ウェブサイト・会員制サイト・アプリ　セキュリティ確認チェックリスト

発注側の経営者・担当者が、制作会社・保守会社に確認するための質問票

内閣官房国家サイバー統括室「個人情報の漏えい等につながる不正アクセスへの対策について ～ウェブサイトやモバイルアプリに関する基本的な対策の徹底～」（2026年11月5日）の8項目を、発注側の確認事項に組み替えたものです。
作成：PJ-T&C合同会社（2026年11月版）　／　解説記事：pj-tc.com「政府が示した個人情報漏えい対策8項目 ― 開発を外注している会社が今週中に確認すべき3つのこと」

使い方

- 自社に当てはまるセクション（A～D）だけ使ってください。コーポレートサイトだけなら A と D で足ります。
- 「聞く相手」が**自社**の項目は、制作会社の回答を待たずに自分で確認できます。
- 制作会社に渡すときは、このまま PDF を送って「回答欄を埋めて返してください」で構いません。答えがすぐ出てこない項目は、それ自体が確認結果です。
- 優先度**高**は、原文が漏えい事案の直接の原因として挙げているもの、または今週中に自社でできるものです。
- 「根拠」列は原文の章・対策例の番号です（例：1-(2) 対策例2 ＝ 第1章（2）の対策例2）。査読・照合用。

聞く相手：　**自社** 自社で確認・実施　**制作会社** 制作会社・保守会社に質問　**契約** 契約書・発注仕様書で担保

優先度：**高** **中**

A. 自社ウェブサイト（コーポレートサイト・EC サイト）

WordPress 等の CMS で作ったサイト、問い合わせフォームや EC を持つサイト。すべてのサイトに当てはまる基本項目。

No.	確認事項	聞く相手	優先度	根拠	回答・メモ
A-1	管理画面（/wp-admin/ 等）、phpMyAdmin、サーバーのコントロールパネルは、IP アドレス制限か追加認証で保護されているか	制作会社	高	1-(2) 対策例2	☐ 確認済
A-2	開発・検証環境（staging、test 等のサブドメイン）がインターネットから見えていないか。見えている場合、本番と同じ個人情報が入っていないか	制作会社	高	1-(2) 対策例2	☐ 確認済
A-3	管理者権限を持つアカウントの全員（自社・制作会社・保守会社・代理店）を一覧にしたか	自社	高	1-(2) 対策例2	☐ 確認済
A-4	A-3 の全員が多要素認証を設定しているか。SMS・認証アプリより、パスキーや物理セキュリティキー（FIDO2）はフィッシングに強い	自社	高	1-(2) 対策例2、NIST SP 800-63B	☐ 確認済
A-5	退職者、契約が終わった制作会社・保守会社のアカウントが残っていないか。残っていれば削除したか	自社	高	3-(1) 対策例1	☐ 確認済
A-6	管理者権限は本当に必要な人だけか。記事を投稿するだけの人に管理者権限を与えていないか	自社	中	10/9 文書 3.(1)	☐ 確認済
A-7	使っているソフトの一覧（CMS 本体、PHP、プラグイン、テーマ、ライブラリ）とバージョンを出してもらえるか	制作会社	高	1-(1) 対策例1	☐ 確認済

A-8	A-7 の中にサポート終了（EOL）のものが無いか。更新が止まったプラグイン・テーマが無いか	制作会社	高	1-(1) 対策例2	☐ 確認済
A-9	CMS 本体・プラグイン・テーマの更新を、誰が、どの頻度で行うか。保守契約に含まれているか	契約	高	1-(1) 対策例3・4	☐ 確認済
A-10	クラウドストレージ（S3 等）、CDN、バックアップファイルが誰でもダウンロードできる設定になっていないか	制作会社	高	1-(2) 対策例2	☐ 確認済
A-11	サイトの移行・複製・バックアップに使ったプラグインのファイル（.wpress、.zip、.sql 等）がサーバーに残っていないか。残っている場合、外部からダウンロードできない場所にあるか	制作会社	高	1-(2) 対策例2・3	☐ 確認済
A-12	このサーバーでは .htaccess によるアクセス制限が静的ファイルに効くか。効かない場合、どの方法で保護しているか	制作会社	中	1-(2) 対策例2	☐ 確認済
A-13	脆弱性診断が保守契約に含まれているか。頻度と、結果の報告書が出るか	契約	中	1-(3) 対策例1	☐ 確認済
A-14	大きな改修（決済・会員機能の追加）のあとに診断を行うか。見つかった問題を誰がいつまでに直すか	契約	中	1-(3) 対策例1	☐ 確認済
A-15	サーバーのアクセスログは保存されているか。保存期間は何日か（事故時に「取られたか」を判定する唯一の材料）	自社	高	1-(3) 対策例2	☐ 確認済
A-16	PHP のエラー表示（display_errors）が本番で無効になっているか。有効だとサーバー内のパスや設定が画面に出る	制作会社	中	IPA 20ヶ条	☐ 確認済

