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

資安週報

Cyber Security Weekly Newsletter

2026.03.26
037

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

內部系統對外開放應審慎評估必要性與存取範圍 以降低資安風險

本週總計接獲13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。有機關於例行檢視郵件伺服器日誌時，發現異常佇列及國外 IP 登入後發信情形，且寄件紀錄遭刪除，研判可能因社交工程郵件導致帳號密碼外洩並遭濫用。

原僅供內部使用之系統一旦開放外部存取，其風險即隨之提高。機關於提供遠端使用便利性時，應審慎評估開放必要性與範圍，避免預設全面對外開放；如確有需求，建議限制存取來源（如評估是否開放國外 IP），並採取多重保護措施（如強化身分驗證及存取管控），以降低不必要之暴露風險。

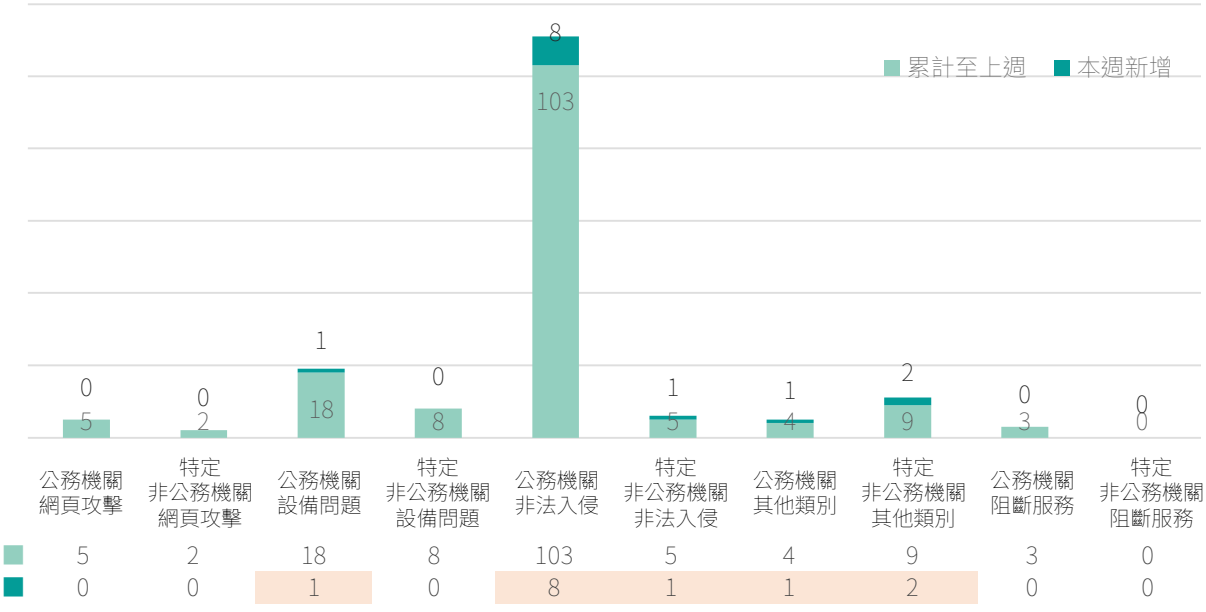

圖1 | 本週公務機關暨特定非公務機關資安事件通報概況

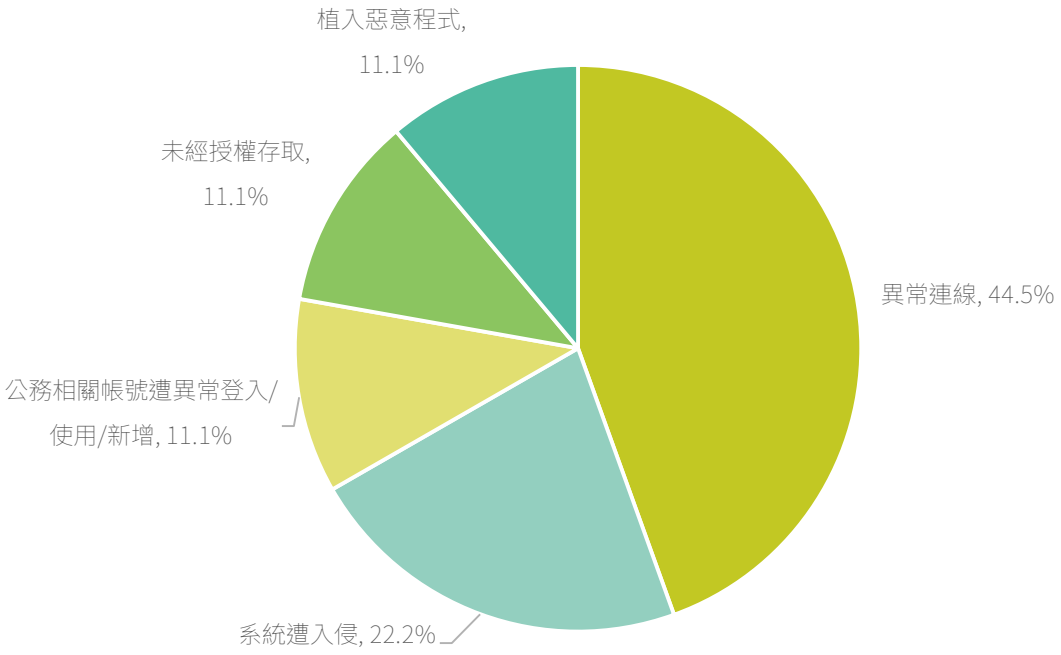

圖2 | 本週公務機關非法入侵事件類型占比

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
➢ 利用帳密外洩遠端登入郵件系統發信 ➢ 刪除郵件紀錄掩蓋攻擊行為軌跡	➢ 強制導入多因子鑑別機制，降低帳號密碼外洩後遭濫用風險 ➢ 建立來源IP與地理位置限制機制，阻擋異常或境外登入行為 ➢ 強化郵件系統日誌保存機制，確保異常行為可追蹤與分析 ➢ 定期辦理社交工程演練與教育訓練，提升人員資安防護意識

