SAMURAI CLOUD
POWERED BY NIPPON CLOUD WORKING GROUP

NCWG
NIPPON Cloud Working Group

「MCP/A2Aの仕組みとその活用」

～AIエコシステムを拡張する新たなプロトコル～

クラウドビジネス推進部会
部会長　藤田　浩之

SAMURAI CLOUD
POWERED BY NIPPON CLOUD WORKING GROUP

NCWG
NIPPON Cloud Working Group

SAMURAI CLOUD
POWERED BY NIPPON CLOUD WORKING GROUP

NCWG
NIPPON Cloud Working Group

大規模言語モデル（LLM）おさらい

僕：
「お前は何でも知ってるな」

LLM:

大規模言語モデル（LLM）おさらい

僕：
「お前は何でも知ってるな」

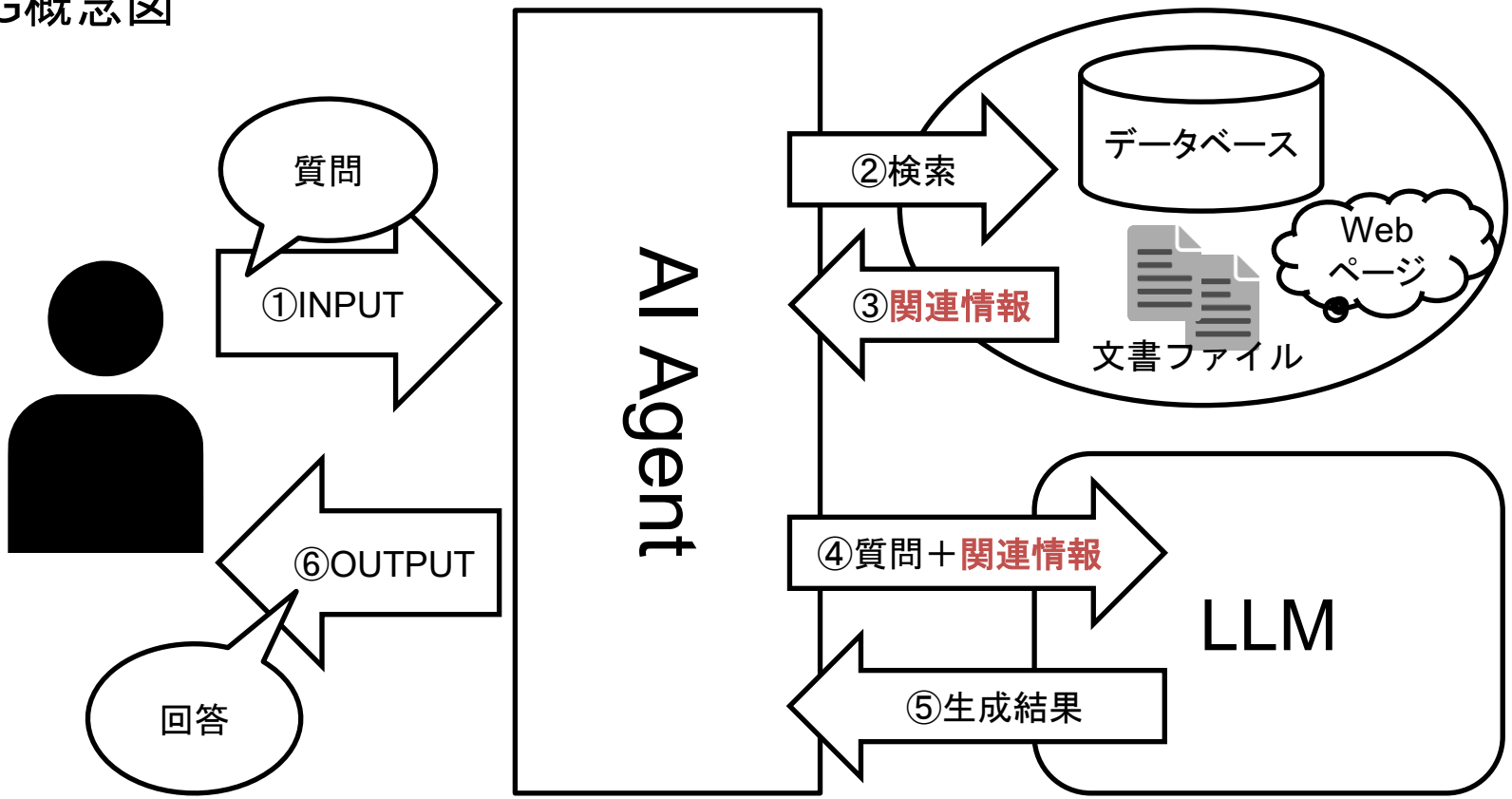
LLM:
「何でもは知らないわよ。知ってることだけ」

※元ネタ知っている人、仲良くなりましょう！

じゃあ、「知らないこと」をどうやって教えるの？

RAG（Retrieval Augmented Generation）の登場

RAG概念図



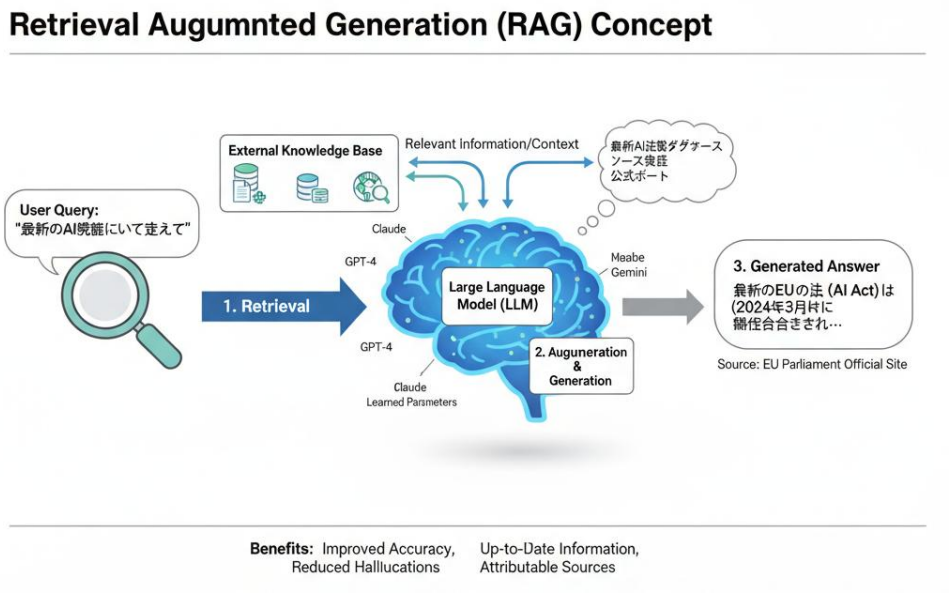
RAGの登場

- RAG（Retrieval-Augmented Generation）とは？
  LLMに外部の最新情報や専門知識を与え、回答の精度と信頼性を向上させる手法・技術。
  日本語訳は「検索拡張生成」

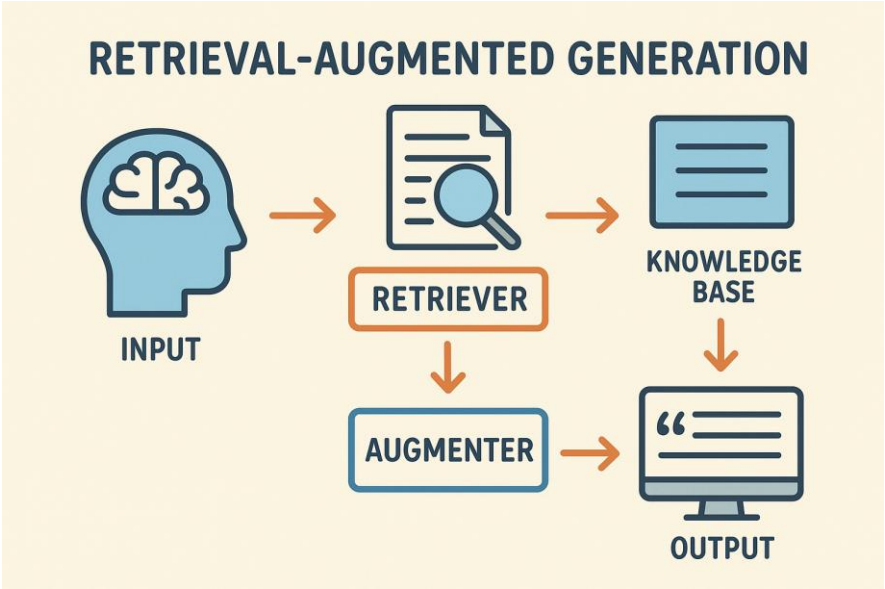
- 効果
  回答に必要な根拠をLLMに提示し、ハルシネーション（虚偽の情報生成）を抑制する。

