監査アソシエイト ・公認情報セキュリティ主席監査人 の資格のレベルも区別する必要がありませんか？		いただいた意見も参考にしつつ、制度構築方針(案)における該当箇所の修正を検討させていただきます。
100	制度構築方針(案)	20	セキュリティ専門家、評価機関及び技術検証事業者の要件 - セキュリティ専門家の要件	セキュリティ専門家に求める資格について、「記載されている資格のいずれか1つを保持していれば要件を満たす」という理解で差し支えないか確認したい。	資格要件の解釈が曖昧な場合、専門家不足や評価実務の停滞につながる恐れがあるため。	御認識のとおりです。
101	制度構築方針(案)	20	セキュリティ専門家、評価機関及び技術検証事業者の要件 - セキュリティ専門家の要件	■該当箇所（対象資料の括弧内に○を記入し、下線部に該当箇所を記載ください。） （○）サプライチェーン強化に向けたセキュリティ対策評価制度に関する制度構築方針（案） → ページ番号：20 ■意見内容 セキュリティ専門家の認定として、CompTIA SecurityX(旧名称CASP+)、またはCompTIAのスタッカブル認定であるCSIE(CompTIA Secure Infrastructure Expert)の追加が望ましいと考えます。	SecurityX(CASP+)はスキル標準ユーザー協会のレベル4認定スキルであること、中堅中小企業でもっとも必要とされるIT＋セキュリティのスキル＝セキュリティ設計や実装力を問われる実務者に関する認定(CASP＝CompTIA Advanced Security Practitioner)であり、★3などの自己評価に必要なスキル・能力が担保された認定であると考えられるため。	本制度では、制度普及の観点も踏まえ、セキュリティ専門家として適切な力量の保有/維持という観点及び関係する国内外の制度との整合という観点も加味にうえ、対象資格を選定しています。いただいた意見については、今後の検討の参考とさせていただきます。
102	制度構築方針(案)	20	セキュリティ専門家、評価機関及び技術検証事業者の要件 - セキュリティ専門家の要件	セキュリティを確認する専門家（評価者）の要件・研修において、秘密分散技術などの「暗号鍵に依存しない」最新技術に関する知識要件を追加し、人材を確保・育成すべきである。		いただいた意見については、今後の検討の参考とさせていただきます。
103	制度構築方針(案)	20	セキュリティ専門家、評価機関及び技術検証事業者の要件 - セキュリティ専門家の要件	研修要件が受講事実に留まり、力量保証の仕掛けが不十分である。ケースベース演習、サンプリング手法、証跡の十分性判定、利害関係・独立性管理、レポーティング品質等を含むシラバスと、筆記＋実技（ケース採点）の合格基準・再評価規程を定義し、資格維持（CPD、定期再評価）まで制度化すべきである。	評価のばらつきを抑えるため、具体的シラバスと合格基準が必要であるため。	いただいた意見については、詳細な制度設計等の検討に当たっての参考とさせていただきます。
104	制度構築方針(案)	21	セキュリティ専門家、評価機関及び技術検証事業者の要件 - 評価機関の要件	評価機関及び技術検証に課す要件については、「脆弱性診断サービス」とともに「情報セキュリティ監査サービス」または「ペネトレーションテスト（侵入試験）」を追加。	脆弱性診断サービスの要件は、アプリケーション、ソフトウェア、プラットフォームなど ITシステムに内在する脆弱性の有無を診断する際の技術を担保するものであり、評価制度の指示するところのセキュリティ監視や IT 資産管理方法の評価に資する知識、技術要件を必ずしも充分に満たすとはいえないと考えます。情報セキュリティ監査サービスは、IT 環境セキュリティ全般の対策評価の知見であり、ペネトレーションテスト（侵入試験）は、IT 環境に対する攻撃において全般的な知識を有していると考えます。(令和 7 年 3 月 31 日付 経済産業省「情報セキュリティサービス基準 第 4.1 版」参照	「ペネトレーションテスト(侵入試験)サービス」については、情報セキュリティサービス基準上、「脆弱性診断サービス」の提供を前提としたサービスであり、いただいた意見を踏まえ、制度構築方針における該当箇所の修正を検討させていただきます。 その他、評価機関及び技術検証事業者の要件については、情報セキュリティサービス基準などの既存制度との整合や、制度普及の観点も踏まえて今後具体的に検討してまいります。
105	制度構築方針(案)	21	セキュリティ専門家、評価機関及び技術検証事業者の要件 - 評価機関及び技術検証事業者の要件	第3者評価者の資格ですが「情報処理安全確保支援士」のみ限定がよいのではないでしょうか。 そうしないと維持費用をかけている意味がなくなります。 少しでも「情報処理安全確保支援士」のブランド力をあげるためにご検討をお願いいたします。		本制度では、制度普及の観点も踏まえ、セキュリティ専門家として適切な力量の保有/維持という観点から対象資格を選定しています。いただいた意見については、情報処理安全確保支援士に係る政策の検討に当たっての参考とさせていただきます。
106	制度構築方針(案)	21	セキュリティ専門家、評価機関及び技術検証事業者の要件 - 評価機関及び技術検証事業者の要件	評価主体と支援主体の厳格な分離 ： 方針案21ページの注釈（注374）を撤回し、同一法人による「支援・販売」と「第三者評価」の兼業を厳格に禁止すること。評価機関の独立性を担保する監視メカニズムの構築が不可欠である。		★4においては、第三者認証制度ではなく各企業のセキュリティ対策状況を評価するための評価制度であることを踏まえ、制度の普及促進やセキュリティ産業振興の観点も考慮して評価機関には厳格な中立性・独立性を求めないこととしています。いただいた意見については、詳細な制度設計等の検討に当たっての参考とさせていただきます。
107	制度構築方針(案)	21	セキュリティ専門家、評価機関及び技術検証事業者の要件 - 評価機関及び技術検証事業者の要件	そもそも、専門家は確認、助言と署名をするよう指定があるが、責任は何なのかも不明瞭であり、本制度を悪用し、資格持ちの少ない中小のSIerやベンダーを業界から締め出したうえでRISSやCISSP、CISA等の資格を持った要員を多数要する大規模なSIerへ利益を誘導しているようにしか見えない。		本制度では、セキュリティ専門家として適切な力量の保有/維持という観点から対象資格を選定しています。 また、経済産業省では、情報処理安全確保支援士等のセキュリティ資格者の更なる普及等に係る施策を進めており、いただいた意見については、今後の施策検討の参考にさせていただきます。
108	制度構築方針(案)	21	セキュリティ専門家、評価機関及び技術検証事業者の要件 - 評価機関及び技術検証事業者の要件	本制度において「セキュリティ専門家の力量の保持・維持要件を満たす資格」として、複数の資格を同列に扱う方向性が示されている点について、意見を述べます。 情報セキュリティに関する第三者的な検証・評価業務は、組織の内部情報や未公開情報、脆弱性情報等、極めて機微な情報を取り扱う重要な業務であり、その担い手には高度な専門性だけでなく、強い倫理性と法的責任の裏付けが求められると考えます。 日本においては「情報処理の促進に関する法律」に基づく登録セキスペは、法令により守秘義務が課されており、違反時には罰則も規定されています。これは、セキュリティ業務に従事する専門家としての信頼性を制度的に担保する重要な要素であると認識しています。 一方、力量要件として想定されている他の資格については、資格制度としての倫理規定や守秘義務が存在する場合があるものの、法的な義務として位置付けられているわけではありません。このため、資格ごとに守秘義務の法的性質や責任の重さには差異があると考えられます。 現時点で公表されている資料においては、これらの違いをどのように整理し、評価制度上どのように考慮するのかについて明確な説明は示されていません。セキュリティ検証業務は制度の信頼性に直結するため、資格の技術的水準だけでなく、守秘義務や責任の担保の在り方についても、制度設計上の考え方を明確に示すことが望ましいと考えます。 つきましては、 ・セキュリティ専門家の力量要件として資格を認める際の考え方 ・資格ごとの守秘義務や責任の違いをどのように評価制度に反映するのか について、今後の制度設計や運用指針の中で整理・明確化されることを要望します。 本制度が高い信頼性を持つ評価制度として定着するためにも、評価を担う専門家に対する責任と信頼の担保について、丁寧な制度設計がなされることを期待します。		いただいた意見については、詳細な制度設計等の検討に当たっての参考とさせていただきます。

No.	該当箇所			寄せられた御意見の概要	理由	提出意見に対する考え方
	該当文書	該当ページ又は項番	該当項目			
109	制度構築方針(案)	21	セキュリティ専門家、評価機関及び技術検証事業者の要件 - 評価機関及び技術検証事業者の要件	セキュリティ専門家の力量を「ITSSレベル4相当」と表現しています。当社にもサプライチェーン上の受託事業者は多く、委託事業者との取引を円滑するためにご努力されている様子を受けています。例えば2026年1月１日施行の取適法に関しても、長年の取引慣行から価格転嫁に踏み切ることが難しい、との声も頂いています。今回の本制度によると、これらの受託事業者はすべて★３に該当すると思われます。 まず地方にはデジタル人材やセキュリティ人材が圧倒的に不足しているという課題を申し上げます。当社の支援しているのは★３つレベルの企業ですが、そのほとんどに情シス専任担当者がおらず、居たとしても総務との兼任です。そのため地方企業において、当制度の要求事項を網羅的に自己評価するのは難しいと感じます。 また外部のセキュリティ専門家に確認の実施をしてもらうにあたって、特に地方ではITSSレベル4相当の専門家は少ないのが現状であるため、適切な専門家探しに難航することが想像されます。制度を広く浸透させるためには、ある程度要件を緩和することも検討していただきたいです。 さらに審査OK後の評価基準の継続維持におけるコストも企業経営を圧迫すると考えます。先述した通り中小企業はデジタル人材が圧倒的に不足しているため、外部からの伴走支援に頼らざるを得ません。当社「サイバーセキュリティお助け隊」として活動しながら、独自に情報マネジメントの伴走支援サービスを提供しています。そこで伴走している内容は人と組織の安全管理措置をサポートする支援ですが、支援の中で一番難易度の高いのは人的安全管理措置、すなわち従業員のセキュリティ教育です。ここには時間がかかるため伴走支援機関もともすると数年に及ぶこともあります。すなわち★３を取得するまでより、取得してからの従業員教育が大事であり、それを支援する外部専門家や伴走支援者のスキーム、またその活動コストを補助する仕組みなどが必要と考えます。	IPA情報処理推進機構　DX人材 https://www.ipa.go.jp/publish/wp-dx/gmcbt8000000botk-att/000108046.pdf IPA情報処理推進機構　セキュスペ登録者数 https://www.ipa.go.jp/jinzai/riss/reports/data/20250401newriss.html フォーバルGDXリサーチ研究所　デジタル人材不足 https://gdx-research.com/wp-content/uploads/2025/06/20250617_researchreport-1.pdf	本制度(★3・★4)については、制度構築方針(案)P.26記載のとおり、SECURITY ACTION(★1・★2)などの関連制度と相互的に補完する制度として位置付けています。 また、セキュリティ専門家による助言・確認については、オンラインにより実施することも想定し、いただいた御意見も参考に今後詳細な制度設計等を進めてまいります。 加えて、★を取得する中小企業への支援策として、サイバーセキュリティお助け隊サービス（新類型）の制度検討などを行っていますが、いただいた御意見は今後の中小企業支援策の参考とさせていただきます
110	制度構築方針(案)	21	セキュリティ専門家、評価機関及び技術検証事業者の要件 - 評価機関及び技術検証事業者の要件	方針案の文書では、セキュリティ専門家となり得る資格として情報処理安全確保支援士、公認情報セキュリティ監査人、CISSP、CISM、CISA、ISO27001主任審査員が明記されていますが、ここに「ITコーディネータ」を追加していただきたい。 現在明記されている各資格の力量の判断条件としてITSSレベル４に位置付けられる、或いは、相当することが記載されています。 一方で、経済産業省推奨資格の「ITコーディネータ」もITSSレベル４に認定されています。また、中小企業や小規模企業の現場において、情報セキュリティの導入・構築・運用の支援に深く携わっている同資格保有者が全国に多く存在しています。但し、力量の維持のために研修やポイント取得などの制度条件を設けることは必須と考えます。	現在明記されている各資格の力量の判断条件としてITSSレベル４に位置付けられる、或いは、相当することが記載されています。 一方で、経済産業省推奨資格の「ITコーディネータ」もITSSレベル４に認定されています。また、中小企業や小規模企業の現場において、情報セキュリティの導入・構築・運用の支援に深く携わっている同資格保有者が全国に多く存在しています。但し、力量の維持のために研修やポイント取得などの制度条件を設けることは必須と考えます。	本制度では、セキュリティ専門家として適切な力量の保有/維持という観点から対象資格を選定しています。いただいた意見については、今後の検討に当たっての参考にさせていただきます。
111	制度構築方針(案)	21	セキュリティ専門家、評価機関及び技術検証事業者の要件 - 評価機関及び技術検証事業者の要件	評価機関／技術検証事業者に対し、情報保護マニュアル整備だけでは粒度が不足している。データ分類（申請書・証跡・脆弱性情報）と保管暗号化、転送要件（TLS/MTLS）、保管期間、削除ログの保存、侵害時通報SLA（例：72時間以内）等を必須統制として明文化し、監査可能な管理基準に引き上げるべきである。	実地審査・技術検証で機微情報に触れるため、取り扱い基準の詳細が必要であるため。	評価機関及び技術検証事業者の要件については、情報セキュリティサービス基準などの既存制度との整合や、制度普及の観点も踏まえて今後具体的に検討してまいります。
112	制度構築方針(案)	21	セキュリティ専門家、評価機関及び技術検証事業者の要件 - 評価機関及び技術検証事業者の要件	評価機関の品質担保策が内部管理中心で、外部独立性による検証が不足している。年1回以上の外部監査（スコープ：評価プロセス、独立性、記録管理）と要約公開・是正計画提出・追跡審査を制度要件として義務化し、評価の一貫性と透明性を確保すべきである。	評価の質担保に第三者監査が必要であるため。	いただいた意見については、詳細な制度設計等の検討に当たっての参考とさせていただきます。
113	制度構築方針(案)	21	セキュリティ専門家、評価機関及び技術検証事業者の要件 - 評価機関及び技術検証事業者の要件	本評価制度の価値を高め、各企業が信頼して利用していくためには、評価機関の評価品質の維持・向上が必要であると考えられる。 例えば、会計監査においては、金融庁および公認会計士協会が監査法人・会計事務所などに赴いて監査法人・会計事務所の監査品質を検査することで、会計監査の品質の維持・向上を図ることで、会計監査の信頼性を確保されている。 本評価制度の品質を維持・向上するための組織を経済産業省内もしくは公認会計士協会のような独立した専門家組織による検査の制度の構築も必要であると考える。		いただいた意見については、詳細な制度設計等の検討に当たっての参考とさせていただきます。
114	制度構築方針(案)	21	セキュリティ専門家、評価機関及び技術検証事業者の要件 - 評価機関及び技術検証事業者の要件	「以下に示す「情報セキュリティサービス基準適合サービスリスト」(脆弱性診断サービス)登録要件*2を満たすこと」とありますが、評価内容の性格から、本制度は「脆弱性診断サービス」よりも「情報セキュリティ監査サービス」の内容に近い制度であると認識しています。 「脆弱性診断サービス」だけでなく、「情報セキュリティ監査サービス」も登録要件に含めるべきではないでしょうか。		技術検証事業者の要件については、技術検証の実施能力や情報セキュリティサービス基準などの既存制度との整合などの観点も踏まえて今後具体的に検討してまいります。いただいた意見については、今後の検討の参考とさせていただきます。
115	制度構築方針(案)	21	セキュリティ専門家、評価機関及び技術検証事業者の要件 - 評価機関及び技術検証事業者の要件	評価実務の明確化と品質管理体制の整備：運用上の形骸化を防ぐため、各評価機関による、評価基準の確認深度や対象範囲の定義の明文化を検討してはどうか。また、制度事務局/指定委員会が評価機関を指定した後も、定期的な品質維持チェックの仕組みや、★４取得組織の対策状況を継続的に確認する枠組みを、制度開始前に明確に整備してはどうか。		いただいた意見については、詳細な制度設計等の検討に当たっての参考とさせていただきます。
116	制度構築方針(案)	21	セキュリティ専門家、評価機関及び技術検証事業者の要件 - 評価機関及び技術検証事業者の要件	利益相反の防止：★４取得希望組織に対しての、コンサルティング支援と評価実務の兼業による形骸化を防ぐため、ファイアウォールの最低要件を具体化することを検討いただきたい。		いただいた意見については、詳細な制度設計等の検討に当たっての参考とさせていただきます。
117	制度構築方針(案)	21	セキュリティ専門家、評価機関及び技術検証事業者の要件 - 評価機関及び技術検証事業者の要件	意見内容: 本制度における「評価機関」の指定要件および運用において、「認定されたISO/IEC 27001（ISMS）認証機関」を、本制度の評価機関として優先的かつ包括的に認定する仕組みを導入することを提言いたします。 具体的には、ISMS-AC（情報マネジメントシステム認定センター）等により認定を受け、現在活動している認証機関（BSI、JQA等）について、申請に基づき簡易な手続きで本制度の評価機関として登録できる枠組みを設けてください。	方針案（p.21）において、評価機関には「品質管理マニュアルの整備」や「ISO 27001主任審査員等の有資格者の配置」が求められていますが、既存のISMS認証機関はこれら全ての要件を既に高水準で満たしています。 新たな評価機関を一から育成・指定するのではなく、既に信頼と実績のある認証機関を本制度の担い手として活用することで、制度開始当初から質の高い審査体制を確保できます。 また、普段から当該企業の審査を行っている機関が評価を行うことで、事業者のビジネスやシステム環境への理解不足による審査の長期化や誤解を防ぐことができます。	いただいた意見については、詳細な制度設計等の検討に当たっての参考とさせていただきます。
118	制度構築方針(案)	23	評価の考え方 – 評価の実施内容	意見内容: ★4で求められる「技術検証（脆弱性検査等）」について、既存の脆弱性診断結果の活用範囲を柔軟かつ明確に規定することを提言いたします。 具体的には、「ISMAP管理基準に基づく脆弱性診断」や「政府情報システムにおける脆弱性診断導入ガイドライン」等に準拠して実施された診断報告書（Webアプリケーション診断、プラットフォーム診断等）を提出することで、本制度における技術検証を実施したものとみなす旨を、ガイドライン等に明文化してください。	p.23において「直近における対象機器への脆弱性検査の実施結果を確認する」ことによる代替が示唆されていますが、その要件が具体的ではありません。クラウドサービス事業者（CSP）は、インターネット境界機器だけでなく、アプリケーション層を含むより深度の深い診断を定期的に実施しています。これらが本制度の技術検証として有効であることを明確に保証することで、事業者の不安を払拭し、無駄な再検査コスト（二重投資）を回避することができます。	いただいた意見については、詳細な制度設計等の検討に当たっての参考とさせていただきます。
119	制度構築方針(案)	23	評価の考え方 – 評価の実施内容	星4だと3年に1回の評価機関の評価で足りるのに対し、それよりも緩やかであるべき星3だと毎年専門家の確認・助言を受けなければならないというのは、不均衡である。 したがって、星3の専門家の確認・助言を3年に1回で足りることとすべきである。		評価の有効性・信頼性確保の観点から★3では有効期間を1年とし、年次でセキュリティ専門家の助言・確認を受けることとしています。加えて、定期的なセキュリティ専門家の助言・確認を受けることで、中小企業等の継続的なセキュリティレベルの向上を図ることとしています。 また、★4においても、有効期間中においては年次で自己評価を実施し評価機関に提出することとしており、当該手続きを通じて、有効期間内におけるセキュリティ対策の維持等を図ってまいります。 いただいた意見については、今後の検討の参考とさせていただきます。
120	制度構築方針(案)	23	評価の考え方 – 評価の実施内容	★4の不適合是正期限が例示で一律「1か月以内」と示されており重大度やリスクに応じた差異が設計されていないため、重大度別（Critical／High／Medium／Low）の標準是正期限と例外運用の要件を定義すべきである。	重大脆弱性と軽微不備を同一の期限で扱うのは不合理であるため。	いただいた意見については、詳細な制度設計等の検討に当たっての参考とさせていただきます。
121	制度構築方針(案)	23	評価の考え方 – 評価の実施内容	実地審査の確認例に内部セグメント分離や東西トラフィック抑止など横展開防止策の評価項目が欠落しており、境界防御偏重とならないよう内部ネットワーク分離・マイクロセグメンテーション・出口対策の検証観点を明示すべきである。	境界突破後の横展開対策が重要であるため。	いただいた意見については、詳細な制度設計等の検討に当たっての参考とさせていただきます。
122	制度構築方針(案)	23	評価の考え方 – 評価の実施内容	合格基準が原則「全適合必須」のみの記述であり、代替コントロールの承認要件・評価手順・期限付き是正計画の扱いが示されていないため、代替コントロールを認める審査フレームと記録様式を制度要件として整備すべきである。	技術制約やレガシー事情への配慮が必要であるため。	本制度は大企業から中小企業まで一律で満たすべきベースラインを定めているところ、要求事項が求めるセキュリティ水準を多くの者が達成できるよう、実証事業での結果を取り得る手段の多様性に配慮して適宜代替策を追加の上、要求事項・評価基準(案)を作成したところです。制度構築方針(案)P.17記載のとおり、今後ガイダンス資料を整備する予定であり、当該資料において実装例等の拡充を図ってまいります。
123	制度構築方針(案)	23	評価の考え方 – 評価の実施内容	★4第三者評価における実地審査・技術検証の簡素化を図ってほしい	事前準備、報告書作成も含めると1社あたりの評価にかなりの工数を要することが想定されるため。	いただいた意見については、詳細な制度設計等の検討に当たっての参考とさせていただきます。
124	制度構築方針(案)	23	評価の考え方 – 評価の実施内容	意見：所用期間（想定）は制度事務局での所用期間も含まれていると考えて良いか？また、含まれない場合は制度事務局での所用期間はどの程度を想定しているか？登録機関がボトルネックとなり契約が円滑に進まない可能性を危惧しています。		いただいた意見については、詳細な制度設計等の検討に当たっての参考とさせていただきます。
125	制度構築方針(案)	23	評価の考え方 – 評価の実施内容	「サプライチェーン強化に向けたセキュリティ対策評価制度に関する制度構築方針（案）」について、23ページの技術検証の実施内容として「取得希望組織がインターネットに公開している機器が対象」と記載されておりますが、ページ上部のグレー枠では「対象をサンプリングして評価実施を想定」とも記載されており、具体的な対象機器の特定方法、サンプリング方法、脆弱性検査方法などについて確認したいと考えております。17ページに記載のガイダンス資料にて、これらの具体的内容が開示される予定でしょうか。また、ガイダンス資料の公開時期は決定しておりますでしょうか。		技術検証等の詳細については、ガイダンス資料に記載する予定です。ガイダンス資料の公開予定時期はスケジュールに記載いたします。
126	制度構築方針(案)	23	評価の考え方 – 評価の実施内容	会計監査等でセキュリティ対応の要求が厳格化する中、本制度の評価結果を監査対応に流用できるように、監査で求められがちな統制項目（アクセス権管理、ログ管理、変更管理、委託先管理等）との対応関係（マッピング）や、監査向けに提示できる標準証跡パッケージ（評価報告書の要約版等）を整備していただきたい。	監査対応の重複作業が削減できれば、制度取得の実務メリットが明確になり、企業の参加インセンティブが高まって普及促進につながるため。	いただいた意見については、詳細な制度設計等の検討に当たっての参考とさせていただきます。
127	制度構築方針(案)	23	評価の考え方 – 評価の実施内容	技術検証 ●内部診断、外部診断が1～2日程度で完了できるような実施内容としていただきたい（例えば、診断対象の端末台数の最大値を設定する、など） ●技術検証による公開サーバへの影響、内部端末への影響緩和策を盛り込んでいただきたい（例えば、公開サーバへの脆弱性診断によりサーバ可用性、パフォーマンスに影響がでないように）。	本制度導入の効果（セキュリティ対策の負担軽減）を高めるため。	いただいた意見については、詳細な制度設計等の検討に当たっての参考とさせていただきます。
128	制度構築方針(案)	23	評価の考え方 – 評価の実施内容	合格基準 原則として、全ての評価基準への適合を求める。 ●評価基準を満たせない場合でも、代替策を実施していることで準合格を得られるような緩和策を認めていただきたい	本制度導入の効果（セキュリティ対策の負担軽減）を高めるため。	本制度は大企業から中小企業まで一律で満たすべきベースラインを定めているところ、要求事項が求めるセキュリティ水準を多くの者が達成できるよう、実証事業での結果を取り得る手段の多様性に配慮して適宜代替策を追加の上、要求事項・評価基準(案)を作成したところです。制度構築方針(案)P.17記載のとおり、今後ガイダンス資料を整備する予定であり、当該資料において実装例等の拡充を図ってまいります。
129	制度構築方針(案)	23	評価の考え方 – 評価の実施内容	■ 意見内容 ・合格基準について、「★3・★4 ともに、原則として、全ての評価基準への適合を求める」と記載されているが、中小企業にとって非常にハードルが高い。 ・評価基準を「必須項目」と「任意項目」に分け、「全体として 8 割の基準を満たせば適合」とするなど、柔軟な達成基準を設けるべき	中小企業にとって、★4 取得のハードルは非常に高く、★3 ですら容易ではない。全評価基準への適合は非常に困難と予想される。本制度の目指す効果は「企業のセキュリティ対策決定を容易・適切なものにする」と定められている（上記資料４ページ目記載） が、全基準適合の要件化は、中小企業が★取得を躊躇または断念する要因となりかねず、本制度の普及という点からも懸念されるものである。 ついては積極的な★取得を促進すべく、一部は達成必須項目、残りは任意項目と分類し、「必須項目すべてと任意項目の一部を合わせて、全体として 8 割の項目を満たせば適合」とするなど、柔軟な達成基準を設けるべき。	本制度では、取得希望組織が一律で満たすべきベースラインとしての基準であることを考慮し、全ての評価基準への適合を求めています。 ★取得を希望する組織(特に中小企業)が適切に★を取得できるよう、サイバーセキュリティお助け隊サービス等の支援施策により、必要な支援を実施してまいります。

No.	該当箇所			寄せられた御意見の概要	理由	提出意見に対する考え方
	該当文書	該当ページ又は項番	該当項目			
130	制度構築方針(案)	23	評価の考え方 – 評価の実施内容	★4における技術検証について、ASM（Attack Surface Management）の観点を取り入れることを検討していただきたい。 現行案では、★4取得企業が申告した外部公開IT機器を前提にネットワーク脆弱性診断を実施する整理となっていると理解しているが、この方法では、企業自身が把握し、既に対策を講じているIT機器に対する確認に留まりやすく、技術検証としての効果が限定的となる可能性がある。 昨今のサイバー攻撃では、企業が自ら把握していない外部公開IT機器が攻撃対象となる事例も増加していることから、ASMとして「外部公開IT機器の調査・検出」を技術検証の要件として位置づけることが有効と考える。 また、ASMによって検出された外部公開IT機器を踏まえ、リスクの高い外部公開IT機器に対してネットワーク脆弱性診断を実施することで、★4に相応しい、より実効性の高い技術検証が実現できると考える。 さらに、外部公開IT機器の検出にあたっては、起点となるドメインのサブドメインのみを対象とするのではなく、起点ドメイン以外も含めた対象を検出可能であること、ならびにWebサービスに限定せず、ネットワーク機器やサーバー等の外部公開IT機器も検出対象とする考え方を含めて整理していただきたい。	★4は制度上、最も高いセキュリティ成熟度を示す区分であり、「把握している範囲内での対策確認」に留まらず、自社が認識していないリスクの発見まで含めた技術検証が求められると考える。 申告ベースの外部公開IT機器のみを対象とした脆弱性診断では、実際の攻撃者視点でのリスク把握が不十分となる可能性があるため、ASMによる網羅的な外部公開IT機器の把握を前提とした技術検証を取り入れることで、制度の実効性向上およびサプライチェーン起因のサイバーインシデント低減に寄与すると考える。	いただいた意見については、今後の検討の参考とさせていただきます。
131	制度構築方針(案)	23	評価の考え方 – 評価の実施内容	本制度における審査費用について、現時点で想定されている目安やレンジがあれば示していただきたい。	企業が制度活用を検討する上で、費用感は重要な判断材料となるため。	現時点では未定となっています。いただいた意見については、今後の検討の参考とさせていただきます。
132	制度構築方針(案)	23	評価の考え方 – 評価の実施内容	特に★3においては、点数制とし、全項目達成までの途中経過も評価することで、底上げを図るべき。		いただいた意見については、今後の検討の参考とさせていただきます。
133	制度構築方針(案)	23	評価の考え方 – 評価の実施内容	本制度においては、★３においては、実地審査を含まない運用を想定されているが、書類提出と書類審査のみによる状況評価には、大きなリスクがあると考える。 本制度の目的は、形式的な体制整備の有無はもちろんであるが、セキュリティ対策が組織文化として根付き、運用できていることを見極める点にある。そのためには、本来であれば現地訪問による確認が望ましい。 一方で、コストや運用負荷の観点から、一律に現地訪問を必須とすることは現実的でないという意見にも、十分な合理性がある。 そこで、現地訪問に代わる措置として、提出書類の内容について説明を受けるヒアリングの場（オンライン可）を設けることを提案したい。書類の背景や運用実態を対話的に確認する機会を設けることで、形式と実態の乖離を防ぐことができ、不必要に過剰な運用となっている点を指摘できるなど、本制度の趣旨に沿った評価が可能になると考える。		★3における助言・確認について、オンラインにより実施することは妨げない想定です。いただいた意見については、今後の検討の参考とさせていただきます。
134	制度構築方針(案)	23	評価の考え方 – 評価の実施内容	他の制度との整合性も踏まえる必要があるため、本項はあくまで当方の問題提起にとどまるが、ことセキュリティ対策に関しては、ルールや手順が定められていること以上に、それらが実際に運用され、回っていることが重要であると考える。 形式的に規程やルールは整備されていても、それが形骸化し有効に機能していない企業は決して少なくない。このような状態を踏まえると、★３の趣旨は「決まっていること」「定義されていること」ではなく、「一定程度、実際に回せていること」こそが本制度の趣旨により適合した評価水準であると考える。 もっとも、「一定程度、回せている」ことの客観的な評価が容易でない点は、当方も十分に認識している。評価基準の明文化、評価基準の設定は非常に困難であり、評価のばらつきを招くおそれすらある。 そのため、本項は直ちに制度へ反映することを期待するものではない。むしろ、前述のヒアリング導入など、対話的な評価手法と組み合わせることで、将来における「目指すべき姿」に向けての課題として議論いただくことを意図している。		いただいた意見については、今後の検討の参考とさせていただきます。
135	制度構築方針(案)	23	評価の考え方 – 評価の実施内容	例として「評価機関による実地審査等実施日から1か月以内」とあるが、「評価機関ならびに制度事務局からの指摘事項が通達されてから1ヶ月以内」が相応しいのではないか。期限設定の基準は指摘時または指摘後にあるべきと考える。		いただいた意見も参考にしつつ、制度構築方針における該当箇所の修正を検討させていただきます。
136	制度構築方針(案)	23	評価の考え方 – 評価の実施内容	是正対応が必要となった場合、再度評価機関による実地審査含めた審査が必要となるのかを明記すべきと考える。 また、是正報告は評価機関に対して提出するものと認識しているが明記すべきと考える。		具体的な評価スキームについては、今後検討してまいります。
137	制度構築方針(案)	24	評価の考え方	本制度の評価プロセスは、既存のシステム監査と重複する部分が多いと考えられます。 サプライチェーンの強靭化には、理論上、末端（最下位）の企業まで検証を行わなければ実効性が確保できませんが、スポット契約等を含めれば対象範囲は膨大となり、全取引先に厳格な審査を行うことは現実的ではありません。 したがって、長期契約等により既に信頼関係が構築されている事業者や、SOCレポート等の客観的な評価文書を提示できる場合については、審査の一部または全部を免除する仕組みを検討していただきたいで す。		本制度をどの範囲のサプライヤー企業にまで適用するかは、契約等の当事者である発注者がリスクや対応工数等を判断の上決定するものであり、制度として何がしか規定を設けるものではないと考えております。 関係他制度との関係整理を含めた対応工数の低減につながる施策については今後取組むべき課題もあると認識しておりますので、いただいた意見については、詳細な制度設計等の検討に当たっての参考とさせていただきます。
138	制度構築方針(案)	24	評価の考え方	脆弱性診断には高度な専門性が求められ、実施者の力量によって結果が大きく異なります。ログ解析等の静的解析に比べ、IDA等のツールを駆使した動的解析には高度なスキルと経験が必要です。また、実務上は海外製のオープンソースツール等が利用されることもありますが、その全機能を把握することは困難です。こうしたツールは、診断行為が攻撃と誤認されるおそれや、ツール自体にバックドアが含まれ新たな脆弱性を招くリスクも孕んでいます。評価の属人性を排し、こうしたツール起因のリスクを回避するため、国が安全性を確認・推奨する特定ツールの実行結果をもって自動的に評価完了とみなすなど、客観的かつ簡易な判定基準を設けることを要望します。		いただいた意見については、詳細な制度設計等の検討に当たっての参考とさせていただきます。
139	制度構築方針(案)	24	評価の考え方 – 評価の有効期間等	軽微変更について自己適合宣誓での運用を認めるのみで累積管理や年間上限、閾値超過時の臨時再評価義務が未定義であるため、軽微変更台帳の提出・年間上限設定・累積影響に応じた再評価トリガを明記すべきである。	軽微変更が累積すると基準乖離の恐れがあるため。	いただいた意見については、詳細な制度設計等の検討に当たっての参考とさせていただきます。
140	制度構築方針(案)	24	評価の考え方 – 評価の有効期間等	★4の維持において年次は自己評価の提出のみで更新可能とされ第三者の介在が不要であるため、少なくとも中間の年に抜き取りの技術検証またはリモート実査を義務化し、重大変更時の臨時再評価を発動する仕組みを設けるべきである。	第三者評価なしの3年間継続は形骸化の恐れがあるため。	いただいた意見については、詳細な制度設計等の検討に当たっての参考とさせていただきます。
141	制度構築方針(案)	24	評価の考え方 – 評価の有効期間等	不正行為の取扱いにおいて虚偽報告・情報隠蔽等の抽象表現のみで具体例や範囲が不明確であり、虚偽・隠蔽・妨害等の具体類型を列挙し、重大度別の段階措置（警告・一時停止・取消し）と再申請制限期間を明文化すべきである。	抑止に明確さが必要なため。	いただいた意見については、詳細な制度設計等の検討に当たっての参考とさせていただきます。
142	制度構築方針(案)	24	評価の考え方 – 評価の有効期間等	評価の有効期限を1年・3年と区分する考え方について、脅威変化やインシデント発生時の再 評価条件を含めて明確化すべきである。	脅威環境や攻撃手法は短期間で変化するため、固定的な有効期限のみを設けると、評価が現状と乖離する恐れがある。重大インシデント発生時や構成変更時に再評価を行う仕組みを制度上明示することが望ましい。	いただいた意見については、詳細な制度設計等の検討に当たっての参考とさせていただきます。
143	制度構築方針(案)	24	評価の考え方 – 評価の有効期間等	評価機関は評価結果について保証することになるのでしょうか。 取得組織において虚偽報告、情報隠蔽等の不正行為があり、★の取消し等の事態が生じた場合、確認の署名を行った評価機関に不利益が生じる懸念があります。このリスクは評価機関が負うべきものであるか、そうでないスキーム等が整理されるのか、どのようにお考えでしょうか。		評価機関の役割・責任については、今後具体的に検討してまいります。
144	制度構築方針(案)	24	評価の考え方 – 評価の有効期間等	/意見の内容： 評価の更新手続きの簡素化や、認定有効期間の柔軟な設定（例：2年周期など）など、継続維持にかかる人的コストを抑制する施策を要望します。 と」とするなど、実効性を維持しながら事務負担を軽減する仕組みが、制度の普及促進につながるかと考えます。	理由1．持続可能な制度運用の確保： 星3が「最低限の施策」と設定される場合でも、その維持・証跡管理には相応工数が発生することが想定されます。特に中小企業の本業を圧迫しない仕組みが必要かと考えます。 理由2．実効性の重視： 形式的な書類審査を毎年繰り返すよりも、例えば「年次はセルフチェックによる簡易レビュー、認定更新は2年ごと」とするなど、実効性を維持しながら事務負担を軽減する仕組みが、制度の普及促進につながるかと考えます。	いただいた意見については、詳細な制度設計等の検討に当たっての参考とさせていただきます。
145	制度構築方針(案)	24	評価の考え方 – 評価の有効期間等	★4の維持にあたり、年1回の自己評価を基本とし、「大きな変更がない場合は第三者評価を不要」とする考え方については、企業の負担軽減の観点から一定の合理性が あると考える。一方で、「大きな変更の判断基準」「自己評価結果の妥当性確認方法」が明確でない場合、実質的なセキュリティ水準の低下を見逃す可能性がある点について懸念がある。	★4は制度上、最も高い成熟度を示す位置づけであることから、「形式的な自己評価に留まらず」「継続的な実装・運用状況の確認」を担保する仕組み（ガイダンスや補足説明等）が重要と考えるため。	いただいた意見については、詳細な制度設計等の検討に当たっての参考とさせていただきます。
146	制度構築方針(案)	24	評価の考え方 – 評価の有効期間等	管理策中心の記述となることで、「何をどの程度達成すれば評価できるのか」という基準・水準が不透明となり、結果として自己申告に依存する運用となる可能性があります。この場合、発注側において調達部門等が委託先に対して必要な段階（★）や要求事項を依頼・説明し、実施状況を確認する際の判断が難しくなり、取引実務上の運用負荷が増大する懸念があります。また、専門家評価の結果が「80%」となった場合に、一定の達成として評価されるのか、100%未達として未達扱いとなるのか等、判定の考え方が明確ではありません。さらに、評価基準ではセキュリティを統括する役員の設置が求められる一方、申請等は専門家対応が前提とされているように見受けられ、役割分担が不明確です。ついては、合否判定、段階付与、部分達成の扱い、証跡・確認深度等を整理するとともに、セキュリティを統括する役員と専門家の関与範囲を明確化いただくことを要望します。		本制度の合格基準としては、取得希望組織が一律で満たすべきベースラインとしての基準であることを考慮し、全ての評価基準への適合を求めることとしています。 その他評価スキームについては、いただいた意見も参考にしつつ、今後具体的に検討してまいります。
147	制度構築方針(案)	24	評価の考え方 – 評価の有効期間等	継続的な状況確認と評価機関の責任：★４取得組織の対策状況について、自己点検のみでは組織内の慣れや形骸化に加え、複雑化するサイバー脅威や環境変化への対応力を客観的に判定すること困難となる懸念があるため、評価機関による継続的な確認を毎年度実施する枠組みを制度開始前に整備してはどうか。あわせて、評価機関が実質的な責任を負わずに評価（いわゆるノーリスクでの評価）が可能になれば、制度自体の信頼性低下を招く懸念がある。適切な評価品質を担保するための仕組みを検討してはどうか。		いただいた意見については、詳細な制度設計等の検討に当たっての参考とさせていただきます。
148	制度構築方針(案)	24	評価の考え方 – 評価の有効期間等	意見内容: ISO/IEC 27001等の維持審査（サーベイランス審査）や更新審査と、本制度の★4第三者評価を「同時実施（統合審査）」できるスキームを制度として明文化し、推奨することを強く提言いたします。 具体的には、以下の運用を可能としてください。 ・事業者が、ISO審査機関に対して本制度の評価を合わせて依頼できること。 ・ISO審査で確認した内容（ガバナンス、物理的対策、人的対策等）については、本制度の評価において「確認済み」として扱い、二重の確認作業を省略できること。 ・ISO審査の工数の中に本制度の確認項目を組み込むことで、日程調整や対応工数を一本化できること。	多くのサプライチェーン企業、特にSaaSベンダー等は、既に年次のISO審査で数日間の拘束と膨大な工数を割いています。これに加え、別の時期に別の評価機関から、類似した項目の審査を受けることは、現場にとって過度な負担（監査疲れ）となります。 「同時実施」が可能となれば、事業者は監査対応のための準備期間や拘束時間を大幅に圧縮でき、費用面でもスケールメリット（移動費や共通管理費の削減）が享受できます。これは、本制度が目指す「企業の負担軽減」と「セキュリティ対策の効率化」を最も具体的かつ強力に推進する施策となります。	いただいた意見については、詳細な制度設計等の検討に当たっての参考とさせていただきます。
149	制度構築方針(案)	24	評価の考え方 – 評価の有効期間等	★4の維持に必要な手続きとして、1年ごとに自己評価を実施、結果を評価機関に提出することとあるが、3年に1回必要となる第三者評価との違いは実地確認の有無となるのであれば明記すべきと考える。また、評価機関への提出スキームについては初年度の評価機関への依頼時に取り決めることとなるのかを明記すべきである。		いただいた意見については、詳細な制度設計等の検討に当たっての参考とさせていただきます。
150	制度構築方針(案)	25	評価結果の登録等	運用開始後に、★を取得した企業が公表されると、取得していない企業がサイバー攻撃の対象として狙われないでしょうか？公表することのリスクは把握済みでしょうか？悪用されることが無いような運用をお願い致します。		本制度では、★を取得した企業を開示することにより、各企業のセキュリティ対策レベルの可視化を図ることとしています。いただいた意見については、今後の開示運用基盤を構築するに当たっての参考とさせていただきます。
151	制度構築方針(案)	25	評価結果の登録等	制度事務局で登録状況を開示する場合、取得企業の登録IDをURLパラメータに含めることで容易にアクセスできるよう検討いただきたい。		いただいた意見については、今後の開示運用基盤を構築するに当たっての参考とさせていただきます。
152	制度構築方針(案)	25	評価結果の登録等	台帳に記載する適用範囲の表記が「全てのネットワーク」等の曖昧な例示に留まり誤解を招くため、対象ドメイン・拠点・クラウドアカウント等の最小限匿名化ルールと具体例をガイドとして明示すべきである。	曖昧な表記は誤解を招く可能性があるため（例：『全てのネットワーク』）。	いただいた意見については、詳細な制度設計等の検討に当たっての参考とさせていただきます。
153	制度構築方針(案)	25	評価結果の登録等	個人事業主の所在地を任意としているため緊急時の連絡性が損なわれ得るので、所在地が任意であってもincident 連携に必要な常設連絡窓口（メール・電話・稼働時間）等の公開を必須化すべきである。	連絡不能はインシデント連携を阻害するため。	いただいた意見については、詳細な制度設計等の検討に当たっての参考とさせていただきます。
154	制度構築方針(案)	26	国内外の関連制度等との連携・整合	既存認証との「完全互換ルール」の明文化 ： ISMS、Pマーク、NIST CSF等に準拠済みの企業に対し、本制度の項目を「自動的に充足している」とみなす完全読み替え規定をガイドライン上で明記し、認証機関及び専門家への依頼不要を含め、追加負担をゼロにすることを保証すべきである 。		いただいた意見については、関連制度等との連携・整合の検討に当たっての参考とさせていただきます。

