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

資安週報

Cyber Security Weekly Newsletter

2026.06.18
049

資安儀表板

事件通報、聯防監控、蜜罐誘捕、重大漏洞、外部曝險分析及實兵演練等六類量化指標

■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

後台帳號安全應透過系統功能需求落實 降低人為設置簡易帳密之風險

本週總計接獲20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異常連線占多數，詳見圖2。本週發現某網站廠商為多個機關建置之網站，後台管理者預設帳號密碼係以機關英文簡稱設定，因具規律性存在遭猜測登入之風險。

建議於系統交付、上線及維護過程中，將後台帳號啟用與登入保護納入必要功能需求，避免使用具規律性或可預測之預設登入資訊。相關需求可包括首次啟用流程、首次登入強制變更密碼、密碼強度限制、登入失敗鎖定、異常登入監控、多因子驗證以及管理介面存取來源限制等，以降低遭猜測破解之風險。

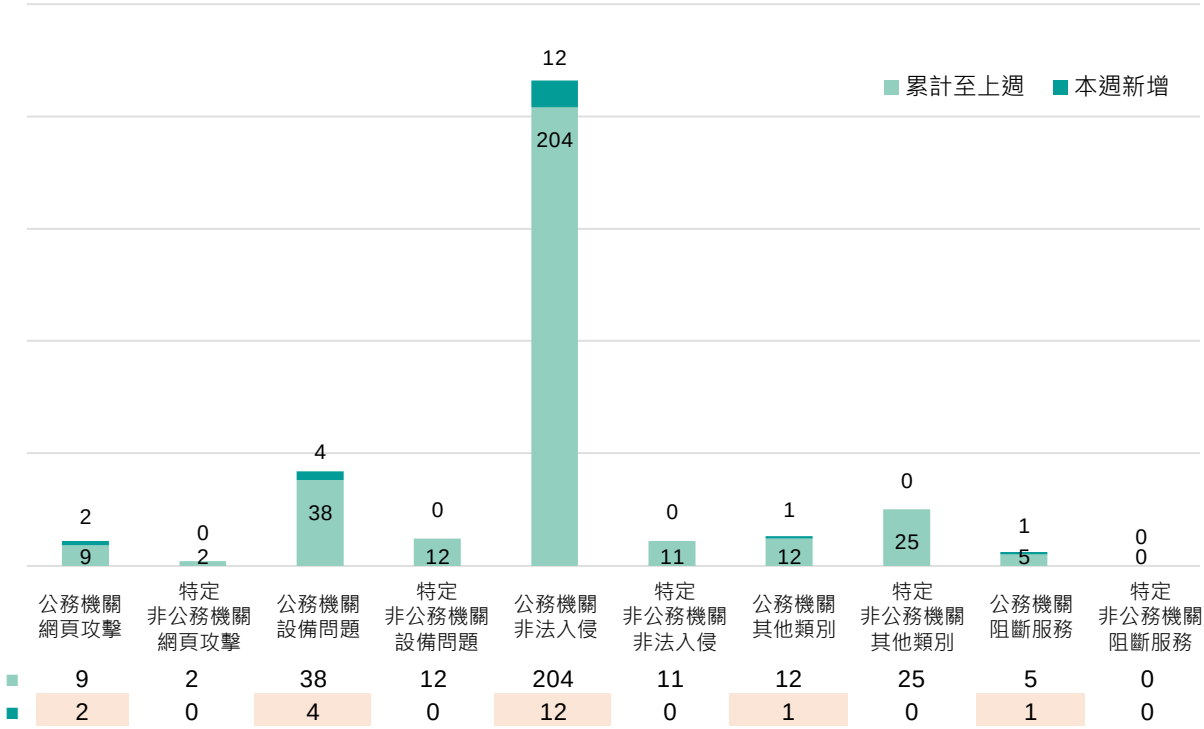

