



國家資通安全研究院

National Institute of Cyber Security

資安週報

Cyber Security Weekly Newsletter

外部曝險分析

整體風險微幅下降 弱加密項目改善但憑證與WAF曝險增加

重大漏洞

Microsoft、SonicWall及Cisco高風險漏洞應盡速修補

實兵演練

實兵演練揭露網站系統已知漏洞 致管理員權限遭未授權取得風險

聯防監控

偵測刺探高居首位 防禦迴避仍具威脅

蜜罐誘捕

網站主機伺服器管理系統及程式遞送控制器(ADC&Gateway)仍為攻擊熱點

事件通報

API應驗證使用者對指定資料之存取權限

網路巡查高風險詐騙

金融投資占比持續上升 產品服務仍為主要風險類型

焦點文章

關鍵基礎設施資安防護檢測發現事項研析

2026.09.17

062

資安儀表板

外部曝險分析、重大漏洞、實兵演練、聯防監控、蜜罐誘捕、事件通報及網路巡查高風險詐騙等七類量化指標

■ 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

整體風險微幅下降 弱加密項目改善但憑證與WAF曝險增加

本次針對93個A、B級關鍵基礎設施(CI)進行EASM資安曝險檢測，前10大風險項目共計2,758項。其中，「元件高風險漏洞」以888項居首，「過時或弱加密協定」725項次之，「TLS憑證不受信任」641項位居第三。前三項合計2,254項，占前10大風險項目總數約81.7%，顯示目前外部曝險風險仍高度集中於元件漏洞、加密協定及憑證管理等議題。相較上期2,803項，本期整體風險數量減少45項，降幅約1.6%，詳見圖1。

進一步分析主要風險變化情形，「元件高風險漏洞」仍為最大宗風險，數量由上期884項增至本期888項，增幅約0.5%。其中，Apache HTTP Server相關弱點(CVE-2024-38475)仍為主要風險來源，該弱點可能造成原始碼洩漏或程式碼執行風險，建議升級至2.4.60以上之已修補版本。「過時或弱加密協定」由807項減至725項，降幅約10.2%；「TLS憑證不受信任」由603項增至641項，增幅約6.3%。另「CSP設定不當」由239項減至235項，降幅約1.7%；「未部署WAF」由121項增至131項，增幅約8.3%。

整體而言，本期外部曝險風險呈現部分改善、部分上升之情形。其中，「過時或弱加密協定」降幅最為明顯，「CSP設定不當」亦較上期減少，顯示部分機關於加密通訊及網站安全設定方面已有改善；惟「元件高風險漏洞」、「TLS憑證不受信任」及「未部署WAF」均較上期增加，顯示元件修補、憑證管理及網站應用程式防護仍有持續強化空間。建議持續落實高風險元件漏洞修補與版本更新，並加強TLS憑證有效性及信任鏈管理，同時評估部署WAF等防護機制，以降低外部資產遭受攻擊及曝險之風險。

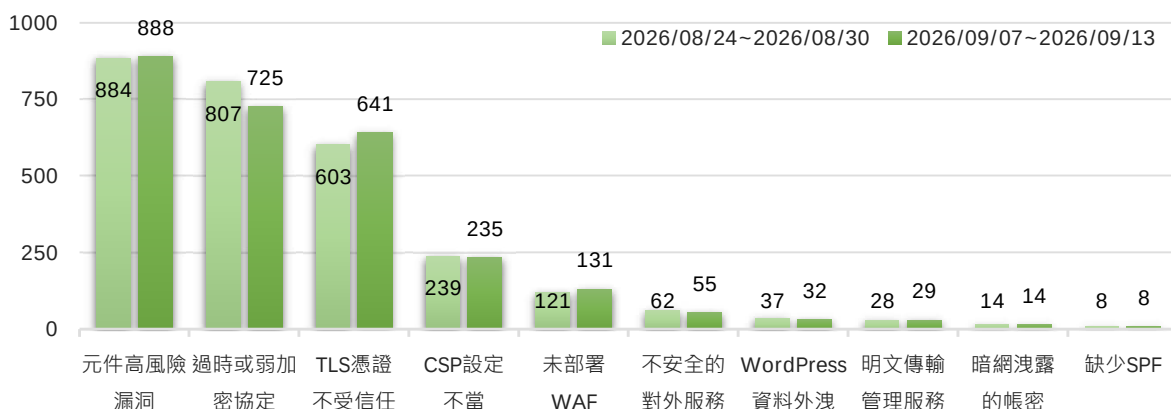


圖1 | EASM檢測結果統計(前10大風險)

防護建議

建議受測單位採取下列防護措施

- 優先修補對外服務所使用元件之高風險漏洞，並依原廠安全公告更新至已修補版本；如短期內無法完成升級，應採取WAF、虛擬修補、來源存取限制或網路區隔等補償性措施，以降低漏洞遭利用之風險
- 依據IETF RFC 10015，檢視TLS 1.2所使用之金鑰交換機制，停用較舊或安全性較低之方式，並優先採用ECDHE等具前向保密性之安全機制，以強化加密通訊安全
- 強化TLS憑證管理，定期檢視憑證有效期限、信任鏈及憑證狀態，並建立到期通知及自動續期機制，避免因憑證失效造成服務異常或安全風險
- 定期檢視網站CSP及WAF等防護設定，並依系統功能及實際業務需求調整安全政策，以降低跨網站腳本、惡意請求及其他

