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

開發套件所造成之供應鏈事件應持續監控憑證與異常存取 防範權限濫用

聯防監控

防禦迴避高居首位 初始入侵仍具威脅

蜜罐誘捕

應用程式遞送控制器與PHP伺服器端腳本語言成攻擊熱點

外部曝險分析

TLS憑證與弱加密風險大幅改善 整體曝險持續下降

網路巡查高風險詐騙

高風險內容持續混入日常購物資訊 近期須留意商品包裝與假客服手法

焦點文章

智慧家庭的資安風險與治理：從使用者行為到產品安全設計的政策路徑

2026.04.09
039

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

開發套件所造成之供應鏈事件應持續監控憑證與異常存取 防範權限濫用

本週總計接獲15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。本週有機關偵測發現異常網域查詢行為，經研判與近期 Axios NPM 供應鏈攻擊事件相關。該事件係駭客於官方套件中植入惡意相依套件，當開發或系統環境執行套件安裝時，惡意程式即於背景自動執行，對外連線至特定網域進行報到，並依不同作業系統下載對應之惡意程式，建立持續性存取管道。整體攻擊過程快速且具隱蔽性，甚至會於執行後自動清除痕跡，使受害主機難以察覺異常。

鑑於此類攻擊可能蒐集開發環境中之憑證、API 金鑰或環境變數，一旦外洩，恐導致雲端服務或內部系統遭未授權存取，風險由單一主機擴大至整體環境。技術面上，除應即時隔離受害主機並阻斷異常連線外，應全面檢視並更換相關憑證與金鑰，盤點其使用範圍與權限，並加強存取紀錄與異常行為監控，以防止後續濫用。管理面上，應強化開發人員對敏感資訊保護之認知，避免將憑證或金鑰明文存放於程式碼或環境中，並建立安全的憑證管理與存取機制(如集中控管、定期輪替與最小權限設定)，同時提升對開源套件風險與異常行為之辨識能力，以降低供應鏈攻擊所帶來之影響。

