INSIDE

AI Agent 元年

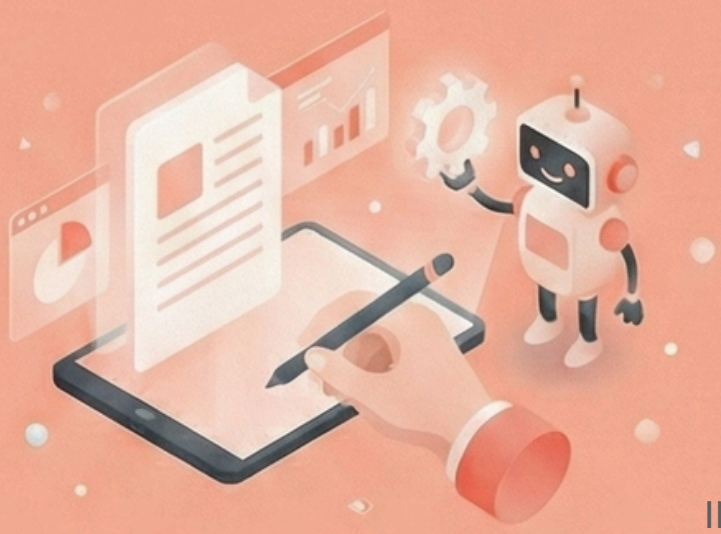
台灣企業的導入現況與未來挑戰

從自動化到自主化：跨越 GenAI 落地鴻溝的關鍵戰略指南

調查期間 2025 年 8 - 11 月
有效樣本 157 份決策層 + 20 家品牌專訪

發布單位 ｜INSIDE 硬塞的網路趨勢觀察　策略夥伴｜SUPER 8 Studio 雲發互動科技

目錄
Table of Contents



編輯序言
Editor's Note

INSIDE 2025 台灣 AI Agent 生態系大調查

從「對話」走向「行動」的生產力革命

過去兩年，生成式 AI (GenAI) 以驚人的速度席捲全球，企業與工作者沉浸於它強大的內容創作與程式碼輔助能力。然而隨著 2025 年的到來，INSIDE 觀察到一個明顯的轉折點：企業不再滿足於跟 AI「聊天」，而是要求 AI 開始「做事」。
當 AI 從單純的「對話工具」進化為具備自主規劃、決策與執行能力的「數位協作者」時，全球正式迎接了 AI Agent（人工智慧代理） 的元年。這不僅是技術架構的升級，也代表著企業數位轉型從被動的「自動化 (Automation)」邁向主動的「自主化 (Autonomy)」。

為了釐清台灣企業在這一波浪潮中的真實站位，INSIDE 硬塞的網路趨勢觀察發起了本次《2025 台灣 AI Agent 生態系大調查》。我們發現一個既焦慮又充滿機會的現實：雖然廣義 AI 工具已成為 43.3% 企業的標配，但具備自主性的 AI Agent 實際落地率僅 15.9% 。

這 27.4% 的巨大落差，即是我們定義的 「GenAI 鴻溝」。

我們發現阻礙企業跨越這道鴻溝的並非單純技術門檻，而是更深層的商業邏輯挑戰 - 高達七成的企業陷入「預算迷霧」，近四成企業苦於「找不到應用場景」，而決策層對「數據幻覺」的擔憂更甚於對效率的追求。

這份白皮書不僅是一份數據報告，更是一份行動指南。我們結合了量化數據與 20 餘家跨產業品牌的實戰經驗，試圖為您解答：如何破解預算困局？如何建立人機協作的新型態？以及如何讓 AI Agent 真正成為驅動營收的增長引擎。願這份報告能協助您在 AI 浪潮中，從觀望轉向行動，跨越鴻溝，掌握自主化的未來。

INSIDE 主編

鍾效京

INSIDE 資深編輯

張雲萱

關鍵研究發現 Key Research Findings

1. 預算迷霧鎖住創新 (The Budget Fog)

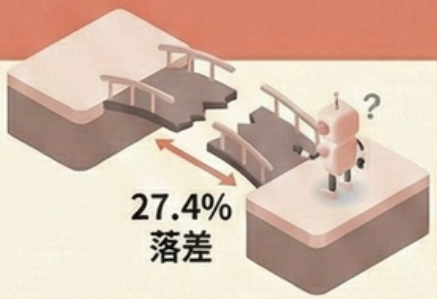
70.9%

企業無法估計年度預算。用量計價與固定預算的結構性衝突，是規模化落地的隱形天花板。

2. 落地鴻溝確實存在 (The GenAI Gap)

廣義 AI 43.3% vs. Agent 15.9%

跨越「實驗室」到「生產線」的死亡之谷，
多數企業卡在技術轉化路徑。



3. 阻礙落地的真相：沒場景、沒人才

並非技術不可行，而是商業邏輯未明。

38.2% 的企業表示「缺乏明確應用場景」是最大障礙，37.6% 苦於「缺乏專業人才」。

4. 信任危機大於效率追求

75.8% 關注可靠性 vs. 26.8% 關注效率

決策層不敢放權的主因是「幻覺」。
若不「誠實可控」，效率再高也買單。

5. 實戰培訓需求強烈

約 67%

企業展現高度學習動能，急需解決
具體問題的實戰指南，而非高深理論。

Chapter 1：受訪輪廓 - 誰在定義台灣的 AI 未來？

摒棄倖存者偏差，還原真實的產業視角

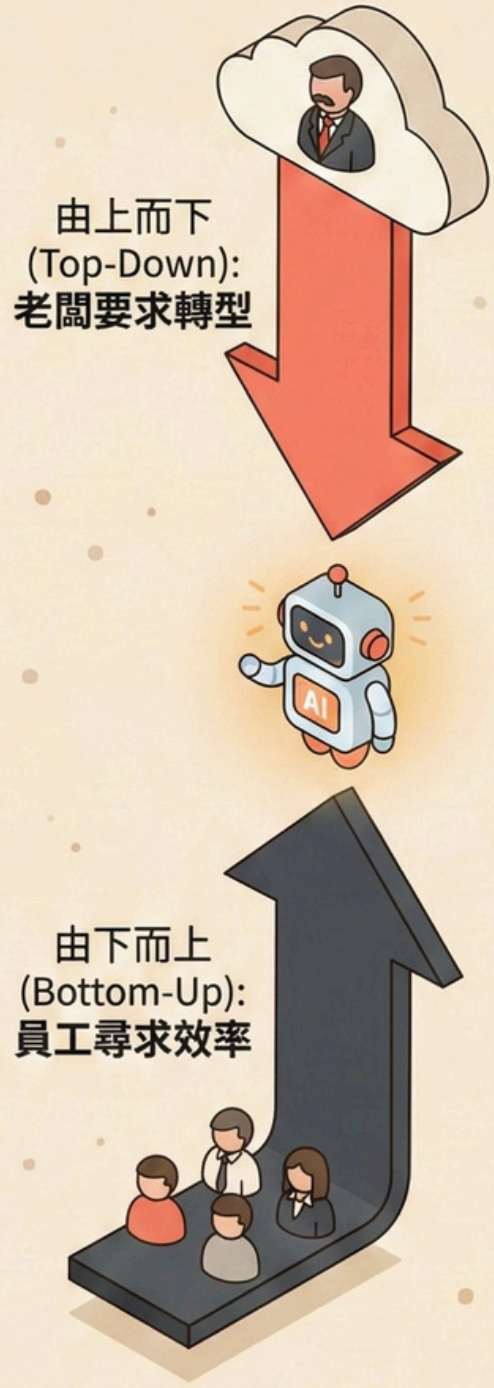
1. 受訪者結構
(Respondent Structure)

決策層
(Decision Makers)
22.4% (C-Level, 企業主)
關注 ROI 與長期競爭優勢，推動大型專案發動機。

中階主管
(Mid-managers)
28.2%
夾在預算與績效之間，感受實際摩擦痛點的執行者。

一般員工
(Staff)
44.2%
第一線使用者，反饋工具是否好用或增加負擔。

AI Agent 推動力：雙向夾擊
(Drivers: Two-Way Pressure)



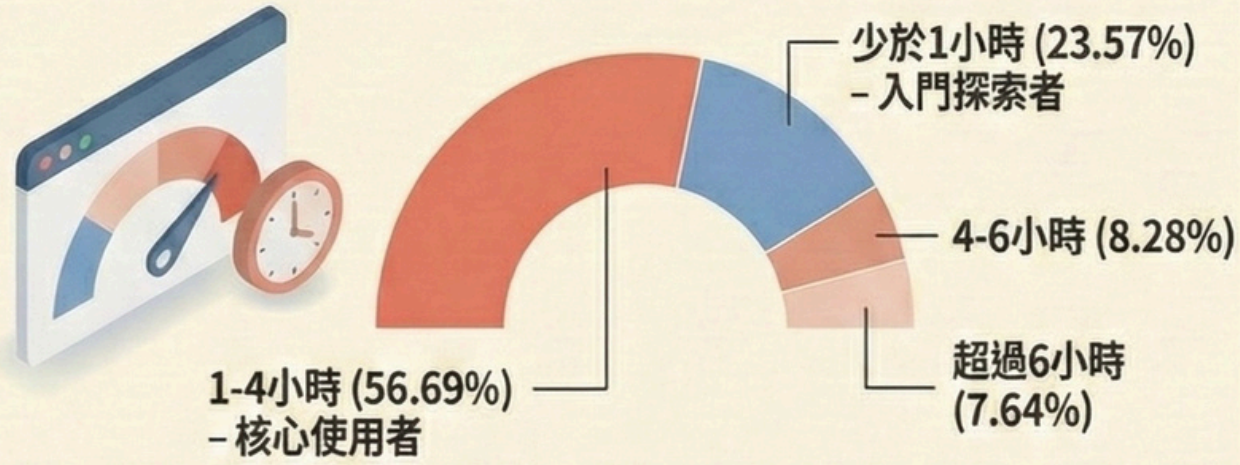
由上而下
(Top-Down):
老闆要求轉型

由下而上
(Bottom-Up):
員工尋求效率

橫向部門間存在巨大「數位落差」

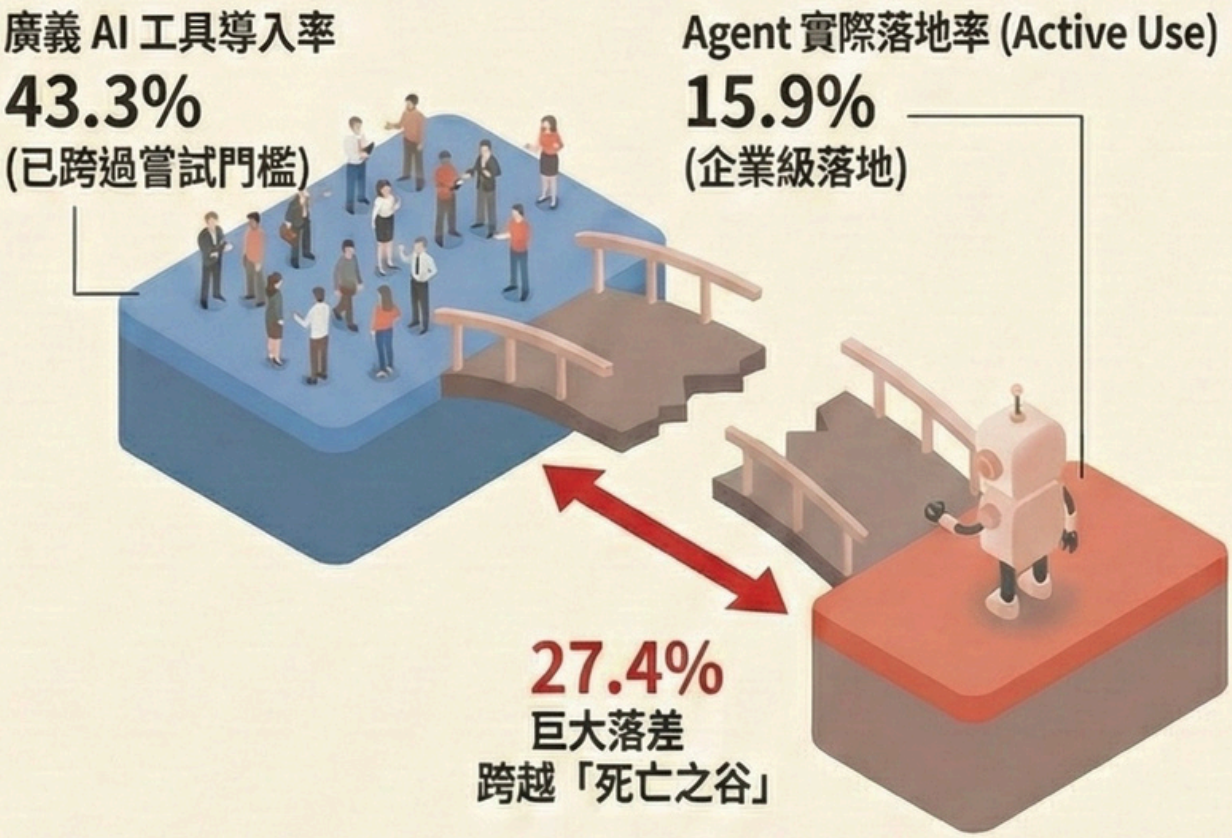
1A. 工作者 AI 工具使用強度與 Agent 導入現況

工作者 AI 工具使用強度 (Worker AI Usage Intensity)



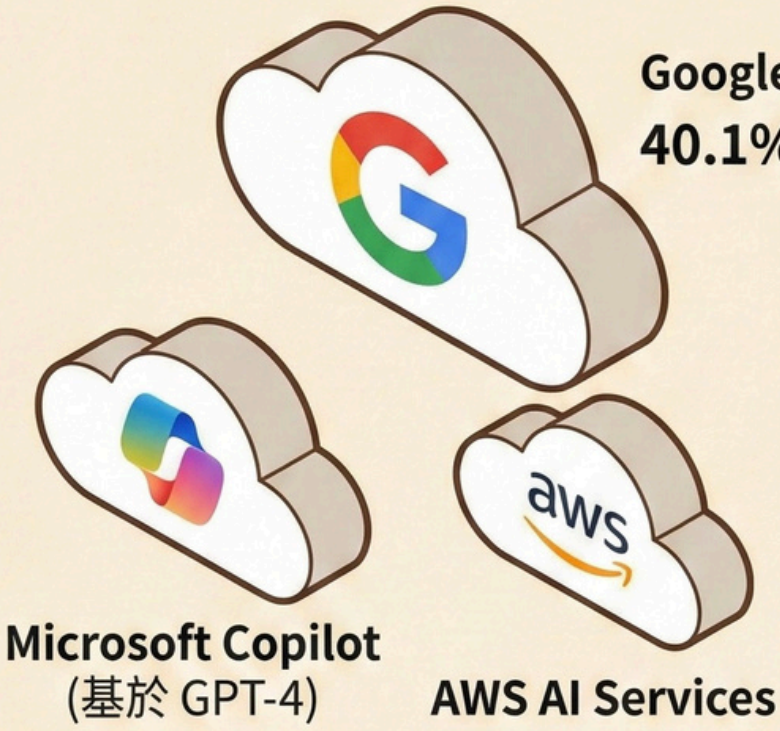
總體普及率 (Total Penetration): 96.18% (員工接受度已是標配)

GenAI 鴻溝的體現 (The GenAI Gap)



企業重心應轉向解決「流程整合」與「場景設計」

市場平台分佈：全球巨頭領跑

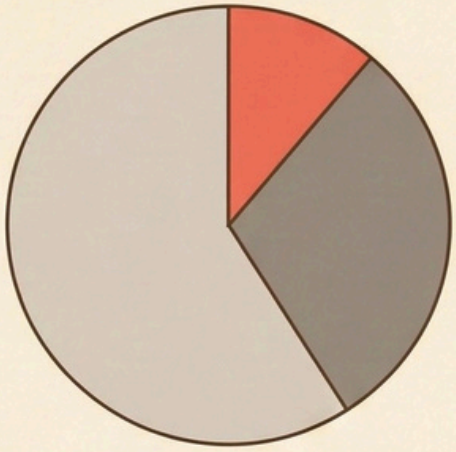


Google Gemini (或相關 Agent 應用)
40.1% (提及度最高)

Microsoft Copilot
(基於 GPT-4)

AWS AI Services

主流選擇：「雲端原生」且「完整生態系」的解決方案。



觀望與評估：40.76%
(11.46% 評估中 + 29.3% 有興趣)

