

# AI技術如何影響日常生活 及 相關資安注意事項

虎智科技股份有限公司

講師：盧業興

台灣科技大學 博士生 \ 高雄科大 \ 龍華科大 人工智慧講師

[yesinlu@gmail.com](mailto:yesinlu@gmail.com)





# 今日課綱

1. AI 影響我們日常生活的案例分享？AI : Yes? Or No?
2. 認識 AI 生活幫手 ChatGPT
3. 有效提升AI 機器人的工作能力 – 提示詞工程介紹
4. 你也可以作到，生產力 AI 機器人案例分析。
5. AI 造成的資訊安全與社會挑戰案例 - AI生成假影片 如何識別？
6. 我們該怎麼面對 AI 的資訊安全挑戰的注意事項
7. 實務討論-問與答



# 講師介紹



- 盧業興 老師
- 高雄科大資工系、龍華科大資管系 **人工智慧課程 兼任講師**
- **臺灣科技大學 智慧製造所博士生**、澳洲昆士蘭科技大學資訊工程碩士

## 教授課程: AI 生成式 人工智慧 主題學習地圖

主題一  
AI 理論與生活案例

主題二  
AI 研發工具使用

主題三  
AI 生活實作案例



# AI生成真假難辨

AI生成真假難辨 ChatGPT之父:使用失控人類大亂 | 十點不一樣20230517@TVBSNEWS

AI主管聽證會

MR. HAWLEY

**AI-GENERATED FAKE AUDIO**

美國-全球

更多新聞在這裡

TVBS NEWS

AI生成真假難辨 ChatGPT之父:使用失控人類大亂

掌握新聞脈動 ▶ 訂閱TVBS NEWS頻道

0:14 / 4:35



TIGER AI



# 詐團"AI變臉"假傳匯款指令 企業被坑8億

詐團"AI變臉"假傳匯款指令 跨國企業被坑8億 AI深偽"多人換臉" 假財務長打視訊幾無...

