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

資安週報

Cyber Security Weekly Newsletter

2026.02.12

031

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

搜尋引擎索引污染可能導致網站搜尋結果呈現異常內容 進而影響對外形象與信任觀感

本週總計接獲27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。本週發現有機關網站於Google搜尋引擎查詢時，搜尋結果出現多筆疑似廣告連結，經調查確認，該現象並非網站實際遭植入廣告頁面，而係搜尋引擎索引機制遭濫用，針對可公開存取且具參數之功能介面進行大量自動化請求，誘使搜尋引擎誤將非官方內容納入索引，並因搜尋結果歷史快取殘留而呈現異常連結，其目的在於借用政府網域之可信度，提高廣告或詐騙內容於搜尋結果中的曝光度與點擊率。

建議檢視並控管網站中可公開存取之參數型介面，透過設定搜尋引擎爬蟲規則（如robots.txt、noindex）限制非正式或動態頁面被索引，並加強對異常大量請求之流量監控與必要存取限制，以降低搜尋引擎索引污染風險，降低誤解與對外觀感影響。

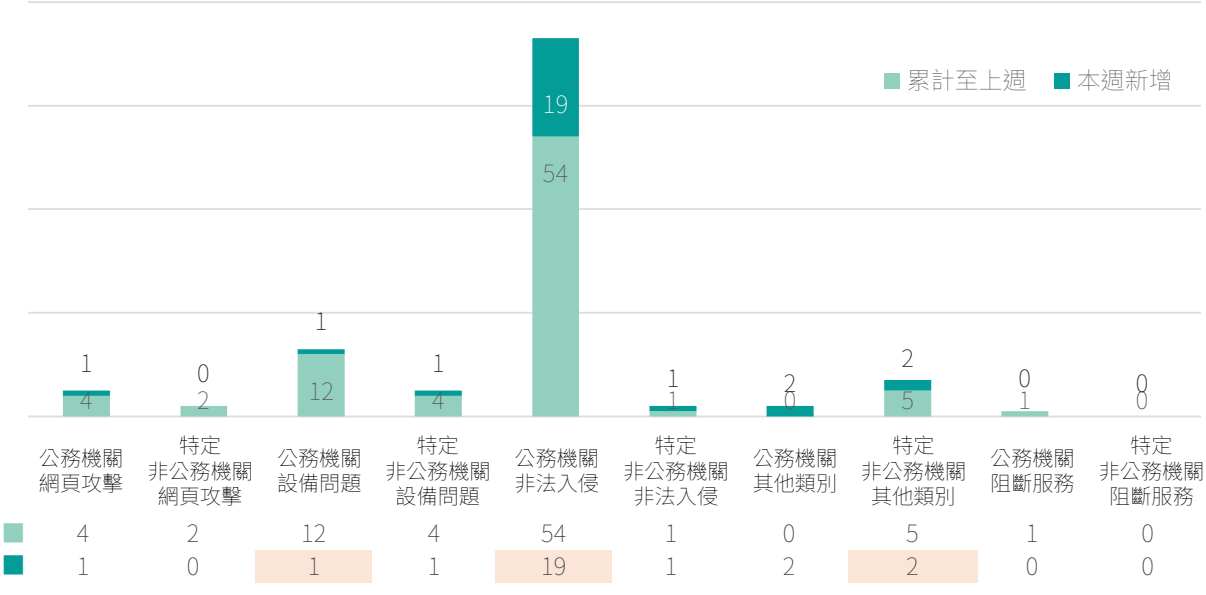

圖1 | 本週公務機關暨特定非公務機關資安事件通報概況

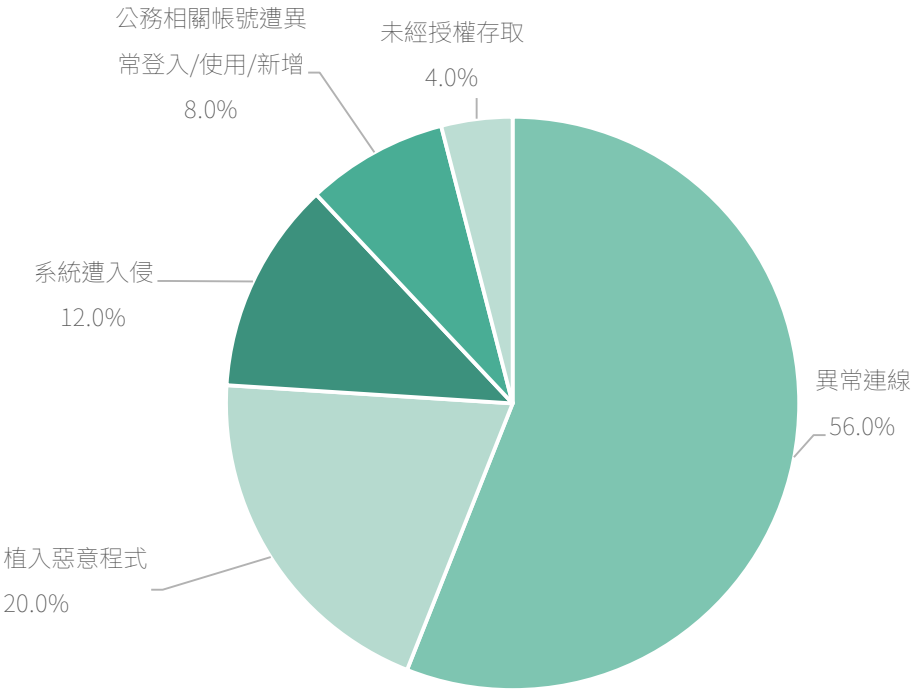

圖2 | 本週公務機關非法入侵事件類型占比

防護建議：除修補漏洞外，應：

- 以攻擊為出發評估潛在風險，如：
  - ✓ 公開參數介面遭濫用，導致搜尋引擎索引污染
  - ✓ 政府網域遭借用，產生詐騙與廣告曝光效果
- 針對潛在風險執行相應改善，如：
  - ✓ 清查並限制可公開存取之參數型功能介面
  - ✓ 設定 robots.txt 與 noindex 阻擋非正式頁面
