

生成式AI應用與管理趨勢

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

2024.04.24

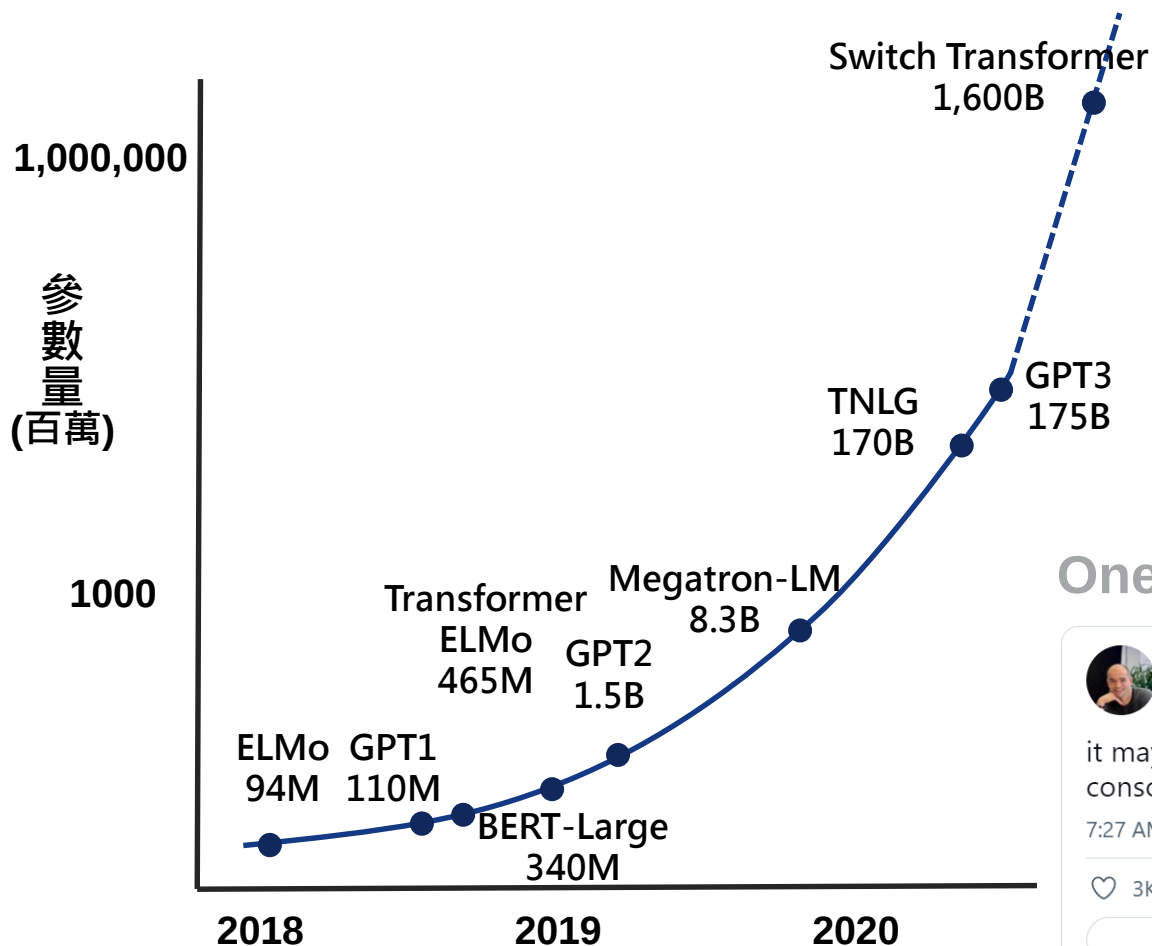
簡報大綱

- 生成式AI技術源起及生態
- 生成式AI新興應用
- 生成式AI管理與安全
- 結論

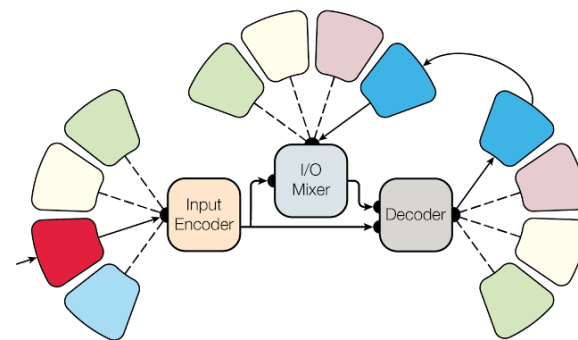
生成式AI技術源起及生態



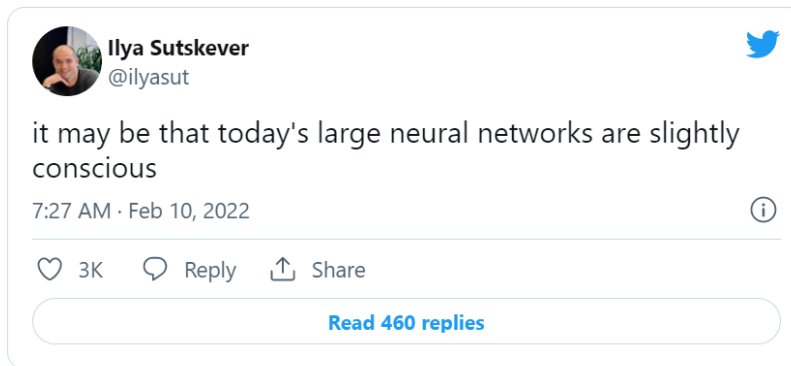
大型語言模型帶來模型具“多模態”能力



資料來源：MIC · 2024年4月



One Model To Learn Them All

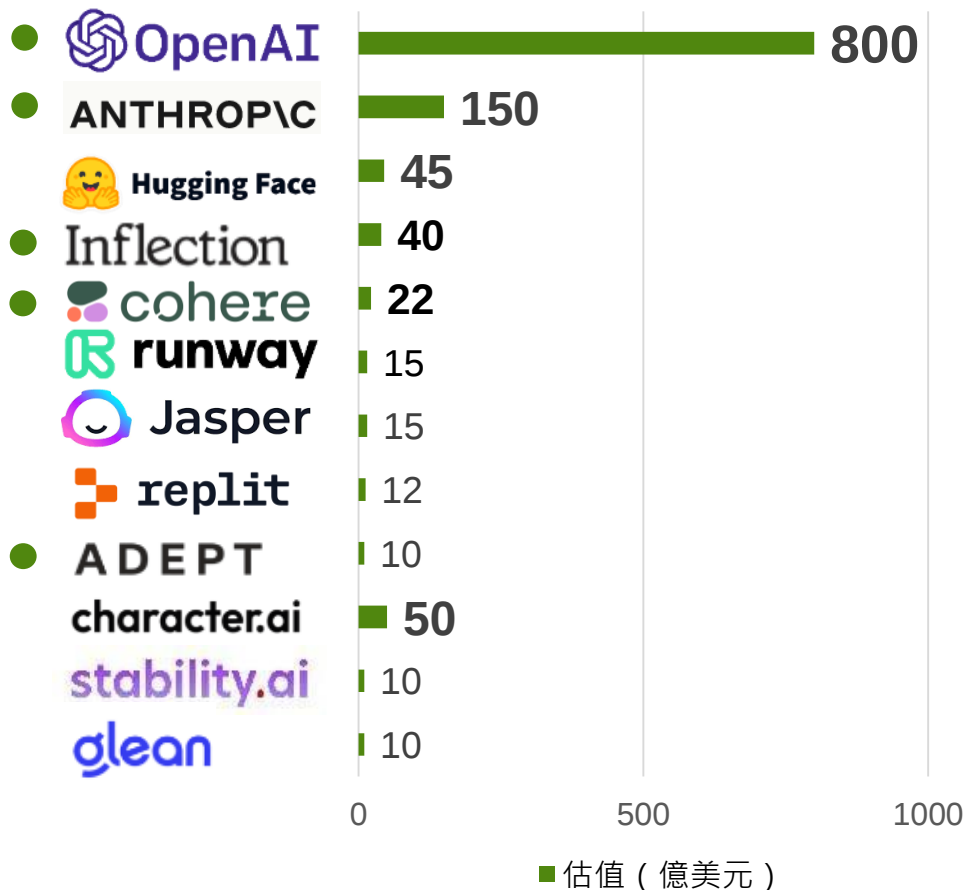


- OpenAI 的首席科學家 Ilya Sutskever 在 Twitter 發文表示提到：「今天的人工智慧的大型神經網絡可能已開始有個人意識」
- 多模態模型形成一個單一大的基礎模型可以看得懂、聽得懂、讀得懂...等綜合能力