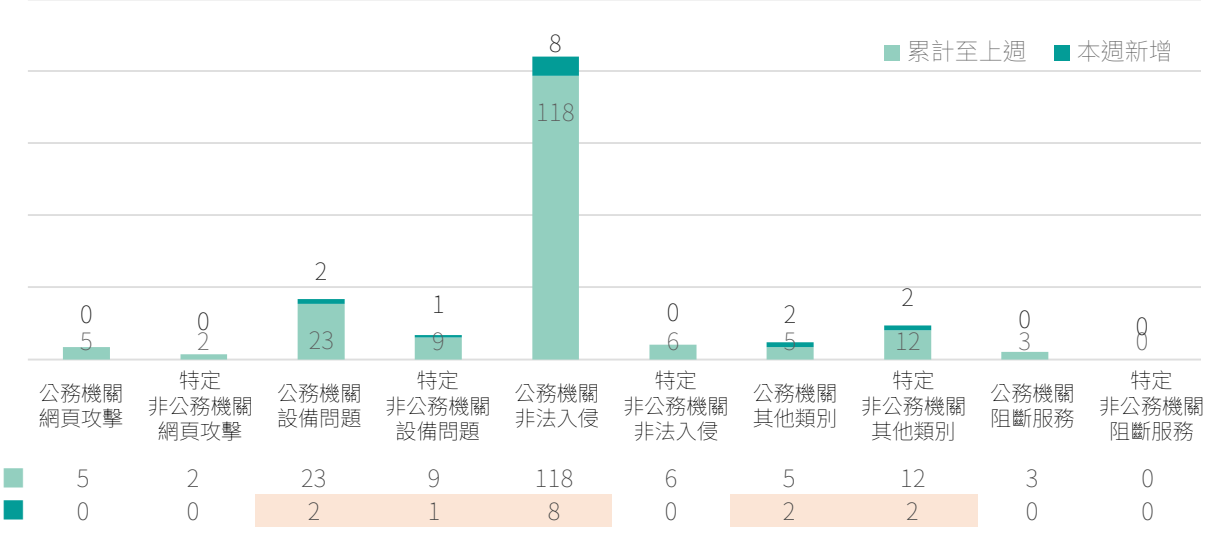

圖1 | 本週公務機關暨特定非公務機關資安事件通報概況

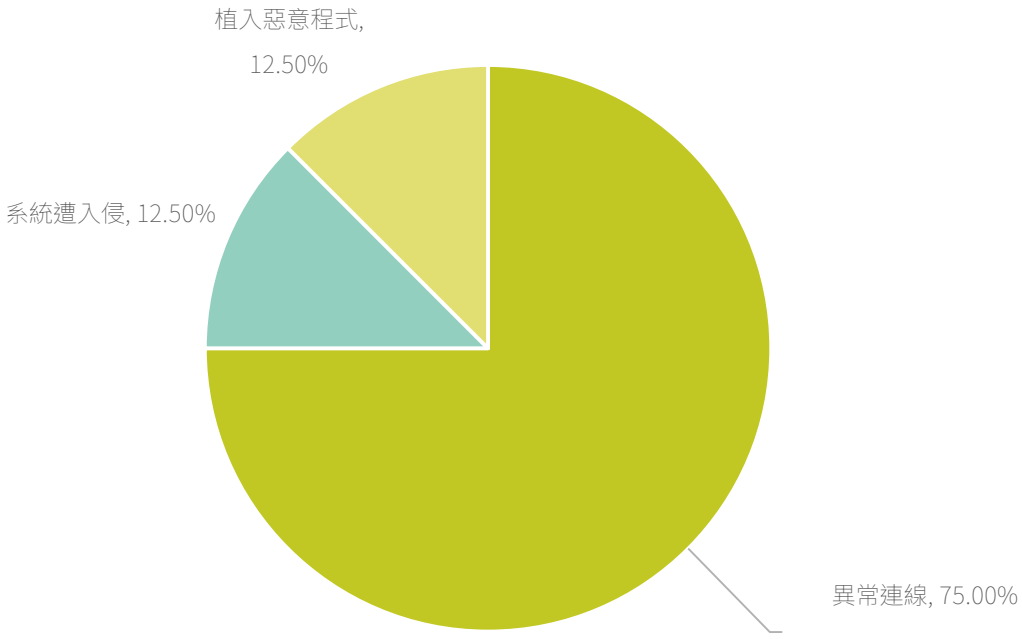

圖2 | 本週公務機關非法入侵事件類型占比

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
➢ 惡意套件植入後門竊取憑證並持續存取 ➢ 供應鏈攻擊橫向擴散影響多系統環境	➢ 建立套件來源驗證機制，避免使用未經審核或異常開源套件 ➢ 強化憑證與金鑰管理機制，落實集中控管與定期輪替措施 ➢ 導入異常連線監控機制，即時偵測對外可疑網域通訊行為 ➢ 建立開發環境安全控管機制，避免敏感資訊明文存放於系統中

2間民間企業揭露重大資安訊息

本週2家民間企業發布重大訊息，產業類別分為電子零組件業及電腦及週邊設備業。

- **公司名稱：** 建通精密工業股份有限公司
- **發布時間：** 115 年 4 月 1 日
- **事件說明：** 建通公司、重要子公司-蘇州建通光電端子有限公司及重要子公司-越南建通電子五金責任有限公司部份資訊系統遭受網路攻擊。已立即啟動資安防禦與復原機制，並委請外部資安技術專家協助處理。經評估對公司營運無重大影響，後續將持續密切監控，並配合外部資安技術專家追查事件及釐清原因，全面檢視系統安全，且加強系統的監控與防護，以提升及強化資安保護及資訊安全。

- **公司名稱：** 振樺電子股份有限公司
- **發布時間：** 115 年 4 月 2 日
- **事件說明：** 振樺電公司接獲外部情資單位通知，官方網頁及部分網路服務資料疑似遭到入侵而導致部分資料外流。公司於獲悉後立即啟動資安應變機制，檢視受影響之範圍並完成帳號全域密碼重設。經檢視雖有資料外流，但未有公司核心資通系統之資料或敏感資訊外洩，對公司產品及客戶隱私無影響，經初步評估對公司財務業務無重大影響。後續將持續加強帳戶之機密身分驗證(MFA)機制、網路服務協議升級及定期執行帳號清理，並持續提升員工資安意識培訓。

■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15.9%，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，顯示攻擊者在攻擊前期持續加大對目標環境的偵查與資訊蒐集力度。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。攻擊者透過自動化工具對大範圍網段進行探測，以識別可存取服務與開放埠，並結合被動式 DNS 分析，掌握目標組織之網域架構、子網域關聯與歷史解析紀錄，進一步描繪完整攻擊面。此類行為結合主動與被動偵查手法，具備低互動、高隱蔽的特性，且能有效提升後續攻擊的成功率。建議強化對異常掃描流量的監控與阻擋機制，定期盤點與控管對外資產與DNS資訊曝光情形，並結合威脅情資分析，以提前辨識潛在攻擊準備活動。

