

セキュリティ対策状況チェックシート

経済産業省「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)」★3の要求事項26件に沿った設問です。

ご回答のしかた 回答は「はい／一部／いいえ／該当なし」から選んでください。「一部」「いいえ」のときは、満たしていない評価基準No.を書いてください。未対応の項目は「いいえ」のままで構いません。現状を知ることが目的です。

設問は評価基準を平易に言い換えたもので、食い違う場合は評価基準の原文(IPA公表、2026年3月27日版)が優先します。本シートの回答は、★3の取得や適合を判定・証明するものではありません。

基本情報

項目	記入欄
会社名	
回答者(部署・氏名・連絡先)	
回答日	
委託されている業務	
取り扱う発注元の情報(個人情報・技術情報など)	
再委託の有無と再委託先	
従業員数(派遣・業務委託を含む)	

設問（SCS★3 要求事項26件）

No	設問	回答	満たしていない 評価基準No.	根拠・証跡(規程名・ツール名／ 提出できるか)	対応する制度・番号
1	【体制】セキュリティを統括する役員と担当部署を決め、役割・責任と連絡先を書面にしていますか。年1回以上見直していますか。	☐ はい ☐ 一部 ☐ いいえ ☐ 該当なし			SCS★3 1-2-1 評価基準 1-2-1-1～3

No	設問	回答	満たしていない 評価基準No.	根拠・証跡(規程名・ツール名/ 提出できるか)	対応する制度・番号
2	【体制】役員・従業員・派遣社員・受入出向者に適用する守秘義務のルールがあり、入社時・受入れ時に説明していますか。	☐ はい ☐ 一部 ☐ いいえ ☐ 該当なし			SCS★3 1-2-3 評価基準 1-2-3-1～2
3	【体制】セキュリティ対応方針を定め、全員が最新版をいつでも見られるようにし、改定したときに周知していますか。	☐ はい ☐ 一部 ☐ いいえ ☐ 該当なし			SCS★3 1-3-1 評価基準 1-3-1-1～3
4	【取引先】取引先(顧客・関係会社・クラウド事業者を含む)が管理していて、自社の機器がつながっているシステムを把握し、年1回以上見直していますか。	☐ はい ☐ 一部 ☐ いいえ ☐ 該当なし			SCS★3 2-1-1 評価基準 2-1-1-1～2
5	【取引先】機密情報を共有する取引先・再委託先と、業務を始める前に「機密情報の定義／利用制限・保管・複製・第三者提供／返還・廃棄」を取り決めていますか。	☐ はい ☐ 一部 ☐ いいえ ☐ 該当なし			SCS★3 2-1-2 評価基準 2-1-2-1
6	【取引先】同じ相手と、事故が起きたときの役割と責任を決めていますか。	☐ はい ☐ 一部 ☐ いいえ ☐ 該当なし			SCS★3 2-1-4 評価基準 2-1-4-1
7	【資産】PC・サーバのメーカー・OS・台数を把握し、導入・ネットワーク接続・パッチ適用の管理ルールを定め、年1回以上点検していますか。	☐ はい ☐ 一部 ☐ いいえ ☐ 該当なし			SCS★3 3-1-1 評価基準 3-1-1-1～4
8	【資産】社内ネットワーク(所在地・用途)と、ネットワーク機器(メーカー・型番・保守業者)を把握していますか。	☐ はい ☐ 一部 ☐ いいえ ☐ 該当なし			SCS★3 3-1-2 評価基準 3-1-2-1～2
9	【資産】機密情報を扱うクラウドなど外部サービスについて、セキュリティ要件を決めて利用時に確認し、提供事業者と機密情報の扱いを合意していますか。	☐ はい ☐ 一部 ☐ いいえ ☐ 該当なし			SCS★3 3-1-3 評価基準 3-1-3-1～2
10	【資産】機密区分のルール(機密の特定・レベルの判定と表示・区分ごとの扱い方・取扱エリア)を定めて年1回以上点検し、重要な機密情報の管理者・保管場所・開示先を把握していますか。	☐ はい ☐ 一部 ☐ いいえ ☐ 該当なし			SCS★3 3-1-4 評価基準 3-1-4-1～3
11	【ID】ユーザIDの発行・変更・削除を申請・承認制にし、IDを共有せず(やむを得ない場合は使った人を特定でき)、不要になったIDと権限をすぐに削除・無効化していますか。	☐ はい ☐ 一部 ☐ いいえ ☐ 該当なし			SCS★3 4-1-1 評価基準 4-1-1-1～4

