112 年度國家資通安全情勢報告

數位發展部

中華民國 113 年 7 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」。

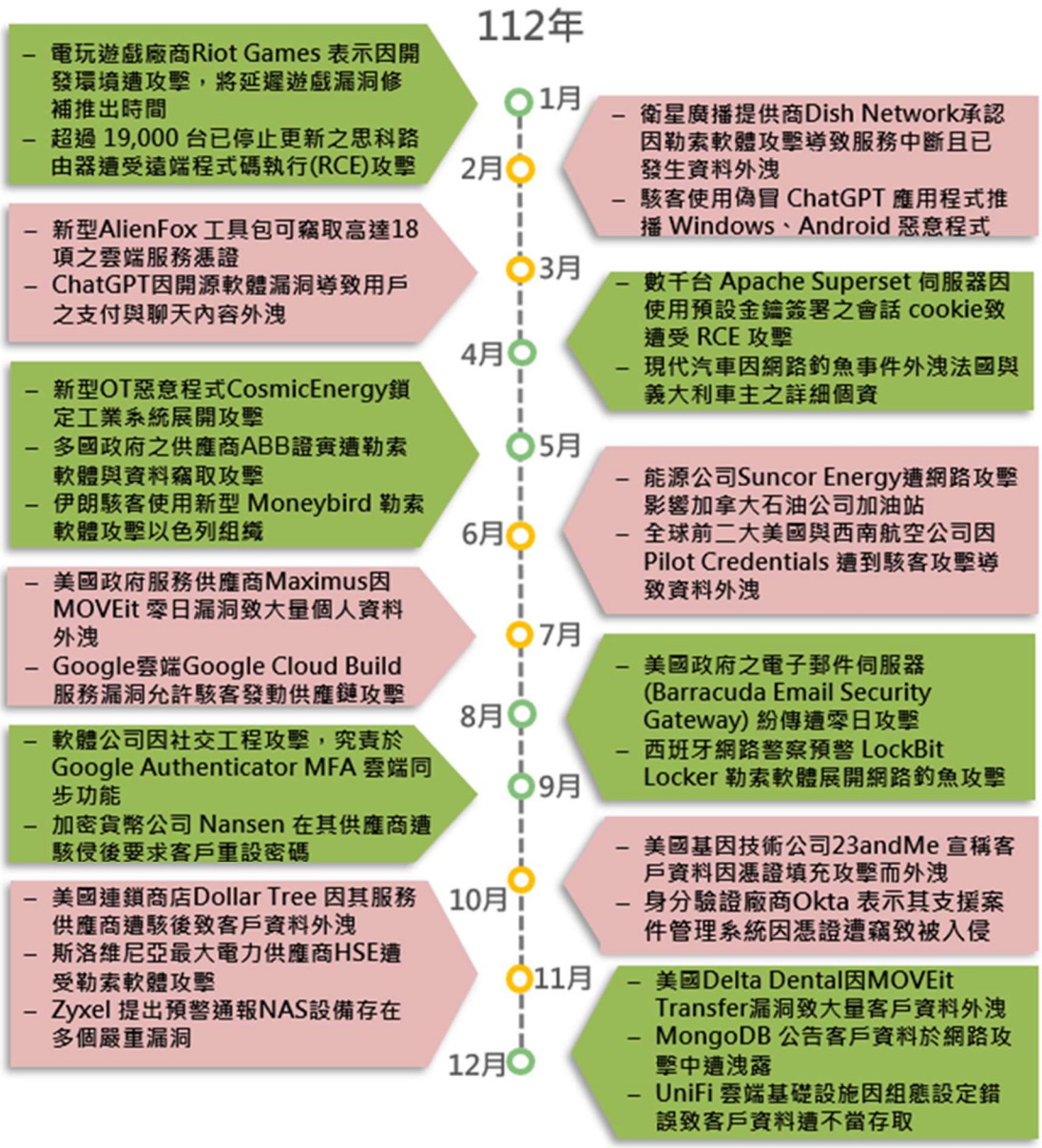
隨著世界衛生組織在 112 年宣布 COVID-19 疫情結束，各項活動蓬勃發展，而俄烏及以哈的衝突，各方支持勢力也讓網路攻擊升溫，另一方面在人工智慧技術越趨成熟下，豐富多樣的新興科技應用，亦衍生對應的資安挑戰及威脅。各界仍需於現有的防護整備下，持續加強偵測及防護。本報告透由研析 112 年全球資通安全威脅情勢及我國政府機關所面臨之資通安全威脅現況，研提相關資安防護建議，協助各機關強化資通安全防護意識，期前瞻擘劃及強化國家整體資源力量，打造安全可信賴之數位國家。

貳、112 年全球資安威脅情勢概要

世界經濟論壇(World Economic Forum, WEF)於「全球 113 年風險報告」(Global Risks Report 2024)中指出，可能引發全球重大危機之前 5 大風險分別為「極端氣候」、「人工智慧技術所生之錯誤訊息與虛假訊息」、「社會或政治兩極化」、「生活成本危機」及「網路攻擊」；在 10 年內可能最嚴重的風險裡，新增「人工智慧技術之不利後果」，且其長期風險更超越「不安全的網路環境」。

越來越容易使用之人工智慧模型介面與平台，衍生偽冒網站、影音及許多生成式 AI 產出的大量仿真訊息，Google Cloud 團隊於 113 年網路安全預測報告(Cybersecurity Forecast 2024)中指出生成式 AI 與大型語言模型即服務(Gen AI and LLMs(Large Language Models) as a Service)可能被用於駭客攻擊活動造成威脅，且已觀察到駭客利用由暗網取得之生成式 AI 服務相關產品，用於社交工程相關攻擊。攻擊者藉由生成式 AI 產生偽冒之文字資訊、聲音或影像，再結合所蒐集之大量資訊攻擊手段，除造成信任危機，也提升檢測與防範之挑戰與難度，故於持續關注網路安全議題外，需全面觀察網路攻擊趨勢之變化，深入了解駭客攻擊手法及入侵之脆弱點，規劃推動對應之防護措施。

分析與綜整 112 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1　112 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)、澳洲網路安全中心(Australian Cyber Security Centre, ACSC)及各資安業者調查等報告資料，112 年全球資安威脅情勢可歸納為 6 大面向，包含「個人資料與憑證外洩致防護機制失效」、「資通系統弱點頻遭揭露利用」、「生成式 AI 致 APT 鎖定與勒索軟體風險增加」、「資安(訊)供應商遭駭破壞邊界防護」、「關鍵資訊基礎設施與 OT(Operational Technology)攻擊面向增加」及「雲端應用服務衍生多元威脅」。

一、個人資料與憑證外洩致防護機制失效

根據 IBM 112 年資料外洩成本報告(Cost of a Data Breach Report 2023)，資料外洩於 112 年平均成本高達 445 萬美元，相較 111 年增加 2.3%，呈現逐年增長趨勢。因資料外洩事件偵測不易，報告統計分析發現高達 67%是由善意第三方通報或由攻擊者下一波惡意動作揭露，僅有 1/3 是由組織自行發現。資料外洩發生主因是網路釣魚、憑證遭竊或洩漏，其中 112 年網路釣魚占首位，而 111 年則為憑證遭竊居多，其他原因依序為雲端組態配置錯誤、商業電子郵件洩漏及系統漏洞。報告另指出惡意內部人員造成資料外洩發生率約 6%，雖相對機率較低，但所致損失卻最高，平均為 490 萬美元，比每次資料外洩之全球平均成本高出 9.6 %。

