SCS評価制度

新評価制度と ISMS との関係・MSQAの専門家育成への取り組み

▶ 約15分で解説

★3 確認（自己評価）

26	81
要求事項	評価基準

登録確認機関

★4 評価（第三者評価）

43	153
要求事項	評価基準

登録審査機関

サプライチェーン上の重要サプライヤー・政府調達関連事業者向け　2026年

MSQA
Management System Quality Association

目次

SCS評価制度 全体構成

① SCS評価制度の背景と概要

1. SCS評価制度とは
2. 制度運営体制
3. 段階別評価の概要（★3・★4・★5）
4. なぜ今SCS評価制度が必要か
2026/10/28 IPA更新情報（最新）

② 評価の仕組み

5. ★3確認と★4評価（2段階評価体系）
6. 評価スキームの概要 ★3確認
7. 評価スキームの概要 ★4評価
8. 評価実施内容とSCSセキュリティ専門家の要件

③ 実装・活用ガイド

9. NIST CSF 2.0・ISMSとの関係
10. ISMS取得済み組織への活用
11. ISMS未取得組織への推奨手順
12. 専門家育成・SCS対応ツール
13. SCS評価制度 導入ロードマップ
14. よくある質問（FAQ）
15. 参考文献・関連資料
16. ご相談・お問い合わせ

2026/10/28 IPA公表

最新情報：要求事項・評価基準 Ver.1.1 変更

変更の概要

IPA事務局より「★3・★4要求事項・評価基準 Ver.1.1」の変更が2026年10月28日に公表。3つの評価基準について整合性確保・リスクベースアプローチ対応のための修正が実施されました。

変更された3つの評価基準

4-4-2-1（★4）

OSサポート確認基準を改訂

EOSのOS・SWをやむを得ず継続利用する場合の更改計画策定と脆弱性悪用リスク低減対策を義務化

4-4-4-1（★3）

情報機器サポート確認基準を改訂

EOSの情報機器をやむを得ず継続利用する場合に脆弱性悪用リスク低減対策の実施を新たに追加

4-4-4-2（★3・★4）

パッチ対応をリスクベースへ変更

CVSS7.0以上への一律14日適用から、攻撃観測状況に応じた対応計画・代替策によるリスク低減管理へ緩和

新しいパッチ対応ルール（評価基準4-4-4-2）の詳細

【ケース①】CVSS7.0以上 ＋ 攻撃が観測済み

IPA「重要なセキュリティ情報」またはCISA「KEV」等の公的機関リストに掲載の脆弱性

→ リリースから14日以内に適用（従来通り継続）

【ケース②】CVSS7.0以上 ＋ 攻撃が未観測または蓄積性が低い

→ 以下を実施することで対応期限の延長が認められる

① 対応計画の策定（完了まで管理・記録）

② 代替策による脆弱性悪用リスクの低減管理

出典：*IPA*「要求事項・評価基準の変更箇所」*2026年10月28日公表*

SCS評価制度とは

サプライチェーン全体のセキュリティ対策状況を「可視化・評価」する第三者評価制度

制度の目的

経済産業省・NISC等の政策方針に基づき、大企業の主要サプライヤー（中小企業）のセキュリティ水準を底上げ。取引先への信頼性証明を実現する。

評価対象

大企業のサプライヤー企業（主に中小企業）・サプライチェーン上の重要な委託先事業者・政府調達に関連するITサービス提供事業者

運営体制

制度運営機関が全体管理・監督。★3確認は「登録確認機関」、★4評価は「登録審査機関」が実施。審査従事者には専門資格と研修が必要。

制度運営体制

経済産業省・NISCの監督のもと、IPAが制度全体を運営します

監督機関

経済産業省

政策立案・制度全体の監督

内閣官房国家サイバー統括室（NISC）

国家安全保障・サイバーセキュリティ政策の統括

IPA（制度運営機関）

事務局

運営管理・★3・★4の登録・普及促進

運営審議委員会

運営方針・制度文書の策定審議

指定委員会

評価機関・技術検証事業者・研修事業者の指定・監督

評価実施機関等

登録審査機関

★4の第三者評価を実施

技術検証事業者

★4の技術検証（脆弱性検査）を実施

SCSセキュリティ専門家

★3の自己評価結果の確認・助言（確認責任者として署名）

研修事業者

セキュリティ専門家向け研修を提供

出典：IPA「SCS評価制度 詳細情報」

段階別評価の概要

SCS評価制度は段階的な評価体系（★3・★4・★5）で構成されています

★3　確認（自己評価）

想定脅威	一般的なサイバー攻撃
水準	基礎的な組織的対策とシステム防御策
要求事項	26件
評価基準	81件
評価方式	専門家確認付き自己評価
有効期間	1年（毎年更新）
実施者	SCSセキュリティ専門家（確認責任者）

