

ニッポンクラウドワーキンググループ

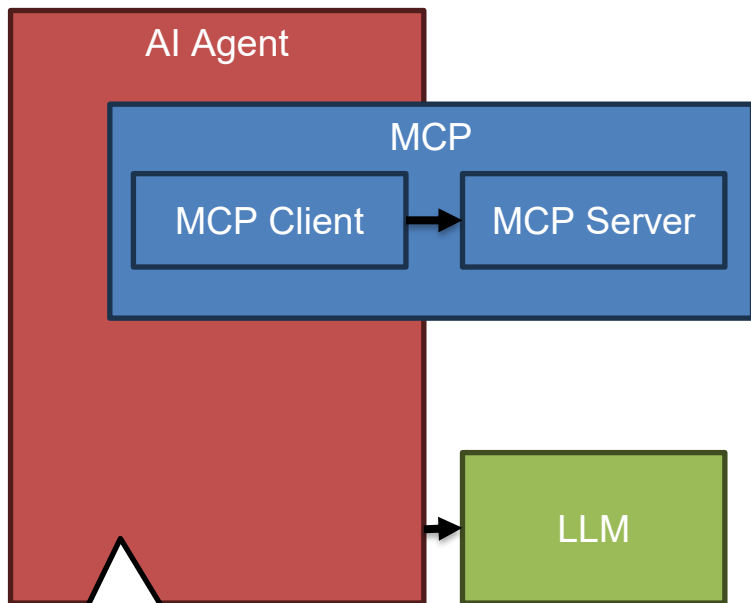
第84回会合
クラウドビジネスサロン

「MCP Apps & Agent Skillsの
クラウドビジネスへの活用！」

2026.09.15

クラウドビジネス推進部会
部会長 藤田 浩之

LLM/AI Agent/MCPのおさらい



※補足: 各AI Agent
はMCP以外、独自の
ツール呼び出しや
機能を有しているこ
とがほとんど

LLM (Large Language Model / 大規模言語モデル)

AIシステムの「頭脳・思考エンジン」。大量のテキストデータから学習した基盤モデル（例: Claude、GPT-4など）。自然言語の理解、テキスト生成、論理的推論、コード生成などを行う。基本的には「**入力されたテキストに対して知的なテキストを返す**」能力に特化。

AI Agent (AIエージェント)

LLMを核にして自律的に動く「作業実行主体（身体）」。
LLM（頭脳）単体では「指示に答える」だけだが、**AI Agentは自ら計画を立て（Planning）、過去のやり取りを記録し（Memory）、外部ツール（Tool Use）を呼び出してタスクを完遂**。「旅行の計画からフライト・ホテルの予約までを自律的に完了させる」といった目標指向型のシステム。

MCP (Model Context Protocol)

AI Agentと外部世界を接続する「標準規格（USB-Cのようなもの）」。
Anthropicがオープンソースとして提唱・公開した通信プロトコル。従来、AIにGoogleカレンダーや各種データベース、社内APIなどの外部システムを繋ぐには、AIごとに個別の接続コード（コネクタ）を書く必要があったが、MCPという共通標準を使うことで、**一度「MCPサーバー」としてツールを作成すれば、どのMCP対応AI Agentからでも即座に利用可能になる**。

MCP Apps

(MCPアプリ)

MCP Appsとは？

MCPの拡張仕様。MCPサーバーがHTMLベースのインタラクティブなUIをAIチャットの会話内に埋め込める仕組み。2026年1月にオープンスタンダードとして公開。

