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
整體曝險風險微幅上升 網站安全設定風險加劇

重大漏洞
多項網路設備與管理系統高風險漏洞遭利用 組織應儘速盤點修補

實兵演練
實兵演練揭露存取控管與驗證機制缺失 導致未授權存取及系統權限遭取得風險

聯防監控
防禦迴避高居首位 偵測刺探仍具威脅

蜜罐誘捕
程式遞送控制器(ADC & Gateway)及網站主機伺服器管理系統成為攻擊熱點

事件通報
雲端服務上線前 應先確認必要日誌已啟用並具備足夠保存期間

網路巡查高風險詐騙
產品服務占比回升 商品功效宣稱吸引購買

焦點文章
政府資料匯流平臺應用實例

2026.10.08
065

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

整體曝險風險微幅上升 網站安全設定風險加劇

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8,138項。其中，「元件高風險漏洞」以3,282項居首，「過時或弱加密協定」1,447項次之，「CSP設定不當」則以1,087項超過「TLS憑證不受信任」1,045項，位居第三。前三項合計5,816項，占前10大風險項目總數約71.5%，顯示目前外部曝險風險仍高度集中於元件漏洞、加密協定及網站安全設定等議題。相較上期8,070項，本期整體風險數量增加68項，增幅約0.8%，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3,273項增至本期3,282項，增幅約0.3%。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」由1,593項減至1,447項，降幅約9.2%；「TLS憑證不受信任」由1,289項大幅減至1,045項，降幅約18.9%。另「未部署WAF」由767項大幅增至853項，增幅約11.2%；「CSP設定不當」由763項大幅增至1087項，增幅約42.5%。

整體而言，本期外部曝險風險較上期小幅增加，其中「過時或弱加密協定」及「TLS憑證不受信任」均呈明顯下降，顯示加密協定及憑證管理已有改善；惟「CSP設定不當」及「未部署WAF」項目明顯增加。建議持續加強高風險元件修補，並強化WAF部署、CSP設定及相關網站安全防護措施，以降低外部曝險風險。

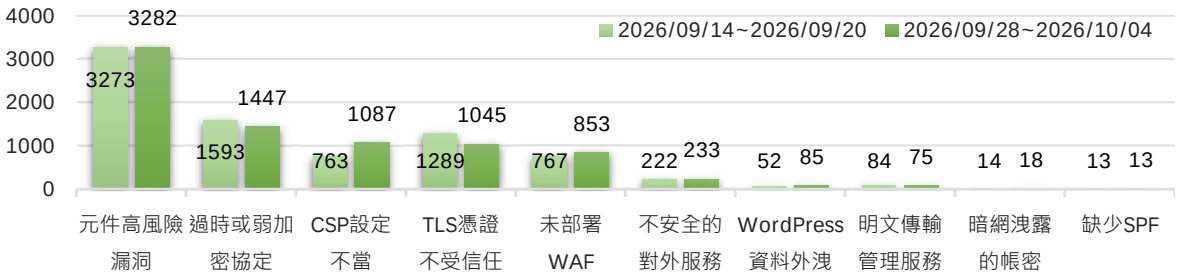


圖1 | EASM檢測結果統計(前10大風險)

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

多項網路設備與管理系統高風險漏洞遭利用 組織應儘速盤點修補

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、Zyxel、Microsoft、pgAdmin、Citrix、Check Point及F5高風險漏洞應盡速修補

- Cisco ISE與ISE-PIC存在多項高風險安全漏洞(CVE-2026-20130、CVE-2026-20192、CVE-2026-20307、CVE-2026-76423及CVE-2026-76460)[1][2][3][4]，類型包含程式碼注入(Code Injection)、不當存取控制(Improper Access Control)、不安全之反序列化(Insecure Deserialization)及身分鑑別繞過(Authentication Bypass)，其中，CVE-2026-76460已遭駭客濫用。
  - CVE-2026-20130：未經身分鑑別之遠端攻擊者可藉由在傳遞至下游元件之輸出中，植入未經妥善處理之特殊元素，於受影響裝置執行任意程式碼。
  - CVE-2026-20192：未經身分鑑別之遠端攻擊者可繞過身分鑑別與授權限制，進而未授權存取受影響裝置。
  - CVE-2026-20307：已通過身分鑑別之遠端攻擊者可藉由向網頁管理介面傳送特製之Java序列化物件，於底層作業系統執行任意程式碼，並將權限提升至root。
  - CVE-2026-76423：未經身分鑑別之遠端攻擊者可藉由向對外開放之REST API連接埠傳送特製HTTP請求，以管理者權限讀取及變更ISE組態與身分資料。
  - CVE-2026-76460：未經身分鑑別之遠端攻擊者可藉由向存在缺陷之API端點傳送特製請求，繞過網頁管理介面之身分鑑別，進而未授權存取受影響裝置。
- Cisco Secure FMC存在多項高風險安全漏洞(CVE-2026-20242與CVE-2026-20324)[5][6]，類型分別為不安全之反序列化(Insecure Deserialization)與不當存取控制(Improper Access Control)。
  - CVE-2026-20242：當啟用外部資料庫存取(External Database Access)功能，且存取清單中已設定主機時，未經身分鑑別之遠端攻擊者可從清單內之主機向特定TCP連接埠傳送特製之Java序列化位元組串流，進而於受影響裝置以root權限執行任意指令。