2. 部門熱力圖：誰跑得快？誰在踩煞車？

領跑者 & 實戰派

- 經營管理 (Management): 63% (由上而下戰略轉型)
- 資訊/IT (IT Dept.): 53% (技術賦能者)
- 行銷/業務 (Marketing/Sales): 50% (現在進行式工具)

- 研發/技術 (R&D/Tech): 41%
- 客戶服務 (Customer Service): 38%

觀望者 - 保守區塊

- **財務/法務 (Finance/Legal): 0%** (防弊大於興利，零容錯)

企業內部「AI 黃金三角」與「保守區塊」溫差明顯

3. 產業分佈：科技領跑，製造跟進

資訊科技/軟體業
(IT/Software) 33.1%
技術提供者與先行者，定義 AI Agent 技術標準。

製造業
(Manufacturing) 14.6%
強烈需求自動化排程與供應鏈優化，提升良率與產能。

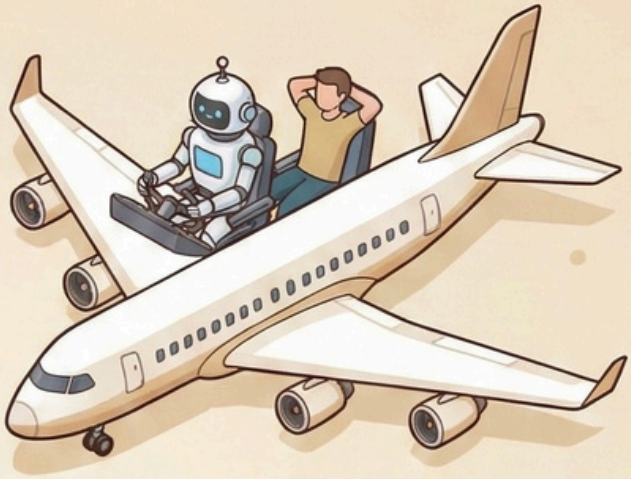
服務業
(Service) 10.2%
聚焦客戶服務自動化，填補大夜班與假日人力缺口。

金融保險業
(Finance/Insurance) 3.2%
高度法規監管與個資考量，處於極早期試點或觀望階段。

Chapter 2：Agent 核心解析 - 大腦、工具與感官：自主系統的技術解構

1. 全球趨勢：從 Copilot 到 Autopilot (Global Trends)

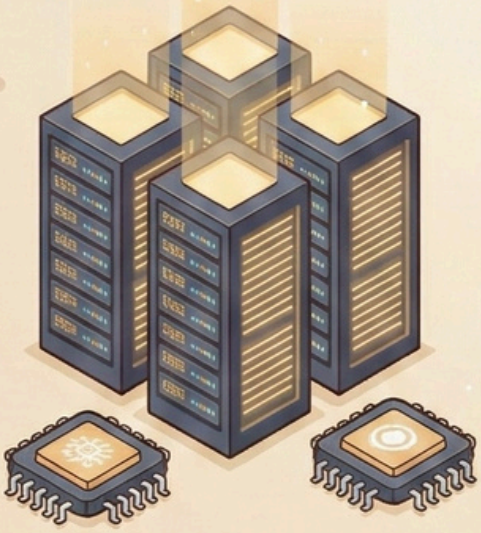
Copilot (副駕駛) - 人機協作
協助寫作、寫程式，人類仍為主導。



Autopilot (自動駕駛) - AI 自主完成
追求 AI 自主完成任務，
軟體即服務結果 (SAAS)。

2025 趨勢轉向

台灣視角：硬體先行，軟體跟進 (Taiwan Perspective)

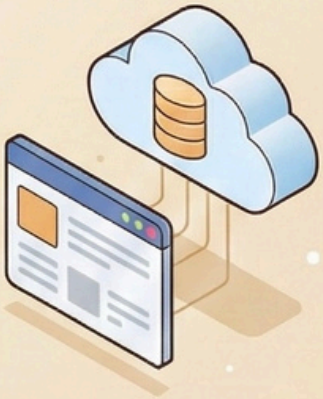


硬體實力：
全球 AI 伺服器軍火庫
(Hardware Leader)

廣義 AI 導入率 **43.3%**

VS

Agent 導入率 **15.9%**

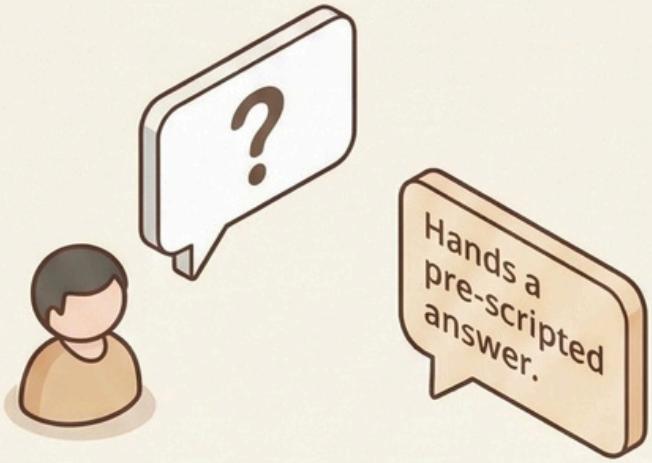


軟體應用：
軟硬整合關鍵時刻
(Software Lagging)

處於從「玩票性質」轉向「生產力落地」的陣痛期。

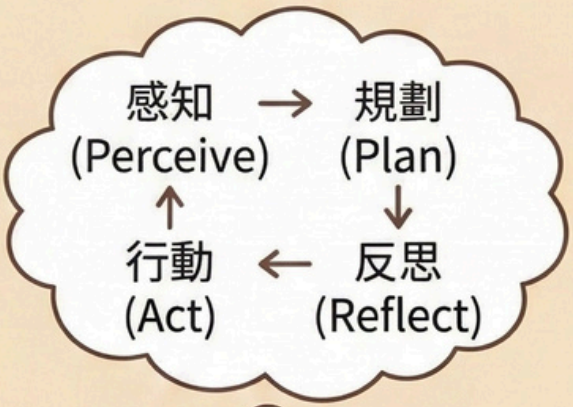
2. 定義：自主性的飛躍 (The Leap to Autonomy)

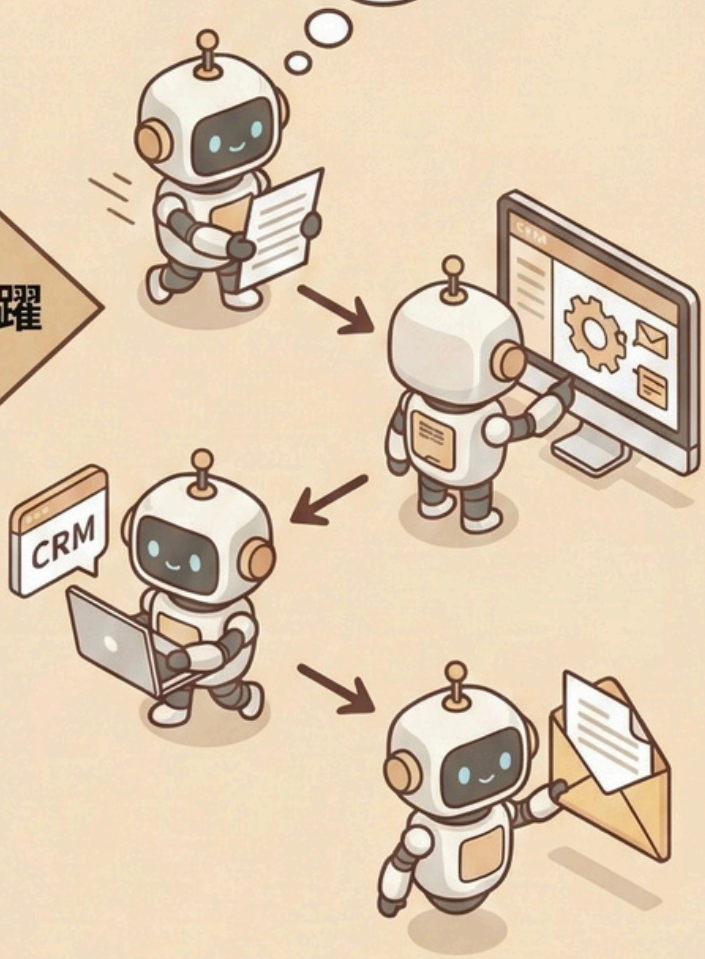
Chatbot (對話機器人)
－被動的諮詢員 (Reactive)



你問它答，只能根據預設腳本或資料庫回應。
無法離開座位解決問題。

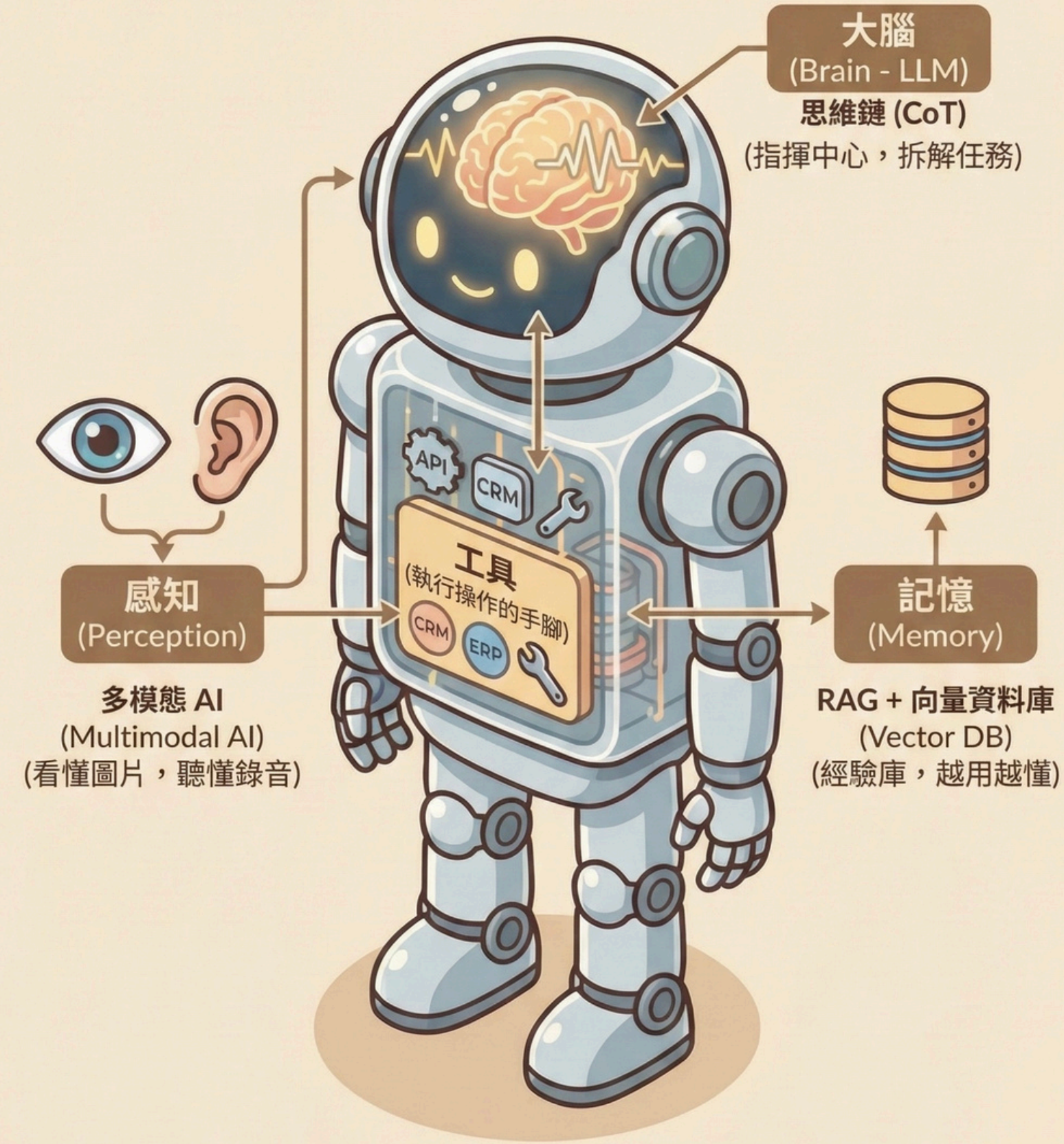
AI Agent (智慧代理)
－主動的特助 (Proactive)





主動幫你跑腿、填表、跨部門溝通。
不只給建議，直接幫你把事情做完。

3. 核心架構剖析
(The Anatomy of an Agent)

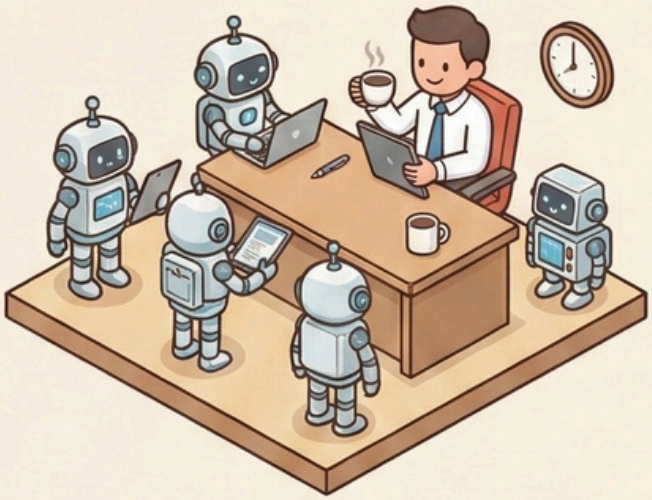


4. 工作型態變革：從「操作者」變為「管理者」(Work Transformation)

過去：操作者 (Operator)
- 人機關係

User 操作軟體，需自行拆解任務。

未來：管理者 (Manager)
- 人機關係重塑



指揮 Agent，懂得拆解任務並驗收成果。

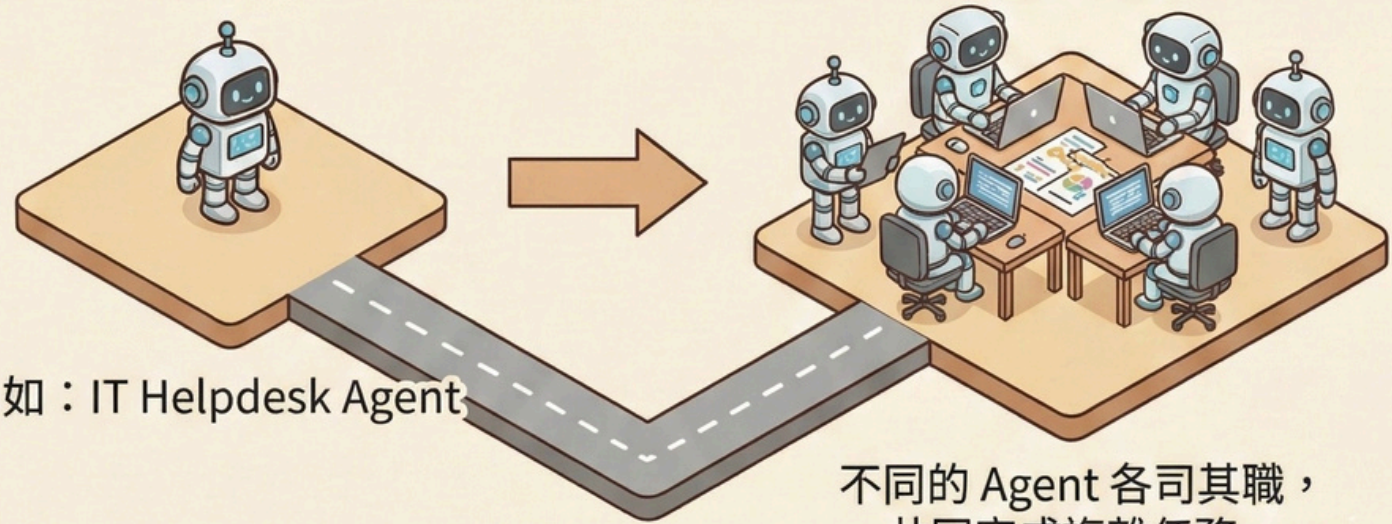
24/7 非同步生產力：Agent 打破時間限制，後台持續工作。

台灣企業主觀點：關注數據可靠性 (75.8%)，需具備「可解釋性 (XAI)」才能贏得信任。

5. 進化路徑：從 Single Agent 到 Multi-Agent Systems (MAS)

