

● 2026

● 台灣重點產業AI化

● 政策建言 ●

目錄

序	3
前言	4
國際 AI 發展現況與台灣 AI 應用現況	5
國際趨勢	6
台灣產業現狀	9
產業 AI 落地挑戰	13
醫療業：從 AI 醫療到 AI 大健康產業，醫療產業的內部轉型與外部助力	13
製造業：台灣智慧製造關鍵字：人才、流程、跨部門協作	17
金融業：生成式 AI 加速金融業變革 信任依舊是最大挑戰	20
結論	23
台灣產業 AI 化的下一步：基於 AI 治理框架與資料共享機制之前瞻佈	23

邁向可信任與主權 AI 的時代

文 / 詹婷怡（人工智慧科技基金會董事長）

人工智慧（AI）正在改寫全球科技競局的秩序。自 2022 年底 ChatGPT 引爆第二波 AI 浪潮以來，世界已從單純的技術突破進入以治理、應用與制度為核心的轉折時代。這不再只是模型性能的比拼，而是一場結合算力、數據、資本與政策的國家級戰略競賽。AI 已從「科技創新」轉化為「制度創新」的戰場，成為重新定義國家韌性與主權的新基礎建設。

在這個重構中的全球格局裡，全球發展呈現從技術競逐，走向以治理為核心的戰略佈局，也採取不同的 AI 治理路徑，整體觀察，各國正試圖在「創新速度」與「社會信任」之間取得平衡，將 AI 能力內化為公共治理效能與產業競爭力；AI 的科學性質正從「分解式研究」轉向「整合與規模化運算」，未來的創新不再只是演算法的突破，而是整個基礎設施體系的協作與優化。

更重要的是，隨著「主權 AI」的提出與建構，算力、能源與資料安全已成為全球戰略資源，AI 已不僅是技術問題，而是國家安全與經濟治理的議題。

對台灣而言，AI 的挑戰不在技術匱乏，而在「認知與實踐之間的鴻溝」、「軟硬發展失衡的結構性瓶頸」、以及「信任與治理機制的亟待建立」。儘管擁有全球最完整的半導體與 ICT 供應鏈優勢，台灣產業多仍停留在「觀望」與「初階導入」階段。在產業導入層面，AI 的挑戰呈現出不同面貌。



本報告為人工智慧科技基金會在《產業 AI 化大調查》基礎上，結合產官學研專家，經由討論及訪談並整合研究產出的階段性研究成果。

在 AI 將成為新時代的「介面」，重構人與技術、政府與社會的互動邏輯的趨勢下，台灣若能從「製造優勢」走向「治理優勢」，以信任為基礎建立資料治理架構，便能將硬體實力轉化為軟性領導力，在新一輪全球 AI 秩序中確立自己的位置。

這不只是科技政策的課題，更是一場關乎國家未來方向的治理考驗。

從技術突破到治理轉折的關鍵國家戰略

隨著人工智慧技術與應用的爆發性成長，全球正經歷一場深刻且劇烈的技術典範轉移與治理思維變革。自 2022 年底 ChatGPT 引爆第二波 AI 浪潮以來，不這場競賽已從單純的模型效能比拚，演變為融合算力、數據、資本與制度的國家級戰略部署。

在此新階段中，技術領先的關鍵不再僅取決於模型效能的優劣，而在於能否將 AI 能力有效轉化為產業韌性、公共治理效能與國家競爭力。產業現已浮現一種共識，AI 發展的成功應以「能否創造社會性價值」為衡量標準，而非僅是技術表現。

對台灣而言，這番話提醒我們，當前挑戰在於如何以既有基礎為起點，發展出具有在地價值與應用深度的 AI 生態體系。而過去引以為傲的硬體優勢，其實尚未有效轉化為人工智慧應用與價值創新的實質動能。這不僅是產業升級的課題，更是一項橫跨資料治理、人才培育與跨域創新的系統性工程。

放眼全球，各主要經濟體正積極從政策、法規與產業推動等層面重新定義 AI 的發展路徑與治理準則。台灣若欲在這場結構性變革中確立策略定位，必須審視自身優勢與挑戰，並提出具體可行的政策行動，從技術導向邁向能力導向，從硬體製造走向智慧創新。

人工智慧科技基金會（AIF）長期關注台灣產業的 AI 化進程，透過系統性調查與跨領域研究，持續觀察企業導入 AI 的現況、挑戰與需


求，並以數據為基礎，協助政府與產業界擘劃可行的 AI 行動藍圖。在 2025 年底以本會發展之分析框架為基礎，彙整今年度多項研究報告，加上兩場專家會議、兩場大型論壇，及六場產業演講的業界意見，做為本報告主要內容之一。

同時，再加入國內外專家對於技術發展、產業應用趨勢、數據治理、風險管理等與 AI 發展密切相關的重要分析。且針對過去幾年台灣產業 AI 化發展的重點產業：醫療、製造，及金融，訪談產業重要推手。藉由他們的觀察與經驗，提供相關產業未來導入 AI 的具體參考；同時，也做為政府推動 AI 政策的重要參考。

成立於 2017 年底的 AIF，是台灣少數獨立營運的非營利組織，由產業與學術界關心台灣 AI 進展的專家們組成董事會，致力於推動台灣產業 AI 化。

透過系統化方法，以課程培訓、技術協作、轉型陪跑、顧問諮詢等方式協助各產業擁有足夠的 AI 技術與管理能力。並藉由《知勢》，持續溝通傳遞正確的 AI 知識、趨勢與挑戰，每週電子報與近五萬位關注 AI 發展的朋友分享。藉由長期累積的技術與論述能力，進行多項調查研究，分享可信任的數據與研究成果，掌握台灣產業 AI 化真實樣貌，並做為政策倡議基礎。

特別感謝學界、企業與法人組織長期以來的支持與合作。相信透過公私協力與不間斷的投入，我們將共同推動台灣邁向一個更具創新力、信任度與永續性的 AI 新時代。



趨勢與現況

國際 AI 發展現況與台灣 AI 應用現況

本文將深入剖析當前 AI 發展的三重關鍵轉向：首先，在國際趨勢，各國如何從單純的技術競逐轉向以治理為核心的戰略佈局；其次，在學術領域，AI 如何顛覆傳統電腦科學的思維，從「分解」走向「整合」；最後，在技術與地緣政治方面，AI 發展重心如何從基礎模型的研究，轉向應用深化與「主權 AI」的建構。理解這三大轉向，是掌握未來十年全球科技與政治經濟互動、發展的關鍵。

電腦科學進入「規模化」「整合」的時代

人工智慧技術的迅速演進，促使電腦科學（Computer Science）領域出現深層且結構性的典範轉移。早期電腦科學的研究者能以有限資源推動理論與應用的突破。然而，隨著 AI 的興起與算力需求的爆炸性成長，研究成本從數百萬美元攀升至動輒數十億美元，其規模與複雜度已可比擬高能物理的粒子對撞機或航太工程的火箭發射工程。

