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

建議強化下載與執行行為之控管 避免依來信指示操作所帶來之風險

聯防監控

防禦迴避高居首位 偵測刺探仍具威脅

蜜罐誘捕

本週整體趨勢維持穩定 與前期相比未有顯著變化

外部曝險分析

整體曝險持續下降約6.9% TLS憑證不受信任風險明顯改善，由29項降至本期未檢出

焦點文章

從交友、素食到公益 「先養後殺」社群詐騙正席捲日常生活

2026.04.23
041

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

建議強化下載與執行行為之控管 避免依來信指示操作所帶來之風險

本週總計接獲16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。本週有機關接獲以業務需求為由要求確認資料 ，承辦人員因附件無法開啟回信詢問後，對方改提供雲端下載連結，致下載並開啟惡意程式。相較傳統寄送惡意附件之手法，本案具「有來有回」之互動特性，攻擊者會依使用者回應調整方式，提升誘導成功率。

此類具「互動性」之社交工程及雲端下載風險，建議在技術面，應持續落實郵件與連結檢測機制，並透過端點偵測(EDR)監控下載與執行行為，以補足由附件轉為下載之防護落差，並強化對雲端下載行為之監控與警示。在管理面，可針對異常檔案情境建立對應控管措施 ，避免直接依來信下載檔案，並限制檔案取得方式與類型。

