国の注意喚起 対応点検表（2026年10月版）入力用 v1.1 2026/10/21

黄色の列だけ入力します。結果を選ぶと、優先度と根拠が自動で出ます。分からないときは「できていない・不明」を選びます。

大項目	#	点検表の項目	言及機関数	確かめる問い	担当	確かめ方の例	判断の目安	結果	優先度	優先度の根拠（経営向けの一言）	対応する人	期限	メモ	問いの出所
A 入口（外から届くもの）	3	外部への公開範囲を見直す	2	自社のドメインにぶら下がるホスト名（サブドメイン）を、すべて把握している	情シス	証明書の公開記録（Certificate Transparency）を検索できる無料のサービスで自社ドメインを調べ、DNS の登録内容と合わせて、資産の台帳と突き合わせる	台帳に無いホスト名が出たら、持ち主を特定する。不要なら止める。持ち主が分からないものがあれば「できていない・不明」		未回答					機関の報告から派生
A 入口（外から届くもの）	3	外部への公開範囲を見直す	2	インターネットから見えるポートとサービスを把握している	情シス	インターネット上の機器を検索できるサービスで、自社の IP アドレスとドメインを検索する（検索だけで、自社の機器に通信は送らない）	管理画面・リモート接続（RDP・SSH）・データベースが見えていたら、公開を止めるか接続元を絞る（JPCERT/CC も管理機能の公開停止を求めている）		未回答					機関の原文
A 入口（外から届くもの）	3	外部への公開範囲を見直す	2	クラウド上の保存領域に、意図しない公開設定が無い	情シス	利用しているクラウドの管理画面で、保存領域ごとの公開設定（誰でも読める・匿名で読める状態か）を一覧する	公開する理由を説明できないものは非公開にする（統括室の注意喚起も保存領域の公開設定の確認を求めている）		未回答					機関の原文
A 入口（外から届くもの）	3	外部への公開範囲を見直す	2	業務で使っている外部サービス（クラウド・VPN サービスなど）を、部署単位まで洗い出している	情シス／調達	シングルサインオンの接続先、経費精算・請求書のサービス名、ブラウザの拡張の管理画面から集める（IPA の点検項目）	管理者が決まっていないサービスは、決まるまで「できていない・不明」		未回答					機関の原文
A 入口（外から届くもの）	4	API の管理状況やアクセス制御を見直す	3	社外に公開している API の一覧があり、最後に更新した日が分かる	開発・運用	スマートフォンアプリと Web 画面が呼ぶ通信先を、ブラウザの開発者ツールや API ゲートウェイの設定から書き出す	一覧に無い API が見つかったら「できていない・不明」。旧版・使っていない API は止める		未回答					機関の報告から派生
A 入口（外から届くもの）	4	API の管理状況やアクセス制御を見直す	3	認証なしで呼べる API が無いと言える	開発・運用	検証環境で、認証情報を付けずに各 API へリクエストを送り、データが返らないことを確かめる（自社の API だけ。本番で試すときは影響を先に確認）	データが返る API があれば最優先で塞ぐ（JPCERT/CC は、公開アプリを解析して API のエンドポイントやキーを特定する手口を報告している）		未回答					機関の報告から派生
A 入口（外から届くもの）	4	API の管理状況やアクセス制御を見直す	3	利用者 A の認証で、利用者 B のデータを取れない	開発・運用	利用者 A のトークンのまま、利用者 B の番号を指定してデータを要求し、拒否されることを確かめる（OWASP API Security Top 10 2023 の1番目「オブジェクトレベル認可の不備」）	取れたら最優先で塞ぐ		未回答					機関の報告から派生
A 入口（外から届くもの）	4	API の管理状況やアクセス制御を見直す	3	アプリに埋め込んだキーで、管理用の操作（権限の変更・アカウントの作成）ができない	開発・運用	管理用の API が、一般利用者の認証やアプリ内のキーで呼べないかを検証環境で確かめる	呼べたら最優先（JPCERT/CC が報告している「画面では実行できない内部 API への攻撃」）		未回答					機関の報告から派生