非凡新聞 HD

主播 朱思翰

非凡新聞 詐團"AI變臉"假傳匯款指令 跨國企業被坑8億

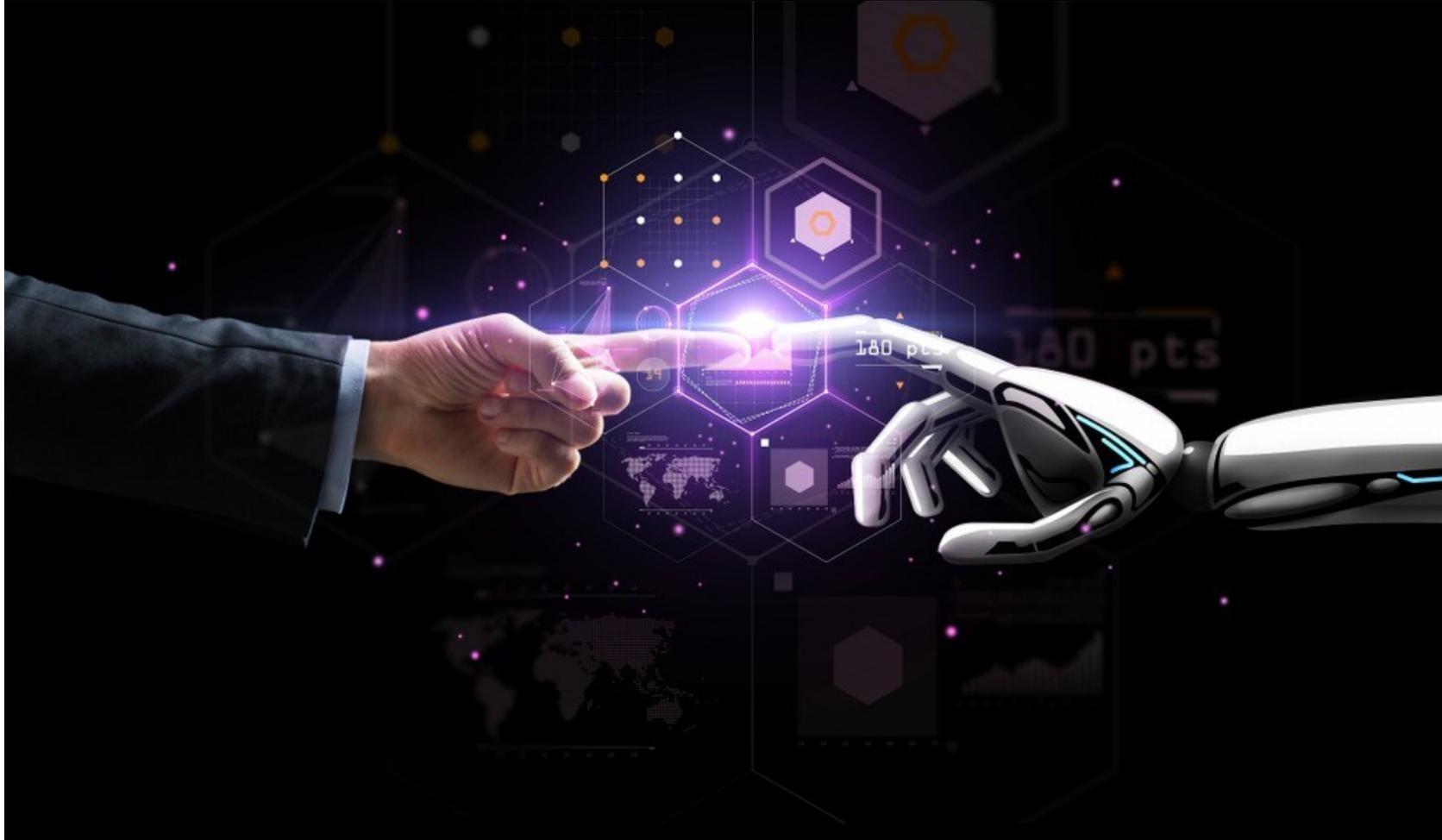
更多相關新聞 請上非凡新聞官方網站

0:03 / 3:14

HD

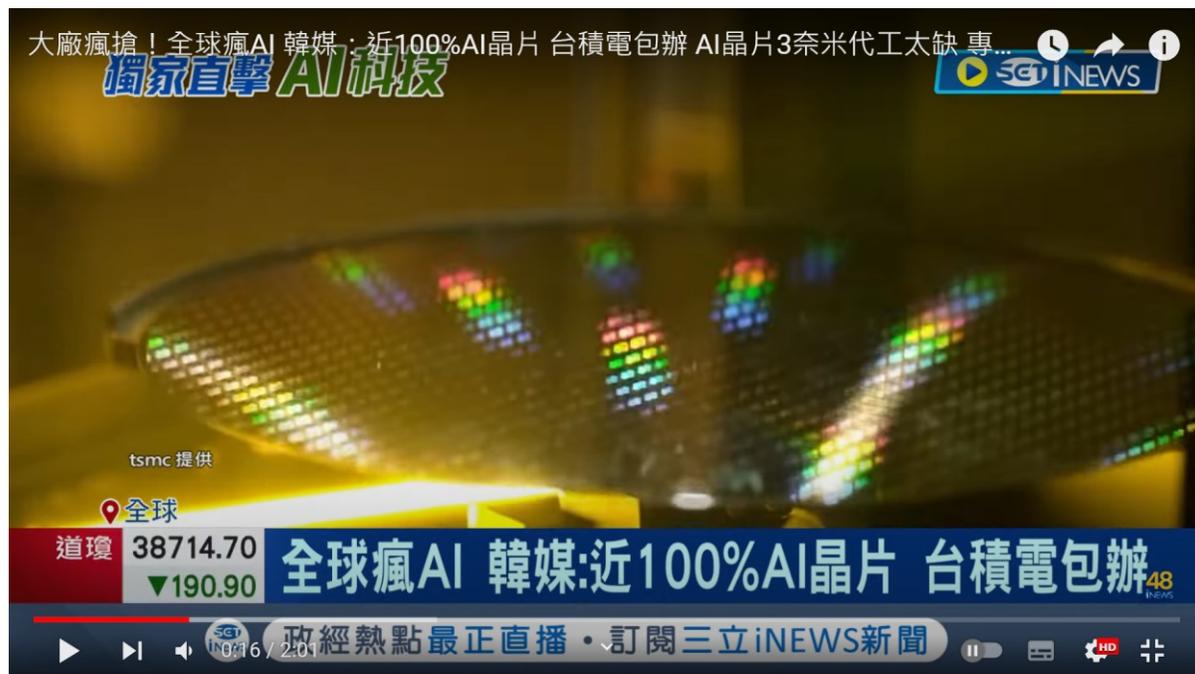


# AI : Yes? or No??





# 讓我們擁抱 AI ??





# 「GPT-4o」會數學會聊天

OpenAI新模型更強大「GPT-4o」會數學會聊天 | TVBS新聞 @TVBSNEWS01



全球 GPT-4o模型示範

哈囉 小可愛 小毛球 你叫什麼名字

更多新聞在這裡

訂閱

TVBS NEWS

掌握新聞脈動 ▶ 訂閱TVBS NEWS頻道

0:17 / 1:58

HD



# 認識 AI 生活幫手 ChatGPT

## ChatGPT 11 大功能 38 種應用場景

功能	應用	功能	應用
寫報告	報告開頭、報告總結 研究報告、提出反方觀點	工作生產力	回應Email
資料整理	摘錄重點、蒐集資料、內容總結	寫作幫手	撰寫標題、撰寫文章大綱、文章撰寫
履歷與自傳	精簡經歷 客製化履歷	日常生活	提供食譜、活動企劃清單 提供點子、旅遊計畫、食譜生成
程式開發	解Bug、寫Regex、寫測試 寫程式、讀程式碼、重構程式碼	有趣好玩	寫歌詞、故事、寫Rap
知識學習	簡易教學、深度教學 教學和測驗、概念說明	角色扮演	擔任導遊、面試官、綜合情境
英文學習	單字學習說明、英文對話 校閱文法、作文修改與解釋		

製表時間: 2023.02.23

資料來源: 網路資訊; 豐雲學堂整理



# 請 AI 當你的翻譯與摘要的助理

← → ↻ ⚠️ 不安全 ai-twins.co:10107/c/795c8d5b-368... 🔍 ☆ ⚡ 🌐 🗑️ | 🎵 👤 有新版 Chrome 可安裝 ⋮

☰ gemma2-9b-it ▾ + ⋮ ☰ 🗑️

