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
近期新增多項重大CVE漏洞 應留意受影響元件版本並及時更新修補

重大漏洞
HPE、WatchGuard及Google高風險漏洞應盡速修補

聯防監控
防禦迴避高居首位 惡意執行仍具威脅

蜜罐誘捕
程式遞送控制器(ADC & Gateway) 及威脅情資平台仍為攻擊熱點

事件通報
SQL Injection防護應涵蓋各類資料查詢與操作功能

網路巡查高風險詐騙
「招財」「貸款」進入前十 皮夾開運訴求與購車借貸需求並行

焦點文章
「資安共好-2026產品資安研討會」高峰論壇總結分析

2026.11.12
070

資安儀表板

外部曝險分析、重大漏洞、聯防監控、蜜罐誘捕、事件通報及網路巡查高風險詐騙等六類量化指標

■ 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

近期新增多項重大CVE漏洞 應留意受影響元件版本並及時更新修補

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2,691項。其中，「元件高風險漏洞」以843項居首，「過時或弱加密協定」707項次之，「TLS憑證不受信任」671項位居第三。前三項合計2,221項，占前10大風險項目總數約82.5%，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2,791項，本期整體風險數量減少100項，降幅約3.6%，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922項減至本期843項，降幅約8.6%。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；另外本期發現PHP相關弱點(CVE-2026-109618、CVE-2026-109619)主要涉及記憶體處理不當，攻擊者可能利用記憶體毀損及釋放後使用問題，在特定條件下造成遠端程式碼執行風險，建議升級至PHP 8.2.35、8.3.36、8.4.27或8.5.12以上之已修補版本，以及發現WordPress核心弱點(CVE-2026-119977)，攻擊者可能利用核心更新期間可預測且可透過網路存取的暫存檔案路徑，在特定條件下造成未經身分驗證的遠端程式碼執行風險，建議升級至WordPress 7.1.4以上版本。「過時或弱加密協定」由720項減至707項，降幅約1.8%；「TLS憑證不受信任」由673項減至671項，降幅約0.3%。另「CSP設定不當」由235項減至226項，降幅約3.8%；「未部署WAF」由102項增至116項，增幅約13.7%。

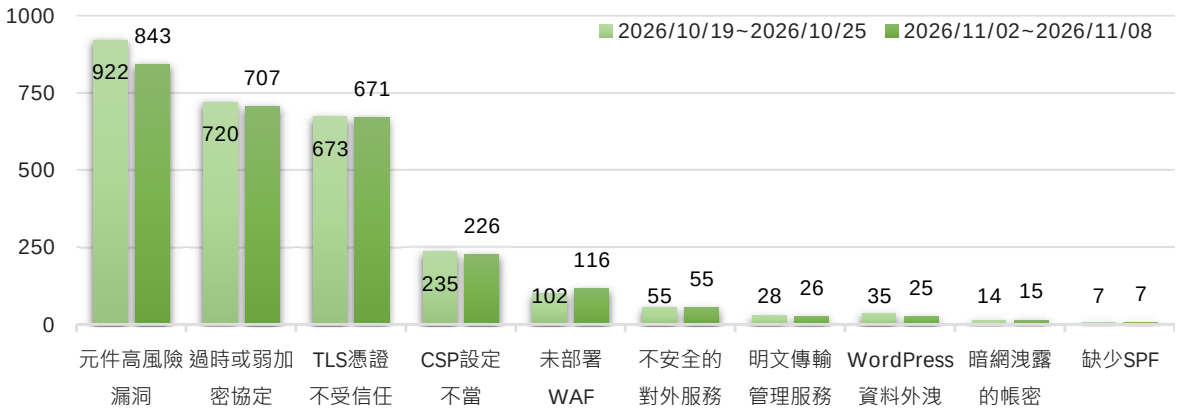


圖1 | EASM檢測結果統計(前10大風險)

整體而言，本期外部曝險風險已有改善跡象，此外，本期發現多項涉及遠端程式碼執行之重大漏洞，包含PHP及WordPress相關弱點，顯示近期重大資安風險持續出現，應提高警覺並加強防範。建議持續關注最新漏洞情資，優先盤點及修補受影響系統，並落實加密協定、憑證管理及網站安全防護措施，以降低重大漏洞遭利用及外部曝險風險。

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

HPE、WatchGuard及Google高風險漏洞應盡速修補

- HPE Networking AOS-10與AOS-8存在多項高風險安全漏洞[1]，類型包含身分鑑別繞過(Authentication Bypass)、緩衝區溢位(Buffer Overflow)、SQL注入(SQL Injection)、指令注入(Command Injection)、敏感資訊洩露(Exposure of Sensitive Information)等，最嚴重可讓未經身分鑑別之遠端攻擊者，繞過既存身分鑑別控制，進而以root權限於底層作業系統執行任意指令。

- WatchGuard Fireware OS存在2項堆積型緩衝區溢位(Heap-based Buffer Overflow)漏洞(CVE-2026-112709與CVE-2026-112710)[2][3]，當Firebox設備設定為Active Directory身分鑑別伺服器時，未經身分鑑別之遠端攻擊者可透過控制或攔截該伺服器之流量，並藉由特製回應觸發漏洞，進而導致阻斷服務或執行任意程式碼。

- Google Android存在越界讀取(Out-of-Bounds Read)漏洞(CVE-2026-58882)[4]，未經身分鑑別之遠端攻擊者可藉由傳送特製之WAP Push簡訊，導致WapPushOverSms.java中decodeWapPdu函式觸發整數溢位(Integer Overflow)造成越界讀取，進而導致阻斷服務。

- Google Brotli存在越界寫入(Out-of-Bounds Write)漏洞(CVE-2026-111497)[5]，未經身分鑑別之遠端攻擊者可藉由特製之Brotli壓縮資料串流(Compressed Stream)，使解碼器記憶體寫入時超出內部緩衝區範圍，進而洩漏記憶體機敏內容、造成服務阻斷或執行任意程式碼，該漏洞已遭駭客濫用。

