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
整體風險小幅下降 個別風險項目呈現兩極化

重大漏洞
Go、GitLab及Oracle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
本週逾四成事件涉及PolarEdge 應優先強化聯網設備弱點修補與異常連線監控

網路巡查高風險詐騙
產品服務占比回升 促銷話術貼近日常需求

焦點文章
十月資安重點：PHP 重大漏洞與第三方供應鏈外洩事件

2026.11.05
069

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

整體風險小幅下降 個別風險項目呈現兩極化

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8,070項。其中，「元件高風險漏洞」以3,128項居首，「過時或弱加密協定」1,530項次之，「TLS憑證不受信任」1,257項位居第三。前三項合計5,915項，占前10大風險項目總數約73.3%，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8,159項，本期整體風險數量減少89項，降幅約1.1%，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3,295項減至本期3,128項，降幅約5.1%。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。「過時或弱加密協定」由1,461項增至1,530項，增幅約4.7%；「TLS憑證不受信任」由1,044項增至1,257項，增幅約20.4%。另「未部署WAF」由906項減至746項，降幅約17.7%；「CSP設定不當」由999項增至1,012項，增幅約1.3%。

整體而言，本期外部曝險風險呈現兩極化，雖然「元件高風險漏洞」及「未部署WAF」數量明顯減少，帶動整體風險下降，但「TLS憑證不受信任」及「過時或弱加密協定」等項目仍持續增加，顯示各類風險改善情形不一，整體資安防護仍有強化空間。另本期發現PHP漏洞，具高度資安威脅，建議各機關優先盤點受影響之PHP版本，儘速完成漏洞修補及版本更新，並持續強化加密協定、憑證管理與網站安全防護措施，以降低外部曝險及潛在入侵風險。

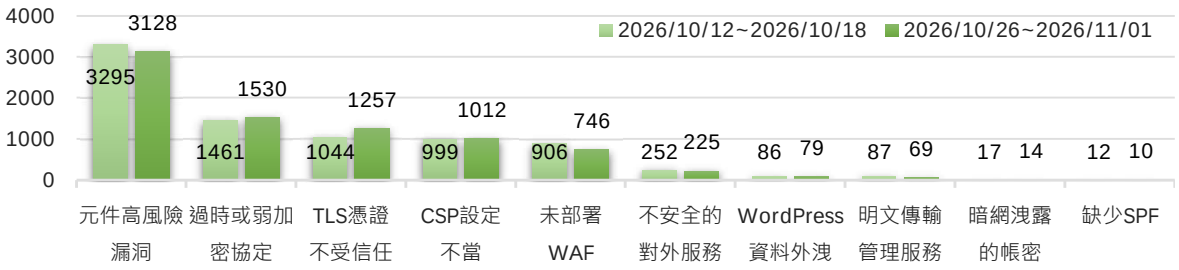


圖1 | EASM檢測結果統計(前10大風險)

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

Go、GitLab及Oracle高風險漏洞應盡速修補

- Go之crypto/x509套件存在不當憑證驗證(Improper Certificate Validation)漏洞(CVE-2026-111943)[1]，因部分情況下系統信任憑證儲存區可能未即時更新，Certificate.Verify函式可能接受含已撤銷或不受信任之中繼憑證授權中心(Intermediate CA)簽發之憑證鏈，攻擊者可藉此進行中間人攻擊。
- GitLab社群版(CE)與企業版(EE)存在2項整數溢位(Integer Overflow)漏洞(CVE-2026-97229與CVE-2026-110264)[2][3]。
  - CVE-2026-97229：前者於特定條件下，未經身分鑑別之遠端攻擊者可藉由於CI/CD組態中使用特製之正規表示式，進而於GitLab伺服器執行任意程式碼。
  - CVE-2026-110264：後者因編譯特製之正規表示式時發生整數溢位，於特定條件下，未經身分鑑別之遠端攻擊者可於GitLab伺服器執行任意程式碼。
- Oracle Java SE、Oracle GraalVM for JDK及Oracle GraalVM Enterprise Edition之JSSE元件存在高風險安全漏洞(CVE-2026-91403)[4]，未經身分鑑別之遠端攻擊者可透過多種通訊協定進行攻擊，進而未經授權存取、新增、刪除或修改重要資料。

