



MWS Cup 2023 振り返り

MWS Cup 2023 実行委員長
株式会社 エヌ・エフ・ラボラトリーズ

保要 隆明



目次

- MWS Cup とは？
- 出題課題
- 参加チーム
- 競技結果
- アンケート結果の共有
- 今後のMWS Cup



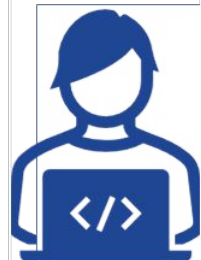
MWS Cupとは？

- MWSで2009年から開催されているセキュリティコンテスト
- マルウェアに関するサイバー攻撃の解析技術を競う
-
- 目的
 - 参加者同士で切磋琢磨することでサイバー攻撃解析に係る技術を向上
 - 実践的なサイバー攻撃解析技術を習得する場を提供
-
- 研究用データセットの活用
 - リアルなサイバー攻撃・マルウェア検体を題材にした実践的な
 - 課題を出題



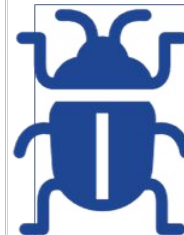
出題課題

- 事前課題: ~10/09 (月) 10:00
- 当日課題: 11/01 (火) (CSS 2日目) 9:00~13:00



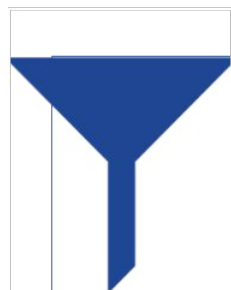
ハッカソン (事前課題)

- セキュリティに関するツールやデータセットを自由な発想で開発



マルウェア静的解析

- GhidraのDBファイル (GZF) からマルウェアの挙動を明らかにする



マルウェア表層情報分析

- マルウェアの表層情報をもとに機械学習を駆使してマルウェアを分類する



攻撃痕跡ログ分析 (DFIR)

- ログ解析し、どのようなインシデントが起きたかを明らかにする



参加チーム、プレイヤー

- ・ チーム数 16
- ・ プレイヤー数 88
- ・ 初参加プレイヤー数 63
- ・ 学生 : 社会人比率 72 : 16
- ・ 現地参加 : オンライン参加 65 : 23 (現地73%)



参加チーム、プレイヤー

- ・ チーム数 14 -> **16**
- ・ プレイヤー数 77 -> **88**
- ・ 初参加プレイヤー数 51 -> **63**
- ・ 学生:社会人比率 60:17 -> **72:16**
- ・ 現地参加:オンライン参加 47 : 30 (現地61%) -> **65 : 23 (現地 73%)**



エントリーチーム (1/2)

チーム名	参加組織
F.SE	大阪大学
SakanaCushion	大阪工業大学
KGU-CSL小林研	工学院大学
人海戦術_Libra	東京電機大学、東京情報大学、静岡大学、日立製作所、日立システムズ
UN頼み	電気通信大学、NTTコミュニケーションズ
𠄎脳筋鹿煎餅𠄎 NEONEO	奈良先端科学技術大学院大学
人海戦術_Virgo	東京電機大学、東京情報大学、静岡大学、日立システムズ
チームいちぴろ	広島市立大学
モンキーポッド	NTTコミュニケーションズ
人海戦術_Lepus	東京電機大学、東京情報大学、静岡大学、日立システムズ



エントリーチーム (2/2)

チーム名	参加組織
Wide Angel	NTTコミュニケーションズ
secu wing B3	岡山大学
Enduring Pug	岡山大学
セキュリティ讃歌	岡山大学
GoGoYossy	早稲田大学
二向聴	早稲田大学



最終結果

総合順位	チーム名	ハッカソン	静的解析	マルウェア分類	DFIR	合計得点
1	UN頼み	24.50	11.00	24.00	25.00	84.50
2	GoGoYossy	20.50	11.00	25.00	11.00	67.50
3	セキュリティ讃歌	18.50	11.00	15.00	19.00	63.50
4	F.SE	16.25	8.00	18.00	18.00	60.25
5	Wide Angel	10.25	6.00	23.00	19.00	58.25
6	SakanaCushion	13.75	11.00	9.00	24.00	57.75
7	𠄎脳筋鹿煎餅𠄎NEONEO	15.00	12.00	3.00	24.00	54.00
8	人海戦術_Libra	21.75	9.00	4.00	19.00	53.75
9	二向聴	6.75	8.00	19.00	15.50	49.25
10	人海戦術_Virgo	18.50	9.00	1.00	18.50	47.00
11	モンキーポッド	13.75	4.00	1.00	20.50	39.25
12	人海戦術_Lepus	8.50	7.00	0.00	22.00	37.50
13	Enduring Pug	0.00	2.00	23.00	7.00	32.00
14	secu wing B3	0.00	2.00	6.00	15.00	23.00
15	チームいちぴろ	0.00	4.00	0.00	10.00	14.00
15	KGU-CSL小林研	0.00	4.00	3.00	7.00	14.00



