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

建立完善帳號控管與監測 提升整體資安防護能力

聯防監控

防禦迴避高居首位 初始入侵仍具威脅

蜜罐誘捕

本週整體趨勢維持穩定 與前期相比未有顯著變化

外部曝險分析

元件高風險漏洞、過時或弱加密協定及TLS憑證不受信任三大風險顯著改善 整體外部曝險總數下降19.2%

網路巡查高風險詐騙

高風險內容持續混入日常購物與服務資訊 近期應留意換季商品、保健護理與假客服串接手法

焦點文章

漏洞通報統計與趨勢

2026.04.02
038

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

建立完善帳號控管與監測 提升整體資安防護能力

本週總計接獲14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。本週有機關SOC偵測發現主機存在異常行為程式，經查係維護廠商於維運作業中使用之 Python 程式，使單一帳號可同時遠端存取多個系統，後續已依機關政策調整。

單一帳號具備多重操作權限(如多重連線、主機操作及遠端控制)，將大幅放大帳號遭濫用時之影響範圍，且相關行為不易與正常維運區隔，提高異常行為偵測困難。建議機關依防護基準落實最小權限原則，僅授予執行業務所需之必要權限，避免權限過度集中；並強化遠端存取管理機制，落實事前授權、使用限制及來源控管，以降低帳號遭濫用及系統被橫向擴散利用之風險。

