

3/18

美國亞洲集團印度分部



科管局投資組顏嘉誼副組長（右2）、美國亞洲集團印度分部Ashok Malik主席暨合夥人（左2）

3/19

日本千葉縣政府企業立地課



科管局投資組翁淑婷科員（右1）、日本千葉縣企業立地課藤崎啓司副課長（右2）

3/19

日本經濟產業省中國經產局



科管局投資組盧宥宇專門委員（右3）、日本經濟產業省中國經產局中村崇課長（左3）



趨勢脈動

影子 AI 對於企業治理與競爭的隱性重構

The Implicit Restructuring of Corporate Governance and Competition by Shadow AI
シャドー AI が企業管理及び競争にもたらした変革

● 文・圖／MIC資深產業分析師 郭唐帷

生成式 AI 快速普及後，AI 不再僅存在於正式導入的系統或策略專案中，而是以低門檻、分散化的方式進入日常工作流程。這些未被正式納管的影子 AI（Shadow AI）使用行為，已開始對企業既有治理架構與風險管理方式產生實質影響。影子 AI 並非單一技術議題，而是一項牽動企業治理模式與競爭基礎的結構性變化。

影子 AI 正逐步改寫企業競爭與治理邏輯

多數企業至今仍將影子 AI（Shadow AI）視為一項需要被控管的風險行為，普遍認為只要補齊內規、強化資安控管，或透過技術手段加以封鎖，風險便能獲得控制。然而，從近年多份企業調查與白皮書所呈現的結果來看，影子 AI 並不是即將出現的未來趨勢，而是已在企業內部廣泛運作的結構性現象。無論企業是否已有正式的 AI 導入計畫，生成式 AI 與各類即取即用的工具，早已以非正式的方式滲透至日常工作之中。

在許多組織內，員工使用 AI 協助資料整理、內容生成、初步分析與報告撰寫，往往並未被視為正式的系統導入，而是個人工作技巧的一部分。正因如此，這些行為長期遊走於制度視野之外，使企業難以即時察覺其規模與影響。這也意味著，影子 AI 不僅改變員工完成工作的方式，更在不知不覺中重塑企業的治理邊界與競爭基礎。

既有治理邏輯正在失效

所謂影子 AI，係指未經企業正式導入、核准或納入治理架構之 AI 工具或模型使用行為。這類使用多由員工基於實際工作需求，自行採用外部生成式 AI 服務、個人帳號或非正式技術管道完成。其往往未被現行制度、資安機制或 IT 管理流程完整掌握，特徵並非高度技術性，而是高度分散、低門檻且難以追蹤。

過去企業技術治理架構與導入多半由中央統一決策，例如 IT 部門負責系統建置與維運，業務單位則在既定系統範圍內運作；其系統邊界清晰，

風險較可透過流程設計與事前審核加以控管。這套模式在 ERP、雲端服務，乃至早期資料分析工具普及的階段，仍具高度適用性，也成功支撐了企業的規模化與效率提升。

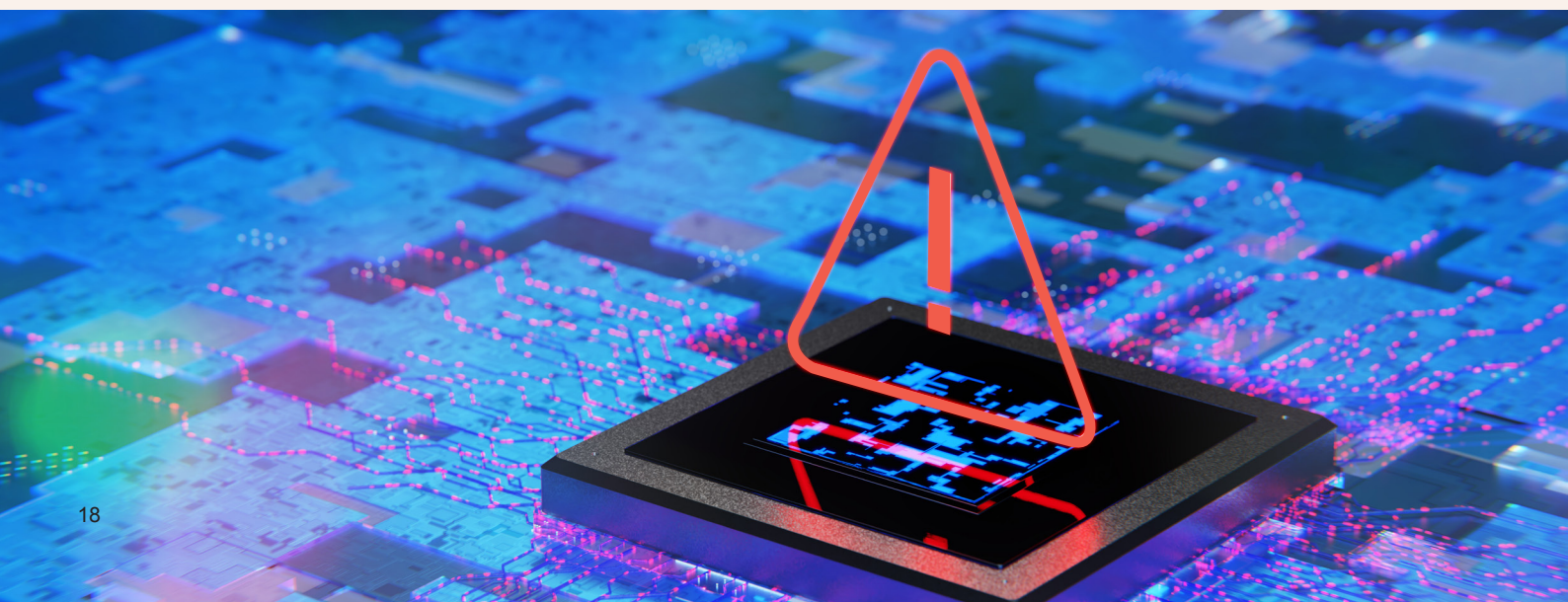
然而，隨著生成式 AI 與個人化工具快速擴散，這套技術治理架構的侷限性開始浮現。AI 不再僅存在於企業正式導入的系統之中，而是以服務、平台或個人帳號的形式，直接進入工作現場，企業的治理邏輯若仍假設只要控管系統即可控管行為，便難以回應這種變化。

