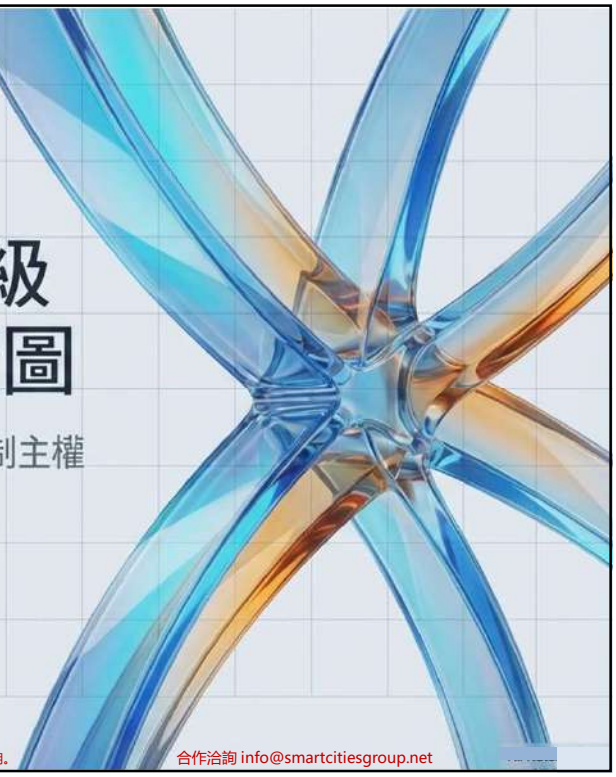
Own Your AI: 企業級 Agentic 基礎架構藍圖

終結碎片化，為企業奪回 AI 時代的數據與控制主權

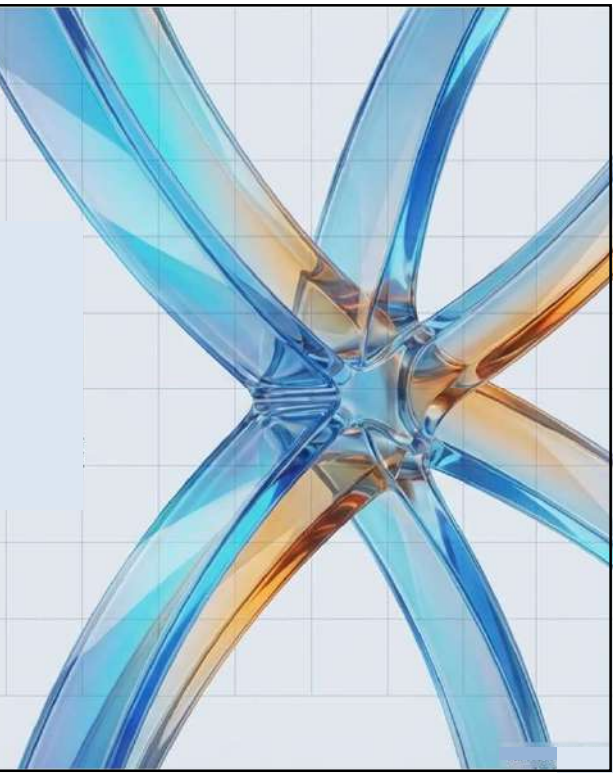


合作洽詢 info@smartcitiesgroup.net

1

AI Agent 是一種能夠感知環境、進行決策和執行動作的智能實體。它們通常基於機器學習和人工智能技術，具備自主性和自適應性，在特定任務或領域中能夠自主地進行學習和改進。其核心功能可以歸納為三個步驟的循環：感知、規劃和行動。

