報道関係者各位

2026年4月30日
株式会社ピーエスアイ

2026年GW明けに急増懸念、生成AI時代のサイバー攻撃に注意
中小企業に広がるリスク、株式会社ピーエスアイが対策ガイド公開

～連休明けに増えるフィッシング詐欺・未更新端末・シャドーITリスクへ注意喚起～

株式会社ピーエスアイ（本社：東京都新宿区新宿5-5-3、代表取締役社長：戸澤 昌典、以下、当社）は、2026年のゴールデンウィーク（以下GW）を前に、「長期休暇明けにおけるセキュリティリスクと対策」に関するガイドを公開しました。

長期休暇前後は、システム更新の遅れや大量メール処理、持ち出し端末の再接続などが重なり、情報セキュリティ事故が発生しやすい時期です。2026年はこれに加え、生成AIの普及により、自然な日本語による詐欺メールや社内ルール未整備のAI利用など、新たなリスクへの対応も求められています。

■2026年も深刻化するサイバー脅威：拡大する中小企業への影響

警察庁が公表した「令和7年におけるサイバー空間をめぐる脅威の情勢等について」によると、2025年のランサムウェア被害報告件数は226件となり、依然として高水準で推移しています。被害企業の中心は中小企業で、2025年上半期には全体の約3分の2を占めました。

また、日本情報経済社会推進協会（JIPDEC）の「企業IT利活用動向調査2026」では、サイバー攻撃被害に伴い「顧客情報や取引先情報などの機密情報が漏えいした」と回答した企業の割合が、前回調査の29.3%から35.1%へと約6ポイント上昇しており、被害の深刻化がうかがえます。

さらに、情報処理推進機構（IPA）が2026年1月29日に発表した「情報セキュリティ10大脅威2026」では、ランサムウェアによる被害が11年連続で組織部門1位となり、生成AIの普及

を背景に、AIを悪用したフィッシングやマルウェア生成など、新たな脅威への警戒も高まっています。

■ 背景：なぜ「連休明け」に注意が必要なのか

2026 年の GW は、日程の組み合わせによって長期休暇となる企業も想定されます。長期休暇期間中は、通常時と比べてシステム運用体制が縮小される場合があり、休暇明けには未対応の更新作業や大量のメール確認などが集中しやすくなります。

特に連休明けは、以下の 3 つの要因に注意が必要です。

1. **OS・ソフトの未更新**：休暇中に公開された修正プログラム（セキュリティパッチ）が適用されていない端末が残る可能性があります。

2. **大量メール処理による確認不足**：大量の未読メールに紛れて不審メールや偽装メールを見落とすリスクがあります。

3. **社外利用端末・外部媒体の持ち込み**：在宅環境や外出先で利用した端末、USBメモリ等を社内ネットワークへ接続する際は注意が必要です。

■ 休暇明けに注意すべき「3つの主要リスク」

1. 緊急対応を装う詐欺メール・ビジネスメール詐欺（BEC）

近年は生成AIの普及により、自然な日本語や実在企業に似せた文面のメールが作成されやすくなっており、従来より見分けが難しくなる傾向があります。特に連休明けは、「支払期限が迫っています」「アカウント再認証が必要です」など、緊急性を装うメールに注意が必要です。

不用意にリンクをクリックしたり、添付ファイルを開いたりすると、認証情報の窃取やマルウェア感染につながるおそれがあります。

2. 未修正の脆弱性を突いた攻撃

休暇中にOS、ブラウザ、VPN機器、業務ソフトウェア等の更新情報が公開される場合があります。しかし更新未実施の状態で利用を再開すると、既知の脆弱性を悪用した攻撃の対象となる可能性があります。業務再開前に、主要機器・ソフトウェアの更新状況確認が重要です。

3. シャドーITによる情報漏えいリスク

「休み中も少しだけ仕事をしよう」という責任感から、会社の許可を得ていない私用のクラウドストレージや個人のSNS、個人のメールアドレスへ業務情報を保存・送信する行為は、一般に「シャドーIT」と呼ばれ、現代のセキュリティにおける最大の死角の一つです。その最大のリスクは、万が一情報が流出しても、会社の管理外であるため「いつ、誰が、何を漏らしたのか」を追跡できないことです。企業は、禁止だけでなく、利用ルール整備と代替手段の提供が重要です。

■ ピーエスアイが推奨する「セキュリティ・チェックリスト」

【休暇前】の確認事項

・使用しない端末や機器の停止、不要サービスの停止確認
・VPN機器、サーバー、PCの更新確認
・持ち出し端末の管理ルール再確認

【休暇明け】の業務開始時のルーティン

・更新確認
OS、ブラウザ、セキュリティソフト、VPN機器等の更新状況を確認する。

・不審なメールは「開かない」
差出人やURL、添付ファイルを確認し、不審な場合は管理者へ相談する。

・外部媒体・持ち出し端末確認
休暇中に使用したUSBメモリなどは、必ずウイルススキャンを行ってから使用する。

当社では、2026年は「生成AIの利便性拡大」と「情報管理リスク増大」が同時進行する年と捉え、企業の現実的な対策支援を強化しています。

【株式会社ピーエスアイについて】

株式会社ピーエスアイ（PSI）は、1994年の設立以来、ITネットワークおよびサイバーセキュリティに特化した専門ディストリビューターとして、海外の最先端技術をいち早く国内へ導入・定着させてきました。

【会社概要】

社名：株式会社ピーエスアイ（PSI）
所在地：〒160-0022 東京都新宿区新宿5-5-3 建成新宿ビル4階
設立：1994年
TEL：03-3357-9980
FAX：03-5360-4488
URL：https://www.psi.co.jp
事業内容：サイバーセキュリティ製品の販売および導入支援、運用サポート、ITコンサルティング

【本プレスリリースに関するお問い合わせ先】
株式会社ピーエスアイ
広報担当：内藤
電話：03-3357-9980
E-mail: psi-press@psi.co.jp