113年度國家資通安全情勢報告

數位發展部

中華民國114年4月

目次

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5條規定，定期公布「國家資通安全情勢報告」。

隨著各種新興科技技術蓬勃發展，衍生對應的資安威脅與挑戰也日益增長，各界須持續加強資安整體防護及提升應變與處理之效率，方能扼止衝擊擴散。本報告透由研析113年全球資通安全威脅情勢及我國政府機關所面臨之資通安全威脅現況，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，以期強化國家整體之資安防護韌性，維持服務可用性，並打造永續經營之數位國家。

貳、113年全球資安威脅情勢概要

世界經濟論壇(World Economic Forum, WEF)於「全球114年風險報告」(Global Risks Report 2025)中指出，可能引發全球重大危機之前5大風險分別為「國家武裝衝突」、「極端氣候」、「地緣經濟衝突」、「錯誤訊息與虛假訊息」及「社會兩極化」；在2年內可能最嚴重的風險排序中，「錯誤訊息與虛假訊息」及「網路間諜活動與戰爭」亦分占第1名及第5名，在10年內可能最嚴重的風險「錯誤訊息與虛假訊息」亦占第5名，「AI技術所引起之不良後果」占第6名，為上升幅度最大風險之一。

AI技術之快速成長，衍生利用生成式AI創造虛假或誤導性內容之風險為首要關注之問題，若依年齡組別統計當前全球風險，發現各年齡層對於錯誤訊息與虛假訊息之排名皆在前5名內，因此可證明此風險幾乎影響所有年齡層。再從利害關係人群組統計，政府、私人產業及學術等領域皆將錯誤訊息與虛假訊息列為最高風險等級，表示這些領域被視為最有可能成為受害或濫用之目標對象。

因應地緣政治關係，網路間諜活動與戰爭之攻擊持續上升，錯

誤訊息與虛假訊息等惡意活動頻傳，除造成民眾信任感降低、社會不安，更可能造成國家動盪，故應積極從法規、管理及技術等不同層面分析情勢發展，及 AI 應用可能之風險。從法規或管理規範上，限制風險性較高之 AI 服務應用下載或使用，從管理規範發展實作之指引，規範機敏資訊不可上傳，或針對 AI 產出成果仍需經人工判斷其真確性；技術上針對 AI 提供實習場域，測試監管機制之可行，以持續提升資安防護韌性。

分析與綜整113年全球重大網路攻擊事件，詳見圖1。

資料來源：國家資通安全研究院整理

圖1　113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)、Gartner 研究報告及各資安業者調查等報告資料，113年全球資安威脅情勢可歸納為6大面向，包含「駭客利用 AI 技術發展新型態入侵與惡意詐騙」、「個人資料與

憑證外洩致防護機制失效」、「社交工程泛濫致 APT 攻擊與勒索軟體風險增加」、「資安(訊)供應商遭駭致破壞供應鏈安全」、「資通系統弱點頻遭揭露利用」及「雲端應用服務衍生多元威脅」。

一、 駭客利用 AI 技術發展新型態入侵與惡意詐騙

依據 Gartner 預測，AI 軟體市場產值將從111年的1,240億美元以複合成長速度到116年的2,979 億美元，AI 商機成長快速，預計將吸引更多廠商投入 AI 軟體供應鏈行列，如未於設計或維運時將資訊安全納入預設原則，或為提升上市時效，犧牲部分安控措施，將成為資安隱憂。

Google Cloud 團隊發表之 Cybersecurity Forecast 2024指出，生成式 AI 與大型語言模型(Large Language Model, LLM)將被濫用於網路釣魚、簡訊及其他社交工程攻擊，所生成之內容將更加擬真，且可大規模運作。

此類資安事件案例中，AI 服務提供商 Hugging Face 之平台存在惡意 AI 機器學習模型之現象。Hugging Face 為開源機器學習社群與平台，該平台共享超過10萬個預訓練模型(Pre-Training Model)、1萬

多個資料集與應用程式。Hugging Face 平台上託管之眾多 AI 機器學習模型中，至少有超過百個存在惡意功能，其中一些後門更可以讓攻擊者於受害電腦上執行惡意程式。雖 Hugging Face 宣稱已部署安控措施，如惡意軟體掃描等，但仍無法完全避免這些潛在之風險，為防範此類威脅，建議各機關於開始使用 AI 工具前，應參考「行政院及所屬機關(構)使用生成式 AI 參考指引」，訂定相關管理與使用規範，以白名單方式列出允許使用之 AI 工具，同時敘明不得於 AI 平台上傳或洩露內部機敏性資訊等措施，依風險評估結果規劃 AI 之系統與網段，並在應用程式介面(Application Programming Interface, API)中加入管控機制，且持續確保政策落實度，並監控任何可疑活動，以防堵威脅發生。

二、 個人資料與憑證外洩致防護機制失效

根據 IBM 113年資料外洩成本報告(Cost of a Data Breach Report 2024)調查顯示，資料外洩於113年平均成本高達488萬美元，相較112年445萬美元增加10%，資料外洩平均成本呈現年年增長趨勢，分析導致資料外洩最主要之攻擊路經來自網路釣魚與個人憑證洩露。

統計報告中指出有35%資料外洩涉及影子資料(Shadow Data)，因雲端環境發展與儲存媒體工具多樣化，影子資料來源可能為內部員工或供應商夥伴將資料儲存於個人設備或未經核可之雲端環境中，其放置原因不外乎備份、資料分享或遷移過程中暫時存放，甚至是使用生成式 AI 不經意洩露，這些無意之儲存資料，未經組織盤點與納管，造成資料外洩事件加劇。

在資料外洩案例中，雲端通訊服務業者 Twilio 所擁有的雙重認證應用程式 Authy 相關之數千萬個電話號碼遭駭客外洩，進而引發後續可能利用外洩電話號碼展開網路釣魚與簡訊之社交工程攻擊，仍需持續提升使用者之資安意識，方可減緩相關攻擊。該事件攻擊是藉由不安全之應用程式介面(API)展開，因未設置嚴謹之身分驗證機制遭入侵。因此，不論是使用自行開發或外部之 API 前，應參考 OWASP 前十大 API 風險，檢測是否存在相關弱點。

三、 社交工程泛濫致 APT 攻擊與勒索軟體風險增加

歐盟網路安全局 ENISA 於113年威脅情勢(Threat Landscape 2024)報告提及其觀測到最主要的威脅為可用性威脅，其次是勒索軟體、

惡意軟體、資料外洩、社交工程、資訊操縱與干擾及供應鏈攻擊等，主要鎖定對象則為公共管理、交通運輸及金融產業。有關社交工程攻擊，其中又以商業電子郵件入侵(Business Email Compromise, BEC)事件數量急劇增加，藉由威脅受駭組織將公開其機敏資訊，迫使受駭組織於限定期間內滿足其勒索金錢要求。

此類資安事件案例中，威脅情資技術與服務業者 EclecticIQ 於113年偵測到 ONNX 網路商店平台提供網路釣魚即服務工具(Phishing-as-a-service)，主要鎖定對象為金融業者，偽冒人資部門發出以薪資更新為標題之郵件，誘使使用者開啓夾帶有二維條碼之 PDF 惡意檔案。掃描二維條碼後，將受害者引導至仿冒微軟365登入頁面，且因二維條碼一般皆是透過手機掃描登入，若組織內部未針對員工所使用之行動裝置進行管理，則該攻擊方式之成功機率將大幅提升。

從研究報告與資安事件中可得知，社交工程攻擊手法越來越多樣化，不僅可透過網路平台取得網路釣魚即服務工具，再加上 AI 工具之推波助瀾，更助長駭客透過社交工程鎖定特定目標後，展開惡

意攻擊。防範社交工程攻擊建議可蒐集相關案例，更新社交工程可能之入侵手法，並持續提供教育訓練宣導攻擊手法、入侵路徑及可能的影響，提升人員資安意識，且應持續監測系統日誌，如發現可疑活動時，應於隔離區域檢測，防止擴散。

