企業のリスクに繋がる！ シャドーITの危険性！

シャドーITとは企業が使用を許可していないIT機器やアプリなどを従業員が無断で導入、利用することです。不正アクセスや情報漏えいなどの引き金となるだけでなく、事故が発生したことに気付かず、大きな損害につながる可能性があるので注意しましょう。

▸シャドーＩＴの主な例

私有デバイス（スマートフォン・パソコン・USBメモリなど）

既にマルウェアに感染している私有デバイスを社内ネットワークに接続してしまうと、社内に感染が広がり、重要なデータが漏れる可能性があります。
また、職場用デバイスに比べてセキュリティ対策が甘くなりやすいと言われているため、勝手に利用するのはやめましょう！

フリーメール

簡単・無料・すぐ使えるフリーメールはその利便性の高さ故、シャドーITとして使われやすいものの一つです。
社外秘情報や個人情報を業務とは全く関係のない人に誤送信する、アカウントが乗っ取られて情報漏えいするなどの危険性が潜んでいます。

メッセージアプリ・ＳＮＳ

メッセージアプリ・SNSは「自分が普段使っているもの」「周りのみんなが利用しているもの」をどうしても利用したくなります。
プライベートで使用しているアカウントを業務で使うと誤送信・情報漏えいのリスクに加え、企業が管理できないところに社内情報が残り、リスク管理が困難になります。

クラウドストレージサービス

インターネット上にファイルの保存や共有ができる「クラウドストレージサービス」を勝手に業務利用していませんか？
公開範囲を間違ってしまい組織の情報が漏えいしたとしても、組織管理していないため、漏えいしたことに気付かず、長期間さらされっぱなし…という状況になってしまうかも。

▸シャドーＩＴへの対策

○社内のシャドーＩＴの現状を把握し、組織の課題や改善点を確認
○シャドーＩＴの危険性について、社内教育を実施
○未許可のデバイスやサービスを使用しなくても業務ができる環境を整備

情報漏えいは組織の信用、信頼に大きな影響を与えます！

２月１日～３月18日はサイバーセキュリティ月間です！