実施事例

WordPress サイトの脆弱性診断と是正

当社のコーポレートサイト（外部の制作会社が制作）で診断により見つかった 13 件の問題と、その日のうちに完了した是正

対象	当社のコーポレートサイト（WordPress・外部の制作会社が制作・公開から約 3 年）
実施日	2026 年 10 月 20 日
検出	診断で 13 件、是正作業中に 1 件、本番反映後の確認で 2 件
結果	当日中にすべて是正・動作確認まで完了

Mana 株式会社

沖縄県石垣市　／　サーバー・Web セキュリティ診断

1. この事例の概要

外部の制作会社に発注し、公開から約 3 年が経過した当社のコーポレートサイトを診断しました。見た目も動作も問題はなく、当社も不具合を感じていない状態でした。

診断の結果、閲覧しただけでは分からない 13 件の問題が見つかりました。うち 2 件は、放置すると会社の信用に直結するものでした。

> **最も重かった 2 件**
>
> ① メール送信用のパスワードが、プログラムの中にそのまま書かれていた。制作データを受け取った人は全員、このパスワードを知り得る状態でした。
>
> ② お問い合わせフォームの送信プログラムが、誰でも直接呼び出せる状態だった。会社のドメイン名で、任意の相手に任意の文面を送れてしまいます。

受領から完了まで、約 50 分

経過	工程	内容
0 分	受領	診断結果とサイトのプログラム一式を受領
10 分	是正と検証	修正版を作成し、複製環境で試験。差分と反映手順書を添えて納品
—	本番反映	修正版を本番に差し替え
36 分	反映後の確認	外部から確認し、古いファイルの残存を検出
47 分	障害対応	フォームが送信できない原因を特定し、解消

※ 経過時間は当社の作業の記録です。本番への差し替え作業の時間は含みません。

2. なぜ 3 年間、誰も気づかなかったのか

今回の問題は、どれもサイトを見ているだけでは分かりません。理由は 3 つあります。

表示にはまったく影響しない

パスワードが書かれていても、フォームが悪用できる状態でも、ページは正常に表示され、メールも届きます。不具合として表面化しないため、気づくきっかけがありません。

制作会社の仕事の範囲に入っていない

制作の契約は通常「指定どおりに作る」ことが範囲で、安全性の検査は含まれません。確認する人がいなかった、ということです。

一般的なチェックツールでは重い問題ほど出てこない

WordPress 向けの検査ツールの多くは「既製の部品が古くないか」を調べるものです。今回の重い 2 件は制作会社が独自に書いた部分にあり、この方式では見つかりません。**同じサイトに一般的なコード規約チェッカーをかけると 224 件の指摘が出ますが、重大な 2 件には実質的に到達しません。**

3. 見つかった問題の一覧

危険度は、悪用のしやすさと、起きた場合の影響の大きさから当社が判定したものです。

危険度	内容	起こりうること
緊急	メール送信用のパスワードがプログラムに直接書かれている	制作データを見た人は誰でもメールアカウントを使える。送信元を偽った請求メールなどに悪用される
緊急	お問い合わせの送信プログラムを誰でも直接呼び出せる	会社のドメイン名で大量の迷惑メールを送られ、ドメインが拒否リストに載る。取引先にメールが届かなくなる
高	バックアップファイルがサーバーに置かれたまま	プログラムの中身を誰でも読める。パスワードの発見にもつながる
高	記事の設定欄の値を確認せずファイルとして読み込んでいる	編集者権限の利用者が、サーバー上の任意のファイルを動かせる
高	保存された値をそのままページに出力している	投稿者権限の利用者が、閲覧者のブラウザで不正なプログラムを動かせる
中	メール送信のデバッグ出力が有効になっている	メールサーバーとのやり取りが訪問者のブラウザに返る。攻撃の手がかりを与える
中	お問い合わせ内容の一部が文字化けする	記号を含むお問い合わせが正しく読めない。商談の取りこぼしにつながる
中	セキュリティ系プラグインが機能しない作りになっている	対策用のプラグインを入れても効果が出ない。入れたつもりで無防備になる
中	固定ページを 1 つ削除すると全ページが表示できなくなる	担当者の操作ミスでサイト全体が停止する
低	転送処理のあとも処理が続いている	転送先のページに不要な内容が混ざる
低	メールの送信日時が日本時間になっていない	問い合わせの受信時刻がずれて記録される
低	画面上の英語表記に綴りの誤りがある	会社の印象を損なう
低	別案件のコメントがプログラム内に残っている	制作が使い回しであることが読み取れる

是正作業中に見つかった不具合（1 件）

修正のためプログラム全体を読む過程で、管理画面の不具合が 1 件見つかりました。一部の編集画面で、表示順序とリンク URL の入力欄が表示されない状態でした。設定名に余分な空白が 1 文字入っていたことが原因です。

当社も「そういう仕様」と思って使い続けていた箇所で、診断の対象には含めていませんでした。同時に修正しています。

4. 重大な 2 件が、実際に何を招くか

① パスワードがプログラムに書かれていた

メール送信に使うアカウントのパスワードが、プログラムの中に文字としてそのまま書かれていました。

- 制作会社、その外注先、過去にデータを受け取った業者など、関わった全員が知り得る状態
- バックアップファイルにも同じものが含まれ、サーバー上から誰でも読める状態
- このアカウントを使われると、会社の正規のメールアドレスから、取引先に偽の請求書を送ることができる

