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
風險維持平穩、部分設定改善 元件高風險漏洞仍待強化

重大漏洞
GitLab與Dell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)仍為攻擊熱點

事件通報
防範水坑式攻擊，應強化端點弱點管理及惡意行為偵測 降低網站遭利用後的影響

網路巡查高風險詐騙
產品服務型占比續升 金融投資型降至末位

焦點文章
從職能出發 勾勒資安人才學習路徑

2026.10.22
067

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

風險維持平穩、部分設定改善 元件高風險漏洞仍待強化

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8,159項。其中，「元件高風險漏洞」以3,295項居首，「過時或弱加密協定」1,461項次之，「TLS憑證不受信任」則以1,044項超過「CSP設定不當」999項，位居第三。前三項合計5,800項，占前10大風險項目總數約71.1%，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8,138項，本期整體風險數量增加21項，增幅約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3,282項增至本期3,295項，增幅約0.4%。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1,447項增至1,461項，增幅約1.0%；「TLS憑證不受信任」由1,045項減至1,044項，降幅約0.1%。另「未部署WAF」由853項增至906項，增幅約6.2%；「CSP設定不當」由1,087項減至999項，降幅約8.1%。

整體變化幅度不大。其中，「元件高風險漏洞」及「過時或弱加密協定」略有增加，「TLS憑證不受信任」則大致持平；「CSP設定不當」明顯減少，顯示部分網站安全設定已有改善，惟「未部署WAF」項目增加，反映網站防護機制仍有強化空間。建議持續推動高風險元件修補，並完善WAF部署及CSP安全設定，以降低外部曝險風險。

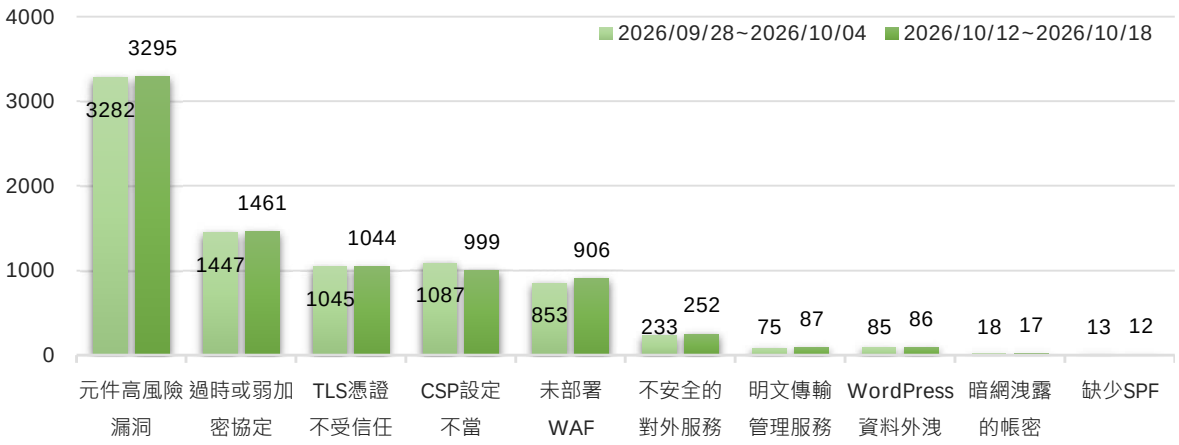


圖1 | EASM檢測結果統計(前10大風險)

防護建議

建議受測單位採取下列防護措施	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

GitLab與Dell高風險漏洞應盡速修補

- GitLab AI Gateway存在沙箱逃逸(Sandbox Escape)漏洞(CVE-2026-90970)[1]，具Duo Agent Platform流程組態與範本設定權限且已通過身分鑑別之遠端攻擊者，可透過提交特製之提示範本逃脫提示範本沙箱限制，進而於AI Gateway上執行任意指令
- Dell System Update存在路徑遍歷(Path Traversal)漏洞(CVE-2026-86360)[2]，未經身分鑑別之遠端攻擊者可利用此漏洞存取檔案系統，進而以root權限執行任意程式碼

