



MWS Cup 2019振り返り (事前課題, 他)

2019/12/09 (月)

MWS2019 実行/企画委員会

MWS Cup 2019



今年は総勢 15 チーム 83 名が参加！

事前課題は2ヶ月間、当日課題は3時間取り組んでももらいました

0

事前課題：MWSにとって有意義なデータセットやツールを検討・作成せよ！

1

当日課題1：悪性トラフィックデータ・クライアントログを分析せよ！

2

当日課題2：マルウェア (RAT) を静的解析せよ！

3

当日課題3：マルウェア表層解析ログを分析・分類せよ！





MWS Cup 2019 結果

MWS

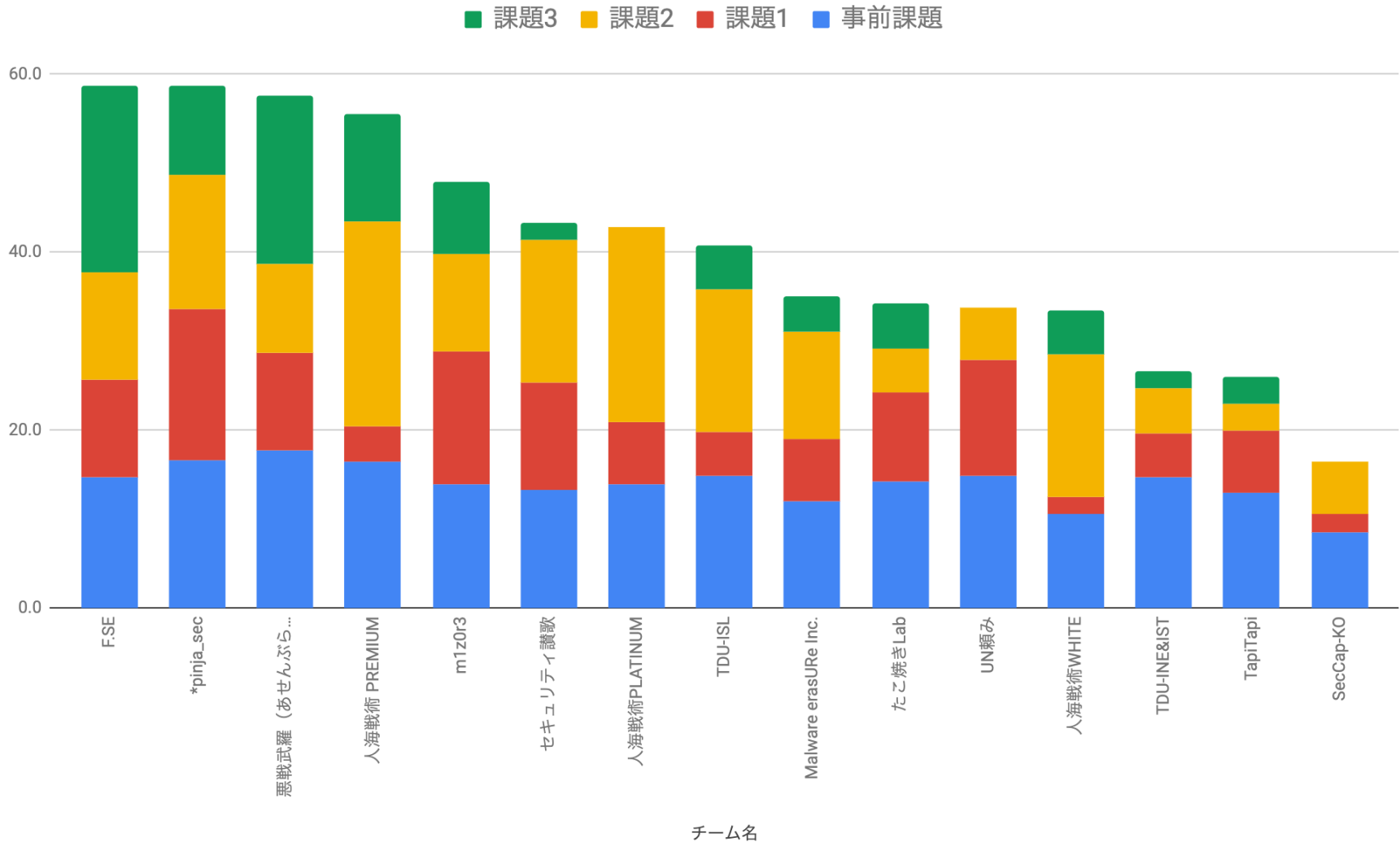
順位	チーム名	事前課題	当日課題1	当日課題2	当日課題3	当日課題合計	総合得点
1	F.SE	14.7	11.0	12.0	21.0	44.0	58.7
2	*pinja_sec	16.7	17.0	15.0	10.0	42.0	58.7*
3	悪戦武羅（あせんぶら）	17.7	11.0	10.0	19.0	40.0	57.7
4	人海戦術 PREMIUM	16.5	4.0	23.0	12.0	39.0	55.5
5	m1z0r3	13.8	15.0	11.0	8.0	34.0	47.8
6	セキュリティ讃歌	13.3	12.0	16.0	2.0	30.0	43.3
7	人海戦術PLATINUM	13.8	7.0	22.0	0.0	29.0	42.8
8	TDU-ISL	14.8	5.0	16.0	5.0	26.0	40.8
9	Malware erasURe Inc.	12.0	7.0	12.0	4.0	23.0	35.0
10	たこ焼きLab	14.2	10.0	5.0	5.0	20.0	34.2
11	UN頼み	14.8	13.0	6.0	0.0	19.0	33.8
12	人海戦術WHITE	10.5	2.0	16.0	5.0	23.0	33.5
13	TDU-INE&IST	14.7	5.0	5.0	2.0	12.0	26.7
14	TapiTapi	13.0	7.0	3.0	3.0	13.0	26.0
15	SecCap-KO	8.5	2.0	6.0	0.0	8.0	16.5

