

セキュリティ診断報告書

外部公開 Web アプリケーション / 詳細チェック

対象 URL	https://example.jp/
ホスト	example.jp
診断 ID	sample-paid-report
診断日時	2026 年 10 月 26 日 11:07 JST
診断の前提	サンプルレポート（実在のサイトではありません）

目次

1	このレポートの読み方と修正の進め方	1
2	エグゼクティブサマリー	2
3	診断範囲と前提	3
4	ソフトウェアバージョン	3
5	所見一覧	4
6	詳細所見と推奨対応	4
7	診断上の制約と免責	12
付録 A	設定例	12
付録 B	診断メタデータ	13
付録 C	詳細ガイド：このサイトの直し方	14
付録 D	WordPress のログイン画面を守る	18
付録 E	WordPress 本体・プラグイン・テーマの更新	22
付録 F	WordPress の公開設定を見直す	24
付録 G	PHP の更新：CMS とは別の作業	26
付録 H	検出された所見ごとの修正手順	29
付録 I	修正後の確認チェックリスト	34

1 このレポートの読み方と修正の進め方

このレポートは、専門知識がない方でも修正の方向性が分かるように、各所見の後ろに「やさしい修正ガイド」を追加しています。ただし、画面の項目名や設定方法は、利用している WordPress のテーマ、プラグイン、サーバー、ホスティング会社によって異なります。修正ガイドの画面イメージは説明用です。実際の画面・項目名・配置は環境により異なります。

1. まず、レポートの「F 番号」と「重大度」を確認します。F 番号は、開発担当者やホスティング会社に質問するときの整理番号として使えます。
2. 修正の前に、必ずサイト全体とデータベースのバックアップを取ります。管理画面やホスティング会社のバックアップ機能を使い、元に戻せる状態を作ります。
3. 可能なら、本番環境ではなくステージング環境やテスト用サイトで先に試します。本番環境を直接編集すると、画面が崩れたりログインできなくなったりする可能性があります。
4. 一度にたくさんの設定を変えず、一つずつ修正して確認します。問題が起きたときに、どの変更が原因か分かりやすくするためです。
5. 「高」や「重大」の所見は、公開前・公開後を問わず優先して確認します。ただし、重大度は「問題の種類」と「実際に悪用できるか」で変わります。レポートの観測内容と再現手順も必ず確認してください。
6. 自動診断の結果には、誤検知（実際には悪用できないもの）や、設定によって影響が変わるものが含まれます。判断に迷う場合は、修正前に専門家へ相談してください。
7. 修正後は、同じ URL をもう一度診断します。所見が消えたことだけでなく、サイトの表示・ログイン・問い合わせ・決済などが正常に動くことも確認します。
8. パスワード、API キー、Cookie、個人情報を、チャット・メール・レポートにそのまま貼り付けないでください。漏えいが疑われる場合は、値そのものを変更（ローテーション）します。

重要な用語: XSS は入力した文字がスクリプトとして動く問題、SQL インジェクションはデータベースへの命令を乗っ取られる問題、CORS は別サイトから API の応答を読める設定、SSRF はサーバーに任意の URL へアクセスさせる問題です。

2 エグゼクティブサマリー

本レポートは詳細レポートです。詳細診断の購入に含まれています。検出内容・証拠に加えて、対象サイトの構成に合わせた修正手順（解決策）、設定例、優先順位、再診断手順を掲載しています。

このレポートは、問題の指摘で終わりません。管理画面の場所、修正手順、修正後の確認、ホスティング会社への依頼文まで掲載しています。

本診断では、対象サイトの外部公開面に対する受動的チェックと、未認証の追加チェックを実施しました。ログインを伴うテストは行っていません。以下は、検出された所見の要約です。

52 / 100

リスクスコア（100 点満点・低いほど要注意）

重大リスク

重大度	件数	意味
-----	----	----

重大	1	即時対応が必要な深刻な問題
高	0	優先的に対応すべき問題
中	3	計画的に対応すべき問題
低	0	ベストプラクティス上の改善項目
情報	6	参考情報

総評: 本レポートの所見は、外部から観測できた範囲（未認証の追加チェック）に基づきます。重大度「高」以上の所見がある場合は、公開環境への影響を確認したうえで、優先的に対策を実施してください。

最初に確認する所見

1. **重大** Outdated PHP version（確度: 高）
2. **中** XML-RPC endpoint reachable（確度: 高）
3. **中** Missing Content-Security-Policy（確度: 高）

3 診断範囲と前提

対象	https://example.jp/
診断範囲	外部公開面の受動的チェック + 未認証の追加チェック
認証・診断の前提	サンプルレポート（実在のサイトではありません）
認証情報の取扱い	未認証の詳細チェック。テストアカウントやログイン情報は使用していません。
診断日時	2026 年 10 月 26 日 11:07 JST
レポート生成	2026 年 10 月 26 日 11:07 JST

4 ソフトウェアバージョン

公開メタデータから確認できたソフトウェアバージョンです。バージョンが非公開の場合は、管理画面やサーバー側で確認してください。

ソフトウェア	検出版	状態
WordPress	6.8.2	要更新（中 / 最新 6.9）
PHP	不明	要更新（重大）
contact-form-7	5.8.1	公開アセットから検出（要確認）
twentytwentyfour	1.2	公開アセットから検出（要確認）

実施した確認

- HTTP レスポンスヘッダー、Cookie 属性、TLS/HTTPS 遷移、公開ファイル、WordPress 関連エンドポイントの受動的確認
- 公開リンク、フォーム、JavaScript、robots.txt、sitemap からの未認証エンドポイント棚卸し
- 反射型 XSS、SQL エラー、ブラインド SQL、SSTI、パストラバーサル、コマンドインジェクション、オープンリダイレクト、CRLF、JSONP、NoSQL の安全な検証
- スキャナ管理カナリアによる SSRF、CORS、HTTP メソッド、公開ファイル、GraphQL、WordPress、CSRF、Cookie、セキュリティヘッダーの確認

実施していないこと

本診断は、ブルートフォース、DoS、エクスプロイト、Web シェル設置、永続化、管理者権限の奪取、本番ユーザー情報の取得を実施していません。また、対象外ホストへのテストは行っていません。

5 所見一覧

重大度の高い順に記載しています。各所見の詳細と推奨対応は次章を参照してください。

ID	検出内容	重大度	確度	分類
F-01	Outdated PHP version	重大	高	サーバー / PHP サポート終了
F-02	XML-RPC endpoint reachable	中	高	WordPress / XML-RPC
F-03	Missing Content-Security-Policy	中	高	HTTP ヘッダー / CSP
F-04	Outdated WordPress core	中	中	CMS / WordPress 更新
F-05	WordPress detected	情報	高	WordPress / 構成情報
F-06	WordPress version detected	情報	高	参考情報
F-07	WordPress plugin detected: contact-form-7	情報	高	参考情報
F-08	WordPress theme detected: twentytwentyfour	情報	高	参考情報
F-09	WordPress login page reachable	情報	高	参考情報
F-10	Hosting / server fingerprint	情報	高	参考情報

6 詳細所見と推奨対応

F-01 Outdated PHP version

重大

分類: サーバー / PHP サポート終了 / 確度: 高

観測内容 PHP 8.3.35 was exposed and is below a release that fixes CVE-2026-109618 / CVE-2026-109619 (php2shell). Update to PHP 8.5.12, 8.4.27, 8.3.36, or 8.2.35.

