

Claude Codeで自社サイトのPHP脆弱性を確認・更新する手順

PHP2Shell (CVE-2026-109618／CVE-2026-109619) 対応

Elefant作成 2026年10月版(10月25日時点の公開情報にもとづく。初版は10月22日)

- 0 この資料の前提と注意
- 1 先に確認すること(チェックリスト)
- 2 共用レンタルサーバーの場合:管理画面での確認手順
- 3 VPS・自社サーバーの場合:Claude Code を使った確認の流れ
- 4 制作会社・サーバー会社への確認メール文例
- 5 更新後の確認項目
- 6 参考リンク(一次情報)

注意 状況は時間単位で変わっています。作業の直前に、PHP公式とご利用中のサーバー会社のお知らせを必ず確認してください。

本資料は一般的な確認手順をまとめたものです。
特定の環境での動作を保証するものではありません。

elefant-inc.jp

0 この資料の前提と注意

必ず守る 本番サーバーを触る前に、サイトのファイルとデータベースのバックアップを取ってください。作業はサイトの担当者の責任で行い、判断に迷ったらその時点で止めて、制作会社・サーバー会社・専門家に相談してください。

- この資料は、攻撃の仕組みや手順を説明するものではありません。**自社サイトが影響を受けるかを確認、修正版に更新するための手順**だけを扱います。
- Claude Code は手順の調査・提案・確認を手伝う道具です。**実行の判断は人が行います**。権限確認（実行前の許可）を有効にしたまま使ってください。
- 共用レンタルサーバーでは、PHP本体の修正はサーバー会社が行います。利用者は自分の版が「適用済み」かをお知らせで確認、8.1 以下なら切替を計画します。

何が起きているか(要点)

深刻度:CVSS v4.0 9.2 (Critical)

2件とも同じ評価。流出時に出回った「CVSS 10.0」は誤り（PHP財団）。

種類:認証不要のリモートコード実行

ログイン不要・ネット経由で、サーバー上でプログラムを動かされる恐れ。サイト乗っ取りにつながる欠陥。

対象:Webリクエストを処理するPHP

PHP-FPM、Apache+mod_php、php-cgi、FrankenPHP、LiteSpeed。PHP公式は mod_php が最も危険としている。

影響する版:PHP 5.4 以降

修正版 (8.5.12／8.4.27／8.3.36／8.2.35) より前のすべての版。

攻撃の状況

試みは10/17から観測、公表後は数百万件規模。成功の公的確認・国内の侵害報道はなし (10/25時点)。

回避策

PHP公式は「完全な緩和策はない。更新だけが安全な選択」としている。WAFや暫定設定は「つなぎ」。

バージョン別の状況

PHPの系統	状況	対応
8.5／8.4／8.3／8.2	● 修正版あり	8.5.12 / 8.4.27 / 8.3.36 / 8.2.35 以上へ更新。 8.2 は 2026年12月31日でサポート終了予定のため、年内に 8.3 以上へ。
7.4／8.0／8.1	▲ 公式リリースなし	最小限のバックポートのみ。共用サーバー各社の独自修正は応急的。8.3 以上への切替を計画。
5.4～7.3	× 公式の修正なし	8.3 以上へ切替（共用サーバーは独自修正の例あり）。系統をまたぐ更新は事前にバックアップと動作確認を。

※ Linuxディストリビューション(AlmaLinux・RHEL 等)のPHPは、修正を取り込んでも `php -v` の番号が変わりません。パッケージの版で判定し、更新後は PHP-FPM／Apache の再起動が必要です (AlmaLinux公式)。

1 先に確認すること(チェックリスト)

作業の前に、次の項目を埋めてください。分からない欄は、制作会社・保守会社・サーバー会社に確認します(文例は4章)。

	確認項目	確認のしかた	メモ
☐	自社サイトはPHPで動いているか	WordPress は PHP で動く。EC-CUBE、Laravel製システム、Drupal、Joomla、MediaWiki、Movable Type など PHP。Shopify・Wix・STUDIO・ペライチ等の SaaS 型は自社で PHP を管理していない(運営会社のお知らせを確認)	
☐	対象のドメイン・サイトをすべて洗い出したか	コーポレートサイト、採用サイト、キャンペーンサイト、予約・EC など。IPA も PHP利用システムの洗い出しを推奨	
☐	サーバーの種類	共用レンタルサーバー → 2 章／VPS・自社サーバー → 3 章	
☐	保守を任せている会社の有無	保守契約があれば、対応の有無・完了日・対象ドメインをメールで確認	
☐	PHPのバージョン(系統)	サーバー管理画面の「PHPバージョン設定」(ドメインごと)／WordPress は「ツール」→「サイトヘルス」→「情報」→「サーバー」	
☐	バックアップの取得	サイトのファイルとデータベース。戻し方も確認しておく	
☐	サーバー会社のお知らせ	適用状況・メンテナンス予定・利用者側の作業の有無	
☐	機器に組み込まれたPHP	ネットワーク機器・アプライアンスにも PHP が使われている場合がある(NCSC-NL が注意喚起)。メーカーの告知を確認	

