111 年度國家資通安全情勢報告

數位發展部

中華民國 112 年 6 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」。

全球性的 COVID-19 疫情影響了大眾生活及工作模式，俄烏戰爭也引發全球資安韌性議題，加上新興科技的多元應用伴隨各式的資安威脅及挑戰，都使得因應資安風險為必須面對之重要課題。本報告藉由研析 111 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，提出相關資安防護建議，協助各機關強化資通安全防護能量，期經由前瞻政策引導及國家整體資源力量，打造安全可信賴之數位國家。

貳、111 年全球資安威脅情勢概要

根據世界經濟論壇(World Economic Forum, WEF)「112 年全球風險報告」指出，隨著全球格局以顯性風險(Manifesting Risks)為主軸，WEF 於 111-112 年全球風險認知調查(Global Risks Perception Survey, GRPS)中，用 3 項時間軸分析了解全球風險，其中「2 年內可能最嚴重的風險」，及「10 年內可能最嚴重的風險」這 2 項時間軸中與科技有關者為「不利的先進科技成果」、「數位權力集中」、「數位落差」、「關鍵資訊基礎設施的癱瘓」及「網路犯罪與資訊不安全的擴張」。再以調查中之影響程度排序可以發現「能源供給危機」、「生活成本負擔困境」、「通膨升溫」、「糧食供給危機」與「關鍵基礎設施遭受網路攻擊」為未來一年最有感的前 5 項風險，其中與科技有關者為排名第 5 的「對關鍵基礎設施之網路攻擊」。

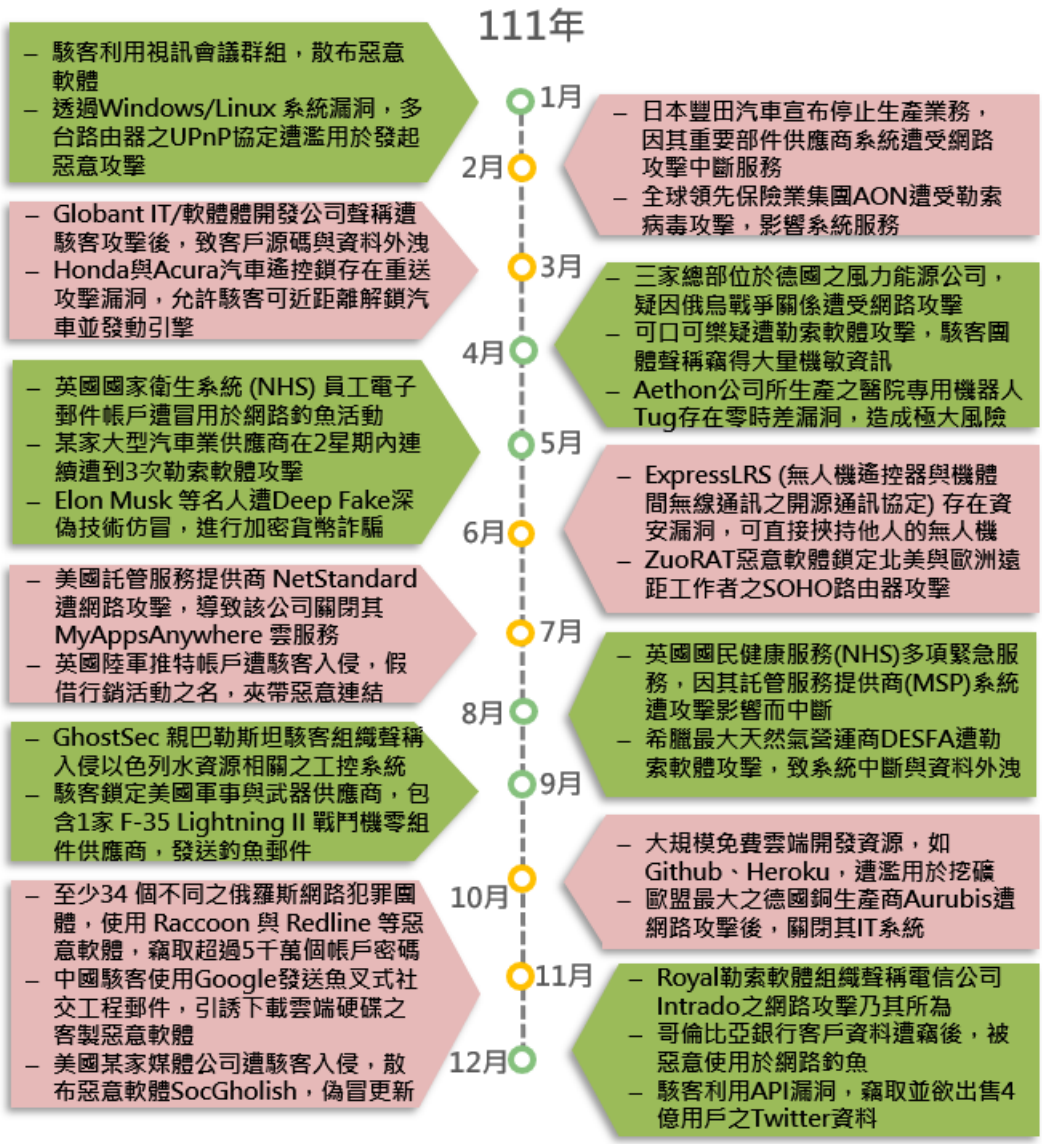
資安防護不僅需要針對資訊基礎設施與環境加強鞏固外，更需面對新興科技與持續變化之挑戰，以靈活變動之因應策略，將風險控管在可接受程度內。新冠肺炎(COVID-19)疫情雖接近尾聲，但全球工作模式已產生顯著的變化，如採取遠距工作或遠端連線、行動式設備運用、大量使用線上社群媒體及雲端平台盛行等，皆大幅增加了資安的潛在風險。

觀測 111 年全球重大網路攻擊事件，因勒索軟體即服務(Ransomware as a Service, RaaS)提供便利且快速之勒索軟體營運模式，逐漸形成駭侵產業生態系統，且發展為三重式勒索，不僅入侵目標對象外，更波及其供應商與客戶，造成衝擊除部分付出贖金之代價外，尚包含個人資料、憑證外洩或聲譽損失。

隨著科技的不斷發展和數位化轉型的推進，更多的組織和企業正在將其業務和資源移轉到雲端環境中，包含資料儲存、應用程式開發、

資料分析、人工智慧和機器學習等領域。同時，使用者也越來越依賴雲端服務，如雲端儲存、郵件服務、社交媒體等。此外，新興技術的發展，如物聯網（IoT）、5G 通信、大數據分析和人工智慧等，也將對雲端服務的需求產生額外的推動力。隨著雲端服務需求漸增，便利或免費的公共雲服務也越來越多，資安防護議題也隨之而生，面對未來不論是基礎設施、應用系統或資料之轉移，皆應思考並預為準備。

以下綜整 111 年全球重大網路攻擊事件，以分析威脅現況與未來資安情勢可能發展。同時，藉由觀測網路攻擊事件，研析相關攻擊手法，從案例學習甚或超前部署相關預防措施，111 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 1　111 年全球重大網路攻擊事件

111 年全球重大網路攻擊事件，可窺見駭客利用社群媒體、社交工程郵件展開初始攻擊，更針對特定組織或國家，以鎖定式攻擊手法逐步滲透，而現今因無人機、汽車產業、智慧居家至智慧城市設備等之聯網需求逐漸提升，亦導致相關風險日益升高。同時，駭客更經常地利用產品或系統漏洞展開入侵行動，如網路通訊等設備產品、關鍵資訊基礎設施及其 OT（Operational Technology，營運技術）設備亦常

為惡意人士目標之一，攻擊相關設施造成之衝擊影響深遠。全球化影響，供應鏈亦擴展至不同邊界，其中因資安管理措施不一，駭客得以鎖定供應商攻擊再橫向入侵至政府機關或產業。新冠疫情雖逐漸趨緩，然對雲端環境需求並未消失，反而因其維運便利與擴充性，成為資訊運用趨勢，管理者對雲端環境之架構與組態安全，應加強其整備度。

綜整研析歐盟網路暨資訊安全局(European Union Agency for Cybersecurity, ENISA)於 111 年 10 月發布之網路安全威脅態勢年度報告(ETL, ENISA Threat Landscape 2022)、WEF 於 111 年 1 月發布之全球網路安全展望(Global Cybersecurity Outlook 2022)及各資安業者調查等報告資料，可歸納為 6 大面向之資安威脅情勢，包含「雲端環境產生相對應風險」、「間歇式加密恐加劇影響」、「物聯網與行動設備資安風險倍增」、「資安(訊)供應商遭駭破壞供應鏈安全」、「關鍵資訊基礎與 OT 設施頻傳鎖定式攻擊」及「社交工程詐騙手法層出不窮」，以下針對 111 年全球資通安全威脅情勢進行分析與說明。

