

編號：3127

議題研析

一、題目：AI 代理金融服務相關法制研析

二、議題所涉法規

人工智慧基本法、人工智慧風險分類框架(草案)

三、背景說明（緣起）

近年生成式人工智慧(Generative AI)快速發展，具備自主規劃、執行任務能力之 AI 代理(AI Agent¹)已逐步導入金融服務領域，應用範圍涵蓋投資建議、資產配置、交易執行及信用管理等。2026 年²，美國線上券商 Robinhood 推出「代理交易」(Agentic Trading)服務，由 AI 代理依投資人設定之策略及風險偏好，自主監控市場並執行股票及選擇權交易，引發市場高度關注。AI 代理金融服務雖有助降低投資門檻、提升交易效率及促進金融創新，惟亦可能衍生演算法透明性、責任歸屬、投資人保護、資訊揭露及風險控管等問題³。

四、問題爭點

當 AI 代理協助授信蒐證、比對交易異常、整理疑似洗錢案件、追蹤法規更新，或在投資研究中自動蒐集資料並形成建議時，風險已

¹ 我國通常將 AI Agent 譯為「AI 代理」或「AI 代理人」，係指具備自主運作 (autonomous) 能力、無需人類介入的 AI 系統。使用者只需下達指令，AI Agent 便能感知環境、解讀意圖；面對高複雜度任務時，它會自行拆解步驟、制定計劃並執行。任務完成後，更具備分析資訊、自我進化的能力。摘自曾子軒，AI Agent 來了，但它是什麼？AI 代理定義、應用、挑戰全解讀，遠見雜誌，115 年 5 月 26 日，網址：<https://www.gvm.com.tw/article/113965?srsltid=AfmBOopFp hWSc9-ARoIiTSA2Xj3wUvRe4czgKnmuTfjjjcKci-3taqYr>，最後瀏覽日期：115 年 7 月 6 日。

² 本文有關年分之使用，原則以民國紀年表述，惟涉及外國法制或立法例部分，改採西元紀年表述。

³ CMoney，AI 代理人殺進華爾街！Robinhood 開啟「自動交易時代」，投資門檻與風險雙雙飆升，115 年 6 月 19 日，網址：<https://cmnews.com.tw/article/cmoneyairesearcher-9e5732fc-6bac-11f1-a306-e4d42e4671f0>，最後瀏覽日期：115 年 7 月 6 日。

不只是「答案是否正確」，而是 AI 是否可能在資料、流程與判斷之間存在未被監督的隱藏破口⁴。面對 AI 代理金融服務快速發展，各國已開始檢視現行金融監理架構是否足以因應相關風險，相關法制發展趨勢，值得我國持續關注。爰簡介美國 AI 代理相關法制規範，以做為我國參考借鏡。

五、探討研析

（一）我國 AI 代理金融服務概況

考量 AI 代理具備目標導向、任務規劃、多步驟執行、可呼叫工具及跨系統存取資料等特性，為引導金融機構善用技術並建立安全治理框架，金融監督管理委員會（下稱金管會）將研議增修相關規範或指引，以引導金融機構安全運用⁵。惟目前我國尚未針對 AI 代理金融服務制定專門法規，相關監理仍以既有金融法規及 AI 治理政策為基礎，並依金融業實際應用情形逐步調整監理措施。此外，為促進 AI 穩健及安全發展，金管會亦配合數位發展部依「人工智慧基本法」發布之「人工智慧風險分類框架」⁶，盤點金融業 AI 應用場景及潛在風險，並據以研訂以風險為基礎之 AI 應用管理規範⁷。

（二）美國 AI 代理金融服務相關規範簡介

美國金融業監管局(FINRA)發布的 2026 年監理報告指出，AI 代理係指能夠代表使用者自主執行及完成任務之系統或程式。此類 AI 代理可強化生成式人工智慧之功能，使使用者得以實現更多元之任務自動化，並能以較傳統流程自動化更迅速且更具成本效益之方式，存