◎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13.5%，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12.0%，為本週占比次高的階段，顯示攻擊者持續加強對目標環境的前期偵查與情報蒐集行動。觀察到的主要手法包括主動式掃描、IP 區段掃描、以及DNS 與被動式 DNS 情資蒐集。攻擊者除透過主動掃描大量網段以識別對外服務與開放埠外，亦利用被動式 DNS 資料分析目標組織之網域結構、子網域關聯與歷史解析紀錄，以建立更完整的攻擊面視圖。此類行為結合主動與被動技術，能有效降低被偵測風險，同時提升後續攻擊的精準度。建議強化對異常掃描流量的監控與阻擋機制，並定期盤點與管控公開資產與DNS資訊曝光情形，搭配威脅情資分析，以提前掌握潛在攻擊準備活動。

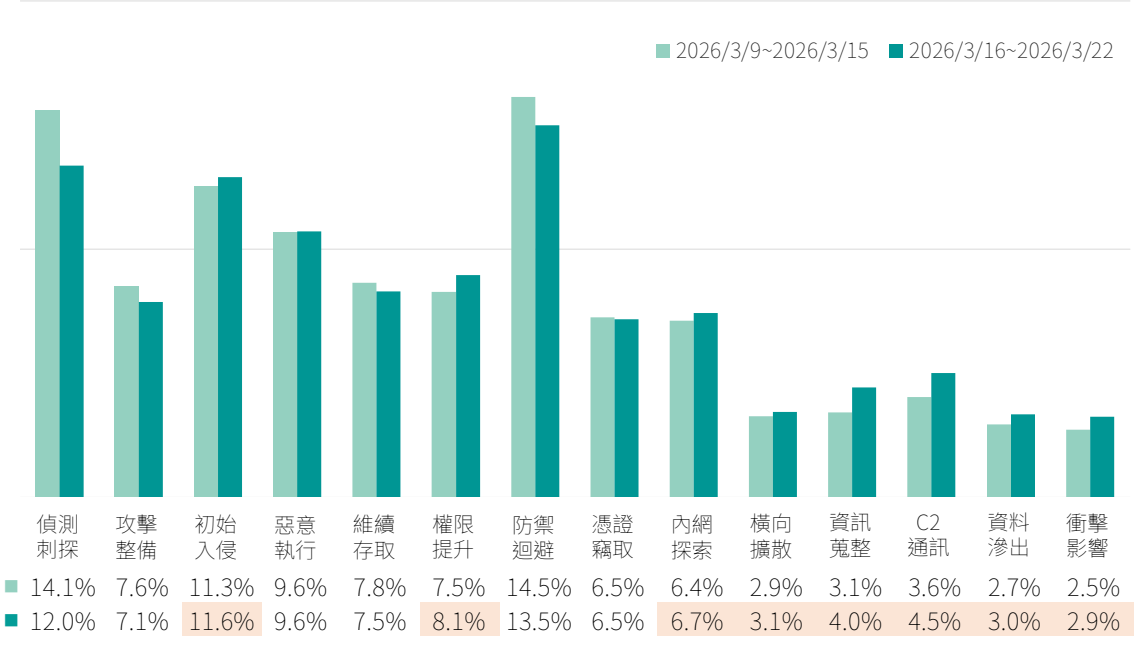

圖3 | 資安聯防監控攻擊階段統計

防護建議 建議機關採取下列防護措施：

- 強化防禦迴避防護
  - ✓ 導入端點防護（EDR / Endpoint Protection）
  - ✓ 加強指令紀錄與稽核能力
  - ✓ 限制高風險工具使用
  - ✓ 強化特權帳號管理
- 強化偵測刺探防護
  - ✓ 監控與阻擋異常掃描行為
  - ✓ 盤點與控管公開資產
  - ✓ 控管 DNS 資訊曝光情形
  - ✓ 結合威脅情資分析

■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

網通設備攻擊趨勢趨緩

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69.74%、「遠端控制」服務攻擊占比25.29%，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63.64%。「遠端控制」服務亦有32.14% 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。

而網通設備管理介面比例大幅下降，主因為CVE-2017-17215遠端程式碼執行漏洞相關攻擊次數明顯減少。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。

