



# 進化的起點： 解讀 2025 三大關鍵趨勢

## AI、量子運算與網路安全的未來藍圖

2025 年，人工智慧將徹底改變規則，量子運算邁向實用化，而網路安全的防禦戰線將挑戰極限。這些預測是否將在未來一年逐一實現？

文／編輯部

川普二度入主白宮，無疑是 2025 年最受矚目的事件之一。另一方面，科技的浪潮並未止步，反而以更驚人的速度席捲全球，重塑著我們生活和工作的樣貌。除了政治版圖的變動，還有哪些值得關注的趨勢呢？人工智慧（AI）的應用正以前所未有的速度滲透到各個領域，從自動駕駛汽車、個人化醫療到網路安全防禦，都可見到 AI 的身影。量子運算的商業化進程也正加速推

進，預計將在未來幾年內為金融、物流和研究等產業帶來顛覆性的變革。此外，網路安全威脅也隨著科技的進步而不斷演變，生成式 AI 創造的惡意軟體、量子運算帶來的加密威脅，以及假訊息攻擊等，都將成為企業需要面對的新挑戰。對於如此瞬息萬變的科技浪潮，企業和個人都必須做好準備，才能在 2025 年及未來掌握先機，立於不敗之地。

## IDC 全球 IT 產業十大預測

1. AI 經濟學
2. AI 轉向障礙
3. 網路彈性
4. 雲端現代化
5. 資料即產品
6. 應用程式蛻變
7. 干擾交付
8. AI 基礎設施脫碳
9. 複合式 AI 的統一平台
10. 新的工作角色

為了讓讀者更深入了解 2025 年的科技趨勢，我們彙整了多家權威機構的報告的精華，整理出最重要的趨勢。這些趨勢看法主要來自於全球知名的市場情報和諮詢服務提供商 IDC，其發布的「2025 年未來展望：全球 IT 產業預測」報告，為我們提供了對 AI 經濟、雲端現代化和網路安全等關鍵趨勢的洞察；全球領先的資訊技術研究和顧問公司 Gartner，其發布的「2025 年十大戰略技術趨勢」報告，揭示了代理式 AI、後量子密碼學和空間運算等前沿科技的發展方向；以及全球最大的專業技術組織 IEEE，其發布的「2025 年及以後科技的影響：一項 IEEE 全球研究」報告，深入探討了 AI、量子運算和機器人技術等領域的發展趨勢，並分析了其對不同產業的影響；還有專注於 IT 研究和諮詢的公司 Info-Tech Research Group，其發布的「2025 年科技趨勢」報告，探討了模擬未來和知識保障等主軸，並分析了 AI 化身、量子優勢和深度偽造防禦等趨勢。

在我們整合這些權威機構觀點後，本文聚焦於以下三大重點趨勢，分析其在 2025 年的發展趨勢和對企業的影響：

- 一、人工智慧的應用與監管。
- 二、量子運算的商業化進程。
- 三、網路安全威脅與防禦的新趨勢。

## 一、人工智慧的應用與監管

企業投資 AI 的動機來自於提高效率 and 生產力、創造新的產品和服務、增強客戶體驗、降低成本並獲得競爭優勢等。像是 AI 可以自動化重複性任務、優化流程並提高決策效率，從而提高企業的效率 and 生產力；幫助企業開發新的產品和服務，例如個人化醫療、自動駕駛汽車和智慧家居；提供個人化推薦、自動化客戶服務和預測客戶需求來改善客戶體驗；透過自動化任務、優化資源配置和減少錯誤來降低企業的營運成本；尤其在當今快速變化的商業環境中，AI 正在成為企業保持競爭力的關鍵因素。

IDC 預測，到 2025 年，全球用於支援 AI 技術的支出將達到 3,370 億美元，到 2028 年將超過 7,490 億美元。這顯示出企業對 AI 的濃厚興趣和投資意願。

