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

資安週報

Cyber Security Weekly Newsletter

半年回顧特刊(2025.7-2026.1)

事件通報

當攻擊建立於被允許的行為上　傳統以漏洞為核心的防護將難以及時介入

聯防監控

政府聯防監控顯示攻擊行為持續聚焦入侵後控制　防禦迴避占比居各階段之首

蜜罐誘捕

Citrix NetScaler ADC與Cisco IOS XE網通設備作業系統成這半年內的攻擊熱點

外部曝險分析

半年期回顧：整體風險總量下降　惟憑證、加密與元件漏洞仍為長期主軸

網路巡查高風險詐騙

春節近半年防詐騙回顧特輯

焦點文章

CODE 2025醫療OT場域設計成果

2026.02.19
032

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

近半年非法入侵事件發生原因統計與分析，同時市場產業別公告次數統計

當攻擊建立於被允許的行為上　傳統以漏洞為核心的防護將難以及時介入

透過近半年非法入侵事件發生原因統計，可發現「使用/下載來源不明之應用程式或套件、弱密碼/密碼遭暴力破解、社交工程」等可歸因於使用者行為之因素，合計占比約70.5%，詳見圖1。此一結果顯示，多數事件並非源自重大系統漏洞或高深攻擊技術，而是發生於「看似正常」的日常操作情境，異常狀況多半直到端點出現對外異常連線後，才被監控機制所偵測與揭露。

此類事件並非單純的偶發性人為疏失，而是攻擊者刻意將初始存取(Initial Access)隱藏於日常工作流程中，使合理且被允許的操作轉化為可被穩定利用的入侵路徑，進而形成可在機關內部持續複製、反覆發生的結構性風險。然而，部分事件於後續處置時，僅止於受駭設備的重建或隔離，未同步檢視帳號、憑證與權限是否可能外洩，致使攻擊者仍可能利用既有身分再次進入系統。

面對此一趨勢，資安治理重點應由事後應變前移至風險成形前的管理。除系統防護與權限管控外，更應將下載、附件、外部網站、可攜式媒體與遠端存取等高風險使用情境納入控管，使日常必要行為在被允許的同時，維持可控與可追溯；並將防護視角由對外連線偵測前移至端點行為觀測，掌握程序執行與檔案行為脈絡，於異常連線發生前即介入處置。對已偵測的異常連線，亦應預設具有身分與存取風險，切斷再次入侵能力納入結案條件，以避免風險反覆發生。

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

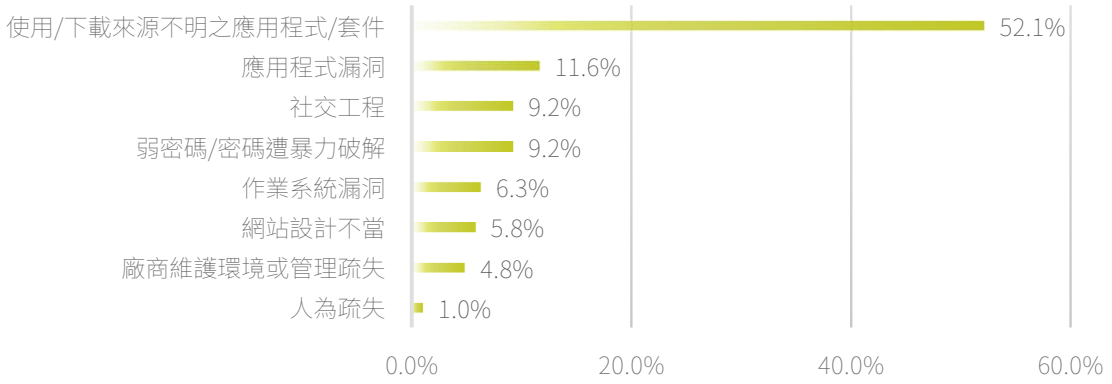

圖1 |近半年非法入侵事件可識別事件發生原因占比

依市場產業別公告次數統計，近半年資安事件重訊通報以通信網路業及生技醫療業占比最高(各16.1%)，為主要受影響對象，詳見圖2。整體而言，資安風險不再集中於特定產業，建議各產業持續強化端點防護、帳號存取管理及供應鏈與委外控管，以降低事件發生與擴散風險。