No.	該当箇所			寄せられた御意見の概要	理由	提出意見に対する考え方
	該当文書	該当ページ又は項番	該当項目			
155	制度構築方針(案)	26	国内外の関連制度等との連携・整合	サプライチェーンの対策の水準の引き上げと、基準策定による効率化の観点で重要な施策であり対応に感謝いたします。 金融分野におけるサイバーセキュリティに関するガイドラインとの記載も考慮し、平仄を合わせた内容となるように留意いただきますようお願い致します。		いただいた意見については、関連制度等との連携・整合の検討に当たっての参考とさせていただきます。
156	制度構築方針(案)	26	国内外の関連制度等との連携・整合	ISMS認証の要求事項と重複する内容が多々あるため、ISMSを取得している場合には、別添★３・★４要求事項及び評価基準の一部評価を簡略化できるような評価制度としていただきたい。 また、第三者機関に評価・技術検証していただく際も同様に、ISMSの評価機関に評価していただく場合には、マネジメントシステムの統合プログラムのように効率よく評価を行っていただきたい。		いただいた意見については、関連制度等との連携・整合の検討に当たっての参考とさせていただきます。
157	制度構築方針(案)	26	国内外の関連制度等との連携・整合	本制度と連携が想定される「IoT製品に対するセキュリティ適合性評価制度（JC-STAR）」について、レベル1が自己評価（自己適合宣言）ベースである場合、暗号モジュール試験及び認証制度（JCMVP）のような第三者認定制度と比較して実効性に懸念が残ります。 一方で、チップやファームウェアを含む厳格な検査を国内制度のみで課した場合、ベンダーはより市場優位性のある米国NISTのCMVP（暗号モジュール検証プログラム）等の取得を優先し、日本の認証制度が忌避される（空洞化する）恐れがあります。したがって、単に国内独自の基準を厳格化するのではなく、NIST CMVP等の国際的な認証取得をもって本制度の要件を満たすものとみなすなど、国際標準との整合性確保および相互承認の仕組みを積極的に導入することを要望します。		JC-STARに関する意見とみられるため、回答対象外としてもよろしいでしょうか。
158	制度構築方針(案)	26	国内外の関連制度等との連携・整合	弊社において個人情報の取り扱いを他社に委託する場合、個人情報保護法の「委託先の監督」に従い、委託先において必要な安全管理措置が講じられているかを委託先に確認しています。そのため、本制度においても個人情報保護法上求められる安全管理措置の内容を要求事項に含めていただけないでしょうか。現状の内容だと個人情報の取り扱いを委託する委託先については個人情報保護法に基づく安全管理措置の実施状況の把握が足りず、結局従来通り独自フォーマットを用いて各委託先にセキュリティ対策状況を確認しにいく部分が残り、制度の活用があまり見込めない状況です。		いただいた意見については、今後の検討の参考とさせていただきます。
159	制度構築方針(案)	26	国内外の関連制度等との連携・整合	英国CEとの相互認証可能性に言及する一方で要求項目の前提差（評価範囲・検証要否・粒度）の明示がなく誤認の恐れがあるため、コントロール項目対応表と相互承認の限定条件を明示し、直接対応しない差分を利用者に明確化すべきである。	相互認証は期待される一方、CEのカテゴリと本制度の★段階は直接対応しないため、誤認リスクがあるため。	いただいた意見については、関連制度等との連携・整合の検討に当たっての参考とさせていただきます。
160	制度構築方針(案)	26	国内外の関連制度等との連携・整合	本制度とISMSの役割比較は示されるものの、業態・規模・クラウド依存度等に応じた取得順序の推奨がなく導入計画の初手が定めにくいため、製造・SaaS/MSP・受託開発等の類型別に取得順序ガイダンスを明示すべきである。	認証取得順序に関して、指針を示さないと企業が迷うこととなるため。	いただいた意見については、関連制度等との連携・整合の検討に当たっての参考とさせていただきます。
161	制度構築方針(案)	26	国内外の関連制度等との連携・整合	ISO27001、SOC2などの認証取得企業への優遇措置などを規定するか？企業にとって複数の認証、評価を取得することはコスト、人員の面から困難。 専門家、第三者評価の認定制度をどのように定めるか。AI活用などで利用企業にとってリーズナブルな評価期間、コストであるべき。		いただいた意見については、関連制度等との連携・整合の検討に当たっての参考とさせていただきます。
162	制度構築方針(案)	26	国内外の関連制度等との連携・整合	自動車産業など、一部業界では既に独自のサイバーセキュリティガイドライン（例：自工会・部工会ガイドライン）が運用されています。 今回公表された SCS評価制度構築方針(案)においても、★3・★4の要求項目が自工会ガイドラインのレベル1・レベル2に対応づけられていることが明記されています。[newton-con...ting.co.jp] しかしながら、現場では発注側企業が既存ガイドラインに基づく独自のセキュリティ水準やチェックシートの運用を継続する可能性が高いと考えられます。 この場合、SCS評価制度とは別体系の基準が取引要件として残り続け、企業（特に中小企業）は引き続き「複数基準への二重対応」を強いられることとなり、制度の普及を妨げる恐れがあります。 SCS評価制度が掲げる「統一基準による可視化」「企業負担の軽減」などの目的（例：チェックシート乱立による負担の軽減）とも矛盾しかねません		いただいた意見については、関連制度等との連携・整合の検討に当たっての参考とさせていただきます。
163	制度構築方針(案)	26	国内外の関連制度等との連携・整合	自工会ガイドラインと SCS評価制度が“対応づけられた別基準”として並立してしまう 結果として、発注元は従来通り自工会基準を用いる可能性が高く、SCS評価制度の浸透が進まない SCS評価制度の「全国横断的な統一基準」という価値が十分に発揮されない SCS評価制度が国家的な統一フレームワークとして機能するためには、業界ガイドライン側にも段階的なSCS準拠や整理統合を促す政策的働きかけが必要と考えます。 SCS制度が「自工会ガイドラインと連携を図った制度設計」を目指していることは公表資料にも記載がありますが、現場レベルでの“実質的な一本化”が進まなければ、制度の意義が薄れてしまいます。		いただいた意見については、関連制度等との連携・整合の検討に当たっての参考とさせていただきます。
164	制度構築方針(案)	26	国内外の関連制度等との連携・整合	業界ガイドライン側への SCS評価制度への準拠促進 自工会・部工会ガイドラインをはじめ、主要業界団体に対して、SCS制度に準拠した体系への移行や整合性確保のロードマップ策定を要請していただきたい。 「業界独自基準を優先しない」旨の省庁公式メッセージの発信 発注者がSCS制度を基本とし、独自基準は例外とするという方向性を明確に示すことが、制度の浸透に不可欠。 SCS制度を活用した契約運用例の具体提供 実際に「★3」「★4」を発注要件として採用するケースのモデル化を推進し、企業間での運用を後押しする。 （経産省が既に法令整理や想定事例を示している方針は非常に有用であり、今後さらに実例を拡充いただきたい。		いただいた意見については、関連制度等との連携・整合の検討に当たっての参考とさせていただきます。
165	制度構築方針(案)	26	国内外の関連制度等との連携・整合	ISMS、SECURITY ACTION、自工会・部工会ガイドライン等との公式マッピング表・互換性ガイドの提供を要望します。 既存の取り組みを生かし、重複作業を避けられれば、利用企業は追加の負担を抑えつつ制度の趣旨に沿った改善に注力できます。 客観的な対応関係が示されることで、社内説明や経営判断も行いやすくなります。	既存の取り組みを生かし、重複作業を避けられれば、利用企業は追加の負担を抑えつつ制度の趣旨に沿った改善に注力できます。 客観的な対応関係が示されることで、社内説明や経営判断も行いやすくなります。	いただいた意見については、関連制度等との連携・整合の検討に当たっての参考とさせていただきます。
166	制度構築方針(案)	26	国内外の関連制度等との連携・整合	ISMS取得企業にとっても、★４に適合するメリットがあるような評価制度にして欲しい。ISMS認証の結果の活用や、文書/証跡の再提出の簡略化、要求事項の差分対応のみで評価可能とする運用にする等。 また、ISMS等の既存認証とSCS評価制度の立ち位置の違いを明確にして欲しい。	現行の★４では、適合するメリットが感じられない。ISMSを取得していれば海外の企業でも通じるが、ISMSとは別に★４の為に第三者評価を受けるメリットを提示できなければ、経営層に説明がつかない。 複数の発注元からのセキュリティ要求への共通回答として、★４取得の登録で一括回答出来る等、発注元への精度理解促進を含めた制度設計を期待する。	いただいた意見については、関連制度等との連携・整合の検討に当たっての参考とさせていただきます。
167	制度構築方針(案)	26	国内外の関連制度等との連携・整合	意見： ISMAP（政府情報システムのためのセキュリティ評価制度）登録サービスや、SOC2 Type2、ISO/IEC 27001等の国際的な認証を取得しているクラウドサービス事業者については、本制度の★3・★4評価を「取得済み」とみなす、あるいは審査項目を大幅に免除する仕組みを明記していただきたいです。 方針案では、クラウドサービスについて「ISMAP登録の有無やSOC2レポートの確認等を行う必要がある」と記載されているものの、クラウドベンダー自身がサプライヤーとして本制度の評価対象となった場合の扱いが不明確です。 大規模クラウドベンダーは既に厳格な国際基準に基づく監査を定期的に受けております。これに加え、本制度独自の審査（特に★4の第三者評価）を個別に求められることは、二重投資となり社会的コストの増大を招きます。既存の信頼できる認証制度との「代替性」や「自動認定」のパスを明確にすることで、サプライチェーン全体の効率化を図っていただきたく存じます。		いただいた意見については、関連制度等との連携・整合の検討に当たっての参考とさせていただきます。
168	制度構築方針(案)	26	国内外の関連制度等との連携・整合	海外企業（外資系企業や海外関連子会社、グローバル本社など）への適用や参照を容易にするため、英語版の制度概要・評価基準の整備を検討いただき、英語圏での理解や普及を考慮いただきたい。制度構築方針（案）資料にあるような Cyber EssentialsやCMMCなど海外諸制度との比較なども非常に有効だと考える。		いただいた意見については、関連制度等との連携・整合の検討に当たっての参考とさせていただきます。
169	制度構築方針(案)	26	国内外の関連制度等との連携・整合	外資企業との取引において、本制度で取得した★を提示することで、C2M2など海外の認証制度と同等の評価を得られるよう、国際的な調整を進める必要がある。日本国内に閉じた制度では、国際取引での有効性が低く、結果として制度自体が形骸化する恐れがある。相互承 認の余地やロードマップを明示すべき。	日本国内に閉じた制度では、外資企業との取引において有効性が低く、結果として制度が形骸化する恐れがある。国際連携により、制度の価値を高める必要があるため。	いただいた意見については、関連制度等との連携・整合の検討に当たっての参考とさせていただきます。
170	制度構築方針(案)	26	国内外の関連制度等との連携・整合	自工会・部工会の文書参照は特定分野に限る要求事項であり広く一般的な制度として割り付けを行う必要はないのではないか。		要求事項・評価基準については、自工会・部工会ガイドラインのほか、英国Cyber Essentials等の他の文献も参照したうえで、必要な事項を抽出して策定しています。
171	制度構築方針(案)	26	国内外の関連制度等との連携・整合	「国内外の関連制度との連携・整合」の記載があるため、自工会ガイドライン（JAMA）Lv3に対応できるよう、★の定義の見直し（対応関係の明示）やLv3相当の追加オプション（追加評価項目）の設定を検討いただきたい。 （★5の位置づけでの検討かと推察する）	現状の制度設計では自工会ガイドラインLv3と整合しておらず、取引先からLv3相当のサプライチェーンアンケートを求められた場合に本制度の結果を転用できない。結果として、アンケートの重複・追加対応が発生し、サプライチェーンアンケートの効率化（負担軽減）につながらない可能性がある。	いただいた意見については、今後の検討の参考とさせていただきます。
172	制度構築方針(案)	26	国内外の関連制度等との連携・整合	「国内外の関連制度との連携・整合」の記載があるため、NIST CSFやCIS Controlsをベースに運用している企業が本制度へ円滑に移行・転用できるよう、要求事項・評価基準のマッピング（対応表）や、差分の吸収方法（同等性判断の考え方、代替証跡の扱い）を制度文書またはガイダンスとして整備することを検討いただきたい。	NIST CSFやCIS Controlsに基づき既に評価・監査を行っている企業は多いと考えられ、整合が不十分な場合、同一内容の評価を二 重に実施する必要が生じる。対応表や同等性判断が用意されれば、既存の評価結果を活用でき、導入障壁の低減とサプライチェーン評価の効率化（負担軽減）につながる。	いただいた意見については、関連制度等との連携・整合の検討に当たっての参考とさせていただきます。
173	制度構築方針(案)	26	国内外の関連制度等との連携・整合	特に金融分野は、業務運営上多層的な委託構造を持ち、サプライチェーンリスクの影響が大きい分野であるため、制度の普及・定着に際しては省庁横断での連携強化をお願いしたく存じます。 金融庁、経済産業省等が一体となって業界横断的に制度を推進することで、事業者側の理解促進および実効性の高い運用につながると期待しております。		いただいた意見については、制度の普及支援や詳細な制度設計等の検討に当たっての参考とさせていただきます。
174	制度構築方針(案)	26	国内外の関連制度等との連携・整合	金融庁「金融分野におけるサイバーセキュリティガイドライン」におけるサードパーティリスク管理に関連する要求事項は、本評価制度との重複部分も多く存在すると考えられることから、可能であれば両者を対応付ける形で整合性を明示いただくことを希望します。 これにより、金融事業者およびその委託先にとって、評価制度の理解が容易となり、効率的な実務運用が可能になると考えます。		いただいた意見については、関連制度等との連携・整合の検討に当たっての参考とさせていただきます。
175	制度構築方針(案)	26	国内外の関連制度等との連携・整合	/意見の内容： 本制度の評価取得の条件として、プライバシーマーク（Pマーク）やISMS（ISO/IEC 27001）等の既存認証の取得を「必須の前提条件」としないことを要望します。	理由1. 中小企業の参入障壁の緩和： 既存の民間認証は、取得・維持にかかる費用および人的リソースの負担が極めて重く、優れた技術力を持つ中小企業やスタートアップがサプライチェーンから排除される要因となっています。 理由2. 機会平等の創出： 国が主導する新たな制度において、特定の民間認証に頼ることなく、技術力や実態に即した公平な評価機会が確保されると考えます。 理由3. 最新セキュリティとの矛盾の解消：過去、既存の認証取得の為の条件にPPAPなどの技術が求められていたことがあり、セキュリティリスクが高くなる要件・条件が何年も評価されずに残されたままになっていたなど、認証を得るために最新のセキュリティ施策を採用できないという矛盾の要因となっています。	本制度の評価取得に当たっては、他の制度による認証取得等の前提条件はありません。
176	制度構築方針(案)	26	国内外の関連制度等との連携・整合	/意見の内容： 本制度の評価を取得した企業については、既存の主要な民間認証と同等、あるいはそれ以上のセキュリティ水準を保持しているものとみなす運用を要望します。	重複投資の解消： 多種の認証を個別に求められる現状は、企業にとって大きな負担です。本制度が公的な「標準指標」として機能し、相互承認が進めば、業界全体の効率化に繋がります。 事業機会の拡大： システムエンジニアリング事業等では取引条件としてPマーク等の保有を求められるケースもありますが、本制度が「既存認証と同等以上の効力」を持つことで、中小企業でも一貫した信頼性を証明できることが期待されます。	いただいた意見については、関連制度等との連携・整合の検討に当たっての参考とさせていただきます。

No.	該当箇所			寄せられた御意見の概要	理由	提出意見に対する考え方
	該当文書	該当ページ又は項番	該当項目			
177	制度構築方針(案)	26	国内外の関連制度等との連携・整合	政府調達や重要インフラにおいて本制度が参照される方針が示されていますが、既にクラウドサービスの政府調達に関してはISMAP（政府情報システムのためのセキュリティ評価制度）が存在し、サプライチェーン・リスクの管理も含む包括的な審査基準が制定されています。規制の簡素化の観点で既存の制度による対応をまずはご検討いただくことを要望します。そのうえでなおクラウドサービスの政府調達における本制度の参照を検討される場合には、以下３点について検討いただくことを要望します。 （１）検討の初期段階において、まずはISMAP制度による一元的な対応ではISMAP制度との役割分担を整理し、事業者に対しても明示いただくこと。 （２）ISMAP登録による「みなし適合」の明記: ISMAP登録事業者は、本制度の要求事項（★3/★4/★5）を網羅的に満たしていると判断し、新たな審査や登録手続きを経ずに、本制度の認定（または同等の評価）を自動的に付与する仕組み（ファストトラック）を構築すること。（資料では「ISMAP登録の有無の確認等を行う必要がある」との記載がありますがその趣旨が定かではありません。） （３）「組織」と「サービス」の評価範囲を整理いただくこと（サービスを対象とするISMAP組織全体のIT基盤対象を対象とする本制度で評価対象が異なるとはいえ、SaaS事業者にとっては事業基盤が不可分です。ISMAP、SOC2、ISMS等を取得済みの事業者に対し、追加で「全社的なガバナンス」等について重複する評価を求めることは、結果的にビジネスにコンプライアンス対応だけのための実質的な二重投資を強いることとなり、不必要なコスト増大やサイバーセキュリティ人材資源の浪費の要因となります。		いただいた意見については、関連制度等との連携・整合の検討に当たっての参考とさせていただきます。
178	制度構築方針(案)	26	国内外の関連制度等との連携・整合	•意見：NIST CSF、ISO/IEC 27001、Cyber Essentials（英国）等の国際基準との整合性を明確にしてください。グローバルサプライチェーンに参加する企業が、複数基準対応で疲弊しない設計を希望します。	•理由：国際取引を行う企業にとって、国内独自基準への対応が追加負担となり、競争力低下につながる懸念があります。既存認証取得企業が「差分対応」で済むような運用ガイドラインや公式なマッピング表の公開を要望します。	いただいた意見については、関連制度等との連携・整合の検討に当たっての参考とさせていただきます。
179	制度構築方針(案)	26	国内外の関連制度等との連携・整合	先進的な運用モデルの参照：本制度案は、先行する自動車産業等のガイドラインとの整合が図られているが、現代のサプライチェーンにおいて不可欠なクラウド事業者は、継続的な変更管理や動的なリスク対応など、極めて高度なセキュリティ運用を実践している。制度の普遍性を高めるため、これらクラウド実務の知見やクラウド利用企業におけるリスク評価・判断の手法を積極的に参照し、議論の枠組みを拡充してはどうか。		いただいた意見については、今後の検討の参考とさせていただきます。
180	制度構築方針(案)	26	国内外の関連制度等との連携・整合	意見内容: ISMAP登録事業者への★4自動付与（みなし適合）：ISMAP（ISMAP-LIU含む）は、政府統一基準に基づく極めて厳格な管理基準（1,000項目以上）への適合を監査・認定する制度であり、本制度の★4で求められる要求事項（ガバナンス、サプライチェーン管理、技術的対策）を高い水準で包含しています。したがって、ISMAP登録の有効期間内にある事業者については、本制度の第三者評価および技術検証を免除し、申請のみで★4を認定する枠組みを設けてください。 ISO 27001/27017認証取得事業者への実地審査免除: 有効なISO/IEC 27001認証を有する範囲については、評価機関による実地審査を原則免除し、書面確認（認証登録証および適用宣言書の確認）や、本制度固有の要件に対する差分確認のみとする「ファストトラック」を導入してください。	方針案（p.28）において、ISMSと本制度は相互補完的とされていますが、ISO/IEC 27001:2022の附属書A（管理策）は、本制度が求める技術的対策やサプライチェーン管理（A.5.20等）を網羅しており、実態としては高い重複性があります。特にSaaSベンダー等は、ISMAPやISO認証の維持のために既に多大なリソースを投じて厳格な監査を継続的に受検しています。これに加え、重複する内容の第三者評価を一律に課すことは、企業の生産性を著しく阻害し、「監査疲れ（Audit Fatigue）」を招く要因となります。限られた国内のセキュリティ監査リソースを有効活用するためにも、既存の高度な認証を取得している企業については審査を免除・簡素化し、未対策の企業への支援にリソースを集中すべきです。	いただいた意見については、関連制度等との連携・整合の検討に当たっての参考とさせていただきます。
181	制度構築方針(案)	26	国内外の関連制度等との連携・整合	EU Cyber Resilience Act（CRA）との整合性について、制度案は情報システム運用・クラウド利用・取引先管理には対応しているが、CRA が求める製品ライフサイクル管理、ソフトウェア部品（SBOM）、脆弱性開示・アップデート提供といった領域は対象外である。制度のスコープ上すべてを包含する必要はないが、最低限、SBOM や脆弱性情報共有など、他制度との連携方針を明示することが望ましい。	CRA は SBOM・脆弱性開示・ライフサイクル管理を要求するが、制度案はこれらを対象としていない。	いただいた意見については、今後の検討の参考とさせていただきます。
182	制度構築方針(案)	26	国内外の関連制度等との連携・整合	記載があるが、自工会アンケート等の各業界、所属団体から出ている個別評価機能との統合を図っていただきたい。具体的には上記に対して、本評価制度による代替もしくは置き換えの推進を強く図って頂きたい。		いただいた意見については、関連制度等との連携・整合の検討に当たっての参考とさせていただきます。
183	制度構築方針(案)	27	★５の位置づけ	まだ検討中段階ではあるが、★5をベストプラクティス準拠としながら選定基準が未定義で評価機関間の解釈ばらつきの恐れがあるため、実証的有効性・国際標準整合・運用可能性・コスト影響評価を軸にした選定基準と公開レビュー手続を早期に明示すべきである。	ベストプラクティスの定義が曖昧だと過剰要求・過少要求が発生するため。	いただいた意見については、今後の検討の参考とさせていただきます。
184	制度構築方針(案)	28	[参考] ISMS適合性評価制度と本制度の比較	本制度の略称をSCからSCS評価制度へ変更いただきたい。		いただいた意見も参考にしつつ、制度構築方針における該当箇所を修正します。
185	制度構築方針(案)	28	[参考] ISMS適合性評価制度と本制度の比較	「[参考] ISMS適合性評価制度と本制度の比較」の表にて、対象をインターネット接続IT基盤とする表現はネットワーク境界前提であり、ゼロトラスト構成のID／セッション／端末状態を基点とする適用範囲定義が不足しているため、IdP・SSO・PAM等を含むゼロトラスト向け範囲定義手順と審査観点を付録で明示すべきである。	境界が薄い環境では資産ベースの定義が必要であるため。	いただいた意見については、今後の検討の参考とさせていただきます。
186	制度構築方針(案)	28	[参考] ISMS適合性評価制度と本制度の比較	★3、★4がベースラインアプローチ、★5がリスクベースアプローチとすると違和感あり。★5はオールハザードアプローチに近くなるというイメージ。		いただいた意見については、今後の検討の参考とさせていただきます。
187	制度構築方針(案)	28	[参考] ISMS適合性評価制度と本制度の比較	（図中、「ISMS 認証」と「今回具体化した範囲」の間にある文「相互補完的な制度として両輪で発展」の下に、以下を追加） ISMS 認証との相互認証も今後検討	例えば、ISMS 認証の外部審査が通れば本制度の★3 が取得可となると、取得に関する負担軽減および自己評価（実効性の担保）の裏付けがされると考えます。ISMS 認証に限らず、類似の認証を取得していれば★3 相当とすると、類似の認証との親和性も高まり、企業全体でのセキュリティ対策水準の向上に寄与すると考えます。	いただいた意見については、関連制度等との連携・整合の検討に当たっての参考とさせていただきます。
188	制度構築方針(案)	28	[参考] ISMS適合性評価制度と本制度の比較	「抽出先行する」の意味がわかりませんでした。別の平易な言葉にかえていただきたいです。		いただいた意見も参考にしつつ、制度構築方針における該当箇所の修正を検討させていただきます。
189	制度構築方針(案)	29	★５の具体化に係る今後の進め方	まだ検討中段階ではあるが、★5での経営層インタビュー導入は有効だが、所要時間・費用・評価機関キャパシティへの影響試算がなく運用設計が不透明であるため、パイロットによる定量試算を公表し、企業規模別の負担軽減策（オンライン実施可・時間配慮）を併記すべきである。	評価機関のキャパシティと費用に影響するため、導入前に試算が必要であるため。	いただいた意見については、今後の検討の参考とさせていただきます。
190	制度構築方針(案)	30	[参考] 関連する制度等との関係性 – JC-STARとの関係性	ＪC-STAR（製品評価）と本制度（企業IT基盤評価）の併用が必要となる条件や判断基準、スケジュール連携、責任分界が示されておらず現場判断が難しいため、併用ガイド（ライフサイクルの交点、適用判定フロー、責任分界、時期連携）を明示すべきである。	製品評価と組織評価の併用条件が不明であるため。	いただいた意見については、関連制度等との連携・整合の検討に当たっての参考とさせていただきます。
191	制度構築方針(案)	30	[参考] 関連する制度等との関係性 – JC-STARとの関係性	「外部ネットワーク境界」に使用される機器は、サプライチェーン防御の一端を担う重要な位置にありながら、それを供給する機器ベンダやその設置を行う業者への導入促進策が無く、基準を満たす努力がユーザー企業のみに課せられている点は本制度の普及を妨げる障害となると考える。基準に適合する機器を提供できるように既存JC-STAR制度との要件整合、制度間関係の整理と公表（p30に整理された表があるが、JC-STAR取得機器が「外部ネットワーク境界」に利用されることは十分考慮されるべきであり、両制度の関係は不可分である）が必要ではないか。また、「お助け隊サービス（新類型）」の制度設計においても仕様・技術情報の提供やセキュリティリスクの診断などにおいて機器ベンダの果たすことのできる役割は大きいと考えており、機器ベンダによるこれらの情報提供に関わる支援策としての導入促進策を検討いただきたい。		いただいた意見については、今後の検討の参考とさせていただきます。
192	制度構築方針(案)	30	[参考] 関連する制度等との関係性 – JC-STARとの関係性	SCS制度（以下、本制度）の構築にあたって、ルータと始めとした(JC-STAR制度における)IoT機器の果たす役割は非常に大きいと考える。これらの機器は「制度構築方針(案)」においては「外部ネットワーク境界」と定義され制度の対象範囲として規定される一方、機器に求められるセキュリティ要件はおもに4-5(および参照されるNo.4-1-3からNo.4-1-6)に置いて定義されていると理解される。これらの要件で外部ネットワーク境界における脅威防御が担保されるかと考えた場合、JC-STAR★1と比較しても限られた技術要件のみしか担保されず、結果としてシステム自体が脆弱になる懸念がある。例えばS1.1-5,10,11が担保されない機器は脆弱性管理、設定管理などにおいて手順化が極めて困難となる。またS1.1-15,16が担保されない機器では、廃棄時の情報漏洩防止策が担保されない。端末・サーバとこれらネットワーク機器のセキュリティ要件は同程度とすることが求められる（片方の要件レベルが低いとそこから侵入され、高いセキュリティ要件を設定する意味がない）ため、これらの要件を含めるよう技術要件を検討する、ないし重複してJC-STAR要件を満たすことを求めるなどの対策が必要と考える。		いただいた意見については、関連制度等との連携・整合の検討に当たっての参考とさせていただきます。
193	制度構築方針(案)	30	[参考] 関連する制度等との関係性 – JC-STARとの関係性	JC-STARに定める技術要件と両立できない技術要件があり、メーカーが「ネットワーク境界」に対応製品を提供することを大いに妨げる懸念がある。例えば、4-5-1-1、4-1-5-1はパスワードを変更することを強制しているが、JC-STAR要件では十分複雑なプリセットを許容している。4-5-1-2はメーカーによって提供を義務付けているため冗長である。4-1-3-2,4-1-3-3,4-1-3-5はネットワーク機器に対しては通信機器★3よりも強い要件を要求している、等の乖離がある。 本要件のネットワーク境界に利用する機器への技術基準にたいしては、極力JC-STARの要求レベルに適合するよう基準を変更するか、JC-STAR認証取得をこれらの要件の代替とするよう要件を変更することを要望する。		いただいた意見については、関連制度等との連携・整合の検討に当たっての参考とさせていただきます。
194	制度構築方針(案)	31	[参考] 関連する制度等との関係性 - 技術情報管理認証(TICS)との関係性	本制度（★3/★4）とTICSの差分が高レベルの言及に留まり、項目IDレベルの対応関係が不明確であるため、要求事項対応表（両制度の項目ID対応、証跡相互流用可否、評価スキーム差分）を公開し重複対応の効率化を図るべきである。	重複取得時の効率化に資する相互流用が難しいため。	いただいた意見については、関連制度等との連携・整合の検討に当たっての参考とさせていただきます。
195	制度構築方針(案)	32	[参考] 関連する制度等との関係性 – 海外諸制度との関係性	海外制度比較が概念レベルの記述に留まり、要求事項IDレベルの対応関係（NIST SP 800-171やTISAX AL等）が提示されていないため、相互承認可能範囲や差分充足手順の設計が困難であり、コントロールID単位の対応表と相互承認ポリシーを公開すべきである。	国際調達での利用に耐えるには詳細マッピングが必要であるため。	いただいた意見については、関連制度等との連携・整合の検討に当たっての参考とさせていただきます。
196	制度構築方針(案)	34	制度の導入促進策	サプライチェーン強化に向けたセキュリティ対策評価制度に関する制度構築方針(案)の P34,P35に掲載されているサイバーセキュリティお助け隊サービス（新類型）について意見を述べさせていただきます。 ・要望 サイバーセキュリティお助け隊サービスに新たな類型（2類）の条件「１類サービスの提供・運用実績が「サイバーセキュリティお助け隊サービス２類詳細ガイドライン」に定める要件を満たすこと。」のように1類型の提供を条件としないで頂きたいと考えています。	保険が必要ないということではないといっているわけではありません。 むしろ重要であると考えています。そのため、お客様はしっかりと保険の専門家に相談し、自社にあった保険を選ぶべきで、サービスに付帯され、詳細の情報もしらないまま、ただ保険に入った安心だけ得て、いざという時に必要な範囲がカバーされていないという事が起きると懸念しています。 しかし、保険を販売するとなると、セキュリティソリューション提供している会社としては新たな事業を立ち上げる必要があり、営業の保険資格はもちろん、その後の運用管理を含め、相当な負荷となります。その対策としての、サービスへの保険付帯は上記説明にあるように、顧客への丁寧な説明はもちろん、保険の選択権を逆に奪うものと考えます。 何が何でも１類型提供を条件とされてしまうと、この保険提供の問題が付いてきます。 是非前向きにご検討を頂きたいと思っております。	【Ｐ】いただいた御意見は、サイバーセキュリティお助け隊サービス（新類型）の制度検討に当たっての参考とさせていただきます。
197	制度構築方針(案)	34	制度の導入促進策	セキュリティ対策コストの価格転嫁について、「パートナーシップ構築」という努力義務的な推奨にとどまらず、より強制力のある枠組みや、具体的なインセンティブ（補助金の優先採択枠の大幅拡充など）を提示していただきたい。特に星4で求められる「技術検証（脆弱性診断等）」は高額になるため、中小企業単独での負担は困難である。	実証報告書（資料3）において、参加企業からコスト負担（ツール導入、診断費用）に対する懸念が多数挙げられている 。資料4では「価格交渉を行い円満に合意」という理想的な事例が示されているが 、立場が弱い受注側企業が発注側に対してコスト負担を求めることは、商慣習上極めてハードルが高いのが実態である。実効性のあるコスト負担の仕組みがないまま制度が始まれば、受注側が一方的にコストを被る構造になりかねない。	想定事例及び解説は、令和４年10月に策定した「サプライチェーン全体のサイバーセキュリティ向上のための取引先とのパートナーシップの構築に向けて」を補足し、私的独占の禁止及び公正取引の確保に関する法律（独占禁止法）や製造委託等に係る中小受託事業者に対する代金の支払の遅延等の防止に関する法律（取適法）との関係を整理し、これらの法令との関係上「問題とならない」事例を作成とすることを目的としたものです。飽くまでも法令との関係を事例の形で整理したものですので、御理解のほどよろしくお願いします。なお、経済産業省としましては、発注者側企業・受注者側企業の双方に対し、作成した想定事例に基づいた価格交渉が実施されるよう普及・啓発を行ってまいります。
198	制度構築方針(案)	34	制度の導入促進策	資料4で示されたチェックリストの内容や運用想定は、実態を無視した理想論に留まっているように見受けられる。現状の法制度（下請法、独占禁止法）における優越的地位の濫用防止などをより厳格に運用、あるいは改正するなどの踏み込んだ措置を行わない限り、この理想論を実態に落とし込むのは非常に難しい制度であると考える。海外のサプライチェーンにおける対策実施状況が高い理由について、その背景にある法規制や商習慣を含めた分析を改めて行い、必要であれば法制度の見直しなど、商習慣の変革を促すような踏み込んだ対策を再検討する必要があると考えます 。		想定事例及び解説は、令和４年10月に策定した「サプライチェーン全体のサイバーセキュリティ向上のための取引先とのパートナーシップの構築に向けて」を補足し、私的独占の禁止及び公正取引の確保に関する法律（独占禁止法）や製造委託等に係る中小受託事業者に対する代金の支払の遅延等の防止に関する法律（取適法）との関係を整理し、これらの法令との関係上「問題とならない」事例を作成とすることを目的としたものです。飽くまでも法令との関係を事例の形で整理したものですので、御理解のほどよろしくお願いします。なお、経済産業省としましては、発注者側企業・受注者側企業の双方に対し、作成した想定事例に基づいた価格交渉が実施されるよう普及・啓発を行ってまいります。