四、 資安(訊)供應商遭駭致破壞供應鏈安全

根據 WEF 114年全球網路安全展望(Global Cybersecurity Outlook 2025)統計，大型組織中有54%受訪者表示要促成網路韌性，其中又以供應鏈為最大風險，再加上缺乏對供應鏈廠商安全等級之要求與監督。另供應鏈之主要安全議題為軟體漏洞，資安廠商 ReversingLabs 於113年軟體安全供應鏈(The State of Software Supply Chain Security 2024)報告中提及所偵測到從109年至112年透過開源軟體套件傳播之威脅增加了1,300%以上，所暴露之惡意軟體套件多係為了竊取資訊。

在113年供應鏈發生資安事件受害嚴重之案例中，CrowdStrike Falcon EDR 感測器因更新錯誤造成微軟系統大當機，導致數以百萬計資通系統遭受影響，而 CrowdStrike 亦面臨客戶與投資者之請求賠

償。依據Gartner預測，114年全球約有45%組織之軟體供應鏈將遭受攻擊，相較於110年增加三倍之多，影響衝擊將難以評估。

資安事件案例中，Leather 加密貨幣錢包(Leather cryptocurrency wallet)之開發商聲稱有用戶通報蘋果應用程式商店(Apple App Store)存在一款惡意應用程式(Wallet Drainers)會俟機竊取加密貨幣，此App 透過取得用戶密碼，成功登入獲取受害者數位資產，該 App 被下架前之評分高達4.9分(滿分為5分)，分析該 App 可能使用 AI 自動產生正面評論，同時加上 Leather 商標及使用典型加密錢包之說明，企圖營造出其為真實 App之假象，誘使用戶下載使用。

從上述案例可了解，供應鏈危害不單侷限於軟體供應鏈，不論是硬體設備、元件、韌體及服務等都應納入供應鏈管理範圍，且應有對應之管理措施，及依議定之服務水準協議與資安要求進行委外廠商監督管理。此外，使用者於獲取使用供應鏈服務時應多方驗證其安全性與真實性，遵循機關組織以白名單方式所訂定之軟體下載與使用規範。

五、 資通系統弱點頻遭揭露利用

資安廠商 Action1發表之113年軟體漏洞評級報告(Software Vulnerability Ratings Report 2024)提及負載平衡器中的漏洞遭利用率創歷史新高，且特別鎖定 NGINX 與 Citrix 等系統成為目標。另一趨勢顯示蘋果作業系統越來越受到攻擊者關注，112年期間蘋果作業系統 MacOS 與 iOS 之利用率分別增加7%與8%。此外，MSSQL 遠端程式碼執行(Remote Code Execution, RCE)漏洞激增1600%，更突顯漏洞利用風險激增，引發使用者對邊緣安全(Edge Security)之憂慮，應加強對遠端連線或連網設備等安全管理。

資安廠商 Akamai 揭露殭屍網路 Mirai 新變種 Hail Cock 鎖定 Digiever 網路監視器與 TP-Link 設備，運用其漏洞擴散 Mirai 殭屍網路，藉此展開分散式阻斷服務(DDoS)攻擊。以 Digiever 為例，受害設備型號 DS-2105 Pro 已上市超過10年，製造商可能已停止維護或未能即時更新設備漏洞，而讓駭客有機可乘。另一個被利用之 TP-Link 設備，美國媒體更傳出將被禁用的消息，美國政府已開始調查其威脅風險，最快可能於114年禁止使用；微軟資安調查報告亦指出駭客運用 TP-Link 設備之既存漏洞，獲取遠端程式碼執行能力，再利用勒

索軟體攻擊。如廠商對產品缺陷未能及時處理，容易導致資安漏洞被利用後發生竊取資訊、服務中斷、甚至涉及間諜活動等攻擊狀況。

Google子公司Mandiant公布之112年弱點分析報告指出，被利用漏洞有70%為零日漏洞(0-day vulnerability)，顯示駭客具備更佳的漏洞挖掘與偵測能力展開零日漏洞攻擊。新漏洞或零日漏洞代表攻擊者之惡意行為可能於修補前就遭攻擊者利用之系統缺陷進行攻擊，因此更需加強即時偵測異常行為，而對於過時或無法更新之漏洞，建議各機關組織應實施強化管控措施或評估下架。

六、 雲端應用服務衍生多元威脅

歐盟網路安全局ENISA於113年威脅情勢(Threat Landscape 2024)報告說明有一項為依靠可信任網站(Living Off Trusted Sites, LOTS)之攻擊手法，攻擊者將惡意行為擴展到雲端環境，藉由使用可信賴環境與合法雲端服務以規避資安檢測，同時亦將命令與控制(Command and Control, C2)指令潛藏於Telegram或雲端通訊軟體Slack上，偽冒為正常流量或無害訊息。

雲端應用服務資安事件中，資安廠商BeyondTrust於官網揭露因

API 金鑰遭外洩，影響遠端支援軟體即服務(Software as a Service, SaaS)客戶，該公司主要為提供特權存取管理(Privileged Access Management, PAM)與遠端安全存取方案之廠商，其客戶包含政府機構、科技產業、醫療保健組織、能源及金融業者。該公司於事件發生當下聘請第三方網路安全公司協助調查與鑑識事件發生根因，調查期間陸續揭露該公司遠端服務與特權存取管理產品，包含自架服務(Self-Hosted)與雲端服務，分別存在2個中度與嚴重程度之漏洞，能讓入侵者執行命令，重置本機應用程式帳戶之密碼，取得權限後，上傳惡意檔案。因從偵測出異常活動至漏洞修補前，尚有一段空窗期，外界認為駭客可能已利用這2個漏洞展開零日攻擊。

從雲端服務應用普及化，再加上部分駭侵團體利用雲端服務規避資安檢測，說明除雲端環境之風險逐漸提升外，威脅辨識之難度亦更具挑戰。上述案例再次驗證縱深防禦之重要性，不僅是地端服務應用需留意漏洞更新，雲端環境漏洞訊息更應加強關注，建議各機關組織參考國家資通安全研究院網站之共通規範專區所公布「政府機關雲端服務應用資安參考指引」，將雲端環境包含在資訊安全要

求之範圍，如資訊保密、存取安全及事件通報程序等列入雙方契約要求辦理，俾利雙方依循相關規範。

參、113年政府資安威脅統計

一、 聯防預警情資

統計分析政府機關資通安全威脅偵測管理(Security Operation Center, SOC)回傳資安監控情資之資安威脅種類，掌握整體資安威脅類別及趨勢，透過資安聯防與情資分享，分析不同威脅種類與數據，如情資數、攻擊跳板來源及國家等，同時藉由跨領域、廠商蒐集之情資，彼此交流協作，促進國家資安聯防。

統計113年1月至12月之監控情資，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(43.2%)，主要係針對透過掃描、探測及社交工程等攻擊手法取得資訊情資之資訊蒐集行為；第2名為入侵攻擊(18.8%)，主要為針對系統與服務成功破壞之行為，造成未經授權存取或取得系統服務資源與權限，包含成為殭屍網路之受害者；而第3名為入侵嘗試(17.9%)，係針對嘗試入侵未經授權主機之情資，包含試圖透過暴力破解或利用已知與未知漏洞等攻擊手法，嘗試破壞與干擾系統服

