愛知県警察
サイバー犯罪対策課

サイバー犯罪対策通信

第R6-11号
組織向け

VPN機器・リモートデスクトップ管理はできてますか？

ランサムウェア対策

VPN機器とリモートデスクトップ

VPNとは、インターネット回線を、あたかも専用線であるかのように利用するサービスのことで、テレワーク等で導入する企業等が増加しています。

リモートデスクトップとは、コンピューター同士をネットワークで接続することで、遠隔操作を可能にするもので、保守管理に使われることが多いWindowsの標準機能です。

こんな会社は危険です！

VPN機器やリモートデスクトップを利用している会社で、次のような場合は非常に危険です。

① VPN機器を使っているが、**ファームウェアのアップデートをしたことがない**
② VPN機器は、委託業者が**たぶんアップデートしてくれていると思う（確認していない）**
③ テレワークでリモートデスクトップを導入したが、今は**使っておらず放置している**
④ **特定しやすいユーザ名**や**単純なパスワード**を使っている
（社員番号や部署名など、類推しやすいものはNG！）

今すぐ確認、見直しをしましょう！

○ VPN機器

① VPN機器のファームウェアを定期的にアップデートする
② 管理を委託している場合は、委託業者がどこまでメンテナンスをしてくれるのか、改めて確認する
③ VPNの認証を強化する
・ユーザ名やパスワードは、特定されにくい複雑なものにする
・多要素認証やワンタイムパスワードなどの導入も検討する

○ リモートデスクトップ

① 使っていなければリモートデスクトップを無効にする
② リモートデスクトップの認証を強化する
・IDやパスワードは、特定されにくい複雑なものにする
・多要素認証やワンタイムパスワードなどの導入も検討する
③ 接続できるIPアドレスを制限する
④ ログイン試行回数を制限する