



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

EASM曝險風險續降 CSP設定改善最明顯

重大漏洞

WatchGuard、Ivanti、MikroTik、HPE、Check Point、Cisco
及Microsoft高風險漏洞應盡速修補

實兵演練

實兵演練揭露API權限控管不當 致使用者個人資料遭未授權存取
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

程式遞送控制器(ADC&Gateway)及大模型API統一介面與代理伺
服器工具成攻擊熱點

事件通報

以Base64取代明文僅屬編碼轉換 無法實質保護驗證資訊

網路巡查高風險詐騙

產品服務占比回升居首 金融投資仍居第二

焦點文章

最新國際產品資安政策趨勢

2026.09.24

063

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

EASM曝險風險續降 CSP設定改善最明顯

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8,070項。其中，「元件高風險漏洞」以3,273項居首，「過時或弱加密協定」1,593項次之，「TLS憑證不受信任」1,289項位居第三。前三項合計6,155項，占前10大風險項目總數約76.3%，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8,415項，本期整體風險數量減少345項，降幅約4.1%，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3,316項減至本期3,273項，降幅約1.3%。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。「過時或弱加密協定」由1,606項減至1,593項，降幅約0.8%；「TLS憑證不受信任」由1,315項減至1,289項，降幅約2.0%。另「未部署WAF」由766項增至767項，增幅約0.1%；「CSP設定不當」由985項大幅降至763項，降幅約22.5%。

整體而言，本期外部曝險風險呈下降趨勢，其中以「CSP設定不當」改善幅度最為明顯；惟「元件高風險漏洞」仍為主要風險來源，建議持續加強高風險元件修補、網站應用防護及相關安全設定，以降低外部曝險風險。

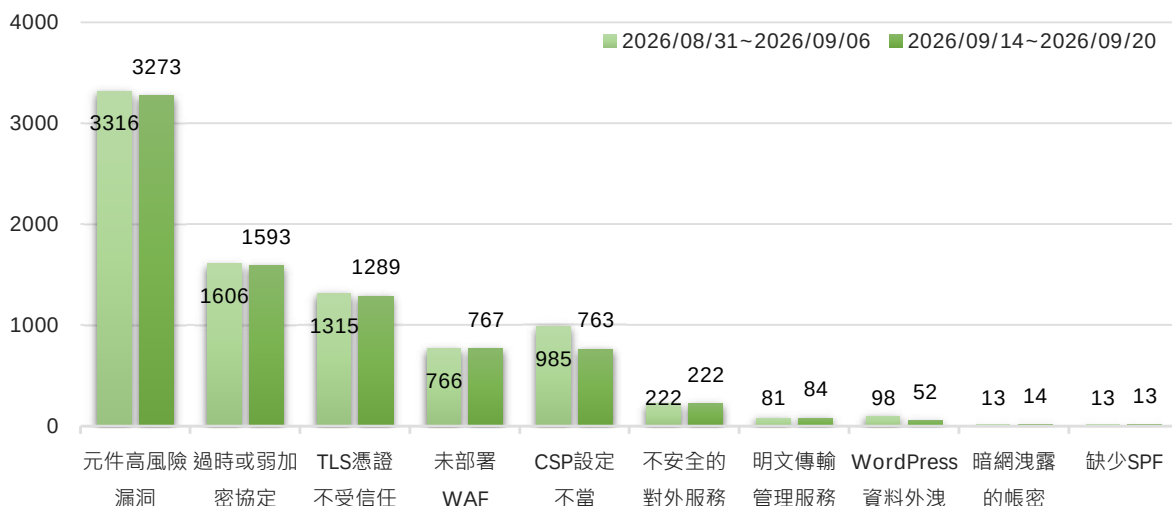


圖1 | EASM檢測結果統計(前10大風險)

防護建議

建議受測單位採取下列防護措施

- 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

建議受測單位採取下列管理措施

- 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

WatchGuard、Ivanti、MikroTik、HPE、Check Point、Cisco及Microsoft 高風險漏洞應盡速修補

- WatchGuard Fireware OS存在多項高風險安全漏洞(CVE-2026-13086、CVE-2026-19313、CVE-2026-19315及CVE-2026-19318)[1]，類型包含堆疊型緩衝區溢位(Stack-based Buffer Overflow)、堆積型緩衝區溢位(Heap-based Buffer Overflow)及類型混淆(Type Confusion)。
 - CVE-2026-13086：已停止支援之 Mobile Security 功能，其端點保護管理(Endpoint Protection Manager)服務存在堆疊型緩衝區溢位漏洞，未經身分鑑別之遠端攻擊者可利用此漏洞執行任意程式碼。
 - CVE-2026-19313：iked程序存在堆積型緩衝區溢位漏洞，未經身分鑑別之遠端攻擊者可傳送特製網路封包，進而執行任意程式碼。
 - CVE-2026-19315：iked程序存在類型混淆漏洞，未經身分鑑別之遠端攻擊者可傳送特製網路封包，進而執行任意程式碼。
 - CVE-2026-19318：iked程序存在堆疊型緩衝區溢位漏洞，未經身分鑑別之遠端攻擊者可傳送特製網路封包，進而執行任意程式碼。
- Ivanti Neurons for ITSM存在8個高風險安全漏洞(CVE-2026-12645至CVE-2026-12648、CVE-2026-12650、CVE-2026-12651、CVE-2026-12744及CVE-2026-12745)[2]，類型包含缺乏授權(Missing Authorization)與不安全之反序列化(Insecure Deserialization)，其中最嚴重之漏洞可使未經身分鑑別之遠端攻擊者，於伺服器執行任意程式碼。
- HPE Aruba Networking AOS-CX存在6個高風險安全漏洞(CVE-2026-73749至CVE-2026-73753與CVE-2026-73782)[3]，類型包含不當存取控制(Improper Access Control)、指令注入(Command Injection)、路徑遍歷(Path Traversal)、作業系統指令注入(OS Command Injection)及使用外部控制之格式化字串(Use of Externally-Controlled Format String)，其中最嚴重之漏洞可使未經身分鑑別之遠端攻擊者，藉由對受影響服務傳送特製封包，進而以較高權限執行任意程式碼。