圖1 | 本週公務機關暨特定非公務機關資安事件通報概況

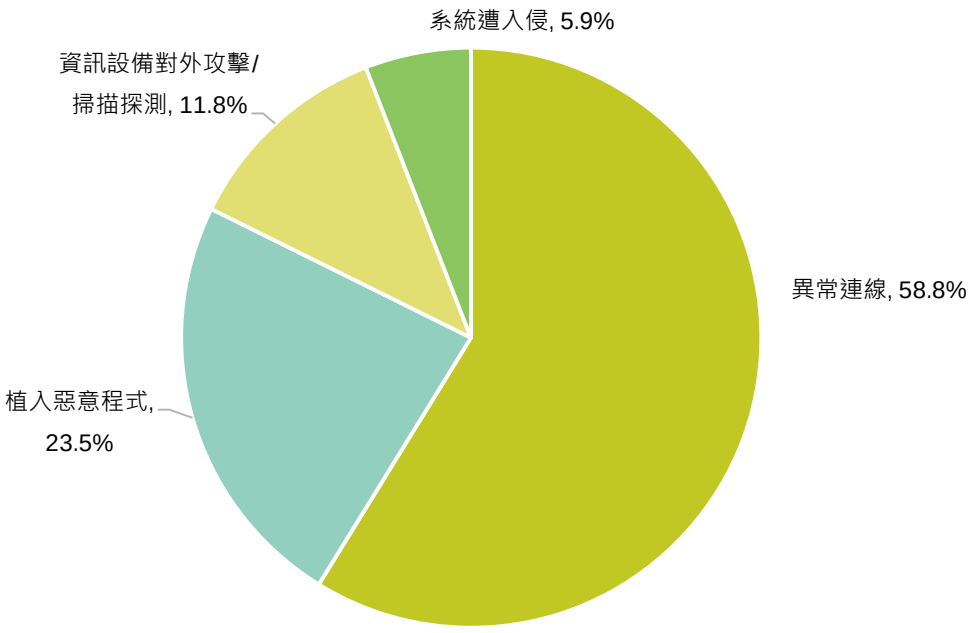

圖2 | 本週公務機關非法入侵事件類型占比

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
➢ 後台採用具規律性預設帳號密碼，易遭攻擊者猜測登入取得管理權限 ➢ 管理介面缺乏登入保護機制，可能遭暴力破解或帳號濫用攻擊	➢ 系統首次啟用或登入時強制變更預設帳號密碼，避免使用固定規則 ➢ 建立密碼強度政策與定期更換機制，降低帳號遭破解風險 ➢ 啟用多因子驗證及登入失敗鎖定功能，強化身分驗證安全性 ➢ 限制後台管理介面存取來源並監控異常登入行為，及早發現攻擊

◎本週無企業發布資通安全事件重大訊息。

■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15.8%，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15%，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。

