SCS評価制度とISMS・ISO27001の違い｜既存認証を活かした対応方法

SCS評価制度への対応を検討する企業の中には、「すでにISMS（ISO/IEC 27001）を取得しているため、追加対応は不要ではないか」と考える方も少なくありません。結論からいえば、ISMS認証はSCS評価制度への対応を大きく効率化できる重要な土台ですが、ISMSを取得しているだけでSCS評価制度の★3・★4を自動的に取得できるわけではありません。

両者はどちらも情報セキュリティを扱いますが、目的と評価の考え方が異なります。ISMSは、組織が情報セキュリティを継続的に管理するためのマネジメントシステムをISO/IEC 27001に基づいて第三者が認証する仕組みです。一方、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）は、取引先・委託先のセキュリティ対策状況を共通の基準で可視化し、サプライチェーン全体のリスク低減につなげることを目的としています。

そのため、ISMS取得済み企業にとっての実務上のポイントは「新しい制度だからゼロから作り直す」ことではなく、既存のISMS文書・運用・証跡を棚卸しし、SCS評価制度で追加的に求められる具体的な対策や技術検証との差分を埋めることです。本記事では、両制度の違いと共通点、既存認証を活かす具体的な進め方を解説します。

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る理由
- ISMSの規程・リスクアセスメント・監査記録などをSCS対応へ転用する方法
- ★3・★4で追加確認しやすい技術対策と証跡
- 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をどう位置付けるか
- 費用と期間を抑えながらSCS評価制度へ対応するための進め方

SCS評価制度とISMS（ISO27001）は何が違うのか

最も大きな違いは、ISMSが「組織として情報セキュリティを継続的に管理する仕組み」を評価する制度であるのに対し、SCS評価制度は「サプライチェーン上の取引先として、共通に求められるセキュリティ対策を実装しているか」を段階別に可視化する制度である点です。

ISMS適合性評価制度では、JIS Q 27001（ISO/IEC 27001）を認証基準として、情報セキュリティ方針、リスクアセスメント、リスク対応、内部監査、マネジメントレビュー、継続的改善といったマネジメントシステム全体の適合性を第三者である認証機関が評価します。

これに対してSCS評価制度では、★3はセキュリティ専門家の確認を伴う自己評価、★4は評価機関による第三者評価と技術検証が予定されています。IPAは、★3・★4を取得するには、それぞれに定められたすべての要求事項・評価基準を満たす必要があるとしています。

比較項目	ISMS（ISO/IEC 27001）	SCS評価制度
主な目的	情報セキュリティマネジメントの継続的な確立・運用・改善	取引・委託におけるセキュリティ対策水準の可視化とサプライチェーンリスク低減

評価の考え方	リスクベースで組織が必要な管理策を選定し運用	★ごとに定められた要求事項・評価基準への適合を確認
評価主体	認証機関による第三者認証	★3：専門家確認付き自己評価／★4：第三者評価＋技術検証
主な活用場面	顧客への信頼性説明、内部統制、継続的改善	調達・委託先管理、取引条件、サプライチェーン管理
技術面	管理策の選定はリスクアセスメントに基づく	★4では文書確認に加え実地審査・技術検証を実施
ISMS取得済み企業への意味	既存の管理体系をそのまま土台にできる	差分確認と不足対策が必要。ISMS認証のみで自動取得にはならない

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

なぜISMS取得済みでもSCS評価制度への対応が必要なのか

理由1：評価する目的が異なる

ISMSは、組織の情報セキュリティマネジメントを継続的に改善するための国際規格です。企業ごとの事業特性やリスクに応じて管理策を選び、リスクを受容するか、低減するか、移転するかなどを判断します。したがって、認証取得企業同士であっても、実装している具体的な対策が完全に同じになるとは限りません。