- MikroTik RouterOS 存在多項高風險安全漏洞 (CVE-2026-67276 與 CVE-2026-86060)[4]，類型包含加密簽章驗證不當(Improper Verification of Cryptographic Signature)與引數注入(Argument Injection)，其中CVE-2026-86060已遭駭客濫用。
 - CVE-2026-67276：未經身分鑑別之遠端攻擊者可利用RouterOS未完整比對SSH授權金鑰之驗證機制缺陷，於已知授權RSA模數情況下，使用指數為1之偽造金鑰產生有效簽章，進而於未持有私鑰之情況下，以目標使用者身分建立SSH命令通道。
 - CVE-2026-86060：攻擊者可透過建立未經身分鑑別之SSH連線，觸發RouterOS登入輔助程式(Login Helper)，並利用SSH登入路徑之引數處理缺失，使用以特定禁用字元開頭之使用者名稱，變更受信任之RouterOS政策遮罩(Policy Mask)，進而提升權限。
- Check Point 多項產品存在多項高風險安全漏洞 (CVE-2026-85102 與 CVE-2026-85103)[5][6]，類型包含不當憑證驗證(Improper Certificate Validation)與堆積型緩衝區溢位(Heap-based Buffer Overflow)。
 - CVE-2026-85102：VPN協商過程中存在不當憑證信任驗證之缺失，未經身分鑑別之遠端攻擊者可利用此漏洞，進而執行任意程式碼。
 - CVE-2026-85103：VPN憑證ASN.1格式解碼流程存在堆積型緩衝區溢位之缺失，未經身分鑑別之遠端攻擊者可利用此漏洞，進而執行任意程式碼。
- Ivanti Endpoint Manager Mobile(EPMM)存在缺乏授權(Missing Authorization)漏洞 (CVE-2026-18851)[7]，已通過身分鑑別之遠端攻擊者，可利用此漏洞取得管理者權限。
- Cisco Secure Email Gateway(SEG)與Secure Email and Web Manager(SEWM)存在多項高風險安全漏洞 (CVE-2026-20353、CVE-2026-76440、CVE-2026-76441、CVE-2026-76443及CVE-2026-76461)[8][9]，類型包含生命週期內資源控制不當(Improper Control of a Resource Through its Lifetime)、路徑遍歷(Path Traversal)、不當存取控制(Improper Access Control)、不當資料清理(Improper Neutralization)及SQL注入(SQL Injection)，其中CVE-2026-76461已遭駭客濫用。

- CVE-2026-20353、CVE-2026-76440、CVE-2026-76441 及 CVE-2026-76443：
未經身分鑑別之遠端攻擊者可利用上述漏洞，造成系統之機密性、完整性及可用性受影響。
 - CVE-2026-76461：Cisco SEG之AsyncOS軟體存在郵件解析邏輯驗證不足之缺失，
未經身分鑑別之遠端攻擊者，可向受影響設備傳送含有惡意SQL語法之特製郵件，
進而於底層作業系統以root權限執行任意指令。
- 微軟釋出 115 年 9 月份安全性更新，共修補包含 Microsoft Exchange Server、Microsoft Office及SQL Server等共978個漏洞[10]，其中包含193個高風險漏洞，且 CVE-2026-81963與CVE-2026-85880已遭駭客利用。

1. <https://www.watchguard.com/wgrd-blog/immediate-action-required-update-your-firebox-now>
2. https://hub.ivanti.com/s/article/Security-Advisory-Ivanti-Neurons-for-ITSM-Multiple-CVEs?language=en_US
3. https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbnw05134en_us&docLocale=en_US
4. <https://mikrotik.com/supportsec/september-2026-vulnerability/>
5. <https://support.checkpoint.com/results/sk/sk1000117>
6. <https://support.checkpoint.com/results/sk/sk1000118>
7. https://hub.ivanti.com/s/article/Security-Advisory---Ivanti-Endpoint-Manager-Mobile-CVE-2026-18851?language=en_US
8. <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-hardening-esa-dfCrfXkm>
9. <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-esa-inj-2bLVGmhX>
10. <https://msrc.microsoft.com/update-guide/releaseNote/2026-Sep>

■ 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API權限控管不當 致使用者個人資料遭未授權存取風險

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9/18止已累計381筆攻擊紀錄，本週新增弱點數量共11筆，分別為「無效的存取控管」7筆、「軟體供應鏈失效」2筆、「不安全的組態設定」1筆及「注入攻擊」1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」。攻擊者使用工具掃描標的網站，發現系統API介面，進一步瀏覽相關功能並逐步操作API，於API中欄位輸入測試字元取得使用者之UserId。攻擊者再將取得之UserId帶入其他API功能進行測試，發現系統未進行適當之身分驗證與存取權限控管，即回傳該使用者相關機敏資料，導致未經授權之使用者可透過API取得其他使用者之敏感個資，造成個人資料遭未授權存取之風險。