■影響 公開ヘッダーから確認できた PHP がサポート終了またはセキュリティサポート終了間近です。今後見つかる脆弱性が修正されない可能性があります。

■**推奨対応** サポートされている PHP (8.2 以降、可能なら 8.3/8.4) へアップグレードしてください。PHP を更新する前に、CMS・プラグイン・テーマの互換性をステージング環境で確認してください。

■**確認方法** サーバーの PHP バージョンと SAPI を確認し、更新後にアプリケーションの動作とエラーログを確認します。

やさしい修正ガイド

何が問題か: 古いソフトウェアを使っているため、既知の脆弱性が残っている可能性があります。**最初に**

確認する場所: WordPress 管理画面の更新、PHP のバージョン、ホスティングの PHP 設定、プラグイン・テーマ。**修正手順:**

1. サイト全体とデータベースのバックアップを取ります。
2. まずステージング環境で WordPress 本体・テーマ・プラグインを更新します。
3. PHP はホスティングの管理画面でサポートされている最新版に変更します。
4. 更新後に表示崩れ、フォーム、ログイン、決済などを確認します。
5. 使っていないプラグインやテーマは削除します。
6. 本番反映後、再度診断してバージョンを確認します。

修正後の確認: 管理画面と診断結果で、WordPress/PHP のバージョンが最新になっていることを確認します。**注意:** 本番環境をいきなり変更しないでください。先にバックアップを取り、可能ならステージング環境やテスト用サイトで同じ手順を試してください。管理画面の設定名や項目名は、利用しているテーマ・プラグイン・サーバーによって異なります。

F-02 XML-RPC endpoint reachable

中

分類: WordPress / XML-RPC / 確度: 高

観測内容 xmlrpc.php responded; disable it if unused.

■**影響** XML-RPC が公開されており、認証試行や増幅攻撃の踏み台に利用される可能性があります。

■**推奨対応** XML-RPC を使用していない場合は無効化してください。使用する場合も、アクセス制限、認証試行の制限、不要なメソッドの無効化を行います。

■**確認方法** 外部から/xmlrpc.php へアクセスし、405 または拒否されることを確認します。

やさしい修正ガイド

何が問題か: この所見は、入力値の扱い・サーバー設定・公開ファイルのいずれかに問題がある可能性を示しています。**最初に確認する場所:** レポートの対象 URL、観測内容、利用している CMS・プラグイン

ン・サーバー設定。修正手順:

1. まず対象 URL と再現手順を確認し、同じ現象がテスト環境でも起きるか確認します。
2. サイト全体とデータベースのバックアップを取ります。
3. 利用している CMS、テーマ、プラグイン、サーバーのバージョンを確認し、最新版に更新します。
4. 該当する設定や入力処理を特定し、許可リスト・エスケープ・認証などの基本対策を実施します。
5. 修正後、同じ URL を再診断し、所見が消えることを確認します。

修正後の確認: 診断を再実行し、同じ所見が出ないことを確認します。判断に迷う場合は、ホスティング会社または開発担当者にレポートの F 番号を伝えてください。**注意:** 本番環境をいきなり変更しないでください。先にバックアップを取り、可能ならステージング環境やテスト用サイトで同じ手順を試してください。管理画面の設定名や項目名は、利用しているテーマ・プラグイン・サーバーによって異なります。

F-03 Missing Content-Security-Policy

中

分類: HTTP ヘッダー / CSP / 確度: 高

観測内容 CSP is not set.

■影響 CSP が未設定のため、XSS 発生時のスクリプト実行や外部リソース読み込みをブラウザ側で抑制できません。

■推奨対応 default-src を基準に、script-src、style-src、img-src などを必要最小限に制限してください。nonce または hash を利用し、'unsafe-inline' の常用は避けます。

■確認方法 ブラウザ開発者ツールで CSP ヘッダーを確認し、正当な機能がブロックされないことをテストします。

やさしい修正ガイド

何が問題か: CSP が未設定、または危険な設定のため、XSS が起きたときにスクリプトの実行を止められない可能性があります。**最初に確認する場所:** Web サーバー、CDN、WordPress のセキュリティプラグイン、テーマの functions.php で CSP ヘッダーを設定している箇所。**修正手順:**

1. まず既存の CSP を確認し、どのスクリプト・画像・スタイルを読み込んでいるか把握します。
2. 最初は Content-Security-Policy-Report-Only でテストし、サイトが壊れないか確認します。
3. default-src 'self' を基本にし、必要な外部ドメインだけを追加します。
4. script-src から unsafe-inline と unsafe-eval を外し、nonce または hash を使います。
5. frame-ancestors 'self' や object-src 'none' も必要に応じて設定します。
6. 修正後、ブラウザの Console に CSP 違反が出ていないことを確認します。

修正後の確認: ブラウザの開発者ツールの Network/Headers で CSP を確認し、Console に違反エラーがないことを確認します。**注意:** 本番環境をいきなり変更しないでください。先にバックアップを取り、可能ならステージング環境やテスト用サイトで同じ手順を試してください。管理画面の設定名や項目名は、利用しているテーマ・プラグイン・サーバーによって異なります。

F-04 Outdated WordPress core

中

分類: CMS / WordPress 更新 / 確度: 中

観測内容 WordPress 6.8.2 is older than the current release (6.9). Update WordPress core, themes, and plugins; verify the site after upgrading.

■**影響** 公開メタデータから確認できた WordPress が最新版より古い状態です。既知の脆弱性が修正されていない可能性があり、プラグインやテーマも同様に更新が必要です。

■**推奨対応** WordPress 本体を最新版へ更新し、テーマ・プラグインの更新状況も確認してください。不要なプラグインやテーマは削除し、更新前にバックアップを取得してください。

■**確認方法** 管理画面または WP-CLI でバージョンを確認し、更新後に公開ページと管理画面の動作を確認します。

やさしい修正ガイド

何が問題か: 古いソフトウェアを使っているため、既知の脆弱性が残っている可能性があります。**最初に確認する場所:** WordPress 管理画面の更新、PHP のバージョン、ホスティングの PHP 設定、プラグイン・テーマ。**修正手順:**

1. サイト全体とデータベースのバックアップを取ります。
2. まずステージング環境で WordPress 本体・テーマ・プラグインを更新します。
3. PHP はホスティングの管理画面でサポートされている最新版に変更します。
4. 更新後に表示崩れ、フォーム、ログイン、決済などを確認します。
5. 使っていないプラグインやテーマは削除します。
6. 本番反映後、再度診断してバージョンを確認します。

修正後の確認: 管理画面と診断結果で、WordPress/PHP のバージョンが最新になっていることを確認します。**注意:** 本番環境をいきなり変更しないでください。先にバックアップを取り、可能ならステージング環境やテスト用サイトで同じ手順を試してください。管理画面の設定名や項目名は、利用しているテーマ・プラグイン・サーバーによって異なります。

F-05 WordPress detected

情報

分類: WordPress / 構成情報 / 確度: 高

観測内容 WordPress assets or REST API were observed.

■影響 WordPress の利用が確認できました。プラグインやテーマを含む更新状況を継続的に管理する必要があります。

■推奨対応 WordPress 本体、テーマ、プラグインを最新状態に保ち、不要なプラグインを削除してください。管理画面へのアクセス制限とバックアップを運用してください。

■確認方法 更新状況、不要プラグイン、管理画面の公開範囲を定期確認します。

やさしい修正ガイド

何が問題か: WordPress の設定や公開ファイルに関する所見です。WordPress は更新と公開情報の整理が重要です。**最初に確認する場所:** WordPress 管理画面、wp-content、wp-config.php、テーマ、プラグイン、サーバー設定。**修正手順:**

1. WordPress 本体・テーマ・プラグインをバックアップします。
2. 不要な readme.html、license.txt、debug.log、バックアップファイルを公開ディレクトリから削除します。
3. XML-RPC が不要なら無効化します。
4. ユーザー一覧を公開しない設定にします。
5. WordPress 本体・テーマ・プラグインを最新版に更新します。
6. 修正後、該当 URL を匿名で開いて 404・403 になることを確認します。

修正後の確認: 対象の WordPress URL を再診断し、該当する所見が消えることを確認します。**注意:** 本番環境をいきなり変更しないでください。先にバックアップを取り、可能ならステージング環境やテスト用サイトで同じ手順を試してください。管理画面の設定名や項目名は、利用しているテーマ・プラグイン・サーバーによって異なります。

F-06 WordPress version detected

情報

分類: 参考情報 / 確度: 高

観測内容 WordPress 6.8.2 was identified from the generator meta tag or a core wp-includes asset.

