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

應留意監視器設備異常下載與可疑指令執行行為 及早發現受駭跡象

聯防監控

防禦迴避高居首位 偵測刺探仍具威脅

蜜罐誘捕

Web服務系統攻擊趨勢增加

外部曝險分析

元件高風險漏洞增幅顯著 整體外部曝險風險較上期上升

焦點文章

政府機關與關鍵基礎設施單位外網曝險統計與研析

2026.05.14
044

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

應留意監視器設備異常下載與可疑指令執行行為 及早發現受駭跡象

本週總計接獲39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。本週偵測到多起監視器遭入侵，疑似針對/cgi-bin/nobody/路徑下之CGI執行命令注入攻擊 ，並透過內建BusyBox wget指令下載惡意程式 。

由於監視器設備受駭情境已非首次出現，建議各機關除持續落實帳密管理、韌體更新及管理介面存取限制外，亦可依設備運作情形主動檢視是否出現異常行為，例如非預期CGI存取行為、異常對外下載行為、wget或sh等可疑指令痕跡，以及 /mnt/firmware等目錄下之不明檔案 ，以利及早發現受駭跡象。

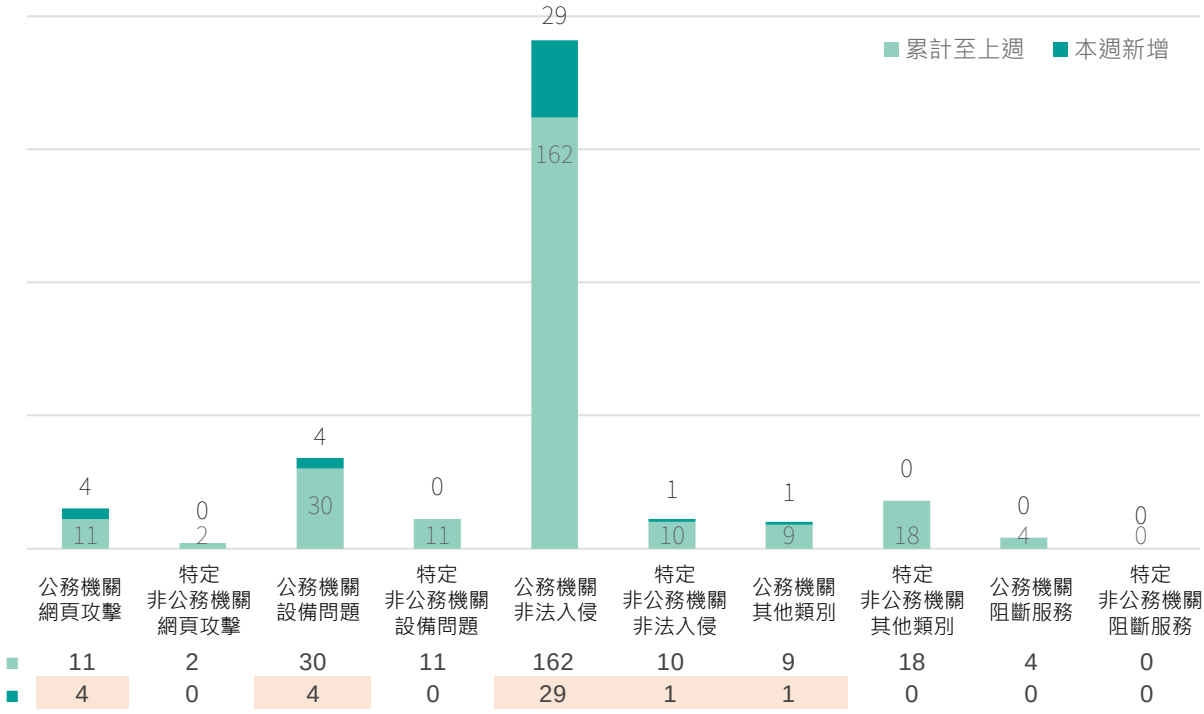

圖1 | 本週公務機關暨特定非公務機關資安事件通報概況

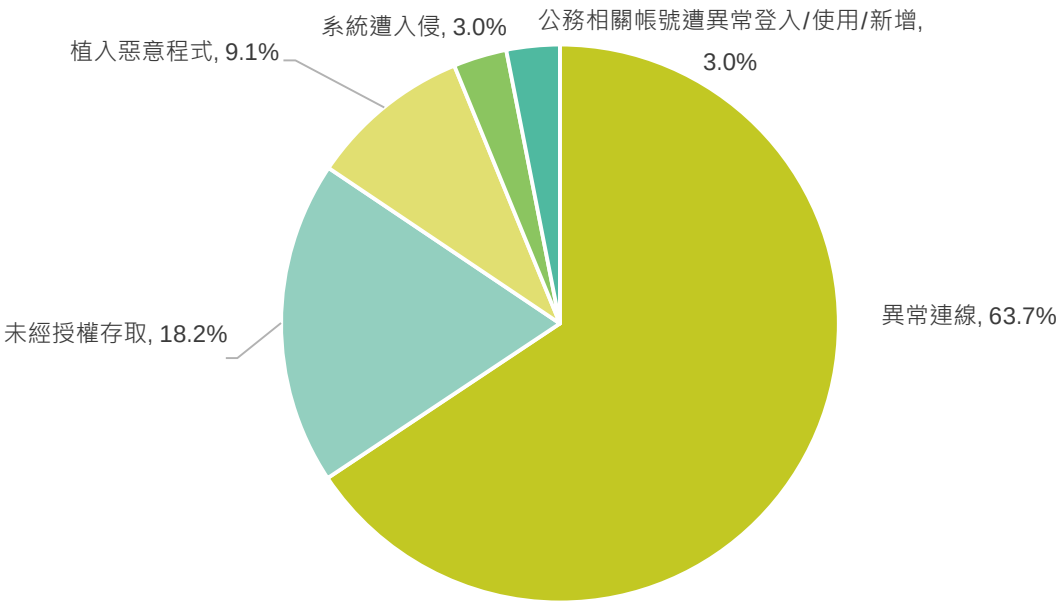

圖2 | 本週公務機關非法入侵事件類型占比

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
