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
整體風險持平 元件高風險小幅增加

重大漏洞
Microsoft、Cisco、Fortinet、Veeam、PHP、Node.js及Citrix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
威脅情資平台及程式遞送控制器(ADC & Gateway)仍為攻擊熱點

事件通報
多因子驗證可降低帳密失守後的帳號接管風險

網路巡查高風險詐騙
產品服務仍占七成以上 金融投資型占比回升

焦點文章
115年度資安稽核技術檢測統計與案例

2026.10.29
068

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

整體風險持平 元件高風險小幅增加

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2,791項。其中，「元件高風險漏洞」以922項居首，「過時或弱加密協定」720項次之，「TLS憑證不受信任」673項位居第三。前三項合計2,315項，占前10大風險項目總數約82.9%，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2,798項，本期整體風險數量減少7項，降幅約0.3%，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895項增至本期922項，增幅約3.0%。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732項減至720項，降幅約1.6%；「TLS憑證不受信任」由695項減至673項，降幅約3.2%。另「CSP設定不當」由237項減至235項，降幅約0.8%；「未部署WAF」維持102項，沒有變化。

整體而言，本期外部曝險風險數量較上期變動不大，風險分布大致維持穩定，顯示各類風險項目雖有小幅增減，但整體尚未呈現明顯改善趨勢。建議持續優先修補高風險漏洞、強化加密協定與憑證管理，並完善網站安全防護機制，以逐步降低外部曝險風險。

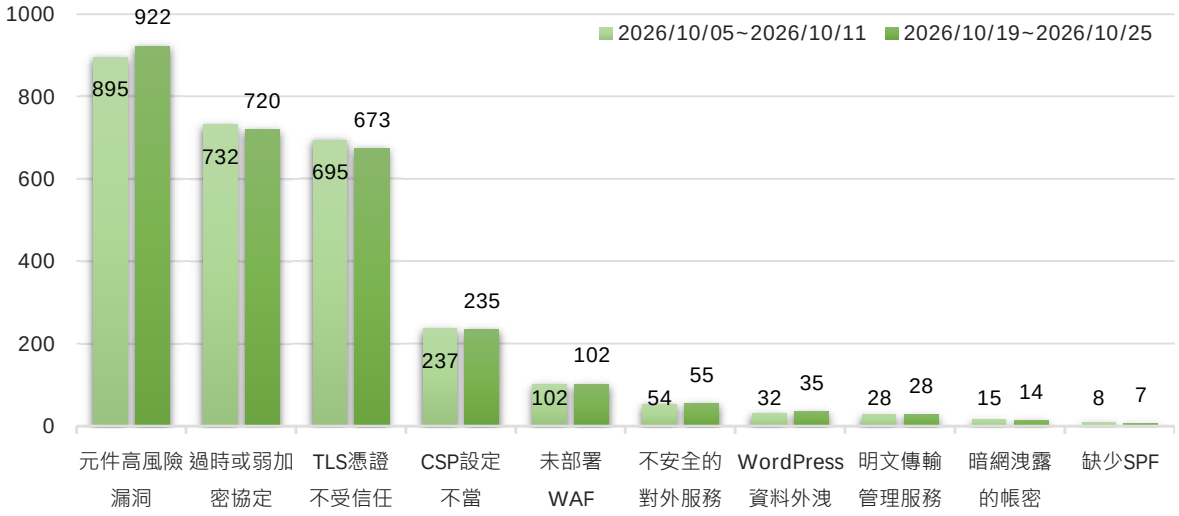


圖1 | EASM檢測結果統計(前10大風險)

防護建議

建議受測單位採取下列防護措施	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

Microsoft、Cisco、Fortinet、Veeam、PHP、Node.js及Citrix高風險漏洞應盡速修補

微軟釋出115年10月份安全性更新，共修補1416個漏洞，其中包含268個高風險漏洞[1]，且CVE-2026-96951已遭駭客濫用。

- Cisco License On-Prem(原名Cisco Smart Software Manager On-Prem)存在缺乏授權(Missing Authorization)漏洞(CVE-2026-20328)[2]，未經身分鑑別之遠端攻擊者可透過網頁管理介面重設任意帳號(含管理者)之通行碼，進而在未經授權之情況下存取系統。
- Cisco Secure Email Gateway (SEG)之Advanced Malware Protection (AMP)功能存在相對路徑遍歷(Relative Path Traversal)漏洞(CVE-2026-76519)[3]，當File Reputation服務啟用時，未經身分鑑別之遠端攻擊者，可藉由向受影響設備寄送含特製附件之電子郵件，進而於底層作業系統寫入任意檔案，並以root權限執行指令，該漏洞已遭駭客濫用。
- Fortinet FortiSIEM存在路徑遍歷(Path Traversal)漏洞(CVE-2026-106173)[4]，未經身分鑑別之遠端攻擊者可藉由傳送特製封包，進而執行未經授權之程式碼或指令。
- Fortinet FortiAnalyzer存在SQL注入(SQL Injection)漏洞(CVE-2025-46773)[5]，已通過身分鑑別之遠端攻擊者可藉由傳送特製請求，進而執行任意指令。
- Veeam Backup & Replication存在不安全之反序列化(Insecure Deserialization)漏洞(CVE-2025-64393)[6]，具備Backup Viewer角色且已通過身分鑑別之遠端攻擊者，可藉由Mount Service對所接收之未受信任資料進行不安全反序列化之缺陷，進而於Veeam備份伺服器(Backup Server)以SYSTEM權限執行任意程式碼。
- PHP存在使用釋放後記憶體(Use After Free)漏洞(CVE-2026-109618與CVE-2026-109619)[7]，攻擊者可透過傳送特製之multipart/form-data HTTP請求，於未經身分鑑別之情況下，於伺服器底層執行任意程式碼，網路上已出現本漏洞概念驗證程式(PoC)。