一方、SCS評価制度は、取引先ごとに異なるチェックシートや要求を共通化し、委託元が委託先の対策状況を確認しやすくすることを狙っています。取引時に「この★水準を満たしているか」を確認できるようにするため、共通の最低ラインを具体的に示す性格が強い制度です。

理由2：★3・★4は定められた要求事項をすべて満たす必要がある

IPAのFAQでは、★3・★4の取得には、それぞれで定められたすべての要求事項・評価基準を満たす必要があるとされています。ISMSのリスクベースアプローチで適切と判断した管理方法であっても、SCS側で明示された基準との間に差分があれば、その部分を追加で整備する必要があります。

出典：IPA「SCS評価制度 よくある質問」https://www.ipa.go.jp/security/scs/faq.html

理由3：★4では技術検証が組み込まれる

★4では、評価機関による文書確認と実地審査に加え、技術検証が求められます。ここがISMS運用だけでは埋まりにくい代表的な差分です。外部公開資産、ネットワーク、Webアプリケーション、クラウド設定などについて、実際の攻撃可能性を技術的に確認する場面が生じます。

そのため、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などを、単発のセキュリティ施策としてではなく、「SCS評価制度で要求される対策を技術面から裏付ける活動」として整理することが重要です。

既存のISMS認証はSCS対応にどう活かせるか

ISMS取得済み企業の最大の利点は、SCS評価制度への対応に必要な「管理の骨格」がすでに存在していることです。特に従業員100～1,000名規模の企業では、規程を一から新設するよりも、既存のISMS文書と運用証跡をSCS要求事項へマッピングする方が、社内負荷と外部委託費の両方を抑えやすくなります。

情報セキュリティ方針・規程類を流用する

ISMSで整備している情報セキュリティ方針、アクセス管理規程、情報資産管理規程、インシデント対応手順、委託先管理規程、バックアップ規程、教育規程などは、SCS評価制度の要求事項を満たすための基礎資料として活用できます。重要なのは文書名をSCS向けに変えることではなく、SCS要求事項が求める内容が実際に規定され、運用されているかを確認することです。

リスクアセスメント結果を対象範囲の決定に使う

ISMSで保有している情報資産台帳、リスクアセスメント表、適用宣言書、ネットワーク構成図は、SCSの適用範囲を決める際に有効です。特に、重要な顧客情報を扱うシステム、外部公開サーバー、VPN、クラウドサービス、業務委託先との接続点などを洗い出す際には、既存のリスク分析結果を利用できます。

内部監査・教育・マネジメントレビューの証跡を活用する

ISMS運用では、教育受講記録、内部監査報告、是正処置記録、マネジメントレビュー議事録などが継続的に残ります。SCS評価でも「規程がある」だけでなく、「実際に運用されている」ことを示す証跡が重要になるため、こうした記録は有力な説明資料になります。

供給者管理・委託先管理の仕組みを発展させる

SCS評価制度はサプライチェーンリスクを直接の対象としています。ISMSで実施している委託先評価、秘密保持契約、再委託管理、クラウドサービス評価、契約終了時の情報返却・削除などの仕組みを、SCSの要求事項に照らして具体化すると効率的です。

ISMS取得済み企業が確認すべき主な追加ギャップ

実務では、ISMSとSCSの要求事項を1項目ずつ比較する「ギャップ分析」を行います。特に確認したいのは、次の領域です。

- 外部公開システムやネットワーク機器の脆弱性管理が、規程だけでなく定期的な確認・是正まで運用されているか
- 管理者アカウント、多要素認証、権限棚卸しなどのアクセス管理が実装され、証跡が残っているか
- EDR、ログ監視、異常検知など侵入後を想定した監視・検知策が機能しているか
- インシデント対応手順が机上の規程ではなく、連絡網、初動判断、証拠保全、復旧まで具体化されているか
- バックアップが本番環境と適切に分離され、復旧テストまで行われているか
- 委託先・再委託先のセキュリティ要求と確認方法が契約・運用に反映されているか
- 技術検証の対象となる可能性があるシステムについて、診断結果と是正状況を説明できるか

