

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（SCS 評価制度）
技術検証事業者指定基準

2026 年 9 月 11 日

SCS 評価制度 制度運営機関

目次

第1章	総則	3
1.1	適用	3
1.2	用語定義	3
1.2.1	★4 登録希望組織	3
1.2.2	★4 要求事項及び評価基準	3
1.2.3	脆弱性診断サービス	4
1.2.4	脆弱性診断	4
1.2.5	診断データ	4
1.2.6	委託元評価機関	4
1.2.7	サービスリスト	4
1.2.8	トップマネジメント	4
1.2.9	技術検証品質マネジメントシステム	4
1.2.10	マネジメントレビュー	4
1.3	引用基準等	5
1.4	優先関係	5
第2章	組織要件	5
2.1	技術検証事業者の責任	5
2.2	技術検証事業者の体制	6
2.3	品質管理	6
2.3.1	品質管理者の割当	6
2.3.2	品質管理マニュアルの整備	6
2.3.3	品質の維持及び向上に関する手続等の導入	6
2.3.4	情報セキュリティサービス基準の活用	7
2.4	内部監査	7
2.5	マネジメントレビュー	8
2.6	技術検証結果の一貫性の確保	8
2.7	公平性	8
2.8	公平性確保のための仕組み	9
2.9	適用範囲の限定	10
2.10	外部委託	10
2.11	秘密保持	10
2.12	苦情及び問い合わせの処理	11
2.13	内部規程及び文書の整備	12
第3章	技術検証要員要件	13
3.1	専門性を有する者の配置	13
3.2	技術検証要員	14
第4章	技術検証業務要件	14
4.1	技術検証の実施及び責任に関する要件	14
4.2	技術検証の実施	14
4.3	技術検証の合意	16
4.4	技術検証の結果	16
4.5	技術検証結果報告書の撤回及び訂正	17
4.6	★4 技術検証責任者の欠員等の報告	17
4.7	情報の提供	18

第1章 総則

1.1 適用

本基準は、技術検証事業者指定規則の規定に基づき、技術検証事業者の指定を受けようとする者及び指定を受けた技術検証事業者が満たさなければならない要件を定める。

技術検証事業者は、評価機関の委託により技術検証を実施するものであり、第三者評価の最終的な責任は評価機関に帰属する。

技術検証結果報告書の内容に関する苦情及び問い合わせは、本基準 2.12 に従い技術検証事業者が受け付ける。

評価機関が自ら技術検証を行う場合においては、当該評価機関は、技術検証事業者として本基準に定める責任を負うものとし、本基準中「委託元評価機関」とあるのは「当該評価機関」と読み替えるものとする。ただし、次に掲げる規定については、それぞれ次に定めるところによる。

- ① 2.10①（外部委託に係る委託元評価機関の事前の承諾）は、適用しない。この場合において、技術検証に係る業務の一部を外部委託するときは、評価機関指定基準 2.11 の定めるところによる。
- ② 4.2④ただし書中「委託元評価機関が」とあるのは、「当該評価機関の★4 評価責任者が」と読み替える。
- ③ 4.3（技術検証の合意）は、適用しない。この場合において、当該評価機関は、4.3 各号に掲げる事項（診断データの保管、消去の方法及び時期を含む。）を内部規程に定めなければならない。
- ④ 4.5②及び 4.6 のうち委託元評価機関への通知に係る部分は、適用しない。制度運営機関への通知については、この限りでない。
- ⑤ 2.12①に規定する苦情及び問い合わせの受付窓口は、当該評価機関が評価機関指定基準2.13に基づき整備する手続と一体のものとして設けることができる。

1.2 用語定義

本基準で用いる用語の定義は、本項以下に定めるもののほか、基本規程に定めるところによる。

1.2.1 ★4 登録希望組織

基本規程 2.1.9 に規定する登録希望組織のうち、★4 の登録を受けることを目的とするものをいう。また、基本規程 2.1.10 に規定する登録組織のうち★4 の登録を受けたものを「★4 登録組織」という。

1.2.2 ★4 要求事項及び評価基準

基本規程 2.2.12 に規定する★3 及び★4 要求事項及び評価基準のうち、★4 に係る

ものをいう。

1.2.3 脆弱性診断サービス

情報セキュリティサービス基準第1章2(3)の定義による。

1.2.4 脆弱性診断

基本規程 1.3.19 に定める「脆弱性診断」（登録希望組織が保有する機器に対し、脆弱性の有無を診断することをいう。）をいう。

この場合において、「機器」には、基本規程 1.3.26 に定める IT 基盤を構成する各 IT 資産並びにこれらに付随し、又はこれらを構成するソフトウェア、ファームウェア及び設定情報を含むものとし、診断の対象となる具体的な範囲及び実施項目は、
★4 技術検証ガイドの定めるところによる。

