2026年10月21日（水）21時55分

修正版の公開まで、あと1時間

PHP の脆弱性と、社会の判断を読み解く

高等学校　情報Ⅰ（1）情報社会の問題解決／（4）情報通信ネットワークとデータの活用

問い（ワークシート①）

首相が、一つのソフトウェアの更新を X で呼びかけた

「皆様に、今夜に対応して頂きたい
大至急のお願いです」

なぜ、
そこまで
急いだのか？

高市早苗首相の X の投稿（10月21日 21時55分ごろ）

→ ワークシート①に、予想を一言で

出典：高市早苗首相の X 投稿（2026-10-21 21:55ごろ）、INTERNET Watch（2026-10-22）

その夜

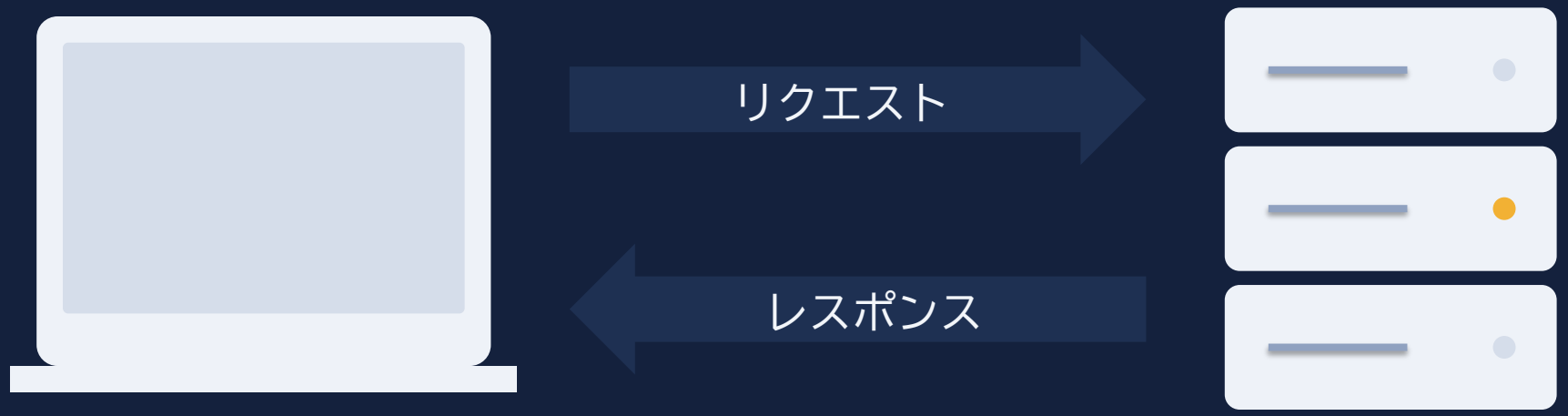
銀行もネットショップもゲームも、予防のために自ら止めた

一時停止	一時停止	一時停止	一時停止	一時停止
銀行	ネットショップ	ゲーム	保育の連絡	省庁のサイト

共通点：PHP を使っていた（または、その可能性を確かめる必要があった）

出典：日本経済新聞（2026-10-21）、Impress Watch（2026-10-21）、ITmedia NEWS（2026-10-21）、ギズモード・ジャパン（2026-10-22）