一、雲端環境產生相對應風險

根據資安業者 Zscaler 發表之 2022 Cloud (In)Security Report 中引述 Venafi 網路安全公司研究顯示，高居 81%的組織在過去一年中，經歷過與公共雲相關之安全事件，當中有 45%受訪者表示他們遭受至少 4 次或更多次數之事件。研究人員分析許多組織仍使用傳統網路安全防禦技術保護雲端環境，管理人員尚未意識到由於雲端環境之複雜性，需要具備更多不同於傳統之資安防護策略與管理責任。分析雲端環境事件中，前三名必須關注且常發生之議題依序為運行時之資安事件(Security incidents during runtime)(34%)、未授權之存取(Unauthorized access) (33%)及組態設定錯誤(Misconfigurations) (32%)。

Zscaler 分析雲端環境主要威脅包含雲端管理責任不明確，據統計有 55.1%之組織利用一個以上之雲提供商所提供之服務，因此如何訂定不同雲端服務提供者與彼此應負之管理責任，必須有共通之合規性策略與防護機制。而雲端資源組態設定錯誤仍是最普遍的雲漏洞，攻擊者可利用此漏洞不當存取雲端資料及服務，公開存取資料、帳號權限、密碼、未加密的資料等，造成大量資料不當外洩。

111 年雲端服務相關資安事件，有資安廠商 Sysdig 之研究團隊(Sysdig TRT)揭露一項大規模之加密貨幣挖礦活動，駭客利用市面上大型雲端與持續整合與部署(CI/CD，Continuous Integration/Continuous Delivery)服務供應商，包含 GitHub、Heroku、Buddy.works 等，以建構、運用及操作這些雲端資源，進行挖礦等活動。其中 TRT 團隊共發現逾 30 多個 GitHub 帳戶、2 千個 Heroku 帳戶及 900 個 Buddy 帳戶，同時這個惡意活動持續鎖定多個平台，準備繼續拓展其加密挖礦商機。駭客透過能自動註冊新 GitHub 帳號之 Shell Script，再藉由 OpenVPN 或 Namecheap VPN 使用不同 IP 連線至 GitHub，並以隨機產生之 GitHub Action 名稱掩飾其挖礦行動，用自動程式管控帳號，利用含有挖礦專用容器之 130 個 Docker Hub 映像檔以進行隨時切換，主要目的為規避服務提供者系統偵測，達到將加密挖礦之成本轉移予服務提供者，服務提供者的成本費用提高，亦將導致其售予合法授權客戶的價格更高。

二、間歇式加密恐加劇影響

根據 WEF Global Cybersecurity Outlook 2022 調查，就組織觀點而言，最關注之前 3 名資安議題分別為勒索軟體、社交工程及惡意內部使用者。若再調查負責資安管理階層，前 3 名最主要資安議題則為基礎設施因網路攻擊而中斷、憑證失竊及勒索軟體。由此可見，防範

勒索軟體，不論是就組織整體業務持續性考量，或資安管理階層而言，均不得不審慎面對且需從長計議，以通盤因應迫近之威脅。

勒索軟體因勒索軟體即服務(Ransomware as a Service, RaaS)輕易助長此類攻擊，對特定組織而言，遭鎖定之勒索軟體攻擊更加深對資安防禦之需求。觀察近來發生之資安事件，發現勒索軟體族群採用新式間歇性加密(Intermittent Encryption)技術，以快速加密受駭者系統，同時減少被偵測機率。根據資安廠商 Sophos 旗下的資安研究團隊，於 111 年發表案例報告指出，有某家大型汽車業供應商在 111 年 5 月時，在 2 星期內連續遭到 3 次勒索軟體攻擊，造成其系統遭到入侵，檔案亦遭加密。3 次勒索軟體分別是 Lockbit、Hive 與 ALPHV/BlackCat，都利用該公司防火牆的 1 個設定上的錯誤，利用 Remote Desktop Protocol（RDP）入侵該公司內網的網域控制器。間歇性加密不同以往勒索軟體加密法，只加密目標文件之部分檔案內容，加速受駭者系統受影響的速度。因其只加密部分內容，所以加密過程幾乎只需完全加密一半的時間，且若無有效之解密方法與密鑰，仍無法回復資料；此加密方式將使過往偵測工具慣用檢測作法，包含統計分析文件、IO 運作強度評估或版本差異性比對，無法即時地有效偵測異常狀況。

美國資安廠商 SentinelLabs 揭露 111 年勒索軟體事件，駭客採用間歇性加密已成為勒索軟體之最新趨勢，LockFile 為第 1 個使用間歇性加密之勒索軟體，依每 16 位元組之間隔執行加密。由於間歇性加密技術相對容易建置，因此越來越多勒索軟體包含 Qyick、Agenda、BlackCat (ALPHV)、PLAY 及 Black Basta 採用此手法。

採用間歇性加密之勒索軟體亦已發展出勒索軟體即服務，早在 110 年暗網就出現第 1 個以 Rust 語言編寫之勒索軟體 BlackCat (ALPHV)。SentinelLabs 於 111 年 8 月時亦觀察到有使用者在暗網販

售 Qyick 勒索軟體，採一次性購買，而非常見之訂閱模式，同時保證若該勒索軟體於購買後 6 個月內被偵測工具檢測出，將獲得一個新樣本，且提供折扣價。間歇性加密因具備可快速加密檔案、能規避既有資安工具偵測且建置容易，因此 SentinelLabs 之分析師預測將有更多勒索軟體使用此方式加密資料。

三、物聯網與行動設備風險倍增

PwC(資誠聯合會計師事務所)針對高階管理層面對未來網路準備調查(A C-suite united on cyber-ready futures: Findings from the 2023 Global Digital Trust Insights)發現，相較於 111 年之攻擊途徑，於 112 年會有顯著增加趨勢，統計第 1 名為行動式設備，有 41%受訪者認同此攻擊方式將會高居不下，物聯網部分則有 29%討論此風險。於萬物聯網之時代，行動式與物聯網設備之資安防禦準備，更需戰戰兢兢，小心應對。

近年來，人工智慧（AI）的發展已相當成熟，人工智慧物聯網(AIoT, Artificial Intelligence of Things)是將人工智慧與物聯網這兩種技術相互結合，創造出的智慧裝置，這些智慧裝置能夠自行學習、分析並做出決策，為人類帶來更加便利的生活，可預見物聯網環境因結合人工智慧而更加蓬勃發展，安全議題亦隨之浮上檯面。醫療物聯網安全解決方案廠商 Cynerio 於 111 年 4 月發現，Aethon 公司所生產之醫院專用機器人 Tug 存在 5 項零時差漏洞，統稱為 JekyllBot:5，這些漏洞預估可能影響全球數百家醫院。Aethon 公司所生產之醫院機器人 Tug 可用於藥物發送、清掃及運送備品，在利用無線電波、傳感器、攝影鏡頭及其他技術於無人協助情況下自在移動，不會撞到人或物體，且可自動開關門、搭乘電梯等。

因為 Tug 機器人可於醫院內獨立移動，故 Cynerio 所發現之

JekyllBot:5 漏洞，可能造成極大之風險。此 5 項零時差漏洞包含 CVE-2022-1066、CVE-2022-26423、CVE-2022-1070、CVE-2022-27494 及 CVE-2022-1059，分別位於 Tug 伺服器之 JavaScript、API 實作及 WebSocket 協定中。其中一項高風險漏洞 CVE-2022-1070，允許駭客透過連接 Tug 伺服器 WebSocket 以接管機器人，直接操作其移動路線與位置。其他漏洞可讓駭客藉由新增具管理權限之用戶帳號與刪改現有帳號、存取用戶之加密憑證、竊取 Cookie、攔截對話資料，甚至可能進一步被利用進行網路釣魚等行為。Cynerio 研究發現利用此 5 項零時差漏洞，不需高超技術且無需特殊權限或任何使用者互動，即可引發危險的攻擊行為，如干擾醫療用品之運送、控制醫院電梯或門鎖、干擾危害患者或手術進行，甚至擅自變更藥品的數量。攻擊者還能透過機器人的拍照和錄影功能，侵犯醫護人員或病患隱私，進一步監控患者或工作人員、竊取醫療紀錄，或是劫持管理員憑證以進行其他網路攻擊或間諜行為。所幸本案在研究人員通報後，Aethon 公司已及時釋出修補程式並部署到醫院機器人，並修補伺服器韌體、軟體漏洞，也修補了數家醫院造成機器人可被遠端存取的防火牆漏洞。

人工智慧物聯網之應用，可預見未來將越來越普遍，面對可能之零時差攻擊，不論是系統廠商或是使用單位，在運用其便利性之時，亦應隨時評估風險。

四、資安(訊)供應商遭駭致破壞供應鏈安全

網路安全公司 Mandiant 網路資安前端洞察與指導報告(M-TRENDS 2022)統計，初始感染或入侵媒介攻擊最常因為漏洞被利用，供應鏈則為 110 年排名第 2 之感染媒介，供應鏈攻擊在 110 年入侵事件中占 17%，而在 109 年時此比例尚未達 1%。歐盟 ENISA 於 111 年 11 月發布之威脅報告(ENISA Threat Landscape 2022)中指出，繼 109

年 SolarWinds 供應鏈攻擊事件，象徵針對供應鏈展開攻擊衍然成為新興趨勢且持續發展中，且因攻擊者採取之策略多為迂迴攻擊、所使用之工具善於規避偵測，偽冒成合法之使用者潛藏於環境中，持續橫向擴散，影響範圍大增。

