國家資通安全研究院
National Institute of Cyber Security

資安週報

Cyber Security Weekly Newsletter

事件通報

完善的日誌管理與保存機制是確保資安事件可追溯性的重要基礎

聯防監控

防禦迴避攻擊持續居高不下 資安專家籲強化端點防護與指令稽核

蜜罐誘捕

Citrix NetScaler ADC與Cisco IOS XE網通設備作業系統成攻擊熱點

外部曝險分析

EASM曝險週增12% 未部署WAF與CSP設定不當增幅最大

網路巡查高風險詐騙

本期高風險內容仍以產品服務為主 請持續留意假商品、假客服與生活化包裝手法

焦點文章

隱私強化技術與應用—資料時代下安全釋放資料價值的全新路徑

2026.03.12
035

資安儀表板

事件通報、聯防監控、蜜罐誘捕、外部曝險分析及網路巡查高風險詐騙等五類量化指標

■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

完善的日誌管理與保存機制是確保資安事件可追溯性的重要基礎

本週總計接獲10件公務機關與特定非公務機關事件通報，詳見圖1，公務機關非法入侵事件中以異常連線占多數，詳見圖2。其中有機關遭偵測發現與 Android 殭屍網路 Vo1d 相關連線特徵，經查該連線係透過機關無線AP對外連線。然而，由於該設備未建立完整的連線日誌紀錄與保存機制，無法回溯實際連線設備與使用者來源，導致事件調查過程缺乏佐證資訊，影響後續追蹤與處置作業。

當網路設備缺乏適當的日誌紀錄與保存機制時，將影響事件調查的可追溯性(Traceability)，使異常行為難以進一步確認來源設備或責任範圍。特別是在無線網路或共用網路環境中，若未保存連線紀錄與設備識別資訊，事件發生後往往難以回溯實際來源。建議機關應建立日誌管理制度，將重要網路設備(如防火牆、無線基地台、VPN、網路閘道等)之連線紀錄納入日誌管理範圍，確保能記錄來源 IP、設備識別資訊(如 MAC 位址)、連線時間與存取紀錄等資訊。同時應訂定適當的日誌保存期限與集中管理機制，以確保於資安事件發生時，能透過歷史紀錄進行追蹤分析，提升事件調查能力與整體資安治理效能。

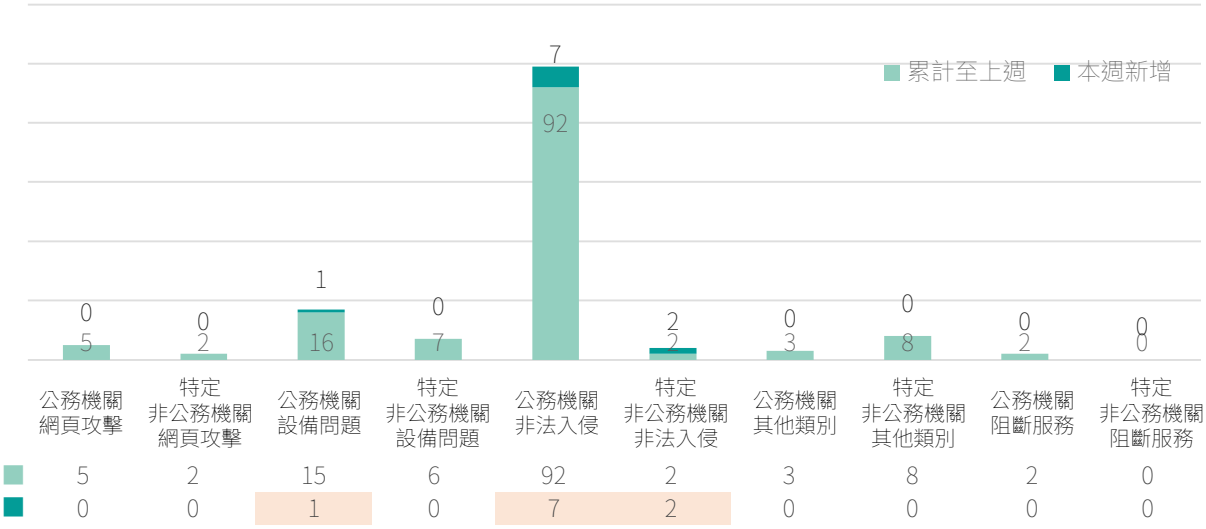


圖1 | 本週公務機關暨特定非公務機關資安事件通報概況

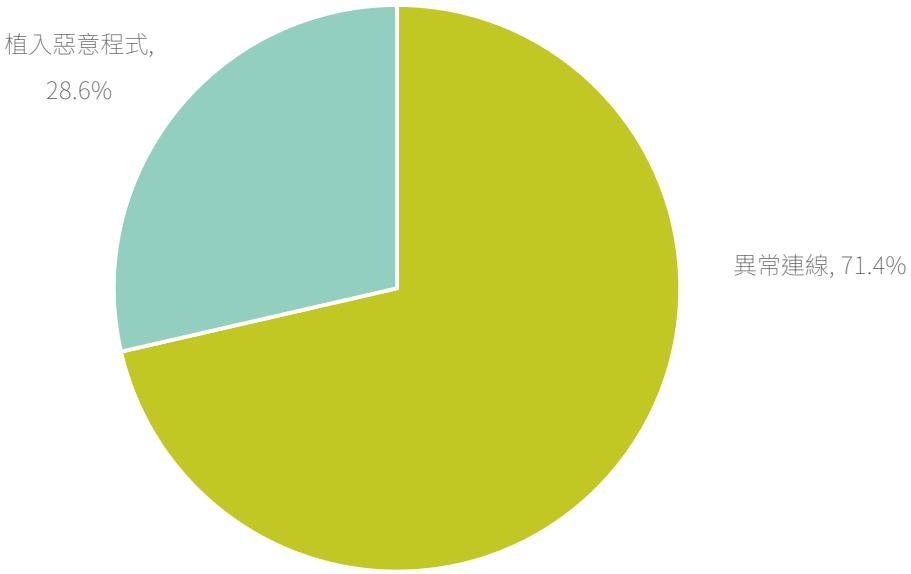


圖2 | 本週公務機關非法入侵事件類型占比

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
➢ 攻擊者利用無線網路匿名連線滲透內網 ➢ 惡意裝置連線建立殭屍網路控制通道	➢ 建立無線網路設備連線日誌紀錄機制，保存來源IP與MAC位址資訊 ➢ 導入集中式日誌管理平台，統一蒐集防火牆與網路設備連線紀錄 ➢ 強化無線網路身分驗證機制，避免未授權設備接入內部網路環境 ➢ 定期監控與分析異常連線行為，及早發現殭屍網路相關可疑活動