[1] https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbnw05162en_us
[2] https://psirt.watchguard.com/CVE-2026-112709
[3] https://psirt.watchguard.com/CVE-2026-112710
[4] https://source.android.com/docs/security/bulletin/2026/2026-11-01
[5] https://github.com/google/brotli/releases

■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 惡意執行仍具威脅

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2。「防禦迴避」為最常見攻擊手法，占比16.7%，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。

「惡意執行」事件本週占比為14.4%，為本週占比次高的攻擊階段，顯示攻擊者持續透過腳本語言及系統內建工具執行可疑指令與惡意程式碼，以達成後續攻擊目的。觀察到的主要手法包括JavaScript 腳本執行、Visual Basic 腳本執行、以及PowerShell 指令執行。攻擊者可能透過惡意網頁或腳本利用 JavaScript 執行可疑指令、下載惡意程式，亦可能藉由 Visual Basic 腳本或惡意文件觸發程式碼執行，並進一步濫用 PowerShell 等系統內建管理工具執行遠端指令、下載攻擊工具或蒐集系統資訊。此類行為多利用合法腳本語言與系統元件進行惡意操作，具有一定隱蔽性，可能增加傳統防護機制的偵測難度，並成為後續權限提升、維持存取及橫向擴散等攻擊活動的重要基礎。

建議機關持續強化腳本執行與異常程序活動的監控，落實 PowerShell 日誌記錄及應用程式執行控管，並限制非必要的腳本執行權限，同時結合端點偵測與回應（EDR）機制，以降低攻擊者濫用合法工具執行惡意程式碼的風險。

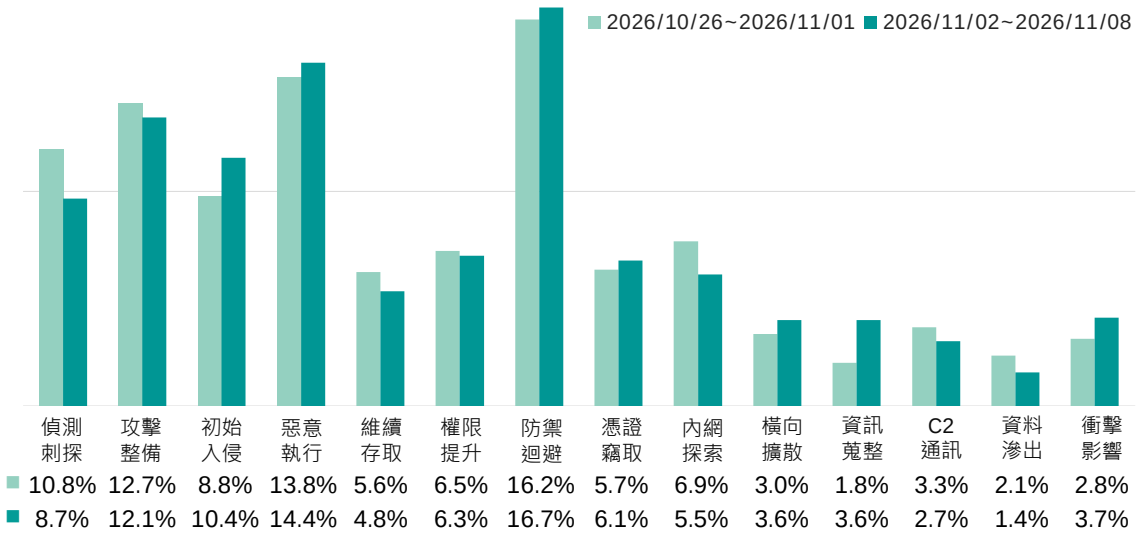
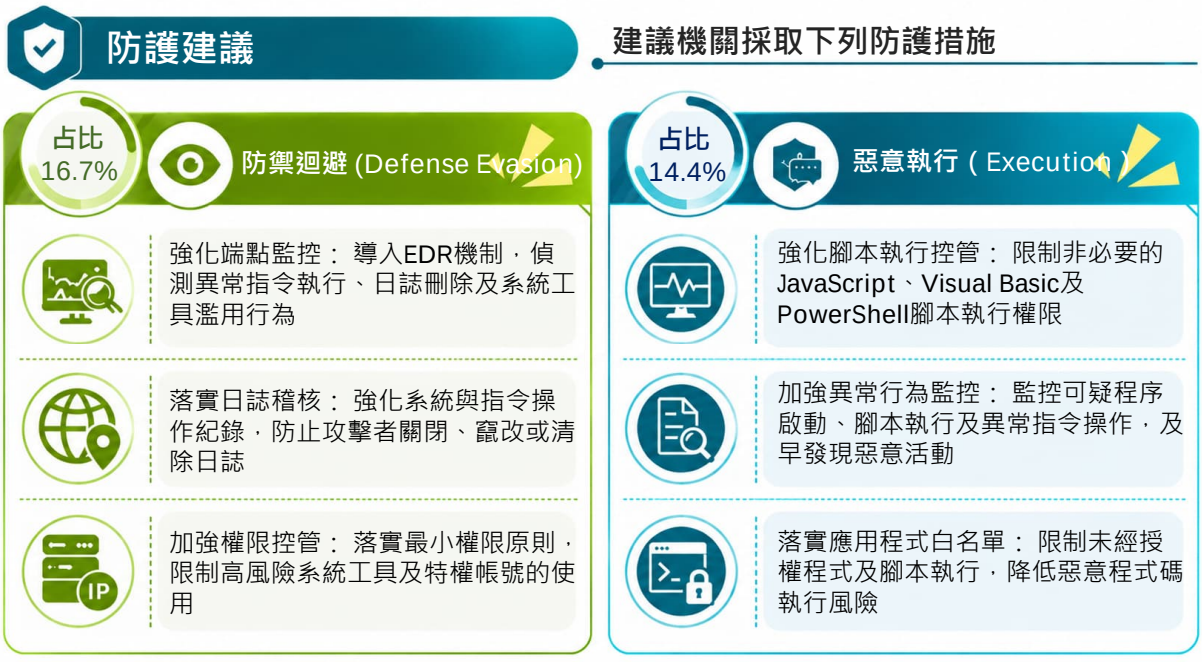