おまけ：生成AIが生成したRAG概念図

プロンプト：プレゼンテーション用に、生成AIのRAGの概念図を作ってください



Generated by Gemini



Generated by ChatGPT

RAG対応における課題

じゃあ、RAGを使うにはどうする？

方法1：自前で実装する

課題

- 技術的なハードル
- 開発コスト・時間

方法2：サービスに機能が組み込まれるのを待つ

課題

- 各社対応までの時間

そこで登場！MCP

ANTHROP\C

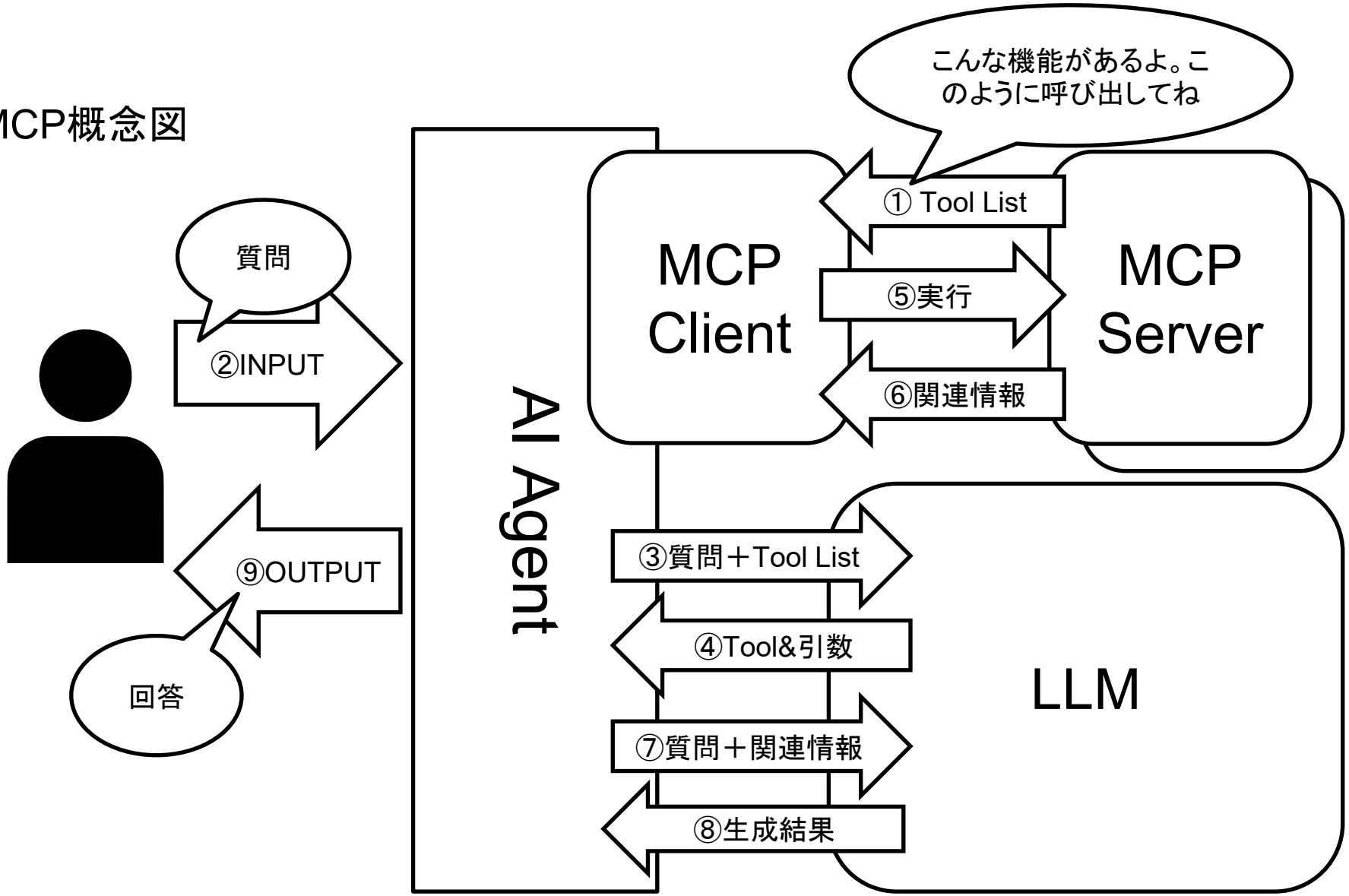
MCPは、Anthropic社が2024年11月に提唱した、LLM（Model）が応答テキストを生成する際に必要となるヒント（Context）を取得するための仕組み（Protocol）。

