2025年11月末日
株式会社ピーエスアイ

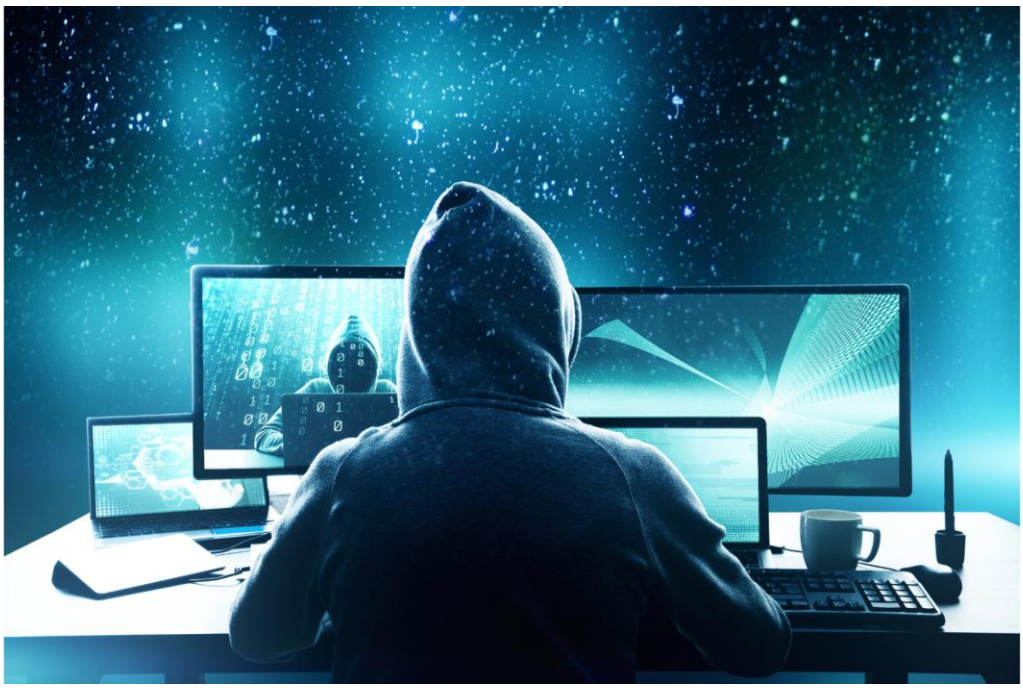
# 【重要】サイバー犯罪が狙う年末年始の「気の緩み」：企業と個人が取るべき対策とは

年末年始は、多くの企業や組織が長期休暇に入り、オフィスでの監視体制が手薄になるなど、セキュリティの「空白期間」が生じがちです。また、一般の方々も、オンラインショッピング、旅行の予約、帰省先でのWi-Fi利用など、普段とは異なるオンライン活動が増加します。

サイバー犯罪グループは、この「手薄になる時期」と「個人の気の緩み」を狙って活動を活発化させる傾向があります。特に2025年は、ランサムウェアによる攻撃で大企業が被害受け広範囲な影響がありました。

ピーエスアイは、皆様の「安心」を守るため、企業・一般ユーザーの皆様に向けて、この時期特有の具体的なサイバーセキュリティの脅威と今すぐ実施できる対策を分かりやすく解説します。

## 脅威その１：長期休暇の混乱に乗じる、巧妙な「なりすまし」フィッシング詐欺



人や物の移動とそれに伴う様々な手続きが増える年末年始は、配送業者、金融機関、ECサイト、旅行会社を装ったフィッシングメールやSMS（スミッシング）が例年急増します。

## 具体的な手口

### ①不在通知・再配達依頼詐欺

「荷物のお届けに失敗しました。詳細はこちらのURLをご確認ください。」といったSMSやメールで、偽のサイトへ誘導し、クレジットカード情報やApple ID/Googleアカウント情報を盗み取ります。

### ②旅行・予約キャンセル料詐欺

実在の旅行会社を装い、「予約がキャンセルされました」「キャンセル料が発生しています」と不安を煽り、決済情報を入力させます。

### ③生成AIによる高度化

生成AIの活用により
・自然な日本語で書かれたメール
・精巧に再現された企業のロゴ
・過去の実際の問い合わせメールを模した偽メールなど、
一見しただけでは判断することが難しくなっています。

