サイバー警察局便り

Cyber Police Agency Letter R5 Vol.14

ログ、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、

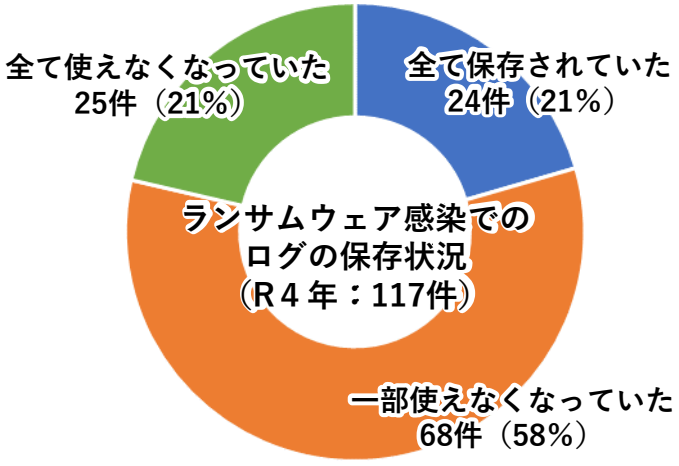
○　サイバー事案等の予兆把握・未然防止

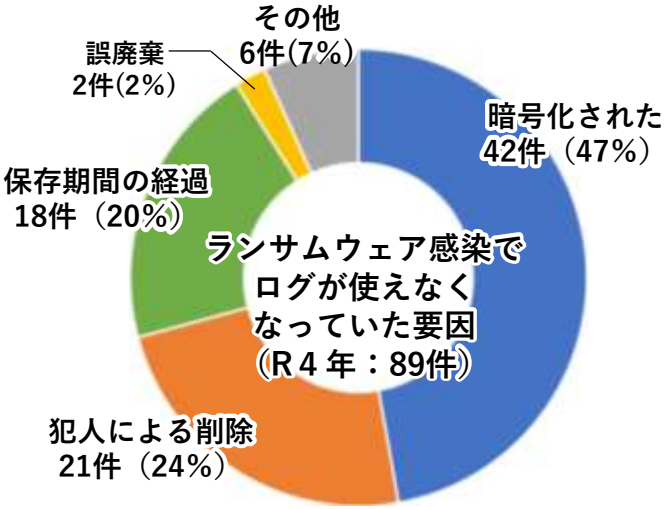
○　サイバー事案等の被害が発生した際の原因究明・再発防止

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

ログの保存はオフラインで

攻撃者による削除・暗号化を防ぐため、ログは**オフラインで保存**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。

警察庁 National Police Agency

ランサムウェア対策をはじめとした各種サイバー事案対策、相談窓口等を掲載しています。⇒ https://www.npa.go.jp/bureau/cyber/index.html