注意 WordPress 本体やプラグインを更新しても、**PHP 本体の欠陥は直りません**。また、SSH で表示される `php -v` の版は、サイトで実際に動いている版と違うことがあります。

2 共用レンタルサーバーの場合：管理画面での確認手順

共用レンタルサーバーでは、PHP 本体の修正版はサーバー会社が入れます。利用者が行うのは、次の確認です。画面の名前や場所は各社で異なるため、ここでは一般的な流れを示します。

- 1 サーバー会社のお知らせを確認する**
修正版の適用が完了したか、メンテナンスの予定、利用者側で必要な作業があるかを確認します。
- 2 管理画面にログインし、「PHPバージョン設定」を開く**
PHP の版はドメインごとに設定されています。複数のドメインを使っている場合は、すべて確認します。
- 3 選んでいる版が、お知らせで「修正適用済み」とされているか確認する**
版を変えずに修正する会社では、番号が修正版 (8.5.12 など) にならないことがあります。8.2 は 2026年12月31日でサポート終了予定のため、8.3 以上が望ましいです。
- 4 8.1 以下を選んでいる場合は、8.3 以上への切替を計画する**
独自修正が当たっていても、今後の欠陥は直らないおそれがあります。システムをまたぐ切替は、テーマ・プラグインが対応しておらず、表示崩れやエラーが出る恐れがあります。**事前にバックアップ**を取り、可能ならテスト環境 (ステージング) で確認し、プラグイン・テーマを先に最新にしてから切り替えます。
- 5 切替・適用後に動作を確認する (5 章)**

WordPress 管理画面の「ツール」→「サイトヘルス」→「情報」→「サーバー」で、サイトで動いている PHP の版を確認できます。WordPress が推奨する PHP の版は wordpress.org/about/requirements/ で確認してください。

主なレンタルサーバー各社の告知 (2026年10月25日 14時時点で確認)

事業者	告知の内容 (確認できた範囲)
エックスサーバー	5.6～8.5は全サーバーで適用完了 (10/22)、5.1～5.5は過半数で完了 (10/23)。5.6～8.1は版を変えずに対策し、急いで版を変える必要はないと案内。管理画面等は10/22から順次再開。VPS は利用者が更新。
Xserverビジネス	エックスサーバーと同一内容。
さくらのレンタルサーバ	選べる全バージョン (8.3～5.2) で対応完了。緊急の対応は不要としつつ、最新版への移行を推奨。緊急メンテナンスは10/23までに終了。
ロリポップ!	全バージョンに修正を適用し、10/22 13時ごろ表示を再開。session.upload_progress を無効化 (動作確認を依頼)。8.1以下は応急的とし8.2以降への切替を依頼。10/24から新規申し込み等を予防的に停止中。
ConoHa WING	全バージョンに適用し10/22 20:45に完了。番号は変わらない場合があるが適用済みで、版変更は不要。10/24から新規申し込みを停止中 (理由の記載なし)。

※ 利用者側の作業の要否は、各社のお知らせ本文で作業の直前に必ず確認してください。

3 VPS・自社サーバーの場合: Claude Code を使った確認の流れ

VPS や自社サーバーでは、担当者が OS のパッケージ更新で PHP を修正版にし、PHP-FPM/Apache を再起動します。Claude Code には「調べる → 提案する → 確かめる」の3段階で依頼し、**変更を伴う操作は1つずつ人が確認してから**実行させます。

必ず守る Claude Code の権限確認(コマンド実行前の許可)は有効にしたまま使います。本番サーバーでは自動承認の設定や、確認を省略するモードを使わないでください。提示されたコマンドは内容を読んでから許可します。