★4　評価（第三者評価）

想定脅威	★3に加え、取引先への影響も考慮した攻撃
水準	被害拡大防止、サプライチェーン強靭化策
要求事項	43件（★3の26件＋追加17件）
評価基準	153件
評価方式	第三者評価と技術検証（評価機関）
有効期間	3年（3年ごとに更新）
実施者	登録審査機関（★4評価従事者）

★5　（今後検討）

想定脅威	未知の攻撃を含む高度なサイバー攻撃
水準	リスクを把握したうえでのベストプラクティス対策
要求事項	今後具体化予定
評価基準	今後具体化予定
評価方式	今後検討
有効期間	今後検討
備考	★3の取得が★4の前提ではありません

出典：IPA「SCS評価制度 詳細情報」

IPA「情報セキュリティ10大脅威2026」より

なぜ今 SCS評価制度が必要か

IPA 10大脅威2026（組織向け）

1位	ランサムウェアによる被害
2位	**サプライチェーン・委託先を狙った攻撃**
3位	システムの脆弱性を突いた攻撃
4位	内部不正による情報漏えい等
5位	機密情報等を狙った標的型攻撃

出典: *IPA「情報セキュリティ10大脅威2026（組織編）」*

サプライチェーン攻撃の連鎖メカニズム

大企業・発注元

直接侵入が困難→攻撃者は迂回路を探す

▼

中小サプライヤー

セキュリティが手薄→「入口」として悪用

▼

ソフトウェア・SaaS

信頼されたツール経由で侵入（SolarWinds型）

▼

委託先・クラウド

VPN・リモートアクセスを踏み台に利用

★3確認 と ★4評価

★3　確認（自己評価）	
対象	26要求事項 ／ 81評価基準
評価方式	自己評価＋登録確認機関による確認
実施者	登録確認機関（★3確認従事者）
有効期間	1年（毎年更新）
主な証拠	自己評価報告書・エビデンス
費用感	比較的低コストで取得可能
位置付け	ベースラインとなる基本的対策水準の確認

上位

★4　評価（第三者評価）	
対象	43要求事項 ／ 153評価基準
評価方式	登録審査機関による第三者評価 （技術検証・ヒアリング・現地確認）
実施者	登録審査機関（★4評価従事者）
有効期間	3年（3年ごとに更新）
主な証拠	技術検証レポート・証跡書類一式
費用感	包括的な審査のため一定コスト要
位置付け	高度な技術的実装水準を第三者が証明

