Agents SDK はじめの一歩

Cloudflare Meetup Tokyo Vol.7 - 2025.03.14

自己紹介

- 新居田 晃史（にいだ あきふみ）

- 所属
  - JBアドバンスト・テクノロジー株式会社
    先進技術研究所 – Technical Expert

- 日本最速ITエンジニア（※週刊BCN編集部調べ）
  - フルマラソン 2:29:56

- コミュニティ活動
  - JAWS-UG 横浜支部
  - AWS Community Builder – Container
  - Cloudflare Meetup
  - ChatGPT Meetup Tokyo
  - JAWS DAYS 2025 実行委員長

Twitter @nid777
Facebook Akifumi Niida

AI Agentとは

「AIエージェント」とは、複雑な目標を自律的に遂行できるAIシステム

LLMの登場によって、与えられた目標を達成するために必要な行動を自ら決定し、実行することができることが可能に

出展：「LangChainとLangGraphによるRAG・AIエージェント[実践]入門」第8章より

なぜ今AIエージェントを学ぶのか

エンジニアとして日々感じるAIエージェントの便利さ

これらの体験は今後、ほぼすべての業種、業務へ

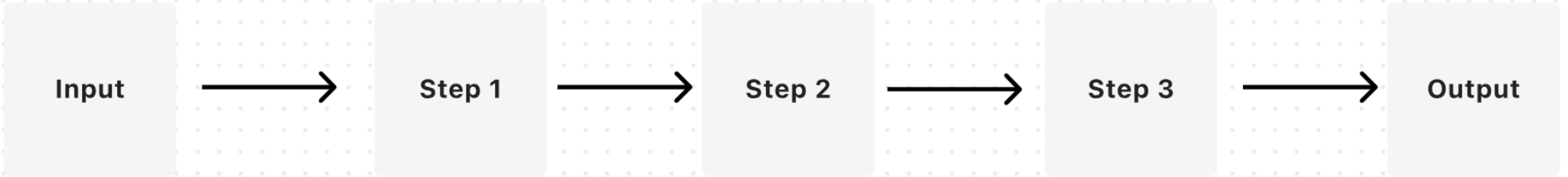
〇〇版Devinを作るのは私たちエンジニア

例：休暇の予約

休暇の予約などのコンテキストでエージェントがどのように機能するのか

従来の自動化システム

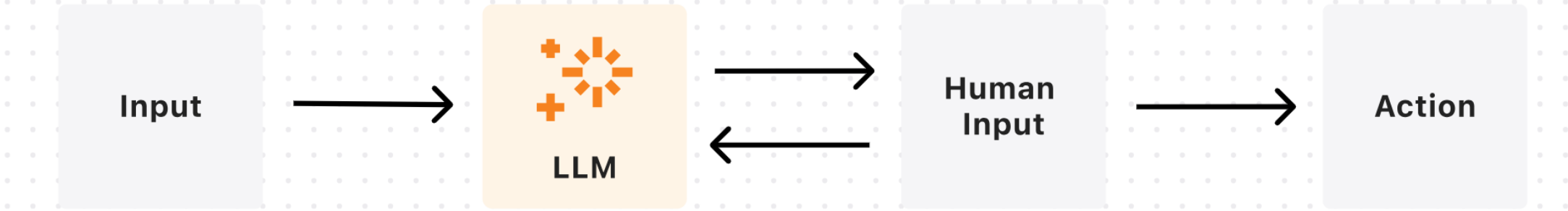
事前に決められたシーケンスに従う



- 具体的な入力（日付、場所、予算）
- 定義済みのAPIエンドポイントを固定順序で呼び出し
- プログラムに基づいて結果を返却
- 予期せぬ状況が発生した場合は対応不可