這場規模化競賽使得 AI 研究逐漸從學術型創新走向資本與基礎設施主導的局面，只有擁有龐大算力與資料資源的大型國家或科技巨頭得以參與其中。在多份全球重要 AI 國力觀察中皆已發現，相對較缺乏資源的個人研究者與學術機構，在基礎模型创新的前沿，幾乎失去了競爭的基本配備。而 AI 已從一門「理論科學」，演變為需要龐大算力、數據與基礎設施支撐的新型科學基礎建設。

再者，當前的大語言模型將過去分屬於不同領域的能力，如語言理解、影像辨識、邏輯推理、程式碼生成與網路搜尋，融合於單一的神經網路架構之中。這顛覆了過往傳統的軟體工程與演算法設計，將複雜問題拆解成更小、更易於管理的單元，進行模組化設計，最後再行整合的方式。

這也使得美國的電腦科學畢業生乃至博士生，

正開始面臨研究方向過度集中、就業職位收斂的現象。因為許多過去需要專職團隊耗費數年開發的特定功能模組，如今皆能被一個強大的基礎模型所涵蓋。AI 正在成為一個跨領域整合工程、數據科學與知識生態的再造體系。

誰能將模型轉化為具體應用，才是競爭關鍵

大型語言模型在這幾年爆炸性指數成長後，發展逐漸趨緩，如近期備受關注的 GPT-5，其性能提升幅度已不如前一代。這也引發全球科技界對技術發展速度是否趨緩的討論。這樣的現象可能反映兩大層面挑戰：其一是組織因素，如頂尖 AI 實驗室可能面臨人才流失、內部治理結構調整與策略分歧的困擾；其二則是技術本身的瓶頸。現行的 Transformer 架構與依賴「預測下一個詞（Next Token Prediction）」的訓練機制，在耗盡了網路上幾乎所有高品質數據後，可能已接近其理論極限。

但技術發展趨緩，並非意味衰退，恰好可視為宣告了「應用時代（Application Time）」的正式來臨。意味著當前世界的重心，正從「創造模型」的競賽，轉向「應用模型」的競賽。未來的競爭關鍵，將不再是誰擁有最大、最先進的模型，而是誰能以最快的速度、最可信任的方式，將 AI 的能力深度整合至各行各業，轉化為實質的生產力提升與社會信任的累積。

對台灣而言，這是至關重要的戰略契機。也

意味著我們應將重心轉向如何善用現有及開源的強大模型，深度結合台灣在半導體、製造業、醫療等領域的在地優勢，發展出具有獨特價值、難以被輕易複製的應用服務與健全的生態系。

地緣政治與主權 AI：新時代的國家賽局

另一方面，隨著 AI 從實驗室走向產業應用，對國家基礎設施的戰略也產生重大影響。由於大型模型的訓練與推論，需要消耗龐大算力與能源，直接牽動了國家安全、產業佈局與能源政策。因此，AI 已不再僅僅是科技議題，更是一個主權議題。「主權 AI（Sovereign AI）」的概念應運而生，成為各國政府關注的焦點。

全球主要強權正圍繞主權 AI 展開新一輪國際競局：如美國憑藉其在雲端運算（GCP, AWS, Azure）與頂尖晶片（NVIDIA, Intel）的雙重生態優勢，試圖鞏固其在全球 AI 領域主導權。

中國則強調數據的本地化與自主可控，透過國家力量推動自有的 AI 技術與治理體系，力求在關鍵技術上不受制於人。

歐洲則另闢蹊徑，以其嚴格的法規（如 GDPR、《AI 法》）與倫理標準為核心，致力於建立一個以「可信任 AI」為品牌的全球秩序，試圖在治理層面掌握話語權。

在這場全球格局重塑的過程中，台灣處於一個極其特殊的位置。我們擁有全球頂尖的晶片製造能力與高覆蓋率的高速網路基礎，這是發展 AI 不可或缺的硬體基石。然而，相較於硬體

無可取代的競爭力，台灣在形成具有戰略高度的國家 AI 政策方面，至今仍未有足夠明確的方向與藍圖

AI 治理應是創新推進器而非枷鎖

在全球 AI 競賽中，創新的治理思維與規範是打造長期競爭優勢的基石。各國正積極轉變監理角色，從傳統的防弊管制，邁向兼顧「促進創新」與「風險控管」的積極治理。歐盟《人工智慧法》以風險分級建立社會信任；新加坡透過自願性框架與沙盒降低新創門檻；日本則利用政府採購引導產業標準；韓國與美國更以國家戰略高度，結合立法與投資鞏固領導地位。以下為各不同經濟體在 AI 治理方向上的重點：

歐盟：以嚴謹框架建立全球標準

歐盟是全球最早也最積極推動 AI 法制的地區。2024 年正式通過的《AI 法》，是其建構數位單一經濟市場的雙軸戰略（資料治理與 AI 治理）下的里程碑。該法案以「風險分級」為核心，從全面禁止的用途（如社會信用評分），到被列為高風險的應用（如關鍵基礎設施、醫療、教育等），設立了一整套嚴格的文件化、監管與透明度義務。透過 2025 年至 2027 年的分階段實施，歐盟為企業提供了清晰的時間表與責任框架，讓投資與產品設計有跡可循。同時，歐盟要求各會員國設立「AI 監理沙盒」，並制定協調標準與通用模型行為準則，確保法規能落實為可操作的測試與稽核流程。歐盟的目標不僅是守住倫理底線，更是要以經濟成長

為導向，建立一套全球供應鏈的共同語言，讓符合其規範的廠商在全球市場上更具競爭力。

新加坡：以輕量化應用工具引導市場快速發展

相較於歐盟的全面性法規，新加坡採取了更為靈活的「自願性框架+可驗證測試」路徑。2024 年推出的《生成式 AI 治理框架》，以九大治理面向提出具體操作建議，並透過 AI Verify 等工具，將抽象的治理原則轉化為可測試、可報告的具體流程。新加坡特別強調可驗證性、資料治理及負責任的部署，並積極推動全球 AI 保證沙盒。這種輕量化、工具導向的模式，不僅降低了新創企業的進入門檻，也方便企業將合規能力轉化為市場信任的背書。

日本與韓國：促進與監管並行的亞洲模式

日本與韓國展示了亞洲國家如何在促進產業發展與風險管理間取得平衡。日本在 2025 年施行的《人工智慧促進法》，以推動研發與應用為主軸，輔以政府的調查與矯正機制。值得注意的是，日本政府透過發布「生成式 AI 採購指南」，巧妙地運用「買方力量」，將風險控管、資料治理與人類監督等要求納入政府採購流程，實質上為市場設定了合規門檻。

韓國則藉 2025 年公布、2026 年施行的《人工智慧基本法》，建立政府與產業共治的架構。該法案一方面推動國家戰略級的 AI 投資與產業聚落發展，另一方面要求高影響力的生成式 AI 落實風險評估與透明義務。藉由法律與投資並行的方式，為企業的長期發展塑造穩固基礎。

