無料・登録不要 / v1.4 / 2026/11/06

国の注意喚起、うちは何から？
——対応点検表（2026年10月版）

2026年10月7日から9日にかけて、個人情報保護委員会、JPCERT/CC、警察庁、国家サイバー統括室、 総務省、経済産業省、IPA、金融庁の8機関が、企業にセキュリティ対策の点検を求めました。 文書は機関ごとに分かれていますが、求めている対策は大きく重なっており、**整理すると17項目にまとまります。 本資料はこの17項目に「やる順番」を付け、1枚の表にしたものです。**

並べ方＝追加費用なしで着手できるものを先に、同じ条件なら**求めた機関が多いもの**を先にしました。「最初に動く人」は、その項目で最初に動く部署です。**順番は「すぐ着手できるか」で付けており、緊急度の順ではありません。**すでに被害が疑われる場合は、3番「侵害の痕跡がないか調査、点検する」を IPA が示すとおり最初に行ってください。
17項目の内訳＝追加費用なしで着手できる**7**／費用がかかることが多い4／当社の診断では一部しか測れない4／当社の診断では測らない**2**。最初の7項目（表の1〜7番）は、すでに持っているツールの設定と運用ルールの見直しで始められます。
いちばん右は当社の診断（25〜27問）で数値化できるかどうかです。**測らないものは「測らない」と書いています**（2ページ目に、自分で確認するためのチェック項目11問を付けました）。読むのに約15分。そのまま上司や経営層に出す1枚として使えます。**迷ったら、Excel 版の「段階1」の3問（A-14・B-1・C-1）から。**

順	対策項目	点検表の問い（ID）	求めた機関数	最初に動く人	費用	当社診断で測れるか
1	経営層が関与する	E-1〜E-2	6	経営層	追加費用なし	測れる
2	脆弱性に対応する	A-13〜A-15	5	情シス	追加費用なし	測れる
3	侵害の痕跡がないか調査、点検する	C-1〜C-3	4	情シス	追加費用なし	測れる
4	権限の付与を見直す	B-3〜B-5	4	情シス	追加費用なし	測れる
5	委託先を含めて管理する	E-3〜E-4	4	情シス＋調達	追加費用なし	測れる
6	インシデント発生時の対応	C-9〜C-13	3	情シス	追加費用なし	測れる
7	保存データを暗号化する	D-3	2	情シス	追加費用なし	測れる
8	自組織のシステムの認証を強化する	B-1〜B-2・B-6〜B-7	4	情シス	有償を含む（目安100〜300万円/年）	測れる
9	ログを取得し一定期間保管する	C-4〜C-6	3	情シス	有償（目安100〜300万円/年）	測れる
10	不正アクセスを検知する仕組みを整える	C-7〜C-8	3	情シス	有償（目安50〜150万円/年）	測れる
11	外部への公開範囲を見直す	A-1〜A-4・A-16〜A-17	2	情シス＋調達	有償（目安50〜150万円/年）	測れる
12	漏えいした情報の悪用を防ぐ	C-14〜C-15	5	情シス	未判定	一部だけ
13	API の管理状況やアクセス制御を見直す	A-5〜A-9	3	開発／運用	未判定	一部だけ
14	不要になったデータを残さない	D-1〜D-2・D-6	3	情シス	未判定	一部だけ
15	通信を暗号化する	D-4〜D-5	2	情シス	未判定	一部だけ
16	被害や攻撃に関する情報を提供、共有する	E-5〜E-7	3	開発／運用	別紙を参照	測らない
17	大量アクセスを制限する	A-10〜A-12	2	開発／運用	別紙を参照	測らない

「求めた機関数」＝2026年10月7日から9日に公表された8機関の文書のうち、その項目に言及していた機関の数。 17項目の区切りは、照らし合わせやすいよう、セキュリティ研究者 piyokango 氏の横断整理（2026年10月11日）に揃え、当社が8機関の原文で照合しました。 当社が加えたのは「すぐ着手できる順」「最初に動く人」「費用の目安」「当社の診断で測れるか」の4列と、測らない項目の確認シートです。 費用の目安は当社が過去の支援で見た範囲のもので、見積ではありません。 費用の欄の「未判定」は、当社がその項目の費用を判定していないという意味です（かからないという意味ではありません）。 「一部だけ」＝一部は当社の診断で測れますが、全体はカバーしていません。「測らない」＝当社の診断の範囲外です。どちらも2ページ目の問いで確かめられます。

