

SCS評価制度とPマークの違い | 既存認証があれば対応不要？

結論からいえば、Pマーク(プライバシーマーク)を取得している企業でも、SCS評価制度への対応が自動的に不要になるわけではありません。両制度には、規程整備、教育、委託先管理、インシデント対応など共通する要素がありますが、制度の目的と評価するリスクの範囲が異なります。Pマークは個人情報の適切な取扱いを中心に評価する一方、SCS評価制度はサプライチェーンを通じたサイバー攻撃や事業停止、機密情報の漏えい、踏み台化などのリスクに対するセキュリティ対策水準を可視化する仕組みです。

そのため、Pマークを保有している企業は「ゼロから準備する」必要はない場合が多いものの、既存の個人情報保護体制をSCS評価制度の要求事項に照らして棚卸しし、不足する技術対策やサプライチェーン管理、ログ監視、脆弱性管理などを追加することが実務的な進め方です。

この記事で分かること

この記事では、SCS評価制度とPマークの違い、Pマーク取得企業がそのままSCS評価制度に対応できるのか、どの領域を追加で確認すべきか、社内でどのように準備を進めればよいかを解説します。特に、従業員100～1,000名規模の企業が、取引先からセキュリティ水準の説明を求められる場面を想定し、経営・情報システム・管理部门が確認すべき実務ポイントを整理します。

SCS評価制度とPマークは何が違うのか

Pマークは「個人情報の適切な取扱い」を評価する制度

プライバシーマーク制度は、JIS Q 15001「個人情報保護マネジメントシステム—要求事項」に準拠した運用指針に基づき、個人情報について適切な保護措置を講ずる体制を整備している事業者を評価し、マークの使用を認める制度です。JIPDECによれば、Pマークは法人単位で付与され、個人情報保護マネジメントシステム(PMS)の構築と運用が重視されます。

つまり、Pマークの中心テーマは「個人情報をどのように取得し、利用し、保管し、委託し、廃棄するか」「個人情報の取扱いに関するルールをどのように継続運用するか」です。もちろん安全管理措置としてアクセス制御や認証、教育、委託先管理、事故対応なども含まれますが、評価の出発点は個人情報保護です。

SCS評価制度は「サプライチェーンのサイバーリスク」を評価する制度

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)は、取引関係を通じたサイバーリスクに対応するため、企業のセキュリティ対策実施状況を段階別の★で可視化する制度です。IPAは、委託先への攻撃を起点とする事業・サービス停止、機密情報の漏えい・改ざん、委託先を踏み台とした不正侵入などのリスクへの対策を促進することを目的として示しています。

★3は一般的なサイバー脅威への対処を想定し、専門家確認付きの自己評価を基本とします。★4は、初期侵入防御だけでなく、侵入後の被害拡大防止やサプライチェーン上の役割に応じた対策まで求め、第三者評価・実地審査・技術検証を含む仕組みです。★3・★4は2027年3月頃の運用開始が予定されています。

違いを一言で表すと「守る対象」と「確認方法」が異なる

PマークとSCS評価制度は、どちらも社内規程、責任体制、教育、委託先管理などを扱うため、実務担当者から見ると似て見える部分があります。しかし、Pマークは個人情報保護を軸としたマネジメントシステムの評価であり、SCS評価制度は取引先との接続やシステム運用、サイバー攻撃への技術的耐性、事業継続まで含むサプライチェーンリスクへの対応を重視します。

そのため「Pマークを持っている＝SCS評価制度の要求事項を満たしている」とは整理できません。反対に、Pマークで整備済みの規程や教育記録、委託先管理台帳、事故対応手順などは、SCS評価制度への準備に活用できる可能性があります。重要なのは、既存認証を“代替”と考えるのではなく、“再利用できる統制資産”として扱うことです。

Pマーク取得済みでもSCS評価制度への対応が必要になる理由

理由1: SCS評価制度は個人情報以外の機密情報・システムも対象になり得る

企業間取引で守るべき情報は個人情報だけではなくありません。設計図、価格情報、営業秘密、認証情報、ソースコード、顧客企業のシステム情報、製造条件、研究開発データなども重大な保護対象です。SCS評価制度では、こうした情報やシステムがサプライチェーン経由で侵害されるリスクを考えます。

たとえば、委託先のリモート接続アカウントが侵害され、発注元の環境に不正侵入されるケースでは、個人情報が含まれなくても事業上の影響は大きくなります。Pマークで個人情報管理が適切でも、特権ID管理、ネットワーク分離、脆弱性管理、EDR、ログ監視などの技術統制が十分かは別に確認する必要があります。