Single Agent (單一智慧體)
- 個人工作者

Multi-Agent Systems (多智慧體協作)
- 專業團隊

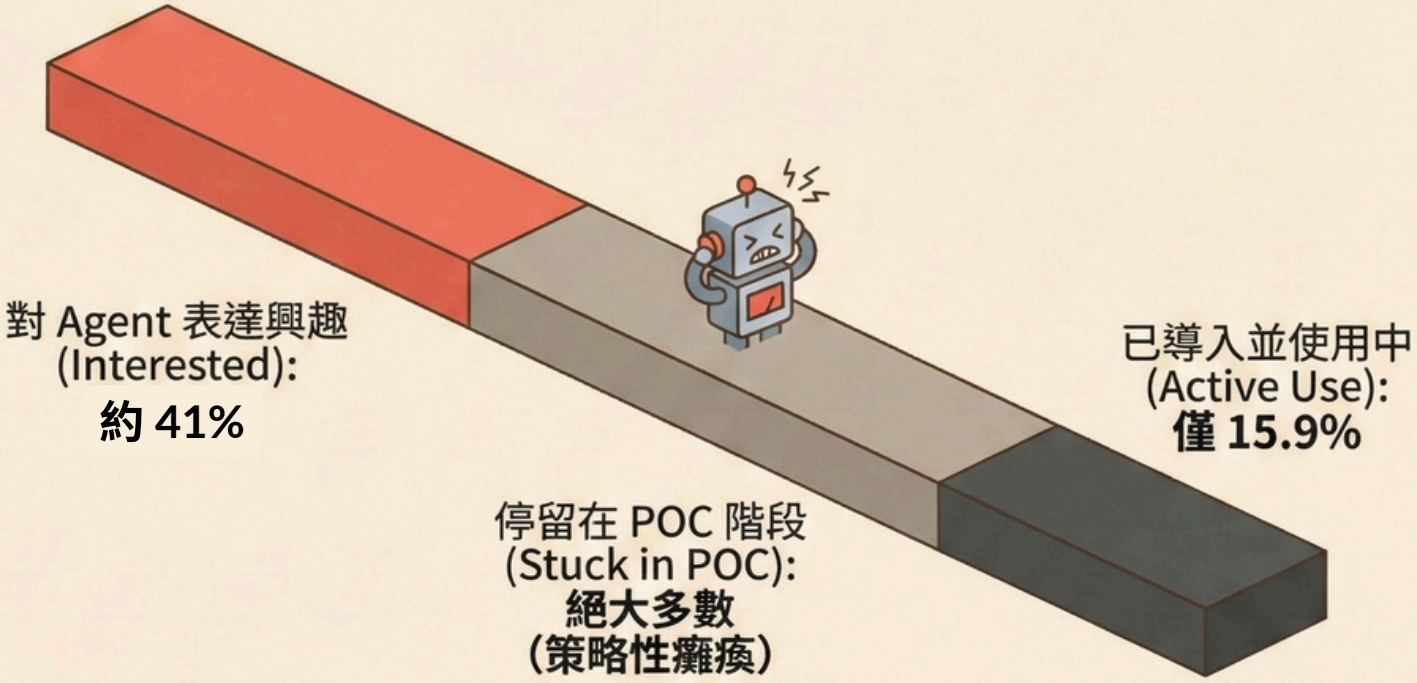


如：IT Helpdesk Agent

不同的 Agent 各司其職，共同完成複雜任務。

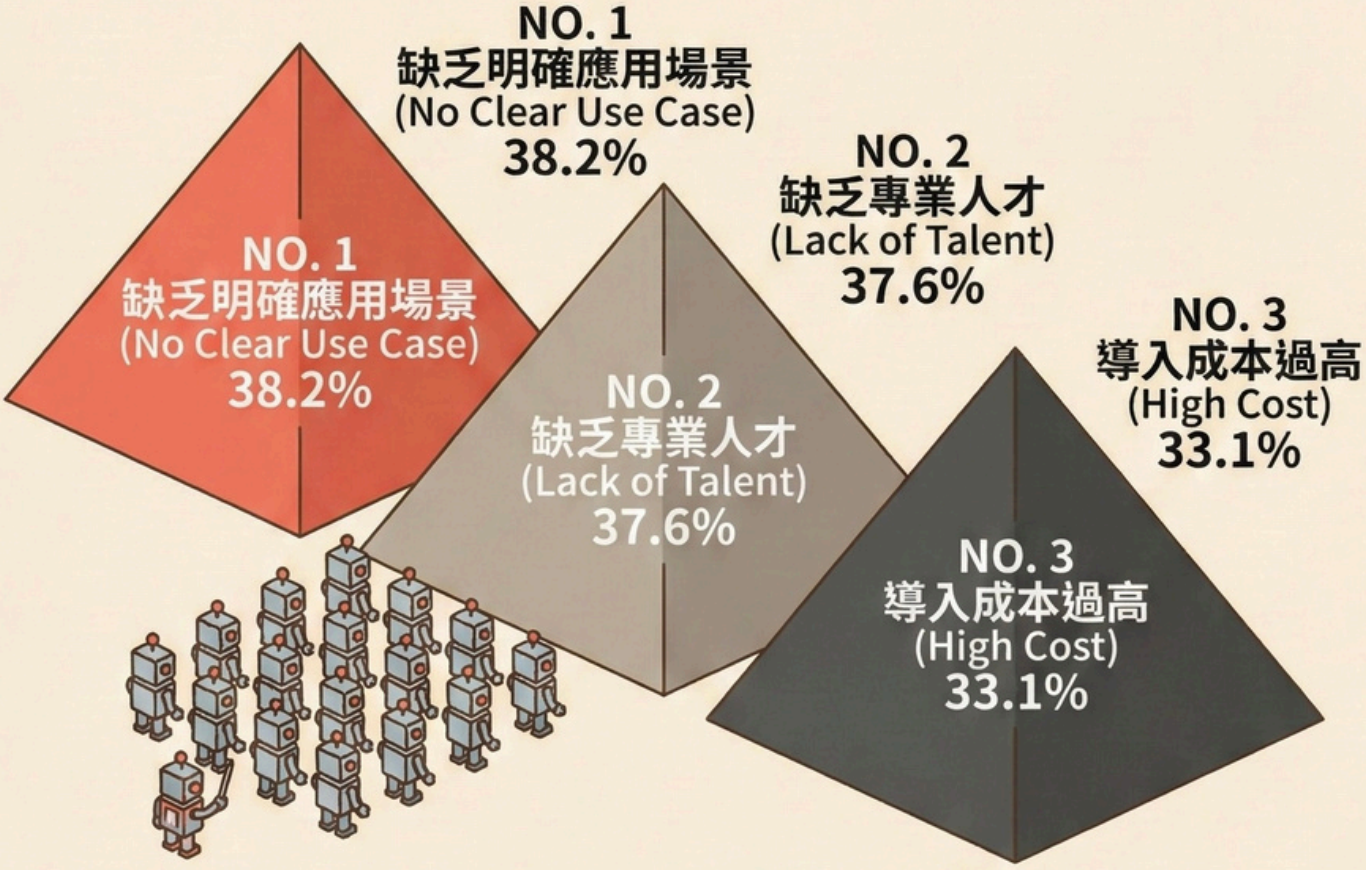
Chapter 3：導入現況 - 跨越落地的「三座大山」

1. 現況點評：從「觀望」到「焦慮」的僵局 (The Stalemate)



知道好，但不知從何下手、誰做、錢怎算。

2. 深度分析：阻礙落地的三座大山 (The Three Big Mountains)



如何移除這三座大山？解方在後頁。

3. 解方一與解方二：移除場景與人才大山 (Solutions 1 & 2)

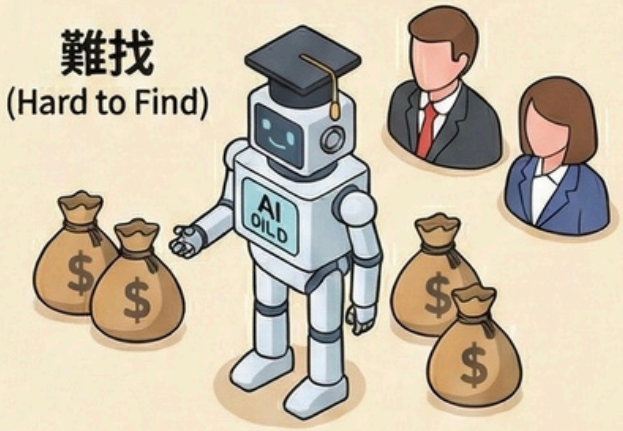
NO. 1 缺乏明確應用場景 (No Clear Use Case) 38.2%

NO. 2 缺乏專業人才 (Lack of Talent) 37.6%

通用模型 (General LLM) - 解決垂直問題

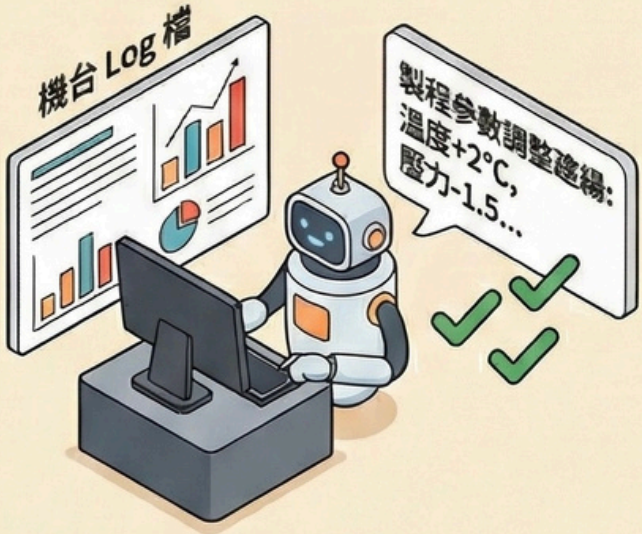
產出結果空泛，無法落地。

招聘 AI 科學家 (Hiring AI Scientists) - 誤區



企業普遍認為需招聘昂貴專家。

【產業標竿】台智雲 (TWS) 垂直 Agent (Vertical Agent) - (FFM)



懂行業 Know-how，找到真正應用場景。

【產業標竿】台智雲 (TWS) AI 代工 (AI Foundry) - (AFS 平台)

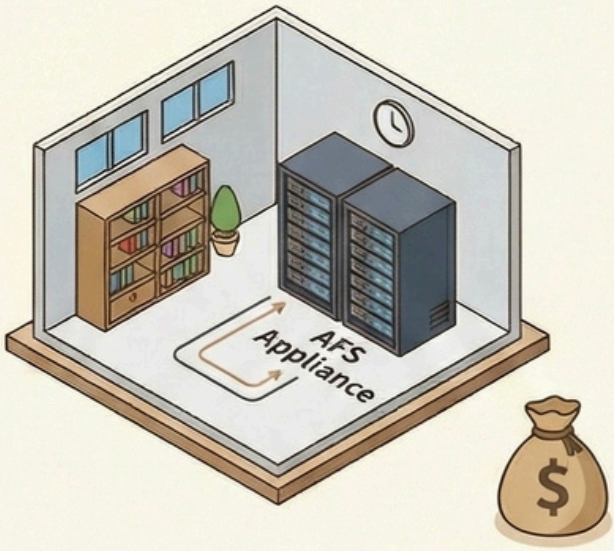
利用現有人力，快速構建專屬 Agent。

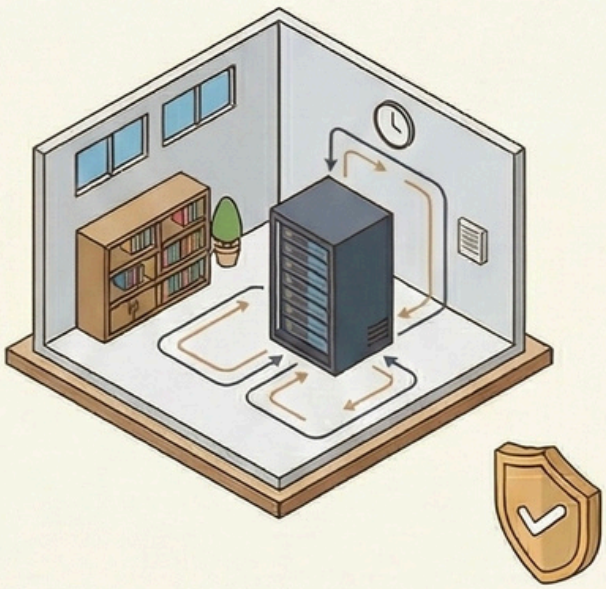
NO. 3 導入成本過高 (High Cost) 33.1% - 解方

公有雲 API (Public Cloud API) - 不可預測性 (Unpredictable)

成本隨 Token 浮動，資料傳輸海外，資安合規風險高。

【產業標竿】台智雲 (TWS) 主權 AI (Sovereign AI) - 地端部署 (On-Premise)





數據不出門，成本可控 (固定投資)，解決資安與合規擔憂。

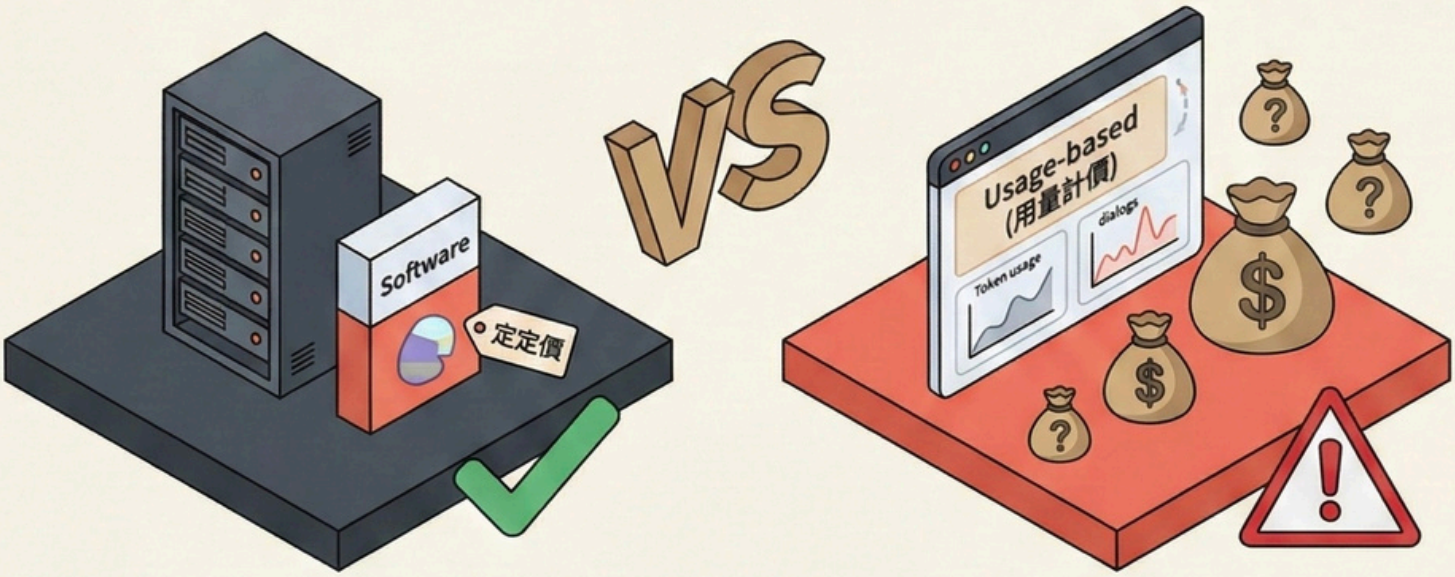
1. 預算迷霧：71% 的不確定性 (The Budget Fog)

「錢不是問題，問題是『不知道該編多少錢』。」

結構性衝突：計價模式劇烈碰撞 (Structural Conflict)

傳統企業 IT 採購
- CapEx (固定資本支出)

AI Agent 採購
- OpEx (營運支出)



成本固定、可攤提
(Fixed Cost, Amortizable)

