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
落實預設帳密變更及管理介面存取限制 有助於降低設備受駭風險

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
TLS憑證與弱加密風險明顯改善 惟元件漏洞仍為主要曝險來源

焦點文章
115年第1季政府領域資安事件趨勢研析

2026.04.30
042

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

落實預設帳密變更及管理介面存取限制 有助於降低設備受駭風險

本週總計接獲27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。通報件數較上週增加，主要係因115年網路攻防演練開始執行所致，其中發現多個機關監視器管理介面仍使用預設帳號密碼，遭攻擊手成功登入。

監視器等網通或 IoT 設備之預設密碼，常可透過搜尋設備型號於網路上取得，一旦管理介面對外暴露，即可能成為攻擊者優先嘗試之目標。建議各機關應清查監視器及相關設備之帳號密碼設定，落實變更預設帳密、限制管理介面存取來源，並關閉不必要之對外存取，以降低遭入侵風險。

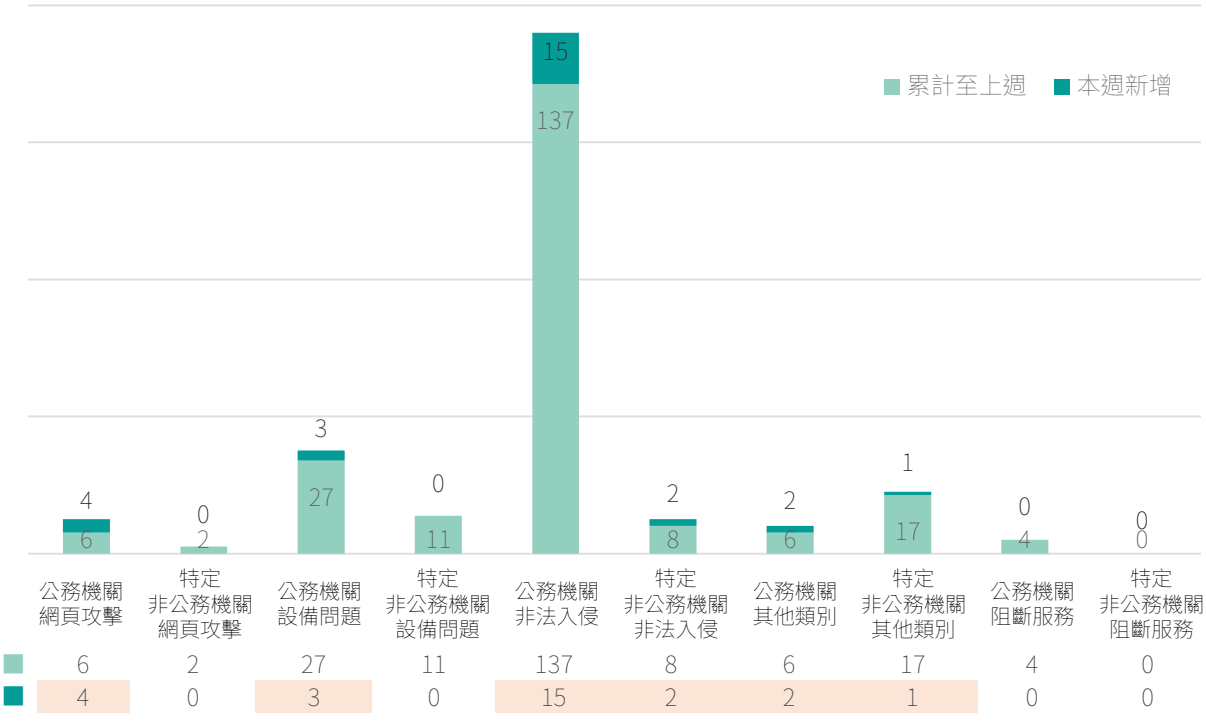

圖1 | 本週公務機關暨特定非公務機關資安事件通報概況

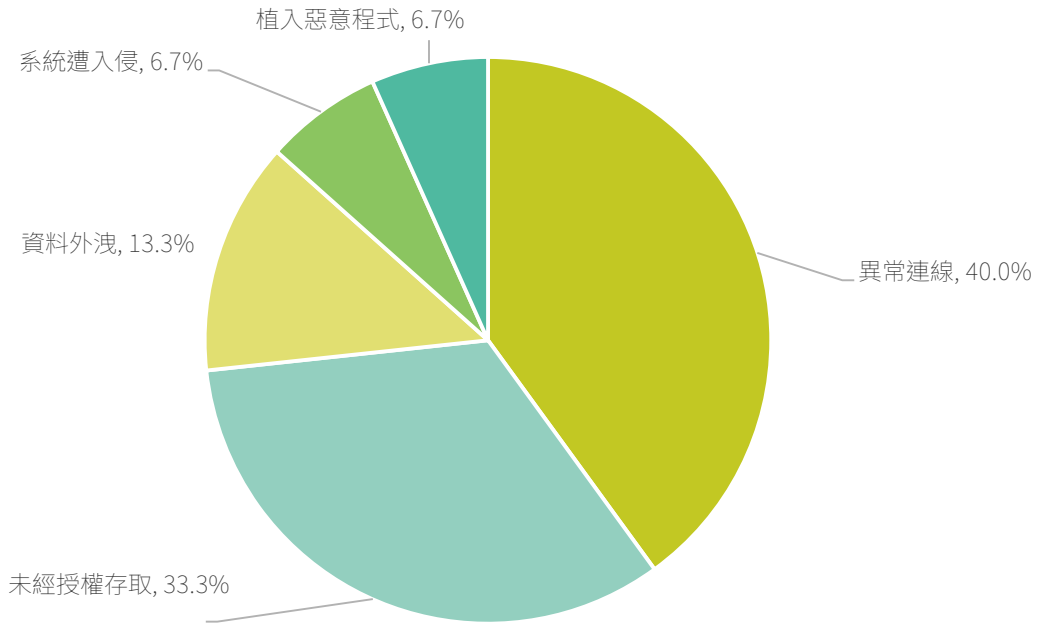

圖2 | 本週公務機關非法入侵事件類型占比

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
➢ 攻擊者利用預設帳密登入控制監視設備 ➢ 管理介面外曝遭掃描入侵取得設備控制	➢ 全面清查設備帳密設定，確實變更預設帳號密碼降低風險 ➢ 限制管理介面存取來源，避免設備直接暴露於公開網路環境 ➢ 關閉不必要對外服務與連接埠，降低被掃描與攻擊機會 ➢ 建立設備資產盤點與定期檢查機制，確保設定符合安全基準

