Google Cloud

データ分析から始める チート / 不正 Bot 対策

渡邉 雄作

Google Cloud

カスタマー エンジニア

スピーカー自己紹介

渡邉 雄作
Google Cloud
カスタマー エンジニア

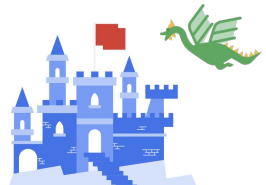
大学卒業後、金融系 SIer で Java プログラマーとしてキャリアをスタート。

その後

- インターネット広告代理店事業会社（約 14 年）
  - ブログやコミュニティサービスの **WEB エンジニアを約 7 年担当**
  - **アドテク事業のアーキテクト、PdM、事業責任者、海外事業**を約 7 年間担当

- CDP（カスタマーデータプラットフォーム）事業会社（約 2 年）
  - **Solution Engineer としてデータ活用領域におけるお客様への技術提案・サポート**

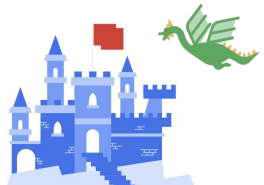
現在は Google Cloud にて**ゲーム業界担当のカスタマー エンジニアとして Google Cloud 全般の技術提案**を担当。



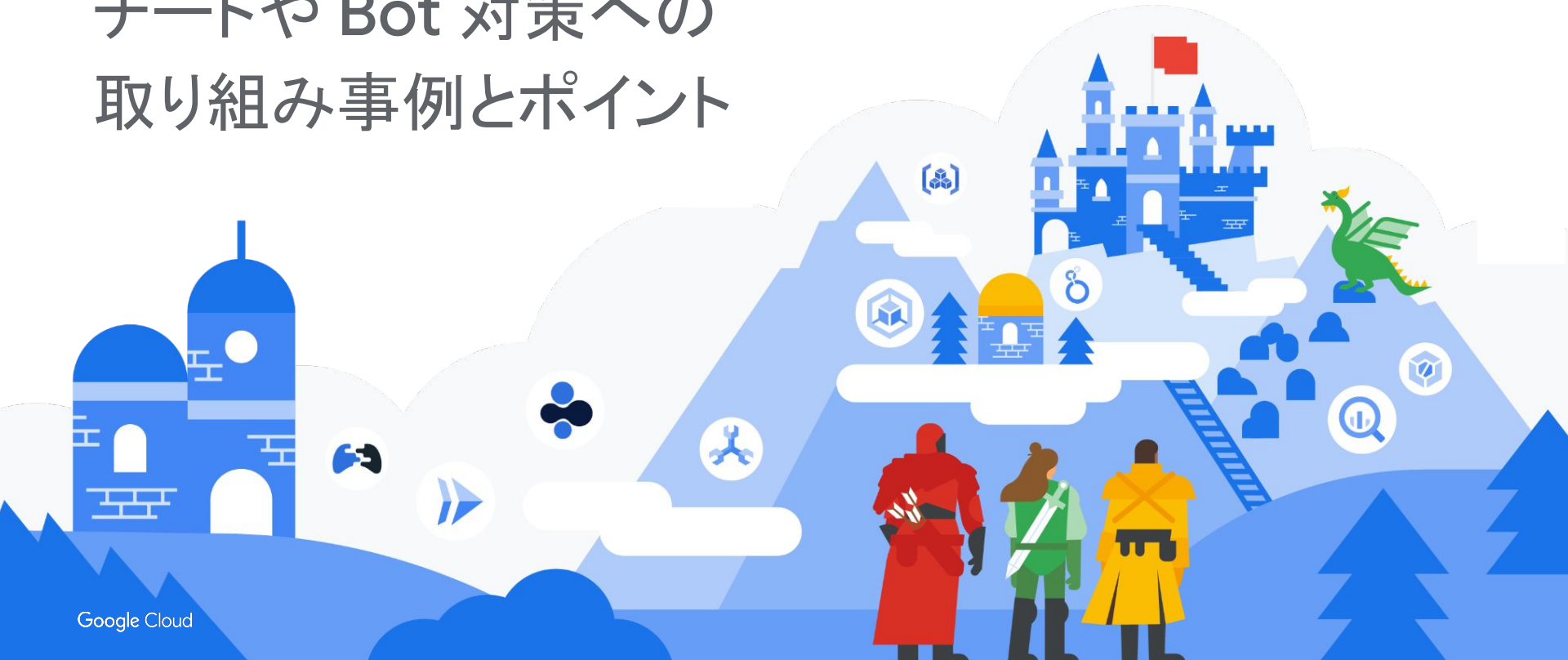
アジェンダ

01 | チートや Bot 対策への取り組み事例とポイント

02 | Phase や目的によってアーキテクチャを決める



チートや Bot 対策への取り組み事例とポイント



Google Cloud

MMORPG における実際のチート対策の事例

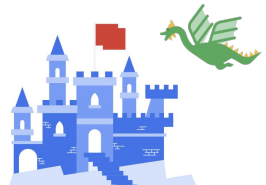
Customer Case for Anomaly Detection in MMORPG (Google Cloud Next '19)

