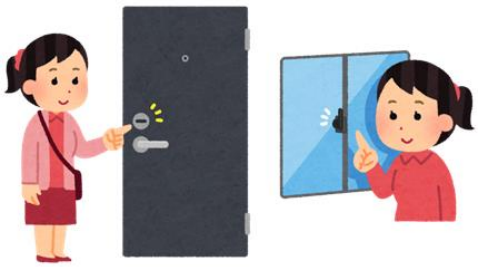
中小企業 と サイバーセキュリティ

第7回「職場の”戸締り”してますか？」

ランサムウェア被害が続く中、狙われているのは大企業だけではありません。攻撃者は、対策が手薄になりがちな中小企業も標的にしています。

では、何から始めればよいのでしょうか。



サイバー防犯でも「戸締り」が基本です

最初の一歩は、家の防犯と同じく「戸締り」です。

鍵が壊れていたり、窓が開いていたり、暗証番号が初期のままでは泥棒が入ってくるのは当然で、サイバー空間でも同じことが言えます。

まず重要なのが、従業員への教育＝「鍵の管理・戸締りの徹底」です。フィッシングメールにだまされて鍵を盗られてしまうことが最大のリスクであり、攻撃者は人の不注意を狙います。

これまで紹介した「そのメール開く前に確かメル」や「ログインさせるメール、SMSは全部偽物」といった意識づけは、効果的な防犯対策になります。

次に、OS・アプリ、VPN機器の更新＝「壊れた鍵の修理」です。古いままの機器は鍵が壊れている状態と同じで、攻撃者に簡単にこじ開けられます。更新は「面倒な作業」ではなく、鍵の修理だと考えてください。

さらに、初期設定のまま放置＝「ダイヤルロックの暗証番号が初期設定（例：0000）」です。工場出荷時のパスワードや設定は、誰でも開けられる鍵と同じです。初期パスワードの変更や不要な共有設定、公開設定の無効化などの誰でも開けられる鍵を閉めることは基本中の基本です。

アップデートは鍵の修理と考えましょう

また、不要なサービスやポートを閉じる＝「使っていない勝手口や窓を閉める」ことも重要です。使っていないリモート接続や古い通信方式が開いたままでは、そこから侵入されてしまいますので、確認の上、止めておきましょう。

サイバー空間でも防犯性能の高い鍵を使いましょう

最後に、パスワード認証の強化＝「ディンプルキーや二重ロック」です。多要素認証やパスワードレス認証に変えることで、攻撃者が突破する難易度を引き上げることができます。

サイバー対策は難しく感じられがちですが、物理的な防犯と同じ発想で、できるところから取り組んでいきましょう。

神奈川県警察サイバーセキュリティ対策本部

※ この記事は川崎市産業振興財団機関紙「産業情報かわさき（2026年5月号）」に掲載されたコラムを再編集したものです。