OXFIDA

OXFIDA INSIGHT｜AI とサイバーセキュリティ

発見の加速、対応の真価

——PHP2Shell が示す企業対応の新たな課題

版：1.0　発行日：2026 年 11 月 13 日　情報基準日：2026 年 11 月 6 日

1　エグゼクティブサマリー

何が起きたか

多くの Web サイトを支える共通基盤である PHP に、2 件の重大な脆弱性が見つかり、各国の行政機関や企業が、修正や安全確認のためにサービスを一時停止した。各社の説明によれば、脆弱性の分析・悪用可能性の実証には AI が活用された。また、修正公開の 4 日前から攻撃試行が観測された。その後、特定の構成のおとりサーバーで悪用成功が観測された。調査会社 Dream は、Palo Alto Networks 製のファイアウォールや管理サーバー計 25 台が侵害されたと報告した。このうち 3 台は、米政府関連とみられる環境にあったという。製造元の Palo Alto Networks も悪用を確認し、攻撃に使われたツールと報告された結果を独自に検証したと説明している。ただし、11 月 6 日時点で、被害を受けた組織の総数、盗まれた情報の内容や量、損失の規模は明らかになっていない。

本件が示す経営上の課題

本件の核心は、**悪用が可能になる時点と、企業が対策を完了する時点の時間差**にある。発見・分析が加速しても、安全な修正の開発・提供、影響範囲の特定、業務部門や委託先との調整には時間がかかる。修正が存在するだけでは、リスクは解消しない。

その間、企業は、不確かな情報の下で、サービスの継続・制限・停止を判断し、実行しなければならない。予防停止は対応の失敗ではなく、侵害を避ける選択肢の一つである一方、現実の業務影響を伴う。また、共通基盤への依存により、同じ判断が多数の組織で同時に求められる。

企業に求められる 4 つの対応能力

- **影響範囲を把握する：** 稼働システム、依存関係、重要業務、管理責任者を把握し、自社への影響を迅速に特定する。
- **対策の完了までの時間を短縮する：** 更新の検証・適用、サポート終了版の移行、供給者との連携を平時から整える。
- **情報が不十分でも判断し、実行する：** 継続・制限・停止・再開の基準と権限を定め、判断待ちを減らす。
- **侵害を検知し、被害を抑えて復旧する：** 侵害の検知、被害の封じ込め、安全な復旧・再開を実行できる状態にする。

AI による発見の加速は、欠陥を早期に修正する機会も広げ得る。その機会を安全性の向上につなげるには、技術対策と、組織の判断・実行能力を併せて強化する必要がある。

本稿の範囲。 影響を受けるバージョン、修正、暫定措置、侵害の確認といった直近の対応については、付録 A に掲げる PHP プロジェクト、各国当局、関連ベンダーの公式案内に従っていただきたい。本稿は、この事象が明らかにしたことと、それが求める長期的な対策に焦点を当てる。

2 事象の概要

多くの Web サイトを動かす「共通の土台」に欠陥

PHP は、Web サイトの裏側で、利用者の要求に応じて情報を処理し、ページを生成するソフトウェアである。PHP2Shell は、この PHP の中核部分に見つかった 2 件の重大な脆弱性の通称である。個別企業のサイトの作り方ではなく、多くのサイトが共通して使う土台に問題があった。W3Techs によれば、11 月 5 日時点で、サーバー側の言語が判明している Web サイトの 69.1%が PHP を利用している。[2][8]

ログインせずに、不正な操作や情報の読み取りが可能に

2 件は別個の欠陥である。CVE-2026-109618 は、リクエストの処理途中でメモリが不足し、データが破損した状態になる問題、CVE-2026-109619 は、以前のリクエストの状態が残り、後続のリクエストで再利用される問題である。[38]これらの欠陥を悪用すると、一定の条件下で、攻撃者がログインせずにサーバー上で不正なプログラムを動かしたり、処理中のメモリから情報を読み取ったりできる。漏えいの対象には、パスワードや、他のシステムへ接続するための認証情報が含まれ得る。2 件とも、脆弱性の深刻度を示す CVSS v4.0 で 9.2 と評価され、最上位の「緊急」区分に該当する。[2][4][32]被害の範囲は、サーバーに与えられた権限や接続先によって異なる。なお、同じ機能に関連する別の脆弱性 CVE-2026-115560 も公表されているが、まれな構成を前提とするものであり、本稿でいう PHP2Shell は上記の 2 件を指す。[42]

AI が悪用可能性の解明を支援

Wiz 社によれば、脆弱なコードは 10 年以上前から存在し、PHP 5.4 以降の版が影響を受ける。関連する問題の兆候は 2024 年に認識されていた。しかし、悪用の方法や安全な修正の検討は難航した。2026 年 8 月、サイバーセキュリティ企業 Calif 社の研究者が、OpenAI の支援プログラムの下で AI を活用し、PHP の欠陥の悪用可能性を実証した。OpenAI と Wiz 社も同じ問題を独立に報告しており、Wiz 社も AI を活用したとしている。これは AI だけによる発見ではなく、人間の研究者が方向付けと検証を行ったものである。[1][4][5]なお、AI が発見・分析を支援したことは報告されている。攻撃側については、攻撃基盤に AI ツールが導入されていた痕跡が調査会社から報告されているが、攻撃コードの作成に AI が使われた直接の証拠はない（3.2 参照）。

修正公開前から攻撃試行があり、各国で予防停止

修正版は当初、10 月 22 日に公開される予定だったが、直前に関連情報の流出や実証動画の誤公開が起きたため、1 日前倒しされ、2026 年 10 月 21 日に公開された。そのため、一部の Linux ディストリビュータでは、実行イメージの提供が修正版の公開と同時にできず、数時間遅れた。Amazon は、確認されている情報流出に先立つ 10 月 17 日に、悪用の試行を観測している。試行の出所や、攻撃者が情報を入手した経路は特定されていない。[1][6][18]

