智能文書處理

首先，一個非常重要且關鍵的問題

在公開的 ChatGPT 網頁版上傳未經處理的公司機密內容，會帶來極高的機密外洩風險。

你可以將標準版的 ChatGPT 想像成一個「半公開的論壇」，你輸入的內容預設情況下**可能**會被 OpenAI 用於訓練和改進模型。這意味著你的機密資訊有朝一日可能會被模型「學會」，並在無意中洩漏給其他使用者。

風險分析：為什麼有風險？

1. **模型訓練 (Model Training)**：
    - **標準版 ChatGPT (免費版/Plus 版)**：根據 OpenAI 的使用條款，除非你主動選擇退出 (例如使用臨時聊天功能或在設定中關閉訓練選項)，否則你的對話內容會被用作訓練資料。這是最大的風險來源。一旦數據進入訓練集，就無法保證它不會以某种形式被重現。
    - **ChatGPT Team/Enterprise 與 API 服務**：**情況完全不同**。OpenAI 承諾，透過其 API 或企業級服務提交的數據**不會**被用於訓練模型。數據僅為處理你的請求而使用，並有最多 30 天的保留期以監控濫用行為，之後便會刪除。
2. **法律與合規風險 (Legal & Compliance)**：
    - 若你的公司資料包含客戶的個人資訊（PII），未經授權上傳到第三方服務可能違反 GDPR、CCPA 等數據保護法規，導致巨額罰款。
3. **供應鏈風險 (Supply Chain Risk)**：
    - 即使是使用 API，你仍然是將數據傳輸給了第三方（OpenAI）。如果 OpenAI 的系統遭到駭客攻擊，你的資料也可能隨之洩漏。

更好的做法應該是？

根據你公司的安全需求、預算和技術能力，可以選擇以下幾種更安全的做法：

- **方案一 :使用企業級或 API 服務 (最快、最直接)**

  這是最容易實施的改進方法，在便利性與安全性之間取得了很好的平衡。
    - **做法**：
        - 不要使用 `chat.openai.com` 的網頁介面。
        - 改為付費訂閱 **ChatGPT Team/Enterprise** 方案，或透過 **OpenAI API** 來進行數據分析。
    - **優點**：
        - OpenAI 官方合約承諾你的數據不會被用於模型訓練。
        - 可以整合到公司內部的應用程式中，建立客製化的分析工具。
    - **適合對象**：絕大多數有 AI 分析需求，且信任 OpenAI 安全措施的中小型及大型企業。
- **方案二：透過主流雲端平台使用 (更安全、合規性更高)**

  將 AI 模型放在你信任的雲端服務供應商 (CSP) 的環境中運行。
    - **做法**：
        - 使用 **Azure OpenAI Service**：這是微軟提供的服務，它將 OpenAI 的模型（如 GPT-4）部署在

微軟的雲端基礎設施內。
        - 使用 **Google Cloud Vertex AI** 或 **Amazon Bedrock**：這些平台同樣提供了多種大型語言模型，並整合了該平台的安全與網路功能。
    - **優點**：
        - 數據保留在你的雲端帳戶環境內，不會傳送給 OpenAI。
        - 可以利用雲端平台既有的企業級安全控制、網路隔離 (VPC/VNet) 和合規認證 (如 HIPAA, SOC 2)。
    - **適合對象**：已經在使用 Azure, GCP, AWS，且對數據主權和合規性有更高要求的企業。
- **方案三：私有化部署開源模型 (最安全、成本最高)**

  對於極度敏感的資料，唯一的萬全之策就是讓數據完全不離開公司內部網路。
    - **做法**：
        - 選擇一個表現優異的開源大型語言模型（例如：Llama 3, Mistral, Qwen）。
        - 在公司自己的伺服器或私有雲（On-premise / Private Cloud）上部署這個模型。
    - **優點**：
        - **完全的數據控制權**：數據從始至終都在你的防火牆之內。
        - 可以實現「氣隙 (Air-gapped)」部署，完全與外部網路隔離。
    - **缺點**：
        - 需要強大的硬體（尤其是 GPU）和專業的技術團隊來部署、維護和微調模型。
        - 成本和複雜性遠高於前兩種方案。
    - **適合對象**：金融、國防、高科技研發等對機密性要求達到頂級的組織。

  Ollama

輔助策略：數據匿名化 (Data Anonymization)

無論採用哪種方案，這都是一個值得推薦的最佳實踐。

- **做法**：在將數據發送給 AI 模型**之前**，先用程式或工具自動識別並移除或遮蔽所有敏感資訊，例如：人名、公司名、身分證號、電話、金額、專案代號等。
- **優點**：作為一道額外的保險，即使後端服務出現問題，洩漏的也只是無關重要的非敏感資訊。

