

令和8年10月22日

関係事業者団体代表者 様

警察庁

PHP のぜい弱性（CVSSv4：9.2）に関する注意喚起について

NCO（国家サイバー統括室）から、PHP Foundation セキュリティチームが『重大な脆弱性 2 件』の公開についての情報提供がありました。脆弱性の詳細については、悪用の恐れがあるため公開されてはいませんが、関連情報については添付ファイルをご参考ください。

この脆弱性の影響範囲が大きいとされ、日本時間 2026 年 10 月 21 日 23:00 に修正されたバージョンがリリースされております。

貴団体様又は加盟事業者様で整備したシステムにおいて当該製品を利用している場合にあっては、システムに対する影響を検討の上、至急、対処をお願いします。

PHP は WordPress 等ウェブアプリケーションに関連するプログラム言語です。多くのウェブサイトやアプリケーションが多大な影響を受けますので、幅広く周知をお願いいたします。

【対象】

PHP 5 以降のすべてのバージョン

【ぜい弱性】

本脆弱性の悪用に成功すると、認証をパスして攻撃者による不正なコード実行につながる可能性があります。

【対策】

対象のバージョンに合わせて修正されたソフトウェアをダウンロードし、インストールしてください。

修正されたバージョンは日本時間 2026 年 10 月 21 日 23:00 にリリースされています。

(参考)【CVSSv4】とは

件名に記載しております「CVSSv4 (Common Vulnerability Scoring System Version 4)」とは、情報セキュリティの脆弱性の深刻度(危険度)を0.0~10.0のスコアとして数値化した国際的な評価体系です。

数値が大きいほど危険性が大きく、速やかな対応が必要です。

# 情報セキュリティ

[トップページ](#) > [情報セキュリティ](#) > [重要なセキュリティ情報](#) > [2026年度](#) >

【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

## 【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

公開日：2026年10月21日

注釈：追記すべき情報がある場合には、その都度このページを更新する予定です。

本情報の対象となる2つの脆弱性について、現時点でIPAが悪用した攻撃を確認しているわけではありません。セキュリティリリースの公開後、速やかに適用できるよう、事前準備をお願いするものです。

PHPの脆弱性については、2024年7月にも悪用した攻撃に関する注意喚起を行っています（[脚注1](#)）。今回の脆弱性についても悪用されるおそれがあるため、予防的に情報を発信しています。

### 概要

The PHP Groupが提供するPHPについて、2026年10月21日 23:00（日本時間）に、2つの脆弱性に対するセキュリティリリースを公開する予定であることが発表されています。

・ [Upcoming Critical PHP Security Release](#) 

また、脆弱性の詳細が公開された場合や、実際に悪用が確認された場合には、公開予定日時を前倒しする可能性がありますとのことです。

本情報の発信時点では、セキュリティリリースは公開されておらず、これらの脆弱性の影響を受ける詳細なバージョン情報や、修正バージョン情報なども確認できていません。

PHPを利用しているウェブサイトの運営者や、PHPを利用したウェブアプリケーションの開発者の皆様は、今後The PHP Groupが公開する情報を注視し、公開後、速やかにセキュリティリリースを適用するなどの対応ができるよう、事前準備をお願いします。可能な範囲で、開発・運用しているプログラムのうち、PHPを利用しているものを棚卸ししてください。

また、PHPは、ウェブアプリケーションだけでなく、ソフトウェア製品やネットワーク機器などの内部でも利用されている場合があります。

製品や機器の内部でのPHPの利用状況は、利用者側では把握できない場合があります。まずは、製品のマニュアルや、開発元・提供元が公開するセキュリティ情報などをご確認ください。公開情報などからPHPの利用が把握できている製品については、今後の情報を注視し、影響や対策が公表された場合に速やかに対応できるよう準備をお願いします。

現時点で、利用しているすべての製品について、内部でのPHPの利用有無を個別に確認することをお願いするものではありません。PHPの利用状況が不明な製品についても、引き続き開発元・提供元からの情報をご確認ください。

なお、これらの2つの脆弱性について、CERT-EUは、複数の情報源に基づき、CVE識別子をCVE-2026-109618およびCVE-2026-109619とする注意喚起を公表しています。また、同注意喚起では、PHP 5以降が影響を受けるとされています。

・ [Critical Vulnerabilities in PHP](#) 

