

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）

★4 技術検証ガイド

2026 年 10 月 28 日

SCS 評価制度 制度運営機関

目次

はじめに.....	4
1. 本ガイドの位置づけ.....	4
2. 用語定義.....	4
3. 技術検証の目的.....	4
4. 実施の免除.....	4
5. 技術検証の実施フロー.....	5
第1部 評価機関・技術検証事業者編.....	7
第1章 实施方式.....	7
1.1 対象機器の範囲.....	7
1.2 診断方式.....	7
1.3 診断ツール.....	7
第2章 事前準備.....	8
2.1 合意事項の確認.....	8
2.1.1 診断行為の許可.....	8
2.1.2 責任範囲.....	8
2.1.3 秘密保持.....	8
2.2 必要情報の収集.....	8
2.3 診断実施条件の確認.....	9
2.3.1 実施期間の決定.....	9
2.3.2 対象機器の選定.....	9
2.4 関係者との調整.....	11
2.4.1 登録希望組織内の調整.....	11
2.4.2 外部サービス事業者との調整.....	11
2.4.3 セキュリティ機器の設定変更.....	11
第3章 診断の実施.....	12
3.1 ポート開放状況の確認.....	12
3.2 脆弱性の有無の確認.....	12
3.3 診断結果の精査.....	12
3.4 技術検証結果報告書の作成及び診断データの提供.....	13
3.5 可否の判定（初回診断時）.....	13
第4章 脆弱性検出時の是正対応.....	14
4.1 是正対応の依頼.....	14
4.2 是正状況の確認.....	14
4.2.1 再診断の実施.....	14
4.2.2 リスク低減策の実施状況確認.....	14
4.3 可否の判定（是正対応後）.....	15

第5章	免除の条件	16
5.1	実施困難時の代替	16
5.1.1	証跡の提出	16
5.1.2	免除の審査	16
5.2	過去の診断実績による代替	17
5.2.1	証跡の提出	17
5.2.2	免除の審査	17
第6章	技術検証の実施者	19
6.1	実施者の資格	19
6.2	実施者の記録	19
6.3	実施時の体制	19
第7章	情報の管理	20
7.1	秘密保持	20
7.2	文書の保管	20
7.3	文書の保管方法	20
7.4	文書の破棄	21
第2部	登録希望組織編	22
1.	免除申請	22
2.	事前準備	23
3.	診断の対応	24
4.	脆弱性検出時の是正対応	24

はじめに

1. 本ガイドの位置づけ

本ガイドは、SCS 評価制度における技術検証について説明するものである。技術検証とは、登録希望組織が管理する適用範囲内の IT 基盤等である機器、システム等に対して、技術的な手法によって★4 要求事項・評価基準への適合性を評価することをいう。

- 評価機関及び技術検証事業者は、「第 1 部 評価機関・技術検証事業者編」の記載事項を踏まえて技術検証を実施するものとする。
- 登録希望組織は、「第 2 部 登録希望組織編」の記載事項を踏まえて技術検証に対応するものとする。

2. 用語定義

本ガイドで使用する用語は、本ガイドに別段の定めがある場合を除き、「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）基本規程」（以下「基本規程」という。）において使用する用語による。

3. 技術検証の目的

★4 要求事項・評価基準のうち、評価基準 No.4-4-4-3（インターネットとの境界に設置されているネットワーク機器の OS 及びファームウェアについては、CVSS の基本値が 7.0 以上の脆弱性を有していないこと）への適合状況を確認するための技術的な検証として、脆弱性診断又はそれに相当する証跡（本ガイド第 5 章参照）の確認を実施する。技術検証において脆弱性が検出された場合は、評価機関による評価基準 No.4-4-4-2 の適合判定に必要な情報を、最小限の範囲で技術検証事業者から評価機関に提供するものとする。ただし、評価基準 No.4-4-4-2 への適合判定は、評価機関が実施するものとする。

4. 実施の免除

次に掲げるいずれかの場合は、証跡の提出及び評価機関による審査をもって脆弱性診断の実施を免除することができる。詳細な免除の条件については、第 1 部第 5 章で規定する。

- 診断範囲内の全ての機器が登録希望組織の管理外であり、管理者であるインターネットサービスプロバイダー等から脆弱性診断の実施許可が得られない場合
- 第三者評価における文書確認の開始日から起算して過去 1 か月以内に本ガイドの記載と同等以上の範囲で脆弱性診断を実施しており、当該診断の実施事業者が技術検証事業者として指定を受けている場合

なお、第三者評価全体の実施フローについては、「★4 第三者評価ガイド」を参照すること。

5. 技術検証の実施フロー

免除の意向の有無に応じ、次に掲げる①又は②のフローで技術検証を実施する。なお、★4 登録の更新時に実施する技術検証についても同様の実施フローとする。技術検証の実施フローを、図 1 に示す。