總結

方案	優點	缺點	適合對象
標準版 ChatGPT	方便、快速、免費/低價	**極高機密外洩風險**	**僅限於非敏感、公開資訊的查詢**
API / 企業版	數據不被訓練、快速導入	數據仍需傳輸給第三方	大多數企業的起點
雲端平台 (Azure/GCP)	數據在自家雲環境、合規性高	成本略高、需雲端平台知識	對安全與合規有更高要求的企業
私有化部署	**數據完全不出內網、最安全**	成本高、技術複雜度極高	機密等級最高的金融、國防、研發單位

AI 在數據分析中的三大角色

在數據分析的領域，我們不該把 AI 看作一個取代者，而是一個「**智能副駕 (Co-pilot)**」。它能輔助我們完成許多任務，主要扮演以下三個關鍵角色：

1. **探索 (Explorer)**
   當你面對一堆原始數據，還沒有頭緒時，AI 就是你最好的探索夥伴。它可以幫你腦力激盪，提出各種值得分析的商業問題。
   - **實作範例**：
     假設我們有一份銷售數據，欄位包含「日期、地區、產品、銷售額」。我們可以這樣問 AI：

     > 「我有一份銷售數據，欄位有『日期』、『地區』、『產品』、『銷售額』，我可以用這些數據回答哪些有趣的商業問題？」

2. **翻譯 (Translator)**
   AI 能將我們用「人類語言」描述的複雜問題，精準地「翻譯」成 Excel 能聽懂的語言——也就是具體的分析步驟或函數公式。
3. **解讀 (Interpreter)**
   當你從 Excel 得到分析結果（例如一張樞紐分析表）後，AI 可以幫助你快速解讀數據背後的趨勢與洞察，並生成初步的結論。

AI 的三種核心能力

1. 精準溝通力 (Prompting)：讓 AI 聽得懂、做得對。
2. 知識賦予力 (RAG)：讓 AI 成為你的專屬領域專家。
3. 流程自動化力 (Agent/Workflow)：讓 AI 為你執行複雜的多步驟任務。

精準溝通 — 成為 AI 的頂尖提示工程師

學習目標： 掌握與大型語言模型 (LLM) 高效溝通的藝術，為所有進階應用打下堅實基礎。

Prompt 的基本概念與定義

什麼是 Prompt？

Prompt (提示詞) 是給 AI 的一段輸入文字或指令，目的是引導模型產生特定的回應、完成某項任務，或進行特定的對話。

可以將 Prompt 想像成是對一位非常聰明但需要明確指示的助理所說的話。說什麼，以及如何說，將直接決定助理如何理解並給出回應。

Prompt 的核心目的

Prompt 的存在，是為了讓 AI 能夠：

1. 理解您的意圖：AI 需要知道你想讓它做什麼。
2. 設定情境：提供足夠的背景資訊，讓 AI 能夠在正確的脈絡下思考。
3. 定義輸出：規範 AI 回應的內容、格式、語氣、長度等。

一個好的 Prompt 應具備的要素

要從 AI 中獲得最佳、最符合預期的回應，你的 Prompt 應盡可能具備以下要素：

1. 清晰明確 (Clarity & Specificity)
    - 定義：避免模糊不清的詞語，直接說明你想執行的 Excel 計算或操作。AI 模型是字面意義上的理解者，**它不會「猜測」你的意思**。
    - 範例：
        - 不好：「給我一個公式。」（太籠統，AI 不知道要算什麼）
        - 好：「**請**給我一個 Excel 公式，計算 `A1` 到 `A10` 儲存格的總和。」（明確指出要計算的動作、範圍和目標）
2. 提供足夠的情境 (Context)
    - 定義：給予 AI 足夠的背景資訊，例如你的**資料結構**、**Excel 版本**、**特殊需求**等，讓它能更好地理解你的需求並選擇最適合的函數。
    - 範例：
        - 「我有一個員工資料表，其中 A 欄是員工編號，B 欄是部門，C 欄是月薪。現在我需要根據員工編號 (在**另一個工作表**的 A2 儲存格)，從這個資料表中查找對應的月薪。我的 Excel 版本是 Microsoft 365。 請給我一個 Excel 公式。」（明確指出 Excel 版本和資料結構，影響 AI 選擇 VLOOKUP 而非 XLOOKUP）
3. 明確的指令 (Clear Instructions)
    - 定義：清楚地告訴 AI 你希望它執行什麼具體的 Excel 動作（例如：計算、查找、篩選、格式化）。
    - 範例：
        - 「計算 A1 到 A10 儲存格的平均值。」
        - 「查找 B2 儲存格的產品名稱在 產品清單 工作表中的對應價格。」
        - 「判斷 C5 儲存格的數值是否大於 100。」
4. 指定輸出格式 (Desired Format)
    - 定義：如果你對 AI 回傳的公式或其解釋有特定的格式要求，明確說明。
    - 範例：
        - 「給我一個 Excel 公式，計算 A1 到 A10 的總和。將公式用程式碼區塊呈現，並附上簡要的中文解釋。」
        - 「給我一個 Excel 公式，計算 A1 到 A10 的總和。以條列式說明公式的每個參數。」
5. 設定限制 (Constraints)
    - 定義：限制公式的行為或其結果的特性，例如錯誤處理、特定條件下的回傳值等。
    - 範例：
        - 「給我一個 Excel 公式，計算 B2 儲存格的銷售額減去 C2 儲存格的成本。確保公式在銷售額為零時不會產生錯誤，並回傳 0。」（限制了公式的錯誤處理行為）
        - 「給我一個 Excel 公式，判斷 A1 儲存格的數字是奇數還是偶數。如果 `A1` 為空，回傳空白。」（限制了公式在特定條件下的回傳值）
6. 提供範例 (Few-shot Examples)
    - 定義：如果你的需求比較複雜、抽象，或者你希望 AI 遵循特定的公式模式，提供一兩個輸入-輸出範例可以幫助 AI 更好地理解你的意圖。

