

サイバーだより



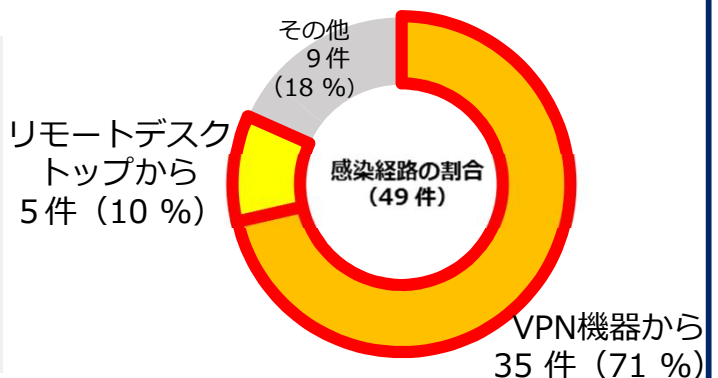
令和5年11月2日第25号

長野県警察本部
サイバー犯罪捜査課
026-233-0110

ノーセキュリティ、ノーテレワーク！

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年上半年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！

1 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

2 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

3 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

4 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

5 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/

