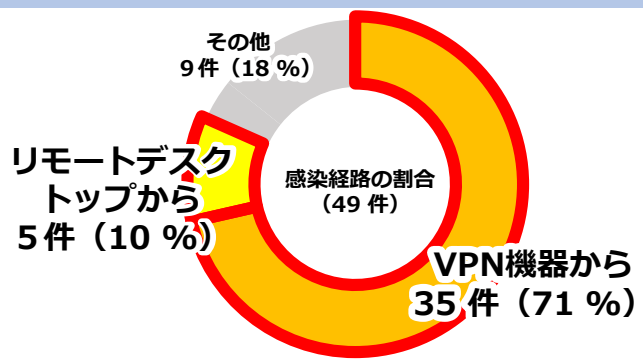
# サイバー警察局便り

Cyber Police Agency Letter R5 Vol.19

# 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！

### 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が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/**

総務省
Ministry of Internal Affairs and Communications

警察庁
National Police Agency