- 範例：
    - 「根據以下範例，為我生成 Excel 公式：
        - 範例 1：
            - 需求：計算 A1 到 A5 的總和。
            - 公式：=SUM(A1:A5)
        - 範例 2：
            - 需求：計算 B1 到 B10 的平均值。
            - 公式：=AVERAGE(B1:B10)
        - 現在請生成：
            - 需求：找出 C1 到 C20 的最大值。」（透過範例，AI 能理解你期望的公式生成模式）

7. 「忘記一切」的重設指令（Forget everything)
    - 定義：強制 AI 清除錯誤記憶與假設，強制重啟對話，解決 AI 陷入重複或迷失情境的問題。
    - 範例指令：「忘記從 [對話中的特定時間點] 開始的一切。重新開始並逐步解決這個問題。」
8. 啟動導師模式(like a teacher)
    - 定義：強迫 AI 在給出最終答案前，像是一位老師以淺顯易懂的方式逐步解釋推理過程，協助提高結果的準確性，讓使用者得以學習 AI 的思考邏輯。
    - 範例：「在給出最終答案前，請逐步解釋你的思考過程。」

簡述 Prompt 五大原則

- **給予方向**
  詳細描述所需的風格,或參考某個相關人物。
- **指定格式**
  定義需要遵循的規則和指定的回應結構。
- **提供範例**
  插入一組可正確完成任務的測試案例。
- **評估品質**
  辨識錯誤並對回應評分,測試有哪些會影響效能的因素。
- **任務分工**
  將任務分為多個步驟,再鏈接起來實現複雜的目標。

AI 不是只有 ChatGPT

- ChatGPT https://chatgpt.com/
- perplexity https://www.perplexity.ai/
- gemini https://gemini.google.com/
- claude https://claude.ai/
- grok https://grok.com/

小工具

- 安裝 gemini CLI
- 重要的小工具 Markdown
- VS Code
- typora
- NotebookLM

> 實作練習(20分鐘)：
>
> 1. 請打開你慣用的 AI 工具網頁（如 ChatGPT, Gemini 等）。
> 2. **任務**：假設你正在分析客戶意見，請複製以下這段模擬的「客戶回饋文字」，並向 AI 提問。

```
> **回饋文字**：「你們的App更新後變得很卡，而且常常閃退。雖然客服人員態度很好，但問題等了好幾天才解決。希望你們能改善穩定性，並加快問題處理速度。」
>
> **你的提問**：「請將這份客戶回饋進行分類，並總結出 3 個主要的客戶抱怨點。」
```

3. 觀察 AI 如何從非結構化的文字中，快速提煉出有價值的資訊。

賦予 AI 記憶 — 個人知識庫

學習目標： 突破通用 AI 的知識限制，使用現成工具建立一個基於個人或專業文件的智慧知識庫。

- 2.1 觀念建立：認識向量資料庫與 RAG
  - 類比教學：用「概念圖書館」的比喻，解釋文字如何變成向量 (Embedding)，以及 AI 如何進行語意搜尋 (Vector Search)。
  - RAG (檢索增強生成)：介紹其作為當前主流知識庫解決方案的運作原理。

