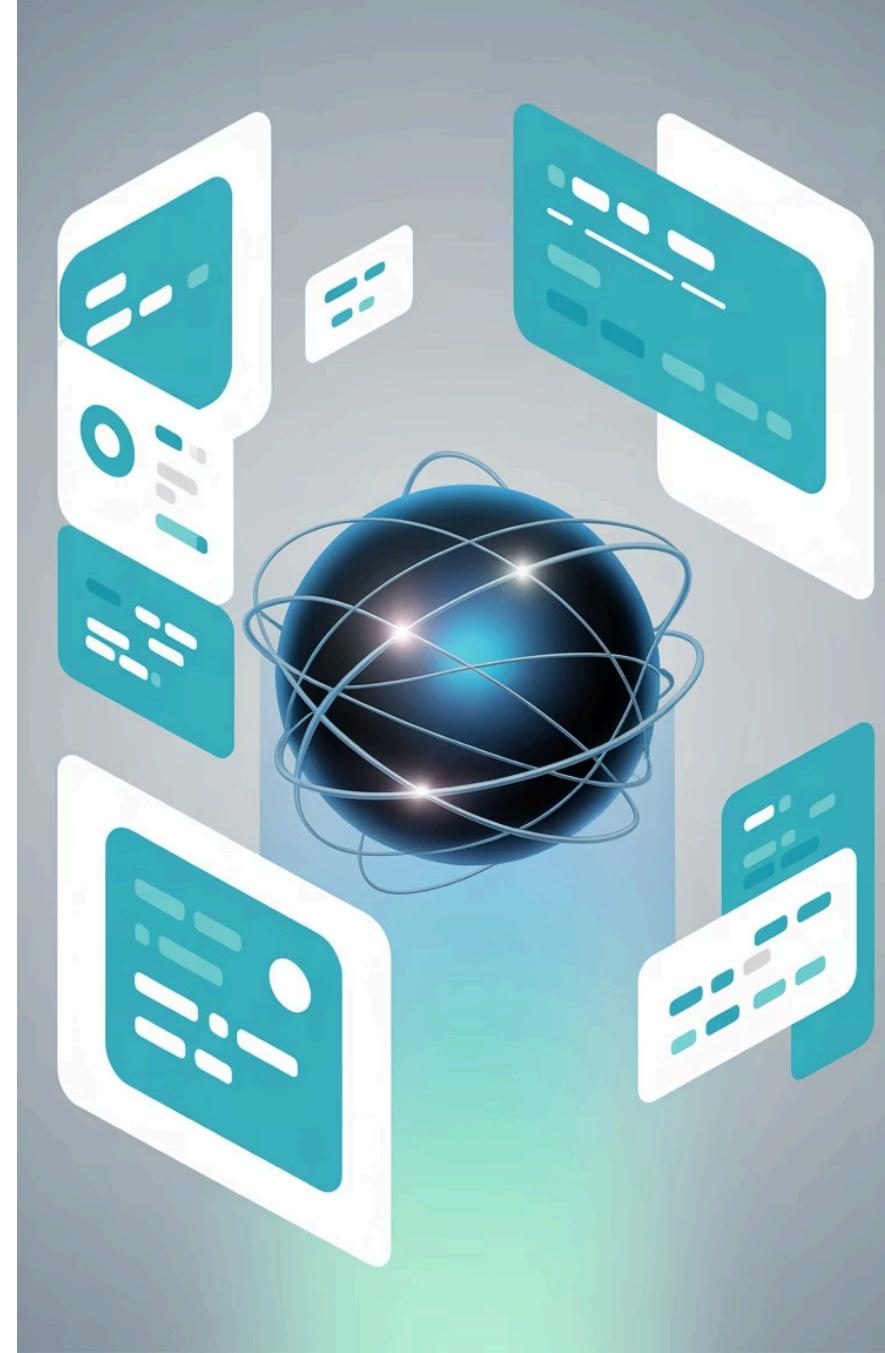


Prompt、Agent、MCP 概念与应用



Prompt Enipunst AI
End Engineering Tool



Adventure Mode

System Prompt

...
Penteact espoopal roomblt copilA

Demeetuing at lopairinolit at IOUJB

User Prompt

...
Cetteaot aspunoid roomlot tcpiA

Cenplacion la rectuir at VUEER

Generate Response

Craft exceptional AI Interactions

AI 基本概念

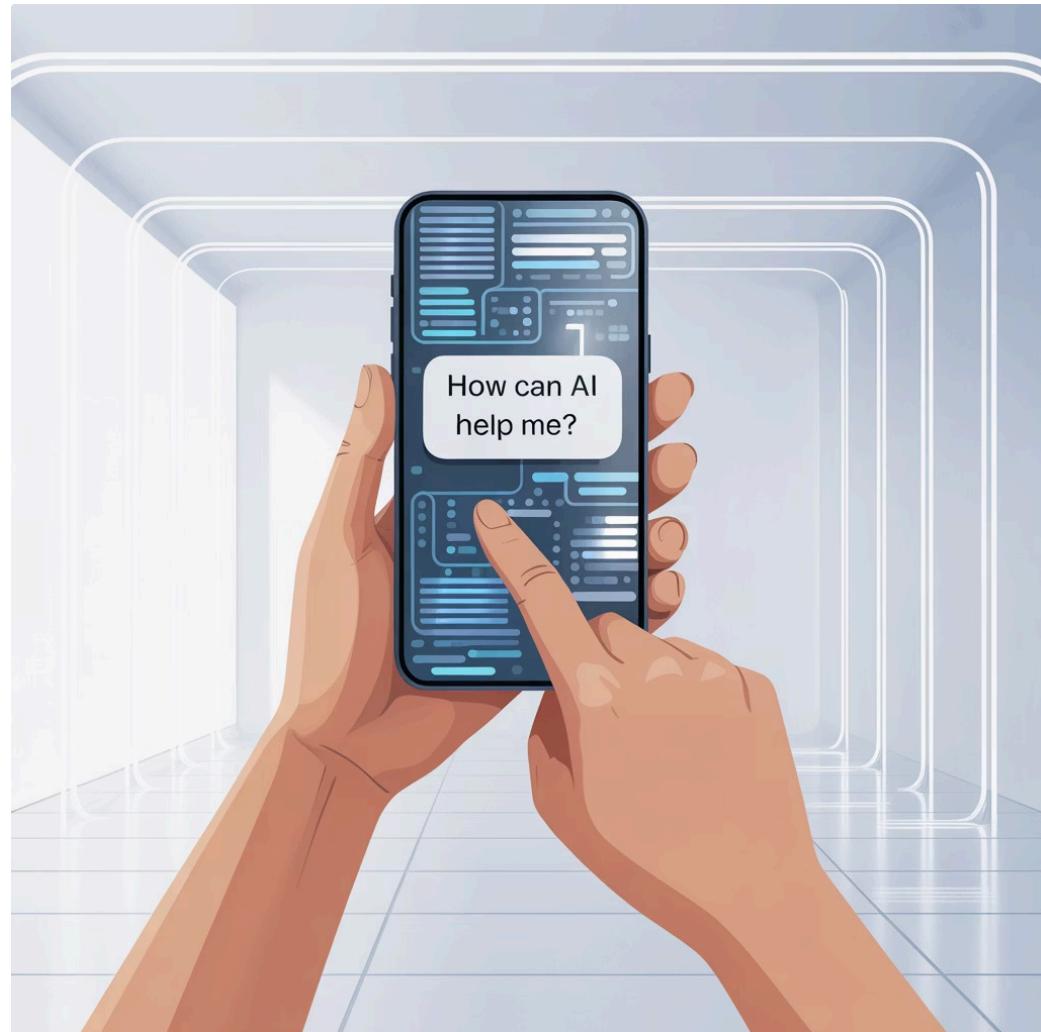
Prompt (提示词)

- User Prompt：使用者输入的讯息
- System Prompt：定义 AI 的角色、性格、背景
- 个性化提示：结合使用者需求与系统提示，产生更贴近情境的回应

提示词类型详解

User Prompt

使用者输入的讯息，直接告诉AI需要什么样的回答或执行什么样的任务



System Prompt

定义 AI 的角色、性格、背景，设定AI应该如何回应

A screenshot of a web-based AI configuration interface. At the top, there are tabs for "Dashboard", "Roles", and "Permissions", along with buttons for "Add Role" and "Create Role". The main area is titled "AI Configuration Panel". It shows three rows of role settings with toggle switches:

- Row 1: Admin (switched on), Editor (switched on), Viewer (switched on)
- Row 2: Auditor (switched off), Moderator (switched off), Data Processor (switched off)
- Row 3: Auditor (switched off), Moderator (switched off), Data Processor (switched on)

Below the roles, there is a section for "Compliance" with a note about "Priority Data Processing" and a "Create Role" button. A sidebar on the left lists "Dashboard", "DOI Overview", "Permissions", and "Audit Logs". At the bottom, there is a footer with links for "Terms of Service" and "Privacy Policy". An illustration of a person interacting with a large screen displaying the interface is visible in the bottom right corner.