- Node.js存在4項高風險安全漏洞(CVE-2026-105482、CVE-2026-105483、CVE-2026-106069及CVE-2026-111497)[8]，類型包含空字元輸入驗證不足、TLS憑證主機名稱檢查繞過(TLS Certificate Hostname Bypass)及越界寫入(Out-of-Bounds Write)。
  - CVE-2026-105482：dns.resolve函式處理含NUL字元之名稱時，會將名稱截斷。
  - CVE-2026-105483：Node.js 24.x與26.x版本中，當IP位址以全形書寫時，攻擊者可繞過TLS憑證之主機名稱檢查。
  - CVE-2026-106069：當主機名稱為非標準格式之IP位址時，攻擊者可繞過TLS憑證之主機名稱檢查。
  - CVE-2026-111497：Brotli解碼器存在越界寫入缺陷，可導致遠端執行程式碼。
- Citrix NetScaler ADC與Citrix NetScaler Gateway存在記憶體溢位(Memory Overflow)漏洞(CVE-2026-107406)[9]，當設備設定為SAML SP或SAML IdP時，未經身分鑑別之遠端攻擊者可觸發記憶體溢位，進而達成執行任意程式碼或造成服務阻斷。

[1] https://msrc.microsoft.com/update-guide/releaseNote/2026-Oct
[2] https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ssm-access-nttb2dhE
[3] https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-esa-afw-zqYJkjxP
[4] https://fortiguard.fortinet.com/psirt/FG-IR-26-180
[5] https://fortiguard.fortinet.com/psirt/FG-IR-26-178
[6] https://www.veeam.com/kb4934
[7] https://www.php.net/archive/2026.php#2026-10-20-1
[8] https://nodejs.org/en/blog/vulnerability/october-2026-security-releases
[9] https://support.citrix.com/support-home/kbsearch/article?articleNumber=CTX697191

■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15.3%，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12.3%，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程式碼，以達成後續攻擊目的。觀察到的主要手法包括 Visual Basic 腳本執行、JavaScript 腳本執行、以及PowerShell 指令執行。攻擊者可能透過惡意文件或腳本觸發 Visual Basic 程式碼執行，亦可能利用 JavaScript 執行惡意指令或下載其他攻擊工具，並藉由 PowerShell 等系統內建管理工具執行遠端指令、下載惡意程式或蒐集系統資訊。此類行為通常利用合法腳本語言與系統元件執行惡意操作，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、持續存取及橫向移動的重要基礎。建議機關強化腳本執行行為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，以降低攻擊者濫用合法工具執行惡意程式碼的風險。