Web攻擊風險

建議受測單位採取下列管理措施

- 建立並定期維護對外資產清冊，納管IP、網域、系統元件及憑證等資訊，以掌握各項資產之用途、版本及使用情形
- 建立高風險漏洞之修補、追蹤及複測機制，依漏洞嚴重程度訂定修補期限，並於完成修補後進行複測，確認改善措施有效落實
- 定期盤點系統所使用之軟體及第三方元件版本，持續追蹤原廠安全公告及CVE弱點資訊，並適時進行版本更新，降低使用已停止支援或存在已知弱點元件之風險
- 將漏洞修補、憑證更新、安全設定調整及後續複測等要求納入委外維運管理，明確訂定處理時限、責任分工及追蹤方式，以確保各項改善措施確實執行

■ 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、SonicWall及Cisco高風險漏洞應盡速修補

- Microsoft Exchange Server存在身分鑑別繞過(Authentication Bypass)漏洞(CVE-2026-62911)¹，已通過身分鑑別之遠端攻擊者可誘使使用者操作特製內容，用以攔截並重送身分鑑別憑證，藉此繞過伺服器之身分鑑別機制，進而提升權限並取得伺服器上使用者信箱之存取權。
- SonicWall NSM On-Prem與SMA1000系列存在多項高風險安全漏洞(CVE-2026-78327、CVE-2026-83548及CVE-2026-83549)^{2 3}，類型包含作業系統指令注入(OS Command Injection)與伺服器請求偽造(Server-Side Request Forgery)。其中，CVE-2026-83548與CVE-2026-83549已遭駭客利用。
 - CVE-2026-78327：已取得管理權限之遠端攻擊者，可藉由於管理介面注入任意作業系統指令，進而於底層主機執行任意程式碼。
 - CVE-2026-83548：未經身分鑑別之遠端攻擊者可利用非預期之替代存取路徑，存取敏感功能並執行未經授權之操作。
 - CVE-2026-83549：於特定條件下，已通過身分鑑別之遠端攻擊者，可透過管理主控台(AMC)以管理員身分執行任意作業系統指令，進而執行任意程式碼。
- Cisco IOS XR Software存在多項高風險安全漏洞(CVE-2026-20274、CVE-2026-20275、CVE-2026-20278、CVE-2026-20279及CVE-2026-20280)⁴，類型包含不當資源生命週期控制(Improper Control of a Resource Through Its Lifetime)、計算錯誤(Incorrect Calculation)、不當中和處理(Improper Neutralization)、不當存取控制(Improper Access Control)及不當檢查或處理異常狀況(Improper Check or Handling of Exceptional Conditions)，未經身分鑑別或已通過身分鑑別之遠端攻擊者可利用該等漏洞，造成系統機密性、完整性或可用性受影響。

1. <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-62911>

2. <https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2026-0015>

3. <https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2026-0016>

4. <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-hardening-iosxr-qg64NcM>

■ 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

實兵演練揭露網站系統已知漏洞 致管理員權限遭未授權取得風險

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9/11止已累計370筆攻擊紀錄，本週新增弱點數量共41筆，分別為「不安全的組態設定」10筆、「軟體供應鏈失效」10筆、「無效的存取控管」8筆、「注入攻擊」7筆、「加密機制失效」3筆及「驗證機制失效」3筆，詳見圖2。

本週演練發現，衝擊性較高之弱點為「軟體供應鏈失效」。攻擊者於瀏覽網頁時發現系統使用某網站建置系統建置網站，並經查詢公開漏洞資訊後，發現存在CVSS v3.1分數為9.8(Critical)之嚴重弱點，屬於使用用戶端驗證(Use of Client-Side Authentication)弱點。攻擊者使用網頁開發人員工具檢視系統前端程式內容，取得網站管理員相關資訊，進一步輸入攻擊語法，成功取得管理員權限。登入系統後，攻擊者可使用管理功能新增資料，並確認成功修改公開頁面內容。

