

AI × 頂級餐廳！

全家聽得懂、團隊落得地的
AI 智慧廚房大冒險

主講：卡皮巴拉主廚 | 2026.08.22

歡迎光臨 AI 智慧餐廳！



分享之前：先說清楚這間餐廳

今天的用途

教育推廣、知識分享、技術科普

今天的比喻

用「餐廳營運」把 AI Agent 的架構說得更生活化

卡皮說：我們今天是來學懂 AI，不是來背艱深名詞！



為什麼聊 AI，常常聊到對方皺眉？

「什麼是 AI Agent？」

如果回答塞滿：
神經網絡、向量資料庫、超參數、API 端點.....

對方：嗯.....所以它到底會做什麼？

卡皮說：先降低理解成本，再把專業名詞放進熟悉的畫面裡。



把複雜工程，翻譯成大家熟悉的餐廳

好的類比，至少要有三件事：

有畫面

看得見

有角色

誰在做

有流程

怎麼完成

今天，我們一起開一間「未來頂級餐廳」！

卡皮說：餐廳是翻譯器：把抽象概念變成看得見的工作現場。



AI 智慧餐廳的三大角色

先記住這個大方向：你提需求，主廚與廚房一起完成。

顧客 | 你 / 人類

提出需求
享受成果
決定想吃什麼

總主廚 | AI Agent

聽懂需求
思考與規劃
調度工具完成任務

廚房系統 | AI System

提供工具
管理資料與規則
守住安全與品質

一句話：你負責提需求，主廚與廚房負責搞定一切！



顧客與主廚：人與 AI Agent

Human / User ↔ AI Agent

以前的電腦比較像計算機：
你按什麼，它動什麼。

現在的 AI 比較像主廚：
你給目標，它會理解、規劃，再一步步完成。

卡皮說：「我想吃清淡晚餐」不是一道菜，而是一個要完成的目標。



點菜單，就是 AI 的提示詞 Prompt

Prompt | 提示詞

今日點餐單

牛排五分熟
黑胡椒醬另附
配菜只要烤蘆筍
請在 10 分鐘內完成

說得越具體，主廚越不需要猜。

卡皮說：Prompt 不是施魔法，而是把點餐需求說清楚！



主廚的腦袋：大型語言模型 LLM

LLM / Foundation Model

想像主廚讀過：

- 各國食譜
- 食材知識
- 料理經驗
- 怎麼推理與解決問題



這些「底蘊」決定 AI 的理解力與推理上限。

卡皮說：LLM 是大腦與基本功，但還需要工具和規則才能穩定出餐。

標準食譜 SOP：AI 技能 Skill

Skill | 技能

招牌舒芙蕾 SOP

1. 預熱烤箱
2. 混合食材
3. 控制時間
4. 檢查成品

把複雜流程包裝起來，就能重複使用、比較不走味。

卡皮說：Skill 決定「這道菜怎麼做」。



套餐等級與瓦斯額度：Plan、Token、Usage Limit

Plan | 方案

不同會員套餐，能用的服務不同。

Token | 消耗

做一道菜會用掉瓦斯、水電與心力。

Usage Limit | 上限

今天最多能用多少資源。

小提醒：任務越複雜，通常需要更多「能量」。



快速複習：點餐篇四寶

先記住畫面，再記住連結！

顧客與主廚

人與 AI Agent

點餐要求

Prompt 提示詞

主廚廚藝

LLM 大模型

標準食譜

Skill 技能



主廚工具台：MCP 工具系統

MCP | Model Context Protocol

光有廚藝，還不能切菜。主廚要能拿起工具！

MCP Tool = 測溫槍、平底鍋
MCP Server = 提供工具的工具房
MCP Client = 主廚挑工具、操作工具的工作台



卡皮說：MCP 的重點：讓 AI 能用標準方式理解與操作工具。

API 是對外窗口，MCP 是手邊工具台

兩者都能幫忙，但工作位置不同。

API | 對外窗口

打電話給肉品供應商
查庫存、叫貨、結帳
重點：怎麼跟外部服務溝通

MCP | 手邊工具台

拿起電子秤、測溫槍
直接操作廚房工具
重點：怎麼讓 AI 使用工具

卡皮說：API 在外面聯絡；MCP 在手邊操作。



眼前點單是 Context，熟客檔案是 Memory

Context | 當前上下文

眼前這桌的訂單、備註、正在做的菜。
做完這桌，內容就可以清空。

Memory | 長期記憶

跨越很久的顧客習慣。
例如：不吃香菜、喜歡熱水。

一個在手上，一個放在檔案櫃。



換一位大廚，和讓同一位大廚多想一下，不一樣！

換模型 | Model Version

