MWS Cup 2024 Post Meeting

MWS Cupでの取り組みについて

UN頼み

篠崎佑馬[1]　渡邉祐貴[1]　小林颯大[1]　松元優斗[1]　首藤朗[1]　松本悠希[2]

[1] 電気通信大学　[2] エヌ・ティ・ティ・コミュニケーションズ株式会社

チーム紹介

チーム紹介

UN頼みチーム

- 電気通信大学(UEC) + NTT コミュニケーションズ 株式会社
- チームメンバーは毎年入れ替わる

今年のチーム構成

- 篠崎佑馬（電通大 修士2年、出場3回目、チームリーダー）
- 渡邉祐貴（電通大 修士2年、出場2回目）
- 小林颯大（電通大 修士1年、出場2回目）
- 松元優斗（電通大 修士1年、初出場）
- 首藤　朗（電通大 学部4年、初出場）
- 松本悠希（NTT コミュニケーションズ）

全体を通して

全体を通して

今年の活動期間

- 2024年6月～2024年12月

チーム全体としての活動

- 週1回の全体ミーティング

マインド

- 絶対優勝するぞ！という気概
- ~~例年先輩がいい成績を取っているプレッシャー~~
- セキュリティのスペシャリストとしても成長したい

役割分担

ハッカソン課題

ゲームアイディア: 首藤
シナリオ: 篠崎、渡邉、小林
実装: 松元、首藤
レビュー: 松本

マルウェア分類

モデル設計: 松元、小林
特徴量作成: 首藤
データ分析: 篠崎、渡邉、首藤

静的解析

篠崎、松元、首藤

DFIR

渡邉、小林、松本

ハッカソン課題

スケジュール

6月 アイデア出し開始

7月 PoC実施・再度アイデア出し&PoC

8月 テーマ決定・仕様策定・基本設計

9月 アジャイル開発

スケジュール

6月 アイデア出し開始

提出3ヶ月前から始動！

7月 PoC実施・再度アイデア出し&PoC

8月 テーマ決定・仕様策定・基本設計

9月 アジャイル開発

スケジュール

6月　アイデア出し開始

7月　PoC実施・再度アイデア出し&PoC

8月　テー

9月　アジャイル開発

6月に出したアイデアのPoCを実施