A 入口（外から届くもの）	4	API の管理状況やアクセス制御を見直す	3	退職者・終了した取引先の API キーやトークンを止めた記録がある	開発・運用	発行済みのキーの一覧と、退職者・契約終了先の一覧を突き合わせる	止めていないキーがあれば止め、止めた日を記録する		未回答					当社の追加
A 入口（外から届くもの）	5	大量アクセスを制限する	2	1つの利用者・1つの IP アドレスからの回数に上限をかけている	開発・運用	WAF・API ゲートウェイ・ロードバランサの回数制限の設定を見る	上限が無ければ「できていない・不明」		未回答					機関の原文
A 入口（外から届くもの）	5	大量アクセスを制限する	2	上限を超えたときに記録が残り、誰かが見る	開発・運用	上限を超えたときのログの出力先と、通知の届け先を確かめる	記録はあるが誰も見ていなければ「一部」		未回答					当社の追加
A 入口（外から届くもの）	5	大量アクセスを制限する	2	IP アドレスを分散されても気づける見方（アカウント単位・API 単位の回数）がある	開発・運用	ログを、アカウントごと・API ごとに集計できるかを試す	集計できなければ「できていない・不明」		未回答					当社の追加
A 入口（外から届くもの）	2	脆弱性に対応する	5	インターネットに面した機器・ソフト（VPN 装置・ファイアウォール・Web サーバ・CMS など）の製品名と版の一覧がある	情シス	入口の確認（A の3番）で見つかった機器・サービスごとに、製品名と版を書き出す	版が分からないものがあれば「できていない・不明」		未回答					機関の報告から派生
A 入口（外から届くもの）	2	脆弱性に対応する	5	一覧の製品に、悪用が確認された脆弱性が残っていない	情シス	米 CISA の Known Exploited Vulnerabilities（KEV）カタログと JVN iPedia で製品名を検索し、自社の版と照らす	KEV に載っていて未修正なら最優先で修正する		未回答					機関の報告から派生
A 入口（外から届くもの）	2	脆弱性に対応する	5	修正の期限（緊急・通常）を決めて運用している	情シス	直近の修正の記録で、公開から適用までの日数を確かめる	期限を決めていなければ「できていない・不明」		未回答					当社の追加
B アカウントと権限	6	自組織のシステムの認証を強化する	4	管理画面・VPN・クラウドの管理コンソール・メールに多要素認証がかかっている	情シス	ID 管理の基盤（社員のログインをまとめて管理するサービス）の認証方法のレポートで、多要素認証が未登録のアカウントを数える	管理者に1件でも未登録があれば最優先		未回答					機関の原文
B アカウントと権限	6	自組織のシステムの認証を強化する	4	利用者向けのログインに、多要素認証などの強い認証を選べる	開発・運用	自社サービスのログイン画面と設定を確かめる	選べなければ「できていない・不明」（漏えいした情報の悪用を防ぐ手当てにもなる）		未回答					機関の報告から派生
B アカウントと権限	7	権限の付与を見直す	4	管理者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説明できる	情シス	クラウドの権限管理と ID 管理の基盤から、管理者の役割を持つアカウントを書き出す	説明できないアカウントがあれば権限を外す		未回答					機関の報告から派生
B アカウントと権限	7	権限の付与を見直す	4	退職者・異動者のアカウントが残っていない	情シス	人事の退職者・異動者の一覧と、有効なアカウントを突き合わせる	残っていれば止め、止めた日を記録する		未回答					機関の報告から派生
B アカウントと権限	7	権限の付与を見直す	4	長く使っていないアカウントやアクセスキー、本来無効のはずのアカウントが有効になっていない	情シス	クラウドの権限管理の画面やレポートで、アカウントとアクセスキーを最後に使った日を確かめる（IPA の点検項目）	心当たりの無い有効化があれば、C の1番（痕跡）へ		未回答					機関の原文
