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
整體曝險風險變化不大 主要風險項目維持穩定

重大漏洞
Cisco與Splunk高風險漏洞應盡速修補

聯防監控
防禦迴避高居首位 偵測刺探仍具威脅

蜜罐誘捕
威脅情資平台及程式遞送控制器(ADC & Gateway)成為攻擊熱點

事件通報
瀏覽器儲存帳密可能擴大端點遭入侵後的影響

網路巡查高風險詐騙
產品服務占比攀升 廣告以日常需求吸引購買

焦點文章
政府領域資安事件趨勢研析

2026.10.15
066

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

整體曝險風險變化不大 主要風險項目維持穩定

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2,798項。其中，「元件高風險漏洞」以895項居首，「過時或弱加密協定」732項次之，「TLS憑證不受信任」695項位居第三。前三項合計2,322項，占前10大風險項目總數約83.0%，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2,795項，本期整體風險數量增加3項，增幅約0.1%，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884項微增至本期895項，增幅約1.2%。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，另外本期發現新增WordPress Core相關弱點(CVE-2026-87902)，該弱點係因WordPress於解析頁面範本時，未妥善限制範本檔案之存取路徑，未經身分鑑別之遠端攻擊者可利用路徑遍歷方式，於特定環境條件下造成程式碼執行風險，建議升級至WordPress 7.1.2以上之已修補版本，或依使用中版本分支更新至官方提供之對應修補版本。「過時或弱加密協定」維持732項，沒有變化；「TLS憑證不受信任」由694項微增至695項，增幅約0.1%。另「CSP設定不當」由240項微降至237項，降幅約1.3%；「未部署WAF」由107項降至102項，降幅約4.7%。

整體而言，本期外部曝險風險數量與上期相比變化不大，整體風險分布維持相對穩定。其中，「元件高風險漏洞」及「TLS憑證不受信任」略有增加，「過時或弱加密協定」維持不變，而「CSP設定不當」及「未部署WAF」則小幅下降，顯示各類風險項目僅呈現輕微波動，尚無明顯改善趨勢。建議持續落實高風險漏洞修補、加密協定與憑證管理，並強化網站安全防護措施，以逐步降低整體外部曝險風險。

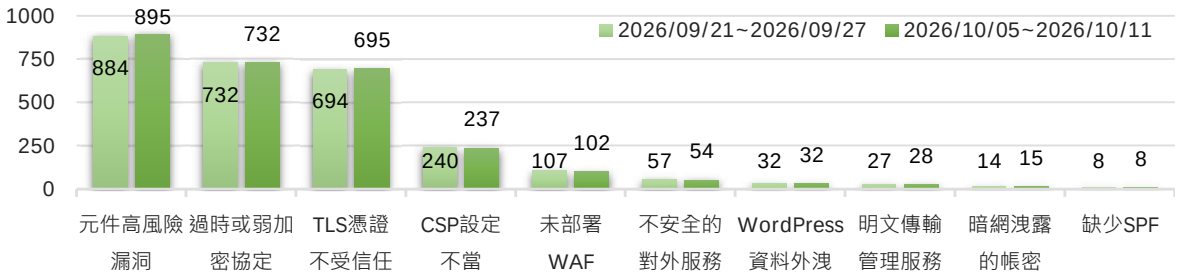


圖1 | EASM檢測結果統計(前10大風險)

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

Cisco與Splunk高風險漏洞應盡速修補

- Cisco Catalyst SD-WAN Manager存在身分鑑別繞過(Authentication Bypass)漏洞(CVE-2026-76504)[1]，未經身分鑑別之遠端攻擊者可藉由傳送經URI編碼之特製HTTP請求，繞過身分鑑別，進而以Admin權限存取受影響系統，該漏洞已遭駭客濫用。
- Splunk Enterprise存在缺乏身分鑑別(Missing Authentication)漏洞(CVE-2026-76268)[2]，未經身分鑑別之遠端攻擊者，可利用Search Head叢集成員之Patroni REST API對關鍵組態操作未要求身分鑑別之缺陷，進而執行任意作業系統指令。

[1] https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-webauth-xr8beuuU
[2] https://advisory.splunk.com/advisories/SVD-2026-1001

