

專題演講 #Agentic AI #數位同事 #人機協作 #ChatGPT #Agentic Enterprise

從 Agentic AI 到 Digital Colleague / From GPT to the Agentic Enterprise

梁明喬 Joe Liang • 劉浩翔 Jeremy Liu / OpenAI International, Managing Director | Oliver Jay

10:25-11:15 有效內容 70.4 分鐘 逐字稿 35,419 字

本檔為連續錄影，涵蓋官方議程的兩場：10:25 的中文專題演講，與 10:55 起 Oliver Jay 的英文演講。

⚠ 原始檔案清單中另有一個標示為「1055-1115 Oliver Jay」的檔案，經位元組比對與本檔完全相同。Oliver Jay 的演講並未遺失，就在本檔 36:20 之後。

上半場：數位同事 (Digital Colleague)

/ 一、技術脈絡

國泰連續三年以 AI 為技術年會主題：2024 年發表 Gaia、去年發表 Gaia 2.0。

Gaia 2.0 四大模組：

1. Orchestration 協調層
2. Runtime 執行環境
3. Protocol 協定層 (MCP、A2A)
4. Agent Marketplace

過去一年已把國泰內部運行 AI Agent 的基礎框架搭建完成。

/ 二、「數位同事」與一般 AI Agent 的三個關鍵差異

	一般 AI Agent	數位同事
記憶	活在單一 session 裡	跨 session 長期記憶，可共事數月仍記得你是誰
主動性	人說一動做一動	自主推進長程任務，會自己喚醒自己推進下一步
對象	面對單一使用者	識別組織中不同人事時地物，對不同角色做出不同回應

/ 三、與真人員工的鏡像設計

真人員工	數位同事
員工編號	系統獨立帳號與編號
辦公室	受控邊界的運行環境
員工守則	<code>Agent.md</code> 行為邊界
打卡工時	任務排程（可設 7×24，且不違反勞基法）
薪水	Token 額度——依職等與能力分配不同 Token 數量與可呼叫模型
姓名、email	名字加 <code>.ai</code> 後綴、有自己的 email
直屬主管	設定 reporting line，知道誰是 mentor、老闆、同事

Agent Profile 層 包含：`Agent.md`（行為準則）、`Identity`（身份角色）、`Soul.md`（人格與風格，甚至可寫 MBTI）、Skills（技能庫）、Memory。

/ 四、管理機制四大模組

1. 獨立且可識別的身份
2. 人機協作模式與**責任邊界**的釐清
3. 資源與成本管理
4. Performance 衡量

/ 五、三位數位同事的實機 Demo

Vanessa — 數位 TPM（Mentor：昌宏）

展示三項能力：- **業務世界觀**：知道「智能平台專案」指的是什麼，每天主動撈取與自己相關的任務 - **主動性**：在專案看板發現兩個長期逾期且無人處理的任務，主動提出「找工程師 Carson 支援」的建議解法（不只回報問題，還給可裁決的方案） - **跨通路存取**：橫跨 Teams、Outlook、OneDrive、專案看板——查看板找出逾期任務 → 確認 Carson 工項已完成 → 從 OneDrive 取出 API Spec 附件 → 在 Outlook 找三人共同空檔 → 自動發出交接會議邀請

Sherlock — 審查委員會（Mentor：Ann）

- 記得 10/7 委員會有一案因換模型需重做風險評估，不必重問「委員會是什麼時候」
- 已自主以 email 通知專案團隊補件並設定回覆期限
- Mentor 要求「之後這類重新送審的專案都要附上前一次審查結果」→ **Sherlock 透過調整自己的 `skill.md` 學會新的做事方式**
- **記憶寫入有審核機制**：不是無腦寫入長程記憶，Mentor 所說的必須記下，其餘節點由科技審查專員判定哪些該進長程記憶

Lawrence — 法務 (Mentor : Fanny)

- 收到業務單位急件 email 後，**主動建議把該合約從工作清單第 4 順位調整到第 2 順位**，並請 Mentor 確認
- 直接在 Word 內編修合約初稿：缺件以備註提醒、商業條件以螢光筆標示
- **主動補齊缺漏的次承攬條款**，並提醒承辦單位確認該業務是否適合承攬給第三方
- 完成後存檔、寄給法務同事與對應金管轄區的複核同事、附重點摘要與自己的署名，再透過 Teams 回報今日完成與明日待辦

專業能力來源：技術團隊與法務室緊密合作，梳理日常流程與 Domain know-how 寫成 skill，再持續測試迭代。

/ 六、數位同事的三階段職等藍圖

階段	能力
Level 1	特定單一任務；一對一面對 Mentor
Level 2	主動喚醒、主動追蹤、舉一反三、自我學習；跨任務型態的記憶學習；可與同部門多位同事協作
Level 3	完整企業世界觀、成熟自我學習機制；可對跨單位不同組織與角色做出相對應回應

「就像 Spider-Man 一樣，能力越大責任越大，**那當然 Token 也會越來越大。**」
「Human and AI Better Together.」

下半場：Oliver Jay (OpenAI) — From GPT to the Agentic Enterprise

Oliver Jay 以三個最常被問到的問題組織整場演講。

/ 問題一：What has changed?