務，各類資安威脅分布詳見圖2。

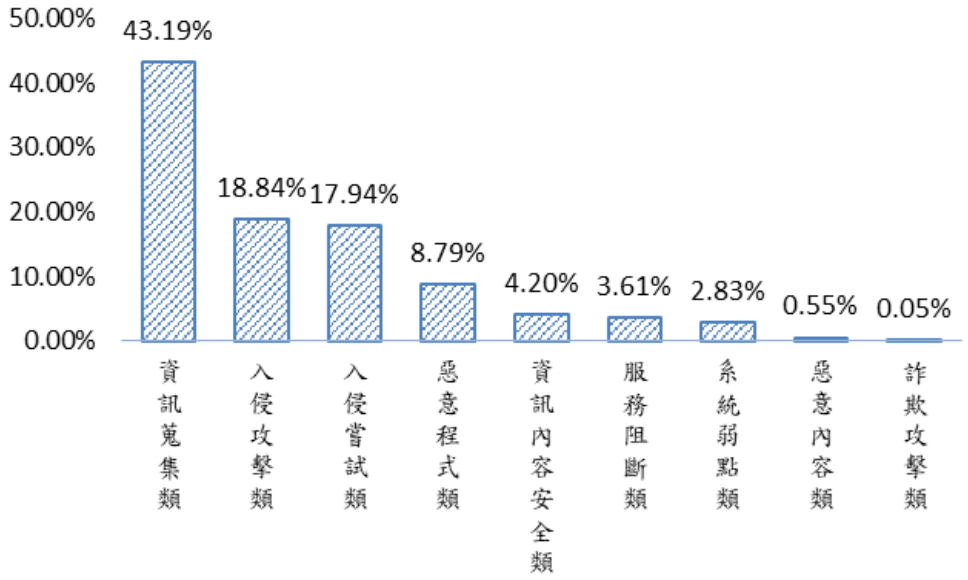

圖2　各類資安威脅分布圖

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

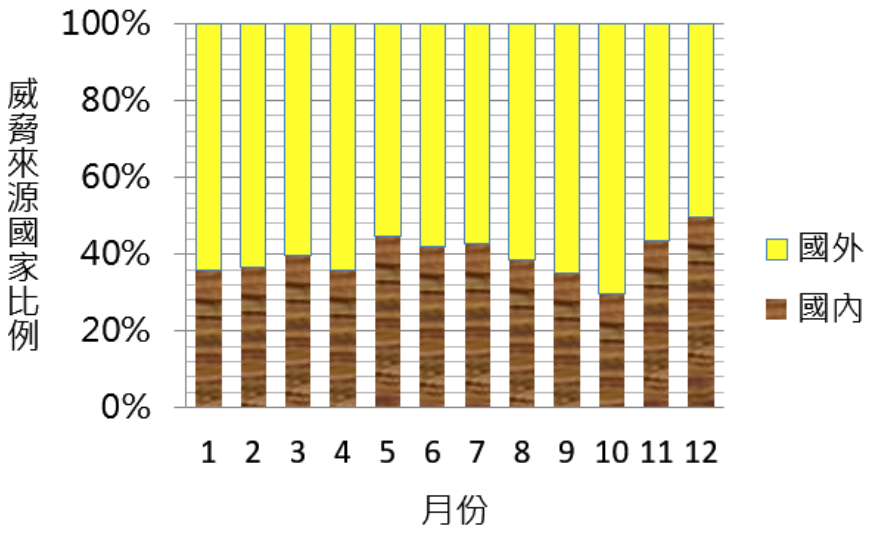

圖3　113年國內外攻擊跳板來源比例

細部分析國外攻擊跳板來源，前3名分別為美國(28%)、荷蘭(23%)及德國(6%)，因攻擊跳板來源國家眾多，其他未列入前5大攻擊跳板來源之國家共占33%，國外攻擊跳板來源資訊詳見圖4，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相關威脅。

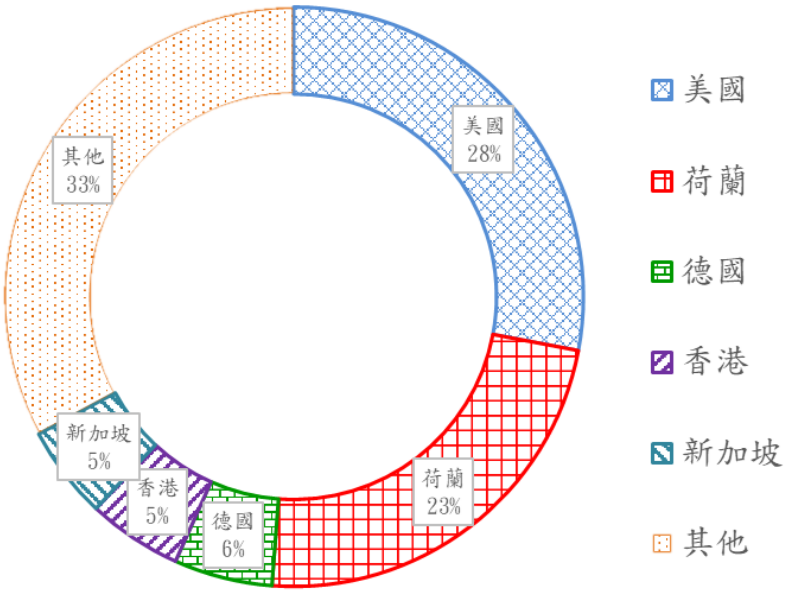

圖4　113年國外攻擊跳板來源國家比例

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一，113年共檢測2餘億(229,111,770)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602餘萬(6,027,182)封，約占整體之2.63%，每月惡意電子郵件偵測數量統計詳見圖5。113年10月偵測到大量商業詐騙郵件散布活動，經分析發現，駭客以協助處理金錢款項為由，誘使收件人回覆並提供個人資訊，以詐術騙取金錢或竊取敏感個人資料。

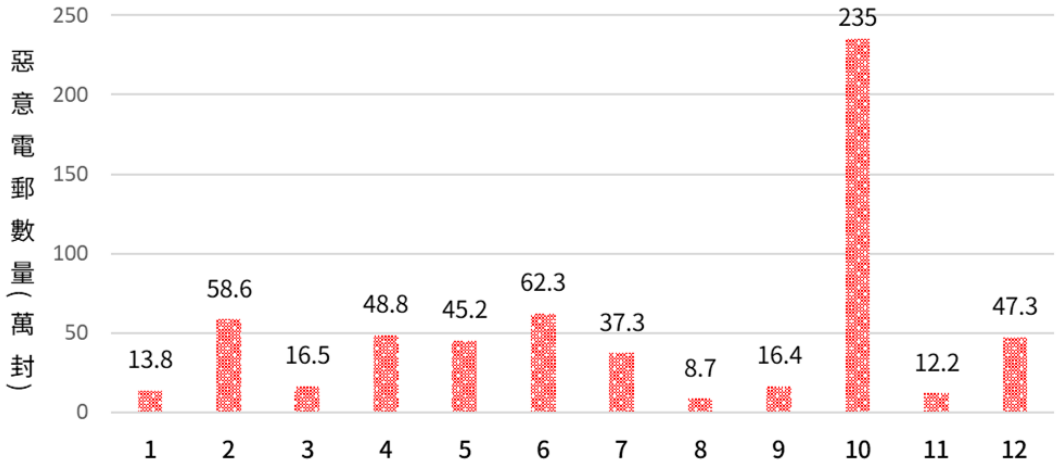

圖5　113年政府骨幹每月惡意電子郵件偵測數量

分析整體惡意電子郵件之風險分布比例詳見圖6，高風險占比為1.09%，需透過沙箱自動化動態分析，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；中、低風險合計共占98.91%，中、低風險之判定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，具有已知惡意態樣或特徵。

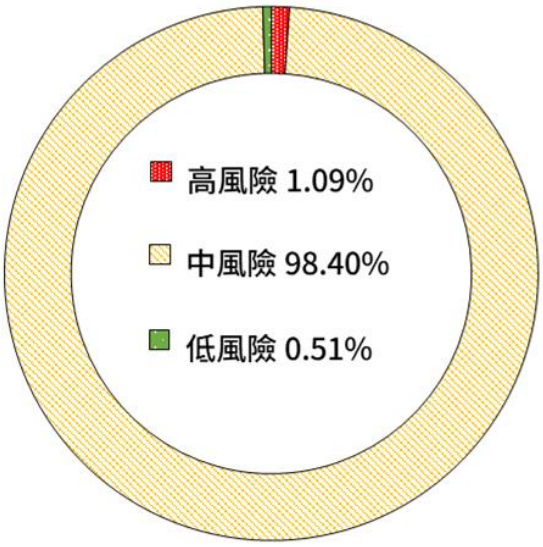

圖6　惡意電子郵件風險分布比例

綜整研析113年政府領域之進階持續性威脅(Advanced Persistent Threat, APT)郵件攻擊手法，可分為6種攻擊手法，其中第一種攻擊手法為駭客透過濫用合法郵件服務，藉由與使用者互動之多層式攻擊策略，引誘使用者下載惡意程式，藉此規避機關組織資安防護機制；第二種攻擊手法係駭客利用受駭學術信箱，以公職人員財產申報相關主旨，對政府機關發動針對性魚叉式釣魚郵件攻擊，散布易取得之 Star RAT 遠端木馬程式進行初步感染，待系統受駭後才部署與其 APT 組織相關之惡意程式；第三種攻擊手法為駭客利用 Office 文件漏洞(CVE-2017-0199)搭配華航訂票相關主旨，引誘相關業務窗口執行惡意附檔並連線中繼站；第四種攻擊手法為利用微軟 MSC 文

