MWS Cup
課題4 DFIR

NFLabs.

Your Security Partner

株式会社エヌ・エフ・ラボラトリーズ
保要　隆明

問題の主担当

2020年

- 主担当
  - 荒木 粧子（株式会社ソリトンシステムズ）
- 問題作成委員
  - 保要 隆明（株式会社エヌ・エフ・ラボラトリーズ）
  - 白鳥 隆史（株式会社ソリトンシステムズ）
  - 後藤 公太（株式会社ソリトンシステムズ）
  - 尾曲 晃忠（株式会社ソリトンシステムズ）
  - 竹澤 一輝（株式会社ソリトンシステムズ）

問題の主担当

2021年

- 主担当
  - 保要 隆明（株式会社エヌ・エフ・ラボラトリーズ）？
- 担当
  - 募集中

DFIRとは？

DFIR = Digital Forensics and Incident Response

Digital Forensics

デジタルデバイスに記録された情報の回収と分析調査などを行うこと

＋

Incident Response

インシデントの検知、分析、封じ込め、根絶、システムの復旧を行う一連の対応

＝

DFIR

デジタルデバイスに記録された情報の回収と分析調査などを行い、インシデントの検知、分析、封じ込め、根絶、システムの復旧の一連の対応を行うこと

課題4 DFIR

デジタルデバイスに記録された情報（ログ）を分析調査し、どのような
サイバー攻撃が行われたか（どのようなインシデントが発生したか）解明

分析する情報（ログ）

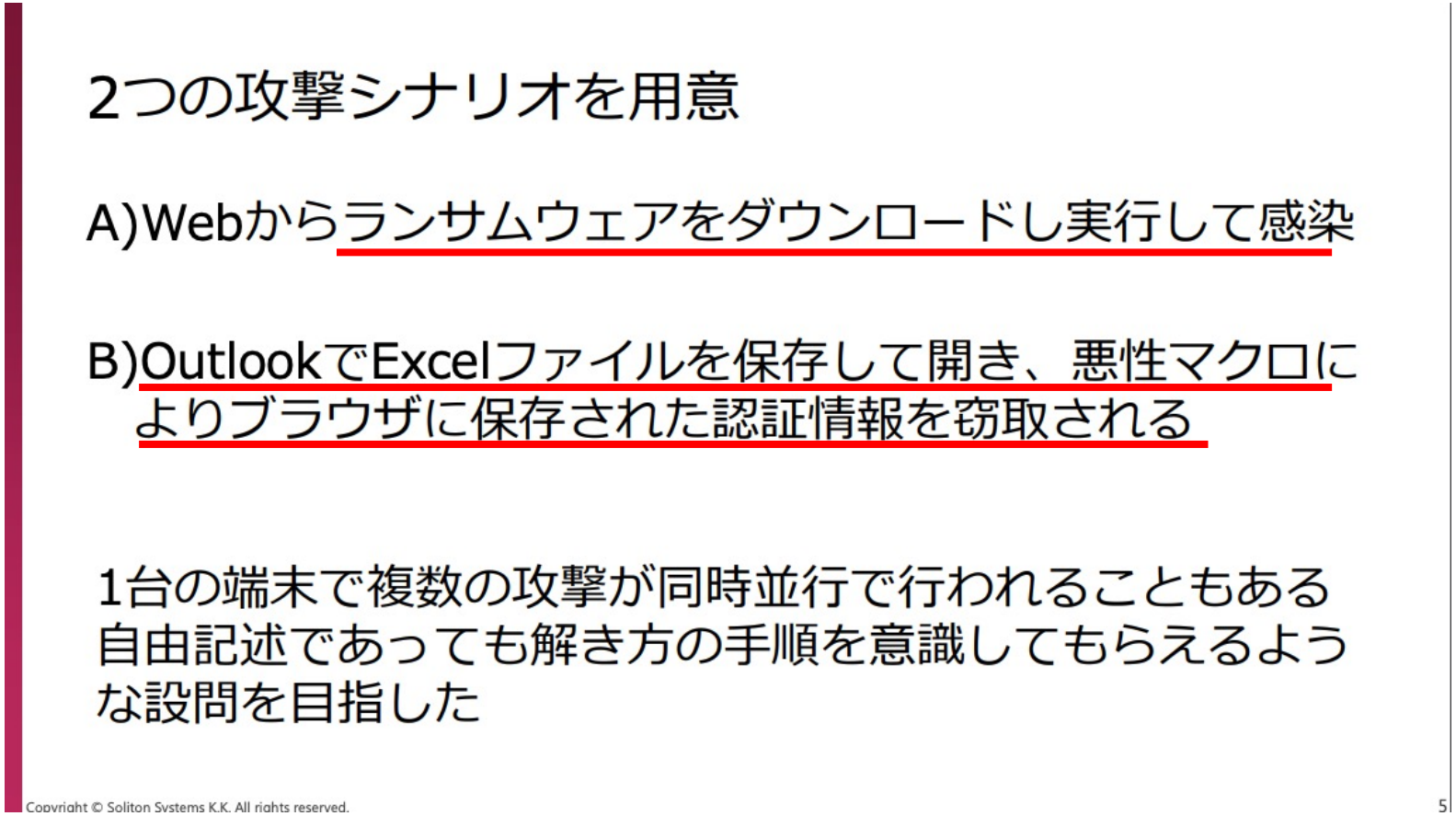
- エンドポイントログ
  - EDR（Soliton InfoTrace Mark II）ログ
  - Soliton Dataset で提供されているデータと同様のフォーマット