- CVE-2026-20324：當啟用sftunnel通訊協定時(系統預設為啟用)，已通過身分鑑別之遠端攻擊者可藉由劫持sftunnel連線，或冒用合法註冊之sftunnel對端身分傳送指令，將惡意檔案寫入裝置任意位置，並以root權限執行任意程式碼。

- Zyxel GS1900系列交換器存在堆疊型緩衝區溢位(Stack-based Buffer Overflow)漏洞(CVE-2026-7273)[7]，未經身分鑑別之同一區網攻擊者可藉由向CGI程式傳送特製HTTP請求，觸發記憶體毀損，進而於受影響裝置執行作業系統指令，該漏洞已遭駭客濫用。

- Microsoft Office SharePoint存在程式碼注入(Code Injection)漏洞(CVE-2026-65660)[8]，已通過身分鑑別之遠端攻擊者可藉由傳送特製請求注入程式碼，進而執行任意程式碼，該漏洞已遭駭客濫用。

- pgAdmin 4存在身分鑑別繞過(Authentication Bypass)漏洞(CVE-2026-86863)[9]，當啟用Webserver身分鑑別來源時，未經身分鑑別之遠端攻擊者可藉由傳送特製HTTP請求標頭冒充任意使用者(包含管理者)，進而取得pgAdmin管理權限，請儘速確認並進行處置。

- Citrix NetScaler ADC與Citrix NetScaler Gateway存在2項高風險安全漏洞(CVE-2026-88771與CVE-2026-88772)[10]，類型分別為不當輸入驗證(Improper Input Validation)與記憶體緩衝區操作限制不當(Improper Restriction of Operations within the Bounds of a Memory Buffer)，該等漏洞皆已遭駭客濫用。

  - CVE-2026-88771：未經身分鑑別之遠端攻擊者可利用輸入驗證缺陷，進而執行任意指令。

  - CVE-2026-88772：當Citrix NetScaler ADC或Citrix NetScaler Gateway啟用DTLS組態(VPN虛擬伺服器預設啟用)時，未經身分鑑別之遠端攻擊者可觸發記憶體溢位，進而執行任意程式碼或造成服務阻斷。

- Check Point Security Management Server、Multi-Domain Security Management Server、Log Server、Multi-Domain Log Server及SmartEvent存在路徑遍歷(Path Traversal)漏洞(CVE-2026-93616)[11]，未經身分鑑別之遠端攻擊者可利用路徑遍歷與檔案上傳缺陷上傳任意腳本，進而執行任意程式碼，該漏洞已遭駭客濫用。

- F5 BIG-IP Access Policy Manager(APM)存在堆積型緩衝區溢位(Heap-based Buffer Overflow)漏洞(CVE-2026-94127)[12]，當APM設定為OAuth授權伺服器時，未經身分鑑別之遠端攻擊者可藉由傳送特定惡意流量，進而執行任意程式碼，該漏洞已遭駭客濫用。

1. https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ISE-ABP-VNSW7Tn5
2. https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-multi-hrP9jQSQ
3. https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-rce-se7bYU57
4. https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-hardening-ise-XU5EwX5T
5. https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-fmc-javarce-y2NypXwk
6. https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-fmc-sftunn-codex-c3O4Jft2
7. https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-stack-based-buffer-overflow-vulnerability-in-gs1900-series-switches-06-16-2026
8. https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-65660
9. https://github.com/pgadmin-org/pgadmin4/issues/10383
10. https://support.citrix.com/support-home/kbsearch/article?articleNumber=CTX697096
11. https://support.checkpoint.com/results/sk/sk1000171
12. https://my.f5.com/manage/s/article/K000162605

■實兵演練

實兵演練係模擬真實攻擊情境，檢驗資通系統弱點、防護能力及應變機制，以提升整體資安防禦韌性

實兵演練揭露存取控管與驗證機制缺失 導致未授權存取及系統權限遭取得風險

本年資通系統實兵演練針對政府機關與關鍵基礎設施提供者，於擇定時間進行演練，截至目前已累計389筆攻擊紀錄，依目前弱點數量統計，排名前3名依序為「無效的存取控管」、「驗證機制失效」及「不安全的組態設定」，詳見圖2。

其中「無效的存取控管」類型計87筆為最多，主要發現系統功能與API未落實適當之身分驗證與授權，攻擊者可透過直接存取功能路徑、竄改查詢參數或檔案路徑等方式，取得未經授權之個人資料或系統敏感檔案；其次為「驗證機制失效」類型計83筆，主要發現預設帳號、弱密碼與驗證流程缺陷等問題，造成攻擊者可透過帳號密碼猜測繞過身分驗證取得系統權限；第三為「不安全的組態設定」類型計81筆，主要發現部分系統之檔案上傳功能僅於前端進行格式限制，攻擊者可繞過限制上傳Webshell並執行系統指令，進一步擴大攻擊影響範圍。

