2026 年 10 月 30 日

株式会社 e プリントサービス

当社の情報セキュリティ対策について

平素より格別のご高配を賜り、厚く御礼申し上げます。

昨今、企業への不正アクセスや情報漏えいの事案が相次いでいるほか、2026 年 10 月には、Web システムで広く使われているプログラミング言語「PHP」において重大な脆弱性が公表されました。こうした状況を受け、お取引先様をはじめ関係者の皆様から、当社のセキュリティ対策についてお問い合わせをいただいております。

つきましては、当社の情報セキュリティに関する取り組みと、今回の脆弱性への対応状況について、以下のとおりご報告いたします。

1. 基本方針

当社は、コンビニエンスストアのプリントサービス、システム開発、IT アウトソーシング等の事業を通じて、お客様の大切な情報をお預かりしております。情報資産の保護を経営上の重要課題と位置づけ、プライバシーマーク（登録番号：10822783）の認定のもと、個人情報保護マネジメントシステムを運用しております。

セキュリティ対策は一度実施すれば終わるものではないと考え、新たな脅威や脆弱性の情報に応じて対策を見直し、継続的に改善しております。

2. PHP の脆弱性への対応

（1）脆弱性の概要

2026 年 10 月 21 日、PHP の開発元から、複数の重大な脆弱性（CVE-2026-109618、CVE-2026-109619）とその修正版が公表されました。悪用された場合、認証を経ずに外部からサーバー上で任意のプログラムを実行されるおそれがあり、深刻度は最も高い水準（CVSS 9.2）と評価されています。10 月 23 日には、特定の設定の場合に影響する関連の脆弱性（CVE-2026-115560）も追加で公表されました。

JPCERT コーディネーションセンターも注意喚起を行っており、攻撃を試みる通信が国内外で観測されています。

（参考）

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」
https://www.jpcert.or.jp/at/2026/at260033.html

（2）当社の対応

当社は公表直後から対応にあたり、以下の措置を講じました。

・当社の自社サービス、社内システム、および当社が開発・運用に携わるお客様向けシステムを対象に、PHP を使用しているシステムを全社で総点検し、影響の有無と範囲を特定しました。
・修正版が提供されているシステムは、修正版への更新を行いました。
・直ちに更新できないシステムについては、開発元および公的機関が推奨する緩和策（設定の変更、リクエストの制限等）を適用しました。
・あわせて、WAF による防御の強化、管理画面等への接続元の制限、不要な公開の停止を行い、攻撃を受けにくい状態にしました。
・アクセスログ・エラーログ等を確認し、不正なアクセスの痕跡がないかを調査しました。
・保守を委託している事業者とも情報を共有し、作業を分担して対応を進めました。

以上により、緩和策を含む暫定措置は完了しております。

（3）現在の状況

本日時点で、当社の自社サービスにおいて、本脆弱性を悪用された被害は確認されておりません。

（4）今後の対応

緩和策は確認されている攻撃手法に対する一時的な措置であり、根本的な対策はサポート中のバージョンへの移行です。当社は、旧バージョンで稼働しているシステムについて、サポート中の PHP への移行を計画的に進めてまいります。また、今後も開発元や公的機関からの追加情報を注視し、必要な対策を継続して実施いたします。

なお、同時期に公表された Node.js 等のその他のソフトウェアの脆弱性についても、影響を確認のうえ、順次更新を進めております。

3. 日常的に実施している対策

今回の脆弱性への対応に限らず、当社では日頃から以下の対策を実施しております。

分野	主な取り組み
管理体制	プライバシーマーク制度に基づく個人情報保護マネジメントシステムを運用しています。 システム管理者による定例会議を開催し、運用状況・インシデント・リスクを継続的に確認しています。 インシデント発生時の報告・対応ルールを定め、社内に周知しています。
脆弱性管理	公的機関や脆弱性情報サービスから日常的に情報を収集し、重要度に応じて速やかに修正プログラムを適用しています。 サポートが終了したソフトウェアは、計画的にサポート中のバージョンへ移行しています。

分野	主な取り組み
Web サービスの防御	WAF（Web アプリケーションファイアウォール）等により、外部からの攻撃を防御しています。 管理画面など重要な画面は、接続元を限定したうえで運用しています。
監視・ログ	サーバーへのアクセスや認証の記録を取得し、監視設定とあわせて定期的に点検・見直しを行っています。
アカウント・認証	管理者アカウントの認証を強化し、多要素認証の適用を進めています。 人事情報と連携してアカウント・グループを管理し、不要なアカウントを整理しています。
端末の保護	業務端末にウイルス対策ソフトを導入し、管理コンソールで一元管理しています。 端末の暗号化について、管理ルールの整備を進めています。
新しいツールの導入	クラウドサービスや生成 AI ツールを新たに導入する際は、事前にリスクを確認する申請手続きを設けています。
委託先との連携	システムの開発・保守を委託している事業者と、脆弱性への対応方針や作業分担を協議し、連携して対策を実施しています。
従業員教育	個人情報保護および情報セキュリティに関する従業員教育を実施しています。

4. お客様への対応について

当社が提供・運用するサービスやシステムに関して、万一お客様に影響が生じた場合、またはご不安な点がございます場合には、事実関係を速やかに確認のうえ、真摯に対応いたします。ご不明な点がございましたら、下記の窓口までお問い合わせください。

今後とも、皆様に安心してご利用いただけるよう、情報セキュリティの維持・向上に努めてまいります。引き続き変わらぬご愛顧を賜りますよう、よろしくお願い申し上げます。

以上

【本件に関するお問い合わせ先】
株式会社 e プリントサービス
担当部署：管理本部
所在地：〒110-0005 東京都台東区上野 7-2-10　上野駅前第一生命ビルディング 5F
TEL：03-5830-1733　E-mail：ep-office@e-pri.co.jp