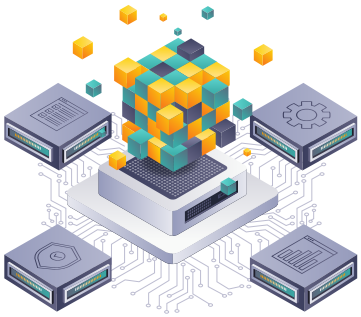

非紅軟體供應鏈成形？國際軟體管制趨勢與契機

Is a Non-Red Software Supply Chain Taking Shape?
International Software Regulation Trends and Opportunities

ソフトウェアサプライチェーンの脱中国　世界中のソフトウェア管制方向及び契機

文／資策會MIC　洪春暉資深產業顧問兼所長、施柏榮產業顧問兼副主任、楊晴資深產業分析師

從美國供應鏈與進出口相關的政策管制規範觀測，可以發現美國對於供應鏈的管控由早期的硬體設備、關鍵原物料擴散至AI模型與安全，顯見國際供應鏈管制已從硬體擴散至軟體端。面對此發展趨勢除了將其視為「風險」，或可思考是一種源自地緣政治所產生的一種新興市場需求，而「數位信任」即是此新興市場拓銷標章。

地緣政治驅動之下，國際供應鏈管制已從硬體擴展至軟體

2018 年美中貿易戰為先聲，美中兩國的競爭與對抗，早已進一步擴展至產品供應鏈。比如 2019 年由美國白宮公布的「確保資訊與通訊技術及服務供應鏈安全行政命令」（Executive Order 13873：Securing the Information and Communications Technology and Services Supply Chain），美國便將確保「ICT 供應鏈的風險」與「國家安全」相結合，形成新的國家上位政策之外，也延展出許多管制手段。

以 2010 年代末期迄今，美國供應鏈與進出口相關的政策管制規範來看，可以發現美國對於供應鏈的想像，2019 年至 2021 年主要關注的焦點為半

表一、美國供應鏈與進出口管制規範

年份	政策項目	內容
2019	確保資訊與通訊技術及服務供應鏈安全行政命令	白宮以國家安全為名，建立一套 ICT 供應鏈風險管理機制，禁止他國敵對勢力掌握、控制 ICT 供應鏈，以造成風險
2021	百日供應鏈審查報告	要求全面檢視半導體、大容量電池、稀土、藥品等貨品之供應鏈，提出本土製造、深化友岸外包等多元化韌性策略
2021	晶片與科學法案	藉由租稅優惠與研發補助等手段，加速半導體製造回流，以降低對特定國家供應鏈的依賴
2023	安全、可靠、可信任的人工智慧開發與應用行政命令	白宮除了強調 AI 應用風險管理之外，也強調與國際盟友與夥伴制定 AI 安全原則與行動準則
2024	連網車輛供應鏈最終規則	美國商務部發布一項規定，限制美國進口、銷售與中國或俄羅斯連網汽車的相關硬體與軟體
2025	人工智慧擴散管理架構	美國商務部修訂《出口管理條例》高階 IC 管制，並新增 AI 模型權重（Model Weights）、高階運算能力等管制
2025	美國人工智慧行動計畫	提出應與同盟國家共同建立 AI 生態系，推動美國完整 AI 技術堆疊，包含軟體、硬體輸出至可信任的國家
2026	促進新建人工智慧創新安全行政命令	要求建立安全評估機制，驅動 AI 開發者於模型公開之前，提供政府進行國家安全與資安測試，並實施 AI 出口規範

資料來源：Executive Office of the President（2019-2025），MIC，2026年7月

導體、資通訊設備以及關鍵原物料，尤以 2021 年的「百日供應鏈審查報告」為代表性例證。2023 年的「安全、可靠、可信任的人工智慧開發與應用行政命令」則可以視為另一個重要的轉折，美國對於供應鏈安全的理解，進一步擴展到 AI 的安全性；甚至在 2025 年進一步擴展至 AI 模型權重（Model Weights）等「軟體」元素。

除了美國之外，以歐盟在 2024 年公布的「人工智慧法案」（AI Act）為始，要求 AI 模型符合安全、可信任的同時，也納入數位信任與軟體管制規範的要素，且在「網路韌性法」（Cyber Resilience Act）之後更為清晰。該法要求所有具有數位元素的硬體與軟體，都必須符合該法所強調的安全設計、資安漏洞規範。不過，歐盟所建構的上位敘述與美國略有差異，美國多半以國家安全、穩固國家競爭力為主要論述支點，除了在某些特殊應用（如自駕車）限制來自中國、俄羅斯的軟體（如車聯網軟體）之外，多半是限制本國的高階軟體出口海外；歐盟則以「數位主權」與「主權 AI」為名，建構新的「市場准入」（Market Access）機制。