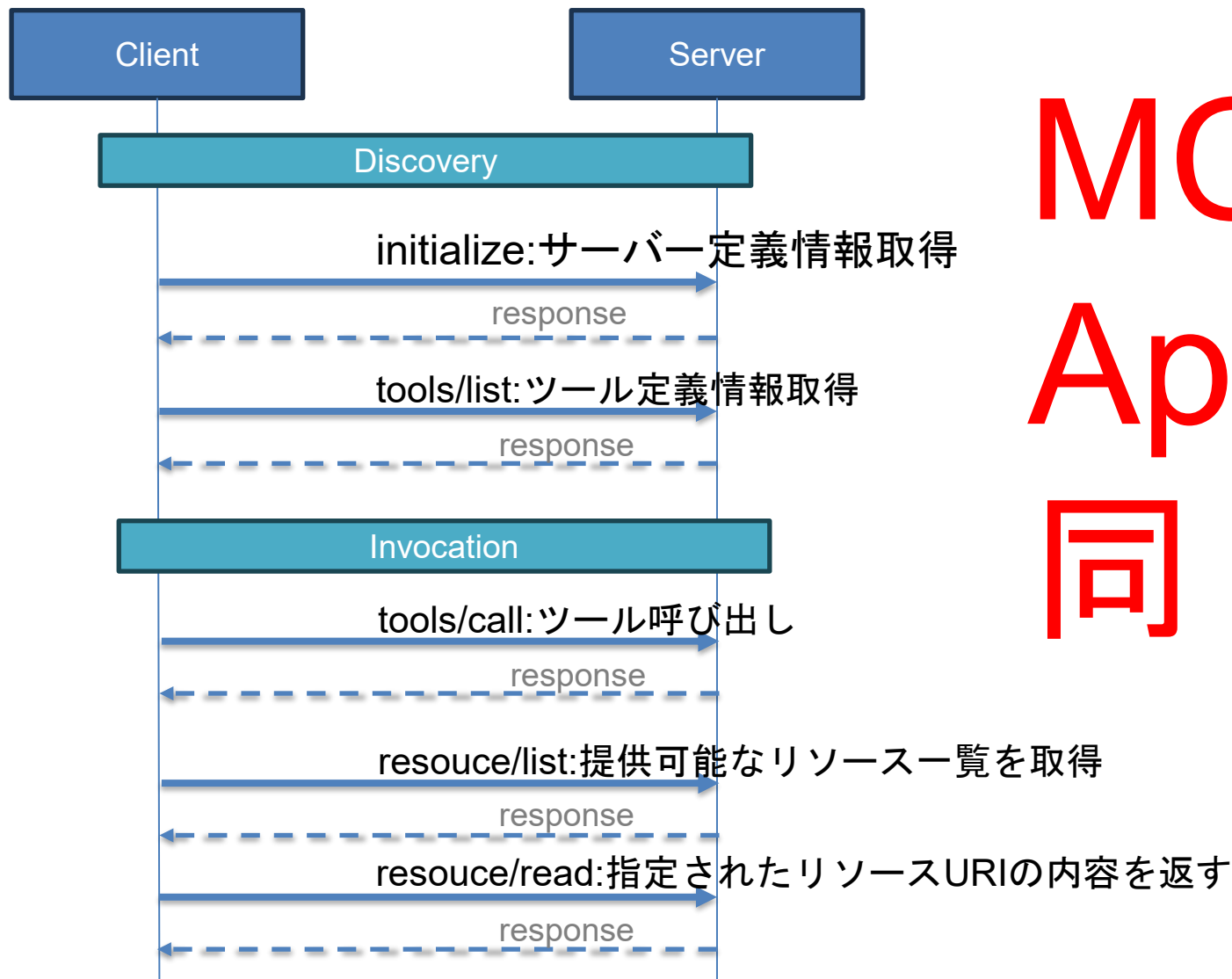
- 単なる「データ連携（Read/Write）」から「体験の提供（UI Rendering）」への進化。
- 必要なUIを、同一コンテキスト内で次々に呼び出せる。
- さまざまな環境で一貫したUIを提供
- セキュリティ
- 省コスト化

背景：テキストチャットの限界

文字だけのやり取りでは、複雑なデータ分析や意思決定に時間がかかる。

課題：情報の断片化、操作のスイッチングコスト。

MCPの処理フロー



MCP
Appsも
同じ

tools/listの応答例

MCP Appsでは、`_meta/ui/resourceUri`というキーで
`ui:hogehoge`のようなuiから始まるURLを返却することで、ツ
ールに対応するリソースのURLを定義する

MCP

```
{
  "jsonrpc": "2.0",
  "id": 1,
  "result": {
    "tools": [
      {
        "name": "get_weather",
        "description": "Get current weather
information for a location",
      },
      {
        . . .
      }
    ]
  }
}
```

