

SCS評価制度とISMSの違いとは？取得済み企業も対応が必要な理由

SCS評価制度（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）への対応を検討する企業から、特に多く出てくるのが「すでにISMS（ISO/IEC 27001）を取得していれば、SCS評価制度への対応は不要なのか」という疑問です。

結論からいえば、ISMSを取得済みであっても、SCS評価制度への対応が別途必要になる可能性があります。両者には共通する管理領域がある一方、制度の目的、評価方法、技術検証の有無、取引先との関係が異なるためです。ISMS認証はSCS評価制度の取得を自動的に代替するものではありません。

ただし、ISMSで整備した情報資産管理、リスクアセスメント、アクセス管理、委託先管理、インシデント対応、教育などの仕組みは、SCS評価制度への準備で大きな土台になります。重要なのは「ゼロから作り直す」のではなく、既存のISMS運用とSCSの要求事項を突き合わせ、不足部分だけを具体的に補強することです。

本記事では、2026年10月14日時点の公表情報をもとに、SCS評価制度とISMSの違い、ISMS取得済み企業が確認すべきポイント、Webアプリケーション診断・プラットフォーム診断・ペネトレーションテストとの関係、社内での進め方まで実務目線で解説します。

この記事で分かること

- SCS評価制度とISMS（ISO/IEC 27001）の目的・評価方法の違い
- ISMS取得済み企業でもSCS評価制度への対応が必要になり得る理由
- 既存のISMS文書・運用をSCS対応へ活用する方法
- ★3・★4で求められる評価と技術検証の考え方
- 対応プロジェクトの進め方、費用・期間を左右する要因、ベンダー選定のポイント

SCS評価制度とは何か

SCS評価制度は、サプライチェーンを構成する企業等のセキュリティ対策状況を共通の基準で可視化し、発注元と委託先の双方がセキュリティ水準を確認しやすくするための制度です。経済産業省と内閣官房国家サイバー統括室が2026年3月に制度構築方針を公表し、IPAが制度運営を担います。

IPAによると、★3は一般的なサイバー脅威に対処し得る水準、★4は初期侵入の防御だけでなく、侵入後の被害拡大防止や取引先のデータ・システム保護、サプライチェーン上の役割に応じた強靱化まで含む水準として整理されています。★3・★4は2027年3月頃の運用開始が予定されています。

出典：IPA「SCS評価制度の詳細情報」「よくある質問」

<https://www.ipa.go.jp/security/scs/details.html>

<https://www.ipa.go.jp/security/scs/faq.html>

★3は専門家確認付きの自己評価

★3では、企業が要求事項・評価基準に沿って自己評価を行い、SCS評価制度の要件を満たしたセキュリティ専門家による確認・助言を受けます。そのうえで経営層による自己適合宣誓を含む評価結果を事務局へ提出し、問題がなければ台帳へ登録・公表される流れです。単なる社内チェックではなく、専門家確認と経営層の関与が組み込まれている点が特徴です。

★4は第三者評価と技術検証が加わる

★4では、評価機関による第三者評価に加え、文書確認、実地審査、技術検証が行われます。IPAは技術検証事業者の主な対象として、脆弱性診断やペネトレーションテストを提供する法人を挙げています。つまり、規程や証跡が整っていることだけでなく、実際のIT環境に技術的な弱点が残っていないかを確認する考え方がより明確です。

出典:IPA「指定申請について(評価機関・技術検証事業者・研修事業者向け)」

<https://www.ipa.go.jp/security/scs/security-experts-organization/shiteishinsei.html>

ISMS(ISO/IEC 27001)とは何か

ISMSはInformation Security Management Systemの略で、情報セキュリティを組織として継続的に管理するための仕組みです。ISO/IEC 27001は、そのISMSに対する要求事項を定めた国際規格です。日本ではJIS Q 27001として国際規格との整合が図られています。

ISMSでは、個別のセキュリティ製品を導入すること自体を目的とするのではなく、自社が保有する情報や事業上のリスクを評価し、必要な管理策を選び、責任者・ルール・運用・監視・改善のサイクルを組織として回すことが重視されます。ISMS-ACが認定した認証機関の審査を受け、要求事項への適合が認められることで認証を取得できます。

