資通安全網路月報

一、資安長話短說

(一)美國 AI 政策展現「創新與安全並重」的特色

2026 年 6 月 2 日，美國總統川普簽署「促進先進人工智慧創新與安全」（PROMOTING ADVANCED ARTIFICIAL INTELLIGENCE INNOVATION AND SECURITY）行政命令，顯示美國 AI 政策「創新與安全並重」的治理模式。

(二)行政命令核心內容

該行政命令主要圍繞在「公私協力、提升防禦、打擊犯罪、拒絕過度監管」，並提出以下多項限期具體行動：

1. **升級聯邦與關鍵基礎設施的系統防禦以因應先進 AI（30 天內）**：應優先升級國家安全系統及戰爭部資訊系統之網路防禦能力；以及提供網路安全工具和服務給偏遠醫院、社區銀行及地方公用業事公司。
2. **建立國家級漏洞資訊中心（30 天內）**：由美國財政部、戰爭部及國土安全部協商，並與自願參加的 AI 產業和關鍵基礎設施提供者，共同建立「國家級漏洞資訊中心(暫譯)」（AI cybersecurity clearinghouse），該中心負責協調軟體漏洞掃描作業，並揭露及驗證此類漏洞，以及處

理後續漏洞修補及發布修補程式等作業。

3. **盤點可用預算以研發 AI 漏洞偵測（30 天內）**：美國行政管理和預算局應與國家網路安全局協調，盤點聯邦可用資金，用於資助研發先進 AI 漏洞檢測技術的申請人。

4. **建立「受監控前沿模型」基準測試與評估機制（60 天內）：**

(1) 制定基準測試流程（Benchmarking Process），用來評估 AI 模型的進階網路能力，並用來界定 AI 模型屬於「受監控前沿模型(covered frontier model)」。

(2) 設計自願性框架（Voluntary Framework）：與 AI 開發者共同設計一個自願參與的框架，開發者與聯邦政府合作，確定正在開發的模型是否符合「受監控前沿模型」的定義；在發布「受監控前沿模型」之前，提前 30 天給聯邦政府使用，並與聯邦政府選擇可信賴的合作夥伴，使其能夠儘早使用「受監控前沿模型」，以研發創新的安全技術，及強化關鍵基礎設施的防護能力。

(3) 針對開發或發布的新 AI 模型（包括前沿模型），皆不建立政府許可制度（Licensing）、預先核准制度（Preclearance）及授權制度（Permitting）。

5. **擴大招募網路安全專家（60 天內）**：美國人事管理辦公室應擴大美國技術部隊（Tech Force Information Cybersecurity）之資訊網路安全

專家的聘用管道與人員招募。

6. **強力打擊 AI 網路犯罪：**優先打擊利用 AI 未授權系統存取、資料竊取、系統破壞、網路犯罪等行為，以及利用 AI 代理（AI agents）非法存取資訊系統或資料等行為。

(三)前沿 AI 模型對我國資安影響與後續因應

從以上美國最新公布的行政命令，可以發現面對新型態 AI 威脅，美國採取開放的態度與民間建立起密切的關係，一同挖掘漏洞、一同建置漏洞資訊中心、一同界定前沿 AI 模型等，一邊加速發展，也不忘持續加強國家重要系統的防護。而數位發展部資通安全署在面對這波 AI 威脅浪潮，仍持續積極面對，除了上個月對外說明應回歸資安基本功，強化資安策略面、管理面、技術面，以及提出「迅速復原」的資安策略，之後將規劃出漏洞修補 SOP、並試圖運用 AI 來檢測重要系統，同時籌組資安菁英，邀請資安專長人員支援國家級資安任務，從各面向精進我國因應前沿 AI 資安因應策略，期強化我國韌性復原力。

二、近期政策重點

(一)為協助企業強化資通訊產品漏洞處理能力，115 年 5 月 15 日已提供 35 家公司產品安全事件應變機制（PSIRT）量測結果，並持續輔導廠商建立相關機制。

(二)預計 2027 年辦理的跨國網路攻防演練，將轉型以藍隊為主之賽制，2026 年將自主建置演練平臺，並扶植國內資安業者。演練重點將對齊 MITRE D3FEND(美國資安技術知識庫)的關鍵防禦能力框架，設計以事件為主之場域與情境，以 AI 生成自動化攻擊腳本，模擬駭客外部至機關內部各階段之真實駭侵攻擊手法。