B. 会員制サイト（ログインして個人情報を扱う）

会員が自分の情報を見る、予約・購入・申込をするサイト。A の全項目に加えて確認する。

No.	確認事項	聞く相手	優先度	根拠	回答・メモ
B-1	ログインした会員が、他の会員のデータを参照・変更できないことを、サーバー側で検証しているか（URL の ID を書き換えても他人のページが見えないか）	制作会社	高	2-(2) 対策例1（BOLA）	☐ 確認済
B-2	一般会員が、管理者向け機能の URL を直接入力しても使えないことを、サーバー側で検証しているか	制作会社	高	2-(2) 対策例1（BFLA）	☐ 確認済
B-3	B-1・B-2 を公開前の診断で確認したか。「フレームワークが自動でやっている」だけの回答なら、具体的にどの処理かまで聞く	制作会社	高	2-(3)	☐ 確認済
B-4	同じアカウントへのログイン失敗が続いたとき、一時的にロックされるか	制作会社	高	2-(2) 対策例3	☐ 確認済
B-5	パスワードリセットの申請が短時間に大量に来たとき、止まるか。複数の IP アドレスからの分散した試行も検知できるか	制作会社	中	2-(2) 対策例3	☐ 確認済
B-6	会員データの一括出力（CSV エクスポート、API での一覧取得）ができる人は誰か。全員が多要素認証を設定しているか	自社	高	10/9 文書 3.(1)	☐ 確認済
B-7	一括出力の操作がログに残り、確認できるか	制作会社	中	1-(3) 対策例2	☐ 確認済
B-8	使っている基盤（CMS の会員プラグイン、フレームワーク、SaaS）は、会員向けにパスキー（FIDO2/WebAuthn）ログインを提供できるか	制作会社	中	NIST SP 800-63B	☐ 確認済
B-9	公開前に脆弱性診断またはペネトレーションテストを行ったか。報告書を受け取ったか	契約	高	2-(3)	☐ 確認済
B-10	報告書に残っている指摘があるか。あるなら、なぜ残ったまま公開したのか、誰がいつまでに直すか	契約	高	2-(3) 対策例1	☐ 確認済
B-11	診断を第三者に委託した場合、その会社はウェブアプリ診断・API 診断の実績があるか。情報セキュリティサービス基準に適合しているか	契約	中	2-(3) 対策例2	☐ 確認済
B-12	会員の氏名・住所等が、注文確認メール・管理画面・ログに必要以上に転記されていないか	制作会社	中	10/9 文書 3.(2)	☐ 確認済

C. ウェブアプリ・モバイルアプリ（自社開発・受託開発）

業務用ウェブアプリ、顧客向けモバイルアプリ、それらが通信するバックエンド。B の項目も当てはまる。

No.	確認事項	聞く相手	優先度	根拠	回答・メモ
C-1	アプリの中（ソースコード・アプリパッケージ）に、サーバーやクラウドサービスの API キー・秘密鍵・DB 接続情報を書いていないか	制作会社	高	2-(2) 対策例2、OWASP Mobile M1	☐ 確認済
C-2	鍵はサーバー側のシークレットマネージャーで管理し、有効期間と定期的なローテーションを設定しているか	制作会社	高	2-(2) 対策例2	☐ 確認済
C-3	コミット時や CI/CD で、鍵の混入を検知するシークレットスキャンを行っているか	制作会社	中	2-(2) 対策例2	☐ 確認済
C-4	すべての API について、呼び出した利用者がそのデータと機能に権限を持つことをサーバー側で検証しているか（アプリ側の画面制御だけでは不十分）	制作会社	高	2-(2) 対策例1、NICT A2B 注意喚起	☐ 確認済
C-5	既存のアプリについて、SBOM（ソフトウェア部品表）またはそれに相当する部品一覧を受け取っているか	契約	中	3-(2) 対策例2	☐ 確認済
C-6	次の改修から、SBOM の提出を発注仕様書に入れるか。検収時に既知の脆弱性・ライセンスの確認結果を受け取るか	契約	中	3-(2) 対策例2	☐ 確認済
C-7	納品後に新しい脆弱性が公表されたとき、自社アプリへの影響を誰が監視・判断するか（自社か制作会社か）	契約	高	3-(2) 対策例1	☐ 確認済
C-8	開発中に自動のセキュリティ検査（SAST / SCA / DAST）を行っているか。検出された問題と対応の記録を見せてもらえるか	制作会社	中	2-(1) 対策例2・3	☐ 確認済
C-9	要件定義の段階で、脅威モデリングと認証・認可・ログ・暗号化の要件を明文化したか（セキュリティ・バイ・デザイン）	契約	中	2-(1) 対策例1	☐ 確認済
C-10	どの深刻度の脆弱性が残っていたら公開しないか（セキュリティゲート）を決めているか。その最終判断は発注側の責任者が行うか	自社	高	2-(3) 対策例1	☐ 確認済
C-11	ストアへの申請・公開を制作会社が代行する場合、公開のタイミングを発注側が承認する手順になっているか	契約	中	2-(3) 対策例1	☐ 確認済

