# 自社サイトを点検する30項目

放置した自社サイト、大丈夫？ 不正アクセスを防ぐための確認票と記録用紙。

## 最初に、対象・担当・更新状況を確認する

公開画面、管理画面、保守会社の記録を組み合わせます。
確認した範囲と日時を残し、不明・要対応に担当と期限を付けます。

| | |
|---|---|
| 公開画面 | 通信・証明書・取得したページの公開設定 |
| 管理画面 | ソフトウェアの版・利用者・権限・設定 |
| 管理者・保守会社 | 実装・契約・作業記録・保存と復元 |

## まず確認する8項目

01 対象URL ／ 02 保守担当 ／ 06 CMS本体 ／ 07 プラグイン
11 管理者 ／ 13 多要素認証 ／ 18 非公開ファイル ／ 26 バックアップ
手順：01・02はp.3、06・07はp.4、11・13はp.5、18はp.6、26はp.8。
状況をつかむ入口です。危険度の順位や、8項目だけで完了する意味ではありません。

## 状態は四つ。件数を安全度に換算しない

| | |
|---|---|
| 確認済み | 必要な根拠がそろい、確認範囲で対応すべき不備がない |
| 要対応 | 修正・整理が必要。担当と完了条件を決める |
| 不明 | 根拠が足りない。質問と回答期限を決める |
| 該当なし | 機能・構成を利用していない。理由を残す |

## 改ざん・不審な管理者・顧客情報の公開を見つけたら

対象・時刻・見えた事実を責任者へ連絡し、管理者が拡大防止と記録保全を進めます。通常点検のつもりでログ削除や上書きを続けないでください。社内の初動対応手順へ切り替えます。

