SECURITY ASSESSMENT

外部からの設定診断 報告書（見本）

サンプル商事株式会社さま　https://www.example.co.jp/

診断の種類	外部からの設定診断（ログイン情報なし）
診断日	20XX年X月X日
作成	株式会社オーバーエックス

この見本について

オーバーエックスがお渡ししている成果物の形式をお見せするための見本です。会社名・人名・数値・内容はすべて架空で、実在の会社やシステムとは関係ありません。

1. 結果の概要

危険度	件数	主な内容
高	1件	PHPのバージョンがサポート終了（8.1）
中	3件	セキュリティ関連のヘッダー未設定、管理画面が外部から開ける、DMARC未設定
低	2件	サーバーのバージョン表示、不要なファイルの公開

優先して対応すべきこと：PHPを8.3以降に更新すること（推奨期限：1か月以内）。管理画面へのアクセス制限も早めの対応をおすすめします。

2. 指摘事項と直し方（抜粋）

No	危険度	指摘	直し方
1	高	PHP 8.1（セキュリティサポート終了）が使われている	サーバーの設定でPHP 8.3以降に切り替え、テーマ・プラグインの動作を確認する
2	中	WordPressの管理画面（/wp-admin/）が誰でも開ける	IPアドレスの制限、または二段階認証を設定する
3	中	HSTS・X-Frame-Optionsなどのヘッダーが未設定	サーバーまたはCDNでレスポンスヘッダーを追加する
4	中	メールのDMARCが未設定	DNSにDMARCのレコードを追加する（まずは監視モード）
5	低	サーバーのバージョンが表示されている	設定でバージョンの表示を止める

3. 確認した項目の一覧

項目	結果
SSL証明書・暗号化通信	良好
http→httpsの転送	良好
セキュリティ関連のヘッダー	注意
PHP・CMS・サーバーのバージョン	要対応
管理画面の公開状態	注意
不要なファイルの公開	低
メールの送信ドメイン認証（SPF・DKIM・DMARC）	注意
改ざんの兆候	見つからず

4. 診断の範囲について

この診断は、公開されている情報と外部からの通常の通信で分かる範囲を確認したものです。サーバー内部の設定やプログラムの脆弱性までは確認していません。重要なシステムでは、内部診断やツール診断をご検討ください。

指摘事項の修正、PHPの更新、サーバー移行は、当社でそのままお受けできます（保守を3か月以内にご契約の場合、診断費用を初月の保守料から差し引き）。