  - ✓ 強化異常大量請求與自動化流量行為監控
  - ✓ 建立存取頻率限制，降低索引濫用風險

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，產業類別皆為電子零組件業。

- **公司名稱：** 驊陞科技股份有限公司
- **發布時間：** 115 年 2 月 2 日
- **事件說明：** 驊陞公司接獲資訊系統出現異常狀況之警訊後，已啟動相關資安應變措施，並加強系統防護及進行內部盤查作業，目前確認未有資料遺失或外洩情事。目前評估對公司財務及業務營運尚無重大影響，後續將密切監控系統狀況，強化資訊安全管理及相關防護措施，以確保資訊系統安全。

- **公司名稱：** 勝德國際研發股份有限公司
- **發布時間：** 115 年 2 月 3 日
- **事件說明：** 勝德公司發現部分資訊系統遭受駭客網路攻擊，已啟動資安防禦及復原機制、委請外部資安技術公司及專家共同處理，後續依程序向主管機關通報。初步評估對公司營運、個資等無重大影響，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

「偵測刺探」與「初始入侵」雙雙攀升 防禦迴避仍居首位

本週資安聯防監控顯示，整體攻擊態勢呈現多元化發展趨勢，詳如圖3。其中「防禦迴避」階段雖較上週下降1.71個百分點，但仍以14.88%居首位，攻擊者持續透過關閉或清除指令紀錄、利用合法工具執行惡意命令等手法規避偵測機制。

值得關注的是「偵測刺探」階段明顯上升至13.48%，較上週增加2.06個百分點，顯示攻擊者正積極進行目標環境的資訊蒐集與弱點探測。此外，「初始入侵」階段亦大幅攀升至12.87% ，增幅達3.17個百分點，反映攻擊行動已從前期偵察逐步轉向實質入侵階段。

另一方面，「維續存取」階段則大幅下降至5.33%，降幅近5個百分點，可能顯示攻擊者策略調整或防護措施奏效。整體而言，本週監控數據顯示攻擊活動正從初期探測階段逐漸進入更具威脅性的入侵與迴避階段，企業組織應提高警覺，強化相應的防護措施與監控機制。