MCP＝ Model Context Protocol

※Anthoropic（アンソロピック）社はLLM Claude（クロード）で有名

MCPの仕組み

MCP概念図



MCPのデファクトスタンダード化

MCP対応表明の状況

- 2024年11月：Anthropic社が発表
- 2025年3月26日：OpenAI 対応表明
- 2025年4月9日：Google対応表明
- 2025年4月29日：Amazon対応表明
- 2025年5月20日：Microsoft対応表明

⇒デファクトスタンダードに

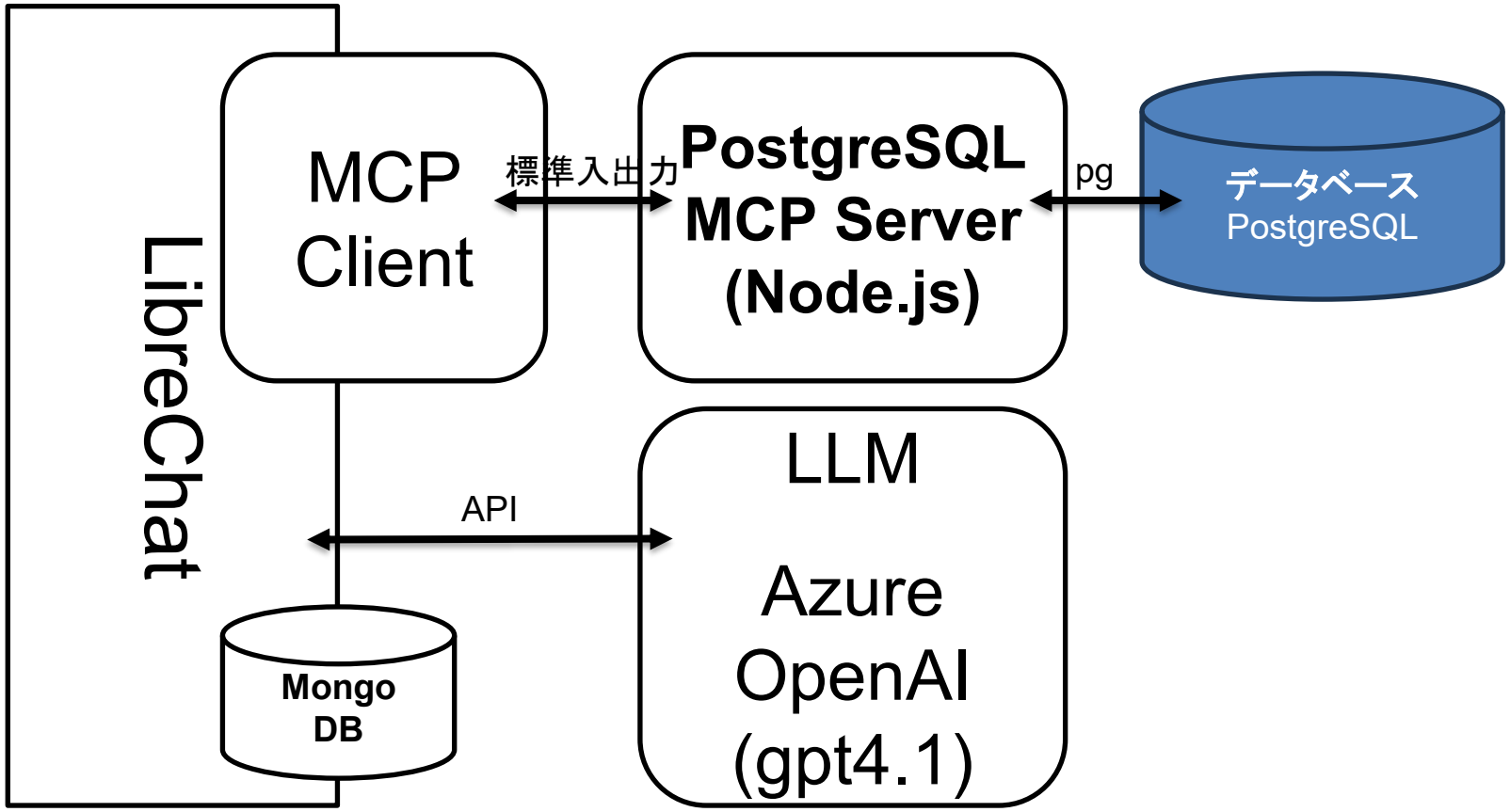
効果

この規格に対応すれば、あらゆるLLM、あらゆる生成AIツールと簡単に連携できる

※仕様は更新中（前回更新は2025年6月）

MCPデモ
（データベース検索）

デモシステム構成



Docker

Ubuntu 22.04

Windows Subsystem for Linux

デモプロンプト

- テーブルを一覧して、テーブルの説明をしてください。
- テーブルの構造から各テーブルの役割について推測してください
- 9月の売り上げトップの5人を表示してください
- 2025年7月～2025年9月の間で売れ筋商品は何ですか？5つお願いします。
- 月別にお願いします。
- 2025年9月1日～2025年9月30日の売り上げを、従業員毎に集計し,トップ5を表示してください。

