CAMPUS AGENT / WEEKLY RESEARCH MEETING

從承辦回覆走到 Production 與 Internal Pilot

115 資工專題 · 2026/08/28 Meeting

承辦回饋 → 文件查證 → 規則修正 → 測試 → 正式部署

這次承辦回覆第一次完整跑過「規則維護迴圈」

老師轉寄問題後，陳靜儀逐題回覆並提供參考文件。

最重要的不是「多拿到幾個答案」，而是把三種東西拆開：

- **正式規定**：可以轉成可引用規則。
- **中央大學收件實務**：可作為判斷參考，但證據層級要分開。
- **灰色地帶**：仍保留人工確認，不把經驗硬寫成法規。

> **承辦人回饋不直接進答案；先查證，再決定要不要進規則庫。**

本輪具體影響：10 條規則、4 個主題、20 個邊界案例

指標	修改前	修改後
規則總數	162	**172**
現行規則	140	**150**
主題數	60	**64**
本輪專門邊界測試	0	**20**

具體修正包括：

- 補充保費不能只用職稱推定，要看給付性質 / 所得分類。
- 口試計程車先判斷計畫相關性，再逐步確認核准與交通條件。
- 軟體細項科目、跨期訂閱仍不自動放行。

正式部署與資料庫也第一次完整分流

正式版已部署到 Render，Release 流程會：

建置映像 → 推 GitHub Container Registry → 觸發正式更新

同時把環境分開：

- **Production Supabase**：真人試用資料。
- **Development Supabase**：開發 / 測試資料。
- **唯讀 audit 帳號**：專題端只能查匿名對話，不能直接改遠端資料。

> **研究資料的查回路徑開始和 production 本身一起被設計，而不是事後補 log。**

對話介面從 Demo 變成可以長時間使用

這週完成：

- 重新整理後恢復原對話。
- 可以查看最近對話、開新對話。
- 判定完成後仍能自然追問或修改條件。
- 每個追問可展開「為什麼要問 / 不同答案會怎樣」。
- 手機實測後，輸入區改成單行起始、自動增高、44 px 送出鍵與 iPhone safe area。

> **真人試用開始後，UX 問題本身也會變成 failure source。**

公開服務先補最低限度的安全邊界

正式站加入：

- Cloudflare Turnstile
- 人機驗證
- 呼叫次數 / 每日額度限制
- 額度紀錄異常時停止付費呼叫
- 關閉舊的未驗證模型入口
- 外部 PR 無法取得正式資料與部署憑證

這些不是研究 novelty，但如果沒有先補，公開測試本身就不安全、也不可持續。

Feedback 開始被當成研究資料，而不是單純按讚

一般使用者：

- 有幫助 / 有問題

Expert Mode：

- 正確程度
- 正式規定 / 實務作法 / 個人建議

每筆 feedback 會保留當時的**判定與規則庫版本**，但不會直接改規則。

> **真人說「有問題」只是 signal；規則仍要回到文件查證與人工審核。**

這場的關鍵決定：可以開始系辦 Internal Pilot 嗎？

Meeting 當時希望老師確認：

> **是否把這一版當成第一輪系辦內部試用版？**

老師另提醒兩個實務焦點：

1. 對話一開始先辨認「這筆支出屬於什麼類別」，再決定要問哪些條件。
2. 系辦最常遇到的問題之一是**聘人**，後續測試要注意這類真實高頻情境。

會後系辦試用邀請已寄出，專題正式從 production 原型走進 internal pilot。