➢ 攻擊者利用命令注入控制監視器設備系統惡意程式下載後建立持續性遠端控制管道	➢ 定期更新設備韌體與修補漏洞，降低命令注入攻擊成功風險 ➢ 限制管理介面與CGI功能對外存取，避免設備暴露於網際網路 ➢ 強化設備行為監控機制，即時發現異常下載與可疑指令執行 ➢ 定期檢查設備目錄與執行檔，清查未授權程式與異常檔案

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，產業類別為其他電子業。

■ **公司名稱**	碩天科技股份有限公司
■ **發布時間**	115年5月7日
■ **事件說明**	碩天公司資安單位發現遭不明駭客入侵主機並將部分伺服器資料加密，已即刻啟動資安防禦及復原機制，並委請外部資訊公司技術專家及系統廠商協助處理。經評估對公司財務、業務及營運皆無重大影響，將持續提升網路與資訊基礎架構之安全管控，以確保資訊安全。

■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

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15.5%，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，顯示攻擊者持續加強對目標環境的前期偵查與資訊蒐集行動。觀察到的主要手法包括IP 區段掃描、主動式掃描、以及憑證資訊蒐集。攻擊者透過自動化工具大規模掃描外部網段與公開服務，以識別可存取主機、開放埠與系統類型，同時蒐集與帳號憑證相關的資訊，作為後續登入嘗試或攻擊行動的基礎。部分活動顯示攻擊者會先進行廣泛探測，再逐步聚焦特定服務與帳號目標，以提高後續攻擊成功率。此類行為多屬攻擊前期準備階段，雖不直接造成破壞，但能有效提升後續滲透與入侵效率。建議強化對異常掃描流量與登入探測行為的監控，定期檢視對外資產暴露情形，並結合威脅情資分析掃描來源，以提前辨識潛在攻擊準備活動。