No.	該当箇所			寄せられた御意見の概要	理由	提出意見に対する考え方
	該当文書	該当ページ又は項番	該当項目			
199	制度構築方針(案)	34	制度の導入促進策	意見内容： 制度の目的には賛同しますが、現状の評価基準や運用方法では中小企業にとって負担が大きく、浸透が難しいと考えます。以下の点を検討いただきたいです。 評価項目の簡素化と段階的導入 ★3レベルの自己評価項目をさらに簡易化し、チェックリスト形式でわかりやすくすることで、中小企業が取り組みやすくなります。 専門家確認のコスト軽減 専門家による確認プロセスをオンラインで簡易化し、補助金や公的支援を活用できる仕組みを明示してください。 中小企業向け支援策の強化 「サイバーセキュリティお助け隊」など既存支援サービスとの連携を制度に組み込み、評価取得に必要な費用や人材不足を補えるようにしてください。 認定のインセンティブ設計 認定取得企業に対して、取引先からの信頼性向上や補助金加点など、実質的なメリットを制度に明記することで、参加意欲を高められます。		いただいた意見については、制度の普及支援や詳細な制度設計等の検討に当たっての参考とさせていただきます。
200	制度構築方針(案)	34	制度の導入促進策	制度案では支援策の方向性が示されていますが、サプライチェーン全体での継続的な成熟度向上を短期間で実現するには、補助・支援の枠組みに加えて、税制を含むより広範な経済インセンティブの設計を、制度と連動して明確化することが有効だと考えます。 特に、サイバー対策は導入一回限りではなく、監視運用、脆弱性管理、訓練、監査対応等の継続費用が中心となりやすく、社会的外部効果（投資便益が自社に閉じない）が大きい領域です。したがって、発注側が取引先の対策費用を一定程度負担する場合も含めて、税制上の優遇（例：一定要件下での税額控除・特別償却等）を制度の到達段階（★3/★4 等）と連動させることにより、発注側・受注側双方の意思決定が進み、結果として社会全体のリスク低減に寄与すると考えます。 （要望）制度導入促進策の中で、「国の支援策」の具体例として、税制措置の検討対象化・方向性・想定適用範囲（発注側の負担も対象となり得ること）を明示していただきたいです。		いただいた意見については、制度の普及支援や詳細な制度設計等の検討に当たっての参考とさせていただきます。
201	制度構築方針(案)	34	制度の導入促進策	制度案が掲げる「セキュリティサービスの標準化によるコスト低減（中長期）」の方向性は重要です。 一方、実務では、たとえ費用負担が合意できたとしても、クライアントごとに異なる個別最適の仕組みを導入すると、運用の断絶・品質ばらつき・監視の抜け漏れが発生し、サプライチェーン全体として“最小強度”が上がりにくいという問題が起こり得ます。これは、制度が意図する「共通の物差しによる底上げ」と逆方向の力学になり得ます。 （要望）★3/★4 の要求事項を満たすための「参照アーキテクチャ／参照運用モデル（例：ログ収集・監視、脆弱性管理、特権ID管理、端末防御、訓練、インシデント対応の共通プロセス等）」を、IPA等と連携して提示し、取引ごとの個別実装の寄せ集めにならないよう誘導していただきたい。加えて、監査・証跡の再利用（重複監査の低減）等、共通基盤を採用することの社会的コスト削減効果が最大化する運用設計を明示していただきたいです。		いただいた意見については、制度の普及支援や詳細な制度設計等の検討に当たっての参考とさせていただきます。
202	制度構築方針(案)	34	制度の導入促進策	制度案では、中小企業が★3/★4を取得しやすい支援策（お助け隊サービスの新類型等）や、専門家の活用を促す枠組みが示されています。これは普及の観点で有効です。 ただし、制度開始後に需要が急増した場合、支援サービスの供給力（人材・運用体制・品質保証）が追いつかなければ、地域・業種による格差や、形式対応の助長につながり得ます。 （要望）支援サービスを提供する事業者（SOC/MSSP、BPO、運用支援等）について、運用品質の標準化、育成・訓練、第三者評価の活用など、供給力を底上げする施策を制度の導入促進策に明示していただきたいです。これは特定企業の優遇ではなく、社会全体で安定的に制度を運用するための基盤整備として必要だと考えます。		いただいた意見については、制度の普及支援や詳細な制度設計等の検討に当たっての参考とさせていただきます。
203	制度構築方針(案)	34	制度の導入促進策	サイバー対策に必要な製品・サービスの多くが国外に依存する場合、費用の国外流出のみならず、供給制約や地政学リスク、サポート継続性等がサプライチェーンの脆弱性となり得ます。 （要望）海外製品の排除を求める趣旨ではなく、(a) 参照モデルにおける相互運用性（オープン標準・API等）を重視しベンダーロックインを避ける、(b) 国内外の選択肢を確保し特定依存を下げる、(c) 重要な運用機能が継続できる供給・サポート体制を評価・運用面で確認する、といった「調達・運用のレジリエンス」を、制度運用の考え方として補足していただきたいです。		いただいた意見については、制度の普及支援や詳細な制度設計等の検討に当たっての参考とさせていただきます。
204	制度構築方針(案)	34	制度の導入促進策	「実装・運用」への直接的予算配分 ： 認証ビジネスへの補助ではなく、EDR、SOC、バックアップ体制等の「実効的な防御設備・運用」の導入費用に対する直接的な税額控除や補助を優先すべきである 。		いただいた意見については、制度の普及支援策の検討に当たっての参考とさせていただきます。
205	制度構築方針(案)	34	制度の導入促進策	今般のセキュリティ評価制度において、運用者（事業者やその従業員など）の行動への要求項目がありますが、これはIT導入補助金をはじめとする物的リソースへの補助では足らないように思われます。 人的リソースはそもそもの就労人口の減少（人口減少に起因する）などによって、金銭で賄うことが困難な事業者も増えてくるように感じています。 また別の側面で、「競争をさせる意図はない」とのことですが、商流の上流に位置する事業者から一定の（例えば星3）基準を満たすことを取引要件とされた時に、物的・人的リソースの関係で応えきれずに事業継続を断念する事業者も出てくることが懸念されます。 このことは、逆に上流に位置する事業者が、取引先を「選別」することを助長することも懸念しています。 独占禁止法の優越的地位の濫用との関係も気にかかるところであります。 例えばガソリンスタンドなどでは、個人のお客様の情報取り扱いもありますので、元売り各社がこの基準によって、セキュリティ対策の強化を図る可能性は十分にあると思います。 ですが、当該業界では、過疎が進んだ地域などで、ご家族で経営されている事業者も当然いらっしゃり、その方々によって、地域のインフラが保たれているという実態もあります。 ご家族での経営でも十分に利益を得ることができている事業者さんもいらっしゃるかもしれませんが、そういった事業者さんは稀だと思います。 そうなった時に、求められる物的・人的リソースから事業継続を断念、地域のインフラが悪化するということも発生しうると考えています。 事業者間のセキュリティ対策の情報共有を促進して、対策を打つべき、また打つことが可能な事業者さんが、その商流全体の最適化を図る、という方向性で進むならば、より安心した経済活動を国民全体が行うことができ、素晴らしいことだと思いますが、いわゆる「弱者」の立場に追い込まれている、また追い込まれる可能性がある事業者、またその業態を踏まえて、実効性の担保と同時に、不当な取り扱いが発生しないようなサポート体制の充実、または運用上の厳格なルール、またルールで解決する場合にはそれを監査する独立した第三者の設置など、考慮していただきたく思います。 叶うならば、資本金別、業種別など、比較的事業者の事業継続は問題なくできるだろう範囲での運用開始によって、問題点や課題の洗い出し、解決、そしてサプライチェーン全体へ波及させる、という流れが好ましいと思われます。 最後に、お客様先などでこの評価制度のお話をしても、8割程の方は存じ上げない状況でした。 制度が固まる前の周知はリスクもあるかと思いますが、相当数の事業者さんが突然コスト増を強制される、と感じる可能性が高いということも付記いたします。 また審査員の要件も有資格者に限定せず、広く審査ができる力量がある人材を積極的に活用することで、多様な審査員の確保と審査の質の向上を目指すほうが良いと考える。		いただいた意見については、制度の普及支援や詳細な制度設計等の検討に当たっての参考とさせていただきます。
206	制度構築方針(案)	34	制度の導入促進策	会計監査における監査法人（公認会計士）の「限定意見」制度のような評価でマーク付与するという例外を設けること。 特に問題になるのが「技術的実装」の部分で、制度案を文言通りに読み込むとソリューション投資が行き届いていなければ要求事項を満たせないことになる。だが、脆弱性を自ら認めており、ログ監視を定期的にするなど、不正アクセスされても早期に検知可能な対策を取っていれば、「限定意見」付きでマーク付与を認めるというもの。ただし、一定期間内に必要な投資をするというコミットメントを取り、再審査の時に未実施なら取り消す、そういった制度設計も考えられるのではないか。というのが一案。 もう一案は、制度案にあった三つのリスクである「事業継続」「データ保護」「不正アクセス」が極めて低いと考えられるなら、マーク付与する。もちろん、事業者による説明内容に説得力やエビデンスが必要なのは言うまでもない。 これらの案は、まさにISMSの思想そのものともいえるものである。 ISMSの本質は、リスクを適切にコントロールしているという信頼を利害関係者に与えることにあるので、アカウンタビリティをトップマネジメントが発揮すればいいだけのこと。現実のISMS運用において、リスク受容基準をいいことに、「ルールはあれど技術的実装はなし」でも、それが組織が定めたルールとして運用されていれば審査で「不適合とならない」という制度の形骸化が生じている。 過去のNTT西日本子会社による10年にわたりUSBメモリ抜き出し個人情報漏洩や2024年のイセトー事件、いずれもアスクルと同様にISMS認証を取得している。 本来のISMSの制度趣旨は、「リスクマネジメントプロセスを適用することで、リスクを適正に管理しているという信頼を利害関係者に与えること」にある。 ★５がISMSと相互補完的な制度として両輪で発展するとは、まさにISMS制度の趣旨をSCS評価制度に取り込むことにあるのではないか。 要求事項案は、昨年のアサヒグループHDのランサムウェア感染事件を踏まえると引き下げてはいけない。 否、そもそも要求事項に企業のセキュリティを適合させるのではなく、現実の脅威を踏まえたセキュリティ対策の見直しサイクルが機能しているかの視点で審査をするべきと考える。 サイバー攻撃の脅威は変化しており、制度設計時におけるベースラインが脆弱になっていることは十分考えられる。でないと、結局、ベンダーが「IT補助金」活用で儲けよう的な税金の無駄遣い、制度の形骸化を助長するだけになる。		いただいた意見については、詳細な制度設計等の検討に当たっての参考とさせていただきます。
207	制度構築方針(案)	34	制度の導入促進策	星3つの取得条件である「専門家による確認・署名」を必須とする現案は、中小企業にとって費用・人材の両面で過度な負担となります。制度の普及を最優先し、専門家への委託以外に、「行政機関または準公的機関による簡易チェック・受理」によって星3つ（またはそれに準ずる認定）を付与する枠組みの構築を要望します。	1.公的お墨付きによる信頼性と普及の加速 経済産業省やIPAなどの公的機関が、提出された自己評価シートの整合性を（書類審査等で）確認する形式であれば、企業は高額なコンサルティング費用を抑えつつ、高い信頼性を獲得できます。これは「SECURITY ACTION」等の既存制度とも親和性が高く、企業の参加意欲を劇的に高めます。」 2.「専門家不足」という物理的制約の回避 現在、日本全体でセキュリティ人材が不足しており、数万社規模の中小企業が同時に専門家の署名を求めることは物理的に不可能です。行政がデジタル技術を活用した一括審査や、AIによる形式チェックを導入することで、民間リソースの偏在による不平等を解消できます。 3.「伴走型支援」としての制度設計 単なる 「審査」ではなく、行政によるチェック過程で不備を指摘し、改善を促す「伴走型」の仕組みとすることで、NIST CSF 2.0が重視する「継続的な改善（Improvement）」を、コストを抑えた形で実現可能となります。	いただいた意見については、今後の検討の参考とさせていただきます。
208	制度構築方針(案)	34	制度の導入促進策	セキュリティー対策評価制度の取得が求められる事業（業務）についてお尋ねします。 国や地方自治体から発注される調査、測量、設計等の業務の受注にあたり、その参加条件等として、本制度の取得が求められる場合が想定されますか。求められる場合、業務の内容の機密の程度（個人情報等）に応じて、★３と★４のレベルの違いを求める・求めないがあるでしょうか。また、令和9年度業務（しばしば令和８年度末に公示される）は対象となる可能性があるでしょうか。		政府調達における本制度の活用については、今後検討してまいります。
209	制度構築方針(案)	34	制度の導入促進策	【別添】 ★３・★４要求事項・評価基準（案）を確認しますと、技術的対策として「★3」であっても高度かつ追加費用が掛かる評価項目が見受けられます。 セキュリティレベル向上のために必要な項目となる場合、特に中小企業においては対応したくとも予算的に厳しい企業も多くなることも懸念されます。 本評価制度の対応のため補助金対応も必要ではと考えますので、ご一考をお願いいたします。		いただいた意見については、今後の制度の普及支援の検討の参考にさせていただきます。

No.	該当箇所			寄せられた御意見の概要	理由	提出意見に対する考え方
	該当文書	該当ページ又は項番	該当項目			
210	制度構築方針(案)	34	制度の導入促進策	業界で噂されていることですが、官公庁の入札要件として本制度の星4の取得が盛り込まれる可能性はあるのでしょうか？ もし盛り込まれるのであれば死活問題ですので、会社として相応の人的リソース、(必要に応じて)投資をして星4を取得する予定なのですが、もし盛り込まれない(入札要件になり得ない)のであれば無理せずまずは星3の取得をしたいと考えています。 急に対応出来る内容ではないので余裕を持って取り組むため、こういった情報を早めに明らかにして頂きたいです。 (入札要件にしないで頂きたい、というわけではありません)		政府調達における本制度の活用については、今後検討してまいります。 なお、「政府機関等の対策基準策定のためのガイドライン」では、例えば、外部委託をする際の基本的対策事項としてログの取得・管理を委託先への契約に含めることを求めているところ、ログの取得については★３の基準には含まれておらず★４の基準となっていますので、このような政府統一基準群と本制度の関係を踏まえた検討を行う必要があると考えています。
211	制度構築方針(案)	34	制度の導入促進策	政府調達での参照・活用は検討レベルの表現に留まり、RFI/RFPの要求事項例、スコアリング基準、契約条項例が示されていないため、発注側・応札側双方の実務を支援するテンプレート一式（RFI/RFP例文、評価表、条項例）を公開すべきである。	入札要件化の曖昧さがあるため。	政府調達における本制度の活用については、その具体的方策も含め、今後検討していまいります。
212	制度構築方針(案)	34	制度の導入促進策	支援策の具体名・参照先リンクが未掲示で企業側の探索コストが高いため、補助金・助成・相談窓口のリンク集を付録として提供し、対象要件・申請期限・問合せ先を要約して掲載すべきである。	企業が支援策探索に手間取るため。	本制度の導入促進策については、★取得のための各プロセスにおいてその活用が進むように、適時適切に広報活動を含む普及促進活動をIPAと共に推進して参ります。
213	制度構築方針(案)	34	制度の導入促進策	人材不足の中、本件制度を推進するため各事業者が人材育成をするための金銭的な補助の制度を検討できないか？		いただいた意見については、今後の制度の普及支援や詳細な制度設計等の検討に活用させていただきます。
214	制度構築方針(案)	34	制度の導入促進策	中小企業向けの簡易評価、段階的準拠、費用助成制度の整備を要望します。	限られた人員・予算でも取り組みやすい選択肢を用意することで、より多くの取引先が継続的にセキュリティ水準を高められます。 高負荷の評価のみだと、必要な対策を始める前に断念する企業が生じ、サプライチェーン全体の底上げが進みにくくなります。	いただいた意見については、今後の検討の参考とさせていただきます。
215	制度構築方針(案)	34	制度の導入促進策	対策にかかる費用負担に関して「国支援策の活用」とあるが、これは恒久的に実施されるものでないと、支援策が止まった時点で制度破綻が起きる可能性があると考えます。特に中小企業においては、こういった施策への依存度が高いのは従前までの各施策でも明確になっていると思っておりますので、ご考慮いただく必要があるではと考えます。		いただいた意見については、今後の制度の普及支援の検討の参考にさせていただきます。
216	制度構築方針(案)	34	制度の導入促進策	本制度の周知を徹底するとともに、発注者に対しては、サプライチェーンのセキュリティ確認は原則として本制度に基づくアンケート（評価）を用いて実施するよう、政府として要請していただきたい。	合理的な理由なく別様式のチェックリスト等による評価を求める運用が残ると、要求の標準化・負担軽減という本制度の趣旨に反するため	本制度が、様々な業界で有効に活用されるよう、引き続き関係機関及び業界団体等とも連携しつつ、普及促進に係る取組を進めて参ります。いただいた意見については、今後の制度の普及支援や詳細な制度設計等の検討に活用させていただきます。
217	制度構築方針(案)	34	制度の導入促進策	本施策の趣旨に「サプライチェーンを構成する中小企業は、セキュリティ対策におけるリソースが限られていること／自社のリスクを踏まえてセキュリティ対策を行うことはハードルが高いことから、活用による効果が大きい」とあるが、本評価制度によるリスク特定後の対策については、自社努力で必要な対策を講じることが困難な状況と思料する。 pp.35-37にその対策支援制度（お助け隊サービス、サイバーセキュリティ対策支援者リスト）について記載があるが、これにより本評価制度としてカバーされる範囲と、されない範囲範囲が理解しやすい様に整理いただきたい。	方針書であることは認識しているが、対象に関する誤認識を防ぐことが、事前準備の効率化の観点から重要であると考えるため。また、中小企業における課題については、明確な支援制度を記載することで、制度全体が推進しやすくなると考えるため。	いただいた意見については、今後の制度の普及支援の検討の参考にさせていただきます。
218	制度構築方針(案)	34	制度の導入促進策	業界毎の特性を踏まえた導入促進 政府機関や重要インフラ事業者等における活用の推進 ●業界での足並みが揃う事により評価制度の効果が発揮されるので、本活動の積極推進を期待します	本制度導入の効果（セキュリティ対策の負担軽減）を高めるため。	政府調達における本制度の活用については、今後検討してまいります。 重要インフラ事業者等についても、所管省庁と連携して検討してまいります。
219	制度構築方針(案)	34	制度の導入促進策	■ 意見内容 ★取得にあたり、専門家への依頼や第三者評価の申請等において多額の費用が発生することが予想されるため、中小企業が申請する際には費用負担を軽減するため補助金制度を設けるべき	中小企業においてセキュリティ対策に投じられるリソースは限られているため、★取得に向けた専門家への依頼費用や、★4 の第三者評価における申請費用が過度な負担となる場合、制度利用を断念する企業が多数発生しうる。 ついては、導入促進に向けた費用支援策として、補助金制度を設けるべき。	いただいた意見については、今後の制度の普及支援の検討の参考にさせていただきます。
220	制度構築方針(案)	34	制度の導入促進策	政府において、企業の「攻めのDX投資」を促す施策や補助金制度が多数展開されていますが、これらと同時に企業の「守り」であるサイバーセキュリティへの投資も不可欠と考えます。 そのため、補助金等の支給要件として本評価制度の★取得を組み込むことや、★取得企業へのインセンティブ付与など、制度の普及を後押しする政策的支援を検討いただけないかと考えます。 これにより、事業者の自発的なセキュリティ投資を促し、サプライチェーン全体のセキュリティレベル向上に寄与することが期待されます。		いただいた意見については、今後の制度の普及支援の検討の参考にさせていただきます。
221	制度構築方針(案)	34	制度の導入促進策	「４．制度の導入促進策について」に対する意見 中小企業・小規模事業者の経営資源は限られており、経営者が対応すべき経営課題はサイバーセキュリティ対策のみならず、多岐にわたっており、経営状況・経営課題の可視化・経営課題解決支援の一つのサービスとしてワンストップで提供されることが効果的と考えられます。 また、政府において重点的に取り組まれているデジタル化・DX化等の生産性向上の施策や取組との連携も効果的と考えられます。 つきましては、支援機関や民間事業者が行っている経営改善やデジタル化・DX化等の取組の過程で、サプライチェーンセキュリティ評価制度の利用やセキュリティ対策がへの誘導を行うための取組が拡がるような施策の検討をお願いします。		いただいた意見については、今後の制度の普及支援や詳細な制度設計等の検討に活用させていただきます。
222	制度構築方針(案)	34	制度の導入促進策	本制度が、サプライチェーン全体のセキュリティ水準の底上げを目的とし、特に中小企業の実装負荷軽減を重視している点について賛同する。一方で、★3・★4の要求事項を「理解し、自走的に実装できる状態」まで引き上げるためには、要求事項本文だけでなく、実務者向けの継続的な教育・伴走支援の位置づけを、制度全体の中でより明確に示すことが重要と考える。	多くの中小企業では、セキュリティ対策を「やるべきこと」として認識していても、「要求事項の読み解き」「自社環境への具体的な落とし込み」「評価時に求められる証跡の整備」において専門人材が不足しており、結果として形式的な対応に留まるリスクがあるため。	制度開始までに、制度の詳細な設計及び実務者の皆様に御活用頂けるドキュメントを含む関連文書の整備を予定しているところ、いただいた意見については、今後の制度の普及支援や詳細な制度設計等の検討に活用させていただきます。
223	制度構築方針(案)	34	制度の導入促進策	官民双方におけるサイバーセキュリティ事故の低減を本制度の目的とするのであれば、完全な任意制度に留まらず、一定の実効性を担保する仕組みやインセンティブ設計についても、今後の検討事項として位置づけることが有効ではないかと考える。 例えば、「公共調達や民間取引における入札仕様書・調達要件への反映」「金融機関による融資・与信判断の際の参考情報としての活用」など、制度の活用場面を広げることで、企業の自主的な取組を後押しすることが期待できる。 また、本制度は、発注者が受注者に対してセキュリティ対策の実装を要請することが重要な役割を果たす制度であると理解している。 そのため、受注者側のみならず、発注者側についても、サプライチェーン起因でインシデントが発生した場合に、当該発注者が適切に星の獲得を要請していたか、あるいは制度の活用を検討していたかといった観点で、一定の説明が求められる仕組みを検討してもよいのではないか。	サプライチェーン全体のセキュリティ水準を引き上げるためには、受注者の自助努力だけでなく、発注者による適切な要請・選定行動が不可欠である。 発注者側の行動が制度上、一定程度可視化・意識づけされることで、制度の形骸化を防ぎ、官民双方におけるサイバーセキュリティ事故の低減につながると考える。	本制度が、様々な業界で有効に活用されるよう、引き続き関係機関及び業界団体等とも連携しつつ、普及促進に係る取組を進めて参ります。そのほかいただいた意見については、今後の制度の普及支援や詳細な制度設計等の検討に活用させていただきます。
224	制度構築方針(案)	34	制度の導入促進策	本制度の取り組みの一環として、サンプル規定の整備は、本制度の実効性を高めるうえで極めて重要であると考える。 しかし一方で、サンプル規定の定義や提示方法を誤ると、それが事実上の「正解」「満たすべき完全解」として受け取られてしまう危険性がある点には、強い懸念を抱いている。 中小企業の現場では、サンプル規定といえど、「お上が定義したもの」となる。その内容を「これは自社には合わない」などと取捨選択することは、心理的にも実務的にも極めて困難である。その結果、すべてを満たそうとして過剰な負担を抱え込むか、逆に最初から取り組みを諦めてしまうケースが十分に想定される。 一方で、何の指針も示されない状態では、どこから手を付ければよいか分からず、現場が立ちすくんでしまうこともまた事実である。このジレンマを解消するためには、サンプル規定の書き方自体に、相当の工夫が求められる。 具体的には、 ＊ 必須事項と推奨・オプション事項を明確に区別すること ＊「満たしていない＝不適合」と短絡的に受け取られない表現とすること ＊ 組織の規模や業態に応じて、省略・簡略化・不採用とする判断が許容されることを、繰り返し、明示的に示すことといった配慮が不可欠である。 「これは必ず守るべき最低限」「これは参考例であり、捨てる判断も含めて検討してよい」というメッセージが、文面から自然に読み取れる構成でなければ、サンプル規定は支援ではなく、足かせとなりかねない。 本意見は、過去にIPAの情報セキュリティ関連規定を用いた伴走支援を行う中で、同様の悩みを多くの企業から受けてきた立場からのものである。中小企業の現実に即した制度とするためにも、ガイドラインおよびサンプル規定の設計については、慎重かつ丁寧な検討を強く要望したい。		いただいた意見については、今後の制度の普及支援の検討の参考にさせていただきます。
225	制度構築方針(案)	34	制度の導入促進策	•意見：段階的な評価レベル設定は適切ですが、最低レベルの達成も困難な中小企業向けの支援措置を明記すべきです。自己評価の信頼性担保の仕組みも具体化してください。 •懸念事項：専門人材不在の中小企業における自己評価の実効性、評価取得コストが取引参加の障壁とならないか、形式的なチェックリスト対応に陥るリスクなどが挙げられます。 •提案：評価未達企業への改善計画テンプレートや支援メニューの提示、公的支援（補助金・専門家派遣等）との自動連動も重要です。中小企業向けに、★3取得までの標準的なロードマップや、評価結果に応じた支援策の明示を要望します。		中小企業向けの支援策として、例えばサイバーセキュリティお助け隊（新類型）、中小企業の情報セキュリティ対策ガイドラインの整備拡充及び中小企業向けサイバーセキュリティ対策支援者リストの整備拡充等の、様々な施策を推進して参ります。
226	制度構築方針(案)	34	制度の導入促進策	•意見：情報処理安全確保支援士の活用を制度に明記し、評価者の独立性・利益相反防止の仕組みを具体化することを提案します。★3以上の評価には情報処理安全確保支援士の関与を要件化し、評価者向けの研修・認定制度の整備も必要です。 •提案： -評価スキームへの必須化：★3・★4評価において、セキスペによる確認・助言を必須要件とする。 -専門家リスト連携：IPA公開のセキスペ専門家リストと制度を連動させ、地域・分野別に検索可能な仕組みを構築。 -地方支援体制：中小企業向けに、地方自治体や商工団体と連携したセキスペ派遣制度を整備。 -研修・実践講習連動：セキスペの継続的専門能力開発（実践講習）と制度研修を連動させ、評価制度に対応可能な人材を育成。 -制度広報での明記：制度の公式ガイドラインや広報資料に、セキスペ活用を明記し、認知度を向上。 -共同評価モデル提案：セキスペと評価機関が協働するモデルを試行し、効率的かつ高品質な評価プロセスを確立し、コスト負担を軽減を図ります。	• 理由：外部監査や国家資格者の関与による客観性担保が、制度全体の信頼性向上につながります。自己宣言の信頼性を担保するには、専門知識を持つ第三者の確認が有効です。	制度構築方針(案)においても、情報処理安全確保支援士の活用を明記しているところですが、制度の詳細化に当たっては、評価者の独立性や利益相反防止の仕組みについても検討し、制度の信頼性向上に努めて参ります。
227	制度構築方針(案)	34	制度の導入促進策	•意見：「評価取得がゴール」とならない継続的改善の仕組みや、PDCAサイクルの組み込みが必要です。政府調達における本制度活用の具体的なロードマップ提示や、民間取引での過度な要求を防ぐガイドラインの整備も求めます。	• 理由：サイバー攻撃の手法は日々進化しており、制度の固定化は有効性を失うリスクがあります。社会情勢や技術変化に応じた制度の柔軟な見直し、定期的なアップデート方針の明文化が必要です。	いただいた意見については、今後の制度の普及支援や詳細な制度設計等の検討に活用させていただきます。
228	制度構築方針(案)	34	制度の導入促進策	•意見：評価取得企業へのインセンティブ（公共調達加点、融資優遇、保険料割引等）や、国際制度との相互認証・情報共有の仕組みも検討すべきです。	• 理由：制度参加の動機付けと、グローバルなサプライチェーンの信頼性向上のため、国際連携は不可欠です。	いただいた意見については、今後の制度の普及支援や詳細な制度設計等の検討に活用させていただきます。
229	制度構築方針(案)	34	制度の導入促進策	制度の導入促進策において、「IT導入補助金」等の既存スキームにおける「セキュリティ枠」で、秘密分散技術（SecuShard等）が優先的に採択されるよう明記・連携を図るべきである。		いただいた意見については、今後の制度の普及促進の検討に活用させていただきます。
230	制度構築方針(案)	35	[参考] サイバーセキュリティお助け隊サービス（新類型）について	現行のサイバーセキュリティお助け隊サービスの価格と同程度のソリューション、サービス価格を期待されている理解で良いか。現行のサービスと比較して範囲が広いため、価格設定が適切か確認いただきたい。		いただいた御意見は、サイバーセキュリティお助け隊サービス（新類型）の制度検討に当たっての参考とさせていただきます。
231	制度構築方針(案)	35	[参考] サイバーセキュリティお助け隊サービス（新類型）について	お助け隊（新類型）で「一定の価格要件」との表現のみで規模・範囲に応じた参考価格帯や工数モデル、成果物範囲が明記されていないため、従業員規模・拠点数・SaaS数等に応じた価格レンジと含まれる成果物の標準明細を提示すべきである。	費用、価格の不透明性は中小企業の意思決定を阻害するため。	いただいた御意見は、サイバーセキュリティお助け隊サービス（新類型）の制度検討に当たっての参考とさせていただきます。
232	制度構築方針(案)	35	[参考] サイバーセキュリティお助け隊サービス（新類型）について	規程整備・教育等の人的支援の品質基準が未定義であり、最低到達基準のチェックリストや成果物テンプレート、利用企業の満足度可視化（標準アンケート指標）を設定し、地域・提供者による品質ばらつきを抑制すべきである。	教育・規程の品質差は効果に直結するため。	いただいた御意見は、サイバーセキュリティお助け隊サービス（新類型）の制度検討に当たっての参考とさせていただきます。