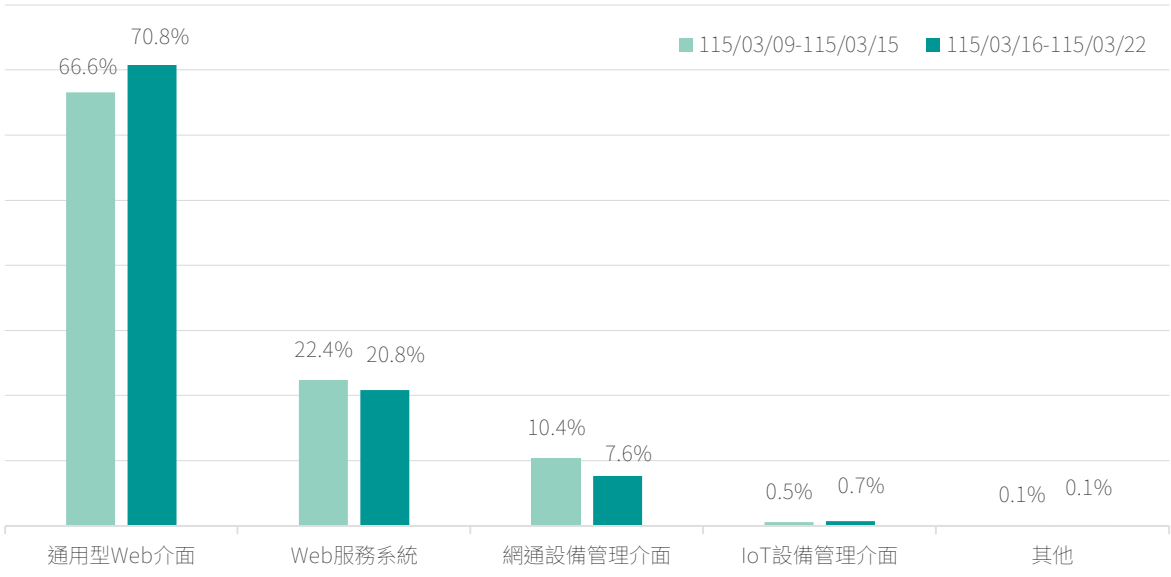

圖4 | 本週網頁應用服務之誘捕攻擊比例統計

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、特權提升、遠端程式碼執行及身分驗證繞過漏洞，攻擊目標涵蓋Citrix NetScaler ADC、Cisco IOS XE網通設備作業系統、PHP、ConnectWise ScreenConnect及 Ivanti EPMM。

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-2023-20198[2]	Cisco IOS XE網通設備作業系統	10
■	3	-	CVE-2024-4577[4]	PHP	9.8
■	4	↑ New	CVE-2024-1709[3]	ConnectWise ScreenConnect	10
■	5	↑ New	CVE-2023-35078[5]	Ivanti EPMM	10

類型 ■越界讀取漏洞 ■特權提升 ■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：

- Microsoft Office SharePoint存在高風險安全漏洞(CVE-2026-20963[6])，類型為反序列化不受信任資料(Deserialization of Untrusted Data)，未經身分鑑別之遠端攻擊者可利用此漏洞執行任意程式碼。
- Veeam Backup & Replication存在8個高風險安全漏洞(CVE-2026-21666至CVE-2026-21672[7-13]與CVE-2026-21708[14])，類型包含遠端執行任意程式碼(RCE)與本機提權(Local Privilege Escalation)等，影響最嚴重之漏洞，可使已通過身分鑑別之攻擊者對備份伺服器(Backup Server)遠端執行任意程式碼，或使具備Backup Viewer權限之攻擊者以postgres身分遠端執行任意程式碼。
- HPE Aruba Networking AOS-CX交換器存在高風險安全漏洞(CVE-2026-23813[15]與CVE-2026-23814[16])，類型分別為身分鑑別繞過(Authentication Bypass)與指令注入(Command Injection)，前者可使未經身分鑑別之遠端攻擊者重設管理者通行碼；後者可使通過身分鑑別之遠端攻擊者注入並執行惡意指令。

1. https://nvd.nist.gov/vuln/detail/CVE-2025-5777
2. https://nvd.nist.gov/vuln/detail/cve-2023-20198
3. https://nvd.nist.gov/vuln/detail/cve-2024-4577
4. https://nvd.nist.gov/vuln/detail/cve-2024-1709
5. https://nvd.nist.gov/vuln/detail/cve-2023-35078
6. https://nvd.nist.gov/vuln/detail/CVE-2026-20963
7. https://nvd.nist.gov/vuln/detail/CVE-2026-21666
8. https://nvd.nist.gov/vuln/detail/CVE-2026-21667
9. https://nvd.nist.gov/vuln/detail/CVE-2026-21668
10. https://nvd.nist.gov/vuln/detail/CVE-2026-21669
11. https://nvd.nist.gov/vuln/detail/CVE-2026-21670
12. https://nvd.nist.gov/vuln/detail/CVE-2026-21671
13. https://nvd.nist.gov/vuln/detail/CVE-2026-21672
14. https://nvd.nist.gov/vuln/detail/CVE-2026-21708
15. https://nvd.nist.gov/vuln/detail/CVE-2026-23813
16. https://nvd.nist.gov/vuln/detail/CVE-2026-23814

