

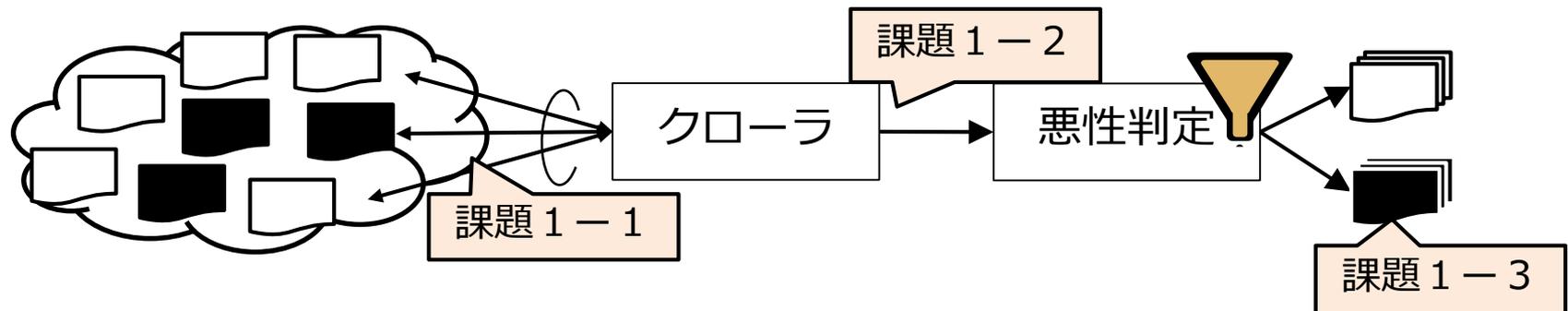
MWS 2016 ポストイベント MWS Cup 課題1 振り返り

MWS 2016 企画委員, 課題作成委員
高田 雄太、市田達也、小寺博和
2016年12月7日

課題 1 は事前準備として出題

• 改ざんされたウェブサイトを発見せよ！

- 課題 1 - 1 : 改ざんサイトを発見するため、「巡回先 URL の選定方法」および「改ざんサイトの検知方法」を述べよ。
- 課題 1 - 2 : 改ざんサイト発見のためのプログラムを提出し、解析の工夫点を含めて「自動化した箇所」「手動の箇所」を説明せよ。
- 課題 1 - 3 : 発見した改ざんサイトについて、観測できる情報や外部情報等を活用し、改ざん攻撃の原因を推測せよ。



- 「改ざんサイトの発見～検知～分析」について、約 1 ヶ月の取り組み期間を設けて取り組んでもらった。

昨年の課題との関係

- 「改ざんされたウェブサイトの発見」という
課題の方針は昨年と同じ*
 - 課題に継続性を持たせることで、**回答の質向上を狙う**
 - 昨年のポストイベントにおける解説資料や
ウェブサイト改ざんに関する各種資料も同時に展開
 - 昨年のMWS Cupをきっかけに研究をスタートさせ、
研究成果の**MWS2016 発表&MWS Cup 活用を期待**
 - そんな素敵なチームが**1チーム存在!**