美國：以國家戰略引領全球

美國的 AI 政策以「積極治理」為核心，其目標明確：鞏固美國在全球 AI 領域的領導地位。從 2019 年的《美國人工智慧倡議》到 2025 年的《人工智慧行動計畫》，AI 始終被視為國家競爭力與安全的基石。其計畫涵蓋超過 90 項政策行動，著重於鬆綁監管以加速創新、強化基礎設施建設、加強出口管制，並在國際上積極推動符合美國價值觀的技術標準。

這些國家路徑雖異，但共同點皆是將監理視為促進產業成熟的推進器，而非抑制創新的枷鎖。這對全球企業傳遞出明確訊息：合規能力已非營運成本，而是進入市場的門票與贏得信任的憑證。

台灣產業現狀

政策與政府倡議：從策略布局到產業落地

隨著生成式 AI 帶動全球新一波人工智慧熱潮，各國政府相繼將 AI 納入國家戰略核心，透過制度化政策與法規強化競爭優勢。台灣政府近年亦持續推動多項 AI 發展計畫，從「臺灣 AI 行動計畫」、「數位國家・創新經濟發展方案（DIGI+）」，到接續的「臺灣人工智慧發展藍圖（AI Taiwan Action Plan 2.0）」，皆以促進 AI 技術落地、提升產業競爭力為核心目標。

自 2024 年起，政府更啟動為期十年的「晶創臺灣方案」，強調以生成式 AI 及半導體晶片優勢為基礎，協助企業在製造、金融、醫療、零售等領域建構 AI 應用場景，並結合「臺灣人工智慧發展藍圖」推動跨部門資料整合與 AI 治理體系。

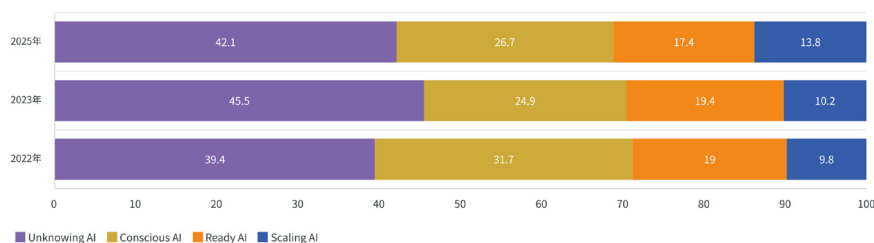
然而，根據人工智慧科技基金會發布的《2025

台灣產業 AI 化大調查》，儘管企業對 AI 的基礎認知有所提升，仍有七成企業停留在初步認知或觀望階段，真正進入規模化應用的比例，在過去三年中幾乎沒有變化。這道從「認知」到「實踐」的巨大鴻溝，成為台灣 AI 發展最迫切需要跨越的關卡。

本文即以此調查為基礎，深入剖析台灣當前的政策倡議、產業優勢與機會，直面基礎設施、數據、人才與法規治理等核心挑戰，擘劃出台灣在全球 AI 競賽中的獨特定位與未來路徑。

產業優勢與機會

台灣擁有完整的半導體供應鏈、精密製造基礎與高密度的 ICT 生態系，這些條件為 AI 落地提供了天然優勢。因此在裝置端 AI（On-device AI）與邊緣運算（Edge AI）領域，具備得天獨厚的發展潛力。當前 AI 模型的演進



根據人工智慧科技基金會《2025 台灣產業 AI 化大調查》顯示，過去兩年來，台灣企業對 AI 的認知顯著提升，「Unknown AI」企業比例從 45.5% 降至 39.4%，「Conscious AI」則增長至 31.7%，顯示 AI 相關知識正在企業間逐步擴散。

方向已從雲端集中訓練走向模型蒸餾（Model Distillation）與輕量化部署，使得 AI 能直接運行於 PC、車載系統與智慧手機等終端裝置上。這樣的趨勢使台灣有機會將既有硬體優勢轉化為「AI 裝置島」的國際定位。

《2025 台灣產業 AI 化大調查》亦顯示，台灣企業在「技術應用」面向的平均分數已達 47 分，為三大指標中成長幅度最高的項目。資通訊業在工具導入、模型應用等面向表現最佳，顯示生成式 AI 工具的普及已初步降低 AI 使用門檻。製造業與政府機關的 AI 使用率亦明顯提升，特別是在影像辨識、預測性維護與流程自動化等場域，已出現具規模的導入案例。

從全球產業鏈角度觀察，AI 與邊緣運算的結合將帶動新一波硬體與軟體創新循環。台灣若能以半導體為基底，整合晶片設計、軟體演算法與場域應用，將有機會在全球 AI 生態中扮演「系統整合樞紐」的角色。這不僅有助於開拓新型出口市場，也可帶動本地新創與中小企業的創新應用，形成具在地價值的 AI 生態體系。

此外，AI 也為傳統產業帶來結構性升級的契機。無論是以資料驅動零售決策、AI 強化金融風險控管，或智慧排程優化製造流程，AI 將漸成為企業營運效率與創新能力的核心驅動力。

國立中央大學資訊工程學系教授蔡宗翰指出，台灣企業若能善用 AI 建立「企業大腦」，將資料視為長期資產並持續優化流程，將能在競爭激烈的市場環境中創造更具韌性的成長模式。

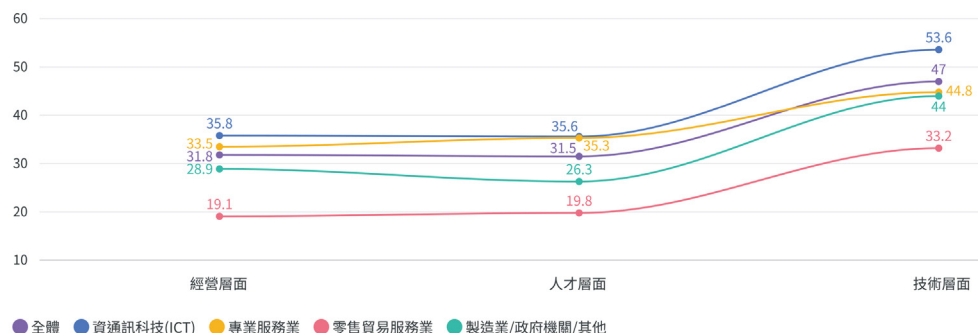
產業挑戰：基礎設施、數據、人才與法規

儘管企業對 AI 的認知明顯提升，調查結果卻顯示落地應用的進展依舊緩慢。根據 AIF 連續三年的調查，約七成企業仍停留在「Unknowing」與「Conscious」兩個早期階段，僅有三成企業進入實作或規模化階段。這種現象揭示了台灣產業在 AI 化進程中存在的結構性瓶頸，主要可歸納為四大挑戰：