2間民間企業揭露重大資安訊息

本週2家民間企業發布重大訊息，產業類別分為光電業與生技醫療業。

- **公司名稱：** 榮創能源科技股份有限公司
- **發布時間：** 115 年 3 月 3 日
- **事件說明：** 榮創公司發現資訊系統遭受駭客網路攻擊，已立即啟動相關防禦機制。目前沒有個資、機密或重要文件資料外洩，經評估後對公司營運無重大影響，後續將持續密集監控，並強化網路與資訊基礎架構之管控，以確保資訊系統安全。

- **公司名稱：** 浩泰精準股份有限公司
- **發布時間：** 115 年 3 月 6 日
- **事件說明：** 浩泰公司與母公司廣泰公司發現遭不明駭客入侵主機，並將伺服器資料加密，導致系統部分無法使用。資安部門立即啟動相關資安防禦與系統復原，目前資訊系統已陸續恢復中，並委請外部資安技術公司及專家共同處理，後續將至調查局報案並依程序向主管機關通報。經初步評估對公司營運無重大影響，後續將持續提升網路與資訊基礎架構之安全管控，以確保資訊安全。

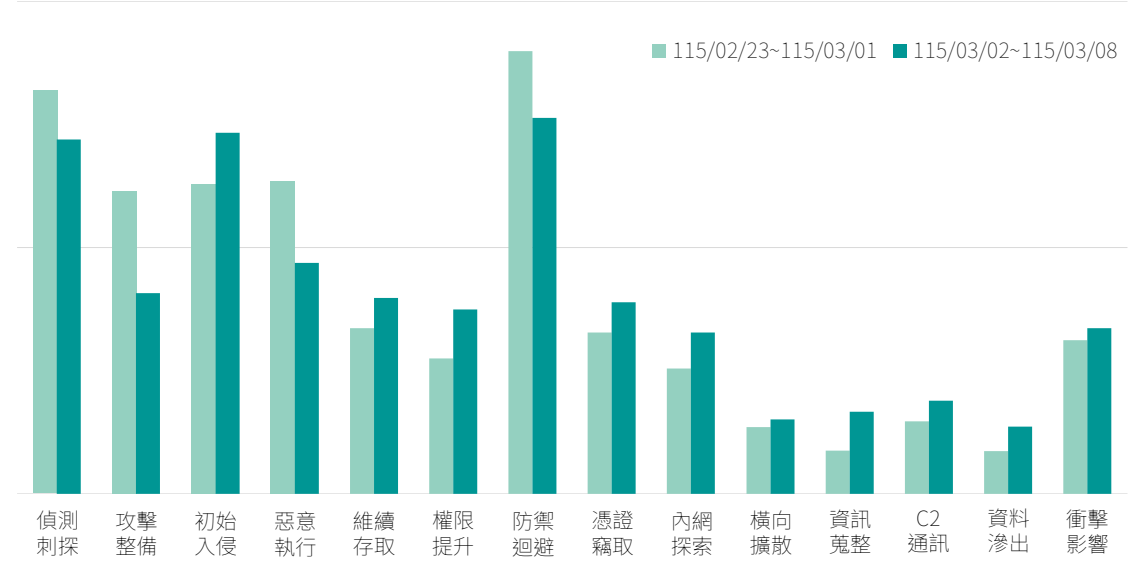
■聯防監控

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

防禦迴避攻擊持續居高不下 資安專家籲強化端點防護與指令稽核

本週資安聯防監控顯示，整體攻擊態勢呈現多元化發展，詳見圖3，其中「防禦迴避」以13.7%持續位居首位，雖較上週16.2%略有下降，但仍是攻擊者最常採用的手法，主要透過關閉或清除指令紀錄、利用合法工具執行惡意命令等技術來規避偵測。其次為「初始入侵」階段，本週佔比13.2%，較上週11.3%明顯上升，顯示攻擊者持續嘗試突破組織防線。第三高為「偵測刺探」階段，佔比12.9%，較上週14.7%有所下降，但仍維持在高位。

值得注意的是，「資訊蒐整」階段從1.6%大幅攀升至3.0%，「C2通訊」也從2.6%增加至3.4%，顯示部分攻擊已進入更深層的滲透階段。此外，「攻擊整備」階段從11.1%降至7.3%，「惡意執行」從11.4%降至8.4%，反映攻擊者策略可能正在調整。整體而言，本週監控數據提醒各組織應持續關注攻擊趨勢是否由初期的偵測刺探進入到更具破壞性的資料竊取與影響階段。



	偵測刺探	攻擊整備	初始入侵	惡意執行	維續存取	權限提升	防禦迴避	憑證竊取	內網探索	橫向擴散	資訊蒐整	C2通訊	資料滲出	衝擊影響
115/02/23~115/03/01	14.7%	11.1%	11.3%	11.4%	6.1%	4.9%	16.2%	5.9%	4.6%	2.4%	1.6%	2.6%	1.6%	5.6%
115/03/02~115/03/08	12.9%	7.3%	13.2%	8.4%	7.2%	6.7%	13.7%	7.0%	5.9%	2.7%	3.0%	3.4%	2.5%	6.1%