送信元が本物であるため、受け取った側が偽物と見抜くのは困難です。

② 送信プログラムを誰でも呼び出せた

お問い合わせフォームの送信プログラムに、「自社のサイトから送られたものか」を確認する仕組みがありませんでした。送信回数の制限もなく、宛先も送信者が自由に指定できる作りでした。

起きること	第三者が、会社のサーバーから、任意の相手に任意の文面のメールを送れる
直接の被害	迷惑メールの送信元として、ドメインが拒否リストに登録される
その後	取引先に自社のメールが届かなくなる。解除には時間がかかり、その間の業務に影響が出る

是正の前に、パスワードの変更をお願いしています

プログラムに書かれていたパスワードは、制作データを受け取った人なら誰でも読める状態にありました。誰が見たかを後から確かめる手立てはありません。

そのため当社は、こうしたパスワードを「すでに漏れたもの」として扱います。プログラムの修正より先に、パスワードそのものの変更をお願いし、変更後の値で動作を確認する順序で進めます。コードを直しても、古いパスワードが有効なままでは危険は残ります。

5. 是正と、その検証

検出して終わりにはしません。修正版を作成し、本番と同じ構成を複製した環境で、実際に動かして確認してから納品しています。

主な修正内容

- パスワードをプログラムから分離し、サーバーの設定ファイルへ移動
- 送信処理を WordPress の正規の受け口に移し、使い捨てトークンによる確認を追加
- 送信回数の上限を設定（同一の送信元・同一の宛先・サイト全体の 3 段階）
- 入力内容の検査を追加（メールアドレスの形式、選択肢の照合、文字数の上限など）
- 自動返信メールから自由記述欄を除外し、第三者への文面送信に使えないよう変更
- 画面に出力する値をすべて無害化。設定値は実在するファイルのみ読み込むよう制限
- 不要なバックアップファイルと、重複していたライブラリを削除

複製環境での試験（すべて期待どおりの結果）

試験	結果
不正な送信リクエスト（6 種類）	すべて拒否。トークンなし、他サイトからの送信、宛先の改ざん、選択肢外の値などを確認
送信回数の上限	3 段階のうち 2 つを実際に発動させ、遮断を確認
正常な送信	ブラウザを自動操作して入力から完了まで実施。メール 2 通の文面を確認
文字化けの解消	記号を含む文面が正しく届くことを確認
管理画面の保存処理	不正な値とトークンなしの保存が拒否されることを確認
設定値の悪用	サーバー上の別ファイルを指定しても読み込まれないことを確認
全ページの表示	エラー・警告ともに 0 件

納品物は、差し替え用の一式・修正前後の差分・反映手順書の 3 点です。差分をお渡しすることで、どこをどう変えたかを制作会社や社内の担当者が確認できます。

6. 本番反映後の確認で、さらに 2 件

修正版を納品した時点では終わりません。本番サーバーに反映されたあと、外部から実際に確認します。この工程で 2 件の問題が見つかりました。

> **反映後の確認で見つかったこと**
>
> ① 古いテーマのフォルダがサーバーに残っていた。新しいテーマは正しく動いていましたが、古い方のバックアップファイルが外部から読める状態のままでした。使われていないファイルでも、URL を直接開けば中身は読めます。
>
> ② お問い合わせフォームが送信できなくなっていた。画面には「送信エラー」としか出ず、原因が分からない状態でした。

② の原因特定

訪問者の画面に詳しい理由を出さないのは、攻撃者に手がかりを与えないための設計です。そのぶん、運営者にも原因が見えません。

そこで一時的に診断用の設定を有効にし、送信を 1 回試しました。返ってきたのは「認証できませんでした」という応答で、接続と暗号化は成功し、ログインの段階で止まっていることが分かりました。設定したパスワードが一致していないと特定でき、設定を修正して解消しました。

報告から原因の特定まで、約 10 分でした。

> **この工程がない場合に起きること**
>
> 古いファイルは残ったままになり、是正の効果が半減します。
>
> お問い合わせフォームは「送信エラー」のまま放置され、その間の問い合わせがすべて失われます。しかも運営者は、フォームが壊れていること自体に気づきません。

7. この事例から言えること

制作から数年経ったサイトは、一度見ておく価値があります

今回のサイトは、特別に作りが悪かったわけではありません。公開時点では一般的だった書き方が、現在の基準では問題になっている箇所が含まれていた、というものです。同じ構造のサイトは多数あります。

「動いている」ことは、安全であることを意味しません

今回の問題の大半は、表示や動作に影響していませんでした。不具合が出ていないサイトほど、確認されないまま時間が経ちます。

検出だけでは、リスクは減りません

問題の一覧を受け取っても、直せなければ状況は変わりません。当社は、検出・修正・検証・反映後の確認までを一続きで行います。今回も、修正版の納品で終えていれば、古いファイルの残存とフォームの停止は見逃されていました。

当社の診断でお渡しするもの

診断報告書	見つかった問題、危険度、起こりうること、対処方法
修正版の一式	そのまま差し替えられる形式
修正前後の差分	変更箇所の一覧。制作会社や社内での確認に使えます
反映手順書	反映の順序、動作確認の方法、問題が起きた場合の対処
反映後の確認	外部からの確認と、問題があった場合の原因特定

お問い合わせ

サーバー・Web セキュリティの診断と保守

Mana 株式会社

〒907-0453　沖縄県石垣市川平 973-12

TEL：050-1754-3500

担当：尾﨑 秀海

2000 年よりネットワークエンジニアとしてサーバーの構築・運用に従事。現在は実務経験と AI による解析を組み合わせ、中小企業の Web サイトとサーバーの安全性を診断しています。