評価スキームの概要 ★3確認（自己評価）

「専門家確認付き自己評価」方式で、4つのSTEPで進みます

STEP 1

自己評価の実施

実施者：取得希望組織

- 要求事項・評価基準に基づきアセスメントシートに自己評価を記入
- SCSセキュリティ専門家の支援も利用可能

STEP 2

セキュリティ専門家による確認

実施者：★3確認責任者

- アセスメントシートの内容を確認
必要に応じて助言・修正を行う
- 全要求事項・評価基準を満たしていると
判断した場合に署名・記名

STEP 3

経営層による宣誓＋提出

実施者：取得希望組織

- 経営層による自己適合宣誓を含む
評価結果を事務局に提出する

STEP 4

台帳登録・公開

実施者：IPA事務局

- 申請内容に問題がなければ
台帳に登録・一般公開

【対象】26要求事項 ／ 81評価基準　　【文書確認のみ】実地審査・技術検証：なし　　【有効期間】1年（毎年更新）

出典：IPA「SCS評価制度 詳細情報」

評価スキームの概要 ★4評価（第三者評価）

「第三者評価」方式で、登録審査機関（評価機関）が7つのSTEPで実施します

STEP 1	STEP 2	STEP 3	STEP 4	STEP 5	STEP 6	STEP 7
評価機関・技術検証事業者の指定	**自己評価の実施**	**評価依頼**	**第三者評価・技術検証**	**評価報告書の提供**	**登録申請**	**台帳登録・公開**
指定委員会	**取得希望組織**	**取得希望組織**	**評価機関**	**評価機関→組織**	**取得希望組織**	**IPA事務局**
IPAの指定委員会が評価機関・技術検証事業者・研修事業者を指定	要求事項・評価基準に基づきアセスメントシートに自己評価を記入	評価機関・技術検証事業者に第三者評価・技術検証を依頼する	文書確認（1～2日）＋実地審査（1～2日）＋技術検証：VPN等脆弱性検査（1～2日）	評価結果をまとめた報告書を取得希望組織に提供する	評価報告書を添えてIPA事務局に登録申請を提出する	申請内容を審査後、台帳に登録し一般公開する

【対象】43要求事項（26＋追加17件）／ 153評価基準　　【文書確認＋実地審査＋技術検証】　　【有効期間】3年（3年ごとに更新）

出典：IPA「SCS評価制度 詳細情報」

評価実施内容とSCSセキュリティ専門家の要件

評価実施内容の比較と、専門家の登録要件を整理します

評価実施内容の比較（★3 vs ★4）

評価項目	★3確認	★4評価
文書確認	1～2日程度	1～2日程度
実地審査	―	1～2日（リモート可）
技術検証	―	1～2日（VPN等）
合計目安	1～2日	3～6日程度
合格基準	全評価基準への適合	全評価基準への適合
不適合対応	是正後、専門家が了承すれば取得可	指摘後一定期間内に是正報告

SCSセキュリティ専門家の登録要件

次のいずれかの資格を保持・維持していること

- ✓ 情報処理安全確保支援士（登録RISS）
- ✓ 公認情報セキュリティ監査人
- ✓ CISSP（公認情報システムセキュリティプロフェッショナル）
- ✓ CISA（公認情報システム監査人）
- ✓ CISM（公認情報セキュリティマネージャー）
- ✓ ISO27001主任審査員

かつ、IPAが定める研修を受講したうえで、
IPA事務局に登録すること

MSQAはSCS-330B研修実施基準に基づく教育研修事業者として申請予定（研修事業者の公表は2026年12月末頃を予定：IPA）

出典：IPA「SCS評価制度 詳細情報」

★4評価の構造

機能	機能名	件数・割合	要求事項・概要（★4対象）
GV	統治 Govern	6件	リスク管理方針・CISO体制・守秘義務・サプライヤー管理方針・経営報告
SC	取引先管理 Supply Chain	5件	取引先把握・機密情報合意・セキュリティ確認・インシデント役割・契約終了管理
ID	識別 Identify	6件	IT資産台帳・ネットワーク図・外部サービス・機密区分・リモートワーク・脆弱性管理
PR	防御 Protect	22件	ID管理・MFA・アクセス権棚卸・教育研修・暗号化・バックアップ・ログ・パッチ・ネットワーク防護（最多・重点）
DE	検知 Detect	3件	ネットワーク監視・挙動監視・インシデントレベル分析
RS	対応 Respond	1件	インシデント対応手順（5フェーズ）
RC	復旧 Recover	1件	事業継続要件に沿った復旧準備

