

打造能被世界信賴的資安系統及產業鏈

國發會產業發展處

壹、前言

近年來數位經濟帶動各個產業朝向跨世代、跨境、跨領域等趨勢發展，隨著物聯網、人工智慧等數位創新科技滲透到各個領域，已帶動經濟活動、社群媒體、生活型態等模式的變革轉型，進而使產業生產力提高、民眾生活品質提升，並影響全球經濟、社會及生活等層面。

然而新興的數位技發展亦帶來如駭客利用人工智慧強化攻擊，物聯網裝置應用環境複雜造成安全防護難度提升、5G 網路安全防護等新的網路安全議題，使資安威脅日益嚴重。因此，總統於本（109）年 5 月 20 日就職演說時，提出六大核心戰略產業，並表示將要發展可以結合 5G 時代、數位轉型、以及國家安全的資安產業，並打造可以有效保護自己，也能被世界信賴的資安系統及產業鏈。

貳、亞太地區資安威脅狀況

微軟於 2019 年 2 月公布第 24 期「智慧資安報告」(Microsoft Security Intelligence Report)，針對 2018 年微軟雲端每日所偵測到的 6.5 兆個網路威脅訊息進行分析，報告中顯示包括澳洲、中國、香港、印度、印尼、日本、馬來西亞、紐西蘭、菲律賓、新加坡、韓國、斯里蘭卡、臺灣、泰國和越南等 15 個亞太地區國家為網路犯罪的熱點，網路威脅主要是利用漏洞進行惡意軟體、加密貨幣挖礦、勒索軟體及偷渡式下載等攻擊。

