2026「AI 與雲端賦能：建構金融產業智慧未來」國際研討會

The International Symposium on " AI & Cloud Empowerment: Shaping the Intelligent Future of Finance "

成果回顧

人工智慧崛起驅動金融科技應用，為協助資產管理從業人員掌握產業最新脈動，增進金融創新與實務應用能力，並配合金融監督管理委員會 115 年度施政計畫重點。

本次研討會聚焦於國際資產管理發展趨勢、金融科技創新，以及 AI 與雲端技術於金融產業中的實務應用等重要議題，並邀請多位來自國內外的實務專家擔任講席，分享其對產業趨勢與策略佈局的專業見解。

研討會議題包括「重塑臺灣金融 AI 生態系」、「AWS 雲端運算與 AI 實務應用案例分享」、「金融業 AI 雲端實務應用」及「GenAI 與雲端技術實踐」。透過與專業講席的深度交流，俾與會者汲取豐富的國際經驗，為臺灣的資產管理生態體系注入養分。

本研討會與會者來自政府單位、金融周邊單位、銀行、證券、期貨、投信投顧業者以及其他金融相關機構，共計 112 位參加。

議程

時間：115 年 5 月 28 日（星期四）
地點：證基會會議廳（台北市萬華區昆明街 77 號 6 樓）

時間	主題	主講人
09:00-09:30	報到	
09:30-09:40	主辦單位致詞	張振山 董事長 證券暨期貨市場發展基金會
09:40-11:10	**專題演講一：** **重塑臺灣金融AI生態系**	王儷玲 主任 國立政治大學 金融科技研究中心
11:10-11:30	休息時間	
11:30-12:30	**專題演講二：** **AWS雲端運算與AI實務應用案例分享** **AWS Cloud Solutions and AI Use Cases**	余昌達 Mark Yu 亞馬遜網路服務公司(AWS) 臺灣金融產業市場開發經理
12:30-14:00	午餐時間	
14:00-15:00	**專題演講三：** **金融業AI雲端實務應用** **The Age of Agentic Wealth - Scaling Institutional Intelligence with AI & Cloud**	Ms. Kate Huang, Chief Technology Officer, International Arta Finance, Singapore
15:00-15:20	休息時間	
15:20-16:50	**專題演講四：** **GenAI與雲端技術實踐**	王俊權 處長 中國信託商業銀行 數位科技處

主辦單位致詞

張振山 董事長
證券暨期貨市場發展基金會

證基會張董事長開場致詞表示，為響應金管會今年度(115 年)施政計畫重點，包括「壯大資產管理計畫」、「促進金融科技創新與服務」及「推動綠色及轉型金融」等方向，規劃辦理本國際研討會。

張董事長指出，近期臺灣 AI 金融科技產業積極布局海外市場，並與國際資產管理機構合作，顯示金融科技解決方案在資產管理與數位金融服務上應用的重要性。

本研討會內容聚焦於「國際資產管理發展趨勢」與「金融科技創新運用」，邀請多位實務經驗豐富的國內外專家進行分享，首先，針對近期備受關注的代理式 AI(Agentic AI)議題，為協助業界掌握國際脈動與政策契機，邀請到國立政治大學金融科技研究中心的王儷玲主任，就臺灣推動「金融主權 AI」與「大語言模型(Large Language Model, LLM)」進行深入探討；此外，中信銀行數位科技處的王俊權處長將分享金融業在 AI 轉型下的治理與實務。本活動亦特別邀請 AWS 亞馬遜網路服務公司臺灣金融產業市場開發余昌達經理，分享 AWS 提供 AI 與雲端服務並與金融業合作案例；以及來自新加坡金融科技公司 Arta Finance 的國際技術長 Ms. Kate Huang，透過視訊分享 AI 於金融業的應用與市場趨勢。活動現場同時設置線上提問平台，鼓勵與會者與講者進行雙向交流。

最後張董事長感謝所有與會嘉賓的蒞臨，並期許本次研討會能夠促進金融科技前瞻思維與創新，為與會者帶來豐厚的知識與啟發，提升金融機構競爭力、優化客戶體驗及強化風險管理能力。

專題演講一：

重塑臺灣金融AI生態系

講　座：

王儷玲　主任

國立政治大學

金融科技研究中心

王儷玲教授擔任國立政治大學金融科技研究中心主任，她指出今年(2026 年)是臺灣推動「金融主權 AI」與大語言模型(LLM)落地的關鍵元年，由銀行業先行啟動，這對臺灣金融科技發展史而言，是一個極具歷史意義的重要里程碑。她表示臺灣在半導體(如台積電)與 AI 硬體供應鏈(如 NVIDIA)上已是全世界的焦點，因此臺灣絕對有實力與能力在金融業的 AI 應用上發揮強大實力。然而，金融業導入 AI 的失敗案例在國際上屢見不鮮，如何透過策略布局降低失敗率、建立標準化平台並達到真正的「落地創新」，是本次演講的核心主軸。

國際金融 AI 技術的進步可分為兩個核心波段，目前正迎來關鍵的典範轉移，從生成式 AI(Gen AI)邁向 Agentic AI，Agentic AI 的崛起，推動「代理即服務 (Agents as a Service, AaaS)」模式的誕生，其核心在於「以行動能力取代單純的 QA 問答」。過去的 AI 僅是單純的工具或裝置，而 Agentic AI 則是有邏輯思考、具備判斷與執行力、且能在錯誤中自我導正與重新學習的「數位同事(AI Agent)」。未來金融機構的運作不再依賴「單一大模型」，而是進入「多模型協作」的新階段，讓不同領域、負責不同數據庫的專屬 AI(如理財 AI、風控 AI、法遵 AI)同時為企業工作，並進行最終的系統整合與人機協作，王主任預估這波趨勢將引領 AI 產業 43%至 44%的爆發性成長。

