主權AI視角下看我國產業機會與挑戰

韓揚銘
產業顧問兼副主任
產業情報研究所
財團法人資訊工業策進會
2025.04.09

簡報大綱

- 主權AI定義與發展現況
- 主權AI三要素分析暨建議
- 結論

主權AI定義與發展現況

國家需要掌握AI自主與自決的權力

主權AI
Sovereign AI

一個國家掌握AI自主與自決的權力

利用本國公民的資料和本土語言，在國內自主研發人工智慧，打造一個與國家文化和價值觀相契合的AI模型

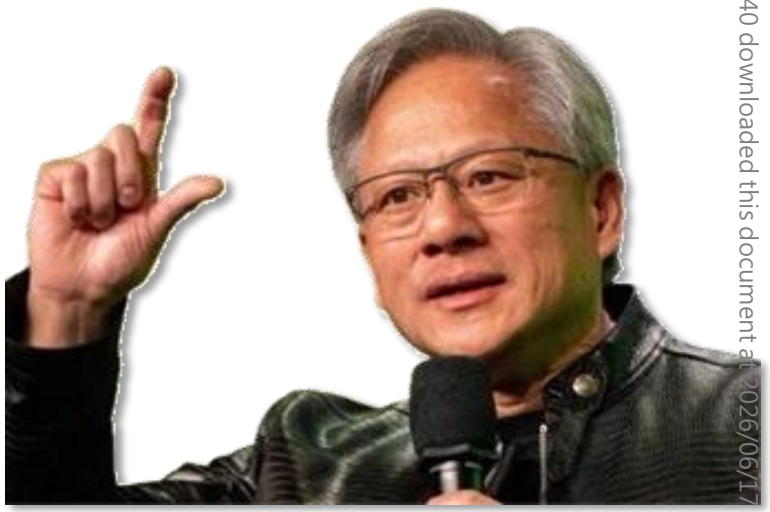
WORLD ECONOMIC FORUM

WEF指出，主權AI的本質是策略性使用AI來強化國家保護和促進利益的能力，減少對外國AI技術的依賴，從而強化自主性。

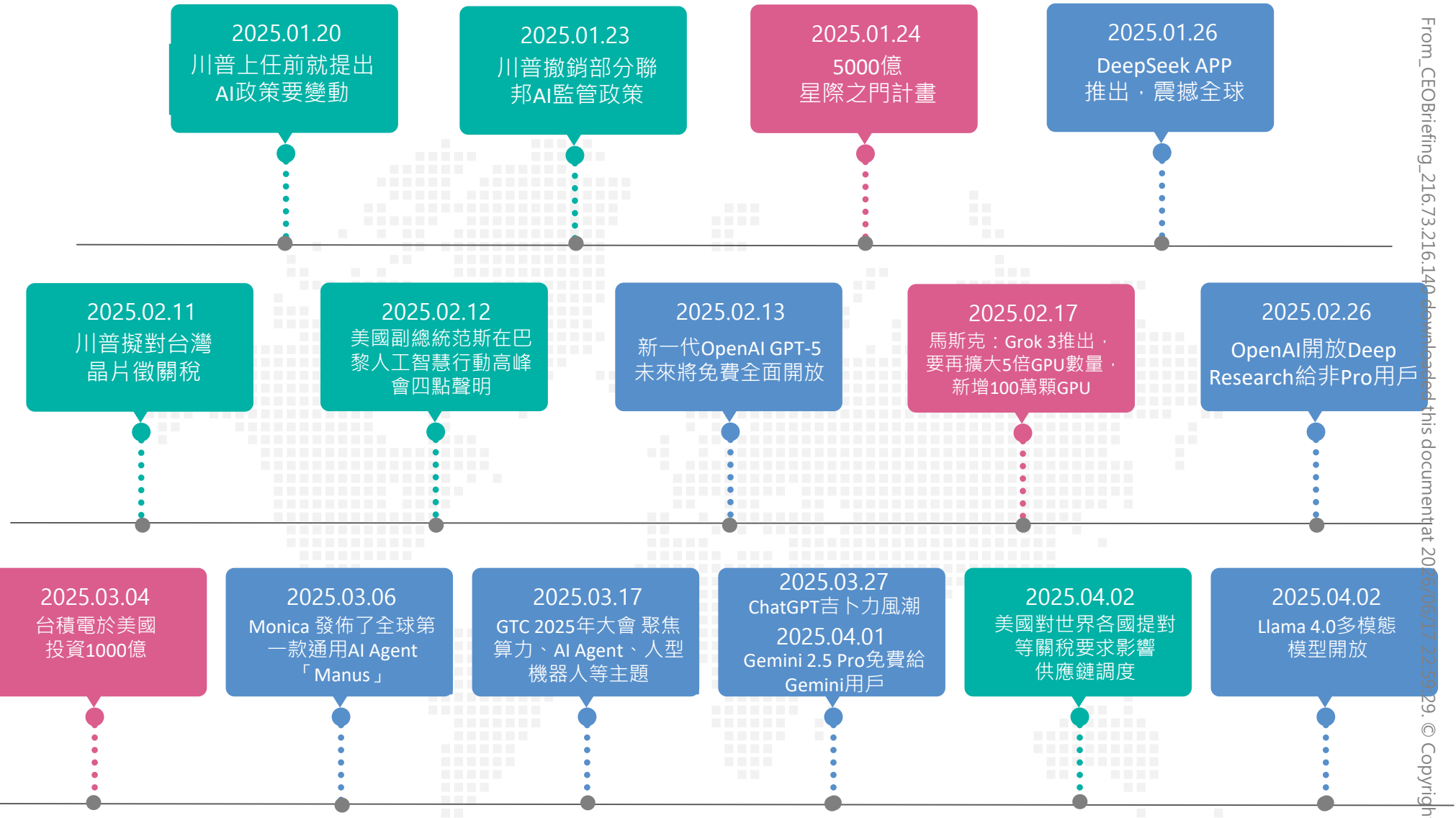
NVIDIA執行長黃仁勳

強調主權AI，各國需擁有自己的AI基礎設施，在享受AI發揮經濟潛力同時，保護自己的文化

發言場合-WGS 2025論壇



2025年1月至4月主權AI重點事件



資料來源：MIC整理，2025年4月

常見國際主權AI政策構面

美國
美國人工智慧倡議

歐盟
人工智慧法案

中國大陸
新一代人工智能發展規劃

印度
印度AI任務

法國
AI產業政策

新加坡
國家人工智慧政府計畫

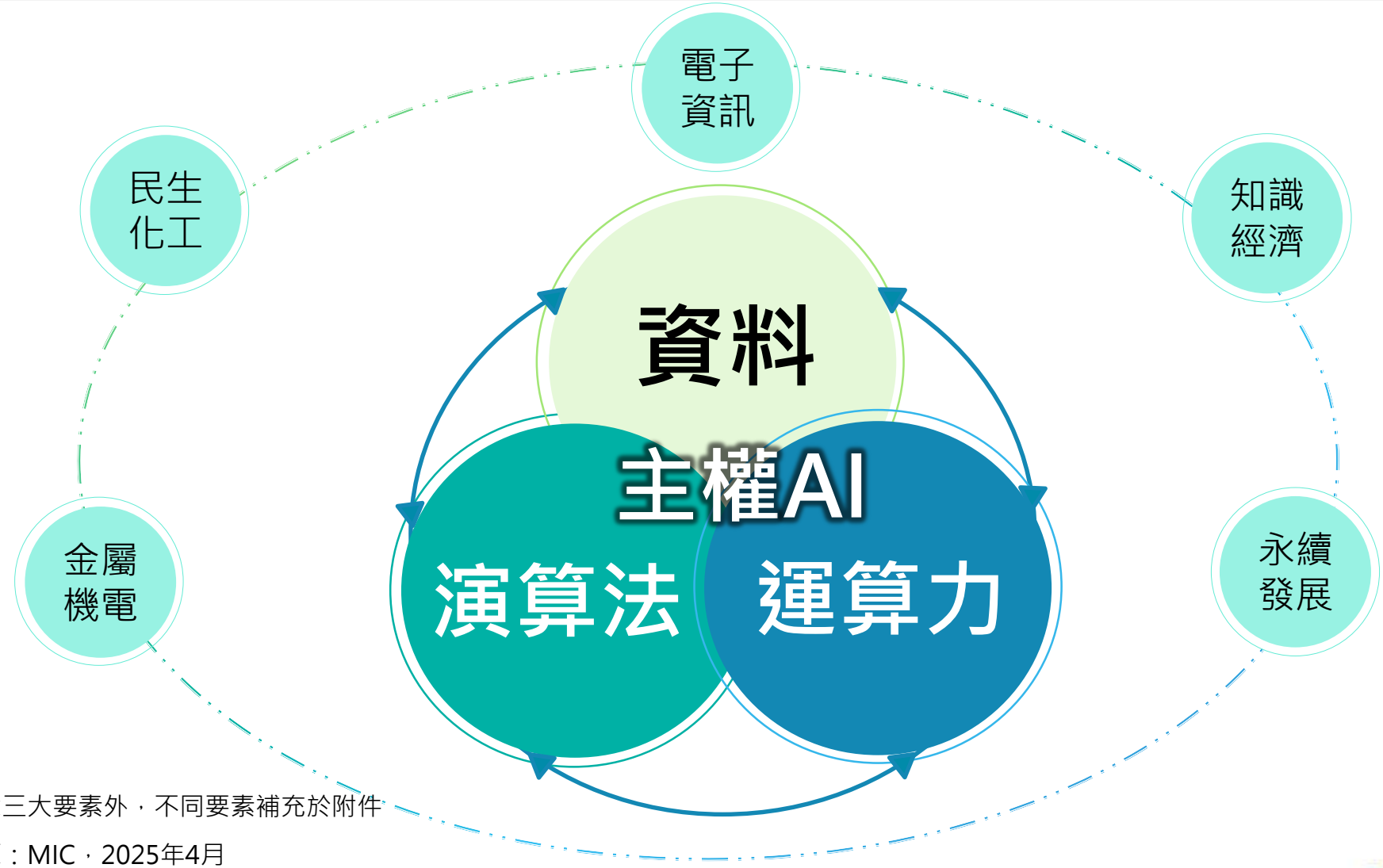
韓國
AI半導體產業發展戰略

加拿大
泛加拿大人工智慧戰略

資料來源：MIC整理，2025年4月

主權AI主要三大要素

主權AI由一國獨有的資料、演算法、運算力三大要素建構而成