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、生技醫療業。

■ 公司名稱	維熹科技股份有限公司
■ 發布時間	115年4月20日
■ 事件說明	維熹公司資訊系統遭受駭客網路攻擊，立即啟動相關防禦機制及復原作業，目前沒有個資、機密或重要文件資料外洩等情事發生，對公司營運無重大影響。後續將持續密集監控，並強化網路與資訊基礎架構之控管，以確保資訊系統安全。
■ 公司名稱	台寶生醫股份有限公司
■ 發布時間	115年4月26日
■ 事件說明	台寶生醫公司發現部分資訊系統遭駭客網路攻擊，資訊部門已全面啟動相關防禦機制與復原作業，同時與外部資安公司技術專家協同處理。目前對所有資訊系統及檔案全面徹底掃描檢查，高標準確認資訊安全後，以日常備份資料復原運作。初步評估對公司運作無重大影響，後續將持續加強資訊安全監控與防禦機制，提升網路與資訊基礎架構之安全管控，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15.1%，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12.8%，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能力與手段。此階段為攻擊鏈的起點，攻擊者透過各種方式取得系統初始存取權限。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。攻擊者多半利用未修補的公開服務漏洞直接入侵系統，或透過預設帳號與弱密碼組合，存取管理不當的服務資源；部分情境中，亦觀察到攻擊者利用既有本機帳號進行登入，以降低觸發告警的風險。此類行為通常不依賴使用者互動，著重於系統弱點與帳號管理缺失，具備高成功率與隱蔽性。建議定期進行對外系統弱點掃描與修補、強化帳號與驗證機制管理，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。

