F－CSNET通信かわら版

令和5年4月 号外

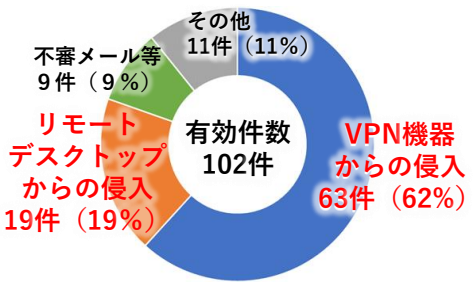
ランサムウェア感染拡大中！！

令和４年中、都道府県警察から警察庁に報告されたランサムウェア被害の件数は230件（前年比57.5％増）と右肩上がりで増加しています。

感染経路は、VPN機器等の遠隔通信からの侵入が80％以上、バックアップから復元できなかった要因はバックアップの暗号化が70％以上を占めました。

ランサムウェア被害の未然防止のためには、遠隔通信におけるセキュリティ対策とオフラインバックアップを適切に行いましょう。

感染経路の割合



基本的なセキュリティを対策を実践

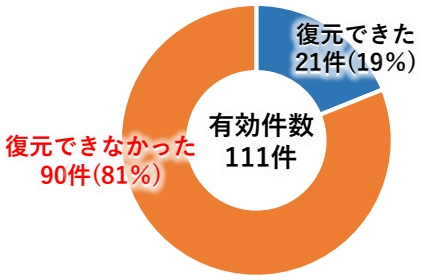
ＶＰＮ機器の更新等

・最新バージョンへの更新（パッチ等の適用）
・パスワードの適切な管理

リモートデスクトップ対策

・OS、ソフトウェアの更新
・外部からのアクセス可能端末やポートの制限
・利用しない機能は切断

バックアップからの復元結果

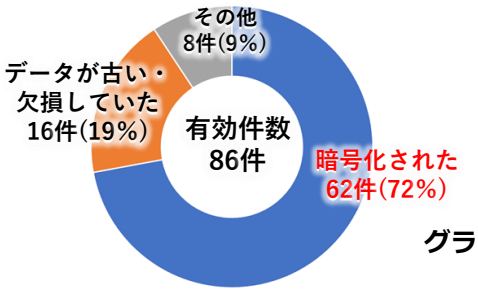


オフラインバックアップを取得

オフラインバックアップ

・　定期的に取得しましょう。
・　復旧の手順を確認しましょう。

復元できなかった理由



■感染したシステム等の復旧までに２か月以上を要した事例
■調査・復旧のために5,000万円以上の費用を要した事例
等の甚大な被害も確認されています。

グラフ出典：「令和４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」（令和５年３月16日警察庁）

◆　福岡県中小事業者サイバーセキュリティ支援ネットワーク（通称：F-CSNET）とは、県内中小事業者のサイバー犯罪被害の未然防止･拡大防止を目的として、県内の中小企業支援団体と公的機関で構築したネットワークです。

◆　福岡県警察本部サイバー犯罪対策課では、最新のサイバー犯罪の手口や対策などをTwitterやホームページに掲載していますので、ぜひご覧ください。

【Twitter】　【HP】