WordPressのためのPHP脆弱性 対策マニュアル v1.1

2026年10月22日版　株式会社スターストリーム・スタジオ

このマニュアルの使い方

2026年10月21日、PHP公式が重大な脆弱性2件（CVE-2026-109618・CVE-2026-109619）をふさいだ修正版を出しました。**ログインしていない人が、外からサーバーにプログラムを動かさせるおそれのある種類**です（深刻度は10段階の9.2）。

v1.0 をお読みいただいた方から多くのご質問をいただきました。言葉が足りなかったところを補い、v1.1 として書き直しています。特に大事な3つを先に書きます。

1. **管理画面だけの話ではありません。**PHPで動くページなら、公開しているページも入口になります
2. **レンタルサーバーなら放っておいてよい、ではありません。**サーバー会社の対応は会社ごとに違います。「どの版を・いつ直したか」を確かめ、自分の画面で番号が上がったことを見るまでが対策です
3. **今日中に修正版にできないなら、サイトをいったん止めることも選びます。**WordPress公式も、海外の公的機関のこの勧告を紹介しています

上から順に印（☐ → ☑）を付けて進めてください。

1. まず知っておくこと

どこが危ないのか

欠陥は、PHPが**届いたリクエストを読み解く部分**にあります。WordPressやプラグインのプログラムが動く**前**の段階です。そのため次のことが言えます。

- PHPで動くページなら、トップページ・記事・問い合わせフォームなど、**公開しているページも入口になる**
- **管理画面を閉じる・管理画面にだけパスワードや接続元の制限をかける、では守れない**
- **WordPress本体・プラグイン・テーマの更新では直らない。**直すのはPHPそのもの

- **WordPressの「メンテナンスモード」のプラグインも、止めたことにはならない**（PHPが動いたあとに画面を出しているため）

どの版が対象か

PHPの版	修正が入った番号（これ以上なら直っている）
8.5	**8.5.12**
8.4	**8.4.27**
8.3	**8.3.36**
8.2	**8.2.35**（8.2は2026年12月31日でサポート終了）
8.1・8.0・7.x 以前	**対象。ただしPHP公式からの修正版は出ない**（影響を受けない、ではない）

よく見かける言い方と、本当のところ

言い方	本当のところ
管理画面を閉じれば大丈夫	× 公開ページも入口。閉じるならサイト全体を止める
WordPressを最新にすれば大丈夫	× 直すのはPHP。WordPress公式も「WordPressの更新は不要・予定なし」
レンタルサーバーなら何もしなくてよい	△ 会社が直すことが多いが、時期と範囲は会社次第。自分で確かめる
WAF・Cloudflareを通しているから大丈夫	△ 補助にはなるが、PHP公式は「完全に直すのは更新だけ」
8.1以前は関係ない	× 影響を受ける。公式の修正版が出ないぶん、むしろ急ぐ
設定を変えれば防げる	△ 公式の「つなぎの設定」は既知の経路を減らすだけ。更新の代わりにならない

2. 今日やること（10分）

☐ **WordPressの管理画面で、PHPの版を見た**

「ツール」→「サイトヘルス」→ 上の「情報」→「サーバー」。次の2つを書き留めます。

PHPバージョン（　　.　　.　　）　PHP SAPI（　　）　見た日（　　月　　日）



PHPの番号を見る場所（実際の画面）

エックスサーバーなら、サーバーパネルの「PHP Ver.切替」でも番号が分かります（WordPressに入れないときの別の道）。

PHP SAPI が `apache2handler` のときは、いちばん急ぎます。この方式（mod_php）で、外から完全に乗っ取れることが確かめられています。`fpm-fcgi` や `litespeed` でも対象であることに変わりはありません。

☐ **1章の表で、修正が入った番号以上かを見た**

以上なら、6章（確認）へ。足りなければ下へ進みます。

☐ **サイトを置いている場所を書き留めた**

☐ レンタルサーバー（会社名：　　）

☐ VPS・クラウド・自分のサーバー（　　）

☐ 分からない（制作会社・担当者に今日中に確かめる：　　）

3. 早見表 — 今日のうちに、どこまでやるか

今の状態	今日やること	進む章
修正が入った番号以上	済み。念のため6章	6章
レンタルサーバー・8.2以上・番号が足りない	会社のお知らせで、直す日時を確かめる。**今日中に直る予定が出ていなければ、7章で止めるかを決める**	4章 → 7章
レンタルサーバー・8.1以前	今日、8.3以上へ切り替える。切り替えられなければ止める	4章 → 7章
VPS・自分のサーバー	今日、更新して再起動する。できなければ止める	5章 → 7章
置き場所も担当者も分からない	分かるまで、止めることを考える	7章

