

SCS評価制度とサイバーセキュリティお助け隊サービスの関係とは？

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）への対応を検討する中で、「サイバーセキュリティお助け隊サービスを導入すれば、SCS評価制度にも対応できるのか」と疑問を持つ企業は少なくありません。結論から言えば、両者は同じ制度ではありません。SCS評価制度は企業の対策状況を段階的に可視化・評価する仕組みであり、サイバーセキュリティお助け隊サービスは、中小企業が必要な対策を導入・運用するための支援サービスです。

特に重要なのは、従来の「サイバーセキュリティお助け隊サービス」と、SCS評価制度の★3・★4取得支援を目的に現在制度化が進められている「新類型」を区別することです。2026年10月22日時点では、新類型は実証事業の段階にあり、15事業者のサービスを用いて、診断・助言、ITツール導入、コンサルティング、教育などを組み合わせた伴走支援の制度設計が進められています。

本記事では、SCS評価制度とサイバーセキュリティお助け隊サービスの関係、既存類型と新類型の違い、自社がどのように使い分けるべきかを、経営・実務の両面から解説します。

出典：IPA「サイバーセキュリティお助け隊サービス（新類型）実証事業」<https://www.ipa.go.jp/security/sme/otasuke-scs.html>

この記事で分かること

- SCS評価制度とサイバーセキュリティお助け隊サービスの役割の違い
- 従来のお助け隊サービスと、SCS★3・★4取得支援を目的とする「新類型」の違い
- お助け隊サービスを導入すればSCS評価制度の要件を満たせるのか
- 従業員100～1,000名規模の企業が利用を検討する際の注意点
- 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含めた実務的な対応の進め方
- SCS評価制度対応を外部支援会社へ依頼する際の選定ポイント

SCS評価制度とサイバーセキュリティお助け隊サービスは何が違うのか

SCS評価制度は「対策水準を評価・可視化する制度」

SCS評価制度は、サプライチェーンを構成する企業について、求められるサイバーセキュリティ対策の水準を★で示し、取引先間で確認しやすくする制度です。2026年3月に経済産業省と内閣官房国家サイバー統括室が制度構築方針を公表し、IPAが運営主体となっています。★3・★4は2027年3月頃の運用開始が予定されています。

★3は「一般的なサイバー脅威に対処しうる」水準で、セキュリティ専門家の確認を経た自己評価です。★4は、初期侵入の防御だけでなく、被害拡大防止や取引先のデータ・システム保護まで含む水準で、第三者評価と技術検証が求められます。SCS評価制度は、単にセキュリティ製品を導入したかどうかではなく、組織的なルール、運用、技術対策が要求事項・評価基準を満たしているかを確認する点が特徴です。

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

サイバーセキュリティお助け隊サービスは「対策を実装・運用するための支援」

一方、サイバーセキュリティお助け隊サービスは、中小企業がサイバー攻撃への対処に必要なサービスを導入しやすくすることを目的に、IPAが2021年春から制度を運営しているものです。民間事業者が提供するサービスのうち、所定の基準を満たしたものが登録されます。従来類型では、相談窓口、異常監視、インシデント発生時の初動対応支援、簡易サイバー保険などをワンパッケージで提供することが基本となっています。

つまり、SCS評価制度が「どの水準まで対策できているかを示すもの」だとすれば、お助け隊サービスは「その対策を実際に導入・運用するための手段の一つ」と理解すると分かりやすいでしょう。

出典:IPA「サイバーセキュリティお助け隊サービス制度」 <https://www.ipa.go.jp/security/sme/otasuketai/index.html>

既存類型とSCS対応の「新類型」は分けて考える

ここが最も誤解されやすいポイントです。現在利用できる従来のお助け隊サービスを契約しただけで、SCS評価制度の★3や★4を自動的に取得できるわけではありません。SCS評価制度では、取得対象となる適用範囲を決め、要求事項・評価基準への適合状況を確認し、★3では専門家確認付き自己評価、★4では第三者評価・技術検証を受ける必要があります。

