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

資安週報

Cyber Security Weekly Newsletter

外部曝險分析
整體曝險持續下降 新揭露弱點仍需關注

重大漏洞
Check Point與WordPress高風險漏洞應盡速修補

實兵演練
實兵演練揭露檔案上傳組態設定不當 致惡意程式執行與權限提升風險

聯防監控
防禦迴避高居首位 偵測刺探仍具威脅

蜜罐誘捕
企業級網路防火牆軟體仍成攻擊熱點

事件通報
AI Agent整合多階段攻擊 攻擊自動化程度提高

焦點文章
工控數位靶場演練：以實戰流程驗證IT/OT資安應變與營運韌性

2026.07.30
055

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、事件通報等六類量化指標

■ 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

整體曝險持續下降 新揭露弱點仍需關注

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9,436項。其中，「元件高風險漏洞」以3,903項居首，「過時或弱加密協定」1,913項次之，「TLS憑證不受信任」1,520項位居第三。前三項合計7,336項，占前10大風險項目總數約77.7%，顯示目前外部曝險風險仍高度集中於元件漏洞、加密協定與憑證管理等議題。相較上期9,630項，本期整體風險數量減少194項，降幅約2%，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4,050項減至本期3,903項，降幅約3.6%。其中，Apache HTTP Server相關弱點(CVE-2024-38475)仍為主要風險來源；Archive_Tar相關弱點(CVE-2020-36193)已見減少，惟本期新增WordPress相關弱點(CVE-2026-60137、CVE-2026-63030)。其他主要風險項目則呈現增減互見，「過時或弱加密協定」由1,989項減至1,913項，降幅約3.8%；「TLS憑證不受信任」由1,525項減至1,520項，降幅約0.3%。另「未部署WAF」由689項增至729項，增幅約5.8%；「CSP設定不當」由924項增至940項，增幅約1.7%。

整體而言，本期外部曝險風險下降，主要來自元件高風險漏洞數量的減少；惟部分元件仍受近期揭露之新弱點影響，受測機關仍應持續盤點元件版本，並密切關注近期揭露之弱點資訊，適時評估影響及規劃修補作業。

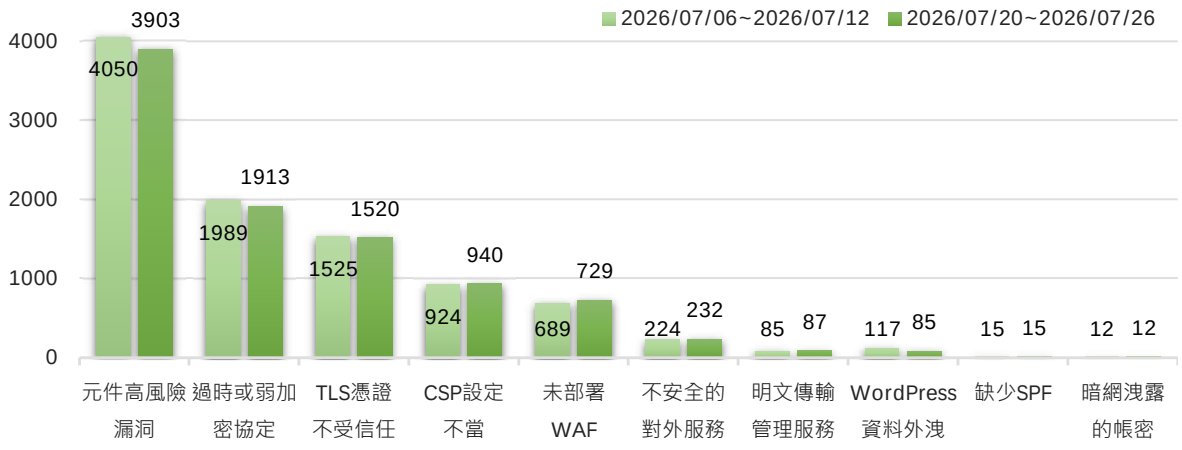

圖1 | EASM檢測結果統計(前10大風險)