なお、1.2.3 に規定する「脆弱性診断サービス」と本項に規定する「脆弱性診断」とは異なる。

1.2.5 診断データ

技術検証の実施の過程で取得され、又は生成された情報のうち、検出された脆弱性の内容、その再現手順、診断に用いたツールの出力その他の診断ログ及び対象システムの構成に関する情報をいう。

1.2.6 委託元評価機関

評価機関指定基準 4.5③の規定により技術検証事業者に技術検証を委託した評価機関をいう。

1.2.7 サービスリスト

経済産業省が策定した情報セキュリティサービス基準への適合性について審査登録機関の審査を受けた者を掲載する情報セキュリティサービス基準適合サービスリストをいう。本基準において、サービスリストに「掲載されている」とは、脆弱性診断サービス区分又はペネトレーションテスト（侵入試験）サービス区分において、有効期限内で掲載されていることをいう。

1.2.8 トップマネジメント

最高位で技術検証事業者を指揮し、及び管理する個人又は人々の集まりをいう。技術検証事業者が法人の一部の組織である場合は、当該組織を指揮し、及び管理する権限並びに当該組織に資源を提供する権限を有する者をいう。

1.2.9 技術検証品質マネジメントシステム

技術検証の品質に関する方針及び目標並びにその目標を達成するためのプロセスを確立するための、相互に関連し、又は相互に作用する技術検証事業者の一連の要素をいう。

1.2.10 マネジメントレビュー

トップマネジメントが行う、技術検証品質マネジメントシステムの適切性、妥当性及び有効性の評価及び見直しをいう。

1.3 引用基準等

次に掲げる規程等は、本基準で引用される限りにおいて、本基準の一部を構成する。ただし、基本規程及び技術検証事業者指定規則は、本基準の上位に位置する文書であり、本基準とこれらの文書との関係は、1.4に定めるところによる。

- ① 基本規程
- ② 評価機関指定基準
- ③ 技術検証事業者指定規則
- ④ 技術検証事業者指定手順
- ⑤ ★4 技術検証ガイド
- ⑥ ★4 要求事項及び評価基準
- ⑦ 情報セキュリティサービス基準
- ⑧ 情報セキュリティサービスにおける技術及び品質の確保に資する取組の例示（以下「例示」という。）

1.4 優先関係

本制度における文書の上下関係は、基本規程、技術検証事業者指定規則、本基準、技術検証事業者指定手順、その他 1.3⑤～⑧に掲げる引用文書の順とする。本基準とこれらの文書の内容が抵触する場合は、この順に優先して適用する。ただし、同一の事項について上位の文書が下位の文書に委任している場合には、当該下位の文書の定めを優先して適用する。

なお、診断データの取扱いについては、4.2④から⑥まで及び 2.11③の定めが、本基準の他の規定並びに技術検証事業者指定規則及び基本規程を除く 1.3④～⑧に掲げる引用文書の定めに優先して適用される。

第2章 組織要件

2.1 技術検証事業者の責任

技術検証事業者は、公平性を確保して技術検証を実施することができるよう、自らの組織体制を整備し、及び運営しなければならない。また、技術検証事業者は、基本規程 2.2 に定める本制度における規程等に従い、その業務を遂行するための方針及び手順を定め、運用しなければならない。

技術検証事業者は、技術検証に関わる要員の責任及び権限を示す組織構造を文書化しなければならない。

2.2 技術検証事業者の体制

技術検証事業者は、その技術検証の業務内容に信頼を与える組織運営機構を備えなければならない。技術検証事業者は、次に掲げる事項を満たさなければならない。

- ① 日本の法令に基づき設立された法人であること。
- ② 技術検証を的確に実施するため、少なくとも第 3 章に定める要員の配置又は確保並びに 2.3 から 2.6 までに定める品質管理の仕組みを有し、これを運用していること。
- ③ ★4 登録希望組織に対する技術検証の委託の受任から技術検証結果報告書の交付に至る一連の活動（以下「技術検証に係る業務」という。）について責任を負うこと。法人の一部の組織が技術検証に係る業務を行う場合においても、当該法人が当該責任を負うことが、定款、内部規程その他の文書により明確にされていること。
- ④ 技術検証事業者指定規則 2.1.2 各号のいずれにも該当しない者であること。
- ⑤ 制度運営機関が行う調査（技術検証事業者指定規則 4.2.1 に規定する定期サーベイランス及び同 4.2.2 に規定する臨時サーベイランスを含む。）を受け入れ、その求めに応じて必要な資料を提出すること。ただし、診断データ（1.2.5 に規定する診断データをいう。）を含む資料の提出を求められた場合には、4.2④ から⑥まで及び 2.11③に従い、当該診断データを提出してはならない。