## 影響を受けるシステム

・ PHP

影響を受ける詳細なバージョン情報は、現時点では確認できていません。なお、CERT-EUの注意喚起では、PHP 5以降が影響を受けると記載されています。

## 対策

### 脆弱性の解消 - 修正プログラムの適用

現時点では、修正プログラムは公開されていません。今後The PHP Groupや各製品の開発元・提供元が公開する情報を確認し、修正プログラムの公開後、速やかに適用できるよう準備してください。

## 推奨対応

自組織で開発・運用しているプログラムや、利用している製品について、PHPの利用状況を可能な範囲で棚卸しし、速やかな対策の適用に向けて準備してください。

IPAが確認したところでは、サポート終了の古いPHPを利用し続けているウェブサイト・ウェブサービスも見受けられます。最近の情勢を踏まえると、攻撃者はこれらの脆弱性を悪用し、極めて短時間で攻撃を実行する可能性もあるため、パッチの公表後、可及的速やかに適用できるよう準備をお願いします。

## 脚注

脚注1 [PHPの脆弱性（CVE-2024-4577）を狙う攻撃について](#)

## お問い合わせ先

## ■ IPA セキュリティセンター

E-mail [vuln-inq@ipa.go.jp](mailto:vuln-inq@ipa.go.jp)

注釈：個別のシステムおよび環境に関するご質問を頂いても回答ができない場合があります。詳しくは製品ベンダなどにお問合せください。

## 更新履歴

2026年10月21日 掲載

### 書籍・刊行物



現在販売中のIPAの書籍・刊行物を掲載しています。

### 採用情報



IPAの採用に関する情報をご紹介します。

### 調達情報



IPAの調達・契約情報をご案内します。



独立行政法人  
情報処理推進機構  
Innovation Platform Agency, Japan

Beyond Digital

〒113-6591  
東京都文京区本駒込二丁目28番8号  
文京グリーンコートセンターオフィス（総合受付13階）

セキュリティ対策Lab / セキュリティニュース / 情報セキュリティ  
/ PHPに2件の重大な脆弱性、10月21日23時に緊急修正予定 CVSS  
9.2、全利用者に更新準備を要請

# PHPに2件の重大な脆弱性、10月21日23時に緊急修正予定 CVSS 9.2、全利用者に更新準備を要請

セキュリティニュース

投稿日時: 2026年10月21日 更新日時: 2026年10月21日



PHP開発チームは2026年10月20日、PHPに存在する重大な脆弱性2件について、緊急のセキュリティ更新を予定していると発表しました。公開予定日時は10月21日14時（UTC）で、日本時間では同日23時です。2件とも深刻度はCVSS v4.0で9.2（Critical）と評価されており、開発チームはPHP利用者に対して、修正版が公開され次第更新できるよう準備を呼びかけています。

欧州連合のCERT-EUも10月21日付で注意喚起を公表しました。PHPの脆弱性をめぐっては、リモートコード実行（RCE）の可能性やCVE

番号に関する情報が先行して広がっていますが、PHP開発チームは現段階で具体的な悪用条件、影響バージョン、修正版を正式に発表していません。

## 目次 [hide]

1. PHPの重大脆弱性2件に関するサマリー
2. PHP開発チームが緊急の事前告知、公開前倒しの可能性も
3. CVE-2026-109618・CVE-2026-109619とRCE報告の扱い
4. WordPress・ECサイトなど、PHPを使うサービスの運用に影響
5. PHP利用企業が修正版の公開前に確認すること
6. 修正公開後に確認する公式情報
7. 出典

## PHPの重大脆弱性2件に関するサマリー

- PHP開発チームは2026年10月20日、重大な脆弱性2件を修正するセキュリティ更新を予告しました。
- 更新の公開予定は10月21日14時（UTC）、日本時間の10月21日23時です。
- 深刻度は2件ともCVSS v4.0で9.2（Critical）です。
- 開発チームは、脆弱性の詳細が先に公開されるか実際の悪用が確認された場合、予定を前倒しする可能性があると説明しています。
- CERT-EUは、PHPを利用するシステムの特定と速やかな更新の準備を推奨しています。
- 「CVE-2026-109618」「CVE-2026-109619」やRCEとの関連は外部のセキュリティ調査情報で示されていますが、PHP公式告知