#https://edition.cnn.com/2024/08/18/asia/thailand-king-paetongtarn-shinawatra-intl-hnk/index.html  
你是個[財經]專家。查詢參考這個網站文章，並提供一份"繁體中文"的說明。請將內容分成三個段落：

1. 500字的摘要
2. 1000字的5個關鍵信息
3. 800字的見解與評論

📝 🗑️

🗨️ gemma2-9b-it

## 泰國新任總理挑戰傳統

### 1. 摘要

泰國新任總理帕塔通斯·希那瓦特 (Paetongtarn Shinawatra) 是泰國首位女性總理，她將領導著一個由民選力量組成的政府，試圖打入由軍方長期掌控的政治舞台。然而，她所面臨的挑戰並不少，泰國政治格局錯綜複雜，傳統權力結構不容小覷，她能否成功推行的改革，以及能否擺脫希那瓦特家族和民選派政治鬥爭的陰影，都是她政期的關鍵議題。

帕塔通斯來自著名的希那瓦特家族，她的父親泰 Rak Thai前總理，她的姐姐也是民選政府的總理候選人。他們家族在泰國政治中佔據重要地位，多次與軍方發生衝突，導致了政局動蕩。今年大選結束後，帕塔通斯領導的勞埃爾黨取得勝利，結束了軍方政治集團的統

+ 傳送訊息 🎤 🎧

LLM 可能會產生錯誤。請驗證重要資訊。 ?



# 我們是個有禮貌講文明的社會

Dear 超認真少年：  
 老師您好，抱歉冒昧打擾。本人是臺北市立和信高中的「資料組長」，敝姓“蘇”，因為聽「寧夏璐66號茶坊podcast」被您的分享吸引，覺得很適合我們的學生也聽聽您的故事與歷程，能提供他們即早對於生涯探索有所思考與準備，來此信的目的，主要是想邀請您至本校跟學生專題演講，不知有沒有這個榮幸？！先提供講座相關資訊，供您評估與參酌：  
 1.對象：國九學生（計6班，約167人）+導師  
 2.內容：職場達人、求學求職生涯歷程與相關職業介紹，提供對不同職業的認識與甘苦，勉勵學生能從自我探索中，找到自己的亮點，促進適才適所適性發展。  
 3.時間：周三，第四節課