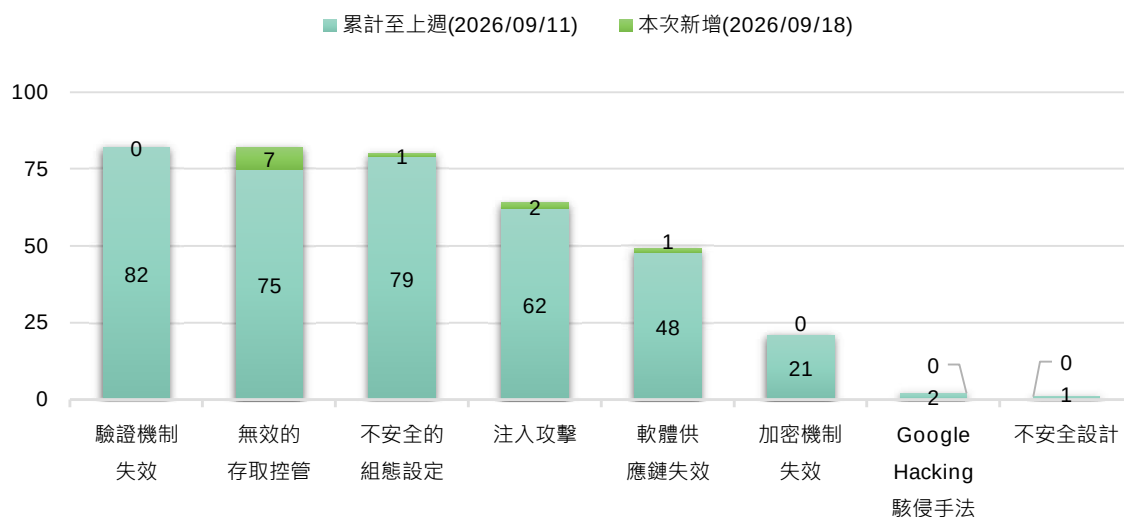


圖2 | 網路攻防演練資通系統實兵演練統計

建議機關及關鍵基礎設施提供者，採取下列防護措施

- 應限制API功能之存取權限，避免未經授權使用者透過公開API取得系統資料
- 應檢視API介面之對外暴露範圍，非必要之API不應直接對外開放，並應透過適當之存取控管機制限制外部使用者存取
- 針對機敏資訊應依資料敏感程度採取適當之遮罩、去識別化或其他保護措施，降低敏感資料遭未授權取得之風險

■ 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 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14.1%，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。

「偵測刺探」事件本週占比為12%，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弱點探測行動。觀察到的主要手法包括主動式掃描、IP 區段掃描、以及漏洞掃描。攻擊者透過自動化工具對大範圍網段進行探測，以識別對外服務、開放埠與系統類型，並進一步針對潛在弱點進行漏洞評估，尋找可利用的攻擊入口。此類行為通常呈現由廣泛掃描逐步聚焦的特徵，顯示其攻擊流程具備階段性與目標導向。由於此階段多發生於攻擊初期，若未及時偵測，將提高後續入侵成功機率。建議加強對異常掃描流量的監控與分析，導入漏洞管理與修補機制，並結合威脅情資比對掃描來源，以提前掌握潛在攻擊準備行為。

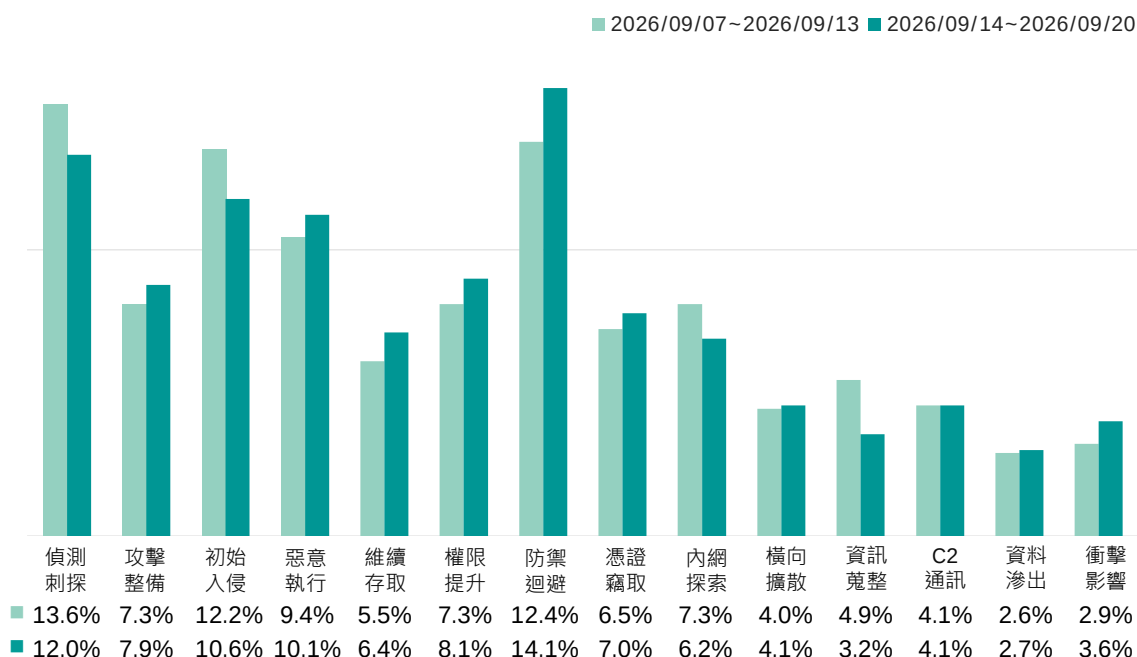


圖3 | 資安聯防監控攻擊階段統計



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 EDR 偵測機制，
監控異常指令及系統工具使用行為



加強 PowerShell、Command
Shell 等指令操作紀錄與集中留存，
避免紀錄遭竄改或刪除



限制高風險系統工具及管理權限，
落實最小權限與特權帳號管理



建立日誌停用、清除或異常中斷的
告警機制，及早發現規避偵測行為



偵測刺探 (Reconnaissance)



加強外部網路掃描、異常連線及大
量探測行為的監控與告警



定期盤點對外服務、開放埠及暴露
資產，降低不必要的外部曝險



落實弱點掃描、風險評估及修補作
業，優先處理高風險與已知遭利用
弱點



結合威脅情資比對掃描來源 IP，針
對高風險來源進行封鎖或提高監控
強度

■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

程式遞送控制器(ADC & Gateway)及大模型API統一介面與代理伺服器工具成攻擊熱點

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71.73%、「遠端控制」服務攻擊占比25.66%，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75.95%。「遠端控制」服務亦有21.13%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Citrix NetScaler ADC & Gateway 記憶體資料外洩漏洞之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。