これに対し、現在制度化が進められている「サイバーセキュリティお助け隊サービス(新類型)」は、まさに★3・★4の取得支援を目的としています。IPAによれば、新類型では課題の可視化を行う診断・助言、推奨ITツールの導入、コンサルティングや教育などをワンパッケージで提供し、伴走支援を行う想定です。2026年9月15日に実証事業が公表され、2026年10月20日時点で15事業者の実証サービスが掲載されています。

出典:IPA「サイバーセキュリティお助け隊サービス(新類型)実証事業」 <https://www.ipa.go.jp/security/sme/otasuke-scs.html>

SCS評価制度・既存お助け隊・新類型の関係を整理

項目	SCS評価制度	既存のお助け隊サービス	お助け隊サービス(新類型)
主な目的	対策水準の評価・可視化	中小企業向けの基本的なセキュリティ対策支援	SCS★3・★4取得に向けた対策実装・伴走支援
位置づけ	評価制度	登録された民間サービス	SCS対応支援のために制度化を進めている新たなサービス類型
対象	サプライチェーンを構成する幅広い企業	主として中小企業	中小企業を主な対象として実証中
提供内容	要求事項・評価基準、評価スキーム	相談、監視、初動対応、保険等	診断・助言、ITツール、コンサルティング、教育等を想定
導入だけで★取得できるか	—	自動的に取得できない	取得支援が目的だが、最終的にはSCS所定の評価・申請手続きが必要

なぜSCS評価制度で「お助け隊サービス」が重要になるのか

中小企業では「要求事項は分かっても実装できない」が起こりやすい

SCS評価制度への対応では、規程を作るだけでは不十分です。例えば、端末やサーバの構成管理、脆弱性への対応、アクセス制御、ログ取得、バックアップ、インシデント発生時の連絡体制など、日常運用まで含めて対策を定着させる必要があります。専任のセキュリティ担当者が少ない企業では、「何が不足しているかは分かったが、具体的な製品選定や運用設計まで手が回らない」という問題が起こりやすくなります。

新類型のお助け隊サービスは、このギャップを埋める支援策として設計されています。課題の可視化からITツールの導入、組織的対策、教育までを一体で支援することで、SCS評価制度の要求事項を実際の業務へ落とし込むことが狙いです。

取引先からの要求に対し、短期間で説明できる状態を作る必要がある

SCS評価制度そのものは任意制度ですが、実際の取引では、委託元が委託先に一定の★を求めることが想定されています。したがって、制度上の義務ではなくても、取引条件、調達基準、委託先評価の一部として対応を求められる可能性があります。取引先から「★3を取得してください」と要請を受けてからゼロから資産管理や規程整備を始めると、契約更新や新規取引のスケジュールに間に合わないケースも考えられます。

お助け隊サービスや外部コンサルティングを活用する意義は、単に人手を補うことではありません。現状評価、優先順位付け、対策実装、証跡整備を並行して進め、取引先へ説明可能な状態を早期に作りやすくする点にあります。

出典：経済産業省「SCS評価制度」 <https://www.meti.go.jp/policy/netsecurity/scs.html>

お助け隊サービスだけでSCS★3・★4に対応できるのか

結論として、サービス導入だけで全ての要求事項への適合が保証されるものではありません。SCS評価制度では、★3・★4の取得にあたり定められた要求事項・評価基準を満たす必要があります。★3では自社が自己評価を行い、登録要件を満たすセキュリティ専門家の確認・助言を経て、経営層の自己適合宣誓を含む申請を行います。★4では、指定された評価機関による第三者評価と技術検証が必要です。

新類型は★取得のための支援を目的にしていますが、どの要求事項をどのサービスで充足できるかは、自社の適用範囲、既存の仕組み、契約するサービス内容によって変わります。例えば、端末監視サービスを導入しても、委託先管理規程、従業員教育、アクセス権限の承認プロセス、インシデント報告手順などの組織的対策は別途整備が必要になる場合があります。

そのため実務では、「サービスを買う」ことを起点にするのではなく、まずSCS要求事項とのギャップを把握し、未達項目のうち、外部サービスで補う項目と自社で整備する項目を切り分けることが重要です。