この段階で重要なのは、すべてを同じ優先順位で改善しないことです。取引先から求められる★水準、重要システム、インターネット公開範囲、情報の機密性、事業停止時の影響を基準に、優先順位を付けて改善します。

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の位置付け

既存のISMS取得企業でも、技術的な安全性を客観的に説明できないケースは珍しくありません。例えば「脆弱性管理規程はあるが、公開Webサービスを最後に診断したのが数年前」「サーバーのパッチ適用ルールはあるが、外部から見える不要ポートを確認していない」といった状態です。

Webアプリケーション診断

Webアプリケーション診断では、認証・認可の不備、SQLインジェクション、クロスサイトスクリプティング、セッション管理、入力値検証など、アプリケーション固有の脆弱性を確認します。顧客向けポータル、EC、SaaS、自社業務システムを外部公開している企業では重要度が高い領域です。

プラットフォーム診断

プラットフォーム診断は、サーバー、ネットワーク機器、OS、ミドルウェア、公開ポート、既知の脆弱性などを確認します。VPN装置やファイアウォール、クラウド上の公開サーバーは、サプライチェーン経由の侵入経路になり得るため、継続的な点検が必要です。

ペネトレーションテスト

ペネトレーションテストは、個別の脆弱性の有無だけでなく、複数の弱点を組み合わせた場合にどこまで侵入・権限拡大・情報到達が可能かを攻撃者視点で確認します。重要事業や機密情報を扱うシステムでは、診断結果を経営リスクとして評価するうえで有効です。

なお、どの技術検証をどの範囲で実施すべきかは、SCSの取得段階、評価対象範囲、システム構成によって異なります。不要な診断を広く実施するより、制度要求と事業リスクに沿って対象を決める方が費用対効果は高くなります。

既存認証を活かしたSCS評価制度対応の進め方

ステップ1：経営層が取得目的と目標★を決める

まず、「取引先から求められる可能性がある」「大手企業との新規取引を想定している」「自社のセキュリティ水準を客観的に示したい」など、取得目的を整理します。★3と★4では評価方法や準備負荷が異なるため、経営層が事業上の必要性を踏まえて目標を決めることが重要です。

ステップ2：ISMS文書とSCS要求事項をマッピングする

情報セキュリティ方針、適用宣言書、各種規程、リスクアセスメント、委託先管理、教育、内部監査などを、SCSの要求事項・評価基準と対応付けます。「既に満たしている」「一部不足」「未対応」「証跡不足」に分類すると、追加作業を可視化できます。

ステップ3：不足している証跡と技術対策を確認する

規程は存在しても、実施記録が残っていないケースがあります。アカウント棚卸し記録、脆弱性対応履歴、バックアップ復旧テスト、教育受講記録、インシデント訓練結果など、実施を証明できる記録を整理します。同時に、Webアプリケーション診断やプラットフォーム診断など技術面の不足も確認します。

ステップ4：事業影響を基準に改善順位を決める

改善項目は、重大な脆弱性、インターネットから直接攻撃される資産、特権ID、顧客情報、基幹業務、復旧困難なシステムなどから優先します。単純な「項目数」ではなく、事故時の売上停止、取引停止、復旧費用、信用毀損への影響で順位を付けることが経営判断として重要です。

ステップ5：審査・評価を想定した証跡セットを作る

評価時に担当者が社内を探し回らないよう、要求事項ごとに規程、手順書、実施記録、システム画面、診断報告書、是正記録をひも付けます。ISMSの審査資料をベースにSCS用の証跡台帳を作ると、更新対応や取引先からの問い合わせにも再利用できます。