No.	該当箇所			寄せられた御意見の概要	理由	提出意見に対する考え方
	該当文書	該当ページ又は項番	該当項目			
233	制度構築方針(案)	35	[参考] サイバーセキュリティお助け隊サービス（新類型）について	補助額の上限緩和を検討してほしい（セキュリティ対策推進枠）	中小企業での現在の対策状況を考慮すると★3・★4取得には上限を超える投資が見込まれるため	いただいた意見については、今後の制度の普及支援の検討の参考にさせていただきます。
234	制度構築方針(案)	35	[参考] サイバーセキュリティお助け隊サービス（新類型）について	（図中、赤点線囲「中小企業セキュリティ普及促進」の「★3・★4 に対応した、新しいお助け隊サービスの開発を検討」に以下を追加） 特に★3 の取得については手厚い支援とする	サイバーセキュリティお助け隊が対象とするのは、これまでサイバーセキュリティ対策に手が回っていない企業に★3 の取得を推進することで、セキュリティ対策水準の底上げに寄与すると考えます。	いただいた御意見は、サイバーセキュリティお助け隊サービス（新類型）の制度検討に当たっての参考とさせていただきます。
235	制度構築方針(案)	35	[参考] サイバーセキュリティお助け隊サービス（新類型）について	■ 意見内容 （図中、上段 2 ポツ目「STEP1（中略）」の文末に、以下を追加） その際、支援内容を部分的に組み合わせて活用できるよう、★ 3 要件を部分的に満たすサービスについても新類型に含める。 ■ 理由（可能であれば、根拠となる出典等を添付又は併記して下さい。） ★取得要件を満たす支援サービスが一定の価格要件の下で導入できることは 魅力だと考えます。他方、要件取得においてアセスメント、ガバナンス強化、技 術要件と横断的なセキュリティサービス提供が必要であり、既に導入している施 策との重複などがある場合、部分的な導入となり価格面でのメリットが受けにくい場合も考えます。また企業にとってベストな組み合わせはそれぞれ異なることから、★要件を部分的に満たすサービスを適宜組み合わせた利用が可能であれば、より活用が進むものと考えます。 併せて、サービス提供側としても、すべての要件を一つの提供事業者のみで完結することは選択肢を狭めることになることから、要件を部分的に支援できる提供事業者も認めることで提供事業者が拡大するものと考えます。	★取得要件を満たす支援サービスが一定の価格要件の下で導入できることは 魅力だと考えます。他方、要件取得においてアセスメント、ガバナンス強化、技 術要件と横断的なセキュリティサービス提供が必要であり、既に導入している施 策との重複などがある場合、部分的な導入となり価格面でのメリットが受けにくい場合も考えます。また企業にとってベストな組み合わせはそれぞれ異なることから、★要件を部分的に満たすサービスを適宜組み合わせた利用が可能であれば、より活用が進むものと考えます。 併せて、サービス提供側としても、すべての要件を一つの提供事業者のみで完結することは選択肢を狭めることになることから、要件を部分的に支援できる提供事業者も認めることで提供事業者が拡大するものと考えます。	いただいた御意見は、サイバーセキュリティお助け隊サービス（新類型）の制度検討に当たっての参考とさせていただきます。
236	制度構築方針(案)	35	[参考] サイバーセキュリティお助け隊サービス（新類型）について	本制度の趣旨であるサプライチェーン全体の対策水準向上を実現するためには、評価制度の提示に加え、対策の実装・運用を支える支援体制が不可欠と考えます。特に中小企業においては、評価取得に向けた準備、未達項目の改善、運用定着までを自力で実施することが難しい場合が多く、制度が普及する過程では支援策の実効性が重要となります。ついては、新お助け隊等の支援策について、支援内容（評価取得支援、改善支援、運用支援等）、提供体制、利用方法、支援範囲や費用負担の考え方等を整理した上で、運用に耐えうる形で準備し、早期に公表いただくことを要望します。		いただいた御意見は、サイバーセキュリティお助け隊サービス（新類型）の制度検討に当たっての参考とさせていただきます。
237	制度構築方針(案)	35	[参考] サイバーセキュリティお助け隊サービス（新類型）について	・製品メーカーが★3　XX項目　★4　XX項目支援可能とプロモーションする場合、取得希望組織または、お助け隊サービスの提供事業者が適正な製品であるかを判断することになりますでしょうか？お助け隊サービスだけではなく、メーカー製品そのものの適正を認証する制度があると取得希望組織は、選定・導入検討を進めやすいですし発注者にも明示しやすいかと思います。 ・既存のサイバーセキュリティお助け隊サービスは、固定メーカーのサービスで提供するソリューションのみが登録されているが、①があれば、お助け隊サービスを提供する事業者が自由にソリューションを組み込め、またエンドユーザーが選択できるため、上記同様にメーカー側による対応製品登録制度があったほうが良いと思います。 ・星4を取るために本制度構築方針(案).のP23に脆弱性検査を行う必要があると掲載されておりますが、取得希望組織が調達時にはその基準が必要最低限クリアしている製品というような要件が必要ではないかという理解です。製品メーカーにとって、その基準と調査内容に対応する必要がありますので、それら情報の公開や、評価制度を作成頂きたいです。 本制度が運用基準であることは理解しておりますが、上記では、基準を満たすために利用する製品も適正であることも、インシデントの防止に重要かと思いますので意見させて頂きました。		いただいた御意見は、サイバーセキュリティお助け隊サービス（新類型）の制度検討に当たっての参考とさせていただきます。
238	制度構築方針(案)	36	[参考] サプライチェーン全体のサイバーセキュリティ向上のための取引先とのパートナーシップ構築促進に向けた想定事例及び解説（概要）	想定事例の（２）（３）において「セキュリティ対策が価格交渉の対象となる」との記述があり、これは発注側企業が受注側企業の対策の金銭負担を容認すると解釈できますが、現行の「下請け法」の内容変更が必要との認識ですが、その準備もされるという事でよろしいでしょうか。		想定事例及び解説は、令和４年10月に策定した「サプライチェーン全体のサイバーセキュリティ向上のための取引先とのパートナーシップの構築に向けて」を補足し、私的独占の禁止及び公正取引の確保に関する法律（独占禁止法）や製造委託等に係る中小受託事業者に対する代金の支払の遅延等の防止に関する法律（取適法）との関係を整理し、これらの法令との関係上「問題とならない」事例を作成とすることを目的としたものです。飽くまでも法令との関係を事例の形で整理するにとどめたものであり、費用負担の在り方にまで言及したものではありませんので、御理解のほどよろしくお願いします。なお、経済産業省としましては、発注者側企業・受注者側企業の双方に対し、作成した想定事例に基づいた価格交渉が実施されるよう普及・啓発を行ってまいります。
239	制度構築方針(案)	36	[参考] サプライチェーン全体のサイバーセキュリティ向上のための取引先とのパートナーシップ構築促進に向けた想定事例及び解説（概要）	要求事項によっては、付加の高い運用やシステムの導入によってしか実現できないものがある。 セキュリティの確保により、発注者も利益を得ることから、発注者も応分の負担を行う旨制度構築の中で明示いただきたい。		想定事例及び解説は、令和４年10月に策定した「サプライチェーン全体のサイバーセキュリティ向上のための取引先とのパートナーシップの構築に向けて」を補足し、私的独占の禁止及び公正取引の確保に関する法律（独占禁止法）や製造委託等に係る中小受託事業者に対する代金の支払の遅延等の防止に関する法律（取適法）との関係を整理し、これらの法令との関係上「問題とならない」事例を作成とすることを目的としたものです。飽くまでも法令との関係を事例の形で整理するにとどめたものであり、費用負担の在り方にまで言及したものではありませんので、御理解のほどよろしくお願いします。なお、経済産業省としましては、発注者側企業・受注者側企業の双方に対し、作成した想定事例に基づいた価格交渉が実施されるよう普及・啓発を行ってまいります。
240	制度構築方針(案)	36	[参考] サプライチェーン全体のサイバーセキュリティ向上のための取引先とのパートナーシップ構築促進に向けた想定事例及び解説（概要）	取引先への要請等に係る考え方の整理に、独占禁止法等との考え方整理に言及はあるものの、セキュリティ費用の転嫁や価格交渉の透明性を担保する実務枠組み（費用算定テンプレート、交渉記録様式、第三者仲裁窓口）が示されておらず、CAPEX/OPEXの内訳モデルと証跡化のフォーマット、紛争解決窓口を導入促進策として明示すべきである。	セキュリティ費用転嫁の妥当性争いを避け、透明性が必要であるため。	想定事例及び解説は、令和４年10月に策定した「サプライチェーン全体のサイバーセキュリティ向上のための取引先とのパートナーシップの構築に向けて」を補足し、私的独占の禁止及び公正取引の確保に関する法律（独占禁止法）や製造委託等に係る中小受託事業者に対する代金の支払の遅延等の防止に関する法律（取適法）との関係を整理し、これらの法令との関係上「問題とならない」事例を作成とすることを目的としたものです。飽くまでも法令との関係を事例の形で整理するにとどめたものであり、費用負担の在り方にまで言及したものではありませんので、御理解のほどよろしくお願いします。なお、経済産業省としましては、発注者側企業・受注者側企業の双方に対し、作成した想定事例に基づいた価格交渉が実施されるよう普及・啓発を行ってまいります。
241	制度構築方針(案)	36	[参考] サプライチェーン全体のサイバーセキュリティ向上のための取引先とのパートナーシップ構築促進に向けた想定事例及び解説（概要）	未対応発注者への是正・救済手段が相談に留まり実務手順が不足しているため、簡易申入れ書式、標準プロセス（期限・回答義務）、第三者メディエーション手続を整備し、紛争予防と迅速解決を図るべきである。	発注者側の不公平に対する救済が必要であるため。	想定事例及び解説は、令和４年10月に策定した「サプライチェーン全体のサイバーセキュリティ向上のための取引先とのパートナーシップの構築に向けて」を補足し、私的独占の禁止及び公正取引の確保に関する法律（独占禁止法）や製造委託等に係る中小受託事業者に対する代金の支払の遅延等の防止に関する法律（取適法）との関係を整理し、これらの法令との関係上「問題とならない」事例を作成とすることを目的としたものです。飽くまでも法令との関係を事例の形で整理するにとどめたものであり、費用負担の在り方にまで言及したものではありませんので、御理解のほどよろしくお願いします。なお、経済産業省としましては、発注者側企業・受注者側企業の双方に対し、作成した想定事例に基づいた価格交渉が実施されるよう普及・啓発を行ってまいります。
242	制度構築方針(案)	36	[参考] サプライチェーン全体のサイバーセキュリティ向上のための取引先とのパートナーシップ構築促進に向けた想定事例及び解説（概要）	受注者が本制度への適合や対策強化（★取得等）のために追加費用を要する場合、発注者が合理的理由なく費用負担の協議を拒否したり、費用協議を理由に取引停止・不利益取扱いを示唆したりしないことを、制度の運用指針（発注者の責務）として明記してほしい。あわせて、費用協議の標準プロセス（見積内訳の標準項目、協議期限、合意形成の手順）を提示していただきたい。	費用負担が受け入れられない運用が常態化すると、受注者が制度対応を継続できず、結果として制度の普及・定着が阻害されるため。	想定事例及び解説は、令和４年10月に策定した「サプライチェーン全体のサイバーセキュリティ向上のための取引先とのパートナーシップの構築に向けて」を補足し、私的独占の禁止及び公正取引の確保に関する法律（独占禁止法）や製造委託等に係る中小受託事業者に対する代金の支払の遅延等の防止に関する法律（取適法）との関係を整理し、これらの法令との関係上「問題とならない」事例を作成とすることを目的としたものです。飽くまでも法令との関係を事例の形で整理するにとどめたものであり、費用負担の在り方にまで言及したものではありませんので、御理解のほどよろしくお願いします。なお、経済産業省としましては、発注者側企業・受注者側企業の双方に対し、作成した想定事例に基づいた価格交渉が実施されるよう普及・啓発を行ってまいります。
243	制度構築方針(案)	37	[参考]中小企業向けサイバーセキュリティ対策支援者リストについて	専門家リストがPDF試行公開前提で検索性・フィルタリング性が低いため、Web検索フォームとAPI連携を提供し、地域・料金帯・対応★要件（★3/★4）・指導テーマ等のフィルタを実装すべきである。	PDFであると中小企業のマッチング効率が悪いため。	専門家リストの改善に向けて、本御意見を今後の検討の参考にさせていただきます。
244	制度構築方針(案)	37	[参考]中小企業向けサイバーセキュリティ対策支援者リストについて	専門家リストに本制度研修（★3作業従事者研修／★4評価従事者研修）の受講ステータスが表示されておらず制度適合性の判断が難しいため、研修受講済みフラグ、最新受講日、受講コース名を必須項目として追加し、検索フィルタで絞り込めるようにすべきである。	制度適合の判別が難しいため。	専門家リストの改善に向けて、本御意見を今後の検討の参考にさせていただきます。
245	制度構築方針(案)	39	今後の検討の進め方及びスケジュール	本制度のスケジュールについて、令和8年度下期運用開始(想定)と記述があるが、これは、本評価制度のエントリーを受付、評価を完了したという意味でしょうか？		本制度の取得に係る申請の受付開始を想定しています。
246	制度構築方針(案)	39	今後の検討の進め方及びスケジュール	運用開始直後の申請集中や評価機関体制の過渡期に備えた段階的申請受付、暫定認定（プロビジョナル）、失効猶予、優先審査、申請スロット制等の移行措置の方針が未記載であり、キャパシティ計画（処理件数・目標リードタイム）と併せて暫定運用を明確化すべきである。	初年度は評価機関の体制未整備や申請集中が懸念されるため。	いただいた意見については、詳細な制度設計等の検討に当たっての参考とさせていただきます。
247	制度構築方針(案)	39	今後の検討の進め方及びスケジュール	こちらは制度に準拠するために準備を行っております。 以前の制度開始は「10月以降」となっていましたが現在は令和８年度末頃、と変わっています。 明確な制度開始時期や、制度整備の進捗をこまめに教えていただきたいです。 いつまでに何をすればよいかハッキリしなくなりますので、進捗はこまめに教えていただきたいです。		いただいた意見については、今後の検討の参考とさせていただきます。
248	制度構築方針(案)	39	今後の検討の進め方及びスケジュール	制度詳細化の過程において、完了した部分から順次公表するなど、企業が制度対応を円滑に進めることができるよう措置を検討いただきたい。	当該制度を活用する企業が、迅速に制度対応を行いサイバーセキュリティの確保を実現するため、できるだけ早いタイミングで詳細化された内容を公表することが求められるため。	いただいた意見については、今後の検討の参考とさせていただきます。
249	制度構築方針(案)	全般		欧州CRA法にも関連するため、OTシステム、製品に組み込まれるシステムにおいても制度策定が並行して求められる。		いただいた意見については、今後の検討の参考とさせていただきます。
250	制度構築方針(案)	全般		国家が最低限のセキュリティ防御基盤を整備・保証し民間ベンダーと役割分担を行いながら中小企業を含むサプライチェーン全体の底上げを図るという枠組みが必要である。 これこそが、「国家の責任において提供・保証されるセキュリティ対策基盤」という位置づけであり、SCS対策評価制度を持続可能な制度とするために不可欠であると考える。		いただいた意見については、今後の検討の参考とさせていただきます。
251	制度構築方針(案)	全般		本制度が、委託元企業の第三者リスク管理を代替するものではなく、補完的な位置づけであることを明確に示すことが重要と考える。認証取得企業が同認証の取得という表面的な情報開示だけを以て、追加の評価や情報開示を拒むようなケースが生じることは避けたい。		いただいた意見については、詳細な制度設計等の検討に当たっての参考とさせていただきます。
252	制度構築方針(案)	全般		弊社として本案に対し賛同の意見を申し上げます。	DX の推進やコロナ禍移行の働き方の変化において、IT システムの重要度が増す中、サプライチェーンへのランサムウェアなど環境破壊型のサイバー攻撃による被害は、我が国の生活基盤や製造業の安定的な生産において大きな課題となっています。 サイバーセキュリティ対策そのもの複雑度が増す中、発注者にとって対策状況の可視化を可能にするだけでなく、サプライチェーンにあたる事業者にとってもセキュリティ対策の度合いが指標化され、具体的に満たすべき基準が貴省から示されたことは、我が国全体のサイバーセキュリティ強化に有用な取り組みとして時宜を得たものと認識しております。 サイバーセキュリティサービスを提供する事業者として、これらの枠組みの活用を推進する取り組みを積極的に参画する所存です。	本制度への賛同の御意見として承りました。

No.	該当箇所			寄せられた御意見の概要	理由	提出意見に対する考え方
	該当文書	該当ページ又は項番	該当項目			
253	制度構築方針(案)	全般		・経産省フォーマットを当社フォーマットへ項目レベルでマッピングし、社内の有資格者（情報処理安全確保支援士／CISSP／CISA）が内容妥当性を承認したうえで 「星3準拠」とする運用を想定している。 併せて、取得企業名・所在地・更新回数・適用範囲等の情報を、当社にてグループ内の星3認定企業を経産省に一括申請する方式を取りたいと考えています。当該運用方式を制度運用に盛り込んで頂きたい。	新設される「★3」は自己診断方式で、当社のセキュリティ調査と類似するため、セキュリティ調査と制度要件の統合を部署内で検討中。 ・今回のパブコメでは、制度運用に関する課題感を提示し、併せて実務担当者レベルでの協議を開始予定。 期待効果（制度と自社調査のアラインメントが図れた場合） ・関係会社への星3取得促進によるグループ全体の信頼性・レピュテーション向上 ・サプライチェーンで用いられるセキュリティチェックシートへの個別回答の代替可能性・負担軽減	いただいた意見については、詳細な制度設計等の検討に当たっての参考とさせていただきます。
	制度構築方針(案)	全般		・日本に商流・サプライチェーンを有する海外企業についても「星3」を取得可能か、可否の判断および必要条件・手続（提出経路、証跡要件、台帳登録の取扱い）をご教示いただきたい。 あるいは、海外各国の同等制度との連携について現時点で予定されていることがあればご教示いただきたい。	新設される「★3」は自己診断方式で、当社のセキュリティ調査と類似するため、セキュリティ調査と制度要件の統合を部署内で検討中。 ・今回のパブコメでは、制度運用に関する課題感を提示し、併せて実務担当者レベルでの協議を開始予定。 期待効果（制度と自社調査のアラインメントが図れた場合） ・関係会社への星3取得促進によるグループ全体の信頼性・レピュテーション向上 ・サプライチェーンで用いられるセキュリティチェックシートへの個別回答の代替可能性・負担軽減	「海外企業」には様々な形態が想定されるところ、少なくとも我が国に拠点又は本社機能等を有する企業(日本企業の海外子会社や外資系企業の日本法人等)であれば、本制度について申請することは可能となる予定です。いただいた意見については、詳細な制度設計等の検討に当たっての参考とさせていただきます。
255	制度構築方針(案)	全般		★3／★4の取得・維持にかかる標準的な費用レンジや所要期間のベンチマークを公表すべき。これらが不透明なままでは、事業会社側での予算立案時に適切な見積りができず、予算不足のリスクが高まる。	情報が不透明なままでは、予算立案時に適切な見積りができず、予算不足や計画遅延のリスクが高まる。透明性を確保することで、企業側の計画精度を向上させるため。	★を取得するためにかかる費用や期間については、各取得希望組織が講ずるセキュリティ対策の状況によって様々であるほか、特に費用については、最終的には市場の競争原理によって決定されるものであると考えられます。 そのうえで、サイバーセキュリティお助け隊サービス(新類型)に係る実証事業等を通じて、★を取得するためにかかる費用の目安については、今後検証してまいります。また、★の取得に必要な評価にかかる期間については、SCS評価制度に係る実証事業にて検証の上、制度構築方針P.23記載のとおり、想定する所要期間を記載しています。
256	制度構築方針(案)	全般		本制度は評価・認定後に侵害が発生した場合の扱いを明確にすべきである。	評価制度は『守れなかった場合』の想定がなければ実効性を持たない。インシデント発生時の報告義務、評価見直し、認定の失効条件等を明示することで、形式的運用を防止できる。	いただいた意見については、詳細な制度設計等の検討に当たっての参考とさせていただきます。
257	制度構築方針(案)	全般		本来的には委託業務のリスクオーナーは委託元であり、委託業務内のリスク管理は委託元自身が行うべきものである。そのため、一般的な対策ではリスクが受容できない場合は、委託元が管理策を明示する責務があり、その責務を果たさなかった場合は委託元の責に帰することは明確にすべきである。		いただいた意見については、詳細な制度設計等の検討に当たっての参考とさせていただきます。
258	制度構築方針(案)	全般		委託元がその立場を利用して正当な対価なくリスク対応を委託先に負わせる行為を制度として禁止すべきである。		想定事例及び解説は、令和４年10月に策定した「サプライチェーン全体のサイバーセキュリティ向上のための取引先とのパートナーシップの構築に向けて」を補足し、私的独占の禁止及び公正取引の確保に関する法律（独占禁止法）や製造委託等に係る中小受託事業者に対する代金の支払の遅延等の防止に関する法律（取適法）との関係を整理し、これらの法令との関係上「問題とならない」事例を作成とすることを目的としたものです。飽くまでも法令との関係を事例の形で整理するにとどめたものであり、費用負担の在り方にまで言及したものではありませんので、御理解のほどよろしくお願いします。なお、経済産業省としましては、発注者側企業・受注者側企業の双方に対し、作成した想定事例に基づいた価格交渉が実施されるよう普及・啓発を行ってまいります。
259	制度構築方針(案)	全般		委託元は委託先でリスクが顕在化した際の全ての責任を委託先に負わせるのではなく、リスクを低減するために委託元も対策を講じる義務があることを明記すべきである。(例： 委託先からのアクセス制限や異常の監視等)		いただいた意見については、今後の検討の参考とさせていただきます。
260	制度構築方針(案)	全般		委託元は委託先が求めるリスク管理ができていない際に取引の停止を選択するのではなく、委託元がリスク対応を代理できるか(環境の提供・端末の貸与等)確認して、対応できることは対応すべきである。		いただいた意見については、今後の検討の参考とさせていただきます。
261	制度構築方針(案)	全般		・現状ISO27001は審査会社の増加によって厳格さに違いがでておりますので、是非新制度では、ばらつきがなるべくでにくい講習・制度設計をお願いできればと思います。		いただいた意見については、詳細な制度設計等の検討に当たっての参考とさせていただきます。
262	制度構築方針(案)	全般		・ISO27000シリーズは経過観察等比較的柔軟な措置がとれる関係で（維持・継続審査にて継続的な改善はもとめられるものの）、ほぼ取得できない会社がいない状態になっている認識です。もちろん取得していないのと比較すると取得しているほうがセキュリティ対策としてはよいものの、実質有名無実化してしまっている部分もあるため、取得可否含めて厳格な制度としていただきたいと思っています。		いただいた意見については、詳細な制度設計等の検討に当たっての参考とさせていただきます。
263	制度構築方針(案)	全般		・ISMAPの初期の時のように審査会社数が足りず、審査依頼を行っても時間がかかる・コストが高すぎる状態にならないようにしていただけると幸いです。		いただいた意見については、詳細な制度設計等の検討に当たっての参考とさせていただきます。
264	制度構築方針(案)	全般		本制度は特にサプライチェーンに中小企業が多く、セキュリティの基準の理解や要請が難しい業界には非常に有用であると思っています。 弊社はセキュリティアセスメントに特化したSaaSを提供している日本の大企業様にサードパーティーリスクマネジメントのサービスとしてご利用をいただいておりますが、大企業になればなるほど、業界や業務ごとのアセスメント内容に特色がでるため、なかなか本評価制度のみで委託先調査を無しとできない会社が多そうであると感じています。（特に★3レベルだとあくまでベースラインであり、大企業の要件を満たさない場合も多い印象） 本制度の目的としては、引き続き案件毎に確認が必要なものについては、企業間で個別のやりとりを想定している認識でよろしいでしょうか。 そうだとすると一部の負荷削減にはなるものの、本質的な課題の解決にまでは至らないのではないかと考えており（逆に管理コストが上がる可能性もあり）、スタンスや今後想定をしている展開があればご教示ください。 例：取引金額や取引重要度によってどこまでの審査を求めるのが適正かもふくめて経産省・公正取引委員会のほうで強く基準をだし、個別の調査がお粉れるような案件を最小限とする ※一方で近年では再委託先審査の負荷が非常に大きくなっているため、再委託については本制度内容のみとできるケースは大いにあるのではと思っており、委託元・委託先両方の負荷軽減になるのではないかと期待をしています。		本制度についてはサプライヤー企業等における共通のベースラインとして活用されることを想定しており、必要に応じて企業間等で個別のやりとりを行うことを想定しています。 いただいた意見については、制度の普及支援や詳細な制度設計等の検討に当たっての参考とさせていただきます。
265	制度構築方針(案)	全般		近年、企業活動におけるサプライチェーンの複雑化・高度化に伴い、サプライチェーン全体に影響を及ぼすサイバーリスクが顕著に増大しています。その中で、本評価制度はサプライチェーン全体でのセキュリティ水準向上を促進する極めて重要な取り組みであり、業種や企業規模を問わず幅広く普及・推進されるべき制度であると考えております。		本制度への賛同の御意見として承りました。
266	制度構築方針(案)	全般		サプライチェーン強化に向けたセキュリティ対策評価制度に関する 制度構築方針(案)(R7年12月発行)のP11に関しまして、 取得希望組織である当社が★３や★４マークの使用許可を得るためには、 IPA事務局への登録申請が必要になるのは理解できます。 しかし、最初から「セキュリティ専門家」や「評価機関」が介入しないと 登録申請が難しいような【登録申請】のフォーマットは回避頂きたく存じます。 当社を含む中小企業には【情報システム専門部門】の設置がない企業が多数存在するものと存じます。そうしますと、★３★４取得はしなければいけない場合に、最小限の支出とするために、直接IPA事務局に★３★４の登録申請を希望したいと考えるはずですが、【登録申請】のフォーマットが最初から複雑であると、「セキュリティ専門家」に確認依頼をする手段しかないと言っても過言ではないと思います。 【登録申請】のフォーマットを可能な限りわかりやすいものとし、 取得希望組織自身で★３★４の登録申請が容易となるように、 【登録申請】時に必要なドキュメントがあれば、その記入例の事前提示、 もしくは、IPA事務局の登録申請の受付(窓口)に申請に係る相談窓口を 設けていただけますと運用性が高まるものと考えております。 P11より、当社(取得希望組織)は、直接IPA事務局に対し、 ★３★４登録申請をする方針となっております。 その実現のために可能な限りの明確な情報開示の程、よろしくお願い申し上げます。		いただいた意見については、詳細な制度設計等の検討に当たっての参考とさせていただきます。
267	制度構築方針(案)	全般		本制度の導入により、発注企業からクラウド事業者に対し、対策状況の確認（アンケートや個別の監査要請）が殺到することが予想されます。対応の円滑化のため以下の措置をご検討いただけますと幸いです。 （１）確認業務の標準化・プラットフォーム化： 多数の顧客が個別にExcel等の独自フォーマットで問い合わせてくる場合、SaaS事業者にとって対応が非常に困難です。SaaS事業者が一度情報を登録・公開すれば、顧客がそれを参照するだけで確認が完了する「共通プラットフォーム（Trustサイト等）」を政府主導で整備することを要望します。 （２）「過剰な要求」の抑制： 一般的に、念のため幅広にという趣旨で取引先からセキュリティや競争上の理由で開示困難な機微情報（例えば詳細なネットワーク図や脆弱性診断のデータ等）を要求されるリスクがあります。そのため、取適法の観点だけでなくセキュリティの観点でも過剰な開示要求を避けるよう周知を徹底いただくとともに、過度な要求を防ぐためのSaaS向けの「標準回答雛形」や「確認ガイドライン」等を策定し、発注企業側含めて周知していただくことを要望します。		いただいた意見については、今後の検討の参考とさせていただきます。
268	制度構築方針(案)	全般		本制度の要求事項自体はNIST CSF等に準拠した標準的なものと認識していますが、制度運用にあたっては、「監査対応コストの増大」がベンダーの負荷増大や価格転嫁によるDX推進の阻害要因とならないよう、ベンダー負担を最小化するための配慮を要望します。 （１）既存認証との重複排除とコスト抑制 多くのクラウド事業者は既にセキュリティ認証を取得しており、本制度の確認事項と多くが重複しています。既存認証の活用により、「既に実施済みの事項を改めて証明する」ための膨大なリソース（金銭・時間・人員）の浪費を避ける施策や、政府による費用支援を検討いただくことを希望します。 中堅・スタートアップへの配慮 特に★4取得時等の第三者評価費用は、中堅・スタートアップ規模のSaaSベンダーにとってビジネス継続に関わる重い負担となります。コスト増がサービス価格へ転嫁されれば、ユーザー側のDX推進を阻害する要因にもなりかねません。 （２）インセンティブ設計と「実質的な強制化」の回避 各企業の認証取得コストを上回るインセンティブの設計を期待します。また、「実質的な強制化」に繋がる運用については、極めて慎重な検討を強く要望します。		いただいた意見については、今後の検討の参考とさせていただきます。

No.	該当箇所			寄せられた御意見の概要	理由	提出意見に対する考え方
	該当文書	該当ページ又は項番	該当項目			
269	制度構築方針(案)	全般		（１）監査リソースの枯渇（ボトルネック）への懸念: 現在でも既にISMAP等の監査において、監査法人のリソース不足により審査期間の長期化、審査費用の高止まりが顕在化しています。本制度で「3年ごとの第三者評価」および「毎年の自己評価提出」を求め、かつ全国規模のサプライチェーン企業が殺到した場合、評価機関のリソースの逼迫に拍車をかける事態となります。監査待ち難民、長期の監査対応等により不当にビジネス機会を損失する事業者が発生しないよう、制度設計の検討を要望します。 （２）「専門家」の要件緩和と自動化の検討: ★3の「セキュリティ専門家」や★4の「評価機関」の要件が厳格すぎると、対応できる人材・組織が限定されます。日本におけるサイバーセキュリティ人材の不足等も踏まえ、SaaS事業者の実態に即し、既存の内部監査体制の活用や、自動化ツールによる技術評価の受入など、柔軟な評価手法が取り入れられることを要望します。 （３）「登録ラッシュ」への対応能力: 制度開始と同時に、発注企業からの要請を受けた多数の事業者が登録に殺到することが予想されます。現在の事務局および評価機関の体制案で、全国規模の申請を遅滞なく処理できるのか、具体的なシミュレーションとキャパシティ計画に基づく制度設計を要望します。 （４）形骸化の防止: リソース不足の中で大量の登録を処理するために、審査が形骸化（チェックリストを埋めるだけの作業）し、本来の目的であるセキュリティレベルの向上が疎かになるリスクがあります。質を担保できない場合は、制度の適用範囲を限定すべきです。		いただいた意見については、今後の検討の参考とさせていただきます。
270	制度構築方針(案)	全般		受審費用の早期提示： 令和８年度下期の実用開始に対し、多くの企業では１月前後に次年度予算を策定する。 普及を促進するため、受審費用や対策工数の目安を速やかに提示し、予算策定における予見性を確保できるよう検討いただきたい。		いただいた意見については、今後の検討の参考とさせていただきます。
271	制度構築方針(案)	全般		暗号鍵管理に依存せず、データを分割・分散して保護する「秘密分散技術」は、ランサムウェア対策や内部不正・外部侵入時の被害最小化の両面で有効であり、評価制度における「推奨される技術的実装例」として明示的に位置付けることが望ましい。		秘密分散技術はセキュリティ侵害に対する被害の最小化に有効な手段の一つと認識しているところ、頂いた御意見は制度開始までに整備を予定するガイダンス資料等の作成の検討に活用させていただきます。
272	制度構築方針(案)	全般		サプライチェーン全体の強靭化と将来的な脅威への対応として、「秘密分散技術（Secret Sharing）」の活用を制度方針の中に明記し、推奨技術として位置付けるべきである。特に、中小企業（SME）への導入促進策として、SecuShard等の秘密分散ソリューションの導入を支援する補助金スキームとの連携を強化すべきである。		いただいた意見については、今後の検討の参考とさせていただきます。
273	制度構築方針(案)	全般		制度を実効性あるものとするため、以下の点を提案します。 1.制度目的として「継続的なサイバーレジリエンス強化」を明文化し、評価・認証の取得自体を目的化しない考え方を明確にすること。 2.各業務部門が自らの改善点を理解できるよう、業務プロセスに埋め込まれた対策を評価するスキームとすること。 3.図書整備の有無だけでなく、運用実績を重視するとともに、ガバナンスや役割分担（部署・役職単位）を明確にすること。 4.KPIの例や見直しトリガー（インシデント、重大な業務変更等）を示し、継続的改善サイクルが自然に回る設計とすること。 5.企業や部門の状況に応じて次の段階へ進めるよう、段階的な成熟度モデルを設定し、移行期間や期間を区切った例外管理を認めることで、現実的な運用を担保すること。 6.セプライヤに対しても自律的な改善を促すため、受注者が発注者に対して提示する改善レバーとなるような評価・契約に用いるテンプレートやガイドの整備など、具体的な支援策を併せて提示すること。 7.期限付き例外を台帳化し、代替措置・責任者・期限・更改計画を明記。延長時は経営承認とリスク差分の説明責任を必須とすること。		いただいた意見については、今後の検討の参考とさせていただきます。
274	制度構築方針(案)	全般		■業界団体に「その業界の実態に即した共通水準の『手引』」を作成させる →例えば電子機器業界と食品業界では「共通的に達成すべき水準」はイコールではないはずである（情報の遣り取りやEDI取引・頻度などは相当の際があるはずである） →「サプライチェーンセキュリティ強化」が目的である以上、個々の企業だけでなく、業界団体は確実にステークホルダーである ■企業毎に自社サプライチェーン企業に本制度への対応を指示させるのではなく、業界団体から対応を指示する ■企業規模に応じ自社に制度案で掲げているセキュリティ有識者（情報処理安全確保支援士等）を必置とすることで、自社対応力を自社で上げる、という方向づけを明確に行う →もはや企業におけるサイバーセキュリティは労働安全衛生法における安全管理者・衛生管理者のレベルにあると考えている（事業・操業環境を適正管理しそれを継続的に維持する役割という点は類似している理解） といったことを、「実効性とフィジビリティを両立させることによる、早期＆確実なサプライチェーンセキュリティ強化」のために制度主管省庁として進めていただきたい。		いただいた意見については、今後の検討の参考とさせていただきます。
275	制度構築方針(案)	全般		企業は取引先企業の「星（★）の取得状況」の確認にとどまらず、可能な範囲で「具体的な対策実施項目の回答（チェックリストの項目別回答など）」を収集することが望ましい旨を要件またはガイドラインのメッセージとして発信していただきたい。	単に「星の取得の有無」を確認するだけでは、バイヤー企業は「自社のサプライチェーン上のどこに具体的な脆弱性が潜んでいるか」を特定することができません。また、産業界のセキュリティ水準向上のためには、バイヤー企業がサプライヤーに対して要求を出すだけでなく、未達成項目について改善策を提案し、対策実行まで伴走支援を行うことが重要です。そのためには「星の取得の有無」だけでなく、どの対策が実施できていないかという「具体的な状況」までも把握する必要があります。制度としてこの重要性を発信することが、実効性のあるサプライチェーン強化につながると考えます。	いただいた意見については、詳細な制度設計等の検討に当たっての参考とさせていただきます。
276	制度構築方針(案)	全般		回答側の負担を軽減するために、発注者が「すでに多くの大企業が実施している調査（BCP、人権DD、CSR等）と合わせて実施する」ことが有効であることを、想定事例として情報共有していただきたい。	効率的かつ統合的なサプライチェーン管理を促進するためにサプライヤーの負担軽減は重要ですが、負担軽減は提出情報の最小化だけでなく、調査の統合によっても実現可能です。 多くのバイヤー企業は重要なサプライヤーに対し、セキュリティ以外にもBCPや人権対応など多岐にわたる調査を行っています。セキュリティ調査を既存の調査とセットで実施することは、サプライヤー・バイヤー双方にとっての工数削減につながると考えます。	いただいた意見については、詳細な制度設計等の検討に当たっての参考とさせていただきます。
277	制度構築方針(案)	全般		サプライチェーンリスク管理について、クラウドサービス提供者や外部情報サービスを対象化している点は評価できるが、再委託先、OSS、共通コンポーネントの脆弱性波及といった間接・連鎖リスクの扱いは限定的である。国際標準では連鎖リスクが重視されており、制度案でも明示的に取り扱うことが望ましい。	・国際標準（CSF2.0・CRA・ISO27001）では、サプライチェーンの連鎖リスクが重要論点とされている。	いただいた意見については、今後の検討の参考とさせていただきます。
278	制度構築方針(案)	全般		昨今発生している大規模なサイバーセキュリティインシデントの多くは、表面的にはVPNの脆弱性や設定ミスと報道されています。しかし、これらは事故に至った「事象」に過ぎず、真の要因はそれらを引き起こす組織構造や労働環境といった「組織的要因」にあります。 ヒューマンエラーは個人の能力や認識不足に帰せられるべきものではなく、エラーを誘発する仕組みや、安全よりも効率を優先せざるを得ない組織風土の問題として捉えるべきです。特にリソースが限られる中小企業や製造現場では、効率性と利便性の追求が優先され、セキュリティが形骸化しやすい実態があります。 VUCAの時代において、サプライチェーンには単なる効率性ではなく、変化に即応できる「レジリエンス（強靭性）」が求められます。失敗を個人の責任として処罰・叱責する文化では、従業員は萎縮し、新たな課題の発見や挑戦を避けるようになります。経営層が自ら「失敗から学習する文化」を推奨し、心理的安全性を確保しながら新しい課題に挑む姿勢を後押しすることが、結果として組織全体の防御力を高めることにつながります。 我が国の製造業は、これまで現場の安全管理において、ジェームズ・リーズンが提唱した「安全文化」を世界に先駆けて体現し、高品質な製品を生み出してきました。この日本が培ってきた「安全に関する知見とノウハウ」は、サイバーセキュリティの領域にも十分に転用可能です。 本評価制度が、単なる技術的なチェックリストに留まることなく、組織文化や経営層のコミットメントを評価軸に組み込み、日本発の「サイバー安全文化」として世界をリードするガイドラインとなることを切に願います。		いただいた意見については、今後の検討の参考とさせていただきます。
279	制度構築方針(案)	全般		本評価を受けることによる、経済的メリットや税制上のメリットの創出をご検討いただきたい。自社に係るサプライチェーン全体で本評価を活用しようとした場合、特に中小企業も含めた包括的対策を取る場合において、多大なセキュリティ費用が発生すると想定されるため優遇措置を期待するものである。		いただいた意見については、今後の検討の参考とさせていただきます。
280	制度構築方針(案)	全般		欧州にて施行されているGDPRを参考にする場合は、法令として義務化させることを念頭において施行することにより、「必要性」の変容を促すべきである。		いただいた意見は、今後の検討の参考させていただきます。
281	要求事項・評価基準案	1-4-1		★4における「定期的な経営層への報告」を有効なものにするためには、年1回のチェックシートによる点での評価に基づいた報告ではなく、継続的な状況把握によって経営層の的確な判断が出来る報告になると考えてます。		いただいた意見については、今後の検討の参考とさせていただきます。
282	要求事項・評価基準案	2-1-3		要求事項 2-1-3、評価基準 No.2-1-3-1 における取引先のセキュリティ対策状況の把握方法（例）として、「セキュリティスコアリングサービスによって第三者の客観的な評価する」といった手法を追記することを検討していただきたい。 近年、取引先のセキュリティ対策状況を継続的に把握・管理する手段として、外部から観測可能な情報をもとに評価を行うセキュリティスコアリングサービスの活用が広がっている。 評価基準において当該手法が例示されることで、企業が本評価基準への適合性を判断しやすくなり、実務に即した対策状況の把握が進むと考える。	サプライチェーンにおけるセキュリティリスク管理では、多数の取引先の対策状況を定期的かつ効率的に把握することが求められる一方、個別の確認やヒアリングのみによる管理には限界がある。 セキュリティスコアリングサービスは、「外部から観測可能な情報をもとに評価を行う」「継続的・定量的な把握が可能である」といった特徴を有しており、取引先のセキュリティ対策状況を把握する実務上の有効な手段の一つである。 評価基準の把握方法の例示に当該手法が含まれていない場合、企業が「評価基準に該当するか否か」を判断できず、活用をためらう可能性があるため、セキュリティスコアリングサービスを把握方法の一例として位置づけることが、制度の実効性および普及性の向上につながると考える。	いただいた意見については、今後の検討の参考とさせていただきます。
283	要求事項・評価基準案	2-1-3		要求事項 2-1-3 の記載について、評価基準においては「自社の事業継続にとって重要な位置づけを持つ取引先」「当該取引先の環境から発注者の内部システムへのアクセスが可能な取引先」といった観点も、対策状況把握の対象として示されている。 一方、要求事項の文言からは、これらの観点が読み取りにくく、「重要な機密情報を取り扱う取引先」のみに対象が限定されているとの誤解を招くおそれがある。 このため、評価基準との整合性を確保し、対象範囲をより明確にする観点から、要求事項 2-1-3 の表現を以下のように修正することを検討してはどうか。 ＜要求事項案＞ サプライチェーン上の関係性により、事業継続リスク及び情報管理リスクの観点から自社に影響を及ぼす可能性のある取引先のセキュリティ対策状況を把握すること。	サプライチェーンに起因するサイバーリスクは、機密情報の漏えいにとどまらず、「取引先を起点とした内部システムへの侵入」や「重要業務の停止による事業継続への影響」といった形で顕在化するケースも多い。 実際、評価基準では「機密情報の取扱い」に加え、「事業継続上の重要性」や「内部システムへのアクセス可否」といった観点が対策状況把握の対象条件として整理されている。 要求事項の文言がこれらの観点を包含していない場合、制度の趣旨や評価対象範囲について誤解を招く可能性があるため、要求事項と評価基準の表現を整合させることが重要である。 これにより、発注者・受注者双方にとって判断基準が明確となり、本制度の実効性の向上および運用の円滑化につながると考える。	いただいた意見も参考にしつつ、要求事項・評価基準における該当箇所の修正を検討させていただきます。
284	要求事項・評価基準案	2-2-1		参考文献として、ISO27001の4.1組織及びその状況の理解,4.3ISMSの適用範囲の決定 が該当すると思います。		いただいた意見も参考にしつつ、要求事項・評価基準における該当箇所の修正を検討させていただきます。
285	要求事項・評価基準案	3-1-3		近年、業務におけるAI（生成AIを含む）の活用が急速に拡大しており、AIは新たなIT資産であると同時に、新たなサイバーリスク要因となり得ると考える。 本制度においても、自社でAIを活用している場合、その利用形態や管理状況によっては、情報漏えい、不正利用、誤動作等のサイバーリスク被害を受ける可能性があるため、AI活用についても評価対象に含まれる旨を明確に言及すべきではないか。	制度の目的である「サプライチェーン全体のセキュリティ水準向上」を実現するためには、AIを例外的な存在として扱うのではなく、クラウドサービスや業務システムと同様に、評価・管理の対象として整理することが重要であると考える。	いただいた意見については、今後の検討の参考とさせていただきます。
286	要求事項・評価基準案	4-1-1		ユーザIDの定期的な棚卸を行うべきではないでしょうか。		ユーザIDについては、No.4-1-1-3に基づき、定期的に棚卸されることを想定しています。