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：

➢ 強化防禦迴避偵測能力
- ✓ 導入端點偵測與回應(EDR)解決方案，即時監控異常行為模式
- ✓ 強化指令紀錄稽核機制，確保所有系統操作留有完整記錄
- ✓ 限制高風險工具的使用權限，防止合法工具遭濫用執行惡意命令
- ✓ 落實特權帳號管理，定期檢視並限縮管理權限範圍

➢ 加強初始入侵防護
- ✓ 定期更新系統與應用程式漏洞修補，減少攻擊面
- ✓ 實施多因素驗證(MFA)，提高帳號安全性
- ✓ 強化電子郵件安全閘道，過濾釣魚郵件與惡意附件
- ✓ 加強員工資安意識訓練，提升社交工程攻擊辨識能力

■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

Citrix NetScaler ADC與Cisco IOS XE網通設備作業系統成攻擊熱點

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66.74%、「遠端控制」服務攻擊占比28.96%，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62.70%。「遠端控制」服務亦有32.76% 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。

而網通設備管理介面比例大幅上升主因為Huawei HG532存在遠端程式碼執行漏洞的CVE-2017-17215，遭攻擊次數大幅上升導致。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。

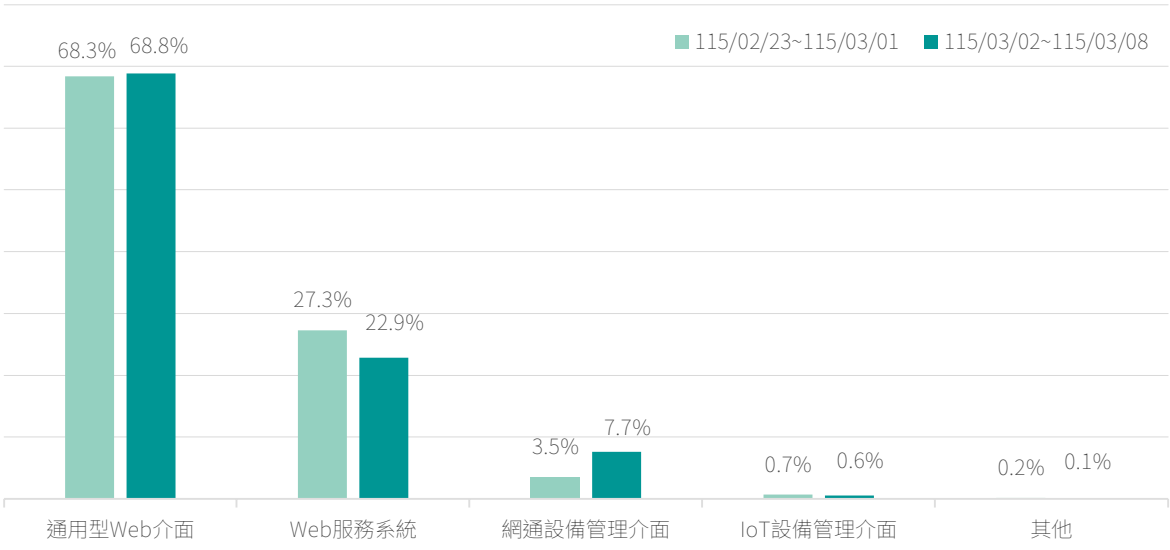


圖4 | 本週網頁應用服務之誘捕攻擊比例統計

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3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、特權提升、遠端程式碼執行及程式碼注入，攻擊目標涵蓋Citrix NetScaler ADC、Cisco IOS XE網通設備作業系統、PHP、GeoServer開放源碼伺服器及Atlassian Confluence Server，顯示此類系統已成為高風險熱點。

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3年漏洞排行列表

排名			漏洞編號	受影響產品	CVSS 3.x Base Score
■	1	-	CVE-2025-5777[1]	Citrix NetScaler ADC	7.5
■	2	-	CVE-2023-20198[2]	Cisco IOS XE網通設備作業系統	10
■	3	↑1	CVE-2024-4577[4]	PHP	9.8
■	4	↓1	CVE-2024-36401[3]	GeoServer開放源碼伺服器	9.8
■	5	↑New	CVE-2024-21683[5]	Atlassian Confluence Server	8.8

類型 ■越界讀取漏洞 ■特權提升 ■遠端程式碼執行漏洞 ■程式碼注入

▶近期重大弱點提醒

近一週本院研究人員發現以下重大弱點資訊，建議組織內部進行檢查與修補：

- Trend Micro Apex One管理主控台存在高風險安全漏洞(CVE-2025-71210[6]與CVE-2025-71211[7])，類型為路徑遍歷(Path Traversal)，當受影響產品之管理主控台服務可被存取時，未經身分鑑別之遠端攻擊者可利用此漏洞上傳惡意檔案並執行任意程式碼。

- Google Chrome、Microsoft Edge、Vivaldi及Brave等以Chromium為基礎之瀏覽器存在10個高風險安全漏洞(CVE-2026-3536[8]、CVE-2026-3537[9]、CVE-2026-3538[10]、CVE-2026-3539[11]、CVE-2026-3540[12]、CVE-2026-3541[13]、CVE-2026-3542[14]、CVE-2026-3543[15]、CVE-2026-3544[16]及CVE-2026-3545[17])，類型包含整數溢位(Integer Overflow)、越界寫入(Out-of-bounds Write)及沙箱逃逸(Sandbox Escape)等，攻擊者可透過特製HTML網頁或擴充程式存取記憶體或執行任意程式碼。

- 葳橋資訊開發之單一簽入暨電子目錄服務系統存在高風險安全漏洞(CVE-2026-3826[18])，類型為本機檔案包含(Local File Inclusion)，未經身分鑑別之遠端攻擊者可利用此漏洞於伺服器端執行任意程式碼。

- Cisco Secure Firewall Management Center (FMC)存在2個高風險安全漏洞(CVE-2026-20079[19]與CVE-2026-20131[20])，類型分別為身分鑑別繞過(Authentication Bypass)與不安全之反序列化(Insecure Deserialization)，前者可使未經身分鑑別之遠端攻擊者透過發送特製HTTP請求繞過驗證機制，並執行任意腳本以取得底層作業系統之root權限；後者可使未經身分鑑別之遠端攻擊者透過發送特製序列化Java物件，於受影響設備以root權限執行任意程式碼。