在資料外洩案例中，基因檢測服務商 23andMe 因大規模資料外洩，據媒體揭露影響數百萬位客戶。駭客入侵成功後將一份名為「Ashkenazi DNA Data of Celebrities.csv」客戶資料公布於駭客論壇，被公開資料包含 DNA 設定之機敏資料。調查後發現，本次 23andMe 事件為駭客使用憑證填充攻擊，進而合法存取該平台，且因該外洩資料檔與其他檔案無完善權限存取原則，導致連結至更多資料。因此，完善存取控制與帳密防護是強化資安防護之關鍵要素。

二、資通系統弱點頻遭揭露利用

依據弱點遭利用情形、漏洞修補率、漏洞存活期間及平均反應/修復時間(MTTR, Mean Time to Respond/Remediate)等項目評估後，資安廠商 Qualys 公布 112 年前十大被利用之漏洞，部分系統漏洞修補率尚未達五成，顯示組織對系統存在弱點之風險及應對處置措施，有待強化。另部分漏洞無法歸類或對應至已知威脅實體或團體，其潛在或新興威脅更應警惕應對，防止駭客組織或惡意人士透過工具搜尋暴露公開網路中之系統服務弱點，加以利用。

一位資安研究員在 111 年 11 月揭露某汽車業者網路應用系統存在嚴重漏洞，該系統允許員工和供應商遠端登錄，並管理公司的全球供應鏈，駭客僅需得知其中 1 個系統使用者之電子郵件帳號便可成功取得該系統之控制權。該研究員在 1 次測試入侵中，發現此漏洞可任

意存取系統內超過 1 萬多家供應夥伴之資訊，包含帳號細節、機密文件、專案資料及供應商排行與評論等敏感訊息。

上述汽車業者提供採 Angular JavaScript 架構設計之 APP，可藉由使用特定的路徑與功能，決定使用者頁面存取，此漏洞允許透過修改 JavaScript 以任意存取頁面；而透過 JSON Web Token (JWT)身分驗證機制，只需輸入任一汽車業者有效之員工帳號，不需密碼即可登入，後續再透過系統 API 漏洞，可允許入侵者成功創建立使用者帳號後，再切換成具特權管理之帳號。該汽車業者於 111 年發生數起資安供應鏈遭駭事件，包含對其供應鏈之網路攻擊與官方連接應用程式 GitHub 儲存庫(Repository)遭揭露。因此，為避免漏洞造成損失擴大，建議各機關組織應快速修補漏洞或實施強化控制措施。

三、生成式 AI 致 APT 鎖定與勒索軟體風險增加

Google 公司 113 年網路安全預測運用生成式 AI(Artificial Intelligence)與 LLMs(Large Language Models)將使網路釣魚活動更加專業，藉由人工智慧與巨量資料衍生之攻擊手法與策略，可將以往之拼字或語法錯誤加以修飾，並客製化成擬真之偽冒訊息以精準攻擊鎖定目標。另 ENISA 112 年威脅情勢(Threat Landscape 2023)分析勒索軟體攻擊事件，發現駭客使用動態策略擴散攻勢，透過經常變更主機名稱、路徑、檔名等多種組合以擴散勒索軟體，該報告提到經 Palo Alto

Unit 42 團隊分析 111 年勒索軟體樣本，以往採電子郵件附件為主要傳播勒索軟體之媒介，傳播方式已改變為透過 URL 連結與網頁瀏覽，約占勒索軟體之案例七成以上。

此類資安事件案例中，資安業者 SlashNext 揭露駭客於暗網與社群媒體平台積極推銷 AI 網路犯罪惡意程式 WormGPT 與 FraudGPT，購買者可輕易使用該工具展開網路釣魚攻擊活動。WormGPT 開發者宣稱該工具為利用 OpenAI 開發之人工智慧聊天機器人，可模擬人類思維設計詐騙訊息，其功能包含能模擬人類思維設計仿真訊息、模仿合作夥伴支付款項或變更交易事項等，該軟體發展目的應為發展網路釣魚電子郵件與商業電子郵件詐騙攻擊，其後，陸續於市場上發現其他款 AI 網路犯罪惡意程式，如 FraudGPT。

另一資安業者 Netenrich 揭露暗網註冊名稱 CanadianKingpin12 之使用者於暗網與社群平台，鎖定網路詐騙者、駭客及垃圾郵件寄送業者行銷其 AI 網路犯罪惡意程式，依其展示可見 AI 網路犯罪惡意程式提供數項功能，包含提供零時差攻擊弱點、協助執行進階社交工程攻擊、揭露一般與關鍵基礎設施等資通系統弱點、提供與製造惡意程式，並且針對勒索軟體攻擊設計發展複雜之網路釣魚活動。該 AI 網路犯罪惡意程式服務之使用者於訂閱後，即能藉由所提供之惡意程式碼、網路釣魚網頁、駭客攻擊工具及系統漏洞輕易發動攻擊，甚至協

助尋找具代表或指標性之服務網站，以精準詐騙更多受害者，其功能亦包含避免被偵測或潛藏軌跡等。此外，隨 AI 網路犯罪惡意程式發展趨勢，針對該類惡意程式開發人員之便利性，亦提供應用程式介面(Application Programming Interface, API)存取，簡化工具整合至惡意使用者之作業流程與程式碼，可能使這類攻擊案例數量上升。

因社交工程入侵工具唾手可得，新興科技將使其攻擊更加專業與便利，搭配各種即服務(as a Service)將推波助瀾攻擊活動，使駭客蒐集系統或漏洞情資更為容易。因此，除提升人員資安意識外，如何第一時間在各個端點偵測、辨識與攔截惡意行為刻不容緩。

四、資安(訊)供應商遭駭破壞邊界防護

依據 Gartner 預測，到 114 年全球約有 45%組織會因軟體供應鏈而遭攻擊，另根據網路安全廠商 Cybersecurity Ventures 發表軟體供應鏈入侵報告(2023 Software Supply Chian Attack Report)預測，至 120 年全球因軟體鏈攻擊事件對組織所造成損失將高達 1,380 億美元。該報告中引述 Juniper Research 研究數據，112 年因軟體鏈攻擊事件經濟損失近 460 億美元，預測 3 年後更將驚人地再增加超過 80 億美元。在最常見入侵手法中，社交工程與網路釣魚是藉由竊取憑證、入侵開發流程之持續整合與持續交付(Continuous Integration/Continuous Delivery, CI/CD)、系統漏洞或開源軟體之元件、偽冒網域名稱或內部

人員威脅等方式入侵，軟體供應鏈可能是發動前述攻擊威脅之管道。

在 112 年供應商發生資安事件案例中，美國某家媒體公司因遭俄羅斯駭客組織 TA569 入侵，並利用該新聞網站散布惡意軟體 SocGholish 引發後續供應鏈攻擊危機，資安廠商 Proofpoint 表示該媒體公司主要透過 JavaScript 指令碼提供其他媒體新聞網站影音內容與廣告。駭客藉竄改該 JavaScript 之基礎程式碼(Codebase)，進而部署惡意程式 SocGholish 執行偽冒假更新(FakeUpdates)，後續引發供應鏈風波並影響逾 250 家新聞網站。經 Proofpoint 追蹤顯示遭供應鏈攻擊之受駭者遭植入惡意軟體，駭客以瀏覽器更新名義，如 Chrome.Updater.zip、Firefox.Update. zip、Opera.Update.zip 等，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，同時 Proofpoint 觀察到受駭者修復數日後又再次遭植入相同惡意軟體。因 FakeUpdates 入侵方式常採取保守策略窺探與篩選其潛在目標，並藉由受駭者瀏覽器 Firefox、Chrome 或 Flash 等更新機制，非貿然一次性對大量目標釋出偽冒假更新，使受駭者通常無法於第一時間警覺發現，導致該類事件重覆上演。因此，為降低因供應商遭駭侵而受到波及的程度，建議宜適當供應商端之資安防護檢測，而非無條件信任。