D. 制作会社・保守会社との契約

発注側が自社の契約と運用を見直す項目。委託先の環境を足掛かりにした侵入は発注元の責任になる。

No.	確認事項	聞く相手	優先度	根拠	回答・メモ
D-1	制作会社・保守会社がサーバーに入る経路（VPN、リモートデスクトップ、FTP/SFTP、保守用回線）をすべて洗い出したか	自社	高	3-(1) 対策例1	☐ 確認済
D-2	D-1 の経路に多要素認証が掛かっているか。難しい経路には、接続元 IP 制限・作業時のみの接続開放・作業記録の取得があるか	自社	高	3-(1) 対策例1	☐ 確認済
D-3	作業が完了した委託先のアカウント、常時付与されたままの管理者権限を棚卸しし、無効化・最小化したか	自社	高	3-(1) 対策例1	☐ 確認済
D-4	契約書に「再委託の手続き（承認）」が入っているか	契約	中	3-(1) 対策例2	☐ 確認済
D-5	契約書に「インシデント発生時の通知義務と連絡先」が入っているか	契約	高	3-(1) 対策例2	☐ 確認済
D-6	契約書に「契約終了時のデータ消去」が入っているか	契約	中	3-(1) 対策例2	☐ 確認済
D-7	深刻な脆弱性（ゼロデイ）が公表されたときの初動手順を決めているか。影響調査の責任者、委託先との役割分担、経営層への報告基準、暫定対策（パッチ・WAF・機能停止）の判断手順	自社	高	3-(2) 対策例1	☐ 確認済
D-8	個人情報の取扱いを委託している場合、個人情報保護法第25条の「委託先の監督」として何をしているか説明できるか	自社	高	3-(1)、個情委ガイドライン通則編	☐ 確認済
D-9	本チェックリストで追加費用が必要になる項目（診断、SBOM 作成、接続経路の多要素認証化）について、費用負担を制作会社と協議したか。一方的な負担の押し付けになっていないか	契約	中	3-(1)、経産省・公取委パートナーシップ	☐ 確認済
D-10	委託先の選定基準に、第三者認証や SCS 評価制度（2027年3月申請受付開始予定）を加えるか	契約	中	3-(1) 対策例2	☐ 確認済
D-11	事故が起きたときに連絡する先（決済代行、サーバー会社、制作会社、フォレンジック調査会社、個人情報保護委員会）と責任分界を一覧にしているか	自社	中	10/9 文書 4.	☐ 確認済

今週中にやる 3 つ（A〜D から抜粋）

制作会社の回答を待たずに、発注側だけで着手できる項目。

No.	確認事項	回答・メモ
A-1 / A-2	管理画面・開発環境が外から見えていないか（自分でブラウザから URL を開いて確認できる）	☐ 確認済
A-3〜5 / D-1〜3	管理者・委託先の全員が多要素認証か。辞めた人・終わった案件のアカウントが残っていないか	☐ 確認済
A-7 / A-8	制作会社に「使っているソフトの一覧と、EOL のもの」を今週中に出すよう依頼する	☐ 確認済

根拠（一次情報）

内閣官房国家サイバー統括室「個人情報の漏えい等につながる不正アクセスへの対策について 〜ウェブサイトやモバイルアプリに関する基本的な対策の徹底〜」2026年11月5日　https://www.cyber.go.jp/pdf/press/261105_taiou.pdf（本票の「根拠」列の章・対策例番号はこの文書のもの）

内閣官房国家サイバー統括室「不正アクセスによる漏えい等の事案を踏まえた対応について」2026年10月9日
https://www.cyber.go.jp/pdf/press/taiou.pdf（「10/9 文書」）

NICT「【注意喚起】相次ぐ情報漏洩、その原因の一つは『アプリ解析からのサーバ攻撃』」2026年10月13日

IPA「安全なウェブサイトの運用管理に向けての20ヶ条」

OWASP API Security Top 10 2023（API1 BOLA / API4 / API5 BFLA）、OWASP Mobile Top 10 2024（M1）

NIST SP 800-63B（フィッシング耐性のある認証方式）

個人情報保護委員会「個人情報の保護に関する法律についてのガイドライン（通則編）」委託先の監督

経済産業省・公正取引委員会「サプライチェーン全体のサイバーセキュリティ向上のための取引先とのパートナーシップの構築に向けて」

経済産業省「SBOM 導入手引 ver2.0」「ASM 導入ガイダンス」「SCS 評価制度」

本チェックリストは公開情報をもとに PJ-T&C合同会社が作成した確認用の資料で、法的助言ではありません。個人情報保護法上の報告要否等は専門家にご確認ください。項目の対応方法に迷う場合はご相談ください（pj-tc.com）。管理者・委託先の多要素認証に物理セキュリティキーをご検討の場合は security.pj-tc.com をご覧ください。