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
遠端存取應落實「原則禁止、例外允許」及短期授權控管

聯防監控
攻擊鏈前期活動頻繁 組織應提高警戒 防範深度滲透

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
擴大檢測範圍：100個A、B級公務機關之外部曝險分析

網路巡查高風險詐騙
網路巡查高風險詐騙-詐騙趨勢

焦點文章
組織內部流量監控的隱私與資安衡平 - 借鏡NIST SP 1800-37建議

2026.02.26
033

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

遠端存取應落實「原則禁止、例外允許」及短期授權控管

本週總計接獲3件公務機關與特定非公務機關事件通報，詳見圖1，其中僅1件為非法入侵事件，調查發現攻擊來源為網站之維護廠商IP，駭客以廠商帳號遠端登入網站主機並植入內網滲透工具，嘗試進行後續內部橫向移動與滲透行為。

鑑於供應鏈風險可能成為入侵跳板，遠端作業應遵循「原則禁止、例外允許」之資安管理原則，僅於確有業務必要時經審核後方可開放，採短天期授權與任務期間啟用機制，完成即關閉，避免長期開放存取權限。技術面上，應搭配多因子驗證、最小權限設計及存取行為監控，並透過網路區隔與來源限制，降低遠端帳號遭濫用時之影響範圍；管理面上，則應建立遠端例外申請與審核流程，明確規範開放期間、權限範圍及責任歸屬，並定期盤點與檢核遠端帳號使用情形，確保遠端維護行為均在可控範圍內，以降低供應鏈相關風險。

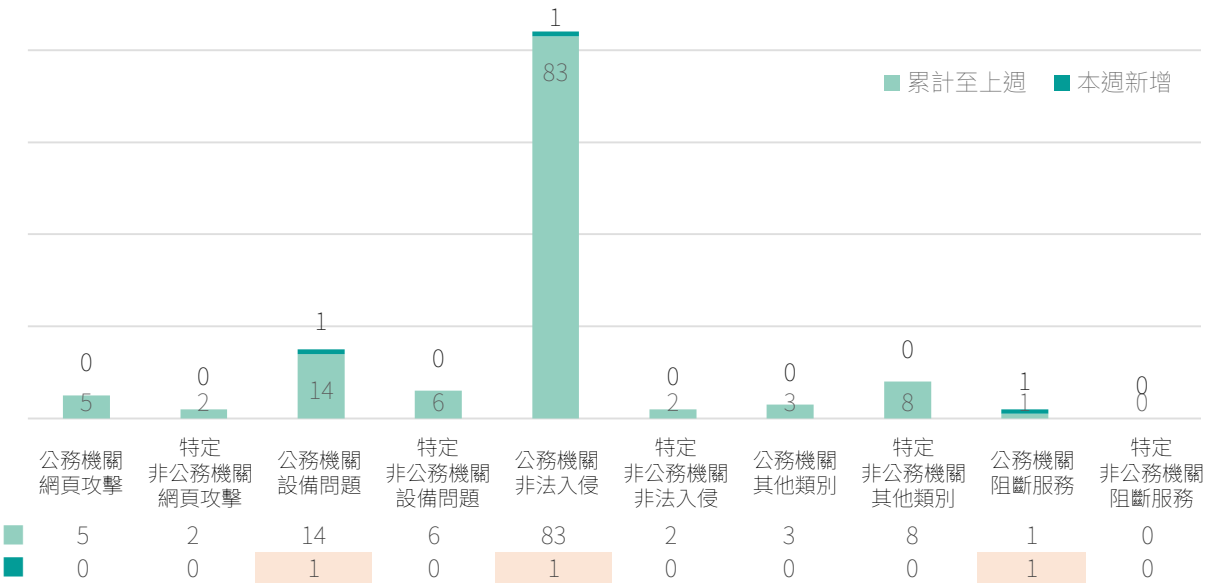

圖1 | 本週公務機關暨特定非公務機關資安事件通報概況

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和生技醫療業。

- **公司名稱：** 台達電子工業股份有限公司
- **發布時間：** 115 年 2 月 10 日
- **事件說明：** 台達電海外子公司資訊系統有異常登入企圖，調查後海外子公司部分系統受到網路攻擊，並有部分業務相關資料及員工個資外洩之風險。目前已啟動防禦程序，主動阻斷惡意連線並進行系統隔離。經評估對公司營運無重大影響，已協同資安顧問完成清查，海外子公司受影響之系統均已完成資安檢視並恢復正常運作，後續將持續提升網路與資訊基礎架構之安全控管，以確保資訊安全。