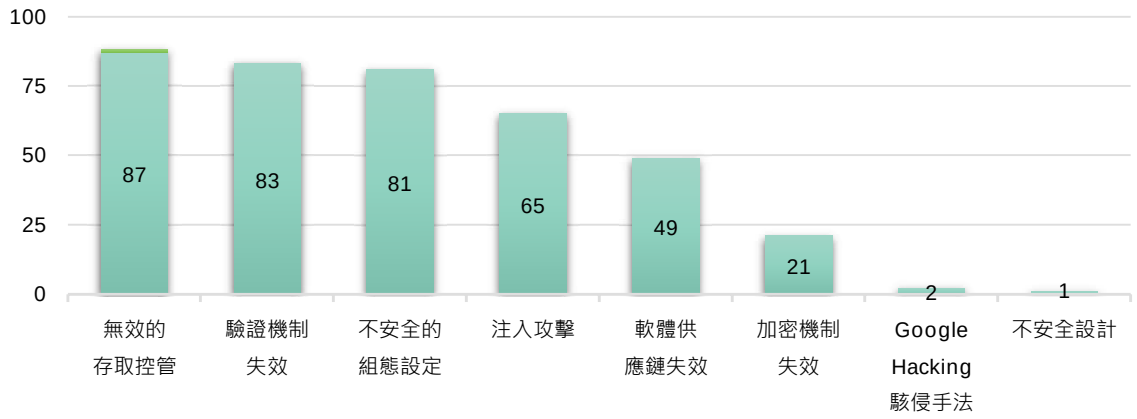


圖2 | 網路攻防演練資通系統實兵演練統計

建議機關及關鍵基礎設施提供者，採取下列防護措施

- 應針對系統功能與API落實身分鑑別與授權機制，依最小權限原則限制資料與功能存取範圍，避免未經授權使用者透過直接存取路徑或竄改參數取得敏感資料
- 應強化帳號與身分驗證機制，避免使用預設帳號與弱密碼，並針對OTP等驗證資訊設定有效期限與單次使用機制，必要時導入多因子鑑別(MFA)，降低驗證機制遭繞過之風險
- 應於伺服器端落實檔案上傳檢核，將上傳目錄與程式執行目錄分離，並限制上傳目錄之程式執行與寫入權限，避免惡意檔案遭上傳後執行

■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3。「防禦迴避」為最常見攻擊手法，占比14.6%，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前期偵查與資訊蒐集行動。觀察到的主要手法包括IP 區段掃描、主動式掃描、以及憑證資訊蒐集。攻擊者透過自動化工具大規模掃描外部網段與公開服務，以識別可存取主機、開放埠與系統類型，同時蒐集與帳號憑證相關的資訊，作為後續登入嘗試或攻擊行動的基礎。部分活動顯示攻擊者會先進行廣泛探測，再逐步聚焦特定服務與帳號目標，以提高後續攻擊成功率。此類行為多屬攻擊前期準備階段，雖不直接造成破壞，但能有效提升後續滲透與入侵效率。建議強化對異常掃描流量與登入探測行為的監控，定期檢視對外資產暴露情形，並結合威脅情資分析掃描來源，以提前辨識潛在攻擊準備活動。

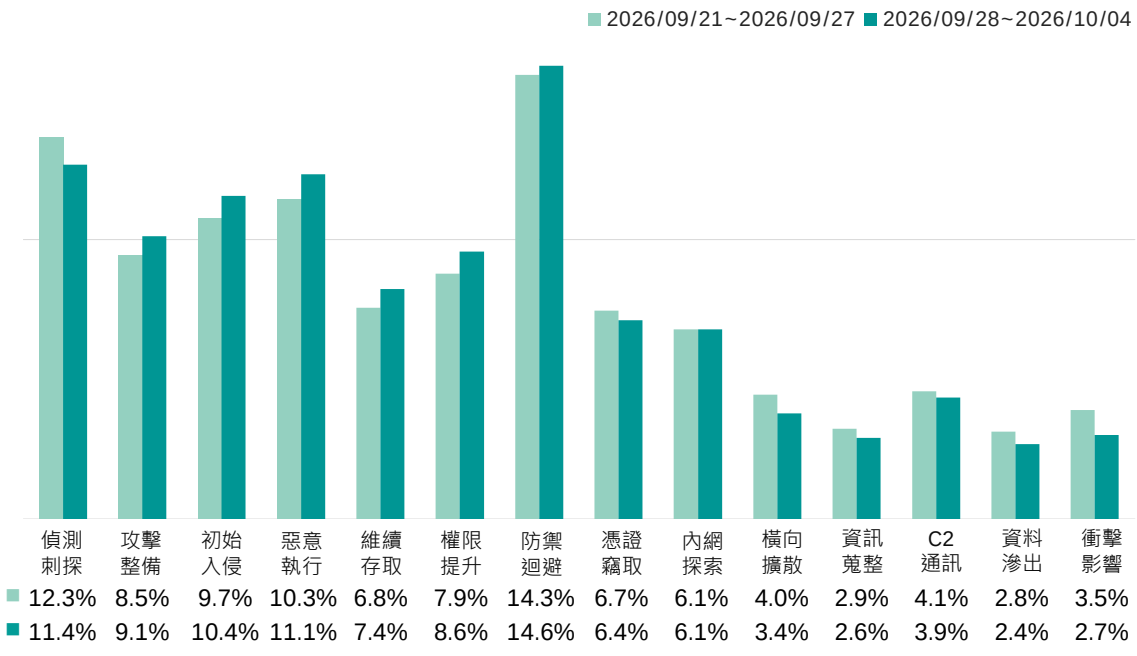


圖3 | 資安聯防監控攻擊階段統計

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（EDR），監控異常指令及系統工具使用行為
- 加強 PowerShell、CMD、Shell 等指令執行與歷程紀錄稽核，避免紀錄遭關閉或清除
- 限制高風險系統工具與管理工具的執行權限，降低合法工具遭濫用風險
- 落實特權帳號與最小權限管理，監控異常權限操作