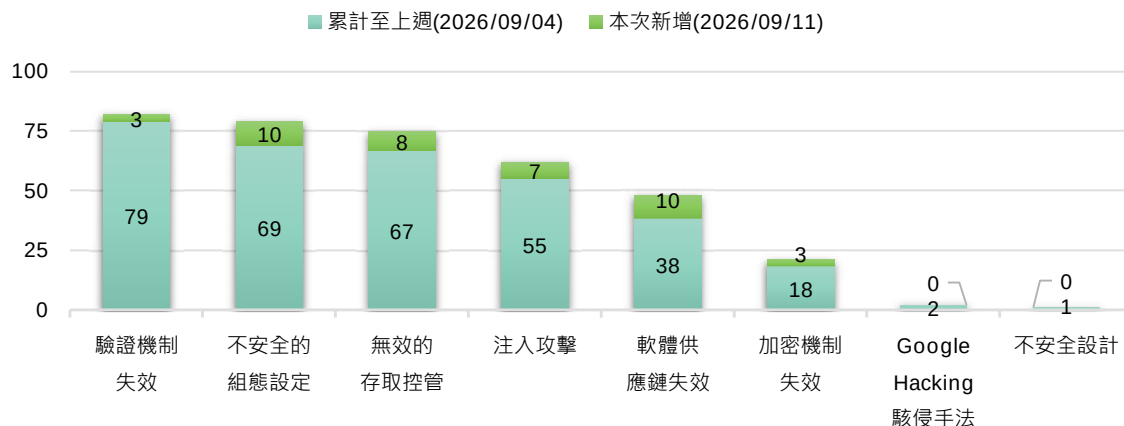


圖2 | 網路攻防演練資通系統實兵演練統計

建議機關及關鍵基礎設施提供者，採取下列防護措施

- 應定期盤點相關設備與版本，持續追蹤CVE漏洞資訊，針對已知高風險漏洞儘速完成安全修補
- 系統身分驗證與權限控管應於後端完整驗證，避免僅依賴前端程式碼或參數判定使用者身分與權限
- 應避免於前端程式碼中揭露管理員帳號或身分識別資訊，降低攻擊者取得管理員資訊並進行身分冒用之風險

■ 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

偵測刺探高居首位 防禦迴避仍具威脅

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。「偵測刺探」為最常見攻擊手法，占比13.6%，顯示攻擊者持續加強對目標環境的前期偵查與弱點探測活動，以掌握對外暴露資產及潛在攻擊入口。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外部網段及公開服務進行大規模探測，以識別可存取主機、開放埠及服務資訊，並進一步針對目標系統進行漏洞掃描，尋找可能遭利用的已知弱點。此類活動通常呈現由廣泛網路掃描逐步聚焦至特定系統與漏洞的特徵，為後續漏洞利用及初始入侵的重要前置作業。建議機關持續監控異常掃描流量與可疑來源，定期盤點對外暴露資產並優先修補高風險漏洞，同時結合威脅情資進行來源分析與阻擋，以提前辨識攻擊者的偵查活動並降低後續入侵風險。

「防禦迴避」事件本週占比為12.4%，為本週占比次高的攻擊階段，顯示攻擊者持續透過規避監控、削弱日誌紀錄及隱藏操作痕跡等方式，降低惡意活動遭安全機制偵測的可能性。觀察到的主要手法包括削弱指令歷程記錄、間接指令執行、以及清除指令歷程。攻擊者可能停用或修改系統指令歷程記錄功能，以降低操作行為的可追溯性，並藉由合法程序、系統元件或其他間接方式執行指令，以規避既有偵測規則；部分活動亦會於完成操作後主動清除 Shell 或指令歷程，進一步隱藏攻擊軌跡並增加事件調查與鑑識難度。此類行為具有高度隱蔽性，可能使攻擊者延長於受駭環境中的潛伏時間。

建議機關強化指令執行及日誌異常變更行為的監控，落實集中式日誌保存與完整性保護，並針對異常程序鏈及間接指令執行建立偵測與告警機制，以降低攻擊者規避防禦及隱匿活動的風險。

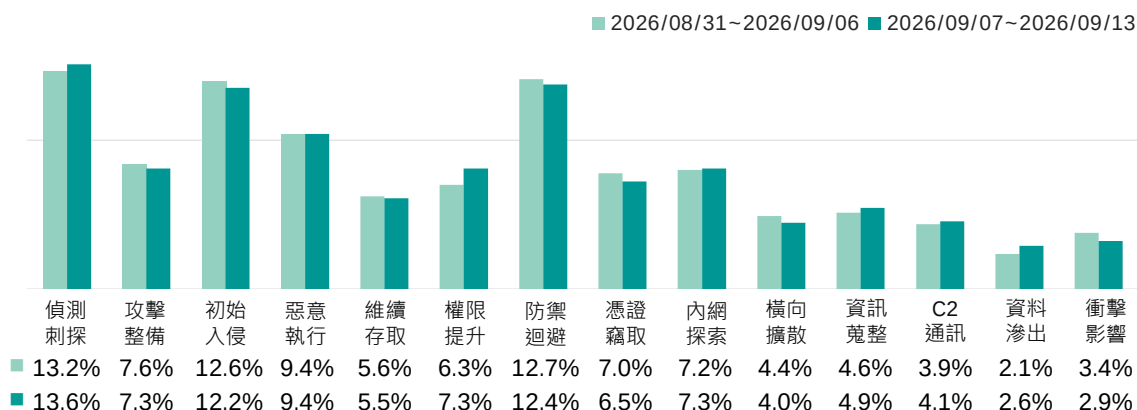


圖3 | 資安聯防監控攻擊階段統計



防護建議

建議機關採取下列防護措施



偵測刺探 (Reconnaissance)



持續監控異常掃描流量、短時間大量連線及可疑來源 IP



定期盤點對外暴露的主機、服務、開放埠及網路資產，降低非必要服務暴露



優先修補高風險及已知遭利用漏洞，降低掃描後遭進一步利用的風險



結合威脅情資分析掃描來源，針對高風險或重複性來源進行告警及阻擋



防禦迴避 (Defense Evasion)