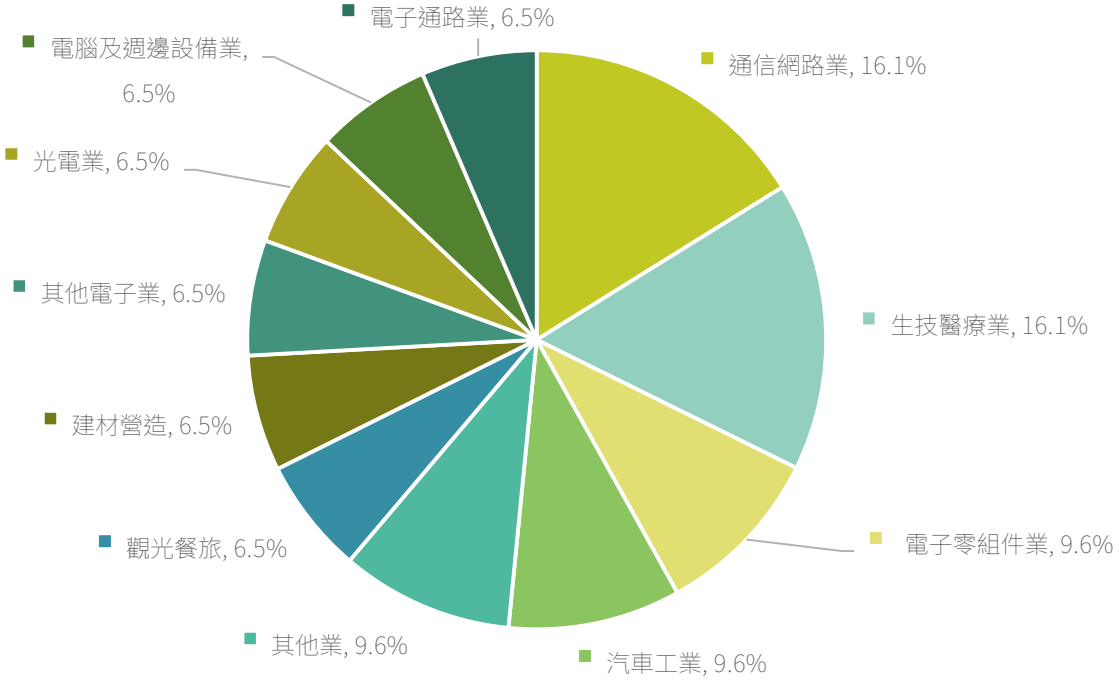

圖2 |近半年資安事件重訊通報市場產業別占比

■聯防監控

近半年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

政府聯防監控顯示攻擊行為持續聚焦入侵後控制　防禦迴避占比居各階段之首

本期(2025年7月至2026年1月)政府資安聯防監控事件依 MITRE ATT&CK 戰術架構統計，整體趨勢顯示攻擊行為明顯集中於入侵後之控制與隱匿階段，各階段分布詳見圖3；其中防禦迴避為占比最高之攻擊階段，約占整體事件的15.8%，顯示攻擊者在取得初步存取後，持續透過削弱或規避稽核機制、清除命令歷程及採用間接執行方式，以降低被偵測風險並延長在受害環境中的存續時間；其次為偵測刺探(11.7%)與惡意執行(11.2%)，反映攻擊活動同時涵蓋入侵前之系統性偵蒐行為與入侵後之實際操作行為，前者多見於網段掃描及DNS相關情資蒐集，顯示對外部資產曝露面的持續探測，後者則大量濫用Visual Basic、PowerShell 與 Python 等腳本語言，作為執行指令與操控系統的主要手段。初始入侵階段占比約為9.5%，仍以對外服務弱點利用、預設帳號及供應鏈相關風險為主要途徑，而攻擊整備階段亦占9.1%，顯示攻擊者在實際入侵前，已具備可規模化之攻擊資源與基礎設施。

整體而言，惡意執行、維續存取、權限提升、防禦迴避與憑證竊取等入侵後相關階段合計占比已接近整體事件的一半，顯示威脅型態已由單純突破防線，轉為著重於隱匿性、持續性與橫向操作能力，建議防禦策略除持續強化對外服務、帳號與弱點治理外，應進一步提升命令與腳本執行行為之可視性與稽核完整性，並針對防禦迴避、間接執行及憑證濫用等高風險行為建立具關聯性的偵測與應處機制，以強化對入侵後活動的整體掌握能力。

