MWS Cup 2019
課題1-1

nao_sec
小池倫太郎（NTTセキュリティ・ジャパン株式会社）
中島将太　（株式会社サイバーディフェンス研究所）
忠鉢洋輔　（株式会社アクティブディフェンス研究所）

課題1におけるこれまでの取り組み

- **2014：pcapを解析せよ！**
  - 概要：複雑なリダイレクトの解析、クローキングの解析
  - 意図：D3Mデータセット解析/活用の促進
- **2015：改ざんされたサイトを発見せよ！**
  - 概要：改ざんされたサイトの発見と解析
  - 意図：独自データセット収集の促進
- **2016：改ざんされたサイトを発見せよ！（再び）**
  - 概要：2015年の続きで、解析の自動化や検知の工夫点
  - 意図：独自データセット収集の高度化および共有の促進

課題1におけるこれまでの取り組み

- **2017：pcapを解析せよ！**
  - 概要：リダイレクトの解析、JavaScript難読化の解析
  - 意図：データセット解析/活用の促進

- **2018：動的解析ログを解析せよ！**
  - 概要：MK2のログから悪性挙動を解析
  - 意図：データセット解析/活用の促進
    - ついにDrive-by Download攻撃ではなくなった…

今年の方針

- **sazを解析せよ！**
  - 概要：リダイレクトの解析、JavaScriptなどの解析
  - 意図：Drive-by Download攻撃の一連の流れを解析
    - 様々な解析技術を必要とした総合的な問題
      - トラフィック
      - HTML, JavaScript, VBScript
      - SWF
      - Shellcode
    - 他の攻撃を解析する際にも役立つ技術の獲得
      - 難読なスクリプトの解析
      - Exploitコードの理解
      - 暗号アルゴリズムの特定

sazファイル

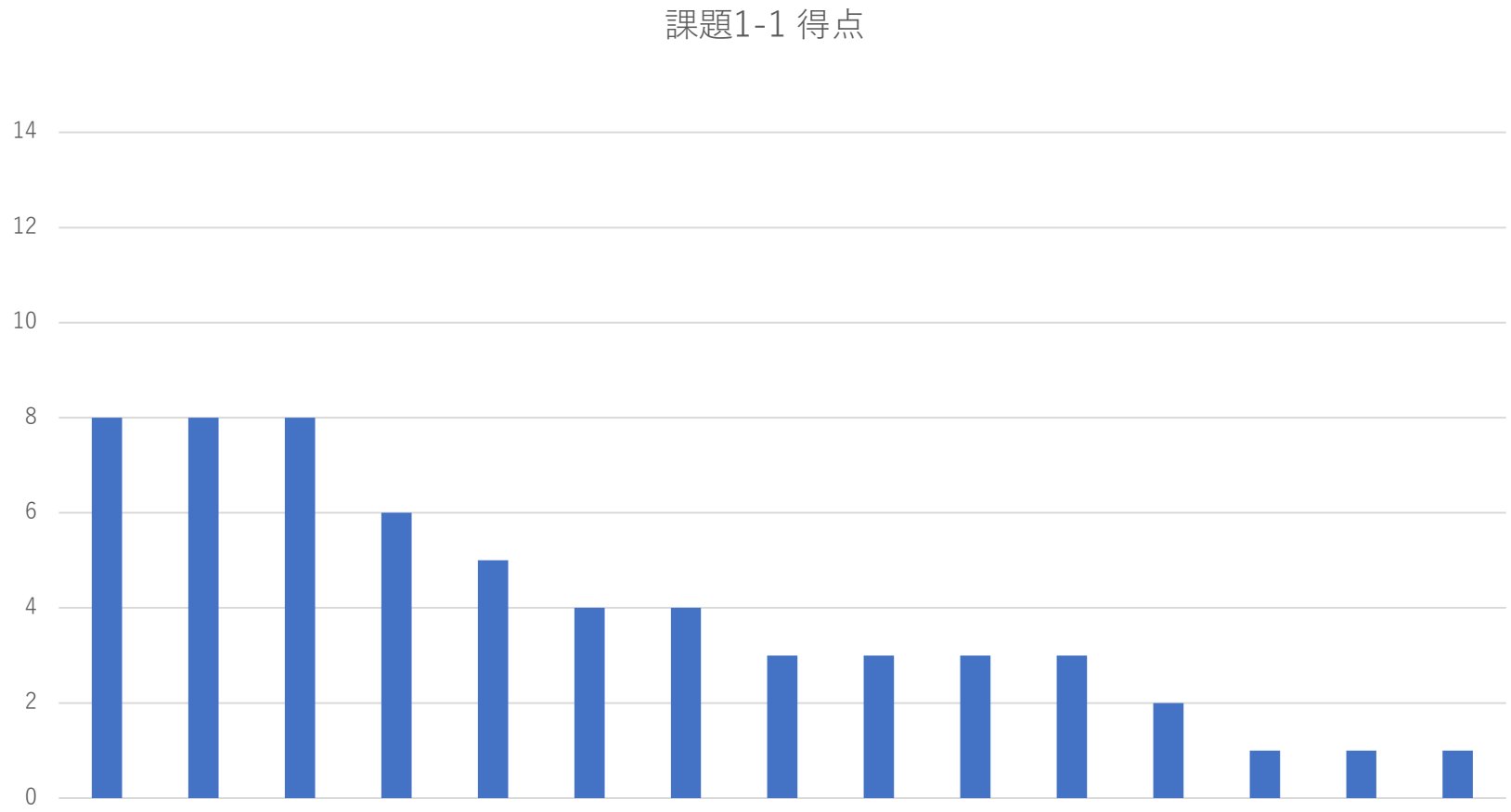
- Fiddlerで使われているフォーマット
  - トラフィックデータをzipの中に保存
    - 事前にFiddlerのインストールは周知済み
      - ただのzipなので、Fiddlerがなくてもunzipすれば解ける
  - DbD解析界隈ではsazファイルを使うのが一般的
    - EK/キャンペーンのHTTPS利用
    - パスワード保護
    - 編集の容易さ
      - pcapファイルを編集するのは結構大変…
    - 優れたツール
      - EKFiddle