2.3 品質管理

技術検証事業者は、次に掲げる要件を満たす品質管理を行わなければならない。

2.3.1 品質管理者の割当

品質の維持及び向上のため、技術検証の品質の管理に関する品質管理者を割り当てていること。ただし、当該品質管理者が専属して技術検証の品質の管理を行うことを必ずしも求めるものではない。

2.3.2 品質管理マニュアルの整備

品質の維持及び向上のため、次に掲げる事項を含む技術検証の品質の管理のためのマニュアルを整備すること。

- ① 技術検証提供プロセスの管理
- ② 技術検証の成果物（技術検証結果報告書その他の技術検証の結果として作成される文書をいう。）の作成、交付及び管理

2.3.3 品質の維持及び向上に関する手続等の導入

品質の維持及び向上のため、次の手続等を行っていること。

技術検証を行った案件について、当該案件の技術検証に従事していない者であって、当該技術検証の内容を理解するために必要な専門的知識及び経験を有する者が、技術検証の実施計画（対象範囲、手法及び実施時期を含む。）及び技術検証結果報告

書についてのレビューを行っていること。この場合において、レビューを行う者は、当該技術検証事業者に所属する者であることを要しない。当該技術検証事業者に所属しない者にレビューを行わせる場合は、2.7③、2.10 及び 2.11 の定めるところによる。レビューの結果及び必要な是正措置を記録すること。

2.3.4 情報セキュリティサービス基準の活用

技術検証事業者に対する次に掲げる要件の充足の確認は、サービスリストへの掲載の有無に応じ、本項の定めるところによる。確認の具体的な方法は、技術検証事業者指定手順の定めるところによる。

- ① 技術検証事業者がサービスリストに掲載されている場合は、3.1①(ア)a、2.3.1 から 2.3.3 まで、3.2②に規定する要件について、当該掲載により担保されている範囲において、確認を簡素化することができる。
- ② 技術検証事業者がサービスリストに掲載されていない場合は、情報セキュリティサービス基準第3章2-1に定める脆弱性診断サービスに係る審査基準と同等の能力を有することについて、次に掲げる事項の確認を受けなければならない。
 - (ア) 専門性を有する者の在籍 (3.1①(ア)に規定する要件をいう。)
 - (イ) サービス仕様の明示 (★4 技術検証ガイドに定める技術検証の実施項目及び実施手順並びに脆弱性診断の結果の取扱い又は同等のものに従って脆弱性診断を行うことを、あらかじめ明らかにしていることをいう。)
 - (ウ) 品質管理者の割当 (2.3.1 に規定する要件をいう。)
 - (エ) 品質管理マニュアルの整備 (2.3.2 に規定する要件をいう。)
 - (オ) 品質の維持及び向上に関する手続等の導入 (2.3.3、3.2②及び 2.4 末段に規定する要件をいう。)
- ③ ①及び②にかかわらず、次に掲げる要件は、サービスリストへの掲載の有無にかかわらず満たさなければならず、かつ、その確認を簡素化しない。
 - (ア) 3.1①(ア)に規定する★4 技術検証責任者の雇用及び配置
 - (イ) 3.1①(ウ)及び3.1②(イ)に規定する IPA が提供する研修の受講
 - (ウ) 2.11①に規定する顧客の情報を保護するための手続の設置及び運用並びに 2.4 末段に規定する当該手続の検証
 - (エ) ②(イ)に規定するサービス仕様の明示のうち、★4 技術検証ガイドに定める技術検証の実施項目及び実施手順に従って脆弱性診断を行うことを明らかにしている部分
- ④ 技術検証事業者は、指定を受けた後にサービスリストへの掲載が有効でなくなったときは、遅滞なくその旨を制度運営機関に届け出るとともに、②各号に掲げる事項の確認を受けなければならない。この場合の手続は、技術検証事業者指定手順の定めるところによる。

2.4 内部監査

技術検証事業者は、技術検証品質マネジメントシステムが実施され、かつ、有効であることを検証するために、計画的かつ体系的な方法ですべての手順について年 1 回以上内部監査を実施しなければならない。ただし、新規に指定を受けた技術検証事業者にあつては、最初の内部監査は、指定を受けた日から 1 年を経過する日まで実施しなければならない。また、技術検証事業者は、次に掲げる事項を実施しなければならない。

- ① 技術検証事業者のトップマネジメントに対して監査結果を通知すること。
 - ② 技術検証事業者のトップマネジメントは、適時かつ適切に是正措置を実施すること。
 - ③ 監査結果を、作成した日から 3 年間以上保管すること。ただし、当該期間の満了の日が指定の有効期間の満了の前となる場合は、当該有効期間の満了の日まで保管すること。
- 2.11①に規定する情報を保護するための手続については、本項に定める内部監査において、当該手続に係る技術検証に従事した者以外の者により年 1 回以上検証すること（又はこれと同等の外部監査により年 1 回以上検証すること）により、その実効性を確保しなければならない。

