



緊急インシデント対応警告！！！！

PHPをご利用の貴社Webサイトは、高危険度の状態にあります。
至急の確認と対応をお願いいたします。

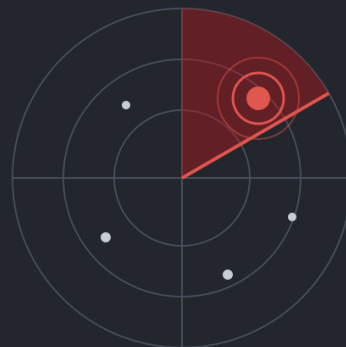
貴社のWebサイト、
“鍵のかかっていない扉”に
なっていませんか？

php2shell

PHP緊急脆弱性
いま起きていること、御社がやるべきこと

2026年10月 | お客様向け緊急解説 | CVE-2026-109618 / CVE-2026-109619

KELA Cyber Intelligence Center の観測情報にもとづく解説



Aegis Application

イージス・アプリケーション株式会社

AI・サイバーセキュリティ ソリューション

高市首相も、PHP脆弱性への緊急対応を呼びかけています



大至急のお願い

PHPを使うWebサイト・社内システム・機器の修正版適用状況を、今すぐご確認ください



内閣総理大臣 高市 早苗 氏

2026年10月21日 | X（旧Twitter）での発信

PHPに“**重大な脆弱性**”。
修正版が出たら、**速やかに適用を**。

1

世界中のWebサイトで使われるPHPに、**重大な脆弱性**が見つかった

2

修正版の公開後、**速やかに適用**できるよう準備を

3

すぐの適用が難しい場合は、**Webサイト機能の一時停止**がリスク低減に有効

出典：時事通信（nippon.com、2026年10月21日）の報道をもとに当社で要約

企業に求められていること



確認する

自社サイト・社内システム・購入機器でPHPが使われていないかを確認



すぐ直す

修正版を速やかに適用。
難しい場合は機能の一時停止も検討



見張り続ける

攻撃者の動きと情報漏えいを
KELAで継続的に監視



国内でも、対応の動きが広がっています

さくらインターネットがクラウドサービスの一部機能を一時停止して対応（2026年10月21日報道）

攻撃は、すでに始まっています

9.2 / 10

危険度は最高ランク「緊急」
(欠陥2件とも)

ログイン不要

外から通信を送るだけで
操られる恐れ

ほぼ全て

2012年公開の
PHP 5.4以降が対象

数時間

公表から攻撃者の議論開始まで
(KELA観測)



Q1 何が起きているの？

PHPの“玄関”部分に、重大な欠陥が2件。
修正版は10月21日に公開済みですが、
攻撃の“試し打ち”は世界中で続いています。



Q2 なぜ、そんなに危険なの？

**パスワードを破る必要すらなく、
細工した通信を送るだけで、
外部からサーバーを操られる恐れがあります。**



Q3 どんな被害につながるの？

**ホームページの改ざん、情報の漏えい、
ランサムウェアによる業務停止、
そして取引先へと広がる被害の連鎖。**



Q4 何をすればいいの？

- ① **PHPを最新の修正版へ、今すぐ更新**
- ② **すでに入られていないか、痕跡を確認**
- ③ **委託先サイト・購入製品のPHPも確認**
- ④ **攻撃者側を監視し、狙われていないか把握**

修正より先に、“弱点の情報”が漏れた

PHPは、Webサイトの“裏側”で動くプログラム言語です。
今回の欠陥は、その“玄関”にあたる部分で見つかりました。
御社が意識していなくても、右のような場所で
使われている可能性があります。