王主任分享國際大型金融機構在 AI 及代理人技術上的實務案例，主要聚焦於三大領域：

1. **高資產財富管理與另類投資優化**
   (1) 摩根大通(JP Morgan)：透過「多重代理(Multi-Agent)」架構為高資產客戶服務。因應跨境投資、家族傳承、ESG、私募及另類投資(如私募股權、私募債權、公共基礎建設)等極其複雜的產品需求，由不同專業領域的 AI Agent 進

行深度調研、會議紀錄、報告分析，並執行定價與風險控管模型，最終整合出最優化的資產配置建議提供客戶。

(2) 摩根士丹利(Morgan Stanley)：其建置的 Private Banking AI Agent 已具備「博士級(甚或教授級)」的 AI 分析能力，可在極短時間內內化龐大的法規與專業論文，提供前瞻性而非僅就過去報表的投資洞察。

2. **傳統核心系統轉移(Legacy System Migration)**

金融業導入 AI 最大的痛點在於舊有核心系統的轉移，過去如南山人壽的核心系統轉換曾因數據錯誤率過高而面臨巨大損失。現在國際上已可利用 AI Agent 自動進行代碼轉譯(如將舊代碼自動轉為 Java 格式)，以更精準、省時且格式化的方式進行大規模歷史數據的清洗與對接，大幅降低系統升級的營運成本與人為風險。

3. **動態計價、智慧防詐與跨境支付**

(1) 加拿大皇家銀行(RBC)：導入 Agentic AI 技術後，對文檔與研究報告的處理能力迎來「10 倍數的提升」，研究報告的產出時間縮短 60%，並且改善精準度，降低分析師工作負擔，使其能專注在更高價值的策略判斷面。

(2) 萬事達卡(MasterCard)與聯卡中心：正積極開創「KYA(Know Your Agent)」架構。未來當人類授權 AI Agent 使用信用卡在線上直接結帳與呼叫 API 時，支付平台必須有技術去驗證該 AI Agent 是否獲得合規授權，這催生出全新的支付商模。

(3) AI 聯防防詐：臺灣目前正由 12 家壽險公司合作，利用「聯邦式學習(Federated Learning)」建置理賠防詐模型，各公司不需交換客戶隱私數據，即可透過共同訓練的模型，精準阻斷高額的詐欺理賠金。

王主任強調，中小型金融機構(如獨立證券商或投信投顧)若單打獨鬥發展 AI，常受限於算力昂貴、缺乏金控資源與 AI 人才而導致高失敗率。為此，在金管會主導與產官學界支持下，臺灣已正式組建「金融 AI 國家隊」，於今年(2026 年)4 月 22 日召開記者會正式啟動「金融 AI 大語言模型計畫」，第一階段由政大與中信金控主導，結合 16 家出資銀行，斥資約新臺幣 6,000 萬打造本土金融大語言模型，先以銀行業大語言模型為核心，預計在今年第三季(9 月前)產出初步模型。2027 年計畫

延伸至保險業，由國泰金控領軍主導，以及證券與投資信託領域。

王主任表示臺灣本土金融大語言模型的一大核心優勢在於維持「數據主權」與「可監管度」。模型由政府與學術單位主導，全數在本土環境訓練，能完美克服繁體中文、臺灣本土法規語意與金融案例的特殊性。該計畫首先由金融研訓院、證基會、保發中心提供法規、判例、商品正確知識與證照題庫；同時，今年也將政大商學院(包含財管、金融、風管、會計等)所有必選修教科書與碩博士論文全數餵給 AI 讀，預計在三個月內建構出極度完備的語意資料庫，讓 AI 具備至少大學畢業生、甚至是碩博士級的縝密邏輯思考與解題能力。

臺灣金融大語言模型計畫與一般開源模型的核心差異，在於政大所建立的專業評測場域。王主任表示，多數企業在進行 AI 效能測試，時常陷入一項致命盲點，就是直接將既有的訓練輸入資料(Input Data)作為測試考題。此舉極易使模型產生「具備高度智慧」的盲目樂觀假象，一旦正式上線營運、直接面對客戶，便會破綻百出。

為此，政大創新中心特別建構專屬的評測機制，由學術界教授與金融業界高階主管共同組成專家委員會，採取「獨立重新出題」的盲測策略。過程中甚至導入「AI 自行出題、委員會嚴格選題與優化(Tune 題)」的前瞻技術，藉此嚴格評定(Grading)AI 模型的盲測表現，確保其生成內容完全符合監管合規性與回報準確性，並有效消除外界對 AI 的「黑盒子疑慮」。未來，參與本計畫的 16 家出資銀行將可無償使用此平台與評測場域；其餘未參與出資之機構，未來則可透過商業模式訂閱，共同享有集體訓練的豐碩成果。

最後，王主任對在座的金融與證券業代表提出未來與 AI 接軌的三大核心策略建議：

1. **基礎工程重盤點(核心與雲端)**：AI 的運作高度耗電且依賴龐大算力與數據。各公司應重新盤點中後台架構、核心作業系統，並積極與雲端平台(如 AWS)協作。若未來難以負擔大型機器的中小型券商，可透過平台「Module(模組)化」或訂閱制的方式，計費共享雲端算力中心，以最低成本換取最高產值。
2. **引進國家隊模型並「內化微調(Tune up)」**：國家隊所 Pre-train(預訓練)出來的模型是標準化的產業基礎。金融機構必須以各公司自己的經營策略、商品結構、法遵與行銷模式進行「常規性的微調」，才能真正轉化成為專屬的、能創造營收

的超級數位員工。

3. **在職教育與人才庫建立：**完美的 AI 治理與人機協作必須仰賴具備專業金融知識的人才。目前具備 AI 工程能力的技術人員往往不懂金融，因此金融業迫切需要對在職人員進行 AI 聯邦模型與提示詞(Prompt)的教育訓練。政大目前已與 NVIDIA、AMD、APMIC 等大廠密集開設相關課程，期盼共同提升全臺金融業的科技底蘊，攜手邁向高收益、低風險的智慧金融新時代。