MCP Apps

```
{
  "jsonrpc": "2.0",
  "id": 4,
  "result": {
    "tools": [
      {
        "_meta": {
          "ui": {
            "resourceUri": "ui://mcp/ get_weather ",
            "description": " Get current weather
information for a location ",
            "name": " get_weather "
          }
        },
        . . .
      }
    ]
  }
}
```

セキュリティと実行環境

内容：iframe/Sandboxによる分離、権限管理（Capabilities）。

安心材料：ローカル環境や機密データを守りつつ、リッチなUIを動かす仕組み。

MCP-UI：ホストが直接UIを表示

MCP-Apps：ホストはUIを解釈しない

CSP（コンテンツセキュリティポリシー）によるセキュリティコントロール

MCP Apps デモ

行政手続等調査データ(約75,000件)を MCPで自然言語分析可能に

デジタル庁

🔍 キーワードやクリエイターで検索

<<

デジタル庁 デジタル庁

デジタル庁の公式noteです。政策・サービスに関するお知らせやTechブログを発信しています。ウェブサイト:

<https://www.digital.go.jp/> 運用ポリシー:

<https://www.digital.go.jp/social-media-policy/>

+フォロー

デジタル庁Techブログ

行政手続等調査データ
(約75,000件)をMCPで
自然言語分析可能に



<https://digital-gov.note.jp/n/n56aaf580bfb6>

デモMCP詳細

MCPサーバーとして4ツールを提供

1. list_datasets
2. inspect_dataset
3. query_records
4. summarize_records

所管府省庁ごとの手続件数ランキング（上位）を教えてください。先にデータセット構造を確認した上で、出典と品質情報も含めてください。

オンライン未実施の手続にはどんな傾向があるか知りたい。まず全体を集計して、そのあと具体例を数件見せて。

Agent Skills

Agent Skillsとは？

AI Agentに専門知識や具体的な作業手順を指示する
「業務マニュアル（レシピ・手順書）」。

Anthropicが提唱しオープン規格化された仕組みで、
SKILL.md という指示ファイルと関連スクリプト、テンプレートなどをひとつのフォルダにまとめたパッケージ形式のファイル群。

AI Agentに必要な手順やドメイン知識をあらかじめ持たせることで、人間が毎回プロンプトで細かく指示しなくても社内ルールや高度なワークフローに従って自律的に動作。

Agentスキルの構成要素

要素	内容
知識	そのタスクに必要なドメイン知識
手順	どんな順序で考え・回答するか
判断基準	何を重視するか（品質・セキュリティ・速度など）
出力フォーマット	どんな形式で結果を返すか

Agent Skillsのフォルダ構造例

フォルダ構造は自由

skills/a-skill-folder/

—— SKILL.md	# 必須:YAMLフロントマター + Markdown指示
—— scripts/	# 任意:Pythonスクリプト等
—— references/	# 任意:詳細ドキュメント
—— assets/	# 任意:テンプレートやフォント、画像等

Tier 1: メタデータ(name, description)

→ 常時ロード

Tier 2: SKILL.md 本文

→ スキル選択時にロード

Tier 3: references/, scripts/

→ 必要時にオンデマンドロード

記述の基本方針

- ・mdファイルの内容は500行程度推奨
(超える場合は、referencesに分割して記述)
- ・内容は1か所に記述
(複数のファイルで内容の重複なし。トークンの無駄遣いを抑制。)
- ・参照階層1
(参照mdファイルからネストした参照は避ける)

Agentスキル（SKILL.md）の 具体的な記述（yamlフロントマター）

name: my-skill-name

description: このskillが何をするか、いつ使うかを記述する。

name:文字数1～64文字、使用可能文字 小文字英数字とハイフンのみ（a-z, 0-9, -）先頭・末尾不可、連続（--）不可

descriptions:文字数1～1,024文字、三人称で記述（システムプロンプトに注入されるため）、「何をするか」＋「いつ使うか」の両方を含める

Agentスキル（SKILL.md）の 具体的な記述（本文）

#スキル名

##手順

- 1.
- 2.
- 3.