* 当日課題合計点数の高いほうが上位ルールのため



MWS Cup 2019 結果

合計得点



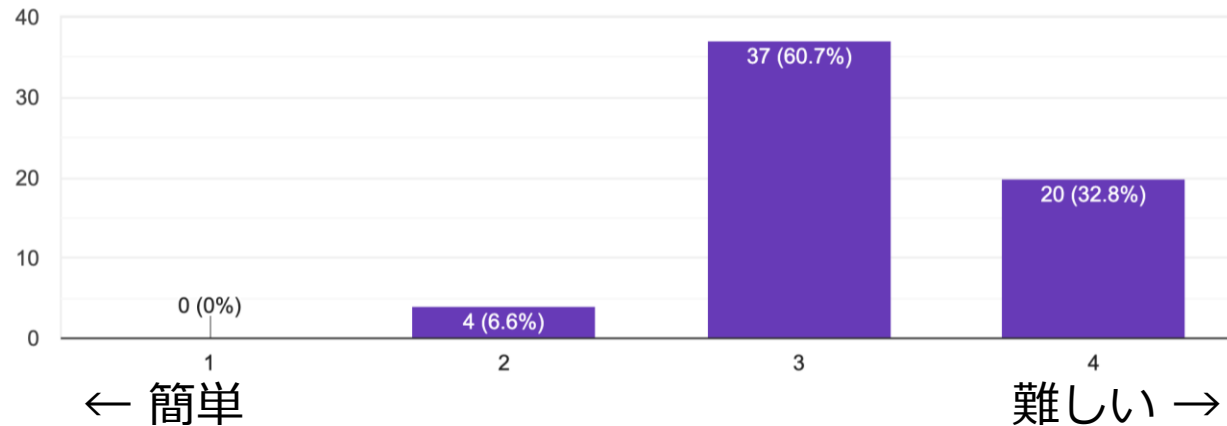


全体に対するアンケート結果MWS

- 今年はチーム単位ではなく、**個人単位**でアンケートを実施

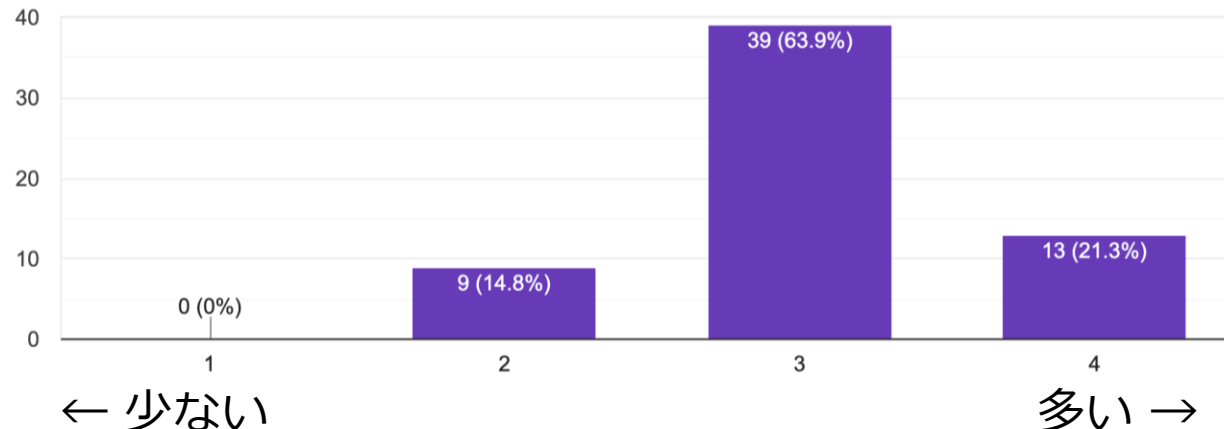
MWS Cup の課題の難易度は全体的にどうでしたか？

61 件の回答



MWS Cup の課題分量はどうでしたか？

61 件の回答



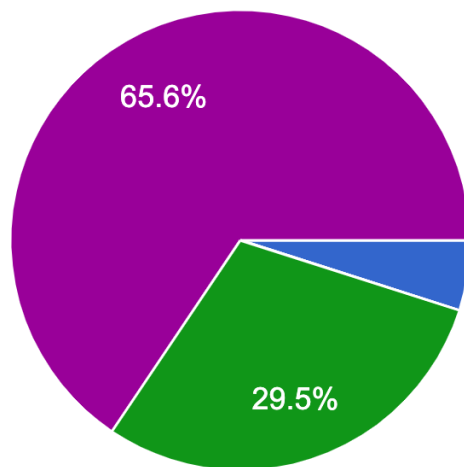


全体に対するアンケート結果

- 来年度のMWS Cup課題作成に協力・・・
 - します！（課題１：DFIR）：**3人！**
 - しろと言われればするかも？：**18人！**

来年度のMWS Cup課題作成に協力・・・

61 件の回答



- します！（課題１：DFIR）
- します！（課題２：静的解析）
- します！（課題３：表層解析）
- しろと言われればするかも？
- しません。。。



事前課題の紹介

- **2017年、2018年に続き、自由課題！**
 - 今年は7/1～9/30の2ヶ月間の取り組み期間を用意
- **条件は以下の通り**
 1. サイバーセキュリティに関連する研究開発/実務/教育等（≡ MWS コミュニティ）において、有意義（コミュニティを活性化させる、第三者が使いたい/欲しいと思う、等）だと思う**データセットやツール等を検討**すること。
 2. MWS コミュニティへ共有できる成果物を生み出すこと。
 3. 成果物は、参加チームが所有する GitHub や Google Drive 等を用いて保存し、その URL を回答すること。
- **参考資料**
 - 過去の事前課題の内容や振り返り資料は、下記にて掲載中
 - <https://www.iwsec.org/mws/mwscup.html>
 - 過去の成果物や発表スライドはMWSDatasetsにも含まれています。