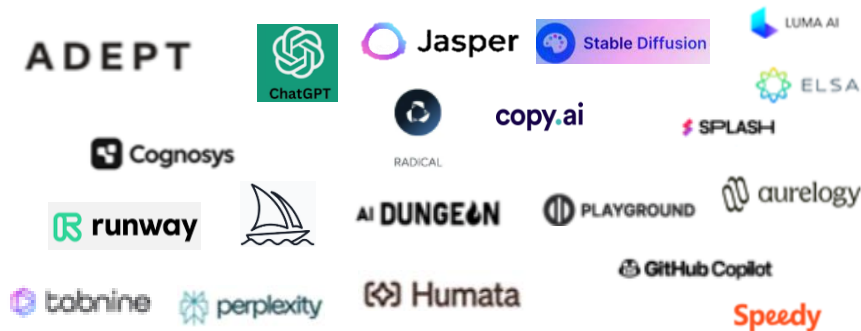
生成式AI投資及廠商家數大幅增加

生成式AI新創估值排行



資料來源：CBInsight · MIC整理 · 2024年4月

355間以上生成式AI新創募資階段

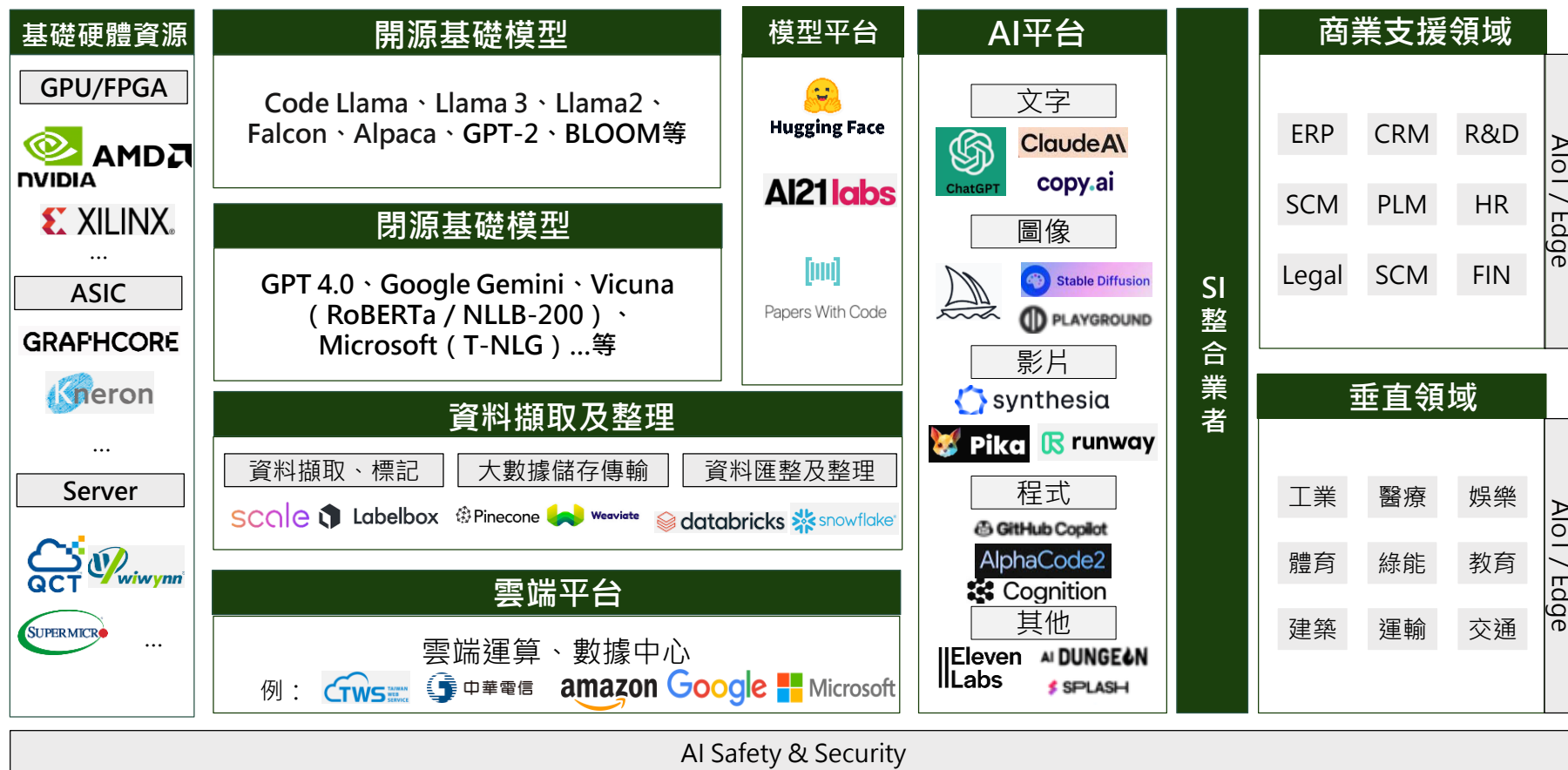


● 生成式AI快速發展，在投資資金大幅提高下，也造就生成式AI的市場



生成式AI再次疊化AI產業生態參與者

- 生成式AI的帶動下，整體AI產業生態再次進行角色上的位移，其中在開源 / 閉源模型庫、基礎模型的開放介接成為新一波應用的重要基礎
- 此外，也帶動新一波AIGC的應用平台的發展，帶來生成文字型、圖像型、影片型或是程式型的生成



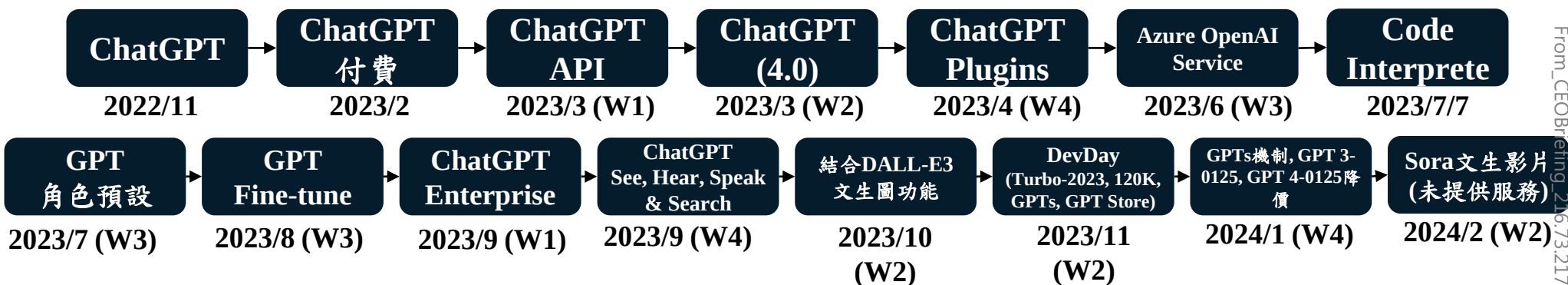
備註：廠商僅擷取部分

資料來源：MIC · 2024年4月

生成式AI新興應用



OpenAI推出ChatGPT後疊加不同服務衝擊全產業



Plug-Ins & Code Interpret

- Web Connected
- Email Reading
- Website Interaction
- Tool Combination (ex. Zapier)
- File Upload (CSV, PDF)
- KM System Upgrade
- Image Explanation and Change
- Plugin connect Plugin....

DALL-E3



GPTS



Sora



資料來源：OpenAI · MIC整理 · 2024年2月



Prompt基礎設定

● 目的和做什麼

- ◆ 是一位部長要去演講....
- ◆ 重寫、總結、翻譯...

● 情境、上下文

- ◆ 你可以先看看相關的資訊.....(附上新聞稿...)

● 範例

- ◆ 例如：。 。 。 。

● 角色設定/請它創建角色

- ◆ 請你當成是你GPT4 / 產業分析師
- ◆ 像彼得.杜拉克、孔子

● 閱讀/受眾對象

- ◆ 請對四歲/國中/學者進行說明...

● 語氣、風格

- ◆ 活潑、創意、

● 翻譯語系

- ◆ 中文、繁體中文
- ◆ #zh-TW

● 希望產出結果的形式

- ◆ 用表格、用心智圖、用Markdown

● 限定詞/反向詞

- ◆ 希望只在....
- ◆ 不要太學術、不要用什麼用語

● 情緒Prompt

- ◆ "This is important to me."
- ◆ "For World peace."
- ◆ "Please think step by step."
- ◆ "Are you Sure?"

● 用英文

- ◆ In English.....

資料來源：MIC整理，2024年4月



ChatGPT 3.5 vs ChatGPT 4.0的理解能力有差異

ChatGPT 3.5

Default (GPT-3.5)

SI 請問東方美人怎麼泡？繁體

 泡妞是一個相當主觀的過程，因為每個人都有不同的喜好和個性。不論是東方或西方的美人，建立成功的關係都需要尊重、誠實和理解。以下是一些泡妞的基本原則，但請記住，最重要的是要尊重對方，並將關係建立在共識和互相喜愛的基礎上：

1. ****認識對方****：首先，你需要認識她，了解她的興趣、價值觀和生活方式。與她交談，試著了解她的想法和感受。
2. ****禮貌和尊重****：無論何時都要保持禮貌和尊重。對待她，尊重她的意見，不要冒犯或對她粗魯。

ChatGPT 4.0

SI 東方美人怎麼泡？

 東方美人，又稱為“東方美人茶”或“白毫烏龍”，是一種台灣的獨特烏龍茶。這款茶受到小綠葉蟬咬噬後，茶葉會產生一種特殊的香氣，這也是東方美人茶的獨特之處。下面是泡製東方美人茶的步驟：

1. **茶具準備**：最好選擇紫砂壺或瓷壺。當然，杯子和茶巾等泡茶用具也都需要准备好。
2. **茶葉量**：依據您的茶具大小調整，但一般來說，約5克茶葉對應150ml的水。
3. **熱水準備**：最好使用沸騰後稍微冷卻到約85°C-90°C的熱水。
4. **熱茶具**：先將熱水倒入茶具中，讓茶具加熱，然後將水倒掉。
5. **放入茶葉**：將東方美人茶葉放入茶具中。



我的英語家教 – ChatGPT (1/2)

- **Prompt**：請當我的英語家教，和我練習不同主題的對話。請您每次回應不要超過5句話。當我說「開始」時,你就問我今天要討論什麼主題，然後就用英文與我對這個主題進行英語對話。當我說「結束」時，請你針對我和你對話的內容再瀏覽一遍，然後看我有什麼語法說錯的地方，請幫我逐句指正，並且告訴我兩個表達的方式

SI: I think the nation trade department needs to negotiate different products and try to balance the import and export of the value and also try to keep the right price and the right cost to their country. The key issue is about

AI: Yes, managing the balance of imports and exports is essential for a country's trade health. Making sure the prices and costs are favorable ensures a stable economy. The "key issue" you were about to mention is intriguing. What do you think that key issue is when it comes to international trade negotiations?

SI: Hmm, it's a good question. It's hard to identify, but sometimes, from an easy way, we need to focus on the price or want to exchange something from your nation's view.

AI: Absolutely. Each nation has its own priorities and interests when it comes to trade. While the price of goods is a significant factor, other considerations like technology transfer, intellectual property rights, employment opportunities, and environmental concerns can also play crucial roles in negotiations. It's a complex web of factors, and finding a balance that benefits both parties can be challenging but is essential for long-term, sustainable trade relationships. What do you think are the long-term impacts of successful trade negotiations on a country's economy and its people?

