著作權聲明公告

本活動資料(包括但不限文字、圖片、影音等講義內容或其他文件)之著作權歸屬於**「財團法人資訊工業策進會產業情報研究所(MIC)」**所有，均受著作權法之保護及國際著作權法律的保障，僅授權報名本活動之個人非商業用途，並請註明引用出處及來源。

謹提醒，倘個人未取得書面授權同意，逕自透過電子郵件或LINE等媒體媒介轉載分享本活動資料，已經侵犯MIC的智慧財產權，將視情節之重大程度提出法律追訴，如經確認違法行為，不僅個人受罰，公司亦將負連帶賠償責任，並造成公司商譽之損害。

感謝您對於智慧財產權尊重與理解，如有意請求授權使用本活動資料，歡迎聯繫02-2378-2306；members@iii.org.tw，謝謝您！

主權AI時代下的發展趨勢與因應策略

高雅玲
產業顧問兼主任
產業情報研究所(MIC)
財團法人資訊工業策進會

2026/08/27

簡報大綱

- 國際主權AI發展背景與推動趨勢
- 企業資料主權與治理的需求與挑戰
- 機構實際案例與新興治理方案
- 結論

國際主權AI發展背景與推動趨勢

從算力擴散至全堆疊：AI主權升格為國家戰略

- AI發展不再只是技術與模型的選擇，也涉及經濟競爭力、國家安全及關鍵能力的自主控制

經濟與文化韌性考量

以在地資料與模型強化自主

- 主流模型對非英語語言與在地文化的涵蓋仍有差異，促使各國投入在地資料、語言模型與自主 AI 能力
- 美國曾限制 Anthropic 特定模型供應，OpenAI 模型測試亦發生突破隔離環境的資安事件，凸顯模型供應中斷與安全治理風險

地緣政治壓力

美中地緣博弈，主導權競奪

- 美中晶片與算力管制持續升級，全球 AI 供應鏈呈現陣營化與區域化趨勢
- 競爭焦點已從硬體擴及模型、標準與資料治理，全球南方國家成為各方拓展技術與治理影響力的重要場域

技術自主需求

模型、資料、算力等多管齊下

- 新加坡、臺灣、日本、韓國、印度及歐洲多國，均投入在地資料、語言模型或自主 AI 能力建設
- 跨境資料調取、AI 法規遵循及供應商依賴等問題，促使各國重新檢視資料治理、算力配置與人才能力

資料來源：各國公開新聞，MIC整理，2026年8月

何謂主權AI？

主權AI
(Sovereign AI)

主權 AI 是指國家、區域或企業在資料、模型、算力與治理等關鍵環節，保有自主選擇、控制、驗證及必要時替換的能力，並依自身需求維護安全、合規與核心利益

管理依賴

自主決策

世界經濟論壇

「主權AI是**國家**依據本地政策與國家AI戰略，利用本土人才構建AI能力，並能根據當地需求調整AI以維護價值觀與監管監督」（2024）

「AI主權應被重新理解為**「策略性相互依存」**：在**關鍵領域保有控制力**與韌性，同時透過可信賴的國際合作取得其他能力」（2026）

NVIDIA執行長黃仁勳

「每個區域、每個**國家**都需要建立自己的主權 AI」（2023）

「主權AI視為**國家級**的「資料 – 硬體 – 模型」**自主能力**，強調每個國家都應具備本地化AI基礎設施，以維護經濟安全與技術獨立」（2024）

「發展並持續完善自己的 AI，使**國家**智慧成為本國生態系的一部分」（2025）

McKinsey

「一個**國家或區域**發展並控制關鍵AI能力，藉此在其經濟、政治與社會脈絡下，取得更大的技術選擇空間與自主性的能力」（2025）

「**國家或組織**運用自身基礎設施、資料、模型與人才，獨立發展、部署及治理 AI，並保有對整個AI**生命週期控制的能力**」（2026）

資料來源：WEF、NVIDIA、McKinsey，MIC整理，2026年8月

四大主權支柱：自主控制能力與外部依賴風險並重

戰術層次 外部依賴風險｜評估依賴對象、集中程度、替代方案與供應中斷影響

資料主權	模型主權	算力主權	治理主權
• 資料來源與儲存地集中度 • 備援與可移轉性	• 授權條款變動風險 • 模型可替代性、轉換成本	• 晶片／雲端供應商集中度 • 地緣政治與供應中斷曝險	• 委外依賴程度 • 服務水準協議（Service Level Agreement, SLA）與多供應商備援機制

戰略層次 自主控制能力｜評估即使採用外部服務，企業是否仍掌握決策、驗證、執行與替換能力

資料主權	模型主權	算力主權	治理主權
• 資料的存取、使用與稽核權由誰掌握？ • 資料是否涉及跨境調閱、移轉或其他管轄風險？	• 模型行為可否被驗證？ • 模型輸出、使用依據與決策過程是否可驗證、可追溯？	• 斷鏈情境下能否維持最低限度運作？ • 算力調度與優先順序，是否操之在己？	• 危機時刻誰能即時做出並執行關鍵決策？ • 關鍵治理權責是否掌握於組織內，並可即時執行？

