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

資安週報

Cyber Security Weekly Newsletter

2026.05.21
045

資安儀表板

事件通報、聯防監控、蜜罐誘捕、外部曝險分析及實兵演練等五類量化指標

■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

強化第三方元件管理 降低網站遭利用風險

本週總計接獲9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。 本週有機關網站疑因 CKEditor 相關功能遭利用，上傳惡意程式至網站目錄，後續已修改程式並移除相關元件。

網站使用第三方編輯元件時，除應考量功能需求外，亦應確認元件本身及其上傳、檔案管理等功能是否具安全風險；若元件版本老舊，或未妥善限制檔案類型、上傳路徑、執行權限及存取控制，即可能成為惡意程式上傳入口。建議定期盤點系統元件版本，確認是否仍持續維護並套用相關安全更新，同時檢查網站目錄中是否存在異常檔案或可疑副檔名 ；同時建立第三方元件使用、更新與汰換機制，對已無使用需求、停止維護或具較高風險之功能，宜評估停用、移除或限制使用，以降低網站遭利用風險。

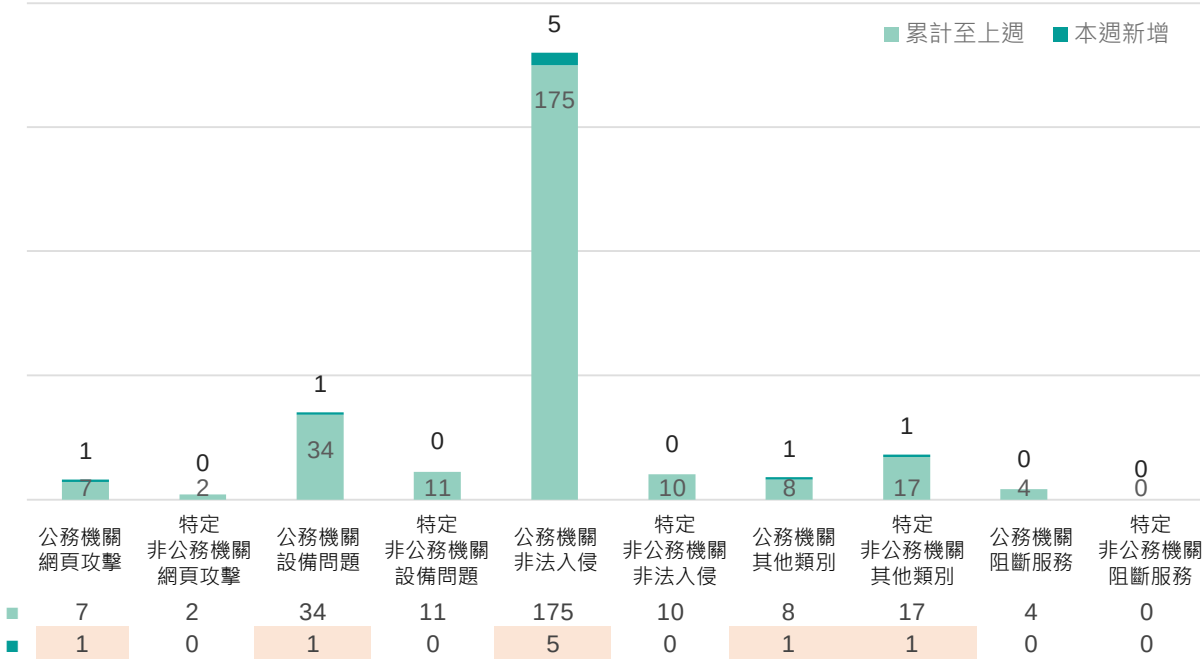

圖1 | 本週公務機關暨特定非公務機關資安事件通報概況

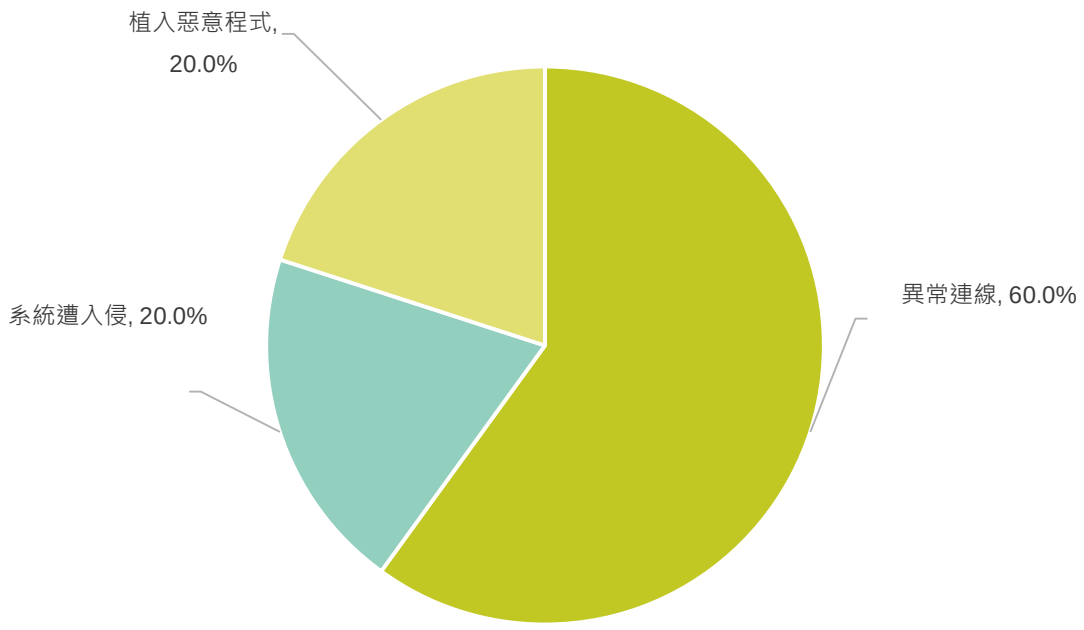

圖2 | 本週公務機關非法入侵事件類型占比

附註：自本期起，週報通報件數統計將不再納入網路攻防演練案件，僅保留一般資安事件通報。因過往統計包含演練案件，爰後續數據與歷期資料比較時，應留意統計基準不同。

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
➢ 攻擊者利用檔案上傳功能植入惡意程式 ➢ 遠端執行漏洞遭利用取得網站控制權	➢ 定期更新網站元件與套件版本，避免已知漏洞遭公開利用攻擊 ➢ 限制檔案上傳格式與執行權限，防止惡意程式上傳與執行 ➢ 強化網站存取與異常行為監控，即時發現可疑檔案操作行為 ➢ 停用未使用第三方元件功能，降低外部元件遭攻擊風險暴露

