サイバーセキュリティの置き薬

2022年
第11号

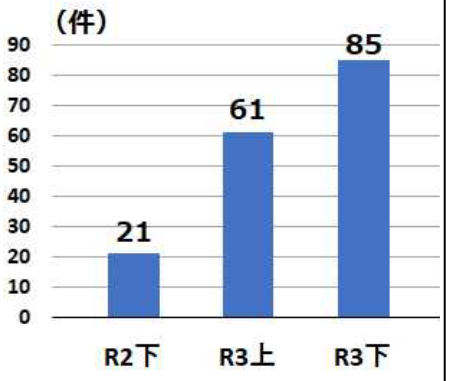
ランサムウェアによる被害が増加しています！

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で、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２年頃からは、特定の個人や企業・団体等を標的とした手口に変化しており、企業のネットワーク等のインフラを狙うようになっています。

令和３年中に警察庁に報告された国内のランサムウェアによる被害件数は、前年以降右肩上がりで増加しており、その被害は、企業・団体等の規模やその業種等を問わず、広範に及んでいます。

【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。

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。
更新ファイル、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、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。

○　電子メール等への警戒

知人や取引先等を詐称してメールを送信し、添付ファイルを開かせる、又はリンク先サイトにアクセスさせるよう仕向ける手口が確認されています。

送信元が正規のものでない可能性を念頭に、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。

被害を軽減するために

- **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。**
- **ユーザアカウントに割り当てる権限やアクセス可能な範囲を必要最小限にしましょう。**
- **感染した端末では、外部のサーバとの間で不審な通信が発生する場合があります。ネットワーク内の不審な挙動を早期に発見することで、感染拡大や外部からの侵入範囲の拡大を阻止することに繋がります。**

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３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
https://www.npa.go.jp/publications/statistics/cybersecurity/data/R03_cyber_jousei.pdf