「歐盟資通訊供應鏈安全工具箱」之建議簡介

2026.2.18 駐歐盟經濟組

歐盟執委會於 2026 年 2 月 13 日公布「歐盟資通訊供應鏈安全工具箱(EU ICT Supply Chain Security Toolbox)」[1]，此係本年 1 月 20 日所提出網路安全法(Cybersecurity Act) 修訂架構之一環，目標在建立更具一致性之歐盟層級供應鏈資安治理模式。該工具箱提供一共同方法，協助辨識、評估及緩解 ICT 供應鏈之網路安全風險，並詳列風險情境(risk scenarios)及建議，謹針對執委會對會員國所列建議簡要說明如下。

一、完善 ICT 供應鏈風險管理架構

建議 1、建立並執行 ICT 供應鏈風險評估：會員國應進一步在國家層級建立並執行 ICT 供應鏈風險評估，並適時支持歐盟層級之協調風險評估。會員國應確保及時評估關鍵產業之供應鏈風險與辨識關鍵供應商，應盡可能預視潛在斷鏈與可能出現之威脅。建議會員國實施以下措施：

- 考量對會員國具有優先性之供應鏈或產業，定義國家風險評估之範疇。
- 定期進行國家供應鏈風險評估，並將歐盟與國際標準、本工具箱風險情境，以及歐盟協調風險評估納入考量。
- 考量在國家風險評估中採用「歐盟層級網路安全風險評估方法之原則。
- 與歐盟執委會及歐盟網路安全局(ENISA)合作，支持由 NIS 合作小組所進行辨識歐盟層級協調安全風險評估之程序
- 確保國家主管機關具備權限與工具，從實體(entities)收集關鍵產

[1] 歐盟資通訊網絡暨科技總署(DG CNECT)https://digitalstrategy.ec.europa.eu/en/library/toolbox-improve-ict-supply-chain-security

業之供應商及其產品之資訊，建立明確之資訊分享指引，以避免過度的行政負擔，並定期監測該些資訊。

- 為相關實體(entities)訂定國家及/或產業層級之指引，以評估其供應商的關鍵性，並將評估結果通報國家機關 。
- 識別關鍵供應商並評估供應鏈風險。
- 在國家層級，分析與比對(map)關鍵依賴性，識別潛在的依賴來源與單一故障點(single points of failure)。
- 將機敏資訊(包括公用與私人)之特定風險納入考量，包括透過 ICT 供應商非法獲取此類資訊之可能性。

建議 2、確保 ICT 供應鏈風險管理之結構化方法：會員國應確保各實體遵循結構化之供應鏈風險管理方法，以補充 NIS2 指令[2]及網路韌性法(CRA)之措施。各實體應認知其 ICT 供應鏈風險(透明度)、分析及緩減該些風險。建議會員國實施以下措施：

- 支持重要及必要實體採取適當且符合比例之網路安全風險管理措施，以管理已識別之供應鏈安全風險，及監測其有效性與進展。
- 為各實體(尤其是中小企業)提供公開且充分之指引，說明管理供應鏈安全風險之適當措施與措施有效性之監測方法。
- 確保各實體透過合約安排與保證機制，確保其關鍵供應商實施適當、符合比例且可衡量的網路安全風險管理措施，以緩減識別的供應鏈安全風險。主管機關應考慮針對修復缺陷之實體提出具約束力之指示。
- 建立供應商與服務提供者名錄，並考量將其擴展至原範圍外的其他實體。
- 進行整備測試或壓力測試，以確保相關實體實施適當的風險管

[2] 高度共通程度之網路安全措施指令(Directive on measures of a high common level cybersecurity across the Union)，簡稱 NIS2 指令

理措施，並對供應鏈威脅具備韌性 。

- 根據已識別的漏洞與威脅，考慮監測或確保實體所交付或使用的產品與服務，在已建立之測試平台或沙盒環境中充分測試。

二、彈性、多元及韌性之 ICT 供應鏈

建議 3、推動多元供應商策略(Multi-vendor strategies)與政策，以因應戰略性依賴風險：會員國應在可行情況下採取政策與監管措施，確保實體制定多元供應商策略，以確保關鍵 ICT 供應鏈。建議會員國實施以下措施：

- 在國家層級發展並實施多元供應商策略與政策，以因應戰略性依賴風險。
- 考慮「友岸外包」(friendshoring) 或「近岸外包」(nearshoring)，以限制地緣政治威脅與氣候相關事件之風險。
- 制定特定 ICT 服務、系統或產品之關鍵多元化供應商之門檻，此門檻應基於客觀條件、國家風險評估，並與受影響實體協商制定。多樣化門檻之標準可包括：供應商市場佔有率依賴、地緣政治風險暴露、供應商網路安全合規性，以及單點故障風險等。
- 透過公共採購要求、財務誘因及監管措施，使實體實施多元供應商策略以符合歐盟及會員國法規框架，確保供應商多元化。
- 當存在一個以上適合之供應商時，關鍵供應鏈之實體應：
  - 發展並實施多元供應商策略與政策以因應高依賴風險。
  - 透過跨區、來源及資產，以多元化 ICT 供應鏈與建立其供應鏈韌性。
  - 致力於供應商充足，如透過雙重或多重來源供應，並確保互通性(interoperability)促進服務間之無縫運作。