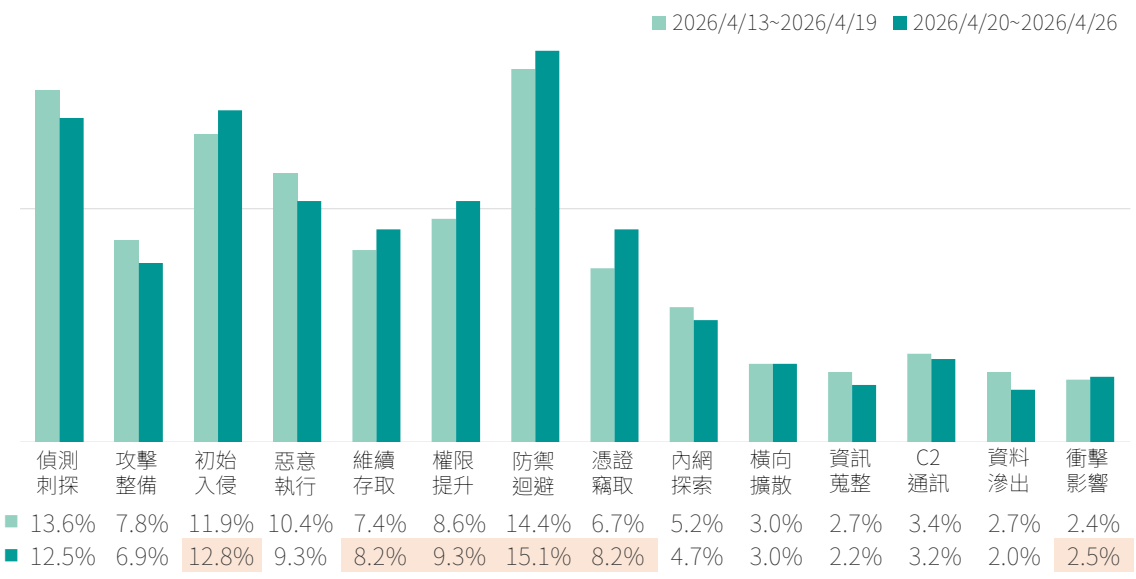

圖3 | 資安聯防監控攻擊階段統計

防護建議 建議機關採取下列防護措施：

防禦迴避（Defense Evasion）

- 強化端點防護與行為監控
- 落實指令紀錄與日誌稽核
- 限制高風險系統工具使用
- 加強特權帳號與權限控管

初始入侵（Initial Access）

- 定期進行弱點掃描與修補
- 強化帳號驗證與密碼政策
- 管控預設帳號與弱密碼
- 導入異常登入行為監控

■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74.28%、「遠端控制」服務攻擊占比21.62%，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73.05%。「遠端控制」服務亦有23.60% 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。

