PECC

4 2024 月號

2024年4月出刊

亞太區域情勢月刊

Asia Pacific Situation Monthly

CTPECC亞太區域論壇「國際地緣政經趨勢與科技政策競合發展」

本期重要內容

本刊物採用環保紙

發行所 / 太平洋經濟合作理事會中華民國委員會
地址 / 台北市德惠街16-8號7樓
電話 / (02)2586-5000
創刊日期 / 1996年1月

訂閱電子報

CTPECC

會議紀實

CTPECC 亞太區域論壇—「國際地緣政經趨勢與科技政策競合發展」（上）

■ CTPECC 秘書處

太平洋經濟合作理事會中華民國委員會（CTPECC）於本（113）年 3 月 19 日假東海大學舉辦 113 年度第 1 場亞太區域論壇。論壇主題為「國際地緣政經趨勢與科技政策競合發展」。本次活動邀請東海大學政治系系主任兼所長王啟明教授、國際貿易學系高惠娟教授、電機工程學系蔣惟丞副教授、國際貿易學系唐運佳副教授、力行國際物流股份有限公司楊力行董事長及本會許峻賓秘書長、張鴻副研究員、李麒緯助理研究員與陳彥如助理研究員就近期國際政治經濟及亞太區域經貿合作等相關議題共同分享與討論。本活動相關紀實茲分述如下：

開幕致詞：東海大學政治學系系主任兼所長 王啟明教授

東海大學政治系系主任兼所長王啟明教授感謝太平洋經濟合作理事會中華民國委員會（CTPECC）辦理亞太區域論壇，本次論壇主題國際地緣政經及科技政策皆為當前國際重要趨勢，而東海大學政治學系及國際貿易學系亦關切亞太區域研究領域進展，期待與會產、官、學各界能藉由本次論壇認識及交流相關議題。

東海大學政治系系主任兼所長王啟明教授發表開幕致詞。（圖 /CTPECC 秘書處）

第一場次：國際地緣政治與經濟發展
從國際局勢看地緣政治 CTPECC 李麒緯助理研究員

本場次由 CTPECC 李麒緯助理研究員擔任講者，說明當前全球面臨的區域與非區域危機類型，接著以「國際秩序的挑戰」及「國家安全延伸」的國際局勢切入東亞地區地緣政治。

在區域危機類型部分，除了肇因於領土、資源、內政等原因的軍事衝突外，許多地區也遭遇來自氣候變遷帶來的威脅；在非區域危機類型部分，主要有能源、氣候變遷、糧食、貧富不平等、國際秩序、民主、全球化、經濟與安全等類型。

李助理研究員建議在分析國際事件時，可從三個層次來思考:國際社會、國家間以及國內。在國際社會層次，強權國家扮演著主要角色；在國家間的層次，可觀察北約東擴及烏克蘭可能加入北約對歐洲整體安全所帶來之影響；而國內層次則以政治菁英為主要行為者，影響著政治、經濟及國防等領域，進而影響國家整體安全。

論及東亞地緣政治局勢，李助理研究員以國際秩序及國家安全角度進行分析，說明美中競爭在這兩面向的體現，如中國、俄羅斯、伊朗等國家對西方秩序帶來挑戰，以及中國提出的三大全球倡議。美中之間的地緣角力，例如印太戰略與一帶一路、IPEF 與 RCEP 等，皆對區域產生影響。整體而言，政治及安全因素才是經濟合作背後之驅動力。最後，李助理研究員表示，儘管美中之間存在競爭，但在雙方於特定領域仍然保有合作關係，像是共同應對氣候變遷。

CTPECC 李麒緯助理研究員進行國際危機說明。
（圖 /CTPECC 秘書處）

強化學習於機器人系統之應用
東海大學電機工程學系 蔣惟丞副教授

蔣惟丞副教授闡述智慧機器人的操作模式，特別著墨於其透過感測器感知環境並與之互動，以實現自主學習的能力。智慧機器人的學習過程主要涉及到深度學習與強化學習兩個主要領域。前者在面對環境資訊不足時，透過錯誤嘗試來建立控制策略；後者則依賴大數據資料庫的學習過程。