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

従業員100～1,000名規模の企業が特に注意したい点

SCS評価制度の対象と、お助け隊サービスの対象は一致しない

SCS評価制度は企業規模を問わず、サプライチェーンを構成する幅広い事業者が対象になり得ます。一方、サイバーセキュリティお助け隊サービスは中小企業向けの支援策です。したがって、従業員100～1,000名規模の企業では、自社が新類型の対象となるかを必ず確認する必要があります。

中小企業基本法上の中小企業者の範囲は業種により異なり、例えば製造業その他では資本金3億円以下または常時使用する従業員300人以下、卸売業では資本金1億円以下または従業員100人以下、サービス業では資本金5,000万円以下または従業員100人以下が原則です。ただし、個別の支援制度では定義が異なる場合があります。従業員数だけで「利用できる・できない」と判断せず、正式な新類型の利用要件を確認することが必要です。

出典: 中小企業庁「中小企業の定義に関するよくある質問」 https://www.chusho.meti.go.jp/faq/faq/faq01_teigi.html

中堅企業では「部分的な外部活用」の方が合理的な場合もある

従業員数が数百名規模になると、拠点数、端末台数、クラウドサービス数、委託先数が増え、単一パッケージだけでは全体をカバーしにくくなります。この場合、お助け隊サービスの利用可否とは別に、SCS要求事項に沿って全社横断でギャップ分析を行い、EDR・SOC・脆弱性管理・インシデント対応・教育などを必要な範囲だけ外部サービスで補う方が合理的なケースがあります。

経営層は「補助制度やパッケージを使えるか」だけではなく、「取引先から求められる★水準に対して、どの適用範囲を、いつまでに、どの予算で整備するか」を意思決定する必要があります。

SCS評価制度対応で実際に進めるべき6つのステップ

1. 取引先から求められる水準と期限を確認する

最初に確認すべきは、★3・★4のどちらを目指すのか、いつまでに必要なのか、どの取引・事業・システムが背景にあるのかです。調達部門や営業部門が取引先から受け取ったセキュリティチェックシートや契約条項も確認します。社内稟議では、単なる「認証取得費用」ではなく、取引継続、新規受注、事業継続の観点から目的を説明すると、経営判断につなげやすくなります。

2. 適用範囲とIT資産を整理する

SCS評価制度では、自社が決定した適用範囲を前提に評価が行われます。対象拠点、端末、サーバ、ネットワーク、クラウド、業務システム、委託先などを洗い出し、資産台帳やネットワーク構成図と整合させます。この段階で対象が曖昧だと、その後の対策費用や評価工数が膨らみやすくなります。

3. 要求事項に対するギャップ分析を行う

規程、運用記録、システム設定、ログ、教育履歴、インシデント対応手順などを確認し、要求事項ごとに「適合」「不足」「確認不能」を整理します。特に「ルールはあるが運用証跡がない」「担当者の経験で対応していて文書化されていない」という状態は、評価時の説明を難しくします。

4. お助け隊サービスや他のセキュリティ施策を組み合わせる

不足項目のうち、監視、端末防御、相談窓口、初動対応などは、お助け隊サービスが有力な選択肢となり得ます。一方で、インターネット公開システムの脆弱性を把握するにはWebアプリケーション診断、サーバやネットワーク機器の設定・既知脆弱性を確認するにはプラットフォーム診断が有効です。攻撃者の視点から侵入可能性や被害拡大経路まで検証する必要がある場合は、ペネトレーションテストを検討します。

ただし、これらの診断やテストを実施したこと自体がSCS★取得を意味するわけではありません。SCSの適用範囲と要求事項に照らし、どの検証が必要かを決めることが重要です。

5. 是正計画を経営課題として優先順位付けする

未達項目を一律に処理するのではなく、取引先への影響、機密情報の重要性、侵害された場合の事業停止時間、対策コスト、実装に必要な期間を踏まえて優先順位を付けます。例えば、インターネットから直接到達できるシステムの重大な脆弱性、多要素認証がない管理者アカウント、復元確認をしていないバックアップなどは、早期に経営判断が必要なテーマになりやすいでしょう。

6. 評価・申請に必要な証跡を整える

対策完了後は、規程、手順書、設定画面、ログ、教育記録、点検記録など、実施を説明できる証跡を整理します。★3では自己評価に対してセキュリティ専門家の確認・助言を受け、★4では評価機関と技術検証事業者による評価に備えます。システム変更やクラウド移行など、対策状況に影響する変更が生じた場合も継続的に見直せる運用にしておくことが重要です。