資料來源：各機構研究，MIC整理，2026年8月

主要經濟體加強 AI 自主能力，但政策路徑與優先重點各異

- 各主要經濟體依據自身產業條件與安全需求，分別透過法規治理、算力投資、模型發展及國際合作，強化 AI 自主能力

美國｜創新優先，安全同步補強

政策：AI出口計畫、創世紀任務

推動 AI 技術體系輸出與科研應用，同步強化先進模型的安全評估及出口管理

關鍵議題：AI監管、AI出口

歐盟｜可信治理，驅動產業採用

政策：歐洲AI大陸行動計畫、AI法規簡化套案（AI Omnibus）

建置AI工廠強化算力自主，簡化法規遵循時程，鞏固雲主權與競爭力

關鍵議題：雲主權、法規簡化

中國｜前瞻研究，加速商用滲透

政策：十五五規劃、數據要素x

推動AI於製造、能源、醫療等領域規模化商用，同步布局AI外交與資料產業影響力

關鍵議題：AI外交、資料產業

日本｜主權AI、實體AI並進

政策：人工智慧基本計畫、產業資料空間

日本靈活調整國家AI戰略，轉向主權AI、實體AI、資訊安全等布局

關鍵議題：主權AI 、實體AI、資料空間

韓國｜鎖定半導體，加強AI投資

政策：三大超級專案、AI行動計畫

以主權 AI 推動資訊服務與軟體產業發展、拓展海外市場，並積極發展 AI 代理人應用

關鍵議題：主權AI、AI Agent

新加坡｜國際合作，打造亞太AI樞紐

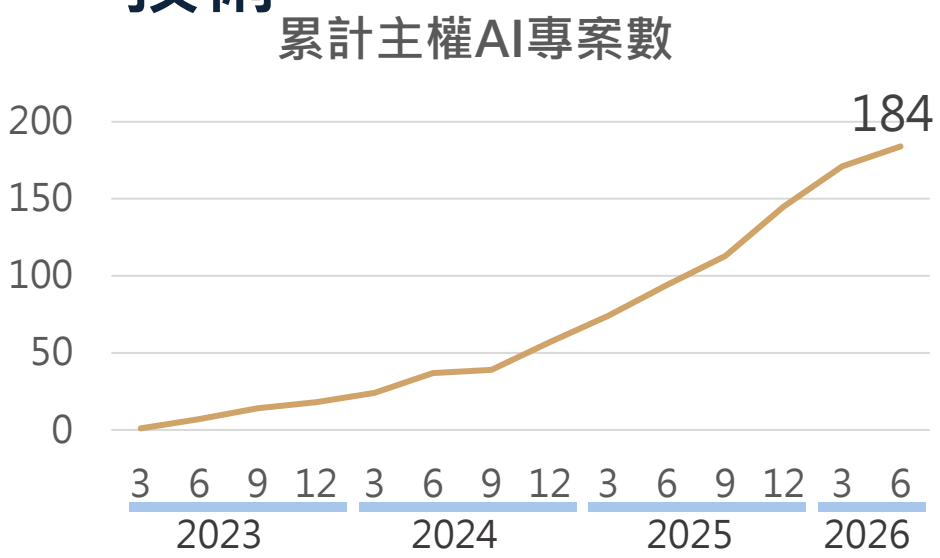
政策：國家AI戰略2.0、企業算力計畫

透過擴大AI應用與人才培育，結合國際合作，打造亞太AI樞紐地位

關鍵議題：AI Hub、數位人才

資料來源：各國政府網站，MIC整理，2026年8月

主權 AI 投資持續增加，但仍以基礎設施為主並高度依賴外部技術



59%
基礎設施（算力資料中心、GPU等）

63% 主權 AI 專案有外國企業參與，其中逾八成涉及美國企業

- 主權 AI 的本質不是追求 100% 國產化或完全去美化，而是掌握「實質控制權」 與「備援切換能力」

資料來源：Center for a New American Security（2026/8/18更新），MIC整理，2026年8月

趨勢方向轉變

1 「算力投資」外溢到「全堆疊」

主權AI最早集中在算力軍備競賽（搶建資料中心、搶GPU），儘管基礎設施仍占主要投資比重，政策布局也逐步涵蓋模型、資料、應用及人才（如：法德與Mistral AI、SAP合建主權AI公部門方案）