備註：除三大要素外，不同要素補充於附件

資料來源：MIC，2025年4月

主權AI三要素分析暨建議

資料

資料為主權AI發展基石，需解鎖資料最大價值

主權AI情境下，資料掌握能促進國家和企業開發符合需求的AI系統，推動智慧化成長，並確保符合我國的價值觀與法規框架

困境

洞察力乾旱

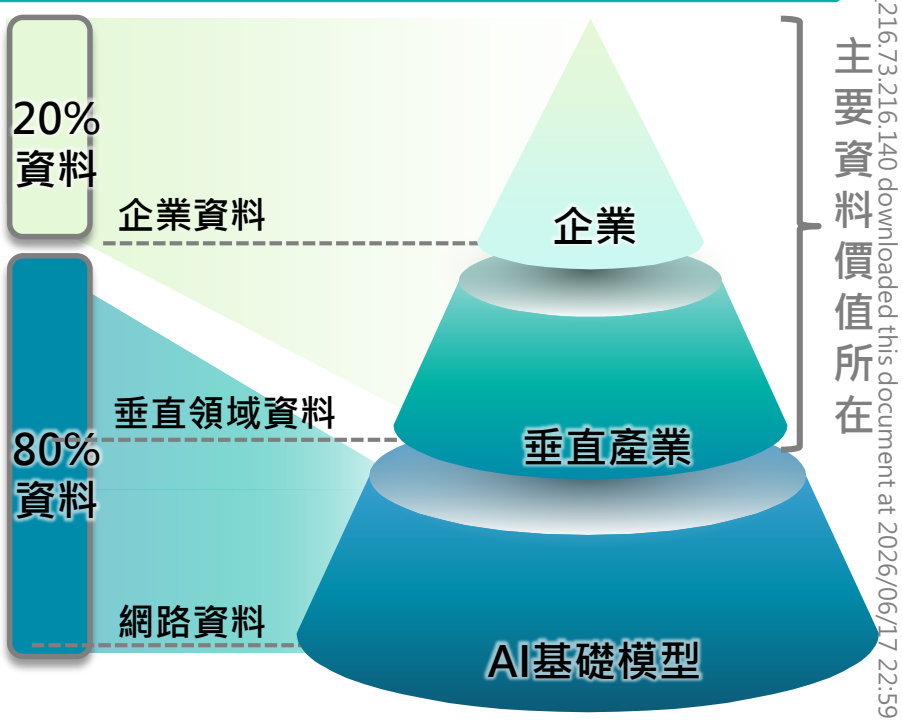
企業難以從既有資料中挖掘出更好的洞察(Insight)或決策建議...

資料悖論
Data Paradox

資料洪流

全球資料總量從1999-2023年增長約10-15萬倍...

現況/趨勢

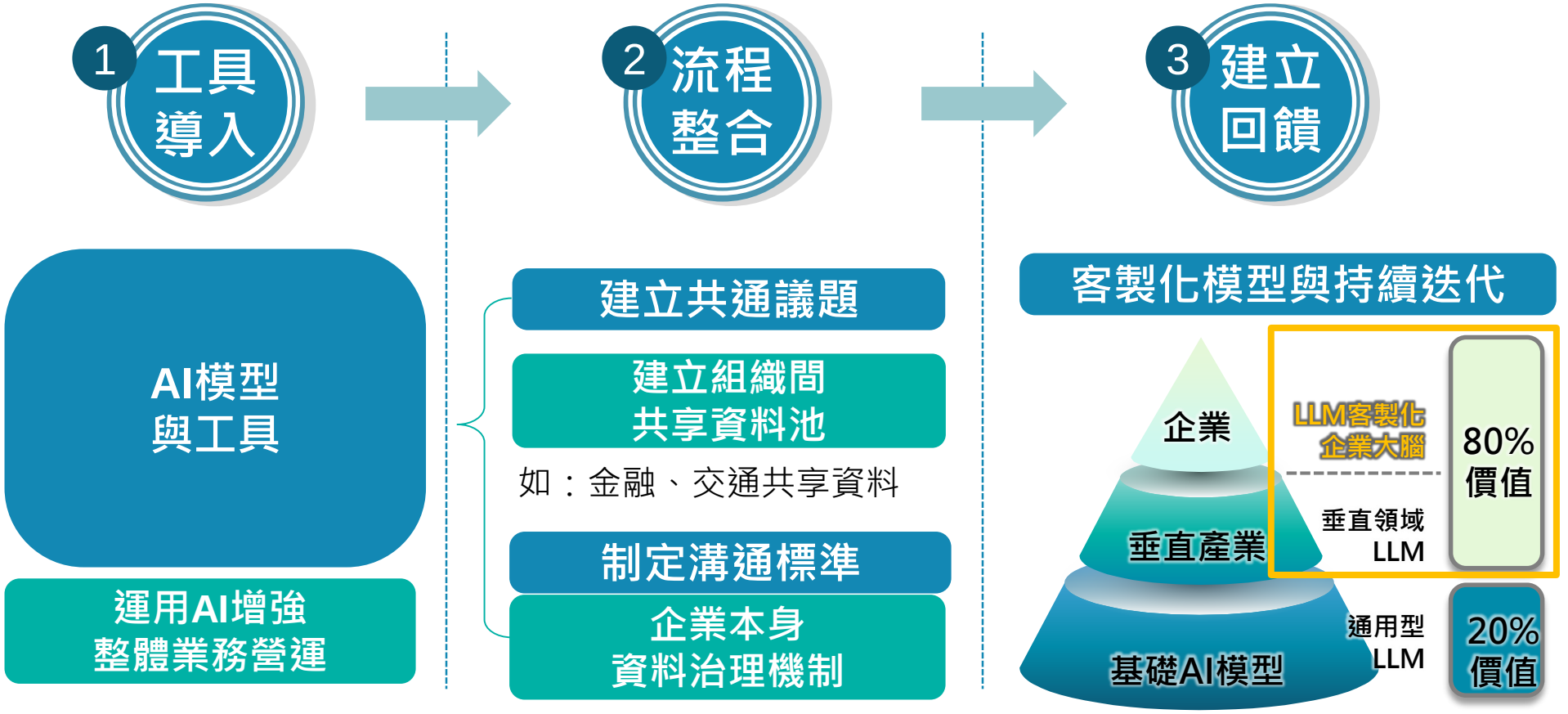


- **隨著資料量增加，AI模型效能卻不一定如預期般提高，甚至可能惡化**
- **目前訓練AI模型有8成都來自於網路資料，剩餘2成領域與企業內部資料仍未完全運用**

資料來源：MIC、 2023 The AI Summit New York ，2025年4月

以跨單位聯盟和共通標準放大資料價值

以降低AI工具導入門檻，成立組織解決資料共通議題，推進組織制訂資料使用規範與交換標準，放大企業資料價值與洞察力



資料來源：MIC，2025年4月

資料治理助力AI應用，建立全面高效的管理框架

前期：資料辨識與整合

1. **資料分類**（Data Classification）
   - 根據資料的敏感性、用途和價值進行分組
2. **資料目錄**（Data Catalog）
   - 統一管理資料來源、格式、關聯性和位置
3. **資料品質**（Data Quality）
   - 確保資料準確、一致、完整和可靠性