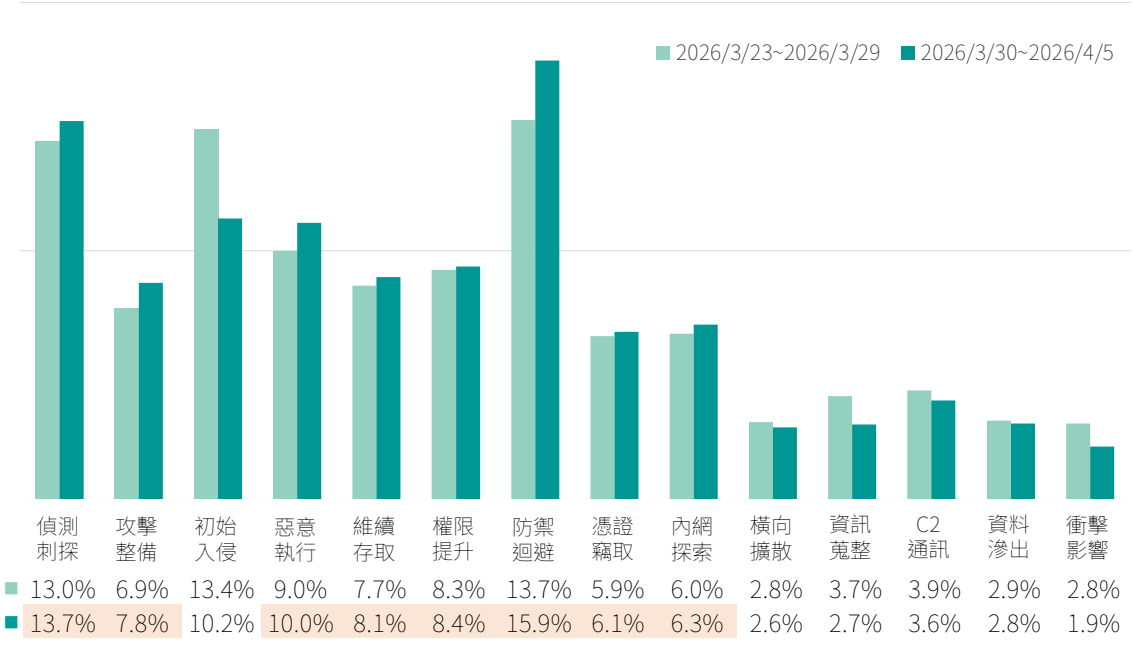

圖3 | 資安聯防監控攻擊階段統計

防護建議 建議機關採取下列防護措施：

- 強化端點防護（EDR / XDR），監控系統工具濫用（如 PowerShell、cmd）
- 啟用並集中化指令紀錄（Command Logging）與稽核機制
- 限制與控管高風險工具使用（如 LOLBins）
- 建立特權帳號管理機制（PAM），降低權限濫用
- 偵測異常行為

防禦迴避（Defense Evasion）

- 部署網路層防護
- 建立流量基準（Baseline），識別異常大量探測行為
- 定期盤點對外資產（External Attack Surface Management）
- 控管 DNS 資訊暴露
- 導入威脅情資（Threat Intelligence）

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

應用程式遞送控制器與PHP伺服器端腳本語言成攻擊熱點

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68.77%、「遠端控制」服務攻擊占比27.42%，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74.88%。「遠端控制」服務亦有21.53% 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。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。