報道によれば、各国の行政機関や企業は、修正や安全確認のために Web サイト・サービスを一時停止した。これらは、侵入が確認されたための停止とは限らず、多くは予防措置である。一方、おとりサーバー上での悪用成功に加え、その後、インターネットに公開されたファイアウォールの管理画面での悪用も確認された（3.2 参照）。[39][40]11 月 6 日時点で、一般組織における侵害・情報漏えいの全体規模は明らかになっていない。[19][20][21][26][33]

図 1　発見・修正・攻撃の時系列——公開前に観測された攻撃試行

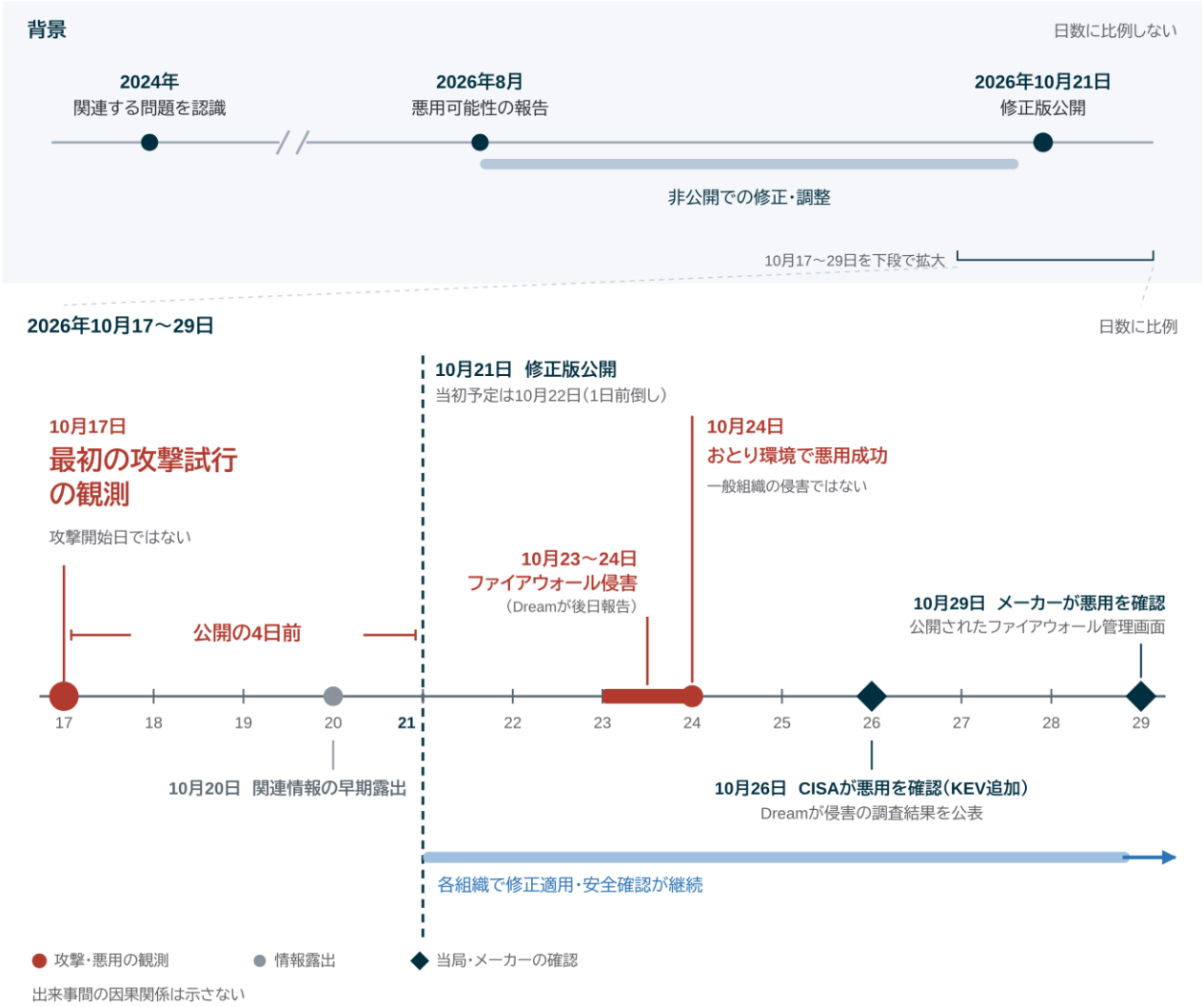


図 1 の注記。 図中の出来事は[1][2][6][33][37][39][40]に基づく。非公開での調整期間は 8 月 11 日から 10 月 21 日までの 71 日間で、修正入りイメージが早期に公開された経緯については、PHP Foundation と当該企業の説明が異なる。[1][18] Wiz 社は、8 月 19 日に最初の欠陥を発見し、8 月 24 日に PHP のセキュリティチームへ報告したとしている。OpenAI は Calif 社が GPT-5.6 Sol を使ったとし、Wiz 社は Wiz Atlas、Gemini 4 Argon、GPT-5.6 Sol を使ったとしている（各社の説明）。[4][5]

3 実際の影響と、被害確認の現状

PHP2Shell では、各国で予防的なサービス停止が生じたほか、実際の組織が運用する機器への侵害も確認された。本章では、サービス停止による業務影響と、攻撃・侵害の確認状況を分けて整理する。