中期：資料合規與保護

4. **資料合規**（Data Compliance）
   - 確保資料使用符合相關法規和內部要求
5. **資料安全**（Data Security）
   - 防止未經授權的訪問、資料洩露或濫用
6. **資料取用**（Data Access）
   - 管理資料的存取權限和使用者角色

後期：資料應用與生態

7. **資料血緣**（Data Lineage）
   - 追蹤資料從來源到流向及變更的整個過程
8. **資料共享**（Data Sharing）
   - 促進資料在組織內部或外部的流通

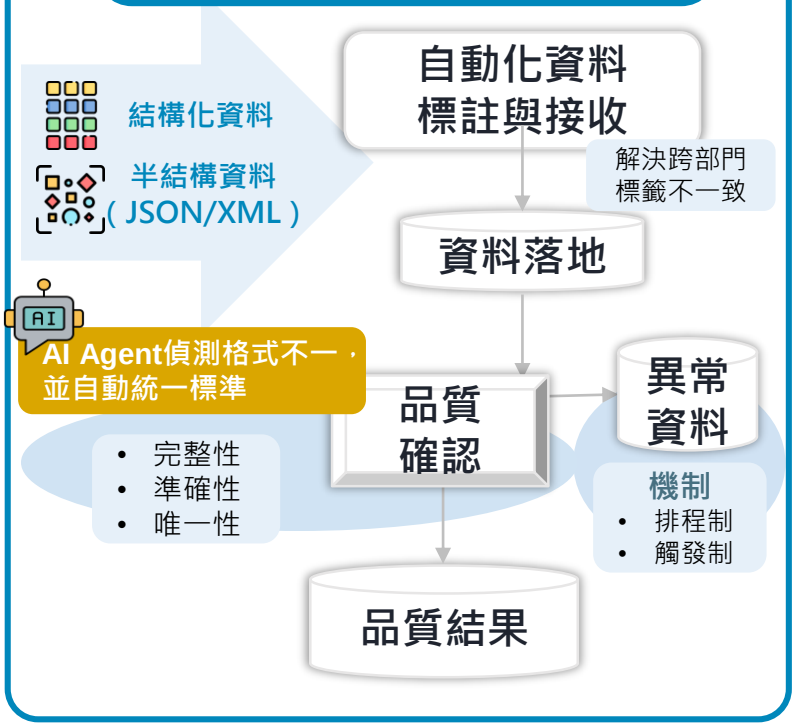
資料來源：MIC，2025年4月

Snowflake：自動化標註與監控提升標準化，強化應用

snowflake Horizon Catalog

憑藉雲端原生架構獲廣泛採用，並於2024年推出snowflake intelligence，幫助用戶建立Data Agents

資料標準化與品質監控



自動化資料接收→資料落地

品質結果

資料品質監控：
自動檢測欄位缺失，統一資料描述與格式，確保模型高品質運行

品質指標與報告：
了解跨部門標準化，提供標準化指標與報告，為訓練奠定基礎

品質可視化分析：
圖形化呈現資料標準化，支援資料監控管理，提升AI應用效率

資料來源：Snowflake，MIC整理，2025年4月

- 標準化與一致性管理：可降低資料整合障礙，提升資料可用性，使AI訓練與資料應用更精確、高效，並能解決標籤不一致與命名混亂等問題
- 自動化資料品質監控：透過品質報告與視覺化分析，確保完整性、準確性、唯一性

BigID：強化AI資料合規與存取管理，確保風險可控

BigID Data Intelligence Platform

Big ID強調自動化、AI驅動的高度可擴展性，在處理結構化與非結構化資料具專業能力，具全面性優勢

支援存取與修改請求：
滿足資料主體權利要求

維護同意歷史：
追蹤證明個資處理同意記錄

自動監測存放地：
評估並確保符合傳輸限制

資料保存政策：
確保符合法規儲存限制

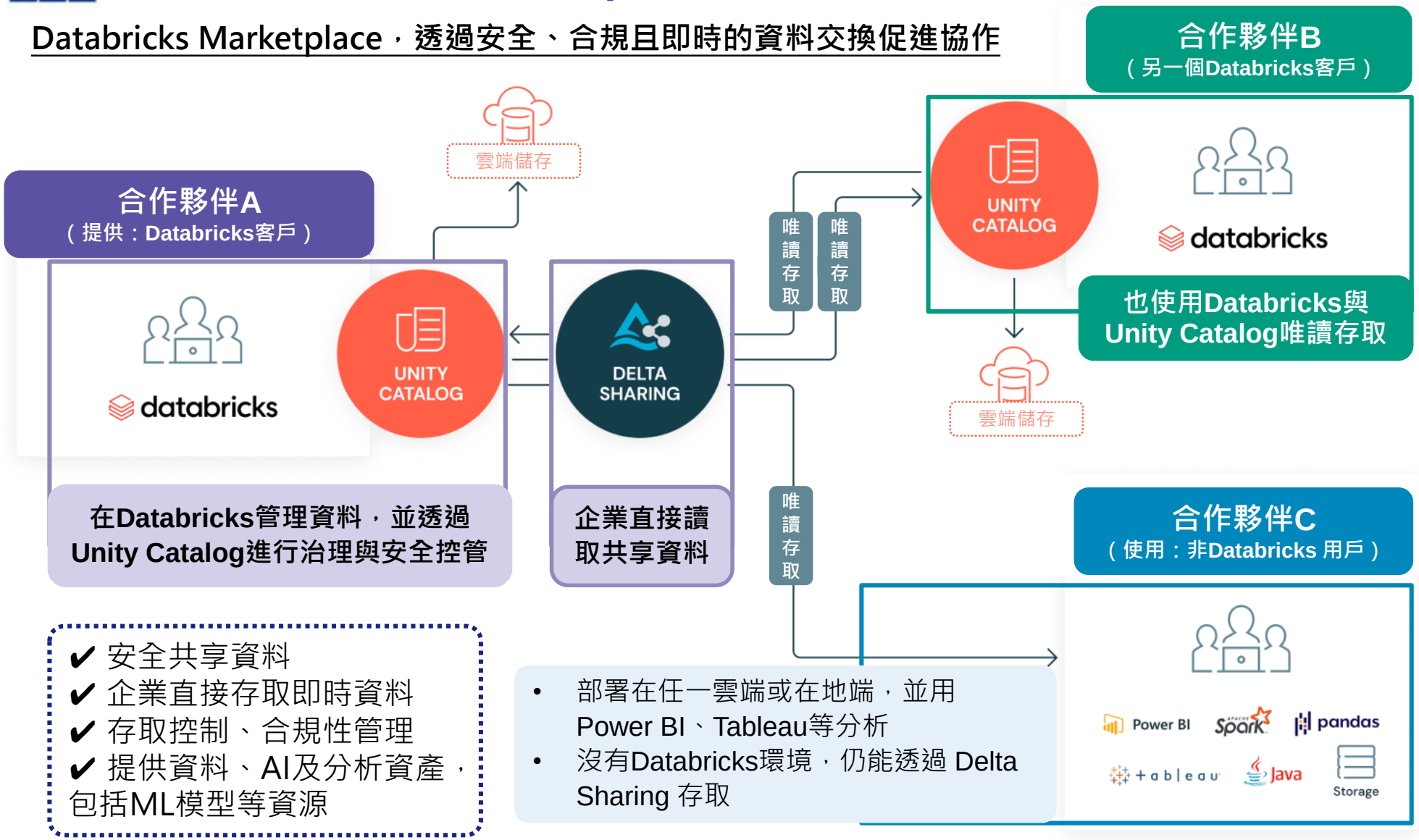
自動偵測暴露風險：
72小時完成外洩影響評估

資料來源：Big ID，MIC整理，2025年4月

- AI資料合規與存取治理：透過自動血緣追蹤與隱私管理，確保來源合法且風險可控
- 全面合規執行與風險管理：透過風險偵測、同意記錄追蹤與法規整改，協助企業符合GDPR、CCPA等全球資料保護標準，確保資料營運安全且透明