- **公司名稱：** 南光化學製藥股份有限公司
- **發布時間：** 115 年 2 月 19 日
- **事件說明：** 南光公司接獲合作廠商通知，發現公司網路系統遭不明人士入侵，部分內部文件簽呈資料等相關資訊疑似遭竊取並於暗網流傳。獲悉後已啟動資訊安全應變機制，資安團隊同步進行系統封鎖與防護作業，以防止風險擴大。經評估後，本事件對公司營運尚無重大影響，後續將持續強化資訊安全管理機制，提升系統防護層級，以確保資訊安全與營運穩定，並保障股東及利害關係人權益。

■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

攻擊鏈前期活動頻繁 組織應提高警戒 防範深度滲透

本週資安聯防監控顯示，攻擊活動主要集中於攻擊鏈的前期與中期階段，詳見圖2。其中「偵測刺探」階段佔比最高達17.2%，顯示攻擊者持續透過掃描、探測等手法尋找潛在目標與系統弱點。其次為「防禦迴避」階段佔16.7%，攻擊者常利用關閉或清除指令紀錄、濫用合法系統工具執行惡意命令等技術，企圖規避資安防護機制的偵測。第三高的「攻擊整備」階段則佔13.8%，反映攻擊者正積極準備攻擊工具與基礎設施。

值得注意的是，「惡意執行」階段亦達12.8%，顯示部分攻擊已進入實際執行惡意程式的階段。相對而言，後期的「橫向擴散」、「資訊蒐整」、「C2通訊」及「資料滲出」等階段佔比較低，均在2%以下，顯示多數攻擊尚未發展至深度滲透或資料竊取階段。整體而言，本週監控數據提醒組織應持續關注攻擊趨勢變化，特別留意攻擊活動是否由初期的偵測刺探逐步演進至更具破壞性的後期階段。

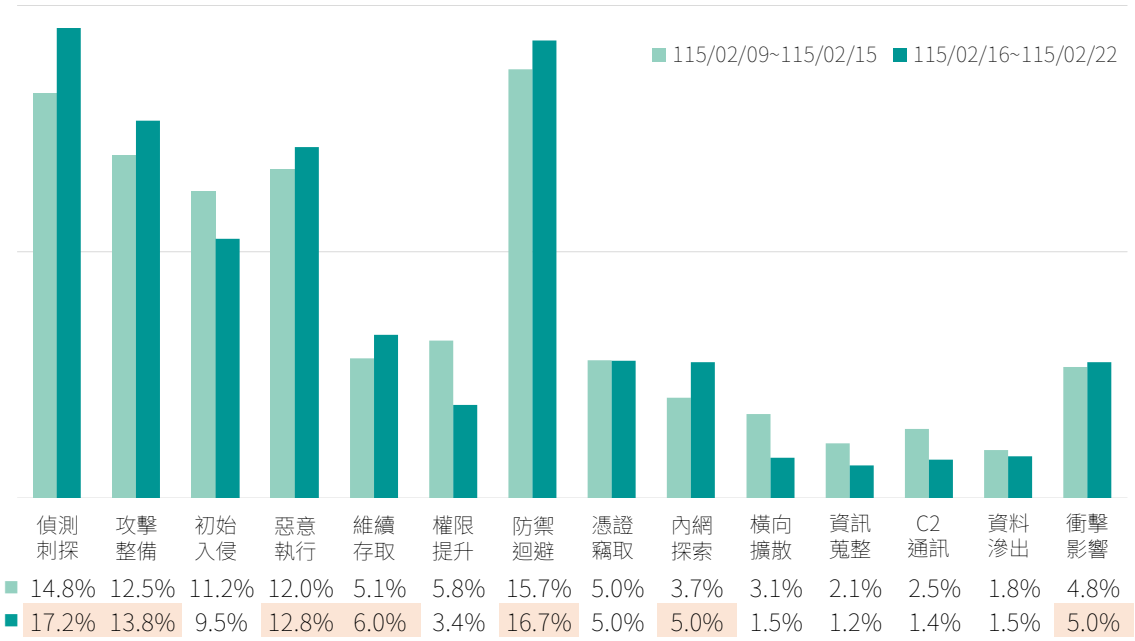

圖2 | 資安聯防監控攻擊階段統計

防護建議 建議機關採取下列防護措施：

➢ 強化偵測刺探防護
- ✓ 部署入侵偵測系統(IDS)與入侵防禦系統(IPS)，即時監控異常掃描與探測行為
- ✓ 定期檢視防火牆規則，限制非必要的對外連線與服務暴露
- ✓ 建立基線行為分析機制，快速識別異常網路流量模式