（一）算力集中與部署需有完整佈局

目前台灣的算力資源仍集中於少數大型研究機構與雲端平台，企業在實際導入過程中，常

近五成企業尚未建立明確的 AI 人才發展策略，即使有策略，往往僅停留在提供相關課程，而未將 AI 技能培養與員工職涯發展連結。



因運算資源不足或成本過高而受限。AIF 建議政府推動「分散式算力」策略，結合地端運算與邊緣 AI，降低對集中式雲端的依賴，以強化自主性與風險韌性。

（二）數據品質與資料治理待加強

超過半數受訪企業表示，資料仍以非結構化或分散儲存為主，導致 AI 模型訓練成效有限。部分零售與製造業者甚至在資料尚未電子化前便嘗試導入模型，形成「資料先天不足、應用後天受限」的困境。雖然越來越多企業設置資

料長（CDO）或資料治理職位，但對「資料交換策略」與「跨組織資料流通規範」的理解仍不足，將成為台灣企業與國際可信任 AI 標準接軌的重大挑戰。

（三）人才斷層與組織轉型困難

在「人才培育」指標中，企業平均僅 31.5 分，且有 47% 企業尚未制定 AI 人才發展策略。多數企業缺乏跨領域能力的 AI 應用型人才，使得技術與業務間的溝通產生落差。AIF 建議企業應從「可賺錢的場景」著手，先在能創造實質



產業 AI 化四大發展階段

「台灣產業 AI 化大調查」透過企業 AI 能力評估，從「經營策略」、「人才培育」及「技術應用」三大面向進行分析，綜合評分後，將企業劃分為「Unknowing AI」、「Conscious AI」、「Ready AI」與「Scaling AI」四個發展階段，以反映企業在 AI 認知與應用上的不同成熟度。

效益的應用場域推動 AI 實驗計畫，再逐步擴大內部共識與培訓規模，形成組織性學習循環。

（四）法規滯後與信任缺口

AI 的推廣若缺乏相應的法規支撐，將無法保障資料使用與隱私安全。調查指出，多數企業對「裝置端 AI」與「雲端 AI」的區別認知不足，容易在資料上傳或模型訓練過程中產生潛在資安風險。AIF 呼籲政府應加速建立 AI 治理與風險管理框架，強化資料匿名化、差分隱私等機制，並推動 AI 產品認證與標準化制度，確保產業能在安全可信的環境中發展。

以「信任」為核心，打造台灣 AI 新動能

《2025 台灣產業 AI 化大調查》揭示，台灣企業在 AI 化進程中雖已啟動，但仍處於早期整備階段。生成式 AI 的興起為台灣帶來轉型契機，也暴露出認知落差、資料治理與人才供給的系統性問題。面對全球 AI 競爭加劇與地緣風險升高，台灣若能以「可信任 AI」為治理核心，以「主權 AI」為戰略方向，並以應用落地為政策主軸，將能在技術與治理雙軌推進下，實現從製造強國走向 AI 強國的關鍵跨越。

AI 發展的最終目標，不在於技術炫目或模型規模，而在於能否提升社會生產力、促進產業升級並創造公共價值。人工智慧科技基金會將持續透過系統化的觀察與政策研究，協助政府與產業界制定可執行的 AI 行動藍圖，推動台灣建立具韌性、信任與創新能量的人工智慧生態體系，邁向更具自主性的智慧國家未來。



AI 應用如何落地成為企業營運流程的環節，是企業導入 AI 最重要的步驟，也是最大關卡。人工智慧科技基金會特舉辦產業論壇，邀請金融、醫療、製造三大領域專家，深度剖析 AI 導入的挑戰與機會。與會者普遍認為，AI 導入的成功關鍵，不僅在技術，更在於資料治理、人才策略、跨部門協作，及能否從企業內部「痛點」出發，找到務實應用場景。

醫療業： 從 AI 醫療到 AI 大健康產業，醫療產業的內部轉型與外部助力

在全球供應重組、關稅與通膨壓力交織下，台灣傳統產業與中小企業正承受前所未有的挑戰。人工智慧（AI）被視為推動創新與生產力的關鍵動能，但同時也伴隨大家不熟悉的治理挑戰與進入門檻，成為企業轉型的重大課題。

醫療 AI 落地的關鍵思維：從深度學習到信任

儘管台灣具備深厚的 ICT 與醫療體系基礎，智慧醫療發展仍然有不少挑戰。當中最關鍵但也最被忽略的，是「信任」這項底層基礎。在「從數據整合到風險治理：金融、醫療、製造業的挑戰與機會」論壇中，與會專家們一致認為，要讓 AI 應用真正融入醫護流程，必須贏得醫護人員與大眾的信賴，這不僅關乎技術，更取決於流程簡化與數據治理。

AI 不只「深度學習」還需要「深度清理」

中國醫藥大學附設醫院巨量資料中心副院長郭錦輯以其十多年的醫療 AI 經驗，點出醫療產業發展的關鍵痛點。他認為，醫療 AI 從技術發想，到真正能被醫護人員採用的過程，遠比想像中艱難。AI 產品必須經歷漫長的產品驗證週

期，包括 FDA 或 TFDA 的嚴格認證，以及後續真實世界的臨床效能試驗。但這樣的驗證時間，對於 AI 應用發展與商品化而言，「是難以想像的緩慢」。

郭副院長以中醫大開發心臟肥大 AI 產品為例，僅一個站點的開發就耗時五年，但產品開發完成總共有六個站點。他坦言，這就像「騎著一個輪子是正方形的腳踏車」，進展非常緩慢，不僅考驗開發者的耐力，也讓 AI 的商業化之路充滿不確定性。

另一個重要的普及應用關鍵，則在於 AI 系統能否融入現有的醫護流程中，郭錦輯稱為「入流」，意即讓醫療 AI 真正融入醫護流程。按照過去多年經驗，中醫大有個重要原則：AI 若要正式佈署進現有流程中，必須達成「絕對簡化」，任何會增加醫護人員額外負擔的 AI 功能都是不可行的。例如，若 AI 跳出警示，仍需醫師再次檢視判斷或進行其他動作，那這個 AI 就失去存在的價值，因為醫護人員的專業本身已足以應對。

郭錦輯強調，每個產業的價值主張與從業人員的思維有其特色，例如醫師普遍具有極高的專業自我認同（Ego），若 AI 不能簡化流程並提供實質幫助，就無法贏得他們的信賴。因此，他認為醫療 AI 的開發不應只著重於「深度學習」（Deep Learning）的模型建構，更應專注於「深度清理」（Deep Cleaning），也就是優化工作流程，將層層加法變成減法，才能讓 AI 真正發揮價值，獲得醫護人員的信任。

數據與法規：建立「信任」的底層基礎

不過，實現 AI 的「入流」，不僅需要技術上的簡化，更需要解決數據與法規層面的信任問題。與會專家幾乎都認為，台灣醫療數據的使用受到嚴格限制，必須取得病人的知情同意書並符合政府法規，這使得數據共享與整合變得極為困難。以中醫大為例，為使用病人數據進行研究，耗費巨大工程重簽所有同意書，但這樣的工程對其他醫院而言，都是巨大的負擔。

專家提醒，若法規不明確，使得醫院無法確認如何讓數據的處理合法合規，對 AI 的發展自然形成極大障礙。正如台智雲總經理、台灣生醫大數據科技公司總經理吳漢章所指出，智慧醫療的商業化與產業化難度普遍被低估，其決勝關鍵不在技術，而是如何建構穩固的「數據信任」架構。

