サイバーセキュリティお助け隊サービス（新類型）実証
説明資料

2026年9月15日

独立行政法人
情報処理推進機構　セキュリティセンター　普及啓発・振興部

お助け隊サービス（新類型）実証の概要

- サイバーセキュリティお助け隊サービス（新類型）は、中小企業が効率よくSCS評価制度の★3・★4を取得できるよう、★取得のための課題の可視化を行う**診断・助言サービス**、推奨される**ITツール**（セキュリティ機器、ソフトウェア等）の導入、及び**ITツール以外の支援**（コンサルティング、教育等）を**ワンパッケージで提供**し、**伴走支援**を行うサービスです。
- 今回の実証事業では、**公募により採択した15事業者の提供するサービス**を中小企業の皆様に実際に参加いただき、「サイバーセキュリティお助け隊（新類型）」の制度化に向け、中小企業が**導入しやすいサービス体系の検証**と、併せて中小企業とサービス提供事業者の双方にとって**適切なサービスの価格要件の検証**を行い、有識者の意見を反映した上で**サービス（新類型）基準を作成、制度化**につなげる予定です。

お助け隊サービス（新類型）のイメージ

STEP1：課題の可視化

診断・助言サービスの実施

- ✓ SCS評価制度の要件項目毎に中小企業の**対策状況を診断**
- ✓ **未達成項目について実施すべき対策**を、改善計画書として取りまとめる

STEP２：対象サービスの選定と対応実施

診断結果に基づき、★3・★4取得に必要な対策を伴走支援

✓ITツールによる支援サービス

★3・★4取得に推奨されるITツールを導入

✓ITツール以外の支援サービス

セキュリティポリシーやインシデント手順書整備、セキュリティ教育など、中小企業が自助努力で達成しづらい項目を支援

STEP3：☆取得申請支援

★取得申請を支援

- ✓ 要求事項の充足を確認し、セキュリティ専門家による確認・評価や、申請書作成を支援

SCS評価制度の要求事項（大分類）

1.ガバナンス整備、2.取引先管理、3.リスク特定、
4.攻撃等の防御、5.攻撃等の検知、
6.インシデント対応、7.インシデントからの復旧

・・・ 中小企業の対策状況によって必要な支援サービス内容は変わる

実証でやりたいこと

必要な支援レベルの検証

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、機器導入では充足とならない項目もあるため、お助け隊サービスとして必要な支援レベルを検証します。

サービス内容の検証

お助け隊サービスを利用する全ての企業が、SCS評価制度の★を取得できるサービス内容であるかどうかを検証します。

幅広い業種への対応を検証

SCS評価制度は、特定業種に限定されないため、幅広い業種（※1）に対応可能かを検証します。

（※1）製造業のほか、情報通信業、金融業、運送業、サービス業、医療業界など

お願い事項

- ✓ 実証後に無理なく導入できたかのアンケートや実証期間中にサービスを利用するにあたって検知した情報の提供（※）にご協力ください。
- ✓ SCS評価制度で取得した★を持続いただくため、実証後もお助け隊サービスの利用を継続いただけると幸いです。

（※）シグネチャや通信情報などを含む場合があります。

（参考）既存のお助け隊サービスとの比較

サイバーセキュリティお助け隊サービス　既存類型と新類型のサービス内容

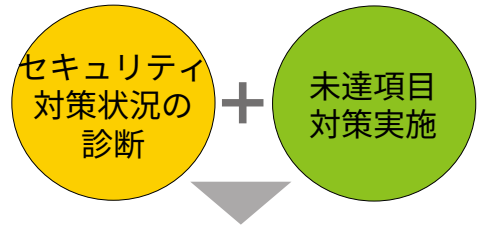
既存類型

セキュリティ対策に不安のある中小企業に向けて、**最低限必要なセキュリティ対策**を安価に提供（2026年3月時点で約10,900件の導入実績有）

ワンパッケージで安価に提供

新類型

SCS評価制度の★３・４取得を目指す中小企業に向けてセキュリティ対策状況を**診断**し、未達成項目の達成実施を**伴走支援**するサービス



SCS評価制度の★取得

実証で検証すること（ITベンダー向け）

中小企業へのサービス提供を通じて以下の項目を検証

1. セキュリティ要求に対応できる**技術要件（サービスの内容・品質等）**を検証

2. サービス導入が継続的に可能な**価格要件**を検証

実証を通して、**ITベンダー・中小企業の双方にとってメリットのあるサービス**を創設する

中小企業の実証参加メリット

1. **組織的対策を含むセキュリティ対策を無料**で実施（実証期間中最大1年程度）

2. SCS評価制度開始後の**★取得要請への備え**が可能

3. サプライチェーン対策に取り組む企業として、**取引先との信頼性向上**に繋がる

（参考）SCS評価制度とお助け隊（新類型）の位置づけ

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）の概要

構築する評価制度

	★3	★4	★5 [検討中※2]
想定される脅威	• 広く認知された脆弱性等を悪用する一般的なサイバー攻撃	• 供給停止等によりサプライチェーンに大きな影響をもたらす企業への攻撃 • 機密情報等、情報漏えいにより大きな影響をもたらす資産への攻撃	• 未知の攻撃も含めた、高度なサイバー攻撃
対策の基本的な考え方	全てのサプライチェーン企業が**最低限実装すべき**セキュリティ対策： • 基礎的な組織的対策とシステム防御策を中心に実施	サプライチェーン企業等が**標準的に目指すべき**セキュリティ対策： • 組織ガバナンス・取引先管理、システム防御・検知、インシデント対応等包括的な対策を実施	サプライチェーン企業等がさらに目指すべき高度な対策： • 国際規格等におけるリスクベースの考え方に基づき、自組織に必要な改善工程を整備、システムに対しては現時点でのベストプラクティスの対策を実施
要求事項 / 有効期間	26件 / 1年	43件 / 3年（毎年自己評価を実施し結果を評価機関へ提出）	（今後検討）
評価スキーム	専門家確認付き自己評価 ※1	第三者評価	第三者評価

