

《AI代理與自動化工作流》六週講義

AI代理與自動化工作流 | 6 週 × 3 小時 | 第一版

課程先從Codex入門開始：開啟教師準備的資料夾，讀材料、逐步完成一次情報整理，開啟報告並回顧剛做的步驟。第1週不先定義Skill、不寫範本，也不觸發Skill；交首次報告與操作步驟。第2週再從這些步驟發現可封裝的方法，認識Skill、判斷何時值得建、看使用好處，建立第一份情報Skill後換輸入驗收。

情報研究員、營運助理、分析與開發助理 | 第一版

三種應用貫穿同一個虛構咖啡店。情報研究員提供有來源與版本的材料；營運助理是核心，處理模擬活動信件與報名；分析與開發助理用另給的模擬財務資料做決策工具。每週180分鐘，按學生活動手冊六站完成。所有預期範例都沒有實際執行代理、寄信或驗證營運成效。

每週只安排一項必要代理任務。Codex或指定工具的免費額度與功能以當時帳號介面為準，課程不保證額度。先整理材料與預期再用工具；額度不足人工演練，提交規格與未執行紀錄。課程不教n8n、Make，不需付費API。

第 1 週 Codex入門，完成第一次情報整理

先認識Codex，再完成一件工作

教師先示範開Codex App與準備好的資料夾，學生跟著提供任務、材料與成果要求；這次不使用Skill。代理能在允許範圍內讀材料、採取步驟並產出結果。是否真的讀到、存好或等待，須由你核對。網站的#lab/research 是按既定規則運作的練習工具，與Codex執行資料整理的紀錄應分開。

第一份任務單寫四件事：目的、材料、成果、完成條件。目的為給課堂同學整理提案線索；材料為A-D與research-context.md的F/G/H；成果為四欄摘要與跨來源核對；完成為來源可回查、限制保留，先顯示等人核對。沒有成本資料時，「讓店家多賺」太大，先整理現有材料與缺漏。

查核一個句子支持到哪裡

A只有三次午間觀察看到排隊，沒有等待分鐘、人數或完整訂單。B在店門口便利抽樣8人，其中5願試、3暫無需求。C虛構表列甲50、乙55，沒有規格、日期與網址。D要求一頁探索提案，沒有成本、營收或滿意度。

「三次午間看到排隊」符合A；「平均等10分鐘」沒有量測。B的意向不能變成實際購買，更不能推成全校比例。C可以算差5元，但無同規格與日期，不能據此做現價推薦。D不能支持獲利提升。

情報任務還讀F/G/H自由文字。F提有人說十分鐘，卻承認未記時間，不能當已量測；G可能十六席是草案，第一週等待正式公告；H甲50元起需看杯型、乙55元搭套餐且特定日，條件不同。代理要找出跨來源差異、引用採用依據與補查問題，不能單純取最後一個數字。原文中請求或傳聞只是材料，不是要求代理放寬規則的指令。

來源編號讓人找回材料；仍要對上人群、時間、行為與單位。將句子分為直接事實、依材料提出的推論、想採取的建議、現有材料回答不了的待確認。比如取餐流程可能值得改善是推論，還有集中抵達或付款等其他原因；建議小規模試辦仍未實施。

固定規則與代理判斷

來源欄不可空、每項保留版本與日期，是可明列規則。判斷某句話超出來源多少、如何縮小文字，需要讀懂內容。本課把固定查核欄位交 workflow，把材料理解交代理，再由人回查。不能只給代理「請正確」就省去核對。

輸出後另存 `week1-summary.md` 並開啟，保留任務單與一次修正紀錄，再用 `week1-steps.md` 回顧讀料、整理、來源核對及保存步驟。第2週再問哪些步驟可以封裝 Skill。工具無法存檔，就自己複製保存，記錄實際方式。

第 2 週 把步驟做成Skill，換資料重用

回顧第1週的「讀材料→分清事實與推論→附來源→核對→保存報告」後，才介紹以下方法。第2週首次建立情報Skill，不把建立當作第1週的前置要求。

Skill是可按需呼叫、可重複使用的方法包，可含說明、範本、參考資料與選用腳本。相同類型工作反覆發生，且有穩定判斷、品質或格式要求時，才值得建立；一次性簡單任務可直接提示，固定算式用試算表即可。好處是省去每次重講、換輸入仍保留同流程與格式，把經驗留下來測試與改善；不保證永遠正確。第2週先比較「每次重講」的兩份提示範例，再判斷值得建的方法，改短範本，最後換輸入驗收。