[*] MWS Cup 2015 課題1 振り返り

http://www.iwsec.org/mws/2015/mws20160114_takata_cup1.pdf

出題の意図

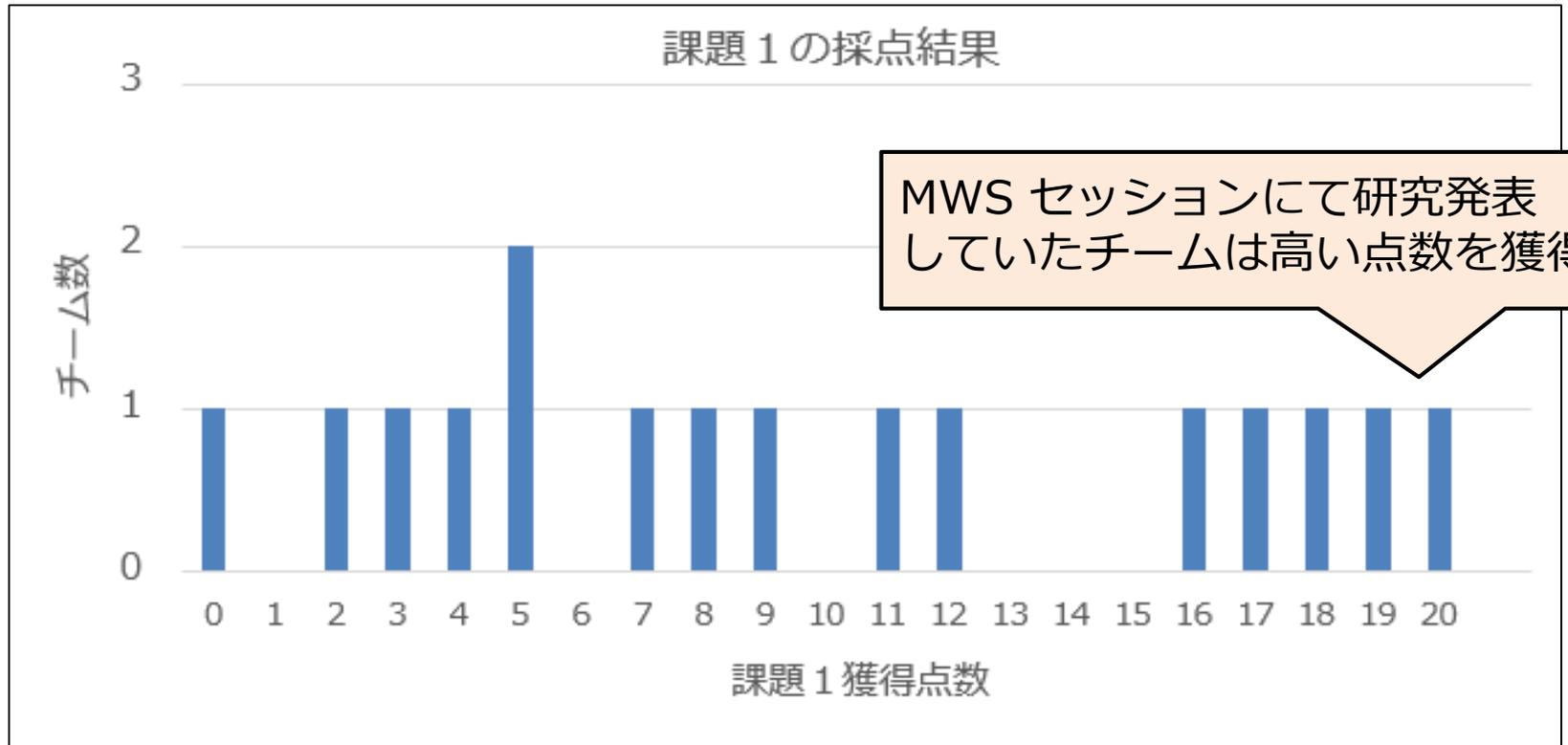
- 答えの定まらない課題への取り組みを通じて、
「考える力, 仮説検証の力, 実験評価の力」
のさらなる向上を推進
 - MWS の主目的は「研究人材の育成」
- **学術的な手法 + 実用的な手法**
 - 攻撃の本質を見極め理解し、
実用に耐え得る技術力・実践的な現場力を養成
 - ウェブ巡回&解析ツールの作成と
MWS コミュニティへの共有を徹底

採点の基準

- **回答内容が技術的に合っているか？**
 - 目的と手法は一致しているか
- **面白い観点で解析しているか？**
 - 仮定に基づき新しいアプローチを考えているか
 - 手法に工夫を凝らしているか
- **課題取り組みへの努力が見られるか？**
 - 新しい知見や技術を獲得しているか

