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
瀏覽器功能與分析工具便利性 仍需留意其可能帶來的資安風險

聯防監控
本週攻擊態勢持續活躍 「偵測刺探」與「防禦迴避」佔比雙雙攀升

蜜罐誘捕
Citrix NetScaler ADC與Cisco IOS XE網通設備作業系統成攻擊熱點

外部曝險分析
元件高風險漏洞明顯上升 躍居外部曝險風險首位

網路巡查高風險詐騙
高風險內容持續貼近日常消費情境 仍須留意假商品、假客服與健康訴求包裝

焦點文章
產業資安情資分享與趨勢重點

2026.03.19
036

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

瀏覽器功能與分析工具便利性 仍需留意其可能帶來的資安風險

本週總計接獲12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植入惡意程式占多數，多係機關端點偵測(EDR)發現惡意程式為主，詳見圖2。近期觀察到部分風險源自瀏覽器功能使用，如人員於公務電腦登入個人瀏覽器帳號後，因同步機制自動帶入既有擴充套件，其中包含代理節點程式，可能使公務設備在不知情情況下持續對外連線；另亦發現有使用瀏覽器套件可分析下載檔案之情形，該類套件在特定情況下可能將檔案自動上傳至 VirusTotal 平台。由於 VirusTotal 為全球情資共享服務，若未留意檔案內容，仍可能導致機關內部文件或系統資訊外洩。

瀏覽器相關功能與分析工具在提供便利性的同時亦伴隨一定風險，使用者若缺乏相關認知，可能在不知情情況下引入非業務程式或將資料上傳至外部平台。建議機關落實公私分離原則，避免於公務設備登入個人帳號或同步個人設定，並定期檢視與控管瀏覽器擴充套件，限制非業務必要或來源不明之套件使用；同時於使用 VirusTotal 等情資共享平台或檔案分析工具時，應審慎評估資料性質，避免上傳公文或系統相關檔案，以降低資訊外洩風險。