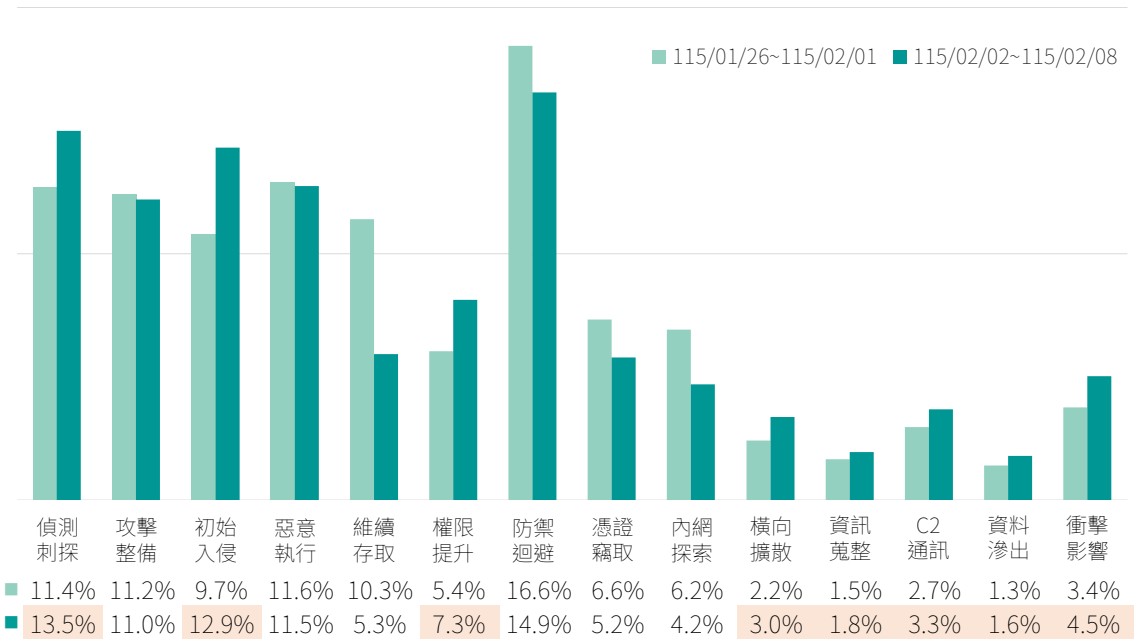

圖3 | 資安聯防監控攻擊階段統計

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
  - ✓ 導入具備行為分析功能的端點防護解決方案，即時偵測異常指令執行模式
  - ✓ 建立完整的指令紀錄稽核機制，確保所有系統操作留存完整日誌且無法輕易清除
  - ✓ 限制高風險工具的使用權限，對PowerShell、WMI等合法但易被濫用的工具實施嚴格管控
  - ✓ 落實特權帳號管理制度，定期檢視管理權限使用情況並實施多因素驗證

- 強化防禦迴避偵測能力
  - ✓ 部署網路流量監控系統，及時發現異常掃描與探測行為
  - ✓ 定期進行弱點掃描與修補作業，降低攻擊者可利用的入侵途徑
  - ✓ 強化邊界防護機制，包含防火牆規則優化與入侵防禦系統更新

■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78.81%、「遠端控制」服務攻擊占比18.00%，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66.20%。「遠端控制」服務亦有29.37%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下降主因為華為HG532存在遠端程式碼執行漏洞的CVE-2017-17215，遭攻擊次數大幅下降導致。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