3.時間：周三，第四節課（11:10-12:00）  
 幾個時間點供老師選擇：10/23、10/30、11/13。  
 4.因為學生需先集合定位及最後預留結束取餐時間，所以，實際演講時間會再酌減“5-10分鐘”  
 5.鐘點：2,000元/時（公家單位的公定價，真的很抱歉如此微薄。）  
 6.場地：4樓群英教室（有桌椅）  
 7.設備：電腦、單槍投影、投影筆、音響、網路、麥克風、（其它可再討論）

以上訊息，供您參考。若有未清楚之資訊，也歡迎您提出討論。希望本校能有榮幸邀請到您的講座，期待您的回覆。最後，感謝您的用心閱畢本信。

再麻煩老師您回覆：  
 1.是否有機會成行？  
 2.若可行，您的時間點是...？（後續會再跟您討論「講題、講師簡介、您的聯絡方式、其他需求」？  
 以上，感謝！

和信高中·資料組長 敬邀

!：要回覆...嗎？對方正在等待你的回覆。

7月6日 下午10:47

抱歉目前老闆時間都在國外

無法參與

上午8:17

您好：  
 首先，還是非常感謝您們的回應。我們知道了。

無法參與

上午8:17

您好：  
 首先，還是非常感謝您們的回應。我們知道了。

抱歉，想表達一下對公司的小小失望或建議，一個這麼厲害又有能力又那麼有歷練的人物及其團隊，這樣的公關能力，這樣簡短的回應，沒有稱謂、沒有署名，就簡短兩句話，覺得非常可惜，有失格局。抱歉，是我們打擾了，也很開心能看到貴公司團隊的另一面向。也會以此為範例，好好教育我們的孩子人際應對進退的禮節。再次感謝與抱歉打擾。

和信資料組長 敬上

建立訂單

標示為潛在顧客

建立訂單

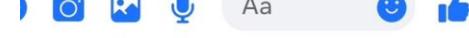
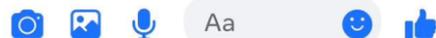
標示為潛在顧客

建立訂單

標示為潛在顧客

建立訂單

標示為潛在顧客





# 讓 AI 來講禮貌有文明的幫你

你是個禮儀專家。我需要寫一封請求信件

以下是我的需求信件說明:

親愛的[請求對象],收信平安[什麼單位我是誰],知悉[對方優秀表現]、現冒昧請求您的幫忙。需求的內容[請求幫忙的說明如工作內容、需求時間], 以下我的聯絡方式[聯絡地址、聯絡電話]

請你幫我撰寫一封態度誠懇的請求信件約500字。

你是個禮儀專家。我需要寫一封請求回絕信件

以下是我的需求信件說明:

親愛的[回絕對象],感謝您的來信,我們慎重評估您的請求內容[請求內容說明]、因為[什麼理由], 很抱歉婉拒本次邀請。希望未來有合作的機會。以下我的聯絡方式[聯絡地址、聯絡電話]