3.1 各国で生じたサービス停止

表は、各行に示した公式発表と報道に基づく。

国・地域	主な対象・停止内容	確認された影響・留意点
英国	中央政府：英国の IT 専門ニュースサイト The Register が報じた貴族院での担当大臣の発言によれば、政府の 32 サービスが利用できず、4 サービスが部分的に利用できなかった。予算責任局（OBR）や複数の自治体にも影響が報じられた[29]。スコットランド：The National によれば、NHS Scotland のサイトも停止[30]	公共サービスの停止。大臣は大半を予防措置とした。中央政府のシステムの侵害は確認されていない（10 月 22 日付報道）
オランダ	DigiD の Web サイトが 10 月 21 日のほぼ終日閉鎖[19]。同国サイバーセキュリティセンター、政府ポータル Overheid.nl、ロッテルダム港のサイトも停止[20]	サイトの閉鎖。DigiD のサイトは同日中に再び利用可能となった（10 月 21 日）
フィンランド	政府 IT 機関が政府の公共ネットワークサービスを停止[20]	公共サービスの停止。具体的な対象範囲は公表されていない（10 月 22 日）
オーストラリア	オーストラリア信号局は、cyber.gov.au を含む政府系サイトに影響し得る障害を公表。内務省は、リスク軽減作業のため一部サイトを一時的に利用できないとした[21]	一時的な利用停止。同局は、実際の悪用は把握していないとした（10 月 22 日付報道）
日本	Impress Watch によれば、pixiv、DMM.com、niconico、BASE、コドモン、さくらインターネットの一部サービス、複数のオンラインゲームが緊急メンテナンスで停止[25]。国家サイバー統括室もサイト運営者に準備を呼びかけた[28]	緊急メンテナンスによる、業種を越えた同時のサービス停止（10 月 21 日）

予防的な停止は、攻撃による侵害被害とは区別されるが、サービスの中断は、当該組織と利用者にとって実際の業務影響である。

3.2 攻撃・侵害はどこまで確認されたか

修正公開の 4 日前から攻撃の試行が観測されている。[6] Check Point 社の観測対象では、約 1 割の組織で試行が検知され、欧州では 14%だった（10 月 22 日公表）。これは試行が検知された組織の割合であり、侵入に成功した割合ではない。[7]

CISA による悪用の確認

CISA は 10 月 26 日、連邦政府の文民機関を対象とする拘束的運用指令（BOD 26-04）の枠組みで、両脆弱性を既知の悪用済み脆弱性（KEV）カタログに追加した。KEV は、実際に悪用されている証拠があると CISA が判断した脆弱性の一覧である。[37]参照した情報では、CISA は確認の根拠や対象組織の詳細を公表しておらず、本稿もこの追加から被害組織や損失内容を推測しない。KEV カタログでは、米連邦政府の文民機関の対応期限を 10 月 29 日とし、修正の適用またはシステムの停止と、侵害有無の調査（フォレンジック・トリアージ）を求めている。[44]

おとり環境での命令実行

The Register によれば、セキュリティ研究者 Adel Karimi 氏は、自らが運用するおとりサーバー3 台で、10 月 24 日に計 35 回のシェル実行の成功を記録し、その結果を GitHub で公開した。サーバーは、Web サーバーソフト「Apache」に PHP 8.4.26 を直接組み込んで動かす構成（mod_php）である。シェルとは、コンピューターへ命令を実行させる仕組みであり、攻撃者が実際にサーバーへ命令を実行させたことを意味する。観測は CVE-2026-109618 の悪用と整合するが、CVE-2026-109619 の関与を示す証拠は見つかっていない。また、おとりサーバー

は、処理を 1 つのプロセスだけで行う、攻撃が成功しやすい設定（単一ワーカー構成）で運用されており、実運用での成功率を示すものではない。[33]

ネットワーク機器での侵害の確認

Palo Alto Networks は 10 月 29 日、インターネットに公開された PAN-OS の管理画面に対して、PHP2Shell が実際に悪用されていることを確認した。[39]同社の脅威調査部門 Unit 42 は、調査会社 Dream が報告した攻撃ツールと結果を独自に検証したとしている。[14]

Dream によれば、攻撃者は PHP2Shell と、Linux カーネルの別の脆弱性を組み合わせ、ファイアウォールと管理サーバー計 25 台で管理者権限を奪った。このうち 3 台は、米政府関連とみられる環境にあったという。この環境では、内部ネットワークへの接続経路の確保、LDAP サービスアカウントの認証情報の取得、利用者・グループの一覧取得も報告されている。ただし、その後に試みられたアカウント作成などが成功したかは分かっていない。また、Dream は攻撃基盤に AI ツールが導入されていたことを報告し、コードの特徴から AI 支援による開発を示唆しているが、攻撃コードの作成に AI が使われた直接の証拠はないとしている。[40]

被害規模に関する確認の限界

11 月 6 日までに確認した公開情報からは、被害を受けた組織の総数、盗まれた情報の内容や量、損失の規模は確定できない。また、自社で痕跡が見つからない場合も、それだけで攻撃を受けていないと判断することはできない。[3]

