CyberCrime Control Project

令和５年11月

広島県警察本部
サイバー犯罪対策課
☎082-228-0110

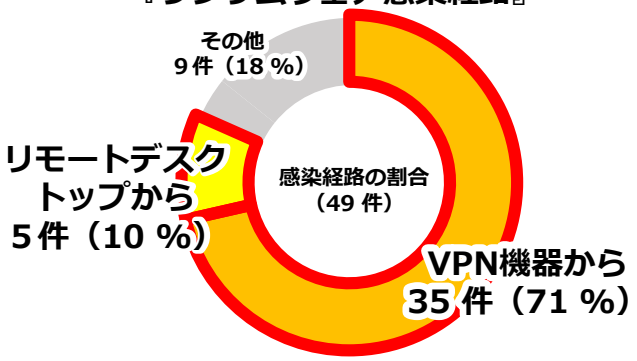
ノーセキュリティ、ノーテレワーク

【セキュリティ対策をしていないテレワークは危険!!】

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%を占めています。
- ☑ テレワーク等に使用される機器の脆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。

『ランサムウェア感染経路』



「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！！

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
（大小英字、数字、記号を混在させた10文字以上のパスワードが推奨）

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/

ランサムウェアなどによるサイバー犯罪被害の相談・通報は・・・

- ▶ サイバー１１０番　☎０８２－２１２－３１１０（平日午前８時３０分から午後５時までの間）
- ▶ 広島県警察本部サイバー犯罪対策課（代表☎０８２－２２８－０１１０）
- ▶ 最寄りの警察署

☑ 過去のセキュリティ情報は県警ホームページで　https://www.pref.hiroshima.lg.jp/site/cyber-security.html ▶▶▶