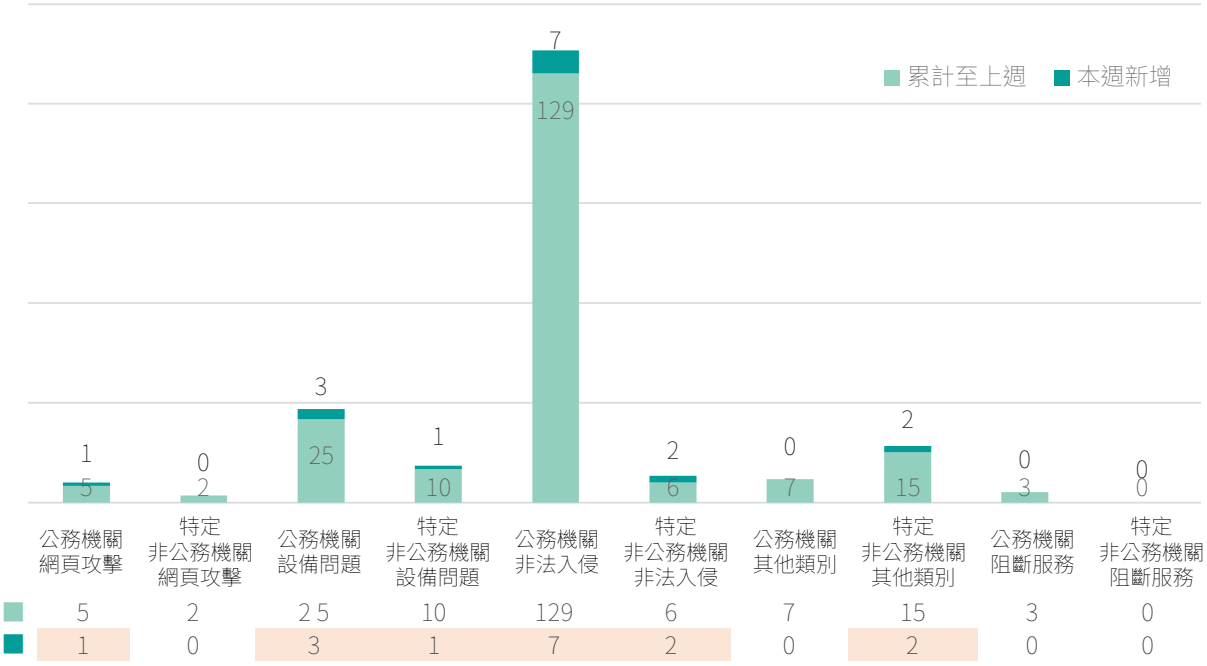

圖1 | 本週公務機關暨特定非公務機關資安事件通報概況

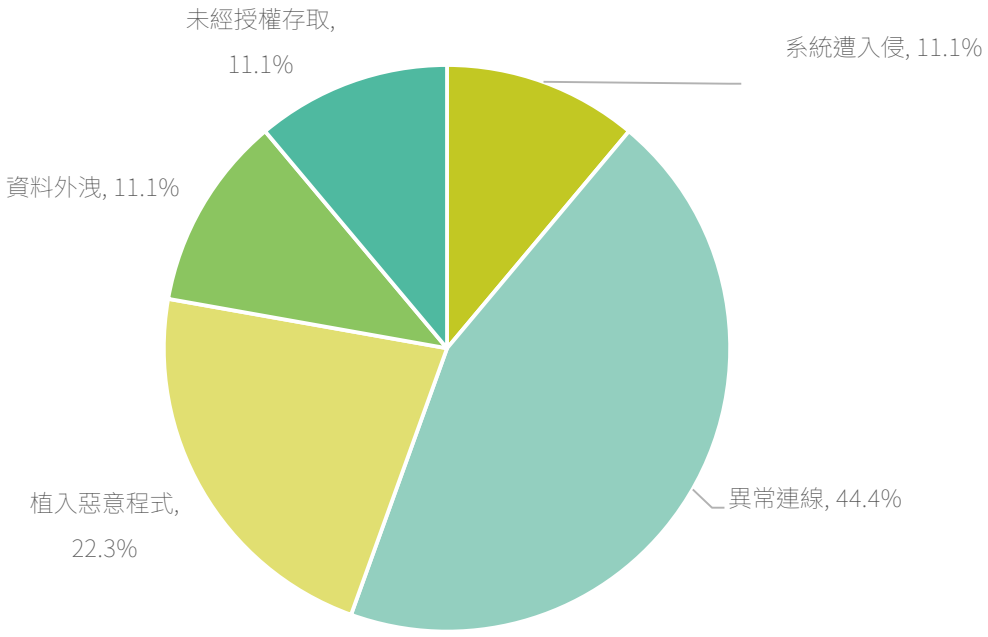

圖2 | 本週公務機關非法入侵事件類型占比

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
➢ 攻擊者透過互動誘導下載惡意程式執行 ➢ 利用雲端連結規避郵件防護進行入侵	➢ 強化郵件與連結檢測機制，防範惡意下載連結繞過郵件防護措施 ➢ 導入端點偵測與回應機制，即時監控檔案下載與執行異常行為 ➢ 建立雲端下載行為控管機制，限制來源與檔案類型降低風險 ➢ 強化人員資安教育訓練，避免依指示下載不明來源檔案

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，產業類別分為電腦及週邊設備業、航運業。

■ 公司名稱	力致科技股份有限公司
■ 發布時間	115年4月13日
■ 事件說明	力致公司發現部分資訊系統遭受駭客網路攻擊，事發當下已全面啟動相關防禦機制與復原作業，同時與外部資安公司技術專家協同處理。目前對所有資訊系統及檔案全面徹底的掃描檢測，經初步評估對公司運作無重大影響，後續將修復安全漏洞並持續提升網路與資訊基礎架構之安全控管以確保資訊安全。

■ 公司名稱	新竹物流股份有限公司
■ 發布時間	115年4月18日
■ 事件說明	新竹物流公司部分資訊系統遭受駭客網路攻擊，已全面啟動相關防禦機制及復原作業，並委請外部資安公司技術專家共同處理，經評估對本公司營運無重大影響。

■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14.4%，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13.6%，為本週占比次高的攻擊階段，顯示攻擊者在攻擊前期持續加大對目標環境的偵查與資訊蒐集力度。觀察到的主要手法包括主動式掃描、IP區段掃描、以及DNS 與被動式 DNS 情資蒐集。攻擊者透過自動化工具對大範圍網段進行探測，以識別可存取服務與開放埠，並結合被動式 DNS 分析，掌握目標組織之網域架構、子網域關聯與歷史解析紀錄，進一步描繪完整攻擊面。此類行為結合主動與被動偵查手法，具備低互動、高隱蔽的特性，且能有效提升後續攻擊的成功率。建議強化對異常掃描流量的監控與阻擋機制，定期盤點與控管對外資產與DNS資訊曝光情形，並結合威脅情資分析，以提前辨識潛在攻擊準備活動。