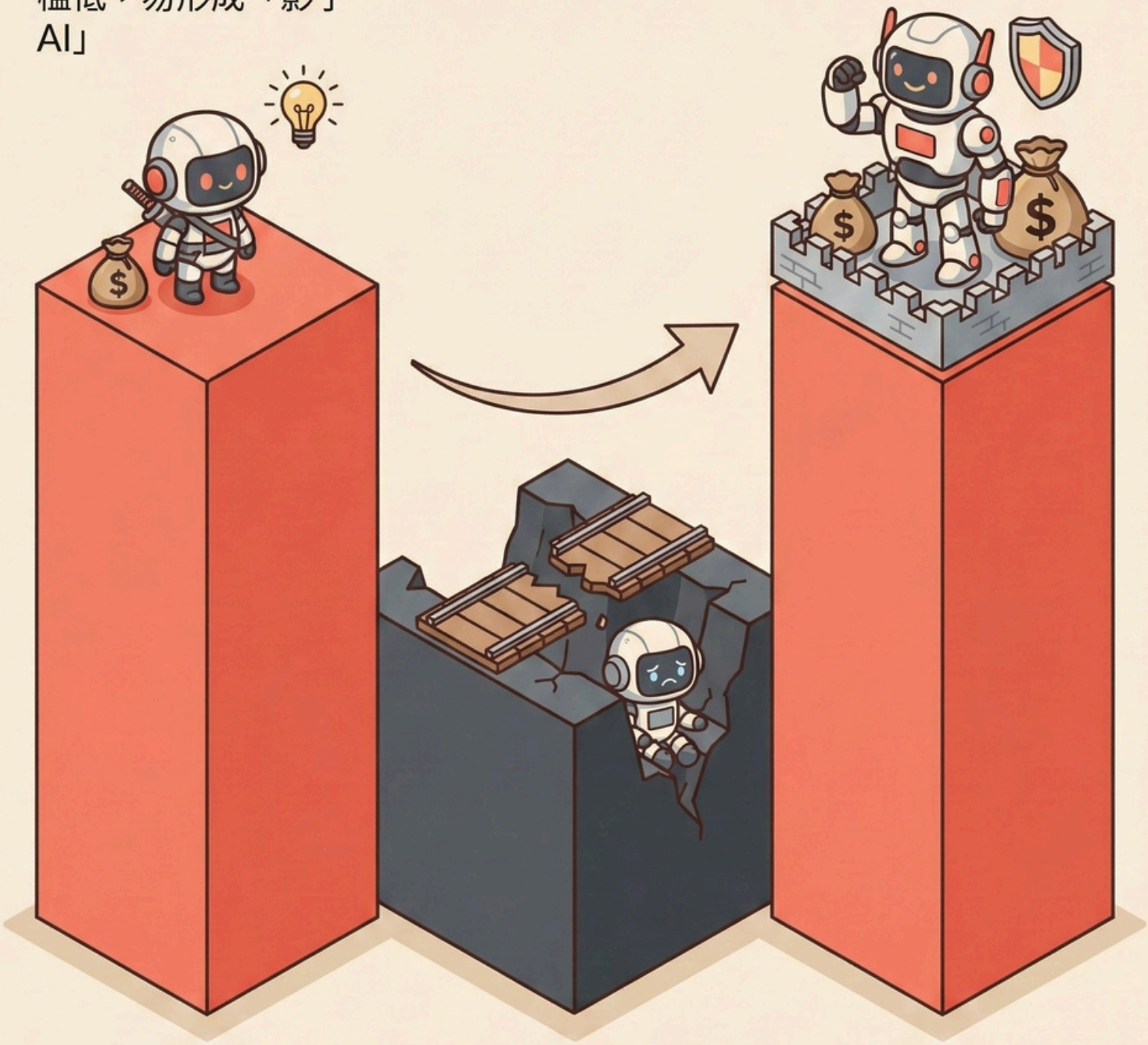
成本浮動、無上限
(Variable Cost, Uncapped)

財務審核黑洞：決策者恐懼不可控成本。

2. 市場極化：M 型化的預算分佈 (The M-Shaped Budget Distribution)

部門級別游擊戰：門檻低，易形成「影子 AI」

跨越信任鴻溝：投資私有化部署與資安



微型試錯 (POC) - < NT$ 10 萬 (52.3%)

部門級別游擊戰：門檻低，易形成「影子 AI」

死亡之谷 (Death Valley) - 10-60 萬 (23.1%)

規模化困境：缺乏 ROI 模型，死在沙灘上

戰略投入 (Enterprise) - > NT$ 60 萬 (24.6%)

跨越信任鴻溝：投資私有化部署與資安

3. 破局策略：333 敏捷預算法則 (The 3-3-3 Rule)

實戰公式：3 個月、30 萬、3 指標

1. 3 個月 (Timebox)

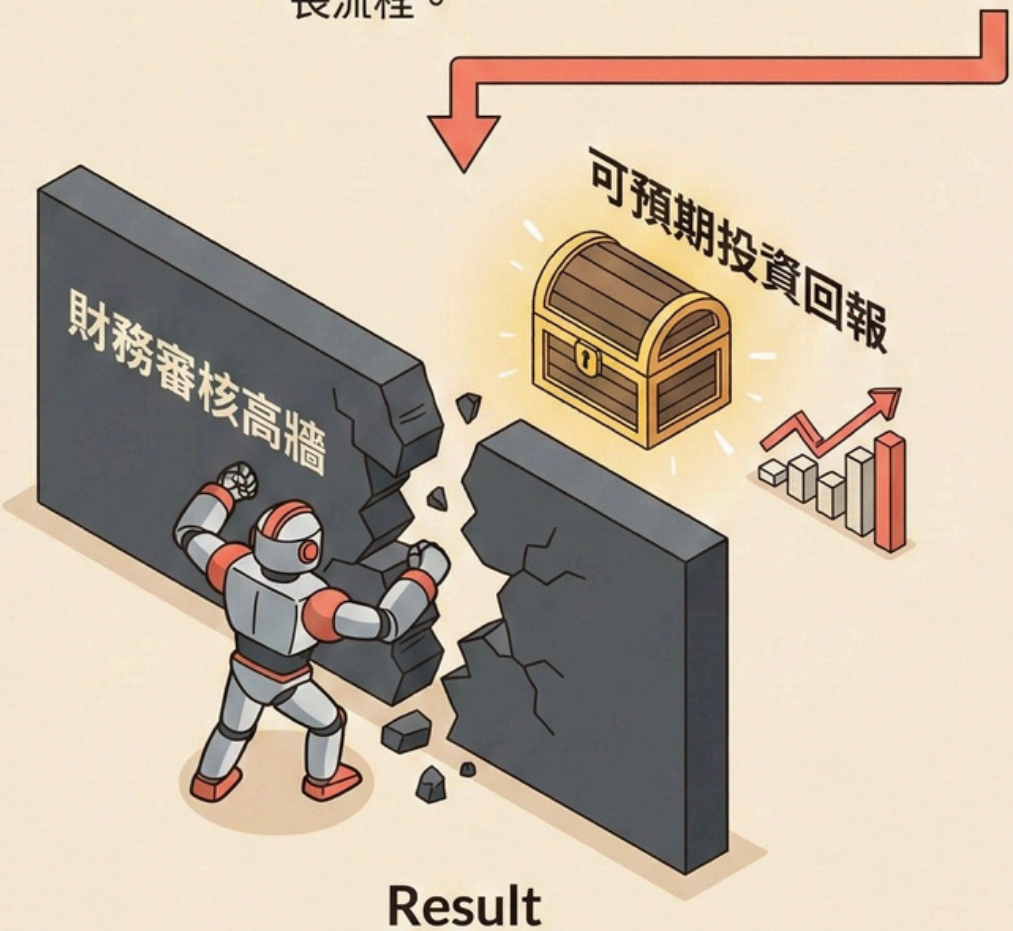
設定嚴格 POC 期限，專注 MVP，避免規格過時。

2. 30 萬 (Budget Cap)

控制在簽核上限，加速啟動，免除冗長流程。

3. 3 指標 (Key Metrics)

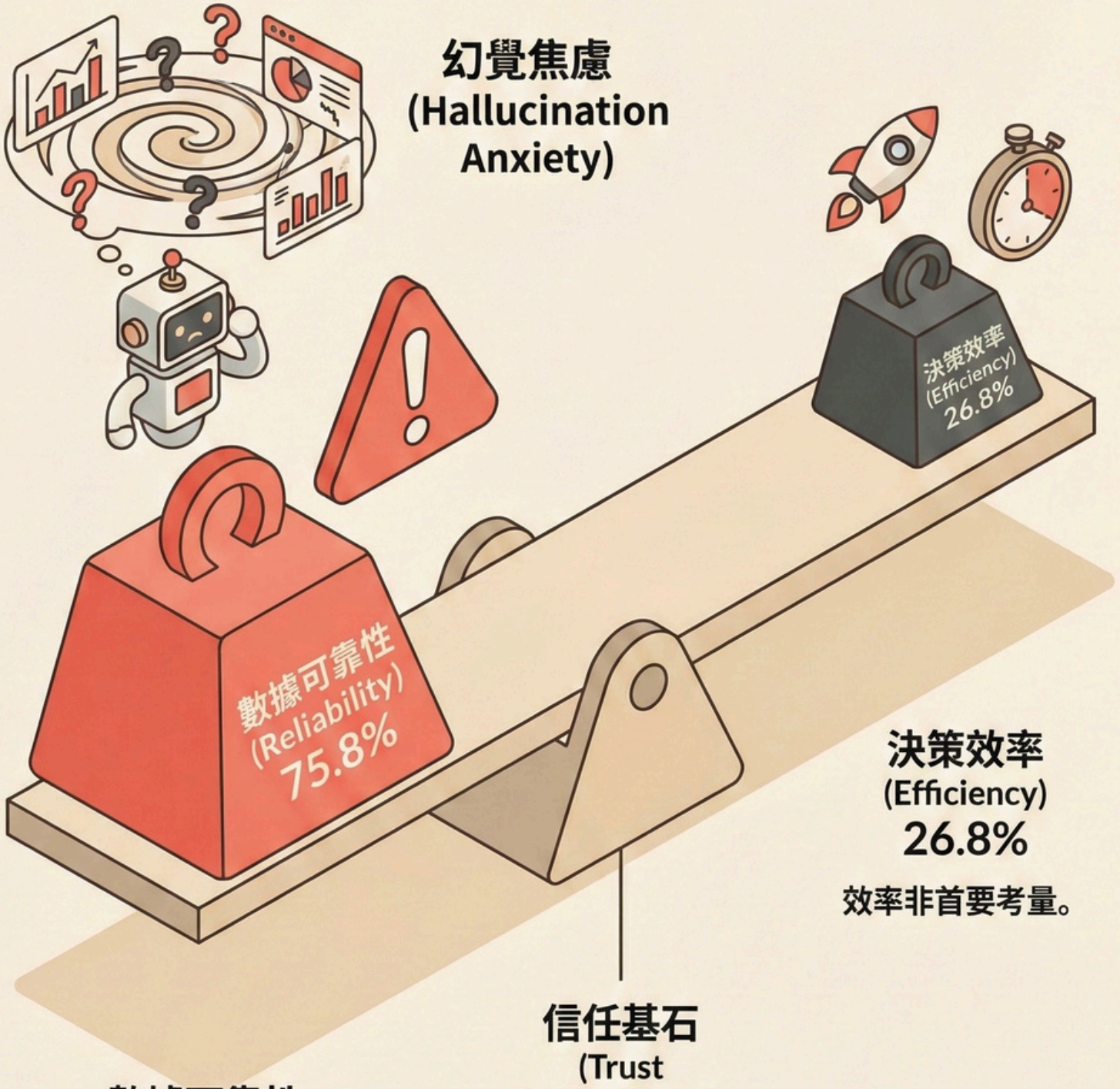
鎖定可量化指標，不只看 AI 準不準。



Result

將不可控 OpEx 轉化為可預期投資，打破審核高牆。

1. 信任危機的根源：75.8% 的恐懼來自「幻覺」(The Root of Trust Crisis)



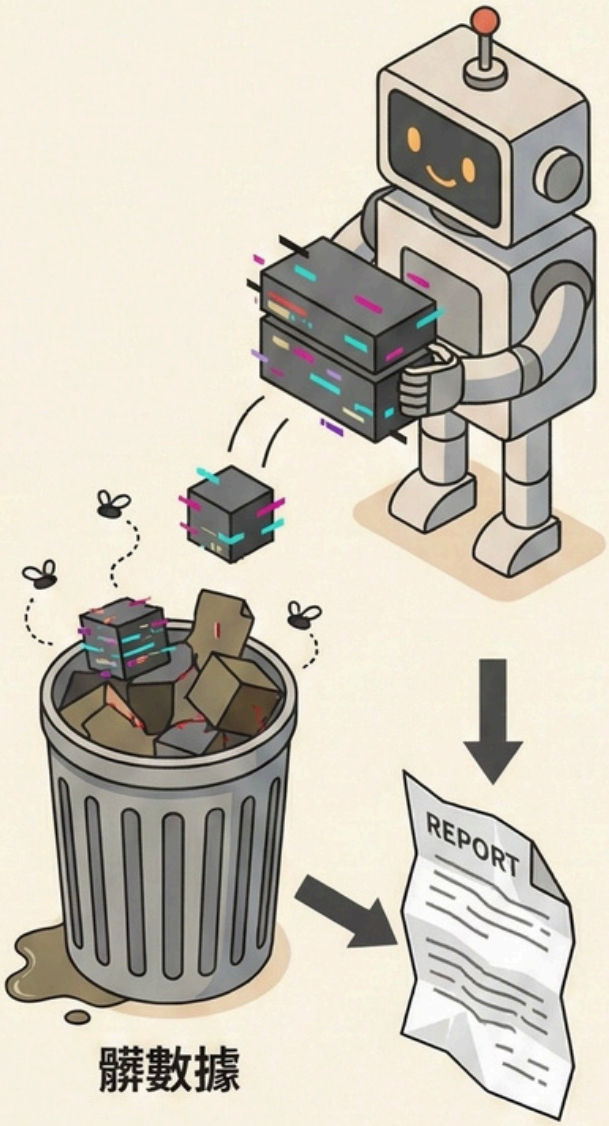
決策效率
(Efficiency)
26.8%
效率非首要考量。

信任基石
(Trust Cornerstone):
決策透明度 (XAI)
42.6%
無法解釋判斷，
只能做副駕駛。

數據可靠性
(Reliability)
75.8%
不敢對產出「簽字負責」。

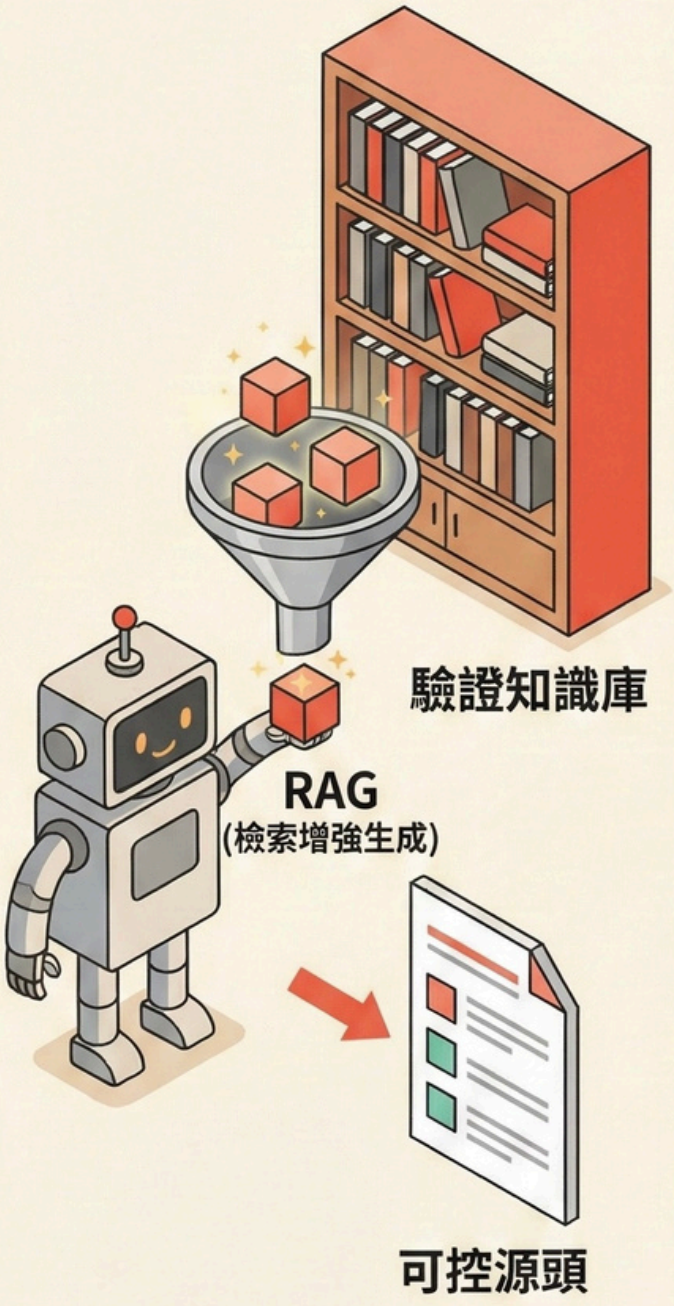
2. 專家觀點：遠傳電信談「AI 準備度」

數據即資產，治理即地基



沒有治理，AI Agent 只是空殼。

務實策略：RAG 為王



限制 Agent 僅根據內部驗證知識庫回答，確保資訊可控。

3. 內部治理：制度先行，圍欄築起

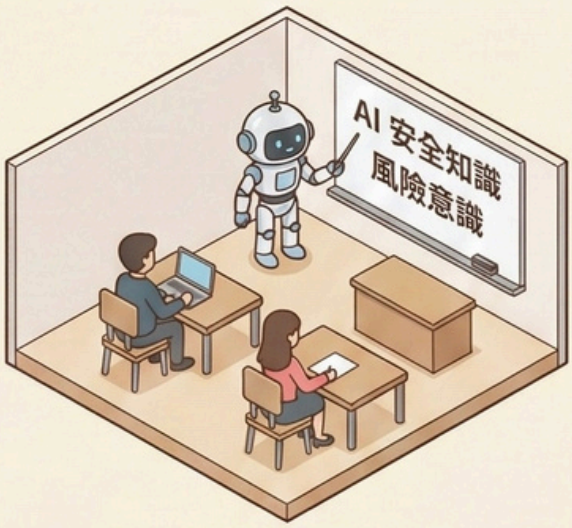
人治重於法治，建立第一道防線

建立內部使用規範 (19.5%)