# サイト台帳と管理する範囲

本体、旧サイト、採用・キャンペーン、検証用、外部フォーム等を確認。足りなければ複写。

会社・部署／記入者／確認日：

対象 1 URL・用途：

構成・外部サービス／扱う情報の種類・保存先：

社内担当・保守先／継続・閉鎖検討・用途確認／次の確認日：

対象 2 URL・用途：

構成・外部サービス／扱う情報の種類・保存先：

社内担当・保守先／継続・閉鎖検討・用途確認／次の確認日：

対象 3 URL・用途：

構成・外部サービス／扱う情報の種類・保存先：

社内担当・保守先／継続・閉鎖検討・用途確認／次の確認日：

ドメイン・DNS・サーバーの契約先／契約範囲の資料の所在：

緊急連絡先・代行／保管する点検記録の所在・閲覧者：

秘密鍵、パスワード、顧客の実データは書かず、必要な社内資料の参照先を記録します。

# A 対象と管理体制 01〜05

対象URL・確認日・確認者は余白または台帳に記入。根拠と次の担当・期限を各項目に残します。

### 01 自社が管理するサイトとURLを一覧にした

確認：DNS・サーバー契約・制作資料を照合し、本体、子ドメイン、旧サイト、検証用、外部フォームを洗い出す

記録・行動：URL、用途、公開状態、構成、所有・管理範囲を台帳に記入。確認できない対象に調査担当を付ける

☐ 確認済み ☐ 要対応 ☐ 不明 ☐ 該当なし

根拠・確認者：

次の担当・期限／該当なしの理由：

### 02 更新と緊急対応の担当・保守範囲を確認した

確認：保守契約と作業記録を開き、本体・部品・サーバー更新、保全、緊急対応の分担を見る

記録・行動：担当者・代行者・契約範囲・連絡先・直近の実施記録。担当不明なら責任者が決める

☐ 確認済み ☐ 要対応 ☐ 不明 ☐ 該当なし

根拠・確認者：

次の担当・期限／該当なしの理由：

### 03 ドメインの更新と管理権限を確認した

確認：登録事業者・DNSの管理画面で会社の管理権限、更新期限、支払・通知先を確認

記録・行動：契約と更新状況、管理・回復先の所在を記録。個人任せや期限切れの懸念を担当へ渡す

☐ 確認済み ☐ 要対応 ☐ 不明 ☐ 該当なし

根拠・確認者：

次の担当・期限／該当なしの理由：

### 04 使わないサイトの停止方針とDNSを確認した

確認：台帳の用途を確認し、旧アプリ、外部契約、DNS参照、メール・認証回復先への依存を調べる

記録・行動：継続・制限・閉鎖の判断、停止対象、残すドメイン、実施後の確認を記録。解約だけで終えない

☐ 確認済み ☐ 要対応 ☐ 不明 ☐ 該当なし

根拠・確認者：

次の担当・期限／該当なしの理由：

### 05 フォーム等で扱う情報と保存先を把握した

確認：問い合わせ、会員、採用、予約等について、入力→送信→保存→閲覧・削除の流れを担当者に確認

記録・行動：情報の種類、保存先、外部サービス、管理担当、不要な収集の整理。実データを点検票に転記しない

☐ 確認済み ☐ 要対応 ☐ 不明 ☐ 該当なし

根拠・確認者：

次の担当・期限／該当なしの理由：

# B 更新と構成 06〜10

対象URL・確認日・確認者は余白または台帳に記入。根拠と次の担当・期限を各項目に残します。

### 06 CMS本体の版と更新状況を確認した

確認：管理画面の更新情報と公式情報を照合。WordPressは「ダッシュボード→更新」を確認

記録・行動：現在版、確認日、適用すべき修正、保守担当の回答。CMSなしなら構成を根拠に該当なし

☐ 確認済み ☐ 要対応 ☐ 不明 ☐ 該当なし

根拠・確認者：

次の担当・期限／該当なしの理由：

### 07 プラグインの版・提供元・必要性を確認した

確認：有効・無効の全一覧を開き、版、配布元、更新、提供継続、利用用途を確認

記録・行動：一覧と対応方針。不要な部品は依存・保全を確認して削除し、必要なものは更新・代替を判断

☐ 確認済み ☐ 要対応 ☐ 不明 ☐ 該当なし

根拠・確認者：

次の担当・期限／該当なしの理由：

### 08 テーマの版・提供元・必要性を確認した

確認：使用中・未使用・親子テーマを確認し、更新と依存関係、独自修正の所在を調べる

記録・行動：版と更新方針、残す理由。親テーマや必要な修正を確認せず削除・上書きしない

☐ 確認済み ☐ 要対応 ☐ 不明 ☐ 該当なし

根拠・確認者：

次の担当・期限／該当なしの理由：

### 09 サーバー等の修正提供とサポート期限を確認した

確認：PHP等の実行環境、OS、Web・DBサーバー、フレームワークの版、修正提供元、実行環境への反映を管理者へ確認

記録・行動：対象、修正告知・作業記録、提供期限、移行方針。版表示だけで判定せず、共用・SaaSは事業者の回答を残す

☐ 確認済み ☐ 要対応 ☐ 不明 ☐ 該当なし

根拠・確認者：

次の担当・期限／該当なしの理由：

### 10 更新の実施結果と動作確認を追える

確認：更新設定、成功・失敗通知、作業記録を確認。変更時の保全・検証・戻し方も点検

