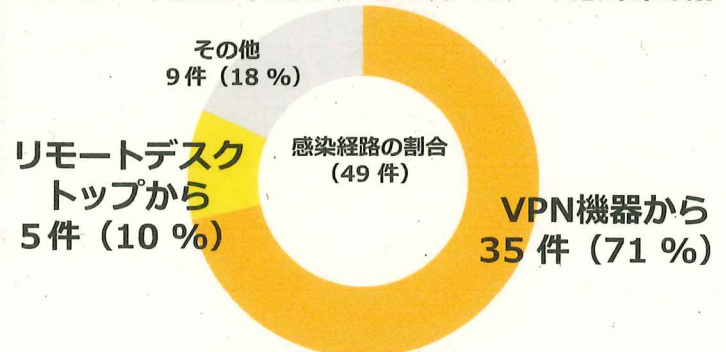


山形県警からのお知らせ

～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、セキュリティが甘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年度上半期ランサムウェアの感染経路〉



「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はこれ！

- VPN機器やソフトウェアはアップデートしよう！**
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適用を実施
- 強力なパスワードを設定しよう！**
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
- 多要素認証を採用しよう！**
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
- セキュリティ対策ソフトを利用しよう！**
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
- オンライン会議時のURLは秘密にしよう！**
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
会議開催時に参加予定者以外の人に参加していないか確認

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/



電話をするならこちら↓

最寄りの警察署又は警察相談専用窓口 ☎ #9110 (全国共通)



山形県警察



警察庁
National Police Agency