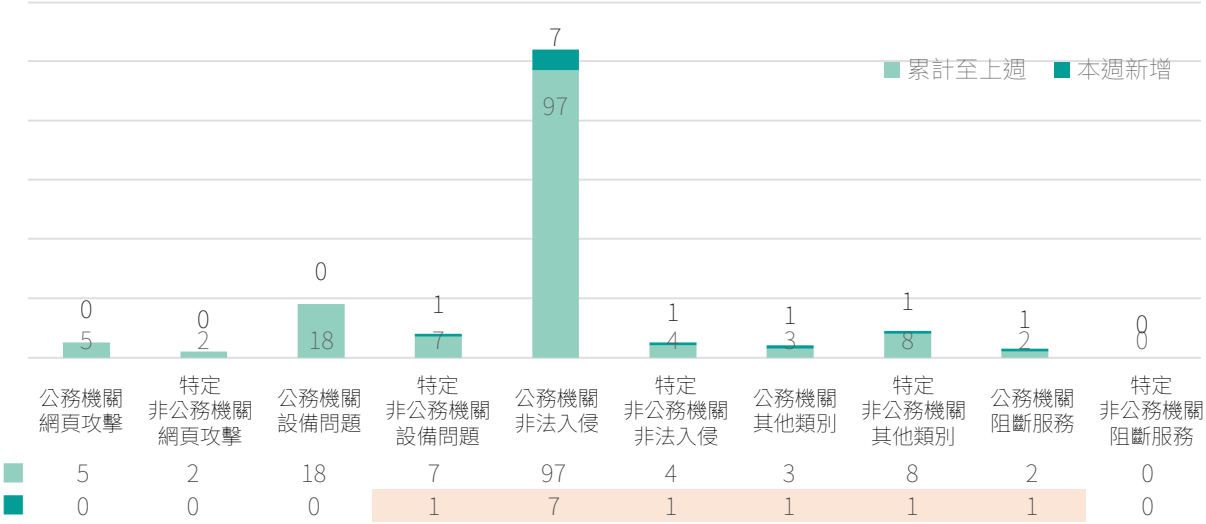


圖1 | 本週公務機關暨特定非公務機關資安事件通報概況

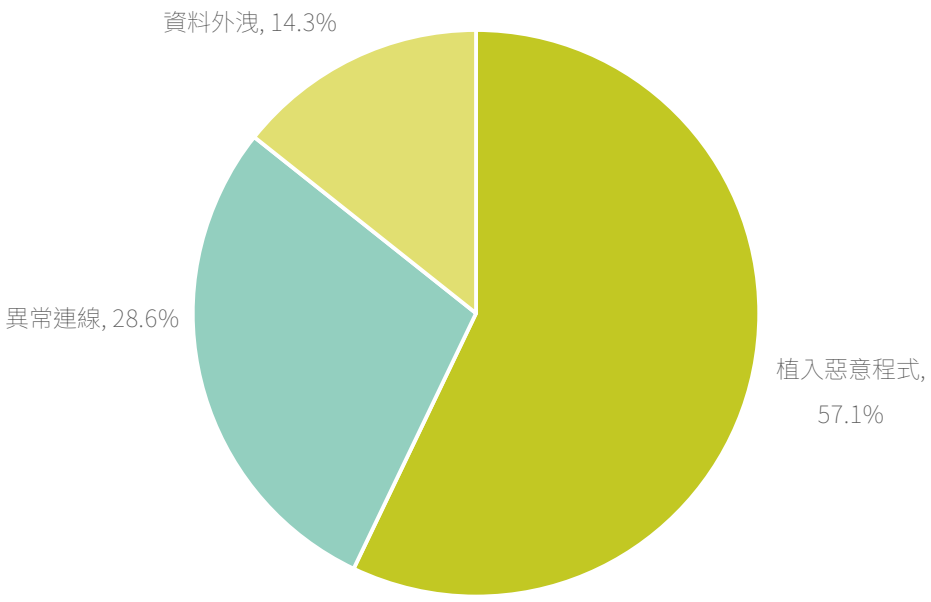


圖2 | 本週公務機關非法入侵事件類型占比

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
➢ 攻擊者利用瀏覽器同步機制植入惡意擴充套件持續對外連線 ➢ 惡意程式誘導上傳檔案至分析平台造成敏感資料外洩	➢ 落實公私帳號分離避免公務設備登入個人瀏覽器帳號 ➢ 定期盤點瀏覽器擴充套件移除非業務必要程式 ➢ 建立瀏覽器套件安裝審核機制限制來源不明套件 ➢ 使用檔案分析平台前先檢視資料避免敏感資訊上傳

1間民間企業揭露重大資安訊息

本週1家民間企業發布重大訊息，產業類為建材營造業。

- **公司名稱：** 新美齊股份有限公司
- **發布時間：** 115 年 3 月 15 日
- **事件說明：** 新美齊公司部分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。經評估對公司財務、業務及營運皆無重大影響，後續將持續密切監控，配合內外部公司技術專家追查事件及釐清原因，全面檢視系統安全，且加強系統監控與防護，以提升強化資安保護及資訊安全。

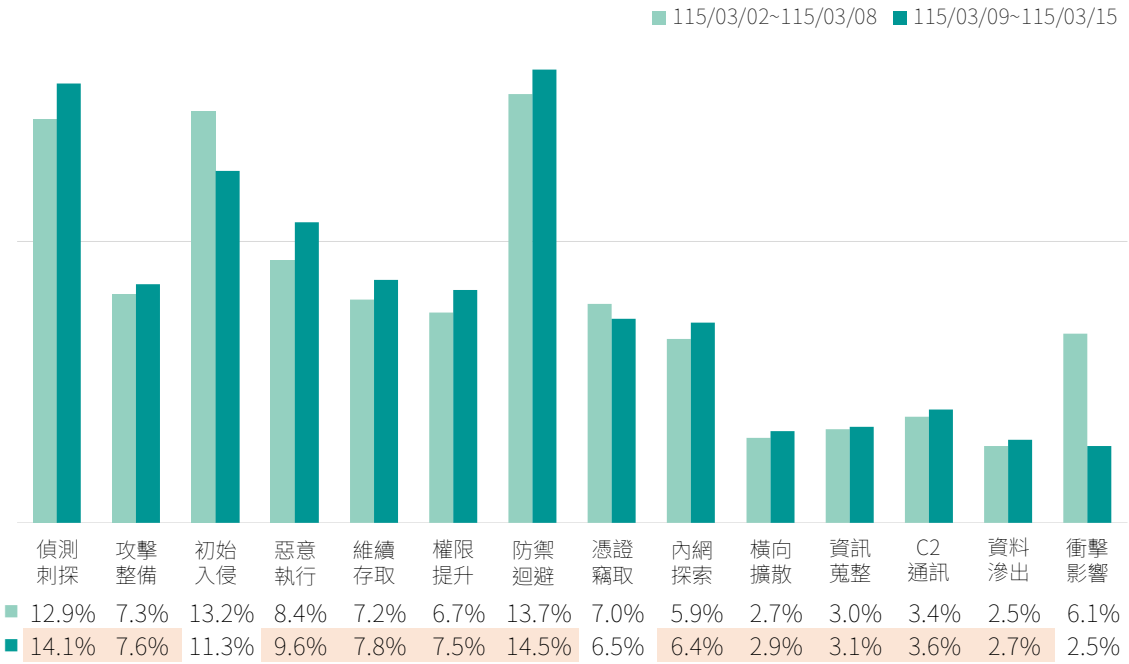
■聯防監控

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

本週攻擊態勢持續活躍 「偵測刺探」與「防禦迴避」佔比雙雙攀升

本週資安聯防監控顯示，整體攻擊態勢呈現持續活躍狀態，詳見圖3，其中「防禦迴避」階段佔比最高達14.5%，較上週增加0.8個百分點，示攻擊者積極運用關閉或清除指令紀錄、利用合法工具執行惡意命令等技術，企圖規避資安防護機制的偵測。其次為「偵測刺探」階段佔比14.1%，較上週上升1.2個百分點，反映攻擊者持續進行目標環境的資訊蒐集與弱點探測活動。第三高為「初始入侵」階段佔比11.3%，雖較上週下降1.9個百分點，但仍維持在高位，顯示攻擊者持續嘗試突破防線建立初步據點。