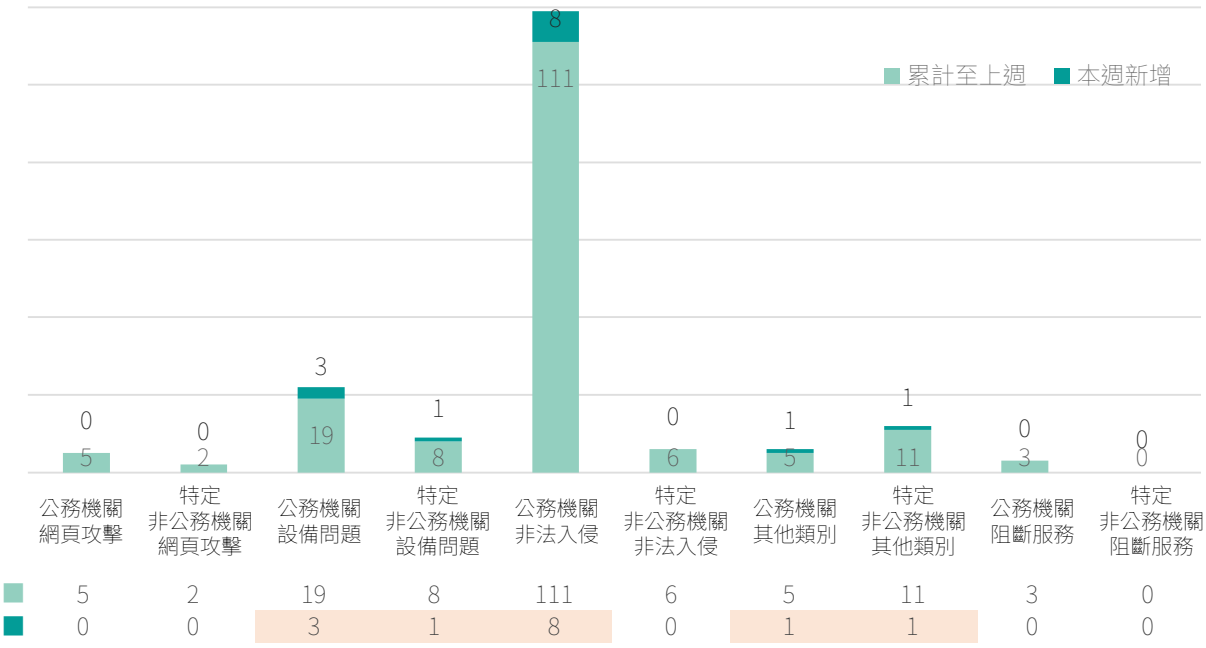

圖1 | 本週公務機關暨特定非公務機關資安事件通報概況

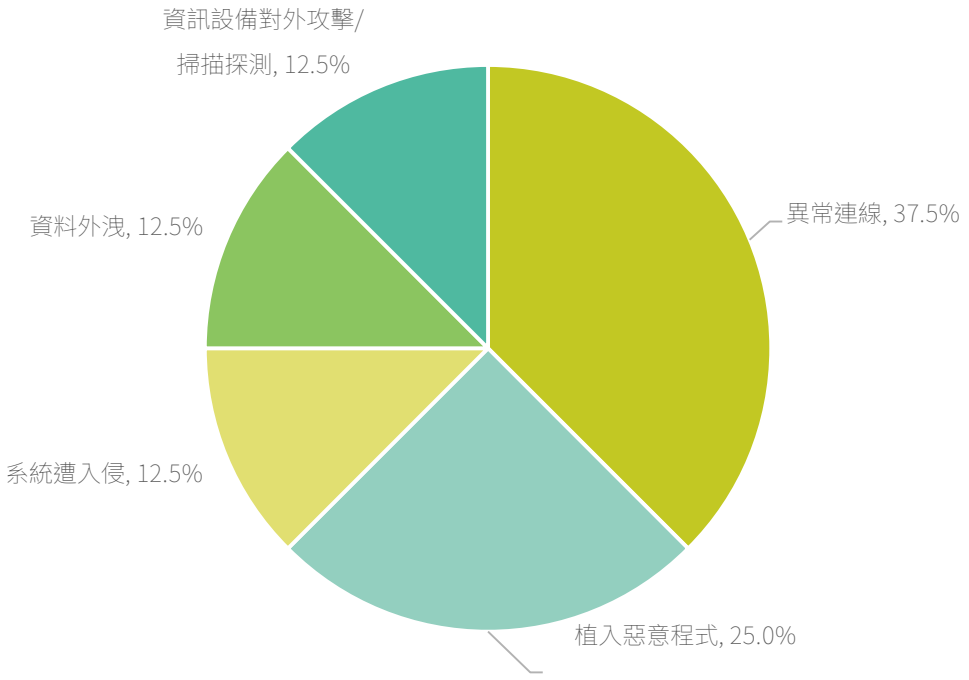

圖2 | 本週公務機關非法入侵事件類型占比

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
➢ 攻擊者濫用高權限帳號橫向移動控制多系統 ➢ 利用維運工具隱匿惡意行為規避監控機制	➢ 落實最小權限原則，限制帳號僅具備執行業務所需最低權限範圍 ➢ 建立遠端存取控管機制，強化來源限制與連線行為審核機制 ➢ 導入特權帳號管理制度，強化操作紀錄留存與即時監控機制 ➢ 強化端點與主機行為監控機制，即時偵測異常程式執行行為

3間民間企業揭露重大資安訊息

本週3家民間企業發布重大訊息，產業類別分為貿易百貨、電腦及週邊設備業和其他。

- **公司名稱：** 特力股份有限公司
- **發布時間：** 115 年 3 月 23 日
- **事件說明：** 特力公司之海外子公司通報其資訊設備遭受外部網路攻擊，第一時間為防止擴大影響範圍，已執行系統隔離作業且同步啟動防禦措施，已委請外部資安專家協助調查與排除，並加強內部資安偵測與防護機制。目前評估該事件對公司財務業務無重大影響，後續將持續強化網路安全架構及控管流程，以維護整體資訊安全。

- **公司名稱：** 融程電訊股份有限公司
- **發布時間：** 115 年 3 月 25 日
- **事件說明：** 融程電公司之資安單位偵測到駭客組織透過非法手段存取第三方雲端平台之部分資料，並收到相關威脅訊息。獲悉後立即啟動資安應變機制，封鎖異常存取來源，並加強帳戶之機密身分驗證與權限稽核。經檢視有資料外流，但未有核心資通系統資料，對公司產產品及客戶隱私無影響，後續將強化雲端之存取控管策略、定期執行帳號清理，並持續提升員工資安意識培訓。

- **公司名稱：** 南六企業股份有限公司
- **發布時間：** 115 年 3 月 29 日
- **事件說明：** 南六公司之資訊系統遭受勒索病毒攻擊，已立即啟動資安應變機制，目前相關資訊系統以陸續恢復正常運作。經初步評估，本事件對公司營運尚無重大影響，後續將持續加強資訊安全監控與防護機制，提升網路與資訊基礎架構之安全管理，並導入更完善之資安控管措施，以降低未來風險。

■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

防禦迴避高居首位 初始入侵仍具威脅

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13.7%，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。

「初始入侵」事件本週占比為13.4%，為本週占比次高的攻擊階段，顯示攻擊者持續強化對目標環境的入侵行動。此階段代表攻擊者首次取得系統或網路的存取權限，為後續攻擊活動的起點。本週主要觀察到的手法包括利用對外應用程式漏洞、預設帳號濫用、以及本機帳號存取。攻擊者多半透過未修補的公開服務漏洞直接入侵系統，或利用預設帳號與弱密碼組合存取管理不當的服務；另有部分行為顯示攻擊者利用既有本機帳號進行登入，以繞過邊界防護機制。此類手法不依賴使用者互動，主要聚焦於系統弱點與帳號管理缺失，具高度成功率與隱蔽性。建議定期執行外部資產弱點掃描與修補、強化帳號管理與驗證機制，並導入異常登入行為監控，以降低攻擊者透過既有存取管道入侵的風險。