では識別子や攻撃条件を明示していません。

- PHP 5以降が広く影響するとの情報もありますが、正式な影響範囲は更新公開時の開発元発表を待つ必要があります。

| 項目          | 2026年10月21日時点で確認できる内容       |
|-------------|-----------------------------|
| 発表元         | PHP開発チーム                    |
| 事前告知日       | 2026年10月20日                 |
| 対象          | PHPの重大な脆弱性2件                |
| 公式の深刻度      | いずれもCVSS v4.0 9.2（Critical） |
| セキュリティ更新の予定 | 2026年10月21日23時（日本時間）        |
| 技術的な詳細      | 更新公開時に公表予定                  |
| 影響バージョン・修正版 | PHP公式では更新公開時に発表予定           |
| 実務上の対応      | 利用資産の特定、更新手順と作業時間の確保、監視の強化  |

## PHP開発チームが緊急の事前告知、公開前倒しの可能性も

PHP公式サイトに掲載された「Upcoming Critical PHP Security Release」によると、今回の更新は重大な脆弱性2件に対応するものです。開発チームは通常の詳細なアドバイザリを出す前に、利用者へ更新準備を促す形で警告を発しました。

公式告知では、詳細情報や影響するPHPのバージョン、修正済みリリースについてはセキュリティ更新と同時に公開すると説明しています。したがって、10月20日に発表された警告を、すでに更新プログラムが配布されたという意味で受け取るべきではありません。

一方、情報が事前に広がっている状況を踏まえ、開発チームは脆弱性の詳細が公表された場合や、実際の攻撃が確認された場合にはリリースを早める方針も示しています。更新作業を翌日以降の通常保守に回すのではなく、公開直後に適用可否を判断できる体制が必要になります。

## CVE-2026-109618・CVE-2026-109619とRCE報告の扱い

セキュリティ企業watchTowrは、CVE-2026-109618およびCVE-2026-109619という識別子を挙げ、PHPのリモートコード実行につながる脆弱性であると報告しています。CERT-EUも10月21日付の注意喚起で両CVEを取り上げ、PHPで動作する公開システムへの影響を警戒するよう促しました。

RCEとは、脆弱性の条件を満たしたシステム上で、攻撃者が遠隔から不正なコードを実行できる状態を指します。仮に公開Webサーバーから悪用できる条件であれば、Webサイトの改ざんや情報窃取、他の内部システムへの侵入の足掛かりとなる可能性があります。ただし、これらは攻撃が成立した場合の一般的な危険性であり、今回の2件で同じ経路が実際に利用可能と確認されたものではありません。

情報の出所によって深刻度にも違いがあります。外部の一部報告では「CVSS 10.0」とされていますが、PHP開発チームが公表した値は**CVSS v4.0で9.2**です。本件の深刻度を記事や社内向け注意喚起に記載する際は、公式値と評価規格を明記する必要があります。

また、PHP 5以降の幅広いバージョンに影響するとの見解も出ていますが、PHPプロジェクトは影響範囲をまだ確定公表していません。

PHP 7系・8系のどちらも無条件に脆弱であると断定したり、特定バージョンなら安全だと判断したりする段階ではありません。

#### 関連資料

### AI時代の脆弱性管理・パッチ管理 | 運用見直しのポイントと製品選定の確認事項

脆弱性の優先順位付けから修復、暫定防御、パッチ管理まで、運用見直しと製品選定で確認したいポイントをまとめた資料です。

資料提供元：株式会社アズジェント

[脆弱性管理の資料を見る](#)

## WordPress・ECサイトなど、PHPを使うサービスの運用に影響

PHPはWebアプリケーションのサーバー側で処理を実行するプログラミング言語で、WordPressなどのCMSやECサイト、業務向けWebシステムでも使用されています。今回警告されているのは、個々のWordPressプラグインなどではなくPHP自体に関する脆弱性です。

PHP本体のセキュリティ修正が必要な場合、WordPress本体やテーマ、プラグインだけを更新しても対処が完了したことにはなりません。PHPの更新主体がサーバー管理者、レンタルサーバー事業者、クラウド運用部門のいずれかを確認する必要があります。

ただし、PHPを利用しているという理由だけで、すべてのWebサイトについて外部からの侵入が可能だと確定するわけではありません。影響する構成、モジュール、実行条件は公式の詳細発表に基づいて判断する必要があります。

