YODOQ
We keep chasing our dream

ご提案書

SCS評価制度への対応と
★3取得に向けた現状診断のご提案

株式会社ヨドック

CONTENTS

目次

01	SCS評価制度とは	国の新しいセキュリティ評価制度の概要
02	★3で求められる対策	26の要求事項と対応の考え方
03	スケジュール・価格	申請受付開始から逆算した進め方

YODOQ
We keep chasing our dream

01

SECTION 01

SCS評価制度とは

経済産業省・内閣官房が構築し、IPAが運営する国のセキュリティ対策評価制度の概要をご説明します。

制度の3つのポイント

POINT 01

★3は26項目・毎年更新

広く認知された脅威に対する基本対策26項目が対象です。専門家確認付き自己評価で取得し、有効期間は1年間です。

POINT 02

取引契約で活用される制度

発注企業が取引先に★取得を提示し、対策状況を確認する仕組みです。自動車・半導体・流通・金融などで活用が進む見込みです。

POINT 03

2027年1〜3月に受付開始

取得企業はIPAのWebサイトで公開されます。上位の★4（43項目・第三者評価・有効期間3年）も同時に開始予定です。

制度の全体像（公式資料）

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※1）の概要

[※1] SCS（supply chain security）評価制度

- 「対策状況は**外部から判断が難しい**」「**複数の取引先から様々な対策を要求**される」等の課題に対し、サプライチェーンにおける重要性を踏まえた上で満たすべき対策を提示しつつ、その状況を可視化する仕組みを構築。※2
- **２社間の取引契約等において、発注企業が、受注側に適切な段階の”★”を提示**し、示された対策を促すとともに実施状況を確認することを想定。 本制度の活用促進を通じ、サプライチェーン全体でのセキュリティ対策水準の向上を図る。※3
- ３段階の水準のうち、★３・★４について、**令和８年**(2026年)**度末頃の制度開始**を予定。

[※2] 企業等のIT基盤が対象。また、評価は取得又は更新の時点において定められた水準を満たしているかを示すものであり、完全なセキュリティの確保等を保証するものではない。
[※3] 発注時等に、必要なセキュリティ対応状況の可視化を目的としたもので、いわゆる「格付け」制度ではない。

構築する評価制度

	★３	★４	★５ [検討中※5]
想定される脅威	• 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	• 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 • 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	• 未知の攻撃も含めた、高度なサイバー攻撃
対策の基本的な考え方	全てのサプライチェーン企業が**最低限実装すべき**セキュリティ対策： • 基礎的な組織的対策とシステム防御策を中心に実施	サプライチェーン企業等が**標準的に目指すべき**セキュリティ対策： • 組織ガバナンス・取引先管理、システム防御・検知、インシデント対応等包括的な対策を実施	サプライチェーン企業等がさらに目指すべき高度な対策： • 国際規格等におけるリスクベースの考え方に基づき、自組織に必要な改善工程を整備、システムに対しては現時点でのベストプラクティスの対策を実施
要求事項 / 有効期間	26件 / 1年	43件 / 3年（毎年自己評価を実施し結果を評価機関へ提出）	（今後検討）
評価スキーム	**専門家確認付き自己評価** ※4	**第三者評価**	第三者評価

[※4] 専門家：登録セキスペ、CISSP等の資格を有し、かつ制度が定める研修を受講したセキュリティ専門家　[※5] ISMS適合性評価制度、★3・4との整合性も踏まえ、対策事項を今後検討

政府調達や重要インフラ事業者等での活用推進

取引先からの対策要請による活用促進

利害関係者への情報開示による対話の促進

サプライチェーン間の結び付きが強固・複雑な主要製造業（自動車、半導体等）、流通、金融業等において、優先的に本制度の利用を促進。

普及施策の例

想定される課題	中小企業等における★取得の負担		中小企業等におけるセキュリティ専門家の確保	サプライヤー企業への★取得要請時の関係法令の適用
施策の概要	サイバーセキュリティお助け隊サービス（新類型）の創設	中小企業ガイドライン整備	専門家の活用促進	取引先への要請等に係る考え方の整理
	★3・★4取得を目的とした、サイバーセキュリティお助け隊サービス（新類型）を創設し、安価な”★”取得を実現	中小企業の情報セキュリティ対策ガイドライン及び付録サンプル規程の整備により、”★”の取得を容易化	「中小企業向けサイバーセキュリティ専門家リスト」の整備により、中小企業と専門家とのマッチングを促進	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案により、費用に係る円満な価格交渉を促進

