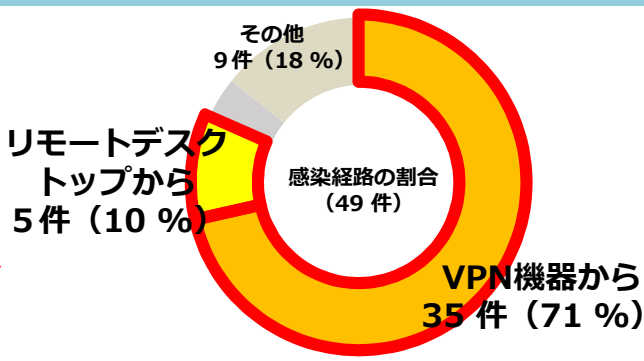
CyberNews

令和5年11月
宮城県警察本部
サイバー犯罪対策課

テレワーク用の機器が狙われています

ランサムウェアの感染経路は
- ＶＰＮ機器からの侵入が71%
- リモートデスクトップからの侵入が10%

を占め、テレワーク等に利用される機器のぜい弱性や強度の弱い認証情報等を利用して侵入したと考えられるものが大半を占めています。



「令和5年上半期におけるサイバー空間をめぐる脅威の情勢等について」（令和5年9月21日警察庁）から抜粋

実施すべき基本対策

① VPN機器やソフトウェアはアップデートを！

ＶＰＮ機器やリモートデスクトップアプリケーション、テレワーク端末のＯＳ等は、最新のアップデートやパッチの適用を実施しましょう。

② 強力なパスワードの設定！

ＶＰＮ機器やアプリケーション、ＯＳ等には、強力なパスワードを設定しましょう。

③ 多要素認証の採用！

システムやサービスへの本人認証には、多要素認証方式を採用しましょう。

④ セキュリティ対策ソフトの利用！

テレワーク端末にセキュリティ対策ソフトをインストールし、定義ファイルの自動更新やリアルタイムスキャンを実施しましょう。

⑤ オンライン会議時のURLは秘密！

オンライン会議にアクセスするためのＵＲＬは正規の参加者以外には非公開にしましょう。

また、会議開催時に参加予定者以外の人が参加していないかも確認しましょう。

その他の対策については総務省のテレワークセキュリティガイドライン等も参考に！
https://www.soumu.go.jp/main_sosiki/cybersecurity/telework/

宮城県警察　警察庁 National Police Agency