⁴ 黃仕杰，當 AI 不只回答、還會執行：代理式 AI 如何重塑金融監理與法遵治理？FIND，115 年 7 月 3 日，網址：https://www.find.org.tw/indus_trend/browse/0e74b85bda6de7e8d66c1f130c4106fd，最後瀏覽日期：115 年 7 月 6 日。

⁵ 金融監督管理委員會，「金融科技發展業務之推動情形與展望」專題報告，立法院第 11 屆第 5 會期財政委員會第 13 次全體委員會議，115 年 5 月 7 日，頁 12。

⁶ 數位發展部，訂定「人工智慧風險分類框架」，並自即日生效，115 年 7 月 7 日，網址：<https://moda.gov.tw/press/bulletin/20086>，最後瀏覽日期：115 年 7 月 14 日。

⁷ 金融監督管理委員會，同註 5，頁 13。

取、處理及運用更廣泛之資料與資訊系統⁸。該報告亦指出，AI 代理之應用仍伴隨多項風險與挑戰，可能對投資人、金融機構及金融市場造成不利影響。因此，FINRA 建議，開發和探索 AI 代理的公司應審慎評估其自主性是否帶來新的監管、監督或操作上的挑戰，並可能需要根據 AI 代理的類型和範圍，制定特定的監管流程⁹。顯示 FINRA 現階段之監理重點，並非針對 AI 代理建立新的法律規範，而係要求金融機構於導入 AI 代理時，應依既有監理要求建立適當之治理、監督及風險管理機制。

目前美國雖少有法律和司法判決明確規範 AI 代理，惟現行法律和監理原則已要求金融機構負有管理、監督及說明 AI 代理運作之責任¹⁰。因此，當 AI 代理依據客戶風險屬性自主提供投資建議、調整資產配置或代為執行交易時，即可能適用「1940 年投資顧問法」(Investment Advisers Act of 1940)¹¹、「最佳利益規則」(Regulation Best Interest)¹²及「市場准入規則」(Market Access Rule)¹³等規範。其中，「1940 年投資顧問法」及「最佳利益規則」要求金融機構應以

⁸ FINRA, FINRA Publishes 2026 Regulatory Oversight Report to Empower Member Firm Compliance, 2025 年 12 月 9 日，網址：<https://www.finra.org/media-center/newsreleases/2025/finra-publishes-2026-regulatory-oversight-report-empower-member-firm>，最後瀏覽日期：115 年 7 月 7 日。

⁹ 林昭衡，RightCapital 推業界首個 AI 財務規劃代理 金融監管機關示警 AI 風險，理財周刊，115 年 6 月 25 日，網址：<https://www.moneyweekly.com.tw/ArticleData/Info/Article/234390>，最後瀏覽日期：115 年 7 月 7 日。

¹⁰ Jonathan Tam, United States: Legal Accountability for AI Agents, Baker McKenzie, 2026 年 7 月 1 日，網址：<https://www.bakermckenzie.com/en/insight/publications/2026/06/united-states-legal-accountability-for-ai-agents>，最後瀏覽日期：115 年 7 月 7 日。

¹¹ SEC 控訴 Delphia 與 Global Predictions 二間投資顧問公司不實且誤導性地誇大其於提供投資建議上對 AI 之運用或謊稱其於提供投資建議上使用 AI，因而違反「投資顧問法」第 206(2)條之「反詐欺條款」，同時違反同法第 206(4)條之「行銷規則」與「合規規則」。摘自陳立承編譯，〈美國證券交易委員會加強管制「AI 不實使用之行銷」投資詐欺行為〉，《經貿法訊》，第 329 期，113 年 5 月 10 日，頁 25。

¹² 在「最佳利益規則」下，只要 AI agent 提供個人化投資建議，它就會被視為券商建議流程的一部分，並必須在揭露、適當性、利益衝突管理與內部控制上全面符合「最佳利益義務」。摘自謝孟珊，金融科技的浪潮襲來——機器人投顧的法制議題分析，法律白話文運動，112 年 3 月 4 日，網址：<https://plainlaw.me/posts/robo-adviser>，最後瀏覽日期：115 年 7 月 6 日。