提問與交流

Q1: 金融業是高度監管的行業，絕不容許對內或對外有錯誤的訊息提示或決策。但 AI 的隨機性非常高，即便經過多方訓練或設定 Prompt 護欄(Guardrails)等措施，仍無法達到百分之百正確。您認為該如何提升 AI 的應用場景？又該如何教育內外部利害關係人，使其對 AI 有更正確的認知？

A1: 有向金管會建議，當金融業在進行 AI 試作時，若擔心可能因錯誤而產生責任，可以採取「試辦」方式。透過給予幾個月、甚至半年到一年的寬限期(必要時可再延長)，以過去監理沙盒的概念，讓金融機構透過試辦申請來進行法規調適。目前金融法規調適小組也非常鼓勵大家提出申請，除了數位資產、穩定幣和真實世界資產(RWA)代幣化之外，AI 應用也是重點。由法規調適小組提出示範模式後，各家公司就能在該範圍內安心進行嘗試。而當金融專屬的大語言模型發展成熟後，其邏輯思考能力會提升，錯誤的頻率就會隨之降低。未來希望推動投資與證券領域的標準化模型，並結合 AI Agent 來解決錯誤提示的問題。

Q2: 未來若有臺灣金融業的大語言模型，是否能出一版「資料格式公版」，讓各金融業者在內部資料管理上趨同，以利於跨單位的資料交換？

A2: 目前跨公司或甚至在同一家公司內部，不同單位在儲存資料時，即便同一個定義或內涵，儲存格式往往也不盡相同(其中以保險業最為複雜)。因此，未來在發展金融大語言模型時，會把標準化的定義做出來。雖然各場景存在差異、需要慢慢推進，但「標準化模型」與「標準化資料公版格式」絕對是未來的趨勢。透過類似開放銀行(Open Banking)的資料交換方式，標準化模式不

僅風險最低，也能讓業者最容易做到「即插即用」，快速將效益分享出去。

Q3: 如果大語言模型未來已經達到大學生的能力等級，您怎麼看待金融學系畢業生未來的就業情況？十年後金融業是否會出現大裁員或就業機會銳減的情況？

A3: 現在即將畢業的學生的確面臨比較大的挑戰，但這也意味著無論是剛畢業還是已在職的人，都必須學會創造自己的「經驗價值」。AI 會是你的工具或同事。員工不能只停留在做例行性的工作，而是要透過在職訓練，思考如何與 AI 協同工作、創造不可取代的價值。而尚未畢業的同學，則建議在校期間就積極投入產學合作或跨領域學習(例如政大金融科技學程就正推動跨領域課程，來銜接市場需求)。雖然近期科技業出現較大編制的裁員，其主要是為降低成本，且科技進步太快，但個人認為金融業不至於出現如此大規模的裁員潮。因為金融業是一個「有溫度」的產業，需要面對客戶，例如保險業的大量業務人員並不會被完全取代，而是需要轉型去學習如何跟 AI 協作。AI 的導入反而會創造出許多以前沒有的新場景與新工作。

Q4: 先前富邦金控的「鷹眼模型」分享給各金融機構後，聽說效果並不是很好，這是否也是您所提到的「因子資料」的問題？另外，聽說金融大語言模型有一些金融機構不參與，是否會擔心因為特定金控主導而顯得過於偏頗或強勢？

A4: 一開始大家可能會誤以為這項計畫只符合大型金控的需求，但事實上，這個模型對中小型銀行的效益反而高過大型銀行，因為中小型銀行根本沒有足夠的資源能自己做。以國泰的 Gaia 模型為例，其投入長達 10 年的計畫、龐大的人力與資料庫，過程中的失敗率也很高，是慢慢調教出來的。至於是否會偏頗或強勢，因為緊接著就要與 16 家銀行進行協商並建立委員會，這是有一套協商機制的。大家不需要給予第一版模型太大的壓力。在年底前僅剩幾個月的時間內，目標是先把平台流程、標準化作法建立起來，先產出一個具備基礎行員能力的「基礎版」模型，後續再讓各家銀行帶回去針對不同情境升級調教(Phase Two)。這是一個協商的過程，有錢的出錢、有力的出力，都是支持金管會的政策。

Q5: 未來臺灣金融大語言模型落地，主要希望的應用方向是什麼？

是由各公司自行開發應用場景嗎？同時，在資料訓練上是否會往「去識別化」方向進行？是否會有各自議題的處理建議？未來提供給大型金融機構使用時，會不會有「資料上雲」的疑慮？或者有什麼限制與規範？

A5: 基本上不需要擔心資料上雲與個資外洩的問題。現在的雲端技術可以讓各金融機構的資料保留在各自獨立的儲存分區(Compartment)中，彼此不會互相分享。此外，可以使用聯邦式學習，各家只需在本地跑出因子後回傳因子來訓練模型，不會直接用到原始個資。針對高度敏感的個資，也可以利用「生成式資料(Synthetic Data)」去模擬真實資料的統計分佈來進行訓練，既不改變資料特性，也能完全保護隱私。這套大語言模型在推動過程中，會建立起一套完善的規範來解決這些問題。至於具體的落地場景，每家公司想要做什麼應用、要投入多少人力、買多少算力，當然是由各家公司自行主導並自行計算投資報酬率。這個共同平台最核心的效益，是讓大家能參考國內外成功的案例與別人訓練過的模型，藉此降低失敗率，並以更快速、更低成本的方式在內部複製、落地 AI 應用。這也是做這個 AI 金融科技平台最重要的價值，希望大家能一起前進 AI 金融科技時代。