出典:情報マネジメントシステム認定センター(ISMS-AC)「ISMS適合性評価制度の概要」

<https://isms.jp/isms/about.html>

SCS評価制度とISMSの違い

両者の最も大きな違いは、ISMSが「組織の情報セキュリティマネジメントの仕組み」を第三者が認証する制度であるのに対し、SCS評価制度は「サプライチェーンにおいて必要なサイバーセキュリティ対策の実施状況を可視化し、取引時の確認に活用しやすくする制度」である点です。

違い1:制度の目的

ISMSは、自社のリスクに基づいて情報セキュリティを継続的に管理し、マネジメントシステムとして機能させることを重視します。一方、SCS評価制度は、委託元から見て委託先の対策状況が分かりにくいことや、委託先が複数の取引先から異なるチェック項目を求められる負担を軽減することを背景に設計されています。

そのため、SCS評価制度は取引先管理、調達、外部委託、サプライチェーンリスクの文脈で利用される可能性が高い制度です。法律上の一律義務というより、発注条件や取引継続の判断材料として求められるケースに備える視点が重要になります。

違い2: 評価の考え方

ISMSは、自社の事業環境、情報資産、脅威、脆弱性を踏まえてリスクを評価し、必要な管理策を選択して運用するリスクベースのアプローチです。これに対しSCS評価制度では、★3・★4ごとに要求事項・評価基準が用意され、取得にはそれぞれ定められた要求事項・評価基準を満たす必要があります。

したがって、「ISMSの審査で問題がなかったから、SCSでもそのまま適合する」とは限りません。逆に、ISMSで適切に運用できている領域については、SCS評価の根拠資料や証跡として活用できる可能性があります。

違い3: 技術検証の位置付け

ISMS審査では、マネジメントシステムが適切に構築・運用されているかが中心となります。技術的な脆弱性診断を毎回必須とする制度ではありません。

一方、SCS評価制度の★4では技術検証が明示されています。対象のIT基盤やシステムの構成によっては、Webアプリケーション診断、プラットフォーム診断、脆弱性診断、ペネトレーションテストなどを通じて、設定不備や既知の脆弱性、認証・権限管理上の問題、攻撃経路を確認することが重要になります。

例えば、ISMS上は「脆弱性管理の手順」が整備されていても、実際の公開サーバーに重大な既知脆弱性が残っている、管理画面がインターネットへ露出している、クラウドのアクセス制御に過剰権限がある、といった状態は別問題です。SCS対応では、管理プロセスと実際の技術状態の両方を見る必要があります。

違い4: 取引先への説明材料としての使われ方

ISMS認証はすでに多くの企業で、委託先選定やセキュリティチェック時の信頼性を示す材料として利用されています。SCS評価制度はさらに、サプライチェーン上で求めるセキュリティ水準を共通化し、発注時等に対策状況を確認しやすくする目的を持っています。

今後、顧客企業が「重要な業務委託先には★3以上」「特に重要なシステムやデータを扱う委託先には★4」といった社内調達基準を設ける可能性があります。自社がISMS認証を取得していても、取引先がSCSの★取得を条件として設定すれば、別途対応が必要になります。

ISMS取得済み企業もSCS評価制度への対応が必要？

はい、必要になる可能性があります。特に、大企業や重要インフラ企業の取引先、顧客情報・機密情報を預かる事業者、クラウド・システム運用を担う事業者、製造業のサプライヤー、BPO・ITサービス事業者は、取引先から具体的な水準を求められる可能性を想定して準備しておくことが合理的です。

ただし、ISMS取得済み企業には大きな優位性があります。規程、情報資産台帳、リスクアセスメント、教育記録、委託先管理、アクセス管理、インシデント対応手順、内部監査、経営レビューなど、SCS対応に関連する文書や運用実績がすでに存在するためです。

したがって実務では、「ISMSとは別の制度だから全部作り直す」のではなく、SCS要求事項と既存ISMSの管理策・証跡をマッピングし、差分を埋める方法が効率的です。

ISMS取得済み企業が最初に確認すべき5つのポイント

1. ISMSの認証範囲とSCSで想定する対象範囲が一致しているか

ISMS認証は、組織全体ではなく特定の部門・拠点・サービスを認証範囲としている場合があります。SCS評価制度で顧客から求められる対象が、ISMSの認証範囲外にあるシステムや子会社、拠点、クラウド環境であれば、既存認証だけでは十分な説明になりません。