[1] https://groups.google.com/g/golang-announce/c/66pojueaQek
[2] https://docs.gitlab.com/releases/patches/patch-release-gitlab-19-4-2-released/
[3] https://docs.gitlab.com/releases/patches/patch-release-gitlab-19-5-1-released/
[4] https://www.oracle.com/security-alerts/alert-cve-2026-91403.html

■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16.2%，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13.8%，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，並為後續權限提升、維持存取及橫向擴散等攻擊活動奠定基礎。

建議機關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。

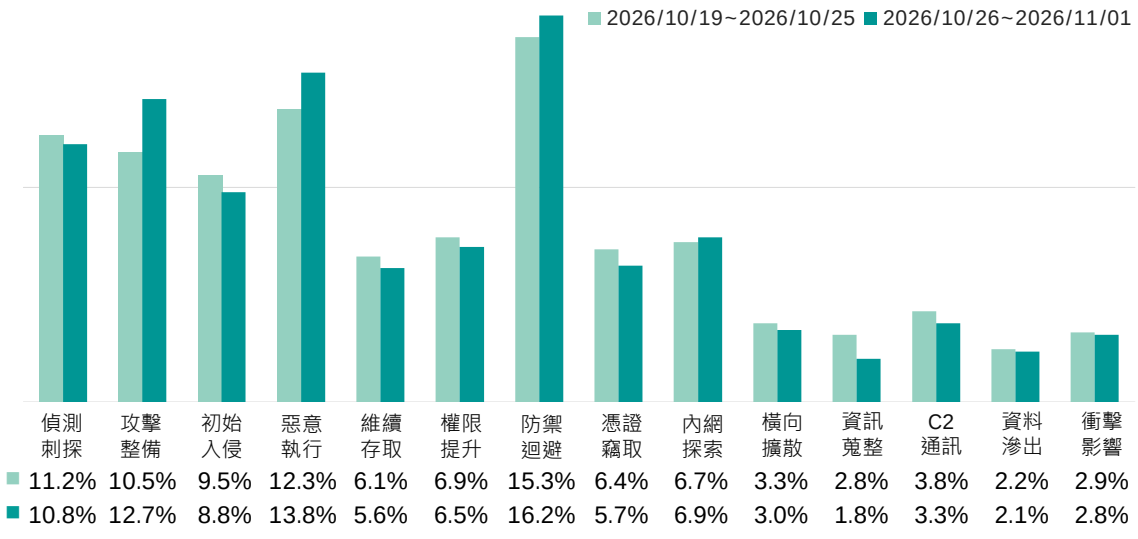
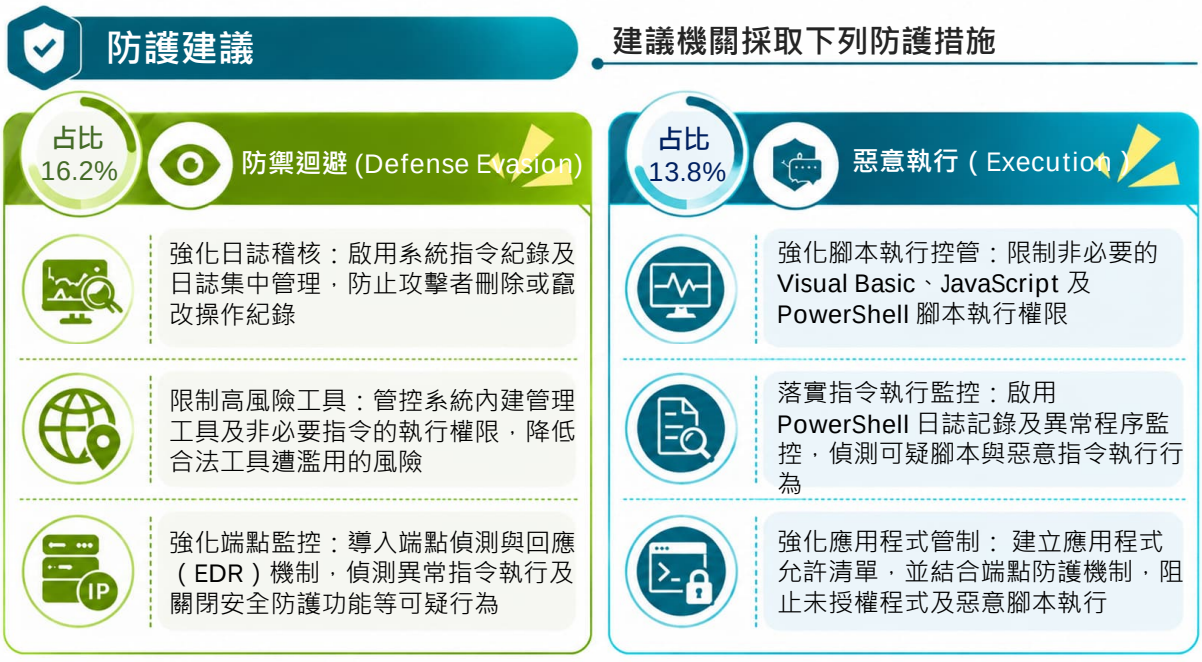