圖2 | 資安聯防監控攻擊階段統計


防護建議
建議機關採取下列防護措施
占比 16.7%
防禦迴避 (Defense Evasion)
強化端點監控： 導入EDR機制，偵測異常指令執行、日誌刪除及系統工具濫用行為
落實日誌稽核： 強化系統與指令操作紀錄，防止攻擊者關閉、竄改或清除日誌
加強權限控管： 落實最小權限原則，限制高風險系統工具及特權帳號的使用
IP
占比 14.4%
惡意執行（Execution）
強化腳本執行控管： 限制非必要的JavaScript、Visual Basic及PowerShell腳本執行權限
加強異常行為監控： 監控可疑程序啟動、腳本執行及異常指令操作，及早發現惡意活動
落實應用程式白名單： 限制未經授權程式及腳本執行，降低惡意程式碼執行風險

■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

程式遞送控制器(ADC & Gateway) 及威脅情資平台仍為攻擊熱點

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66.39%、「遠端控制」服務攻擊占比28.12%，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66.67%。「遠端控制」服務亦有28.09% 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3。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ConnectWise ScreenConnect 存在驗證繞過漏洞之CVE-2024-1709，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。

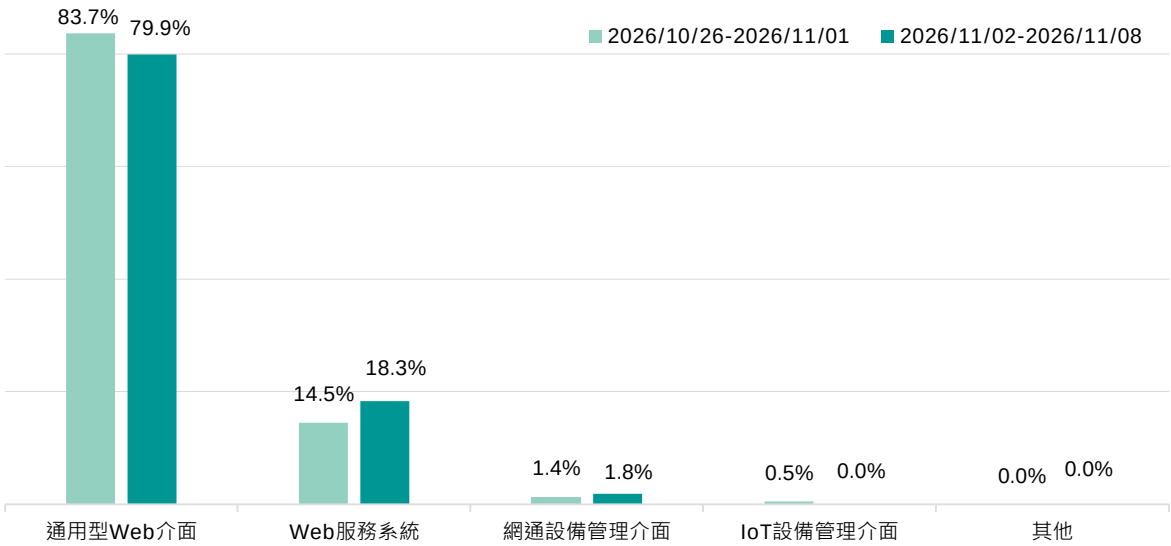


圖3 | 本週網頁應用介面之誘捕攻擊比例統計

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、權限提升漏洞、釋放後使用漏洞、身分驗證繞過漏洞及指令注入漏洞，攻擊目標涵蓋程式遞送控制器(ADC & Gateway)、威脅情資平台、網頁瀏覽器、網站主機伺服器管理系統及雲端檔案管理平台與企業行動裝置安全存取控制系統。

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-2026-3055[1]	NetScaler ADC & Gateway	9.8	✓
■	2	-	CVE-2026-27960[2]	OpenCTI	9.8	
■	3	⬆new	CVE-2026-10961[3]	iOS 版 Chrome 瀏覽器	8.3	
■	4	⬇1	CVE-2026-41940[4]	cPanel & WHM	9.8	✓
■	5	-	CVE-2026-10520[5]	Ivanti Sentry	10	✓

類型 ■ 越界讀取漏洞 ■ 權限提升漏洞 ■ 釋放後使用漏洞
■ 身分驗證繞過漏洞 ■ 指令注入漏洞

1. https://nvd.nist.gov/vuln/detail/CVE-2026-3055
2. https://nvd.nist.gov/vuln/detail/CVE-2026-27960
3. https://nvd.nist.gov/vuln/detail/CVE-2026-10961
4. https://nvd.nist.gov/vuln/detail/CVE-2026-41940
5. https://nvd.nist.gov/vuln/detail/CVE-2026-10520

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

SQL Injection防護應涵蓋各類資料查詢與操作功能

本週總計接獲58件公務機關與特定非公務機關事件通報，詳見圖4，公務機關非法入侵事件中以異常連線占多數，詳見圖5。本週除仍持續觀察到機關觸發PolarEdge殭屍網路連線情形之外，發現多個機關遭受SQL Injection攻擊。SQL Injection雖屬已知多年的網站攻擊手法，實務上仍可能因部分查詢功能未採安全的參數化處理、動態SQL直接組合外部輸入，或僅以特殊字元過濾作為防護，而留下可被利用的查詢路徑。