■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

TLS 與過時協定風險下降六成 惟元件高風險漏洞仍居高不下

本次針對曝險程度較高之 100 個 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 7,599 項，詳見圖5。其中，「元件高風險漏洞」以 3,943 項居首，「CSP 設定不當」988 項次之，「過時或弱加密協定」916 項位居第三，此三項合計占比約 76%，顯示漏洞修補與加密通訊管理仍為當前主要資安挑戰。相較於上期的 9,839 項，整體風險數量減少 2,240 項，降幅約 23%，反映外部曝險整體情勢有所改善。

進一步分析重大風險變化，「元件高風險漏洞」從 3,779 項微幅增加至 3,943 項，增幅約 4%；「TLS 憑證不受信任」從 1,853 項大幅減少至 625 項，降幅達 66%；「過時或弱加密協定」從 2,318 項大幅減少至 916 項，降幅達 60%，均呈現顯著之改善趨勢。此外，「CSP 設定不當」從 829 項增加至 988 項，增幅達 19%；「未部署 WAF」從 558 項微幅增加至 576 項，增幅約 3%，顯示網站安全防護措施仍有待加強。

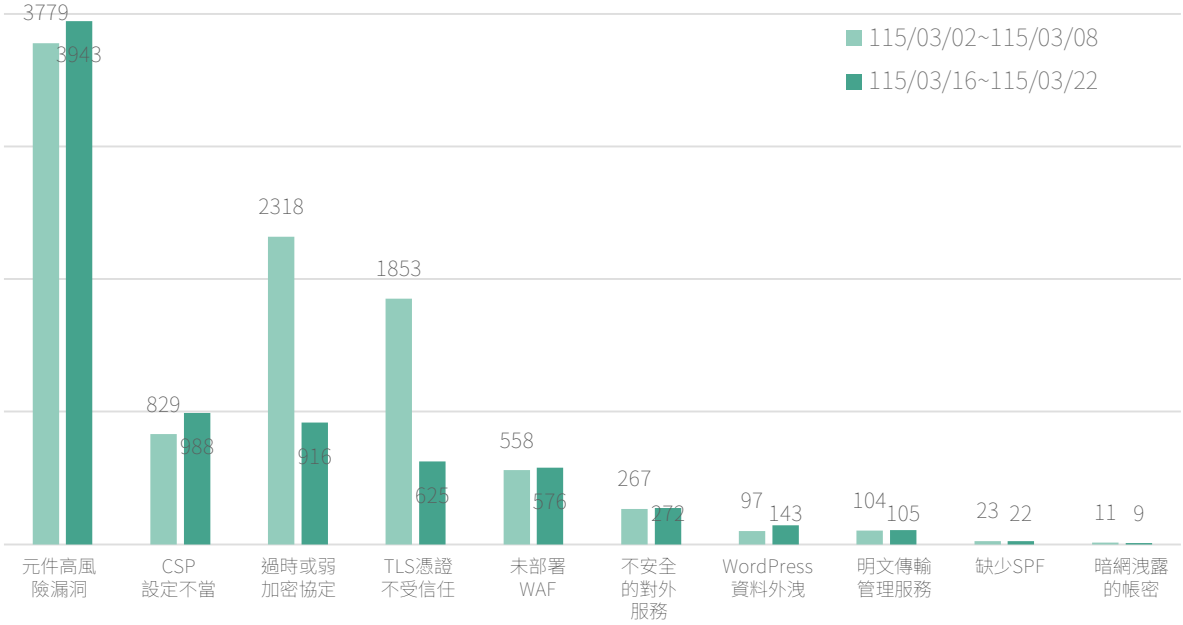

圖5| EASM檢測結果統計(前10大風險)

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
➢ 定期更新憑證，全面啟用 TLS 1.2 以上版本協定，停用未加密或舊版協定 ➢ 儘速修補已知漏洞，淘汰無維護之軟體版本 ➢ 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，若需遠端管理服務應嚴格限制來源 IP 並改採加密通道 (如 SSH)	➢ 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流程，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於憑證管理、加密配置及服務設定之安全意識

■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

生活消費型包裝仍是主軸 近期尤須留意保健護理、清潔用品與假客服延伸手法

綜觀本期高風險詐騙內容，整體樣態與前期大致相近，仍主要圍繞民眾日常最常接觸的購物、服務與互動場景展開，顯示詐騙訊息持續以生活化題材降低戒心，詳見圖6。這類內容常披著商品廣告、優惠資訊、健康管理或客服通知的外衣，看似只是一般商業宣傳，實際上卻可能在點擊、私訊與付款流程中暗藏風險。提醒民眾，面對各類網購訊息、促銷活動、客服通知或健康相關廣告時，仍應保有基本查證意識，避免在未確認資訊真偽前即進一步互動。

就風險類型而言，「產品服務」仍是本期最主要的高風險來源，且內容包裝持續朝向更貼近日常需求的方向發展。從本期常見素材觀察，相關訊息多聚焦於牙齒清潔、個人保養、關節與足部舒緩、衣物清潔、穿搭配件及健康調理等題材，並搭配「推薦」、「必備」、「優惠」、「安心」、「舒適」、「台灣」等語彙，營造商品實用、熱門且值得立即購買的印象。此類內容常進一步結合「限時活動」、「升級配方」、「快速有感」、「客服在線」、「售後服務」等話術，引導民眾點擊連結、私訊詢問，甚至轉往站外完成交易。由於其版型、語氣與一般電商廣告相近，民眾在瀏覽時往往不易第一時間察覺異常，須特別留意。

