サイバーセキュリティ通信 Vol.17

令和５年２月

サイバーキャッチくん

長崎県内の事業所がランサムウェア被害！
～VPN・リモートデスクトップの弱点が狙われる！～

今年1月、県内の事業所が使用している**複数の業務用サーバがランサムウェアに感染したことが分かりました。**

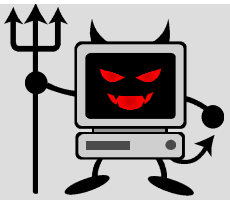
現在、ランサムウェア感染により、この事業者の事業用データは暗号化されているため、この事業者だけでなく、関係がある団体の業務にも影響を及ぼしています。

全国・本県の被害事例をみますと、**ランサムウェアによる攻撃者はVPN・リモートデスクトップの弱点（ぜい弱性）を狙っています。**

◎VPN・リモートデスクトップのセキュリティ状況を点検してください

ランサムウェアとは？

感染したパソコンをロックしたり、ファイルを暗号化することによって使用不能にした後、元に戻すことと引換えに「身代金」を要求する不正プログラム



① VPNの確認　～接続機器のバージョンを最新にする！

VPN接続を自前で行われている場合は、VPN機器が最新の状態に更新されているか確認し、業者に保守管理を委託している場合には、最新の状態となっているか確認するよう依頼してください。

② リモートデスクトップの確認　～不正アクセス対策の徹底！

- システムにアクセスできる職員を限定する
- ユーザーごとにアクセスできる範囲を設定する
- ログインの試行回数を設定する
- 多要素認証（パスワード＋指紋認証など）を導入する

③ バックアップの適切な保管　～3・2・1ルールで被害を最小限に！

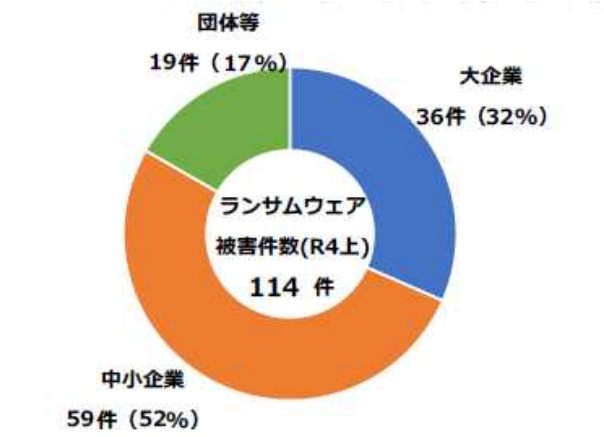
ルール3：データを3つ持つ（元データのコピーを2つ作成する）
ルール2：2種類の異なるメディアでバックアップをとる
（クラウドストレージとHDDなど）
ルール1：バックアップの1つはオフラインで保管する

裏面につづく

【参考資料】全国のランサムウェア被害状況（令和４年上半期）

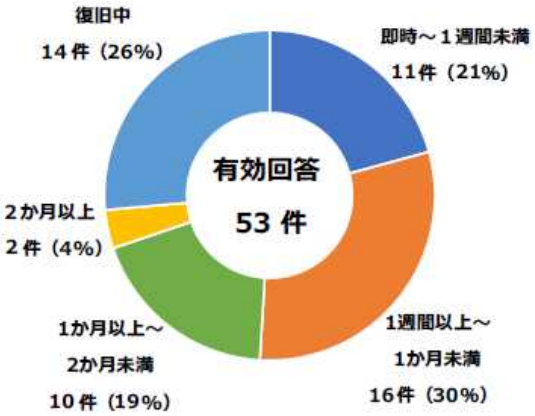
令和4年上半期（1月～6月）に都道府県警察から警察庁に報告があった企業・団体のランサムウェア被害（114件）について、警察庁がとりまとめた資料の一部を紹介します。詳しくご覧になりたい方はインターネットで【警察庁　サイバー空間をめぐる脅威の情勢等】と検索してください。

１　被害企業・団体の規模



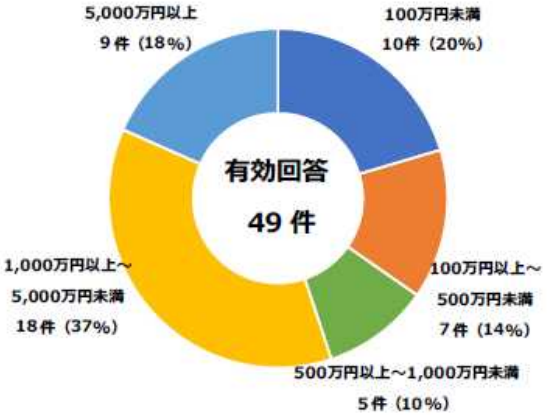
被害は、企業・団体の規模を問わず発生しています。

２　復旧に要した期間



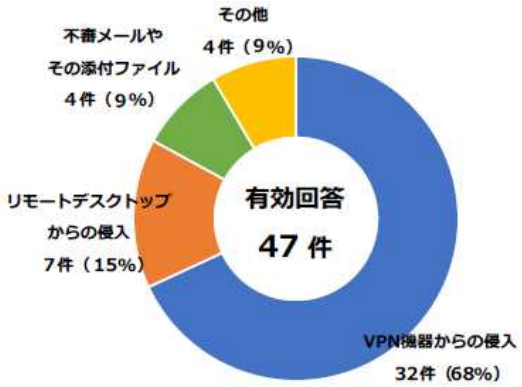
復旧までに1か月以上を要したものが12件ありました。

３　調査・復旧費用の総額



復旧費用総額が1,000万円以上要したものが55%を占めています。

４　感染経路



注　図中の割合は小数第１位以下四捨五入しているため、総計が必ずしも100にならない。

VPN機器からの侵入が68%、リモートデスクトップからの侵入が15%を占めています。

上記のとおり、被害に遭った場合には復旧までに長期間を要するだけでなく、事業活動ができないことによる損失とは別に復旧だけに多額の費用が必要です。「**安定的な事業活動には被害防止対策が必要**」となっています。

サイバー犯罪被害に関する届出・相談などは最寄りの警察署又は警察本部サイバー犯罪対策課へ連絡ください。

長崎県警察本部生活安全部サイバー犯罪対策課　095-820-0110（3451・3452）