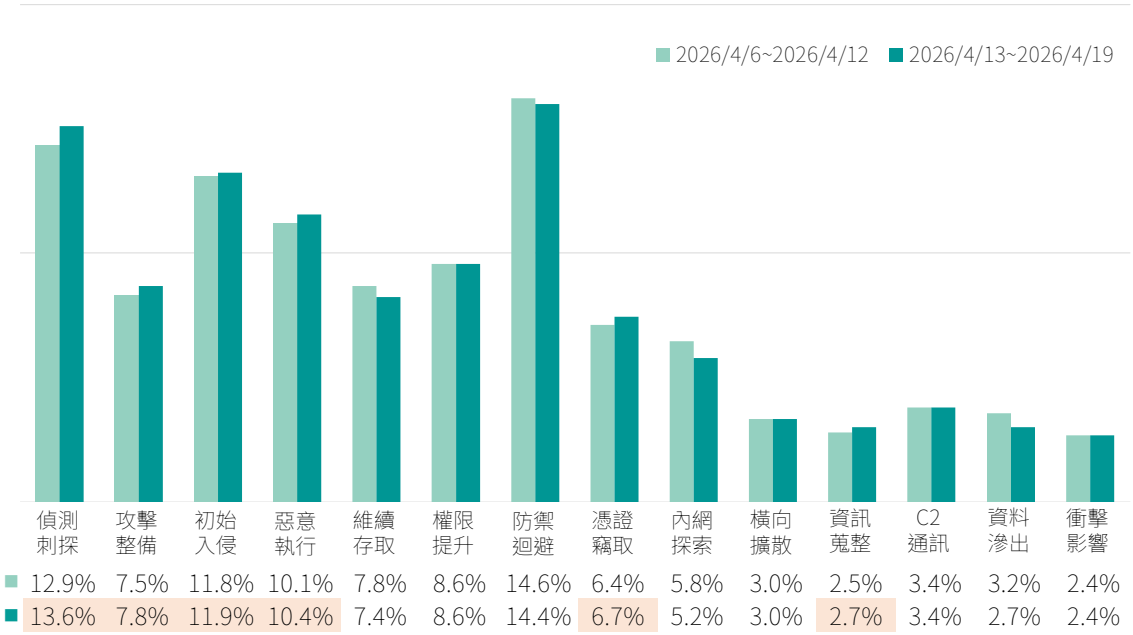

圖3 | 資安聯防監控攻擊階段統計

防護建議 建議機關採取下列防護措施：

- 強化日誌集中與防竄改
- 監控高風險系統工具使用
- 限制內建工具濫用（白名單）
- 落實特權帳號控管
- 偵測關閉日誌/防護機制行為

防禦迴避（Defense Evasion）

- 偵測並阻擋異常掃描流量
- 定期盤點對外資產
- 強化 DNS 安全與監控
- 降低公開資訊曝露
- 結合威脅情資分析

偵測刺探（Reconnaissance）

■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

本週整體趨勢維持穩定 與前期相比未有顯著變化

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73.64%、「遠端控制」服務攻擊占比23.06%，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74.28%。「遠端控制」服務亦有21.62% 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。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。

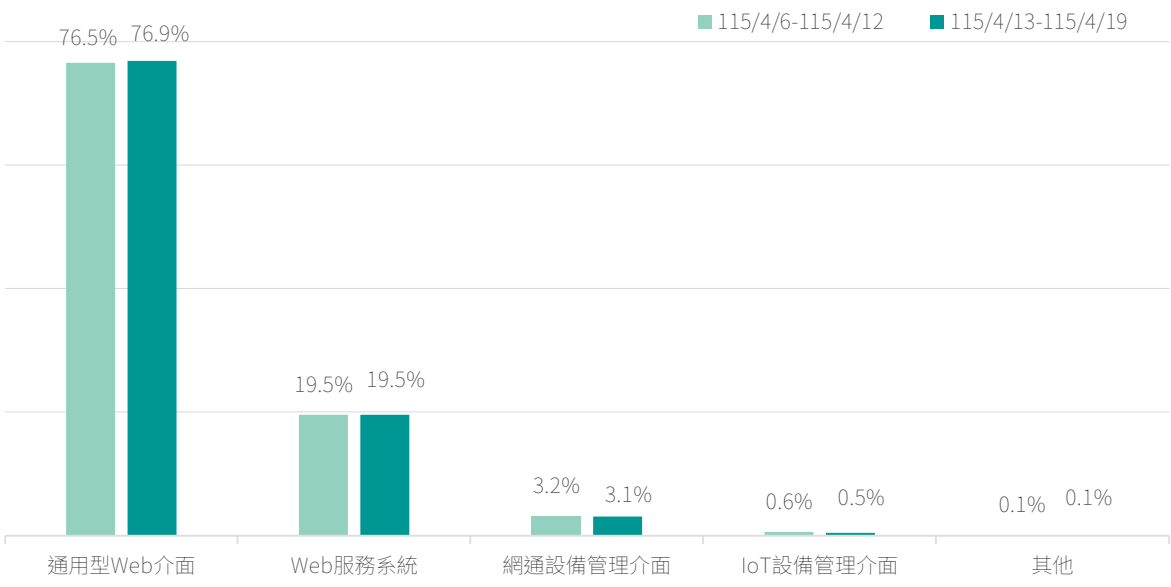

圖4 |本週網頁應用介面之誘捕攻擊比例統計

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、遠端程式碼執行漏洞、程式碼注入漏洞及目錄遍歷漏洞，攻擊目標涵蓋應用程式遞送控制器(ADC)、PHP伺服器端腳本語言、知識管理與團隊協作系統、行動裝置管理系統及VPN Gateway。

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-2024-4577[2]	PHP	9.8
■	3	-	CVE-2024-21683[3]	Atlassian Confluence Server	8.8
■	4	⬆1	CVE-2025-4428[4]	Ivanti Endpoint Manager Mobile	7.2
■	5	⬇1	CVE-2024-24919[5]	Check Point VPN Gateway	8.6