MCPの価値

- 拡張性の向上

  エージェントの機能が外部サービスによって無限に拡張される。
- 専門化と分業

  各MCPサーバーが特定の機能に特化し、連携して複雑なタスクを遂行できる。
- 相互運用性

  異なるベンダーのエージェントとも連携が可能になる。連携が可能になる。
- リソース効率

  必要な時に必要な機能だけを利用できる。
- 迅速な開発とイノベーション

  共通規格なので、リリースされた新たなサービスをすぐに活用できる。

MCPの価値

- ユーザーにとって

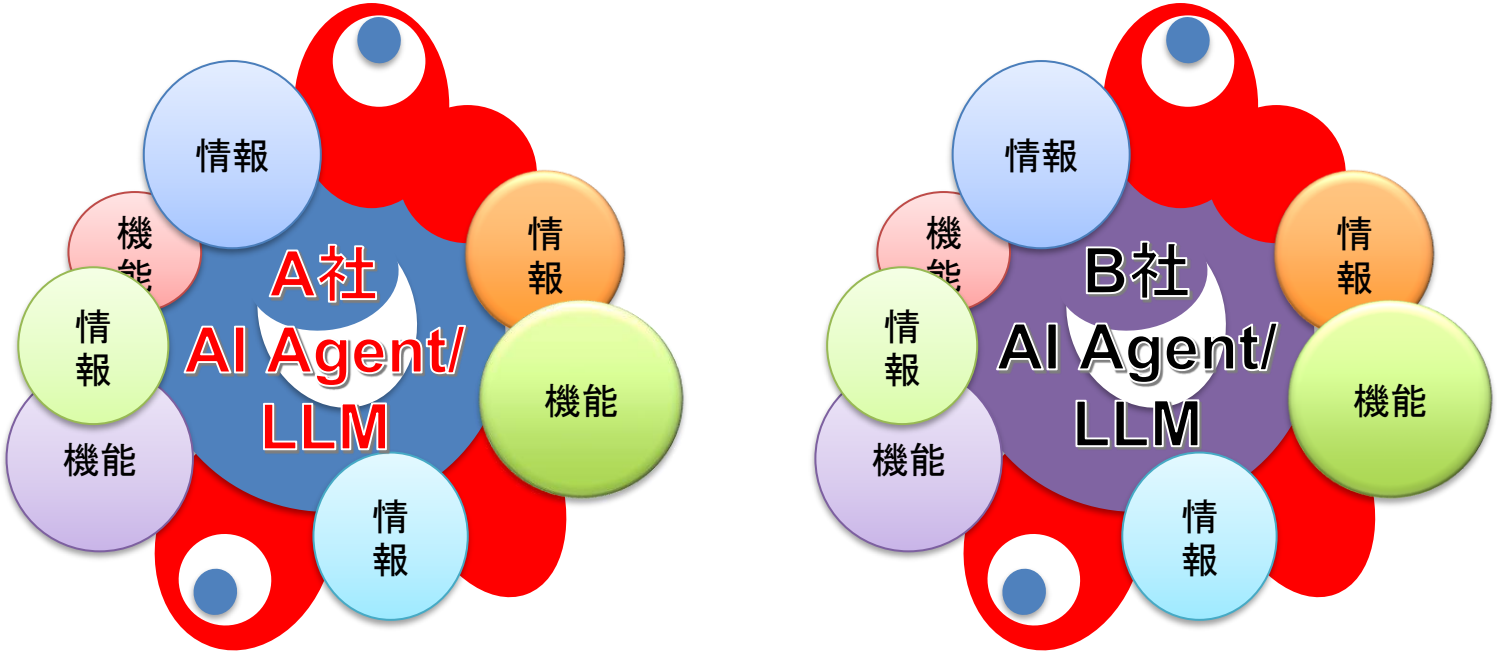
例）いつも使っているAIツールから、社内データベースや特定ウェブサイトの最新情報を簡単に取得できる。
⇒生成AIでできることが増加。生産性向上。