合計　43要求事項 ／ 153評価基準（★4）

NIST CSF 2.0

NIST CSF 2.0 とは

策定機関

米国国立標準技術研究所（NIST）が策定。民間・政府機関を問わず世界中で活用される事実上の国際標準フレームワーク

目的

組織がサイバーセキュリティリスクを管理・低減するための共通言語と実践指針を提供。規制ではなく自主的適用が前提

改訂の背景（2.0）

2014年のCSF 1.1から10年ぶりの大改訂。サプライチェーンリスク管理の強化とガバナンス機能（GV）の新設が最大の変更点

SCSとの関係

経産省・IPAはSCS評価制度の技術的枠組みとしてNIST CSF 2.0を採用。6機能にSCS独自の「SC（取引先管理）」を追加した7機能体系で運用

NIST CSF 2.0 標準の 6 機能

GV

統治（Govern）

【2.0新設】セキュリティ方針・リスク管理・役割責任・CISO体制。経営レベルのガバナンス確立が目的

ID

識別（Identify）

資産台帳・リスクアセスメント・サプライチェーンの把握。「何を守るか」の出発点

PR

防御（Protect）

認証・アクセス管理・暗号化・教育・パッチ管理。最多の要求事項を持つ中心的機能

DE

検知（Detect）

脅威監視・異常検知・インシデント判断。攻撃を早期に発見するための体制

RS

対応（Respond）

インシデント対応計画・封じ込め・証拠保全・ステークホルダー通知

RC

復旧（Recover）

事業継続計画・システム復旧・教訓の取込みと改善サイクル

SCS評価制度では、NIST CSF 2.0の6機能に加え「SC（取引先管理・Supply Chain）」を独自追加 → 7機能体系で運用

ISMSとSCS評価制度の関係

ISMS（JIS Q 27001:2023）

情報セキュリティマネジメントの枠組み
（プロセス・体制・リスク管理全般）

- **A.5.19 サプライヤー関係における情報セキュリティ**
- **A.5.20 サプライヤーとの合意のセキュリティ**
- **A.5.21 ICTサプライチェーンの情報セキュリティ管理**
- **A.5.22 サービス提供の監視・レビュー・変更管理**
- **A.5.23 クラウドサービス利用のセキュリティ**

その他：A.8.x システム・A.6～7.x 人的物理等

←→ **連携・補完**

SCS評価制度

サプライチェーン特化の
技術的セキュリティ対策評価

GV（統治）： 方針策定・CISO体制・守秘義務	**A.5.19対応**
SC（取引先管理）： 選定・契約・モニタリング	**A.5.20～5.22**
ID（識別）： 資産台帳・クラウド管理・リスク評価	**A.5.21～5.23**
PR（防御）： アクセス制御・暗号化・パッチ管理	**A.8.x連携**
DE（検知）： ログ監視・挙動検知・情報収集	**A.5.22対応**
RS/RC（対応・復旧）： インシデント手順・BCP	**A.5.26対応**

