國家資通安全研究院
National Institute of Cyber Security

資安週報

Cyber Security Weekly Newsletter

2026.08.27
059

資安儀表板

外部曝險分析、重大漏洞、實兵演練、聯防監控、蜜罐誘捕、事件通報及網路巡查高風險詐騙等七類量化指標

■ 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

整體曝險風險呈下降趨勢 未部署WAF及CSP設定不當風險仍呈上升

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9,040項。其中，「元件高風險漏洞」以3,428項居首，「過時或弱加密協定」1,811項次之，「TLS憑證不受信任」1,536項位居第三。前三項合計6,775項，占前10大風險項目總數約74.9%，顯示目前外部曝險風險仍高度集中於元件漏洞、加密協定及憑證管理等議題。相較上期9,302項，本期整體風險數量減少262項，降幅約2.8%，詳見圖1。

進一步分析主要風險變化情形，「元件高風險漏洞」仍為最大宗風險，數量由上期3,632項減至本期3,428項，降幅約5.6%。其中，Apache HTTP Server相關弱點(CVE-2024-38475)仍為主要風險來源，該弱點可能造成原始碼洩漏或程式碼執行風險，建議升級至2.4.60以上之已修補版本。本期另檢測出Drupal所使用之PEAR Archive_Tar函式庫相關弱點(CVE-2020-36193)，可能導致目錄遍歷風險；並發現Apache Tomcat之AJP(Apache JServ Protocol)相關弱點(CVE-2020-1938)，攻擊者可能透過可存取之AJP服務讀取Web應用程式內任意檔案，特定情況下甚至可能導致遠端程式碼執行。此外，本期觀察到Drupal所使用之Archive_Tar函式庫相關弱點(CVE-2020-28949)數量較上期減少，顯示部分機關已逐步完成相關弱點改善。「過時或弱加密協定」由1,898項減至1,811項，降幅約4.6%；「TLS憑證不受信任」由1,580項減至1,536項，降幅約2.8%。另「未部署WAF」由725項增至799項，增幅約10.2%；「CSP設定不當」由980項增至1019項，增幅約4.0%。

整體而言，本期外部曝險風險呈下降趨勢，惟「未部署WAF」及「CSP設定不當」呈現上升，顯示網站應用程式防護及安全標頭設定仍有改善空間，建議持續強化WAF部署及CSP設定，以降低相關曝險風險。

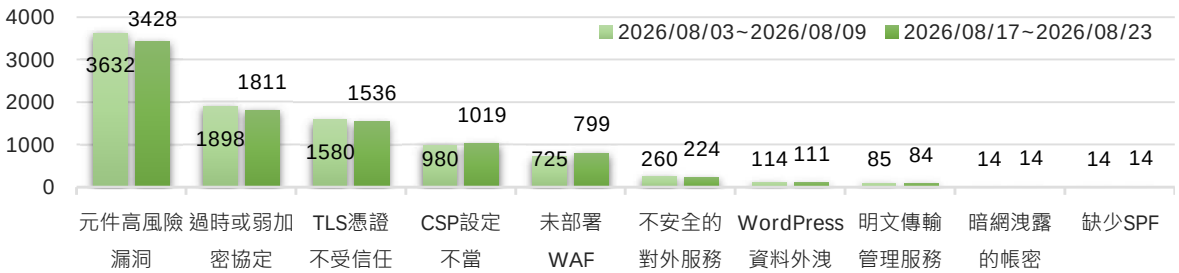

圖1 | EASM檢測結果統計(前10大風險)

防護建議

建議受測單位採取下列防護措施	建議受測單位採取下列管理措施
➢ 優先修補對外服務所使用元件之高風險漏洞，並依原廠安全公告更新至已修補版本；如短期內無法完成升級，應採取WAF、虛擬修補、來源存取限制或網路區隔等補償性措施，以降低漏洞遭利用之風險 ➢ 依據IETF RFC 10015，檢視TLS 1.2所使用之金鑰交換機制，停用較舊或安全性較低之方式，並優先採用ECDHE等具前向保密性之安全機制，以強化加密通訊安全 ➢ 強化TLS憑證管理，定期檢視憑證有效期限、信任鏈及憑證狀態，並建立到期通知及自動續期機制，避免因憑證失效造成服務異常或安全風險 ➢ 定期檢視網站CSP及WAF等防護設定，並依系統功能及實際業務需求調整安全政策，以降低跨網站腳本、惡意請求及其他Web攻擊風險	➢ 建立並定期維護對外資產清冊，納管IP、網域、系統元件及憑證等資訊，以掌握各項資產之用途、版本及使用情形 ➢ 建立高風險漏洞之修補、追蹤及複測機制，依漏洞嚴重程度訂定修補期限，並於完成修補後進行複測，確認改善措施有效落實 ➢ 定期盤點系統所使用之軟體及第三方元件版本，持續追蹤原廠安全公告及CVE弱點資訊，並適時進行版本更新，降低使用已停止支援或存在已知弱點元件之風險 ➢ 將漏洞修補、憑證更新、安全設定調整及後續複測等要求納入委外維運管理，明確訂定處理時限、責任分工及追蹤方式，以確保各項改善措施確實執行

■重大漏洞

近一週本院研究人員發現以下重大漏洞資訊，建議組織內部進行檢查與修補

Fortinet與SonicWall高風險漏洞應盡速修補

- Fortinet FortiWeb 存在不當驗證(Improper Authentication)漏洞(CVE-2026-26035)[1]，當設備啟用特定非預設之遠端RADIUS類型管理者身分鑑別組態時，未經身分鑑別之遠端攻擊者可使用任意使用者名稱與通行碼登入FortiWeb之圖形管理介面(GUI)或命令列介面(CLI)，進而取得管理者權限並控制受影響設備。

