mini TALK
No.77　2025.11.4
The Gifu Shinkin Bank Newsletter

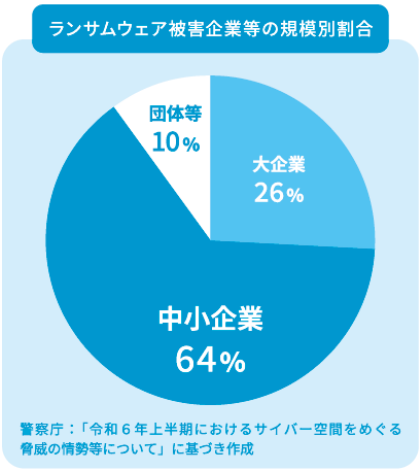
サイバー攻撃への備え、万全ですか？
～経営リスクへの対策～

1．サイバー攻撃の情勢

近年、企業や自治体、医療機関などを狙ったサイバー攻撃が全国的に多発しています。攻撃手口は年々巧妙化・多様化しており、ウイルス感染による情報流出だけでなく、業務システムを停止させて身代金を要求する「ランサムウェア攻撃」や、取引先になりすました「不正送金メール」など、実被害が相次いでいます。こうした攻撃はもはや大企業だけの問題ではなく、あらゆる組織にとって「いつ」「どこで」起きてもおかしくない身近な経営リスクになっています。

2．中小企業も攻撃の対象に

「うちは小規模だから狙われない」と思われる方も少なくありません。しかし、攻撃者は防御体制の脆弱な中小企業を“狙いやすい標的”として位置づけています。サイバー攻撃被害（ランサムウェアによる被害）の約６割が中小企業であり、大企業に限ったものではありません。サイバー攻撃により、被害が連鎖して取引先やその先々で企業の業務が停止する等、社内外を問わず攻撃対象が拡大していることも見逃せません。



3．被害にあった場合の影響

一度サイバー攻撃を受けると、その影響は想像以上に広がります。例えば、重要な取引データや顧客情報が暗号化されたり、流出した場合、業務停止に伴う売上減少に加え、復旧対応の専門業者費用、外部への謝罪・通知、法的対応、信用失墜による取引停止など、甚大な損害が発生します。特に中小企業では、システム部門の人員や予備費が限られているため、一度の攻撃で経営が大きく揺らぐことも珍しくありません。これは自然災害や供給網の分断と同様、事業継続（BCP）の観点からも深刻なリスクです。

岐阜信用金庫　広報サステナビリティ統括部　岐阜市神田町6丁目11番地　TEL058－266－2373

４．対策

（１）常にＯＳ、ソフトウェア、ネットワーク機器を最新の状態にする。

古いバージョンのＯＳやソフトウェアをアップデートせずに放置していると、ネットワークに侵入され、ランサムウェアなどの被害に遭うことがあります。パソコンやネットワーク機器は常に最新の状態にしておき、攻撃者が侵入できる弱点をふさいでおきましょう。

（２）クラウドサービスの共有設定や公開範囲を適切に設定する。

インターネット上にデータを保存できるクラウドサービスの共有設定を誤ったため、情報が漏洩するトラブルが増えています。初期設定を適切に変更したり、従業員の異動や退職に伴い権限を見直したりすることが重要です。

（３）パスワードは長く、複雑なものにする。

パスワードを推測されたり、ウェブサービスから窃取したＩＤ・パスワードが流用されることで、不正にログインされる被害が増えています。パスワードは「長く」「複雑に」「使いまわさない」ようにして強化しましょう。

（４）メールの添付ファイルやリンクを安易にクリックしないよう従業員教育をする。

取引先や関係者と偽ってウイルス付のメールを送ってきたり、正規のウェブサイトに似せた偽サイトを立ち上げてＩＤ・パスワードを盗もうとする巧妙な手口が増えています。メールに存在しない業務フロー構築など複数の手段の活用が検討されています。

（５）ＩＴ導入補助金を活用したセキュリティ対策支援を検討する。

中小企業・小規模事業者等の労働生産性の向上を目的として、デジタル化やＤＸ等に向けたＩＴツール（ソフトウェア、サービス等）の導入を支援する補助金が活用されています。

（６）備えとしてのサイバー保険へ加入する。

サイバー攻撃による損害賠償やシステム復旧費用、外部対応費用、さらには専門家による初動支援など、幅広い補償を受けることが可能です。万が一の被害時に、経営へのダメージを最小限に抑えるための“経営防衛策”として導入する企業が増えています。

ぜひご相談ください

サイバー攻撃は「もしも」ではなく「いつ起きてもおかしくない」時代です。経営者も従業員も、詳しい担当者だけに任せるのではなく、社内の全員が知識を身に着け、対策を取らなければなりません。自社の防御体制だけでなく、万が一の損害への備えとして、自社のセキュリティ状況の確認やサイバー保険の活用を検討してみてはいかがでしょうか。

詳しくは、お取引店舗までお気軽にご相談ください。

出典：IPA 情報処理推進機構 https://www.ipa.go.jp/security/sme/list.html
サイバーセキュリティ月間 2025 特設サイト

岐阜信用金庫　広報サステナビリティ統括部　岐阜市神田町6丁目11番地　TEL058－266－2373