## PSIからの対策アドバイス

### ①差出人を徹底的に確認する

メールの送信元アドレスや、SMSに記載されたURLをタップ/クリックする前に、企業の公式サイトURLと一致するかを必ず確認してください。

### ②公式アプリ・公式サイトから確認する

不安な通知が来たら、メールやSMSのリンクからではなく、いつも使っている公式アプリやブラウザのお気に入りからアクセスし、通知内容が事実かを確認しましょう。

### ③多要素認証（MFA）を設定する

サービスにログインする際は、IDとパスワードだけでなく
・本人だけが知っている情報
・指紋や顔などの生体情報

など、スマートフォンやSMSを使った多要素認証（MFA）を必ず設定してください。万が一パスワードが盗まれても、不正ログインを防ぐことができます

## 脅威その２：【企業向け】ネットワークの「入口」を狙う、VPN・ルーターへのランサムウェア攻撃


長期休暇中は、企業のネットワーク監視が緩むため、外部からアクセスするためのVPN機器や、オフィス内のルーターといった「ネットワークの入口」が狙われやすくなります。

### どのような被害が発生するか

**①VPN機器の脆弱性悪用**
企業が利用するVPN機器の脆弱性が突かれ、社内ネットワークへ不正侵入されます。

**②ランサムウェアの感染拡大**
不正侵入後、ランサムウェア（身代金要求型ウイルス）を仕掛けられ、企業の重要データが暗号化され、業務停止や巨額の身代金要求につながります。

**③顧客情報の漏洩**
データが暗号化されるだけでなく、「公開する」と脅され、顧客や取引先の機密情報が外部に漏洩するリスクも伴います。

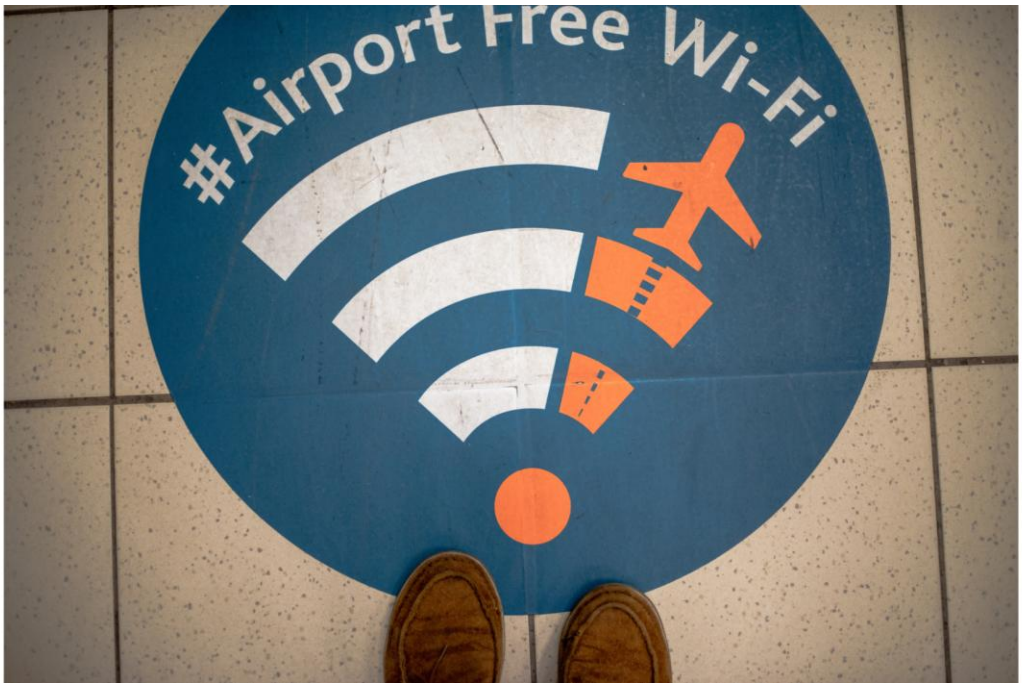
PSIからの対策アドバイス（企業・組織向け）

**①休暇前のパッチ適用を徹底する**
長期休暇に入る直前（最終営業日）に、VPN機器、ファイアウォール、サーバーOSなど、全てのネットワーク機器とシステムに対し、最新のセキュリティパッチが適用されているか最終確認を行いましょう。

**②ログ監視体制を維持する**
休暇中も、VPNアクセスや重要なサーバーへのアクセスログを監視する体制（外部委託やアラートシステム）を維持し、異常な通信がないかをチェックできるようにしてください。

**③バックアップを物理的に隔離する**
ランサムウェアに感染してもデータを復旧できるよう、最新のバックアップをネットワークから切り離された状態（オフライン）で保管しましょう。

## 脅威その３：知らぬ間に、自分が”加害者”になることも！公共Wi-Fiと家庭内IoT機器のリスク




帰省先や旅行中に利用する公共の無料Wi-Fi、そして年末に購入するスマート家電には、気づかないうちに「情報漏えいの被害者」になるだけでなく、自分の端末や家電が “攻撃の踏み台＝加害者” にされてしまうリスクがあります。

## どのようなリスクがあるか

**①悪意ある公共Wi-Fi（空港・カフェ・ホテルなど）**
攻撃者が用意した偽のWi-Fiアクセスポイント（例：「Free_Airport_Wi-Fi」など）に接続してしまうと、通信が全て傍受され、送受信するパスワードや個人情報が盗み見られる可能性があります。

