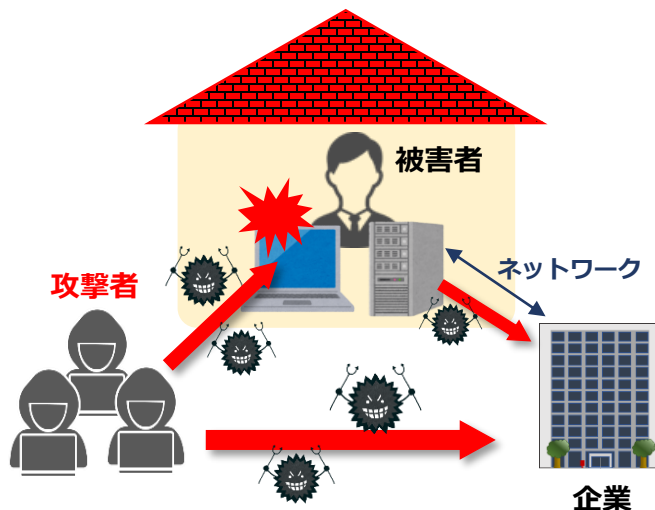
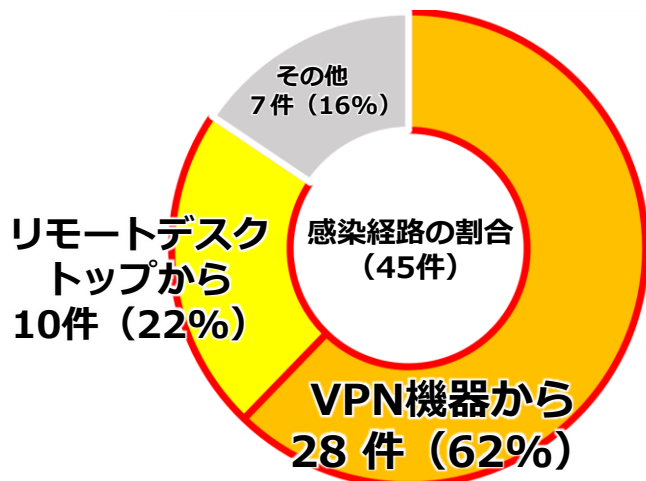




## テレワーク環境のセキュリティは万全ですか？

ランサムウェアの感染経路はVPN機器やリモートデスクトップなど、**テレワークに利用される機器の脆弱性を利用して侵入**したと考えられるものが多い。



出典：警察庁「令和7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」

## 自身の脆弱性をチェックしましょう！

- ☒ 不審なメールのリンクなどを開かない
- ☒ アカウント・パスワードを適切に管理する
  - パスワードは長く複雑にし、多要素認証も活用する
  - ✗ 使いまわしや簡易な文字列、推測しやすいもの
  - ✗ 初期アカウントや使わないアカウントが残っている
- ☒ セキュリティアップデートが出たら更新
- ☒ セキュリティインシデント発生時の速やかな報告



PASSWORD...



## みなさんに役立つ情報はこちらから



政府広報オンライン「ランサムウェア、あなたの会社も標的に?被害を防ぐためにやるべきこと」  
<https://www.gov-online.go.jp/useful/article/202210/2.html>



政府広報

総務省のテレワークセキュリティガイドライン

[https://www.soumu.go.jp/main\\_sosiki/cybersecurity/telework/](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9時から午後0時、午後1時から午後4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> ▶▶▶