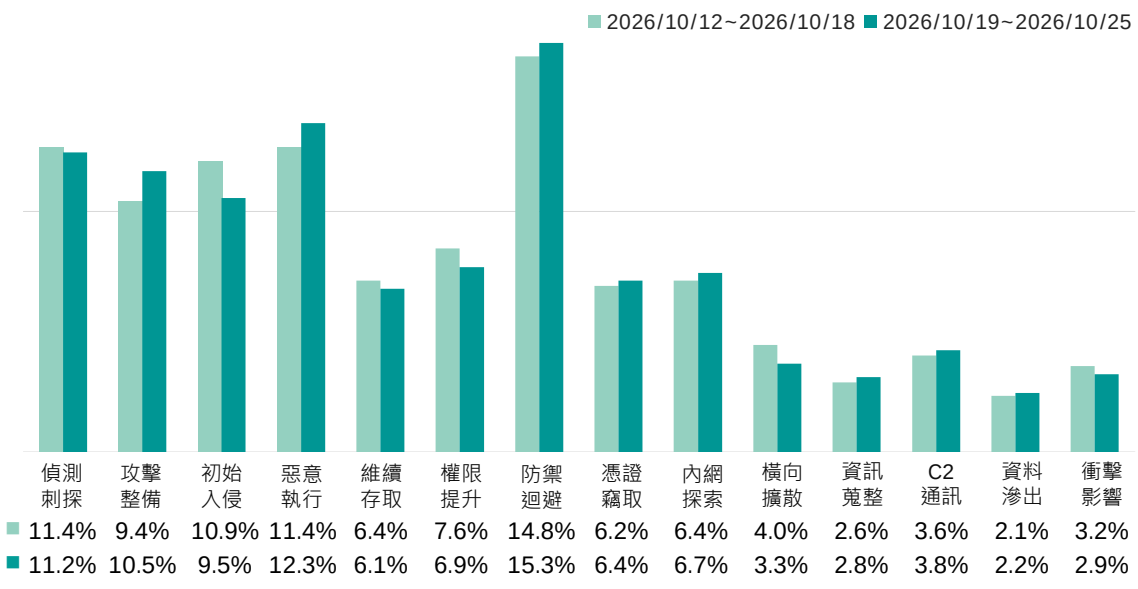


圖2 | 資安聯防監控攻擊階段統計

防護建議

建議機關採取下列防護措施

防禦迴避 (Defense Evasion)

占比 15.3%

- 強化端點偵測與防護： 部署 EDR 等端點防護機制，監控異常程序及可疑指令執行行為
- 加強日誌稽核與保存： 啟用系統指令及操作日誌紀錄，並集中保存，防止攻擊者刪除或竄改紀錄
- 限制高風險工具使用： 監控系統內建管理工具的異常使用行為，降低合法工具遭濫用的風險
- 落實最小權限原則： 限制特權帳號及系統管理權限，避免攻擊者取得修改安全設定或清除紀錄的能力

惡意執行（Execution）

占比 12.3%

- 強化腳本執行監控： 監控 PowerShell、Visual Basic 及 JavaScript 等腳本的異常執行行為
- 落實應用程式執行控管： 建立應用程式允許清單，限制未授權程式及惡意腳本執行
- 加強 PowerShell 日誌稽核： 啟用 PowerShell Script Block Logging 等機制，偵測可疑指令及惡意操作
- 限制腳本執行權限： 依業務需求限制非必要的腳本執行功能，降低攻擊者利用系統內建工具執行惡意程式碼的風險

■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

威脅情資平台及程式遞送控制器(ADC & Gateway)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74.55%、「遠端控制」服務攻擊占比20.20%，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65.93%。「遠端控制」服務亦有30.09% 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服務系統比例下降主因為Parse Server存在資訊外洩漏洞之CVE-2025-53364，遭攻擊次數下降導致。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。

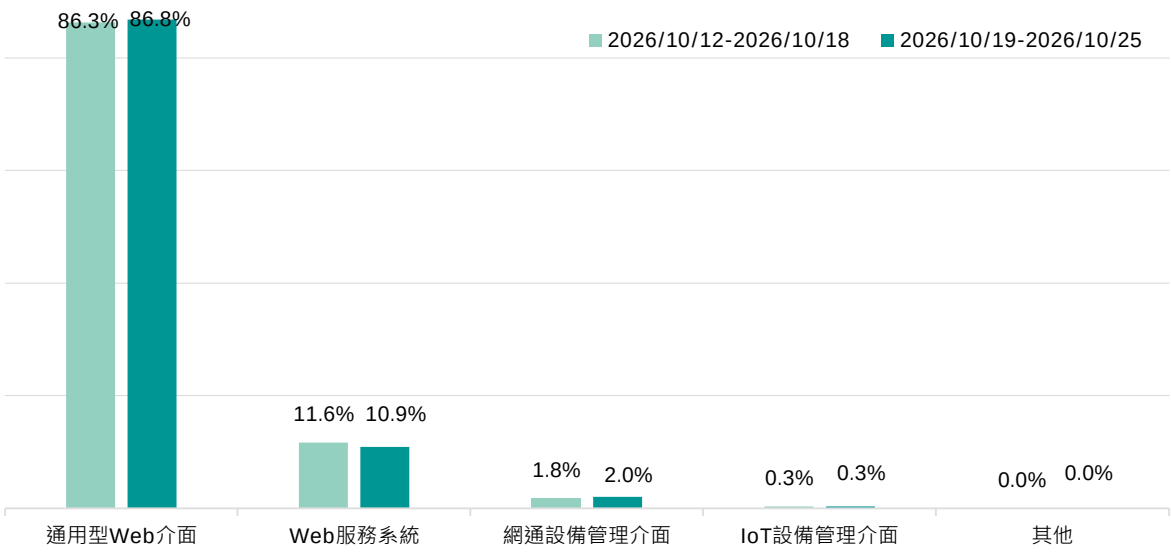


圖3 | 本週網頁應用介面之誘捕攻擊比例統計

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權限提升漏洞、越界讀取漏洞、釋放後使用漏洞、SQL注入漏洞及身分驗證繞過漏洞，攻擊目標涵蓋威脅情資平台、程式遞送控制器(ADC & Gateway)、網頁瀏覽器、網頁應用程式框架及網站主機伺服器管理系統。

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-2026-27960[1]	OpenCTI	9.8	
■	2	-	CVE-2026-3055[2]	NetScaler ADC & Gateway	9.8	✓
■	3	⬆new	CVE-2026-10961[3]	iOS 版 Chrome 瀏覽器	8.3	✓
■	4	⬆new	CVE-2026-1207[4]	Django	8.3	
■	5	⬇1	CVE-2026-41940[5]	cPanel & WHM	9.8	✓