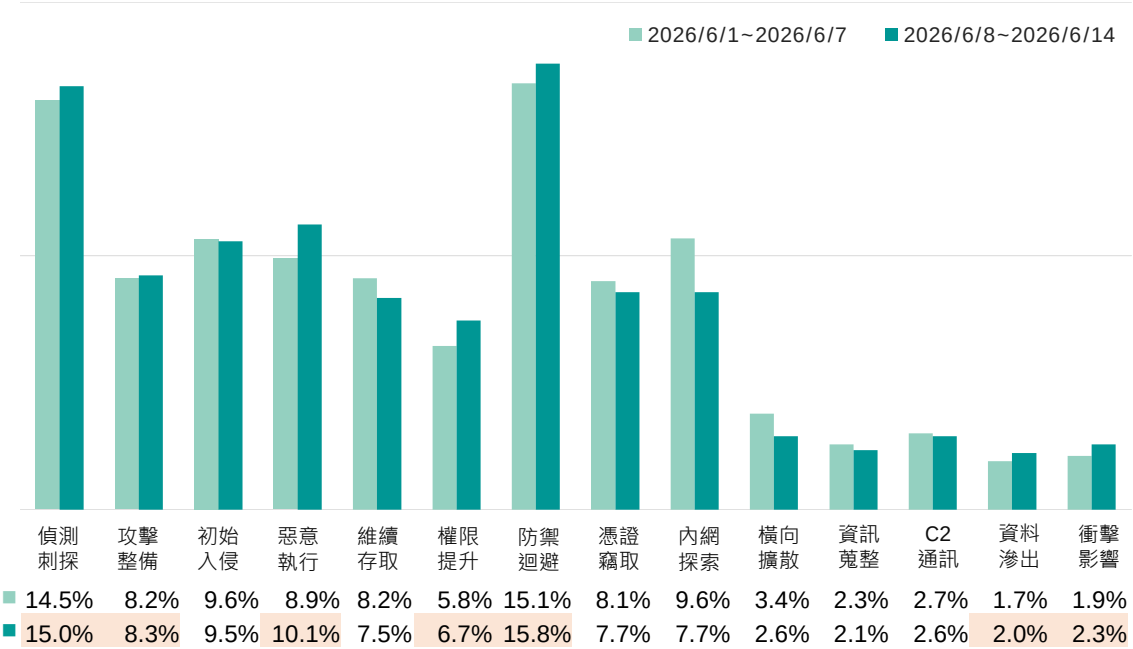

圖3 | 資安聯防監控攻擊階段統計

防護建議 **建議機關採取下列防護措施：**

防禦迴避（Defense Evasion）

- 強化端點偵測與回應（EDR）機制，監控可疑行為
- 啟用並保護系統與指令操作日誌，避免遭竄改或刪除
- 限制 PowerShell、WMI、PsExec 等高風險系統工具使用權限
- 建立特權帳號管理（PAM）機制，落實最小權限原則
- 監控異常程序執行及合法工具（Living-off-the-Land）濫用行為
- 定期檢視防毒、防護軟體是否遭停用或規避

偵測刺探（Reconnaissance）

- 部署 IDS / IPS、流量分析平台，監控異常掃描行為
- 建立網路掃描與探測行為告警規則
- 關閉非必要對外服務與連接埠，減少攻擊面
- 定期執行弱點掃描與修補作業，降低可利用漏洞
- 導入威脅情資（Threat Intelligence），識別惡意掃描來源
- 實施網路分區（Network Segmentation），降低橫向探測範圍

■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服務系統攻擊趨勢減少

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71.94%、「遠端控制」服務攻擊占比24.43%，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71.39%，「遠端控制」服務亦有23.84% 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服務系統比例下降主因為cPanel & WHM在登入流程中存在身份驗證繞過漏洞的CVE-2026-41940，遭攻擊次數下降導致。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。

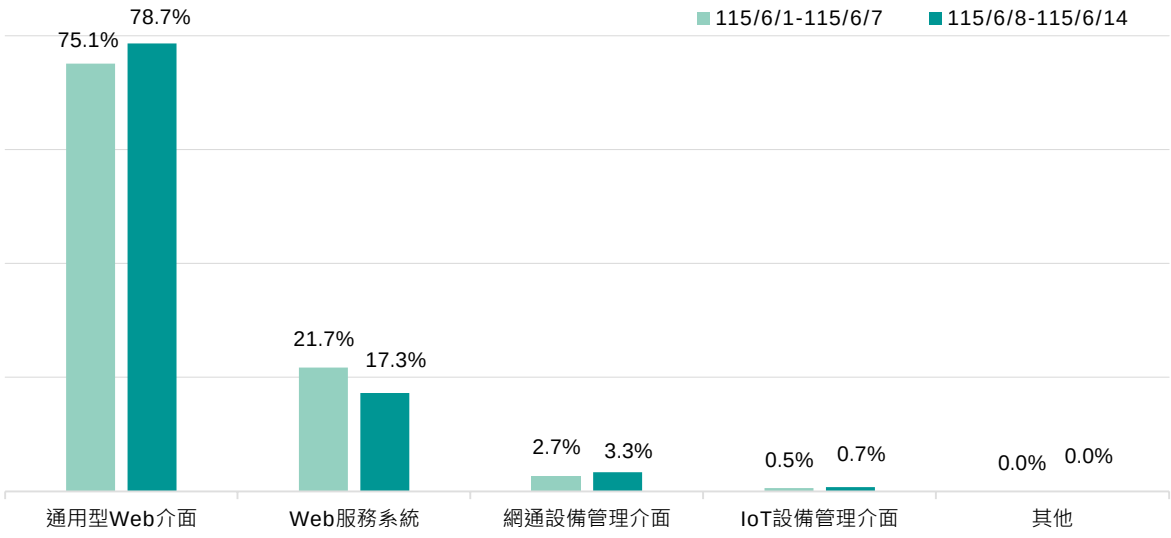

圖4 | 本週網頁應用介面之誘捕攻擊比例統計

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2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、跨站請求偽造、身分驗證繞過漏洞、授權缺失漏洞及路徑遍歷漏洞，攻擊目標涵蓋程式遞送控制器(ADC)、多選下拉選單元件、網站主機伺服器管理系統、企業級網路防火牆軟體及內容管理系統之網站優化外掛程式。