後疫情時代，智慧醫療進入發展新周期

從產業發展周期來看，2020 年襲擊全球的 COVID-19 疫情徹底改變了產業版圖，對醫療系統的認知與期待也隨之翻新。伴隨著已發展國家高齡化與少子化的人口結構趨勢，吳漢章歸納出目前智慧醫療聚焦的三大領域分別是：個人化健康（Personalized Health）、遠距照護（Virtual Care），以及確保醫院服務量能的醫院韌性（Hospital Resilience）。無論哪種應用，都離不開結合 AI 技術，使得這些應用真實融入人們的生活。

另一個值得關注的領域則是長照陪伴。早在

2016 年，Zenbo 機器人便引發醫護人員對於長照陪伴應用的詢問。當時社會已預見少子化帶來的「孤獨」與「孤老」等社會現象，而陪伴被認為能減緩長者身心功能的退化。然而，當時的 AI 技術尚顯稚嫩，難以理解國、台、客語夾雜的日常對話，更遑論展現同理心。

但隨著 2022 年底以來生成式 AI 的突飛猛進，AI 已能流暢地進行多語對話並展現同理心，使產品真正具備走入市場、服務人群的能力。

技術到位，價值未現：AI 落地的關鍵困境

從診斷、照護到健康管理，雖然有許多技術開發應用，成功的醫療專案也不在少數，但是許多熟悉醫界 AI 應用的專家都指出一個關鍵困境：對於醫院而言，AI 至今仍然是成本支出，尚未創造新的價值。究其原因，在於這些先進技術並未真正落地整合。

建構一個穩固且具公信力的數據治理框架

另一方面，可信任與資料治理也是台灣智慧醫療發展不可或缺的核心，吳漢章表示，目前在健康資料治理主要有兩種路徑：

1. 個人授權資料庫：

此模式以美國衛生研究院（NIH）2015 年推動的「All of US」計畫為代表。該計畫採取民眾「知情同意」方式蒐集健康數據，並依三種授權等級（公開、註冊、控管）開放利用。

華碩團隊在 2018 年後，參酌「All of US」做法，在健保署支持下，與健康存摺合作試行建立「Databank」，透過手機 APP 實現個人健康大數據的授權應用，採用全面電子化方式，讓民眾能參與、捐助並控管個人資料。同時，華碩也試著套用歐盟嚴謹的 GDPR 規範，並參酌歐盟「Horizon 2020」轄下的「歐盟 PULSE 計畫」在基隆市進行百人研究案，協助民眾開通健康存摺，實踐完整知情同意流程，結果顯示 72% 民眾認為對健康管理有幫助。

2. 醫療病例共享資料庫：

此模式以醫院為主體，如 2013 年成立的 TriNetX 公司，專注提供真實世界數據（RWE）解決方案。醫院在取得民眾同意後，共享匿名的電子病歷、保險理賠等數據。此模式源於歐盟的「EHR4CR 計畫」，旨在讓藥廠能合法合規利用醫院數據。

吳漢章指出，此商業模式的優勢在於「資料不離院」、匿名化處理、符合多項國際法規（GDPR、HIPAA 等），醫院不僅無需投資資訊系統，甚至能從中獲得收益。

然而，他坦言，將此服務引入台灣時，仍因適法性疑慮，醫院導入意願不高，普遍都希望監管單位能出具同意證明。

公私協力 打造可信研究環境

從兩種不同資料治理路徑可以看出，一個具公信力的諮詢單位是不可或缺的。唯有透過良

好的對話機制，讓相關數據獲得社會共識與公信力認證，才能實現醫療數據治理的落地。

吳漢章認為，公私協力（PPP）模式，正可以彌補商業公司在處理醫療數據時所面臨的質疑，整合政府的公信力與民間的技術活力，為建立一個高效、合規、可信賴的數據協作環境提供了最佳路徑。

台灣的生醫數據，特別是醫療資料，具有高度的敏感性，如果無法建立一個讓所有參與方都能信任的基礎，智慧醫療的發展將難以突破。與會專家們共同呼籲政府與企業應攜手合作，建立一個能夠信任的 AI 生態系。

專家也建議，政府可建立類似「駕照」的標準化認證機制，讓 AI 產品一旦通過審核，醫療院所便能更安心地採用，減輕自行評估與承擔風險的負擔。

台灣 AI 醫療的發展正處於一個關鍵的十字路口。要讓 AI 從實驗室裡的技術、臨床的實驗，轉變為能夠簡化流程、創造價值、贏得信任的實用工具，需要政府、企業與學研界共同努力，克服法規、數據、人才與資安的挑戰，讓 AI 醫療不僅是「可能」，更能成為「可行」。

製造業：台灣智慧製造關鍵字：

人才、流程、跨部門協作

在當前的全球產業競爭中，數位轉型與 AI 浪潮是生存永續必須面對的議題，而川普的關稅與匯率起伏，更是製造業無法迴避的壓力。對於製造業而言，從這兩年的經濟數據可以看出，這不僅是一場技術的軍備競賽、是關於人才、組織文化與企業治理的深度變革，更是嚴苛的生存之戰。台灣製造業如何在這場變革中找到自己的位置和下一步？

堆高機與物流設備製造商勤工、全球知名的紡織與成衣製造商旭榮集團，還有面板製造龍頭群創光電，這三家各具代表性的企業，分享了 AI 落地過程中的挑戰與洞察。

勤工突破員工焦慮與抵抗 以「人」做為 AI 落地核心

以堆高機與物流運輸設備製造起家的勤工，近年來已成功將業務擴展到無人化設備領域。然而，這場轉型並非一帆風順。勤工執行長林少顥指出，製造業導入 AI 的一大挑戰，來自於員工對於 AI 的焦慮感。他觀察到，傳統的電焊與組裝工人與新世代的 AI 工程師之間存在巨大的鴻溝，雙方語言不通，甚至會產生「這是要監督我、操控我」的抗拒心理。

為解決「人的問題」，勤工重新審視了 AI 落地的核心，強調 AI 應該是「賦能」而非「取代」。因此，公司推動了一項名為「專才變通才」的計畫，透過跨部門工作坊，打破各個職能部門之間的隔閡。林少顥認為，過去只專注於自身技能的「專才」模式已經過時，現在每個人

都必須成為能夠互相理解與協作的「同儕」。

在工作坊中，大家會面對面討論問題、分配資源，而不是透過書面文件互相推卸責任。公司的目標不是要「檢討任何人」，而是要「解決問題」。此外，勤工還透過工作坊與問卷調查，確保 AI 專案的成果能夠被員工「有感」地體驗到，這比評估能賺多少錢或省多少錢更為重要。一路走到現在，勤工將 AI 視為協助客戶與自身共同成長的夥伴，並將品牌重新定位為「賦予你的行動力量（Empower your move）」。