最初に、取引先へ提供しているサービス、保存・処理している情報、利用しているシステム、外部委託先、ネットワーク境界を整理し、どこをSCS対応の対象とするかを明確にします。

2. 規程だけでなく運用証跡が残っているか

規程が存在していても、アカウント棚卸しの記録、パッチ適用履歴、教育受講記録、インシデント訓練記録、バックアップ復元試験結果などが残っていなければ、実際に運用されていることを説明しにくくなります。

SCS対応を見据えるなら、既存のISMS運用を「監査で見せるための文書」ではなく、「現場で実施し、証跡を残す仕組み」として再確認することが重要です。

3. 実システムの脆弱性を把握できているか

情報システム部門は、インターネット公開資産、Webアプリケーション、サーバー、ネットワーク機器、クラウド環境を一覧化し、脆弱性管理の対象漏れがないか確認します。

Webアプリケーションでは認証回避、アクセス制御不備、SQLインジェクション、クロスサイトスクリプティングなど、プラットフォームでは古いミドルウェア、不要ポート、脆弱な暗号設定、管理インターフェースの露出などが代表的な確認対象です。重要度の高い環境では、単純なスキャンだけでなく、攻撃者の視点で侵入可能性や横展開を確認するペネトレーションテストが有効な場合があります。

4. 委託先・再委託先まで管理できているか

サプライチェーンリスクは、自社だけで完結しません。クラウド事業者、開発会社、運用保守会社、コールセンター、物流会社など、自社の事業継続や機密情報に影響する委託先を整理し、契約上のセキュリティ要求、事故報告、再委託、アクセス権限、データ返却・消去などの管理状況を確認します。

5. 経営層がリスクと投資判断に関与できているか

SCS評価制度の★3では経営層による自己適合宣誓が想定されています。セキュリティを情報システム部門だけの作業にせず、どの取引を守るのか、どこまで投資するのか、未対応リスクを受容するのかを経営判断として整理する必要があります。

SCS評価制度への対応を進める具体的な手順

ステップ1: 取引先から求められる水準を確認する

まず、主要顧客や親会社、調達部門からSCS評価制度に関する要求が出ているかを確認します。現時点で明示されていなくても、取引更新、入札、監査、セキュリティチェックシート改定のタイミングで要求が追加される可能性があります。売上依存度や契約上の重要性を踏まえ、優先順位を付けます。

ステップ2: 既存ISMSとSCS要求事項をマッピングする

情報セキュリティ方針、リスクアセスメント、適用宣言書、情報資産台帳、組織体制、教育記録、委託先管理、アクセス管理、ログ管理、バックアップ、脆弱性管理、インシデント対応、事業継続関連資料などを収集し、SCS要求事項との対応関係を整理します。

ここで「対応済み」「一部対応」「未対応」「証跡不足」に分類すると、追加対策の全体像が見えやすくなります。

ステップ3: 技術面の現状を確認する

文書確認と並行して、IT資産の棚卸し、外部公開資産の確認、脆弱性診断などを実施します。対象範囲が広い企業では、全システムを一度に診断するのではなく、顧客データを扱う環境、インターネット公開システム、特権アクセスが集中する基盤など、リスクの高い領域から着手すると現実的です。

ステップ4: ギャップをリスクベースで改善する

未対応項目をすべて同じ優先度で処理すると、費用も期間も膨らみます。外部から侵入される可能性、扱う情報の重要性、事業停止時の影響、取引先への波及、是正コストを踏まえて優先順位を付けます。

例えば、インターネット公開システムの重大な脆弱性、特権IDの多要素認証未導入、バックアップからの復旧不能、インシデント時の連絡体制不備などは、単なる文書体裁より優先度が高くなることがあります。

ステップ5: 評価に備えて証跡を整える

改善後は、規程だけでなく実施証跡を揃えます。成果物としては、対象範囲一覧、要求事項対応表、ギャップ分析結果、改善計画、診断報告書、是正記録、教育実績、インシデント対応訓練記録、経営層への報告資料などを整理しておく、評価対応が進めやすくなります。

期間と費用を左右する要因

SCS評価制度への対応期間や費用は、企業規模だけでは決まりません。既存のISMS成熟度、対象範囲、拠点数、システム数、クラウド利用状況、外部公開資産、委託先数、必要な技術診断、現状の証跡整備状況などで大きく変わります。