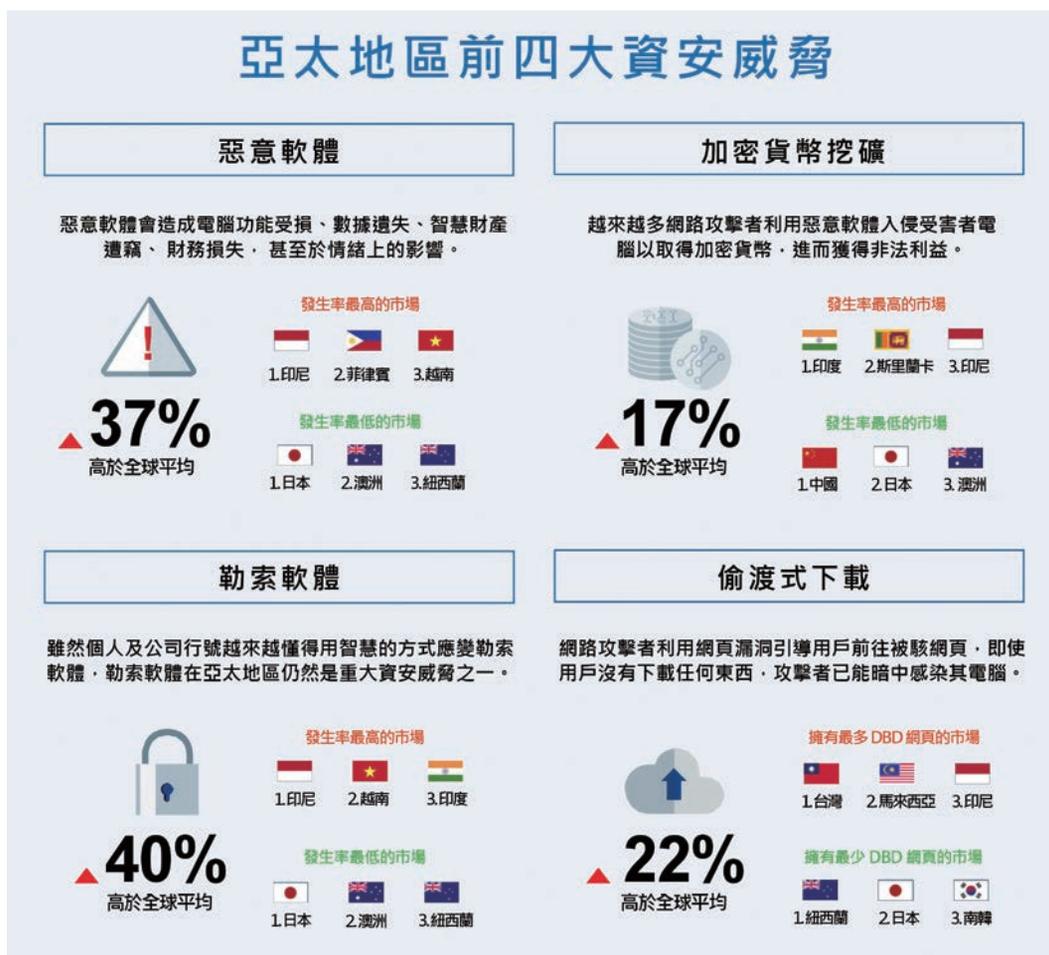


圖 1 微軟「智慧資安報告」重點圖表

資料來源：微軟新聞中心網站。

報告指出，在 2018 年 1 月至 12 月期間，全球惡意軟體攻擊頻率下降 34%，亞太地區的惡意軟體發生頻率卻比全球平均高出 37%，其中印尼、菲律賓和越南是亞太地區惡意軟體發生頻率最高的國家，突顯了發生頻率與使用盜版軟體、瀏覽具潛在風險的網站等不良使用方式有關，而發生頻率最低的日本、澳洲和紐西蘭等國家則擁有成熟的網路安全基礎設施與良好的網路使用安全意識。

在 2018 年間犯罪份子搭上挖礦潮，透過惡意軟體入侵受害者的電腦藉此開採加密貨幣。報告發現攻擊頻率隨著加密貨幣價值起伏而變動，而亞太地區加密貨幣挖礦惡意軟體攻擊發生頻率則比全球平均高出 17%。另外，因企業和個人對勒索軟體威脅變

得更加警覺，使全球勒索軟體發生頻率減少 73%。雖然全球比例下降，但亞太地區的發生頻率依然比全球平均高出 40%。

偷渡式下載是在使用者瀏覽網站時，將惡意程式下載到毫無防備的使用者電腦上，更進階的偷渡式下載還會在受害者電腦上安裝勒索軟體，甚至是加密貨幣挖礦惡意軟體。2018 年全球偷渡式下載頻率雖然減少 22%，但亞太地區偷渡下載頻率卻比全球平均高出 22%，其中攻擊最頻繁的地區是臺灣、馬來西亞和印尼。

叁、臺灣資安產業狀況

依據工研院產業科技國際策略發展所（以下稱工研院產科所）調查發現，2019 年臺灣資安產業廠商數達到 324 家廠商，就業人數約在 8,800 人，資安產值約 493.4 億元臺幣，年成長率為 12.3%。資安產品在硬體與模組部分的產值約為 253.9 億（51.4%），軟體部分的產值約為 47.8 億（9.7%），服務部分的產值約為 191.8 億（38.9%），顯示我國資安產品仍以硬體為主。

工研院產科所將臺灣資安產業廠商依產業鏈上中下游分為八大類型，包含上游的「終端與行動裝置防護」有 31 家廠商、「網路安全」有 53 家、「資料與雲端應用安全」有 24 家、「物聯網安全」有 13 家，中游提供專業資安服務的「資安營運管理服務」13 家及「資安檢測稽核顧問服務」48 家，下游則是廠商家數最多的「系統整合服務」132 家及「資安支援服務」12 家。