政府調達や重要インフラ事業者等での活用推進

取引先からの対策要請による活用促進

利害関係者への情報開示による対話の促進

サプライチェーン間の結び付きが強固・複雑な主要製造業（自動車、半導体等）、流通、金融業等において、優先的に本制度の利用を促進。

［※1］専門家：登録セキスペ、CISSP等の資格を有し、かつ制度が定める研修を受講したセキュリティ専門家　［※2］ISMS適合性評価制度、★3・4との整合性も踏まえ、対策事項を今後検討

普及施策の例

想定される課題	中小企業等における★取得の負担	中小企業等におけるセキュリティ専門家の確保	サプライヤー企業への★取得要請時の関係法令の適用
施策の概要	**サイバーセキュリティお助け隊サービス（新類型）の創設** ★3・★4取得を目的とした、サイバーセキュリティお助け隊サービス（新類型）を創設し、安価な”★”取得を実現	**中小企業ガイドライン整備** 中小企業の情報セキュリティ対策ガイドライン及び付録サンプル規程の整備により、”★”の取得を容易化	**専門家の活用促進** 「中小企業向けサイバーセキュリティ専門家リスト」の整備により、中小企業と専門家とのマッチングを促進	**取引先への要請等に係る考え方の整理** 取引先とのパートナーシップ構築促進に向けた想定事例及び解説案により、費用に係る円満な価格交渉を促進

本事業

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

目的：①技術要件・価格要件の検証、②サービス基準案の策定

（参考）SCS評価制度で用いるセキュリティ要求事項・評価基準の概要

- NIST Cyber Security Framework(CSF)の機能に対応した６つの分類に、取引先管理に重点を置いた分類を加えた７つの分類において、それぞれレベルごと達成すべき対策を提案。

大分類	★3	★4	NIST CSFにおける機能
ガバナンスの整備	**企業として最低限のリスク管理体制の構築** • 自社のセキュリティ担当の明確化 [No.1-2-1] • セキュリティ対応方針の策定 [No.1-3-1]	**継続的改善に資するリスク管理体制の構築** • 定期的な経営層への報告、不備の是正等 [No.1-4-1]	統治(GV)
取引先管理	**取引先に課す最低限のルール明確化** • 他社との機密情報の取扱い明確化 [No.2-1-2] • 接続している外部情報サービスの把握 [No.3-1-3]	**取引先の管理・把握及び取引先との役割・責任の明確化** • 機密情報共有先の把握 [No.2-1-1] • 重要な取引先等の対策状況把握 [No.2-1-3] • インシデント発生時の他社との役割等の明確化 [No.2-1-4]	
リスクの特定	**自社IT基盤や資産の現状把握** • 情報資産やネットワークの把握 [No.3-1-1,3-1-2] • 外部情報サービスの管理 [No.3-1-3]	**脆弱性など最新状況の把握と反映** • 脆弱性管理体制、管理プロセスの明確化 [No.3-2-1]	識別(ID)
攻撃等の防御	**不正アクセスに対する基礎的な防御** • ID管理手続、アクセス権限の設定[No.4-1-1,4-1-2] • パスワードの安全な設定及び管理 [No.4-1-4,4-1-5] • 内外ネットワーク境界の分離・保護 [No.4-5-1] **端末やサーバーの基礎的な保護** • 適時のアップデート適用、不要ソフトウェアの削除[No.4-4-1,4-4-4] • 端末等へのマルウェア対策 [No.4-4-1,4-4-4]	**多層防御による侵入リスクの低減** • 重要な保管データの暗号化 [No.4-3-1,4-3-2] • ログの収集・定期的な分析の実施 [No.4-4-3] • 社内システムにおける適切なネットワーク分離 [No.4-5-1] • 社外への不正通信の遮断(出口対策) [No.4-5-2]	防御(PR)
攻撃等の検知	**ネットワーク上の基礎的な監視等** • ネットワーク接続・データの監視[No.5-1-1]	**迅速な異常の検知** • 情報機器等の状態、挙動の監視・対応や分析[No.5-1-1,5-1-2]	検知(DE)
インシデントへの対応	**インシデント発生に備えた対応手順の整備** • インシデント対応手順の作成 [No.6-1-1]	*大分類「インシデントへの対応」において、★４での追加項目はなし	対応(RS)
インシデントからの復旧	**インシデント発生から復旧するための対策の整備** • インシデント発生から復旧するための対策の整備[No.7-1-1]	**インシデントからの復旧手順等の整備** • 復旧ポイント、復旧時間を満たす手順等の整備[No.7-1-1]	復旧(RC)