アンケート結果共有



アンケート結果共有

- MWS Cup 実施後に参加者にアンケートを実施
- 参加者 41/88名 が回答

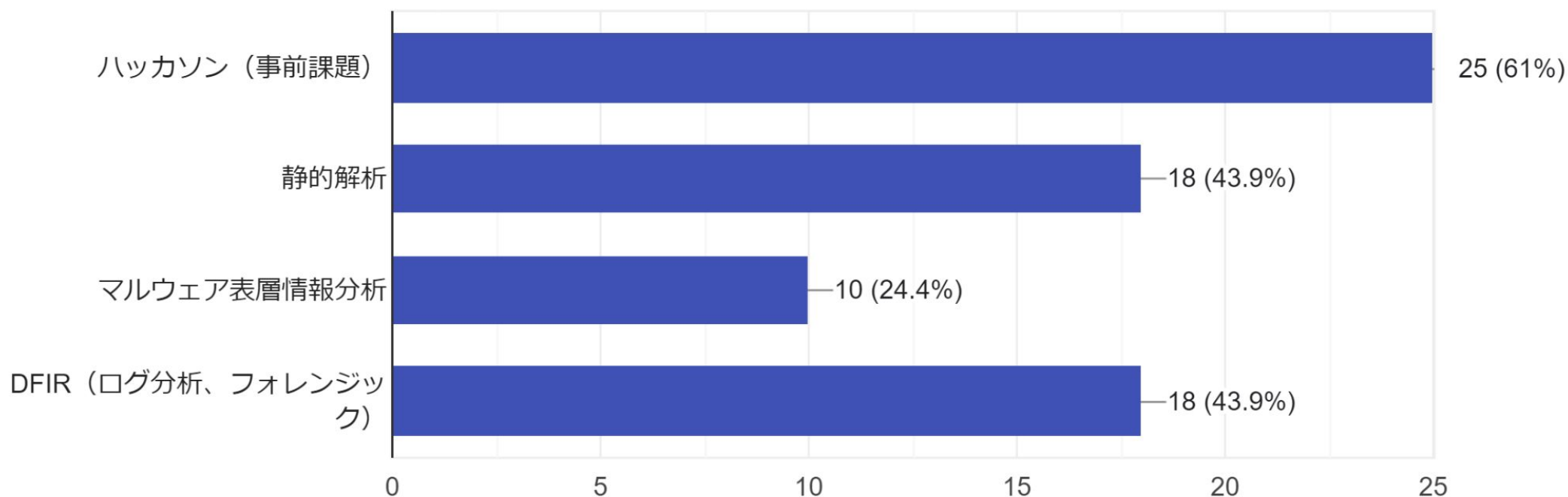
アンケートにご回答いただいた皆様、
ありがとうございました！



取り組んだ課題

あなたが取り組んだ課題を選択してください。（...い課題についての回答は任意回答となります。）

41 件の回答



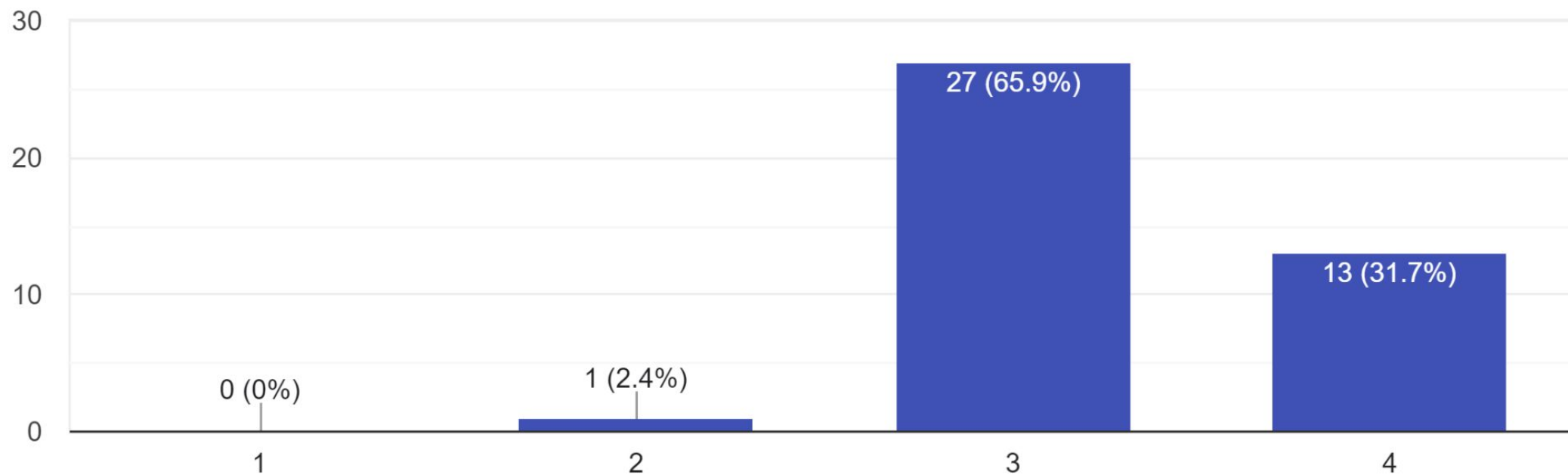
静的解析、DFIRを解いてる人の回答が多い



全体難易度

MWS Cup の課題の難易度は全体的にどうでしたか？

41 件の回答



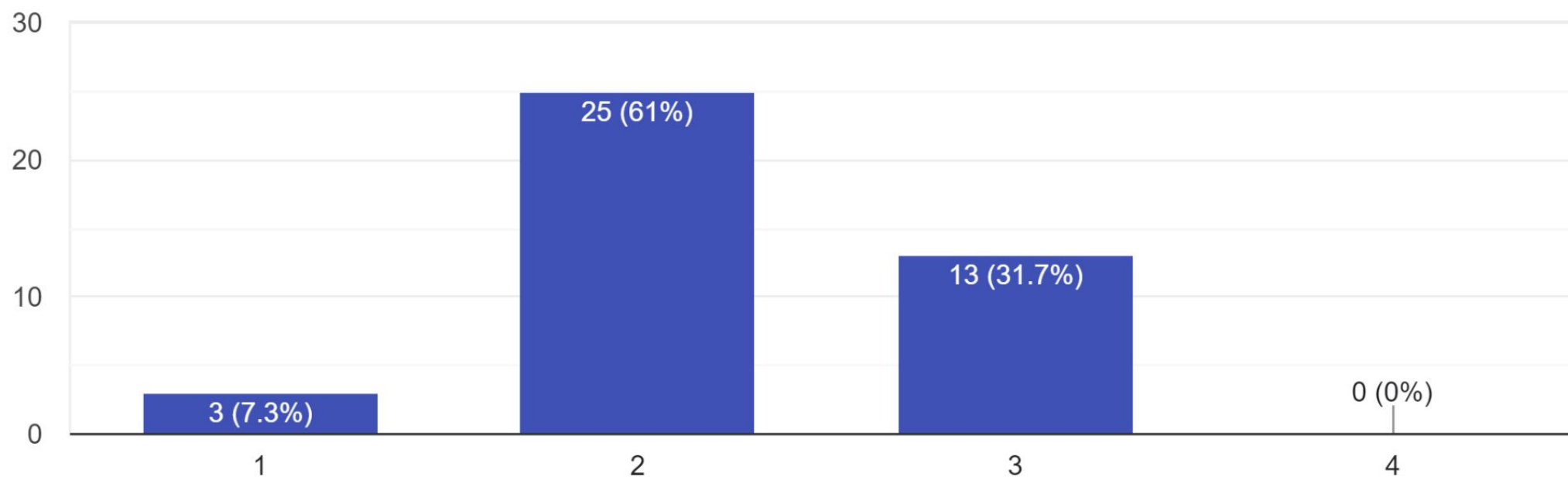
ちょっと難しい？



競技時間

MWS Cup の競技時間はどうでしたか？

41 件の回答



ちょっと短い？

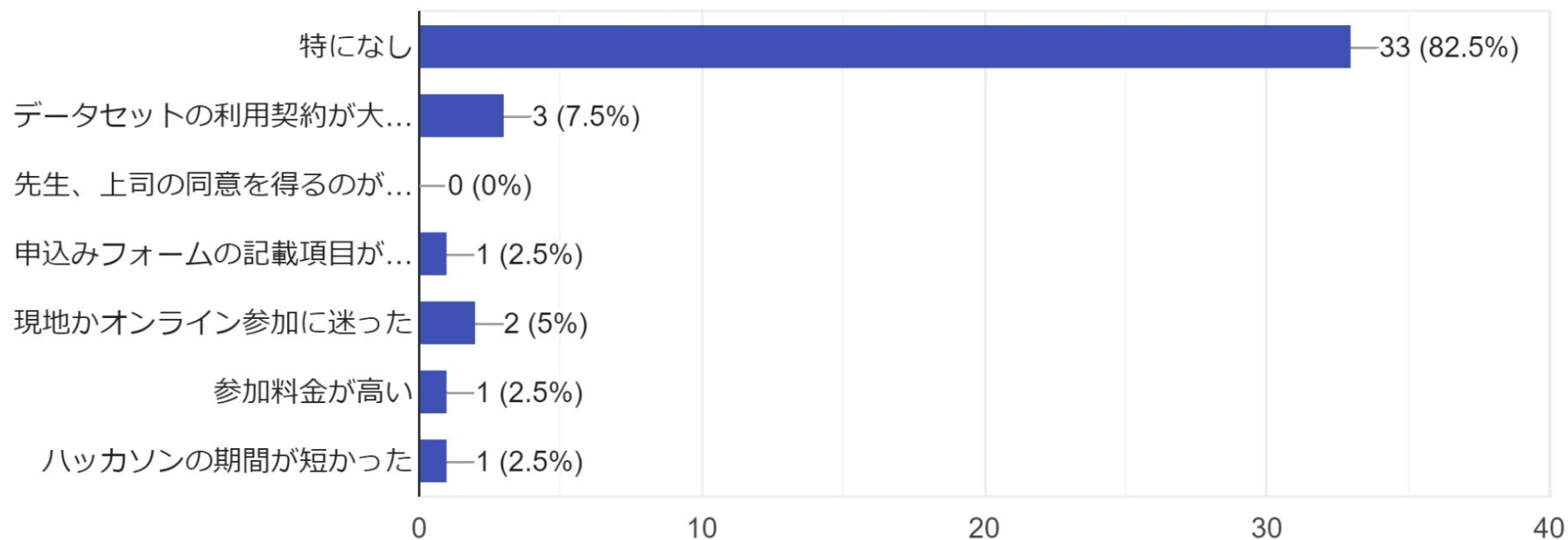


申込みの障壁は？