值得注意的是，「衝擊影響」階段從上週的6.1%大幅下降至2.5%，降幅達3.6個百分點，顯示本週破壞性攻擊活動有所減緩。然而，「惡意執行」、「維續存取」及「權限提升」等中後期攻擊階段均呈現微幅上升趨勢，提醒各單位應持續關注攻擊行為是否由初期偵測刺探逐步演進至更具威脅性的階段，及早採取對應防護措施。



	偵測刺探	攻擊整備	初始入侵	惡意執行	維續存取	權限提升	防禦迴避	憑證竊取	內網探索	橫向擴散	資訊蒐整	C2通訊	資料滲出	衝擊影響
115/03/02~115/03/08	12.9%	7.3%	13.2%	8.4%	7.2%	6.7%	13.7%	7.0%	5.9%	2.7%	3.0%	3.4%	2.5%	6.1%
115/03/09~115/03/15	14.1%	7.6%	11.3%	9.6%	7.8%	7.5%	14.5%	6.5%	6.4%	2.9%	3.1%	3.6%	2.7%	2.5%

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：

➢ 針對「防禦迴避」攻擊手法
- ✓ 導入端點偵測與回應(EDR)解決方案，強化對異常行為的即時監控與告警能力
- ✓ 落實指令紀錄稽核機制，確保系統日誌完整性，避免攻擊者清除入侵痕跡
- ✓ 限制高風險工具的使用權限，建立白名單機制管控合法工具的濫用風險
- ✓ 強化特權帳號管理，實施最小權限原則，定期檢視帳號權限配置的合理性
- ✓ 部署行為分析技術，識別利用合法工具執行惡意命令的異常模式

■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

Citrix NetScaler ADC與Cisco IOS XE網通設備作業系統成攻擊熱點

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62.70%、「遠端控制」服務攻擊占比32.76%，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69.74%。「遠端控制」服務亦有25.29% 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上升主因為Huawei HG532存在遠端程式碼執行漏洞的CVE-2017-17215，遭攻擊次數大幅上升導致。

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。

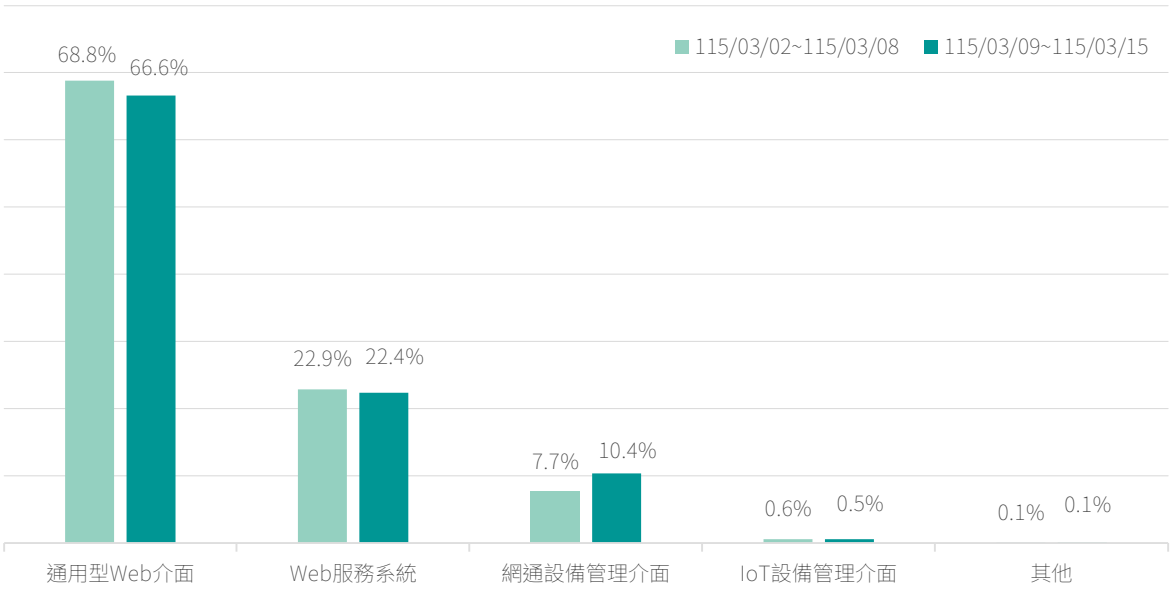


圖4 | 本週網頁應用服務之誘捕攻擊比例統計

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、遠端程式碼執行及輸入驗證不當漏洞，攻擊目標涵蓋Citrix NetScaler ADC、Cisco IOS XE網通設備作業系統、PHP、n8n及Atlassian Confluence Server。其中n8n開源工作流程自動化平台存在2026年公開之CVE-2026-21858新型漏洞，該軟體主要用於企業內部串接各類API與系統服務以建立自動化流程，此漏洞屬於輸入驗證不當之弱點，攻擊者可透過注入指令觸發伺服器端漏洞邏輯，具備自動化擴散特性。以上趨勢顯示此類型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	-	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-2026-21858[4]	n8n	10
■	5	-	CVE-2024-21683[5]	Atlassian Confluence Server	8.8

