研　習　紀　錄

很榮幸邀請國立台北科技大學魏銷志副教授講演，深刻點出了在生成式AI（GenAI）普及後，資安防禦所面臨的典範轉移。首先，最令人警惕的是攻擊門檻的大幅降低與社交工程的進化，在演講中提及 2024 年初發生的 Arup 集團案例，詐騙集團利用 Deepfake 技術偽造了整場視訊會議中的同事與財務長，成功騙取鉅額款項。這凸顯傳統資安驗證機制已不足以應對現今網路攻擊及社交工程，因為眼見不一定為憑，組織必須培養員工具備更深層的批判性思維與查證能力 。

其次為「影子 AI（Shadow AI）」與資料外洩成為企業內部的隱形炸彈。許多員工為了效率，在未經核准下將公司機密或個資輸入至外部 GenAI 平台，導致敏感資料流出。講者於演講中強調，單純的禁止難以奏效，企業應轉向「治理」，例如導入 AI DLP（資料外洩防護）技術來偵測敏感資料 ，並建立明確的 AI 使用政策與白名單機制 。

於演講最後中提出的解決方案從技術延伸至管理層面，強調了導入 ISO/IEC 42001 人工智慧管理系統的重要性 ，以及未來 AI 系統部署可能需要類似軟體物料清單的「AIBOM」來確保模型來源與訓練資料的透明性與可追溯性 。

備註：一、研習紀錄內容請用電腦繕打。
二、研習紀錄請先上傳（校園入口網　其他類 E 話系統　研討會心得上傳），連同補助教師舉辦校內研習申請表及研習相關資料影本，並經單位主管簽章後，送人事室核銷。

記錄者簽章	單位主管簽章	人事室主任簽章
年　月　日	年　月　日	年　月　日