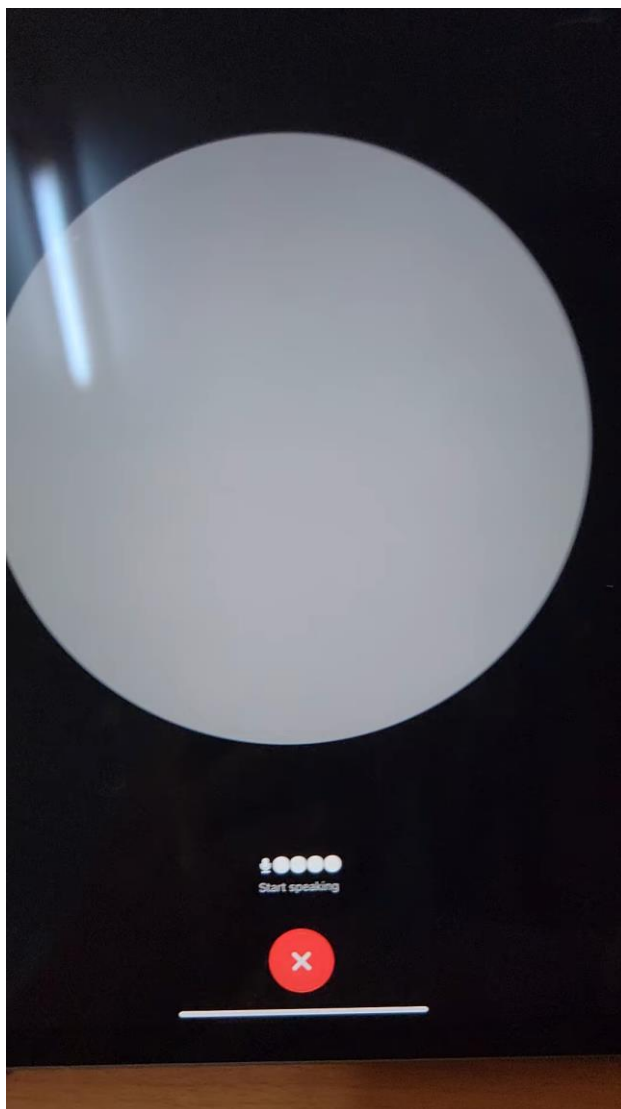
SI: 結束

AI: Alright, let's review our conversation:

- You said:** "how about we can talk about the economic"
 - Correction:** "How about we talk about the economy?"
 - Alternative:** "Can we discuss the economy?"
- You said:** "I can understand your meaning to dynamic economic" and "
 - Correction:** "I understand what you mean by the economic"
 - Alternative:** "I get what you're saying about the dynamics of the economy."
- You said:** "Oh yes, because if your country just provide, perhaps, semiconductor and people or other country cannot provide, the people will pay more money to buy your semiconductor in your nation."
 - Correction:** "Yes, if your country is the only provider of, say, semiconductors and other countries can't produce them, then people will pay more to buy those semiconductors from your country."
 - Alternative:** "Indeed, if only your country produces semiconductors and others don't, they'll pay a premium to get them from you."



我的英語家教 – ChatGPT (2/2)





ChatGPT – DALL-E3結合文生圖

SI You
生成三種圖，
1. 台北101
2. 捷運站
3. 植物圖騰-粗線條, 黑白圖



SI You
結合1及3圖.



資料來源：MIC整理，2024年4月

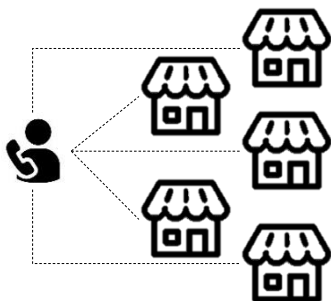


DigiBuild-自動詢價議價，快速掌握市場



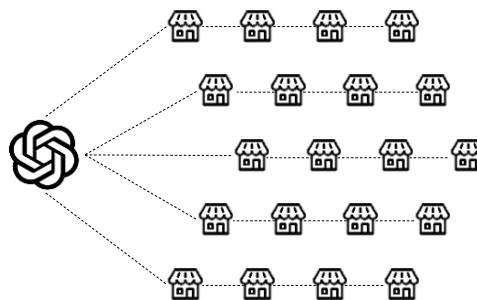
- DigiBuild 在 Y Combinator 支持下，運用 ChatGPT 引入建築材料供應商詢價，以此協助採購人員快速進行尋料、購料及議價的工作

Before

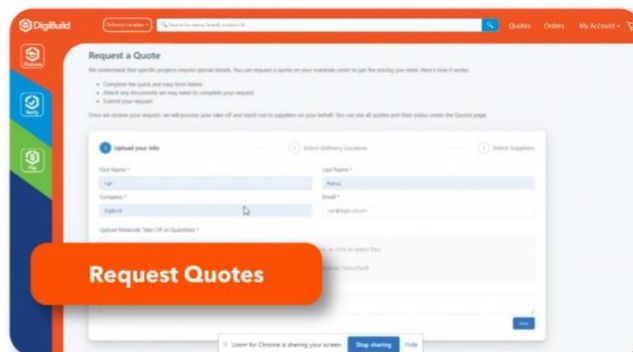
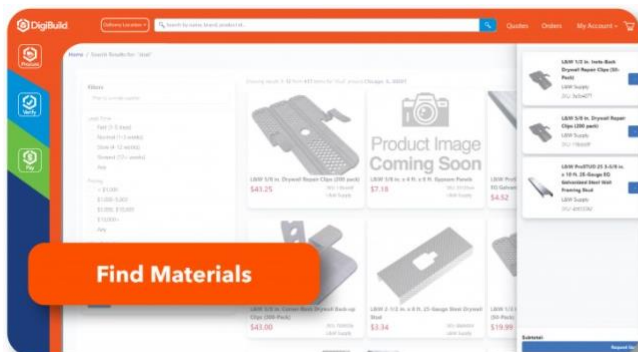