實務上，網站與資料庫互動的功能不只出現在登入、搜尋等常見欄位，排序、篩選、報表、資料匯出或其他查詢功能，也可能將外部輸入帶入資料庫。建議機關檢視網站中所有會查詢或存取資料庫的功能，避免直接將使用者輸入內容組成資料庫查詢指令；並將登入、搜尋、排序、篩選、報表及匯出等不同使用情境納入弱點檢測及程式碼檢視。另不宜僅依賴特殊字元過濾或WAF阻擋，仍應從程式設計面採用安全的查詢方式，降低SQL Injection遭利用的風險。

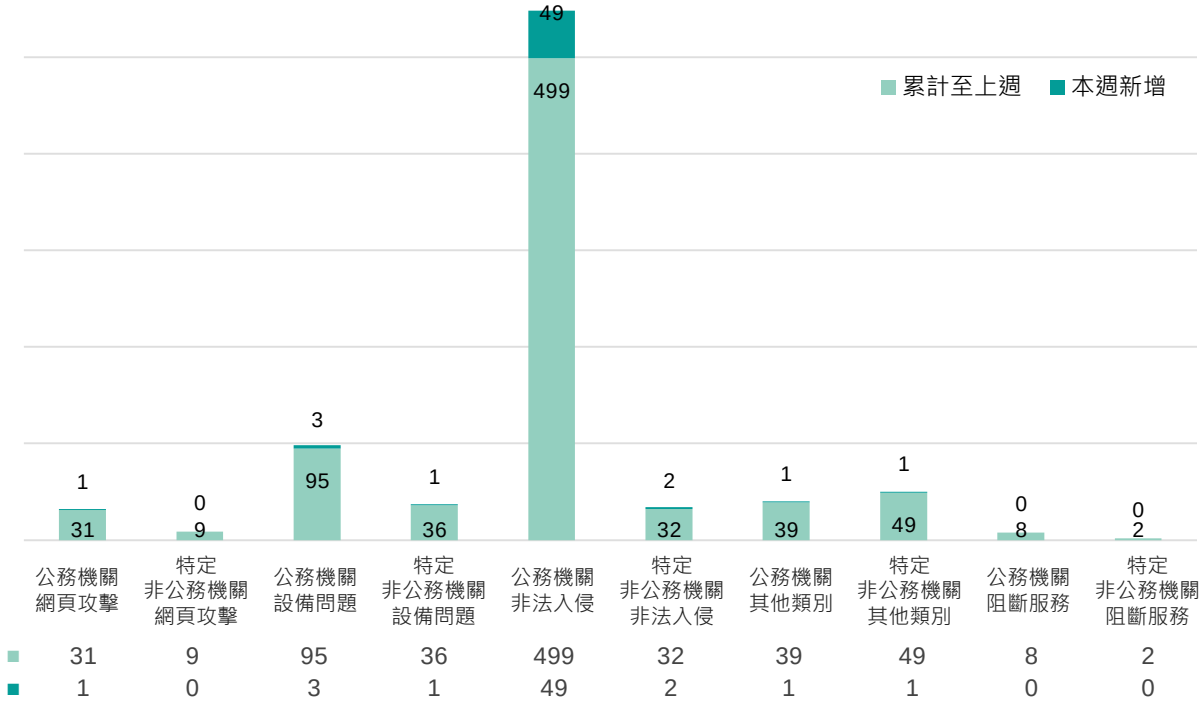


圖4 | 本週公務機關暨特定非公務機關資安事件通報概況

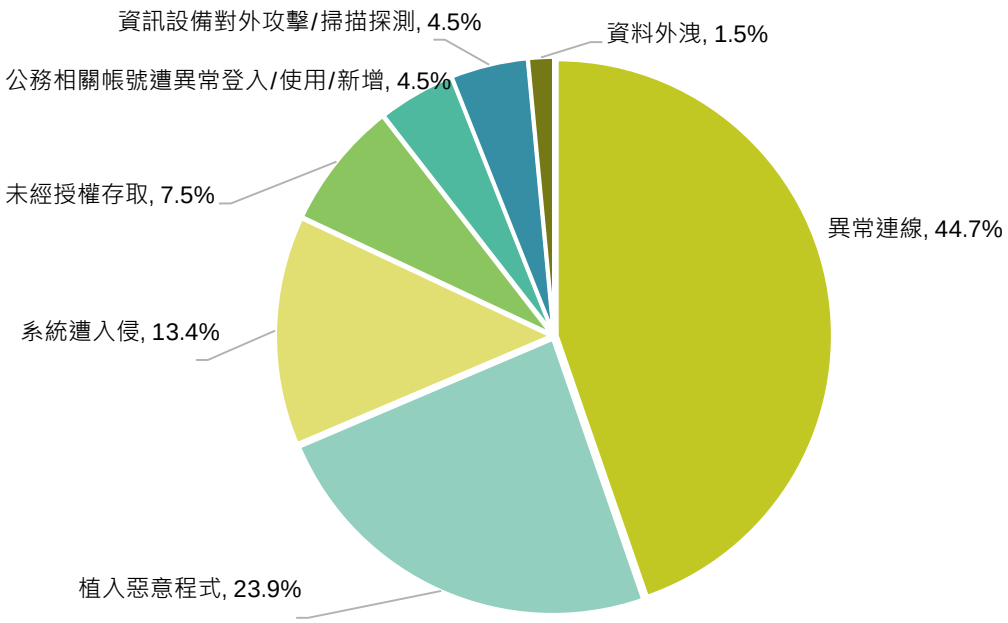


圖5 | 本週公務機關非法入侵事件類型占比

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SQL注入漏洞竊取資料庫內部敏感資訊 ➢ 攻擊者操控資料庫查詢指令竄改或刪除重要業務資料	➢ 全面採用參數化查詢及預備陳述式，避免外部輸入直接組成SQL指令 ➢ 檢視登入、搜尋、排序、篩選及報表功能，確認資料庫查詢安全性 ➢ 定期執行網站弱點掃描及程式碼安全檢測，及早發現SQL注入漏洞 ➢ 落實資料庫帳號最小權限原則，搭配WAF及異常查詢監控降低攻擊影響