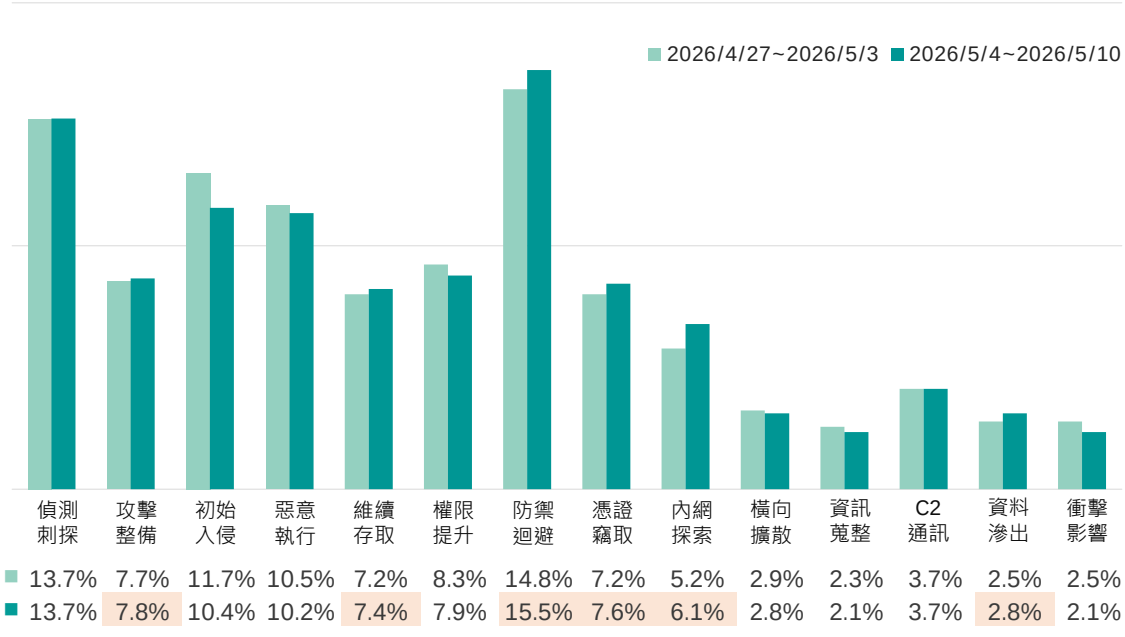

圖3 | 資安聯防監控攻擊階段統計

防護建議 建議機關採取下列防護措施：

防禦迴避（Defense Evasion）

- 強化端點防護機制（EDR / 防毒）並定期更新規則
- 啟用並保留系統與指令操作紀錄，避免遭關閉或刪除
- 限制 PowerShell、PsExec、WMI 等高風險工具使用權限
- 加強特權帳號管理，落實最小權限與多因素驗證（MFA）
- 監控異常指令執行、程序注入與可疑系統工具使用行為
- 建立集中式日誌保存機制，避免攻擊者清除本機紀錄

偵測刺探（Reconnaissance）

- 強化對外服務與網段的掃描行為監控
- 部署 IDS / IPS 或流量分析機制，偵測異常探測流量
- 定期盤點與檢視對外暴露資產，降低攻擊面
- 監控異常登入嘗試與憑證蒐集行為
- 封鎖已知惡意來源IP，並結合威脅情資分析掃描來源
- 針對公開服務落實弱點修補與存取限制
- 建立異常掃描與探測行為告警機制，

■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

Web服務系統攻擊趨勢增加

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53.83%、「遠端控制」服務攻擊占比43.70%，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62.81%。「遠端控制」服務亦有34.56% 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Web服務系統比例上升主因為Apache Log4j遠端程式碼執行漏洞的CVE-2021-44228，遭攻擊次數上升導致。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。

