日本：金融廳提出 AI 徵詢文件 (3/4)

■ 日本金融廳提出「促進金融領域合理運用人工智慧之初步探討要點」，重點如下：

背景

- 生成式 AI 效能顯著提升推動社會變革，AI 可望大幅提高金融等各行各業以及日常生活各個層面的效率和便利性，提高人民生活水準和促進國家經濟發展。
- 生成式 AI 的使用帶來挑戰和新出現的風險，例如濫用導致犯罪和錯誤訊息的傳播。
- 雖然金融業正在積極探索 AI 之使用，但對風險和監管妨礙的擔憂產生疑慮。
- 金融業須意識到，若不積極導入 AI 之風險(risk of not taking actions)，恐將面臨技術創新落後，進而於中長期內難以持續提供高品質之金融服務。

■ 與 AI 使用相關挑戰

挑戰	面向	原因
傳統 AI 和生成式 AI 的共同挑戰	• 資料開發	• 因 AI 廣泛使用及發展，使金融機構面臨到確保模型建構所需之足夠訓練數據及數據的品質控制皆是挑戰。
	• 與第三方的合作及其風險管理	• 運作複雜 AI 模型需要專業知識，許多金融機構考慮利用外部廠商提供之解決方案。 • 為確保過度依賴外部廠商，金融機構須有具相關知識之人員，並考慮商業環境、工作流程及客戶需求。 • 對第三方廠商合作及集中於部分服務提供者，可能會造成系統性風險。
	• 投資報酬率	• 使用 AI 的收益難以估計，難以用來解釋其投資報酬率。 • 由外部廠商提供之生成式 AI 多數以使用量定價，成本可能因使用頻率而大幅增加。

使用生成式 AI 而更難解決的問題	• 問責制	• 生成式 AI 透過大量參數及參考文字、音訊或圖像等多面向資源生成答案，因此很難明確顯示如何得出最終之結果。
	• 偏誤	• AI 訓練數據、演算法及模型運算過程之偏誤，可能造成對部分客戶或員工產生不當對待之風險。 • 當訓練數據不充分，可能會強化偏誤風險。
	• 模型風險管理	• 雖然已開發 AI 風險管理架構，但針對生成式 AI 的發展、運作及管理仍在早期階段，尚未建立系統評估。 • 生成式 AI 的特有屬性造成傳統風險管理方式無法充分了解及控制所有潛在風險。
	• 個人資料保護	• 在下列應用時針對個資保護無明確規範。 (1)使用生成式 AI 將包含客戶資訊等個人資料作為訓練數據。 (2)將 AI 模型之發展及訓練過程交由外部廠商。 (3)使用伺服器位於海外之生成式 AI 平台。
	• 資訊安全與網路安全	• 包含生成式 AI 在內可能增強攻擊者的能力，增加金融機構受網路攻擊的可能性及影響。 • 金融機構使用生成式 AI 時，客戶資訊及重要業務資訊有外洩風險。 • 提示詞攻擊等攻擊可能造成 AI 系統故障及資料外洩。 • AI 模型本身也可能受到如資料汙染攻擊。
	• 人力資源	• 許多金融機構意識到需要雇用或培訓 AI 模型開發、營運及管理方面專家。 • 依賴外部廠商可能會影響組織內部之專業知識及智慧財產權的累積，減緩內部人力資源的發展。 • 缺少可以為持續營運及選擇最佳方案之人才，以及可以作為業務部門及 IT 部門溝通橋樑之人才。 • 因生成式 AI 特有風險，傳統 AI 教育尚有不足。
生成式 AI 帶來的新挑戰	• 人工智慧幻覺	• 提供不正確資訊或產生導致信用或法律風險的結果，可能損害金融機構之信譽。 • 如果商業設計不恰當、參考來源選擇不夠充分及準確度無法提升，即使採取檢索增強生成方式，仍有產出錯誤之風險。

		• 員工使用生成式 AI 對外回應可能會有傳達錯誤資訊之風險。
	• 濫用生成式 AI 進行金融犯罪	• 隨著生成式 AI 可產生自然的文字、音訊與視訊，犯罪技術變得複雜，金融機構及客戶面臨的風險增大。 • 除網路釣魚詐騙等手段日益複雜外，深度偽造技術產生之虛假視訊及音頻，使詐騙更加容易。 • 傳統的 KYC 程序和身分驗證系統難以區分真人和網路詐騙。
	• 金融穩定挑戰	• 國際上持續討論生成式 AI 對金融穩定的影響及風險，各項風險將持續受到國際組織之關注。

■ **結論**

多方利害關係人相互合作之重要性

- 隨著 AI 的應用加速，強化金融業和整個社會的合作以克服挑戰和最大限度地發揮 AI 所帶來之利益。
- 因小型金融機構的能量有限，產官可合作推動 AI 治理。
- 日本金融廳將推動下列措施：
  - ✓ 與其他部會和機構合作及參與國際規則制定。
  - ✓ 計畫協助金融業妥善利用 AI。
  - ✓ 持續利用日本金融科技週[註 1] 等為國內外公共和民間利害關係人溝通，實現開放式創新，並提升監管的可預見性。
  - ✓ 計畫主導 AI 多方利害關係人研究群(Multi-stakeholder Study Group)。

■ **徵求意見**

- 日本金融廳就本案對外徵詢意見及建議[註 2]，其強烈贊成妥善使用 AI，並表示本文件僅為初步分析，議題可能會隨著技術創新和商業環境改變產生重大變化。

註 1：此活動將舉行各項金融科技相關活動，致力於促進日本金融科技創新之發展，提供日本及世界各地之金融科技專業人士交流。

註 2：如有意見可聯繫金融科技與創新辦公室，此單位隸屬金融廳策略發展管理局風險分析課，其主要業務包含金融系統風險、趨勢進行綜合性或個別分析研究，金融科技與創新辦公室負責協助金融科技相關業務。

資料來源：日本金融廳