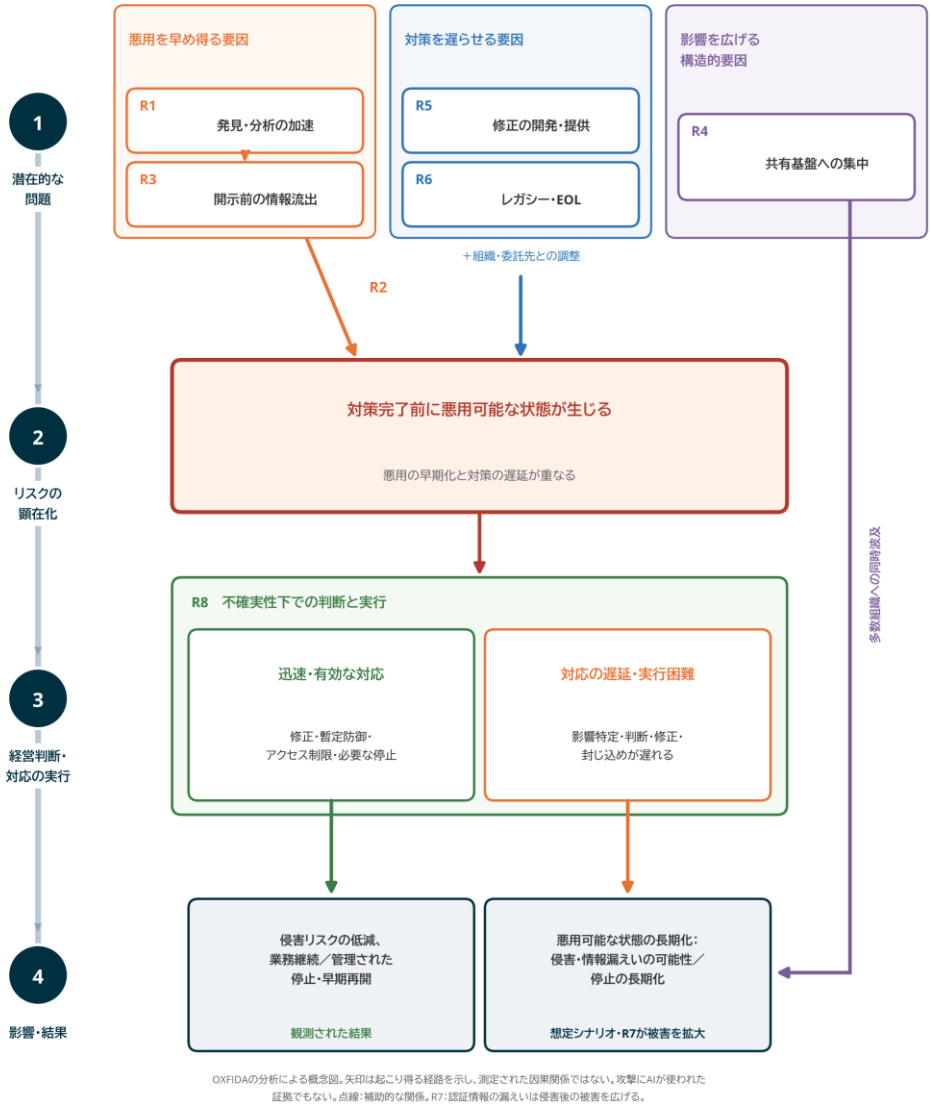
> **補足。** 欧州政府機関への侵入を PHP2Shell に関連付けた Palo Alto Networks（Unit 42）の初期評価は、10 月 25 日に同社が撤回している。[14][27]また、脅威インテリジェンス企業（サイバー攻撃の動向を調査・分析する企業）の SOCRadar 社は、攻撃者が使っていたサーバー上で、悪用ツールと、攻撃対象のサイトを選び出すためのプログラムを発見した（10 月 22 日報告、23 日更新）。このプログラムは約 20 サイトを調べていたが、結果が残っていた 11 サイトはいずれも、悪用に必要な条件を満たしていなかった。攻撃の準備が進んでいたことは分かるが、侵害が起きたことを示すものではない。[36]

4 リスクの構造——何が結果を左右するか

本件で浮き彫りになったのは、脆弱性が悪用され得る状態になってから、対策が完了するまでの時間差である。この間の被害の広がりは、情報が不十分ななかで、システムやサービスの継続・制限・停止、さらに再開をどう判断し、実行するかに左右される。図 2 は、この時間差と対応判断の関係を示している。

4.1 リスクの全体像

図 2　対応判断・実施と、侵害リスク・業務影響の関係



OXFIDAの分析による概念図。矢印は起こり得る経路を示し、測定された因果関係ではない。攻撃にAIが使われた証拠でもない。点線：補助的な関係。R7：認証情報の漏えいは侵害後の被害を広げる。

リスクが被害や業務への影響につながる仕組み

図のポイントは、次の 3 点である。

- **発見・分析が速くなっても、対策が追いつくとは限らない。**脆弱性の発見・分析の加速や、開示前の情報流出によって、悪用が可能になる時期は早まり得る。一方、修正の開発・提供、旧システムへの適用、組織内の調整には時間がかかる。そのため、悪用が可能になってから対策が完了するまでに、時間差が生じ得る。

- **対応の判断と実施によって、被害や業務への影響は変わる。**修正やアクセス制限、必要に応じた停止を適時に実施できれば、侵害リスクを抑えられる。反対に、判断や対応が遅れれば、悪用可能な状態や業務停止が長引くおそれがある。なお、被害を防ぐための予防的な停止は、対応の失敗ではなく、被害を抑える選択肢の一つである。
- **共通基盤への依存や認証情報の漏えいによって、影響が広がり得る。**多くの組織が利用する共通基盤に問題が生じると、複数の組織に同時に影響が及び得る。また、認証情報が漏えいした場合には、それを足掛かりに、侵害されたシステムの接続先へ被害が広がるおそれがある。

これらは、被害や業務への影響が生じる可能性のある経路を示したものであり、必ずこのとおりに進むわけではない。次の表では、今回確認された事実と、それぞれがリスクの観点から何を示すのかを整理する。

4.2 PHP2Shell で確認された事実と、そこから見えるリスク

表では、リスクに関わる 8 つの要因を整理する。ただし、各要因を数値で評価するだけの根拠がないため、点数化は行わない。R1～R7 は、悪用を早める要因、対策を遅らせる要因、被害を広げる要因を扱う。一方、R8 は、被害や業務への影響を左右する組織の対応を扱う。