PHP はサーバー側で動く言語。使う言語が分かるサイトの約7割



クライアント
（ブラウザ）

サーバー
（PHP）

69.2%

サーバー側の言語が分かるサイトのうち

直すのは、サーバーを運営する側

出典：W3Techs（2026-10-27）サーバー側の言語が分かるウェブサイトのうち 69.2%、ギズモード・ジャパン（2026-10-22）

2 件の脆弱性（PHP2shell）

認証なしで、外からサーバー上のコードを実行されうる

CVE-2026-109618
メモリ不足（OOM）の途中で、
中途半端なデータが残る

CVE-2026-109619
前のリクエストの、解放された
メモリを指す状態が残る

CVSS v4.0　2 件とも

9.2 / 10

完全な回避策はなく、
更新だけが安全な選択

近くの人と30秒：「認証なし」「リモート」「コード実行」。3つがそろうと、なぜ最悪？

出典：PHP 公式発表（php.net、2026-10-21）、The PHP Foundation（2026-10-21）、IPA（2026-10-22）

時系列①　公開まで

伏せて直すはずが、公開の前に情報が漏れた

8月	10月17日	21日 未明	21日 日中
報告が届き 修正を始める	攻撃の試みを 観測（AWS）	番号が漏れ 1日前倒しへ	動画が広まり PoC が出回る

見方が割れる： AWS「公開の約12時間前から複数の PoC」
PHP 側「公開時点で、機能する攻撃コードは把握せず」

出典：The PHP Foundation（2026-10-21）、Amazon Threat Intelligence（AWS、2026-10-21）

時系列②　公開の夜と、その後

23時に公開。26日、米 CISA が「悪用が確認された脆弱性」の一覧に

21日 午後	21時55分	23時	22日	26日
NCO が注意喚起	首相が呼びかけ	修正版を公開	IPA が注意喚起	CISA の一覧に載る

IPA（10月27日）：国内での攻撃被害の事例は「把握しておりません」。ただし更新は今も必要

出典：共同通信（2026-10-22）、INTERNET Watch（2026-10-22）、The PHP Foundation（2026-10-21）、IPA（2026-10-22 掲載、10-27 更新）

一般論：修正の公開は、弱点の公開

一般に、修正の差分は攻撃の手がかりになる

修正前のコード

修正後のコード

差分

1時間足らず

AI が差分から攻撃コードを作るまで（Firefox などでの研究。PHP ではない）

数時間

今回、公開後に PoC が次々と出るまで

今回急いだ理由は両方：公開前の漏れ（→ 1日前倒し）と、公開後に差分から来る攻撃

出典：Anthropic Frontier Red Team（2026-06-08、Firefox と Windows での研究）、Amazon Threat Intelligence（AWS、2026-10-21）

NIST CSF 2.0 の 6 つの機能

6 つは順番ではなく、同時に回す。真ん中に「統治」

統治　誰が決め、誰に伝えるか（ほかの 5 つを貫く中心）

識別	防御	検知	対応	復旧
どこで動いている？	更新する	攻撃の跡を探す	止める・知らせる	直して再開

この夜、ふだんから持っていないと困ったのは？（一つでなくてよい）

出典：NIST「サイバーセキュリティフレームワーク（CSF）2.0」（2024-02-26、日本語訳：IPA）

話し合い：ワークシート②（個人1分 → 班5分 → 発表3班）

21時。あなたはサービスの責任者。止める？ 止めない？

止めると	止めないと
・利用者が使えない ・売上・信用への影響 ・問い合わせが増える	・認証なしで乗っ取られるおそれ ・会員の情報が盗まれるおそれ ・ほかへの攻撃の踏み台に