蔣教授進一步指出，在機器人群體合作的情況下，溝通成本相對較高。因此，時常會讓機器人在缺乏溝通的環境下自行嘗試並找到最佳解決方案。在實際應用中，深度學習與強化學習常常相互結合，互相彌補不足，形成深度強化學習的模式。例如，Alpha GO 即是深度強化學習的一個代表性案例。

儘管 AI 技術目前仍處於起步階段，應用領域相對有限，主要體現在翻譯與文書處理等方面，而在自動駕駛、醫療等更為先進的領域仍需時日。雖然現階段臺灣的 AI 品牌發展面臨著諸多挑戰，但臺灣學術界不斷致力於研究本土 AI 模型及方法，持續為 AI 技術發展貢獻。

圖為東海大學蔣惟丞教授進行簡報。
（圖 /CTPECC 秘書處）

當全球化遇上地緣政治貿易碎片化崛起 東海大學國際貿易學系高惠娟教授

高惠娟教授以經濟與貿易角度切入探討地緣政治現況，從回顧全球化歷史著手，解析現今貿易型態的新轉變，進而推估未來的經濟與展望。全球貿易集團可大致區分為美國為首的西方集團（Western Bloc）、中國或俄羅斯為首的東方集團（Eastern Bloc）以及不結盟國家。1980 年代後期冷戰結束，全球普遍崇尚自由貿易，使得全球貿易量持續增加，1990 年代至 2000 年更達到全球貿易最頂峰。

自 2001 年中國加入 WTO 後，其貿易快速成長。中國的快速發展對美國製造業造成明顯衝擊，導致美國製造業就業人數大幅下降。2016 年，美國總統川普（Donald Trump）提出一系列針對中國的貿易政策方案，後續便開啟美中貿易戰。近年來，新冠疫情及地緣政治等因素下，全球化貿易模式逐漸式微，轉變為「在不傷害國家安全、不傷害現在或未來的科技領先條件下進行」的新模式。

隨著新貿易模式興起，地緣經濟的碎片化現象顯著。美中貿易戰後，雙方對彼此實施高額關稅，中國不再是美國最大的貿易夥伴。全球供應鏈轉為近岸（friend-shoring）及友岸外包（near-shoring），盛行「中國 +1」策略，移轉至印度、東協、墨西哥及中東歐等四大區域，反而促進不結盟新興國家的貿易與投資。但卻導致全球供應鏈不斷延長，使得經濟成本上升，並削弱專業化分工效率，進一步縮小規模經濟效應。不過，不結盟國家透過第三地運輸發揮其緩和對立之角色，並帶動自身經濟增長。

圖為東海大學高惠娟教授解析現今的新貿易型態。
（圖 /CTPECC 秘書處）

最後，有關 2024 年經濟展望，高教授指出將持續地緣經濟碎片化的新趨勢，可能導致全球貿易陷入「新冷戰」的狀態。保護主義仍是主導全球貿易與經濟發展的主要力量。因此，企業必須具備韌性及靈活性以因應不確定性。在總體經濟方面，通膨逐漸降溫趨勢，並預計美國聯準會將於 2024 年中後期降息。而政策方面，值得關注 2024 年美國大選，其結果將左右未來經濟及貿易政策走向。除此之外，亦值得關注全球 AI 與科技產業之投資，以及氣候變遷下能源轉型與綠色產業鏈。

地緣政治對國際物流業之影響 力行國際物流股份有限公司 楊力行董事長

楊力行董事長以其在物流產業的豐富經驗，深入探討國際政治知識於該產業中的實際應用及案例。物流產業與國際貿易緊密相關，受到地緣政治因素的密切影響。近年來中美貿易戰之下，關稅政策變化對臺灣的物流業者產生顯著影響，使得企業必須提高韌性，以應對不確定性並評估風險。當時部分企業紛紛採取應急措施，例如短期的繞道策略。即透過印尼、馬來西亞等東南亞地區進行轉運，以減少貿易戰風險對供應鏈的衝擊。然而，此種策略的實施有其限制，並非長久之計。