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
➢ 定期更新憑證，全面啟用TLS 1.2以上版本協定，並停用未加密或舊版協定 ➢ 儘速修補已知漏洞，並淘汰已停止維護之軟體版本 ➢ 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、主機及應用服務是否已確實下線，避免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 ➢ 建立弱點修補與驗證機制，確保風險持續改善 ➢ 強化資安教育訓練，提升系統維運人員對憑證生命週期管理、加密協定設定及對外服務管理之安全意識

■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

Check Point與WordPress高風險漏洞應盡速修補

- Check Point Security Management Server與Multi-Domain Security Management Server存在身分鑑別繞過(Authentication Bypass)漏洞(CVE-2026-16232)[1]，此漏洞允許未經身分鑑別之遠端攻擊者取得應用程式登入Token，並使用該Token透過SmartConsole 登入管理伺服器，進而取得管理者權限，該漏洞已遭到駭客利用，請儘速確認並進行修補。

- WordPress存在兩項高風險安全漏洞(CVE-2026-60137與CVE-2026-63030)[2]，類型分別為SQL注入(SQL Injection)與REST API批次端點路由判讀錯誤問題。其中CVE-2026-60137已遭駭客利用，請儘速確認並進行修補。

1. https://support.checkpoint.com/results/sk/sk185169
2. https://wordpress.org/news/2026/07/wordpress-7-0-2-release/

■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

實兵演練揭露檔案上傳組態設定不當 致惡意程式執行與權限提升風險

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7/24止已累計236筆攻擊紀錄，本週新增弱點數量共11筆，分別為「不安全的組態設定」5筆、「注入攻擊」3筆、「無效的存取控管」2筆及「軟體供應鏈失效」1筆，詳見圖2。

本週演練發現，衝擊性較高之弱點為「不安全的組態設定」。攻擊者於系統提供之檔案上傳功能進行測試時，發現系統僅於前端限制上傳檔案格式，伺服器端未針對副檔名與檔案內容進行驗證，攻擊者繞過限制並成功上傳ASP Webshell檔案。攻擊者進一步利用後門程式，將提權檔案上傳至伺服器，並利用後門程式執行提權程式，最終成功取得作業系統最高權限。

顯示系統未妥善限制檔案上傳功能、上傳目錄之存取及執行權限，導致攻擊者得以利用該弱點擴大攻擊影響範圍。

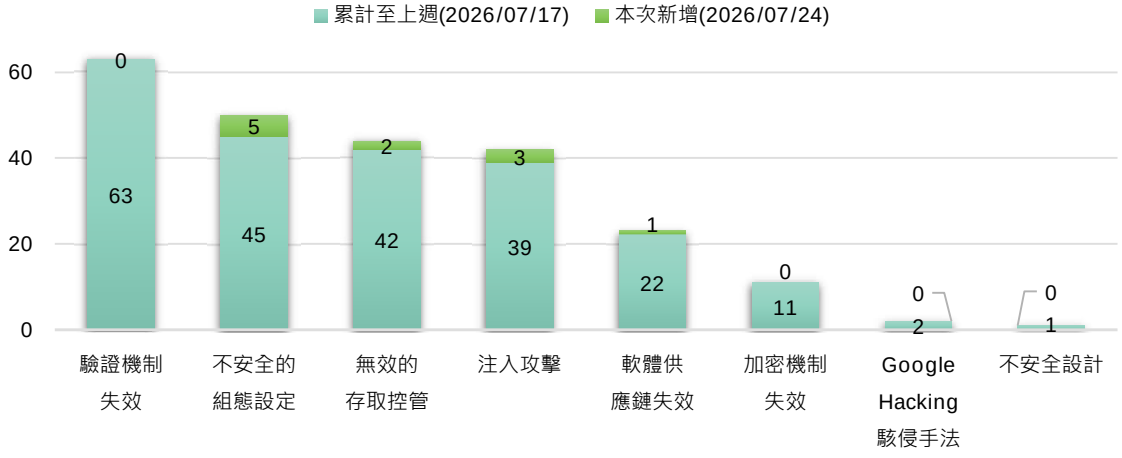

圖2 | 網路攻防演練資通系統實兵演練統計

建議機關及關鍵基礎設施提供者，採取下列防護措施

- 應於伺服器端落實檔案驗證機制，包含副檔名、MIME Type及檔案內容檢查，避免攻擊者透過偽造格式或混淆方式繞過檢核機制上傳惡意程式，以降低惡意程式執行風險
- 應將檔案上傳目錄與程式執行目錄分開，並限制上傳目錄執行權限，避免攻擊者上傳可執行檔案後遭利用
- 應依最小權限原則設定系統目錄與檔案存取權限，限制暫存目錄、上傳目錄及系統檔案之存取與寫入權限，避免未經授權操作