類型 ■越界讀取漏洞 ■遠端程式碼執行漏洞 ■程式碼注入漏洞 ■目錄遍歷漏洞

▶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：

- 微軟釋出115年4月份安全性更新，共修補包含Windows IKE Extension、Microsoft PowerApps及Windows Shell等共165個漏洞[6]，其中包含8個高風險漏洞與1個已遭利用之漏洞。
- 以Chromium為基礎之瀏覽器存在60個高風險安全漏洞(CVE-2026-5858至CVE-2026-5915、CVE-2026-5918及CVE-2026-5919[7])，類型包含堆積型緩衝區溢位(Heap-based Buffer Overflow)與使用釋放後記憶體(Use After Free)等，最嚴重可使未經身分鑑別之遠端攻擊者透過特製HTML頁面造成記憶體損毀或執行任意程式碼。
- Cisco Identity Services Engine(ISE)存在3個高風險安全漏洞(CVE-2026-20147[8]、CVE-2026-20180[9]及CVE-2026-20186[11])，類型包含指令注入(Command Injection)與路徑遍歷(Path Traversal)。
  - CVE-2026-20147：已取得管理者權限之遠端攻擊者可藉由發送特製HTTP請求執行任意作業系統指令。
  - CVE-2026-20180與CVE-2026-20186：已取得唯讀管理者權限之遠端攻擊者可藉由發送特製HTTP請求執行任意作業系統指令。
- Cisco Webex Services存在高風險安全漏洞(CVE-2026-20184[10])，類型為不當憑證驗證(Improper Certificate Validation)，當此服務之Control Hub與SSO整合時，未經身分鑑別之遠端攻擊者可藉由提交特製之認證資料，冒充服務中任意合法使用者。
- Oracle Fusion Middleware存在高風險安全漏洞(CVE-2026-21962[12])，類型為不當存取控制(Improper Access Control)，未經身分鑑別之遠端攻擊者可透過HTTP存取受影響服務，進而於未授權之情況下建立、刪除、修改或存取系統重要資料。

- Apache ActiveMQ Classic存在高風險安全漏洞(CVE-2026-34197[13])，類型包含不當輸入驗證(Improper Input Validation)與程式碼注入(Code Injection)，因Web Console暴露之Jolokia JMX-HTTP介面允許執行特定操作且缺乏輸入驗證，使已通過身分鑑別之遠端攻擊者可傳入惡意參數，進而執行任意程式碼。

- Adobe Acrobat Reader存在高風險安全漏洞(CVE-2026-34621[14])，類型為原型鏈汙染(Prototype Pollution)，未經身分鑑別之攻擊者可誘使使用者開啟特製惡意檔案，污染程式執行時之物件原型，進而以當前使用者權限執行任意程式碼。

1. https://nvd.nist.gov/vuln/detail/CVE-2025-5777
2. https://nvd.nist.gov/vuln/detail/cve-2024-4577
3. https://nvd.nist.gov/vuln/detail/cve-2024-21683
4. https://nvd.nist.gov/vuln/detail/cve-2025-4428
5. https://nvd.nist.gov/vuln/detail/cve-2024-24919
6. https://msrc.microsoft.com/update-guide/releaseNote/2026-Apr
7. https://chromereleases.googleblog.com/2026/04/stable-channel-update-for-desktop.html
8. https://nvd.nist.gov/vuln/detail/CVE-2026-20147
9. https://nvd.nist.gov/vuln/detail/CVE-2026-20180
10. https://nvd.nist.gov/vuln/detail/CVE-2026-20184
11. https://nvd.nist.gov/vuln/detail/CVE-2026-20186
12. https://nvd.nist.gov/vuln/detail/CVE-2026-21962
13. https://nvd.nist.gov/vuln/detail/CVE-2026-34197
14. https://nvd.nist.gov/vuln/detail/CVE-2026-34621

■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

整體曝險持續下降約6.9% TLS憑證不受信任風險明顯改善，由29項降至本期未檢出

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5,959項，詳見圖5。其中，「元件高風險漏洞」以3,548項居首，「CSP設定不當」997項次之，「未部署WAF」552項續居第三。前三項合計5,097項，占前10大風險項目總數約85.5%，顯示當前風險仍高度集中於元件漏洞、內容安全政策設定及應用層防護面向。相較上期6,403項，整體風險數量減少444項，降幅約6.9%，整體曝險情勢穩步收斂。

進一步分析主要風險變化情形，「TLS憑證不受信任」由29項降至本期未檢出，顯示相關憑證信任問題已有明顯改善；「未部署WAF」由705項降至552項，減少153項，減幅約21.7%；「過時或弱加密協定」由446項降至359項，減少87項，降幅約19.5%；「元件高風險漏洞」由3,718項降至3,548項，減少170項，減幅約4.6%，前述4項均呈現改善趨勢。另一方面，「不安全的對外服務」由264項增至275項，增加11項，增幅約4.2%；「CSP設定不當」由989項增至997項，增加8項，增幅約0.8%；「明文傳輸管理服務」亦由96項增至99項，增加3項，增幅約3.1%，顯示部分機關在對外服務曝險管控、內容安全政策設定及管理介面防護等方面，仍有持續精進之空間。