4. レンタルサーバーの人

修正の入ったPHPをサーバーに入れるのは、サーバー会社です。ただし対応の早さと範囲は会社ごとに違います。**エックスサーバーとさくらは、PHP 8.2〜8.5の修正を10月22日の朝までに入れ終えた**と発表しています。エックスサーバーかさくらで8.2以上なら、やることは番号を1回見るだけです。一方で、8.2〜8.5は順次、それ以外は調整中とした会社もあります。サーバーを止めて更新し、古い版を強制的に上げた会社もありました。

エックスサーバーの管理画面に入れないときは：エックスサーバーは21日16時から、予防のためにサーバーパネルなど自社の管理画面を止めていました。乗っ取りではなく、サイトの表示もそのままです。22日の朝から順に戻っています。重いときは時間をおいて開いてください。

☐ **サーバー会社の公式サイトで、今回の件のお知らせを開いた**
　ブックマークか、自分で検索して開く。メールのリンクからは開かない。

☐ **お知らせから、次の3つを書き留めた**
　どの版を直すか（　　）　いつ直すか・直したか（　　月　　日　　時）　利用者に求めていること（　　）

☐ **お知らせに自分の版が入っていない、または日時が書かれていないときは、サポートに問い合わせた**
　「PHP ○.○ を使っています。CVE-2026-109618とCVE-2026-109619の修正はいつ入りますか」と聞けば通じます。

☐ **会社が「直した」と出したあと、サイトヘルスで番号が上がったことを見た**
　お知らせだけで済ませない。自分の画面の番号が正です。

サーバー会社の管理画面が止まっていることについて：いくつかの会社が、自社の管理画面やサイトを一時的に止めました。会社側を守るための措置です。**止まっている間も、あなたのサイトは表示され、PHPも古い番号のまま動いています。**

8.1以前を使っている人（今日、8.3へ上げる）

作業の前に必ずバックアップを取ります。古いプラグインやテーマが新しいPHPに対応しておらず、画面が真っ白になることがあります。

☐ **1. WordPressのバックアップを取った**（ファイルとデータベース。手元のパソコンにも保存）
☐ **2. プラグインとテーマを最新にした**（何年も更新されていないものは書き出す：　　）
☐ **3. サーバーの管理画面で、PHPを8.3以上に切り替えた**（「PHP Ver.切替」「PHP設定」などの名前）
☐ **4. 表示を確かめた**　☐ トップ　☐ 記事　☐ 固定ページ　☐ フォームの送信　☐ 管理画面へのログイン　☐ スマホ
☐ **5. おかしければ、原因が分かるまでサイトを止めた**
　元の版に戻すと、穴の開いた状態に戻ります。戻すのではなく、7章の方法で止めたうえで、プラグインを1つずつ止めて原因を探します。

5. VPS・自分のサーバーの人

更新するのは自分です。

☐ **1. バックアップを取った**（WordPressのファイルとデータベース、できればサーバーのスナップショットも）
☐ **2. OSのパッケージを更新した**（Debian・Ubuntuなど主な配布元は修正済みの版を出しています）
☐ **3. PHP-FPM と Webサーバーを再起動した**（再起動しないと、古いPHPが動き続けます）
☐ **4. `php -v` と サイトヘルスの両方で、修正が入った番号になったことを確かめた**

remi（rpms.remirepo.net）からPHPを入れている場合：公開された日の時点で更新が出ていなかったため、PHP公式は配布元のパッケージか、ソースからのビルドへの切り替えを強く勧めています。

8.1以前を自分で動かしている場合：PHP公式は 7.4・8.0・8.1 向けに最小限の修正（ソース）を出しています。配布元やサポート契約先が修正を出していないかを確かめ、無ければサポート中の版へ上げます。**WordPress公式は、8.2より前を自分で動かしているなら、サーバーを止めることも考えるよう書いています。**

すぐ更新できないときの「つなぎの設定」（PHP公式の案内）

更新の代わりにはなりません。既知の攻撃の道筋を減らすだけで、別の道筋は残ります。php.ini・PHP-FPMの設定・Webサーバーの設定に書き、WordPress側（.user.ini や ini_set）には頼らないこと、という注意つきです。

```
session.upload_progress.enabled = 0
post_max_size = 8M          ; ファイルのアップロードが要るなら 32M
; upload_max_filesize は post_max_size より小さくする
memory_limit = -1           ; アプリ側から上書きできない形で設定する
fatal_error_backtraces = 0  ; PHP 8.5 のときだけ
```

