國家資通安全研究院
National Institute of Cyber Security

資安週報

Cyber Security Weekly Newsletter

事件通報

適逢報稅期間，應特別留意以稅務議題為名之社交工程郵件 避免因下載或執行不明檔案導致設備受駭

聯防監控

防禦迴避高居首位 偵測刺探仍具威脅

蜜罐誘捕

Web服務系統攻擊趨勢增加

外部曝險分析

元件漏洞為主要曝險來源 整體風險較上期上升

焦點文章

NPO資安共學計畫推動：強化資安基礎能力培育

2026.05.07
043

資安儀表板

事件通報、聯防監控、蜜罐誘捕、外部曝險分析及網路巡查高風險詐騙等五類量化指標

■事件通報

近一週公務機關資安事件通報之類型與數量，同時包含民營機構依規定揭露重大資通安全訊息

適逢報稅期間，應特別留意以稅務議題為名之社交工程郵件 避免因下載或執行不明檔案導致設備受駭

本週總計接獲12件公務機關與特定非公務機關事件通報，詳見圖1，公務機關非法入侵事件中以未經授權存取占多數，詳見圖2。 本週有機關接獲以「免稅原則」等稅務議題為名之社交工程郵件，因誤信郵件內容導致設備遭植入後門程式與連線中繼站行為。

適逢報稅期間，駭客常利用免稅、退稅、稅務申報或補件通知等主題寄送社交工程郵件，藉以降低收件人警覺並提高點擊或下載意願。建議各機關除持續強化郵件過濾、端點偵測與異常行為監控外，亦應提醒同仁對涉及稅務、付款或附件下載之郵件提高警覺，避免直接開啟不明檔案或執行相關程式，以降低受駭風險。