- SonicWall GMS存在2項高風險安全漏洞(CVE-2026-66145與CVE-2026-66147)[2]，類型均為程式碼注入(Code Injection)。

  - CVE-2026-66145：未經身分鑑別之遠端攻擊者可藉由zipslip讀取機敏檔案與寫入任意檔案，進而執行任意程式碼。

  - CVE-2026-66147：未經身分鑑別之遠端攻擊者可藉由特製請求注入系統指令，進而執行任意程式碼。

1. https://fortiguard.fortinet.com/psirt/FG-IR-26-158
2. https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2026-0011

■實兵演練

實兵演練係模擬真實攻擊情境，檢驗資通系統弱點、防護能力及應變機制，以提升整體資安防禦韌性

實兵演練揭露檔案存取控管失效 致公開圖片遭未授權替換

本年資通系統實兵演練針對政府機關與關鍵基礎設施提供者，於擇定時間進行演練，至8/21止已累計289筆攻擊紀錄，本週新增弱點數量共20筆，分別為「軟體供應鏈失效」6筆、「無效的存取控管」4筆、「注入攻擊」4筆、「驗證機制失效」4筆及「不安全的組態設定」2筆，詳見圖2。

本週演練發現，衝擊性較高之弱點為「無效的存取控管」。攻擊者透過Dirb工具掃描目標網站，發現「/ckeditor」路徑，進一步存取「/ckfinder.html」檔案管理功能。攻擊者於未經授權之情況下，成功上傳檔案至系統，並透過重新命名方式，置換網站圖片。顯示系統未妥善限制檔案管理功能路徑之存取權限，導致未經授權使用者可異動供民眾瀏覽之檔案與圖片，造成網站內容遭置換之風險。

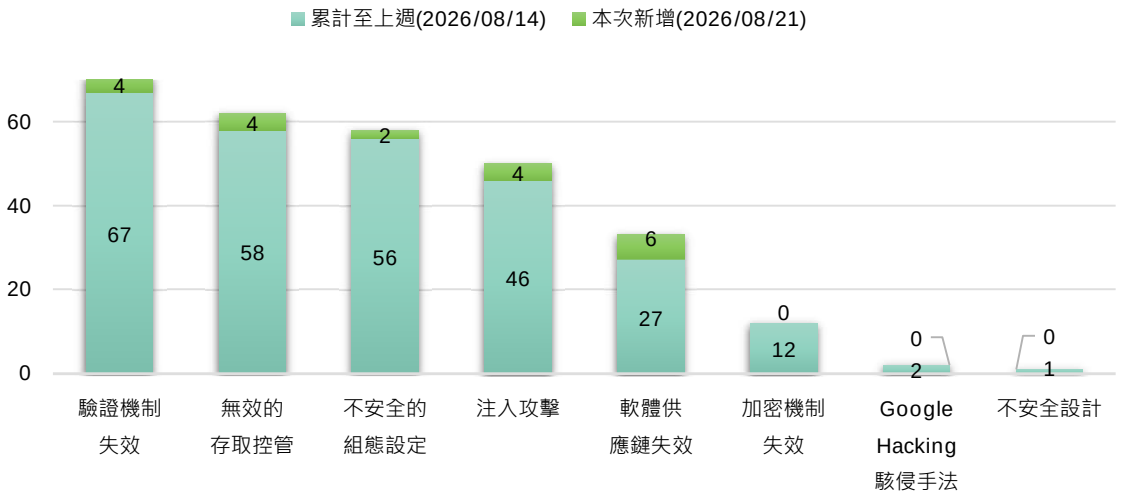

圖2 | 網路攻防演練資通系統實兵演練統計

建議機關及關鍵基礎設施提供者，採取下列防護措施

- 應針對檔案管理功能落實身分驗證與存取權限控管，避免攻擊者透過直接存取特定URL繞過前端限制並操作管理功能
- 應依使用者角色與功能需求設定檔案管理權限，避免因管理功能遭濫用而影響其他網站資源或系統檔案
- 針對網站重要圖片及靜態資源建立檔案完整性監控與異常告警機制，以利即時發現未授權之網站內容竄改行為

■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 偵測刺探仍具威脅

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。

「偵測刺探」事件本週占比為13%，為本週占比次高的攻擊階段，顯示攻擊者持續加強對目標環境的偵查與資訊蒐集活動，以提升後續攻擊行動的成功率。觀察到的主要手法包括主動式掃描、憑證資訊蒐集、以及IP 區段掃描。攻擊者透過自動化工具對外部網段與公開服務進行大規模探測，蒐集系統架構、開放埠與服務資訊，同時搜尋與帳號憑證相關的公開資料或外洩資訊，作為後續登入嘗試與目標鎖定的依據。部分活動呈現由廣泛掃描逐步聚焦特定系統與帳號的特徵，顯示其偵查行為具備明確的攻擊目標與規劃。此類行為雖多屬攻擊前期準備階段，但其蒐集成果往往成為後續入侵與橫向移動的重要基礎。