17間民間企業揭露重大資安訊息

本週17間民間企業發布重大訊息，產業類別為數位雲端業、化學工業、生技醫療業、觀光餐旅業、食品工業、半導體業、電腦及週邊設備業 ，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
任開數位媒體行銷股份有限公司	2026年11月03日	任開數位外部伺服器遭受自動化攻擊，致部份資料遭非法擷取。已立即啟動資通安全事件之通報及應變機制，依法通報相關主管機關，並持續採取必要防護措施，以降低事件影響。此外，為防範會員資料遭不當利用，亦透過官網、電子郵件、簡訊及會員APP等管道主動通知會員，提醒提高警覺，並加強反詐騙宣導，以降低潛在風險。目前評估對公司營運無重大影響。
毛寶股份有限公司	2026年11月03日	毛寶於例行性資安監控過程中，偵測發現電商網站遭外部不明人士進行異常網路攻擊，隨即啟動資安緊急應變及防護措施，並會同系統維運廠商及第三方專業資安團隊進行事件調查、鑑識分析與安全性檢測，以確認事件影響範圍並強化相關防護機制。另已依相關規定辦理主管機關通報，並主動通知受影響顧客，提醒提高防詐警覺，留意不明來電、可疑簡訊及不明連結。經初步評估，對公司整體營運及財務尚無重大影響，相關事件調查及影響範圍確認作業仍持續進行中。
中天生物科技股份有限公司	2026年11月03日	中天生物科技重要子公司棉花田生機園地股份有限公司接獲委外購物網站服務廠商通知，委外服務系統近期發現異常資料存取狀況，於發現異常後已阻擋異常存取行為。棉花田

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
中天生物科技股份有限公司 (續)	2026年11月03日	接獲通知後，立即啟動資安事件應變與調查機制，並要求委外廠商儘速確認受影響系統、資料範圍及採取必要之防護措施。影響資料範圍待委外廠商進一步調查，目前網站營運正常運用，並未中斷。初步評估對公司營運無重大影響。
葡萄王生技股份有限公司	2026年11月04日	葡萄王生技接獲電子商城線上平台委外服務廠商通知，其資料庫部分資料遭未經授權之異常存取。已依內部個資相關規定組成個資事故緊急應變小組，並召開應變會議，採取必要防護措施以降低事件影響。透過電子商城官網發布及以簡訊通知等方式提醒會員、消費者提高防詐騙警覺，避免損失。已主動通報相關主管機關，另要求委外服務廠商儘速釐清事件原因、及公司「購健康」訂單資料或消費者個資是否遭未經授權存取及可能受影響範圍，並進行資安檢視及必要強化措施。截至目前對公司財務及業務並無重大影響。
王品餐飲股份有限公司	2026年11月04日	王品子公司萬鮮股份有限公司接獲委外購物網站服務廠商通知，委外服務系統近期發現異常資料存取狀況，於發現異常後已阻擋異常存取行為。萬鮮公司接獲通知後，立即啟動資安事件應變與調查機制，並要求委外服務廠商儘速確認受影響系統、資料範圍及採取必要之防護措施。影響資料範圍待委外服

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
王品餐飲股份有限公司(續)	2026年11月04日	務廠商進一步調查，目前網站營運正常，並未中斷，初步評估對公司營運無重大影響。
遠東生物科技股份有限公司	2026年11月05日	遠東生技公司接獲電子商城線上平台委外服務廠商通知，其資料庫部分資料遭未經授權之異常存取。遠東生技公司接獲通知後，即持續關注事件發展，並確認事件處理及後續改善情形。已透過電子商務平台會員EDM、電子商城網站最新消息及社群平台發布防詐騙提醒，提醒會員及消費者提高防詐騙警覺，避免損失。另要求委外服務廠商儘速釐清事件原因、確認訂單資料或消費者個資是否遭未經授權存取及可能受影響範圍，並進行資安檢視及採取必要之強化措施。截至目前對公司財務及業務並無重大影響。
騰勢股份有限公司	2026年11月05日	騰勢接獲委外服務廠商通知，委外服務系統近期發現異常資料存取狀況，於發現異常後已阻擋異常存取行為。已立即啟動資安事件應變與調查機制，並要求委外廠商儘速確認受影響系統、資料範圍及採取必要之防護措施。目前評估對公司營運及財務無重大影響。
知識科技股份有限公司	2026年11月05日	知識科技發現GMB系統遭網路攻擊後，隨即啟動資安應變事件機制，展開調查及維護作業。經目前調查，受影響範圍限於GMB系統，尚未發現攻擊擴及至其他系統之情形。目前評估對公司財務、業務及營運皆無重大影響。