理由2: SCS評価制度では技術的な実効性がより重視される

SCS評価制度の★4では、文書確認に加えて実地審査と技術検証が想定されています。規程に「脆弱性を定期的に確認する」と書いてあっても、実際に対象システムが適切な頻度と範囲で診断されているか、重大な脆弱性が放置されていないか、是正が追跡されているかといった実装面が問われます。

この点では、Webアプリケーション診断やプラットフォーム診断、必要に応じたペネトレーションテストが重要になります。Webアプリケーション診断は、Webサービスに対してSQLインジェクションや認証・認可不備などの脆弱性を確認するものです。プラットフォーム診断は、OS、ミドルウェア、ネットワーク機器等の設定不備や既知脆弱性を確認します。ペネトレーションテストは、攻撃者の視点で複数の弱点を組み合わせ、実際にどこまで侵入・権限拡大・情報到達が可能かを検証する方法です。

理由3: 取引先から求められる説明が変わる可能性がある

IPAは、SCS評価制度について、2社間の取引契約等において委託元が委託先に適切な段階(★)を提示し、対策の実施を促し、状況を確認する活用を想定しています。つまり、今後の取引先管理では「Pマークがあります」という説明だけでなく、「SCS評価制度ではどの水準を満たしているか」「取引対象システムにどの対策を実装しているか」といった説明を求められる可能性があります。

特に、重要な情報やシステムへのアクセスを許可される委託先、クラウドやSaaSの運用事業者、システム開発・保守事業者、製造業のサプライヤーなどでは、セキュリティ水準の客観的な説明が取引上の論点になりやすいと考えられます。

Pマーク取得企業がSCS評価制度対応で活用できる既存資産

規程・責任体制・教育記録は流用できる可能性が高い

Pマーク取得企業には、個人情報保護方針、内部規程、責任者・担当者の役割、教育記録、内部監査、事故対応、委託先管理などの仕組みがすでに存在します。これらはSCS評価制度への対応でも有効な土台になります。新しい制度だからといって、すべての規程を一から作り直す必要はありません。

実務では、まずSCS評価制度の要求事項と既存文書に対応付ける「ギャップ分析」を行い、既存資料で証明できる項目と追加整備が必要な項目を分けます。これにより、重複作業を減らし、追加コストと準備期間を抑えやすくなります。

一方で技術対策は別途棚卸しが必要

Pマーク取得企業でも、情報システム部門の運用がPMS文書とは別管理になっていることがあります。たとえば、パッチ適用基準、サーバーの構成管理、クラウド設定、MFA（多要素認証）、EDR、バックアップ、ログ保管、SOC監視、脆弱性診断の実施状況などです。

SCS評価制度を見据える場合は、こうした技術対策を「実施しているか」だけでなく、「対象範囲が明確か」「例外管理があるか」「証拠が残っているか」「発見事項が期限管理されているか」まで確認する必要があります。

対応しなかった場合に起こり得る問題

SCS評価制度そのものは、すべての企業に取得を法律上義務付ける制度ではありません。しかし、取引先が調達条件や委託先評価の基準として★取得や同等水準の対策を求める場合、未対応は商談や契約更新の説明負担につながる可能性があります。

また、取引先からセキュリティチェックシートを受け取った際に、社内の情報が分散していて回答に時間がかかる、証拠が不足して回答できない、対策済みと思っていたが実装状況を確認できない、といった問題が起きやすくなります。制度取得そのものよりも、取引先への説明能力を高めることが重要です。

経営上は、セキュリティ対策が受注継続、取引信用、事業継続に関係する点も見逃せません。サイバー事故が発生すれば、復旧費用だけでなく、取引停止、違約対応、顧客説明、信用毀損、経営層の意思決定負荷まで波及する可能性があります。

SCS評価制度対応の対象をどう決めるか

法人全体ではなく、まず重要な取引・システムから整理する

SCS評価制度では、各取得希望組織が適用範囲を決定し、その中からサンプリングして評価等を実施する考え方が示されています。したがって、準備段階では、どの取引・事業・拠点・システムを重要対象とするかを整理することが欠かせません。

優先度が高いのは、取引先の機密情報を扱う業務、外部からアクセス可能なWebシステム、クラウド管理画面、VPN・リモート接続、ソースコード管理基盤、顧客システムへの保守接続、事業停止時の影響が大きい基幹システムなどです。

経営層が判断すべき3つの事項

経営層は、第一にどの取引先・事業を優先するか、第二に★3と★4のどちらを目標とするか、第三に不足対策へどこまで投資するかを判断する必要があります。すべてを同時に最高水準へ引き上げるのではなく、取引重要度と事業影響を踏まえた優先順位付けが現実的です。