建立內部使用規範 (19.5%)

訂定使用守則，禁止上傳機密。

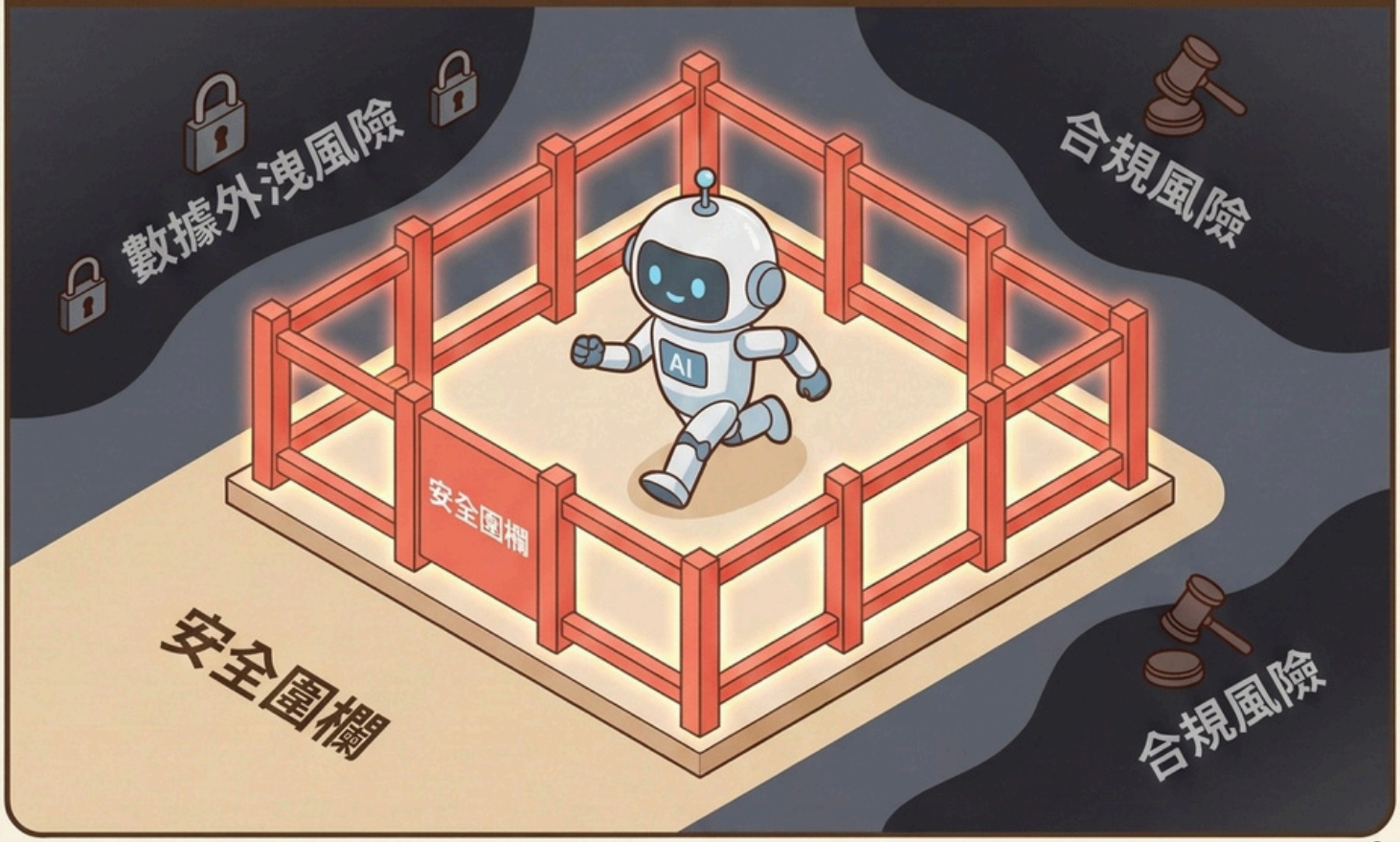
員工培訓 (19.4%)



員工培訓 (19.4%)

提升全員 AI 素養與風險意識。

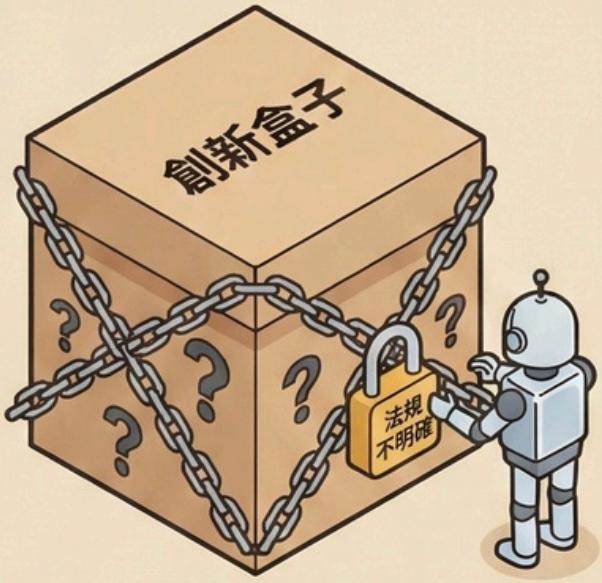
建立安全圍欄



先建立安全圍欄，才敢放手讓 AI 在圍欄內奔跑。

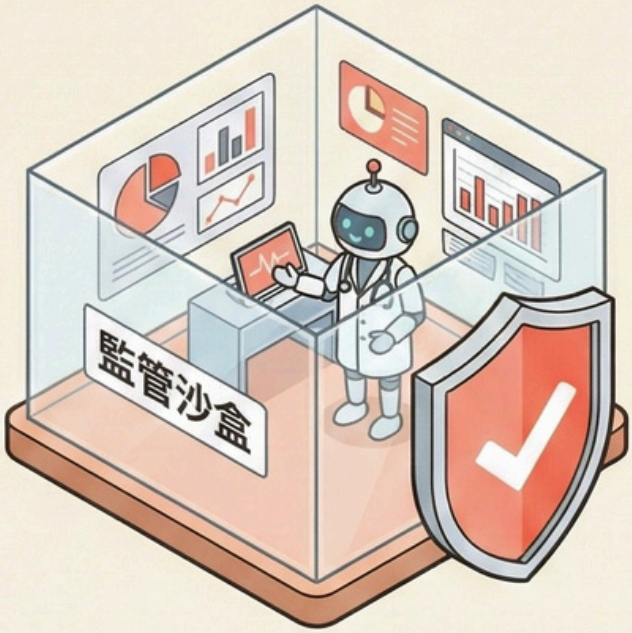
4. 外部政策呼聲：期待「監管沙盒」與明確指引

法規不確定性阻力 (4.1%)



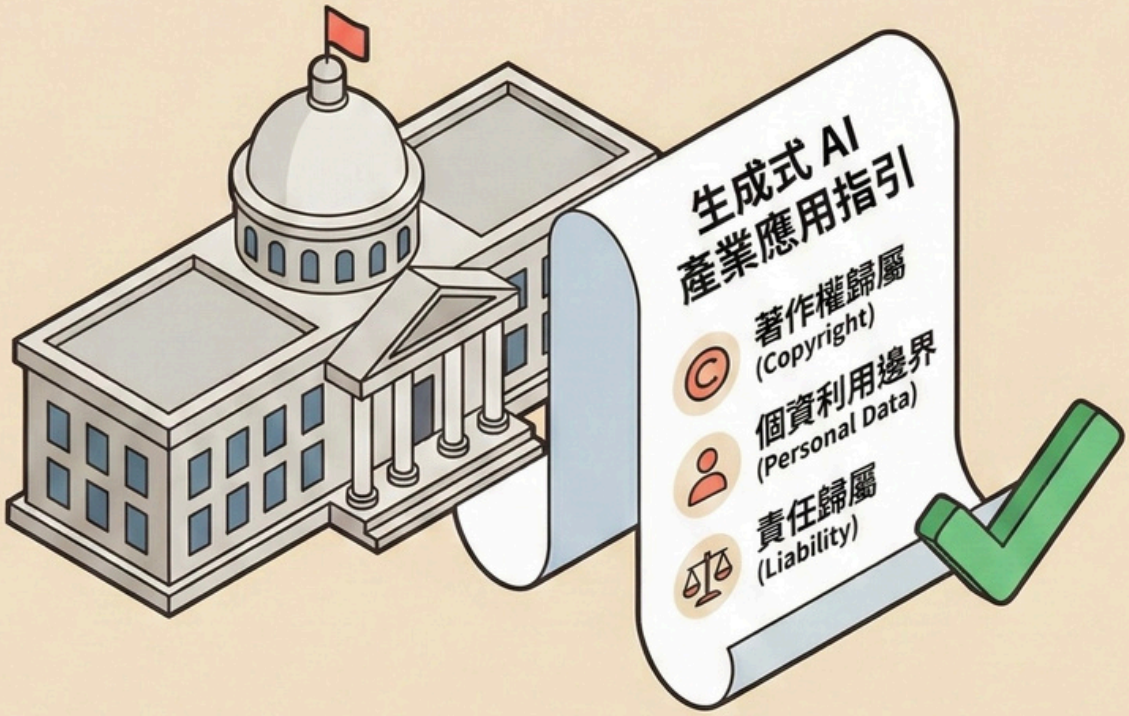
高監管產業因法規不明而遲疑。

期待「監管沙盒」



允許在可控風險內測試高風險應用。

政策建議：盡速發布「生成式 AI 產業應用指引」

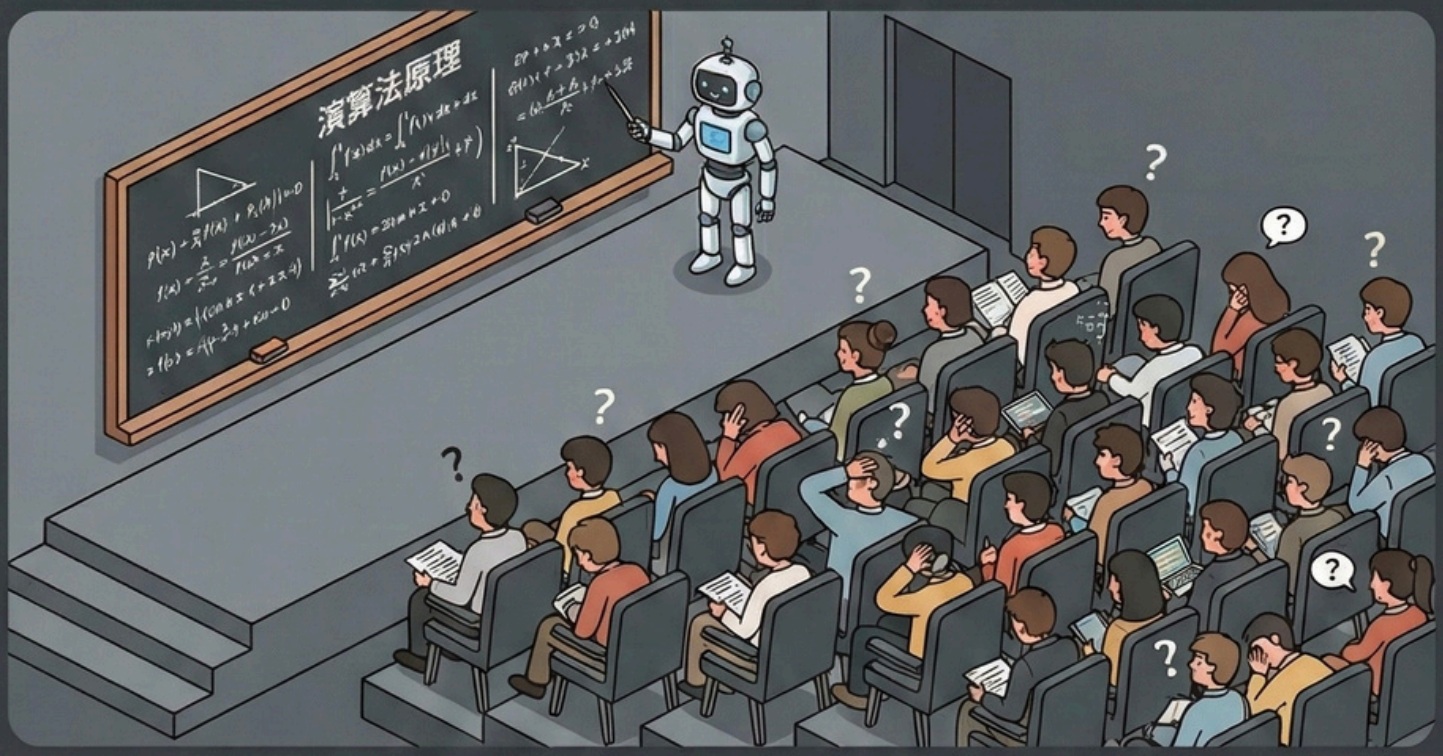


「遊戲規則」明確時，企業才敢大膽投資核心商業模式。

Chapter 6：人才戰略 - 從 Coding 到 Orchestration

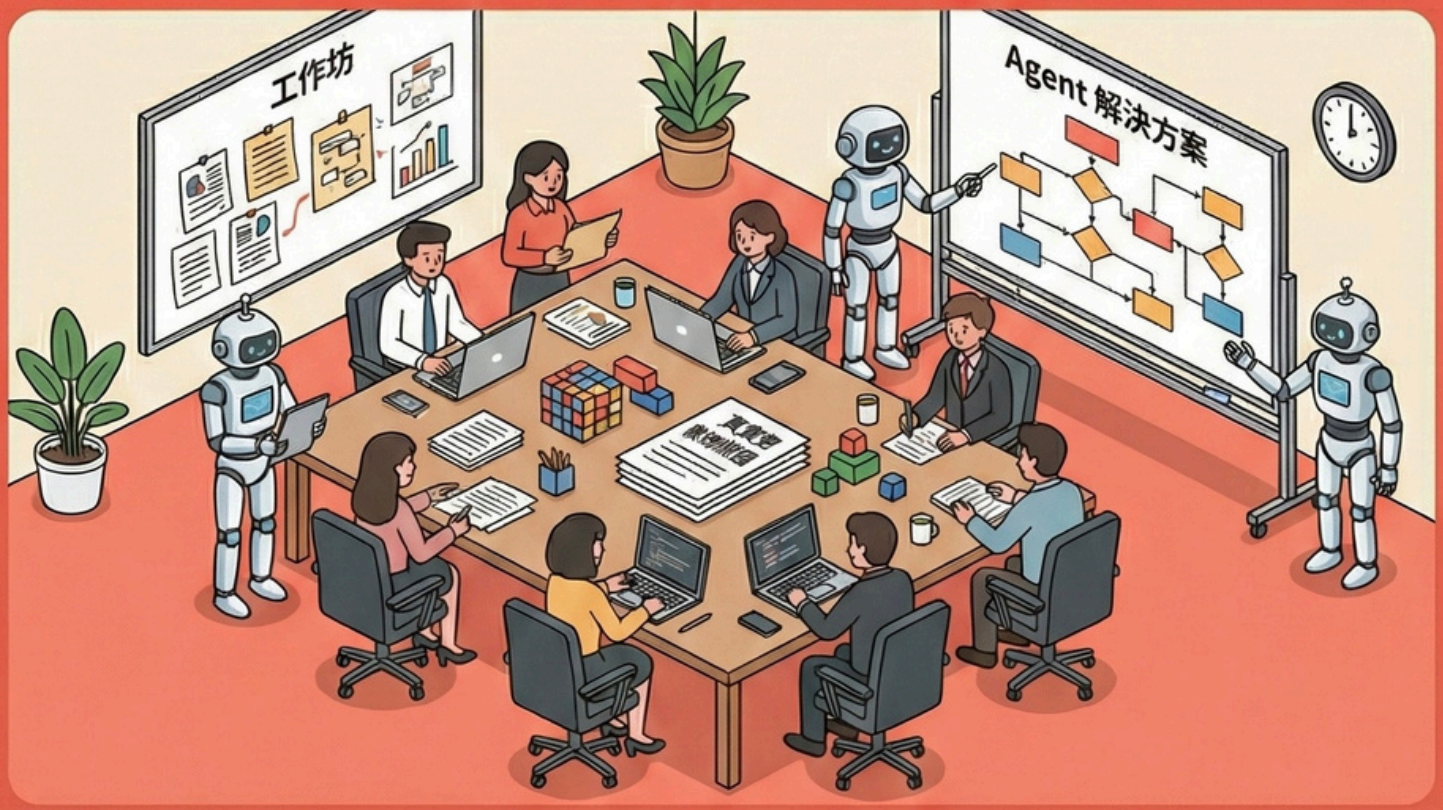
1. 培訓需求：從「理論科普」轉向「場景實戰」

舊模式：理論科普 (16.7%)