林少顥強調，只有解決了「人」的問題，AI 這項工具才能真正發揮價值。

旭榮「坦誠與分享」文化 讓 AI 成為員工自發的解決方案

今年正好歡渡 50 歲生日的旭榮集團，是台灣紡織業知名品牌，數位轉型之路起步甚早，近年來更將 AI 導入作為重點，並創產業之先設立「AI 長」職位。旭榮 AI 長郭羿伶指出，AI 成功落地的關鍵之一是 IT 團隊對生產流程的深刻理解。為達此目的，公司 IT 人員經常到工廠駐點，才能將技術與產線的領域知識緊密連結。

然而，比技術和流程更重要的是旭榮的企業文化：坦誠與分享。許多 AI 專案並非來自高層指令，而是由員工主動提出痛點，形成「由下而上」的推動模式。例如，在中國地區的財務部門，有員工自學 RPA（機器人流程自動化）技術，不僅改善了自己的工作流程，還主動服

務其他部門，號召大家「誰有痛點來找我」。

郭羿伶認為，AI Agent 非常擅長處理資料比對這類繁瑣且耗時的工作。例如，過去業務人員需要花兩到三個小時手動將客戶的 PDF 訂單轉換成 ERP 系統能讀取的資料，現在透過 AI Agent，這個時間可以縮短到 20 分鐘。旭榮會定期評估每支 AI Agent 的使用量和滿意度，確保它們真正解決了員工的痛點。透過小規模的成功案例，並在內部定期分享與表揚，能夠激勵更多員工參與。

郭羿伶強調，因為主要使用自然語言來撰寫，AI Agent 的開發門檻其實不高。所以她認為，具備「願意嘗試與樂於分享」特質的員工，最適合成為 AI 種子。AI 並不會取代人類，而是會淘汰那些不會善用 AI 的人。她鼓勵員工以開放的心態，將 AI 視為一個能幫助他們更快、更穩地完成重複性工作的工具。

群創從「三軸四刻度」到「泥巴與光」 打造跨域協作文化

身為面板製造龍頭的群創光電，在面對中國面板廠的激烈競爭下，更是必須快速追求轉型。群創光電智能與自動化解決方案事業中心總經理廖健宏，分享了公司的核心轉型戰略：重塑新文化、建立方法論與善用技術。他強調，轉型成功的關鍵在於高層的決心與員工的積極參與，必須是「由上而下」與「由下而上」的結合，缺一不可。

在方法論上，群創採用獨特的「三軸四刻度

模型」，將轉型分為自動化、數據化與智能化三個軸向。每個軸向都有四個刻度，讓每個專案都能在啟動時清楚定位，並根據投入產出比來調整目標。廖健宏也指出，在導入 AI 之前，必須先做好基本功，也就是流程改善的 ECRS 原則（排除、合併、重排、簡化）。群創自 2012 年起全面推動自研自動化技術，讓一條原本需要 100 人的生產線，現在只需要 7.5 人。面對少子化的壓力，已提早布署因應方法。

在人才策略上，廖健宏提到 AI 專案需要三種人才協作：領域專家（Domain Expert）、數據科學家（Data Scientist）與 IT 人員。這三種人才專業和理念不同，容易產生「油水不互融」的情況。為了促進協作，公司會讓資深員工帶領新進的數據科學家，讓他們「身上要有泥巴，臉上要有光」。這意味著數據科學家必須深入現場實做，親身了解流程，才能真正發揮價值。

廖健宏也坦言，評估 AI 專案的投資回報率（ROI）是一大挑戰。過去曾嘗試讓各部門自己計算效益，結果每個部門都說效益很大，但實際加總後卻遠低於預期。因此，群創後來改為根據不同部門的專業領域來設定具代表性的關鍵績效指標（KPI）。

他最後用一個寓言故事來總結：不要成為那個「很忙」，而沒空嘗試新方法的「方形輪子推車」工人。他強調，企業可以透過尋找有感染力的「領跑者」員工，先做出成功的示範，久而久之就能帶動整個組織文化的改變。

完善治理機制與跨部門協作是成功密碼

從三家企業的經驗來看，製造業在 AI 轉型上的突圍之路，專注於技術本身絕對是不夠的，人才培育與文化打造才是根本。勤工與旭榮的經驗都證明，AI 導入成功與否，最終取決於「人」的接受度。透過工作坊、內部訓練和開放的分享文化，可以有效消除員工的焦慮，並激發他們主動參與的熱情。

若從痛點出發，追求「小而美」的成功。廖健宏和郭羿伶的觀點不謀而合，都強調要從「效益大、容易做」的小專案開始，解決員工日常工作中的痛點，讓 AI 的價值被實際感受到。這不僅能建立信心，也能為後續更複雜的專案奠定基礎。

完善的企業治理與跨部門協作機制不可或缺。從群創的「三軸四刻度模型」到旭榮的「坦誠與分享」，成功的企業都建立了明確的流程和溝通機制，確保各部門能夠有效協作。這不僅包括數據治理，也包括如何在不同專業之間建立共同語言，以及如何評估效益並共享成果。

金融業：生成式 AI 加速金融業變革

信任依舊是最大挑戰

在台灣談到 AI 導入，金融業往往是最先被提及的產業。許多人認為這是因為金融業「資源相對充足」，更關鍵的原因在於，金融業受到最嚴格的法律與監管要求，因此在資料管理上相對完整、規範。正因如此，金融業雖具備 AI 發展的優勢，卻同時承擔了更高標準的挑戰。

為深入了解台灣產業 AI 落地的真實困境，人工智慧科技基金會特別舉辦產業論壇，並安排金融專場，邀請 KPMG 安侯建業聯合會計師事務所顧問部副總張智淵、中信銀數位科技處處長王俊權，及台北富邦銀行數位科技研發部協理鄭仁豪，共同探討金融業 AI 落地與部署難題。將 AI 融入營運核心，以確保未來競爭力。

作為國內消費金融業務龍頭，中信銀早在 2016 年便啟動數位轉型，憑藉龐大的客戶基礎與數據優勢，可說是產業轉型的先行者。然而，王俊權坦言，生成式 AI 的崛起徹底改變了遊戲規則，也動搖過往的優勢基礎，讓內部感受到前所未有的壓力。未來的競爭版圖，可能同時存在「霸權」與「平權」兩股現象：大型金控仰賴雄厚資金與資源，或許能率先取得優勢；但靈活的小型金融機構若能善用創新，同樣能快速切入市場、創造破壞式影響。這意味著，AI 的普及正加速推動金融產業迎來翻天覆地的變革。

他進一步指出，回顧數位 1.0 時代，誰能掌握數位化，誰就能展現更佳的經營能力與獲利表現；而進入數位 2.0，也就是 AI 時代，真正的關鍵則在於能否將 AI 深度融入核心能力，才

能確保未來競爭力，不致被市場淘汰。

鄭仁豪也提到，生成式 AI 的應用雖然為金融業帶來助力，但關鍵仍在於與實際場景結合。以富邦銀行與 Costco 聯名卡為例，當時湧入龐大的新客戶量，使得客服中心電話瞬間飆升至尖峰水位，幾乎無法承接。而智能客服在此時成為第一道防線，讓客服的解決率從 30% 一舉提升至 80%，成效相當明顯。