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

▶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：

- 微軟釋出115年3月份安全性更新，共修補包含SQL Server、Microsoft Office SharePoint及Active Directory Domain Services等共84個漏洞[6]，其中包含16個CVSS達8.8分之高風險漏洞。
- Google Chrome、Microsoft Edge、Vivaldi、Brave及Opera等以Chromium為基礎之瀏覽器存在31個高風險安全漏洞(CVE-2026-3909[7]、CVE-2026-3910[8]、CVE-2026-3913至CVE-2026-3932及CVE-2026-3934至CVE-2026-3942[9])，類型包含越界寫入(Out-of-bounds Write)、程式碼注入(Code Injection)及使用釋放後記憶體(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頁面於瀏覽器沙箱環境執行任意程式碼。其中CVE-2026-3909與CVE-2026-3910已遭駭客利用。
- Ivanti Endpoint Manager存在高風險安全漏洞(CVE-2026-1603[10])，類型為身分鑑別繞過(Authentication Bypass)，未經身分鑑別之遠端攻擊者可取得特定身分鑑別資料。

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-2026-21858
5. https://nvd.nist.gov/vuln/detail/cve-2024-21683
6. https://msrc.microsoft.com/update-guide/releaseNote/2026-Mar
7. https://chromereleases.googleblog.com/2026/03/stable-channel-update-for-desktop_13.html
8. https://chromereleases.googleblog.com/2026/03/stable-channel-update-for-desktop_12.html
9. https://chromereleases.googleblog.com/2026/03/stable-channel-update-for-desktop_10.html
10. https://nvd.nist.gov/vuln/detail/CVE-2026-1603

■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

元件高風險漏洞明顯上升 躍居外部曝險風險首位

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，前10大風險項目共計2,535項，較上週2,454項增加81項，增幅約3.3%，顯示整體外部曝險風險仍呈小幅上升趨勢，詳見圖5。其中，「元件高風險漏洞」由上週622項增加至749項，增幅約20.4%，並由上週第二位升至本週首位，成為本週最主要之外部曝險風險項目；「過時或弱加密協定」714項次之，「TLS憑證不受信任」575項位居第三，前三項合計占比約80.4%，顯示當前外部曝險風險仍高度集中於元件漏洞、加密通訊與憑證管理等議題。

進一步觀察各項重大風險變化，「過時或弱加密協定」由793項減少至714項，減幅約10%，「TLS憑證不受信任」由596項減少至575項，減幅約3.5%，顯示部分機關於加密協定汰換與憑證管理方面已有改善成效。然而，「元件高風險漏洞」增幅明顯，反映部分對外系統在元件版本控管、弱點修補及淘汰過時套件方面，仍存在較高風險壓力。此外，「CSP設定不當」由215項增加至235項，增幅約9.3%，「未部署 WAF」由98項增加至127項，增幅約29.6%，顯示網站安全防護設定相關風險亦有升高情形，值得持續關注。