圖2 | 資安聯防監控攻擊階段統計


防護建議
建議機關採取下列防護措施
占比 16.2%
防禦迴避 (Defense Evasion)
強化日誌稽核：啟用系統指令紀錄及日誌集中管理，防止攻擊者刪除或竄改操作紀錄
限制高風險工具：管控系統內建管理工具及非必要指令的執行權限，降低合法工具遭濫用的風險
強化端點監控：導入端點偵測與回應（EDR）機制，偵測異常指令執行及關閉安全防護功能等可疑行為
IP
占比 13.8%
惡意執行（Execution）
強化腳本執行控管：限制非必要的 Visual Basic、JavaScript 及 PowerShell 腳本執行權限
落實指令執行監控：啟用 PowerShell 日誌記錄及異常程序監控，偵測可疑腳本與惡意指令執行行為
強化應用程式管制： 建立應用程式允許清單，並結合端點防護機制，阻止未授權程式及惡意腳本執行

■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65.93%、「遠端控制」服務攻擊占比30.09%，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66.39%。「遠端控制」服務亦有28.12% 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Apache ActiveMQ 的 Fileserver Web存在輸入驗證不當漏洞之CVE-2016-3088，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。

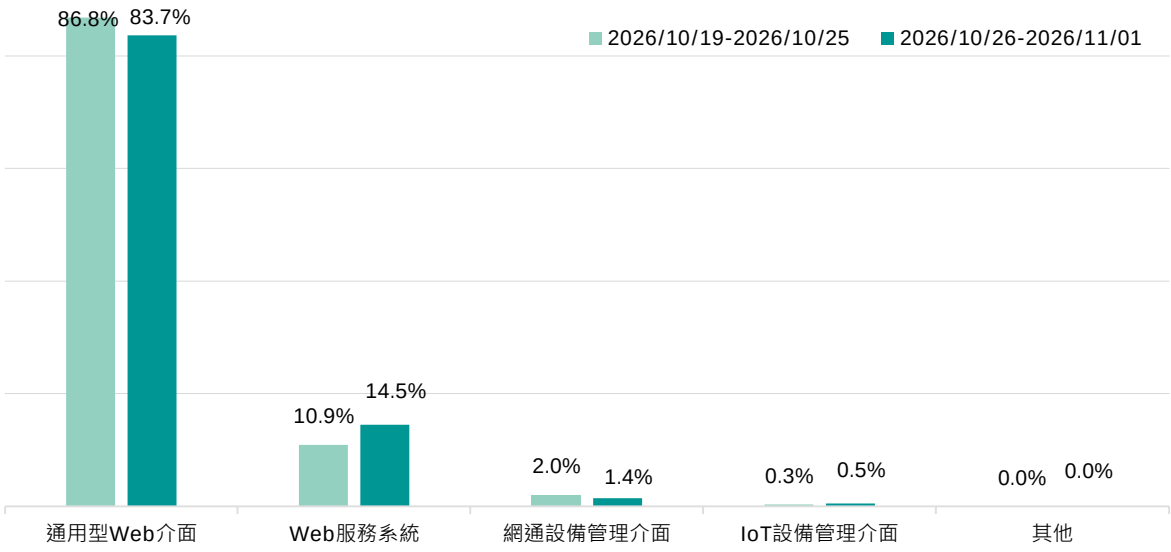


圖3 | 本週網頁應用介面之誘捕攻擊比例統計

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、身分驗證繞過漏洞、輸入驗證不當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	↑1	CVE-2026-3055[1]	NetScaler ADC & Gateway	9.8	✓
■	2	↓1	CVE-2026-27960[2]	OpenCTI	9.8	
■	3	↑2	CVE-2026-41940[3]	cPanel & WHM	9.8	✓
■	4	↑new	CVE-2026-88771[4]	NetScaler ADC & Gateway	9.8	✓
■	5	↑new	CVE-2026-10520[5]	Ivanti Sentry	10	