由於地緣政治緊張引發紅海危機，許多商用貨船遭受攻擊，航運業者則面臨更高的安全風險。因此，重新評估其航線安全，並暫時停止在紅海地區的航運活動，甚至繞道好望角，被迫增加其航程及運輸成本。除此之外，亦面臨氣候變遷挑戰。極端氣候造成巴拿馬運河水位降低，使得大型船隻通行受到限制，導致許多貨物延誤。然而，這也為部分企業提供新型服務的機遇，祭出多種運輸方式及事前風險管理，努力減少供應鏈干擾之影響。

在科技進步的影響下，航運及物流業也正在經歷巨大的變革。楊董事長自 2008 年開始將部分業務進行線上化，未來應用 AI 技術導入物流運輸成為趨勢，企業也積極朝向數位轉型邁進。■

圖為楊力行董事長分享企業實際經驗。（圖 /CTPECC 秘書處）

金融資安

金融科技應用中的資訊安全與隱私保護議題

■ 左瑞麟
國立政治大學資訊科學系 特聘教授

金融科技的發展與資安威脅

金融科技（FinTech）是近年來非常熱門的議題。透過科技創新並應用於金融服務中，可達到降低成本、提高效率，或優化金融服務的效果。隨著金融科技創新應用的快速發展，相關應用漸漸成熟，除了帶來前所未有的便利性和效率，也正顛覆著傳統金融服務業。相信未來金融科技將成為未來數位化社會不可或缺的一部份。然而，在另一方面，這種發展同時也引發了一系列資訊安全與隱私保護相關的議題與挑戰。

首先，資安議題在金融科技領域格外重要。隨著越來越多的金融交易和服務移轉至線上，資訊或資料（Data）的保護成為關鍵議題之一。駭客攻擊、資料外洩、社交工程、網路詐騙和勒索病毒等網路犯罪日益增加，對用戶的財產安全和金融機構的業務運營造成直接威脅。金融科技應用可能成為攻擊者針對的對象，攻擊者通過植入惡意程式或進行釣魚攻擊來獲取利益，例如著名駭客犯罪團體LockBit於今（2024）年 1 月針對金融科技公司 EquiLend 發動勒索軟體攻擊，導致該公司每月處理數萬億美元證券借貸交易之公司的部分業務關閉。根據美國網路安全和基礎設施安全局（America's Cyber Defense Agency）的資料顯示，LockBit 自 2020 年以來已實施了 1,700 多次駭客攻擊，並向受害者勒索了至少 9,100 萬美元。

其次，隱私保護在金融科技領域同樣面臨重大挑戰。金融科技應用（如行動支付、個人理財應用等）經常需要蒐集大量個人資料，包括交易歷史、位置資訊、個資，甚至是人臉特徵等生物識別資訊。這些資訊的收集和處理可能對用戶隱私構成威脅。若未經妥善管理，這些機敏資訊可能被不當使用或洩漏給第三方，導致重大的隱私侵犯事件，例如美國最大的非銀行抵押貸款服務商 Mr. Cooper 在 2023 年遭受駭客攻擊，導致近 1500 萬人的個資外洩，包括姓名、地址、電話號碼、社會安全號碼（Social Security number，SSN）、出生日期和銀行帳戶號碼等。此外，康

卡斯特有線通信公司（Xfinity）也在一次 Citrix 服務器漏洞中發生資料外洩事件，包含了用戶名和經過雜湊[1]（Hash）處理過的密碼等。

除此之外，新興的技術的應用，如區塊鏈（Blockchain）、智慧合約（Smart Contract）和人工智慧（AI）等，在提高金融服務品質與效率的同時，確實可能帶來新的安全與隱私問題，例如區塊鏈的去中心化技術雖然在某些方面提供了更強的安全性與可信賴性，但也存有潛在的資安風險，像是所有交易記錄都公開的儲存在鏈上，所以如未經加密保護或處理，有可能造成資料外洩。此外，比特幣或以太幣等區塊鏈貨幣強調的匿名性也可能成為詐騙或洗錢的管道，造成監管的困難。智慧合約的執行雖然自動化，但其條件判斷和結果可能因此暴露用戶的敏感訊息，如年齡、職業或薪資所得等等。而人工智慧和大數據技術在分析企業或用戶行為和偏好時，則可能在無意中洩漏其他企業或用戶的機敏資訊。因此，儘管生成式 AI 如 ChatGPT 對企業創新與提高效率上有正面的作用，但為了避免企業內部機敏資料外洩，還是有許多企業開始禁止使用 ChatGPT 等生成式 AI 的工具。