MWS Cup

参加申込みにあたり迷ったこと、障壁となったことはありましたか？あれば教えてください。

40件の回答





オンライン/会場について

現地会場について

- 去年より会場が広く集中できて良かった
- 電源タップがたくさんあって助かりました！
- 今年はネットワークが会場で提供されており、問題なく使えました
- グループ名のプレートをいただけて良かったです。記念に飾ります
- 現地でやると他の参加者と交流ができて楽しかったです。
- 現地開催をしてくださることによって、企業の方と交流ができ、よかったです。
- 会場のwifiが弱くて最初challengeが見れなかった
- 会場のキャパシティが少し小さかったように感じましたので、来年以降はもう少し大きい会場だとありがたく思います。

オンライン会場について

- オンライン参加でしたが特段困りごとはありませんでした
- オンライン開催されていたため、参加のハードルが低く参加しやすかったです



MWS

MWS Cup の全体への意見や感想

- 学生の自分には全体的に難しい課題でしたが、おもしろかったです。
 - 毎年新しいセキュリティの知識を身につけることができるため、セキュリティ業界への就職を考えている身としてはとてもありがたいです。問題を解くこと自体も楽しく、継続して開催していただきたいと考えています。
 - セキュリティに関する課題を限られた時間で挑戦するというのは初めてだったのでとても楽しかった。
 - 研究室で上下やほかの研究室とコラボするとても良い機会になっている
-
- 個人的には年々Cupのレベルが上がり、投入しなければいけないリソースも莫大になりつつある点が不安に思う。要はコンテストとしての練度が上がり、ほかのチームに勝つためにはほかのチーム以上の努力が必要で、多くの場合は努力=時間になるのかと思う。



来年以降のMWS Cupの展望

- ・ オンライン/現地のハイブリッドは継続したい
 - ・ CSSの開催形態に依存
- ・ 現地では、広い部屋、ネットワーク、電源、チームプレートを準備
 - ・ チームプレート以外は、CSS会場の状況に依存
- ・ MWSのスコープ拡大によっては、MWS Cup の課題も変更を検討