

課程名稱：18511_以 OpenClaw 為例介紹 AI Agent 的運作原理 課程摘要

本摘要由 Gemini AI 協助生成，僅供參考

1. 適合對象與能力門檻

- **適合族群：**初學者與對 AI Agent 技術感興趣者。本課程透過拆解熱門開源專案 OpenHall（原名 CloudBar），引導學員理解自主執行 AI Agent 的背後運作原理。
- **能力門檻：**普通。若預先具備機器學習導論的基本概念，上課過程會更為順暢。

2. 課程核心大綱與架構圖

- **章節架構：**
 - **章節一：**AI Agent 簡介與演進背景 — 介紹 AI Agent（如 OpenHall）與一般 LLM 的差異，並展示 AI 自主建立 YouTube 頻道與參賽的實際案例。
 - **章節二：**AI Agent 架構解剖與 System Prompt 運作 — 說明 AI Agent 本質為人與 LLM 之間的介面，解析如何透過 System Prompt 及 .md 文字檔（如 soul.md）賦予角色設定與記憶。
 - **章節三：**工具呼叫、自主創建工具與 Sub-Agents 派工 — 解析 AI Agent 如何執行電腦指令、自己撰寫程式碼小工具，以及透過 Sub-Agents 分工與 Context Engineering 節省上下文空間。
 - **章節四：**記憶機制、心跳與安全防禦 — 剖析短期/長期記憶與 RAG 檢索、CronJob 與心跳機制（Heartbeat）、Context Compaction 機制，以及 Prompt Injection 防護與安全執行環境設置。

3. 必備前置知識清單

- **機器學習導論基礎：**建議預先了解語言模型（LLM）的基本運作原理（如 Prompt、Token 與 Context Window）。
- **作業系統與獨立硬體觀念：**了解基本命令列操作，並理解將 AI Agent 部署於獨立或格式化電腦上的安全性考量。

4. 專有名詞與概念辭典

- **AI Agent**：並非人工智慧本身，而是跑在電腦上、介於使用者與大型語言模型（LLM）之間的介面，能自主呼叫工具與執行任務。
- **System Prompt**：每一次呼叫語言模型時，AI Agent 系統自動附加在前端的長段文字，包含身份設定、可用工具說明與行為準則。
- **Sub-Agent (Spawn)**：大龍蝦（主 Agent）繁殖出的子 Agent，協助處理耗費大長度上下文的子任務，藉此達成 Context Engineering 並節省主 Agent 的 Context Window。
- **Skill**：文字檔形式的工作流程 SOP，只有在需要時才載入上下文（按需讀取），以節省 Token 消耗。
- **Heartbeat（心跳機制）**：每隔固定時間自動觸發並發送指令給語言模型，讓 AI Agent 能自主定期檢查任務（如排程檢查郵件或推動目標）。
- **Context Compaction（上下文壓縮）**：當對話歷史快超出 Context Window 限制時，自動將舊對話送給語言模型進行摘要並替換，讓系統能長期運作。

5. 課程學習職能對照

- **對應職能名稱**：AI Agent 系統架構師 / AI 自動化流程開發工程師
- **主要工作任務/能力指標**：
 - **分析與決策能力**：能運用 Context Engineering 技巧（如子任務拆解、按需讀取 Skill、對話壓縮）優化 LLM 的上下文使用率，並具備 AI 安全防禦與沙盒環境規劃能力。
 - **工具操作與執行能力**：能整合與開發 AI Agent 框架，配置 System Prompt、MCP、CronJob 排程系統，並串接外部工具（如語音合成、Web 搜尋、郵件）實現自動化工作流程。