始める前に

- サイトのファイル・データベース・設定ファイルのバックアップを取得し、戻し方を確認しておく
- 可能なら、本番と同じ構成のテスト環境で先に試す(8.1 以下から 8.3 以上へシステムをまたぐ場合は特に。テーマ・プラグインの非対応で表示崩れやエラーが出る恐れ)
- 作業時間帯と、うまくいかなかったときに一時停止する判断基準を決めておく
- 認証情報(パスワード・APIキー)や顧客データをプロンプトに貼らない
- 作業前に VPS のスナップショットを取る。10/23 の推奨設定(`session.upload_progress.enabled=0`)の要否は保守会社と判断(3件目は修正版でも未修正)

STEP 1 現状を調べる(変更なし)

このサーバーで動いているPHPの版・SAPI (PHP-FPM/Apache+mod_php 等) ・ディストリビューションのパッケージ版を調べ、PHP2Shell (CVE-2026-109618/CVE-2026-109619) の修正済みかどうかを判定して。ディストリ版は `php -v` の番号が変わらないので、パッケージの版とディストリの公式告知で判定して。複数のPHPが入っている場合は、Webサイトで実際に使われているものを特定して。まだ何も変更しないで。調べた結果と判定の根拠だけを報告して。

ねらい: SSH の `php -v` とサイトで動く版が違うことがあるため、実際に使われている PHP とその版を特定させる。

STEP 2 更新手順を提案させる(実行は1つずつ確認)

修正版への更新手順を提案して。バックアップの取り方、更新するパッケージ、PHP-FPM/Apache の再起動、うまくいかなかったときの戻し方を含めて。各コマンドは実行前に必ず私に確認を取って。確認なしに実行しないで。

ねらい: 手順と戻し方を先に文章で出させ、人が読んで納得してから1つずつ実行する。

STEP 3 更新後に確かめる

更新後、サイトの主要ページ(トップ・会社概要・お問い合わせ等)とフォームのページが HTTP 200 で返るか確かめて。あわせて、PHP のパッケージ版が修正版になったこと、PHP-FPM/Apache が再起動済みであることを再確認して。フォームの送信テストをする場合は、実在のお客様のデータを使わないで。

ねらい: 「更新した」と「サイトが動く」を別々に確かめる。

4 制作会社・サーバー会社への確認メール文例

〔〕内を書き換えてお使いください。先に各社のお知らせを確認し、書かれていないことを問い合わせると、回答が早くなります。

制作会社・保守会社あて

件名：【ご確認のお願い】PHPの脆弱性（PHP2Shell）への対応状況について

〔制作会社名〕
〔ご担当者名〕様

いつもお世話になっております。〔自社名〕の〔氏名〕です。

10月21日に修正版が公開されたPHPの重大な脆弱性（通称 PHP2Shell、CVE-2026-109618／CVE-2026-109619）について、弊社サイトの対応状況を確認させてください。

対象サイト：〔URL／ドメインをすべて記載〕

1. 各サイトで使われているPHPのバージョン（系統）
2. 修正版（8.5.12／8.4.27／8.3.36／8.2.35以降）への更新の要否と、完了日（予定日）
3. 8.1以下の場合、8.3以上への切替の可否と、表示崩れ等の影響の見込み
4. 更新後の動作確認（主要ページ・お問い合わせフォーム）の結果
5. 今回の対応が保守契約の範囲内か、別途費用が必要か

お忙しいところ恐縮ですが、〔月日〕までにご回答いただけますと幸いです。
どうぞよろしくお願いいたします。

サーバー会社あて

件名：PHPの脆弱性（CVE-2026-109618／CVE-2026-109619）対応についての確認

〔サーバー会社名〕 ご担当者様

〔契約者名〕（契約ID／サーバーID：〔記載〕）の〔氏名〕です。

PHPの脆弱性（CVE-2026-109618／CVE-2026-109619）について、次の点を教えてください。

1. 契約中のサーバーへの修正版の適用状況（完了日時）
2. 利用者側に必要な作業の有無（PHPバージョンの切替など）
3. 8.1以下のバージョンを選んでいる場合の扱い

