專題

生成式人工智慧輔助主計相關業務應用的限制與發展

生成式人工智慧（Generative AI）近年來進步飛快，其潛力無疑地再次燃起以資訊技術成功提升政府效能的希望。因此，可否應用至主計業務增加工作效率，舒緩人力負擔成為眾多主計同仁的期待。但生成式 AI 仍存在相當多技術及應用限制，並非無所不能，為避免過多錯誤的期待，本文就目前比較成熟的應用方式如何輔助主計相關業務，提供主計人員參考。

張文熙（財政部財政資訊中心主任）

壹、前言

生成式 AI 係依據大量預訓練資料轉換模型生成包含文字、圖像、聲音等不同形式內容（Kalota, 2024）。生成式 AI 生成內容過程，雖然係依使用者輸入提示需求就已學習的資料結合系統參數生成內容，但使用者並無法直接控制生成結果，且經常有超乎使用者預想的可能，其優點是可以生成具有創意的答案，缺點可能產出無中生有的虛構結果。但傳統主計業務，包含預算、會計、統計等，均強調計算及細緻精準數值分析，生成式 AI 卻存在生成結果不受控的特性，可能與主計人員預計有所差距，不只不利於業務輔助，甚至造成業務錯誤，應用時不得不慎。本文針對這些情況，提出常見的有效控制措施以及必須避免的使用情境，分別針對發展趨勢、可用技術、風險控制等必要手段加以描述，提供有意運用生成式 AI 功能的主計同道作為發展參據。

貳、AI 應用前提

沒有 AI 技術背景或運作經驗的組織欲導入 AI，往往依賴承包商所設想的管理方式，經常是見樹不見林，並不容易貼近特定領域需要。現階段 AI 工具建置成本高，理論內容複雜，不僅非技術人員不易理解，資訊人員也未必能夠深入，AI 應用常被視作黑箱，解決根本

之道必須有計畫設計推動 AI 認知教育，有正確認知後才能正確規劃，否則失敗機會非常大。以財政部財政資訊中心爲例，109 年起即開始推動機器學習教育訓練，直到 112 年起才能眞正進入稅務應用情境內取得成果。而生成式 AI 引用至今，仍在試驗可能應用範圍，預計於 114 年 12 月才能完成第一階段營運上線，意謂推動生成式 AI 應用需要較長時間耕耘，不易立即收效。

政府機關引用新興科技時，先決條件是要考量是否符合組織架構與當責等政治框架的限制，主計單位亦同。因此，建立信任、瞭解風險、安全管理及風險控管，是主計單位應用生成式 AI 解決方案前，必須考慮的四大支柱基礎。由於提供可信任的結果是公部門應用的首要條件，生成式 AI 工具存在幻覺（hallucination）的特性是最主要的應用障礙，若產出無中生有的虛構事實，造成用戶不可信任的結果將嚴重影響機關信譽及運作錯誤，後果不難想像。大體上，主計核心業務可適用的生成式 AI 工具，以文字生成功能應用爲主，生成內容又必須本於法規內容，但法規存在明顯地域性及語言差異，大型語言模型原始預訓練資料又來自於網際網路，未經篩選的資料再加上幻覺的副作用，生成結果不依我國主計規定的回答機率很高，也意謂結果無法使用。此外，生成結果的解釋性對實務使用性影響也很大，AI 技術理論複雜，非專業人士難以理解，當結果產生懷疑或歧義時，如何解釋 AI 的推理過程成爲重要的裁處依據，大型商用 AI 工具若其演算法非屬公開程式時無從瞭解推理過程，阻礙持續使用的意願。所以，主計人員應用 AI 前，先了解生成特性可能造成的風險，進行安全管理及控制風險措施投入開發有其必要。

參、封閉式環境的需要

主計是一般行政機關中重要的幕僚單位，執行內部審核，協助各機關發揮內部控制的功能，是機關業務順暢的重要基礎。在內部審核過程中需要大量文件審查，ChatGPT 等生成式 AI 工具擁有可以快速閱讀資料進而摘要分析的能力，雖然輸出結果存在不可完全信任的風險，但仍足以協助部分帳務與費用查核工作，惟必須維持人工把關的防線（human in the loop），雙重驗核對機關治理與內部控制有加成之效。此外，應用生成式 AI 另一顧慮是文件審查過程中，必須上傳待審資料到服務商伺服器內的大型語言模型處理，這些位於境外的大型語言模型，能否確保機關在資料傳輸及處理過程中，其資料機敏性不受侵害是主計人員相當關切的事項。使用開放式商業模型只能由使用者自行約束上傳資料內容，不易落實管制。採用封閉式環境建置生成式 AI 是最直接解決上述顧慮的有效方式，確保所有上傳資料都在機關可控範圍內進行處理不致外洩。目前各界積極朝主權式 AI（sovereign AI）發展避免技術及資料受控於特定國家而損及國家利益，其源於歐盟國家強調由國家或特定地區自主研發、掌控和應用 AI 的技

