

主題	ISACA 白皮書：保護 AI 代理程式的資安建議 Cybersecurity Recommendations for Securing AI Agents
類別	訊息新知 (Oct. 2026)
內容	當生成式人工智慧快速走入企業營運，AI 代理程式已不再只是回覆問題的工具，而是能夠主動擷取資訊、分析情境、呼叫系統並執行任務的新型數位工作者。它帶來效率、創新與服務升級的巨大潛力，也同步擴大資訊安全與治理風險。一旦代理程式受到提示注入、權限設定不當、惡意內容或供應鏈弱點影響，原本用來提升生產力的能力，就可能轉化為資料外洩、未授權操作、財務損失與法遵事件。 AI 代理程式可擷取不受信任的內容、針對企業資料進行推理，並透過工具、API 與自動化工作流程採取行動，因此帶來獨特的風險樣貌。要保護這類代理程式，必須結合傳統資安控制與 AI 專屬防護，以因應提示注入、工具濫用、過度自主、記憶體洩漏，以及模型或供應鏈遭入侵等風險。本白皮書為企業人員提供一組控制措施及安全預設檢查清單，協助企業保護 AI 代理程式。 本白皮書值得所有正在評估、導入或管理 AI 應用者細讀。不僅說明 AI 代理程式的特殊攻擊面，更以十一項實務類別，完整整理治理與風險權責、安全開發、身分驗證、最低權限、網路分段、沙箱執行、提示注入防禦、資料與記憶體保護、工具及 API 整合、政策強制執行、人工監督、持續監控、事件應變及供應鏈安全等關鍵控制。 更多詳細的內容，可以參考底下的連結： https://www.isaca.org/resources/white-papers/2026/cybersecurity-recommendations-for-securing-ai-agents