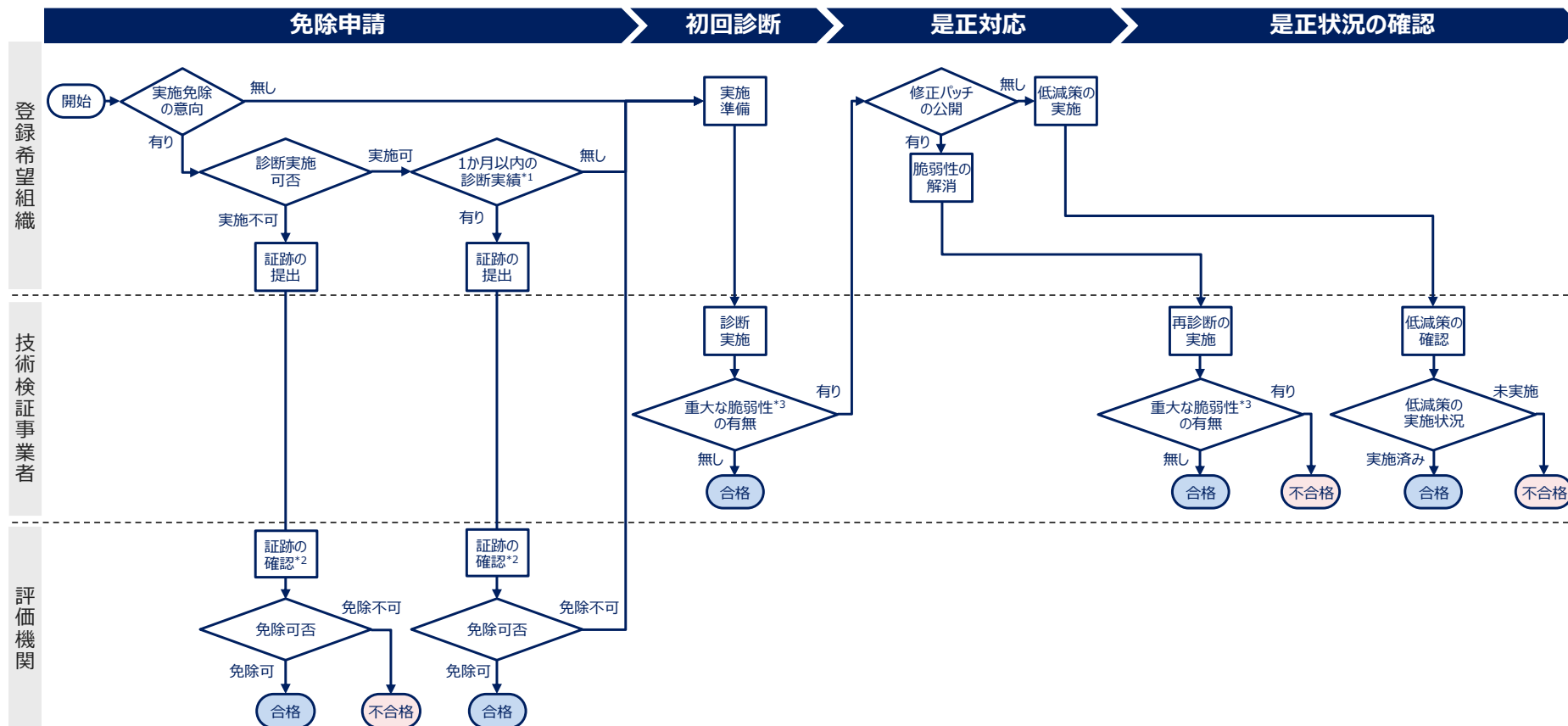
① 実施免除の意向がある場合

登録希望組織に実施免除の意向がある場合は、登録希望組織による証拠の提出をもって評価機関が免除可否の審査を行う。実施困難時の代替としての実施免除が認められない場合は、評価基準 No.4-4-4-3 への不適合及び技術検証への不合格とする。過去の診断実績による代替としての実施免除が認められない場合は、技術検証事業者が脆弱性診断を行う。

② 実施免除の意向がない場合

登録希望組織に実施免除の意向がない場合は、技術検証事業者が脆弱性診断を行う。

なお、技術検証事業者による脆弱性診断の詳細については、第 1 部第 1 章から第 4 章で規定する。



*1: 文書確認の開始日から起算して過去1か月以内の診断実績

*2: 必要に応じて技術検証事業者の支援の下で確認

*3: CVSS基本値 7.0以上の脆弱性

図1 技術検証の実施フロー

第1部 評価機関・技術検証事業者編

第1章 実施方式

1.1 対象機器の範囲

登録希望組織が決定した適用範囲内において、脆弱性を悪用された場合に登録希望組織の IT 基盤に対する攻撃の起点となり得る機器であり、外部から直接アクセス可能な VPN 装置、ルータ、ファイアウォールその他これらに類する通信制御機能を有する機器を対象とする。なお、適用範囲とは、登録希望組織が SCS 評価制度における評価対象として定める IT 基盤の範囲をいう。適用範囲の考え方及び定め方については、「★3・★4 自己評価等ガイド」を参照すること。

1.2 診断方式

外部診断による脆弱性診断を実施することとし、対象機器に外部から疑似的な攻撃の通信を行うことで、CVSS の基本値が 7.0 以上の脆弱性の有無を確認する。

1.3 診断ツール

使用する診断ツールは任意とし、情報セキュリティサービス審査登録制度における「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」に記載のプラットフォーム脆弱性診断のツールを参考に、技術検証事業者が選定する。技術検証事業者は、ツール内の脆弱性情報を診断実施時点において最新の状態に更新するとともに、技術検証の目的や診断範囲に照らして適切な診断ポリシーを選定しなければならない。

参考：経済産業省「情報セキュリティサービス審査登録制度」

■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
(<https://www.meti.go.jp/policy/netsecurity/shinsatouroku/touroku.html>)

第2章 事前準備

2.1 合意事項の確認

技術検証事業者は、次の 2.1.1 から 2.1.3 に掲げる全ての事項を登録希望組織との間で事前に合意しなければならない。なお、評価機関が技術検証事業者を兼ねる場合は、評価機関が登録希望組織と合意することで足りるものとする。

2.1.1 診断行為の許可

技術検証事業者は、対象機器に対する外部からのポートスキャンを含む疑似的な攻撃通信を実施するに当たり、登録希望組織からその実施について明示的な許可を受けるとともに、その内容について契約等により合意しなければならない。

2.1.2 責任範囲

技術検証事業者は、脆弱性診断が稼働中のサービスを停止させたりパフォーマンスを低下させる等の影響が及ぶ可能性があることを十分に説明し、脆弱性診断の実施に伴い登録希望組織の IT 基盤、サービス又は業務に影響が生じた場合の責任範囲について、登録希望組織との間で契約等により合意しなければならない。