件之新型態攻擊手法，透過文件 XSS 漏洞搭配 AppDomainManager 注入攻擊，進而下載 Cobalt Strike 後門程式；第五種攻擊手法為利用人民陳情之相關主旨，針對政府機關特定業務窗口寄送惡意電子郵件，並利用 RTLO(Right to Left Override)手法將惡意 EXE 執行檔名稱偽裝為 DOC 文件，誘騙收件人開啟該執行檔，並使用側載 DLL 函式庫(DLL Sideloading)手法載入惡意 DLL 檔，此外，駭客並於郵件嵌入追蹤像素(Tracking Pixel)，藉此追蹤郵件主旨或內容是否成功誘騙攻擊目標開啟郵件；第六種攻擊手法利用內含惡意巨集之 Word 文件做為附件，誘使目標執行後，多次連線至遠端下載站，透過分段下載、動態解密及組合技術，藉此有效規避自動化沙箱偵測機制，增加最終後門程式被取得或攔截之難度。

「社交工程釣魚郵件」與「惡意程式垃圾郵件」為惡意電子郵件威脅中常見之攻擊類型，113年共偵測236餘萬(2,360,384)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，並透過架設與偽冒政府機關所使用之郵件服務登入頁面，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，113年共偵測38餘萬(380,350)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址至惡意網站下載惡意檔案，進而安裝後門程式於收件人主機執行攻擊。短網址服務(如 bit.ly、reurl)與雲端硬碟空間(如 Dropbox、Google 雲端硬碟)等第三方服務，亦常被駭客利用做為惡意程式下載之轉址與儲存媒介，藉此散布惡意檔案，降低被防護機制偵測之風險，並增加分析人員追蹤難度。其次，近年來惡意程式垃圾郵件之散布活動常利用各式民生相關帳單做為誘餌，如以「電信帳單」、「水電費帳單」及「健保帳單」等繳費通知為主旨，並利用竊取之郵件資訊做為惡意電子郵件內容，使收件人難辨識真偽。經分析，此類惡意垃圾郵件皆使用.pdf與.zip副檔名之惡意附件，並利用具規避偵測技術之 GuLoader 惡意程式下載器，搭配多階段惡意程式下載流程，躲避資安防護偵測機制，其散布之惡意程式包含 Remcos 與 NanoCore 等遠端木馬。

此外，113年4月與12月，發現多起以指控侵害版權名義，散布Lumma Stealer 資料竊取惡意程式之攻擊行動，駭客於社交工程郵件內以超連結方式，於偽製成 PDF 檔名之字串內嵌下載連結，誘騙使用者下載惡意檔案，且其惡意檔案大小皆超過自動化分析工具之上限，試圖規避防毒軟體偵測與沙箱自動化分析機制。

113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 CVE-2017-0199與 CVE-2017-11882相關漏洞利用之惡意程式為大宗，占整體惡意程式38.9%。CVE-2017-0199與 CVE-2017-11882為微軟 Office 系列之遠端執行漏洞，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的漏洞之一，且列為美國網際安全暨基礎設施安全局(CISA)公布之最常被利用漏洞其中之一，其餘偵測發現之惡意程式族群依序為 XRed 後門程式、Remcos 及 AgentTesla 遠端木馬等。

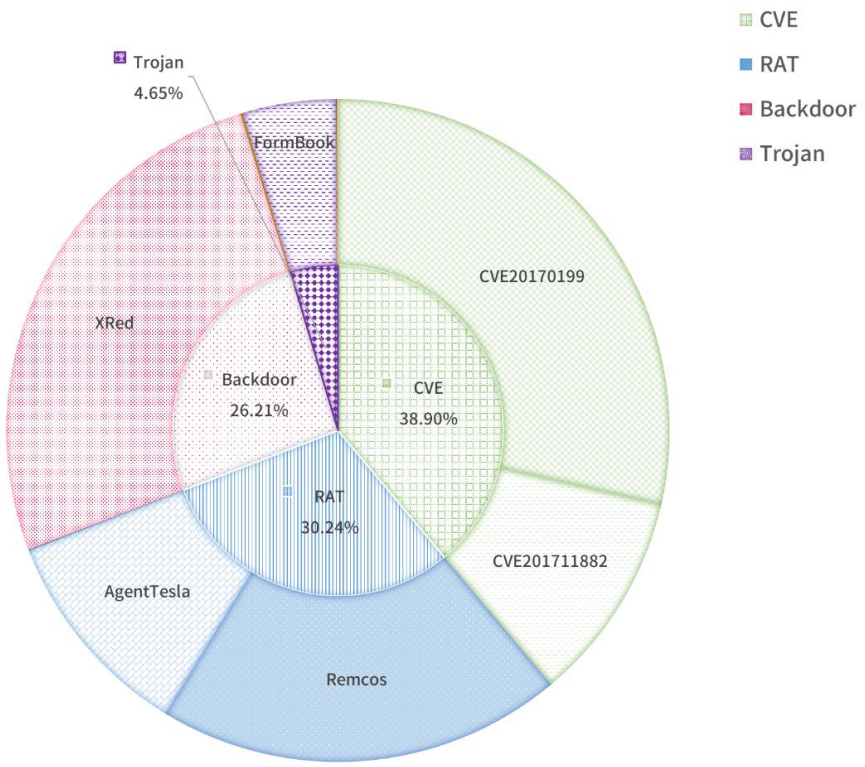

圖7　主要惡意程式族群分布比例

三、 資安攻防演練

為提升政府機關資安防禦及應變能力，113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之潛在脆弱點，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。113年計71個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。

113年度網路攻防演練71個機關3,459個對外系統，演練結果發現50個機關對外資通系統存在弱點，占演練機關總數70.42%，詳見圖8。

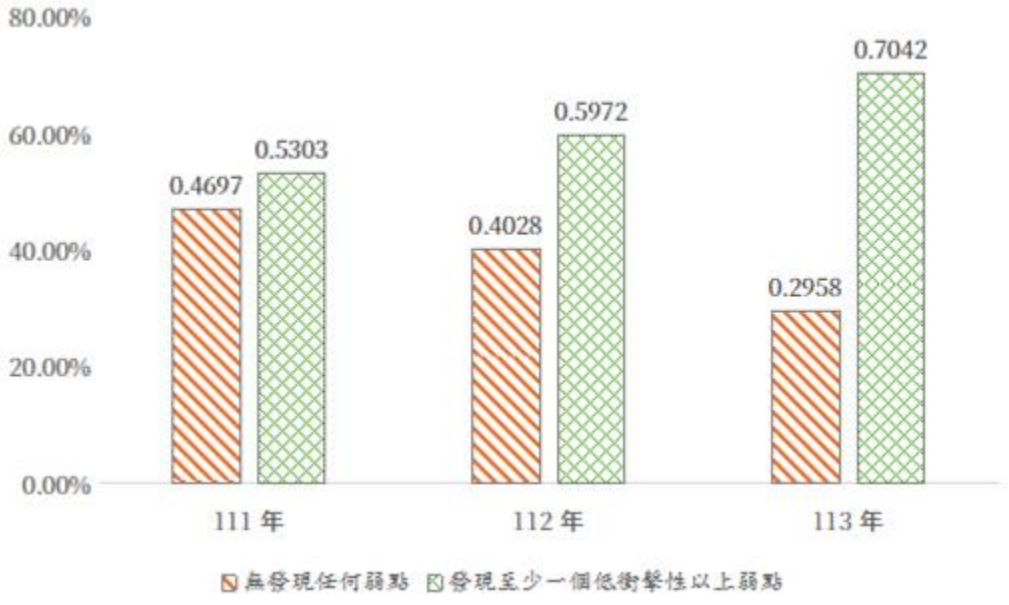

圖8　發現弱點機關比例

針對機關存在之資通系統弱點，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。113年度網路攻防演練共發現554個弱點，其中重大衝擊性弱點數量92個，占整體弱點數量16.61%，高衝擊性弱點數量195個，占整體弱點數量35.2%；中衝擊性弱點數量71個，占整體弱點數量12.82%；低衝擊性弱點數量196個，占整體弱點數量35.38%，詳見圖9。