[1] https://docs.gitlab.com/releases/patches/other-patches/patch-release-gitlab-ai-gateway-19-4-1-released/
[2] https://www.dell.com/support/kbdoc/en-us/000515843/dsa-2026-324-security-update-for-dell-system-update-dsu-vulnerabilities

■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14.8%，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11.4%，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偵查與資訊蒐集活動，以提升後續攻擊行動的成功率。觀察到的主要手法包括主動式掃描、憑證資訊蒐集、以及IP 區段掃描。攻擊者透過自動化工具對外部網段與公開服務進行大規模探測，蒐集系統架構、開放埠與服務資訊，同時搜尋與帳號憑證相關的公開資料或外洩資訊，作為後續登入嘗試與目標鎖定的依據。部分活動呈現由廣泛掃描逐步聚焦特定系統與帳號的特徵，顯示其偵查行為具備明確的攻擊目標與規劃。此類行為雖多屬攻擊前期準備階段，但其蒐集成果往往成為後續入侵與橫向移動的重要基礎。建議組織加強監控異常掃描流量與帳號探測行為，定期盤點對外暴露資產，並結合威脅情資分析可疑來源，以提前發現潛在攻擊準備活動並採取防禦措施。

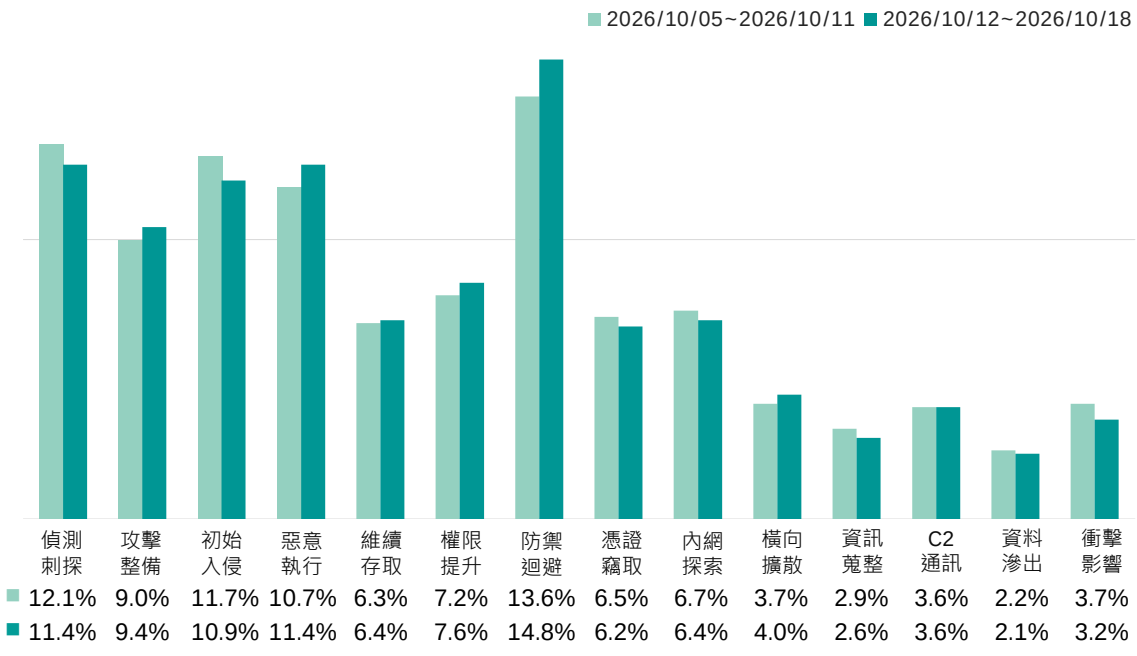


圖2 | 資安聯防監控攻擊階段統計

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： 部署 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： 集中收容系統與指令操作日誌，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使用權限，降低攻擊者規避偵測的機會

偵測刺探 (Reconnaissance)

