

【出差結案報告】2023 全國大專院校資訊行政主管研討會

蒲正寧

日期：9月21、22日

地點：東海大學

主辦單位：教育部

主題：未來大學、數位科技

前言：本次分享圍繞在兩大主題：資訊安全 (約 1/3)、AI 人工智慧(約 2/3)。我將針對這兩大主題，按照我的筆記整理出相關重點。本文會省略一些技術議題的討論以及廠商針對自身產品的介紹。

主題 1- 資訊安全

本次與會的資訊安全專家，深刻意識到網路世界快速變化所帶來的挑戰。這種變化不僅影響了各行各業，也使得資安工作變得越來越複雜。應用程式已經不再僅限於本機端或校內伺服器，更多的資源已移至外部的網路雲端，並且數量呈爆炸式增長。這些網路工具、平臺和服務帶來了便利性，同時也增加了資訊安全的風險。

使用者如今可以在任何地方工作，需要隨時存取資訊並與其他員工進行即時的交流。然而，由於資訊安全的相對脆弱性，企業界最容易受到攻擊的行業仍然是金融產業，因為他們掌控的資金量最多，同時也需要投入更多資源進行資安工作。

對於大專院校而言，資訊安全攸關學術研究及學生個人資訊的保護。過去的統計數據顯示，學術產業受到的資安攻擊相對較少，而更多的是資料外洩問題。然而，大專院校需要投入多少資金和人力在治安工作上？資安工作所需的成本非常高昂，這對於一般中小型大學來說可能是一個考驗。

資訊安全的工作並不會立即見效，這使得資訊安全投入的回報常常被忽視。然

而，缺乏顯著的安全事件並不意味著沒有成果。相反，這可能意味著資訊安全團隊在防止問題發生時起到了關鍵作用。因此，對於大專院校而言，重視資訊安全是至關重要的。

根據統計，過去兩年最常見的資安問題是跨網站指令碼攻擊(Cross-Site Scripting)和資料庫木馬。此外，個人電腦的病毒感染和勒索軟體的問題也一直存在。勒索軟體對學校和企業造成了巨大的損失。另一個資安隱憂是電子郵件與附件的問題，包括釣魚攻擊。這些攻擊威脅大專院校內部的資安。有約一半的勒索軟體攻擊源自軟體漏洞，其次才是暴力破解和釣魚攻擊。

大專院校在資安工作中應注意以下幾點：多重身分認證、更新管理、安全警報、注重密碼安全。此外，人為教育的重要性不可忽視。

針對教育環境，在保護資訊安全方面，教育部提出以下建議：

全面了解校內的資訊環境：學校應詳細瞭解其資源、系統和網路結構，以便更好地設計和執行資訊安全策略。

設定標準化的軟硬體更新流程：確保所有系統和應用程式都按時進行更新，修補軟體漏洞並提升安全性。

固定檢測包含網域和 SSL 憑證：定期進行網域安全檢測，以確保網站和憑證的安全性。

採用零信任思維：對所有使用者和設備採取嚴格的身分驗證和授權措施，不輕易信任內部或外部來源。

提供完整的教育訓練：所有員工應接受關於資訊安全和相關風險的教育訓練，以提高他們的安全意識。

透過以上的建議和措施，大專院校可以更好地保護資訊安全，確保學術研究和學生資訊的安全性，並減少資安事件對學校造成的損失。資訊安全需要持續的關注和投入，只有這樣才能保護教育機構不受未來的資安威脅影響。

主題 2- AI 人工智慧在教育界的應用與挑戰

近年來，人工智慧 (AI) 的發展席捲各行各業，對大專院校而言，AI 的蓬勃發

展既帶來了機會，也帶來了挑戰。本次研討會對此議題有很深入的探討。

過去一年，ChatGPT 的問世為教育界帶來了不小的震撼。無論是教師還是學生，都對如何使用 ChatGPT 這樣的生成式 AI 產生了熱烈討論。ChatGPT 在推出僅僅兩個月後就突破了一億使用人數，但同時其使用也引發了一些疑慮。因此，針對 AI 技術在教育上的運用，學者一般認為需要制定明確的使用指引，以平衡其應用的利與弊。

AI 將成為未來職場的主要驅動力之一，預計在 2030 年，有 85% 的職場工作將屬於新興工作 (現在還沒有的)。對企業而言，提升員工的技能和 AI 應用能力至關重要，否則就可能迎來被市場淘汰的命運。根據 AI 趨勢預測，在 2026 年，將有超過六成以上的企業主動運用內建 AI 的資訊系統，在不需要技術人員的情況下，從而獲得更好的績效。此外，預計明年將有三成以上的企業採用無需寫程式的 AI 開發工具，以加速數位轉型，實現全民化 AI。這些趨勢表明，AI 的應用範圍將不斷擴大，且 AI 將在企業決策過程中扮演重要的角色。

