

ランサムウェア、うちの会社は大丈夫？

3つの数字と、今月決める3つのこと

会社のデータを暗号化して業務を止め、「戻してほしければ払え」と脅す攻撃です。狙われているのは大企業だけではありません。入口もはっきり分かっています。

知っておく3つの数字

約6割

被害に遭った企業のうち、中小企業の割合

令和7年の警察庁集計。「うちは小さいから狙われない」は通用しません。

87.0%

VPN機器とリモートデスクトップからの侵入

2025年の感染経路(VPN 66.3%+リモートデスクトップ 20.7%)。メールの添付ファイルは2.2%だけ。

3,800万円

被害額の中央値(身代金は払っていない)

被害組織へのアンケートで、直近2年の値。払った組織はゼロ。業務停止による損失は含まれず、実際はこれより大きい。

実例: 保守契約を切ったVPN機器から JNSA 被害組織調査 No.4

製造業(従業員20~999名)。VPN機器の保守サービスを途中で解約していた。

→ 脆弱性が残ったVPN機器から侵入され、サーバーが暗号化される

→ カード情報の確認にも時間がかかり、業務の正常化まで約7か月

担当者のふり返し: 「他人事と捉えていた」

1億2,400万円

損害の合計。最大の費目は、お客様へのお詫びの品(4,500万円)。システム復旧費(4,000万円)より多かった。

今月決める3つのこと 担当と期限を書いて、社長が確認してください

	やること	なぜ	担当・期限
1	VPN機器・リモート接続の棚卸し 機種名、保守契約が続いているか、最新版に更新済みかを一覧にする。使っていない接続は止める。	侵入の87.0%がここから。上の実例は保守を切ったことが原因だった。	
2	社外からのログインに二段階認証 VPN、リモートデスクトップ、メールの順に、パスワードだけで入れない状態にする。	盗まれたパスワードや推測しやすいパスワードで入られるのを防ぐ。	
3	戻せるバックアップ ネットから切り離れた複製を1つ持つ。年に1回以上、実際に戻す練習をする。	データを戻せた組織の大半はバックアップから。暗号を解いて戻せたのは1件だけ。	

☐ 3つとも担当を決めた ☐ 次の確認日: 月 日

確認印

出典 中小企業の割合: 警察庁「令和7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」p.14 / 感染経路: IPA「情報セキュリティ10大脅威2026 解説書[組織編]」p.34(警察庁統計を表にしたもの) / 被害額・身代金・復旧方法・実例: JNSA「インシデント損害額調査レポート 別紙『被害組織調査』第2版」(2025年7月) p.24-25、p.40-42

もっと詳しく やさしいサイバーセキュリティ「ランサムウェア被害13社を調査 | 平均6,019万円の請求書」「ランサムウェアのバックアップ対策 | 9割でも復元は2割」
／ 自社の点検には IPA「5分できる! 情報セキュリティ自社診断」(無料)