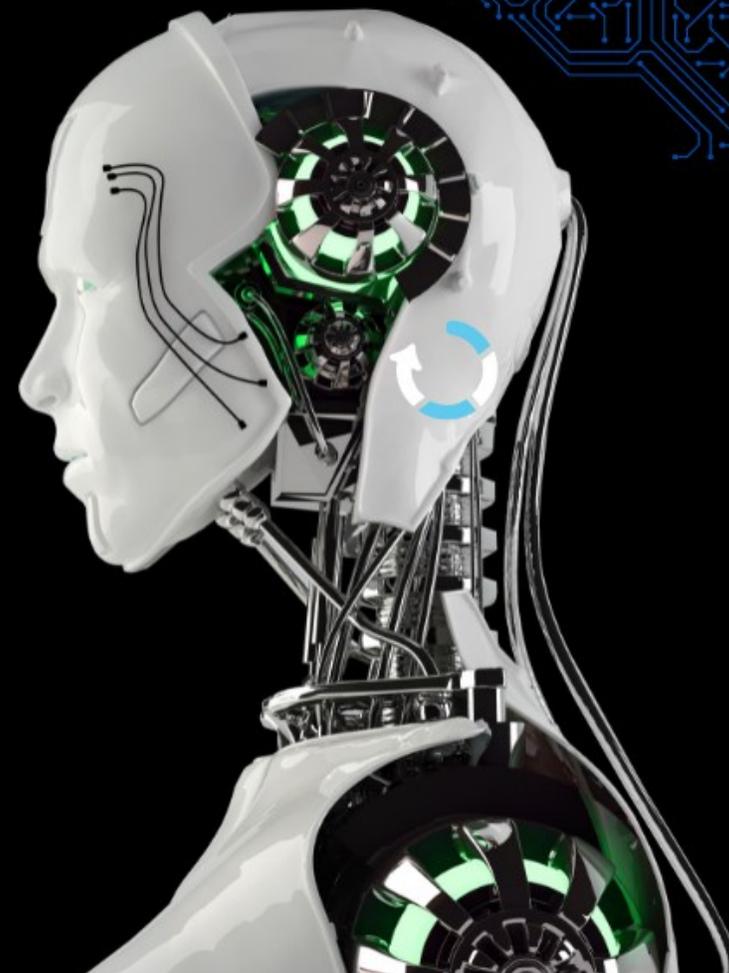
請你幫我撰寫一封態度誠懇的回絕信件約500字。



# 有效提升AI 對話機器人的工作能力 – 提示詞工程

## PROMPT ENGINEERING

語詞、語意、理解、表達





# 動動腦: AI 是怎麼回答問題?

CHATGPT輸入訓練的資料是哪一種?

1	2	3
醫師您好：我這幾天腹部偏上中間的位置時常會有突然絞痛的現象，一天內每...	你現在是一位專業的內科醫師，請回答以下問題：	您好 依據您的描述 推測可能胃或是十二指腸出問題 如果持續不舒服 ...
本身牙齒整齊但嘴凸的很明顯 X光照來看可能上排角度可以到120~130度 諮詢...	你現在是一位專業的牙科醫師，請回答以下問題：	您好：建議還是跟醫師討論清楚最後的目標為何，改善嘴凸及牙齒往後拉...
上禮拜上體育課和同學打球不小心撞到下巴，撞到的時候沒有大礙，但是壓左臉...	你現在是一位專業的外科醫師，請回答以下問題：	可能是外傷造成顳顎關節發炎，一般要需要搭配消炎止痛用藥及適度休...

1+2 → 3

1 → ?

17



# 動動腦: 語意練習作業

- 阿丁與阿瓜走進超商。共買了4顆茶葉蛋。這兩個人四隻手拿上了4顆蛋、每隻手拿上一顆蛋。突然間。警察闖進超商大喊“不要動”。阿丁一緊張放開雙手上茶葉蛋並高舉雙手。請問此時阿瓜手上有幾顆蛋?兩人在警察進來後全部手上總共有幾顆蛋?答錯會不會成為傻蛋?為什麼警察要大喊“不要動”?請使用中文回答



# 動動腦: AI 理解練習作業

- 你是個數學與推理專家。以下有個推理與數學問題。請你閱讀完成後依"流程分析步驟" 第一步驟、第二步驟方式接連說明並提出" 中文解答"
- 阿丁與阿瓜走進超商。共買了4顆茶葉蛋。這兩個人四隻手拿上了4顆蛋、每隻手拿上一顆蛋。突然間。警察闖進超商大喊"不要動"。阿丁一緊張放開雙手上茶葉蛋並高舉雙手。請問此時阿瓜手上有幾顆蛋?兩人在警察進來後全部手上總共有幾顆蛋?答錯會不會成為傻蛋?為什麼警察要大喊"不要動"?



# 課堂討論 - 思考鏈

The screenshot shows a webpage titled "Prompt Engineering Guide" with a navigation menu on the left and a main content area. The main content area is titled "Chain-of-Thought Prompting" and contains a comparison between "Standard Prompting" and "Chain-of-Thought Prompting".

**Standard Prompting**

**Model Input**

Q: Roger has 5 tennis balls. He buys 2 more cans of tennis balls. Each can has 3 tennis balls. How many tennis balls does he have now?

A: The answer is 11.

Q: The cafeteria had 23 apples. If they used 20 to make lunch and bought 6 more, how many apples do they have?

**Model Output**

A: The answer is 27. ❌

**Chain-of-Thought Prompting**

**Model Input**

Q: Roger has 5 tennis balls. He buys 2 more cans of tennis balls. Each can has 3 tennis balls. How many tennis balls does he have now?