- 過去需數個小時才能聯繫到5-10家供應商

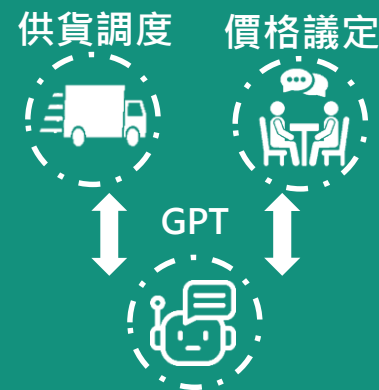
After



- ChatGPT可以在一分鐘與100家供應商進行溝通



功能描述



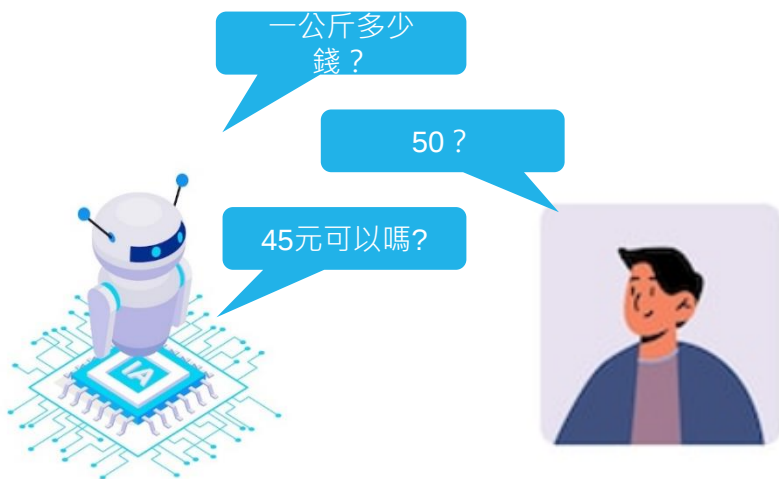
資料來源：DigiBuild · MIC整理 · 2024年4月



未來場景-機器人自動詢價

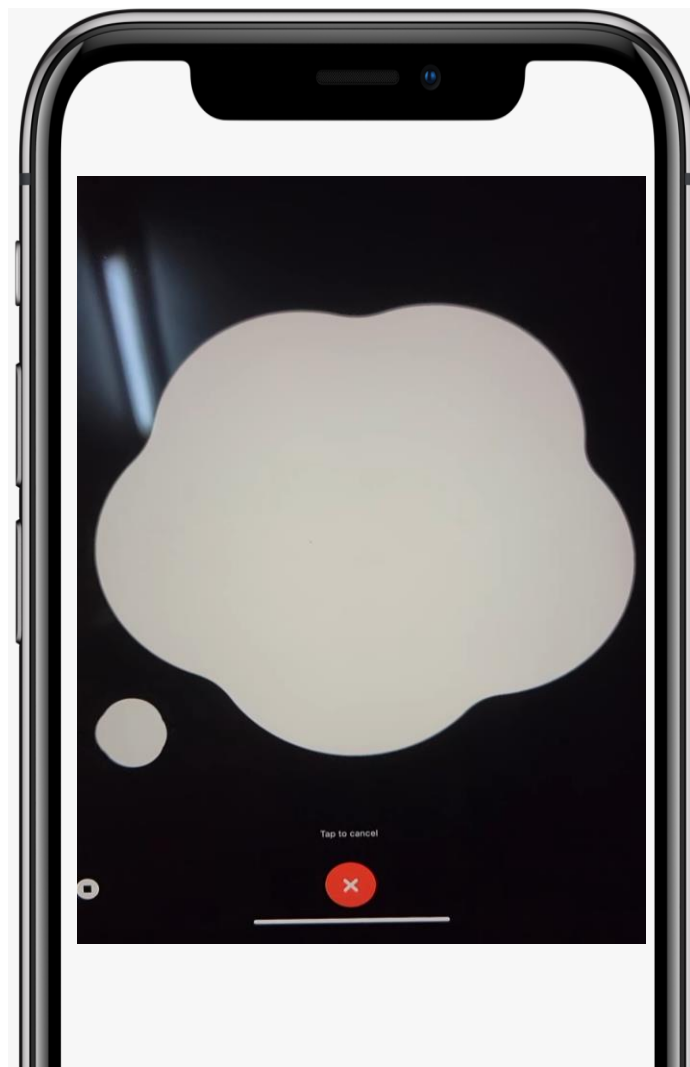
情境 / 任務 設定

- 機器人是採購人員
- 要求詢問塑膠顆粒每公斤多少台幣
- 價格不可以超過45元/公斤
- 有今年度到8月份的訂購價格記錄為參考



圖片來源：freepik

資料來源：MIC · 2024年4月





各種LLM功能用於工作流程中

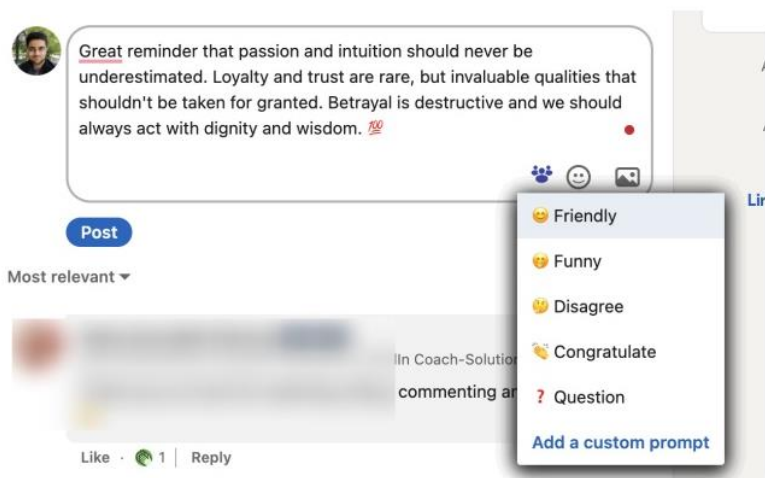
重點總結工具 - Transcript & Summary



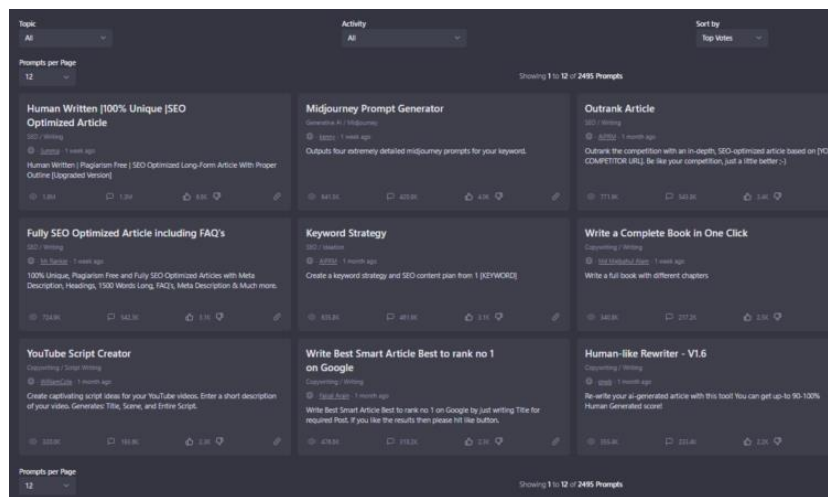
智慧即時翻譯櫃台 - 群創光電



協助回覆訊息 - Engage AI



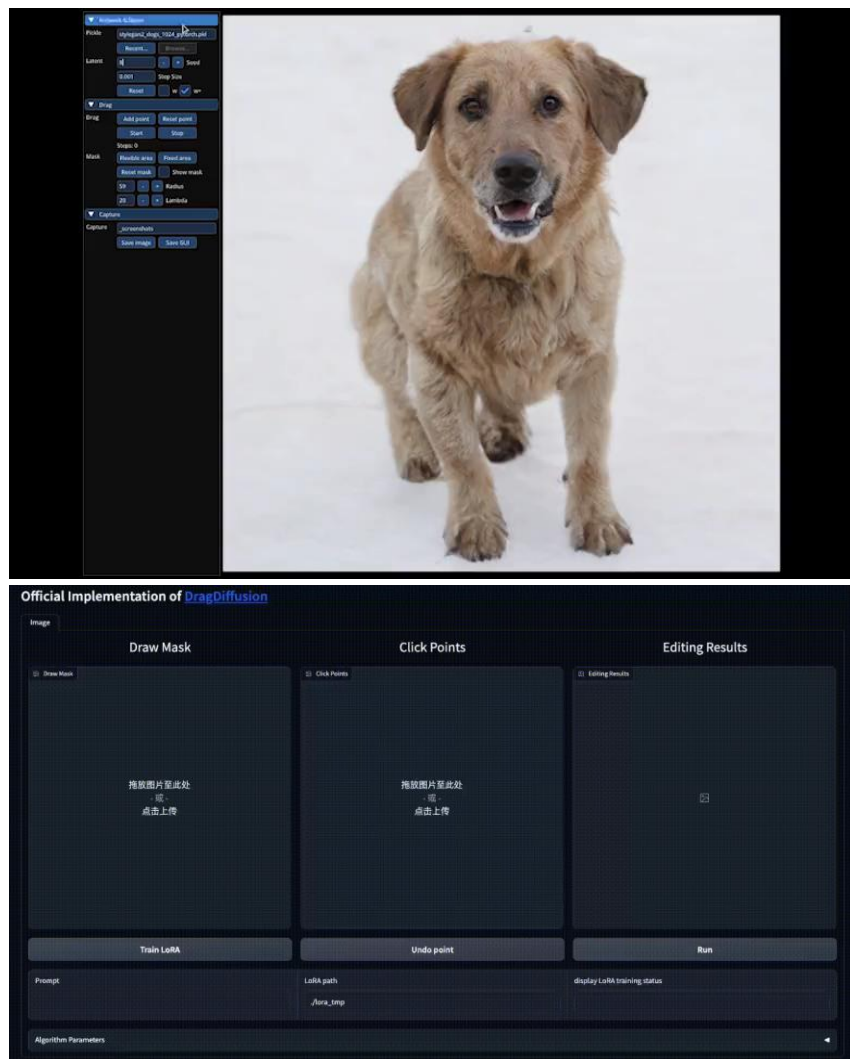
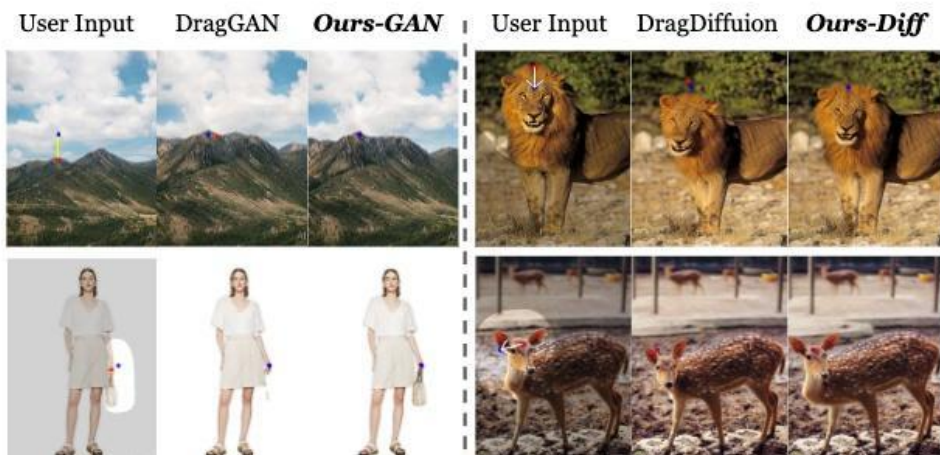
各種Prompt模組化 - AIPRM





拖拉修圖，大幅降低使用者編修成本

- DragGAN、DragDiffusion和StableDrag能夠創造新的圖像內容，以達到與使用者最直接想要的修改程度
- 使用者若想讓照片中的人物展現微笑、獅子轉頭，直接使用便可進行調整，還能產生相應的所需的圖像，並適當地改變



資料來源：DragGan、DragDiffusion、StableDrag，MIC整理，2024年4月

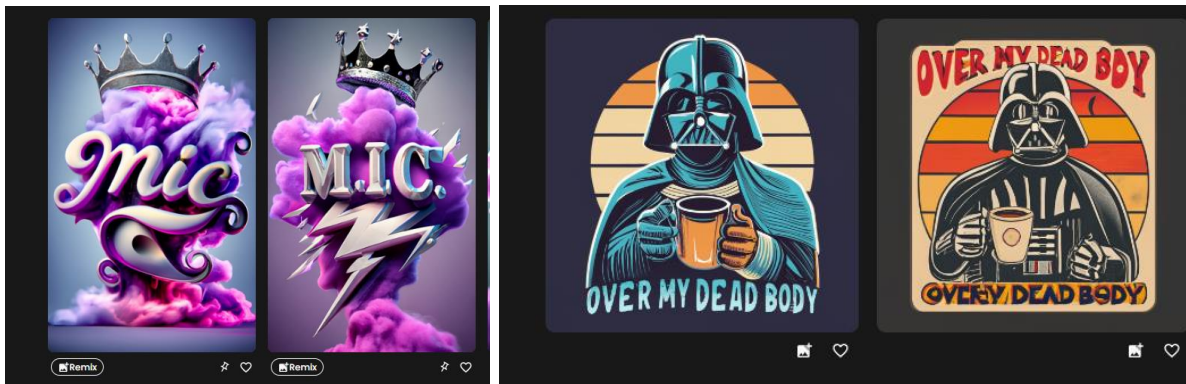


文生圖再變化，可給文字、可給定區域同步生圖



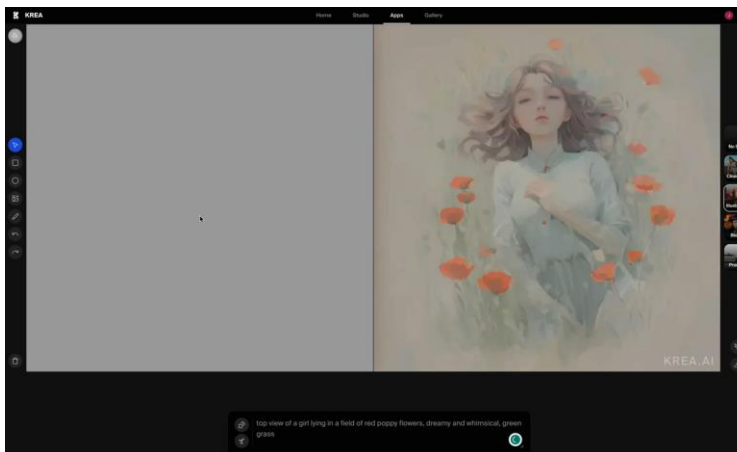
Ideogram AI

- Ideogram 最大的一個特色在於 Ideogram 可以很容易的把要生成的字放在圖中



- Krea AI 如現今的生成式 AI 公司，其功能包括常見的文生圖、AI Pattern 及 Logo illusions 等功能
- 近期因「同步生圖」的功能而備受使用者期待使用，有助設計人員大幅提升創意發展的效益