ISMS取得済みで運用が定着している企業は、文書整備の工数を抑えやすい一方、技術検証で重大な課題が見つかれば、改修費や再診断費用が発生します。また、複数事業を一括で対象にするか、主要サービスから段階的に対象化するかでプロジェクト規模は変わります。

社内稟議では「制度取得費用」だけを説明するのではなく、重要顧客との取引継続、入札要件への対応、委託先監査への回答工数削減、セキュリティ事故による事業停止リスクの低減といった事業上の目的を合わせて示すと、投資判断につながりやすくなります。

SCS評価制度の支援会社を選ぶポイント

支援会社を選ぶ際は、規程作成だけを行う会社か、技術診断だけを行う会社かではなく、制度要求と技術対策を横断して支援できるかを確認することが重要です。

RFPや見積依頼では、SCS要求事項とのギャップ分析、既存ISMS文書の活用範囲、対象範囲の決定支援、脆弱性診断・ペネトレーションテストの実施可否、改善計画の作成、再診断、証跡整備、経営層向け報告まで、どこまで含まれるのかを確認します。

また、診断で個人情報や機密情報に触れる可能性がある場合は、データの保存場所、アクセス権限、再委託、報告書の保管・廃棄、インシデント発生時の連絡方法について契約前に確認しておく必要があります。

よくある失敗と注意点

「ISMSがあるから大丈夫」と判断して差分確認をしない

最も避けたいのは、ISMS認証をSCS適合の証明と同一視することです。重複する領域は多くても、SCS独自の要求や技術検証を確認しなければ不足を見落としします。

評価直前に診断を実施し、改修期間が取れない

脆弱性診断で重大な問題が見つかる可能性を考えると、評価直前ではなく早めに技術確認を行う方が安全です。改修、テスト、再診断までを含めて計画します。

情報システム部門だけで進める

契約、調達、委託先管理、教育、事業継続、経営判断は複数部門にまたがります。管理部門、法務、調達、営業、事業部門、経営層を早期に巻き込むことで、後戻りを減らせます。

Librus株式会社が提供できるSCS評価制度対応支援

Librus株式会社では、SCS評価制度への対応を、チェックリストの作成だけで終わらせず、現状分析、技術検証、改善、運用まで一気通貫で支援します。

ISMS取得済み企業に対しては、既存の規程・リスクアセスメント・運用証跡を活かしながらSCS要求事項とのギャップを整理し、追加対応が必要な領域を明確化します。ISMSを未取得の企業についても、SCS取得に必要な体制・ルール・技術対策を企業規模や取引状況に応じて設計できます。

技術面では、Webアプリケーション診断、プラットフォーム診断、ペネトレーションテスト、レッドチーム演習などを組み合わせ、制度上の要求と実システムのリスクを結び付けて確認します。診断で課題が見つかった場合も、優先順位付け、改善方針、再診断、継続運用まで支援可能です。

さらに、経営層向けのリスク整理、情報システム部門と現場部門の役割整理、取引先監査への対応、SOC／CSIRT構築・運用支援、インシデントレスポンス、教育・訓練など、SCS評価制度の取得後を見据えた運用設計にも対応します。

よくある質問

Q1. ISMSを取得していればSCS評価制度の★3・★4も取得済み扱いになりますか？

いいえ。ISMS認証とSCS評価制度は別の制度です。ISMS取得済みであっても、SCSの要求事項・評価基準に沿った評価・申請が必要です。ただし、既存のISMS文書や運用証跡を活用できる領域は多くあります。

Q2. SCS評価制度に対応するためにISMSを取得する必要がありますか？

SCS評価制度の取得要件として、企業がISMS認証を事前取得しなければならないとは公表されていません。SCSの要求事項に適合する体制と対策を整備することが重要です。

Q3. ISMSとSCS評価制度はどちらを優先すべきですか？

取引先要求と自社の経営目的によって異なります。取引先からSCSの★取得を求められる可能性が高い場合はSCS対応を優先しつつ、中長期的な情報セキュリティ管理の基盤としてISMSを活用する方法も考えられます。すでにISMS取得済みであれば、その仕組みをSCS対応の土台として利用するのが効率的です。

