114年度國家資通安全情勢報告

數位發展部
中華民國 115 年 3 月

目　錄

圖目次

壹、依據及目的

本部依資通安全管理法（以下簡稱資安法）第 6 條規定，定期公布「國家資通安全情勢報告」。

隨著全球資安威脅多層次且高度複雜化，AI 技術快速發展、社交工程與國家級威脅持續升高，各界應建立風險管理、持續偵測、零信任及資料保護機制，並透過情資共享強化預警與應變能力。本報告透由研析 114 年全球資通安全威脅情勢及我國政府機關所面臨資通安全威脅現況，研提相關資安防護建議，協助各機關了解威脅趨勢調整資安政策，並強化資通安全防護意識，以期強化國家整體資安防護韌性，維持服務可用性，並打造永續經營之數位國家。

貳、114 年全球資安威脅情勢概要

根據世界經濟論壇（World Economic Forum, WEF）發表 2026 年全球風險報告（Global Risk Report 2026）指出，18%受訪者將地緣經濟對抗（Geoeconomic Confrontation）列為 2026 年最可能引發重大全球危機之首要風險，前十大風險中，與資訊技術相關風險包含占居第 5 名「錯誤與虛假訊息」（Misinformation and Disinformation）、第 8 名「人工智慧技術的不良後果」(Adverse outcomes of AI)及第 9 名「不安全網路」(Cyber Insecurity)，其中「人工智慧技術的不良後果」為所有風險排名上升幅度最大，於 10 年期全球風險嚴重程度調查攀升至第 5 名，顯示長期風險影響力深遠，應即早評估其衝擊與預做因應策略。

AI 技術快速發展，不僅帶來新型網路威脅與安全弱點，也成為推動資安變革之重要因素，隨著 AI 應用滲透各領域，攻擊手法日益多樣化，地緣政治緊張使網路戰爭與國家級攻擊頻繁發生，組織因此將關鍵基礎設施防護、國家級資助攻擊與情報蒐集納入資安策略。同時，供應鏈高度關聯但透明度不足，第三方軟硬體與雲端服務之安全缺陷可能引發系統性風險與連鎖效應，凸顯整體防護韌性之重要性。

網路犯罪亦隨著技術進步而演變，呈現高度組織化與商業化，特別是 AI 被廣泛應用於攻擊過程中，使詐騙、釣魚及身分盜竊手法更加精準且難以防

範；同時，犯罪即服務平台降低操作門檻，進一步擴大攻擊規模與複雜度，多數組織的網路韌性仍處於初期階段，面對快速變化的威脅、供應鏈漏洞及專業人才不足，提升韌性顯得刻不容緩。透過國際風險報告及全球重大網路攻擊案例分析，可掌握中長期資安風險趨勢與短期威脅手法，為政府機關部署防護措施提供重要參考。

分析與綜整 114 年全球重大網路攻擊事件，詳見圖 1。

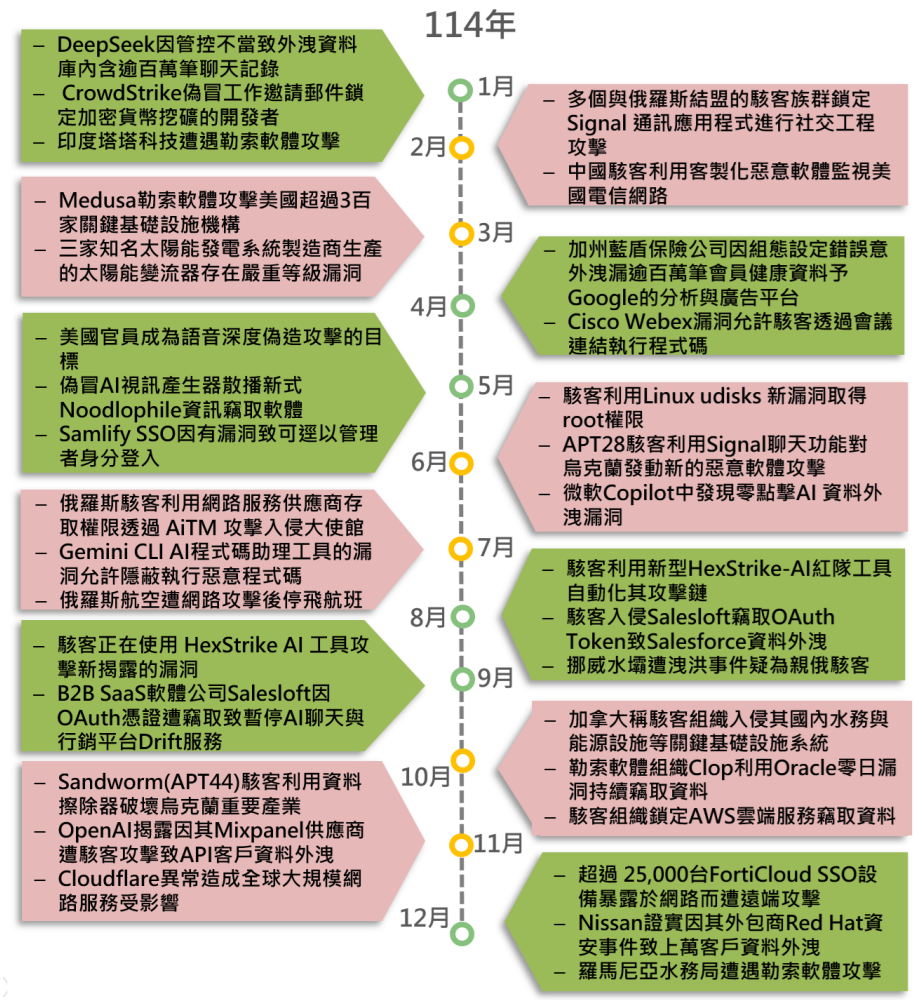

圖 1　114 年全球重大網路攻擊事件

綜整研析世界經濟論壇（WEF）、歐盟網路暨資訊安全局（European Union Agency for Cybersecurity, ENISA）及各資安業者調查報告等資料，114年全球資安威脅情勢可歸納為6大面向，包含「AI成為威脅態勢中的關鍵因素」、「網路釣魚與社交工程攻擊日益嚴峻」、「國家級威脅驅動APT鎖定與勒索軟體風險」、「資安（訊）供應鏈加劇數位生態系統風險」、「資通系統弱點頻遭利用」及「雲端應用衍生多元威脅」。

一、AI成為威脅態勢中的關鍵因素

IBM於2025年發表資料外洩成本報告（Cost of a Data Breach Report 2025）新增多項AI議題與調查，反映於數位環境下採用生成式AI與自動化工具後，組織於威脅情勢、資安風險及防禦策略將面臨重大轉變。導致資料外洩成本攀升之三大關鍵因素分別為「供應鏈漏洞」、「安全系統複雜度」及「影子AI」，其中「影子AI」取代「資安技能短缺」，成為資料外洩事件中成本衝擊前三大因素之一。雖然AI資安事件於整體外洩案例中仍屬少數，惟調查顯示有13%組織曾遭遇與AI模型或應用程式工具相關資料外洩事件，其中97%缺乏完善的AI存取控管機制，主要風險源自AI供應鏈環節，如受感染或竄改的應用程式、不安全API介接及第三方外掛模組管理疏失等，可能引發連鎖安全效應。

駭客透過HexStrike-AI滲透測試自動化平臺，鎖定尚未修補公開漏

洞對象，於獲取漏洞資訊後自動生成程式碼，再迅速執行遠端程式碼攻擊，同時植入遠端控制工具 Webshell 以維持後續存取與控制能力。此類結合 AI 自動化漏洞攻擊流程，使漏洞從揭露到被大規模利用時間，從原本以數日或數週計，縮短至以分鐘計。另因 HexStrike-AI 具備重試與自動恢復機制，能於攻擊過程遭遇錯誤時可自行調整參數並重新執行，進一步提高攻擊成功率。