3間民間企業揭露重大資安訊息

本週3家民間企業發布重大訊息，產業類別分別為鋼鐵工業、數位雲端、其他電子業，詳見表1。

表1 | 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
彰源企業股份有限公司	115年5月11日	彰源公司的資訊系統遭受網路攻擊時，已立即啟動相關防禦機制。目前評估沒有個資、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。已委託國際級網路資訊安全處理公司協助解決，後續將持續提升網路與資訊基礎架構之安全控管，並持續密切監控，以確保資訊安全。
偉康科技股份有限公司	115年5月11日	偉康科技已針對駭客攻擊啟動防禦應變，目前評估對公司營運無重大影響，後續將持續強化資安管控。
鴻海精密工業股份有限公司	115年5月12日	鴻海集團位於北美的部分廠區遭受網路攻擊，第一時間資安團隊已啟動應變機制，並採取多項因應措施，確保生產與交付的連續性，目前受影響廠區之生產營運均維持正常。

■聯防監控

近一週以MITRE ATT&CK Matrix 分析攻擊者行為，建議加強對指令執行與日誌異常變更行為的監控，啟用集中式日誌保存機制，並針對可疑腳本與程序鏈進行行為分析，以降低攻擊者規避偵測的風險。

偵測刺探高居首位 防禦迴避仍具威脅

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。「偵測刺探」為最常見攻擊手法，占比15.5%，顯示攻擊者持續擴大對目標環境的前期偵查與資訊蒐集活動。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。攻擊者通常利用自動化工具對大量網段與公開服務進行探測，以識別可存取主機、開放埠及服務版本資訊，並同步蒐集與帳號憑證相關的資訊，作為後續登入攻擊或滲透行動的依據。部分活動呈現由大範圍掃描逐步聚焦特定目標的特徵，顯示其偵查行為具備明確目的性與階段性。此類行為雖多屬攻擊前期準備階段，但將直接影響後續攻擊成功率與精準度。建議組織加強對異常掃描流量與帳號探測行為的監控，定期盤點對外暴露資產，並結合威脅情資分析來源活動，以提前辨識潛在攻擊準備跡象。