建議組織加強監控異常掃描流量與帳號探測行為，定期盤點對外暴露資產，並結合威脅情資分析可疑來源，以提前發現潛在攻擊準備活動並採取防禦措施。

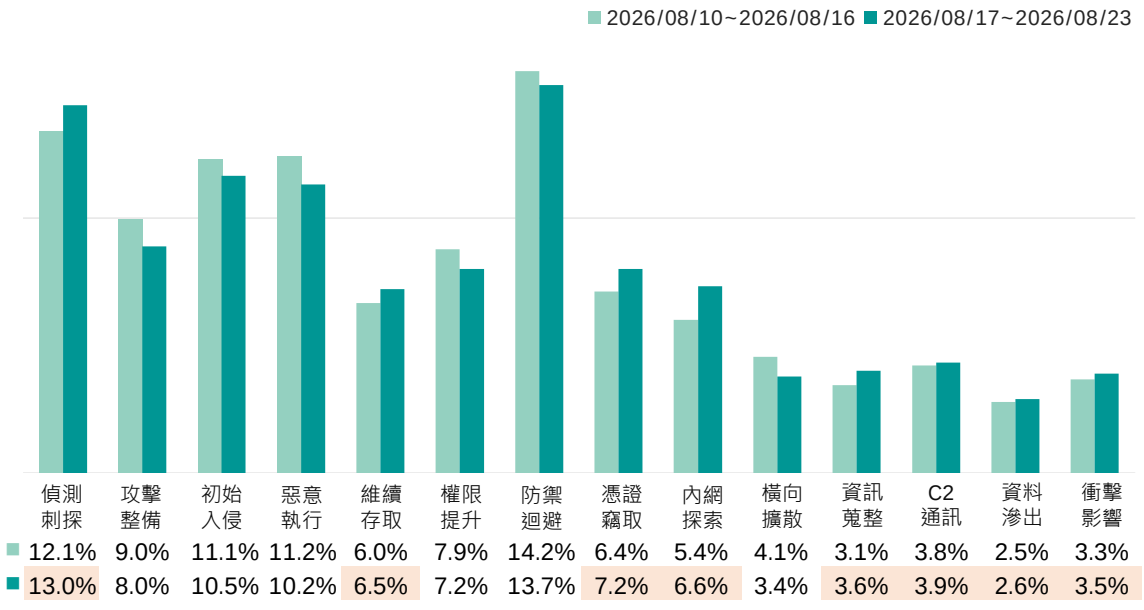

圖3 | 資安聯防監控攻擊階段統計

防護建議

建議機關採取下列防護措施

防禦迴避(Defense Evasion)

- 強化端點防護與惡意行為偵測機制
- 完整保留並集中管理指令及系統操作紀錄，避免遭竄改或刪除
- 限制高風險系統工具與合法工具遭濫用
- 落實特權帳號權限控管及異常操作監控

偵測刺探(Reconnaissance)

- 監控異常掃描、IP區段探測及大量連線行為
- 定期盤點對外暴露的系統、服務及開放埠，降低攻擊面
- 加強帳號與憑證資訊保護，掌握可能的外洩情形
- 結合威脅情資辨識可疑來源，及早封鎖或限制惡意探測活動

■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

AI應用套件及企業級端點與安全管理系統成攻擊熱點

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77.35%、「遠端控制」服務攻擊占比19.42%，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76.86%。「遠端控制」服務亦有19.49%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。而網通設備管理介面比例上升主因為NetScaler ADC & Gateway存在越界讀取漏洞之CVE-2025-5777，遭攻擊次數上升導致。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。

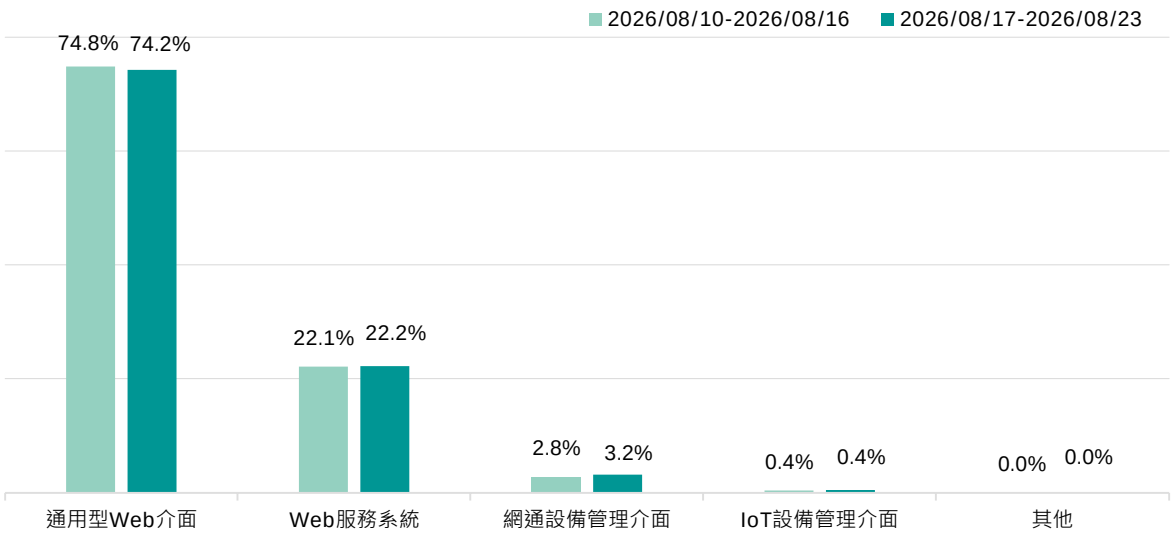

圖4 | 本週網頁應用介面之誘捕攻擊比例統計

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1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指令注入漏洞、身分驗證繞過漏洞、越界讀取漏洞及SQL注入漏洞，攻擊目標涵蓋大模型API統一介面與代理伺服器工具、網站主機伺服器管理系統、程式遞送控制器(ADC&Gateway)及企業級端點與安全管理系統。