容器安全新創公司 Anchore 於 111 年提出之軟體供應鏈安全調查報告(2022 Security Trends: Software Supply Chain Survey)中指出，軟體供應鏈攻擊影響高達 62%之組織。軟體供應鏈安全廠商 Sonatype 於 111 年所發表之年度軟體供應鏈狀況報告(8th Annual State of the Software Supply Chain report)指出，於過去 3 年軟體供應鏈攻擊的平均年成長率高達 742%，其中發現有 96%是屬於已知存在弱點之開放資源，應可以避免下載，關鍵在於是否有定期檢視更新軟體中所使用的第三方開放資源之安全性。

美國某家媒體公司 111 年因遭駭客入侵，資安廠商 Proofpoint 觀察到該媒體公司透過 JavaScript 指令碼提供影音內容與廣告予其他媒體新聞網站。駭客藉由竄改此 JavaScript 之基礎程式碼(Codebase)，進而部署惡意程式 SocGholish，偽冒假更新(FakeUpdates)至逾 250 家新聞網站，因此引發一波供應鏈遭波及之風波。

此次事件經 Proofpoint 追蹤後，顯示為俄羅斯駭客組織 TA569 利用新聞網站散布惡意軟體 SocGholish，利用虛假更新和網站重新導向來感染用戶，並在檔案中嵌入勒索軟體，導致受駭者遭植入勒索軟體等惡意軟體。Evil Corp 網路犯罪團體也曾在一起類似的攻擊中使用過 SocGholish，當時他們透過數十個被感染的美國報紙網站發送虛假軟體更新警報，一旦成功感染目的電腦，駭客就會將這些設備作為入侵企業網路的跳板，嘗試部署勒索軟體。受駭網站則以瀏覽器更新，如 Chrome.Updater.zip、Firefox.Update.zip、Opera.Update.zip 之名義，誘騙

使用者下載內含鍵盤側錄工具(Keylogger)等惡意軟體之壓縮檔案，致後續可能的帳密外洩等進一步駭侵攻擊。同時 Proofpoint 觀察到受駭者成功修復經數日後，又再次遭植入相同之惡意軟體，顯示除使用者應加強資安意識外，系統管理者亦需採取步驟式，清楚確認風險已移除，並將事件於內部進行經驗學習案例分享，方能避免事件再次重演。

此類資安事件一再發生也緣自於 FakeUpdates 通常採取保守入侵作法，不會貿然一次性地對大量目標對象釋出假更新，其策略為對潛在目標進行窺探與篩選，根據使用者之瀏覽器，跳出 Firefox、Chrome 或 Edge 等更新訊息，因此使用者通常無法於第一時間警覺發現。鑑於 FakeUpdates 攻擊時有所聞，使用者在收到更新訊息時，應多加驗證其真實性，除檢視其訊息來源之正確性外，亦應至其官網、論壇或諮詢窗口多方查證訊息之真確性，較安全的做法是僅從官方網站等可信任的來源下載軟體更新，避免從不明網站、電子郵件或彈出視窗中點擊下載連結，並經常更新軟體。另外透過提高使用者的資安意識，教育其識別和避免假更新的風險，訓練使用者警覺社交工程和釣魚攻擊，以確保他們不會受騙點擊惡意連結。

五、關鍵資訊基礎與 OT 設施頻傳鎖定式攻擊

微軟在 111 年 12 月發表第 3 期網路威脅情報研究報告 Cyber Signals 指出，在其客戶的 OT 網路中發現，有超過 75%最常見之工業控制器存在高嚴重性之漏洞且未修補。就漏洞揭露趨勢來看，從 109 年到 111 年間，於主要供應商生產之工業控制設備中，被揭露為高嚴重性漏洞之數量成長至少 78%。雖然有高嚴重性漏洞之威脅風險，但發現即使是資源充分與管理良好之組織，面臨需要將關鍵資訊基礎設施停機以修補漏洞之情形時，管理人員仍常選擇讓高風險之漏洞繼續存在，以維持其系統運作之可用性。如此一來，當這些漏洞被揭露於

外或利用時，就容易成為有心人士入侵之破口。

資安專家分析針對工業設備之重大網路攻擊並不常見，主要是必須先累積大量該工業設備領域之專業知識的門檻。惟關鍵資訊基礎與 OT 設施一旦發生資安事件，影響範圍深遠，觀測從 110 年美國最大燃油管道 Colonial Pipeline 公司遭勒索軟體攻擊，導致美國政府宣布進入緊急狀態。另自俄烏戰爭開始後，關鍵基礎設施如核電廠等之安危，就一直成為雙方攻防戰重要指標。因此關鍵基礎設施除需持續強化其韌性外，更需加入關注資安數位轉型之議題。關鍵基礎設施和營運技術(OT)數位轉型之步調，因其固有架構與涉及整體議題，相較 IT 領域轉型通常來得緩慢，然關鍵資訊基礎與 OT 遭相關攻擊事件頻傳，且系統漏洞亦越來越多被揭露，其資安防護與數位轉型已刻不容緩。

發生於 111 年關鍵資訊基礎與 OT 設施攻擊之受駭事件，為 3 家總部位於德國之風電產業相關公司遭受網路攻擊。自俄烏戰爭開打以來，因各國政府開始計畫性地放棄使用俄羅斯燃料，進而發現德國風力發電機製造商與其維護廠商相繼成為攻擊對象，目的為藉以製造再生能源產業之混亂狀況。

當俄烏戰爭開始初期，德國渦輪機製造商 Enercon GmbH 之衛星公司即遭受攻擊，超過 5 千台風力發電機之遠端控制系統受影響，無法順利控制，僅能在自動操作模式下運作。而另一渦輪機製造商 Nordex SE 則表示，在該公司發生資安事件後，迫使他們不得不緊急關閉相關系統，同時隨即有親俄羅斯政府之勒索軟體團體 Conti 聲明，該攻擊事件為其所發起。另一家維護風力發電機之企業 Deutsche Windtechnik AG 表示，遭受駭客攻擊後，約關閉 2 千台風力發電機之遠端控制程式，導致遠端控制系統中斷 1 天左右，造成近 2 千組風力發電機組無法繼續生產電力。

六、社交工程詐騙手法層出不窮

社交工程理論與執行技巧簡單，但隨著新興科技之進步，如採用人工智慧或深偽技術，再加上時事議題，未來影響範圍恐將無孔不入。美國聯邦貿易委員會 FTC 在 111 年官網發布 110 年詐騙報告(Reports of romance scams hit record highs in 2021)指出，因愛情詐騙損失超過 13 億美元，近年來此類詐騙數字激增，單單 110 年就達到 5.47 億美元，相較 109 年增加近 80%。此類詐騙於網路上使用虛假資訊或仿冒名人，許多詐騙行為初始來自於臉書或 IG 等其他社群媒體，詐騙目的包含個人資料、財務，甚或誘騙使用者投資假虛擬加密貨幣。

資安業者趨勢科技發表 2023 年資安預測指出，就企業來說電子郵件詐騙 (Business Email Compromise, BEC)盛行，再加上近年發展出之變臉詐騙服務 (BEC as a Service)，趨勢預估 112 年這類 BEC 市場預計將以 19.4%之年複合成長率持續增長。

社交工程技術多樣化，但從社群媒體發起初始入侵則為常見手法。社群媒體帳號遭入侵後，駭客常藉此竊取資訊與謀取利益。111 年發生數起遭駭事件，第一起案例為英國陸軍推特帳戶及 YouTube 頻道近期同時遭駭客入侵，它們分別擁有逾 36 萬名粉絲與 18 萬人訂閱，英國陸軍推特頁面遭竄改成 The Possessed NFT Project 之頁面，並於推文中假借非同質化代幣（NFT）行銷活動之名，夾帶惡意連結；Youtube 頻道則遭頁面更換，由 Cathie Wood 創立之方舟投資 ARK Investment Management 頁面，並循環播放改製特斯拉創辦人 Elon Reeve Musk 與推特聯合創始人 Jack Patrick Dorsey 於受訪時提到加密貨幣的舊影片，駭客把這個片段進行加工，於網路循環播放宣傳假影片，宣稱可協助使用者將比特幣與乙太幣翻倍，誘使用戶落入加密貨幣騙局，此類手法曾於 24 小時內賺取價值約 130 萬美元之虛擬貨幣。

另一起案例為近期發現駭客利用 YouTube 改製遊戲教學或破解

攻略影片，於影片中夾帶惡意軟體套件組，遭假借知名遊戲包含 FIFA、Final Fantasy、Forza Horizon、Lego Star Wars 及 Spider-Man 等。資安廠商 Kaspersky 報告指出，在所散播之 RAR 壓縮檔中隱藏一系列惡意軟體，其中 RedLine 為目前揭露最為廣泛之資訊竊取軟體。使用者一旦安裝，RedLine 便會竊取受駭者網路瀏覽之相關資訊，包含 cookie、帳戶密碼、信用卡資訊、即時通訊內容及破解加密貨幣錢包。此外，該壓縮檔內尚暗藏挖礦程式，駭客進一步可利用受駭者之系統資源挖礦，藉此獲得更多利益。同時，在此惡意軟體套件組中，有一合法之 Nirsoft NirCmd 公用程式，可在不啓動任何視窗下執行運行，因此更讓使用者難以發現其蹤跡。