三、近期資安事件分享

機關後台管理介面暴露與存取控制缺失

近期於網路攻防演練執行期間，發現有機關的網站可透由調整網址路徑方式，成功繞過登入驗證進入機關的後台管理介面，並修改網站公開頁面內容，反映網站後台即便未設置於前台或未對外公告，只要相關頁面仍存在且可被外部存取，即可能遭掃描工具或攻擊者發現並進一步利用。另外，攻擊者往往先藉由路徑掃描蒐集可用資訊，掌握系統中可能存在之管理頁面、測試功能或隱藏入口，再作為後續弱點探測、登入測試或功能濫用等惡意行為。

經驗學習(Lessons Learned)

網站後台或功能入口即使未設於前台選單或未對外公告，若相關頁面仍存在且可由外部存取，仍可能遭路徑掃描工具發現，並作為後續探測或利用之起點。尤其當登入驗證、授權檢查或網址存取限制未妥善實作時，攻擊

者即可能由「找到入口」進一步發展為「成功存取與操作」，造成網站內容遭竄改或非公開功能遭濫用，建議機關從下列面向持續強化防護作為：

1. 定期清理正式環境中不必要之頁面與功能，包括測試頁面、舊版後台、備份檔案或未使用功能，避免因系統改版或維護後未清理而留下可被探測之入口。
2. 落實後台與敏感功能之驗證及存取控制，不應僅以「未公開網址」作為保護方式，仍應確實執行登入驗證、權限檢查及必要之來源限制，避免在入口遭發現後仍可被直接利用。
3. 進行自主檢查，透過網站巡檢、路徑掃描或弱點掃描等方式，確認是否仍存在不應暴露之頁面、目錄或功能入口，及早發現並修正風險。
4. 檢視網站程式與設定是否洩漏路徑資訊，包括前端原始碼、JavaScript、錯誤訊息、robots.txt、sitemap 或其他設定檔，避免間接暴露管理路徑或功能位置。

四、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 8 萬 7,511 件(較上月減少 1,735 件)，分析可辨識的威脅種類，第 1 名為資訊蒐集類(48%)，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(29%)，主要係嘗試

入侵未經授權的主機；以及入侵攻擊類(10%)，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。

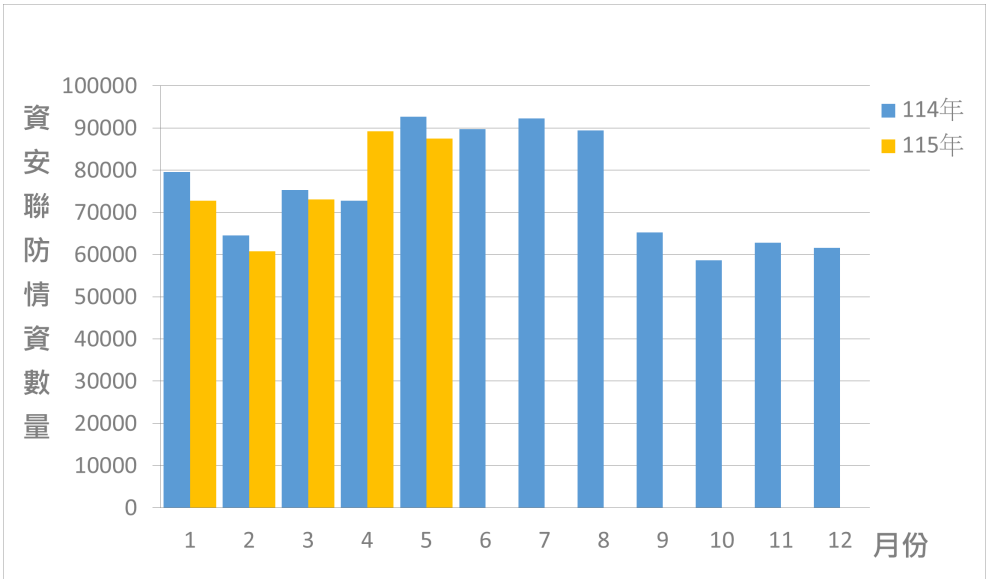

圖 1 資安聯防監控資安監控情資統計

駭客濫用免費圖片分享空間作為惡意檔案散布平台

經進一步彙整分析聯防情資資訊，發現近期駭客以「政治獻金申報異常需補件」為由，針對特定機關窗口發動社交工程攻擊。駭客於郵件主旨中強調「逾期將移送監察院裁罰」，營造具法律效力與急迫性之假象，藉此提高收件者點選惡意下載連結之意願。本次攻擊中，駭客先入侵一般民間網站並植入網頁後門腳本，作為導轉頁面使用，再將惡意壓縮檔放置於 Dropbox 雲端空間，最後於社交工程郵件中內嵌完整導轉網址，以降低資安防護設備對惡意連線與檔案下載行為之偵測與阻擋機率，進而提升攻擊成功率，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 106 件（包含攻防演練數量 40 件），為去年