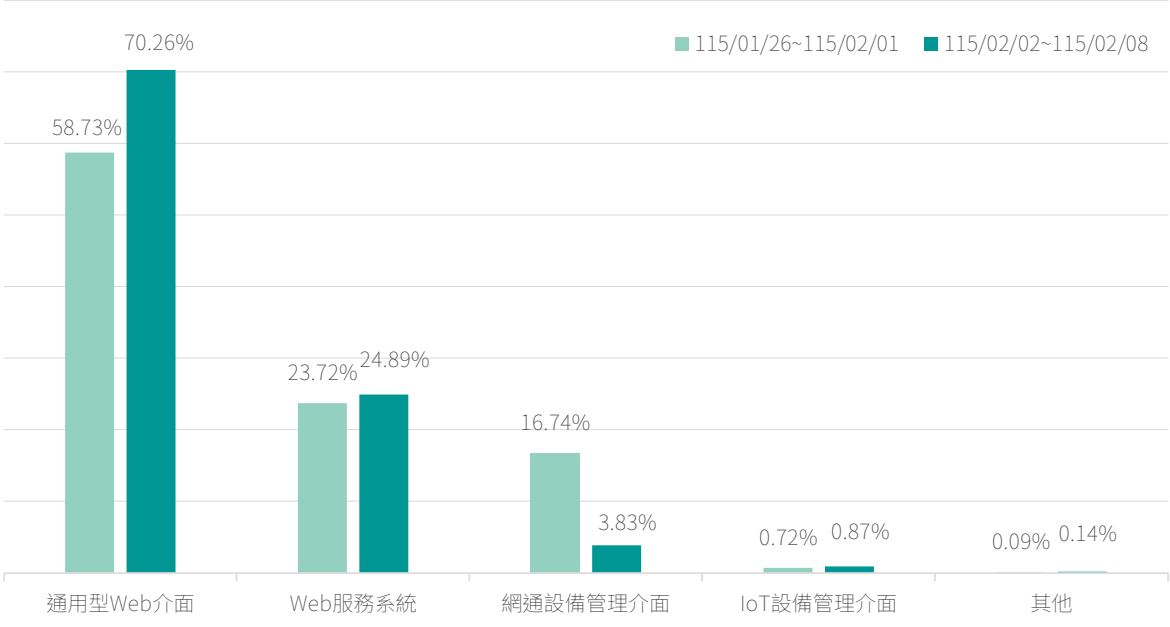

圖4 | 本週網頁應用服務之誘捕攻擊比例統計

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。

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、程式碼注入及遠端程式碼執行漏洞，攻擊目標涵蓋Citrix NetScaler ADC、Cisco IOS XE網通設備作業系統、GeoServer開放源碼伺服器、PHP及Ivanti資安軟體，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。

類型 ■越界讀取漏洞 ■特權提升 ■程式碼注入 ■遠端程式碼執行漏洞

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	-	CVE-2024-36401[3]	GeoServer開放源碼伺服器	9.8
■	4	-	CVE-2024-4577[4]	PHP	9.8
■	5	↑New	CVE-2024-21887[5]	Ivanti資安軟體	9.1

表1 | 本週前5大攻擊使用之近3年漏洞排行列表

▶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：

- Cisco Meeting Management憑證管理功能存在高風險安全漏洞(CVE-2026-20098[6])，類型為任意檔案上傳(Arbitrary File Upload)，已通過身分鑑別且取得video operator(含)以上角色權限之遠端攻擊者可透過傳送特製HTTP請求至受影響設備，並覆寫由root帳號處理之檔案，進而執行任意程式碼。

- Microsoft Office存在高風險安全漏洞(CVE-2026-21509[7])，類型為安全功能繞過(Security Feature Bypass)，未經身分鑑別之攻擊者可透過發送惡意Office文件並誘使用戶開啟，進而繞過元件物件模型(Component Object Model, COM)與物件連結與嵌入(Object Linking and Embedding, OLE)防護機制，使原本應該被阻擋之COM/OLE控制元件仍能執行。

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-2024-21887
6. https://nvd.nist.gov/vuln/detail/CVE-2026-20098
7. https://nvd.nist.gov/vuln/detail/CVE-2026-21509

■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

過時或弱加密協定風險明顯增加 成為主要惡化項目

本期針對43個公部門單位進行EASM資安曝險檢測，共計發現311項重大與高風險弱點，其中包含4項重大風險與307項高風險弱點，詳如圖5。結果顯示，整體外部曝險情勢較上期(310項)略有上升，風險總數增加約0.3%。從風險類別分布觀察，本期仍以「過時或弱加密協定(102項)」、「TLS憑證不受信任(87項)」、「CSP設定不當(53項)」及「元件高風險漏洞(37項)」為主要類別，四類合計占比約90%，此一分布反映多數單位在憑證管理、漏洞修補及網站安全設定上仍存在普遍性風險，亦為現階段資安防護的主要挑戰。

進一步比較兩期差異，「過時或弱加密協定」由83項增至102項，增幅達23%，為本期惡化最明顯項目；「TLS憑證不受信任」由101項降至87項，降幅達14%，為本期改善最顯著項目；「元件高風險漏洞」由36項微增至37項，「CSP設定不當」由54項降至53項，「未部署WAF」則由19項增至20項，三者變化幅度不大，整體維持相對穩定。

