

MWS



MWS Cup 2026 について

**MWS Cup 2026 委員長
株式会社 F F R I セキュリティ**

桑原 翼



目次

- MWS Cup とは？
- 出題課題（予定）
- LLM 利用について
- 事前学習の参考資料
- 表彰・参加賞
- 開催形態
- 参加人数・スケジュール
- 参加方法
- 運営メンバーの募集



MWS Cup とは？

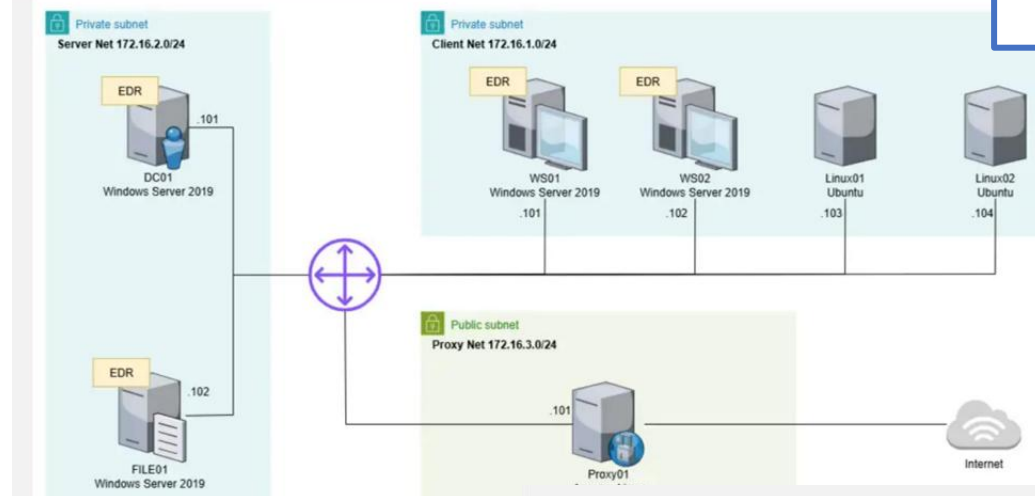
- MWSで2009年から開催されているセキュリティコンテスト
- サイバー攻撃の解析技術を競う
- 目的
 - 参加者同士が切磋琢磨することでサイバー攻撃解析に係る技術を向上
 - 実践的なサイバー攻撃解析技術を習得する場を提供
 - 研究用データセットの活用促進
- リアルなサイバー攻撃・マルウェア検体を題材にした実践的な課題を出題





実践的な課題を提供

イーデンカレッジのIT環境構成図



実際に環境を構築し収集した
ログを用いて課題提供

実際のマルウェアを静的解析

1-3. APIの構造体

- 0x210, 0x160, 0x290を探すと、それぞれ0xe, 0x3, 0xb
- 難読化解除すると答えは「CreateProcessW, ReadFile, Sleep

CreateProcessW

```
168     else if (uVar7 == 0xe) {
        *(longlong *) (param_1 + 0x210) = lVar4;
    }
```

```
40  local_228[0xe] = "GpeaveRpsgeWw[";
```

ReadFile

```
135     else if (uVar7 == 3) {
        *(longlong *) (param_1 + 0x160) = lVar4;
    }
```

```
29  local_228[3] = "PeafDine";
```

Sleep

```
157     else if (uVar7 == 0xb) {
        *(longlong *) (param_1 + 0x290) = lVar4;
    }
```

```
37  local_228[0xb] = "Wneer";
```

すべての攻撃が成功するわけじゃない

攻撃者も最初からターゲット環境のすべてを把握して行動しているわけではない
探索->実行->失敗->探索->実行->失敗->...->実行->成功
こういった試行錯誤をしてターゲット環境を侵害し、目標達成を目指している

実務から見える実情を
課題に反映



今年は失敗したコマンドも多い



出題課題（予定）



ハッカソン（事前課題）

- マルウェア解析やサイバー攻撃対策のツールやデータセットを開発する



静的解析

- マルウェアを静的解析して挙動を明らかにする



表層解析

- ファイルの特徴とOSINTを活用して脅威の有無や動作を推定する



DFIR + Offensive

- ログを解析し、オフenseンシブ視点を交えつつインシデントを明らかにする



出題課題（予定）



ハッカソン（事前課題）

- マルウェア解析やサイバー攻撃対策のツールやデータセットを開発する



静的解析

- マルウェアを静的解析して挙動を明らかにする



表

- 審査基準範囲外の優れた部分がある場合に特別賞として加点を検討中
審査基準含めた詳細は MWS-Slack でアナウンス予定

活用して有無の有無や動作を推定する



エンジン
エンジンデ
ポイントを明らかにする



昨年の変更点は継続予定

- **表層解析（マルウェア分類）課題**
 - 課題の範囲を広げマルウェア分類だけでなく、表層解析全般（ツールの使い方、OSINT収集、マルウェア分類など）を出題予定
 - Kaggleは使用せず、当日課題のみ
- **DFIR + Offensive（DFIR）課題**
 - Offensive視点の問題を追加予定
- **現地参加**
 - 現地参加を希望するチームのうち、応募順で現地参加を決定し、可否を早めにご連絡
 - 後述の参加手続きをすべて実施されていないチームの方には、現地参加をご遠慮いただく可能性があります
- **ポスター**
 - MWS Cupのポスターを作成検討中
- **参加賞**
 - 参加賞として缶バッジ等を検討中
 - 配布は現地で行う予定です、MWS Cupに現地参加できない方も、CSS自体にはぜひ現地参加を！



LLM 利用について

- MWS Cup 2026 の AI の利用方針は以下を予定
 - 作問はまだまだこれからなので、変更する可能性は十分にあります
 - 変更点あれば MWS-Slack にてアナウンスします