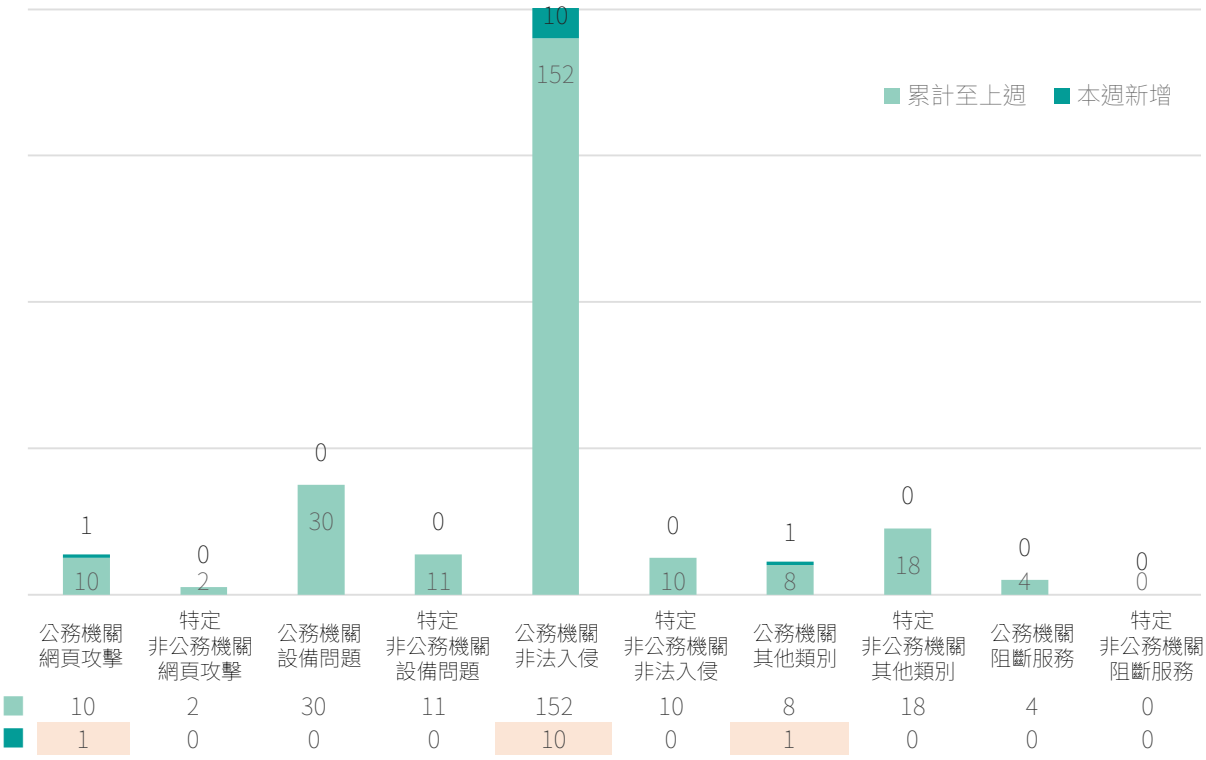

圖1 | 本週公務機關暨特定非公務機關資安事件通報概況

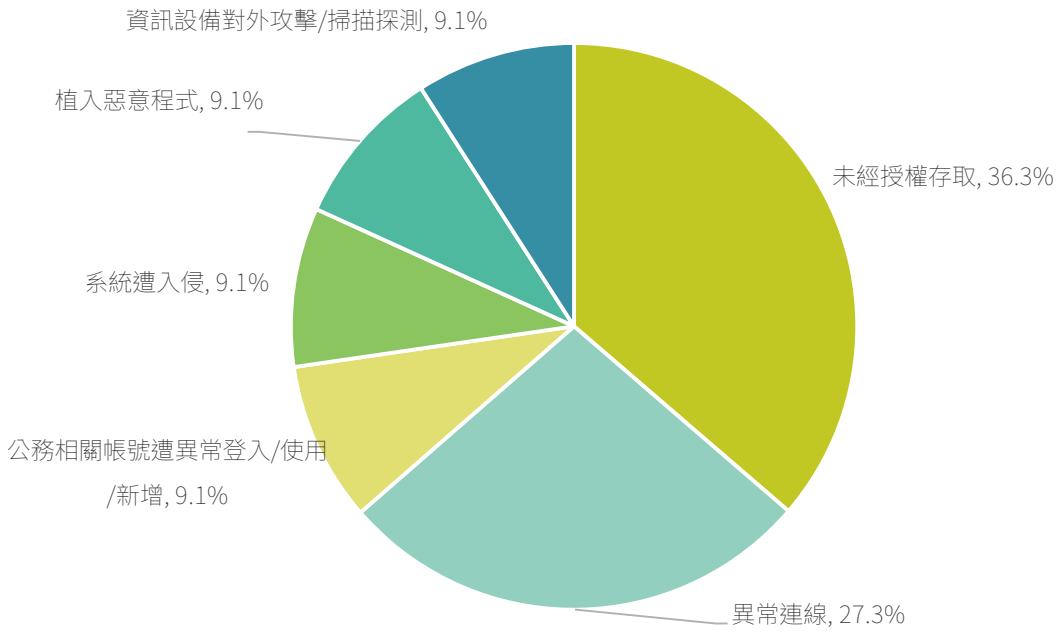

圖2 | 本週公務機關非法入侵事件類型占比

防護建議　除修補漏洞外，應：

以攻擊為出發評估潛在風險	針對潛在風險執行相應改善
➢ 社交郵件誘導點擊下載植入後門程式 ➢ 惡意程式建立中繼站擴散內部網路存取	➢ 強化郵件過濾與惡意附件偵測機制，降低社交工程郵件進入風險 ➢ 導入端點偵測與回應機制，即時發現後門程式與異常連線行為 ➢ 建立異常連線監控機制，阻斷設備作為中繼站對外通訊行為 ➢ 加強人員資安意識宣導，提升對稅務主題郵件之辨識能力

1間民間企業揭露重大資安訊息

本週1家民間企業發布重大訊息，產業類別為電機機械業。

■ 公司名稱	新代科技股份有限公司
■ 發布時間	115年4月29日
■ 事件說明	新代公司資訊單位接獲異常通報後，經查證確認為加密攻擊，已啟動資安應變機制，並進行全面性檢測與防護處理作業。經初步確認，內部資訊系統及官方網站運作正常，未發現有機密資料或重要文件外洩之情事。後續將持續強化監控與防護措施，以確保資訊系統安全與營運穩定。

