経済産業省

国家サイバー統括室
National Cybersecurity Office

「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）」及び「★３・★４要求事項・評価基準（案）」に対するパブリックコメントへの対応について

令和８年３月

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

事務局

パブリックコメントの実施概要・主な御意見

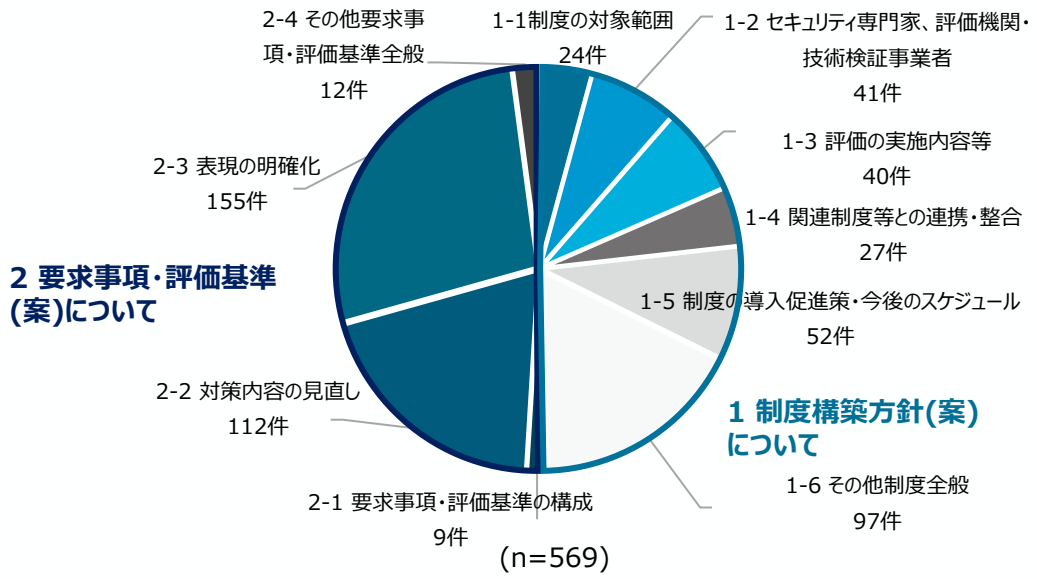
- 「サプライチェーン強化に向けたセキュリティ対策評価制度に関する制度構築方針（案）」及び「★３・★４要求事項・評価基準（案）」について、意見公募（パブリックコメント）を実施し、93件の御意見を受領。
- 頂いた御意見を踏まえ、記載内容の補足や具体化、表現の修正等の観点から記載の内容の修正を行った。

結果の概要

実施期間	令和7年12月26日～令和8年1月24日
意見数	93件（意見の内容ごとに細分化すると569件）
主な御意見のカテゴリ	1 制度構築方針(案)について -1 制度の対象範囲について -2 セキュリティ専門家、評価機関・技術検証事業者について -3 評価の実施内容等について -4 国内外の関連制度等との連携・整合について -5 制度の導入促進策・今後のスケジュールについて -6 その他制度全般について 2 要求事項・評価基準(案)について -1 要求事項・評価基準の構成について -2 対策内容の見直しについて -3 表現の明確化について -4 その他要求事項・評価基準全般

意見の分類・内容

- ✓ 意見の半数以上が「要求事項・評価基準(案)」に対するものであり、またその多くはエディトリアルな修正を求めるものや解釈の確認を求めるものであった。
- ✓ 「制度構築方針(案)」に対しては、評価スキームに対する意見のほか、制度の導入促進策に対する要望が多く上がった。



（参考）パブリックコメントの実施概要・主な御意見　(1/2)