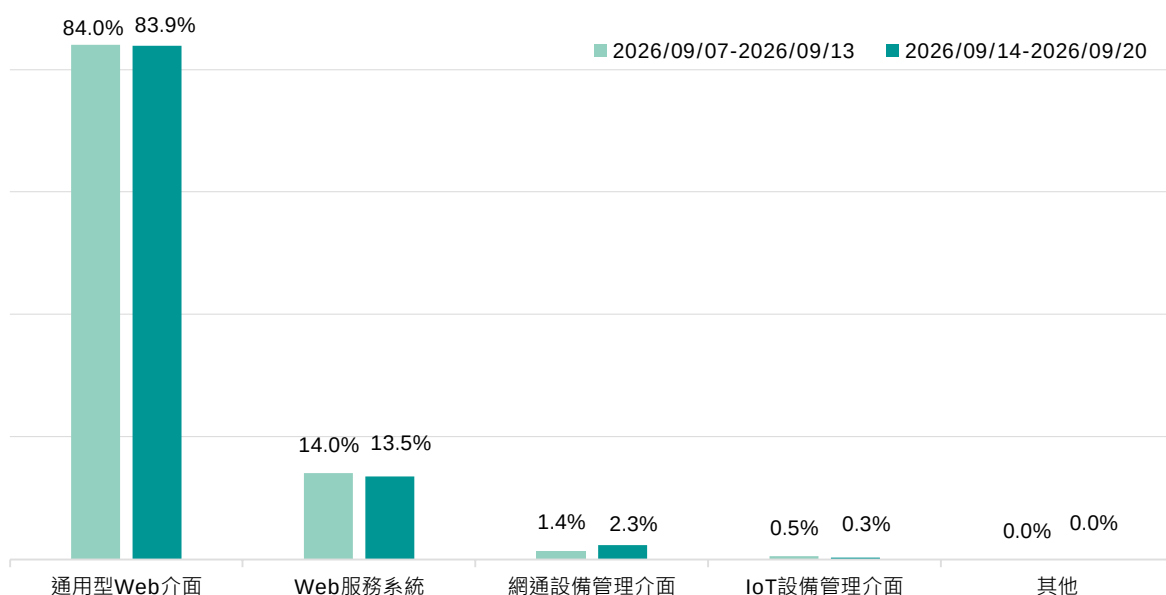


圖4 | 本週網頁應用介面之誘捕攻擊比例統計

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越界讀取漏洞、指令注入漏洞及身分驗證繞過漏洞，攻擊目標涵蓋程式遞送控制器(ADC&Gateway)、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、企業級郵件伺服器軟體及資安防護系統與雲端檔案管理平台。

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	↑1	CVE-2026-3055 ¹	NetScaler ADC & Gateway	9.8	✓
■	2	↑1	CVE-2026-42271 ²	LiteLLM	8.8	✓
■	3	↓2	CVE-2026-41940 ³	cPanel & WHM	9.8	✓
■	4	↑new	CVE-2026-24423 ⁴	SmarterTools SmarterMail	9.8	✓
■	5	↓1	CVE-2026-2699 ⁵	Progress ShareFile	9.8	

類型 ■ 越界讀取漏洞

■ 指令注入漏洞

■ 身分驗證繞過漏洞

1. <https://nvd.nist.gov/vuln/detail/CVE-2026-3055>
2. <https://nvd.nist.gov/vuln/detail/CVE-2026-42271>
3. <https://nvd.nist.gov/vuln/detail/CVE-2026-41940>
4. <https://nvd.nist.gov/vuln/detail/CVE-2026-24423>

5. <https://nvd.nist.gov/vuln/detail/CVE-2026-2699>

■ 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

以Base64取代明文僅屬編碼轉換 無法實質保護驗證資訊

本週總計接獲26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。本週發現機關網站驗證碼機制存在設計缺失，網站將驗證碼答案以Base64編碼後，直接包含於前端回傳的路徑資訊中，攻擊者僅需解碼即可取得驗證碼明文，無須實際辨識驗證碼內容。由於Base64僅屬資料編碼，並非加密保護，此設計可能使驗證碼失去阻擋自動化操作之效果，進而遭利用進行大量查詢、資料爬取或帳號密碼嘗試等行為。

建議驗證碼答案應由伺服器端產生及驗證，前端僅傳送使用者輸入內容及無法推導答案的識別資訊，不應將正確答案以明文、Base64或其他可還原形式回傳至瀏覽器。驗證碼亦應設定有效期限、單次使用及與當次操作或工作階段綁定，並搭配查詢頻率限制、連續失敗偵測及異常大量操作監控，避免驗證碼遭繞過後即可持續自動化存取。