基礎 AI 概念普及：員工不知道明天上班該用 AI 做什麼。

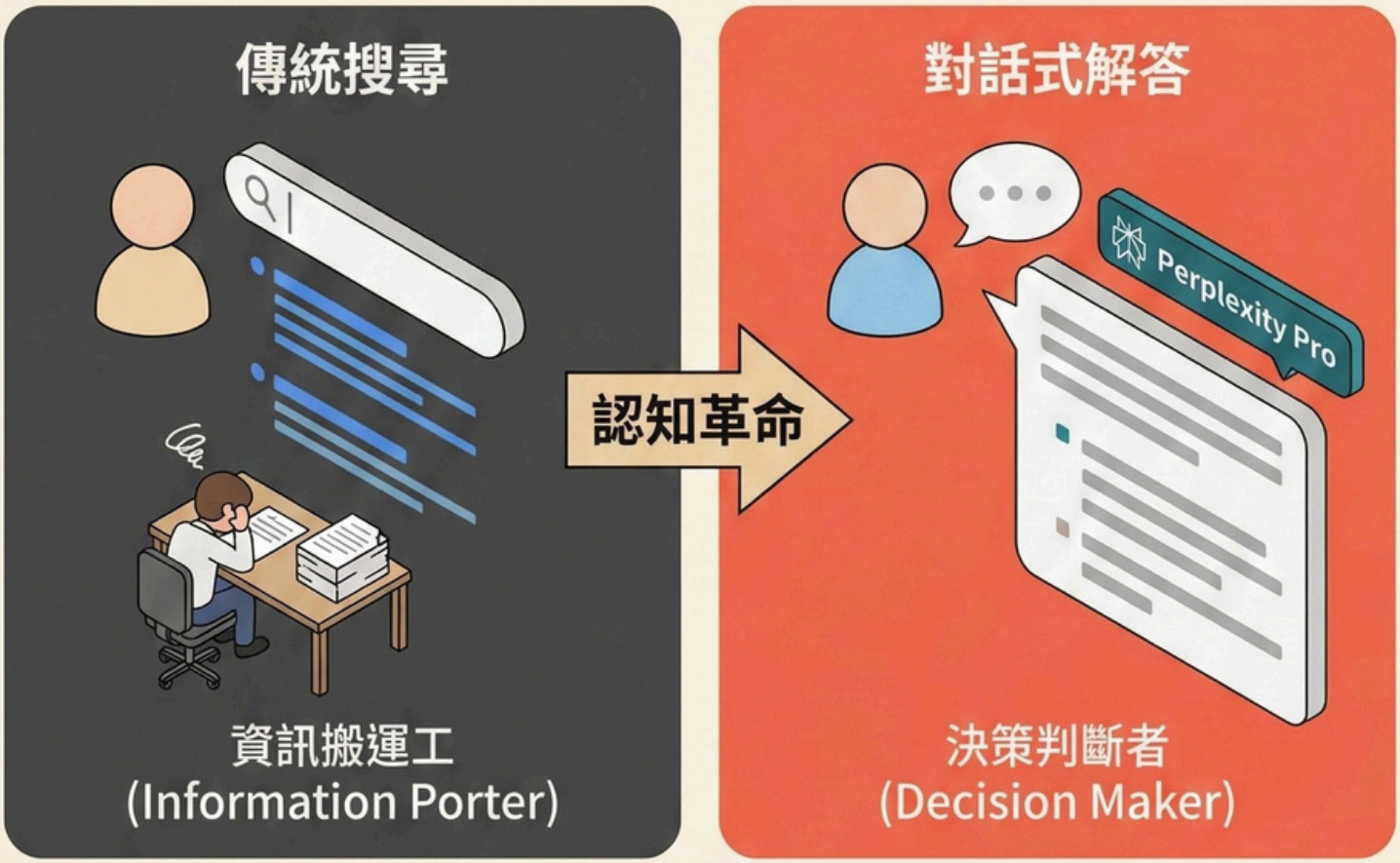
新模式：場景實戰 (20.9%)



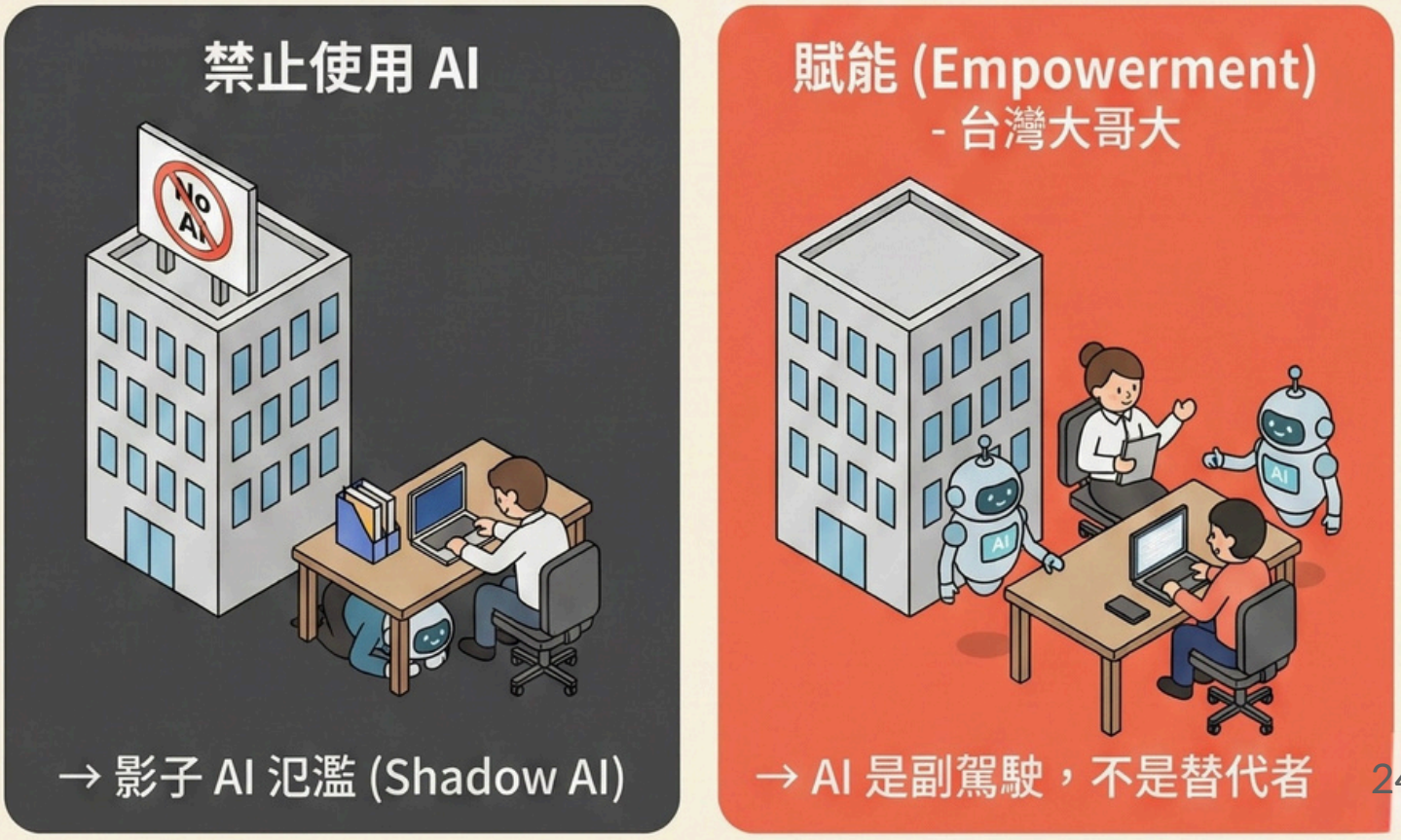
AI Agent 實務應用與案例分享：帶著問題進來，帶著解方出去。

2. 企業標竿：台灣大哥大用 Perplexity Pro 掀起「認知革命」

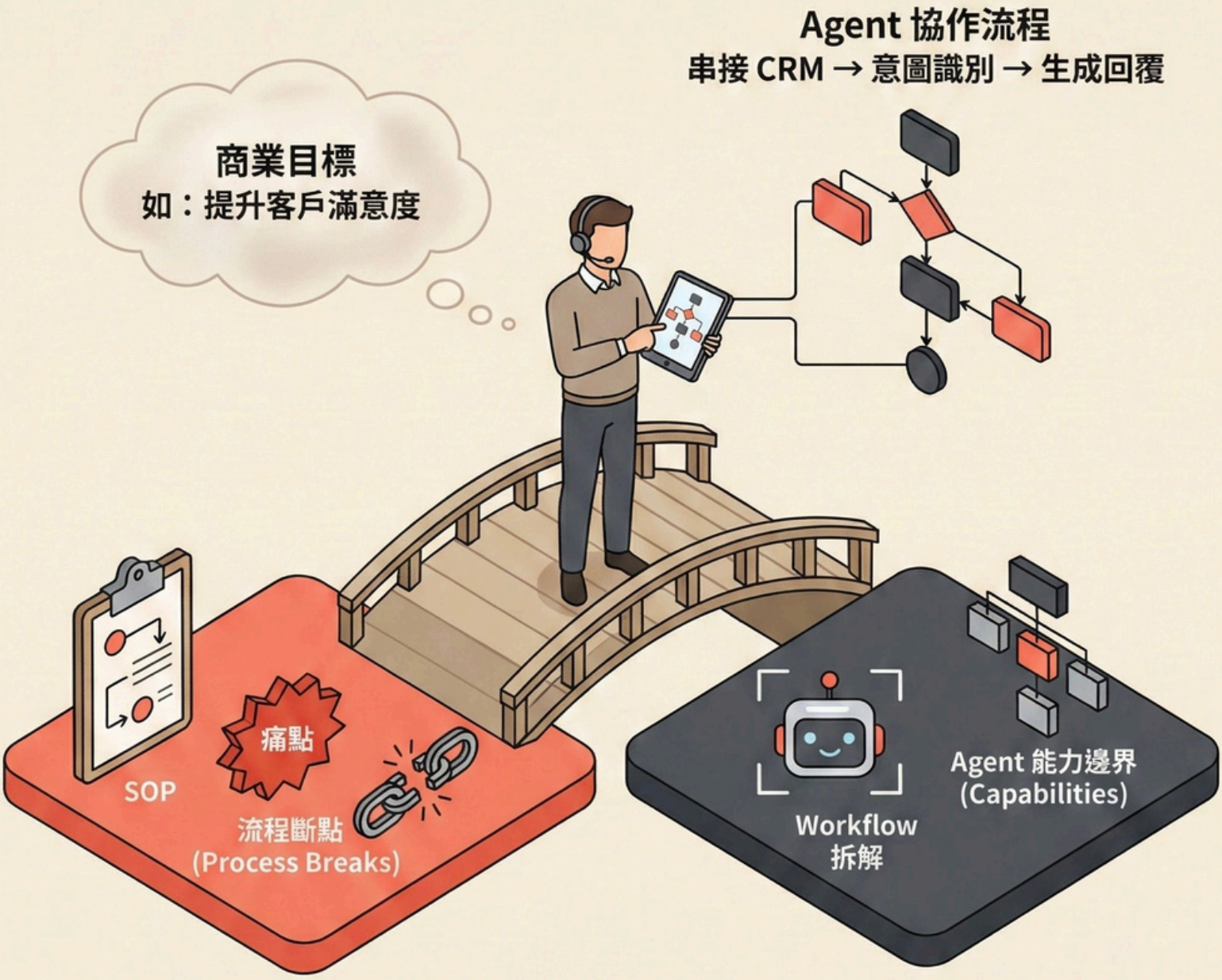
從「搜尋 (Search)」升級為「解答 (Answer)」



建立「人機協作」的心理契約 (Psychological Contract)



3. 新職位崛起：AI 流程架構師 (AI Orchestrator)



懂業務 (50%)
(Business Domain)

懂 AI (50%)
(AI Tech)

他們是連接「痛點」與「技術」的橋樑：
具備極強邏輯拆解能力，將模糊目標轉譯為精密 Agent 流程。

Special Chapter: SUPER 8 Studio

全通路變革 - AI Agent 戰術手冊

剖析真正落地的 AI Agent：
打破人力成本與業績增長的零和博弈

CASE 1：卡柏蒂 CUPETIT - 精品甜點的數位客服 (降本增效)

驚人成效：
半年省下
60%
營運成本

自動歸檔 CRM，
自動歸檔 精準行銷

CASE 2：美賣科技 meimaii - 3 人團隊扛下千人服務量 (效率革命)

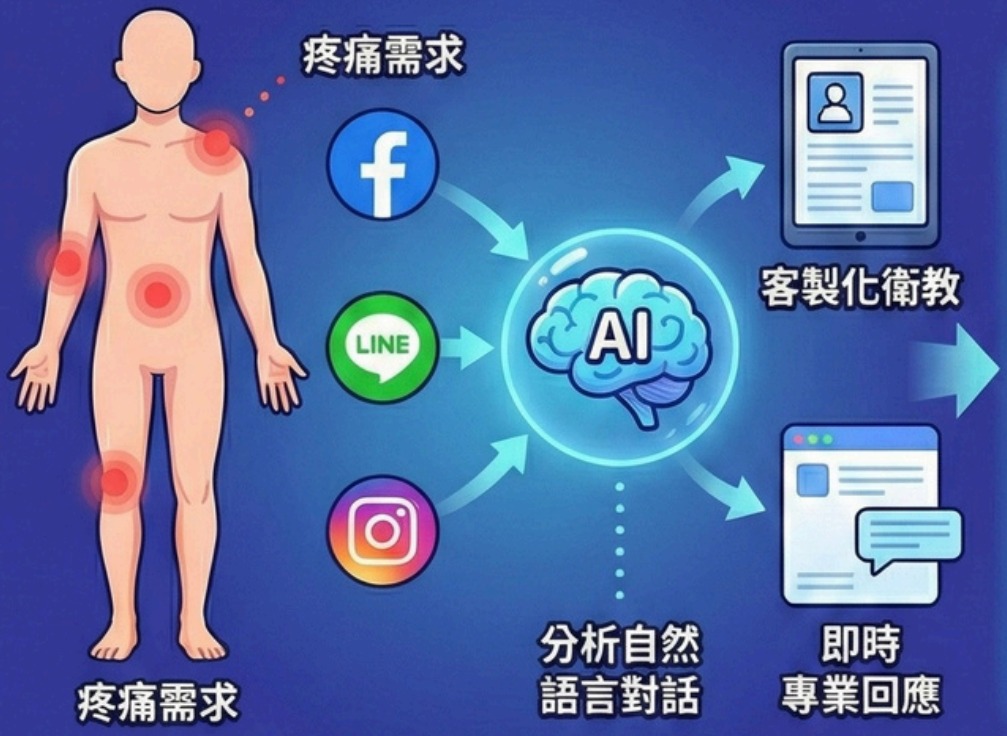
驚人成效：
僅 3 人編制
維持高品質
服務

行銷客服深度融合，
即時掌握脈絡

SUPER 8 Studio

實戰案例：體驗優化與規模化應對

CASE 3：生生優動 AICARE - 物理治療智慧分診 (體驗優化)



