Grant Thornton

＿マンスリー・ハイライト　拝啓社長殿

マネジメントのための経営財務情報

第 670 号　この資料は全部お読みいただいて 2 分です。

テーマ：脆弱性対応は経営判断　～PHP2shell から考える～

バックナンバー
はこちらから

2026 年 10 月、広く使われる「PHP」に深刻な脆弱性が公表され、数日で悪用が確認されました。脆弱性対応が「経営の判断事項」である理由と、平時の備えを整理します。

修正版公開から約 5 日で「現実の脅威」に

2026 年 10 月 21 日に修正版が公開された 2 件の脆弱性（通称「PHP2shell」）は、悪用されるとサーバーを遠隔から乗っ取られるおそれ（リモートコード実行：RCE）があり[i]、米国 CISA は 10 月 26 日に「悪用が確認された脆弱性」に追加しました[ii]。2024 年 7 月にも PHP の脆弱性が悪用され、IPA が注意喚起を行っています[iii]。

項目	2024 年 7 月[ii]	2026 年 10 月[i,iii]
脆弱性	CVE-2024-4577	CVE-2026-109618・109619
影響範囲	Windows 上で動作する一部の環境	Web の処理に使われる PHP 全般
悪用状況	国内の複数組織で被害を確認	悪用を確認（国内被害は 10/27 時点で未把握）

同じ製品で深刻な脆弱性が繰り返し見つかり、影響範囲も広がっています。PHP は VPN 機器の管理画面などにも組み込まれており[i]、「自社は無関係」と即答できる企業は多くありません。

i 独立行政法人情報処理推進機構（IPA）「PHP の脆弱性対策について（PHP2shell）」
https://www.ipa.go.jp/security/security-alert/2026/alert20261022.html, 2026 年 11 月 2 日取得

ii Cybersecurity and Infrastructure Security Agency (CISA)「Critical Vulnerabilities in PHP Require Immediate Patching」
https://www.cisa.gov/news-events/alerts/2026/10/21/critical-vulnerabilities-php-require-immediate-patching,
2026 年 11 月 2 日取得

iii 独立行政法人情報処理推進機構（IPA）「PHP の脆弱性（CVE-2024-4577）を狙う攻撃について」
https://www.ipa.go.jp/security/security-alert/2024/alert_20240705.html, 2026 年 11 月 2 日取得

なぜ経営層の判断が必要なのか

基本は修正版の適用ですが、保守契約がない、サポートが終了しているなど、すぐに適用できない場合もあります。IPA はその際、サービス停止やシステム廃止も視野に、経営層を含めて検討するよう求めています[i]。「止めるか、刷新するか」は売上や取引先に影響する経営判断であり、判断の遅れはそのまま攻撃にさらされる時間となります。停止すれば一時的に業務や顧客対応に影響が出ますが、放置して侵入を許せば、情報漏えいや取引先からの信頼低下など、より大きな損失につながりかねません。この比較を現場だけで判断するのは難しく、経営層の決断が求められます。

平時に備えておきたい 3 つのポイント

① **IT 資産と委託先の把握**：システム・機器と保守窓口を一覧化しておく
② **判断基準と権限の事前合意**：優先順位の基準と「停止」を判断する責任者を決めておく
③ **ライフサイクルと予算の管理**：サポート終了時期を把握し、更新費用を確保する

お見逃しなく！

脆弱性は今後も必ず見つかります。問われるのは、見つかった後にどれだけ早く正しく判断できるかです。「止める判断」を誰が下すのかをあらかじめ決めておくことが、被害を最小限に抑える何よりの備えとなります。

© Grant Thornton Japan. All rights reserved.

太陽グラントソントン