鉄道や企業のHPが一斉休止

「PHPの脆弱性」とは何か？

一般の人がやること・
クリニック経営者の確認手順



2026年10月21日～22日

鉄道・百貨店・大学・公的機関のHPが一斉に休止

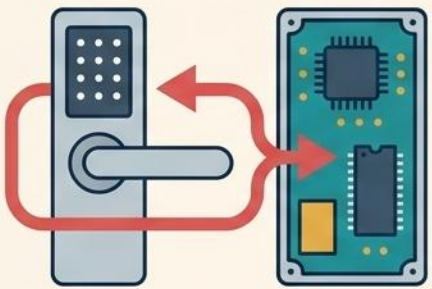


PHPはホームページの「建物の共通システム」



WordPressなど世界中の多くのサイトで利用

合鍵なしで外から命令を実行される弱点



2件の脆弱性
(CVE-2026-109618 / CVE-2026-109619)



深刻度は最高ランク
「Critical（CVSS 9.2）」

すべてが攻撃されて壊れたわけではない



鍵を交換して安全を確認する
までの「予防的な休止」



新しい鍵（修正プログラム）
はすでに公開済み

立場によってやることが違う



ネットを見るだけの個人：スマホ・PCの更新作業は不要



無料ブログ・SaaS利用者：運営会社が対応するため作業不要



独自サーバー・WordPress運営者：PHPの更新確認が必須

一般のネット利用者が気をつけること



1. 「PHPの更新が必要」と装う偽メール（詐欺）に注意



2. パスワードの使い回しを避け、ログイン情報を守る

なぜクリニック・医療機関のHPが危ないのか



多くのクリニックHPは
「WordPress（PHP）」で稼働



開業時に外注したまま保守が
放置されているケースが多い

公開HPが乗っ取られたときの3つの実害



1. 来院患者がウイルスや詐欺サイトへ誘導される



2. お問い合わせ・求人フォームの個人情報が漏えいする



3. HPの長期閉鎖と再構築コストが発生する

誤解1：開業から動いているから大丈夫？



PHP 8.1以前はすでに公式サポート終了（放置は危険）



現役サポート版はPHP 8.2 / 8.3 / 8.4 / 8.5のみ

誤解2：メンテナンス画面プラグインで防げる？



Apache（mod_php）環境ではWordPressが動く前に攻撃が成立

設定変更は緩和策にとどまり、解決策はアップデートのみ

クリニック経営者が今日確認する3つのステップ

ステップ1：サーバーの管理主体（制作会社か自院か）を確認



ステップ2：PHPが修正版（8.5.12 / 8.4.27 / 8.3.36 / 8.2.35）か確認



ステップ3：予約システムと院内端末の切り分け

外部のWEB予約・問診システムは提供元の案内を確認



電子カルテ端末で一般サイト閲覧やメール受信をしない



まとめ：立場に合わせた冷静な確認を

個人は「作業不要・便乗詐欺に注意」



クリニックHP（WordPress）は「PHPを修正版へ更新」



チャンネル登録、高評価をよろしくお願いします。