

PHP脆弱性対応チェックリスト

目的	今回公表されたPHPの脆弱性について、「影響の有無 → 悪用の形跡 → 対応 → 対応後」の順に確認します。	<本件に関するお問合せはこちら> 株式会社クロスフォース TEL : 03-5643-9902 メール : info@cross-force.jp	
使い方	担当者でも確認できる項目と、専門知識が必要な項目を分けています。判断できない項目は無理に「問題なし」とせず、エンジニアへ確認してください。		

大項目	確認項目	解説・判断のポイント	チェック内容 (こうなっていれば問題なし！)	想定される作業者
1. 今回の脆弱性の影響を受けるか				
	使用中のPHPバージョン	まず、サイトで使用しているPHPのバージョンを確認します。今回の脆弱性の影響対象かどうかを判断するための前提情報です。分からない場合はサーバー管理画面等で確認するか、エンジニアへ確認してください。	使用中のPHPバージョンを特定できている。 以下のバージョンであれば問題なし。 8.2.35 8.3.36 8.4.27 8.5.12	担当者／エンジニア
	今回の脆弱性の対象か	確認したPHPバージョンが、今回公表された脆弱性の影響を受けるバージョンか確認します。バージョン番号だけで判断できない場合もあるため、不明な場合はエンジニアへ確認してください。	今回の脆弱性の影響対象外、または影響対象であることを把握できている。	エンジニア推奨
	サーバー会社の対応状況	レンタルサーバー等では、サーバー会社側ですでに修正が適用されている場合があります。公式のお知らせや管理画面で、今回の脆弱性への対応状況を確認します。	サーバー会社の対応状況を確認済みで、自社側で追加対応が必要か判断できている。	担当者でも可
	現在の環境に修正が反映されているか	サーバー会社の対応を含め、今回の脆弱性に対する修正が実際の利用環境へ反映されているか確認します。専門的な判断が必要なため、エンジニアへの確認を推奨します。	今回の脆弱性に対する修正が、実際に稼働している環境へ適用済み。	エンジニア
2. すでに悪用された形跡がないか				

	サイト上に目に見える異常がないか	意図しない別サイトへの転送、身に覚えのない文章・リンク・広告・ページなどがいないか確認します。これらがなくても安全とは限らないため、次の技術的な確認も行います。	意図しない転送・文章・リンク・広告・ページなどが確認されない。	担当者でも可
	検索結果に身に覚えのないページがないか	Googleで「site:自社ドメイン」と検索し、作成した覚えのないページや不自然なタイトルが表示されていないか確認します。検索結果には時間差があるため、補助的な確認です。	検索結果に、作成した覚えのないページや不自然なタイトルが確認されない。	担当者でも可
	アクセス・セキュリティログに攻撃の痕跡がないか	アクセスログやWAF（Webサイトへの攻撃を検知・遮断する仕組み）のログを確認し、今回の脆弱性を狙った攻撃や不審な通信がないか調べます。ログの判断はエンジニアへ確認してください。	今回の脆弱性を悪用した攻撃・侵入の形跡がログ上で確認されない。	エンジニア
	Webサイトのファイルに不正な変更がないか	PHPファイルなどに、運営側が行っていない変更や不審なコードが追加されていないか確認します。更新日時だけでは判断できない場合があります。	運営側が行っていないファイル変更・追加ファイル・不審なコードが確認されない。	エンジニア
	管理者・サーバーへの不正ログインがないか	WordPress等に身に覚えのない管理者アカウントが追加されていないか、FTP・SSHなどサーバーへのログイン履歴に不審なものがないか確認します。	身に覚えのない管理者アカウントや不正なログインが確認されない。	担当者／エンジニア
	データベース・自動実行処理に不正な変更がないか	記事・設定・ユーザー情報などのデータベースや、cron等の自動実行処理に、運営側が行っていない追加・変更がないか確認します。専門的な調査になるためエンジニアへ確認してください。	データベースや自動実行処理に、意図しない追加・変更が確認されない。	エンジニア
3. 必要な対策を行う				
	安全なPHP環境へ更新する	影響を受ける環境の場合は、Webサイトとの互換性を確認したうえで、修正版または安全なPHPバージョンへ更新します。サポート終了済みの古いPHPを使用している場合は、今回に限らず更新を検討します。	影響対象の場合、安全なPHPバージョンまたは修正版へ更新済み。影響対象外の場合は対応不要と判断できている。	エンジニア
	同じサーバー内の他サイトも確認する	1台のサーバーで複数サイトを運用している場合、同じPHP環境や権限の影響を受ける可能性があります。対象サイトだけでなく、同一サーバー内のサイトも確認します。	同一サーバー内に他サイトがある場合、それらも影響確認済み。該当サイトがない場合は対象外。	エンジニア