記録・行動：最後の結果、実際の版、正常機能の確認、失敗時の担当。自動更新オンだけでは完了にしない

☐ 確認済み ☐ 要対応 ☐ 不明 ☐ 該当なし

根拠・確認者：

次の担当・期限／該当なしの理由：

# C 管理用アカウントと権限 11〜15

対象URL・確認日・確認者は余白または台帳に記入。根拠と次の担当・期限を各項目に残します。

### 11 管理用アカウントと権限を整理した

確認：CMS・サーバー・DNS等の利用者、用途、権限、退職・契約終了先、既存セッションと鍵・トークンを確認

記録・行動：失効対象と結果を台帳に記録。不要な権限・ログイン状態・鍵を失効し、連携への影響を確認。不審な管理者は初動へ

☐ 確認済み ☐ 要対応 ☐ 不明 ☐ 該当なし

根拠・確認者：

次の担当・期限／該当なしの理由：

### 12 管理用の認証情報を会社で管理している

確認：パスワードの使い回し、共用状態、作業鍵・トークンの利用先と保管・失効方法を確認

記録・行動：管理方法、担当、失効対象を記録。秘密値は載せず、会社管理の安全な保管先へ整理

☐ 確認済み ☐ 要対応 ☐ 不明 ☐ 該当なし

根拠・確認者：

次の担当・期限／該当なしの理由：

### 13 多要素認証と回復方法を確認した

確認：対応する管理サービスで適用対象と認証方法を確認し、通常のログインと回復先を点検

記録・行動：適用結果、確認日、回復情報の管理先。未対応サービスはアクセス制限等の代替策を検討

☐ 確認済み ☐ 要対応 ☐ 不明 ☐ 該当なし

根拠・確認者：

次の担当・期限／該当なしの理由：

### 14 管理画面・作業経路への接続を保護した

確認：管理画面の接続制限・試行制御、暗号化された管理通信・ファイル転送、不要な入口を確認

記録・行動：許可範囲・例外・設定・正規作業の動作結果。URL変更だけを完了の根拠にしない

☐ 確認済み ☐ 要対応 ☐ 不明 ☐ 該当なし

根拠・確認者：

次の担当・期限／該当なしの理由：

### 15 ファイルやDBの書き換え権限を確認した

確認：Web実行ユーザー、配置・アップロード先、DB接続ユーザーの権限を保守担当に確認

記録・行動：必要な書込範囲と設定根拠、変更後の更新・投稿等の結果。権限を一律に緩めず対象ごとに整理

☐ 確認済み ☐ 要対応 ☐ 不明 ☐ 該当なし

根拠・確認者：

次の担当・期限／該当なしの理由：

# D 通信と公開範囲 16〜20

対象URL・確認日・確認者は余白または台帳に記入。根拠と次の担当・期限を各項目に残します。

### 16 必要なページと送信先のHTTPSを確認した

確認：主要URL・フォーム送信先・読み込み先の通信、証明書の対象と期限、HTTPからの転送を確認

記録・行動：確認URL・日時・応答・更新担当。HTTP指定等があれば管理者が変更し、実際の動作も確認

☐ 確認済み ☐ 要対応 ☐ 不明 ☐ 該当なし

根拠・確認者：

次の担当・期限／該当なしの理由：

### 17 非公開ページと資料の閲覧権限を確認した

確認：制限対象の設定と認可を管理者が確認。架空データで未ログイン・権限の異なるテスト利用者の表示を確認

記録・行動：対象・条件・制限結果。noindexやrobots.txtだけの場合は閲覧制限を整備。公開発覚は初動へ

☐ 確認済み ☐ 要対応 ☐ 不明 ☐ 該当なし

根拠・確認者：

次の担当・期限／該当なしの理由：

### 18 設定・バックアップ等を公開領域から分離した

確認：公開ディレクトリと配備ルールを確認し、設定、DBのコピー、秘密鍵、Git等の保管場所を照合

記録・行動：配置設定と既知の対象の確認結果。外部検査で未検出だけでは完了にせず、公開があれば制限と初動判断

☐ 確認済み ☐ 要対応 ☐ 不明 ☐ 該当なし

根拠・確認者：

次の担当・期限／該当なしの理由：

### 19 不要な詳細エラーやファイル一覧を表示しない

確認：本番のデバッグ・一覧表示設定を確認し、通常の404や許可された検証環境で応答を確認

記録・行動：設定、応答例、ログの保管先。利用者向け表示と管理者向け記録を分ける

☐ 確認済み ☐ 要対応 ☐ 不明 ☐ 該当なし

根拠・確認者：

次の担当・期限／該当なしの理由：

### 20 外部タグ・JavaScriptの読み込み元を管理している

確認：ソース・タグ管理・ブラウザの通信記録で提供元・用途を照合。タグを公開できる人、変更履歴、不要なタグも確認

記録・行動：読み込み元の台帳、公開権限、変更結果。必要性を確認して削除・更新し、SRI等は提供方式に応じ検討

☐ 確認済み ☐ 要対応 ☐ 不明 ☐ 該当なし

根拠・確認者：

次の担当・期限／該当なしの理由：

# E フォームと防御設定 21〜25

対象URL・確認日・確認者は余白または台帳に記入。根拠と次の担当・期限を各項目に残します。