- Broadcom VMware存在2個高風險安全漏洞(CVE-2026-22719[21]與CVE-2026-22720[22])，類型分別為指令注入(Command Injection)與儲存型跨網站腳本攻擊(Stored Cross-Site Scripting)，前者於Aria Operations支援協助產品遷移(Support-assisted product migration)流程中，可使未經身分鑑別之遠端攻擊者利用此漏洞於受影響設備執行任意指令，此漏洞已遭駭客利用；後者可使具建立自訂評估標準(Custom benchmark)權限之遠端攻擊者注入惡意腳本，進而以管理者權限執行系統操作。

1. https://nvd.nist.gov/vuln/detail/CVE-2025-5777
2. https://nvd.nist.gov/vuln/detail/cve-2023-20198
3. https://nvd.nist.gov/vuln/detail/cve-2024-36401
4. https://nvd.nist.gov/vuln/detail/cve-2024-4577
5. https://nvd.nist.gov/vuln/detail/cve-2024-1709
6. https://www.zerodayinitiative.com/advisories/ZDI-26-136/
7. https://www.zerodayinitiative.com/advisories/ZDI-26-137/
8. https://nvd.nist.gov/vuln/detail/CVE-2026-3536
9. https://nvd.nist.gov/vuln/detail/CVE-2026-3537
10. https://nvd.nist.gov/vuln/detail/CVE-2026-3538
11. https://nvd.nist.gov/vuln/detail/CVE-2026-3539
12. https://nvd.nist.gov/vuln/detail/CVE-2026-3540
13. https://nvd.nist.gov/vuln/detail/CVE-2026-3541
14. https://nvd.nist.gov/vuln/detail/CVE-2026-3542
15. https://nvd.nist.gov/vuln/detail/CVE-2026-3543
16. https://nvd.nist.gov/vuln/detail/CVE-2026-3544
17. https://nvd.nist.gov/vuln/detail/CVE-2026-3545
18. https://nvd.nist.gov/vuln/detail/CVE-2026-3826
19. https://nvd.nist.gov/vuln/detail/CVE-2026-20079
20. https://nvd.nist.gov/vuln/detail/CVE-2026-20131
21. https://nvd.nist.gov/vuln/detail/CVE-2026-22719
22. https://nvd.nist.gov/vuln/detail/CVE-2026-22720

■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

EASM曝險週增12% 未部署WAF與CSP設定不當增幅最大

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9,839項，詳見圖5。其中「元件高風險漏洞」以3,779項居首，「過時或弱加密協定」2,318項次之，「TLS憑證不受信任」1,853項位居第三，三項合計占比約81%，顯示漏洞修補與加密通訊管理仍為當前主要資安挑戰。

相較於上週的8,810項，整體風險數量增加1,029項，增幅約12%，反映外部曝險情勢依然嚴峻。在重大風險變化方面，「元件高風險漏洞」從3,762項微幅增加至3,779項，「TLS憑證不受信任」從1,460項大幅增加至1,853項，增幅達27%，「過時或弱加密協定」從2,080項增加至2,318項，增幅達11%，均呈現惡化趨勢。此外，「CSP設定不當」從591項增加至829項，增幅達40%，「未部署WAF」從367項增加至558項，增幅達52%，顯示網站安全防護措施仍有待加強。

防護建議	
建議機關或關鍵基礎設施採取下列防護措施	建議機關或關鍵基礎設施採取下列管理措施
➢ 定期更新憑證，全面啟用TLS 1.2以上版本協定，停用未加密或舊版協定 ➢ 儘速修補已知漏洞，淘汰無維護之軟體版本 ➢ 部署網站應用程式防火牆(WAF)並導入內容安全政策(CSP)等網站安全標頭，以降低XSS攻擊與惡意存取風險 ➢ 關閉不必要之對外服務，若需遠端管理服務應嚴格限制來源IP並改採加密通道(如SSH)	➢ 定期盤點並更換外洩帳號憑證，搭配多因素驗證(MFA)以強化存取安全 ➢ 建立弱點修補與驗證流程，確保風險持續改善 ➢ 強化資安教育訓練，提升系統維運人員對於憑證管理、加密配置與服務設定的安全意識