術和系統（Mügge, 2024），此概念強調 AI 技術本土化，內容經由國家控制，結合封閉式環境佈建，便可確保資料自主及合於本土文化及意識形態的推理邏輯生成各式內容。

封閉式環境佈建有兩種做法，一種是落地自建主機移植大型語言模型，資料完全在所屬機關內部，僅自行進行模型推理。但高效能主機建置成本高，大部分機關無法且無力負擔大型設備，只能購置小型設備選用參數量少的縮小模型，導致相對生成功能就少。自建還有一項重大缺點，就是主機圖形處理器（GPU）比傳統主機更需要散熱，除本身耗電外，空調負擔十分吃重，供電要求很高，中小型規模政府機關無法維運。折衷方案是選擇封閉式介接外部大型語言模型較爲可行，不須自行處理設備維運工作相對划算。例如，共用政府自建於國家高速網路中心的泰德語言模型（TAIDE），是我國朝主權 AI 發展的具體案例，但目前算力規模仍不如主要的三大境外服務商，更新及微調速度慢。其以虛擬私有網路連線（Virtual Private Network），資料及網路不會和其他用戶混雜，可確保資料不會輕易外洩，用租用的方法解決算力不足的問題。泰德模型的優勢在於以較多本土中文文件訓練，回答語義及語法較符合國人用法。未來類似 DeepSeek-r1（Guo et al., 2025）的技術驗證大型語言模型經過特殊蒸餾等方法可以縮小訓練資料及模型，主計單位可能有機會自建落地語言模型應用，不僅降低使用成本外，大大降低資料外流的風險，建置生成式 AI 的選項就更趨多元。

肆、主計業務數位轉型

主計基本業務進行方式，若因爲採用生成式 AI 工具改變傳統預算編製方式、帳務會計處理、統計分析等流程，稱爲主計作業典範的轉移（paradigm shift），因而得到更好更佳的作業品質，才是數位轉型，例如運用自然語言處理（NLP）技術，可快速處理大量資訊，提供快速摘要，找出內涵的洞見，如此便可協助檢視大量佐證文件並可自行比較，有助於內部審核實務應用。生成式 AI 要能在主計業務中發揮典範轉移的角色，並不能只依賴單一大型語言模型，必須將其功能融入現有系統及作業流程中，並與自動化功能結合，才可能達成轉型的目標。具體成效呈現應從現有主計業務的痛點著手，若因 AI 技術引入得以局部改善才有可能全面擴大，否則生成式 AI 僅能在少數輔助功能發揮功效，例如外語翻譯、會議摘要、會議紀錄製作等，雖有行政輔助的效益，但不會對業務產生革命性的進步。生成式 AI 的幻覺問題，須透過修正語言模型、利用已知資料微調、調整系統參數等方法改善，但就一般主計同仁而言，學習成本過高並不可行。利用已知知識設計有限範圍檢索，再將檢索所得重新以關鍵字描述，以主計人員的標準論述再輸入大型語言模型生成內容的做法，成本最低也能得到可以接受的結果。這種先行檢索再生成的方法，稱 augmented retrieval

generation（RAG）（Gao et al., 2023），結合主計法規等規範建立出 AI 主計專家的能力比較可行。

生成式 AI 提供自然語言對話能力取代指令操作，降低電腦使用門檻，加速了普及應用，提供更快速高效的運作、更細緻且精準的分析，以及更準確的預測等，使主計人員有更多精力從日常性工作投入到具價值創造性的工作中，才能達成誘發革命性變革，尚有待發掘更多顯著的效益案例才能奏效。生成式 AI 不僅取代中低階工作，事實上卻證實部分高階工作也可以被取代，未來將影響組織結構設計、業務分配、資源配置等。過去，主計電腦化作業基本上是依據人工流程思考設計電腦資訊流，而主計數位轉型則是依據主計最終目標以電腦邏輯蒐集所需資訊進行處理，顯然作業概念不同，將導致流程再設計可讓作業實質變革突破作業瓶頸。

伍、建立治理框架

生成式 AI 的應用能否成功，奠基於 AI 治理框架指引應用技術朝有效管理的方向發展，包括應用結果的透明性、解釋性、問責性、公平性、穩健性、隱私保護和資料安全等。生成式 AI 源自於大型語言模型原始訓練資料及演算法偏誤所造成的幻覺，透過資料治理機制以確保資料品質，建立模型測試和驗證機制，定期評估和改進治理框架可以降低部分風險，便可提高主計應用的可行性，包含資料治理、模型治理以及風險治理。