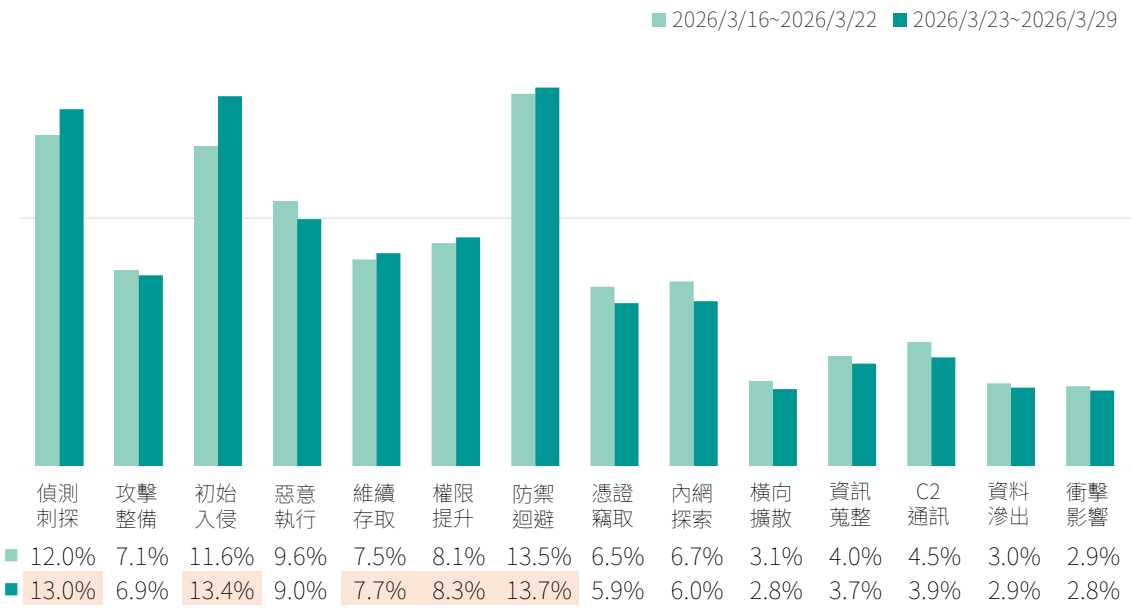

圖3 | 資安聯防監控攻擊階段統計

防護建議 建議機關採取下列防護措施：

防禦迴避防護建議

- 強化指令與日誌稽核
- 限制系統工具濫用
- 導入端點防護（EDR/XDR）
- 加強特權帳號管理
- 防止日誌刪除與關閉

初始入侵防護建議

- 定期弱點掃描與修補
- 強化帳號與驗證機制
- 管控本機帳號使用
- 建立異常登入監控
- 降低對外攻擊面

整體強化

- 導入零信任架構
- 建立MITRE對應與監控
- 強化持續監控與應變能力

■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

本週整體趨勢維持穩定 與前期相比未有顯著變化

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63.64%、「遠端控制」服務攻擊占比32.14%，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68.77%。「遠端控制」服務亦有27.42% 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。

而本週受影響產品類型排行僅有些微變化，網通設備Citrix ADC and Citrix Gateway之CVE-2023-24488與NetScaler ADC and NetScaler Gateway之CVE-2023-4966攻擊使用排行提升至第4~5名。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。

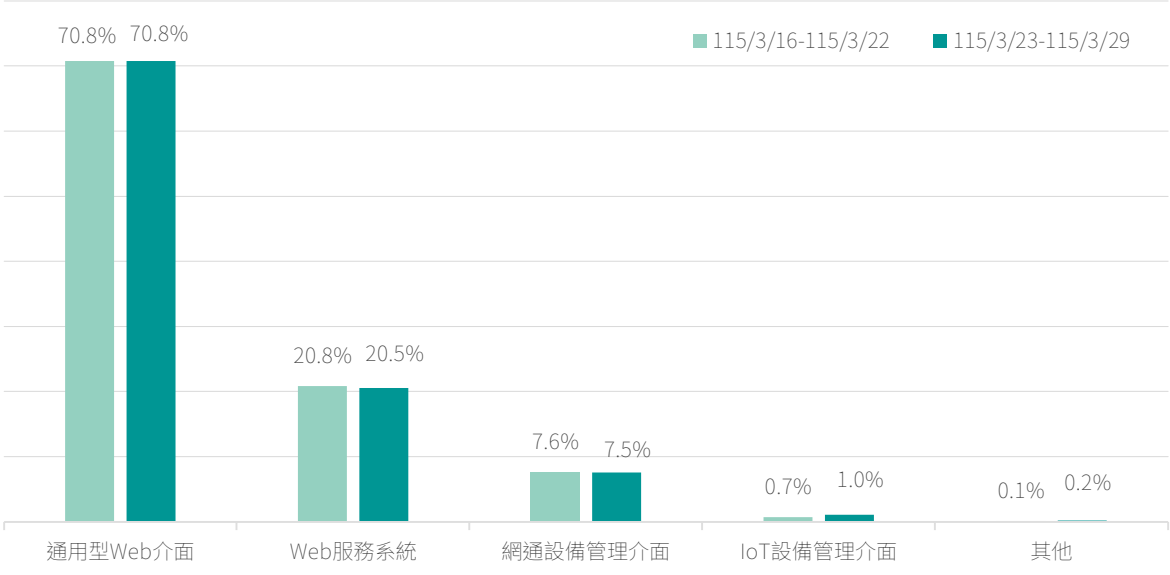

圖4 |本週網頁應用介面之誘捕攻擊比例統計

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、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、Citrix ADC and Citrix Gateway及 NetScaler ADC and NetScaler Gateway。

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[3]	PHP	9.8
■	4	↑ New	CVE-2023-24488[4]	Citrix ADC and Citrix Gateway	6.1
■	5	↑ New	CVE-2023-4966[5]	NetScaler ADC and NetScaler Gateway	9.4

類型 ■越界讀取漏洞 ■特權提升 ■遠端程式碼執行漏洞 ■輸入驗證不當漏洞 ■緩衝區溢位漏洞

▶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：

- QNAP作業系統存在高風險安全漏洞(CVE-2025-66277[6])，類型為連結追蹤(Link Following)，未經身分鑑別之遠端攻擊者可利用此漏洞存取未授權之檔案系統路徑。
- NetScaler ADC與NetScaler Gateway存在高風險安全漏洞(CVE-2026-3055[7])，類型為越界讀取(Out of Bounds Read)，當NetScaler ADC與NetScaler Gateway被設定為SAML IDP，未經身分鑑別之遠端攻擊者可利用此漏洞讀取記憶體資訊。
- Oracle Identity Manager與Oracle Web Services Manager存在高風險安全漏洞(CVE-2026-21992[8])，類型為缺乏身分鑑別(Missing Authentication)，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。

