

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。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、12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6／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／当社の診断では測れない3。最初の6項目（表の1～6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（22問）で数値化できるかどうかです。**測れないものは「測れない」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10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。

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

「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項目の整理は、セキュリティ研究者 piyokango 氏が公開した横断整理（2026年10月11日）をそのまま使っています。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、測れ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」＝その項目の一部は22問で測れますが、全体はカバーしていません（何が測れていないかは当社サイトに記載）。

別紙：当社診断の対象外 3項目のチェック項目

表の最後の3項目は、当社の22問では測っていません。 **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。

API の管理状況やアクセス制御（4問）

- ☐ 1
- 社外に公開している API の一覧がある（最後に更新したのはいつか）
- ☐ 2
- API ごとに「誰が呼べるか」が決まっていて、鍵やトークンの有効期限がある
- ☐ 3
- 退職者・終了した取引先の鍵を止めた記録がある
- ☐ 4
- 認証なしで呼べる API がゼロだと言える（言えないなら、どれか）

被害や攻撃に関する情報の提供・共有（3問）

- ☐ 5
- 同業・取引先と情報を共有する先が決まっている（団体名・窓口）
- ☐ 6
- 当局への報告先と期限を、誰かが知っている（個人情報保護委員会・所管省庁）
- ☐ 7
- 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ある

大量アクセスの制限（3問）

- ☐ 8
- 1つの利用者・1つの IP からの回数に上限をかけている
- ☐ 9
- 上限を超えたときに記録が残り、誰かが見る
- ☐ 10
- 正規の利用を止めずに制限できることを、一度試した

「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11～14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1問が、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1問
11	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	☐ 11 漏えいが起きたとき、誰に何を通知するかが文書にある
12	侵害の痕跡がないか調査、点検する	Q06 ログ集約／Q07 検知	過去に遡って点検したかどうか	☐ 12 直近1か月のログを誰かが実際に見た記録がある（見た日・見た人）
13	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	☐ 13 保持期限を過ぎたデータを削除した記録がある
14	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）	☐ 14 期限切れの証明書が無いと言える

「診断で測れる部分」の Q から始まる番号は、当社の診断（22問）の設問番号です。「自分で確認する1問」の太字の番号は、このページの通し番号です（上の10問に続く11～14番）。「はい」と言い切れない項目が、3項目の確認と同じく今週の宿題になります。

チェックが埋まらなかったとき

このページの7項目（14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。** 答えが出ないまま表を埋めないでください。空欄のほうが、あとで役に立ちます。

当社の診断で「測れる」10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. **22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10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「対策ができていない」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。**

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・登録不要・社内での複製と配布は自由（出典を残してください）／2026/10/14（v1.0）／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。10行は当社の診断のスコアを、7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

1～10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×。

11～17行＝別紙（2ページ目）の該当番号を見ます。「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探ります**（例＝L4 と L2 なら△）。**⚠ 分からないものは×ではなく、「次の一手」の欄に「誰に聞くか」を書いてください。**

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

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
Q07	不審な動きを検知して誰かが気づけるか	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

⚠ 診断の結果レポート（PDF）には設問と回答は載りません。1～10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。 国の注意喚起 対応点検表（2026年10月版） v1.0 合同会社SecuROI