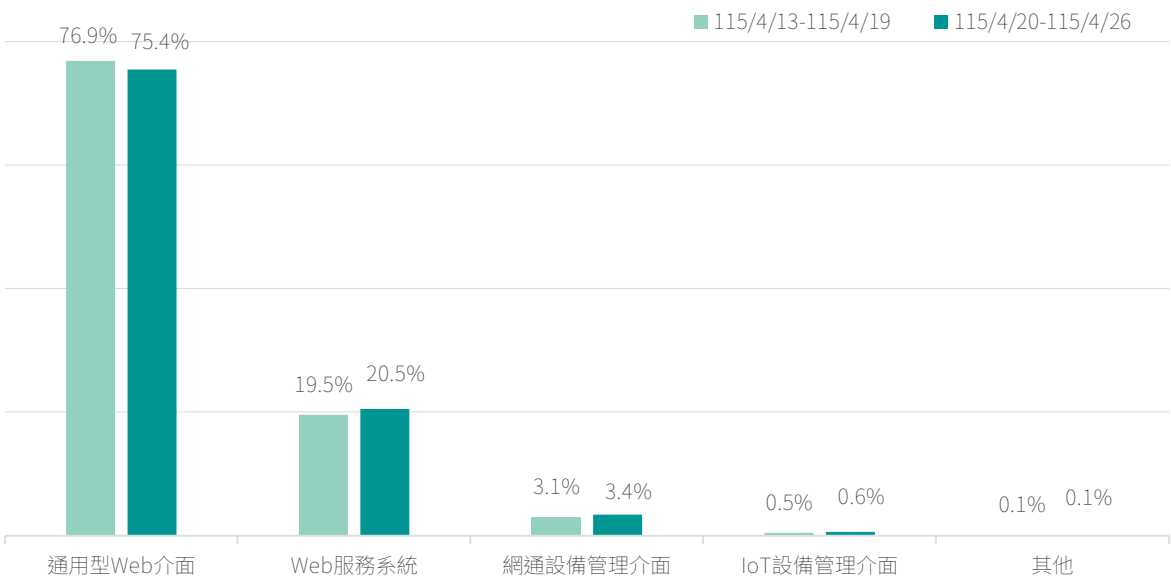

圖4 |本週網頁應用介面之誘捕攻擊比例統計

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及目錄遍歷漏洞，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、知識管理與團隊協作系統及VPN 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-2024-4577[2]	PHP	9.8
■	3	-	CVE-2024-21683[3]	Atlassian Confluence Server	8.8
■	4	⬆1	CVE-2024-24919[4]	Check Point VPN Gateway	8.6
■	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 ■命令注入漏洞

▶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：

- 杜浦數位安全ThreatSonar Anti-Ransomware存在高風險安全漏洞(CVE-2026-5967[6])，類型為權限提升(Privilege Escalation)，已通過身分鑑別且具shell操作權限之遠端攻擊者可注入作業系統指令並以root權限執行。
- 桓基科技iSherlock存在高風險安全漏洞(CVE-2026-6349[7])，類型為作業系統指令注入(OS Command Injection)，未經身分鑑別之本機端攻擊者可注入任意作業系統指令並於伺服器上執行。

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-2024-21683
4. https://nvd.nist.gov/vuln/detail/cve-2024-24919
5. https://nvd.nist.gov/vuln/detail/cve-2024-21887
6. https://nvd.nist.gov/vuln/detail/CVE-2026-5967
7. https://nvd.nist.gov/vuln/detail/CVE-2026-6349

■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憑證與弱加密風險明顯改善 惟元件漏洞仍為主要曝險來源

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1,462項，詳見圖5，較上期1,849項減少387項，降幅約20.9%。其中，「元件高風險漏洞」以693項居首，「過時或弱加密協定」256項次之，「CSP設定不當」240項排名第三；「TLS憑證不受信任」則降至60項，排名由上期第三降至第五。前三項合計1,189項，占前10大風險項目總數約81.3%，顯示目前外部曝險風險仍集中於元件漏洞、加密通訊及網站安全設定等議題，惟整體曝險數量已較上期明顯下降。

進一步分析主要風險項目變化情形，「元件高風險漏洞」較上期微增2.5%，顯示元件漏洞仍為後續優先修補重點。相較之下，「TLS憑證不受信任」較上期大幅下降77.0%，「過時或弱加密協定」亦下降38.5%，顯示憑證管理及加密協定設定已有明顯改善。另「CSP設定不當」僅微幅上升0.8%，整體變化有限；「未部署WAF」則下降23.3%，顯示部分對外網站應用層防護已有改善，惟網站安全設定與攻擊防護能力仍須持續強化。