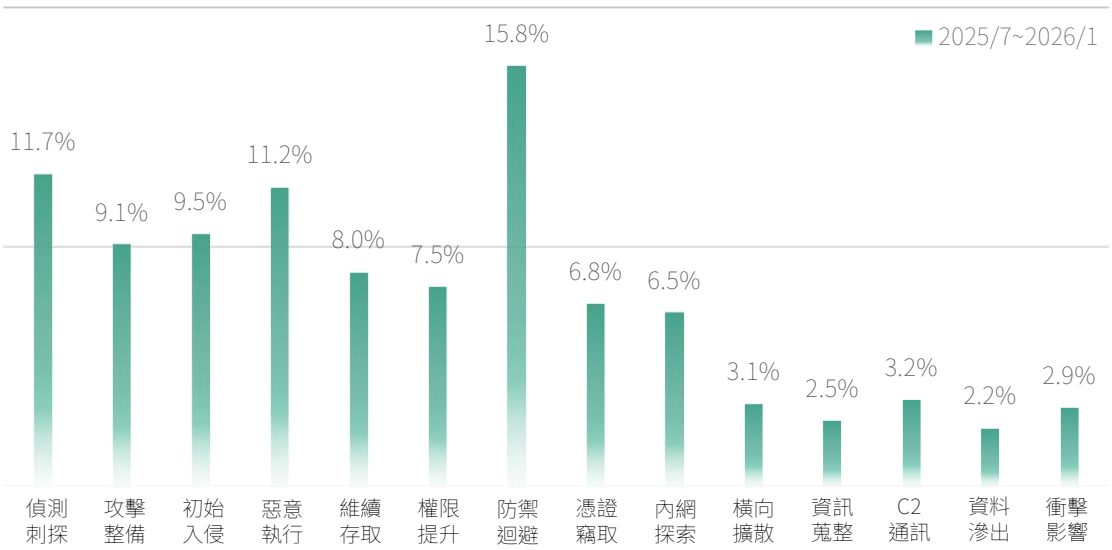

圖3 | 資安聯防監控攻擊階段統計

■蜜罐誘捕

近半年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這半年內的攻擊熱點

於2025/07/07至2026/01/25之半年內透過部署於國內外之蜜罐系統觀測攻擊行為動態，各類服務之平均偵測攻擊比例結果顯示「網頁應用」服務為攻擊主軸，占比高達83.25%。「遠端控制」服務亦有14.39%的誘捕比例，反映攻擊者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。近半年網頁應用介面之誘捕狀況，詳見圖4。近半年通用型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。

另外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。

而近半年Web服務系統數量最高的漏洞為微軟開放管理基礎架構 (OMI) 遠端執行程式碼的CVE-2021-38647漏洞。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。而近半年通設備管理介面數量最高的漏洞為Citrix NetScaler ADC 越界讀取的CVE-2025-5777漏洞。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。

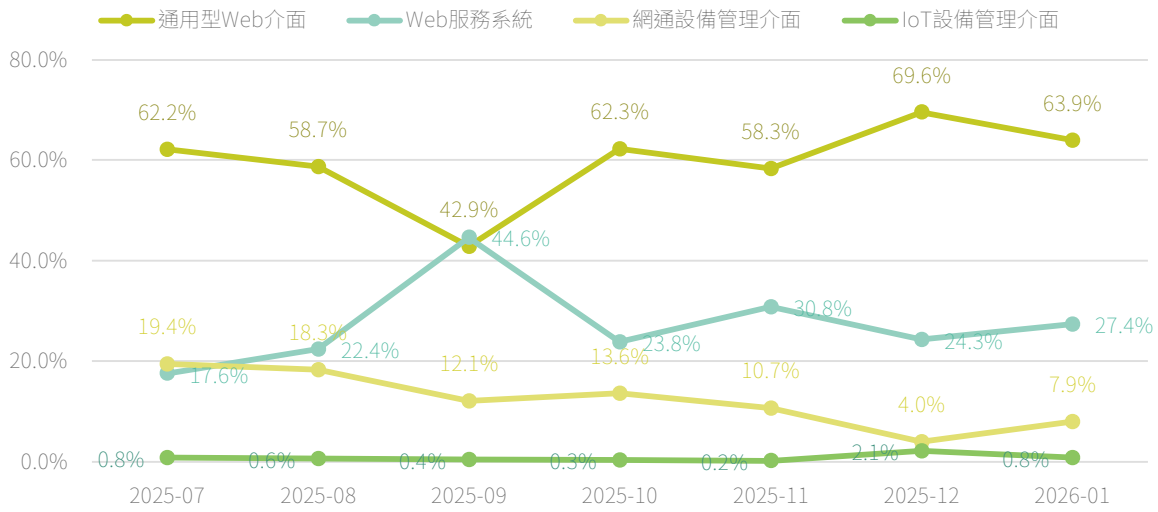

圖4 |半年內網頁應用介面之誘捕攻擊比例趨勢統計

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15大攻擊以「網頁應用」服務之漏洞為主要入侵路徑，近半年內漏洞類型多集中於越界讀取漏洞、特權提升、遠端程式碼執行漏洞、程式碼注入、身分驗證繞過漏洞、存取控制破壞漏洞、目錄遍歷漏洞及作業系統命令注入漏洞，攻擊目標涵蓋Citrix NetScaler ADC、Cisco IOS XE網通設備作業系統、Apache Solr企業搜尋平台、GeoServer開放源碼伺服器、JetBrains TeamCity 持續整合/交付平台、Atlassian Confluence Data Center and Server、Check Point VPN Gateway、Palo Alto Networks PAN-OS作業系統、PHP、Ivanti資安軟體、TKB的DVR設備、Fortra GoAnywhere MFT、Zyxel NAS326及JetBrains TeamCity 持續整合/交付平台，顯示此類系統已成為高風險熱點。

表1 |半年內前15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	漏洞類型	CVSS 3.x Base Score
1	CVE-2025-5777[1]	Citrix NetScaler ADC	越界讀取漏洞	7.5
2	CVE-2023-20198[2]	Cisco IOS XE網通設備作業系統	特權提升	10.0
3	CVE-2023-50386[3]	Apache Solr企業搜尋平台	遠端程式碼執行漏洞	8.8
4	CVE-2024-36401[4]	GeoServer開放源碼伺服器	程式碼注入	9.8
5	CVE-2023-42793[5]	JetBrains TeamCity 持續整合/交付平台	身分驗證繞過漏洞	9.8
6	CVE-2023-22515[6]	Atlassian Confluence Data Center and Server	存取控制破壞漏洞	9.8
7	CVE-2024-21683[7]	Atlassian Confluence Server	遠端程式碼執行漏洞	8.8
8	CVE-2024-24919[8]	Check Point VPN Gateway	目錄遍歷漏洞	8.6
9	CVE-2025-0108[9]	Palo Alto Networks PAN-OS作業系統	身分驗證繞過漏洞	9.1
10	CVE-2024-4577[10]	PHP	遠端程式碼執行漏洞	9.8