2.5 マネジメントレビュー

技術検証事業者のトップマネジメントは、技術検証品質マネジメントシステムが本基準の要求事項を満たし、かつ、継続して適切、妥当かつ有効であることを確実にするため、年 1 回以上、これを評価し、及び見直さなければならない。ただし、新規に指定を受けた技術検証事業者にあつては、最初のマネジメントレビューは、指定を受けた日から 1 年を経過する日までに実施しなければならない。

技術検証事業者は、マネジメントレビューの検討項目に、次に掲げる事項を含めなければならない。また、技術検証事業者は、マネジメントレビューの結果を、作成した日から 3 年間以上保管しなければならない。ただし、当該期間の満了の日が指定の有効期間の満了の前となる場合は、当該有効期間の満了の日まで保管しなければならない。

- ① 技術検証業務の内容
- ② 技術検証業務の実施結果
- ③ 苦情及び問い合わせの内容
- ④ 法律及び制度の変更、運営審議委員会及び指定委員会の要望その他重要な外部要因の有無とその影響
- ⑤ 内部監査の結果

2.6 技術検証結果の一貫性の確保

技術検証事業者は、★4 技術検証責任者が複数在籍する場合には、★4 技術検証責任者の判断のばらつきを把握し、及び是正するための手続を整備し、運用しなければならない。当該手続には、事例共有、相互レビューその他必要な措置を含む。

2.7 公平性

- ① 技術検証事業者は、技術検証を公平に行わなければならない。
- ② 技術検証事業者は、公平性の確保に関する規程を定め、これを運用しなければならない。

ならない。公平性を確保するための具体的な仕組みの水準については、各技術検証事業者が自らの状況に応じて定めるものとする。ただし、当該仕組みには、少なくとも 2.8 各号に掲げる事項を含めなければならない。

- ③ 技術検証事業者は、次のいずれかに該当する場合、当該★4 登録希望組織の技術検証を行ってはならない。
 - (ア) ★4 技術検証責任者又は★4 技術検証責任者の監督の下で技術検証に従事する者（以下「★4 技術検証従事者」という。）が★4 登録希望組織の従業員、取締役又は経営判断に影響を与える株主である場合
 - (イ) ★4 技術検証責任者又は★4 技術検証従事者が★4 登録希望組織に対して経営判断に影響を与える財務的な利害（出資又は投資等）を有している場合
 - (ウ) ★4 技術検証責任者又は★4 技術検証従事者の家族が★4 登録希望組織の取締役又は経営判断に影響を与える株主である場合
 - (エ) 技術検証事業者が★4 登録希望組織を所有している、又は★4 登録希望組織が技術検証事業者を所有している場合又は一方が他方の経営方針、事業運営若しくは意思決定に実質的な影響を及ぼし得る場合
 - (オ) ★4 技術検証責任者又は★4 技術検証従事者が★4 登録希望組織の評価対象となるシステム運用に携わる者と同一人物である場合
 - (カ) ★4 技術検証責任者又は★4 技術検証従事者が、当該技術検証の受任日から起算して過去 3 年以内に、★4 登録希望組織に対して構築支援、運用支援、セキュリティ対策の実装その他利害関係を生じ得る業務を提供し、又は同組織に雇用されていた場合
- ④ 技術検証事業者は、自ら又はその親会社、子会社、関連会社その他密接な関係を有する者が、★4 登録希望組織に対して構築支援、運用支援、セキュリティ対策の実装その他利害関係を生じ得る業務を提供している場合について、公平性への影響を評価し、必要な措置を講じなければならない。

2.8 公平性確保のための仕組み

技術検証事業者は、2.7②に基づき定める公平性の確保に関する規程及びその運用により、公平性を確保するための仕組みを整備し、運用しなければならない。

技術検証事業者は、当該仕組み（規程及び運用）に、少なくとも次に掲げる事項を含めなければならない。

- ① 利害関係の申告
- ② 利害関係者の技術検証案件からの除外
- ③ 公平性リスクの定期的な評価
- ④ 公平性に関する記録
- ⑤ 公平性に関する責任者又は委員会

技術検証事業者は、技術検証の実施に先立ち、技術検証の公平性に影響を及ぼすおそれのある利害関係を特定し、その影響を評価するとともに、必要な回避又は低減措置を講じ、その結果を記録しなければならない。

2.9 適用範囲の限定

本制度における技術検証は、当面の間、脆弱性診断サービスに係る業務として実施するものとし、本基準が技術検証事業者に求める要員要件及び品質管理要件は、当該業務に適用する。

技術検証事業者は、★4 技術検証ガイドに定める技術検証の対象となる評価基準について、同ガイドに定める判定基準に従い、適合又は不適合の判定を行う。技術検証の対象とならない要求事項及び評価基準への適合性の判断並びに第三者評価の結論（★4 要求事項及び評価基準の全体としての適合の判断及び評価報告書の作成をいう。）は、評価機関が行う。

