



滋賀県警察

サイバーセキュリティ海賀

サイバー犯罪からあなたを守るセキュリティ情報をお届けします。

R8年度 No.19

セキュリティ注意喚起

WordPressを御利用の事業者様へ

Webサイトの乗っ取り被害を防ぐため、至急バージョンを御確認ください

■概要：世界規模で深刻な攻撃が展開されており、国内においてもサイバー攻撃が観測されています。

現在、多くの事業者のWebサイトで利用されているホームページ作成システム(CMS:コンテンツマネジメントシステム)「WordPress(ワードプレス)」において、**認証なしで外部からサイトを乗っ取られる極めて深刻な脆弱性(CVE-2026-60137、CVE-2026-60303、通称「WP2Shell」)**が確認されています。

放置すると「**不正な管理者の追加**」、「**ホームページの改ざん**」、「**訪問者を詐欺サイトへ誘導**」、「**ウイルスのばらまき元**」などの被害に遭うおそれがあります。

自社のWebサイトを守るための【今すぐ行うべき3つの対策】

対策1 WordPressを最新バージョンへアップデート（最優先）

すでに開発元から修正版が提供されています。管理画面で最新版への更新を行ってください。

対策バージョン WordPress 6.9.0～6.9.4 ⇒ **対応** 6.9.5以上に更新

対策バージョン WordPress 7.0.0～7.0.1 ⇒ **対応** 7.0.2以上に更新

- ※ 自動更新を設定している場合でも、正常に更新が完了しているか、必ず管理画面で御確認ください。
- ※ 対策バージョン以外のバージョンの場合は、本件の脆弱性の対象外となります。

対策2 管理ユーザーに「覚えのないアカウント」がないか確認

すでに攻撃を受け、不正な管理者が作成されている可能性があります。

- ☐ 管理画面の「ユーザー一覧」を確認し、心当たりのない管理者権限（Administrator）のアカウントが存在しないか確認する。
- ※ 「対策1」で該当バージョンを利用されている場合は、「対策2」、「対策3」を確認してください。

対策3 「身に覚えのないプラグイン」が追加されていないか確認

攻撃者によってバックドア(不正アクセスの抜け道)が仕掛けられている場合があります。

- ☐ 管理画面の「プラグイン一覧」を確認し、自社で導入した覚えのないプラグインが有効化されていないか確認する。

💡 自社で操作・確認が難しい場合

Webサイトの制作会社や保守・管理を担当している委託先ベンダーに情報共有していただき、「WordPressの最新パッチの適用と不正アクセスの有無の点検」を御依頼ください。

万が一、改ざんや不審な挙動を発見した場合は、Webサイトの停止等の応急措置を行うとともに、最寄りの警察署へ御相談ください。



←X

滋賀県警察本部警備部外事課 TEL : 077-522-1231（代表）

<https://www.pref.shiga.lg.jp/police/seikatu/304409/index.html>

県警Webページ→