2.1.3 秘密保持

技術検証事業者は、脆弱性診断の過程で取り扱う秘密情報について、利用目的、取扱範囲、保管方法、共有先及び廃棄方法を含め、登録希望組織との間で契約等により合意しなければならない。

2.2 必要情報の収集

技術検証事業者は、1.1 で定める対象機器の範囲内において、登録希望組織が把握している全ての機器の製造元、モデル、グローバル IP アドレス及び利用ポートが確認できる資料の提出を登録希望組織に依頼しなければならない。さらに、2.3.2 で定める対象機器の選定が完了した後、選定された対象機器の OS 及びファームウェアのバージョン情報が確認できる資料の提出を登録希望組織に依頼しなければならない。また、必要に応じて資料の記載事項等に関する説明を登録希望組織に依頼し、診断に必要な情報を収集しなければならない。なお、クラウド事業者等の外部サービス事業者が提供する機器が診断対象に含まれる場合は、本ガイド 2.4.2 に記載する情報についても、併せて収集しなければならない。

2.3 診断実施条件の確認

技術検証事業者は、次の 2.3.1 及び 2.3.2 に掲げる全ての事項を登録希望組織との間で事前に確認しなければならない。

2.3.1 実施期間の決定

技術検証事業者は、登録希望組織と調整の上、診断の実施期間を事前に決定しなければならない。対象機器に疑似的な攻撃の通信を行うため、登録希望組織の IT 基盤の稼働等に影響を与えるリスクがあり、必要に応じて休日、夜間又はメンテナンス時間帯に診断を行い、業務への影響を可能な限り避けることが望ましい。なお、技術検証事業者は、実際に診断を開始した時点及び終了した時点で、登録希望組織にその旨を通知しなければならない。

2.3.2 対象機器の選定

技術検証事業者は、2.2 で定める必要情報及び登録希望組織への確認に基づき、次の①から⑤に掲げる全ての手順により、原則として 5 台の対象機器候補を選定しなければならない。対象機器候補の選定フローを、図 2 に示す。

- ① 1.1 で定める対象機器の範囲に含まれる機器を整理し、台数を確認する。ただし、登録希望組織の管理外であり、管理者であるインターネットサービスプロバイダー等から脆弱性診断の実施許可を得られない機器は除外する。なお、1.1 で定める対象機器の範囲に含まれる全ての機器が除外される場合は、5.1 で定める免除申請の対象となる。
- ② ①の結果、機器数が 5 台以下の場合は、全ての機器を対象機器候補として選定する。
- ③ ①の結果、機器数が 6 台以上の場合は、製造元とモデルが同一の機器を代表機 1 台に集約する。
- ④ ③の結果、機器数が 5 台以下の場合は、集約前の機器一覧から 5 台の対象機器候補を選定する。
- ⑤ ③の結果、機器数が 6 台以上の場合は、集約後の機器一覧から 5 台の対象機器候補を選定する。

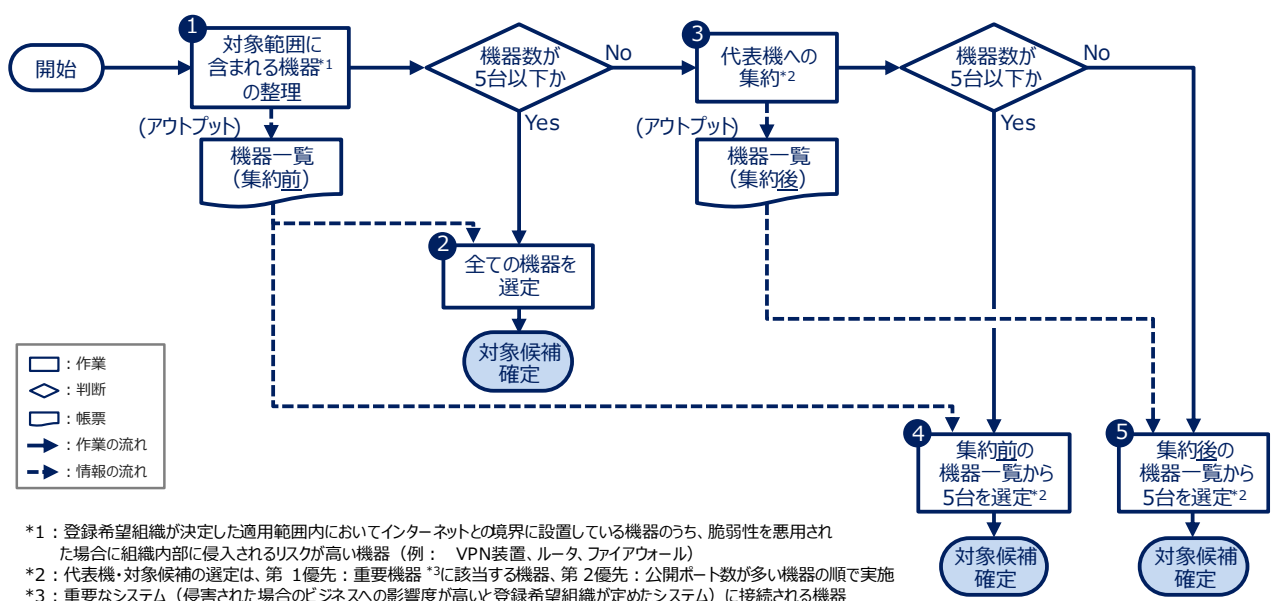


図 2 対象機器候補の選定フロー

技術検証事業者は、③から⑤の手順において代表機又は対象機器候補を選定する際は、次に掲げる優先順位により選定しなければならない。

- 第一に、重要なシステムに接続される機器（以下「重要機器」という。）を優先する。重要なシステムとは、侵害された場合の自社業務や取引先業務への影響度が高いと登録希望組織が定めたシステムである。
- 第二に、外部から通信可能な公開ポート数が多い機器を優先する。