- アイテム不正取得など売上に直接的な影響があった
- 元々 Rule ベースで対応していたのでノウハウはあった
- ML ありきではなく、どのような方法が最適なのか綿密な事前の議論を行った
- アングラサイトでチート方法が拡散されるのを検知
- リスト作成を ML で行い、最終的には人の目で判断

MLAI233:
Customer Case:
Anomaly Detection In MMORPG

Jason Baek, Customer Engineer, Google Cloud
Etsuji Nakai, Solutions Architect, Google Cloud
Jennifer Oh, ML Engineer, Netmarble

Google Cloud



事例からわかること

01

不正の種類を整理して、**ビジネス影響を把握**する

02

Rule ベースでもしっかりエ数を割いて運用を行い**ソウハウを貯める**

03

サービス内だけで
完結させずに、**外部情報も監視**して包括的に
対応する

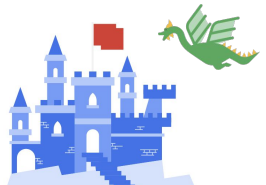
04

完璧な Solution は
存在しないので、
アドホックに最適化する

05

手法についてはしっかり時間をとって**社内外の専門家と方針の議論**を行う

- 社内エンジニア
- パートナー企業
- Google Cloud (TAM / PSO の活用)



なぜうまくいかないのか？

部門ごとの課題意識の違いや個別で見た時のインパクトの見積もりの難しさが影響する。

インフラチーム

無駄なトラフィックやデータを排除してコスト削減

運用チーム

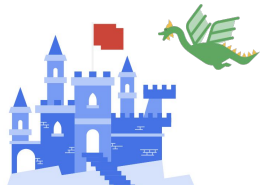
チートや不正 Bot の判断や Ban の対応作業コスト削減

分析チーム

ゴミデータの混入による分析コスト削減と精度の向上

企画、ビジネスチーム

ユーザーコミュニティの過疎化や課金売上への影響



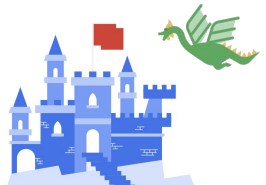
どうすればうまくいくのか？

トップダウンで実施する

- ユーザー コミュニティの動向を把握する
- 既存データから見込まれる売上への影響を推定する
- 各部門で True KPI になることによる目標設定の見直しを行う

各部門でまずは小さく始める

- チートや不正 Bot とみなす Rule を個別に作成し、それを少しずつ追加、洗練させる
- Rule を再利用可能な形で管理し、最終的には部門を跨いで適用する
- ML モデル構築時のヒントとして活用する