資料來源：Krea AI · MIC · 2024年4月





將內容、影片長度自動調整成其他語言

RASK

		English	Hey there! Here is a quick demo of Rask AI tool for video localization
		Spanish	Aqui hay una demostracion rapida de la herramienta Rask AI para la localizacion de videos
		German	Hier ist eine kurze Demo des Rask AI-Tool fur die Video Lokalisierung
		Arabic	فيما يلي عرض توضيحي سريع لأداة Rask AI لترجمة الفيديو.
		Japanese	ここでは、動画ローカライズ用AIツール Rask AI のデモを簡単にご紹介します。

HeyGen



資料來源：RASK.AI、HeyGen、MIC整理，2024年4月

Explainers

Education
Videos

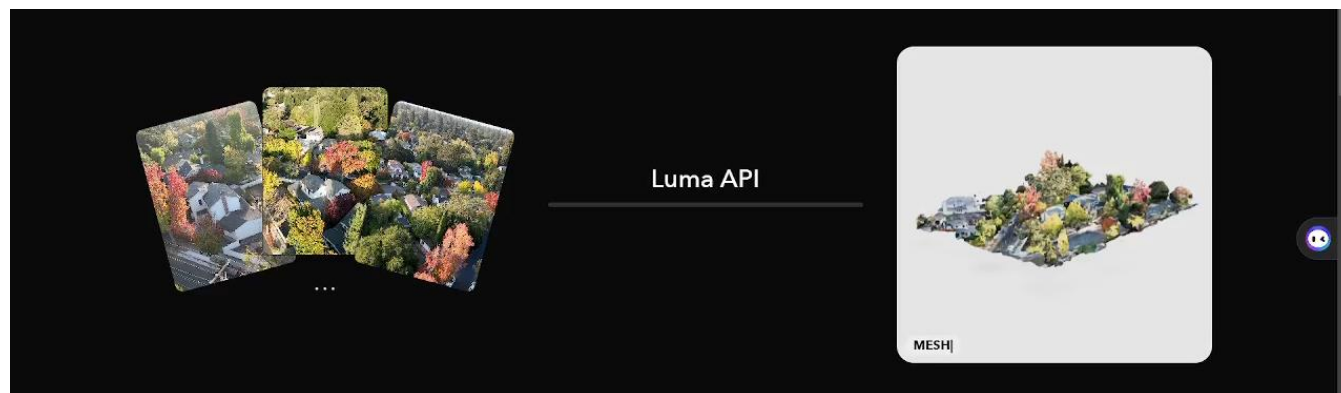
Marketing

Employee
Training

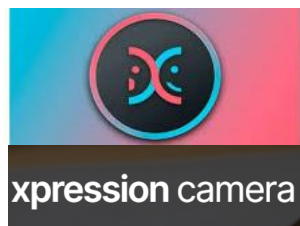
Content
Creation

Youtube
Multitracks

Video to 3D及Video to Fake – 影像生成技術獲實用

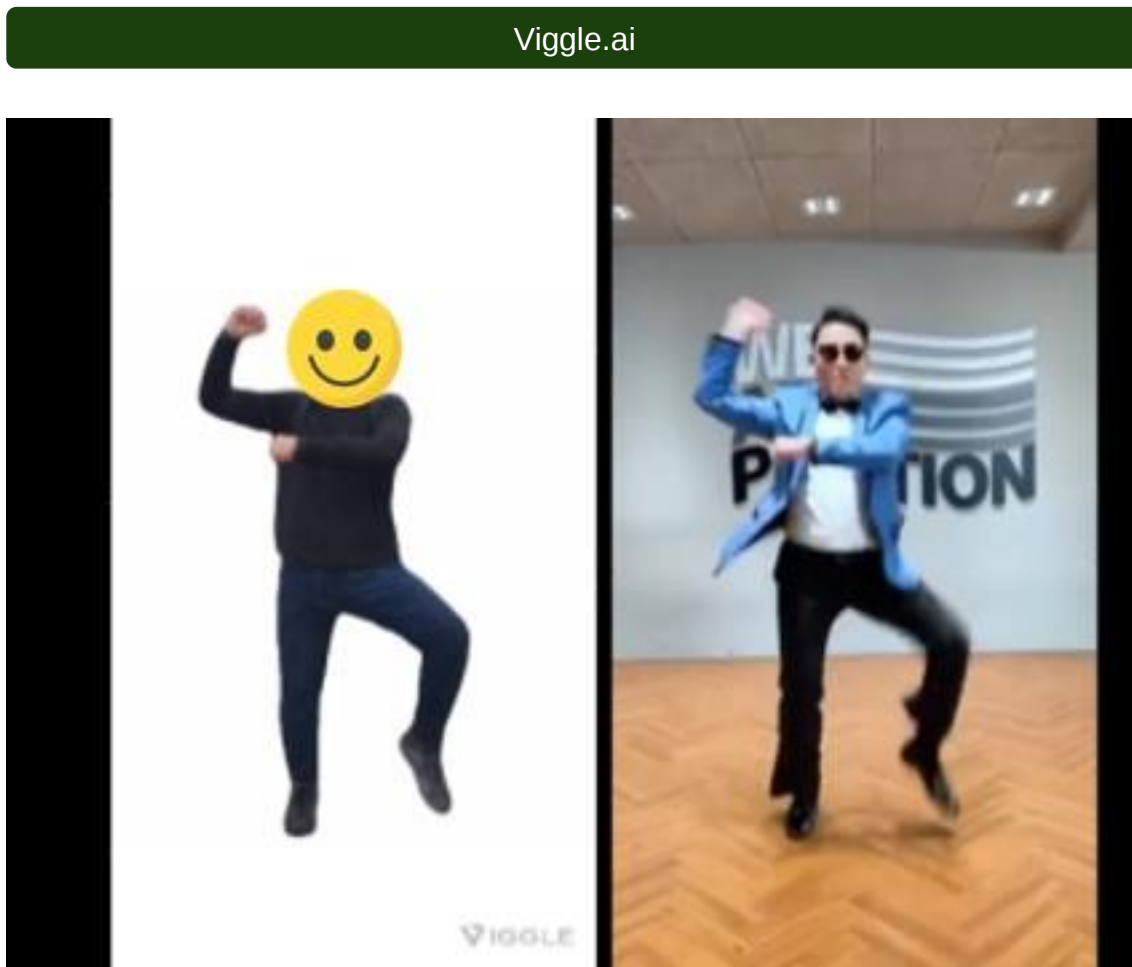
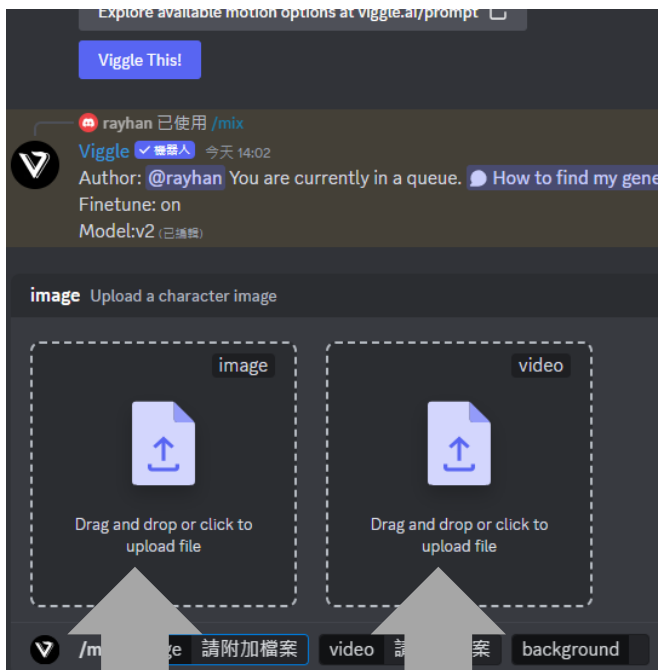