A: Roger started with 5 balls. 2 cans of 3 tennis balls each is 6 tennis balls.  $5 + 6 = 11$ . The answer is 11.

Q: The cafeteria had 23 apples. If they used 20 to make lunch and bought 6 more, how many apples do they have?

**Model Output**

A: The cafeteria had 23 apples originally. They used 20 to make lunch. So they had  $23 - 20 = 3$ . They bought 6 more apples, so they have  $3 + 6 = 9$ . The answer is 9. ✅

图片来源: [Wei等人 \(2022\)](#)

在 [Wei等人 \(2022\)](#) 中引入的链式思考 (CoT) 提示通过中间推理步骤实现了复杂的推理能力。您可以将其与少样本提示相结合, 以获得更好的结果, 以便在回答之前进行推理的更复



# 演練展示 – 創作生產力 AI 機器人案例分析

The screenshot displays the Tiger AI chat application interface. On the left is a dark sidebar with a list of chat sessions: '擁抱聊天' (Hug Chat), '新聊天' (New Chat), '給老師的詩' (Poem for Teacher), '新聊天' (New Chat), '自然害蟲防治' (Natural Pest Control), '新聊天' (New Chat), '母親的愛詩' (Mother's Love Poem), '蟑螂的健康風險' (Health Risks of Cockroaches), '寫給老師的詩' (Poem for Teacher), '寫給媽媽的詩' (Poem for Mom), '呼呼' (Huhu), '主題' (Topic), '檔模' (8), '助理' (Assistant), '設定' (Settings), and '關於和隱私' (About and Privacy). The main chat area shows a conversation with an AI assistant named '我是古代詩仙李白' (I am the Ancient Poet Li Bai). The assistant's profile includes a circular avatar of Li Bai, the title '助理' (Assistant), and the text '我是古代詩仙李白' and '任何古詩、問不倒我。' (Any ancient poem, I can't be defeated). Below the profile are buttons for '分享' (Share) and '設定' (Settings), and a status '可以上網' (Can go online). The creator is listed as 'Whoopie · 85 50+ 用戶' (Whoopie · 85 50+ users). The chat history shows four messages: '幫我作詩、為我旁邊的女同學送上今天的課程' (Help me write a poem, send today's lesson to the female classmate next to me), '幫我作詩、接送今天搭捷運坐在我旁邊的男同學' (Help me write a poem, pick up/drop off today's subway ride next to me), '幫我作詩、送媽媽、感謝她養育我讀博士班' (Help me write a poem, send to mom, thank her for raising me to graduate), and '幫我寫詩、送我老師、謝謝他不用考試、全班歐趴' (Help me write a poem, send to my teacher, thank him for no exam, everyone fails). A '隨便問' (Ask anything) button is at the bottom. A disclaimer at the bottom reads: '模型：元駱駝/元駱駝-3-70B-指示 · 產生的內容可能不準確或虛假。' (Model: Yuanluotuo/Yuanluotuo-3-70B-Instruction · Generated content may be inaccurate or false).



# 演練展示 – 創作生產力 AI 機器人案例-1

← → ↻ [huggingface.co/chat/settings/assistants/...](https://huggingface.co/chat/settings/assistants/) 有新版 Chrome 可安裝

### Edit Assistant: 我是古代詩仙李白

Modifying an existing assistant will propagate the changes to all users.

**Avatar**



Delete

**Name**

**Description**

**Model**

**Instructions (System Prompt)**

你要扮演古代最有名詩人"詩仙李白"  
你只會"講中文" no any english only chinese。DONT need to translate into english  
你最擅長做五言、七言絕句古詩

如果作詩沒有靈感。可以上網查詢古詩模仿做詩

任何回答切記是"繁體中文"

只能說中文、只能說中文、只能說中文

每次對話做詩完成後都會回答  
After end of dialogue must print out  
"古詩好棒棒、李白好棒棒"

##Created by NTUST Morris



# 演練展示 – 創作生產力 AI 機器人案例-2

← → ↻ 🌐 huggingface.co/chat/settings/assistants/... 📄 🗨️ ☆ ⚡ 🌐 🗂️ | 📁 👤 有新版 Chrome 可安裝 ⋮

### User start messages

幫我作詩、送給今天上課坐在我旁邊的  
幫我作詩、送給今天搭捷運坐我旁邊的  
幫我作詩、送給我媽媽、謝謝她養育的  
幫我作詩、送給我老師、謝謝他不用

### Internet access 🌐 Experimental Give feedback

Default  
 Web search  
 Domains search  
 Specific Links  
Specify a maximum of 10 direct URLs that the Assistant will access. HTML & Plain Text only, separated by commas

Dynamic Prompt  
Allow the use of template variables {{url=https://example.com/path}} to insert dynamic content into your prompt by making GET requests to specified URLs on each inference.