類型 ■ 越界讀取漏洞 ■ 權限提升漏洞 ■ 身分驗證繞過漏洞
■ 輸入驗證不當漏洞 ■ 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-2026-41940
4. https://nvd.nist.gov/vuln/detail/CVE-2026-88771
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

本週逾四成事件涉及PolarEdge 應優先強化聯網設備弱點修補與異常連線監控

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。本週發現多個機關連線至PolarEdge殭屍網路相關之主機，占本週總通報件數43%。初步清查連線設備疑似為分享器與監視器等聯網設備，攻擊者若利用設備漏洞或管理介面取得控制權，可能進一步下載並執行惡意程式，使設備在原有功能仍可正常運作的情況下，進一步成為外部攻擊流量的中繼或殭屍網路節點。

PolarEdge主要鎖定路由器、儲存設備及其他網路邊緣或IoT設備，建議機關優先清查分享器、監視器及其他對外連網設備，掌握設備型號、韌體版本及原廠安全更新狀態，並檢視是否存在異常對外連線、可疑檔案下載或程式執行行為；對已出現相關跡象之設備，應進一步確認是否遭入侵，必要時更新或重刷韌體、更換管理帳密，並同步清查同型號或同網段設備。

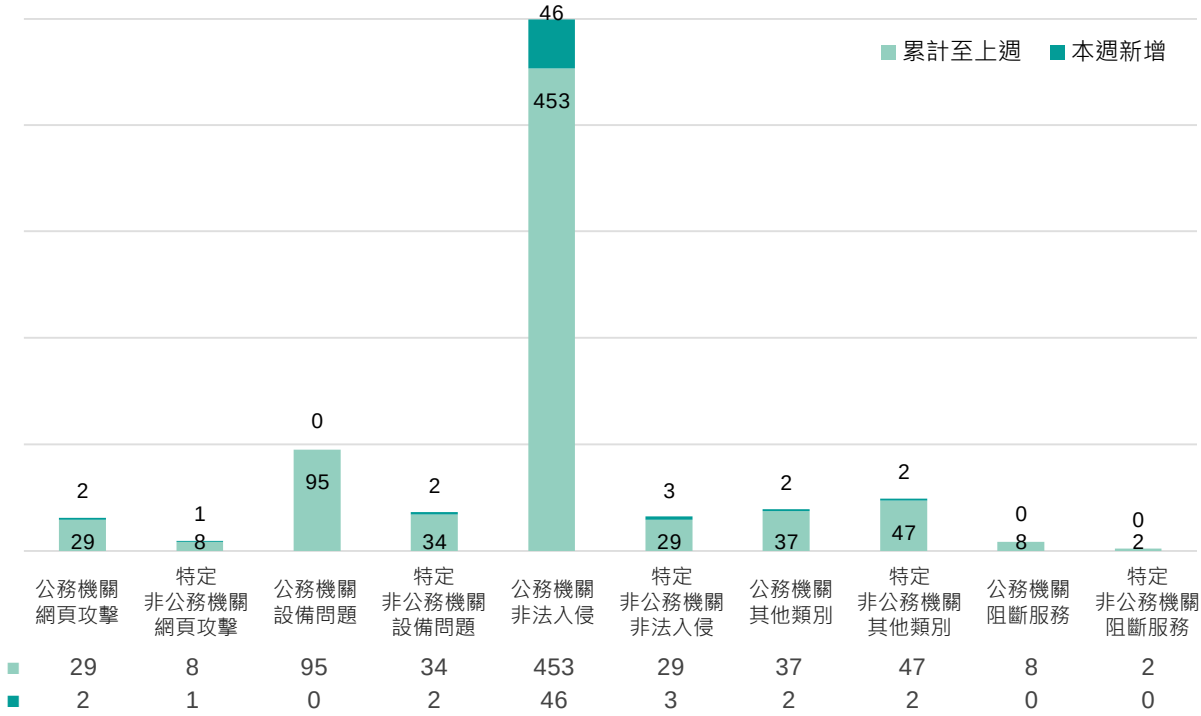


圖4 | 本週公務機關暨特定非公務機關資安事件通報概況

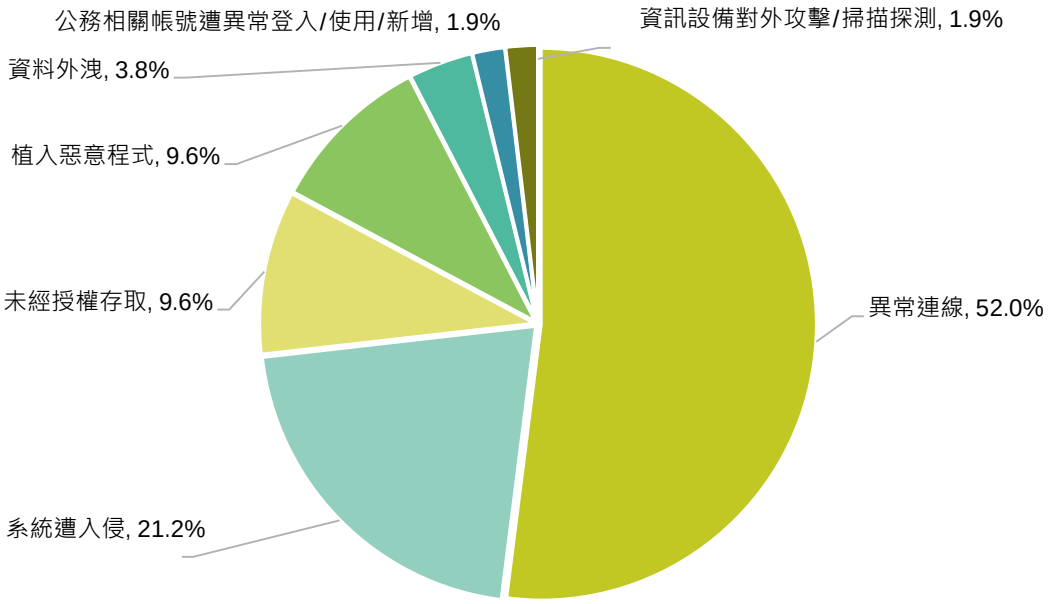


圖5 | 本週公務機關非法入侵事件類型占比

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