なお、同一の優先順位に該当する機器が複数存在する場合は、登録希望組織への確認により、業務上の重要性がより高いと考えられる機器を優先する。重要機器かつ公開ポート数が多い機器を優先した選定例として、③の手順における代表機への集約例を表 1 に、⑤の手順における対象機器候補 5 台の選定例を表 2 に示す。

表 1 代表機への集約例

機器	製造元・モデル	重要機器	公開ポート数	集約結果
A	同一	該当	3	代表機
B		該当	1	機器 A に集約
C		非該当	3	機器 A に集約
D		非該当	1	機器 A に集約

製造元・モデルが同一の 4 台を、重要機器かつ公開ポート数が多い「機器 A」に集約

表 2 対象機器候補 5 台の選定例

機器	重要機器	公開ポート数	選定結果
A	該当	3	選定
E	該当	2	選定
F	該当	1	選定
G	非該当	4	選定
H	非該当	3	選定
I	非該当	2	選定外

公開ポート数は F より I の方が多いが、重要機器を優先するため、「機器 I」は選定外

技術検証事業者は、IT 基盤の稼働等に影響を与えるリスクを考慮の上、候補の中から対象機器を選定するよう登録希望組織に依頼し、確定させなければならない。なお、登録希望組織の希望により、6 台以上の機器又は全ての機器を対象としても差し支えない。

2.4 関係者との調整

技術検証事業者は、診断の阻害、診断に伴う業務影響、その他の支障を防止するため、事前に関係者との調整を登録希望組織に依頼しなければならない。

2.4.1 登録希望組織内の調整

技術検証事業者は、次に掲げる全ての事項について、登録希望組織に実施を依頼しなければならない。

- 経営層又は情報セキュリティ責任者による診断実施の承認
- 診断トラフィックに対して検知、遮断又は警報を行う可能性のある CSIRT/SOC 等の関係者への事前通知
- 診断中の緊急連絡体制の確認

2.4.2 外部サービス事業者との調整

技術検証事業者は、クラウド事業者等の外部サービス事業者が提供する機器が診断対象に含まれる場合は、外部サービス事業者が定める脆弱性診断に関するポリシーへの準拠、必要な事前申請又は通知要否、診断可能な範囲、その他診断に関連する事項を確認の上、必要な対応を実施するよう登録希望組織に依頼しなければならない。

2.4.3 セキュリティ機器の設定変更

技術検証事業者は、次に掲げる全ての事項に基づき、登録希望組織にセキュリティ機器の設定変更を依頼しなければならない。

- 診断実施時の接続元 IP アドレスを登録希望組織に通知する。
- IPS 又は WAF の管理者と事前に調整の上、接続元 IP アドレスからの通信に対する遮断除外又は通信許可の設定を実施することを登録希望組織に依頼する。設定変更を行う場合は、2.3.1 で決定した診断の実施期間に限定して適用するよう依頼する。なお、設定変更を実施しないことにより、3.1 から 3.3 で定める確認が阻害され、結果として所定の技術検証を実施できず評価に必要な根拠を確認できない場合は、不適合として取り扱う。
- 診断終了後、遮断除外又は通信許可の設定から復旧するよう登録希望組織に依頼の上、復旧が完了したことを登録希望組織との間で相互に確認しなければならない。

第3章 診断の実施

3.1 ポート開放状況の確認

技術検証事業者は、次に掲げる全ての事項に基づき、ポート開放状況を確認しなければならない。

- 対象機器のグローバル IP アドレスに対するポートスキャンを実施し、外部から通信可能な TCP 及び UDP のポートを確認する。
- TCP は、1～65535 番ポートの全てを対象とする。
- UDP は、登録希望組織側で利用を把握しているポート及び技術検証事業者が選定する一般に利用頻度の高い上位 100 ポートを確認対象とする。なお、技術検証事業者は、使用するツールが推奨するポート及び Nmap 等の公開情報を参考に、一般に利用頻度の高い上位 100 ポートを選定する。

3.2 脆弱性の有無の確認

技術検証事業者は、3.1 で定める診断により、外部から通信可能であることが確認されたポートに接続を試み、対象機器の OS 及びファームウェアのバージョン情報を確認しなければならない。その際、登録希望組織から提供された対象機器の OS 及びファームウェアのバージョン情報を参考情報として利用することができる。対象機器の仕様や設定等によりバージョン情報を取得できない場合は、登録希望組織に、対象機器の管理画面上のバージョン情報やベンダーが発行するサポート情報等の提供を依頼し、当該情報を用いてバージョン情報を確認するものとする。

技術検証事業者は、対象機器の OS 及びファームウェアのバージョン情報の確認結果を踏まえ、対象機器の OS 及びファームウェアにおける CVSS の基本値が 7.0 以上の脆弱性の有無を確認しなければならない。

なお、3.2 に基づく確認は、評価基準 No.4-4-4-3 に係る最低限の確認範囲であり、インターネットとの境界に設置されているネットワーク機器以外のミドルウェア、アプリケーションその他のソフトウェア等のすべてについて、脆弱性がないことの確認を求めるものではない。ただし、診断の過程で OS 及びファームウェア以外の脆弱性を発見した場合、登録希望組織に対し是正対応を促すことが望ましい。

3.3 診断結果の精査

技術検証事業者は、3.2 の結果として CVSS の基本値が 7.0 以上の脆弱性が検出された場合は、対象機器に直接アクセスしての確認等を実施し、ツールによる自動検出の結果を手動で精査することで誤検出（偽陽性）を防止しなければならない。また、必要に応じて登録希望組織にアップデートプログラムの適用履歴等の提供を依頼し、脆弱性の有無を精査しなければならない。