相較之下，「身分冒充」雖非本期最醒目的主軸，但仍持續存在於購物與服務流程之中，尤其容易以客服、賣家、售後窗口、物流通知或退款協助等名義與民眾接觸。此類訊息的風險不一定出現在第一時間，而常是在民眾已經點擊廣告、表達購買意願，或進入後續交易流程後，才透過假客服或假通知延伸詐騙操作。從內容樣態來看，常見說法包括協助確認訂單、處理補件、重新付款、售後追蹤或驗證身分等，目的多是進一步取得個人資料、驗證碼、帳戶資訊，或將民眾導向不明頁面操作。提醒民眾，若遇到主動聯繫要求重新確認資料、處理退款、解除設定或補件驗證等情形，應先中止互動，再改由官方網站、官方App 或正式客服管道重新查證。

至於「金融投資」雖仍不是本期風險焦點所在，但其高損失特性依然不可輕忽。此類詐騙通常以投資理財、快速獲利、專人帶單、名人推薦、社群邀請等方式吸引民眾，再透過看似專業的說明、對帳畫面、獲利展示或課程包裝，引導投入資金。雖然本期整體風險重心

仍以商品與生活消費題材為主，但這也意味著民眾更容易把注意力放在「看起來像購物廣告」的內容上，而忽略其他同樣具有高風險、高損失特性的詐騙樣態。對於任何標榜穩定收益、保證獲利或快速回本的資訊，仍應維持高度警覺。

整體而言，本期高風險詐騙內容延續前期結構，仍以「產品服務」為核心，並持續借用保健護理、穿搭用品、居家清潔與健康調理等生活化題材進行包裝；「身分冒充」則多與購物、退款、售後與物流通知等流程結合，藉由假客服或假窗口延伸詐騙操作；「金融投資」雖非本期主軸，仍屬高損失風險類型，須持續防範。本期特別值得注意之處，在於詐騙內容不再只訴求低價或搶購，而更常結合「改善生活品質」、「健康照護」、「方便實用」、「立即見效」等語感包裝，使其更接近一般商業行銷內容，迷惑性相對更高。

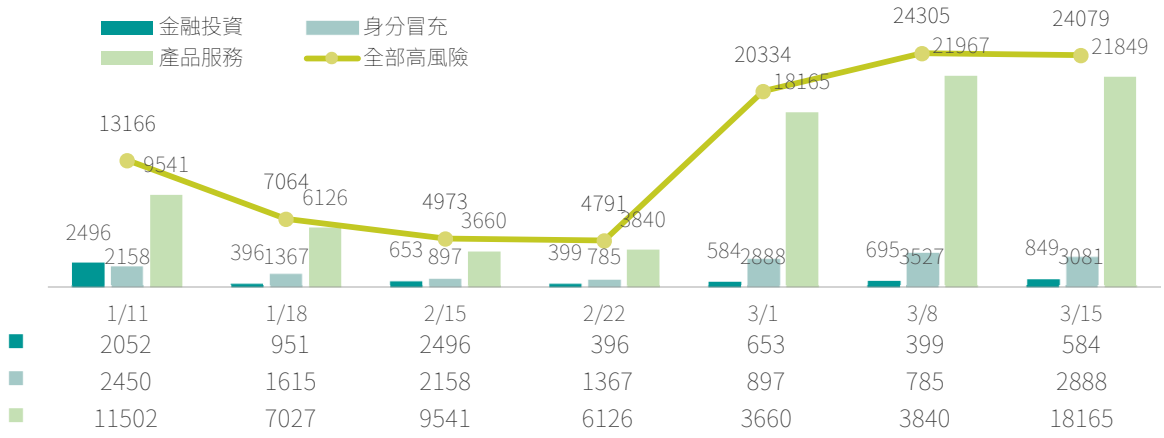

圖6 | 偵獲高風險金融投資、身分冒充、產品服務類詐騙週趨勢

高風險詐騙偵測趨勢分析與提醒

留意以健康、清潔與穿搭題材包裝的商品訊息

- ✓ 面對「產品服務」相關訊息，若內容強調「推薦使用、限時優惠、台灣出貨、升級配方、快速有感、安心使用」等字眼，應提高警覺，避免因文案完整、畫面精緻或見證豐富而直接下單。
- ✓ 對於主打保健護理、個人清潔、足部舒緩、衣物清潔、穿搭修飾或健康調理等商品內容，若同時要求私訊洽談、改由站外交易或點擊不明連結，應視為高風險警訊。
- ✓ 對宣稱效果明顯、保證改善、醫師推薦、天然配方、敏感肌適用或使用後立即見效的廣告，尤其應審慎辨識其真實性與付款安全。

強化購物流程中的客服與通知來源查證

- ✓ 如對方自稱客服、賣家、售後人員、物流或付款協助窗口，並要求重新付款、提供驗證碼、確認帳戶、點擊補件連結或配合操作，均應立即停止互動。
- ✓ 接獲與購物、出貨、退款、取消訂單或售後追蹤有關的通知時，不宜直接依訊息內容操作，應回到官方網站、官方 App 或公開客服資訊重新確認。
- ✓ 對「客服即時處理」「售後無憂」「私訊快速協助」「訂單異常需立即確認」等語句，應保持警覺，避免因其貼近真實服務流程而誤信對方身分。

