



MCP — AI 模型與數據世界的橋樑

生成式AI大串連 企業流程將再造（1）

儘管「代理型 AI」仍處於起步階段，但如同微軟提出的「代理式網路」（agentic web）的概念，已經將「AI 代理」進一步往前推動，而「模型上下文協定（MCP）」則被視為實現「代理式網路」和可擴展 AI 應用（包括生成式 AI）的關鍵基礎。

編譯 / Frances

在人工智慧領域快速發展的背景下，尤其是大型語言模型（LLMs）在推論和內容生成方面的顯著進步，企業面臨著一個關鍵挑戰：如何讓這些強大的 AI 模型有效地與其現有的資料、工具和系統進行互動。過去，每個資料來源或工具都需要建立客製化的連接器，導致 Anthropic 公司將其描述為「N×M」（多乘多）的資料整合問題，使得真正互聯的 AI 系統難以擴展。

為了解決這項挑戰，「模型上下文協定」（Model Context Protocol, MCP）應運而生。MCP 是由大型語言模型開發商 Anthropic 於 2024 年 11 月推出的一項開放標準與開源框架。目的在於標準化 AI 模型（特別是 LLMs）與外部工具、系統和資料來源整合及共享資料的方式。許多技術作家將 MCP 譽為「AI 應用程式的 USB-C 連接埠」，強調其作為語言模型代理與外部軟體之間通用連接器的目

標。MCP 提供了一個與模型無關的通用介面，用於讀取檔案、執行功能和處理語境提示。

MCP 的技術架構：如何實現無縫整合

MCP 的核心運作基於「伺服器-客戶端」(server-client) 架構，這使得 AI 模型能夠安全地、雙向地連接到各種資料來源和 AI 驅動的工​​具。

|| MCP 伺服器 (MCP Servers)

MCP 伺服器是提供執行特定功能或公開資料能力的實體。它們可以是企業內容儲存庫、業務工具或開發環境的介面。

開發人員可以選擇透過 MCP 伺服器公開他們的資料。例如，Anthropic 維護了一個開源的 MCP 伺服器實作儲存庫，支援流行的企業系統，如 Google Drive、Slack、GitHub、Git、Postgres 和 Puppeteer 等。

企業也可以建立客製化的 MCP 伺服器來連接專有的系統或特定的資料來源到 AI 模型。

|| MCP 客戶端 (MCP Clients)

MCP 客戶端通常是 AI 代理 (AI agents)，它們充當 MCP 伺服器與 AI 模型之間的中介者。

當使用者向 MCP 客戶端提出自然語言請求時，客戶端會利用 AI 模型 (例如 LLM) 來處理該請求。

接著，客戶端會根據 AI 模型處理的結果，指示 MCP 伺服器執行所需的操作。

MCP 協定的作者指出，該協定刻意重用「語言伺服器協定」(Language Server Protocol, LSP) 的訊息流概念，讓編輯器和 IDE 能夠與程式語言後端服務溝通，從而提升對多種程式語言的支援能力。

同時，MCP 透過 JSON-RPC 2.0 進行傳輸，這意味著 MCP 建立在現有的、成熟的協定基礎上，有助於其廣泛採用，也就是說，JSON-RPC 2.0 正是 MCP 讓 AI 代理能夠與外界「說話」和「行動」的具體「物流」系統，確保訊息能夠

被正確地發送和接收。Anthropic 也釋出了包含 Python、TypeScript、Java 和 C# 等多種程式語言的軟體開發套件 (SDKs)，以幫助開發者快速上手。

MCP 的應用方式與未來展望

MCP 的設計目的在於讓 AI 系統更簡潔、更可靠地存取所需資料。其應用範圍廣泛，涵蓋：

- **桌面助理**：例如 Claude Desktop 應用程式可以在本地運行 MCP 伺服器，讓 AI 安全地存取系統工具和使用​​者檔案。
- **企業助理**：允許內部 AI 助理從專有文件、客戶關係管理 (CRM) 系統和公司知識庫中檢​​索資訊。
- **多工具代理工作流程**：支援代理式 AI 系統協調多個工具，例如結合文件查詢與訊息 API，以實現跨分散式資源的鏈式思考推論。
- **軟體開發工具**：整合到程式碼編輯工具中，使 AI 程式碼助理能夠即時存取專案上下文。

MCP 的開放標準特性促使其獲得了迅速的採納，有助於實現類似 HTTP 之於網際網路或 SMTP 之於電子郵件的革命性影響。微軟 (Microsoft)、Cloudflare、OpenAI 和 Google DeepMind 等業界巨頭都已宣布支持 MCP，這股強勁的動能表明 MCP 有望成為實現代理式 AI 革命的關鍵基礎。

總體而言，MCP 的出現為生成式 AI (特別是 LLMs) 克服了資料隔離的限制，將其從單純的「生成」資訊，提升為能夠「理解、行動並協調」的自主系統，為企業帶來更深層次的自動化和價值創造。它為 AI 應用程式提供了一個統一的連接器，使得 AI 能夠從孤立的情報庫中解脫出來，真正融入到企業的營運核心。