



静岡県警察からのお知らせ

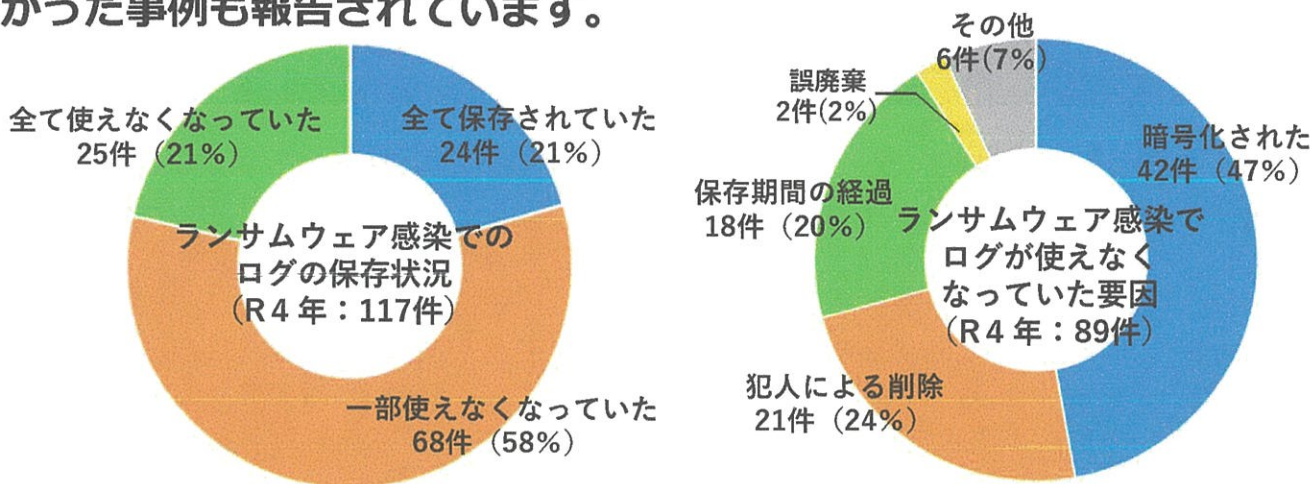
ログ（記録）、保存していますか？

ログ保存の重要性

- 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。

攻撃者はログを削除・暗号化します！

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

コピーしたログの保管はオフラインで

ログが暗号化・削除がされてしまうと、その要因が外部からの攻撃によるものか、内部不正によるものかなどの特定が出来ず、被害拡大を招くおそれがありますので、ログのコピーを作成し、定期的に**オフラインで保管**してください。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**してください。

【保存期間の例】クレジットカード業界のセキュリティ基準であるPCI DSS v4.0では、「監査ログの履歴を少なくとも12カ月間保持（略）する。」とされています。

