対象と担当を一枚にする

EC・ブログ・フォーム・関連サイトを分けて記録します。足りない欄は複写してください。

会社・部署／記入者／確認日：

1 ECの標準機能

対象URL・用途：

社内担当・保守先：

契約範囲・直近の確認記録の参照先：

2 ブログ・独自プログラム

対象URL・用途：

社内担当・保守先：

契約範囲・直近の確認記録の参照先：

3 問い合わせ・外部フォーム

対象URL・用途：

社内担当・保守先：

契約範囲・直近の確認記録の参照先：

4 関連サイト・その他

対象URL・用途：

社内担当・保守先：

契約範囲・直近の確認記録の参照先：

担当が不明な作業／問い合わせ先／回答期限：

緊急時の連絡先・代行／記録を保管する場所：

パスワード、APIキー、顧客の実データは記入せず、社内資料の参照先を残してください。

保守の確認12項目

根拠がない場合は「不明」。対象外には理由を残し、未対応には担当と期限を付けます。

01 EC・ブログ・フォームの担当を一覧にする

☐ 確認済み ☐ 未対応 ☐ 不明 ☐ 対象外

根拠・対象外の理由の参照先：

02 停止した機能のサーバー側処理を確認する

☐ 確認済み ☐ 未対応 ☐ 不明 ☐ 対象外

根拠・対象外の理由の参照先：

03 フォームのサーバー側の入力条件を確認する

☐ 確認済み ☐ 未対応 ☐ 不明 ☐ 対象外

根拠・対象外の理由の参照先：

04 同時受付と記録失敗時の試験結果を確認する

☐ 確認済み ☐ 未対応 ☐ 不明 ☐ 対象外

根拠・対象外の理由の参照先：

05 変更したフォームのメール到達を確認する

☐ 確認済み ☐ 未対応 ☐ 不明 ☐ 対象外

根拠・対象外の理由の参照先：

06 古い・重複したスクリプトの扱いを確認する

☐ 確認済み ☐ 未対応 ☐ 不明 ☐ 対象外

根拠・対象外の理由の参照先：

07 表示データとURLの出力処理を点検する

☐ 確認済み ☐ 未対応 ☐ 不明 ☐ 対象外

根拠・対象外の理由の参照先：

08 独自管理機能の権限とnonceを確認する

☐ 確認済み ☐ 未対応 ☐ 不明 ☐ 対象外

根拠・対象外の理由の参照先：

09 再有効化で既存設定を消さないか確認する

☐ 確認済み ☐ 未対応 ☐ 不明 ☐ 対象外

根拠・対象外の理由の参照先：

10 秘密情報・バックアップの公開制限を確認する

☐ 確認済み ☐ 未対応 ☐ 不明 ☐ 対象外

根拠・対象外の理由の参照先：

11 プラグイン操作後も保護が残るか確認する

☐ 確認済み ☐ 未対応 ☐ 不明 ☐ 対象外

根拠・対象外の理由の参照先：

12 復元データと再適用する修正を照合する

☐ 確認済み ☐ 未対応 ☐ 不明 ☐ 対象外

根拠・対象外の理由の参照先：

詳しい結果と次の対応は3ページへ。復元は4ページへ。対象・日時・担当をそろえて記録します。

改修前後の結果を残す

1件の改修ごとに記入・複写。拒否すべき条件と、必要な正常動作を両方確認します。

対象サイト・機能／対応するチェック番号：

分かった問題と、今回変更する内容：

担当者／実施日時／承認・連絡先：

変更前の保全と、問題時に戻す方法：

保管場所の参照先、復旧担当、切戻しを判断する条件

拒否する条件と、確認結果：

不正入力・権限不足・非公開対象など。試験条件と記録の参照先

正常動作の条件と、確認結果：

表示・操作・メール到達など。模擬試験か実動作かも記入

未確認・残る問題／次の担当・期限：

再確認日／確認者／次回に確認する操作：

「対策済み」だけで終えず、何をどの条件で確認したかを記録してください。

復元できた範囲を記録する

保存・復元・内容照合・修正の再適用・業務操作を分けて確認します。

取得日時／ファイル・DBの対象／保管先：

暗号化・鍵を利用できる担当／復元先の環境：

秘密値は書かず参照先のみ。検証時の外部送信停止も確認

照合した記事・画像・設定／結果と記録の参照先：

含まれない外部資産・設定／再適用する修正：

業務操作の確認／未確認事項／担当・期限：

主な参考資料

IPA：ECサイト構築・運用セキュリティガイドライン

futureshop：ECサイトのセキュリティ

WordPress：Nonces

WordPress：Backups

PHP：flock

OWASP：Secrets Management

公開情報から、自社サイトの現状を確認する

無料のAIセキュリティ検査を始める →