企業
ホームページ



ネット
ショップ



会員・
予約サイト

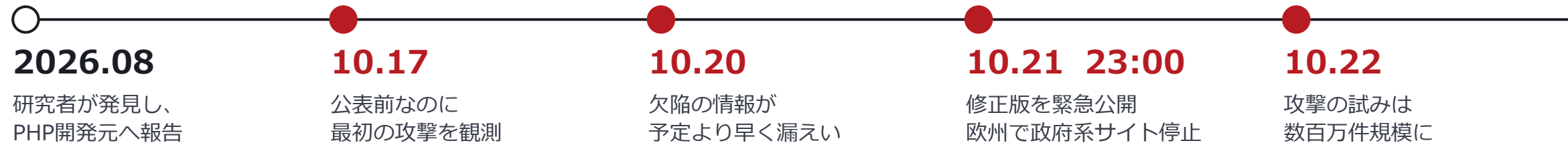


社内の
業務システム



購入した
製品・機器

これまでの経緯（日本時間）



どんな欠陥？	細工された通信で誤作動し、外部の命令を実行してしまう
どれほど危険？	危険度9.2／10点。ログイン不要で攻撃が成立
誰が対象？	PHPを使うWebサーバーのほぼ全て（PHP 5.4以降）
どう直す？	修正版へ更新（8.5.12／8.4.27／8.3.36／8.2.35） 8.1以前は公式の修正版なし → 移行が必要

 わかっていること

- 修正版は公開済み
- 標準設定で攻撃成功を実証
- 主要11ソフトで攻撃成功
- 世界中で大量の攻撃の試み

 まだわかっていないこと

- 被害企業の公表
- 米CISA「悪用確認済み」
- リストへの登録

「未確認」は
「安全」ではありません

攻撃者の世界は、すでにざわついている

闇フォーラムやチャットを常時監視するKELA CTIは、公表から数時間以内に、次の場所で議論が広がる様子を捉えました。

数時間以内

公表から議論開始まで

約150件

フォーラム・SNS等の投稿（2日間）

110件超

Telegramのメッセージ（同期間）

25以上

Telegramのチャンネル・グループ

ロシア語の闇フォーラム

Exploit.in / XSS

英語圏のフォーラム・闇市場

Cracked / BreachForums /
TierOne

php2shell
の話題

情報共有（ペースト）サイト

攻撃コードの断片が拡散

Telegram

25以上のチャンネル

図：KELA CTIが議論を確認した主な場所（KELA公表内容をもとに当社作成）

KELAの評価

“声”は大きいが、
まだ“実力”は追いついていない。
ただし、その差は
急速に縮まっている。

次の危険信号：腕のある攻撃者が
php2shell経由の侵入口を売り始めたとき。
その時点で、更新の猶予はもうない。
（KELA責任者の見解を要約）

FORUM ▶ Exploit.in

スレッド | 2026年10月20日～

PHP2Shell (CVE-2026-109618 и CVE-2026-109619)
- У кого-нибудь есть?

訳：「誰か（攻撃コードを）持っていないか？」

返信：初日だけで数十件 | 言語：ロシア語

図：KELAの観測内容をもとに当社で再構成したイメージ（実際の画面ではありません）



攻撃道具の“共有”と改良

試作の攻撃プログラムが
出回り、手直しが続く



“売り込み”も登場

「どこでも侵入可能」と謳う
宣伝も。多くは便乗商法



「誰か持っていないか？」

使える道具や、狙える先の
探し方を求める声が続出



実際の“下見”が進行中

10/21朝から、攻撃道具の
特徴を持つ通信を記録

放置すれば、被害は“階段を上るように”進む

想定シナリオ

架空のA社（製造業・従業員300名） 企業HP：WordPress / 取引先ポータル：古いPHPのまま / 通販：外部委託

※KELAが「脅威が本格化するサイン」として挙げる段階をもとに当社が構成した説明用シナリオです。実在の企業・事例ではありません。

危険度 高 想定される影響

STEP 1

いま起きている

無差別の
“下見”