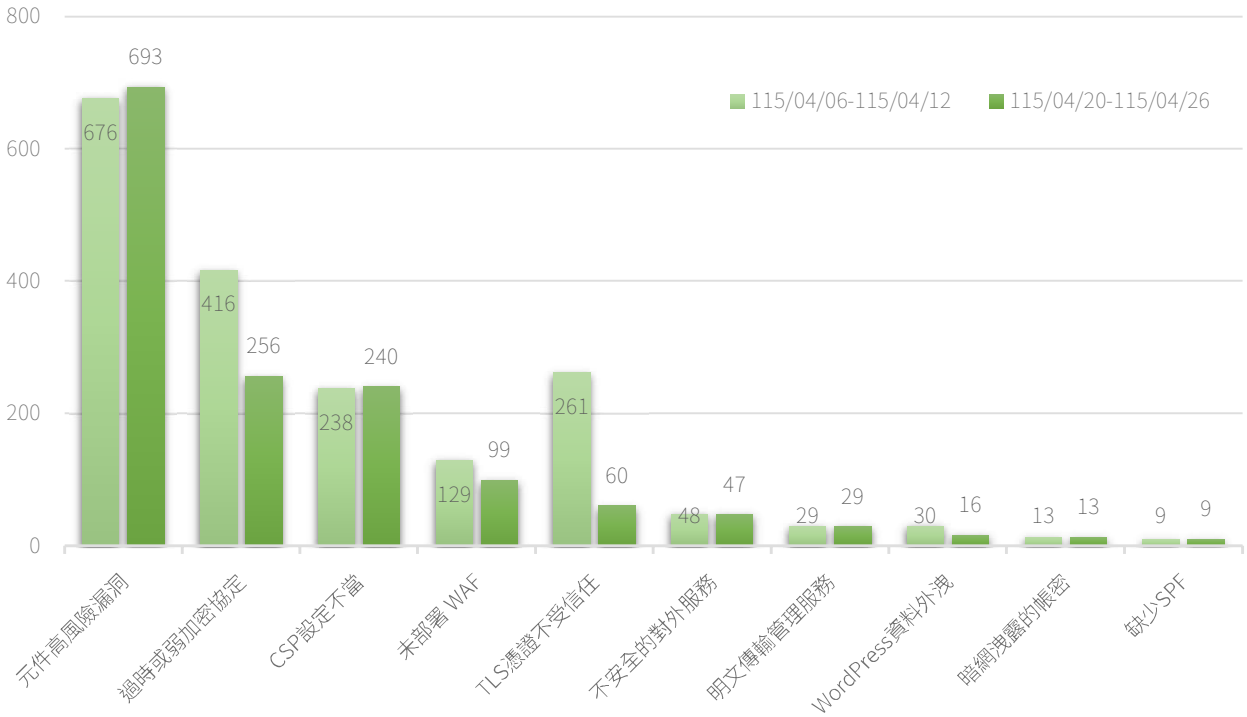

圖5 | EASM檢測結果統計(前10大風險)

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TLS憑證，全面啟用TLS1.2以上版本協定，停用未加密、舊版協定及弱加密套件 ➢ 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、複測與驗證機制，確認已通報風險完成改善並持續追蹤未結案件 ➢ 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、網站安全標頭及對外服務設定之安全意識

焦點文章

115年第1季政府領域資安事件趨勢研析

本季資安事件顯示，風險仍主要集中於使用者行為、已知系統弱點及廠商維運管理落差

115年第1季資安事件統計顯示，詳見圖6，本季可識別之資安事件原因，主要集中於使用者行為與系統／軟體弱點，另亦可見部分事件與廠商維運管理問題有關。整體而言，相關風險多屬既有且可辨識之類型，顯示當前資安事件並非全然來自新興攻擊，反映當前仍舊以弱點利用、供應鏈攻擊及使用者資安意識薄弱為主要攻擊趨勢；顯示出現有且已知防護策略需充分落實以因應現有威脅。