■影響 現時点で脆弱性を示すものではない参考情報です。

■推奨対応 追加の対応は不要です。診断結果の記録として保管してください。

■確認方法 次回診断時に変化がないか確認します。

やさしい修正ガイド

何が問題か: WordPress の設定や公開ファイルに関する所見です。WordPress は更新と公開情報の整理が重要です。**最初に確認する場所:** WordPress 管理画面、wp-content、wp-config.php、テーマ、プラグイン、サーバー設定。**修正手順:**

1. WordPress 本体・テーマ・プラグインをバックアップします。
2. 不要な readme.html、license.txt、debug.log、バックアップファイルを公開ディレクトリから削除します。
3. XML-RPC が不要なら無効化します。
4. ユーザー一覧を公開しない設定にします。
5. WordPress 本体・テーマ・プラグインを最新版に更新します。
6. 修正後、該当 URL を匿名で開いて 404・403 になることを確認します。

修正後の確認: 対象の WordPress URL を再診断し、該当する所見が消えることを確認します。**注意:** 本番環境をいきなり変更しないでください。先にバックアップを取り、可能ならステージング環境やテスト用サイトで同じ手順を試してください。管理画面の設定名や項目名は、利用しているテーマ・プラグイン・サーバーによって異なります。

F-07 WordPress plugin detected: contact-form-7

情報

分類: 参考情報 / 確度: 高

観測内容 Plugin contact-form-7 assets were observed with version 5.8.1. Public asset versions can be stale or manipulated; verify the installed version in the admin area.

■影響 現時点で脆弱性を示すものではない参考情報です。

■推奨対応 追加の対応は不要です。診断結果の記録として保管してください。

■確認方法 次回診断時に変化がないか確認します。

やさしい修正ガイド

何が問題か: WordPress の設定や公開ファイルに関する所見です。WordPress は更新と公開情報の整理が重要です。**最初に確認する場所:** WordPress 管理画面、wp-content、wp-config.php、テーマ、プラグ

イン、サーバー設定。修正手順:

1. WordPress 本体・テーマ・プラグインをバックアップします。
2. 不要な readme.html、license.txt、debug.log、バックアップファイルを公開ディレクトリから削除します。
3. XML-RPC が不要なら無効化します。
4. ユーザー一覧を公開しない設定にします。
5. WordPress 本体・テーマ・プラグインを最新版に更新します。
6. 修正後、該当 URL を匿名で開いて 404・403 になることを確認します。

修正後の確認: 対象の WordPress URL を再診断し、該当する所見が消えることを確認します。**注意:** 本番環境をいきなり変更しないでください。先にバックアップを取り、可能ならステージング環境やテスト用サイトで同じ手順を試してください。管理画面の設定名や項目名は、利用しているテーマ・プラグイン・サーバーによって異なります。

F-08 WordPress theme detected: twentytwentyfour

情報

分類: 参考情報 / 確度: 高

観測内容 Theme twentytwentyfour assets were observed with version 1.2. Public asset versions can be stale or manipulated; verify the installed version in the admin area.

■**影響** 現時点で脆弱性を示すものではない参考情報です。

■**推奨対応** 追加の対応は不要です。診断結果の記録として保管してください。

■**確認方法** 次回診断時に変化がないか確認します。

やさしい修正ガイド

何が問題か: WordPress の設定や公開ファイルに関する所見です。WordPress は更新と公開情報の整理が重要です。**最初に確認する場所:** WordPress 管理画面、wp-content、wp-config.php、テーマ、プラグイン、サーバー設定。**修正手順:**

1. WordPress 本体・テーマ・プラグインをバックアップします。
2. 不要な readme.html、license.txt、debug.log、バックアップファイルを公開ディレクトリから削除します。
3. XML-RPC が不要なら無効化します。
4. ユーザー一覧を公開しない設定にします。
5. WordPress 本体・テーマ・プラグインを最新版に更新します。
6. 修正後、該当 URL を匿名で開いて 404・403 になることを確認します。

修正後の確認: 対象の WordPress URL を再診断し、該当する所見が消えることを確認します。**注意:** 本番環境をいきなり変更しないでください。先にバックアップを取り、可能ならステージング環境やテスト用サイトで同じ手順を試してください。管理画面の設定名や項目名は、利用しているテーマ・プラグイン・サーバーによって異なります。

F-09 WordPress login page reachable

情報

分類: 参考情報 / 確度: 高

観測内容 The standard wp-login.php page is publicly reachable. Protect it with strong passwords, two-factor authentication, login rate limiting, and updates.

■影響 現時点で脆弱性を示すものではない参考情報です。

■推奨対応 追加の対応は不要です。診断結果の記録として保管してください。

■確認方法 次回診断時に変化がないか確認します。

やさしい修正ガイド

何が問題か: WordPress の設定や公開ファイルに関する所見です。WordPress は更新と公開情報の整理が重要です。**最初に確認する場所:** WordPress 管理画面、wp-content、wp-config.php、テーマ、プラグイン、サーバー設定。**修正手順:**

1. WordPress 本体・テーマ・プラグインをバックアップします。
2. 不要な readme.html、license.txt、debug.log、バックアップファイルを公開ディレクトリから削除します。
3. XML-RPC が不要なら無効化します。
4. ユーザー一覧を公開しない設定にします。
5. WordPress 本体・テーマ・プラグインを最新版に更新します。
6. 修正後、該当 URL を匿名で開いて 404・403 になることを確認します。

修正後の確認: 対象の WordPress URL を再診断し、該当する所見が消えることを確認します。**注意:** 本番環境をいきなり変更しないでください。先にバックアップを取り、可能ならステージング環境やテスト用サイトで同じ手順を試してください。管理画面の設定名や項目名は、利用しているテーマ・プラグイン・サーバーによって異なります。

F-10 Hosting / server fingerprint

情報

分類: 参考情報 / 確度: 高

観測内容 Server: nginx. Hosting hint: Kinsta. This is a passive response-header fingerprint. A CDN, reverse proxy, or WAF can hide the origin hosting provider; do not treat it as proof of the physical server.

