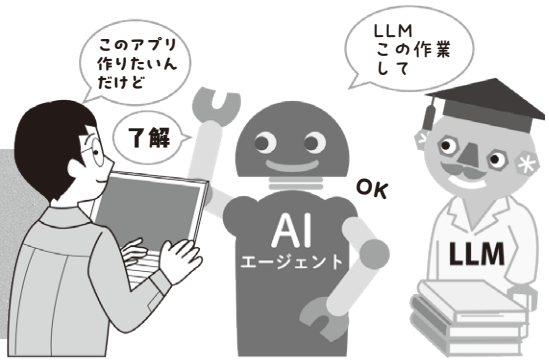
ダウンロード・データあります

2025年12月号特集「自分専用！ LLMの作り方」フォローアップ

OpenAI Agents SDKで始める 自分専用 AIエージェント開発



第3回 サンプル・プログラムを使ってLLMを実行してみる

ご購入はこちら

氏森 充

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

前回まで，エージェント開発に使用するOpenAI Agents SDKの機能の紹介を行ってきました．今回は，OpenAI Agents SDKに付属するサンプル・プログラムを試してみます．この過程で，OpenAI Agents SDKは単なるLLM（Large Language Models：大規模言語モデル）呼び出しライブラリではなく，モデル選択など前提条件の上に業務フローを設計，実装するための基盤であることを説明します．なお，本稿で扱うサンプルは，いずれも最小構成を基本としています．そのため，ここでは，高度なエージェントを作ることよりも，OpenAI Agents SDKが提供する設計上の枠組みや前提条件を理解することに主眼を置いています．

● サンプル・コード利用時の注意

▶モデル指定は必ず明示する

OpenAI Agents SDKでは，エージェント作成時にモデルを明示しない場合，環境に応じたデフォルト・モデルが使用されます．この挙動は動作確認としては便利ですが，次の問題を引き起こします．

- アカウントの契約状態によって実行可否が変わる
- 想定外に高コストなモデルが選択される
- 実行結果やトークン消費量の再現性が失われる

そのため，検証用途であってもモデルは必ず明示的に指定します．モデル指定は単にコスト削減のためではなく，設計および検証の前提条件を固定するために必要な作業です．

▶API keyは実行前に確定させる

OpenAI Agents SDKは，SDKのインポートの時点で環境変数`OPENAI_API_KEY`を参照します．そのため，Python実行中に後から環境変数を設定しても，SDK側に反映されない場合があります．API keyは必ずプロセス起動前に設定します．スクリプト内で動的に切り替える場合は，SDKが提供する「明示的にAPI keyを設定するAPI」を利用という前提で構成します．

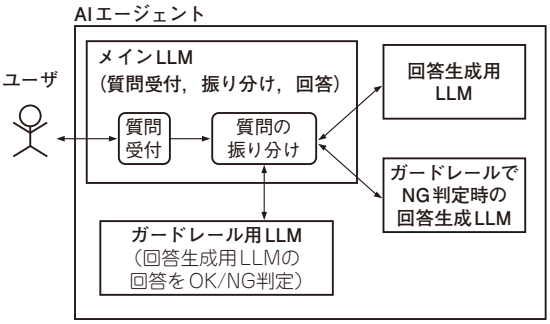


図1 本連載で作成するAIエージェントのイメージ
LLMの回答が適切か判定する別のLLM（ガードレール用LLM）を組み込む

LLMを検証…価格，生成内容，トークン使用量など

● サンプル・プログラムでOpenAI Agents SDKの基本動作を確認

サンプルとして用意されている`hello_world.py`（**リスト1**）を実行し，OpenAI Agents SDKの基本動作を確認します．このサンプルは，最も単純なエージェント呼び出しのみを行う構成になっています．従って，SDKのインストールやAPI key設定，モデル指定が正しく行われているかを確認する目的に適しています．以降のサンプルを試す前に，本プログラムが問題なく実行できることを確認するとよいでしょう．

本サンプルのソースコードでは，比較的低価格なモデルを明示的に指定しています．そのため，初回実行時や検証用途でも，クォータ消費を抑えながら動作確認が可能です．モデル指定を省略した場合はデフォルト・モデルが選択され，アカウント設定によってはエラーが発生する可能性があるため，モデルを明示する

本連載サポート・ページ（https：//interface.cqpub.co.jp/aiagents2601/）にて補足資料などを掲載