セキュリティチェックリスト

【毎日チェック】

☐ **サイト表示の異常確認**
ECサイトのトップページや商品ページに乱れ、改ざんや障害表示がないか目視で確認します。
ロード速度の極端な低下やレイアウト崩れがないかをチェックします。

☐ **ログイン履歴　不審なアクティビティの確認**
WordPress管理画面やセキュリティプラグイン（例：Wordfence、SiteGuard WP Plugin）のログイン履歴で異常な時間やIPアドレスからのアクセスがないか確認します。
多数のログイン失敗や、普段使用していない国からのアクセスがある場合は注意しましょう。

☐ **注文管理　顧客情報の整合性**
受注一覧や顧客情報に異常な登録、注文数や金額に急な増減がないかをチェックします（大量の無意味な注文など）。ステータスが適切に進行しているか、エラーやキャンセルが増加していないかを確認します。

☐ **スタッフ向け周知事項　メールのフィルタリング**
スタッフ宛てに届いたメールやチャットツールに「怪しいメール」（フィッシング、詐欺請求書など）が届いていないか、周知　共有体制をチェックしましょう。

【毎週チェック】

☐ **WordPress／Welcart／プラグインのアップデート状況**
管理画面の更新があるか、WordPressコア　プラグイン　テーマが最新版かどうかを確認します。
Welcart公式サイトやフォーラムにて提供されているアップデート情報や不具合報告もチェックしましょう。

☐ **セキュリティプラグインのスキャン結果**
Wordfenceなどでファイル改ざんスキャンや脆弱性スキャンを実施し、検出結果をレビューします。特定のマルウェア兆候をプラグインから通知が出ます。

☐ **バックアップログの確認**
UpdraftPlusやBackWPupなどの実行ログを見て、自動バックアップが正常に行われているか確認します。DropboxやGoogle Driveなど外部ストレージへの保存状況もチェックしましょう。

☐ **スタッフPCのウイルス対策ソフト　OS更新状況**
ウイルス対策ソフトの有効性やOSの更新状態を確認し、必要に応じてアップデートを行います。
社外端末や在宅勤務用デバイスも対象に含めます。

☐ **アクセス解析　不審なIPチェック**
Google Analyticsやサーバーログを確認し、特定の国や異常IPからのアクセス数増加がないかを確認します。
CloudflareやWAFでブロックされたリクエストを確認し、新しい攻撃パターンがないかを見ます。

【毎月チェック】

☐ **バックアップの復元テスト**
取得したバックアップをステージング環境に復元し、正常に復旧できるかをテストします。
サイトが想定通り動作するかを確認し、運用スタッフと共有します。

☐ **サーバー環境　バージョン確認**
PHPやMySQLのバージョン確認、不必要なモジュールの削除などを行います。
.htaccessやNginx設定も見直し、セキュリティ上重要な設定ミスがないかチェックします。

☐ **スタッフ権限　アカウント棚卸し**
WordPressやFTP、サーバーのアカウントを整理し、不要なものや退職者の権限を無効化
削除します。必要な権限だけを付与しているかを見直し、過剰権限のチェックも行います。

☐ **セキュリティ研修やマニュアルのアップデート**
スタッフ向けに最新のフィッシング事例などを共有し、定期勉強会や情報共有の場を持ちます。
運用マニュアルに改善点があれば追記し、最新版を共有します。

【四半期　半年に一度の追加チェック】

☐ **緊急時対応フローのシミュレーション**
改ざん発見　ウイルス感染などのシナリオをもとに、ロールプレイ訓練を行います。
連絡体制・対応フローに不備がないか確認します。

☐ **テーマ　プラグインのコードレビュー（可能な範囲で）**
使用中のテーマやプラグインが継続的に保守されているかを確認します。
非推奨コードや古いPHPバージョンの使用有無を確認し、必要に応じて書き換え・置換します。

☐ **法令遵守　ポリシーの更新**
個人情報保護　Cookieポリシーなどが最新の法令に適合しているか確認します。
「特商法の表記」「利用規約」なども定期的に見直します。