專題演講二：

AWS雲端運算與AI實務應用案例分享

AWS Cloud Solutions and AI Use Cases

講 座：

余昌達 Mark Yu 經理

亞馬遜網路服務公司(AWS)

臺灣金融產業市場開發

余昌達經理指出，自 2023 年起，人工智慧(AI)已成為全球科技與商業投資的絕對核心。從美股「科技七姐妹」(Magnificent Seven)的市場表現到臺灣本土企業的策略轉型，最大規模的資本支出與科技投資

均集中於 AI 技術，特別是算力與 AI 應用的建置。然而，將生成式 AI 引進高度專業且受嚴格監管的資本市場與金融體系時，企業將普遍面臨三大嚴峻挑戰：

1. **幻覺問題(Hallucination)**：大語言模型(LLM)基於機率生成文本，時常會憑空捏造看似合理卻完全錯誤的資訊。在對準確度要求零容忍的金融與證券市場中，這類錯誤可能導致嚴重的合規風險與經濟損失。
2. **資料品質與切片管理**：金融數據龐大且雜亂，如何將內部非結構化資料(如研究報告、財務報表)進行高品質的清洗、切小顆粒管理，並即時更新，是技術落地的瓶頸。
3. **資訊安全與隱私合規**：金融業受到高度法規監管，核心資產與客戶資密數據絕不能外洩，如何在保護隱私的前提下發揮 AI 的最大價值，是架構設計上的首要考量。

為解決上述挑戰，余經理深入淺出地剖析目前 AI 基礎架構中最重要的三大技術支柱：

1. **「檢索增強生成(Retrieval-Augmented Generation, RAG)**：是克服 AI 幻覺的特效藥。其運作邏輯是在用戶提問之前，系統先至企業內部安全且經過驗證的資料庫(如公司財報、內部規章)中尋找相關知識，再將這些「標準答案」作為提示詞(Prompt)餵給大語言模型。余經理強調，透過 RAG 技術，我們可以下達嚴格的 Prompt 指令，例如：*「請在提供的範圍內尋找答案，若沒有找到，請回答不知道。」* 這能確保 AI 的回答完全限制在合規的框架內，徹底杜絕幻覺產生。
2. **「模型脈絡協定(Model Context Protocol, MCP)」**：余經理將 MCP 生動地比喻為「萬用插座」。過去，AI 模型要調用外部數據(如路透社新聞、彭博終端機、交易所即時股價)時，工程師必須針對每種數據源單獨編寫對接協議(Protocol)。而 MCP 提供一個標準化的統一介面，讓 AI 能夠透過這個萬用插座，自由地呼叫各種 API、下載市場分析報告、存取多元資料庫。MCP 的出現，等於是讓原本只能「動口回答問題」的 AI 顧問，忽然長出雙手，升級為能真正動手執行任務的員工。
3. **從 Chatbot 到 Agentic AI 的演進**：從 2023 年僅能單純依照 RAG 的提示進行標準化、一問一答的 Chatbot 對話階段；自 2024 年至今，AI 開始具備自主規劃、串聯與協同作戰的能

力，多個扮演不同角色的 AI 分析師(例如：技術分析專家、總經專家、法規合規專家)，能夠透過 MCP 互相溝通、傳遞資料，形成一個高效率的「AI 專家團隊」，為投資人或企業內部同仁提供全方位的智慧代理協助。

AWS 在全球金融市場累積豐富的成功經驗，余經理特別挑選兩大代表性案例進行深度分享：

1. **穆迪(Moody's)：千人千面的個人化智慧投資助理**

   全球信用評等與風險管理巨頭穆迪，透過 AWS 的技術建置高度創新的面向客戶/前台(Customer-Facing)解決方案。該系統實踐「千人千面」的資訊消化(Digest)模式。當投資人查詢自身持股時，AI 會主動收集近期所有相關的科技反彈、重大宣布或合作關係，並將關鍵資訊標註(Tag)給使用者。最令人驚豔的是，系統會根據資產類別的特性自動切換分析邏輯，例如用戶查詢虛擬貨幣(如比特幣)，AI 會自動聚焦於法規變化與 ETF 的發行狀況；若查詢傳統股票，則切換至財務基本面與產業新聞。這種特別量身打造的投資助理，大幅提升客戶黏著度。

2. **納斯達克(Nasdaq)：AI 驅動的金融犯罪偵知系統**

   納斯達克利用 AWS 的雲端算力與大語言模型，開發出極為強大的金融犯罪偵知與反洗錢系統。這類高密度的法規遵循系統以往需要耗費海量的人力與時間進行人工審查，如今透過 AI 的自動化模型與多 Agent 協作機制，能精準捕捉異常交易行為。此外，納斯達克將此成熟的解決方案上架至 AWS Marketplace(AWS 所推出的線上數位軟體商店)，其他金融機構不需自行組織龐大的銷售或開發團隊，便能透過 AWS Marketplace 直接訂閱、上架與部署，形成卓越的金融科技生態圈。

綜上所述，生成式 AI 在資本市場與金融產業的應用，已正式從早期的「技術狂熱」跨入「務實落地」的全新階段。企業透過 RAG 架構有效抑制 AI 幻覺、運用 MCP 賦予 AI 實質執行力，並藉由多 Agent 機制打造出高效的專家協作團隊，在兼顧「安全」與「效率」的雙重指標下穩步推動數位轉型。

尤為關鍵的是，AWS 臺北區域(Taipei Region)於 2025 年 6 月 6 日的正式啟用，無疑為臺灣金融科技發展注入最強大的催化劑。這座

在臺灣本地建置、具備三可用區(Availability Zones, AZ)的高可用架構的世界級基礎設施，不僅以極低延遲與超高頻寬滿足金融業最嚴格的異地備援與不斷電營運要求，更徹底解決過去受限於主管機關「數據出境」與「雲端委外」的監管痛點。透過將機密財務與客戶資料百分之百留存於本地(Data Residency)，Taipei Region 為臺灣證券期貨業與銀行業引進 GenAI 開闢一條安全合規的綠色通道。