持續防範高損失型金融投資風險

- ✓ 對任何投資社群、帶單邀請、保證獲利、穩賺不賠或快速回本等訊息，均應維持高度警覺，不可因表面包裝專業而輕信。
- ✓ 對於以貸款、補助、快速審核、免費諮詢或資產管理名義要求先提供個資、帳戶資料或先行匯款者，應多方查證，避免落入金融型詐騙。
- ✓ 凡涉及資金投入、帳戶驗證、投資操作或入金流程者，應先確認對方身分、平台合法性與資訊可追溯性，不宜僅憑對話截圖、社群貼文或片面說法即採取行動。

善用檢舉與官方通報資源

- ✓ 遇到疑似詐騙內容，請立即通報 165 反詐騙專線或平台客服，並保留廣告畫面、對話紀錄、連結、帳號與匯款資訊等相關證據。
- ✓ 建議持續留意政府、金融機構與平台公告的最新詐騙手法，特別是「假購物、假客服、假投資」彼此串接的複合型樣態。
- ✓ 建議平台與相關單位持續強化對「私訊下單、不明連結、假客服售後、誇大效果、健康訴求包裝」等高風險樣態的偵測與攔阻。

本週代表性詐騙關鍵字 Top 10 以「設計」、「必備」、「推薦」等字眼最常出現，另外也常搭配「優惠」、「台灣」、「配方」、「健康」、「安心」、「舒適」、「神器」等用語，詳見圖7。從這些高頻字眼可以看出，詐騙訊息仍常假裝成一般商品廣告、保健資訊或生活用品推薦，利用「設計貼心」、「很多人都在買」、「日常一定用得到」這類說法吸引民眾注意。常見情況像是強調商品好用、效果明顯、生活必備，或打出推薦款、熱銷款、限時優惠等字樣，讓人覺得划算又值得買，接著再把人引導到不明網站、假購物頁面，甚至要求填寫個資或直接付款。

本週也常看到以「設計」、「必備」、「神器」、「舒適」來包裝的商品宣傳，例如標榜「貼心設計」、「簡單好用」、「生活必備」、「清潔神器」、「穿著更舒適」等，讓民眾覺得商品實用又方便，買了就能立即改善日常生活。這類貼文常會再加上「一鍵操作」、「長輩小孩都能用」、「限量補貨」、「現在下單再送贈品」等話術，讓人一不小心就想趕快下單。提醒民眾，看到這種一直強調功能很好、使用方便、買到就賺到的廣告時，務必要先查清楚賣家和網站來源，不要只看圖片吸引人、文字寫得很專業，就直接點連結或下單。

另外，從「推薦」、「配方」、「健康」等關鍵字來看，本週也有不少詐騙內容是假借保健、調理或專業背書的名義來吸引民眾。這類訊息常會說商品是「專利配方」、「天然植萃」、「專家推薦」、「有助健康」、「深層修護」等，甚至搭配使用者見證、效果對比、熱銷數字或快速見效等描述，讓人誤以為商品真的有效。實際上，這類手法往往是利用民眾對健康、外觀、疼痛不適或清潔保養的需求，進一步誘導購買、留下聯絡資料，或導向來路不明的網站與客服。提醒民眾，凡是宣稱效果太神、見效太快，或說什麼問題都能一次改善的商品，都要特別提高警覺，不要因為幾句廣告話術就輕易相信。

此外，本週常見的詐騙宣傳也會使用「台灣」、「安心」、「優惠」等字眼，刻意營造可信、安全又划算的感覺。例如標榜「台灣設計」、「台灣熱銷」、「敏感肌安心使用」、「限時優惠」、「買一送一」、「前50名下單即贈好禮」等，讓民眾以為商品來源可靠、品質有保障、現在買最划算。不過，這些字眼也可能只是詐騙集團用來包裝假賣場、假客服或假付款流程的手法，後續可能造成個資外洩、信用卡資料被盜用、重複扣款，甚至付款後根本收不到商品。提醒民眾，不要因為看到「台灣出貨」、「安心使用」或「限時優惠」就放下戒心，仍應先確認網站是否可信、商家資訊是否清楚、付款方式是否安全。

另從整體話術來看，詐騙訊息也很常用「必備」、「推薦」、「舒適」、「神器」這些字眼，讓商品看起來不只是便宜，而是「很多人都在用」、「現在就該買」、「買了生活會更方便」。再搭配「全台熱銷」、「每幾秒賣出一罐」、「限量補貨」、「手慢就沒了」等說法，很容易讓民眾在還沒查證清楚前，就急著做決定。提醒民眾，只要看到廣告一直強調效果很好、數量不多、優惠快截止，或催促趕快填資料、點外部連結、完成付款時，都應先停一下、多查一下，不要急著操作。

綜合本週觀察，常見詐騙手法多半是先用「設計」、「必備」、「推薦」等吸睛字眼吸引注意，再用「配方」、「健康」、「舒適」這類說法增加可信度，接著以「台灣」、「安心」、「優惠」降低民眾戒心，最後再透過「神器」、「熱銷」、「限量」等話術催促下單，把人引導到站外頁面、假賣場或不明付款流程。提醒民眾，只要遇到要求點擊不明連結、填寫個人資料、提供信用卡資訊，或先付款才能取得商品、優惠或服務的情況，都要提高警覺、先查證再操作。建議優先透過官方網站、公開客服或可信賴平台確認真偽，避免落入詐騙陷阱。

