

MWS Cup 2024 Post Meeting

# MWS Cupでの取り組みについて



UN頼み

篠崎佑馬<sup>1</sup> 渡邊祐貴<sup>1</sup> 小林颯大<sup>1</sup> **松元優斗<sup>1</sup>** 首藤朗<sup>1</sup> 松本悠希<sup>2</sup>

<sup>1</sup> 電気通信大学 <sup>2</sup> 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

### 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)
- 渡邊祐貴 (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

## 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
- ~~例年先輩がよ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

## ハッカソン課題

ゲームアイデア: 首藤  
シナリオ: 篠崎、渡邊、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、渡邊、首藤

## 静的解析

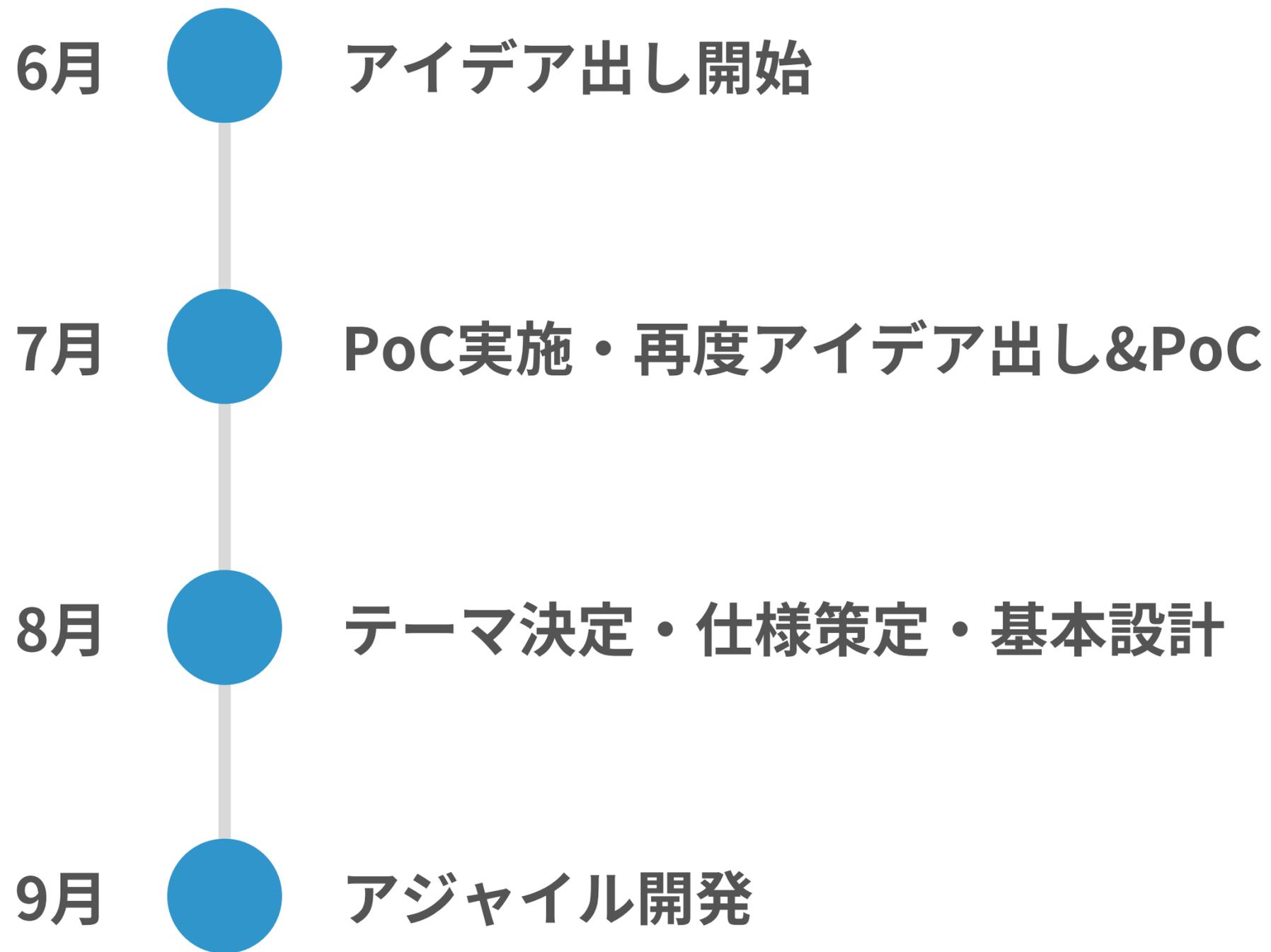
篠崎、松元、首藤

## DFIR

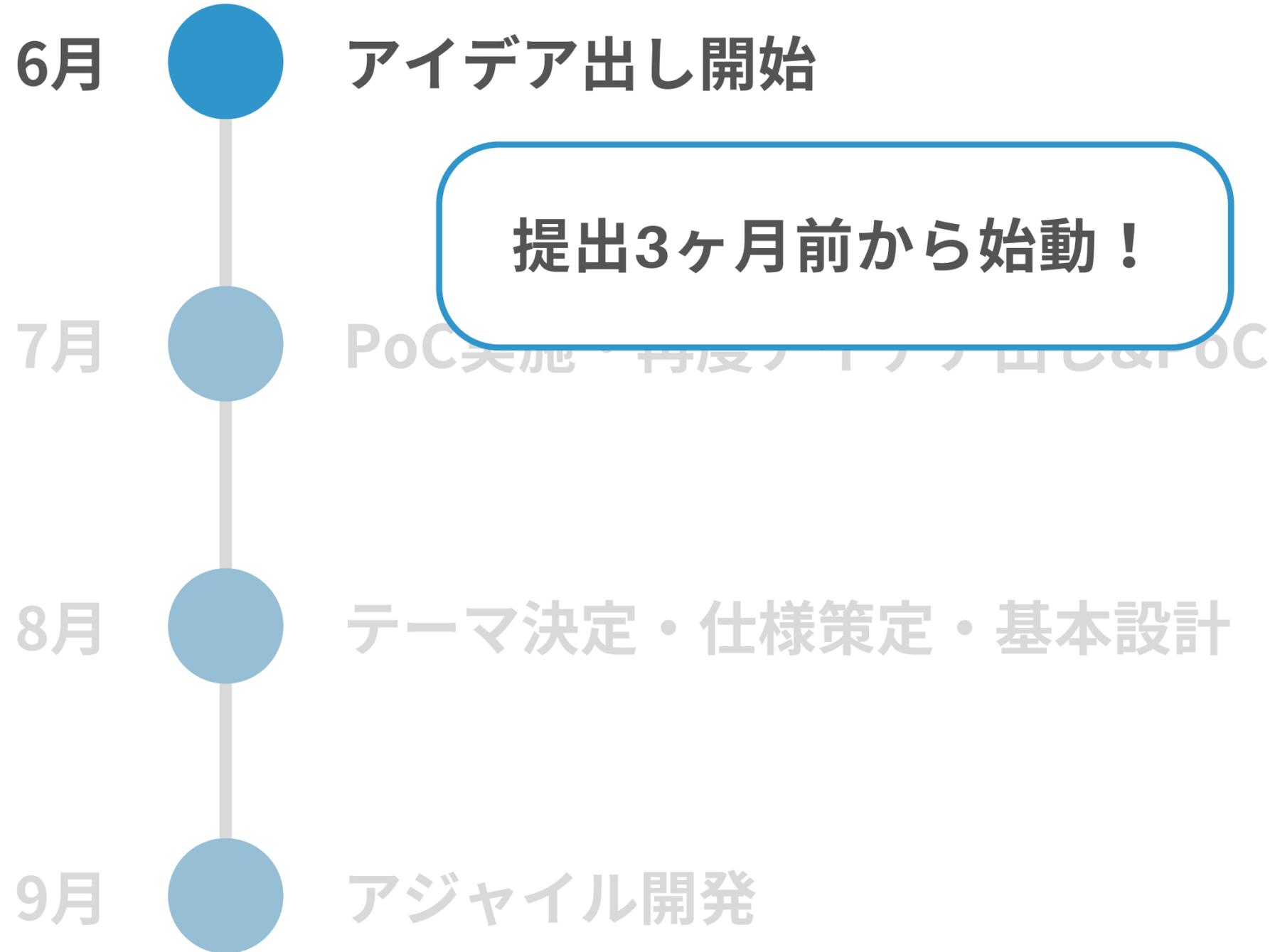
渡邊、小林、松本

# ハツカソン課題

# スケジュール



# スケジュール



# スケジュール

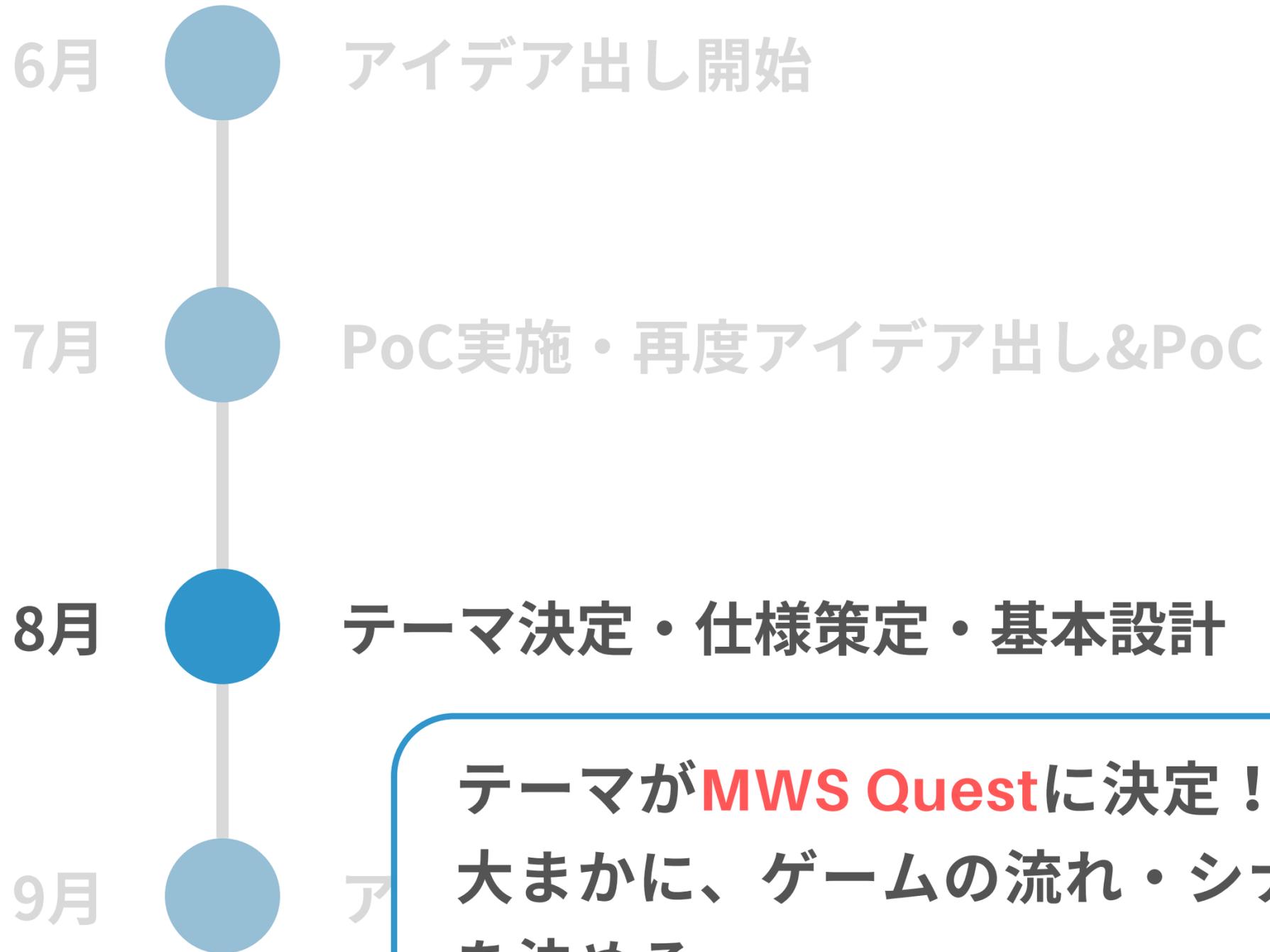