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-2023-24488
5. https://nvd.nist.gov/vuln/detail/cve-2023-4966
6. https://nvd.nist.gov/vuln/detail/CVE-2025-66277
7. https://nvd.nist.gov/vuln/detail/CVE-2026-3055
8. https://nvd.nist.gov/vuln/detail/CVE-2026-21992

■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

元件高風險漏洞、過時或弱加密協定及TLS憑證不受信任三大風險顯著改善 整體外部曝險總數下降19.2%

本次針對曝險程度較高之93個A、B級關鍵基礎設施(CI)進行EASM資安曝險檢測。結果顯示，前10大風險項目共計2,049項，其中以「元件高風險漏洞」630項最多，「過時或弱加密協定」532項次之，「TLS憑證不受信任」376項位居第三，詳見圖5。前三項合計1,538項，占前10大風險項目總數之75.1%，顯示目前外部曝險風險仍高度集中於元件漏洞、加密通訊及憑證管理等議題。

自三月起，本院擴大EASM檢測範圍，並依檢測結果啟動警訊發布機制，針對存在元件重大風險或評估未達標準之機關單位發送通知，告知其曝險情形。透過「持續監控與重點通知」之作業模式，協助各機關單位掌握風險並加速弱點修補，已展現具體減量成效。相較上期之2,535項，整體風險數量減少486項，減幅約19.2%，顯示整體外部曝險風險已有明顯下降。進一步分析重大風險變化，「軟體元件高風險漏洞」由749項降至630項，減少119項，減幅15.9%；「過時或弱加密協定」由714項降至532項，減少182項，減幅25.5%；「TLS憑證不受信任」由575項降至376項，減少199項，減幅34.6%，均呈現顯著改善。另一方面，「CSP設定不當」由235項增至240項，增加5項，增幅約2.1%；「未部署WAF」由127項增至136項，增加9項，增幅約7.1%，顯示網站安全防護措施仍有持續強化之必要。

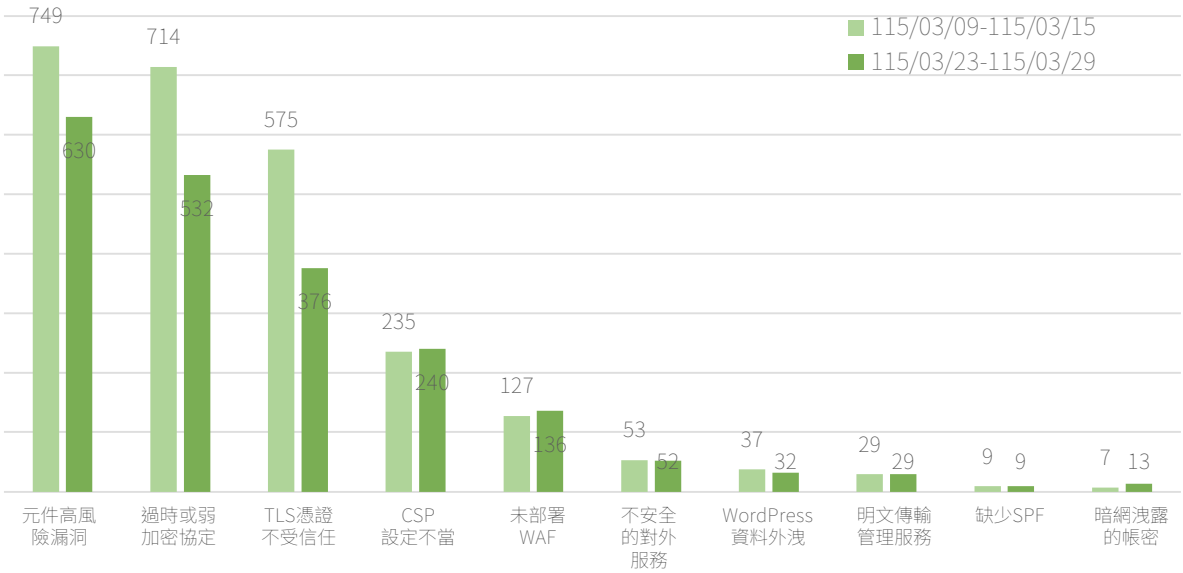

圖5 | EASM檢測結果統計(前10大風險)

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TLS1.2以上版本協定，停用未加密或舊版加密協定 ➢ 儘速完成已知漏洞修補，並汰換已停止維護或不再支援之軟體版本 ➢ 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 ➢ 關閉非必要對外服務；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)進行管理	➢ 定期盤點並更換外洩帳號憑證，並搭配多因素驗證(MFA)以強化存取安全 ➢ 建立弱點修補、驗證及追蹤機制，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、加密設定及服務配置之安全意識

■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

高風險內容持續混入日常購物與服務資訊 近期應留意換季商品、保健護理與假客服串接手法

本期高風險詐騙內容顯示，詐騙樣態仍未脫離民眾最熟悉的生活場景，而是持續包裹在購物、服務、保養與日常消費資訊之中，詳見圖6。相較於過去較易辨識的誇張話術，近期內容更傾向以「看起來像正常廣告、正常通知、正常推薦」的方式出現，使民眾在瀏覽時不易立即察覺異常。也就是說，風險不一定來自陌生感，反而往往藏在過於熟悉、過於自然的訊息外觀裡。面對這類內容，仍應維持基本的查證意識，不宜因訊息貼近日常需求，就在未確認真偽前直接點擊、私訊或付款。