■影響 現時点で脆弱性を示すものではない参考情報です。

■推奨対応 追加の対応は不要です。診断結果の記録として保管してください。

■確認方法 次回診断時に変化がないか確認します。

やさしい修正ガイド

何が問題か: この項目は、脆弱性そのものではなく、診断結果や確認状況を説明する情報です。**最初に確認する場所:** レポートの対象 URL と観測内容。**修正手順:**

1. 内容を確認し、必要に応じて開発担当者やホスティング会社に共有します。
2. 脆弱性を示す所見ではない場合、無理に設定を変更する必要はありません。
3. 次回の診断で同じ情報が表示されるか確認します。

修正後の確認: 再診断で所見の内容が変わらないこと、または意図した状態になっていることを確認します。**注意:** 情報所見でも、内容によっては追加調査が必要です。判断に迷う場合は専門家に確認してください。

7 診断上の制約と免責

本診断は、外部から観測できた範囲（未認証の追加チェック）で実施した自動診断です。以下を保証するものではありません。

- すべての脆弱性の検出、または修正後の安全性の完全な保証
- 本番ユーザー全体の権限境界、業務ロジック、内部 API の安全性
- 第三者サービス、外部 SDK、インフラストラクチャ設定の完全な確認

本レポートは依頼者および許可された関係者向けの機密情報です。対象サイトの所有者・管理者の許可なく第三者へ公開しないでください。

付録 A 設定例

以下は一般的な設定例です。実際の設定はホスティング環境、既存のヘッダー、CMS、CDN によって異なります。変更前にバックアップとステージング環境での確認を行ってください。

WordPress / nginx の例

```
location = /xmlrpc.php { deny all; return 403; }
location ~* /wp-config\.(php|bak|old|save|swp)$ { deny all; }
location ~ /\.(?!well-known/) { deny all; }
location ~* /(readme|license)\.(html|txt)$ { deny all; }
```

付録 B 診断メタデータ

レポート版	41
診断 ID	sample-paid-report
対象ホスト	example.jp
診断日時	2026 年 10 月 26 日 11:07 JST
診断の前提	サンプルレポート（実在のサイトではありません）
所見数	重大 1 / 高 0 / 中 3 / 低 0 / 情報 6

付録 C 詳細ガイド：このサイトの直し方

この章は、専門用語に慣れていない方でも、上から順番に実行できるように書いています。すべてを一度に行う必要はありません。まずバックアップを取り、影響の大きい項目から一つずつ直してください。自分で進められる作業を先に示し、ホスティング会社の管理画面が必要な作業は、その画面名と依頼文まで記載しています。分からない作業を無理に進めるより、該当する章だけホスティング会社や制作会社に見せて「この順番で対応してください」と依頼するほうが安全です。

このレポートが前提にしているアクセス権

このレポートは、次の2つにログインできる方を対象にしています。サイトの管理画面（WordPress など）だけ、ホスティングの管理画面だけ、という場合でも、どこまで自分で直せるかをこの節で確認してください。WordPress 以外のサイトでは、WordPress 専用の章（ログイン、本体更新など）を読み飛ばし、PHP、公開ファイル、F 番号ごとの手順を使ってください。

アクセス先	必要度	このレポートで使う作業
サイト管理画面	必須	CMS 本体・プラグイン・テーマの更新、ユーザー、2 段階認証、XML-RPC、公開設定
ホスティング管理画面	必須	PHP の更新、バックアップ、WAF、403 設定、アクセスログ

■**サイトの管理画面だけある場合** WordPress などの CMS 本体、プラグイン、テーマ、ログイン設定は自分で直せます。PHP の更新だけはホスティング管理画面が必要です。この章の「PHP の更新」に、そのまま送れる依頼文を用意しています。FTP しかない場合、PHP のバージョンは変更できません。FTP で CMS 本体を直接編集するより、ホスティング会社へ依頼してください。

■**ホスティング管理画面だけある場合** PHP、バックアップ、WAF、403 設定は操作できます。CMS 本体・プラグイン・テーマの更新は、サイトの管理者にこの章を渡してください。管理画面のログイン情報を、作業代行の人に必要以上に共有しないでください。

■**どちらの管理画面もない場合** このレポートを、サイトの管理者、制作会社、またはホスティング会社へ渡してください。レポートには、変更する画面、現在のバージョン、修正版、確認方法を記載しています。FTP のファイル編集やデータベースの直接変更から始めないでください。復旧が難しくなります。

■**ホスティング会社が分からない場合** 請求書、契約時のメール、ドメインの DNS 設定、ブラウザのブックマークを確認してください。サイトの管理画面にサーバー情報の項目があれば確認できますが、契約しているホスティング会社までは分かりません。主な管理画面は次のとおりです（2026 年 10 月時点の目安）。

ホスティング	管理画面の入口
Xserver	https://www.xserver.ne.jp/login_server.php
ConoHa WING	https://www.conoha.jp/login/
さくらのレンタルサーバ	https://secure.sakura.ad.jp/
ロリポップ!	https://user.lolipop.jp/
Kinsta	https://my.kinsta.com/
WP Engine	https://my.wpengine.com/

このガイドの使い方

1. 最初に、サイトとサーバーのバックアップを取ります。バックアップがない状態で設定を変えないでください。
2. 作業は、アクセスが少ない時間帯に行います。作業中はサイトを閉じる、またはメンテナンス画面を出すことをおすすめします。
3. 一度にたくさんの設定を変えず、一項目ずつ変更します。変更した日時、変更前の値、変更後の値をメモします。
4. 各手順の最後に「確認」があります。確認が終わるまで次の項目へ進まないでください。
5. 画面の名称は CMS の種類、バージョン、テーマ、プラグイン、ホスティング会社によって少し異なります。目的の項目が見つからない場合は、似た名前の項目を探るか、ホスティング会社のサポートに画面名を伝えてください。
6. パスワード、API キー、Cookie、個人情報を、このレポートを共有する相手以外に送らないでください。
7. 修正後に問題が起きた場合は、バックアップから戻せることを確認してから作業を始めてください。

このサイトで確認できた構成

対象 URL	'https://example.jp/
確認されたホスト	example.jp
WordPress	検出されました
WordPress ログイン画面	公開されています
PHP 関連の所見	検出されました
公開情報から検出した PHP	8.3.35
推定ホスティング	Kinsta
ホスティングの手がかり	Server: nginx. Hosting hint: Kinsta. This is a passive response-header fingerprint. A CDN, reverse proxy, or WAF can hide the origin hosting provider; do not treat it as proof of the physical server.

作業前に用意するもの

- サイトの管理者アカウント（WordPress など）。管理者権限がない場合は、サイトの管理者にこの章を渡してください。
- ホスティング会社の管理画面のログイン情報。PHP の更新、WAF、バックアップ、アクセスログは、CMS の管理画面ではなくホスティング側で操作することがあります。
- CMS のバックアッププラグイン、またはホスティング会社の自動バックアップ。どちらか一方だけでなく、可能なら両方を確認してください。
- パスワード管理アプリ。同じパスワードを使い回さないために必要です。
- 作業メモ。日時、変更した画面、変更前の値、変更後の値を記録します。
- スマートフォンなど、作業とは別の端末。2 段階認証の設定確認に使用します。

このサイトの修正順序

まずバックアップを取り、次の表の上から順に進めてください。作業時間は初回の目安です。同じ画面で複数の項目を直せる場合は、まとめて確認してかまいません。

ID	検出内容	重大度	最初にすること	目安
F-01	Outdated PHP version	重大	ホスティング管理画面で PHP を修正版へ変更	20 分

ID	検出内容	重大度	最初にすること	目安
F-02	XML-RPC endpoint reachable	中	使っていなければ XML-RPC を無効化	10 分
F-03	Missing Content-Security-Policy	中	ホスティング画面または CDN でヘッダーを追加	20 分
F-04	Outdated WordPress core	中	ダッシュボード → 更新で WordPress 本体を更新	15 分
F-05	WordPress detected	情報	本体・テーマ・プラグインの更新状況を確認	10 分
F-06	WordPress version detected	情報	サイトヘルスで最新版か確認	10 分
F-07	WordPress plugin detected: contact-form-7	情報	プラグイン → インストール済みプラグインで更新・削除	15 分
F-08	WordPress theme detected: twentytwentyfour	情報	外観 → テーマで更新・削除	10 分
F-09	WordPress login page reachable	情報	2 段階認証とログイン試行制限を設定	30 分
F-10	Hosting / server fingerprint	情報	情報のみ。作業は不要	なし

