知らないと出遅れる？

セキュリティ対策評価制度とは

～2026年度開始予定～

BCC株式会社

1.「SCS評価制度」を一言でいうと？

一言でいえば、「企業のセキュリティ対策レベルを『星の数』で客観的に証明する、公的なものさし」です。

これまでは、「ウチはセキュリティしっかりやってます！」と企業が自己申告していても、取引先はそれが本当かどうか判断するのが難しい状況でした。この制度ができることで、国が決めた基準に基づいて専門家がチェックし、その結果を「星」で表示することで、
「この会社はこれくらいセキュリティがしっかりしている」という信頼がひと目で分かるようになります。

2．なぜこの制度が必要なのか？（背景）

ITの世界では、一つの小さな会社のセキュリティが破られると、そこを「踏み台」にして、取引先の大手企業や重要なシステムへ次々と攻撃が広がる「**サプライチェーン攻撃**」が大きな問題になっています。

- **今の悩み:**
  大手企業は取引先1社ずつに「セキュリティはどうなっていますか？」と
  アンケート（チェックシート）を送っていますが、形式的になりがちで、手間も膨大です。

- **解決したいこと:**
  共通の基準で評価することで、チェックの手間を省きつつ、
  サプライチェーン全体のセキュリティレベルを底上げしたい、というのが国の狙いです。

3．セキュリティレベルを分けている

評価は「★3」から「★5」の3段階で設定されています。

※★1と★2は、すでに存在する「SECURITY ACTION（自己宣言）」という制度がその役割を担います。

評価	レベル感	評価方法
★3	基礎的な対応。最低限実装すべきライン	専門家の確認付き自己評価
★4	標準的な対策。機密情報を扱う企業向け。	第三者（認定評価機関）による審査
★5	高度な対策。さらに厳しい環境向け。	第三者による高度な審査

重要ポイント: これは企業を優劣で競わせる「格付け」ではありません。
「うちはこのレベルの対策をしています」という信頼の証明書として活用するためのものです。

4．私たち（情シス担当者）はどう備えればいい？

1.現状を知る:

自社が現在どの程度のセキュリティ対策ができているか、チェックリストで確認します。

2.目的を決める:

取引先から「★3以上を取得してほしい」と言われるのか、それとも自社の信頼向上のために取るのか、目標を決めます。

3.不足を埋める:

足りない部分を強化します。国も「お助け隊」のような支援策を用意する予定なので、中小企業でも対応しやすい環境が整えられていくはずです。

概要まとめ：この制度で何が変わる？

取引の効率化	毎回バラバラな形式のセキュリティ調査票に回答する必要が減ります。
信頼の可視化	名刺やWebサイトに「★3取得済み」と書けるようになり、営業上の強みになります。
防御力の向上	何をすればいいか明確になるため、サイバー攻撃を受けにくい会社になります。

今はまだ詳細を詰めている段階ですが、2026年度下期にかけて、
今後「何をすればいいか」の具体的なガイドラインが出てきます。

※特に★5はまだまだ不確定事項が多いです。

最新情報は順次IPA公式サイトで公表されています。
https://www.ipa.go.jp/security/scs/index.html

続いてもう少し詳しいお話です

SCS評価制度において、**ITツールの導入（技術的対策）以上に重要視されるのが、「組織的対策」です**。ツールを入れても、それを運用するルールや人間側の意識がなければ、セキュリティは守れないからです。
★3と★4それぞれで求められる**「組織的対策」のポイントを解説**します。

1．★3（三つ星）に必要な組織的対策

【コンセプト：基礎的な守りの体制作り】 すべての企業が最低限やるべき「基本」の整備です。
「何かあったらどう動くか」を文書化し、ルール通りに実行できる状態を目指します。

セキュリティポリシーの明文化	「誰が責任者か」「どのような情報を扱うか」を社内ルールとして言語化します。
インシデント手順書の整備	「ウイルス感染や情報漏洩が発生したとき、誰に連絡し、どう封じ込めるか」という初動対応の手順を明確にします。
定期的なセキュリティ教育	全社員に対して「パスワード管理」や「不審なメールの扱い」など、基礎的なセキュリティ意識の向上を行います。
管理体制の構築	経営層がセキュリティに関心を持ち、必要な予算や人員を割く意志を表明（宣言）することが求められます。