強化 PowerShell、Shell、CMD 等指令執行與異常操作行為監控



監控指令歷程遭停用、修改或清除等異常行為，並建立相關告警規則



採集中式日誌保存並強化完整性保護，避免攻擊者竄改或刪除本機紀錄



監控異常父子程序、程序鏈及間接指令執行行為，辨識利用合法工具規避偵測的活動

■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

網站主機伺服器管理系統及程式遞送控制器(ADC & Gateway)仍為攻擊熱點

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80.34%、「遠端控制」服務攻擊占比16.63%，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71.73%。「遠端控制」服務亦有25.66%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服務系統比例大幅下降主因為Cisco Secure ASA & FTD 缺少授權漏洞之CVE-2025-20362，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。

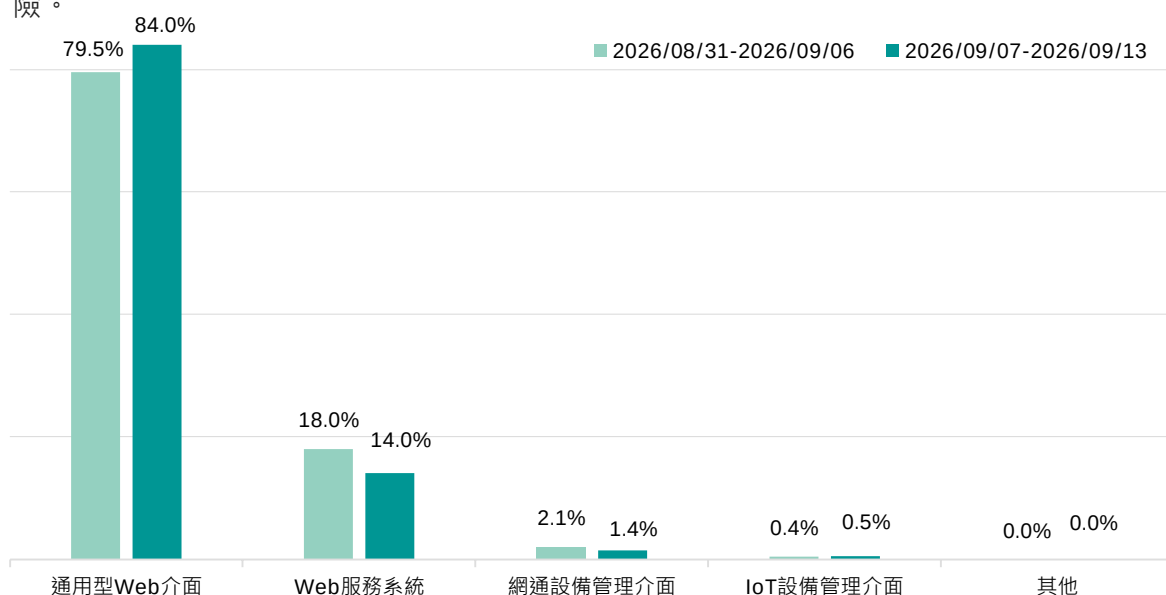


圖4 | 本週網頁應用介面之誘捕攻擊比例統計

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1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身分驗證繞過漏洞、越界讀取漏洞及指令注入漏洞，攻擊目標涵蓋網站主機伺服器管理系統、程式遞送控制器(ADC&Gateway)、大模型API統一介面與代理伺服器工具、資安防護系統及雲端檔案管理平台與企業行動裝置安全存取控制系統。

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1年漏洞排行列表

排名			漏洞編號	受影響產品	CVSS 3.x Base Score	已知遭利用漏洞 (KEV)
■	1	-	CVE-2026-41940 ¹	cPanel & WHM	9.8	✓
■	2	-	CVE-2026-3055 ²	NetScaler ADC & Gateway	9.8	✓
■	3	-	CVE-2026-42271 ³	LiteLLM	8.8	✓
■	4	↑1	CVE-2026-2699 ⁴	Progress ShareFile	9.8	
■	5	↑new	CVE-2026-10520 ⁵	Ivanti Sentry	10	✓

類型 ■ 身分驗證繞過漏洞 ■ 越界讀取漏洞 ■ 指令注入漏洞

1. <https://nvd.nist.gov/vuln/detail/CVE-2026-41940>

2. <https://nvd.nist.gov/vuln/detail/CVE-2026-3055>

3. <https://nvd.nist.gov/vuln/detail/CVE-2026-42271>

4. <https://nvd.nist.gov/vuln/detail/CVE-2026-2699>

5. <https://nvd.nist.gov/vuln/detail/CVE-2026-10520>

■ 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

API應驗證使用者對指定資料之存取權限

本週總計接獲25件公務機關與特定非公務機關事件通報，詳見圖5，公務機關非法入侵事件中以未經授權存取占多數，相關事件多與網站身分驗證及存取控制機制缺失遭利用有關，詳見圖6。本週發現機關網站API以會員ID作為資料查詢條件，未要求Cookie、Token或Session等身分驗證資訊，即可回傳對應會員之身分證號、姓名、地址、電話及電子郵件等個人資料；攻擊者僅需變更會員ID，即可能進一步取得其他會員資料。

建議機關檢視涉及 ID、案件編號或其他資料識別值之 API，於後端依使用者身分、角色及權限確認其可存取之資料範圍，不應僅依外部傳入之識別值直接回傳資料；測試時亦應嘗試變更相關識別值，確認無法取得或操作超出權限範圍之資料。另可參考 OWASP 建議，使用較難預測的 GUID/UUID 取代連續編號，降低識別值遭猜測及大量列舉的風險，但仍不得取代後端實際的權限檢查。