■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2。「防禦迴避」為最常見攻擊手法，占比13.6%，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12.1%，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活動，以掌握對外暴露資產及潛在攻擊入口。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外部網段及公開服務進行大規模探測，以識別可存取主機、開放埠及系統服務資訊，並進一步針對目標系統進行漏洞掃描，尋找可能遭利用的已知弱點。此類活動通常呈現由廣泛網路掃描逐步聚焦至特定系統與潛在漏洞的特徵，可協助攻擊者掌握目標環境的安全弱點，作為後續漏洞利用及初始入侵的重要依據。建議機關持續強化異常掃描流量與可疑來源的監控，定期盤點對外暴露資產並優先修補高風險漏洞，同時結合威脅情資進行掃描來源分析與適當阻擋，以提前辨識潛在攻擊準備活動並降低後續入侵風險。

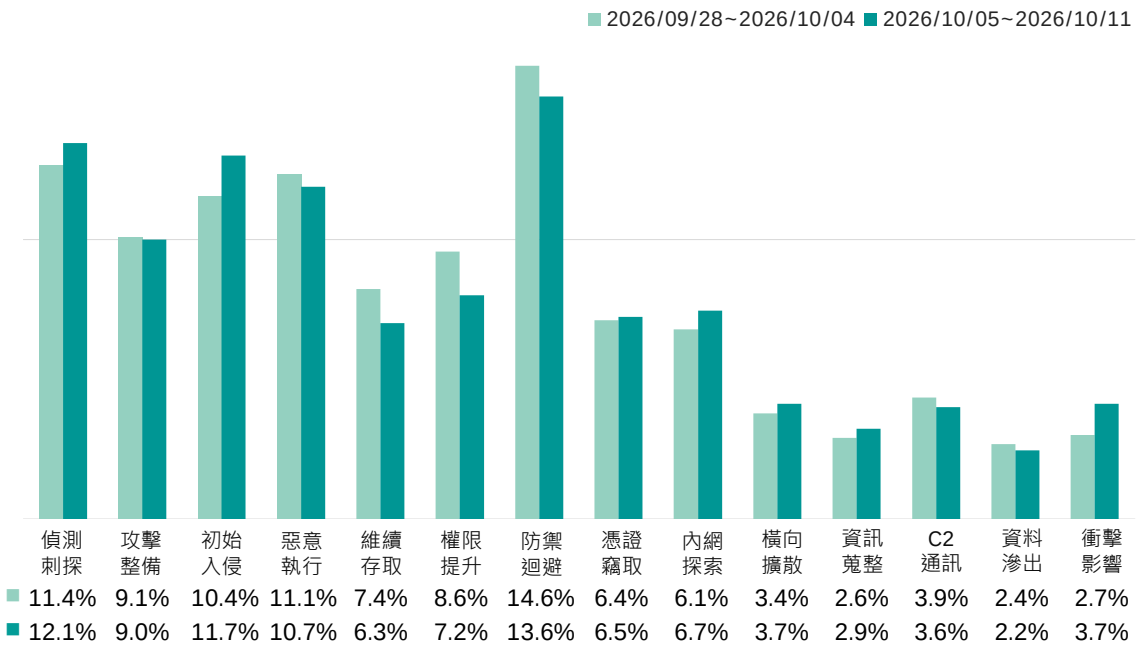


圖2 | 資安聯防監控攻擊階段統計


防護建議
建議機關採取下列防護措施
防禦迴避 (Defense Evasion)
強化端點偵測與防護： 導入 EDR 等端點防護機制，監控異常指令執行及可疑系統工具使用行為
加強日誌稽核與保存： 集中管理系統及指令操作紀錄，偵測日誌遭停用、刪除或竄改等異常行為
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權限，降低攻擊者規避監控的機會
偵測刺探 (Reconnaissance)
強化異常掃描偵測： 監控短時間大量連線、IP 區段掃描及漏洞探測等可疑網路行為
定期盤點與修補弱點： 清查對外暴露資產及開放服務，優先修補高風險漏洞，降低潛在攻擊面
結合威脅情資進行防護： 分析可疑掃描來源 IP，透過防火牆、IPS 等設備適當阻擋惡意掃描流量

