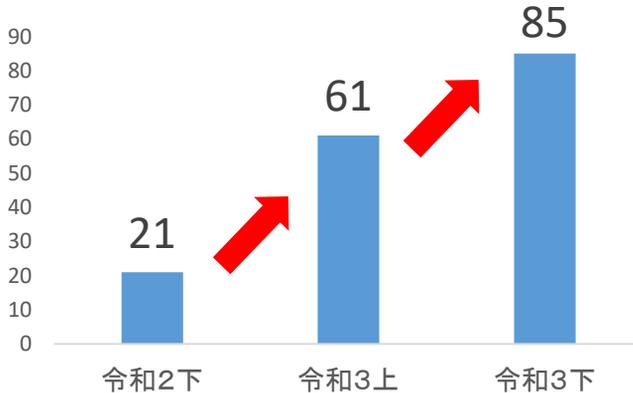




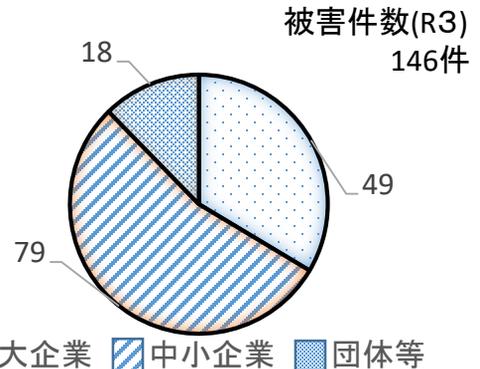
ランサムウェアとみられる被害が発生!!

企業や団体のネットワークに侵入し、データを暗号化する『ランサムウェア』が急増しています。

企業・団体等における被害の報告件数



被害企業・団体等の規模別報告件数



引用:「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」(警察庁)

先日来の報道のとおり、ランサムウェアを始めサイバー攻撃等の被害を受けると、その企業・団体にとどまらず社会全体に影響を及ぼす可能性があります。

昨今の情勢を踏まえると、サイバー攻撃の脅威は非常に高まっており、業種や企業・団体の規模を問わず、注意が必要です。



ランサムウェアとは

パソコンなどの端末やサーバ上のデータを暗号化し、正常にアクセスできないようにして、元に戻すための対価として金銭を要求する不正プログラムです。

さらにデータを盗んだ上で、

「対価を支払わなければデータを公開する」などと金銭を要求する『ダブル・エクストーション』(二重恐喝)という手口も発生しています。



ランサムウェアの

被害に遭わないために

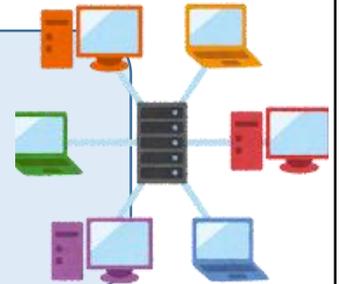
- ・電子メール等に注意する
- ・OS等の脆弱性を放置しない
- ・ウイルス対策ソフトを導入する



OS、ソフトウェア、VPN機器など利用している機器の更新ファイル、パッチ等を適用し、脆弱性を残さないようにしましょう。

被害を軽減させるために

- ・データのバックアップを取っておく
- ・ネットワークを監視する
- ・アクセス権等の権限を最小化しておく



データのバックアップを取っておけば、もし暗号化された時も早期に復旧できます。ただし、バックアップデータがネットワークに接続されていれば、バックアップデータまで暗号化されてしまう危険性があるので、可能な限り切り離して保管するか、複数のバックアップを残すようにしてください。

被害が発生してしまったら

- ・感染を拡げないためにネットワークを遮断する
- ・インシデント発生時の連絡体制に速やかに連絡する
- ・金銭の要求には応じないことを推奨します



お金を払ったとしてもデータが復旧できる保証はありません。お金を払うことでさらに犯罪を助長させるおそれもあります。

基本的な対策をすること
そして「うちの会社は大丈夫」、「自分に関係ない」という
気持ちをなくし、インターネットを使う方は全て、身近に
危険は迫っているという意識をお持ちください。



情報流出等の被害が発生していない場合でも、サイバー攻撃等に関連する不審な動きを検知した場合は早期に対処するため警察本部又は警察署にご連絡ください。