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
天仁茶葉股份有限公司	2026年11月06日	天仁茶葉接獲委外服務廠商91APP通知，其資料庫遭受自動化攻擊。已啟動應變機制，持續採行必要防護措施，以降低事件影響機率。另為防範資料遭不當利用，已透過天仁熟客圈官網與APP通知會員，加強反詐騙宣導。目前評估對公司財務、業務及營運皆無重大影響。
臺鹽實業股份有限公司	2026年11月06日	臺鹽實業接獲電子商城線上平台委外服務廠商通知，其資料庫部分資料遭未經授權之異常存取。 臺鹽實業已依內部個資相關規定組成個資事故緊急應變組，並召開應變會議，採取必要防護措施以降低事件影響。透過台鹽線上購發布及以E-mail通知等方式提醒會員、消費者提高防詐騙警覺，避免損失。已主動通報相關主管機關。另要求委外服務廠商儘速釐清事件原因、訂單資料或消費者個資是否遭未經授權存取及可能受影響範圍，並進行資安檢視及必要強化措施。截至目前對公司財務及業務並無重大影響。
精材科技股份有限公司	2026年11月06日	精材科技發現不明IP異常侵入內部資訊系統，造成某客戶、部分供應商及少數員工之名稱與商務郵件聯絡資訊外洩。已立即啟動資安應變機制，採取網路阻斷及系統隔離相關防護措施，同時依規定向主管機關通報。為防範資訊遭惡意詐騙利用，已對相關對象進行通知，並公告全體同仁進行反詐騙宣導。目

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
精材科技股份有限公司(續)	2026年11月06日	前公司資訊系統與營運均正常運作，對公司無重大影響。
宏碁智醫股份有限公司	2026年11月06日	宏碁智醫子公司宏碁健康股份有限公司之線上商店委外服務廠商，所服務之部分客戶發生資料庫部分資料發生未經授權之異常存取情事，截至目前為止，尚無接獲類似情事之通知。宏碁智醫公司持續關注事件發展，但為求慎重，已先行停止線上商店之營運，以避免可能之資安事件發生。並透過公司網站或線上商店提醒會員、消費者提高警覺、避免詐騙、避免損失。目前對公司財務及業務並無重大影響。
宏碁智新股份有限公司	2026年11月06日	宏碁智新線上商店委外服務廠商，發生資料庫部分資料未經授權之異常存取情事。自媒體公開訊息獲悉後，即停止線上商店營運，並求證受影響資料範圍。隨即成立應變小組，調查事件原因，並儘速提供完整調查結果及相關改善措施。透過公司網站或線上商店提醒會員、消費者提高警覺、避免詐騙、避免損失。針對疑似受影響之少數消費者，將個別通知當事人，提醒提高警覺、避免詐騙。宏碁智新將準備相關資料通報主管機關，並持續追蹤事件調查進度，視調查結果採取必要之因應措施，以維護消費者權益及資訊安全。截至目前為止對公司財務及業務並無重大影響。

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
展碁國際股份有限公司	2026年11月06日	展碁國際之子公司好漾生活股份有限公司，其線上商店委外服務廠商所服務之部分客戶資料庫發生未經授權之異常存取情事，截至目前為止，尚無接獲類似情事之通知。 好漾生活持續關注事件發展，但為求慎重，已先行停止線上商店之營運，以避免可能之資安事件發生。並透過公司網站或線上商店提醒會員、消費者提高警覺、避免詐騙、避免損失。目前對公司財務及業務並無重大影響。
倚天酷碁股份有限公司	2026年11月06日	倚天酷碁-創線上商店委外服務廠商，發生資料庫部分資料未經授權之異常存取情事。自媒體公開訊息獲悉後，即停止線上商店營運，並求證受影響資料範圍。隨即成立應變小組，調查事件原因，並儘速提供完整調查結果及相關改善措施。透過公司網站或線上商店提醒會員、消費者提高警覺、避免詐騙、避免損失。針對疑似受影響之極少數消費者，將個別通知當事人，提醒提高警覺、避免詐騙。倚天酷碁-創將準備相關資料通報主管機關，並持續追蹤事件調查進度，視調查結果採取必要之因應措施，以維護消費者權益及資訊安全。截至目前為止對公司財務及業務並無重大影響。

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
倚天酷碁股份有限公司	2026年11月06日	倚天酷碁-創之子公司宏碁風尚股份有限公司，其線上商店委外服務廠商發生資料庫部分資料未經授權之異常存取情事。宏碁風尚獲悉後，即停止線上商店營運，求證受影響資料範圍，並成立應變小組，調查事件原因，並儘速提供完整調查結果及相關改善措施。透過網站或線上商店提醒會員、消費者提高警覺、避免詐騙、避免損失。針對疑似受影響之極少數消費者，將個別通知當事人，提醒提高警覺、避免詐騙。宏碁風尚將準備相關資料通報主管機關，並持續追蹤事件調查進度，視調查結果採取必要之因應措施，以維護消費者權益及資訊安全。截至目前為止對公司財務及業務並無重大影響。
諾貝兒寶貝股份有限公司	2026年11月08日	諾貝兒寶貝接獲線上商店平台委外服務廠商通知，其資料庫部分資料遭未經授權之異常存取。 諾貝兒寶貝於接獲通知後，立即啟動資安事件應變及處理流程機制，並持續採取必要防護措施，以降低事件影響。為防範會員個資遭不當利用，亦透過官網、簡訊、email等管道主動通知會員，提醒提高警覺，並加強反詐騙宣導，以降低潛在風險，並要求委外服務廠商進行資安檢視及採取必要之強化措施。

■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

「招財」「貸款」進入前十 皮夾開運訴求與購車借貸需求並行

詐騙類型趨勢

本週仍以產品服務型為主，占比略降，接近四分之三，詳見圖6。其中，「保暖外套」廣告以「寒流將至」吸引注意，再用限時折扣及數量有限催促下單。同樣鎖定日常需求的「美妝」廣告，則以睫毛持久捲翹、成分溫和、敏感肌也能使用的說法，吸引重視妝容效果與使用安全的民眾購買。另有「男性營養補充品」廣告，針對持續為懷孕做準備、卻遲遲未懷孕的夫妻，宣稱短期內能「提高懷孕機率」，並承諾無效全額退款。這些廣告以優惠、成分溫和的訴求或退款承諾提高購買動機。