- 強化異常掃描監控： 監控短時間大量連線、IP 區段掃描及異常服務探測行為，及早識別可疑來源
- 定期盤點對外暴露資產： 檢視公開服務、開放埠及系統弱點，降低遭攻擊者探測與利用的風險
- 加強帳號憑證安全： 定期檢查帳號憑證外洩情形，落實多因素驗證（MFA）及異常登入監控
- 結合威脅情資分析： 比對可疑來源 IP 與已知惡意情資，適時採取封鎖或流量限制措施

■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76.14%、「遠端控制」服務攻擊占比19.51%，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74.55%。「遠端控制」服務亦有20.20% 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WordPress WP01外掛套件存在路徑遍歷漏洞之CVE-2025-30567，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。

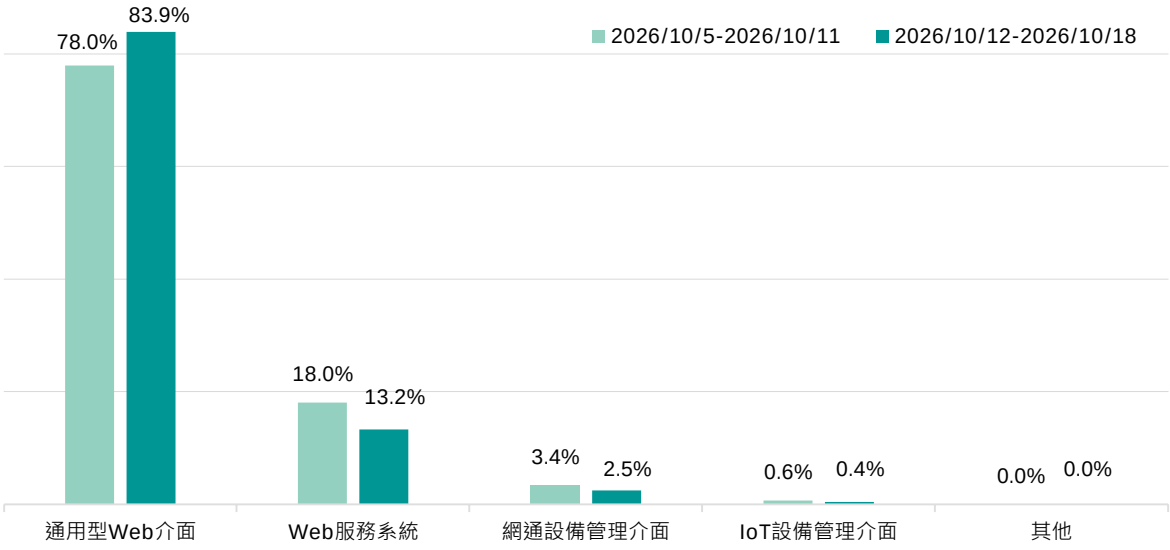


圖3 | 本週網頁應用介面之誘捕攻擊比例統計

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、身分驗證繞過漏洞及指令注入漏洞，攻擊目標涵蓋威脅情資平台、程式遞送控制器(ADC & Gateway)、網站主機伺服器管理系統及大模型API統一介面與代理伺服器工具。

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	-	CVE-2026-88771[3]	NetScaler ADC & Gateway	9.8	✓
■	4	⬆new	CVE-2026-41940[4]	cPanel & WHM	9.8	✓
■	5	⬆new	CVE-2026-42271[5]	LiteLLM	8.8	✓

類型 ■ 權限提升漏洞 ■ 越界讀取漏洞 ■ 輸入驗證不當漏洞 ■ 身分驗證繞過漏洞 ■ 指令注入漏洞

1. https://nvd.nist.gov/vuln/detail/CVE-2026-27960
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-2026-41940
5. https://nvd.nist.gov/vuln/detail/CVE-2026-42271

