【2026/10/23 PHP に関する重大な脆弱性に関しての DDS 見解】

【推奨事項】
今回公表された PHP の脆弱性については、対象となる PHP バージョンを利用している場合には影響を受ける可能性があるため、まずは各 Web サイト（コーポレートサイト、採用サイト等）の管理会社または運用委託先に状況確認を行うことを推奨します。

【確認項目】
確認項目としては、少なくとも以下を依頼するとよいと考えております。

・当該サイト・サーバにおける PHP 利用有無
・利用中の PHP バージョン
・修正版（PHP 8.5.12、8.4.27、8.3.36、8.2.35 相当）の適用状況
・OS やミドルウェアベンダーによるセキュリティパッチ提供状況
・PHP 本体を直接更新していない場合の代替的な対策内容
・利用中バージョンのサポート状況
・まだ PHP を最新版に更新できていなくても、脆弱性の影響を受けないよう何か対策をしているか
・不正アクセスや異常ログ等の有無

PHP のバージョン番号が古く見えても、OS ベンダーが脆弱性修正のみを取り込んでいる場合があります。そのため、バージョン番号だけで安全・危険を判断せず、「今回の脆弱性への修正が適用済みか」を管理会社へ確認することが重要です。
そのため、単純なバージョン番号の確認だけではなく、「当該脆弱性に対する修正が適用済みであること」を管理会社へ確認することが重要と考えます。

【見解】
現時点での被害や侵害の事実が確認されていないとした場合、まずは影響有無およびパッチ適用状況の確認を優先し、その結果を踏まえて追加対応の要否を判断する進め方が適切と考えます。

以上、ご参考にしていただければ幸いです。