6月 アイデア出し開始

7月 PoC実施・再度アイデア出し&PoC

8月 テー  
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！

9月 アジャイル開発

# スケジュール



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**

## 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



# 開発の様子

The screenshot displays a Jira Sprint Backlog for the project 'MWS-Quest'. The interface is organized into five columns representing different stages of task completion:

- Icebox (6 items):** Tasks that are not yet started. Examples include:
  - MWS-Quest #68: ダイアログの改行位置を綺麗にする (enhancement, 実装)
  - MWS-Quest #40: メニュー画面の作成 (wontfix, 実装)
  - MWS-Quest #71: 村人が話すTipsを増やして、ランダムに話させたい (wontfix, シナリオ, 実装)
  - MWS-Quest #21: ログイン機能のバックエンド作成 (wontfix, 実装)
  - MWS-Quest #5: 建物の中に入る機能の実装 (wontfix, 実装)
- Todo (1 item):** Tasks planned for the current week.
  - MWS-Quest #66: 解説シーンの画像差し替え (実装)
- In Progress (1 item):** Tasks currently being worked on.
  - MWS-Quest #103: 解説シーンで戻る機能を付けたい (enhancement, 実装)
- Review (0 items):** Tasks currently under review.
- Done (64 items):** Completed tasks. Examples include:
  - MWS-Quest #114: BGM/SEのバリエーション追加 (#117)
  - MWS-Quest #91: ログイン画面でEnterキーによるログインを可能にする (enhancement, 実装, #118)
  - MWS-Quest #120: 「呪文の痕跡」画面において正規表現で検索できることを明記する (documentation, #121)
  - MWS-Quest #106: 全体テスト
  - MWS-Quest #88: UN頼みのロゴ作成

## スプリントバックログの管理

The screenshot shows a GitHub pull request interface. At the top, the title is "CONTRIBUTING.mdの追記 #116". A purple "Merged" badge indicates that "konekotech merged 3 commits into main from IR-107/sound-document on Oct 1". Below the title, navigation tabs show "Conversation 1", "Commits 3", "Checks 0", and "Files changed 1". A diff bar shows "+63 -3" changes. The main content area displays a comment from "konekotech" on Sep 30: "音声ファイルなどに関する追記を行いました。". Below this is a commit update: "update: CONTRIBUTING.md" by "7fe9a71". A red "Requested changes" icon indicates that "marokoro7636 requested changes on Sep 30". A comment from "marokoro7636" follows: "決定ボタンの音に関する記述も入れてください。". On the right sidebar, the "Reviewers" section lists "stokob", "alpher0221", and "marokoro7636", each with a green checkmark. The "Assignees" section shows "No one" with a link to "assign yourself". The "Labels" section has a label named "実装". The "Projects" section shows "None yet". The "Milestone" section is currently empty.