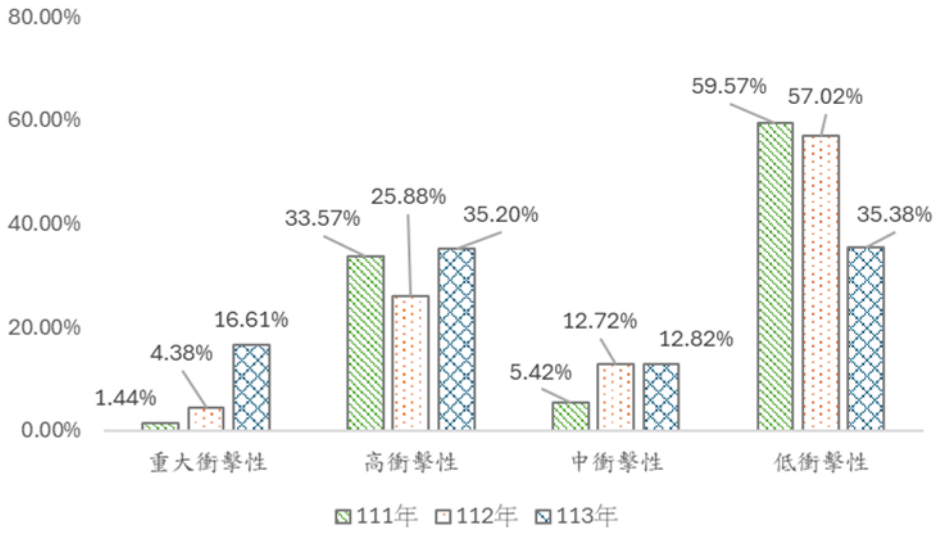

圖9　弱點衝擊性比例分布圖

(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。

113年電子郵件演練71個機關，受測人數計有1萬9,986位，45個機關開啟郵件，占演練機關數量之60.56%，近3年開啟郵件機關比例詳見圖10；有37個機關點閱連結/附件，占演練機關數量52.11%，近3年點閱連結及附件比例詳見圖11；簡訊演練69個機關，有33個機關點閱簡訊連結，占演練機關數量47.83%，近3年點閱簡訊比例詳見圖12。

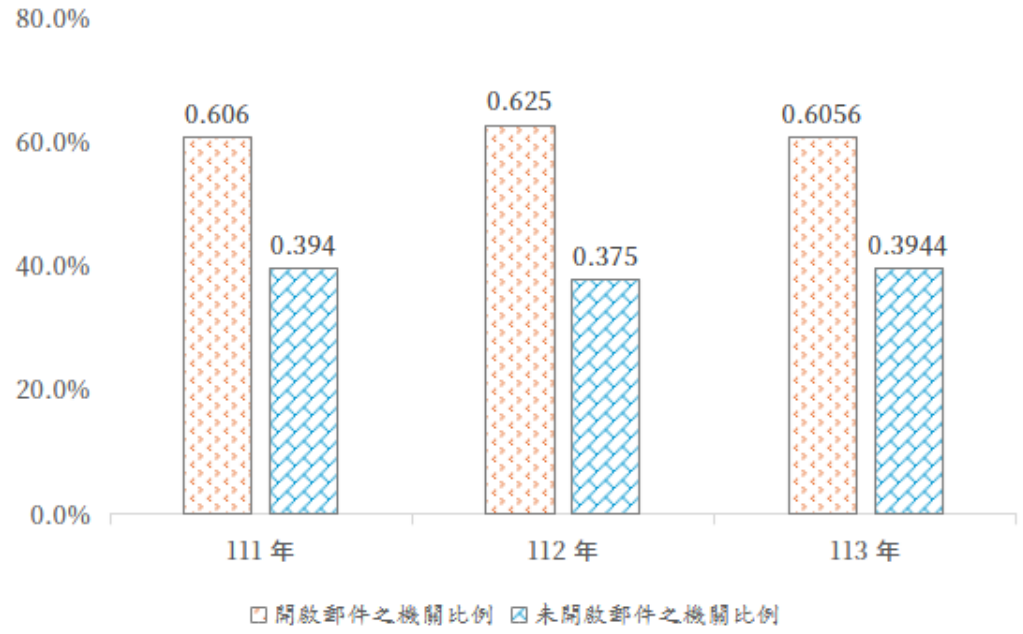

圖10　開啟郵件機關比例圖

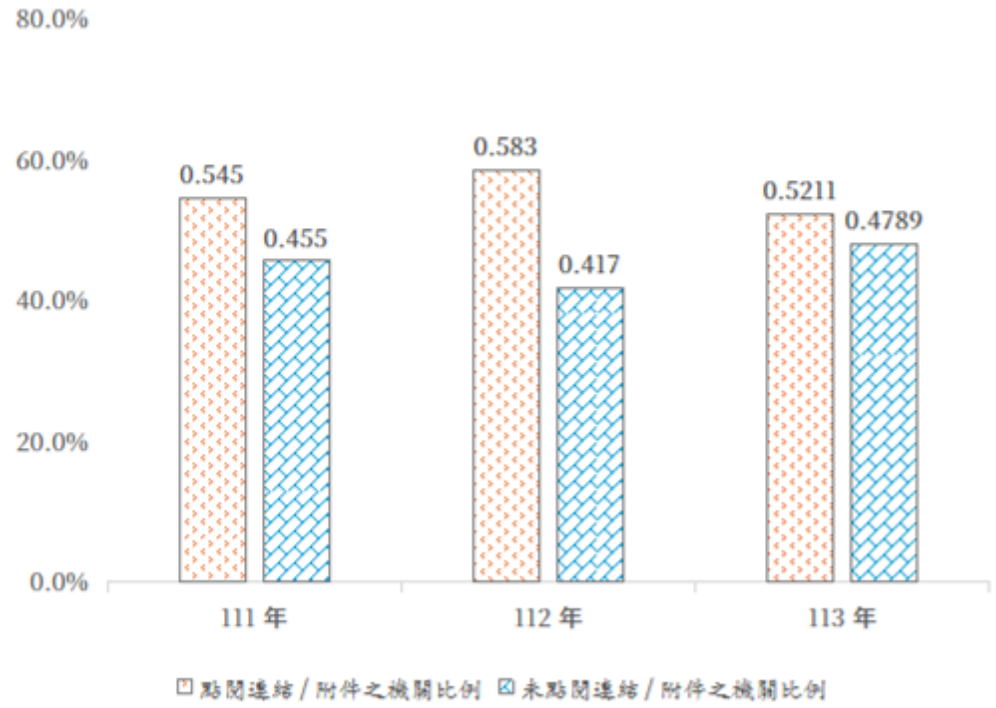

圖11　點閱郵件連結/附件機關比例圖

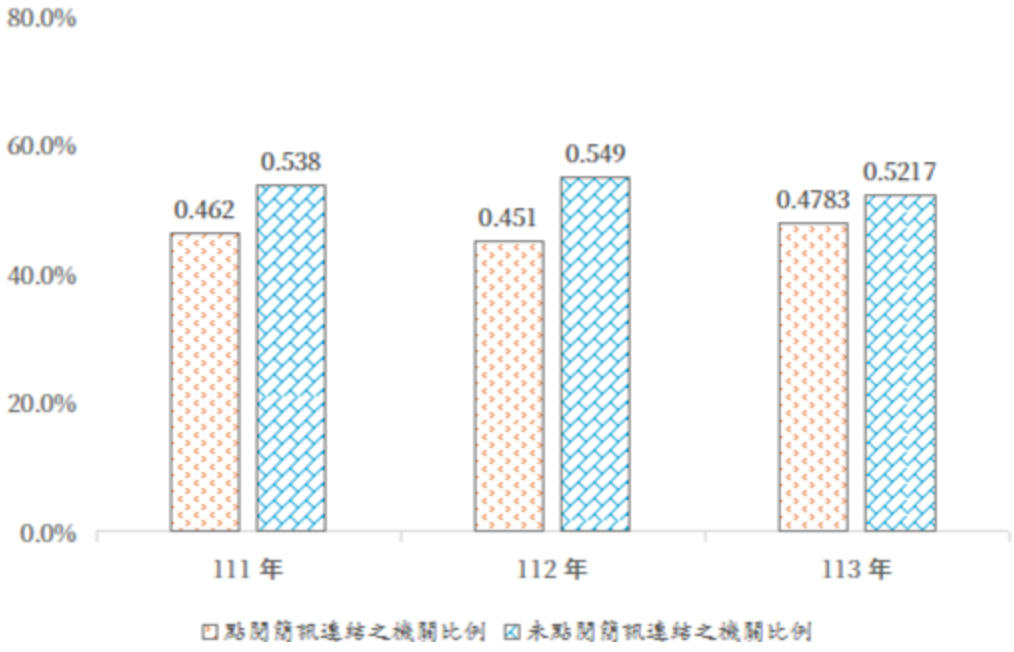

圖12　點閱簡訊機關比例圖

113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之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、資訊安全管理系統(ISMS)、受稽機關之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。