「防禦迴避」事件本週占比為15.4%，為本週占比次高的攻擊階段，顯示攻擊者持續強化規避監控與降低偵測機率的能力，以隱藏其惡意活動痕跡。觀察到的主要手法包括削弱指令歷程記錄、間接指令執行、以及清除指令歷程。攻擊者可能透過停用或修改系統指令記錄機制，降低安全設備對操作行為的可視性，亦會利用合法程序或腳本間接執行惡意命令，以避免觸發傳統防護規則；部分案例中，攻擊者於完成操作後主動清除 Shell 或系統指令歷程，以掩蓋活動軌跡並阻礙事後鑑識。此類手法具高度隱蔽性，能有效延長攻擊者在環境中的潛伏時間。建議加強對指令執行與日誌異常變更行為的監控，啟用集中式日誌保存機制，並針對可疑腳本與程序鏈進行行為分析，以降低攻擊者規避偵測的風險。

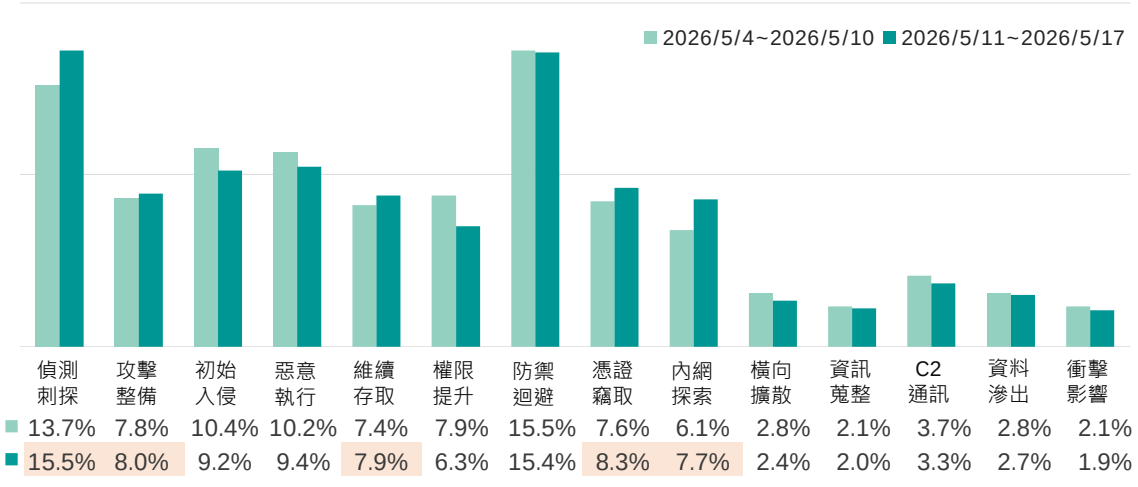

圖3 | 資安聯防監控攻擊階段統計

防護建議 **建議機關採取下列防護措施：**

偵測刺探（Reconnaissance）

- 強化異常掃描流量監控，偵測大量 IP 掃描與埠探測行為
- 定期盤點與下架不必要的對外服務及公開資產
- 限制管理介面對外曝露，降低被探測風險
- 導入威脅情資比對機制，識別惡意來源 IP 與掃描活動
- 加強帳號保護措施，如 MFA、多次登入失敗告警與帳號鎖定機制
- 監控憑證探測與異常登入嘗試，及早發現帳號蒐集行為

防禦迴避（Defense Evasion）

- 啟用集中式日誌保存，避免本機日誌遭竄改或刪除
- 監控指令歷程異常清除、停用紀錄功能等行為
- 強化 Shell、PowerShell、腳本執行紀錄與稽核設定
- 偵測異常程序鏈與間接指令執行行為（如 script interpreter、living-off-the-land 工具）
- 建立 EDR/XDR 行為分析規則，識別可疑腳本與隱匿操作
- 限制高權限帳號使用範圍，降低攻擊者操作空間
- 定期檢查安全機制與日誌服務狀態，避免遭停用或繞過

■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62.81%、「遠端控制」服務攻擊占比34.56%，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64.79%。「遠端控制」服務亦有30.72% 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Atlassian Confluence Server遠端程式碼執行漏洞的CVE-2024-21683，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。