Databricks：Marketplace打破障礙，強化企業資料流通

Databricks Marketplace，透過安全、合規且即時的資料交換促進協作



- ✔ 安全共享資料
- ✔ 企業直接存取即時資料
- ✔ 存取控制、合規性管理
- ✔ 提供資料、AI及分析資產，包括ML模型等資源

- 部署在任一雲端或在地端，並用Power BI、Tableau等分析
- 沒有Databricks環境，仍能透過 Delta Sharing 存取

資料來源：Databricks，MIC整理，2025年4月

主權AI三要素分析暨建議

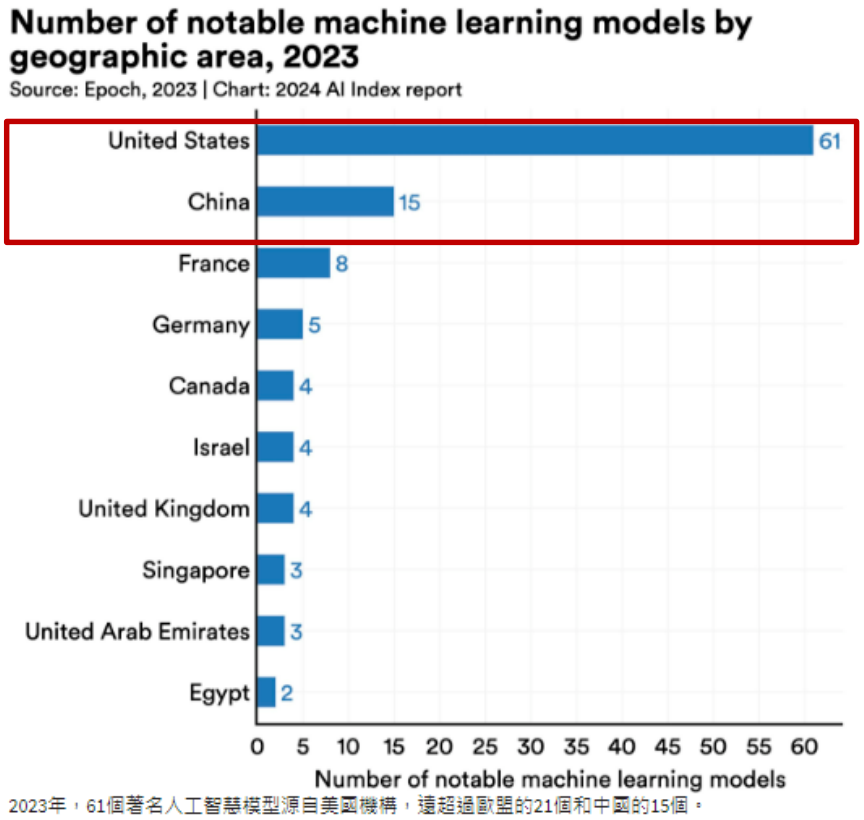
演算法

LLM多由美國開發，我國企業應用要找合適之主權AI模型

為確保LLM符合企業需求，我國應協助企業發展符合產業需求的主權AI模型

困境

- 主流LLM偏重他國價值觀

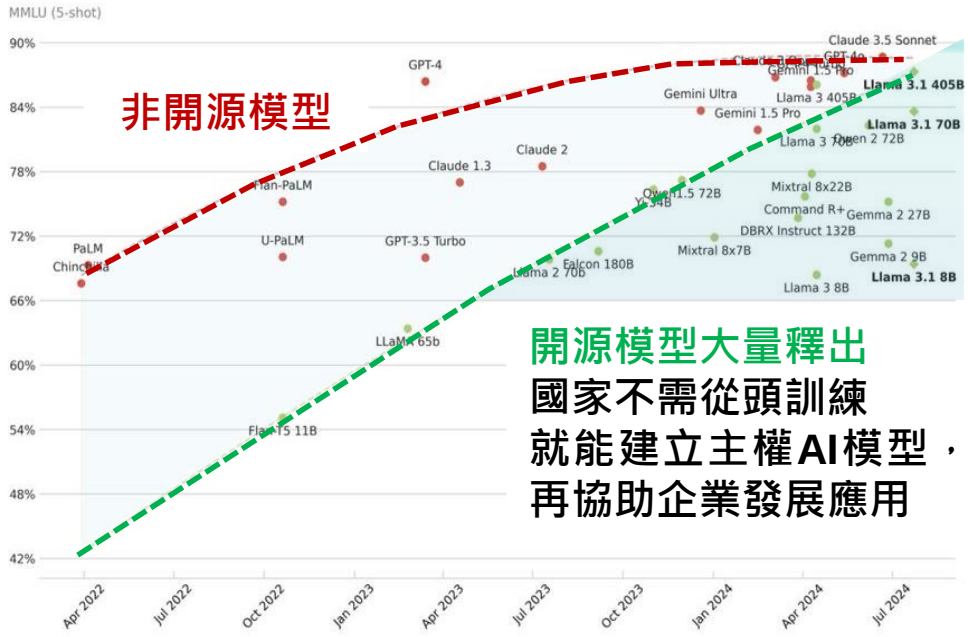


2023年，61個著名人工智慧模型源自美國機構，遠超過歐盟的21個和中國的15個。

資料來源：史丹佛AI Index，2025年4月

現況/趨勢

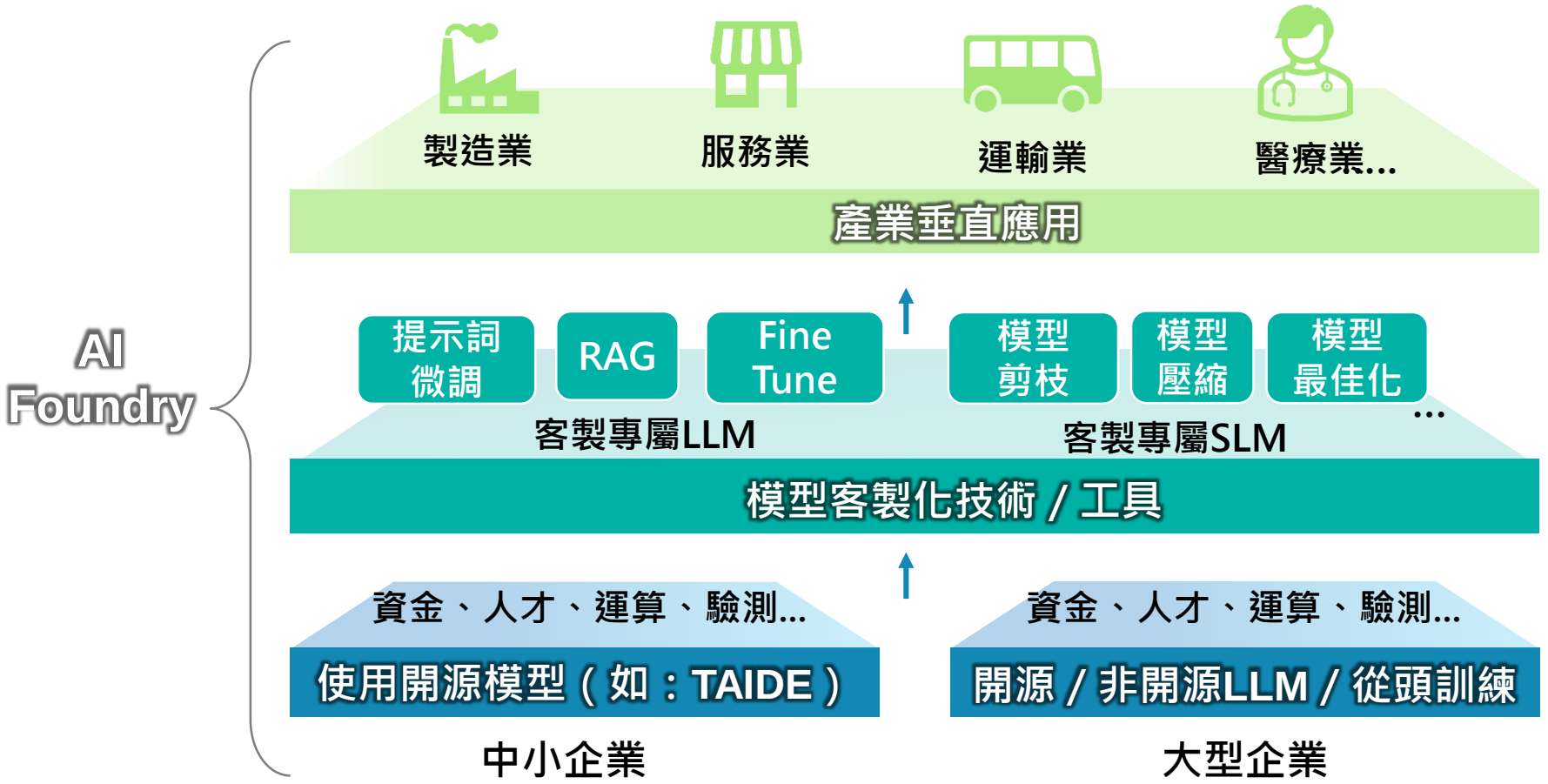
- 多國家已借助開源模型發展獨有LLM
- 模型客製化技術（如：微調）能夠協助企業在主權AI模型上發展產業應用