➢ 攻擊者利用聯網設備漏洞植入惡意程式並取得控制權 ➢ 遭入侵設備成為殭屍網路節點協助發動外部網路攻擊	➢ 全面盤點分享器、監視器及聯網設備，掌握型號、韌體版本與弱點狀態 ➢ 定期更新設備韌體並修補已知漏洞，限制管理介面對外存取及連線來源 ➢ 強化設備異常連線與惡意程式監控，及早發現殭屍網路通訊及可疑行為 ➢ 針對疑似受駭設備進行隔離與調查，更新韌體、變更帳密並清查同型設備

8間民間企業揭露重大資安訊息

本週8間民間企業發布重大訊息，產業類分別為生技醫療業、居家生活業、其他電子業、文化創意業、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
高林實業股份有限公司	2026年10月27日	高林公司官方購物網站之訂單系統由91APP提供之服務，其資料庫遭自動化攻擊，部分資料遭非法擷取。經確認部分會員之訂單相關資料可能受影響，並持續確認中，本事件對公司營運及財務尚無重大影響。目前已啟動資安應變機制與備援作業，並持續與91APP確認受影響資料範圍，亦透過官網、社群及會員通知提醒消費者防範詐騙，後續將持續強化供應商資安管理與監控機制。
天良生物科技企業股份有限公司	2026年10月27日	天良公司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，並要求其釐清公司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，並已於公司官網加強反詐騙宣導。
京站實業股份有限公司	2026年10月27日	京站數位廣場股份有限公司接獲消費者反映收到冒用本公司名義之詐騙郵件，經確認委外廠商91APP管理之Qonline購物平台疑似遭第三方不當取得資料，已進行相關調查、檢視及必要之修補改善，並透過電子郵件聯繫消費者。