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

1. https://nvd.nist.gov/vuln/detail/CVE-2026-27960
2. https://nvd.nist.gov/vuln/detail/CVE-2026-3055
3. https://nvd.nist.gov/vuln/detail/CVE-2026-10961
4. https://nvd.nist.gov/vuln/detail/CVE-2026-1207
5. https://nvd.nist.gov/vuln/detail/CVE-2026-41940

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

多因子驗證可降低帳密失守後的帳號接管風險

本週總計接獲32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系統遭入侵占多數，詳見圖5。本週發現部分機關之 Web Mail 及網站登入功能遭受暴力破解攻擊。其中某機關 Web Mail 已啟用雙因子驗證，當帳號密碼驗證通過後，系統仍會透過行動裝置推播要求使用者再次確認登入身分，因此攻擊者即使取得或猜中帳號密碼，仍無法直接完成登入及後續操作。此案例顯示，僅依帳號密碼進行身分驗證，當密碼遭猜測、重複使用或外洩時，容易直接形成帳號遭接管風險；導入多因素驗證則可增加額外的身分確認程序，降低單一密碼失守所造成的影響。

建議機關針對 Web Mail、遠端存取、管理後台及其他可由外部登入之重要系統，優先導入多因素驗證，避免僅憑帳號密碼即可完成登入；並持續監控短時間大量登入失敗、單一帳號遭多來源嘗試及異常地區登入等行為。採用推播式驗證時，亦應提醒使用者僅核准本人發起之登入要求，對於非本人操作之驗證通知應拒絕，並依機關內部資安通報程序通知資訊或資安單位，確認帳號是否遭暴力破解、密碼外洩或其他異常存取。