MWS Cup 2019 事前課題

MWS

MWS Cup 2019 事前課題

2019/7/1 (月) に公開 × ⋮

本事前課題は自由課題 (自由研究) であり、必須事項は以下の3点です。

1. サイバーセキュリティに関連する研究開発/実務/教育等 (≒ MWS コミュニティ) において、有意義 (コミュニティを活性化させる、第三者が使いたい/欲しいと思う、等) だと思うデータセットやツール等を検討すること。
2. 1の検討において、MWS コミュニティへ共有できる成果物を生み出すこと。
3. 2の成果物は、参加チームが所有する GitHub 等のソースコードホスティングサービスアカウントや Google Drive 等のストレージサービスアカウントを用いて保存し、その URL を回答すること。

なお、評価は、以下の評価基準に基づき審査委員による採点が行われます。

- ・新規性 = 今までに無い成果か、新しい課題設定か、等
- ・実用性 = 誰でもすぐ使えるか、現存する脅威やデータに効果的か、等
- ・プレゼンテーション = 成果のアピールが必要十分に行えているか、起承転結ロジカルな説明か、ハキハキ大きな声で落ち着いて発表してるか、等

その他、当日のプレゼンセッション聴講者による投票結果に比例した追加点も検討しております。

事前課題の取り組み期間は、参加登録日から *** 2019年9月30日 (月) 23:59 JST まで *** とし、

*** 各チームの課題取り組み内容を MWS 会期中にプレゼンしていただきます。 ***

「何をしたら良いか分からない」「どのような内容が評価されるのか分からない」といった疑問を持った参加者の方々は、Web に掲載している参考資料 (<https://www.iwsec.org/mws/mwscup.html>) や MWS Slack の #mwscup チャンネルでも質疑応答をベストエフォートで受け付けておりますので、気軽にご活用ください。なお、過去の各チームの成果物や発表スライドは MWSDatasets に含まれております。