表1 |半年內前15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	漏洞類型	CVSS 3.x Base Score
11	CVE-2024-21887[11]	Ivanti資安軟體	遠端程式碼執行漏洞	9.1
12	CVE-2024-3721[12]	TKB的DVR設備	作業系統命令注入漏洞	6.3
13	CVE-2023-0669[13]	Fortra GoAnywhere MFT	遠端程式碼執行漏洞	7.2
14	CVE-2024-29973[14]	Zyxel NAS326	作業系統命令注入漏洞	9.8
15	CVE-2024-27198[15]	JetBrains TeamCity 持續整合/交付平台	遠端程式碼執行漏洞	9.1

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。

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-2023-50386
4. https://nvd.nist.gov/vuln/detail/CVE-2024-36401
5. https://nvd.nist.gov/vuln/detail/CVE-2023-42793
6. https://nvd.nist.gov/vuln/detail/CVE-2023-22515
7. https://nvd.nist.gov/vuln/detail/CVE-2024-21683
8. https://nvd.nist.gov/vuln/detail/CVE-2024-24919
9. https://nvd.nist.gov/vuln/detail/CVE-2025-0108
10. https://nvd.nist.gov/vuln/detail/CVE-2024-4577
11. https://nvd.nist.gov/vuln/detail/CVE-2024-21887
12. https://nvd.nist.gov/vuln/detail/CVE-2024-3721
13. https://nvd.nist.gov/vuln/detail/CVE-2023-0669
14. https://nvd.nist.gov/vuln/detail/CVE-2024-29973
15. https://nvd.nist.gov/vuln/detail/CVE-2024-27198

近半年重大弱點提醒

利用之「漏洞利用預測評分系統」(Exploit Prediction Scoring System, EPSS)為FIRST組織提出之項目，利用機器學習模型評估漏洞被利用之可能性，EPSS分數可視為漏洞被利用的機率(範圍為0至100%)，表示未來30天內可能會被利用的機率，因此根據評估時間不同，分數亦可能有所改變。

本院研究人員根據近半年發布之漏洞警訊，透過EPSS即時評分機制判斷各項漏洞於2月份遭受實際利用之可能性，針對機關常用、高風險及高利用率之漏洞整理詳見表2，建議組織內部進行檢查與修補。

表2 |近半年發布之漏洞警訊利用機率表

項次	CVE編號	受影響產品名稱	漏洞類型	CVSS3.1	利用機率
1	CVE-2025-53770[1]	Microsoft SharePoint Server	反序列化不受信任資料	9.8	91%
2	CVE-2025-64446[2]	Fortinet FortiWeb	相對路徑遍歷	9.8	90%
3	CVE-2017-6736[3]	Cisco IOS與IOS XE Software	緩衝區溢位	8.8	89%
4	CVE-2025-61882[4]	Oracle E-Business Suite	伺服器端請求偽造/CRLF注入/XSLT注入	9.8	87%
5	CVE-2025-57819[5]	Sangoma FreePBX	身分鑑別繞過	9.8	76%
6	CVE-2025-59287[6]	Windows Server Update Service (WSUS)	不安全之反序列化	9.8	71%
7	CVE-2025-25257[7]	Fortinet FortiWeb	SQL注入	9.8	66%
8	CVE-2025-33073[8]	Windows SMB	NTLM反射	8.8	54%
9	CVE-2025-57790[9]	Commvault	絕對路徑遍歷	8.8	50%
10	CVE-2025-58034[10]	Fortinet FortiWeb	作業系統指令注入	7.2	48%
11	CVE-2025-14733[11]	WatchGuard Fireware OS	越界寫入	9.8	41%
12	CVE-2025-25256[12]	Fortinet FortiSIEM	作業系統指令注入	9.8	40%

1. https://nvd.nist.gov/vuln/detail/CVE-2025-53770
2. https://nvd.nist.gov/vuln/detail/CVE-2025-64446
3. https://nvd.nist.gov/vuln/detail/CVE-2017-6736
4. https://nvd.nist.gov/vuln/detail/CVE-2025-61882
5. https://nvd.nist.gov/vuln/detail/CVE-2025-57819
6. https://nvd.nist.gov/vuln/detail/CVE-2025-59287
7. https://nvd.nist.gov/vuln/detail/CVE-2025-25257
8. https://nvd.nist.gov/vuln/detail/CVE-2025-33073
9. https://nvd.nist.gov/vuln/detail/CVE-2025-57790
10. https://nvd.nist.gov/vuln/detail/CVE-2025-58034
11. https://nvd.nist.gov/vuln/detail/CVE-2025-14733
12. https://nvd.nist.gov/vuln/detail/CVE-2025-25256