PHP開発チームの[サポート対象バージョン一覧](#)では、2026年10月時点のサポート対象は8.2、8.3、8.4、8.5の各系統です。PHP 7.4や8.1

などのサポート終了版については、今回の更新とは別に移行計画を進める必要があります。サポート対象という事実も、今回の2件に影響しないことを保証するものではありません。

直近では2026年9月24日にもPHP 8.2～8.5向けのセキュリティリリースが公表されましたが、[9月に修正された11件の脆弱性](#)と、今回の緊急予告にある2件を同一視しないよう注意が必要です。

## PHP利用企業が修正版の公開前に確認すること

今回の警告を受け、情報システム部門とWebサイト運用担当者は次の対応を準備できます。

- 1. PHP稼働資産を把握する。** 公開Webサーバー、WordPress、業務システム、API、バッチ処理、コンテナなどで利用するPHPの系統とバージョンを記録します。サーバー上のCLI版とWebサイトが実際に使用するPHP-FPMなどのバージョンが一致するとは限らないため、稼働環境ごとに確認します。
- 2. 更新元と管理者を確認する。** Linuxディストリビューションのパッケージ、コンテナイメージ、レンタルサーバーの管理画面、アプリケーションベンダーの配布物など、利用するPHPの提供元によって更新方法が異なります。更新作業を実施する担当と通知先を決めます。
- 3. 検証・適用手順を事前に用意する。** アプリケーションとPHPの互換性、拡張モジュール、ログイン、注文・予約処理、外部API連携などの確認項目をまとめ、必要なバックアップと復旧手段を確保します。
- 4. 公開サーバーの監視を強化する。** WebサーバーとPHPのエラーログ、不自然なリクエスト、予期しないプロセスやファイル変更を監視します。ただし、今回の2件に固有の検知ルールやIOCは、公式技術情報が公表されてから確認します。
- 5. 更新できないシステムの公開範囲を再評価する。** CERT-EUは、直ちに修正できないインターネット公開アプリケーションについ

て、修正版の適用まで外部ネットワークから隔離することを検討するよう勧めています。業務上停止できない場合も、到達元制限や管理機能の非公開化など、実際に実施可能な措置を確認します。

6. **公式発表後に影響範囲を再判定する。** CVEごとの影響バージョン、利用条件、修正済みリリースを照合し、適用後には実際に稼働するPHPのバージョンとアプリケーションの動作を確認します。

WAFやCDNの利用は、攻撃の監視や一部の通信制限に役立つ場合がありますが、今回の脆弱性に対する確実な回避策が公表されたわけではありません。Webアプリケーションへの防御機能を設定済みであっても、PHP本体の更新要否を別途判断する必要があります。

多数のWebシステムを抱える組織では、外部公開状況、資産の重要度、更新可能時期を台帳で管理し、修正の優先順位を付ける方法が考えられます。資産の把握から修正確認までの流れは、[脆弱性管理の進め方](#)でも整理しています。

## 修正公開後に確認する公式情報

PHP開発チームは、更新公開時に対象バージョンと修正版、技術的詳細を説明する予定です。各組織は[PHP公式サイト](#)と[ダウンロードページ](#)に加え、利用しているOS、ホスティング事業者、コンテナイメージ提供元の更新情報を確認してください。

2026年10月21日の公開予定時刻は日本時間23時です。発表が前倒しされる可能性がある一方、予定通りの時刻に修正版が出ることも現時点での計画であり、具体的なリリース番号を先回りして記載することは避けるべきです。

## 出典

- [Upcoming Critical PHP Security Release（2026年10月20日）  
– PHP開発チーム](#)
- [PHP公式サイト・最新リリース情報 – PHP開発チーム](#)
- [Supported Versions – PHP開発チーム](#)
- [Security Advisory 2026-018: Critical Vulnerabilities in PHP –  
CERT-EU](#)
- [PHP Remote Code Execution FAQ: CVE-2026-109618 &  
CVE-2026-109619 – watchTower](#)

この記事シェアする



## メールマガジン

最新のセキュリティ情報やセキュリティ対策に関する情報をお届けします。

登録する

 Googleで優先ソースに追加

 Googleニュースで最新記事を見る

Googleアカウントへのログインが必要です

投稿者：三村