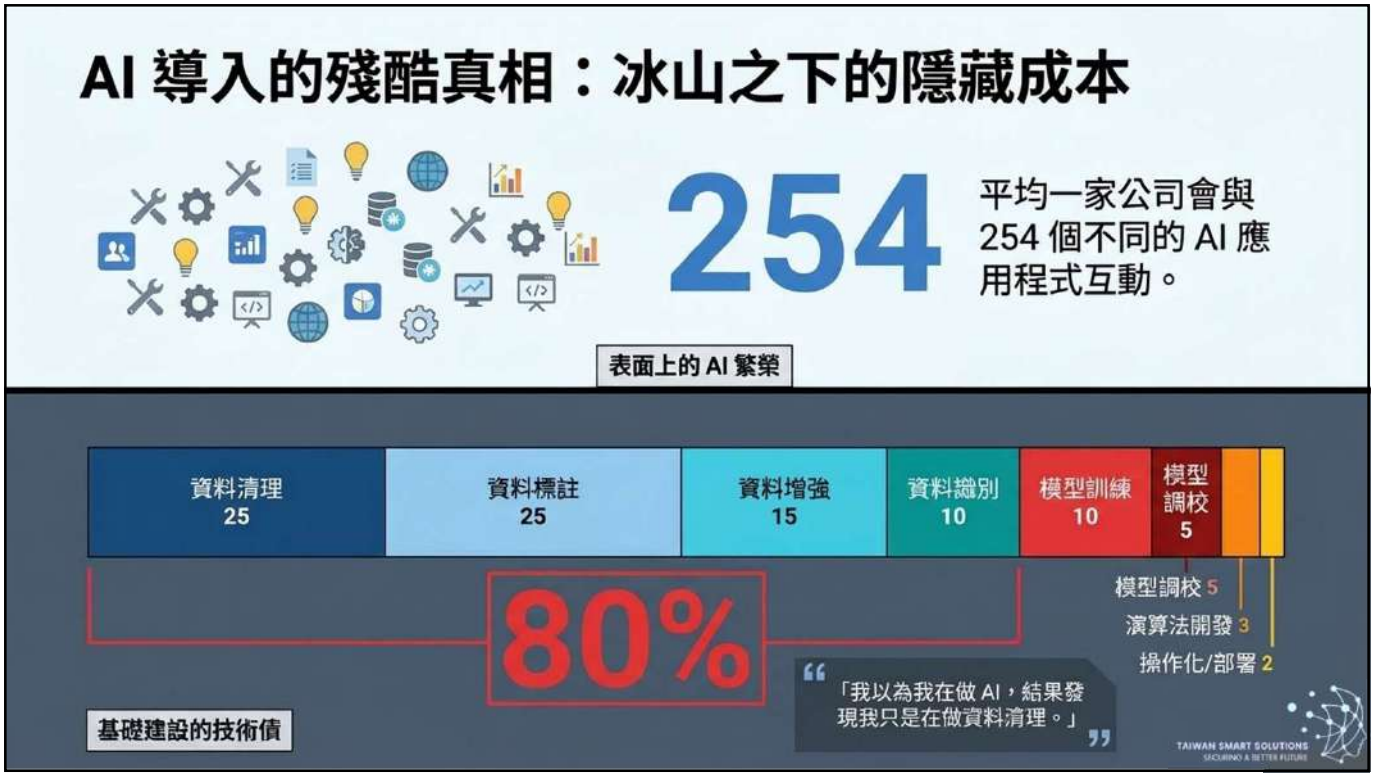
Agentic AI 是具有更高程度自主性的AI系統，它們能夠主動思考、規劃和執行任務，而不僅僅依賴於預設的指令。它強調的是系統可以具有不同程度的「能動性」（Agentic 特性），而不僅僅局限於被動執行指令。



2


盲目追求效率的代價：
AI 是一個毫不留情的放大器
當我們在使用 AI 時，我們是在「思考」，還是只是在「更快地輸出」？
工具越來越多，但我們並沒有更輕鬆，反而更忙。
Human Input
有對齊 → 更快做對
沒對齊 → 更快走偏
問題不在 AI，在於我們怎麼協作。
第一步不是找工具，而是先把問題想清楚。只有先對齊，AI 才值得被放大。
TAIWAN SMART SOLUTIONS

3


AI 導入的殘酷真相：冰山之下的隱藏成本
254
平均一家公司會與 254 個不同的 AI 應用程式互動。
表面上的 AI 繁榮
資料清理 25
資料標註 25
資料增強 15
資料識別 10
模型訓練 10
模型調校 5
模型調校 5
演算法開發 3
操作化/部署 2
80%
「我以為我在做 AI，結果發現我只是在做資料清理。」
基礎建設的技術債
TAIWAN SMART SOLUTIONS