https://developers.cloudflare.com/agents/concepts/what-are-agents/

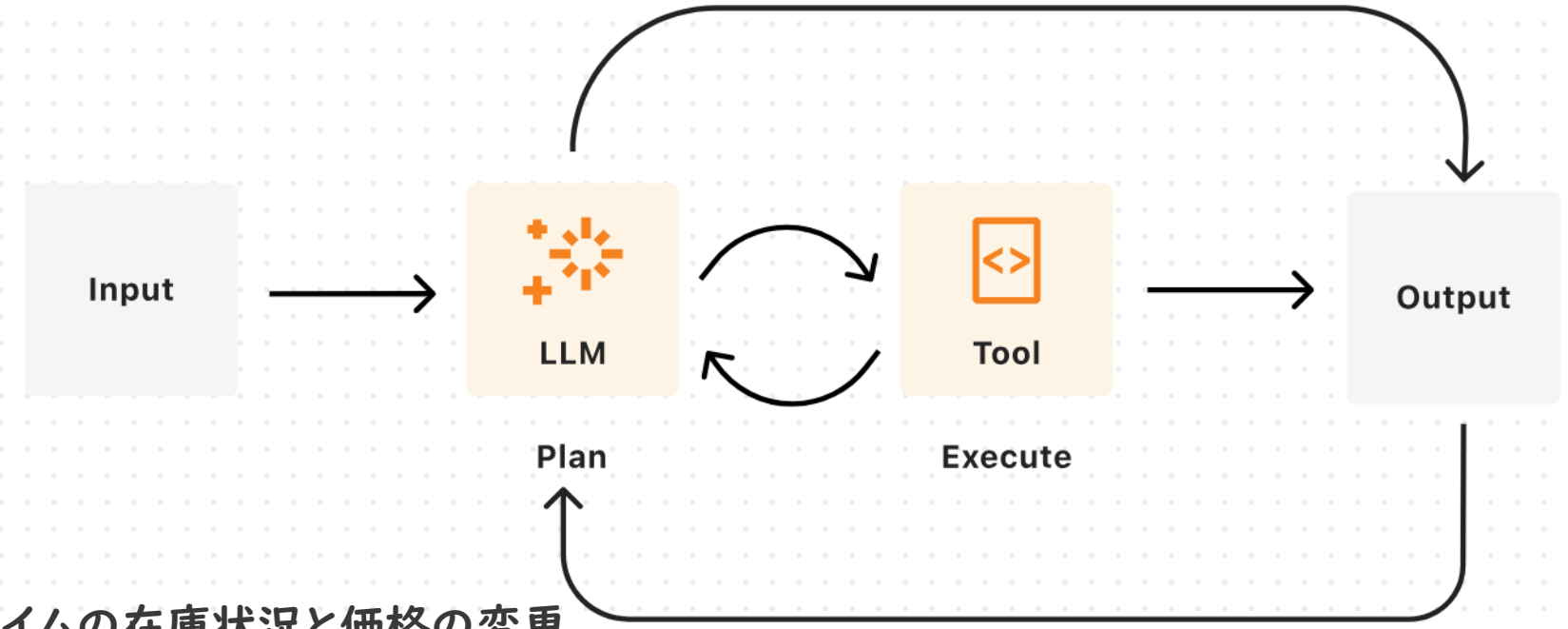
Copilotは次のようなインテリジェントなアシスタントとして機能



- 利用者の好みに応じてホテルや旅程の提案を提供
- 自然言語によるクエリを理解し、応答
- ガイダンスと提案を提供
- 実行には人間の意思決定と行動が必要

https://developers.cloudflare.com/agents/concepts/what-are-agents/

AI の判断能力と関連ツールの呼び出し能力を組み合わせてタスクを実行



