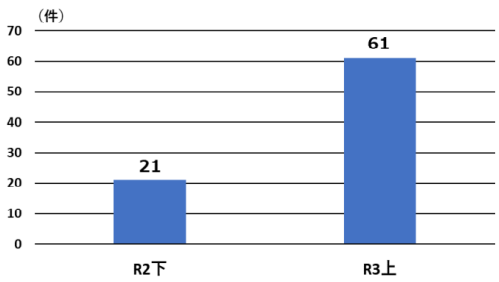
回　覧　印　印　印　印　印　印　印　印　印　印　印　印

ASAMA Security Newsletter Vol.76

あさまセキュリティニュースレター

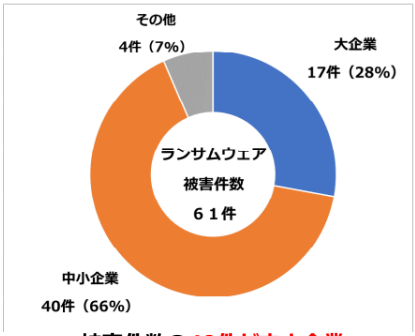
ランサムウェア被害増！中小企業、二重恐喝、テレワーク・・・（2021年9月10日）

【図表１：企業・団体等におけるランサムウェア被害の報告件数の推移】



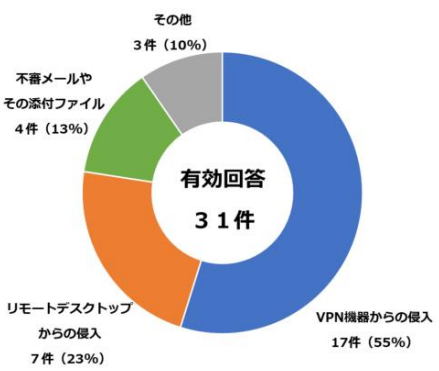
企業・団体等におけるランサムウェア被害として、令和３年上半期に 都道府県警察から**警察庁に報告のあった件数は61件**

【図表４：ランサムウェア被害の被害企業・団体等の規模別報告件数】



被害件数の40件が中小企業規模を問わず発生

【図表７：感染経路】



テレワーク等の普及を利用して侵入したと考えられるものが全体 の８割近く

データの暗号化のみならず、データを窃取した上、企業等に対し「対価を支払わなければ当該データを公開する」などと 金銭を要求する二重恐喝という手口が確認 警察として金銭の要求手口が確認できた35件の内、二重恐喝は27件

復旧等に要した期間・費用の記載もあり↓

出典:「令和３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」(警察庁)
・(https://www.npa.go.jp/publications/statistics/cybersecurity/data/R03_kami_cyber_jousei.pdf)

事業継続に関わるため、被害にあっても報告されないケースもあり
常にリスクがあることを前提に、セキュリティに対する意識を全員が持つ、バックアップはどうしているか確認しましょう。

攻撃のパターン

- 様々な攻撃手法により、企業・組織のネットワークに侵入（VPNソフト・機器の脆弱性も悪用される）
- 侵入後、社内データが入っているサーバや共有データを暗号化
- 社内の端末やサーバを一斉に暗号化させる攻撃も（復旧を阻害するため、バックアップ等も同時に）
- 一般的に、攻撃の進行を検知しにくく、暗号化された時点で被害に気付く
- データ暗号化を戻すための金銭要求 ＋ 盗んだデータを公開されたくなければと、金銭要求（二重の脅迫）

さらにDDoS攻撃（不正な通信でシステムやネットワークをダウンさせる）、顧客や取引先への嫌がらせを行うという四重の脅迫まで

対策

- 利用中のソフト・ネットワーク機器・ファームウェアのバージョンアップや見直しはできているか？
- 外部からのアクセスを利用している場合は、設定が適切か？
- ウイルス対策ソフト未導入の端末で、社内データにアクセスしているものはないか？
- バックアップは取れているか、何世代か前に戻せる仕組みがあるか？
- 社員全員でセキュリティに対する意識を高める、情報共有しているか？

ウイルス対策、不正アクセス対策、脆弱性対策など、基本的な対策を確実かつ多層的に適用することが重要！！

情報源

・警視庁サイバー犯罪対策プロジェクト　https://www.npa.go.jp/cyber/index.html
・IPA　ランサムウェア対策特設ページ　https://www.ipa.go.jp/security/anshin/ransom_tokusetsu.html

浅間商事株式会社　〒110-0005　東京都台東区上野7-15-70 浅間第一ビル　0120-830-414