事前課題の成果物

チーム名	種類	成果物のタイトル
TDU-INE&IST	新規ツールの作成	JavaScript難読化解除ツール
悪戦武羅（あせんぶら）	新規ツールの作成	NTFS-EA-operation-library
TDU-ISL	新規ツールの作成	cuckoo-vm
たこ焼きLab	新規ツールの作成	Soliton Dataset 解析支援ツール 2019
SecCap-KO	新規ツールの作成	通信の暗号化に使われている共通鍵を推測するツール
*pinja_sec	新規ツールの作成	BINARY PINJA
F.SE	新規ツールの作成	Intelligent Blocker
人海戦術PLATINUM	新規ツールの作成	データセット活用支援ツール
人海戦術 PREMIUM	新規ツールの作成	JFAP(JINKAI Forensics Analyzer PREMIUM)
Malware erasURe Inc.	新規ツールの作成	SEdetector
UN頼み	既存ツールの改良	opticle
セキュリティ讃歌	既存ツールの改良	DyNa
TapiTapi	既存ツールの改良	CTFdの改良
人海戦術WHITE	データセットの作成	Jinkai White Dataset 2019
m1z0r3	その他	Tokyo2020 Domain Gazer

事前課題の感想

漠然としたルールだと感じているのですが、一方で**他チームの成果物が想像つかない分発表を含めて楽しく聞くことができました**。来年も事前課題のシステムを継続していただけると幸いです。

事前課題の作成がチャレンジですが楽しかった、**みんなのアイデア、知識が必要で、非常に勉強になりました**。

普段は自身の興味を研究のモチベーションとしていたため、成果物の検討に当たって**コミュニティへの貢献という視点を求められたのが新鮮であり有意義だった**と感じます。

それなりに意義のあるものをチームでしっかり協力して作成することができ、**みんなの仲も深まり非常にやってよかったです**。

事前課題に対して、**現場の意見やプロの方たちの不満点などの情報がまったくなく、その成果物が本当に有意義であるかどうかであるかの判断が本番にならないとわからない**というのが現状でした。Slackがあるので、事前準備の段階でアイデアを出し、そのアイデアに対してオープンな場所でのフィードバックがもらえる環境などがあると、より良いと感じました。

MWSコミュニティへ「共有できる成果物」を生み出すとのことでしたが、**MWSコミュニティで必要とされているツールやシステムに関する議論の公開情報が少なく、テーマを決める点では難しかったです**。作成した成果物については「他人に定量的に評価してもらえる」場が少ないと思ったため、中間発表のような場があればフィードバックをうまく生かした成果物ができたのではと思いました。

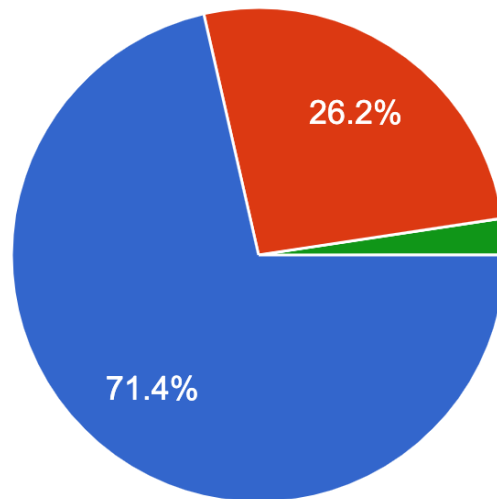
有意義なものとは何かの解を出すのが難しかった。各チームの事前課題に対するコメントを公開すれば、次の年のチームが有意義なものを作るのに参考になると思った。



事前課題の感想

事前課題で最も大変だったのはどの条件・過程ですか？

42 件の回答



- 1. サイバーセキュリティに関連する研究開発/実務/教育等において、「有意義」だと思うデータセットやツール等を検...
- 2. MWS コミュニティへ「共有できる成果物」を生み出すこと。
- 3. 成果物は、参加チームが所有する「GitHub や Google Drive 等を用いて保存し、その URL を回答する」こと。
- 6分のプレゼン時間でいかにアピールするかを考えるのが大変でした。



その他共有事項

- **事前課題の成果物は公開しないんですか？**
 - します。MWS Datasets にも同梱されます。
 - <https://docs.google.com/spreadsheets/d/1XohwngzstgMRgeEtP89vD2OWRomw58efWqhsQtg9Hmg/>
- **当日課題の模範解答がほしい。**
 - 後日 Web サイトに公開します。
- **Web サイト**
 - MWS トップページ; <https://www.iwsec.org/mws/index.html>
 - MWS Cup ページ; <https://www.iwsec.org/mws/mwscup.html>
 - MWS データセット利用実績ページ;
<https://www.iwsec.org/mws/achievements.html>