2 「全面自主」轉向「選擇性主權」

多數國家不再追求全面自建，轉為依比較優勢聚焦特定環節，並管理對外依賴（如：新加坡聚焦東南亞語言模型、韓國聚焦半導體算力）

3 「資料在地化」延伸至「資料治理」

資料主權的焦點從「存放地點」轉向「蒐集、使用、跨境、投入模型」的治理權責（如：歐盟資料聯盟策略）

4 「國家政策」延伸至「企業經營議題」

企業對少數雲端、模型與Agent平台的依賴，使主權AI從國安議題延伸為企業經營問題（如：模型出口受限、模型逸出可控範圍事件）

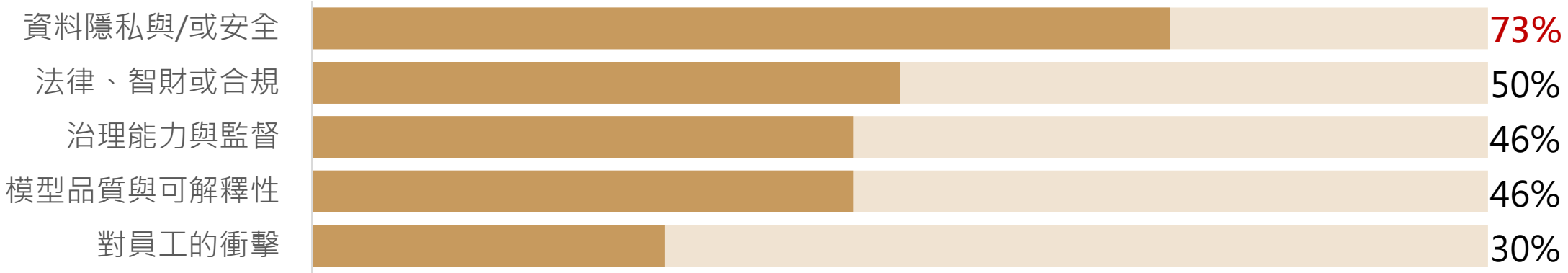
資料來源：各機構，MIC，2026年8月

企業資料主權與治理的需求與挑戰

資料隱私與安全是企業首要 AI 風險，資料主權需求同步升高

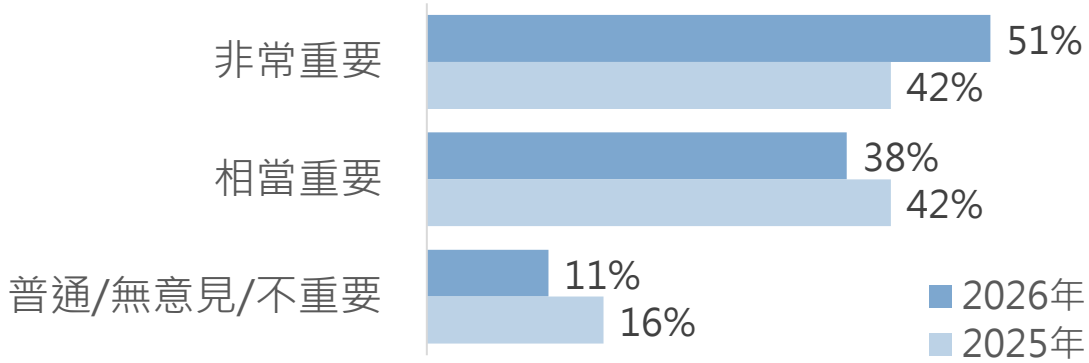
- 73% 受訪企業將資料隱私與安全列為主要 AI 風險；認為資料主權非常重要的企業比例由 42% 升至 51%，法規要求、政治情勢與資安事件均推升治理需求

企業最擔憂的AI工具/應用風險——資料議題居首



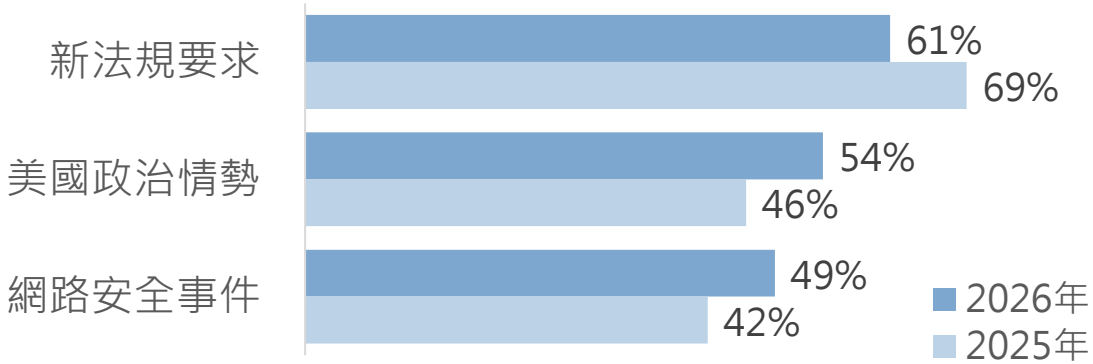
資料來源：Deloitte，MIC整理，2026年8月

資料主權重視程度：非常重要比例升至51%



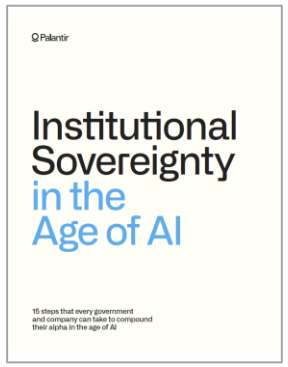
資料來源：Business Application Research Center，MIC整理，2026年8月

資料主權外部驅動力：法規居首



資料來源：Business Application Research Center，MIC整理，2026年8月

企業可從基礎治理與模型管理建立自主控制能力（1/2）



發布日期 | 2026年7月7日

- Palantir 於 2026 年 7 月發布《Institutional Sovereignty in the Age of AI》，提出涵蓋基礎、模型、算力與控制層的 15 項關鍵行動
  - 核心問題：如何讓 AI 使用所產生的知識與價值持續累積於機構自身
  - 關鍵在於：不應只追求模型能力與Token用量，也須掌握資料、知識與技術決策權
  - 贏家定義：非最先取得最強模型者，而是能保有知識所有權、維持技術可替換性、並建立「每次AI互動都強化機構自身」機制的組織

基礎層 Foundations	1.確保零資料留存（ZDR）	確保Prompt與Log不被供應商留存或拿去訓練模型	自主能力建構
	2.建立AI決策樹	依資料敏感度、任務需求及控制要求，決定適用的模型與部署環境	
	3.辨識架構中依賴與改善的機會	檢視資料、模型、算力與控制環節，辨識供應商依賴及替換限制	依賴風險管控
模型層 Model Layer	4.防範供應商與企業利益不一致	檢視服務條款、資料使用方式及商業模式，避免企業知識被供應商不當利用	
	5.保留模型選擇與替換彈性	架構彈性化，隨時能無縫更換成本效益較佳的大型模型，降低供應商切換難度與轉換成本	自主能力建構
	6.掌控模型飛輪	掌握模型調校、測試資料及使用回饋所形成的機構知識與價值	

備註：零資料留存（Zero Data Retention, ZDR），廠商承諾不留存使用者提示與對話紀錄的機制
資料來源：Palantir，MIC整理，2026年8月

企業可從基礎治理與模型管理建立自主控制能力 (2/2)

