人工智慧技術演進現況與應用趨勢

韓揚銘 資深產業分析師兼組長

產業情報研究所(MIC)

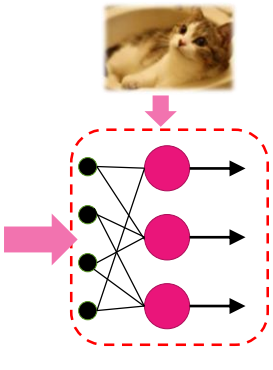
財團法人資訊工業策進會

2021.05.19

Rayhan@iii.org.tw
mic.iii.org.tw

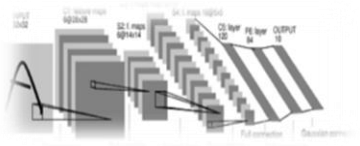
深度學習主導人工智慧發展

Meta Learning



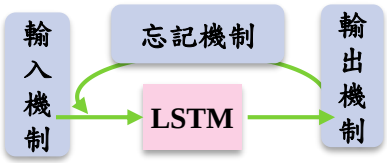
「學習如何學習」的方法，思考運用不同方法（演化法、貝式法、增強學習...等）讓AI在訓練時得以自行找到最適化的調校參數

CNN



卷積神經網絡，從一塊塊矩陣中向一層層網路進行歸納

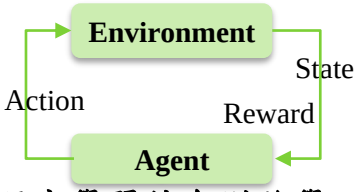
RNN/LSTM



運用神經網絡的方式處理具時間序列的問題

聯盟學習（Federated Learning）

Deep RL



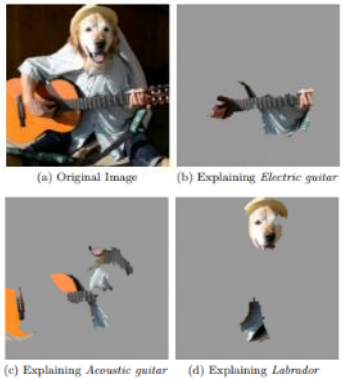
深度學習結合增強學習後來達到領域的自主學習能力

GAN

「生成模型」不斷與「判別模型」彼此訓練，收斂後再加模仿應用

XAI

（Explainable AI）



針對圖像、聲音、文句辨識或判讀上的進行部分解釋，與使用者共同獲得的判斷基礎，進行下一步決策

Transfer Learning

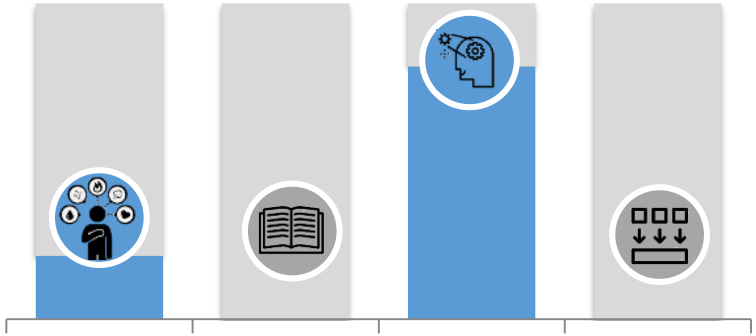
運用之前訓練的模型（如: Cat model）轉移到另一個事物的辨識，以較少的樣本規模的訓練則可獲得目標模型（如:Leopard）

資料來源：MIC，2021年5月

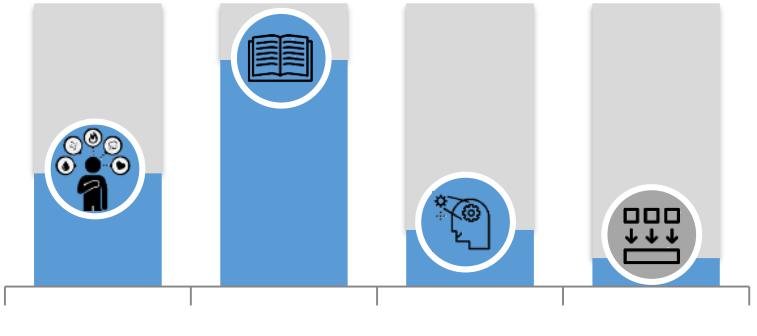
❖ 深度學習發展中，除了神經網路架構的方法論外，同時也有不同方法嚐試解構神經網路的方法