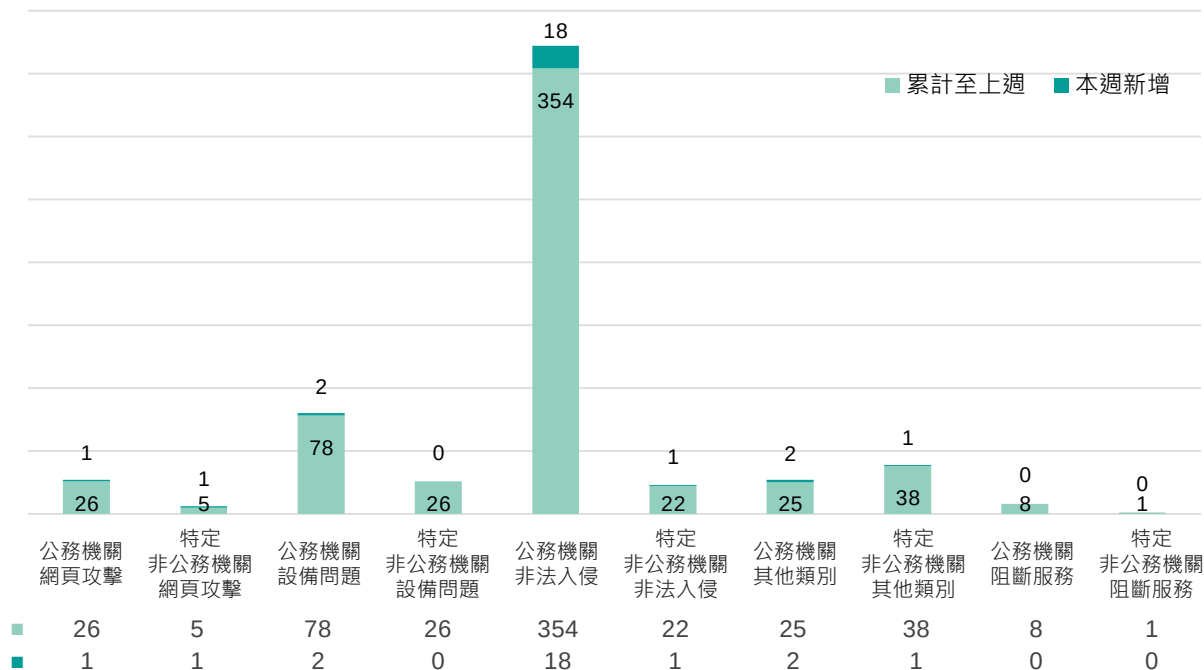


圖5 | 本週公務機關暨特定非公務機關資安事件通報概況

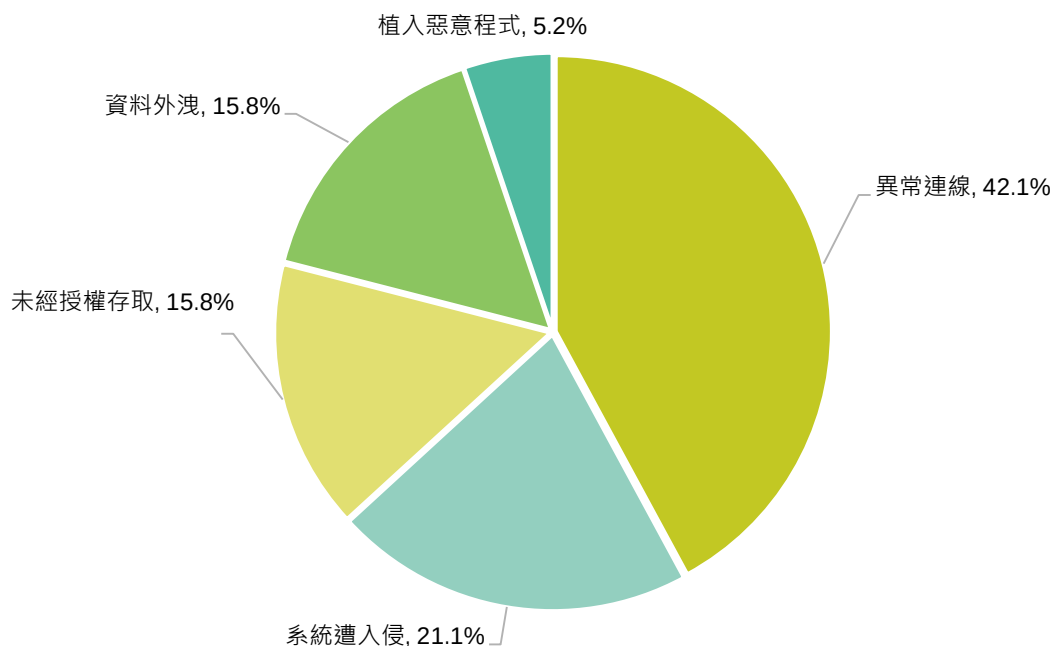


圖6 | 本週公務機關非法入侵事件類型占比

防護建議

除修補漏洞外，應：

以攻擊為出發評估潛在風險

- 攻擊者解碼取得驗證碼答案繞過自動化操作防護機制
- 驗證碼失效後遭大量查詢爬取資料或嘗試帳號密碼

針對潛在風險執行相應改善

- 驗證碼答案應於伺服器端產生及驗證，不得以可還原形式傳送前端
- 驗證碼應設定有效期限及單次使用，並與當次操作或工作階段綁定
- 建立查詢頻率與連續失敗限制，降低自動化大量操作及暴力嘗試風險
- 強化異常操作行為監控與告警，及早發現大量查詢及資料爬取行為

6間民間企業揭露重大資安訊息

本週6間民間企業發布重大訊息，產業類別為電子零組件業、航運業、通信網路業、居家生活業、其他，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
崑崙精密科技股份有限公司	2026年09月14日	崑崙於9月14日上午發現資訊系統遭駭客入侵，部分系統資料遭加密鎖定，已立即啟動資安應變機制，進行網路斷線及系統隔離，並委請外部資安團隊進駐協助調查及復原。受影響範圍包含公司網路系統、電子郵件系統及部分業務營運相關系統，未影響工廠生產作業，目前尚未發現機密資料或個人資料外洩之具體跡證。網路及電子郵件系統預計於當日晚間恢復，業務營運相關系統預計於二至三日內逐步恢復，事件處理成本約新台幣100萬元，經初步評估對財務及業務營運無重大影響。後續將持續配合資安團隊調查與監控，並強化端點防護、網路監控、帳號權限管理及資安教育訓練。
長榮航空股份有限公司	2026年09月15日	長榮航空發現有不明人士透過惡意IP入侵公司內部資訊環境，取得員工姓名與公務聯繫資訊，已立即依公司程序應變並採取必要防護措施，同時主動通報相關主管機關，並公告全體同仁知悉。目前評估對公司所有業務均不受影響，後續將重新檢視可能造成資安疑慮的因子並持續加強監控。

表2 | 本週民間企業重大資安訊息彙整 (續)