■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15.2%，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12.9%，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情報蒐集活動，以提升後續攻擊成功率。觀察到的主要手法包括主動式掃描、IP 區段掃描、及憑證資訊蒐集。攻擊者透過自動化工具持續掃描外部網段與公開服務，蒐集系統架構、開放埠及服務資訊，同時探查與帳號憑證相關的資訊，藉以鎖定潛在攻擊目標及可利用的存取管道。

此類活動通常由廣泛掃描逐步聚焦至特定主機或服務，具備高度自動化及目標導向特性，為後續漏洞利用、帳號攻擊或初始入侵的重要前置作業。建議機關持續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，以提前掌握攻擊者的偵查活動並降低後續入侵風險。

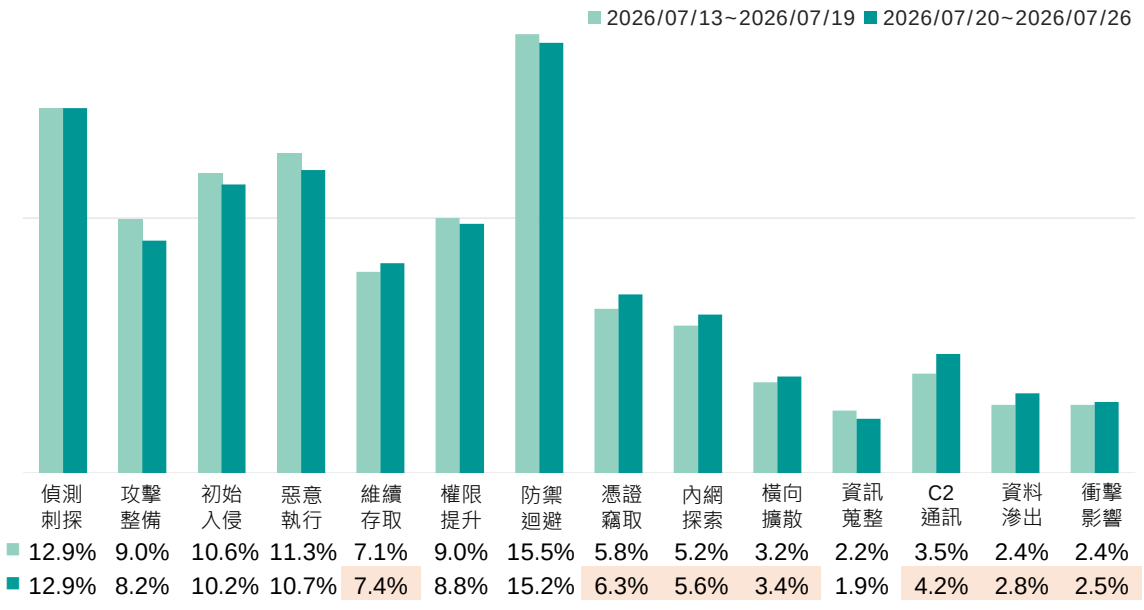

圖3 | 資安聯防監控攻擊階段統計

防護建議

建議機關採取下列防護措施：

防禦迴避(Defense Evasion)

- 啟用端點偵測與回應(EDR)，監控異常行為
- 保留並定期稽核系統與指令執行紀錄(如 PowerShell、Shell)
- 限制高風險系統工具(如 PowerShell、cmd、WMI、PsExec)使用權限
- 落實最小權限原則，強化特權帳號管理與多因素驗證(MFA)
- 建立異常程序執行、日誌清除及防毒停用等行為的告警機制

偵測刺探(Reconnaissance)