実施期間と費用を左右する要因

ISMS取得済み企業では、未取得企業に比べて規程整備や管理体制の構築を短縮できる可能性があります。しかし、期間と費用は、ISMS認証の有無だけでは決まりません。

特に影響が大きいのは、対象拠点数、外部公開システム数、クラウド環境の数、委託先の数、既存文書の整備状況、運用証跡の量、脆弱性診断・ペネトレーションテストの対象範囲、発見された問題の改修難易度です。

社内稟議では「SCSの申請費用」だけでなく、ギャップ分析、規程改定、システム設定変更、診断、改善、再確認、社内工数を分けて説明すると予算の妥当性を示しやすくなります。また、取引要件への対応、新規取引機会、顧客監査対応工数の削減、事故発生時の損失抑制といった事業効果も合わせて整理すると、単なるコンプライアンス費用として扱われにくくなります。

SCS対応支援会社を選ぶ際のポイント

ISMS取得済み企業が外部支援を利用する場合、単に規程テンプレートを提供する事業者ではなく、既存ISMSとの重複を見極め、必要最小限の追加対策に整理できる会社を選ぶことが重要です。

- ISMS／ISO 27001とSCS評価制度の双方を理解しているか
- 規程・リスク管理だけでなく、ネットワークやWebアプリケーションの技術対策まで支援できるか
- 脆弱性診断やペネトレーションテストを制度対応と一体で設計できるか
- 要求事項ごとの証跡整理、是正計画、経営報告まで支援できるか
- 評価対象範囲を過度に広げず、事業リスクに応じて設計できるか
- 個人情報や機密情報を扱う資料の管理方法、再委託方針が明確か

RFPや見積依頼では、「SCS取得支援一式」だけでなく、ギャップ分析、文書改定、証跡整備、技術診断、改善支援、評価前レビューを分けて見積もってもらうと、比較しやすくなります。

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

既存認証は大きな強みですが、SCSは目的と評価基準が異なります。まず要求事項をマッピングし、差分を客観的に確認する必要があります。

規程だけ追加して運用証跡が残っていない

審査・評価では、ルールの存在だけでなく実際に運用しているかが重要です。新しい規程を増やしすぎると現場運用が追い付かないため、既存ISMSの仕組みに統合する方が継続しやすくなります。

診断結果を取得しただけで改善が止まる

脆弱性診断は「発見」が目的ではありません。重大度、悪用可能性、対象システムの重要度を踏まえて改修順位を決め、修正後の再確認まで実施する必要があります。

情報システム部門だけで進める

SCS評価制度は取引や委託管理と密接に関係するため、経営層、情報システム部門だけでなく、営業、調達、法務、総務、事業部門の関与が必要です。特に取引先から要求される★水準や契約更新時期は営業・調達部門が把握しているケースがあります。

Librus株式会社が提供できる支援

Librus株式会社では、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）への対応を、制度要件の確認だけで終わらせず、技術対策と運用改善まで一気通貫で支援します。

ISMS取得済み企業に対しては、既存の情報セキュリティ方針、規程、リスクアセスメント、内部監査資料、委託先管理、教育記録などを確認し、SCS要求事項との対応関係を整理します。そのうえで、不足している証跡、技術対策、運用プロセスのみを優先して改善することで、重複投資を抑えた対応を目指します。

また、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、SOC／CSIRT支援、インシデントレスポンス、デジタルフォレンジック、SBOM、リスクアセスメントなどを組み合わせ、制度対応で見つかった課題を実装・改善までつなげることが可能です。経営層には事業・財務・取引上のリスクとして整理し、情報システム部門には具体的な技術課題と優先順位として提示するなど、経営と現場の双方が判断しやすい形で支援します。

よくある質問

ISMSを取得していればSCS評価制度の★3・★4は自動的に取得できますか？

いいえ。ISMS認証とSCS評価制度は別制度です。IPAは、★3・★4の取得には各段階で定められたすべての要求事項・評価基準を満たす必要があるとしています。ISMSの規程や運用は有効に活用できますが、差分確認が必要です。