➢ 防禦迴避對策
- ✓ 導入端點偵測與回應(EDR)解決方案，強化端點層級的威脅可視性
- ✓ 落實指令紀錄稽核機制，確保系統日誌完整性且無法被輕易竄改或刪除
- ✓ 限制高風險工具(如PowerShell、WMI)的使用權限，僅授權予必要人員
- ✓ 實施特權帳號管理(PAM)，嚴格控管具備系統管理權限的帳號使用

➢ 攻擊整備階段監控
- ✓ 強化對可疑網域、IP位址及檔案雜湊值的威脅情資比對
- ✓ 監控異常的檔案下載行為與外部通訊連線
- ✓ 定期進行弱點掃描與修補作業，降低攻擊者可利用的系統漏洞

■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62.01%、「遠端控制」服務攻擊占比32.34%，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59.26%。「遠端控制」服務亦有35.40% 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3。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服務系統比例上升，主因為ConnectWise ScreenConnect使用備用路徑或通道繞過身分驗證漏洞的CVE-2024-1709，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。

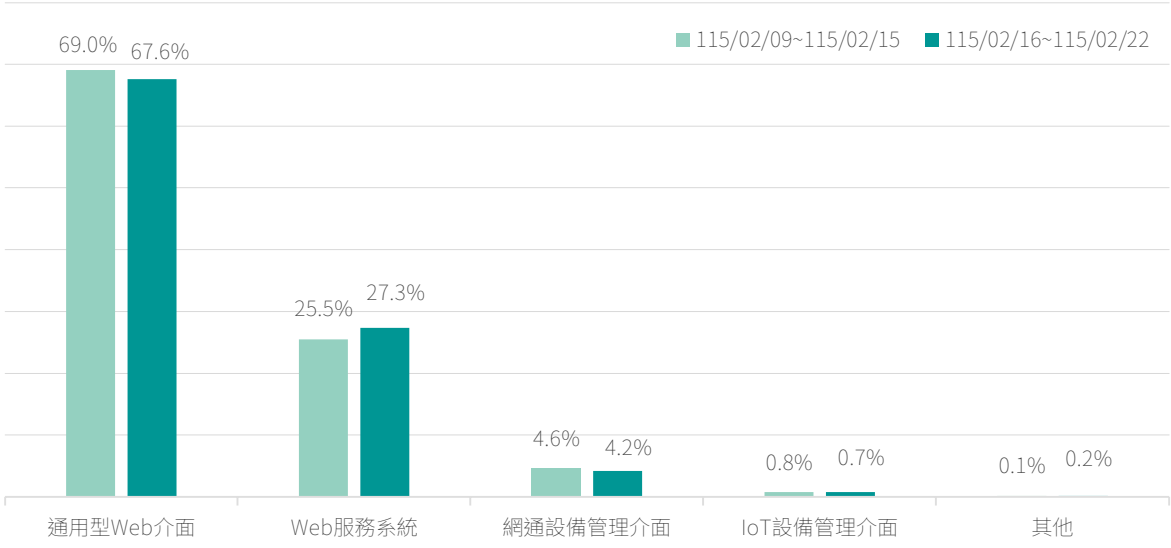

圖3 | 本週網頁應用服務之誘捕攻擊比例統計

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、程式碼注入及遠端程式碼執行漏洞，攻擊目標涵蓋Citrix NetScaler ADC、Cisco IOS XE網通設備作業系統、GeoServer開放源碼伺服器、PHP及Atlassian Confluence Server，顯示此類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-2024-36401[3]	GeoServer開放源碼伺服器	9.8
■	4	-	CVE-2024-4577[4]	PHP	9.8
■	5	-	CVE-2023-21683[5]	Atlassian Confluence Server	8.8

