

2026 年 10 月 22 日

お客様・パートナー各位

株式会社日本システムブレイズ
情報セキュリティ管理責任者

PHP の脆弱性（CVE-2026-109618、CVE-2026-109619） に関する弊社の対応状況について（ご報告）

拝啓 時下ますますご清栄のこととお慶び申し上げます。平素は格別のご高配を賜り、厚く御礼申し上げます。

さて、2026 年 10 月 21 日、The PHP Group より、PHP における複数の脆弱性（CVE-2026-109618、CVE-2026-109619。通称「PHP2Shell」）に関するセキュリティアドバイザリが公表されました。また、同年 10 月 22 日には、独立行政法人情報処理推進機構（IPA）および一般社団法人 JPCERT コーディネーションセンター（JPCERT/CC）から注意喚起が発出されております。

弊社では、本件の公表を受け、弊社が提供する業務システムおよび弊社ウェブサイトへの影響について確認を行いました。つきましては、その結果および対応状況を下記のとおりご報告申し上げます。

敬具

記

1. 本脆弱性の概要

項目	内容
脆弱性識別子	CVE-2026-109618（メモリ不足エラー処理に起因する脆弱性） CVE-2026-109619（リクエスト処理に関連する脆弱性）
公表元	The PHP Group（2026 年 10 月 21 日公表）
想定される影響	遠隔の第三者により、PHP の実行プロセスの権限で任意のコードを実行される可能性
影響を受けるバージョン	PHP 8.2.35、8.3.36、8.4.27、8.5.12 より前の各系列のバージョン（PHP 8.1 以前のサポート終了版を含む）
修正済みバージョン	PHP 8.2.35、8.3.36、8.4.27、8.5.12

2. 弊社提供業務システムへの影響

弊社がお客様およびパートナーの皆様提供している業務システムは、いずれも PHP を利用していません。したがって、本脆弱性による影響はございません。

弊社業務システムに関し、お客様およびパートナーの皆様における追加のご対応は不要です。

3. 弊社ウェブサイトへの影響および対応状況

(1) 利用状況：弊社ウェブサイト (<https://nsb-inc.co.jp/>) では、PHP を利用しております。

(2) 対策の実施状況：本脆弱性を修正したセキュリティパッチを適用済みです（適用日：[2026 年 10 月 22 日]、適用後のバージョン：[PHP 8.4.27]）。

(3) 被害の有無：2026 年 10 月 22 日現在、本件に起因する不正アクセスおよび情報漏えいは確認されていません。

4. 今後の対応

弊社では、弊社ウェブサイトの監視を継続するとともに、関係機関等から発信される最新情報の収集に努めてまいります。新たにご報告すべき事項が判明した場合には、速やかにお知らせいたします。

5. 参考情報

(1) 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（CVE-2026-109618、CVE-2026-109619：PHP2Shell）](#)」（2026 年 10 月 22 日）

<https://www.ipa.go.jp/security/security-alert/2026/alert20261022.html>

(2) 一般社団法人 JPCERT コーディネーションセンター（JPCERT/CC）「[PHP における複数の脆弱性（CVE-2026-109618、CVE-2026-109619）に関する注意喚起](#)」（JPCERT-AT-2026-0033、2026 年 10 月 22 日） <https://www.jpcert.or.jp/at/2026/at260033.html>

(3) The PHP Group「[Security advisory: Critical remote code execution vulnerabilities, update now](#)」（2026 年 10 月 21 日）
<https://www.php.net/archive/2026.php#2026-10-21-5>

6. 本件に関するお問い合わせ先

個人情報・特定個人情報／情報セキュリティに関する苦情・相談窓口

電話：03-3861-1121（受付時間：平日 [9:00～17:00]）

E-mail：privacy@nsb.jp

以上