別紙：当社の診断では測らない 2項目（自分で確かめる）

> 1ページ目の「当社診断で測れるか」の見方＝**測れる**は、当社の診断に設問があり、次の一手（実行地図のタスク）まで出る項目です。**一部だけ**は、項目の一部しか設問で測れない項目、**測らない**は、当社の診断の範囲に入れていない項目です。

表の最後の2項目は、当社の診断（25〜27問）の範囲に入れていません。 **そのかわり、自分で確認できる形にしました。** 「はい」と言い切れない欄が、今週の宿題です。

被害や攻撃に関する情報を提供、共有する（3問）

- ☐ **E-5**　同じ業界や取引先と、情報を共有する先（団体・窓口）が決まっている
- ☐ **E-6**　個人情報保護委員会のほかに報告が要る当局（所管の省庁など）と、その期限を、誰かが知っている
- ☐ **E-7**　社外に共有してよい情報と、出してはいけない情報の線引きが文書になっている

大量アクセスを制限する（3問）

- ☐ **A-10**　同じ相手からの大量のアクセスに、回数の上限をかけている
- ☐ **A-11**　上限を超えたアクセスが記録に残り、誰かが見ている
- ☐ **A-12**　IP アドレスを変えながらの大量アクセスにも気づける（アカウントごと・API ごとに回数を数えられる）

「一部だけ」の4項目＝測れる部分と、自分で確認する部分

表の12〜15番は、当社の診断で**一部は測れますが、全体はカバーしていません。** どこまでが測れて、どこからが自分で確認する部分かを分けました。右端の問いが、その項目の宿題です。

順	対策項目	診断で測れる部分	測れない部分	自分で確認する問い
12	漏えいした情報の悪用を防ぐ	Q19 社外（監督官庁・顧客）への連絡先	本人への通知と、二次被害を防ぐ手当て	☐ **C-14**　情報が漏れたとき、誰に何を知らせるかが文書になっている
13	API の管理状況やアクセス制御を見直す	Q27 システムをつなぐ鍵の管理	他人のデータが見えないか・鍵で管理者の操作ができないか（検証環境での試験が要る）	☐ **A-7**　利用者 A のログインのまま、利用者 B のデータを見ることができない ☐ **A-8**　アプリの中に入っている鍵（API キー）で、管理者用の操作（権限の変更・アカウントの作成）ができない
14	不要になったデータを残さない	Q15 重要度の定義／Q16 個人データの所在と流れ	保持期間の決めと、削除の運用	☐ **D-1**　保存期間を過ぎた個人情報を消した記録がある
15	通信を暗号化する	Q17 保存・通信データの暗号化	設定の中身（TLS の版・証明書の有効期限）	☐ **D-5**　期限が切れた、または切れそうな証明書が無い

「診断で測れる部分」の Q から始まる番号は、当社の診断（25〜27問）の設問番号です。 太字の A-7 などは、Excel 版と同じ問いの ID です（最後のページの一覧にも載っています）。

チェックが埋まらなかったとき

このページの6項目（11問）は、情報システム部門だけでは答えが出ないことがあります （API は開発側、情報の共有は法務・経営側、証明書の期限は運用側）。 **まず「誰に聞けば分かるか」を1行書いて、次の会議に持っていくのが近道です。** 答えが出ないまま「はい」で埋めないでください。分からない問いは「できていない・不明」として残すほうが、あとで役に立ちます。

当社の診断で「測れる」11項目を数値にする手順

1. 当社サイト（www.securoi.com）から**無料相談を申し込む**。会社のメールアドレス1つで、決済は不要です
2. 担当より**1営業日以内**にメールで返信します
3. **25〜27問に答える**（15〜20分。情報システム担当の方1人で回答できる設問です）
4. **スコアと優先順位付きのレポート（PDF）**が出ます。表で「測れる」と書いた11項目の現在地が数値になります
5. 結果を専門家と読み合わせたい場合は、**単発スタンダード**（1回55,000円・税込・Web会議60分付き）があります