Makrdown形式で、プ
ロンプトを書く

##フォーマット

Agentスキル（SKILL.md）の 具体的な記述（参照例）

#Skill Name

手順

1. 以下のコマンドを実行する

``bash scripts/script.sh``

2. 出力結果のエラー有無を確認する

3. 結果を日本語で分かりやすく要約する

～～～

Table References

- ○○ の場合, ``references/finance.md`` を読む

- xxの場合, read ``references/product.md`` を読む

Agentスキル (SKILL.md) の 具体的な記述 (MCPの参照例)

#Skill Name

Tool References

- Use the `BigQuery:bigquery\_schema` tool to inspect table schemas
- Use the `GitHub:create\_issue` tool to create issues

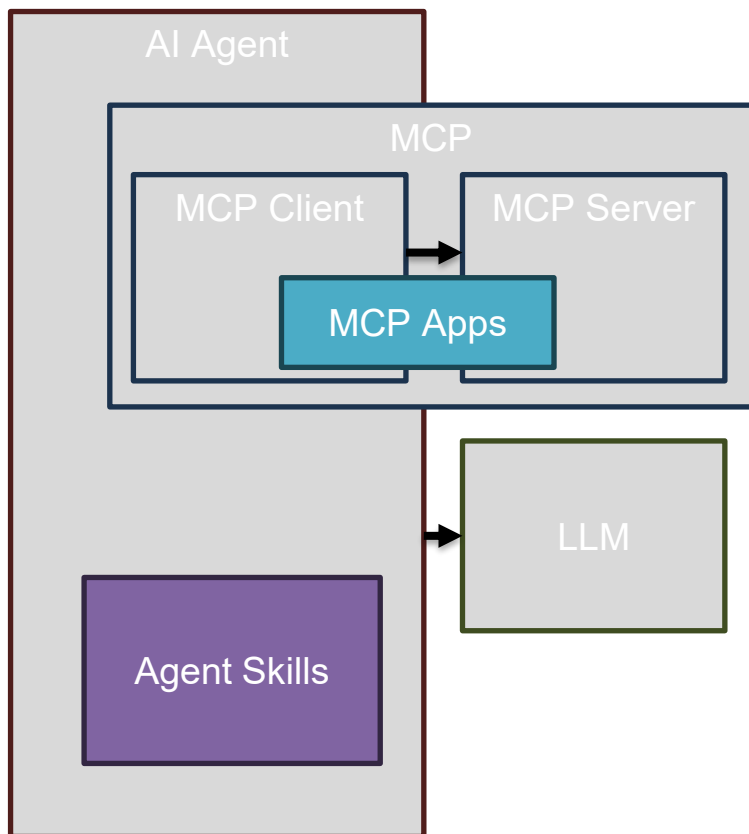
サーバー名:ツール名 の形式が必須

Agent Skills

デモ

まとめ

MCP Apps / Agent Skills



MCP Apps (MCP・アプリ)

MCP Appsは、ツールの実行結果としてHTMLや操作可能なウィジェット（グラフ、地図、入力フォームなど）をチャット画面上に直接レンダリングできるようにした機能・アプリ形態。

AIが言葉で長々と説明する代わりに、ユーザーが直接触れる画面（UI）を提供することが可能。

Q. AI Agentが直接必要なUIを生成すれば良いのでは？

A. 究極的には可能だが、現状は下記課題を解決

1. 生成コストを減らす
⇒時間、消費電力、利用料金
2. 生成されるUIの一貫性・専門性を担保する

Agent Skills (エージェント・スキル)

AI Agentに専門知識や具体的な作業手順を指示する「業務マニュアル（レシピ・手順書）」。

Anthropicが提唱しオープン規格化された仕組みで、SKILL.md という指示ファイルと関連スクリプト、テンプレートなどをひとつのフォルダにまとめたパッケージ形式のファイル群。AI Agentに必要な手順やドメイン知識をあらかじめ持たせることで、人間が毎回プロンプトで細かく指示しなくても社内ルールや高度なワークフローに従って自律的に動作。

ご清聴ありがとうございました