要因・論点	PHP2Shell で起こったこと	リスク構造としての意味
R1 発見・分析の加速	複数の主体が独立に問題を報告し、AI 支援による分析・実証が行われた（各社の説明）	AI 支援による発見・分析の加速は、早期修正の機会を広げ得る。一方、他者による独立した発見・分析も早まる可能性がある（OXFIDA の分析）。英国 NCSC は、AI による脆弱性の「パッチの波」への備えを求めている[10]
R2 公開前・公開直後の悪用可能性	修正公開の 4 日前に攻撃試行が観測され[6]、その後おとりサーバー[33]と、公開されたファイアウォールの管理画面[39][40]で悪用成功が確認された	公開日を、危険な期間の始まりとみなすことはできない。公開前の攻撃を想定した検知・調査の重要性が高まる。AI による攻撃側の加速も今後の懸念である[9][15]。本件では攻撃基盤に AI ツールの痕跡が報告されたが、攻撃コードの作成に AI が使われた直接の証拠はない[40]
R3 開示前の情報流出	識別番号、実証動画、修正入りイメージが予定公開前に外部に出た。修正入りイメージが早期公開された経緯については、関係者の説明が異なる	防御の準備が整う前に、攻撃の手掛かりが利用可能になり得る
R4 共有基盤への集中	共通の PHP 基盤の問題で、複数国・業種が同時に対応を迫られた	影響の広がりは、各社の管理水準だけでなく、共通の依存関係にも左右される
R5 修正の開発・提供の制約	保守体制の制約で修正が停滞し[1]、組み込み製品では提供まで時間を要した[26]。PHP 本体の修正は 10 月 21 日に公開された一方、PAN-OS の修正版は系統ごとに 10 月 25～29 日に順次提供された。Dream が後日報告した侵害の発生日は 10 月 23～24 日で、この提供期間に先行する。なお、修正版の提供前から、管理画面へのアクセス制限などの軽減策は案内されていた[39][40]	発見が加速しても、修正・検証・配布の能力が同じ速度で拡大するとは限らない。修正の提供時期を自社だけでは制御できない
R6 レガシー・EOL の制約	PHP サイトのかなりの割合が、公式の修正を受けられない版で稼働している	修正の入手・適用が難しい環境が、悪用可能な状態を長引かせる。過去の類似例として、Log4Shell では公開後も長期間にわたり悪用が観測された[16][17]
R7 認証情報等の漏えい	メモリ上のパスワード、トークン、API キーの読み取りが実証された。実際の窃取の規模は不明[4]。これとは別に、侵害後に機器の設定から認証情報が取得され、内部の認証基盤への攻撃に使われたとの報告がある。PHP のメモリからの漏えいとは異なる、侵害後の被害拡大経路である[40]	被害は、侵害されたサーバーから、その認証情報で到達できる接続先へ広がり得る

要因・論点	PHP2Shell で起こったこと	リスク構造としての意味
R8 不確実性下での判断と実行	複数国で予防的な停止が報じられた[19][20][21]。このうち DigiD のサイトは 10 月 21 日中に再開した[19]。英国 NCSC は、暫定措置を適用できない場合のシステム停止を勧めた[11]。英国政府は公開前に省庁横断の体制を整えた[29]	修正が存在しても、判断や調整の遅れによって対策の完了は遅れる

補足

R1：PHP のセキュリティチームは、2026 年 7 月 1 日から修正版の公開までに 15 件の CVE を公表し、無効・重複の報告を 100 件以上処理した。[1]保守側の負荷の大きさは分かるが、過去の同じ期間との比較や AI の利用状況は示されていないため、この数字だけで AI によって発見が加速したとは言えない。

R2：2024 年のプレプリントでは、実験環境で、LLM エージェント（GPT-4）が既知の脆弱性 15 件を悪用できるかを検証した。成功率は、CVE の説明文を与えた場合に 87%、与えなかった場合に 7%だった。[15]公開情報が AI による悪用を助け得ることを示すが、査読前の研究であり、本件の攻撃に AI が使われたことを示すものではない。

R4：サーバー側言語が判明しているサイトの 69.1%が PHP を使用している（11 月 5 日時点）。[8]Unit 42 は、潜在的に脆弱な公開インスタンスを 2,260 万と報告した。[14]オランダ NCSC は、PHP に依存する製品の一覧を作成した。[13]いずれも利用や依存の広さを示すが、2,260 万はインスタンス数であり、固有の Web サイト数や組織数、実際の被害件数ではない。

R5：Cisco の Expressway と Duo Access Gateway には修正版が示され、URWB（Ultra-Reliable Wireless Backhaul）と Unified Industrial Wireless Software の修正版 26.2.1.9 も、11 月 6 日の更新で利用可能と案内された。[43]製品ごとに修正の提供時期が異なるため、利用者が対策を終えられる時期にも差が出得る。

R6：W3Techs がバージョンを特定できた PHP サイトのうち、約 34%が PHP 7 以前で稼働している（11 月 5 日時点）。[8]PHP 8.1 以前は、PHP プロジェクトの通常の更新対象外である。ただし本件では、7.4・8.0・8.1 向けに最小限のソースコードのバックポートが提供されており、一部のディストリビューションや LTS ベンダーも修正を提供している。利用者は提供元の対応状況を確認する必要がある。なお、8.2 のサポートも 2026 年 12 月 31 日に終了する。[2]ただし、旧バージョンの利用率だけでは、本件の影響を受ける割合や、対策が遅れた割合は分からない。

> **OXFIDA の分析**　AI によって脆弱性をより早く発見できるようになれば、攻撃者が悪用する機会が増える一方で、防御側も早期に修正できる可能性が広がる。この機会を生かせるかどうかは、次章で示す 4 つの対応能力を、平時から備えているかにかかっている。

5 企業に求められる 4 つの対応能力

直ちに必要な対応については、付録 A に示す公式案内を参照されたい。第 4 章では、対策が完了する前に脆弱性が悪用され得る理由と、被害や業務への影響を左右する要因を整理した。本章では、これらを踏まえ、企業が平時から備えるべき 4 つの対応能力を示す。

図 2 で示した関係に沿って整理すると、①影響範囲を把握する、②対策の完了までの時間を短縮する、③情報が不十分でも判断し、実行する、④侵害を検知し、被害を抑えて復旧する、の 4 つである。これらは順番に実施する手順ではなく、平時から並行して強化すべき能力である。