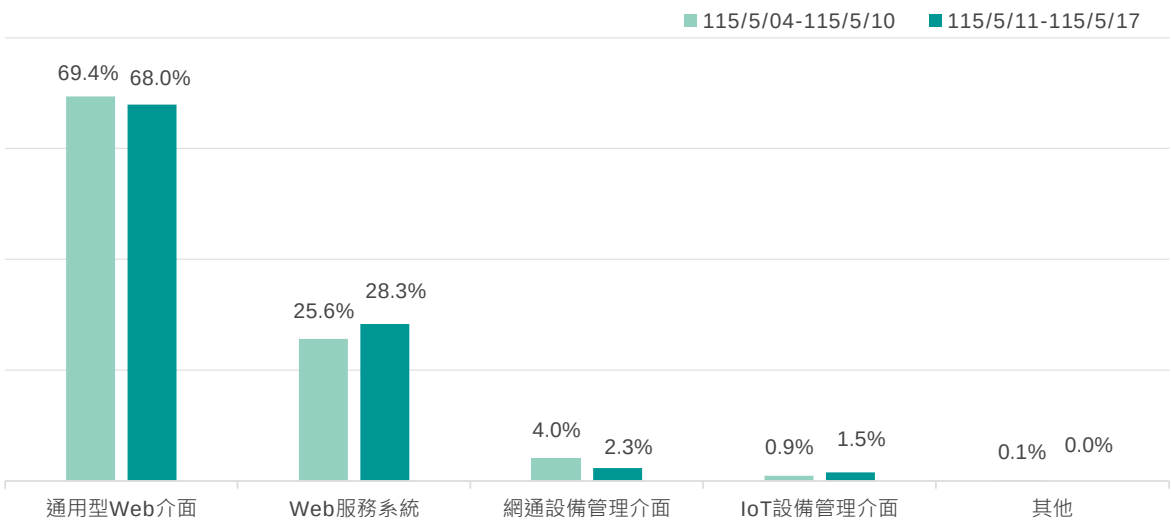

圖4 |本週網頁應用介面之誘捕攻擊比例統計

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2。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授權缺失漏洞、越界讀取漏洞、遠端程式碼執行漏洞、跨站請求偽造及作業系統命令注入漏洞，攻擊目標涵蓋企業級網路防火牆軟體、程式遞送控制器(ADC)、知識管理與團隊協作系統、Bootstrap Multiselect及PHP伺服器端腳本語言。

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2 | 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	⬆New	CVE-2025-20362[1]	Cisco Secure ASA&FTD	6.5
■	2	⬇1	CVE-2025-5777[2]	Citrix NetScaler ADC	7.5
■	3	⬆1	CVE-2024-21683[3]	Atlassian Confluence Server	8.8
■	4	⬆New	CVE-2025-47204[4]	Bootstrap Multiselect	6.1
■	5	⬇3	CVE-2024-4577[5]	PHP	9.8

類型 ■ 授權缺失漏洞 ■ 越界讀取漏洞 ■ 遠端程式碼執行漏洞
■ 跨站請求偽造 ■ 作業系統命令注入漏洞

▶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：

- 微軟釋出115年5月份安全性更新，共修補包含Azure DevOps、Microsoft Office SharePoint及SQL Server等共139個漏洞[6]，其中包含30個高風險漏洞與1個已遭利用之漏洞。

- Ivanti Endpoint Manager(EPM)與Endpoint Manager Mobile(EPMM)存在高風險安全漏洞(CVE-2026-5786[7]、CVE-2026-5787[8]及CVE-2026-8111[9])，類型分別為不當存取控制(Improper Access Control)、不當憑證驗證(Improper Certificate Validation)及SQL注入(SQL Injection)。
  - CVE-2026-5786：已通過身分鑑別之遠端攻擊者可取得管理者存取權限。
  - CVE-2026-5787：已通過身分鑑別之遠端攻擊者可冒充已註冊之Sentry主機，並取得有效CA簽章用戶端憑證。
  - CVE-2026-8111：已通過身分鑑別之遠端攻擊者可注入任意SQL指令進而執行任意程式碼。

- Fortinet FortiSandbox、FortiSandbox Cloud、FortiSandbox PaaS及FortiAuthenticator存在高風險安全漏洞(CVE-2026-26083[10]與CVE-2026-44277[11])，類型分別為缺乏授權(Missing Authorization)與不當存取控制(Improper Access Control)，未經身分鑑別之遠端攻擊者可透過發送特製請求執行未經授權之程式碼或指令。