■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)成為攻擊熱點

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68.38%、「遠端控制」服務攻擊占比26.66%，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76.14%。「遠端控制」服務亦有19.51%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React伺服器端元件存在遠端程式碼執行漏洞CVE-2025-55182，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。

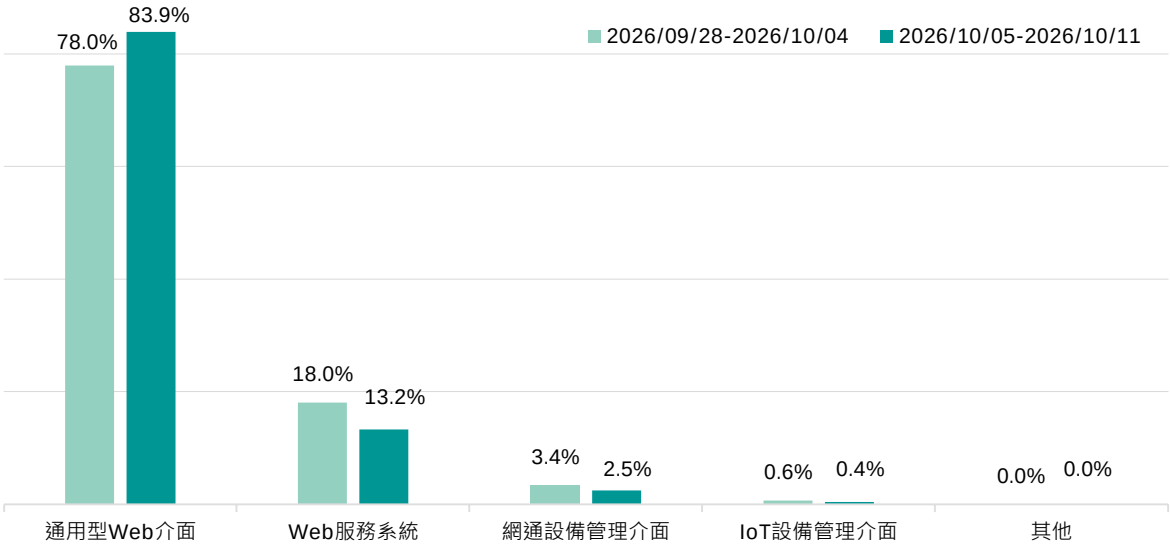


圖3 | 本週網頁應用介面之誘捕攻擊比例統計

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、輸入驗證不當漏洞及SQL注入漏洞，攻擊目標涵蓋威脅情資平台、程式遞送控制器(ADC & Gateway)、企業級端點與安全管理系統及網頁應用程式框架。

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	⬆new	CVE-2026-27960[1]	OpenCTI	9.8	
■	2	⬇1	CVE-2026-3055[2]	NetScaler ADC & Gateway	9.8	✓
■	3	⬆new	CVE-2026-88771[3]	NetScaler ADC & Gateway	9.8	✓
■	4	-	CVE-2026-21643[4]	Fortinet FortiClientEMS	9.8	✓
■	5	⬆new	CVE-2026-1207[5]	Django	8.3	

類型 ■ 權限提升漏洞 ■ 越界讀取漏洞 ■ 輸入驗證不當漏洞 ■ SQL注入漏洞

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-2026-88771
4. https://nvd.nist.gov/vuln/detail/CVE-2026-21643
5. https://nvd.nist.gov/vuln/detail/CVE-2026-1207

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

瀏覽器儲存帳密可能擴大端點遭入侵後的影響

本週總計接獲21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植入惡意程式與異常連線占多數，詳見圖5。使用者為便利登入，常將網站帳號密碼儲存於瀏覽器，部分服務亦會長時間保留登入狀態。當電腦遭惡意程式入侵或瀏覽器設定檔遭竊取時，攻擊者可能進一步取得已儲存之帳密、登入憑證或工作階段資訊，進而嘗試存取電子郵件、雲端服務、社群平台及其他曾登入之系統，使單一端點事件擴大為多個帳號遭接管的風險。