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)期更新

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

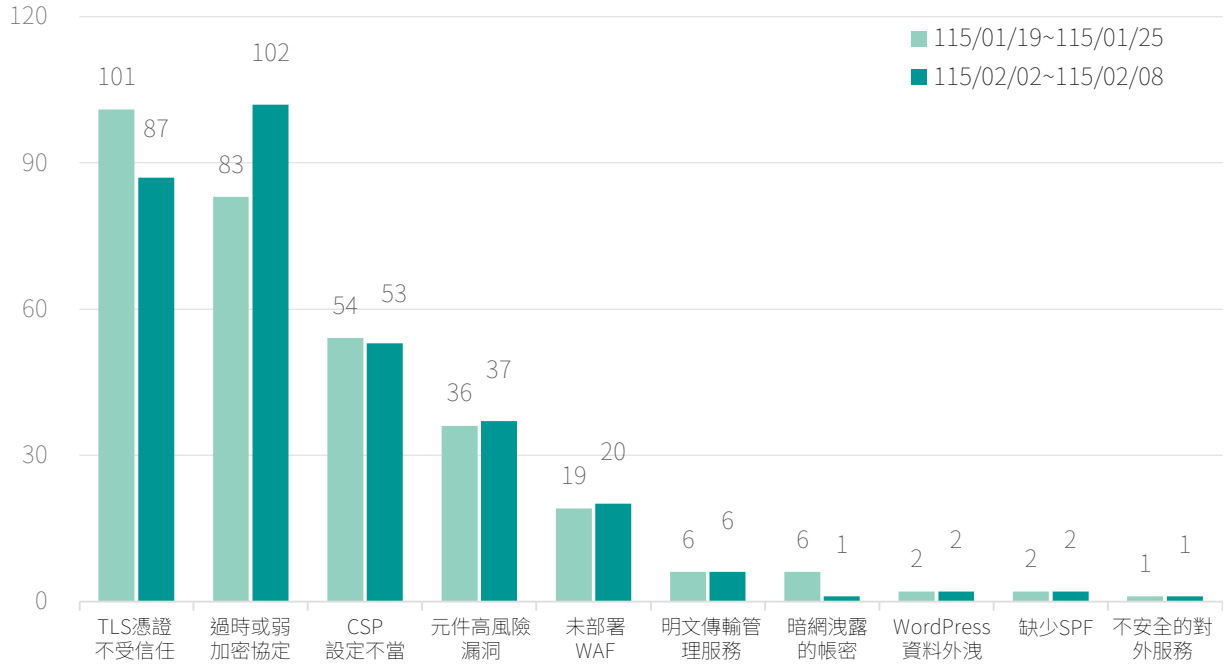

圖5| EASM檢測結果統計(前10大風險)

■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

2025 年詐騙高風險廣告手法分析/焦點分析

上半年較常見投資帶單與入群引導；年中開始換檔，下半年更常見導購促銷與生活化包裝，年末檔期辨識難度最高。

「立即／加入／免費／領取／點擊」等引導語全年反覆出現，形成穩定的引流骨架，常把受眾帶往私域互動後再推進金流或個資。

進入 10～12 月，導購語氣與活動包裝更強，面對「優惠＋點擊＋領取」等訊息務必保持冷靜、先查證再行動。

一 全年共通骨架：少數高頻引導語，反覆把人推向「私下互動」

從全年關鍵字脈絡可見，不同月份題材會更換，但「引流骨架」相當穩定，常由以下三類詞組成：

- 催促決策：如「立即」等，製造急迫感，讓人來不及查證。
- 導入互動：如「加入」等，把互動從公開場域導向社群或私訊。
- 利益誘因：如「免費」「福利」「領取」等，降低戒心、促使點擊與留資。

常見推進路徑可概括為：
急迫感 → 加入／點擊 → 領取／福利 →（後續再導向金流或個資）。因此，即便表面上看起來像投資、像優惠活動、像生活資訊，實際上常是同一套流程在不同包裝下運作。

二 1～2 月：年初「投資氛圍」較強，常見「先入群、再帶單」的節奏」

年初常見內容更偏向投資語境，特徵是先用「免費／加入」降低戒心，再以「機會」與「節奏」推動後續互動。這階段常見手法是把「資訊落差」塑造成優勢，讓人以為只要加入就能獲得更好的資訊或操作指引。

三 3 月：投資帶單語氣最典型，強調「節奏、跟上、進出場」

3 月的內容風格最像「投資帶單模板」：

- 時間節奏強：例如「早上」「準時」「立即」等語氣，暗示必須跟上特定時點。
- 進出場暗示：如「明牌」「報牌」「上下車」「黃金期」等，營造「跟著做就能掌握機會」。