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2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	⬆1	CVE-2025-47204[2]	Bootstrap Multiselect	6.1
■	3	⬇1	CVE-2026-41940[3]	cPanel & WHM	9.8
■	4	-	CVE-2025-20362[4]	Cisco Secure ASA & FTD	6.5
■	5	⬆new	CVE-2025-30567[5]	WordPress WP01	7.5

類型 ■ 越界讀取漏洞 ■ 跨站請求偽造 ■ 身分驗證繞過漏洞
■ 授權缺失漏洞 ■ 路徑遍歷漏洞

1. https://nvd.nist.gov/vuln/detail/CVE-2025-5777
2. https://nvd.nist.gov/vuln/detail/CVE-2025-47204
3. https://nvd.nist.gov/vuln/detail/CVE-2026-41940
4. https://nvd.nist.gov/vuln/detail/CVE-2025-20362
5. https://nvd.nist.gov/vuln/detail/CVE-2025-30567

■重大漏洞

近一週本院研究人員發現以下重大漏洞資訊，建議組織內部進行檢查與修補

Microsoft與Chromium瀏覽器高風險漏洞應儘速修補

- 微軟釋出115年6月份安全性更新，共修補包含Azure HorizonDB、Windows DHCP Client及Windows Kernel等共204個漏洞[1]，其中包含18個高風險漏洞。
- 以Chromium為基礎之瀏覽器存在74個高風險安全漏洞(CVE-2026-11628至CVE-2026-11701[2])，類型包含使用釋放後記憶體(Use After Free)與越界記憶體存取(Out-of-Bounds Memory Access)等，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。其中CVE-2026-11645已遭駭客利用。

1. https://msrc.microsoft.com/update-guide/releaseNote/2026-Jun
2. https://chromereleases.googleblog.com/2026/06/stable-channel-update-for-desktop_0153744567.html

■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

元件漏洞仍居首 加密與憑證風險明顯升溫

本次針對外部曝險程度較高之100個A、B級公務機關進行EASM檢測，前10大風險項目共計9,783項，較上期9,419項增加364項，增幅約3.9%，整體曝險風險呈小幅上升。其中，「元件高風險漏洞」以4,192項居首，「過時或弱加密協定」1,959項次之，「TLS憑證不受信任」1,632項位居第三；前三項合計7,783項，占前10大風險項目總數約79.6%，顯示外部曝險風險仍高度集中於元件漏洞、加密協定與憑證管理等面向，詳見圖5。

進一步分析主要風險變化情形，「元件高風險漏洞」雖仍為最大宗風險，惟數量已由上期4,232項微降至本期4,192項，減少40項，降幅約0.9%。其中，Apache HTTP Server相關弱點(CVE-2024-38475)仍較為集中，且本期新增PEAR Archive_Tar相關弱點(CVE-2020-28949)，顯示對外網站伺服器、CMS及第三方套件之版本維護仍為後續改善重點。相較之下，與加密通訊安全相關之風險明顯上升，其中「過時或弱加密協定」由 1,720項增至1,959項，增加239項，增幅約13.9%；「TLS憑證不受信任」亦由1,386項增至1,632項，增加246項，增幅約17.7%。另「CSP設定不當」由949項降至888項，減少 61項，降幅約6.4%；「未部署WAF」則由705項降至684項，減少21項，降幅約3.0%。整體而言，本期外部風險增幅主要來自加密協定與憑證管理問題，後續宜優先追蹤相關設定、憑證有效性及弱加密協定停用情形。