3.4 技術検証結果報告書の作成及び診断データの提供

技術検証事業者は、「技術検証事業者指定基準」4.4に従って実施した脆弱性診断の結果に基づき技術検証結果報告書を作成しなければならない。技術検証事業者は、作成した技術検証結果報告書を評価機関に提出しなければならない。

また、技術検証事業者は、実施した脆弱性診断に係るデータ（以下「診断データ」という。脆弱性の検出結果を含む。）を作成し、登録希望組織に提供しなければならない。

3.5 合否の判定（初回診断時）

技術検証事業者は、診断対象として選定した機器における CVSS の基本値が 7.0 以上の脆弱性の有無に応じて、次に掲げるいずれかの合否判定を行わなければならない。

- 全ての機器に CVSS の基本値が 7.0 以上の脆弱性が存在しないことが確認できた場合は、評価基準 No.4-4-4-3 への適合及び技術検証への合格として判定する。
- いずれかの機器に CVSS の基本値が 7.0 以上の脆弱性が存在することが確認された場合は、合否の判定を保留し、第 4 章で定める是正対応の対象として取り扱う。

技術検証事業者は、合否の判定結果を登録希望組織及び評価機関に通知しなければならない。また、脆弱性が検出された場合は、技術検証結果報告書への記載その他の方法により、評価機関による評価基準 No.4-4-4-2 の適合判定に必要な情報を、最小限の範囲で評価機関に提供しなければならない。

第4章 脆弱性検出時の是正対応

4.1 是正対応の依頼

技術検証事業者は、診断の結果、CVSS の基本値が 7.0 以上の脆弱性が検出された場合、登録希望組織に対し、アップデートプログラムを適用して当該脆弱性を解消する必要がある旨を通知しなければならない。ただし、アップデートプログラムが公開されておらず、当該脆弱性を解消することができない場合は、技術検証事業者は、登録希望組織に対し、次に掲げるいずれかの脆弱性悪用のリスク低減策を実施することを求める。

- 脆弱性悪用の対象となる機能を無効化すること。
- ベンダーが推奨する回避策を実施すること。
- 対象となる機器を適用範囲内のネットワークから分離すること。
- 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により、対象となる機器と適用範囲内外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検出できるよう設定を強化すること。

4.2 是正状況の確認

技術検証事業者は、次の 4.2.1 及び 4.2.2 に掲げる事項を踏まえ、登録希望組織における CVSS の基本値が 7.0 以上の脆弱性に対する是正状況を確認しなければならない。是正期間の時系列を、第 1 部第 5 章の図 3 に示す。

4.2.1 再診断の実施

技術検証事業者は、登録希望組織が 4.1 で定める脆弱性の解消を実施した場合、3.5 で定める初回診断における合否結果を登録希望組織に通知した時点から 1 か月以内の期間において再診断の実施依頼を受け付け、3.1 から 3.4 に定める方法により、CVSS の基本値が 7.0 以上の脆弱性が検出された機器への再診断を実施しなければならない。

4.2.2 リスク低減策の実施状況確認

技術検証事業者は、登録希望組織が 4.1 で定める脆弱性悪用のリスク低減策を実施した場合、3.5 で定める初回診断における合否結果を登録希望組織に通知した時点から 1 か月以内の期間において、当該リスク低減策の実施状況の確認依頼を受け付け、当該実施状況を確認できる証拠の提出を登録希望組織に依頼し、当該リスク低減策が実施されていることを確認しなければならない。

4.3 合否の判定（是正対応後）

技術検証事業者は、次に掲げるいずれかの場合は、評価基準 No.4-4-4-3 への適合及び技術検証への合格として判定しなければならない。

- 4.2.1 で定める再診断の結果として CVSS の基本値が 7.0 以上の脆弱性が解消されたことを確認できた場合
- 4.2.2 で定める確認の結果として 4.1 で定めるリスク低減策の実施が認められた場合
技術検証事業者は、次に掲げるいずれかの場合は、評価基準 No.4-4-4-3 への不適合及び技術検証への不合格として判定しなければならない。
- 3.5 で定める初回診断における合否結果を登録希望組織に通知した時点から 1 か月以内に再診断又はリスク低減策の実施状況確認の依頼がなかった場合
- 4.2.1 で定める再診断の結果として CVSS の基本値が 7.0 以上の脆弱性が解消されなかった場合
- 4.2.2 で定める確認の結果として 4.1 で定めるリスク低減策の実施が認められなかった場合

技術検証事業者は、合否の判定結果を登録希望組織及び評価機関に通知しなければならない。また、技術検証結果報告書への記載その他の方法により、4.2 に基づく確認結果のうち、評価機関による評価基準 No.4-4-4-2 の適合判定に必要な情報を、最小限の範囲で評価機関に提供しなければならない。

第5章 免除の条件

5.1 で定める実施困難時の代替又は 5.2 で定める過去の診断実績による代替の条件に合致する場合、証拠の提出及び評価機関による審査をもって脆弱性診断の実施を免除することができる。脆弱性診断の実施が免除された場合は、評価基準 No.4-4-4-3 への適合及び技術検証への合格として判定される。

5.1 実施困難時の代替

1.1 で定める対象機器の範囲内において、全ての機器が登録希望組織の管理外であり、管理者であるインターネットサービスプロバイダー等から脆弱性診断の実施許可を得られない場合は、評価基準 No.4-4-4-3 への適合状況が確認できる証拠の提出及び評価機関による審査をもって脆弱性診断の実施を免除することができる。

5.1.1 証拠の提出

評価機関は、次に掲げる全ての証拠の提出を登録希望組織に求める。

- 脆弱性診断の実施許可を得られない旨が確認できる資料（インターネットサービスプロバイダー等との契約書、利用規約、サービス仕様書等）
- インターネットサービスプロバイダー等が公表するセキュリティ維持及び脆弱性対応に関する方針、サポート提供状況を示す資料、インターネットサービスプロバイダー等が実施した脆弱性診断結果、その他当該機器のセキュリティ管理状況が確認できる資料