頂いた御意見のカテゴリ		該当箇所	頂いた主な御意見(例)	御意見への対応の考え方
1 制度構築方針(案)について	1-1 制度の対象範囲について	制度構築方針 P.9	• 以下についても、適用範囲に含めるべきである。 - スタンドアロン機器も評価に含めるべきである。 - サポート期限切れのソフトウェア等	• 制度の対象範囲(制度構築方針P.8、9)について、御意見を踏まえ、考え方を再度整理し修正。
	1-2 セキュリティ専門家、評価機関・技術検証事業者について	制度構築方針 P.20	• セキュリティ専門家の要件として、以下の資格も追加を検討すべき。 - 公認情報セキュリティ主任監査人 - 情報セキュリティ監査人補 - ISO審査員 - ISO審査員補 - システム監査技術者　等	• 既に規定している資格と同等以上と考えられる資格(公認情報セキュリティ主任監査人)については含まれることがわかるように追記。 • その他の資格については、今後の検討の参考とさせていただく。
		制度構築方針 P.21	• 評価機関・技術検証事業者の要件として、「脆弱性診断サービス」に加えて、以下についても追加を検討すべき。 - 情報セキュリティ監査サービス - ペネトレーションテスト（侵入試験）	• 「ペネトレーションテスト（侵入試験）」については、情報セキュリティサービス基準上、既に規定している「脆弱性診断サービス」の提供を前提としたサービスであるため、含まれることがわかるように追記。
	1-3 評価の実施内容等について	制度構築方針 P.23	• 評価結果の不適合時の是正報告期間について、起算日を明確にすべきではないか。	• 評価結果の不適合時の是正報告期間について、起算日を「評価機関からの指摘事項の通知日」に修正。
	1-4 国内外の関連制度等との連携・整合について	制度構築方針 P.26	• ISMS、ISMAP等の他の認証制度等と相互認証(部分認証を含む。)を実施してほしい。	• 国内外の関連制度等との連携・整合に係る検討や推進の参考とさせていただく。
	1-5 制度の導入促進策・今後のスケジュールについて	制度構築方針 P.34-36	• ★取得に関して補助金の導入や税制優遇等を検討してほしい。 • お助け隊サービス(新類型)について、地域・提供者による品質ばらつきを抑制するよう、対策を講じるべきである。	• 今後の制度の導入促進策等に係る検討や推進の参考とさせていただく。
		制度構築方針 P.39	• 制度に係るガイダンス資料の公表時期を示してほしい。	• 御意見を踏まえ、今後のスケジュールを更新。
	1-6 その他制度全般について	ー	• 制度開始時に十分なセキュリティ専門家・評価機関の数を確保してほしい。 • ★取得申請時のフォーマットを整備してほしい。	• 今後の制度の詳細設計等に当たっての参考とさせていただく。

（参考）パブリックコメントの実施概要・主な御意見　(2/2)

頂いた御意見のカテゴリ		該当箇所	頂いた主な御意見(例)	御意見への対応の考え方
2 要求事項・評価基準(案)について	2-1 要求事項・評価基準の構成について	評価基準 No.3-1-5-1	• 3-1-5-1(リモートワークで使用する情報機器に関するルールの策定及び周知)については、他の要求事項・評価基準と平仄を合わせて策定要件と周知要件に分離すべきではないか。	• 御意見を踏まえ、3-1-5-1(ルール策定)と3-1-5-2(ルール周知)に評価基準を分割。
		評価基準 No.4-1-4-1	• 4-1-4-1(端末へのログオンに関するルール)と4-1-4-2(例外措置)は統合し、一つの評価基準とすべきではないか。	• 御意見を踏まえ、一つの評価基準に統合するなど、構成を一部見直し。
		評価基準 No.4-4-4-2	• 4-4-4-2(アップロード適用に関するルール)と4-4-4-3(例外措置)は統合し、一つの評価基準とすべきではないか。	
	2-2 対策内容の見直しについて	評価基準 No.4-4-4-3	• 脆弱性悪用リスク低減策には、対象端末へのEDR導入も追加すべきではないか。	• 御意見を踏まえ、アップデート適用を期限内に完了できない際の脆弱性悪用リスク低減策として、対象端末へのEDR導入も追加
	2-3 表現の明確化について	評価基準 No.3-1-3-2	• 「外部情報サービスの接続先」について、「外部情報サービスが通信する相手」を指すのか「サービス提供事業者」を指すのかわかりくい。	• 御意見を踏まえ、「外部情報サービスの提供事業者」を指すことがわかるように、表現を修正
		評価基準 No.4-1-3-5	• 他の要求事項・評価基準を引用する際には、具体的なNo.を示し、引用先を明確化すべきである。	• 御意見を踏まえ、具体的な評価基準No.を適示するように修正。
		評価基準 No.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…」とあるが、マルウェア対策ソフトのスキャンに係る評価基準である旨を明確化すべきではないか。	• 御意見を踏まえ、マルウェア対策ソフトのスキャンに係る評価基準であることがわかるように、表現を修正
		ー	• 要求事項・評価基準における用語の定義を明確にすべきではないか。	• 今後、要求事項・評価基準に係る用語集を整備させていただく。
	2-4 その他	評価基準 No.4-4-4-3	• 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ほしい	• 今後の制度の詳細設計等に当たっての参考とさせていただく。

