Google Cloud

Professional Agentic Architect

認定試験ガイド

Google Cloud Certified Professional Agentic Architect は、Google Cloud で AI を活用した自律型エージェント ワークフローを設計、管理する技術実務者です。信頼性、パフォーマンス、費用、セキュリティ、スケーラビリティを考慮しながらエージェント ソリューションを構築する、経験豊富な開発者またはアーキテクトであり、大規模言語モデル（LLM）の利用、エージェント設計パターンの適用、コードの記述、Google Cloud でのデータソースの統合に関する豊富な経験を有しています。

セクション **1:** ローコード ツールを使用したエージェントの構築（試験内容の約 **13%**）

1.1 ローコード ツールを使用してエージェント ワークフローとエージェントの動作を構成する。以下のような内容が評価対象となります。

- Gemini Enterprise ツールを使用して、状態ベースのワークフロー（ページ、遷移ルート、イベント ハンドラ）を構成する（例: Gemini Enterprise Workflow Builder、Customer Experience Agent Studio [CX Agent Studio]）
- エージェントの動作をガイドするシステム指示とコンソール内プロンプト テンプレート（例: 少数ショット、Chain-of-Thought）を作成する（例: Workflow Builder、CX Agent Studio）

1.2 エンタープライズ データを Gemini Enterprise に接続する。以下のような内容が評価対象となります。

- 企業独自のデータソースに安全に接続してクエリを実行できるようにエージェントを構成する（例: Gemini Enterprise、エージェント検索）
- 非構造化マルチモーダル データ（例: 動画、音声、画像）をエージェント ワークフローに取り込んで処理する

セクション **2:** アプリケーション開発におけるコーディング エージェントの使用（試験内容の約 **17%**）

2.1 コーディング エージェントを効果的に使用する。以下のような内容が評価対象となります。

- Model Context Protocol（MCP）サーバー、カスタムスキル、ツールへのアクセスを使用してコーディング エージェントを構成する（例: Antigravity、Google Cloud 上の Claude Code）
- 安全なサンドボックスでコーディング エージェントを使用する（例: Google Kubernetes Engine [GKE]、Cloud Workstations、Antigravity）
- コーディング エージェントを使用して、ソースコードのリファクタリング、実行ランタイムの最適化、アプリケーション レイヤの脆弱性に対するパッチ適用を行う

2.2 エンタープライズ ワークフロー向けにコーディング エージェントをカスタマイズする。以下のような内容が評価対象となります。

- Antigravity を使用してスキル、プラグイン、拡張機能フック、ルール、サブエージェントを作成する
- Agents CLI で Antigravity を強化し、エージェントの構築と、デプロイされたエージェントのスケーリング、管理、最適化を行う

セクション **3:** カスタム エージェントの開発（試験内容の約 **33%**）

3.1 コードでエージェント ワークフローを設計、構築する。以下のような内容が評価対象となります。

- 費用、セキュリティ、エージェント アーキテクチャを考慮して、適切な言語モデル（例: 大規模言語モデル [LLM] か小規模言語モデル [SLM] か、セルフホスト型か Software as a Service [SaaS] か、オープンソース ソフトウェア [OSS] か商用 LLM か）を選択、構成する
- オープンソース ライブラリを使用してカスタム エージェントを構築する（例: Agent Development Kit [ADK]）
- セッションとメモリを構成する（例: Agent Platform メモリバンク、マネージド セッション）
- Agents CLI を使用してスキルを構成する（例: プラグイン、エージェント モードか人間モードか）

3.2 企業の専門分野に関する知識を統合する。以下のような内容が評価対象となります。

- ベクトル データベースなどの適切なサービスを使用して、検索拡張生成（RAG）パイプラインとベクトル取得システム（例: エンベディング モデル、類似性のスコアリング、再ランキング）を設計、構成、管理する（例: Vector Search、Agent Retrieval）
- エージェントの権限を構成する（例: Agent Identity）
- Google Cloud ツール（例: Agent Registry、Google Cloud MCP サーバー）を使用して、事前構築済みの機能とカスタム機能を構成する（例: マネージド データベース、API インテグレーション、およびエージェントをサードパーティの SaaS ツールやリモート サーバーに接続する MCP サーバー向けのカスタム インテグレーション レイヤ）