No.	該当箇所			寄せられた御意見の概要	理由	提出意見に対する考え方
	該当文書	該当ページ又は項番	該当項目			
287	要求事項・評価基準案	4-1-1		・ハードウェア、OS及びソフトウェアの安全な構成を →ハードウェア、OS、ファームウェア、デバイスドライバ及びソフトウェアの安全な構成 ・ハードウェア、OS、ファームウェア、デバイスドライバ及びソフトウェアの安全な構成を確立し、維持すること。を →ハードウェア、OS、ファームウェア、デバイスドライバ及びソフトウェアの安全な構成を確立し、維持すること。 にした方が良いと思います。 また、参照文献は以下を追加したほうが良いと思います。 NIST SP 800-147 整合（BIOS 保護） NIST SP 800-193 整合（ファームウェアレジリエンス）		いただいた意見については、今後の検討の参考とさせていただきます。
288	要求事項・評価基準案	4-1-2		管理者IDの定期的な棚卸を行うべきではないでしょうか。		管理者IDについては、No.4-1-2-6に基づき、定期的に棚卸されることを想定しています。
289	要求事項・評価基準案	4-1-3		評価基準 4-1-3-2 および 4-1-3-5 において、多要素認証の実装が求められている点については、なりすまし対策の観点から妥当であり、本制度の趣旨にも合致していると考える。 一方で、他の評価基準では「当該対策を実施できない場合の代替対策」が明示されているのに対し、多要素認証に関しては代替対策の記載がない点について、実務上の課題があると考える。	多要素認証は有効な対策である一方、実装可否がシステムごとに異なるため、「代替対策を一切認めない場合、制度活用が進まない」「形式的な適合を目的とした無理な構成変更が発生する」といった懸念がある。 代替対策の考え方を明示することで、「実務に即した評価」「制度の柔軟性と実効性の両立」が図られると考える。	本制度は大企業から中小企業まで一律で満たすべきベースラインを定めているところ、要求事項が求めるセキュリティ水準を多くの者が達成できるよう、実証事業での結果を取り得る手段の多様性に配慮して適宜代替策を追加の上、要求事項・評価基準(案)を作成したところです。制度構築方針(案)P.17記載のとおり、今後ガイダンス資料を整備する予定であり、当該資料において実装例等の拡充を図ってまいります。
290	要求事項・評価基準案	4-1-3		評価基準 No.4-1-3-2 において、「常に多要素認証を使用すること」と記載されているが、実際のクラウドサービスや認証基盤の運用においては、SSO（シングルサインオン）を含む多要素認証の実装方式により、認証タイミングやセッション管理の考え方が異なる場合がある。 そのため、「常に」という表現について、多要素認証を前提としつつも、実装上の一般的な運用（初回認証時のMFA、セッション有効期間内での再認証省略等）を考慮した補足説明又は注釈を追加することを検討してはどうか。 具体的な注釈案は以下である。 ※本項における「常に多要素認証を使用すること」とは、認証時に多要素認証を必須とすることを指し、適切に管理されたセッション有効期間内における再認証の省略を否定するものではない。	多要素認証の実装手段として、SSO や IdP（認証基盤）を活用する方式は、ユーザ・管理者双方の利便性とセキュリティを両立できる有効な手段として広く採用されている。 一方で、SSO を含む多くの多要素認証方式では、初回アクセス時に多要素認証を実施した後、一定のセッション有効期間内においては再認証を省略する運用が一般的であり、「すべてのアクセス操作ごとに多要素認証を要求する」運用を意味するものではない。 評価基準における「常に」という表現が、アクセスの都度、多要素認証を実施することを求めていると解釈された場合、現実的なシステム運用や、SSO 等の標準的なセキュリティ実装との乖離が生じるおそれがある。 そのため、多要素認証を必須とする趣旨を維持しつつ、実装上許容される一般的な運用形態を明確化することで、評価基準の解釈の統一および実務への適合性が高まると考える。	制度構築方針(案)P.17記載のとおり、今後要求事項・評価基準に係る評価方法や取組み事例等を具体的に解説する各種ガイダンス資料等を整備する予定です。いただいた意見については、当該ガイダンス資料等の作成に当たっての参考とさせていただきます。
291	要求事項・評価基準案	4-1-5		NISTの最近のガイドでは、長さ15文字以上となっていましたので、そうされることを検討いただきたいです。		いただいた意見については、今後の検討の参考とさせていただきます。
292	要求事項・評価基準案	4-1-9		参考文献として、ISO27001のA.7.9構外にある資産のセキュリティも該当すると思います。		いただいた意見も参考にしつつ、要求事項・評価基準における該当箇所の修正を検討させていただきます。
293	要求事項・評価基準案	4-2-1		セキュリティの意識向上とセキュリティ教育ですので、意識向上・教育が適当だと思います。		いただいた意見も参考にしつつ、要求事項・評価基準における該当箇所の修正を検討させていただきます。
294	要求事項・評価基準案	4-2-1		インシデントにつながる事象を早期に発見するために、ISO27001のA.6.8情報セキュリティ事象の報告を評価基準に追加するべきであると思います。		いただいた意見については、今後の検討の参考とさせていただきます。
295	要求事項・評価基準案	4-2-1		4-2-1-4と4-2-1-6は、★４とされていますが基本的な対策ですので、★３でも評価を求めるべきではないでしょうか。		各要求事項・評価基準については、自工会・部工会サイバーセキュリティガイドライン等の参照文献との整合に配慮し、★3・★4の区分を検討しています。
296	要求事項・評価基準案	4-2-2		評価基準の分離 「教育」と「訓練」を同一項目で評価するのではなく、それぞれの評価基準を独立した項目として分離することを提案します。	評価性質の相違「教育」は知識の習得（インプット）、「訓練」は行動の検証（アウトプット）であり、評価すべき指標が異なります。	他の参照文献との整合等に考慮し、要求事項No.4-2-2についてはセキュリティに係る教育・訓練を規定しています。
297	要求事項・評価基準案	4-3-4		要求事項の記述を「データの暗号化」から「データの保護（暗号化または秘密分散）」へと改め、技術的な選択肢を広げるべきである。具体的修正案：「情報機器及び情報システムの保管データを適切に暗号化または秘密分散技術を用いて保護するようルールを定め…」		いただいた意見については、今後の検討の参考とさせていただきます。
298	要求事項・評価基準案	4-4-3		「リモートアクセスのログ」「エンドポイント（パソコン、サーバー）の操作ログ」を明示的に評価対象として追加することを提案したい。	これらのログは、インシデント対応時の調査や原因分析において極めて重要であり、ログ取得の有無が被害拡大防止および再発防止策の質に大きく影響するため。	いただいた意見については、今後の検討の参考とさせていただきます。
299	要求事項・評価基準案	4-5-1		参考文献として、ISO27001のA.8.20ネットワークセキュリティも該当すると思います。		いただいた意見も参考にしつつ、要求事項・評価基準における該当箇所の修正を検討させていただきます。
300	要求事項・評価基準案	4-5-1		ネットワーク境界防御に関する記述について、一般にゼロトラスト環境を導入している方がよりセキュリティ強度が高いと考えるが、この点について加点的要素は無いのか。あるいは評価機関によるヒアリング時に、この点を踏まえて説明を行うことで他対策の不足分をカバーすることが可能となるのか。保有するセキュリティリスク強度を推し量るうえで、多層・複合的な対策を持ってリスク低減を判断することが一般的と考えるため、この点についてどのように取り扱えばよいか。		今回の要求事項・評価基準では、取得希望組織が一律で満たすべきベースラインとしての基準であることを考慮し、要求事項・評価基準の全件を達成することを合格基準としています、要求事項・評価基準の達成に当たっては、加点要素を設けることは想定していません。
301	要求事項・評価基準案	5-1-1		【別添】 ★３・★４要求事項・評価基準（案） の記載のうち、5 攻撃等 の検知 5-1 継続的監視 5-1-1 ネットワーク接続・データの監視 の評価基準として挙げられている5-1-1-1～5-1-1-3の各項目が、これらだけ他の項目よりも遥かに解像度が高く、明らかにIDS/IPSあるいはNDRを導入しないと実現できるとは思えない内容となっている。本当にこれは中小企業が満たさなければいけない要件なのか、再考を望むものである。		サイバーセキュリティお助け隊サービスなど、中小企業であっても一定価格でIPS/IDS機能を有する機器等の提供を受けられる環境が整備されていることも踏まえ、No.5-1-1-1では不正アクセスをリアルタイム検知・遮断する仕組みの導入を求めています。
302	要求事項・評価基準案	7-1		インシデントからの復旧（インシデント復旧計画の実行）に関する評価基準において、対応手順や体制の整備に加え、万が一の事態において計画を実行可能とするための【リソース確保（予算面を含む）】という観点を追加することを検討してはどうか。	インシデント発生時には、初動対応や復旧対応を迅速に実施できるかどうかが、被害の拡大防止および事業継続に大きく影響する。 その際、フォレンジック調査を含む専門的な対応や、外部専門家への依頼、システム復旧等により、短期間で追加的な費用が発生するケースが多い。 一方で、特に中小企業においては、あらかじめ対応予算が確保されていないことを理由に、本来実施すべきフォレンジック調査や十分な原因分析を行わず、暫定的な復旧のみに留まってしまう事例が実務上見受けられる。 このような場合、「インシデントの根本原因が特定されない」「再発防止策が十分に講じられない」といった課題が生じ、結果として同種インシデントの再発や被害の長期化につながるおそれがある。 そのため、インシデント復旧計画の実行性を担保する観点から、対応手順や体制の整備に加え、万が一の事態において計画を実行可能とするためのリソース確保（予算面を含む）についても評価対象として整理することが、制度の実効性向上に資すると考える。	いただいた意見については、今後の検討の参考とさせていただきます。
303	要求事項・評価基準案	1-1-1-1		セキュリティに関連する適用法令や業界基準のリストアップの網羅性が不明である 特に関係者からの要求事項に関する関係者の具体性も不明である。	定義が曖昧で運用差・監査不適合の恐れがある（明確化の必要がある）	いただいた意見も参考にしつつ、要求事項・評価基準の該当箇所について修正を検討させていただきます。 また、いただいた意見については、ガイダンス資料の作成等に当たっての参考とさせていただきます。
304	要求事項・評価基準案	1-1-1-1		取引先が提示する制限事項も含めた,関係者からの要求事項 社内ルールにおいて、特定の取引先が提示する事項を都度取り入れることは現実的ではない。また、この文中の関係者とは何か明らかにしていただきたい。		本要求事項における「社内ルール」とは、セキュリティ対応方針(セキュリティポリシー)を除く、本要求事項・評価基準で策定を求めるセキュリティ対策基準、運用手順その他のセキュリティ関連規程を指します。 取引先が提示する制限事項や要求事項については、都度、組織全体の規程類に反映することを求めるものではなく、必要に応じて、当該取引に係る運用ルール等に適切に反映することを想定しております。 また、「関係者」とは、主として当該取引先を指しますが、いただいた御意見も踏まえ、要求事項・評価基準における当該箇所の修正を検討させていただきます
305	要求事項・評価基準案	1-1-1-2		社内ルールの見直し頻度が『年1回以上』の「以上」と曖昧な要素となっているので、どのようなタイミングで必要なのかを言及する要素が不足している。	定義が曖昧で運用差・監査不適合の恐れがある（明確化の必要がある）	今回の要求事項・評価基準では、取得希望組織が一律で満たすべきベースラインとしての基準であることを考慮し、最低限年1回、見直しを行うこととしています。各取得希望組織の任意の取り組みとして、それ以上の頻度等で見直しを行うことは否定されるものではありません。
306	要求事項・評価基準案	1-1-1-3		社内ルールの周知にとどまらず、該当者への理解の確認要件が不明である どのようなタイミングで必要なのかを言及する要素が不足している。	定義が曖昧で運用差・監査不適合の恐れがある（明確化の必要がある）	本制度の要求事項・評価基準においては、評価工数を考慮し、従業員等における社内ルールの理解度の確認までは、必ずしも求めてはおりません。
307	要求事項・評価基準案	1-2-1-1		セキュリティ統括役員や担当部署の役割・責任範囲の定義が不明それに境界や権限委任の明確化の必要がある。	定義が曖昧で運用差・監査不適合の恐れがある（明確化の必要がある）	制度構築方針(案)P.17記載のとおり、今後要求事項・評価基準に係る評価方法や取組み事例等を具体的に解説する各種ガイダンス資料等を整備する予定です。いただいた意見については、当該ガイダンス資料等の作成に当たっての参考とさせていただきます。
308	要求事項・評価基準案	1-2-1-1 等		セキュリティを統括するのは役員でないと不可でしょうか？責任者を定められていれば、役員でなくも任命可能ですか？		具体的な要件については今後検討する予定ですが、セキュリティに対する経営層の関与という観点から、ここでは役員であることが望ましいと考えられます。
309	要求事項・評価基準案	1-2-1-2		平時連絡先リストの鮮度管理の規定が弱く、連絡不能リスクが残存する可能性がある。	制度文言の実務適合性・明確性の向上が必要である	今回の要求事項・評価基準では、取得希望組織が一律で満たすべきベースラインとしての基準であることを考慮し、最低限年1回、点検を行うこととしています。各取得希望組織の任意の取り組みとして、それ以上の頻度等で点検を行うことは否定されるものではありません。

No.	該当箇所			寄せられた御意見の概要	理由	提出意見に対する考え方
	該当文書	該当ページ又は項番	該当項目			
310	要求事項・評価基準案	1-2-1-3		平時体制の点検が『年1回以上』の「以上」と曖昧な要素となっているので、どのようなタイミングで必要なのかを言及する要素が不足している組織再編や人事異動への追随が遅れる恐れがある。	定義が曖昧で運用差・監査不適合の恐れがある（明確化の必要がある）	今回の要求事項・評価基準では、取得希望組織が一律で満たすべきベースラインとしての基準であることを考慮し、最低限年1回、点検を行うこととしています。各取得希望組織の任意の取り組みとして、それ以上の頻度等で点検を行うことは否定されるものではありません。
311	要求事項・評価基準案	1-2-1-3		年1回以上の頻度でNo.1-2-1-1及びNo.1-2-1-2にて定めた平時の体制について点検すること。 点検とは何か。最新化することか。		一覧等について棚卸を行い、適宜アップデートすることを想定しています。 例えば、1-2-1-3では、整備しているセキュリティ推進体制や連絡先について、人事異動や組織改編などにより修正する必要がないかどうかを確認し、必要に応じて最新のものにアップデートすることが想定されます。
312	要求事項・評価基準案	1-2-1-3		・セキュリティリスクは、経営に重大な影響を及ぼすことを理解し、その対応について情報セキュリティ委員会等の経営判断ができる体制を設置すること。 経営に重大な影響を及ぼすことを理解し、とは誰が理解するのか。理解の定義は何か。 対応は委員会で合議でよいのか。セキュリティーリスクの粒度は3-2-1にあるような詳細リスク分析に基づく技術的対応方針を、委員会のような上位組織で定めるべきものなのか。それは経営判断ではなく対応判断であり委員会のするべき仕事ではないのではないか。		評価基準No.1-2-1-3では、自社のセキュリティリスクについて、経営的に判断できる体制(例:情報セキュリティ委員会)が整備されていることを求めるという趣旨であり、詳細な体制や意思決定方法などについては、各取得希望組織の実情に応じて定めることを想定しています。 なお、当該評価基準については、いただいた意見も参考に修正を検討させていただきます。
313	要求事項・評価基準案	1-2-1-4		経営判断体制の設置と記載されているが、委員会体制人数や運営(開催頻度/KPI/議事録保管など）の具体的な要素が不明である。	定義が曖昧で運用差・監査不適合の恐れがある（明確化の必要がある）	今回の要求事項・評価基準では、取得希望組織が一律で満たすべきベースラインとしての基準であることを考慮し、情報セキュリティ委員会の設置を求めたうえで、運営体制等については、各取得希望組織で決定することを想定しています。
314	要求事項・評価基準案	1-2-2-1		非公開情報の入手は、弊社のような一般企業は困難だと思いますが、その入手ができなくても、本制度には適合するのでしょうか？		非公開情報が入手できない場合でも、公開情報が活用できる体制が整備されていれば本評価基準は適合となる想定です。
315	要求事項・評価基準案	1-2-2-1		公開/非公開の脅威・脆弱性情報の活用体制を整備とあるが、当該項目をクリアOKとなる具体的な方法が不明である。	定義が曖昧で運用差・監査不適合の恐れがある（明確化の必要がある）	制度構築方針(案)P.17記載のとおり、今後要求事項・評価基準に係る評価方法や取組み事例等を具体的に解説する各種ガイダンス資料等を整備する予定です。いただいた意見については、当該ガイダンス資料等の作成に当たっての参考とさせていただきます。
316	要求事項・評価基準案	1-2-2-1		・サイバー攻撃及び脆弱性に関する公開情報・非公開情報を活用する体制を整備すること。 非公開情報とは何か。非公開の情報をどのように取得するのかご教示いただきたい。		ISAC等の限られた範囲内で公開される脆弱性に関する情報を指します。 なお、非公開情報を入手できない環境であっても、直ちにNo.1-2-2-1が不適合となるものではありません。
317	要求事項・評価基準案	1-2-2-2		なにをもって相関分析を具現化し、どのような検知KPIなどの運営指針が示されていない。	可観測性・検知能力の強化が必要である（監視/相関分析の充実）	制度構築方針(案)P.17記載のとおり、今後要求事項・評価基準に係る評価方法や取組み事例等を具体的に解説する各種ガイダンス資料等を整備する予定です。いただいた意見については、当該ガイダンス資料等の作成に当たっての参考とさせていただきます。
318	要求事項・評価基準案	1-2-3-1		守秘義務ルールはあるが、委託/派遣等の外部要員までの適用境界が不明確である。	定義が曖昧で運用差・監査不適合の恐れがある（明確化の必要がある）	ここでいう守秘義務のルールについては、外部要員も含め、自社の守るべき情報資産にアクセスする全ての要員に適用されることを想定しています。
319	要求事項・評価基準案	1-2-3-2		入社・受入時教育の内容・評価方法の具体化がされておらず、不明確である。	定義が曖昧で運用差・監査不適合の恐れがある（明確化の必要がある）	制度構築方針(案)P.17記載のとおり、今後要求事項・評価基準に係る評価方法や取組み事例等を具体的に解説する各種ガイダンス資料等を整備する予定です。いただいた意見については、当該ガイダンス資料等の作成に当たっての参考とさせていただきます。
320	要求事項・評価基準案	1-2-3-3-		守秘義務の誓約書を提出は、法的根拠がないと理解しているが、国の指針で強制するのか確認したい。		守秘義務の誓約書については、企業と従業員等との関係の中で提出することを想定しています。
321	要求事項・評価基準案	1-2-3-3 1-2-3-4		誓約書提出は従業員のみ対象で、外部要員の取扱いが別建となっており、運用上の齟齬が生じる可能性がある(外部要員は、要員元の会社と守秘義務締結とあり、会社単位だと要員個人にいきわたらない可能性がある)。	制度文言の実務適合性・明確性の向上が必要である	派遣社員や受入出向者については、派遣元企業等との契約の範囲内において、守秘義務について必要な対応を行うことが想定されます。
322	要求事項・評価基準案	1-3-1-1		セキュリティ対応方針とは何を指しているのか明文化してほしい。		一般的には、トップマネジメントによって正式に表明された組織のセキュリティに係る意図や方向付け及び、そのような意図や方向付け基づいてセキュリティ対策を行うために組織が定めた規定が該当します。 いただいた意見については、要求事項・評価基準の開設のためのガイダンス資料作成等に当たって参考とさせていただきます。
323	要求事項・評価基準案	1-3-1-2		セキュリティ対応方針の参照容易性は示されるが、単一の『最新版』を確認する事項が不足する可能性がある。	定義が曖昧で運用差・監査不適合の恐れがある（明確化の必要がある）	いただいた意見も参考にしつつ、要求事項・評価基準における該当箇所の修正を検討させていただきます。
324	要求事項・評価基準案	1-3-1-3		方針改正時の周知に関する各要員が認識をできたことの確認方法が不足する可能性がある。	定義が曖昧で運用差・監査不適合の恐れがある（明確化の必要がある）	本制度の要求事項・評価基準においては、評価工数等を考慮し、従業員等へのセキュリティ対応方針の周知状況の確認までは、必ずしも求めてはおりません。
325	要求事項・評価基準案	1-3-1-4		1-1-1-2の社内ルールの点検と、1-3-1-4のセキュリティ対応方針の点検は、内容的に重複していないでしょうか？ なお、対応方針 （ポリシー）の方が社内ルールよりも上位に位置づけられるとの認識です。		いただいた意見も参考にしつつ、要求事項・評価基準における該当箇所の修正を検討させていただきます。
326	要求事項・評価基準案	1-4-1-1		1-3-1-3でなく1-3-1-4ではないか。		いただいた意見も参考にしつつ、要求事項・評価基準における該当箇所の修正を検討させていただきます。
327	要求事項・評価基準案	1-4-1-1		セキュリティ対策推進計画の報告項目に、KPI/予算/リスク優先度の定義が不足している。	制度文言の実務適合性・明確性の向上が必要である	いただいた意見については、今後の検討の参考とさせていただきます。
328	要求事項・評価基準案	1-4-1-1		役員指示の記録・是正に関するとセキュリティ担当部署のプロセス（証跡/共有期限/是正）の定義が不明である。	定義が曖昧で運用差・監査不適合の恐れがある（明確化の必要がある）	制度構築方針(案)P.17記載のとおり、今後要求事項・評価基準に係る評価方法や取組み事例等を具体的に解説する各種ガイダンス資料等を整備する予定です。いただいた意見については、当該ガイダンス資料等の作成に当たっての参考とさせていただきます。
329	要求事項・評価基準案	1-4-1-1		セキュリティを統括する役員や関係部門に対して今後の対策推進計画を報告する旨の記載がありますが、ガバナンス面を強調する上では、報告し「承認を得る」ことを明記すべきではないでしょうか。		いただいた意見も参考にしつつ、要求事項・評価基準における該当箇所の修正を検討させていただきます。
330	要求事項・評価基準案	1-4-1-2		外部管理システムの把握範囲（顧客/子会社/クラウド等）の網羅性と更新頻度が不明確のため、第三者接続台帳を作成し、所有者/接続方式/データ種別/責任分担を定義し半期棚卸が必要である。	定義が曖昧で運用差・監査不適合の恐れがある（明確化の必要がある）	自社の資産が接続しているシステムに係る情報の点検の頻度については、NO.2-1-1-2のとおり、最低限年１回以上としています。 また、最低限自社の資産が接続しているシステムについて把握することとしていますが、各取得希望組織の任意の取り組みとして、それ以外の情報について把握することは否定されるものではありません。
331	要求事項・評価基準案	1-4-1-2		1-4-1-1で、対策推進計画を「セキュリティを統括する役員(例えば、CISOを設置する会社の場合は、当該CISO)及び関係部門に対して」報告するとありますが、ガバナンス面を強調する上では、「関係部門」はあえて記述しなくともよいのではないでしょうか。 1-4-1-2の「役員からの改善に向けた指示があった場合」という記述とも整合をとるべきと考えます。		いただいた意見も参考にしつつ、要求事項・評価基準における該当箇所の修正を検討させていただきます。
332	制度構築方針(案)	2.2.2		【意見内容】 「企業は個社/(国内又は海外を含む)企業グループ/事業部等と★の取得範囲を柔軟に定めることができる。」とのことですが、多数の事業を手掛ける個社において、全体は★4を取得、一部の部門だけ★3を取得というレベルを分けた取得は、「適用範囲の考え方」に従って分離さえ行えば可能なのでしょうか。取得パターンの例示資料を作成する予定はあるでしょうか。		適用範囲を決定するに当たっては、制度構築方針P.9記載の考え方に基づき、適用範囲内外の通信の制御等を行うことが前提となります。 そのうえで、制度構築方針P.12のとおり、セキュリティ専門家(★3)又は評価機関(★4)による適用範囲の妥当性の確認を経たうえで、事業部単位を申請主体とすることも想定しています。
333	要求事項・評価基準案	2-1-1-1		・自社以外の組織(顧客・子会社・関係会社・クラウドサービス提供者を含む取引先)が管理・提供し、自社の資産が接続しているシステムを把握するための仕組みを整備すること。 自社の資産が接続するという具体的な内容は何か。端末がブラウザでサイトを閲覧しているだけでも、自社の資産(端末)が接続していると解釈される。		ここでは、自社の情報資産(データ)が当該システムで管理・運用されているかどうかを基に自社の資産が接続しているシステムについて判断することが想定され、単なるサイト閲覧等は含まれません。
334	要求事項・評価基準案	2-1-1-2		把握した内容の点検ではなく、把握すべき内容（項目）の点検で間違いないか。		ここでは、No.2-1-1-1の仕組みにより「把握している」情報について、更新漏れがないか等の点検や棚卸を行うことを想定しています。
335	要求事項・評価基準案	2-1-1-2		・年1回以上の頻度でNo.2-1-1-1において把握すべき情報の内容を点検すること。 把握したの誤記か？		いただいた意見も参考にしつつ、要求事項・評価基準における該当箇所の修正を検討させていただきます。
336	要求事項・評価基準案	2-1-1-3		会社ごとに取り交わす情報と、取引に伴い授受・使用される情報資産は同一のものか、異なるものか。異なるものの場合、差異につきご教示いただきたい。		両者は同一のものと考えています。なお、いただいた意見も参考にしつつ、要求事項・評価基準における該当箇所の修正を検討させていただきます。
337	要求事項・評価基準案	2-1-2-1		機密情報の取り扱いに関する取り交わす調整期間が不明確である。	定義が曖昧で運用差・監査不適合の恐れがある（明確化の必要がある）	制度構築方針(案)P.17記載のとおり、今後要求事項・評価基準に係る評価方法や取組み事例等を具体的に解説する各種ガイダンス資料等を整備する予定です。いただいた意見については、当該ガイダンス資料等の作成に当たっての参考とさせていただきます。
338	要求事項・評価基準案	2-1-3-1		重要取引先のセキュリティ対策を把握することでの取引先選定基準、対策未達成の場合の対応が不明である。	定義が曖昧で運用差・監査不適合の恐れがある（明確化の必要がある）	制度構築方針(案)P.17記載のとおり、今後要求事項・評価基準に係る評価方法や取組み事例等を具体的に解説する各種ガイダンス資料等を整備する予定です。いただいた意見については、当該ガイダンス資料等の作成に当たっての参考とさせていただきます。
339	要求事項・評価基準案	2-1-3-1		セキュリティ対策チェックシートの内容が不明であるため、チェックシートの内容を定義する必要がある。	定義が曖昧で運用差・監査不適合の恐れがある（明確化の必要がある）	制度構築方針(案)P.17記載のとおり、今後要求事項・評価基準に係る評価方法や取組み事例等を具体的に解説する各種ガイダンス資料等を整備する予定です。いただいた意見については、当該ガイダンス資料等の作成に当たっての参考とさせていただきます。
340	要求事項・評価基準案	2-1-4-1		インシデント時の役割・責任は定義されるが、連絡方法や再発防止協議のプロセスが不明である。	定義が曖昧で運用差・監査不適合の恐れがある（明確化の必要がある）	契約等の取り決めにより、それぞれ必要に応じた内容が定められることを想定しています。
341	要求事項・評価基準案	2-1-4-1		2-1-4-1では、「機密情報を共有する子会社又は取引先」としており、機密情報については「自社の」をあえて省いているのか、関係会社クラウドサービス提供者も省いているのか		いただいた意見も参考にしつつ、要求事項・評価基準における該当箇所の修正を検討させていただきます。
342	要求事項・評価基準案	2-1-4-1		再発防止策の協議方法とは何か、ご教示いただきたい。		再発防止策の策定・報告義務などを指し、契約等の取り決めにより定めることを想定しています。 なお、いただいた意見も参考に、要求事項・評価基準における該当箇所について修正を検討させていただきます。

No.	該当箇所			寄せられた御意見の概要	理由	提出意見に対する考え方
	該当文書	該当ページ又は項番	該当項目			
343	要求事項・評価基準案	2-1-4-1等		インシデント発生時の再発防止策の協議方法は事前に決定しなければならないでしょうか？実際の現場では、再発防止を委託先の契約解除とすることもあるため、違和感があります。再発防止を検討することを重視するのであれば、インシデント対応プロセスの中で再発防止の検討が組み込まれていること、という要件の方が適しているかと考えます。また、再発防止の協議方法は事前に決めた連絡手段（メールやチャットツール）のやり取りの中で行う、というのが通例かと思います。		いただいた意見も参考に、要求事項・評価基準の修正を検討させていただきます。
344	要求事項・評価基準案	2-1-5-1		契約終了時の機密/アクセス権の回収手順はあるが、検証方法・証跡保管の具体化が不十分である。	定義が曖昧で運用差・監査不適合の恐れがある（明確化の必要がある）	制度構築方針(案)P.17記載のとおり、今後要求事項・評価基準に係る評価方法や取組み事例等を具体的に解説する各種ガイダンス資料等を整備する予定です。いただいた意見については、当該ガイダンス資料等の作成に当たっての参考とさせていただきます。
345	要求事項・評価基準案	2-1-5-1		2-1-5-1では、「自社の機密情報を提供・共有する子会社又は取引先」としているが、関係会社クラウドサービス提供者は意図して省いているのか		ここでは、クラウドサービス事業者等まで対象とすることは想定していません。
346	要求事項・評価基準案	2-1-5-1		アクセス権は初出だが、何を指しているのか。機密情報と同様の扱いであれば、その他の機密情報と同様に管理も項目に加えるべきではないか。		ここでは、重要な機密情報を提供等するために子会社又は取引先の従業員等に付与したアクセス権限を指します。
347	要求事項・評価基準案	3-1-1-1		適用範囲内とは何か、ご教示いただきたい。		★を取得する際の適用範囲のことを指し、制度構築方針(案)P.9における適用範囲と同義です。
348	要求事項・評価基準案	3-1-1-1		3-1-1の『要求事項』に「ハードウェア、OS及びソフトウェアの把握」と書いてあるのに、『評価基準』にパソコンおよびシンクライアントは製造元とOSだけ把握していれば良いのか？という意見です。 また、デバイスドライバー、ファームウェアの脆弱性を狙ったサイバー攻撃が顕在化しているため、 『要求事項』は「ハードウェア、OS及びソフトウェア、の把握」を →「ハードウェア、ファームウェア、デバイスドライバ、OS及びソフトウェア、の把握」にした方が良いと思います。 3-1-1-1の『適用範囲』パソコン及びシンクライアントの製造元、OS及び台数を把握するための仕組みを整備すること。」も →パソコン及びシンクライアントの製造元、ファームウェア、デバイスドライバ、 OS、ソフトウェア及び台数を把握するための仕組みを整備すること。にした方が良いと思います。		いただいた意見については、今後の検討の参考とさせていただきます。
349	要求事項・評価基準案	3-1-1-1 ～ 3-1-1-7		PC/VDI、サーバ、スマートデバイスの在庫把握は規定されるが、IT資産や構成要素の状態の正確性が不足している。	定義が曖昧で運用差・監査不適合の恐れがある（明確化の必要がある）	No.3-1-1-7(★4)において、PC/VDI、サーバ、スマートデバイス等の一覧等の情報について、年1回以上の頻度で点検することとしています。
350	要求事項・評価基準案	3-1-1-1 ～ 3-1-1-7		導入/設置/接続/パッチ適用のルールはあるが、違反時の是正フローが不明であるため、構成変更はCAB承認を必須化し、逸脱検知時の是正チケット起票を自動化する必要がある。	定義が曖昧で運用差・監査不適合の恐れがある（明確化の必要がある）	今回の要求事項・評価基準では、取得希望組織が一律で満たすべきベースラインとしての基準であることを考慮し、最低限、情報機器、OS及びソフトウェアについて、導入、設置、ネットワーク接続及びセキュリティパッチ適用のルールを含む管理ルールを定めることとしています。各取得希望組織の任意の取り組みとして、それ以外の管理ルールや承認フローを追加することは否定されるものではありません。
351	要求事項・評価基準案	3-1-1-4		3-1-1-3の管理ルールそのものの点検ではなく、遵守状況の点検で間違いないか。その場合は1-4-1-1の対象で間違いないか。他の項目は状況ではなく、ルールや項目の点検が目的と推察されるため確認したい。		御認識のとおり、ここでは、3-1-1-3で作成した管理ルールの遵守状況の点検を指し、また、1-4-1-1の対象となると想定しています。
352	要求事項・評価基準案	3-1-1-6		重要機器の設定情報把握はあるが、セキュアベースライン/変更履歴の管理の実施が不明である。	定義が曖昧で運用差・監査不適合の恐れがある（明確化の必要がある）	今回の要求事項・評価基準では、取得希望組織が一律で満たすべきベースラインとしての基準であることを考慮し、最低限、重要機器については設定情報を把握することとしています。各取得希望組織の任意の取り組みとして、それ以外の情報を把握の対象とすることは否定されるものではありません。
353	要求事項・評価基準案	3-1-1-6		設定情報を把握するための仕組みとは具体的に何をさすか、ご教示いただきたい。		一般的にはコンフィグ管理ツールや、コンフィグ情報の保存等により対応することが想定されます。
354	要求事項・評価基準案	3-1-1-7		『年1回以上』の点検は、定期を想定していると思われるが、変更都度の更新トリガーが不明である。	定義が曖昧で運用差・監査不適合の恐れがある（明確化の必要がある）	今回の要求事項・評価基準では、取得希望組織が一律で満たすべきベースラインとしての基準であることを考慮し、最低限年1回、点検を行うこととしています。各取得希望組織の任意の取り組みとして、それ以上の頻度等で点検を行うことは否定されるものではありません。
355	要求事項・評価基準案	3-1-2-1 ～ 3-1-2-2		ネットワーク関連の把握に所在地/目的の記載が求められているが、バージョン管理や管理責任者が不明であるため、ネットワーク図に版/更新日/作成者を記載し、リポジトリで承認済み最新版のみ参照できるようにする。	定義が曖昧で運用差・監査不適合の恐れがある（明確化の必要がある）	今回の要求事項・評価基準では、取得希望組織が一律で満たすべきベースラインとしての基準であることを考慮し、最低限、ネットワークの所在地及び目的を把握することとしています。各取得希望組織の任意の取り組みとして、それ以外の情報を把握の対象とすることは否定されるものではありません。
356	要求事項・評価基準案	3-1-3-1		セキュリティ要件とは何を指しているのか明文化いただきたい。		事業者がクラウドサービスを利用する際に考慮すべきものであり、サービス選定に係る要件、運用に係る要件、その他セキュリティ管理に係る要件等が含まれると想定しています。
357	要求事項・評価基準案	3-1-3-1		外部情報サービス利用ルールがあったとしても、自社の役員又は従業員が承認した証跡の扱いが不明である。	定義が曖昧で運用差・監査不適合の恐れがある（明確化の必要がある）	制度構築方針(案)P.17記載のとおり、今後要求事項・評価基準に係る評価方法や取組み事例等を具体的に解説する各種ガイダンス資料等を整備する予定です。いただいた意見については、当該ガイダンス資料等の作成に当たっての参考とさせていただきます。
358	要求事項・評価基準案	3-1-3-2		外部情報サービスの接続先とは何か、ご教示いただきたい。		クラウドサービスであればクラウドサービス事業者が該当します。
359	要求事項・評価基準案	3-1-3-2		機密情報の取扱いについて取り交わすとは、何を取り交わすのか、ご教示いただきたい。		機密保持契約や規約等により、保存する機密情報の取り扱いについて取り交わすことを想定しています。
360	要求事項・評価基準案	3-1-3-2		「外部情報サービスの接続先」について、文意からは「サービス提供事業者」を指すと思われますが、「外部情報サービスが通信する相手」とも読め、何を指すのかが分かりづらいです。		いただいた意見も参考にしつつ、要求事項・評価基準における該当箇所の修正を検討させていただきます。
361	要求事項・評価基準案	3-1-4-1		機密区分に応じた管理ルールとして、ラベル付けや自動DLPの実装などの要素もいれないのかが不明である。	定義が曖昧で運用差・監査不適合の恐れがある（明確化の必要がある）	今回の要求事項・評価基準では、取得希望組織が一律で満たすべきベースラインとしての基準であることを考慮し、最低限、機密区分に応じた管理ルールを定めることとしています。各取得希望組織の任意の取り組みとして、情報管理のための製品・ソリューション等を導入することは否定されるものではありません。
362	要求事項・評価基準案	3-1-4-3		高機密の台帳（管理者/保管場所/期限/開示先）の整備は記載されるが、更新周期、責任が不明である。	定義が曖昧で運用差・監査不適合の恐れがある（明確化の必要がある）	No.3-1-4-1(★4)において、高い機密区分の情報等の一覧等について、年1回以上の頻度で点検することとしています。
363	要求事項・評価基準案	3-1-4-4		脱字と思われます。 × 内容ついて ○ 内容について		いただいた意見も参考にしつつ、要求事項・評価基準における該当箇所の修正を検討させていただきます。
364	要求事項・評価基準案	3-1-4-5		退職/任期満了時の回収はあるが、ID無効化/物理回収の同期化が不明である。	定義が曖昧で運用差・監査不適合の恐れがある（明確化の必要がある）	いただいた意見については、今後の検討の参考とさせていただきます。
365	要求事項・評価基準案	3-1-4-6		3-1-4-6の管理ルールそのものの点検ではなく、遵守状況の点検で間違いないか。その場合は1-4-1-1の対象で間違いないか。他の項目は状況ではなく、ルールや項目の点検が目的と推察されるため確認したい。		御認識のとおり、ここでは、3-1-4-6で作成した管理ルールの遵守状況の点検を指し、また、1-4-1-1の対象となると想定しています。
366	要求事項・評価基準案	3-1-4-7 ～ 3-1-4-8		廃棄時の『復元不可』要件はあるが、具体的な検証方法（消去証跡）が不足している。	制度文言の実務適合性・明確性の向上が必要である	制度構築方針(案)P.17記載のとおり、今後要求事項・評価基準に係る評価方法や取組み事例等を具体的に解説する各種ガイダンス資料等を整備する予定です。いただいた意見については、当該ガイダンス資料等の作成に当たっての参考とさせていただきます。
367	要求事項・評価基準案	3-1-5-1		要求事項「3-1-5：リモートワークにおけるルール」は★4 のみに設定されている。一般的にリモートワークとはコロナ禍で広がった在宅勤務のみならず、出張先の業務、工事現場の一時的作業場での業務等、社外(主にインターネット接続環境)ネットワークに接続する環境下でエンドポイント機器を使用する業務全般を指すものと解される。したがって、リモートワークは、企業規模に関わらず、一般的に通常発生しうる業務(および業務環境)と考えられる。 しかしながら、本案の★3 にはリモートワークは要求事項/評価基準に含まれていない。 ★3 を取得した評価主体であっても、リモートワークで当然行うべきセキュリティ対策が行われるかは不明なままとなる。これは、サプライチェーンにおいて「★3 取得済みであれば最低限のセキュリティが担保されている」という過信を誘発する恐れがある。 具体例としては、★4 評価基準「4-5-1-8：ソフトウェアファイアウォールを有効化」と記載されている。一方、★3 においてエンドポイント機器のファイアウォールは評価対象外である。ファイアウォールは、エンドポイントにおける標準的なセキュリティ対策の 1 つである。それにも関わらず、★3 レベルの企業における「リモートワーク環境下のエンドポイント機器の保護」が不十分であっても制度上許容される。このような要求事項/評価基準の設計自体がセキュリティ上の脆弱性となることは容易に予見される。 「サプライチェーン強化に向けたセキュリティ対策評価制度に関する制度構築方針(案)」9ページの「適用範囲の考え方-適用範囲に含むもの-1.IT 基盤」に「エンドポイント機器」が明示された点は範囲の明確化として高く評価できる。 これは昨今のセキュリティ事案等の教訓からエンドポイント機器セキュリティの状況可視化と対策強化が急務であるという認識の下、明示されたものと推察される。しかしながら、制度側においてエンドポイント機器セキュリティの状況可視化と対策強化の必要性を認識しつつも★3 の要求事項/評価基準案において、リモートワークの対策を含めないという矛盾が生じる。これは「★３・★４要求事項及び評価基準案」に構造的問題が生じていると言わざるを得ない。 以上のことから、「★３・★４要求事項及び評価基準」を策定するに当たっては、「★3 における想定使用環境」の再検討、「エンドポイント機器」観点を明示的に要求事項および評価基準に含めることの 2 点を提案する。 なお、JIS Q 27001:2023 に準拠した情報セキュリティ管理基準（令和７年改正版）では「8.1 利用者エンドポイント機器」において当該事項が定められており、セキュリティ対策が重視されている状況である。但し、「エンドポイント機器」は CSF2.0 機能の「識別(ID)、防御(PR)、対応(RS)」等多岐にわたると認識、「8.1 利用者エンドポイント機器」のみに限らず広範な要求事項と評価基準が必要と考えられる点、留意が必要である。	制度側においてエンドポイント機器セキュリティの状況可視化と対策強化の必要性を認識しつつも★3 の要求事項/評価基準案においてリモートワークの対策を含めないという矛盾が生じている。「★３・★４要求事項及び評価基準案」に構造的問題が存在するため、意見する	各要求事項・評価基準については、自工会・部工会サイバーセキュリティガイドライン等の参照文献との整合に配慮し、★3・★4の区分を検討しています。
368	要求事項・評価基準案	3-1-5-1		3-1-5-1は1-1-1-1、1-1-1-3のように何故作成要件と周知要件が分かれていないのか。		いただいた意見も参考にしつつ、要求事項・評価基準における該当箇所の修正を検討させていただきます。
369	要求事項・評価基準案	3-1-5-1 ～ 3-1-5-2		リモートワーク端末/データのルールはあるが、BYOD可否、管理や許容データの詳細が不明である。	定義が曖昧で運用差・監査不適合の恐れがある（明確化の必要がある）	制度構築方針(案)P.17記載のとおり、今後要求事項・評価基準に係る評価方法や取組み事例等を具体的に解説する各種ガイダンス資料等を整備する予定です。いただいた意見については、当該ガイダンス資料等の作成に当たっての参考とさせていただきます。