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

防範水坑式攻擊，應強化端點弱點管理及惡意行為偵測 降低網站遭利用後的影響

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異常連線占多數，詳見圖5。本週發現水坑攻擊事件，攻擊者先入侵特定網站並植入惡意JavaScript程式碼，當使用者正常瀏覽該網站時，惡意程式碼即隨網頁載入，進一步嘗試利用使用者端軟體或元件弱點下載惡意程式。此類攻擊不同於傳統釣魚郵件，使用者可能僅是瀏覽平時正常使用的網站，即接觸到攻擊內容。

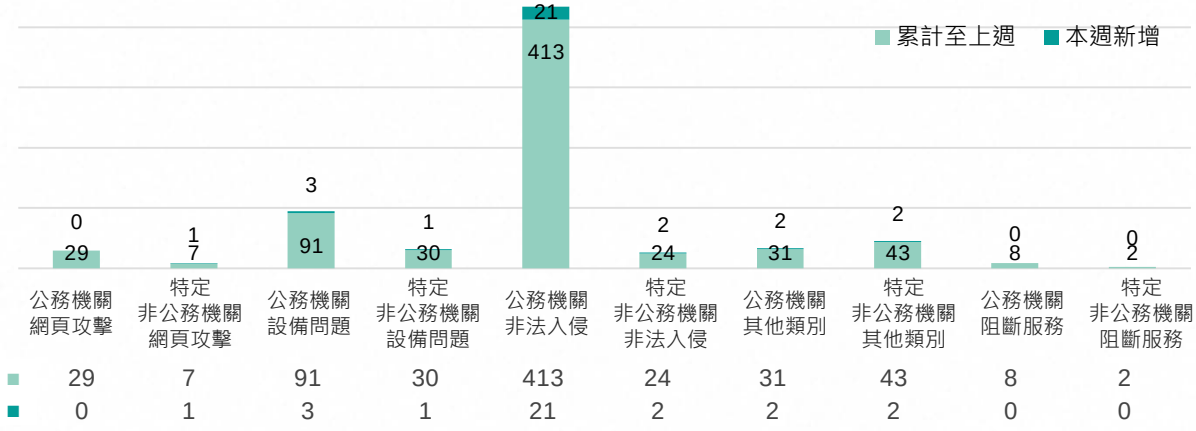


圖4 | 本週公務機關暨特定非公務機關資安事件通報概況

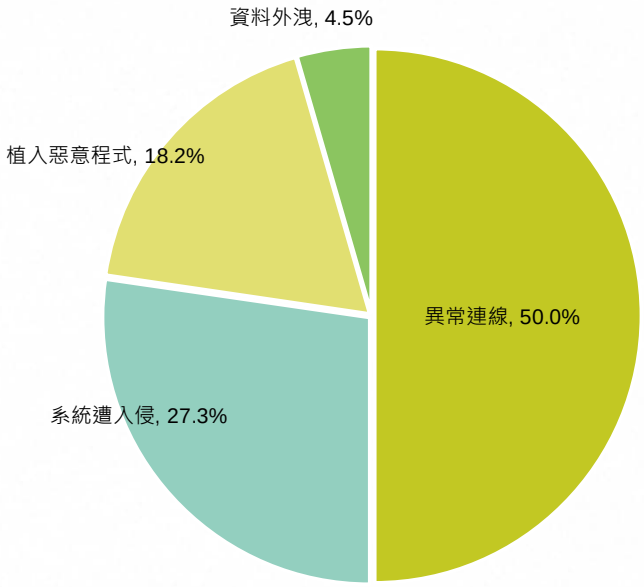


圖5 | 本週公務機關非法入侵事件類型占比

重點說明

水坑式攻擊通常鎖定特定族群經常造訪的網站，先控制網站後再等待目標使用者上門，因此僅依網站是否熟悉或過往是否正常，並不足以判斷當下內容是否安全。建議機關持續更新瀏覽器、作業系統及使用者端相關軟體與元件，降低惡意網頁利用已知弱點之機會；端點亦應啟用惡意程式防護及行為偵測，對瀏覽網站後異常產生的程式下載、腳本執行或外部連線進行偵測與阻擋。