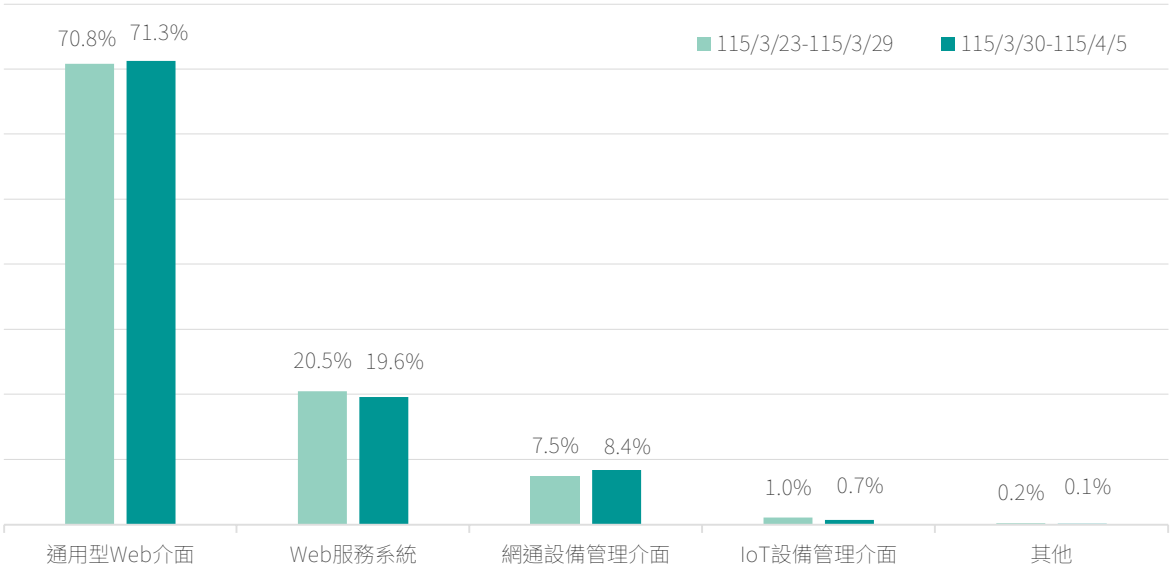

圖4 |本週網頁應用介面之誘捕攻擊比例統計

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、遠端程式碼執行漏洞、目錄遍歷漏洞及程式碼注入漏洞，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、VPN Gateway及行動裝置管理系統，顯示網通設備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	↑1	CVE-2024-4577[2]	PHP	9.8
■	3	↑New	CVE-2024-24919[3]	Check Point VPN Gateway	8.6
■	4	↑New	CVE-2025-4428[4]	Ivanti Endpoint Manager Mobile	7.2
■	5	↑New	CVE-2024-21887[5]	Ivanti Connect Secure	9.1

類型 ■越界讀取漏洞 ■遠端程式碼執行漏洞 ■目錄遍歷漏洞 ■程式碼注入漏洞

▶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21個高風險安全漏洞(CVE-2026-5272至CVE-2026-5292[6])，類型包含緩衝區溢位(Buffer Overflow)與使用釋放後記憶體(Use After Free)等，最嚴重可使未經身分鑑別之遠端攻擊者利用特製HTML頁面逃離瀏覽器沙箱環境並執行任意程式碼。

- FortiClient EMS存在高風險安全漏洞(CVE-2026-21643[7]與CVE-2026-35616[8])，類型分別為SQL注入(SQL Injection)與不當存取控制(Improper Access Control)，兩者皆能使未經身分鑑別之遠端攻擊者執行任意程式碼。

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-2024-24919
4. https://nvd.nist.gov/vuln/detail/cve-2025-4428
5. https://nvd.nist.gov/vuln/detail/cve-2024-21887
6. https://chromereleases.googleblog.com/2026/03/stable-channel-update-for-desktop_31.html
7. https://nvd.nist.gov/vuln/detail/CVE-2026-21643
8. https://nvd.nist.gov/vuln/detail/CVE-2026-35616

■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憑證與弱加密風險大幅改善 整體曝險持續下降

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6,403項。其中，「元件高風險漏洞」以3,718項居首，「CSP設定不當」989項次之，「未部署WAF」705項排名上升至第三位；「過時或弱加密協定」則降至446項，排名下滑。前三項合計5,412項，占前10大風險項目總數約84.5%，顯示當前風險重點已轉向應用層防護與漏洞管理面向。相較上期7,599項，整體風險數量減少1,196項，降幅約15.7%，顯示相關機關於接獲警訊通知後，已陸續採取改善措施，整體曝險情勢已有所改善，詳見圖5。

進一步分析重大風險變化情形，「元件高風險漏洞」由3,943項降至3,718項，減少225項，減幅約5.7%；「TLS憑證不受信任」由625項大幅降至29項，減少596項，降幅約95.4%；「過時或弱加密協定」由916項降至446項，減少470項，降幅約51.3%，均呈現明顯改善趨勢。依本週機關回應情形，部分改善係因機關重新檢視既有站台與服務後，發現部分資產雖已停用，惟未確實完成下線或關閉，經立即關閉相關服務後，相關風險項目隨之下降。「CSP設定不當」由988項微增至989項，增幅約0.1%，變化不大；「未部署WAF」則由576項增至705項，增加129項，增幅約22.4%，顯示部分對外網站在WAF部署及應用層攻擊防護方面仍有待強化。