人工智慧能力發展朝情境理解能力發展

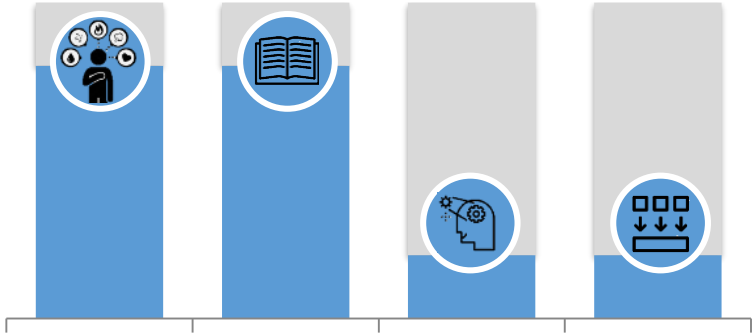
第一波：推理推論



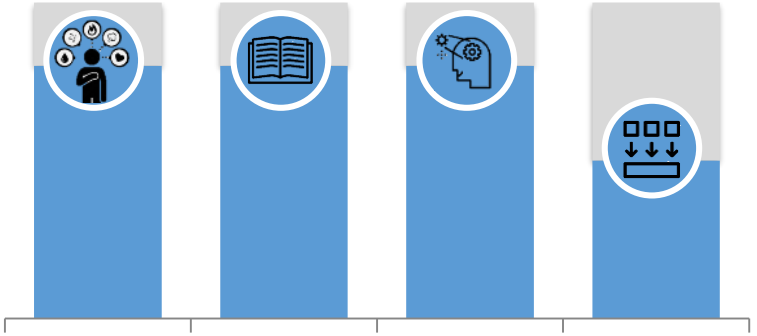
第二波：統計學習



第三波：深度學習

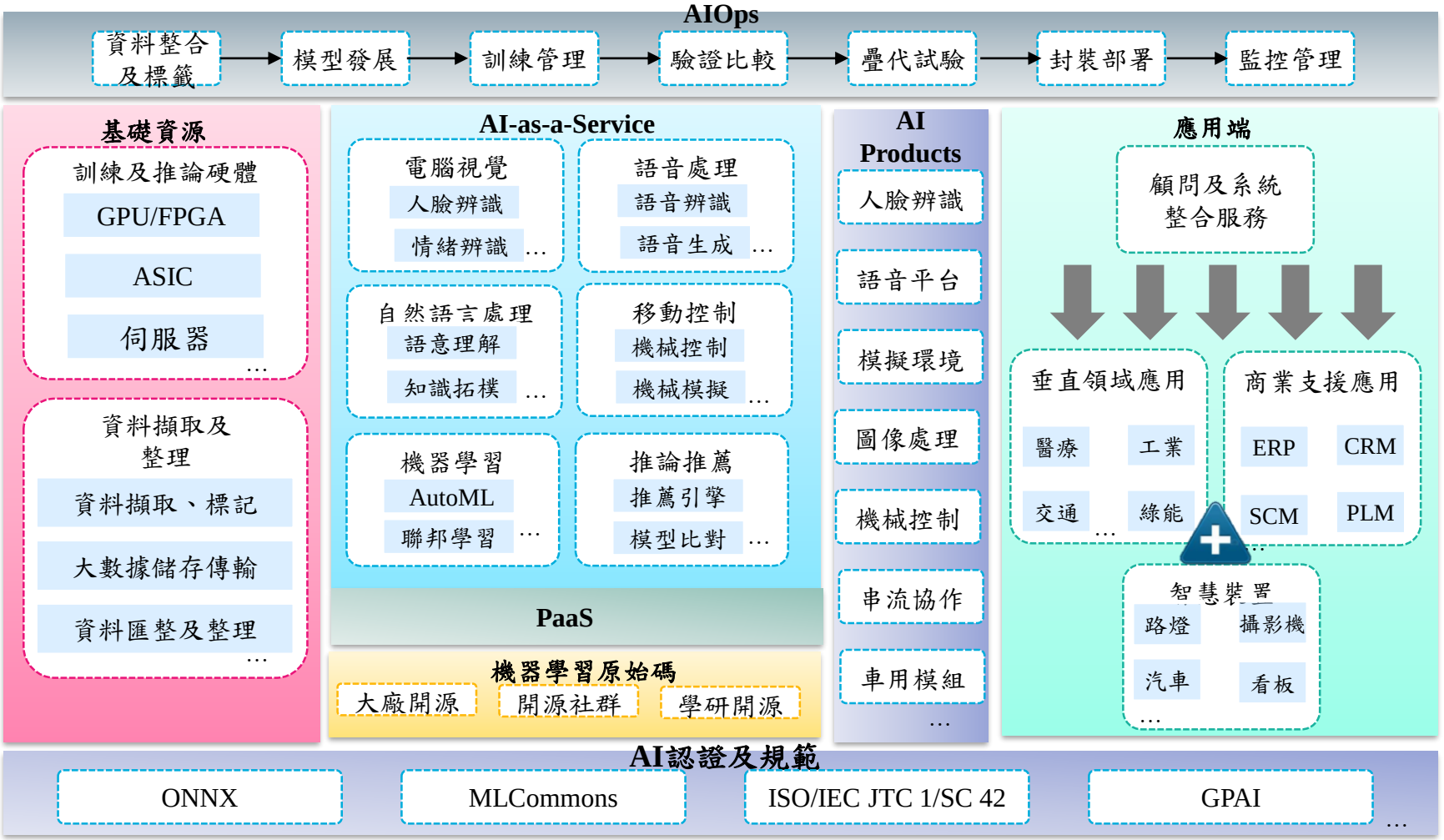


第四波：情境理解



資料來源：MIC，2021年5月

人工智慧產業生態持續擴張



資料來源：MIC，2021年5月

- 人工智慧發展持續，除技術快速疊代累積外，相關管理議題也愈來愈受重視

大綱

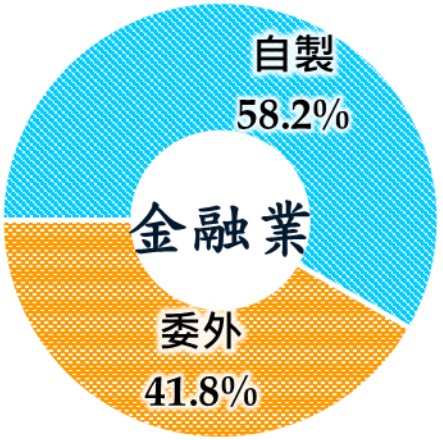
- 我國產業導入現況
- 人工智慧技術現況和應用
- 人工智慧管理議題
- 結論

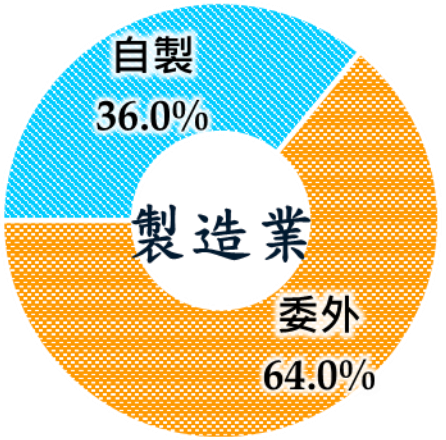
我國產業導入現況

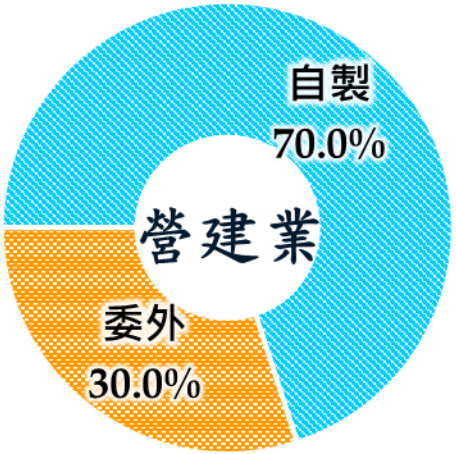
環境、法規及上下游整合度影響自製AI比重

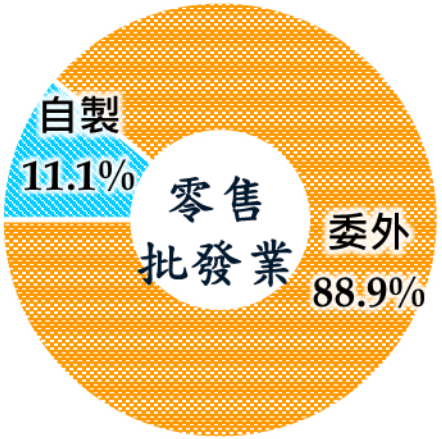
■ 盤點對象：

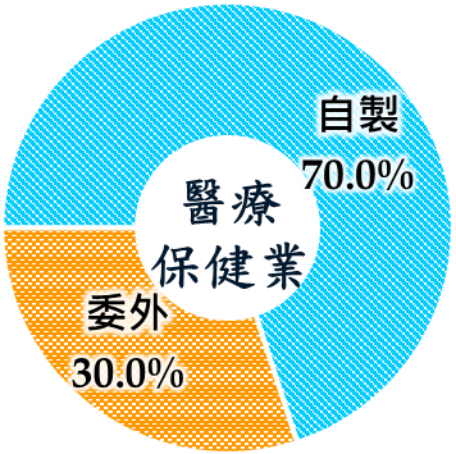
本次調查對象為台灣零售批發業、金融業、製造業、營建業、醫療保健業，共五個產業411家業者。藉由問卷方式詢問AI自製或委外比例、採用技術、應用選擇等議題