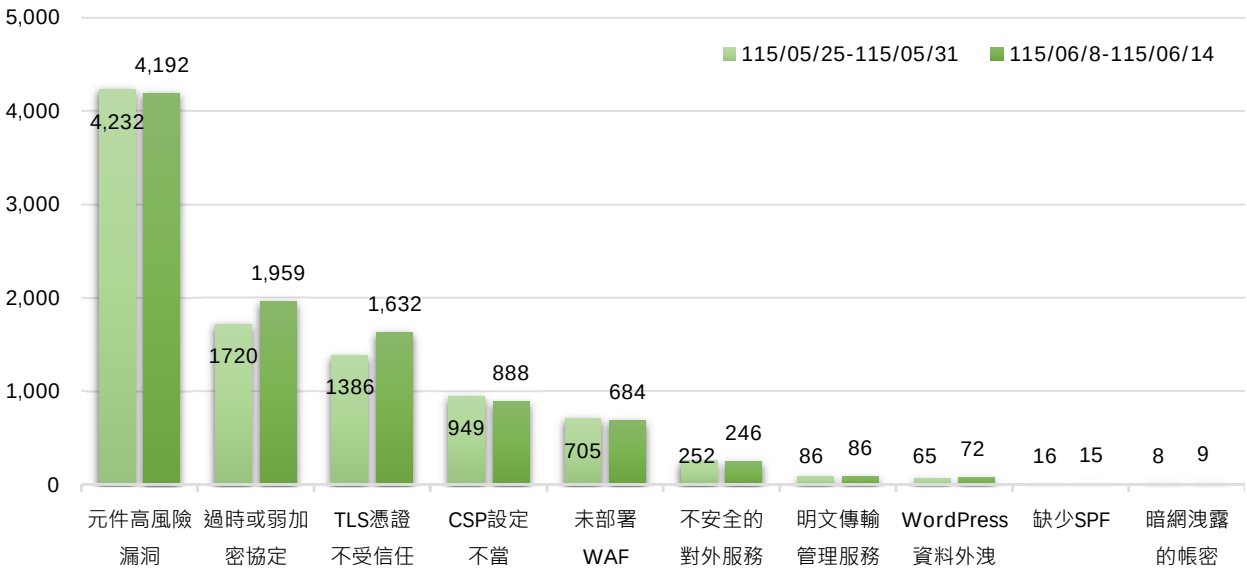

圖5 | EASM檢測結果統計(前10大風險)

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
➢ 定期檢視及更新網站憑證，全面啟用TLS 1.2以上版本協定，並停用未加密或舊版協定 ➢ 儘速修補已知漏洞，盤點並汰換已無維護之軟體版本，降低元件漏洞遭利用風險 ➢ 部署網站應用程式防火牆(WAF)，並導入內容安全政策(CSP)等網站安全標頭，以降低XSS攻擊與惡意存取風險 ➢ 關閉不必要之對外服務，並定期盤點已停用站台、主機與應用服務是否已確實完成下線，避免因資產未完全關閉而持續對外曝露；如確有遠端管理需求，應嚴格限制來源IP，並採用加密通道(如SSH)進行存取	➢ 定期盤點並更換外洩帳號憑證，搭配多因素驗證(MFA)，以強化存取安全 ➢ 建立弱點修補與驗證機制，確保風險持續改善 ➢ 強化資安教育訓練，提升系統維運人員對憑證管理、加密配置及服務設定之安全意識

■實兵演練

實兵演練係模擬真實攻擊情境，檢驗資通系統弱點、防護能力及應變機制，以提升整體資安防禦韌性

實兵演練揭露遠端存取驗證機制缺失 避免使用預設帳號與弱密碼

本年資通系統實兵演練針對政府機關與關鍵基礎設施提供者，於擇定時間進行演練，至6/12止已累計144筆攻擊紀錄，本週新增弱點數量共14筆，分別為「驗證機制失效」6筆、「注入攻擊」3筆、「無效的存取控管」3筆、「軟體供應鏈失效」1筆及「不安全的組態設定」1筆，詳見圖6。

本週演練發現，衝擊性較高之弱點為因主機對外開啟遠端桌面服務(Remote Desktop Protocol, RDP)埠3389，且使用預設管理者帳號(Administrator)與常見易於猜測之密碼，攻擊者透過帳號密碼猜測即成功取得本機管理員權限，屬於驗證機制失效之重大風險弱點。