若從風險類型切入觀察，「產品服務」仍是本期最主要的高風險來源，而且相關內容持續往生活化、功能化與情境化方向延伸。常見題材包括口腔清潔、穿搭修飾、草本護理、泌尿調理、家用清潔與健康保養等，整體呈現方式與一般商品行銷內容極為接近。這類訊息經常透過「必備」、「推薦」、「台灣設計」、「安心配方」、「快速有感」、「限時優惠」等字句，塑造商品值得立即購入的印象，再搭配見證式敘述、功效強調、限量補貨、加贈活動或客服協助等元素，逐步將民眾引導至連結點擊、私訊洽談或站外交易。由於其版型、用語與一般電商廣告相似，尤其在換季商品、保健護理與居家清潔等主題上，更容易降低民眾警覺。

另一方面，「身分冒充」仍持續出現在購物與服務流程周邊，並與商品型內容形成前後串接。這類手法往往不是一開始就直接暴露詐騙意圖，而是先讓民眾誤以為自己只是與客服、賣家、物流或售後窗口進行正常互動，之後再逐步導向訂單異常、退款處理、補件通知、重新付款或帳戶驗證等操作。換言之，真正的風險常不在第一則訊息，而是在後續接續而來的「處理流程」中發生。從本期樣態來看，假客服、假通知與假售後等名義仍是此類風險的重要包裝方式，目的多在於取得個人資料、驗證碼、帳戶資訊，或引導民眾進入不明頁面完成特定操作。遇到這類主動聯繫時，仍應以中止互動、另循官方管道重新確認為原則。

至於「金融投資」雖然不是本期最突出的風險焦點，但並不代表相關風險已經減弱。這類詐騙通常不以大量生活化曝光取勝，而是以較高損失、較深介入的方式造成影響。常見包裝包括投資機會、專人帶單、社群邀請、名人推薦、資產配置或短期獲利等，再透過績效展示、操作畫面、群組對話或課程內容逐步建立信任，最後引導民眾投入資金。也因此，

即使本期整體高風險內容仍偏向生活消費與商品場景，對於任何宣稱穩定收益、保證獲利、低風險高報酬或快速回本的資訊，仍不能掉以輕心。此類內容雖不一定最常出現，卻往往伴隨更高損失風險，仍須持續保持警覺。

圖6顯示近期數據看似明顯上升，主要因為資料擷取技術改進，且新增網路巡檢關鍵字，致使資料擷取量提升，近期數據因而呈現明顯上升。惟依類型比例分析，各類型案件分布尚屬穩定，案件趨勢比例與過往情形大致相符。

整體來看，本期高風險詐騙內容仍由「產品服務」主導，並持續向日常消費、保健護理、功能型用品與換季需求等場景擴散；「身分冒充」則多半嵌入購物、退款、物流與售後流程之中，透過假客服或假通知延伸後續操作；「金融投資」雖非本期主軸，仍屬不可忽視的高損失風險類型。若就本期較值得留意的特徵加以歸納，可發現詐騙內容不再只是單純訴求便宜、限量或搶購，而更常借用「生活改善」、「健康照護」、「方便實用」、「立即有感」等敘事方式，使其更貼近一般商業行銷與日常服務訊息，因而具有更高迷惑性。

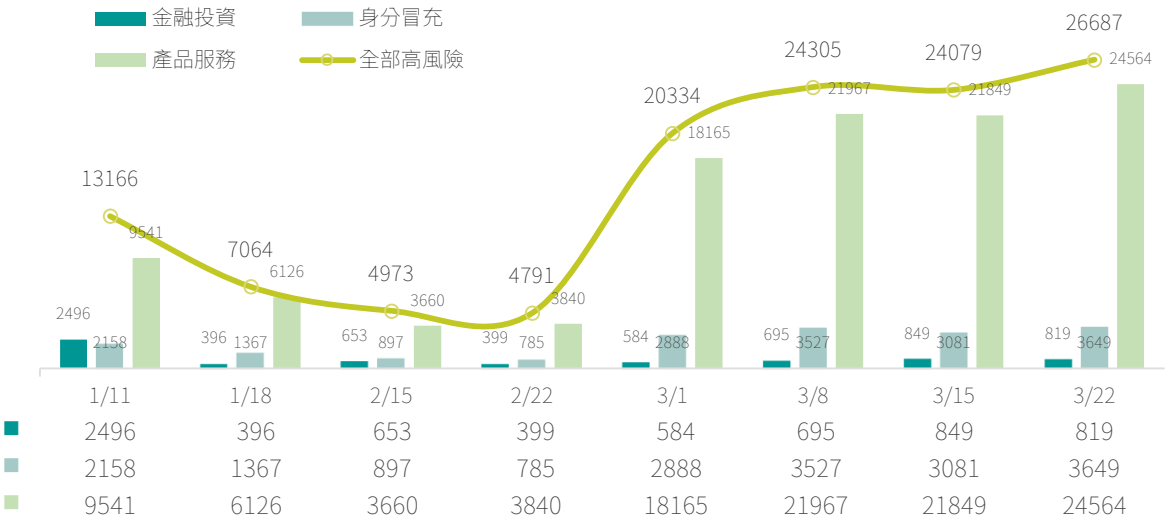

圖6 | 偵獲高風險金融投資、身分冒充、產品服務類詐騙週趨勢

近期高風險手法辨識重點

民眾接觸資訊時可優先留意的幾類情境

商品廣告越像日常分享，越要提高警覺

近期高風險內容常披著日用品、保健護理、清潔用品、穿搭配件或功能型商品的外衣出

現，表面上像是一般推薦文、促銷資訊或使用心得，實際上卻可能一步步將人引導至不安全的交易流程。這類訊息若反覆強調「現在下單最划算」「台灣設計」「很多人在買」「效果很快就看得到」「客服可即時協助」等說法，往往是在利用熟悉感與急迫感壓低判斷門檻。面對這類內容，民眾不宜只因畫面完整、文案自然或看起來像一般商家宣傳就放下戒心，而應先確認來源、販售管道與付款方式是否正常。