2.10 外部委託

- ① 技術検証事業者は、委託元評価機関の書面による事前の承諾を得た場合を除き、技術検証に係る業務を第三者に外部委託してはならない。この場合において、技術検証の判定に直接関与する業務は外部委託してはならない。また、脆弱性診断の実施に係る業務を外部委託する場合にあっては、委託先は本制度の技術検証事業者の指定を受けた者でなければならない。
- ② 前号の承諾を得て外部委託を行う場合においても、技術検証事業者は、外部委託を受けた者が行った委託に基づく行為について、当該者による本基準の遵守を含め、最終的な責任を負わなければならない。この場合において、技術検証事業者は、外部委託を受けた者に対し、2.7、2.8、2.11 並びに 4.2④から⑥までに規定する事項を遵守させなければならない。
- ③ 技術検証事業者は、外部委託に当たり、委託範囲、責任分界、秘密保持、記録の作成及び保存並びに技術検証事業者への提供その他必要な事項を、契約その他の文書により明確にしなければならない。
- ④ 技術検証事業者は、外部委託の有無及びその内容を記録し、委託元評価機関の求めに応じて提示しなければならない。
- ⑤ 技術検証事業者は、外部委託を受けた者の能力、適格性及び本基準への適合状況を定期的に確認しなければならない。

2.11 秘密保持

- ① 技術検証事業者は、技術検証に係る業務を通じて得られた又は生じたすべての情報（対象システムの脆弱性に関する情報を含む。）について、顧客の情報を保護するための手続を設け、運用しなければならない。なお、当該手続の実効

性は 2.4 に従い検証するものとする。

- ② 技術検証事業者は、前号の情報のうち、当該情報に係る★4 登録希望組織又は委託元評価機関が公開している情報及び公開に同意している情報を除き、秘密情報とし、その管理について、責任を負わなければならない。ただし、基本規程 6.1 各号のいずれかに該当する情報については、この限りでない。
- ③ 前号ただし書の規定にかかわらず、診断データについては、法令に基づく開示の請求又は裁判所その他の権限のある機関の命令による場合を除き、第三者に開示してはならない。ただし、委託元評価機関及び★4 登録希望組織の同意に基づき、当該★4 登録希望組織に対して診断データを提供する場合は、この限りでない。この場合において、技術検証事業者は、提供の日時、相手方、提供した範囲及び同意を確認した方法を記録しなければならない。また、法令等に基づき開示した場合は、開示の日時、相手方、開示した範囲及び根拠となる法令の規定を記録し、遅滞なく委託元評価機関及び制度運営機関に通知しなければならない。
- ④ 技術検証事業者は、委託元評価機関に対する技術検証結果の提供その他業務上正当な理由がある場合又は当該★4 登録希望組織の同意がある場合を除き、秘密情報を開示してはならない。
- ⑤ 技術検証事業者は、★4 登録希望組織以外（例えば、苦情を申し出た者又は規制当局）から得られた当該★4 登録希望組織に関する情報を、秘密として取り扱わなければならない。
- ⑥ 技術検証事業者は、情報保護管理者を割り当てなければならない。

2.12 苦情及び問い合わせの処理

- ① 技術検証事業者は、委託元評価機関及び★4 登録希望組織からの苦情及び問い合わせを受け付ける窓口を設置し、これを受領し、処理し、その経過を追跡できる手続を有していなければならない。
- ② 技術検証事業者は、当該技術検証の受任日から起算して過去 3 年以内に当該★4 登録希望組織に対して構築支援、運用支援、セキュリティ対策の実装その他利害関係を生じ得る業務を提供し、又は同組織に雇用された要員を、当該組織に係る苦情又は問い合わせの解決のレビュー又は承認に従事させてはならない。
- ③ 技術検証事業者は、苦情又は問い合わせを受領したときは、遅滞なくその旨を苦情又は問い合わせを行った者に通知し、処理の結果及び終了を苦情又は問い合わせを行った者に通知しなければならない。
- ④ 技術検証事業者は、苦情又は問い合わせの内容、対応経過及び結論を記録し、4.2③に定める期間、保管しなければならない。