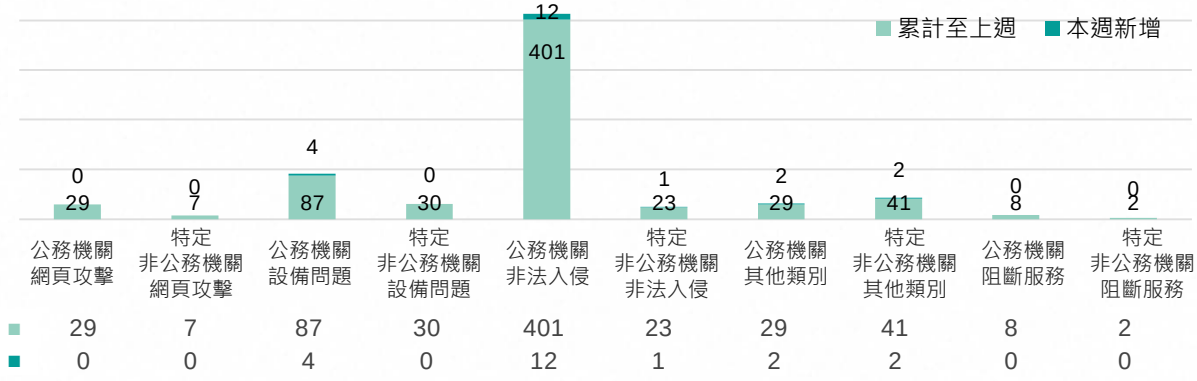


圖4 | 本週公務機關暨特定非公務機關資安事件通報概況

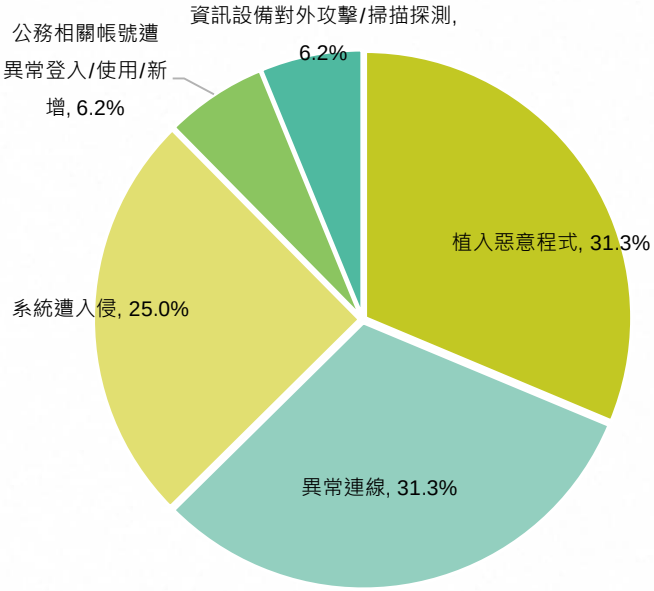


圖5 | 本週公務機關非法入侵事件類型占比

重點說明

建議公務或具管理權限之帳號避免任意儲存於瀏覽器，並優先使用機關核准之密碼管理工具及多因子驗證；如使用者電腦疑似遭入侵，除處理惡意程式及更換主要帳號密碼外，亦應盤點該瀏覽器曾儲存或登入之其他重要帳號，必要時一併更換密碼、撤銷既有登入工作階段及檢查異常登入紀錄。

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
➢ 攻擊者竊取瀏覽器儲存帳密進而接管多個重要系統帳號 ➢ 惡意程式竊取登入憑證與工作階段資訊繞過身分驗證	➢ 禁止公務及特權帳號任意儲存於瀏覽器，改用機關核准之密碼管理工具 ➢ 強化重要帳號多因子驗證與登入控管，降低帳密外洩後遭接管之風險 ➢ 電腦遭入侵時應全面盤點瀏覽器儲存帳號，並更換密碼及撤銷登入憑證 ➢ 強化端點惡意程式偵測及異常登入監控，及早發現帳密竊取與帳號濫用

