CyberCrime Control Project

令和５年８月

広島県警察本部
サイバー犯罪対策課
☎082-228-0110

【ログ】保存していますか？

ログ保存の重要性

- ☑ ログとは、利用状況や通信状況等の**詳細な記録**のこと。
- ☑ ログの保存は、重要な**セキュリティ対策**の一つ。
- ☑ ログが保存されていれば、サイバー攻撃等の被害時に、**攻撃経路、攻撃の時期、感染したファイルの特定**等が判明する場合がある。

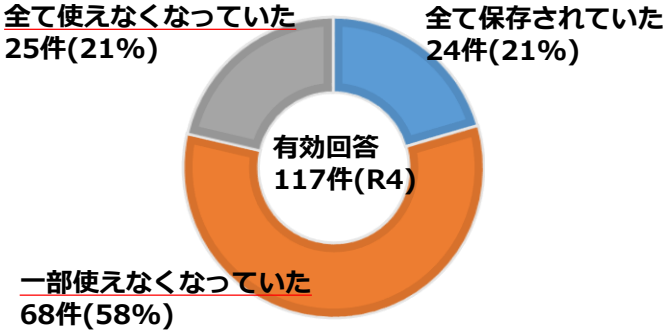
ログ(例)

192.168.2.xx	30/Aug/2023 00:02:01	GET/******
192.168.2.xxx	30/Aug/2023 00:02:05	POST/******
IPアドレス	日時	動作等

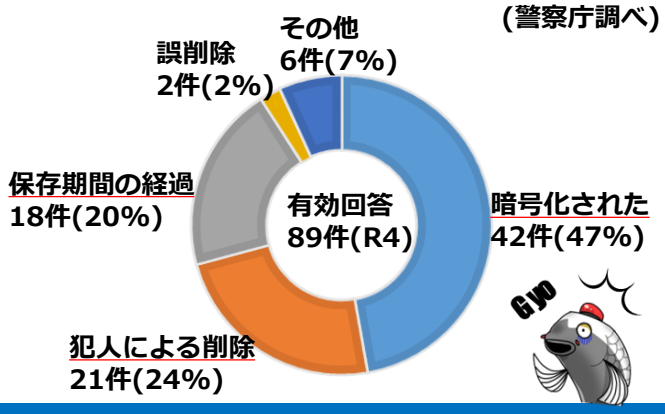
攻撃者はログを削除・暗号化します！！

- ☑ ランサムウェアでは、攻撃者はログを**暗号化**、**削除**する場合がある。
- ☑ 保存期間が**経過**していたためログが使えなかった事例も・・・。

▶ランサムウェア感染でのログの保存状況
(警察庁調べ)



▶ランサムウェア感染でログが使えなくなっていた要因
(警察庁調べ)



ログの保存はオフラインでも！！

- ☑ 攻撃者による削除・暗号化を防ぐため、ログは**オフライン**でも保存。
- ☑ 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。

【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、「監査ログの履歴は少なくとも１２カ月保持(略)する。」とされています。

ランサムウェアなどによるサイバー犯罪被害の相談・通報は・・・

- ▶ サイバー１１０番　☎０８２－２１２－３１１０（平日午前８時３０分から午後５時までの間）
- ▶ 広島県警察本部サイバー犯罪対策課（代表☎０８２－２２８－０１１０）
- ▶ 最寄りの警察署