Ai 與向量資料庫

想像一下，你走進一個「概念圖書館」。

1. 一般圖書館的運作方式 (類似傳統資料庫)
   - 你想找一本書，你得知道書名、作者，或是一些關鍵字，比如「電腦科學」。
   - 你到查詢系統輸入「電腦科學」，系統會給你所有標籤為「電腦科學」的書。
   - 這種方式很精確，但如果你想找「**關於蘋果公司創辦人賈伯斯那種創新精神的書**」，系統就不知道怎麼辦了，因為沒有一本書叫做「賈伯斯創新精神」。
2. 概念圖書館的運作方式 (AI + 向量資料庫)
   - 在這個圖書館裡，沒有傳統的分類標籤。取而代之的是，每本書都被一位博學的「AI管理員」讀過。
   - 讀完後，AI管理員會給每本書一組「意義座標」（這就是 向量 Vector），例如 [0.8, 0.2, -0.5, ...] 這樣一長串數字。這組座標代表了這本書在「意義空間」中的位置。
   - 意義相近的書，它們的座標就非常接近。例如，關於賈伯斯、伊隆·馬斯克的傳記，以及討論破壞式創新的書，它們的「意義座標」在空間中都會聚集在一起。

    - 現在，你跟 AI 管理員說：「我想找關於創新、熱情、改變世界的書」，AI 管理員會把你的這句話也轉換成一組「意義座標」。
    - 然後，它不去查關鍵字，而是去尋找書庫中，哪些書的座標離你這句話的座標最近。
    - 最後，它推薦給你的可能是賈伯斯的傳記、某本設計思考的書、甚至是某本關於文藝復興的書，因為它們在「意義」上都和你的需求很接近。

AI 與向量資料庫的角色分工

在這個比喻中：

- AI (特別是 Embedding 模型)：就是那位博學的「AI 管理員」。
    - 它的核心工作是「**理解**」和「**翻譯**」。
    - 它負責把非結構化的資料（如文字、圖片、聲音）讀懂，並將其「翻譯」成一組能代表其核心意義的數字座標——也就是 **向量**（Vector） 或稱為 **嵌入**（Embedding）。
    - AI 是 意義的產生者。
- 向量資料庫 (Vector Database)：就是那座「概念圖書館的**館藏系統**」。
    - 它的核心工作是「**儲存**」和「**快速查找**」。
    - 它專門被設計來存放數百萬、甚至數十億筆的「意義座標」（向量），並提供超高效率的「相似性搜索」（Similarity Search）功能。
    - 當給定一個查詢座標時，它能光速找出離這個座標最近的 N 個鄰居。
    - 向量資料庫是 意義的管理者與檢索者。

他們如何協作？

一個典型的 AI 應用流程如下：

1. 資料準備（建立索引）：
    - Step 1: 你有大量的資料（例如：公司所有產品文件、所有商品圖片）。
    - Step 2: 你用 AI 模型去讀取每一份文件、每一張圖片，並把它們轉換成一個個向量。
    - Step 3: 你將這些向量以及它們對應的原始資料（或ID）存入向量資料庫。
2. 使用者查詢（執行搜索）：
    - Step 1: 使用者提出一個問題（例如：「我的藍牙耳機無法配對怎麼辦？」或上傳一張他喜歡的衣服圖片）。
    - Step 2: 你的應用程式再次使用同一個 AI 模型，將使用者的問題或圖片也轉換成一個「查詢向量」。
    - Step 3: 應用程式拿著這個「查詢向量」去向量資料庫中，下達指令：「請找出資料庫裡跟這個向量最相似的 10 個向量」。
    - Step 4: 向量資料庫快速回傳最相似的 10 筆資料。這些資料可能就是最相關的產品說明、解決方案或最相似的衣服。

核心結論與應用

> 一句話總結：AI 負責將萬事萬物轉化為「意義座標」，而向量資料庫則負責高效地管理和搜索這些座標。

這種組合催生了許多強大的現代 AI 功能：

- 語意搜索 (Semantic Search)：搜索的是意義而不是字面。例如，搜索「給我看**便宜又好吃**的午餐」，它能找到「**高CP值**商業午餐」，即使沒有出現「便宜」或「好吃」的字眼。

- RAG (Retrieval-Augmented Generation)：這是讓大型語言模型（如 GPT）回答問題時能引用外部知識的關鍵技術。模型先去向量資料庫中找到最相關的資料，再基於這些資料生成更準確、更可靠的答案，避免胡說八道。
- 推薦系統 (Recommendation Engines)：根據你喜歡的商品（A），在向量空間中找到與 A 最接近的其他商品推薦給你。
- 以圖搜圖 (Image Search)：上傳一張圖片，系統將其轉換為向量，然後在資料庫中尋找向量最接近的其他圖片。