No.	該当箇所			寄せられた御意見の概要	理由	提出意見に対する考え方
	該当文書	該当ページ又は項番	該当項目			
370	要求事項・評価基準案	3-2-1-1		脆弱性情報とは、組織内の情報を指すのか、公開されている情報を指すのか明記してほしい。		ここでいう脆弱性情報には、インターネット等において公表された、製品・ソフトウェア等の脆弱性に関する情報のほか、ISAC等の限られた範囲内で公開される脆弱性に関する情報が含まれます。
371	要求事項・評価基準案	3-2-1-1		脆弱性管理の役割・責任はあるが、SLA（評価/適用期限）や重大度基準の明確化が不足する可能性があるため、CVSS等の基準に応じたSLA（例：重大は7日以内）を定義し、進捗ダッシュボード化すべきである。	定義が曖昧で運用差・監査不適合の恐れがある（明確化の必要がある）	いただいた意見については、今後の検討の参考とさせていただきます。 なお、今回の要求事項・評価基準では、取得希望組織が一律で満たすべきベースラインとしての基準であることを考慮し、国内外の他の文献等を参照したうえで重大な脆弱性について14日以内に対応することとしています。
372	要求事項・評価基準案	3-2-1-2		情報源/ツール/頻度は規定されるが、クラウド/OT等の領域別の収集責任分担が不明であるため、領域別（IT/クラウド/OT）の情報収集責任者と週次レビュー会の設定が必要である。	定義が曖昧で運用差・監査不適合の恐れがある（明確化の必要がある）	いただいた意見については、今後の検討の参考とさせていただきます。
373	要求事項・評価基準案	3-2-1-3		対応要否判断基準・手順はあるが、例外承認や緊急適用のガイドラインが不明であるため、例外の承認権限と期限、緊急適用フロー（緊急CAB）を定義し、ガイドライン化すべきである。	定義が曖昧で運用差・監査不適合の恐れがある（明確化の必要がある）	いただいた意見については、ガイダンス資料の作成に当たっての参考とさせていただきます。
374	要求事項・評価基準案	3-2-1-4		残存脆弱性の把握仕組みはあるが、スキャン頻度や対象範囲の具体化が不足しているため、資産分類に応じて週次/月次スキャンを定義し、逸脱時アラートを設定するべきである。	定義が曖昧で運用差・監査不適合の恐れがある（明確化の必要がある）	いただいた意見については、今後の検討の参考とさせていただきます。 なお、No.4-4-5-2(★3)において、情報機器に応じたスキャン範囲及びスキャン頻度を定めることとしています。
375	要求事項・評価基準案	3-2-1-5		対応漏れがあった場合の措置について記載はしないのか。		No.3-2-1-3及びNo.4-4-4で示すルールに基づき、該当する脆弱性への対応を実施することを想定しています。
376	要求事項・評価基準案	3-2-1-5		対応履歴の月次点検はあるが、クリティカル対応の即時エスカレーションが不明で、クリティカルは即日/24hでエスカレーションし、是正完了までのフォローを自動化すべきである。	定義が曖昧で運用差・監査不適合の恐れがある（明確化の必要がある）	いただいた意見については、今後の検討の参考とさせていただきます。
377	要求事項・評価基準案	4-1-1-1		ユーザIDの申請・承認はあるが、JML連携や権限過多検知の仕組みが不足している。	定義が曖昧で運用差・監査不適合の恐れがある（明確化の必要がある）	いただいた意見については、今後の検討の参考とさせていただきます。
378	要求事項・評価基準案	4-1-1-1		自社の従業員、派遣社員及び受入出向者に 他の項目のように役員が含まれない理由があるかご教示いただきたい。		いただいた意見も参考にしつつ、要求事項・評価基準における該当箇所の修正を検討させていただきます。
379	要求事項・評価基準案	4-1-1-1		パソコン、サーバ及びスマートデバイスで利用を許可していないソフトウェアをすべて削除又は無効化とは、バンドルされている全てのソフトウェアに対して確認を実施することを求めているか。OS等のアップデートが発生した際には、全て見直すことを求めているか。		いただいた意見も参考にしつつ、要求事項・評価基準における該当箇所の修正を検討させていただきます。
380	要求事項・評価基準案	4-1-1-2		共有IDの例外運用時、利用者特定方法の具体化が不足（PAM/セッション記録等）している。	定義が曖昧で運用差・監査不適合の恐れがある（明確化の必要がある）	制度構築方針(案)P.17記載のとおり、今後要求事項・評価基準に係る評価方法や取組み事例等を具体的に解説する各種ガイダンス資料等を整備する予定です。いただいた意見については、当該ガイダンス資料等の作成に当たっての参考とさせていただきます。
381	要求事項・評価基準案	4-1-1-2		やむを得ず管理者IDの共有が必要な場合(例えば、システムの仕様により、使用人数分のIDを発行することができない場合)は、共有の管理者IDを利用したユーザを特定できるようにするのは、誰が担保することを想定しているか (※社内のシステム、外部に使わせるシステム、様々な利用が想定される)		適用範囲として定めた全てのシステムを対象としています。
382	要求事項・評価基準案	4-1-1-4		「特別なアクセス権限」が何を指すのかが分かりづらいです。例（スタッフの役割が変わった場合）を見る限りでは「付与したアクセス権限」程度の意味のように思えますが、特権や管理者権限と誤解される可能性があります。		制度構築方針(案)P.17記載のとおり、今後要求事項・評価基準に係る評価方法や取組み事例等を具体的に解説する各種ガイダンス資料等を整備する予定です。いただいた意見については、当該ガイダンス資料等の作成に当たっての参考とさせていただきます。
383	要求事項・評価基準案	4-1-2-4		開発要員が運用業務を兼務している場合、これらの要件を満たすことができないため、「必要な場合を除いて」や、「承認・認証を必要とすること」など制限をつけたうえで管理者権限操作ができることを検討いただきたい。		ここでは、システム開発を実施する役員、従業員、派遣社員及び受入出向者が本番環境において、開発環境における管理者権限で操作できないようにすることを求めています。 いただいた意見も参考にしつつ、要求事項・評価基準における該当箇所の修正を検討させていただきます。
384	要求事項・評価基準案	4-1-2-4		開発者の本番操作禁止はあるが、緊急時のブレークグラス手順が不明である。	定義が曖昧で運用差・監査不適合の恐れがある（明確化の必要がある）	各取得希望組織において、緊急時における管理者権限の使用手順等を定めることは否定されるものではありません。
385	要求事項・評価基準案	4-1-2-4		システム開発を実施する役員、従業員、派遣社員及び受入出向者が本番環境において、管理者権限で操作できないようにすることとは、何を具体的に求めているのか。		システム開発環境における管理者権限を、本番環境で操作できないようにすることを想定しています。 なお、いただいた意見も参考にしつつ、要求事項・評価基準における該当箇所の修正を検討させていただきます。
386	要求事項・評価基準案	4-1-2-4		「・システム開発を実施する役員、従業員、派遣社員及び受入出向者が本番環境において、管理者権限で操作できないようにすること。」とありますが、意味が分かりづらいです。 開発担当者と運用担当者を分け、本番環境では運用担当者のみが管理者権限で操作する、ということでしょうか。		システム開発環境における管理者権限を、本番環境で操作できないようにすることを想定しています。 なお、いただいた意見も参考にしつつ、要求事項・評価基準における該当箇所の修正を検討させていただきます。
387	要求事項・評価基準案	4-1-2-5		仕組みとは、運用ルールやドキュメントによる方法も含まれ、システムによる管理手法に限定されないか。		御認識のとおりです。
388	要求事項・評価基準案	4-1-2-6		未使用IDの無効化の『速やかに』の定義が不明である。	定義が曖昧で運用差・監査不適合の恐れがある（明確化の必要がある）	未使用IDのリスク等を考慮し、各取得希望組織にて無効化タイミングを判断することを想定しています。
389	要求事項・評価基準案	4-1-2-6		管理者IDが不要になった場合(例えば、管理者が組織を退職した場合及びIDが一定期間使用されなかった場合)、速やかに管理者IDを削除又は無効化することは、管理者IDを共有する(例えばネットワーク機器)場合は不可能であるがどうするか、ご教示いただきたい。		管理者IDを引き続き使用する場合は、削除又は無効化する必要はありません。
390	要求事項・評価基準案	4-1-3-1		一意の認証情報とは、ユーザー間で同一のパスワードとなることを許さないような記載に見えるが、認証要素の組み合わせがユーザーごとに一意であることを記載している理解でよいか。		御認識のとおりです。
391	要求事項・評価基準案	4-1-3-2		重要クラウドでのMFAは必須だが、対象サービスの定義/網羅性が不明である。	定義が曖昧で運用差・監査不適合の恐れがある（明確化の必要がある）	制度構築方針(案)P.17記載のとおり、今後要求事項・評価基準に係る評価方法や取組み事例等を具体的に解説する各種ガイダンス資料等を整備する予定です。いただいた意見については、当該ガイダンス資料等の作成に当たっての参考とさせていただきます。
392	要求事項・評価基準案	4-1-3-2		評価基準4-1-3-2などで「クラウドサービス」についての評価基準を定めている箇所が複数ありますが、内容としてはクラウドサービスではなくともwebシステムであれば自社システム（独自の在庫管理システムなど）も対象とすべきです。 評価基準を満たすことが何らかの理由で難しいとき、「クラウドサービスではなくホスティングサーバ上で動かしているので対象外ではないか」とわざと曲解する余地が残ります。 「★3・★4自己評価ガイド(仮称)」にてその解説をすることになるかと想像しますが、それよりは評価基準上の文言を「インターネットから利用できるシステム」などに書き換えることで曲解する余地をなくしていただけると、セキュリティ専門家による確認・指導において取得希望組織との無用なコミュニケーション工数をとることがなくなるため助かります。		いただいた意見については、今後の検討の参考とさせていただきます。
393	要求事項・評価基準案	4-1-3-2 等		※「サプライチェーン強化に向けたセキュリティ対策評価制度に関する実証報告書 P52 [参考]実証結果を踏まえた要求事項・評価基準の見直し」では「一部の多段階認証を含む」とあるが、評価基準 No.4-1-3-2、4-1-3-3、4-1-3-4 では多段階認証の記載がなく、多要素認証のみ適合と読み取れます。 「一部の多段階認証を含む」という内容を評価基準にも反映いただきたい。 ※第 6 回 産業サイバーセキュリティ研究会 ワーキンググループ 1 サプライチェーン強化に向けたセキュリティ対策評価制度に関するサブワーキンググループ 開催資料 3	評価基準 No.4-1-3-3 の「※利用者のメールアドレス、電話番号等に対してワンタイムパスワードを送信して利用者に入力させる方法及びスマートフォンへの認証要求を利用した認証方式を含む。」を「一部の多段階認証」とする場合は、その旨を明記いただきたい。	いただいた意見も参考にしつつ、要求事項・評価基準における該当箇所の修正を検討させていただきます。
394	要求事項・評価基準案	4-1-3-3		MFA要素の定義に『その他(IPアドレス)』が含まれるが、強度評価の基準が不明である。	定義が曖昧で運用差・監査不適合の恐れがある（明確化の必要がある）	制度構築方針(案)P.17記載のとおり、今後要求事項・評価基準に係る評価方法や取組み事例等を具体的に解説する各種ガイダンス資料等を整備する予定です。いただいた意見については、当該ガイダンス資料等の作成に当たっての参考とさせていただきます。
395	要求事項・評価基準案	4-1-3-4		パスワード最短8文字は最低基準で、高リスクには不十分な可能性がある。	頻度/基準が低くリスク変化に追随できない（実務適合性の改善）	いただいた意見については、今後の検討の参考とさせていただきます。
396	要求事項・評価基準案	4-1-3-5		「★3で対象としている」ではなく、4-1-3-1と具体的に指定してほしい		いただいた意見も参考にしつつ、要求事項・評価基準における該当箇所の修正を検討させていただきます。
397	要求事項・評価基準案	4-1-3-5		1台の共有PCを複数の管理者で使用する場合、アクセスログのみでは使用者の特定が困難になると考えられます。そのため、別途アクセス管理簿を作成し、管理者（使用者）情報およびシステムの利用日時を管理・把握することでよいでしょうか？		御認識のとおりです。
398	要求事項・評価基準案	4-1-3-5		インターネット経由の管理者アクセス/高機密アクセスのMFAはあるが、例外管理が不明である。	定義が曖昧で運用差・監査不適合の恐れがある（明確化の必要がある）	評価機関等との協議により了承を得られた場合等を除き、ここでは適用範囲内における例外措置を認めることは想定していません。
399	要求事項・評価基準案	4-1-4-1		端末ログオンのアカウントロック設定はあるが、閾値/遅延設定の標準が不明である。	定義が曖昧で運用差・監査不適合の恐れがある（明確化の必要がある）	No.4-1-4-1のとおり、失敗回数の閾値は10回以下としています。また、遅延設定については、「試行回数を調整し、試行が失敗するたびに試行間隔が長くなるようにする」ことのほか、★3・★4の要求事項・評価基準としては定めていません。
400	要求事項・評価基準案	4-1-4-1		意見：4-1-4-1において、「試行が10回以上失敗するとアカウントをロックする」との記載がございますが、これではリスクを考慮して10回未満の試行でアカウントロックを設定することが排除されてしまっています。 個々のリスクに応じて回数を最低限許容できる閾値として記載し、リスクベースアプローチが取れるように内容を変更したほうがよいと考えております		いただいた意見も参考にしつつ、要求事項・評価基準における該当箇所の修正を検討させていただきます。
401	要求事項・評価基準案	4-1-4-2		設定不可時の代替策はあるが、例外記録/承認のプロセスが不明である。	定義が曖昧で運用差・監査不適合の恐れがある（明確化の必要がある）	制度構築方針(案)P.17記載のとおり、今後要求事項・評価基準に係る評価方法や取組み事例等を具体的に解説する各種ガイダンス資料等を整備する予定です。いただいた意見については、当該ガイダンス資料等の作成に当たっての参考とさせていただきます。
402	要求事項・評価基準案	4-1-4-2		4-1-4-1と統合すべき内容と思われます。		いただいた意見も参考にしつつ、要求事項・評価基準における該当箇所の修正を検討させていただきます。

No.	該当箇所			寄せられた御意見の概要	理由	提出意見に対する考え方
	該当文書	該当ページ又は項番	該当項目			
403	要求事項・評価基準案	4-1-4-3		端末ロック解除のPIN/パスワード6文字以上は最低基準で、機密端末にはパスワードの機密性が不足している。	頻度/基準が低くリスク変化に追随できない（実務適合性の改善が必要である）	いただいた意見については、今後の検討の参考とさせていただきます。
404	要求事項・評価基準案	4-1-4-3		不正ログイン対策としてのシステムのアカウントロックと、パソコン及びスマートデバイスの画面ロックが同列に記述されており、違和感があります。		いただいた意見も参考にしつつ、要求事項・評価基準における該当箇所の修正を検討させていただきます。
405	要求事項・評価基準案	4-1-5-1		デフォルトパスワード変更はあるが、初期構築/引継ぎ時の検証手順が不明である。	定義が曖昧で運用差・監査不適合の恐れがある（明確化の必要がある）	いただいた意見については、今後の検討の参考とさせていただきます。
406	要求事項・評価基準案	4-1-5-2		要求事項には「周知する」の記載があるが、評価基準にも「周知する」の記載が必要、または「周知する」ことを明記した評価基準の追加が必要ではないか。		いただいた意見も参考にしつつ、要求事項・評価基準における該当箇所の修正を検討させていただきます。
407	要求事項・評価基準案	4-1-5-2		推測されやすい単語の禁止はあるが、禁止リスト/漏洩PWチェックの仕組みが不明である。	定義が曖昧で運用差・監査不適合の恐れがある（明確化の必要がある）	いただいた意見については、今後の検討の参考とさせていただきます。
408	要求事項・評価基準案	4-1-5-3		パスワード長ルールが条件分岐で複雑で現場での誤適用リスクである。	認証強度が最新ベストプラクティスに不足している（ゼロトラスト整合が必要である）	制度構築方針(案)P.17記載のとおり、今後要求事項・評価基準に係る評価方法や取組み事例等を具体的に解説する各種ガイダンス資料等を整備する予定です。いただいた意見については、当該ガイダンス資料等の作成に当たっての参考とさせていただきます。
409	要求事項・評価基準案	4-1-5-4		パスワード使い回し禁止はあるが、SSO/パスワード管理の推奨が記載がない。	認証強度が最新ベストプラクティスに不足している（ゼロトラスト整合が必要である）	いただいた意見については、今後の検討の参考とさせていただきます。
410	要求事項・評価基準案	4-1-5-4		誤字と思われます。 × 情報機器及びサービス間でのパスワードの使い回さないこと ○ 情報機器及びサービス間でパスワードを使い回さないこと ○ 情報機器及びサービス間でのパスワードの使い回しを行わないこと		いただいた意見も参考にしつつ、要求事項・評価基準における該当箇所の修正を検討させていただきます。
411	要求事項・評価基準案	4-1-6-1		紙/アプリでのPW保管は許容されるが、組織的な管理（権限/監査）が不明である。	定義が曖昧で運用差・監査不適合の恐れがある（明確化の必要がある）	いただいた意見については、今後の検討の参考とさせていただきます。
412	要求事項・評価基準案	4-1-6-1		紙媒体への記載及び施錠保管、パスワード管理アプリの利用等により、パスワードを安全に保管することには、ブラウザのパスワード記録機能は含まれるか否か。		
413	要求事項・評価基準案	4-1-6-2		要求事項No.4-1-6 /評価基準No.4-1-6-2 ・「設定可能な場合は・・・強制しないこと。」とあるが、 何の設定が可能な場合を指しているか不明確ではないでしょうか？ 管理ルール（定期的な変更が設定してあれば）？ 設定ルール（4-1-5項が満足していればOK）？ パスワード自体なのか？複雑なパスワードのことを指している？ 多要素認証や二段階認証なのか？		いただいた意見も参考に、要求事項・評価基準の修正を検討させていただきます。
414	要求事項・評価基準案	4-1-6-2		「【別添】 ★３・★４要求事項・評価基準（案）」の「4-1-6-2 ・設定可能な場合はパスワードの定期的な変更を強制しないこと。」については、一定の条件下においては、という前置きが必要と考えます。条件の具体例としては、 同一のIDを使用するすべてのシステムにおいて、 ・多要素認証が具備されていること。 ・強固なパスワード設定を強制できていること。 ・パスワードが漏洩したことが検知できていること。 というものが挙げられるかと考えます。 このような条件を満たさない状況でパスワードの定期的な変更を行わない場合、システムへの侵害を受けた際に長期にわたり侵害を受けることとなり、被害がより深刻となることが想定されます。		いただいた意見も参考に、要求事項・評価基準の修正を検討させていただきます。
415	要求事項・評価基準案	4-1-6-2		定期的変更を強制しない方針は適切だが、漏洩検知時の自動強制変更の仕組みが不明である。	定義が曖昧で運用差・監査不適合の恐れがある（明確化の必要がある）	いただいた意見については、今後の検討の参考とさせていただきます。 なお、No.4-4-6-3(★3)において、パスワードの漏洩が判明した場合等におけるパスワードを変更する手順を定めることとしています。
416	要求事項・評価基準案	4-1-6-2		設定可能な場合はパスワードの定期的な変更を強制しないことは、多要素認証ではない環境であっても実施すべきであり、定期変更を求めている場合は、違反として認識するという要求でよいか。		No.4-1-6-1-については、設定可能な場合であれば、環境を問わず実施する必要があります。 なお、いただいた意見も参考に、要求事項・評価基準における該当箇所の修正を検討させていただきます。
417	要求事項・評価基準案	4-1-6-3		パスワード漏洩時はパスワード変更だけでなく、セッションの切断や不審な多要素認証デバイスの登録解除などを行う必要があるのではないか。★5でも構わないがパスワード変更だけでなくアカウント侵害に利する設定の確認および変更の手順について定めるよう記載をお願いしたい。		いただいた意見については、今後の検討の参考とさせていただきます。
418	要求事項・評価基準案	4-1-7-2		アクセス権管理ルールはあるが、権限の棚卸頻度（年1回）が高リスクには不足している。	定義が曖昧で運用差・監査不適合の恐れがある（明確化の必要がある）	今回の要求事項・評価基準では、取得希望組織が一律で満たすべきベースラインとしての基準であることを考慮し、最低限年1回、点検を行うこととしています。各取得希望組織の任意の取り組みとして、それ以上の頻度等で点検を行うことは否定されるものではありません。
419	要求事項・評価基準案	4-1-7-3 ～ 4-1-7-6		重要システムでの権限分離は規定されるが、実装（個人別二重アカウント）までの要求が不足している。	制度文言の実務適合性・明確性の向上が必要である	いただいた意見については、今後の検討の参考とさせていただきます。
420	要求事項・評価基準案	4-1-7-5		「情報利用者及びシステム管理者の権限を分離し、個人に権限が集中しない環境とすること。」とありますが、情報利用者（ユーザ）とシステム管理者の権限は当然異なるものと思われます。権限の分離（職務の分離）とは、例えば申請者と承認者を分けるといったことではないでしょうか。		いただいた意見も参考にしつつ、要求事項・評価基準における該当箇所の修正を検討させていただきます。
421	要求事項・評価基準案	4-1-7-6		「定期的」は一年以内を想定しているのか。期間を明記いただきたい。		いただいた意見も参考にしつつ、要求事項・評価基準における該当箇所の修正を検討させていただきます。
422	要求事項・評価基準案	4-1-8-1 ～ 4-1-8-4		サーバ設置エリアの入退管理はあるが、監査証跡の保管期間（6カ月）が短い可能性がある。	制度文言の実務適合性・明確性の向上が必要である	今回の要求事項・評価基準では、取得希望組織が一律で満たすべきベースラインとしての基準であることを考慮し、最低限保管すべき期間をを定めています。各取得希望組織の任意の取り組みとして、それ以上期間保管することは否定されるものではありません。
423	要求事項・評価基準案	4-1-8-3		4-1-8-2と4-1-8-3は統合してよいと思われます。		4-1-8-3については、4-1-8-2のいずれかのパターンにおいて使用する施錠について、適切に管理することを求める評価基準であるため、独立した評価基準としています。
424	要求事項・評価基準案	4-1-8-4		施錠が出来ないエリア（専用ラックで施錠保管）は対象外としていただきたい。	サーバ室以外に設置しているサーバもあるため。	ここでは、施錠有無にかかわらず、No,4-1-8-1で定めたサーバ設置エリアについて、当該エリアに入退場した可能性がある者を特定することを目的に、入退場記録を取得することとしています。
425	要求事項・評価基準案	4-1-9-1 ～ 4-1-9-3		可搬媒体の持込み/持出しルールはあるが、例外承認/違反検出の仕組みが不明である。	定義が曖昧で運用差・監査不適合の恐れがある（明確化の必要がある）	制度構築方針(案)P.17記載のとおり、今後要求事項・評価基準に係る評価方法や取組み事例等を具体的に解説する各種ガイダンス資料等を整備する予定です。いただいた意見については、当該ガイダンス資料等の作成に当たっての参考とさせていただきます。
426	要求事項・評価基準案	4-1-9-3		遵守状況の点検についてはどのような対応を想定されているのか。ヒアリングやアンケート回答で問題ないのか、ログなどトレーサビリティのある情報の保管が必要なのか明記頂きたい。		御認識のとおり、ヒアリングやアンケート回答による点検を想定しています。
427	要求事項・評価基準案	4-2-1-1		この機会とは具体的にどういったものを想定しておりますでしょうか？		セキュリティに係る研修等が想定されます。
428	要求事項・評価基準案	4-2-1-1		本項目「・経営層が情報セキュリティに関する役割及び責任を理解するための機会を設けること。」は「理解する」というプロセスに留まっており、経営層が主体となって「何を成すべきか（目的）」や「組織にどう影響を与えるか（文化醸成）」という視点が不足しています。 特に製造業でも一般的である安全文化（Security Culture）のような組織文化の定着はトップダウンの姿勢が不可欠ですので、その意図を反映し以下のような修正案を提案いたします。 【案１】 「経営層は、情報セキュリティインシデントの発生抑制および発生時の迅速な対応における自らの役割と責任を明確化したうえで、それらを深く習熟するための機会を継続的に設けること。」 【案２】 「経営層は、サイバーセキュリティを組織の持続的成長を支える『安全管理』の根幹と位置づけ、インシデントの発生抑制および有事の対応における自らの指導的役割と責任を明確化すること。また、現場から経営まで一貫したセキュリティのための組織文化を醸成するため、その責務を深く理解し、体現するための機会を継続的に設けるものとする。」	参考：ISO45001:2018 5 リーダーシップ及び働く人の参加 5.1 リーダーシップ及びコミットメント 「安全管理の根幹」: セキュリティを単なるコストや技術的対策ではなく、日本企業が得意とする「安全労働」や「品質保証」と同等の経営基盤として再定義しました。 「指導的役割」: 単なる理解（Understand）に留まらず、リーダーとして組織を牽引する（Lead）姿勢を求めています。 「一貫した安全文化」: 日本の強みである「現場の規律」と「経営の決断」が連動する状態を指し、サイバーレジリエンス（回復力）を高める意図を込めています	いただいた意見については、今後の検討の参考とさせていただきます。
429	要求事項・評価基準案	4-2-1-1 ～ 4-2-1-6		経営層の役割理解機会はあるが、マネジメント訓練プログラム/報告プロセスが不明である。	定義が曖昧で運用差・監査不適合の恐れがある（明確化の必要がある）	制度構築方針(案)P.17記載のとおり、今後要求事項・評価基準に係る評価方法や取組み事例等を具体的に解説する各種ガイダンス資料等を整備する予定です。いただいた意見については、当該ガイダンス資料等の作成に当たっての参考とさせていただきます。
430	要求事項・評価基準案	4-2-1-2		「セキュリティの重要性を再認識する機会」とありますが、やや抽象的に思われます。No.4-2-1-4の教育でカバーできるように思われますし、不足するのであればより具体化して示していただきたいです。		いただいた意見も参考にしつつ、要求事項・評価基準における該当箇所の修正を検討させていただきます。