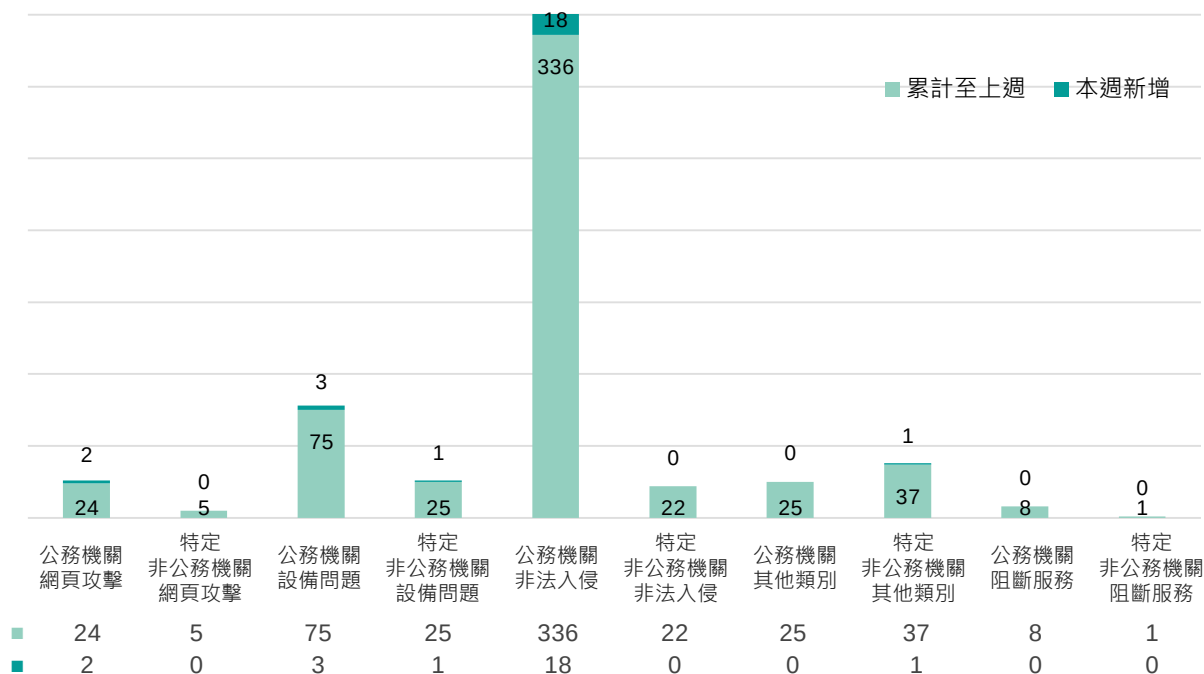


圖5 | 本週公務機關暨特定非公務機關資安事件通報概況

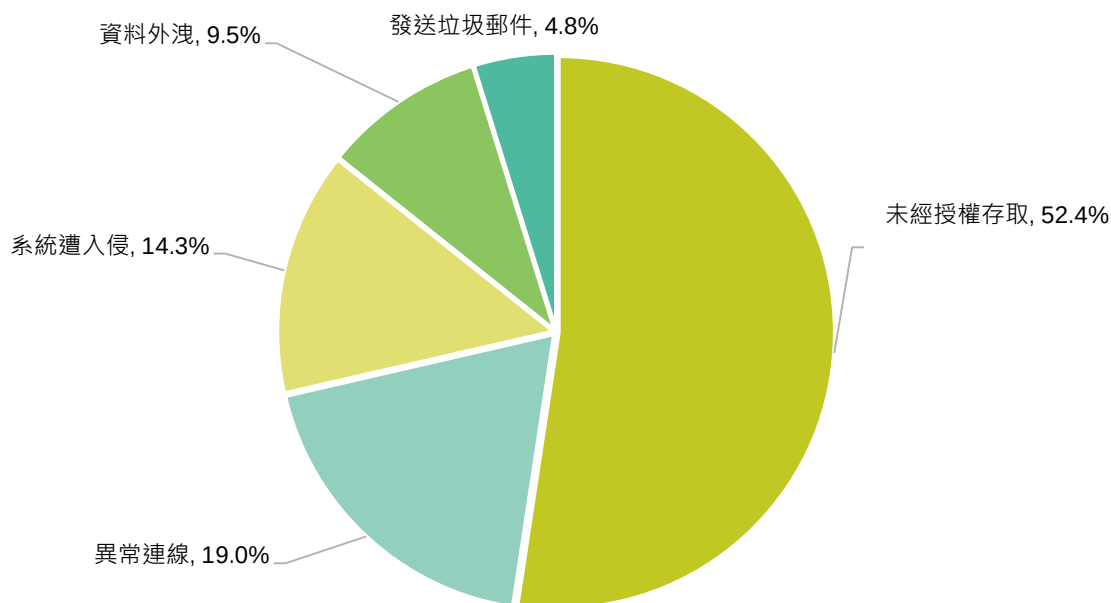


圖6 | 本週公務機關非法入侵事件類型占比

防護建議

除修補漏洞外，應：

以攻擊為出發評估潛在風險

- 攻擊者竄改會員ID大量列舉並取得其他會員個人資料
- API缺乏身分驗證及權限檢查造成跨帳號敏感資料外洩

針對潛在風險執行相應改善

- 每次API請求均應驗證使用者身分與權限，禁止僅依會員ID回傳資料
- 後端應依帳號角色限制可查詢資料範圍，防止跨帳號越權存取
- 測試時應變更ID及案件編號等識別值，確認無法取得非授權資料
- 可採GUID或UUID降低識別值遭猜測風險，但不得取代後端權限檢查