IDC 也預計 2025 年 AI 支出中的 67%，將來自於將 AI 功能嵌入其核心業務營運的企業。

而企業要在 2025 年加大 AI 投資，以下方向是應該優先考量的：

### Gartner 2025 年 三大主軸十大策略科技

#### 一、AI 驅動與風險：

- 代理型 AI
- AI 治理平台
- 虛假資訊安全

#### 二、運算新領域：

- 後量子密碼學 (PQC)
- 智慧隱形環境感知
- 節能運算

- 混合運算

#### 三、人機協作：

- 空間運算
- 多功能機器人
- 神經功能增強

- **生成式 AI**：生成式 AI 是 2025 年的主要技術趨勢之一，它能夠創造高度複雜且類似人類的內容，從文字和圖像到音訊和複雜的模擬。企業正在將生成式 AI 整合到工作流程中，以加快創新速度並大規模提供個人化服務。預計到 2030 年，生成式 AI 市場規模將達到 6,679 億美元，複合年增長率為 24.4%。
- **代理式 AI**：Agentic AI 是一種更進階的 AI 形式，它可以自主地規劃和執行行動以達成用戶設定的目標。簡單來說，代理式 AI 就是一個虛擬的員工，可以協助、分擔和增強人類或傳統應用程式的任務。代理式 AI 藉由大型語言模型（LLMs）的力量，結合商業數據和 IT 洞察力，引導工作流程、支援團隊和解決問題。它可以管理複雜的任務、發現潛在的問題，甚至自動修復 IT 故障，讓組織能夠順利運作，而無需人工干預。根據 Techopedia 的報導，ScienceLogic 產品與工程副總裁 Priyanka Kharat 指出代理式 AI 將在 2025 年達到投資回報點。
- **AI 治理平台**：隨著 AI 系統越來越融入關鍵決策過程，企業需要確保 AI 的可靠和負責任的使用。AI 治理平台可以幫助企業管理 AI 相關的風險，同時在利益相關者之間建立信任，並遵守法規標準。
- **AI 網路安全**：AI 在增強網路安全方面至關重

要，它可以自動化複雜的流程來檢測和應對威脅。AI 系統可以分析大量數據以找出異常模式、預測潛在威脅並部署即時防禦。

## 二、量子運算的商業化進程

量子運算能夠以比傳統電腦快指數級的速度處理特定任務的資訊。可以加速機器學習演算法的訓練速度，並提高其準確性。企業可以投資開發新的量子機器學習演算法，並將其應用於藥物研發、材料科學、金融建模等領域。另外，AI 可以用於設計和優化量子演算法，使其更有效率地運行於量子電腦上。

未來可能會出現結合傳統電腦和量子電腦的混合式運算架構。AI 可以用於協調和管理這些混合式運算系統，充分發揮兩者的優勢。

儘管量子運算這項技術仍處於萌芽階段，但它有望透過解決傳統電腦難以處理的複雜問題來徹底改變各行各業。而對於企業在量子運算的投資方向，建議企業可以及早擬定策略。例如準備基礎設施建設、人才招聘和培訓、演算法研發、合作夥伴等，提早一步進行佈局。

IEEE 在 2024 年 10 月所進行的一項針對全球技術領袖的調查則顯示，超過三分之一（35%）的技術專家預計，量子運算將在 2025 年開始整合並應用到他們公司的業務中。此外，約三分之一（30%）的受訪者預計到 2025 年量子運算將在其公司全面部署，另有略多於四分之一（28%）的受訪者表示將在 2025 年考慮部署量子運算。該調查還顯示，受訪者估計五分之二（44%）的企業將在未來三年內部署量子電腦。

### II 企業需特別留意的「後量子密碼學」發展

特別值得留意的，是量子運算的快速發展對現有的加密方法同時也構成威脅，因為量子電腦有潛力破解目前廣泛使用的密碼系統。為了應對這種威脅，企業將可能需要部署「後量子密碼學」（PQC）來保護其數據安全。