重大度が「高」または「重大」の項目は、公開サイトで優先的に確認してください。ただし、重大度は「攻撃されたらどうなるか」の目安であり、実際に攻撃されている証拠ではありません。不審なアクセス、知らない管理者、見覚えのないプラグインがある場合は、設定変更より先にホスティング会社へ相談してください。情報（info）の項目は、直ちに修正が必要な脆弱性ではないことがあります。表の「情報のみ」は、記録として残すだけで構いません。

付録 D WordPress のログイン画面を守る

このサイトでは、WordPress の標準ログイン画面（wp-login.php）が公開されていることを確認しました。WordPress を使う限りログイン画面は必要なものですが、インターネット上の自動攻撃は、この画面に対して繰り返しパスワードを試します。ログイン画面を隠すことだけに頼らず、パスワード、2 段階認証、試行回数の制限、更新を組み合わせてください。



画面イメージ：ユーザー→プロフィールで 2 段階認証を設定します。実際の画面は環境により異なります。

手順 1：バックアップと管理者アカウントの確認

1. ホスティング会社の管理画面で、WordPress のファイルとデータベースのバックアップを作成します。バックアップの作成日時と保存先をメモします。
2. WordPress の管理画面にログインし、左メニューの「ユーザー」→「ユーザー一覧」を開きます。
3. 管理者権限のユーザーを確認します。使っていない管理者、退職した担当者、心当たりのない管理者が残っていないか確認します。
4. 心当たりのない管理者がいる場合は、そのユーザーを削除する前に、ホスティング会社または制作会社へ相談してください。攻撃を受けている可能性があります。
5. 管理者が複数いる場合は、全員のパスワードを、他のサイトと違う長いパスワードに変更します。
6. ユーザー名を「admin」にしている場合は、表示名だけでなくログイン名も変更できるか確認します。WordPress の仕様上、ログイン名そのものは変更しにくいいため、新しい管理者ユーザーを作成して古いユーザーを削除する方法もあります。ただし、コンテンツの所有者が変わるため、必ずバックアップ後に行ってください。

手順 2：2 段階認証を有効にする

パスワードが漏れても、2 段階認証（2FA）があればログインを防げる可能性が大きくなります。次のどれかを導入してください。

- SiteGuard WP Plugin：日本国内の WordPress でよく使われるログイン保護プラグインです。ログイン試行制限、ログイン URL 変更、画像認証などを設定できます。
- Wordfence Security：ログイン試行制限、2 段階認証、WAF、診断などをまとめて設定できます。無料版でも基本的な保護を設定できます。
- ホスティング会社が提供する WAF、または WordPress のログイン保護サービス。

導入時の注意点：

1. WordPress の「プラグイン」→「新規追加」を開きます。
2. プラグイン名を検索し、配布元、最終更新日、対応する WordPress バージョン、レビューを確認します。
3. 「今すぐインストール」→「有効化」を押します。
4. プラグインの設定画面を開き、2 段階認証を有効にします。スマートフォンの認証アプリ（Google Authenticator、Microsoft Authenticator、Authy など）で QR コードを読み取ります。
5. 表示された回復コード（バックアップコード）を、紙またはパスワード管理アプリに保存します。回復コードをなくすと、スマートフォンを紛失したときにログインできなくなります。
6. シークレットウィンドウ（プライベートブラウズ）でログアウトし、再度ログインして、2 段階認証が実際に要求されることを確認します。

手順 3：ログイン試行回数を制限する

自動攻撃は、短時間に何百回もログインを試します。次のいずれかを設定してください。

1. SiteGuard WP Plugin の「ログイン試行制限」を有効にし、一定回数失敗したら一定時間ログインを拒否する設定にします。
2. Wordfence Security の「Login Security」または「Brute Force Protection」を有効にします。
3. ホスティング会社の WAF で、WordPress のログイン画面に対するレート制限を設定できるか確認します。

設定値の目安は、5 回失敗で 15 分から 30 分ロックです。ただし、正規の管理者がロックアウトされる可能性もあるため、回復方法を確認してから設定してください。

手順 4：XML-RPC を無効にする

XML-RPC は、WordPress を外部アプリから操作するための古い仕組みです。使っていない場合は、攻撃の入口を減らすために無効化を検討してください。

1. SiteGuard WP Plugin または Wordfence Security の設定画面で、XML-RPC を無効にする項目を探します。
2. 設定を保存したあと、ブラウザで「https://このサイトのドメイン/xmlrpc.php」を開きます。
3. 「XML-RPC server accepts POST requests only.」のような画面が出る場合は、まだ有効です。設定が反映されているか確認してください。
4. XML-RPC を業務で使っているアプリがある場合は、無効化すると動かなくなります。先に利用状況を確認し、必要な場合だけ許可リストを設定します。

手順 5：ユーザー名を推測されにくくする

WordPress では、投稿者の一覧や REST API からユーザー名の手がかりが公開されることがあります。次の対策を検討してください。

1. 「設定」→「パーマリンク」で、投稿者アーカイブを無効にできるか確認します。テーマによっては設定が異なります。
2. 「ユーザー」→「ユーザー一覧」で、表示名をログイン名と同じにしないようにします。
3. WAF またはセキュリティプラグインで、/wp-json/wp/v2/users への不要なアクセスを制限します。
4. ユーザー名を隠すだけではログイン攻撃は止まりません。2 段階認証と試行回数の制限を必ず併用してください。

手順 6：ログイン URL の変更を検討する

ログイン URL を変更すると、一般的な自動攻撃の一部を減らせます。ただし、URL を知られれば同じ攻撃ができるため、これは補助的な対策です。

1. SiteGuard WP Plugin の「ログイン URL 変更」を開きます。
2. 新しいログイン URL を、推測されにくい文字列にします。英数字とハイフンを使い、サイト名そのまは避けます。
3. 変更後の URL を管理者全員に安全な方法で共有し、ブラウザのブックマークを更新します。
4. シークレットウィンドウで新しい URL からログインできることを確認します。
5. 元の URL にアクセスしたときに、ログイン画面が表示されないことを確認します。

URL 変更後に管理画面へ入れなくなった場合は、ホスティングのファイルマネージャーで該当プラグイ

ンのフォルダ名を一時的に変更し、元に戻してください。操作が分からない場合は、ホスティング会社へ連絡してください。

手順 7：ログインの監視と記録

1. Wordfence Security の「Live Traffic」または「Login Attempts」を確認し、不審な IP や失敗ログインがないか見ます。
2. ホスティング会社のアクセスログで、`wp-login.php` への大量アクセスがないか確認します。
3. 心当たりのない管理者、見覚えのないプラグイン、投稿の改変があれば、設定変更より先にホスティング会社とセキュリティ専門家へ相談してください。
4. ログイン試行の記録は、個人情報を含む場合があるため、共有範囲に注意してください。

手順 8：最後に確認すること

1. シークレットウィンドウで、管理者ログイン、2 段階認証、ログアウト、再ログインを確認します。
2. 一般の閲覧者が、管理画面に入れないことを確認します。
3. サイトの表示、問い合わせフォーム、検索、決済など、通常の機能が壊れていないことを確認します。
4. 数日後にもう一度ログインし、2 段階認証と試行制限が有効なままか確認します。

ログインできなくなったとき

2 段階認証やログイン URL 変更で管理画面に入れなくなった場合は、あわてず次の順番で戻します。

1. ホスティング会社のファイルマネージャーまたは FTP で、WordPress のプラグイン一覧を開きます。
2. 直前に設定したセキュリティプラグインのフォルダ名を、`plugin-name.disabled` のように一時変更します。フォルダを削除しないでください。
3. WordPress のログイン画面に戻り、通常のパスワードでログインできるか確認します。
4. ログインできたら、プラグインを元のフォルダ名に戻し、設定を見直します。
5. どうしても戻せない場合は、ホスティング会社のバックアップから復元します。復元すると、作業後の投稿や設定も戻るため、必要に応じてエクスポートを取っておきます。