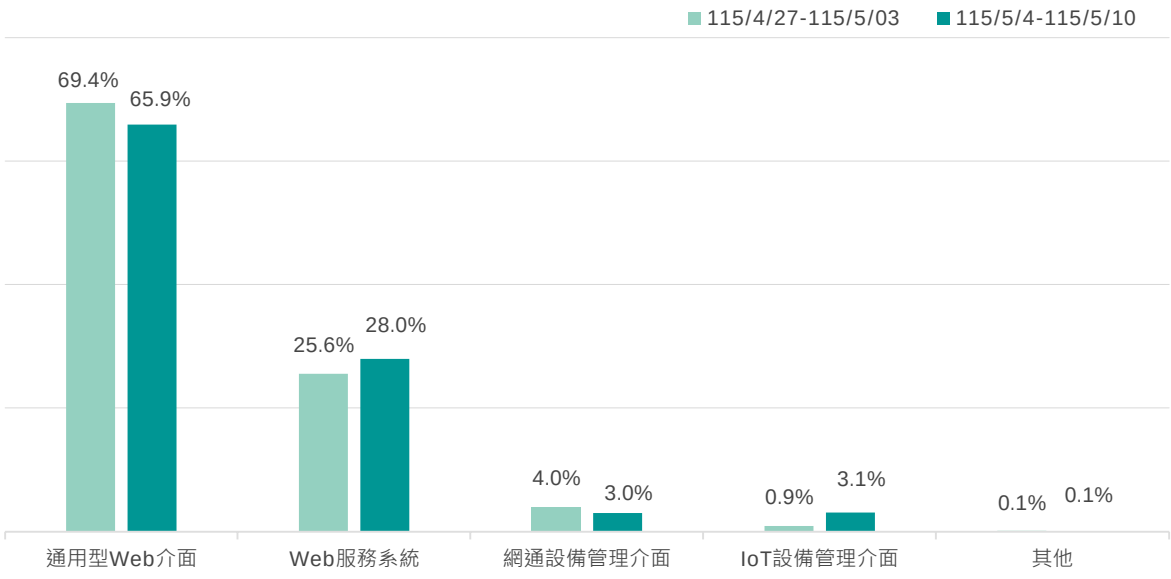

圖4 |本週網頁應用介面之誘捕攻擊比例統計

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、作業系統命令注入漏洞、指令注入漏洞、遠端程式碼執行漏洞及資訊外洩漏洞，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及知識管理與團隊協作系統。

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	↑New	CVE-2024-21887[3]	Ivanti Connect Secure	9.1
■	4	↓1	CVE-2024-21683[4]	Atlassian Confluence Server	8.8
■	5	↑New	CVE-2024-24919[5]	Check Point VPN Gateway	8.6

類型 ■越界讀取漏洞 ■作業系統命令注入漏洞 ■命令注入漏洞 ■遠端程式碼執行漏洞 ■資訊外洩漏洞

▶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：

- Cisco Secure Firewall Adaptive Security Appliance (ASA)與Secure Firewall Threat Defense(FTD) 存在高風險漏洞(CVE-2025-20333[6])，類型為緩衝區溢位(Buffer Overflow)，已取得一般權限之遠端攻擊者可藉由發送特製HTTP(S)請求，利用此漏洞於設備上以root權限執行任意程式碼，該漏洞近期已遭中國駭客組織利用。
- Palo Alto Networks PAN-OS存在高風險安全漏洞(CVE-2026-0300[7])，類型為緩衝區溢位(Buffer Overflow)，未經身分鑑別之遠端攻擊者可透過發送特製封包，於PA系列及VM系列防火牆上以root權限執行任意程式碼。