- 持續監控異常掃描流量、IP 探測及連線行為
- 定期盤點並降低對外暴露資產，移除不必要服務與開放埠
- 強化外部服務存取控制，限制來源 IP 或採用 VPN 等保護措施
- 建立帳號探測、暴力破解及憑證蒐集行為的偵測規則
- 結合威脅情資封鎖已知惡意來源，並持續分析可疑偵查活動

持續監控與最小權限並行，降低攻擊成功風險

■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

企業級網路防火牆軟體仍成攻擊熱點

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73.71%、「遠端控制」服務攻擊占比22.96%，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73.06%。「遠端控制」服務亦有23.38% 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家用無線路由器存在遠端程式碼執行漏洞之CVE-2017-17215，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。

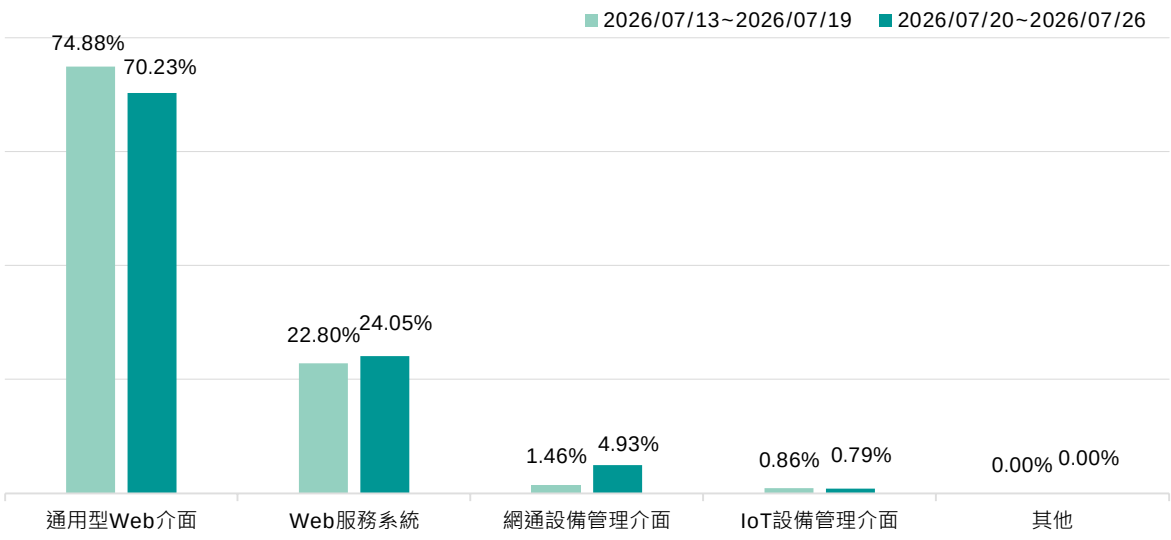

圖4 | 本週網頁應用介面之誘捕攻擊比例統計

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2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授權缺失漏洞、資訊外洩漏洞、跨站請求偽造、身分驗證繞過漏洞及路徑遍歷漏洞，攻擊目標涵蓋企業級網路防火牆軟體、開源後端伺服器框架、多選下拉選單元件、網站主機伺服器管理系統及內容管理系統之網站優化外掛程式。

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2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-2025-20362[1]	Cisco Secure ASA & FTD	6.5
■	2	⬆2	CVE-2025-53364[2]	Parse Server	5.3
■	3	-	CVE-2025-47204[3]	Bootstrap Multiselect	6.1
■	4	⬆new	CVE-2026-41940[4]	cPanel & WHM	9.8
■	5	-	CVE-2025-30567[5]	WordPress WP01	7.5

類型 ■ 授權缺失漏洞 ■ 資訊外洩漏洞 ■ 跨站請求偽造 ■ 身分驗證繞過漏洞 ■ 路徑遍歷漏洞

1. https://nvd.nist.gov/vuln/detail/CVE-2025-20362
2. https://nvd.nist.gov/vuln/detail/CVE-2025-53364
3. https://nvd.nist.gov/vuln/detail/CVE-2025-47204
4. https://nvd.nist.gov/vuln/detail/CVE-2026-41940
5. https://nvd.nist.gov/vuln/detail/CVE-2025-30567