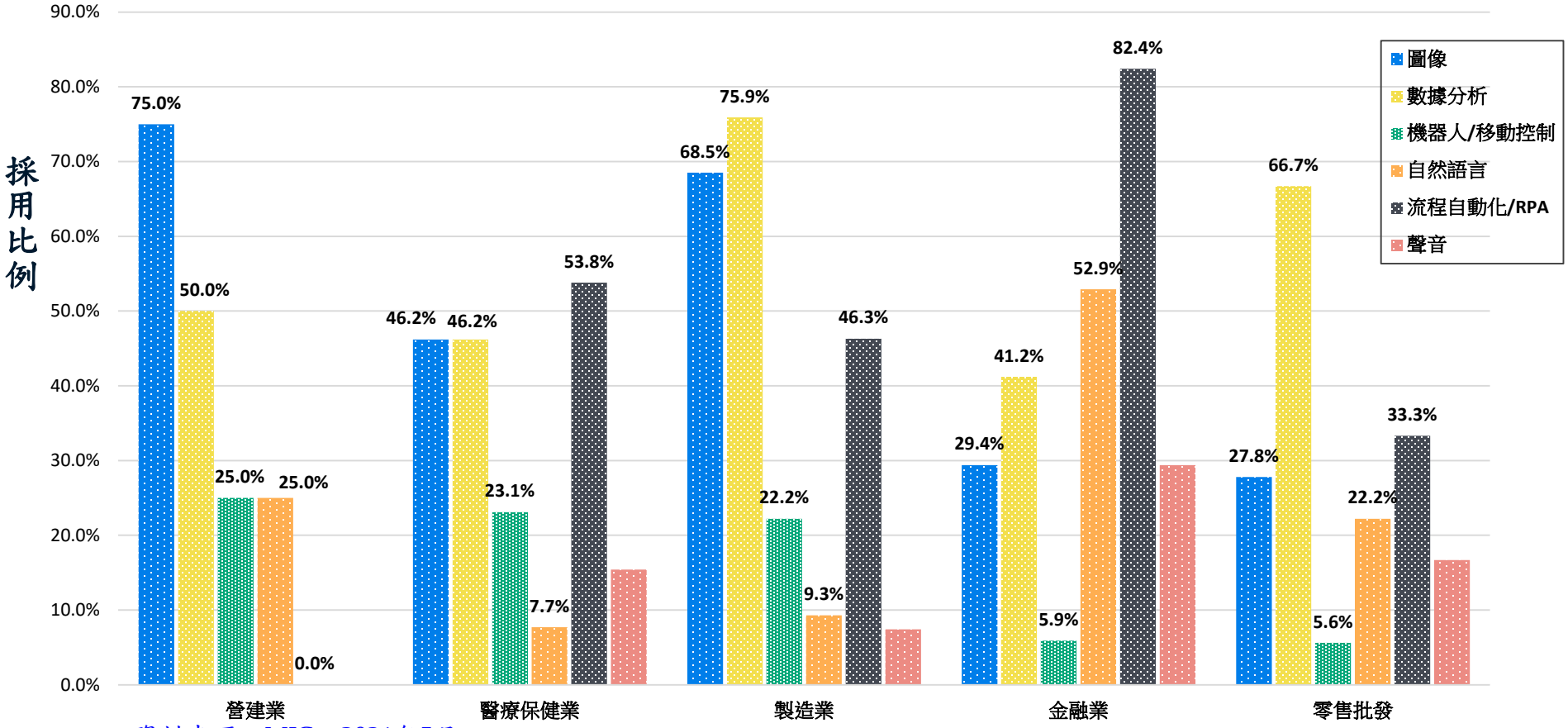




資料來源：MIC，2021年5月

❖ 公司在選擇AI自製或委外(含外購）的判斷在於產業環境的限制、法規的要求或是上下游整合需求等原因而做選擇

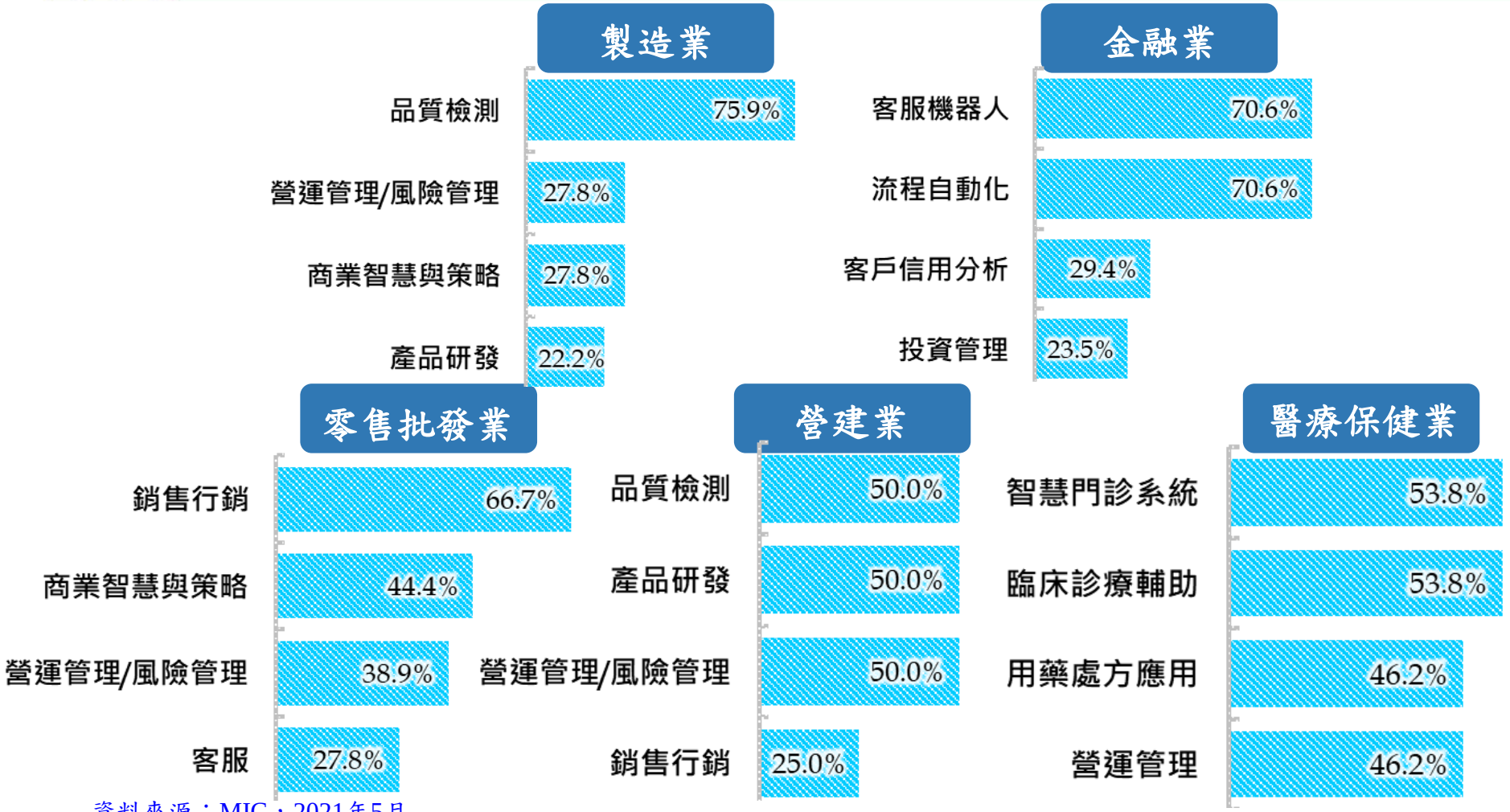
不同行業偏好採用不同人工智慧技術



資料來源：MIC，2021年5月

- 營建業在AI技術中使用圖像技術最多，另因數位化之原故，如製造、批發零售和醫療保健也運用大數據的方式進行數據分析。然而，自然語言處理上，金融業採用的比例最高
- 此外，近年因流程自動化需求，在金融業及醫療保健有高比例採用流程自動化RPA (Robotic Processing Automation)

導入應用以優化現有營運及客戶體驗為主



資料來源：MIC，2021年5月

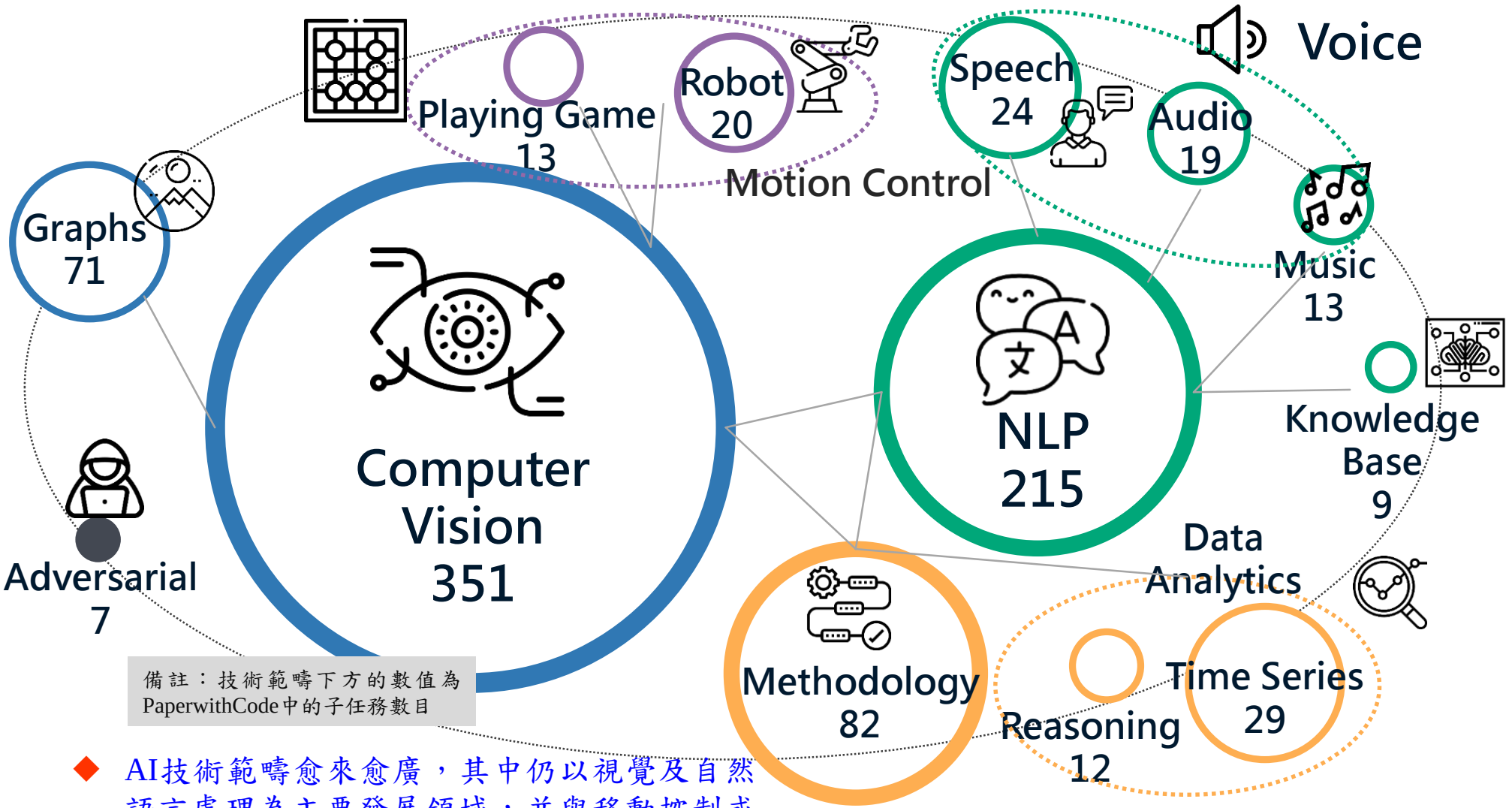
- 五大領域的前四項產業應用以現有營運流程優化、客戶體驗及相關領域的風險管理為主