- 製品／サービスベンダーにとって

例）自社の製品／サービスをMCP対応させるだけで、OpenAI, Google, Anthropicなど、複数のLLMと連携可能になる。
⇒開発コスト削減。利用機会の創出。

AIアプリケーションのUSB-Cポート？

「MCPはAIアプリケーション用のUSB-Cポートのようなもの」



この「エコシステム」こそが、MCPの真価

MCPアーキテクチャ概要

プロトコル層

メッセージ形式に応じた処理や認証、タイムアウトを管理

トランスポート層

実際の通信を担当

種類

1. 標準入出力(stdio): ローカル環境での利用に最適
2. Server-Sent Events(SSE): 旧版のリモート接続向けの方式
3. StreamableHTTP: 最新版(2025-03-26)のリモート接続向けの方式

MCPのメッセージングプロトコル

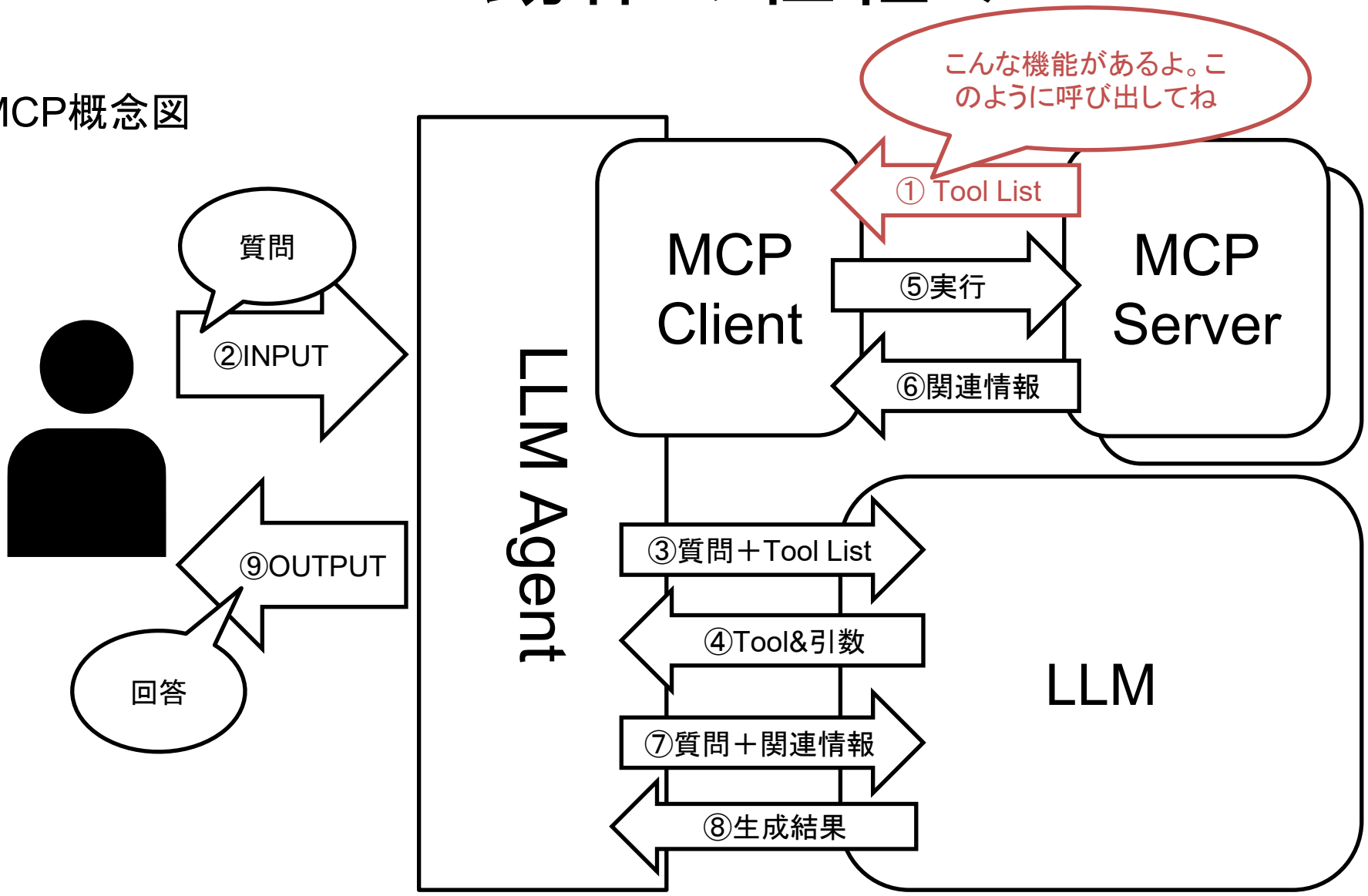
- **JSON-RPCベースの通信**

  MCPで使用されるメッセージは全てJSON-RPC 2.0形式に準拠

種類	説明	主なフィールド
Request	処理要求（応答必須）	jsonrpc, method, id, params(省略可)
Response	成功応答	jsonrpc, result, id(Requestと同じ値)
Error	エラー応答	jsonrpc, error, id(Requestと同じ値)
Notification	通知（応答不要）	jsonrpc, method

MCP動作の仕組み

MCP概念図



MCP Server ツール定義
例）Oracleデータベース検索

ツール名	説明	ヒント
execute_oracle	OracleDatabaseに対してSQLクエリを実行し、結果を返します。 Args: query: 実行するSQLクエリ（必須） params: バインド変数に使用するパラメータ（辞書型　例：{{"parameter1": 5}}） max_length: 応答の最大文字数（integer型、デフォルト: 1024） max_rows: 取得する最大行数（integer型、デフォルト：100）	文字数制限にかかったときは、max_lengthを大きくしてください。 