- リアルタイムの在庫状況と価格の変更
- 制約の動的な優先順位付け
- 失敗から回復する能力
- 中間結果に基づく適応的な意思決定

https://developers.cloudflare.com/agents/concepts/what-are-agents/

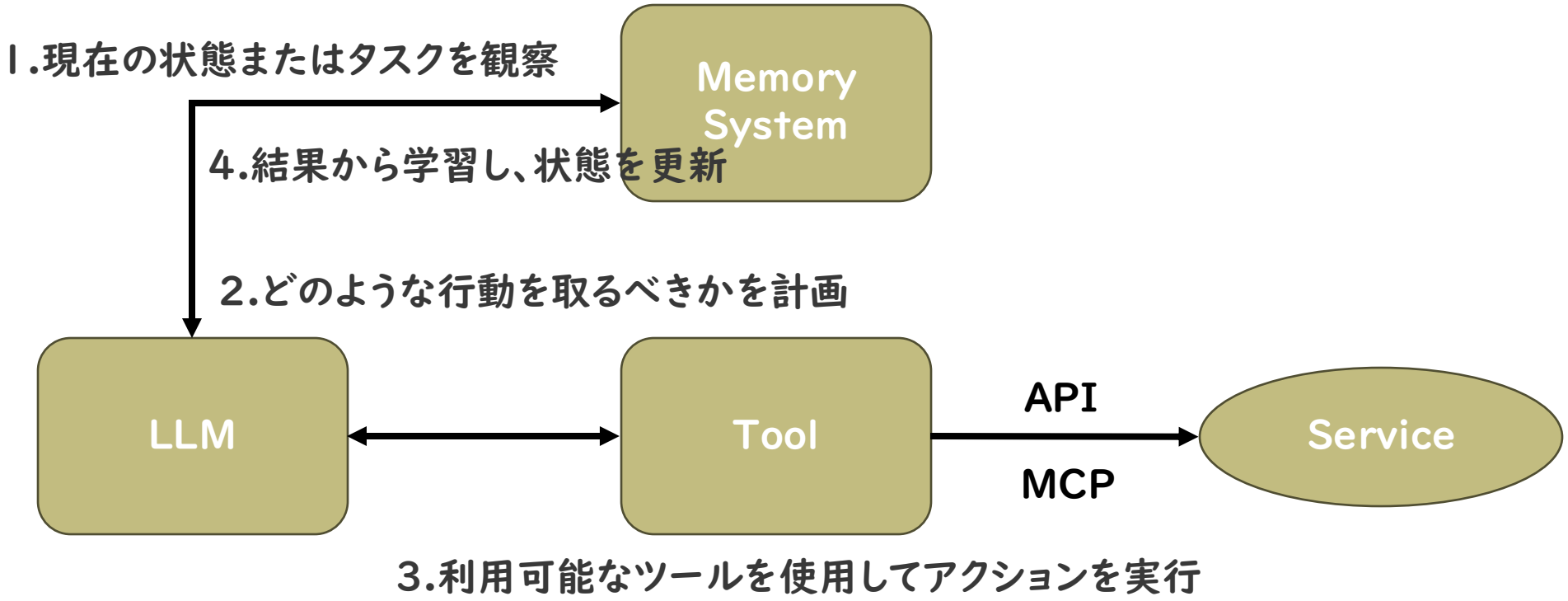
エージェントシステムの 3 つの主要コンポーネント

1. **Decision Engine:** アクションステップを決定するLLM

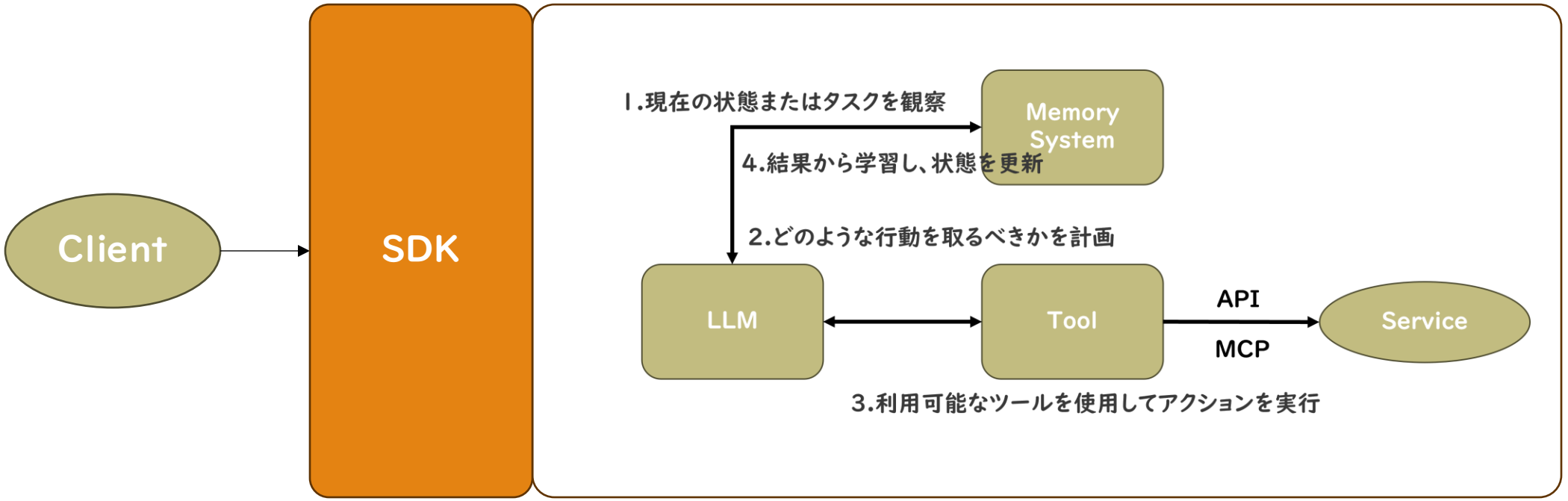
2. **Tool Integration:** エージェントが利用できる API、機能、サービス

