サンプル会社公式サイト

WordPress セキュリティ診断報告書（サンプル）

報告日　2026 年 11 月　版 1.0

株式会社 ONE WEB

このサンプルについて

本書は、当社の診断報告書の構成と記載の深さをご紹介するためのサンプルです。会社名、環境、ファイル名、指摘内容は、実在のサイトの診断をもとに一般化した架空のものです。実際の報告書は、お客様のサイトの構成・サーバー・運用に合わせて作成します。

診断で見つかった指摘事項 F-01〜06 と改善事項 I-01〜03 への対策、および設定ファイルの直接アクセス遮断を、テスト環境で確認したうえで本番環境へ反映しました。両環境でサイト内検索と、問い合わせ・資料請求フォームの送信を確認しています。

第 1〜6 章に診断時の所見と対応計画、第 7 章に実施した対策、第 8 章にテスト・本番での確認結果を記載しています。

診断の概要

項目	内容
対象	サンプル会社公式サイトの WordPress データ、レンタルサーバー上のテスト環境と本番環境
重点対象	稼働中のテーマとフォーム処理。指摘箇所は、原則としてテーマからの相対表記で報告します（本サンプルでは省略）。
方法	静的コード解析、設定確認、対策反映後の HTTP 応答・フォーム送信・非公開ログの確認
実施期間	診断　約 1 週間／反映・確認　1 日
対象外	侵入試験、WAF の実効性評価、プラグインの網羅的な脆弱性照合

指摘事項の一覧

ID	重要度	指摘事項	確認状況
F-01	高	検索欄の反射型 XSS	コード上確認
F-02	中	フォームの CSRF 検証不備	コード上確認
F-03	低	エラー応答での内部情報の表示	コード上確認
F-04	条件付き	権限検証のないメタ更新 AJAX	読み込み無効
F-05	条件付き	ホスト名に依存する URL 生成・転送	設定・コード確認
F-06	条件付き	PHP エラーの画面表示設定	設定確認
I-01〜03	改善	TLS 検証、旧コピー、不要ファイル	ファイル確認

重要度と確認状況は診断時点の評価です。反映後の結果は第 7 章と第 8 章を参照してください。「条件付き」は、特定の条件がそろった場合にだけ影響が出る指摘です。

1 優先して修正する問題

F-01 検索欄の反射型 XSS　重要度 高

検索語を、HTML の入力欄の属性値へそのまま出力しています。細工した URL を閲覧者が開いた場合、ページ内で意図しないスクリプトが実行される可能性があります。共通ヘッダーや検索ブロックを使用するページが影響対象です。

```
value="<?php echo isset($_GET['s']) ? $_GET['s'] : '' ?>"
```

原因は、外部入力を HTML 属性用にエスケープしていないことです。WordPress が入力に付加するバックスラッシュは、HTML 属性の引用符を安全にする対策にはなりません。

対応方針：入力が文字列であることを確認し、wp_unslash() で整えた後、出力時に esc_attr() を適用します。同様の実装が旧コピーなどに残っていないかも確認します。

```
$search_value = isset($_GET['s']) && is_string($_GET['s'])
  ? wp_unslash($_GET['s']) : '';
// 属性値を出力する箇所
value="<?php echo esc_attr($search_value); ?>"
```

確認方法：引用符や山括弧を含む検索語が入力欄に文字として表示され、HTML の構造が変わらないことを確認します。

F-02 フォームの CSRF 検証不備 重要度 中

フォームの正規操作を確認するトークン検証が、条件式の組み方により省略されます。外部からの不正なフォーム操作や迷惑送信につながる可能性があります。問い合わせ・資料請求の確認ページが該当し、送信ページも確認ページの処理を読み込む構成です。

操作名が空でない場合、AND 条件の最初が偽となって後続のトークン検証が実行されません。また、不正時のリダイレクトの後に終了処理がありません。

対応方針：確認・送信の各段階で、HTTP メソッド、許可する操作、トークンを個別に検証し、不正時は必ず処理を終了します。トークンは検証後に消費する実装のため、段階ごとの再発行も設計します。