結果、全てのアイデアがボツに！
再度アイデアを出し直し！

スケジュール

6月　アイデア出し開始

7月　PoC実施・再度アイデア出し&PoC

8月　テーマ決定・仕様策定・基本設計

9月　ア

テーマがMWS Questに決定！
大まかに、ゲームの流れ・シナリオ・画面デザイン等を決める

スケジュール

6月　アイデア出し開始

7月　PoC実施・再度アイデア出し&PoC

8月　テ

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

9月　アジャイル開発

開発中(9月)の取り組み方

スプリントプランニング

1スプリント(1週間)で完了すべきタスク
(スプリントバックログ)を作成

GitHub issueと、GitHub Projectsの
カンバンボードを利用

実行

スプリントバックログを元に、
実装やシナリオ作成・デザインを進める

タスクの完了には2人以上の
レビューが必須

スプリントレトロスペクティブ

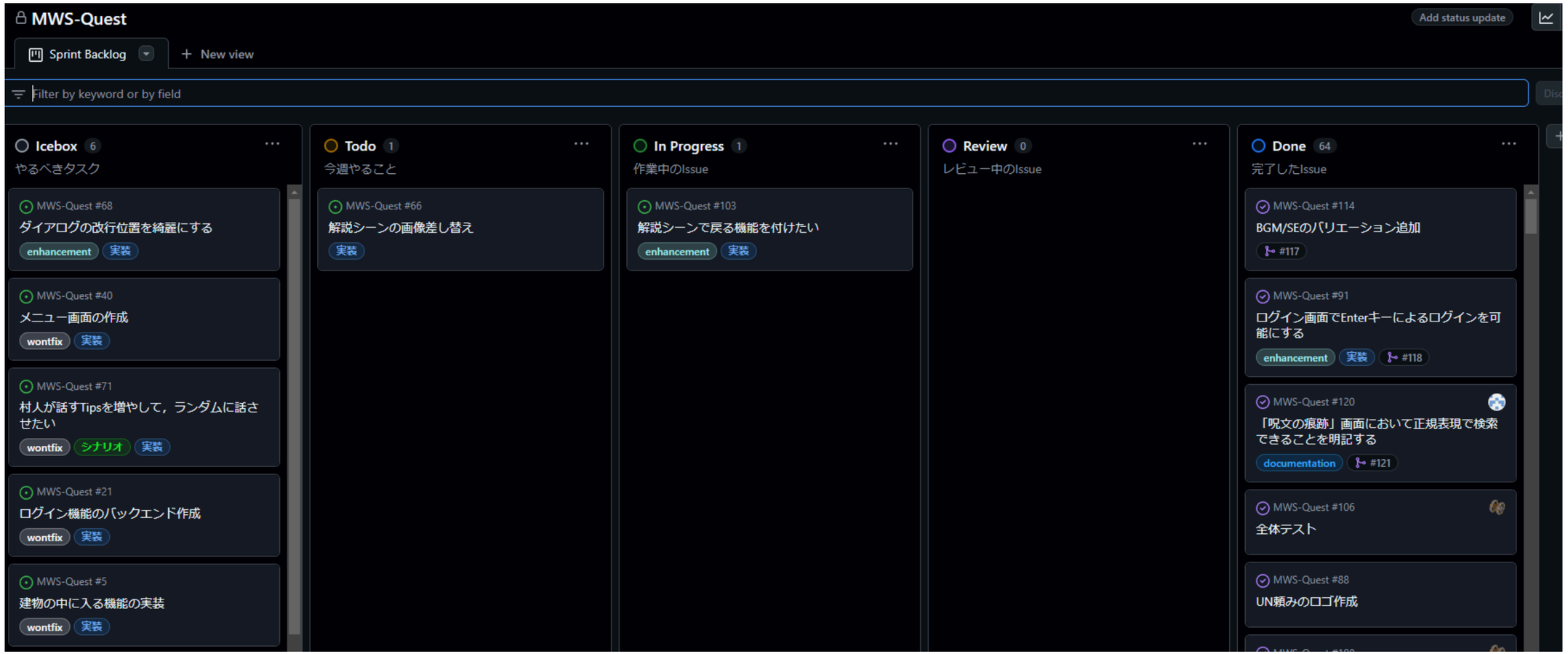
スプリント自体の振り返り
KPT法(Keep, Problem, Try)を利用

スプリントレビュー

スプリント期間中に達成した成果物や
進捗状況を共有

※実際のスクラム開発とは厳密には少し異なる

開発の様子



スプリントバックログの管理

開発の様子

レビューの様子

マルウェア分類課題

スケジュール

課題公開前

- 過去問や過去のKaggleを行いたかったが、多忙で実現できず...

課題公開後

- メンバー各々のやり方で課題に手をつける
  - 研究で機械学習をしているメンバーが主導
- 作業時はDiscordのボイスチャットに参加
- 実施内容はKaggle掲載のWriteupを参照

使用したサービス・ツール

- Git / GitHub
  - 作成したコードの管理 → **提出時の commit のルールづけ**
- uv
  - パッケージやバージョンの管理
  - pipより高速・高機能