个性化提示的力量

个性化提示：结合使用者需求与系统提示，产生更贴近情境的回应

通过结合用户的具体需求和系统设定的角色定位，AI能够提供更符合特定场景和个人需求的回答，大大提高了交互的效率和满意度。

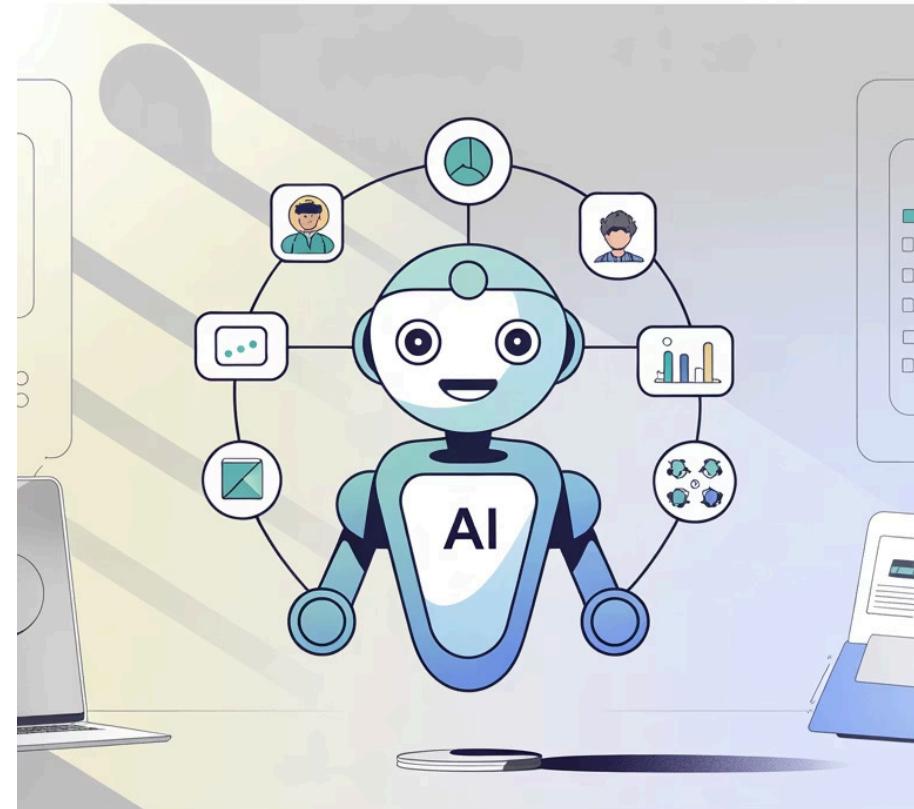
AI 代理 (Agent) 概述

AI 回答问题有限，任务执行仍需人类操作

AutoGPT 范例：协助管理电脑档案

Agent 定义：作为 AI 模型与使用者之间的桥梁

能调用各种代理工具 (Agent Tools) 来完成任务



Unlock seamless collaboration

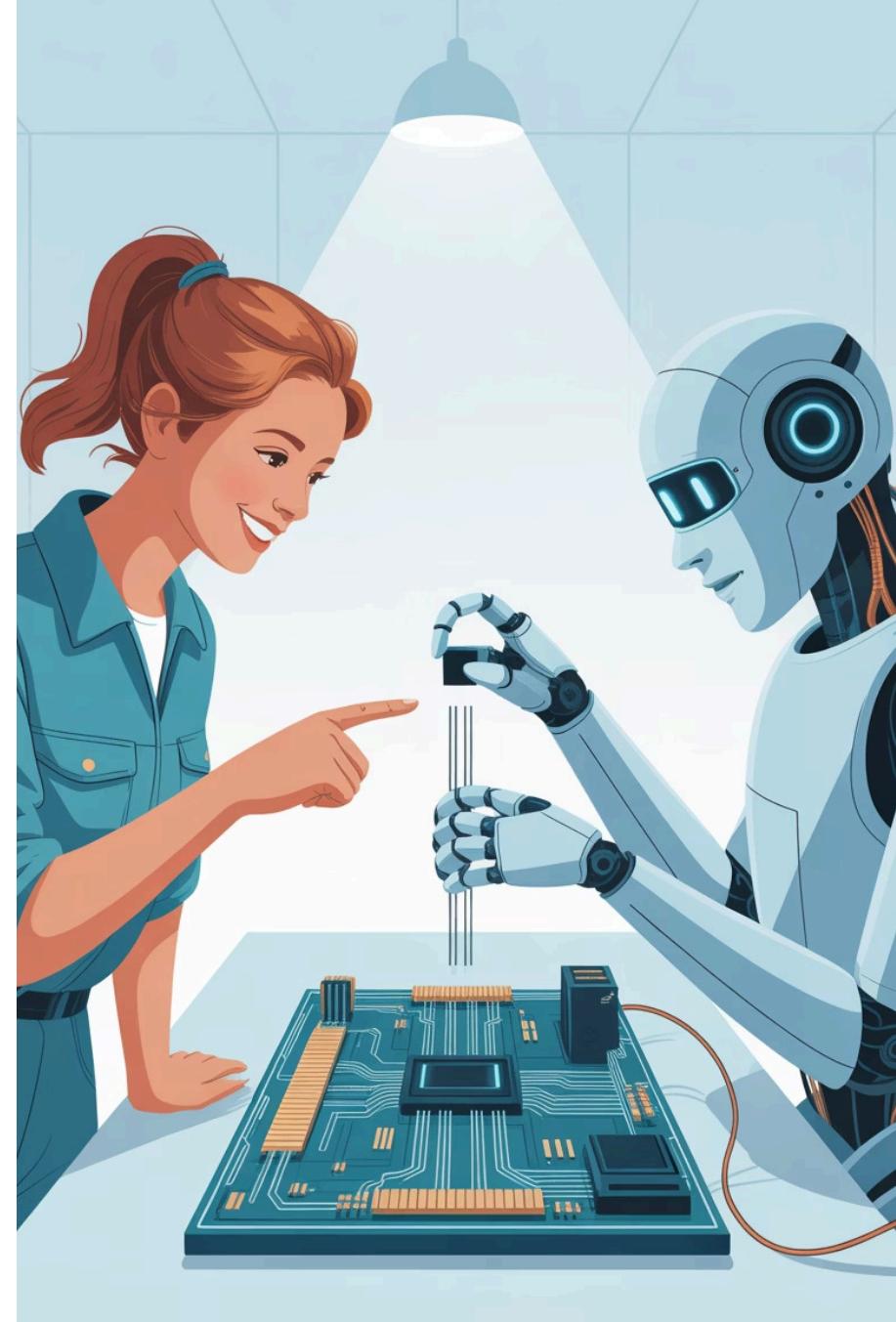
Your **AI-powered partner**
for efficient workflows