2.13 内部規程及び文書の整備

技術検証事業者は、次に掲げる事項を定めた内部規程を整備し、並びに次に掲げる文書を整備しなければならない。

① 内部規程に定めるべき事項

- (ア) 技術検証に係る業務の実施体制及び意思決定の責任範囲並びに法人の一部の組織が当該業務を行う場合における当該法人の責任
- (イ) ★4 技術検証ガイドに基づく技術検証の実施プロセス並びに結果の判定及び判断基準
- (ウ) 委託元評価機関からの委託の受任、技術検証の実施、レビュー及び結果の通知並びに技術検証結果報告書の様式その他の技術検証の実施に係る具体的手続
- (エ) 委託元評価機関との合意において定めるべき事項
- (オ) 技術検証結果報告書の撤回及び訂正に関する手続
- (カ) 技術検証の結果の文書化並びに技術検証実施記録及び診断データの管理（保管期間、消去の手続並びにその記録の作成を含む。詳細は 4.2 に定めるところによる。）並びに秘密保持、正確性及び完全性の確保。
- (キ) 業務上取得する情報の管理区分及び取扱方法並びに情報保護水準の維持及び向上のための管理措置
- (ク) 技術検証に従事する者の教育、研修及び資格管理
- (ケ) ★4 技術検証責任者が複数在籍する場合における判断のばらつきの把握及び是正の手続
- (コ) 外部委託を行う場合における委託元評価機関の事前の承諾の取得、外部委託の記録及び外部委託を受けた者に対する管理（詳細は 2.10 に定めるところによる。）
- (サ) 委託元評価機関及び★4 登録希望組織からの苦情及び問い合わせの受付窓口の設置並びにこれらの受領、処理及び追跡に関する手続並びに利害関係を有する要員を当該案件のレビュー又は承認に従事させないための措置
- (シ) 制度運営機関が行う調査への対応に関する手続
- (ス) 内部監査及びマネジメントレビューの実施に関する手続（実施の頻度、監査結果の通知、是正措置及び記録の保管を含む。）

② 整備すべき文書

- (ア) 品質管理マニュアル
- (イ) 情報保護（顧客情報保護手続）に関する手続書
- (ウ) 公平性の確保に関する規程
- (エ) 技術検証の実施手順書
- (オ) 技術検証に関わる要員の責任及び権限を示す組織構造を文書化したもの
- (カ) 技術検証実施記録及び診断データの管理（保管期間、消去の手続及びその記録の作成を含む。）に関する文書

第3章 技術検証要員要件

3.1 専門性を有する者の配置

技術検証事業者は、次に掲げる要員要件に該当するものであること。

① ★4 技術検証責任者

(ア) 技術検証事業者は、技術検証の品質確保のため、技術検証に従事する要員のうち、次のいずれかの要件を満たす者を★4 技術検証責任者として 1 名以上雇用し、自らが行う技術検証における責任者として配置しなければならない。

- a 例示 1-2-1 に定める資格又は同等のものを有する者
- b 例示 2-1 に定める専門家コミュニティ又は同等のものにおける講師若しくはリーダーの経験又は高等教育機関における脆弱性診断の技術を対象とする講師経験を有する者
- c 次のいずれかの事業において申請日（更新申請の場合にあつては、更新申請日）から起算して過去 3 年以内に合計で 5 件（契約件数。包括的な契約の場合は 1 年間分で 1 件とみなす。）以上の実績（診断方法は問わない。）を有する者
 - ・ Web アプリケーション脆弱性診断
 - ・ プラットフォーム脆弱性診断
 - ・ スマートフォン／タブレット端末アプリケーション脆弱性診断
 - ・ その他ソフトウェア、システムの脆弱性対策を目的とした診断又はテスト
- d 例示 3-1 に定める研修又は同等のものを修了している者

(イ) 技術検証事業者は、★4 技術検証ガイドに定める技術検証を適切に実施するために必要な知識及び実務能力を有する★4 技術検証責任者に、技術検証に従事する者及び成果物に対する監督を行わせ、技術検証結果報告書の品質について責任を負わせなければならない。

(ウ) 技術検証事業者は、★4 技術検証責任者に対し、IPA が提供する研修を受講させなければならない。

② ★4 技術検証従事者

(ア) 技術検証事業者は、★4 技術検証責任者の監督の下で技術検証に従事する者（★4 技術検証従事者）を配置することができる。

(イ) ★4 技術検証従事者を配置する場合、技術検証事業者は、★4 技術検証従事者に対し、IPA が提供する研修を受講させなければならない。

(ウ) 技術検証事業者は、★4 技術検証従事者を配置する場合には、★4 技術検証従事者に技術検証の判断を単独で行わせてはならない。

3.2 技術検証要員

- ① 技術検証事業者は、★4 技術検証ガイドに定める技術検証の対象（ネットワーク境界に係る機器を含む。）について脆弱性診断を適切に実施する能力その他技術検証の実施に必要な専門的な知見及び能力を有する者を確保しなければならない。
- ② 技術検証事業者は、技術検証に従事する者に対して、例示 7-2 に定める教育及び研修等又は同等のもののいずれかを実施し又は受講させなければならない。
- ③ 技術検証事業者は、技術検証に関係する者に、2.11 の定めに従い、正当な理由がある場合を除き、技術検証を実施する過程で得られた又は生じたすべての情報について秘密を守らせなければならない。