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

AI Agent整合多階段攻擊 攻擊自動化程度提高

本週總計接獲25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系統遭入侵占多數，詳見圖6。本週發現攻擊者利用OpenClaw、Hermes Agent等開源 AI Agent 框架，針對政府網站自動執行漏洞探測、入侵攻擊及敏感資訊蒐集，例如取得帳密、API金鑰與網站目錄後，再進一步掃描內網IP及服務，並透過多個Proxy切換攻擊來源。

過往上述行為通常須由攻擊者分別操作多項工具並依結果調整後續步驟；AI Agent則可依預先設定的任務與技能，自動選用工具、解析結果並接續執行下一階段，使不同攻擊手法得以快速組合。此一趨勢並未改變弱密碼、系統漏洞或敏感資訊暴露等既有風險本質，卻可能縮短攻擊者由發現弱點至擴大入侵的時間，並擴大探測範圍及提高攻擊頻率。建議強化帳號驗證、漏洞修補及敏感資訊管理，並關聯分析登入、探測、資料存取及內網掃描等異常行為；同時限制對外網站主機連線至內部網路及非必要服務，降低攻擊擴散風險。

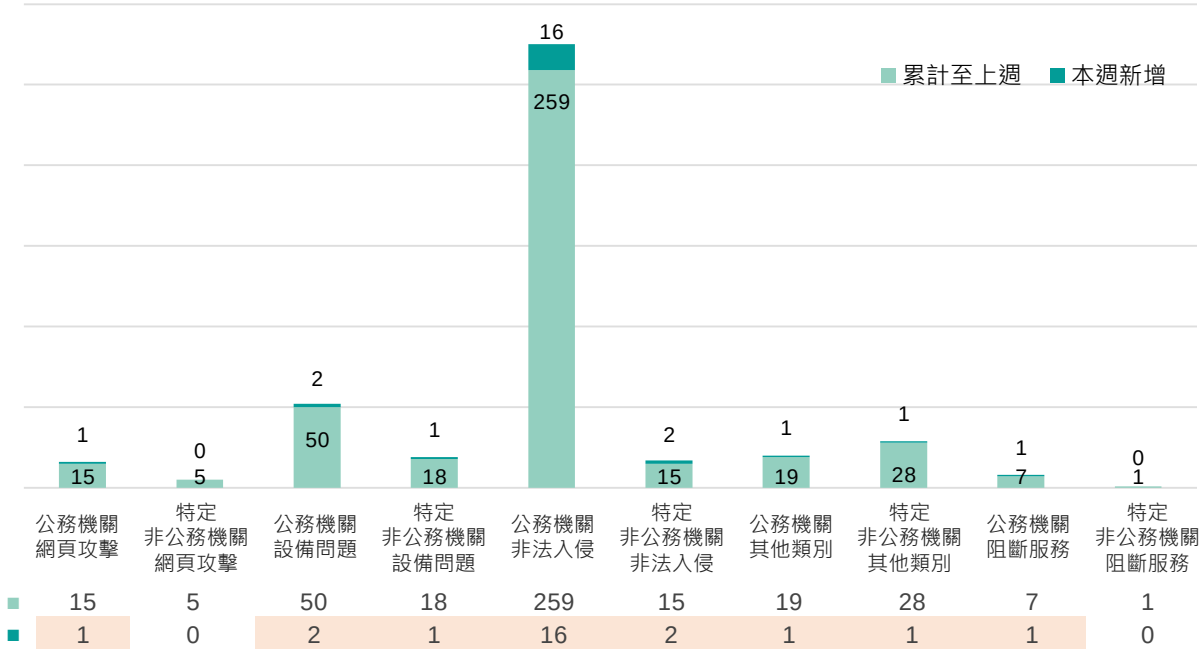

圖5 | 本週公務機關暨特定非公務機關資安事件通報概況

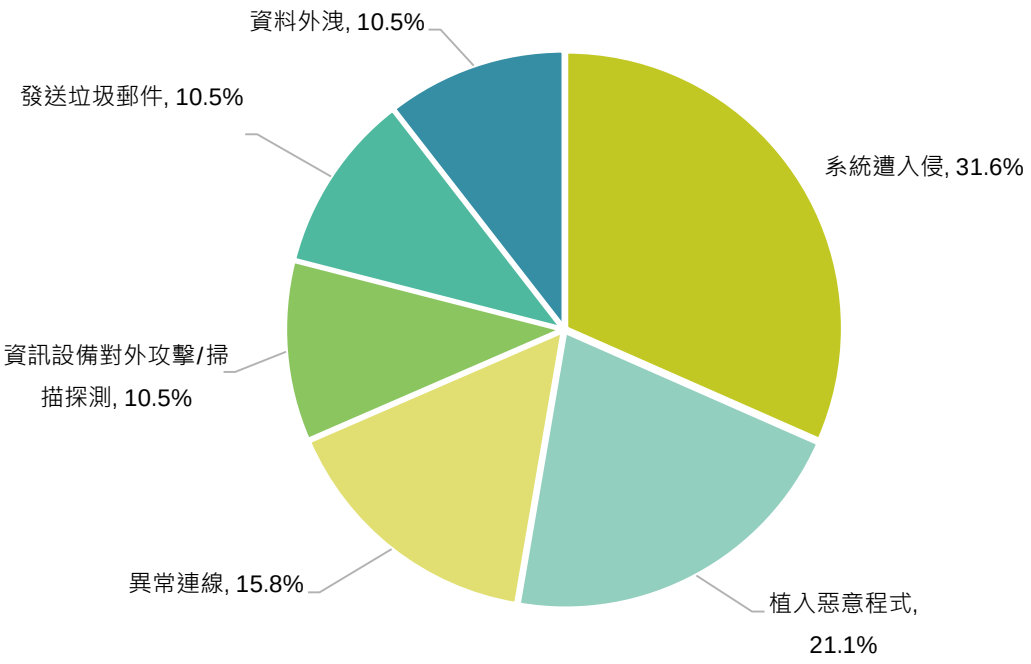

圖6 | 本週公務機關非法入侵事件類型占比

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
➢ AI Agent自主串聯攻擊快速擴大入侵範圍 ➢ 敏感資訊遭竊取後橫向滲透內部網路	➢ 強化多因子驗證及帳號管理機制，降低弱密碼與帳號遭濫用風險 ➢ 落實系統及第三方元件漏洞修補，縮短弱點暴露與攻擊利用時間 ➢ 建立敏感資訊管理機制，避免帳密、API金鑰及憑證外洩遭利用 ➢ 關聯分析登入、探測及內網掃描行為，限制網站主機存取內部網路