五、關鍵資訊基礎設施與 OT 攻擊面向增加

工業網路社區(Industrial Cyber Community)論壇指出美國關鍵基

礎設施 112 年面臨之網路威脅遽增，尤其是醫療健康與供水設施，其呼籲相關部門應採取行動且加強防範措施以因應相關攻擊。美國政府部門，如國土安全部(Department of Homeland Security, DHS)、網路安全與基礎設施安全局(Cybersecurity and Infrastructure Security Agency, CISA)以及聯邦緊急事務管理局(Federal Emergency Management Agency, FEMA)等，因發現關鍵基礎設施威脅而公布發展護盾就緒(Shields Ready)行動，藉以要求關鍵基礎設施所有利害關係者提出具體防禦計畫時程以降低特定威脅風險。

此外，自俄烏戰爭起，關鍵基礎設施多為主要攻擊目標，鎖定水壩、火力、核電廠等設施企圖造成恐慌，更可能引發更多衝擊；而這些攻擊活動，除持續實體戰爭外，亦利用系統入侵同步展開網路戰爭。

關鍵基礎設施相關資安事件中，美國 CISA 發出警訊提醒入侵者正透過侵入暴露於公眾網路上 Unitronics 可程式化邏輯控制器(Programmable Logic Controller, PLC)嘗試破壞該國供水設施。據報導，賓州水務局遭到中東網路駭客組織 Cyber Av3ngers 攻擊，該組織過往專門鎖定以色列水處理供應站，而這波攻擊活動中，則針對以色列與美國等多處供水站。賓州水務局發現此次入侵活動，已能控制該局管理範圍內 2 個城鎮遠端加壓站，因攻擊活動觸發警訊已即時回應處理，並於事發之際緊急停用系統且切換手動操作，經內部評估後對供

水或飲用水現況皆安全無虞。本次攻擊受感染的 Unitronics PLC 屬於工控環境中關鍵之控制與管理設備，其操作包含中斷供水、水泵超載或開關閥門等，駭客取得控制權後可遠端操控設備。該資安事件經調查後，據初步評估駭客是透過 Unitronics PLC 人機介面(Human Machine Interface, HMI)預設密碼未修改所致。

據統計數據，關鍵資訊基礎設施與 OT 攻擊資安事件雖非主流攻擊，惟此類攻擊之影響與衝擊將難以估計，因此在關鍵資訊基礎設施部份資料從封閉網路傳輸外部網路之際，除正視 IT 管理外，應加強分析與因應 OT 面向攻擊。

六、雲端應用服務衍生多元威脅

根據資安廠商 Thales 112 年雲端安全研究報告(2023 Cloud Security Study)，調查有超過 3/4 受訪者表示有 2 個以上雲端服務供應商，組織擁有多個雲端服務供應商已成趨勢。針對機敏資訊置於雲端情形，110 年調查有 49%受訪者表示會將機敏資訊置於雲端，而 112 年則增加至 75%；受訪者表示平均約 40%之機敏資訊置於雲端，當中平均只有 45%之機敏資料被加密。雖只有部分機敏資料經過加密，但超過五成受訪者表示雲端架構複雜，其管理與操作資料更加不易，導致雲端資料外洩主因多為人為錯誤。

雲端應用服務資安事件中，全球網路通訊技術廠商 Ubiquiti 發生

因雲端組態設定錯誤遭不當存取客戶資訊，該公司為全球知名且市占率高之網路設備製造商，管理者可透過其雲端 UniFi 平台單一登入管理自身的設備。該事件是由其客戶通報可透過該公司 UniFi Protect 雲端服務收到來自其他使用者攝影監視器之錯誤通知，經由此監視設備可意外看見其他使用者之監視影像，並窺見其他用戶之設備與通知事項。此外，另有某客戶反應當登入 UniFi Site Manager 管理其設備時，可同時瀏覽另一位客戶幾近百台設備，因同時具存取權限表示亦可輕易變更其他人之網路設備配置。回報該問題之客戶於社群媒體 Reddit 平台提出疑義，經 Ubiquiti 調查後，表示其 UniFi 雲端基礎設施於升級過程未設定正確組態，導致不同群組客戶間錯誤關聯，致使可存取他人資訊。因此使用者如有隱私外洩疑慮，建議應先關閉雲端功能，之後可啟用雙重驗證機制避免其隱私或資料被侵犯或濫用。

參、112 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)回傳之資安監控情資進行資安威脅種類，掌握整體資安威脅類別及趨勢，透過資安聯防監控月報提供威脅情資、政府資安監測預警與服務，強化整體資安聯防作業。

112 年彙整之監控情資，依資安威脅類別區分為惡意內容、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，第 1 名為資訊蒐集(41.6%)，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料蒐集行為；第 2 名為入侵嘗試(25.4%)，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與服務之嘗試；而第 3 名為入侵攻擊(20.2%)，主要為針對系統與服務成功破壞行為，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，各類資安威脅分布詳見圖 2。

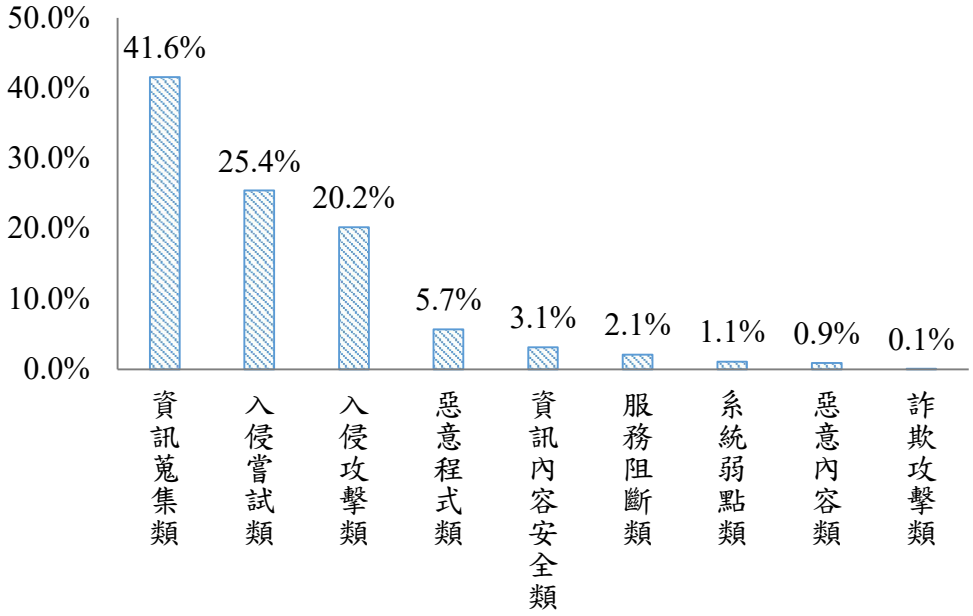


圖2　各類資安威脅分布圖

二、惡意電子郵件分析

惡意電子郵件一直是政府機關主要資安威脅來源之一，當中以「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。112 年共檢測 3.7 億餘(378,784,437)封電子郵件，分析其行為資訊，發現可疑惡意電子郵件 781 萬餘(7,810,205)封電子郵件約占整體之 2%，詳見圖 3；另分析電子郵件之惡意檔案類型比例前 3 名分別為 RAR、ZIP 及 RTF document，皆屬政府機關常接收之檔案類型，駭客藉此類常見檔案，以降低使用者警覺。