価格は単発（1回）33,000円（税込）から。お支払いは請求書払い（銀行振込・後払い）です。 診断は「対策ができているか」の現在地を測るもので、**対策そのものの実装は行いません。 この点検表だけで足りる場合は、それで構いません。**

最後のページに、Excel 版と同じ ID（A-1〜G-3）の61問の一覧（社内で使う AI の6問と、借りている基盤の3問を含む）を付けました。確かめ方と判断の目安は Excel 版にあります。

提供	合同会社SecuROI（法人番号：5011203005053）／代表社員 小山 幸輝／東京都中野区上鷺宮一丁目1番6-903号（設立：2026年6月）
サービス	SecuROI（セキュロイ）｜https://www.securoi.com｜support@securoi.com
この資料	無料。出典（合同会社SecuROI・www.securoi.com）を残し、問いの趣旨を変えなければ、複製・転送は自由です。登録は不要です。／2026/11/06（v1.4）／各機関の文書は公表時点の内容に基づきます
ご注意	本資料は各機関の公表文書を当社が整理したもので、各機関の見解や認定を示すものではありません。対策の実施にあたっては、必ず各機関の原文を確認してください。

17項目 現在地シート（記入式）

1ページ目の表と同じ順番・同じ番号です。 **11行は当社の診断のスコアを、6行は別紙で出した答えを書き写すと、17項目すべての現在地が1枚に揃います。** そのまま上司や経営層に出せます。

> **現在地（○△×）の付け方**
> **1〜11行＝診断の回答確認画面を見ます。**回答のとなりに **L1〜L4** のバッジが出ています。**L4 なら○／L2・L3 なら△／L1 なら×。**
> **12〜17行＝別紙（2ページ目）の該当する問い（ID）を見ます。「はい」と言い切れれば○／一部・確認中なら△／いいえ・分からないなら×。**
> どちらも、複数に当たる行は**いちばん低いものを採ります**（例＝L4 と L2 なら△）。⚠ **分からないときは×（できていない・不明）。把握できていないこと自体が、確かめるべき穴です。**

順	対策項目	どこを見るか	現在地	次の一手	期限
1	経営層が関与する	Q11・Q12	○ △ ×		
2	脆弱性に対応する	Q03	○ △ ×		
3	侵害の痕跡がないか調査、点検する	Q25・Q06・Q07	○ △ ×		
4	権限の付与を見直す	Q05・Q01	○ △ ×		
5	委託先を含めて管理する	Q14	○ △ ×		
6	インシデント発生時の対応	Q09・Q08・Q19・Q23	○ △ ×		
7	保存データを暗号化する	Q17	○ △ ×		
8	自組織のシステムの認証を強化する	Q02	○ △ ×		
9	ログを取得し一定期間保管する	Q18・Q06	○ △ ×		
10	不正アクセスを検知する仕組みを整える	Q07	○ △ ×		
11	外部への公開範囲を見直す	Q10・Q24	○ △ ×		
12	漏えいした情報の悪用を防ぐ	別紙 C-14	○ △ ×		
13	API の管理状況やアクセス制御を見直す	別紙 A-7・A-8	○ △ ×		
14	不要になったデータを残さない	別紙 D-1	○ △ ×		
15	通信を暗号化する	別紙 D-5	○ △ ×		
16	被害や攻撃に関する情報を提供、共有する	別紙 E-5〜E-7	○ △ ×		
17	大量アクセスを制限する	別紙 A-10〜A-12	○ △ ×		

この表に出てくる設問（回答確認画面では通し番号で並ぶため、番号が合わないときはこの要点で照合してください）

Q01	退職時の停止	Q02	多要素認証はどこまで入っているか	Q03	危険な脆弱性は期限を決めて直しているか	Q05	管理者権限の付与と棚卸
Q06	ログ集約	Q07	検知	Q08	訓練	Q09	誰が何をするかすぐ動けるか
Q10	外部からアクセスできるものの一覧は最新か	Q11	方針の文書化	Q12	リスクを定期評価し経営に上げる仕組み	Q14	外部委託先・利用SaaS のセキュリティ確認
Q17	保存・通信データの暗号化	Q18	ログの保存期間と改ざん防止	Q19	連絡先	Q23	復旧目標
Q24	クラウドの外部共有	Q25	侵入の跡の点検				