113年遴選40個受稽機關，包含16個公務機關及24個特定非公務機關，分季執行資安稽核作業。稽核小組包含稽核領隊、稽核委員、技術檢測人員及工作人員等成員，共同執行資安實地稽核作業，分別由策略面、管理面及技術面3個構面進行訪談。

經檢視公務機關實地稽核個別項目成績分布，詳見圖13，其中「資安人力及經費配置」表現較佳；「核心業務及其重要性」仍有強化改善空間。

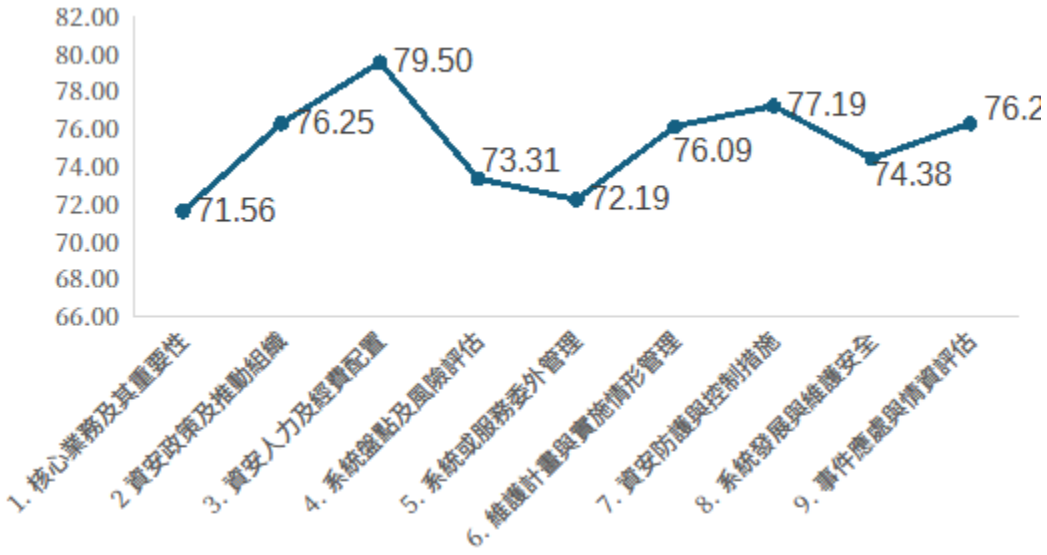

圖13　公務機關實地稽核個別項目成績分布圖

綜合分析公務機關實地稽核各構面之表現情形，詳見圖14，自策略面、管理面及技術面三個構面檢視，整體表現尚屬平均，其中「管理面」表現與其他構面稍有落差。

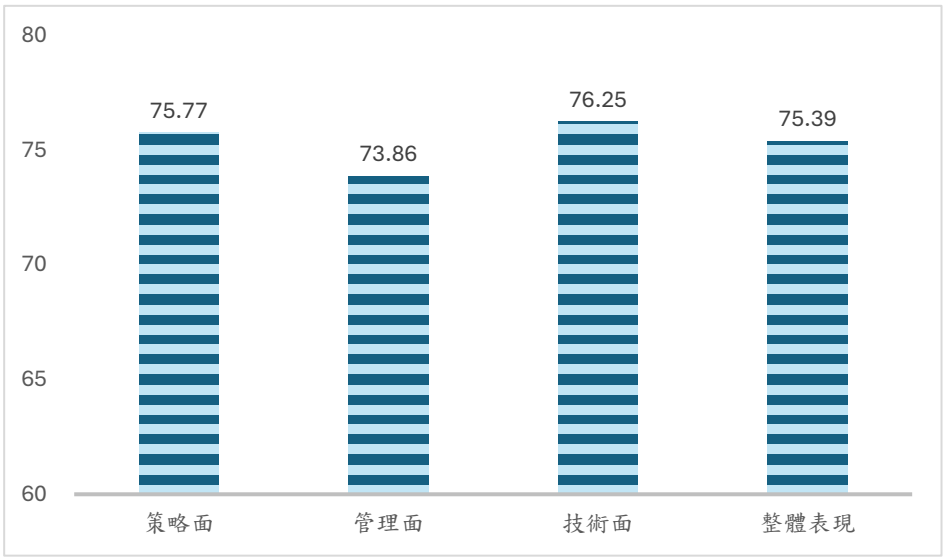

圖14　公務機關實地稽核各構面成績分布圖

五、 資安事件通報

分析113年公務機關通報事件(不含實兵演練)，以機關收到發布警訊後，再行通報之事件通報為主，占所有通報事件48.08%，顯示協助整體資安偵測防護之重要性，彙整通報比例資訊詳見圖15。

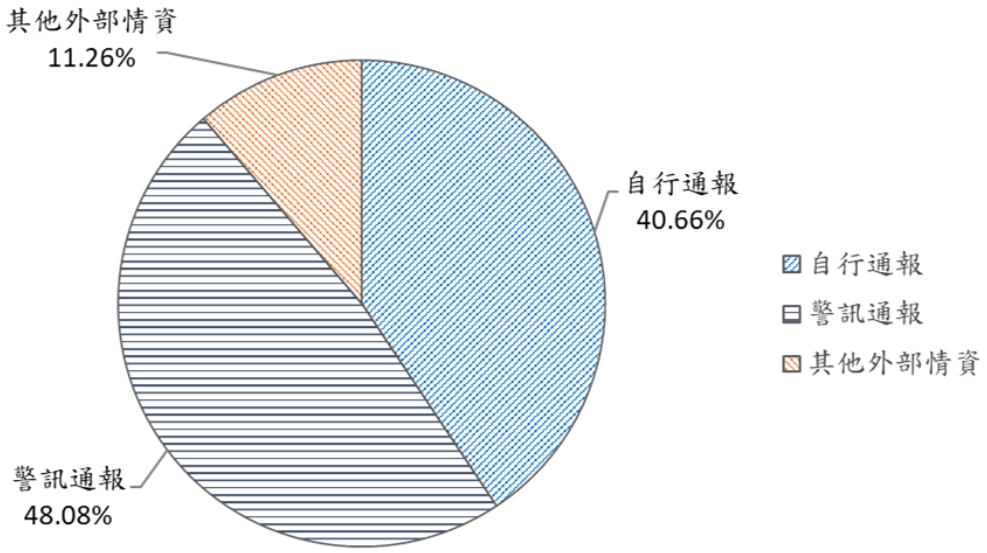

圖15　113年警訊通報占總通報件數統計

機關依資通安全事件通報及應變辦法規定，視資安事件造成機密性、完整性及可用性衝擊之影響程度，通報之資安事件等級由輕至重區分為「1級」、「2級」、「3級」及「4級」。統計113年機關通報之資安事件，以1級資安事件占83.97%為大宗，2級資安事件占13.91%居次，3級資安事件占2.12%，4級資安事件則無發生，資安事件等級比例詳見圖16。