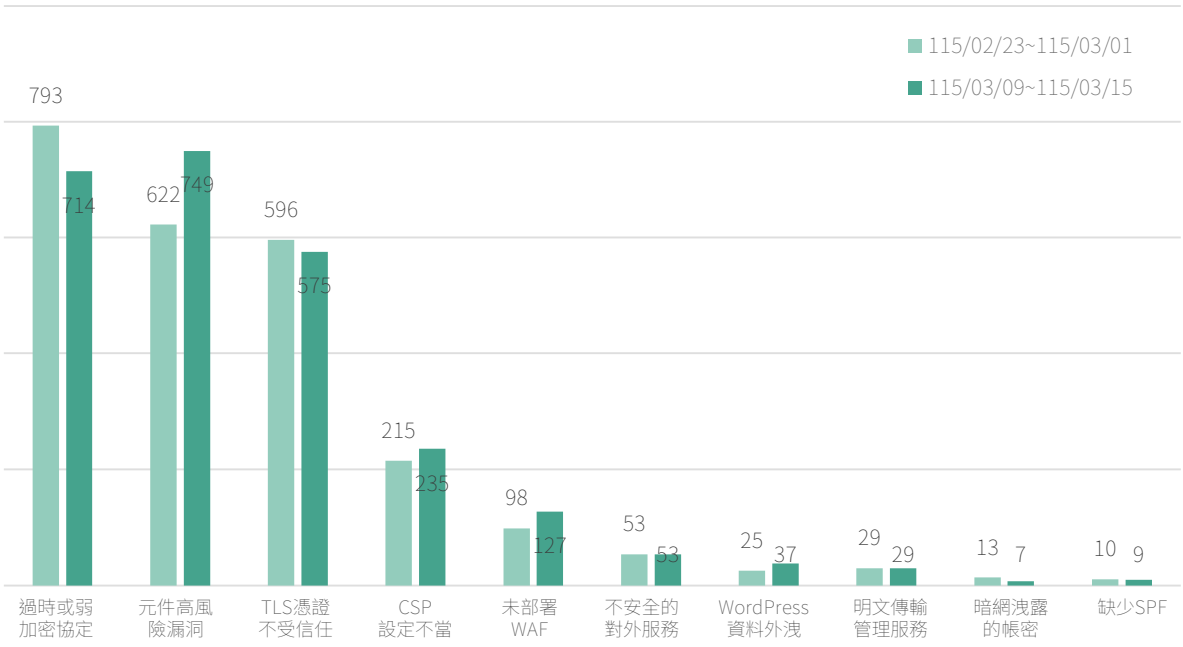


圖5| EASM檢測結果統計(前10大風險)

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WAF並導入CSP等網站安全標頭，降低跨站攻擊與惡意存取風險 ➢ 關閉不必要對外服務，管理服務改採加密通道(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 ➢ 強化資安教育與演練，提升人員對憑證、加密與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

高風險內容持續貼近日常消費情境 仍須留意假商品、假客服與健康訴求包裝

從本期高風險詐騙內容來看，整體風險樣態仍與民眾日常接觸最頻繁的消費、交易與客服互動情境高度重疊，顯示詐騙訊息持續朝生活化、常態化方向包裝，詳見圖6。這類內容往往披著促銷資訊、商品推薦、健康管理或服務通知外衣，容易使人誤認為是一般商業訊息而降低警覺。提醒民眾，面對各類網購、優惠活動、客服通知或健康相關廣告時，仍應保持查證習慣，避免在未確認資訊真偽前即進行點擊、回覆或交易。

就風險類型觀察，「產品服務」仍是本期最主要的高風險來源。相關內容多圍繞商品銷售、促銷活動、居家用品、保健美容、個人護理及日常消費場景，並常以熱銷商品、實用好物、保養調理、車用配件等主題吸引目光。其常見表述包括「台灣出貨」「線上客服」「售後服務」「限時優惠」「名額有限」「推薦使用」等，透過結合信任感與急迫感，引導民眾點擊連結、私訊詢問，甚至轉往站外交易。此類訊息版型與語言風格往往與一般商業行銷接近，外觀辨識不易，須特別提高警覺。

此外，「身分冒充」仍為本期持續可見的重要風險類型。此類內容常依附在購物、物流、退款、售後、交易確認等流程之中，假借客服、賣家、售後窗口或通知單位名義與民眾接觸，藉此延伸後續操作。從內容樣態來看，詐騙訊息經常透過「客服協助」「售後處理」「私訊通知」「補件驗證」等說法，營造正常服務流程的假象，進一步要求提供個人資料、驗證碼、帳戶資訊，或引導至不明頁面操作。提醒民眾，若遇主動聯繫要求處理退款、驗證、補件、重新付款或解除設定等情形，應立即停止互動，並改以官方網站、官方App 或正式客服管道重新查證。

至於「金融投資」雖非本期最主要的風險焦點，但仍屬高損失風險類型，不能因表面上較不突出而輕忽。此類詐騙通常以投資理財、快速獲利、專人帶單、名人推薦、群組邀請等方式吸引民眾加入，再透過看似專業的說明、操作畫面、獲利展示或話術包裝，逐步引導投入資金。即使本期整體風險重心較偏向商品與生活消費情境，對於任何標榜穩定獲利、保證收益或快速回本的資訊，仍應維持高度警覺，以免落入高損失陷阱。

綜合觀察，本期高風險詐騙內容延續既有樣態，仍以「產品服務」為主，並大量結合日常生活中的商品銷售、健康護理與消費需求進行包裝；「身分冒充」則常透過假客服、假賣

家、假售後等名義串接後續詐騙流程；「金融投資」雖非本期主軸，仍須持續防範。

整體而言，本期最值得留意的特徵，在於詐騙內容持續以「看似熟悉、實則誘導」的方式滲透日常資訊接觸場景，尤其在商品促銷、健康訴求、客服協助與生活化廣告包裝方面，具有較高迷惑性。