⚠ **診断の結果レポート（PDF）には設問ごとの回答は載りません。** 1〜11行を埋めるときは、**回答確認画面**（診断の「回答を確認」）を開いてください。

61問の一覧（Excel 版と同じ ID）

> ○＝できている／△＝一部／×＝できていない・不明。**分からないときは×**。自社に当てはまらない問い（例：社外に公開している API が無い）は「該当なし」と書きます。確かめ方と判断の目安は Excel 版にあります。「委託先」に○がある問いは、委託先にも聞けます。

ID	確かめること	委託先	現在地
A 社外から見えている入口			
A-1	自社のドメイン（例：example.co.jp）の下にあるサブドメイン（www・mail・vpn など）を、すべて把握している	○	○ △ ×
A-2	社外から接続できる窓口（管理画面・リモート接続・データベースなど）が、どれだけ開いているか分かっている	○	○ △ ×
A-3	クラウドの保存場所（ファイル置き場）が、意図せず誰でも見られる設定になっていない	○	○ △ ×
A-4	業務で使っているクラウドサービス（経費精算・チャット・VPN など）を、部署ごとに洗い出している	○	○ △ ×
A-16	公開しているサーバーの設定ファイルやバックアップが、外から取り出せない	○	○ △ ×
A-17	自社のサイトが読み込んでいる他社のスクリプト（計測タグ・決済など）の一覧があり、中身が変わったときに気づける	○	○ △ ×
A-5	社外に公開している API（アプリや他社のシステムがデータをやり取りする窓口）の一覧がある	○	○ △ ×
A-6	ログインしなくても呼べる API が無い	○	○ △ ×
A-7	利用者 A のログインのまま、利用者 B のデータを見ることができない	○	○ △ ×
A-8	アプリの中に入っている鍵（API キー）で、管理者用の操作（権限の変更・アカウントの作成）ができない	○	○ △ ×
A-9	辞めた社員や契約が終わった取引先に渡した API キーを、止めた記録がある	○	○ △ ×
A-10	同じ相手からの大量のアクセスに、回数の上限をかけている	○	○ △ ×
A-11	上限を超えたアクセスが記録に残り、誰かが見ている	○	○ △ ×
A-12	IP アドレスを変えながらの大量アクセスにも気づける（アカウントごと・API ごとに回数を数えられる）	○	○ △ ×
A-13	社外に面した機器・ソフト（VPN 装置・ファイアウォール・Web サーバー・CMS など）の製品名とバージョンの一覧がある	○	○ △ ×
A-14	その一覧の製品に、実際に悪用されている脆弱性が残っていない	○	○ △ ×
A-15	脆弱性を直す期限（緊急なら何日・通常なら何日）を決めて守っている	○	○ △ ×
B ログイン・アカウント・管理者の権限			
B-1	管理者・VPN・クラウドの管理画面・メールに、多要素認証（パスワード＋スマホの確認など）をかけている	○	○ △ ×
B-2	自社のサービスの利用者が、多要素認証などの強いログイン方法を選べる	○	○ △ ×
B-6	委託先が自社のシステムにつなぐアカウントに、多要素認証をかけ、つなげる場所（IP アドレス）を絞っている	○	○ △ ×
B-7	他社のアカウントでログインする連携の一覧があり、使っていない連携を止めている	○	○ △ ×
B-3	管理者の権限を持つアカウントの一覧があり、全員について理由を言える	○	○ △ ×
B-4	辞めた人・異動した人のアカウントが残っていない	○	○ △ ×
B-5	長く使われていないアカウントや鍵、止めたはずのアカウントが、使える状態になっていない	○	○ △ ×
C 侵入に気づく・対応する			
C-1	公開しているサーバーに、身に覚えのないファイルや、説明できない変更が無い	○	○ △ ×
C-2	アカウントの作成や権限の変更の記録に、身に覚えのないものが無い	○	○ △ ×
C-3	直近1か月の記録（ログ）を、誰かが実際に見たことを残している（見た日・見た人）	○	○ △ ×