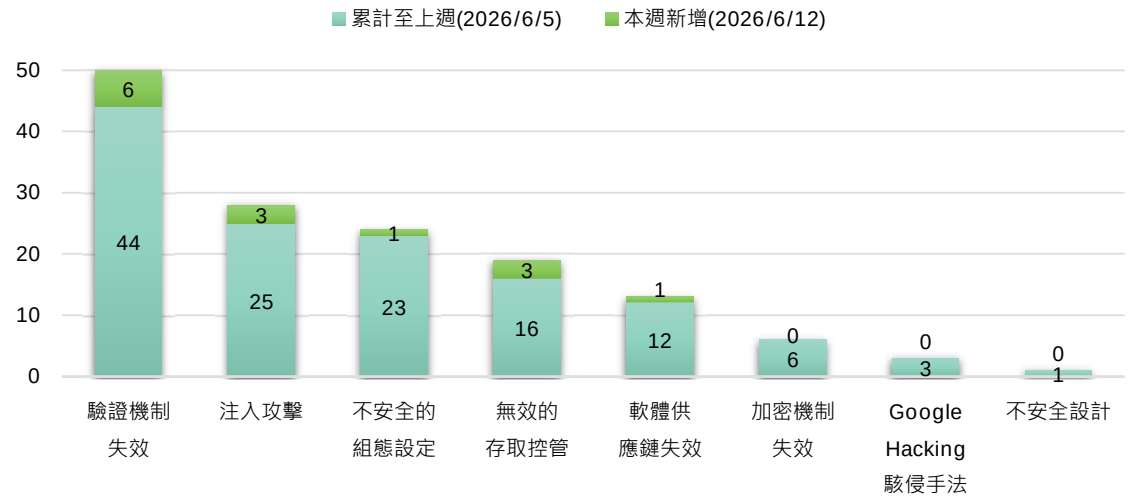

圖6 | 網路攻防演練資通系統實兵演練統計

建議機關及關鍵基礎設施提供者，採取下列防護措施

- 關閉非必要對外服務埠，如須開放使用，應限制來源IP或網段
- 停用或重新命名預設管理者帳號(Administrator)，避免攻擊者直接利用已知帳號進行密碼猜測
- 建立高強度密碼政策，避免使用常見或易猜測之密碼組合
- 設定登入失敗次數限制與帳號鎖定機制，降低暴力破解風險
- 定期檢視登入紀錄及帳號權限，建立異常登入告警機制

■網路巡查高風險詐騙

追蹤詐騙訊息與手法演變，掌握政府機關實施之打詐政策與機制，是否達成其控制目標

低門檻話術結合私訊導流成詐騙主要手法

本週高風險詐騙關鍵字分析

本週高風險詐騙訊息仍以「私訊」作為主要導流方式，但與前期相比，「免費」、「推薦」、「優惠」、「台灣」、「設計」等字眼更明顯地被用來降低民眾戒心。從廣告內容觀察，詐騙訊息常先用免費補發、限時折扣、多人推薦、台灣熱銷、專業設計等說法吸引注意，再導向私訊、LINE、短網址或不明表單，進一步要求民眾提供個資、聯絡方式、財務資料或進入付款流程，詳見圖7。

「免費」不是終點，而是引導互動的開端

本週「免費」出現頻率明顯偏高，常見於樹苗販售、保健商品、線上體驗、貸款或工作招募等情境。例如以「死苗免費補發」、「栽種後不結果全額退款」、「免費體驗」、「免費教學」、「0 元帶回家」等說法，讓民眾覺得參與成本低、風險不高，進而願意留言、私訊或加入 LINE。

提醒民眾，凡是以免費、退費、補發、零元、免頭期等話術吸引互動，但後續要求提供姓名、電話、地址、身分證件、帳戶資料，或要求先支付運費、訂金、手續費者，都應提高警覺，避免因低門檻話術而落入個資蒐集或付款陷阱。

用「推薦、台灣、安心」堆疊可信度，讓廣告看起來更像正常交易

本週「推薦」、「台灣」、「安心」、「品質」等關鍵字多次出現，廣告內容常標榜「院長親自推薦」、「台灣優質水果樹苗」、「台灣女生瘋搶」、「品質保證」、「售後無憂」等，營造商品有人背書、來源清楚、交易有保障的印象。部分內容也會加入「日本進口」、「官方認證」、「GMP 品質認證」等字眼，提高專業感。

惟上述字眼本身不代表交易安全。若賣場僅提供私訊、LINE 或短網址，且缺乏明確公司資訊、產品標示、退換貨規範及公開客服管道，仍可能涉及假賣場、假認證、誇大不實或付款後失聯風險。民眾不宜僅憑「台灣」、「推薦」、「安心」等文字即判斷可信。

把身體與生活問題包裝成「快速有感」解方

本週「健康」、「問題」、「保養」、「配方」、「身體」、「調理」、「草本」、「枇杷」等字眼集中出現，顯示保健與身體焦慮仍是主要話術之一。相關廣告常針對喉嚨乾癢

、咳嗽、血脂、代謝、體重、肝臟保養、肌膚狀態、疲勞或兒童消化等需求，搭配「一喝有感」、「三效潤喉」、「排毒」、「燃脂」、「草本配方」、「醫師親選」等說法，讓民眾誤以為商品能快速改善身體問題。