- 可信感包裝：以「公佈」「眼見為憑」等語意，讓人降低查證需求。

這類內容的目的往往不是一次說服，而是讓人先加入社群或轉入私訊，後續才逐步推進更高風險的操作或金流。

四 4～5 月：投資題材延伸，但包裝更「像專業建議」，更強調權威與安全感

4～5 月仍可看到投資語境延續，但話術更常轉向「專業」「實力」「可信」等形象塑造，使內容更像一般投顧討論或市場分析，降低一般受眾的戒心。

這段期間常見的風險點在於：表面看似資訊分享，實際仍在引導加入、導向私訊，並建立「由他人帶操作」的依賴關係。

五 6 月：手法開始「換檔」— 從投資主軸逐步轉向「產品服務／周轉議題」

進入 6 月後，內容包裝更常見「產品服務」與更生活化的切入點，投資話術的主導感下降。這階段的常見方向包括：

- 用「資金」「周轉」「貸款」等語境切入，主打「協助處理」或「快速方案」。
- 用較中性、生活化的語氣降低警覺，讓人更願意私訊或留下聯絡方式。

提醒民眾：凡是以「協助周轉」為名、要求加 Line、填表單、提供身分資料或驗證資訊者，都應提高警覺。

六 7 月：暑期「生活化入口」明顯增加，常見「先聊天建立信任、再推進」

7 月是全年「生活化入口」最具代表性的月份之一，常見兩類路徑：

- 情緒／關係議題切入：如「八字」「感情」「聊天」「分手」「吵架」等，先建立互動與信任，再慢慢引導到付費、課程或金流。
- 看似一般貼文／小店／課程：以「福利」「價格」「保證」「課程」等語彙，讓內容看起來像正常行銷或社群販售，降低受眾防備。

這個月的重點不是某一類題材特別多，而是「入口更日常、辨識更困難」：越像一般聊天與貼文，越要回頭查來源、查連結、查是否導向私域操作。

七 8 月：整體熱度偏低，但手法更分散、更像「試探式投放」

8 月常見現象是量體感受較低、題材更分散，內容外觀更像一般廣告或一般互動貼文。這種「分散投放」常被用來測試哪一種包裝更容易引發點擊與私訊，後續再把有效模板放大。

八 9 月：導購與互動型內容逐步回升，「領取／福利」與「加入」再次成為推進核心

9 月開始，導購與互動型語氣逐步回溫，常以「福利」「領取」「加入」等字眼作為入口，推動點擊或加入社群。這時候的風險常落在：外部連結、表單留資、以及私訊導向的後續操作。

九 10 月：年末前哨期—「導購包裝」與「投資元素」開始混搭

10 月常見的變化是：內容仍以導購與互動型語氣為主，但會夾帶「機會」「推薦」等語意，並逐步把人導向更封閉的互動場域（社群／私訊）。

這是進入年末高風險檔期前常見的鋪陳：先用活動與福利降低戒心，再把人導入下一階段。

十 11 月：混合型手法最明顯—「免費／活動」與「股票／投資」並行

11 月的特色是「混合包裝」：

- 一方面以「免費」「領取」「福利」「活動」作為入口，提高互動率。
- 另一方面同時置入「股票」「投資」「機會」等語彙，把受眾導向投資社群或後續操作。

提醒民眾：當「活動福利」與「投資機會」同時出現時，往往是組合拳式引流，特別容易把人快速帶進私域。

十 12 月：年末促銷檔期—導購語氣更強，最常見「優惠＋點擊＋領取」

12 月的內容外觀更像一般行銷：

- 「優惠」「點擊」「領取」「活動」「推薦」等詞彙更常一起出現。
- 風險常集中在「導向外部連結／表單」與「要求輸入個資或驗證資訊」的情境。
- 也更容易出現仿冒頁面或假客服引導，讓受眾在不經意間交出資料。

提醒民眾：遇到「優惠＋點擊＋領取」等組合時，務必先查網址、查官方公告，避免在不明頁面輸入個資、信用卡資訊或 OTP 驗證碼。

焦點一：3 月的投資帶單模板最完整，節奏與權威話術同時強化

3 月的內容最能看到投資詐騙的典型組合：用「立即／準時」製造時間壓力，用「明牌／報牌／上下車」暗示進出場，用「公佈／眼見為憑」塑造可信度，最後引導加入社群或私訊。