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
➢ 攻擊者入侵常用網站植入惡意腳本誘使訪客遭感染 ➢ 惡意網頁利用端點軟體弱點下載程式並控制受害主機	➢ 定期更新瀏覽器、作業系統及相關元件，降低惡意網頁利用已知弱點之風險 ➢ 強化端點偵測與回應機制，即時阻擋惡意腳本執行及異常程式下載行為 ➢ 建立網站存取與異常連線監控機制，及早發現遭植入惡意程式之網站 ➢ 限制非授權程式執行及使用者權限，降低惡意程式感染後之影響範圍

1間民間企業揭露重大資安訊息

本週1家民間企業發布重大訊息，產業類別為數位雲端業，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
91APP, Inc.	2026年10月16日	91APP公司查知Commerce Cloud 資料庫受到自動化攻擊，並對部分資訊非法擷取，目前已獲得控制，並已向警方報案。本公司已依個資事故通報及處理流程啟動應變會議，委請第三方資安公正單位協助調查，並採取必要防護措施降低影響。後續為防範個資遭詐騙集團利用，已透過電子郵件等相關管道進行反詐騙宣導。

■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

產品服務型占比續升 金融投資型降至末位

詐騙類型趨勢

產品服務型占比升高，約占本週四分之三，詳見圖6。保健品廣告以不必刻意節食的訴求吸引有體重管理需求者，宣稱餐前服用即可阻隔糖分吸收，並提供60天試用與無效退費承諾。另有主打血管保健的產品宣稱能溶解血栓，同樣以不滿意退款促購，把健康改善的期待與售後保障結合，降低民眾嘗試購買的顧慮。

身分冒充型占比略降，但成為本週第二大類型。穴位保健廣告聲稱獲醫師認可，並宣稱能緩解身體不適，藉專業名義吸引有腰酸、頭痛困擾的民眾，再以圖解與口訣強調容易學習。按摩腰帶廣告則以藝人推薦增加可信度，主打居家使用的便利性，搭配國慶限時贈禮與現貨快速出貨的說法，引導點擊購買。

本週金融投資型占比回落，在三類中最低。海外房產講座廣告主打永久產權、交通便利及免費購屋指南，以名額有限催促報名，註冊後再由房產顧問聯繫。另有 AI 股票分析課程，宣稱能協助整理股價走勢與技術指標，搭配限時折扣，吸引希望節省研究時間、掌握投資判斷依據的民眾購課。