費用と期間を左右する要因

SCS評価制度対応の費用は、単純な「申請費用」だけでは決まりません。大きく影響するのは、適用範囲の広さ、拠点数、端末・サーバ数、クラウド環境の数、既存規程の整備状況、未達要求事項の数、導入するセキュリティ製品、診断・テストの対象範囲、専門家支援の工数です。新類型のお助け隊サービスについても、2026年10月22日時点では実証事業を通じてサービス体系と価格要件の検証が進められている段階であるため、正式サービスの料金は公表内容を確認する必要があります。

期間についても同様で、すでにISMS等を運用している企業と、資産管理や規程整備から始める企業では差が出ます。取引先から期限を指定されている場合は、最初に簡易ギャップ分析を行い、「制度申請に必要な作業」と「中長期で改善する作業」を分けると、現実的なロードマップを作りやすくなります。

サービス提供会社を選ぶ際のチェックポイント

SCS評価制度対応では、単に製品を販売できる会社よりも、要求事項を理解し、組織面と技術面を横断して支援できる会社を選ぶことが重要です。RFPや見積依頼では、SCS要求事項への対応範囲、ギャップ分析の方法、成果物、専門家確認への対応、脆弱性診断やペネトレーションテストの実施可否、改善支援、機密情報の取り扱い、再診断・継続監視まで確認するとよいでしょう。

また、★3取得支援を依頼する場合は、SCS評価制度上の「セキュリティ専門家」として求められる資格・研修・登録要件への対応状況も確認が必要です。★4を目指す場合は、評価を行う機関とコンサルティング支援の役割、中立性・公平性に関する制度要件を踏まえて体制を設計します。

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

よくある失敗と注意点

「お助け隊サービスを入れればSCS対応完了」と考える

最も避けたいのは、サービス契約そのものを制度対応のゴールにしてしまうことです。SCS評価制度では要求事項への適合が必要であり、ツール導入以外の規程・教育・委託先管理・運用証跡なども確認対象になります。必ず要求事項を起点にして不足項目を確認しましょう。

対象範囲を決める前に製品を購入する

適用範囲が不明確な状態でEDR、監視サービス、診断などを発注すると、必要台数や対象システムが後から増え、追加費用が発生しやすくなります。資産と対象範囲を整理してから見積りを依頼することが、コストとスピードの両面で有効です。

制度開始前の情報を確定事項として扱う

SCS評価制度とお助け隊サービス新類型はいずれも制度詳細の整備が続いています。特に新類型は2026年10月時点で実証段階です。社内資料や取引先への説明では、公表日と参照元を明示し、今後変更される可能性を織り込んで計画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、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）への対応について、制度要件の整理から現状分析、技術対策、改善運用まで一気通貫で支援します。お助け隊サービスを利用できる企業については、その活用を含めて全体設計を検討し、利用対象外の企業や、パッケージだけでは不足する企業については、個別の環境・事業リスクに応じた対策を設計します。

具体的には、SCS★3・★4要求事項とのギャップ分析、適用範囲の整理、規程・手順の整備、リスクアセスメント、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、SOC／CSIRT構築・運用支援、インシデントレスポンス、教育・訓練などを組み合わせることが可能です。診断結果を提示して終えるのではなく、改善優先順位、予算、社内稟議、取引先への説明まで含め、実際に運用できる状態を目指します。

SCS評価制度対応は、セキュリティ部門だけで完結するテーマではありません。経営層、情報システム部門、営業・調達部門、現場部門の間で目的や優先順位をそろえることが必要です。Librus株式会社は、技術と経営の両面から課題を整理し、各部門の橋渡しを行いながら支援します。

よくある質問

Q1. サイバーセキュリティお助け隊サービスを導入すればSCS★3を取得できますか？

導入だけで自動的に★3を取得できるわけではありません。★3では要求事項・評価基準を満たしたうえで、専門家確認付き自己評価と所定の申請が必要です。新類型は★3・★4取得支援を目的としますが、最終的な適合確認と申請手続きはSCS評価制度に従います。