提醒民眾，凡保健商品宣稱可快速見效、改善多種症狀、逆轉身體狀況，或以醫師、院長、日本進口、專利配方作為主要賣點者，都應先查證產品來源、標示內容及是否涉及誇大療效，不宜只憑廣告案例、使用者見證或推薦說法就下單。

圖7 | 詐騙關鍵字文字雲

從「適合、必備、設計」放大需求，製造立即購買理由

本週亦可見大量商品以「適合」、「必備」、「設計」、「簡單」、「穩定」、「神器」等字眼包裝，常見於果樹苗、夏季涼鞋、保養品、居家用品及家電促銷。例如強調「適合盆栽地栽」、「新手容易照顧」、「夏日必備神鞋」、「快速繫帶設計」、「一用就有感」等，將商品描述成容易上手、馬上需要、錯過可惜的生活解方。

此類內容常再搭配「限時優惠」、「限量補貨」、「買到賺到」、「手慢等明年」等急迫語氣，促使民眾在未查證前快速下單。提醒民眾，對於商品資訊不完整、只提供短網址或要求私訊下單的廣告，應先確認賣家身分、交易平台及付款方式是否安全。

感情、緣分與在家工作話術，轉向情緒與機會焦慮

除商品與保健廣告外，本週也出現感情挽回、緣分解析、線上體驗、AI 創業及在家工作等內容，常以「老師」、「感情」、「緣分」、「體驗」、「了解」、「歡迎」等字眼吸引民眾接觸。相關廣告會透過失戀、出軌、自我懷疑、人生方向或高薪兼職等情境，讓民眾在情緒脆弱或尋找機會時，主動留言、加入 LINE 或報名體驗。

提醒民眾，凡感情諮詢、命理體驗、AI 創業、語音聊天兼職等內容，若要求提供個資、私下匯款、繳交教材費、保證金、開通費，或以高收入、快速翻身作為主要誘因，均應先暫停操作並查證業者合法性。

本週防詐提醒

1. 「私訊」仍是本週最重要的風險訊號，凡廣告要求私訊、加 LINE、留言後才提供價格、連結、教學、報名或下單方式者，應先查證商家身分與交易保障。
2. 「免費補發」、「全額退款」、「免費體驗」、「0 元帶回家」、「免頭期」等低門檻話術，不代表沒有風險；若後續要求提供個資、帳戶或先付款，應立即提高警覺。
3. 保健商品若宣稱「一喝有感」、「排毒燃脂」、「草本配方」、「醫師親選」、「日本進口」、「快速調理」等，應查證產品標示、合法來源及是否涉及誇大療效。
4. 樹苗、服飾、家電、保養品等商品若以「台灣熱銷」、「限時優惠」、「適合新手」、「必備神器」催促下單，且導向短網址或私訊交易，應先確認賣家與付款安全。
5. 感情諮詢、命理體驗、AI 創業、在家工作等廣告若要求加入群組、提供個資或先繳費，應先暫停並查證，不要因情緒焦慮或高薪誘惑而倉促操作。

綜合觀察

綜合本週資料觀察，詐騙訊息多半先以「免費」、「優惠」、「推薦」吸引互動，再以「台灣」、「安心」、「品質」、「設計」包裝可信度，並透過「健康」、「問題」、「調理」、「草本」放大需求，最後以「私訊」、「LINE」、「點擊」完成導流。尤其本週可見低門檻話術與私訊導流高度結合，從樹苗、保健品、車貸、感情諮詢到在家工作，均可能透過看似一般廣告的內容，引導民眾提供資料或付款。

提醒民眾，凡遇到不明連結、短網址、私訊交易、資訊不完整，或要求提供個資、信用卡、銀行資料及先付款才能取得商品或服務者，均應先行查證，以降低受騙風險。

焦點文章

建立中小企業資安防護力：從培訓課程到專家諮詢

本年以培訓課程、學習資源與專家諮詢三軌並進，協助中小企業逐步建立資安防護能力

近年來，資安議題與企業經營關係日益密切，無論企業規模大小，都可能面臨勒索病毒攻擊、帳號遭入侵或資料外洩等風險，而這些事件往往不僅影響資訊系統，更可能衝擊企業營運、客戶信任與商業合作關係。

然而，企業面臨的挑戰往往是在實際推動過程中，常常不知道應該從何開始準備、哪些措施最值得優先投入，以及當面臨問題時可以向誰尋求協助。因此，如何協助企業將抽象的資安概念轉化為具體可行的行動，並建立持續精進的能力，成為中小企業資安推動的重要方向。