焦點提醒：凡是要求「跟單、跟時點、加入群組」的投資訊息，先停、先查、先問。

焦點二：6 月出現換檔訊號，產品服務與周轉語境更常用來降低戒心

6 月後內容更常以「周轉」「資金」「協助」等語境接觸，外觀看起來更像一般服務或諮詢；但若導向私訊、要求填資料、或以流程名義索取敏感資訊，風險就會快速升高。

焦點提醒：任何「先留資料再說」「先驗證再處理」都要查證來源。

焦點三：7 月生活化入口增加，常見「先互動、後推進」的路徑

暑期常見的不是單一題材，而是「建立關係」的節奏：先聊天、先陪伴、先給建議，再逐步導向課程、付費、或金流。

焦點提醒：只要對話開始從「聊天」轉向「金錢／個資」，就應立即停下並查證。

焦點四：10 月到 11 月的混合期，福利活動與投資元素交錯，最容易讓人降低戒心

這段期間常見先用「免費／福利／活動」當入口，再帶入「股票／投資／機會」等語彙導向社群。

焦點提醒：免費活動不等於安全；越是強調「機會」與「名額」，越要反向查證。

焦點五：12 月促銷檔期導購語氣最強，「優惠＋點擊＋領取」是高風險組合

年末期間內容外觀更像一般廣告，辨識難度上升；風險集中在外部連結、表單留資、仿冒頁面與假客服引導。

焦點提醒：遇到要求點擊、領取、輸入資料的流程，先確認網址與官方來源，避免在不明頁面輸入敏感資訊。

焦點文章

金盾二十・韌性前行

從競賽到生態系，建構國家級資安人才之戰略展望

一 前言｜超越賽事：啟動資安人才的自我迭代引擎

資安技能競賽金盾獎，從來都不只是一場年度競賽，而是臺灣資安人才培育上，最具生命力的「自我迭代引擎」。邁入第二十週年，我們承載著國家資安政策的期待，不只是在選拔技術尖兵，更在國家資通安全研究院(以下稱本院)的領航下，建構一個能自動翻新技術能量、傳承實戰經驗的國家級人才生態系。

二 戰略高度：以「實務演義」定義新世代全域防禦戰力

對於多數網路原生世代的參賽者而言，藉由「網路」與「大型語言模型」自動化餵養知識，儼然是一件理所當然的事。然而，本院就人才培育的角度，更加重視年輕參賽者習得正確參賽心態與韌性，期待各參賽隊伍能從競賽中習得「主動」求取新知之合作經驗、獲取深入資安領域之「興趣」，以及真正習得資安「虛實整合」之防禦技術。

有鑒於此今年情境題型設計以「RPG 情境題材料包」將真正在機房、拉線現場會用到的工具與元件帶入題型中，讓參賽者們能在情境任務中，習得理解它們各自的用途並應用。讓參賽學子在跨越軟硬體界限的挑戰中，鍛鍊出應對全域威脅的直覺，下述分享三場精彩的「實務演義」情境題型：

1. 地緣真相 —— 韌體與硬體安全思維：

本題以「拆彈任務」為情境載體，希望訓練參賽者之韌體分析與硬體安全思維。選手須針對電路板韌體進行深層解析，理解控制邏輯與保護機制，方能推導出正確之剪線操作順序以達成任務、取得 Flag。

透過模擬高度壓力及資訊不對稱之極端情境，磨練選手透過程式行為與訊號反應做出正確決策之能力。此外，題目電路板背面也刻印上了入圍決賽隊伍之名稱，供選手留存紀念。

焦點文章

2. 幽光竊語 —— 實體層通訊安全與緊急應變實務：
本題題材取自俄烏戰爭初期「關鍵基礎設施於戰時遭破壞」之真實威脅情境，引導參賽者理解——除傳統網路設備與系統層級外，傳輸介質亦為不容忽視之攻擊面。選手須於模擬情境中實作「光纖通訊內容攔截」，藉此獲取關鍵情資以取得 Flag。

此外，本題同步整合「光纖冷接」技術實作。光纖冷接為電信工程實務中至關重要之職能，廣泛應用於光纖到府等佈建工程。另從資安維度來看，當面臨緊急搶修或需迅速恢復通訊之關鍵時刻，具備此項技能可大幅縮短系統修復時程，有效提升資安事件發生時之緊急應變效率。

3. 熱控失序 —— 工控安全與操作技術防禦：
本題為模擬由可程式化邏輯控制器（Programmable logic controller，PLC）自動控制之暖通空調（Heating, ventilation and air conditioning，HVAC）系統，揭示其工控環境可能遭遇之資安風險。

系統組件如蒸發器、加熱器及多組風扇，平時依循 PLC 自動控制邏輯運轉；然而，若通訊、權限或指令驗證不足，攻擊者即可在未碰觸硬體的情況下，透過網路操控設備運轉狀態。本題任務目標明確：選手須同時完成讓蒸發器與所有風扇關閉、但讓加熱器開啟之特定啟閉組合，方可完成任務並取得flag。

本道題目的核心目的在於強化參賽者對工控資安影響力之認知——威脅不僅限於數據外洩，更可能直接導致實體設備異常運轉，進而衝擊公共安全與營運效能。

三　循環生態：啟動「技術回流」的人才迭代機制

本競賽核心策略在於建構能持續具備自我演進能力的人才生態系，建立「從獲獎者到引領者」的典範轉移，鼓勵歷屆優秀參賽人才「技術回流」，將競賽能量轉化為誘發國家資安年輕人才的持續動能。

