資通安全網路月報

一、資安長話短說

當 AI 進化為專屬助理，享受高效便利時，不可不知的五大資安防線

隨著人工智慧（AI）技術快速發展，具備自主執行能力的「代理型 AI（AI Agent）」逐漸成為焦點。近期廣受社群熱烈討論的開源專案 OpenClaw（俗稱小龍蝦或龍蝦），正展現了這股浪潮。這類工具不僅能主動完成任務、串接外部服務，甚至操作作業系統，讓 AI 從單純的輔助工具，蛻變為無所不能的全能數位管家。

代理型 AI 聰明與高效率，更得防範其潛在風險

然而，在享受 AI 帶來的極致效率時，是否也將系統大門敞開？隱含資安威脅？為實際瞭解代理型 AI 的應用服務，訪談使用人士，受訪者表示平時運用 OpenClaw 登載行事曆及採買生活用品、比價等非敏感性事務，發現此工具確實帶來極大便利性。過去需要自己整理的資料，現在只要下達指令或截圖，AI 助理就能直接完成。受訪者甚至表示，龍蝦非常聰明且學習極快，回應就如同真人一般。不過，受訪者在導入初期便意識到其潛在風險，與一般生成式 AI 不同，OpenClaw 可以自主連接外網、變更電腦設定，甚至安裝程式，權限與風險極高，因此該名受訪者將龍蝦安裝於雲端虛擬機（VM），與實體環境區隔，且僅用於處理一般性事務。

事實上，該受訪者的風險意識絕非多慮。這類型的 AI 代理工具，風險是全面性的。攻擊者不需要駭入主機，只要在 AI 會讀取的網頁或社群留言中埋入惡意指令，就可能誘騙 AI 幫駭客開啟後門、刪除檔

案或進行格式化；網路上供人下載的第三方「技能包（Skill）」，也可能暗藏惡意程式的下載連結或惡意指令。更別提 AI 在 24 小時運作後，為了節省記憶體，經常會觸發「記憶壓縮」而引發「失憶症」，遺忘使用者最初設定的安全守則。

導入代理型 AI 之五大安全防護建議

為了在極致便利與資安防線間取得平衡，資安署建議大家在導入這類新型 AI 工具時，可參考下列幾項做法：

(一) 落實環境隔離：安裝於獨立環境，不要把 AI 代理安裝在存放機密或日常辦公的主力電腦上，而是將它養在全新、格式化過的另一部電腦，或是專屬虛擬機（VM）、容器（Container）中。

(二) 只給「臨時通行」：為 AI 代理註冊專屬的獨立帳號（包含專用電子郵件及社群平臺帳號），避免將個人日常使用的帳號與密碼直接提供給 AI 代理。若 AI 代理必須登入外部服務，建議設定具有時效性的臨時授權憑證，時間一到權限即自動失效，避免日後因疏於管理而導致帳號遭竊。

(三) 設置人類「煞車」機制：針對高風險操作（如存取憑證、發送郵件或執行系統指令），應於系統設定中強制啟用人工審核，要求每次執行前必須經由人員手動確認方可放行。

(四) 將安全守則寫入「長期記憶」：定期檢視且備份 AI 的長期記憶檔。務必將重要的安全限制（例如：刪除郵件前必須經過人員同意）直接寫入「核心記憶檔案」（如：龍蝦的 MEMORY.md）中，確保每次運作時都會強制載入安全守則，避免因記憶壓縮而遺忘設定好的防護設定。

(五) 審慎檢查技能包：在安裝任何第三方技能擴充套件前，應先對其內容說明與程式碼進行完整的安全掃描。若發現內容中有要求下

載不明檔案、連線至不明網站等可疑行為，應立即停止安裝，並向平台檢舉。

在使用新型態軟體或服務時，皆可以掌握一個原則：「如果不能掌控或確定能避免風險的工具就要謹慎使用，在做任何事的時候都要有資安意識」。目前代理型 AI 強大的自主學習與操作能力無疑能有效提升工作效率，但唯有妥善規劃防護機制，才能真正安心享用 AI 帶來的數位便利。