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
橙的電子股份有限公司	2026年10月28日	橙的公司部份區域網路儲存設備遭受勒索病毒攻擊，資安團隊於第一時間立即啟動防禦機制與斷網隔離措施，並啟動相關資安應變機制。初步評估對公司整體營運不致有重大影響，後續將持續加強資訊安全防護機制，提升網路與資訊基礎架構之安全管理，並導入更完善之資安管控措施，以確保資訊系統之安全。
全家便利商店股份有限公司	2026年10月29日	全家公司接獲委外服務廠商91APP通知，其資料庫遭受自動化攻擊，導致線上平台「行動購」部分會員資料遭非法擷取。已立即依個資事故通報及處理流程啟動應變機制，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，為防範會員個資遭不當利用，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。
康那香企業股份有限公司	2026年10月30日	康那香公司接獲委外服務廠商91APP通知，其資料庫遭受自動化攻擊，部分資料遭未經授權存取，該資料庫包含電子商城訂單資料，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。已立即依個資事故通報及處理流程啟動應變機制，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

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
康那香企業股份有限公司 (續)	2026年10月30日	會員個資遭不當利用，亦透過電子郵件、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。
台灣數位光訊科技股份有限公司	2026年10月30日	台數科公司及子公司資訊系統遭受外部不明駭客網路攻擊，致使部分伺服器檔案遭惡意加密，已立即啟動資安事件應變機制，執行受影響設備隔離、帳號權限管制與密碼變更、部署端點偵測監控（EDR）及透過安全備份進行系統還原等措施，並持續進行鑑識分析、事件監控及影響範圍調查。目前評估沒有個資外洩，亦沒有核心機密或重要文件資料外洩等情事發生，對公司及子公司營運及財務無重大影響。
鑫傳國際多媒體科技股份有限公司	2026年10月30日	鑫傳公司及子公司資訊系統遭受外部駭客網路攻擊，致使部分檔案無法解密，影響部分內部作業系統之正常運作。已立即啟動資安事件應變機制，執行受影響設備隔離、帳號權限管制與密碼變更及透過備份進行還原等措施，事件監控及影響範圍調查。目前評估尚無個資、大量內部文件檔案資料有外洩之虞，對公司營運及財務無重大影響。

■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 促銷話術貼近日常需求

詐騙類型趨勢

產品服務型占比小幅回升，持續居本週首位，詳見圖6。其中「服飾與皮夾」廣告以「多件低價」、「買一送一」及「雙十一早鳥」優惠等話術吸引民眾購買，把日常穿用需求與限時折扣連結。「電動修枝剪」廣告則宣稱商品為進口貨，並承諾在 12 年內提供換貨服務。廣告以工廠直銷的宣傳方式，吸引買家私訊下單，並透過售後服務等承諾，減輕對網路購物詐騙的疑慮，吸引有購物需求的民眾聯繫。

身分冒充型在三類中占比最低，本週較前週下降。其中「居家量測儀」廣告藉知名醫療器材品牌名稱與「醫師推薦」塑造專業形象，宣稱產品可量測血壓與血糖，並具備醫用級精準度。廣告再以照顧長輩的健康等話術吸引注意，並用「限量折扣」營造必須即早購買的急迫感，催促民眾透過購物連結下單。

金融投資型占比小幅回升，本週維持第二位。「澳洲房產」廣告以法律保障為訴求，並宣稱當地購買房產可免徵遺產稅與贈與稅，將「分散市場風險」、「跨國配置」及「財富傳承」等話術作為誘，再規劃安排房產投資與移民講座等相關說明會，強調有資深移民團隊及案例分享，把購屋需求連結到家庭長期規劃，吸引想學習資產配置的民眾報名。