分析攻擊手法後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，例如：第三方免費架站服務、線上表單服務及 Google 網站翻譯服務轉址功能等，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密碼以取得機敏資訊。

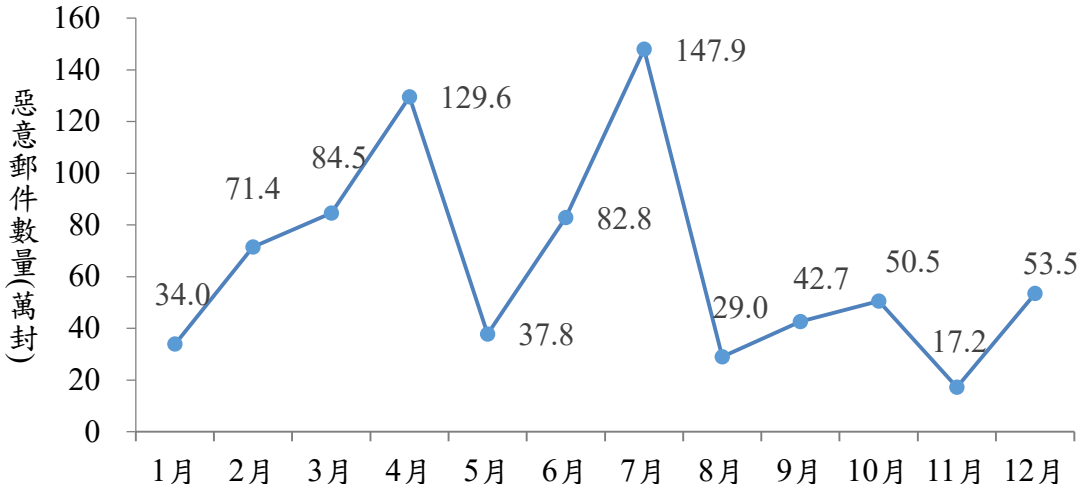


圖3　112 年政府骨幹每月惡意電子郵件偵測數量

三、資安攻防演練

為強化機關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，112 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，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；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。112 年計 72 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，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，藉以測試機關偵測及通報應變能力。

112 年度網路攻防演練 72 個機關 3,461 個對外系統，演練結果發現 43 個機關對外資通系統存在弱點，占演練機關總數 59.72%，詳見圖 4。

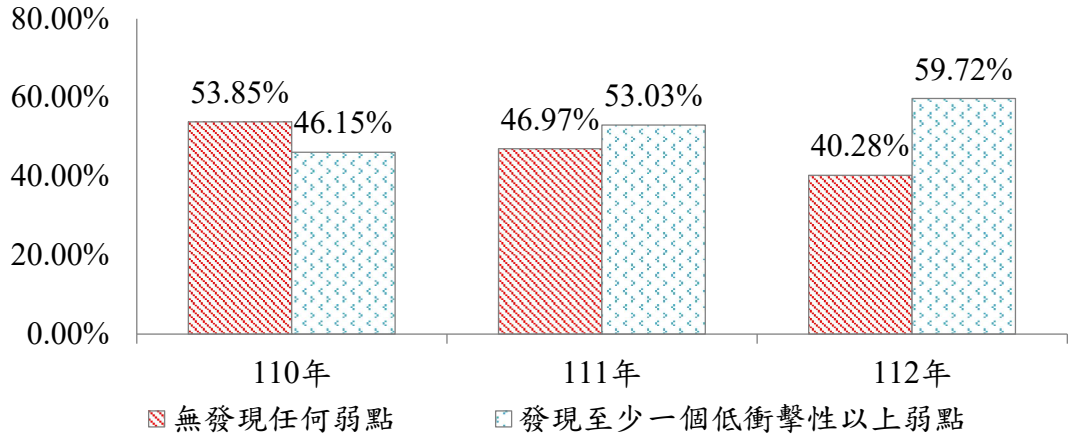


圖4　發現弱點機關比例

針對機關存在之資通系統弱點，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。112 年度網路攻防演練共發現 228 個弱點，其中重大衝擊性弱點數量 10 個，占整體弱點數量 4.39%，高衝擊性弱點數量 59 個，占整體弱點數量 25.88%；中衝擊性弱點數量 29 個，占整體弱點數量 12.72%；低衝擊性弱點數量 130 個，占整體弱點數量 57.02%，詳見圖 5。

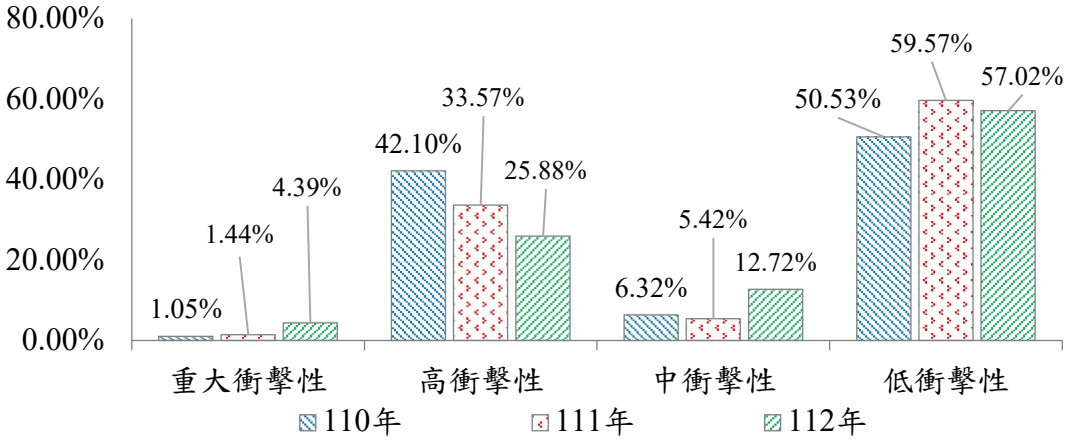


圖5　弱點衝擊性比例分布圖

(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。

112 年電子郵件演練 72 個機關，受測人數計有 2 萬 404 位，45 個機關開啟郵件，占演練機關數量之 62.5%，近 3 年開啟郵件機關比例詳見圖 6；有 42 個機關點閱連結/附件，占演練機關數量 58.33%，近 3 年點閱連結及附件比例詳見圖 7；簡訊演練 71 個機關，有 32 個機關點閱簡訊連結，占演練機關數量 45.07%，近 3 年點閱簡訊比例詳見圖 8。