二、近期資安事件分享

專案系統權限控管失效，獨立網段未納監控成資安死角

機關接獲外部情資，指出其轄內某專案系統存在權限控管失效(Broken Access Control)漏洞，非授權人員可讀取、修改或刪除專案參與者資料。經查該系統為自行開發應用，因權限驗證機制不足所致，且該專案使用之獨立網路未納入機關資安監控範圍，以致資訊單位未能即時掌握系統風險。機關已緊急中斷對外連線，並進行影響範圍釐清及修補作業。

經驗學習(Lessons Learned)

單位因業務或專案需求申請獨立網路，若未同步落實機關資安責任等級之防護要求，易形成資安監控與管理盲區。建議機關將獨立網路與專案系統納入整體資安治理範圍，並透過定期檢視與制度化管理，降低整體防護弱點：

1. 強化獨立網路納管與監控機制

各單位申請獨立網路專線時，應依機關資安責任等級要求配置必要防護措施(如防火牆、入侵偵測)，並納入機關資安監控(SOC)範圍；同時定期檢視網路架構與對外連線情形，確保所有網路均在納管範圍內。

2. 落實安全開發與權限控管檢核

針對自行開發或委外建置系統，應於開發與上線過程納入資安檢核，特別強化權限驗證機制設計；上線後定期進行弱點掃描或檢測，並持續追蹤修補情形。

3. 建立盤點與內部稽核機制

定期盤點對外線路與連網設備，避免未經核准之連線存在；並將使用獨立網路之專案納入內部稽核與定期檢視範圍，確保其防護措施持續有效並符合機關資安要求。

三、資通安全趨勢

(一) 我國政府整體資安威脅趨勢

【事前聯防監控】

本月蒐整政府機關資安聯防情資共 7 萬 3,093 件(較上月增加 1 萬 2,329 件)，分析可辨識的威脅種類，第 1 名為資訊蒐集類(49%)，主要是透過掃描、探測及社交工程等攻擊手法取得資訊；其次為入侵嘗試類(24%)，主要係嘗試入侵未經授權的主機；以及入侵攻擊類(11%)，大多是系統遭未經授權存取或取得系統/使用者權限。統計近 1 年情資數量分布，詳見圖 1。