出典：経済産業省「SCS評価制度の概要」（2026年3月27日公表資料）

★3・★4で求められる水準（公式資料）

3. 構築する評価制度

3.3 制度において設ける段階（★３・★４）　3.3.1 段階別評価の概要

- ★３については、一般的なサイバー脅威に対処しうることを水準として規定。
- ★４は、初期侵入の防御にとどまらず、内外への被害拡大防止・目的遂行のリスク低減によって取引先のデータやシステム保護に寄与する点や、サプライチェーンにおける自社の役割に適合したサプライチェーン強靭化策が講じられていることを水準として想定。
- ★５については、より高度なサイバー攻撃への対応として、自組織のリスクを適切に把握・マネジメントした上で、システムに対する具体的な対策としては既存のガイドライン等も踏まえた上で現時点でのベストプラクティスに基づく対策を実行する形を想定(★3・4の精査も踏まえ、今後更に具体化)。
- 上位の段階はそれ以下の段階で求められる事項を包括するため、例えば、★3を事前に取得していなければ★4を取得できないという関係とはならない。

	★３[*1]	★４	★５[*4]
想定される脅威	• 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**	• **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 • 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	• **未知の攻撃**も含めた、**高度なサイバー攻撃**
対策の基本的な考え方	• 全てのサプライチェーン企業が**最低限実装すべきセキュリティ対策**として、**基礎的な組織的対策とシステム防御策**を中心に実施	• サプライチェーン企業等が**標準的に目指すべきセキュリティ対策**として、組織ガバナンス・取引先管理、システム防御・検知、インシデント対応等**包括的な対策**を実施（**実地審査及び技術検証を含む評価**によって対策実施状況の確認を行う。）	• サプライチェーン企業等が**さらに目指すべき高度な対策**として、**国際規格等におけるリスクベースの考え方に基づき、自組織に必要な改善プロセスを整備した**上で、**システムに対しては現時点でのベストプラクティスに基づく対策**を実施
脅威に対する達成水準(イメージ)	• **組織内の役割と責任が定義**されている。 • 一般的なサイバー脅威への対処を念頭に、自社**IT基盤**への初期侵入、侵害拡大等への対策が講じられている。 • インシデント発生時に、**取引先を含む社内外関係各所への報告・共有に必要な最低限の手順が定義、実施**されている。	• **取引先のシステムやデータを含む内外**への被害拡大や攻撃者による目的遂行のリスクを低減する対策が講じられている。 • **事業継続に向けた取組や取引先の対策状況の把握**など、自社の位置づけに適合した**サプライチェーン強靭化策が講じられている**。	• 組織において**国際規格等に基づくマネジメントシステム**が確立されている。 • **リスクを適宜適切に把握**した上で、インシデントに対して迅速に検知・対応するなど、**ベストプラクティスに基づくサイバーレジリエンス確保策**が講じられている。 • 取引先等への指導や共同での訓練の実施など、**自社サプライチェーン全体の対策水準向上に資する対策**が講じられている。
要求事項数	26件	43件	今後検討することを想定
評価スキーム	**専門家確認付き自己評価**[*2]	**第三者評価**[*3]	**第三者評価**[*3]
有効期間	1年	3年	今後検討することを想定
ベンチマーク (対象企業やリスクが同様であり、対策項目を検討する上で参考)	• 自工会・部工会ガイドLv1 • Cyber Essentials ⇒★3で対処する脅威等に照らして精査し、対策事項を抽出	• 自工会・部工会ガイドLv2～3(Lv3については一部の項目) • 分野別ガイドライン 等 ⇒★4で対処する脅威等に照らして精査し、対策事項を抽出	• ISO/IEC27001 • 自工会・部工会ガイドLv3 等

*1　★１・★２については、IPAが運営する「SECURITY ACTION」を参照されたい。
*2　★取得希望組織が自ら実施した評価の結果について、セキュリティ専門家による確認及び助言を経て、取得希望組織の評価結果として確定させることをいう。
*3　★取得希望組織が自ら実施した評価の結果について、★取得希望組織以外の組織(評価機関)による評価等を経て、評価結果として確定させることをいう。
*4　ISMS適合性評価制度との制度的整合性、★3・4との整合性も踏まえ、今後対策事項を検討