3間民間企業揭露重大資安訊息

本週3間民間企業發布重大訊息，產業類別為通信網路業、數位雲端業、生技醫療業，詳見表2。

表2 | 本週民間企業重大資安訊息彙整

公司名稱	發布時間	事件說明
富爾特科技股份有限公司	2026年09月07日	富爾特之子公司格帝控股偵測到部份伺服器遭受網路勒索病毒攻擊，資安團隊於偵測到異常之第一時間，已立即啟動防禦機制與斷網隔離措施，並啟動相關資安應變機制，全面檢視資安系統與加強相關防護。對公司整體營運及財務尚不致有重大影響，後續將持續密集監控，並強化網路與資訊基礎架構之管控，以確保資訊系統安全。
台灣大車隊股份有限公司	2026年09月09日	車隊之重要子公司全球商務發現部分資訊系統遭受網路攻擊，已立即啟動資安應變機制，並委請資安專業人員進行事件調查、系統修復及影響範圍盤點。現階段尚無直接證據顯示客戶資料已遭下載、複製或外洩，相關資料是否曾遭未授權存取及實際影響範圍，仍持續調查確認中。後續將持續進行資安鑑識、系統安全強化及相關風險控管作業；如調查結果或事件發展有重大變化，將依相關法令規定辦理資訊揭露。

表2 | 本週民間企業重大資安訊息彙整 (續)

公司名稱	發布時間	事件說明
達爾膚生醫科技股份有 限公司	2026年09月11日	達爾膚公司部分內部資訊系統遭受網路攻擊事件，於偵測異常後立即啟動資訊安全應變機制與斷網隔離措施，全面檢視資安系統與加強相關防護，初步評估對公司營運無重大影響，截至目前亦未發現個資外洩情形。後續將持續強化網路與資訊基礎架構之安全管控，以確保資訊安全。

■ 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

金融投資占比持續上升 產品服務仍為主要風險類型

詐騙類型趨勢

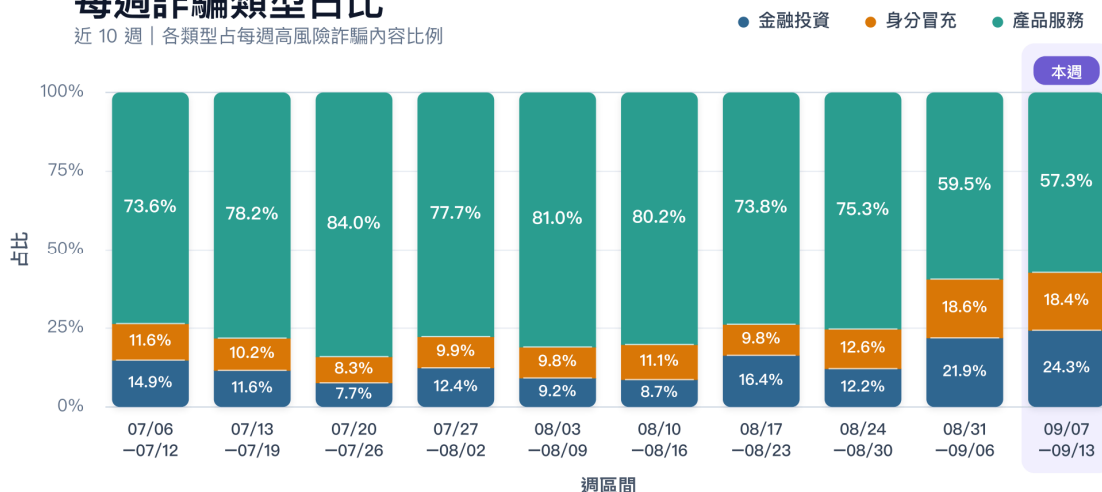
金融投資型占比持續上升，仍為本週第二大高風險類型，個人財務規劃教學與股票期貨課程以改善財務狀況為訴求，搭配交易紀律及實戰策略吸引學習者。廣告搭配講師經驗、學員人數建立專業形象，以免費體驗課程吸引報名，詳見圖7。

身分冒充型占比小幅回落，宣稱可改善皮膚問題的商品與護眼商品借用醫院團隊、醫師推薦及機關認證營造可信度。廣告聲稱不必到醫院處理皮膚問題、無需手術即可改善眼疾，再搭配使用者見證、限時優惠價格或退貨承諾吸引購買。

產品服務型占比持續下降但仍居首位，男性保健與減重商品以效果保證吸引注意，旅行收納用品則強調防盜設計與最後一次團購機會。這些內容分別以改善身體狀況的承諾、出遊安全需求及限時購買訴求，推動民眾下單或留言索取團購連結。