**②家庭内IoT機器の乗っ取り**
ネットワークカメラ、スマートスピーカー、ゲーム機などのIoT機器は、初期設定のままの簡単なパスワード（例: admin や 123456）を利用していると、外部から乗っ取られ、盗聴や踏み台攻撃の拠点に利用されてしまいます。

## PSIからの対策アドバイス（一般ユーザー向け）

**①公共Wi-Fiでは「VPN接続」を徹底する**
帰省・旅行先では、必ずVPNサービスを経由し、通信を暗号化して情報傍受のリスクを排除しましょう。

**②「https://」を確認する**
重要な情報を入力するサイトは、必ずURLの先頭が「https://」で始まっているか（鍵マークがあるか）を確認してください。

**③IoT機器のパスワード変更**
新しいIoT機器を設定する際は、すぐに初期パスワードを複雑で他と異なるものに変更し、ファームウェアを最新の状態にアップデートしましょう。

**④OS/アプリの自動アップデート設定**
ご自身のスマートフォンやPCのOS、各種アプリの自動アップデート設定をオンにし、常にセキュリティを最新の状態に保ってください。

## 脅威その４：年始明けの「業務再開」を狙う攻撃

長期休暇の終了後、従業員が業務に戻るタイミングもまた、サイバー攻撃の格好の標的となります。休暇中の出来事や未処理の業務に関するメールを装った攻撃は、特に警戒が必要です。

### 具体的な手口

#### ①長期休暇中の未対応メールを装った攻撃

「〇〇（休暇中に発生した事案）に関する緊急対応依頼」「未払い請求に関する重要なお知らせ」といった、業務に関連する緊急性を装ったメールが増加します。

#### ②出勤直後の混乱に乗じたフィッシング

休暇中にシステムメンテナンスが行われたと偽り、新しいログイン画面へのアクセスを促すなど、混乱に乗じた認証情報窃取を狙います。

### PSIからの対策アドバイス（企業・組織、一般ユーザー向け）

#### ①出勤直後のメールは「ひと呼吸おいて」確認する

休暇明けの大量のメール処理で急いでいる時こそ、件名や差出人が少しでも不審なメールは、一度立ち止まって差出人のアドレスや内容を慎重に確認して下さい。

②IT部門への連絡体制を確認する

不審なメールや通信を発見した場合、どこに、誰に報告すべきか、休暇明けであってもすぐに連絡できるよう、社内の連絡フローを再確認して下さい。

## まとめ

年始年末は、サイバー犯罪グループに狙われる時期です。従業員への社内周知やルールの徹底を促し、もし巻き込まれたときの為の復旧対策を再度見直しましょう。

PSIでは、こうした年末年始のリスク対策に役立つソリューションを各種提供しています。詳しくは、以下の製品一覧からご確認ください。

https://www.psi.co.jp/maker/

【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丁目5-3 建成新宿ビル 4F
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

【報道関係者様からのお問い合わせ先】

株式会社ピーエスアイ 広報担当：内藤
電話番号：03-3357-9980
Eメールアドレス： psi-press@psi.co.jp