參、111 年政府資安威脅統計

一、聯防預警情資

為協助公務機關資通安全威脅情勢，國家資通安全研究院定期綜整資安監控情資，以掌握資安威脅類別及趨勢，並提供政府資安監測預警與服務。

經統計 111 年期間所彙整之監控情資，並將資安威脅類別區分為掃描刺探類、入侵攻擊類、政策規則類、惡意程式類、攻防演練類、系統服務類、阻斷服務類等 7 類，第 1 名為掃描刺探類(47.2%)，主要係針對已知漏洞、遠端服務及密碼猜測之探測行為；第 2 名為入侵攻擊類(26.9%)，係針對網頁入侵行為，包含針對系統攻擊以獲取非法權限等；而第 3 名為政策規則類(13.3%)，主要為針對違反機關特權帳號被異常存取、或由預期外之主機登入等行為，各類資安威脅分布詳見圖 2。

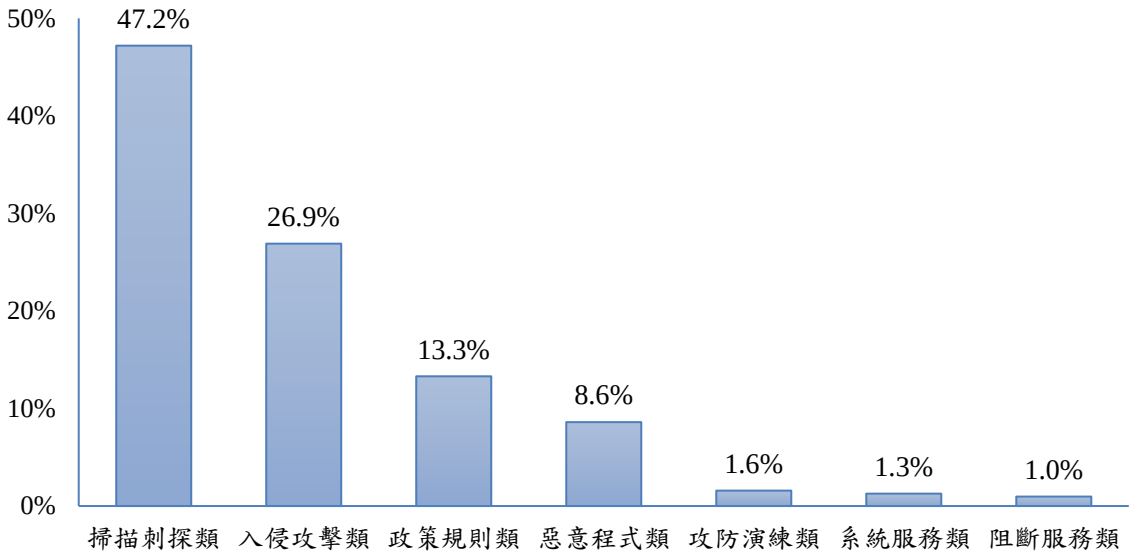


圖 2　各類資安威脅分布圖

二、惡意電子郵件分析

電子郵件長久以來一直是政府機關主要威脅來源之一，透過系統自身漏洞或透過內部人員資安意識不足所致，攻擊手法為藉由入侵政府機關系統、對人員寄送惡意郵件或至暗網購買獲取個人郵件憑證，尤其於因新冠疫情關係，許多社交工程郵件皆與疫情相關，如疫情補助、防疫獎勵、紓困福利及醫療訊息等，因其主題與時事生活習習相關，造成入侵成功機率增加。且現今管道不僅透過電腦入侵，有越來越多使用者於行動式設備上收取郵件，因此惡意電子郵件入侵途徑日益增加，也造成政府機關之機敏資訊外洩風險提升。而弱密碼亦是電子郵件攻擊途徑之一，駭客透過駭侵工具暴力破解多組機關人員郵件帳號密碼，並透過受駭電子郵件帳號申請機關內部系統取得登入資訊，進而入侵機關內部。綜上分析 111 年數據中，共檢測 458,361,569 封電子郵件，可疑惡意電子郵件約占整體之 2.96%，詳見圖 3，以及分析電子郵件之惡意檔案類型比例，主要以 Office Excel 系列與 RAR、ZIP 等壓縮檔為主，為政府機關常見之接收檔案類型，駭客藉此類常見檔案，以降低使用者警覺。

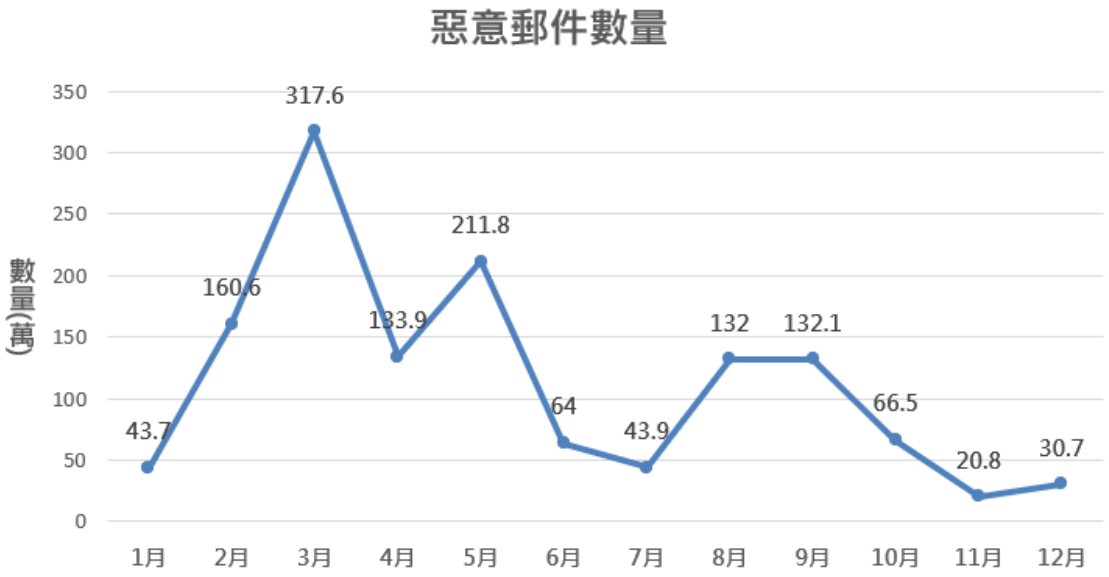


圖 3　每月 111 年政府骨幹每月惡意電子郵件偵測數量

三、資安攻防演練

資安攻防演練方式為模擬駭客角色，運用駭客常用手法，自機關外部對資通系統進行攻擊，以檢測機關資安防護及偵測能力，強化在遭遇資安事件時之通報、緊急應變、系統復原及協調管控等作業反應，並以社交工程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。111 年計 66 個機關參與演練，演練內容包括「資通系統實兵演練」及「社交工程演練」兩類，111 年演練結果說明如下：

(一)資通系統實兵演練

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攻擊方式，實際攻擊機關之系統與網路，檢測出現存之系統漏洞，模擬駭客入侵手法進行攻擊，藉以測試機關通報應變能力與資通環境組態設定之正確性。

111 年度網路攻防演練共針對 66 個演練機關 5,406 個對外系統進行演練，演練結果發現 35 個機關對外資通系統存在弱點，占演練機關總數 53.03%，詳見圖 4。

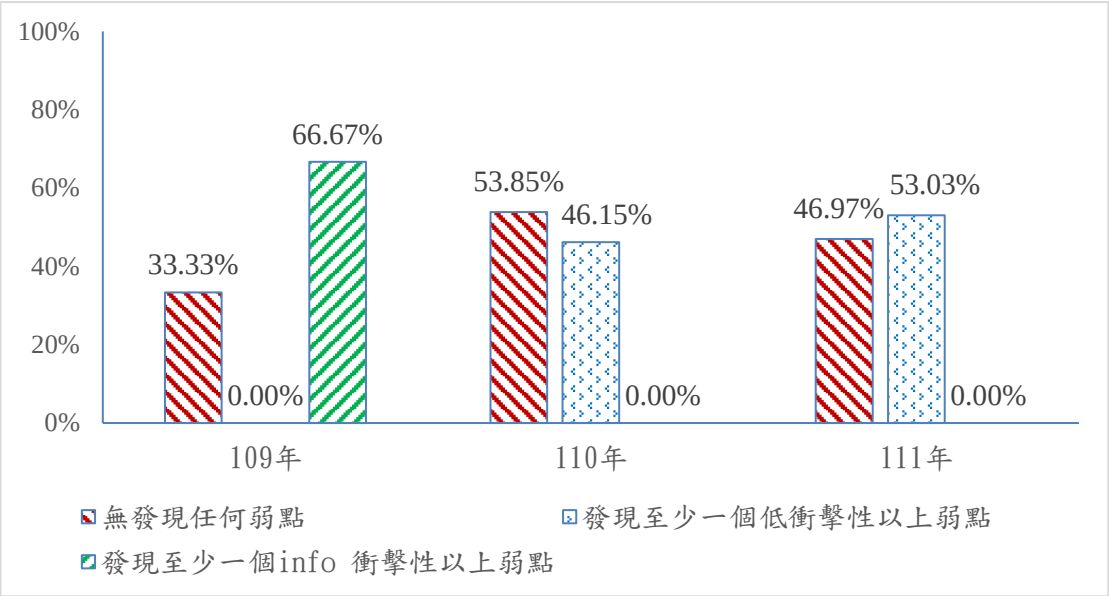


圖 4　發現弱點機關比例

針對機關存在之資通系統弱點，如遭受攻擊產生之衝擊性，區分為重大衝擊性、高衝擊性、低衝擊性及尚無衝擊性 4 種弱點類型。本次演練共發現 277 個弱點，其中重大衝擊性弱點數量 4 個，占整體弱點數量 1.44%，高衝擊性弱點數量 93 個，占整體弱點數量 33.57%；中衝擊性弱點數量 15 個，占整體弱點數量 5.42%；低衝擊性弱點數量 165 個，占整體弱點數量 59.57%，詳見 5。