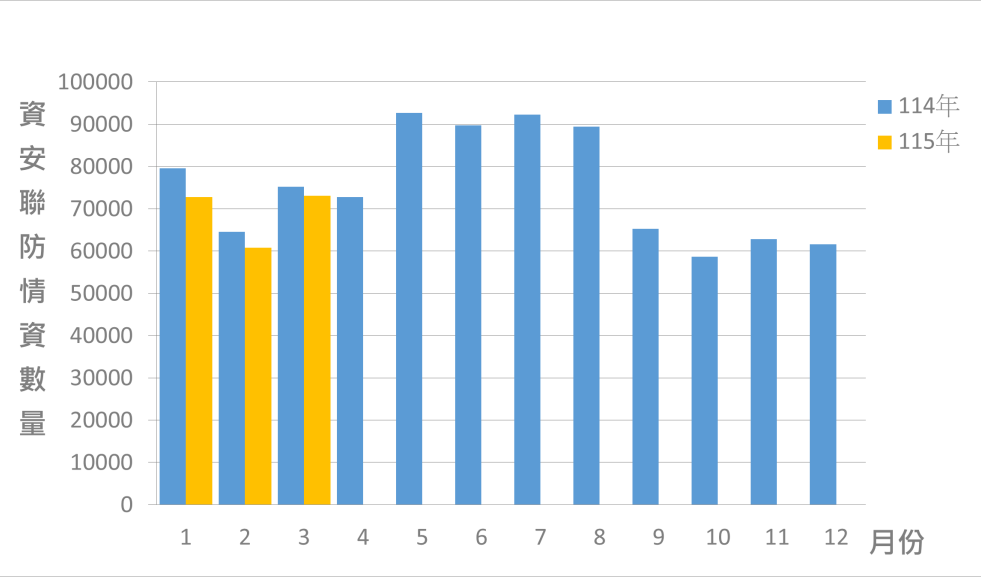

圖 1 資安聯防監控資安監控情資統計

從釣魚信件到記憶體執行：PowerShell 隱蔽攻擊剖析

經進一步彙整分析聯防情資資訊，發現近期駭客透過社交工程郵件誘導使用者執行捷徑檔，進而觸發多階段 PowerShell 腳本，從合法雲端服務下載並在記憶體中執行惡意程式，以降低被偵測的風險，駭客所使用之離地攻擊手法，使惡意程式可直接於記憶體中執行，可避免檔案落地至硬碟，從而降低被防毒軟體或資安設備偵測之機率，相關情資已提供各機關聯防監控防護建議。

【事中通報應變】

本月資安事件通報數量共 55 件，為去年同期的 0.67 倍，通報類型以非法入侵為主，占本月通報件數 65.45%。本月持續發現多個機關因安裝冒牌軟體而遭植入惡意程式之情形。過往相關案例多以冒牌通訊軟體為主要手法，惟近期觀察攻擊者已逐步擴展至其他類型軟體，肇因為「使用/下載來源不明之應用程式/套件」的事件總數占總通報件數 10.90%。近 1 年資安事件通報統計詳見圖 2。