針對前述威脅與挑戰，金融科技公司必須積極應對，通過強化技術安全措施、嚴格遵守隱私保護規定，以及與監管機構合作來提高行業標準。同時，消費者教育也至關重要，幫助用戶了解如何安全地使用金融科技服務，以及如何保護自己的個人訊息和資產。只有這樣，金融科技才能在保障安全和隱私的基礎上，實現其全面的潛力。

金融資安與隱私保護的國際發展趨勢

在當今全球數位化的時代，金融資安與隱私保護是全球各國高度重視的議題，也是國際社會需共同面對的挑戰。面對這些挑戰，國際間在金融資安與隱私保護的發展趨勢上展現了幾個明顯的方向，包括法規強化、技術創新、國際合作以及公私部門間的共同合作。

- 法規強化：首先，在法規強化方面，全球多個國家和地區正致力於更新或制定更加嚴格的資料保護相關法律。例如，歐盟的通用資料保護規則（GDPR）設立了高標準的隱私和資料的保護規則，對企業如何處理個人資料提出了嚴格要求。此外，加州消費者隱私法（CCPA）也提供了類似的保護，強調消費者對於個人資料的控制權。這些法規的實施，促使全球企業必須重新評估其資料保護措施，以符合國際標準。
- 技術創新：在技術創新方面，金融機構和科技公司皆積極探索利用先進技術來提升資安防護和隱私保護的能力。首先，區塊鏈技術以其透明性、不可篡改性和分散性的特點，被視為一種潛在的解決方案，能夠在不同的金融應用中提供安全的資料儲存與交易機制。但如前所述，區塊鏈的隱私保護能力相對較弱，因此各國皆開始發展相關的密碼學技術以強化資安與隱私保護的能力。例如，同態加密（Homomorphic Encryption）、安全多方計算

1 雜湊函數（Hash function）是一種從任意大小的檔案或數據計算出一個固定大小數據的函數。這個函數所產出的固定大小的數據稱為雜湊值 (Hash value)。安全的雜湊函數具有抗碰撞性，也就是不同的輸入，會對應到不同的雜湊值。因此雜湊值可以說是訊息或檔案在數位世界中的指紋，具有唯一性。目前廣泛使用的雜湊函數標準為 SHA-256 或 SHA-3 等。雜湊函數廣泛應用於許多領域，例如用於計算訊息指紋，對檔案或數據進行完整性驗證以及用於數位簽章等。

（Secure Multi-Party Computation）以及 FIDO 無密碼身分驗證技術等。同態加密是一種允許在加密數據上以密文方式直接進行計算的加密方法。因此金融機構可以在不解密資料的情況下直接對資料進行分析和處理，為資料隱私和安全性提供了一層額外的保護。另外，安全多方計算允許多個參與方能夠共同進行數據分析和決策制定，而無需共享他們的敏感數據。金融機構可以利用安全多方計算來合作解決如反洗錢（AML）、信用評估和風險管理等問題。最後，金融 FIDO（Fast Identity Online）是一種用於身份認證的技術標準，旨在提供更安全、更便捷的用戶認證方式，以取代傳統利用密碼（Password）進行身分驗證的方式。FIDO 支持多因素認證，包括生物識別和基於硬體的安全金鑰，這有助於減少對傳統密碼的依賴。由於傳統密碼可能有被盜或是弱密碼被猜測導致破解的風險，因此利用 FIDO 以替代密碼可以增強安全性。國際合作：國際合作也是金融資安與隱私保護的一個重要發展趨勢。面對跨國網路犯罪和資料外洩事件的日益增多，各國政府和國際組織意識到單獨行動的局限性，開始通過多邊平台和協議加強合作。例如，全球反洗錢監管機構金融行動特別工作組（FATF）和國際刑警組織等，都在加強跨境合作，共同打擊金融犯罪