■外部曝險分析

經由近半年外部曝險檢測結果，分析公部門與關鍵基礎設施業者現況，及早發現曝露於外部之風險，並提出改善方向與防護建議

半年期回顧：整體風險總量下降　惟憑證、加密與元件漏洞仍為長期主軸

綜整114年7月至115年1月之EASM檢測結果，涵蓋公部門與關鍵基礎設施(CI)兩類受測對象。整體數據顯示，兩類對象在曝險量級上存在明顯差距：如表3所示，CI單位的平均風險項目數為2,042項，約為公部門405項的5倍，且最高曾出現單期3,283項之紀錄。此一差異反映 CI 因系統架構規模較大、對外服務範圍較廣，其外部攻擊面亦相對更為複雜，爰宜建立規模化之管理機制，並依標準作業流程推動風險管控與改善措施。

表3 |半年期 EASM 檢測結果統計總覽

受測單位類型	受測單位數量	風險項目平均數量	風險項目 最低數量/最高數量
公部門	43	405	225 / 676
關鍵基礎設施	46	2,042	1,203 / 3,283

就趨勢面而言，兩類對象在維持量級差距的同時，亦呈現同步下降之走勢。如圖5所示，CI單期「風險項目總數」介於1,203–3,283，並由早期高點逐月下降，至114/12–115/01已降至約1,200水準(依月份平均值彙整)。相對地，公部門單期風險總數多落於百級量體，並由376(114年8月)下降至310(115年1月)，顯示公部門在弱點處置與改善作業上已逐步累積成效。綜合而言，半年期趨勢可概括為「總量下降，但量級差距仍明顯」，後續仍需持續以制度化方式推動改善，俾利維持下降動能。

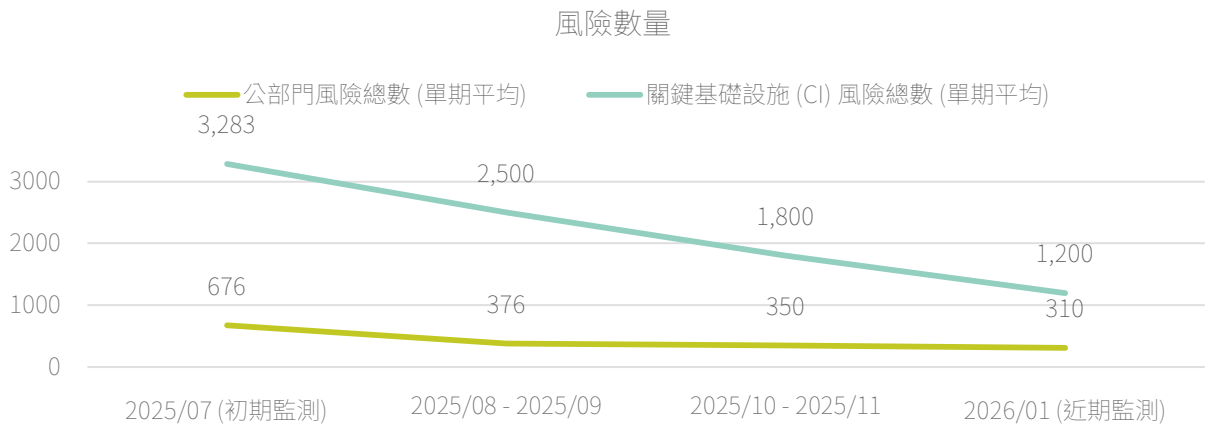

圖5|半年期 EASM 風險項目總數趨勢

雖整體量級呈下降趨勢，但風險結構仍高度集中於既有主軸。如圖6所示，公部門單期統計多以「TLS 憑證不受信任、過時或弱加密協定、CSP 設定不當、元件高風險漏洞」等類別為主要來源；CI 期末亦呈現相近型態，且主要類別集中度高，四項類別合計占比約90%。此一結果顯示，半年期主要改善重點並非風險類型快速變動，而係若干基礎性安全設定與常見弱點類型長期反覆出現，並集中於「憑證管理、加密協定設定、元件漏洞修補、網站基礎防護」四大面向。後續改善策略建議持續以此四類為優先辦理項目，以確保風險下降趨勢得以穩定延續。