結合 AWS 從底層 AI 專用晶片、中間層的模型管理與安全連接(Amazon Bedrock)，到上層開發工具與 Customer-Facing(面向客戶/前台)應用方案的一條龍完整技術支援，臺灣金融機構已擁有最堅實且合規的轉型後盾。

展望未來，臺灣金融證券業將在此安全基石上，加速內部創新與端對端服務優化，並在全球 AI 浪潮中，迎來更蓬勃的跨國金融科技交流與全新商機。

提問與交流

Q1: 詐騙或犯罪集團是否也有使用雲端服務？以及各大供應商如何避免被利用助紂為虐？

A1: 詐騙集團確實有可能在使用雲端服務，但基本上各大雲端供應商在提供服務前，都會要求客戶進行簽約並執行嚴格的合規審查。以 AWS 為例，在與使用者簽署雲端服務合約時，會明確規範並確保其使用的方向符合正確、合法的範疇；同時，系統也會要求客戶註冊相關資訊，一旦偵測到註冊來源屬於異常警示地區或奇怪的網域時，後台機制便會主動進行阻擋，以此防止雲端資源遭到犯罪集團惡意利用。

Q2: 如何確認 AI 彙整的資訊都是正確、即時的且沒有 AI 幻覺？如果未來過度依賴 AI，導致使用錯誤資料做決策，該如何解決？

A2: 要確認 AI 彙整資訊的正確性，關鍵在於不能直接使用通用的公開大模型來回答特定專業問題，而是必須引進 RAG 架構來限制並維護 AI 回答的資料範圍。此外，在系統架構的中間層需要建立完善的治理機制，這包含兩大核心步驟：第一是確保 AI 只能存取到正確且經過授權的內部資料，第二則是引進評估機制來反覆驗證輸出的正確性與合規性，透過 RAG 限制範圍與後端評估把關雙管齊下，即可有效杜絕幻覺並確保決策資料的正確性。

Q3: AI 的隨機性非常高，即便經過多方調教、訓練或設定 Prompt 護

欄，仍無法達到百分之百正確。而金融業是高度監管的行業，不容許對內對外有錯誤訊息或提示，該如何提升 AI 的應用場景？又該如何教育內外部關係人對 AI 有更正確的認知？

A3: 面對 AI 無法達到百分之百正確的特性，目前技術上除利用 RAG 限制回答範圍外，也開始導入多代理人機制(Multi-Agent)，透過基金代理人、總經代理人、合規代理人以及多數表決代理人等協作專家團隊，從不同面向共同評估與驗證答案。更重要的是，「內外部利害關係人必須建立正確的認知」，因為現在的 AI 技術尚未發展到「完全自主」的階段，其本質是「賦能」工具，旨在幫使用者高效蒐集資料並留存完整的推理流程，因此在現階段的應用場景中，人為的最終判定與把關仍是不可或缺且不可避免的，最後的決策權與確認權依然在人身上。

Q4: 臺灣投顧未來會大量啟用這些 AI 代理工具嗎？研究員的價值跟人力需求是不是會大幅的減少？

A4: 雖然十分鼓勵投顧業大量使用 AI 代理工具，且從國外如橋水基金(Bridgewater)或穆迪(Moody's)的經驗來看，AI 確實將原本需要一週才能產出的信用報告(Credit Memo)大幅縮短至一小時，但在全球少子化與人力精簡的趨勢下，研究員的人力需求並不會因此減少。AI 的導入反而能解放研究員的時間，將原本耗費在例行性資料蒐集的時間，轉而投入在最寶貴的知識判斷上，用專業去審查 AI 做出的內容是否正確，這將顯著提升每個人的工作品質與產出效率，而非取代人力。

Q5: 如果公司目前是微軟的愛用者，有沒有建議可以讓公司的資訊人員多看看其他的雲端供應商(如 AWS)？

A5: AWS 最特別的優勢在於它定位為一個中立、開放的「平台與工具」，而非綁定特定技術的封閉系統。以 Amazon Bedrock 平台為例，企業可以自由調用 GPT、Anthropic Claude、AWS Nova 甚至是各種開源的小模型，我們不會鎖定或強迫客戶一定要使用哪一種模型；AWS 的核心精神是「為客戶賦能」，把選擇權與最全面的工具箱交給企業去靈活組合運用。

Q6: 相較於財務報表和研究調查資料，AI 是不是也可以協助機構或投資人分析川普等名人的發文？

A6: 這在 AI 領域屬於「輿情分析(Sentiment Analysis)」的範疇，目前技術已經完全成熟且有許多知名機構(如納斯達克、倫敦證券交

易所)運用。AI 能將名人的語句字眼與歷史上龐大的交易紀錄、大盤走勢進行交叉比對與關聯性分析，從中找出共通性與市場連接點，進而預測該發言背後對市場造成的潛在經濟影響；不只是川普的發文語氣，AI 甚至能分析其過往發言後市場未平倉的變化與特定股票的波動，這在未來大語言模型的應用中會扮演越來越重要的角色。

Q7: 部分金融機構採用 Microsoft Azure (微軟的公有雲端運算平台)是因為可以確保上傳的資料有簽保密協定、不會用於資料訓練，請問 AWS 如何處理個資保護與合規性的問題？

A7: 保密與合規一直都是 AWS 在臺灣金融業深耕最核心的基石，早在國內金融雲端法規起草設立之初，AWS 的專家團隊就參與許多相關的探討與研究。微軟所擁有的保密協定與資料不落入訓練的承諾，AWS 同樣完全具備，且能提供相對應的架構比對資料供業界探討；金融機構在引進 AWS 時，可以透過建置「登陸區域(Landing Zone)」等專屬金融安全防禦邊界與合規服務，確保所有機密數據在傳輸與儲存時皆符合臺灣金融主管機關最嚴格的監理精神，百分之百做到個資去識別化、隱私隔離與安全保密。