偵測刺探 (Reconnaissance)

- 加強監控大量 IP、Port 掃描及短時間高頻連線等異常探測行為
- 定期盤點對外服務與網路資產，降低非必要服務及管理介面的暴露
- 強化帳號與憑證保護，監控異常登入、帳號列舉及憑證探測行為
- 結合威脅情資分析掃描來源 IP，針對高風險來源進行告警、封鎖或持續追蹤

■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)及網站主機伺服器管理系統成為攻擊熱點

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68.64%、「遠端控制」服務攻擊占比26.08%，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68.38%。「遠端控制」服務亦有26.66%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4。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Langflow 1.3.0之前的版本存在身分驗證漏洞之CVE-2025-3248，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。

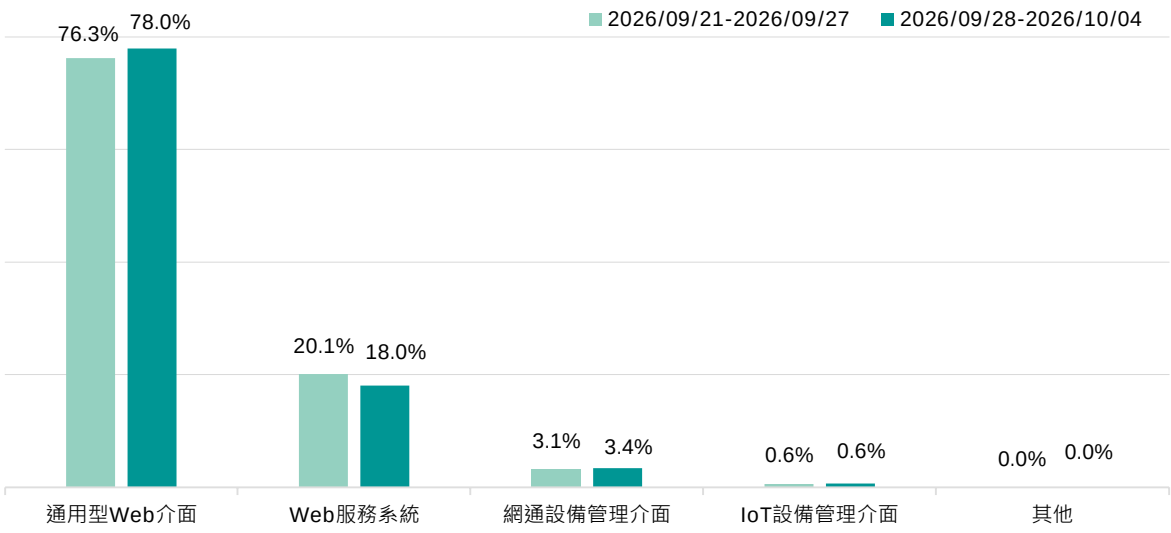


圖4 | 本週網頁應用介面之誘捕攻擊比例統計

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、身分驗證繞過漏洞、指令注入漏洞及SQL注入漏洞，攻擊目標涵蓋程式遞送控制器(ADC & Gateway)、網站主機伺服器管理系統、大模型API統一介面與代理伺服器工具、企業級端點與安全管理系統及資安防護系統與雲端檔案管理平台。

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	⬆1	CVE-2026-41940[2]	cPanel & WHM	9.8	✓
■	3	⬆1	CVE-2026-42271[3]	LiteLLM	8.8	✓
■	4	⬆new	CVE-2026-21643[4]	Fortinet FortiClientEMS	9.8	✓
■	5	⬆new	CVE-2026-2699[5]	Progress ShareFile	9.8	

類型 ■ 越界讀取漏洞 ■ 身分驗證繞過漏洞 ■ 指令注入漏洞 ■ SQL注入漏洞

1. https://nvd.nist.gov/vuln/detail/CVE-2026-3055
2. https://nvd.nist.gov/vuln/detail/CVE-2026-41940
3. https://nvd.nist.gov/vuln/detail/CVE-2026-42271
4. https://nvd.nist.gov/vuln/detail/CVE-2026-21643
5. https://nvd.nist.gov/vuln/detail/CVE-2026-2699

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

雲端服務上線前 應先確認必要日誌已啟用並具備足夠保存期間

本週總計接獲24件公務機關與特定非公務機關事件通報，詳見圖5，公務機關非法入侵事件中以植入惡意程式占多數，詳見圖6。本週發現機關使用雲端服務時，因未完整設定相關稽核與存取日誌，事件發生後缺乏足夠紀錄可追查異常存取來源及憑證可能外洩管道，增加事件調查難度。