ISMSを取得済みならSCS対応の負担は小さくなりますか？

既存の方針、規程、リスクアセスメント、内部監査、教育、委託先管理、証跡を活用できるため、ゼロから体制を作る企業より効率化できる可能性があります。ただし、技術対策や証跡が不足していれば追加対応が必要です。

ISO27001の適用範囲とSCSの対象範囲は同じにすべきですか？

必ずしも同一とは限りません。取引先から求められる範囲や重要システム、サプライチェーン上の役割を踏まえてSCSの対象範囲を整理する必要があります。

SCS対応では脆弱性診断が必須ですか？

必要となる技術検証の具体的な範囲は取得段階や対象環境によって異なります。特に★4では技術検証が組み込まれるため、外部公開資産や重要システムについて診断が必要になる可能性があります。

ISMSの内部監査報告書はSCSの証跡に使えますか？

要求事項との対応関係を説明でき、対象期間や実施内容が適切であれば有力な証跡になります。内部監査だけで不足する項目については、追加の実施記録や技術資料を用意します。

SCS対応のためにISMS規程を全面改定する必要がありますか？

通常は全面改定から始める必要はありません。まず既存文書を要求事項へマッピングし、足りない内容だけを改定・追加する方が運用負荷を抑えやすくなります。

★3と★4のどちらを目指すべきですか？

取引先から求められる水準、事業の重要性、扱う情報、供給停止時の影響などで判断します。★4は第三者評価と技術検証を伴うため、準備負荷も大きくなります。

いつから準備を始めるべきですか？

★3・★4は2027年3月頃の運用開始が予定されています。規程改定だけでなく運用実績や是正期間が必要になるため、取引先から要求されてから着手するのではなく、早めにギャップ分析を行うことが有効です。

まとめ｜ISMSを「土台」にしてSCS評価制度の差分を埋める

SCS評価制度とISMS（ISO/IEC 27001）は、同じ情報セキュリティ領域の制度でも目的と評価方法が異なります。ISMSは組織のリスクに応じて情報セキュリティマネジメントを継続的に運用するための国際規格であり、SCS評価制度はサプライチェーン上で共通に求めるセキュリティ対策水準を可視化する制度です。

したがって、ISMS取得済み企業もSCS対応が不要になるわけではありません。しかし、既存の規程、リスクアセスメント、内部監査、教育、委託先管理、改善活動はSCS対応の大きな資産になります。最初に行うべきことは、新しい文書を大量に作ることではなく、既存ISMSとSCS要求事項のギャップを整理することです。

そのうえで、証跡不足、アクセス制御、脆弱性管理、監視・検知、インシデント対応、バックアップ、委託先管理、技術検証などを優先順位に沿って改善すれば、制度対応と実際のセキュリティ強化を同時に進められます。

SCS評価制度は2027年3月頃の★3・★4運用開始が予定されています。今の段階でISMS資産を棚卸しし、差分と必要予算を把握しておけば、取引先から要求された際にも対応計画を立てやすくなります。

既存ISMSを活かしたSCS評価制度対応をご相談いただけます

Librus株式会社では、「ISMSは取得しているが、SCS評価制度で何が追加になるのか分からない」「★3・★4のどちらを目指すべきか決まっていない」「規程はあるが、技術面や証跡に不安がある」といった段階からご相談いただけます。

既存のISMS文書・運用を確認し、SCS要求事項との重複部分と不足部分を整理することで、不要な規程作成や重複投資を避けながら、実務に即した対応計画を立てることができます。必要に応じて、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、運用体制整備、改善支援まで一気通貫で対応します。対象範囲や実施方法がまだ固まっていない場合でも、取引状況・システム構成・既存認証を踏まえ、優先順位と進め方の整理から支援可能です。

参考情報

- 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
- 経済産業省「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」
  https://www.meti.go.jp/press/2025/03/20260327001/20260327001.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