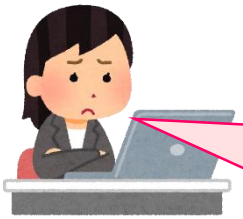
F－CSNET通信かわら版

令和5年8月 号外

ログをオフラインで保存しましょう！

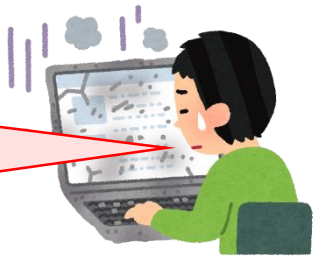
サーバやパソコン、通信機器等のログは、ランサムウェア感染などのサイバー事案の予兆把握・未然防止や、被害が発生した際の原因究明・再発防止に必要不可欠ですので、必ずログを取得し保存しましょう。

■ ログを保存していないと…



当社のシステムは、ログを保存していないから、不審な通信を把握できず心配だわ。

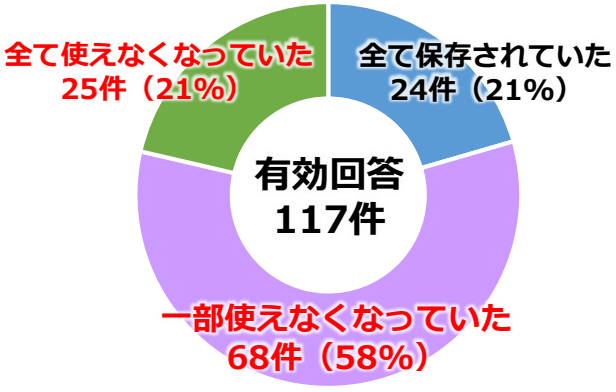
ファイルが暗号化された！ログを保存していなかったから、被害の状況が分からないよ。



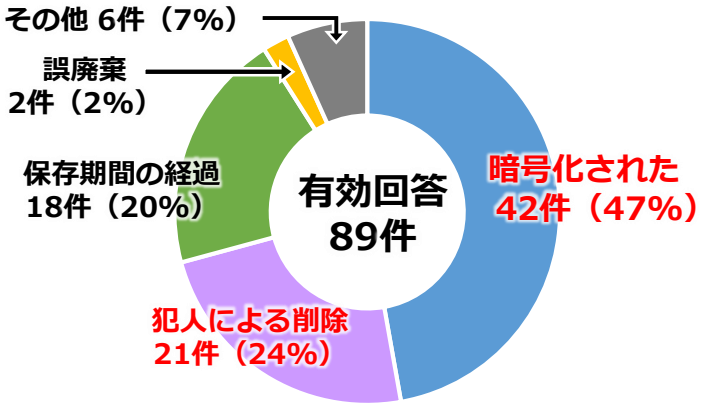
■ ランサムウェア被害におけるログの保存状況（令和４年中）

ログが使用不能になった要因は、犯人による暗号化又は削除が過半数を占めています。

ログの保存状況



ログが使用不能になった要因



※「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）から抜粋

■ ログ保存の留意点

攻撃者によるログの削除・暗号化を防ぐため、ログはオフラインで保存しましょう。
また、ログの保存期間はシステムの目的、要件等を踏まえて決定しましょう。

《参考》NISC（内閣サイバーセキュリティセンター）及びJPCERT/CC（一般社団法人JPCERTコーディネーションセンター）は、ログの保存期間を１年以上にすることが望ましいとしています。

ランサムウェアや不正アクセス等のサイバー犯罪の被害に遭われた場合は、最寄りの警察署に通報・相談してください。

◆ 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、X（旧 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。

【X】（旧 Twitter）【ホームページ】