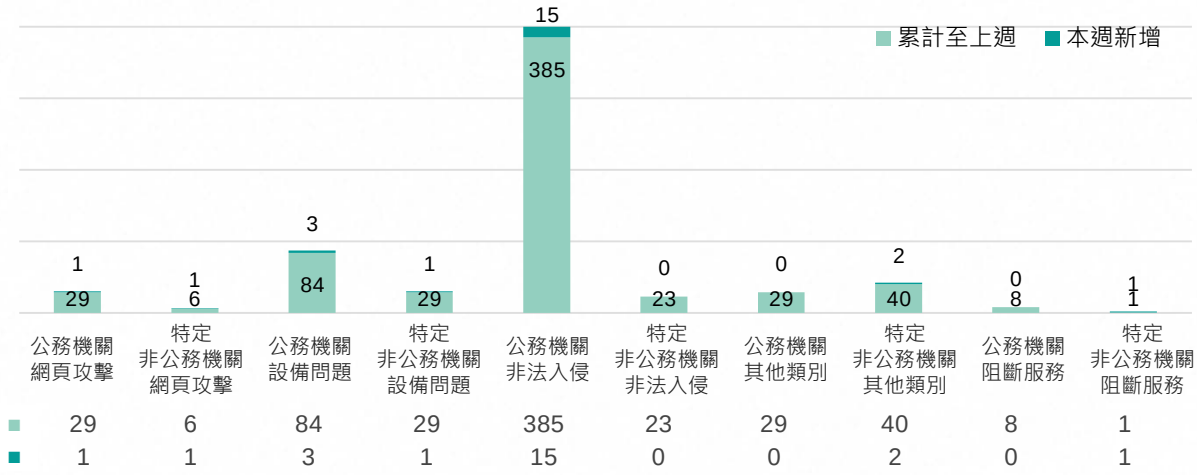


圖5 | 本週公務機關暨特定非公務機關資安事件通報概況

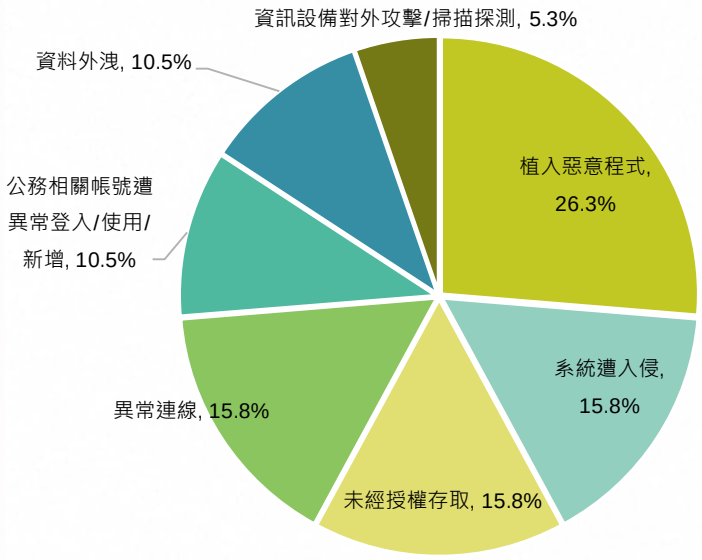


圖6 | 本週公務機關非法入侵事件類型占比

雲端服務通常提供管理操作、身分驗證、資源存取及 API 使用等不同類型日誌，使用單位應於服務啟用初期即確認所需日誌是否已開啟、保存期限是否足以支援事件調查，並建立異常存取與大量使用之監控機制，避免事件發生後才發現缺乏必要紀錄。

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
➢ 雲端日誌不足導致異常存取來源與攻擊行為難以追查 ➢ 憑證遭竊後持續存取雲端資源且缺乏紀錄難以及時發現	➢ 雲端服務啟用時完整開啟管理、驗證、資源存取及API使用日誌 ➢ 依事件調查需求設定適當日誌保存期限，確保關鍵紀錄可供後續追查 ➢ 建立異常登入與大量資源存取監控，及時發現憑證遭濫用之可疑行為 ➢ 定期檢視雲端日誌設定與蒐集狀態，確認必要紀錄持續完整留存可用

3間民間企業揭露重大資安訊息

本週3間民間企業發布重大訊息，產業類別為通信網路業、文化創意業、觀光餐旅業，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
神腦國際企業股份有限公司	2026年09月29日	神腦公司外部伺服器遭受自動化攻擊，並對部份訂單資訊做擷取。本公司接獲通知後，已依個資事故通報及處理流程啟動應變會議，並採取必要防護措施降低影響，同時委請第三方資安廠商協助處理。經評估對本公司營運、財務及服務提供無重大影響，後續將全面強化網路偵測、系統監控與安全管控，以確保資訊安全。

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
鈊象電子股份有限公司	2026年09月29日	鈊象公司發現不明IP異常侵入公司營運資訊設備，當日資安團隊偵測發現後，隨即啟動資安緊急應變機制。目前評估對公司營運尚無重大影響，後續將持續提升資安防禦，強化監控與防護層級。
安心食品服務股份有限公司	2026年10月01日	安心公司接獲少數消費者反映，疑似有第三方不當取得資料並透過電子郵件聯繫消費者，針對此情形已責成委外廠商立即進行相關修補改善，未來將持續強化委外廠商之資安管控機制，以確保客戶權益。

■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 商品功效宣稱吸引購買

詐騙類型趨勢

金融投資型的占比持續上升，仍是本週第二大類型，詳見圖7。以 AI 投資工作坊為例，宣傳列出的教學內容包括用人工智慧整理行情、分析台股、美股等市場，以及解釋交易判斷背後的理由。這類宣傳抓住想學投資、又想了解新工具的需求，以免費參加吸引民眾先來了解，再強調名額有限，催促有興趣的人報名到場學習。

