

MWS



MWS Cup 2024 振り返り

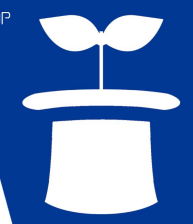
MWS Cup 2024 副委員長
株式会社FFRIセキュリティ

桑原 翼



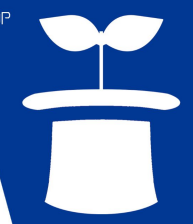
目次

- ・ 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



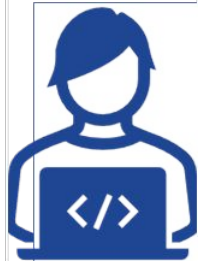
MWS Cupとは？

- ・ MWSで2009年から開催されているセキュリティコンテスト
- ・ 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



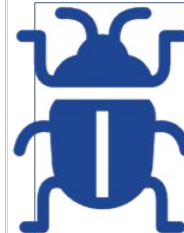
出題課題

- ・ 事前課題: ~10/01 (火) 10:00
- ・ 当日課題: 10/23(水)(CSS 2日目) 9:00~13:00



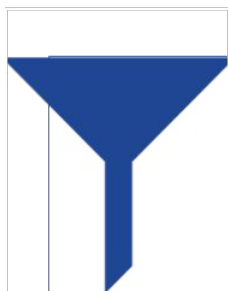
ハッカソン (事前課題)

- ・ 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



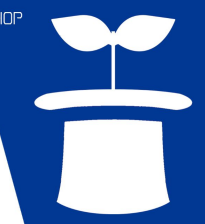
攻撃痕跡ログ分析 (DFIR)

- 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 19
- プレイヤー数 97
- 初参加プレイヤー数 66
- 学生:社会人比率 86:11
- 現地参加:オンライン参加 77 : 20 (現地79%)



参加チーム、プレイヤー

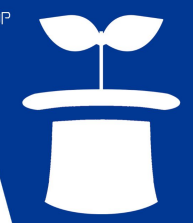
- チーム数 16 -> **19**
- プレイヤー数 88 -> **97**
- 初参加プレイヤー数 63 -> **66**
- 学生:社会人比率 72:16 -> **86:11**
- 現地参加:オンライン参加 65 : 23 (現地73%) -> **77 : 20 (現地 79%)**

チーム名	参加組織
UN頼み	電気通信大学、NTTコミュニケーションズ
チームいちぴろ	広島市立大学、SBテクノロジー
セキュリティ讃歌	岡山大学
44GK44Gk44GL44KMIQ==	工学院大学
F.SE	大阪大学
THE SKY	早稲田大学
全無太郎	株式会社ZenmuTech
𐄂脳筋鹿煎餅𐄂 NEONEONEO	奈良先端科学技術大学院大学
Moo	早稲田大学
人海戦術_Backdoor	静岡大学、東京情報大学、東京電機大学、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
SakanaCushion	大阪工業大学
BirdStone	大阪工業大学
DSOL11G	NTTコミュニケーションズ
人海戦術コードブルー	東京情報大学、静岡大学、東京電機大学、日立システムズ
Gunmataro	群馬大学
Gunmahanako	群馬大学
人海戦術_ハッカソンズ	静岡大学、東京電機大学、日立製作所、東京情報大学
Enduring Pug	岡山大学
𐄂脳筋鹿煎餅𐄂 NEONEO	奈良先端科学技術大学院大学、名古屋工業大学



最終結果

同点の場合はKaggle
のスコアで順位づけ

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	23.40	18	23.00	23.00	87.40
2	SakanaCushion	21.40	10	22.00	21.00	74.40
3	人海戦術_backdoor	13.40	7	22.00	21.00	63.40
4	THE SKY	8.80	9	22.00	22.00	61.80
5	Moo	18.60	10	24.00	9.00	61.60
6	セキュリティ讃歌	15.20	10	22.00	13.00	60.20
7	BirdStone	11.40	7	22.00	12.00	52.40
8	F.SE	0.00	14	24.00	10.00	48.00
9	チームいちぴろ	8.40	9	20.00	9.00	46.40
10	人海戦術コードブルー	22.40	5	5.00	9.00	41.40
11	𐄂脳筋鹿煎餅𐄂 NEONEONEO	0.00	7	22.00	12.00	41.00
12	Gunmataro	0.00	8	22.00	10.00	40.00
13	Enduring Pug	0.00	0	22.00	17.00	39.00
14	Gunmahanako	0.00	8	22.00	6.00	36.00
15	𐄂脳筋鹿煎餅𐄂 NEONEO	0.00	14	22.00	0.00	36.00
16	44GK44Gk44GL44KMIQ==	0.00	13	0.00	16.00	29.00
17	人海戦術_ハッカソソズ	0.00	14	0.00	15.00	29.00
18	DSOL11G	0.00	4	7.00	10.00	21.00
19	全無太郎	0.00	0	0.00	6.00	6.00



