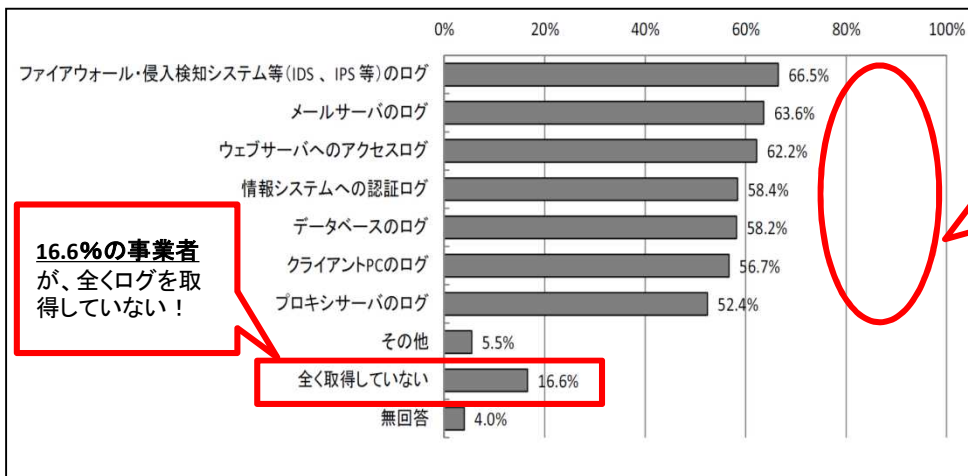


サイバー攻撃への対処には ログの取得・保存が不可欠です！

事業者におけるログの取得実態

特定の業種、地域に偏りのないよう、全国の3,089事業者を無作為に抽出し、回答を得た704事業者のログ取得状況について集計



いずれのログも
3割を超える
事業者
が取得していない！

16.6%の事業者
が、全くログを取
得していない！

引用：平成28年 警察庁生活安全局情報技術犯罪対策課「不正アクセス行為対策等の実態調査」
<https://www.npa.go.jp/cyber/research/>

ログの重要性

- ログを取得し、ネットワーク上の全ての通信を把握することで、不審な通信等にいち早く気づくことができます。
- また、ログを保存しておけば、インシデントが発生したとしても、
 - ・ 「どこから侵入されたのか」
 - ・ 「何をされたのか」
 等の追跡調査が可能となるため、迅速的確な復旧、再発防止対策等を行うことができます。

お願い

サイバー攻撃を受けることを前提に、可能な限り幅広く、長期間のログの取得・保存に努めてください！