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1年漏洞排行列表

排名			漏洞編號	受影響產品	CVSS 3.x Base Score	已知遭利用漏洞 (KEV)
■	1	-	CVE-2026-42271[1]	LiteLLM	8.8	✓
■	2	-	CVE-2026-41940[2]	cPanel & WHM	9.8	✓
■	3	-	CVE-2026-3055[3]	NetScaler ADC & Gateway	9.8	✓
■	4	⬆new	CVE-2026-1603[4]	Ivanti Endpoint Manager	8.6	✓
■	5	⬆new	CVE-2026-21643[5]	Fortinet FortiClientEMS	9.8	✓

類型 ■ 指令注入漏洞 ■ 身分驗證繞過漏洞 ■ 越界讀取漏洞 ■ SQL注入漏洞

1. https://nvd.nist.gov/vuln/detail/CVE-2026-42271
2. https://nvd.nist.gov/vuln/detail/CVE-2026-41940
3. https://nvd.nist.gov/vuln/detail/CVE-2026-3055
4. https://nvd.nist.gov/vuln/detail/CVE-2026-1603
5. https://nvd.nist.gov/vuln/detail/CVE-2026-21643

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

落實網站服務最小權限控管 降低弱點遭利用後之影響範圍

本週總計接獲23件公務機關與特定非公務機關事件通報，詳見圖5，公務機關非法入侵事件中以異常連線占多數，詳見圖6。本週發現機關網站未妥善限制檔案路徑，攻擊者修改 url 參數為 ../../etc/shadow 後，即可讀取作業系統敏感檔案，屬目錄遍歷/任意檔案讀取弱點。除應修正路徑檢核外，亦顯示網站服務程序若具過高作業系統權限，將使攻擊者進一步存取系統敏感檔案。

建議機關定期檢視網站服務實際使用之執行帳號、所屬群組及檔案存取權限，並採專用且低權限帳號執行，不應使用root、Administrator或具系統管理權限之帳號；並確認該帳號僅能存取網站程式等業務必要目錄，對 /etc/shadow、系統設定檔、SSH金鑰等非網站運作所需之敏感檔案不得具有讀取權限。