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-2024-21887
4. https://nvd.nist.gov/vuln/detail/CVE-2024-21683
5. https://nvd.nist.gov/vuln/detail/cve-2024-24919
6. https://nvd.nist.gov/vuln/detail/CVE-2025-20333
7. https://nvd.nist.gov/vuln/detail/CVE-2026-0300

■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

元件高風險漏洞增幅顯著 整體外部曝險風險較上期上升

本次針對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1,562項。其中，「元件高風險漏洞」以834項居首，「過時或弱加密協定」244項居次，「CSP設定不當」236項位居第三，詳見圖5。前三項合計1,314項，占前10大風險項目總數約84.1%，顯示目前外部曝險風險仍高度集中於元件漏洞、加密通訊及網站安全設定等議題。相較上期1,462項，整體風險數量增加100項，增幅約6.8%。

進一步分析重大風險變化情形，「元件高風險漏洞」由693項大幅增至834項，增加141項，增幅約20.3%；「TLS憑證不受信任」由60項大幅降至34項，減少26項，降幅約43.3%；「過時或弱加密協定」由256項降至244項，減少12項，降幅約4.7%；「CSP設定不當」由240項降至236項，減少4項，降幅約1.7%；「未部署WAF」則由99項增至104項，增加5項，增幅約5.1%。整體而言，元件高風險漏洞問題較上期擴大，部分憑證與網站安全設定已有改善，惟應用層防護機制仍待持續強化。

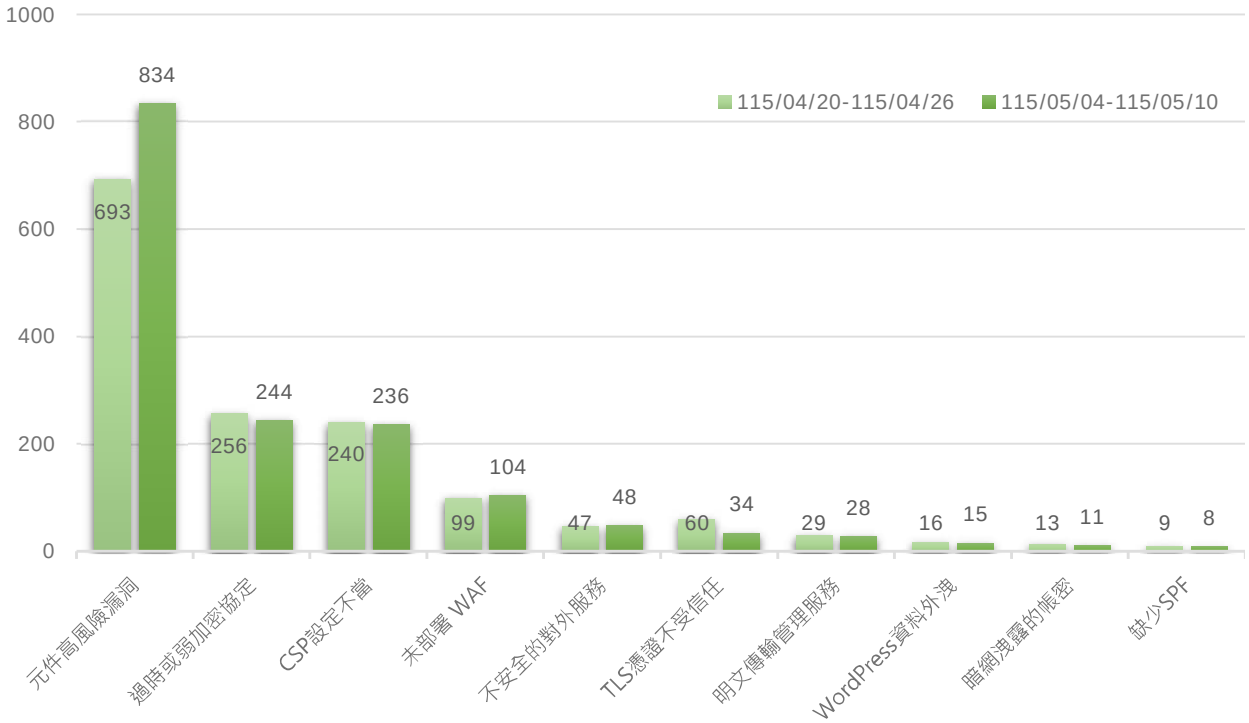

圖5 | EASM檢測結果統計(前10大風險)