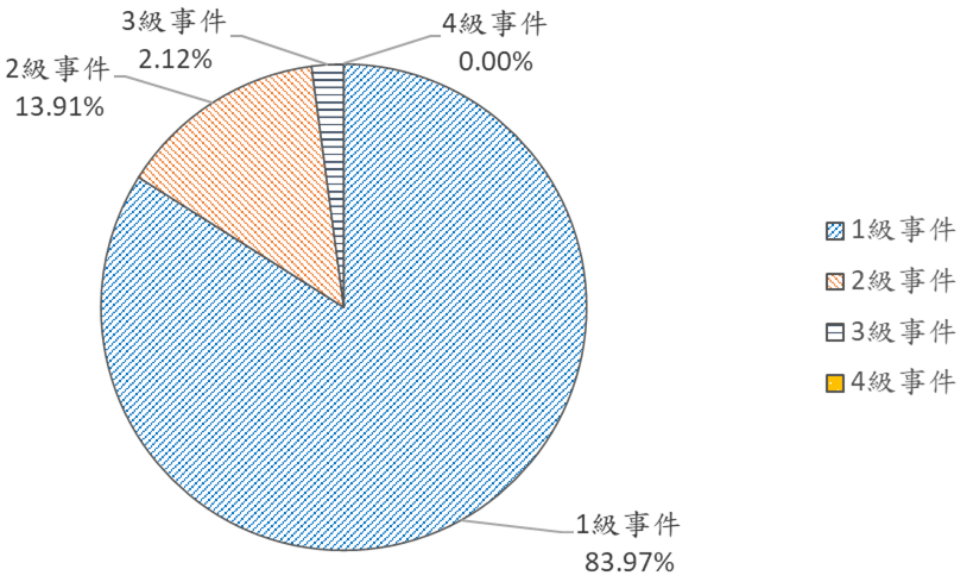

圖16　113年資安事件等級比例

分析所接獲之資安事件類型，排除「其他」類型後，以非法入侵事件居多占62.52%，其次為設備問題占14.17%、阻斷服務占5.7%及網頁攻擊占4.9%，各資安事件類型比例，詳見圖17。

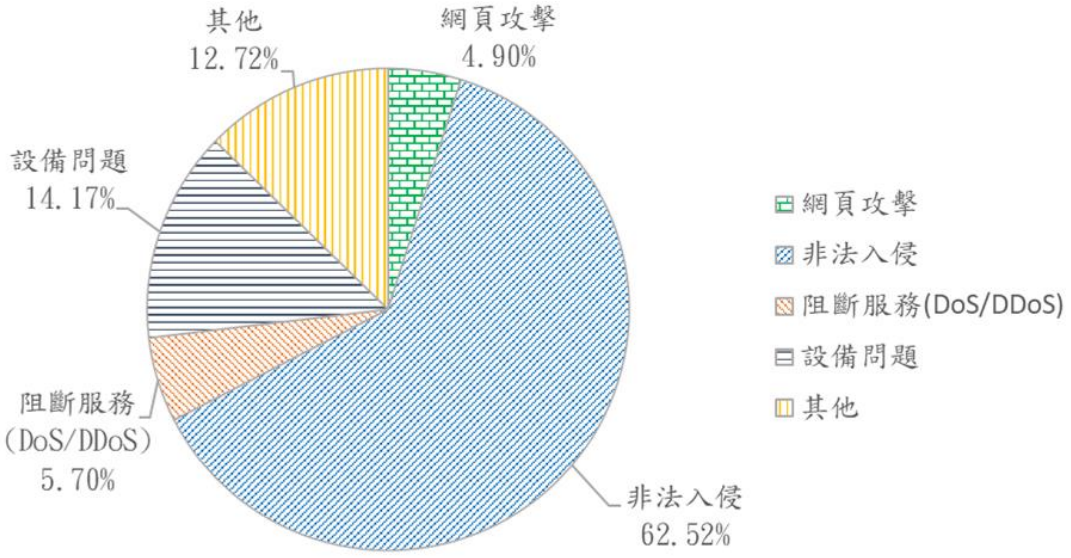

圖17　113年資安事件類型比例

上述通報案件中，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，以應用程式漏洞占6.94%為最高，例如 PHP(CVE-2024-4577)與 GeoServer(CVE-2024-36401)高風險安全漏洞遭利用攻擊成功；次之為弱密碼/密碼遭暴力破解占4.13%，詳見圖18。

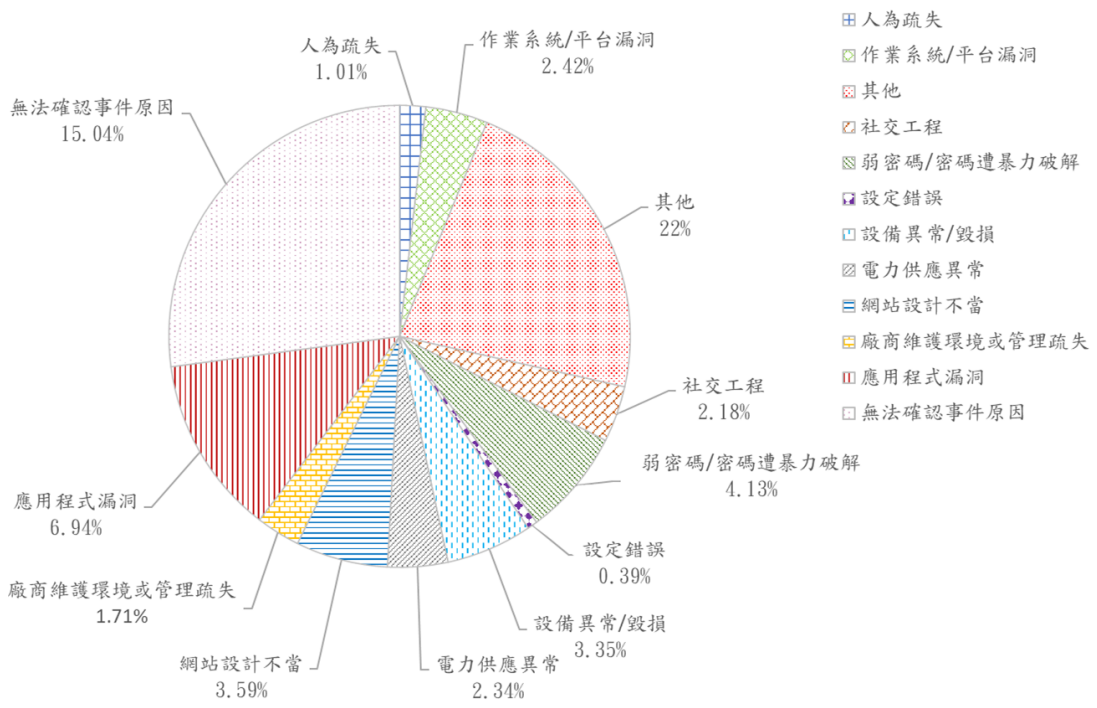

圖18　113年資安事件發生原因比例

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113年政府機關資安事件通報案例，分析駭客入侵常用手法，檢視共通性弱點，研提「網站使用弱密碼遭破解變更網站公告內容」、「誤載惡意程式與不慎點選惡意郵件導致公務電腦受駭」、「供應鏈因遭遇資安事件致公務系統受牽連服務中斷」、「資訊設備因疏於更新與維護致存在惡意程式」、「惡意郵件內嵌雲端硬碟下載連結以規避資安防護檢測」及「遭受 DDoS 攻擊導致服務受影響」等6個政府機關面臨之資安威脅與相對防護建議，提供各機關參考。

一、 網站使用弱密碼遭破解變更網站公告內容

自事件通報案例中，機關藉由內部端點偵測軟體(Endpoint Detection and Response, EDR)發現其對外服務之平台遭嘗試上傳後門程式，經檢視根因為後台管理者帳號使用弱密碼，且平台為委外開發建置，廠商遲未執行密碼變更作業，亦未對可遠端存取管理之功能加以限制。

另一案例為機關發現其對外粉絲專頁遭駭客盜用，且張貼不當

圖片，經調查發現同樣為管理者帳號之密碼設置過於簡單，遭駭客破解成功登入後，將其設為管理者並移除其他管理人員，導致機關無法登入與更正粉絲專頁內容，後續向粉絲專頁之管理權責業者申訴下架遭駭之粉絲專頁，並重新建立新粉絲專頁。針對類此案件資安防護建議如下：