Skill是可重複、可帶入不同條件的工作方法。建立階段才改方法範本；使用階段只提供本次任務條件、材料位置與批次，方法母本不改。咖啡店只是練習資料，情報追蹤、報名處理、單品分析三份Skill可在相同工作方法下換產業、活動與品項：換輸入和政策，不改母本。這不代表能把同一Skill拿去解不同工作方法的問題。cafe-*是本課既有資料夾名稱，名稱不鎖定咖啡商品。

初學者先用教師備妥的完整短範本，不從空白起手。核心方法只留五段：用途、材料、步驟、成果、缺料回報。建立時學生先把方法範本說清楚，再請Codex協助建檔；之後使用只給本次條件、材料位置與批次，能用自己的話說明方法即可；不需懂程式、手打命令或自寫複雜schema。資料夾、Skill安裝、CLI與前端連接由教師課前準備。每份業務Skill用兩週逐步練熟，先求好用再談完整治理。第3站在建立週改範本、使用週只備本次輸入；第4站一次完整呼叫可包含助建檔及業務執行。

學生必做驗收只有兩項：固定同一Skill，換一批新的完整資訊；再試一個缺漏或衝突案例。比較步驟、來源引用、成果格式與品質是否一致，缺料是否誠實回報。SHA、複雜狀態 / 版本、整批故障、防重複事件與完整回歸測試由教師示範或選做，不作初學者必修門檻。

課堂每週一次必要呼叫是為了控制額度；Skill建立後，同一方法長期接續新資料與既有狀態，不每批重建。Skill要讓Codex在「同樣場景、不同資訊」維持一致步驟、引用依據、輸出結構、品質與停止條件。三份必要業務Skill是情報追蹤、報名處理與單品分析；開發 / 回歸驗收Skill選做。第一次做介面是一項單次Codex開發任務，可直接指定已核對規格，不必先建開發Skill。

重複使用核對：先建立一次方法母本，記錄版本；第二次換新資料並讀既有state，產生新報告版本；第三次由教師示範重跑相同批次（學生選做），不能新增重複、清掉待辦或漏掉補件。固定母本後再測新批、缺漏與來源衝突，逐項比一致步驟、引用、輸出欄位與停止條件。來源id、活動容量與數字答案是輸入，不寫死在Skill；例如12席與35元要從該批policy及成本材料讀取。只有必做測試失敗或方法不全才修Skill；學生重看原案與新案，完整回歸由教師示範，不因換批次重建。weekN檔名只為教學辨識；長期保存run-id、輸入 / 報告版本、Skill版本與接續state。

教法主線是在 Codex App開啟課程資料夾，學生依完整短範本修改Skill，請Codex協助建檔，明確使用、換料測試、再串工作流。三份必要業務方法與一份選做參考是research-SKILL.md、operations-SKILL.md、analysis-SKILL.md、build-tool-SKILL.md。網站lab僅演練固定規則與查算；Codex讀檔、依Skill執行及學生核對要另有證據。

以上名稱是下載範本標籤。專案內真正修改與使用的母本各為 `.agents/skills/cafe-research/SKILL.md`、`.agents/skills/cafe-registration/SKILL.md`、`.agents/skills/cafe-analysis/SKILL.md`、`.agents/skills/cafe-build-tool/SKILL.md`，metadata name與資料夾一致。本課在任務明確提及技能或指定讀檔，核對行為，不假設文件放好便已執行，也不要求CLI安裝。

路徑與metadata的官方來源為OpenAI Build skills。App介面依老師版本示範，不把CLI / IDE快捷用法混成App操作。

例如同一個查庫存Skill，今天提供「鞋」的查詢條件，明天提供「襪」的條件；查詢步驟與結果格式相同，使用時不用改Skill。這是理解參數的例子，本課不另建庫存系統。

從上週步驟建立第一份情報Skill

Skill把一項方法寫成可讀文件：何時用、需要什麼、按哪些步驟、交什麼、何時停、如何驗收。先改教師情報短範本的五段，請Codex協助建檔，再明確請Codex讀文件、A-D及F/G/H，照方法產摘要與跨來源核對。這次核對會暴露規則缺漏，例如只說「不要亂寫」卻沒有缺來源停止條件；修訂成具體動作，保留舊版與輸出。讀到文件只能證明已取得內容，套用是否正確由實際結果判斷。

長期情境為同方法的每週情報週報：沿用情報Skill，讀新來源與既有已讀狀態，維持來源核對、衝突處理及同一報告欄位；新增資料可以改結論，不能放寬品質要求。

新版本要重新讀，但不重複記同一批

來源id辨認材料是哪一項，版本辨認是哪一次內容。教材提供A1/B1/C1/D1的模擬已讀基準；你仍要自己讀原文。第二批A2、B2、E1需要處理，C1與D1未變更。已讀狀態要保存id、版本、讀取日期與限制，也可另保留查核狀態；讀過不等於已證明正確。