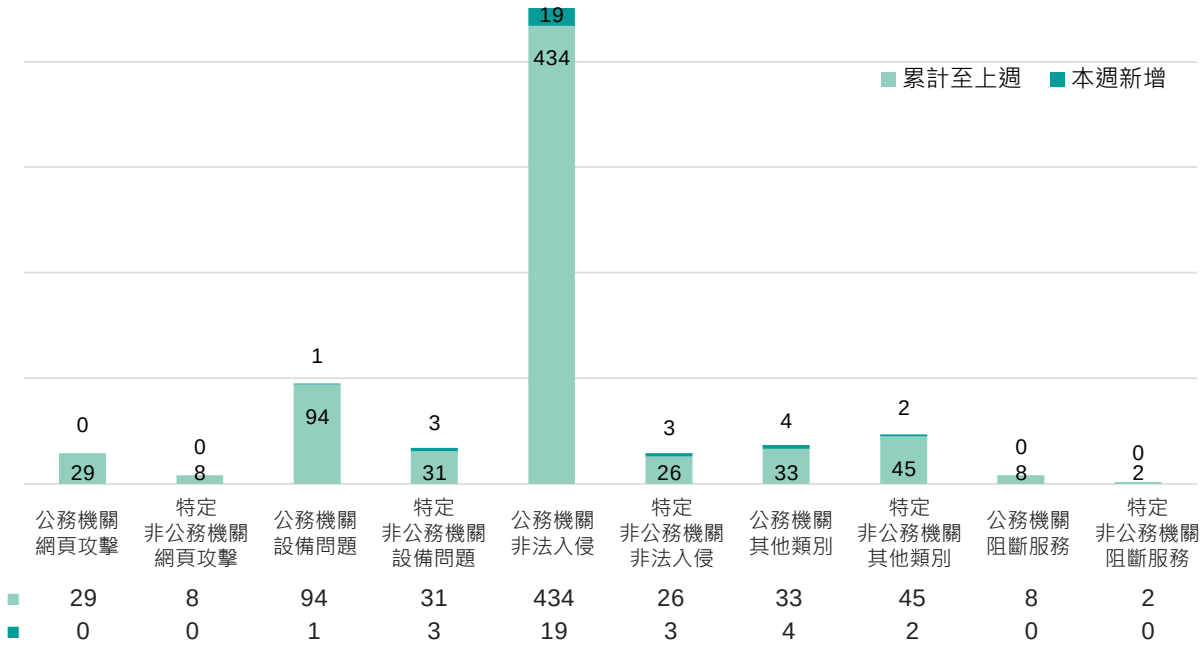


圖4 | 本週公務機關暨特定非公務機關資安事件通報概況

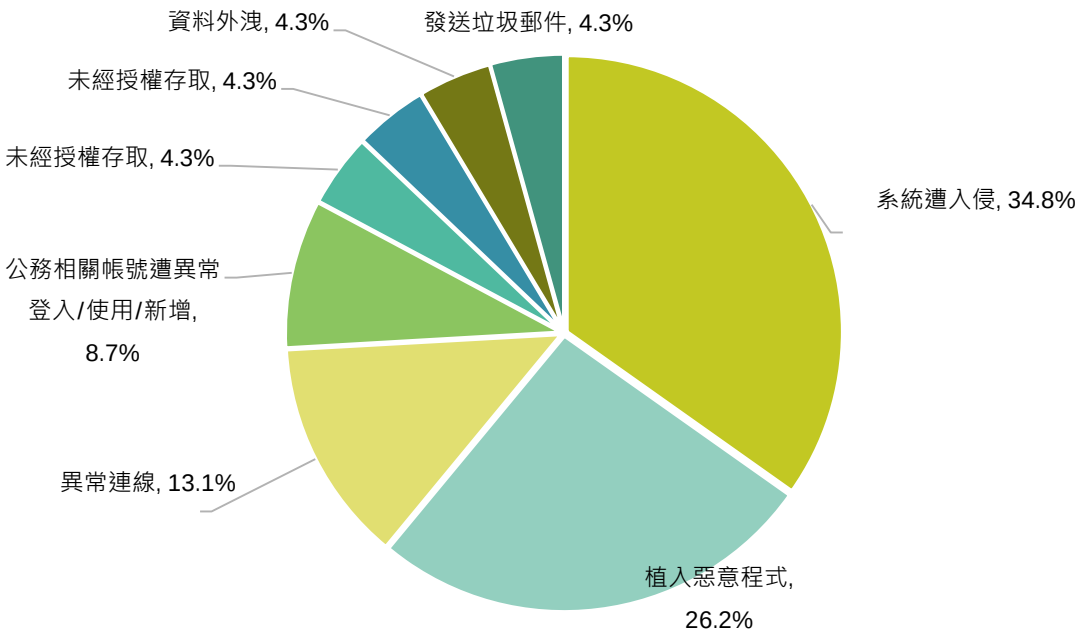


圖5 | 本週公務機關非法入侵事件類型占比

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
➢ 攻擊者透過暴力破解或外洩密碼登入系統接管重要帳號 ➢ 攻擊者持續發送惡意驗證推播誘騙使用者核准登入要求	➢ 重要系統全面導入多因素驗證機制，避免僅憑帳號密碼即可完成登入 ➢ 建立登入失敗次數限制及異常告警，防範暴力破解與密碼猜測攻擊 ➢ 強化異常來源及地區登入監控，及早發現多來源嘗試與帳號濫用行為 ➢ 加強推播驗證安全宣導，要求使用者拒絕非本人登入並通報異常通知

7間民間企業揭露重大資安訊息

本週7間民間企業發布重大訊息，產業類分別為居家生活業、生技醫療業、觀光餐旅業、運動休閒業、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
滿心企業股份有限公司	2026年10月19日	滿心公司委外服務平台業者所提供之資料庫發生自動化攻擊事件，部分資訊遭非法擷取，近日接獲消費者反映疑似個資外洩情形。已立即與委外服務平台業者聯繫，並要求其釐清相關資料是否涉及本次資安事件及實際受影響範圍，同時啟動內部應變及調查機制，採取必要之防護及風險控管措施，且已於公司官網及APP加強反詐騙宣導。
立康生醫事業股份有限公司	2026年10月21日	立康公司接獲消費者反映疑似個資外洩事件，公司委外廠商管理之平台，疑似有第三方不當取得資料並透過電子郵件聯繫消費者。獲悉後已立即啟動資安事件應變機制，並責成購物網平台委外廠商立即進行相關調查、檢視及必要之修補改善。
開曼美食達人股份有限公司	2026年10月21日	台灣子公司美食達人股份有限公司發現部分資訊系統遭受駭客網路攻擊，資安部門已全面啟動相關防禦機制與備援作業，同時協調外部資安公司技術專家共同合作處置，經初步評估，並綜合考量係單一市場事件，目前尚未對合併公司整體之營運及財務造成重大影響。

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
清淨海生技股份有限公司	2026年10月22日	清淨海公司接獲消費者反映，公司委外廠商管理之平台疑似有第三方不當取得資料，並透過電子郵件聯繫消費者。已立即啟動資安事件應變機制，並責成官網平台委外廠商立即進行相關調查、檢視及必要之修補改善。目前事件原因及可能影響範圍尚在調查釐清中。
科懋生物科技股份有限公司	2026年10月22日	科懋公司接獲線上會員通知個資洩漏情形，經查主因本公司產品線上銷售平台之系統服務委外廠商其對外服務系統遭自動化攻擊，並對線上訂單資料庫擷取。已主動聯繫系統服務委外廠商並依個資事故通報及處理流程啟動應變會議，並採取必要通知及防護措施以防堵、及降低影響，同時已主動通報相關主管機關；此外，也持續透過官網、Facebook、會員APP及簡訊進行反詐騙宣導。
歐都納股份有限公司	2026年10月22日	歐都納公司委外服務平台業者資料庫受到自動化攻擊事件，部分資訊遭非法擷取，後續接獲消費者反映疑似個資外洩情形，獲悉相關情事後，已立即啟動資安事件應變機制，並與委外服務平台業者聯繫要求其釐清公司實際受影響範圍，目前事件原因及可能影響範圍尚在調查釐清中。

