主題	**ISACA Journal : AI 的可用性風險** **Information Security Matters: Artificial Intelligence Availability Concerns**
類別	訊息新知 (Nov. 2026)
內容	企業談到 AI 資安時，通常著重於資料隱私、模型攻擊、資訊完整性及可稽核性，卻容易忽略另一項關鍵風險，也就是 AI 系統的可用性。隨著 AI 快速導入財務、客服、人力資源及其他重要業務流程，企業不僅要確認 AI 是否安全，也必須評估系統中斷時，關鍵營運能否持續。 AI 系統具有「動態性」與「非確定性」，模型可能隨著資料、訓練及執行環境持續改變。因此，即使系統完成復原，也不代表復原後的模型與故障前完全一致，更無法直接認定其輸出品質及安全控制仍然可靠。對 AI 而言，「服務恢復（Recoverability)」不等於「恢復可信（Reliability)」。 此外，AI 的備份與復原比傳統資訊系統更複雜。企業必須同步保存演算法、模型狀態、訓練與測試資料，以及相關運算環境；大型語言模型還涉及龐大資料量及高成本的 AI 晶片資源，完整備份與快速復原在實務上可能相當困難。 為降低中斷風險，企業可採用檢查點式訓練（checkpoint-based training)、溫備援或熱備援（warm and hot standby）模型，並透過跨區域部署（multiregional implementation）避免單點故障。同時，應將 AI 可用性納入公司治理、風險管理、災難復原及營運持續計畫，建立服務降級、人工接管與定期復原演練機制。 企業導入 AI 時，不能只評估模型是否準確、效能是否良好，更應確認：當 AI 停擺時，業務能否繼續；當 AI 恢復時，系統是否仍然可信。 更多詳細的內容，可以參考底下的連結: https://www.isaca.org/resources/isaca-journal/issues/2026/volume-5/artificial-intelligence-availability-concerns