■聯防監控

近一週以MITRE ATT&CK Matrix 分析攻擊者行為，提醒公務機關留意攻擊趨勢變化，是否由初期之偵測刺探進入影響層面更大竊取資料與破壞資通系統

防禦迴避高居首位 偵測刺探仍具威脅

本週政府領域資安聯防監控參考MITRE ATT&CK Matrix分析TTP戰術框架分布顯示，本週趨勢相較上週無顯著差異，詳見圖3。「防禦迴避」為最常見攻擊手法，占比14.8%，攻擊者通常會透過關閉或刪除指令紀錄，並利用合法的系統工具間接執行惡意命令，以達到規避監控的目的。因應此類威脅，建議導入端點防護措施，加強指令紀錄的稽核能力，限制高風險工具的濫用，並強化特權帳號的管理，以避免攻擊者繞過偵測並消除其行為痕跡。

「偵測刺探」事件本週占比為13.7%，為本週占比次高的攻擊階段，顯示攻擊者持續加強對目標環境的前期偵查與弱點探測行動。觀察到的主要手法包括主動式掃描、IP 區段掃描、以及漏洞掃描。攻擊者透過自動化工具對大範圍網段進行探測，以識別對外服務、開放埠與系統類型，並進一步針對潛在弱點進行漏洞評估，尋找可利用的攻擊入口。此類行為通常呈現由廣泛掃描逐步聚焦的特徵，顯示其攻擊流程具備階段性與目標導向。由於此階段多發生於攻擊初期，若未及時偵測，將提高後續入侵成功機率。建議加強對異常掃描流量的監控與分析，導入漏洞管理與修補機制，並結合威脅情資比對掃描來源，以提前掌握潛在攻擊準備行為。

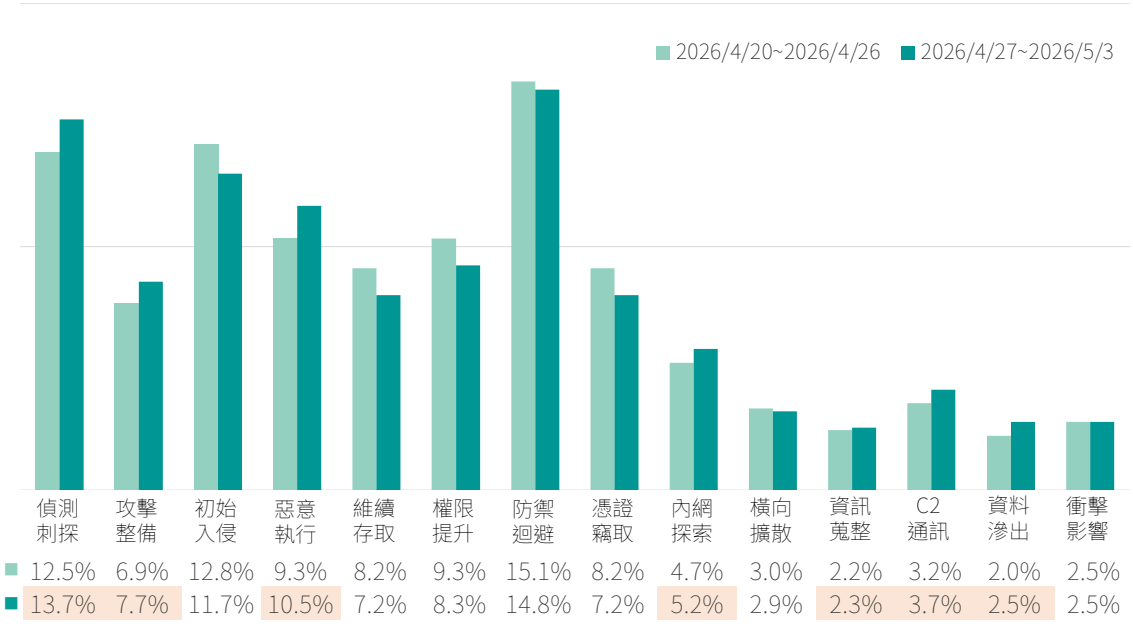

圖3 | 資安聯防監控攻擊階段統計

防護建議 建議機關採取下列防護措施：

- 強化端點防護（EDR / XDR），監控異常指令與行為
- 啟用並集中管理指令紀錄（如 PowerShell、Shell logging）
- 建立日誌不可竄改與長期保存機制（防刪除/清除）
- 限制系統內建工具（Living-off-the-Land）濫用（如 WMIC、PsExec）
- 落實特權帳號控管（最小權限、MFA、多層審核）
- 偵測可疑行為鏈（如關閉日誌 → 執行命令 → 清除痕跡）