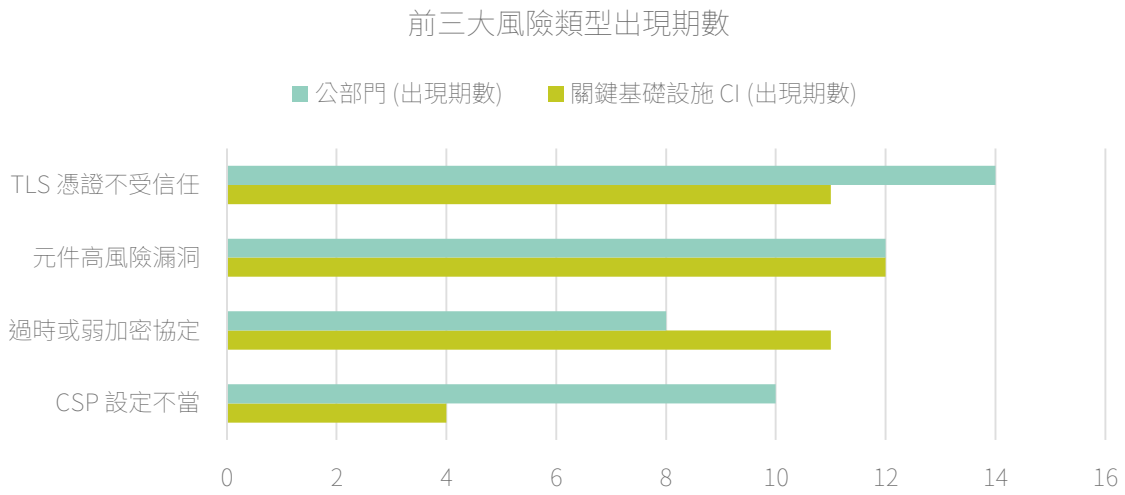

圖6|半年期EASM主要風險類型出現期數統計(前三大)

防護建議

- 建議機關或關鍵基礎設施採取下列防護措施：
  - 定期更新網站加密憑證，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 WAF 並導入 CSP 等網站安全標頭，降低跨站攻擊與惡意存取風險
  - 關閉不必要對外服務，管理服務改採加密通道(如 SSH)

- 建議機關或關鍵基礎設施採取下列管理措施：
  - 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
  - 強化資安教育與演練，提升人員對憑證、加密與服務設定之安全意識

■網路巡查高風險詐騙

分析近半年詐騙訊息與手法演變，於控制措施實施後，觀察各類詐騙變化趨勢

春節近半年防詐騙回顧特輯

守住荷包，過好年：免費不一定是福利，點擊常常是陷阱。

一 半年數據快照：量能高、波動大，年底最熱

- 期間：2025/07/07 ～ 2026/01/25(共 29 週 / 203 天)
- 近半年高風險總量：299,995(約 30 萬)
- 平均每天：約 1,478
- 平均每週：約 10,345
- 最高峰週：2025/11/03 ～ 11/09：23,232
- 低點週：2025/08/18 ～ 08/24：1,170
- 波動幅度：最高約為低點的 19.9 倍

12月最突出：單月占比約 24.9%，是近半年最高量能月份；顯示年末檔期(購物、促銷、活動、年終資金流)常被詐團「借勢放大」，詳見圖7。

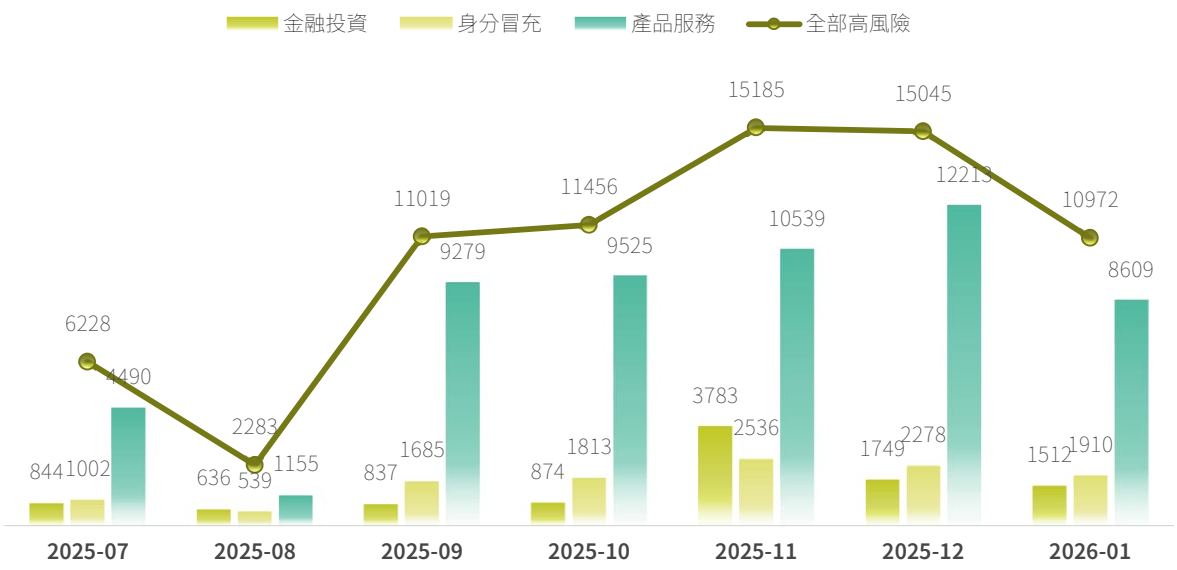

圖7 | 偵獲高風險金融投資、身分冒充、產品服務類詐騙趨勢

三 3 大風險主題：各有主場，但常「混搭」出手

- 產品服務：長期主力、12 月更旺
  - 近半年累計標記 230,444(相對總量的標記比約 76.8%)
  - 常見包裝：健康、必備、神器、課程、體驗、限量、名額
  - 常見套路：用「優惠/贈品/限時」逼你快決定，最後導去私訊、外部連結或不明網站付款
- 金融投資：10/27 ～ 11/09 兩週「集中爆量」
  - 2025/10/27 ～ 11/09 兩週合計高風險 42,957，其中金融投資標記 16,120
  - 這段期間關鍵字特徵很明顯：股票、投資、股市、高息、策略、資金，典型「假投資」在熱點期會加大投放，主打「名單、帶單、明牌、穩賺」
- 身分冒充：穩定高發，年末也同步升溫
  - 近半年累計標記 49,122
  - 常見冒充對象：客服、平台、人員、老師、機構(名稱會一直換)
  - 常見收割點：要求驗證碼、轉帳、解綁、補繳、解除設定，或引導下載不明 App