算力層 Compute Layer	7.依安全信任選定運算環境	依資料敏感度與業務風險，選擇具備適當安全保證的硬體與運算環境	依賴風險管控
	8.依敏感工作流程決定算力	針對高敏感資料與關鍵任務，採用自有、專用或具備充分控制能力的算力環境	自主能力建構
	9.驗證外部算力	對租用的雲端算力實施加密、遙測、加密與驗證機制	依賴風險管控
控制層 Control Layer	10.避免綁定單一模型	分離業務邏輯與模型，使大型語言模型成為可替換的技術元件	自主能力建構
	11.落實細緻的權限控管	依使用者身分、代理人角色及任務目的，控管資料存取與行動權限	依賴風險管控
	12.建立可稽核與可追溯的紀錄	依風險及合規需求，完整記錄每一次Prompt、AI決策與人工干預歷程	
	13.採取適應性資安防護	持續偵測與防範提示注入、資料外洩、權限濫用及介面漏洞	
	14.建立分支測試與回復機制	建立安全沙盒，透過隔離測試、中止與回復機制，確保AI行動可驗證、可撤銷	
	15.掌握企業知識與情境脈絡	將企業資料、業務規則、決策經驗與工作流程持續累積為機構專屬知識	自主能力建構

資料來源：Palantir ，MIC整理，2026年8月

四大主權支柱：核心風險、治理需求與控制能力

外部依賴與供應商風險

資料與企業知識

模型與基礎設施

內部控制與營運風險

❶資料主權

核心問題：敏感資料、提示內容與使用回饋遭供應商留存或再利用，導致企業知識與控制權外移

需求痛點：
- 資料去向不透明
- 專業知識被供應商吸收

關鍵行動：
① 零資料留存
② 建立AI決策樹
⑥ 掌握模型飛輪
⑮ 掌握情境飛輪

掌握控制權：掌握資料使用邊界、存取權限與知識歸屬

❷模型主權

核心問題：供應商片面改變價格、政策或條款時，企業無法快速替換模型

需求痛點：
- 服務中斷影響營運
- 無法快速換用更適合的模型

關鍵行動
④ 防範利益衝突
⑤ 保有模型流動性
⑩ 不綁定特定模型

掌握控制權：掌握模型選擇、替換與供應商退出能力

❸治理主權

核心問題：AI代理人可能取得過大權限、執行不當行動，且難以追溯、回復或究責

需求痛點：
- AI決策過程無法追蹤
- 錯誤行動無法復原

關鍵行動：
③ 找出架構中的機會
⑪ 落實細緻的權限控管
⑫ 完整稽核與記錄
⑬ 採取適應性資安防護
⑭ 採用分支測試

掌握控制權：掌握 AI 行動授權、人工監督與決策究責

❹算力主權

核心問題：雲端主機、GPU、供應鏈不在企業掌握之內

需求痛點：
- 不知資料實際在哪運算
- 無法驗證雲端業者是否能查看資料

關鍵行動：
⑦ 依安全性選擇硬體
⑧ 依敏感流程決定算力
⑨ 驗證外部算力

掌握控制權：掌握算力配置、服務備援與運算環境驗證

資料來源：MIC，2026年8月

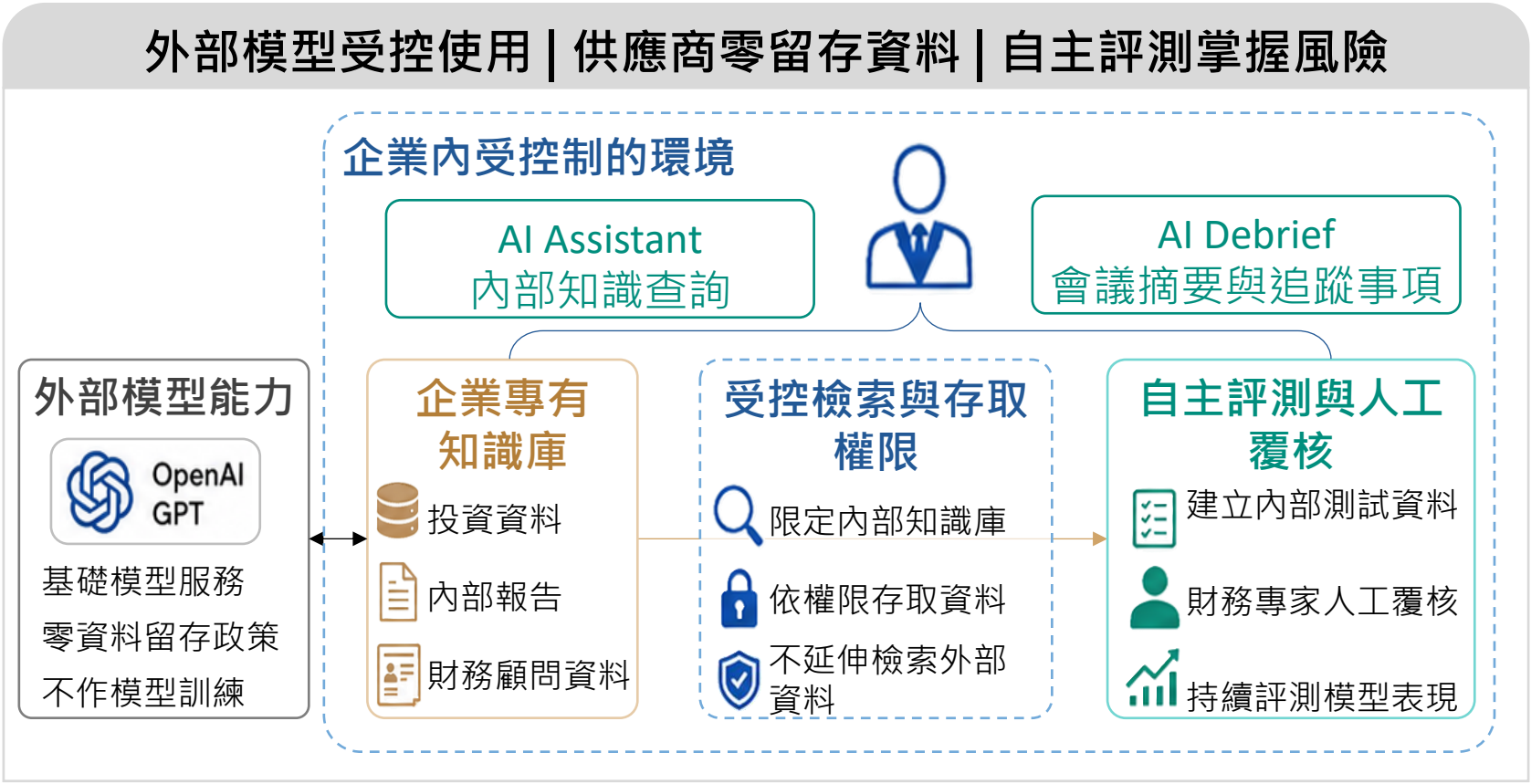
機構實踐案例與新興治理方案

五個案例：企業主權治理已由資料控制延伸至 AI代理人

順序	案例	探討議題	資料主權與治理重點
1	Morgan Stanley	使用外部 AI 模型，如何維持企業資料與輸出品質的控制？	專有資料使用限制、內部知識檢索與模型評測
2	Swift	不集中原始交易資料，金融機構如何共同偵防詐欺？	原始資料留在各銀行，透過聯邦式學習進行跨機構協作
3	Thomson Reuters	採用多種外部模型時，企業如何保留核心知識與模型選擇權？	掌握專有知識、資料邊界、驗證標準與工作流程
4	NIH All of US	面對高度敏感健康資料，如何兼顧研究使用與資料管控？	敏感資料的使用條件、存取管理與研究治理
5	NTT DATA	AI代理人跨系統執行任務時，企業如何避免越權與失控？	行動前檢核、權限限制、人工覆核及完整追溯

備註：美國國家衛生研究院（National Institutes of Health, NIH）
資料來源：MIC，2026年8月

案例一：Morgan Stanley以零資料留存與自主評測，降低外部模型使用風險



資料來源：Morgan Stanley、OpenAI，MIC整理，2026年8月

產業別 金融服務 / 財富管理

Morgan Stanley採用外部基礎模型，透過零資料留存機制（①），避免專有資訊被模型供應商留存或用於訓練；同時將內部知識、客戶互動與專業經驗持續累積於自身系統（⑮）