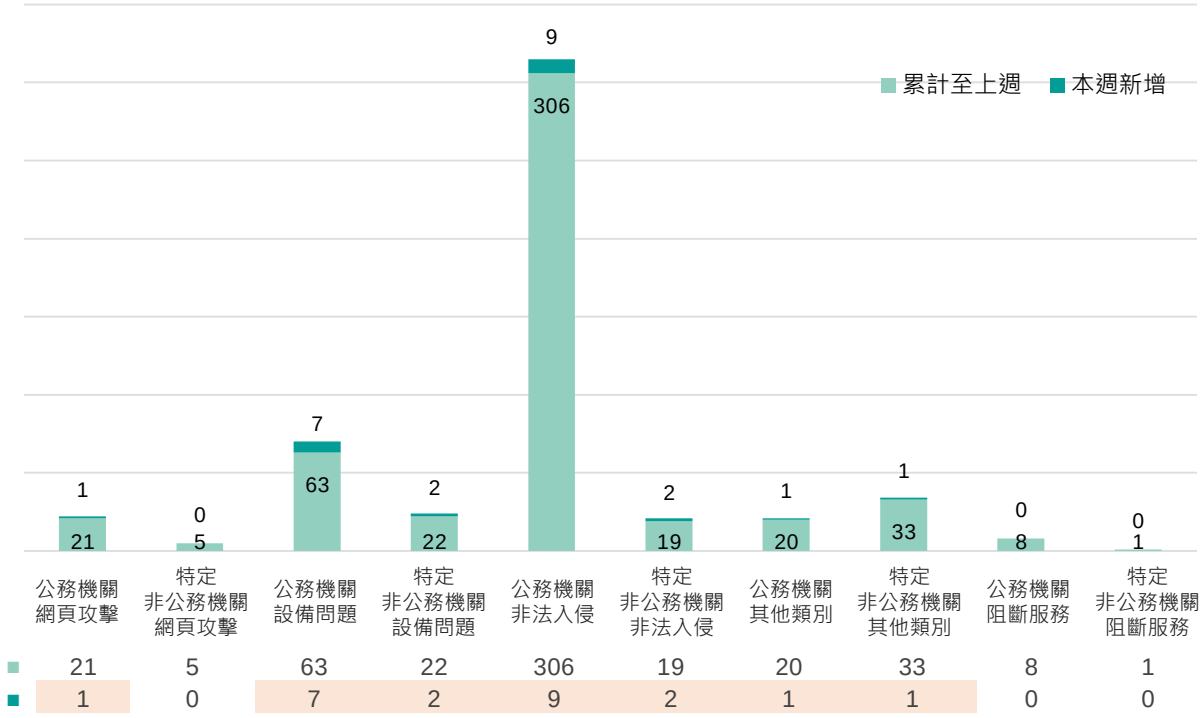

圖5 | 本週公務機關暨特定非公務機關資安事件通報概況

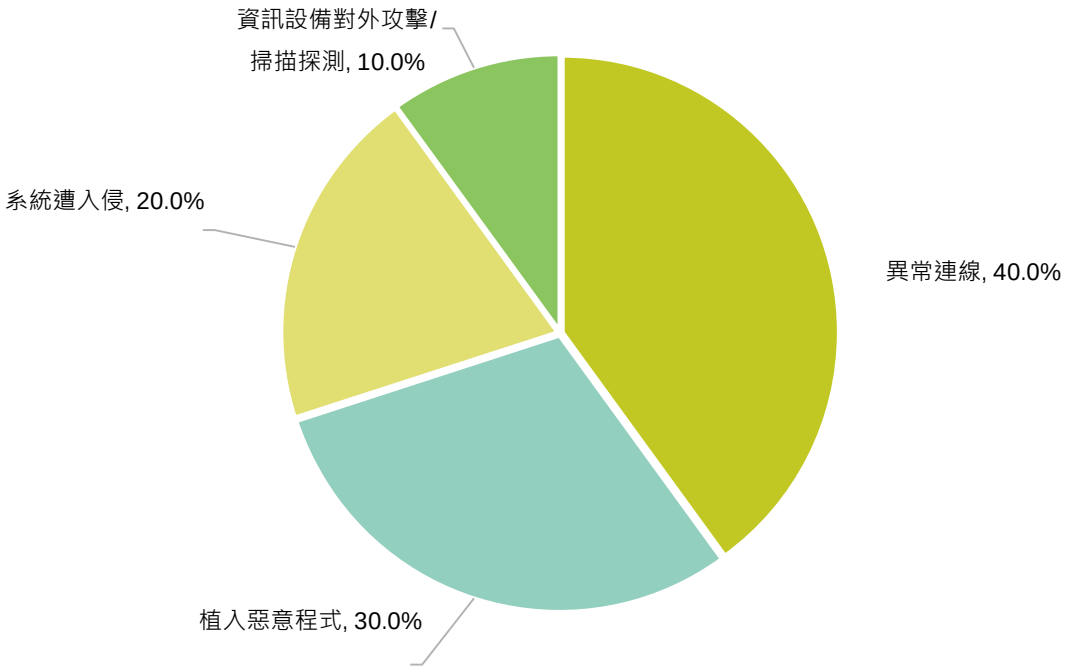

圖6 | 本週公務機關非法入侵事件類型占比

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
➢ 攻擊者利用目錄遍歷竊取系統敏感檔案 ➢ 網站服務權限過高擴大入侵後影響範圍	➢ 強化伺服器端路徑檢核與正規化處理，阻擋目錄遍歷及任意檔案讀取 ➢ 網站服務採專用低權限帳號執行，避免使用具系統管理權限之帳號 ➢ 依最小權限原則限制檔案存取範圍，禁止網站帳號讀取系統敏感檔案 ➢ 強化網站日誌及異常請求監控，偵測路徑跳脫與敏感檔案存取行為

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，產業類別為通信網路業、數位雲端業，詳見表2。

表2 | 本週民間企業重大資安訊息彙整

公司名稱	發布時間	事件說明
上詮光纖通信股份有限公司	2026年08月19日	上詮公司資訊系統遭受駭客網路攻擊，部分主機與電腦遭受病毒攻擊，資安團隊已立即啟動防禦機制及備援作業，並與外部資訊技術專業人員共同合作處理。 目前評估對公司營運無重大影響，後續將持續檢視與提升網路與資訊基礎架構之安全控管，以確保資訊安全。
數字科技股份有限公司	2026年08月20日	數字公司發現591網站登入行為異常，經查發現外部攻擊者利用登入機制之弱點，繞過部分安全檢核並進行未授權登入。資安團隊於偵測發現後，隨即啟動資安緊急應變機制，並完成相關漏洞修補及異常存取路徑阻斷，隨後同步進行系統存取紀錄清查、可疑連線封鎖、相關密鑰輪替及全站程式碼安全檢視。經評估對公司營運尚無重大影響。

■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

金融投資風險回升 免費領取與私訊導流同步升溫

本週金融投資型占比明顯回升，詳見圖7，為三類中增幅最大。相關內容以「免費領取」、「限時名單」及熱門產業題材吸引民眾索取投資訊息；另以高報酬、被動收入、資產翻倍及長期保障包裝境外不動產機會，再透過私訊或連結導入後續投資流程。

身分冒充型占比較前週下降。相關內容持續借用權威證書、臨床驗證及專業人士認可建立信任，並搭配「天然」、「安全」、「真品保證」及具體成效數字，強化產品的專業形象。

產品服務型占比較前週下降，仍是本週主要高風險類型。內容涵蓋清倉商品、美妝保健、翡翠競標、寵物用品、中古車貸款及彈性工時招募，並以免費換新、大幅折扣、限量釋出、免頭款及具體功效數字促購，再引導民眾私訊或點擊連結。