レビューの様子

# マルウェア分類課題

## 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

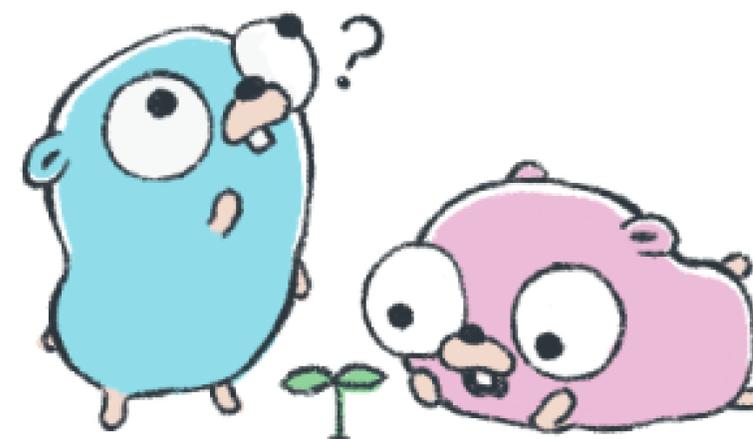
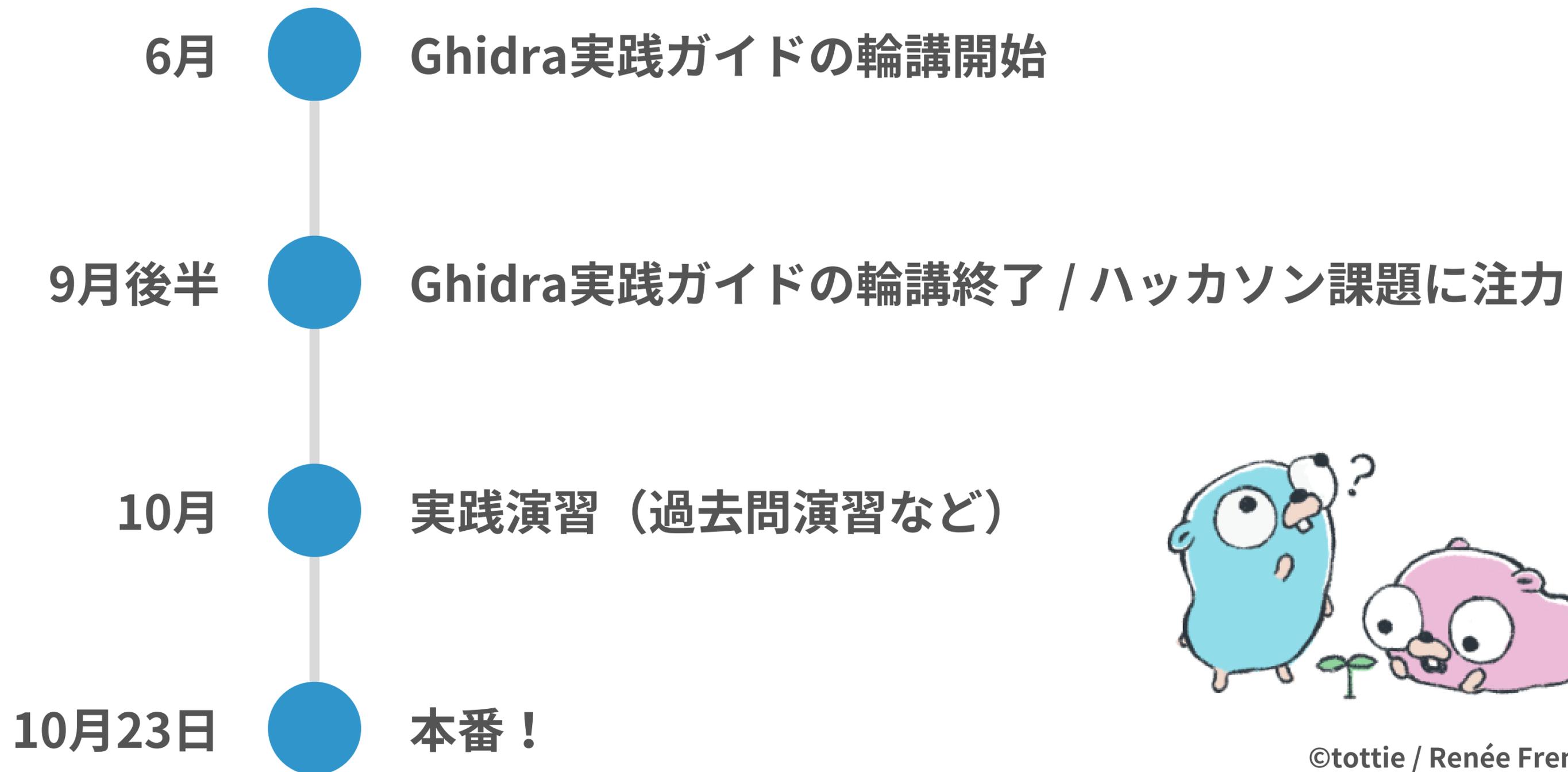
- Git / GitHub
  - 作成したコードの管理 → 提出時の commit のルールづけ
- uv
  - パッケージやバージョンの管理
  - pipより高速・高機能