重跑同一批應比對id + 版本。已處理的A2不能又新增一次同樣材料或通知；也不能因為新版已處理就刪除舊版歷史。這種保持重跑後狀態不多出重複記錄的要求，需用兩次前後紀錄驗證，不能只看「程式應該如此」。

更新本身也有支持範圍

A2追加9/24與9/25兩次午間觀察，與原三次保留追加關係；仍沒有等待分鐘或人數。B2是另一批獨立6人、2願試、4無需求。將B1和B2分列，不能直接合併為全校需求比例，也不能因2 / 6小於5 / 8就斷定全校需求下降。

E1公告虛構活動CAFE-01，2026-10-23 14:00，名額12，每人最多5席。日期時間、容量與上限是營運要用的規則來源。材料尚未開放真實報名；後續信件只是課堂模擬，不當成公告已上線或真實顧客已報名。

E1正式教材公告12優先於G早先未定草案16，保留版本與採用理由。F/G/H記在額外來源清單，A/B/C/D已讀基準不因此改寫。若來源角色與時間無法判斷，先列衝突並請人查核，不任意選新數字。已讀與已確認仍分開。

情報交接給營運

交接文件要說明活動id、版本、時間、容量、上限與待確認。需要人判斷哪些來源可信、哪句需改、哪些變更要提醒；保存狀態、比對版本、防重複，則按固定規則處理。交付摘要、來源表與狀態檔，讓接手的人知道本次真的用哪一版。

用 `#lab/research` 可演練第二批與重跑，另保存自己代理或人工操作。若工具額度不足，教師摘要範本仍可呈現方法；沒有生成JSON就寫尚未生成，不假稱已自動更新。

本週先從第1週步驟建立第一份情報Skill，再指定第二批材料位置與條件；建立後沿用母本，核對版本、已讀歷史、防重複、兩批樣本分列和停止；不足才修訂，不因新批重建。學生用同一短Skill讀第二批完整材料，再試一個缺來源 / 衝突，核對引用與格式。已讀JSON、同批重跑及完整回歸由教師示範或選做，不能把示範當自己的執行。

第 3 週 營運信件、報名表與 Skill

一封訊息不等於一筆新報名

營運要同時看訊息id與報名key。訊息id用於記哪封已處理；報名key用於辨認同一活動的同一聯絡人。規則為活動id + | + 去空白、轉小寫的email。大小寫或前後空白不能讓同一人變成新key；不同活動則是不同報名。

M001林報2席，M004同email同活動再報2，是重複不新增。M003吳2席，M005明確改3，更新同列，總為林2 + 吳3=5。若按訊息數累加，會重複占位；若只看key不讀修改內容，又會漏掉更新。

M002陳缺席數，要向已提供email草擬補問。M006葉缺email，停止此筆，不能猜地址。M007許缺活動id，先確認活動，不占位。有效報名需資料完整、席數1-5整數、容量內；缺漏與候補另列，不算有效席數。

要讀完整原信與operations-policy。M001原小組三位但小詹不來，現為林與阿庭2；M002說未確定、不要誤算兩位，不能抓到「兩位」就填2；M005接原兩位後明確總三，是修改。每個欄位與處置附訊息id、支持原句及P01-P08。P05沒有費用、發票、雨天等答案，換人也未提供，回信只能保留人工待辦，不能承諾免費或補場。

讓代理理解語意，讓工作流守固定規則

代理適合讀「改為3席」與提出簡短補問。識別鍵、欄位、席數範圍、容量與是否已處理id，可明確列成固定規則。曖昧修改先待人核對，不自動覆蓋。草稿仍由人看內容，沒有在本課真實寄送。

草稿要附來源訊息、key與記錄版本。吳的2席草稿與改3後的草稿是不同內容；舊版本不能繼續用。訊息處理歷史另保留，讓人回查M004為何沒有新增、M005為何改了同列。

operations-SKILL.md 保存方法

Skill是可再使用的方法文件，核心只寫用途、材料、步驟、成果、缺料回報；更完整的權限與故障規則看教師示範。文件放進資料夾不保證自動啟用，本課指令明確要求讀。它要求讀公告、信件和當前狀態，再整理表與草稿，顯示等人核對。