- 公私部門間的共同合作：最後，公私部門間的共同合作對於提升整體金融資安亦至關重要。這種合作模式通常涉及政府、金融機構、科技企業及其他利益相關者之間的協調與合作，旨在共同應對日益複雜的網路安全威脅和隱私保護挑戰。這種跨界合作不僅有助於快速響應安全事件，也促進了創新解決方案的開發，進一步加強了金融系統的整體韌性。例如，歐洲警察局（Europol）的網絡犯罪中心（EC3）就與私營部門合作，共同打擊跨國網路犯罪。這包括與銀行、金融技術公司和科技巨頭合作，交換情報、進行聯合調查等。亞太經濟合作會（APEC）跨境隱私規則系統（CBPR）則是一個跨國的框架，旨在促進亞太地區內個人資料的跨境流動，同時保護這些資料的隱私。該系統即通過公私部門的共同合作，建立了一套隱私標準，確保個人資料在跨境傳輸過程中受到保護，並按照一致的隱私標準處理。

金融科技安全的未來與挑戰

隨著科技的進步，金融科技安全在未來的威脅與挑戰，主要會在量子計算與人工智慧兩個方面。

首先，量子計算機的發展預示著對現有加密技術的重大威脅。量子計算機利用量子力學的

金融科技概念圖（由 ChatGPT 生成）

原理，能夠在極短的時間內處理複雜計算，這使得量子電腦在理論上被證明能夠破解當前的許多密碼演算法，包括前面所提到的隱私保護相關密碼技術以及數位簽章等。這樣的能力說明未來量子電腦成熟的時代，金融科技應用服務中用於保障資訊機密性，完整性，不可否認性，以及勇於保護隱私的各項密碼技術都將變得脆弱，從而威脅到金融體系的安全和客戶的隱私。

另外，在 AI 方面，雖然 AI 技術能夠提高金融服務的效率和準確性，但同時也帶來了新的安全議題與風險。Deepfake 深偽技術可以用來創造高度逼真的偽造影像，聲音或圖片。駭客可以利用深偽技術假冒公司高層，進行金融詐騙，或利用假訊息配合深偽影像或圖片等，進行社交工程攻擊，以獲取企業機密，用戶個資或者金錢等不法利益。而面對這些威脅，目前我們除了教育用戶提高資安意識與警覺心之外，幾乎沒有其他預防的方法。面對未來 AI 的發展，這樣的威脅將越來越嚴重，也越來越難以預防。

總結

隨著科技的快速發展，金融科技已成為現代社會不可或缺的一部分。然而，這種發展同時，也帶來了對個人隱私與資訊安全的挑戰。面對這些資安威脅，密碼以及隱私保護的創新技術，在提供安全、透明和高效金融服務方面發揮著關鍵作用。這些技術不僅保護了用戶的財務資訊和隱私，也因此促進了金融服務的創新和發展。除了技術創新外，在國際趨勢上，全球範圍內正逐漸形成更加嚴格的資安和隱私保護標準，如歐盟的

量子電腦與資訊安全示意圖（由 ChatGPT 生成）

通用數據保護條例（GDPR）已成為全球許多地區效仿的標準。此外，國際間在資安威脅資訊共享、技術合作等方面的合作也在加強。亞太地區在這些方面也在積極跟進，以提升整體的資安和隱私保護能力。

未來，隨者量子計算機以及 AI 技術的發展，金融科技所面對的資安威脅將越來越嚴重。面對這些未來的威脅與挑戰，我們需要提前規劃與採取積極措施，包括開發抗量子電腦攻擊的密碼學技術，以抵抗未來量子電腦的威脅。另外，針對利用 AI 進行攻擊的威脅，除了需加強 AI 系統的安全性和透明度，還需要學界或業界共同合作，研發能偵測或抵抗深偽技術進行攻擊技術。此外，由於資安最大的威脅通常都在於使用者的資安意識不足，因此藉由資安相關的教育訓練，增進全民的資安意識與素養，以提高對這些新興技術威脅的認識和應對能力，也是不可或缺的。唯有如此，我們才可以期待並確保未來金融科技創新應用的永續發展。■

