依然猛威を振るうランサムウェア

ランサムウェアとは？

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。

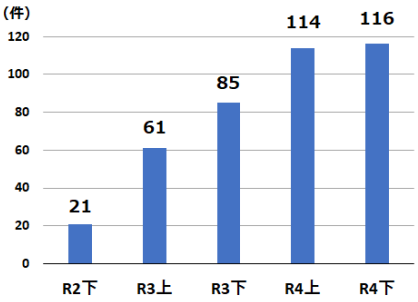
最近では、データの暗号化のみならず、データを窃取した上、企業等に対し「対価を支払わなければデータを公開する」などと金銭を要求する二重恐喝（ダブルエクストーション）という手口が多くを占めています。

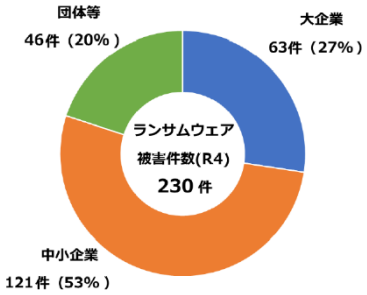
従前は「電子メール送信型」が主流でしたが、現在では、VPN機器をはじめとする企業のネットワーク等のインフラの脆弱性を狙って侵入するなど、特定の個人や企業・団体等を標的とした手口に変化しています。

○　企業・団体等におけるランサムウェア被害

被害件数

令和４年に都道府県警察から警察庁に報告のあった件数は230件（令和４年上半期114件、下半期116件）であり、令和２年下半期（21件）以降、右肩上がりで増加しています。





規模

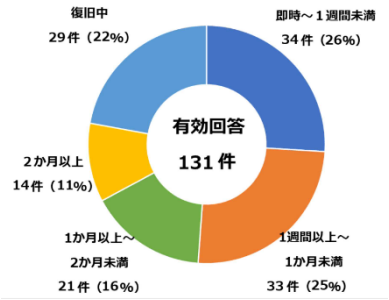
被害件数（230件）の内訳を被害企業・団体等の規模別にみると、大企業は63件、中小企業は121件であり、企業・団体の規模を問わず被害が発生しています。

復旧等に要した期間・費用

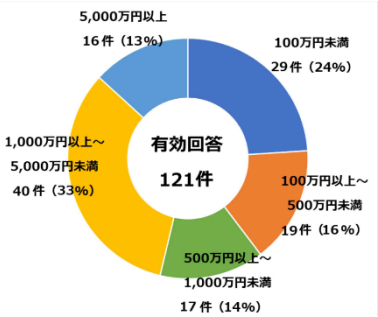
復旧に要した期間については、１週間以内に復旧したものが34件と最も多かったですが、２か月以上要したものもありました。

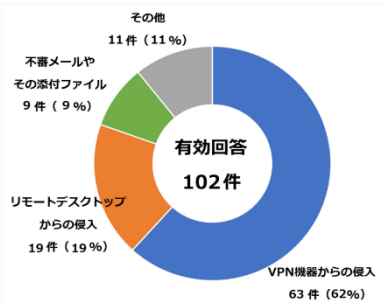
調査・復旧費用の総額については、1,000万円以上の費用を要したものが40件で最も多く、全体の33%を占めています。

［期間］



［費用］



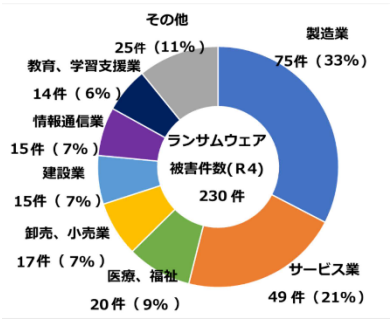


感染経路

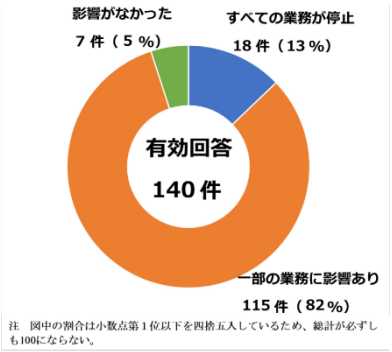
感染経路については、VPN機器からの侵入が63件で62%、リモートデスクトップからの侵入が19件で19%であり、この二つの侵入経路だけで約８割を占めており、機器等のぜい弱性や強度の弱い認証情報等を利用して侵入する手法がさらに拡大していることが分かります。

【参考】

［ランサムウェア被害の被害企業・団体等の業種別報告件数］

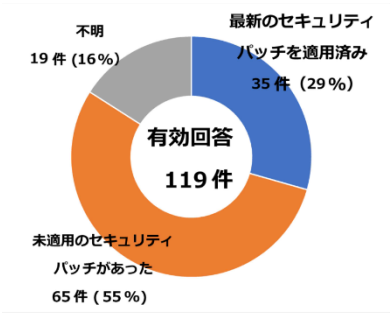


［ランサムウェア被害が業務に与えた影響］

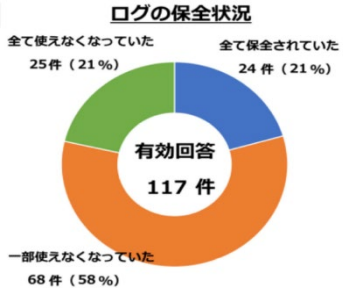


注　図中の割合は小数点第1位以下を四捨五入しているため、総計が必ずしも100にならない。

［侵入経路とされる機器のセキュリティパッチの適用状況］



［ランサムウェア被害における被害企業・団体等のログの保全状況］



セキュリティ対策の盲点

令和４年のランサムウェア情勢は、沈静化どころかこれまでにない勢いで猛威を振るいました。

上記のグラフを見ると、ネットワーク機器には最新のセキュリティパッチを適用することが重要なところ、回答を得た企業の実に半数以上で未適用パッチがあったことが分かります。

せっかくセキュリティ機器や最新の設備を導入しても、セキュリティパッチを適用しなかったり、設備のアクセスに係るパスワードを初期設定のままにしておくと、**本来守れるはずのデータを守れなかったり、攻撃者にとって格好の侵入経路と化したり**してしまいます。

ランサムウェアに限らず、セキュリティ対策では「**相手に隙を与えない**」ことが重要です。

☆　***パスワードは初期設定から必ず変更する***

☆　***セキュリティパッチを確実に適用する***

☆　***外部メールの添付ファイルを無警戒に開かない***

等、専門的技術を要しない誰でもできる「基本」こそがセキュリティ対策に最も有効なのです。

セキュリティ機器等を導入したり、バックアップを取っただけで安心することなく、導入後の保守点検を確実に行うことで、大切なデータを守り抜きましょう。

ランサムウェアの被害に遭わないための有効な対策

○　**バックアップの取得**

バックアップはネットワークから外れた環境に保管しましょう。

○　**インシデント発生時の手順の事前確認**

バックアップからの復旧が可能であることを確認しておきましょう。

※　R4では実際に復元を試みた企業・団体のうちわずか19%（111件中21件）しか復元成功しなかったという統計結果が出ています（警察庁調査）

○　**ウイルス対策ソフトの導入等基本的なセキュリティ対策の実施**

ウイルス対策ソフトはパターンファイルを最新のものに更新してください。

○　**セキュリティ更新プログラムの適用**

OSだけではなく、ソフトウェアやVPN機器等についてもぜい弱性を修正しておいてください。

「サイバー攻撃かも？」と思ったら警察にご相談ください。

☎（088）826-0110　高知県警察本部警備部警備第一課