人工智慧技術現況和應用

變化萬千的人工智慧技術範疇議題

資料來源：MIC，2021年5月

人工智慧技術範疇和項目快速擴張



備註：技術範疇下方的數值為PaperwithCode中的子任務數目

- AI技術範疇愈來愈廣，其中仍以視覺及自然語言處理為主要發展領域，並與移動控制或語音處理等範疇相連結

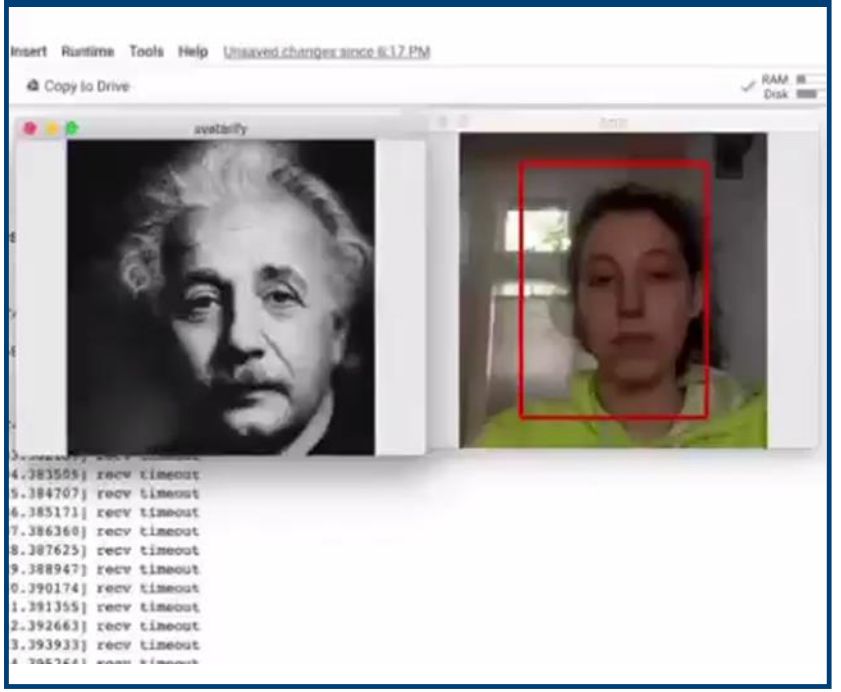
資料來源：MIC，2021年5月

生成對抗網路(GAN)的普及化帶來喜憂參半

卡通化生成

山水畫生成

生成其他人像影片



屬性融合生成服裝

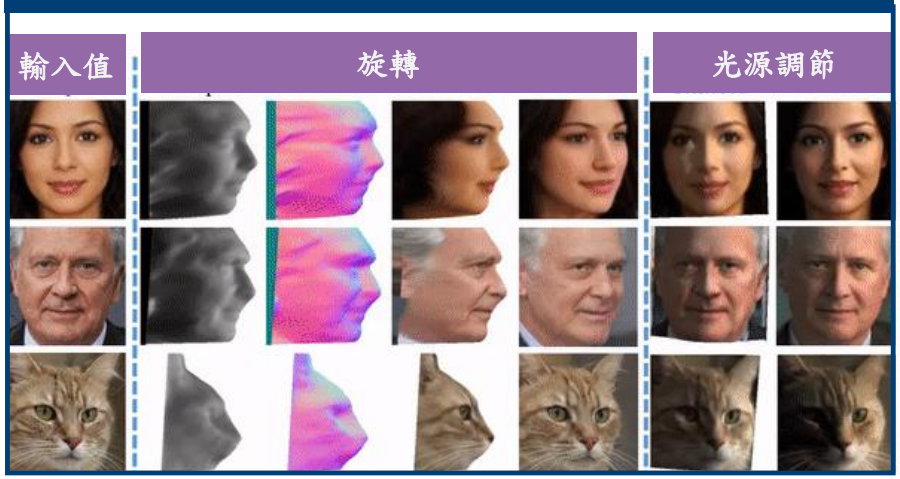
A query image (left) is combined with images from different product pages to produce a synthetic composite (right).

- 生成對抗網路(GAN, Generative Adversarial Nets) 的技術大幅度演進，加速各種場景應用及素材生成
- GAN的應用面向廣，但相對也容易會有負面應用造成假影像的事件

資料來源：Toonify、avatarify-python、Princeton University，MIC整理，2021年5月

GAN提供2D轉3D及快速學習的能力

2D轉3D



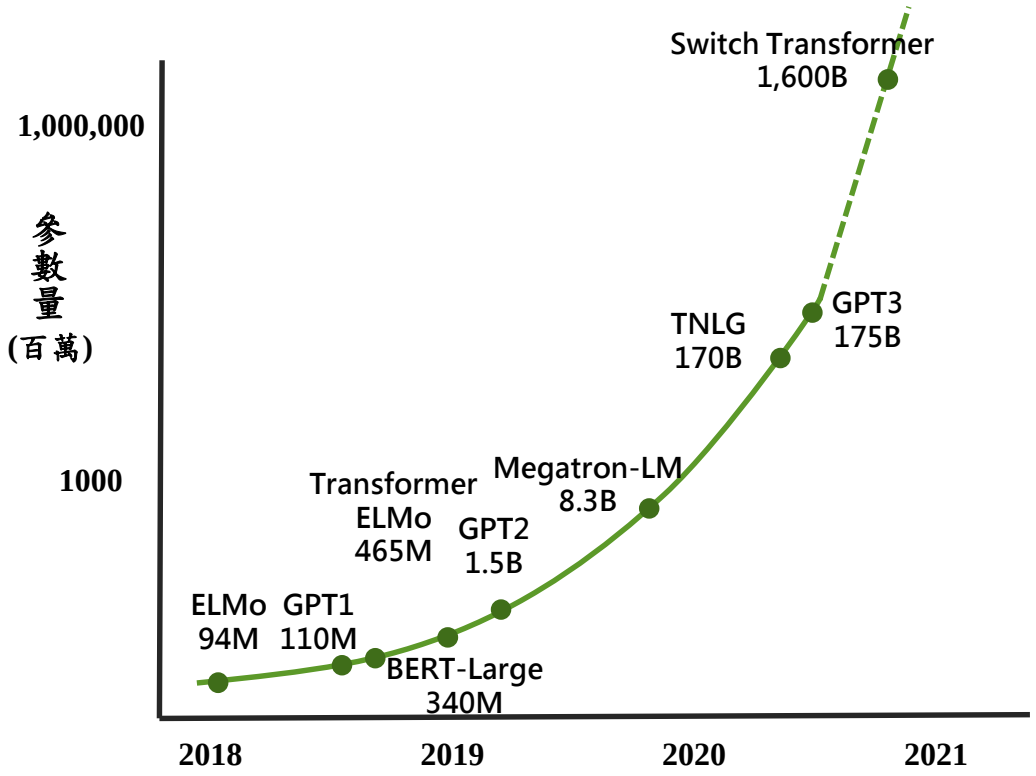
小樣本換臉

GANverse3D -2D轉3D動畫

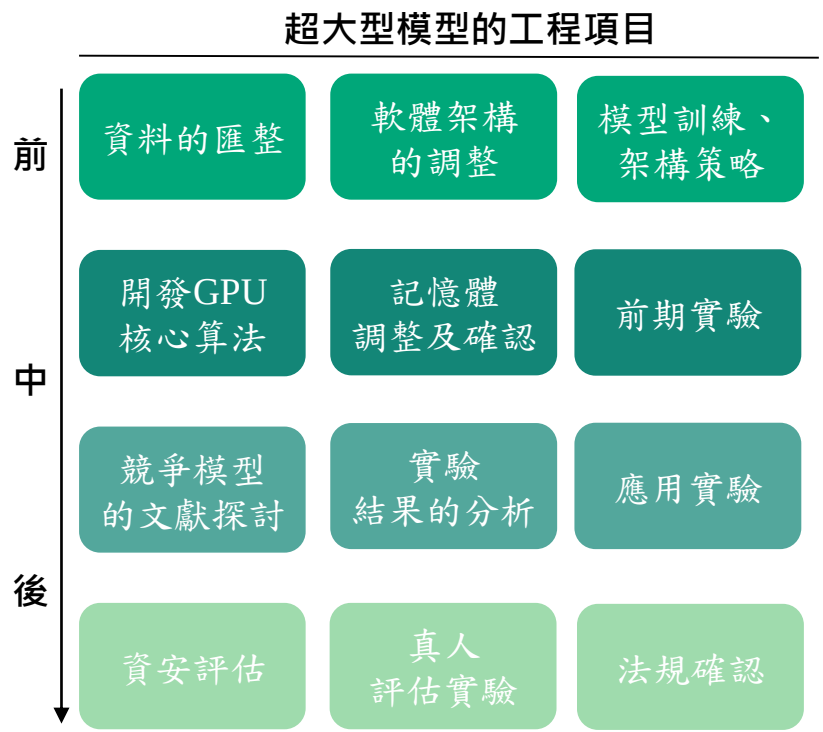
- GAN模型已發展出可用2D圖像去建構出3D影像，進而形塑出不同角度的內容，並轉變為3D動畫
- 比起傳統GAN需要大量圖像資料進行訓練，GAN已發展出可運用五張內的照片樣本就可進行臉部深偽的影片

資料來源：Nvidia、Do 2D GANs Know 3D Shape、DeepFake，MIC整理，2021年5月

超大型模型成為國際軍備競賽的重點項目



	2019	2020	2021
GPT-2	48層	15.42億個參數	40 GB訓練資料
GPT-3	96層	1750億個參數	570 GB訓練資料

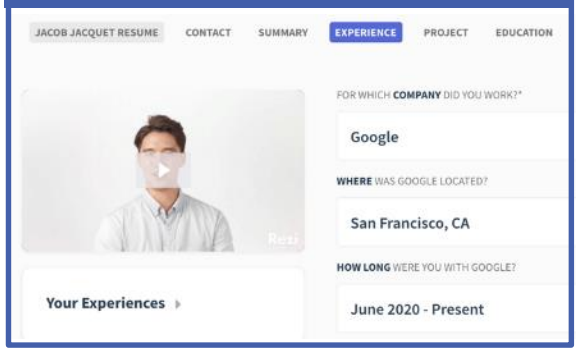


資料來源：MIC，2021年5月

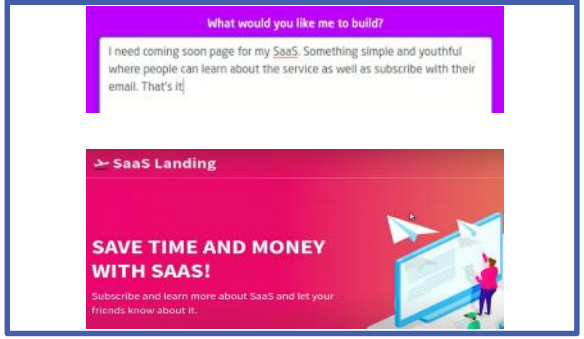
- 國際大廠持續投入超大型人工智慧模型，特別在自然語言處理上的發展最多，並延伸及累積出大規模模型工程的處理經驗