ID	確かめること	委託先	現在地
C-4	ログイン・管理者の操作・API の利用の記録（ログ）を取っている	○	○ △ ×
C-5	ログを、決めた期間どおりに残している	○	○ △ ×
C-6	ログを消したり書き換えたりできる人を、限られた人にしている	○	○ △ ×
C-7	怪しいログインや大量のデータ取り出しに気づいたとき、誰に知らせが届くか決まっている	○	○ △ ×
C-8	直近1か月の知らせを、誰かが実際に見て判断した記録がある	○	○ △ ×
C-9	被害が起きたときに、誰が何をするか（止める・調べる・報告する・公表する）が文書になっていて、連絡先が最新	○	○ △ ×
C-10	個人情報保護委員会へ報告する手順と担当が決まっている	○	○ △ ×
C-11	外部の相談先（調査会社・弁護士など）が決まっている	○	○ △ ×
C-12	バックアップから実際に戻す試験を、この1年以内にやった記録がある（試した日・戻したもの・結果）	○	○ △ ×
C-13	バックアップの複製が、本番の管理者アカウントでは消せない場所にもある	○	○ △ ×
C-14	情報が漏れたとき、誰に何を知らせるかが文書になっている	○	○ △ ×
C-15	利用者にパスワードの変更などを呼びかける手順がある	○	○ △ ×
D 大事なデータの守り方			
D-1	保存期間を過ぎた個人情報を消した記録がある	○	○ △ ×
D-2	本番以外の場所（検証環境・書き出したファイル）にある個人情報の置き場所を把握している	○	○ △ ×
D-6	委託先の作業が終わった後、渡した個人情報を消したことを、記録で確かめている	○	○ △ ×
D-3	データベース・バックアップ・ノートパソコンの中身を暗号化している	○	○ △ ×
D-4	公開しているサイトと API がすべて https で、古い方式（TLS 1.0・1.1）を受け付けない	○	○ △ ×
D-5	期限が切れた、または切れそうな証明書が無い	○	○ △ ×
E 経営・委託先・社外との連絡			
E-1	この点検の結果を経営に報告し、対応の順番と予算を決めた		○ △ ×
E-2	点検で出た論点が、自社の「事業等のリスク」（有価証券報告書）や社内のリスク一覧に入っているかを見た		○ △ ×
E-3	個人情報を預けている委託先と、自社のシステムにつながる委託先の一覧がある		○ △ ×
E-4	今回の注意喚起を受けて、主な委託先に点検の状況を聞いた		○ △ ×
E-5	同じ業界や取引先と、情報を共有する先（団体・窓口）が決まっている		○ △ ×
E-6	個人情報保護委員会のほかに報告が要る当局（所管の省庁など）と、その期限を、誰かが知っている		○ △ ×
E-7	社外に共有してよい情報と、出してはいけない情報の線引きが文書になっている		○ △ ×
F 社内で使う AI（当社の追加）			
F-1	業務で使う AI（AI エージェントや、外部の生成 AI とのつなぎ込み）に、人とは別の専用のアカウントや鍵を割り当てている	○	○ △ ×
F-2	AI に渡した権限を、その用途に必要な範囲だけに絞っている	○	○ △ ×
F-3	AI がした操作（読んだデータ・実行した処理・外への送信）が記録に残り、あとから人が追える	○	○ △ ×
F-4	外への送信・データの削除・設定の変更など、取り消せない操作は、AI が実行する前に人が承認する	○	○ △ ×
F-5	AI の動きを止める担当者と手順（鍵を無効にする・つなぎ込みを外す）が決まっていて、すぐにできる	○	○ △ ×
F-6	使っている外部の AI サービス（生成 AI・AI のコーディング支援など）を、委託先の一覧に入れている	○	○ △ ×
G 借りている基盤（当社の追加）			
G-1	借りている基盤（VPS・仮想デスクトップなど）が、ほかの契約者と分けられていることを、事業者の資料で確かめている	○	○ △ ×
G-2	借りている基盤の全体を管理する ID とパスワードが、利用者が使う環境に置かれていない	○	○ △ ×
G-3	借りている基盤の事業者が侵害されたときの連絡の窓口と、止める手順が決まっている	○	○ △ ×