尤其是口腔清潔、身體調理、草本護理、家用清潔、衣著修飾與保健養生等題材，近來特別容易被包裝成高風險內容。若商品頁面或貼文進一步要求改用私訊洽談、跳轉其他通訊軟體、另開連結下單，或刻意避開正式平台交易機制，便應視為明顯警訊。凡是強調立即見效、快速改善、專家推薦、天然無負擔，甚至暗示長期困擾可快速解決者，都應審慎辨識，不宜在情緒被帶動時就直接完成交易。

真正危險的，往往不是廣告本身，而是後續被接上的「客服流程」

不少詐騙手法並不急著在第一時間暴露目的，而是先讓民眾相信自己只是進入了一般購物或售後流程，接著再藉由假客服、假賣家、假物流或假通知窗口進一步延伸操作。這類內容經常出現在訂單確認、出貨追蹤、退款處理、補件通知、付款失敗或帳戶異常等情境中，看似只是協助解決問題，實際上卻是在引導民眾交出更多資訊，甚至進行不必要的金融操作。

因此，只要對方主動要求重新付款、補登資料、提供驗證碼、確認帳戶、點擊補件連結，或配合某些「快速處理」步驟，都應先停止互動。正確做法不是繼續在原訊息中回覆，而是直接離開對話，改由官方網站、官方 App 或正式公開客服資訊重新確認。詐騙者最常利用的，就是民眾以為自己只是在處理一件普通的小問題；也因此，越像正常流程的訊息，越需要重新核對來源。

即使本期焦點偏向生活消費，也不能忽略投資型高損失風險

與商品型詐騙相比，投資型詐騙不一定在接觸頻率上最顯眼，但一旦受害，損失往往更高。這類內容多半以投資機會、專人帶單、社群邀請、資產配置、名人推薦或短期獲利作為切入點，再透過績效截圖、操作畫面、投資群組、課程諮詢或所謂成功案例逐步建立信任。當民眾被說服後，下一步往往就是入金、驗證、下載工具或轉入特定平台。

因此，只要訊息涉及穩定收益、保證獲利、低風險高報酬、短時間快速回本等說法，就應

直接提高警覺。面對貸款、補助、資產管理、快速審核或免費諮詢等名義要求先提供個資、帳戶資料或匯款者，也不宜因包裝看似專業就放鬆戒心。凡牽涉資金投入、帳戶綁定、身分驗證或平台操作時，都應先確認對方是否可被查證、平台是否合法、資訊是否具可追溯性，而非僅憑片面說法或截圖就採取行動。

面對疑似詐騙內容，保留證據與即時通報同樣重要

遇到可疑訊息時，除了不中斷查證意識，也應同步保留相關畫面與互動紀錄。包括廣告頁面、對話內容、連結、帳號名稱、付款資訊與匯款紀錄等，都是後續判斷與處理的重要依據。若已察覺異常，應儘速通報 165 反詐騙專線或平台客服，避免風險持續擴散，也有助於後續釐清手法與來源。

同時，建議持續留意政府、金融機構與平台公告的最新風險樣態，特別是那些會把「假購物、假客服、假投資」串成同一條詐騙流程的複合型手法。對平台與相關單位而言，也宜持續強化對私訊導購、不明連結、假售後通知、誇大效果與健康訴求包裝等內容的偵測與攔阻，降低高風險訊息在日常資訊流中的滲透程度。

本週高風險詐騙關鍵字分析

本週代表性詐騙關鍵字 Top 10 以「設計」、「必備」、「推薦」最常出現，另外也常搭配「台灣」、「神器」、「優惠」、「安心」、「配方」、「問題」、「健康」等字眼，詳見圖7。從這些高頻關鍵字可以看出，詐騙訊息仍常假冒一般商品廣告、保健宣傳或生活用品推薦，先用「設計貼心」、「生活必備」、「多人推薦」等說法吸引民眾注意，再以「台灣出貨」、「安心使用」、「限時優惠」等字眼降低戒心，讓人誤以為只是普通的購物資訊或日常保健分享，進而點擊連結、填寫資料，甚至進入付款流程。

本週也常見以「設計」、「必備」、「神器」包裝的商品宣傳，例如強調商品「簡單好用」、「居家必備」、「一用就有感」、「生活更方便」等，讓民眾覺得商品實用、買了就能立刻改善日常需求。這類內容常搭配「全台熱銷」、「限量補貨」、「買一送一」、「現在下單再送贈品」等話術，營造商品熱門且值得立即購買的氛圍，容易讓人在尚未查證前就直接下單。提醒民眾，凡遇到過度強調商品功能、使用便利性或熱銷程度的廣告內容，都應先確認賣家資訊、交易平台及付款方式是否可信，不要只因圖片吸引人、文案看起來專業，就直接進行操作。