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，產業類別為其他電子業、電機機械業，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
淳安電子股份有限公司	115年07月20日	淳安公司資訊安全單位接獲異常通報後，經查證確認為加密攻擊，已即時啟動資安應變機制，並進行全面檢測與防護處理作業。經初步確認，內部資訊系統及官方網站運作未受實質影響，後續將持續強化監控與防護措施，以確保資訊系統安全與營運穩定。
湧盛電機股份有限公司	115年07月23日	湧盛電機針對媒體報導有關地下論壇販售疑似企業管理存取權限之事件澄清，經檢視防火牆登入紀錄，確認無外部入侵之情事。已採取先行風險降低措施和制度化治理與稽核精進，包含防火牆帳號密碼提高難度及雙重驗證機制、強化異常偵測與伺服器端風險控管、盤點並調整紀錄與存取控管政策、持續推動資訊安全與個資管理制度等。

焦點文章

工控數位靶場演練：以實戰流程驗證IT/OT資安應變與營運韌性

透過工控數位靶場驗證跨域防護、事件應變及營運韌性

工控數位靶場演練透過隔離、可重置且可觀測的擬真環境，協助組織驗證資訊科技(IT)與營運技術(OT)的資安防護、事件應變及營運持續能力，將制度與技術轉化為可量測、可改善的實戰成果。

一、前言

隨著雲端服務、遠距維運及工業物聯網普及，原本相對封閉的工控環境逐漸與企業內網、第三方系統及雲端服務連結。攻擊影響也可能由辦公端延伸至工程工作站(Engineering Workstation, EWS)、人機介面(Human-Machine Interface, HMI)、可程式邏輯控制器(Programmable Logic Controller, PLC)及資料採集監控系統(Supervisory Control and Data Acquisition, SCADA)等關鍵資產。