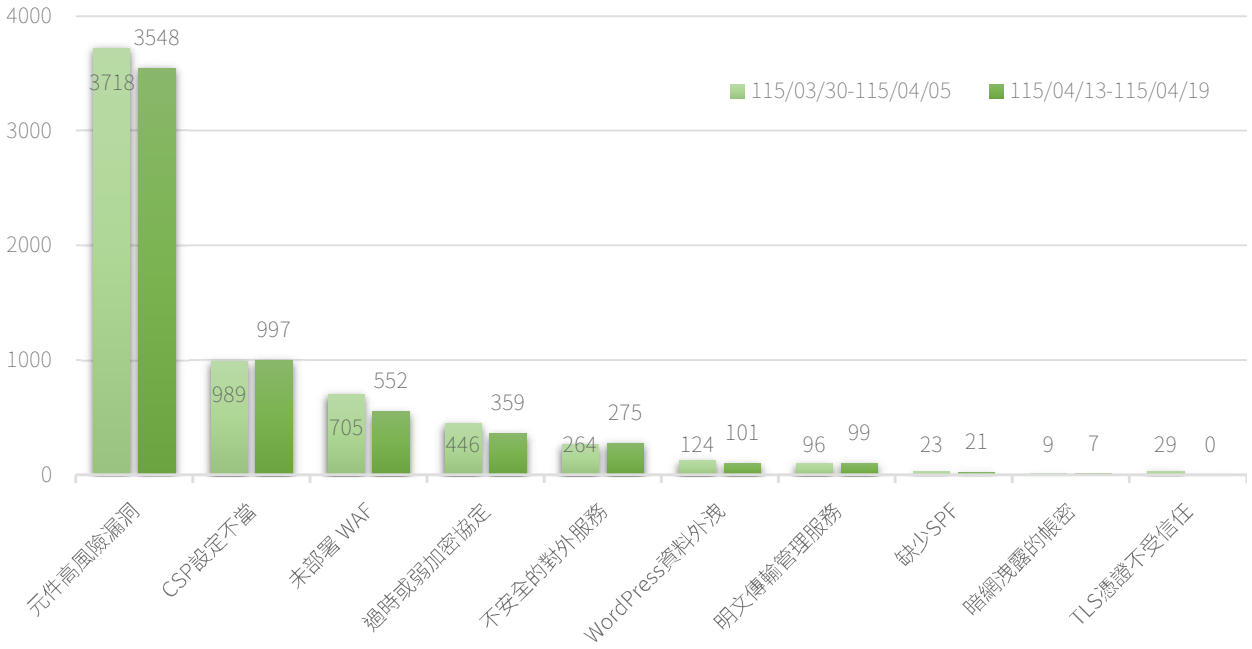

圖5 | EASM檢測結果統計(前10大風險)

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，並停用未加密或舊版加密協定 ➢ 儘速修補已知漏洞，並汰換已停止維護之軟體版本，以降低元件層級之曝險風險 ➢ 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，定期盤點已停用之站台、主機與應用服務，確認是否已確實完成下線，避免因資產未妥善關閉而持續對外暴露；如確有遠端管理需求，應嚴格限制來源IP，並採用加密通道(如SSH)進行存取	➢ 定期盤點並更換外洩帳號憑證，並搭配多因素驗證(MFA)機制，以強化存取控制安全性 ➢ 建立系統性之弱點修補與驗證機制，確保風險改善成效可持續追蹤與落實 ➢ 強化資安教育訓練，提升系統維運人員對憑證管理、加密保護及服務安全設定之認知與實作能力

焦點文章

從交友、素食到公益 「先養後殺」社群詐騙正席捲日常生活

看似單純的興趣社團與資訊分享，其實是長期經營的信任攻擊

當詐騙不是從陌生電話開始，而是從「想過更好生活」開始...
2025年8月，一名民眾在一個以素食、修行、慈善為主題的 LINE 社群內，認識一位自稱熱心分享「善行」觀念的成員。對方長期在群內轉發勵志文章、推廣「行善積德」，很快取得大家信任。某天，這位成員私訊他，介紹一個名稱聽起來相當「正能量」的方案——「食素修德與善同行之善緣基石：300 萬元扶持善因素心方案」，強調「既能幫助弱勢，又能穩定理財」，完全貼合群組一貫的價值觀。

受害人依指示下載虛擬貨幣 App、透過指定換匯管道，在全聯停車場把 300 萬現金交給自稱「專員」的人，事後收到看似正式的 USDT 入帳截圖，但錢包裡始終沒有任何進帳，才驚覺自己掉進一個從素食社群慢慢培養信任、最後一次收割的大型陷阱。

這不是單一個案，而是「先養後殺」（又稱「養套殺」、「殺豬盤」）在台灣日常社群中的最新變形——它不再只從愛情交友或高報酬投資切入，而是從你覺得「很健康」、「很公益」、「很日常」的生活圈開始。

刑事局：生活化活動成為最新誘餌

刑事局2025年8月公布「165 打詐儀錶板」最新統計時就提醒，詐騙廣告樣態已經「進化」：不再只打「高獲利、穩賺不賠」等投資字眼，而是以司機招募、親子活動、夏令營、植物交流、素食推廣等日常主題包裝，實際目的是引導民眾加入特定 LINE 群組，再進一步進行投資詐騙、竊取個資，甚至招募車手。

也就是說，你以為只是幫小孩找夏令營、找人一起跑步、加入素食社團，背後可能早就有一整套「先養後殺」劇本在運作，詳見圖6。

焦點文章

事實查核平台 MyGoPen 今年陸續接到多起回報，出現一類常見貼文描述「尋找運動、公益、登山活動夥伴」，用「志同道合、一起跑步、一起做志工」等文字吸引有心想運動、想做公益的人，之後透過私訊邀請加好友，接著再拉進投資群組，慢慢把話題從活動轉向「高報酬投資」。MyGoPen 分析，這類廣告有幾個共通點：一開始強調的是「夥伴」、「熱血」、「公益」，讓你先相信「這裡的人跟我價值觀相近」，之後才慢慢導向理財與投資話題。