分析調査する観点

- どのホストがインシデントの影響を受けているのか？
- どのように攻撃者は侵入/マルウェアに感染したのか？
- どのようにネットワーク内部で侵害を拡大したのか？
- どのような情報が漏えい/暗号化されたのか？
- など

これまでのDFIR問題

2018年（課題1）



https://www.iwsec.org/mws/2018/20181220/MWSCup2018_PostMTG_Soliton_20181220.pdf

これまでのDFIR問題

2019年（課題1）

課題1 動的解析（DFIR）

■ 目的
- 実環境で観測されたDrive-by Downloadトラフィックと
  そこで得られた検体の動作ログから侵害を明らかにする

■ 概要
- Soliton Dataset 2019で提供されているデータと
  同じフォーマットの以下のファイルの解析

■ 課題1-1　Drive-by Downloadトラフィック（15点）
– sazファイルで提供、Fiddler＋EKFiddleを利用して解析

■ 課題1-2　マルウェア動作ログ（10点）
– テキストファイルで提供、Grep、同梱MK2Tree（Pythonツール）、Excel、独自
  ツールなどで解析

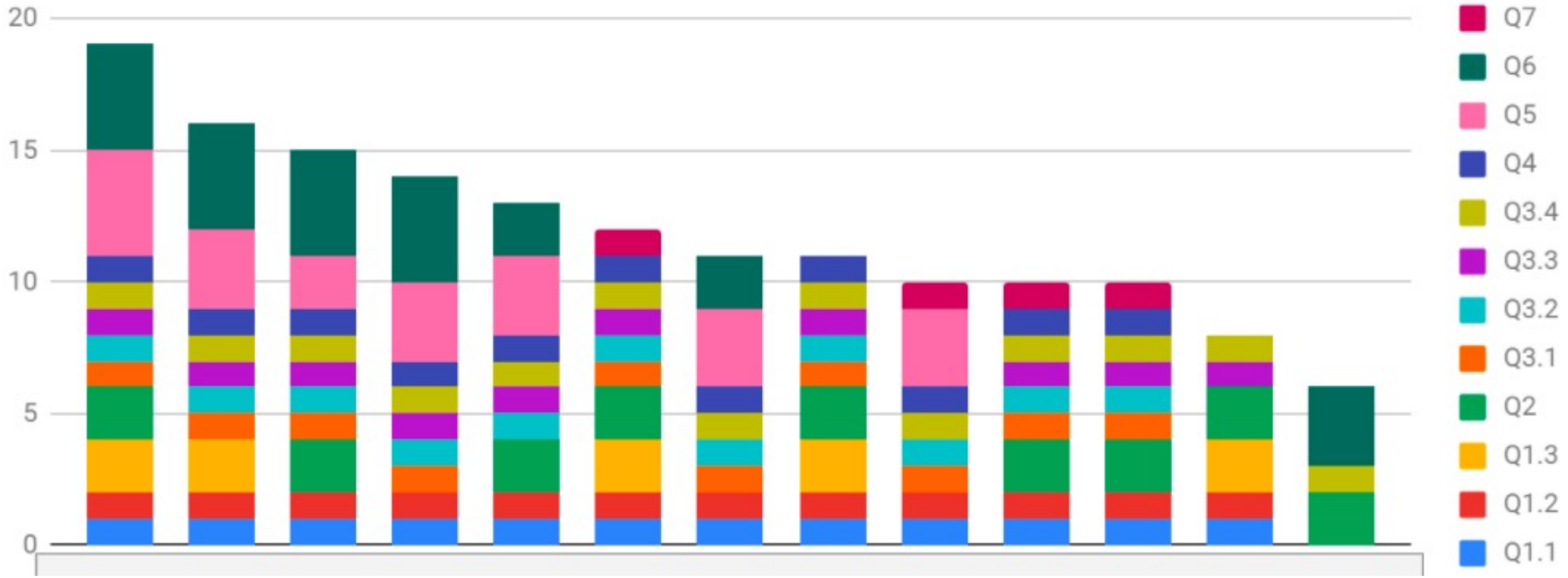
3

https://www.iwsec.org/mws/files/MWSCup2019_c1-2.pdf

これまでのDFIR問題

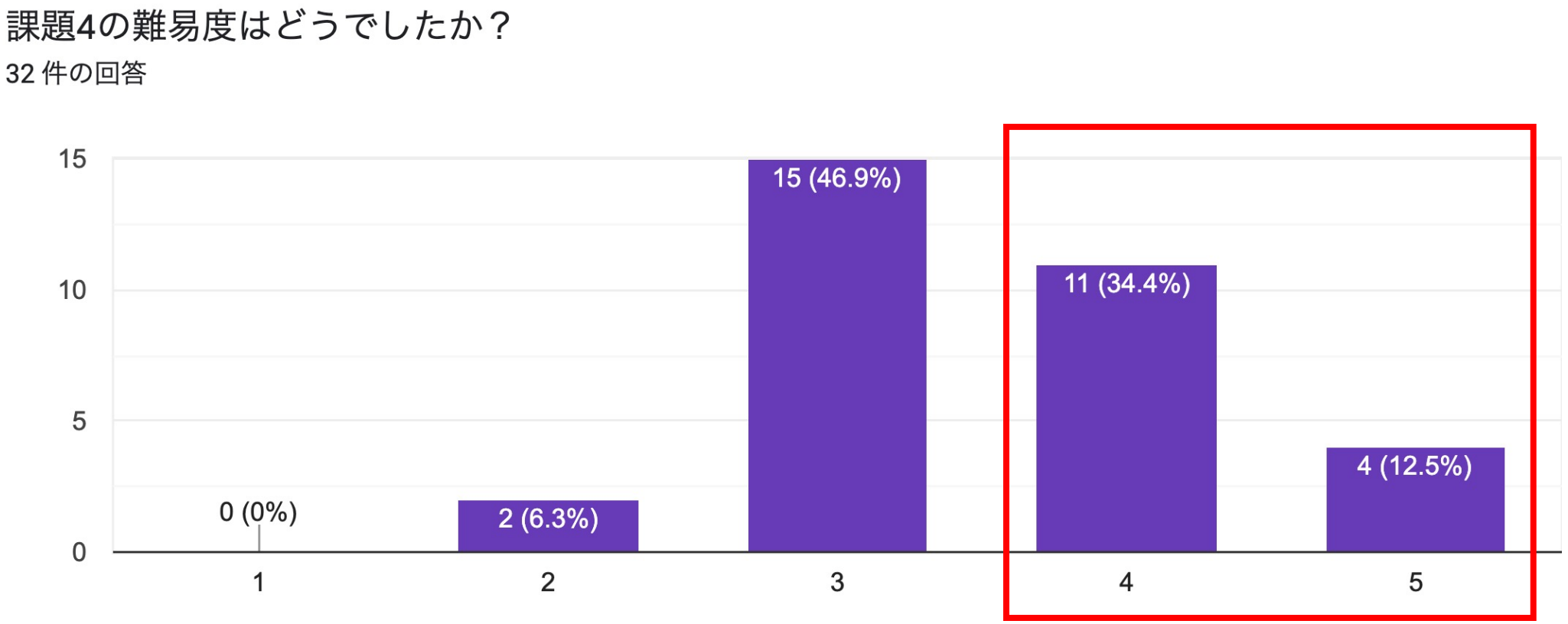
2020年（課題4）

昨年の競技結果



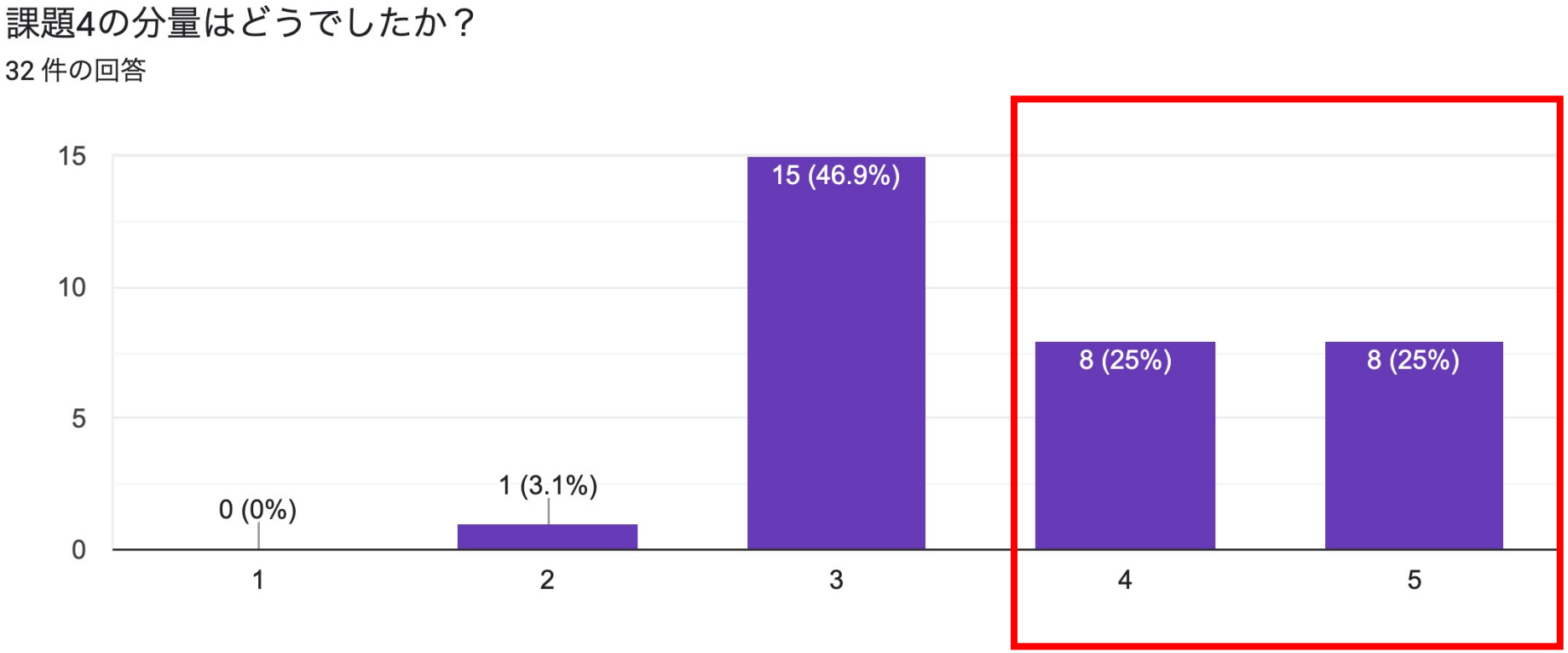
昨年のアンケート結果

- 約半数の参加者が「難しい」



昨年のアンケート結果

- 約半数の参加者が「分量が多い」、難易度より5をつける人が多い



昨年のアンケートの結果

頂いたコメント（抜粋）

- 実務的な問題が多く、勉強になりました。自分が解いた問題に対する、攻撃視点での解説はとても貴重で勉強になりました。
- 解説がログベースと攻撃者視点の両側からあり、MitreのATT&CKの分類からも理解が深まりました
- IRの流れ等が学べると思うので、良い問題だったなと感じた。
- 個人的にはとても楽しく取り組むことができました。

- 解析対象になる環境の情報は事前に公開しても良いのではないかと感じました。
- 初出場なので例年との比較ができないのですが、少し分量が多かった気がします
- 制限時間に対して問題量が若干多かったかなと感じています。

今年の課題4の方針

- 今年も人手による攻撃はやりたい
  - 攻撃側と防御側の目線の両方を知ってもらい、より効果的なセキュリティ対策を考えてもらいたい
- 今年も参加者に楽しみながら問題を解いてもらいたい
- エンドポイントだけでなくネットワークのログも併せて解析してもらいたい
- 事前に環境情報やログフォーマットはアナウンスしたい

課題4の勉強のポイント

- “正常”な状態を知ろう
  - OSやネットワークの通常時に挙動をモニターツールを用いて確認してみる
  - 正常な状態のログを確認してみる
  - ググる

- “異常”な状態を知ろう
  - 攻撃されているログを分析してみる
  - 攻撃が許可されている環境に攻撃を行い、攻撃の特徴を分析してみる
  - 世の中で起きているインシデントを追ってみる
  - ググる

- ログのフォーマットを知ろう
  - 課題で扱う対象のログのフォーマットを事前に把握しておこう
  - ググる

Thank you for listening