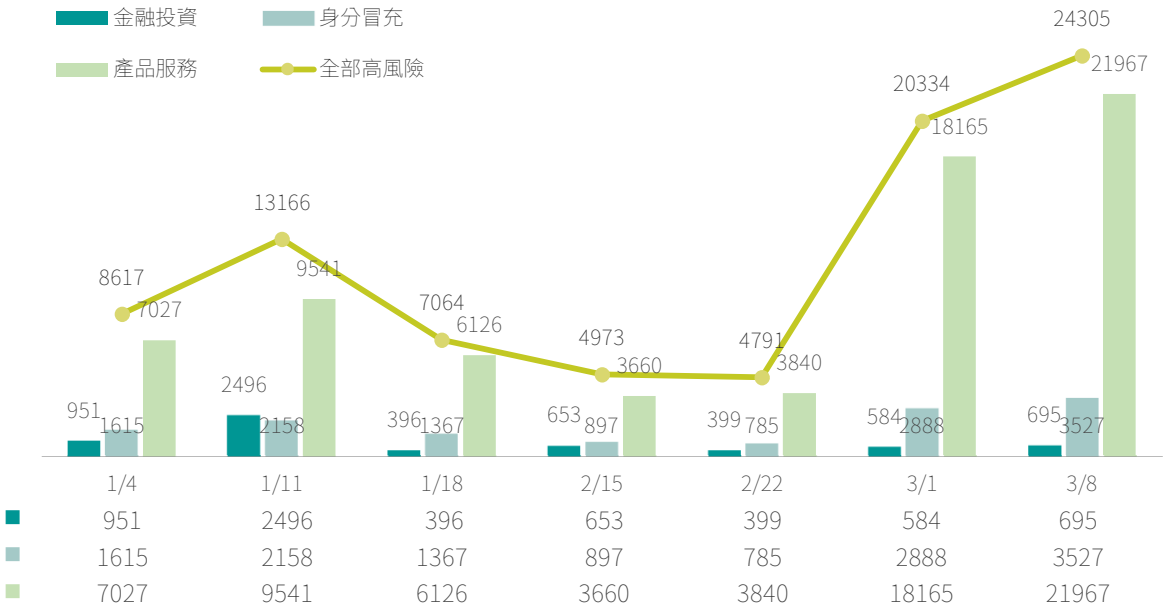


圖6 | 偵獲高風險金融投資、身分冒充、產品服務類詐騙週趨勢

高風險詐騙偵測趨勢分析與提醒

留意生活化商品廣告的誘導設計

- ✓ 面對「產品服務」相關訊息，若內容強調「限時優惠、限量名額、台灣出貨、售後保障、推薦使用、快速見效」等字眼，應提高警覺，避免在未查證前直接下單。
- ✓ 對於要求私訊洽談、改至站外交易、點擊不明連結，或要求轉往其他通訊軟體聯繫者，應視為高風險警訊；交易與付款資訊應以官方 App、官網或正式平台頁面為準。
- ✓ 宣稱效果明顯、保證見效、過度強調推薦見證、醫師背書或使用前後差異的廣告，尤其是保健、美容、修復、個人護理、居家清潔與車用品類內容，應審慎辨識其真實性。

強化客服、賣家與通知來源的查證意識

- ✓ 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、操作 ATM 或點擊補件連結，均應立即停止互動。
- ✓ 接獲與購物、出貨、退款、取消訂單或售後處理有關的通知時，不應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「客服即時回覆」「售後無憂」「可私訊快速協助」等話術，應保持警覺，避免因其看似貼心而誤信對方身分。

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，不可因話術包裝專業而輕信。
- ✓ 對於以貸款、補助、福利、快速審核或免費諮詢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，不宜僅憑截圖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、促銷包裝」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」、「推薦」、「必備」等字眼最常出現，另外也常搭配「健康」、「配方」、「優惠」、「安心」、「問題」、「台灣」、「調理」等用語，詳見圖7。從這些高頻字眼可以看出，詐騙訊息很常假裝成一般商品廣告、保健資訊，或看起來很生活化的購物貼文，利用「很好用」、「很多人推薦」、「家裡一定要有」這類說法吸引民眾注意。常見情況像是強調商品設計很貼心、效果很好、很多人都在買，或打出優惠價、限時活動等字樣，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」來包裝的商品宣傳，例如標榜「貼心設計」、「簡單好用」、「生活必備」、「人人都適用」等，讓民眾覺得商品很實用、買了馬上就用得到。這類貼文通常還會再加上「限時優惠」、「數量有限」、「現在下單更划算」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、現在買最划算的廣告時，務必要先查清楚賣家和網站來源，不要只看圖片好看、文案吸引人，就直接點連結或下單。

另外，從「推薦」、「健康」、「配方」、「調理」、「問題」等關鍵字來看，本週也有不少詐騙內容是假借健康、保養或身體調理的名義來吸引民眾。這類訊息常會說商品是「專家推薦」、「草本配方」、「改善問題」、「調理身體」、「效果很快」，甚至搭配見證分享或前後對比圖，讓人誤以為真的很有效。實際上，這類手法往往是利用民眾對健康、外觀或身體不適的在意，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，或說什麼問題都能處理的商品，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「台灣出貨」、「在地服務」、「安心購買」、「限時優惠」等，讓民眾以為賣家很可靠、交易也有保障。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」或「安心購買」就放鬆警覺，還是要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「推薦」、「必備」、「健康」、「調理」這些字眼，詳見圖7，讓商品看起來不只是便宜，而是「很多人都在用」、「現在就該買」、「買了就能改善問題」。再搭配「限量」、「熱銷」、「立即搶購」、「錯過可惜」等說法，很容易讓人在還沒查證清楚前，就急著做決定。提醒民眾，只要看到廣告一直強調效果很好、名額不多、優惠快結束，或催促趕快填資料、加好友、點外部連結時，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」、「推薦」、「必備」等吸睛字眼吸引注意，再用「健康」、「配方」、「調理」、「改善問題」這類說法增加可信度，接著用「台灣」、「安心」、「優惠」降低民眾戒心，最後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。