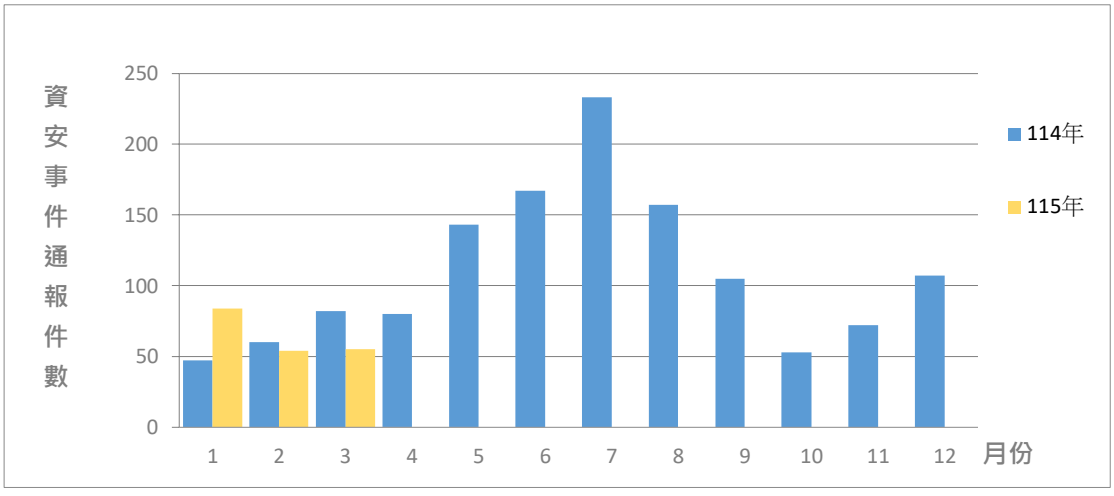

圖 2 資安事件通報統計

(二) 重要漏洞警訊

警訊	類別	內容說明
漏洞警訊	**備份與復原系統** Veeam Backup & Replication 嚴重程度：最高 CVSS 9.9 （CVE-2026-21666、CVE-2026-21667、CVE-2026-21668、CVE-2026-21669、CVE-2026-21670、CVE-2026-21671、CVE-2026-21672、CVE-2026-21708）	• 研究人員發現 Veeam Backup & Replication 存在 8 個高風險安全漏洞，類型包含遠端執行任意程式碼（RCE）本機提權等。 • 影響最嚴重之漏洞，可使已通過身分鑑別之攻擊者或低權限角色於備份伺服器遠端執行任意程式碼。 • 官方已釋出修補版本，建議儘速更新版本。 參考資料：https://www.veeam.com/kb4830、https://www.veeam.com/kb4831
	網路交換器 HPE Aruba Networking AOS-CX 交換器 嚴重程度：最高 CVSS 9.8 （CVE-2026-23813、CVE-2026-23814）	• 研究人員發現 HPE Aruba Networking AOS-CX 交換器存在身分鑑別繞過與指令注入漏洞。 • CVE-2026-23813 可使未經身分鑑別之遠端攻擊者繞過驗證，部分情況下甚至可重設管理員密碼；CVE-2026-23814 則可使低權限遠端攻擊者注入惡意命令。 • 官方已發布安全公告，請儘速依受影響版本套用修補更新。
	身分識別與中介軟體 Oracle Identity Manager 與 Oracle Web Services Manager 嚴重程度：CVSS 9.8 （CVE-2026-21992）	• Oracle Identity Manager 與 Oracle Web Services Manager 存在缺乏身分鑑別（Missing Authentication）漏洞。 • 未經身分鑑別之遠端攻擊者可利用此漏洞執行任意程式碼。 • Oracle 已發布 Security Alert，建議立即依官方公告修補。
已知遭駭客利用之漏洞	**協作與文件平台** Microsoft Office SharePoint 嚴重程度：CVSS 8.8 （CVE-2026-20963）	• Microsoft Office SharePoint 存在反序列化不受信任資料漏洞。 • 未經身分鑑別之遠端攻擊者可利用此漏洞執行任意程式碼。 • 官方已針對漏洞釋出修復更新，請參考官方說明進行更新。

	端點管理系統 Ivanti Endpoint Manager (EPM) 嚴重程度：CVSS 8.6 （CVE-2026-1603）	• Ivanti Endpoint Manager 存在身分鑑別繞過漏洞。 • 未經身分鑑別之遠端攻擊者可取得特定身分鑑別資料。 • 官方已針對漏洞釋出修復更新，請參考官方說明進行更新。
	網頁瀏覽器 Chromium 為基礎之瀏覽器 嚴重程度：最高 CVSS 8.8 （CVE-2026-3909、CVE-2026-3910）	• Google Chrome 與其他以 Chromium 為基礎之瀏覽器存在 Skia 越界寫入與 V8 不當實作漏洞。 • 攻擊者可藉由特製 HTML 頁面觸發越界記憶體存取或在沙箱環境內執行任意程式碼。 • 建議儘速更新 Chrome 版本，並同步確認 Edge、Brave、Vivaldi、Opera 等相關瀏覽器更新狀態。

警訊說明：

「漏洞警訊」: 為已驗證漏洞但尚未遭攻擊者大量利用，修補速度建議儘快安排更新。

「已知遭駭客利用之漏洞」: 已知有漏洞成功攻擊情形，建議即刻評估修補

四、國際資安新聞

➢ CISA 確認 FileZen CVE-2026-25108 漏洞已被利用 (資料來源：The Hacker News)

CISA 確認 Soliton Systems FileZen 檔案傳輸軟體中存在嚴重作業系統命令注入漏洞 CVE-2026-25108 (CVSS:8.7) 已被利用。此漏洞允許具有普通權限的使用者透過 HTTP 請求執行任意作業系統命令，進而可能導致系統被入侵。此漏洞影響 FileZen 4.2.1 至 4.2.8 版本以及 5.0.0 至 5.0.10 版本。Soliton 表示，啟用「防毒檢查選項」時，漏洞可被利用，並已報告至少一起利用事件。該公司建議用戶立即升級至 5.0.11 或更高版本，並更改所有用戶密碼以降低風險。CISA 將該漏洞添加到其已知利用漏洞(KEV)目錄中，並建議聯邦民事行政部門(FCEB) 機構在 3 月 17 日之前應用修復程序。

