IT Expert ServicesによるSCS評価制度への対応のご紹介

今回のITトピックスでは、IT Expert Services による「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（以下SCS評価制度）」への対応についてご紹介します。

経営者

ニュースではよく見かけるけど、実際何をしたらいいかよくわからない。

経済産業省が出している資料を見たけど、難しくて対応方法がわからない！

社員

SCS評価制度の概要

SCS評価制度はサプライチェーン全体でサイバー攻撃に強くなるために、 経済産業省（以下経産省）が運用開始を目指している制度です。企業のセキュリティ対策をIPAのSECURITY ACTION※1の★による定義を拡張し、新たに★3～5の段階を設ける予定で検討が進められております。 ★3・4について2026年度末頃の運用開始を目指しています。

★の基準で分かりやすく見える化し、発注側・受注側の両方が、適切なレベルの対策を選びやすく・説明しやすくすることを目的としています。

（事業者のセキュリティ対策レベルを競わせることを目的とした格付けのようなものではありません。）

※1出典：IPA「SECURITY ACTION」
https://www.ipa.go.jp/security/security-action/sa/

成熟度の定義	三つ星（★3）	四つ星（★4）	五つ星（★5）検討中
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**到達点として目指すべき対策**： • 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プロセスを整備した上で、システムに対しては現時点でのベストプラクティスに基づく対策を実施
評価スキーム	専門家確認付き自己評価	第三者評価	第三者評価

出典：経産省「サプライチェーン強化に向けたセキュリティ対策制度に関する制度構築方針」
(弊社にて再編集)　https://www.meti.go.jp/files/900017305.pdf

次ページに続く

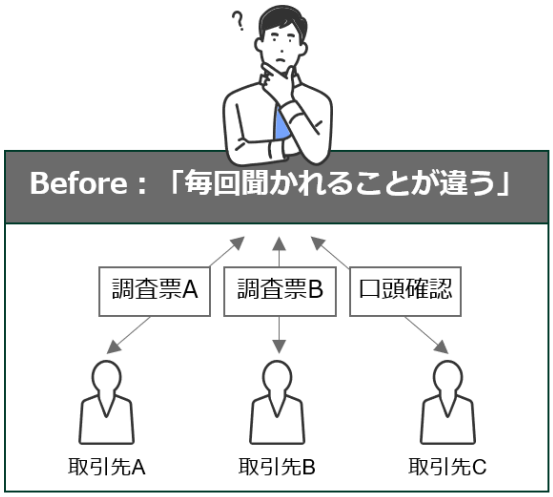
サプライチェーン企業が★を取得するメリット

現在の調達では、発注者ごとに異なる要求対応が求められ、複数社と取引を行う場合には、それぞれの会社からの要求に対応するのが困難な状況です。

SCS評価制度を運用した場合、★の取得が、発注企業・受注企業双方にとっての**「共通のものさし」**となり、**対応工数の削減や業務の標準化・効率化**につながります。

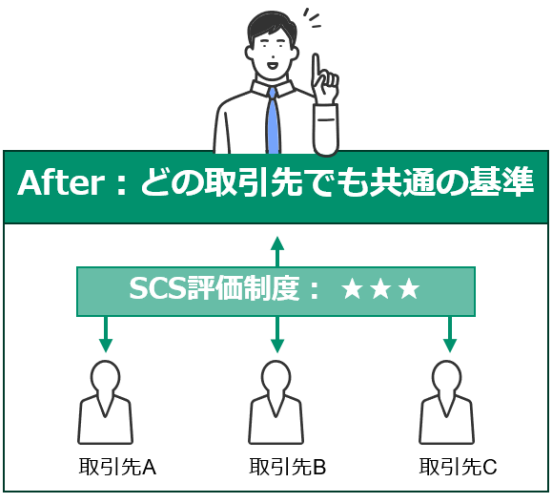
SCS評価制度導入によりセキュリティチェックのプロセスが明確に、容易になる。

現在の調達



取引先（発注者）ごとに求めてくるセキュリティ要件がバラバラで対応が大変…

SCS評価制度に基づく調達



受注者側が★評価を公表することで、取引先（発注者）も受注者もセキュリティ要件確認が容易になる

IT Expert ServicesによるSCS評価制度への対応

SCS評価制度に対応するためには、経産省が定めた評価基準に対応する必要があります。本トピックでは、★3の基準に対するIT Expert Servicesの対応についてご紹介します。
2026年3月27日更新の経産省の公表内容を元に対応を弊社で想定してみました。
(今秋経産省より、要求項目・評価基準を満たす実装例などをまとめた評価ガイド等公表される予定です)

