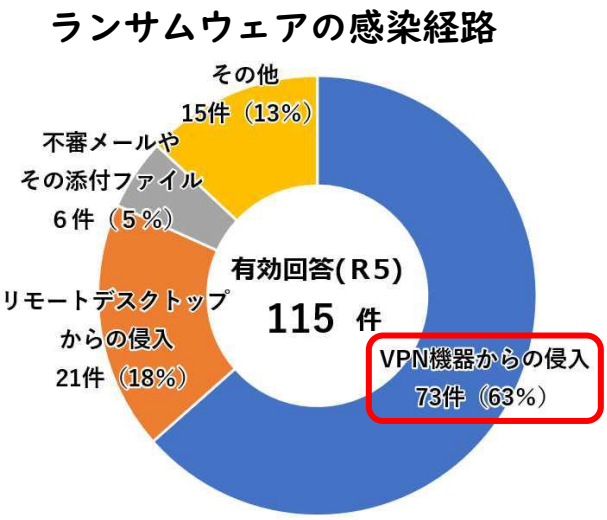
S.P.P Cyber Bureau
Cybercrime
Countermeasures Division

埼玉県警察 サイバーセキュリティレポート

R6.3月

ランサムウェア感染経路の約６割がVPN機器!!

令和５年のランサムウェアの被害企業（※）の63%は「VPN機器からの侵入」が感染経路でした。
テレワークなどの運用をしていなくても、**保守事業者によるメンテナンスのために VPN機器を設置している場合**もあります。
閉鎖されたネットワークであってもVPN機器の有無を確認して下さい。



※ 令和６年３月14日警察庁「令和５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」参照

「アップデートしたから大丈夫!!」は間違い！

VPN機器の脆弱性情報が公開された際に、アップデートだけで対応を終了していませんか？アップデートを行うまでにサイバー攻撃を受けていた場合、既に盗まれたアカウント情報を悪用され、被害に遭う可能性があります。
VPN機器を常に最新の状態にすることに加え、以下の対策もお願いします！

ＶＰＮ機器対策

〇初期アカウントの設定を「admin」等の初期設定から必ず変更する！
〇試験的に使用した「test」や「demo」などのアカウントは必ず削除！
〇パスワードは推察されにくいもの（長く、複雑にする）に設定する
〇脆弱性対応（アップデート）後は、必ずパスワードを変更する！

これらの対策は、被害事例から教訓となっている対策です！
もし自組織で確認できない場合は、保守・管理事業者に確認してください。