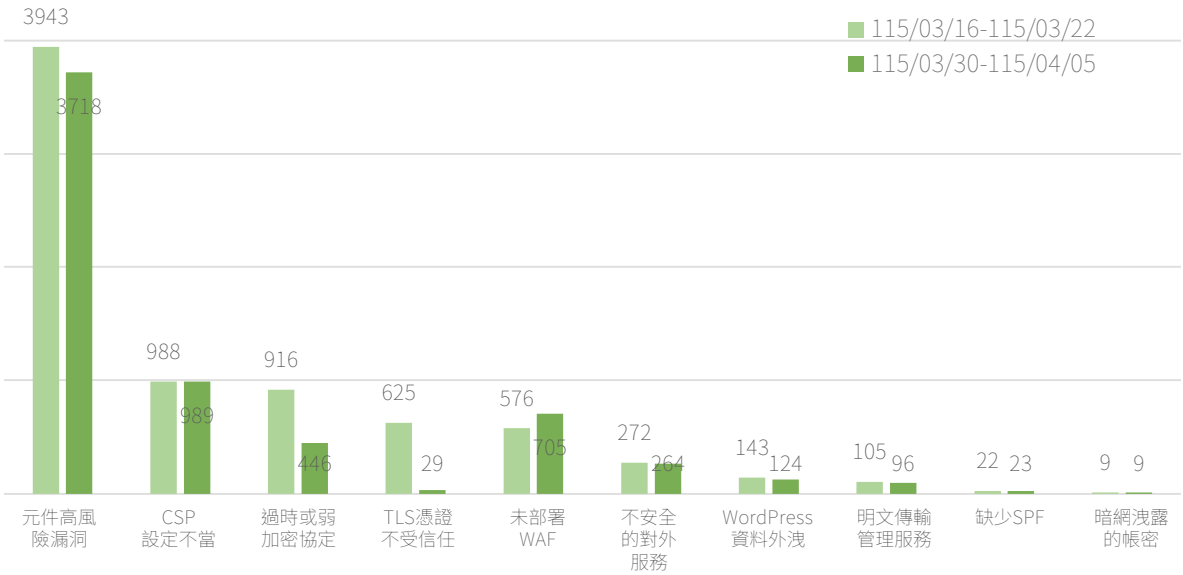

圖5 | EASM檢測結果統計(前10大風險)

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
➢ 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，並淘汰已無維護之軟體版本 ➢ 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，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)	➢ 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

■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資訊，近期須留意商品包裝與假客服手法

本期高風險詐騙內容仍以日常消費場景為主，常見題材涵蓋 3C 配件、穿搭、美容保養、保健護理與家用商品等。這類訊息外觀與一般促銷貼文相近，容易讓民眾在瀏覽時降低戒心，詳見圖6。

從風險類型來看，「產品服務」仍是主要來源，常以「推薦使用」「限時優惠」「快速有感」「現貨供應」等說法吸引注意，進一步引導點擊連結、私訊洽談或站外交易。「身分冒充」則多出現在後續流程中，常由假客服、假賣家或假物流名義介入，藉退款、補件、付款異常等情境要求提供驗證碼、帳戶資料或進一步操作。「金融投資」雖非本期主軸，但凡涉及保證獲利、快速回本、專人帶單等內容，仍須保持警覺。