焦點文章

■ 金盾歷屆獲獎選手回流命題

本屆賽事創新導入「歷屆獲獎傑出校友之命題機制」，策略性邀請多位具備金盾歷屆競賽佳績與國際賽事（如 DEF CON CTF等）獲獎實戰經驗者擔任命題委員。此舉不單是技術層面的交流，更是人才培育路徑的典範轉移。

透過讓具備產、學界前瞻視野的「前輩」加入金盾賽事命題，不僅能將最前線的國際資安威脅趨勢、攻防思維及實戰經驗融入考題，更能有效打破校園與實務邊界，達成技術深耕與薪火相傳之實質意義。

■ 以賽促訓之思維與模式傳承

為持續傳遞金盾獎辦理價值，藉由「以賽促訓」加速學子接觸到與全球資安演進趨勢同步的技術水平，成為誘發國內學子觸及頂尖資安思維的一大門路與培養出參賽者應對新型態威脅的專業底蘊技術試煉場。

■ 人機協作新定義

因應生成式AI技術的快速崛起，本賽事首度開放使用大型語言模型與生成式AI工具。透過此項變革，引導選手思考「人機協作」下的專業分工，確保國家級資安人才在 AI 時代仍具備無可取代的判斷力、戰略思維與扎實底層技術，進而提升整體防禦體系的應變韌性。

四 文化底蘊：凝聚「資安守護者」的社群認同

資安人才的培育不應僅止於技術的堆疊，更需建立深厚的職業榮譽感與文化認同。透過「金盾 20 周年」的契機，我們成功地將競賽場域轉化為情感鏈結的空間。

■ 從歷史看見未來 - 沈浸式體驗下的榮譽共感

走過臺灣資安發展二十載，此次特別策劃了「金盾 20 周年回顧特展」。此次分為動靜態展區，靜態展牆以「20年重點大記事翻翻牆」記錄競賽年度大事紀演進的里程碑、「歷屆小書展」與「立體拼圖」重現歷屆經典徵件作品、「經典語錄牆」共振參賽過程的酸甜苦辣。

焦點文章

動態展區則增設「數據傳送封包」、「危機快手任務」闖關關卡，此互動設計將抽象的網路安全概念轉化為實體挑戰，讓參賽選手、帶隊老師及貴賓透過直觀的操作，理解資料傳輸過程中的潛在風險與防護必要性。在趣味互動中成功傳達資安專業理念，並深化與會者對網路環境安全之認知。

藉由將抽象技術歷程具象化為感官互動的設計，整體達4.59分（滿分5分）的高度滿意度評價，更在無形中提升了參與者對於自身為「資安守護者」身分的榮譽感，讓金盾獎成為連結過去技術積累與未來創新展望的關鍵節點。

五　金盾展望：量能擴張下的社群共鳴與認同

金盾獎的品牌影響力已具體反映在持續攀升的年度賽事報名參與數據中，本年度總報名人數已成長至589人。值得關注的是，初賽中有高達177位（79%）為首次參賽之新秀、45位曾入圍歷屆金盾獎決賽，且女性參賽比例亦提升至24%的正向趨勢，多重顯示賽事在維持回流參賽者的同時，亦成功吸引眾多資安新秀投入，有效擴大資安競賽的參與族群，並厚植資安人才儲備。

在二十周年專屬回顧影片中，我們跨越時空框架，邀請歷屆衛冕冠軍校友與當屆新秀進行對話，這不僅是一場敘事影像，更是資安社群集體記憶的重塑。

六　結語｜下一哩路：建構產學無縫接軌的攻防體系

透過「數據成長」與「情感共振」的雙軌併行，本院已成功將金盾獎從一個單純的年度賽事，轉化為資安學子心目中的「重要里程碑」。這種跨世代的經驗共鳴，不僅厚植了本院長年辦理競賽的品牌價值，更強化了資安院在推動技術傳承上的社群影響力，使金盾獎成為國內資安生態圈中最具黏著度與擴散力的指標性賽事。

未來，金盾獎將持續作為資安新秀邁向實務界的孵化器，並期待能強化與更多產、官、學、研的資源鏈結，持續以嶄新樣貌推陳出新，厚植臺灣資安年輕人才。

焦點文章

關鍵字：金盾獎、工控安全、人機協作

刊　　名　資安週報第 31 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