## 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

# 靜的解析課題

# スケジュール



©tottie / Renée French

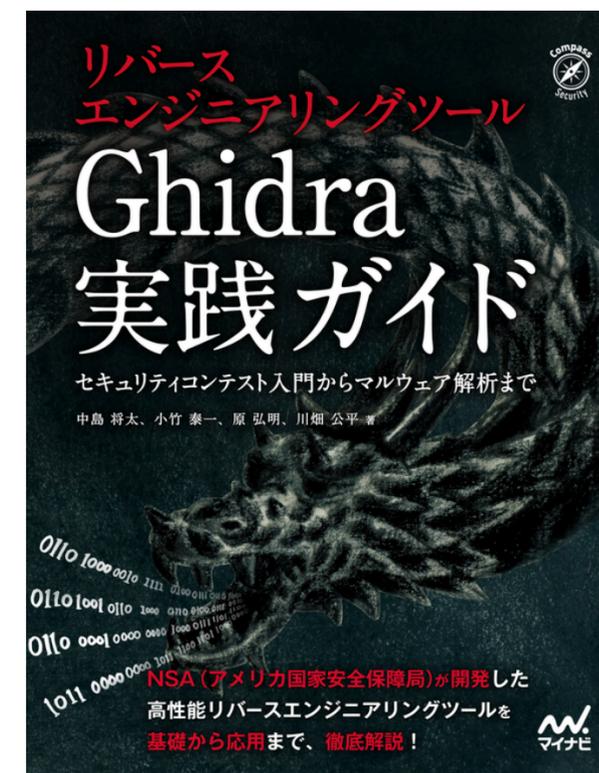
# 『Ghidra実践ガイド』を教科書として使用

- **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**の感覚をしっかりと身につける



©tottie / Renée French

## 自分でもバイナリをつくってみる

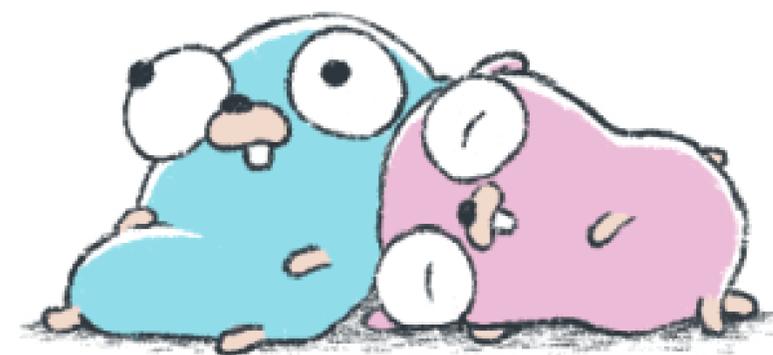
- Goバイナリは他のバイナリと比較して少し特殊なため、**コードとバイナリを照らし合わせて理解する**作業が必要だった
- FFRI様の技術ブログなどを活用

## 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



# DFIR課題

## 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

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

2連覇

# 総合優勝



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！