類型 ■越界讀取漏洞 ■特權提升 ■程式碼注入 ■遠端程式碼執行漏洞

▶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2月份安全性更新，共修補包含Azure SDK、Azure Front Door(AFD)、Windows Shell及Windows Notepad App等共72個漏洞[6]，其中包含9個CVSS達8.8分之高風險漏洞與6個已遭利用之漏洞。
- 台灣智園Tronclass存在安全漏洞(CVE-2026-2997[7])，類型為不安全之物件參照(Insecure Direct Object Reference)，已通過身分鑑別之遠端攻擊者於取得課程ID後可修改特定參數獲得課程邀請碼，藉此加入任意課程。
- Notepad++存在高風險安全漏洞(CVE-2025-15556[8])，類型為更新完整性驗證不足(Insufficient Update Integrity Verification)，未經身分鑑別之遠端攻擊者可於使用者更新Notepad++程式時，誤導安裝程式至惡意伺服器下載並執行惡意程式。
- BeyondTrust Remote Support(RS)與Privileged Remote Access(PRA)存在高風險安全漏洞(CVE-2026-1731[9])，類型為作業系統指令注入(OS Command Injection)，未經身分鑑別之遠端攻擊者可注入任意作業系統指令並於伺服器上執行。
- Dell RecoverPoint for Virtual Machines存在高風險安全漏洞(CVE-2026-22769[10])，類型為使用硬刻之帳號通行碼(Use of Hard-coded Credentials)，未經身分鑑別之遠端攻擊者可使用硬刻之帳號通行碼取得底層作業系統之root權限。

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-2024-36401
4. https://nvd.nist.gov/vuln/detail/cve-2024-4577
5. https://nvd.nist.gov/vuln/detail/cve-2023-21683
6. https://msrc.microsoft.com/update-guide/releaseNote/2026-Feb
7. https://nvd.nist.gov/vuln/detail/CVE-2026-2997
8. https://nvd.nist.gov/vuln/detail/CVE-2025-15556
9. https://www.beyondtrust.com/trust-center/security-advisories/bt26-02
10. https://www.dell.com/support/kbdoc/zh-tw/000426773/dsa-2026-079

■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

擴大檢測範圍：100個A、B級公務機關之外部曝險分析

本次針對曝險程度較高之100個A、B級公務機關進行EASM檢測，前10大風險項目累計達8,810項(包含重大與高風險)，詳見圖4。檢測結果顯示，「元件高風險漏洞」共計3,762項，為最主要的資安威脅，反映出多數單位系統系統元件老舊且未及時修補。「過時或弱加密協定」共計2,080項，「TLS憑證不受信任」共計1,460項，顯示傳輸加密安全亦為主要防護破口之一，以上三項指標合計佔總風險項目的82.9%。整體而言，受測單位普遍面臨多重風險威脅，建議立即採取修復與防護措施。

防護建議：

建議機關或關鍵基礎設施採取下列防護措施：

- 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)

建議機關或關鍵基礎設施採取下列管理措施：

- 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

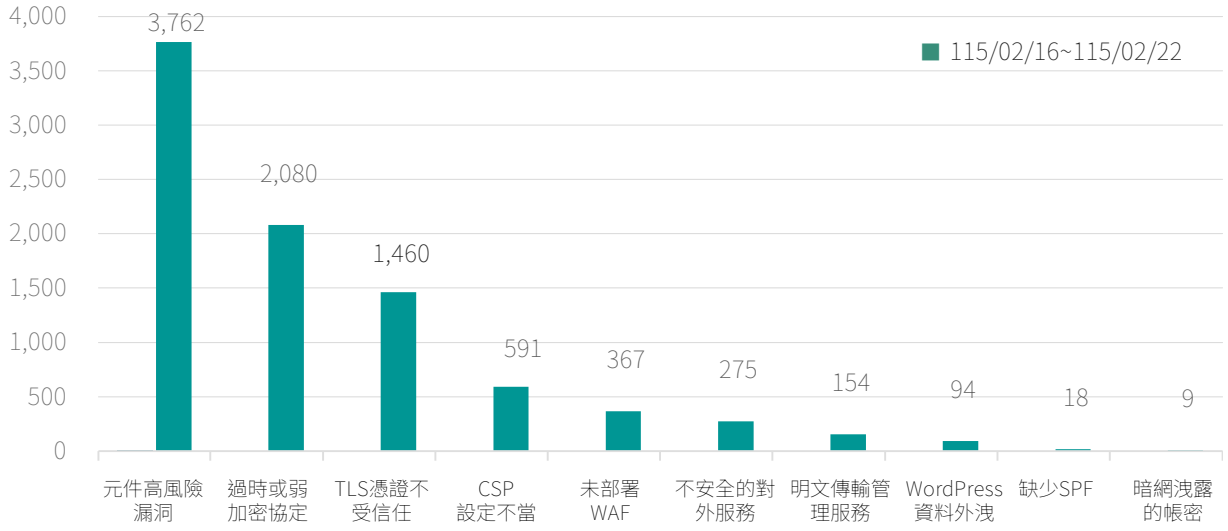

圖4| EASM檢測結果統計(前10大風險)

