

サイバーセキュリティ - 最低限の対策_1

1. サイバーセキュリティは経営判断の一部

企業規模に関係なく、最低限の防御策が重要

サイバー攻撃のリスクは大企業だけでなく、中小企業や製造業にも及びます。どの程度のセキュリティ対策を講じるかは、経営者の判断によって決まり、企業の信用や業務継続に直結します。



企業のセキュリティ対策は「家の鍵」と同じ。鍵をかけなければ誰でも侵入できますが、頑丈な鍵を使えば泥棒を防ぐことができる。企業も最低限の防御策を整えることで、情報資産を守りましょう。

2. 必須の防御層、EPP とファイアウォール

企業の基本的な防御策としての 2 つの要素

EPP(Endpoint Protection Platform)は企業の端末を総合的に保護し、ウイルスやランサムウェアなどの脅威を防ぐ役割を果たします。一方、ファイアウォールはネットワークへの不正アクセスをブロックし、外部の脅威から企業を守ります。企業の規模や業務環境を問わず、これらの対策は不可欠です。



EPPは「家の防犯カメラ」、ファイアウォールは「玄関のセキュリティゲート」のようなもの。カメラが異常を検知し、ゲートが侵入者を防ぐことで、安全な環境を維持する。

サイバーセキュリティ - 最低限の対策_2

3. 経営方針による選択肢

EPP 導入が難しい場合の代替策

一部の企業は、EPP の導入が困難な場合があります。
PC が 2~3 台しかない企業では、
市販のセキュリティソフトを活用することで、最低限の防御策を確保できます。
ただし統合管理機能がないため、PC の定期的なアップデートが不可欠です。



EPP を導入できない企業は「防犯システムなしでドアにチェーンをかける」ようなもの。
完全な防御ではないが、何も対策しないよりは幾分か安全になります。

4. 企業に最適なセキュリティ戦略を構築する

統合管理か低コスト運用か、適切な選択を

EPP と市販のセキュリティソフトはそれぞれにメリット・デメリットがあるため、
企業の運用体制に応じた選択が重要です。
さらに、ファイアウォール導入の必要性も業務環境によって異なります。
経営者は外部の専門家と相談しながら、適切な防御策を決定することが求められます。



セキュリティ戦略の選択は「自宅の防犯プランを選ぶ」と同じ。セキュリティ会社と相談しながら最適なシステムを導入することで、安全性を最大化できます。