No.	該当箇所			寄せられた御意見の概要	理由	提出意見に対する考え方
	該当文書	該当ページ又は項番	該当項目			
431	要求事項・評価基準案	4-2-1-2		本項目を、「役員、従業員、派遣社員及び受入出向者を対象に、サイバーセキュリティインシデントを未然に防ぎ、あるいは発生時に迅速な対応を行うために必要な知識・技能を習得する機会を、月次等の極めて高い頻度で継続的に提供すること」に変更する。 （実施手段の例：最新の攻撃手法を模した疑似攻撃訓練の実施や、実務に即した対処フローを確認するマイクロラーニングを日常の業務ルーティンに組み込むこと）	「最低基準のゴール化」による慢心の防止と空白期間の解消 「年1回以上」という規定は、本来「最低限の頻度」を示すものですが、実態として多くの組織において「年1回実施すれば十分である」という誤った認識や慢心を生む原因となっています。この結果、規定の遵守自体がゴール（ノルマ）となり、実施内容が形骸化するだけでなく、次回の実施まで最新の脅威情報がアップデートされないという長期間の「防御の空白」が生じています。サイバー攻撃の手法およびIT環境は日進月歩で変化しており、この頻度の少なさが組織の防衛レベルを底下げしてしまう事態を避けるためにも、より高い頻度での実施を促す記述への見直しが不可欠です。 精神論から実効的な「防衛スキル」への転換 従来の「重要性の再認識」という表現は、個人の意識や心構えに依存する側面が強く、具体的な攻撃に対する防御能力の向上を客観的に評価することが困難です。サイバー攻撃が巧妙化・複雑化する現状においては、脅威を正しく識別し、手順に基づいた適切な対処を行うための「具体的な知識と技能の習得」を目的として定義すべきです。 忘却曲線に基づいた教育効果の最大化と形骸化の防止 一度に大量の情報を提供する年1回の集中教育よりも、短時間の学習を反復する（マイクロラーニング等の）手法の方が、知識の定着率およびインシデント発生時の反射的な対応力（即応力）を高めることが認知科学的にも証明されています。また、規定の頻度を高めることで、「実施すること自体が目的」となる形骸化を防ぎ、セキュリティ対策を組織文化の一部として定着させることが期待できます。	いただいた意見については、今後の検討の参考とさせていただきます。
432	要求事項・評価基準案	4-2-1-3		本項目[・職場特有のリスクの理解及びルールの遵守が必要な場合、職場単位で重要なルール及びリスクについて、年１回以上の頻度で周知すること。]を、 「業務実態に即したセキュリティ課題やリスクを現場単位で能動的に特定し、セキュリティ担当部門との協議を通じて、既存ルールを実効的な内容へと柔軟に改定し続けるプロセスを構築すること。また、ルールの改定時は遅滞なく周知・徹底を行い、その理解度と遵守状況を継続的に確認する仕組みを設けること」 に変更する。 （具体的運用の例：現場の業務フローと現行ルールの乖離を定期的にヒアリングし、形骸化したルールの見直しを行う。また、改定されたルールは即座に社内ポータル等で共有し、理解度テスト等を通じて定着を確認する。）	• ルールの形骸化に伴う「隠蔽・逸脱リスク」の排除 「年1回、既存のルールを周知する」という受動的な運用では、現場の実態とルールとの乖離（シャドーITの利用や運用の簡略化など）を放置することに繋がります。ルールが業務の妨げとなった際、現場が独断でルールを逸脱したり、その事実を隠蔽したりするリスクを最小化するためには、現場と専門部門が協調してルールを適正化し続けるプロセスが不可欠です。 • 「実効性」を重視した動的なリスクマネジメントへの転換 IT環境やビジネスモデルが変化し続ける中で、固定化されたルールを一方的に周知するだけの活動は実効性に欠けます。現場単位で「今の業務におけるリスク」を再発見し、それに基づき規定を柔軟にアップデートするサイクルを定義することで、組織のレジリエンス（回復力・適応力）を高めることが可能となります。 • 周知の即時性と理解度の定量的把握 ルールは「作成して終わり」ではなく、変更が即座に末端まで浸透し、正しく理解されていることが担保されなければなりません。周知の頻度を年1回などの期間で縛るのではなく、「ルールの最適化が行われた時点で、即座に教育・周知を行う」という即時性を重視した基準へシフトすることで、常に最新の防御態勢を維持する狙いがあります。	いただいた意見については、今後の検討の参考とさせていただきます。
433	要求事項・評価基準案	4-2-1-4		以下のトピックについて、役員、従業員、派遣社員及び受入出向者を対象に、新規受入れ時、かつ、年１回以上、教育資料配布・掲示、e ラーニング、集合教育等による教育を実施すること。 - 電子メールによるマルウェア感染の予防 - Web 閲覧によるマルウェア感染の予防 - 機密区分の定義と取扱い		ここでは、自工会・部工会サイバーセキュリティガイドライン等を参照のうえ、取得希望組織が最低限実施すべきセキュリティ教育の項目として電子メールによるマルウェア感染の予防、Web 閲覧によるマルウェア感染の予防、機密区分の定義の3つを規定しています。各取得希望組織の任意の取り組みとして、それ以外の項目についてセキュリティ教育を実施することは否定されるものではありません。
434	要求事項・評価基準案	4-2-1-4		マルウェア予防/機密取扱い教育はあるが、釣りメール訓練や実践演習の記載が不足している。	制度文言の実務適合性・明確性の向上が必要である	今回の要求事項・評価基準では、取得希望組織が一律で満たすべきベースラインとしての基準であることを考慮し、最低限セキュリティ教育として、電子メール・web閲覧によるマルウェア感染予防及び機密区分に関する内容を実施することとしています。各取得希望組織の任意の取り組みとして、それ以上の内容のセキュリティ教育を行うことは否定されるものではありません。
435	要求事項・評価基準案	4-2-1-4		本項目を、「ヒューマンエラーに起因するインシデントを未然に防止するため、役員、従業員、派遣社員及び受入出向者を対象に、最新の脅威動向や法規制の改正に即応した教育・訓練（標的型攻撃メール訓練など）を、月次等の高い頻度で継続的に実施すること。また、教育に関連するリソースへ常時アクセス可能な環境を整備し、全ての対象者に公平かつ多様な学習機会を提供すること」に変更する。 （具体的トピックの例） ソーシャルエンジニアリング攻撃（心理的隙を突く攻撃）への対処 内部不正・情報漏洩等に伴う刑事・民事上の法的責任の理解 機密区分の定義と実務に即した具体的な取扱い方法	• 攻撃手法の高度化に伴う「人的レジリエンス」の強化 従来の「メールやWebの閲覧注意」といった限定的な教育では、近年の巧妙なソーシャルエンジニアリング（サポート詐欺、ビジネスメール詐欺や音声やビデオを使った心理的な誘導等）を防ぐことは困難です。技術的な対策を回避して「人」を標的とする攻撃に対し、具体的な手口や背景を学ぶ機会を高頻度で提供することで、組織全体の防御力を「知識」から「習慣」のレベルまで引き上げる必要があります。 • 法的責任の明確化による内部不正の抑止と意識改革 情報の取扱不備や内部不正が、組織のみならず個人に対しても刑事罰や多額の損害賠償請求（民事責任）を招き得ることを正しく周知することは、強い心理的抑止力となります。単なるマナーとしてのセキュリティではなく、法遵守（コンプライアンス）に直結する重要課題として再定義することで、役員から派遣社員まで一貫した危機意識の醸成を図ります。 • 「教育の民主化」とアクセシビリティの確保 「年1回の集合研修」のような限定的な機会では、勤務形態や就業場所の異なる多様な従業員の間で、知識の格差が生じるリスクがあります。常時アクセス可能な学習環境を整備し、マイクロラーニング等の手法を通じて公平な学習機会を担保することで、組織内の特定の層がセキュリティの「弱点」となる事態を構造的に防ぎます。	いただいた意見については、今後の検討の参考とさせていただきます。
436	要求事項・評価基準案	4-2-1-5		[・No.4-2-1-4で実施した教育の実施状況を記録し、保管すること。] 本項目を、「実施した教育および訓練の受講状況を詳細に記録・保管するとともに、部門別および個人別の受講率を定期的に分析すること。受講率の低い対象についてはその要因を特定し、受講環境の改善や動機付けといった具体的な向上施策を継続的に講じること」に変更する。 （具体的運用の例：ダッシュボード等でリアルタイムに受講率を可視化し、未受講者が多い部門に対しては、業務負荷の調整や教育形態の見直しを部門長と連携して実施する。）	• 「形骸化した記録」から「実効的な管理」への転換 教育の記録は、単に「実施した事実」を証明するためのものではなく、組織全体の防御力の偏りを把握するための経営データであるべきです。記録を保管するだけでなく、受講率の低い箇所を特定・分析するプロセスを明文化することで、組織内に「セキュリティ教育の未受講」という脆弱性を放置させない仕組みを構築します。 • 要因分析に基づく学習環境の最適化 受講率が低い背景には、業務多忙、コンテンツの不適合、あるいは物理的なアクセス困難など、現場固有の課題が隠れている場合が多くあります。画一的に受講を督促するのではなく、要因に応じた改善策を継続的に講じることで、形骸化を防ぎ、全従業員が実効性のある教育を等しく受けられる体制を担保します。 • 継続的なPDCAサイクルによる「全社的防御力」の底上げ 高頻度な教育（マイクロラーニング等）を導入する場合、その受講状況を迅速にフィードバックし、改善に繋げるサイクルが不可欠です。分析と向上策をセットで義務付けることにより、一部の意識高い層だけでなく、組織全体のセキュリティ意識と技能を底上げする「ラストワンマイル」の取り組みを強化する狙いがあります。	いただいた意見については、今後の検討の参考とさせていただきます。
437	要求事項・評価基準案	4-2-1-6		[年１回以上の頻度でセキュリティの意識向上のための教育・研修の実施内容について点検すること。] 本項目を、「教育・研修の実施内容およびその成果について、月次や四半期等の高い頻度で定期的に評価・点検すること。教育実施後のアンケートや理解度テストを通じてプログラムの実効性を分析し、速やかに内容の改善や更新に反映させること。その際、異なる業務内容や役職に応じた最適化を図り、画一的な研修や知識の詰め込みといった一方的な教育形態を回避すること」 に変更する。 （具体的運用の例：職種ごとに異なるリスク（例：開発職なら脆弱性、営業職なら外出先での紛失等）に応じた教育コンテンツを提供し、受講者のフィードバックに基づいて毎月教材をブラッシュアップする。）	• 「一方的な教育」による形骸化と学習意欲低下の防止 全従業員に対して画一的、あるいは一度に大量の知識を詰め込む教育は、受講者にとって「自分とは無関係な業務負担」と感じられやすく、結果として学習効果が著しく低下します。役職や職種に応じた「自分事化」できる内容へ最適化し、双方向の改善プロセス（フィードバックの反映）を取り入れることで、能動的な学習姿勢を促す必要があります。 • 高速な改善サイクルによる「教育の鮮度」の維持 サイバー脅威の変遷に対し、年1回の点検では教育内容が容易に陳腐化します。月次や四半期単位で点検を行い、現場の声（アンケート結果等）を即座に反映させることで、常に実務に即した「生きた教育プログラム」を維持することが可能となります。 • 教育の「質」と「実効性」の定量的・定性的評価 単に「実施した」という事実の点検ではなく、「その教育によってリスクがどう低減したか」「従業員の理解がどう深まったか」という成果に主眼を置いた評価基準が必要です。現場の声を吸い上げ、教育のあり方を柔軟にアップデートし続けることで、組織全体のセキュリティ・レジリエンスを実質的に向上させます。	いただいた意見については、今後の検討の参考とさせていただきます。
438	要求事項・評価基準案	4-2-2-1		年1回以上の意識向上はあるが、受講率/理解度KPIが未定義である。	頻度/基準が低くリスク変化に追随できない（実務適合性の改善が必要である）	受講率や理解度のKPIについては、各取得希望組織において任意で設定されることを想定しています。
439	要求事項・評価基準案	4-2-2-1		e ラーニング又は集合教育による教育・訓練を実施の教育・訓練とは、教育及び訓練か、教育もしくは訓練か、ご教示いただきたい。		4-2-2-1では、セキュリティインシデント発生時の対応について、最低限eラーニング又は集合教育による教育を実施したうえで、各取得希望組織の必要に応じて訓練についても実施することを想定しています。
440	要求事項・評価基準案	4-2-2-1		"教育・訓練を実施すること"は、"教育もしくは訓練を実施すること"と解釈するのでしょうか？それとも"教育かつ訓練を実施すること"と解釈するのでしょうか？御教示ください。		4-2-2-1では、セキュリティインシデント発生時の対応について、最低限eラーニング又は集合教育による教育を実施したうえで、各取得希望組織の必要に応じて訓練についても実施することを想定しています。
441	要求事項・評価基準案	4-2-2-1		教育・訓練の対象とするセキュリティインシデントの具体例を示していただきたい。 不審メール受信など一般従業員を意識したレベルなのか、BCP対応レベルのインシデントまで、なのか？		No.5-2-1-1において各取得希望組織ごとに定めたセキュリティインシデントの基準に照らして、各社で教育・訓練の内容を検討することを想定しています。
442	要求事項・評価基準案	4-2-2-1		本項目を、「役員、従業員、派遣社員及び受入出向者を対象に、セキュリティインシデント発生時の対応について、各対象者の役割（一般従業員、情報システム・CSIRT担当、経営層等）に応じた専門性の高い教育・訓練を実施すること。また、心理的安全性を確保し、インシデントやヒヤリハットの早期報告を奨励する『ジャストカルチャー（公正な文化）』を醸成することで、叱責や処罰を恐れた隠蔽を防ぎ、失敗から組織的に学習できる環境を構築すること」 に変更する。 （具体的運用の例：経営層向けには意思決定演習、現場向けには初動対応訓練を別個に行う。併せて、些細なミスや懸念を速やかに報告した者を正当に評価し、その事例を再発防止の学習教材として活用するサイクルを設ける。）	• 役割に応じた実効的な対応能力の習得 インシデント発生時に求められる行動は、経営判断を行う層と実務を行う層で大きく異なります。画一的な教育資料の配布ではなく、それぞれの役割に直結したシナリオベースの訓練を行うことで、有事の際の実効的な即応力を担保する必要があります。 • 「隠蔽」による被害拡大リスクの最小化 インシデントの初期段階における報告遅延や隠蔽は、被害を壊滅的な規模に拡大させる最大の要因です。過度な叱責や個人への処罰に偏った文化は、現場の萎縮と情報の隠蔽を招きます。報告者を非難せず、事象の原因を組織的に究明する「ジャストカルチャー」を制度として明文化することで、潜在的なリスクの早期発見を可能にします。 • 「失敗からの学習」による組織レジリエンスの向上 ヒヤリハットを含む小規模な事象を隠さず共有することは、組織全体にとって極めて貴重な学習機会となります。これらの情報を収集・分析し、教育プログラムへ機動的にフィードバックする仕組みを設けることで、重大なインシデントの発生を未然に防ぐ、自律的な防衛体制を構築するためです。	いただいた意見については、今後の検討の参考とさせていただきます。
443	要求事項・評価基準案	4-2-2-2		教育実施状況の記録はあるが、保持期間/監査での活用が不明である。	定義が曖昧で運用差・監査不適合の恐れがある（明確化の必要がある）	ここでは、教育・訓練の実施内容・実施方法・実施時期の見直し及び受講対象者における受講状況の把握に支障がない範囲内で、各取得希望組織により任意で保管期間を定めることを想定しています。
444	要求事項・評価基準案	4-2-2-3		インシデント対応教育・訓練の点検方法はあるが、点検のみで改善有無が不明である。	定義が曖昧で運用差・監査不適合の恐れがある（明確化の必要がある）	本評価基準における「点検」とは、セキュリティインシデント発生時の対応に関する「教育・訓練の実施内容」について、その適切性や有効性を確認する行為を指しており、教育・訓練の実施自体を「点検」と表現しているものではありません。 点検の結果、取得希望組織において改善の必要性が認められた場合には、必要に応じて教育・訓練の内容の修正又は更新を行っていただくことを想定しております。
445	要求事項・評価基準案	4-3-1-1		社外持出し機器/高機密の暗号化ルールはあるが、鍵管理/復旧手順が不明である。	定義が曖昧で運用差・監査不適合の恐れがある（明確化の必要がある）	制度構築方針(案)P.17記載のとおり、今後要求事項・評価基準に係る評価方法や取組み事例等を具体的に解説する各種ガイダンス資料等を整備する予定です。いただいた意見については、当該ガイダンス資料等の作成に当たっての参考とさせていただきます。

No.	該当箇所			寄せられた御意見の概要	理由	提出意見に対する考え方
	該当文書	該当ページ又は項番	該当項目			
446	要求事項・評価基準案	4-3-1-1		■意見内容 暗号化について、情報のライフサイクル全体を通じて適切な技術的保護が維持されることが重要であることが明確に分かる文言の追記	評価基準No.4-3-1-1およびNo.4-3-1-2において「暗号化」と表現されている内容について、 保存時に暗号化されているか否かのみを指すものと解釈される余地があるように思われます。 一方で、暗号化された情報であっても、利用時に暗号化が解除され平文状態となる場合には、 当該情報が第三者に取得され得る状態となることから、暗号化の有無を保存時のみで評価することは、実際のリスクの捉え方として十分ではないと考えられます。 そのため、暗号化については、単に保存時に暗号化されていることにとどまらず、利用時を含め、暗号化又は同等の技術的保護が情報のライフサイクル全体を通じて維持されることが重要である旨が、評価基準の表現から明確に読み取れるようにすることが望ましいと考えます。 例えば、「利用時に暗号化が解除されることを前提とした場合においても、情報が不適切に取得されないような技術的保護が講じられていることが重要である」といった趣旨が分かる表現への修正を検討してはどうでしょうか。	いただいた意見については、今後の検討の参考とさせていただきます。
447	要求事項・評価基準案	4-3-1-2		3-1-4-3の対象者にだけ周知するのか、適用範囲全体に周知するのか明記頂きたい。		ここでは適用範囲全体に周知することを想定しています。
448	要求事項・評価基準案	4-3-1-2		職場単位の周知はあるが、高い機密区分の定義が不明である。	定義が曖昧で運用差・監査不適合の恐れがある（明確化の必要がある）	No.3-1-4-1にて各社で定めた機密区分のうち、高い機密区分に該当する情報を指しています。
449	要求事項・評価基準案	4-3-1-2		No.3-1-4-3における高い機密区分の情報とあるが、同No.は『機密区分のうち、高い機密区分の情報並びに当該情報ごとの管理者名、部署名、保管場所、保管期限、開示先及び管理者の連絡先を把握するための仕組みを整備すること』と書かれていて不整合ではないか。		ここでのNo.3-1-4-3における高い機密区分の情報とは、例えば、各取得希望組織における情報管理規程等のルールにて策定した機密区分表の中で、高い機密区分に該当する情報のことを指しています。
450	要求事項・評価基準案	4-3-2-1		社内ネットワーク上である必要はあるのか。クラウドサービス上には保管しないように指示しているのであれば明記頂きたい。		いただいた意見も参考にしつつ、要求事項・評価基準における該当箇所の修正を検討させていただきます。
451	要求事項・評価基準案	4-3-2-1		重要データの保管は『安全な区域のサーバ』推奨だが、ローカル保存禁止基準が不明である。	定義が曖昧で運用差・監査不適合の恐れがある（明確化の必要がある）	制度構築方針(案)P.17記載のとおり、今後要求事項・評価基準に係る評価方法や取組み事例等を具体的に解説する各種ガイダンス資料等を整備する予定です。いただいた意見については、当該ガイダンス資料等の作成に当たっての参考とさせていただきます。
452	要求事項・評価基準案	4-3-2-1		相対的に安全な区域とは具体的に何か、ご教示いただきたい。		一般的には、インターネットからのアクセスが一定程度制限されたネットワーク上の区域が想定されます。
453	要求事項・評価基準案	4-3-3-1		社外共有時の『送信履歴が残らない方法の禁止』は適切だが、許容手段の具体化が必要である。	定義が曖昧で運用差・監査不適合の恐れがある（明確化の必要がある）	制度構築方針(案)P.17記載のとおり、今後要求事項・評価基準に係る評価方法や取組み事例等を具体的に解説する各種ガイダンス資料等を整備する予定です。いただいた意見については、当該ガイダンス資料等の作成に当たっての参考とさせていただきます。
454	要求事項・評価基準案	4-3-3-2		明記されていない記録の保管期間は任意でよいのか。		ここでは、教育・訓練の実施内容・実施方法・実施時期の見直し及び受講対象者における受講状況の把握に支障がない範囲内で、各取得希望組織により任意で保管期間を定めることを想定しています。
455	要求事項・評価基準案	4-3-4-1		バックアップ対象/頻度/保管期間は規定されるが、復元に関する頻度が不足している。	定義が曖昧で運用差・監査不適合の恐れがある（明確化の必要がある）	いただいた意見については、今後の検討の参考とさせていただきます。
456	要求事項・評価基準案	4-3-4-2		遠隔地の基準について教えていただけますでしょうか。		一般的には、災害発生時でも安全な保管ができる程度には、拠点と距離が確保された場所を指すことが想定されます。
457	要求事項・評価基準案	4-3-4-2		遠隔地バックアップはあるが、ネット分離/暗号化/整合性検証の要件が不明である。	定義が曖昧で運用差・監査不適合の恐れがある（明確化の必要がある）	制度構築方針(案)P.17記載のとおり、今後要求事項・評価基準に係る評価方法や取組み事例等を具体的に解説する各種ガイダンス資料等を整備する予定です。いただいた意見については、当該ガイダンス資料等の作成に当たっての参考とさせていただきます。
458	要求事項・評価基準案	4-4-1,4-4-2		各要求事項について、セキュリティリスクの重大性に応じて適切なレベルの対応を行なえば、評価基準を満たすのではないかと考えるが、この点は評価機関に対し、根拠を持って説明を行うことで認められるのか。		★4においては、評価機関による第三者評価を経たうえで、評価を取得することができます。具体的な評価手続等については、いただいた意見も参考にしつつ、今後具体的に検討してまいります。
459	要求事項・評価基準案	4-4-1-1		WindowsPCなどデフォルトで多種のSWがインストールされており、業務利用しないソフトウエア全てを削除、無効化でなく、利用不可のルール設定をもって対応とみなしていただきたい。	全PC・サーバに対して業務利用しない全SWの削除は膨大な手間とリスクを伴うため。	いただいた意見も参考にしつつ、要求事項・評価基準における該当箇所の修正を検討させていただきます。
460	要求事項・評価基準案	4-4-1-1 ～ 4-4-1-2		不要ソフト/サービス無効化は規定されるが、許可リスト（Allowlist）と自動適用の整備が不足している。	例外管理・SLA・承認プロセスが不十分（ガバナンス/監査可能性の強化が必要である）	いただいた意見については、今後の検討の参考とさせていただきます。
461	要求事項・評価基準案	4-4-1-2		外部媒体の自動実行無効化はあるが、対象OS/適用方法（GPO等）の標準化が不明である。	定義が曖昧で運用差・監査不適合の恐れがある（明確化の必要がある）	制度構築方針(案)P.17記載のとおり、今後要求事項・評価基準に係る評価方法や取組み事例等を具体的に解説する各種ガイダンス資料等を整備する予定です。いただいた意見については、当該ガイダンス資料等の作成に当たっての参考とさせていただきます。
462	要求事項・評価基準案	4-4-1-3		設定変更の申請/承認はあるが、変更のリスク評価/ロールバック計画が不明である。	定義が曖昧で運用差・監査不適合の恐れがある（明確化の必要がある）	制度構築方針(案)P.17記載のとおり、今後要求事項・評価基準に係る評価方法や取組み事例等を具体的に解説する各種ガイダンス資料等を整備する予定です。いただいた意見については、当該ガイダンス資料等の作成に当たっての参考とさせていただきます。
463	要求事項・評価基準案	4-4-1-4		「ルールに定めた不要サービスについては、原則、無効化する」などの緩和案を検討いただきたい。	不要サービス・プロトコルの列挙、およびそれを全端末に求めることは困難であるため	どのサービスが不要かについては、各取得希望組織において判断されることを想定しています。
464	要求事項・評価基準案	4-4-1-5		デフォルトユーザIDの停止はあるが、初期アカウントの棚卸と監査の仕組みが不明である。	定義が曖昧で運用差・監査不適合の恐れがある（明確化の必要がある）	いただいた意見については、今後の検討の参考とさせていただきます。
465	要求事項・評価基準案	4-4-1-5		デフォルトユーザ ID の利用を停止することは、ローカルアドミン等で不可能ではないか。そもそもsystemやroot等で使われている。利用者によるデフォルトユーザ ID の利用停止を意図しているのか。		adminやrootなどの第三者が容易に想像可能なデフォルトユーザIDは、不正ログインなどのサイバー攻撃で狙われやすく、リスクが高いため、評価基準No.4-4-1-5では停止することとしています。 なお、いただいた御意見も参考に、要求事項・評価基準における該当部分について修正を検討させていただきます。
466	要求事項・評価基準案	4-4-1-5		従業員が利用するパソコンを対象とするなど、組織の実態にあわせた緩和案を検討いただきたい。	全端末にデフォルトユーザIDの利用停止を求めることが困難であるため	adminやrootなどの第三者が容易に想像可能なデフォルトユーザIDは、不正ログインなどのサイバー攻撃で狙われやすく、リスクが高いため、評価基準No.4-4-1-5では停止することとしています。 なお、いただいた御意見も参考に、要求事項・評価基準における該当部分について修正を検討させていただきます。
467	要求事項・評価基準案	4-4-1-6		ベンダ推奨設定参照はあるが、社内標準との差分管理が不明である。	定義が曖昧で運用差・監査不適合の恐れがある（明確化の必要がある）	いただいた意見については、今後の検討の参考とさせていただきます。
468	要求事項・評価基準案	4-4-1-6		統一的な標準構成・設定ルールを定めることは困難であるため、組織の実態にあわせた緩和案を検討いただきたい。	統一的な標準構成・設定ルールを定めることは困難であるため	ここでは、全社統一の標準構成・設定ルールを定める必要はないと考えています。
469	要求事項・評価基準案	4-4-2-1		非サポートOS/ソフトの更改計画は求められるが、例外時の代替制御の必須化が不足している。	例外管理・SLA・承認プロセスが不十分（ガバナンス/監査可能性の強化が必要である）	いただいた意見については、今後の検討の参考とさせていただきます。
470	要求事項・評価基準案	4-4-2-1		「サポート期限の切れたOS及びソフトウェアの利用停止及び更改を実施すること。」を →「サポート期限の切れたOS 、ファームウェア、デバイスドライバ及びソフトウェア利用停止及び更改を実施すること。」 にした方が良いと思います。		いただいた意見については、今後の検討の参考とさせていただきます。
471	要求事項・評価基準案	4-4-2-1		更改計画を完了させる期日はあるか。保有するリスクを適切に管理し、継続的なリスク低減活動を行うことが説明可能であれば認められるのか。		制度構築方針(案)P.17記載のとおり、今後要求事項・評価基準に係る評価方法や取組み事例等を具体的に解説する各種ガイダンス資料等を整備する予定です。いただいた意見については、当該ガイダンス資料等の作成に当たっての参考とさせていただきます。
472	要求事項・評価基準案	4-4-3-1		プロキシサーバのログはリクエスト元IPアドレスと"リクエスト先"URLで問題ないか。		制度構築方針(案)P.17記載のとおり、今後要求事項・評価基準に係る評価方法や取組み事例等を具体的に解説する各種ガイダンス資料等を整備する予定です。該当箇所については、いただいた意見も参考にしつつ、当該ガイダンス資料等で具体化してまいります。
473	要求事項・評価基準案	4-4-3-1		取得/保管すべきログの種類/期間はあるが、クラウドサービスの取得制約時の選定基準が不明である。	定義が曖昧で運用差・監査不適合の恐れがある（明確化の必要がある）	制度構築方針(案)P.17記載のとおり、今後要求事項・評価基準に係る評価方法や取組み事例等を具体的に解説する各種ガイダンス資料等を整備する予定です。いただいた意見については、当該ガイダンス資料等の作成に当たっての参考とさせていただきます。
474	要求事項・評価基準案	4-4-3-1		意見： ログの取得・保管要件において、「プロキシサーバのログ」や「IPアドレス」等の特定技術・項目を明示的に求める記述は、サーバーレスアーキテクチャやコンテナ環境等のモダンな構成と整合しない場合がございます。「トレーサビリティの確保」等の目的ベースの記述に改め、ログの種類を限定しないように変更していただきたいです。 要求事項では、取得すべきログとして「プロキシサーバのログ」や「接続元IPアドレス」が具体的に列挙されています。しかし、クラウドネイティブな環境（ゼロトラストネットワークやサーバーレス構成）では、固定的なIPアドレスが存在しない、あるいはプロキシを介さない通信制御を行う場合もございます。特定のレガシーなネットワーク構成を前提とした要件定義は、クラウドのメリットである柔軟性を損なう可能性があるため、技術的中立性を保った記述（例：「アクセス元を特定可能な情報」など）に変更していただきたく存じます。		いただいた意見も参考にしつつ、要求事項・評価基準における該当箇所の修正を検討させていただきます。

No.	該当箇所			寄せられた御意見の概要	理由	提出意見に対する考え方
	該当文書	該当ページ又は項番	該当項目			
475	要求事項・評価基準案	4-4-3-2		ログの喪失を防ぐため、外部のシステムへの保管を求めるべき。	ランサムウエアからの復旧時においてどのポイントから復旧させるべきか、においては攻撃の時系列を遡ることが大きなファクターになりますがログを喪失してしまうと、どのタイミングであれば攻撃を受けていないか判断できず復旧できないため追加が望ましいと考えます。	いただいた意見については、今後の検討の参考とさせていただきます。
476	要求事項・評価基準案	4-4-3-3		こちらは全サービスに対して実施必須でしょうか？リスクベースで重要な情報を扱うサービスに絞って行うなどのリスクベースアプローチを適用を想定されていますでしょうか？ 実際、数十から100を超えるサービスを扱っている場合、そのログは膨大であり、またSIEM等へ集約し、一括で監視しようにもログの連携機能を提供していないサービスも多く存在します。そのような場合、自社事業特性などを鑑みたリスクベースアプローチを取るのが通例かと思います。		4-4-3-3では、適用範囲内にあるIT基盤を構成するシステムを対象としたうえで、当該システムに係る認証サーバのログのモニタリングを実施すること想定しています。
477	要求事項・評価基準案	4-4-3-3		認証サーバのログ月次モニタはあるが、高リスク期間の臨時モニタ/自動異常検知の要件が不足している。	認証強度が最新ベストプラクティスに不足（ゼロトラスト整合が必要である）	いただいた意見については、今後の検討の参考とさせていただきます。
478	要求事項・評価基準案	4-4-3-3		モニタリングとは具体的に何を指しているか、ご教示いただきたい。		不審な認証試行がないか、ログを精査することを指します。
479	要求事項・評価基準案	4-4-3-3		「以下の保管期間の規則」とありますが、それらしい記述が見当たりません。		いただいた意見も参考にしつつ、要求事項・評価基準における該当箇所の修正を検討させていただきます。
480	要求事項・評価基準案	4-4-4-1		4-4-4-2の対象は必ずしも仮想パッチを導入できる機器ではありません。 以下に修正案を提案いたします。 「ベンダーが提供するワークアラウンド策を実施した上でアップデート計画を立てること」 また、「仮想パッチ」という言葉は誤解を生みやすいため、別の言葉に置き換えた方が好ましいと考えます。 エンドポイントで実装されるホスト型IPSを想定している場合：ホスト型IPS 脆弱性を持つ機器、機能に到達するまでのNW上で防御する場合：IPSまたはWAF 要は脆弱性そのものへの修正プログラムを当てられない場合でも、外部の防御によって応急処置を行うものと捉えられますのでより具体的な表現に修正頂く事を提案いたします。		いただいた意見も参考にしつつ、要求事項・評価基準における該当箇所の修正を検討させていただきます。
481	要求事項・評価基準案	4-4-4-1		ライセンス/サポート/自動更新の状態要件はあるが、可視化するダッシュボードが不明である。	定義が曖昧で運用差・監査不適合の恐れがある（明確化の必要がある）	制度構築方針(案)P.17記載のとおり、今後要求事項・評価基準に係る評価方法や取組み事例等を具体的に解説する各種ガイダンス資料等を整備する予定です。いただいた意見については、当該ガイダンス資料等の作成に当たっての参考とさせていただきます。
482	要求事項・評価基準案	4-4-4-1		可能であれば、自動アップデートが有効化の可能であればにつき、機能か運用か。一律に不具合発生を考慮せずに有効化せよ、ということか。		自動アップデートを有効にした際の不具合の影響度や無効にした際のリスクを考慮したうえで、有効化するか否かを判断することを想定しています。
483	要求事項・評価基準案	4-4-4-2		公表された脆弱性は必ずしも利用環境と合致しない場合があります。 たとえば該当機能を利用していない場合。 そのため、以下項目を条件に追加される事を提案いたします。 「当該アップデートにより修正される脆弱性を含む機能または設定を利用している場合」		いただいた意見も参考にしつつ、要求事項・評価基準における該当箇所の修正を検討させていただきます。
484	要求事項・評価基準案	4-4-4-2		アップデートの基準としてCVSS v3の基本スコアが採用されていますが、KEVやEPSS等の他の指標も適宜組み合わせて使っていくのが望ましく、何を用いるかを一律定めるよりは企業の判断に任せたほうがよいと考えます。		今回の要求事項・評価基準では、取得希望組織が一律で満たすべきベースラインとしての基準であることを考慮し、企業の裁量に委ねた基準とするのではなく、国際的に広く普及している代表的な指標として、CVSSを脆弱性の評価指標として採用しています。なお、KEVやEPSS等の他の指標も同様に有用なものであり、個々の企業による採用を何ら妨げるものではありません。
485	要求事項・評価基準案	4-4-4-2		アップデートの基準としてCVSS v3の基本スコアが採用されていますが、KEVやEPSS等の他の指標も適宜組み合わせて使っていくのが望ましく、何を用いるかを一律定めるよりは企業の判断に任せたほうがよいと考えます。そのため、例えば「当該アップデートが企業にとって緊急度の高い脆弱性を修正するものである（緊急度はCVSS、KEV、EPSS等のリスク評価指標をもとに判断）。」のように採用するリスク評価指標に幅を持たせていただきたいです。		今回の要求事項・評価基準では、取得希望組織が一律で満たすべきベースラインとしての基準であることを考慮し、国際的に広く普及しているCVSSを脆弱性の評価指標として採用しています。なお、KEVやEPSS等の他の指標も同様に有用なものであり、個々の企業による採用を何ら妨げるものではありません。
486	要求事項・評価基準案	4-4-4-2		重大/高リスクのアップデート『14日以内』の遵守の期限が不明であるため、パッチSLAの遵守率をKPI化し、期限超過は自動通知/是正計画提出を義務化すべきである。	定義が曖昧で運用差・監査不適合の恐れがある（明確化の必要がある）	いただいた意見については、今後の検討の参考とさせていただきます。 なお、今回の要求事項・評価基準では、取得希望組織が一律で満たすべきベースラインとしての基準であることを考慮し、国内外の他の文献等を参照したうえで重大な脆弱性について14日以内に対応することとしています。
487	要求事項・評価基準案	4-4-4-2		評価基準 No.4-4-4-2 を以下のとおり見直しいただきたい。 ・適用範囲内のシステム、情報機器及びソフトウェアについて、脆弱性を修正するためのアップデートプログラムに関する適用基準・適用までの期間を定め、適宜アップデートを実施すること。 ・以下の対象機器について、当該アップデートがベンダーまたは公的機関により緊急性の高いと説明される脆弱性を修正するものである場合は、アップデートプログラムがリリースされてから 14 日以内にアップデートすること。 [対象] ・インターネットとの境界に設置されているサーバやネットワーク機器 ・上記機器の OS 及びファームウェア	外部公開サーバや VPN 装置など、インターネット境界に配置されるサーバ／ネットワーク機器についてはリスクが高いため、14 日以内に対応することが妥当と考えます。 一方で、その他のシステム・機器等は、業種ごとの状況や社内に閉じた環境によりリスクが異なることから、同じ期間での対応が現実的に難しいです。 また、脆弱性評価には CVSS だけでなく、KEV ｶﾀﾛｸﾞや EPSS などの指標が存在するため、CVSS の基本スコアを一律で指定することは、実際の対応と整合しない場合があるため。	今回の要求事項・評価基準では、取得希望組織が一律で満たすべきベースラインとしての基準であることを考慮し、国際的に広く普及しているCVSSの基本スコア等の判断指標に基づき、一定要件のアップデートについては一律で14日以内の対応を求めています。 また、対応が難しい場合については、一定の代替措置を認めているところです。
488	要求事項・評価基準案	4-4-4-2		「アップデートプログラムがリリースされてから14日以内にアップデートを実施する」という要件は、情報システム部門が限定的な★3事業者にとっては、実務上対応が困難なケースが想定されます。 特に、他業務との兼務や運用リソースの限定など中小規模事業者における事情を踏まえると、14日以内の適用は現実的に厳しい場面が発生し得ると考えます		今回の要求事項・評価基準では、取得希望組織が一律で満たすべきベースラインとしての基準であることを考慮し、一定要件に該当するアップデートについては一律で14日以内の対応を求めています。 また、対応が難しい場合については、一定の代替措置を認めているところです。 いただいた意見については、今後の検討の参考とさせていただきます。
489	要求事項・評価基準案	4-4-4-2		評価基準に記載の【対象】の「-会社支給のパソコンの OS、ブラウザ及びOffice ソフト」を →「 -会社支給のパソコンの OS、デバイスドライバー、ファームウェア、ブラウザ及びOffice ソフト」にした方が良いと思います。		いただいた意見については、今後の検討の参考とさせていただきます。
490	要求事項・評価基準案	4-4-4-3		対象： 中小零細企業の運用実態を踏まえ、「アップデートプログラムがリリースされてから14日以内に、アップデートすること」「仮想パッチ適用」の条件を見直し、設定変更や段階展開等の代替・補完措置を評価対象に明記することを求めます。 ・14日以内のアップデートの一律要求は、中小零細企業では現実的でない場合が多く、検証期間の確保や事業継続上の調整が必要です。 ・「アップデート」「仮想パッチ適用」「ネットワーク分離」「検知機器導入」のみを代替措置として扱うのではなく、設定変更による脆弱性回避（機能無効化・アクセス制御・セグメンテーション・WAF/IPSルールの適用等）を評価基準に含めていただきたいです。実務では設定変更で速やかにリスク低減できるケースが少なくありません。 ・ベンダーのアップデートには新機能追加や挙動変更が含まれることがあり、予期せぬ影響の回避のための検証・動作確認を行った上での適用が望まれます。「14日以内の適用」を一律とすると、検証不十分なままの適用を促す副作用が懸念されます。	・14日以内のアップデートの一律要求は、中小零細企業では現実的でない場合が多く、検証期間の確保や事業継続上の調整が必要です。 ・「アップデート」「仮想パッチ適用」「ネットワーク分離」「検知機器導入」のみを代替措置として扱うのではなく、設定変更による脆弱性回避（機能無効化・アクセス制御・セグメンテーション・WAF/IPSルールの適用等）を評価基準に含めていただきたいです。実務では設定変更で速やかにリスク低減できるケースが少なくありません。 ・ベンダーのアップデートには新機能追加や挙動変更が含まれることがあり、予期せぬ影響の回避のための検証・動作確認を行った上での適用が望まれます。「14日以内の適用」を一律とすると、検証不十分なままの適用を促す副作用が懸念されます。	いただいた意見も参考にしつつ、要求事項・評価基準における該当箇所の修正を検討させていただきます。
491	要求事項・評価基準案	4-4-4-3		4-4-4-2への統合が望ましい	4-4-4-3は例外規定で独立した評価基準にあたらないため	いただいた意見も参考にしつつ、要求事項・評価基準における該当箇所の修正を検討させていただきます。
492	要求事項・評価基準案	4-4-4-3		評価基準 No.4-4-4-2 の基本要求と評価基準 No.4-4-4-3 の代替措置は、一つの評価基準としていただきたい。なお、他の評価基準（No. 4-1-1-2, 4-1-2-2, 4-4-2-1）では、上記のようなケースは一つの評価基準となっています。	評価基準 No.4-4-4-3 の代替措置に適合しているが、評価基準 No.4-4-4-2 の基本要求は不適合というケースが考えられます。 「サプライチェーン強化に向けたセキュリティ対策評価制度に関する制度構築方針(案)P24 3.5 制度における評価スキーム 3.5.3 評価の考え方−評価の有効期間等」では、合格基準は原則、全ての評価基準への適合であり不合格となるため	いただいた意見も参考にしつつ、要求事項・評価基準における該当箇所の修正を検討させていただきます。
493	要求事項・評価基準案	4-4-4-3		脆弱性悪用リスク低減案には、対象となる情報機器内にEDR等を導入し不正な挙動を検知し即時対応できるようにする、という条件を追加いただきたい。		いただいた意見も参考にしつつ、要求事項・評価基準における該当箇所の修正を検討させていただきます。
494	要求事項・評価基準案	4-4-4-3		制度構築方針(案)では、4-4-4-3において「アップデートが実施できない場合には通信の監視等によりリスク低減を図る」旨が記載されています。そのため、本要件については、14日以内にアップデートが困難な状況であっても、適切な監視体制により代替管理が行われていれば、★の取得に影響を及ぼさないという理解でおります。 この点について、制度の正式版でも 代替コントロールの有効性が適切に評価されること を明示いただけると、対象事業者にとって制度がより運用しやすいものとなると考えております。		いただいた意見については、詳細な制度設計等の検討に当たっての参考とさせていただきます。
495	要求事項・評価基準案	4-4-4-3		境界部分の通信監視について、不正な挙動監視とはリアルタイム性が必要なのか。正常時との比較を定期的に行うことも可とするのか。		ここでは、IPS/IDS等の機器により、リアルタイム又はそれに近い頻度で監視することが求められます。
496	要求事項・評価基準案	4-4-5-1		実際の製造現場への理解が不足していると感じます。 製造業の生産設備に付帯してくるPCにおいては、メーカーよりマルウェア対策ソフト導入を禁止しているところがあります。 さらにこのPCを社内ＮＷに接続させたいという要望もかなえる必要があるため、このPCと社内NWの間にUTMを設置し ・必要な通信のみ許可する ・通過するトラフィックにマルウェアや攻撃・不審通信が無いか確認する ・上記についてトラフィックログを取得する という対策を取ることで例外として社内NWへの接続を認めている場合があります。 これら対策を取る事を条件に社内ネットワークへの接続を認めるよう提案いたします。		制度構築方針(案)P.8記載のとおり、製造環境等の制御(OT)システムについては、他の制度・ガイドライン等に基づき対策を行うことを想定しており、本制度としてはスコープ外としています。
497	要求事項・評価基準案	4-4-5-1		OT機器の定義については各社で定めてよいのか。		御認識のとおりです。
498	要求事項・評価基準案	4-4-5-1 ～ 4-4-5-3		マルウェア対策の導入/更新はあるが、EDRの導入基準が不明である。	定義が曖昧で運用差・監査不適合の恐れがある（明確化の必要がある）	いただいた意見については、今後の検討の参考とさせていただきます。
499	要求事項・評価基準案	4-4-5-2		「情報機器に応じたスキャン範囲及び頻度を規定し、スキャンを実行すること」について、ここでは「マルウェアが侵入していないかどうかのマルウェア対策ソフトウェアのスキャン」を指すと考えられますが、単にスキャンとしか書かれていないため、「マルウェアが侵入する隙がないかの脆弱性スキャン」や「既知の脆弱性以外も含めた総合的な環境のスキャン」と誤解される可能性があります。		いただいた意見も参考にしつつ、要求事項・評価基準における該当箇所の修正を検討させていただきます。
500	要求事項・評価基準案	4-4-5-4		不正な Web サイトだけでよいのか。通信先とすべきではないか。		いただいた意見については、今後の検討の参考とさせていただきます。