驚人成效：

高解決率

80%

客服問題解決率
大幅提升

100%

全通路覆蓋，
跨渠道整合

CASE 4：威訊 WaySim - 出國上網即時後援 (規模應對)

驚人成效：

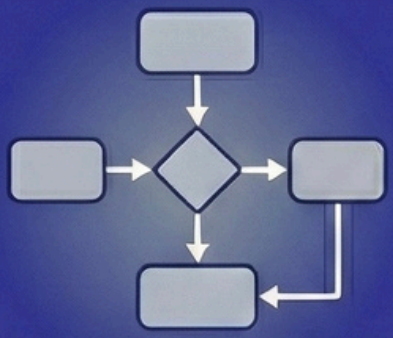
海量吞吐

4,000-5,000
筆/日
成功處理客戶查詢

降低 70% 人工
客服量，人機協作

展望 2026：SUPER 8 Studio 對話式商務三大典範轉移

趨勢一：從「行銷自動化」走向「AI 主動對話引導」



舊模式：事件觸發
(做了A才收到B)

新模式：即時挖掘需求，
越聊越精準的互動飛輪

趨勢二：多元 AI Agent 部署，跨境營運底層能力

私有雲 / 地端部署

一套 AI，多國在地化溝通

趨勢三：No-Code 下一步，「說話就能完成設定」

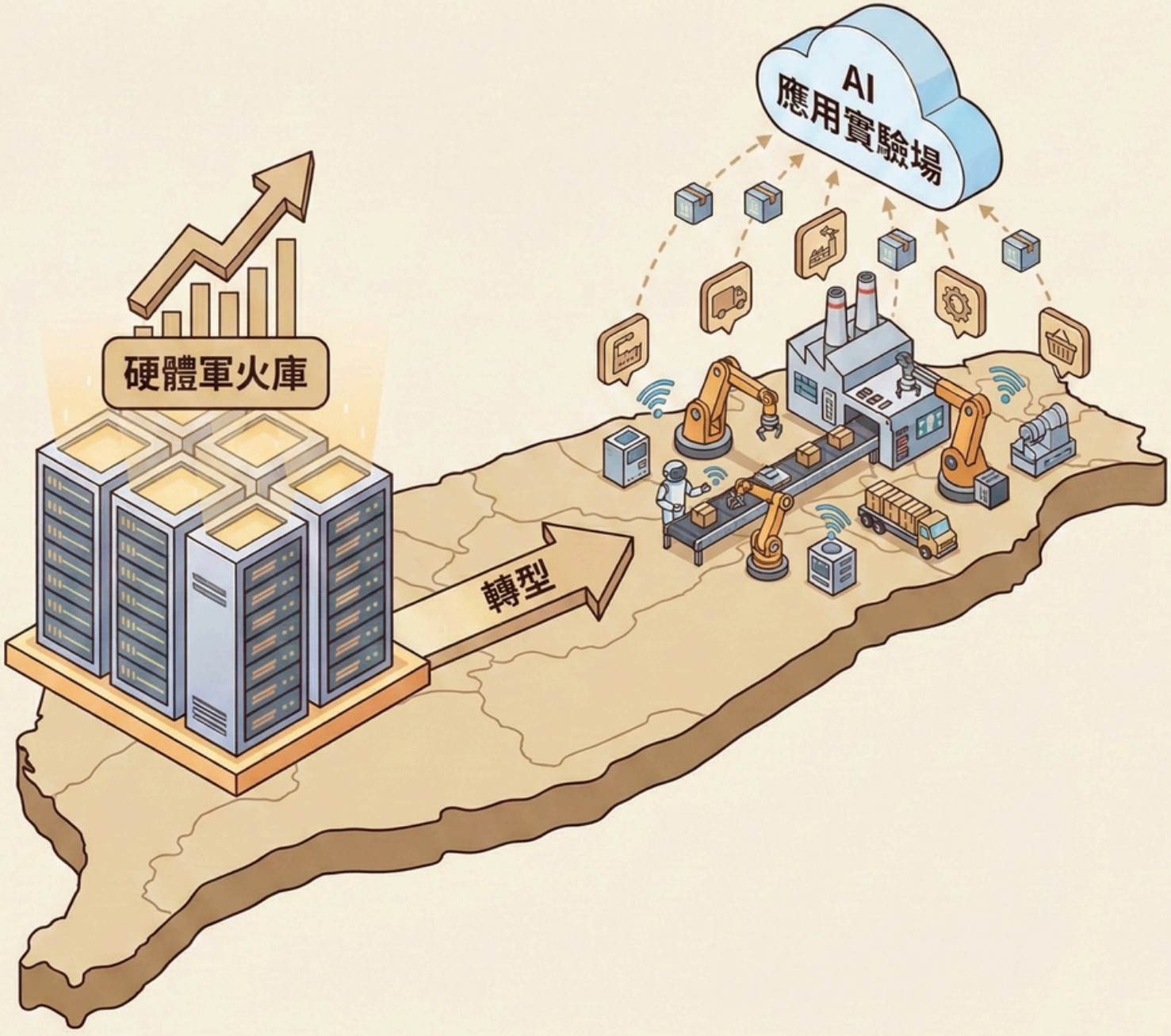
Super 8 Copilot：你的數位個人助理

總結：AI Agent 是企業生存標配！

數據證明：平均提升 80% 客服效率，同時提升 30% 轉換率↗

Chapter 7：預見 2026 – 從雲端落地
邊緣：AI Agent 經濟圈的台灣主場

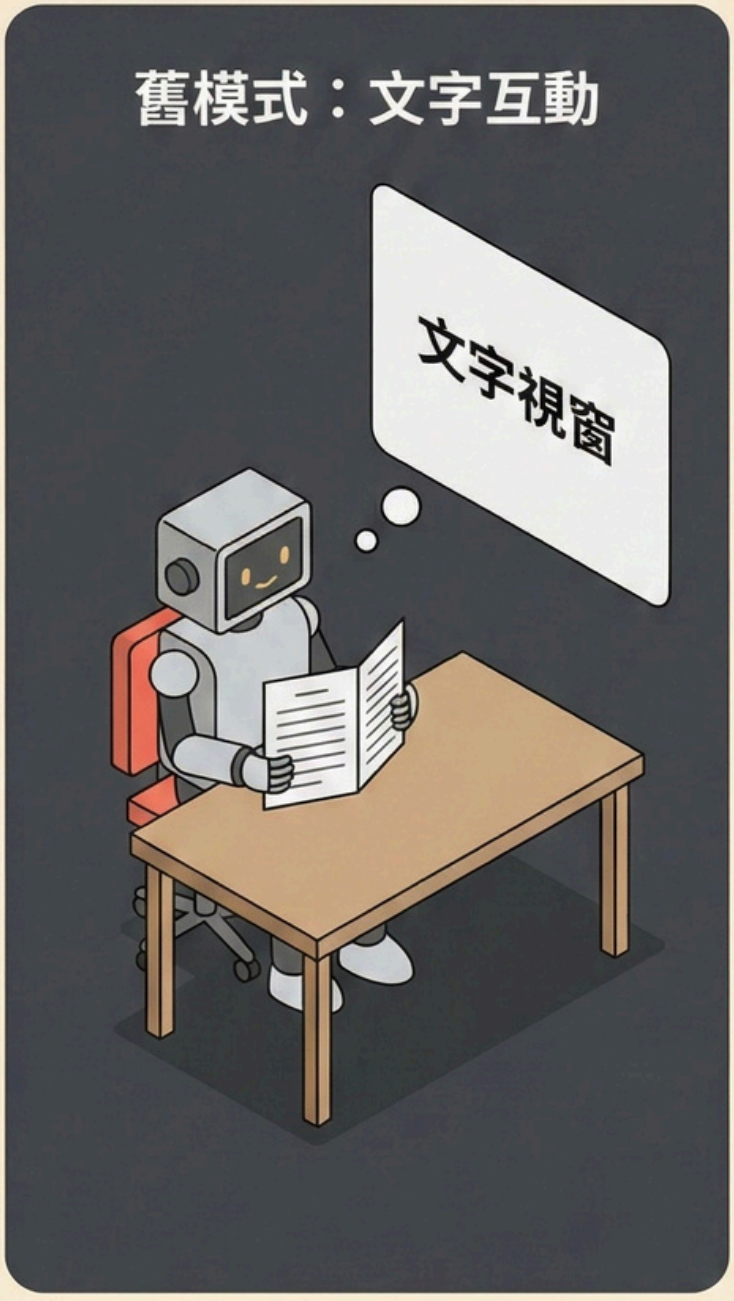
「如果 2025 是 Agent 的落地元年，2026 將是台灣利用『邊緣算力』與『垂直數據』，從 AI 硬體軍火庫轉型為為 AI 應用實驗場的關鍵時刻。」



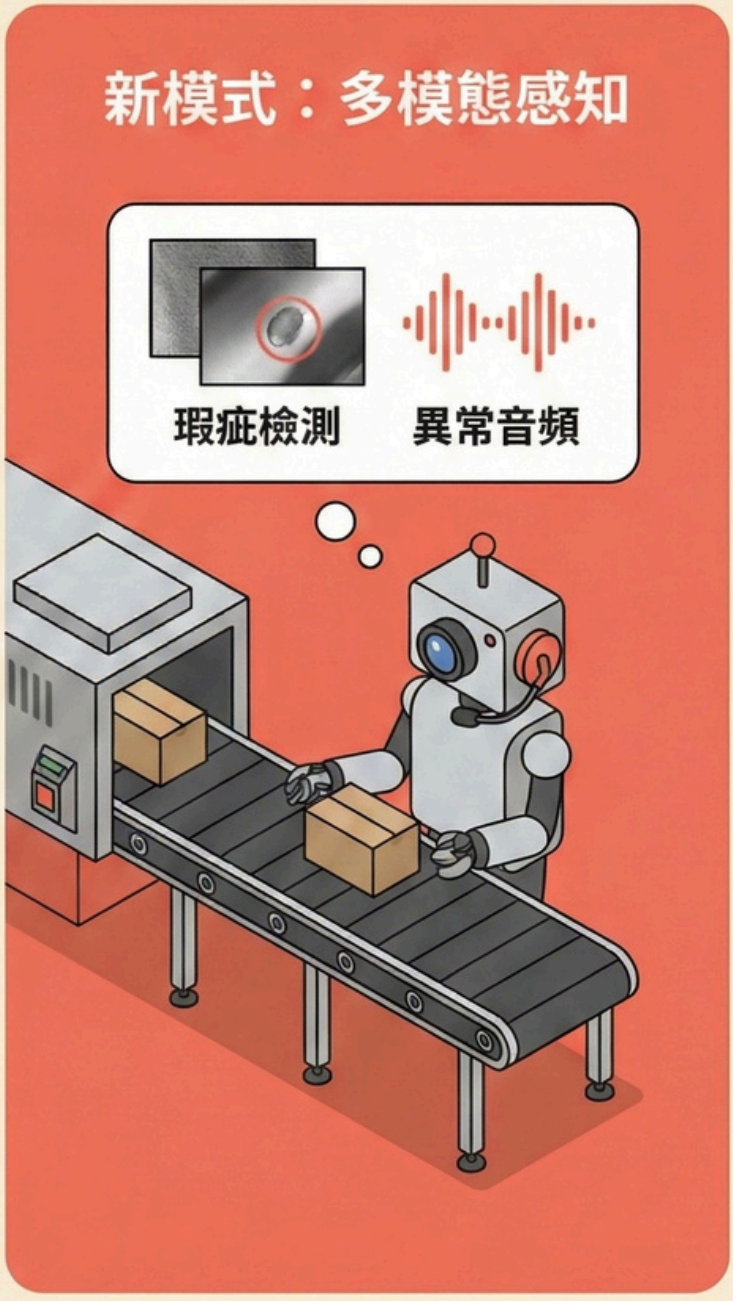
2025：落地元年 → **2026：邊緣落地 + 垂直數據**

1. 多模態標配化(Multimodal Standard)：從「讀懂文字」到「看見世界」

「視覺與聽覺將成為 Agent 的標配感官，這正是台灣製造業的主場。」



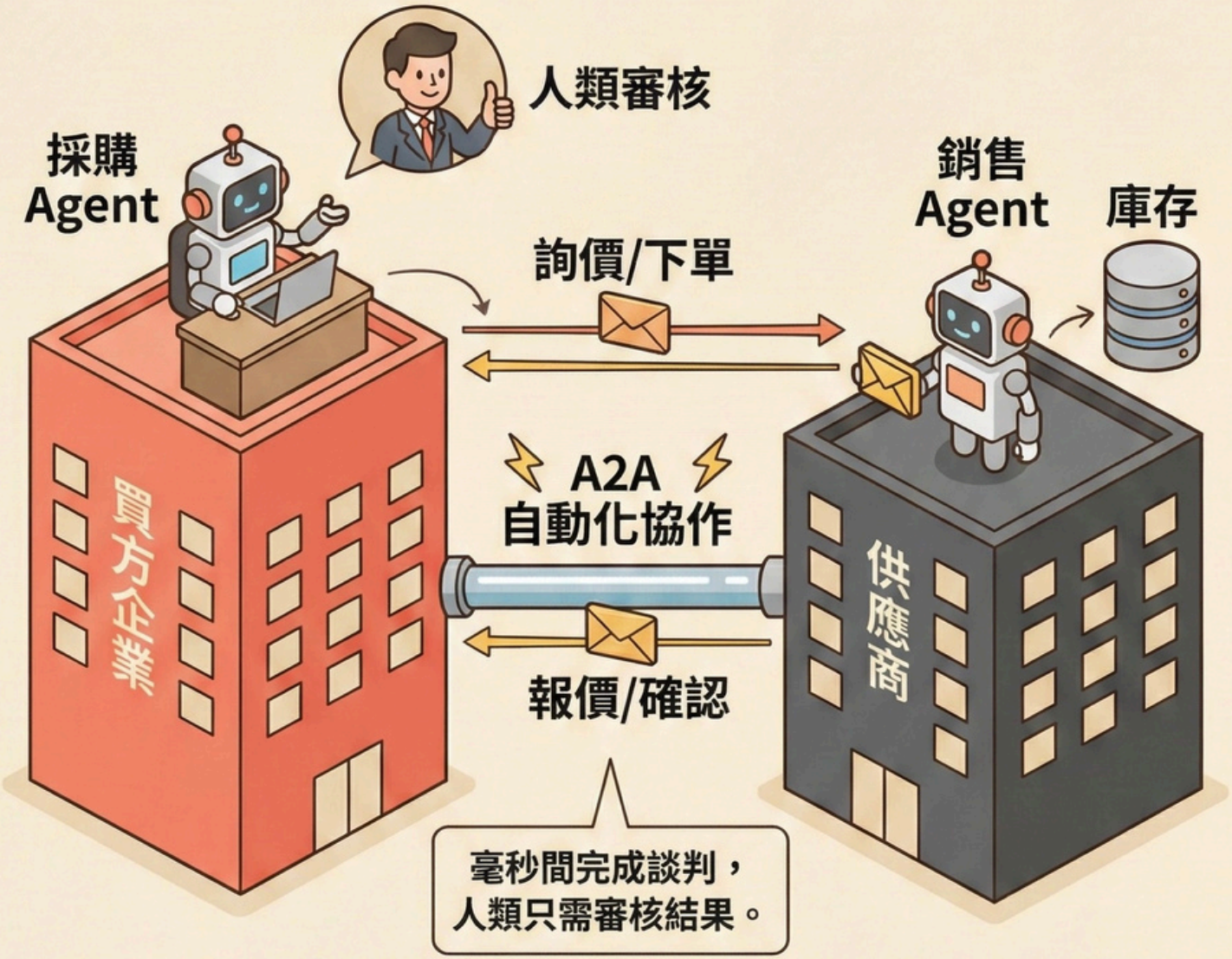
Agent 侷限於文字視窗，僅能處理結構化資訊。



Agent 具備視覺與聽覺，能能感知物理世界，指揮機械手臂實現「關燈工廠」。

2. Agent to Agent (A2A) 經濟圈：B2B 商業模式的重構

「未來的商業互動，將是『機器對機器』的談判。
台灣綿密的供應鏈聚落，是 A2A 經濟的最佳實驗室。」



未來航向：AEO
(Agent Engine Optimization)