機關組織應從多面向強化資安防禦，包含持續接收與更新威脅情勢、即時漏洞修補、強化異常行為偵測、落實邊界設備監控及事件鑑識等措施，評估導入以 AI/ML 驅動之偵測系統，透過端點行為與網路流量等分析工具，建立異常行為模型，俾利即時發現潛在攻擊跡象，提升整體防禦效能。

二、網路釣魚與社交工程攻擊日益嚴峻

根據 ENISA 2025 年威脅情勢報告（Threat Landscape 2025）分析，網路釣魚仍為現今最普遍且具破壞力的初始入侵手法，占所有入侵事件近 60%。駭客常透過電子郵件、簡訊、假登入頁面或語音詐騙等方式，誘使受害者執行看似正常、實則具惡意行為的操作，如點擊連結、輸入帳密或下載惡意檔案，隨著釣魚即服務（Phishing-as-a-Service）工具日趨成熟與普及，攻擊門檻大幅降低，相關平台能自動生成偽冒登入頁面並

快速大量散播釣魚連結，使不具技術能力攻擊者也能發動大規模釣魚行動。另 AI 技術濫用亦成為網路釣魚與社交工程攻擊快速成長的關鍵因素，包含駭客利用越獄大型語言模型（Jailbroken Models）、合成影音媒體（Synthetic Media）、以及模型中毒（Model Poisoning）等技術，促使攻擊模式朝向高度自動化與大規模擴散發展，使攻擊威脅持續攀升。

Google 揭露駭客利用 Signal 跨平台開源即時通訊應用程式的設備連結功能，展開網路釣魚活動，駭客族群濫用 Signal「設備連結」功能，該功能允許 Signal 使用者掃描二維條碼後，於多個設備上使用。因此駭客製作惡意二維條碼，當受害者掃描條碼後，所傳訊息將自動同步予駭客，因受害者設備功能並無異動，若未主動確認連結設備列表，駭客能持續潛藏竊聽受害者通訊內容，且缺乏可用監控機制，入侵活動可能潛藏許久而不被發現。

為降低即時通訊應用程式之資安風險，機關應明確規範可使用之通訊程式，限制僅能使用官方授權版本，同時停用不必要附屬功能，避免於群組中討論或傳輸機敏資訊，並留意群組成員異動情形，以防範不明對象加入。此外，應強化使用者資安意識，面對更新通知、群組邀請、二維條碼或其他要求立即操作連結時，應先確認來源真偽，以降低偽冒更新與社交工程攻擊風險。

三、國家級威脅驅動 APT 鎖定與勒索軟體風險

根據資安廠商 CrowdStrike 2025 年全球威脅報告（2025 Global Threat Report）觀測全球國家級威脅族群，以中國相關 APT 組織成長最為明顯，其整體攻擊活動較 2023 年增加 150%，其中以金融服務、媒體、製造業及工業控制等關鍵產業攻擊量增幅最高，相較過往年度成長 200%至 300%。另就攻擊目標而言，中國駭客族群最常鎖定政府、科技及電信等三大領域，2024 年入侵活動相較 2023 年增加 50%，攻擊模式已由以往廣泛且快速攻擊行為，轉為精準且任務導向行動，並採取長期潛伏、持續情報蒐集及高度整合入侵資源等協作方式執行，使滲透活動更為隱匿且難以偵測。

資安廠商 ESET 於 2025 年 Q2 與 Q3 APT 活動報告指出，俄羅斯駭客族群 Sandworm(APT44)持續針對烏克蘭及其支援國家發動大規模網路攻擊，並部署多款新型破壞性抹除工具，如 ZEROLOT 與 Sting，主要鎖定烏克蘭政府機構、能源設施、物流業者及糧食出口產業，以削弱戰時經濟與關鍵基礎設施運作能力。此駭客族群入侵模式延續「假勒索、真破壞」戰術，雖模仿勒索軟體介面，但實際不具備解密或復原機制，透過覆寫開機記錄、破壞檔案系統或清除系統檔案，對系統造成不可逆損害，並藉勒索假象轉移鑑識焦點、延誤事件調查。

對於此類入侵活動，機關應先建立離線備份機制，定期進行備援與復原演練，以確保系統遭破壞時仍能維持最小服務水準。其次，應強化異常行為偵測與應變能力，建立對應入侵指標，以即時掌握威脅跡象。同時，應加強端點防護、採用零信任架構、妥適規劃網路區隔並限制存取權限，透過多層次防護措施，提升整體防禦效能，應對持續演化的威脅情勢。

四、資安（訊）供應鏈加劇數位生態系統風險

根據資安廠商 BlueVoyant 發表 2025 年供應鏈防禦現狀報告（The State of Supply Chain Defense: Annual Global Insights Report 2025）指出，供應鏈資安事件對組織已造成幾近全面性衝擊，即便成熟市場投入較多強化防禦資源，仍因駭客手法持續演進，攻擊頻率居高不下。同時，96%組織預期未來一年供應商生態系將持續成長，意味全球第三方服務或供應鏈環境規模不斷擴張，攻擊面亦隨之增加，若缺乏風險分級機制、工具整合及跨部門協作流程，供應商關係將成為新的資安脆弱點，主要挑戰包括供應鏈持續擴張導致管理效能不足、缺乏治理機制、資源分配不當，以及未落實動態風險監控與整體供應鏈管理。

另外，根據 ENISA 2025 年威脅情勢報告指出，數位依賴濫用（Abuse of Cyber Dependencies）現象明顯加劇，攻擊者透過入侵開源程式庫、植入惡意瀏覽器擴充功能及滲透服務供應商，將風險擴散至整個互聯數

位生態系統。此類攻擊利用信任供應鏈展開橫向攻擊，僅需單一節點入侵成功，就能引起整體供應鏈連鎖衝擊，形成系統性風險。

駭客針對 Salesloft 的 AI 聊天機器人與行銷自動化服務（Drift）展開攻擊，進而竊取大量身分驗證令牌（OAuth Token），再利用該等令牌以合法身分登入多家企業雲端客戶關係管理平台（Salesforce）系統。駭客進一步搜尋未加密敏感資訊或明碼憑證，藉此橫向擴散至其他雲端環境或內部系統。駭客於操作完成後會刪除查詢與匯出紀錄，並透過 Tor 瀏覽器或雲端代理服務隱匿來源與行為軌跡，以降低被偵測與追查風險。

對於 OAuth 供應鏈攻擊事件，防護核心應著重於第三方 SaaS 整合安全控管，確認所有內部與外部服務所使用 OAuth Token 有效性，包含有效期限、授權範圍及使用狀態，並落實 Token 輪替與最小化權限原則，避免長期有效或過度授權憑證成為攻擊者濫用入侵管道。同時，於雲端服務平台建立對 API 行為即時監控，以便快速識別資料外洩風險。最後，應訂定明確管理規範，對於雲端存取或儲存機敏資訊採加密保護，以降低外洩後被用於橫向擴散攻擊之可能性。

五、資通系統弱點頻遭利用

根據資安廠商 Fortinet 2025 年全球威脅態勢報告（2025 Global Threat Landscape Report）指出，全球自動化網路掃描活動正急遽攀升

，2024 年全球網路掃描數量創新高，較前一年增長 16.7%，每秒達 3 萬多次掃描行為，駭客廣泛利用開源與商用掃描工具來擴大偵察範圍，以識別可被利用的脆弱目標，主要鎖定暴露於網際網路服務與通訊協定，包含 SIP、RDP 及 OT/IoT 等，顯示駭客積極於系統漏洞修補前，先行迅速鎖定目標並制定攻擊計畫。