各部門でまずは小さく始める

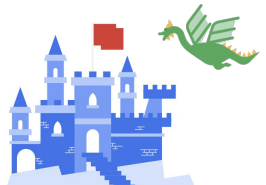
Phase. 1
Rule ベースでチート/ 不正
Bot をリスト化

Phase. 2
リスト化された
アクセスやユーザーを
目視確認して精査

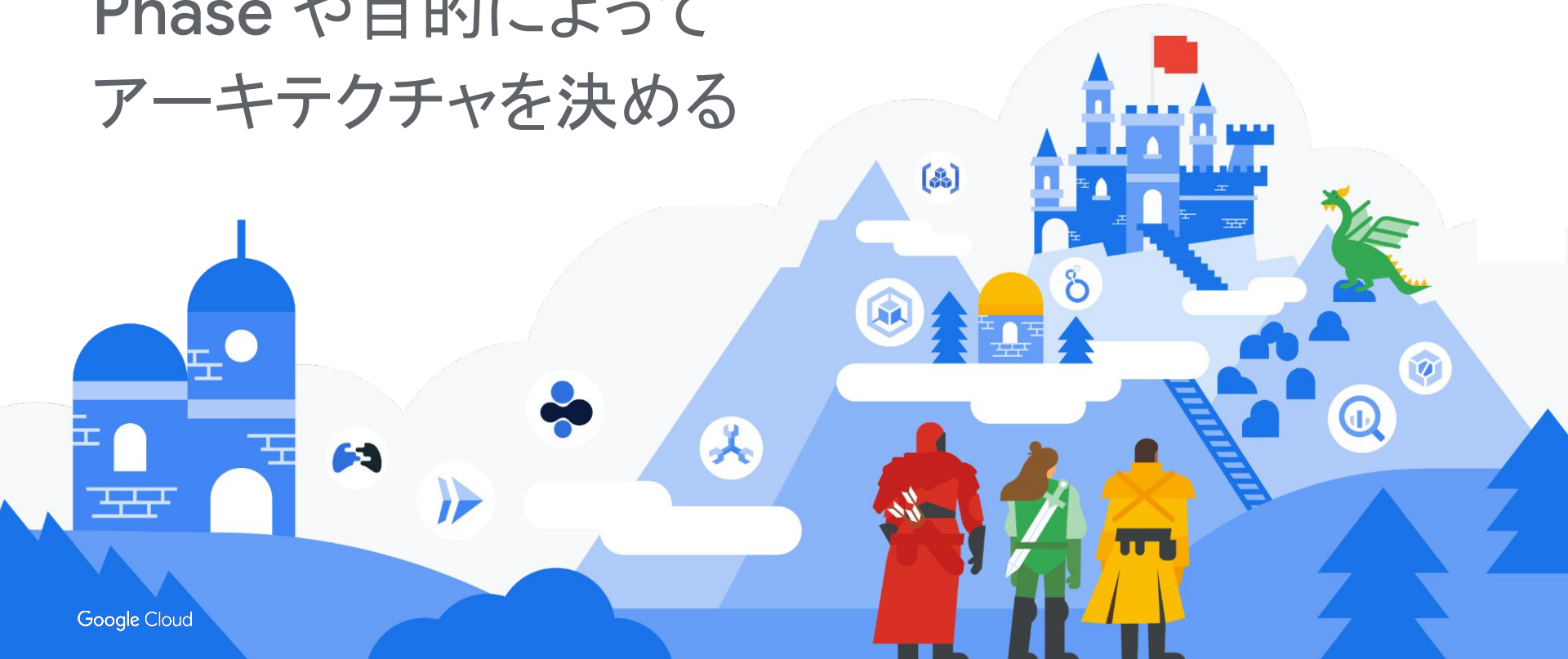
Phase. 3
トラフィックやユーザー数、
アイテム取得数などに対する割合を算
出し、ビジネス インパクトを計測