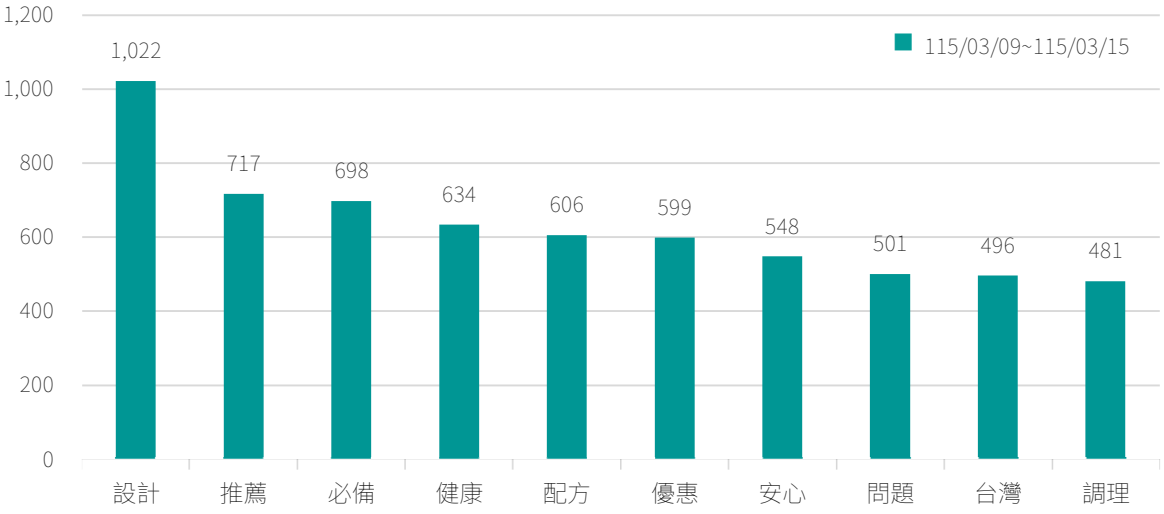


圖7 | 本週代表性詐騙關鍵字 Top 10

焦點文章

產業資安情資分享與趨勢重點

以情資驅動預防、應變與復原能力，縮短風險空窗期並降低擴散與重複受害

根據114年1、2月 TWCERT/CC 情資發送統計，以「駭侵事件」占比最高，超過七成，「漏洞情資」次之，詳見圖8。若再進一步從通報的資安事件類型分析可見，通報內容主要集中在「漏洞通報」與「產品安全」相關事件，合計接近九成，詳見圖9，顯示當前最普遍、最具擴散風險的威脅來源，仍是產品與軟體的安全漏洞，應列為優先處置重點。

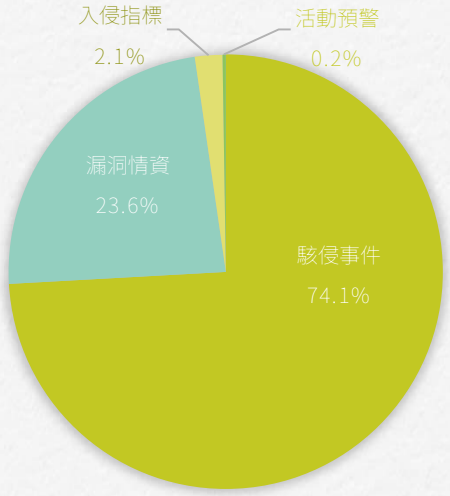


圖8 | TWCERT/CC情資發送類型

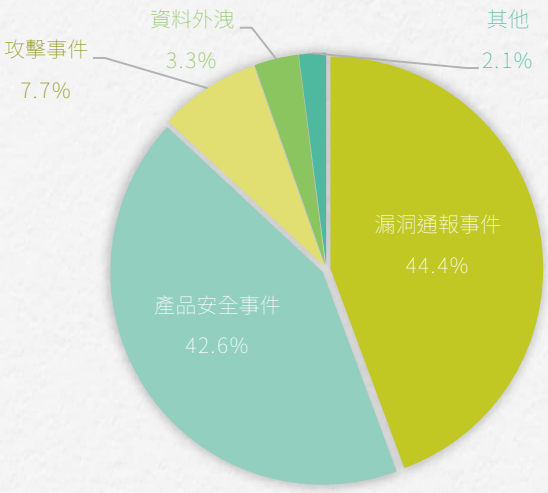


圖9 | TWCERT/CC通報資安事件類型

駭侵事件 攻擊事件告警與情資分享

「駭侵事件」為 TWCERT/CC發送占比最高的情資類型，涵蓋漏洞通報、產品安全問題、入侵攻擊、資料外洩等多種資安事件樣態。當 TWCERT/CC 透過國際情資合作、暗網監控或自動化觀測等管道，發現某網站或系統可能存在可被利用的弱點、疑似已遭未授權存取或資料外流跡象，甚至已成為攻擊行動的目標時，即使相關單位尚未察覺，亦會主動聯繫告知，協助其及早確認影響範圍、採取應變與修補措施，以降低後續擴散與損害。