資料來源：Maxime Labonne，2025年4月

「AI Foundry」協助百工百業用AI

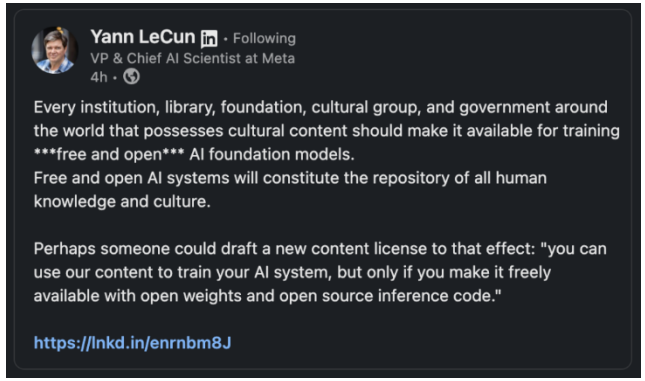
在台灣主權AI模型基礎上(如：TAIDE)，發展「AI Foundry」模式，透過模型客製化技術協助企業建立專屬LLM或SLM，促進百工百業用AI



備註：AI Foundry指為滿足百工百業AI應用需求，以垂直分工方式發展「可供企業訓練的LLM或SLM」，提供相對應的專業知識
資料來源：MIC，2025年4月

AI新時代，面臨開源定義的調整及再定義

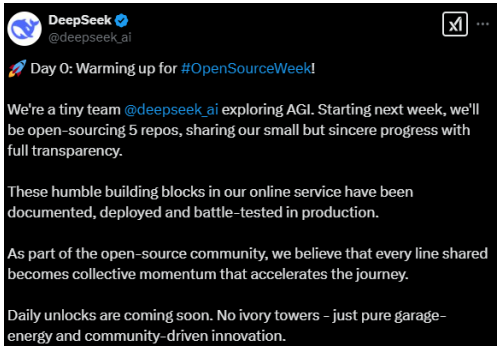
資料



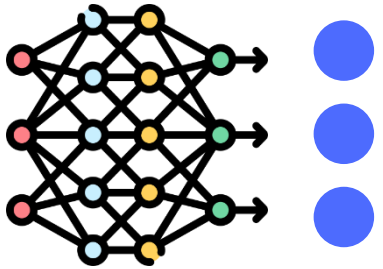
- Yann LeCun建議開放資料給大家訓練，但也希望AI公司開放模型權重（視為文化儲存庫)
- 少部分已開放資訊，但大部分未有正式說明訓練資料集

程式碼

- 2025.2.21 DeepSeek開源週



權重



deepseek V3

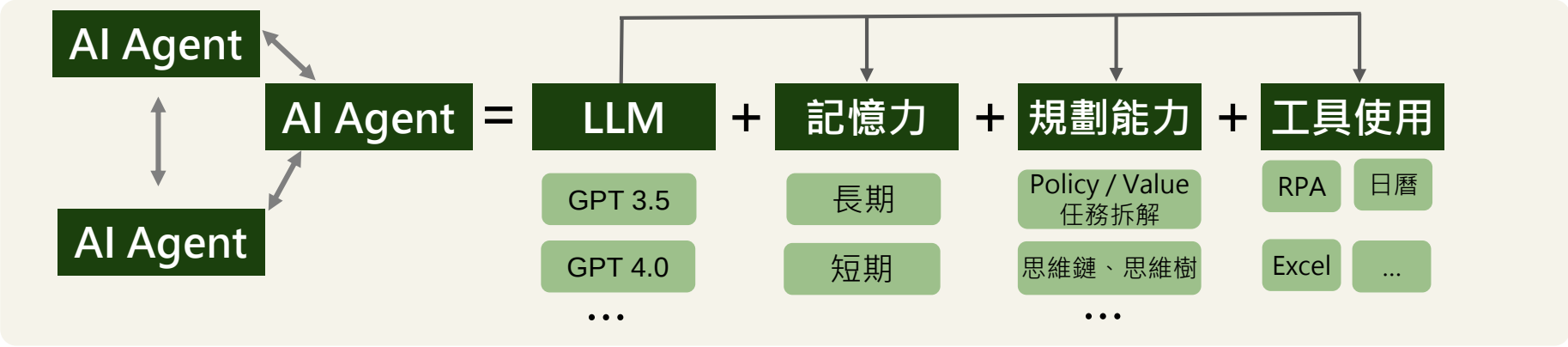
deepseek R1

- MIT授權-可讓人修改，相對開放的幅度最大。但若有法律議題時，依中華人民共和國為準據法*。

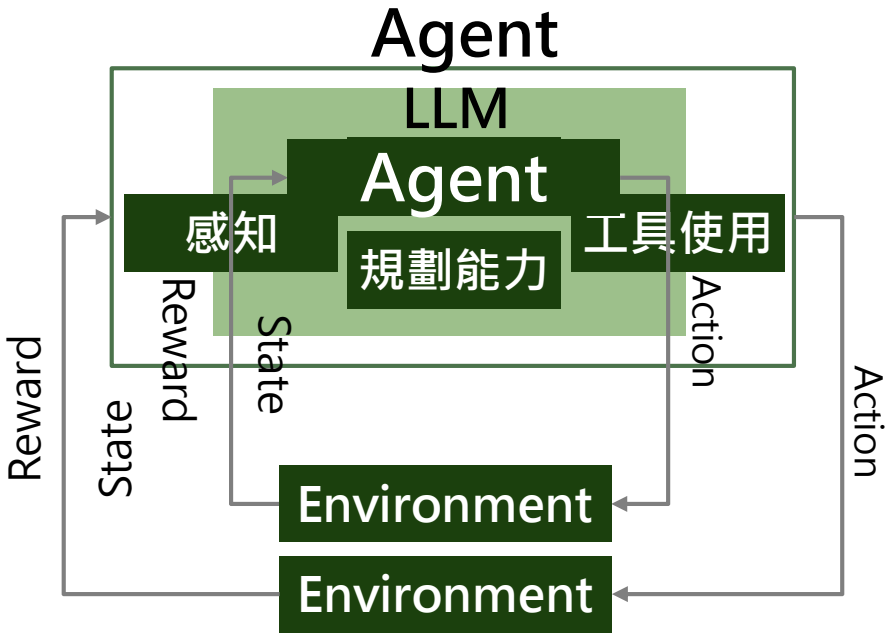
*From:台灣開源法律網絡共同創辦人林誠夏

- AI時代來臨，對於開源的定義，會重新出現新的方向及適用範圍。但由於會提到有限制使用目的和範圍、有附加條款，如：可撤回（如國家法令重新定義）或是部分不公開，因此就有不夠符合開源原則之討論，不過也形成這波「準」開源模式
- 對此，在模型選擇上，除了模型能力、模型大小外，相關開源方式也是重要的考量因素

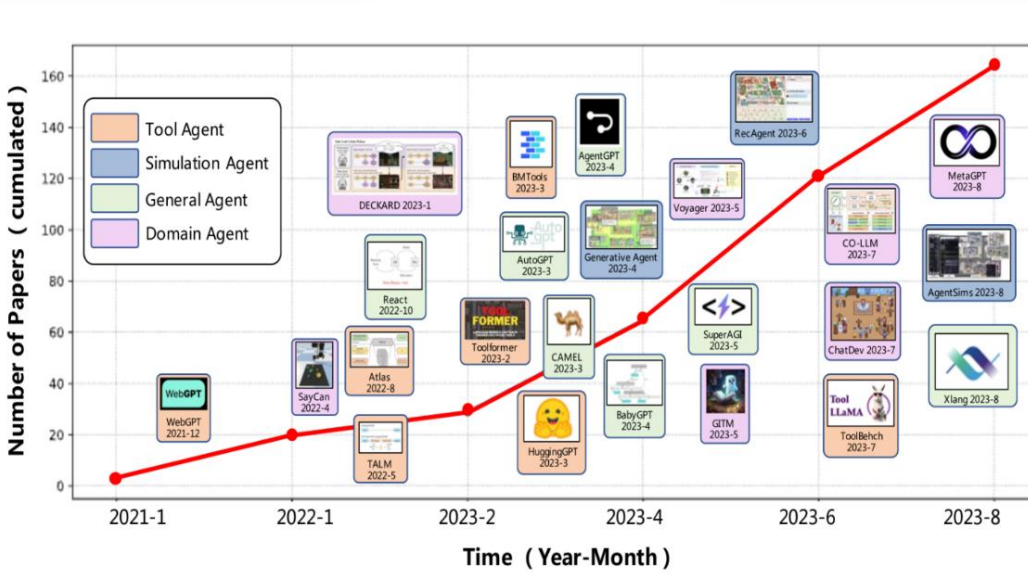
不斷與環境互動的AI Agent



資料來源：MIC，2024年12月



資料來源：MIC，2024年12月



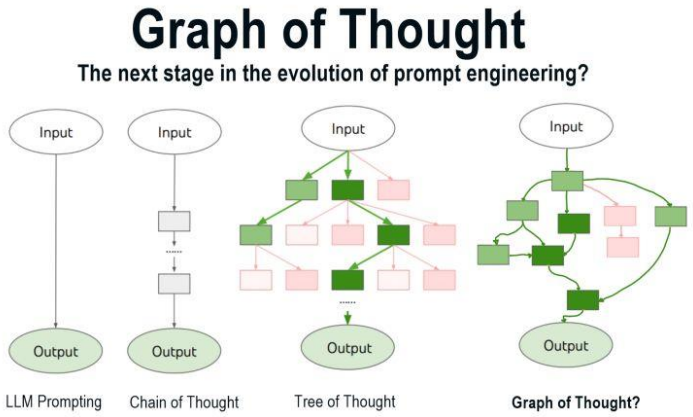
資料來源：A Survey on Large Language Model based Autonomous Agents， MIC整理，2024年12月