Q4. ★4では脆弱性診断やペネトレーションテストが必須ですか？

★4では技術検証が制度上明示されています。具体的な検証内容は対象環境や評価手順に従って決まります。IPAは技術検証事業者の業務として脆弱性診断を挙げており、対象によってはWebアプリケーション診断、プラットフォーム診断、ペネトレーションテスト等が関連します。

Q5. ★3を取得してからでないと★4を取得できませんか？

いいえ。IPAは、上位段階が下位段階の事項を包含するものの、★3を事前取得していなければ★4を取得できない関係ではないと説明しています。自社の取引上の必要性和現状のセキュリティ水準を踏まえて検討します。

Q6. SCS評価制度への対応はいつから始めるべきですか？

★3・★4は2027年3月頃の運用開始が予定されています。対象範囲整理、ギャップ分析、技術診断、改修、証跡整備には一定の期間が必要になるため、主要取引先から要求される可能性がある企業は、制度開始前から現状確認を進めることが望ましいでしょう。

Q7. まだ★3と★4のどちらを目指すか決まっていなくても相談できますか？

可能です。まず取引先から想定される要求、自社の事業・システム・情報の重要度、現状のISMS運用や技術対策を整理することで、どの水準を目指すべきか判断しやすくなります。

まとめ：ISMS取得済みでも、SCS評価制度は「差分確認」が必要

SCS評価制度とISMS（ISO/IEC 27001）は、いずれも企業の情報セキュリティ向上に役立つ仕組みですが、目的と評価方法は同じではありません。ISMSは情報セキュリティマネジメントシステムを継続的に運用する枠組みであり、SCS評価制度はサプライチェーンにおけるセキュリティ対策状況を共通基準で可視化し、取引時に活用しやすくする制度です。

そのため、ISMS認証を取得済みでもSCSへの対応が不要になるわけではありません。一方で、ISMSで蓄積した規程、リスクアセスメント、運用証跡、内部監査などは大きな資産です。既存の仕組みをSCS要求事項へマッピングし、技術面を含む不足箇所だけを補強することで、効率的な準備が可能になります。

特に重要なのは、制度取得だけを目的にせず、主要取引先との関係、事業継続、顧客データの保護、実際のシステムリスクまで含めて対応計画を作ることです。

SCS評価制度と既存ISMSの整理からご相談いただけます

「ISMSを取得しているが、SCS評価制度で何が追加になるのか分からない」「★3と★4のどちらを目指すべきか判断できない」「取引先から求められる前に準備しておきたい」といった段階でもご相談いただけます。

Librus株式会社では、既存のISMS文書・運用状況を確認したうえで、SCS要求事項とのギャップ、追加で必要な技術対策、脆弱性診断やペネトレーションテストの対象、改善優先順位を整理します。対象範囲や実施方法がまだ決まっていない場合でも、事業上の重要度や取引先との関係を踏まえて、過不足のない進め方を検討できます。

制度対応を単なる認証取得の作業にせず、取引先への説明力向上と実際のセキュリティ強化を同時に進めたい場合は、現状整理の段階からご相談ください。

参考・出典

IPA「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）」:

<https://www.ipa.go.jp/security/scs/index.html>

IPA「SCS評価制度の詳細情報」: <https://www.ipa.go.jp/security/scs/details.html>

IPA「要求事項・評価基準」: <https://www.ipa.go.jp/security/scs/requirements-criteria.html>

IPA「よくある質問」: <https://www.ipa.go.jp/security/scs/faq.html>

IPA「指定申請について（評価機関・技術検証事業者・研修事業者向け）」:

<https://www.ipa.go.jp/security/scs/security-experts-organization/shiteishinsei.html>

ISMS-AC「情報セキュリティマネジメントシステム（ISMS）適合性評価制度の概要」:

<https://isms.jp/isms/about.html>

監修者

鎌田光一郎: 青山学院大学法学部卒業。SMBC日興証券株式会社にて証券営業、経営管理業務に従事したのちPwCコンサルティング合同会社に転籍。金融機関に対するコンサルティング業務に従事。その後、Librus株式会社を設立、代表取締役役に就任。

お問い合わせ先

Librus株式会社（代表取締役 鎌田光一郎）

105-0004 東京都港区新橋6丁目13-12 VORT新橋Ⅱ 4F

03-6772-8015

お問い合わせフォーム

<https://librus.co.jp/contact>