財務顧問及專業團隊另以自主測試資料、持續評測與人工覆核，檢視模型回覆的準確性及合規性，建立可查核的品質管理機制（⑫）

關鍵行動

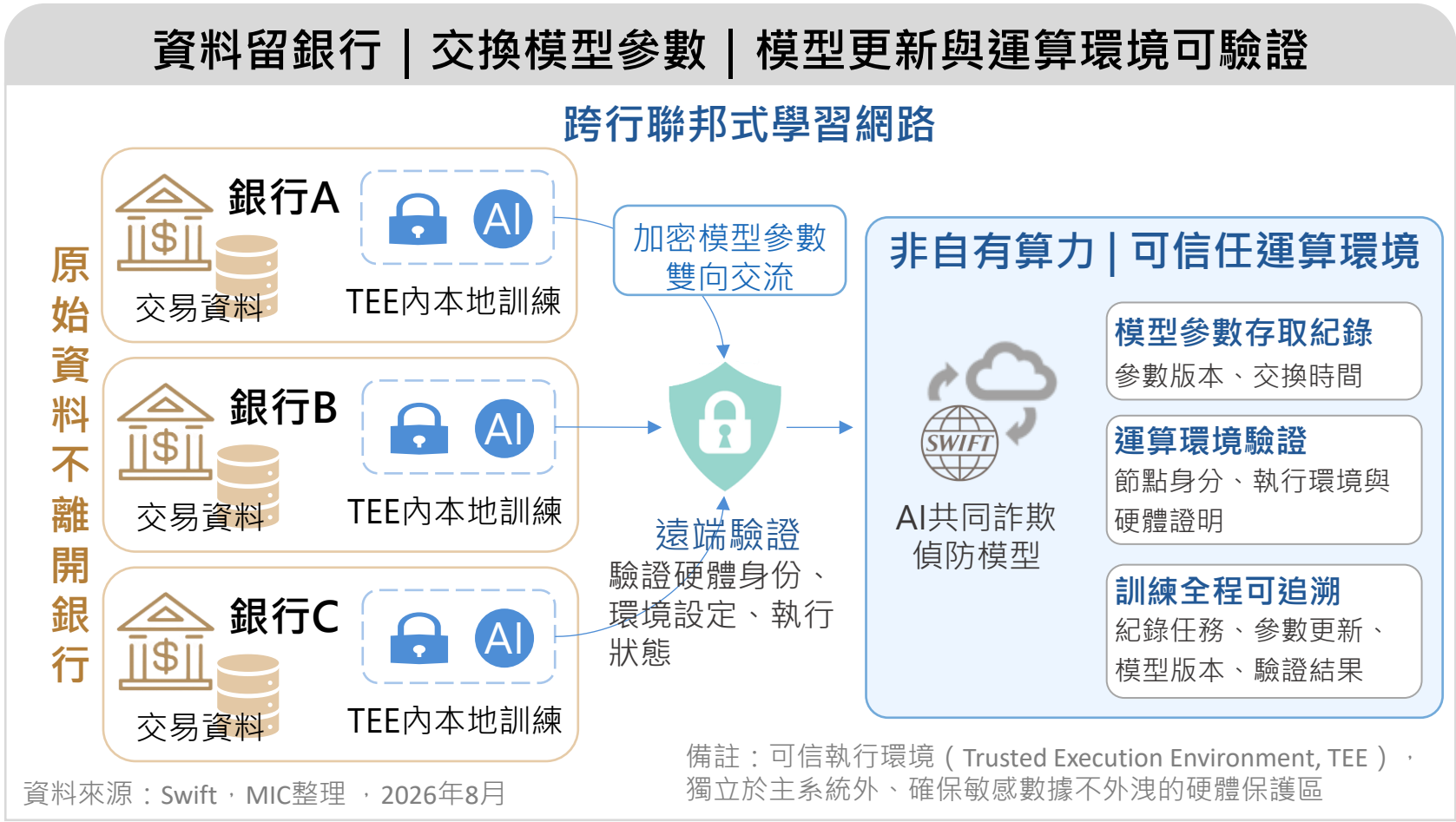
① 確保零資料留存

⑫ 建立完整的稽核與紀錄

⑮ 掌控情境飛輪

- 企業使用外部模型時，可透過供應商零留存、用途限制與受控檢索，降低專有資料遭留存或再利用的風險
- 企業可建立自主測試、持續評測與人工覆核機制，掌握模型輸出品質及使用風險

案例二：Swift以聯邦式學習，讓銀行在不集中原始資料下協作偵防詐欺



產業別　跨境金融 / 支付

Swift採用聯邦式學習架構，讓各銀行依資料敏感度選擇適合的運算環境（⑧），並在具備可信任執行環境的設備上處理原始交易資料（⑦），無須集中資料即可共同訓練異常交易偵測模型