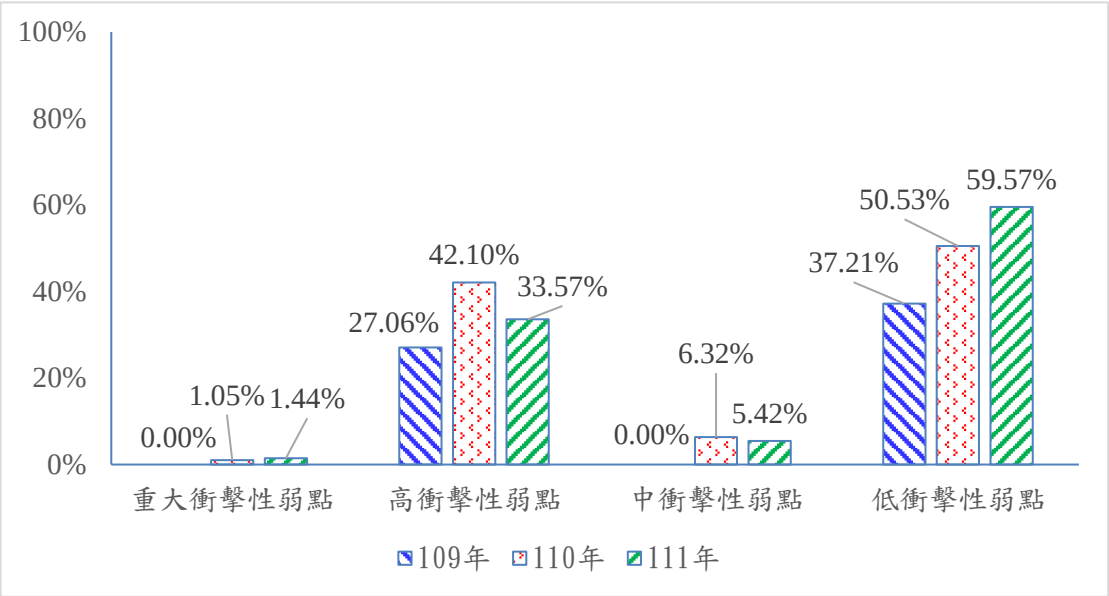


圖 5　弱點衝擊性比例分布圖

(二)社交工程演練結果

以電子郵件與簡訊方式測試機關人員對於社交工程攻擊之資安意識與警覺性。測試接收行為分別有「開啓郵件」、「點閱郵件附件或連結」及「點閱簡訊連結」等 3 種。

本次郵件演練部分範圍共計 66 個機關(受測人數共 12,718 位)，開啟郵件有 40 個機關(開啟人數共 509 位)，占演練機關數量之 60.6%，近 3 年開啟郵件比例詳見圖 6；點閱連結/附件有 36 個機關，占演練機關數量 54.5%，近 3 年點閱連結及附件比例詳見圖 7。簡訊演練部分範圍共計 65 個機關，點閱簡訊連結有 30 個機關，占演練機關數量 46.2%，近 3 年點閱簡訊比例詳見圖 8。