整體而言，本期高風險內容仍以商品型包裝為主，並持續嵌入購物與售後流程之中；詐騙訊息愈來愈像一般日常商品資訊，辨識難度也隨之提高。

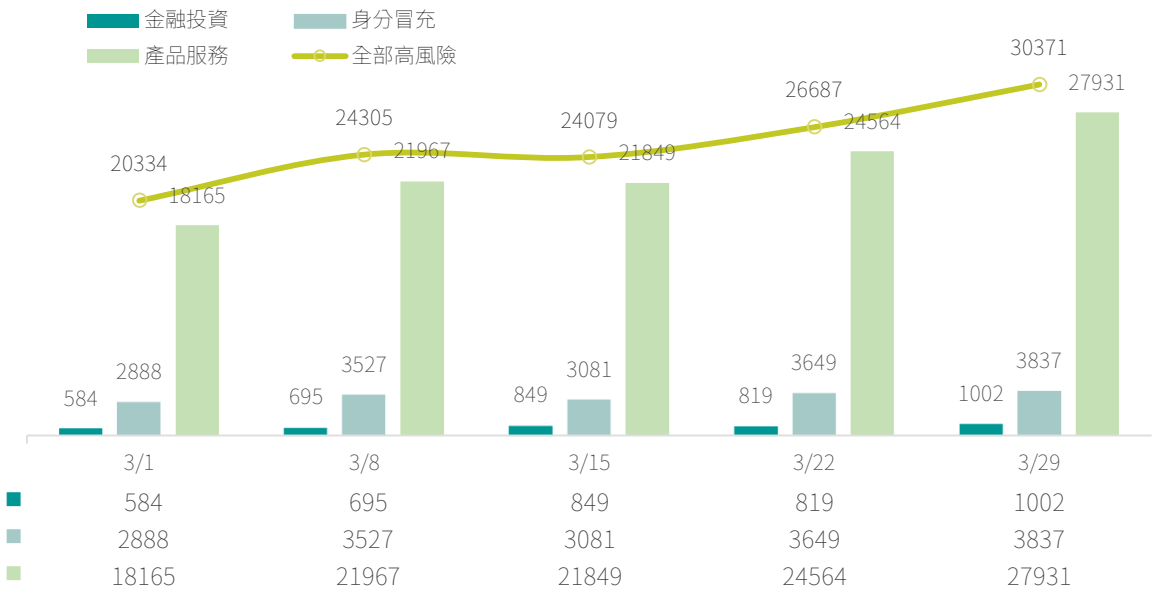

圖6 | 偵獲高風險金融投資、身分冒充、產品服務類詐騙週趨勢

近期高風險手法辨識重點

越像日常購物資訊，越要多查一步

若商品訊息同時出現私訊下單、另開連結、站外交易或改用其他通訊工具洽談等情況，應視為高風險警訊。

後續客服流程往往才是真正風險點

凡要求重新付款、提供驗證碼、確認帳戶或點擊補件連結者，都不應直接照做，應改由官方管道重新確認。

先保留證據，再通報查證

遇到疑似詐騙內容時，應保留廣告畫面、對話紀錄、連結與付款資訊，並儘速通報 165 反詐騙專線或平台客服。

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」、「優惠」為主要高頻字眼，並搭配「推薦」、「配方」、「神器」、「台灣」、「安心」、「健康」等用語，詳見圖7。整體來看，詐騙訊息仍多以商品行銷、優惠促銷及保健宣傳作為包裝，先用「設計貼心」、「生活必備」、「限時優惠」等說法吸引注意，再以「推薦使用」、「安心配方」、「台灣熱銷」等字眼提高可信度，讓民眾誤以為只是一般商品資訊，進而點擊連結、留下資料或進入付款流程。

此外，這類訊息也常以「簡單好用」、「一用就有感」、「買一送一」、「限量補貨」等話術製造商品熱銷與立即下單的急迫感；另有部分內容假借「醫師推薦」、「草本配方」、「有助健康」等說法，包裝商品具專業性或保健效果，藉此降低民眾戒心。也常見以「台灣設計」、「安心使用」、「可刷卡」、「可分期」等字眼，營造來源可靠、交易安全的印象，但實際上可能是包裝假賣場、假客服或假付款頁面的手法。

綜合本週觀察，常見詐騙手法多半是先以「設計」、「必備」、「優惠」等關鍵字吸引注意，再用「推薦」、「配方」、「安心」、「健康」等說法增加可信度，最後將民眾引導至不明連結、假賣場或付款頁面。提醒民眾，凡遇要求點擊不明連結、填寫個人資料、提供信用卡資訊，或先付款才能取得商品、優惠或服務者，都應提高警覺，先查證再操作。