### 21 フォームの送信後の処理を確認した

確認：開発担当へ、サーバー側入力検証、SQLのパラメーター化等、表示時の文脈に合う出力処理を確認

記録・行動：対象機能・実装の説明・許可された環境の確認結果。正常送信や必須項目だけで安全としない

☐ 確認済み ☐ 要対応 ☐ 不明 ☐ 該当なし

根拠・確認者：

次の担当・期限／該当なしの理由：

### 22 アップロードの受付・保存条件を確認した

確認：添付機能の必要性、許可種別、容量、内容確認、保存場所、実行・閲覧権限を開発担当に確認

記録・行動：設定・実装・安全なテストの結果。機能なしなら根拠付きで該当なし。拡張子だけで完了にしない

☐ 確認済み ☐ 要対応 ☐ 不明 ☐ 該当なし

根拠・確認者：

次の担当・期限／該当なしの理由：

### 23 ログイン状態と重要操作の保護を確認した

確認：セッションの発行・更新・失効、認証用Cookieの属性、状態変更時の認可・CSRF対策を確認

記録・行動：対象処理・設計・テスト結果。Cookie用途を分け、全Cookieに同じ属性を強制しない

☐ 確認済み ☐ 要対応 ☐ 不明 ☐ 該当なし

根拠・確認者：

次の担当・期限／該当なしの理由：

### 24 WAF等の適用範囲と例外を確認した

確認：利用する防御機能の対象サイト、ルール、記録・遮断の動作、除外、更新、確認担当を確認

記録・行動：適用設定と記録、正規機能の動作結果。未導入なら必要性・代替策を判断。連続送信制御の有無も確認

☐ 確認済み ☐ 要対応 ☐ 不明 ☐ 該当なし

根拠・確認者：

次の担当・期限／該当なしの理由：

### 25 ブラウザの保護設定を用途に合わせて確認した

確認：応答ヘッダーと設定でCSP、埋め込み制限、nosniff、HSTS等の必要性・適用・例外を確認

記録・行動：対象ページ、設定理由、実際の応答と正常動作。ヘッダーの存在だけを安全性評価にしない

☐ 確認済み ☐ 要対応 ☐ 不明 ☐ 該当なし

根拠・確認者：

次の担当・期限／該当なしの理由：

# F 復旧と継続点検 26〜30

対象URL・確認日・確認者は余白または台帳に記入。根拠と次の担当・期限を各項目に残します。

### 26 必要なデータのバックアップと保護を確認した

確認：ファイル・DB・必要設定の対象、成功日時、世代、保管先と権限、同じ侵害で失われにくい構成を確認

記録・行動：バックアップの範囲・時点・保持条件・復旧可能な期間。サーバー会社の自動保存だけで未確認を埋めない

☐ 確認済み ☐ 要対応 ☐ 不明 ☐ 該当なし

根拠・確認者：

次の担当・期限／該当なしの理由：

### 27 別環境で復元し、必要な機能を確認した

確認：管理者が本番から分けて復元し、表示・管理ログイン・フォーム等を架空データで確認

記録・行動：復元元、条件、所要時間、確認結果、未復元範囲。実メールや決済等をテスト用へ切り替える

☐ 確認済み ☐ 要対応 ☐ 不明 ☐ 該当なし

根拠・確認者：

次の担当・期限／該当なしの理由：

### 28 必要なログを取得・保管・確認できる

確認：ログイン、管理操作、アクセス、エラー等の取得対象、期間、時差、権限、確認担当を確認

記録・行動：実際の取得例、保管期間、見方、不足範囲。秘密値や不要な個人情報を記録しない設計も確認

☐ 確認済み ☐ 要対応 ☐ 不明 ☐ 該当なし

根拠・確認者：

次の担当・期限／該当なしの理由：

### 29 改ざん等の通知と受信先を確認した

確認：利用中の監視、ホスト通知、Search Console等の対象・権限・受信先・通知を確認

記録・行動：通知先と対応担当、確認した画面と日時。テスト機能があれば受領確認。通知なしを被害なしとしない

☐ 確認済み ☐ 要対応 ☐ 不明 ☐ 該当なし

根拠・確認者：

次の担当・期限／該当なしの理由：

### 30 次回点検日と臨時確認の条件を決めた

確認：担当・代行・次回日、重要な脆弱性情報の確認先、担当交代・構成変更等の再確認条件を決める

記録・行動：点検予定と受領、通知の確認担当、異変時の連絡先。要対応・不明に担当と期限を付ける

☐ 確認済み ☐ 要対応 ☐ 不明 ☐ 該当なし

根拠・確認者：

次の担当・期限／該当なしの理由：

# 保守会社への確認依頼

対象と点検番号を絞り、現在の状態・根拠・保守範囲を尋ねます。未回答は不明のまま記録。

対象サイト・範囲／対象の点検番号：

宛先・担当／当社担当と連絡先／回答希望日：

当社で確認できた事実：

不明なこと・確認したい質問：

回答：現在の状態・確認日・根拠・保守範囲／未確認事項：

### 依頼に添える文面

対応が必要な場合は、対象、業務への影響、作業内容、費用・保守範囲、実施時期、変更前の保全と戻す方法、変更後の確認方法を提示してください。未確認・保守範囲外の事項は、その旨と確認先を教えてください。作業の実施は、内容を確認してから調整します。