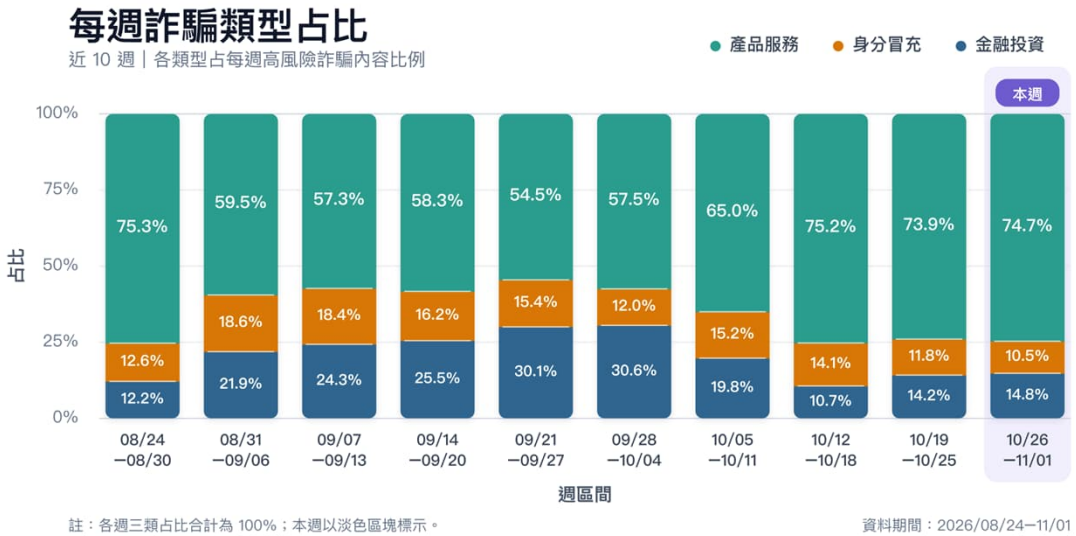


圖6 | 每週詐騙類型占比

關鍵字趨勢

「優惠」仍居首位，詳見圖7，升至第 6 名的「輕鬆」則出現在車輛買賣廣告。相關廣告主打零頭期款、低月付與優惠利率，吸引民眾私訊詢問；雖另註明零元交車須依審核條件辦理，但重點仍放在降低購車門檻的話術上。「點擊」首度進入前 10 名並升至第 3 名，廣告以多件優惠與不滿意全額退款等承諾，催促民眾前往購物連結選購。

「配方」升至第 2 名，與退居第 9 名的「健康」共同出現在口服錠劑廣告。相較前週「配方」強調體重管理與代謝，本週轉以入睡困難、輪班及作息不規律等情境吸引注意，宣稱配方可改善睡眠並引導點擊選購。「日常」維持第 8 名，相關人蔘廣告以藥膳進補與舒緩疲勞為訴求，將保健需求帶入家庭飲食。

「投資」退居第 7 名，本週出現於宗教祈福廣告內，廣告以財運、事業卡關為訴求，再以信眾見證邀請民眾參加法師主持的補財庫儀式，屬關鍵字命中，非金融投資型廣告。「限量」維持第 4 名，廣告情境由前週保養品轉向股票教學，搭配課程折扣、教材及選股軟體吸引報名。

整體來看，本週前十大關鍵字仍圍繞三條主線：以折扣與限時優惠促購、以睡眠與保健需求帶動健康食品銷售、以改善財運或學習交易為名吸引理財需求，詐騙集團持續貼著民眾的日常需求設計話術。