13

出典：経済産業省・内閣官房「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」（2026年3月27日） p.13

02

SECTION 02

★3で求められる対策

★3の26の要求事項を3つの領域に整理し、対応の考え方をご説明します。

★３で求められる対策

26項目は3つの領域に整理できます

領域 01

文書・ルールの整備

セキュリティ方針・管理規程・台帳・対応手順書などの整備です。Pマーク・ISMSの既存文書を活かすことができます。

領域 02

技術的な対策

資産管理・ウイルス対策・ネットワーク防護・多要素認証・バックアップ等です。既存製品が要件を満たせば追加導入は不要です。

領域 03

運用と記録

パッチ適用・ID棚卸・訓練などの実施と、その記録（証跡）の蓄積です。月次の運用支援で負担を軽減できます。

当社がワンストップでご支援します

支援 01

文書整備支援

約25種の規程・台帳ひな形を基に、貴社の実態に合わせてカスタマイズし整備します。

支援 02

製品導入・設定

IT資産管理・EDR・UTM・多要素認証・バックアップ等から不足分のみを選定し、導入・設定します。

支援 03

運用・専門家確認

月次の運用支援で証跡を蓄積し、国家資格者等のセキュリティ専門家による確認・申請まで支援します。

★3取得の流れ：専門家確認付き自己評価（公式資料）

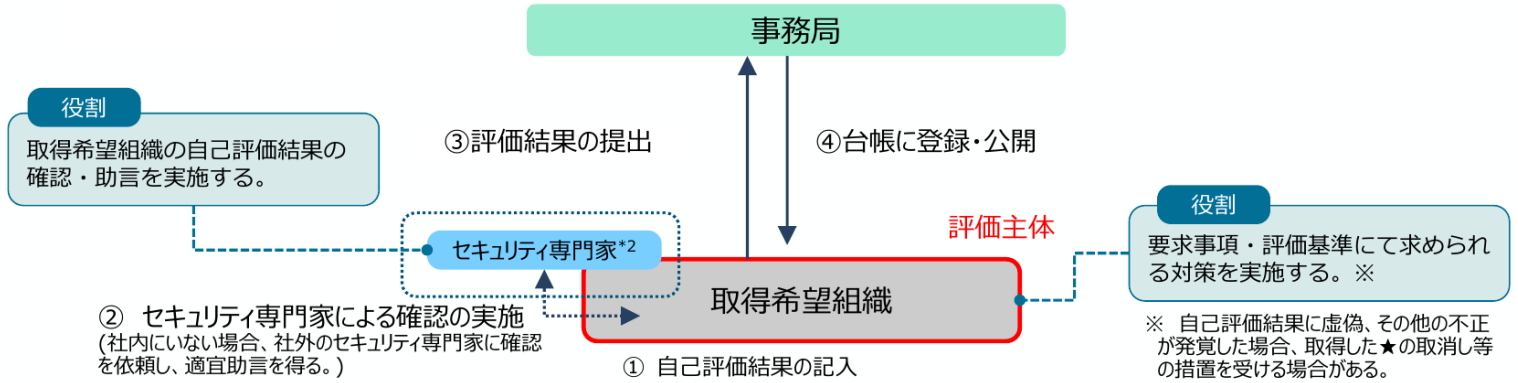
3. 構築する評価制度

3.5 制度における評価スキーム　3.5.1 各段階の評価スキームの概要 - ★3

- ★３は、セキュリティ専門家による確認を経た取得希望組織による自己評価*1(専門家確認付き自己評価)を求めるスキームとする。

専門家確認付き自己評価：★3

① 取得希望組織は、★3要求事項・評価基準に基づき自己評価を記入(必要に応じて社内外のセキュリティ専門家からの支援を得ることも可)
② 社内外のセキュリティ専門家は、取得希望組織が記入した内容を確認するとともに、必要に応じて評価結果の修正を含む助言を行い、最終的に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
③ 取得希望組織は、経営層による自己適合宣誓を含め、事務局に評価結果(セキュリティ専門家による署名を含むもの)を提出
④ 事務局は、申請内容に問題が認められない場合には台帳に登録し、公開