（参考）主な変更点について新旧の対照（1/4）

頂いた御意見のカテゴリ		該当箇所	意見の概要	修正箇所	
				旧	新
1 制度構築方針(案)について	1-1 制度の対象範囲について	制度構築方針 P.9	• スタンドアロン機器も評価に含めるべきである。 • サポート期限切れのソフトウェア等について適用範囲に含めるべきではないか。	◆適用範囲に含むもの 1.及び2. (略) 3.その他 • 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) ◆適用範囲に含めないもの • 製造環境等の制御(OT)システム (例：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) • 発注元等に提供する製品等、自社のIT基盤に係るネットワークに接続していない機器 ◆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 • 本制度の要求事項を満たすことが困難なIT機器やソフトウェア(例：サポート期限切れのソフトウェア等) ※ 本事由により適用範囲から除外する場合は、具体的に除外理由を明記し、セキュリティ専門家(★3)又は評価機関(★4)は妥当性を評価すること	◆適用範囲に含むもの 1.及び2. (略) ◆適用範囲に含めないもの • 製造環境等の制御(OT)システム (例：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) • 発注元等に販売する製品等、取得希望組織の管理・運用下にない機器 ◆その他 • 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)

（参考）主な変更点について新旧の対照（2/4）

頂いた御意見のカテゴリ		該当箇所	意見の概要	修正箇所	
				旧	新
1 制度構築方針(案)について	1-2 セキュリティ専門家、評価機関・技術検証事業者について	制度構築方針 P.20	• セキュリティ専門家の要件として、ISO審査員、ISO審査員補や公認情報セキュリティ主任監査人、情報セキュリティ監査人補などは含まれないのか。 • 他の資格(例:システム監査技術者)に含めるべきではないか。	<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> - 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	<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> - 情報処理安全確保支援士 - 公認情報セキュリティ監査人 ※公認情報セキュリティ主任監査人を含む。 - CISSP - CISM - CISA - ISO27001　主任審査員
		制度構築方針 P.21	• 「情報セキュリティ監査サービス」や「ペネトレーションテスト（侵入試験）」を評価機関の要件に含めるべきではないか。	<★4 技術検証を行うために満たすべき要件> 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 *2「情報セキュリティサービス基準第 4.1 版」	<★4 技術検証を行うために満たすべき要件> 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*2)登録要件*3を満たすこと *2「ペネトレーションテスト（侵入試験）サービス」を含む。 *3「情報セキュリティサービス基準第 4.1 版」
	1-3 評価の実施内容等について	制度構築方針 P.23	• 評価結果の不適合時の是正報告期間について、起算日を明確にすべきではないか。	<不適合の指摘及び改善 - ★4> 不適合事項の是正報告を、指摘時から一定期間内(例：評価機関による実地審査等実施日から1か月以内)に提出し、内容について了承を得られれば★4を取得可能	<不適合の指摘及び改善 - ★4> 不適合事項の是正報告を、指摘時から一定期間内(例:評価機関からの指摘事項が通知されてから1ヶ月以内)に提出し、内容について了承を得られれば★4を取得可能
	1-5 制度の導入促進策・今後のスケジュールについて	制度構築方針 P.39	• 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。 • 制度に係るガイダンス資料の公表時期を示してほしい	評価用ガイド、制度規程、評価機関等の公表時期について、スケジュールに追記	