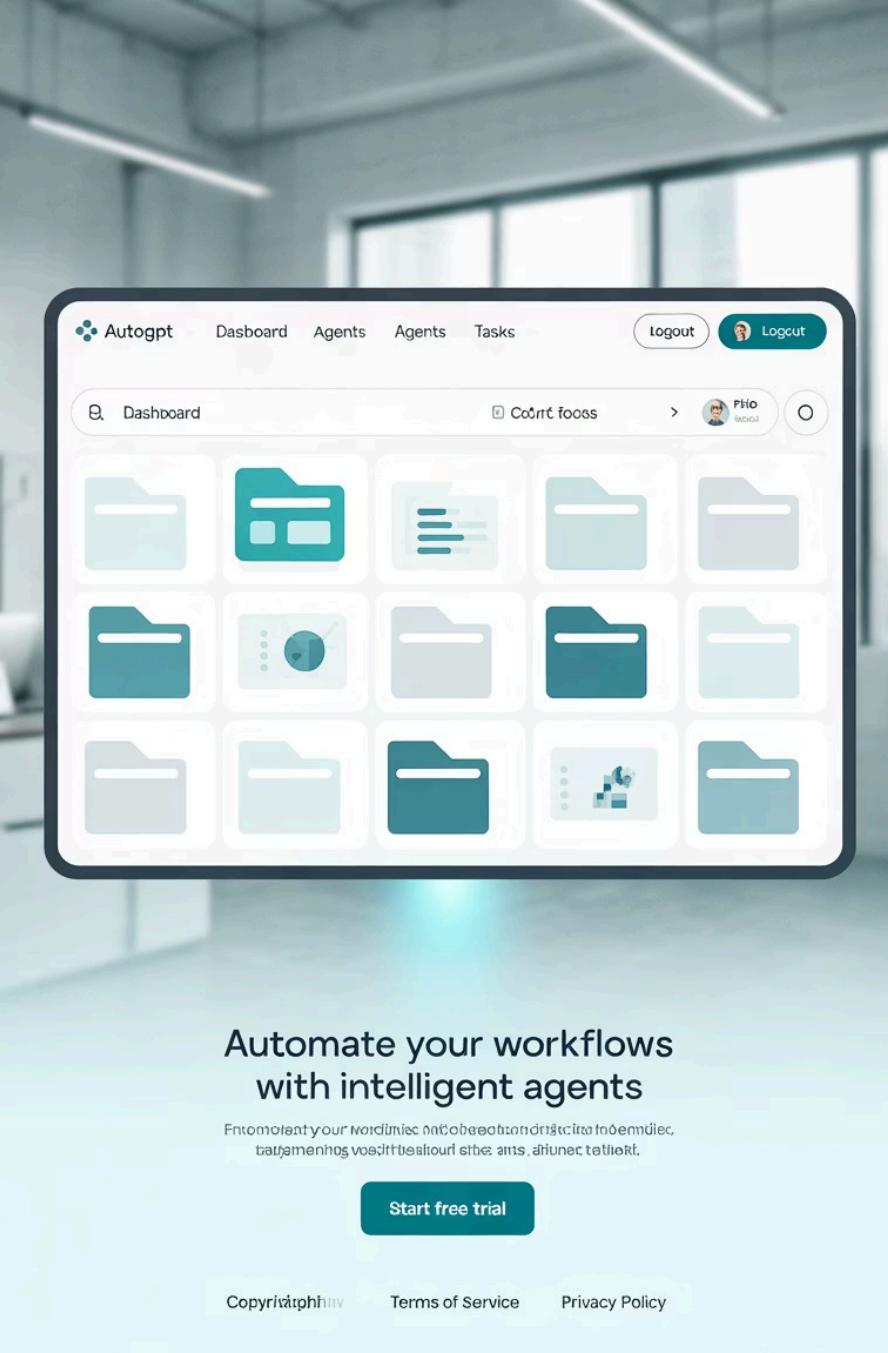
Explore plans

AI 代理的局限性

⚠ AI 回答问题有限，任务执行仍需人类操作

尽管AI能够提供信息和建议，但在实际执行复杂任务时，仍然需要人类的参与和操作。这是当前AI技术的一个重要限制。





AutoGPT：AI代理的实例应用

AutoGPT 范例：协助管理电脑档案

AutoGPT作为一种AI代理的实现，能够帮助用户管理电脑文件，展示了AI代理如何在特定领域提供实用价值。

Automate your workflows
with intelligent agents

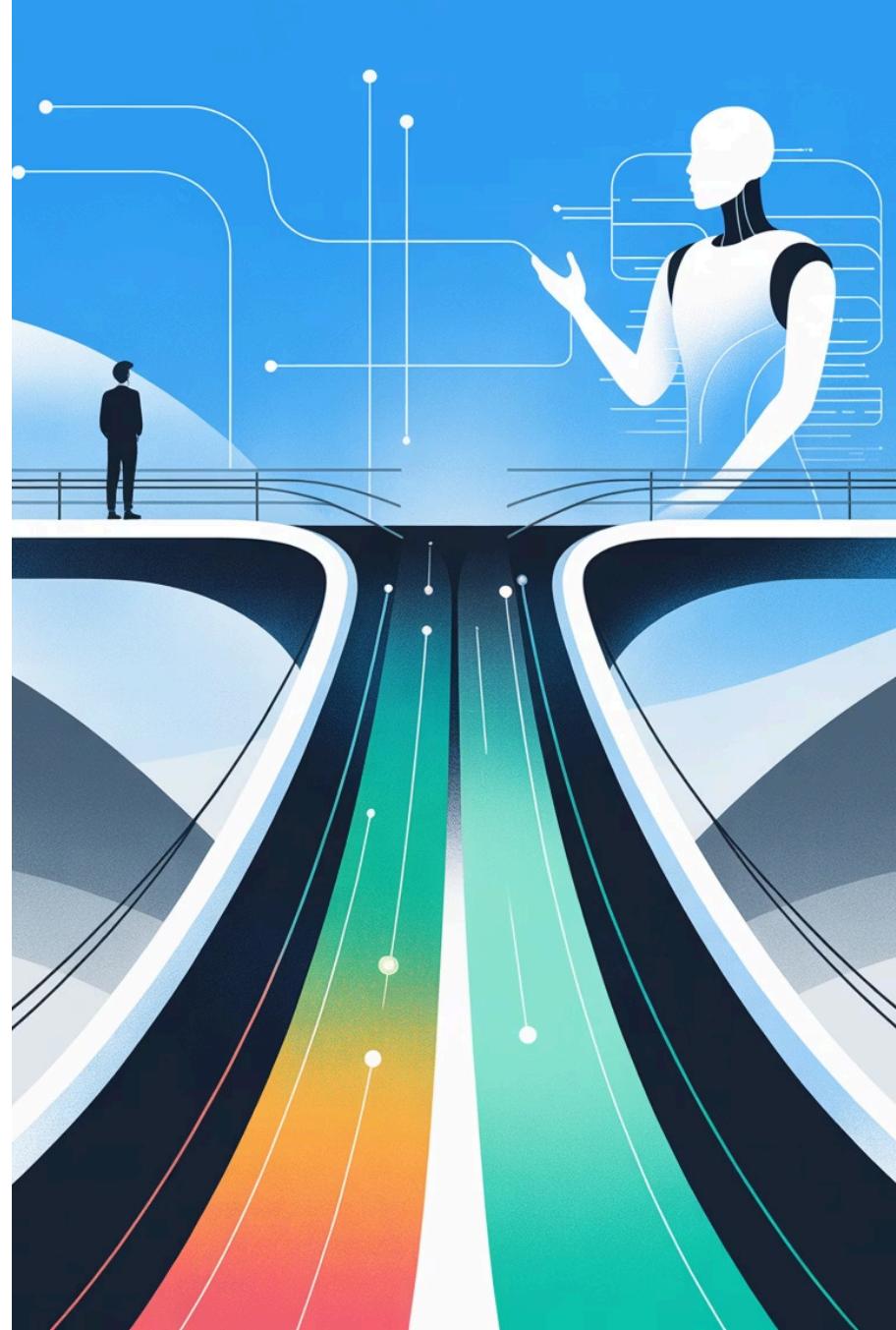
Automate your workflows with intelligent agents.
协管档案，轻松完成工作。

Start free trial

Agent 的核心定义

AI模型与使用者之间的桥梁

Agent作为连接用户和AI模型的中介，能够理解用户需求并调动适当的AI能力来满足这些需求。



代理工具 (Agent Tools)

能调用各种[代理工具](#)来完成任务



网络搜索

查询最新信息

$$\frac{f}{dx}$$

计算工具

处理数学问题



日程管理

安排时间和提醒



文档处理

创建和编辑文件

功能呼叫 (Function Calling)