同期的 0.74 倍，通報類型以非法入侵為主，占本月通報件數 55.66%。本月觀察發現，多起事件之受害設備為監視器與刷卡機等設施，多未設置防火牆或存取控管機制，亦未定期進行安全性檢查或韌體更新。近 1 年資安事件通報統計詳見圖 2。

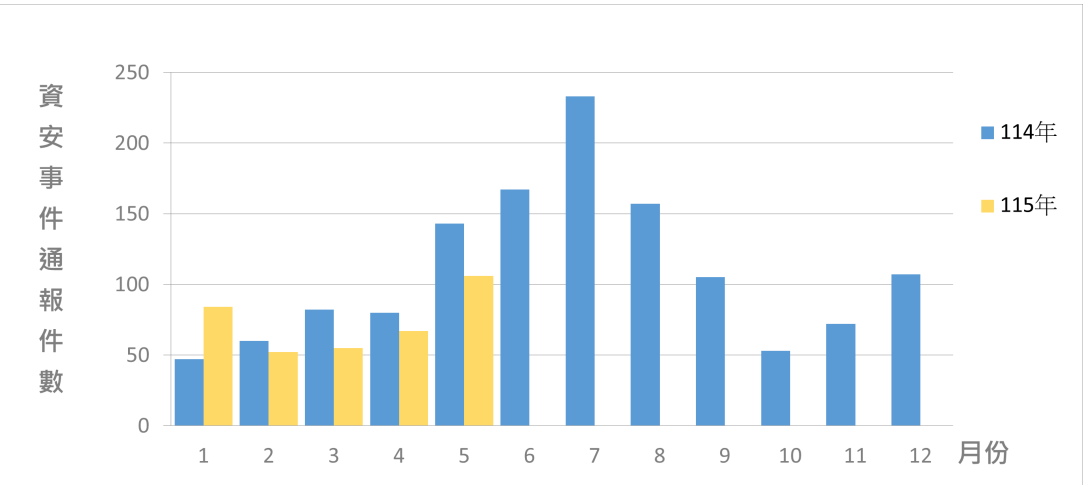

圖 2 資安事件通報統計

(二) 重要漏洞資訊，詳請參考附錄。

五、國際資安新聞

CISA 及其合作夥伴發布 AI 代理工具的安全新指南

(資料來源：Cyber News)

4 月 1 日，CISA 聯合英國、加拿大、澳洲及紐西蘭等國的網路安全機構，共同發布人工智慧（AI）代理安全指南。該指南指出，隨著 AI 代理在關鍵基礎設施及國防領域的應用日益普及，相關風險亦隨之增加，因此需建立更

完善的安全控管措施。CISA 表示，AI 代理能夠在有限的人為介入下，自主進行規劃、推理及執行多步驟任務，但若缺乏適當管理，可能導致生產力下降、服務中斷、隱私資料外洩，甚至引發網路安全事件。指南將相關風險歸納為五大類別，包括權限管理、設計與配置、行為控制、系統架構及問責機制。CISA 並指出，現行安全框架尚不足以全面因應這些風險，未來仍需透過持續研究與跨國合作，進一步強化 AI 代理的安全治理能力。

微軟：全球網路安全機構發布 AI 軟體物料清單 (SBOM) 指南，以因應 AI 供應鏈風險

(資料來源：Info Security)

作為七國集團（G7）網路安全工作小組成員的多個政府網路安全機構，近日共同發布一份 AI 軟體物料清單（AI SBOM）指引，旨在建立 AI 供應鏈透明度與可追溯性，進一步強化供應鏈安全管理。該報告提出 AI SBOM 的最低資訊要素架構，涵蓋七大類別，包括詮釋資料（Metadata）、系統層級屬性（System-Level Properties, SLP）、模型（Model）、資料集屬性（Dataset Properties, DP）、關鍵績效指標（Key Performance Indicators, KPI）、基礎設施（Infrastructure）及安全屬性（Security Properties, SP）。報告同時指出，AI SBOM 僅為提升供應鏈安全的重要基礎工具，無法單獨確保整體網路安全，仍須結合漏洞管理系統、安全公告機制及其他安全治理措施共同運作。該框架採彈性設計，可隨技術發展持續調整與演進，以因應日益複雜的 AI 供應鏈風險。

六、資安宣導資訊

(一) 調整 ISO 類資通安全專業證照採認標準與限制

有關《資通安全責任等級分級辦法》中資安專職人員持有資通安全專業證照相關規定，為兼顧實務需求與簡化規範，資安署已調整 ISO 類相關證照之認可要求，只要符合市場機制與國際採認標準，凡透過「完整課程（Full Course）」、「轉版課程（Transition Course）」或「轉換課程（Conversion Course）」所取得之合格證照，均予以採認；爰此，同步修正資安署「資通安全專業證照清單」備註中關於 ISO 類相關證照有效性之認定限制。