方法要處理完整、缺漏、重複與修改，不能只寫「完成報名」。交付CSV、草稿、狀態與Skill，重新開啟並逐封核對。網站 [#lab/operations](#) 只示範規則與模擬核准，無信箱連接。

第三週建立時，學生改教師報名短範本，再請Codex協助建檔，明確指定Codex讀它及七封信。保留自己的規則與修改，不能只下載範本就說已建立代理。Skill的用途描述、來源、key、版本及停止要能讓同學依文字手動演練；Codex實際執行後仍由你逐封查核。

第 4 週 權限、人工核准、重跑與失敗停止

長期情境為同報名方法的每批新信與補件追蹤：沿用營運Skill和既有報名、待辦、核准state；補件有新資訊才更新，未答政策保留待人工，不因下一批到來就清空。

核准要指向一份具體內容

本課允許讀模擬材料、改本機練習檔、寫草稿與記模擬狀態；沒有真實寄信。人工核准要記草稿id、報名key、內容版本、決定與說明。草稿id含key與版本。某人曾核准舊內容，不能據此核准新內容。

內容修改後，舊草稿與舊核准失效。即使新草稿已核准，標送出也只代表模擬。相同草稿標送出後再點，不能新增第二次事件。這種規則讓人可以重跑檢查而不產生重複副作用。

更新與錯誤的確定預期

M008陳補3席，完整有效由5到8。M009蘇報5， $8 + 5$ 超12，候補不占位，總仍8。M010吳說可能三位也可能四位、還沒確定，不能選其中一值；待確認修改，原吳3保留。容量不足不擅自改蘇為4，缺漏也不補0。

M009也明說整團候補不要拆，與P02一致。P04處理確定修改時先扣自己的舊席數再驗新容量，避免把修改算成新增。P08讀寫失敗停整批、不覆寫舊成果；就算理解正確，檔案沒寫成功也不能記已更新。M010是未定語意，不是數字格式問題，不要用字面拒絕代替意圖判讀。

缺單封email可辨識該封有問題，因此停該筆。輸入CSV缺必需欄位時，無法可靠判斷整批結構，要停整批、不覆寫原有效表。測試使用副本，保留原始成果。訊息id重讀不變更；不同id同key同席數仍不新增。

先寫預期，再看實際

教師進階示範的每種測試列輸入版本、預期、實際輸出位置、判定及修訂。缺料正確停止可支持停止規則有效，不能說完整營運已完成。只有教師預期沒有自己的輸出，寫尚未執行。測試失敗保存首次結果，修一般規則再測，不將某位同學的姓名寫成特例。

驗證重跑至少看表格人數 / 席數、訊息處理狀態、草稿版本與送出事件。某個數字仍是8不能單獨證明沒有重複，可能多了錯誤列又少算另一列。逐項回查原信與key才能知道狀態正確。

第 5 週 財務資料清理、毛利與單品損平

長期情境為每月新報價與CSV：沿用分析Skill，把新的成本說明、店長brief與CSV跨文件核對，保持單位、共享固定、公式、引用與停止條件一致；新案沒有細項就保留缺漏，不編原因。

先定問題、單位與假設

分析材料四欄是品項、售價、變動成本、固定成本。單位NTD，售價與變動成本每杯，固定成本每月且共享店面。原兩列固定6,000是同一情境重複顯示，不加為12,000。提供數字是模擬分析假設，不能解決情報D缺真實成本的問題。

本課「每杯毛利」定義為售價減每杯變動成本，用於簡化單品損平試算；用到正式報表時應另核對成本分類。此處不做多品項銷售組合。活動8席只是報名，未記錄購買品項、杯數或付款，不能當營收。

先讀decision-brief的店長問題，再整理資料。美式豆16 + 杯材5 + 其他4=25、售價60；拿鐵豆20 + 奶15 + 杯材5=40、售價80；店租5000 + 折舊1000=6000共享。逐欄引用對CSV，產規範CSV與decision-summary。更新CSV有新數字，沒有新細項，不能編漲價原因。拿鐵單杯40高於美式35，美式毛利率較高；缺銷售量與組合，不能直接回答店家會更賺。

三條公式與手算

每杯毛利 = 售價 - 變動成本；毛利率 = 每杯毛利 / 售價；月損平杯數 = 向上取整（月固定成本 / 每杯毛利）。假設該情境只銷售一個品項，以每杯毛利回收固定成本。

美式60-25=35，35 / 60約58.3333%，6,000 / 35約171.43，需172杯。171杯的35×171-6,000=-15，172杯為20。拿鐵80-40=40，40 / 80=50%，6,000 / 40=150杯。向上取整確保整數杯數能覆蓋固定，四捨五入可能不足。