公司名稱	發布時間	事件說明
長榮航太科技股份有限公司	2026年09月15日	長榮航太發現部分內部資訊系統遭受網路攻擊，已即刻啟動資安應變機制，對受影響設備進行隔離，並委請外部資安技術團隊協助鑑識，後續將依程序向主管機關通報。經初步評估，核心資訊系統及營運業務運作皆維持正常，尚未發現公司及涉客戶或第三方敏感個資外洩情事。後續將持續監控整體資訊系統運作狀況，並檢討強化現有資安防護措施。
友訊科技股份有限公司	2026年09月18日	友訊於網站監控中發現登入記錄異常，查知外部攻擊者利用既有登入機制，以大量帳號密碼進行網站登入驗證，已立即啟動緊急應變機制，並進行系統登入紀錄清查、可疑連線封鎖及全站程式碼安全檢視。截至公告時未再發現相同方式之異常登入行為，網站服務維持正常運作，目前評估對公司營運尚無重大影響。後續將強化網站登入驗證、存取控制、異常行為偵測及網頁應用程式防火牆，委請資安專家檢視系統架構與防護機制，並通知受影響用戶及提供聯繫管道。
萬達寵物事業股份有限公司	2026年09月19日	萬達寵物陸續接獲少數客戶反映遭遇疑似第三人取得消費資料、並以電子郵件聯繫之疑似個資外洩情事，目前已針對公司系統進行資料保存及調查事件詳情。截至目前對公司財務或業務並無重大影響，如有任何發現，將進行必要資安防護升級。

表2 | 本週民間企業重大資安訊息彙整 (續)

公司名稱	發布時間	事件說明
威旭數據科技股份有限公司	2026年09月20日	威旭發生電話系統資安事件(事實發生日為9月18日)，因公司電話遭電信警察通報為詐騙電話，目前已暫停使用。公司已向165反詐騙專線通報，並配合警政及電信單位進行電話狀態管制(暫停受話 / 限制撥入)，同時要求電話系統廠商全面進行資安清查與防護機制強化。客戶仍可透過電話以外的方式聯繫公司，目前對營運尚無影響。後續將於官網及社群媒體發布打詐公告，與電信公司及電話系統廠商確認IP位址，依規定向警政機關報案並於核定後申請復話，並持續強化資訊安全。

■ 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

產品服務占比回升居首 金融投資仍居第二

詐騙類型趨勢

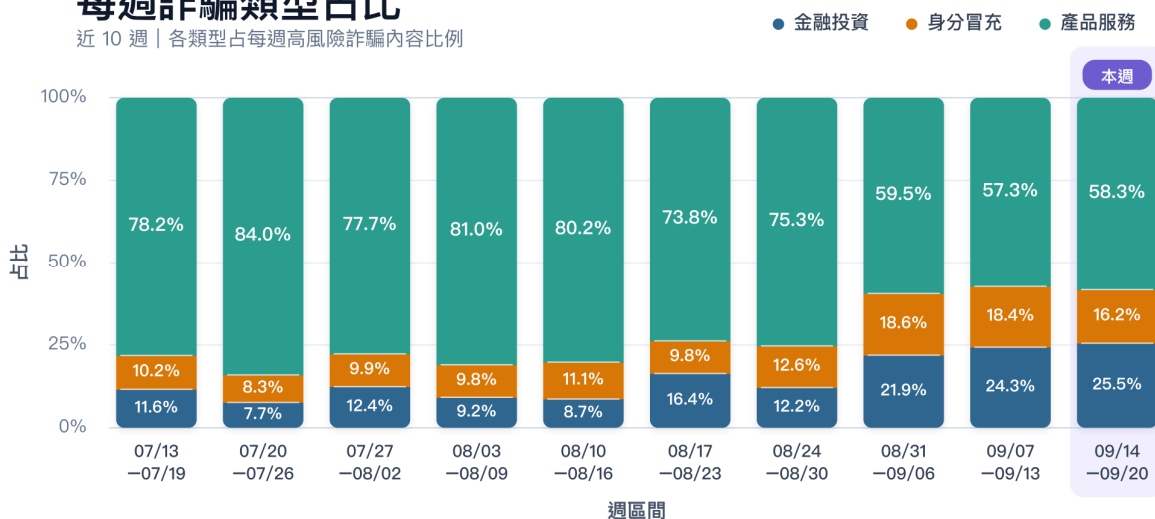
本週金融投資型占比續升，仍居第二，詳見圖7，相關內容以理財規劃、股票期貨教學與選股工具吸引民眾。廣告結合講師投資經歷、交易策略與資金流向分析，營造專業形象，再引導民眾報名免費體驗課程，或點擊了解選股應用程式的功能。

身分冒充型占比回落，相關眼霜廣告以醫師名義宣傳，並宣稱可掃碼驗證真偽、由台灣原廠出貨，搭配假一賠十承諾建立信任。內容另宣稱能改善眼袋與細紋，再用限量、降價及買四送四促購，將醫師名義與真品保證包裝成下單理由。

產品服務型占比回升，仍居本週首位，相關購車與服飾團購廣告皆以優惠訴求吸引民眾。購車廣告主打免繳半年車貸、較低的每月還款金額及線上下訂金折扣；服飾團購則結合中秋限定、多件優惠與正品保證，附上購買連結吸引下單。

每週詐騙類型占比

近 10 週 | 各類型占每週高風險詐騙內容比例



註：各週三類占比合計為 100%；本週以淡色區塊標示。

資料期間：2026/07/13—09/20

圖7 | 每週詐騙類型占比

關鍵字趨勢

「免費」升至本週首位，詳見圖8，新進本週 Top 10 的「了解」位居第 8 名，分別以當日撥款訴求及整合轉貸規劃吸引諮詢，並以免聯徵或專人協助降低申辦顧慮。「優惠」退居第 2 名，相關購車廣告以免繳半年車貸、線上下訂金折扣等優惠吸引買家，再引導民眾點擊聯繫、詢問貸款方案。