Pマーク取得企業が進めるべき具体的な対応手順

ステップ1: 既存のPマーク文書とSCS要求事項を対応付ける

まず、Pマークで保有している規程、台帳、監査記録、教育記録、委託先評価記録、事故対応記録などを一覧化します。そのうえでSCS評価制度の要求事項・評価基準と照合し、流用可能、不足、対象外の3区分程度で整理します。

ステップ2: 技術対策を現状確認する

情報資産台帳やシステム一覧、ネットワーク構成図、クラウド利用一覧、アカウント管理表、パッチ管理記録、バックアップ設計、ログ監視状況、脆弱性診断報告書などを確認します。文書上は対策済みでも、現場運用で例外が常態化していないかを確認することが重要です。

ステップ3: 脆弱性診断・技術検証の必要性を判断する

外部公開Webサービスやインターネット接続機器については、Webアプリケーション診断やプラットフォーム診断を検討します。重要なシステムや高度な攻撃を想定する環境では、ペネトレーションテストにより侵入経路や権限拡大、横展開の可能性を確認する方法もあります。診断の種類は「制度対応だから実施する」のではなく、守る対象と想定脅威に合わせて選択します。

ステップ4: 発見事項をリスクベースで是正する

指摘事項は、単純な件数ではなく、悪用可能性、影響範囲、外部公開の有無、保有情報の機密性、事業停止時の影響などを踏まえて優先順位を決めます。重大な脆弱性は早期対応し、中長期対応が必要な課題は経営承認を得て改善計画へ落とし込みます。

ステップ5: 証跡を残し、取引先への説明可能性を高める

評価対応では、ルールが存在するだけでなく、実際に運用されていることを示せる証跡が重要です。教育履歴、レビュー記録、パッチ適用結果、診断報告書、是正記録、バックアップ試験、インシデント訓練の結果などを保存し、必要なときに提示できる状態を作ります。

費用と期間を左右する要因

SCS評価制度対応の費用は、単に申請費用だけでは決まりません。既存の規程や技術対策がどこまで整備されているか、対象システム数、拠点数、クラウド利用数、診断対象URL・IP数、追加導入するセキュリティ製品、改修の難易度、★3・★4のどちらを目標とするかによって大きく変わります。

Pマーク取得企業は、規程・教育・内部監査・委託先管理などの基盤があるため、非取得企業に比べて準備を短縮できる可能性があります。一方、技術対策の不足が大きい場合は、MFA導入、EDR導入、ログ監視、バックアップ強化、脆弱性対応などに追加投資が必要です。

社内稟議では「認証取得費用」だけでなく、取引継続、取引先監査への対応工数削減、事故リスク低減、システム停止リスク、顧客からの信用といった経営効果を含めて説明すると、投資目的が伝わりやすくなります。

SCS評価制度の支援会社を選ぶポイント

制度解説だけでなく、技術実装まで支援できるか

SCS評価制度では、規程整備だけでなく技術的な実効性が重要です。支援会社を選ぶ際は、要求事項の解釈だけでなく、脆弱性診断、ペネトレーションテスト、SOC／CSIRT、インシデントレスポンス、クラウド・ネットワーク対策などを理解し、発見した課題を実装レベルまで落とし込めるかを確認するとよいでしょう。

既存認証を尊重し、重複作業を減らせるか

PマークやISMSなどをすでに運用している企業に対して、すべてを作り直す支援は効率的とは限りません。既存規程・証跡・監査プロセスを評価し、SCS評価制度との差分だけを明確にできる事業者のほうが、社内負担を抑えやすくなります。

RFP・見積依頼で確認したい項目

見積依頼時には、ギャップ分析の対象範囲、成果物、技術診断を含むか、改善支援の範囲、再診断の有無、機密情報の取り扱い、再委託の有無、担当者の資格・経験、想定スケジュールを確認します。SCS評価制度そのものの第三者評価と、取得に向けたコンサルティング・技術支援は役割が異なるため、どこまでを依頼するのかを明確にすることも重要です。

よくある失敗と注意点

「Pマークがあるから大丈夫」と確認を止めてしまう

最も注意したいのは、既存認証を理由に追加確認をしないことです。Pマークで十分に整備された領域がある一方、SCS評価制度ではサプライチェーンリスクや技術対策の観点から追加確認が必要になります。

規程整備を優先し、技術的な未対応を後回しにする

制度対応では、文書を整えることより、実際のリスクを減らすことが本質です。外部公開サーバーに重大な脆弱性が残っている、退職者アカウントが残存している、バックアップから復旧できない、といった問題は、規程だけでは解決できません。