2．★4（四つ星）に必要な組織的対策

【コンセプト：継続的改善と被害拡大の防止】 ★3の内容に加え、「より高度な脅威」や「サプライチェーンへの影響」を考慮した管理が求められます。

継続的改善（PDCA）	一度決めたポリシーや手順が古くなっていないか定期的に見直し、 改善し続ける仕組みが必要です。
実践的な対応演習	手順書があるだけでなく、実際にシミュレーションを行い、 事故発生時に組織がスムーズに連携できるかをテスト・記録します。
取引先管理の強化	自社だけでなく、自社の取引先（委託先等）に対してもセキュリティ管理を 要求し、サプライチェーン全体で守る体制を整えます。
リスク管理の高度化	最新の攻撃手法や自社の脆弱性を常に把握し、脅威の変化に合わせて 対策を機動的に更新する運用が求められます。

★3・★4 組織的対策の比較表

対策項目	★3（基礎）	★4（標準・高度）
ポリシー	基本ルールの策定・文書化	最新の脅威に合わせたルールの定期更新・適用
インシデント対応	手順書の整備・連絡ルートの確立	定期的な演習（机上演習など）の実施と記録
セキュリティ教育	全社員向けの基礎教育	役職や業務内容に応じたより専門的な教育
体制・管理	経営層の関与・方針表明	組織全体での継続的改善（PDCAサイクル）の確立
評価主体	専門家の確認＋自己評価	第三者評価機関による客観的な審査

3.情報処理安全確保支援士が得意とするサポート分野

情報処理安全確保支援士の役割は、単にファイアウォールを設置することではなく、「**ビジネスを止めないためのルール作りと、それを守る仕組みの運用**」です。

セキュリティポリシーの策定	企業の業種、規模、扱う情報資産に合わせて 「何をどこまで守るべきか」を定義し、文書化をサポートします。
インシデント対応計画の策定	どんな事故が起きそうかを想定し（リスクアセスメント）、 その際の報告フローや復旧手順を設計します。
教育・トレーニング	従業員向けの研修プログラム作成や、 理解度を測るためのテスト作成などを行います。
制度適合のための ギャップ分析	「現在の社内ルール」と「SCS評価制度の要件」を比較し、 何が足りないかをリストアップ（ギャップ分析）して、優先順位をつけて 修正案を提示してくれます。

4.★3と★4でのサポート内容の違い

支援士の方に依頼する際、★のレベルによってアプローチが変わります。

求めるレベル	支援士に依頼する際のポイント
★3（基礎）	「テンプレートの活用と最適化」 ゼロから作ると大変なポリシーや手順書を、標準的な雛形をベースに自社向けにカスタマイズしてもらう作業が中心です。
★4（標準・高度）	「運用実績の裏付けと改善」 規程を作るだけでなく、それが実際に機能しているか（演習の評価や、脆弱性の定期的チェック）を客観的に評価し、PDCAを回すための「監査役」のような立ち位置で支援してもらいます。

5.なぜ「支援士」に頼むのが一番の近道か？

第三者の視点	社内の人間だと「うちはこれで十分だ」と思い込んでいる箇所を、支援士は「SCSの評価基準では、ここが不十分です」と冷静に指摘できます。
最新情報のアップデート	SCS評価制度は今後、細かいルールやガイドラインが更新されていく可能性があります。支援士は専門家として常に最新の法改正や脅威情報を追いかけているため、制度の動向に合わせた最適なアドバイスがもらえます。

アドバイス

「技術的な構築は社内でやるから、組織的なルール作りと審査を通るためのドキュメントチェックをサポートしてほしい」と具体的に相談すると、予算も抑えられ、かつ効率よく進められるはずです。

まず専門家と一緒に、現状の「棚卸し」から始めてみませんか？

「まずは★3の要件を満たしているか確認したい」

「自社の現在のセキュリティレベルを客観的に知りたい」

そうした段階でも全く問題ありません。
導入の有無にかかわらず、貴社のセキュリティ対策に関する現状や課題について
お気軽にご相談いただけます。
新制度に向けて少しでも気になる点や不安がございましたら、
まずはお気軽に弊社までお問い合わせください！

お問い合わせはこちら

会社概要

商号	ＢＣＣ株式会社		
事業所	東京本社 ：東京都千代田区外神田６-15-９ 明治安田生命末広町ビル９Ｆ 大阪本社 ：大阪市中央区今橋2-5-8 トレードピア淀屋橋9Ｆ		
代表取締役社長	伊藤一彦		
創立	2002年3月	主要部門	・営業アウトソーシング ・ソリューション
カンパニー名	IT営業アウトソーシングカンパニー	カンパニー長	松村健太
許認可	一般労働者派遣事業（派27-302361） 有料職業紹介事業（27-ユ-302045） プライバシーマーク認定（第10861424(07)号） 電気通信事業（E-28-03972)		
主要取引先	株式会社インターネットイニシアティブ(IIJ) 日鉄ソリューションズ株式会社 ダイワボウ情報システム株式会社 日本電気株式会社(NEC)		