付録 E WordPress 本体・プラグイン・テーマの更新

WordPress の更新は、セキュリティ修正だけでなく、不具合修正や新機能も含まれます。ただし、更新によって画面やプラグインが動かなくなることがあるため、必ずバックアップと確認を行います。



画面イメージ：ダッシュボードの「更新」を開きます。実際の項目名は環境により異なります。



画面イメージ：プラグイン一覧で更新状況を確認します。実際の画面は環境により異なります。

手順 1：バックアップ

1. ホスティング会社の管理画面で、ファイルとデータベースをバックアップします。
2. WordPress の「ツール」→「エクスポート」でコンテンツのバックアップも取ります。
3. バックアップファイルの保存先と日時をメモします。

手順 2：更新の順番

1. WordPress の管理画面で「ダッシュボード」→「更新」を開きます。
2. まず WordPress 本体を更新します。更新前に「詳細」を開き、PHP の対応バージョンを確認します。
3. 次に、プラグインを一つずつ更新します。すべてを一度に更新せず、重要なプラグインから順番に更新し、その都度サイトを確認します。
4. 最後にテーマを更新します。子テーマを使っている場合でも、親テーマの更新内容を確認します。
5. 更新後、トップページ、固定ページ、投稿、問い合わせ、決済、ログインを確認します。

手順 3：使っていないプラグインとテーマを減らす

1. 「プラグイン」→「インストール済みプラグイン」で、使っていないプラグインを確認します。
2. 無効化して問題がないことを確認してから削除します。いきなり削除しないでください。
3. 「外観」→「テーマ」で、使っていないテーマも削除します。バックアップとして一つだけ残す場合は、最新版に更新します。
4. 出所が分からないプラグイン、更新が長期間止まっているプラグイン、ライセンス不明のプラグインは、削除または代替品への移行を検討します。

手順 4：自動更新の設定

1. WordPress 本体のマイナー更新は自動更新にできます。メジャー更新は、事前確認のうえ手動で行うことをおすすめします。
2. プラグインの自動更新は、提供元と互換性を確認できるものだけに限定します。
3. 自動更新を有効にした場合も、定期的にサイトとバックアップを確認してください。

付録 F WordPress の公開設定を見直す

XML-RPC

XML-RPC は、古い外部アプリ連携の仕組みです。使っていない場合は、SiteGuard WP Plugin または Wordfence Security で無効化します。サーバー側で無効化する場合は、ホスティング会社に「xmlrpc.php へのアクセスを 403 にしてください」と依頼します。無効化後に、サイトの通常機能が動くことを確認してください。

readme.html、license.txt、debug.log

これらは公開されていても直ちに攻撃につながるとは限りませんが、バージョンや内部情報の手がかりになります。

1. ホスティングのファイルマネージャーで、WordPress のルートにある `readme.html` と `license.txt` を確認します。削除ではなく、サーバー設定で 403 にする方法がおすすめです。WordPress の更新で戻ることがあります。
2. `wp-content/debug.log` がある場合は、中身を確認し、個人情報や API キーが含まれていないか確認します。含まれている場合は、値を変更し、ファイルを削除します。
3. `wp-config.php` に `WP_DEBUG_LOG` を指定している場合は、本番環境ではログの保存先と公開範囲を見直します。

ユーザー列挙

WordPress の投稿者アーカイブ、REST API、oEmbed からユーザー名の手がかりが得られることがあります。セキュリティプラグインまたは WAF で、`/wp-json/wp/v2/users` や `?author=` への不要なアクセスを制限します。ユーザー名を隠すだけでなく、2 段階認証と試行制限を併用してください。

セキュリティヘッダーと Cookie

不足しているヘッダーは、WordPress のプラグインではなく、ホスティング会社のサーバー設定、CDN、WAF で追加するのが一般的です。WordPress のプラグインで追加する場合は、管理画面や決済画面が壊れないか必ず確認してください。

バックアップと復元の確認

バックアップは、取っただけでは意味がありません。一度テスト環境で復元し、ファイル、データベース、画像、問い合わせ内容が戻ることを確認してください。



画面イメージ：ホスティングのバックアップ画面。実際の画面は契約により異なります。

付録 G PHP の更新：CMS とは別の作業

PHP は、WordPress などの CMS を動かしているサーバー側のプログラムです。CMS の更新だけでは PHP の脆弱性は直りません。2026 年 10 月に公表された php2shell（CVE-2026-109618 / CVE-2026-109619）は、PHP そのものの重大な脆弱性で、修正版は PHP 8.5.12、8.4.27、8.3.36、8.2.35 です。より新しい安定版が提供されている場合は、そちらを優先してください。

項目	このレポートで確認できた内容
公開情報の PHP	8.3.35
推定ホスティング	Kinsta
PHP 変更画面の目安	MyKinsta → 対象サイト → 「Tools」 → 「PHP settings」 → 「Change」
修正版の目安	8.5.12、8.4.27、8.3.36、8.2.35 以降



画面イメージ：ホスティングの PHP 設定画面。実際のメニュー名は契約により異なります。

手順 1：現在の PHP バージョンを確認する

- WordPress の管理画面で「ツール」→「サイトヘルス」→「情報」タブを開きます。
- 「サーバー」の項目を開き、「PHP バージョン」を探します。
- ホスティング会社の管理画面にも「PHP バージョン」「PHP 設定」「MultiPHP Manager」「Select PHP Version」などの項目があります。
- バージョンが表示されない場合は、ホスティング会社のサポートに「現在の PHP バージョンと、php2shell の修正版に更新可能か」を問い合わせます。

手順 2：更新前の準備

1. ホスティング会社の管理画面で、ファイルとデータベースのバックアップを取ります。WordPress を使っている場合も、WordPress のバックアッププラグインだけに頼らず、ホスティング側のバックアップを確認します。
2. 可能ならステージング環境（本番と別のテスト用サイト）を用意します。難しい場合は、アクセスの少ない時間帯に作業します。
3. 使用中のテーマ、プラグイン、決済、問い合わせフォームが、更新後の PHP で動くか、提供元の対応バージョンを確認します。
4. 変更前の PHP バージョンをメモします。問題が起きたときに戻せるようにします。

バックアップ画面の目安: MyKinsta → 対象サイト → 「Backups」

手順 3：ホスティング側で PHP を更新する

このサイトで確認できたホスティングは Kinsta です。次の画面を開きます。

変更画面の目安: MyKinsta → 対象サイト → 「Tools」 → 「PHP settings」 → 「Change」

注意: Kinsta は MyKinsta のサイト単位で PHP を変更します。ステージング環境がある場合は、先にステージングで確認してください。

1. ホスティング会社の管理画面にログインします。
2. 対象ドメインに適用されている現在の PHP を確認し、変更前の値をメモします。
3. 修正版（8.5.12、8.4.27、8.3.36、8.2.35 以降）を選びます。ホスティング会社が提供している最新の安定版を選んでください。
4. 保存または適用を押します。反映まで数分かかることがあります。
5. サイトの管理画面またはホスティング画面で、表示が変わったことを確認します。

手順 4：更新後の確認

1. トップページ、固定ページ、投稿、検索、お問い合わせ、ログイン、決済を順番に確認します。
2. WordPress の管理画面で、PHP の警告やエラーが出ていないか確認します。
3. プラグインの設定画面を開き、保存できるか確認します。
4. 問題があれば、ホスティング側で変更前の PHP バージョンに戻し、使用中の CMS・プラグイン提供元へ互換性を確認します。
5. 更新後、このレポートの再診断を実行し、PHP の所見が消えたことを確認します。