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
柏文健康事業股份有限公司	2026年10月23日	柏文公司接獲電子商城線上平台委外服務廠商通知其 Commerce Cloud資料庫受到攻擊，部分資料遭未經授權存取，該資料庫包含本公司電子商城訂單資料，惟截至目前為止，平台委外服務廠商尚無法釐清相關資料是否受到影響及其範圍。之後陸續接獲線上會員反映，疑似有第三方不當取得資料，並透過電子郵件聯繫消費者，經比對郵件內容與本公司電子商城訂單資訊有關。目前已依個資事故通報及處理流程召開應變會議，並採取必要防護措施以降低事件影響；此外，為防範電子商城訂單資料遭詐騙集團利用，本公司已透過電子商城官網、線上會員電子郵件及簡訊發布防詐騙提醒。

■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

產品服務仍占七成以上 金融投資型占比回升

詐騙類型趨勢

產品服務型占比回落，仍占本週高風險內容七成以上，詳見圖6。車用吸塵器廣告把清潔毛髮、替輪胎充氣等需求放在一起，宣稱一機兼具多種用途，再搭配光復節與雙十一活動、工廠清倉及「僅限今日」促銷，引導民眾點擊了解商品。收納包廣告先強調商品可以集中整理零錢、鑰匙等隨身小物，方便外出攜帶，再推出雙十一早鳥限時優惠，吸引民眾趁優惠期間下單購買。

身分冒充型本週降為三類中占比最低。眼霜廣告借用醫師名義，聲稱由醫師親手配製、能淡化細紋，並以掃碼驗真與「假一賠十」承諾減輕真偽疑慮，再搭配買四送四吸引購買。面膜廣告宣稱韓國原裝進口、取得正規授權，以網紅推薦塑造可信形象，吸引民眾留言，再由小編私訊團購連結。

金融投資型本週回升至第二位。房產廣告以低自備款與 30 個月包租保證吸引買方，宣稱購屋後即可收租，也把捷運預計通車描繪為房價上漲的理由，吸引期待日後以較高價格轉售獲利的民眾預約了解建案。海外房產說明會主打跨國配置與財富傳承，宣稱當地房市穩健、具稅制優勢，再以移民團隊駐場及案例分享塑造專業形象，招攬民眾報名了解房產投資與移民規劃。

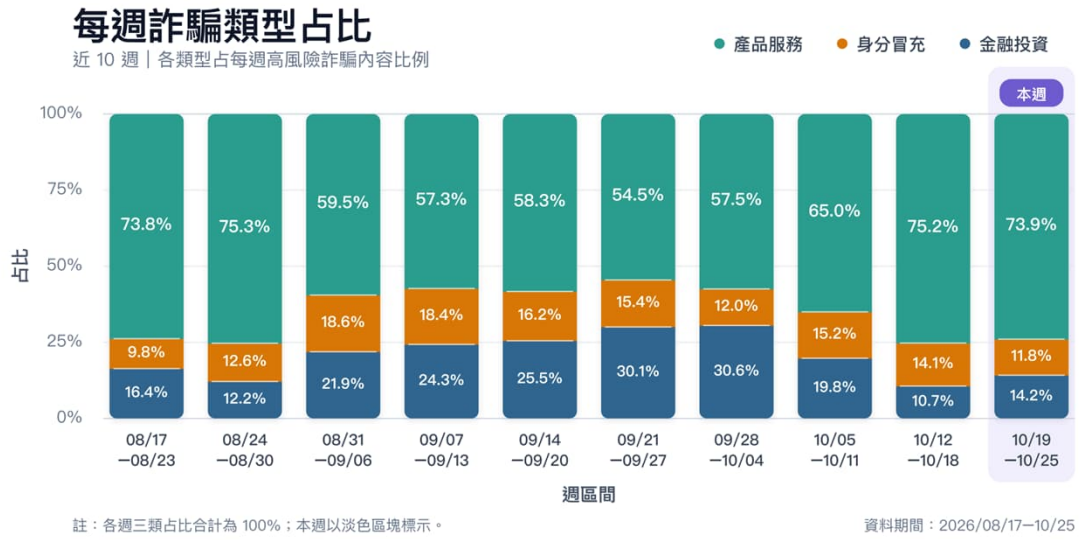


圖6 | 每週詐騙類型占比

關鍵字趨勢

「優惠」續居首位，防曬美妝廣告延續前週的一瓶多用與限時低價訴求，將日常妝前準備包裝得簡單省事。「免費」升至第 3 名，相關廣告從前週的房貸評估轉向購車貸款諮詢，搭配線上下訂折扣與前三至六期免繳車貸的承諾，以減輕初期付款負擔為訴求，吸引民眾詢問可貸額度與每月還款金額，詳見圖7。

「配方」與「日常」進入本週前 10 名，分居第 5、第 8 名。「配方」相關廣告以控制體重為訴求推銷保健品，宣稱食用後能提高代謝、增加熱量消耗，並把餐前吃兩顆的效果比擬為騎腳踏車 40 分鐘。廣告再搭配會員折扣，吸引想控制體重的民眾購買。「日常」相關廣告推銷嚨片，宣稱能舒緩喉嚨乾癢，並主張經常說話或待在冷氣房的人，即使沒有感冒也需要使用，再以試用無效可退費的承諾吸引購買。