问题：

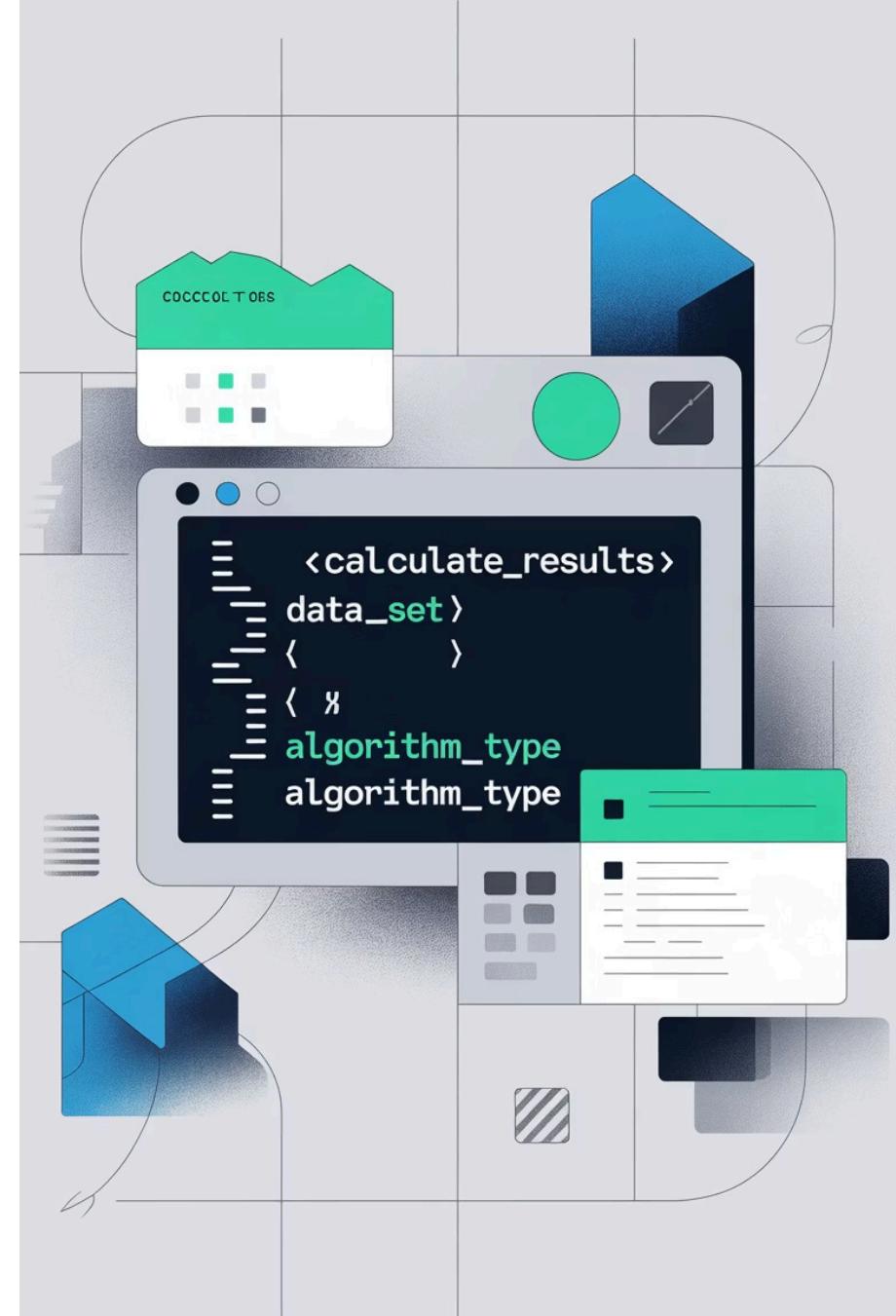
AI 回应格式可能不一致

解决方案：

Function Calling

- 统一工具描述与 AI 输出格式
- 提高开发与训练效率

限制：目前不同公司 API 标准仍未统一



Function Calling 的优势



统一格式

确保AI输出的一致性，便于系统处理



提高效率

简化开发流程，减少格式转换的工作



易于集成

便于与其他系统和工具无缝对接



Function Calling 的局限性

- ✖ 限制：目前不同公司 API 标准仍未统一

尽管Function Calling提供了统一格式的解决方案，但行业内不同公司的API标准仍然存在差异，这给开发者带来了额外的适配工作。

MCP 协议 (Model Context Protocol)

作用：标准化 AI 代理与工具服务的互动



MCP 服务器

提供工具、资源、提示模板（可在本地或网络运行）



MCP 客户端

负责与模型交互，传递资源



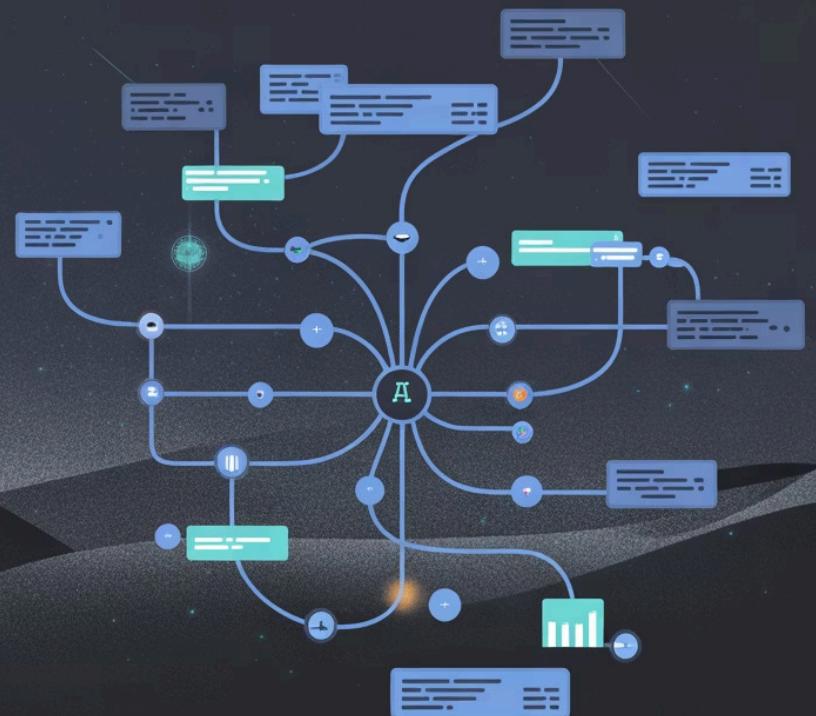
MCP Protocol Architecture

MCP 服务器详解

MCP 服务器：提供工具、资源、提示模板

MCP服务器是整个协议的核心组件，负责存储和提供各种工具和资源，可以在本地计算机或远程网络上运行，为AI代理提供必要的功能支持。





MCP 客户端功能

MCP 客户端：负责与模型交互，传递资源

MCP客户端作为用户与AI模型之间的接口，负责将用户的需求传递给模型，同时从MCP服务器获取必要的资源和工具，确保整个交互过程的顺畅进行。

MCP 的两种沟通方式



系统提示 (System Prompt)