快思 VS 慢想 – 具備科學腦的模型
GPT o1、DeepSeek R1、Gemini 2 Flash Thinking

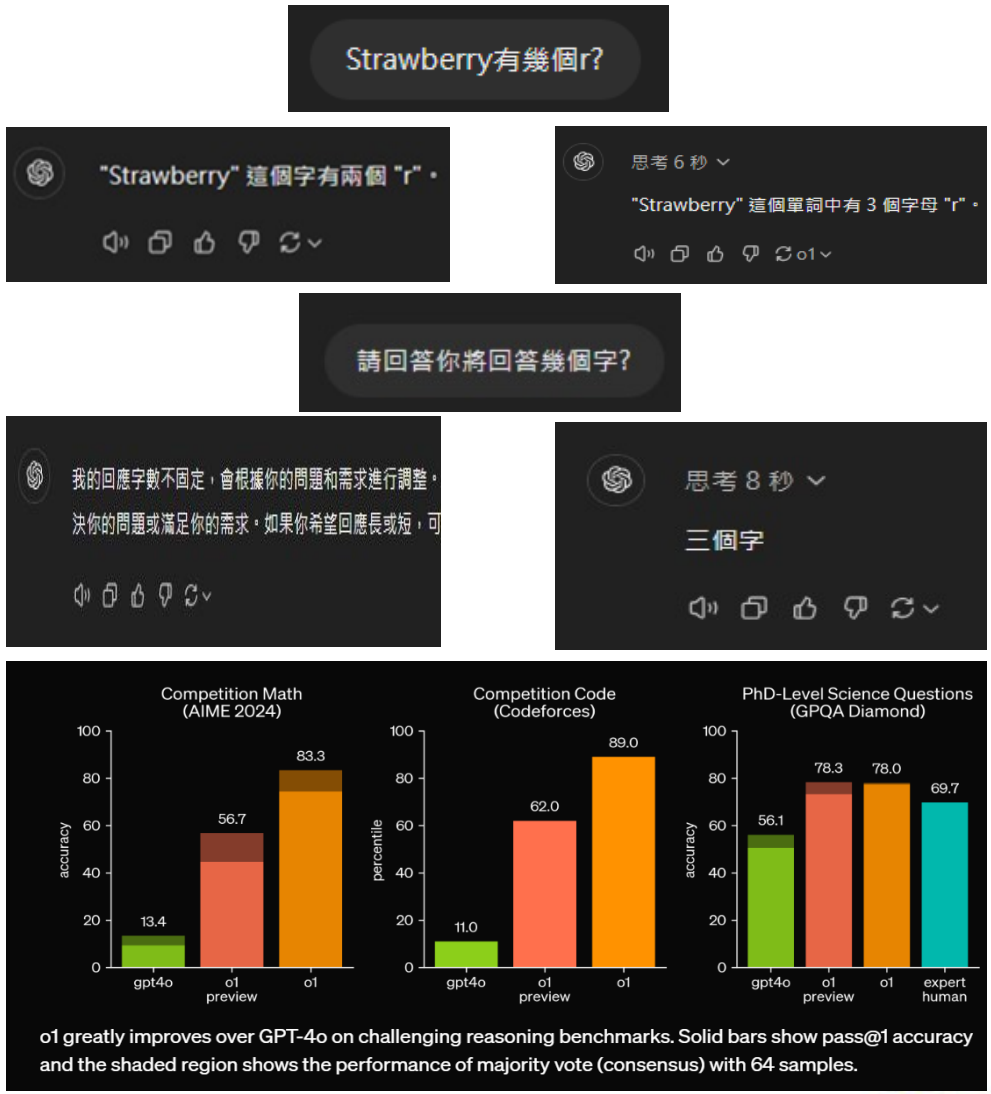
- GPT o1是運用思考鏈去運作的AI模型，比起直接產成結果的模型來看，更會在產出結果前，先做自我推論及反思的動作。

Whom it's for

These enhanced reasoning capabilities may be particularly useful if you're tackling complex problems in science, coding, math, and similar fields. For example, o1 can be used by healthcare researchers to annotate cell sequencing data, by physicists to generate complicated mathematical formulas needed for quantum optics, and by developers in all fields to build and execute multi-step workflows.



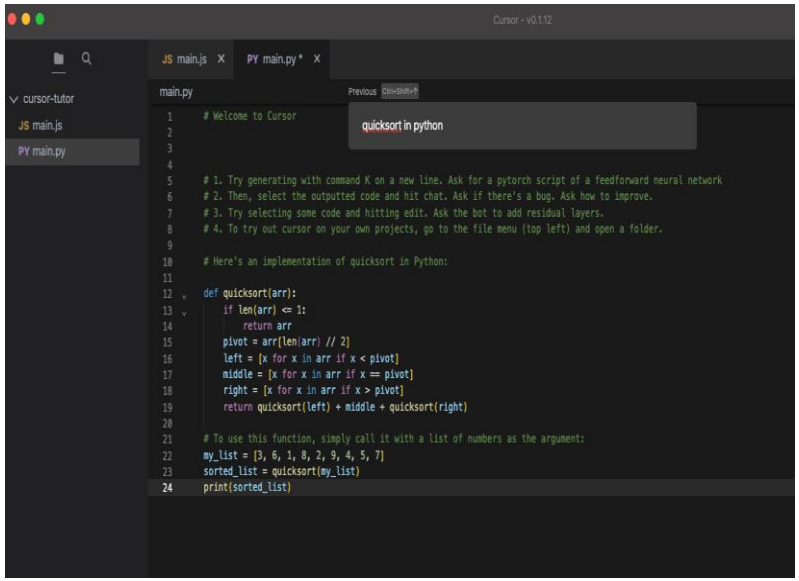
GPT 4o　　GPT o1



資料來源：OpenAI，MIC整理，2024年12月

Cursor借力使力，自串生態系

- Cursor產品立志要建立 AI Native的IDE，基於 VSCode及結合各種不同庫(Repository)和檔案之間的編輯
- Cursor也因為Llama 3及Claude Sonnet 3.7模型快速反應的能力，使得使用者也在使用Cursor AI時獲得好的體驗