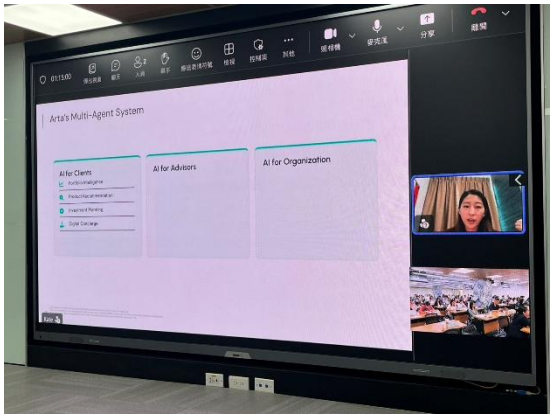
專題演講三：

金融業AI雲端實務應用

The Age of Agentic Wealth - Scaling Institutional Intelligence with AI & Cloud

講 座：

Ms. Kate Huang,
Chief Technology Officer, International
Arta Finance, Singapore



Ms. Kate 是新加坡 Arta Finance 的國際技術長，負責該公司所有核心科技與 AI 架構研發，她曾在美國矽谷 Google 總部工作。Arta Finance 目前約有一百多名員工，多數來自 Google 等頂尖科技巨頭或

資深金融產業。該公司亦獲得新加坡政府官方主權或相關基金的注資，是一家結合科技與國際金融思維的金融科技公司。

Kate 首先分享 Arta Finance 的創立初衷，是填補「大眾富裕階層(Mass Affluent，資產約 100 萬至 500 萬美元)」在傳統銀行與私人銀行之間所面臨的巨大服務斷層。她以自己 2010 年在美國灣區工作時買房的經驗為例，當時面對百萬美元的房價，她選擇變賣當時手頭上極具價值的 Google 股票。她事後回想，如果當時懂得財富管理工具，得知市場上有「股票抵押借貸」服務，根本不需變賣股票，即可將 Google 股票作為抵押物向銀行低利借貸以付清房款，既能保留未來大幅增值的股票，又能滿足購屋需求。她藉由此案例分享這種知識上的落差，正是財富無法極大化的主因。

因此，Arta Finance 的使命是利用雲端科技與 AI 人工智慧，將過去專屬於資產數千萬美元富豪的頂級私人銀行理財工具「數位化」與「自動化」，讓一般客戶也能以極低的門檻享受機構級的財富管理智慧工具。

Kate 強調 Arta Finance 將複雜的私人銀行產品全數程式化，為客戶打造數位化投資體驗，完全打破傳統需要面對面對話的架構，主要提供以下三大核心數位產品：

1. **公開市場投資(Public Market Strategies)**：Arta Finance 擁有自己的內部專業策略團隊，除提供機器人理財服務外，更主打「主題式投資組合」。其技術核心在於「即時客製化反應」，用戶若看好特定市場，可直接在 App 上手動調整某些標的權重，系統在後端雲端會即時重新計算，立刻在前端呈現該客製化組合的歷史績效與數據分析，用戶評估後即可一鍵執行完成投資組合配置。
2. **私有市場與另類投資(Private Market & Alternatives)**：Arta Finance 持有對應的資產管理牌照，提供以往散戶難以企及的私募股權、私募債權、房地產投資、信託及稅務規劃。由於金融法規嚴格，私募投資通常無法公開宣傳基金名稱，因此 Arta Finance 將所有合規數據、策略與定價透明化地整合在 App 內的數位資料房(Data Room)中。用戶可進行「一鍵投資(One-Click)」，後續的數位簽章與後台流程皆在線上完成。當私募市場發出「資本認繳通知（Capital Call）」時，Arta Finance 的自動化系統能與用戶的公開市場資產連動，自動變現部分

機器人理財的資金來支應私募股權的交割，完全無需人工介入。

3. 結構型商品建構(DIY Builder)：為 Arta Finance 自行研發，用戶可以在平台上自由選擇 1 到 4 個標的物，自行輸入想要的投資規模、投資期限及下檔保護(Downside Protection)比例。提出申請需求後，系統會在雲端即時算出報價，該報價在 1 小時內有效，用戶可直接在線上進行配對與投資。App 甚至提供匿名社群功能，讓會員參考其他匿名用戶建構出高達 73%收益率的特殊結構商品。

Kate 最後在現場 Demo Arta Finance 開發的語音 AI 代理人「Arthur」，不僅打破傳統理財 App 密密麻麻、需逐頁翻找圖表的繁複體驗，更為金融業示範「AI 原生(AI-Native)」與雲端技術深度結合的樣貌：

1. **極致的 Edge Cases 處理能力：**面對講者突如其來的現場互動與「向全場打招呼」的非預設情境，AI Agent 展現具備擬真情緒停頓與極具幽默感的自然語言對答，證明其已超越死板的罐頭客服。
2. **即時個人帳戶穿透與風控提示：**AI 代理人能即時調閱雲端資料庫，將分散在數筆不同交易明細中的股息總額精確計算輸出，展現強大的底層數據整合力。
3. **機構級的投資歸因分析與合規風控：**在即時調閱個人帳戶回報率的同時，AI 能主動給予專業的金融風控提示(如說明計算未計入結構型商品)；更能聯動全球財經大事件(如 Tesla 銷量下滑、Alphabet 併購案等)，將散落的新聞與用戶資產波動進行深度邏輯綁定，提供媲美頂級私銀分析師的分析報告。

Arta Finance 的核心突破在於將金融數據代碼化，並在雲端架構上部署具備主動性與理解力的 AI 代理人語音模型。用戶不再需要迷失在傳統網銀的數字迷宮中，只需透過最自然的對話，就能在數秒內獲得極度個人化、機構級的財富管理智慧。這不僅打破傳統私人銀行因高昂人工成本而無法規模化的限制，更徹底顛覆並重塑未來人類與個人財富互動的全新模式。