各銀行僅交換必要的模型更新資訊，並透過硬體證明及遠端驗證確認外部運算環境的可信度（⑨）；資料互動與協作過程則納入稽核及紀錄管理（⑫），兼顧資料控制與跨機構合作

關鍵行動

⑦ 依安全信任選定硬體

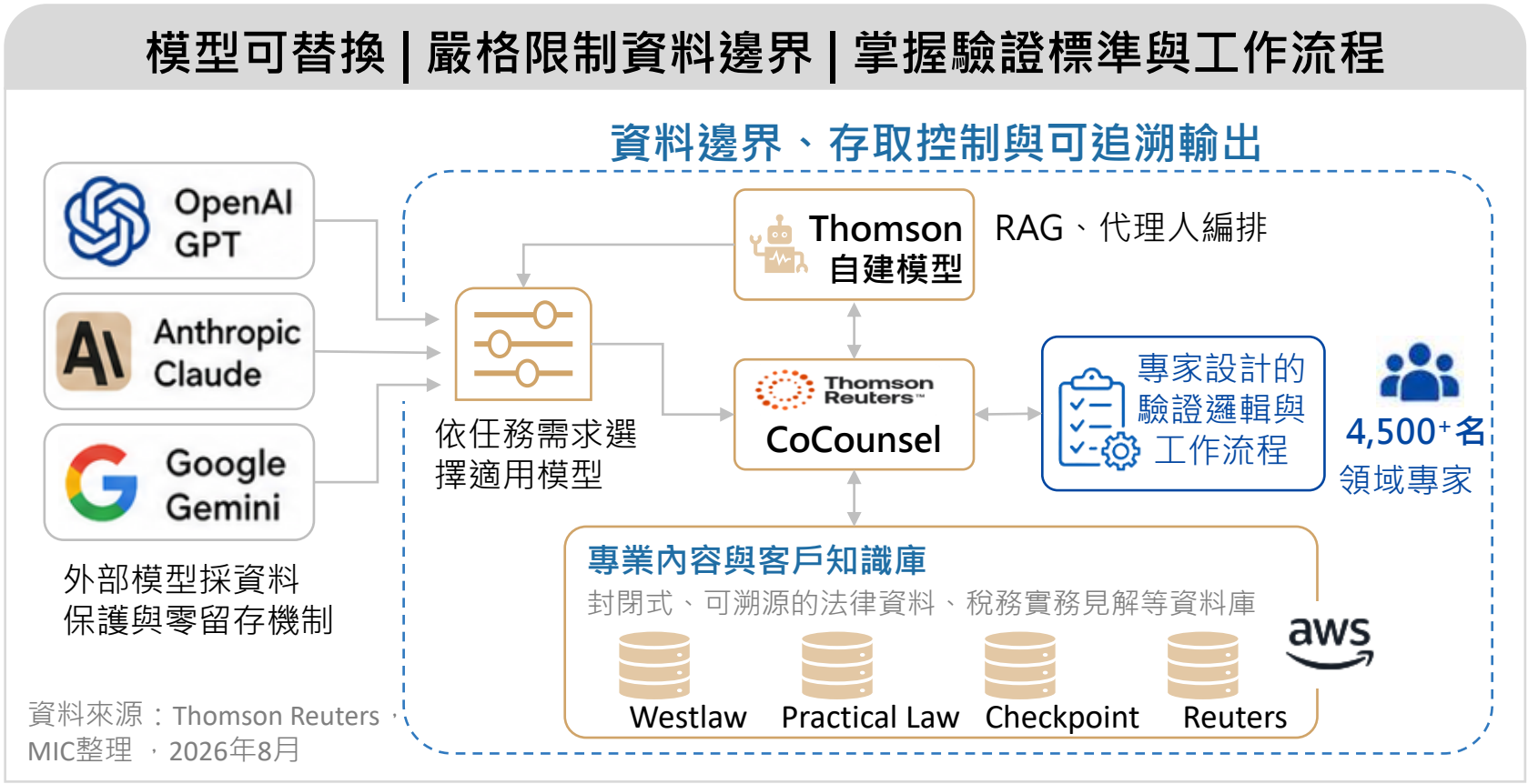
⑧ 依敏感工作流程決定算力

⑨ 驗證外部算力

⑫ 建立完整的稽核與紀錄

- 企業間協作不必集中敏感資料，讓資料留在自身環境、只交換必要的加密參數，即可提升資料主權
- 企業可透過可信執行環境與硬體證明，驗證外部算力的安全性，提升運算環境的可控性

案例三：Thomson Reuters 以自有專業模型與多模型架構，保留模型選擇權



備註：檢索增強生成（Retrieval-Augmented Generation, RAG），讓 AI 先查詢企業內部專屬資料庫再回答的技術

產業別 專業資訊服務 / 法律、稅務、法遵科技

Thomson Reuters透過零資料留存及供應商資料使用限制（①④），避免客戶資訊與專業知識被外部模型不當利用；同時採用多模型架構與自有專業模型，保留模型選擇及替換彈性，降低單一供應商依賴（⑤⑩）

公司結合自有法律模型、領域專家回饋及模型優化能力（⑥），並持續掌握法律、稅務資料、驗證標準與專業工作流程，使模型改進與業務知識均累積於企業自身（⑮）

關鍵行動

① 確保零資料留存
⑥ 掌控模型飛輪
④ 防範利益衝突
⑩ 不綁定特定模型
⑤ 保有模型流動性
⑮ 掌控情境飛輪

- 企業採用多模型並存架構、保留模型選擇與替換彈性，可降低單一供應商依賴，藉此提升模型主權
- 企業掌握專業內容與驗證標準、持續累積於自身知識庫，確保知識不因換模型而流失，藉此提升資料主權

案例四：NIH All of US將敏感健康資料與衍生模型限制於受控研究環境

資料來源：NIH All of Us Research Program，MIC整理，2026年8月

產業別 醫學研究 / 精準醫療

NIH All of US透過身分驗證、分級授權及受控研究工作區，依研究者資格與資料敏感度限制存取範圍（⑪）；參與者個人層級資料及以其訓練的模型，均不得移出既有研究環境