確認方法：トークンの欠落・不正・再利用を拒否し、通常の確認から送信までの操作が完了することを、テスト用の送信先で確認します。Cookie 設定や reCAPTCHA の設定が未確認の場合、実際の不正送信が成立するかどうかは断定しません。

2 情報表示と未使用コードの問題

F-03 エラー応答での内部情報の表示 重要度 低

問い合わせ・資料請求の送信処理で例外が発生すると、サーバー内の PHP ファイルの絶対パスと行番号を応答に表示します。攻撃者によるサーバー構成の調査に利用される可能性があります。

```
$returnE .= 'File: ' . $e->getFile() . ' at line ' . $e->getLine();
die($returnE);
```

WP_DEBUG=false でも、この独自の画面出力は抑止されません。利用者には一般的なエラーメッセージだけを表示し、詳細は公開しないログへ記録してください。

確認方法：テスト環境で入力不足などのエラーを起こし、応答に内部パス・行番号・認証情報が含まれないことを確認します。

F-04 権限検証のないメタ更新 AJAX 条件付き

投稿などの付加情報を変更する AJAX 処理に、未ログインでの呼び出しを登録するコードがあります。nonce 検証、対象を編集する権限の確認、更新可能なフィールド名の制限がありません。読み込まれた場合、第三者が指定した対象のメタ情報を真偽値に変更できる実装です。

ただし、このコードの読み込み行はコメントアウトされており、稼働中のエンドポイントとしては扱いません。未収録の外部コードからの読み込みは未確認です。

対応方針：使用しない場合は撤去します。再利用する場合は、未認証用の登録を削除し、対象ごとの編集権限と nonce を検証したうえで、更新可能なフィールドを許可リストに限定します。

確認方法：非ログイン・権限不足・不正な nonce・許可されていないフィールド名による更新が、すべて拒否されることを確認します。

3 保守と設定に関する改善事項

I-01 TLS 証明書検証を無効にする補助関数

HTTPS 取得用の補助関数が、証明書の検証を無効（CURLOPT_SSL_VERIFYPEER=false）にしています。使われている場合、通信相手の証明書チェーンを検証せず、中間者による応答改変の余地が生じます。テーマ内では定義以外の呼び出しを確認できませんでした。未使用であれば撤去し、使用する場合は証明書検証を有効化します。WordPress HTTP API の利用も選択肢です。

I-02 旧テーマと日付付きコピーの残存

旧テーマのディレクトリや、現行テーマ内の日付付きコピー（*_日付.php など）が残っています。これらの存在だけで侵入可能とは判定しませんが、古いコードの誤使用や保守漏れの原因となります。使用状況を確認し、不要なコピーは公開ディレクトリから撤去して、バージョン管理または公開領域外で保管してください。

I-03 不要な管理用メタファイル

WordPress データ内に、macOS が自動生成する .DS_Store が多数残っています。配信される設定ではファイル名などの情報が得られる可能性があります。不要ファイルを削除し、デプロイ対象から除外します。

コード上で確認できた既存の対策

確認した内容	評価と確認上の留意点
WP_DEBUG=false	デバッグ表示を抑制する設定。ただし独自出力は別途対策が必要。
DISALLOW_FILE_EDIT=true	管理画面からのテーマ・プラグインのファイル編集を禁止する設定あり。
自動更新の方針	本体のマイナー更新とプラグインの自動更新を許可するコードあり。実行可否は運用設定次第。
フォームの保護処理	ハニーポット、段階確認、メールアドレスの改行拒否あり。reCAPTCHA は設定時のみ実行。
セキュリティ用プラグイン	関連ファイルあり。有効化状態・実効性は別途確認。

補足：送信間隔のチェックは、利用者が送る時刻値とセッション値が一致する場合のみ短時間送信を拒否します。強い頻度制限とは評価せず、サーバー側の時刻と送信履歴を基準にした制限へ見直します。

