

AI Agent 未來企業的現在進行式？

文／廖肇弘

「AI 是否會取代人類？」這個爭論許久的問題，基本上有兩種思路：第一是「體力」上的取代，我們順著「人形機器人（Humanoid Robotics）」的發展脈絡可以繼續探索下去；第二則是「腦力」上的取代，這就是近期非常熱門的「AI Agent」的議題了。

這一年來，生成式 AI 在 LLM 各家大型語言模型的競爭與推波助瀾下，智力幾乎是以光速前進。不論是 Gartner、BCG、Accenture、IBM、Deloitte...幾乎所有研究機構的研究報告還有許許多多的專家學者們都說：2025 是 AI Agent 代理或自主 AI（Agentic AI，中國大陸稱為「智能體」）的落地年！

值此 2025 年初，我們就來看看 AI Agent 對於企業未來的運轉模式將產生何種衝擊與影響？企業又應該如何掌握 Agentic AI 帶來的新機會？

AI Agent 重量級報告的關鍵數據

讓我們先看一些重量級報告的關鍵數據。

Gartner 不僅在 2025 十大新興科技趨勢報告中將 Agentic AI 擺在首位，而且直接預測到 2029 年，Agentic AI 將在無需人工干預的情況下，自主解決 80% 常見客戶服務問題，從而將營運成本降低 30%。

此外，根據 McKinsey 《Superagency in the Workplace》報告，AI 在企業應用上的長期潛力高達 4.4 兆美元的生產力增長，但目前只有 1% 的企業真正邁入 AI 成熟階段，能夠有效地將 AI 深度整合到核心工作流程中，並持續創造可觀的業務價值。

與此同時，92% 的企業計劃在未來三年內大幅增加 AI 投資，但矛盾的是，47% 的 CXO 高層卻坦言，他們的企業在 AI 發展的步伐上仍然顯得遲緩，未能充分釋放 AI 的潛力。

研究發現，擴展 AI 的最大障礙不是員工（他們已準備就緒），而是領導者，他們行動不夠迅速。其實員工比領導者想像的更願意接受 AI，他們更熟悉 AI 工具，想要獲得更多支援和培訓，並且更可能相信 AI 在不久的將來會取代至少三分之一的工作。

企業領導者顯然低估了員工使用生成式 AI 的廣泛程度。CXO 們估計只有 4% 的員工將生成式 AI 用於至少 30% 的日常工作，而調查顯示，員工自述的比例實際上是這個數字的三倍。

儘管如此，高達 87% 的企業高層預計未來三年內生成式 AI 將帶來營收增長，約一半的人表示在此期間營收增長可能超過 5%。

AI Agent 浪潮下的企業應用場景

那麼，AI Agent 在企業中有哪些應用場景與案例呢？

1. 智能客服與客戶關係管理（CRM）：效率與情感的平衡

客服領域的應用，如亞馬遜的 Amazon Connect AI，透過語意分析顯著提升了客戶滿意度 40%。然而，當 AI 取代了部分人工客服的角色，如何保持品牌的情感連結與個性化體驗，成為企業必須思考的問題。過度依賴 AI 可能導致客戶體驗的同質化，削弱品牌獨特性。

2. 供應鏈與物流管理：數據依賴與風險應對

DHL 等企業利用 AI 預測貨運需求，有效降低了運輸成本 25%。然而，AI 的預測模型往往基於

歷史數據，這可能使其在面對突發事件（如疫情、戰爭）時失去準確性。企業需要建立更具彈性的 AI 系統，能夠應對不可預測的市場變化。

3. 財務與風險管理：演算法偏差與決策透明度

摩根大通等金融機構採用 AI 監測金融詐欺，提高了檢測準確率 85%。然而，AI 風險模型的演算法偏差可能導致財務錯誤，甚至產生歧視性結果。企業在利用 AI 進行財務決策時，必須確保演算法的公平性和透明度。

4. 產品創新與市場行銷：創意與品牌形象的契合

Adobe Sensei AI 等工具優化了廣告投放 ROI，提升了轉換率 30%。然而，AI 生成內容如何確保符合品牌形象，避免「AI 同質化」，成為企業面臨的挑戰。企業需要建立完善的內容審核機制，確保 AI 生成的內容與品牌價值觀一致。