另外，從「推薦」、「配方」、「問題」、「健康」等關鍵字來看，本週也有不少訊息是假借專業形象、健康訴求或身體調理名義來吸引民眾。這類內容常以「醫師推薦」、「草本配方」、「改善問題」、「有助健康」等說法包裝商品，並搭配見證分享、快速見效、一次改善等描述，讓人誤以為產品具備明顯功效。實際上，這類手法常是利用民眾對身體不適、健康保養或日常健康管理的在意，進一步誘導購買、留下聯絡資料，或導向不明網站與客服。提醒民眾，凡是宣稱效果過於神奇、見效過快，或標榜「多種問題都能改善」的產品資訊，都應特別提高警覺，不可因廣告話術就輕易相信。

此外，本週常見的詐騙內容也會使用「台灣」、「安心」、「優惠」等字眼，刻意營造在地、可靠又划算的感覺。例如標榜「台灣設計」、「台灣熱銷」、「安心使用」、「現正優惠」、「刷卡服務」、「分期付款」等，讓民眾以為商品來源明確、交易有保障，進而降低戒心。不過，這些字眼也可能只是詐騙集團用來包裝假賣場、假客服或假付款頁面的手法，後續可能造成個資外洩、信用卡資料遭冒用、重複扣款，甚至付款後根本收不到商品。提醒民眾，不要因看到「台灣」或「安心」等字樣就放下防備，仍應優先查核網站真實性、商家資訊及客服管道是否公開透明。

另從整體宣傳方式觀察，本週詐騙訊息也很常把「必備」、「推薦」、「神器」、「健康」這些字眼結合使用，讓商品看起來不只是便宜，而是「很多人都在買」、「現在不買可惜」、「買了就能解決問題」。再配合「前50名」、「限時加贈」、「手慢就沒了」、「錯過可惜」等字句，進一步製造急迫感，促使民眾在尚未查證前就快速做出決定。提醒民眾，只要看到廣告一直強調效果很好、名額有限、優惠快截止，或要求儘快點擊外部連結、留下聯絡資料、加入通訊帳號時，都應先停下來查證，不要因一時心急而落入詐騙陷阱。

綜合本週觀察，常見詐騙手法多半是先用「設計」、「必備」、「推薦」等高頻字眼吸引注意，再用「配方」、「問題」、「健康」等說法增加可信度，接著以「台灣」、「安心」、「優惠」降低民眾戒心，最後透過「神器」、「熱銷」、「限量」等行銷話術催促下單，將人引導至站外頁面、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，或先付款才能取得優惠、商品或服務的情況，都

應提高警覺、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，以降低受騙風險。

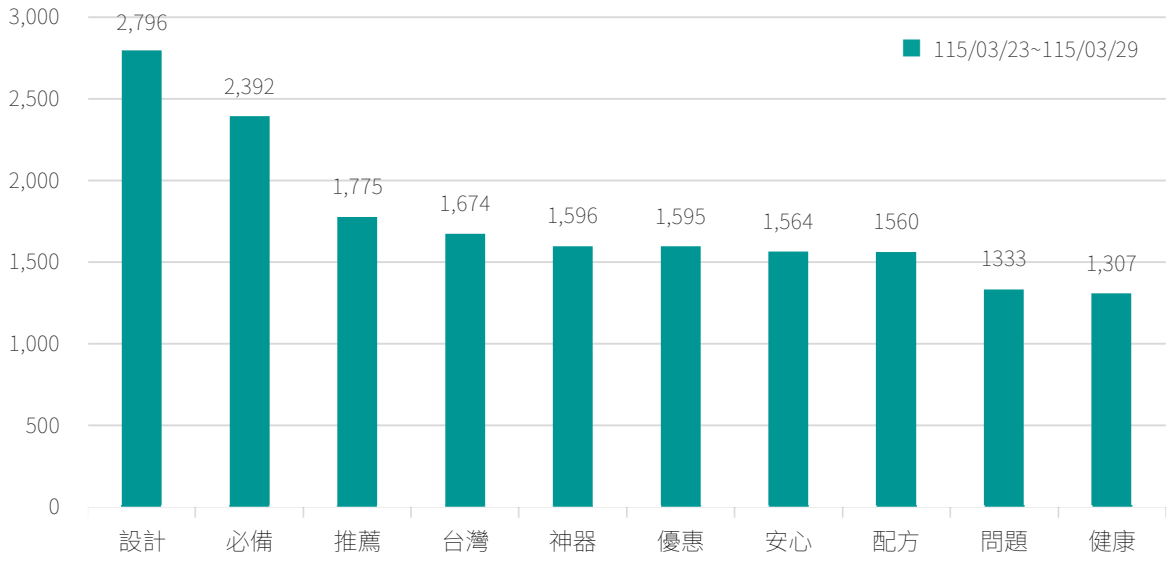

圖7 | 本週代表性詐騙關鍵字 Top 10

焦點文章

漏洞通報統計與趨勢

本季漏洞通報統計顯示，市面常見系統與軟體產品仍以「輸入驗證不足」為主要安全問題來源，同時於身分鑑別、授權機制及系統設定等面向，亦持續存在一定程度之資安風險。

為進一步了解漏洞分布情形，以下針對115年1月至3月期間之實際通報資料進行分析，詳見表2，TWCERT/CC TVN平台公告共計51筆漏洞，依其成因可進一步歸納為四大類別，包含輸入驗證、身分鑑別與授權、設定與環境及記憶體破壞。

