報道関係者各位

2026年2月18日
株式会社ピーエスアイ

# サイバーセキュリティのピーエスアイ、年度末の「退職・入社」に伴う情報漏洩リスクに警鐘

## 巧妙化する内部不正と“見えないデータ持ち出し”を防ぐ「3つのセキュリティ再点検ポイント」を公開

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、人の入れ替わりが激しくなる新年度（3月～4月）にかけて、企業の機密情報や顧客データの持ち出しリスクが高まることを受け、サイバーセキュリティ月間の取り組みの一つとして企業が取り組むべき「情報漏洩対策の再点検」についてチェックポイントを公開しました。

### ■年度末は「うっかり情報漏洩」と「悪質な持ち出し」の境界線に

例年、年度末から新年度にかけては退職や異動、新入社員の受け入れが一気に進み、組織内の情報管理が一時的に緩みやすい時期です。IPA（独立行政法人情報処理推進機構）の調査によると、企業における情報漏洩の主な原因は「内部不正」や「不注意」であり、これらは2016年以降、「情報セキュリティ10大脅威」として10年連続で取り上げられています。

特に退職者が「自身が作成した成果物だから」という誤った認識でデータを持ち出すケースが後を絶ちません。また、昨今のテレワーク定着やクラウドサービスの普及により、USBメモリだけでなく、個人のクラウドストレージやチャットツールを通じた**「見えない持ち出し」**が容易になっている点も、企業にとって大きな脅威となっています。

## ■ピーエスアイが提言する「年度末に見直すべき3つのセキュリティ死角」

当社がこれまでに蓄積した知見に基づき、この時期に特に見直すべきチェックポイントを公開いたします。

### 1.「ID・アカウント」の即時削除プロセス

退職者が利用していたSaaS（クラウドサービス）や社内システムの権限が、退職後も数日間有効なまま放置されているケースが目立ちます。これを悪用した外部からの不正アクセスを防ぐための自動連携システムの構築が急務です。

### 2.「シャドーIT」によるデータの持ち出し

会社が許可していない個人のUSBメモリやストレージサービスへの書き出し制限。特に重要ファイルに対する「コピー」「印刷」のログを監視していることを社内に周知するだけで強い抑止力となります。

### 3.「入社時・退職時」のセキュリティ教育の再設計

形式的な誓約書の提出だけでなく、「何が機密情報にあたるのか」「持ち出した場合の法的リスク」を具体的事例とともに共有するリテラシー教育が、最大の防御壁となります。

## ■ピーエスアイ担当営業からのメッセージ

情報漏洩対策は、もはやIT部門だけの問題ではありません。人の入れ替わりが発生するこの時期に、情報管理体制を見直せているかどうかは、企業のガバナンスや経営姿勢そのものが問われるポイントです。

デジタル化が進み、**情報の持ち出しは“一瞬で”行える**ようになりました。特に年度末は、多忙な業務の陰でセキュリティへの意識が希薄になりがちですが、私たちは、製品の提供だけでなく、こうした『人の動き』に伴うリスクを可視化し、企業の大切な資産を守るための支援を続けてまいります。

### 【株式会社ピーエスアイについて】

株式会社ピーエスアイは、長年サイバーセキュリティ製品の販売や導入支援を通じて、国内のIT環境の安全に寄与してまいりました。脅威が複雑化する現代において、情報の鮮度は最大の防御策となります。当社ホームページ上では「PSI CyberSecurity Insight」を通じた質の高いセキュリティ情報を発信継続しております。皆様が安心してデジタル技術を活用できる社会の実現に貢献してまいります。

「PSI CyberSecurity Insight」はこちらからご覧いただけます。
URL：https://www.psi.co.jp/topics/insight_list.html

**【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

**【お問い合わせ先】**
本プレスリリースに関するご質問は、下記までお気軽にご連絡ください。

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