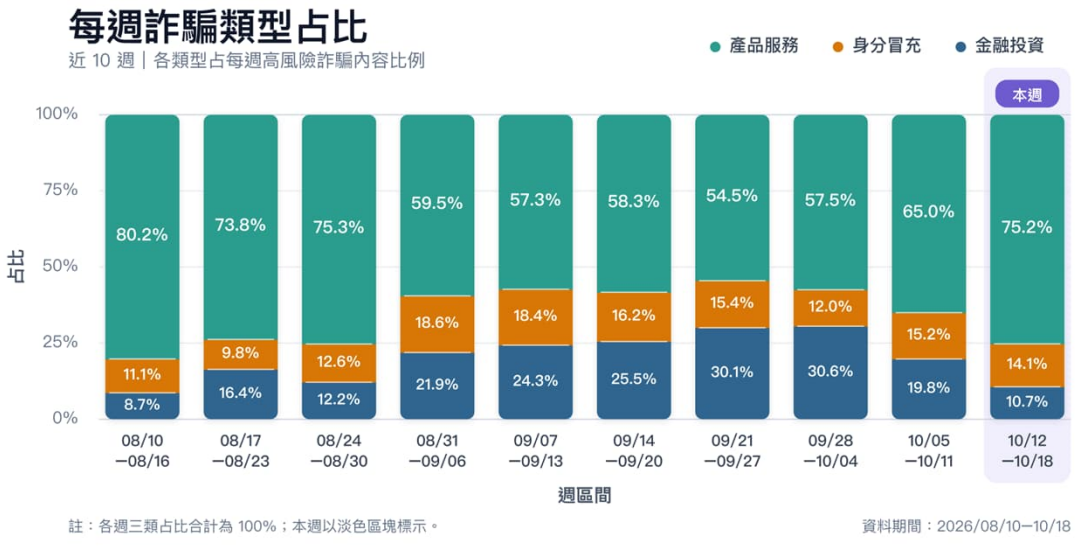


圖6 | 每週詐騙類型占比

關鍵字趨勢

「優惠」仍居首位，防曬美妝廣告宣稱一瓶兼具防曬、潤色與妝前打底功能，再以每瓶最低 216 元的限時價格促購。「限量」升至第2名，護膚霜廣告針對熟齡保養需求，宣稱能改善暗沉、滋潤肌膚，搭配週年慶組合只剩最後10組的說法，要求有意購買者留言，並以額滿截團催促回應，詳見圖7。

「DIY」「出清」與「縫補」進入本週前10名，分居第 7、8、9名，共同呈現縫紉用品的促購主題。相關廣告以補衣服、改褲長等日常需求切入，主打桌上型不占空間、新手易上手；出清廣告再以「真的要離開了」與「倉庫限量出清」的說法營造錯過難再買的急迫感，搭配下單贈禮催促購買。

「投資」退居第6名，前週相關廣告介紹選股與存股課程，本週則出現補財庫服務，以信眾回饋宣傳改善財運，邀請財運不佳、事業遇到瓶頸的民眾預約免費諮詢。從本週前十大關鍵字來看，商品促購以日常保養與家用需求為主，常見手法是限時限量催促回應，以及用操作簡單、方便收納吸引購買。

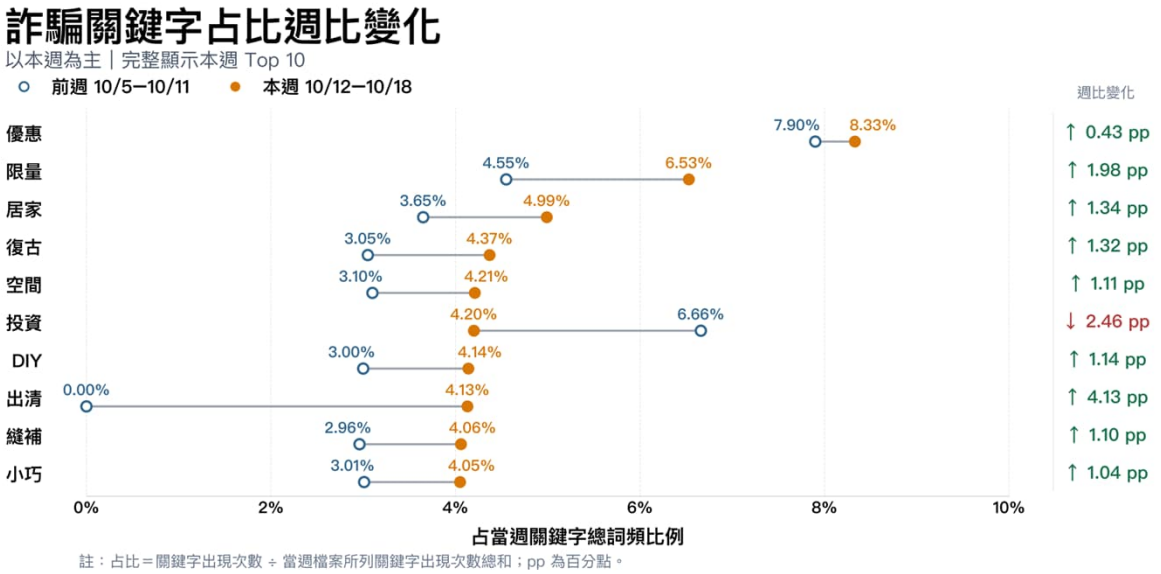


圖7 | 詐騙關鍵字占比週比變化

焦點文章

從職能出發 勾勒資安人才學習路徑

從工作需求到學習方向，讓每一步成長都有跡可循

數位科技快速發展，資安要學的東西也越來越多。對於想投入資安領域的人，可能很快就會遇到一個問題：「課程這麼多，我應該從哪裡開始呢？」或是已經在資安領域工作一段時間的人來說，也可能會出現另一種困惑：「課上了、證照也考了，但如果想往其他方向發展，下一步該補強什麼呢？」

