WordPressセキュリティ・脆弱性診断評価レポート

評価日	
対象サイト	

■お問い合わせ
株式会社ツクイ・インターナショナル
Web制作事業部 WP Plus
E-mail： info@wpplus.jp
URL： https://wpplus.jp

■サマリー

セキュリティ・脆弱性診断結果サマリー	スコア（0～100）	評価	評価コメント
	19	改善が必要	Wordpressを運用するにあたり求められるセキュリティ設定がなされていません。 また現状利用しているWordPressは脆弱性が報告されているバージョンであることから、早急な対応が求められます。

ウイルス・マルウェア感染チェック結果サマリー	評価	評価コメント
	× 複数のマルウェアを検知	複数のマルウェアを検知いたしました。 ページにアクセスしたユーザーの情報を抜き取るマルウェアであることから、早急な対応が必要です。

■セキュリティ・脆弱性診断結果

#	診断項目	評価	診断結果	推奨対応
1	使用WordPressバージョンにおける脆弱性の有無	×	利用中のWordPress 6.0.2には複数の脆弱あり https://ja.wordpress.org/2022/10/18/wordpress-6-0-3-security-release/	最新版のWordPressへのアップデートを推奨
2	導入しているプラグインの脆弱性の有無	×	複数のプラグインにて脆弱性あり XXXプラグイン　クロスサイトスクリプティングの脆弱性あり。当該プラグインを使用しているWordPress にログインしているユーザのウェブブラウザ上で、任意のスクリプトを実行される可能性あり YYYプラグイン　PHPオブジェクトインジェクションの脆弱性あり。リモートから第三者に任意のPHPコードを実行される可能性あり	最新版のへのアップデートを推奨 既にプラグインの更新が停止されていることから削除を推奨。 代替プラグインとしてZZZプラグインの利用が可能。
3	ホームページ ⇔ 閲覧ユーザー端末間の通信の暗号化	×	SSL（インターネット上でデータを暗号化して送受信する仕組み）の設定はなされているものの、一部の要素は暗号化なしの状態でやり取りされている	全ての通信を暗号化するための追加設定が必要
4	サーバー上のファイル、フォルダへの不正アクセス制御	×	サイトの設定を管理している重要なファイルに対して外部からアクセス可能な状態になっている .htacces wp-config.php	 外部からアクセスできないよう設定を追加する 適切なパーミッションを追加する 外部からアクセスできないよう設定を追加する 適切なパーミッションを追加する
5	ハッキングによるファイル改ざん検知機能の有無	×	ファイル改ざん検知機能なし	ファイル改ざん検知機能を設定する
6	不正ログインリスク低減、 ログイン画面への総当たり攻撃（ブルートフォースアタック）対策	○	ログイン画面のURLが初期設定から変更されている	対応不要
		×	サイト上に表示される"投稿者名"と"ログインユーザー名"が同一である	サイト上に表示される"投稿者名"を"ログインユーザー名"以外の名称に変更する
		×	推測されやすいログインユーザー名が使用されている admin root	 ユーザー名を変更する ユーザー名を変更する
		×	ファイル改ざん検知機能なし	ファイル改ざん検知機能を設定する
7	ページ改ざん、マルウェア埋め込み対策	×	外部からの不正な攻撃を防ぐためのソフトウェア（Web Application Firewall)が未設定	Web Application Firewall（WAF)を導入する
		×	HTTPセキュリティヘッダーの設定が不十分	セキュリティヘッダーの設定を追加する
		×	メールフォーム等の入力値を制限するバリデーション処理がなし	メールフォームにバリデーション処理を追加する
		×	一部入力フォームにて、エスケープ処理がなし	既存のプログラムにエスケープ処理を追加する
8	ホームページ上の記事に対するスパムコメント対策	○	コメント機能が無効化されている	対応不要
9	問い合わせフォームを利用したスパムメールの送信回避	○	スパムメール送信をブロックする仕組み（reCAPTCHA）が導入されている	対応不要
10	WordPressデータ（DB含む）のバックアップ	×	定期的なバックアップ未取得	定期的なバックアップ取得の設定を追加する

■ウイルス・マルウェア感染チェック結果

#	診断項目	評価	診断結果	推奨対応
1	ウイルス・マルウェアの感染チェック	×	複数のファイルにてマルウェアの感染を確認 **index.php**　index.phpファイルに、不自然な処理（文字列）が追加されていることを検知 ページを開く度に、追加された処理が実行されてしまっている **manage.php**　wordpressのコアファイルではない、不自然なPHPファイルが存在 ファイルには、別のファイル（マルウェア本体）を呼び出す処理が記載されいる	 早急にマルウェアの除去が必要 早急にマルウェアの除去が必要