5間民間企業揭露重大資安訊息

本週5間民間企業發布重大訊息，產業類別為數位雲端業、電腦及週邊設備業、文化創意業、生技醫療業、資訊服務業，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
一零四資訊科技股份有限公司	2026年10月06日	一零四發現APP系統異常讀取情形，經調查確認，約12萬筆履歷資料遭未經授權讀取，已立即採取相關防護及阻斷措施，並結合外部公正第三方資安機構進行鑑識與強化。目前系統與營運正常運作，對公司尚無重大影響，已採取相關防護及阻斷措施，並持續進行資安鑑識及強化資訊安全防護機制。

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
上福全球科技股份有限公司	2026年10月07日	上福代重要子公司Katun Corporation發布重大訊息，Katun Corporation發現部分資訊系統異常存取行為，已立即啟動資安事件應變機制，執行受影響設備隔離、權限管控、系統檢查及相關防護強化措施，並進行鑑識分析、事件監控及影響範圍調查。後續將進一步強化資訊安全管理、遠端存取管控、網路安全防護及員工資訊安全教育訓練，以降低類似事件再次發生之風險。
鈊象電子股份有限公司	2026年10月07日	鈊象公司於115年9月29日發現不明IP異常侵入公司營運資訊設備，造成公司遊戲營運資料外洩，包含部分遊戲之玩家姓名、電話、電子郵件之個資，已於當日偵測發現後，隨即啟動資安緊急應變機制。目前評估對公司營運無重大影響，後續將持續提升資安防禦，強化監控與防護層級，且依事件調查結果檢視並強化相關資訊安全管理及防護措施。
杏一醫療用品股份有限公司	2026年10月07日	杏一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。杏一公司獲悉後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。

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
杏一醫療用品股份有限公司 (續)	2026年10月07日	已立即啟動資安事件應變作業，針對相關系統、存取紀錄及可能涉及之資料範圍進行調查，並要求官網平台委外廠商同步進行資安檢視及必要之強化措施。
緯致科技股份有限公司	2026年10月09日	緯致公司偵測到內部系統有異常存取情形，經調查確認，部分員工資訊與公務聯繫資訊遭未經授權存取，於發現異常後已立即採取網路阻斷、系統隔離及相關防護措施，並委請外部公正第三方資安機構進行數位鑑識與安全強化。對公司整體系統與營運正常運作尚無重大影響，目前已採取相關防護、阻斷及修補措施，並持續強化資訊安全防護機制。

■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

產品服務占比攀升 廣告以日常需求吸引購買

詐騙類型趨勢

金融投資型占比回落至19.8%，仍居第二，詳見圖6。推薦股票的廣告以「別等漲了才追」強調搶先掌握行情，宣稱每天提供值得留意的股票名單、大戶的買賣動向與買賣時機。另有廣告以免費公開股票名單為訴求，要求加入社群並私訊領取。這類廣告以取得最新股市消息、提早找到投資機會為誘因，吸引民眾加入社群或私訊詢問。

身分冒充型占比回升至15.2%。行動電源廣告宣稱推出媽祖聯名款，藉「加持」「守護」等語句連結宗教信任，並聲稱電池防爆、不易發熱。廣告把聯名身分與用電安全訴求結合，塑造值得信賴的形象，再用限量、錯過不再催促點擊購買。

產品服務型占比升至65.0%，為本週最大類型。霧化棒廣告宣稱吸入即可補充維生素，並以零尼古丁與提神等說法，包裝成隨身可用的健康選擇，再用限時優惠引導點擊了解商品。另有旅行用免洗內褲廣告，鎖定出差、出遊的衛生顧慮，以獨立包裝、拆封即穿強調使用便利，搭配多件特價吸引購買，要求留言後再取得專屬購物連結。