然而，他特別提醒，AI 的效益高度依賴場景，唯有找到正確的應用切入點，AI 才能真正發揮價值。以「千人千面行銷」為例，雖能快速生成不同內容，但在金融業真正的瓶頸，往往不在內容產製，而是法遵審核。少數專員每天必須處理上百封行銷文案，判斷其是否符合規範，效率極為有限。雖然生成式 AI 可以輔助檢視，但最終仍取決於法律見解的一致性，而這是無法單靠 AI 技術就能解決的難題。

實際導入的多重困難：創新與法規平衡

要讓技術真正深入銀行的核心運作，挑戰遠比表面看到的複雜。若從風險管理的角度來看，更能清楚辨識 AI 究竟是推動產業前行的助力，還是潛藏的不確定因素。而在這個過程中，如何妥善權衡多重影響，正是金融業無法迴避的核心課題。

張智淵觀察到，近來金融業的挑戰主要集中幾個面向：人才培育不足、風險控管困難，及導入成本偏高；且隨著金管會相關規範即將上路，中信、富邦、國泰等領頭銀行，皆已積極

與主管機關展開討論，以因應未來的合規需求。

值得注意的是，治理與問責機制仍是金融業的核心挑戰。除了內部組織架構外，調查發現仍有三成以上的金融機構會將 AI 導入工作委外，使得外包廠商也成為治理體系的一環。如何確保隱私與客戶權益、公平競爭、透明性與可解釋性，逐漸成為業界最受關注的議題。尤其在資料利用上，避免個資被目的外使用，以及建立健全的資料刪除與取回機制，已成為必須正視的風險管理重點。

張智淵提到，隨著生成式 AI 的快速發展，產業界開始意識到「資料治理」的重要性正被重新凸顯。過去即便是依靠人工處理，透過共識仍能完成資料定義與應用；然而，AI 的導入迫使企業必須正視資料品質與治理機制。

「生成式 AI 讓我們重新檢視資料的重要性，也讓大家理解未來的 AI 應用若要成功，必須建立在完善的資料治理基礎之上。」他強調，這不僅是企業內部營運的必然要求，更是全球觀點下的共同挑戰。

從國際趨勢來看，資料治理已被視為 AI 發展的核心前提。包括 GPAY 與 OECD 等組織均已強化並合併其治理架構，進一步凸顯「Data Governance」在全球 AI 規範與發展中的關鍵地位。這意味著，企業若要在生成式 AI 時代掌握先機，不僅需要導入 AI 工具，更應同步建立標準化、可信任的資料治理體系，確保技術應用能真正落地並創造價值。

變與不變之間：信任與消費者的期待

王俊權指出，過去十年間，消費者的使用習



相比製造與醫療，金融業在 AI 應用上受到更嚴格的監管限制。從數據使用到產品認證與部署，都有嚴謹且複雜的法遵流程，導入速度相對較為受限。然而，生成式 AI 的出現一方面為金融服務帶來創新契機，另一方面也揭露了該產業在流程、數據治理與人才培育上的瓶頸。金融業在面對新一波技術變革時，既有機遇，也難掩焦慮。

(圖片：人工智慧科技基金會)

慣已大幅數位化，並在此過程中產生並累積了大量數據。當其他行業都在積極導入 AI 以提升服務時，消費者的耐心變得更少、需求更即時，同時也期待被個人化對待，這場「百工百業的革命」正快速改變金融服務的標準。

「每個人都是 VIP，」王俊權直言，過去只有高資產客戶才能享有的專屬服務，如今 AI 讓小額存款的消費者，也能獲得同等的個人化體驗。金融業若能順應這股趨勢，將 AI 轉型真正聚焦於「自主、即時、個人化」，就能滿足新一代消費者的期待，也為自身開創新的競爭優勢。

鄭仁豪也補充，過去金融業往往由不同事業或產品單位分別對應客戶，但如今客戶的期待已經轉變。不僅要有產品，更要有整合性的服務，甚至能感受到量身打造的個人化體驗。這意味著，金融業必須從「銷售角色」轉型為「顧問角色」，才能真正回應客戶需求。

他進一步指出，這種轉變並非金融業獨有，數位平台與搜尋引擎也在積極發展，讓使用者能自主完成理解與任務。對金融業而言，過去以 BU（事業單位）為核心的架構，未來勢必打破藩籬，走向「統一窗口」，以整合方式服務單一客戶，這將成為一項重要挑戰。

他舉例，富邦最新推出的 App 設計理念強調「簡單、直覺、懂我」。這不僅代表功能上的優化，更象徵客戶對金融服務的信任、黏著度與滿意度。最終，AI 導入所帶來的，不只是效率提升，而是金融業建立長期競爭優勢的關鍵。

台灣產業 AI 化的下一步： 基於 AI 治理框架與資料共享機制之前瞻佈局

隨著全球 AI 技術快速演進，生成式 AI 雖持續推動創新，但大語言模型的技術突破已逐漸趨緩。各國開始從「模型競賽」轉向「應用落地」、「信任治理」與「人才韌性」的下一階段。對台灣而言，關鍵問題已不再只是掌握硬體優勢，而是如何在現有基礎上發展出具有本地價值的 AI 应用能力與產業生態。臺灣若要在這波新局中確立戰略地位，必須以結構性調整與精準佈局為核心，AI 不應被視為單一技術項目，而是一套橫跨資料治理、產業轉型與知識體系重構的國家級基礎建設。政策應從算力與模型的部署，轉向資料、制度與應用的整合發展，建立兼具創新與安全的技術治理體系。

一、從「能不能做 AI」到「台灣如何做 AI」

台灣 98% 的企業為中小企業，數位轉型與 AI 導入多仍處於起步階段。企業面臨的主要挑戰，並非技術不可得，而是缺乏清晰的導入路徑與實作方法。對中小企業而言，「可落地的方法論」比單一技術更具價值。唯有透過明確的導入路線圖、跨部門協作機制與可驗證的成效指標，AI 才能從概念走向實踐，真正成為強化流程效率與決策品質的生產力引擎。未來的政策方向應從「技術補助」轉向「體系建構」，從「活動推廣」轉向「能力累積」。政府應協助建構以場域為核心的 AI 平台與知識體系，讓企業能在真實產業環境中學習、驗證並複製成功經驗。製造業可作為起點，逐步形成可擴散、可驗證的導入模式，並透過公私協力建立具資安保障的共用平台，加速邊緣運算與本地化模型的研發，縮短「想做」與「能做」之間的落差。

在技術策略上，台灣的 AI 發展不應侷限單一路線，而應採取大小模型協作互補的策略。大型語言模型（LLM）代表全球技術的成熟基礎，小語言模型（SLM）則是貼近本地產業的應用前線。透過 LLM 的知識支援與技術框架，可高效微調、訓練並部署符合在地需求的 SLM，實現高效能、低延遲與高可信度的 AI 運作。