- Luma AI可運用影片來自動產生3D圖檔，並可與各個3D軟體進行串接應用



- Xpression camera可運用表情捕捉再加上臉部影像生成的技術，用於會議系統可用照片「代為」出席的應用

一張照片生成影片，自動補充肢體及服裝

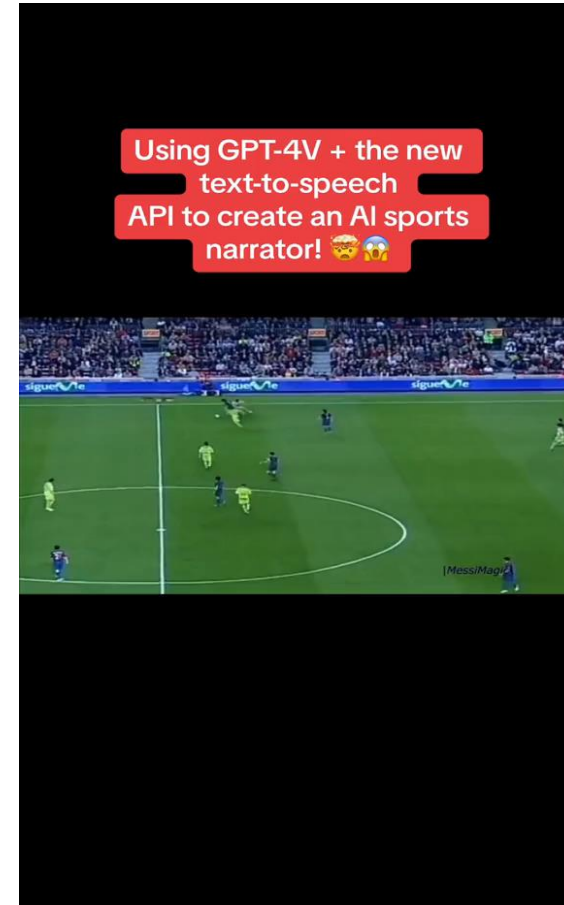
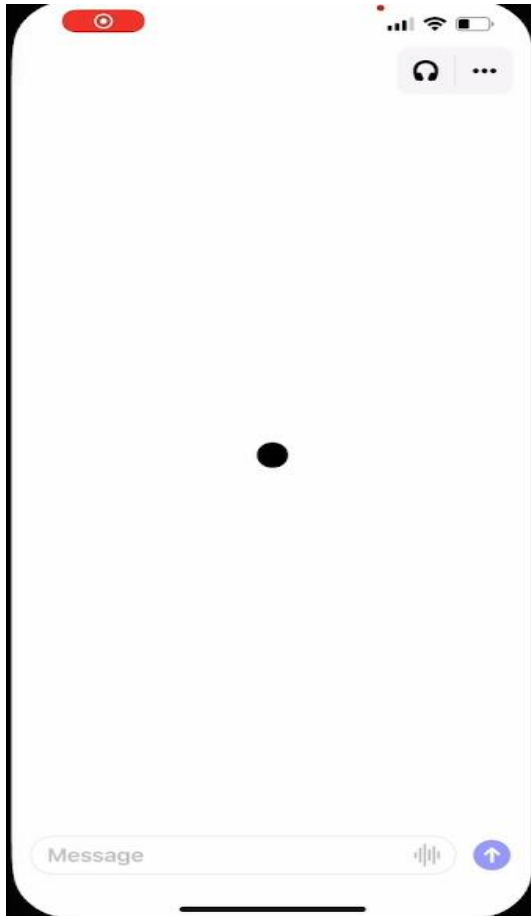


資料來源：Viggle.ai · 2024年 4 月



In the Near Future

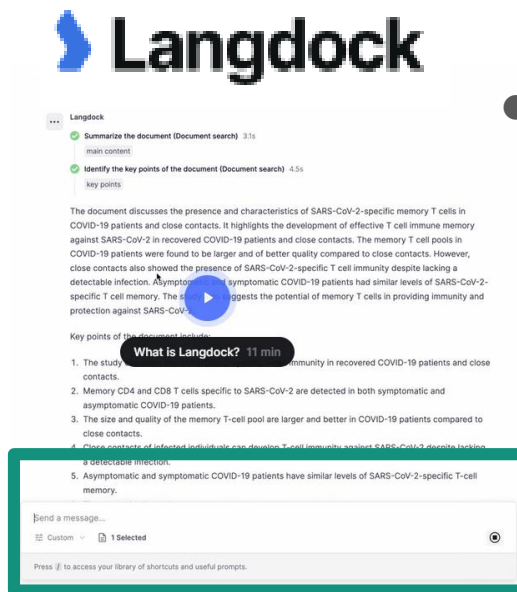
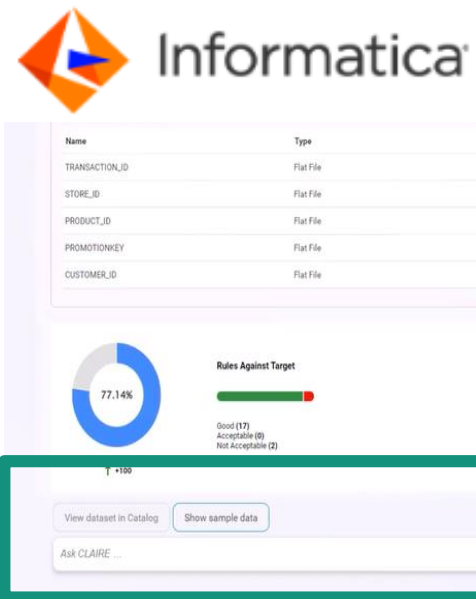
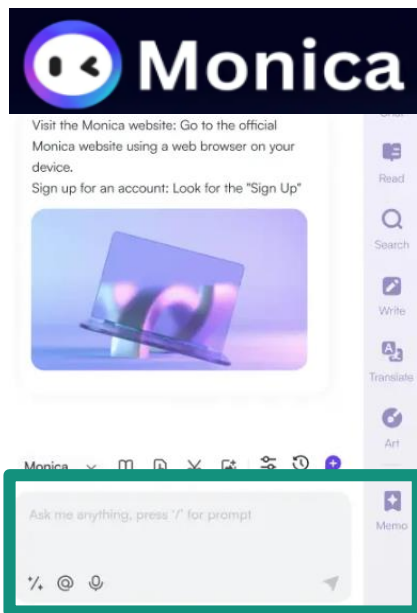
-多模態應用促成下一波新應用發想



- OpenAI的GPT-4V模型擁有多模態能力，在同一時間可看懂圖片、影片等訊息後，另可用語音和文字進行互動，以此達到更為自然的多功互動能力



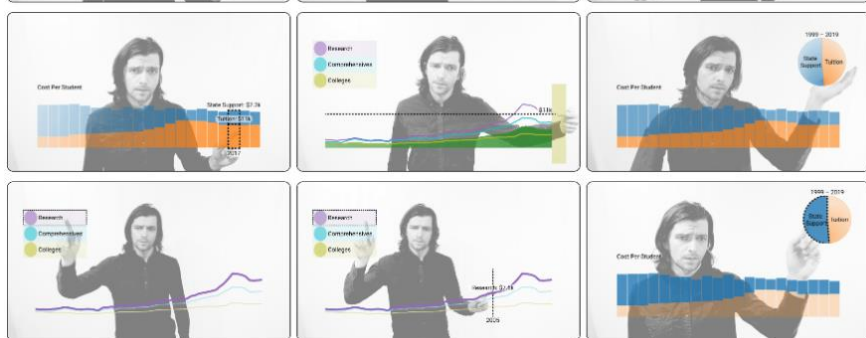
Copilot加多模態成為主要貼身助手， 協助完成各種工作



- Copilot模式會輸入最新資料（結合RAG技術），並以多模態模型進行無縫接軌的互動方式與人進行合作



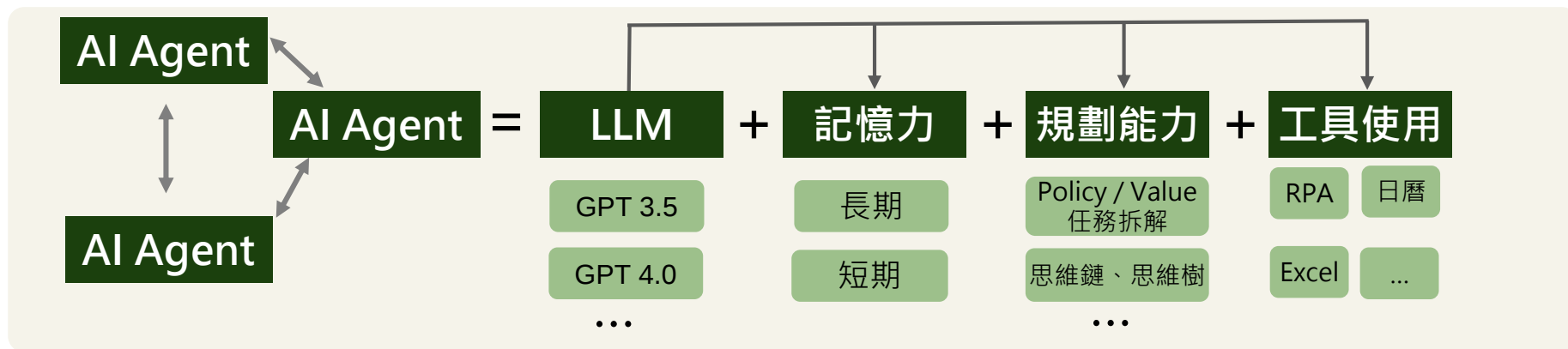
- Tableau開發運用筆電鏡頭可偵測使用者手部動作來與數據互動



資料來源：Monica、Informatica、Langdock、Tableau、MIC整理，2024年4月



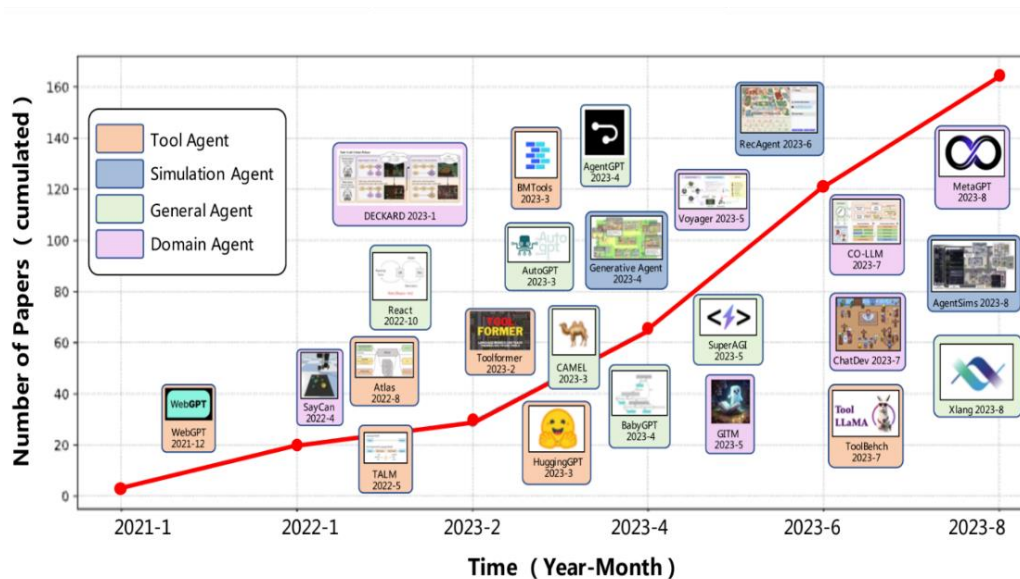
In the Near Future 走進全面的 - AI Agent



資料來源：MIC · 2024年4月



資料來源：MIC · 2024年4月



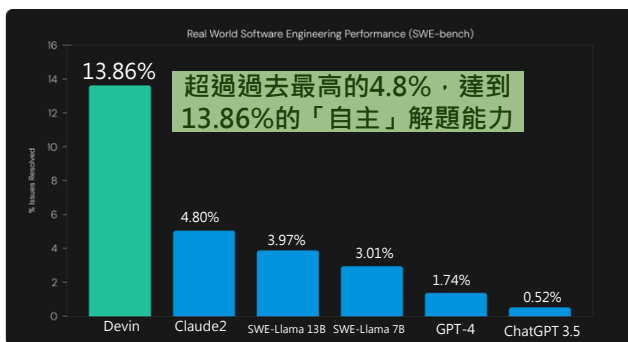
資料來源：A Survey on Large Language Model based Autonomous Agents · MIC整理 · 2024年4月