每週詐騙類型占比

近 10 週 | 各類型占每週高風險詐騙內容比例



註：各週三類占比合計為 100%；本週以淡色區塊標示。

資料期間：2026/07/06—09/13

圖 7 | 每週詐騙類型占比

關鍵字趨勢

「優惠」仍居首位，詳見圖8，與退至第 10 名的「輕鬆」分別出現在男性保健及減重商品，以醫師親自測試、無副作用或不復胖等宣稱吸引注意。「限量」維持第 3 名，轉以免費命理諮詢、運勢解析及每日名額限制招攬預約，透過留言或加入通訊軟體帳號，將改善生活的期待帶入後續互動。

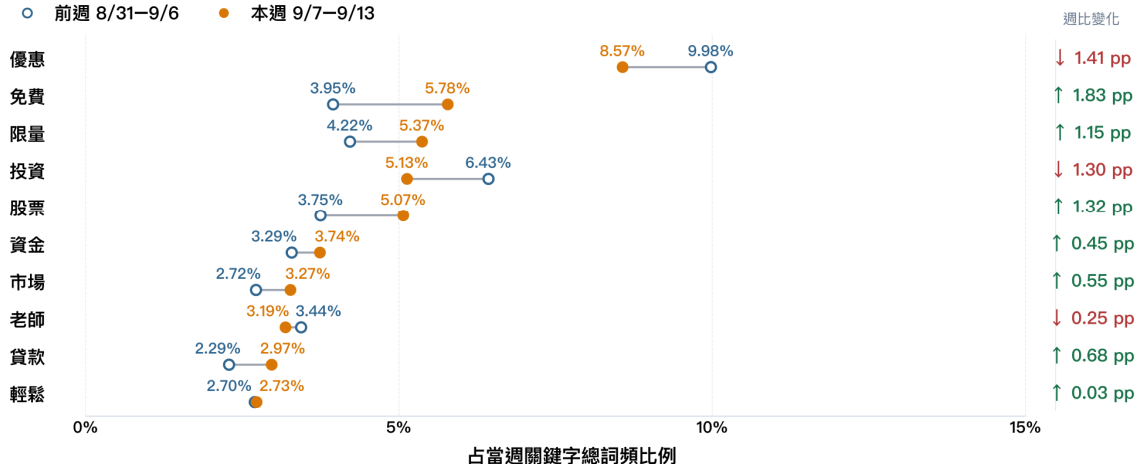
「投資」退居第 4 名，「股票」維持第 5 名，「市場」升至第 7 名，相關課程以財務規劃、數據判讀及多空交易策略吸引學習者。退至第 8 名的「老師」則由前週命理服務轉向存股投資教學，運用實務案例建立專業形象，搭配限時優惠與分期付款吸引民眾購買課程。

「免費」升至第 2 名，與升至第 6 名的「資金」共同聚焦借貸，透過免費諮詢、貸款額度試算與降低每月還款金額等訴求引導民眾傳送訊息。新進前十名的「貸款」位居第 9 名，廣告以購車折扣、零頭期款及較低的每月還款金額，吸引民眾私訊詢問貸款條件。本週從功效保證、投資教學到借貸服務，以效果、專業與付款便利回應需求。

詐騙關鍵字占比週比變化

以本週為主 | 完整顯示本週 Top 10

○ 前週 8/31-9/6 ● 本週 9/7-9/13



註：占比 = 關鍵字出現次數 ÷ 當週檔案所列關鍵字出現次數總和；pp 為百分點。

圖8 | 詐騙關鍵字占比週比變化

焦點文章

關鍵基礎設施資安防護檢測發現事項研析

■ 整體檢測發現概述

關鍵基礎設施承載能源、水資源、交通及其他重要民生服務，其資訊技術(IT)與營運技術(OT)環境除須面對日益複雜之網路威脅，更須兼顧設備穩定與營運持續性。因此，關鍵基礎設施之資安防護除既有弱點掃描與安全設備監控外，亦須透過持續性威脅狩獵(Threat Hunting)，從實際網路通訊、端點行為、帳號使用及設備組態等面向，掌握場域實際安全狀態。

國家資通安全研究院於115年上半年度執行一系列關鍵基礎設施資安防護檢測，綜整各受測場域結果發現，雖各單位之產業特性、系統架構及設備種類有所差異，惟整體發現事項仍具有相當程度之共通性。多數問題並非源自單一設備或特定弱點，而是反映資產管理、網路通訊、遠端維護、身分管理及設備安全設定等基礎資安管理機制仍有持續精進空間。尤其OT設備生命週期普遍較長，且須兼顧製程穩定性與營運持續性，使部分系統較難比照一般資通系統頻繁更新或調整設定，更凸顯持續性檢測與風險管理之重要性。

綜整檢測結果，可將常見發現歸納為治理層、網路層、邊界層、端點層、身分層及組態層等六個面向，藉由不同層面之交叉分析，進一步掌握場域管理制度與實際運作狀況間之落差。

■ 治理層：資產可視性與管理完整性

檢測期間於各受測場域均發現未列於資產清冊之IP位址、設備或服務，顯示部分資產於建置、異動或維護後，未能同步完成資產清冊更新。此類問題與工控環境設備生命週期長、系統持續擴充，以及涉及不同管理與維護單位等特性有關，容易造成現場實際設備與既有管理文件不一致之情形。