AI 應用關鍵基礎在於欲處理問題有充足資料。由於資料品質足以決定 AI 模型的有效性，若資料來源並未隨之擴展，無法發揮 AI 預期成效。在演算法不變的情形下，維持資料即時性、正確性、一致性決定 AI 系統品質。實務上必須先完成資料前處理作業後，才能進入建模作業。若能建立自動化資料治理應用系統而執行資料清洗、正規化、標準化等置前處理程序，更快速完成建模準備狀態，就能縮短模型上線時間加速應用。

因爲模型是基於所蒐集的資料透過數學描繪成公式，因此模型會隨資料及行爲變更影響偵測有效性，經常性觀測模型有效性，調校模型參數以維持一定的準確率成爲應用 AI 的新課題，否則往往造成上線初期可發揮效果，之後就逐漸衰減而失效。以詐騙偵測爲例，當詐騙者發現被偵測時必會想方設法推敲偵測邏輯，再想辦法規避，甚至也應用 AI 工具對抗或反制。以風險爲導向進行管理原則之設計，透過識別風險、風險分類分級、對高風險 AI 應用場景進行控管措施規劃。透過 AI 風險治理框架，制定相應的政策和程序，才能維持管理和監控有效性，包括確定治理目標和原則、明定權責及政策、訂定 AI 風險評估策略、明定模型生命周期要求，藉以設置相對應監測及檢測機制。

根據 Deloitte AI 研究院「企業人工智慧應用現狀分析報告」調查顯示，94%的受訪企業領導者表示 AI 在未來五年內對其企業成功至關重要，另

外 50％的受訪者提出 AI 相關風險管理是企業擴大 AI 專案規模的最大障礙之一，儘管如此，卻僅有 33％的受訪者將 AI 風險管理納入企業整體風險管理範疇。主計單位發展 AI 應用系統和模型時採取相關開發、測試和評估方式，以有助於確保其符合 AI 可信任原則。及時識別和應對 AI 潛在的問題和風險建立查核程序，透過制定具體的查核標準和指標，評估生成式 AI 應用系統合規性，在主計單位應用成功性才能提高。

陸、結論

目前政府機關業務系統應用生成式 AI 的情形普遍還處於初起步階段，僅著手嘗試小範圍功能應用以驗證可行性，更多仍是個人利用這類工具協助圖片、文稿生成或簡報等行政輔助，尚缺乏廣泛全面應用規劃。其中部分原因係大型語言模型進步太快，往往數週內就出現更新版本，租用單價也隨功能波動調高，對於作業性質固定的業務，如主計相關業務者，經常性變動造成規劃應用的困擾也會影響系統穩定性，不利實務推動及後續維運，加上大多數主計從業人員對 AI 技術原理瞭解並不深入，無法判斷正確實質條件限制為何，普遍於需求中存在過多不可行的期待而阻礙了發展。主計人員在這場主計業務典範轉移的變革中比資訊技術人員的角色更為重要，究竟希望生成式 AI 協助評估審查，或者取代多數的主計人員，將影響生成式 AI 選用及建置策略，需要主計人員訂出方向。故建議強化主計人員 AI 教育訓練，加入 AI 模型治理，以及評估治理成熟度等能力，方有足夠能力判斷現有主計機制能否適合生成式 AI 執行。由於政府機關對於內容生成不確定性以及資料上傳的風險顧慮遠大於民間機構，相對採取更保守的策略，加上 AI 的複雜性和自主性愈來愈高，存在著似是而非的結果、刻意偽造和不確定性等問題，若無法有效解釋其內容，將破壞對使用 AI 的信任。主計單位導入生成式 AI 應用，應同步導入防護和監控措施，若沒有建立有效的資料保護機制，可能面臨模型開發安全性疑慮和資料外洩等問題，導致不敢進一步運用生成式 AI 協助推動主計業務的進步，將會是相當可惜的結果。

參考文獻

1. Guo, D., Yang, D., Zhang, H., Song, J., Zhang, R., Xu, R., Zhu, Q., Ma, S., Wang, P., & Bi, X. (2025). Deepseek-r1: Incentivizing reasoning capability in llms via reinforcement learning. arXiv preprint arXiv:2501.12948.
2. Kalota, F. (2024). A primer on generative artificial intelligence. Education Sciences, No.14(2), p.172.
3. Müge, D. (2024). EU AI sovereignty: for whom, to what end, and to whose benefit? Journal of European Public Policy, No.31(8), p.2200-2225. https://doi.org/10.1080/13501763.2024.2318475
4. Gao, Y., Xiong, Y., Gao, X., Jia, K., Pan, J., Bi, Y., Dai, Y., Sun, J., Wang, H., & Wang, H. (2023). Retrieval-augmented generation for large language models: A survey. arXiv preprint arXiv:2312.10997, 2.❖