3.3 エージェント ワークフローのオーケストレーションと調整を行う。以下のような内容が評価対象となります。

- エージェント プロトコル（例: MCP、Agent2Agent [A2A]）を使用して、エージェントのオーケストレーションを行う
- Google Cloud ツールを使用して、マルチエージェントのハンドオフとワークフロー（例: 並列エージェント、シーケンシャル エージェント、グラフ ワークフロー）を選択、調整する（例: Agent Identity、Agent Registry、Agent Runtime、エージェント ポリシー）

セクション **4:** エージェント ワークフローの評価とデプロイ（試験内容の約 **22%**）

4.1 開発環境と本番環境でエージェントを評価する。以下のような内容が評価対象となります。

- エージェントの評価用のテストセット（例: ゴールデン データ、プロンプト、エッジケース）を作成する
- 確立された成功基準に基づいてエージェントのツール実行を評価する継続評価パイプラインを作成する
- 適切な評価フレームワークとツール（例: ADK 評価ツール（evalset）、Agent Platform Gen AI evaluation service、カスタム自動評価ツール）を決定する
- ゴールデン データセットに照らしてエージェント システムを評価し、エージェントの回答と検索の品質を評価する（例: ADK の使用）

4.2 本番環境ワークロードをデプロイしてスケーリングする。以下のような内容が評価対象となります。

- ユースケース、要件、費用に基づいて最適なデプロイ ランタイムを選択する（例: Agent Runtime、Cloud Run、GKE）
- エージェントの問題（例: ドリフト、ツール呼び出し遅延、エージェントの推論ループ、システム障害）のトラブルシューティングを行う
- パフォーマンス、信頼性、費用を考慮してエージェントのモニタリングと最適化を行う（例: 論理エラー、遅延のボトルネック、ハルシネーションの特定）

セクション **5:** エージェント ワークフローのセキュリティとガバナンス（試験内容の約 **15%**）

5.1 エージェントのセキュリティとガバナンスを構成する。以下のような内容が評価対象となります。

- 認証と安全なツール実行を実装する（例: OAuth 2.0 を使用したエージェントからツールへの API 呼び出し）
- Agent Identity を使用してプリンシパル アクセス境界（PAB）ポリシーを構成する
- トラフィックをモニタリングし、エージェントを追跡するように Agent Gateway を構成する
- エージェントのガバナンスとポリシー適用を設計し、構成する（例: Agent Registry、Model Armor）

5.2 安全なエージェントの動作と実行を実装する。以下のような内容が評価対象となります。

- 適切な安全フレームワークとガードレールを設計する（例: Agent Gateway、Model Armor、人間参加型 [HITL]）
- データへの安全なアクセスと ID 伝播を構成する（例: Agent Gateway、Agent Registry）

この試験の対象となるツールは以下のとおりです。

- Agent Development Kit（ADK）
- Agent Gateway
- Agent Identity
- Agent Registry
- Agent Retrieval と Vector Search
- Agent Runtime（旧称 Agent Engine）
- エージェント検索（旧称 Vertex AI Search）
- エージェント プロトコル（例: Agent2Agent [A2A]、MCP）
- Agent Platform の Agents CLI
- Antigravity（CLI、SDK、アプリ）
- Auth Manager（OAuth 2.0）
- BigQuery
- Cloud Run
- Cloud SQL
- Cloud Storage
- Firestore
- Gemini Enterprise
- Gemini LLM
- Google Cloud Observability（Cloud Logging と Cloud Trace）
- Google Kubernetes Engine（GKE）
- Memorystore for Redis
- Model Armor
- Model Context Protocol（MCP）サーバー
- Model Garden
- RAG Engine
- Sensitive Data Protection
- Skill Registry
- Workflow Builder (旧称 Agent Designer)