通过系统级别的指令定义AI行为

函数调用 (Function Calling)

通过标准化函数接口执行特定任务

AI 协作架构概览

代理运作流程

从 MCP 服务器检索工具

转换为系统提示 / 函数调用格式

与使用者提示一同传给模型

调用工具（如 `web_browse`）并整合结果

生成回应给使用者

代理运作流程：第一步

步骤1：从 MCP 服务器检索工具

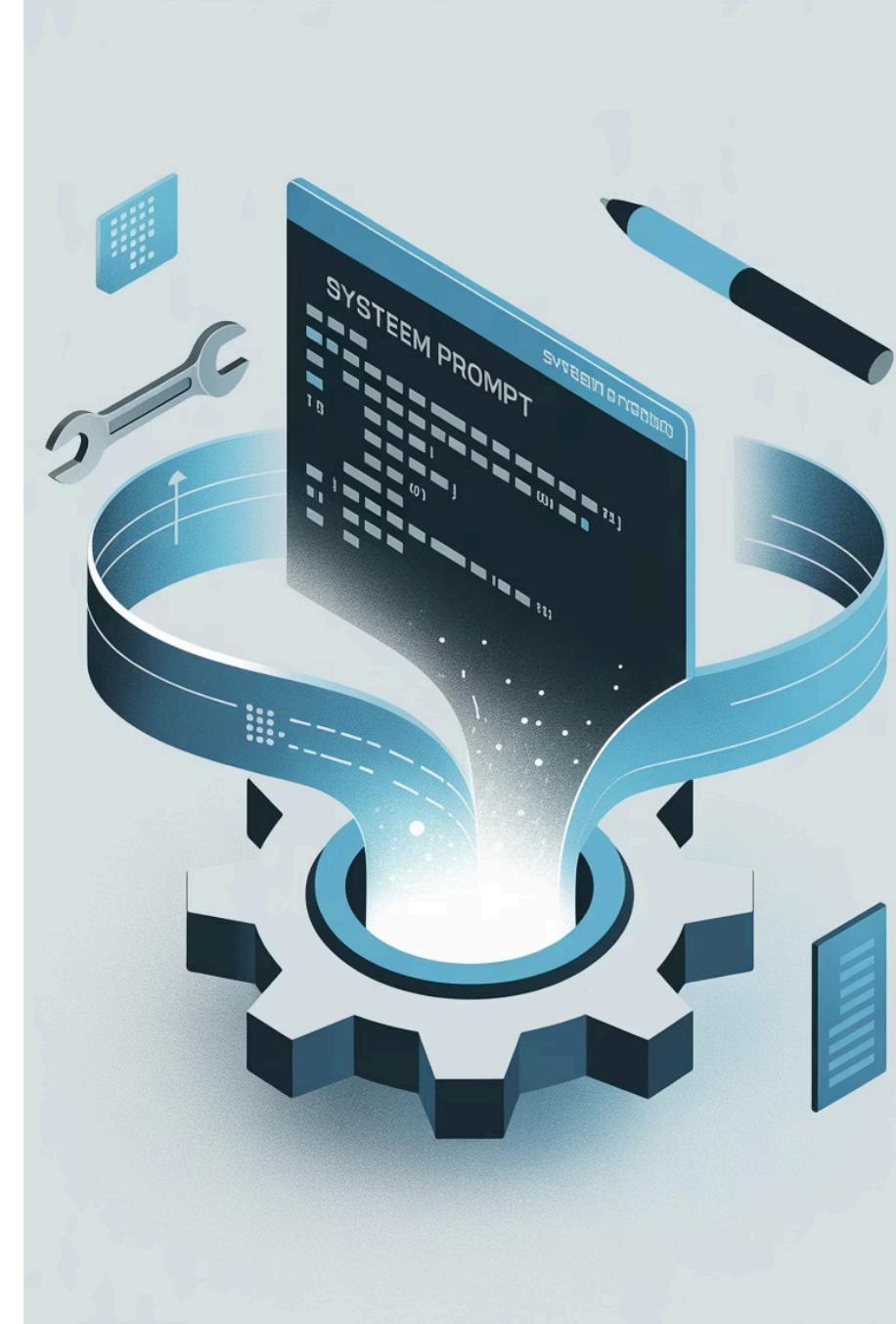
AI代理首先需要从MCP服务器获取完成任务所需的各种工具和资源，这是整个流程的起点，确保代理拥有执行任务的能力。