焦點文章

- 資安產品漏洞，VPN 設備成為常見入侵管道。近期觀察到攻擊者頻繁鎖定 VPN 設備作為入侵跳板，原因可能是產品本身存在已知但尚未修補的安全漏洞，或是員工帳號密碼因釣魚攻擊或資料外洩而遭竊取。一旦取得 VPN 存取權，攻擊者即可進一步滲透組織內部網路。
- 漏洞通報，網站被入侵後的惡意行為。漏洞通報中常見情境是網站被植入惡意程式、出現異常頁面或不明跳轉，代表攻擊者可能已取得網站權限並用來散播惡意內容或導向外部站點。這類事件的風險在於不只影響管理端，也可能波及所有瀏覽者。

漏洞情資 高風險漏洞通知

「漏洞情資」是指軟體或硬體產品中被發現的安全缺陷。這些缺陷一旦被駭客掌握，就可能成為入侵的門戶。TWCERT/CC 持續追蹤高風險漏洞，特別是那些已經有駭客在真實攻擊中使用的漏洞，並發出通知提醒單位盡速更新修補。

- 已遭利用漏洞升溫，入侵速度持續加快。今年初，多個廣泛使用的產品漏洞相繼被列入 CISA KEV名單，代表這些弱點已被實際應用在攻擊行動中，且具有高度擴散風險。這類漏洞一旦存在於對外服務或常見端點上，往往會在短時間內被大量掃描與嘗試利用，造成「還沒察覺就已被入侵」的狀況，該類漏洞應優先視為高風險處置項目。
- 漏洞成為勒索組織利用工具。勒索組織常以漏洞做為入侵起點，把漏洞當成工具箱，透過大量掃描找出未及時修補的入口，進入內往後立刻擴散、竊取資料，再加密勒索。只要漏洞被列為高風險、或已出現被利用跡象，就應該把修補當成第一順位。

入侵指標(IoC) 快速辨識惡意行為的關鍵特徵

「入侵指標」(IoC，Indicators of Compromise)是指駭客攻擊時留下的蛛絲馬跡，例如惡意程式連線的網址、IP 位址、惡意檔案的雜湊值等。掌握這些指標，資安人員可以在自己的環境中主動比對，提早發現是否遭受相同攻擊，是威脅偵測的重要基礎。IoC 的目的在於讓單位能快速比對、封鎖與告警，縮短發現時間。

- 多元情資管道整合，共享可識別的入侵線索。TWCERT/CC 透過公私情資交換、國際合作、暗網監控與事件通報等管道，持續蒐集並彙整各區域及各領域的入侵指標，並依威脅類型整理為可直接比對、封鎖與追查的線索，多元情資管道讓入侵指標的覆蓋面更廣，使各單位取得的線索更貼近真實威脅態勢。

焦點文章

活動預警　資安攻擊活動共通性分析

「活動預警」是指 TWCERT/CC 觀察到特定攻擊手法正在擴散、或整體威脅情勢明顯升溫時，於尚未造成大規模影響前主動發布警示，提醒單位提早採取防範措施，降低受害風險。此類預警常見於駭客活動頻率升高、社交工程與假冒手法擴散，或關鍵弱點與常見系統元件出現大規模掃描與嘗試利用等情境，顯示攻擊活動正快速升溫，需及早檢視曝險面、加強監控告警並完成必要的修補或緩解措施。

- 駭客越來越會「先摸底、再出手」。在真正造成影響前，攻擊者往往先蒐集資訊並進行小規模試探，確認最容易得手的對象後再擴大行動。因此，活動預警的價值在於提前揭示這些「尚未爆發但已升溫」的訊號，提醒單位提高警戒、強化監控與宣導，並完善通報機制，把風險壓在擴大之前。

結語

從 TWCERT/CC整理的情資趨勢來看，各單位面對的資安威脅正在加速演變：攻擊者組織化程度持續提升、漏洞被利用的速度越來越快、受害對象也從大型企業延伸至各類規模的組織與個人。這意味著資安不再是「遇到再處理」的問題，而是必須把情資視為日常治理的一部分，將預警、事件、漏洞與入侵指標快速轉為可執行的防護行動。

建議單位在情資驅動下，同步強化「預防、應變、復原」三段能力。當資安攻擊活動情勢升溫時，先完成曝險面檢視、宣導與監控加強，避免在同一波攻擊中被動挨打；若接獲事件通知或出現異常行為，優先封堵入侵點並保全日誌與證據，以利追查根因與後續通報；對已遭利用的高風險漏洞立即優先修補，無法即時修補者採取替代緩解降低曝險；同時把可疑的網域、IP及檔案特徵加入封鎖或告警設定。如此才能在攻擊擴大前及早攔阻風險，並在事件發生時加速研判、有效控損與復原。

關鍵字：情資分享、企業聯防、產業資安

刊　　名　資安週報第 36 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