半導體發展之潛藏風險 資策會科法所：應注意國際供應鏈資安政策趨勢與國際標準

(中央社訊息服務20210706 17:13:52)

COVID-19疫情，加速各行各業數位轉型，帶動遠距上班、遠距教學等生活型態轉變，進一步推升資通訊技術（ICT）產品的需求，連帶使得作為電子、3C商品、手機等產品的核心組成元件—晶片的需求量大增。ICT產品之生產製造，基於成本控制考量，具有供應鏈全球化的現象，惟在較難確保外部技術與元件安全性的情況下，可能衍生受資安攻擊的風險。長期關注資安法律議題的財團法人資訊工業策進會科技法律研究所（資策會科法所）表示，我國以生產晶片的半導體產業為關鍵發展產業，尤應留意ICT產業供應鏈的資安防護。

ICT已廣泛應用至各產業領域，而在ICT產業供應鏈的全球化浪潮下，委外設計、開發、採購外部軟、硬體元件、技術或服務已成常態。若供應商、合作單位的資安防護完整度不足，將使得駭客有機會以特定廠商作為跳板，入侵或滲透供應鏈上、下游中特定公司之資訊系統，進行資安攻擊，甚至形成大範圍感染或擴散。ICT產業供應鏈對國家經濟、國防安全極具重要性，國際間也已陸續發布相關的安全政策或要求，如美國「2021年改善國家安全的行政命令」、歐盟/北約「布拉格5G安全會議之提案與共識」、歐盟「ICT產品與服務之資安驗證機制」、歐盟ENSIA「物聯網供應鏈安全指引」等。



資策會科法所副法律研究員阮韻蒨指出，美國已逐步推動ICT產業供應鏈安全相關法制政策，提醒我國半導體廠商可留意相關規範與其未來發展

資策會科法所副法律研究員阮韻蒨表示，自2019年美國白宮發布「確保資通訊技術與服應鏈安全行政命令」後，便逐步推動ICT供全相關法制政策，近來因應美中貿易戰，除出口管制相關規範與搭配實體清單方式，加通訊產品或服務的出口控管之外，亦建立乾路政策打造安全ICT產業供應鏈，並邀請他參與響應。此外，為強化軍事、國防工業供資訊安全防護，建立資安成熟度模型驗證機（CMMC），要求相關承包商應通過驗證，藉以確保國防工業供應鏈之資訊安全。阮韻蒨提醒，我國半導體廠商若有與美國聯邦政府和ICT產業合作往來時，可留意相關規範與其未來發展。

應美國建立資安成熟度模型驗證機制（CMMC），要求承包商應通過網路安全驗證，
資策會科法所提醒我國廠商應留意相關規定

資策會科法所另針對半導體產業供應鏈之IC設計、晶片製造，研析相關資安國際標準或產業標準，如軟體安全成熟度模型（BSIMM）、IEC 62443（工業自動化控制系統管理）標準、國際半導體產業協會(SEMI)相關資安標準草案之提案等，期望藉此引導國內業者掌握國際上重要供應鏈資安政策趨勢，進而導入企業組織內部提升資安管理，落實ICT產業供應鏈的資安防護，以增加其在國際供應鏈中之競爭優勢。

上稿時間： 2021年07月06日

新聞來源： https://www.cna.com.tw/postwrite/Detail/295828.aspx