基於 **機器學習** 的 **人工智慧 供應鏈 資安** 新議題

隨著機器學習和人工智慧在供應鏈管理中的應用越來越廣泛，已經成為一個重要的趨勢，卻也同時引發一些日益重要的資安議題，包含以下：

* 數據隱私保護：供應鏈中涉及的數據通常包含敏感的商業和個人信息，範圍擴及供應商和客戶。機器學習和人工智慧的應用中，這些數據需要被收集、儲存和處理，因此如何保護這些數據的隱私和安全性變得至關重要，包含數據加密、身份驗證、存取控制等資安措施，應用於供應鏈中的數據交換過程。
* 對抗性機器學習：人工智慧技術的應用也帶來了新的風險，例如adversarial attacks對抗性機器學習，這是對機器學習演算法的攻擊。  
  供應鏈是一個複雜的系統，涉及多個參與者和環節，攻擊者可能試圖利用機器學習和人工智慧的漏洞或弱點進行對手攻擊，包括數據偽造、模型竄改、釣魚攻擊等，故意修改或干擾機器學習模型的輸入數據，導致機器誤判或誤操作，使得訂單或交付過程中發生錯誤或中斷。因此，供應鏈中的各方需要研究對此類攻擊的防禦，開發更強大的機器學習模型和檢測方法，以識別和防止異常操作。

機器學習和人工智慧的應用在供應鏈管理中也帶來了一些資安風險。企業若未採取適當的風險評估、監測和防禦措施，將會對運營造成損害，在財務及信任層面付出高昂代價，因此，保護供應鏈中的數據和機器學習模型的安全性變得至關重要。