■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

網路巡查高風險詐騙-詐騙趨勢

本週資安週報的關鍵數據顯示，「全部高風險」通報事件數相較上週明顯下降，詳見圖5。整體偵測量自「115/01/12~115/01/18」進入「115/02/16~115/02/22」後出現一波回落。研判主要與春節假期後的上網行為變化與投放節奏調整有關，導致短期偵測量下滑，但風險並未實質消失。在各類別事件方面，「產品服務」仍是「全部高風險」中的最大宗來源。

雖然本週相較上週呈現明顯下降，但占比依舊最高，顯示與「網購交易」、「服務訂閱」相關的詐騙仍具持續性，且常見於交易與付款流程中。「身分冒充」本週同樣較上週減少，但變化幅度相對溫和。顯示以「官方客服」、「親友借款」、「機關通知」為包裝的詐騙仍維持穩定活動量，推估詐騙集團持續以低成本、高頻率的方式進行撒網式操作。「金融投資」則在本週出現較大幅度的回落，相較上週明顯減少。

以「投資理財」、「虛擬貨幣」、「穩賺不賠」為訴求的詐騙，可能在先前已完成一波集中投放，本週進入相對收斂期。整體而言，本週總通報事件數與各類別事件量皆較上週下降，但仍需持續追蹤是否出現反彈與手法變形。

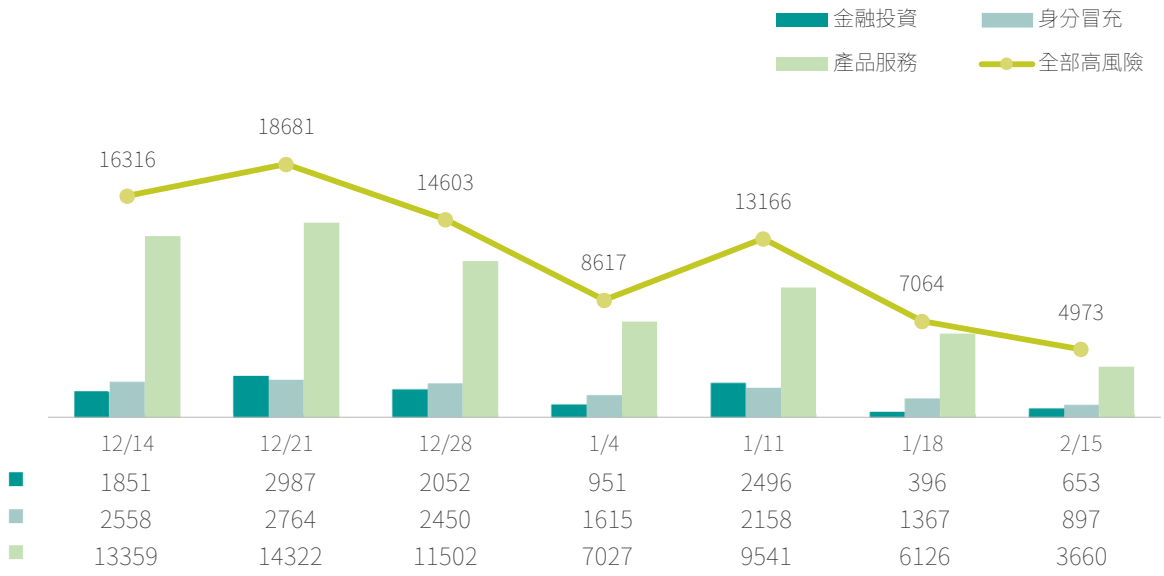

圖5 | 偵獲高風險金融投資、身分冒充、產品服務類詐騙週趨勢

高風險詐騙偵測趨勢分析與提醒

➢ **強化「產品服務」詐騙防護(網購與服務訂閱情境)**

- ✓ 針對「網購交易」與「服務訂閱」相關平台，建議企業與機關加強風險告警，例如於官網、APP 登入頁與結帳頁顯示「高風險詐騙」提醒，並特別標註「超低價」、「先匯款再出貨」、「跳轉至陌生支付頁面」等關鍵風險徵兆。
- ✓ 一般使用者應避免透過「不明連結」或「社群貼文」直接下單，優先從「官方網站」或「官方 APP」進入，並確認網址是否為「HTTPS」及網域拼字正確。
- ✓ 遇到自稱「客服」要求操作「ATM 解除分期」、「提供一次性驗證碼」、「加 LINE 處理退款」等情境時，應立即中止對話，改由「官方客服專線」或「官方 APP 內建客服」重新查證。