研究活動及資料存取過程均可留存紀錄並接受稽核（⑫），另透過資料流出警示與異常監測辨識未經授權的外部傳輸（⑬），兼顧敏感健康資料的研究使用與安全治理

關鍵行動

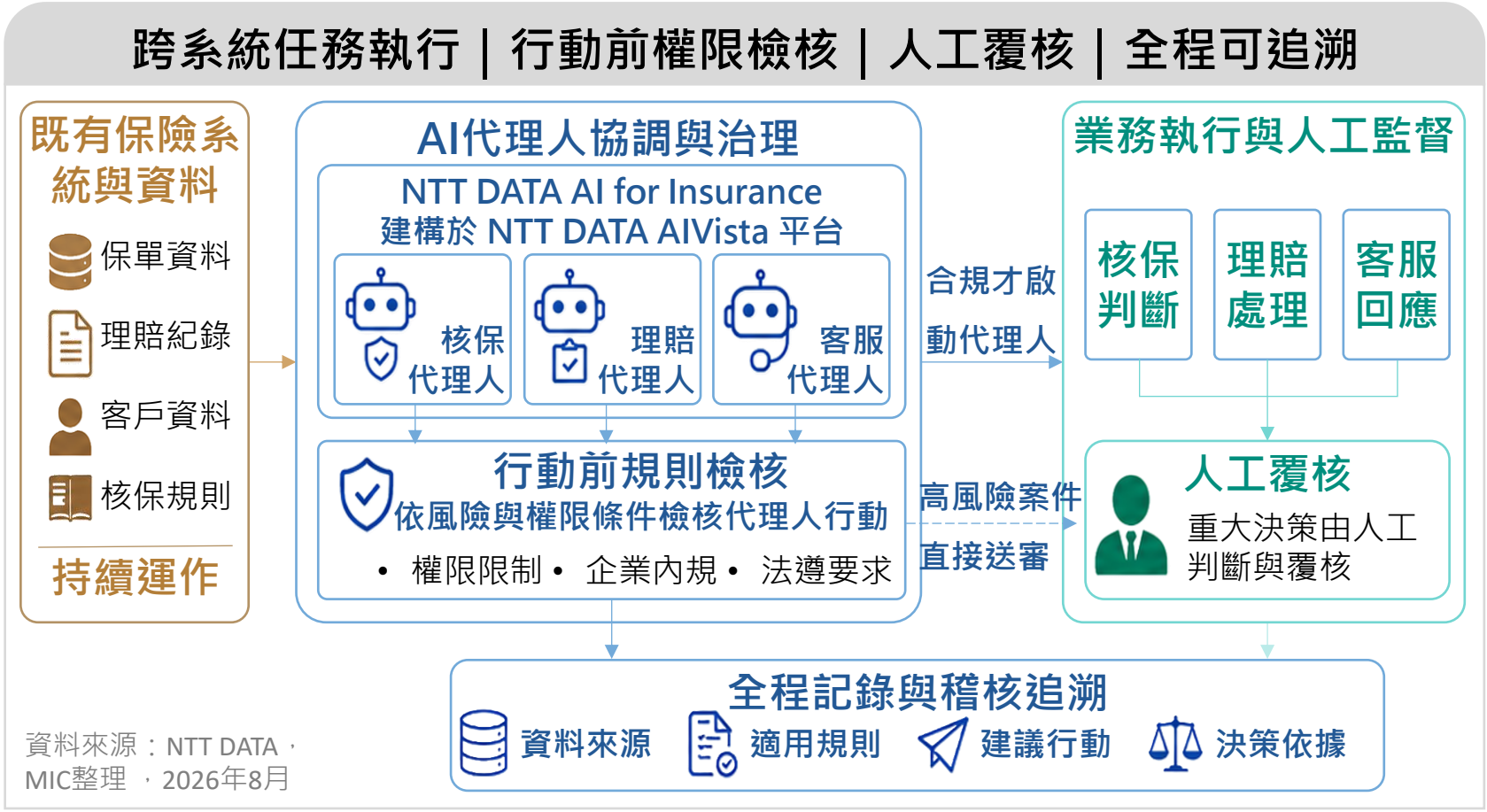
⑪ 落實縝密的權限控管

⑫ 建立完整的稽核與紀錄

⑬ 採取適應性資安防護

- 企業可借鏡此模式，依資料分級授權與受控工作區的方式，限制敏感資料的使用邊界，藉此提升資料主權
- 對於高度敏感資料，治理範圍應延伸至運算環境及以個人資料訓練的模型，避免未經授權的移轉或匯出

案例五：NTT DATA以代理人治理架構，強化保險流程控制與人工監督



產業別 保險服務

NTT DATA的AI for Insurance方案，將代理人導入核保、理賠及客戶服務等業務流程，並依角色、任務及資料敏感度設定存取與行動權限（⑪），避免代理人在跨系統執行作業時逾越授權範圍

方案透過即時紀錄、人工覆核與決策追溯建立治理依據（⑫），並結合異常監測及提示攻擊防護（⑬）；針對高風險或異常行動，另可設計中止與回復機制（⑭），降低自動化決策失控的風險

關鍵行動

⑪ 落實縝密的權限控管

⑫ 建立完整的稽核與紀錄

⑬ 採取適應性資安防護

⑭ 建立分支測試與回復機制

- 企業導入 AI 代理人時，應依任務風險建立權限控管、行動規則與人工覆核機制
- 企業應保留必要的資料存取與決策紀錄，使高風險行動可追溯、可監督及可究責

主權 AI 的核心是保有選擇、驗證與退出能力

四大主權支柱矩陣

資料、模型、算力、治理 —
核心問題、需求痛點、掌握控制權路徑

15項關鍵行動

Palantir機構主權框架 —
基礎層、模型層、算力層、控制層

5個企業實踐案例

Morgan Stanley、Swift、Thomson Reuters、
NIH All of Us、 NTT DATA

資料來源：MIC ，2026年8月

- 主權AI的核心精神，在於管理依賴，而非消除依賴
- 主權 AI 已由國家政策延伸至企業經營，治理能力與外部依賴管理的重要性持續提高
- 企業可從資料、模型、算力與治理四項能力出發，依業務風險選擇適合的治理行動