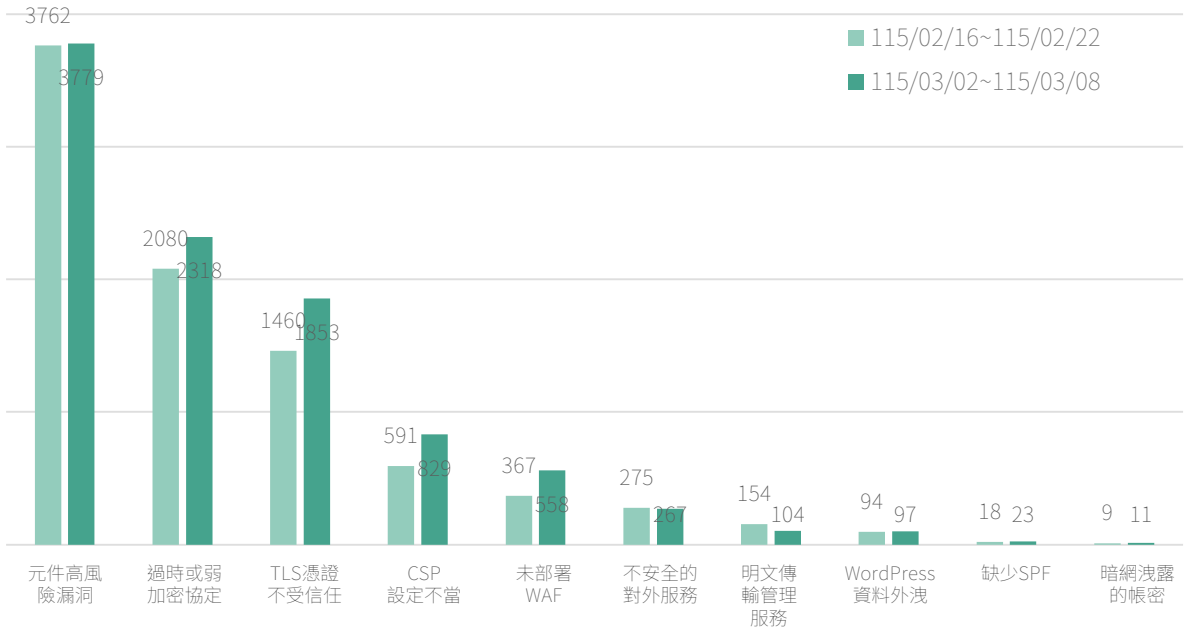


圖5| EASM檢測結果統計(前10大風險)

■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

本期高風險內容仍以產品服務為主 請持續留意假商品、假客服與生活化包裝手法

整體觀察本期高風險詐騙內容，風險樣態仍集中在與日常生活高度相關的消費、交易與客服互動情境，顯示詐騙訊息持續朝向生活化、日常化的方向包裝，容易讓民眾在看似一般促銷、商品推薦或服務通知的情況下放下戒心，詳見圖6。提醒民眾，面對各式網購、客服與優惠資訊，仍應落實「先查證、再互動、再交易」原則，避免因一時疏忽而受害。

從詐騙類型來看，「產品服務」仍為主要風險來源。本期相關內容多與商品銷售、促銷廣告、居家用品、保健美容及日常消費情境有關，且常見以熱銷商品、實用好物、健康保養、車用配件等題材包裝，再搭配「台灣出貨」「客服在線」「售後服務」「限時優惠」「名額有限」「推薦使用」等話術，營造可信度與急迫感，進一步誘導民眾點擊連結、私訊下單或改以站外方式交易。此類內容外觀往往與一般商業廣告相似，辨識不易，仍須提高警覺。

「身分冒充」亦為本期持續可見的重要風險類型。從內容樣態觀察，不少詐騙訊息會結合購物、出貨、售後、退款、交易確認等互動情境，假冒客服、賣家、售後人員或相關通知窗口，藉此延續接觸流程，進一步要求提供個人資料、驗證碼、帳戶資訊，或引導民眾進入不明頁面完成操作。提醒民眾，凡遇主動聯繫要求處理退款、補件、驗證、重新付款或解除設定等情形，務必先中止互動，再改由官方 App、官網或正式客服管道查證。

「金融投資」雖非本期最主要的風險焦點，但仍屬高損失風險類型，不能掉以輕心。此類詐騙常以投資理財、快速獲利、專人帶單、名人背書、群組邀請等方式吸引民眾加入，再透過看似專業的說明、獲利展示或話術包裝，誘導入金或持續投入資金。即使本期整體焦點較偏向商品與生活消費情境，對於任何宣稱穩賺不賠、保證收益、快速回本的投資訊息，仍應保持高度警覺。

綜整而言，本期高風險詐騙內容仍以「產品服務」為主，且多以貼近日常生活的商品銷售與消費情境進行包裝；「身分冒充」則常透過假客服、假賣家、假售後等名義延伸詐騙流程；「金融投資」雖非本期主軸，但仍屬高損失風險類型，後續仍需持續加強宣導與防範。整體而言，值得特別留意的是，詐騙內容持續以「看似正常、實則誘導」的方式降低民眾戒心，尤其在商品促銷、客服協助與生活化廣告包裝方面，更具迷惑性。