表2 | 115/1~115/3 漏洞資料分析

漏洞類型		數量統計	
輸入驗證 (Input Validation)	Path Traversal	6	32
	SQL Injection	6	
	Arbitrary File Upload	5	
	OS Command Injection	4	
	Cross-site Scripting	4	
	Download of Code Without Integrity Check	2	
	Insecure Deserialization	1	
	Open redirect	1	
	Improper Certificate Validation	1	
	Insecure Direct Object Reference	1	
	Local File Inclusion	1	

漏洞類型		數量統計	
身分鑑別與授權 (AuthN & AuthZ)	Missing Authentication	8	14
	Incorrect Authorization	2	
	Missing Authorization	1	
	Authentication Bypass	1	
	Local Privilege Escalation	1	
	Client-Side Enforcement of Server-Side Security	1	
設定與環境 (Config & Env)	Use of Hard-coded Credentials	1	4
	Insufficiently Protected Credentials	1	
	Sensitive Data Exposure	1	
	DLL Hijacking	1	
記憶體破壞 (Memory Corruption)	Stack-based Buffer Overflow	1	1
總計		51	

AuthN=Authentication，身分鑑別
AuthZ=Authorization，授權

焦點文章

以下將依各類型漏洞之比例與影響，逐一說明其重點與防護建議：

一 輸入驗證為主要漏洞類型(占比62.7%)

此類別漏洞占總數超過六成，顯示多數系統開發時，尚未建立完善之驗證與過濾機制，無法有效過濾或驗證使用者輸入的資料。

- 路徑遍歷(Path Traversal)與SQL注入(SQL Injection)各6件，為最主要類型，顯示檔案路徑與資料庫操作相關參數未妥善控管，易遭攻擊者利用以存取敏感資訊或竄改資料內容。
- 任意檔案上傳(Arbitrary File Upload)共5件，若未妥善檢查檔案內容與副檔名，可能導致攻擊者上傳後門程式，進而取得伺服器控制權，風險相對較高。

整體而言，輸入驗證不足仍為多數應用系統最基礎且關鍵之資安弱點。

防護建議

應採用「預設拒絕」原則，僅允許符合預期格式之輸入資料，防止任何非預期的輸入。
使用參數化查詢機制，以降低SQL Injection風險。

二 身分管理機制不健全(占比27.4%)

此類別漏洞主要集中在缺乏身分鑑別(Missing Authentication)類型，共計8件，占此類漏洞之多數。

- 身分鑑別包含管理介面、API及內部功能，即使管理介面已設置身分驗證機制，若驗證流程設計不佳，仍可能遭攻擊者透過不同面向繞過驗證檢查，進而直接存取特定功能。
- 授權管理亦為重要環節，包含不當授權(Incorrect Authorization)、缺乏授權(Missing Authorization)及本機提權(Local Privilege Escalation)等類型，共計4件。此類漏洞可能導致攻擊者提升權限，進而存取機敏資訊或遠端執行任意程式碼。

整體而言，此類問題多源於系統功能設計未完整考量權限邊界，或驗證邏輯存在缺陷。

防護建議

落實最小權限原則，確保每個帳號僅有執行任務所需之最小權限。
確保每項功能僅有對應權限帳號可以存取，並停用不必要之帳號。

焦點文章

三 設定與環境管理不當(占比7.9%)

此類漏洞多與系統部署與設定管理不當有關，通常因開發者為了便利或減少開發成本而導致，常見情境包括使用預設設定、未加密或儲存機敏資料，或直接採用第三方套件而未根據自身環境進行適當安全設定與調整等。

上述問題多非技術困難所致，而是源於安全設定與管理機制未落實所導致。

防護建議

嚴禁將金鑰、通行碼寫在程式碼或設定檔中，並避免使用預設密碼。
建立軟體清單(SBOM)，定期比對已知漏洞公告(CVE)，並及時更新第三方函式庫。
確保所有機敏資訊於儲存與傳輸之過程中，皆採取加密或其他適當措施。

四 記憶體使用不嚴謹(占比2%)

此類漏洞成因為記憶體操作未妥善控管邊界，導致實際使用超出原配置範圍，進而影響到其他記憶體空間，嚴重時可能造成程式執行流程異常或遭惡意控制。

此類漏洞比例雖低，惟一旦被利用，可能對系統穩定性與安全性造成重大影響，仍需謹慎因應。

防護建議

建議確保開啟編譯器安全防護功能，如位址空間配置隨機化(ASLR)、資料執行防止(DEP/NX)及堆疊金絲雀(Stack Canaries)。
採用相對安全版本之記憶體操作函式，請勿使用舊版函式。
妥善限制輸入的資料大小，以防超過配置之記憶體空間。

焦點文章

五 結語

本次統計數據顯示，我國市面系統與軟體產品廠商在「輸入驗證」與「身分鑑別與授權機制」等基礎安全面向，仍有明顯的改善空間，相關問題多屬開發與設定階段即可預防之類型，顯示基礎資安實務尚未全面落實。

建議相關廠商及開發單位參考OWASP Top 10之防護準則，並將上述資安防護策略整合至軟體安全開發生命週期(SSDLC)中，透過資安左移，從設計階段即導入安全要求，逐步強化系統整體安全性。

關鍵字：漏洞通報、TWCERT/CC、TVN

刊　　名　資安週報第 38 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