資產可視性不足除影響日常管理外，亦可能使部分設備未納入弱點盤點、修補、帳號管理及安全監控範圍。因此，除定期資產盤點外，亦應將設備建置、異動、移除及汰換納入生命週期管理，並適度結合被動式資產盤點及網路流量分析，持續比對資產清冊與實際網路活動，以提升資產管理之完整性。

焦點文章

網路層：未加密通訊與認證資訊暴露風險

透過長時間網路流量側錄與封包分析，發現部分設備管理介面或系統服務仍使用HTTP與Telnet等明文傳輸通訊協定，相關帳號密碼與認證資訊可直接由封包內容辨識。此類情形多與既有工控設備建置年代較早，以及後續系統整合仍須維持設備相容性有關。

由於部分管理介面具備設備設定修改或系統管理等高權限功能，一旦認證資訊遭取得，可能進一步衍生未授權存取風險。因此，應優先採用具加密機制之安全通訊協定。對於受設備限制而無法立即改善者，則可透過網路分區、限制管理來源及專屬維護網段等替代性措施降低風險。

邊界層：外部連線與遠端維護管理

檢測期間發現部分場域存在對外連線與遠端維護工具相關通訊。由於設備原廠維護、系統更新、授權驗證及資料交換等作業均可能產生必要之外部連線，因此外部通訊本身並不必然代表異常，其管理重點應在於連線是否符合實際業務需求、是否經適當授權，以及是否建立相對應之管理與監控機制。

若用途不明、未經授權或長期未受管理之外部通訊持續存在，可能增加外部攻擊與未授權遠端存取之風險。因此，應持續盤點外部通訊需求，並建立外部連線基準，記錄合法連線之目的、設備、通訊對象及使用期間，對已無需求之連線予以停用，必要連線則納入申請、審查及定期檢討機制。

端點層：已知弱點與軟體生命週期管理

端點檢測結果發現，部分OT工作站與工程師維護主機仍使用已停止支援(End of Life, EOL)之軟體版本，或存在已公開揭露之已知漏洞。由於工控系統須優先維持穩定運作，部分應用程式亦與特定設備、驅動程式或系統版本相依，軟體更新可能衍生相容性與營運風險，使部分場域無法比照一般IT環境即時進行更新。

對於無法立即修補之設備，應依設備特性採取限制對外連線、強化網路存取控制、縮減可

焦點文章

存取範圍及持續監控等替代性防護措施，並將版本更新納入年度停機維護或設備汰換規劃，以降低已知漏洞長期存在所造成之風險。

身分層：帳號權限與遠端存取管理

檢測結果亦發現部分場域存在共用帳號與高權限帳號長期使用，以及透過RDP、AnyDesk及TeamViewer等工具進行遠端維護之情形。由於關鍵基礎設施須維持全年不中斷運作，設備故障排除與原廠技術支援等作業可能須透過遠端方式進行，因此管理重點並非全面禁止遠端維護，而是確保實際操作人員可識別、使用權限受到適當限制，且操作過程具備可追蹤性。

因此，應建立遠端維護申請、核准、執行及結束確認等管理程序，並完整保留相關操作紀錄。同時逐步降低共用帳號之使用比例，依實際使用者與工作職責配置適當權限，並透過定期帳號盤點與權限審查，降低帳號遭不當使用之風險。

組態層：設備安全組態與持續性檢核

設備組態分析發現，部分防火牆、核心交換器及其他網通設備仍存在預設功能未調整、管理服務限制不足、帳號安全設定未完善及日誌記錄功能未完整啟用等情形。此類問題多與設備建置後長期投入營運，後續維護較著重於服務可用性，而較少重新檢視安全組態有關。

設備安全組態應由一次性建置工作逐步轉變為持續性管理機制，配合設備異動、韌體更新及年度維護作業，定期檢視各項安全設定，並可運用自動化工具比對設備組態與安全基準之差異，以降低設定偏離與人工檢查疏漏所造成之風險。

綜合研析與後續防護重點

綜合上半年度檢測結果可發現，關鍵基礎設施場域之資安風險往往並非源自單一高風險弱點，而是由多項基礎管理與技術控制缺口長期累積而形成。資產未完整納管可能形成監控盲點，未加密通訊可能造成認證資訊暴露，未受管理之外部連線可能增加遠端存取風險，若再結合未修補端點、高權限帳號及不安全設備組態，個別問題即可能相互影響並擴大整體風險。

因此，威脅狩獵之價值不應僅著重於發現單一弱點，而應透過長時間蒐集與分析實際網路與端點活動，掌握管理制度、設備設定與實際運作間之落差。後續防護亦應由單點修補逐步朝

焦點文章

持續性管理發展，將資產盤點、網路監控、弱點管理、外部連線、帳號權限及設備組態納入常態性檢視與改善追蹤機制。

透過持續性威脅狩獵與改善機制，可使檢測成果由單次風險發現進一步轉化為場域安全態勢掌握與防護措施驗證之依據，協助關鍵基礎設施單位持續提升整體資安防護能力與營運韌性。

關鍵字：關鍵基礎設施、資安防護檢測、威脅狩獵

刊 名 資安週報第 62 期
發 行 人 國家資通安全研究院 龔化中院長
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