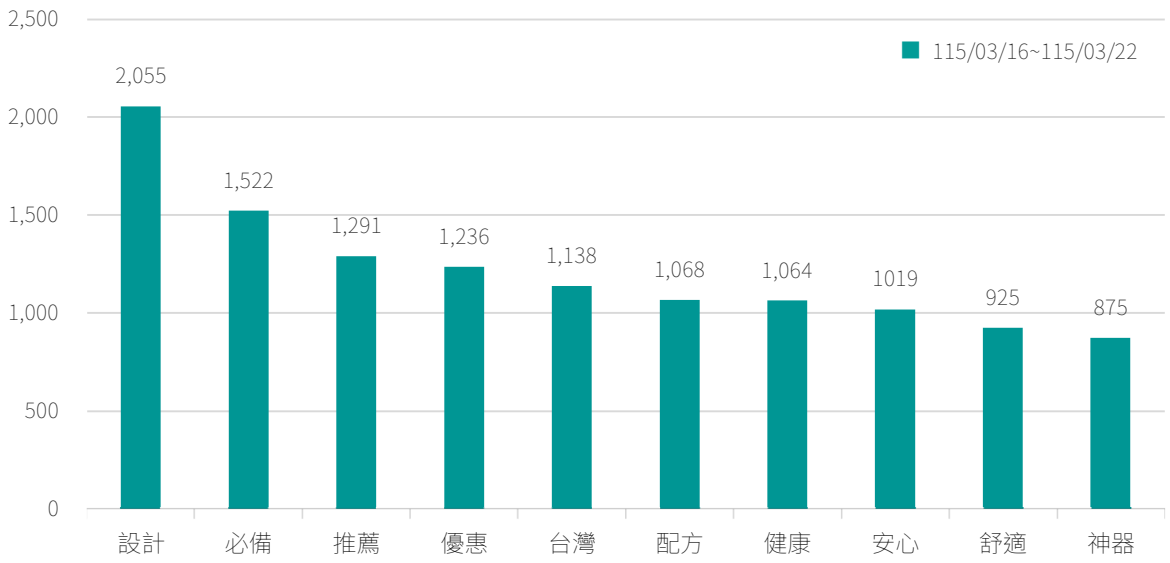

圖7 | 本週代表性詐騙關鍵字 Top 10

焦點文章

模擬APT攻擊鏈：防禦演練平台強化資安應變能力

本文簡介透過擬真情境進行模擬演練，有助提升組織的資安監控與事件應變能力，強化政府與企業的威脅偵測能力與整體資安防護韌性。

一 面對進階持續性威脅(APT)的防護挑戰

隨著資訊化發展與網路威脅興起，許多企業和政府機構已深刻意識到網路攻擊帶來的嚴重風險。面對日益嚴峻的網路安全環境，傳統的被動防禦已難以應對手法細膩且具備長期潛伏特性的進階持續性威脅(Advanced Persistent Threat, APT)，尤其是政府機關、民間企業或關鍵基礎設施(Critical Infrastructure, CI)。一旦核心系統遭受勒索軟體、內部威脅或供應鏈攻擊，將面臨營運停擺、社會信任崩解及國家安全受損等連鎖反應。

二 防禦演練平台的核心概念與關鍵機制

防禦演練平台可以以數位靶場(Cyber Range)為基礎架構，模擬企業網路與APT攻擊場景，在安全且貼近現實的空間內，提供人員進行實戰演練與技術測試，確保在演練過程中，不會對既有營運環境造成任何危害。

為有效模擬APT攻擊的隱蔽性與多階段特性，防禦演練平台通常具備下列關鍵機制：

- 擬真情境設計與管理：情境設計是平台的核心機制，負責規劃與建構多階段的攻擊模擬情境。平台通常會建置一系列實戰型的技術演練架構與腳本，模擬APT攻擊組織在各資安事件中可能採用的攻擊手法(如密碼暴力破解、SQL注入攻擊、Webshell上傳、內網橫向移動等)，參與者必須在平台中調查各個事件的封包與日誌紀錄，找出關鍵入侵指標(Indicators of Compromise, IOC)。
- 成效評估與量化報告：演練結束後會對演練結果進行評估，以了解參與者在演練過程中攻擊的偵查能力、事件發生的應變能力及防禦策略的有效性。透過尋找關鍵入侵指標(IOC)與填答事件單(Ticket)欄位，以量化方式評估參與者，對於網路流量與系統日誌分析的防禦能力。

焦點文章

三 APT防禦演練平台的演練運作

目前國家資通安全研究院已發展一套「APT防禦演練平台」，演練遭遇APT攻擊時的入侵指標偵查。在APT防禦演練平台演練過程中，參與者將扮演資安監控中心(Security Operations Center, SOC)成員，在擬真的SOC Room環境中進行以下任務：

1. 調查與分析： 追蹤可疑事件並識別關鍵威脅指標(IOCs)。
2. 驗證發現：進行技術分析後，仿照SOC運作流程，在一定時間內處理與判斷分析結果，並確認所調查威脅指標之正確與否。
3. 決策遞交： 遞交調查結果後，系統將依據正確性回饋「Resolved(已解決)」或「Rejected(已退回)」，訓練參與者的判斷力。