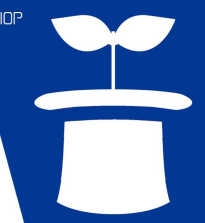
アンケート結果共有



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 78/97名 が回答

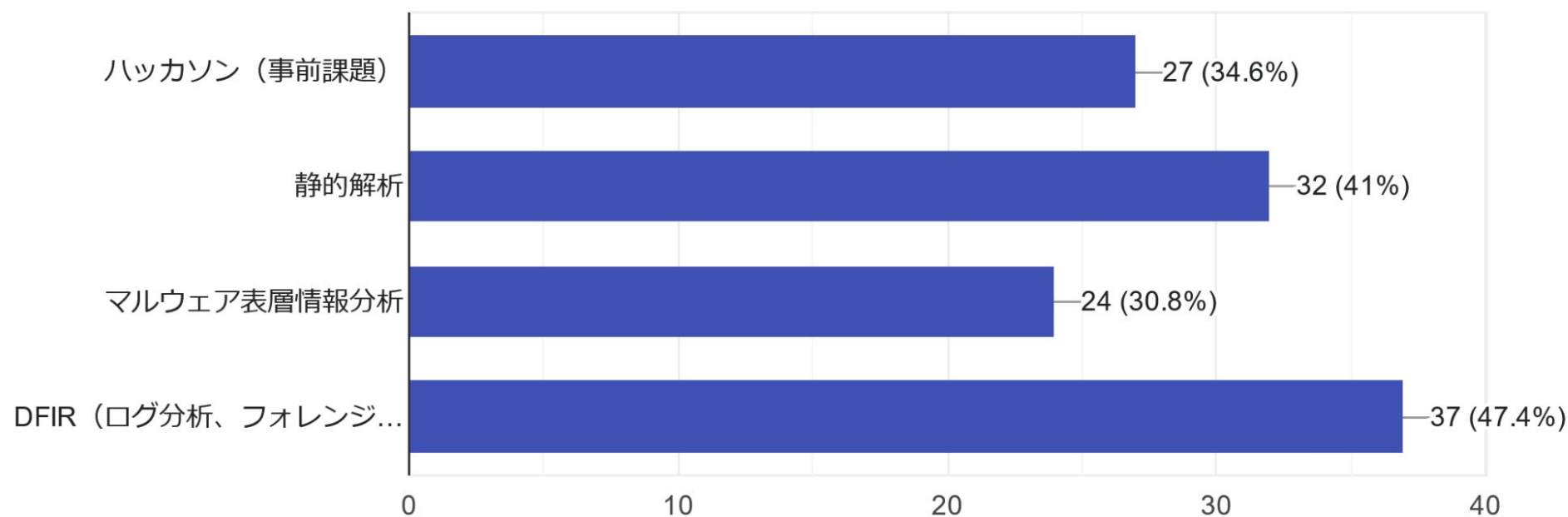
アンケートにご回答いただいた皆様、
ありがとうございました！



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。）

78 件の回答



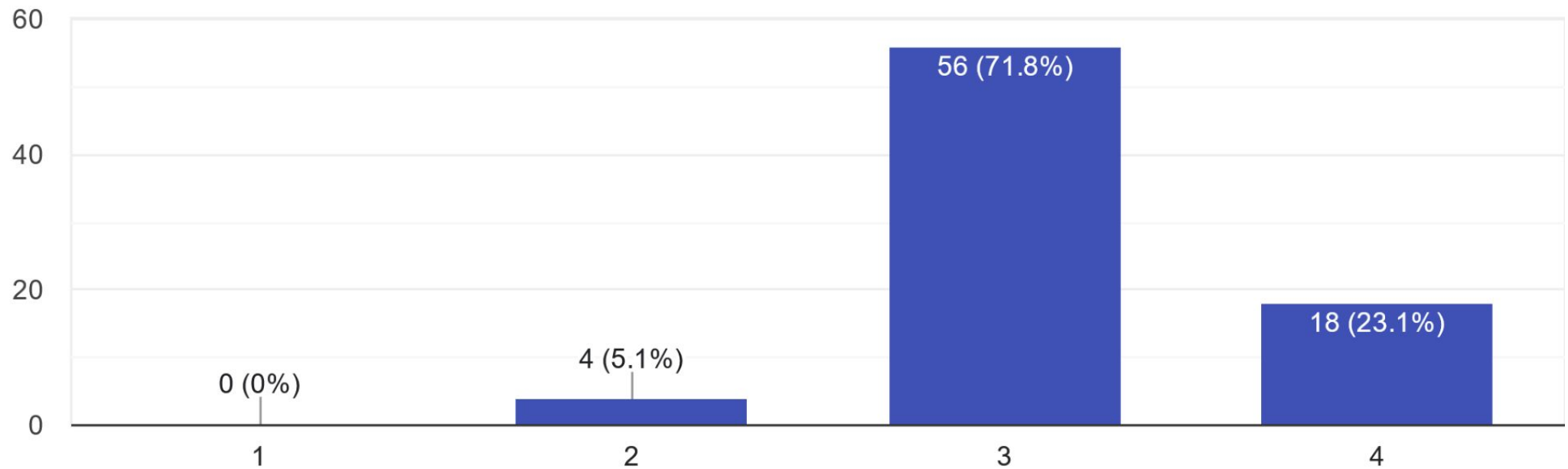
静的解析、DFIRを解いてる人の回答が多い



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？

78 件の回答



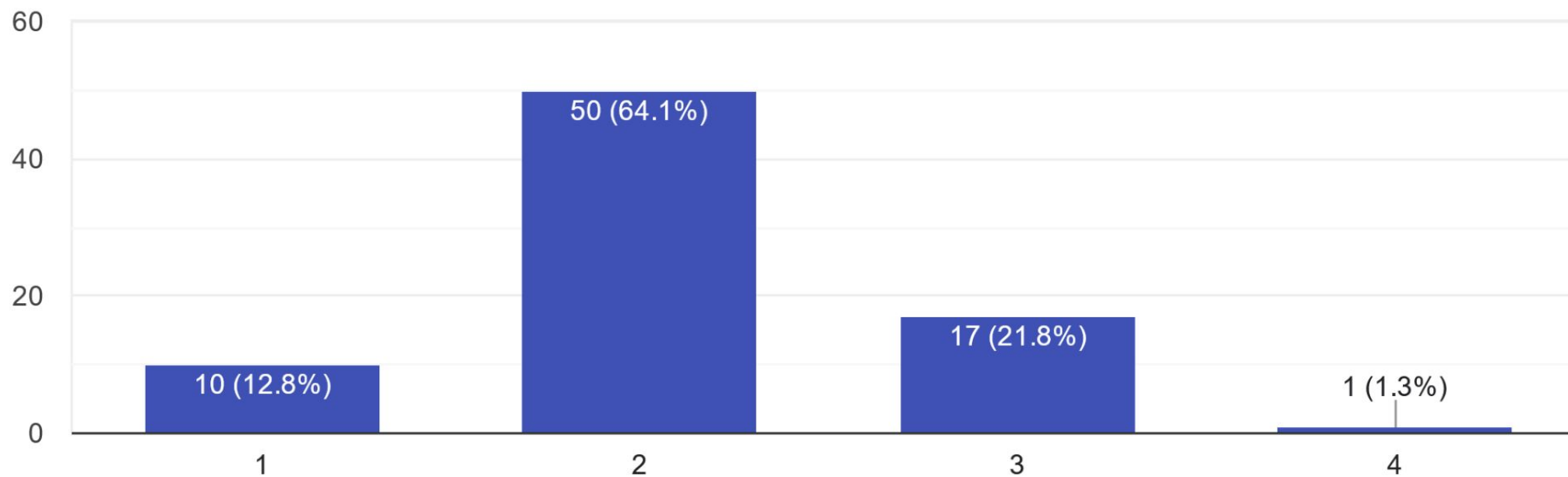
ちょっと難しい？



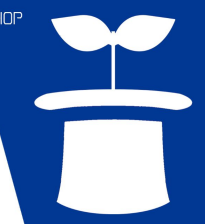
競技時間

MWS Cup の競技時間はどうでしたか？

78 件の回答



ちょっと短い？

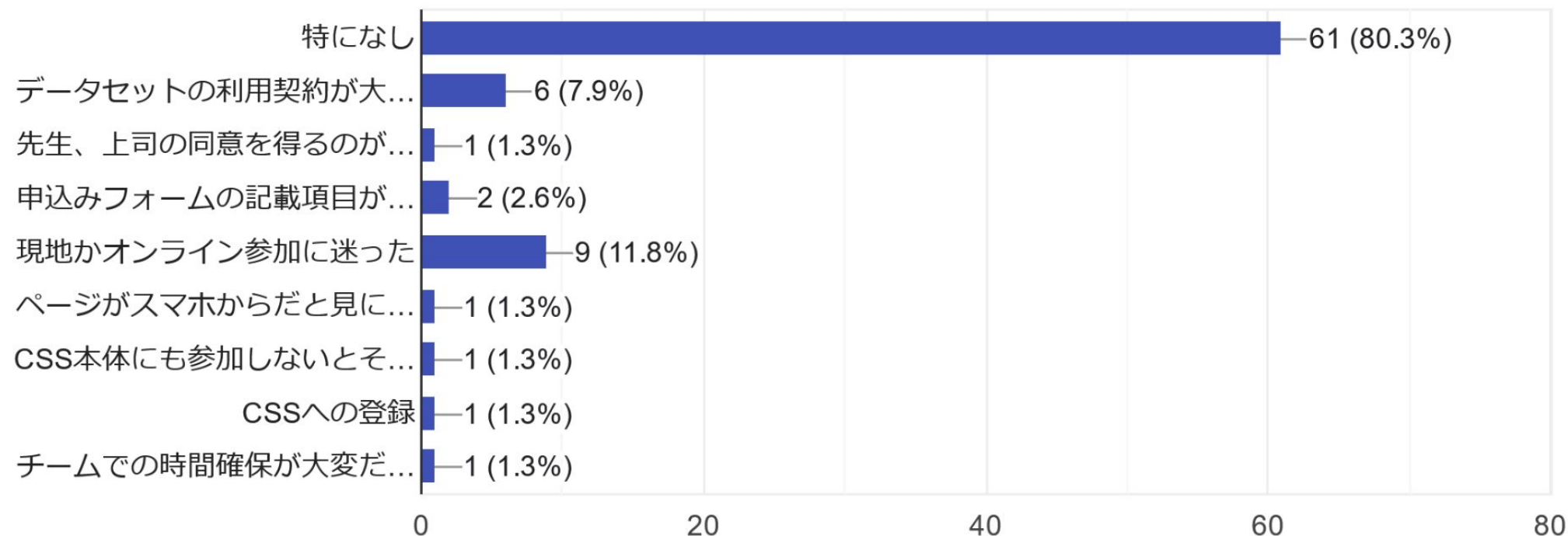