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

政府機關與關鍵基礎設施單位外網曝險統計與研析

外網曝險明顯收斂，主動監測與警訊通知展現風險減量成效

本院為落實主動防禦機制並協助政府機關強化資安治理，現行針對外部曝險管理(EASM)採雙週循環檢測方式辦理，單數週掃描100個A、B級公務機關，雙數週掃描93個A、B級關鍵基礎設施(CI)單位。透過週期性檢測，持續掌握重要機關之外網曝險變化趨勢，並針對曝險程度較高或元件存在已知重大弱點之受測單位，陸續發布警訊通知，提醒其辦理弱點修補與風險改善。

一、多期數據呈現收斂，主動監測具體掌握曝險變化

統計自3月起至本期之EASM檢測結果，公務機關與CI之外網曝險總量整體呈現收斂趨勢，顯示主動監測機制已能持續掌握外部攻擊面變化，並協助定位高風險項目與改善重點。

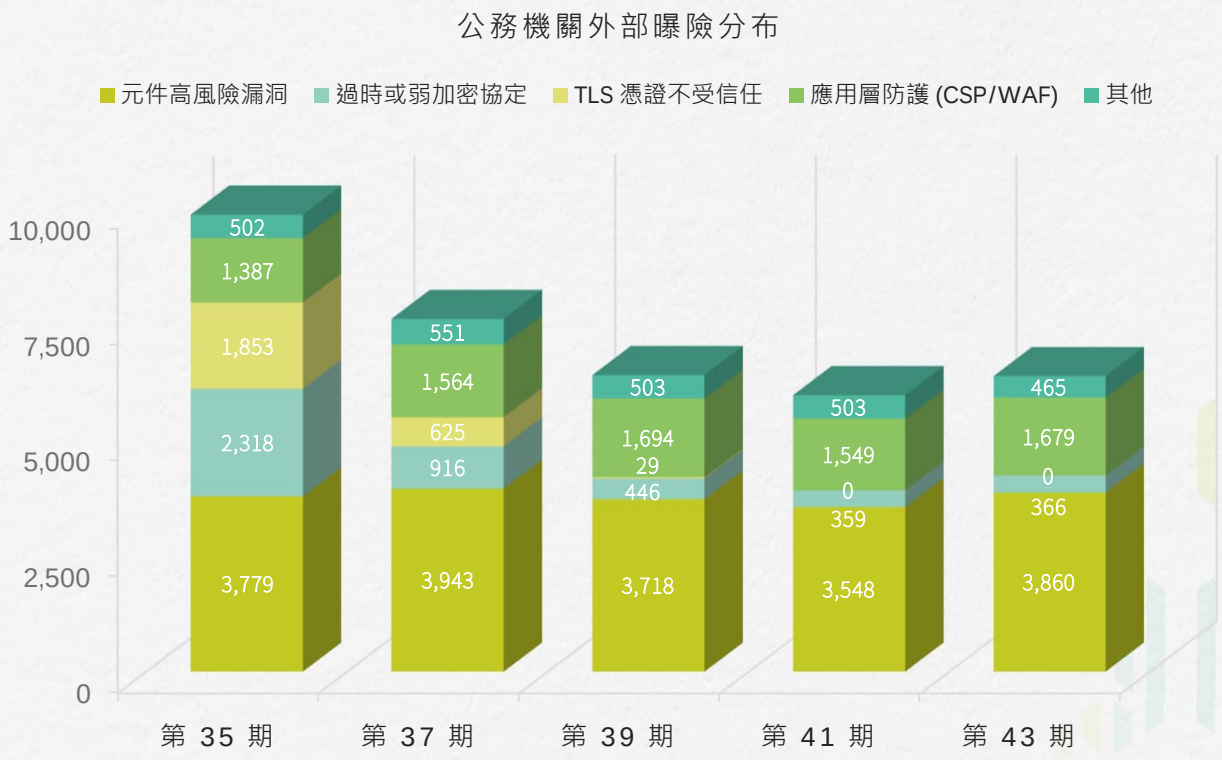

圖6 |公務機關外部曝險分布

焦點文章