4 公開ルートとアプリケーション設定

F-05 ホスト名に依存する URL 生成と転送 条件付き

HTTPS への転送先に受信した Host を用い、www 付きのホスト名も固定の許可リストを使わずに書き換えています。アプリケーションの設定ファイルも、HTTP_HOST と転送プロトコルの情報からサイトの基準 URL を組み立て

ます。

この基準 URL は、問い合わせフォームの送信先などに使われます。想定外の Host がアプリまで届く構成では、別ホストを指す転送先やリンクが生成されるおそれがあります。仮想ホストや上流プロキシで拒否される場合もあり、実際に成立するかは環境次第です。

対応方針：環境ごとに正規ホストを固定し、想定外の Host を入口で拒否します。転送プロトコルのヘッダーは、信頼できるプロキシから受ける場合に限定します。URL を HTML へ出力するときは esc_url() を適用します。

F-06 PHP エラーの画面表示設定 条件付き

PHP の設定で display_errors=On となっています。有効な環境では、WordPress の初期化前や WordPress を通らない PHP 処理で、エラー詳細が利用者に表示される可能性があります。実効値はサイトヘルスなどで確認します。本番では画面表示を無効化し、非公開ログへの記録を維持してください。F-03 の独自出力は、PHP 設定とは別に修正します。

設定ファイルの配置と保護

アプリケーション設定ファイルが公開ルートの直下にあり、公開 URL から直接リクエストできる配置でした。直接アクセスを拒否する設定も、ファイル自体に実行を停止する処理も見当たりません。公開領域外へ移すか、直接リクエストを拒否してください。

補足：X-Frame-Options は DENY を送信しています。Content-Security-Policy の送信処理は無効、reCAPTCHA のキーは未設定、SMTP は無効でした。上流でのヘッダー付与と実環境のフォーム設定は、別途確認が必要です。

5 WordPress とプラグインの構成

本番の管理画面で、WordPress 本体とプラグインの状態を確認しました。プラグインはすべて自動更新が有効で、構成は次のとおりです（サンプルのため、プラグイン名は種別に置き換えています）。

プラグインの種別	件数	状態
カスタムフィールド・エディタ拡張	2	有効
スパム対策	1	有効
サイト保護（ログイン保護など）	1	有効
WAF・マルウェアスキャン	2	停止
画像最適化・多言語対応・ページ送り・サイトマップ・投稿の並び替え・複製	6	有効

WAF の稼働状況

管理画面上では WAF プラグインが停止中です。一方、PHP の設定には、起動時に WAF を読み込む指定（auto_prepend_file）が残っています。実効状態は、PHP 設定、読み込み先ファイルの存在、WAF 側の有効設定

の組み合わせに依存します。

WAF の保護は、実効状態が確認できるまで評価に加えません。手元のバージョンと本番の表示版が異なっていたため、バージョンの整合も併せて確認します。サーバー側の WAF が提供される場合は、別途、稼働状態を確認してください。

プラグインの自動更新の成否、公式ファイルとの一致、既知の脆弱性との照合は、確認範囲外です。

6 診断時の対応計画と確認範囲

推奨する対応順序

優先	対応内容	完了の確認基準
1	F-01 検索欄の出力修正	引用符・山括弧を含む検索語でも HTML 構造が変わらない。
2	F-02 フォームの検証修正	不正トークンを拒否し、正規の確認・送信が完了する。
3	F-05 ホスト名と転送先の検証	想定外のホストを拒否し、正規ホストの検索とフォームが動く。
4	F-03・06 エラー表示の見直し	エラー応答から内部詳細を除き、非公開ログへの記録を確認する。
5	F-04 と I-01〜03 の整理	不要なコードと旧コピーを整理し、必要な処理を安全化する。

この順序で、ローカル環境とテスト環境で確認してから本番へ反映します。

診断の限界

当初の診断は、静的レビューと提供資料の確認を対象としました。本書では、実環境での機能確認と非公開ログの確認を追加しています。侵入試験、改ざん調査、公式チェックサムの照合、最新の脆弱性情報との照合、WAF の実効性評価は対象外です。