申込みの障壁は？

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せんか？あれば教えてください。

76 件の回答





オンライン/会場について

現地会場について

- 例年通り、十分な競技スペースを確保していただいたので、満足しております。
- 電源タップや机等環境が整備されていて良かったと感じました。
- チームの立て札やMWSCup終了後に現地参加者で写真撮影があり記念になった
- 現地参加をすることで、様々な人との交流をすることができて大変良かった。来年以降もこの形式を続けてほしい。
- 会場のwifiが繋がりにくかった
- 現地参加枠にもう少し余裕があるとうれしかった
- 現地参加ができない場合の連絡がもう少し早いと助かります。

オンライン会場について

- 会場のキャパシティ以上の人数が参加できる点がよかった。
- 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 Cup の全体への意見や感想

- 初めての参加でしたが、取り組むべき内容やヒントが提示されたおかげで勉強しやすいと感じました。
- 学生のためにこのような勉強の場を用意していただき、とても有難いです。MWS Cupをきっかけにして、各種ツールの使い方や実際の解析の流れを踏まえて勉強を進めることができ、非常に有意義でした。特に作問が良質であり、学生が取り組みにくい部分をうまく補助しつつも、解いたときに「面白い！」と思えるような骨のある問題セットが印象的でした。
- 解析を実際にできたことはCTFとはまた違った視点で考えることができた。また、解説をすぐに聞けることで理解が良く深まったと感じた。
- トラブルとはいえ会場のWiFiが使えなかったのが不便でした。



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の開催形態に関わらず
- ・ 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
 - ・ ただし、会場ネットワークに依存しすぎない運用を検討
- ・ 事前に出したヒントは好評だったので、事前勉強しやすいように今後も可能な範囲で出したい
- ・ MWSのスコープ拡大によっては、MWS Cup の課題も変更を検討
 - ・ ディフェンシブな課題が多いため、オフエンシブな課題を検討したい
- ・ **作問にご協力いただける方募集中**
 - ・ **@桑原翼_FFRI までご連絡ください**