★3の要求項目は26個あり、さらに評価基準に分解すると81の項目に分かれます。その中では、組織のルールや運用にかかわるルールを整備することが記載されており、13項目については、ツールでの対応が可能な項目になっています。そのうちIT Expert Servicesでは、10の項目をカバーすることが可能と考えております。　(2026年7月時点での評価基準に対する弊社解釈による)

次ページに続く

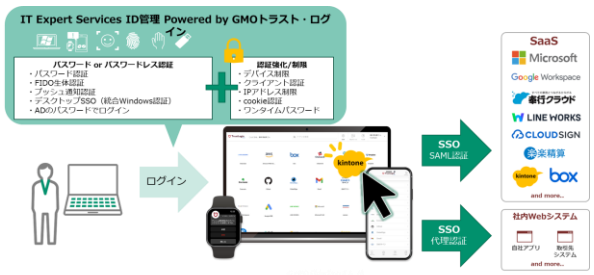
SCS評価制度の評価項目に対する対応

(2026年3月27日経済産業省公表の構築方針への対応を弊社にて想定)

大分類	項番	★3　要求事項名(26項目)	ルール整備	ツール要否	IT Expert Servicesで対応
ガバナンスの整備	1	セキュリティ推進活動部門	○		
	2	守秘義務のルール	○		
	3	セキュリティポリシーの策定	○		
取引先管理	4	取引先とのビジネス又はシステム上の関係	○		
	5	機密情報の取扱い	○		
	6	セキュリティインシデント発生時の役割・責任	○		
リスクの特定	7	情報機器、OS及びソフトウェアに関する情報の把握	○	○	○
	8	ネットワークに関する情報の把握	○	○	
	9	外部情報サービスの管理	○		
	10	機密区分に応じた情報の管理	○		
攻撃等の防御	11	ユーザIDの管理手続	○	○	○
	12	管理者IDの管理手続	○	○	○
	13	認証の強度・実装方法の決定	○	○	○
	14	アカウントロック制御	○		
	15	パスワード設定ルール	○	○	○
	16	パスワード管理ルール	○		
	17	アクセス権の管理ルール	○		
	18	セキュリティインシデント発生時の教育・訓練	○	○	
	19	適切なバックアップ	○	○	○
	20	ハードウェア、OS及びソフトウェアの安全な構成	○	○	
	21	セキュリティパッチ・アップデートの手続	○	○	○
	22	マルウェア感染からの保護	○	○	○
	23	ネットワーク境界防護	○	○	○
攻撃等の検知	24	ネットワーク接続・データの監視	○	○	○
インシデントへの対応	25	インシデント対応手順	○		
インシデントからの復旧	26	事業継続要件に沿った復旧準備	○		

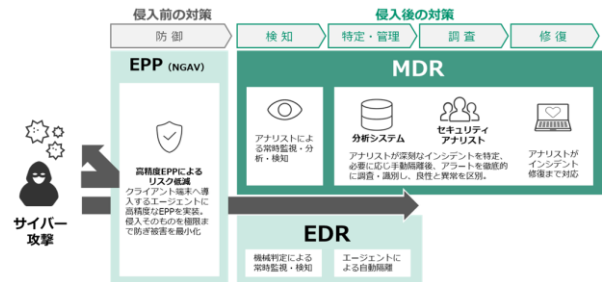
SCS評価制度へ対応するIT Expert Servicesの主なサービス

ID・パスワード管理
IT Expert Services ID管理



多要素認証やSSO機能を提供し、SCS評価制度における「認証の強化」やアクセス制御にご利用いただくことができます。更にパスワードを覚える必要がなくなることでお客様の業務効率UPにも貢献します。

端末セキュリティ
IT Expert Services EDR/MDR



EPPおよびEDRのツールを提供するとともに、それらを用いてインシデントの対応も行うMDRもご用意しており、「端末内の挙動を検知」や「インシデントの対応・復旧」としてご利用いただけます。

今回は、IT Expert Services によるSCS評価制度対応についてご紹介しました。制度対応に向けて、弊社ではアセスメントや、IT Expert Services以外にも具体的なセキュリティソリューションを展開しております。制度に関する詳しい内容等につきましては、以下、弊社公式HPでご確認ください。

経済産業省セキュリティ対策評価制度の対応についてお任せください

(2026年8月発行月次レポート「ITトピックス」の内容を一部修正して掲載しております。)