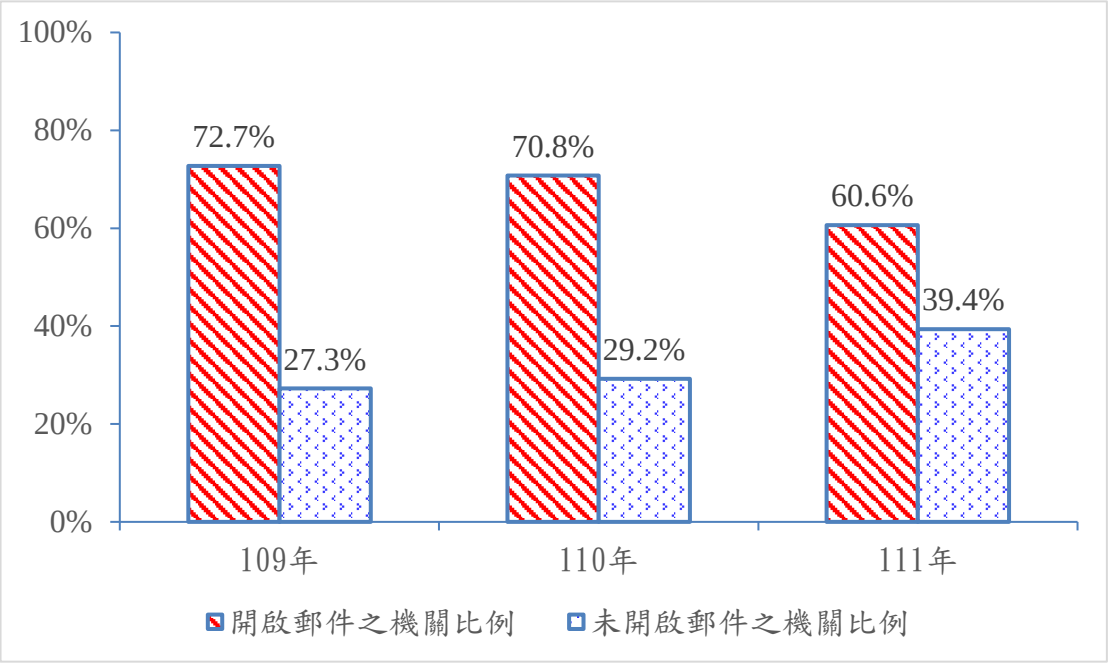


圖 6　開啟郵件機關比例圖

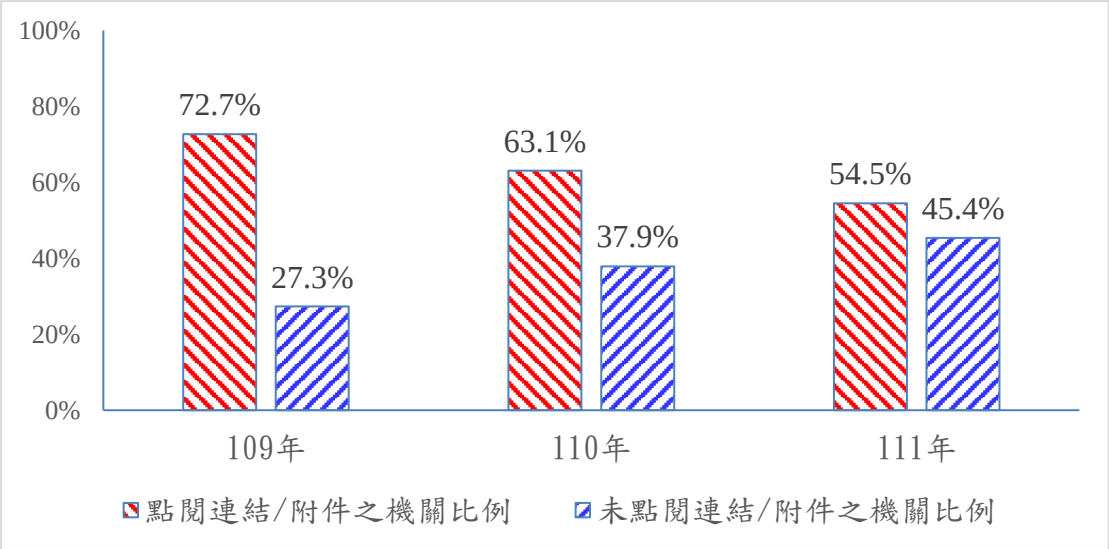


圖 7　點閱郵件連結/附件機關比例圖

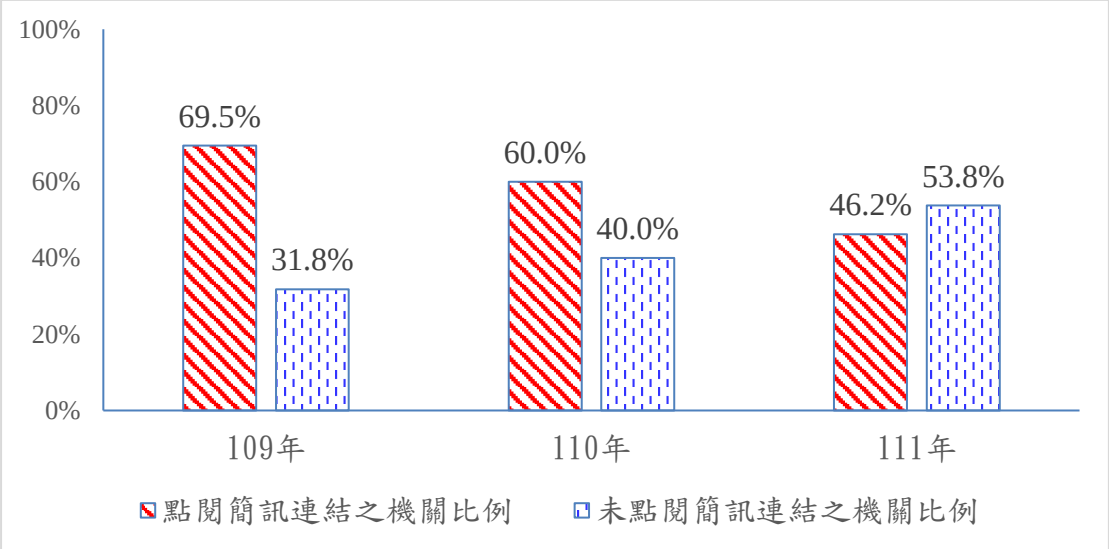


圖 8　點閱簡訊機關比例圖

隨著行動式設備之普及，從演練結果之點閱簡訊連結機關數來看，近 3 年有逐漸減少之趨勢，顯示機關對社交工程攻擊之警覺性，已不限於電子郵件，應宣導教育使用者於使用行動式設備或收取相關簡訊時，應小心求證以免遭受社交工程的攻擊。

四、資安稽核作業

為協助政府機關了解其資安防護之完備與效度，依據資通安全管理法及其子法、資訊安全管理系統國家標準、受稽機關之資通安全維護計畫及實施情形等，據以規劃稽核項目，並採取實地稽核方式進行檢視作業。

111 年依遴選原則從中遴選 23 個受稽機關，包含 17 個公務機關及 6 個特定非公務機關，分季執行稽核作業。稽核小組由稽核領隊、稽核委員、技術檢測人員、工作人員組成，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。

經檢視實地稽核個別項目成績分布，詳見圖 9，其策略面、管理面及技術面在整體表現平均，其中「資通安全政策及推動組織」表現最好；「資訊及資通系統盤點及風險評估」成績最低，仍待改善。

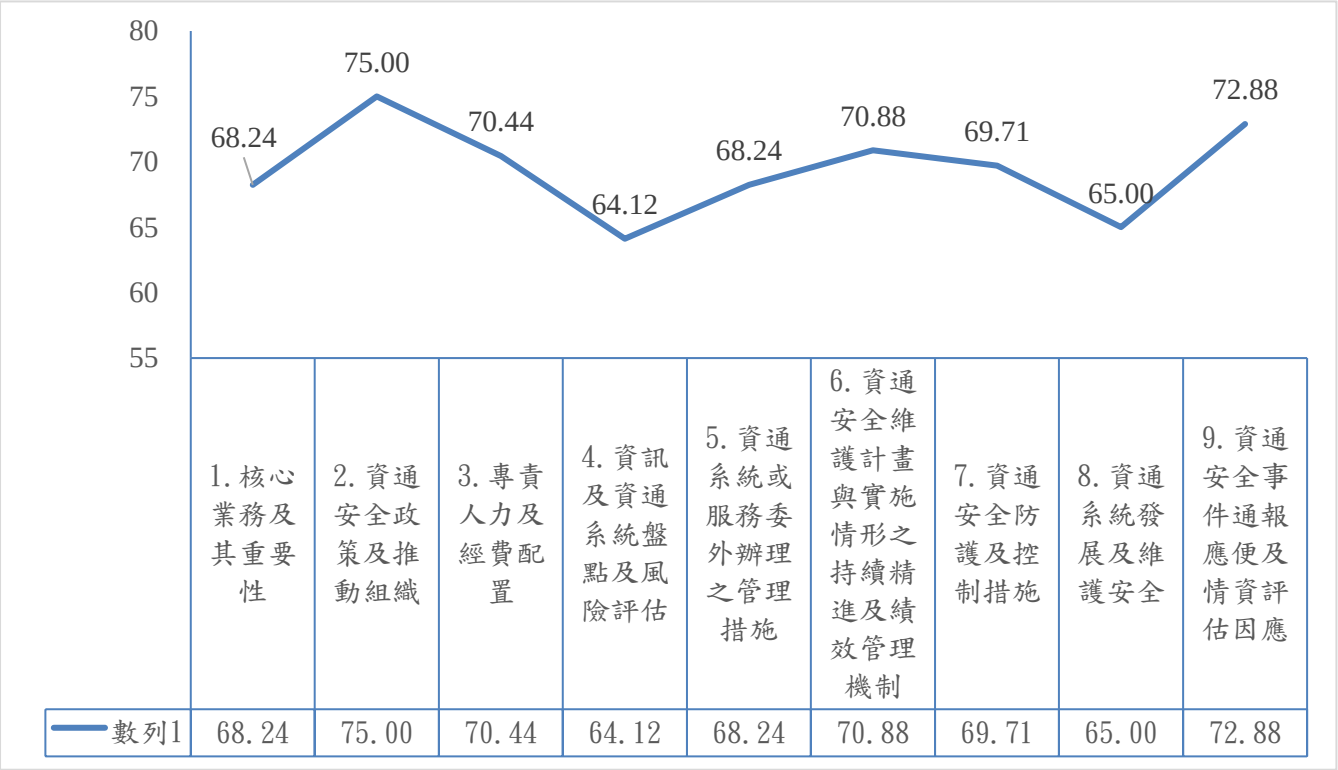
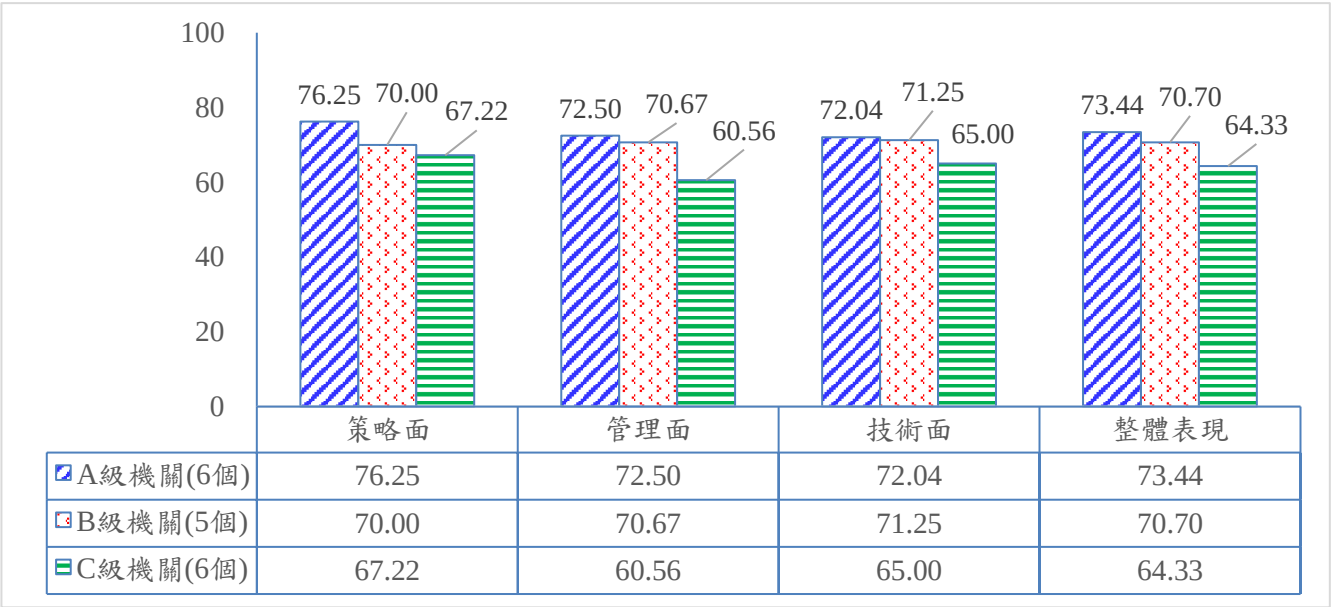


圖 9　公務機關實地稽核個別項目成績分布圖

綜合分析實地稽核各構面(策略面、管理面及技術面)之表現情形，詳

見圖 10。



	策略面	管理面	技術面	整體表現
A級機關(6個)	76.25	72.50	72.04	73.44
B級機關(5個)	70.00	70.67	71.25	70.70
C級機關(6個)	67.22	60.56	65.00	64.33

圖 10　公務機關實地稽核個別項目成績分布圖

五、資安事件通報

資安法納管機關應依「資通安全管理法」之子法「資通安全事件通報及應變辦法」規定，協助公務機關與特定非公務機關處理資安事件，並提供機關資安事件通報窗口、資安事件通報諮詢管道、資安事件損害管制建議，以及資安事件處理建議。

統計 111 年期間，公務機關與特定非公務機關(公營事業、財團法人及關鍵基礎設施提供者)通報之資安事件共 765 件。1 級事件占 79.47%(608 件)，2 級事件佔 15.69%(120 件)，3 級事件佔 4.83%(37 件)，無 4 級事件，事件影響等級比例圖，詳見圖 11