(一)針對帳戶與密碼原則未納入政府組態基準及資通系統防護基準之系統或平台，應進行清查盤點並遵循帳密設定原則。

(二)實施弱點掃描時應包含所有資通系統，以識別弱點之風險並及時完成修補。

(三)管理者因具備較高權限，建議應採多因子驗證方式登入，以加強身份鑑別機制。

二、 誤載惡意程式與不慎點選惡意郵件導致公務電腦受駭

政府通報之資安事件中，某機關偵測到內部電腦遭執行異常 PowerShell 指令，下載並執行惡意程式。經調查分析根因為機關資訊人員因內部系統檢測之業務需要使用免費開源工具，惟並未察覺此開源工具來源為惡意網站，網站提供機器人驗證之功能，必須點

選「我不是機器人驗證」才能至下一步，過程中誘導使用者執行 PowerShell 指令，後端之惡意程式實為竊取個資軟體。另有一案例為使用者欲下載通訊軟體，亦未確認網站之真實性，下載含有後門之程式，進而導致電腦向惡意中繼站報到連線。

社交工程郵件攻擊不曾停歇，以113年資安事件為例，駭客以郵件主旨為薪資評估通知搭配加薪之訊息內容，寄送社交工程電子郵件攻擊政府機關。此外，亦發現駭客利用美國航空航天學會網站存在重新導向之漏洞，嵌入釣魚網址，企圖誘騙收件人點擊連結與提供敏感資訊。針對類此案件資安防護建議如下：

(一)指定專人負責蒐集威脅情資與社交工程等入侵手法，並持續更新應變防處措施及提供相關教育訓練，減少入侵之可能性。

(二)開啟業務相關之電子郵件前，除應判斷郵件來源之正確性，若發現附件檔案名稱中存在異常字元(如副檔名為 pdf, zip, msc, lnk, rcs, exe, moc，或檔名含有亂碼或簡體字等)，亦應通知負責人員進一步確認是否為社交工程郵件。

(三)落實資通系統之安全修補與病毒碼更新，包含作業系統、程式套件及防毒軟體等。

三、 供應鏈因遭遇資安事件致公務系統受牽連服務中斷

政府通報之資安事件中，某機關因共構機房火警致網路服務中斷，核心資通系統無法正常提供服務，此外，因其所屬機關(構)之網路與網域名稱系統(Domain Name System, DNS)採取向上集中之方式，導致其所屬機關(構)之相關網站與資通系統亦無法對外服務。

另一案例則為 CrowdStrike Falcon EDR 更新異常致資通系統出現微軟系統故障之藍色螢幕(Blue Screen of Death, BSOD)或重複執行開機現象，導致服務受到影響。針對類此案件資安防護建議如下：

(一)應清楚定義供應鏈之範圍及相關人員，將供應鏈之基本安全要求與服務水準協議納入契約文件規範。

(二)評估業務重要性與資源配置，建置備援機制，以維持資通系統可用性，定期辦理業務持續運作演練並納入複合性情境，讓相關人員熟悉回復之標準程序，於訂定之目標回復時間點完成復原。

(三)資通系統維護人員在規劃變更管理作業，應增強軟體測試程序，並執行版本控制與變更管理。

四、 資訊設備因疏於更新與維護致存在惡意程式

113年發現數個政府機關之差勤系統遭駭客植入惡意程式，檢視其共同點為使用公版差勤系統，因該系統出現系統漏洞，致駭客利用該弱點入侵後，企圖上傳惡意程式，分析其漏洞成功被利用之原因亦含開放遠端連線，其允許外部攻擊者能透過掃描工具偵測到此服務。

另一案例為發現機關資訊設備開啟 FTP 服務，遭上傳挖礦相關程式，受駭設備包含印表機或監視器主機等 IOT 裝置，調查發現根因係部分設備未修改預設密碼或使用弱密碼，遭駭客以暴力破解方式登入成功，且相關設備同樣開啓對外服務。針對此類事件資安防護建議如下：

(一)政府機關使用公版系統，應納入 EDR 偵測管理範圍，並偵測異常連線行為。

(二)依照政府組態基準(GCB)之要求訂定安全原則，更改預設密

碼或弱密碼之設定，訂定安全之存取連線規則。

(三)評估資通訊設備連網之需求，若不需對外網路服務應考量將對外服務埠關閉或限制僅供內部 IP 存取，以減少相關資安風險。

五、 於惡意郵件內嵌雲端硬碟下載連結以規避資安防護檢測

政府通報之資安事件中，某機關偵測發現其資訊設備執行異常指令，經調查為駭客使用社交工程手法，利用官網民意信箱陳情，要求業務承辦人自 Google 雲端硬碟連結下載壓縮檔案，且提供密碼供開啟，當承辦人依要求下載並解壓縮檔案，再點擊偽裝成 PDF 文件之捷徑檔(LNK)後，惡意程式即遭載入並執行。

另一案例為駭客仿冒機關對外服務之業務通知內容，利用業務相關主旨寄送社交工程郵件，並附上惡意附檔。其惡意附檔內含第1階段 Guloader 惡意程式下載器，執行後再連線至 Google 雲端硬碟下載第2階段 Remcos 遠端木馬，最終連線至駭客中繼站並回傳受駭主機資訊，該惡意程式行為包含遠端控制、網路通訊及鍵盤記錄等。針對類此案件資安防護建議如下：

(一)訂定雲端服務之允許使用原則，識別雲端資訊及相關聯資產之安全原則。

(二)檔案下載前應經過端點防護或防毒軟體掃描，特別是經風險評估為高風險來源之檔案，應移至隔離區域檢測。

(三)不將機敏資訊上傳於個人或業務用之雲端環境，若需上傳敏感性資訊應輔以加密機制。

六、 遭受 DDoS 攻擊導致服務受影響

113年發現多個政府機關對外網站遭遇阻斷服務(DDoS)攻擊，致網站服務中斷或受影響，綜整各事件後，分析其攻擊手法多為常見之阻斷服務攻擊方式，如 HTTPS Flood 與 TCP SYN Flood，惟機關均可於短時間內恢復，且未有系統遭進一步破壞，顯現機關對於此類攻擊已有初步之防禦及復原機制。

此類攻擊雖非新式攻擊手法，惟隨著新興技術之發展，以及物聯網設備之普及，當受害對象被攻擊者鎖定後，透過短暫且快速之流量請求，即可成功引起某種程度之侵擾，因此機關除應持續注意維運系統或服務上之漏洞以避免被利用外，更應密切監控異常流量，

方能於第一時間即時阻擋攻擊。針對類此案件資安防護建議如下：

(一)事前：設置入侵偵測與防護系統，監控異常或可疑流量，並規劃流量清洗與 CDN(Content Delivery Network)備援機制，以即時應對相關攻擊。此外應定期演練 DDoS 攻擊之營運持續計畫，檢視其應變措施之適切性。

(二)事中：應即時通報攻擊事件，分析並阻擋攻擊來源，判斷攻擊類型與影響範圍，同步啟動流量清洗服務，且完整保留系統日誌，俾後續調查。

(三)事後：檢視是否已確實阻擋攻擊並確認影響範圍，啓動復原計畫，由應變或鑑識小組分析遭攻擊原因、攻擊流量來源、使用技術或工具等，並修補相關弱點或更新改善計畫，以制定更積極有效之防禦策略。

伍、結語

網路世界蓬勃發展，駭侵工具唾手可得，提升資安意識、加強教育訓練及強化防禦措施皆需與時俱進，本部將持續關注國內外資安威脅情資與趨勢、供應鏈之資安危機、社交工程之攻擊手法、雲端服務及阻斷服務攻擊等議題，研議相對應之偵測及防禦作法，以持續對抗資安威脅，並針對身分驗證、存取控制、系統弱點及設備漏洞等議題，持續推動各機關強化資安防護量能，並確保供應鏈安全，進而提升國家資安韌性及攻防能量。

為加強建構具備資安韌性之可信賴政府數位環境，持續研析資安技術、提升資安意識完備程度及強化資安聯防機制，並推動機關導入弱點通報機制、端點偵測及回應及零信任網路架構等各項資安防護措施，期藉由建立國內外良好的溝通管道，透過情資分享以協助各機關掌握資安威脅趨勢，提升我國資安防護能量。