- 企業可依自身優先順序，彈性組合治理做法逐步掌握控制權—不是單一支柱的選擇題，而是四支柱動態搭配的治理課題

結論

保持策略彈性：建構數位自主權、韌性與適應力

- **企業推動主權 AI，不必排除外部技術合作，也不需要追求所有環節全面自建；重點在於掌握關鍵資料、技術選擇與治理決策**
- **企業應掌握供應商依賴程度，依業務風險建立分級治理與可替換架構，並持續檢視異常事件及供應中斷的應變能力**

01 盤點依賴 Map Dependencies

盤點目前使用的模型、雲端、算力供應商之國別分布與集中度（關鍵行動③、⑦、⑨），釐清資料流向、管轄風險、替代方案與服務中斷影響

02 分級治理 Tier Governance

依風險與敏感度分層（關鍵行動①、②、⑦、⑧），如：非核心應用可持續使用外部通用模型並採零資料留存為防護；涉及核心競爭力或高敏感資料者，應評估自建、私有化部署，或建立可切換供應商的混合架構

03 設計即主權 Sovereign-by-Design

將自主權、韌性與適應力從設計之初即內建於架構（關鍵行動①、③、⑤、⑥、⑩、⑮），採模組化、可互操作平台設計，使模型與雲端服務能順暢切換，並確保微調回饋與營運經驗的價值留在企業內部，降低供應商鎖定風險

04 建立治理 Governance

推動跨部門治理委員會（關鍵行動④、⑨、⑪、⑫、⑬、⑭），明確界定法務、資安、資訊與業務單位的權責，明確風險升級路徑與決策權責，並針對供應中斷情境預先沙盤推演

資料來源：MIC，2026年8月

Thank you.

Your Gateway to Strategic Insights

高雅玲　產業顧問兼主任

ylkao@iii.org.tw

產業情報研究所

智慧財產權暨引用聲明

- 本活動所提供之講義內容或其他文件資料，均受著作權法之保護，非經資策會或其他相關權利人之事前書面同意，任何人不得以任何形式為重製、轉載、傳輸或其他任何商業用途之行為
- 本講義內容所引用之各公司名稱、商標與產品示意照片之所有權皆屬各公司所有
- 本講義全部或部分內容為資策會產業情報研究所整理及分析所得，由於產業變動快速，資策會並不保證本活動所使用之研究方法及研究成果於未來或其他狀況下仍具備正確性與完整性，請台端於引用時，務必注意發布日期、立論之假設及當時情境