三 話術總榜：詐騙最愛用的「誘餌詞」Top 10

- 近半年關鍵字加總(出現次數最高)前 10 名如下，詳見表4：

表4 |前10大關鍵字

排名	關鍵字	次數	排名	關鍵字	次數
1	免費	24,857	6	點擊	11,818
2	加入	15,856	7	推薦	10,776
3	優惠	15,069	8	市場	9,983
4	立即	14,840	9	設計	9,731
5	領取	14,466	10	台灣	9,427

- 你可以把它想成一個「詐騙廣告的句型」：免費 / 優惠 / 領取(誘因) → 點擊 / 加入 / 立即(催促行動) → 私訊 / 轉帳 / 安裝 App(轉場收割)

四 3 個高峰週：用關鍵字看「當週主打法」

- 高峰 1：2025/11/03～11/09(總量 23,232)
  - 當週關鍵字：免費、股票、加入、領取、投資、推薦、市場
  - 解讀：典型假投資「免費名單」+「社群帶單」的組合拳，先降低戒心，再導入群組與操作
- 高峰 2：2025/10/27～11/02(總量 19,725)
  - 當週關鍵字：立即、加入、股票、資金、股市、高息、免費
  - 解讀：強催促(立即)+ 高報酬(高息)+ 投資關鍵詞，常見於「限時名額」式的投資群拉人
- 高峰 3：2025/12/22～12/28(總量 18,684)
  - 當週關鍵字：免費、機會、優惠、點擊、領取、推薦、設計、加入
  - 解讀：年末促銷檔期更容易被「優惠/免費」綁架判斷，詐團會把假活動、假折扣、假贈品包裝得更像真的

五 重點提醒：過年前後最需要守的 7 件事

- 投資類：「保證獲利」就是警訊
  - 任何「穩賺、翻倍、內線、明牌、帶你操作」都要先停下來
  - 不加陌生投資群、不信私訊報牌、不下載來路不明 App
- 冒充類：先掛電話，再查證
  - 對方只要催你「馬上處理」，九成是在搶你的判斷時間
  - 用官方管道回撥、回信、回到原本平台查，不要照對方提供的連結走
- 網購/活動類：「領取」之前先確認「你要付什麼」
  - 詐騙常把成本藏在後面：運費、稅金、保證金、手續費、解鎖費
  - 能走平台就走平台，避免私下轉帳與不明收款連結
- 借貸/資金類：先收費、先押金、先保證金＝高風險
  - 正規金融機構不會用「先付費才能撥款」當流程
- 任何類型：看到 「立即 / 限量 / 名額」，先冷靜 30 秒
  - 詐團最怕你冷靜，因為冷靜就會查證、會問人、會發現破綻
- 任何類型：不要交出 驗證碼 / 密碼 / 身分資料
  - 包含簡訊驗證碼、一次性密碼(One Time Password，OTP)、銀行/平台登入資訊

- 最後一道防線：有疑慮就打 165
  - 不確定就問，寧可多問一次，也不要多付一次學費(緊急狀況可同時聯繫 110)

六 給民眾的建議

- 近半年資料告訴我們：詐騙不一定看起來像詐騙。它常常穿著「免費、優惠、推薦、加入」的外衣，趁你最忙、最想省、最怕錯過的時候下手
- 今年過年，把「先查證、再行動」當作全家的共同默契：守住錢，也守住心安

焦點文章

CODE 2025醫療OT場域設計成果

以真實攻擊情境建構醫療OT風險樣貌，打造可驗證、可攻防之資安演練場域

CODE演練緣起與目的

行政院國家資通安全會報(National Information & Communication Security Taskforce, NICST)自2013年起，每兩年舉辦跨國網路攻防演練(Cyber Offensive and Defensive Exercise, CODE)以演練關鍵基礎設施之資安防護與應變能力，並自2019年之跨國網路攻防演練(CODE 2019)首次採實兵演練方式辦理，當年以金融領域為標的，並邀請國內外資安團隊共同參與演練，2021與2023年延續2019年執行方式，各自以能源與水資源領域作為標的。CODE 2025則將演練領域延伸至緊急救援與醫院領域，並新增情資分享與資安聯防，考驗醫療院所面對資安事件之應處能力。