	WordPress等の更新状況も確認する	今回のPHP脆弱性とは別に、WordPress本体・プラグイン・テーマにも脆弱性が存在する場合があります。別の侵入経路を残さないため、既知の脆弱性や更新状況もあわせて確認します。	WordPress本体・プラグイン・テーマ等について、既知の重大な脆弱性を放置していない。	担当者／エンジニア
	侵害の疑いがある場合は認証情報を変更する	不正ログインや改ざんの疑いがある場合は、WordPress管理者、FTP・SSH、サーバー管理画面などのパスワード・認証情報を変更します。異常がない場合に一律で行う項目ではありません。	侵害の疑いがある場合、必要な認証情報を変更済み。侵害の疑いがない場合は対応不要。	エンジニア判断
	復旧できるバックアップがあるか確認する	問題発生時に戻せるよう、Webサイトのファイルとデータベースのバックアップについて、取得日時・保存先・復元可否を確認します。	必要時に復旧できるWebサイトのファイル・データベースのバックアップが確保されている。	担当者／エンジニア
4. 対応後に問題がないか確認する				
	主要ページ・主要機能が動作するか	PHP更新後に、主要ページの表示、お問い合わせ・申込・購入・ログイン・検索など、そのサイトで重要な機能を実際に確認します。これは脆弱性の有無ではなく、対応による不具合がないかの確認です。	PHP更新後も、主要ページとお問い合わせ・申込・購入・ログイン・検索等の主要機能が正常に利用できる。	担当者でも可
	更新後にエラーが発生していないか	画面上では問題がなくても内部でエラーが発生している場合があります。PHPエラーログ等を確認し、更新による新たなエラーがないか調べます。	PHP更新に起因する新たなエラーが、エラーログ等で確認されない。	エンジニア
5. 不正アクセスがあったか確認する				
	Webサイトへの不審なアクセスがないか	サーバーのアクセスログやWAF（不正な通信を検知・遮断する仕組み）の記録を確認します。大量アクセスや攻撃を試みた形跡がないか調べます。	不正アクセスの成功や侵入を示す形跡が確認されない。攻撃の記録がある場合も、遮断状況と影響を確認できている。	エンジニア
	管理画面への不正ログインがないか	WordPressなどの管理画面で、ユーザー一覧やログイン履歴を確認します。知らない管理者が追加されていないか、身に覚えのないログインがないか調べます。	身に覚えのない管理者アカウントや、不正なログインが確認されない。	担当者／エンジニア

	サーバーへの不正ログインがないか	FTP・SFTP・SSH（サーバーに接続してファイル操作などを行う仕組み）やサーバー管理画面のログイン履歴を確認します。	身に覚えのない接続元・日時からの不正なログインが確認されない。	エンジニア
	Webサイトのファイルが改ざんされていないか	サーバー内のファイルについて、更新日時や変更内容を確認します。身に覚えのないPHPファイルや、不審なプログラムが追加されていないか調べます。	運営側が行っていないファイルの追加・変更や、不正なプログラムが確認されない。	エンジニア
	Webサイト内部に不正な変更がないか	データベース（Webサイトの情報を保存する場所）や自動実行処理を確認します。知らないユーザー・データ・処理が追加されていないか調べます。	データベースや自動実行処理に、身に覚えのない追加・変更が確認されない。	エンジニア