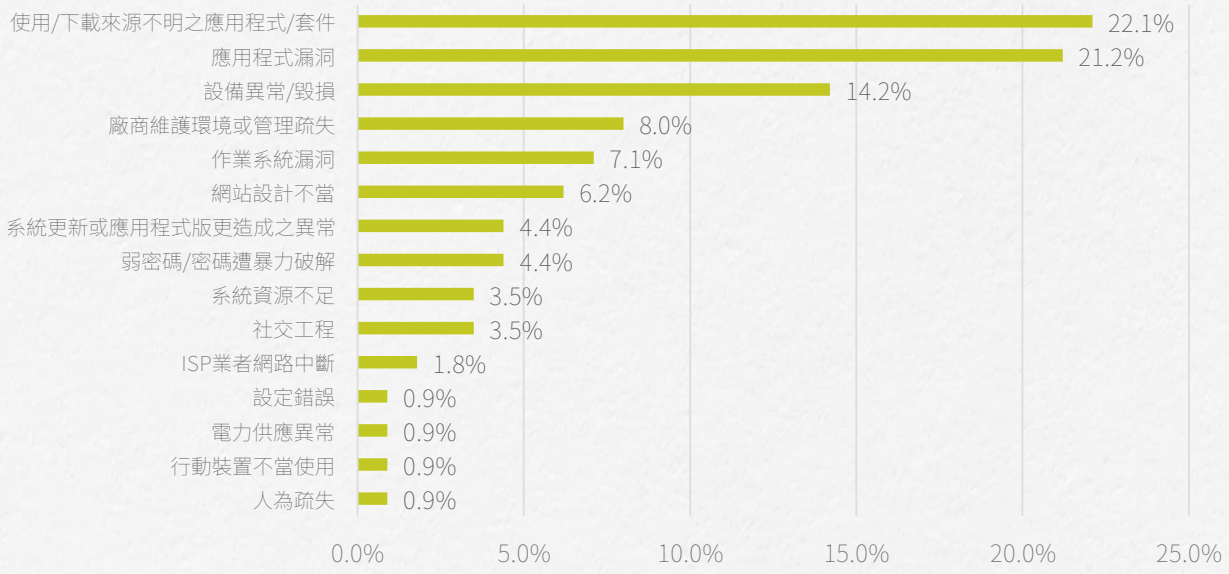

圖6 | 115年第1季資安事件統計

一、使用者行為仍是主要入侵入口

本季持續發生因使用或下載來源不明之應用程式／套件而受駭之情形，包括偽冒 LINE與遊戲平台等軟體。此類事件多非利用系統漏洞，而是透過使用者下載、安裝或執行不明程式形成入侵機會，顯示端點使用行為仍是重要風險來源。若缺乏應用程式來源控管、下載行為監控及端點可視性，相關事件將持續反覆發生。

焦點文章

二、已知弱點未修補，持續成為攻擊目標

系統／軟體弱點仍為本季重要事件原因，例如 CVE-2021-22005、CVE-2019-9193、CVE-2024-4577 等已知漏洞，攻擊者得以利用既有公開資訊或工具進行攻擊，均反映部分系統仍存在未修補或未納入持續管理之情形。此類風險多具可預期性，重點在於弱點管理、資產盤點與修補追蹤是否落實。

三、廠商維運管理不當，成為間接風險來源

部分事件源於廠商環境安全性不足、維運作業管理不當或遠端存取控管不足。相關情境包括廠商自身環境遭入侵後，被作為跳板攻擊服務機關，資安風險已不僅侷限於機關自身系統環境，委外廠商之安全管理能力與遠端維運作業，同樣會直接影響整體防護強度。若未將維護環境、帳號權限、連線來源及操作紀錄納入管理範圍，相關風險將持續存在。

綜合本季事件觀察可知，當前資安事件之成因雖形式多樣，但其核心仍可歸納為三項重點：一是使用者對不明軟體或檔案之操作行為；二是已知系統／軟體弱點未被即時修補；三是維運與委外管理機制存在落差。此一趨勢顯示，資安防護應由單純關注「是否遭受攻擊」，進一步回到「哪些既有風險未被有效管理」之角度思考。未來仍應持續強化使用者行為控管、落實弱點管理與修補機制，並提升廠商維運與遠端存取之安全要求，以降低資安事件發生之可能性，並強化整體組織之資安韌性。

關鍵字：使用者行為、系統弱點、廠商維運

刊　　名　資安週報第 42 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