あなたの会社のセキュリティ本当に大丈夫ですか？

最新のセキュリティ機器だけでは守り切れません！

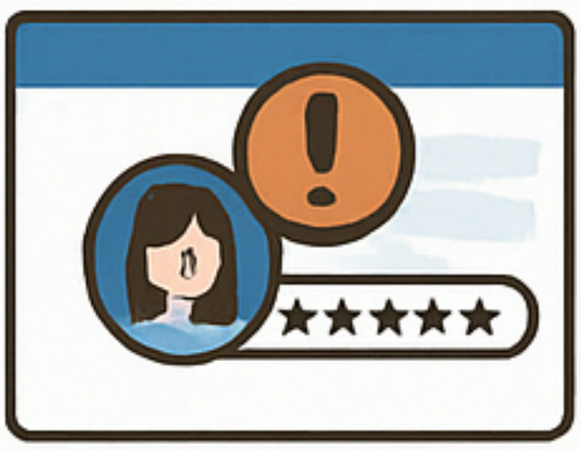
近年、様々なセキュリティ機器が登場し、「どれを導入すればいいのか分からない」と感じていませんか？ UTM、EDR、多要素認証…確かにこれらは重要です。しかし、どんなに優れた機器を導入しても、たった一つのヒューマンエラーが、情報漏洩やランサムウェア感染、その他のサイバー攻撃のきっかけになることをご存知でしょうか？

攻撃の約 8 割は「人」が狙われる

巧妙化するサイバー攻撃の多くは、システムの脆弱性よりも「人の心理」を巧みに突いてきます。
フィッシングメール、標的型攻撃、不審な Web サイトへの誘導…これらはすべて、人のうっかりミスや知識不足を狙ったものです。鉄壁のセキュリティシステムも、従業員一人ひとりの意識が低ければ意味がありません。

ヒューマンエラーを防ぐために、今日からできること

高価な危機を導入する前に、まずは従業員一人一人の意識を高め具体的な対策を講じることが最も効果的です。



OS やソフトウェアは常に最新に

OS やソフトウェアのアップデートには、セキュリティの穴を塞ぐ重要な更新が含まれる場合があります。

怪しいメールに警戒を！

・見知らぬ差出人、緊急を装う件名（例：「アカウント凍結」など）には注意。
・メール内のリンクはクリック前に URL を確認する。
例：「rakuten.co.jp」に見せかけた「rakuten-login.xyz」などの偽装が多発しています。
・添付ファイルも要注意。特に「請求書 .zip」や、「.exe」「.scr」など見慣れない拡張子のファイルは絶対に開かないこと。マクロの有効化も NG です！

パスワードは強固に！そして管理の工夫を！

・**複数のサービスで使い回さない**ことが鉄則。
ひとつ漏れれば、他も芋づる式に危険にさらされます。
・パスワードは英数字・記号を含む長くて複雑なものに（例：「s3cuR1ty_F0r_You!」）。
・安全なパスワード管理ツールを活用すれば、
記憶に頼らず安全性を保てます。

社内ルールと意識づけが基本

・セキュリティを守る第一歩は、社内で定められた基本ルールを確実に守ることです。一人の気のゆるみが、大きな事故につながることもあります。
・ウイルス感染や情報漏えいのきっかけを作らないよう心がけましょう。特に無料を謳うツールやサービスサイトは要注意。見た目は正常でも裏で情報を盗むマルウェアが仕組まれている可能性があります。
・疑問点は IT 担当者に相談することを習慣化しましょう。

詳しく知りたい方はクイックスまで！

クイックス株式会社
03-5456-1511　dial@quix.co.jp