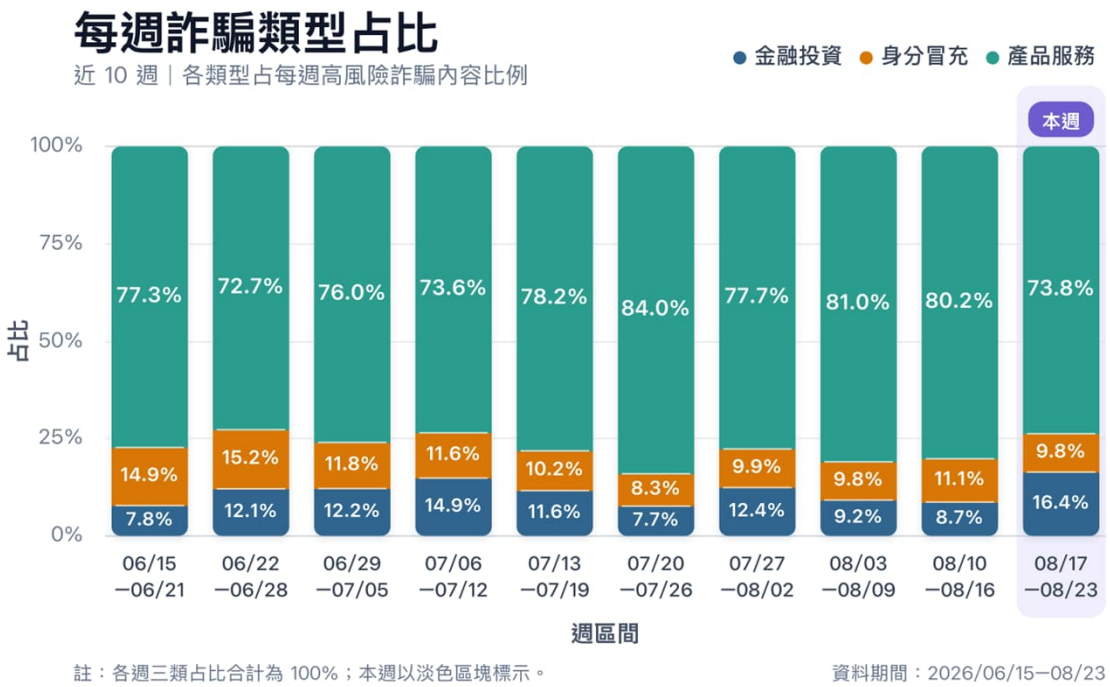

圖7 | 每週詐騙類型占比

「免費」升至本週首位，詳見圖8，相關話術以庫存清倉、免費換新及最後搶購製造高性價比印象。「優惠」占比較前週下降，仍居本週第 2 名，主要透過大幅折扣、限時優惠及多功能設計促進商品銷售。

「配方」與「健康」占比均較前週下降，分居本週第 3 名及第 4 名。相關內容運用植物萃取、臨床驗證、專業人士認可及具體改善比例，強調美妝與保健產品的安全性及效果。

「私訊」升至本週第 5 名，主要反映翡翠競標以私訊詢價、權威證書及限時結標推動交易。「加入」升至本週第 6 名，相關內容則透過會員人數、每日優惠及社群交流建立信任，將公開廣告流量導向私密對話與封閉社群。

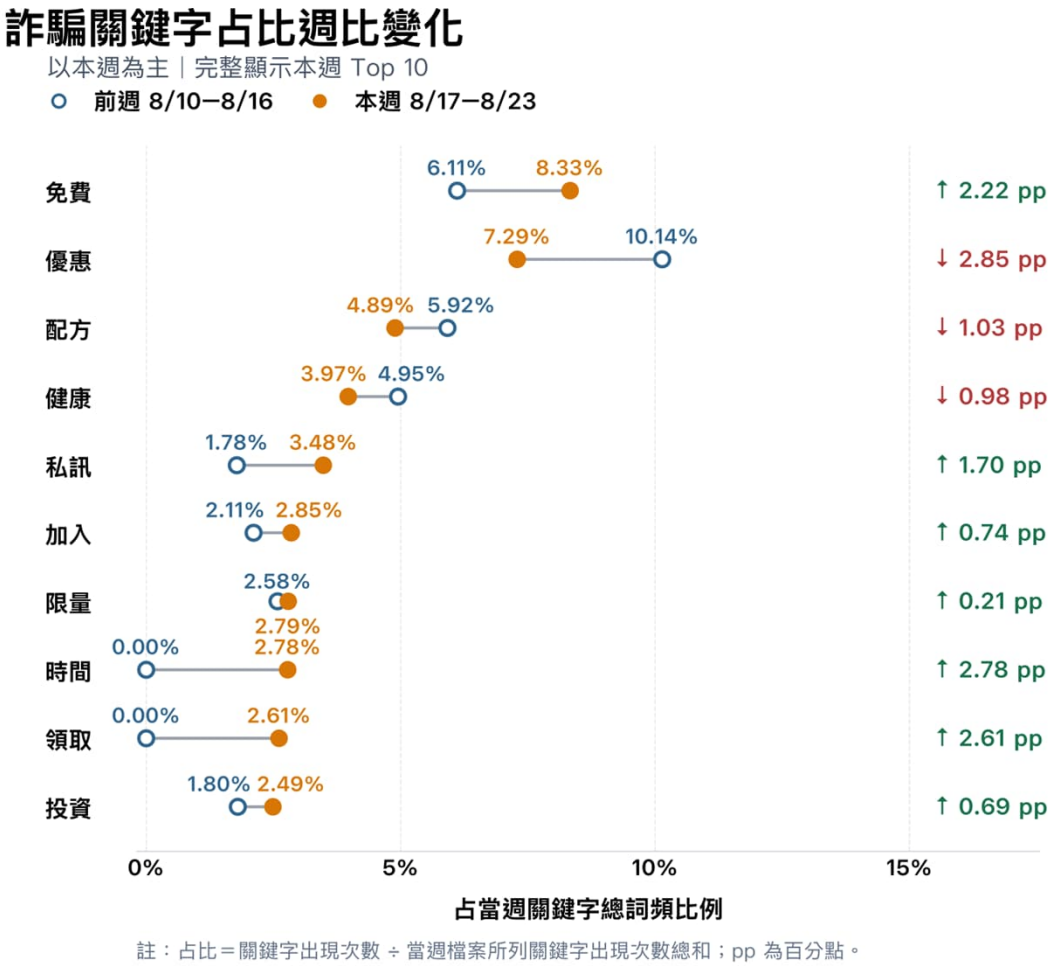

圖8 | 詐騙關鍵字占比週比變化

「時間」與「領取」新進本週 Top 10，分居第 8 名及第 9 名，呈現彈性工時招募與限時投資名單等訴求。「投資」進入本週第 10 名，相關內容以高報酬、被動收入及資產翻倍包裝境外不動產機會。整體而言，本週免費誘因、私訊導流與投資訊息領取同步升溫。