対応能力と目的	主な取り組み	対応力を確かめる問い	関連要因
① 影響範囲を把握する **自社のどのシステムや業務が影響を受けるかを、迅速に判断する**	● どのシステムがどこで稼働し、誰が管理し、どの業務を支えているかを把握する。 ● SBOM や資産台帳を手掛かりに、ベンダー製品やコンテナイメージに含まれる PHP も確認する。さらに、実際に稼働するプロセスが使用しているバージョンと修正状況を確かめ、外部公開の有無、悪用の成立条件、重要業務への影響に応じて、対応の優先順位を付ける。	重大な脆弱性が判明したとき、影響を受けるシステムとその責任者を何時間で特定できるか。	R4、R6 （全体にも関連）
② 対策の完了までの時間を短縮する **脆弱性が悪用され得る状態を、できるだけ短くする**	● 更新の検証・配布・適用から、稼働環境での適用結果の確認までを、全社で迅速かつ継続的に行える体制を整える。[10][34] ● サポートが終了したバージョンの利用状況を把握し、予算・責任者・期限を明確にして、計画的に利用を終了する。 ● サプライチェーンや OSS への依存関係を把握・管理し、修正や通知に関する契約条件の確認、保守者への支援を行う。AI 関連の構成要素にも同じ管理方針を適用する。[24]	修正や封じ込めが完了していない重要なシステムは何件あり、誰が対応期限を管理しているか。	R1、R2、R3、R5、R6
③ 情報が不十分でも判断し、実行する **判断待ちによる対応の遅れと、必要以上の業務影響を抑える**	● 重大な脆弱性が予告なく判明することを前提に、サービスの継続・制限・停止・再開の判断者と判断基準、現場に委ねる権限の範囲をあらかじめ定める。併せて、一時停止の手順を整える。 ● 情報が不十分でも判断できるよう、一次情報の確認、判断根拠や例外の記録、再評価の条件、関係者との調整、上位責任者への判断の引き上げの手順を定める。 ● 適用される報告・通知義務を確認し、対応責任者と判断手順を定める（例：EU CRA における、実際に悪用された脆弱性の報告義務は、2026 年 9 月 11 日から製造者に適用）。[22][23]	責任者が不在のときや夜間でも、必要な制限・停止を判断し、実行できるか。	R8 （副次的：R2、R3、R5）
④ 侵害を検知し、被害を抑えて復旧する **侵害を早期に把握し、被害の拡大と復旧の負担を抑える**	● 特定の CVE 情報だけに頼らず、異常や侵害を検知できるようにする。また、脆弱性の公表前の活動も遡って調査できるよう、取得・保全の方針を定めてログを残す。 ● 一か所の侵害が他のシステムへ広がらないよう、ネットワークの分離、権限の最小化、認証情報が露出し得る範囲の限定や有効期間の短縮を行う。 ● 封じ込め、侵害の原因や痕跡の除去、安全な状態への復旧、サービス再開に必要な技術的条件を定め[35]、演習で確かめる。	1 台のシステムが侵害された場合、被害はどこまで広がり得るか。また、何を確認できれば、安全に再開できると判断するか。	R2、R4、R7、R8

4 つの対応能力は、NIST CSF 2.0 の機能[31]を参考に、OXFIDA が経営層向けに対策を再編したものであり、CSF の公式な分類ではない。各対策は複数の機能や要因にまたがり、厳密な一対一の対応を意味しない。

6 AI 専門家の視点

以下のコメントは、各専門家の個人としての見解である。

> 「最近の PHP2Shell の脆弱性は AI 支援の手法によって発見されたが、その発見は同時に、AI によって悪用が加速するリスクが高まっていることも浮き彫りにしている。セキュリティ研究者が複雑な脆弱性を発見することを可能にするのと同じ能力は、攻撃者が欠陥を素早く分析し、実際に使える攻撃コードを開発し、攻撃を大規模に自動化するためにも利用され得る。こうした AI の二面性により、脆弱性の公表から広範な悪用に至るまでの時間が短くなるおそれがある。そのため組織には、攻撃者に悪用される前にセキュリティ上の弱点を検知し、優先順位を付け、緩和することが、これまで以上に求められている。」
>
> **Stephen Roberts** オックスフォード大学 機械学習教授

> 「PHP2Shell は、AI がリスクのガバナンスをどう変えるのか、その一端を先取りして示した。AI の支援による発見、とりわけソフトウェアの脆弱性の発見は、欠陥の悪用を大幅に加速させるだろう。定期的な見直しと、既知のリスクを記録した固定的な台帳を軸とするガバナンスでは、この新たな変化の速さに追いつけない。代わりに必要なのは、不確実なリスク環境を管理でき、人間の監督者に誠実で信頼できるリスク評価を提供する、動的なガバナンスである。PHP2Shell は、リスクのガバナンスの変革に取り組むすべての組織が受け止めるべき警告である。」
>
> **Maike Osborne** オックスフォード大学 機械学習教授

付録 A　直近の対応に関する公式案内

最新の対象バージョン、暫定措置、侵害の確認方法については、以下の情報源に従っていただきたい。状況に応じて更新されている。

- The PHP Group：セキュリティ勧告とリリース告知[2]
- JPCERT/CC：JPCERT-AT-2026-0033[3]
- 英国 NCSC：「Critical security issue affecting PHP」[11]
- カナダ・サイバーセキュリティセンター：AL26-026[12]
- オランダ NCSC：PHP に依存するソフトウェア製品の一覧[13]
- Palo Alto Networks：PAN-OS 等への影響に関するセキュリティアドバイザリ[39]
- シンガポール・サイバーセキュリティ庁（CSA）：AL-2026-157（ネットワーク・セキュリティ製品）[41]
- Red Hat：RHSB-2026-013[42]