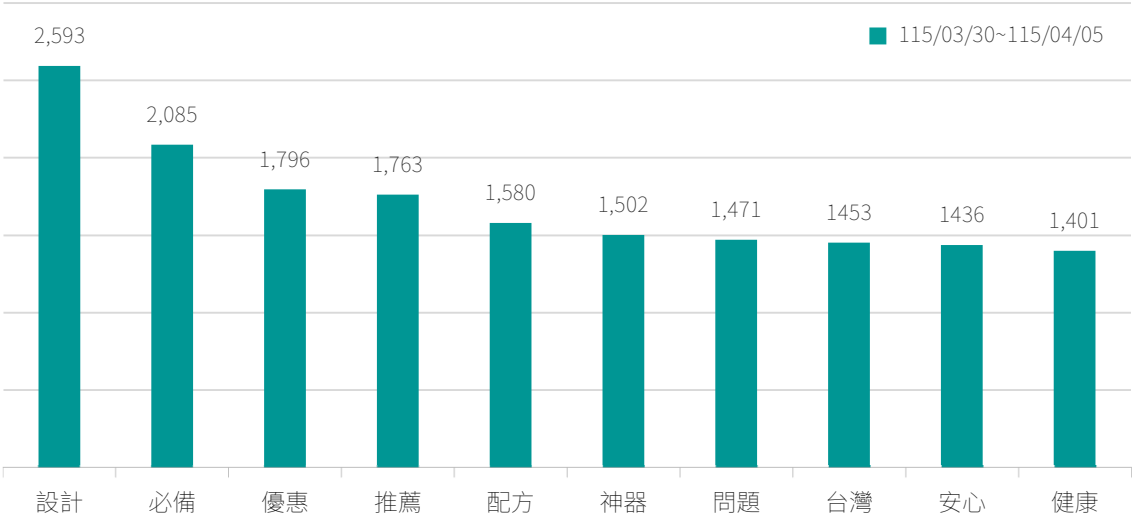

圖7 | 本週代表性詐騙關鍵字 Top 10

焦點文章

智慧家庭的資安風險與治理：從使用者行為到產品安全設計的政策路徑

一 前言：智慧家庭時代的資安挑戰

隨著物聯網（Internet of Things, IoT）技術快速發展，各類連網裝置逐漸融入家庭生活，形成「智慧家庭」（smart home）環境。例如智慧音箱、連網攝影機與智慧門鎖等應用裝置，雖可提升便利性，但亦可能帶來未經授權存取、資料外洩或遠端操控等資安與隱私風險[1]。

本文參考德國聯邦資訊安全局（BSI）《家用IT安全管理報告》（IT-Sicherheitsmanagement in Haushalten, ISiH）與相關文獻，從家用物聯網裝置的風險成因出發，分析使用者行為與裝置弱點如何形成安全風險，並探討使用者防護措施與政府制度如何引導安全設計與弱點管理[2]。

二 智慧家庭的資安風險地圖

不同於企業環境，智慧家庭裝置多由使用者自行安裝與設定，其安全性與維護難易程度差異甚大。例如使用弱密碼、未啟用多因子驗證（MFA）或未定期更新韌體等情形均可能提高裝置遭入侵或濫用的風險。

（一）使用者行為風險

研究指出，裝置風險不僅來自技術弱點，也與使用者的安全行為與風險認知不足相關，以下重點摘要：

1. 裝置與帳號共用，權限與密碼管理不易

家庭環境普遍有帳號與裝置共用之情形，使多人共用同一裝置並共用帳號密碼，例如家庭成員共用寵物攝影機、智慧門鈴等遠端監控裝置之帳號密碼，均可能增加帳戶遭竊或濫用的風險[3]。

2. MFA使用率偏低

多因子驗證（MFA）的使用率偏低，主因在於使用者認為操作繁瑣，或誤認家庭環境較為安全。因此，一旦攻擊者取得登入憑證或驗證資訊，便可於未重新驗證的情況下持續控制裝置，或用於從事其他惡意網路活動[4]。

焦點文章

3. 未更改不安全原廠設定

由於部分使用者在裝置啟用後未更改預設帳號與密碼，或忽略權限與存取設定等，使裝置長期暴露於風險之下[5]。

4. 裝置汰除與廢棄及韌體更新相關風險

部分消費者於裝置汰除或廢棄時，未對裝置進行妥善處置，而有資料外洩疑慮。此外，家用物聯網裝置之韌體安全性更新與資安密切相關，當裝置未能持續進行更新時，其防護能力將隨時間逐漸下降，增加資安風險。

（二） 技術與裝置風險

智慧家庭裝置在硬體、軟體、韌體與網路層面均可能存在弱點，使其成為常見攻擊目標，主要包括：

1. 預設憑證與認證機制薄弱

弱密碼與預設憑證（Default Credentials）是物聯網裝置最常見的安全弱點之一，故使用者若未變更原廠設定，攻擊者可透過自動化掃描工具搜尋使用預設憑證的裝置，並利用暴力破解或憑證填充攻擊（Credential stuffing）取得存取權限。進一步，攻擊者可將裝置納入殭屍網路，用於分散式阻斷服務攻擊（DDoS）或橫向移動至家戶網路環境中的其他裝置。

2. 通訊協定安全強度不足

當裝置在資料傳輸過程中缺乏加密或動態驗證機制時，攻擊者可能攔截、竄改或重發通訊訊號。例如在「重放攻擊」（Replay Attack）中，攻擊者擷取合法控制指令後重新發送，即可在未經授權的情況下模擬使用者操作並控制裝置。