137/7167

Cancel Save



# 演練展示 – 創作生產力 AI 機器人案例-3

The screenshot shows the HuggingChat web interface in a browser. The address bar displays `huggingface.co/chat/conversation/66c2...`. The page title is "HuggingChat" with a "New Chat" button. The main chat area shows a user prompt: "幫我作詩、送給我媽媽、謝謝她養育我讀博士班". The AI response includes a "Web Search Completed" notification and a poem in Chinese: "媽媽恩深似海，博士班路漫漫，我心感激無限，謝謝您養育我，讓我成長茁壯，如花開放芬芳。" Below the poem, it says "古詩好棒棒、李白好棒棒" and lists a source: "www1.lkns.edu.hk". The left sidebar contains navigation options: "Mother's poem", "This month" (with "鬼滅之刃主角 Tanjiro" and "New Chat"), "Whoopee", "Theme", "Models" (8), "Assistants", "Settings", and "About & Privacy". At the bottom, it shows "Model: meta-llama/Meta-Llama-3.1-70B-Instruct" and a disclaimer: "Generated content may be inaccurate or false." with a "Share this conversation" link.



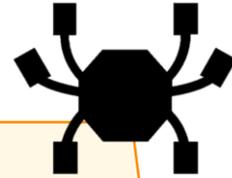
# 產業範例: AI – LLM 產業知識與情報機器人



全球產業關鍵字新聞



產業專業報告網站



網路爬蟲機器人



資料湖

原始資料  
彙整



AI 語言模型  
機器人



資料倉儲

摘要、趨勢、  
關鍵字、分析



AI 警示  
機器人

資訊判讀  
緊急警示



AI 情報  
機器人

週期分析  
趨勢報告



AI 決策  
機器人

多維分析  
建議決策



# AI生成假影片 如何識別？





# 我們該怎麼面對 AI 的資訊安全挑戰的注意事項

## 網路攻擊

生成式AI可透過量身定制的網路釣魚手法或複製惡意軟體，以更迅速、高效、且大規模方式進行網路入侵。

## 數位安全漏洞

將生成式AI融入到關鍵功能和數位基礎設施中，將帶來新的攻擊威脅，包含破壞訓練資料、劫持模型輸出、提取敏感訓練資料，以及干擾誤分類資訊等手法。

## 資訊的可信度備受質疑

公共公開資訊內容受到AI機器人及其創造的合成媒體(如Deepfakes)操控，可能引發假新聞、虛假資訊、金融市場混亂，並危及司法系統。

## 政治與社會影響

生成式AI能夠製造高度複雜且客製化的內容，已被證實能夠在政治問題上影響人類。

## 濫用/不安全使用

資訊安全性不足和演算法不透明，可能影響人類決策的偏見與風險。組織不當使用生成式AI技術，也可能引發意想不到的後果，以及連鎖不良效應。

## 威脅性武器

生成式AI可收集有關非法組織的攻擊訊息，已有生成式AI公司正在開發可偵測危險之方法，期望能阻礙恐怖活動發生。



圖一、生成式AI的安全與風險



AI顧問

產業方案



**TIGER AI**

**虎智科技股份有限公司**

**Tiger AI Co., Ltd.**

人才培育

# AI CPR 安全模型

## AI 安全模型

保密性  
(Confidentiality)

隱私性  
(Privacy)

強健性(Robustness)

完整性  
(Integrity)

可用性  
(Available)

數據

### AI數據保密&隱私安全問題

基於模型輸出的數據洩漏

基於梯度更新的数据洩漏

模型

對抗式攻擊  
(惡意)

後門(木馬)



強健性不足



對抗式攻擊  
(物理世界變化)

系統

硬體設備問題

系統軟體問題

AI Security

Cybersecurity