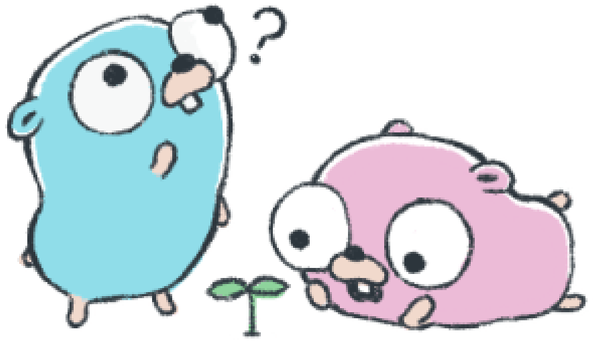
今後使用したいツール

- MLFlow
  - スコアやパラメータ、モデルの管理
  - 今回は Git だけで頑張っていたので、**MLOpsを強化したい**

静的解析課題

スケジュール

6月	Ghidra実践ガイドの輪講開始
9月後半	Ghidra実践ガイドの輪講終了 / ハッカソン課題に注力
10月	実践演習（過去問演習など）
10月23日	本番！



©tottie / Renée French

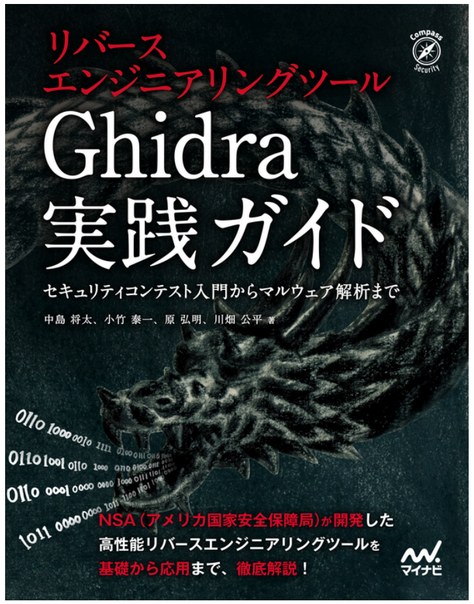
輪講

『Ghidra実践ガイド』を教科書として使用

- **ハンズオン形式**でマルウェア解析を学べる
- さまざまなバイナリ・シチュエーションに対応
- 5-5のGoバイナリに関しては、gotoolsの開発ストップのため **GolangAnalyzerExtension**を使用 → 本番でも使うことに

週に1回の輪読開催

- 1日0.5〜1章程度のペース
- 担当者が本を読みながら**手を動かし**解説
- 適当なタイミングで交代



※ 表紙画像は出版社の許諾を得て掲載しております。

過去問の有効活用

- 過去3年分の過去問を、**本番と同じ時間で解く**
- **時間配分**の感覚をしっかり身につける

©tottie / Renée French

自分でもバイナリをつくってみる

- Goバイナリは他のバイナリと比較して少し特殊なため、**コードとバイナリを照らし合わせて理解する**作業が必要だった
- FFRI様の技術ブログなどを活用

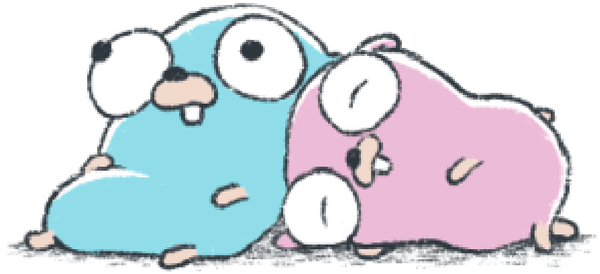
本番

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



©tottie / Renée French

DFIR課題

取り組み方

過去問演習

- 各自で**過去問**を解いて、**隔週の勉強会**で解き方を発表
- 直近2年分は担当メンバーが集まって、**本番と同じ環境**で演習

既存ツールの拡張

- 配布されたプロセスツリーに**機能追加**
- ログの読み取りを補助する**独自ツール**の作成

来年取り組みたいこと

- Hack The Box等で**攻撃手法を学習する**

結果

結果

ハッカソン課題

部門優勝

マルウェア分類

3位

静的解析

部門優勝

DFIR

部門優勝

結果

2連覇

総合優勝

終わりに

終わりに

非常に有意義で楽しいコンテストを開催いただき
ありがとうございました！

©tottie / Renée French