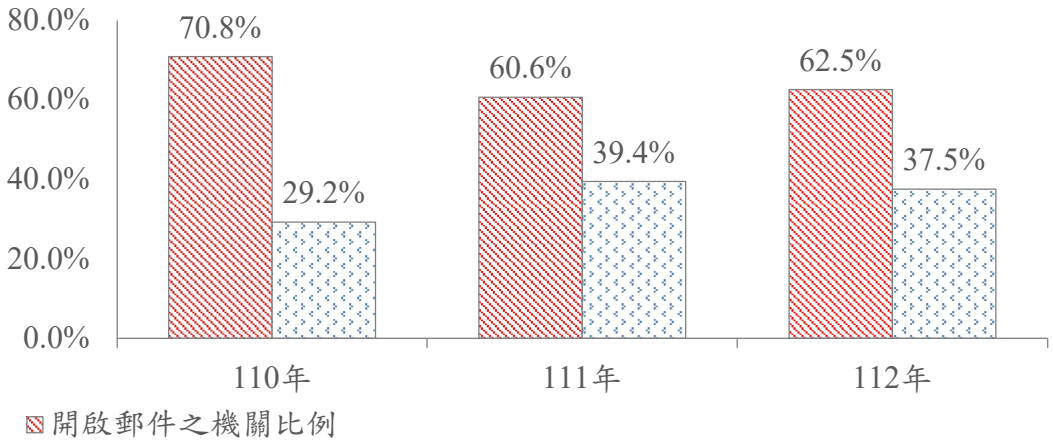


圖6　開啟郵件機關比例圖

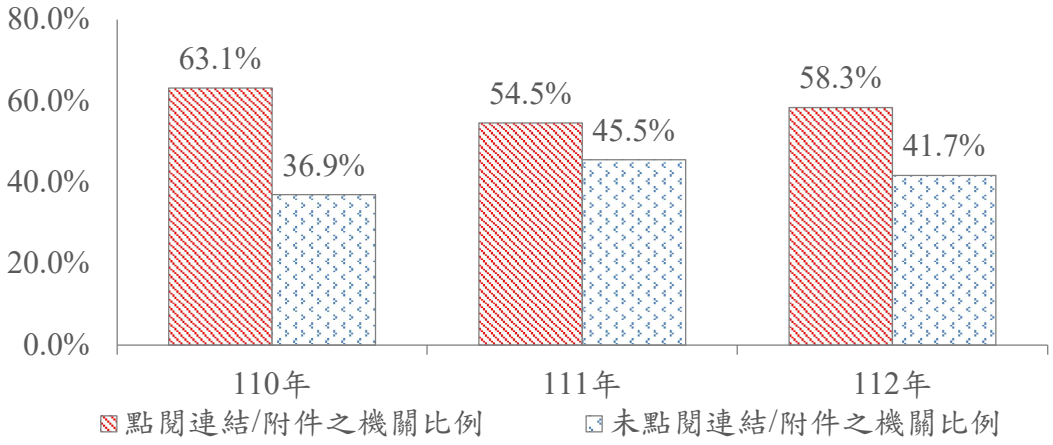


圖7　點閱郵件連結/附件機關比例圖

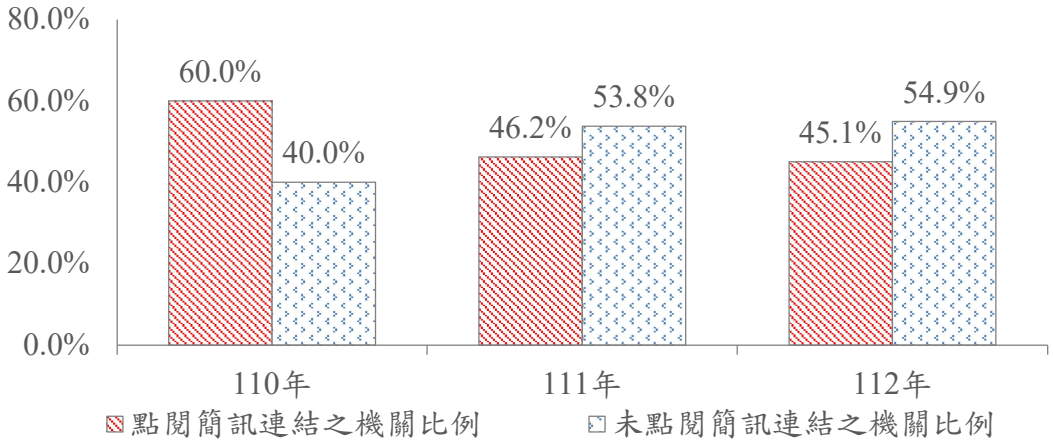


圖8　點閱簡訊機關比例圖

112 年度郵件演練樣本納入擬真公務類型郵件，112 年的社交工程點演練結果，其中開啟郵件及點閱郵件連結/附件比例雖略高於 111 年，惟未有明顯增加，未來仍應持續宣導教育使用者收取郵件或簡訊時，應小心求證以降低資安風險。

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。

112 年遴選 40 個受稽機關，包含 24 個公務機關及 16 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 9，其中「資通安全政策及推動組織」表現最好；「資通安全事件通報應變及情資評估因應」仍需持續加強。