結合國際威脅情資與國內資安事件經驗之攻擊情境設計

CODE 2025在攻擊情境設計上，除參考國際已知進階持續性威脅駭客組織APT41之行為模式，亦整合2025年初Crazy Hunter駭客組織鎖定我國醫療院所進行勒索軟體攻擊之脈絡與手法，並納入近年國內資安事件通報案例所揭露之攻擊型態與風險特徵，藉由「真實資安事件」、「實際攻擊路徑」及「常見弱點態樣」等三面向，建構貼近臺灣醫療環境所面臨之真實威脅樣貌，透過演練強化醫療院所發生攻擊事件時之通報、應變及情資分享能力。

醫療數位化浪潮之IT/OT整合風險挑戰

隨著醫療數位化與智慧醫療之快速發展，醫療場域中大量醫療儀器逐漸與IT系統高度整合，從網路掛號系統、醫療資訊系統(Hospital Information System, HIS)，到智慧雙向輸液幫浦、血壓血氧生理監視器及行動護理裝置，皆成為潛在攻擊面，為醫療服務帶來便利性之同時，也將醫療院所推向資安風險之最前線。CODE 2025即以此為核心，打造一個「可被攻擊、可被觀測、可被驗證」之醫療OT演練場域，透過四個連續且相互關聯之攻擊場景，完整呈現攻擊者如何逐步由外而內，利用提升權限、橫向移動，最終影響臨床作業流程與病患安全。

場景一：社交工程郵件所引發之初始滲透

第一個場景模擬外部攻擊者如何透過公開資訊蒐集醫師個人簡介與電子郵件等相關資訊，並鎖定特定醫療人員作為初始目標。攻擊者利用弱密碼、通行碼重複使用或外洩憑證等弱點，成功取得Webmail系統之存取權限，並進一步結合社交工程與釣魚郵件手法，入侵並

焦點文章

取得院內使用者電腦之存取權限，進而作為後續滲透院內系統與擴大攻擊行為之起點。此一場景凸顯人員資安意識與帳號管理在醫療環境中之關鍵性，也是多數進階持續性攻擊常見之起始階段。

場景二：內部橫向移動與權限提升風險

在取得初步存取權後，第二個場景著重於攻擊者於院內環境中之橫向移動與權限提升行為。攻擊者自低權限帳號出發，透過蒐集院內系統資訊、分析使用者行為模式，並結合逆向工程與憑證濫用等手法，逐步擴大在網域環境中之存取權限與可視範圍。隨著權限不斷提升，攻擊者得以接觸更多核心系統與關鍵資料，進一步增加後續攻擊之影響範圍。此一場景具體呈現醫療院所在帳號權限控管、系統分區及身分鑑別管理等面向之常見弱點，說明攻擊者如何在不易察覺之情況下持續攻城掠地、擴張版圖，成為滲透院內關鍵系統之重要跳板。

場景三：套件更新機制遭濫用之供應鏈攻擊

第三個場景模擬攻擊者進一步鎖定醫療場域中之系統更新與部署流程，透過竄改檔案伺服器中之更新套件來源，發動供應鏈攻擊。攻擊者利用組織對既有更新來源與內部流程之信任關係，將惡意程式隱匿於看似正常之更新套件中，藉此繞過既有防護與偵測機制。當OT伺服器依定期排程進行系統更新時，惡意程式即隨之植入，使攻擊得以在不易察覺之情況下進入OT環境並建立存取能力。此一設計凸顯醫療OT系統在更新流程控管、來源驗證及完整性檢查等面向之資安風險，也反映供應鏈攻擊已成為醫療關鍵基礎設施必須高度重視之威脅情境。

場景四：醫療設備遭脅持對病患安全之衝擊

最終場景將攻擊影響延伸至實際臨床作業現場，模擬當攻擊行為成功進入醫療儀器後，可能對病患安全與醫療服務造成之實質衝擊。攻擊者透過院內攝影機取得即時影像，蒐集臨床作業流程與環境資訊，進而逐步掌握操作線索，控制醫療護理推車、護理人員行動裝置、超音波探頭、血壓血氧生理監視器及智慧雙向輸液幫浦等重要醫療儀器，進行錯誤藥品或不當劑量設定等高風險操作，具體呈現資安事件如何由資訊系統層面，直接轉化為影響臨床治療與病患安全之風險。此一場景再次強調，醫療OT資安不僅是資訊防護議題，更與醫療品質與病患生命安全息息相關。

焦點文章

以實戰演練強化醫療OT資安韌性

CODE 2025透過高度擬真之醫療IT/OT混合場域，結合真實資安事件之攻擊路徑與手法，完整呈現醫療院所在數位化發展下所面臨之資安風險樣貌。藉由四個循序漸進之演練場景，不僅可驗證技術防護能力，更強化醫療院所對於人員操作風險、營運流程弱點及臨床醫療儀器資安議題之整體認知。同時，透過資安事件通報流程、跨領域協作及情資交流機制，促進醫療體系資安聯防，由以往各自應對之防禦模式，逐步轉向醫療體系共同守護醫療資訊安全之資安治理架構。展望未來，CODE將持續透過演練方式強化關鍵基礎設施提供者之資安防護能量，以打造堅韌、安全及可信賴之智慧國家。

關鍵字：跨國網路攻防演練、緊急救援與醫院領域、資安聯防

刊　　名　資安週報第 32 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