➢ **提升對「身分冒充」與「官方客服」詐騙的識別能力**

- ✓ 機關與企業應主動公告「不會透過電話要求提供帳號密碼、不會要求操作網銀或 ATM」等「官方政策」，並在簡訊、Email與社群貼文中反覆強調，降低民眾對假「官方客服」的信任度。
- ✓ 一般民眾接獲自稱「銀行」、「電商平台」、「政府機關」或「親友」的緊急匯款要求時，務必採取「二次驗證」原則，例如改用「通訊軟體語音通話」、「親自回撥官方電話」、「透過其他親友側證」確認真偽。
- ✓ 對於聲稱「帳戶遭凍結」、「涉及刑案需協助調查」、「需立即匯款保全資金」等高壓話術，應視為「高風險關鍵字」，第一時間拒絕提供任何個資與金融資訊，並可直接撥打「165 反詐騙專線」諮詢。

➢ **防範「金融投資」與「投資理財」詐騙**

- ✓ 建議金融機構與企業資安單位加強對「投資社群」、「投資 APP 下載連結」、「不明投資廣告」的監測與通報，並主動對員工與客戶發布「高風險投資詐騙」警示。
- ✓ 一般使用者面對標榜「穩賺不賠」、「保證獲利」、「老師帶單」、「內線消息」的「投資理財」邀約時，應一律視為高風險，避免加入不明「LINE 群組」、「Telegram 群組」或安裝來源不明的「投資 APP」。
- ✓ 投資前應透過「金管會」、「證期局」等官方管道查驗平台與業者是否具備合法牌照，並避免將資金匯入「個人帳戶」或「境外帳戶」，一旦遇到「只收 USDT 或虛擬貨幣」的投資方案，更應提高警覺。

➢ **建立長期防護機制與事件通報流程**

- ✓ 機關與企業應建立「資安事件通報機制」，將疑似「高風險詐騙」訊息(如假冒官方名義、偽造網站、釣魚簡訊)納入通報範圍，並定期彙整成「資安週報」，作為調整防護策略與教育訓練的依據。
- ✓ 建議導入「郵件與網址威脅偵測」工具，對員工收發的郵件與點擊的連結進行即時過濾與阻擋，降低因誤點釣魚連結而導致帳號外洩的風險。
- ✓ 一般使用者則可透過「啟用兩步驟驗證」、「定期更換密碼」、「分帳戶管理資金」(例如日常小額帳戶與主要資產帳戶分離)等方式，降低單一帳號遭入侵時的整體損失風險。

本週代表性詐騙關鍵字 Top 10 以「免費」、「領取」、「贈送」等誘因型字眼為主軸，並出現「訂閱」等涉及會員服務之用語，顯示詐騙訊息仍常以「贈品、免費福利、免費會員」作為入口，營造看似正當的促銷或回饋活動，進而引導民眾採取下一步行動，詳見圖6。常見情境包含「免費領取」、「免費贈送」、「訂閱免費」等說法，藉此降低戒心，後續再要求點擊連結、加入特定帳號或導向站外頁面，進行蒐集個資、誘導付款、要求匯款或綁定付款方式等操作。

本週亦可見以「慶祝」、「週年」、「成立」等字眼包裝之活動型宣傳，常以「週年慶回饋」、「成立紀念加碼」、「限時慶祝贈禮」等名目，提高可信度並吸引點閱。此類貼文易搭配「現在訂購就加贈」、「名額有限立即領取」等話術，促使民眾在未充分查證前即進入交易流程；後續可能導向不明購物頁、陌生客服窗口，或要求填寫個人資料。提醒民眾，遇到以知名品牌、周年慶或紀念活動名義提供高價贈品、加碼回饋者，務必優先至品牌官方網站或公開客服管道查證，不宜僅憑貼文內容即下單或提供資料。

此外，本週常見宣傳文字亦包含「正在」、「完全」等強化語氣之措辭，常用於營造「限時進行、立即可得」之急迫感，例如強調「正在加碼」、「完全免費」、「立即領取」等，以加速民眾決策並降低查證意願。提醒民眾，凡遇以急迫性話術催促點擊或要求立即完成資料填寫、付款設定者，均應先行暫停操作並進行來源查核，以避免在時間壓力下誤入高風險流程。

綜合本週觀察，常見手法多為先以「免費/領取/贈送」作為入口，再以「週年慶祝/成立紀念」等活動包裝提高可信度，並透過「訂閱免費/會員升級」等話術引導民眾進入站外頁面或提供敏感資訊，進一步推動付款、匯款或綁定付款方式。

提醒民眾：凡要求先點不明連結、先填寫資料或先綁定付款方式才能「領取」或「免費取得」者，請立即停止操作並先行查證；建議優先透過官方網站與公開客服管道確認真偽，以降低受騙風險。