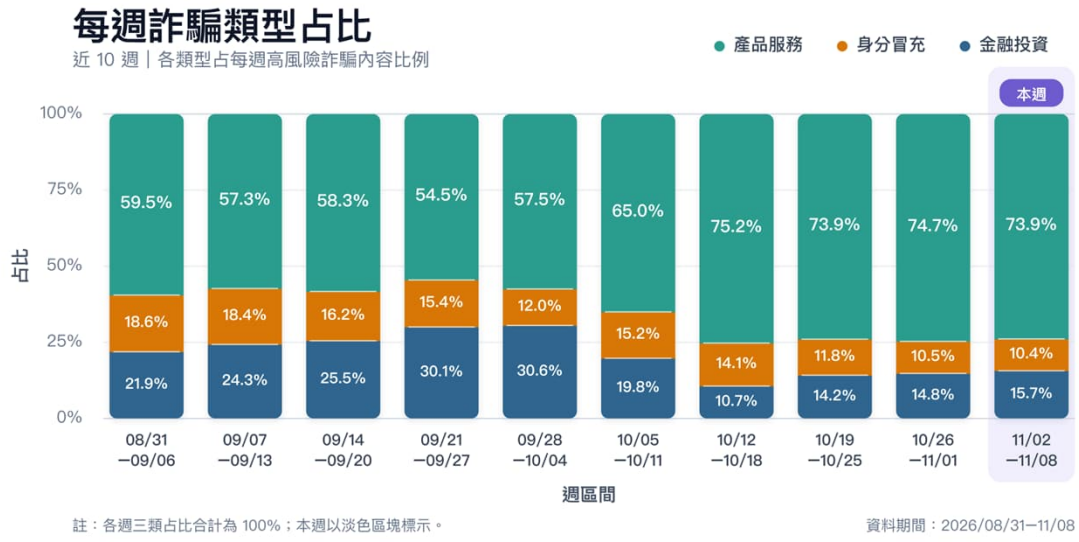


圖6 | 每週詐騙類型占比

身分冒充型占比最低，本週較前週略降。其中，「皮夾」廣告假藉「宮廟名義」宣傳，宣稱商品獲得授權、經過加持，並以虎爺形象強調招財寓意，吸引民眾購買。除了宗教訴求，廣告也強調輕薄、大容量且容易保養，再搭配贈品與抽獎機會增加吸引力；接著邀請民眾先追蹤帳號並留言，以取得購物連結。從宮廟授權、加持到商品用途與贈品，這類廣告持續提供購買動機，將民眾對宗教的信任帶入購買判斷。

金融投資型占比回升，維持本週第二大類型。例如，「選股課程」廣告從買進後股價續跌、追高時難以判斷趨勢等困擾切入，藉講師解說選股條件與交易流程塑造專業形象，搭配免費體驗吸引報名，並以名額有限催促參與。除了課程，也有「宣傳群組」的廣告，其宣稱盤前公布選股資訊，邀請民眾加入群組觀察，於開盤後驗證選股效果，並強調不滿意

可退出。兩者都以看懂行情、掌握買點的期待吸引注意，再藉免費參與降低門檻，引導民眾報名課程或加入群組。

關鍵字趨勢

「優惠」居本週首位，詳見圖7，例如保暖外套廣告以寒流將至吸引注意，再用限時折扣催促民眾下單。轉看睫毛美妝宣傳，「配方」「輕鬆」分居第 3 名及第 9 名，廣告藉配方說明與上妝教學，強調成分溫和、容易使用。第 7 名的「健康」相關廣告鎖定為懷孕做準備的民眾，藉其對未來孩子健康的期待推銷營養補充品。至於第 6 名的「招財」，係皮夾廣告將宮廟加持等宗教情境結合，增加民眾購買理由。

「投資」位居本週第 2 名，相關命理廣告從投資失利、家庭開銷與錢留不住的困擾切入。與這類諮詢訴求相連的「老師」「財運」，分居第 4 名及第 5 名。顯示廣告除了財務困擾外，進一步結合工作起伏、人際不順與改運等作為話術。為了吸引民眾進一步諮詢，廣告強調「每個人的原因都不同」，以老師能協助釐清個人問題的說法，邀請民眾留言或私訊老師，尋求改善現況的方法。

「貸款」位居本週第 10 名，相關中古車廣告主打全額貸款購車與原車融資，吸引有購車或週轉需求的民眾詢問。延續借貸主題，第 8 名的「免費」用於小額借款的線上試算，吸引民眾了解借款服務。這則借款廣告鎖定有工作者，宣稱沒有薪轉、勞保，或已有其他借貸也可申請。