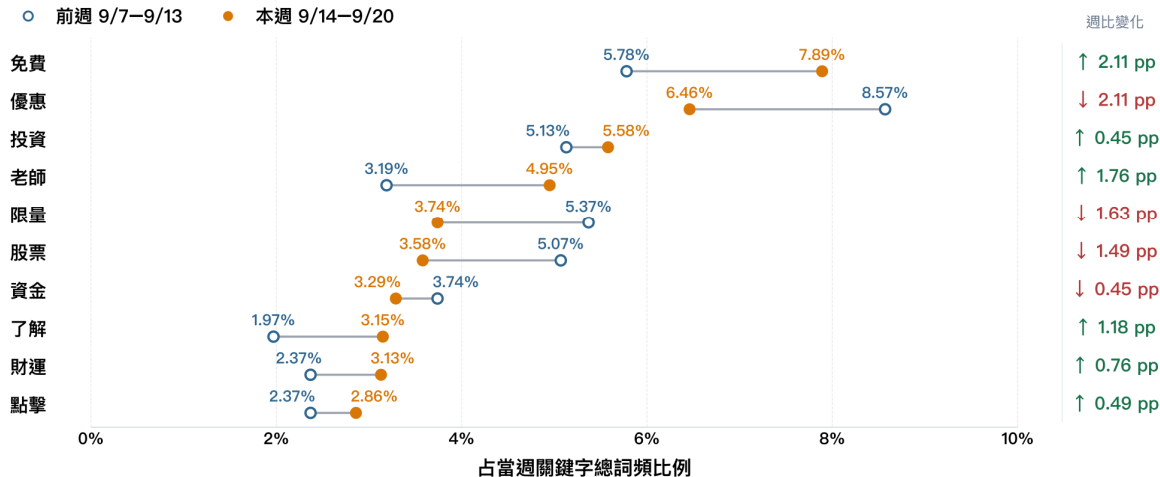
「投資」升至第 3 名，「股票」與「資金」分居第 6 名及第 7 名，相關廣告透過講師經歷、交易紀律與盤勢分析塑造專業形象，引導民眾報名體驗課程或查看選股工具。其中，「資金」的情境由前週借貸轉向資金流向與強勢股分析。

「老師」升至第 4 名，新進本週 Top 10 的「財運」位居第 9 名，相關廣告以免費分析運勢為訴求，吸引民眾私訊詢問。另有廣告宣稱配戴水晶手鍊能改善財運，搭配信眾見證推動購買。「老師」的情境由前週投資教學轉向命理服務，也反映本週廣告不只以借貸與投資學習吸引民眾，還以改善財運為訴求，引導民眾私訊詢問命理服務或購買宣稱能改善運勢的商品。

詐騙關鍵字占比週比變化

以本週為主 | 完整顯示本週 Top 10

○ 前週 9/7-9/13 ● 本週 9/14-9/20



註：占比＝關鍵字出現次數÷當週檔案所列關鍵字出現次數總和；pp 為百分點。

圖8 | 詐騙關鍵字占比週比變化

焦點文章

最新國際產品資安政策趨勢

國際產品資安政策朝生命週期管理發展，企業持續性漏洞管理與PSIRT建置日益重要

一、前言

近年來，連網產品面臨的資安風險持續增加。人工智慧降低漏洞探測及惡意程式撰寫的技術門檻，供應鏈攻擊也可能使單一元件的漏洞影響大量下游產品。隨著車載系統、工業控制設備等裝置之廣泛連網應用，產品資安事件的影響亦已可能擴及企業營運、公共服務。

面對此類風險，僅依靠產品上市前的資安檢驗已不足以因應，各國產品資安規範亦逐步延伸至產品生命週期的持續管理。製造商除須確保產品符合上市時之資安要求，也須持續處理支援期間所發現的漏洞，並提供安全更新及進行資訊揭露。

隨著製造商承擔的責任增加，如何建立相應的漏洞管理及事件應變機制，亦成為產品資安政策的重要課題。本文以下先介紹歐盟、英國及日本近年推動的產品資安制度，接著說明作為承接組織產品漏洞管理與相關應變機制的產品資安事件應變小組（Product Security Incident Response Team, PSIRT），最後歸納相關政策發展的共同趨勢。

二、國際產品資安政策概況

近年歐盟、英國及日本在產品資安制度上均有具體進展，三者採取的政策工具及規範強度則各有不同，以下分別說明。

（一）歐盟《網路韌性法》（Cyber Resilience Act, CRA）

歐盟於2024年通過CRA，針對具有數位元素的產品建立統一的產品資安要求。製造商除須於設計、開發及生產階段納入資安考量，也須於產品上市後之支援期間持續處理產品及其元件的漏洞、提供安全更新，並建立協調漏洞揭露政策。對於已遭利用的漏洞及重大資安事件，製造商另負有通報義務，違反相關規定者並設有行政罰則[1]。

隨著CRA逐步上路，歐盟執委會於2026年已開始就法規適用及執行提供進一步說明，內容包括產品適用範圍、支援期間、資安風險評估及通報義務等，以利後續法規適用[2]。

焦點文章

(二) 英國《產品安全與電信基礎設施法》(Product Security and Telecommunications Infrastructure Act, PSTI)

英國PSTI相關規範自2024年4月起施行，主要針對消費性連網產品建立最低資安要求，包括禁止使用通用或容易猜測的預設密碼、提供資安問題通報方式，以及揭露安全更新的最低支援期間。違反相關規定者，主管機關得加以裁罰或採取其他執法措施[3]。

(三) 日本JC-STAR制度

日本自2025年起實施日本網路安全技術評估要求 (Japan Cyber-Security Technical Assessment Requirements, JC-STAR) 分級標章制度，依產品使用情境及風險設定不同等級的資安要求。相關要求涵蓋密碼管理、漏洞通報方式及安全更新等事項，並透過政府採購等政策工具推動業者採用[4]。