3. **Memory System:** コンテキストを維持し、タスクの進行状況を追跡

エージェントの働き


1.現在の状態またはタスクを観察
Memory System
4.結果から学習し、状態を更新
2.どのような行動を取るべきかを計画
LLM
Tool
API
MCP
Service
3.利用可能なツールを使用してアクションを実行

Agents SDKとは




```
import { Agent } from "agents-sdk";

class MyAgent extends Agent {
  // Define methods on the Agent
}

export default MyAgent;
```

- クライアントからエージェントへの接続
- エージェントの状態保存
- エージェントが公開するメソッド
- エラー処理

https://developers.cloudflare.com/agents/api-reference/sdk/

インストール

まずはスターターキットが理解に役立つ

```
npm create cloudflare@latest agents-starter -- --template="cloudflare/agents-starter"
```

既存プロジェクトに組み込む場合はこちら

```
npm i agents-sdk
```

https://developers.cloudflare.com/changelog/2025-02-25-agents-sdk/

デプロイ

```
npm run deploy
```

wranglerを事前にセットアップしておく

https://zenn.dev/kameoncloud/articles/1fac9762aab4ec

Durable Objectsを使用するので、WorkersのプランがFreeだと以下のエラーが出る

```
In order to use Durable Objects, you must switch to a paid plan at
https://dash.cloudflare.com/f0835162f7500cd0957f828b4dfdccab/workers/plans. [code: 10084]
```

Memory System

this.setState（高レベルAPI）でエージェントの状態を管理

```
export class MyAgent extends Agent {
    …
    // Handle incoming messages
    async onMessage(message) {
        if (message.type === "update") {
            this.setState({
                ...this.state,
                ...message.data,
            });
        }
    }
    …
}
```

実態はSQL Lite in Durable Object
参考：亀田さんブログ

https://zenn.dev/kameoncloud/articles/675562016 2d430

https://developers.cloudflare.com/agents/examples/manage-and-sync-state/

Toolの追加

src/tools.ts で処理を追加可能
Xにポストする例

```
…
const postToX = tool({
  description: "post a message to x",
  parameters: z.object({ message: z.string() }),
  execute: async ({ message }) => {
    console.log(`Posting to X: ${message}`);
    return `Posted to X: ${message}`;
  },
});
…

export const executions = {
  …
  postToX: async ({ message }: { message: string }) => {
    // Xにポストする処理をここに記述
    return `Posted to X: ${message}`;
  }
};
```

Toolを追加するだけでエージェントが
自動的に使用してくれる

SDKの全体像を理解したい人はこちらのブログがおすすめです

https://note.com/kyutaro15/n/n34bf7b99b5fb?sub_rt=share_pw

まとめ

- AIエージェント時代に備えよ
- 従来のアプリケーション設計は応用できる
- エージェントに計画を立てさせてツールを使う部分などはやってみれば理解がはかどる
- Cloudflare workersの開発者体験でエージェントを作れるのが良い
- LLMが正しく計画を立てているか、期待されるレスポンスがあるかなどは観測できるようにしたい