すべての企業が狙われる!?

VPN機器の適切な管理で防ぐ

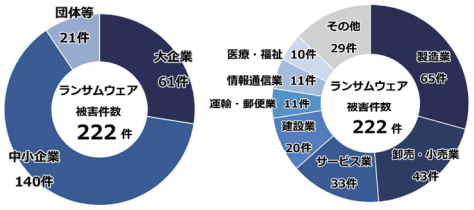
サイバー攻撃

最新の被害傾向

攻撃者は無差別に狙う

サイバー攻撃は機密情報や知的財産を所有する企業を狙うと考えていませんか？
最近のシステムを破壊するランサムウェア攻撃者は企業規模や業種を問わず、**穴がある企業を手当たり次第に攻撃**してきます。

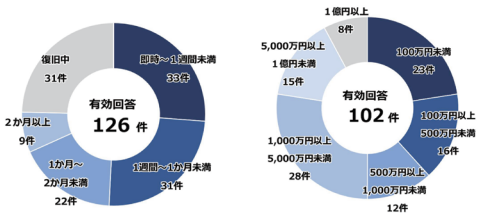
● 被害企業・団体等の規模別／業種別報告件数



※出典：警察庁サイバー警察局「令和６年における サイバー空間をめぐる脅威の情勢等について」

一度攻撃に合えば事業に深刻な影響

● 復旧等に要した期間／調査費用の総額／復旧期間と費用の関係性



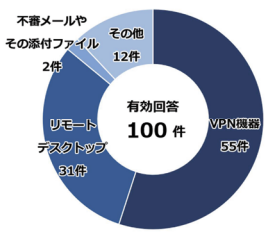
※出典：警察庁サイバー警察局「令和６年における サイバー空間をめぐる脅威の情勢等について」

ランサムウェア攻撃を受けてしまうと事業に深刻な影響が生じます。稼働中のサーバやパソコン、**過去の取引データのバックアップは暗号化（ロック）され使用できなくなります。**それらのシステムの入れ替えにも多大な影響が生じるだけではなく、取引先にも影響が。取引先とのメールや見積もり、預かっている機密情報は攻撃者に盗まれ、不特定多数に公開されることも珍しくありません。

攻撃者はVPN機器から侵入してくる

上記のような攻撃を仕掛けてくる攻撃者はどこからあなたの会社に侵入してくるのでしょうか？
日本国内で被害にあった**企業の半数以上は管理不十分な VPN** 機器からの侵入が原因でランサムウェアの被害にあっています。

● 感染経路



※出典：警察庁サイバー警察局「令和６年における サイバー空間をめぐる脅威の情勢等について」

裏面の対策ポイント3つを実施して被害を防ぎましょう。

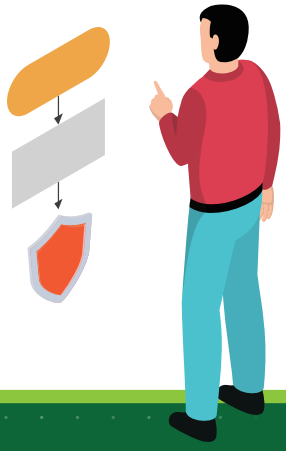
VPN機器の防御力をあげる3か条

対策1 パッチ適用の徹底

鍵が壊れ、窓が開き、警備員がいない建物は泥棒が侵入し放題。セキュリティホール（脆弱性）を放置することはそれと同じ状態です。攻撃者の侵入経路となるため、VPN 機器や OS、ソフトウェアはパッチを適用し最新の状態に保ちましょう。

対策2 多要素認証の設定

ID とパスワードの入力だけで済んでしまう“簡単な鍵”だけではすぐ破られてしまいますが、“複数のカギ”を掛ければ攻撃者の侵入は極めて困難となります。
VPN 機器の機能を有効化し、ログイン時にパスワード＋ワンタイムコードなど複数の要素を組み合わせることで、安全性を高められます。



対策3 複雑なパスワードの設定

よくある単純なパスワードは、泥棒が合鍵を持っているものと同じです。英大文字・小文字・数字・記号を組み合わせた強固なログイン用のパスワードを設定しましょう。

神奈川県警察
問い合わせ先 #9110 又は、最寄りの警察署までご相談ください
協力：株式会社マクニカ