➢ **有人公開洩漏了一款可入侵數百萬支 iPhone 的漏洞工具包**
(資料來源：Tech Crunch)

一款名為 DarkSword 的駭客工具包新版本已在 GitHub 上洩漏並發布，使得攻擊者能夠輕鬆利用運行舊版 iOS 系統(尤其是 iOS 18 或更早版本)的 iPhone 和 iPad 的漏洞。該工具包由 HTML 和 JavaScript 構成，結構簡單，這意味著即使技術水平有限的攻擊者也能快速部署。DarkSword 讓攻擊者可以從 iPhone 或 iPad 中讀取並竊取具有取證價值的文件，包括聯絡人、簡訊、通話記錄和 iOS 鑰匙圈秘密，並將這些文件傳送到攻擊者控制的伺服器。蘋果已經意識到該漏洞針對運行舊版作業系統的設備，並於 3 月 11 日發布緊急更新，以修復無法運行最新 iOS 版本的設備。蘋果也建議用戶啟用鎖定模式以降低風險。

五、資安宣導資訊

為提升各機關弱點管理效能，優先處理關鍵風險，本署 VANS 已綜整 3 項國際資安漏洞評估指標供參考

(一)考量資安威脅趨勢遽增與弱點管理實務需求，為協助各機關強化資通系統與相關資產的弱點管理效能，本署資通安全弱點通報系統(VANS)現已納入下列 3 項國際常用資安漏洞評估指標；機關可透過綜合運用漏洞評估指標資訊，掌握需優先處理的關鍵風險：

1. CVSS (Common Vulnerability Scoring System): 係指漏洞的嚴重程度指標，現由國際組織資安事件應變小組論壇 (FIRST) 所維護。該指標將漏洞技術細節量化為 0.0 至 10.0 分，並區分為嚴重(Critical，9.0~10.0)、高(High，7.0~8.9)、中(Medium，4.0~6.9)、低 (Low，0.1~3.9) 及無 (None，0.0) 等嚴重等級。
2. KEV (Known Exploited Vulnerabilities): 係指已知被利用的資

安漏洞清單，由美國網路安全暨基礎設施安全局（CISA）所維護，透過評估漏洞遭利用之真實情況，提醒機關優先處理已遭駭客利用於網路攻擊的漏洞，以降低重大資安風險。

3. EPSS（Exploit Prediction Scoring System）：係指預測漏洞被利用機率指標，由國際組織資安事件應變小組論壇（FIRST）所提出。該指標透過機器學習模型預測漏洞於未來 30 天內被駭客利用的可能性(以 0 至 1 分呈現，代表機率為 0%至 100%)。

(二)應用範例：針對 CVSS 7.0 以上且標示為 KEV 的資安漏洞，優先投入資源，即時修補或採行緩解措施，並得使用 EPSS 排序進一步決定處理順序。

(三)上述功能操作說明，均已同步更新 VANS 教育訓練教材並公告於國家資通安全研究院官網 VANS 專區 https://gov.tw/Q47，如參閱教材後仍有系統操作疑問，可逕洽技術客服窗口，聯絡電話(02)6631-6423，電子信箱 Vansservice@nics.nat.gov.tw。

六、近期重要資安會議及活動

日期	活動/會議	對象
5 月 6 日上午	資安長共識營	行政院所屬二、三級機關、行政院所屬四級機關（構）、行政法人，且資安責任等級為 A 級者及各縣市政府
5 月 6 日下午	資安之友	資安在學或在職之專業人員（如菁英班結訓學員、網路攻防演練攻擊手、DEFCON CTF 決賽參加隊伍選手、公協會成員等）