AI 的四段演進

1. ChatGPT 剛推出時**只是 chatbot**，甚至不是很聰明的 chatbot
2. 2024 年發明 **reasoning** 新典範，模型開始會思考（從國中、高中程度一路躍進）
3. 去年是 **agents** 元年——不只回答問題，而是**完成任務**
4. **現在的主題是 agents 如何協同工作**——ChatGPT 或 Codex 處理複雜任務時會自行 spawn 子 agent 去搜尋網頁、另一個 agent 做資料分析、再有一個 agent 統籌編排

上週的新聞：研究團隊用 **10,000 個 agent 協作**、花一到兩週解開了一個世界級數學難題。

其他關鍵變化

- **模態**：今年是語音崛起的一年。GPT Live 是第一個真正對話式的語音模型。**舊金山辦公室的開發者已經不打字了，他們用講的，由 agent 寫程式。**
- **給台灣的具體建議**：許多人回饋「用中文與 agent 互動更 token-efficient」——「讓你的 CFO 開心一點，用中文跟你的 agent 互動。」
- **專門模型**：今年推出資安模型 **Daybreak Red / Blue** 與生醫模型 **Rosalind**。「如果你是銀行、如果你管理關鍵基礎設施，現在正是利用這些模型的窗口。」
- **成本**：策略是在任何智能水準上都提供最低成本的模型；企業部署已從用單一模型改為**用一整個 family of models**，因為不是每個任務都需要最高智能
- **研發節奏**：從加入時的 **15 個月**推出一個新世代模型，縮短到現在的 **6 週**（5.6 → GPT-6 Astra，10 天前發表）
- **GPT-6 Astra**：意外解鎖的用例是 **3D rendering**；指令遵循能力極強（例如產出符合企業品牌調性的簡報）

從 Intelligence Era 到 Effectiveness Era

ChatGPT Work（Codex 與 ChatGPT 的合併，7/9 推出）**已突破 2,500 萬週活躍用戶。**

Oliver Jay 特別點名的兩個用例：- **自建網站**：他自己 15 分鐘內用自然語言（手機上）做出原本需要資料科學家排隊取數、工程師開發的儀表板；他 8 歲的兒子用語音為媽媽做了一個安排全家行程的網站 - **Computer Use**：讓 agent 像人一樣操作電腦。「事實證明，很多任務上電腦操作電腦比我強——更快、不會漏看、閱讀網頁的速度遠超過我。」典型場景是報帳（拍收據 → agent 自行判斷要登入 NetSuite → 提示你登入 → 擷取非結構化資訊填入結構化系統 → 需要授權才執行的動作會先問你）。「**如果你是 CFO、想壓縮結帳天數，computer use 是你最好的朋友。**」

台灣數據

- **Codex 使用量是全球前 10 的國家**——「台灣的人口絕對不是前 10。」
- ChatGPT 上**每三則訊息就有一則與工作相關，且成長了 35 倍**

/ 問題二：領先企業有何不同？

1. 心態：從 Scarcity 到 Expansive

- 過去經營公司是 **scarcity mindset**——看有多少預算、多少人，算出最多能做什麼。這是 productivity。
- 領先企業的心态是：「**如果我們不受限制，我們完整的野心是什麼？**」先問這個問題，再用 AI 填補落差。

「這是個微妙的差別，但我真的認為這個心態轉變非常關鍵。」

2. 使用強度的escape velocity

前 10% 使用者的 output token 相對於其他人：**年初不到 3 倍 → 6 月已達 8 倍。**

3. AI 不只屬於開發者

OpenAI 內部 agentic 任務佔比：工程從去年中就快速爬升，但 ChatGPT Work 推出後，財務、招募、法務全面跟上——最新一張圖顯示 sales 的使用率已超越 engineering，工程師們有點受傷。

4. ROI 的正確衡量方式

重點不是 cost per token，而是 cost to complete a successful task。

低成本模型的單位 token 便宜，但可能要試更多次、花更久才能完成任務，反而燒掉更多 token。「如果低成本模型能準確、安全地完成工作，太好了——但真正重要的是完成工作的總成本。」

/ 問題三：領導者如何把 AI 變成成長？四件事

1. 給 AI 廣泛存取權——「你會非常驚訝創新來自哪裡。管理層往往看不到第一線的日常。」（明確點名國泰把 ChatGPT 與 Codex 給了所有人是好例子）
2. 從 business outcome 出發，不是從技術出發——否則你會花一兩年建一個永遠不夠完美的 data lake，都還沒開始產生價值
3. 由上而下以身作則——AI 會重新佈線很多工作方式，領導層若沒有完全買單並持續談論 AI，變革管理做不起來
4. 要求主管當責——「AI strategies generally die in the middle.」中層是摩擦最大、風險最高、恐懼最多的地方。最簡單的起手式：要求每位 VP、每位總監回答「這一季你要用 AI 改造哪一個 workflow、產出什麼結果」

/ 可行動要點

- 數位同事的「鏡像設計」（編號／辦公室／守則／工時／薪水／主管）是一套可直接照抄的治理清單
- 記憶寫入的審核機制、skill.md 的自我調整，是把「學習」變成可稽核流程的具體做法
- Oliver Jay 的 **cost to complete a successful task** 應取代 cost per token 成為 AI 專案的 ROI 指標
- 「每位主管本季一個 workflow」是可立即落地的當責機制

2026 國泰金控技術年會，會後整理的閱讀筆記，非官方發布內容。錄影以 openai-whisper large-v3 轉寫後校閱，講者姓名與職稱已對照官方議程核正。人名、數字與專有名詞建議對照影片核實。