ISMSは「管理の枠組み」、SCSは「技術実装水準の証明」— 両者は相互補完関係にある

ISMS取得済み組織へ

ISMSを既に取得・運用している組織にとって、SCS評価はスムーズに取り組めます

01

ISMS審査証跡の活用

ISMSで既に整備しているポリシー文書・手順書・台帳類の多くがSCS評価の証跡として転用可能。ゼロからの構築不要。

▶ **A.5.19～5.23 の証跡 → SCS GV/SC機能に直接対応**

02

ギャップ分析から始める

ISMS附属書Aとの対応表を使い、SCS要求事項との「カバレッジギャップ」を特定。技術的に不足する項目（ログ取得・MFA等）に集中して追加対応。

▶ **MSQAが提供する「フィット＆ギャップ分析」サービスで効率化**

03

審査効率の向上

SCS★4登録を取得することで、ISMS審査時にサプライヤー管理（A.5.19～5.23）の確認が効率化。審査員の深度ある確認に応えられる。

▶ **取引先・発注元への信頼証明としても活用可能**

04

ISMS審査員のスキルアップ

SCS評価従事者（★4）として認定されたISMS審査員は、サプライチェーン審査の専門性を証明。MSQAの専門家育成研修でCPD単位を取得できる。

▶ **MSQAは教育研修事業者として申請中（SCS-330B準拠）**

SCS評価制度が「スタートライン」になる

ISMS未取得組織へ

ISMSがなくても大丈夫。SCS評価制度はセキュリティ対策強化の出発点として最適です

STEP 1



現状把握（ギャップ分析）

SCS実装管理台帳（26～43項目）を使って現在のセキュリティ対策状況を棚卸し。何ができていて何が不足しているかを可視化する。

▶ **MSQA現状調査サービスで代行可能**

STEP 2

★3取得からスタート

まず★3確認（26要求事項/81基準）に取り組むことで、基本的なセキュリティ対策を体系的に整備。段階的な対応で無理なく進められる。

▶ **会員ツール 実装管理台帳で進捗管理**

STEP 3



★4評価で信頼を証明

★3で基盤を構築後、★4評価（43要求事項/153基準）で技術実装水準を第三者評価。取引先・発注元への強力な信頼証明となる。

▶ **MSQAの専門家が審査準備をサポート**

STEP 4



ISMS取得へのステップアップ（任意）

SCS対応で整備した証跡・台帳・手順書の多くはISMSの審査証拠として活用可能。
SCS→ISMS取得への自然なステップアップが実現できる。

▶ **MSQAのISMS内部監査支援で並走**

専門家育成と力量定義

SCS評価制度では「評価従事者の力量」が明確に定義されており、体系的な専門家育成が制度の根幹

力量定義の3区分（SCS-230）

★3確認従事者

・登録確認機関に所属　・自己評価結果の妥当性確認
・81評価基準の理解　・書類審査・ヒアリング実施

★4評価従事者

・登録審査機関に所属　・技術検証・ヒアリング・現地確認
・153評価基準の深い理解　・SCS-330B研修修了（CPD5単位）

主任評価従事者

・★4評価の統括　・評価チームのリード
・評価報告書の最終責任　・定期的な能力維持研修

MSQAの専門家育成への取り組み

★ MSQAは教育研修事業者として申請を進めています（SCS-330B準拠）

CPD研修（SCS評価制度） — 5単位
★4評価従事者向けCPD研修。NIST CSF 2.0・ISMS統合・ケーススタディ含む。修了でCPD 5単位取得。

フィット＆ギャップ分析 — 単独依頼可
現在のセキュリティ対策状況とSCS要求事項のギャップを専門家が分析。優先対応事項を明確化。

会員専用ツール提供 — 会員特典
実装管理台帳（★3:30項目、★4:43項目）・証跡管理台帳・ISMS27002対応表等をLMSで提供。

ISMS内部監査支援 — 相談無料
ISMS取得済み組織向けに審査員資格を持つメンバーが内部監査を実施。SCS対応にも対応。

SCS対応を効率化するMSQA提供ツール群

SCS実装管理台帳（★3版）

4シート構成（26項目）

実装管理台帳 / 進捗サマリー / 証跡管理台帳 / 記入ガイド

- ✓ 26要求事項・81評価基準を収録
- ✓ 実装状況をプルダウンで入力（未着手～完了）
- ✓ ISMS JIS Q 27001:2023 / 27002:2024 対応列あり
- ✓ 進捗サマリーシートで経営報告に活用

SCS実装管理台帳（★4完全版）

5シート構成（43項目）

実装管理台帳 / 評価基準詳細 / 進捗サマリー / 証跡管理台帳 / 記入ガイド

- ✓ 43要求事項・153評価基準を完全収録
- ✓ 評価基準詳細シートで審査根拠を参照可能
- ✓ 証跡管理台帳で保管場所・期間を一元管理
- ✓ 第三者評価申請前の最終チェックリストとして活用

SCS-ISMS 27002:2024 対応表

クロスリファレンス表

SCS要求事項 ⇔ JIS Q 27002:2024 管理策 相互参照

- ✓ SCS全項目とISMS附属書A管理策の対応関係
- ✓ 既存ISMS証跡の転用可能項目を即座に確認
- ✓ ギャップ分析の出発点として使用
- ✓ ISMS審査員のサプライヤー審査準備に活用

会員専用サイト（LMSコース）から全ツールをダウンロード可能 ｜ お問い合わせはMSQAまで

ISMS取得状況別の推奨パス

SCS評価制度 導入ロードマップ

■ ISMS取得済みの場合

Phase 1 （1～2ヶ月）	Phase 2 （2～4ヶ月）	Phase 3 （1ヶ月）	Phase 4 （1～2ヶ月）
ギャップ分析	**不足項目の追加対応**	**★3確認申請**	**★4評価申請**
ISMS証跡とSCS要求事項を照合。フィット＆ギャップ分析で差分特定。	ログ取得・MFA・脆弱性管理等の技術的不足項目を優先対応。	登録確認機関に申請。自己評価報告書・エビデンス提出。	登録審査機関に申請。技術検証・ヒアリング・現地確認を受審。

