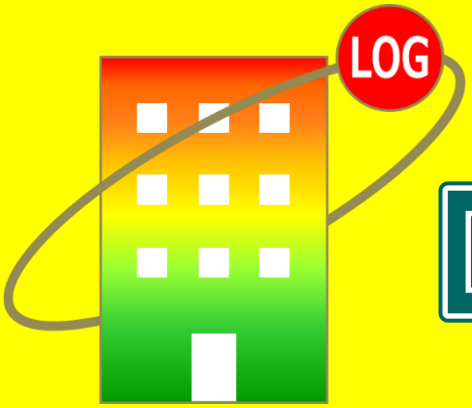


セキュリティインシデントから

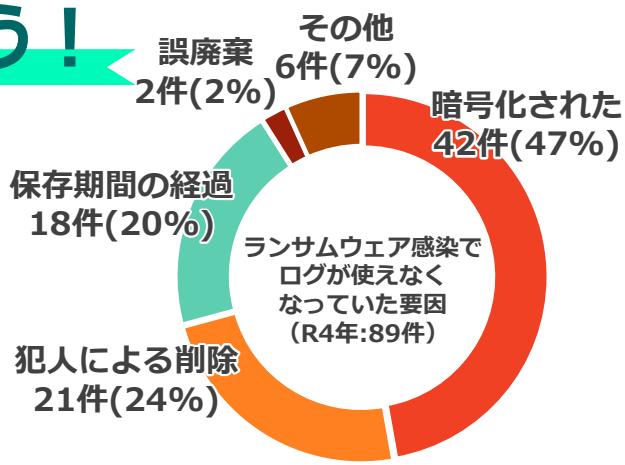
ログは会社を救う

1 ログって何に役立つの？

サーバーやパソコン、通信機器などのログは
不正アクセスなどの予兆把握や未然防止
被害発生時の原因究明、再発防止
に役立てることができます

2 攻撃者はログを狙う！

ランサムウェア感染事案等では、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

3 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か月間保持(略)する。」とされています。

岡山県警察本部サイバー犯罪対策課

警察庁
National Police Agency