サイバーセキュリティの置き薬

2023年 第1号

ランサムウェア被害防止対策の徹底を！

～まずはネットワーク機器本体ソフトウェアを更新～

ランサムウェアとは、感染すると端末等に保存されているデータを暗号化して使用できない状態にした上、そのデータを復号する対価として金銭を要求する不正プログラムです。

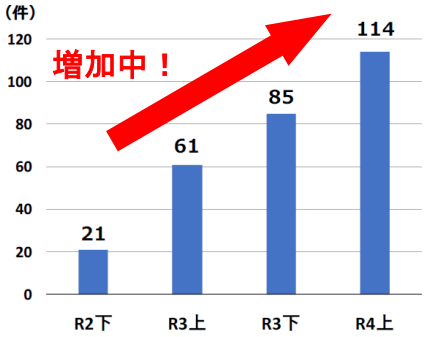
令和４年上半期の国内におけるランサムウェア被害件数は114件で、右肩上がりで増加しており、その被害は企業・団体等の規模、業種等を問わず、広範囲に及んでいます。

最近特に多いのは、**VPN機器等ネットワーク機器の脆弱性（セキュリティホール）を突いて侵入する**手口です。

脆弱性を抱えたまま運用していると、**被害リスクが極めて高くなる**ため、**VPN機器等ネットワーク機器本体のソフトウェアを点検**し、**速やかに最新の状態に更新（バージョンアップ）**しましょう。

富山県警察では、ランサムウェアに関する注意喚起動画をYoutubeで公開していますので、セキュリティ教育等にご活用ください。

【被害報告件数の推移】



※企業・団体等におけるランサムウェア被害として都道府県警察から警察庁に報告のあったもの。

https://youtu.be/watch?v=mUPLF970JIE
（通信費はご利用者の負担となります）

被害に遭わないための対策

○　脆弱性対策

感染経路としては、VPN機器やリモートデスクトップからの侵入が大半を占めています。
機器本体ソフトウェアの最新化、パッチ等を適用し、脆弱性を残さないようにしましょう。

○　認証情報の適切な管理

VPN機器等やリモートデスクトップの認証パスワードは、英数字記号を組み合わせた推測されにくいものを設定し、２要素認証等による強固な認証手段を導入しましょう。

○　なりすまし電子メール等への警戒

知人や取引先等からと思われる電子メールであっても、詐称されている可能性を念頭に、不用意に添付ファイルを開いたり、リンク先にアクセスしないようにしましょう。

○　ウイルス対策ソフトの導入等によるマルウェア対策

マルウェアやハッキングツール等を利用した侵入のリスクを抑えるため、ウイルス対策ソフトを導入し、定義ファイルを最新の状態に保ちましょう。

○　データのバックアップの取得

不測の事態に備え、バックアップはこまめに取得し、ネットワークから切り離して保管しましょう。

ランサムウェア被害を受けた場合は、警察への通報をお願いします！

【参考】
警察庁：ランサムウェア被害防止対策
https://www.npa.go.jp/cyber/ransom/index.html
警察庁：令和４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
https://www.npa.go.jp/publications/statistics/cybersecurity/data/R04_kami_cyber_jousei.pdf