No	設問	回答	満たしていない 評価基準No.	根拠・証跡(規程名・ツール名/ 提出できるか)	対応する制度・番号
12	【ID】すべてのサーバ・ネットワーク機器に管理者と責任者を決め、管理者IDが必要な人に限定・非共有・最小権限・申請承認制にし、開発環境の管理者権限で本番環境を操作できないようにしていますか。	☐ はい ☐ 一部 ☐ いいえ ☐ 該当なし			SCS★3 4-1-2 評価基準 4-1-2-1～8
13	【認証】すべてのIDでパスワードなどによる認証を行い、重要な機密情報を扱うクラウドサービスでは常に多要素認証(パスワードは8文字以上)を使っていますか。	☐ はい ☐ 一部 ☐ いいえ ☐ 該当なし			SCS★3 4-1-3 評価基準 4-1-3-1～4
14	【認証】PC・スマートデバイスは、ログオンに10回以上失敗するとロックされる設定(失敗のたびに待ち時間が延びる設定でも可)で、パスワードかPINは6文字以上ですか。	☐ はい ☐ 一部 ☐ いいえ ☐ 該当なし			SCS★3 4-1-4 評価基準 4-1-4-1～2
15	【認証】パスワードのルール(初期パスワードの変更・推測されやすい語の禁止・長さ・使い回しの禁止)を定め、全員に周知していますか。	☐ はい ☐ 一部 ☐ いいえ ☐ 該当なし			SCS★3 4-1-5 評価基準 4-1-5-1～5
16	【認証】パスワードの安全な保管方法(管理アプリなど)と、漏れたとき・漏れた疑いがあるときにすぐ変更する手順を定め、周知していますか。	☐ はい ☐ 一部 ☐ いいえ ☐ 該当なし			SCS★3 4-1-6 評価基準 4-1-6-1～3
17	【権限】システム・PCのアクセス権と、機密を扱う部屋への入室権限について、申請承認制・必要な範囲だけに限定・棚卸・台帳管理のルールを定めていますか。	☐ はい ☐ 一部 ☐ いいえ ☐ 該当なし			SCS★3 4-1-7 評価基準 4-1-7-1
18	【教育】入社・受入れ時と年1回以上、事故が起きたときの対応について、資料の配布に加えてeラーニングか集合研修を行い、実施記録を残していますか。	☐ はい ☐ 一部 ☐ いいえ ☐ 該当なし			SCS★3 4-2-2 評価基準 4-2-2-1～3
19	【データ】バックアップの対象・頻度・保管期間を決めて取得し、重要な機密情報は遠隔地にも保管し、対象ごとに復元手順書がありますか。	☐ はい ☐ 一部 ☐ いいえ ☐ 該当なし			SCS★3 4-3-4 評価基準 4-3-4-1～3
20	【端末】許可していないソフトの削除(またはインストール制限)、USBなどの自動実行の無効化、サーバ・ネットワーク機器の設定変更の申請承認制を行っていますか。	☐ はい ☐ 一部 ☐ いいえ ☐ 該当なし			SCS★3 4-4-1 評価基準 4-4-1-1～3

No	設問	回答	満たしていない 評価基準No.	根拠・証跡(規程名・ツール名/ 提出できるか)	対応する制度・番号
21	【端末】サポートが切れた製品を使わず(またはネットから遮断し)、 重大・高リスク(CVSS 7.0以上など)の更新は公開から14日以内に 適用していますか。	☐ はい ☐ 一部 ☐ いいえ ☐ 該当なし			SCS★3 4-4-4 評価基準 4-4-4-1～2
22	【端末】ネットワークにつながる全PC・サーバにマルウェア対策ソフトを 入れ、スキャンの範囲・頻度を決めて実行し、定義ファイルを 更新していますか。	☐ はい ☐ 一部 ☐ いいえ ☐ 該当なし			SCS★3 4-4-5 評価基準 4-4-5-1～3
23	【境界】ファイアウォール・ルーターの初期管理パスワードを変更(または リモート管理を無効化)し、認証されていない外からの通信を遮断し、 通信ルールを管理して不要分を削除していますか。ネット経由で設定を 変えるときは多要素認証かIP制限をしていますか。	☐ はい ☐ 一部 ☐ いいえ ☐ 該当なし			SCS★3 4-5-1 評価基準 4-5-1-1～7
24	【検知】外から社内への不正な通信と、社内から不正なサーバへの 通信を、リアルタイムに検知・遮断する仕組みがあり、アラートを 担当者が判断し、速報が届く体制ですか。	☐ はい ☐ 一部 ☐ いいえ ☐ 該当なし			SCS★3 5-1-1 評価基準 5-1-1-1～3
25	【事故対応】事故対応の手順(発見報告→初動→調査・ 対応→復旧→最終報告)、社内外の連絡先と報告ルート、責任者の 役割、報告様式を定めて年1回以上点検し、事例を社内で 共有していますか。	☐ はい ☐ 一部 ☐ いいえ ☐ 該当なし			SCS★3 6-1-1 評価基準 6-1-1-1～6
26	【復旧】事業上重要なシステムについて、サイバー攻撃を想定した 目標復旧レベルを決め、待機系や人手で業務を続ける手段(取引先の 連絡先・複数の連絡手段など)を用意していますか。	☐ はい ☐ 一部 ☐ いいえ ☐ 該当なし			SCS★3 7-1-1 評価基準 7-1-1-1