問題の解説

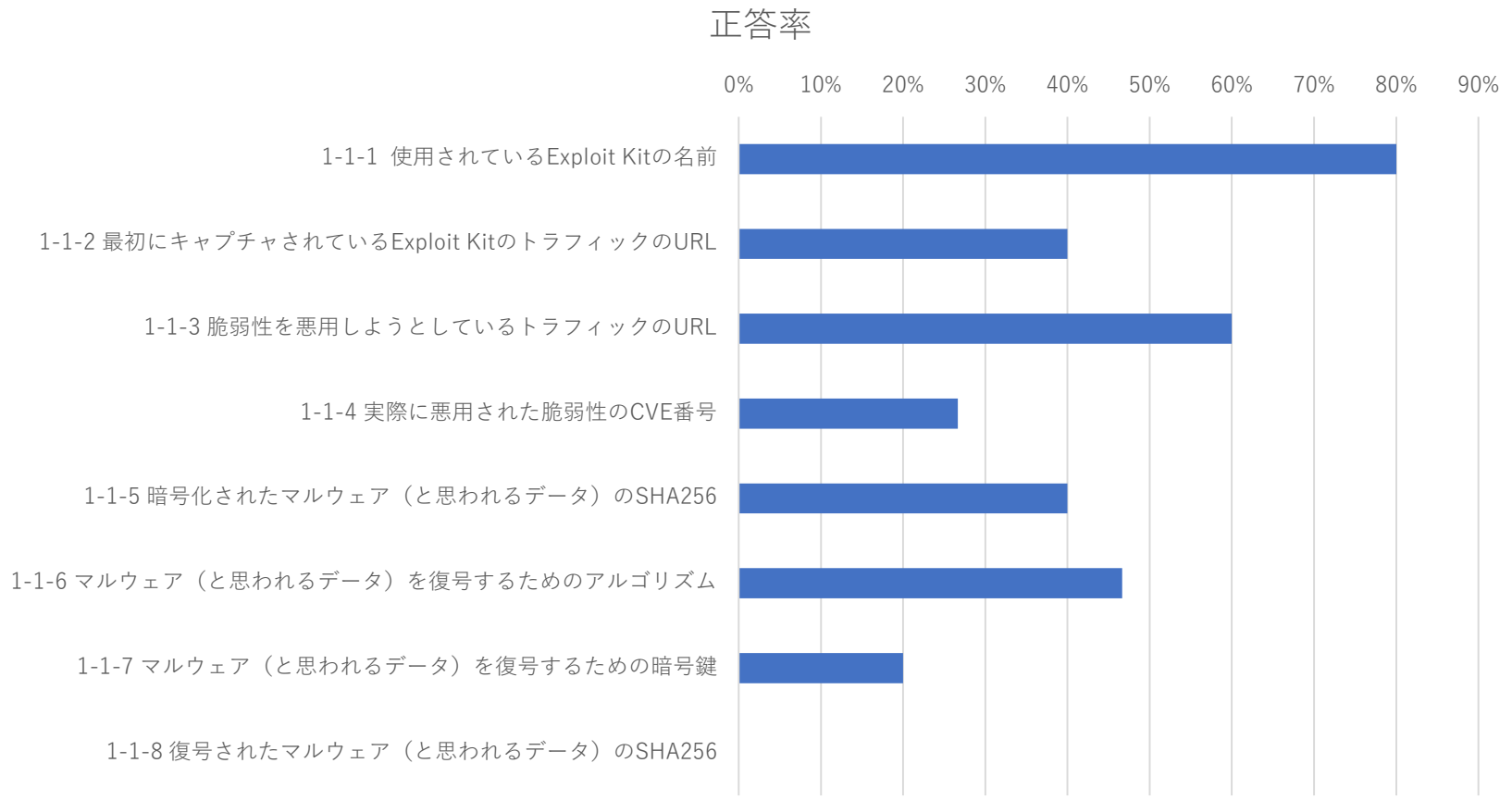
- このあと保要さんがやってくださるので省略

- もし分からないことや気になることがあれば、個別に私へご連絡ください
  - 連絡先：info[at]nao-sec.org

採点結果

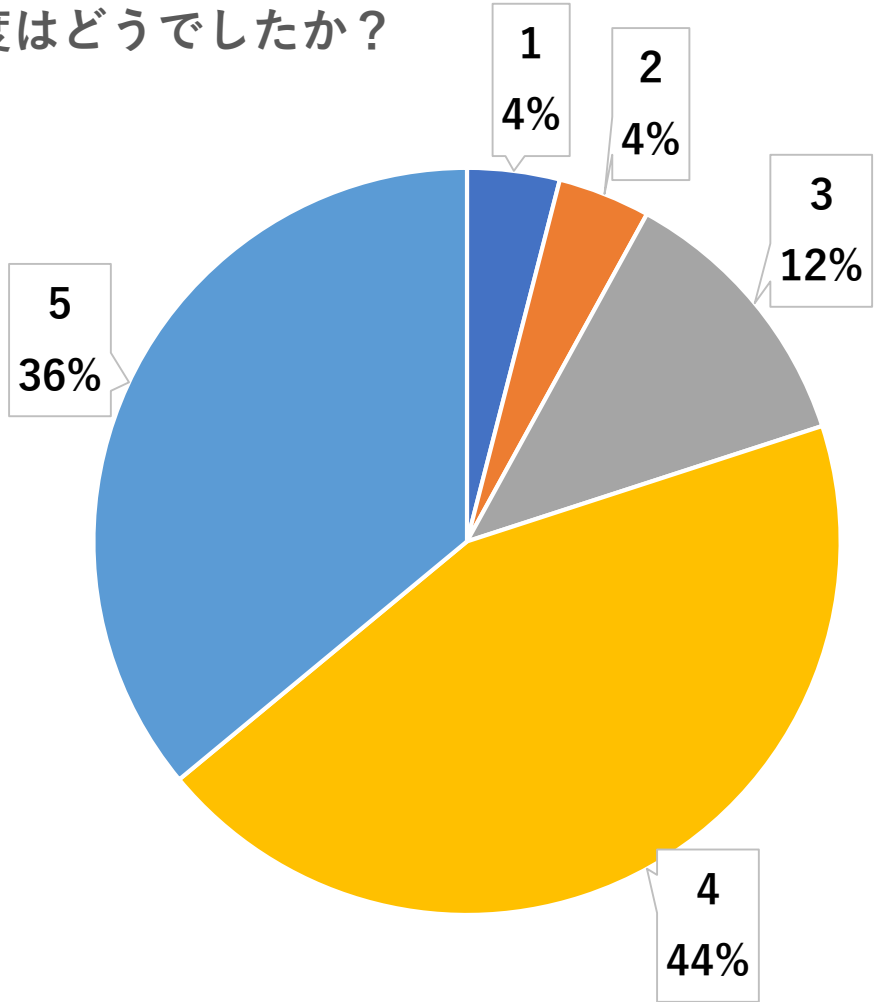


正答率



アンケート

課題1-1の難易度はどうでしたか？



アンケート

- **事前アナウンスについて**
  - MacではFiddlerが重くて動かない！
    - そう言われても…
  - Fiddlerを当日までに使いこなせなかった
    - もう少し早めにアナウンスしても良かったかもしれない

アンケート

- **勉強方法を教えて下さい**
  - MWSデータセットを活用する
    - Soliton Dataset 2019
    - Jinkai Dataset 2017
    - D3M Dataset
  - 一般に公開されているデータを活用する
    - Malware-Traffic-Analysis
    - traffic.moe
  - 今回の暗号アルゴリズムに限って言えば、選択肢は4つしかないので、一般的な実装と比較することで解ける

まとめ

- **今年もDrive-by Download攻撃を解析する問題**
  - 様々な解析技術を要する
    - 教育的なコンテンツ
    - 全体的にあまり点数が良くなかった
  - そろそろネタがなくなってきた
    - 旬ではない
- **来年以降はどうなるか分からない**
  - 事前にアナウンスされる内容には要注意