第4章 技術検証業務要件

4.1 技術検証の実施及び責任に関する要件

技術検証事業者は、技術検証の具体的手続（委託元評価機関からの委託の受任、技術検証の実施、レビュー及び結果の通知、技術検証結果報告書の様式その他を含む。）を、★4 技術検証ガイド並びに 2.13 に基づき整備する内部規程及び手順書により定め、これに従って実施しなければならない。

なお、技術検証事業者の指定に係る手続は、技術検証事業者指定手順の定めるところによる。

4.2 技術検証の実施

- ① 技術検証事業者は、★4 技術検証ガイドに基づく技術検証の実施プロセス並びに結果の判定及び判断基準を内部規程に定め、技術検証を実施する体制を整備しなければならない。
- ② 技術検証事業者は、技術検証ごとに、少なくとも次に掲げる事項を含む記録（以下「技術検証実施記録」という。）を文書化しなければならない。技術検証実施記録には、診断データを含めない。技術検証実施記録は診断データと明確に区分して管理しなければならない。
 - (ア) 技術検証の対象範囲、手法及び実施時期
 - (イ) 技術検証に従事した★4 技術検証責任者及び★4 技術検証従事者並びにその役割
 - (ウ) 2.3.3 に定めるレビューの実施者、実施日及び結果並びに必要な是正措置
 - (エ) 2.8 に定める利害関係の特定、評価及び措置の結果
 - (オ) 技術検証結果報告書の写し及びその交付の日
 - (カ) 技術検証の対象となる評価基準ごとの適合又は不適合の判定及びその理由並びに検出された脆弱性の件数及び深刻度の区分ごとの内訳

(キ) ⑥に基づく診断データの消去の記録（④ただし書に基づき保有を継続した場合にあっては、同ただし書に基づく記録を含む。）

③ 技術検証事業者は、技術検証実施記録を、正確かつ秘密保持した状態で、委託元評価機関に技術検証結果報告書を交付した日から3年間保管しなければならない。ただし、技術検証結果報告書を交付しないで技術検証を終了した場合（中止した場合その他これに準ずる場合を含む。）は、当該技術検証を終了した日から起算して3年間保管しなければならない。

④ 技術検証事業者は、診断データを、委託元評価機関に技術検証結果報告書を交付した日から3か月を超えて保有してはならない。この場合において、技術検証結果報告書を交付しないで技術検証を終了したとき（中止したときその他これに準ずるときを含む。）は、当該技術検証を終了した日から起算するものとする。ただし、次のいずれかに該当する場合は、当該目的の達成に必要な期間に限り、保有することができる。

(ア) 委託元評価機関が、評価機関指定基準 4.7①の確認、不適合と判定された事項に係る是正の確認若しくは再度の技術検証の実施、評価機関指定基準2.13に定める異議の申出、苦情若しくは紛争の処理、本基準 4.5 に定める撤回若しくは訂正又は本基準2.12に定める苦情及び問い合わせの処理のために必要と認めて書面により求めた場合

(イ) 制度運営機関がその行う調査のために必要と認めて書面により求めた場合（制度運営機関が診断データを保有しない方法による確認を求める場合に限る。）

(ウ) 技術検証事業者が、本基準 4.5 に定める撤回若しくは訂正又は本基準2.12に定める苦情及び問い合わせの処理のために必要と認めた場合

この場合において、技術検証事業者は、保有を継続する事由、対象となる診断データの範囲及び保有を継続する期限を記録し、遅滞なく委託元評価機関及び制度運営機関に通知しなければならない。当該期限は、技術検証結果報告書を交付した日（技術検証結果報告書を交付しないで技術検証を終了した場合は当該技術検証を終了した日）から通算して1年を超えてはならない。ただし、制度運営機関が必要と認めた場合はこの限りでない。

⑤ 技術検証事業者は、委託元評価機関及び★4 登録希望組織の同意に基づき、診断データを★4 登録希望組織に提供することができる。この場合において、当該提供は、前号に規定する保有の期間に影響を及ぼさない。

⑥ 技術検証事業者は、4.2④に規定する期間が経過したときは、遅滞なく診断データを消去しなければならない。この場合において、その対象、方法及び実施日を記録しなければならない。

⑦ 当該技術検証に直接従事した者は、当該技術検証結果について2.3.3に定めるレビューを行ってはならない。

4.3 技術検証の合意

技術検証事業者は、委託元評価機関と、その技術検証に関し、法的に拘束力のある合意を結ばなければならない。当該合意は、技術検証事業者及び委託元評価機関が負うべき責任を考慮に入れなければならない。当該合意は、書面（電磁的方法を含む。）により締結しなければならない。