行数制限にかかったときは、max_rowsを大きくしてください。 結果をマークダウンで表示する場合には、テーブル名に含まれる$記号記号が特殊文字として扱われるため、バックスラッシュでエスケープすることを忘れないでください。
list_tables	データベース内のテーブル一覧を表示します。 Args: max_rows: 取得する最大テーブル数（integer型、デフォルト:100 order_by: 並び順（TABLE_NAME'または‘CREATED’、デフォルト: ‘TABLE_NAME'）	
describe_table	データベースのテーブルの構造を表示します。 Args: table_name: テーブル名（必須）	結果をマークダウンで表示する場合には、テーブル名に含まれる"$"記号などのエスケープを忘れないでください。

引用元：[MCPが便利そうなので Oracle DB とおしゃべりする MCP サーバーを作ってみた（SELECT AI 対応：2025/5/3 更新） #Python - Qiita]

生成AIでSQLを生成するためのプロンプト

- データベースは下記のように、従業員:employee、商品マスタ:item_master、売り上げデータ:sales_dataのテーブルで定義されています。

＜＜テーブル定義情報＞＞

- あとは、先ほどのデモプロンプトと同様。ただしSQLは実行してくれないので、生成されたSQLを手動で実行。

MCPって結局・・・

MCPでやっていることは、これまでのプロンプト技術の応用。
能力は生成AIにかなり依存。いわば、生成AIが脳だとしたら、MCPは手足。

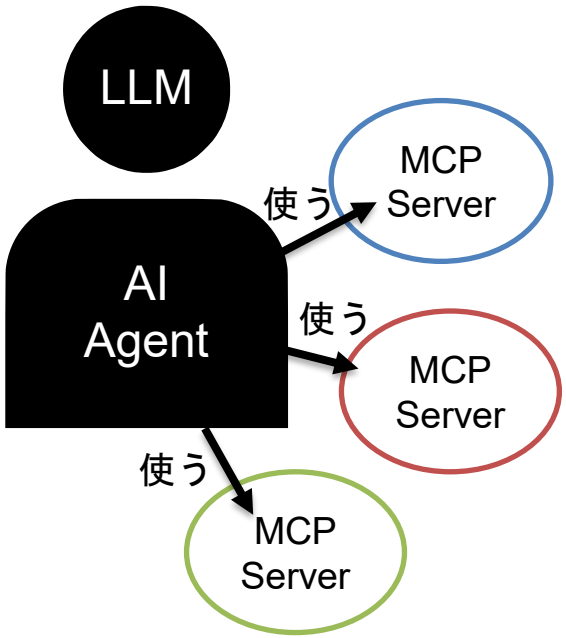
A2Aとは？

A2A（Agent-to-Agent）は、異なるベンダーや技術基盤で構築されたAIエージェント同士が安全かつ効率的に連携できるように設計された共通プロトコル。Googleが2025年4月9日に発表。