網路安全業者 Forescout 發表研究報告指出，全球六大太陽能變流器廠商，其中三家所製造設備存在數十個系統漏洞，對電網服務穩定性與使用者隱私可能造成嚴重影響。這些漏洞包含不安全 API 致未經授權存取、Web 應用程式存在跨站腳本（Cross-site scripting, XSS）漏洞、授權控管失效漏洞、雲端 Web 應用程式因檔案上傳機制不受限制致使遠端程式碼（Remote Code Execution, RCE）執行，以及未經身分驗證的無線韌體更新導致 RCE 與設備遭控制等。依據報告揭露太陽能發電系統元件，如儲能與監控系統大部分為中國製造，其次為印度，再者為美國，因中國於太陽能供應鏈具主導地位，意味全球市場對中國製造依賴度極高，在現今地緣政治緊張或貿易限制情況下，可能發生供應鏈脆弱性議題。

建議於建置與維運 IT 與 OT 生命週期時，需將安全需求納入採購考量，評估設備製造商資安成熟度等級，於部署設備時進行風險評估與弱點掃描，並落實網路區隔措施，以確保系統整體安全防護。

六、雲端應用衍生多元威脅

根據資安廠商 Orca Security 發表 2025 年雲端安全狀況報告（2025 State of Cloud Security Report）指出，隨著組織擴大採用雲端服務，全球雲端應用市場依然高度集中於三大雲端服務供應商，且多雲部署架構發展亦明顯成長，報告統計 55%組織使用兩個以上雲端服務供應商。研究顯示組織逐漸採用多雲應用服務主要原因包含希望利用不同雲端供應商於特定領域技術（如 AI 相關服務）優勢，並基於安全與服務韌性考量，降低單點失效及單一供應商依賴風險。

該報告亦提及多項雲端應用統計調查風險，其中 76%組織至少有一項對外公開雲端資源，此類資源一旦遭入侵，可能遭利用進行橫向移動；13%組織至少存在一項雲端資源資安缺陷，如組態設定錯誤、弱點暴露、不當授權控管或資源間缺乏區隔，衍生可被駭客利用攻擊路徑；38%組織於資料庫存放敏感資料，且資料庫暴露於公開環境，以及 85%組織將敏感憑證以明文形式存放於原始碼程式庫。

Cloudflare 於 114 年 11 月與 12 月分別發生兩次重大可用性事件，導致全球網路流量受干擾。其中 11 月事件為該公司近年最嚴重的中斷服務事件，起因於例行資料庫權限更新，機器人管理（Bot Management）系統生成過大設定檔，超出系統限制，造成流量於路由過程中崩潰，由於此

資料庫存取控制變更，引發全球性連鎖影響，導致許多網站與平台近 6 小時無法連線。12 月事件則因修復 React2Shell 漏洞而引發組態配置錯誤，導致代理伺服器無法正常處理請求，部分流量出現延遲或中斷情形。

Cloudflare 事件喚起組織應重點盤點並重視單點失效風險，特別是關鍵服務仰賴於單一服務供應商時，更應審慎評估其潛在影響，並預先建置因應方案，以強化監督管理、提升供應鏈韌性及完善備援機制。除避免將關鍵服務完全仰賴單一服務供應商外，亦可評估採用多雲或具快速切換備援架構。同時，應強化對第三方雲端服務監督管理，包含即時監控服務狀態、要求落實契約變更管理與事件通報責任，並透過供應鏈中斷情境演練，提升整體應變機制。

參、114 年政府資安威脅統計

一、聯防預警情資

資安聯防監控旨在蒐集政府領域各類威脅情資，透過資安聯防與情資分享機制，分析不同威脅類型及相關數據指標，如情資數量、攻擊跳板來源與國別分布等，並結合跨領域及各廠商所蒐集情資，評估監控效度，強化彼此間溝通協作，以促進國家資安聯防體系整體運作。

統計 114 年資安監控情資，依資安威脅類型區分為惡意內容、惡意程式、資訊蒐集、入侵嘗試、入侵攻擊、服務阻斷、資訊內容安全、詐欺攻擊及系統弱點等 9 類，資安威脅類型排名第 1 名為資訊蒐集（36.5%），主要係透過掃描、探測及社交工程等攻擊手法取得資訊；第 2 名為入侵攻擊（27.8%），大多為系統遭未經授權存取或取得系統/使用者權限；而第 3 名為入侵嘗試(19.8%)，主要係嘗試入侵未經授權的主機，各類資安威脅分布詳見圖 2。

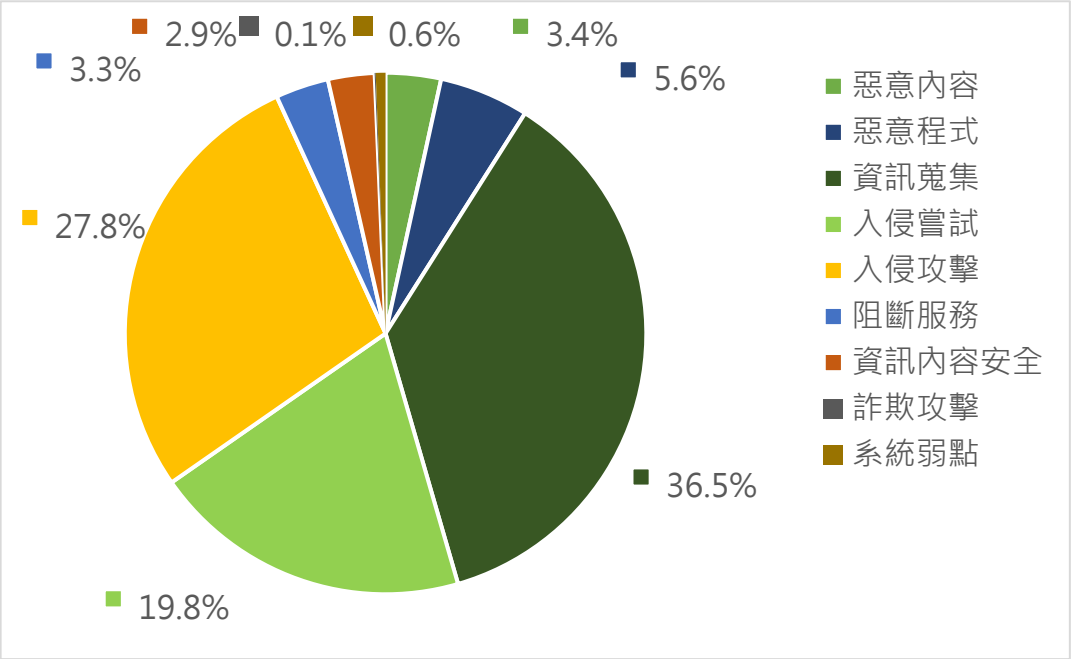

圖 2　各類資安威脅分布圖

另分析整體資安監控情資攻擊跳板來源 IP，國外來源 IP 高於國內來源 IP，比例約為 60%與 40%，顯示 GSN 主要遭受來自國外網路攻擊，各月國內外威脅跳板來源 IP 比例詳見圖 3。

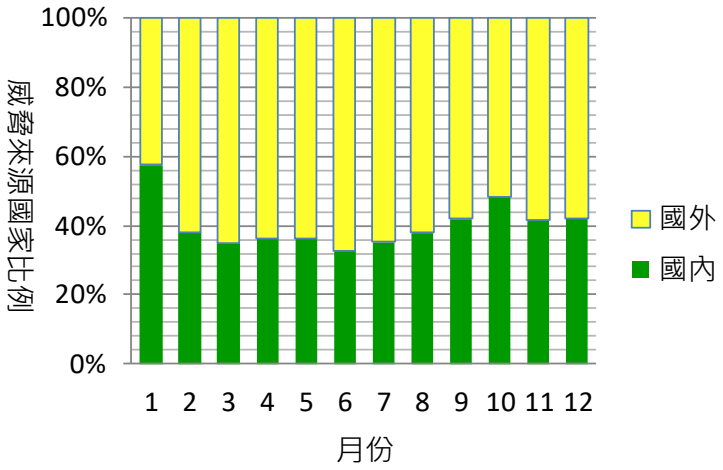

圖 3　114 年國內外攻擊跳板來源比例

細部分析國外攻擊跳板來源，前 3 名分別為美國（52%）、荷蘭（11%）及日本（6%），其他攻擊跳板來源國家眾多，未列入前 5 大攻擊跳板來源國家共占 21%，國外攻擊跳板來源資訊詳見圖 4。