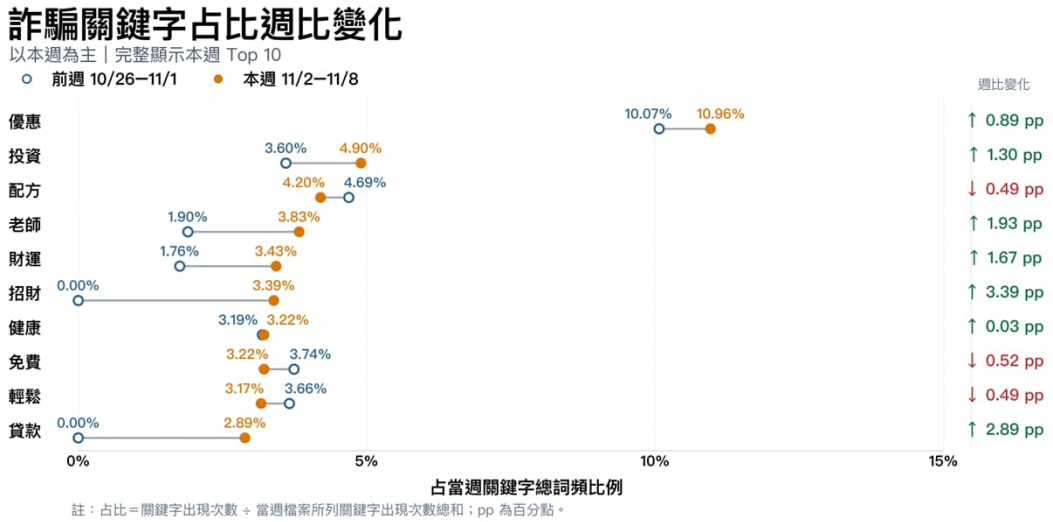


圖7 | 詐騙關鍵字占比週比變化

結語

本週高風險廣告以生活需求與財務困擾吸引注意，透過限時優惠、功效與授權宣稱、免費體驗，引導民眾購買或聯繫。因此，民眾看到這類型的廣告時，應先查證商品業者、授權機關等真實身分，再確認付款、退費等具體方法。即使有贈品或免費等誘因，仍應多花時間核對資訊，避免急著改善現況而倉促決定。

焦點文章

「資安共好-2026產品資安研討會」高峰論壇總結分析

2026年10月8日，數位發展部資通安全署與國家資通安全研究院舉辦「資安共好 - 2026年產品資安研討會」，詳見圖8。其中，高峰論壇以「政府、產業、學研與社群如何攜手共創產品資安新局」為主題，邀集台灣資安主管聯盟、財團法人開源基金會、中華民國資訊軟體服務商業同業公會及國立臺灣科技大學等專家，以產業實務需求為核心，聚焦PSIRT 與 SBOM、開源軟體治理、AI 漏洞驗證、中小企業導入及人才培育等議題，共同探討產品資安的實務挑戰與未來合作方向。



圖8 | 資安共好-2026產品資安研討會

註：由左至右依序為國家資通安全研究院林志堯副院長、台灣資安主管聯盟游政卿副會長、財團法人開源基金會蔡祈岩董事長、中華民國資訊軟體服務商業同業公會吳明蔚理事及國立臺灣科技大學鄭欣明教授。
圖片來源：本研究團隊提供。

一、整合 PSIRT 與 SBOM 建立完整的產品漏洞管理流程

產品安全事件應變團隊（PSIRT）與軟體物料清單（SBOM）是企業建立漏洞管理能力的重要基礎。與談人指出，PSIRT應具備跨部門協調能力，讓外部漏洞通報能有效連結研發、品質管理及客戶服務等單位，完成漏洞分析、影響評估、修補決策與資訊揭露。SBOM則應融入產

焦點文章

品開發流程，並隨產品版本更新持續維護元件資訊，以利企業於漏洞發生時，迅速確認可能受影響的產品及版本。

二、開源軟體管理與長期維護責任成為企業新挑戰

隨著開源軟體廣泛應用於網通設備、嵌入式系統及各類數位產品，如何掌握第三方元件風險並維持長期安全支援為企業關注面向。與談人指出，傳統製造業過去較重視產品開發與交付，但隨著產品資安要求逐步延伸至上市後的支援期間，企業須重新評估軟體更新、漏洞修補及長期維護所需的人力與資源。

三、AI 加速漏洞挖掘，驗證與處置能力成為管理關鍵

AI Agent、自動化分析工具及沙盒驗證環境的整合，正逐步提升原始碼分析、漏洞挖掘及概念驗證程式產生的效率。然而，漏洞發現速度提升，也可能增加企業在技術確認、風險評級及修補排序上的負擔，尤其自動化工具產生的分析結果仍可能存在誤判，讓漏洞驗證與處置成為新的管理挑戰。

與談人建議，企業可結合AI工具、自動化沙盒與產品實際使用情境，強化漏洞重現、影響分析及處置分流能力，降低人工驗證負擔。同時，AI產生的分析結果及修補程式仍須經過必要的技術確認、品質測試與人員審查，確保漏洞處置結果的可靠性。

四、由大帶小與實作輔導，降低中小企業導入門檻

相較於大型成熟的企業，中小企業在建立產品漏洞管理機制時，經常面臨缺乏專業人才、技術資源及導入誘因等問題。與談人建議，可透過大型企業帶動供應商，依產品風險及供應鏈角色，優先協助中小企業建立漏洞通報窗口、SBOM管理方式及產品支援期限等基本能力。在政策推動方面，宜兼顧企業規模與資源差異，透過分級要求、共享工具及實作輔導等方式降低企業導入負擔，亦可結合國際標準與國內產業需求，提供中文化教材、實作工作坊及陪伴式輔導，協助企業實際演練漏洞通報、影響評估與修補流程，促進產品資安管理制度落地。

焦點文章

五、結合資源以共享技術與人才資源

隨著開源軟體維護需求增加及AI工具快速發展，企業所需的資安能力已從傳統漏洞挖掘與修補，逐漸延伸至開源元件維護、漏洞驗證、風險評估及自動化工具應用。與談人建議，透過政府、產業、學研及開源社群合作，鼓勵國內工程師參與國際開源組織與專案，累積實際開發及安全維護經驗。

六、總結

綜整本次論壇討論，企業面臨的挑戰主要涉及管理流程整合、開源元件長期維護、自動化漏洞驗證、供應鏈資源落差及專業人才不足等面向。本次高峰論壇呈現企業在產品漏洞管理、開源軟體維護及新興技術應用方面的實際需求，相關成果可作為後續研擬企業實務指引、規劃產業輔導措施及深化技術合作的參考，逐步提升我國產業的產品資安管理與應變能力。

關鍵字：產品資安、PSIRT、SBOM、開源軟體、AI 漏洞驗證、中小企業、人才培育

刊　　名　資安週報第 70 期
發 行 人　國家資通安全研究院　龔化中院長
主編中心　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

本刊所有圖文內容均受著作權法保護，未經授權，禁止翻印、複製、轉載。