*1　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。
*2　取得希望組織が実施した自己評価結果に対してその内容の確認・助言を実施する者であって、一定のセキュリティ関連資格を有し、かつ、制度側で指定した研修を受講したものをいう。確認・助言に係る作業については、制度側で指定した研修を受講した作業従事者に実施させることができる。(20ページ参照)

出典：経済産業省・内閣官房「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」（2026年3月27日） p.18

評価の実施内容：★3と★4の違い（公式資料）

3. 構築する評価制度

3.5 制度における評価スキーム　3.5.3 評価の考え方 – 評価の実施内容

- ★3では、セキュリティ専門家が、取得希望組織が作成した書類の確認を行う。
- ★4では、評価機関・技術検証事業者が、文書確認に加え、実地審査及び技術検証(脆弱性検査)を行う。
  ※ 以下の評価プロセスでは、各取得希望組織で決定した適用範囲の中から対象をサンプリングの上、評価等を実施することを想定。
  ※ より具体的な実施内容を、本方針に基づき、令和８年度に検討・詳細化予定。

評価プロセス	所要期間(想定)	実施内容等	
		★3	★4
文書確認 (提出書類の確認)	1日~2日程度	• 取得希望組織が作成した自己評価の結果を確認する。 (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想定) • 文書確認の結果、記載内容に明らかな不適合が認められない場合、 ✓ ★3では、取得希望組織は事務局に申請を行い、申請内容に問題等がなければ★3を取得することができる。 ✓ ★4では、実地審査及び技術検証に進む。	
実地審査 (取得希望企業へのヒアリング、規程、操作画面等の確認による評価) ※リモートでの実施も可	1日~2日程度 ※ 事前準備、報告書作成は除く	(実施なし)	• 相対的に重要性が高いと考えられる対策事項について証跡確認を含めた評価を実施 [実地審査で確認すべき事項(例)] ✓ 脆弱性の管理体制、管理プロセス ✓ セキュリティインシデント対応手順 ✓ 事業継続要件に沿った復旧準備
技術検証 (取得希望企業の管理する対象機器に対して既知脆弱性の悪用等の一般的な攻撃パターンを試行)	1日~2日程度 ※ 事前準備、報告書作成は除く	(実施なし)	• 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)を対象として、技術的な検証として脆弱性検査を実施する(検証対象とする評価基準：4-4-4-3) ※　当該検証の実施結果に相当する証跡(例：直近における対象機器への脆弱性検査の実施結果)の提出及び確認をもって検証実施の代替とみなすことも検討する。
合格基準	-	• ★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。	
不適合の指摘及び改善	-	• 評価結果に不適合が発見された場合であっても、適切に是正対処し、セキュリティ専門家から当該是正について了承を得られれば★3を取得可能。	• 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。

23

出典：経済産業省・内閣官房「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」（2026年3月27日） p.23

