資料來源：ChatGPT　編輯：屏東大學 周國華老師

以下為 **MCP（Model Context Protocol，模型情境協議）** 的清楚說明與應用整理，幫助您快速理解其概念、架構與實務角色。

☑ MCP 是什麼？

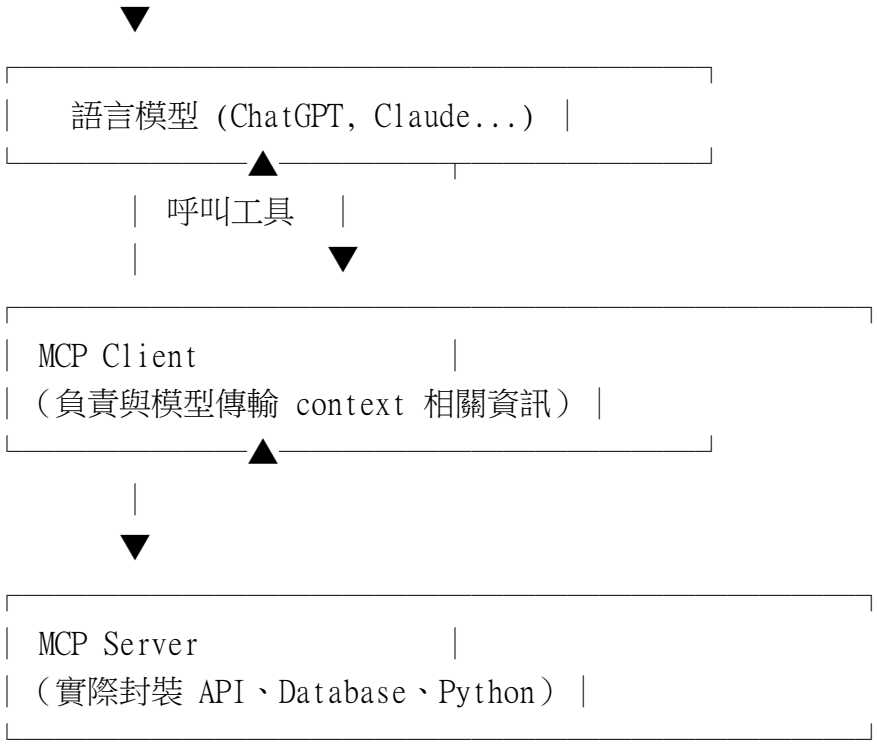
MCP（Model Context Protocol，模型情境協議） 是 OpenAI 在 2024 年提出的一種標準化協議，用於讓大型語言模型（LLM）能夠安全、統一地連接到外部資料、工具與使用者情境（context），提供一致的「模型與外部世界溝通方式」。

☑ 核心目的

目的	說明
標準化模型與外部工具的互動	讓 AI 模型能使用 API、資料庫、程式碼執行器等工具，而不是依賴各家廠商的私有接口。
安全可控的工具使用流程	每一次工具請求都需經由「允許/拒絕」，避免模型直接執行高風險操作（如寫檔案、刪資料）。
長期記憶與上下文管理	協助模型保存使用者偏好、歷史對話、工作任務狀態。
讓 AI 成為可擴充的“作業系統層”	使用者未來可以自己設計工具、知識庫，模型直接使用。

☑ MCP 的運作架構

問題/指令



☑ MCP 與現有技術的比較

技術	功能	與 MCP 差異
OpenAI Plugins	ChatGPT 插件架構	MCP 是更底層標準，插件是其應用之一
Tool Calling / Function Calling	讓模型調用 API	MCP = 多種工具 + 記憶 + 安全機制
LangChain / LlamaIndex	AI 工具框架	MCP 更偏「通訊標準」而非程式庫
Agentic AI	AI 自動執行任務	MCP 是 Agent 使用外部工具的標準方式

☑ 實際應用範例

❑ 查詢資料庫

模型說：「請幫我查一下昨天銷售報表。」

→ MCP manager：

- 把此需求轉成 query
- 呼叫資料庫 API（透過 MCP Server）
- 回傳模型可理解的 json 格式

---

❷ 自動化會議紀錄

使用者：「幫我總結上週會議紀錄
並更新任務清單到 Notion。」

✔ 模型 → MCP：查會議錄音 → 轉文字
✔ 模型 → MCP：總結並產生任務 → 更新 Notion

---

❸ 管理使用者偏好與記憶（Memory）

使用者：
「從現在開始，我希望報表統一用 Excel 並用繁體中文標題。」
✔ MCP 可把此偏好寫入 memory server → 未來自動套用。

☑ MCP 的 3 大構成項目

元件	功能
Context	儲存使用者偏好、任務狀態、長期記憶
Tools	API、資料庫、Python 執行等具體操作能力
Messages	模型 ↔ MCP server 之間的溝通協議格式

☑ 用一句話總結 MCP

MCP 就是「讓 AI 模型像作業系統一樣，可以安全地使用外部工具、資料與記憶的通訊標準」。

如您需要：

- MCP 架構圖（PPT 用）
- JSON 指令格式範例
- 如何將自己的 API/資料庫接上 MCP
  我都可以幫您設計與示範！

要繼續嗎？