1. https://nvd.nist.gov/vuln/detail/CVE-2025-20362
2. https://nvd.nist.gov/vuln/detail/cve-2025-5777
3. https://nvd.nist.gov/vuln/detail/cve-2024-21683
4. https://nvd.nist.gov/vuln/detail/CVE-2025-47204
5. https://nvd.nist.gov/vuln/detail/cve-2024-4577
6. https://msrc.microsoft.com/update-guide/releaseNote/2026-May
7. https://nvd.nist.gov/vuln/detail/CVE-2026-5786
8. https://nvd.nist.gov/vuln/detail/CVE-2026-5787
9. https://nvd.nist.gov/vuln/detail/CVE-2026-8111
10. https://nvd.nist.gov/vuln/detail/CVE-2026-26083
11. https://nvd.nist.gov/vuln/detail/CVE-2026-44277

■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

元件高風險漏洞風險上升 重大弱點修復時效仍待提升

本次針對100個曝險程度較高之A/B級政府機關進行EASM資安曝險檢測，前10大風險項目共計6,760項，詳見圖5。其中，「元件高風險漏洞」以4,185項居首，占比約61.9%，已逾整體6成，且高於其餘9項合計2,575項，為目前政府機關最主要之外部曝險來源。相關風險多集中於舊版Apache HTTP Server，後續各機關宜將其列為升級、修補與版本汰換之首要重點。「CSP設定不當」則以962項居次，「未部署WAF」以739項位居第三。前三項風險合計達5,886項，占前10大風險項目總數約87.1%，顯示外部曝險風險仍高度集中於元件漏洞、應用層邊界防護及安全標頭設定等三大面向。本期整體風險數量較上期6,370項增加390項，增幅約6.1%，整體曝險程度呈上升趨勢。

進一步觀察風險消長情形，「元件高風險漏洞」由上期3,860項增至4,185項，淨增325項，增幅約8.4%，占本期整體增加風險數量約83.3%，為推升整體風險的主要因素。「TLS憑證不受信任」由上期0項突增至49項，反映近期有部分機關網站對外憑證集中出現未及時展延、信任鏈異常或網域配置不符等維運疏漏，建議相關單位優先檢視網站之憑證有效性與網域配置。「未部署WAF」由上期694項增至739項，增加45項，增幅約6.5%，代表部分網站之前端應用層邊界防護仍需強化。相較之下，「CSP設定不當」及「過時或弱加密協定」變化幅度較小，整體大致持平。

另持續追蹤自3月5日起政府機關EASM重大弱點(Critical Findings)之修補成效，累計發現1,688個弱點。截至本期已有901個重大弱點完成修復，整體修復率達53.4%，顯示政府機關對重大威脅已陸續進行實質改善與曝險收斂。然而，修補時效仍有精進空間。統計顯示，於弱點發現後30天內即完成修補改善者僅有375個(修補率22.2%)；迄今仍有787個弱點尚未完成改善(未修補率達46.6%)，導致外部受攻擊面暴露時間過長。目前尚未修補之項目主要集中於「元件高風險漏洞」(595個)與「不安全的對外服務」(188個)，後續將列為優先追蹤與改善重點，以加速弱點修復並降低政府機關外部曝險。