No.	該当箇所			寄せられた御意見の概要	理由	提出意見に対する考え方
	該当文書	該当ページ又は項番	該当項目			
501	要求事項・評価基準案	4-4-5-4 ～ 4-4-5-5		Webフィルタ/メール検査はあるが、カテゴリ/ルールの定期見直しが不明である。	定義が曖昧で運用差・監査不適合の恐れがある（明確化の必要がある）	いただいた意見については、今後の検討の参考とさせていただきます。
502	要求事項・評価基準案	4-5-1-2		4-3-4-3のように手順"書作成"までせずとも、手順が定まっていればよいのか。またここで定める手順は操作手順を指すのか、関係者連絡含む運用手順を指すのか明記頂きたい。		ここでは運用手順について、何らかの形で定められていれば問題ないと想定しています。
503	要求事項・評価基準案	4-5-1-3		FW/ルータの認証強化はあるが、遠隔管理の無効化/制限の網羅性が不明であるため、管理面はVPN＋MFA経由のみ許可、不要なリモート管理は完全無効化すべきである。	定義が曖昧で運用差・監査不適合の恐れがある（明確化の必要がある）	いただいた意見については、今後の検討の参考とさせていただきます。
504	要求事項・評価基準案	4-5-1-3		ファイアウォール及びルータに係る認証は、No.4-1-3からNo.4-1-6までに定める認証、パスワード設定等に関する基準を満たすことは、管理者IDの削除は不可能ではないか。		いただいた意見も参考にしつつ、要求事項・評価基準における該当箇所の修正を検討させていただきます。
505	要求事項・評価基準案	4-5-1-4		"デフォルトで"の記載が機器の仕様によるものを想定しているのかがわかりづらい。意図するところが"明示的な通信許可以外"を指すのであればそのように明記頂きたい。		いただいた意見も参考にしつつ、要求事項・評価基準における該当箇所の修正を検討させていただきます。
506	要求事項・評価基準案	4-5-1-4		インバウンド遮断デフォルトはあるが、例外ルールのレビュー頻度が不明。	定義が曖昧で運用差・監査不適合の恐れがある（明確化の必要がある）	いただいた意見については、今後の検討の参考とさせていただきます。
507	要求事項・評価基準案	4-5-1-6		不要ルール削除はあるが、変更依頼から適用までの承認/検証プロセスが不明であるため、例外ルールは四半期ごとに棚卸し、未使用は自動無効化を実施すべきである。	定義が曖昧で運用差・監査不適合の恐れがある（明確化の必要がある）	いただいた意見については、今後の検討の参考とさせていただきます。
508	要求事項・評価基準案	4-5-1-7		FWルール変更のMFA/信頼IP制限はあるが、管理プレーンの分離が不明であるため、管理プレーン専用セグメントを設け、到達はジャンプホスト＋MFAのみ許可すべきである。	定義が曖昧で運用差・監査不適合の恐れがある（明確化の必要がある）	いただいた意見については、今後の検討の参考とさせていただきます。
509	要求事項・評価基準案	4-5-1-8		FW有効化はあるが、例外時の代替制御（ネットワークACL等）が不明であるため、例外台帳に代替制御（ACL/セグメント隔離）を記載し、期限付きで是正すべきである。	定義が曖昧で運用差・監査不適合の恐れがある（明確化の必要がある）	いただいた意見については、今後の検討の参考とさせていただきます。
510	要求事項・評価基準案	4-5-1-8		利用中のOSが対応していない場合を除いて、すべてのパソコン及びサーバにおいて、ソフトウェアファイアウォールを有効化することは、サーバーにおいては、ネットワーク機器で対応していることの方が多いが(セグメンテーション)、一律に有効化を求めるのか。		多層防御の観点から、原則として一律で有効化を求めることとしています。
511	要求事項・評価基準案	4-5-1-8		ソフトウェアファイアウォールの導入は不要ポートへの不正アクセスや意図しない外部接続を防ぐ目的と理解しておりますが、要件の実現には周囲のネットワーク機器での対応もありうると考えます。「可能なものについては、」という緩和案を検討いただきたい。	全てのケースでの適用は現実的ではないので	多層防御等の観点から、原則として一律で有効化を求めることとしています。
512	要求事項・評価基準案	4-5-1-9		セグメント化はあるが、横断移動防止の細粒度制御が不明である。	定義が曖昧で運用差・監査不適合の恐れがある（明確化の必要がある）	いただいた意見については、今後の検討の参考とさせていただきます。
513	要求事項・評価基準案	4-5-1-9		当該要件の実現のためには必ずしも専用ネットワークセグメントへの配置が必須ではなく、当該機器へのアクセス制限等で実現が可能と考えます。組織の実態にあわせた緩和案を検討いただきたい。	全てのケースで専用ネットワークの適用は現実的ではないので	いただいた意見については、詳細な制度設計等の検討に当たっての参考とさせていただきます。
514	要求事項・評価基準案	4-5-2-1		★4 の評価として 4-5-2/評価基準 4-5-2-1 では以下が記載されている。 ➢ 社内から不正なサーバへの通信を遮断する仕組みを導入すること。 4-5-2-1 の参考文献は ISO/IEC 27001:2022 A.8.12 であり、4-5-2-1 は情報漏えい抑止観点での評価基準であることから、当該目的は情報漏えい防止を目的とした評価項目である と推察される。当然、その目的(意図)から簡便であれば不正クラウドストレージへのアクセスを遮断するという対策等、厳重であれば情報の機密度に応じた DLP 対策等が必要とされると解される。 一方、要求事項 5-1-1/評価基準 5-1-1-1 では★3 の評価として以下が記載されている。 ➢ 社内外ネットワークの境界又は端末において、インターネットから社内への通信及び社内から不正なサーバへの通信の双方について、不正アクセスをリアルタイム検知・遮断する仕組みを導入すること。 5-1-1-1 の参考文献は ISO/IEC 27001:2022 A.8.16 であり、5-1-1-1 は「社内外ネットワークの境界又は端末」を対象として「IPS/IDS または、マルウェア対策ソフトウェアによるC&C 宛て通信遮断の機能等(不正アクセスをリアルタイム検知・遮断する仕組み)」を実装、運用されていることが求められると解される。 4-5-2-1 と 5-1-1-1 の評価基準は「社内から不正なサーバへの通信を遮断する仕組みを導入」と同様の文言であるが、その目的は別であることが明示されておらず、評価主体が誤認を招く恐れがある。また、その評価基準も具体性を欠く。現時点ではそれを確認、助言するセキュリティ専門家も参考文献を基に釈する以外に手段を有さない。今後、ガイダンス等が整備されることでこの点は解決されるものと推察されるが「★３・★４要求事項及び評価基準」の解釈に別資料を用いなければならない要求事項、評価基準には問題がある。 以上のことから、「★３・★４要求事項及び評価基準」を策定するに当たっては、全般的に要求事項には「目的(意図)」、評価基準には「対象」と「具体策」を明示することを提案する。	「★３・★４要求事項及び評価基準」において、評価主体が誤認を招く恐れがある。また、その評価基準も具体性を欠く。現時点ではそれを確認、助言するセキュリティ専門家も参考文献を基に解釈する以外に手段を有さない。要求事項、評価基準には問題があるため、意見する	制度構築方針(案)P.17記載のとおり、今後要求事項・評価基準に係る評価方法や取組み事例等を具体的に解説する各種ガイダンス資料等を整備する予定です。いただいた意見については、当該ガイダンス資料等の作成に当たっての参考とさせていただきます。
515	要求事項・評価基準案	4-5-2-1		不正なサーバという表現が何を指しているかわかりづらい。		ここではC2サーバ等のサイバー攻撃を指令するサーバやその他の通常アクセスすることが想定されない不審なサーバを想定しています。
516	要求事項・評価基準案	4-5-2-1		社外への不正通信遮断はあるが、DNS/プロキシ/エンドポイントの多層制御が不明である。	定義が曖昧で運用差・監査不適合の恐れがある（明確化の必要がある）	いただいた意見については、今後の検討の参考とさせていただきます。
517	要求事項・評価基準案	4-5-2-1		社内から不正なサーバへの通信を遮断する仕組みを導入することとは、具体的に何を求めているか、ご教示いただきたい。		一般的には、IPSの導入が想定されます。
518	要求事項・評価基準案	4-5-2-1、 5-1-1-1		4-5-2-1と5-1-1-1は同内容であるため、いずれかを削除するか、統合してよいと思われます。		いただいた意見も参考にしつつ、要求事項・評価基準における該当箇所の修正を検討させていただきます。
519	要求事項・評価基準案	5-1-1-1		リアルタイム検知・遮断の仕組みを具体的に示唆していない(監視位置/ログ連携設計が不明である)。	定義が曖昧で運用差・監査不適合の恐れがある（明確化の必要がある）	制度構築方針(案)P.17記載のとおり、今後要求事項・評価基準に係る評価方法や取組み事例等を具体的に解説する各種ガイダンス資料等を整備する予定です。いただいた意見については、当該ガイダンス資料等の作成に当たっての参考とさせていただきます。
520	要求事項・評価基準案	5-1-1-1		アラートの「即時発報」を「可及速やかに発報」と修正する。	即時とはどれくらいのスピードが要求されるのか定義が明確ではないが、メールでの発報を前提にしていると読める。 その場合、すべての検知を即時メールすると一日に数千通もの「メールの洪水」の発生が懸念され、重要な通知を見過ごすおそれがある。 また、UTMと外部のメールサーバーとの連携「SMTPの準備」が課題となる。 そのため、発報について自動メールを前提に即時発報と記載するのではなく、別の方法でも発報できるよう表現を変更した方が良いのではないか。	いただいた意見も参考にしつつ、要求事項・評価基準における該当箇所の修正を検討させていただきます。
521	要求事項・評価基準案	5-1-1-1		不正アクセスをリアルタイム検知・遮断の、不正アクセスとは、不正アクセス禁止法に定める不正アクセスという認識か。具体的にどのような行為を指すか。		認証権限や脆弱性の悪用により、不正に社内ネットワーク等に侵入することを指し、不正アクセス禁止法における不正アクセスと概ね同義です。
522	要求事項・評価基準案	5-1-1-3		「関連したセキュリティ事象の速報レポート」 とありますが、安価なSIEM製品ではデフォルトで用意されたパターンにマッチした場合のみアラートを上げそれを通知する程度が現実的な機能ラインと考えます。 上記アラートを「関連したセキュリティ事象の速報レポート」として扱って良いでしょうか。 認められない場合、より高価なSIEM製品を検討する必要があるため★4に格上げする事を提案いたします。		制度構築方針(案)P.17記載のとおり、今後要求事項・評価基準に係る評価方法や取組み事例等を具体的に解説する各種ガイダンス資料等を整備する予定です。該当箇所については、いただいた意見も参考にしつつ、当該ガイダンス資料等で具体化してまいります。
523	要求事項・評価基準案	5-1-1-3		アラート/速報レポートはあるが、24/7体制やエスカレーション基準が不明である。	定義が曖昧で運用差・監査不適合の恐れがある（明確化の必要がある）	いただいた意見については、今後の検討の参考とさせていただきます。
524	要求事項・評価基準案	5-1-1-3		関連したセキュリティ事象の速報レポートが作成され、通知されることとは、どこに通知されることを想定しているか		機器の管理者やネットワークを監視する組織等に通知されることを想定しています。
525	要求事項・評価基準案	5-1-2-1		許可ソフト一覧はあるが、デバイス別差異と自動配布が不明である。	定義が曖昧で運用差・監査不適合の恐れがある（明確化の必要がある）	いただいた意見については、今後の検討の参考とさせていただきます。
526	要求事項・評価基準案	5-1-2-2		自由インストール禁止はあるが、ローカル管理者権限の付与基準/監査が不明である。	定義が曖昧で運用差・監査不適合の恐れがある（明確化の必要がある）	いただいた意見については、今後の検討の参考とさせていただきます。
527	要求事項・評価基準案	5-1-2-3		ソフトインストール状況の年1回点検は頻度不足の恐れ。	定義が曖昧で運用差・監査不適合の恐れがある（明確化の必要がある）	今回の要求事項・評価基準では、取得希望組織が一律で満たすべきベースラインとしての基準であることを考慮し、最低限年1回、点検を行うこととしています。各取得希望組織の任意の取り組みとして、それ以上の頻度等で点検を行うことは否定されるものではありません。
528	要求事項・評価基準案	5-1-2-4		外部ファイルの安全性確認はあるが、サンドボックスの適用範囲/例外規定が不明である。	定義が曖昧で運用差・監査不適合の恐れがある（明確化の必要がある）	制度構築方針(案)P.17記載のとおり、今後要求事項・評価基準に係る評価方法や取組み事例等を具体的に解説する各種ガイダンス資料等を整備する予定です。いただいた意見については、当該ガイダンス資料等の作成に当たっての参考とさせていただきます。
529	要求事項・評価基準案	5-2-1-1		インシデント対象範囲/レベルの定義はあるが、事業影響評価指標（RTO/RPO等）が不明である。	定義が曖昧で運用差・監査不適合の恐れがある（明確化の必要がある）	制度構築方針(案)P.17記載のとおり、今後要求事項・評価基準に係る評価方法や取組み事例等を具体的に解説する各種ガイダンス資料等を整備する予定です。いただいた意見については、当該ガイダンス資料等の作成に当たっての参考とさせていただきます。
530	要求事項・評価基準案	5-2-1-2		4-4-3-3で検出した不正認証に対してもインシデント判定を行う必要があるのではないか。		いただいた意見も参考にしつつ、要求事項・評価基準における該当箇所の修正を検討させていただきます。
531	要求事項・評価基準案	5-2-1-2		アラート分析の責任者判断はあるが、二次レビュー/品質管理が不明である。	定義が曖昧で運用差・監査不適合の恐れがある（明確化の必要がある）	いただいた意見については、今後の検討の参考とさせていただきます。

No.	該当箇所			寄せられた御意見の概要	理由	提出意見に対する考え方
	該当文書	該当ページ又は項番	該当項目			
532	要求事項・評価基準案	6-1-1-		評価基準 No.6-1-1-3 および No.6-1-1-4 について、 セキュリティインシデント発生時に自社のみで対応できない場合を想定し、あらかじめ外部の専門事業者（フォレンジック調査、インシデント対応支援等）の委託先選定や連携体制を整備しておく旨を明確にした方が良いと考える。 具体的には、インシデント発生後に初めて委託先を検討・選定するのではなく、平時から委託先候補を選定し、連絡・依頼が可能な状態にしておくことを評価の観点として追記することを検討してはどうか。	サイバーセキュリティインシデント発生時には、初動対応の遅れが被害拡大や事業停止期間の長期化につながることが多い。 特に、自社内に十分な専門人材や対応体制を有していない企業においては、インシデント発生後に外部委託先の検討・契約を行うことで、対応開始までに相当の時間を要するケースが少なくない。 あらかじめ外部の専門事業者を選定し、必要に応じて迅速に支援を要請できる体制を整備しておくことで、インシデント対応の実効性が高まり、被害の最小化および早期復旧につながると考えられる。 そのため、インシデント対応体制の整備を求める本評価基準において、自社対応が困難な場合の外部委託体制の事前整備についても、評価の観点として明示することが有効である。	制度構築方針(案)P.17記載のとおり、今後要求事項・評価基準に係る評価方法や取組み事例等を具体的に解説する各種ガイダンス資料等を整備する予定です。いただいた意見については、当該ガイダンス資料等の作成に当たっての参考とさせていただきます。
533	要求事項・評価基準案	6-1-1-2		IR手順（①～⑤）はあるが、コミュニケーション計画/法規制報告の詳細が不明である。	定義が曖昧で運用差・監査不適合の恐れがある（明確化の必要がある）	今回の要求事項・評価基準では、取得希望組織が一律で満たすべきベースラインとしての基準であることを考慮し、最低限インシデント対応手順に含めるべき内容を定めています。取得希望組織の任意の取組として、これ以外の事項を含めることは、否定されるものではありません。
534	要求事項・評価基準案	6-1-1-2		6-1-1-1と6-1-1-2は統合してよいと思われます。		いただいた意見も参考にしつつ、要求事項・評価基準における該当箇所の修正を検討させていただきます。
535	要求事項・評価基準案	6-1-1-3		セキュリティインシデントの基準については5-2-1-1で定義されているもので問題ないか。		御認識のとおりです。なお、要求事項・評価基準として重複している箇所については、御意見も参考にして修正を検討させていただきます。
536	要求事項・評価基準案	6-1-1-3		連絡手段の冗長化（電話/メール/メッセージ等）が不明である。	定義が曖昧で運用差・監査不適合の恐れがある（明確化の必要がある）	No.7-1-1-2(★4)のとおり、必要に応じて電話、FAX等の様々な連絡手段における連絡先を整備するコトヲ想定しています。
537	要求事項・評価基準案	6-1-1-5		IR体制の年1回点検はあるが、重大インシデント後の事後レビュー/是正の反映が不明である。	定義が曖昧で運用差・監査不適合の恐れがある（明確化の必要がある）	いただいた意見については、今後の検討の参考とさせていただきます。
538	要求事項・評価基準案	6-1-1-6		報告フォーマットのメタデータ（時刻/影響/対応状況）の標準化が不明である。	定義が曖昧で運用差・監査不適合の恐れがある（明確化の必要がある）	制度構築方針(案)P.17記載のとおり、今後要求事項・評価基準に係る評価方法や取組み事例等を具体的に解説する各種ガイダンス資料等を整備する予定です。いただいた意見については、当該ガイダンス資料等の作成に当たっての参考とさせていただきます。
539	要求事項・評価基準案	6-1-1-7		事例共有はあるが、ナレッジベースの検索性/アクセス権が不明である。	定義が曖昧で運用差・監査不適合の恐れがある（明確化の必要がある）	いただいた意見については、今後の検討の参考とさせていただきます。
540	要求事項・評価基準案	6-1-1-7		「インシデント事例及びその対応策を社内部署へ共有していること」とありますが、単に「共有」することを求めるのではなく、「同様の事例が発生することを防ぐために対策を行う」ことも含めて要求すべきと思われます。		いただいた意見については、今後の検討の参考とさせていただきます。
541	要求事項・評価基準案	7-1-1-1		評価基準に「事業継続上重要なシステム」が含まれている。一方、「事業継続上重要なシステムの把握」が大分類「3 リスクの特定」の要求事項/評価基準には含まれていない。 評価基準に「事業継続上重要なシステム」を明記するのであれば、「事業継続上重要なシステム」を識別(ID)の「3 リスクの特定」において「事業継続上重要なシステム」を識別すべきと考えられる。 一般的に「NIST Cyber Security Framework(CSF)」(「統治」があるため 2.0 と認識)に対応した 6つ機能を採用するとあるが、「資産管理カテゴリの ID.AM-02」に「組織が管理するソフトウェア、サービス、及びシステムのインベントリ（一覧）が維持されている。」とあり、システムの一覧を整備することについての事項が記述されている。このことから、「★３・★４要求事項及び評価基準」では、CSF(2.0)の6機能を活用しつつもカテゴリ、サブカテゴリといった体系までは意識されておらず、フレームワークの整合性自体にひずみが生じ、結果として構造的な問題に直結していると推察される。 併せて、「サプライチェーン強化に向けたセキュリティ対策評価制度に関する制度構築方針(案)」26 ページの「3.7 国内外の関連制度等との連携・整合」に記載の相互補完に必須とされるのは体系づけ(フレームワーク化)された要求事項に基づく、明確かつ具体的な評価基準の存在が必須である。 以上のことから、「★３・★４要求事項及び評価基準」を策定するに当たっては、全般的に網羅性を以て CSF2.0 の機能、カテゴリ、サブカテゴリといった観点に基づく検討を行い、検討の結果についてそのカテゴリ、サブカテゴリの採用/不採用を明示すること、独自の要求事項および評価基準を追加した場合は、独自であることを明記する等、「体系(フレームワークとマッピング)を意識」して策定することを提案する。 なお、本提案は先行する仕組みや国際基準である ISMS 適合性評価制度等との相互補完的な制度として本制度を発展させることを目指す点と何ら矛盾しないと考えられる。	「★３・★４要求事項及び評価基準」では、CSF(2.0)の 6 機能を活用しつつもカテゴリ、サブカテゴリといった体系までは意識されておらず、フレームワークの整合性自体にひずみが生じ、結果として構造的な問題に直結していると推察されるため、意見する。	いただいた意見については、関連制度等との連携・整合の検討に当たっての参考とさせていただきます。
542	要求事項・評価基準案	7-1-1-1		目標復旧レベル設定はあるが、業務継続の代替手段整備が不明である。	定義が曖昧で運用差・監査不適合の恐れがある（明確化の必要がある）	制度構築方針(案)P.17記載のとおり、今後要求事項・評価基準に係る評価方法や取組み事例等を具体的に解説する各種ガイダンス資料等を整備する予定です。いただいた意見については、当該ガイダンス資料等の作成に当たっての参考とさせていただきます。
543	要求事項・評価基準案	7-1-1-2		復旧準備（バックアップ/トランザクションログ/リストア検証）はあるが、検証頻度/合格基準が不明である。	定義が曖昧で運用差・監査不適合の恐れがある（明確化の必要がある）	制度構築方針(案)P.17記載のとおり、今後要求事項・評価基準に係る評価方法や取組み事例等を具体的に解説する各種ガイダンス資料等を整備する予定です。いただいた意見については、当該ガイダンス資料等の作成に当たっての参考とさせていただきます。
544	要求事項・評価基準案	7-1-1-2		既存システムにおいて、求められる復旧時間で復元できることの確認は実機で実施することは、現実的ではないケースがあるため、机上確認を可とするなどの緩和案を検討いただきたい。	全てのケースでの適用は現実的ではないの	制度構築方針(案)P.17記載のとおり、今後要求事項・評価基準に係る評価方法や取組み事例等を具体的に解説する各種ガイダンス資料等を整備する予定です。いただいた意見については、当該ガイダンス資料等の作成に当たっての参考とさせていただきます。
545	要求事項・評価基準案	全般		（意見内容） 総じてチェック項目が拡充された点は評価できるが、チェックの粒度や判断基準があいまいな項目が見受けられる。 実効性のある対策が実施されているかが確認されず、形式的なチェックにとどまることで制度が形骸化することが強く懸念される。		制度構築方針(案)P.17記載のとおり、今後要求事項・評価基準に係る評価方法や取組み事例等を具体的に解説する各種ガイダンス資料等を整備する予定です。いただいた意見については、当該ガイダンス資料等の作成に当たっての参考とさせていただきます。
546	要求事項・評価基準案	全般		1年以上の頻度で点検する対象が大半かと思われ、1-4-1-1と同様に集約できるのではないか。		実証での各参画企業からの意見を踏まえ、参照しやすさを考慮して、評価基準を分割しています。
547	要求事項・評価基準案	全般		★5でも構わないが所有ドメインに関するルールをスコープとして検討いただきたい。		いただいた意見については、今後の検討の参考とさせていただきます。
548	要求事項・評価基準案	全般		以下の評価基準を追加することを提案します。 ・組織やサプライチェーンの攻撃対象領域（アタックサーフェス）を定期的に調査し、攻撃される前に脆弱なアセットを特定し改善する。 ・リスクに基づいてユーザー,サービス,ハードウェアを定期的に再認証する(ゼロトラストアーキテクチャなど) ・改ざん不可なバックアップ（イミュータブルバックアップ）を複数世代に渡り保管すること。 ・バックアップが侵害されていないか等の正常性を確認可能な機能、もしくは確認手順を完備する事 ・LOTL（Living off the land）や内部不正など潜在的に有害な事象を発見するために、振る舞い検知等より人員の活動とテクノロジーの使用を監視すること。	・とりわけMITRE AttackにおいてResource DevelopmentのMitigationとしてはPre-Compromizeのみであることから対策として追加が望ましいと考えます。 ・高度化する攻撃に対するリスク最小化施策として、NIST CSF2.0にも記載されているゼロトラストアーキテクチャの追加が望ましいと考えます。 ・設備故障や障害時のバックアップとセキュリティのため（ランサムウエア対策）のバックアップは明確に異なり、追加が望ましいと考えます。 ・現状はマルウエアレス攻撃が大半を占めている理解です。ユーザーやシステム管理者を装う事でセンサーを回避する攻撃も増加していることから追加が望ましいと考えます。	いただいた意見については、今後の検討の参考とさせていただきます。
549	要求事項・評価基準案	全般		別添★３・★４要求事項及び評価基準案の「評価基準」項目は、達成の条件であり、具体的なスケールになっていないため、各項目に対する基準を定める必要がある。	各項目に人によって解釈が異なる内容になっているため、スケール要素の判断基準を定まる必要がある	制度構築方針(案)P.17記載のとおり、今後要求事項・評価基準に係る評価方法や取組み事例等を具体的に解説する各種ガイダンス資料等を整備する予定です。いただいた意見については、当該ガイダンス資料等の作成に当たっての参考とさせていただきます。
550	要求事項・評価基準案	全般		「評価基準」の個々の項目に細かな指摘をしますが、判断がブレない全体的なガイドラインで取りまとめる必要がある。	各項目の評価基準のスケールを定めたガイドラインを用意する必要がある	制度構築方針(案)P.17記載のとおり、今後要求事項・評価基準に係る評価方法や取組み事例等を具体的に解説する各種ガイダンス資料等を整備する予定です。いただいた意見については、当該ガイダンス資料等の作成に当たっての参考とさせていただきます。
551	要求事項・評価基準案	全般		取引先管理においては、対象をどこにするのかについては読み違えや意見の違いなどが起きやすい。例えばクラウドサービスは対象にするのか、など。 2-1-1-1では取引先のことを 「自社以外の組織(顧客・子会社・関係会社・クラウドサービス提供者を含む取引先)」 としており、明確である。 一方、それ以外のNoでは、どこまで対象なのか、もしくは省いてしまってよいという意思表示なのかがわかりにくい。 2-1-1-3、2-1-2-1では、「自社の機密情報を共有している取引先」としているが、これには、2-1-1-1で言及している、子会社・関係会社クラウドサービス提供者はあえて省いているのかどうか。（それでよい） 同様に2-1-3-1では、「以下に示す条件のいずれか若しくは複数に該当する子会社又は取引先」としているが、関係会社クラウドサービス提供者は含まれないのか。（クラウドサービス提供者の対策状況は変化しうるところであり、自社にも影響が出る可能性があるところであるため、Webサイト上での確認等の簡易な対策状況の把握はあってもよいと考える）		いただいた意見も参考にしつつ、要求事項・評価基準における該当箇所の修正を検討させていただきます。
552	要求事項・評価基準案	全般		別添★３・★４要求事項及び評価基準案 について、社内で活用するにあたり、PDF版だけではなく、Excel版もご提供いただけますと幸いです。		以下のページにて、既にExcel版の要求事項・評価基準を提供済みとなっています。 https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_seido/wg_supply_chain/20251226_report.html
553	要求事項・評価基準案	全般		評価基準や要求事項の変更時は最低6か月以上の周知期間の確保を制度として明記してください。	利用企業が予算化・体制調整・調達を計画的に進められるよう、十分なリードタイムが必要です。 周知期間が確保されれば、拙速な対応による品質低下や業務影響を避け、持続的なセキュリティ向上につながります。	いただいた意見については、今後の検討の参考とさせていただきます。
554	要求事項・評価基準案	全般		中間報告版で付与されていた★3No、★4No項目を追加いただきたい	対象者が★3、★4それぞれの取得を目指すにあたって、対応が必要な項目として分かりやすい表現であったため	要求事項・評価基準の参照しやすさを考慮し、それぞれに一意の番号を付与しています。なお、★3・★4それぞれの要求事項・評価基準については、Excelファイル上のソート機能等により、抽出することが可能となっています。
555	要求事項・評価基準案	全般		「別添★３・★４要求事項及び評価基準案」について、評価基準No.2-1-3-1の「重要な機密情報」、No.4-1-3-2「重要な情報」、No.4-1-3-5「重要情報」の定義はありますでしょうか（※「重要情報」のみ複数の評価基準に記載あり）。評価基準No.2-1-2-1では「機密情報」の定義や取扱いは自社・取引先間で取り交わすとされておりますが、上記の「重要な～情報」についても取得希望組織の判断に委ねられるものですか。その場合、「重要さ」の判断基準はございますでしょうか。各組織で恣意的に定義可能となりますと、評価の客観性が損なわれる懸念がございます。		制度構築方針(案)P.17記載のとおり、今後要求事項・評価基準を具体的に解説する各種ガイダンス資料等を整備する予定です。いただいた意見については、当該ガイダンス資料等の作成に当たっての参考とさせていただきます。
556	要求事項・評価基準案	全般		近年の大企業での被害事例を踏まえ、外部接続機器対策やEDR導入に加えて*侵入後の拡大防止（ネットワーク分離・権限管理）と復旧（バックアップ/リストア訓練・RTO/RPO）等、業務停止を抑える項目を要求事項・評価基準に追加（または必須化）していただきたい。	一般的対策を講じていても侵入後の横展開や暗号化で業務影響が生じ得るため、検知だけでなく封じ込め・復旧まで含めて評価しないと実効性が担保できない。	いただいた意見については、今後の検討の参考とさせていただきます。

No.	該当箇所			寄せられた御意見の概要	理由	提出意見に対する考え方
	該当文書	該当ページ又は項番	該当項目			
557	要求事項・評価基準案	全般		クラウドサービスにおける対策が、認証とログ取得についてしか書かれておらず、不十分であるように思われます。接続元IPアドレスによるアクセス制御や、公開範囲などの適切な設定についても言及すべきでないでしょうか。		いただいた意見については、今後の検討の参考とさせていただきます。
558	要求事項・評価基準案	全般		評価基準の語尾が「文書化すること」「一覧化すること」といった具体的手段の表現から、「定めること」という表現に統一されている点について、目的が達成されていれば手段は問わない、という理解で差し支えないか確認したい。	評価基準の意図が明確になることで、「過度に形式的な対応」「不要な文書作成」を避け、実効性重視の運用につながると考えるため。	御認識のとおりです。
559	要求事項・評価基準案	全般		自工会GL85-89に該当する項目について、SCS制度においても、少なくとも部分的には要求事項を整備すべきと考えます。 USBやHDD/SSD等、データ保存媒体そのものに対する物理的アクセス制御に関する要件（規定化・監視等）は、データやソフトウェアの管理以上に重要です。関連する既存の要件（例えば規定の整備やデータ暗号化の義務づけ、インシデント発生時の態勢整備）だけでは、実体的には大きな攻撃界面を残すことに繋がります。つまり、物理的アクセス制御が欠落することにより、他の要件を形式的に充足していても致命的な侵害事象が発生しうるものと捉えます。 侵害事象の例としては、勤務時間外に不法侵入者が忍び込んでPCに未知のUSBデバイスを挿入する、非正規のPC修理業者がHDD/SSD内部に不正プログラムを導入する、監視カメラのない部屋においてサーバー管理者が離席時に他のスタッフが自由に出入りできる等が想定されます。これらの事象が発生した場合、インシデントの発生に繋がることは否定できません。 情報セキュリティ水準の底上げを促進する制度の趣旨からして、こうした侵害事象を確実に防止するための要求項目を整備すべきではないでしょうか。 ※物理的な筐体のセキュリティ(PCの開封防止機構・盗難防止ケーブル等)については、現時点の基準（☆4以下)については必須ではないものと捉えております。		本制度の要求事項・評価基準では自工会・部工会ガイドラインNo.85～89の内容について、No.87を除きそれぞれ同程度の内容を規定しています。 いただいた意見については、今後の検討の参考とさせていただきます。
560	要求事項・評価基準案	全般		評価基準の更新：継続的な対策と状況変化に対応するためには、当制度におけるセキュリティ要求事項・評価基準なども一定の期間で改訂し続けていく必要がある。★取得組織にとっても影響が大きいため、セキュリティ脅威の高まりを見つつ、制度運用において改訂スケジュールを一定程度事前に公開していくことを検討いただきたい。		いただいた意見については、詳細な制度設計等の検討に当たっての参考とさせていただきます。
561	要求事項・評価基準案	全般		意見内容: 要求事項の「参照文献」欄において、NISTやISO 27001に加え、「ISMAP管理基準」との対応関係（マッピング）を明記することを提言いたします。	本制度はサプライチェーン全体の強化を目的としており、その中核を担うクラウドサービス事業者（CSP）の参加と協力が不可欠です。多くのCSPが準拠しているISMAP基準との整合性を公式に示すことで、ISMAP取得企業が本制度への適合状況を容易に判断できるようになり、制度の円滑な導入と普及促進に大きく寄与します。	いただいた意見については、関連制度等との連携・整合の検討に当たっての参考とさせていただきます。
562	要求事項・評価基準案	全般		O列の参照文献は、評価基準単位になっていますが、ほとんどは、要求事項単位で同じ内容でした。要求事項の右横の列に、要求事項単位での参照文献も示していただけると理解しやすくなると思いました。		いただいた意見については、今後の検討の参考とさせていただきます。
563	要求事項・評価基準案	全般		参照文献にCSF2.0のカテゴリ、サブカテゴリ―を追加いただくと利用しやすいと思いました。現状では、機能単位のみのため。		いただいた意見については、今後の検討の参考とさせていただきます。
564	要求事項・評価基準案	全般		原案では受注者の対策チェックシートとして「要求事項」「評価基準」「参照文献」「NIST CSFにおける機能」のらんとなっていますが、まだ最終のものではないかもしれませんが、実際に使用する場合は、かもしれませんが、 「セキュリティ要件適合評価及びラベリング制度（JC-STAR）の「★1（レベル1）チェックリスト」の欄居合わせたほうがよいと思います。 すなわち、JC-STARでは「セキュリティ要件」、「適合基準」、「評価結果」、「エビデンスの名称」、「エビデンスに基づく根拠」となっています。。	「エビデンスの名称」、「エビデンスに基づく根拠」がないと自己適合宣言の場合、安易に適合していると報告してしまう可能性が否めない。	いただいた意見については、自己評価実施時の証跡の取り扱いの検討に当たっての参考とさせていただきます。
565	要求事項・評価基準案	全般		サプライチェーンに関するチェック項目が少ないように思います。 例えば 販売、原材料調達、配送、決済機能等を事故発生に部分的に遮断できること 上流システムと下流システムが事故発生時分離できること 上流システムと下流システムそれぞれのシステム責任者と連絡先を共有しておくこと 高付加時にシステムがダウンしないようにサプライチェーン全体で対策をとること 発注者が守るべきことを明確にし、発注者に伝えること システムメンテナンスはサプライチェーン全体への影響を配慮して計画すること	サプライチェーンに重点を置いた評価制度とするため。	いただいた意見については、今後の検討の参考とさせていただきます。
566	要求事項・評価基準案	全般		★3（全企業向けベースライン）の要求事項が ISO/IEC 27001:2022 の管理策を広範に踏襲しており、「最低限の基礎的対策」という制度趣旨に比して負荷が大きい。特に中小企業にとっては ISMS の簡易版に近く、変化の激しいサイバーリスクに対する柔軟性やレジリエンス（復旧・適応）要素が十分に組み込まれていない。制度目的が「底上げ」である以上、より軽量でリスクベースの基準に再設計することが望ましい。	★3・★4要求事項案は ISO/IEC 27001:2022 の管理策（A.5 系）を広範に参照しているため、ベースラインとしては負荷が大きい。	いただいた意見については、今後の検討の参考とさせていただきます。
567	要求事項・評価基準案	全般		NIST Cybersecurity Framework (CSF) 2.0との整合性について、★3・★4は GV（ガバナンス）、ID（識別）、PR（防御）、DE（検知）、RS（対応）の一部には対応しているが、RC（復旧）機能に該当する要求事項がほぼ存在しない。CSF2.0 は「攻撃を前提としたレジリエンス」を中核に据えており、復旧・事業継続・教訓反映を含む体系的なレジリエンス能力の評価が不可欠である。	NIST CSF 2.0 は Identify–Protect–Detect–Respond–Recover の5機能を要求するが、制度案には Recover に該当する要求事項が確認できない。	いただいた意見については、今後の検討の参考とさせていただきます。
568	要求事項・評価基準案	全般		CSF2.0 のガバナンス（GV）が求める「レジリエンスとしてのガバナンス」が制度案から欠落している。具体的には、①レジリエンス目標（復旧時間等）の設定、②レジリエンス能力の評価・改善、③インシデント後の教訓反映、④サプライチェーン全体での共同復旧・共同演習、⑤レジリエンスの有効性に関する経営層の監督といった要素が制度案には含まれていない。これらは国際的に必須とされる要素であり、制度の実効性確保のためにも追加が必要である。	CSF2.0 の GV.RR（Risk & Resilience Management）、GV.OV（Oversight）等に相当するレジリエンスガバナンスが制度案に存在しない。	いただいた意見については、今後の検討の参考とさせていただきます。
569	要求事項・評価基準案	全般		「サプライチェーン強化に向けたセキュリティ対策評価制度に関する制度構築方針(案)」9ページの「適用範囲の考え方-適用範囲に含むもの-1.IT基盤」に「エンドポイント機器」が明示された点は範囲の明確化として高く評価できる。一方、要求事項および評価基準案では、「エンドポイント機器」が「情報機器」、「パソコン」、「スマートデバイス」、「端末」といった名称で表記されており、「用語の不統一」が生じている。なお、「エンドポイント機器」のみならず、他の資産においても同様に「用語の不統一」が散見される。 このことから「★３・★４要求事項及び評価基準案」において用語が厳密に定義されておらず、判定に主観が入り込む余地が大きく要求事項や評価基準の解釈の揺れが生じる懸念がある。 用語が厳密に定義されていない「★３・★４要求事項及び評価基準」で運用が開始された場合、評価者、セキュリティ専門家において認識齟齬が生じ、結果として本制度の評価に係る客観性や適切性、評価結果の再現性が損なわれる懸念が払しょくできない。 以上のことから、「★３・★４要求事項及び評価基準」を策定するに当たっては、用語定義も併せて実施することを提案する。なお、評価対象となる資産の用語定義例として「CIS Controls v8.1.2」の「Asset Classes」を挙げる。	「★３・★４要求事項及び評価基準案」において用語が厳密に定義されておらず、判定に主観が入り込む余地が大きく要求事項や評価基準の解釈の揺れが生じる懸念があるため、意見する。	制度構築方針(案)P.17記載のとおり、今後要求事項・評価基準を具体的に解説する各種ガイダンス資料等を整備する予定です。いただいた意見については、当該ガイダンス資料等の作成に当たっての参考とさせていただきます。