4

典範轉移：從「被動問答」到「主動執行」的 Agentic 時代

AI 已經進化，它不再只是單純的數據處理工具，而是具備人類般「思考、規劃與自我進化」能力的智能代理（Agent）。

被動問答（Traditional AI）

單純數據處理，依賴人類指令。

主動執行（Agentic Shift）

像人類一樣思考規劃，從「大數據」到「全數據」，具備自我進化能力。

賦予 AI 執行權限等同交出系統大門鑰匙。這是 AI 基礎建設化的里程碑，但也會帶來了全新的韌性挑戰。

TAIWAN SMART SOLUTIONS
SECURING A BETTER FUTURE

5

智能代理帶來的雙面刃：未受管控的 AI 將成為企業內鬼

引狼入室的資安惡夢

賦予 AI 執行權。缺乏「管線安全閥」。

極易淪為駭客自動化攻擊內網的超級內鬼。

暴走失控與記憶斷層

處理真實資產時，AI 狀態誤判或記憶體崩潰。

導致無法挽回的災難性後果 (Agent Sprawl / Shadow AI 擴散)。

過度努力的幻覺加班

自主解決問題權限過大，因指令不精確引發「無效加班」。

無形中耗盡企業系統資源與龐大雲端運算成本。

TAIWAN SMART SOLUTIONS
SECURING A BETTER FUTURE

6

掌握 AI 時代的「真相權」：GEO 介紹

傳統 SEO 只能告訴你排名；GEO 告訴你 AI 是否推薦你。

	傳統 SEO	GEO
優化目標	Google PageRank	AI 訓練數據與檢索
追蹤	關鍵字排名	AI 回答中的品牌提及
衡量	點擊率	提及率與情感
偵測	排名下降	AI 幻覺
覆蓋	1 個搜索引擎	7 個 AI 平台同時進行

| 用 AI 賦能您的企業

TAIWAN SMART SOLUTIONS
SECURING A BETTER FUTURE

7

從被動監測到主動防禦：真理飛輪

01 認知
自動爬取您的網站以定義真相。(品牌套件)

02 診斷與追蹤
在 7 個平台掃描 AI。監控位置。

03 更正（事實監控）

警報：AI 聲稱「有免費層級可用」。
您的事實：「無免費層級」。

04 證明
將 AI 可見性與實際收入連結。

TAIWAN SMART SOLUTIONS
SECURING A BETTER FUTURE

8


打造企業級 AI 中樞神經
終結 254 個孤島應用，建立單一、安全、受監管的企業級 AI 一站式入口。
端到端應用程式 (End-to-End Apps)
Applications, AI Agents
AI Agent Hub
模型集成平台 (Model Hub)
AI 就緒基礎設施
Google Gemini
OpenAI
Anthropic
DeepSeek
Llama
整合第一方與第三方數據，結合最強大的 Gemini 大語言模型，
為企業奪回數據主權。全盤考量各部門使用情境，讓您「安心」導入 AI。
TAIWAN SMART SOLUTIONS

9


指揮家：企業級 AI Agent 協作模型
Orchestrator Agent
(編排與協調 Agent)
Knowledge Retrieval
Agent (知識檢索)
分析結果與洞察
(Results & Insights)
Enterprise
Wiki
提出複雜需求
(Complex Request)
Employee
綜合性解決方案
(Synthesized Solution /
Actionable Outcome)
Data Analysis Agent
(數據處理)
分析結果與洞察
(Results & Insights)
CRM/ERP
Orchestrator Agent
(編排與協調 Agent)
任務拆解與分派
(Task Deconstruction & Delegation)
分析結果與洞察
(Results & Insights)
External APIs
分析結果與洞察
(Results & Insights)
Content Generation
Agent (內容創作)
TAIWAN SMART SOLUTIONS