Devin AI - 具自主規劃能力的程式撰寫AI



- Cognition公司發表AI程式人員，命名為「Devin」
- 具備自我規劃能力、使用不同工具、會找文章自我學習等工作，進而達成所要求的程式撰寫工作
- 在SWE-bench的測試中，其能力遠遠超過過去的能力達3倍左右



備註：SWE-bench是在GitHub過去所遇到真實軟體工程問題的測試集

資料來源：Cognition · MIC整理 · 2024年4月

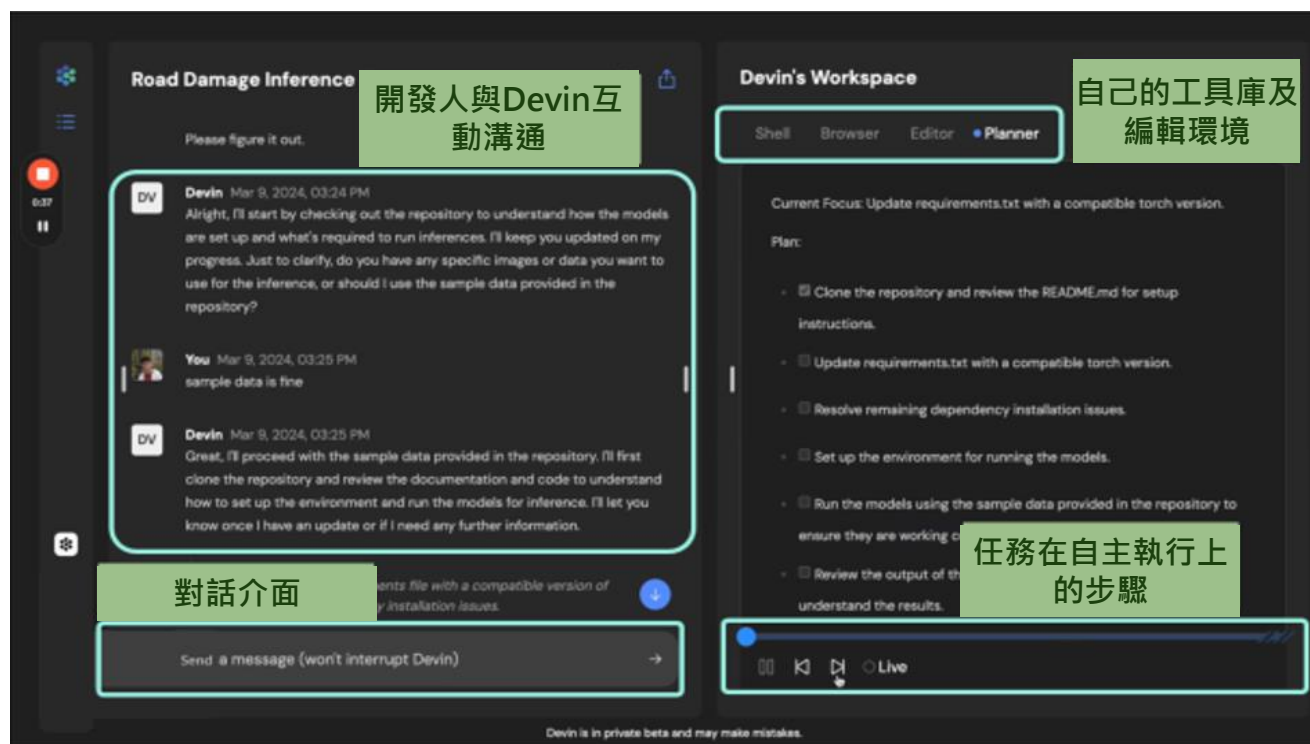
讀文章學習複雜的安裝方法

自主規劃及執行部署工作

找到程式碼錯誤及自動修復

為LLM自主進行微調

...





Sora文生影片造就長影片生成市場

現況

- OpenAI的Sora文生圖可產生60秒的影片
- 技術主要運用擴散模型來生圖外，另外透過Transformer概念將影格視為一單元做時間跨度和內容生成上的理解

缺點

- 技術上難以準確模擬複雜物理場景的因果關係及效果。如：咬了一口餅乾，可能沒有咬痕。
- 混淆提示的空間細節，例如，搞錯左右及角色出現的前後順序



Prompt：考古學家在沙漠中發現了一把塑料椅，小心翼翼地挖掘並清理它。

Weak：未能將椅子建模為一個剛性實體物品，導致物理效應的因果不對



Prompt：籃球穿過籃框然後爆炸。

Weak：物理建模物在籃框上出現「變形」及「穿透」的情況

資料來源：OpenAI · MIC整理 · 2024年2月

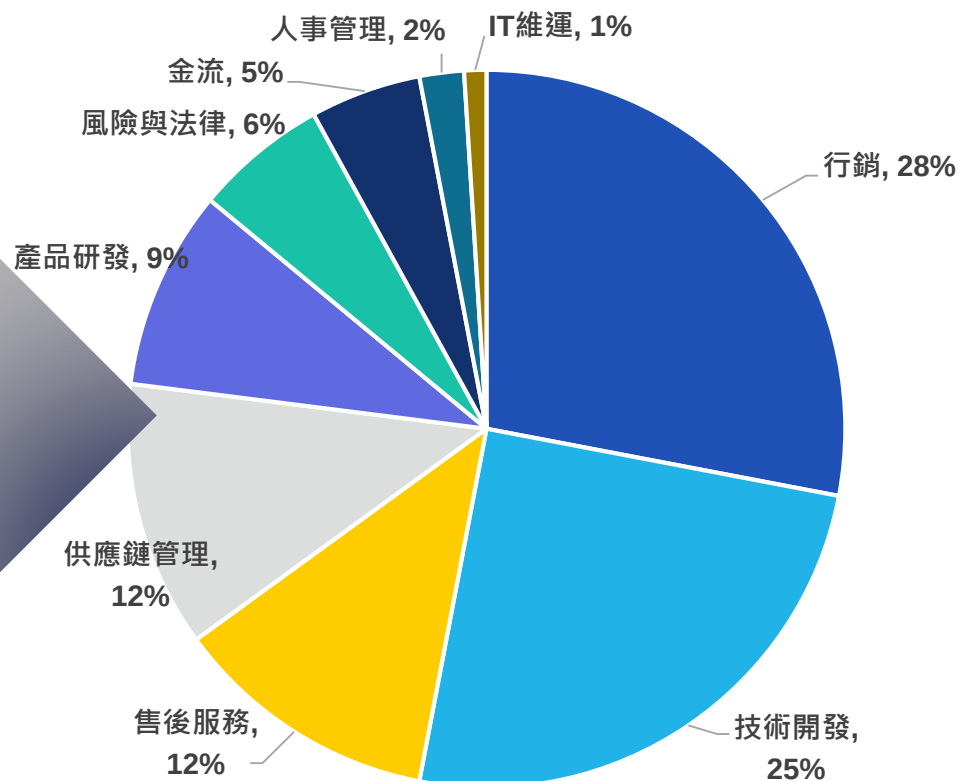
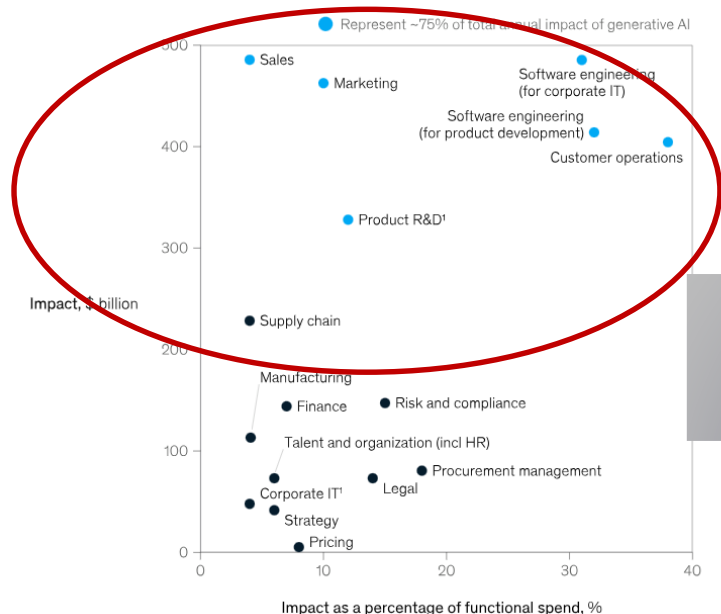
生成式AI管理與安全



生成式AI的使用影響垂直領域及各功能領域

以組織功能區隔看生成式AI影響預測

Using generative AI in just a few functions could drive most of the technology's impact across potential corporate use cases.