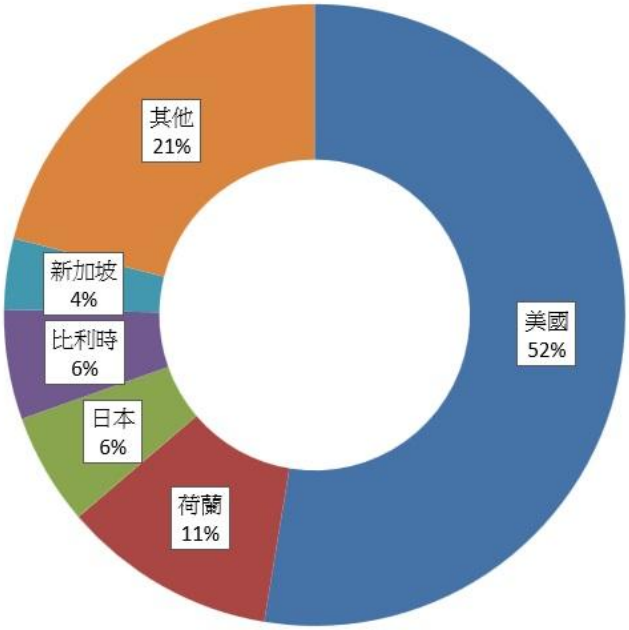

圖 4　114 年國外攻擊跳板來源國家比例

前 5 大國外攻擊跳板來源國家威脅類型，主要為「外對內防火牆大量阻擋」、「外部主機執行掃描探測攻擊」及「外部主機對內進行遠端維運工具連線」。根據過往情資，美國持續為主要攻擊跳板來源國家，建議機關加強監控相關攻擊跳板來源，並持續注意國外攻擊跳板來源國家之威脅。

二、惡意電子郵件分析

惡意電子郵件一直是政府機關主要資安威脅來源之一，114 年共檢測 1 億餘（109,590,054）封電子郵件，蒐集相關資訊進行分析，發現可疑惡意電子郵件 148 萬餘（1,489,180）封，約占整體 1.36%，每月惡意電子郵件偵測數量統計，詳見圖 5。114 年 3 月、6 月及 12 月偵測到大量詐騙釣魚郵件散布活動，經分析發現，駭客聲稱已入侵電腦裝置並監控網路活動為由，勒索使用者支付比特幣。

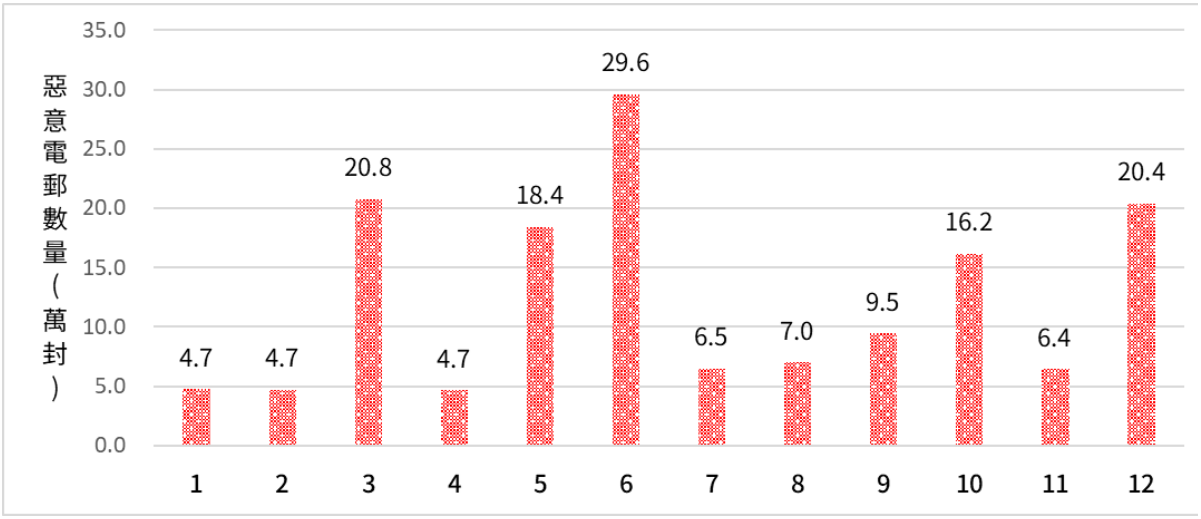

圖 5　114 年政府骨幹每月惡意電子郵件偵測數量

整體惡意電子郵件風險分布差異，詳見圖 6，中低風險共占 98.23%，為惡意電子郵件內嵌可疑連結經威脅情資比對或附檔經防毒軟體靜態掃描，具有已知惡意樣態或特徵；高風險占比為 1.77%，需透過虛擬沙箱自動化動態分析評估，偵測惡意電子郵件附檔具有已知 CVE 漏洞利用或存在進階威脅行為。

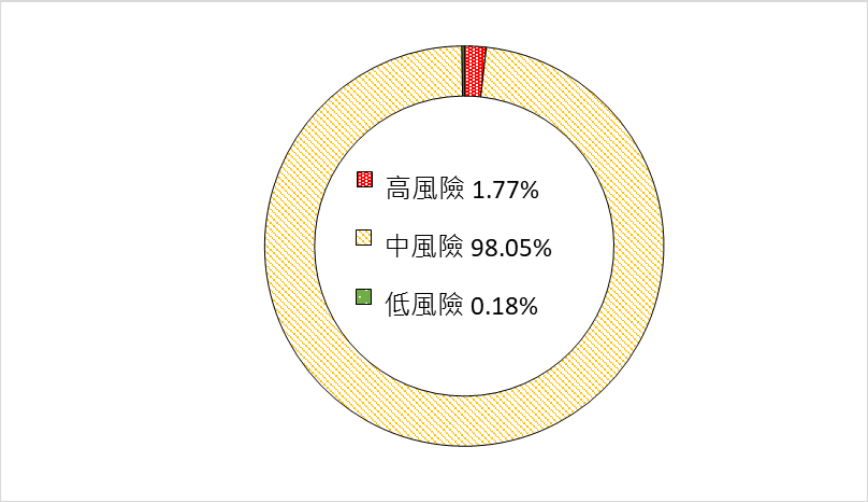

圖 6　惡意電子郵件風險分布比例

綜整 114 年政府進階持續性威脅（Advanced Persistent Threat, APT）惡意電子郵件攻擊手法，可歸納為五波攻擊行動，第一波攻擊手法著重於前期偵查，駭客透過偵查電子郵件確認目標帳號有效性，隨後利用 LNK 捷徑檔結合合法系統工具（如 PowerShell）下載並執行惡意程式；第二波攻擊，駭客改以受駭之合法電子郵件帳號搭配業務與內部公告為主旨寄送惡意電郵，同時部署多種惡意程式以提升攻擊成功率，其中亦發現新興惡意程式藉由雲端服務 API 回傳受駭主機資訊，並將合法雲端服務作為中繼通道，以降低惡意流量遭偵測機率；接續第三波攻擊則以志工招募為由夾帶惡意附件之社交工程郵件為主要手法，駭客誘使收件人執行附檔後植入 Python 後門程式，最終與中繼站建立連線，以達成指令接收與資料回傳目的；第四波攻擊中，駭客透過多層規避與隱蔽技術，包含通行碼以圖片形式呈現、以壓縮檔包裝惡意內容、透過捷徑檔觸發複合式執