質問例：No.26の保存対象にファイルとDBが含まれるか、最後の成功日時と、復旧できる期間を教えてください。

### 回答の判断例（架空）

「保存あり」でもDBの対象が分からなければ「不明」。必要な修正の未適用が確認できれば「要対応」です。管理画面に入れない場合も「不明」とし、契約先の正式な窓口へ引き継ぎを依頼します。

# 改善と再確認の記録

一つの対応につき1枚。設定の反映と、必要な業務機能の動作を確かめて閉じます。

対象番号・判明した問題：

対応順を決めた理由（公開範囲・扱う情報・業務への影響）：

判断する人／作業する人／確認する人：

行う変更・実施予定：

変更前の保全・検証場所・戻す方法：

完了条件（設定・必要な業務機能）：

実施内容・日時：

再確認の条件・結果・根拠：

残る問題・不明点／次の担当・期限：

作業進捗：　☐ 未着手　☐ 対応中　☐ 完了

点検の四つの状態と、作業の進捗を分けます。変更後に不明点が残れば、その確認を引き継ぎます。

# 次回点検と未完了事項の引き継ぎ

定期確認に加え、重要な脆弱性情報・担当交代・構成変更・外部サービス終了時も確認。

対象サイト／今回の確認日・担当／次回点検日・担当・代行：

| きっかけ | 確認先・担当 | 時期・条件 |
| --- | --- | --- |
| 定期点検 | | |
| 重要な脆弱性情報 | | |
| 担当・契約・構成変更 | | |
| 外部サービス終了 | | |

## 未完了事項は、回答を受け取る人まで指定する

対象番号・要対応／不明の内容：

次の行動・担当・期限／回答・引き継ぎの受領確認：

対象番号・要対応／不明の内容：

次の行動・担当・期限／回答・引き継ぎの受領確認：

異変発見時の連絡先／社内の初動対応手順の所在：

不明な項目も、公開範囲と扱う情報から確認順を決めます。重要な通知や具体的な異変は、次の定期日まで待たずに確認・連絡してください。

# 出典と、公開設定を確認する入口

出典確認：2026年10月24日。資料07は2026年10月18日の確認記録を参照。

01 IPA：運用管理の20ヶ条
クリックで公式資料を開く
02 IPA：安全なウェブサイトの作り方
クリックで公式資料を開く
03 WordPress：セキュリティ強化
クリックで公式資料を開く
04 WordPress：更新画面
クリックで公式資料を開く
05 WordPress：自動更新
クリックで公式資料を開く
06 PHP：サポート対象の版
クリックで公式資料を開く
07 JVN iPedia：管理者向けガイド
クリックで公式資料を開く
08 JPRS：ドメイン廃止の注意
クリックで公式資料を開く
09 Microsoft：子ドメイン管理
クリックで公式資料を開く
10 OWASP：多要素認証
クリックで公式資料を開く
11 Google：robots.txt
クリックで公式資料を開く
12 OWASP：外部JavaScript
クリックで公式資料を開く
13 OWASP：アップロード
クリックで公式資料を開く
14 OWASP：セッション管理
クリックで公式資料を開く
15 OWASP：CSRF対策
クリックで公式資料を開く
16 OWASP：HTTPヘッダー
クリックで公式資料を開く
17 OWASP：CSP
クリックで公式資料を開く
18 MDN：HSTS
クリックで公式資料を開く
19 Cloudflare：WAFルール
クリックで公式資料を開く
20 WordPress：バックアップ
クリックで公式資料を開く
21 Google：セキュリティの問題
クリックで公式資料を開く
22 OWASP：認可
クリックで公式資料を開く
23 Google：noindex
クリックで公式資料を開く
24 Red Hat：修正のバックポート
クリックで公式資料を開く
25 PHP：コマンドライン実行
クリックで公式資料を開く

資料の対象と時点を確認してください。各機関による本サービスの認定を示すものではありません。

## 自社サイトの公開設定を、無料で確認

Web AI Securityは、通信・証明書や取得したページの公開設定を確認します。最大10ページ・40項目、約3分が目安。内部権限やバックアップは、この点検票と管理者の確認で補ってください。サイト全体の安全保証ではありません。

無料AIセキュリティ検査を始める →