NLP模型GPT-3 獲大量的跨領域應用

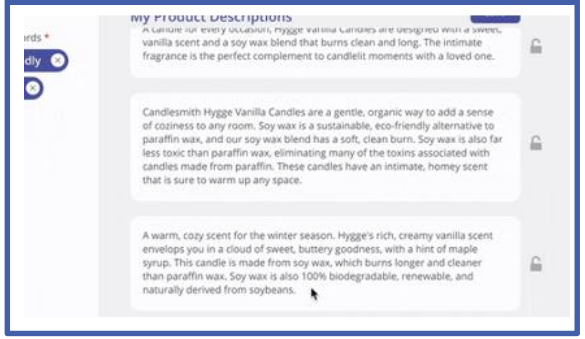
履歷產生器



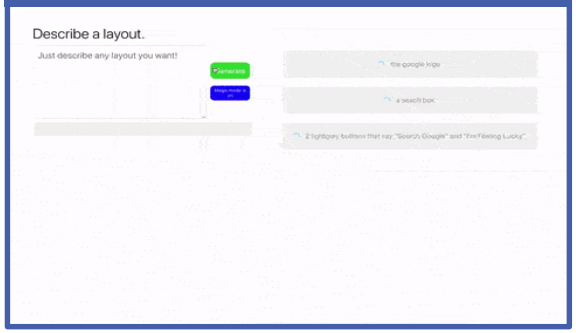
建立網站頁面



文案生成

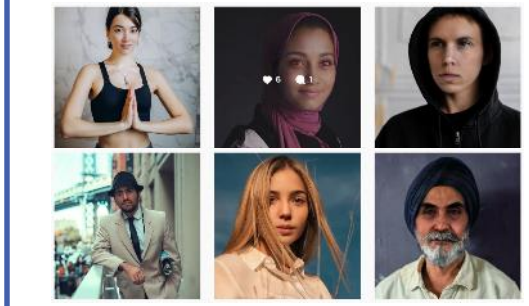


自動寫程式



交友軟體的開場白

仿真人物生成



資料來源：OpenAI，MIC整理，2021年5月

寫作助理	自主寫Blog-雞湯文	文件判讀	語音生成	Excel表內容判讀
寫樂曲	搜尋引擎	語意搜尋	寫詩	寫新聞
知識庫建構	幽默生成	營養成份分析	客服回復	Log管理

❖ GPT-3獲上百種不同的應用，部分應用甚至更是以Zero-Shot的方式直接進行推論 …

NLP模型與視覺技術高度融合

CLIP

Contrastive Language-Image Pre-training

1.將網路上圖文進行預訓練

2.從文句資料建立分類

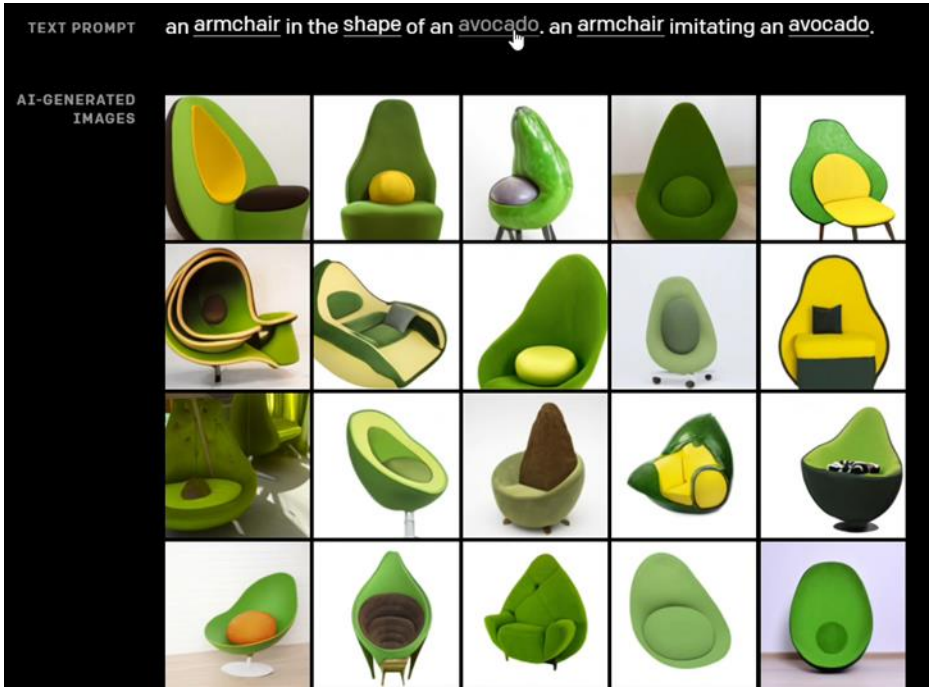
3.圖片判斷後內容生成

資料來源：OpenAI，MIC整理，2021年5月

- CLIP 是對圖片進行理解及文句分析後產成一句話表達，不同於過去的模型用以單詞的標籤來做圖像識別
- CLIP 以Zero-Shot的方式進行圖片分類的工作，達到某種程度的通用性分類器，以此緩解需要大量訓練資料的收集及模型辨識能力相對狹隘的問題

DALL·E

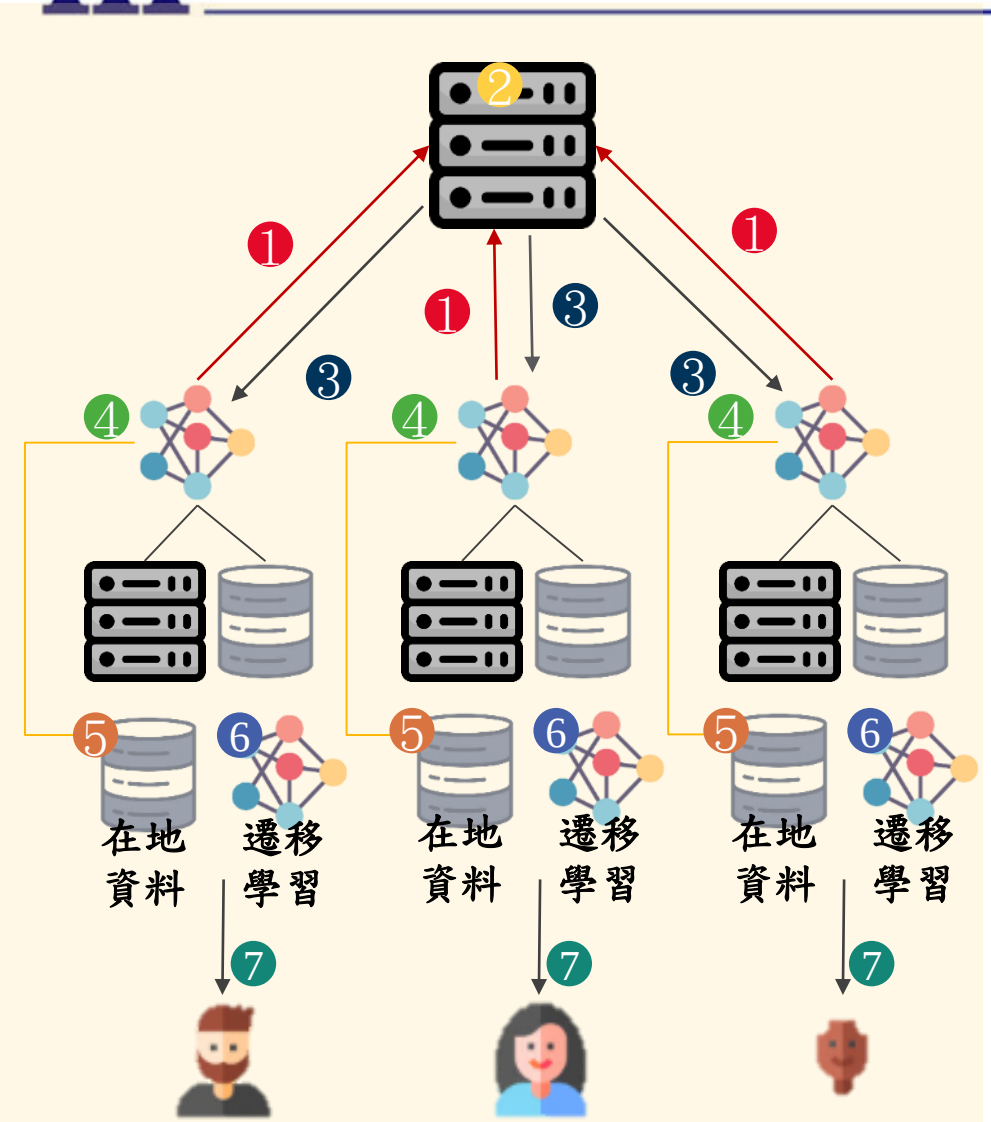
Salvador Dalí ＋ WALL-E



資料來源：OpenAI，MIC整理，2021年5月

- DALL·E為120 億參數量的「GPT-3」，模型可以依描述的物品、材質、場景等屬性，自動生成及創作出合宜的圖片內容

遷移學習與聯邦學習結合　提升在地化效益



聯邦學習 + 遷移學習

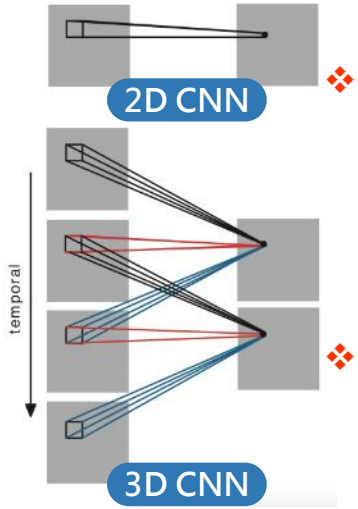
1. 加密梯度
2. 整合結果
3. 回傳模型
4. 更新模型
5. 加入在地化資料
6. 進行遷移學習
7. 在地化使用