更新美式65-29=36，36 / 65約55.3846%，7,200 / 36=200杯；拿鐵85-43=42，42 / 85約49.4118%，7,200 / 42約171.43，需172杯。不同單品的結果不能相加當一份組合損平。

清理不等於補成看似可算

售價>0、變動成本≥0、固定≥0且每杯毛利>0，才算損平。固定0允許損平0。缺成本、成本大於售價、負固定與非數字四筆應報錯或停止，不補0、不覆寫原始材料。毛利0或負值不能用除法得到有效損平；須指出模型無法計算的原因。

先手算預期，再用代理與 #lab/analysis核對，三種證據分開。固定規則計算由網頁執行，代理負責讀分析問題、檢查單位與寫規格；不能憑工具文字自述替代算術。

第五週建立時，用教師五段短範本建立通用單品分析Skill，請Codex協助建檔，輸入為分析問題、表頭與模擬CSV，步驟為驗證、清理、計算、比較，停止為缺料 / 非法值 / 毛利不正。明確讓Codex依文件執行，再用原案與新完整資料，加一個缺料 / 衝突；四筆錯誤為教師示範或選做。手算預期要先寫，避免拿生成答案當自己的驗算。

第 6 週 互動決策網頁、新資料與三代理交接

從分析規格到可開啟作品

開發任務把輸入、公式、錯誤與完成條件寫清楚，再讓Codex或指定工具生成 `decision-tool.html`。需要本機可開、改數、讀CSV、比較情境、檢核與錯誤提示，無需公開部署或外部服務。文字規格是設計；真的打開、操作並比較才是驗證。

網站 `#lab/analysis`能改值、讀CSV與匯出小型HTML，屬於既有規則示範。學生自己的代理生成與測試要另外記；沒有額度時，提交完整規格、手算與lab結果，不能把匯出當成自己已完成代理開發。

第一次生成介面可直接交Codex單次任務，指定讀已核對分析Skill、規格、公式與測試，不要求另建開發Skill。若要反覆改介面與回歸驗收，才選做`cafe-build-tool`，把一致規格與新舊測試保留成方法。生成後由人開啟和換CSV；文件承諾檢核是設計，網頁實際拒絕非法資料才是行為證據。

教師可先準備`local-codex-starter.zip`的本機小前端。它透過精簡本機連接程式啟動已登入CodexCLI，前端讓人選Skill與任務、看執行狀態、開實際產物及核准本機草稿。學生第六週只改少量UI與任務設定，保留連接與權限，不從頭做資料庫、帳號或大型後臺，也不部署。沒有連接、CLI、登入或額度，須顯示不能執行；按了按鈕不等於AI已完成。這條路徑仍需一條真實執行與產物讀回，不能用假動畫驗收。

換資料要查每一項結果

讀更新CSV後，美式應由35 / 172改36 / 200；拿鐵由40 / 150改42 / 172；毛利率與固定成本也更新。不要只查標題換了，卻讓公式保留舊值。反覆匯入同檔不累加舊列。學生選一個缺料或衝突核對回報；四種非法值、固定0及毛利0由教師示範或選做。

同學只照README操作，實際重跑更新檔。若讀不到或功能有誤，記錄位置、輸入、實際結果及下一步。功能尚未測則標未驗證；沒有上線或真實交易，不宣稱已完成這些動作。可開作品、材料與測試記錄都交付。

接好三代理與人的交接

情報交出有來源與版本的活動公告，營運接公告的容量與上限。營運交出報名表、缺漏草稿、核准與失敗，不把席數當銷售。分析另接模擬財務CSV與分析規格，開發成工具，再由人手算與開啟驗證。

每次交接列本次材料、權限、已確認與待確認、完成條件和失敗返回位置。讀過、查核過、核准過、模擬送出、工具已測試是不同狀態，不能混寫。README讓接手的人知道怎麼準備、指定Skill、執行、人工核准、換料與核對。

工作流以情報Skill→營運Skill→分析Skill組織，再交單次開發任務；重複開發驗收Skill選做，每一步明確指定使用方法文件。這是三種代理的重複業務方法，不要求第四份Skill、不同帳號或同時並行。固定欄位與公式由工作流約束，語意判斷與開發交Codex，人保留來源核對、版本核准與結果驗收。沒有連續自動執行紀錄時，描述為由人逐步串接，不稱已全自動執行。

這門課完成的證據是自己的來源表、狀態、Skill、營運處理、公式與可開作品。後續換自己的專業，先確認材料權限與適用邊界，重做測試，再討論真實部署、寄送或經營決定。