Phase. 4
該当のトラフィックや
ユーザーの Ban / Deactive
作業の自動化

Phase. 5
AI / ML 活用も視野に検出精度の
向上やリスト作成の自動化



Phase や目的によって
アーキテクチャを決める



対策を実施するタイミングの違い

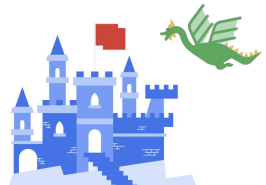
事前に防ぐ

Cloud Armor Adaptive Protection

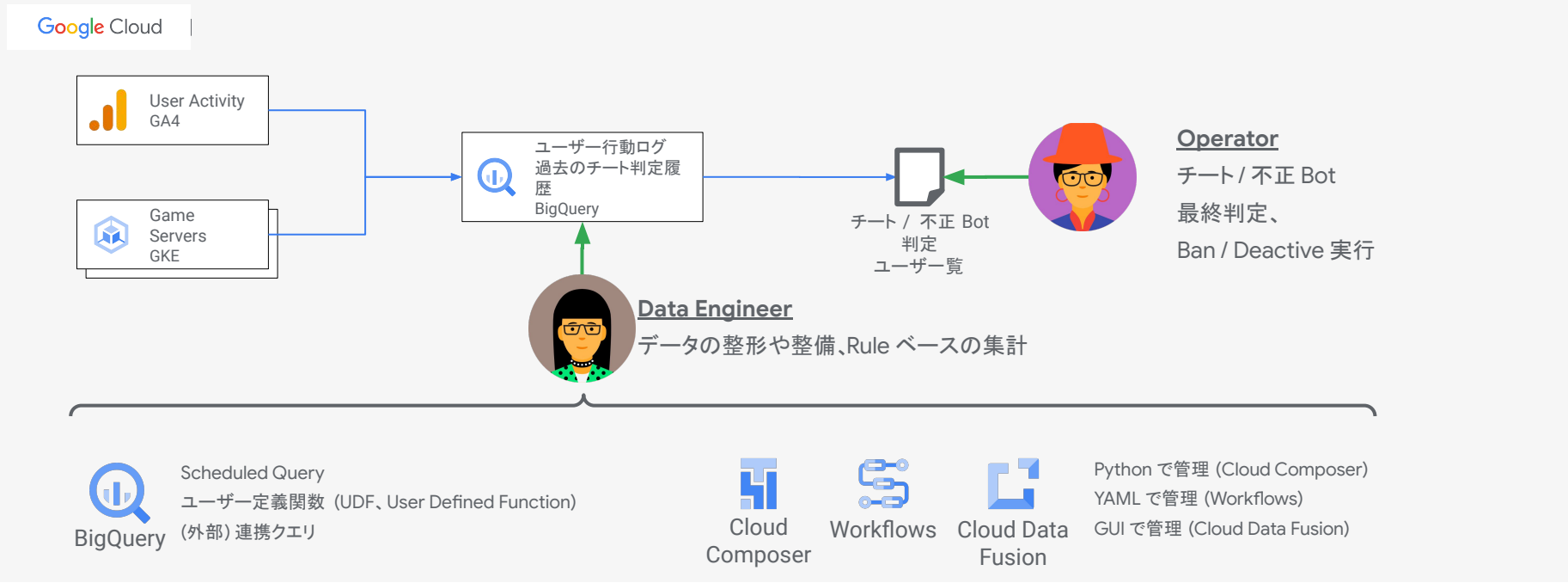
- L7 での Rule ベース防御
- ML による異常トラフィック検知 (Adaptive Protection)
- 用意された WAF や IP リスト (Managed Protection Plus)

事後に対応する

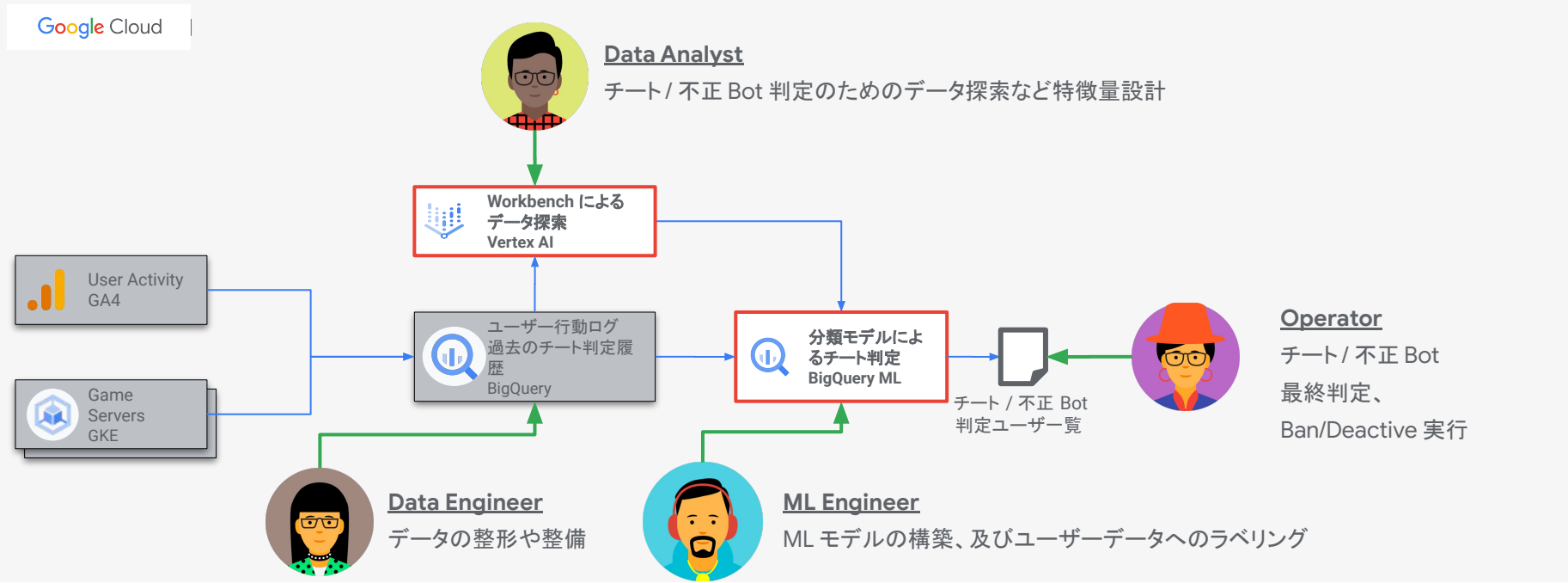
- 保存クエリ、with 句、UDF、外部データソース クエリの活用
- 定期実行、自動化
- ML での異常なアクティビティ検知や類似ユーザー抽出など