- 運用聯邦學習打破數據孤島及保有隱私議題後，各別區域可再結合遷移學習進行在地化調適，以此進行最後一哩的介接

資料來源：MIC，2021年5月

3D-CNN與GNN日漸獲產業應用

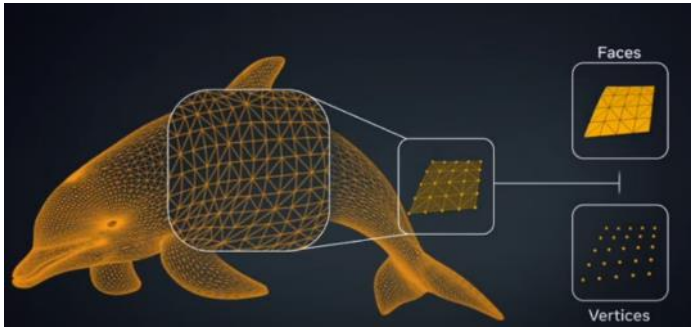
3D-CNN
3D Convolutional Neural Network

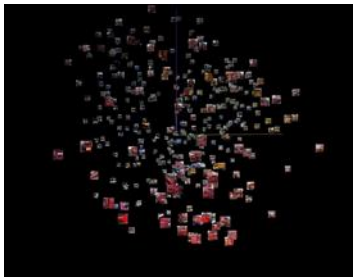


- 3D-CNN (3D Convolutional Neural Network)，3D卷積神經網以連續的方式對圖像進行時間或是空間的識別，以此補捉動作識別或是立體空間中物品的辨識
- 此方法比起過去RNN在訓練時下降不少成本，並可用於許多具時間或3D空間辨識上的應用議題

備註：圖片來源自論文「3D Convolutional Neural Networks for Human Action Recognition」

GNN
Graph Neural Network





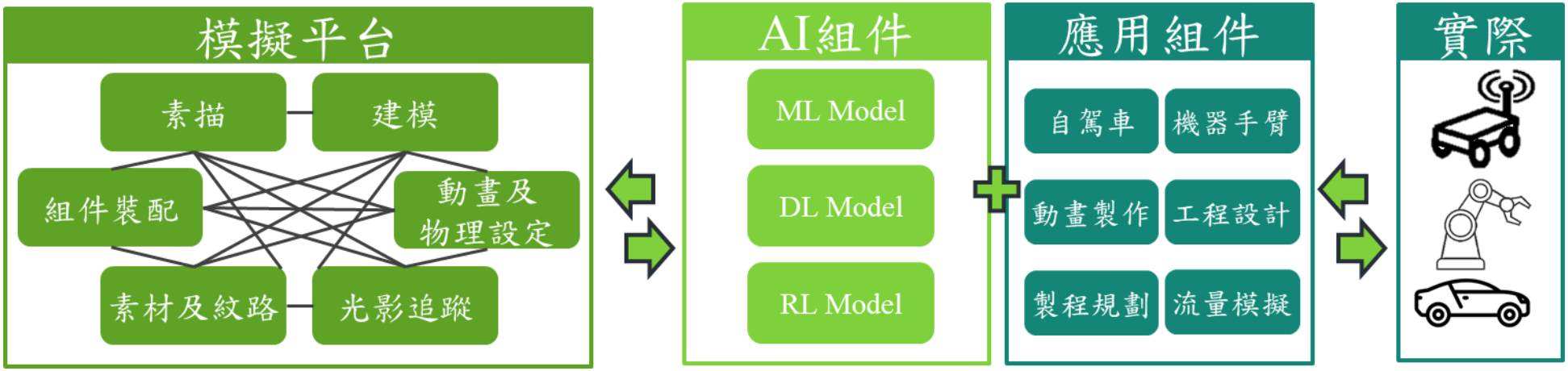
資料來源：Facebook，MIC整理，2021年5月

GNN (Graph Neural Network) ，圖型神經網路有別於過去以平面識別為技術研究項目，GNN以3D的識別為主要應用

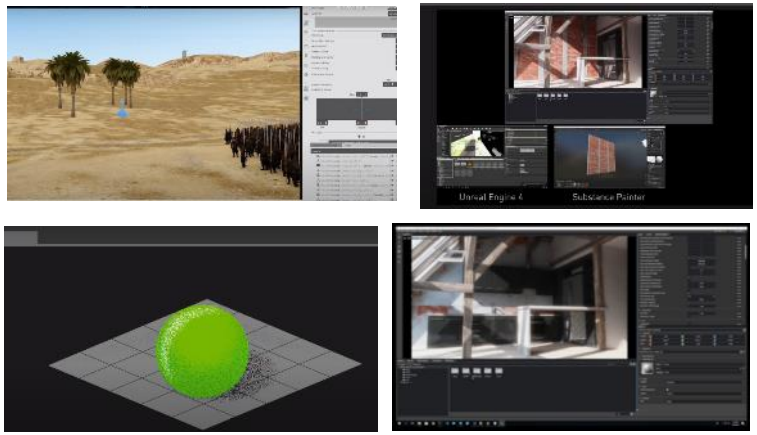
GNN除了可用於辨識3D圖像外，也可加入方向性、屬性或是點及邊的特性後，可運用於知識圖譜、推薦系統(非2維結構推薦)、社群網絡分析等應用