建議 4、在會員國層級管理、限制或排除高風險供應商：會員國應

評估關鍵供應商的風險狀況，以識別高風險供應商。此評估應基於所蒐集之供應商資訊、比對(mapping)及預設之條件。會員國應採取措施管理高風險供應商。建議會員國實施以下措施：

- 基於辨別高風險供應商之預設條件，建立國家框架以評估關鍵供應商，該些條件包括：
  - 供應商受第三國干擾的可能性，其原因可能包括：供應商與第三國政府緊密連結、第三國法治或民主制衡機制不健全或缺乏安全與資料保護協定、供應商企業所有權的特質、第三國施壓之可能性等。
  - 估應商限制或拒絕供應、或提供未授權物品之可能性。
  - 供應商網路安全實務，包括其供應鏈控制程度、是否充分將網路安全視為優先。
  - 供應商風險狀況評估可將歐盟及會員國主管機關所發出之注意(notice)納入考量。
  - 供應商受第三國司法管轄，該第三國已進行造成威脅之惡意網路活動或攻擊。
  - 供應商受第三國司法管轄，該第三國收集網路漏洞用於攻擊。
- 確保各實體依據預設條件與指引，辨識高風險供應商及對其依賴度，以評估供應商之風險情形。
- 確保國家政策與法規，限制或排除供應鏈中高風險供應商，採取適當措施讓該供應商對供應鏈之風險降到最低。
- 依據供應商風險概況評估及可能限制或排除等措施(包括在政府採購隊 ICT 服務、系統、產品之網路安全相關要求、調整評選標準(awarding criteria)等)，以確保 ICT 供應鏈安全及鼓勵私部門亦採取同樣作法。

三、情勢認知與營運合作：

建議 5、促進資訊交換、認知與訓練：會員國應致力加強資訊交換及 ICT 供應鏈安全最佳實務之合作。歐盟網路安全局(ENISA)應促進歐盟層級之資訊分享，提供會員國及產業指引，發展訓練計畫，促進供應鏈網路安全之認知、確保 ICT 服務、系統或產品之採購與使用。建議會員國實施以下措施：

- 將國家風險評估結果通報 NIS 合作小組，並對歐盟層級風險評估有所貢獻。
- 在 NIS 合作小組分享執行供應鏈安全措施之進展與挑戰。
- 建立並標準化 ICT 供應鏈相關事件之蒐集與分析，在可行且不影響國家安全職權下，將下列事項納入考慮：
  - 各國特定之情報(如國家安全威脅評估)；
  - 已知事件及網路威脅情報；
  - 含數位元素之特定產品類別，其歐盟整體依賴性評估結果。
- 在 NIS 合作小組等組織，分享有關 ICT 供應鏈事件之資訊。
- 支持相關實體建立管理供應鏈安全之適當技能。
- 與 ENISA 合作，在國家層級推廣供應鏈安全認知。
- 在 NIS 合作小組，交流落實本工具箱建議之最佳實務。
- 在國家與國際層級之網路安全演練中，推動使用本工具箱所列之風險情境。

四、韌性、信賴且透明之工業基礎

建議 6、開發並支持確保供應鏈之互通生態系(interoperable ecosystem)：會員國應促進歐盟層級建立一生態系，以提升供應鏈安全與發揮經濟效益。降低戰略性依賴，強化歐洲供應商生態系之倡議，均應在會員國及歐盟層級推動。建議會員國實施以下措施：

- 推動歐盟倡議，以發展歐洲供應商生態系及支持歐盟產業供應鏈安全，並與歐洲網路安全能力中心(European Cybersecurity

Competence Centre, ECCC)密切合作。

- 確保或公共資金支持之 ICT 專案，反映網路安全風險，並遵循本工具箱之建議。
- 在公共採購中納入 ICT 服務、系統及產品之網路安全相關要求及調整評選條件，以確保供應鏈安全，並鼓勵企業採取同樣作法。
- 確保採取適當且合宜之措施支持中小企業(SMEs)，如認知提升、支持計畫協助中小企業合規與轉型需求。
- 促進開源軟體與硬體之安全性與可見性，尤其在可強化關鍵實體供應鏈安全下，鼓勵採用安全之開源替代方案，例如：
  - 將現有公部門解決方案開源化，
  - 設立開源專案辦公室，
  - 多元化數位網路設施。

建議 7、透過適當標準與認證之採用與發展促進互通性 (interoperability)：會員國應在歐盟層級推動適當標準與認證機制之發展與採用，並以現有歐洲與國際框架為基礎，與歐洲標準化組織及其他相關機構合作。歐盟層級之框架、標準或歐洲網路安全認證機制，應促進互通性，以形成跨歐盟之效果、市場認知及公平競爭環境。建議會員國實施以下措施：

- 在現有標準化及認證論壇中，確保歐洲利益充分表達。
- 確保充分參與認證機制與標準之維護，納入新漏洞之相關資訊及確保相關資訊在供應鏈適切傳遞。
- 推動漏洞(vulnerabilities)協調一致的評估，整合來自市場監管、產業及安全研究人員之資源，並將歐盟框架及內部市場整體一致性納入考量。
- 推動開放標準(open standards)及安全即設計(secure-by-design)原則，以促進多元供應商環境。