CHECK SHEET

不正アクセス対策チェックシート

社内と委託先に確認したい6つのポイント



記入日 _____　記入者 _____　対象のシステム・サービス _____

使い方

1. 6つの問いに○△×で答える
2. △と×は、2ページ目の例文で社内・委託先に確認する
3. 担当と期限を決めて、答えを埋めていく

観点	確認すること	答え	担当・期限
観点1 知る	**インターネットに公開しているWebサイト・アプリ・API・管理画面を、一覧で把握できていますか** 要注意 一覧がない／作った人がわからないサイトや管理画面がある メモ	○ △ ×	担当 期限
観点2 直す	**それぞれ脆弱性診断を受けていますか。受けている場合、管理画面・API・スマートフォンアプリまで診断の範囲に含まれていましたか** 要注意 ログイン後の画面・管理画面・APIが対象外／アプリを診断していない メモ	○ △ ×	担当 期限
観点3 直す	**過去の診断で指摘された項目や、ソフトウェアの更新への対応は済んでいますか** 要注意 指摘が「様子見」のまま／サポートが終わったソフトを使っている メモ	○ △ ×	担当 期限
観点4 知る	**委託先や外部サービスに預けているシステム・データも把握できていますか** 要注意 契約に事故時の報告義務がない／再委託の有無を知らない メモ	○ △ ×	担当 期限
観点5 減らす	**使い終わった個人情報を持ち続けていませんか** 要注意 保存期間のルールがない／本番データのコピーが散らばっている メモ	○ △ ×	担当 期限
観点6 備える	**異常に気づいたとき、誰が判断し、どこに相談するか決まっていますか** 要注意 サービスを止める判断をする人が未定／ログの保存場所がわからない メモ	○ △ ×	担当 期限

結果の見方

△や×がついた観点が、確認を始める場所です。すべてを一度に直す必要はありません。「個人情報を扱っている」「インターネットに公開している」「脆弱性診断を受けていない（範囲が狭い）」の3つが重なるものから優先して確認しましょう。

国家サイバー統括室、IPA、個人情報保護委員会、JPCERT/CCの注意喚起（2026年10月）をもとに作成

UBsecure

CHECK SHEET

そのまま使える 聞き方の例文

社内チャットやメールに貼り付けて、確認の依頼に使えます



観点1 知る — 公開しているものの把握

社内へ

「当社名義で公開しているWebサイト、アプリ、API、管理画面を一覧にしたいです。各部署で独自に作ったキャンペーンサイトや、契約しているクラウドサービスの管理画面も含めて、ご存じのものを教えていただけますか。」

委託先へ

「御社に運用をお願いしている当社のシステムについて、インターネットからアクセスできるURL、サブドメイン、APIの接続先、管理画面、検証環境の一覧をいただけますか。使っていないものがあれば、あわせて教えてください。」

観点2 直す — 脆弱性診断の範囲

社内へ

「前回の脆弱性診断の見積もりで、予算の都合で外した画面や機能はありましたか。外した部分がその後どう扱われているかを確認したいです。」

委託先へ

「直近の脆弱性診断の報告書を共有いただけますか。ログイン後の機能や管理画面を含んだか、権限ごとに確認したか、スマートフォンアプリとアプリが使うAPIを対象にしたかを教えてください。」

観点3 直す — 指摘事項・更新への対応

社内へ

「管理画面や、部署で使っているクラウドサービスの管理者アカウントは、多要素認証になっていますか。退職者や異動者のアカウントが残っていないか確認させてください。」

委託先へ

「前回の診断で指摘された項目ごとに、対応済み・対応予定・対応しない（理由付き）の状況を一覧でいただけますか。サポートが終了している、または終了が近いソフトウェアがあれば教えてください。」

観点4 知る — 委託先・外部サービス

社内へ

「各部署で契約しているクラウドサービスやSaaSを洗い出したいです。サービス名、契約部署、扱っているデータ、管理者を教えてください。」

委託先へ

「当社の個人情報を扱う作業に、再委託先は関わっていますか。事故やその疑いがあった場合、何時間以内に誰へ連絡いただける取り決めになっているかも確認させてください。」

観点5 減らす — 使い終わった個人情報

社内へ

「当社が保有している個人情報について、何を、どこに、いつまで保存するかのルールはありますか。退会者や終了したキャンペーンのデータが残っていないか確認したいです。」

委託先へ

「当社の個人情報のコピーやバックアップ、検証環境用のデータはどこにありますか。契約や業務の終了時に削除した記録をいただくことはできますか。」

観点6 備える — 異常時の判断と相談先

社内へ

「不正アクセスが疑われる連絡が夜間や休日に来た場合、最初に誰へ報告し、サービスを止めるかどうかを誰が判断しますか。」

委託先へ

「当社システムのアクセスログや操作ログは、何日分、どこに保存されていますか。異常が見つかった場合、どの範囲のログを、どれくらいで提供いただけますか。」

国家サイバー統括室、IPA、個人情報保護委員会、JPCERT/CCの注意喚起（2026年10月）をもとに作成

UBsecure

CHECK SHEET

異常に気づいたときの連絡先メモ

夜間・休日でも迷わないように、事前に書き込んでおきましょう



社内と委託先の連絡先

役割	氏名・部署	電話	メール
サービスを止める判断をする人			
情報システム・技術の担当			
委託先の窓口（平日）			
委託先の窓口（夜間・休日）			
広報・法務の担当			

初動の流れ（終わったらチェック）

- ☐ 1 **異常に気づく** ― 委託先からの連絡、利用者の問い合わせ、不審なログなど
- ☐ 2 **社内の判断者へ報告する** ― 上の表の「サービスを止める判断をする人」へ
- ☐ 3 **委託先に状況確認とログの保全を依頼する** ― 記録が消える前に残してもらう
- ☐ 4 **インシデントと判断する** ― サービスを止めるかどうかも、ここで決める
- ☐ 5 **相談・報告する** ― 下の相談窓口、所管省庁、個人情報保護委員会、警察
- ☐ 6 **専門事業者に詳しい調査を依頼する** ― 原因と影響範囲を確かめる

公的な相談窓口

JPCERT/CC　インシデント対応依頼
https://www.jpcert.or.jp/form/

IPA　企業組織向けサイバーセキュリティ相談窓口
https://www.ipa.go.jp/security/support/soudan.html

個人データの漏えいなどが起きた場合は、個人情報保護委員会への報告と本人への通知が法律上必要になることがあります。

点検の進め方を整理したい方へ

ユービーセキュアでは、Webアプリケーション診断やスマートフォンアプリ診断などで、外部に公開しているシステムの点検をお手伝いしています。
何から手をつければよいか整理したい段階でも、無料相談会（オンライン・1時間）をご利用いただけます。

https://www.ubsecure.jp/free-consultation

国家サイバー統括室、IPA、個人情報保護委員会、JPCERT/CCの注意喚起（2026年10月）をもとに作成

UBsecure