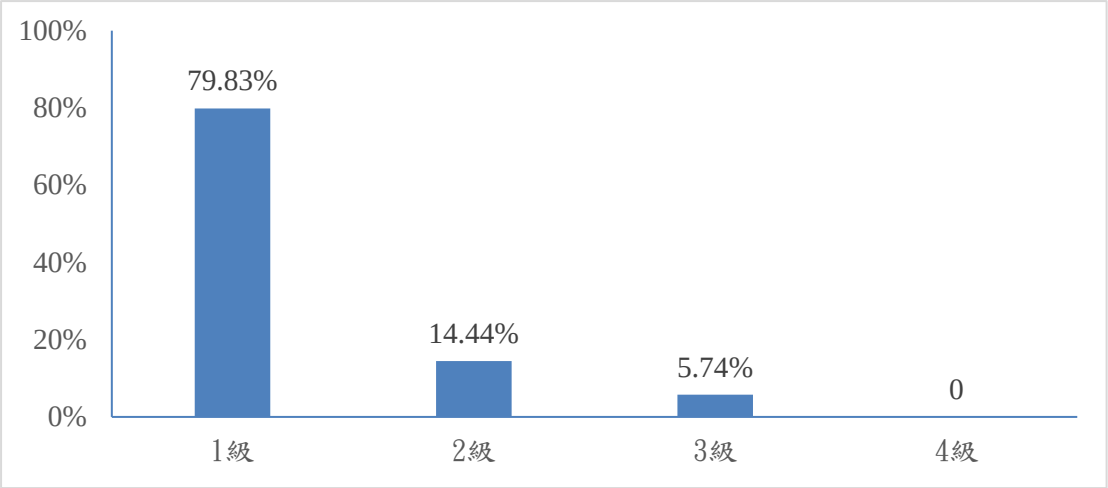


圖 11　事件影響等級比例圖

3 級事件以資料外洩事件居多，其中遭網路攻防演練成功攻擊「認證及驗證機制失效」、「注入攻擊」、「無效的存取控管」及「不安全的組態設定」等弱點，造成機密性衝擊為大宗；因可用性衝擊而通報 3 級事件則是以特定非公務機關為主，肇因多為設備異常或故障影響涉及關鍵基礎設施維運之資通系統或業務。

分析通報應變網站所接獲之資安事件通報肇因，排除其他類型後，以非法入侵為主、設備問題次之，各通報類型比例，詳見圖 12。

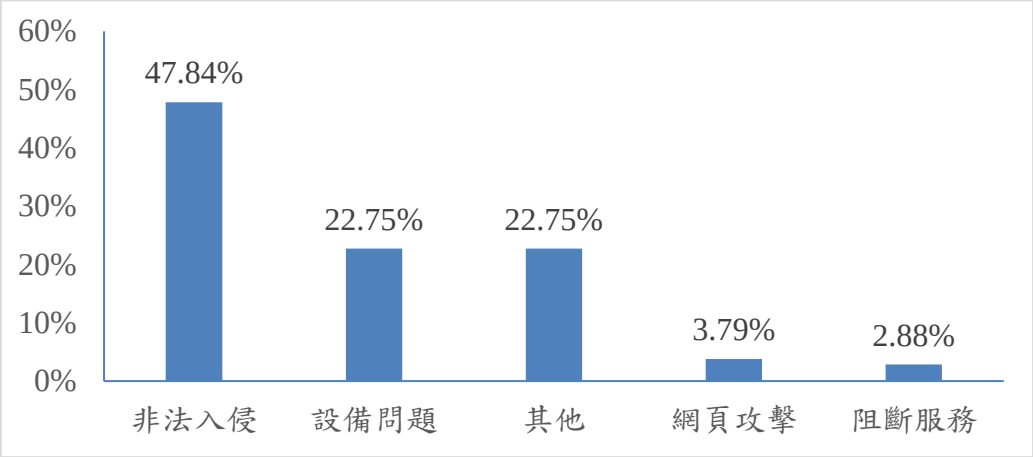


圖 12　通報類型比例

綜整已完成結報之通報案件發生原因，詳見圖 13。

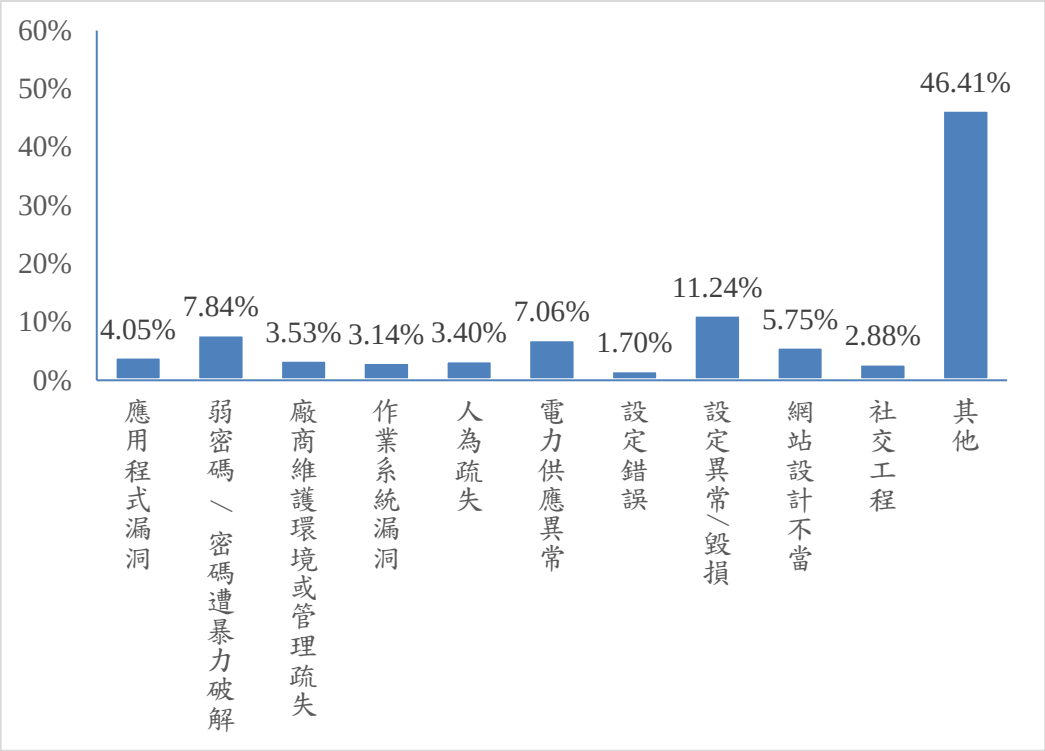


圖 13　通報案件發生原因

在全部事件中，網站設計不當、弱密碼或密碼遭暴力破解，以及設備異常或毀損占資安事件發之前三名。

肆、政府資通安全威脅情勢與防護建議

一、雲端服務應注意防範駭客利用其掩護非法行為

雲端服務因其便利與擴展性，越來越多組織將營運架構移轉至雲端，使用者亦越來越習慣將資訊放置雲端儲存；俄烏戰爭中，烏克蘭政府將數據轉移到雲端，透過公共雲或位於歐洲各地的數據中心，保存重要關鍵資訊，從而維持其軍事行動及民生營運，提升政府數位韌性。

當眾多雲端服務可供選用，許多挑戰也接踵而來，包含各雲端服務平台之安全性、管理組態設定及存取權限等議題。特別是自新冠疫情發展至今，更多的使用者習慣使用雲端服務，導致資料在不經意的情況下外洩，例如某機關人員使用私人電腦安裝雲端同步軟體，透過雲端硬碟服務同步資料至機關外，致使業務相關個資外洩。隨著雲端服務普及與使用範圍擴展，勢必成為駭客鎖定目標之一。

政府機關相關事件案例發現攻擊者會使用雲端服務架設中繼站，藉此規避防護阻擋並隱匿行蹤。111 年 7 月經偵測發現某機關遭駭客利用紅隊演練工具，產製 Cobalt Strike 後門工具程式，再搭配雲端服務建置中繼站，使用合法 IP 位址與域名進行惡意行為，透過域名隱匿(DNS Tunneling)與 HTTP Beacon 通訊兩種方式，將惡意傳輸流量隱藏於合法流量中，使資安防護偵測機制無從察覺其惡意行為。

針對本案例之資安防護，建議部署具備內容分析之資安偵測機制，協助察覺網路或應用程式試圖規避偵測之惡意行為，並定期檢視網路可疑連線。網站或系統主機應定期進行作業系統更新、啟用作業系統防火牆功能、安裝防毒軟體並定期更新病毒碼。另針對雲端服務之存取行為建立控管機制，並訂定一致性之安全組態設定規則，如機敏資料放置雲端時，應採取加密機制，確保其機密性。

二、資料外洩仍為重要處理議題

新冠疫情期間，駭客利用社交工程手法，偽冒政府機關大規模散布假衛福部紓困訊息，藉以騙取民眾身分個資與網路銀行資訊；分析111年通報之3級資安通報事件，資料外洩案件仍佔多數，主要原因包含人員資安意識不足、不當操作或設定、誤將未遮蔽之個人資料公開或錯置於未限制存取之公開區域等。