AI 的三大關鍵能力：RAG, MCP 與 Agent

一個強大的 AI系統，它的威力不僅僅來自於模型本身有多大，更多是來自於我們如何賦予它三種關鍵能力：

1. 獲取知識的能力 (RAG)
2. 深度思考的能力 (MCP)
3. 採取行動的能力 (Agent)

接下來，我們逐一拆解這三個概念。

RAG — 讓 AI 成為博學的學者

我們遇到的問題：健忘且無知的 AI

想像一個只會「閉卷考試」的學生。他很聰明，但只記得教科書裡的舊知識，對於昨天發生的事、公司的內部文件一無所知。這就是標準的 LLM。

解決方案：給 AI 一本「參考書」進行開卷考試

RAG (Retrieval-Augmented Generation - 檢索增強生成) 的核心思想就是把「閉卷考試」變成「開卷考試」。

- 流程拆解：

1. 檢索 (Retrieval)：當 AI 收到你的問題時，它不急著回答，而是先去你指定的「參考書」（你的知識庫，如 PDF、網站）中，快速找到最相關的幾頁。
2. 增強 (Augmented)：AI 把找到的這幾頁資料，附在你的問題後面，形成一個內容更豐富的「考試題目」。
3. 生成 (Generation)：AI 根據這個「問題 + 參考資料」的組合包，生成一個有憑有據的答案。

- 核心優勢：
    - 準確性：答案基於你提供的資料，大大減少 AI「瞎掰」的可能。
    - 時效性：你可以隨時更新「參考書」，讓 AI 掌握最新資訊。
    - 隱私性：AI 無需「學習」你的隱私文件，只需在回答時「參考」一下。
    - 可追溯性：你知道答案是從哪份文件的哪個段落來的（如 NotebookLM 的引用功能）。

> RAG 的一句話總結：讓 AI 從「我猜」變成「我查過資料，答案是...」。

MCP — 教 AI 成為嚴謹的思想家

我們遇到的問題：思考跳躍的 AI

有時候，即使給了 AI 參考書，它在面對複雜問題時，還是可能因為思考不夠周全而得出錯誤結論。就像一個雖然開卷，但解題思路混亂的學生。

解決方案：要求 AI「寫下詳細的解題步驟」

MCP (Multi-step Chain-of-thought Prompting - 多步驟鏈式思維提示法) 的核心思想是，透過精心設計的 Prompt，強迫 AI 進行一步步、有邏輯的思考。

- 這是一種高階的「提示工程 (Prompt Engineering)」技巧。 你不是問一個問題，而是給 AI 一張「思考地圖」。
- MCP 風格的 Prompt 範例：

> 「你是一位資深商業分析師。請遵循以下步驟，分析『超級 A 產品』銷量下滑的原因：
>
> 1. 步驟一：提出假設。 列出三種可能的內外部原因。
> 2. 步驟二：分析原因。 評估每一種原因的可能性。
> 3. 步驟三：提出建議。 針對每種原因提出解決方案。
> 4. 步驟四：總結。」

- 核心優勢：
    - 邏輯性：引導 AI 進行嚴謹、結構化的推理，提高複雜問題的正確率。
    - 透明性：AI 的思考過程變得可見，方便我們除錯或評估其思路。
    - 可控性：能將一個龐大的任務，拆解成一系列可控的小任務。

> MCP 的一句話總結：讓 AI 從「直接給答案」變成「給你看我如何思考的」。

> 實作練習(10分鐘)：開啟 sales_chart.png 請 AI 進行分析

Agent — 賦予 AI 成為能幹的執行者

3.1 我們遇到的問題：只會說、不會做的 AI

即使 AI 既能查資料 (RAG)，又能深度思考 (MCP)，它最終還是只能「說」出結果。它不能真的幫你訂機票、發郵件、操作軟體。

3.2 解決方案：給 AI 「手和腳」去連接世界

AI Agent (自主代理) 的核心思想是，賦予 AI 一個能自主規劃、使用工具、並自我修正的循環，以達成你設定的目標。

- 一個能幹的「超級管家」
- 下達目標：「幫我安排下週去東京出差。」
- 管家開始行動：
    1. 規劃 (Planning)：(運用 MCP 思維) 拆解任務：查日期 -> 查行事曆 -> 查政策 -> 搜機票 -> 搜飯店 -> 預訂 -> 更新行事曆。
    2. 使用工具 (Tool Use)：自主選擇並使用它的「工具箱」：
        - 網路搜尋 (查會議日期)

        - 知識庫查詢 (用 RAG 查公司差旅政策)
        - API 呼叫 (訂機票、訂飯店、更新 Google Calendar)
    3. 觀察與修正 (Observation & Self-Correction)：發現直飛航班超預算，於是自動修正計畫，改為搜尋轉機航班。
    4. 執行與回報 (Execution & Response)：完成所有預訂後，向你報告結果。
- 核心優勢：
    - 自主性：能獨立完成從規劃到執行的完整任務。
    - 行動力：能與真實世界的數位工具（API、軟體、網站）互動。
    - 適應性：能在遇到障礙時，進行有限度的自我修正和調整。

