

關鍵基建新規 鞏固 AI 優勢

明年1月1日起，《保護關鍵基礎設施（電腦系統）條例》正式生效，成為本港網絡安全發展的重要里程碑。法例涵蓋金融、公共事業、醫療及交通等範疇，既是防禦框架，也是保障智能系統的策略藍圖。



科網人語

雖然新法例沒明確提及人工智能（AI），但在數碼經濟中，AI已成為基建的「大腦」與「神經系統」，應用於交通管理、能源調度、金融監察及醫療診斷等核心系統。其廣泛採用同時帶來舊式模型、黑箱算法及供應商不透明等風險，影響韌性與問責性。

新法例要求「關鍵基礎設施營運者」（CIOs），保障內部及第三方系統的安全，包括雲端與供應商平台。由於AI深度嵌入複雜資訊科技（IT）架構，界定「關鍵電腦系統」（CCSs）並不容易。此外，AI性能偏移、缺乏可解釋性及新型威脅，均需持續監察。一旦發生事故，必須於12至48小時內通報，對即時監控與應變機制提出高要求。

全球各地均加強法規以應對網絡威脅。相比之下，香港法例在細節上較新加坡完善、在靈活度上勝過歐盟、在促進創新方面優於美國。其引入CCS概念、設定通報時限，並保障營運者身份，避免惡意報復。法例聚焦系統完整性與服務持續性，而非個人資料監管，平衡安全與創新。

條例鼓勵建立安全、可審計及具韌性的AI系統，以提升公眾信任。此務實框架既符合全球最佳做法，又保留本地創新空間，推動企業採取「AI優先」與「韌性優先」策略。AI已深度參與民生決策，如貸款批核及醫療診斷，倫理設計不可或缺。法例強調透明與問責，並應涵蓋防範偏見、公平性及包容性。科技界需推動負責任AI，確保系統公平服務所有市民，避免

無意傷害。

在地緣政治與跨境司法挑戰下，CIOs必須評估供應商是否受外國法規影響，影響數據主權與控制權。這促使業界探索混合架構與亞洲區AI供應商，以提升透明度與合規性，亦可能加速區域AI生態系統發展。

全球對安全、可解釋、可審計AI的需求持續上升，香港的法例讓本地在此領域具有領先優勢。聚焦關鍵系統而非全面監管，使香港既能保持科技樞紐的地位，又能確保基建長遠可持續。

在風險驅動的數碼經濟中，能保障AI系統完整性的城市，將更能吸引資金、人才與信任。要在新法例下蓬勃發展，建議CIOs採取以下策略：

1. 盤點AI系統：識別內外部AI組件並評估漏洞；
2. 建立治理框架：確保透明度、可解釋性、公平性及事故應變能力；
3. 確保供應鏈安全：第三方AI必須符合數據主權、審計與通報要求；
4. 部署監察工具：偵測異常並即時警示；
5. 與監管機構接軌：把AI合規納入企業整體策略。

香港素以靈活及進取著稱，《關鍵基礎設施條例》為發展新篇章。此法例不只是防禦工具，更是推動智能創新的平台，引領香港以誠信設計、以韌性部署、以遠見領導。未來的基建將更智能化、自主化與安全化。憑藉前瞻監管、倫理設計與創新文化，香港有望成為數碼轉型的核心引擎。

陳漢偉博士
香港理工大學
電子計算學系實務教授