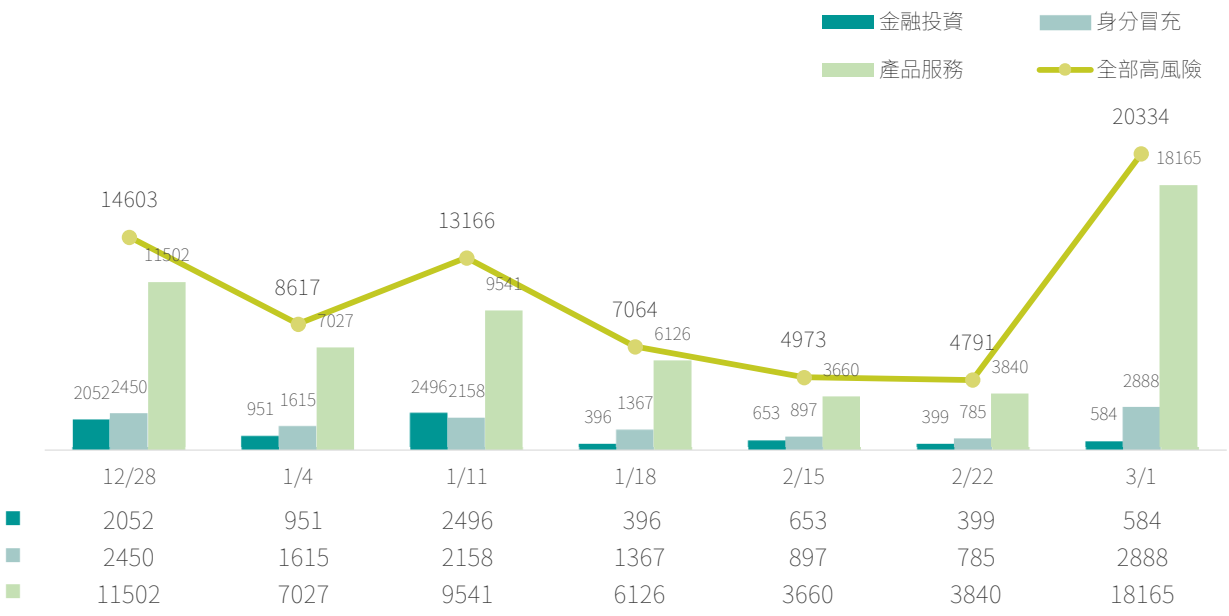


圖6 | 偵獲高風險金融投資、身分冒充、產品服務類詐騙週趨勢

高風險詐騙偵測趨勢分析與提醒

提升商品廣告與促銷訊息警覺

- ✓ 面對「產品服務」相關內容，凡出現「限時優惠、限量名額、台灣出貨、售後無憂、推薦使用、快速見效」等強化信任與催促交易的字眼，請先停下查證，不要因文案看似完整就直接下單。
- ✓ 對要求私訊下單、站外交易、點擊不明連結、改以其他通訊軟體聯繫者，應提高警覺；交易資訊請回到官方 App、官網或具保障的正式平台確認。
- ✓ 對於宣稱效果過強、保證見效、過度強調使用見證或誇大話術的廣告，尤其是保健、美容、修復、居家清潔與車用品類內容，請特別留意其真實性與付款安全。

強化客服與賣家身分查證

- ✓ 若對方自稱客服、賣家、售後人員、物流或付款協助窗口，並要求重新付款、提供驗證碼、確認帳戶、操作 ATM 或點擊補件連結，均屬高風險警訊，請立即中止互動。
- ✓ 接獲與購物、出貨、退款、取消訂單有關的通知時，請不要直接回覆訊息中的連結或電話，應改由官方網站、官方 App 或平台公開客服資訊自行查詢。
- ✓ 對「客服全天在線」、「售後無憂」、「可私訊快速處理」等說法應保持警覺，因這類話術容易被用來降低戒心並延伸詐騙流程。

持續防範高損失型金融投資詐騙

- ✓ 對於任何投資社群、帶單老師、保證獲利、穩賺不賠或快速回本等訊息，均應維持高警覺，不宜因題材表面變化而降低防備。
- ✓ 對於以貸款、補助、福利、快速審核、免費諮詢等名義要求先提供個資、帳戶資料或先行匯款者，務必多方查證，避免落入金融型詐騙。
- ✓ 凡涉及資金操作、入金投資或帳戶驗證，請務必確認對方身分與合法性，不要輕信片面資訊或截圖佐證。

善用官方資訊與檢舉機制

- ✓ 遇到疑似詐騙內容，請立即通報 165 反詐騙專線或平台客服，並保留廣告畫面、對話紀錄、連結、帳號與匯款資訊等證據。
- ✓ 建議持續關注政府、金融機構與平台公告的最新詐騙手法，特別留意「假購物、假客服、假投資」彼此串接的常見樣態。
- ✓ 建議平台與相關單位持續加強對「私訊下單、不明連結、假客服售後、誇大效果、促銷包裝」等高風險樣態的偵測與攔阻。

本週代表性詐騙關鍵字 Top 10 以「設計」、「推薦」、「必備」等字眼最常出現，另外也常搭配「配方」、「台灣」、「安心」、「優惠」、「神器」、「健康」、「舒適」等用語。這顯示詐騙訊息很常假裝成一般商品廣告，利用「看起來很好用」、「很多人推薦」、「生活一定要有」這類說法，吸引民眾點擊或下單。常見情況像是宣稱商品有特別設計、效果很好、家裡一定用得到，或是打出推薦款、熱銷款、優惠價等字樣，讓人覺得很划算、很值得買，進一步就可能把人導到不明網站、假購物頁面，甚至要求填寫個資或直接付款。

本週也常看到以「設計」、「必備」、「神器」、「舒適」包裝的商品宣傳，例如標榜「貼心設計」、「居家必備」、「超實用神器」、「使用更舒適」等，讓民眾覺得這些商品真的能改善生活、買了就很方便。這類貼文常會再加上「操作簡單」、「人人都適用」、「限時優惠」、「現在下單更划算」等話術，讓人更容易一時衝動購買。提醒民眾，遇到這類過度強調功能、效果或方便性的廣告內容時，務必要先確認賣家是否可信，不要只看貼文內容或留言推薦就直接下單。

另外，從「推薦」、「配方」、「健康」等關鍵字來看，本週也出現不少假借專業形象或健康訴求的詐騙內容。這類訊息常會說商品是「專家推薦」、「精心研製」、「特殊配方」、「有助健康」，甚至搭配見證分享、前後對比照，讓人誤以為產品真的有效。實際上，這種手法常是利用民眾對健康、保養或身體不適的焦慮來吸引購買，後續可能導向來路不明的網站，或要求留下聯絡資料、付款資訊。提醒民眾，凡是宣稱效果太神奇、見效太快，或強調「用過都說有效」的商品，都要特別小心，不要因為廣告話術就輕易相信。

此外，本週常見的詐騙宣傳也會使用「台灣」、「安心」、「優惠」等字眼，營造可信、安全的感覺。例如標榜「台灣出貨」、「在地服務」、「安心購買」、「限時優惠」等，讓民眾覺得賣家可靠、交易有保障。但這些字眼也可能只是詐騙集團用來包裝假賣場、假客服或假付款頁面的手法，後續可能造成信用卡資料外洩、被重複扣款，甚至付款後根本收不到商品。提醒民眾，不要因為看到「台灣出貨」或「安心購買」就掉以輕心，還是要先查證網站、商家資訊和付款方式是否安全。

另從整體話術來看，詐騙訊息也很常用「必備」、「神器」、「健康」、「舒適」這些字眼，讓商品看起來不只是便宜，而是「現在就該買」、「買了生活會更好」。再搭配「熱

銷」、「大家都在買」、「錯過可惜」等說法，容易讓民眾在沒有多想的情況下就快速做決。提醒民眾，只要看到廣告一直強調效果很好、現在最便宜、現在就要下單，就應該先停下來查證，不要急著點連結、留資料或付款。

綜合本週觀察，常見詐騙手法多半是先用「設計」、「推薦」、「必備」等吸睛字眼吸引注意，再用「配方」、「健康」提升可信度，接著以「台灣」、「安心」、「優惠」降低戒心，最後把民眾引導到站外頁面、假賣場或不明付款流程。