圖6 |生活化活動成為最新誘餌示意圖

假素食真投資：以愛心、善行包裝的養套殺

這些人可能不是貪心，只是想結交朋友、運動健康、做善事。詐騙的新戰場，就是我們以為最安全、最單純的『同好社群』。

宗教與素食社群也成了新戰場。最近有詐騙集團假冒素食品牌，打著「試吃體驗」、「分享素食資訊換禮券」名義吸引人加入 LINE 群組，先在群內塑造「善行、愛心」形象，再進一步推銷所謂「善循環投資」，甚至以假案例營造高獲利，最後讓參與者血本無歸。

焦點文章

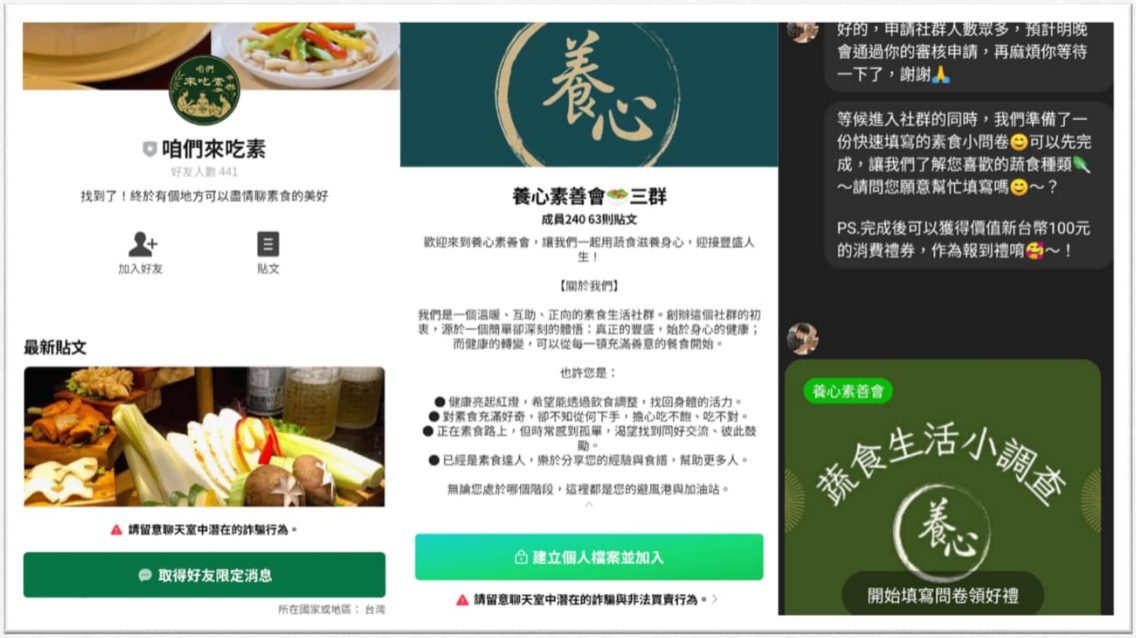

圖7 |「先養後殺」鋪陳示意圖

從案例畫面中可以清楚看到「先養後殺」是怎麼鋪陳的，詳見圖7。左邊看起來像是一個單純的素食品牌或社群帳號，版面乾淨、菜色照片看起來健康可口，介紹文字也只是「終於有個地方可以盡情聊素食的美好」。對多數人而言，這完全符合「安全又正向」的第一印象，很難聯想到詐騙風險。中間的社群頁面則進一步包裝成「素善會」「素食生活社群」，強調互助、關懷、分享健康飲食與善行，還用條列的方式寫出社群宗旨，營造一種有制度、有理念的氛圍。

接著，真正關鍵的「養」出現了。畫面右邊的對話內容顯示，管理者在你申請加入社群之後，會私訊表示「人數眾多，需要審核」，一方面讓你覺得這個社群很熱門，另一方面也提高被選上、被「接納」的期待感。緊接著，他們提出一份「快速填寫的素食小問卷」，說是為了了解你的飲食習慣，並且承諾填完可以獲得百元禮券當作禮物。表面上只是調查素食生活方式，實際上卻藉由問卷一步步蒐集你的姓名、年齡、職業、收入、家庭狀況與聯絡方式，為後續推銷投資方案、評估你「可以下手的程度」做準備。

從資安角度看，這樣的流程其實已經具備一個完整的「行銷漏斗」：入口是看似無害的素食資訊與社群認同，中段是問卷與建檔，出口則是後續一對一的投資邀約或「善行理財方案」。也就是說，真正的關鍵風險並不在畫面上那幾道菜或那句「一起養身養心」，而是在

焦點文章

你一邊感到被接納、一邊交出越來越多個人資訊的過程。當詐騙集團掌握了你的經濟壓力、家庭結構、宗教或飲食信仰，再加上長期聊天建立的情感連結，要說服你拿出大筆資金，其實就只是時間問題。