IT場域通常著重資料的機密性、完整性與可用性，事件發生時可採取隔離、重啟或重灌等措施；OT場域則更重視安全、穩定與持續運作，任何處置都必須同時評估製程、設備及人員安全。因此，組織需要在不影響正式產線的環境中，預先驗證跨域偵測、通報、隔離與復原流程。工控數位靶場正是連結IT與OT團隊、降低實地測試風險的重要訓練機制。

二、工控數位靶場演練的核心價值

工控數位靶場演練主要是為了檢驗事件發生時，組織是否能在壓力下正確判斷、協調與處置。其主要價值包括：

- 驗證跨域偵測能力：模擬攻擊者由釣魚郵件、帳號外洩、VPN弱點或企業內網橫向移動至OT網段，檢視監控機制能否辨識異常連線、工控協定封包、控制指令或設備狀態變化。
- 確認OT應變措施可行：驗證何時可隔離設備、降載、切換手動操作、啟動備援或執行停機，避免套用IT處置方式而造成製程中斷或現場風險。
- 強化IT與OT協作：讓資安人員理解設備與製程影響，也讓OT維運人員熟悉日誌、封包與威脅判讀，釐清通報窗口、決策權責及資訊需求。
- 降低營運衝擊：在隔離且可復原的環境中反覆演練，縮短異常發現、影響研判、控制擴散及服務恢復時間，並將演練結果轉化為正式場域的改善措施。

焦點文章

三、工控數位靶場演練規劃與執行重點

工控數位靶場演練應該要以實際營運風險為基礎，首先盤點關鍵製程、網路分段、遠端維運管道、資料交換介面、備援機制及現場操作流程，再依高風險情境設定目標。常見情境包括企業內網被入侵後存取OT網段、EWS遭植入惡意程式、HMI顯示遭竄改、PLC邏輯被未授權變更、SCADA通訊異常或勒索軟體影響監控與排程系統等。工控數位靶場的規劃與執行通常包含以下重點：

1. 設定目標與範圍：聚焦每次演練要驗證的能力，例如IT入侵擴散、OT異常流量偵測、控制邏輯變更辨識、事件通報或復原作業，並設定可量測的評估指標。
2. 建立模擬實務環境：以虛擬化、模擬器及部分實體設備重現企業內網、跳板主機、防火牆、工控交換器、HMI、PLC、SCADA、日誌平台與封包側錄機制，使演練具備足夠的設備互動與觀測資料。
3. 訂定安全邊界與停止條件：明確規範演練過程中可允許的操作和被禁止的行為、可用的測試工具、設定網路隔離及緊急中止條件，確保惡意程式、漏洞利用或控制指令不會連線至正式環境，也不會對設備造成不可逆影響。
4. 分配角色並執行演練：由紅隊模擬攻擊，藍隊負責監控、研判、通報、隔離及復原，紫隊協助交流與學習回饋；OT 維運人員與現場工程師則評估設備狀態、製程影響及復原可行性。演練過程應記錄異常發現時間、研判依據、隔離決策、現場回報及服務恢復時間。
5. 演後檢討並形成改善循環：依據演練結果辨識技能缺口、流程落差及技術不足，例如工控協定判讀能力不足、通報窗口不明、隔離措施影響產線或復原時間過長，並據以修正偵測規則、應變程序、備援架構及訓練內容。

四、結語

工控數位靶場演練的成效，不取決於攻擊劇本有多複雜或設備是否完全複製正式環境，而在於能否真實驗證人員、流程與工具的協作能力。面對IT/OT融合與工控系統連網化，企業與關鍵基礎設施營運單位應將演練納入常態化資安訓練與營運韌性驗證，透過「規劃、執行、評估、改善、再驗證」的循環，持續提升偵測、應變、復原及跨單位協作能力，降低真實事件對OT 穩定運作與關鍵服務的衝擊。

關鍵字：工控數位靶場演練、OT 資安、工控系統、事件應變、營運韌性

刊　　名　資安週報第 55 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