與歐盟相似，韓國在 2026 年 6 月公布「軟體供應鏈安全增強路徑圖」中，韓國政府清晰指出：當前軟體已成為各產業與社會運作的核心，但是當代的軟體大量依賴開源軟體、第三方元件、AI 生成程式碼及跨企業網絡的協作，使得軟體的供應鏈愈趨複雜，也提高了供應鏈受阻斷、攻擊的風險。值得留意的是，韓國的思考雖與歐盟相似，都具有「產品安全性審查」與「市場准入」的機制；然而韓國政府更加關注本國軟體企業在相關軟體產品的開發初期階段，就能夠符合歐盟等國家之標準。換言之，韓國「軟體供應鏈安全」的思考不僅是國家內部安全環境的維持，也是本國軟體產品向海外擴展的手段。

同樣的「科技民族主義」，但反映出不同的軟體管制國家意識與作為

回顧美國、歐盟、韓國軟體供應鏈管制規範，無論是軟體的輸出或者輸入，皆與過去強調全球專業化分工、技術擴散的「科技全球主義」（Techno-globalism）存在相當明顯的差異，反而有非常顯著的「科技民族主義」（Techno-nationalism）的內涵，也因此各國進一步創造出管制標準、規範與門檻。

表二、美、歐、韓三國軟體供應鏈管制意識與作為比較

	美國	歐盟	韓國
全球位階	AI 的超級強權	AI 治理與數據權力引領者	軟體技術後進追趕者代表
國家意識	國家安全、非紅供應鏈	人權、非紅供應鏈（部分國）	國家安全、本國產業扶植
產業敘事	美國全棧式 AI 對外輸出	主權 AI、數據主權	全球軟體供應鏈信賴夥伴
管制作為	・建構數位信任標準 ・軟體輸出管制 ・部分產品海外軟體的輸入禁令（自駕車）	・建構數位信任標準 ・市場准入（軟體輸入管制）	・市場准入 ・輔導本國軟體業者，符合國際軟體標準（資安與數位信任）

資料來源： MIC，2026年7月

然而，能否將近年軟體供應鏈的管制規範，直接定義為「非紅軟體供應鏈」的形成？雖然以美國來看，2024 年的「連網車輛供應鏈最終規則」中，明確指出禁止中國、俄羅斯的車聯網軟體，其餘並未直接特定的國家生產之軟體。同樣的，歐盟的「網路韌性法」也並未直接指稱特定國家，畢竟，這可能會衍生出貿易歧視的風險與爭端。

由此觀之，「非紅軟體供應鏈」更傾向於被生產出來的產業競爭論述，而非具體的管制規範或制度。此外，軟體供應鏈管制也與硬體管制存在差異，其中軟體供應鏈管制會因為產品的「屬性」而在管制難度上有所區別，主要原因可能包括軟體產品之原產地判斷更為不易，且流通的形式也更加複雜，因此要對「軟體產品」進行管制的難度可能更高。

當非紅供應鏈成為「地緣政治經濟學」，而「數位信任」即是新的市場拓銷標章

面對國際軟體管制的發展趨勢，除了將其視為「風險」，更應積極的思考是一種源自地緣政治所產生的一種新興市場需求，如韓國「軟體供應鏈安全增強路徑圖」即值得臺灣參考。據此，臺灣後續的契機有三：

第一，臺灣在 AI 伺服器、網通設備、工業電腦、邊緣運算裝置等具有相對優勢，亦掌握產品設計與整機整合能力。此類在臺灣具有輸出優勢的 ICT 硬體產品，可針對其內建之軟體與國際大廠建立共同可信任之軟體規範，同時強化輸出優勢。

第二，面對歐盟等國之軟體供應鏈安全規範，輔導國內軟體開發者，於初期產品設計及開發階段即導入對應的安全設計、漏洞揭露、安全系統開發生命週期（SSDLC）機制，降低後續法規遵循成本之外，也藉此提升國際市場競爭力。

第三，持續建立國家可信任軟體驗證平台，整合軟體安全檢測、AI 模型安全測試及法規符合性驗證等能力，提供中小企業及軟體開發者使用，進一步孕育臺灣的可信任軟體驗證與第三方測試服務能量。

當國際供應鏈管制已從硬體擴散至軟體端，「信任」與其被認知為軟體開發的標準，它更應該被視為一種面對非紅供應鏈時，在「地緣政治經濟學」下的臺灣產品國際拓展標章。

表三、硬體與軟體供應鏈管制特性比較

供應鏈管制	硬體	軟體
管制主體	晶片、零組件、終端產品	OS、AI 模型、軟體套件
產地判斷	較容易判斷製造國、組裝地	難以判斷，程式碼來自全球開發者
流通形式	海關、物流	跨境數位交付、雲端平台、隨硬體交付
檢驗方式	檢測、抽驗、產品認證	漏洞掃描、原始碼審查

資料來源： MIC，2026年7月