「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）」に対する意見

2026年1月23日

一般社団法人　日本貿易会
情報システム委員会

近年のサイバー攻撃増加を受け、サプライチェーン全体の対策強化と可視化を目的に、経済産業省及び内閣官房国家サイバー統括室は運用体制案、セキュリティ評価基準等を盛り込んだ制度構築方針（案）を作成した。
経済産業省商務情報政策局が2025年12月26日、「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構築に向けた制度構築方針（案）」に関するパブリックコメントを募集したことを受け、情報システム委員会は2026年1月23日付で意見を提出した。

本制度については、サプライチェーン全体のセキュリティ水準向上やチェック項目の標準化・負担軽減という「方向性」には賛同。特に中小企業にとっては評価制度と支援策を組み合わせることで効果が大きいとの声もある。
一方で、信頼性確保・適用範囲の整理・責任とコストの公平な分担・要求内容の明確化が不十分な状況にて、この案をベースとしつつも改めて業界等にもう少しヒアリングし、実態に則したものにすべきではとの考えの下、以下の意見を提出する。

	該当案	該当箇所	意見内容	理由
1			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。
2			本コメントは、親会社の情報システム部門として、グローバルに展開する関係会社群に対しセキュリティ統制施策を実施する立場から提出する。 当社は世界各地域に数百社規模の関係会社を抱えており、統制対象として管理しており、統制施策としてNIST CSF 2.0を基盤とした自主回答型アンケートを年次で展開・回収し、各社の対策水準把握と改善のPDCAを運用している。 当該アンケートの業務プロセスに経産省「★3」制度の要件を統合し、アンケート回答内容を星3準拠判定へ接続することで、統制施策の効用を高めたいと考える。 【意見内容】 ・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。 ・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
3			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。
4			★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。

5			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。
6			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。
7			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。
8			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。
9	制度構築方針（案）	全体	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。	
10	制度構築方針（案）	全体	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。	
11	制度構築方針（案）	全体	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）	
12	制度構築方針（案）	全体	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。	
13	制度構築方針（案）	全体	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。
14	制度構築方針（案）	全体	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。	

15	制度構築方針（案）	p.8	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。
16	制度構築方針（案）	p.8	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。
17	制度構築方針（案）	p.9	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。
18	制度構築方針（案）	p.9	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。
19	制度構築方針（案）	p.9	「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。
20	制度構築方針（案）	p.12	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。
21	制度構築方針（案）	p.13	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。
22	制度構築方針（案）	p.13	★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。

23	制度構築方針（案）	p.13	【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。	
24	制度構築方針（案）	p.13	【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。	
25	制度構築方針（案）	p.17,19	★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。
26	制度構築方針（案）	p.18	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。
27	制度構築方針（案）	p.18	★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。
28	制度構築方針（案）	p.24	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。
29	制度構築方針（案）	p.26	「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。
30	制度構築方針（案）	p.26	「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。

31	評価基準案		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。
32	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。	
33	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。	
34	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。	
35	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。	
36	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。	
37	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。	
38	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？	
39	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。	
40	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。	
41	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。	
42	評価基準案	3-1-1-1, 3-1-1-2等	適用範囲内とは何か、ご教示いただきたい。	
43	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。	
44	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。	
45	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。	

46	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。	
47	評価基準案	4-1-1-2	やむを得ず共有ID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のか。 (※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)	
48	評価基準案	4-1-2-2	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)	
49	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。	
50	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。	
51	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。	
52	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。	
53	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。	
54	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。	
55	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。	
56	評価基準案	4-4-1-1	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。	
57	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。	
58	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。	
59	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。	

60	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。	
61	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。	
62	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。	
63	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。	
64	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。	
65	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。	