5.1.2 免除の審査

評価機関は、提出された証拠に不備があり 5.1.1 で定める事項が確認できない場合は、登録希望組織に再提出を依頼しなければならない。評価機関は、提出された証拠の内容及び必要に応じた登録希望組織への事実確認に基づき、次の①及び②に掲げる全ての条件に合致することを確認できた場合は、脆弱性診断を免除するものとして判定する。評価機関は、免除の判定結果を登録希望組織に通知しなければならない。

- ① 1.1 で定める対象機器の範囲の全ての機器が登録希望組織の管理外であり、管理者であるインターネットサービスプロバイダー等から脆弱性診断の実施許可を得られないことが確認できること。
- ② 利用しているインターネットサービスプロバイダー等が適切な脆弱性対応又は脆弱性診断を実施している等、1.1 で定める対象機器の範囲の全ての機器において CVSS の基本値が 7.0 以上の脆弱性が存在しない蓋然性が確認できること。

5.2 過去の診断実績による代替

文書確認の開始日から起算して過去 1 か月以内に本ガイドの記載と同等以上の範囲で脆弱性診断を実施しており、当該脆弱性診断を実施した事業者（以下「診断実施事業者」という。）が技術検証事業者として指定を受けている場合は、評価基準 No.4-4-4-3 への適合状況が確認できる証拠の提出及び評価機関による審査をもって脆弱性診断の実施を免除することができる。なお、本ガイドの記載に限定した診断を個別に実施している必要はなく、内部診断等を含むより広範囲の診断と併せて実施していても差し支えない。免除及び是正期間の時系列を、図 3 に示す。

5.2.1 証拠の提出

評価機関は、次に掲げる全ての証拠の提出を登録希望組織に求める。

- 2.2 で定める必要情報
- 脆弱性診断の実施結果
- 診断実施事業者の名称
- 脆弱性診断の実施時点から文書確認の開始日までの間に OS 及びファームウェアのバージョン並びに利用ポートに変更がないことが確認できる資料（ただし、CVSS の基本値が 7.0 以上の脆弱性に対応するために変更を実施した場合は、その内容が確認できる証拠の提出をもって代えることができる）

5.2.2 免除の審査

評価機関は、提出された証拠に不備があり 5.2.1 で定める事項が確認できない場合は、登録希望組織に再提出を依頼しなければならない。

評価機関は、提出された証拠の内容及び必要に応じた登録希望組織への事実確認に基づき、次の①から⑦に掲げる全ての条件に合致することを確認できた場合は、脆弱性診断を免除するものとして判定しなければならない。評価機関は、免除の判定結果を登録希望組織に通知しなければならない。

- ① 診断実施事業者が技術検証事業者として指定を受けており、登録希望組織との資本関係等に関して公平性の要件を満たしていること。公平性の要件については、「技術検証事業者指定基準」を参照すること。
- ② 文書確認の開始日から起算して過去 1 か月以内に脆弱性診断を実施していること。
- ③ 1.1 で定める診断範囲内において、2.3.2 で定める方法で選定する対象機器と同等以上の範囲に対し、脆弱性診断を実施していること。
- ④ 3.1 で定める方法と同等以上の範囲に対し、ポート開放状況を確認していること。
- ⑤ 3.2 で定める方法により、対象機器の OS 及びファームウェアのバージョンを確認していること。
- ⑥ 実施時点から文書確認の開始日までの間に対象機器の OS 及びファームウェアのバージョン並びに利用ポートに変更がないこと。ただし、CVSS の基本値が 7.0 以上の脆弱性に対応するために変更を実施した場合を除く。
- ⑦ 上記①から⑥の結果、対象機器の OS 及びファームウェアが CVSS の基本値が 7.0 以上の脆弱性を有していないこと。