行流程，並利用 DLL 側載函式庫（DLL Sideloading）手法載入惡意程式（Cobalt Strike），成功與中繼站建立連線並完成後門部署；駭客於最後一波攻擊改以合法雲端服務作為惡意檔案散布管道，透過寄送含下載連結之社交工程郵件誘使目標下載並執行檔案，成功入侵後植入後門程式，以規避資安防護機制檢測。整體而言，攻擊手法由單一入侵逐步演進為多階段、跨工具與高度隱匿之攻擊鏈，顯示 APT 郵件攻擊策略持續朝向系統化與防偵測能力強化方向發展。

114 年政府領域社交工程郵件攻擊趨勢，共偵測 93 萬餘（933,737）封社交工程釣魚郵件，經分析發現，駭客濫用各式網際網路應用服務蒐集電子郵件帳號資料，如第三方免費架站服務、線上表單服務、星際檔案系統（InterPlanetary File System, IPFS）之分散式架構及合法網站轉址功能等，並透過架設偽冒政府機關所使用郵件服務登入頁面，如微軟 Outlook 與 HiNet 郵件服務，搭配釣魚郵件誘騙收件人輸入帳號與通行碼以取得機敏資訊。

此外，114 年共偵測 84 萬餘（841,554）封惡意程式垃圾郵件，經分析發現，駭客主要仍以壓縮檔、微軟 Office 文件及 HTML 檔案等作為惡意電子郵件附檔，附檔內藏惡意程式或轉導至惡意網址下載惡意檔案，進而在收件人主機安裝後門程式並執行攻擊活動。短網址服務（如

Rebrandly 與 T.LY）與雲端硬碟空間（如 Google、CatBox 雲端硬碟）等第三方服務常被駭客做為惡意程式下載的轉址與儲存媒介，藉此散布惡意檔案，降低被防護機制偵測風險；第三方電子郵件服務（如 Google mail），亦常用來寄送內含惡意附檔社交工程電子郵件。其次，近年來惡意程式垃圾郵件會利用確認通知做為誘餌，如以「產品訂單」、「確認付款」及「麻煩協助確認」等通知為主旨，並透過夾帶程式 PIF（Program Information File, PIF）資訊檔，利用 PIF 隱藏副檔名特性，誘使收件者誤認為一般文件，以提升開啟附件並連線惡意中繼站成功率；此類惡意垃圾郵件亦會使用通行碼保護惡意壓縮檔，企圖繞過防毒軟體，並誘使目標收件人開啟惡意附件以達竊取電腦敏感資料目的。此外，114 年 6 月發現駭客以業務相關報價名義，散布 Remcos RAT 等惡意程式，其主要提供攻擊者對受感染系統的遠端控制能力，包含監控使用者活動、蒐集系統及使用者資訊，此類惡意垃圾郵件以罕見副檔名.ARJ 作為附檔，並將檔名偽裝為常見文件格式（如.pdf），藉由其罕見性以規避傳統垃圾郵件與防毒引擎偵測機制。

114 年惡意程式垃圾郵件主要惡意程式族群分布，詳見圖 7。其中，以散布漏洞利用為大宗，占整體惡意程式 70.48%。CVE-2017-11882 與 CVE-2017-0199 為微軟 Office 系列遠端執行漏洞，因適用平台廣泛且容

易被觸發，故自 106 年發現至今仍為駭客最常利用漏洞之一，同時名列美國網際安全暨基礎設施安全局（CISA）公布最常被利用漏洞，其餘偵測發現惡意程式族群依序為 AgentTesla 遠端木馬、Nemucod 勒索軟體及 Formbook 後門木馬等。

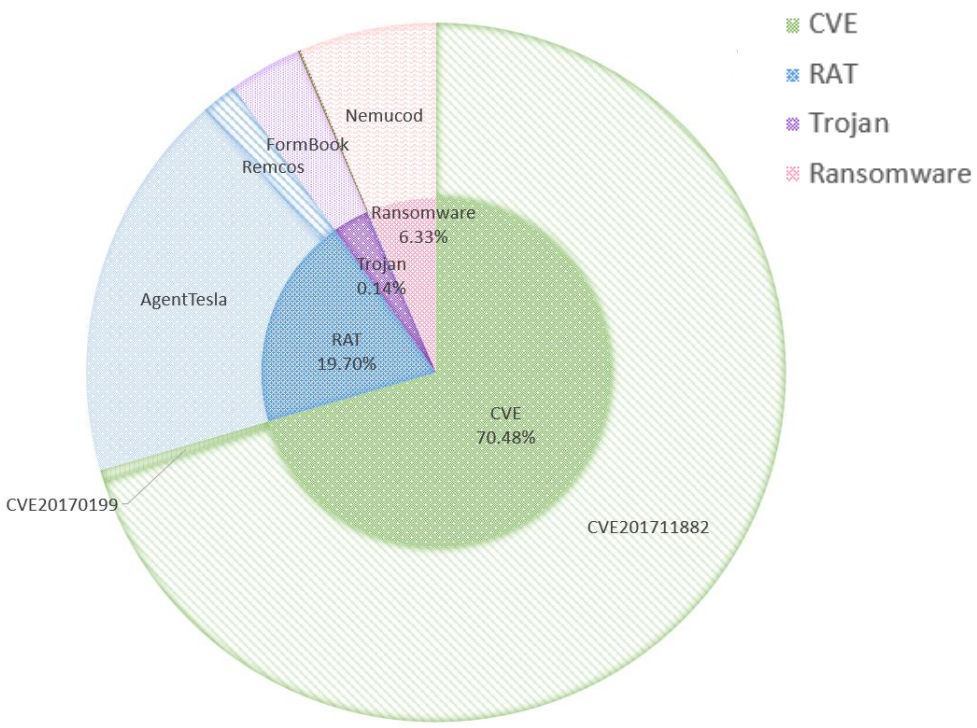

圖 7　主要惡意程式族群分布比例

三、資安攻防演練

為提升政府機關資安防禦及應變能力，114 年持續以「資通系統實兵演練」及「社交工程演練」兩類演練方式並行，並透過官學研界合作，以公私協力方式，使用滲透測試手法檢測公務機關對外資通系統潛在脆弱點，協助機關持續強化對外服務之安全防護措施及應變能力；同時以社交

工程方式檢視各演練機關資安意識及警覺性，藉以促進各級機關落實資安防護作為。114 年計 71 個機關、資安責任等級 A 級之關鍵基礎設施提供者及資安法納管之公務機關參與資安攻防演練，結果說明如下：

（一）資通系統實兵演練

以弱點掃描或滲透測試等方式進行，模擬駭客攻擊手法，嘗試由遠端取得機關內部機敏資料或資通系統控制權限等，實際攻擊機關之系統與網路，檢測出現存之系統漏洞後，並模擬駭客嘗試入侵，藉以測試機關資安事件發生時之偵測及通報應變能力。

114 年度網路攻防演練計有 71 個機關 3,823 個對外系統（不含 CIP），演練結果發現 39 個機關對外資通系統存在弱點，占演練機關總數 54.93%。

針對機關存在資通系統弱點，依若遭受攻擊產生之衝擊性，區分為重大衝擊性、高衝擊性、中衝擊性及低衝擊性 4 種弱點類型。114 年度網路攻防演練共發現 441 個弱點，其中重大衝擊性弱點數量 20 個，占整體弱點數量 4.54%；高衝擊性弱點數量 66 個，占整體弱點數量 14.97%；中衝擊性弱點數量 15 個，占整體弱點數量 3.4%；低衝擊性弱點數量 340 個，占整體弱點數量 77.1%。