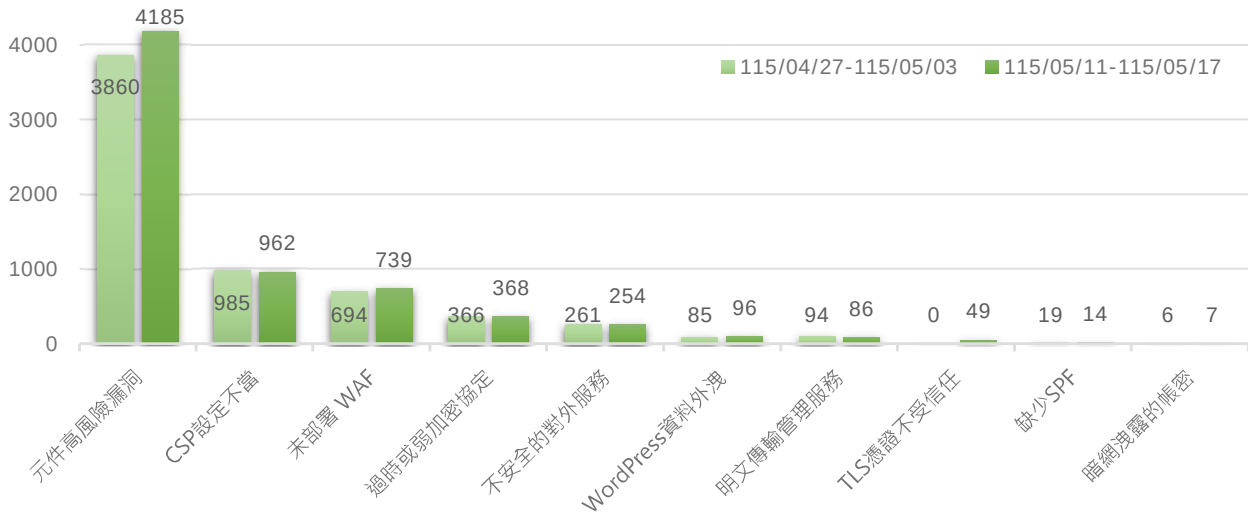

圖5 | EASM檢測結果統計(前10大風險)

防護建議

建議機關或關鍵基礎設施採取下列防護措施

- 優先盤點對外網站使用之元件版本，針對舊版Apache HTTP Server等高風險元件儘速修補或升版
- 修正CSP設定不當問題，導入必要網站安全標頭，降低XSS攻擊及惡意腳本載入風險
- 針對重要對外網站逐步部署WAF，並搭配規則調校與警示監控，強化應用層防護能力
- 停用未加密連線、舊版或弱加密協定，全面採用TLS1.2以上版本；遠端管理服務應使用加密通道，並限制來源IP
- 關閉不必要之對外服務，定期盤點已停用站台、主機及應用系統，避免資產持續對外曝露

建議機關或關鍵基礎設施採取下列管理措施

- 建立元件漏洞優先修補機制，針對高風險及已遭利用之漏洞設定改善期限，並追蹤複測結果
- 將CSP、WAF、加密協定及對外服務設定納入例行檢核，定期追蹤未改善項目
- 強化對外資產生命週期管理，確認測試站、舊站台及停用服務均已完成下線

■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IoT設備管理介面曝險與弱密碼風險

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5/15止已累計42筆攻擊紀錄，依弱點數量排名前3名依序為「不安全的組態設定」15筆、「注入攻擊」11筆及「無效的存取控管」6筆，詳見圖6。經演練發現，部分IoT設備與其設備管理服務存在不安全的組態設定情形，導致攻擊者可直接存取管理介面，並使用預設帳號密碼或弱密碼登入後取得帳號管理權限，成功新增使用者帳號。此外，攻擊者可透過新增帳號存取設備服務，並進一步取得設備資訊與使用者清單。

