



## ～ V P N 装置 が 狙 わ れ る ～

一般従業員向け

VPN  
って何？



社内だけで使う通信の他に、リモートワーク等実現のため、社内と社外(家等)を繋ぐ安全な通信が必要⇒これがVPN！

簡単に言うと...

公共交通機関

他人と共有して使うのでコストが割安。ただ、すり等の被害も...？



共有回線を通常通り使う

自家用車

道路自体は共有だが車内という一定空間においてプライバシーやセキュリティは確保



VPN

これ！

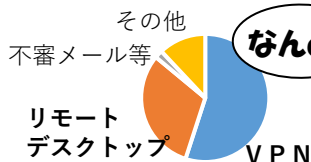
秘密の私道

非常に安全で快適だが多額のコストが必要



物理的な専用回線

...とはいえ外を走るの、犯人のターゲットになることも...



なんと！

ランサムウェアの感染経路

55%がVPN経由！

（リモートデスクトップ経由も含めると実に全体の86%に！）

※令和6年におけるサイバー空間をめぐる驚異の情勢等について（警察庁）

危機感を持った対策を！

従業員のセキュリティ意識を高める

すごく重要！

十分な知識がないまま導入すると、マルウェア感染や乗っ取りなどリスク大！  
リモートアクセス時等のルールを利用する従業員全員が正しく認識し、決められたルールは必ず遵守しましょう！

VPN使用時はフリーWi-Fiを避ける

便利だからと、気軽に使っていませんか？フリーWi-Fiはセキュリティリスクが高く、攻撃者に不正アクセスされる可能性が！

認証情報の管理と定期的な更新

重要！

IDやパスワード、使い回していませんか？  
別のところから流出した認証情報が流用されるかも...

私用端末での通信は禁止 ...など

個人の端末は企業のセキュリティポリシーや管理体制が整っていないことが多く、ウイルス感染やデータ漏えい、外部からの脆弱性が高くなります



サイバーセンター公式「X」(旧Twitter)

兵庫県警察サイバーセンターではX（旧Twitter）で、サイバー犯罪やサイバーセキュリティの情報をいち早くお届けしています。

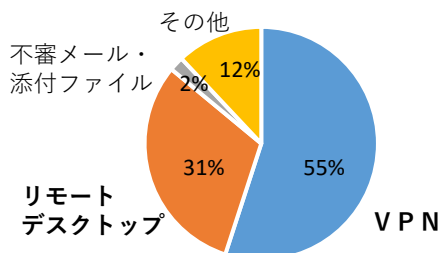
[https://x.com/HPP\\_c3division](https://x.com/HPP_c3division)





## ～ V P N 装置 が 狙 わ れ る ～

担当者向け



ランサムウェアの感染経路、  
なんと**55%**が**VPN**経由です！！

（リモートデスクトップ経由も  
含めると実に全体の**86%**に！）

※令和6年におけるサイバー空間をめぐる驚異の情勢等について（警察庁）

### 危機感を持った対策を！

#### 従業員の**セキュリティ意識**を高める

・VPNの利用ルールを明確に定め、従業員に重要性を認識させましょう。また、従業員がセキュリティ意識を保ち続けるために、定期的に最新のセキュリティに関する知識のアップデートを！

利用ルール（私用端末での通信は禁止  
多要素認証を導入する …等

#### VPN装置を定期的に**アップデート**する **重要！**

VPN装置も他のネットワーク機器と同様に、時間が経過するにつれ脆弱性が発見されることがあります。常に最新の状態に保ちましょう。

- 事例
- ①よく使う装置だけ最新版になっていたが、現在**ほとんど利用していない装置は更新がされずに放置されており、セキュリティホールとなっていた**
  - ②24時間稼働しており、**アップデート処理をするタイミングがなく放置していた**

#### 通信端末の**セキュリティ対策**をする

企業の管理下にあるモバイル端末を一元管理してセキュリティポリシーを強制するなど、様々な対策があります。自社にあったものを検討し対策してください。

#### 利用権限を定期的に**点検**する **重要！**

中途退職者の権限がそのまま放置されておりいつまでも利用できるようになっていた、などの事例が散見されます。定期的に点検しましょう。



#### ランサムウェア等の被害にあった際は**警察に通報！** **重要！**

併せて、セキュリティベンダー等にも早急に報告し、被害の最小化に努めてください。

#### サイバーセンター公式「X」(旧Twitter)

兵庫県警察サイバーセンターではX（旧Twitter）で、サイバー犯罪やサイバーセキュリティの情報をいち早くお届けしています。

[https://x.com/HPP\\_c3division](https://x.com/HPP_c3division)