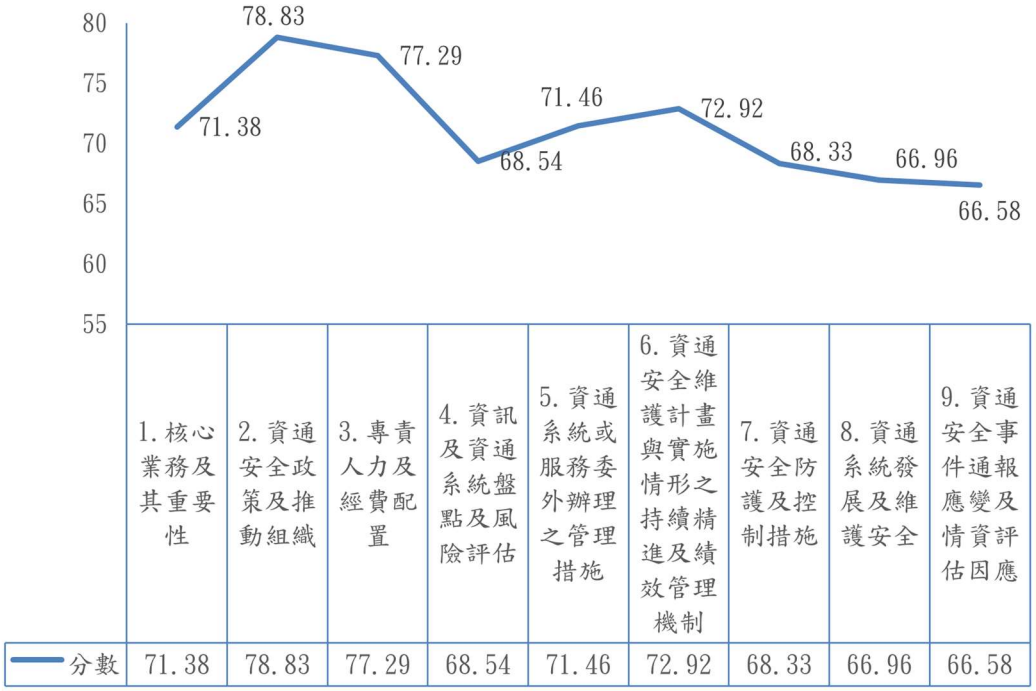


圖9　公務機關實地稽核個別項目成績分布圖

綜合分析公務機關實地稽核各構面之表現情形，詳見圖 10，自策略面、管理面及技術面三個構面檢視，A 級公務機關整體表現平均，B 級公務機關「技術面」則待加強。

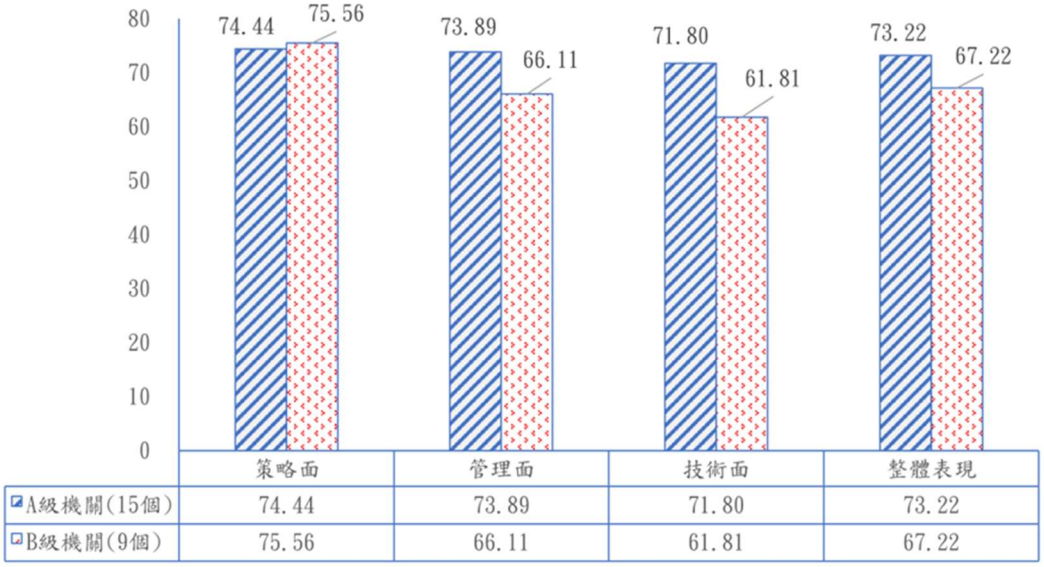


圖10　公務機關實地稽核各構面成績分布圖

五、資安事件通報

分析 112 年公務機關通報事件共 697 件，其中機關收到發布警訊之事件通報占所有通報事件 49.93%為大宗，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 11。

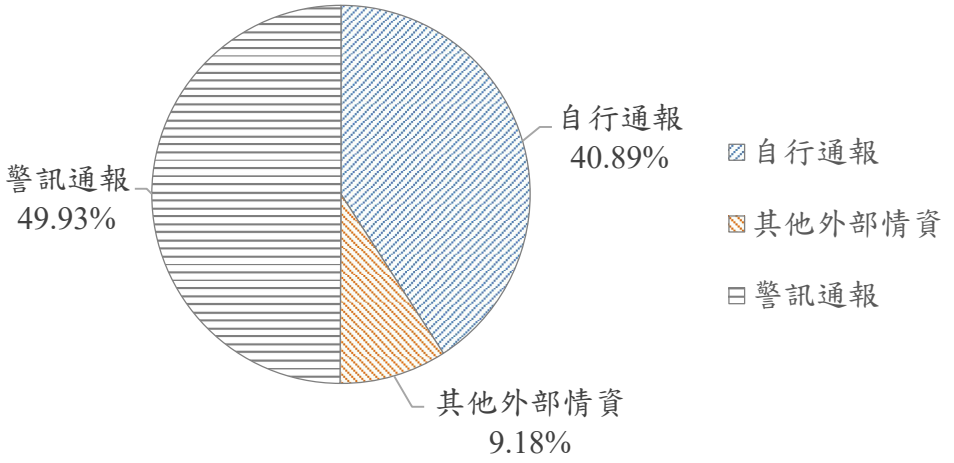


圖11　112 年警訊通報占總通報件數統計

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情形，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 112 年機關通報之資安事件，以 1 級資安事件占 81.78%(570 件)為大宗，2 級資安事件占 15.78%(110 件)居次，3 級資安事件占 2.44%(17 件)，無 4 級資安事件，各級資安事件占比詳見圖 12。

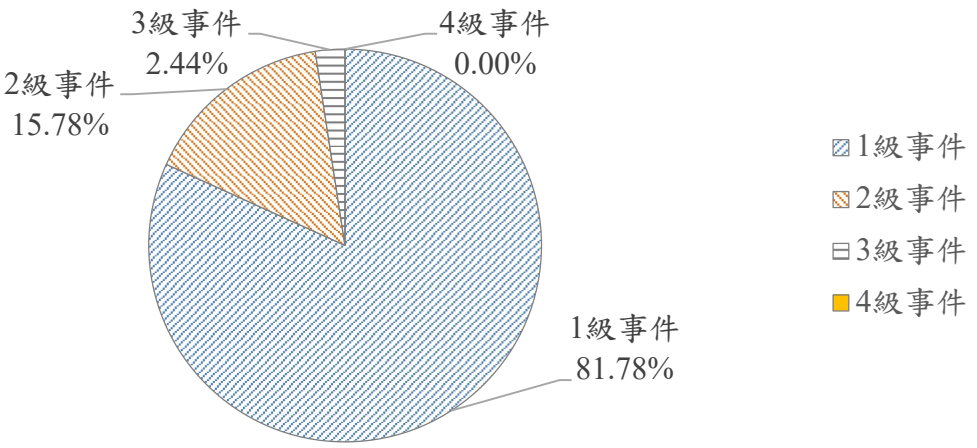


圖12　112 年資安事件等級占比

所接獲資安事件通報中，以非法入侵事件居多占 63.85%，其次為設備問題占 12.91%、阻斷服務占 4.88%及網頁攻擊占 3.37%，各資安事件類型占比，詳見圖 13。

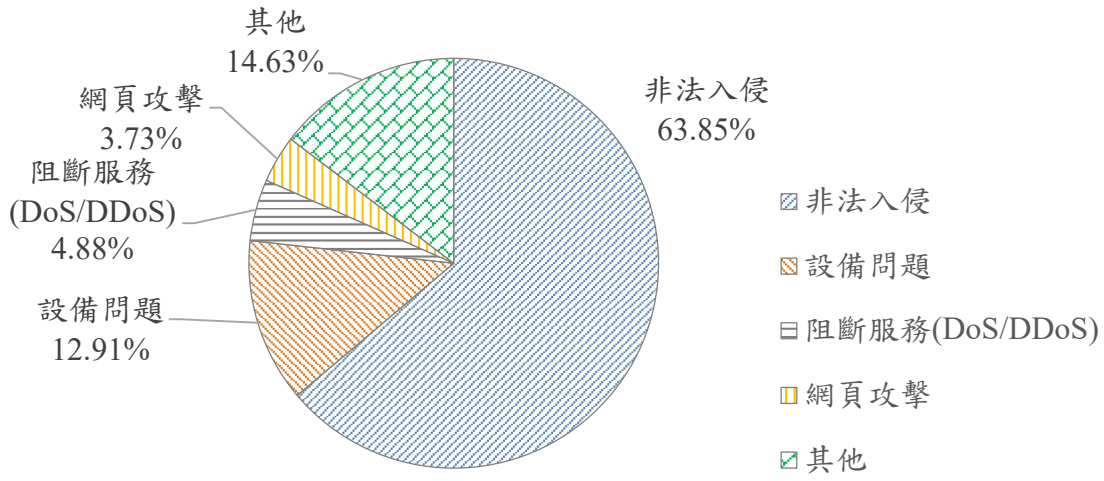


圖13　112 年資安事件類型占比

上述通報案件中，針對非法入侵、設備問題、網頁攻擊等項目分析發生原因，排除「其他」與「無法確認事件原因」後，前 2 名分別為弱密碼/密碼遭暴力破解占 8.79%與應用程式漏洞占 8.16%，多係網