提醒民眾，只要遇到要求點擊不明連結、填寫個資、提供信用卡資料，或先付款才能享有優惠的情況，都應提高警覺、先停下來查證。建議優先透過官方網站、公開客服或可信賴的購物平台確認真偽，避免落入詐騙陷阱。

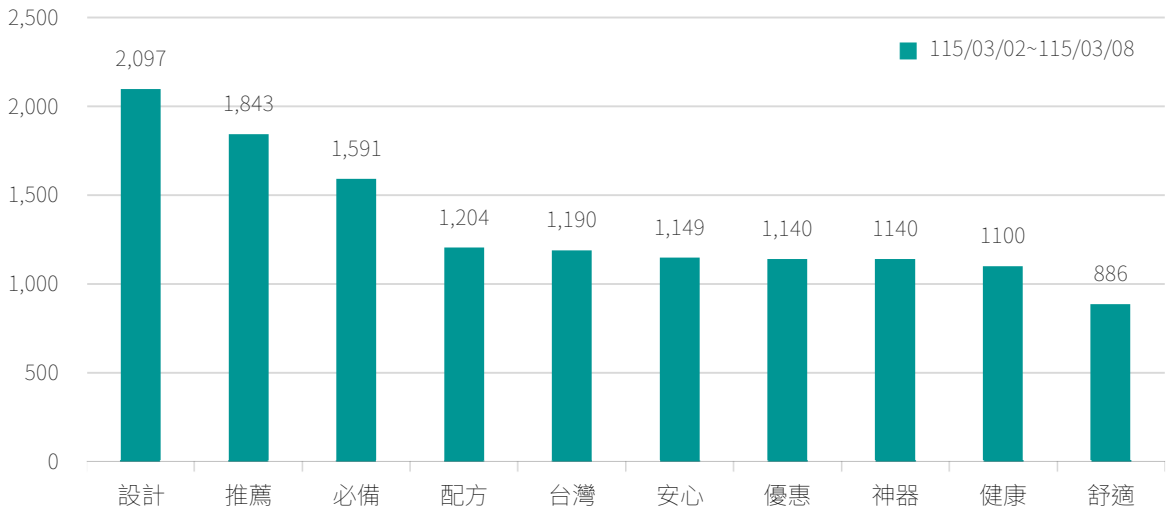


圖7 | 本週代表性詐騙關鍵字 Top 10

焦點文章

隱私強化技術與應用—資料時代下安全釋放資料價值的全新路徑

一 緒論

在人工智慧與大數據技術加速演進的全球浪潮下，公部門、研究機構乃至私人企業對資料應用的需求與日俱增，資料已成為當代最具戰略價值的核心資源之一。人工智慧系統的開發與優化高度仰賴海量資料的驅動，資料的規模與多樣性直接決定模型的效能上限；然而，如何在推動資料創新應用的同時兼顧個人隱私保護，始終是這場技術躍進中難以迴避的核心議題。於合規前提下有效運用個人資料(以下簡稱個資)，確保隱私不受侵害，安全實踐資料去識別化處理與流程，為隱私強化技術(Privacy-Enhancing Technologies, PETs)發展目標。

二 去識別化核心概念

(一) 法遵合規需求

我國參酌歐盟《一般資料保護規則》(GDPR)相關規範，修訂《個人資料保護法》(下稱個資法)[1]，就個人資料的蒐集、處理及利用建立完整規範架構，旨在防範人格權遭受侵害，同時促進個人資料的合理流通與應用。依個資法第 2 條第一款，個人資料係指涵蓋一切能與特定個人建立連結的多元形式資訊。個資法亦明定公務機關於蒐集、處理及利用個資時，除須明確告知當事人資料蒐集標的與使用目的外，應採行適當的去識別化措施，切斷資料與特定個人之關聯，並遵循相關法規的稽核要求。尤其，公務機關若欲基於業務需要將機敏資料另作統計分析或學術研究，依個資法第 16 條目的外利用規定，其第五款明確要求資料須經處理至「無從識別特定當事人」，方得應用於上述用途。

(二) 去識別化目標與技術層次

為達上述「無從識別特定當事人」之要求，去識別化旨在透過明確目的導向的資料處理，在保留資料分析效用的同時，最大程度降低資料與特定個人之間的可連結性[2]。實務上，去識別化技術依其保護強度，大致可區分為假名化與匿名化兩大類別，假名化(pseudonymization)係將個人機敏資料以替代識別符號取代，雖能降低資料與真實個體直接連結，但仍存在透過串接其他資料集而間接還原個人身份的可能性。

焦點文章

匿名化(anonymization)則進一步破壞或移除資料中足以辨識真實個體的資訊，使資料在理論與實務上均無從回溯至特定當事人。

(三) 重新識別風險

值得注意的是，假名化在法規定義上並不等同於匿名化，即便已採行去識別化處理，資料仍可能因外部資訊的串接而遭到重新識別，因此法規要求應竭盡所能降低此類風險，方能達到匿名化的法遵效力。為系統性量化去識別化後資料的重新識別風險，實務上可採用 Anonymeter 工具，依據歐盟匿名化技術評估標準，從三個核心面向進行保護力評估[3]：

1. 指認性(singling out)：資料集是否存在足以唯一鎖定特定個體的欄位組合
2. 連結性 (linkability)：是否能跨資料集串接並歸因至同一當事人
3. 推斷性(inference)：是否能由現有欄位推導出當事人未揭露的隱藏資訊

三 隱私強化技術 (PETs)

(一) 技術範疇與核心理念

若說去識別化概念奠定了個資保護的法遵基礎，PETs 則將這一基礎進一步延伸，構築出更全面的資料保護框架。PETs 泛指一系列旨在保護個人隱私的技術集合，其核心價值不僅在於防範資料洩漏，更在於使跨機構資料分析成為可能，將資料最小化原則的效益發揮至最大[4]。