対象ドメイン：〔ドメインをすべて記載〕

よろしくお願いいたします。

5 更新後の確認項目

「更新した」と「サイトが正しく動く」は別物です。次の項目を1つずつ確かめ、日時と確認者を記録してください。

	確認項目	確認のしかた・ポイント
☐	PHPの版が修正版になった	共用サーバーはお知らせで「適用済み」かを確認（版を変えずに修正する会社では番号が変わらない）。VPS 等はパッケージの版で判定（ディストリ版は <code>php -v</code> の番号が変わらない）
☐	PHP-FPM／Apache を再起動した	VPS・自社サーバーの場合。更新後の再起動が必要
☐	すべての対象ドメインで確認した	PHP の版はドメインごとに設定されている
☐	トップページ・主要ページが表示される	スマートフォンとパソコンの両方で。表示崩れ・エラー表示がないか
☐	お問い合わせフォームが動く	入力 → 確認 → 送信まで。自動返信メールと通知メールが届くか（テスト用の宛先で）
☐	管理画面にログインできる	WordPress 等の管理画面。プラグインのエラー表示がないか
☐	見覚えのない管理者ユーザー・ファイル・ページの改ざんがないか	公表の4日前から攻撃の試みが観測され、JPCERT/CC も侵害有無の調査を求めているため確認する。不安があれば制作会社・専門家に調べてもらう
☐	予約・決済・会員機能、ファイルのアップロード（ある場合）	お客様が使う主要な機能を一通り。対策でアップロード進捗の機能を止めたサーバー会社もあるため、添付・画像投稿も確認
☐	一時停止していた場合は再開した	再開後も上記を確認
☐	8.2 を使っている場合の次の予定	8.2 は 2026年12月31日でサポート終了予定。年内に 8.3 以上へ切り替える計画を立てる

すぐ更新できない場合

高市総理は、すぐ適用できない場合はウェブサイト等の一時停止もリスク低減の有効策の一つと言及しています。止める場合は、WordPress の「メンテナンスモード」プラグインではなく**サーバー側**で止めます（メンテナンスモードでは PHP 本体の脆弱性は防げません）。WAF や暫定設定は「つなぎ」で、PHP 公式は更新だけが安全な選択としています。

6 参考リンク(一次情報)

- **PHP公式(セキュリティリリース告知)**
<https://www.php.net/archive/2026.php#2026-10-21-5>
- **GitHub Security Advisory** (CVE-2026-109618／CVE-2026-109619)
<https://github.com/php/php-src/security/advisories/GHSA-w8hw-w9fx-j79w>
<https://github.com/php/php-src/security/advisories/GHSA-6wmf-4rv5-p3rp>
- **発見者 Calif**
<https://calif.io/php2shell/>
- **Wiz Research**
<https://www.wiz.io/blog/php2shell-php-rce>
- **PHP公式(10/23 関連する3件目 CVE-2026-115560 の告知)**
<https://www.php.net/archive/2026.php#2026-10-23-1>
- **IPA「PHPの脆弱性対策について」(10/22)**
<https://www.ipa.go.jp/security/security-alert/2026/alert20261022.html>
- **JPCERT/CC 注意喚起(侵害調査の観点を含む、10/22)**
<https://www.jpcert.or.jp/at/2026/at260033.html>
- **高市総理の投稿(X)**
https://x.com/takaichi_sanae/status/2112890642590564386
- **AlmaLinux(ディストリ版の判定と再起動)**
<https://almalinux.org/blog/2026-10-21-php2shell-cve-2026-109618-cve-2026-109619/>
- **Cloudflare(WAFルールの展開)**
<https://blog.cloudflare.com/php-vulnerabilities-waf-protection>
- **CERT-EU Advisory 2026-018**
<https://cert.europa.eu/publications/security-advisories/2026-018/>
- **カナダ CCCS AL26-026**
<https://www.cyber.gc.ca/en/alerts-advisories/al26-026-critical-vulnerabilities-impacting-php-cve-2026-109618-cve-2026-109619>
- **NCSC-NL(機器組み込みのPHPを含む注意喚起)**
<https://github.com/NCSC-NL/php2shell>
- **WordPress の推奨環境**
<https://wordpress.org/about/requirements/>

レンタルサーバー各社のお知らせ

- **エックスサーバー** https://www.xserver.ne.jp/news_detail.php?view_id=19734
- **Xserverビジネス** https://business.xserver.ne.jp/news/detail.php?view_id=19734
- **さくらインターネット** <https://help.sakura.ad.jp/notification/n-2700>
- **ロリポップ!** <https://lolipop.jp/info/news/8239/>
- **ConoHa WING** <https://www.conoha.jp/wing/news/?ap=2015054909>
(10/24の告知) <https://www.conoha.jp/wing/news/?ap=2015054918>

※ 本資料は 2026年10月25日時点で確認できた公開情報にもとづいています(初版は10月22日時点)。最新の情報は各リンク先でご確認ください。