聘請更強、更有經驗的大師。
像從一般主廚換成三星主廚。

提高推理強度 | Reasoning Effort

同一位主廚先停下來多想幾秒。
推演火候、順序與風險。

卡皮說：換人是升級能力；深思是增加思考時間。



彩色點餐機 vs 黑底廚房終端機

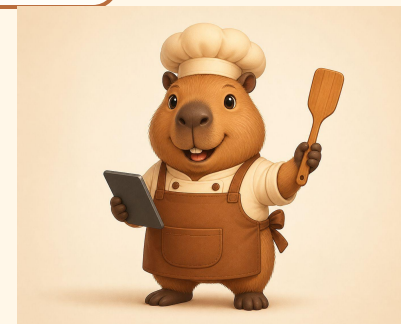
GUI | 圖形介面

看得到按鈕、圖片和選單。
親切、直覺，適合大多數人。

CLI | 命令列介面

用文字指令快速操作。
適合批次工作與自動化。

一個像前台點餐機，一個像後台高速工作螢幕。



快速複習：工具與記憶四寶

工具在手、窗口在外、眼前在單、記憶在冊！

廚具工作台

MCP 工具協議

叫貨窗口

API 介面

菜單與熟客本

Context / Memory

換大廚與深思

Model / Reasoning



Skill 是食譜，Harness 是整間廚房的運行制度

AI Harness

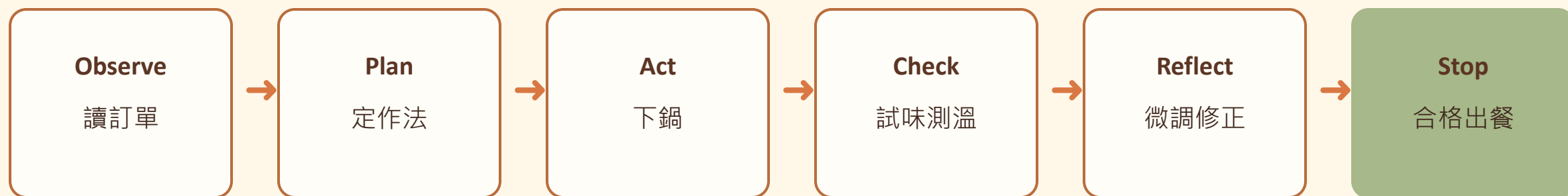
只有食譜還不夠。還要有：

- 工作環境
- 可用工具
- 權限與安全規則
- 失敗時怎麼重試
- 什麼情況一定要停下來



卡皮說：Skill 決定菜怎麼做；Harness 決定廚房怎麼運作。

一道好菜，會經過「觀察到達標」的循環



Loop 不是無腦重試，而是：觀察 → 規劃 → 行動 → 檢查 → 修正 → 達標停止



米其林廚房的四道安全防線

每一道防線，都在不同時間點保護成果。

Hook | 自動觸發

訂單送出，出單機自動印單。

Guardrail | 護欄

花生過敏？先鎖住危險食材。

Validator | 驗證器

檢查是否符合規範與衛生。

Checker | 核對員

出餐前逐項對照清單。



主廚喊「好了」，還不能直接端出去！

AI 自己說「完成了」，只是起點。

真正完成，要通過外部驗收：

1. 做對需求了嗎？
2. 通過測試了嗎？
3. Checker 核對通過了嗎？

主廚說完成 ≠ 真正完成

卡皮說：Done Criteria 就是「什麼條件都達到，才算完成」。



快速複習：工程品管四寶

制度定邊界、循環做修正、四重防線守、驗收才出餐！

廚房制度

AI Harness

修正流水線

Loop Engineering

安全防線

Hook / Guard / Validator /
Checker

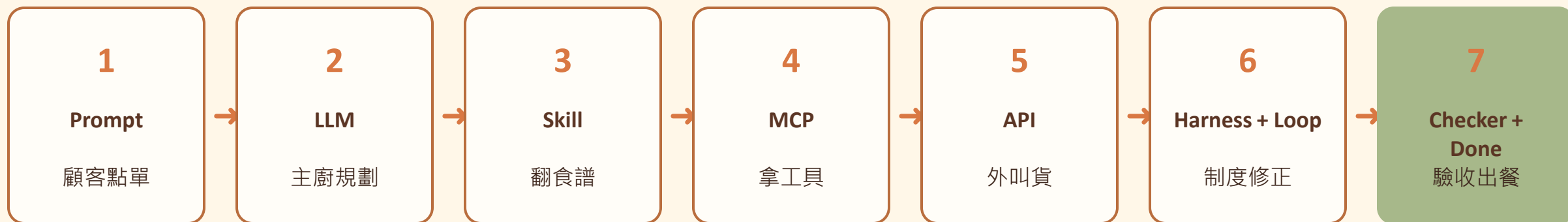
完成標準

Done Criteria



全景整合：一盤牛排的 7 步誕生之旅

把前面學到的概念，串成一條完整出餐線。



帶得走的黃金七句口訣

把每個大名詞，換回一個餐廳畫面。

Agent = 總主廚

Prompt = 點餐要求

Skill = 標準食譜

MCP = 百寶廚具台

API = 對外叫貨窗口

Harness = 廚房運行制度

Loop = 接單到合格出餐的閉環



主廚隨堂考：看圖猜概念！

先猜，再看下一頁揭曉答案。

A Skill | 食譜



B Guardrail | 護欄



C MCP Tool | 工具



D Checker | 核對



恭喜大家通關收服！

答案揭曉：

- A Skill：照著食譜做
- B Guardrail：先擋下危險
- C MCP Tool：拿起工具操作
- D Checker：出餐前核對

你已經抓住 AI Agent 的核心骨架！



今日料理心得：哪個比喻最有感？

請選一個你最想帶回家分享的畫面。

A API 是打電話叫貨，MCP 是自己拿工具！

B Skill 是食譜，Harness 管整間廚房！

C Loop 不是亂重試，而是測溫試味再修正！

D 主廚說完成不算，Checker 通過才是 Done！



簡報是一座橋：把複雜變成理解

一端是複雜的 AI 技術
另一端是聽眾的理解與微笑

分享主題	→	料理的美味
聽眾需要	→	今晚的饕客
預期結果	→	飽足與驚喜
結構設計	→	完美的饗宴



卡皮說：簡報不是把你懂的全部倒出來，而是牽著對方走到理解的另一邊。

Bon Appétit !

感謝光臨 AI 智慧餐廳

主講者：秦郁安

日期：2026.08.22

To Be Continued · 歡迎提問與交流！

卡皮巴拉主廚：下次見！