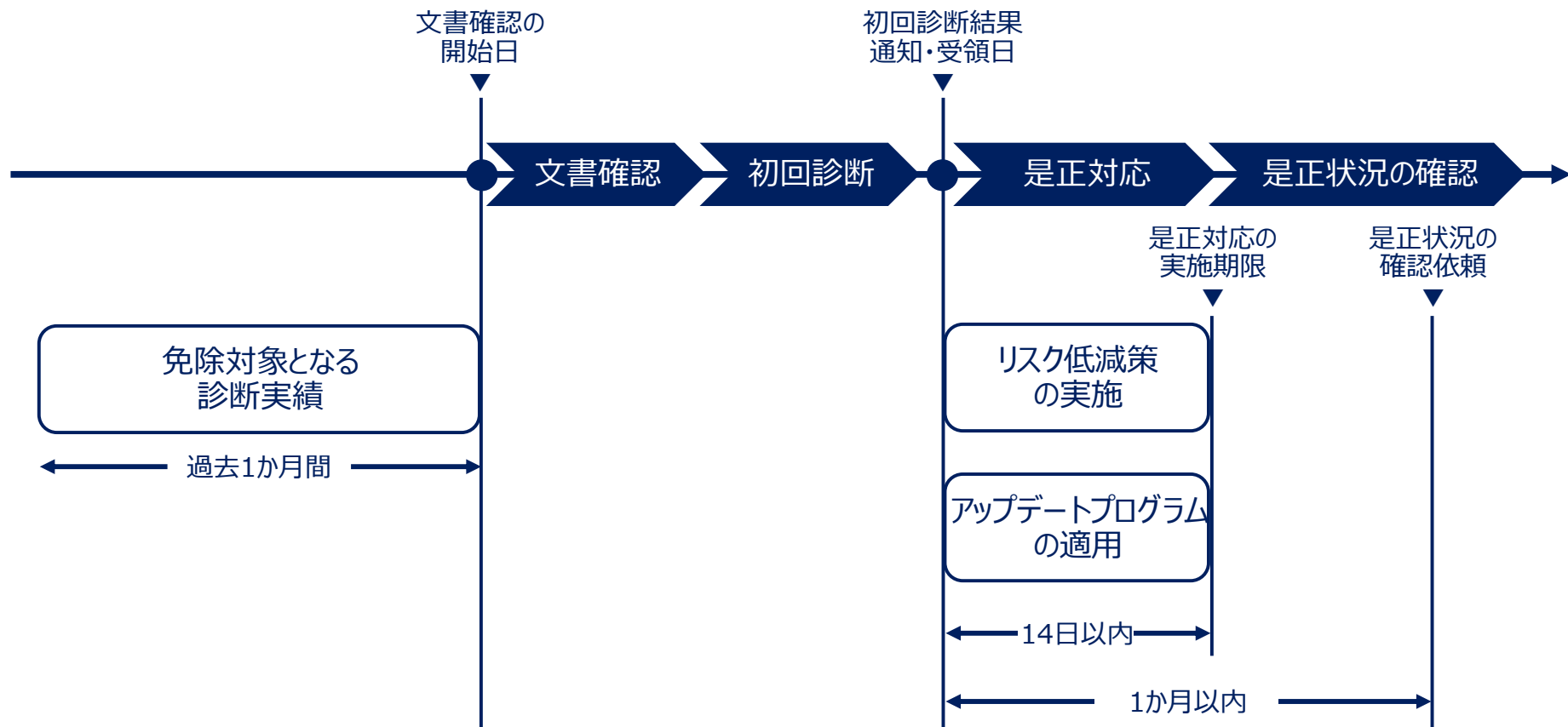


図3 免除・是正期間の時系列

第6章 技術検証の実施者

6.1 実施者の資格

技術検証事業者は、「技術検証事業者指定基準」に規定する★4 技術検証責任者及び★4 技術検証従事者の要件を満たす者に、技術検証を行わせなければならない。また、★4 技術検証責任者は、技術検証事業者内部の者でなければならない。詳細については、「技術検証事業者指定基準」を参照すること。

6.2 実施者の記録

技術検証事業者は、★4 技術検証責任者及び★4 技術検証従事者に関して、次に掲げる全ての事項について記録し、かつ当該記録を最新の状態に維持しなければならない。

- ① セキュリティに関する専門的資格
- ② 制度が指定する研修の受講履歴
- ③ 技術検証の実施実績
- ④ 記録を更新した直近の年月日

なお、①については、「技術検証事業者指定基準」に規定する専門性を有する者の要件を参照の上、必要な事項を記録するものとする。

6.3 実施時の体制

技術検証事業者は、登録希望組織への技術検証を実施する際、★4 技術検証責任者を含む1名以上の人員により実施時の体制を構成しなければならない。その際、技術検証事業者は、「技術検証事業者指定基準」に規定する公平性の要件を満たしていることを確認・記録しなければならない。

第7章 情報の管理

7.1 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全ての情報（対象システムの脆弱性に関する情報を含む。）を、当該情報に係る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。
- ② 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。
- ③ 技術検証事業者は、登録希望組織以外（例：苦情を申し出た者又は規制当局）から得られた当該登録希望組織に関する情報について、秘密として取り扱わなければならない。

7.2 文書の保管

評価機関は、評価結果に係る文書（本ガイド第5章で定める免除審査の記録を含む）について、「評価機関指定基準」4.2に従って保管しなければならない。また、技術検証事業者は、実施した技術検証に係る文書（技術検証結果報告書及び診断データを含む。）について、「技術検証事業者指定基準」4.2に従って保管しなければならない。

7.3 文書の保管方法

前項において技術検証に係る文書を安全に保管するために、技術検証事業者は、★3・★4 要求事項・評価基準において「重要な機密情報」に課せられる管理方法と同等の管理方法として、次に掲げる全ての項目を実施しなければならない。

- ① 文書を管理するに当たって、文書の管理者名、管理部署名、保管場所、保管期限、開示先及び管理者の連絡先を記録する。
- ② 文書を紙媒体で保管する場合には、施錠可能な場所に保管する。
- ③ 文書のファイルデータを保管する場合には、暗号化を実施する。
- ④ 文書をシステムに保管する場合には、当該システムのアクセス権を付与するための条件を定めるとともに、ユーザ及び管理者ごとに必要最小限の権限を付与する。
- ⑤ ④で付与したアクセス権の運用/利用状況を監視する仕組みを導入する。（例：アクセスログの収集・保管等）
- ⑥ 文書を社内ネットワーク上のシステムに保管する場合には、当該システムを分離されたネットワークセグメントに設置し、セグメント内外のアクセスを必要最小限に限定する。
- ⑦ 文書をクラウドサービスに保管する場合又はインターネット経由で文書にアクセスする際には多要素認証を実装する。

7.4 文書の破棄

技術検証事業者は、「技術検証事業者指定基準」4.2 で定める保管期間が終了したときは、技術検証に係る文書について復元できないよう抹消処理（例：データの場合は、記憶媒体の抹消処理、紙文書の場合は、文書裁断等）を行い破棄しなければならない。破棄した後、技術検証事業者は、破棄した文書名、破棄した日付及び破棄した方法についての記録を、評価機関及び登録希望組織に送付しなければならない。

第2部 登録希望組織編

1. 免除申請

登録希望組織は、次に掲げる①又は②に該当する場合は、評価機関に対し脆弱性診断の実施免除を申請することができる。

- ① 診断範囲内の全ての機器が登録希望組織の管理外であり、管理者であるインターネットサービスプロバイダー等から脆弱性診断の実施許可が得られない場合
- ② 第三者評価における文書確認の開始日から起算して過去1か月以内に本ガイドの記載と同等以上の範囲で脆弱性診断を実施しており、当該診断の実施事業者が技術検証事業者として指定を受けている場合