（二） 社交工程演練結果

透過社交工程演練(電子郵件與簡訊方式)測試機關人員資安意識與警覺性。測試接收行為區分為「開啓郵件」、「點閱郵件附件或連結」及「點閱簡訊連結」等 3 種。

114 年電子郵件演練 71 個機關，受測計有 2 萬 259 個郵件帳號，30 個機關開啟郵件，占演練機關數量 42.25%；28 個機關點閱連結/附件，占演練機關數量 39.44%，郵件開啟率為 1.7%，郵件附件/連結點擊率 1.31%；簡訊演練 70 個機關，有 25 個機關點閱簡訊連結，占演練機關數量 35.71%，簡訊點擊率為 4.16%。

114 年社交工程演練結果，經過歷年演練與宣導，多數機關人員對於社交郵件已有基本資安意識，惟對於簡訊則相較缺乏警覺性。從結果顯示仍有部分機關人員社交工程防範意識需強化，尤其針對釣魚簡訊應加強宣導，並提醒社交工程途徑非僅限於電子郵件。

四、資安稽核作業

依據資安法及其子法、國家資通安全發展方案、資訊安全管理系統（ISMS）、受稽機關資通安全維護計畫及實施情形等，規劃資安稽核項目，並採取實地檢視方式，以協助政府機關了解其資安防護之完整性與有效性。

114 年遴選 40 個受稽機關，包含 20 個公務機關及 20 個特定非公務機關執行資安稽核作業，稽核小組由稽核領隊、稽核委員、 觀察員、工作人員、技術檢測人員及觀摩人員組成。

受稽核公務機關之資通安全責任等級如為 A 級，於實地稽核前先行辦理技術檢測，其他機關直接進行實地稽核。實地稽核分為策略面、管理面及技術面 3 個構面，如有維運工控系統或運營科技（OT）之機關，額外辦理 OT 實地稽核，就管理面及技術面 2 個構面由稽核委員進行實地訪談查證。

技術檢測機關共 9 個，8 個檢測項目之平均分數經標準化後，檢視個別項目得分情形，其中「網域主機安全防護檢測」、「資料庫安全檢測」、「網路惡意活動檢視」等 3 個項目表現較佳，各項目得分情形詳見圖 8。

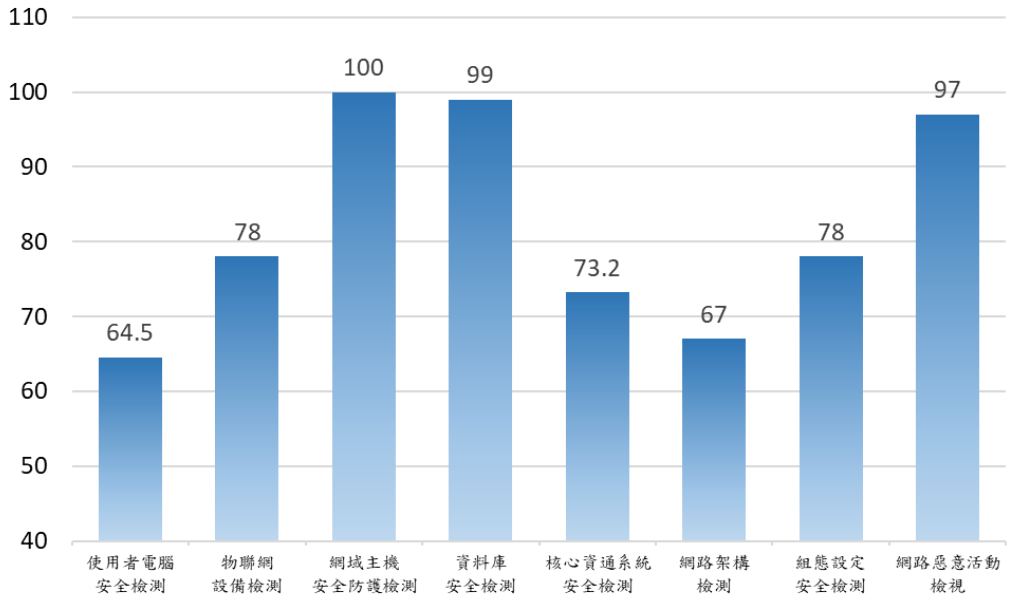

圖 8　技術檢測各項目得分情形

實地稽核 9 個項目之平均得分經標準化後，檢視個別項目得分情形，其中「專責人力及經費配置」得分最高，「資通安全政策及推動組織」次之，各項目得分情形詳見圖 9。

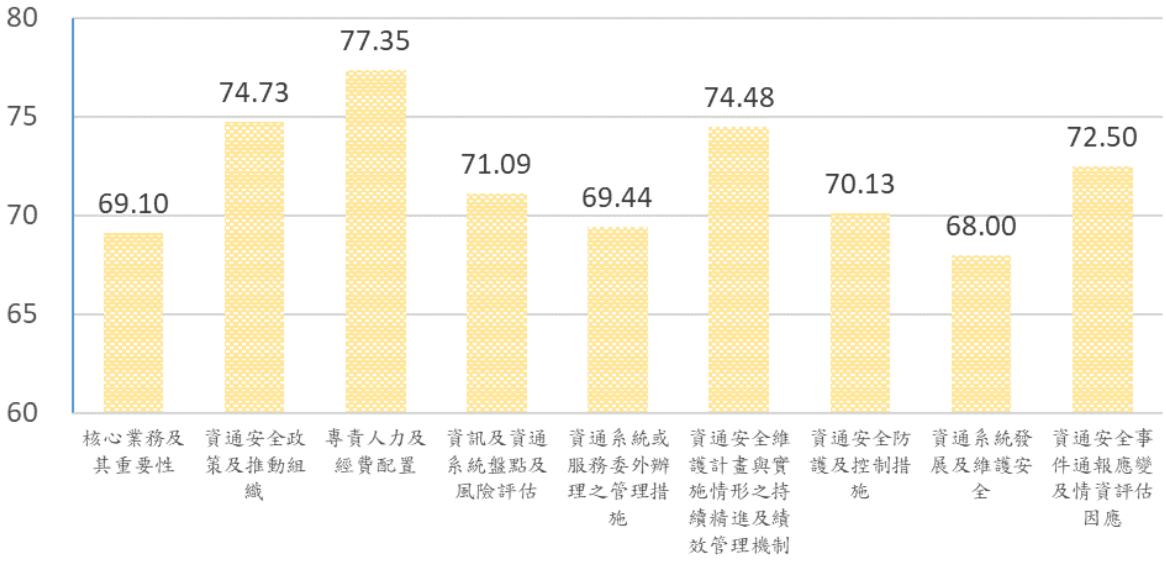

圖 9　實地稽核各項目得分情形

綜合分析實地稽核各構面表現情形，詳見圖 10，自策略面、管理面及技術面 3 個構面檢視，整體表現尚屬平均，其中「技術面」表現與其他構面稍有落差。

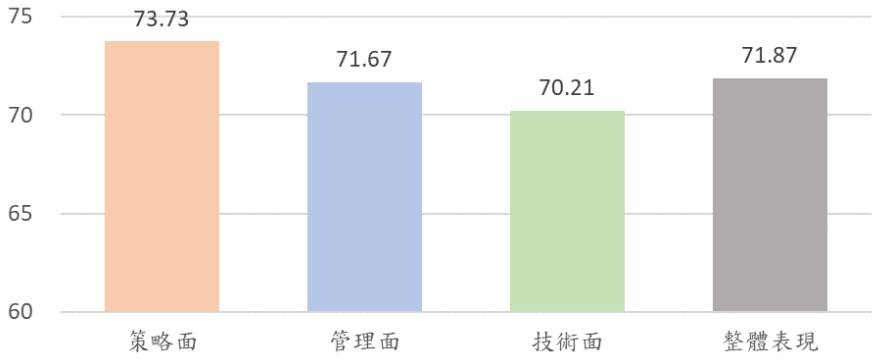

圖 10　實地稽核各構面成績分布圖

五、資安事件通報

分析 114 年公務機關通報事件，以機關收到資安警訊後，再行通報之警訊通報為主，占所有通報事件 72.89%，顯示協助整體資安偵測防護重要性，彙整通報比例資訊詳見圖 11。