03

SECTION 03

スケジュール・価格

SCS★3・★4取得支援サービス

提案から契約までの費用フロー

フロント商材　Phase 0（全提案先に実施）

① 説明（約1時間）

SCS評価制度の説明と
ヨドックでできることのご紹介

無料

希望者のみ

② ギャップ分析（約2時間）

要求事項の充足チェック
＋診断報告書の作成・提出

（★3：26項目／★4：43項目）

★3　無料　　**★4　10万円**

診断報告書（1〜2週間後）

ギャップ分析を希望しない場合
→ 説明のみで終了（費用なし・継続フォロー）

本サービスへ進む場合
→ 契約金額1／2をお支払い

ご契約（サポート契約）　※ギャップ分析結果に基づき個別見積り。★4取得支援（第三者評価・技術検証対応）にも対応

本サービス　Phase 1〜4（サポート契約 約6か月）　※★3標準／★4は上位プラン

Phase 1
アセスメント

ギャップ診断（要求事項の現状評価）・対応計画策定
特定されたギャップに対し、対応計画と概算費用を明確にします。

Phase 2
整備

規程・台帳ひな形キット約25種の提供とカスタマイズ、体制構築
規程・台帳を整備し、不足している技術対策を導入します。並行して運用記録の蓄積を開始します。

Phase 3
導入

製品導入（資産管理/EDR/UTM/MFA/バックアップ等）と設定
必要な製品の導入を実施し、対策を実施します。

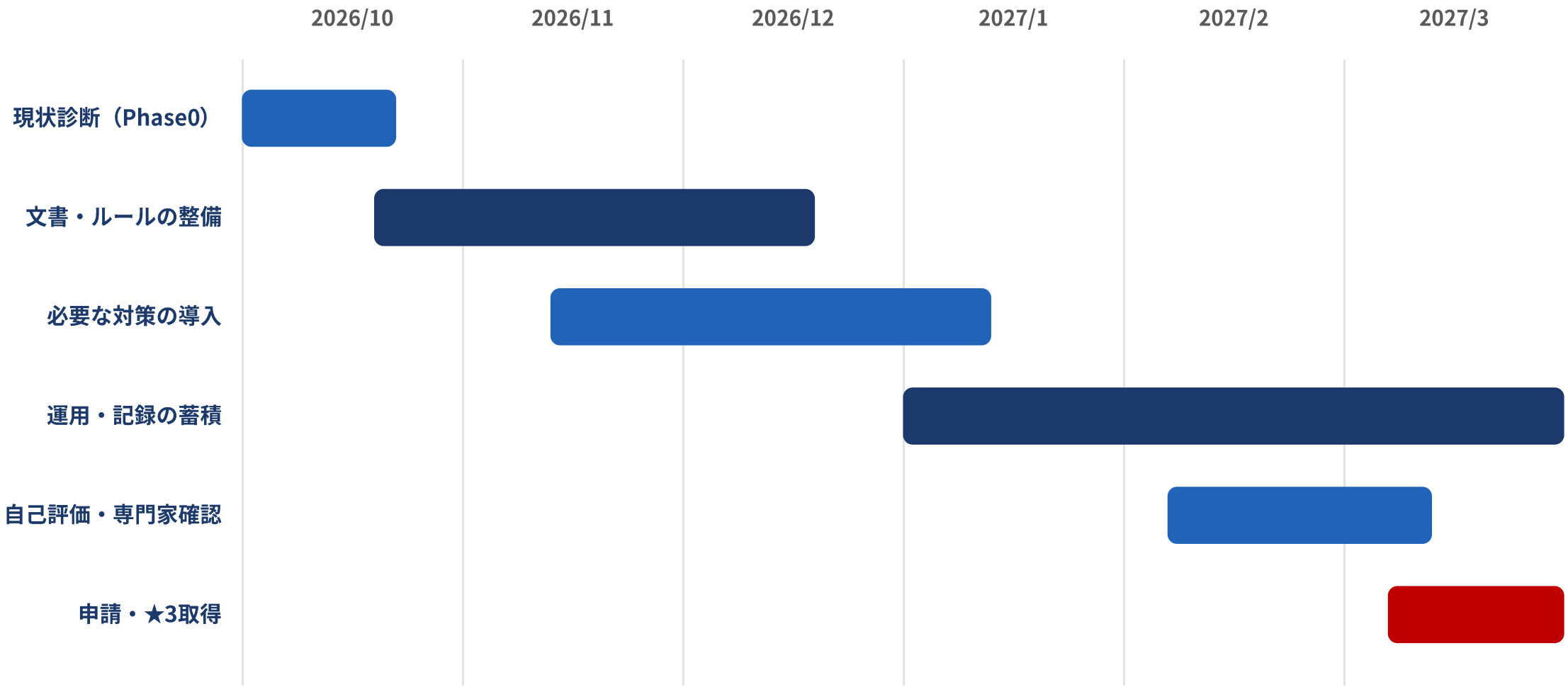
Phase 4
運用・取得

月次運用・年次訓練・自己評価支援・
専門家確認・申請サポート
※★4は第三者評価・技術検証に対応

Phase 1〜3：初期費用（個別見積り／30万円）　※契約時にギャップ分析費（★4:10万円）を値引き

Phase 4：月額＋年次費用

標準スケジュール例（2026年10月開始の場合）



※ 評価用ガイド（2026年度下期にIPAから公表予定）の内容により一部前後する可能性があります。★3の有効期間は1年間のため、取得後は毎年の自己評価・更新が必要です。