聯合國對 PETs 的定義[5]，精準揭示了其三大核心特質：資料最小化使用(僅處理達成目的所必要的最少量資料)、最大化資料安全(在整個資料生命週期中維持高強度保護)、以及個人資料賦權(還原當事人對自身資料的自主掌控能力)。這三項特質共同構成 PETs 有別於傳統去識別化技術的關鍵優勢，不僅消極地「降低風險」，更積極地「創造安全流通的條件」[6]。

(二) 資料生命週期的多重防護

資料從蒐集、處理到結果發布，貫穿完整的生命週期，隱私風險亦隨之在不同節點以不同形式浮現。PETs 依據保護介入的時機，將隱私保護需求區分為輸入隱私與輸出隱私兩大

焦點文章

類別，分別對應資料生命週期的上下游，形成首尾呼應的雙重防護機制。

輸入隱私(input privacy)強調「資料可用但不可見」，目的是確保個人原始資料在參與運算的過程中，不會以任何形式暴露於非授權方，使資料的分析價值得以實現，而原始內容始終受到屏障。輸出隱私(output privacy)則聚焦於資料生命週期的末端，著重於實踐「結果可用但不可逆推」，即便分析結果對外發布，非預期使用者亦無法從中反推出原始機敏資訊，防止資料價值的釋放成為隱私洩漏的缺口。

(三) PETs 綜合比較

本節將四個常用 PETs 特點、適用場景與優缺點整理、比較如表2，各 PETs 因應不同資料特性、資料分析與隱私需求而有不同特性。

表2 | PETs綜合比較表

	輸入隱私			輸出隱私	
聯合學習[7]	技術特點	僅交換模型參數，無需共享原始資料	差分隱私[8]	技術特點	查詢結果中加入隨機雜訊，無法識別單一紀錄
	適用場景	跨機構協作、邊緣設備學習		適用場景	政府數據統計、欲公開資料統計分析
	優點	共享模型、可使用較大量資料集進行訓練		優點	實作方法簡單、隱私保護強度有數學保證
	缺點	傳輸過程有被竊聽、攻擊、竄改數據風險		缺點	仍未有明確方式擇定隱私預算大小
同態加密[9]	技術特點	直接於密文上計算，原始資料始終保持加密狀態	合成資料[10]	技術特點	統計特性與真實資料相似但不包含真實紀錄的人工資料
	適用場景	雲端敏感資料計算、外包分析		適用場景	軟體測試、機器學習訓練
	優點	高隱私保護		優點	使用彈性大、應用場景廣
	缺點	運算複雜度高		缺點	生成資料可能忽略真實資料一些特徵

焦點文章

四 PETs 的實證部署與應用推展

(一)標準化工具套件的建構

開發 PETsARD(Privacy Enhancing Technologies Analysis, Research, and Development，/pəˈtard/)程式套件[11]，針對合成資料的產製與評估流程提供端對端的自動化支援，將原本高度仰賴人工判斷的技術流程，轉化為可重複、可驗證的標準化作業。

(二) 代表性實證場域

- 政府統計資料的合成資料轉型：內政部統計處案例

  內政部統計處長期以模擬方式釋出「人口、建物與地利資訊模擬資料」，提供產官學界作為分析基礎[12]。然而，現行演算法高度依賴個案客製化設計，難以快速擴展至其他泛用目的，形成業務瓶頸。本團隊以合成資料技術重塑人房地資料模擬資料產製流程，基於領域知識與分層合成策略，並導入標準化資料品質評測機制。

- 跨機構聯合學習的隱私保護實踐：新光人壽壽險理賠案例

  因應新光人壽偕同多家業者共同建立「壽險理賠樣態共享生態圈」的需求，本團隊從資料保護核心概念出發，於聯合學習的理賠防詐模型建構流程中導入合成資料，在不暴露各機構原始資料的前提下實現跨域模型協作。

五 結語

本文從法規制度與技術實作兩個層面，系統性梳理去識別化技術與 PETs 的核心概念、發展脈絡與實證應用。本院將持續深化 PETs 的研發能量與實證部署，致力在技術創新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。

焦點文章

參考文獻

1. 《個人資料保護法》，https://law.moj.gov.tw/LawClass/LawAll.aspx?PCode=I0050021。
2. 隱私強化技術應用指引，數位發展部 ，https://hackmd.io/@petworks/rJ-UOh9Rn。
3. Giomi, M., Boenisch, F., Wehmeyer, C., & Tasnádi, B. (2022). A unified framework for quantifying privacy risk in synthetic data. arXiv preprint arXiv:2211.10459.
4. ICO (2022), “Chapter 5: Privacy-enhancing technologies (PETs)”, Information Commissioner’s Office, London, https://ico.org.uk/media/about-the-ico/consultations/4021464/chapter-5-anonymisation-pets.pdf.
5. United Nations Committee of Experts on Big Data and Data Science for Official Statistics. (2023). The PET Guide. United Nations Publications.
6. 隱私強化技術：平衡資料保護與資料應用，數位發展部，https://moda.gov.tw/press/multimedia/blog/12810。
7. Konečný, J., McMahan, H. B., Yu, F. X., Richtárik, P., Suresh, A. T., & Bacon, D. (2016). Federated learning: Strategies for improving communication efficiency. arXiv preprint arXiv:1610.05492.
8. Near, J. P., & Abuah, C. (2021). Programming differential privacy. URL: https://uvm.
9. 隱私強化技術：平衡資料保護與資料應用，數位發展部，https://moda.gov.tw/press/multimedia/blog/12810。
10. The Synthetic Data Vault. https://docs.sdv.dev/sdv/single-table-data/modeling/synthesizers/gaussiancopulasynthesizer.
11. PETsARD GitHub repository. https://github.com/nics-tw/PETsARD.
12. 內政大數據模擬資料，https://segis.moi.gov.tw/STATCloud/BigData。

關鍵字：隱私強化技術、去識別化技術、個人資料保護

刊　　名　資安週報第 35 期
發 行 人　國家資通安全研究院　林盈達院長
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