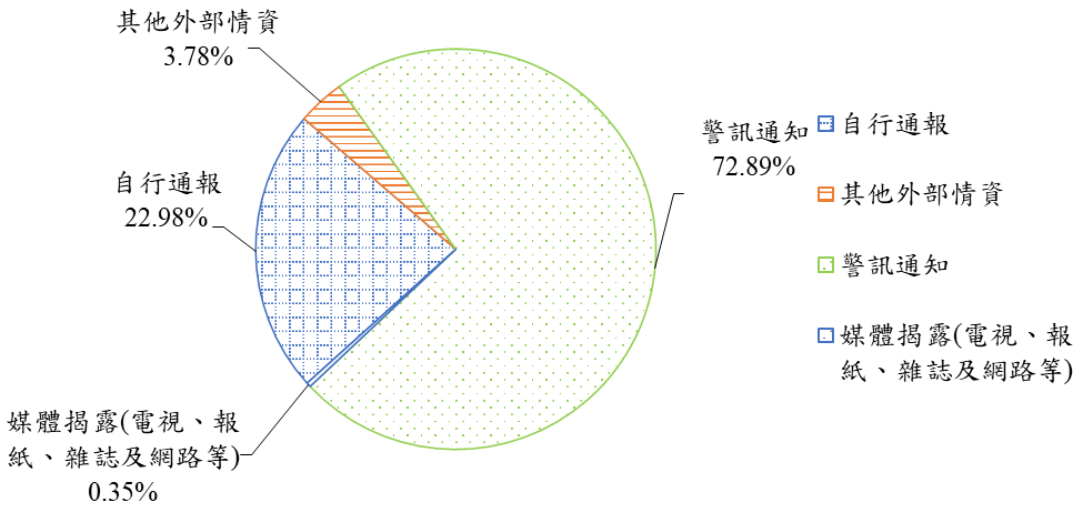

圖 11　114 年警訊通報占總通報件數比例

機關依資通安全事件通報應變及演練辦法規定，依事件機密性、完整性及可用性衝擊嚴重程度，由輕至重區分為「1 級」、「2 級」、「3 級」及「4 級」。統計 114 年機關通報資安事件，以 1 級資安事件為大宗占 85.48%，2 級資安事件居次占 9.86%，3 級資安事件占 4.66%，無發生 4 級資安事件，資安事件等級比例詳見圖 12。

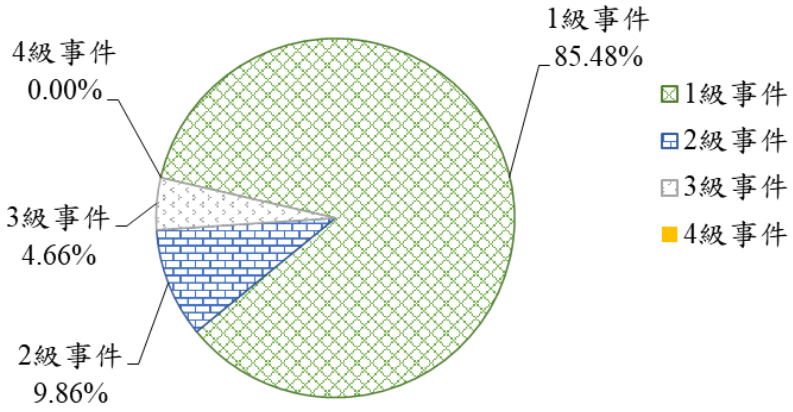

圖 12　114 年資安事件等級比例

分析所接獲資安事件類別，排除「其他」類型後，以非法入侵事件居多占 57.13%，其次為網頁攻擊占 12.85%、設備問題占 9.68%及阻斷服務占 3.17%，各資安事件類型比例，詳見圖 13。

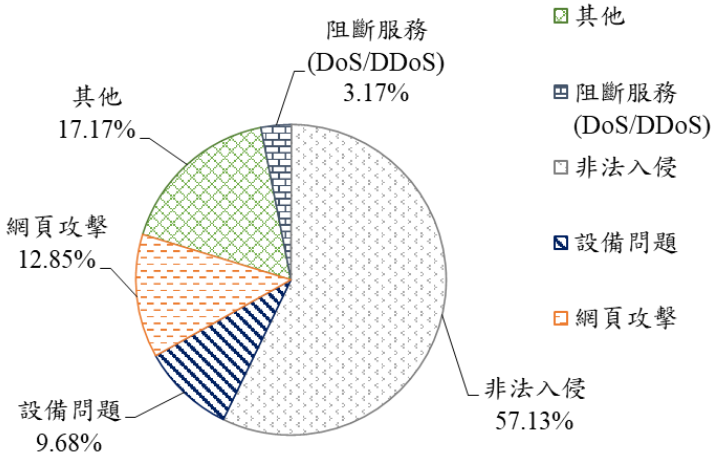

圖 13　114 年資安事件類型比例

上述資安事件類型中，針對非法入侵、設備問題、網頁攻擊分析發生原因，排除「其他」與無法確認事件原因後，以網站設計不當最高占 15.69%，多數機關因網站存在注入攻擊、無效的存取控管或加密機制失效等弱點，遭實兵演練攻擊成功，執行惡意腳本或取得非公開資料；其次為使用/下載來源不明之應用程式/套件占 11.30%，多為機關人員誤至非官方網站下載偽冒安裝程式，導致電腦遭植入後門程式，詳見圖 14。