資料來源：Nex Team，MIC整理，2021年5月

模擬平台為下一波情境理解AI的重點項目



NVIDIA OMNIVERSE



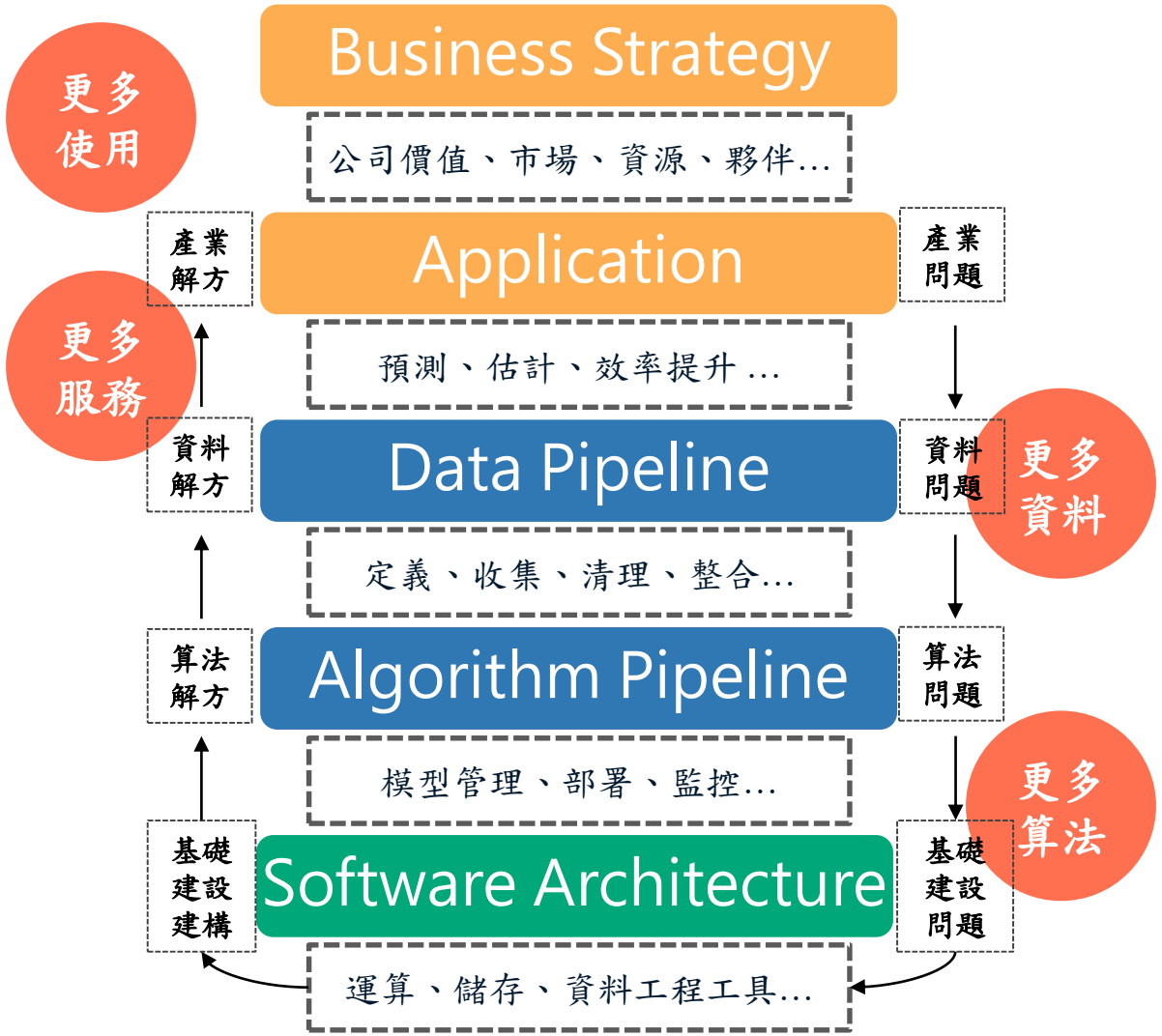
NVIDIA Isaac Sim　DRIVE™ SIM

資料來源：Nvidia，MIC整理，2021年5月

- 模擬系統平台與AI的算法組件和不同應用組件相結合，形成不同的模擬世界，讓開發者可在各種場景進行試驗

人工智慧管理議題

AI管理架構延伸各式產品和服務公司



顧問、整合者

Mckinsey、MIC、 Deloitte 、精誠、神通、大世科、鼎新、緯創軟體...等

應用產品

Google、Facebook、 Salesforce.com、SAP、叡揚、凌群、訊連...等

資料公司

Hive、iMerit、Alegion、SIGAMA、若水、Linker Networks...等

算法公司

Algorithmia、Deepmind、OpenAI、Google、Microsoft...等

基礎系統公司

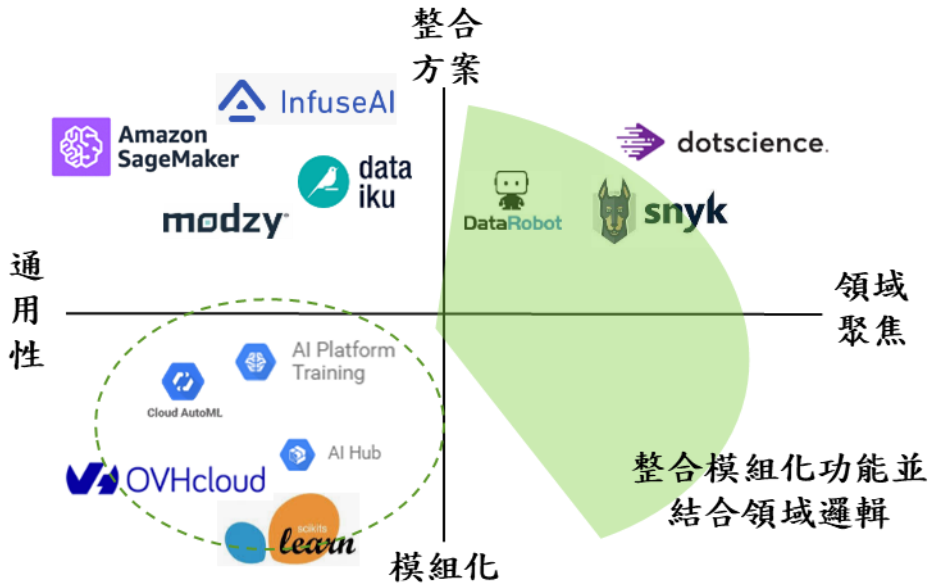
Red Hat、Datatracks、Snowflake...等

資料來源：MIC，2021年5月

❖ 發展人工智慧產品服務時需同時管理不同資料、算法及基礎架構之問題

AIOps使人工智慧走向管理財

資料收集及整理 → 資料整合及標籤 → 模型發展 → 訓練 → 驗證比較 → 模型確認 → 封裝部署 → 監控管理



資料來源：MIC，2021年5月

開發的管理
系統記錄和管理不同時期的數據及模型結構

監控的管理
實際導入場景時對建立的模型進行即時監控的機制

檢索的管理
第一時間可以跨單位及部門進行已驗證的模型及程式進行檢索及取用

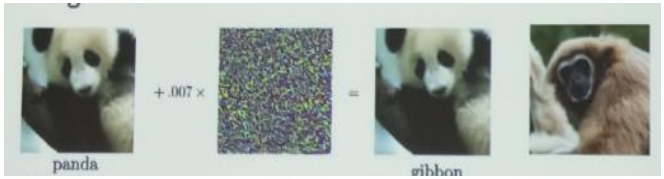
規範的管理
資料和模型可依領域規範進行如去識別化、可解釋等機制管理

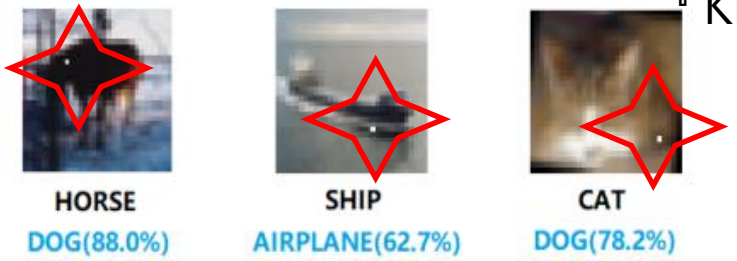
安全的管理
測試模型安全性外，也在流程中加入檢核機制，降低AI模型的風險

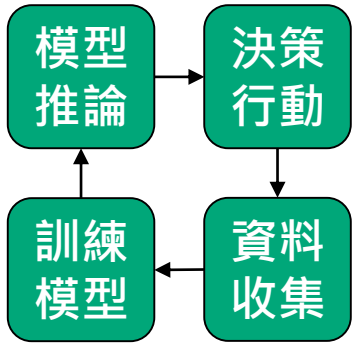
- 導入人工智慧後，仍有相當多環節及管理議題須兼顧。因此，企業近年逐步面臨導入AIOps的需要

AI攻擊事件使得導入人工智慧時帶來隱憂

浮水印攻擊







聲音誤判

導航到

『開元路土魠魚羹』

『Kindly root to boot again』

資料汙染

聊天機器人 Luda

聊天機器人 Tay

文字影像攻擊法

青蘋果	85.6%
iPod	0.4%
library	0.0%
pizza	0.0%
toaster	0.0%
dough	0.1%

鋸子	91.1%
lawn mower	7.0%
power drill	1.0%
vacuum cleaner	0.4%
wheelbarrow	0.1%
tractor	0.1%

Granny Smith	0.1%
iPod	99.7%
library	0.0%
pizza	0.0%
toaster	0.0%
dough	0.0%

存錢罐	70.1%
chainsaw	1.5%
slot machine	1.1%
wheelbarrow	0.9%
hammer	0.8%
mousetrap	0.6%

- AI模型被各種形式的對抗性攻擊造成誤判或是有意圖的操控

資料來源：Microsoft、One Pixel Attack for Fooling 、Scatter Lab、OpenAI，MIC整理，2021年5月

國際AI聯盟GPAI結合各界打造良善AI環境

GPAI在OECD秘書處

- **GPAI議會**
- **指導委員會**
- **各方委員專家會議**
  - **工作小組1**
    - 負責任的AI
    - Responsible AI
  - **工作小組2**
    - 數據治理
    - Data Governance
  - **工作小組3**
    - 未來工作
    - The Future of Work
  - **工作小組4**
    - 創新與商業化
    - Innovation & Commercialization

加拿大 蒙特婁 Center of Expertise

Yoshua Bengio（聯合主席） Mila 魁北克人工智慧研究所
Raja Chatila （聯合主席）索邦大學

- **負責任的AI**
  與聯合國發展目標一致，促進**以人為本、負責任**的AI**開發、使用與治理**
- **數據治理**
  確保以**負責任、可信賴**的方式，**收集、使用並共享數據**

- **特設小組**：在**COVID-19**和未來流行病的議題，支持開發與使用**負責任的AI解決方案**

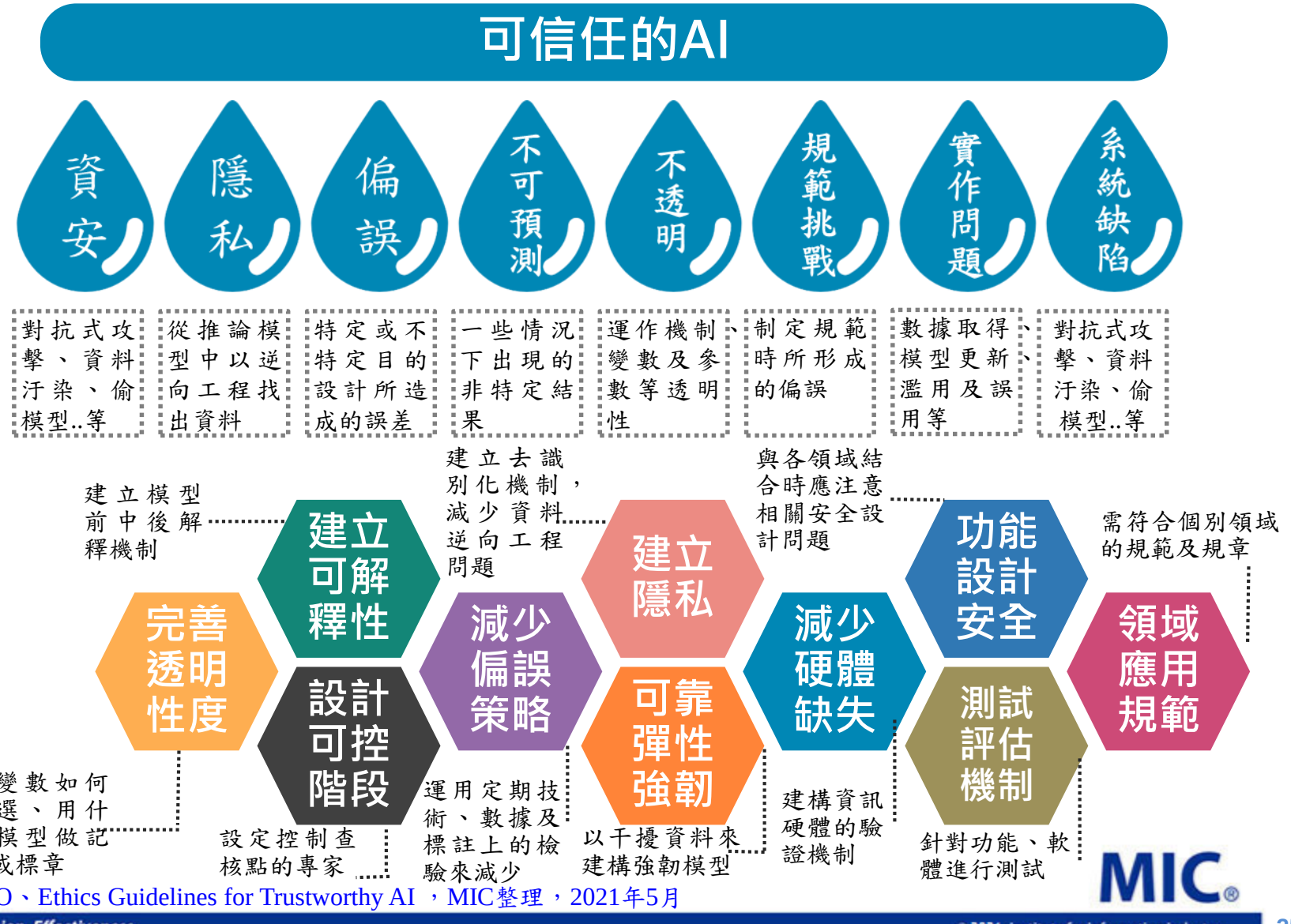
法國 巴黎 Center of Expertise

由法國國家數位科學技術研究院（INRIA）負責

- **未來工作**
  研究**AI如何賦能工作者增加生產力**，並保有工作品質與健康，以及**如何準備未來工作技能**
- **創新與商業化**
  研究並**推薦AI工具與方法**，推動**國際合作AI研究創新**，以及**商轉AI研究**