Q2. 従来のお助け隊サービスと新類型は同じものですか？

同じではありません。従来類型は相談・監視・初動対応・簡易サイバー保険などの基本的対策をワンパッケージで提供する制度です。新類型はSCS★3・★4取得支援を目的に、診断・助言、ITツール、コンサルティング、教育等を組み合わせる方向で実証が進められています。

Q3. 新類型は現在すぐに利用できますか？

2026年10月22日時点では実証事業の段階です。IPAは15事業者の実証サービスを公表しており、実証結果を踏まえてサービス基準や価格要件を検討するとしています。最新の募集・提供状況はIPAの公式ページで確認してください。

Q4. 従業員500名の企業でもお助け隊サービスを利用できますか？

一律には判断できません。お助け隊サービスは中小企業向けであり、中小企業の定義は業種・資本金・従業員数、さらに個別制度の要件によって異なります。一方、SCS評価制度そのものは幅広いサプライチェーン企業が対象です。

Q5. SCS★3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？

実施の要否は要求事項・評価基準と自社の適用範囲、システム構成を踏まえて判断する必要があります。診断やペネトレーションテストを実施しただけで★取得になるわけではありませんが、技術的な弱点を把握し、対策の実効性を確認する手段として有効です。

Q6. お助け隊サービスとSOCはどちらを選ぶべきですか？

目的と規模によります。基本的な監視・相談・初動支援を効率的に導入したい中小企業ではお助け隊サービスが候補になります。一方、多数の拠点・端末・クラウドを横断して高度な監視や分析が必要な企業では、SOCやMDRなど個別設計のサービスが適する場合があります。

Q7. SCS対応はいつから準備すべきですか？

取引先から要請を受ける前の準備が有効です。資産管理、規程、バックアップ、権限管理、教育などは短期間で整備しにくいので、まず現状と要求事項のギャップを確認し、予算化・是正計画を進めておくこと対応しやすくなります。

Q8. SCS対応の相談時に何を用意すればよいですか？

可能であれば、組織図、情報セキュリティ規程、IT資産一覧、ネットワーク構成図、利用クラウド一覧、取引先から受領したセキュリティ要求、過去の診断・監査報告書などを準備すると現状把握が進みやすくなります。資料が揃っていない段階でも、対象範囲の整理から開始できます。

まとめ | SCS評価制度とお助け隊サービスは「評価」と「実装支援」の関係

SCS評価制度とサイバーセキュリティお助け隊サービスは、競合する仕組みではなく、役割が異なります。SCS評価制度はサプライチェーン企業に求められるセキュリティ対策水準を評価・可視化する制度であり、お助け隊サービスは企業が必要な対策を実装・運用するための支援策です。

特に、現在制度化が進むお助け隊サービスの新類型は、SCS★3・★4取得を支援することを明確な目的としています。ただし、新類型を利用すれば自動的に★を取得できるわけではありません。自社の適用範囲を決め、要求事項とのギャップを確認し、組織的対策と技術的対策を整えたうえで、SCS評価制度が定める評価・申請手続きを進める必要があります。

従業員100～1,000名規模の企業では、お助け隊サービスの利用要件だけに注目するのではなく、自社の事業規模、システム構成、取引先から求められる水準に応じて、コンサルティング、脆弱性診断、ペネトレーションテスト、SOC／CSIRT、教育などを組み合わせる視点が重要です。

SCS評価制度への対応方法が決まっていない段階からご相談いただけます

「お助け隊サービスを使えるのか分からない」「★3と★4のどちらを目指すべきか判断できない」「取引先から取得を求められたが、何から始めるべきか分からない」といった段階でも、Librus株式会社へご相談いただけます。

現状のIT環境、取引先からの要求、社内体制、予算・期限を整理したうえで、SCS評価制度の要求事項とのギャップを可視化し、自社で対応する項目と外部サービスを活用する項目を切り分けます。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、SOC／CSIRT支援、規程整備、教育まで一気通貫で検討できるため、個別に複数のベンダーへ相談する前に全体像を整理することが可能です。

取得そのものを目的にするのではなく、取引先への説明力、事業継続性、実際のセキュリティ水準の向上につながる対応計画と一緒に設計します。

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>