■ ISMS未取得の場合

Phase 1 （1～2ヶ月）	Phase 2 （3～6ヶ月）	Phase 3 （1～2ヶ月）	Phase 4 （6～12ヶ月）
現状調査（ギャップ分析）	**基本対策の整備**	**★3確認取得**	**★4評価 or ISMS取得**
実装管理台帳（30項目）で現状棚卸し。MSQAによる代行も可能。	★3の26要求事項に対応。方針策定・台帳整備・教育実施等を段階的に。	自己評価完了後に登録確認機関へ申請。初回は★3が最初の目標。	★4追加対応（17項目）かISMS取得かを状況に応じて選択。

MSQAはどのフェーズからでもサポートします

フィット＆ギャップ分析（単独依頼可） ／ 会員ツール（実装管理台帳） ／ CPD研修（★4評価従事者向け） ／ ISMS内部監査支援

よくある質問（FAQ）

Q SCS評価制度は必須ですか？強制されますか？

A 現時点では任意の評価制度です。ただし、大企業が取引先に対してSCS評価取得を要件化する動きが広がっており、事実上の要件になるケースが増えています。政府調達関連では要件化が進む可能性があります。

Q ISMSを取得していないと受けられませんか？

A いいえ、ISMS未取得でもSCS評価は受けられます。SCS評価制度はISMSとは独立した制度です。ただし、ISMSの基盤がある組織は取り組みがスムーズになります。まず★3確認から始めることをお勧めします。

Q 費用・期間はどのくらいかかりますか？

A 費用は登録機関によって異なります。期間は準備状況にもよりますが、現状対応済みの組織でも★3取得まで2〜4ヶ月、★4取得まで6〜12ヶ月程度が目安です。MSQAのギャップ分析から始めることで効率化できます。

Q MSQAの研修はいつ受講できますか？

A MSQAはSCS-330B研修実施基準に基づく教育研修事業者として申請を進めています。
受講申請は https://isms-society.stores.jp/reserve/msqaからご確認ください。最新情報はサイトにてご案内します。

Q 会員ツール（実装管理台帳等）はどこで入手できますか？

A MSQAの会員専用サイト（LMSコース）から入手できます。★3対応版（26項目）と★4完全版（43項目）の2種類を提供。ISMS 27002:2024との対応表も利用可能です。

Q フィット＆ギャップ分析だけ依頼することは可能ですか？

A はい、可能です。SCS評価制度への取り組み前の現状把握として、フィット＆ギャップ分析のみのご依頼も承っています。まずはお気軽にご相談ください。相談は無料です。

主要参考文献・関連資料

SCS評価制度	IPA公開資料	国際・国内規格
・SCS-230 研修事業者指定規則（2026年8月28日施行）	・IPA「情報セキュリティ10大脅威2026（組織編）」（2026年1月公表）	・JIS Q 27001:2023 情報セキュリティマネジメントシステム要求事項
・SCS-330B 研修実施基準（2026年9月11日施行）	・IPA「サプライチェーン・サイバーセキュリティ対策のガイドライン」	・JIS Q 27002:2024 情報セキュリティ管理策の実践のための規範
・SCS★3・★4 要求事項・評価基準（最新版）	・IPA「情報セキュリティ白書2025」	・NIST Cybersecurity Framework 2.0（2024年2月公表）

相談は無料です

ご相談・お問い合わせはお気軽に

現状調査（フィット&ギャップ分析）

導入のための現状調査のみのご依頼も可能。SCS実装管理台帳（26～43項目）で現在の対策状況を棚卸し。

会員専用ツール

実装管理台帳（★3:26項目、★4:43項目）、ISMS27002対応表等をLMSで提供。

SCS評価制度 解説研修

SCS-330B研修実施基準に基づくCPD研修。★4評価従事者向けに5単位取得可能。受講申請はQRから。

ISMS内部監査支援・審査準備サポート

ISMS取得済み組織向けに審査員資格を持つメンバーが内部監査を実施。SCS対応にも並走対応。

MSQA（Management System Quality Association）

解説研修のご案内・お申込みへ

QRコードからお申込みへ

MSQAご紹介・現状調査について

MSQAご紹介

現状調査

一般社団法人 マネジメントシステム品質協会（MSQA）