☐ 設定を書いた　☐ PHPのワーカーを再起動した　☐ 更新の予定日を決めた（　　月　　日）

6. 修正が入ったかを確かめる

☐ サイトヘルスの「PHPバージョン」を、もう一度見た（見た日：　　月　　日）
☐ 1章の「修正が入った番号」以上になっていた　→ **完了です**

☐ なっていない（レンタルサーバー）→ 4章の問い合わせへ。今日中に直らないなら7章
☐ なっていない（自分のサーバー）→ 5章をやり直す

念のため見ておくこと： 直る前の期間に、見覚えのない管理者ユーザー・見覚えのないプラグインやファイルが増えていないか。あれば、制作会社やサーバー会社に相談してください。

7. 今日中に直せないときは、いったん止める

止めると、その間は問い合わせも売上も止まります。それでも、**乗っ取られたサイトは、止めるより長く、大きく止まります。**迷ったら止める側を選んでください。

止める目安

☐ 修正が入った番号になっておらず、今日中に直る見込みもない
☐ 8.1以前で、今日中に8.3以上へ切り替えられない
☐ PHP SAPI が `apache2handler` で、番号が足りない
☐ サイトの置き場所・担当者が分からず、確かめようがない

ひとつでも当てはまれば、止めることを考えます。

止め方（PHPまでリクエストが届かない形で）

- **サーバー会社の管理画面で、そのサイト（ドメイン）の公開を止める・アクセス制限をかける**
  サイト全体にベーシック認証や接続元の制限をかけると、外からのリクエストがPHPまで届きません。**管理画面（wp-admin）だけにかけるのとは別物**です
- 止め方が分からなければ、サーバー会社のサポートに「CVE-2026-109618の修正が入るまで、サイトを止めたい」と相談する
- **WordPressのメンテナンスモードのプラグインは、止めたことになりません**（1章）

☐ 止めた（日時：　　月　　日　　時）　☐ お客さまや関係者に知らせた　☐ 再開の条件（修正の番号を確かめたら）を決めた

8. 複数のサイトを確かめる表

制作を頼まれているお客さまのサイトや、自分の別のサイトをまとめて確かめるときに使ってください。

サイト名	置き場所	PHP（確認日）	SAPI	早見表の行	修正版を確認
					☐
					☐
					☐
					☐
					☐

9. 便乗のメールにだまされないための5つ

大きなセキュリティのニュースのあとは、それに便乗した偽のメールが出やすくなります。

☐「脆弱性が見つかりました。こちらから更新してください」のリンクは押さない
☐「アカウントが停止されます」「24時間以内に」と急がせるメールほど疑う
☐ サーバー会社のお知らせは、ブックマークか自分で検索した公式サイトで見る
☐ PHPの更新のために、メールのリンク先でパスワードやカード番号を入れることはない
☐ WordPressの管理画面のパスワードを、ほかのサービスと使い回していない（使い回していたら変えて、二段階認証も入れる）

出典

- PHP公式「Security advisory: Critical remote code execution vulnerabilities, update now」（2026年10月21日）https://www.php.net/archive/2026.php
- PHP公式のセキュリティ勧告 GHSA-w8hw-w9fx-j79w（CVE-2026-109618）https://github.com/php/php-src/security/advisories/GHSA-w8hw-w9fx-j79w
- PHP公式のセキュリティ勧告 GHSA-6wmf-4rv5-p3rp（CVE-2026-109619）https://github.com/php/php-src/security/advisories/GHSA-6wmf-4rv5-p3rp
- WordPress公式「Critical PHP security release」（2026年10月21日）https://wordpress.org/news/2026/10/critical-php-security-release/
- IPA「【事前準備のお願い】PHPのセキュリティリリース公開予定について」（2026年10月21日）https://www.ipa.go.jp/security/security-alert/2026/pre-alert20261021.html

- さくらインターネット・カゴヤ・ジャパン・IDCフロンティア（Zenlogic）の各社のお知らせ（2026年10月21〜22日）

このマニュアルは2026年10月22日時点の公式の発表をもとにしています。サーバー会社ごとの対応は日々変わるので、必ず各社の公式のお知らせで確かめてください。