公務機關部分，前10大風險項目合計數由第35期9,839項，降至第43期6,370項，降幅約35.3%，顯示整體曝險總量已明顯低於初期水準，詳見圖6。CI部分，前10大風險項目合計數由第34期2,454項，於第36期升至2,535項高點後，逐步下降至本期(第44期)1,562項，降幅約38.4%，顯示CI單位外網曝險總量仍較初期明顯收斂，詳見圖7。

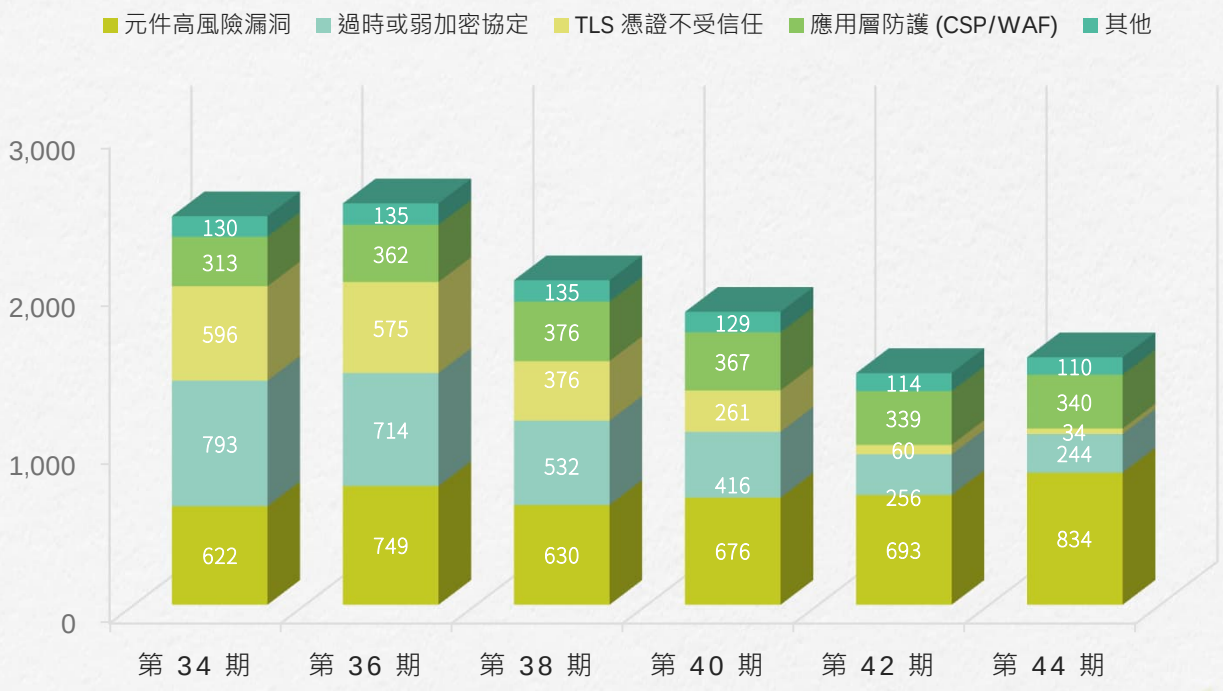

圖7 | CI外部曝險分布

二、基礎連線風險持續下降

各受測單位在「過時或弱加密協定」及「TLS憑證不受信任」等基礎連線安全項目已有明顯改善。以公務機關為例，第35期「TLS憑證不受信任」為1,853項，至第41期已未檢出。CI單位部分，「TLS憑證不受信任」由第34期596項降至本期34項，降幅約94.3%；「過時或弱加密協定」亦由793項降至本期244項，降幅約69.2%。顯示憑證管理與加密通訊維運方面已持續改善，基礎連線安全風險已明顯降低。