站具認證及驗證機制失效之弱點遭利用成功，或機關電子郵件設置弱密碼或具規則性密碼遭成功猜測/暴力破解取得並利用，第 3 名則為設備異常/毀損占 8.01%，詳見圖 14。

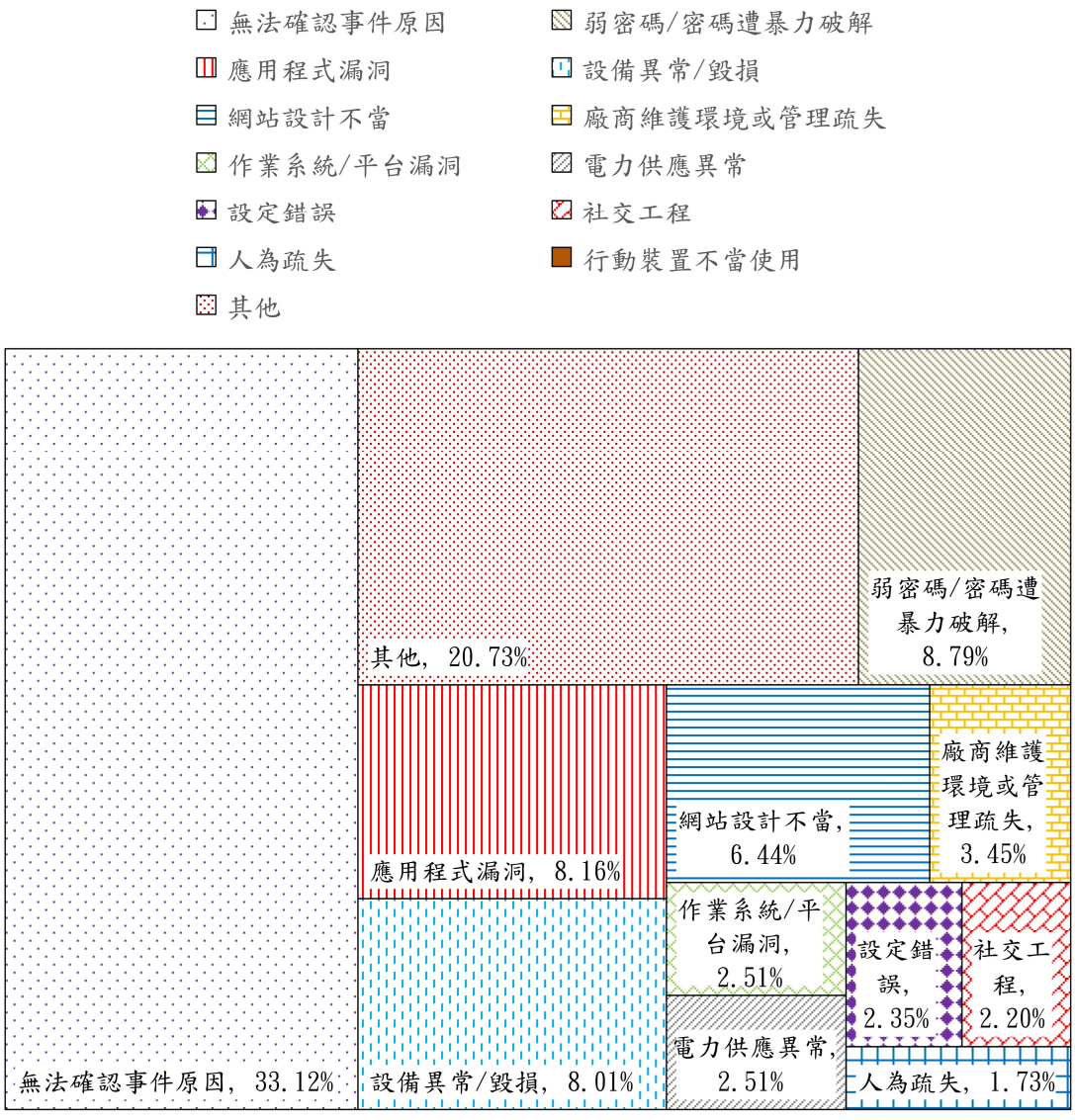


圖14　112 年資安事件發生原因比例圖

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 112 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「郵件帳號密碼遭破解致資料外洩」、「網通設備遭殭屍網路惡意程式連線」、「以社交工程手法竊取個人資料」、「供應商因維護疏失造成機關發生資安事件」、「工業控制系統存在高風險漏洞」及「利用正規之雲端服務架設惡意中繼站」等 6 個政府機關面臨之資安威脅情勢及相對防護建議，提供各機關參考。

一、郵件帳號密碼遭破解致資料外洩

隨著科技運算技術提升，將加速帳號密碼破解；另設備可能存在預設密碼或漏洞，使得駭客可以輕易入侵並取得控制，進而進行各種攻擊。傳統基於信任邊界的網路威脅模型，邊界內存取受信任、邊界外存取不受信任，惟許多攻擊直接或間接來自信任邊界內，且面對複雜的網路環境變化，邊界的定義越發困難。

近期機關帳號密碼外洩仍為重點資安風險項目，自事件通報案例中，仍發現某機關帳號密碼外洩事件，經發布資安警訊通知機關應處，追查發現因設定弱密碼而遭密碼成功猜測或暴力破解。駭客利用帳密暴力破解工具，如 Sanmao SMTP Mail Cracker，制定破解密碼表，當破解成功後，即可設定轉傳郵件。針對類此案件資安防護建議如下：

(一)以自動化或定期檢視機制管理密碼設置原則，透過

GCB(Government Configuration Baseline)密碼原則設定與套用，並強制要求變更預設密碼與定期變更，且須符合複雜度與長度。

(二)除了避免弱密碼、強制要求變更預設密碼與定期變更密碼外，建議採用多因子驗證，確保資料存取機制，並導入零信任網路架構，強化身分鑑別機制，降低密碼遭破解之風險。

(三)定期清查電子郵件帳號，停用或刪除閒置帳號，確保帳號有效性。

二、網通設備遭殭屍網路惡意程式連線

網通設備安全性措施通常較弱，並易疏於更新與維護，是近期常見之駭客攻擊目標。112 年度發現某機關部分網通設備(如路由器或防火牆)出現疑似殭屍網路惡意程式連線行為，經檢測發現設備舊版本存在漏洞可能遭駭客利用入侵，且部分設備本身容量限制，相關紀錄已遭覆寫，無法進一步確認根因。

此外，駭客會使用殭屍網路攻擊進行 DDoS(Distributed Denial-of-service Attack)攻擊，影響政府機關對外服務網站之可用性，經事件案例發現駭客鎖定網域名稱系統(Domain Name System，DNS)展開混合式攻擊、洪水攻擊(Flood Attack)、水刑式攻擊(DNS Water-torture)等手法阻斷服務。針對類此案件資安防護建議如下：