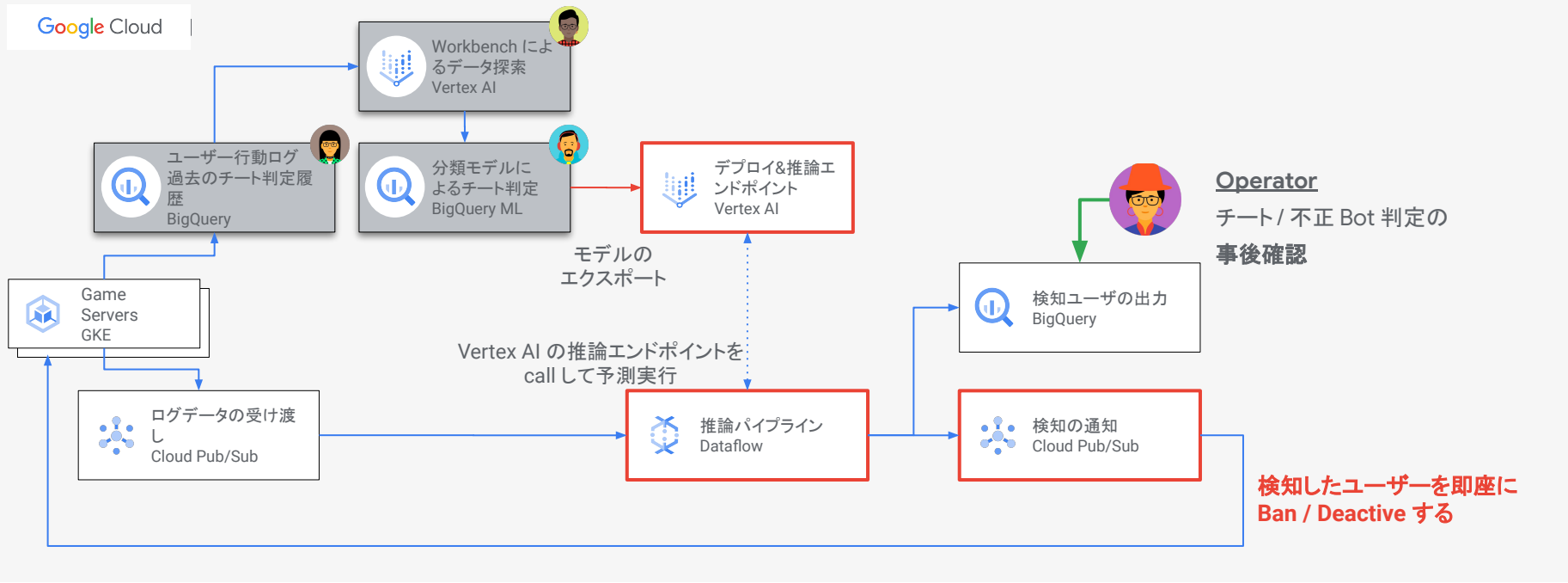
まずは BigQuery 上で Rule ベースの集計を行う



バッチ で ML を使った チート / 不正 Bot 検知をする



リアルタイムに ML でチート / 不正 Bot を検知して Ban / Deactive する



チーム構成のスキルセット例

Data Analyst

SQL を使って KPI の分析や BI ツールでの可視化などをしている

ML Engineer

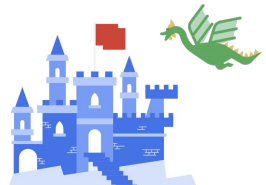
ML モデルの構築からデプロイまで、MLOps を担当している

Operator

SQL を使って、必要なデータを抽出してレポートなどを作成している

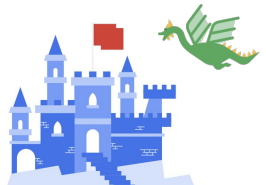
Data Engineer

保存されているデータのマイグレーション、正規化、パフォーマンス・チューニングなどを担当している



まとめ

- チート / 不正 Bot 対策は局所最適な取り組みが必要
- 事前対応と事後対応でそれぞれ目的とインパクトで使い分ける
- **事前**対応ならマネージドサービス活用が可能
- **事後**対応なら BigQuery でまずは集計から始める
  - AI / ML を使ってさらに洗練された検出や運用改善も可能
- Google Cloud の Professional Services の活用



Google Cloud

Thank you