

うちの会社の「やりがち」点検24項目

多くの会社でついやってしまうことを、経済産業省のSCS評価制度★3の要求事項に沿って24項目にまとめました。当てはまるものに印を付けるだけで、10分ほどで終わります。

点検するあなたにとって

こんなとき	このシートがあると
社長や上司に「うちは大丈夫？」と聞かれた	10分で、どこが弱いかを1枚で答えられます
取引先からセキュリティのチェックシートが届いた	どの設問でつまずきそうか、届く前に分かっています
対策や予算を提案したい	全項目に国の制度の番号が付いているので、自分の意見ではなく基準として出せます
全部を一人で直すのは無理だと思っている	項目ごとに「自分でできる／社内で決める／専門家向き」を付けています。抱えるのは一部だけで済みます

使い方

1. 当てはまる項目の「印」の□に印を付けます。分からない項目も、当てはまるとして印を付けてください
2. 印の付いた項目を、右の「誰がやるか」ごとに分けます
3. 最後のページの「結果の生かし方」で、次の一手を決めます

点検項目（当てはまるものに印）

No	やりがちなこと	印	困ること	誰がやるか	SCS★3
1	【体制】セキュリティの責任者が決まっていない	☐	事故や取引先の問い合わせが来たとき、誰が判断するかで止まる	社内で決める	1-2-1
2	【体制】社内ルール(方針)を作ったきり、誰も見ていない	☐	ルールがあっても守られていなければ、取引先には「ない」のと同じに映る	社内で決める	1-3-1
3	【取引先】取引先と機密情報の扱いを口約束で済ませている	☐	漏えいしたとき、どちらが何をするかで揉める	社内で決める	2-1-2
4	【取引先】委託先・再委託先が事故を起こしたときの連絡方法を決めていない	☐	委託先での事故に気づくのが遅れる	社内で決める	2-1-4
5	【資産】PC・スマホの台数と使っている人の一覧がない	☐	更新漏れや紛失に気づけない	自分でできる	3-1-1

No	やりがちなこと	印	困ること	誰がやるか	SCS★3
6	【資産】社員が業務でどのクラウドサービスを使っているか把握していない	☐	会社の知らない場所に顧客情報が置かれる	社内で決める	3-1-3
7	【資産】共有リンクを「リンクを知っている全員」で出したままにしている	☐	リンクが転送されると、誰でも見られる状態になる	自分でできる	3-1-4
8	【ID】退職・異動した人のアカウントが残っている	☐	使われていないIDは、乗っ取られても気づきにくい	自分でできる	4-1-1
9	【ID】1つのIDを複数人で使い回している	☐	誰が操作したのか後から分らない	社内で決める	4-1-1
10	【ID】社員全員がPCの管理者権限を持っている	☐	不審なソフトが入ったとき、PC全体に影響が広がる	専門家向き	4-1-2
11	【認証】メール・クラウドに多要素認証を設定していない	☐	パスワードが漏れると、そのままログインされる	自分でできる	4-1-3
12	【認証】パスワードを複数のサービスで使い回している	☐	1か所で漏れると、ほかのサービスにも入られる	自分でできる	4-1-5
13	【認証】ルーター・複合機・NASの初期パスワードを変えていない	☐	初期パスワードは公開されていることが多い	専門家向き	4-1-5 4-5-1
14	【認証】パスワードを付箋や共有のExcelに書いている	☐	見た人、開けた人なら誰でも使える	自分でできる	4-1-6
15	【教育】不審なメールを開いたときの報告先を、全員は知らない	☐	報告が遅れるほど被害が広がる	社内で決める	4-2-2
16	【データ】バックアップを、社内に常時つないだNASにだけ取っている	☐	ランサムウェアはつながった保存先も暗号化することがある	専門家向き	4-3-4
17	【データ】バックアップから元に戻せるか、試したことがない	☐	いざ戻そうとして戻らないことに、その時に気づく	社内で決める	4-3-4 7-1-1
18	【端末】WindowsやブラウザのUpdateを後回しにしている	☐	修正済みの弱点を、そのまま突かれる	自分でできる	4-4-4
19	【端末】サポートが切れたPC・ソフト・機器を使っている	☐	弱点が見つかって、もう修正されない	社内で決める	4-4-4
20	【端末】マルウェア対策ソフトが入っていない、または期限切れのPCがある	☐	不審なファイルを止められない	自分でできる	4-4-5
21	【境界】VPN機器・ファイアウォールの更新を誰が見ているか分らない	☐	社外から入る入口の弱点は、狙われやすい	専門家向き	4-4-4 4-5-1
22	【境界】Webサイトや問い合わせフォームの更新を、制作会社任せにしている	☐	外から見える場所は、誰でも調べられる	専門家向き	4-4-4 3-1-3

No	やりがちなこと	印	困ること	誰がやるか	SCS★3
23	【検知】不正な通信を見つける仕組みがあるか分からない	☐	侵入されても気づかないまま時間が過ぎる	専門家向き	5-1-1
24	【事故対応】事故が起きたとき、誰に何を報告するかが決まっていない	☐	最初の数時間を、連絡先探しに使ってしまう	社内で決める	6-1-1

内訳:自分のできる 8項目／社内で決める 10項目／専門家向き 6項目

結果の生かし方

印の数で良し悪しを決めるものではありません。「誰がやるか」ごとに、次の一手が決まります。

誰がやるか	目安	次の一手
自分ができる	設定の変更や整理で済むもの。手順はメーカーやサービスの公式ヘルプにあります	今週中に、印の付いたものから片づける
社内で決める	担当やルールを決めれば済むもの。お金はほとんどかかりません	このシートを上司に見せて、担当と期限を決めてもらう
専門家向き	機器の設定や外からの調査に、専門の知識が要るもの	自分で調べ切ろうとせず、外部に任せる

専門家向きの項目は、まとめて任せられます

「よく分からないので、もうお願いしてしまいたい」という項目は、Moshiruにまとめてご相談いただけます。

- ・ 外から見える範囲の無料スキャン: Webサイトなど、外から見える場所の弱点を確認します(実施の許可と所有の確認をいただいたうえで行います)
- ・ 取引先から届いたチェックシートの回答: この点検で分かった現状をもとに、回答を作ります
- ・ 打合せなし: やり取りはすべてテキストで完結します

moshiru.com / info@moshiru.com

このシートについて

- ・ 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)」の★3 要求事項・評価基準(IPA公表、2026年3月27日版)のうち、多くの会社で抜けやすい点を24項目に言い換えたものです。★3の全項目(26件)ではなく、★3の取得や適合を判定するものでもありません
- ・ ★3の全26項目で確認したい場合は、同じ基準で作った「委託先セキュリティ対策状況チェックシート」を自社に当てはめて使えます
- ・ 出典: IPA「SCS評価制度 ★3・★4 要求事項・評価基準」<https://www.ipa.go.jp/security/scs/rcu1hd0000007a2i-att/20260327001-c.xlsx>
- ・ 作成: Moshiru(岡崎悠太)。無料で使えます。社内で自由に改変・配布して構いません