三、元件漏洞仍為主要曝險來源

「元件高風險漏洞」仍長期位居公務機關與CI單位風險排行榜首，為目前最主要之外網曝險來源，須持續列為警訊通知與改善追蹤重點。公務機關部分，第43期「元件高風險漏洞」為3,860項，占前10大風險項目合計數6,370項之60.6%，且主要集中於舊版Apache HTTP Server已知漏洞未修補，反映部分對外服務仍有元件版本老舊、修補延宕或汰換管理不足等問題。CI單位部分，本期「元件高風險漏洞」由上期693項增至834項，增幅約20.3%，占本期前10大風險項目合計數1,562項之53.4%。此變化顯示，CI單位本期風險數量回升，主因為元件高風險漏洞增加，後續應優先強化對外服務元件盤點、版本控管及修補追蹤。

四、網站應用層風險浮現，後續仍須強化防護縱深

隨著基礎連線安全與憑證問題逐步降低，網站應用層安全設定不足問題逐漸浮現。公務機關第39、41及43期前三大風險項目，均包含「CSP設定不當」與「未部署WAF」；CI單位本期「CSP設定不當」為236項，位居第三，「未部署WAF」則由上期99項增至104項(這兩項目加總即圖7之「應用層防護」的340項)，增幅約5.1%。

五、後續防護建議

外網曝險治理將持續運用週期性監測與警訊通知機制，推動受測單位落實弱點修補、元件版本管理及網站應用層防護等，建議機關可採取下列安全措施：

(一)落實軟體資產盤點與元件版本管理

各單位應優先盤點對外網站、公開服務及相關系統元件版本，特別針對Apache HTTP Server等高風險通用元件，建立版本清冊、弱點比對、修補追蹤及汰換管理流程，避免已知漏洞長期曝露於外部攻擊面。

(二)強化網站應用層防護能力

針對重要對外業務網站，應評估部署Web應用程式防火牆(WAF)，並依網站服務型態、流量特徵及攻擊樣態定期調校防護規則。同時，應正確設定內容安全政策(CSP)及其他網站安全標頭，以降低跨站腳本攻擊、惡意內容載入及網站遭偵查利用之風險。

(三)持續降低不必要之外部攻擊面

各單位應定期清查對外開放之站台、主機、連接埠及應用服務，確認非必要服務已關閉，無維護或已停止使用之資產確實下線。針對遠端管理或維運需求，應限制來源IP，採用加密通道，並強制啟用多因素驗證(MFA)。

六、結語

整體而言，自3月起至本期之EASM檢測結果顯示，公務機關與CI單位之外網曝險總量已較初期明顯收斂，基礎連線安全與TLS憑證管理問題亦有具體改善，顯示主動監測與警訊通知機制已逐步發揮風險減量成效。

惟本期CI單位整體風險數量較上期增加100項，主因為元件高風險漏洞增加，顯示外部曝險仍會因元件漏洞揭露、版本更新及維運變更而持續變動。未來本院將持續透過週期性EASM檢測、警訊發布通知及重點風險追蹤，協助受測單位掌握外部攻擊面變化，落實弱點修補與曝險減量，逐步強化我國政府機關與CI單位之整體資安韌性。

關鍵字：元件高風險漏洞、外部攻擊面管理(EASM)、關鍵基礎設施(CI)

刊　　名　資安週報第 44 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