身分冒充型占比較前週下降。羊毛上衣廣告打出品牌聯名的名義，並宣稱「官方正品保證」，讓民眾相信買到的是品牌正品。廣告再承諾提供售後服務，減輕民眾對商品有問題卻無人處理的擔心，接著搭配雙十限定、多件低價的優惠，吸引民眾點擊購物連結。

產品服務型占比回升，仍占整體一半以上，與金融投資型的差距也擴大。汽車鍍膜劑廣告搭配雙十節促銷，宣稱能填補車漆表面的細縫，效果可維持一年以上，再以三瓶優惠價吸引車主。廣告先用保養效果引起興趣，再強調優惠只在節日期間提供，讓有保養需求的人覺得現在買更划算，進而點擊連結下單。

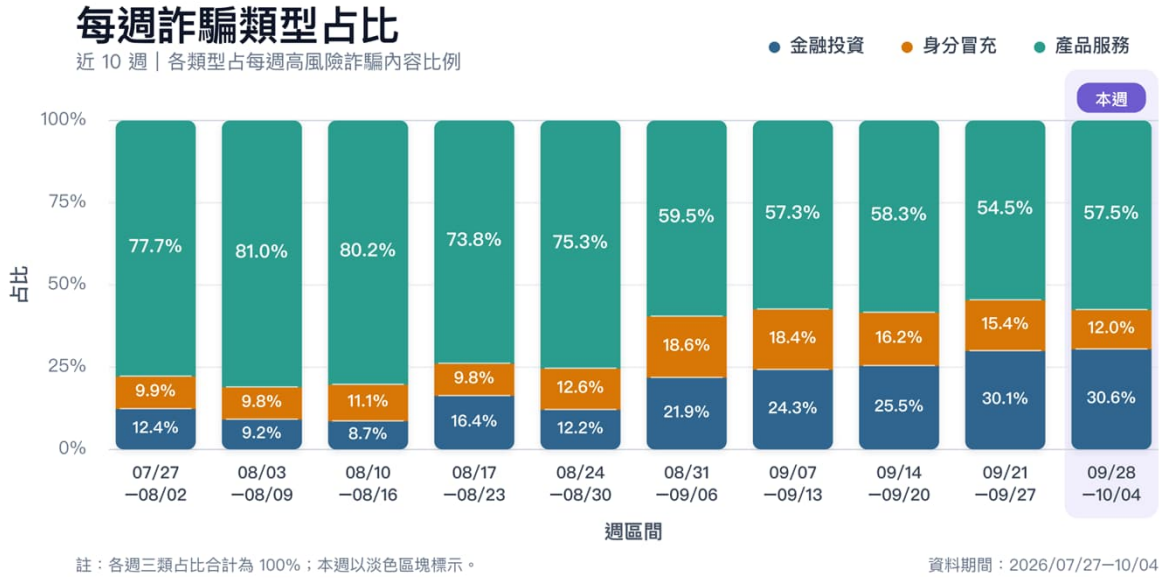


圖7 | 每週詐騙類型占比

關鍵字趨勢

「市場」升至本週第 1 名，詳見圖8，相關廣告推銷美股課程，強調從開戶、下單到選股都會教，並宣稱已有許多學員參加，讓想學投資的人覺得課程值得一試。「投資」退居第 2 名，課程廣告以靠股息支付生活開銷的故事吸引民眾，再用限時折扣和留言領券，鼓勵讀者進一步了解課程。

「領取」升至第 4 名，「資訊」和「上下車」進入前 10 名，分居第 5、6 名。這些廣告主打每天免費提供股票名單，以及買進、賣出時機的提示，再用「別等漲了才追」催促民眾點擊加入。與前週「資訊」廣告整理新聞、提供直播解析的方式相比，本週更直接以買賣提示吸引人，讓民眾期待能掌握買進、賣出的時機。

「優惠」升至第 3 名，防曬美妝廣告宣稱一瓶兼顧防曬和妝前打底，再以限時低價吸引購買。「免費」退居第 9 名，借貸廣告仍用免費諮詢吸引聯繫，並宣稱不看條件、一小時內就能通過審核。整體而言，本週前十大關鍵字以投資學習、股票資訊為主，也可見用低價商品與快速審核吸引人的廣告。