(二) 爭取資安最高榮耀！公務機關資安業務績效評核提醒事項

1. 為獎勵資安業務績效優良之公務機關及人員，資安署 115 年 4 月 29 日已函知各機關評核作業注意事項並公告於「資安署首頁/業務專區/公務機關資通安全業務績效評核」；再補充說明如下：

(1) 獎勵內容：

A. 機關組：特優團體獎座及獎金 12 萬元；優等團體獎座及獎金 8 萬 5,000 元；良等團體獎座。

B. 個人組：績優人員獎座及獎金 2 萬元。

(2) 評核項目「其他資通安全管理業務促進活動或特殊創新作為」占總分達 15 分，對機關成績具有關鍵性影響。機關須於 7 月 31 日前提

交書面報告送審，逾期 7 日內將酌扣分數，逾期 7 日以上則以 0 分計算。

歡迎各機關與資安同仁踴躍參與，共同展現資安防護實力，競逐最高榮譽！

參考附錄-重要漏洞警訊

警訊	類別	內容說明
漏洞警訊	沙箱分析設備 Fortinet FortiSandbox、FortiSandbox Cloud 和 FortiSandbox PaaS 嚴重程度：(CVE-2026-26083：CVSS 9.8)	● 研究人員發現 Fortinet FortiSandbox、FortiSandbox Cloud 與 FortiSandbox PaaS 的網頁介面存在缺少授權漏洞(CVE-2026-26083)。 ● 未經身分鑑別之遠端攻擊者可透過 HTTP 請求執行未授權的程式碼或命令。 ● 官方已釋出修補版本，建議依公告儘速完成更新。
	工作負載防護系統 Cisco Secure Workload 嚴重程度：(CVE-2026-20223：CVSS 10.0)	● 研究人員發現 Cisco Secure Workload 存在缺乏身分鑑別的 API 存取漏洞(CVE-2026-20223)。 ● 未經身分鑑別之遠端攻擊者可透過特製 API 請求，以 Site Admin 權限存取資源並讀取敏感資訊或修改設定。 ● 官方已提供修補建議，請儘速更新至 Cisco 公告之修復版本。
	網路安全設備 Palo Alto Networks PAN-OS 嚴重程度：(CVE-2026-0300：CVSS 9.8)	● 研究人員發現 Palo Alto Networks PAN-OS 的 User-ID 驗證入口網站服務存在緩衝區溢位漏洞(CVE-2026-0300)。 ● 未經身分鑑別之遠端攻擊者可透過特製封包，於 PA 系列與 VM 系列防火牆上以 root 權限執行任意程式碼。 ● 官方已發布公告，請依受影響版本儘速完

警訊	類別	內容說明
		成更新。
	資料庫與 REST 資料服務 Oracle Database Server 與 Oracle REST Data Services 嚴重程度：(CVE-2026-46833：CVSS 9.0) (CVE-2026-46840：CVSS 10.0)	● Oracle 旗下 Database Server 與 REST Data Services 存在多項重大資安漏洞，其中 CVE-2026-46833 影響 Net Service 元件，CVE-2026-46840 影響 Backend-as-a-Service 元件。 ● 未經身分鑑別之遠端攻擊者可分別透過 TLS 或 HTTPS 網路存取受影響元件。 ● 官方已發布公告，建議依公告儘速完成修補。
已知遭駭客利用之漏洞	行動裝置管理系統 Ivanti Endpoint Manager Mobile (EPMM) 嚴重程度： (CVE-2026-6973：CVSS 7.2)	● CISA 已將 CVE-2026-6973 列入 KEV 清單，Ivanti 指出該漏洞已在極少數攻擊中遭實際利用。 ● 此漏洞為不當輸入驗證，具管理權限之遠端攻擊者可利用 Ivanti EPMM 達成遠端程式碼執行。 ● 官方已針對漏洞釋出修復更新，請參考官方說明進行更新。
	通訊設備 Cisco Catalyst SD-WAN Controller 與 Manager 嚴重程度： (CVE-2026-20182：CVSS 10.0)	● CISA 已將 CVE-2026-20182 列入 KEV 清單，Cisco 亦表示該漏洞已遭積極利用。 ● 此漏洞為身分驗證繞過，未經身分鑑別的遠端攻擊者可取得管理權限帳號，進一步存取 NETCONF 並修改 SD-WAN 架構設定。 ● 官方已提供公告與修補建議，請依官方說明儘速更新至修補版本。

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