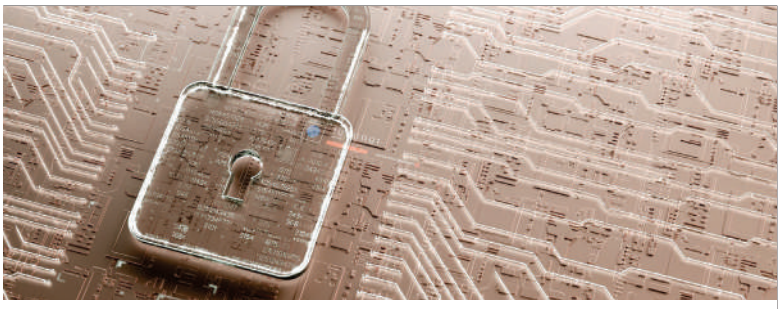


中小企業のためのサイバー攻撃対策

小規模事業者を守る最新のセキュリティ対策

サイバー攻撃の現状と脅威

サイバー攻撃の増加傾向と主な手法

サイバー攻撃の増加

近年、特に中小企業を狙ったサイバー攻撃が増加し、被害が拡大しています。

代表的な攻撃手法

ランサムウェア、フィッシングメール、ビジネスメール詐欺が主要な攻撃方法です。

被害の巧妙化

攻撃はますます巧妙化し、従業員が気づかず被害が広がる場合があります。

中小企業の対策重要性

適切な対策は企業の存続と信頼維持に不可欠な課題です。

中小企業の被害事例とリスク要因

実際の被害事例と影響

顧客情報漏洩

サイバー攻撃により中小企業の顧客情報が漏洩し、信頼を大きく損なう結果となりました。

業務停止の影響

マルウェア感染で社内システムが停止し、数日間の業務停止で売上損失が発生しました。

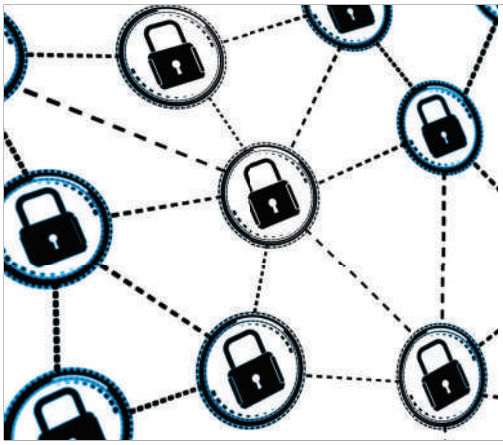
信頼関係の悪化

取引先との信頼が失われ、契約解除に至るなど企業の信用が大きく低下しました。

中小企業のリスク認識

セキュリティ体制が弱い中小企業は被害が深刻化しやすく、リスク認識と対策が必要です。

中小企業が狙われる理由



セキュリティの脆弱性と攻撃者の視点

中小企業の予算制約

多くの中小企業は限られたセキュリティ予算で対策が不十分になりやすいです。

IT人材の不足

専門知識を持つIT担当者不足が、攻撃時の初期対応の遅れを招いています。

サプライチェーンの脆弱性

中小企業は大企業のサプライチェーンの一部として攻撃の標的になることがあります。

基本的なサイバーセキュリティ対策

すぐに実施できる防御策

定期的なソフト更新

OSやソフトウェアの更新は脆弱性を修正し、サイバー攻撃のリスクを減らします。

強固な認証設定

強力なパスワードと多要素認証（MFA）の導入はアクセスを安全に保ちます。

従業員教育

従業員へのフィッシング対策教育により人的ミスによる侵入を防止します。

定期的なバックアップ

データの定期バックアップは万一の復旧を迅速にする重要な対策です。

中長期的なセキュリティ強化策

継続的な対策と外部支援の活用

セキュリティポリシー策定

企業独自のセキュリティポリシーは従業員の行動指針となり、守るべきルールを明確にします。

外部専門家の診断活用

ペネトレーションテストなどの外部診断で脆弱点を客観的に把握し、改善に役立てます。

サイバー保険の検討

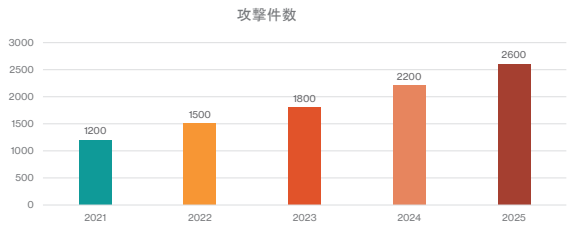
サイバー保険加入で被害発生時の金銭的リスクを軽減し、企業の安心を支えます。

インシデント対応計画

攻撃時の対応手順を事前に整備し、迅速かつ的確な対応で被害拡大を防ぎます。

サイバー攻撃件数の推移

攻撃件数の年次推移と傾向



浅間商事のご提案

取り組むべきこと

- UTMの導入によるネットワーク防御強化
- Windows11への入れ替えで最新のセキュリティに

守るべき資産の明確化

まず守るべき重要な資産を特定し、優先順位をつけることが防御の第一歩です。

人・技術・ルールの統合防御

人材教育、最新技術、明確なルールを組み合わせた三位一体の防御体制が必要です。

従業員意識の向上

従業員のセキュリティ意識を高めることが、即効性のある効果的な対策になります。

中長期的な対策と継続改善

外部支援の活用や保険検討とともに、脅威の変化に応じて見直しを続けることが不可欠です。