「先養後殺」在社群裡怎麼運作？四階段劇本拆解

雖然每個案件標題內容不同，但概念非常相近，可以用四個階段來深入理解：

第一步：拉人進場

靠興趣、親子公益吸睛，此時完全不談投資、不談錢，只有共同興趣與價值觀

一開始，詐騙集團會先在 Facebook、IG 等平台大量投放廣告，主題看起來都很生活化，例如「親子免費體驗」、「徵跑步夥伴」、「揪團登山」、「素食餐廳好康」、「公益志工招募」等等，讓人直覺聯想到的是健康、家庭與助人，而不是金錢與投資。另一種做法，是長期潛伏在既有的興趣社團裡，零星分享看似有用的資訊與心得，慢慢建立「資深群友」、「熱心大哥大姐」的形象。這個階段幾乎完全不談投資、不談錢，只有共同的興趣與價值觀，看起來就像一般社群裡的正常互動。

第二步：慢慢「養」

透過互動、情緒價值、共感理念把你養成「願意聽他說話、願意相信他的人」

當你加入社群後，這些看似熱心的成員會開始在群組裡頻頻回覆你的問題、幫你的貼文按讚，偶爾主動關心你的工作、家庭或健康狀況，讓你覺得「這裡的人很真、很親切」。在素食、宗教或公益相關的群組裡，他們會不斷強調「行善積德」、「照顧弱勢」、「一起為社會做點事」等口號，營造出一種充滿愛心與使命感的氛圍，讓你的防備心慢慢放下。到了某個時間點，對方可能會改用私訊，分享自己的「人生故事」與「轉折經歷」——這些故事聽起來很真實，其實是精心編排好的腳本。透過長期陪伴和頻繁互動，他們把你養成一個「願意聽他說話、願意相信他的人」，這就是「先養」的核心。

焦點文章

第三步：開始下圈「套」

小額投資、名義募款、私下連結，一切行動都是為了步入信任陷阱

關係經營到一定程度，詐騙者會悄悄把話題轉向金錢，但一開始多半非常「溫和」。他們可能提出一個「小額、短期、風險低」的投資機會，說是群裡幾個人一起參與的虛擬貨幣專案，還搭配一句「因為你很認真參與公益／素食，所以特地偷偷拉你進來」，讓你感覺自己是被特別看重的少數。也可能打著「善心」與「助人」名義，包裝看似兼具慈善與理財功能的方案，例如某些案件中的「善因素心方案」，標榜既可以扶持弱勢、又能替家人累積資產。這時，他們會要求你加入另一個「核心投資群」、「內圈群」，或下載指定的理財App、加某個專員的LINE，讓你完全走進他們掌控的封閉空間。為了加深你的信任，對方還可能先讓你看到幾筆「試單」的小獲利，透過偽造的對帳單、入帳截圖，或者讓群組中的暗樁貼出「今天又賺多少」的截圖，營造一種大家都在穩定獲利的假象。

第四步：最後「殺」豬離場

高額匯款、掏空資產，甚至再來一輪二次詐騙

當你開始投入數十萬、數百萬，或交出大量個資之後，劇本就進入收割階段。投資平台可能會突然出現各種理由，例如「系統維護」、「帳戶異常凍結」、「需要再加碼才能解鎖出金」，逼你不斷投入更多資金。等到你終於起疑，對方有時會換上一套新角色，以「協助追回損失」為名安排假律師、假顧問出場，誘使你再付一次法律費、服務費，形成所謂的「二次詐騙」。如果你拒絕配合，對方多半就直接消失，留下的是空掉的群組、關不掉的聊天紀錄，以及受害者心中揮之不去的羞恥與自責。

這整套從「拉人進場」到「最後一殺」的劇本，已經在國內外無數投資和愛情詐騙案件中被反覆驗證。

資安與金融監理單位的分析都指出，先透過長期互動建立情感或價值認同，再把人導流到特定投資平台或要求私下匯款，已經成為典型的「殺豬盤」模式。差別只在於，現在這些劇本披上的外衣，不再只是浪漫愛情與暴利投資，而是你以為最安全的「興趣社團」與「善行社群」。

焦點文章

為什麼「認真生活的人」特別容易被「先養後殺」？

素食群組、親子活動到公益社團，實務上看到的受害者，往往不是那種「想一夕致富」的人。很多是想讓孩子多參加活動、有更好資源的家長；是下班後真心想運動、想交朋友的上班族；也是對宗教、善行有熱情、願意付出的信徒或素食者。換句話說，他們的動機其實都很單純——只是想把生活過得好一點，想和一群理念相近的人在一起。

詐騙集團看準的，就是這樣的心理。第一個關鍵是「歸屬感與認同需求」。在興趣社群裡被按讚、被稱讚、被喊名字，會讓人很自然把這個群體當成「自己人」。久而久之，很多人會不自覺地把「大家都這樣說」等同於「風險大家一起承擔」，對風險的敏感度就被稀釋掉了。

第二個關鍵是「認知負荷轉移」。當你長期把某個社團、某個管理員當成資訊來源，「他都幫我查好了」「他人這麼好，應該不會害我」這種想法就會慢慢浮現。久了，對活動來源、公司背景、投資標的是否真的存在，反而不太會再額外查證，因為大腦已經把這件事外包給「群體」了。