5. 人力資源管理（HRM）：效率與公平性的權衡

LinkedIn 等平台利用 AI 提升人才匹配度 60%，提高了招聘效率。然而，AI 在人力規劃過程中可能產生無意識的歧視偏差，導致不公平的招聘結果。企業在利用 AI 進行人才管理時，必須確保演算法的公平性和包容性。

總而言之，AI Agent 將為企業帶來巨大的發展機遇，但也伴隨著一系列挑戰。企業在擁抱 AI 的同時，必須深入思考其潛在風險，建立完善的管理機制，才能充分發揮 AI 的價值，實現可持續發展。

AI Agent 是企業的「超級助理」還是「黑箱風險」？

AI Agent 的核心魅力在於其高度的「自主決策」與強大的「執行力」。AI 不再是被動地執行指令的工具，而是在預設的規則、目標和價值觀框架

下，自主地感知環境、分析問題、制定策略並高效執行複雜任務的智能體。

然而，這種「自主性」，如同硬幣的另一面，也為企業帶來了前所未有的挑戰 — 當 AI 深度參與甚至主導決策過程時，企業是否還能清晰地理解、有效地監督和最終掌控決策結果？由此，我們必須正視下列關於 AI Agent 的核心能力與風險：

1. 自主決策與執行：

AI 可以加速決策，但如果其決策過程缺乏透明度，企業如何確保結果符合業務目標？

2. 跨平台整合：

AI 可以無縫串聯企業內部系統，但當 AI 的推薦與人類決策產生衝突時，誰該負責？

3. 學習與適應：

AI 透過機器學習技術不斷優化決策能力，但如果數據偏差或模型訓練不完整，是否會導致系統性風險？

此外，企業也應注意「AI 過度自動化風險」。當 AI 開始主導業務流程時，若企業缺乏適當的人工監管與糾錯機制，將可能導致系統性風險。例如，在供應鏈管理中，若 AI 過度依賴歷史數據，可能無法應對突發的市場變動（如疫情、地緣政治衝突）。

結語

我們只要稍微想像一下就可以發現，未來的企業很可能都是依賴幾個重要的 AI Agent 全天候 24 小時運轉。不可諱言地，這其中存在著無比巨大的機會與風險。

企業導入 AI Agent 的關鍵策略，必須先從 PoC 試點開始，逐步擴展 — 確保 AI 的決策結果可驗證，並在小範圍測試後才擴大應用。此外也必須建

立數據基礎設施與監管機制 — 確保 AI 的數據來源透明，決策不受偏差影響。再來也必須強化 AI 人才與企業文化 — AI 並非只屬於 IT 部門，而是所有員工都需要理解的新工具。

真正值得企業深思的，是如何積極擁抱並駕馭 AI 浪潮，將其轉化為提升競爭力的核心動能。在即將不久的未來，AI Agent 將會以前所未有的速度滲透企業的各個角落，企業領導者更需要從戰略高度審視這場變革，並且預先面對這些 AI Agent 時代的靈魂拷問：

- AI Agent 如何從根本上重塑企業的決策機制？決策權的邊界將如何劃分？
- 高度自主的 AI 是否會演變成難以預測和控制的「黑箱」，導致企業失去對核心業務的掌控？
- 在人機協同的新時代，企業應如何設計更具韌性、更富效率、更人性化的新型組織架構，以適應員工與 AI Agent 共存的新常態？
- 如何有效應對 AI 系統可能帶來的倫理風險、安全風險、營運風險和法律合規風險，確保 AI 的發展與企業的可持續發展目標相一致？

AI 會不會取代人類？這一題我還沒有答案。不過，我可以非常確定的預測 — 未來沒有部署 AI Agent 的企業，很快就會被積極導入 AI Agent 的企業取代！與諸君共勉之。



作者廖肇弘博士，現為工研院產業學院數位訓練長。曾任國內外多所大學 EMBA 教授及 Microsoft、IBM、PwC 等世界 500 強企業顧問。曾擔任許多大型專案及政府計畫主持人與諮詢委員，專注於數位科技與創新管理等議題。