這些問題背後，其實都指向同一件事情——人才培育不只是開設更多課程，而是要先回到「這份工作需要具備什麼能力」來思考，這也是資安院近年推動資安人才培育時，逐步將「課程導向」走向「職能導向」的原因。

先了解工作需要什麼能力，再決定該學什麼

資安的工作範圍很廣，有人負責治理與風險管理，有人專注事件應變、數位鑑識，也有人每天和弱點、威脅情資打交道，雖然大家都叫「資安人才」，但每天面對的工作任務卻不盡相同。

因此，資安院持續從「職能」角度思考人才培育，研析不同資安角色實際執行的工作任務，以及完成這些任務所需要的知識與技能，再回頭思考應該安排哪些課程與學習資源。今年資安院持續推動職能框架研析，預計完成12類資安人才職能框架，並針對「滲透測試工程師」、「數位鑑識調查分析師」及「資安威脅情資分析師」等專業人才發展教材。

換句話說，人才培育不是先決定「要開什麼課程」，而是先思考「不同的資安工作，需要學會什麼？」透過研析各類資安人才的職能需求，再將所需的知識與技能轉化成具體的學習內容，讓教材不只是知識的集合，也能與實際工作建立更清楚的連結。

串聯公私領域職能需求，讓培訓更貼近實務

不同領域的資安人才，所需的專業能力各有側重，例如，政府部門著重於法規遵循、風險管控及系統安全等防護工作，而產業領域則因應不同產業特性與營運需求，更加重視資安技術實務、威脅偵測與分析及營運持續等能力。雖然兩者的工作環境與任務有所不同，但都需要具備相應的專業知識與技能。

焦點文章

為了讓學習路徑更清楚，也能適用於不同領域，資安院以資安人才職能框架作為基礎，結合政府機關資安專職人員的資安職能訓練發展藍圖，思考哪些內容可透過公部門訓練強化，哪些專業技術可善用既有的市場培訓資源，逐步建立不同領域的人才角色、工作任務、所需職能與訓練課程之間的關係。

透過這樣的整合，未來無論是剛投入資安領域，或是希望朝不同專業方向發展的學習者，都能依據工作角色與能力需求，找到適合自己的學習資源與精進方向，讓有限的學習時間，真正花在工作需要訓練的地方。

從學習走向能力，讓人才成長更有方向

資安人才培育很像規劃一趟旅程，職能框架就像標示目的地所需要具備的能力，學習路徑協助規劃前進的方向，課程與教材則提供沿途所需的知識與技能。未來，若能進一步結合能力鑑測，就像在旅途中設置檢查點，協助學員了解自己目前走到哪裡，還有哪些能力需持續精進。

為了讓人才培育不只停留在「學過什麼」，更能進一步了解「具備什麼能力」，資安院也將持續研議資安人才能力鑑測機制，思考如何以職能框架為基礎，建立相應的能力鑑測方式，逐步串聯職能需求、學習資源到能力鑑測，建立更完整的連結，讓每一步學習都更有目標，也更貼近實際工作需求。

資安人才的成長，不會因為修完一門課、取得一張證書就畫下句點。真正重要的是，讓每個人都能清楚自己為什麼而學、下一步可以往哪裡走。無論是剛踏入資安領域的學生、希望精進專業的在職人員，或是正在規劃人才發展的組織，都能透過職能的指引與學習資源，找到適合自己的成長方向。

畢竟，資安要學的東西這麼多，至少在「下一步該學什麼」這件事上，希望讓大家少一點摸索，多一點方向。

焦點文章



關鍵字：資安人才培育、資安職能框架、資安學習路徑

刊　　名　資安週報第 67 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。