焦點文章

掌握軟體供應鏈風險：SBOM 概念與應用流程

現代軟體系統開發多仰賴外部資源，鮮少完全由單一團隊自行撰寫。即便是架構單純的業務系統，亦常整合數十至數百個開源套件、軟體框架、容器映像、商用元件，以及委外廠商交付之第三方模組。由於各元件之維護團隊、更新週期、授權條款與弱點揭露機制均不盡相同，大幅增加了整體系統的安全管理複雜度。

軟體物料清單（Software Bill of Materials, SBOM）係指以機器可讀之標準格式，完整記載軟體系統內所包含之各項元件、版本號碼、產製者資訊、識別碼及其相依性結構。
本篇文章自機關資安管理視角出發，闡述 SBOM 應具備的關鍵格式要素，並詳述自取得 SBOM 階段至弱點處置過程的整體作業流程與相應工具之定位。

一、為什麼需要 SBOM

在觀念上，SBOM 可比擬為食品之「原料成分表」。當特定批次原料發現品質瑕疵或安全疑慮時，可據此迅速盤查受影響之成品範疇；同理，當軟體系統發生資安弱點或智慧財產授權爭議時，政府機關亦能藉由 SBOM 精確定位並確認潛在受影響之系統範疇與對應版本，或應由哪一個內部單位或供應商處置，縮短影響範圍確認時間。

二、SBOM 最少資料欄位

SBOM 應對應系統、版本或建置產品，而非一次產出後永久有效的靜態報表。
依據2026 年 CISA、NSA、FBI 及國際夥伴更新 SBOM 最低要素指引，指出可用的 SBOM 除元件名稱、製作者、版本、識別資訊、相依關係及與產品的對應外，亦應保留雜湊值、授權及產製來源等可追溯資訊，並說明物料清單涵蓋範圍、未知項目、交付與更新機制，如表3[1]。

表3 | SBOM 資料欄位與定義

資料欄位	定義與說明
Component Name	元件名稱
Component Version	元件版本

焦點文章

資料欄位	定義與說明
Component Producer	元件之供應商、開發者或產製者名稱
Component Identifiers	元件之標準化識別碼（如 Package-URL等）
Component Dependency Relationship	元件之間的直接與間接相依關係
Component License	元件所使用之授權條款資訊
Component Hash Algorithm	用於計算元件雜湊值之演算法（如 SHA-256）
Component Hash Value	元件檔案之雜湊值，用於驗證完整性
SBOM Author	產製或建立此份 SBOM 之人員或團隊組織
SBOM Author Signature	SBOM 建立者之數位簽章，用以確保不可否認性與來源可信度
SBOM Timestamp	SBOM 產製之日期與時間戳記
SBOM Data Format Name	SBOM 所使用的標準資料格式名稱（如 SPDX, CycloneDX）
SBOM Data Format Version	SBOM 資料格式之版本
SBOM Version	此份 SBOM 文件本身的版本號碼
SBOM Tool Name	用於自動化產生此份 SBOM 之工具名稱
SBOM Tool Version	產製 SBOM 工具之版本號碼
SBOM Generation Context	SBOM 產製時的情境與範圍說明（如原始碼、容器映像或部署環境）

機關可據此檢視供應商資料是否包含以上資料欄位，足以支援弱點與供應鏈風險檢視，並將授權資訊納入授權風險管理。

其中 SBOM 所載的授權資訊，可協助機關確認特定產品或版本使用了哪些元件，及早辨識需要法務、採購或系統維運單位共同審視的授權義務及使用風險。

依據 SBOM 最低要素相關指引，建議優先採用國際通用格式，如 SPDX 或 CycloneDX，以利後續與既有工具介接，並進行元件識別、弱點比對及自動化分析[2][3]。

焦點文章

SBOM 導入可透過開源或商用工具產製與管理：

1. 開源工具例如 Syft、Trivy、CycloneDX cdxgen 及 Microsoft SBOM Tool，可針對原始碼、套件相依關係、建置產出物或容器映像產製 SBOM，其中 Syft、Trivy 及 cdxgen 均支援常見的 SPDX 或 CycloneDX 格式。
2. 商用工具則可採用 Mend、Checkmarx One SCA 等方案，除 SBOM 產製外，通常亦整合元件管理、弱點分析、授權風險及持續監控等功能。

機關辦理軟體採購或委外開發時，宜將 SBOM 格式、必要欄位、版本與建置產出物對應方式、更新頻率及交付方式納入需求說明書內[4]。

三、從取得到處置：SBOM 的四步驟管理循環

（一）取得SBOM：自行開發系統可在建置流程或交付產品時產製 SBOM；委外或商用系統則宜要求供應商提供與交付版本相符的SBOM。

（二）檢核SBOM：確認SBOM檔案包含上述的最少資料欄位外，還要能由工具解析出元件版本、識別資訊與相依關係，且未知、版本不明或無法確認來源的項目已明確標示。

（三）弱點比對與判讀：將產生的 SBOM 資訊，利用 OSV-Scanner 工具查詢 OSV 資料庫，確認元件是否有已知的安全漏洞。

（四）處置與更新：確認受影響範圍後，安排修補、升級、移除未使用元件、停用功能或採取緩解措施，並保留責任人、期限、例外核准及複查紀錄。發布新版、元件異動或緊急修補後，應一併更新相對應的 SBOM，並再次回到循環起點進行檢核，以確保供應鏈安全管理能因應威脅變化持續應處。