在教育領域，人工智慧必將與教育共存。生成式 AI 的產出雖然令人興奮，但也常常產生錯誤。未來，AI 將不知不覺地決定教育中的許多事情。那些掌握 AI 技能的人必將勝過那些不了解 AI 的人。然而，教育界使用 AI 也面臨著兩大問題，即學術誠信和版權問題。學術誠信包含內容產生的來源是否為 AI 生成，或是由教師或學生自行撰寫。版權問題涉及到 AI 所生成的內容是否具有著作權，以及用於訓練 AI 模型的資料是否經過授權，是否存在侵權的疑慮。同時，在使用 AI 時，也需要關注個人資料的保護，以避免敏感資料的外洩。

此外，AI 的偏見問題也不容忽視。當訓練資料本身具有偏見時，AI 很容易產生偏見。例如，在美國使用 AI 來預測犯罪時，很多被 AI 預測為嫌疑犯的人都是有種人。這引發了業界對於 AI 是否會失控的擔憂。因此，為了避免 AI 失控，歐美政府開始加緊立法，對 AI 的發展進行管控。

判定一個 AI 系統的優劣涉及多個面向，包括準確性、可靠性、客觀性、安全性、可解釋性和隱私性等。AI 系統的發展週期涉及資料蒐集處理、AI 模型的建立、應用環境的部署以及操作與監管，任何一個時期的錯誤都可能導致不良後果。因此，對於 AI 系統的評估標準和規範至關重要。

在全球教育產業中，有超過九成的教育工作者認為他們正在經歷新興科技帶來的轉變有點疲憊不堪，超過一半的高等教育員工考慮在未來 12 個月內尋找其他工作或退休。而疫情過後，有八成以上的學生更偏好混合式教學，這表明了人們對於 AI 在教育中的需求和改變。全球高等教育年度調查還提到了教育界面臨的主要任務，包括對新一代網路基礎架構的提升與變革、教務相關應用的開發與控制，以及 IT 和教學基礎設施以及資訊安全教育的提升。

對於大學而言，AI 的應用將包含多個方面。首先，AI 可以提供差異化教學，提供精準的教學、輔助、學習指導和學習診斷。其次，AI 亦能改進溝通模式，實現有效且長期持續的評估和改進，建立自動化評估和評分機制。此外，AI 也能提供個性化的教學輔助工具，根據學生特質提供教育研究和教學改進。除此之外，AI 還能推動更多的實驗與探索，提供實驗室模擬工具，並建立對照模型。AI 能像一位虛擬導師一樣工作，提供多語言和跨文化學習。最後，AI 能改進教學模式的效率，通過數位互動體驗，讓學生更容易吸收和理解所學。

總結來說，AI 時代為大專院校帶來了無限的機遇與挑戰。針對 AI 的使用，需要制定明確的使用指引，以平衡其應用的利與弊。以下是一些建議供參考：

1. **就 AI 的使用制定規範：**制定明確的政策和指引，確定 AI 在教育中的使用範圍和目的。這些指引應包括對學術誠信、版權和個人隱私的保護等方面的注意事項。
2. **謹慎選擇 AI 工具和平台：**在選擇 AI 工具和平台時，要仔細考慮其準確性、可靠性、安全性和隱私性等方面的要求。同時，要確保所選工具和平台具有良好的技術支持和持續的更新。
3. **加強師生 AI 素養培訓：**教職員需要通過培訓了解 AI 的基礎知識和應用技能，以更好地運用 AI 技術進行教學、研究和管理。學生也應該接受相應的培訓，以提高其 AI 的應用能力和理解。
4. **強調倫理和責任：**教育工作者應該強調 AI 的倫理使用和責任意識。他們應該教導學生嚴守學術誠信，避免抄襲和盜用 AI 生成的內容。同時，教育機

構應該處理個人隱私和版權問題，確保合法合規的使用 AI。

5. **監測和評估：**教育機構應該建立監測和評估機制，以確保 AI 在教學中的有效性和安全性。這可以通過定期的教師和學生評估、技術支持和使用反饋來實現。
6. **提倡跨學科合作：**AI 的應用涉及多個學科領域，包括資訊科學、教育學、心理學等。教育機構應該鼓勵跨學科合作，促進教師、研究人員和技術人員之間的交流和合作，以推動 AI 在教育中的最佳應用。
7. **實施持續改進：**AI 技術不斷發展，教育機構應該與時俱進，持續改進 AI 應用的方法和策略。這需要與業界和學術界的合作，參與 AI 相關的研究和項目，以保持教育機構在 AI 領域的領先地位。