資料來源：Cursor.AI，MIC整理，2025年4月

剪貼翻譯機

多引擎搜尋器

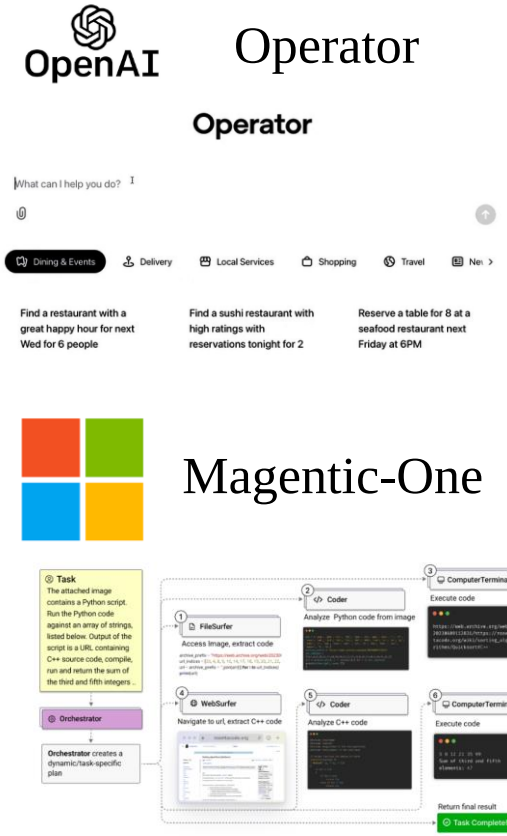
計時器

資料來源：MIC整理，2025年4月

物體檢測記錄儀

經典句子收集器

Claude AI –「Computer Use服務」做電腦使用Agent

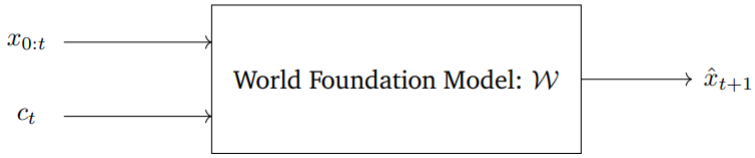


資料來源：Anthropic、微軟、OpenAI， MIC整理，2025年4月

藉生成影像來降低自駕車的訓練門檻

自主 Bot

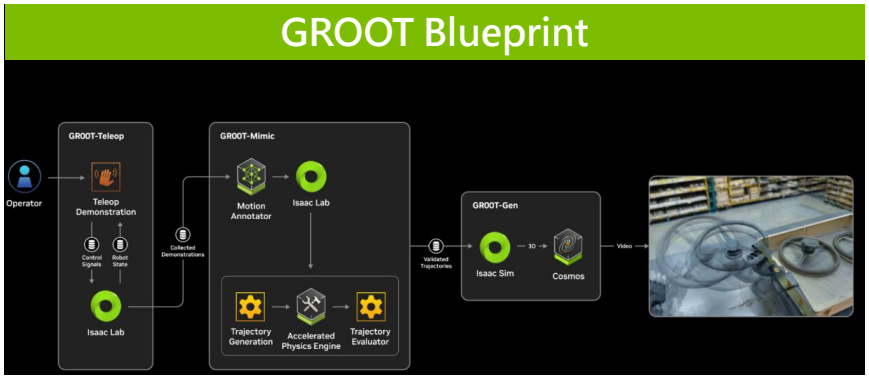
NVIDIA – 提供World Model給全球應用於人型機器和載具

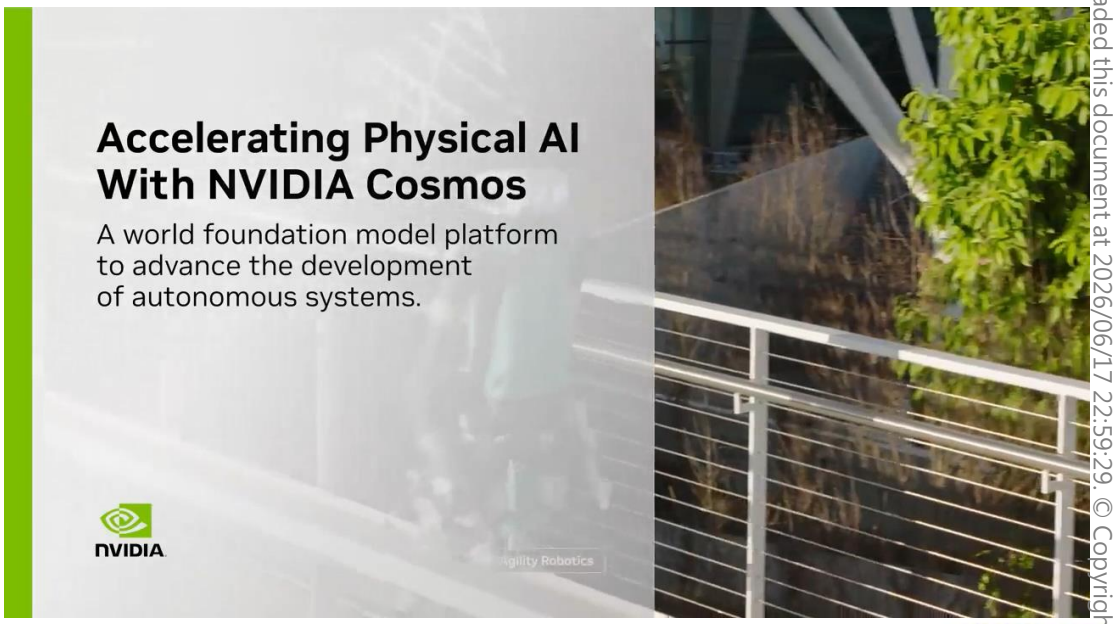


- WFM主要是將現在X0:t的情況及Ct (擾動)至WFM做下一時段的預測($\hat{x}t+1$)

場景	資料占比
Driving	11%
Hand motion and object manipulation	16%
Human motion and activity	10%
Spatial awareness and navigation	16%
First person point-of-view	8%
Nature dynamics	20%
Dynamic camera movements	8%
Synthetically rendered	4%
Others	7%