> Agent 的一句話總結：讓 AI 從「給你一份計畫書」變成「報告老闆，事情已經辦妥了」。

RAG, MCP, Agent 如何協同工作？

這三者並非獨立，而是一個完美的協作團隊。

場景：打造一個「自動化市場分析報告生成器」

1. 目標 (Goal)：你對 Agent 說：「幫我生成一份關於『AI 醫療市場』的最新趨勢報告。」
2. 規劃 (MCP)：Agent 的大腦 開始運作，它規劃出步驟：
    a. 搜尋近期相關新聞與研究報告。
    b. 查詢我們內部知識庫的過往分析。
    c. 整合資訊並提取重點。
    d. 生成報告。
3. 行動 (Tool Use)：
    - Agent 選擇網路搜尋工具，找到了 5 篇最新的市場分析文章。
    - Agent 接著選擇知識庫查詢工具 (RAG)，從公司內部資料庫中，找到了 2 份相關的歷史報告。
4. 思考與生成 (MCP + Generation)：
    - Agent 將 RAG 和網路搜尋到的所有資料，餵給一個MCP 風格的 Prompt：「根據這些資料，分析市場規模、主要玩家、新興技術和未來挑戰，並生成一份結構化的報告。」
5. 輸出 (Execution)：Agent 最終生成一份完整的 Word 文件報告，並透過郵件 API 發送給你。

關係圖：

```
Agent (超級管家)
└── 大腦 (MCP 思考模式)
└── 工具箱 (Toolbelt)
    ├── 知識庫查詢 (RAG)
    ├── 網路搜尋
    ├── API 呼叫
    └── 程式碼執行器
```

市場主流工具

概念	終端使用者產品範例	開發者框架/平台範例
RAG	NotebookLM, Perplexity AI, Notion AI, ChatPDF	LangChain, LlamaIndex, Pinecone, Chroma
MCP	(主要體現在各種 AI 應用的 Prompt 設計中)	OpenAI Playground, LangChain, Flowise, Dify.ai
Agent	ChatGPT (Code Interpreter, Actions), Devin	LangChain Agents, AutoGen, CrewAI

課程總結：

- RAG 是 AI 的「長期記憶」，負責**提供知識**。
- MCP 是 AI 的「邏輯思維」，負責**深度思考**。
- Agent 是 AI 的「雙手雙腳」，負責與世界**互動並完成任務**。
- 工具實戰：使用 NotebookLM 快速上架知識庫
    - 步驟一：建立知識來源：引導學員上傳多種資料來源（PDF 報告、網頁文章、文字筆記）。
    - 步驟二：基礎問答與答案溯源：學習如何向知識庫提問，並利用 NotebookLM 的引用功能驗證答案來源。
    - 步驟三：進階應用：練習使用比較、總結、表格生成等指令，對多份文件進行整合分析。
- 應用場景探索
    - 案例討論：探討個人知識庫在不同場景的應用，如：
        - 學術研究：快速消化論文與文獻。
        - 職場應用：成為公司規章、產品規格的問答專家。
        - 個人學習：建立特定主題（如投資、健身）的專屬教練。

指揮 AI 工作 — 設計多步驟自動化任務

學習設計和執行由多個步驟組成的 AI 工作流，將 AI 從「聊天對象」升級為「自動化員工」。

- 觀念建立：認識 AI 代理 (Agent) 與工作流
    - 從單一步驟到多步驟：解釋為何複雜任務需要被拆解。

全自動化簡報生成系統 Canvas 簡報製作三步驟

1. **進入 Canvas 介面：** 在 Gemini 頁面中，點擊工具選單並選取「Canvas」模式。
2. **輸入指令或上傳檔案：** 在 prompt 對話中，輸入簡報主題描述，例如「建立一個有關量子運算的 10 頁簡報」，或上傳文章、文件檔案或網址，指示 Gemini 根據內容摘要製作簡報。

```
讀取上傳檔案後對內容進行分析，完成一份教學用簡報
設計風格參考蘋果發布會簡報
內容語法說明盡可能完整
```

> 實作練習(10 分鐘):開啟 練習.md 檔，將文件改寫成完整的 markdown 格式

3. **即時預覽與匯出 Google 簡報：** Gemini 會在數分鐘內生成完整的簡報投影片，使用者可透過即時預覽調整指令修改，並將成果匯出至 Google 簡報或下載 PDF 檔案。

