CCSI

CROSS&CROWN GROUP

サイバー保険請求チェックリスト

改訂: 2026-02-16

（WordPress 改ざん・不正アクセス・マルウェア被害向け）

最重要：復旧より先に「証拠保全」
復旧作業を先に行うと、攻撃の痕跡（ログ・不正ファイル・DB 改ざん）が消え、保険会社から追加証拠を求められた際に対応できないことがあります。
保険請求を検討している場合は、復旧前に「証拠保全」を優先してください。

このチェックリストは、サイバー保険請求に向けて「必要情報」「証拠」「提出物」を漏れなく準備するための実務用テンプレートです。
※ 保険商品・約款により必要書類は異なります。最終的には保険会社の案内に従ってください。

1. 基本情報（まず埋める）

会社名 / 団体名

担当者名 / 連絡先（電話・メール）

対象サイト URL

契約しているサイバー保険（保険会社 / 商品名 / 証券番号）

被害発覚日時（わかった範囲で）

現在の状況（例：改ざん表示 / 404 / リダイレクト / 警告表示 など）

2. 初動（発覚〜24 時間）

2-1. 影響拡大の抑止（安全側で実施）

☐	項目
☐	サイトの改ざん表示・リダイレクト等を確認し、画面キャプチャを保存（URL と時刻が分かる形）
☐	サイト運用者・関係者へ一次連絡（影響範囲・暫定対応・再現条件）
☐	管理画面 / FTP / SSH / DB など、関係アカウントのパスワード変

	更（可能なら強制ログアウトも実施）
☐	WAF / CDN / サーバ側での緊急遮断（不審 IP、特定 URL、ログイン試行、攻撃パターン）
☐	改ざんページの一般公開停止（メンテ / 503 / 静的退避など）※ ただし証拠保全の前にファイルを削除しない
☐	社内/委託先の作業ログ（誰が・いつ・何を）を記録開始（後で請求・説明に使います）

2-2. 保険会社への連絡準備

☐	**項目**
☐	保険証券番号・加入プラン・免責・補償上限・事故通知期限を確認
☐	事故通知の窓口（電話/メール/フォーム）と受付番号を記録
☐	被害の概要を 1 枚で整理（いつ/何が/どうなった/現時点の影響）
☐	保険会社が求める「証拠の形式」や「提出期限」を確認し、メモを残す

3. 証拠保全（復旧前に実施）

3-1. 取得する証拠（推奨）

※ 復旧や削除は、証拠保全後に行う（「原本」と「作業用コピー」を分離）。

☐	**項目**
☐	アクセスログ（SSL 含む）・エラーログ・WAF/CDN ログ（可能な範囲で期間を広めに）
☐	WordPress 一式（ファイル）を“原本”として取得（作業用コピーとは分離）
☐	データベースダンプ（スキーマ＋データ）を取得
☐	サーバ情報（OS/ミドル/WordPress/プラグイン・テーマのバージョン一覧）を記録
☐	不審メール・警告画面・検索結果等のスクリーンショット（URL/時刻入り）
☐	保全データの保管場所・アクセス権限（誰が触れるか）を決める

3-2. 改ざん防止（完全性の担保）

☐	項目
☐	保全データにハッシュ値（SHA-256 推奨）を付与し、取得直後に記録
☐	コピー後も同じハッシュになることを確認（原本は以後触らない）
☐	証拠取扱記録（Chain of Custody）を残す（担当者/時刻/作業内容/保管場所）
☐	時刻の基準（サーバ時刻・端末時刻・NTP）を確認し記録

4. 被害状況の整理（保険会社が見たいポイント）

4-1. 何が起きたか（インシデント概要）

☐	項目
☐	改ざん内容（表示改ざん/リダイレクト/マルウェア設置/不正送信/管理者追加 など）
☐	発生期間（最古の痕跡〜復旧完了まで）※ 不明なら推定根拠も残す
☐	影響範囲（対象サイト数、サブドメイン、関連サーバ、外部連携）
☐	業務影響（停止時間、売上影響、問い合わせ増加、信用毀損 等）
☐	第三者への影響（顧客・取引先への波及、フィッシング誘導など）

4-2. 情報漏洩の有無（重要）

☐	項目
☐	漏洩可能性のある情報の種類（個人情報/会員情報/決済情報/メールアドレス など）
☐	漏洩経路の可能性（DB 抽出/フォーム改ざん/ログイン情報窃取 など）
☐	現時点の判断（漏洩なし/可能性あり/調査中）と根拠
☐	外部報告が必要な場合の記録（委員会報告、顧客通知、取引先報告）

5. 復旧・再発防止の記録（請求・説明に効く）

5-1. 実施した対応（時系列で記録）

☐	項目
☐	一次対応（遮断・停止・パスワード変更等）の実施日時と担当者
☐	不正ファイルの特定・隔離・除去（削除前に原本保全済みか）
☐	脆弱性の修正（プラグイン更新、設定変更、権限見直し）
☐	WordPress/プラグイン/テーマの整合性確認（正規ファイルとの差分）
☐	管理者アカウント・API キー・SMTP・外部連携の不正設定がないか確認
☐	再発防止策（WAF/2FA/アクセス制限/ログ保全期間延長 等）の実施
☐	復旧後の監視（再侵入の兆候、異常アクセス、改ざん再発）

6. 保険請求の提出パッケージ（例）

6-1. 提出物（一般的な例）

※ 保険会社から「追加の証拠」を求められることがあります。根拠が示せる形（ログ・差分・タイムライン）で整理します。

☐	項目
☐	事故通知書 / 保険会社指定の請求書類（記入済み）
☐	被害状況の説明資料（1〜2 ページの概要＋詳細）
☐	調査報告書（侵入経路・攻撃手法・被害範囲・タイムライン）
☐	証拠データ一覧（取得物リスト、ハッシュ値、保管場所）
☐	作業記録（対応作業ログ、作業時間、外注費用の内訳）
☐	関連する請求書・見積書（調査費用、復旧費用、監視/再発防止費用等）

7. よくある不備（提出前の最終確認）

7-1. NG になりやすい点

☐	**項目**
☐	復旧を先に行い、ログや不正ファイルが失われている（証拠不足）
☐	発覚日時・発生期間の根拠がない（推定でも根拠を残す）
☐	どの費用が何の作業に対応するか紐付いていない（明細不足）
☐	証拠データの完全性（ハッシュ）や取扱記録がなく、改ざん疑義が残る
☐	提出物が点在し、保険会社の担当者が追えない（1 パッケージ化不足）

8. 付録（メモ欄）

・保険会社からの指示 / 確認事項：

・提出期限 / 受付番号：

・追加で求められた証拠：