以企業需求角度規劃資安培訓課程

為協助中小企業建立基礎資安能力，數位發展部資通安全署（以下稱資安署）與國家資通安全研究院（以下稱資安院）本年共同辦理「防駭與資料保護基礎必修課」二日培訓課程，詳見圖8，以企業最常面臨的資安風險為主軸，聚焦於「勒索病毒防護」與「企業資料保護」兩大主題，以協助企業掌握關鍵的資安觀念和實務作法。

除了專家講授基礎觀念外，課程也透過實際案例分享、企業經驗交流及實作演練等方式，引導企業從真實情境理解資安風險與可能影響，進一步思考如何將資安措施融入日常營運管理。本次課程亦邀請企業主管及資安實務工作者現身分享，從第一線經驗出發，說明企業在推動資安過程中實際面臨的挑戰，以及如何逐步建立符合自身需求的防護措施。透過同儕交流與實務分享，讓參與企業不僅學習知識，更能了解資安在企業經營中的具體應用。

圖8 | 防駭與資料保護基礎培訓課程剪影

建立持續學習的資安資源

資安能力的建立並非透過一次課程即可完成，而是需要持續累積。因此，除了實體培訓課程外，資安署與資安院近年亦持續建置適合中小企業運用的資安學習資源。

目前已發佈包含「資安星際指南」系列手冊、基礎資安線上課程、中小企業基本資安

焦點文章

防護指引及資安自檢工具等多元資源，內容涵蓋資安基礎概念、網路安全管理、資料保護、系統委外安全及資安制度建立等主題，協助企業依據自身需求選擇合適的學習方式，建立資安防護能力。

這些資源的共同特色即是將專業資安知識轉譯為企業能夠理解與實踐的具體行動，協助企業從日常營運出發，逐步建立符合自身需求的資安管理機制。

中小企業資安專家會客室 - 諮詢會談服務啟動

為協助企業進一步將學習成果落實於組織管理與日常作業，資安署與資安院將於本年下半年推出「中小企業資安專家會客室」諮詢服務。

本服務採一對一專家諮詢方式辦理，經媒合後，由資安專家依據企業現況與需求提供深度交流與建議，協助企業盤點風險、釐清問題，並規劃後續改善方向。與一般課程著重知識傳遞不同，諮詢服務可針對企業實際資安痛點，提供客製化的改善建議。本次諮詢服務聚焦於三項中小企業最常關注的資安議題，包含：

1. 勒索病毒防護與復原：協助企業檢視現有防護措施、資料備份機制及災難復原準備情形，了解面對勒索病毒事件時的應變能力與復原規劃。
2. 企業機敏資料保護：協助企業盤點重要資料與權限管理機制，檢視資料保護措施及帳號管理流程，降低資料外洩風險。
3. 資安管理與制度建立：協助企業從資安政策、風險評估、事件應變流程等面向檢視現況，逐步建立符合組織需求的管理制度與運作機制。

企業於會談後還可獲得專屬行動建議備忘錄，作為後續推動改善工作的參考依據，協助企業將討論內容轉化為可落實的行動方案。

持續推動中小企業資安能力

從第一期課程(6月5至6日)交流過程中可以觀察到，企業對於資安需求已逐漸從「認識風險」進一步走向「如何落實」，並期待獲得更多符合實際營運情境的指引與協助。

第二期「防駭與資料保護基礎必修課」將於7月17日至18日辦理，提供實體與線上參與方式，持續開放報名中；「中小企業資安專家會客室」諮詢服務亦已開放預約，希望透過與

焦點文章

專家諮詢交流，協助企業將課程所學進一步轉化為具體可執行的改善措施。

未來資安署與資安院將持續透過培訓課程、學習資源與專家輔導等多元方式，協助更多中小企業建立符合自身需求的資安防護能力，讓資安真正融入企業日常營運之中，詳見圖9。

圖9 | 資安署與資安院共同辦理中小企業資安培訓課程合影

相關資源

【防駭與資料保護基礎必修課】課程資訊與報名：https://reurl.cc/L2bDDL

【中小企業資安專家會客室】資安諮詢會談線上預約：https://reurl.cc/9W8lej

【資安星際指南手冊】全系列電子版：https://reurl.cc/Wb2v8L

關鍵字：中小企業資安、資安學習資源、資安意識推廣

刊　　名　資安週報第 49 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