提問與交流

Q1: 臺灣金融業若想推展金融科技，因技術本身並非專業，且自身

傳統業務部門僅有實體通路認知，對於與金融科技結合興趣缺缺，您建議可以如何凝聚既有業務部門接觸金融科技的共識，進而發揮業務更大的可能性？

A1: 這確實是一個不容易且非常有挑戰性的問題，要凝聚組織內部的共識，舉辦像今天這樣的研討與展示活動就是一個很好的起點，能讓傳統金融領域較為資深的人員對科技在金融行業的應用產生具體想像 。在推動時並不一定要追求一步到位做到全方位的 AI Agent，而可以透過展示實體 Demo 來開啟組織內部的對話。許多擁有百年歷史的傳統金融機構本身很難自發做改變，通常是依靠內部一、兩位想要推動轉型的主管(如 CTO 或特定部門主管)在內部發起，或是借助外部合作夥伴的力量從外部向上推動，因此在推動組織轉型時，找到關鍵的內部贊助者或領導者才是最為核心的關鍵。

Q2: 在臺灣金融監理相對嚴格，取得銀行或券商庫存需要簽署許多同意書且要定期(如每年)更新，請問像 AI 這樣的服務在推動的過程當中有沒有遇到過類似的問題？以及這項服務在臺灣與未來跨境管理的發展可能性為何？

A2: 金融業的監管確實相當不容易，即便是歐洲非常老牌且嚴謹的大型銀行客戶也會面臨極其嚴格的檢視，但推動 AI 服務時並不一定要一步到位。相較於直接將投資規劃等應用直接推給終端客戶，若能先將 AI 體驗導入給內部的基金經理人使用，在技術推行上會相對容易，因為經理人在使用時一定會進行人工審查才會推介給客戶，這就是一個很不錯的進步。從目前在新加坡所觀察到的趨勢來看，無論是美國、歐洲還是阿聯酋等地的金融機構，全球都在朝著科技與金融結合的潮流前進，因此臺灣也勢必需要引領並跟著做出改變。

Q3: 可以請您分享亞洲或中港台金融業的合作經驗嗎？另外，可否稍微說明 Arta Finance 與新加坡金融管理局(Monetary Authority of Singapore, MAS)的合作內容？

A3: 在亞洲合作經驗方面，目前團隊確實有與臺灣的部分銀行正在進行合作探討與討論，但基於商業保密協議，在尚未正式對外宣布之前，具體的合作對象與內容目前還不便對外透露。而關於與 MAS 的合作，由於金管會屬於監理機構，Arta Finance 作為持牌機構，每年都必須依法接受嚴格的年度審查。與此同時，

新加坡政府在推動科技與新金融結合上非常積極，例如先前我們在新加坡舉辦產品發表會時，政府高層便特別派員出席，並積極協助我們對接與引薦不同的產業資源，雙方的合作涵蓋非常多元的面向。

專題演講四：

GenAI與雲端技術實踐

講　座：

王俊權　處長

中國信託商業銀行

數位科技處

王俊權處長強調自己並非科技或技術背景出身，而是從金融業務前台與風險管理第一線走過來的管理者，由於具備豐富的風險控管與跨部門整合經驗，他在 2018 年被管理階層委任開創中信的大數據與 AI 轉型團隊。該團隊從最初的 20 人規模，歷經多次與數位金融、科技研發處的組織整合，至今已發展至 220 人的核心部門。王處長結合其風險控管思維，剖析金融高管在面對 AI 轉型時的策略藍圖與實務應用。

自 2022 年底 ChatGPT 問世以來，AI 被視為 50 年來最重要的科技變革，其影響將全面深入個人、企業、產業與國家。目前高達 75%至 90%的企業首長已將生成式 AI 列為經營策略的三大重點之一，不論大中小企業都陷入「AI FOMO(Fear Of Missing Out)」的變革焦慮中。臺灣雖然站在全球 AI 硬體製造的風口浪尖，但製造業賺取的是價值鏈底層的利潤。更關鍵的是，臺灣在使用 AI(應用端)上仍處於初期階段。對金融業等服務業而言，應用 AI 與製造業直接靠硬體賺錢的邏輯不同，金融業必須先投入龐大且高昂的算力與建置成本，才能經由流程轉化產生價值。這導致多數金融高管一邊面臨看不到實質短期回報的憂慮，一邊又因 FOMO 焦慮而不得不持續投入。

王處長表示以中國信託等大型銀行為例，財富管理業務一年能賺取兩三百億元的利潤，但這些利潤並非來自大眾市場，而是由僅占 4%(約 40 萬名)的高資產客戶所貢獻，呈現嚴重的「九一法則」。在 AI

時代，如果競爭對手或新創科技能利用 GenAI 技術，以極低的成本將原本專屬於富豪的精準、客製化理財與徵信服務普及至廣大的小資族，那麼傳統銀行的生存之道將面臨嚴峻挑戰。一旦這 4%的核心客戶因科技變革而變心，對銀行而言將是致命的商業危機。因此，管理層必須體認到，未來十年至二十年間，放款、徵信、理財等核心業務能力，將會逐漸被一個又一個的「AI Agent(AI 代理人)」所取代。王處長強調並非所有問題都需靠 AI 解決。有時候在既有流程上做個小幅優化(如簡單的系統串接或自動化調整)，就能輕易產生高達節省「100 個人年」的巨大效益，因此實務上應理智評估工具的適用性。

王處長建議金融機構在推動 AI 應用時，應遵循清晰的機制，在對象面，優先從內部員工的輔助工具做起，確保安全與準確性後，再逐步走向面對外部客戶；在複雜度方面，從簡單、被動的資訊查詢與客服，逐步演進至複雜、主動的業務協作、精算與智慧化決策。