判断に必要な情報は？ どこで動いている？ 外から届く？ 誰が決める？

参考：国家サイバー統括室の X 投稿（2026-10-21）「…リスクを低減させるための有効策の一つと考えられます」

誰が、何をするか

直すのはサーバーの運営者。利用者にも、利用者の仕事がある

サーバーの運営者

- どこで PHP が動くかを調べる
- 修正版に更新する
- 難しければ一時停止・利用者に告知

利用者（私たち）

- 止まったことを受け止める
- 公式の発表で確かめる
- 漏れた情報やうわさを広めない

参考：ギズモード・ジャパン（2026-10-22）、IPA（2026-10-22）

自分にできること（「今回」と「ふだん」を分ける）

情報社会の一員として、今日からやる4つ

1 ふだん

更新を後回しにしない

自動更新をオンに。
再起動も早めに。

2 ふだん

パスワードを使い回さない

今回の攻撃とは別。
管理の仕組みと
多要素認証を。

3 今回も

情報源を確かめる

公式の発表を見る。
漏れた情報を
広めない。

4 今回も

運営するなら担当を決める

部活のサイトや
個人の開発も。

ふり返り（ワークシート③④）

この夜を、自分の言葉で説明する

③ 自分がとる行動を一つ（いつ・何を）　← 授業の中で

---

④ 10月21日に何が起きたか（200字）　← 宿題でよい

使う言葉：「脆弱性」「修正の公開」「一時停止」

最後に：①の予想を、一言で言い直す

守りは、それぞれの仕事の組み合わせ。自分の分を、今日から。

この作品は クリエイティブ・コモンズ 表示 4.0 国際 ライセンスで提供されています。
出典：Data is CITY（teleport.jp/dataiscity/）
https://creativecommons.org/licenses/by/4.0/deed.ja

付録 A（時間があれば・質問が出たら）

侵入された後、組織の中に広がる速さ

29分

侵入から、別のマシンへ
広がるまでの平均（2025年）

27秒

観測された最速

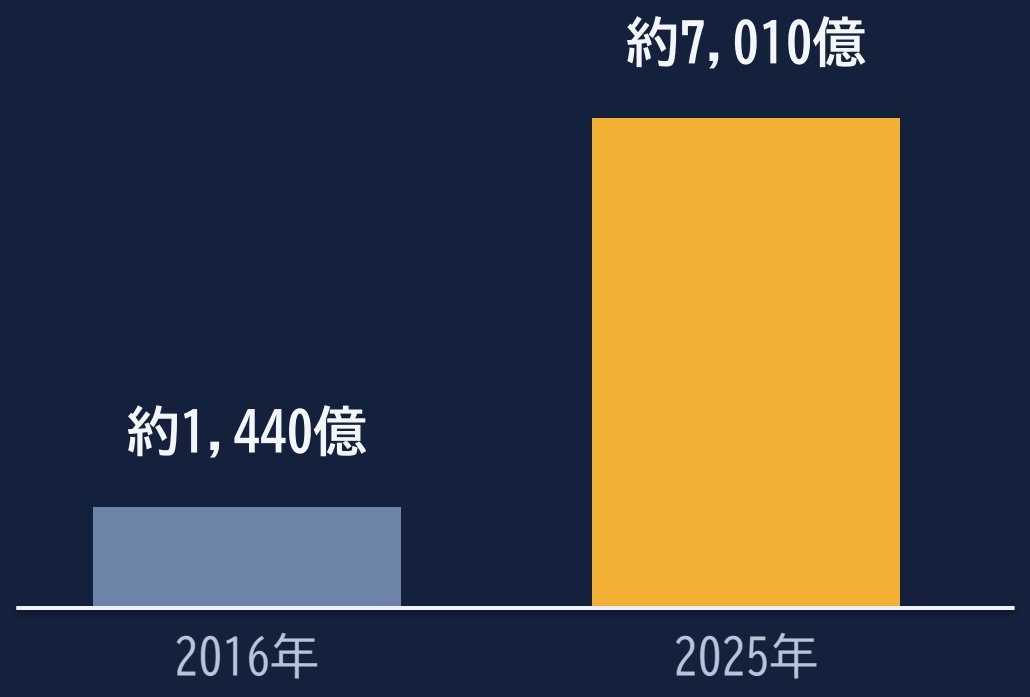
対応は
「7日・30日」でなく
「時間」で測る
（AWS の提言）

侵入された後に中で広がる速さ。修正を当てる速さとは別の量（PHP の攻撃の速さではない）

出典：CrowdStrike「2026 Global Threat Report」（2025年の eCrime の値）、AWS（2026-10-21）

付録 B（時間があれば・質問が出たら）

使われていない番地に届く通信は、2016年から9年で約4.9倍



約4.9倍

年間の総観測パケット数
2025年の約55% は
調査目的のスキャン
（すべてが攻撃ではない）

出典：情報通信研究機構（NICT）「NICTER 観測レポート 2025」（2026-02-05）