C 痕跡の確認と、気づく・動く	1	侵害の痕跡がないか調査、点検する	4	公開サーバに、見覚えのないファイル（Web シェルなど）や説明できない更新が無い	開発・運用	Web の公開ディレクトリで、直近に追加・更新されたファイルを一覧し、デプロイの記録と照らす	説明できないファイルがあれば、この表を止めて被害への対応（段階1）へ		未回答					機関の報告から派生
C 痕跡の確認と、気づく・動く	1	侵害の痕跡がないか調査、点検する	4	アカウントの作成・権限の変更のログに、心当たりの無いものが無い	情シス	ID 管理の基盤とクラウドの操作ログで、直近の管理者の操作を確かめる（IPA の点検項目）	心当たりが無いものがあれば、この表を止めて被害への対応（段階1）へ		未回答					機関の原文
C 痕跡の確認と、気づく・動く	1	侵害の痕跡がないか調査、点検する	4	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）	情シス	ログの閲覧記録や、点検の記録を確かめる	記録が無ければ「できていない・不明」		未回答					当社の追加
C 痕跡の確認と、気づく・動く	11	ログを取得し一定期間保管する	3	認証・管理操作・API へのアクセスのログを取っている	情シス／開発・運用	それぞれのログの出力先を書き出す	取っていないものがあれば「一部」		未回答					機関の原文
C 痕跡の確認と、気づく・動く	11	ログを取得し一定期間保管する	3	決めた保存期間どおりに残っている	情シス	各ログで、残っている最も古い日付を確かめ、決めた期間と比べる	期間を決めていなければ「できていない・不明」		未回答					機関の原文
C 痕跡の確認と、気づく・動く	11	ログを取得し一定期間保管する	3	ログを消したり書き換えたりできる人が限られている	情シス	ログの保存先の権限を書き出す	管理者なら誰でも消せる状態なら「一部」		未回答					当社の追加
C 痕跡の確認と、気づく・動く	12	不正アクセスを検知する仕組みを整える	3	不審なログインや大量の取得を検知したとき、誰に届くかが決まっている	情シス	検知の設定と、通知の届け先を書き出す	届け先が退職者・共有アドレスだけなら「一部」		未回答					機関の報告から派生
C 痕跡の確認と、気づく・動く	12	不正アクセスを検知する仕組みを整える	3	直近1か月の通知を、誰かが実際に見て判断した記録がある	情シス	通知の履歴と、対応の記録を突き合わせる	記録が無ければ「できていない・不明」		未回答					当社の追加
C 痕跡の確認と、気づく・動く	13	インシデント発生時の対応	3	誰が何をするか（封じ込め・調査・報告・広報）が文書にあり、連絡先が最新	情シス／法務・総務	対応手順の文書と連絡先の一覧を開き、最後に更新した日を確かめる	1年以上更新していなければ「一部」		未回答					機関の報告から派生
C 痕跡の確認と、気づく・動く	13	インシデント発生時の対応	3	個人情報保護委員会への報告の手順と担当が決まっている	法務・総務	個人情報保護法 第26条（漏えい等の報告）に沿った社内の手順があるかを確かめる	決まっていなければ「できていない・不明」		未回答					機関の原文
C 痕跡の確認と、気づく・動く	13	インシデント発生時の対応	3	外部の調査会社・弁護士など、相談先が決まっている	法務・総務	契約の有無と連絡先を確かめる	決まっていなければ「できていない・不明」		未回答					機関の報告から派生
C 痕跡の確認と、気づく・動く	14	漏えいした情報の悪用を防ぐ	5	漏えいが起きたとき、誰に何を通知するかが文書にある	法務・総務	通知の文案と、対象者を特定する手順を確かめる	無ければ「できていない・不明」		未回答					当社の追加