診断結果を受け取って終了する

脆弱性診断やペネトレーションテストは、報告書を受領することが目的ではありません。発見事項を修正し、再診断で解消を確認し、同種の問題を繰り返さない運用に反映することが重要です。

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「規程作成だけ」「診断だけ」で切り分けず、企業ごとの事業・取引・システム環境に応じて一気通貫で支援します。Pマークなど既存認証を取得している企業には、既存の規程・台帳・証跡を活かしながら、SCS評価制度とのギャップを整理し、不足する管理策を優先順位付けします。

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構築・運用支援、インシデントレスポンス、デジタルフォレンジック、SBOM支援、リスクアセスメントなど、技術対策から運用改善まで対応可能です。

制度取得そのものを目的にするのではなく、取引先に説明できるセキュリティ体制を整え、改善活動を継続できる状態を目指します。経営層への説明、情報システム部門の実装、管理部門の規程・証跡整備を横断して整理できる点も、SCS評価制度対応では重要です。

よくある質問

Q1. Pマークを取得していればSCS評価制度は取得不要ですか？

一律に不要とはいえません。PマークとSCS評価制度は目的・評価対象が異なるためです。Pマークの既存統制を活用しつつ、SCS評価制度の要求事項との差分を確認する必要があります。

Q2. PマークとSCS評価制度で共通する対策はありますか？

あります。責任体制、規程、教育、委託先管理、インシデント対応、内部監査などは重なる可能性があります。ただし、SCS評価制度ではサイバー攻撃やサプライチェーンリスクへの技術的な対策がより重要になります。

Q3. Pマーク取得企業なら★3は簡単に取得できますか？

既存の管理体制を活用できるため準備負担を減らせる可能性はありますが、取得を保証するものではありません。SCS評価制度の要求事項・評価基準に照らして、不足部分を確認する必要があります。

Q4. SCS評価制度では脆弱性診断が必要ですか？

対象となる要求事項や評価水準、対象システムによって必要性を判断します。特に外部公開システムや重要システムでは、Webアプリケーション診断やプラットフォーム診断などの技術検証が有効です。★4では第三者評価に加え、技術検証が制度上想定されています。

Q5. ISMSを取得している場合も同じですか？

ISMSもSCS評価制度と完全に同一ではありません。経済産業省の制度構築方針でも、SCS評価制度（★3・★4）とISMS適合性評価制度は目的・アプローチが異なるものとして整理されています。既存のISMS運用は有力な基盤になりますが、SCS要求事項との差分確認が必要です。

Q6. ★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、扱う情報・システムの重要度、サプライチェーン上の役割を踏まえて判断します。高度な技術検証や第三者評価が求められる取引では★4が候補となります。

Q7. 何から始めればよいですか？

最初に、取引先から求められている要求水準と対象範囲を確認し、既存のPマーク文書・情報セキュリティ規程・技術対策を棚卸しします。その後、SCS評価制度とのギャップ分析を行うと、優先順位が明確になります。

まとめ | Pマークは有効な土台だが、SCS評価制度の代替ではない

SCS評価制度とPマークは、どちらも企業の信頼性向上に役立つ制度ですが、目的は同じではありません。Pマークは個人情報保護マネジメントを中心に評価し、SCS評価制度はサプライチェーンを通じたサイバーリスクへの対応水準を評価します。

したがって、Pマーク取得企業でもSCS評価制度への追加対応が必要になる可能性があります。ただし、すでに整備している規程、教育、内部監査、委託先管理、事故対応などは大きな資産です。既存体制を活かして差分だけを整備することが、コストとスピードの両面で合理的です。

重要なのは、認証やマークの数を増やすことではなく、自社の取引先・事業・システムに対して必要なセキュリティ対策を説明でき、実際に運用できる状態を作ることです。

SCS評価制度と既存認証の整理からご相談いただけます

「Pマークを取得しているが、SCS評価制度で何を追加すべきか分からない」「★3と★4のどちらを目指すべきか判断できない」「取引先から質問さ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Pマーク・ISMS等の規程や証跡を確認し、SCS評価制度とのギャップを整理したうえで、必要な技術対策、脆弱性診断、改善計画、社内説明まで支援します。対象範囲や実施方法が決まっていなくても、取引上の重要度と現在のセキュリティ体制から優先順位を整理することで、過剰な投資を避けながら実務的な準備を進められます。

出典・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>
- JIPDEC「プライバシーマークとは」：<https://privacymark.jp/system/about/index.html>
- JIPDEC「制度の概要」：https://privacymark.jp/system/about/outline_and_purpose.html
- 個人情報保護委員会「個人情報の保護に関する法律についてのガイドライン（通則編）」：
https://www.ppc.go.jp/personalinfo/legal/guidelines_tsusoku/

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>