後量子密碼學是一種新的密碼學，目的在抵抗量子電腦的攻擊。它的關鍵在於使用新的數學

### Info-Tech Research Group 2025 關注的三大類六大科技

#### 一、指數級人工智慧：

- 專家模型
- 人工智慧主權

#### 二、前量子基礎：

- 量子優勢
- 後量子密碼學

#### 三、數位人類：

- 人工智慧化身
- Deepfake 防禦

演算法來建立即使量子電腦也難以破解的密碼系統。

針對未來 PQC 的演變，企業目前可以進行的除了評估風險、評估不同的 PQC 演算法外，也要預先制定從現有密碼系統遷移到 PQC 的計劃，包括時間表、資源需求和測試流程。因為 PQC 演算法不能直接替換現有的 RSA、ECC、ElGamal，以及 DSA 等非對稱算法。企業可能需要重新編寫應用程式，並進行測試，以確保性能不受影響。另一方面，也可以預先朝增強員工意識、與安全專家和供應商合作，獲取最新的安全情報和技術支援等方向邁進。

目前量子運算的發展，根據 Oak Ridge 國家實驗室量子科學中心主任 Travis Humble 指出，量子運算在 2025 年將比 2020 年的早期階段取得顯著進展，全球各地的公司和研究人員正在開發各種相互競爭的方法，例如 transmons、離子和中性原子。這種多元化代表著量子運算系統相較於五年前的有限系統取得了重大飛躍。他認為，雖然量子技術很有前景，但目前的巨大挑戰是在量子系統發展過程中，如何管理和減輕可能的錯誤。Humble 指出，一些公司已經制定了技術路線圖，預計在未來五年內將推出量產規模的系統，混合方法的改進將提供對潛在產業影響的更清晰見解。

### 三、網路安全威脅與防禦的新趨勢

隨著 AI、量子運算、機器人技術等新興技術的快速發展，網路安全威脅也日益複雜和多樣化。企業需要更加重視網路安全，並採取更先進的防禦策略來保護自身安全。依照前述 IDC 對 AI 支出的預測，也等同顯示出企業必須在網路安全方面的應用加大投資。

此外，IEEE 在 2024 年 10 月進行的一項調查顯示，37% 的科技領袖正在考慮將人形機器人應用於業務，35% 的科技領袖預計將開始部署人形機器人，而 18% 的科技領袖預計將人形機器人完全應用於業務。這表明機器人技術在企業中的應用越來越廣泛，隨之而來的「機器人安全」