ホスティング会社へそのまま送れる文例

次の文をコピーし、サイト URL と現在の PHP バージョンを埋めて、ホスティング会社のサポートへ送ってください。サイトの管理画面だけでは PHP は変わらないため、この依頼が必要です。

件名：PHP バージョン更新のお願い（CVE-2026-109618 / CVE-2026-109619）

本文：

現在、対象サイト（サイト URL：_____）の PHP が 8.3.35 で動作しています。

PHP の脆弱性 CVE-2026-109618 / CVE-2026-109619 の修正版（8.5.12、8.4.27、8.3.36、8.2.35 以降）へ更新可能でしょうか。

更新前にファイルとデータベースのバックアップを取り、更新後にサイトの管理画面、問い合わせフォーム、決済、ログインが正常に動くことの確認までお願いできますか。

更新後の PHP バージョンと、問題があった場合の戻し方も教えてください。

ホスティング会社が更新しない場合

1. サポートに、CVE-2026-109618 / CVE-2026-109619 の修正版をいつ提供するか確認します。
2. 更新予定がない場合は、別のホスティング会社への移行を検討します。WordPress のファイル、データベース、ドメイン設定、メール設定を移行する必要があります。
3. 一時的な緩和として WAF が使える場合がありますが、WAF は PHP の更新の代わりではありません。
4. 深刻な影響が想定される場合は、専門家に相談し、公開を一時停止するかどうか判断してください。

付録 H 検出された所見ごとの修正手順

この節では、検出された所見を一つずつ、専門用語をできるだけ避けて説明します。レポートの F 番号と照合しながら読んでください。すべての所見を一度に直す必要はありません。重大度の高いものから順に、バックアップ、変更、確認の順に進めてください。サイトの管理画面（WordPress など）とホスティング管理画面の両方にログインできる前提で書いています。片方しかない場合は、前の「このレポートが前提にしているアクセス権」を確認してください。

F-01 Outdated PHP version

重大 確度: 高 作業目安: 20 分

観測された内容: PHP 8.3.35 was exposed and is below a release that fixes CVE-2026-109618 / CVE-2026-109619 (php2shell). Update to PHP 8.5.12, 8.4.27, 8.3.36, or 8.2.35. **この所見の意味:** サーバー側の PHP が古い、または修正版ではない可能性があります。WordPress の更新だけでは解決せず、ホスティング側の PHP 更新が必要です。 **最初に開く画面:** ホスティング管理画面で PHP を修正版へ変更 **修正手順:**

1. WordPress の「ツール」→「サイトヘルス」→「情報」→「サーバー」で現在の PHP バージョンを確認します（公開情報からの検出値: 8.3.35）。
2. ホスティング管理画面の MyKinsta → 対象サイト → 「Tools」→ 「PHP settings」→ 「Change」を開きます。
3. ファイルとデータベースのバックアップを取り、変更前の PHP バージョンをメモします。
4. 修正版（8.5.12、8.4.27、8.3.36、8.2.35 以降）を選び、保存または適用します。
5. トップページ、固定ページ、検索、問い合わせ、ログイン、決済を確認します。問題があれば変更前の PHP に戻します。
6. 再診断を実行し、PHP 関連の所見が消えたことを確認します。

修正後の確認: サイトの主要ページ、管理画面、ログイン、問い合わせ、決済を確認し、このレポートを再診断してください。 **元に戻す場合:** 作業前のバックアップ、またはホスティング会社のバックアップから復元します。設定変更だけなら、変更前の値をメモに従って戻します。

F-02 XML-RPC endpoint reachable

中 確度: 高 作業目安: 10 分

観測された内容: xmlrpc.php responded; disable it if unused. **この所見の意味:** 外部アプリ連携を使っていない場合、XML-RPC は不要な入口になることがあります。無効化できるか確認してください。 **最初に開く画面:** 使っていないければ XML-RPC を無効化 **修正手順:**

1. XML-RPC を業務で使っているアプリがないか確認します。

2. SiteGuard WP Plugin または Wordfence Security で XML-RPC を無効化します。
3. サーバー側で無効化する場合は、ホスティング会社に「xmlrpc.php へのアクセスを 403 にしてください」と依頼します。
4. サイトの通常機能、外部連携、投稿アプリが動くことを確認します。

修正後の確認: サイトの主要ページ、管理画面、ログイン、問い合わせ、決済を確認し、このレポートを再診断してください。**元に戻す場合:** 作業前のバックアップ、またはホスティング会社のバックアップから復元します。設定変更だけなら、変更前の値をメモに従って戻します。

F-03 Missing Content-Security-Policy

中 確度: 高 作業目安: 20 分

観測された内容: CSP is not set. **この所見の意味:** 公開情報から観測された設定・露出です。実際の影響はサイトの構成によって異なるため、修正前にバックアップと確認を行ってください。**最初に開く画面:** ホスティング画面または CDN でヘッダーを追加**修正手順:**

1. レポートの観測内容に書かれた URL、パラメータ、設定を管理画面またはホスティング画面で確認します。
2. バックアップを取ります。
3. 提供元のドキュメント、またはホスティング会社のサポートに修正方法を確認します。
4. テスト環境、またはアクセスの少ない時間帯に設定を変更します。
5. サイトの主要機能を確認し、再診断で所見が消えたことを確認します。

修正後の確認: サイトの主要ページ、管理画面、ログイン、問い合わせ、決済を確認し、このレポートを再診断してください。**元に戻す場合:** 作業前のバックアップ、またはホスティング会社のバックアップから復元します。設定変更だけなら、変更前の値をメモに従って戻します。

F-04 Outdated WordPress core

中 確度: 中 作業目安: 15 分

観測された内容: WordPress 6.8.2 is older than the current release (6.9). Update WordPress core, themes, and plugins; verify the site after upgrading. **この所見の意味:** WordPress 本体、プラグイン、テーマ、または公開設定に、更新・見直しの余地があります。**最初に開く画面:** ダッシュボード → 更新で WordPress 本体を更新**修正手順:**

1. WordPress、プラグイン、テーマ、PHP のバックアップを取ります。
2. WordPress 管理画面にログインし、「ダッシュボード」→「更新」を開きます。
3. 更新前に「詳細」を開き、PHP の対応バージョンを確認します。
4. 「WordPress 本体を更新」を押し、完了後にトップページと管理画面を確認します。
5. プラグインを一つずつ更新します。重要なプラグインから順番に進め、その都度サイトを確認し

ます。

6. 最後にテーマを更新します。子テーマやカスタマイズがある場合は、親テーマの更新内容も確認します。
7. 再診断を実行し、WordPress 本体の所見が消えたことを確認します。

修正後の確認: サイトの主要ページ、管理画面、ログイン、問い合わせ、決済を確認し、このレポートを再診断してください。**元に戻す場合:** 作業前のバックアップ、またはホスティング会社のバックアップから復元します。設定変更だけなら、変更前の値をメモに従って戻します。

F-05 WordPress detected

情報 確度: 高 作業目安: 10 分

観測された内容: WordPress assets or REST API were observed. **この所見の意味:** WordPress 本体、プラグイン、テーマ、または公開設定に、更新・見直しの余地があります。**最初に開く画面:** 本体・テーマ・プラグインの更新状況を確認**修正手順:**

1. WordPress、プラグイン、テーマ、PHP のバックアップを取ります。
2. 「ダッシュボード」→「更新」で WordPress 本体を更新します。
3. プラグインを一つずつ更新し、その都度サイトを確認します。
4. 使っていないプラグインとテーマを削除し、出所不明のものは代替品に移行します。
5. 更新後に再診断し、バージョン所見が解消したか確認します。