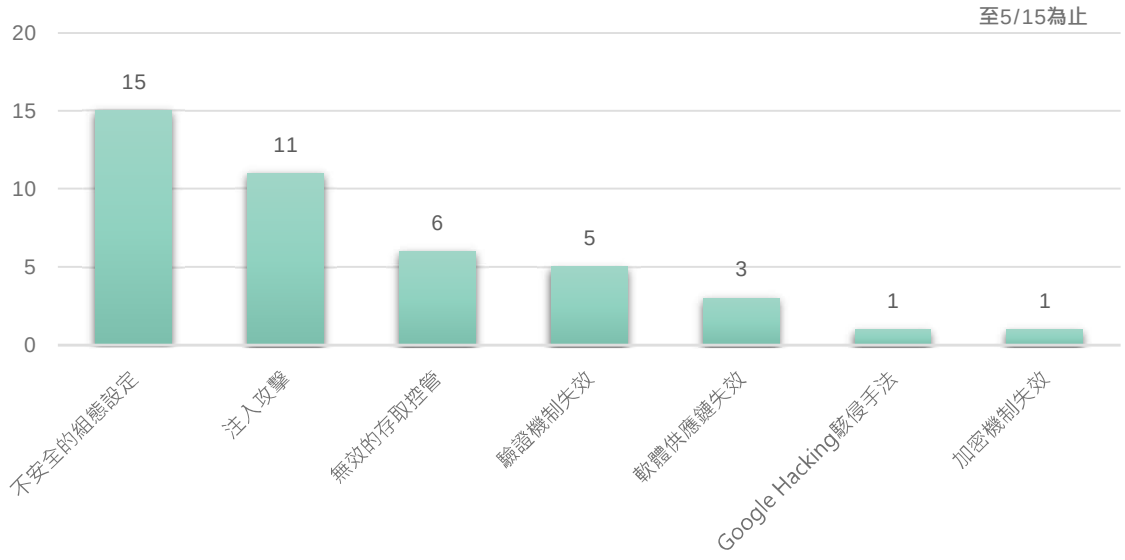

圖6 | 網路攻防演練資通系統實兵演練統計

建議機關及關鍵基礎設施提供者，採取下列防護措施

- 應定期檢視對外開放之服務與通訊埠，關閉非必要對外服務埠，避免管理介面暴露於外網
- 設備啟用後應立即停用預設帳號或修改預設密碼，並建立高強度密碼
- 針對管理介面應限制存取來源IP，以降低未經授權存取風險

焦點文章

從被動到主動—中小企業資安治理的轉向

各國正透過能力建構、基準設定與驗證誘因，協助中小企業因應日益普遍的資安風險

中小企業是各國推動數位轉型的重要主體，但在數位化程度提升的同時，資安風險也已成為不可忽視的經營風險。Hiscox《Cyber Readiness Report 2025》指出，在近 6,000 家、橫跨七個國家的受訪中小企業中，有 59% 表示過去 12 個月曾遭遇網路攻擊[1]。英國政府《Cyber Security Breaches Survey 2025》亦指出，43% 受訪企業在過去 12 個月曾遭遇資安侵害或攻擊[2]。這顯示資安事件對企業而言，已非少數個案，而是高度普遍的經營風險。

中小企業的問題，不只是防護不足，更是治理不足

從實務面來看，中小企業面臨的關鍵挑戰，往往不在於完全沒做資安，而在於尚未把零散措施轉化為可持續、可管理的治理機制。日本 IPA 於2025年5月公布的調查顯示，約七成企業已做到作業系統與防毒軟體更新，但在威脅情報掌握與內部共享、將資安措施規則化並明示予員工、以及事故應變體制等較具治理性質的作法上，落實比例均僅約四成左右[3]。這反映許多中小企業雖已有基礎技術防護，卻仍停留在個別、零散的應對，尚未進入制度化治理階段。

資安弱點會外溢到交易對象與供應鏈

中小企業資安治理薄弱，影響的不只是企業自身，也可能波及交易對象與供應鏈。IPA 調查同樣指出，在所有曾遭不當存取的受害企業中，有 19.8% 表示攻擊是經由交易對手、集團企業等作為入侵途徑；另在遭遇資安事件的企業中，認為該事件有對其營運造成影響的企業中，約七成表示事件亦對交易對象造成影響。換言之，中小企業一旦出現資安事件，不僅可能造成自身資料外洩、營運中斷，也可能成為供應鏈入侵與風險擴散的入口。

各國政策走向：從技術防護走向治理、基準與驗證

近年各國政府特別針對中小企業資安治理的政策工具，大致可歸納為三個方向。

第一，資安責任上移到高階管理層，將資安納入企業治理與整體風險管理。英國國家網路安全中心（NCSC） 於 2025 年發布《網路治理實務守則》（Cyber Governance Code of Practice），其目的即在協助董事會與董事治理資安風險，並指出該守則係為董事會與董事

焦點文章

所設計，而非僅供日常資安管理人員使用[4]。美國NIST的《網路安全框架 2.0》（Cyber Security Framework 2.0, CSF 2.0）亦將「治理」（Govern）納入核心功能，把資安擴張到組織治理、風險容忍與管理責任[5]。

第二，建立中小企業可負擔的最低治理能力。例如澳洲2025年的《小企業資安指引》除提供企業基礎資安措施外，也建議已完成該等措施的企業，可逐步朝該國資安成熟度第一級邁進[6]。加拿大政府亦建議中小企業可優先從事件應變計畫、系統與應用程式修補、強化身分驗證、備份與加密等基礎控制做起，循序建立最低防護與管理能力[7]。

第三，提升可驗證性與市場誘因。此部分做法如新加坡網路安全局推動的 Cyber Essentials 認證，特別透過低門檻的基礎驗證、驗證費補助、顧問協助等誘因，鼓勵中小企業申請標章驗證，期望既能讓中小企業採取可被驗證的基本資安措施，並可一併提供對外信任標示等誘因，讓其更容易做得起、做得到，也看得到效益[8]。