### IEEE 全球研究： 2025 年及以後科技的影響

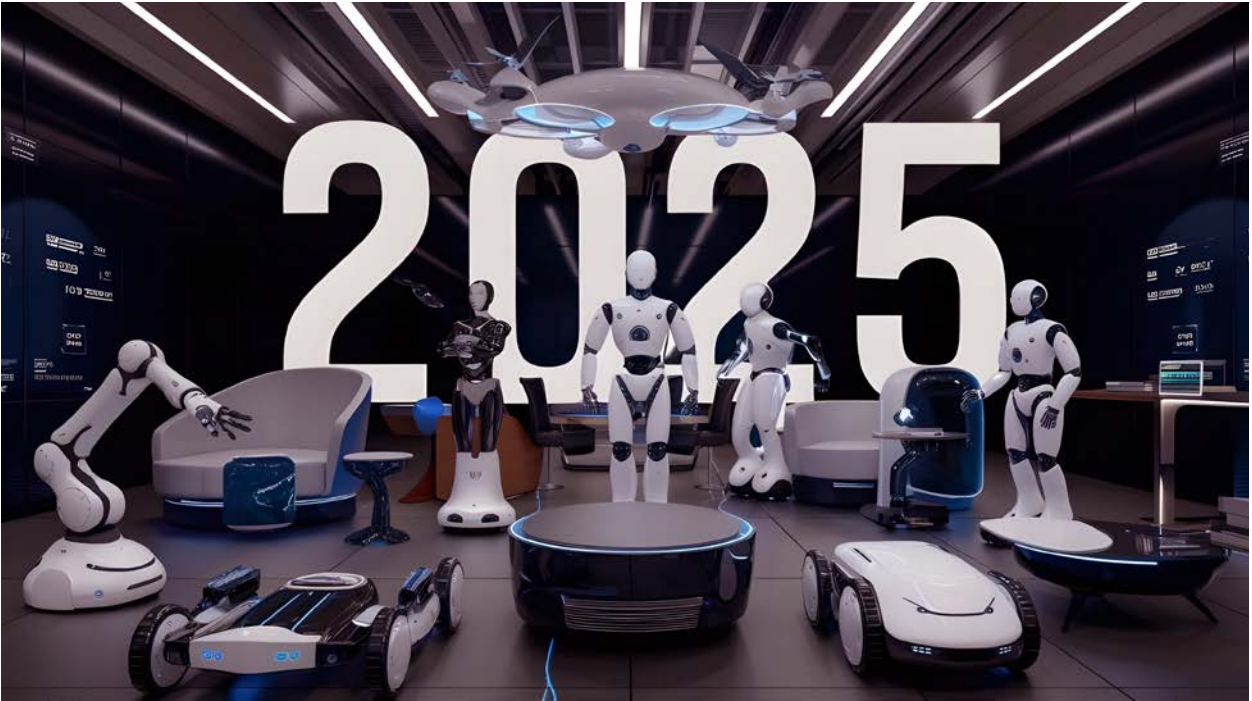
1. 人工智慧 (58%)
2. 雲端運算 (26%)
3. 機器人 (24%)
4. 擴充實境 (21%) ;
5. 工業物聯網 (19%) ;
6. 量子運算 (17%)
7. 電動車/電動車充電 (17%)

也將成為網路安全的重要議題。該調查還顯示，41% 的技術人員預計他們公司將在 2025 年開始將機器人網路安全機制配置到營運中，這表明企業也將更重視機器人安全，並將其視為網路安全策略的一部分。

而 2025 年的網路安全趨勢與 2024 年相比，預計將出現突破性的變革。主要原因是新興技術的快速發展，如人工智慧和量子運算，為網路安全帶來了新的挑戰和機遇。AI 技術的進步使得企業在提升網路防禦能力的同時，也為網路攻擊者提供了更強大的工具。攻擊者同樣可以利用 AI 自動化生成惡意軟體、發動更具針對性的網路釣魚攻擊，甚至模仿人類行為來繞過安全防禦系統。其次是前述提過的量子運算，對現有的加密演算法構成嚴重威脅。量子電腦強大的運算能力，可能破解當前廣泛使用的加密演算法，例如 RSA 和 ECC，危及企業和政府機構的數據安全。

面對 AI 和量子運算帶來的挑戰，企業需要考量採用更先進的網路安全防禦策略：

- **網路安全網格 (cybersecurity mesh)**：網路安全網格是一種分散式的安全架構，將安全控制措施分散到整個網路環境中，而不是集中在單一的安全邊界。這種方法可以提高安全性、靈活性和可擴展性，更有效地應對日益複雜的網路攻擊。
- **統一網路安全平台**：統一網路安全平台將企業內部部署、雲端和 AI 驅動的安全系統整合到單



一平台上，提供跨環境的視覺化和集中式威脅管理。這種整合可以簡化安全管理、提高效率並增強整體安全態勢。

- **後量子密碼學（PQC）**：為了應對量子運算的威脅，企業需要評估現有的加密系統，並開始規劃向 PQC 的遷移。PQC 使用量子電腦無法破解的演算法，保護數據安全。
- **AI 驅動的安全解決方案**：AI 可以用於自動化威脅檢測和響應、分析大量安全數據，並提供更主動的安全防禦措施。

2025 年的網路安全格局將與 2024 年截然不同。新的威脅和防禦技術將不斷湧現，企業需要積極應對，採用新的策略和技術來保護自身安全。