技術検証事業者は、当該合意に、少なくとも次に掲げる事項を定めなければならない。

- ① 技術検証の範囲及び実施条件
- ② 技術検証事業者及び委託元評価機関それぞれの責任の範囲
- ③ 秘密保持
- ④ 技術検証の実施に係る許諾の確認（対象範囲、実施方法及び実施時期の特定を含む。）。この場合において、技術検証事業者は、★4 登録希望組織が当該許諾を与えたことを示す書面（電磁的記録を含む。）の写しの提供を委託元評価機関から受け、これを保管しなければならない。当該許諾の範囲を超える技術検証を行ってはならない。技術検証事業者は、当該許諾の範囲が★4 技術検証ガイドに定める技術検証の対象を満たさないと認めるときは、遅滞なくその旨を委託元評価機関に通知し、許諾の範囲の変更を求めなければならない。この場合において、範囲の変更が行われなるときは、技術検証事業者は、判定を行うことができなかった評価基準及びその理由を技術検証結果報告書に明示しなければならない。
- ⑤ 技術検証結果の取扱い及び委託元評価機関への提供の範囲
- ⑥ 契約の解除及び技術検証を中止する場合の取扱い
- ⑦ 外部委託を行う場合における委託先の名称及び当該委託先に対する秘密情報の提供に関する事項
- ⑧ 診断データの保管及び消去に関する事項及び時期並びに 4.2④ただし書に基づき保有の継続を求める場合の手続
- ⑨ 技術検証の実施時期及び技術検証結果報告書の提出期限並びに委託元評価機関が指摘した事項に係る再検証を行う場合の手続、期限及び費用の負担

4.4 技術検証の結果

技術検証事業者は、技術検証結果報告書の内容及びこれに含まれる技術検証の結果について責任を負い、かつ、その判定に関する権限を有しなければならない。技術検証事業者は、技術検証結果報告書を委託元評価機関に交付しなければならない。

評価機関は、当該技術検証結果報告書を利用して行った評価判断及び第三者評価の結論について責任を負う。

技術検証事業者は、技術検証の品質確保のため、委託元評価機関に提供する技術検

証結果報告書その他の成果物において、少なくとも次に掲げる事項を明示しなければならない。

- ① ★4 要求事項及び評価基準に従って技術検証を実施したこと
- ② 技術検証の対象範囲、手法及び実施時期
- ③ 技術検証の対象となる評価基準ごとの適合又は不適合の判定及びその理由
- ④ ★4 技術検証ガイドに定める脆弱性診断の結果の取扱い（又は同等のもの）
- ⑤ 技術検証結果報告書には、診断データを記載してはならない。③の判定理由は、次に掲げる事項の範囲で記載しなければならない。
 - (ア) 検出された脆弱性の深刻度の区分ごとの件数
 - (イ) ★4 要求事項及び評価基準への適合性の判断に必要な限度における、検出された脆弱性の類型及びその対処の状況
 - (ウ) 技術検証に用いたエビデンスの種類及びその十分性に関する評価

4.5 技術検証結果報告書の撤回及び訂正

- ① 技術検証事業者は、交付した技術検証結果報告書について、記載の誤り、技術検証の根拠とした情報の重大な誤りその他の事由により、当該技術検証結果報告書の内容が適正でないことが判明した場合は、遅滞なく当該技術検証結果報告書を撤回し、又は訂正しなければならない。
- ② 技術検証事業者は、前号の措置を行ったときは、委託元評価機関及び制度運営機関に対し、遅滞なくその旨及び理由を通知しなければならない。
- ③ 技術検証事業者は、①及び②の措置及びその記録を、4.2③に定める期間保管しなければならない。
- ④ 技術検証結果報告書の撤回又は訂正に必要な場合は、当該技術検証実施記録その他保存されている記録に基づき対応する。

4.6 ★4 技術検証責任者の欠員等の報告

技術検証事業者は、★4 技術検証責任者の欠員その他技術検証を適正に実施し得ない状態を知ったときは、遅滞なく、当該状態の発生日、対象となる技術検証案件及び影響範囲を委託元評価機関及び制度運営機関に通知しなければならない。通知には、少なくとも影響を受ける可能性のある技術検証案件の一覧を含めなければならない。

技術検証事業者は、当該状態が解消されるまでの間、新たな技術検証の受任及び技術検証結果報告書の交付を行ってはならない。この場合における通知その他必要な手続並びに当該状態への対応については、技術検証事業者指定手順の定めるところ

による。

4.7 情報の提供

技術検証事業者は、次の情報を維持し、委託元評価機関その他の利害関係者からの要請に応じて利用できるようにしなければならない。これらの情報は最新の状態に維持し、内容に変更が生じた場合は遅滞なく更新しなければならない。

- ① 技術検証の手続についての情報
- ② 技術検証事業者が委託元評価機関に課す料金に関する一般的情報
- ③ 委託元評価機関の権利及び義務の記述
- ④ 苦情及び問い合わせの処理手順に関する情報並びに 2.12①に規定する受付窓口の連絡先

附則（2026 年 9 月 11 日）

①この基準は、2026 年 9 月 11 日から施行する。

改定履歴

日付	改定内容
2026 年 9 月 11 日	施行