防禦迴避（Defense Evasion）

- 部署網路流量監控（NDR / IDS）偵測異常掃描行為
- 設定掃描行為告警（大量連線、Port Scan、IP Sweep）
- 導入漏洞管理機制（定期掃描 + 修補）
- 建立外部攻擊面盤點（公開服務、開放埠）
- 比對威脅情資（封鎖惡意掃描來源 IP）
- 實施速率限制與防火牆策略（降低掃描成功率）

偵測刺探（Reconnaissance）

■蜜罐誘捕

近一週誘捕系統所捕捉到的攻擊樣態趨勢變化以及所利用的弱點趨勢

Web服務系統攻擊趨勢增加

本週透過部署於國內外之蜜罐系統觀測攻擊行為動態，相較於上週「網頁應用」服務攻擊占比73.05%、「遠端控制」服務攻擊占比23.60%，本週各類服務之平均偵測攻擊比例無明顯變化，結果顯示「網頁應用」服務仍為攻擊主軸，占比高達53.83%。「遠端控制」服務亦有43.70% 的誘捕比例，反映攻擊者仍積極針對公開遠端連線介面進行入侵行動。

網頁應用是最為常見之對外服務類型，若存在已知漏洞，將面臨高風險曝露情形，易成為攻擊者入侵與滲透重要管道，為優先防護之項目。本週網頁應用介面之誘捕狀況，詳見圖4。本週通用型Web介面占比最高，此類別為攻擊者廣泛的進行HTTP掃描與探測，顯示攻擊者企圖尋找可能存在之Web漏洞進行攻擊。

另Web服務系統類別包含各類以網頁為基礎的服務與應用，例如常見的網頁框架、應用程式伺服器、檔案傳輸與資料管理平台等，由於此類服務多建置於企業應用環境，且直接面向外部提供功能與資料交換，為僅次於通用型介面的攻擊目標。而Web服務系統比例大幅上升主因為端點管理系統中存在身分驗證繞過漏洞的CVE-2026-1603及管理式檔案傳輸系統中存在身分驗證繞過漏洞的CVE-2024-0204，遭攻擊次數大幅上升導致。網通設備管理介面涵蓋路由器、防火牆等網通設備管理介面，以及智慧攝影機、NAS等物聯網設備管理介面，皆容易遭受攻擊者透過弱密碼、預設帳號或已知漏洞進行入侵。其他類型服務雖比例極小，但若涉及關鍵業務系統，仍需留意潛在風險。