「投資」升至第 2 名，命理廣告列舉投資失利、家庭開銷等困擾，以釐清留不住錢的原因吸引留言或私訊諮詢。「股票」進入本週前 10 名。前週相關課程廣告主打利用人工智慧分析股價，本週則以教導如何判斷放空股票的時機為訴求。放空是一種以股價下跌獲利為目標的交易方式，廣告藉此吸引擔心行情下跌、希望學習這類交易方法的民眾報名。綜觀本週前十大關鍵字，商品促購之外，財務焦慮也被用來招攬諮詢與課程報名。

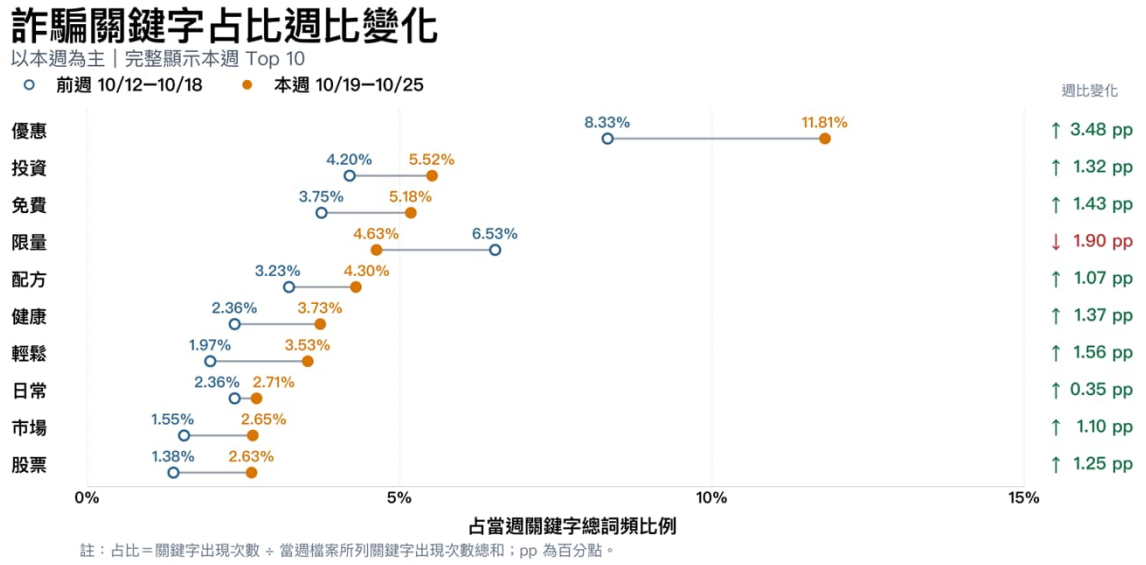


圖7 | 詐騙關鍵字占比週比變化

焦點文章

115年度資安稽核技術檢測統計與案例

115年本院執行政府機關資安稽核技術檢測，已完成年度10個公務機關之技術檢測作業。檢測結果顯示，多數機關已具備基本之資安防護能力；於八大檢測構面中，「資料庫安全檢測」、「網路惡意活動檢視」、「組態設定安全檢測」及「網域主機安全防護檢測」屬於表現較為優異之項目。而「使用者電腦安全檢測」、「核心資通系統安全檢測」、「網路架構檢測」及「物聯網設備檢測」於所有受檢機關皆屬有進一步精進資安防護空間之項目。

八大檢測構面檢測共同性發現結果：

1. 使用者電腦安全檢測：共發現高風險弱點89項、中風險弱點50項，作業系統支援已知遭破解之加密演算法(如3DES、DES及RC4)。
2. 物聯網設備檢測：共發現高風險弱點35項、中風險弱點43項，主要缺失為設備SNMP代理程式使用預設社群名稱、支援已知遭破解之加密演算法，以及SNMP服務未對GETBULK請求進行限制等。
3. 網域主機安全防護檢測：共檢測AD網域主機9台，均已安裝防毒軟體並完成病毒碼更新且未發現惡意程式，僅2台網域主機未落實安全性更新修補作業。
4. 資料庫安全檢測：共發現4個機關之資料庫於傳輸加密安全機制上未啟用強制加密。
5. 核心資通系統安全檢測：內網滲透測試共發現高風險弱點59項、中風險弱點10項及低風險弱點7項，弱點類型最多為無效的存取控管與注入攻擊；防護基準檢測則發現29項不符合項目，多為未限制新密碼不得與前3次使用之密碼相同、使用預設密碼登入時未要求立即變更，以及逾越許可閒置時間時系統未自動將使用者登出。
6. 網路架構檢測：共發現高風險17項、中風險22項及建議項目6項，主要缺失包含網路設備未妥善存取控管、未適當限制服務區域連線、未完整部署入侵偵測 / 防禦系統及網路設備未正確校時等。
7. 組態設定安全檢測(GCB)：共發現31台使用者電腦、1台網域主機、6台網通設備及5台伺服器主機之組態設定未符規範，顯示部分機關在基礎設定上仍有未落實之情形。
8. 網路惡意活動檢視：發現5個機關未能完全阻擋惡意中繼站名單，其餘機關均已達100%阻擋率，本年度未發現APT網路惡意流量。

