PHP 脆弱性対応チェックリスト

2026年11月19日に公開された PHP の修正版（8.5.13・8.4.28・8.3.37・8.2.36）への対応に使うチェックリストです。

確認日	担当者	対象のサーバー・サービス
年　　月　　日		

1. 対象の洗い出し

確認	確認すること	メモ
☐	PHP が動いているサーバー・サービスを一覧にした（自社のサーバー、レンタルサーバー、保守を委託しているサイト、WordPress など）	
☐	サーバーごとに PHP の版を確認した（php -v、サーバーの管理画面、phpinfo など）	
☐	PHP の動かし方を確認した（PHP-FPM・PHP-CGI・Web サーバーのモジュール）	
☐	使っている拡張を確認した（session・SOAP・PHAR・DOM など）	
☐	保守の委託先と連絡先を確認した	

2. 版の判定

系列	修正版	セキュリティサポートの期限	対応
8.5	8.5.13 以降	2029年12月31日	修正版に更新
8.4	8.4.28 以降	2028年12月31日	修正版に更新
8.3	8.3.37 以降	2027年12月31日	修正版に更新
8.2	8.2.36 以降	2026年12月31日	修正版に更新し、8.3 以降への移行を計画
8.1 以前	提供なし	終了	8.3 以降へ移行

Linux のディストリビューションが配る PHP のパッケージは、版の番号が上の表と異なることがあります。ディストリビューションのセキュリティ情報で、CVE ごとに修正済みかを確認します。

3. 更新

確認	確認すること	メモ
☐	更新の前にバックアップを取った（プログラム・データベース・設定ファイル）	
☐	検証環境で更新し、主な画面と機能を確認した	
☐	本番環境に適用し、PHP-FPM・Web サーバーを再起動した	
☐	更新後の版を確認した（コマンドラインと、Web から動く PHP の両方）	
☐	更新後のエラーログと主な画面を確認した	
☐	レンタルサーバー・委託先の分は、更新の予定と完了を確認した	

4. すぐに更新できないときの対応

確認	確認すること	メモ
☐	PHP-FPM のステータスページ（pm.status_path）を外部から見られないようにした	
☐	PHP-CGI を Web から直接呼び出せる設定になっていないことを確認した	
☐	使っていない拡張（SOAP など）を無効にした	
☐	更新の予定日を決め、関係者と共有した	

5. 記録と報告

確認	確認すること	メモ
☐	対象ごとに、更新前後の版・対応の内容・対応日を記録した	
☐	上長・情報セキュリティの責任者に報告した	
☐	必要に応じて、取引先・利用者へのお知らせを出した	

6. 次回への備え

確認	確認すること	メモ
☐	脆弱性の情報を確認する担当者と頻度を決めた（php.net・JVN・ディストリビューションのセキュリティ情報）	
☐	この手順を社内のマニュアルにまとめ、置き場所と改訂の担当を決めた	

参考：2026年11月19日の修正版で修正された脆弱性

CVE	内容	対象の系列
CVE-2026-115560	セッションのシリアライザの不一致による、遠隔からのコード実行	8.2〜8.5
CVE-2026-126714	一部が上書きされたセッションファイルによる、遠隔からのコード実行	8.2〜8.5
CVE-2026-129496	タイムゾーンのキャッシュの解放後使用による、遠隔からのコード実行	8.2〜8.5
CVE-2026-129474	マジックメソッドのバックトレースの解放後使用による、遠隔からのコード実行	8.5
CVE-2026-129291	PHP-FPM（epoll）の解放後使用による、ローカルでの権限昇格	8.2〜8.5
CVE-2026-129289	PHP-FPM で読まれなかったリクエスト本文による、リクエストスマグリング	8.2〜8.5
CVE-2026-129292	PHP-FPM のステータスページのクロスサイトスクリプティング（XSS）	8.2〜8.5
CVE-2026-129538	PHP-CGI の PATH_INFO の補正での範囲外の読み書き	8.2〜8.5
CVE-2026-128090	PHAR の OpenSSL 署名の、アルゴリズムのダウングレードによる回避	8.2〜8.5
CVE-2026-128064	大文字・小文字が混ざった HTTPS・FTPS の URL で、データが暗号化されずに送られるおそれ	8.2〜8.5
CVE-2026-127960	折り返された HTTP レスポンスヘッダーによるサービス妨害（DoS）	8.2〜8.5
CVE-2026-15353	SOAP の不正な配列の次元による情報漏えい	8.2〜8.5
CVE-2026-129506	SOAP の DTD の実体参照の処理での解放後使用	8.2〜8.5
CVE-2026-129481	中断されたセッションの終了処理の後の解放後使用	8.3〜8.5
CVE-2026-129501	DOM の XML の書き出しでの二重解放	8.4〜8.5
CVE-2026-129182	終了処理の後に致命的エラーのバックトレースが設定されることによる解放後使用	8.5
CVE-2026-129438	長すぎる入力での RFC 3986 の URI の誤った組み立て	8.5
CVE-2026-48841	URI の拡張が使う uriparser の脆弱性（uriparser 1.0.3 に更新）	8.5

出典：php.net の ChangeLog（2026年11月19日）。シャノン合同会社
https://shannon.co.jp/insights/php-vulnerability-checklist/