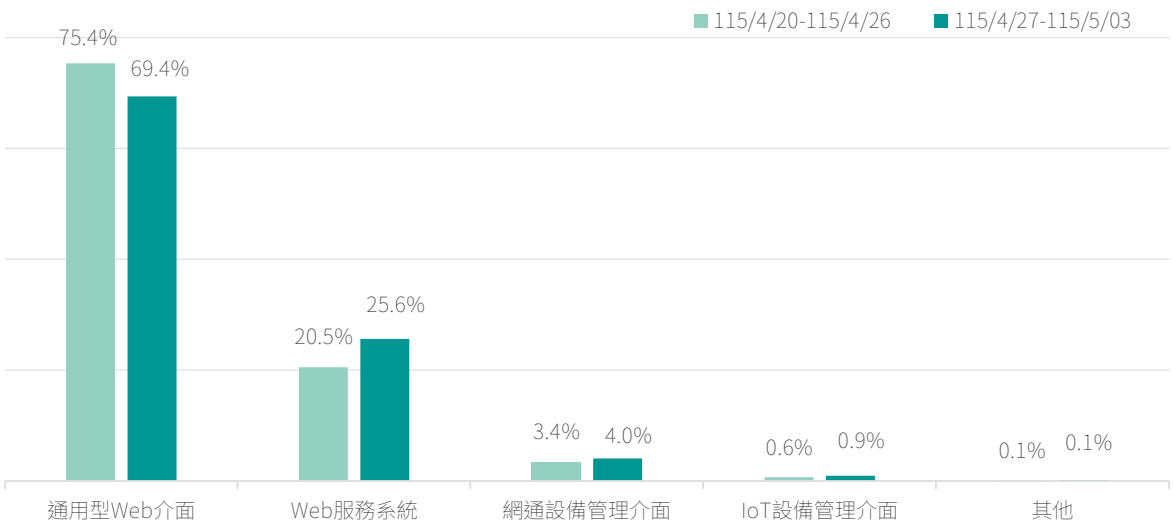

圖4 |本週網頁應用介面之誘捕攻擊比例統計

進一步解析國內外之蜜罐系統誘捕漏洞攻擊之情形，詳見表1。近3年揭露之攻擊漏洞，前5大攻擊以「網頁應用」服務之漏洞為主要入侵路徑，本週漏洞類型多集中於越界讀取漏洞、作業系統命令注入漏洞、遠端程式碼執行漏洞及身分驗證繞過漏洞，攻擊目標涵蓋應用程式遞送控制器(ADC)、PHP伺服器端腳本語言、知識管理與團隊協作系統、端點管理系統及管理式檔案傳輸系統。其中Ivanti Endpoint Manager存在身分鑑別繞過之CVE-2026-1603漏洞，未經身分鑑別之遠端攻擊者可取得特定身分鑑別資料，顯示以上類型系統已成為高風險熱點。

防護建議

建議存在漏洞之設備應更新至最新版本軟體或韌體以修補漏洞；若原廠已無法提供更新支援，應考慮汰換存在漏洞之設備或軟體套件，如因故無法汰換，應採對應之漏洞緩解措施。

表1 | 本週前5大攻擊使用之近3年漏洞排行列表

排名			漏洞編號	受影響產品	CVSS 3.x Base Score
■	1	-	CVE-2025-5777[1]	Citrix NetScaler ADC	7.5
■	2	-	CVE-2024-4577[2]	PHP	9.8
■	3	-	CVE-2024-21683[3]	Atlassian Confluence Server	8.8
■	4	⬆New	CVE-2026-1603[4]	Ivanti Endpoint Manager	8.6
■	5	⬆New	CVE-2024-0204[5]	Fortra's GoAnywhere MFT	9.8

類型 ■越界讀取漏洞 ■作業系統命令注入漏洞 ■遠端程式碼執行漏洞 ■身分驗證繞過漏洞

▶近期重大弱點提醒

近一週本院研究人員發現以下重大弱點資訊，建議組織內部進行檢查與修補：

- 以Chromium為基礎之瀏覽器存在30個高風險安全漏洞(CVE-2026-7333至CVE-2026-7361與CVE-2026-7363[6])，類型包含使用釋放後記憶體(Use After Free)與堆積型緩衝區溢位(Heap-based Buffer Overflow)，最嚴重可使未經身分鑑別之遠端攻擊者誘使使用者開啟特製HTML頁面，進而於瀏覽器沙盒環境內執行任意程式碼。
- Apache ActiveMQ存在2個高風險安全漏洞(CVE-2026-40466[7]與CVE-2026-41044[8])，類型包含不當輸入驗證(Improper Input Validation)與程式碼注入(Code Injection)，已通過身分鑑別之遠端攻擊者可利用此漏洞，使ActiveMQ載入惡意設定檔，進而執行任意程式碼。

1. https://nvd.nist.gov/vuln/detail/CVE-2025-5777
2. https://nvd.nist.gov/vuln/detail/cve-2024-4577
3. https://nvd.nist.gov/vuln/detail/cve-2024-21683
4. https://nvd.nist.gov/vuln/detail/CVE-2026-1603
5. https://nvd.nist.gov/vuln/detail/cve-2024-0204
6. https://chromereleases.googleblog.com/2026/04/stable-channel-update-for-desktop_28.html
7. https://nvd.nist.gov/vuln/detail/CVE-2026-40466
8. https://nvd.nist.gov/vuln/detail/CVE-2026-41044