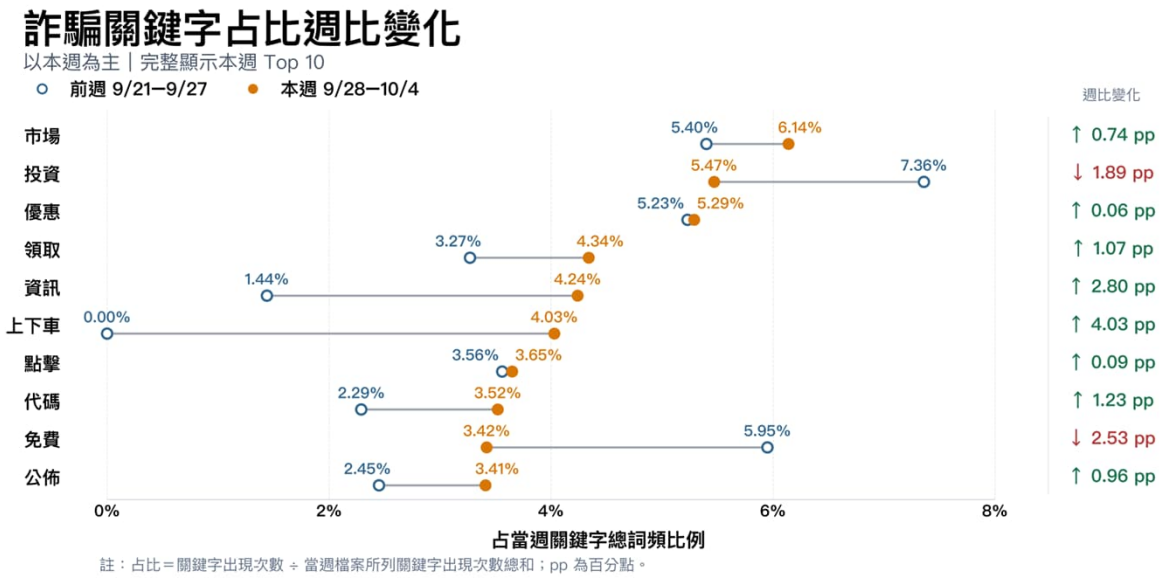


圖8 | 詐騙關鍵字占比週比變化

焦點文章

政府資料匯流平臺應用實例

一、跨機關資料協作困境

於人工智慧驅動治理時代中，資料儼然成為與土地、人才等並列之關鍵國家資源，分析、利用大量資料集之需求日益擴張。我國政府各機關依其法定執掌蒐用資料，雖迄今已累積可觀巨量資料可供後續政策分析之用，惟其資料治理基礎建設結構歧異，產生跨機關資料分享藩籬而無法妥善利用資料價值，而形成「資料孤島」現象。該現象使機關循證治理窒礙難行，以致無法妥善利用跨機關資料豐富價值，而面臨技術、法制、政治層面上等多方實務缺口：

- 技術層面：各機關已有各自獨立且不相容之資料基礎建設，且各自採用不同資料去識別化與資料處理流程，無兼容於多個機關之資料系統。
- 法制層面：因跨機關資料協作所衍生之法遵議題複雜，各機關恐因須審慎處理個資以保護資料隱私，進而遏止資料協作意願。
- 政治層面：機關釋出資料意願用於資料協作之誘因不足，除因上述兩層面實務缺口而產生之隔閡，各機關亦無明確管道知悉可用於資料協作之資料集資訊。

因缺乏對於跨機關資料治理之完整擘劃，導致跨機關資料協作面臨技術層面的系統架構與標準歧異、法制合規要求與隱私資料保護等困難，以致難以全面掌握跨領域複雜問題，整合跨部門資訊敏捷回應各式新興挑戰。政府資料匯流機制正是為了解決此問題，緩解我國政府跨機關資料協作困境，為一重要政府資訊基礎建設。

二、資料匯流平臺與機制概述

（一）平臺服務目標與參與機關角色

基於我國政府循證治理之決策基礎下，本院建置「政府資料匯流協作分析平臺」（下稱本平臺），作為以跨機關資料協作與分析結果為釐清政策成效、制定新政策之關鍵依據。依我國個資法遵要求，本平臺設計理念採「資料可用而不可識別」、「近用而非移轉」原則，於不移轉機關原始資料情形下，完成跨機關資料關聯分析。於資料協作案中，依參與機關與本平臺對資料掌控程度、處理方式之異同，可將資料協作案參與各方分為以下三類：

焦點文章

- 資料需求者：指為履行特定業務或循證治理目的，而具有透過本平臺向其他參與者請求並整合相關資料之需求之政府機關。
- 資料提供者：指存放或保有政府資料，且介接本平臺之政府機關，具備審核資料需求者申請資料運用目的與合法性之權限。
- 資料處理者：指負責維運本平臺，並於資料需求者及資料提供者確定之資料運用範疇內，受託處理資料之政府機關。

（二）創新資料系統架構設計原則

本平臺採用以下四種創新資料系統架構設計原則，以實現前述資料協作流程：

- 隱私優先設計：確保資料可用而不可識別，提供全資料生命週期隱私保護，彰顯機關資料主權，並從源頭落實資料最小化。
- 聯邦式資料流架構：貫徹近用而非移轉原則，各機關節點僅與管理平臺溝通，由平臺協調跨機關資料流且不儲存任何原始資料。
- 功能模組化鬆耦合設計：平臺各元件、功能採模組化設計，分層服務且權責明確，平臺功能得以擴充而不破壞既有結構。
- 協調式控制運作機制：平臺端管理平臺負責編排、控管資料處理流程，統一控管各節點運算資源，並保存日誌紀錄以資後續稽核所需。

（三）平臺資料保護技術施用與評測

本平臺於跨機關資料協作過程中施用資料保護技術，以降低受處理資料之重新識別風險，使資料提供機關得以在可接受之風險下提供資料，以減少協作過程中之合規磨擦。本平臺以動態假名化保護用於跨機關連結之直接識別欄位，並視資料協作案應用目的選用合適之資料保護技術，整理如表3所示。另外，本平臺提供資料品質評測指標，以便機關承辦人快速評估資料保護成效。