攻撃道具による
探索がA社にも届く。
記録は残るが、
誰も見ていない。

確認済み：
探索の通信

STEP 2

数日～数週間後

攻撃道具が
完成に近づく

どの環境でも使える
攻撃方法が出回る。
古いPHPのポータル
には修正版がない。

KELAが監視：
汎用的な攻撃道具

STEP 3

侵入

“裏口の鍵”が
売買される

侵入専門の業者が、
A社への侵入口を
闇市場に出品する。

KELAが監視：
侵入口の販売出品

STEP 4

被害の発生

ランサムウェア・
情報漏えい

侵入口を買った犯罪
グループが社内へ。
業務停止、情報流出、
暴露をちらつかせた
脅迫へ。

KELAが監視：
ランサム集団の利用



ホームページ改ざん

偽情報・ウイルス
配布の踏み台に



情報の漏えい

顧客・取引先の
データが流出



業務の停止

ランサムウェアで
システムが停止



攻撃の“手先”に

他社攻撃の装置に
組み込まれる



取引先への連鎖

委託先・購入製品
経由で被害が拡大



信用・法的な負担

報告・説明責任、
損害賠償

まずは“更新の優先順位”を決めて、すぐ動く

STEP A | 今日から48時間で行うこと



サーバー別 パッチ適用の優先度（指針）

※期限は当社推奨の目安です

優先度	対象となるサーバー（例）	期限の目安	行うこと
最優先 A	インターネットに公開しているWebサーバー （ホームページ・ネットショップ・会員サイト） 個人情報・取引情報を扱うサーバー	即日～48時間	修正版へ更新・再起動 更新できない場合は 一時停止・遮断を検討
優先 B	取引先など社外から使う業務システム 委託先が運営するサイト PHPを内蔵した購入製品	1週間以内	委託先・メーカーに 対応状況を確認し、 修正版を受けて更新
計画 C	社内専用の業務システム 開発・検証環境、コンテナの元イメージ PHP 8.1以前の古いサーバー	1か月以内	計画的に順次更新 （環境の作り直しを含む） 古い版はサポート版へ移行

優先度を決める4つのものさし

- 

外から見えるか

インターネットに公開している？



大事な情報があるか

個人情報・取引情報を扱う？



古い版ではないか

8.1以前は公式の修正版なし



自社で直せるか

委託先・製品は確認が必要

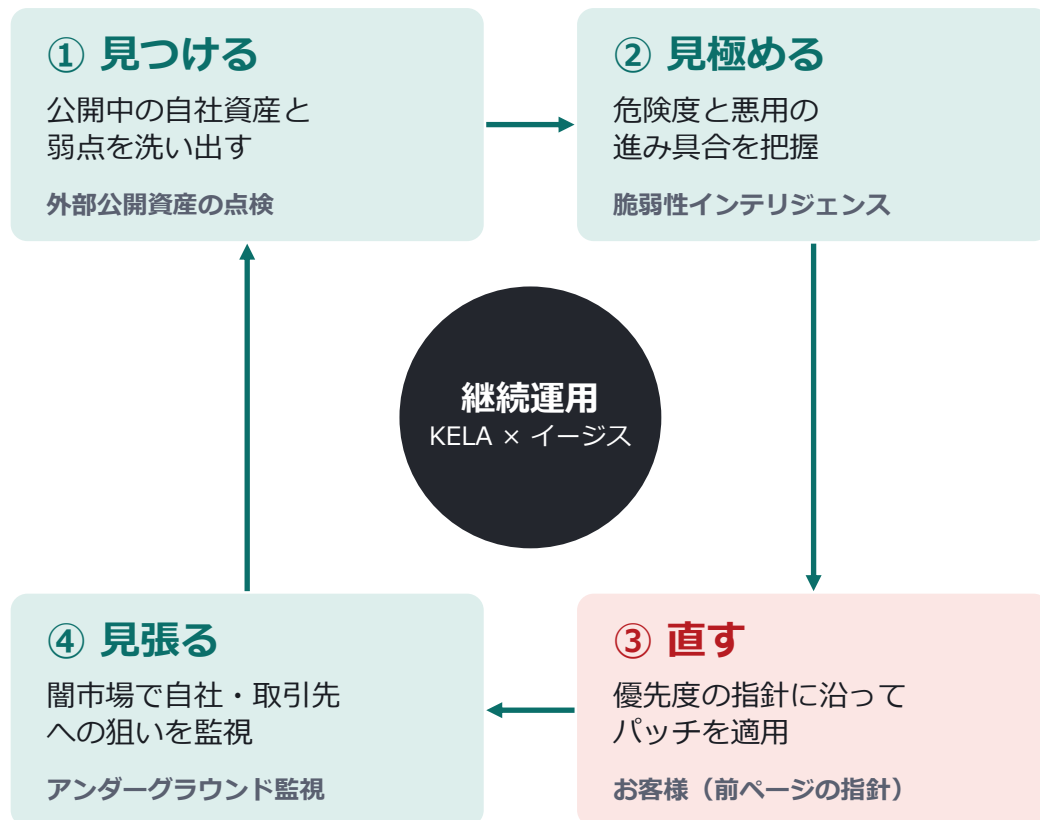
応急処置や防御装置は“つなぎ”。
根本対策は修正版への更新のみ

出典：KELA Cyber Intelligence Center ブログ（2026年10月22日 13:00 UTC時点）をもとに、イージス・アプリケーション株式会社が再構成