C 痕跡の確認と、気づく・動く	14	漏えいした情報の悪用を防ぐ	5	利用者にパスワードの変更や多要素認証を呼びかける手順がある	開発・運用／法務・総務	告知の手段（メール・サイト）と、強制的にパスワードを変更させる機能の有無を確かめる	手段が無ければ「できていない・不明」（JPCERT/CC は平時からの二次被害防止の呼びかけを求めている）		未回答					機関の原文
D データ	8	不要になったデータを残さない	3	保存期間を過ぎた個人データを削除した記録がある	情シス／開発・運用	保存期間の決めと、直近の削除の記録を確かめる	期間を決めていなければ「できていない・不明」		未回答					機関の原文
D データ	8	不要になったデータを残さない	3	本番以外（検証環境・書き出したファイル）にある個人データの置き場所を把握している	開発・運用	検証環境のデータの出どころと、共有ドライブの書き出しファイルを確かめる	本番のデータがそのまま置かれていれば「できていない・不明」		未回答					当社の追加
D データ	9	保存データを暗号化する	2	データベース・バックアップ・ノートパソコンの保存データが暗号化されている	情シス	クラウドの暗号化の設定と、端末管理のディスク暗号化のレポートを確かめる	暗号化されていないものがあれば「一部」		未回答					機関の原文
D データ	10	通信を暗号化する	2	公開しているサイトと API がすべて HTTPS で、古い版の TLS を受け付けない	開発・運用	TLS の設定を外から調べる無料の診断サービスで、自社のサイトと API を調べる	TLS 1.0・1.1 が有効なら「一部」		未回答					機関の報告から派生
D データ	10	通信を暗号化する	2	期限切れや、期限が近い証明書が無い	開発・運用	証明書の一覧で有効期限を確かめる	期限切れがあれば「できていない・不明」		未回答					当社の追加
E 経営・委託先・情報共有	16	経営層が関与する	6	点検の結果を経営に報告し、対応の優先順位と予算を決めた	経営層／情シス	この表の「集計」シートを経営会議に出す	報告していなければ「できていない・不明」		未回答					機関の報告から派生
E 経営・委託先・情報共有	16	経営層が関与する	6	点検の論点が、自社の「事業等のリスク」章や社内のリスク一覧にあるかを照らした	経営層	有価証券報告書・届出書の「事業等のリスク」章で、本調査の20語（API・不正アクセスなど）を検索する	無い論点は、主要なリスクとして書くか、書かない判断を記録するかを決める		未回答					当社の追加
E 経営・委託先・情報共有	15	委託先を含めて管理する	4	個人データや自社システムへの接続を委ねている委託先の一覧がある	調達／情シス	契約の一覧から、個人データを預けている先と、システムに接続している先を抜き出す	一覧が無ければ「できていない・不明」		未回答					機関の報告から派生
E 経営・委託先・情報共有	15	委託先を含めて管理する	4	今回の注意喚起を受けて、主要な委託先に点検の状況を確かめた	調達／情シス	この表の問いを委託先に送り、回答を受け取る	回答が無い委託先があれば「一部」		未回答					機関の報告から派生
E 経営・委託先・情報共有	17	被害や攻撃に関する情報を提供、共有する	3	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）	法務・総務	加盟している業界団体と、その窓口を確かめる	決まっていなければ「できていない・不明」		未回答					機関の報告から派生
E 経営・委託先・情報共有	17	被害や攻撃に関する情報を提供、共有する	3	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）	法務・総務	担当者に聞き、手順の文書と照らす	知っている人がいなければ「できていない・不明」		未回答					機関の報告から派生
E 経営・委託先・情報共有	17	被害や攻撃に関する情報を提供、共有する	3	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	法務・総務	文書の有無を確かめる	無ければ「できていない・不明」		未回答					当社の追加