WordPress 緊急対応フローチャート

ハッキング・不正アクセスが疑われたときの初動から復旧まで

01 異常を発見・記録

- 不審な表示・転送・管理者追加
- 発見日時、URL、画面を記録
- 直前の変更と通知を保存

02 被害拡大を防ぐ

- 利用者への危険があれば公開制限
- 認証情報の悪用も考慮
- 独断でファイルを消さない

03 証拠を保全する

- アクセス・エラーログを確保
- ファイル・DBの現状を保存
- 感染疑いのデータは隔離

04 連絡・原因調査

- 社内責任者／制作・保守会社
- サーバー会社・専門業者へ相談
- アカウント／脆弱性／改ざん調査

最優先： 利用者の安全と被害拡大防止。状況によっては、証拠保全と並行してアクセス遮断を進めます。

※具体的な遮断・復旧操作は環境により異なります。判断できない場合は専門担当者へ相談してください。

05 安全な復旧を実施

- 不正コードと侵入経路に対処
- 安全性を確認したデータを利用
- 各種認証情報・権限を見直す

06 公開前の動作確認

- 全ページと不審な転送を確認
- フォーム・購入・予約を検証
- 安全性を確認後に公開判断

07 外部への対応

- Search Consoleの警告を確認
- 必要時は修正後に審査申請
- 個人情報の影響と報告要否確認

08 再発防止・記録

- 本体・テーマ・プラグイン更新
- 2段階認証／権限／バックアップ
- 経緯と対応手順を記録

緊急連絡先（記入欄）

社内責任者：＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿　制作・保守会社：＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿　サーバー会社：＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

注意：バックアップ復元だけでは再感染のおそれがあります。漏えいの疑いがある場合は法令に基づく報告・通知の要否を確認してください。