若從法制趨勢觀察，政策焦點也不只是擴大納管，而是依部門重要性、規模與風險程度，逐步把資安要求嵌入治理與供應鏈責任架構。以歐盟 NIS2 為例，其原則上將特定部門中的中型與大型企業納入範圍，並保留會員國將高風險小型實體納入的裁量。這顯示中小企業政策設計的重點，不必然是比照大型企業加重合規要求，而是建立與其規模相稱、可持續執行的最低治理能力。

從能力建構走向治理導向：我國中小企業資安政策的下一步

就我國現況而言，現行《資通安全管理法》納管對象包括公務機關及特定非公務機關；後者包含關鍵基礎設施提供者、公營事業、特定財團法人及受政府控制之事業、團體或機構，一般中小企業並非直接法定納管對象。

儘管在實務上，中小企業業已透過政府採購、委外與供應鏈要求，被間接納入資安責任體系。但整體而言，我國目前對中小企業之資安政策仍以輔導、補助及能力建構為主，考量我

國中小企業占整體企業的比例極高，且普遍面臨資源、人力與專業能力限制，此類以輔導與能力建構為核心的政策措施在協助企業建立基本資安意識與初步防護能力方面，仍有重要作用。例如數發部資通安全署在2026年4月中發布的《中小企業基本資安防護指引》[9]，或是2026 年初與經濟部及資安院合作推出「中小企業基本資安諮詢服務」、「中小企業資安教育訓練影片」及「資安星際指南」等工具，即為此一政策方向的具體展現[10]。

展望未來，我國若要進一步補強中小企業資安治理，政策上或可優先從三個面向著手：一是把資安從 IT 問題提升為經營治理議題；二是建立適合中小企業、低負擔但可持續的最低治理基準；三是透過驗證、採購誘因與產業輔導，提高中小企業資安能力的可驗證性。藉由基礎能力建構逐步銜接至治理機制強化，以降低個別企業資安脆弱性外溢為供應鏈乃至整體產業系統性風險的可能。

參考文獻

1. “ Hiscox Cyber Readiness Report 2025 ” Hiscox. November 6, 2025. https://www.hiscoxgroup.com/hiscox-cyber-readiness-report-2025.
2. “ Cyber Security Breaches Survey 2025. ” GOV.UK. April 10, 2025. https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2025/cyber-security-breaches-survey-2025.
3. “「2024年度 中小企業における情報セキュリティ対策に関する実態調査」” IPA 独立行政法人情報処理推進機構. 2024. https://www.ipa.go.jp/security/reports/sme/sme-survey2024.html.
4. “ Cyber Governance Code of Practice. ” GOV.UK. April 7, 2025. https://www.gov.uk/government/publications/cyber-governance-code-of-practice/cyber-governance-code-of-practice.
5. “ The NIST Cybersecurity Framework (CSF) 2.0. ” NIST. 2024. https://doi.org/10.6028/nist.cswp.29.
6. “ Small Business Cyber Security Guide ” Australia Government & Australian Signals Directorate. 2023. https://www.cyber.gov.au//sites/default/files/2025-03/Small%20business%20cybersecurity%20guide%20%28January%202025%29.pdf. 該指引初版為 2023 年，2025年1月為最新版。

7. “ Top Measures to Enhance Cyber Security for Small and Medium Organizations (ITSAP.10.035). ” Canadian Centre for Cyber Security. June 1, 2021. https://www.cyber.gc.ca/en/guidance/top-measures-enhance-cyber-security-small-and-medium-organizations-itsap10035.
8. “ Certification for the Cyber Essentials Mark. ” Cyber Security Agency of Singapore. 2026. https://www.csa.gov.sg/our-programmes/support-for-enterprises/sg-cyber-safe-programme/cybersecurity-certification-for-organisations/cyber-essentials/certification-for-the-cyber-essentials-mark/.
9. “ 資安署發布中小企業基本資安防護指引 三大面向16項檢核協助產業防駭 ” 數位發展部. 2026. https://moda.gov.tw/ACS/press/news/press/19496.
10. “ 數發部資安署攜手經濟部中企署與資安院 打造中小企業資安防護體系. ” 數位發展部. 2026. https://moda.gov.tw/ACS/press/news/press/18810.

關鍵字：中小企業 、供應鏈資安、資安治理基準、管理層責任 、資安驗證

刊　　名　資安週報第 45 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