

SecurityNews

2

身近なミスを防ぐセキュリティ習慣

あなたの会社も「他人事」ではない！ VPNサイバー攻撃対策ガイド

テレワークで利用されるVPNがサイバー攻撃の標的となり、業務停止や情報漏洩など甚大な被害につながるケースが増えています。会社全体で取り組むべき具体的なセキュリティ対策を提示します。

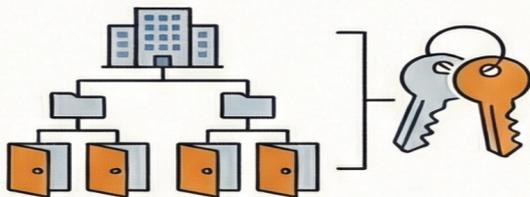
経営者が断行すべき 「3つの防壁」



- 1 アップデートの徹底**
VPN機器やPCを常に最新の状態に保ち、セキュリティの穴を塞ぎます。

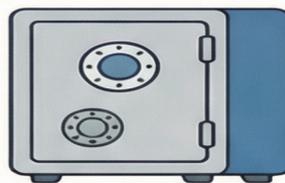


- 2 多要素認証 (MFA) の義務化**
不正ログインを防ぐための最終防衛ラインとして導入します。

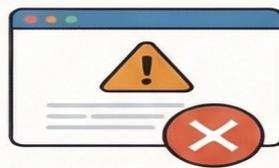


- 3 権限の最小化と整理**
不要な侵入口を減らし、万一の際の被害範囲を限定します。

全社員が実践すべき 「セキュリティ3ヶ条」



- 1 パスワードは「長さ」が重要**
15文字以上のパスフレーズを設定し、使い回しは絶対にしません。



- 2 身に覚えのない通知は即報告**
不審なログイン通知は「拒否」し、すぐにシステム担当へ報告します。



- 3 「少しの違和感」を見逃さない**
不審なメールやPCの異常は、攻撃のサインかもしれません。迷わず報告します。



エフシーバンク

サイバーリスク対策の専門店