追加シート（発注元から依頼があった場合のみ）

SCS★4にだけある要求事項17件です。回答の欄は上と同じです。

No	設問	回答	満たしていない 評価基準No.	根拠・証跡(規程名・ツール名/ 提出できるか)	対応する制度・番号
A1	【体制】自社に関する法令・業界の基準・取引先の要求を把握して社内ルールを定め、年1回以上見直して周知していますか。	☐ はい ☐ 一部 ☐ いいえ ☐ 該当なし			SCS★4 1-1-1
A2	【体制】攻撃や脆弱性の情報を集め、ログなどと突き合わせて予兆を見つける体制がありますか。	☐ はい ☐ 一部 ☐ いいえ ☐ 該当なし			SCS★4 1-2-2
A3	【体制】年1回以上、対策の実態と推進計画を統括役員に報告し、指示を記録して計画に反映していますか。	☐ はい ☐ 一部 ☐ いいえ ☐ 該当なし			SCS★4 1-4-1
A4	【取引先】影響の大きい取引先・再委託先のセキュリティ対策状況を、年1回以上把握していますか。	☐ はい ☐ 一部 ☐ いいえ ☐ 該当なし			SCS★4 2-1-3
A5	【取引先】契約終了時に、取引先・再委託先から機密情報とアクセス権を回収・廃棄させたことを確認する手順がありますか。	☐ はい ☐ 一部 ☐ いいえ ☐ 該当なし			SCS★4 2-1-5
A6	【資産】リモートワークで使う機器(個人所有を含む)と扱える機密情報のルールを定め、周知し、年1回以上点検していますか。	☐ はい ☐ 一部 ☐ いいえ ☐ 該当なし			SCS★4 3-1-5
A7	【資産】脆弱性情報の集め方・対応の判断基準・担当を定め、対応履歴を記録して月次で漏れを点検していますか。	☐ はい ☐ 一部 ☐ いいえ ☐ 該当なし			SCS★4 3-2-1
A8	【物理】サーバの設置場所を施錠し、入れる人を限定し、入退場記録を6か月以上保管していますか。	☐ はい ☐ 一部 ☐ いいえ ☐ 該当なし			SCS★4 4-1-8
A9	【物理】PC・スマホ・カメラ・USBなど(個人所有を含む)と機密書類の持込み・持出しルールを定め、年1回以上点検していますか。	☐ はい ☐ 一部 ☐ いいえ ☐ 該当なし			SCS★4 4-1-9
A10	【教育】経営層を含む全員に、入社時と年1回以上、セキュリティの意識向上の教育を行い、記録していますか。	☐ はい ☐ 一部 ☐ いいえ ☐ 該当なし			SCS★4 4-2-1

No	設問	回答	満たしていない 評価基準No.	根拠・証跡(規程名・ツール名/ 提出できるか)	対応する制度・番号
A11	【データ】社外に持ち出すPC・記憶媒体と、重要な機密情報を暗号化するルールを定め、周知していますか。	☐ はい ☐ 一部 ☐ いいえ ☐ 該当なし			SCS★4 4-3-1
A12	【データ】業務に欠かせないデータはPCではなく、より安全なサーバやクラウドに保管するルールがありますか。	☐ はい ☐ 一部 ☐ いいえ ☐ 該当なし			SCS★4 4-3-2
A13	【データ】社外とのファイル共有・送信のルール(共有する相手・送り方)を定め、周知していますか。	☐ はい ☐ 一部 ☐ いいえ ☐ 該当なし			SCS★4 4-3-3
A14	【端末】サポート切れのOS・ソフトを使わないか、やむを得ず使う場合は代替りの対策と更新の計画がありますか。	☐ はい ☐ 一部 ☐ いいえ ☐ 該当なし			SCS★4 4-4-2
A15	【ログ】ファイアウォールなど事故調査に必要なログを決めた期間保管し、認証サーバのログを月1回以上確認していますか。	☐ はい ☐ 一部 ☐ いいえ ☐ 該当なし			SCS★4 4-4-3
A16	【検知】会社支給PCで使ってよいソフトの一覧を作って年1回以上点検し、外から受け取ったファイルを自動でスキャンしていますか。	☐ はい ☐ 一部 ☐ いいえ ☐ 該当なし			SCS★4 5-1-2
A17	【事故対応】事故のレベルとレベルごとの対応範囲を定め、周知していますか。	☐ はい ☐ 一部 ☐ いいえ ☐ 該当なし			SCS★4 5-2-1

出典:IPA「SCS評価制度 ★3・★4 要求事項・評価基準」(2026年3月27日版)。シート作成:Moshiru(moshiru.com)