在跨國制度合作方面，日本與英國已就JC-STAR與PSTI建立相互承認之制度[5]，並自2026年起實施。符合相關條件的產品，得以符合性資料證明已落實對方制度的相關要求，以減少業者因應不同市場規範時的重複作業。

整體而言，歐盟與英國均以法規課予製造商產品資安義務，並設有相應的裁罰機制；日本則透過分級標章及政府採購等政策工具，引導業者提升產品資安。三者採取的規範方式及強制程度雖有不同，但對通報接收、安全更新等要求已有相近發展方向。

三、PSIRT與生命週期管理

前述國際規範顯示，上市後的產品資安義務已逐漸成為製造商應履行的責任，也意味著企業須建立一套可持續運作的漏洞管理機制，確保漏洞從發現、評估、修補到對外揭露，均有明確的處理流程與權責分工。

PSIRT即是組織內部承接此類工作的重要機制。國際事件應變與安全團隊論壇 (Forum of Incident Response and Security Teams, FIRST) 提出的《PSIRT Services Framework[6]》文件，將PSIRT的工作區分為不同服務領域，就產品漏洞處理而言，主要包括：

焦點文章

1. 漏洞發現與受理：建立對外通報管道，接收產品漏洞通報，並掌握產品本身及第三方元件的漏洞資訊。
2. 漏洞分析與處理：確認漏洞影響的產品及版本，評估風險，並協調後續修補。
3. 資訊發布與溝通：依漏洞處理情形發布相關資訊，並與內部開發團隊、外部元件供應者、產品使用者，以及其他 PSIRT、CSIRT或漏洞協調機構進行溝通與協調。

上述框架為各國推動產品資安政策時的重要參考。以日本為例，獨立行政法人情報處理推進機構（Innovation Platform Agency, IPA）於 2026 年改版發布之《產品開發者指引》（製品開発者向けガイド），從產品開發者角度提出漏洞管理作法，其中將 PSIRT 的建置與維運列為建議作法之一，並就組織分工、內外部協作及相關功能提供具體說明[7]。

綜合觀察，PSIRT 所處理者與近年產品資安規範所要求之事項高度相關。歐盟 CRA 與英國 PSTI 雖未明文要求製造商設置 PSIRT，但其規範的漏洞處理、安全更新及資訊揭露等事項，均涉及 PSIRT 相關職能；日本《產品開發者指引》則進一步將 PSIRT 直接列入建議作法。

四、產品資安政策趨勢

綜整國際產品資安政策發展，除前述由上市前擴及生命週期的共同方向外，尚可觀察到兩個值得關注的趨勢。

第一，PSIRT或相似功能之組織機制，逐步成為製造商合規的主要基礎。隨著各國產品資安規範陸續落實，製造商所承擔的責任已不再止於產品上市時符合相關安全要求，更須在產品支援期間持續掌握及處理新發現的漏洞，並建立相應的處理流程與分工。企業建置 PSIRT或類似機制的需求，將隨之持續提高。此一發展亦透過國際供應鏈影響非直接受規範國家的製造商。

第二，各國產品資安制度陸續建立後，不同制度間的銜接亦開始受到重視。英國與日本推動 PSTI 與 JC-STAR 的相互承認，即反映產品進入不同市場時可能面臨重複驗證及法規遵循問題。各國在持續強化產品資安要求的同時，如何提高不同制度間相互承認的程度、降低業者進入不同市場的重複遵循成本，也可能成為後續國際產品資安政策值得觀察的方向。

焦點文章

五、結語

上述國際規範已陸續進入實施及調整階段，相關要求對我國業者的影響亦將逐步顯現。尤其我國資通訊產業高度參與全球供應鏈，業者除須掌握不同市場的產品資安要求，也須將漏洞處理、安全更新及資訊揭露等工作納入既有產品開發與維運流程。未來各國制度的實際執行情形、相互承認及國際標準的發展，均值得持續關注。

面對產品資安責任逐步延伸，本院近年亦持續推動企業建置PSIRT，並透過 TWCERT/CC 作為國內產品漏洞通報與協調的窗口。後續亦將持續關注國際規範對我國產業的影響，作為產品資安政策及產業輔導措施調整之參考。

參考文獻

- [1] European Parliament and Council of the European Union. (2024). Regulation (EU) 2024/2847 (Cyber Resilience Act). Official Journal of the European Union. Retrieved Sep 21, 2026, from <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02024R2847-20241120>
- [2] European Commission. (2026, July 27). Commission publishes new guidance to support timely Cyber Resilience Act implementation. <https://digital-strategy.ec.europa.eu/en/library/commission-publishes-new-guidance-support-timely-cyber-resilience-act-implementation>
- [3] Legislation.gov.uk. (2023). The Product Security and Telecommunications Infrastructure (Security Requirements for Relevant Connectable Products) Regulations 2023, Schedule 1. <https://www.legislation.gov.uk/ukxi/2023/1007/schedule/1>
- [4] IPA. (n.d.). Japan Cyber STAR (JC-STAR). Retrieved Sep 23, 2026, from <https://www.ipa.go.jp/en/security/jc-star/index.html>
- [5] IPA. (2026, June 1). Regarding Mutual Recognition Application for PSTI Compliance Certification & JC-STAR. https://www.ipa.go.jp/en/security/jc-star/shinsei/psti_e.html
- [6] FIRST. (2020). Product Security Incident Response Team (PSIRT) Services Framework (Version 1.1). https://www.first.org/standards/frameworks/psirts/FIRST_PSIRT_Services_Framework_v1.1.pdf
- [7] IPA. (2026). 製品開発者向けガイド. https://www.ipa.go.jp/security/guide/vuln/rcu1hd000000a5en-att/guide_for_dev.pdf

關鍵字：產品資安、漏洞通報、PSIRT、歐盟網路韌性法

刊 名 資安週報第 63 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