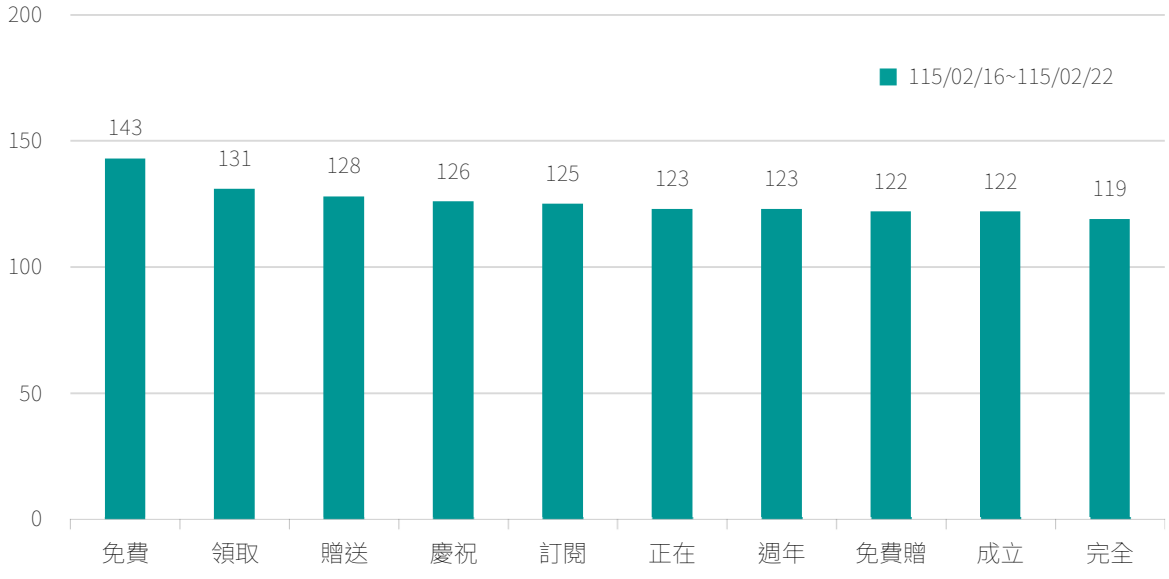

圖6 | 本週代表性詐騙關鍵字 Top 10

焦點文章

組織內部流量監控的隱私與資安衡平 - 借鏡NIST SP 1800-37建議

傳輸層安全通訊協定(TLS)已成為現代網際網路之基礎安全機制，其核心功能在於建立加密通道，確保資料於傳輸過程中之機密性與完整性。目前主流版本TLS 1.3強制啟用前向保密(forward secrecy)功能，每次建立連線(session，或稱會話)的加密金鑰都將在連線結束後失效，使得封包內容(payload)更難以被解密，資料傳輸的安全更加提升。但對於組織而言，不能解密的封包內容會導致深度封包檢視(DPI)失效，影響內部網路流量的可視性(visibility)，同樣對資安防護構成挑戰。

在此背景下，美國國家標準暨技術研究院(NIST)於2025年透過國家網路安全卓越中心(NCCoE)發布SP 1800-37[1]，示範在不修改TLS 1.3標準之前提下，如何於組織可控環境中恢復一定程度之流量可視性。不過，此類作法雖有助於偵測惡意活動，卻亦直接涉及隱私、資料最小化及攻擊面擴張等議題。本文旨在說明NIST所提出之三大技術方向及其隱私挑戰，並對照台灣政府現行制度加以檢視。

NIST SP 1800-37：在「組織內部」進行DPI之技術示範

承上所述，NIST SP 1800-37所提三大技術方向的適用範圍，限於「組織內部」具有DPI需求之情境，包含網路故障排除、效能監控、網路威脅分類與鑑識及合規稽核等場景。文件假設組織對端點、伺服器與金鑰管理具有高度控制能力，並不包含跨組織或對外服務流量之解密監控。

其提出之主要技術方向、潛在挑戰及衡平作法的建議，整理概括詳見表2。這三種技術方向的共同特徵，在於均涉及對TLS加密通道內傳輸封包的payload進行存取或還原。與僅分析封包標頭(header)不同，payload通常包含完整應用層資料，例如電子郵件內容、API請求參數或使用者輸入資訊。此類資料可能涉及個人資料、商業機密或受法律保障之通信內容。因此，相關技術之導入，不僅是資訊安全架構問題，更涉及資料最小化、目的特定性、存取授權與保存期間等隱私治理議題。NIST文件亦強調必須採取最小權限、強化金鑰控管與完整日誌紀錄，以避免解密能力被濫用。換言之，NIST SP 1800-37的核心並非鼓勵全面監控，而是在既有治理基礎下，提供有限情境之技術示範。