用語集

用語	意味
CVE	公開された脆弱性に付与される識別番号。
CVSS	脆弱性の技術的な深刻度を 0〜10 で示す共通評価手法。9.0 以上は「緊急」に区分される。
サポート終了（EOL）	保守者からセキュリティ修正が提供されなくなったバージョン。
メモリ開示	プログラムのメモリ内容（パスワードやキーなど）を攻撃者が読み取ること。
SBOM（ソフトウェア部品表）	製品やシステムに含まれるソフトウェア部品の一覧。
遠隔コード実行（RCE）	攻撃者がネットワーク越しに、他のコンピューター上で任意の命令を実行すること。
ハニーポット（おとりサーバー）	攻撃を観測するために設置するおとりのサーバー。

濵田 全次郎｜Senior Vice President, OXFIDA

AI ガバナンスやモデルリスク管理等の事業・製品戦略を担う。元 Goldman Sachs 投資銀行部門 Vice President。経営層への助言と AI 事業の実務経験を基に、技術変化が企業のリスク管理と意思決定に及ぼす影響を考察する。

免責事項。 本稿は一般的な情報提供を目的としたものであり、セキュリティ、法律、投資に関する専門的な助言ではない。

参考文献

[1] The PHP Foundation, “Today’s PHP Security Release, and How We’re Strengthening PHP Security”, 21 Oct 2026. https://thephp.foundation/blog/2026/10/21/todays-php-security-release-and-how-were-strengthening-php-security/

[2] The PHP Group, security advisory (21 Oct 2026), informational advisory (23 Oct 2026) and PHP 8.2.35 release note. https://www.php.net/archive/2026.php

[3] JPCERT/CC, JPCERT-AT-2026-0033, 22 Oct 2026, updated 29 Oct 2026. https://www.jpcert.or.jp/at/2026/at260033.html

[4] Wiz Research, “PHP2Shell: AI uncovers critical RCE vulnerabilities affecting 70% of the Internet” (title as published), 21 Oct 2026. https://www.wiz.io/blog/php2shell-php-rce

[5] OpenAI, “Patch the Planet: global response coordination as agents uncover critical vulnerabilities”, 21 Oct 2026. https://openai.com/index/coordinated-disclosure-of-critical-vulnerabilities/

[6] Amazon Threat Intelligence, “Amazon Threat Intelligence identifies PHP2Shell exploitation prior to public disclosure in MadPot”, 21 Oct 2026, updated 22 Oct 2026. https://aws.amazon.com/blogs/security/amazon-threat-intelligence-identifies-php2shell-exploitation-prior-to-public-disclosure-in-madpot/

[7] Check Point Research, “PHP2Shell Update: One in ten organizations impacted as Europe bears the brunt”, 22 Oct 2026. https://blog.checkpoint.com/ai-security/php2shell-one-in-ten-organizations-impacted-as-europe-bears-the-brunt/

[8] W3Techs, “Usage statistics of PHP for websites”, as of 5 Nov 2026. https://w3techs.com/technologies/details/pl-PHP

[9] UK NCSC, “Impact of AI on cyber threat from now to 2027”, 7 May 2025. https://www.ncsc.gov.uk/report/impact-ai-cyber-threat-now-2027

[10] UK NCSC (O. Whitehouse), “Preparing for a ‘vulnerability patch wave’”, 1 May 2026. https://www.ncsc.gov.uk/blogs/prepare-for-vulnerability-patch-wave

[11] UK NCSC, “Critical security issue affecting PHP”, 21 Oct 2026. https://www.ncsc.gov.uk/news/critical-security-issue-affecting-php

[12] Canadian Centre for Cyber Security, AL26-026, 21 Oct 2026. https://cyber.gc.ca/en/alerts-advisories/al26-026-critical-vulnerabilities-impacting-php-cve-2026-109618-cve-2026-109619

[13] NCSC-NL, php2shell operational information and software inventory. https://github.com/NCSC-NL/php2shell

[14] Palo Alto Networks Unit 42, “Threat Brief: Critical Vulnerabilities in PHP”, Oct 2026 (updated 25 Oct 2026, retracting the 23 Oct update on a European government agency; updated 29 Oct 2026 on PAN-OS exploitation). https://unit42.paloaltonetworks.com/cve-2026-109618-cve-2026-109619/

[15] Fang, R. et al., “LLM Agents can Autonomously Exploit One-day Vulnerabilities”, arXiv:2404.08144 (preprint), 2024. https://arxiv.org/abs/2404.08144

[16] Singh, A. et al., “A Longitudinal Measurement Study of Log4Shell Exploitation from an Active Network Telescope”, arXiv:2601.04281 (preprint), Jan 2026. https://arxiv.org/abs/2601.04281

[17] Hiesgen, R., Nawrocki, M., Schmidt, T. C., Wählisch, M., “The Log4j Incident: A Comprehensive Measurement Study of a Critical Vulnerability”, IEEE TNSM 21(6), 2024. https://doi.org/10.1109/TNSM.2024.3440188

[18] The Register (J. Lyons), “PHP blames supply chain security biz Chainguard for putting huge chunks of the web at risk”, 22 Oct 2026, updated 23 Oct 2026 (includes Chainguard’s response). https://www.theregister.com/security/2026/10/22/php-blames-supply-chain-security-biz-chainguard-for-putting-huge-chunks-of-the-web-at-risk/5304611

[19] ANP via Nieuws.nl, “Website DigiD weer toegankelijk”, 21 Oct 2026. https://nieuws.nl/algemeen/website-digid-weer-toegankelijk

[20] Al Jazeera, 22 Oct 2026. https://www.aljazeera.com/news/2026/10/22/whats-the-php-coding-flaw-that-could-pull-down-70-percent-of-the-internet

[21] InDaily (F. Farid and L. Garbutt-Young, with AAP), “‘Critical’ software flaw hits Australian government sites”, 22 Oct 2026. https://www.indailysa.com.au/news/just-in/2026/10/22/critical-software-flaw-hits-australian-government-sites