■外部曝險分析

經由外部檢測政府機關資通安全狀況，例如使用EASM工具或實兵演練，及早發現曝露於外部之風險

元件漏洞為主要曝險來源 整體風險較上期上升

本次針對100個曝險程度較高之A、B級公務機關進行EASM資安曝險檢測，前10大風險項目共計6,370項，詳見圖5。其中，「元件高風險漏洞」以3,860項居首，單項即占前10大風險項目總數約60.6%，不僅逾整體6成，亦高於其餘9項合計2,510項，顯示元件漏洞為本期最主要且最集中的曝險來源。元件漏洞以舊版Apache HTTP Server相關風險較為集中，顯示部分對外網站仍使用具已知漏洞之伺服器元件版本，建議列為後續修補與版本汰換重點。「CSP設定不當」985項次之，「未部署WAF」694項位居第三，前三項合計5,539項，占前10大風險項目總數約87.0%，顯示目前外部曝險風險仍高度集中於元件漏洞、應用層安全防護及網站安全設定等議題。相較上期5,959項，整體風險數量增加411項，增幅約6.9%。

進一步分析主要風險變化情形，「元件高風險漏洞」由3,548項增至3,860項，增加312項，增幅約8.8%；「CSP設定不當」由997項降至985項，減少12項，降幅約1.2%，變化不大；「未部署WAF」由552項大幅增至694項，增加142項，增幅約25.7%；「過時或弱加密協定」由359項微增至366項，增加7項，增幅約1.9%，變化不大。整體而言，本期外部曝險仍以元件漏洞為主要風險來源，且未部署WAF項目增幅明顯，顯示部分對外網站在弱點修補、WAF部署及應用層攻擊防護方面仍有待強化。

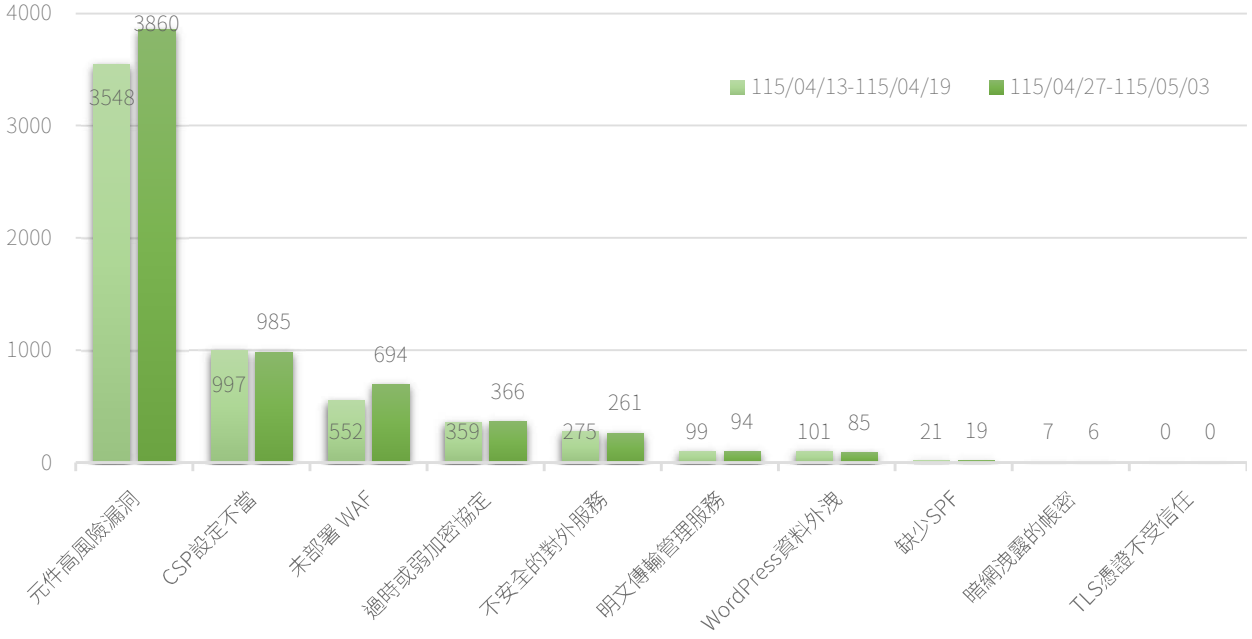

圖5 | EASM檢測結果統計(前10大風險)