政策趨勢

新加坡 AI 政策及人才發展趨勢

■ 陳彥如
CTPECC 秘書處助理研究員

2023 年 8 月全球求職社群平臺領英（LinkedIn）發布「未來工作報告」（Future of Work Report）提出 AI 於不同國家上班族與各職業擴散率，隨著 AI 在許多工作領域自動化，強調軟技能將日益關鍵。自 2016 年以來，新加坡領英會員個人資料新增 AI 技能的比例成長 20 倍，全球平均成長率 8 倍多，可見新加坡為全球 AI 擴散率最高的國家。而領英認為新加坡 AI 技術發展迅速的原因，主要為健全的數位基礎設施、強大的智慧財產權保護框架，以及對 AI 技術發展投入大量資金的蓬勃投資生態[1]。

根據新加坡總統尚達曼（Tharman Shanmugaratnam）表示，AI 將比過去科技更快速地取代人類工作，同時也為人類提供工作協助。隨著大型語言模型（large language model, LLM）驅動的聊天機器人不斷發展，未來機器將具有更多人類特徵，並與過去的科技發展相比，將造成不同之結果。

尚達曼特別指出，早期的科技浪潮，包括自動化等技術，主要取代例行且重複性高的工作，而 AI 的不同之處在於，其將接管認知工作，即需要更高教育水準或更高收入的工作。因此，AI 可能將顛覆傳統之職業階層。現今普遍對智商（intelligence quotient, IQ）優於情商（emotional quotient EQ）的價值觀也可能會改變，未來可能將更重視需要情商、團隊合作與想像力的工作技能或特質[2]。雖然 3 至 4 年內不會發生巨大變化，但在 10 至 15 年內，這場科技革命將對勞工產生深遠影響。

新加坡 AI 發展政策

新加坡於 2019 年發布第一個「國家人工智慧戰略」（National AI Strategy），提出未來 AI 發展的願景及重點戰略，且為最早推出國家人工智慧戰略的國家之一。此戰略引領對 AI 研究的投資需求，鞏固新加坡的人才，建立數位基礎設

1 Linkedin. (2023, August). “Future of Work Report: AI at Work.” https://economicgraph.linkedin.com/research/future-of-work-report-ai

2 Timothy Kang. (2023). AI will replace human tasks faster than previous technologies: Singapore's president Tharman Shanmugaratnam, yahoo, https://finance.yahoo.com/news/ai-will-replace-human-tasks-faster-than-previous-technologies-singapore-president-tharman-shanmugaratnam-022155630.html

施，以打造 AI 生態系，並強調研究界、產業界及政府間三螺旋式的夥伴關係，增進國際合作[3]。

在 AI 研究開發（R&D）的投資方面，根據新加坡研究機構 AI Singapore（AISG）下的 2020 年與 2025 年「研究、創新及企業」（Research, Innovation and Enterprise, RIE）計畫，新加坡政府已承諾投入超過 5 億新元。在 AI 治理方面，2019 年推出全球首個人工智慧治理模型框架（Model AI Governance Framework）。2022 年則推出全球第一個人工智慧治理測試框架和工具包（AI Governance Testing Framework and Toolkit）—AI Verify，並於 2023 年 6 月開源供開發人員使用。

在上述 AI 政策及基礎之下，新加坡副總理黃循財（Lawrence Wong）表示，政府必須以更有系統的方法運用 AI 來促進公共利益，同時降低其對民眾就業與生計的負面影響，例如深度偽造（Deepfake）、詐騙、網路詐騙與錯誤訊息等風險。因此，2023 年更新既有戰略，推出「國家人工智慧戰略 2.0」（Singapore National AI Strategy 2.0, NAIS 2.0），顯示新加坡全力推動 AI 發展的決心[4]。