修正後の確認: サイトの主要ページ、管理画面、ログイン、問い合わせ、決済を確認し、このレポートを再診断してください。**元に戻す場合:** 作業前のバックアップ、またはホスティング会社のバックアップから復元します。設定変更だけなら、変更前の値をメモに従って戻します。

F-06 WordPress version detected

情報 確度: 高 作業目安: 10 分

観測された内容: WordPress 6.8.2 was identified from the generator meta tag or a core wp-includes asset. **この所見の意味:** WordPress 本体、プラグイン、テーマ、または公開設定に、更新・見直しの余地があります。**最初に開く画面:** サイトヘルスで最新版か確認**修正手順:**

1. WordPress、プラグイン、テーマ、PHP のバックアップを取ります。
2. 「ダッシュボード」→「更新」で WordPress 本体を更新します。
3. プラグインを一つずつ更新し、その都度サイトを確認します。
4. 使っていないプラグインとテーマを削除し、出所不明のものは代替品に移行します。
5. 更新後に再診断し、バージョン所見が解消したか確認します。

修正後の確認: サイトの主要ページ、管理画面、ログイン、問い合わせ、決済を確認し、このレポートを

再診断してください。**元に戻す場合:** 作業前のバックアップ、またはホスティング会社のバックアップから復元します。設定変更だけなら、変更前の値をメモに従って戻します。

F-07 WordPress plugin detected: contact-form-7

情報 確度: 高 作業目安: 15 分

観測された内容: Plugin contact-form-7 assets were observed with version 5.8.1. Public asset versions can be stale or manipulated; verify the installed version in the admin area. **この所見の意味:** WordPress 本体、プラグイン、テーマ、または公開設定に、更新・見直しの余地があります。**最初に開く画面:** プラグイン → インストール済みプラグインで更新・削除**修正手順:**

1. WordPress 管理画面 → 「プラグイン」 → 「インストール済みプラグイン」 → 「contact-form-7」を探します。
2. バックアップを取り、更新前にプラグインの提供元と対応 WordPress バージョンを確認します。
3. 「更新があります」と表示されたら「今すぐ更新」を押します。
4. 更新が表示されない場合は、配布元の最終更新日と対応バージョンを確認します。長期間更新がない場合は、代替プラグインへの移行を検討します。
5. 使っていないプラグインは、無効化して問題がないことを確認してから削除します。
6. 問い合わせフォーム、決済、表示が正常に動くことを確認し、再診断を実行します。

修正後の確認: サイトの主要ページ、管理画面、ログイン、問い合わせ、決済を確認し、このレポートを再診断してください。**元に戻す場合:** 作業前のバックアップ、またはホスティング会社のバックアップから復元します。設定変更だけなら、変更前の値をメモに従って戻します。

F-08 WordPress theme detected: twentytwentyfour

情報 確度: 高 作業目安: 10 分

観測された内容: Theme twentytwentyfour assets were observed with version 1.2. Public asset versions can be stale or manipulated; verify the installed version in the admin area. **この所見の意味:** WordPress 本体、プラグイン、テーマ、または公開設定に、更新・見直しの余地があります。**最初に開く画面:** 外観 → テーマで更新・削除**修正手順:**

1. WordPress 管理画面 → 「外観」 → 「テーマ」を開きます。
2. バックアップを取り、使用中のテーマに更新があるか確認します。
3. 更新がある場合は「今すぐ更新」を押します。子テーマを使っている場合も親テーマの更新内容を確認します。
4. 使っていないテーマは削除します。バックアップとして残す場合も、最新版に更新します。
5. トップページ、固定ページ、投稿、スマートフォン表示を確認し、再診断を実行します。

修正後の確認: サイトの主要ページ、管理画面、ログイン、問い合わせ、決済を確認し、このレポートを

再診断してください。**元に戻す場合:** 作業前のバックアップ、またはホスティング会社のバックアップから復元します。設定変更だけなら、変更前の値をメモに従って戻します。

F-09 WordPress login page reachable

情報 確度: 高 作業目安: 30 分

観測された内容: The standard wp-login.php page is publicly reachable. Protect it with strong passwords, two-factor authentication, login rate limiting, and updates. **この所見の意味:** WordPress のログイン画面は正常な機能ですが、自動的なパスワード試行の対象になります。2 段階認証と試行回数の制限で守る必要があります。**最初に開く画面:** 2 段階認証とログイン試行制限を設定**修正手順:**

1. 「ユーザー」→「ユーザー一覧」で管理者を確認し、使っていない管理者を整理します。
2. SiteGuard WP Plugin または Wordfence Security で 2 段階認証を有効にし、回復コードを保存します。
3. ログイン試行回数の制限を 5 回失敗・15 分ロック程度に設定します。
4. XML-RPC を無効化し、必要ならログイン URL 変更も設定します。
5. シークレットウィンドウでログイン、2 段階認証、ログアウト、再ログインを確認します。

修正後の確認: サイトの主要ページ、管理画面、ログイン、問い合わせ、決済を確認し、このレポートを再診断してください。**元に戻す場合:** 作業前のバックアップ、またはホスティング会社のバックアップから復元します。設定変更だけなら、変更前の値をメモに従って戻します。

F-10 Hosting / server fingerprint

情報 確度: 高 作業目安: なし

観測された内容: Server: nginx. Hosting hint: Kinsta. This is a passive response-header fingerprint. A CDN, reverse proxy, or WAF can hide the origin hosting provider; do not treat it as proof of the physical server. **この所見の意味:** 公開情報から観測された設定・露出です。実際の影響はサイトの構成によって異なるため、修正前にバックアップと確認を行ってください。**最初に開く画面:** 情報のみ。作業は不要**修正手順:**

1. この項目はホスティングやサーバーの手がかりであり、それ自体は脆弱性ではありません。
2. PHP の更新や 403 設定を行うときの管理画面を探すために使います。
3. CDN が表示されている場合、PHP を動かしている元のホスティング会社は別です。
4. ホスティング会社が分からない場合は、請求書、契約メール、またはドメインの DNS 設定を確認します。

修正後の確認: サイトの主要ページ、管理画面、ログイン、問い合わせ、決済を確認し、このレポートを再診断してください。**元に戻す場合:** 作業前のバックアップ、またはホスティング会社のバックアップから復元します。設定変更だけなら、変更前の値をメモに従って戻します。

付録Ⅰ 修正後の確認チェックリスト

1. バックアップから復元できることを確認しましたか。
2. CMS 本体、プラグイン、テーマ、PHP のバージョンを確認しましたか。
3. サイトのログイン画面で、2 段階認証と試行回数の制限が有効ですか。
4. 一般の閲覧者が管理画面に入れないことを確認しましたか。
5. トップページ、固定ページ、投稿、検索、お問い合わせ、決済が正常に動きますか。
6. セキュリティヘッダー、Cookie、CORS の変更で、埋め込みコンテンツや外部連携が壊れていませんか。
7. 不審な管理者、プラグイン、投稿の改変がありませんか。
8. PHP を更新した場合、ホスティング管理画面とサイトの管理画面の両方で新しいバージョンを確認しましたか。
9. このレポートを再診断し、修正した所見が消えたことを確認しましたか。

対象ホスト: `example.jp`

修正作業の記録（日時、変更した画面、変更前の値、変更後の値、確認結果）を残してください。次回の診断や、ホスティング会社・制作会社への引き継ぎに役立ちます。

管理画面に入れない、または作業に不安がある場合は、このレポートの F 番号と該当する章を、サイト管理者またはホスティング会社へ渡してください。自分で全部やる必要はありません。ただし、パスワードや API キーをレポートに書き込まないでください。