代理运作流程：第二步

步骤2：转换为系统提示 / 函数调用格式

获取工具后，AI代理需要将这些工具转换为系统能够理解的格式，可以是系统提示或函数调用的形式，为后续的处理做好准备。

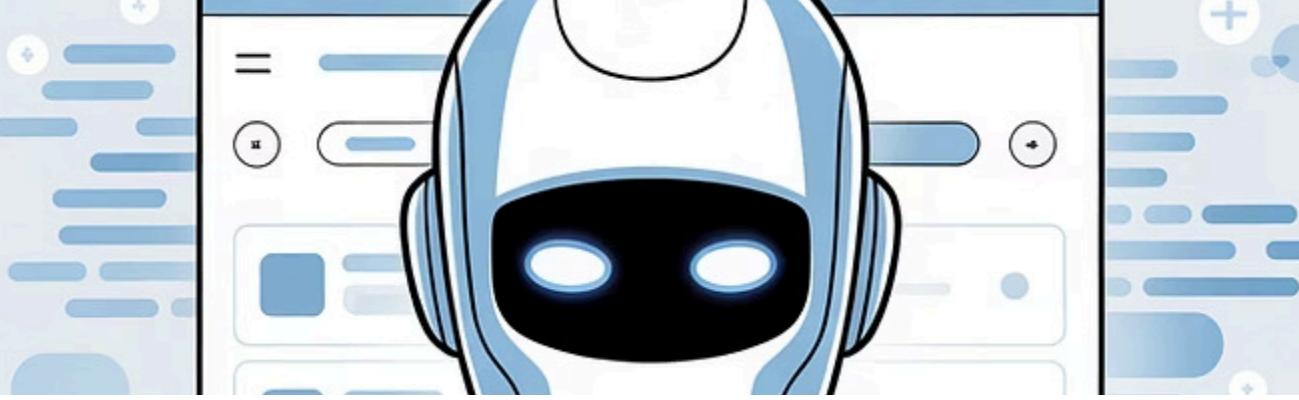




代理运作流程：第三步

步骤3：与使用者提示一同传给模型

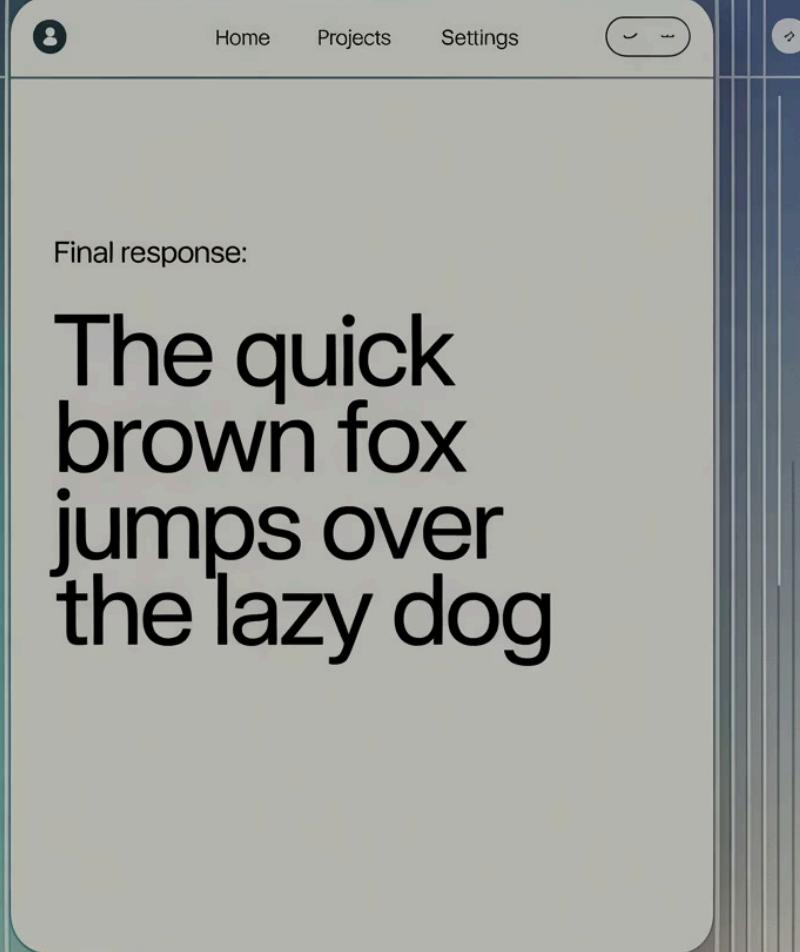
转换完成后，AI代理将用户的提示与转换后的工具信息一起传递给AI模型，让模型能够理解用户需求并调用适当的工具。



代理运作流程：第四步

步骤4：调用工具并整合结果

AI模型根据用户需求调用相应的工具（如网络浏览工具），获取必要的信息，并将这些信息进行整合和处理。



代理运作流程：第五步

步骤5：生成回应给使用者

最后，AI代理根据整合的结果生成最终的回应，并将其呈现给用户，完成整个交互过程。



整体架构：协同运作

如齿轮般协同运作 (User Prompt + System Prompt + Agent + MCP + 工具)

整个AI系统的各个组件就像精密的齿轮一样紧密配合，共同工作，确保系统能够高效地满足用户的各种需求。

未来展望：挑战与机遇

挑战

AI 技术快速进步带来挑战与焦虑



机遇

鼓励积极学习，主动理解并拥抱 AI 变革





结语：拥抱AI新时代

积极学习

持续更新知识，跟上AI发展步伐

主动理解

深入了解AI技术原理和应用场景

拥抱变革

将AI视为助手而非威胁，探索合作可能