例如某機關委託廠商辦理競賽活動，並提供活動資訊，欄位包含參賽人員姓名與行動電話號碼等，廠商工作人員為協助宣傳活動成果，將參賽人員資訊上傳至個人公開網站，造成個資外洩；某機關透過臉書(Facebook)粉絲專頁宣導活動資訊，並利用Message接收報名資訊，惟粉絲專頁管理員疑似遭社交工程攻擊成功，導致帳號密碼外洩，進而造成民眾個資外洩疑慮。亦有違反資訊安全規定之離職人員，濫用存取權限，擅自下載機關持有的民眾個人資料並試圖於社交平台兜售。

111年10月媒體披露2300萬筆戶籍資料遭上網販售，經比對資料欄位、資料編碼與格式，部分與戶役政系統原始資料有所出入，惟因已無107年追查數位跡證資料，致未能釐清外洩原因，但仍應盤點可能的脆弱點，再予強化。針對持有全國性資料之彙整機關，建議強化以下作為：

- 連結機關：盤點介接機關，要求資安作為(如比照A、B級機關)、加強稽核、取消離線媒體交換(如光碟等)。
- 資料保護：資料加密儲存、查詢過程遮蔽及最少揭露、大量資料查詢之審核預警機制、資料查詢日誌查核。
- 使用權限：個人資料蒐集，應以最小且必要為原則，限縮申請項目及內容、職務異動即時清除權限。
- 核心系統納入資安威脅偵測管理(SOC)、導入端點偵測及應變機制

(EDR)，定期檢視存取日誌，以及早預警。

- 強化使用者資安及資料保護意識，若需上傳至公開網站，應確認機敏等級與保護措施，並訂定適當存取權限，定期清查系統帳號權限及使用狀況。

三、萬物聯網衍生資安風險應納入資安防護規劃

萬物聯網時代，可聯網設備多樣且應用廣泛，使用者包含管理階層、資訊人員及一般使用者。因此全面提升資安意識，將是未來在規劃教育訓練時不可或缺之要點。同時，針對繁多的物聯網設備種類，其安全性之要求或檢測亦應列為採購前或使用時定期檢視之重點。

相關案例偵測發現政府機關多個網路服務暴露於網際網路上，111 年 9 月，經偵測發現某機關設備有異常連線行為，進一步確認時發現該機關受駭設備為門禁系統，且存在身分驗證繞過漏洞，駭客透過該漏洞入侵設備，並安裝惡意程式。

另如 RDP、VNC 及 Telnet 等遠端管理通訊協定，以及機關架設之智能設備管理系統，其資料庫管理系統 phpMyAdmin 介面直接暴露於公開網路中，如此一來，很有可能被駭客鎖定致遭受大量遠端服務暴力破解與弱點探測，進而可能入侵相關設備造成內部橫向感染擴散。

同時，在機關所架設之智能設備管理系統服務發現，除可於網際網路直接存取相關服務與 phpMyAdmin 資料庫管理介面外，其中 phpMyAdmin 後台頁面存在使用預設密碼之狀況，外部人士可藉由預設密碼登入系統並存取與控制相關裝置，顯示管理人員在架設相關系統前，並未針對所管理系統在需求或建置階段定義清楚之資安需求。

建議機關應於系統管理介面建立適當並符合資通系統防務基準之控制措施，例如限制使用者設定符合規範之密碼等，以降低被外部

入侵之風險，同時應將相關設備納入資安監控範圍，監測網路活動日誌，並定期檢視存取權限與使用行為。

另機關應定期盤點 IT 與 OT 資產、防火牆規則，依循資安政策限制外部存取，檢討遠端服務連線之必要性，並納入風險評估，定期檢測系統漏洞、檢視防火牆規則更新情形，以降低不必要的風險產生。

四、應強化供應商資安管理，以免波及委託機關

政府機關通報之資安事件中，其中廠商維護環境或管理疏失占3.53%，供應鏈安全落差亦應列為政府機關關注之議題，以避免供應商遭鎖定為攻擊目標後，成為駭客入侵政府機關之跳板，並橫向感染而波及政府機關。

某機關之委外廠商人員電腦設備遭入侵，同時被植入惡意程式，該廠商未事先檢測設備安全性，便攜至委託機關連網維護，致機關亦遭植入惡意程式。另有機關委外廠商遠端 VPN 連線維護之電腦，亦有被植入惡意程式情形，致委託機關同時成為受駭者。類似案例尚有廠商電腦因系統未更新，存在安全性漏洞遭利用後，試圖利用網路芳鄰協定對機關內部其他主機進行連線或攻擊行為。

供應商風險逐漸升溫，因此開放供應商連線時，包含遠端或至內部存取系統時，皆應先進行相關風險評估，輔以妥善之管理機制，方能開放存取。

建議機關在委外辦理資通系統之建置、維運或資通服務之提供時，應依資通安全管理法要求，評估及選任適當之受託者，並依訂定之資訊安全服務水準協議，定期監督或稽核其包含組織、人員、實體及技術之資通安全維護情形，另要求廠商依「資通系統籌獲各階段資安強化措施」，於需求、建置及維運階段落實相應資安防護措施。契約結束後，應監督廠商完成資料之返還、移交、刪除或銷毀。

當委外廠商因業務需求申請遠端連線或維護時，其遠端存取開放應採「原則禁止、例外允許」方式，期間則以短天期為原則。遠端連線作業執行前，機關或廠商應將相關連線設備之作業系統與防毒軟體更新至最新版本、更新修補漏洞並針對廠商連線至機關系統之設備進行安全性檢測，以降低遭外部入侵風險。同時，機關應建立異常行為管理機制，檢視遠端存取開放期間之資訊設施活動日誌是否有異常行為，俾利異常行為發生時能及早發現應處。

五、釣魚網站仍是主要攻擊手法，應落實黑名單阻擋並持續加強同仁資安意識

國家資通安全研究院透過觀測政府領域惡意電郵偵測機制，每月所偵測出之可疑惡意電子郵件在所有政府領域電子郵件中約占 1~3%，其中與 IPFS 相關者於 111 年度平均約占 0.2%左右，雖然占比不高，但以長期觀測與統計來看，111 年度使用 IPFS 之釣魚郵件攻擊數量有明顯逐月上升趨勢。

IPFS 為一種去中心化之分散式檔案共享系統協定，不同於傳統集中式主從架構，在伺服器停擺或連線中斷時無法傳輸檔案，IPFS 是根據內容定址、檔案分散儲存在多個網路空間，可以輕易利用多個網路節點傳送檔案，維持其存續性。雖然部分 IPFS 閘道服務商已經開始針對釣魚網頁或惡意程式下載進行過濾阻擋，惟駭客只需要變更 IPFS 閘道，內容定址之 Content ID (CID)不變，則依然可以瀏覽與存取資料，難以阻絕，更無法取締下架。

觀察所偵測到之惡意電子郵件，駭客係透過在 IPFS 上架設與儲存釣魚網站頁面或惡意程式，並偽冒機關名稱與利用「密碼更新或郵件帳號更新」等名義主旨，寄送含有釣魚網站頁面或惡意程式下載連結之社交工程電子郵件，企圖騙取政府機關人員帳號密碼。進一步分

析其攻擊步驟顯示，駭客除利用 IPFS 建立惡意連結，更將該惡意連結利用 Google 網站翻譯服務或是採用 IPFS 的第三方網頁託管服務進行轉址，取得具有合法域名(例如*.translate.goog)與憑證之惡意連結，放入釣魚郵件中散播，便可利用合法掩護非法躲過許多偵測，藉此規避黑名單阻擋與資安防護機制，讓這些惡意連結不僅難以阻絕更加難以偵測。

駭客利用 IPFS 能避免網站遭到分散式阻斷服務攻擊之分散式架構特性，讓所建立之釣魚網站及惡意程式，透過分散式架構散佈在網際網路上，使 IPFS 成為釣魚網站及惡意程式的新溫床，並進一步藉由合法服務轉址導向，躲避 URL 信譽評等、自動化 URL 分析服務的偵測，導致建立在 IPFS 的釣魚網站或惡意程式連結相較傳統集中式主從架構更加難以偵測阻擋。

針對釣魚網站及惡意程式連結之資安防護，建議管理人員應建立網路威脅情資機制，確實更新黑名單，阻擋已被通報之可疑釣魚網站或惡意程式連結。另一方面應強化使用者資安意識，提升訊息辨識及警覺心，於開啟郵件前先行檢視郵件正確性，如：來源電子郵件是否為業務來往之單位、郵件寄件者是否為該單位人員、郵件電子簽章是否有效等，開啟郵件內夾帶連結或開啟一般網頁時，則應確認是否為官方正式網站，留意網頁域名並確認域名正確性。

伍、結語

透由檢視 111 年國內資安威脅情資，本部將持續關注雲端服務遭非法利用之態樣、去中心化的技術可能讓偽冒網站更為猖獗等議題，研議相對之偵測防禦作法；而資料外洩、萬物聯網及供應鏈安全等議題，亦待持續推動各機關落實資安防護作業，以確實降低資安風險。我國政經情勢特殊，除面對全球新興資通訊技術外，尚有較其他國家更為險峻之資安威脅，本部亦將持續研析主動式防禦機制、零信任網路架構等各項資安防護措施，以打造安全可信賴之數位國家。