主題	**授權危機迫在眉睫？傳統 IAM 已無法駕馭「代理型 AI」** **The Looming Authorization Crisis: Why Traditional IAM Fails Agentic AI**
類別	訊息新知 (Feb 2026)
內容	隨著人工智慧技術的演進，「代理型 AI」(Agentic AI) 正迅速成為企業自動化的新主力。與傳統的被動工具不同，這些 AI 代理具備高度自主性，能夠獨立決策、執行跨系統任務，甚至生成子代理(Sub-agents) 來協作完成目標。然而，這種技術飛躍也暴露了現有資安架構的嚴重裂痕——傳統的身份與存取管理 (IAM) 系統，正逐漸失去對這些「數位員工」的控制力。 企業正面臨一場「授權危機」。傳統 IAM 主要是為人類使用者所設計，依賴靜態的角色與長效的權杖 (Tokens)。但 AI 代理的運作模式截然不同：它們需要的是動態、細顆粒度且基於上下文的即時授權。當我們試圖用管理「單一用途程式」的舊邏輯，去規範能夠自主互動、甚至代表多個委託人行事的 AI 代理時，就會產生巨大的安全漏洞——從非人類身份 (Non-Human Identity) 的爆炸性增長，到難以追蹤的複雜委派鏈，這一切都讓「零信任」架構面臨前所未有的考驗。 那麼，當您的 AI 代理在毫秒間生成了數個子代理並存取敏感 API 時，您是否真的知道「誰」在執行操作？此外，當發現異常行為時，現有的系統是否具備「全域即時撤銷」的能力，能在代理造成破壞前切斷所有連結？ 在這篇文章中，深入探討了為何傳統 IAM 在 Agentic AI 時代宣告失靈。文章分析了「秘密蔓延」(Secret Sprawl)、複雜的委派歸屬以及全球登出困難等核心挑戰。這不僅是技術問題，更是深刻的策略難題。本文呼籲組織必須立即行動，重新思考身份治理策略，建立能適應動態機器經濟 (Machine Economy) 的新型防護網，避免因過時的安全假設而陷入災難性的濫用風險。 全文詳閱: https://www.isaca.org/resources/news-and-trends/industry-news/2025/the-looming-authorization-crisis-why-traditional-iam-fails-agentic-ai