這些小而精準的模型能服務製造、醫療、營建、物流等垂直場域，利用少量但高品質的在地資料，產生更具即時性與可解釋性的智慧應用。台灣的真正競爭力，不在模型規模，而是能對資料的深度理解與場域智慧的應用能力。

開源模型的崛起正為台灣帶來新契機。它讓企業能參與訓練、自行部署，並結合既有的雲端平台與基礎模型，發揮「聰明運用、在地創造」的優勢。藉此，台灣可在全球技術重構中建立更高的軟體與文化資料主導性，強化自身在國際 AI 生態系中的定位與價值。

二、四大層面強化主權 AI 基礎

AI 的長期競爭力來自創造力與自主性。為確保在全球 AI 競爭中維持主導權，台灣應從四個層面強化主權 AI 的基礎：

自主算力：建構混合型運算架構，整合本地 GPU、雲端與邊緣算力，支援大小模型協作訓練與推論。

自主模型：鼓勵企業與研究機構結合開源 LLM 進行 SLM 微調與在地部署，打造跨領域應

用模型。

創新機制：建立開放的試驗場域與加速器體系，推動新創與產學界共同驗證 AI 創新場景。

政策落實：制定 AI 基本法與資料治理規範，明確風險分類、算力分配與模型標準，以制度確保安全與透明。

同時，應推動資料治理、標準制定與場域實證三大支點，並以「負責任 AI」為發展原則，強化跨部門與國際協作，使台灣 AI 生態系具備可持續發展與全球信任力。

三、治理與法規：以信任為核心的制度設計

在全球 AI 競賽中，治理與規範的創新設計已成為建立長期競爭優勢的關鍵。各國正積極轉變監理角色，從「防弊式管制」走向「促進創新與風險控管並重」的積極治理模式。

歐盟透過《AI 法》建立風險分級制度，強化市場信任與透明度；新加坡以自願性框架與沙盒機制降低新創進入門檻；日本則運用政府採購引導產業標準；韓國與美國更將 AI 視為國家戰略核心，結合立法與投資強化技術主權。

這些路徑雖各有差異，但共同點在於監理不再被視為抑制創新的枷鎖，而是促進產業成熟的推進器。合規能力成為市場準入的門票，也是企業建立信任與品牌聲譽的關鍵資產。在創新治理思維的規範基礎下，企業若能及早將監理要求轉化為競爭優勢，在全球 AI 產業鏈中占

得先機。

台灣長期存在「既抗拒規範、又倚賴法律」的矛盾心態，使得治理在面對快速變化的科技時代，常陷入兩難。未來的 AI 法制建構應走向「輕觸式管制（light-touch regulation）」，以彈性取代僵化，讓創新與治理並行。

但台灣在推動 AI 治理上仍面臨結構性困境。跨部門的責任劃分模糊，績效導向的考核機制壓抑了長期協作，使創新屢受制度掣肘。歐盟的經驗提供了可借鏡的方向：透過多方利害關係人的治理機制，讓政策形成過程本身成為協作平台。這種「對話即治理」的模式，將技術專家、法律學者與社會代表納入政策討論，不僅強化透明性，也累積信任資本。對台灣而言，這樣的機制不只是行政改革，而是一種治理思維的更新。

此外，許多 AI 相關議題，其實已有現行法規可供適用，例如資料使用、隱私保護、智慧財產權、演算法透明度等。企業不必等待「AI 專法」出台，方能展開治理實踐。同時，政府在制定新 AI 法規前，應先盤點現行法規可適用範圍，或可引入 ISO 42001 等國際 AI 風險管理標準，以防止法規碎片化與執行重疊。

真正的關鍵在於如何讓技術運作過程可被審視、可被驗證、也可被修正。AI 治理的最終目標，是在跨領域的框架下維持系統一致性，避免法規割裂與執行落差，建立「可信任 AI」的社會基礎。

四、人才培育：重新定義 AI 人才範疇

推動 AI 的核心不只是技術研發，更在於人。若台灣希望把握 AI 帶來的契機，公部門必須扮演引領者的角色，推動 AI 的廣泛採用，並投資建構活躍且開放的 AI 生態系。政府應積極參與全球 AI 治理框架的制定，確保台灣能在國際規範形成過程中發聲，同時以負責任與可問責的方式發揮 AI 的潛能。

此外，政府更應率先將 AI 深度整合至公共服務與行政流程中，以科技創新提升效率與透明度。並推動涵蓋公務體系、產業勞動者與開發者的全面 AI 能力培育計畫，確保全社會都能為 AI 時代的轉型做好準備。

另一方面，儘管台灣政府近年積極培養 AI 人才，但企業對「AI 人才」的定義仍相當模糊，導致培訓成果難以轉化為實際應用。隨著 AI 技術的快速演進，人才策略必須從短期培訓轉為國家級長期設計，從技術導向轉向整合導向，並兼顧公共利益與產業發展。

AI 人才的培育，不能只侷限於程式與模型開發，而應延伸至商業策略、管理決策、法律倫理與人文社會等跨域能力。未來的 AI 人才必須能理解技術、需求、整合知識，將演算法轉化為具經濟與社會價值的應用。可參考 ISO 30414 及國際 AI 治理標準，建立對齊全球趨勢的「人工基礎建設 (Human Infrastructure)」，以銜接教育、產業與政策。

AI 將逐漸成為新的使用者介面 (AI = UI)。

這意味著人才必須理解垂直產業的運作脈絡、流程邏輯與場域挑戰，才能真正發揮 AI 的應用潛力。從這個角度出發，企業在導入 AI 前，不應急於招募技術人員，而應先釐清問題本質，盤點現有人力與資訊資源，從商業模式出發再逐步延伸至技術整合。當 AI 工具愈來愈容易取得，關鍵已不在於「是否懂 AI」，而在於「如何讓既有人才與 AI 共同成長」。

同時，台灣的人才政策應以國際標準接軌為目標，建立能力評估、認證與報告體系，讓企業與教育體系能在共同語言下協作。AI 的發展不僅是產業升級，更是國家競爭力的再定義。唯有以人為核心、以系統為支撐，才能形成具有信任、韌性與創新精神的 AI 人才生態。

以信任為基礎，構築臺灣的 AI 韌性國力

在全球 AI 競賽中，台灣正處於關鍵轉折點。未來台灣應以「可信任 AI」與「主權 AI」為雙核心，建構明確的國家治理戰略，將半導體與製造優勢轉化為 AI 時代的整體領導力。

「主權 AI」不僅涵蓋在地語言模型的發展，更延伸至自主算力、資料治理、人才培育與創新生態的完整體系。若忽略這一佈局，台灣恐在應用與內容層面過度依賴國際供應鏈。

由於完善的治理機制是產業創新與社會信任的根基。台灣當前亟需建立具包容性與前瞻性的資料治理架構，兼顧創新應用與個資保護，為可信任 AI 的長期發展奠定制度根基。



財團法人人工智慧科技基金會
Artificial Intelligence Foundation