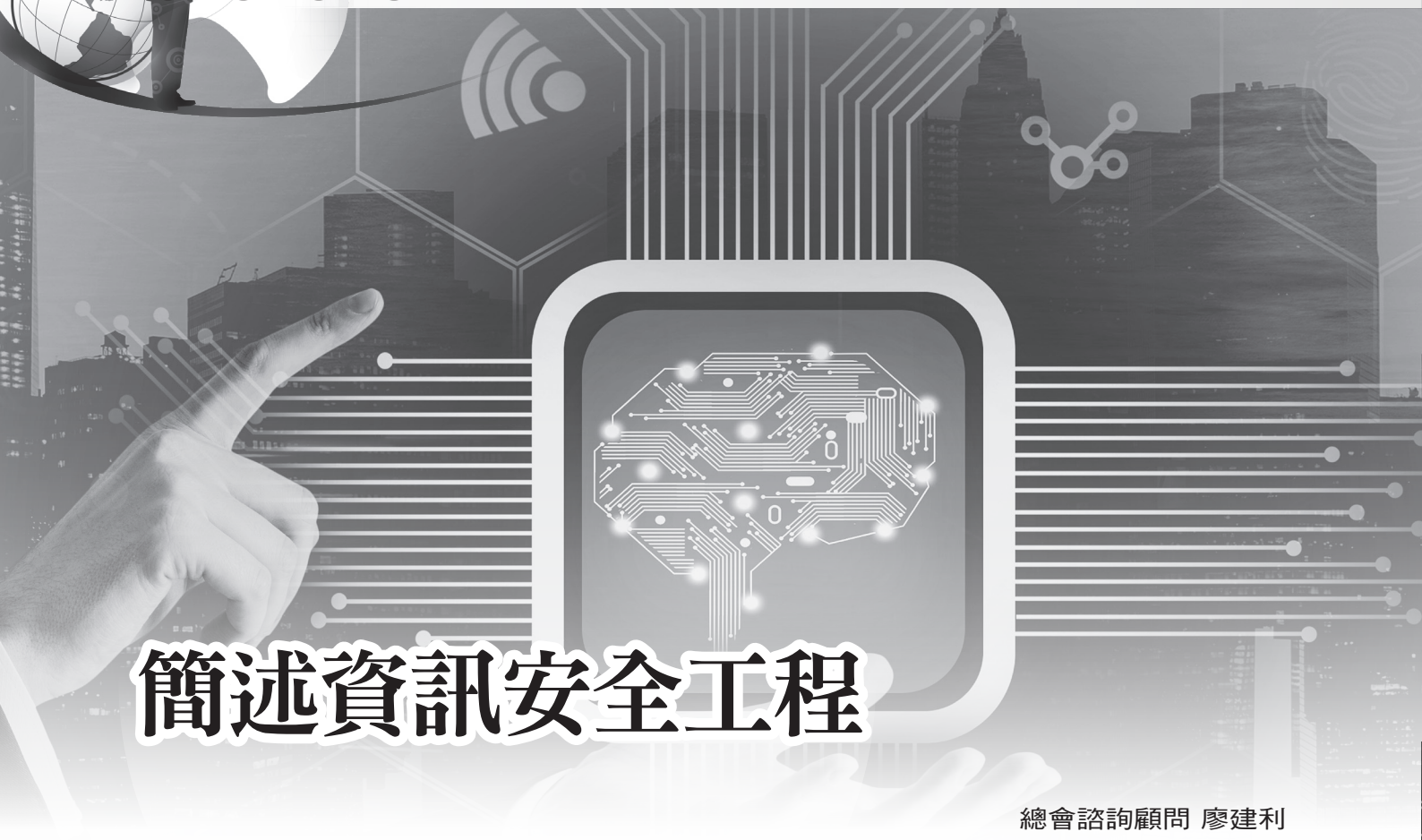

簡述資訊安全工程

總會諮詢顧問 廖建利

資訊安全工程是一個關鍵性的領域，意在保護電腦系統、網路和數據不得授權的訪問、損壞或滲透。該領域重點關注發展有效的安全策略和措施，以應對不斷變化的威脅和攻擊手段。

信息安全工程包括多個關鍵步驟。首先，進行風險評估，創造潛在的風險和威脅。其次，制定適合組織需求的安全策略和控制措施，確保系統和數據的特異性和可用性。然後，實施技術和物理安全措施，例如防火牆、入侵檢測系統和身份驗證，以防止未經授權的訪問。同時，執行教育和培訓計劃，提高用戶的安全意識和知識，減少人員對安全的潛在影響。

另外，資訊安全工程需要定期進行安全審查和漏洞掃描，以確保系統和應用程序的漏洞得到及時修復。還要製定應急響應計劃，以查找可能的安全事件和事故，迅速提供服務並減少損失。

資訊安全工程的目標是建立一個穩固且可靠的安全環境，確保數據得到保護，系統運行不止，並確保組織和用戶的信心行為。隨著技術的發展和威脅的不斷演變，資訊安全工程將繼續成為企業和組織中塔的一部分，以保護其業務和資產塔潛在的威脅和攻擊。

資訊安全工程是保護電腦系統、網絡和數

據倉庫未經授權訪問、損壞或入侵的領域。它包含以下主要領域和相關注意事項：

◎系統安全：確保計算機系統和服務器的安全性，包括操作系統和應用程序的安全設置、漏洞修復、防火牆和入侵檢測系統的使用等。

◎網絡安全：保護企業網絡貨物攻擊和未授權的訪問，使用加密通訊和虛擬私人網絡（VPN）等技術。

◎數據安全：確保敏感數據的保密性和完整性，利用加密技術、訪問控制和備份措施來保護數據。

◎身份驗證和訪問控制：確保只有授權用戶才能訪問特定數據和系統，使用多身份驗證（MFA）等增強的機制驗證。

◎安全審查和監測：定期進行安全審查和監測，發現並獲取潛在的安全漏洞和事件。

◎安全意識培訓：提供安全意識培訓，教育用戶識別並應對安全威脅。

在未來措施方面，技術創新隨著科技的發展，新的安全威脅不斷出現。資訊安全工程師需要密切關注技術創新，並持續採用新的安全措施來應對新的威脅。

◎人工智慧和機器學習：人工智慧和機器學習技術可以用於威脅檢測、行為分析和安全預測。