7 実施した対策

各対策をテスト環境で確認し、本番へ反映しました。反映前に、変更対象と退避対象のバックアップを取り、ファイルの照合を行っています。

項目	実施内容
F-01 検索欄の反射型 XSS	共通ヘッダーと検索ブロックの 3 箇所で、検索語を文字列として受け取り、HTML 属性向けにエスケープして出力するよう修正しました。
F-02 フォームの CSRF	フォームと処理段階ごとに、使い切りのトークンを発行します。確認と送信では、POST、操作名、トークンを検証し、送信間隔の判定にはサーバーに記録した確認時刻を使います。

F-03 フォームのエラー表示	利用者には共通のエラー案内を表示します。エラー理由・内部ファイルパス・行番号は、公開ルート外の PHP ログへ記録します。
F-04 メタ更新 AJAX	読み込みが無効だったメタ更新処理と、管理画面の呼び出しコードを撤去しました。
F-05 ホスト名と転送先	環境ごとに正規の公開 URL と HTTPS 転送先を固定しました。許可リストにないホスト名でのアクセスを拒否し、受信した転送ヘッダーを URL 生成に使う処理を除去しました。
F-06 PHP のエラー表示	PHP エラーの画面表示を無効にし、公開ルート外のログを指定しました。本番とテストで共有されていた設定ファイルを分離し、ログ先を環境別に設定しました。
I-01 TLS 検証	TLS 証明書の検証を無効にしていた未使用の補助関数を撤去しました。
I-02 旧テーマと日付付きコピー	両環境の旧テーマと、本番に残っていた日付付きコピーを公開ルート外へ退避しました。
I-03 不要なメタファイル	公開領域から .DS_Store を退避しました。
設定ファイルの保護	Web サーバーで直接アクセスを拒否し、PHP 側にも直接実行を終了する判定を追加しました。WordPress から設定ファイルを読み込む経路の動作を確認しています。

8 テスト環境と本番環境の確認結果

テスト環境と本番環境で確認しました。フォームは指定の検証用メールアドレスで試験し、試験後に通常の通知設定へ戻しています。

確認項目	テスト環境	本番環境
サイト内検索	検索結果を表示。引用符や山括弧を含む検索語も、入力欄に文字として表示。	同じ検索条件で結果を表示。検索欄 3 箇所で、文字として表示されることを確認。
問い合わせと資料請求	両フォームで確認から送信完了画面まで進み、利用者向け・管理者向けの計 4 通を受信。	同じ操作で、計 4 通を受信。
CSRF とフォームエラー	トークンの欠落・不正・再利用は HTTP 403。入力不備は HTTP 400 となり、応答に内部パスや行番号は出ない。	同じ条件で HTTP 403 と 400 を確認。エラーの詳細は非公開ログに記録。
ホスト名と HTTPS 転送	想定外ホストを拒否。正規ホストの HTTP アクセスは、検索条件を保持して正規の HTTPS URL へ転送。	想定外ホストを拒否。HTTP と www からのアクセスも、検索条件を保持して正規の HTTPS URL へ転送。
PHP エラーとログ	PHP 警告は画面に出ず、フォーム例外とともに公開ルート外のログに記録。	同様に、公開ルート外の本番用ログに記録。

旧コードと不要ファイル	旧 AJAX アクションの未登録と、補助関数の撤去を確認。公開領域に旧テーマと .DS_Store が残っていない。	同様に確認。日付付きコピーも残っていない。
設定ファイルの直接アクセス	HTTP 403。WordPress からの読み込みは正常。	HTTP 403。WordPress からの読み込みは正常。

確認時に見つかった設定差

テスト環境でフォームの拒否応答が HTTP 200 になる挙動を確認したため、WordPress のステータス設定を使うよう修正しました。修正後に、両環境で HTTP 403 と 400 を確認しています。本番の PHP ログは、設定ファイルの分離後に、本番用ファイルへの記録を確認しました。

両環境で reCAPTCHA のキーが未設定だったため、reCAPTCHA を通す経路は確認対象に含めていません。