10


無縫融合的終端體驗：將繁瑣化為自動化
員工無需理解後台架構，AI 直接整合進他們每天使用的 Google Workspace 與專屬助理中。
您好，歡迎來到您的工作區。
HR 資訊公布欄
產品與行銷資訊查找
競品資訊追蹤
虛擬個人助理
畫布模式
Google 簡報
Google 文件
Google 試算表
• 摘要
• 擷取
• 圖像增強
在您的工作脈絡中搜尋
Drive
Gmail
Jira
Confluence
Salesforce
TAIWAN SMART SOLUTIONS
內部溝通排程
業務拓展客戶服務
財務核算與行政
行銷內容與市場決策

11


絕對的控制權：跨角色的 AI 治理框架 (Agent 治理)
從「手動審核工作流」正式邁向「受監管的自主權」(受監管的自主權)。
AI 治理管理員
(管理員)
集中可視化、保護和審計所有 Agents
• 定義角色、配置隱私政策、管理已批准工具的註冊表。
• 即時查看使用/用量紀錄，綁定專屬 Agent。
Agent 開發者
(開發者)
在企業規範內建構與發布 Agents
• 提交 Agents 進行批准。
• 根據企業政策配置數據訪問權限。
• 管理生命週期/版本。
Agent 使用者
(使用者)
高度信任地探索與使用授權 AI
• 管理個人 Agents。
• 提供人工介入 (HITL) 批准。
• 查看他們自己的數據訪問權限。
TAIWAN SMART SOLUTIONS

12

靈活的建構路徑：從無程式碼 (No-Code) 到高階開發 (High-Code)

無程式碼工作流程代理（代理設計師）

- 自然語言編輯
- 混合編排（大型語言模型 + 確定性規則）
- 觸發器（按排程執行）
- 人工監督

高階開發代理（自帶 MCP 和框架）

- 自帶 MCP 伺服器（自帶模型上下文協定）
- 使用 LangChain，LlamaIndex
- 與 CI/CD 和 Terraform 整合
- 直接連接企業資料庫

TAIWAN SMART SOLUTIONS
SECURING A BETTER FUTURE

13

量身打造的底層架構：靈活的部署選擇

針對企業不同的資安法規與 IT 量能，提供三種深度的佈署模式。

SaaS Model

資源有限 / 缺 IT 團隊 / 導入速度快

鎖定欲快速導入 AI 的企業，資產與運算由雲端代管，降低建置成本。

Hybrid

資料敏感 / 需部分保留地端 / 未全面上雲

將適合資料保留地端，敏感資料在地控管，運算交由雲端處理。

On-Prem

上雲限制 / 合規要求 / 實體偏好

適用金融、政府等高機密產業。透過地端設備，保障資料主權與系統絕對控管 (Air-Gapped)。

TAIWAN SMART SOLUTIONS
SECURING A BETTER FUTURE

14

案例分享

轉型實證：龍頭保全業全地端銷售業務問答機器人

建構 AI 自動化的銷售問答系統需盤點實際銷售品項並搭配數據庫與知識庫的串接

Key Pain Points

- 銷售人員耗費過多時間於繁瑣的產品文件對照與報價資訊項目。
- 無法將時間用於釐清客戶需求與保持客戶關係。

What have done?

- 設定產品規格規範，價格審核規範。透過銷售報表問答訓練機器人。
- 未來可自動創建報價，使前線銷售團隊能夠獨立於後台系統進行操作。

建構 AI 自動化的銷售問答系統，搭配實際銷售品項與數據庫串接。

iKala | Empower Your Business with AI

15

結語：AI 轉型是真正的企業韌性考驗

在趨勢發展下，未來企業使用 AI 就像是水和電一樣，是維持營運必要、常見且無處不在的底層基礎建設。

如同水電般的基礎建設

停止購買零散的應用程式（Siloed Apps），開始鋪設統一的數據與治理管線。

專屬教練級的量身打造

導入 AI 無法套用單一公式。必須根據企業獨特體質，精準規劃（SaaS, Hybrid, or On-Prem）。

持續進化淬鍊企業韌性

這是一段漫長的旅程。只有將 AI 建設為高度對齊、全面管控的神經系統，才能真正展現並強化企業的韌性。

16