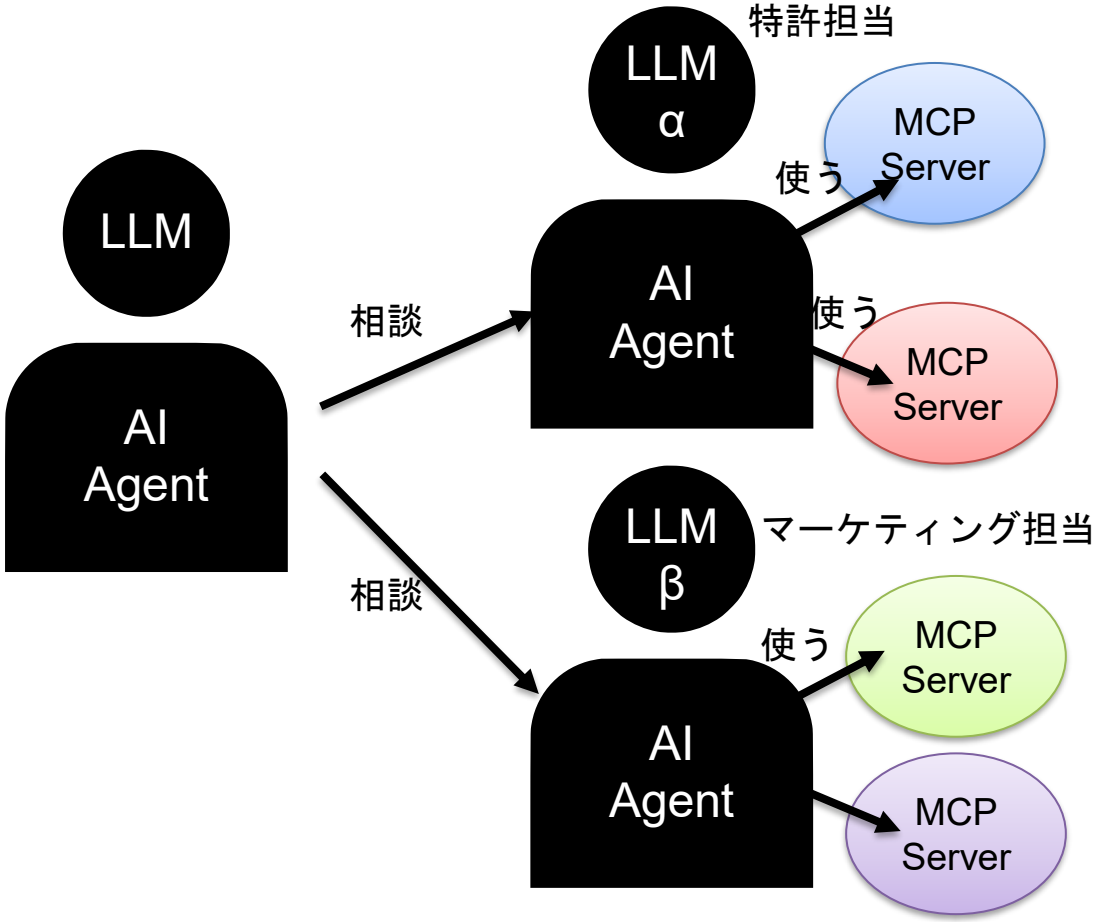
複数の専門エージェントが共通ルールに基づいて通信しながら複雑なタスクを自律的に実行する

MCPとA2Aの違い

MCPは道具



A2Aは専門家への相談



自社製品/サービスをMCPに対応させる意義

新たな顧客層の獲得

AIツール経由での利用が増加。

既存ユーザーの利便性向上

AIツールと連携することで、ユーザーはよりシームレスにサービスを利用できる。

競争優位性の確保

業界標準にいち早く対応することで、先行者利益を得られる。

AI開発コストの削減

ゼロからAI機能を開発するのではなく、MCPを介して外部LLMと連携する。

SAMURAI CLOUD
POWERED BY NIPPON CLOUD WORKING GROUP

NCWG
NIPPON Cloud Working Group

MCP対応かA2A対応か

まずはMCP。
他社と差別化をはかるにはA2A。

SAMURAI CLOUD
POWERED BY NIPPON CLOUD WORKING GROUP

NCWG
NIPPON Cloud Working Group

何故今“MCP/A2A”推しなのか？

- ✓ 日本から発出するクラウドビジネスモデルの構築を意義としての「サムライクラウド」
- ✓ ＩＤやアプリケーション、ＵＩ、ＤＡＴＡ連携など日本から発出できるクラウドサービスの技術的意義としての「サムライクラウド」

SAMURAI CLOUD
POWERED BY NIPPON CLOUD WORKING GROUP

NCWG
NIPPON Cloud Working Group

ご清聴ありがとうございました