焦點文章

表2 | NIST SP 1800-37之技術示範

技術方向	簡要說明	相對隱私風險	潛在挑戰(隱私/資料保護/治理)	建議
被動檢查：使用有限壽命DH金鑰(Bounded-Lifetime DH Keys)	僅限在組織內部的核心系統(如資料中心)之環境實施	低	1. 如何界定組織的核心系統屬治理問題 2. 內部濫用風險，例如由例外措施轉為常態監控	針對組織核心系統的界定應明確比例原則，並為此例外措施設計授權與雙重控管機制
由伺服器匯出會話金鑰(Export of TLS session keys)	由受控伺服器將會話金鑰安全匯出至監控設備，用於被動解密	中	1. 雖屬被動解密，但仍可還原完整通訊內容 2. 金鑰集中管理將提高風險，一旦金鑰外洩，可能導致既有與歷史通訊內容被回溯還原	落實資料最小化原則，並嚴格限制解密條件與使用程序
中介設備終止TLS(TLS termination / proxy)	於組織邊界或內部閘道終止TLS，再重新加密轉送，以取得明文payload進行檢測	高	1. 常態性取得通訊內容，可能涉及通信秘密與個資處理合法性問題 2. 將明文payload集中於中介設備，可能形成大規模隱私資料的聚集點(privacy concentration risk)，使之成為高價值攻擊目標，擴大攻擊面	必須建立明確之使用目的、存取權限與保存期間限制，否則易出現超出原資安目的之資料使用情形

資料來源：參考文件自行整理

對照臺灣政府制度與實務

長期以來，我國政府機關一直是進階式持續性威脅(APT)組織的重點目標，於合法的前提下，就機關內部網路流量建立必要程度之可視性，確有其資安實務上的需求。然而，政府機關內部網路流量仍可能被認定屬於《通訊保障及監察法》所稱之「通訊」，使用者

焦點文章

對於其通訊內容，在許多情境下或將被認為仍具有合理之隱私期待；因此，不論係檢視封包標頭(header)或進一步還原封包內容(payload)，均可能涉及法律適用與權限界定之議題。相關技術措施若能更明確法源、制度依據，並設定明確之適用標準與稽核機制，將有助於確保監控行為之合法性。

另一方面，我國政府機關在實務上主要藉由政府網際服務網(GSN)作為其網際網路連線之單一窗口，並以此建置各項公務基礎服務。依GSN官方網站說明，GSN係為提升政府行政效率與便民服務而建置之整體性網路環境，以網際網路技術為基礎，形成涵蓋骨幹網路、接取網路及多項基礎與應用服務之共同基礎設施，供中央與地方各級政府機關建置行政應用及為民服務系統之用。該網路自規劃初期即以支援電子公文交換、電子郵件、行政通知與跨機關資料交換為重要功能，構成政府機關運作之基礎資訊環境。

在此脈絡下，機關對機關透過GSN的網路流量，多數是執行公務所產生，爰或可借用NIST SP 1800-37的概念進一步延伸，討論是否及如何強化流量可視性。依現行由數位發展部主管之《政府網際服務網管理規範》，主要係就網路管理、連線機制與安全維運事項加以規範，並未明確界定GSN上流量之性質或其法律定位。此外，規範雖授權數位發展部掃描與監測，惟其範圍偏向網路維運與資安事件應處，並未明確提及TLS加密內容之還原或檢視事項。

倘若未來能於相關服務條款或管理規範中，清楚說明「GSN為提供政府機關執行公務之專用網路環境」；揭示其必要之安全監控範圍(如僅檢視header，或是在特定條件下有必要解密payload)與目的；並落實授權管控，將有助於釐清公務網路流量與一般私人通訊之區別，確保合法範圍內各項監控任務之執行，使資安防護與法律保障並行發展；這也與NIST SP 1800-37建議的「預先通知可視性政策」(out-of-band notification)不謀而合。

[1] NIST, NIST SP 1800-37 Addressing Visibility Challenges with TLS 1.3 within the Enterprise: High-Level Document Share to Facebook Share to X Share to LinkedIn, available at: https://csrc.nist.gov/pubs/sp/1800/37/final.

關鍵字：NIST SP 1800-37、TLS 1.3、DPI、流量監控、個資保護

刊　　名　資安週報第 33 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