（参考）主な変更点について新旧の対照（3/4）

頂いた御意見のカテゴリ		該当箇所	意見の概要	修正箇所	
				旧	新
2 要求事項・評価基準(案)について	2-1 要求事項・評価基準の構成について	評価基準 No.3-1-5-1	• 3-1-5-1(リモートワークで使用する情報機器に関するルールの策定及び周知)については、他の要求事項・評価基準と平仄を合わせて策定要件と周知要件に分離すべきではないか。	• リモートワークを実施する場合は、リモートワークで使用する情報機器及び機密情報の条件について、以下の事項に関するルールを定め、リモートワークを行う全ての役員、従業員、派遣社員及び受入出向者に対して周知すること。 - (略)	• リモートワークを実施する場合は、リモートワークで使用する情報機器及び機密情報の条件について、以下の事項に関するルールを定めること。 - (略) • No.3-1-5-1で定めたルールをリモートワークを行う全ての役員、従業員、派遣社員及び受入出向者に対して周知すること。
		評価基準 No.4-1-4-1	• 4-1-4-1(端末へのログオンに関するルール)と4-1-4-2(例外措置)は統合し、一つの評価基準とすべきではないか。	• 業務で利用するシステムを構成する端末へのログオン(パソコンへのログオン及びスマートデバイスのロック解除)にあたって、設定が可能な場合、以下のいずれかを適用すること。 - (略)	• 業務で利用するシステムを構成する端末へのログオン(パソコンへのログオン及びスマートデバイスのロック解除)にあたって、設定が可能な場合、以下のいずれかを適用すること。 - (略) • 上記で示す要件のいずれも設定することができない場合、No.4-1-5で求められるよりも強度の高いパスワードを用いる等の代替策を用いること。
		評価基準 No.4-1-4-2		• No.4-1-4-1で示す要件のいずれも設定することができない場合、No.4-1-5で求められるよりも強度の高いパスワードを用いる等の代替策を用いること。	(4-1-4-1へ統合)

（参考）主な変更点について新旧の対照（4/4）

頂いた御意見のカテゴリ		該当箇所	意見の概要	修正箇所	
				旧	新
2 要求事項・評価基準(案)について	2-2 対策内容の見直しについて	評価基準 No.4-4-4-3	• 脆弱性悪用リスク低減策には、対象端末へのEDR導入も追加すべきではないか。	• 以下のいずれかに該当する場合、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。 - (略) • やむを得ず上記のとおりアップデートができない場合(例えば、動作検証に一定期間を要し、期限内にアップデートが完了しない場合)は、アップデート適用までの間、以下のいずれかにより脆弱性悪用のリスクを低減する対策を実施すること。 - (略) - 対象となる情報機器と適用範囲内のネットワークとの境界部分に、通信を監視して不正な挙動を検知する機器を導入すること。	• 以下のいずれかに該当する場合、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。 - (略) • ・やむを得ず上記のとおりアップデートができない場合(例えば、動作検証に一定期間を要し、期限内にアップデートが完了しない場合)は、アップデート適用までの間、以下のいずれかにより脆弱性悪用のリスクを低減する対策を実施すること。 - (略) - 対象となる情報機器と適用範囲内のネットワークとの通信を監視し、当該脆弱性を悪用する不正な通信を遮断する機器又はソフトウェアを導入すること。
	2-3 表現の明確化について	評価基準 No.3-1-3-2	• 「外部情報サービスの接続先」について、「外部情報サービスが通信する相手」を指すのか「サービス提供事業者」を指すのかわかりくい。	• 外部情報サービスの接続先と機密情報の取扱いについて取り交わすこと。	• 外部情報サービスの提供事業者と機密情報の取扱いについて取り交わすこと。
		評価基準 No.4-1-3-5	• 他の要求事項・評価基準を引用する際には、具体的なNo.を示し、引用先を明確化すべきである。	• ★3で対象としているクラウドサービスへのアクセスに加えて、以下に示す場合は、常に多要素認証を使用すること。 - (略)	• No.4-1-3-2で対象としているクラウドサービスへのアクセスに加えて、以下に示す場合は、常に多要素認証を使用すること。 • - (略)
		評価基準 No.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…」とあるが、マルウェア対策ソフトのスキャンに係る評価基準である旨を明確化すべきではないか。	• 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。	• 情報機器に応じたマルウェア対策ソフトの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。

METI
Ministry of Economy, Trade and Industry

経済産業省のサイバーセキュリティ政策ウェブページはこちら⇒
https://www.meti.go.jp/policy/netsecurity/index.html