> 實作練習(20 分鐘): https://markdown.tw/

- 工作流設計與實作
  - 多步驟任務設計：學習如何將一個大目標 (如「完成一份會議記錄」) 拆解成一系列 AI 可執行的小步驟。
  - 範例一：會議記錄自動化
    1. 觸發：上傳一段錄音檔。
    2. 步驟 1：檔案是一個中文的訪談記錄，轉錄成逐字稿。
    3. 步驟 2：根據逐字稿，總結會議重點。
    4. 步驟 3：提取所有待辦事項 (Action Items) 並指派負責人。
    5. 輸出：生成一份結構化的會議記錄文件。

    > 實作練習(20分鐘)：開啟 04討論提案第1案.mp3 檔，建立一份完整會議紀錄。

  - 範例二：自動化表單生成
    1. 觸發：建立一份測試考題。
       - 步驟 1：分析需求，識別需要收集的資訊欄位。
       - 步驟 2：生成 Google Forms 所需的結構化問題列表。

       ```
       1.讀取參考文件(PDF) 文件的內容。
       2.根據 PDF 內容，生成 20 題選擇題。
       3.將生成的題目和答案以 Markdown 格式輸出。
       ```

       - 步驟 3：生成程式碼 (Google Apps Script)。

       ```
       1.讀取上傳文件
       2.生成一段建立 google 表單程式碼 (Google Apps Script)
       3.測驗主題為 智能報表應用測試
       4.增加兩個題目，學員姓名及學員編號，不列入計分，必填
       5.每題分數為 5分
       ```

       ```
       function createForm() {
           // 1. 建立表單並命名
           var form = FormApp.create('訪談回饋與滿意度調查');

           // 2. 設定表單說明
           form.setDescription('這是一份自動生成的測試表單，用於收集訪談後的回饋。');

           // 3. 新增「單選題」
           form.addMultipleChoiceItem()
               .setTitle('您對本次訪談的整體滿意度為何？')
               .setChoiceValues(['非常滿意', '滿意', '普通', '不滿意', '非常不滿意'])
               .setRequired(true); // 設定為必填
       ```

```
  // 4. 新增「簡答題」
  form.addTextItem()
      .setTitle('請問您的姓名是？')
      .setRequired(true);

  // 5. 新增「段落問答」
  form.addParagraphTextItem()
      .setTitle('對於未來的訪談流程，您有什麼建議？');

  // 6. 取得表單編輯連結與發布連結
  Logger.log('表單已建立！');
  Logger.log('編輯連結: ' + form.getEditUrl());
  Logger.log('發布連結: ' + form.getPublishedUrl());
}
```

- 步驟 4：執行程式碼 。
  1. 前往 Google Apps Script 點擊「新專案」。
  2. 將編輯器內的程式碼全部刪除，貼上上述程式碼。
  3. 點擊上方工具列的「儲存」圖示 (磁碟片)。
  4. 點擊「執行」按鈕。
  5. 執行完畢後，查看下方的「執行記錄」，複製「編輯連結」即可查看生成的測驗卷。

> **執行時的注意事項：**
>
> 第一次執行時，Google 會跳出視窗要求您「核對權限」，請選擇您的帳號，若出現「Google 尚未驗證這個應用程式」，請點選「進階」>「前往 (專案名稱) (不安全)」，最後點選「允許」。這是因為這是您自己寫的腳本，Google 會做標準的安全提醒。

> 實作練習(20分鐘)：以這份 pdf 為主題，建立一份測驗。

- 上下文維持與記憶功能
  在多步驟任務中，確保 AI 能「記住」並連貫執行任務，是**提示詞工程 (Prompt Engineering)** 的核心技巧。

  本質上，目前的 AI 模型（如 Gemini, ChatGPT）多半是「無狀態」的（Stateless），每一次對話對它來說都是新的計算。所謂的「記憶」，其實是我們將「過去的對話」重新打包餵給它。

  要讓 AI 在任務中保持連貫性，您可以採用以下幾種策略：

  1. 提示詞串接 (Prompt Chaining)
     這是最有效的方法。不要試圖一次把所有步驟塞在同一個指令裡，而是將任務拆解，並明確指示 AI 使用「上一步的輸出」作為「這一步的輸入」。
     - **作法：** 明確指涉。
     - **範例指令：**

       > 「**根據上一步驟生成的**逐字稿，請幫我提取 5 個關鍵結論。」
       > 「**承接上題的** 5 個結論，請針對每一個結論撰寫 100 字的分析。」

  2. 賦予角色與維持上下文 (Context Maintenance)
     在同一個對話視窗（Chat Session）中，AI 擁有短期記憶（Context Window）。為了強化連貫性，您可以在每一步驟開頭重複「當前目標」。