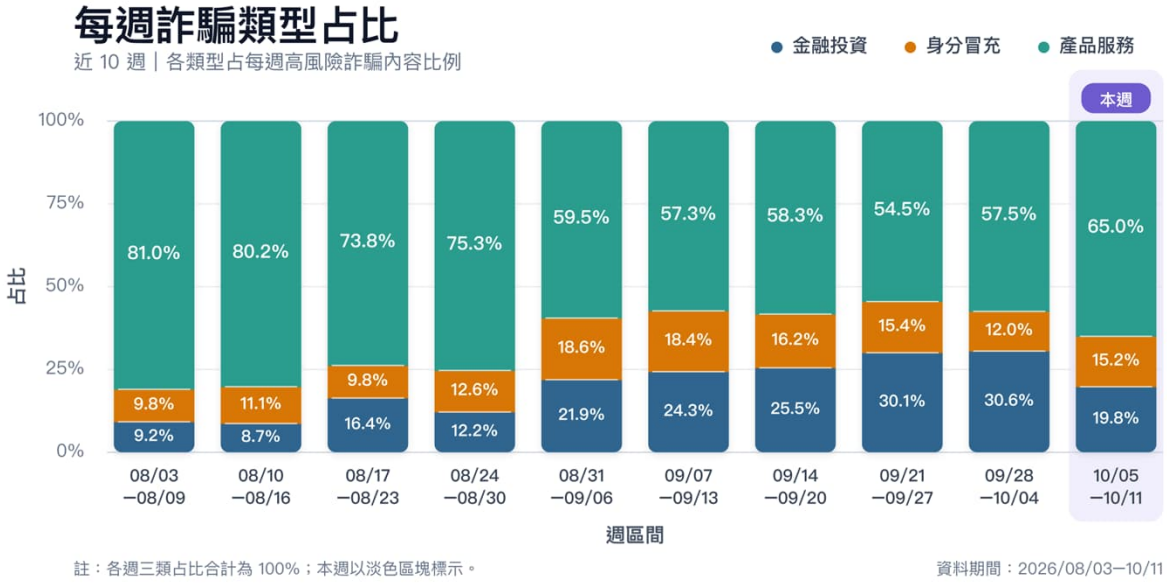


圖6 | 每週詐騙類型占比

關鍵字趨勢

「優惠」本週升至首位，詳見圖7。兩週的廣告案例都以價格優惠吸引注意：前週的防曬商品廣告主打限時低價，本週的遊戲儲值廣告同樣強調折扣，並宣稱每日登入可領取代金券。不過，代金券須搭配儲值才能使用，民眾領券後仍需付費儲值，才能享用優惠。升至本週第 3 名的「免費」，也被用來吸引有貸款需求的民眾諮詢。以房貸廣告為例，廣告宣稱可免費評估貸款方案，並承諾過件前不收費。這些承諾用來減輕民眾對費用的顧慮，吸引他們填寫諮詢表單，了解自己的房屋能貸多少。

「居家」與「小巧」分居第 5、10 名，皆進入本週前 10 名。前者的防水噴劑廣告宣稱一噴止漏、不需專業師傅，後者的迷你縫紉機則列出褲腳修改與衣物縫補等用途，強調新手也能操作。兩者都以簡單操作減輕自行修繕的顧慮，再分別以限時特價、倉庫出清吸引購買。

「投資」維持第 2 名，「市場」退居第 6 名，「股票」升至第 7 名，三者都可見投資教學訴求。以「股票」為例，課程廣告宣稱可運用 AI 建立股票分析助理，吸引想省下研究時間、改善判斷的民眾購課。綜觀本週前 10 名，生活用品以便利與價格吸引購買，投資課程以提升分析能力招攬學習。