金融業具備「客戶多、資料多、資金多」的特性，因此 AI 治理不能只看單一專案，必須提升至基礎建設的策略層級。中信將其歸納為「五大類基建治理」，要求建構一幅企業級的大藍圖，以集中投資、明確權責，並確保開發出來的 AI 模組能被各部門跨單位複用，避免資源重複浪費。過去銀行的產品規範、法規合規文策、銷售話術等知識，多分散在 Word、PDF 或 PPT 等非結構化檔案中。GenAI 的治理實務，核心在於將這些企業自身的「顯性知識」有系統地灌輸給模型，將其轉化為 AI 可靈活調用的「隱性知識」。

以中信開發的「AI 徵信助理」為例，剛上線時其能力可能僅相當於工作 6 個月的新進員工，表現並不完美；但隨著企業知識持續注入與機器學習，上線 1 年後就能快速提升至相當於 3 年資歷的熟練徵信員，進而超越目前處內平均年資 2 年的同仁。在此實務過程中，企業必須制定明確的營運模式，定義好人與機器之間的邊界與責任分工(如 Human-in-the-loop 人機協作)。同時，管理層必須評估自身的風險胃納，因為「沒有風險就沒有收益(No risk, no revenue.)」，治理必須在風險控管與商業效益之間取得細緻的平衡。為落實治理並解決導入時的流程細節，金融機構必須成立跨功能的「AI COE(Center of Excellence，AI 卓越中心)」。透過這個包含決策委員會、推動中心、業務前台、技術團隊、資安與風控單位的虛擬組織，來進行全行的資源調度與技術落實。

王處長最後總結，這個世界與 AI 模型並不完美，隨之而來的幻

覺與盲點依賴人類去把關。越是在 AI 鋪天蓋地的時代，人類的獨立提問能力、批判性思考與反覆驗證的核心價值就越發關鍵。企業與員工不應只是恐懼被取代，而是要思考「有哪些事情是 AI 學不會的」，主導人機協作的節奏，用其好處並避其壞處，這才是金融業高階管理階層在數位轉型下的正道。

提問與交流

Q1: 傳統金融業在推動金融科技跟 AI 轉型時，往往面臨由上到下的觀念凝聚與文化挑戰。中信在實務經驗上，對上如何說服高層投入 AI 資源並凝聚共識？對下若同仁面臨抵抗情緒，有何突破的心法？中信是否有具體的量化指標來追蹤轉型進度？當同仁活用 AI 產生想法時，管理階層又如何重新定義生產力，以避免「依賴 AI 等於沒有生產力」的矛盾觀點？

A1: 說服高層的核心心法在於運用「ALIVE」活著原則，亦即提案必須務實且可執行(Actionable)、從小做起並追求快贏的低投入(Low effort)、能讓老闆快速看到成效(Immediate)、成果顯而易見(Visionable)以及能講出打動人心故事的情感連結(Emotional)，中信便是依循此原則讓高層願意在八、九年間持續投入數億資金。而在推動過程中，基層同仁通常不是最大問題，反而是各業務單位因各擁兵權與資金、皆想主導 AI 主權而難以合作，這時必須訴諸跨單位的「數據與 AI 治理學」，透過拉高至董事長或治理委員會的策略層級來做決策與收斂。對於整體的轉型、分工與生產力評估，中信建立「治理委員會討論機制」，將所有提案依據價值、排序和特質分流至不同艦隊(業務單位主導、科技單位創新研發、或 IT 單位直接外購 Solution)，儘管實務上各單位在爭執中磨合是金融業常態，但透過容錯創新與頂層治理的架構，便能有效地讓案子源源不絕地務實落地。

Q2: 關於 AI 金融落地的三個關鍵實務挑戰：第一，前中後台與 IT 如何進行角色分工與互補，傳統 RPA 又如何更新科技協同？第二，若金融業大力投入，為何智能客服的成效仍然不如理想狀態？第三，面對 FinLLM 的幻覺與顯性知識文件源頭寫錯的風險，我們要如何確保 AI 輸出的正確性？

A2: 面對生成式 AI 的幻覺風險，中信在早期技術未完全成熟時，會將 AI 嚴格限制在「理解客戶內容」的範疇而非直接執行 Action，

理解後再由系統提供建議並透過「人機協作」模式進行最終輸出，藉此將幻覺影響降到最低。隨著今年生成式 AI 客服正式上線 To C 服務，團隊透過演算法設計控制、紅隊滲透測試與高達 5,000 題的測試，成功將正確率拉升至 99.9%以保持可控，但由於 AI 仍存在犯錯可能，目前中信皆將其定位在「服務」而非產品銷售，並在前端提供充分的警示提醒。最重要的是，管理階層與內部治理委員會必須建立「AI 如同新人也會犯錯」的願意容錯心智，上線後更要有專責團隊不斷針對 Try and error 的過程進行版本優化與客訴容錯機制，創新的 AI 科技才有可能在高度監管的金融業順利上線落地。

總結

「AI 與雲端賦能：建構金融產業智慧未來」國際研討會在來自國立政治大學金融科技研究中心、AWS、Arta Finance 及中信銀行等國內外專業講者的精彩分享中圓滿落幕。講者們從政策發展、金融 AI 生態系、雲端技術應用，到生成式 AI 實踐案例等面向，深入探討 AI 與雲端技術如何驅動金融產業未來發展，全面剖析資產管理產業發展的機會與挑戰，並提供深具洞見的觀點與建議。與會者涵蓋主管機關、銀行、證券、投信等各界金融專業人士，現場互動熱絡，提問踴躍。未來證基會將持續配合主管機關政策與全球趨勢，舉辦多元主題活動，促進金融知識交流，協助我國金融從業人員掌握產業脈動，共同思考金融產業未來的創新方向與發展契機。