CyberNews

令和5年9月
宮城県警察本部
サイバー犯罪対策課

ログを保存していますか？

《 ログ保存の重要性 》 ※ログとはコンピュータの利用状況などの履歴や情報の記録のこと。

サーバやパソコン、通信機器等のログは、

○ サイバー事案等の予兆把握・未然防止

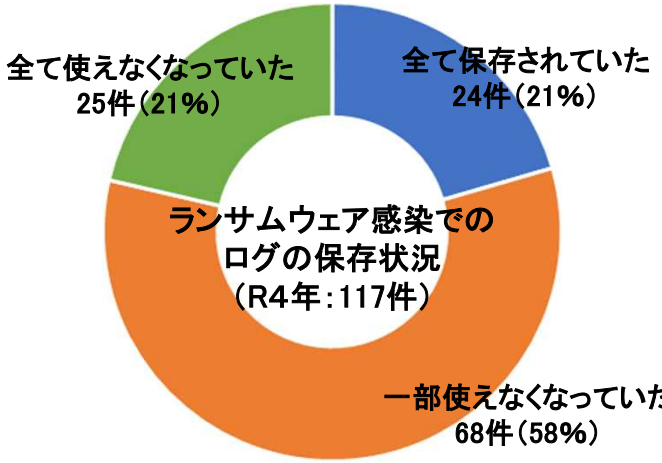
○ サイバー事案等の被害が発生した際の原因究明・再発防止

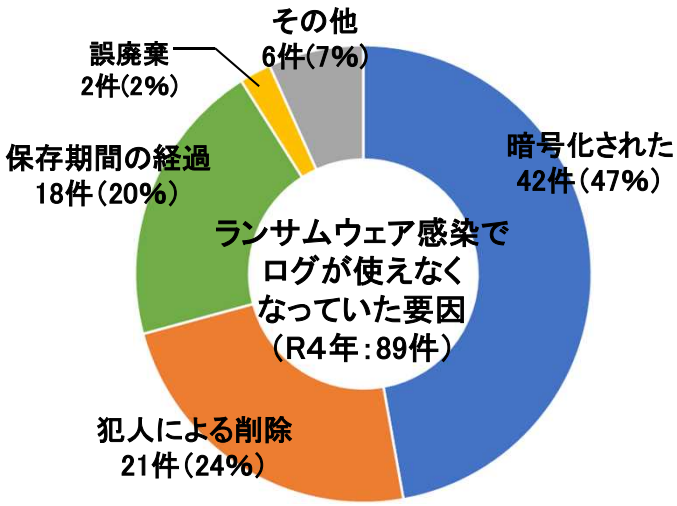
に必要不可欠です。

必ずログを取得し保存しましょう。

攻撃者はログを暗号化・削除します

ランサムウェア感染事案等のサイバー事案では、攻撃者はログを暗号化・削除します。
また、保存期間が経過していたためにログが使えなかった事例も報告されています。





「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

攻撃者による暗号化・削除を防ぐために

◇ ログの保存はオフラインで実施しましょう。

◇ 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てください。