第三，是很多受害者心裡其實想的不是賺大錢，而是「不要落後」。在包裝成善行或公益的投資案裡，詐騙者會不斷強調「既能幫助別人，又能讓自己的錢更有力量」。面對群組裡一張張「已經匯款」「已經領回利息」的截圖，真正的壓力往往不是「我要不要暴富」，而是「如果我不跟上，是不是錯過一個又善良又划算的機會」。這種「我不是貪心，只是怕自己錯過」的 FOMO，比單純的高獲利誘惑更有殺傷力。

最後，是常被忽略的「羞恥感」。一旦發現自己受騙，很多人腦中冒出的第一句話是：「我平常這麼認真、這麼小心，竟然會在素食群、親子活動裡被騙？」這種自責會讓人不敢對家人、朋友，甚至警方開口，更不會主動在社群裡提醒其他人。結果就是，明明已經有好幾個人先跌倒，整個社群卻看起來一片風平浪靜，讓同樣的手法可以一再重複。

焦點文章

實務防範：對個人、社群管理者與機關的三層防線

看完前面的案例與分析後，我們繼續探討具體可行的防範建議：

（一）一般民眾：看到這些情境時先按下「暫停鍵」

對多數人來說，最實用的第一步，是把「活動／社團＋加 LINE／加好友」視為高風險組合。只要遇到任何活動貼文，要你留言 LINE ID 或私訊加陌生帳號，就先把它當成紅色警訊，而不是覺得「這樣聯絡比較方便」。事實查核單位過去就發現，有些詐騙粉專會直接偷用真實活動的照片與文字，貼文本身是假的，真正目的只是把你的帳號「撈進來」，方便後續一對一詐騙。

一旦對話開始談到投資、金錢或匯款，就更需要刻意「換場景」查證。不要邊跟對方聊天邊 Google，也不要只在原來的群組裡問「這個是不是安全」。比較好的做法是跳出對話，改用官方網站、165 反詐騙專線、獨立新聞報導等管道重新檢查，避免被群體氛圍壓著走。

在工具設定上，也有一些可以立刻做的事。例如在 LINE 裡關閉「允許利用 ID 加入好友」，可以降低被陌生帳號主動加好友的機率；收到陌生帳號邀請時，也盡量不要因為共同朋友很多就放下戒心。至於金額較大的投資，不論對方看起來多熱心、多「有緣」，都應該只透過合法金融機構與監理機關核准的平台進行。任何強調「內圈群組」「私下機會」「不要對外說」的投資邀約，都可以直接歸類到高風險區。

（二）社團版主、主揪：讓社群本身長出「防詐公約」

對社群管理者來說，真正有力量的防護不是事後刪文，而是事先訂規則。可以在社團簡介或置頂貼文中明確寫出幾條原則，例如「本社團禁止推銷投資產品與借貸」「不討論任何代收、代付、代開帳戶相關內容」，讓成員一開始就知道這裡對金流議題是高度敏感的。

同時，也要鼓勵成員「覺得怪就問」，甚至提供匿名管道讓大家回報可疑帳號。當版主收到回報時，可以先提醒全體成員留意相關帳號的貼文與私訊，必要時協助蒐證並封鎖對方，而不是擔心「這樣會不會太小題大作」。如果社團本身能養成「懷疑是正常的」文化，任何想在裡面養套殺的詐騙者，壓力就會大很多。

焦點文章

版主也可以定期轉貼刑事局165、MyGoPen 、台灣事實查核中心等單位整理的最新詐騙案例，用實際故事提醒大家，即使主題是素食、親子或運動，也可能被拿來當作詐騙誘餌。這種「社群內部的防詐教育」，往往比單向的官方宣導更能打到目標族群。

（三）公部門與平台：從個案處理走向「模式偵測」

最後一層，是政策與平台的角色。公部門已經開始透過 165 儀錶板彙整「最新詐騙廣告樣態」，讓民眾可以看到近期常見的假活動、假社團主題，這有助於掌握趨勢、調整宣導重點。但在「先養後殺」型的社群詐騙上，還需要更多針對模式的偵測與因應。

例如，平台端可以針對短時間內大量投放、內容高度相似的活動廣告建立風險模型，對頻繁導向特定 LINE 帳號或外部網址的貼文提高審查門檻；在接獲事實查核單位或警方通報時，也應該有更快速的下架與凍結流程，避免同一組圖文一再出現在不同粉專和社團之間流竄。公部門則可強化與事實查核組織、平台業者的合作機制，讓「發現新型態 → 快速警示 → 儘早下架」變成常態流程，而不是每次都從個案開始、慢慢重複。

當個人懂得按下暫停鍵、社群願意建立防詐文化，平台和機關又能及早偵測異常模式時，「先養後殺」這種長期培養信任的詐騙手法，就比較難在我們以為最安全的生活圈裡，悄悄養肥下一個獵物。

關鍵字：先養後殺詐騙、社群滲透與信任建立、假公益／素食投資誘導

刊　　名　資安週報第 41 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