資料來源：Mckinsey · 2024年4月



生成式內容氾濫衍生資訊可靠度的議題



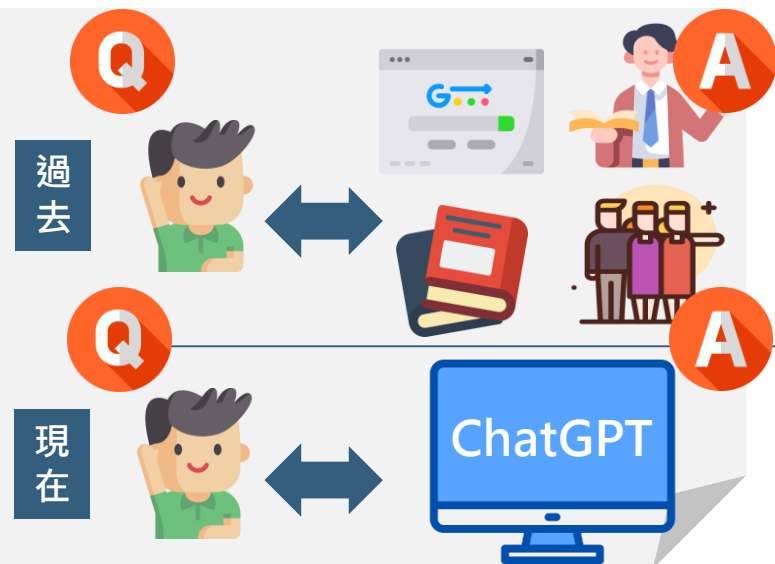
知識訊息的可靠性與真實性成疑

- 知識傳遞單一化：

過去尋求知識需透過不同管道得到解答，如今學生、使用者只需透過生成內容即可，恐導致知識、語言和文化面臨單一化

- 假新聞、假消息、作弊抄襲氾濫：

若沒經過審查過濾，將面臨虛假消息和作弊抄襲問題



LLM十大風險

提示詞注入
Prompt
Injections

資料洩漏
Data Leakage

不合適的隔離
Inadequate
Sandboxing

非授權程式碼執行
Unauthorized
Code Execution

SSRF漏洞
SSRF
Vulnerabilities

過度依賴生成內容
Overreliance on
LLM-generated
Content

AI目的未一致
Inadequate AI
Alignment

訪問控制不足
Controls Insufficient
Access

錯誤處置不當
Improper Error
Handling

訓練數據汙染
Training Data
Poisoning

*SSRF (Server Side Request Forgery，伺服器端請求偽造)

資料來源：OWASP(2023/06)，MIC整理，2024年4月

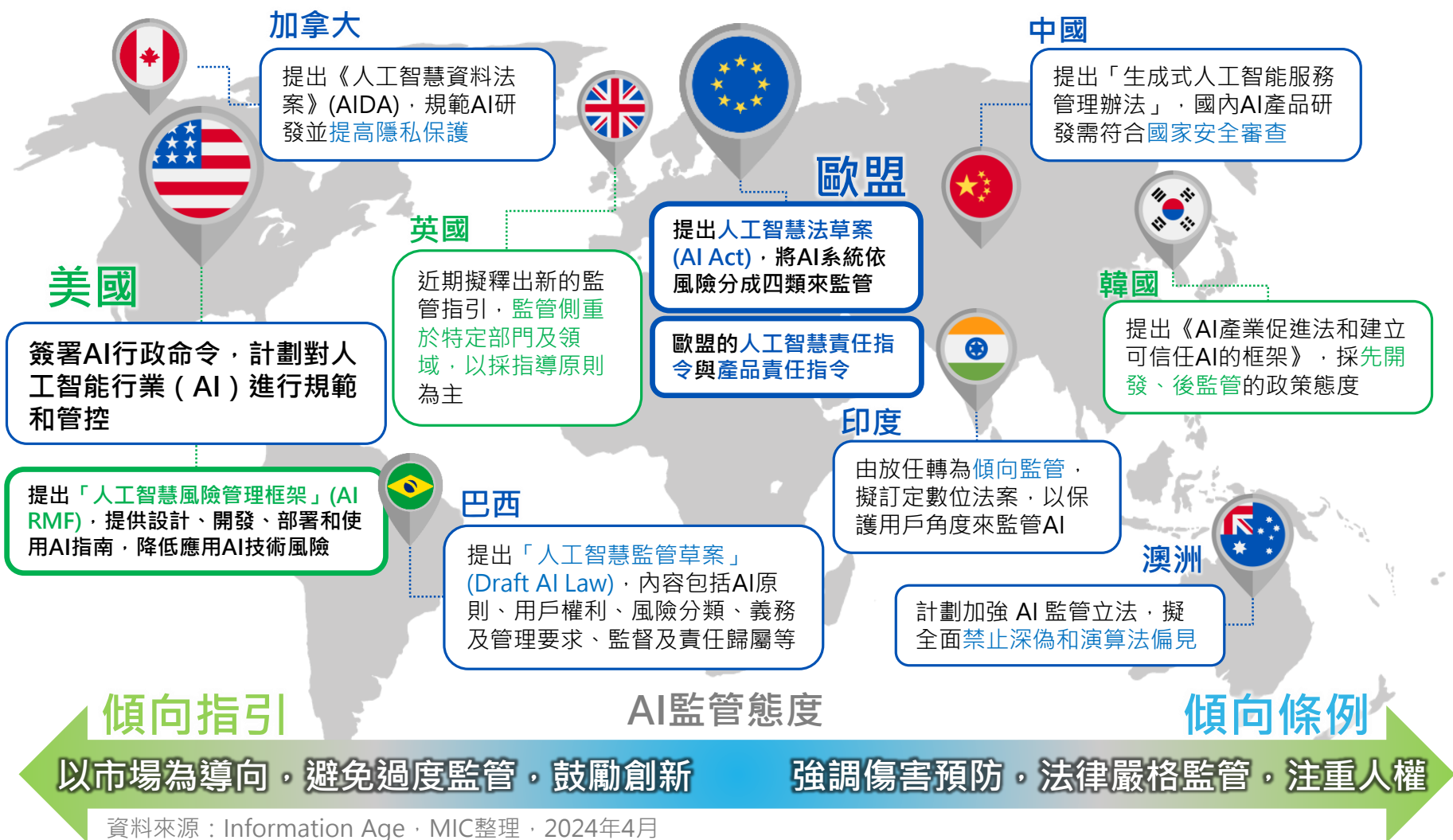


AI x 資安的攻防面向



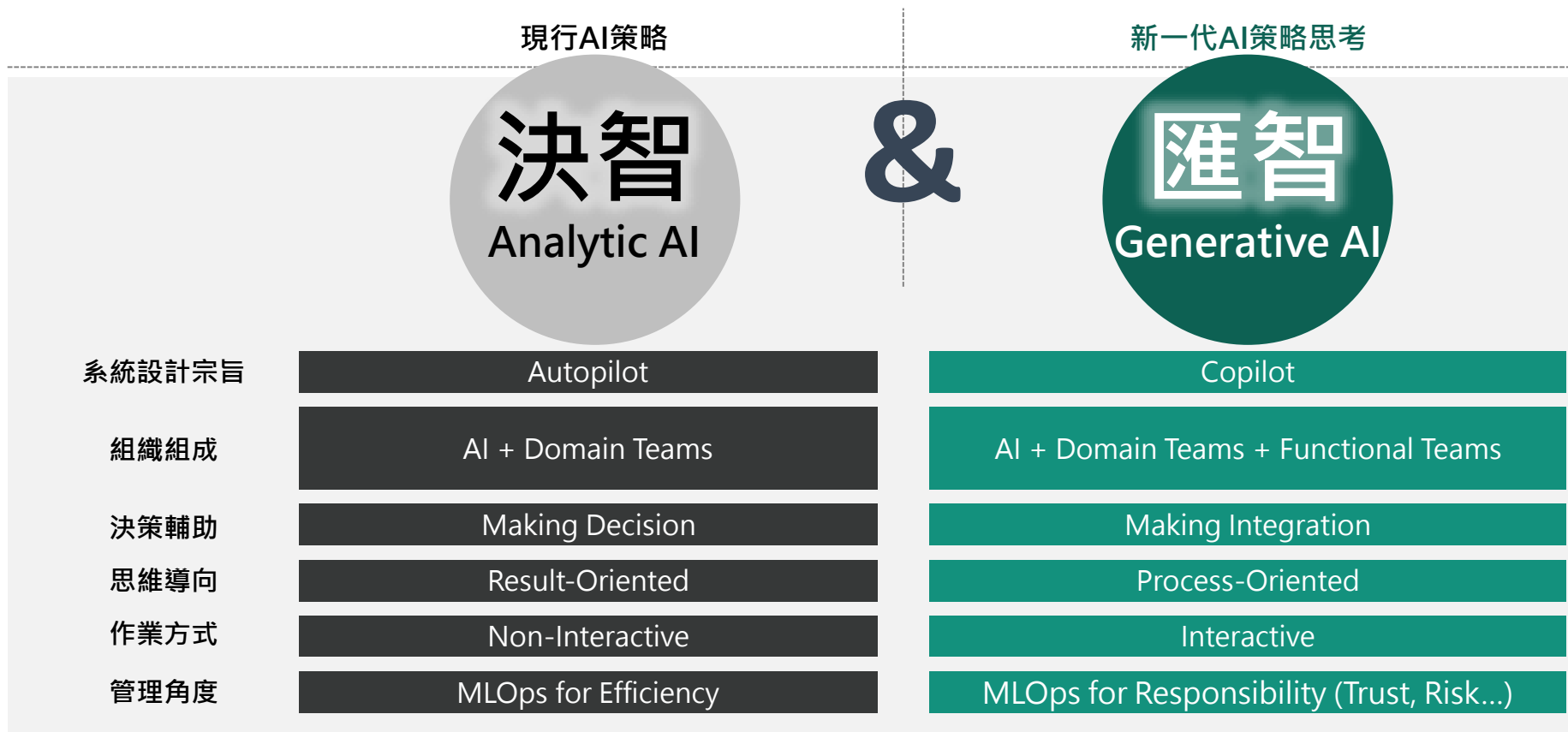


全球AI監管政策主要依循指引及條列兩軌發展





新一波AI趨勢下之策略要素的改變



資料來源：MIC · 2024年4月

結論



結論

- **生成式AI帶動全產業應用，企業應結合新興技術提升智慧化能力**
 - ◆ 企業可及時了解並掌握最新的生成式AI應用趨勢，從中思考如何將其導入到產業中，以提高產業效益
 - ◆ 企業應用中對於手段和目的需快速識別，以此達到企業應用目的
- **生成式AI普及加速，帶動各領域產品及服務革新契機，對此迎接未來新時代**
 - ◆ 在快速變化的生成式AI競爭下，對於現有及新合作夥伴上應快速溝通及整合軟硬體和系統，藉此來達到市場不同場景需求
- **生成式AI的影響深遠，也使得生成式AI受到各面向的挑戰**
 - ◆ 無論從微觀或是宏觀的角度來看，生成式AI仍需面對社會信任、技術基礎、經濟和環境、以及政策法律下的權衡後才得以健全發展



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