- **作法：** 在指令前加上背景提醒。
- **範例指令：**

> 「我們正在進行一份關於『智能報表』的訪談分析。現在我們已經完成了摘要（見上文），**接下來請根據該摘要**，製作一份待辦事項清單。」

3. 使用結構化輸出 (Structured Output) 作為「記憶錨點」
   要求 AI 輸出特定的格式（如 JSON, 表格, Markdown），這樣在下一個步驟引用時，AI 更容易精準抓取資訊，不會「產生幻覺」或遺漏。

- **作法：** 定義輸出格式。
- **情境：** 假設第一步是分析訪談。
- **指令：**

> 「請分析訪談內容，並**以 Markdown 表格輸出**，包含欄位：『問題點』、『受訪者情緒』、『建議解法』。」

- **下一步指令：**

> 「請讀取**上方的表格**，針對『建議解法』欄位，生成對應的執行程式碼。」

4. 定期「總結」以釋放記憶體 (Summarization for State Management)
   如果對話非常長，AI 的記憶（Context Window）可能會被填滿，導致它「忘記」最前面的設定。

- **作法：** 在任務中段要求 AI 進行總結。
- **範例指令：**

> 「我們已經討論了很多細節。在進入下一步之前，**請先總結我們目前達成的所有共識與已生成的內容**，確保我們沒有偏離目標。」

5. 單一指令內的「思維鏈」(Chain of Thought)
   如果任務必須在一次對話中完成，可以要求 AI 展現思考過程，強迫它在生成最終結果前，先列出中間步驟。

- **作法：** 使用 `Step-by-Step` 指令。
- **範例指令：**

> 「請執行以下任務，並**逐步思考 (Think step-by-step)**：
>
> 1. 先閱讀文件。
> 2. **基於文件內容**，列出大綱。
> 3. **根據大綱**，撰寫正式報告。
>
> 請依序顯示每一個步驟的結果。」

實際應用在您的案例

以您剛剛的「訪談錄音轉表單」為例，如果要確保 AI 記住細節，對話流可以是：

1. **第一步（輸入）：**「這是訪談逐字稿...（貼上內容）...請整理出重點。」
2. **第二步（記憶）：**「好，**根據你剛剛整理的重點**，請幫我設計 10 個測驗題，格式要是選擇題。」
3. **第三步（執行）：**「現在，**利用這 10 個題目**，寫一段 Google Apps Script 程式碼來自動生成表單。」

重點在於使用「指代詞」（根據上文、利用剛剛的結果、承接上題）來建立連結。

下一步：
您想試試看用這種「串接」技巧，根據剛剛做好的測驗題程式碼，請 AI **自動生成一封「寄給學員的測驗通知信」草稿**嗎？（它會記得測驗的主題和內容）

工具實戰：使用 NotebookLM 快速上架知識庫

1. 基本功能說明
2. 建立筆記本
3. 新增資料來源
    - 上傳文件
    - 新增相關知識連結
        - https://www.cw.com.tw/article/5134388
        - https://www.bnext.com.tw/article/81728/notebooklm-tutorial
        - https://grenade.tw/blog/notebooklm-google-ai-notebook/
        - https://www.cc.ntu.edu.tw/chinese/epaper/home/news_content_n_17852_sms_26963_s_250833.html
4. 自訂虛擬人格
    - 點選對話框右手邊的**設定筆記本** ICON
    - 你是一個專業顧問，擅長以幽默風趣的方式說明複雜的概念，並且擅長舉實際案例進行補充說明。
    - 儲存
5. 學習指引模式
6. 工作室
    - 語音摘要:男性負責說明，女性負責提問
7. 心智圖
8. 儲存至記事
9. 複製
10. APP 完成紀錄
    1. 安裝 NotebookLM App
    2. 開啟錄音程式進行錄音
    3. 分享，選擇 將轉錄高分享至 NotebookLM
11. 自動生成投影片
12. 生成圖表

> 實作練習： 整合前面的所有技能，完成一個從無到有的自動化簡報生成專案，展現綜合應用能力。

專案藍圖設計

- 定義目標：我們要打造一個系統，只需給定「主題」和「參考資料」，就能自動生成一份完整的簡報大綱。

輸入：簡報主題：東京五日游行程規劃 + 數份參考文件 (PDFs)。

1. 利用 NotebookLM 上傳參考文件，透過提問與總結，提取核心論點、關鍵數據和案例。
2. 設計一個 Prompt，將提取出的雜亂資訊，結構化為一份包含「封面頁、行程、行程內容、注意事項」的簡報大綱文字稿。
3. 將結構化的文字稿，輸入到 AI 簡報工具或使用範本快速生成簡報。