¹³ 「市場准入規則」即美國證券交易法(Securities Exchange Act)第 15c3-5 條(Rule 15c3-5)，要求所有可直接進入交易所或另類交易系統(ATS)的證券經紀商(broker-dealers)，必須實施嚴格的風險管理控制與監督程序，以確保金融體系的穩定與市場誠信。摘自 databento, What is the Market Access Rule? 網址：<https://databento.com/microstructure/market-access-rule>，最後瀏覽日期：115 年 7 月 6 日。

客戶最佳利益為優先，建立適當之利益衝突管理及資訊揭露機制¹⁴；若 AI 代理涉及自動執行交易，則尚應依「市場准入規則」建立交易前風險控制及監督措施¹⁵。即使相關投資決策係由 AI 代理完成，其法律責任仍由金融機構或投資顧問負擔，而非 AI 代理本身¹⁶，即 AI 目前在法律上不具備獨立人格，仍視為金融機構延伸之工具。

此外，美國證券交易委員會(SEC)及 FINRA 近年亦持續強化人工智慧應用之金融監理要求，包括建立模型治理、演算法監督、決策紀錄保存及風險管理等機制，並要求金融機構防範利益衝突及誤導性 AI 宣傳(AI Washing)¹⁷。

因應自主型 AI 代理快速發展，美國政府亦開始關注 AI 代理所衍生之新興治理議題。2026 年，美國國家標準暨技術研究院(NIST)提出「AI Agent Standards Initiative」，研議 AI 代理之技術標準與治理架構¹⁸；同年，美國國會亦提出「AI Agent Act」草案，規劃建立 AI 代理之安全標準及責任機制¹⁹。雖相關措施尚未完成立法，但已顯示美國監理方向除持續依循既有金融法規規範 AI 應用外，亦逐步朝建立 AI 代理之治理制度發展。

(三) 結語

¹⁴ 謝孟珊，同註 12。

¹⁵ Anthony Scott, What Is Algorithmic Trading? Definition, How It Works, and Is It Worth It, TradeAlgo, 2026 年 4 月 1 日，網址：<https://www.tradealgo.com/trading-guides/ai-trading/what-is-algorithmic-trading-definition-how-it-works-and-is-it-worth-it>，最後瀏覽日期：115 年 7 月 8 日。

¹⁶ Jonathan Tam，同註 10。

¹⁷ Kevin LaCroix, Guest Post: AI, the SEC, and the 2026 Reporting Season, The D&O Diary, 2026 年 2 月 5 日，網址：<https://www.dandodiary.com/2026/02/articles/artificial-intelligence/guest-post-ai-the-sec-and-the-2026-reporting-season/>，最後瀏覽日期：115 年 7 月 7 日；Global AI Governance, SEC AI Governance Guidance, 網址：<https://aigovernance.com/entry/sec-ai-governance-guidance>，最後瀏覽日期：115 年 7 月 7 日。

¹⁸ NIST, Announcing the "AI Agent Standards Initiative" for Interoperable and Secure Innovation, 2026 年 2 月 18 日，網址：<https://www.nist.gov/news-events/news/2026/02/announcing-ai-agent-standards-initiative-interoperable-and-secure>，最後瀏覽日期：115 年 7 月 7 日。

¹⁹ Mark Warner, Warner Unveils Discussion Draft of Legislation to Create Innovative Market for Secure Artificial Intelligence Agents, 2026 年 6 月 29 日，網址：<https://www.warner.senate.gov/newsroom/press-releases/warner-unveils-discussion-draft-of-legislation-to-create-innovative-market-for-secure-artificial-intelligence-agents/>，最後瀏覽日期：115 年 7 月 7 日。

AI 代理金融服務所涉及之責任歸屬、演算法治理、資訊揭露及投資人保護等議題，均可能對現行金融監理帶來新的挑戰。鑑於美國目前係採既有金融法規配合 AI 治理之監理模式，並持續研議相關制度及技術標準，我國未來可持續關注其法制發展及實務運作經驗，同時衡酌國內金融市場發展情形，適時檢視現行法制及監理措施，俾利兼顧金融創新、風險管理及投資人、金融消費者權益保障。

撰稿人：林鈺琪