而此次影子 AI 的關鍵差異，在於 AI 能力首次以低門檻、即取即用的形式，直接嵌入個人層級的日常工作之中。員工無須等待系統建置，也未必理解模型架構或資料治理原則，便已能運用 AI 影響分析結論、內容產出，甚至對外的業務判斷。這使 AI 的實際使用速度，遠遠超過企業制度更新與治理調整的節奏。在此情境下，企業過去長期依賴的事前審核與系統上線即治理模式，已難以涵蓋實際的 AI 使用樣態。

競爭門檻正在重新塑造

多數企業在面對影子 AI 時，直覺反應仍是透過內規宣告、資安限制或技術封鎖來降低風險。然而，相關研究亦顯示，這類作法成效有限。員工基於效率與實務需求，仍會持續使用外部或未經核准的 AI 工具，甚至在規範越嚴格的環境中，使用行為反而更趨隱蔽，間接影響實際使用行為與正式制度之間的落差持續擴大。

表面上，企業似乎維持了合規狀態，內規齊





備、系統防護完備；實際上，卻逐步喪失對 AI 使用情境的可視性。企業往往無法清楚掌握哪些工作流程已高度依賴 AI、哪些資料曾被輸入外部模型，以及這些使用行為對營運與風險結構產生了何種影響。

影子 AI 的核心特徵之一，正是企業難以清楚掌握誰在何時、以何種方式使用 AI，以及其產出如何影響業務流程與判斷結果。當 AI 使用長期處於制度視野之外，治理重點便不再侷限是否違規，而是企業具備基本的風險辨識、評估與回應能力。

影子 AI 現況下的治理現實

多數影子 AI 相關研究並未主張企業應全面禁止 AI 使用，反而聚焦在缺乏治理可視性、與制度落後於實際使用行為，才是風險持續累積的主因。換句話說，影子 AI 本身並非問題的起點，問題在於這些 AI 使用行為企業看不見、不了解、也未被納入治理視野，才是產生企業治理失效風險的關鍵。

企業首要任務並非立即擴張 AI 投資或導入更多工具，而是先建立對既有 AI 使用行為的基本掌握，包括哪些類型的工作已實際使用 AI、使用情境集中於何處、以及這些使用行為對既有流程的影響範圍，若缺少這層理解，任何規範或控管措施都難以發揮實質效果。

對於企業而言，面對影子 AI 的關鍵抉擇，不在於是否容許或禁止，而在於治理的重心轉向。應從單點封鎖或事後究責，轉向如何在不完全阻斷使用的前提下，逐步恢復對 AI 使用情境的理解與掌握。實務上，這並非要求企業介入具體工具選擇或操作細節，而是必須在組織管理層級釋出清楚訊號—影子 AI 是一項需要被看見、被討論、被納入治理框架的現實，而非只能被地下化處理的違規行為。

影子 AI 已是企業治理須正視的長期現實

影子 AI 並非短期管理亂象，而是 AI 能力全面個人化與低門檻化之後，企業必然面對的一種長期結構性現實。影子 AI 現況所揭示的，並不是紀律鬆動或工具管理失當，而是既有治理架構是否仍能如實反映企業內部的實際運作情境，以及是否具備因應新型態風險的調整能力。

在當前影子 AI 普遍存在的情況下，企業所面臨的挑戰已不在於是否能完全避免 AI 的非正式使用，而是如何在可視性有限、使用行為高度分散的環境中，維持基本的治理有效性與風險掌握。現代企業必須重新檢視過往以制度完整性與事前控管為核心的治理思維，並思考在新常態下，如何轉向更貼近實際運作的治理方式。

對企業而言，能否及早正視影子 AI 所反映的結構變化，並將其納入治理視角，而非僅視為例外或偏差行為，將深刻影響未來風險管理的穩定性與組織調適能力。能夠完成這項轉換的企業，將更有條件在高度不確定的 AI 環境中，建立長期且可持續的治理基礎。

MIC AISP 網址：<https://mic.iii.org.tw/AISP>

著作權所有，非經資策會書面同意，不得翻印或轉讓。

以上研究報告資料係經由 MIC 內部整理分析所得，並對外公告研究成果，由於產業倍速變動、資訊的不完整，及其他不確定之因素，並不保證上述報告於未來仍維持正確與完整，引用時請注意發佈日期，及立論之假設或當時情境，如有修正、調整之必要，MIC 將於日後研究報告中說明。敬請參考 MIC 網站公告之最新結果。