7

“点数”ではなく、“実際に狙われているか”で守る

STEP B | KELAで続ける4つのサイクル



VULNERABILITY INTELLIGENCE | 見える化

脆弱性インテリジェンス — 欠陥の“いまの危険度”が1画面で

危険度

悪用される可能性

悪用の進み具合

対処方法

リスクの推移

インテリジェンス・フィード

欠陥に触れたアンダーグラウンドの投稿を、そのまま確認できます。
点数から推測するのではなく、攻撃道具が議論・売買・共有されている
“現場のスレッド”を直接読めます。



外部公開資産の点検

公開中の自社資産から
弱点や危険な入口を発見



取引先リスク評価

委託先・取引先を外側から
評価し、更新を促す先を特定



アンダーグラウンド監視

自社や取引先が標的リスト・
販売・暴露投稿に出ていないか

導入効果



パッチの順番を
“狙われ度”で決められる



自社の記録では見えない
攻撃者の動きを把握できる



取引先経由のリスクにも
先回りできる

NEXT STEP | ご相談・お問い合わせ

イージス・アプリケーションが、 KELAの導入から運用まで 伴走します。

01

現状のヒアリング

PHPの利用状況と
公開資産を整理



02

試行導入（POC）

1週間で環境整備
2か月間POC、
KELAで攻撃者側を可視化



03

本格運用

KELAマネージド
サービスで継続監視



Aegis Application

イージス・アプリケーション株式会社

AI・サイバーセキュリティ ソリューション

お問い合わせ

イージス・アプリケーション株式会社 [樋口寿徳] [hisanori.higuchi@aegis-application.com]

出典：KELA Cyber Intelligence Center ブログ「php2shell」（2026年10月22日）

なぜPHPの脆弱性で、 首相が異例の緊急警告を 出したのか？

2026年10月21日夜の「大至急」要請と、
Web社会を揺るがした背景

A1

基礎知識と当夜の動き

A2

反響と検証

A3

今後の教訓



Aegis Application

イージス・アプリケーション株式会社

AI・サイバーセキュリティ ソリューション

PHPとは何か、10月21日深夜に何が起きたのか



Webサイトの約7割を動かす基盤

WordPressや決済・通販サイトの裏側で動くエンジン。
ネットの店舗で言えば「商品管理室や金庫番」に相当。



外部からの遠隔乗っ取りの脅威

細工した通信を送るだけで、外部から操られる恐れ。
攻撃者は防御装置（WAF）を迂回する手口も議論。

10月21日深夜に起きた「連動ドミノ」

10月20日



開発元が修正版を予告

PHP開発チームが、21日23時の
緊急修正版の公開を事前に告知



10月21日 21:55



首相による「大至急」の要請

Xで「今夜に対応して頂きたい
大至急のお願い」と呼びかけ



21日夕方～22日未明



主要サービスの予防停止

BASE、pixiv、ニコニコ、Cygames
のゲームなどが緊急メンテナンス



首相自らが、修正版の公開前から予防的な対応を呼びかけた異例の事例

時刻・停止事例は報道（GIGAZINE、2026年10月21日）による

なぜ大きな議論を巻き起こしたのか



評価：経営層の即断を後押し

- 通常なら承認に時間がかかる夜間停止を、
国のトップが肯定した
- 現場のエンジニアが、
即座に対処できる環境をつくった



改善点：一般ユーザーへの波及

- 「スマホをどうすればいい？」など、
一般ユーザーに不要な不安が拡散
- 技術的なメッセージの伝え方に、
課題が残る結果に

企業への示唆

トップが判断を示せば、夜間停止のような
“痛みを伴う対策”も即断できる。

だからこそ平時から、攻撃者側の動きを経営層と共有できる体制が重要です。



「先手で止める」能動的サイバー防御へ

これまで

起きてから謝る

事後対応



これから

先手で止める

能動的サイバー防御



企業・管理者側

パッチの迅速な適用と、予防的な遮断を
ためらわない体制をつくる



一般ユーザー側

操作は不要。便乗した
「偽の緊急更新詐欺」に警戒する



先手を打つために

攻撃者側の動きを常時把握し、狙われる前に手を打つ — KELAとイージスが、その体制づくりを支援します