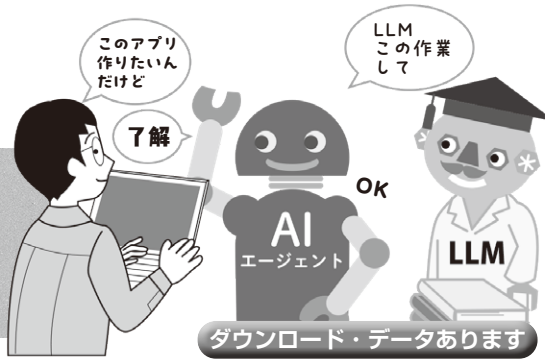
OpenAI Agents SDKで始める 自分専用 AIエージェント開発



第2回 OpenAI Agents SDK設定②…開発管理ツールの使い方

氏森 充

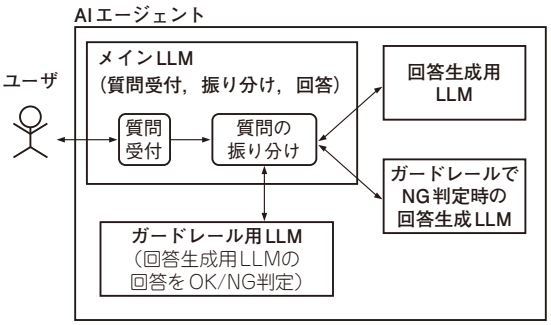


図1 本連載で作成するAIエージェントのイメージ
LLMの回答が適切か判定する別のLLM（ガードレール用LLM）を組み込む

本連載では，筆者が特に注目しているOpenAI Agents SDKを使って，AIエージェントを開発していきます．AIエージェントはさまざまなことができますが，本連載では例として，プロンプトや生成された内容が不適切とされた場合，処理を中断させるものを中心に取り上げます（**図1**）．これを開発していく中で，その特徴や設計思想，実装スタイルについて詳しく解説します．

● 今回のテーマ

前回は，OpenAI Agents SDKを利用する上で必須となるAPI keyの取得手順について紹介しました．今回はその続きとして，取得したAPI keyを安全かつ効率的に管理し，エージェント開発を安定して進めるための基盤となるOpenAI Platformを解説します．

OpenAI Platformは，LLM（Large Language Models）を利用したアプリケーション開発を支える管理コンソールです．単なるAPI key管理画面にとどまらず，開発，運用，デバッグに不可欠な情報を一元的に可視化できる点が大きな特徴です．具体的には，次のような情報を確認できます．

- 利用状況（課金，トークン消費）の把握
- レート・リミットの確認
- API 実行ログの確認
- Agents SDK実行時の詳細なトレース解析

図2 画面OpenAI公式サイトからログインする

特にAgents SDKでは，1回のユーザ入力に対して内部で複数回のAPI呼び出しやFunction実行が行われます．そのため，OpenAI Platformを利用せずに開発を進めると次のような問題に直面しがちです．

- 想定外のトークン消費
- 意図しない課金増加
- エージェント挙動の原因不明な不具合

本稿では，Agents SDKを利用する開発者が最低限押さえておくべきOpenAI Platformの要点に絞って解説します．

AIエージェント開発の管理ツール「OpenAI Platform」

OpenAIアカウントを作成し，OpenAI公式ページ（`https://openai.com/ja-JP/`）（**図2**）にログインすると，管理コンソールであるOpenAI Platformにアクセスできるようになります（**図3**）．OpenAI Platformでは，API keyの管理，モデル設定，Usage（利用状況）の確認などを行えます．

特にAgents SDKを利用する場合，このPlatformは単なる設定画面ではなく，エージェントの挙動を確認，解析するための重要な役割を果たします．中でもLogs画面やTraces 画面では，エージェントがどのような処理を行い，どのAPIツールがどの順序で呼び出されたのかを詳細に確認できます．Agents SDKを用いた開発では，コードの実装と並行してOpenAI Platformを常に確認しながら作業を進めることが重要です．