- WFM主要由2,000萬小時的影像資料所訓練



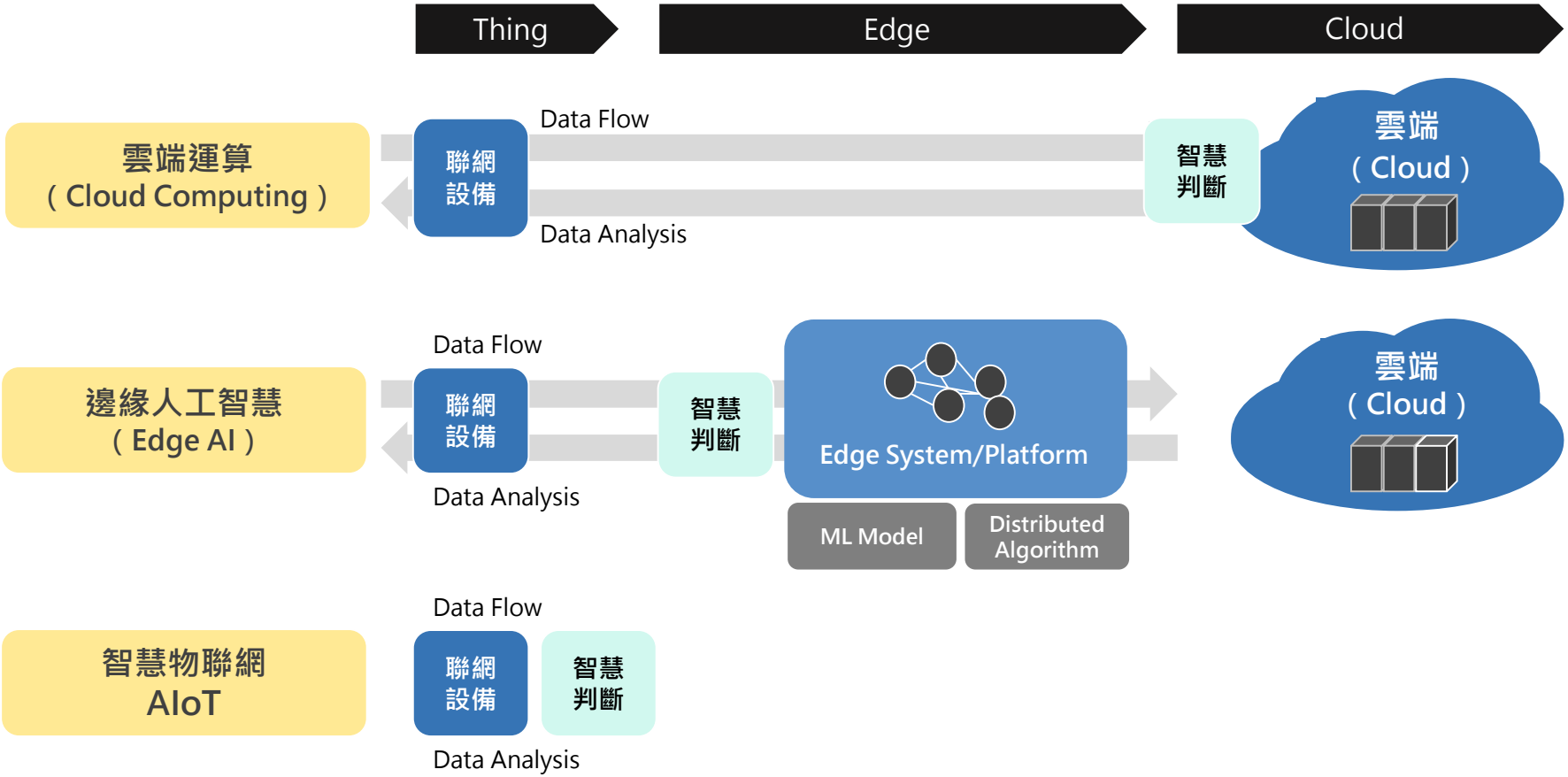


資料來源：NVIDIA ，MIC整理，2025年1月

主權AI三要素分析暨建議

雲、邊、物的運算力

新興AI運算依靠雲、邊、物AI運算架構



資料來源：MIC整理，2025年4月

- 高速的人工智慧發展下，對於不同先進人工智慧要求下，需依賴現行雲端、邊緣以及物聯設備的算力協同配合，方能使得使用者獲得較好的體驗

混合式AI成為未來主流，終端裝置為發展重點

生成式AI發展從雲端逐步邁向邊緣

AI運算處理過往由雲端支援，未來將逐漸往終端裝置發展實現本地運算

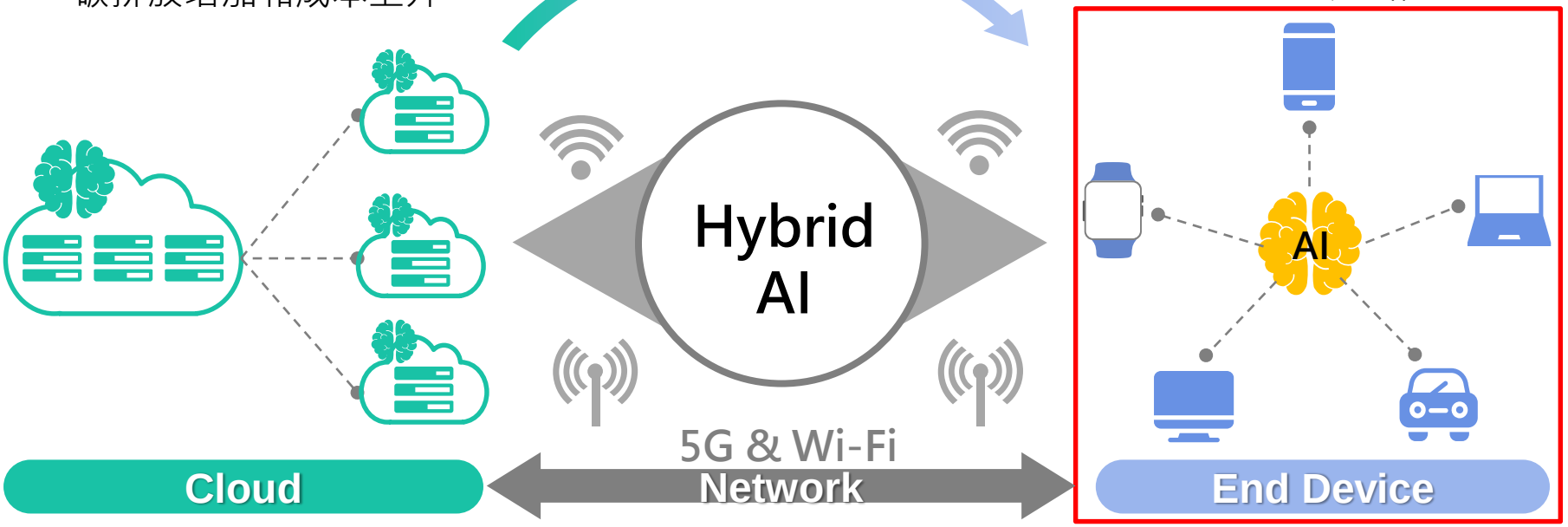
可部署雲端>100億

雲端GPU算力資源將導致碳排放增加和成本上升

From Cloud to Edge

可部署終端<100億

終端算力NPU可同時解決延遲和隱私揭露問題



降低雲端成本

增加終端裝置算力，可減少雲端部署成本

增強用戶隱私

用戶使用應用時，不需連網，增強隱私保護

降低體驗延遲

避免因連網造成用戶使用體驗不佳

強化運算效率

AI應用可在本地端直接運算，不須依靠雲端

資料來源：MIC，2025年4月

台灣需要更多主權AI運算力並建立安全認證機制

1 台灣主權AI運算力規劃

政策目標：假設2028年製造業5成導入AI應用

2028年所需運算力**7,557**PFLOPS

優嵐 UBILINK　雲高 DCT　國網 NCHC　TWS TAIWAN WEB SERVICE　GMI　Enlight 翔耀實業股份有限公司

台灣現已公開規劃算力至2028年新增

1,048PFLOPS，仍有將近**7倍**的差距

（運算力建置主管機關為國科會、數位部、通傳會）

2 歐日推動主權AI硬體認證機制

gaia-x

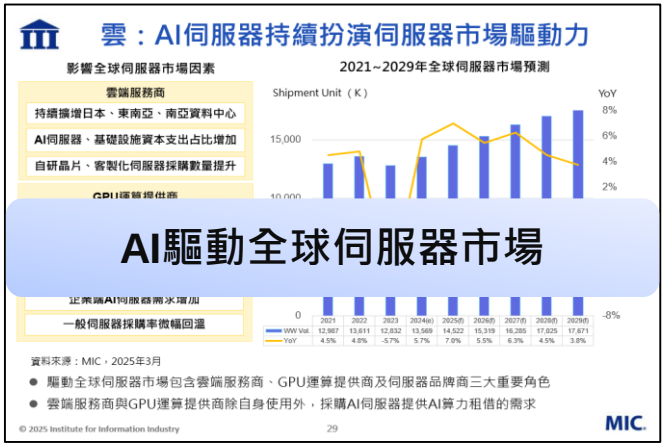
歐洲主權雲Gaia-x，採用歐盟雲端認證計劃(EUCS)，雲端服務商需與當地業者合作，且**伺服器須通過產品認證**

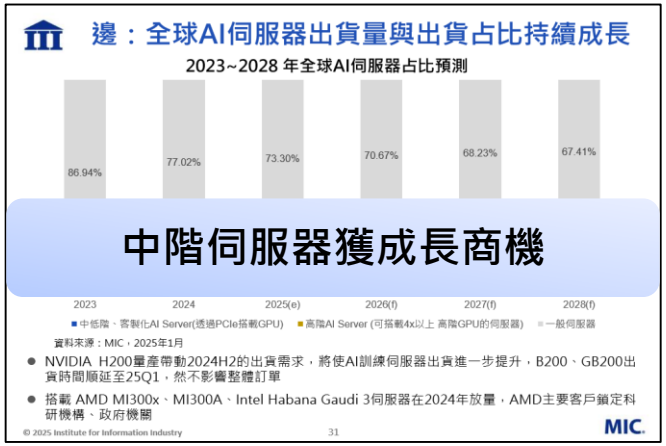
經濟安全保障推進法

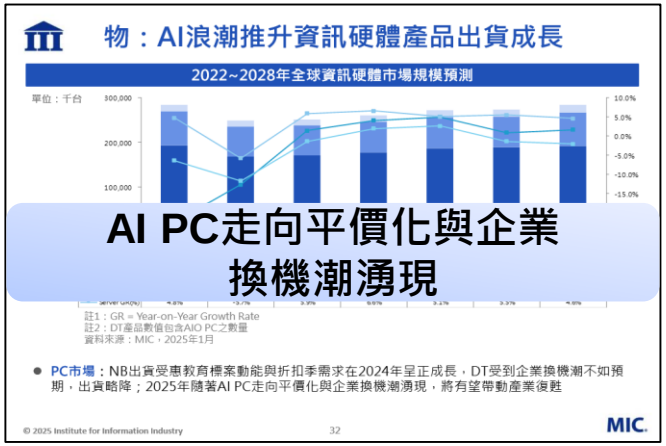
日本經濟安全保障推進法，針對**關鍵基礎設施**，是否使用具疑慮的國外設備，事先進行**安全性審查**

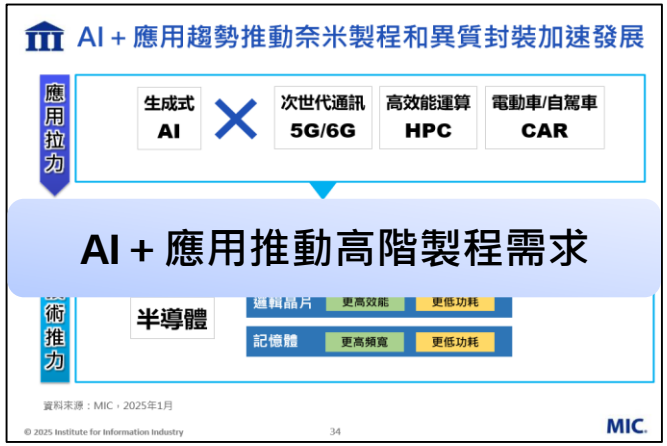
資料來源：MIC，2025年4月

AI再次觸發雲、邊、物商機









資料來源：MIC，2025年4月

- 雲端服務商、各場景所需的邊緣運算以及各式穿載及物聯網裝置皆在AI同步協作運算要求下，獲得新一波升級和換機之需求

結論

結論

- **【資料】以跨單位制定資料共通標準，放大企業資料價值**
  - 輔助降低AI工具導入門檻，並召集跨單位解決產業資料共通議題，推進組織制訂資料使用規範與交換標準，放大企業資料價值與洞察力
- **【演算法】以主權AI為基礎，協助企業打造符合需求的模型及發展領域型AI Agent應用**
  - 在台灣主權AI模型基礎上(如：TAIDE)，發展「AI Foundry」，以模型客製化技術協助企業建立專屬LLM或SLM，促進百工百業用AI Agent
- **【運算力】完善基礎建設，主權AI硬體需求帶動雲、邊、物商機**
  - 台灣需擴大至2028年的AI運算力部署規劃，強化基礎建設量能
  - 雲、邊、物商機因全面AI應用落地獲成長及換機商機

MIC 產業提昇的關鍵力量

Thank You

韓揚銘　產業顧問兼副主任

rayhan@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