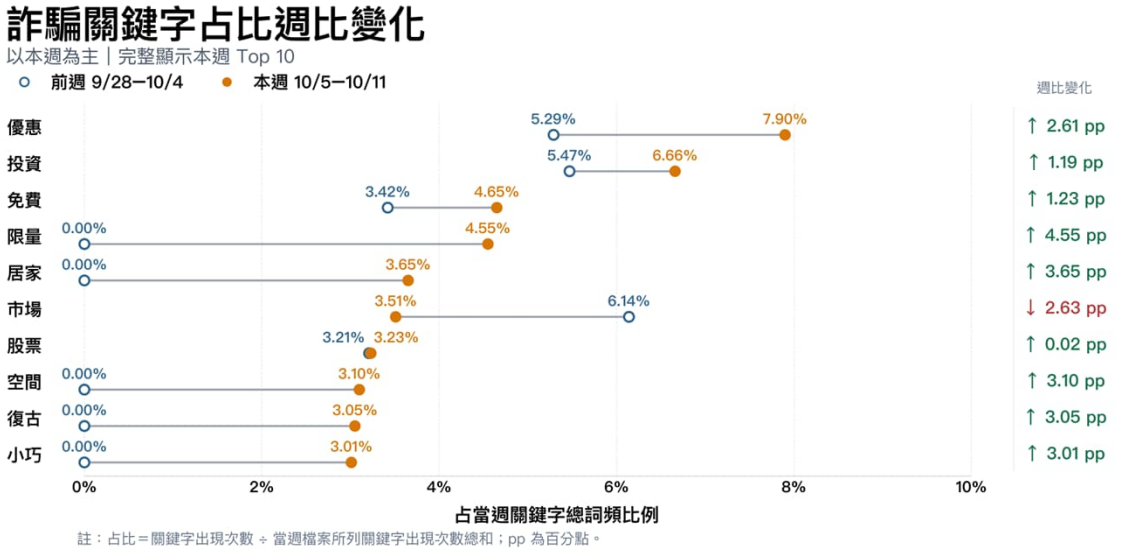


圖7 | 詐騙關鍵字占比週比變化

焦點文章

政府領域資安事件趨勢研析

API安全應兼顧存取授權、業務邏輯與安全設計

隨著政府數位服務普及，應用程式介面(Application Programming Interface, API)已廣泛應用於資料查詢、業務操作及系統介接。近期從AI Agent相關攻擊紀錄觀察到，攻擊者透過探索API端點、調整請求參數及分析系統回應，測試網站既有功能的安全控制。其中，部分缺失並非源自已知軟體漏洞，而是涉及API存取授權、認證憑證保護及業務邏輯設計等問題。

一、API缺乏存取與請求驗證

部分網站透過API提供資料查詢、檔案下載及業務操作等功能，卻未妥善實施存取限制，使外部使用者無須登入，即可直接呼叫原應受保護的API，取得資料或執行系統功能。此外，部分API對請求參數缺乏適當驗證，即使未提供必要欄位、傳入空白值或不符合預期格式的資料，仍可能接受請求或回傳結果。若同時缺乏存取授權檢查，攻擊者便可能透過反覆變更參數，進一步探索系統功能及資料範圍。

二、API已驗證身分，卻未落實資料與功能授權

部分API雖透過JWT等機制驗證使用者身分，卻未進一步確認請求者對指定資料或功能的操作權限。例如，攻擊者使用自己的有效JWT，僅透過修改資料識別參數，即可取得或修改其他使用者的資料，涉及物件層級授權控管不當(Broken Object Level Authorization, BOLA)；若一般使用者可直接呼叫原應限定管理者執行的功能，則可能涉及功能層級授權控管不當(Broken Function Level Authorization, BFLA)。

三、API Key使用與保管不當衍生安全風險

API Key常用於識別服務呼叫來源、管理使用量或進行系統間認證。部分網站將API Key配置於前端程式，供瀏覽器呼叫服務，此類設計不一定構成漏洞，仍須視金鑰用途及權限範圍判斷。然而，若將前端可取得的金鑰作為保護敏感資料的唯一憑證，便可能遭外部使用者取得並重複利用。另有案例顯示，部分API直接回傳原應保密的API Key，使攻擊者可能取得相關憑證後，循正常認證程序取得有效Token，進一步存取受保護的API。

綜合上述觀察，API安全風險不僅涉及技術性漏洞，亦與系統存取授權、認證憑證管理及業務

焦點文章

邏輯設計密切相關。由於部分缺失須依據資料公開範圍、使用者角色及實際業務需求判斷，傳統弱點掃描難以全面辨識跨帳號資料存取、角色越權及業務流程等問題。建議機關除持續落實弱點掃描與修補外，亦應將API存取控制、授權規則及憑證保護納入安全軟體開發生命週期(SSDLC)，並結合情境式滲透測試，驗證不同使用者身分及操作條件下的安全控制是否符合預期，以降低既有功能遭未經授權利用之風險。

關鍵字：API安全、存取授權、業務邏輯安全

刊　　名　資安週報第 66 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。