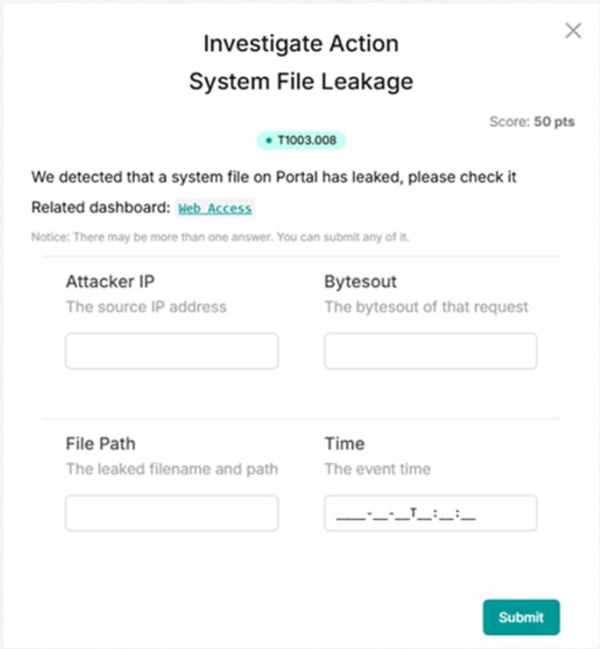

圖8 | APT防禦演練平台各事件之關鍵入侵指標偵查

i	_time	src_ip	http_user_agent	status	response_time	http_method	uri	bytes_out	uri_query	post_data
›	2026-02-25T10:06:56.000+08:00	10.101.0.60	User-Agent: Mozilla/5.0 (Linux...	200	0.020	GET	/	15923	p=11	-
›	2026-02-25T10:06:43.000+08:00	10.101.0.103	User-Agent: Mozilla/5.0 (iPhon...	200	0.016	GET	/	14983	cat=2	-
›	2026-02-25T10:06:43.000+08:00	10.88.0.1	Mozilla/5.0 (Windows NT 6.1) A...	200	0.020	GET	/favicon.ico/	4906		-
›	2026-02-25T10:06:43.000+08:00	10.88.0.1	Mozilla/5.0 (Windows NT 6.1) A...	301	0.012	GET	/favicon.ico	279		-
›	2026-02-25T10:06:43.000+08:00	10.88.0.1	Mozilla/5.0 (Windows NT 6.1) A...	200	-	GET	/wp-content/themes/twentytwentyone/assets/css/print.css	3144	ver=1.4	-

圖9 | APT防禦演練平台SIEM分析(以Web Logs示意)

圖8與圖9顯示APT防禦演練平台的資安監控中心(SOC)，平台依時序逐步演練APT駭客組織發動各項攻擊步驟，參與者(即SOC成員)則需透過安全資訊與事件管理(Security Information and Event Management, SIEM)之工具(如Splunk)中各個流量與日誌分析，仿照真實監控人員填寫事件單中的欄位。

焦點文章

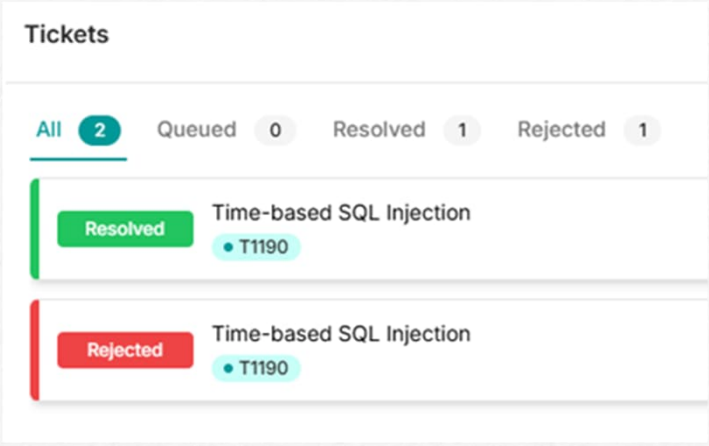

圖10 | APT防禦演練平台事件單「Resolved」或「Rejected」狀態

一旦正確答出關鍵入侵指標，則該事件單會顯示Resolved（已解決)(綠色)；若關鍵指標內容錯誤，該事件單則會被退回(Rejected)(紅色)，則演練人員便須繼續找出正確的入侵指標，以確認演練人員對於該事件的了解程度，詳見圖10。

此外，系統後台也可以針對各個團隊成員解題狀況，了解其在每個事件所需要強化的能力，詳見圖11。

圖11 | APT防禦演練平台各個團隊成員解題狀況

四 提升應變能力與防禦韌性

透過APT防禦演練平台的系統化情境模擬與實戰演練，可協助企業與組織強化威脅偵測與分析能力，在面對潛在資安事件時提升應變決策效率。持續推動此類實戰演練，也有助於政府機關與關鍵基礎設施單位提升資安監控與事件應變能力，進一步強化整體資安防護韌性。

關鍵字：APT攻擊、資安演練平台、資安防護韌性

刊　　名　資安週報第 37 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