(一)應定期盤點及檢視設備是否有釋出韌體或安全性更新，搭配業務持續性排定更新時程，建立弱點通報及處理機制，縮短暴險時間。

(二)掌握產品服務生命週期，預先規劃汰換或補償控制措施，並建立健全日誌保存機制。

(三)關閉不必要之網路服務埠或功能，評估以白名單方式限制存取。

(四)建立異常流量即時偵測機制，以組態設定限制查詢，同時評估導入流量清洗服務、建置靜態網頁或部署網站內容傳遞網路(Content Delivery Network, CDN)等機制，並定期演練，提升服務韌性。

三、以社交工程手法竊取個人資料

社交工程攻擊仍為近期常見攻擊手法，通過欺騙或誘導人員，以取得機敏資訊或存取權限等其他惡意行為，如誘騙郵件或偽造網站釣魚手法屢見不鮮；在電子郵件監測過程中，發現駭客偽冒利用機關業務相關主旨寄送社交工程郵件，攻擊政府機關與一般民眾。駭客先竊取並模仿與該公司來往郵件內文做為誘餌，附上惡意附檔以大量散布惡意程式垃圾郵件，進行廣泛社交工程攻擊，再透過植入後門程式竊取個人資料;研析某案例之攻擊手法為郵件惡意附檔內含 Guloader 惡

意程式下載器，執行後連線至 Google 雲端硬碟下載並執行 NanoCore 遠端木馬惡意程式，利用第三方服務散布惡意檔案，最終連線至駭客中繼站報到，並回傳受駭主機資訊。NanoCore 遠端木馬程式常被使用於惡意電郵散布活動，以竊取受駭主機資訊，包括電子郵件憑證、瀏覽器與文件傳輸協議之帳密資訊及鍵盤紀錄等，以及遠端操控受駭主機進行惡意活動。針對類此案件資安防護建議如下：

(一)規劃電子郵件進階威脅檢測，包含動態與異常檢測，並實施社交工程演練，強化資安意識。

(二)藉由資安宣導與訓練課程等提醒使用者謹慎確認電子郵件附檔屬性或檔名後之正確性，限制開啓檔案名稱存在異常字元之附件，如 zip, exe 等可執行檔案副檔名、亂碼等。

(三)因應新興攻擊手法，建立惡意郵件過濾機制，規劃自動化識別與偵測機制，分析異常連線行為。

四、供應商因維護疏失造成機關遭遇資安事件

政府通報之資安事件中，廠商維護環境或管理疏失占 3.45%，供應商應同時提供多個機關服務，如遭受駭侵，將成為機關資安風險來源，供應商安全管理成為重要議題，應督促強化其維護資通系統環境，降低管理疏失。

由某機關網站 WordPress Plugin 目錄遭植入惡意程式之鑑識發現，

該事件根因係該網站維護商為方便維護網站，於維護當日調整該目錄權限放寬為所有人皆可寫入，惟完成維護作業後，未將該目錄權限復原，造成當日即遭駭客逕行存取並植入惡意程式。針對類此案件資安防護建議如下：

(一)連線開放須經申請，並遵循「原則禁止、例外允許」原則，經確認維護需求後，依表單核可情況開放與關閉連線，開放連線期間應加強偵測。

(二)限制維護商之電腦與來源位址，確認連線身分與設備安全性，資通系統與服務委外須落實供應商管理。

(三)定期維護重要系統之映像檔俾利快速回復，同時維護更新之備份資料且應保持備份資料離線狀態，謹守備份 3-2-1 原則，維持備份至少 3 份、使用 2 種儲存媒體及規劃異地備份。

(四)應避免不同設備設置相同帳密，且要求定期變更密碼。此外，強化身分驗證機制且應識別敏感資訊，實施重要或敏感加密保護措施。

五、工業控制系統存在高風險漏洞

針對關鍵基礎設施所發動之網路威脅激增，尤其是針對工業控制系統如存在高風險漏洞，更應加強防範措施以因應相關攻擊。112 年度發現機關之部分工業控制系統(Industrial Control System, ICS)相

關設備公開於網際網路中，經進一步檢視發現為該機關之可程式化邏輯控制器(Programmable Logic Controller, PLC)設備，經分析相關PLC 存在多個漏洞，且含括關鍵(Critical)或高(High)風險漏洞，如CVE-2022-1161 允許駭客以遠端程式執行惡意程式碼、CVE-2022-1159 允許注入攻擊、CVE-2022-38773 為資料完整性驗證等漏洞。針對類此案件資安防護建議如下：

(一)盤點機關內部設備系統是否使用 ICS 相關設備與系統，並識別與造冊管理 ICS 廠牌、型號資訊及使用之工控協定。

(二)評估相關 ICS 設備是否需存取外部 IP，並檢驗防火牆規則，確認個別系統限制開放所需對外提供服務之通訊埠與對應IP，避免非授權存取。

(三)定期對設備系統進行監控稽查，包含異常網路流量監控、系統活動紀錄檢視及存取權限檢視等。

六、利用正規之雲端服務架設惡意中繼站

雲端服務快速發展，提供更便捷的架設環境，組織面對多個雲端服務供應商已成為未來趨勢，雲端應用服務亦因此衍生多元威脅；駭客可利用合法雲端服務架設惡意中繼站，藉此規避資安異常偵測機制，甚至隱匿行蹤，提升網路釣魚攻擊成功之可能性。以 112 年資安事件為例，駭客濫用 Cloudflare R2 免費網站代管雲端儲存服務設置釣魚

網站，並將釣魚網站之網址混淆融入政府機關網域名稱，搭配業務資訊寄送郵件攻擊政府機關與民眾。

駭客亦常利用社群平台進行攻擊，包含利用平台檔案分享功能放置其惡意程式，以進一步詐騙或入侵，或因平台系統開發缺陷、管理者未將存取權限區隔等，造成敏感資料遭揭露。針對類此案件資安防護建議如下：

(一)限制存取雲端服務，以白名單方式列管雲端服務，並蒐集入侵指標進行域名分析與阻擋。

(二)部署具備內容分析之資安偵測機制，如網路型入侵偵測系統(Network Intrusion Detection System, NIDS)、端點偵測及應變機制(Endpoint Detection and Response, EDR)等，加強惡意程式與異常行為分析。

(三)規劃雲端服務之檢測機制，包含架構檢視、安全性檢測等，定期檢視雲端服務之威脅與風險可能性。

(四)資料於公開網路服務平台上線前，應規劃安全資料管控措施，如系統安全性檢視、權限區隔或將敏感資料加密。

伍、結語

面對全球新興資通訊技術外，我國因政經情勢特殊，較其他國家之資安威脅更為險峻，本部將持續關注國內外資安威脅情資與趨勢、雲端服務遭非法利用、社交工程攻擊手法氾濫、關鍵資訊基礎設施與 OT 攻擊等議題，研議相對之偵測防禦作法，並針對資料外洩、系統弱點、供應鏈安全等議題，持續推動各機關落實資安防護作業降低資安風險。

為逐步提升政府數位韌性，研析主動式防禦機制、精進資安防護集中管理能量、導入零信任網路架構及推動工控資安治理成熟度評估等各項資安防護措施，亦為持續推動之重要項目，期整體提升民眾對數位系統與環境之信任度，打造堅韌安全之智慧國家。