[22] European Commission, “Cyber Resilience Act – Reporting obligations”. https://digital-strategy.ec.europa.eu/en/policies/cra-reporting

[23] Regulation (EU) 2024/2847 (Cyber Resilience Act), Articles 14 and 71. https://eur-lex.europa.eu/eli/reg/2024/2847/oj/eng

[24] UK NCSC and partners, “Guidelines for secure AI system development”. https://www.ncsc.gov.uk/collection/guidelines-secure-ai-system-development

[25] Impress Watch, 国内大手サービスで緊急メンテやサービス停止 PHP 脆弱性で対策, 21 Oct 2026. https://watch.impress.co.jp/docs/news/2150159.html

[26] BankInfoSecurity (M. J. Schwartz), “PHP2Shell Actively Exploited, US Cybersecurity Agency Warns”, 27 Oct 2026 (secondary source; reports CISA’s KEV listing of 26 Oct and the related federal requirements). https://www.bankinfosecurity.com/php2shell-actively-exploited-us-cybersecurity-agency-warns-a-33219 (The page shows inconsistent date labels; the publication date is taken as 27 Oct 2026, as stated in the article.)

[27] The Hacker News, “PHP2Shell Exploitation Attempts Continue Amid Suspected N. Korea Global Scanning Activity”, 25 Oct 2026 (updated with Unit 42 retraction). https://thehackernews.com/2026/10/php2shell-exploitation-hits-government.html

[28] GIGAZINE, ニコニコや pixiv など各種ウェブサイトおよびアプリが PHP の緊急パッチに対応するべくメンテナンス入り, 21 Oct 2026. https://gigazine.net/news/20261021-php-php2shell-maintenance/

[29] The Register (C. Page), "PHP2Shell puts dozens of UK government services out of service", 22 Oct 2026 (reporting House of Lords proceedings). https://www.theregister.com/security/2026/10/22/php2shell-puts-dozens-of-uk-government-services-out-of-service/5304840

[30] The National via Yahoo News UK, "NHS Scotland website remains offline as critical internet flaw sparks security fears", 22 Oct 2026. https://uk.news.yahoo.com/nhs-scotland-website-remains-offline-070029113.html

[31] NIST, "The NIST Cybersecurity Framework (CSF) 2.0", NIST CSWP 29, Feb 2024. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf

[32] Fastly, blog post on critical RCE vulnerabilities in core PHP (CVE-2026-109618, CVE-2026-109619), Japanese edition, 21 Oct 2026. https://www.fastly.com/jp/blog/critical-rce-vulnerabilities-discovered-core-php-cve-2026-109618-cve-2026-109619

[33] The Register, "CISA confirms PHP2Shell under attack as researchers clock successful exploits", 27 Oct 2026 (links to the researcher's report at github.com/0x4D31/honeypot-data; only the repository and its description of 35 case folders were confirmed, not the detailed report). https://www.theregister.com/cyber-crime/2026/10/27/cisa-confirms-php2shell-under-attack-as-researchers-clock-successful-exploits/5305681

[34] Souppaya, M. and Scarfone, K., "Guide to Enterprise Patch Management Planning: Preventive Maintenance for Technology", NIST SP 800-40 Rev. 4, Apr 2022. https://doi.org/10.6028/NIST.SP.800-40r4

[35] Nelson, A. et al., "Incident Response Recommendations and Considerations for Cybersecurity Risk Management: A CSF 2.0 Community Profile", NIST SP 800-61 Rev. 3, Apr 2025. https://doi.org/10.6028/NIST.SP.800-61r3

[36] SOCRadar, "PHP2Shell Exploit Tooling Found on Exposed Attacker Server", 22 Oct 2026, updated 23 Oct 2026. https://socradar.io/blog/php2shell-exploit-tooling-attacker-server/

[37] CISA, "CISA Adds Two Known Exploited Vulnerabilities to Catalog", 26 Oct 2026. https://www.cisa.gov/news-events/alerts/2026/10/26/cisa-adds-two-known-exploited-vulnerabilities-catalog

[38] OffSec, "PHP2Shell – Critical Vulnerabilities in PHP Core (CVE-2026-109618/CVE-2026-109619)", 22 Oct 2026. https://offsec.com/blog/php2shell-critical-vulnerabilities-in-php-core/

[39] Palo Alto Networks, "CVE-2026-109618 Impact of Critical Vulnerabilities in PHP (CVE-2026-109618, CVE-2026-109619) on Palo Alto Networks Products", security advisory, 21 Oct 2026, updated 29 Oct 2026. https://security.paloaltonetworks.com/CVE-2026-109618

[40] Dream, "Chained PHP2Shell Exploit Roots 25 Servers", 26 Oct 2026, updated 29 Oct 2026. https://dreamgroup.com/blog/chained-php2shell-exploit-roots-25-servers

[41] Cyber Security Agency of Singapore, "Active Exploitation of PHP2Shell Vulnerabilities Affecting Network and Security Products" (AL-2026-157), 3 Nov 2026. https://www.csa.gov.sg/alerts-and-advisories/alerts/al-2026-157/

[42] Red Hat, "RHSB-2026-013 Request handling memory corruption - php (CVE-2026-109618, CVE-2026-109619, CVE-2026-115560) - "php2shell"", 21 Oct 2026, updated 23 Oct 2026. https://access.redhat.com/security/vulnerabilities/RHSB-2026-013

[43] Cisco, security advisory cisco-sa-php-october26-Jj384Daq on PHP vulnerabilities in Cisco products, version 1.11, updated 6 Nov 2026. https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-php-october26-Jj384Daq

[44] CISA, Known Exploited Vulnerabilities Catalog, entries for CVE-2026-109618 and CVE-2026-109619 (added 26 Oct 2026). https://www.cisa.gov/known-exploited-vulnerabilities-catalog