なお、第三者評価全体の実施フローについては、「★4 第三者評価ガイド」を参照すること。

上記①に該当する場合、登録希望組織は次に掲げる全ての証跡を評価機関に提出しなければならない。

- 脆弱性診断の実施許可を得られない旨が確認できる資料（インターネットサービスプロバイダー等との契約書、利用規約、サービス仕様書等）
- インターネットサービスプロバイダー等が公表するセキュリティ維持及び脆弱性対応に関する方針、サポート提供状況を示す資料、インターネットサービスプロバイダー等が実施した脆弱性診断結果、その他当該機器のセキュリティ管理状況が確認できる資料

上記②に該当する場合、登録希望組織は次に掲げる全ての証跡を評価機関に提出しなければならない。

- 登録希望組織が適用範囲内において把握している全ての機器の製造元、モデル、グローバルIPアドレス及び利用ポートが確認できる資料
- 脆弱性診断の実施結果
- 診断実施事業者の名称
- 実施時点から文書確認の開始日までの間にOS及びファームウェアのバージョン並びに利用ポートに変更がないことが確認できる資料（ただし、CVSSの基本値が7.0以上の脆弱性に対応するために変更を実施した場合は、その内容が確認できる証跡の提出をもって代えることができる）

なお、評価機関による免除可否の審査方法については、第1部第5章を参照すること。

2. 事前準備

免除申請を実施しない登録希望組織は、技術検証事業者からの依頼に応じた事前準備を行わなければならない。技術検証事業者が登録希望組織に依頼する事項についての詳細は第1部第2章を参照すること。準備の実施に当たっては、必要に応じてシステムの運用や保守の委託先から資料を取得し、技術検証事業者に提出する。

- ① 免除申請を実施しない登録希望組織は、診断が業務やシステムに及ぼす影響を十分に考慮の上、技術検証事業者から提示された対象機器候補の中から対象機器を選定し、実施期間を決定する。
- ② 登録希望組織は、次に掲げる全ての事項について、組織内の調整を行う。
 - 経営層又は情報セキュリティ責任者による診断実施の承認
診断対象となる機器の管理に責任を有する者（経営層又は情報セキュリティ責任者）から、診断を実施することについてあらかじめ承認を得ること。
 - 診断トラフィックに対して検知、遮断又は警報を行う可能性のある CSIRT/SOC 等の関係者への事前通知
診断が業務やシステムに及ぼす影響を十分に考慮の上、診断トラフィックに対して検知、遮断又は警報を行う可能性のある CSIRT/SOC 等の関係者に対して、事前に診断を実施することについて通知すること。
 - 診断中の緊急連絡体制の確認
障害発生等の診断中における緊急事態が発生した際の、社内（経営層、情報セキュリティ責任者、情報セキュリティ担当者、CSIRT/SOC 等）及びシステムの運用や保守の委託先等の連絡先、連絡手段等をあらかじめ把握しておくこと
- ③ 技術検証事業者からの依頼に基づき、セキュリティ機器の設定変更を行う。セキュリティ機器の設定変更について、社内です承が得られない場合は、設定変更を行わずに診断を行っても差し支えない。なお、設定変更を実施しないことで診断が阻害され、結果として所定の技術検証を実施できず評価に必要な根拠を確認できない場合は、不適合として取り扱われる点に留意する。

3. 診断の対応

登録希望組織は、技術検証事業者によるポート開放状況の確認、脆弱性の有無の確認、診断結果の精査、診断データの提供及び合否の判定（初回診断時）を受けなければならない。技術検証事業者が登録希望組織に対して実施する診断についての詳細は第1部第3章を参照すること。

登録希望組織は、次に掲げる全ての注意事項を踏まえ、診断に対応しなければならない。

- 脆弱性の有無の確認に当たっては、技術検証事業者からの依頼に応じ、機器の管理画面上のバージョン情報やベンダーが発行するサポート情報等を提供する。
- 診断結果の精査に当たっては、技術検証事業者からの依頼に応じ、アップデートプログラムの適用履歴等を提供する。

4. 脆弱性検出時の是正対応

登録希望組織は、診断の結果として CVSS の基本値が 7.0 以上の脆弱性が検出された場合、診断結果を受領した日から 14 日以内に、次に掲げる①又は②の方法により、検出された脆弱性への対応を実施しなければならない。是正期間の時系列を、第1部第5章の図3に示す。

- ① 原則として、アップデートプログラムの適用により当該脆弱性を解消する。
- ② 例外として、アップデートプログラムが公開されておらず、脆弱性を解消することができない場合に限り、以下のいずれかにより脆弱性悪用のリスク低減策を実施する。
 - 脆弱性悪用の対象となる機能を無効化すること。
 - ベンダーが推奨する回避策を実施すること。
 - 対象となる機器を適用範囲内のネットワークから分離すること。
 - 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により、対象となる機器と適用範囲内外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検出できるよう設定を強化すること。

登録希望組織は、上記①又は②を実施した場合、初回診断における合否結果を受領した時点から1か月以内に、技術検証事業者に再診断又はリスク低減策の実施状況確認を依頼することができる。その際、技術検証事業者からの依頼に応じ、再診断又はリスク低減策の実施状況の確認に必要な情報を提供しなければならない。なお、期間内であれば再診断又は実施状況の確認を複数回依頼しても差し支えない。

再診断の結果、CVSS の基本値が 7.0 以上の脆弱性が解消されたことを確認できた場合又は実施状況の確認の結果、リスク低減策の実施が認められた場合は、評価基準 No.4-4-4-3 への適合及び技術検証への合格として判定される。技術検証事業者による合否の判定方法については、第1部第4章を参照すること

改定履歴

日付	改定内容
2026 年 10 月 28 日	初版発行