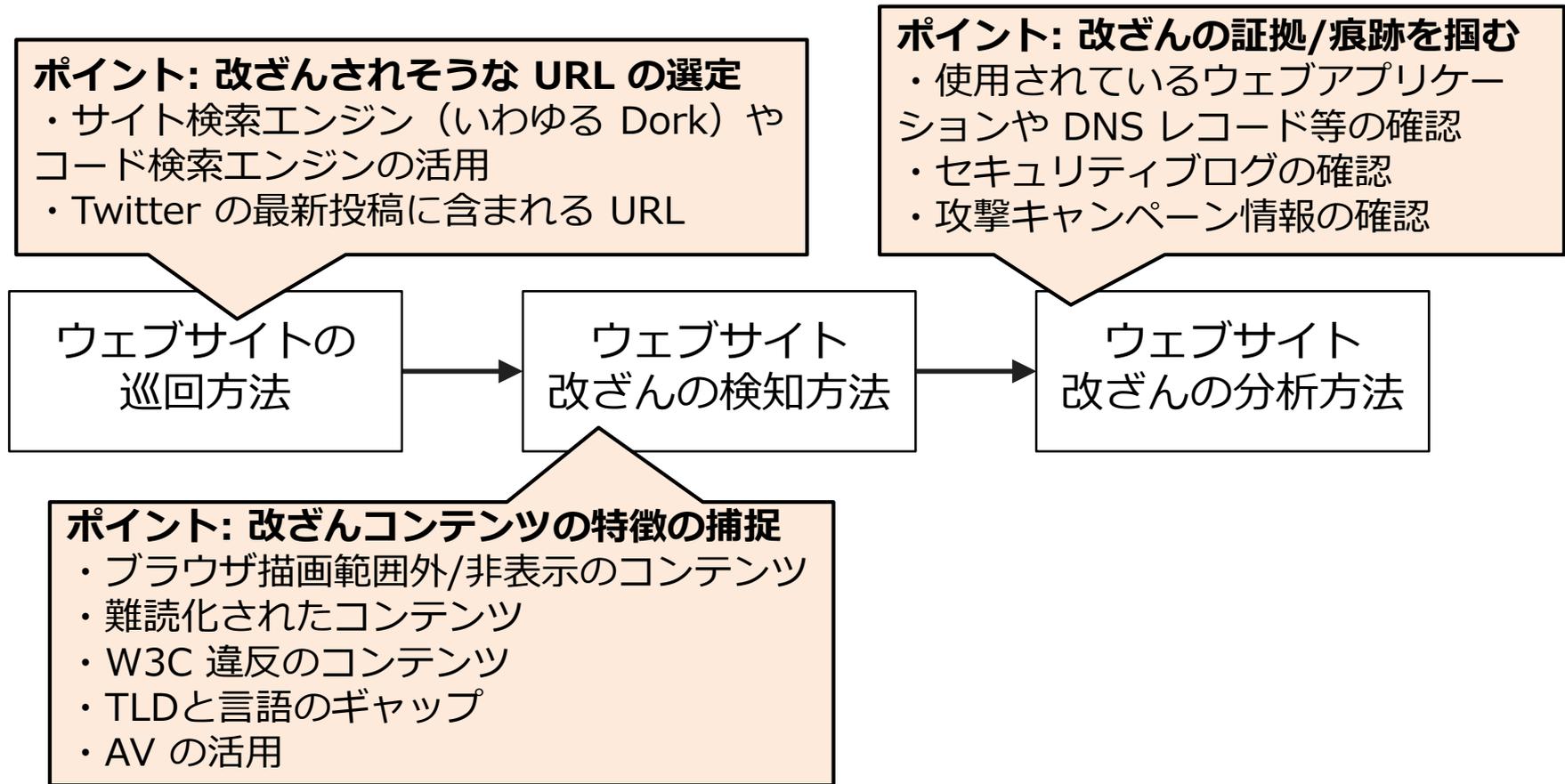
採点の結果

- 点数は偏ることなくバラバラ。
- 回答日に応じた加点は特に効果がなく、どのチームも期限ギリギリに回答。



回答の紹介

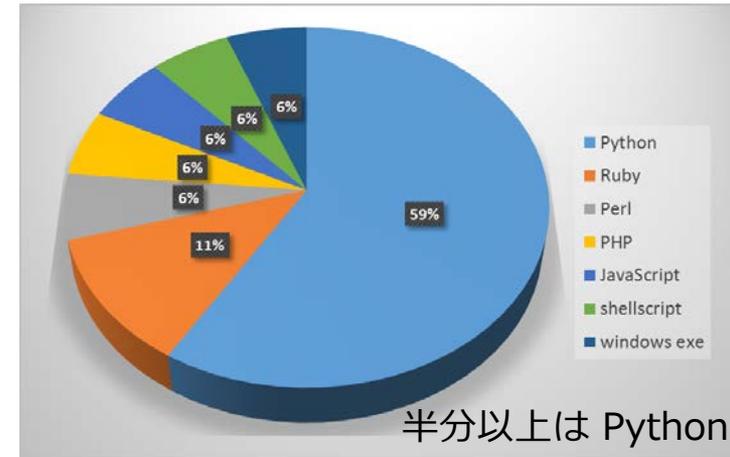
• 各チームのアプローチを一部抜粋



今後に向けて

• 発表資料/ツールの共有

- 発表資料: 7/16 チーム
- ツール: 3/16 チーム
 - 自らコードを GitHub に公開する能動的なチームも!



• 悪性データの共有

- 提出された悪性 pcap データ : 10/16 チーム
 - 参考になるデータは、**MWSDatasests2017**として提供
- MWS 参加者が自立してデータ収集できるよう、その基盤作りのきっかけを MWS Cup の場で提供し続けていきたい。
 - i.e., 「データセット収集そのもの」に関する研究を推進

さいごに

- 市田様、小寺様、MWS Cup 2016 課題 1 の作成にご協力いただき、誠にありがとうございます。
- 来年の課題作成担当者／協力者を早速募集
 - 来年はさすがに別の課題？
 - MWS Cup 2016 上位チームへの協力依頼 + 公募