課題	利用可否
ハッカソン	利用可能
DFIR + Offensive	利用可能 - 詳細は MWS-Slack 上の資料をご参照ください。（本日中午に Up します）
表層解析	利用不可 - MWS は人材育成ワークショップなので人材育成という観点を大事にします - 実務でも多くの場面で LLM を利用するが、ここでは LLM の使い方ではなく解析に必要な知識とその方法を課題を通して学んでほしいと考えています - MWS Cup で学んだことを糧に、研究や実務で LLM の出力を検証し理解するための能力を獲得いただきたいです
静的解析	



事前学習の参考資料

- 以下の資料が特に参考になります
 - MWS Cup の過去問: Dataset + <https://www.iwsec.org/mws/mwscup.html>
 - 2024 年優勝チームの「MWS Cup での取り組みについて」：
https://www.iwsec.org/mws/2024/files/MWS2024_post_Cup2024_undano_mi.pdf

スケジュール

6月 アイデア出し

ハッカソンや事前学習の
スケジュール

7月 PoC実施・再度アイデア出し&PoC

最後の1ヶ月はラストスパート！
技術班と非技術班に分かれ、スクラム開発の手法を
取り入れて開発

8月 テ

9月 アジャイル開発

本番

MWS Cup 当日の取り込み方

コミュニケーションを大切に

- 「全員が同じ情報を知っている」状態にすることを意識
- 問題ごとに手分けするのではなく、全員で同じ問題を解く

時間配分を考えて問題をトリアージする

- まずは全問眺めてから、解けそうな問題から解く
- スタックしそうな問題は、考えるタイムリミットを設ける



表彰・参加賞

- ・ **表彰を予定している賞**

- ・ 総合優勝
- ・ 総合準優勝
- ・ ハッカソン部門優勝
- ・ 静的解析部門優勝
- ・ 表層解析部門優勝
- ・ DFIR + Offensive部門優勝

- ・ **参加賞**

- ・ 参加賞として缶バッジ等を検討中
- ・ 配布は現地で行う予定です、MWS Cupに現地参加できない方も、CSS自体にはぜひ現地参加を！



副賞の紹介 (2025年)

- ・ **副賞 (2025年の実績)**
 - ・ 総合優勝、準優勝チームメンバーにオリジナルTシャツ
 - ・ 各部門優勝チームに出題者チームが選んだ技術書1冊
 - ・ 下表が 2025 年に贈呈した書籍

部門優勝	書籍
ハッカソン部門優勝	ソフトウェア開発現場の「失敗」集めてみた。42の失敗事例で学ぶチーム開発のうまい進めかた
静的解析部門優勝	Linuxカーネルプログラミング 第2版
表層解析部門優勝	データ分析に必須の知識・考え方 認知バイアス入門
DFIR部門優勝	実践サイバーセキュリティ入門講座 現場に残された痕跡からハッカーの攻撃を暴け



受賞チームへのお願い

- **発表協力をお願い**
 - 受賞チームのうち 1~2 チームに、MWS ポストミーティングでの発表をご依頼予定
- **発表内容**
 - 事前学習や当日の取り組み・工夫について共有いただく想定
 - 部門優勝チームには、受賞課題分のみご依頼予定
- **Write Up 歓迎**
 - 全チームからの Write Up などの共有も大歓迎



参加人数・スケジュール

- ・ **参加人数**

- ・ 1チーム最大6名まで
- ・ 1名でも参加可能

- ・ **競技期間・時間**

- ・ 一部の課題では事前に提出いただく予定
- ・ 当日の日程・競技時間は未定

- ・ **補足**

- ・ **事前に課題いただく課題が未提出でも当日課題に挑戦可能**
- ・ 当日、すべての課題に取り組みなくて問題ありません



開催形態

- ・ **オンラインとオフラインのハイブリッド開催を予定**
 - ・ CSS 2026の開催形式に合わせる形
 - ・ CSS の Zoom および MWS の Slack を利用予定
 - ・ MWS Cup 参加申込にて オンライン / 現地参加 の希望を選択
- ・ **現地参加の注意点**
 - ・ 会場ネットワークは有線 LAN の配備を検討中
 - ・ 各チームに 6 ポート以上準備
 - ・ LAN ケーブル（必要な人は Type-C との変換ケーブル）を持参ください
 - ・ 現地参加の部屋が定員に達した場合、オンライン参加に変更をお願いする可能性あります
 - ・ 早めにご連絡できるようにいたします



参加方法（重要）

1. **Slack-MWS 参加（無料）**
 - a. https://www.iwsec.org/mws/mws_ml.html
2. **MWSデータセット利用手続き（無料）**
 - a. 研究責任者（大学教員、企業人）による申請
 - b. 「4. MWS Cup 2026 参加登録」にて登録状況を確認し、未登録のチームには個別で利用手続きをご案内予定
3. **CSS 2026 参加登録（有料）**
4. **MWS Cup 2026 参加登録**
 - a. Slack-MWS にてアナウンス



運営メンバー募集

- 自分の経験を次の世代に還元したい方
- 運営メンバー（大会運営準備、Webサイト作成、広報活動 など）
 - セキュリティ関連の研究をしている学生を応援したり、交流したい方
- 静的解析問題作問
 - 業務や趣味でマルウェア解析をゴリゴリやってる方
- 表層解析問題作問
 - ファイルの特徴やOSINT等を利用して脅威を解析する問題の作問をしてみたい方
- DFIR + Offensive問題作問
 - リアルなフォレンジック業務や攻撃手法に精通している方
 - 様々な攻撃ツールを検証してみたい方

興味がある方は、[MWS Slack @桑原翼_FFRI](#) または [@Akitada Omagari](#) までDMでご連絡ください