得意先から「セキュリティ対策は？」と聞かれたら、答えられますか。

中小企業を狙うサイバー攻撃が急増中。「うちは小さいから大丈夫」が、いちばん危険です。

対策できない会社が、取引先から外される時代が始まっています。



- ☐ VPN・リモート接続を使っている
- ☐ HPやネットショップがある
- ☐ 取引先からセキュリティ対策の質問を受けた

→ 1つでも当てはまれば、このチラシの対象です。

実際に起きています ― 身近な会社の被害事例

CASE 01

事例1〈医療〉 大阪急性期・総合医療センター（2022年）

復旧まで73日

賠償10億円



給食委託先のVPN機器から侵入され電子カルテが停止。損失20億円超。侵入経路となった取引先側の3社が解決金10億円を支払う和解に。

取引先が「加害者」になった事例です

CASE 02

事例2〈製造・通販〉 田中屋本店（新潟市・笹だんごの老舗和菓子メーカー／2025年）

カード情報677名分漏えいの可能性



従業員80名の会社。ネットショップを改ざんされ、個人情報5,610名分も漏えいの可能性。カードの不正利用も確認。

従業員80名の"地方の団子屋さん"でも狙われます

もし漏えい事故が起こったら

被害総額 約9,000万円

・調査・システム復旧　約2,500万〜2,800万円　・顧客対応・カード不正監視　約1,200万〜1,300万円　・再発防止・罰金・売上減少　約5,100万〜5,800万円

※事例2と同規模の企業を想定した試算（総被害額 約8,800万〜9,900万円）

セキュリティが"取引条件"になる時代へ

★★★★☆

★1〜★5の5段階評価

経済産業省「SCS評価制度」 **2026年度末 開始予定**

大手企業への攻撃も多くは取引先・委託先経由。今後、大手は取引先にもセキュリティ水準を求めてきます。

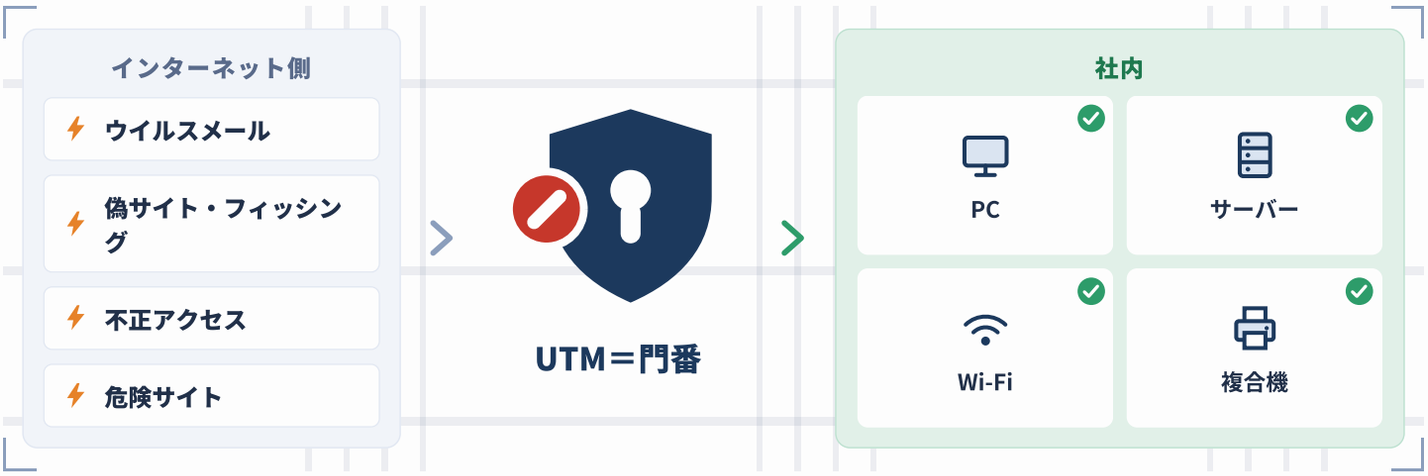
「今言われていなくても、必ず言われる」時代に。

取引先からセキュリティ対策を求められていませんか？答えられないままだと、取引先の選定から外されかねません。

対策は 月々15,000円（1日あたり約500円）から。

» 裏面をご覧ください

会社を守る"門番" — UTM（統合脅威管理）



オフィスの標準的な守り方

①入口対策＝UTM	②PC対策＝ウイルス対策ソフト・更新	③ルールと教育	④バックアップ・保険

UTMは全ての土台。SCS評価制度で求められる基本対策の多くをカバーします。

UTM1台でできること

- ウイルス侵入をブロック（検知データを自動更新）
- 迷惑メール・フィッシング詐欺メール対策
- 危険サイト・業務外サイトのブロック
- 外部からの不正アクセス防御
- テレワーク・拠点間の安全な接続（VPN）
- 脅威の「見える化」レポート

付帯サービス
- PCウイルス駆除サービス無料
- サイバー保険 標準付帯（最大100万円補償）
- 安心の日本製、国内サポート

導入イメージ

月々 **15,000円**（税別） ＝ 1日あたり 約 **500円**

約9,000万円のリスクに、100分の1以下の備え。

・5年リース／設置工事費込み／初期費用0円
・PCおよそ15台までの標準構成の目安
・リース料は与信により多少変動。台数・環境に応じて最適構成をお見積り。一括購入も可

無料 現状チェック実施中

5分の聞き取りシートにご記入いただくだけで、概算費用をその場でお出しできます。

このチラシをお持ちした担当者に、お気軽にお声がけください。