四、從弱點公告到處置判讀

當常用函式庫揭露重大弱點時，資安人員可先以公告的套件識別碼（Package-URL）及受影響版本範圍，與既有 SBOM 進行比對，快速找出可能受影響的系統，並進一步確認其實際正式部署系統內的版本與使用情形。再請系統供應商提供弱點可利用性資訊（Vulnerability Exploitability eXchange, VEX），說明對特定已知弱點的影響狀態，例如受影響、不受影響、已修復或調查中[5]。

焦點文章

機關取得 VEX 後，仍應結合系統實際部署環境、功能使用情境、弱點可達性及既有補償控制措施進行審視，再據以決定修補、緩解或其他風險處置方式。

五、常用工具與使用情境

導入 SBOM 工具前，應先釐清實際需求，是著重於 SBOM 產製、清冊品質檢核、弱點比對，或後續處置與持續追蹤。整理常見工具及其在 SBOM 管理流程中的主要用途，詳見表4，供機關評估導入時參考：

表4 | SBOM 工具於管理流程的主要用途

工具	類型 / 主要定位	適合的工作階段
Syft	開源 SBOM 產製工具	於掃描原始碼、容器映像或建置系統時產製 SBOM
Trivy	開源 SBOM 產製工具	於掃描原始碼、容器映像或建置系統時產製 SBOM
CycloneDX cdxgen	開源 SBOM 產製工具	於掃描原始碼與建置系統時產製 SBOM
Microsoft SBOM Tool	開源 SBOM 產製工具	於掃描原始碼與建置系統時產製 SBOM
Mend	商用 SBOM 產製工具	開發流程中的元件、弱點與授權管理
Checkmarx One SCA	商用 SBOM 產製工具	開發流程中的元件、弱點與授權管理
Dependency-Track	SBOM追蹤平台	匯入 SBOM 並持續追蹤元件與弱點資訊
OSV-Scanner	開源弱點比對工具	以 SBOM 或套件清單查詢 OSV 資料庫比對已知弱點

焦點文章

無論採用開源或商用工具，應了解工具可提升效率，但不能取代資料品質檢核與風險判讀，所以均應確認以下三項事項：

1. SBOM 是否對應實際部署系統版本
2. 元件識別資訊與版本是否足以進行判讀比對
3. 發現問題後能否連結至負責人員、修補期限及例外處置

六、機關試辦：品質檢核與衡量指標

建議先選擇一套可取得原始碼的自行開發系統，以及另一套仍有供應商窗口的系統試辦，分別驗證「自行產製」與「供應商交付」兩種取得方式。

試辦時可先採用下列品質檢核：

1. 檔案格式可由既有工具解析，且產品版本、元件版本與識別資訊足以使用。
2. 相依關係與未知項目均有記錄，可說明清冊的涵蓋範圍與限制。
3. SBOM 能對應建置產品與實際部署資產，避免以非正式版本進行判讀。

衡量成效時，不宜僅計算產出份數，而是選用有意義的指標包括：

1. SBOM 產製或交付成功率，以及可由既有工具解析的比例。
2. 可識別元件、版本資訊與相依關係的完整程度。
3. 新弱點出現後，確認受影響範圍及取得供應商回覆所需時間。

七、常見誤解

1. 誤解一：有了 SBOM，就等於完成弱點掃描，也能直接判定系統是否存在弱點。
   SBOM 的主要功能是記錄系統所包含的元件、版本及相依關係，本身並不等同於弱點掃描結果，也不能直接判定系統是否實際受到特定弱點影響。實務上仍須搭配弱點情報、系統使用情境、執行環境及人工判讀，才能確認實際風險。

2. 誤解二：同一套系統只需要維護一份 SBOM。
   同一系統的不同版本，可能使用不同元件、套件版本或建置內容，因此每一個正式發布或部署版本，都應對應相符的 SBOM。若沿用舊版 SBOM，可能無法正確反映實際部署狀態，進而影響後續弱點比對與事件應變。

焦點文章

3. 誤解三：SBOM 列出元件授權資訊，就代表已完成授權合規確認。

   SBOM 可協助盤點軟體元件及其授權資訊，作為授權管理與審視的基礎，但不能單憑 SBOM 判定是否符合授權條件。實際是否合規，仍須依元件的使用方式、修改情形、散布或發布模式及契約內容進一步確認，必要時應由法務專業人員進行判讀。

結語

SBOM 的核心價值，是讓機關從「確認系統是否受影響」進一步掌握「哪一個元件、哪一個版本、實際是否受影響，以及由誰處理」。先以少數系統建立取得、檢核、比對、處置與更新的循環，即可逐步累積可用、可追溯的軟體供應鏈風險管理能力。

參考資料

[1] Cybersecurity and Infrastructure Security Agency, National Security Agency, Federal Bureau of Investigation, and international partners. (2026). 2026 Minimum Elements for Software Bill of Materials (SBOM). https://www.cisa.gov/resources-tools/resources/2026-minimum-elements-software-bill-materials-sbom

[2] SPDX. Specifications. https://spdx.github.io/spdx-spec/

[3] OWASP CycloneDX. Specification Overview. https://cyclonedx.org/specification/overview/

[4] National Institute of Standards and Technology. (2022). NIST SP 800-218: Secure Software Development Framework (SSDF) Version 1.1.

[5] OASIS. (2022). Common Security Advisory Framework (CSAF) Version 2.0: VEX Profile. https://docs.oasis-open.org/csaf/csaf/v2.0/csaf-v2.0.html

關鍵字：SBOM (軟體物料清單)、軟體供應鏈安全、資安管理

刊　　名　資安週報第 59 期
發 行 人　國家資通安全研究院　龔化中院長
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