防護建議	
建議機關或關鍵基礎設施採取下列防護措施	建議機關或關鍵基礎設施採取下列管理措施
➢ 優先盤點對外網站使用之元件版本，針對舊版ApacheHTTPServer等高風險元件儘速修補或升版 ➢ 修正CSP設定不當問題，導入必要網站安全標頭，降低XSS及惡意腳本載入風險 ➢ 針對重要對外網站逐步部署WAF，並搭配規則調校與警示監控，強化應用層防護 ➢ 停用未加密連線、舊版或弱加密協定，全面採用TLS1.2以上版本；遠端管理服務應使用加密通道並限制來源IP ➢ 關閉不必要之對外服務，定期盤點已停用站台、主機與應用系統，避免資產持續對外曝露	➢ 建立元件漏洞優先修補機制，針對高風險及已遭利用漏洞設定改善期限並追蹤複測結果 ➢ 將CSP、WAF、加密協定及對外服務設定納入例行檢核，定期追蹤未改善項目 ➢ 強化對外資產生命週期管理，確認測試站、舊站台及停用服務均已完成下線

焦點文章

NPO資安共學計畫推動：強化資安基礎能力培育

結合國際資源與在地實務，建構可擴散的資安學習模式

因應數位風險升溫，資安人才培育成為關鍵戰略

全球數位風險持續升溫，各領域皆有資安防護之需求，資安防護將不再侷限於資安專責人員，亦須提升組織內部各層級人員之基本能力。有鑑於此，國家資通安全研究院與思科網路學院（Cisco Networking Academy）攜手合作，針對沒有資安背景之非營利組織第一線成員，規劃整合基本資安防護概念與實務操作能力的課程，計畫以「Cyber Skills for Good」為核心理念，將資安教育延伸至公益領域，打造安全可信賴之公益數位環境。

共學導向：以互動與回饋強化學習成效

課程以淺顯易懂的案例內容，結合國際教材與在地實務，課程首先從資安基本概念出發，說明資訊保護對象、個人與組織資料差異，以及駭客攻擊動機，使學員建立整體風險認知。最後進一步介紹常見攻擊手法，包括詐騙、釣魚及密碼攻擊等，並解析攻擊如何透過人為疏失或系統漏洞入侵，強化學員對實際威脅的辨識能力。希望透過由淺入深之課程安排，使學員能將資安概念轉化為日常可實踐之行動，詳見圖6。

圖6 | 課程介紹

焦點文章

知識落地：課後回饋驗證學習成效

基於非營利性質組織，日常需處理大量會員及捐款相關的個人資料，對資訊安全的需求格外直接，從課後回饋觀察，學員普遍對「資料與隱私保護」相關課程內容評價最高，認為這個內容對於工作的執行最有幫助，同時也是學員最期待能夠深入探討的主題。

講師表現同樣獲得學員肯定，從教學態度、內容表達及理論與實務結合的能力，均給予高度評價，整體滿意度維持在高水準，反映出課程在專業性與實用性上達到一定程度的平衡。

學習成效方面，多數學員表示課程有助於理解資安概念，而不只是課堂上的知識，而是能開始嘗試把資安觀念帶入實際工作場景中，顯示本計畫已具備促進「知識落地」之成效。

持續強化資安能力，落實日常防護

資安威脅不會停歇，但防範的起點其實很簡單——建立基本觀念、養成正確的操作習慣，就是最務實的防線。本計畫透過系統化課程與共學交流，帶領學員認識常見風險，把資安意識融入日常的工作流程中，以提升組織整體防護能力。

未來將持續以實務需求為導向，透過交流與分享，讓學習成果不只是留在課堂裡，而是真正轉化為組織日常運作的一部分，讓整體防護能力隨著時間慢慢累積，逐步提升整體資安防護能量，打造安全、值得信賴的數位環境。

關鍵字：資安共學、資安教育訓練、資安意識、非營利組織

刊　　名　資安週報第 43 期
發 行 人　國家資通安全研究院　林盈達院長
主　　編　國家資通安全研究院　國際合作及資安治理中心
出 版 者　國家資通安全研究院
網　　址　www.nics.nat.gov.tw
訂閱網址　www.nics.nat.gov.tw/newsletter/
讀者信箱　www.nics.nat.gov.tw/mail2center/

國家資通安全研究院
National Institute of Cyber Security