焦點文章

本年度資安稽核技術檢測發現之弱點案例說明如下：

一、SWEET32弱點 部分使用者電腦存在SWEET32弱點，攻擊者若處於同一實體網段，極易規避中強度加密演算法，詳見圖8 。

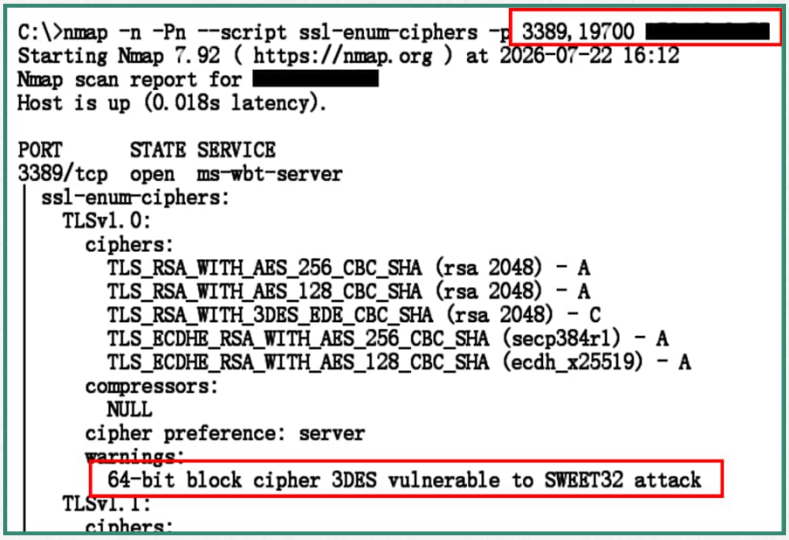


圖8 | SWEET32弱點示意圖

二、資料庫傳輸機制未啟用強制加密功能 傳輸資料若未加密將流於明文狀態，攻擊者可透過網路監聽工具(如Wireshark)直接竊聽並獲取所有帳號密碼與個資，或發動中間人攻擊(MitM)攔截並竊取完整通訊內容，詳見圖9。

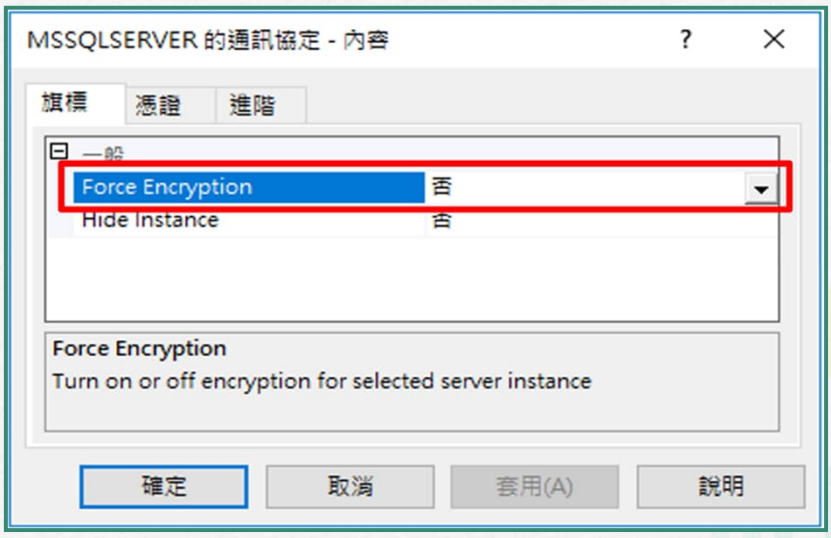


圖9 | 資料庫傳輸機制未啟用強制加密功能示意圖

焦點文章

防護建議：

建議各機關應全面停用作業系統與物聯網設備中已知遭破解之加密演算法(如3DES、DES及RC4)；落實物聯網設備管理，變更SNMP預設社群名稱並限制GETBULK請求；持續辦理網域主機安全性更新與修補。

資料庫連線應全面啟用傳輸強制加密機制，以防範網路監聽與中間人攻擊(MitM)；檢討並強化核心資通系統之存取控管與注入攻擊防護，確實落實密碼歷程限制、強制變更預設密碼及閒置自動登出機制。

收斂網路設備存取控制規則，完善入侵偵測防禦系統與校時設定，並確實落實各項設備之政府組態基準(GCB)；同時持續精進惡意中繼站黑名單部署管理，以達到全面阻擋可疑連線，確保整體資安防護能量持續提升。

關鍵字：資安稽核技術檢測、SWEET32、資料庫傳輸加密

刊　　名　資安週報第 68 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

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。