3. 韌體弱點與更新機制不足

若製造商缺乏完善的安全更新機制或長期維護計畫，裝置在新弱點被發現時可能無法及時修補。此外，若裝置不支援自動更新或更新頻率過低，攻擊者亦可能利用未修補的弱點入侵並植入惡意程式。

焦點文章

三 智慧家庭資安治理的多層次緩解策略

如前所述，智慧家庭的資安風險往往來自使用者行為與技術弱點的交互作用，因此需從使用者行為、產品設計與制度治理等多個層面共同因應。

（一）使用者層面的防護措施

在家庭環境中，使用者的安全習慣是防護的重要基礎。首先，建議啟用多因子驗證（MFA），以提升帳號安全性並降低帳號遭竊用的風險。其次，使用者可透過密碼管理工具或帳號分級等措施，避免家庭成員共用帳號或重複使用特定密碼。

此外，留意檢查權限與存取設定是否適當，或其他如定期更新裝置韌體等，亦是降低風險的重要措施。同時，因部分使用者可能認為系統更新繁瑣費時或過於複雜，此時製造商如設計背景自動更新機制供選用，即可提升使用者更新意願。至於裝置汰除或廢棄時，須落實資料抹除或以實體破壞資料存儲設備，以避免資料遭惡意復原與利用。

（二）技術與產品層面的安全措施

因消費者常難以自行判斷產品安全性，若僅依賴自發之市場機制或使用者自我防護，難以有效降低風險。因此，近年各國政府逐漸透過法規與標準建立產品資安要求，要求製造商在產品設計與生命週期管理中納入安全機制，並持續推廣全民資安意識，以降低潛在風險。

在國際政策發展上，歐盟於2024年正式通過《網路韌性法》（Cyber Resilience Act, CRA），要求製造商在產品設計與開發階段納入資安風險評估與安全設計，並在產品上市後持續處理弱點與提供安全性更新服務。此外，CRA亦要求製造商建立弱點通報與修補機制，並敘明其支援期限，以確保消費者在產品生命週期內能持續取得安全性更新，且若業者未能符合相關要求，產品可能被禁止於歐盟市場銷售，並面臨高額罰鍰。

在我國制度方面，《資通安全管理法》亦建立政府與關鍵基礎設施提供者的資安防護要求，要求各公務與非公務機關須建立資安管理制度，並針對資訊系統採購、委外辦理訂定嚴謹之管理要求，未來可透過訂定類似CRA之法規來進一步強化產品資安。

焦點文章

四 結論

隨著智慧家庭裝置日益普及，資安風險已成為家戶安全的重要議題。此風險是使用者行為、裝置設計與制度環境交互作用的結果，包括弱密碼、未啟用多因子驗證、未更新韌體或軟體弱點等使用行為，以及裝置安全機制不足等因素相互影響，因而提高裝置遭入侵或濫用的可能性。

因此，未來智慧家庭資安治理，除「使用者自我防護」外，允宜強化「安全預設（secure-by-default）與設計即安全（security-by-design）」的制度架構。除持續提升使用者資安意識並落實基本防護措施外，亦應透過法規與政策機制，要求製造商於產品設計及生命週期管理中納入資安考量，以構築兼具安全與信任的智慧家庭環境。

參考資料

1. Vardakis, G., Hatzivasilis, G., Koutsaki, E., & Papadakis, N. （2024）. Review of smart-home security using the Internet of Things. Electronics, 13（16）, 3343. https://doi.org/10.3390/electronics13163343
2. Bundesamt für Sicherheit in der Informationstechnik. （2025）. Qualitative Befragung von Verbraucherinnen und Verbrauchern zum Thema IT-Sicherheit in Privathaushalten （DVS-Bericht）. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/DVS-Berichte/Studie_Haushaltsbefragung.pdf
3. Ganiuly, D., Bolatbek, N., & Smaiyl, A. （2025）. Security risks introduced by weak authentication in smart home IoT systems. arXiv. https://arxiv.org/abs/2512.21374
4. Tang, H., Hu, Y., Sun, J., & Zhang, Y. （2025）. Scaling law for video generation with generative world models. arXiv. https://doi.org/10.48550/arXiv.2512.21374
5. 同前註1。

關鍵字：物聯網（IoT）安全、安全設計（Security-by-Design）、網路韌性法（CRA）

刊　　名　資安週報第 39 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