NAIS 2.0 更進一步強化 AI 人才的培育，重新設計 AI 學徒計畫（AI Apprenticeship Program, AIAP），加速推廣在地企業的 AI 應用，以及透過在職培訓提升勞工的 AI 技能。繼而，積極吸引全球頂尖的 AI 專業人才，亦加強在資料科學、機器學習及工程領域等領域之本土人才培育，並進一步建立 AI 基地，培育本土的 AI 專業知識社群。預計透過此戰略新加坡 AI 相關從業人員的數量將提升至 1 萬 5,000 人。

新加坡 AI 人才培育計畫

在國家人工智慧戰略下，AI 人才培育計畫針對不同對象背景或年齡層，設計不同形式及難易度的培訓課程，幫助一般民眾與 AI 相關工作的專業人士開啟 AI 學習。針對所有人的 AI for Everyone（AI4E），作為國家通用的 AI 知識基礎教育；針對職業訓練的 AI 學徒計畫（AI Apprenticeship Program, AIAP）為全職培訓計畫，旨在增加 AI 相關的就業機會，學員必須具備基礎程式設計能力，例如 AI 及 Python 或機器學習。該課程包含 2 個月的深度技能學習，以及 7 個月的專案執行與企業實習，期間每月提供 3,500 至 5,500 新元的培訓津貼；針對產業應用的 AI 中小企業計畫（AI for SME, AI4SME），此計畫連結中小企業與 AI 解決方案的供應商，中小企業可以透過 AI 就緒指數（AI Readiness Index, AIRI）評估組織的 AI 成熟度，對此協助中小企業找尋相關業務應用的案例。最終，媒合解決方案的供應商提供中小企業導入 AI 應用其業務，幫助中小企業提升銷售業績及曝光度，並且增加可信度[5]。

3 Smart Nation Singapore. (2019). National Artificial Intelligence Strategy, https://www.smartnation.gov.sg/files/publications/national-ai-strategy.pdf.

4 Singapore Economic Development Board. (2023, December). Singapore updates AI strategy with aim to contribute globally valuable breakthroughs, https://www.edb.gov.sg/en/business-insights/insights/singapore-updates-ai-strategy-with-aim-to-contribute-globally-valuable-breakthroughs.html

5 AI Singapore. (2023, August 16). Accelerating AI in Singapore, https://learn.aisingapore.org/.

此外，新加坡協助企業 AI 人才轉型不遺餘力。2020 年推出「人工智慧時代的工作重新設計指南」（A Guide to Job Redesign in the Age of AI），提供運用於各產業的方法，幫助企業管理 AI 對員工的影響，並協助企業導入與應用 AI，以為未來數位轉型做好準備。例如重新設計現有工作角色，以利用 AI 的潛力，從而提高工作價值。該指南建立標準化的工作任務定義，辨別不同工作之間的路徑圖，並將工作任務重新組合成未來可能的崗位。同時，考慮工作中的數位轉型障礙，還提供雇主與員工之間潛在的有效溝通解決方案。透過上述政策措施與實例，新加坡成功塑造 AI 職業訓練及孕育人才的環境，有助於其勞動力在科技變化下仍可保持競爭力。■

2023 年 11 月全球首屆人工智慧安全峰會，含美歐中等 28 國宣布加強全球合作，反映 AI 發展趨勢。（Pic: Marcel Grabowski / UK Government）

資訊欄

「亞太區域情勢月刊」係由太平洋經濟合作理事會中華民國委員會(CTPECC)出版，CTPECC為國內產官學所組成的非營利性區域經濟合作組織。

本月刊長期徵文，詳細說明請參考右方QR Code。
歡迎投稿，請寄至以下信箱：d35056@tier.org.tw，會再由專人回覆您！歡迎您不吝惠賜稿件。

歡迎加入「太平洋經濟合作理事會中華民國委員會」**Facebook**粉絲頁。

本刊將減少紙本印刷量，敬請訂閱電子報

讀者問卷

徵文資訊

ISSN 1605-240-4