WordPress セキュリティ・チェックシート

本チェックシートは、企業とお客様双方の信頼を守るための実践的なチェックシートです。
定期的にチェックを行い、対応が不十分な項目があれば、速やかに改善を行いましょう。

CHECK 1 予防は最大の防御

攻撃前に脆弱性を排除し、被害を未然に防ぐ

- ☐ CMS（WordPress等）は最新バージョンに更新しているか
- ☐ プラグインやテーマは不要なものを削除し、常にアップデートしているか
- ☐ サーバーやミドルウェア（PHP、MySQL等）の更新を定期的に行っているか
- ☐ SSL/TLS証明書を導入し、サイト全体を常時SSL化しているか

CHECK 2 最小権限の原則

必要最低限のアクセス権、プログラム、通信範囲

- ☐ 管理者アカウントは必要最低限の人数に限定しているか
- ☐ パスワードは強固にしていて、適宜更新をしているか
- ☐ パスワード管理のルールはあるか
- ☐ サーバーの不要なポートやサービスは無効化しているか

CHECK 3 多層防御

単一の防御策に依存せず、複数レイヤーで守る

- ☐ WAF（Webアプリケーションファイアウォール）を導入しているか
- ☐ ログイン試行回数制限やCAPTCHAを設置しているか
- ☐ ウイルス対策ソフトやサーバー監視ツールを併用しているか
- ☐ バックアップを定期取得し、外部環境に保存しているか

CHECK 4 検知と即応

インシデントの早期発見と初動対応が被害拡大を防ぐ

- ☐ アクセスログ・エラーログを定期的に確認しているか
- ☐ 不正アクセスや改ざんを検知できる仕組みがあるか
- ☐ セキュリティインシデント発生時の初動手順（連絡・復旧）が決まっているか
- ☐ 外部セキュリティ会社や専門家に相談できる窓口を確保しているか

CHECK 5 継続的改善

環境や脅威を知り、変化に合わせて対応を図る

- ☐ 半年に一度以上、サイトのセキュリティ診断を実施しているか
- ☐ 最新の脆弱性情報を収集・反映しているか
- ☐ 社内でセキュリティルールを共有し、教育を行っているか
- ☐ 定期的にチェックシートを見直し、改善を行っているか

株式会社ネクスト・アクションでは、企業のWebセキュリティを確保するために「予防・最小権限・多層防御・検知即応・継続改善」の5つの原則を提唱しています。ほんの少しの油断が大きな被害につながります。基本的なセキュリティ対策を徹底していれば、多くのリスクを未然に防ぐことができます。

nextaction

【お問い合わせ先】株式会社ネクスト・アクション
contact@next-action.co.jp TEL 04-7186-6026