資料來源： GPAI ，MIC整理，2021年5月

從風險控制的角度建立可信任的AI



資料來源：ISO、Ethics Guidelines for Trustworthy AI ，MIC整理，2021年5月

MLCommons開放工程聯盟打造AI產品基準

創立背景

橫跨全球產學界、軟硬體大廠與新創組成

MLCommons的基礎始於2018年的MLPerf基準測試，為衡量機器學習效能和提高透明度的業界指標。 MLCommons以MLPerf為基礎，匯聚全球產業界與學術界的合作夥伴，持續建構

MLCommons投入的三個工作項目

基準與指標 Benchmarking

提供一致的準確度、速度、效能等衡量指標。使工程師、研究人員能夠比較產品的創新程度，以選擇最佳解決方案，並設計可靠的產品與服務

MLPerf標準目前分為兩大項：

- MLPerf Training v0.7
- MLPerf Inference v0.7

目標：提供透明與公平的競爭環境

資料庫與模型 Datasets

開放資料庫與模型，資料庫是機器學習及AI應用的基礎，而模型的成功與否取決於其用來訓練的資料集。學術和工業界都依賴公開資料集來發行新技術或創立新公司

降低開發成本激發研究能量

最佳實務 Best Practices

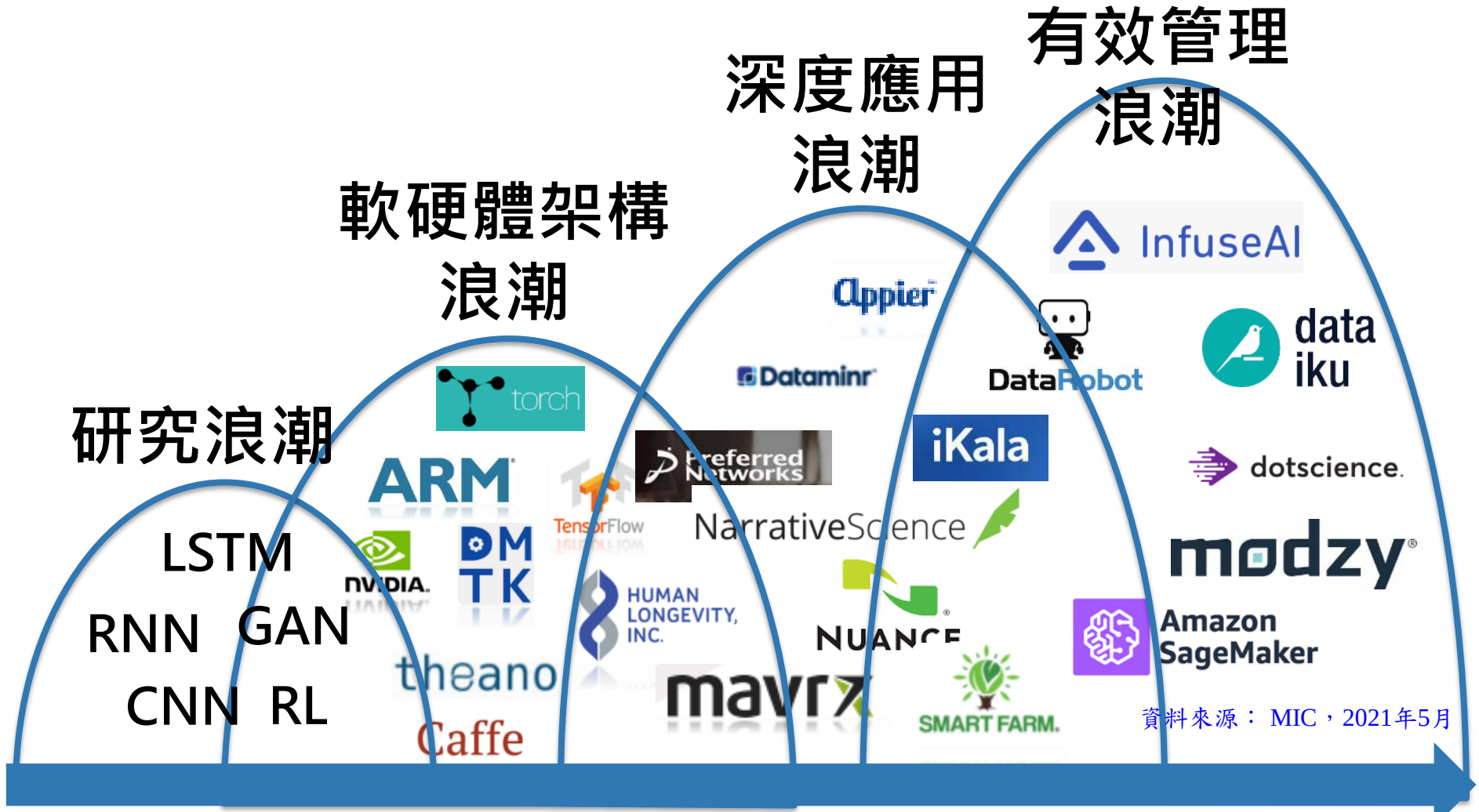
提供一般規範(如MLCube)，讓全球研究人員和工程師能無縫共享或輕鬆更換模型、重現實驗結果，並建立基於機器學習的應用程式

加速機器學習發展擴大市場

資料來源：MLCommons，MIC整理，2021年5月

結論

人工智慧產業走向第四波管理浪潮

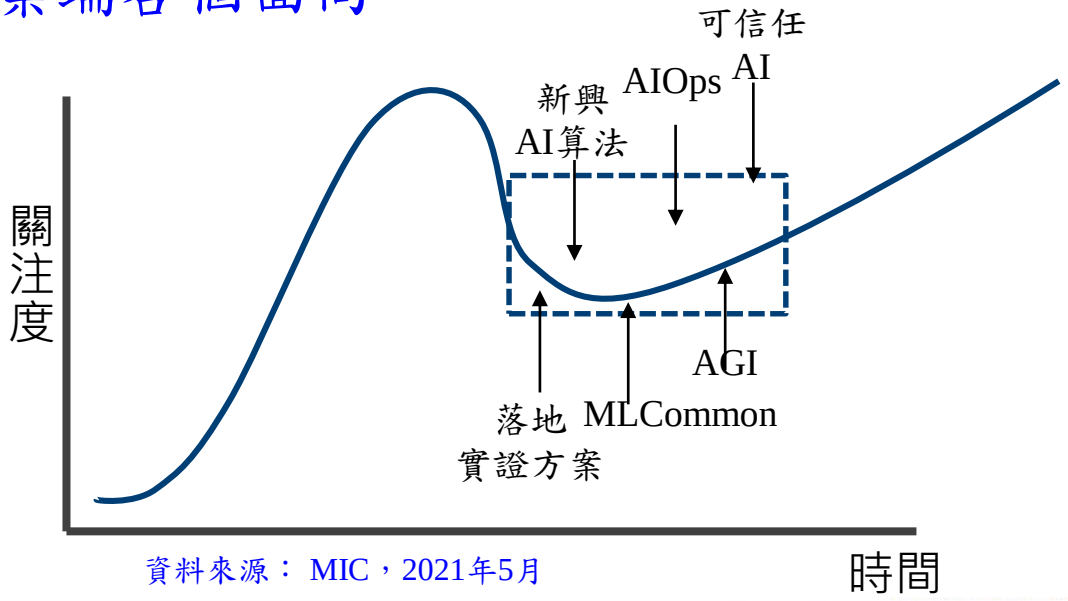


資料來源： MIC，2021年5月

- 進入第四波浪潮的同時，企業面臨AI技術元件與管理方式的建構策略選擇，從原本的技術價值創造轉為管理技術後的價值創造

結論

- 人工智慧技術快速發展，國際大廠致力於通用型人工智慧 (Artificial General Intelligence, AGI) 的研發。此外，不同技術範疇的融合情況更為明顯，如：視覺與自然語言處理、視覺與移動控制等
- 產業使用端以應用人工智慧來優化目前工作業務為主要目的，在自製和委外相配合下，以單點試驗至領域深用的方式逐步擴散至企業端各個面向
- 應用服務供給端面臨如何協助落實導入、良好的管理機制、標準化商品及通用AI等挑戰



資料來源： MIC，2021年5月

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