焦點文章

表3 | 資料保護技術最佳實踐與評測指標整理

項目	K 匿名	合成資料	差分隱私
技術說明	經分組泛化後，使任一筆資料至少與 K - 1 筆紀錄相似	依據真實資料統計特性生成之模擬資料	藉由加入隨機雜訊，確保資料集中單一個體資訊不可被辨識
輸出樣態	資料清單	資料清單	聚合統計量
應用目的	泛用資料分析	模型訓練資料	統計指標釋出
隱私性指標	檢查風險	指認性、可鏈結性、推論性	成員推論攻擊風險
可用性指標	抑制率	屬性分佈相似度、屬性對趨勢	等效雜訊量

三、應用實例——外國專業人才在臺就業狀況分析

（一）實例場景背景說明

本平臺正進行應用實例以「外國專業人才在臺就業狀況」為題，針對持有效聘僱許可之外國專業人才在臺就業狀況，基於跨部會資料統籌分析，評估政策執行效益與新政策制定之參考。資料需求者為國家發展委員會（下稱國發會），依循證治理目的、採個資法第 16 條但書規定目的外利用要件，整合勞動部勞動力發展署（下稱勞發署）、內政部移民署（下稱移民署）、衛生福利部中央健康保險署等跨機關資料，以統一證號、護照號碼等欄位進行資料關聯。

（二）跨機關資料協作流程

一趟完整資料協作歷程整理如圖9所示，為了說明方便，該示意圖僅展示勞發署與移民署部分。資料協作案由國發會向本平臺提出協作申請，經勞發署、移民署同意後始得進行。機關原始資料由部署於機關內部存取節點進行擷取，施以動態假名化保護直接識別欄位，並進行資料前處理產製必須欄位資訊；過程中僅擷取必要之欄位資訊，以符合資料最小化原則。各機關隨後便以加密分段方式、通過加密保護通道，傳輸至本平臺進行關聯與後處理，並施以資料保護技術以進一步保護間接識別欄位資訊，有效降低資料協作最終成果重新識別風險。最後，國發會得以該結果遂行循證治理用途。

焦點文章

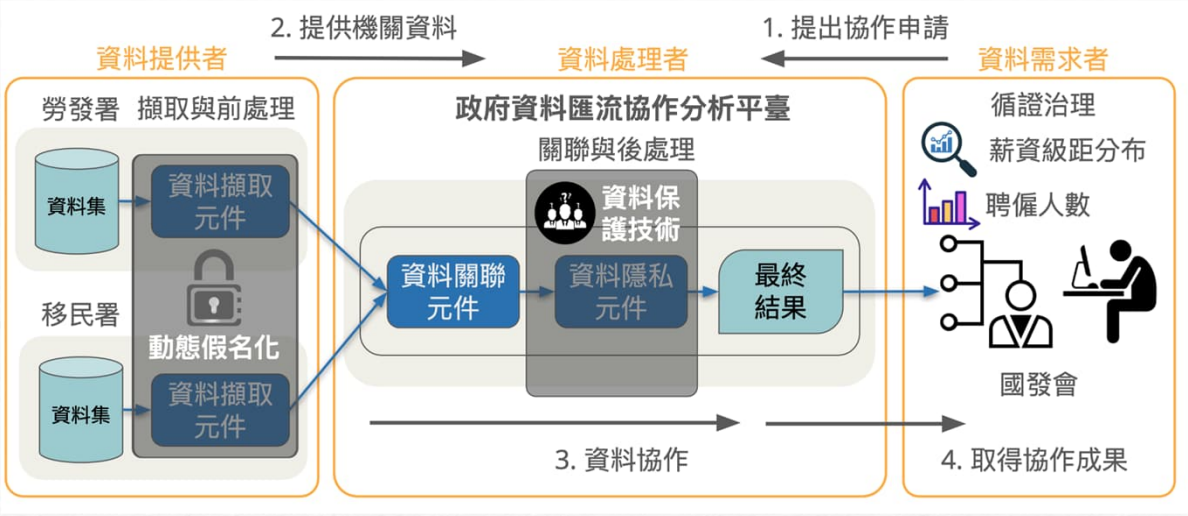


圖9 | 跨機關資料協作完整資料處理流程示意圖

四、結語

本平臺有效緩解現今跨機關協作痛點，提供一多層面服務整合平台解決方案：

- 打破跨機關資料孤島（技術面、困境一、困境二）：本平臺為各機關均可介接之標準化資料匯流分析協作平臺，可用於執行我國政府機關基於循證治理之跨機關資料協作與分析需求。
- 實現資料保護法遵要求（法制面、困境二）：本平臺提供加密傳輸安全通道、資料保護技術施用與評測等功能，並訂定介接要點、申請表等程序文件，以實現我國資料保護與各機關法遵需求。
- 加速機關導入指引與推廣（政治面、困境一）：本平臺已經模擬實證案驗證可承載實務上大量資料處理需求，可作為我國資料協作分析典範，以期加速各機關導入、推廣使用。

本院將持續深化平臺功能發展與實證部署，致力於資料利用與隱私保護之間尋求最適平衡，為我國邁向以信任為基礎的資料流通生態系，提供堅實的技術支撐與制度支援。

關鍵字：資料孤島、資料保護技術、跨機關資料協作

刊　　名　資安週報第 65 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。