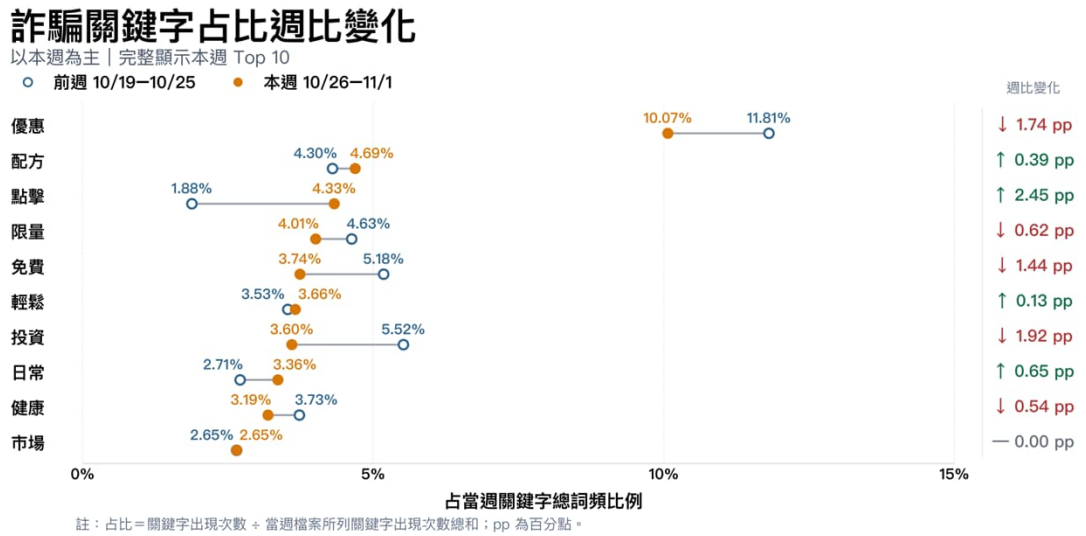


圖7 | 詐騙關鍵字占比週比變化

焦點文章

十月資安重點：PHP 重大漏洞與第三方供應鏈外洩事件

從多筆重大資安漏洞公告到客戶資料外洩的資安事件回顧

過去一個月內，PHP、Node.js、Go 等主流語言環境，以及 GitLab、Oracle Java SE 等開發維運工具接連揭露高風險漏洞。針對相關風險，資安院與TWCERT/CC皆已於第一時間發布告警，提醒政府機關與企業組織進行漏洞更新；多國資安組織亦密集發布預警，部分單位則採取預防性關閉對外網站服務的處置措施。 同時，國內外亦接連傳出第三方 SaaS 供應商遭入侵，導致電商客戶資料外洩並引發後續社交工程詐騙的連鎖事件。

十月 PHP 重大遠端程式碼執行(RCE)漏洞

PHP 官方於十月下旬釋出緊急安全更新，修補 CVE-2026-109618 與 CVE-2026-109619 兩項 CVSS v4.0 評分達 9.2 的重大漏洞 。此為釋放後記憶體使用(Use-After-Free)弱點，未經授權的遠端攻擊者僅需發送特製 HTTP 請求，即可在伺服器端執行任意程式碼(RCE)；目前社群已釋出概念驗證程式碼(PoC) 。

由於 PHP 廣泛應用於各類網頁系統與 CMS，本次漏洞直接牽動供應鏈上中下游。近期 TWCERT/CC 即接獲通報，企業因以 PHP 為核心的WordPress建置ERP系統，疑似未及時更新而遭入侵，導致內部機敏資料外洩。相關軟體廠商須清查相依套件並釋出修正，企業維運團隊亦需密切追蹤原廠更新以完成部署，避免系統遭利用已公開的 PoC 進行攻擊。

客戶資料外洩與社交工程連鎖效應

TWCERT/CC於10月間接獲多起電商平台資料外洩事件，調查顯示多數源於整合的第三方 SaaS 平台遭未授權存取。由於此類服務普遍串接購物車、會員、金流及物流資料，一旦供應商端遭入侵，衝擊將直接波及所有合作商家，造成大量消費者個資與完整訂單紀錄外洩。在近期的攻擊活動中，亦觀察到攻擊者導入 ARTEX 等 AI 滲透測試工具，快速探測防禦弱點並竊取資料。

目前此類真實外洩資料已被用於社交工程詐騙。攻擊者假冒品牌客服、銀行或物流人員，核對精確的消費時間與品項以降低受害者防備心，再以重複扣款或設定錯誤為由，誘騙消費者操作 ATM、網銀轉帳，或騙取一次性驗證碼(OTP)，衍生後續財務損失。

焦點文章

企業因應建議

針對核心元件漏洞與供應鏈外洩風險，企業應從掌握套件清冊、廠商治理與資料防護著手因應：除要求委外及軟體廠商交付標準軟體物料清單(SBOM)供內部集中納管、以便在重大弱點公告時自主比對受影響範圍以爭取應變時間外，亦應將外部 SaaS 業者納入合約資安規範與定期稽核，並在內部落實最小權限原則及敏感欄位加密遮罩，降低底層元件或第三方服務遭突破時的資料外洩衝擊 。

關鍵字：漏洞修補、社交工程、SBOM

刊　　名　資安週報第 69 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。