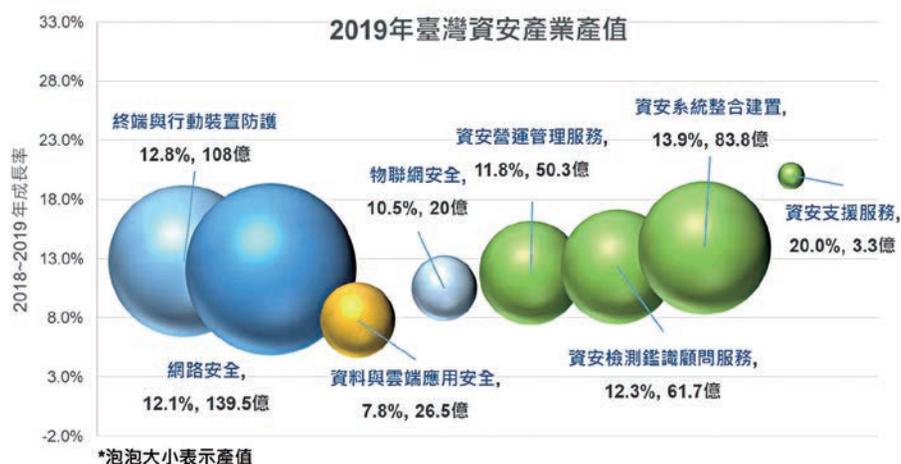


圖 2 2019 年臺灣資安產業產值分布

資料來源：工研院產科所。

肆、發展資安卓越產業

為因應 5G、AIoT 等技術帶動的數位轉型及智慧化需求，國內必須有強大的資安產業做後盾，因此政府規劃推動資安卓越產業發展方案，藉由臺灣易受駭客多樣攻擊之獨特環境，協助我國業者以此掌握特殊資安攻擊模式，發展資安利基產品。方案規劃以強化新興領域防護及打造高階實戰場域為主軸，發展 5G、半導體等新領域資安國際解決方案並建置國際攻防場域及高階資安人才基地，推動重點如下：

一、研發 5G、半導體等前瞻技術

(一) 以科專計畫研發 IC 設計檢測、5G 等防護技術與 AI 輔助偵防

1. 開發 5G 與晶片安全檢測技術，於 5G 產品出廠及晶片設計階段驗證其安全性，並針對 5G 應用、半導體及智慧醫療等領域開發相關防護技術與安全機制。
2. 開發 AI 輔助偵防技術，並與新興資安應用整合以協助進行資安情資分析，達到自動化資安偵防的目標。

(二) 建立 5G 網路資安管理機制、邊緣運算資安檢測及驗證實驗室

1. 配合 5G 技術標準之演進，針對 5G SA 網路架構、5G 多接取邊緣運算 (MEC) 之安全管理進行研析，並研提資安管理機制。
2. 建置 5G 網路資通安全檢測實驗室，提供業者其服務與應用軟體所需之資安評估及檢測服務，以協助業者完備 5G 網路資安防護能量。

二、開發 AIoT 及醫療等新興領域解決方案

(一) 推動跨域聯防計畫，由資安業者與 5G、物聯網及醫療等新興產業組成團隊，開發防護產品。

由法人、資安業者與 5G、物聯網及醫療等新興產業業者組成資安旗艦團隊，建立長期合作導入應用之關係，以開發新興領域資安整體解決方案，並共同行銷國際。

(二) 透過各產業推動平台，盤點並導入核心產業所需資安

透過六大核心戰略產業與五十二產業創新計畫等各產業推動平台，協助盤點並導入各核心產業所需之資安解決方案。

三、成立資安攻防及跨國合作機構

(一) 進行國防、國安所需前瞻資安研究

進行國家任務導向型研究，以提供政府機關短中期所需之資安應用技術，包括技術面（如主動式防禦技術等）及政策面（如跨國網路戰之國際法規研究等）議題。

(二) 建置關鍵基礎設施模擬場域，進行攻防演練

建置國內關鍵基礎設施之工控場域，如能源、水資源、交通、衛生醫療等領域，以支援教育訓練並進行實戰攻防演練。

(三) 與歐美如柏克萊大學、NATO 聯合網路防禦中心等機構合作

合作對象以美國、歐洲等國家級或以資安著名之研究機構為合作對象，初期將鎖定資安重點學校，後續逐步擴展至國家實驗室或標準制定機構。

四、完善資安高教環境

針對國立大學資安相關科系增加師資名額，同時加碼提供彈性薪資補助，目標於 4 年內增聘 80 名編制內專任教師。

伍、結語

在數位化時代，許多新興領域應用都快速發展中，使資安的重要性日益增加。臺灣具備頂尖資安人才，加上臺灣處在受駭客攻擊的特殊環境，透過政府與產業共同合作發揮前述優勢，將可打造能被世界信賴的資安系統及產業鏈，使臺灣成為國際上的關鍵力量。🌐