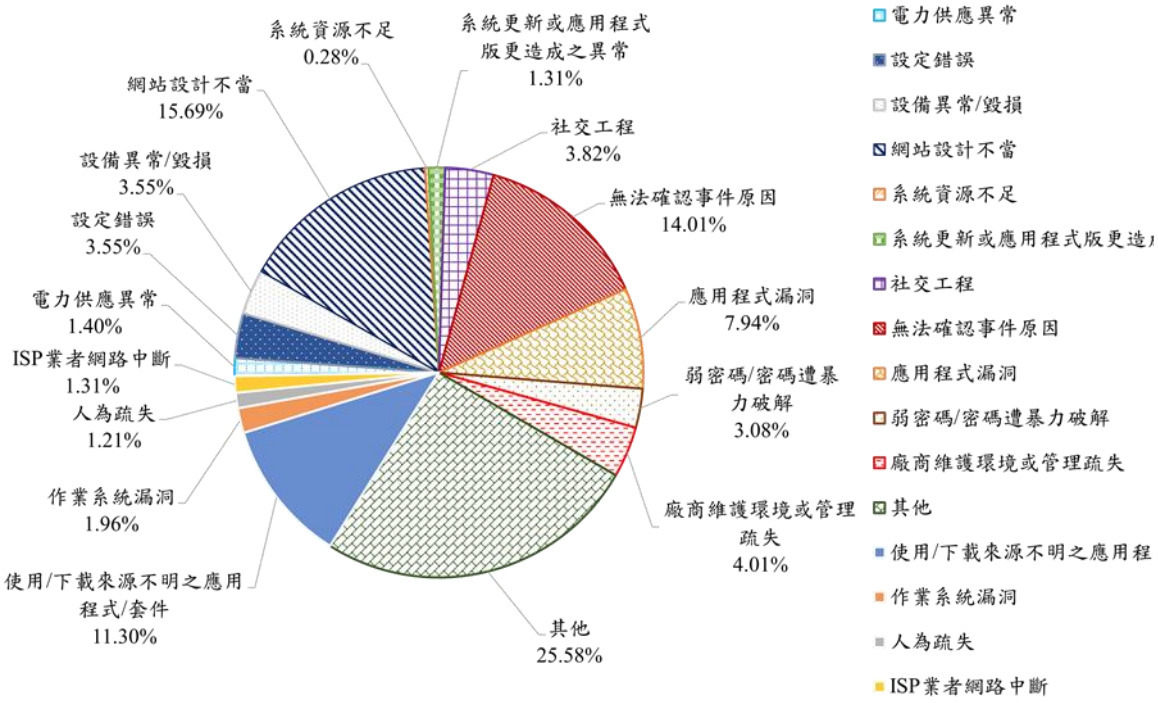

圖 14　114 年資安事件發生原因比例

肆、政府資通安全威脅情勢與防護建議

根據資安威脅情勢與 114 年政府機關資安事件通報案例，分析駭客入侵常用手法，研提「網路釣魚手法日益詭譎，機關未查證誤安裝偽冒即時通訊程式」、「勒索團體以自帶驅動程式手法入侵並迴避偵測」、「供應鏈管控疏漏，系統維護廠商於網站主機上安裝遠端桌面軟體，遭駭客暴力破解密碼登入機關網站」、「網路邊緣設備存在漏洞或組態設定風險，導致發生惡意連線行為」及「社交工程攻擊並結合雲端服務濫用，導致資料外洩風險」等 5 個政府機關資安事件案例與相對應防護建議，提供機關檢視相關防護措施完備度。

一、網路釣魚手法日益詭譎，機關未查證誤安裝偽冒即時通訊程式

自 114 年初起，陸續偵測到多個機關資訊設備疑似安裝冒牌軟體，產生 Gh0st RAT 惡意程式連線，經機關調查，多為使用者在設備汰換或取得新電腦時，透過搜尋引擎查找通訊軟體(Line)時不慎自非官方網站下載偽冒通訊軟體，導致電腦遭植入後門程式。針對此類案件資安防護建議如下：

(一) 建立資通系統變更管理與下載控管機制，要求軟硬體及應用程式安裝須申請與審核，並以最小權限及白名單等機制，限制未經授權操作與降低潛在風險。

(二) 強化端點防護與檢測機制，藉由部署防毒軟體與 EDR 系統，偵測並阻

擋惡意程式。同時，啟用檔案完整性檢查，防止偽冒安裝檔載入後門程式。

（三）建立異常連線監控機制，並制定事件通報與隔離流程，確保迅速處理受駭設備。

二、勒索團體以自帶驅動程式手法入侵並迴避偵測

某機關發現多台主機遭勒索軟體加密，經研判攻擊者透過網站漏洞對主機植入後門程式，並搭配自帶驅動程式(Bring Your Own Vulnerable Driver, BYOVD）手法，利用具漏洞驅動程式終止防毒軟體與 EDR 處理程序，以規避資安防護偵測機制，再橫向移動至其他主機部署勒索軟體，導致多台伺服器與電腦受駭。針對此類案件資安防護建議如下：

（一）定期執行網站漏洞掃描與修補，同時導入 Web 應用防火牆，阻擋惡意請求。

（二）建立驅動程式安裝審核機制，禁止使用未經驗證或具漏洞之驅動程式，部署 BYOVD 攻擊偵測工具，以監控驅動程式異常行為。

（三）建立端點防護持續運作機制，啟用防毒軟體與 EDR 自我防護功能，定期更新防護產品與威脅偵測規則，確保防毒軟體及 EDR 防護功能持續有效，避免異常終止與安全規則失效風險。

三、供應鏈管控疏漏，系統維護廠商於網站主機上安裝遠端桌面軟體，遭駭客暴力破解密碼登入機關網站

機關系統維護廠商為方便維護管理作業，於主機上安裝遠端桌面軟

體（AnyDesk），惟未搭配防火牆白名單及存取限制等控管機制，導致攻擊者透過 AnyDesk 遠端連線主機，破解密碼登入後，再透過遠端桌面通訊協定（RDP）橫向滲透至其他主機，導致多台設備受駭。針對此類案件資安防護建議如下：

（一）訂定供應商安全管理規範，如存取權限控管、資料保護措施、漏洞管理流程及事件通報等規範，並定期執行資安稽核與合規檢查。

（二）強化遠端存取安全控管機制，禁止未經授權遠端桌面軟體，並建立申請與審核流程，維護連線白名單與 IP 存取限制。

（三）部署入侵偵測系統與行為分析，設定異常登入警示及定期檢視存取日誌，以即時監控異常遠端連線。

四、網路邊緣設備存在漏洞或組態設定風險，導致發生惡意連線行為

政府機關工控設備控制登入頁面公開暴露於網際網路，且缺乏存取限制機制，亦未變更預設登入密碼，導致設備遭入侵成功，並建立對外連線至殭屍網路（Botnet）事件。

其他案例包含網路邊緣設備存在未修補漏洞而遭入侵，如監視或網路設備未即時更新韌體與安全修補程式，遭駭客成功入侵並下載惡意腳本。針對此類案件資安防護建議如下：

（一）工控設備控制頁面設定為僅允許內網或 VPN 存取，對外連線採用白名單策略，封鎖非必要通訊埠。將 IT 與 OT 網段分離，並對敏感區域

採取嚴謹存取控管，以降低入侵後橫向移動風險。

（二）強制變更預設帳號與密碼，並採用零信任或多因子驗證。定期檢視設備設定與存取紀錄，以及時發現異常行為。

（三）定期盤點網路邊緣設備型號與韌體版本，建立持續性更新與驗證流程，確保漏洞及時修補。

五、社交工程攻擊並結合雲端服務濫用，導致資料外洩風險

駭客偽冒政府機關名義，對政府機關與民間企業發動社交工程電子郵件攻擊，並針對具財務敏感資訊存取權限人員，以要求查看報告為由，誘導收件者開啟並點擊 PDF 附檔，經檢視附檔夾帶雲端硬碟下載惡意連結，駭客將惡意檔案置於雲端硬碟，藉由濫用雲端服務來降低基礎設施維護成本，並達到規避防護設備偵測機制目的。

其他雲端安全管理案例，機關承辦人員於辦理活動期間，將活動簡章存放於雲端硬碟供民眾下載，惟承攬廠商亦將包含個人資料報名者資訊上傳至該雲端硬碟，且未妥適設定存取權限，導致民眾個人資料外洩。針對此類案件資安防護建議如下：

（一）導入電子郵件過濾與沙箱檢測機制，攔截惡意附件與連結。限制雲端硬碟共享權限，並啟用檔案上傳掃描機制，對雲端連結進行安全檢測，以避免惡意檔案散布。

（二）定期辦理使用者教育訓練，說明多樣化社交工程手法，分享常見攻擊

樣態、惡意連結及檔案指標（如雜湊值、檔名、檔案型態或行為特徵等），輔以定期社交工程演練，以提升資安防範意識。

（三）規範雲端服務使用流程，限制僅使用經核可雲端平台，並落實最小權限原則。針對敏感資料要求加密管理，並設定檔案存取權限與共享屆期失效機制。

伍、結語

綜觀全球資安情勢，攻擊者已廣泛運用 AI、自動化掃描與弱點偵測技術，結合釣魚郵件與社交工程手法，對政府機關及關鍵基礎設施發動持續性滲透攻擊，且在地緣政治風險升高下，國家級 APT 威脅更形嚴峻。為此，政府除強化情資蒐整與跨域聯防外，已公布並施行人工智慧基本法，並研擬公部門 AI 應用參考手冊，明確規範 AI 導入生命週期之風險評估、治理架構與維運管理。另配合修正資安法，從法遵面要求禁用危害國家資通安全產品，並強化供應鏈安全查核機制，擴大第三方稽核範圍與技術面合規要求。在技術防護上，推動弱點通報與盤點制度，優先修補高風險漏洞，並強化雲端資產辨識、權限控管與行為監測；同時，持續優化 GCB 設定與社交工程訓練教材，結合人才培育與國際情資合作，全面提升威脅偵測、事件應變與整體資安韌性。