優化商品資訊與 API，讓別人的 Agent
「優先讀取」與「選擇」你的服務。

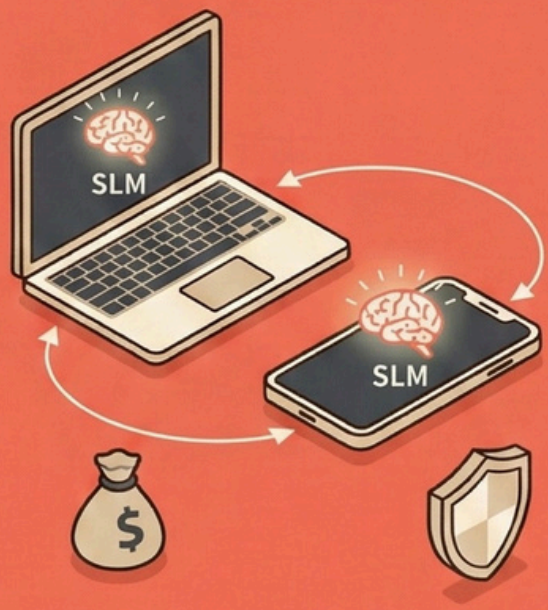
3. SLM 邊緣運算 (Small Language Models)：隱私與算力的完美平衡

「AI 將從雲端走入終端。這不只是技術選擇，
更是台灣『AI PC / 手機』硬體生態系的巨大紅利。」

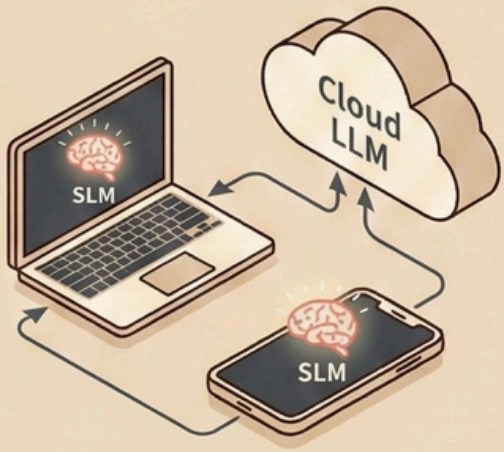
雲端巨型模型 (Cloud LLM)

高成本 (High Cost)，
隱私風險 (Privacy Risk)，
依賴網路。

邊緣專用小模型 (Edge SLM)



低成本 (Low Cost)，
絕對隱私 (Absolute Privacy)，
離線可用。



未來航向：混合式 AI (Hybrid AI) 架構

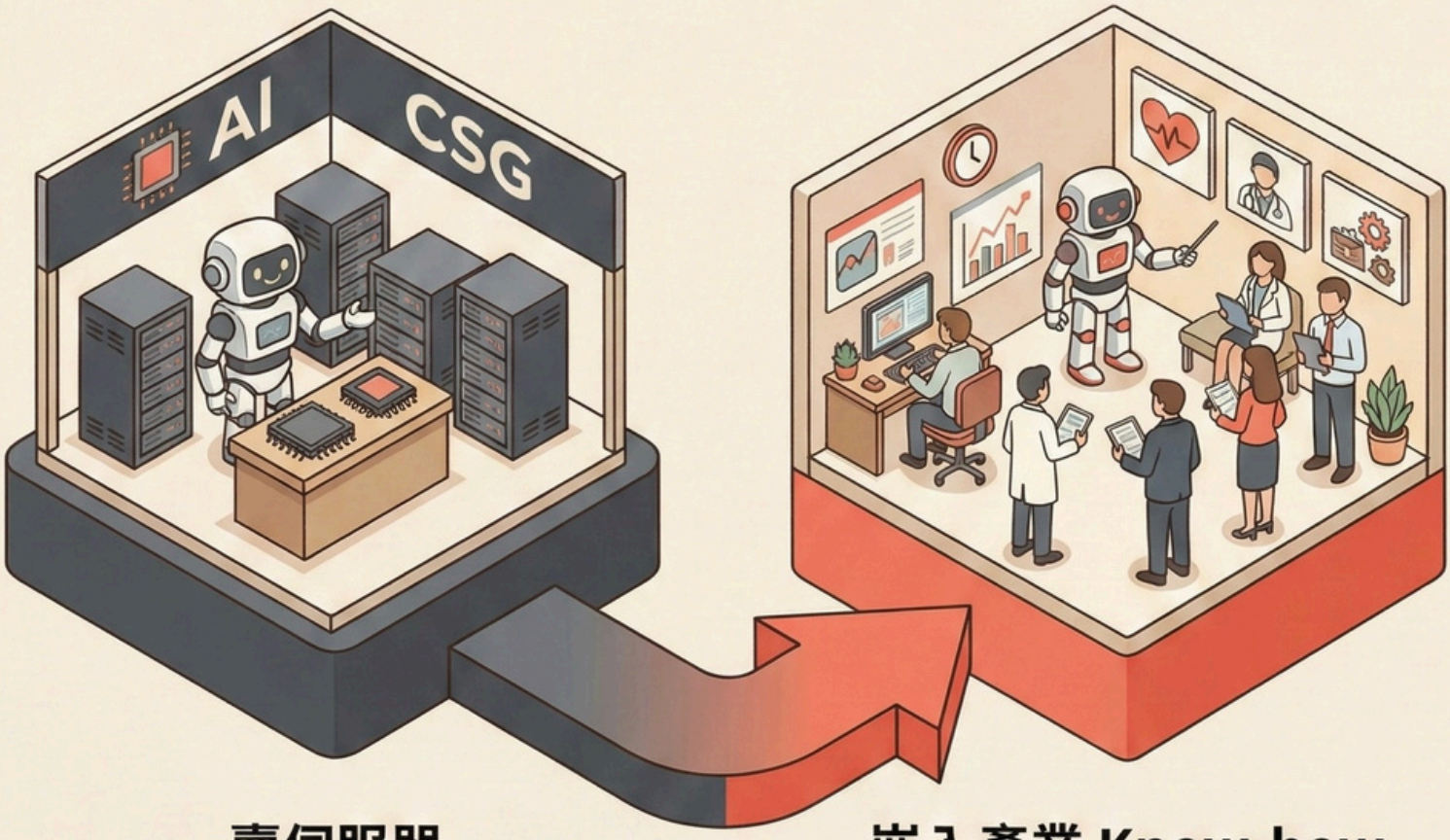
核心機密 Agent 部署本地端 SLM，
廣泛知識任務交給雲端 LLM。
兼顧成本、效能與安全。

💡 總結：台灣的戰略機會點

「我們不應只滿足於做 AI 時代的『軍火商』，
更要成為善用武器的『精銳部隊』。」

過去：AI 硬體軍火商

未來：AI 應用精銳部隊



賣伺服器

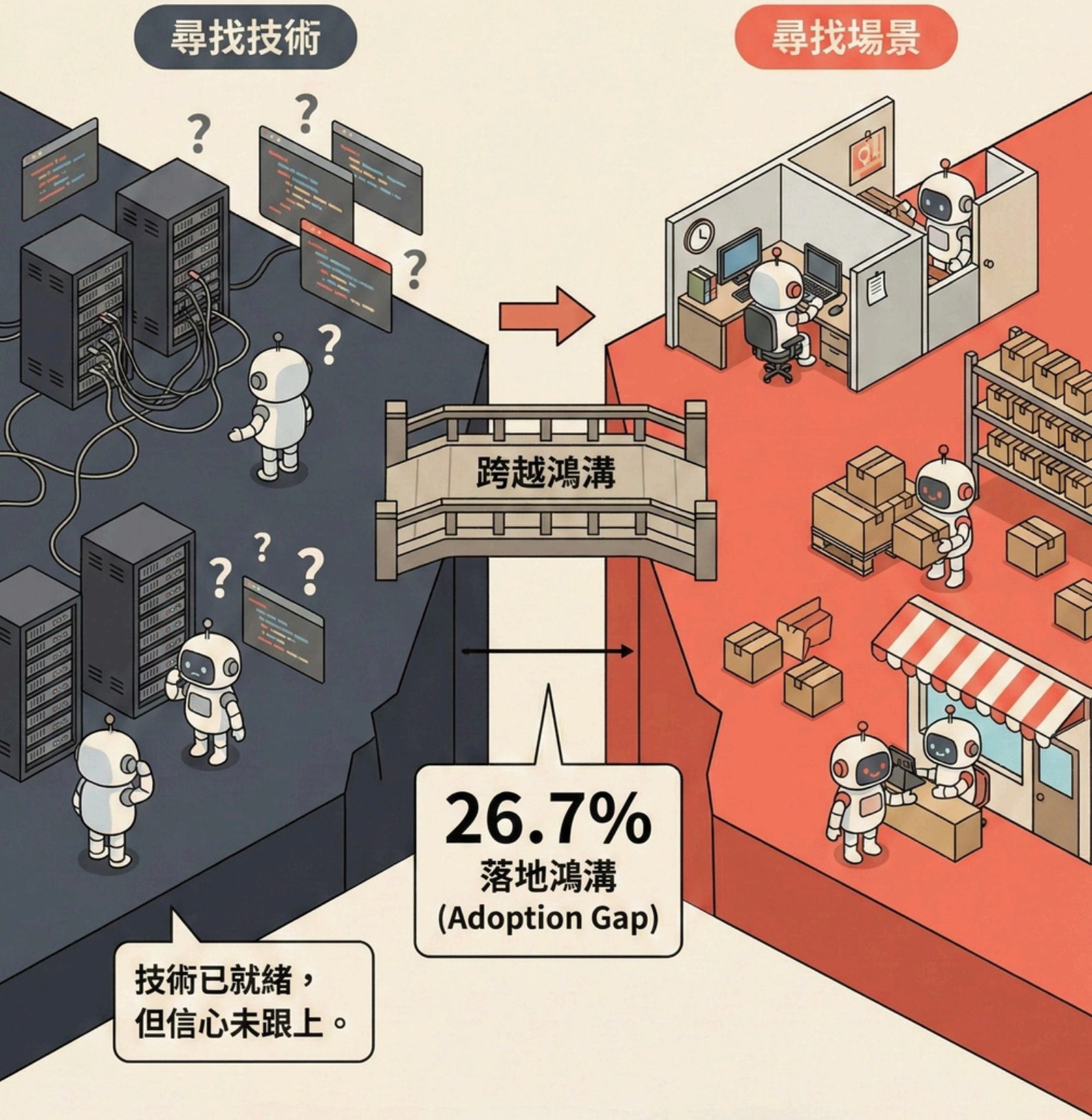
嵌入產業 Know-how

1. 利用硬體優勢（邊緣運算）
2. 結合垂直產業知識（多模態數據）
3. 在高密度供應鏈驗證（A2A 協作）

跨越 GenAI 鴻溝，航向自主化未來。

Conclusion：給企業主的行動指南

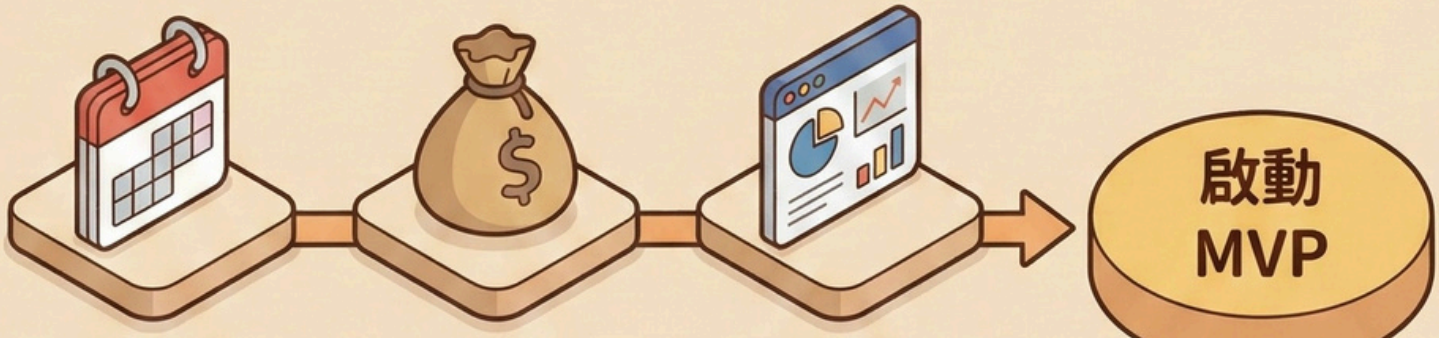
跨越鴻溝，從「尋找技術」轉向「尋找場景」



1. 致決策者 (To Decision Makers)：擁抱敏捷預算，容許小規模試錯

挑戰：
遲遲不敢簽核第一筆投資

行動指南：「333 敏捷法則」



3 個月
設定嚴格 POC 期限

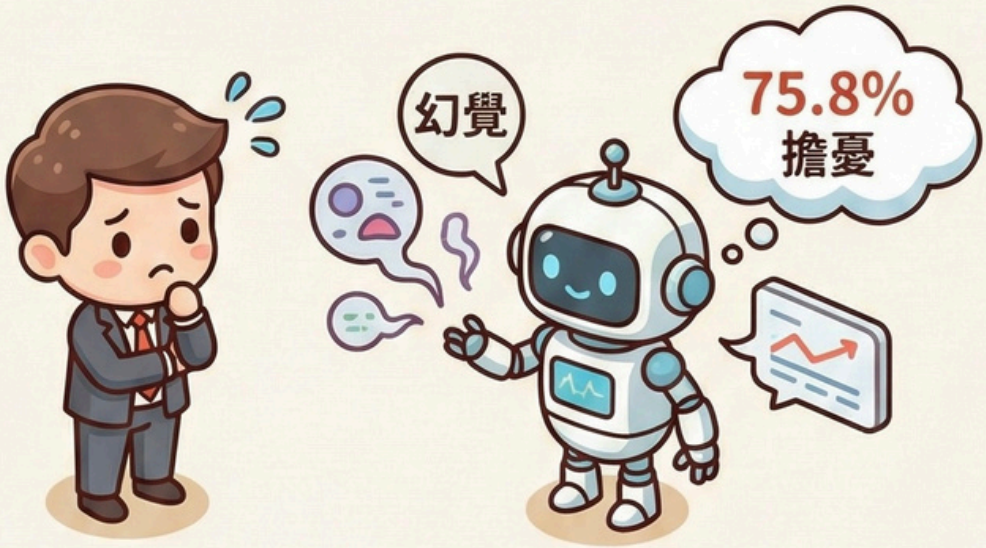
30 萬
部門級小額預算試點

3 指標
鎖定單一痛點 (如 IT 報修)

先求有，再求好
用真實數據打破僵局

2. 致管理者（To Managers）：數據治理是地基，SOP 是導航

挑戰：



挑戰：害怕 AI 產生幻覺，造成災難

行動指南：建立 RAG 架構與數據治理

盤點 SOP 與歷史數據，劃定安全知識邊界
數據治理是核心資產

3. 致執行者 (To Executors)：從「操作者」升級為「指揮官」

操作者

挑戰：擔心被取代，親手處理繁瑣雜事。

指揮官

行動指南：展現 AI 編排力，將 Agent 視為專屬實習生。

懂 AI 的人不會被取代
成為駕馭 AI 的流程架構師

PUBLISHED BY

INSIDE

RESEARCH PARTNER

SUPER 8 Studio

聯絡我們 Contact Us
Website: www.inside.com.tw
Email: contact@inside.com.tw

訂閱 INSIDE 網路趨勢觀察電子報

版權與免責聲明 Copyright & Disclaimer