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

國際資安政策法制觀測週報

第 73 期

2025 年 4 月 8 日

(3/29-4/4, WEEK 1)

國際合作及資安治理中心

目次

※本報告單元《壹一》之觀測內容，主要係收錄來自重要國家、國際組織或機構網站之資安政策與法規相關新聞(news)及活動訊息(events)。單元《壹二》之資料來源，尚包含國際上重要之前瞻科技公司與媒體。

※單元《貳》則來自我國政府機關網站或媒體。此外，本報告亦不定時選摘重要之研究文獻，供讀者進一步參考。

壹、全球資安暨人工智慧政策法制動態

一、重要國家與組織資安政策法制動態

1. 美洲

名稱	資安相關重點	關鍵字
加拿大	**網路安全中心(CCCS)：** 於 4 月 3 日偕美國國家安全局(NSA)、網路安全暨關鍵基礎設施安全局(CISA)、聯邦調查局(FBI)、澳洲網路安全中心(ACSC)及紐西蘭網路安全中心(NCSC-NZ)等單位，發布有關 Fast Flux 技術的聯合指引[1]。 Fast Flux 是一種威脅行為者(Threat Actors)用來混淆惡意伺服器位置的技術，可快速變更與網域名稱(Domain Name)相關的網域名稱系統(DNS)紀錄，讓威脅行為者可建立更具彈性且得以隱藏其活動的攻擊基礎架構，對國家安全構成重大威脅。 此份聯合指引的發布主要是為提醒各界 Fast Flux 所驅動的惡意活動所構成的持續威脅，並指出目前在偵測與阻擋上仍存在落差，強調應建立準確且可靠的分析能力並提供有關 Fast Flux 的偵測與緩解建議，以保護關鍵基礎設施與敏感資訊。以下簡要概述偵測與緩解建議之重點： 1. 有關偵測，因 Fast Flux 難被偵測的關鍵在於其頻繁變更的網域與 IP 位址，因此建議防禦者運用威脅情報、DNS 日誌分析與地理資訊比對等方式輔以機器	● **國家安全** ● **網路犯罪** ● **參考指引** ● **資安威脅發展趨勢** ● **國際合作**

名稱	資安相關重點	關鍵字
	學習，建立偵測異常流量與行為模式的能力。透過自動化的資料分析工具，有助於辨識異常變化頻率高、來源分散的可疑網域，進而區隔出惡意活動。 2. 有關緩解，指引建議組織透過 DNS 和 IP 封鎖、流量引流 (Sinkholing)[2]、信譽過濾 (Reputational Filtering)[3]與強化監控日誌[4]等方式，阻斷 Fast Flux 網域的存取並分析可疑流量來源。同時也強調資訊共享與跨機構合作的重要性，例如透過政府或產業情資分享機制，提升整體對 Fast Flux 威脅的應變速度與準確度。 3. 對負責資安防禦任務之單位，指引提醒不應假設現有服務供應商(例如保護型 DNS 服務)已具備偵測與封鎖 Fast Flux 的功能，應主動驗證其防護範圍。若導入具備 Fast Flux 偵測與阻斷能力的解決方案，將能有效提升網路防護並降低組織被入侵的風險。	

2. 亞洲

名稱	資安相關重點	關鍵字
韓國	**科學技術資通訊部(MSIT)：** 於 4 月 4 日公布《2024 年網路使用動態調查》(2024 Internet Usage Survey)[5]，調查對象涵蓋全國 25,509 戶家庭逾 6 萬名 3 歲以上之個人，分析韓國民眾在 AI 服務、影音串流、網路銀行、訂閱制消費與跨境購物的使用行為趨勢。	● **民意調查** ● **數位政府** ● **數位涵容** ● **數位平權**

名稱	資安相關重點	關鍵字
	今年調查結果顯示，隨著 AI 科技的普及，已有近 6 成的韓國民眾使用過 AI 服務，較 2021 年 32.4%幾乎成長一倍。在 AI 應用方面，交通領域的 AI 使用滿意度最高(98.3%)；而受訪者最期待 AI 應用於居家領域，例如智慧家電與家用機器人，有超過 7 成認為有其必要且有近 6 成民眾願意實際使用。生成式 AI 使用率也快速上升，從 2023 年的 17.6%提升至 2024 年的 33.3%，主要用途為資訊搜尋、文件撰寫與編輯、外語翻譯、創作與興趣活動以及程式開發。 在數位經濟方面，訂閱服務的使用率從 2023 年的 13.1%躍升至 2024 年的 49.4%，成長近 3.8 倍，主要由年輕族群帶動，青少年與 20、30 多歲族群的使用率分別上升了 43.6、40 與 37%。 在跨境購物方面則呈現成長趨勢，受惠於全球平台進入韓國市場。2024 年有 34.3%的網路使用者曾進行海外購物，較去年的 20%成長 1.7 倍，又以 30 多歲使用者比例最高(47.2%)，20 多歲與 40 多歲族群分別為 43.5%與 36.8%。 在韓國家庭的網路普及率幾近飽和達 99.97%；個人使用率也上升至 94.5%。每日上網者比例高達 90.5%，平均每週使用時間為 20.5 小時。 在具體網路活動方面，即使通訊使用率達 97.7%，其中 KakaoTalk 最受歡迎(98.0%)。影音串流平台則有 95.4%的使用率，以 YouTube 最受歡迎(68.3%)。	

名稱	資安相關重點	關鍵字
	國情院(NIS)： 為應對北韓等駭客勢力近年對韓國醫療資訊系統進行網路攻擊，NIS 於 4 月 3 日發布《醫院資訊系統安全指引》(병원정보시스템 보안 가이드라인)[6]，指引內容涵蓋醫療系統、外部連接系統、病患入口網站等六大領域，並提供資安政策、系統營運、病患個資保護等各面向的安全對策。此份指引利於醫院資安人員使用，另為有效推廣此份指引，NIS 分別於 3 月 14 日及 4 月 3 日舉辦醫療資安研討會向醫院資安人員進行指引的詳細說明。	● **產業資安** ● **醫療產業** ● **參考指引**
新加坡	**網路安全局(CSA)：** 於 7 月 29 日至 30 日將舉辦 2025 年營運技術網路安全專家論壇(Operational Technology Cybersecurity Expert Panel Forum 2025)，主題為「信任與夥伴關係：共同塑造營運技術網路安全的未來」(Trust and Partnership in Shaping the Future of OT Cybersecurity)，聚焦於營運技術(OT)領域在數位轉型與網路威脅交錯下的安全挑戰與解方，講者包含 Dragos 公司執行長兼共同創辦人 Robert M. Lee、InfraGard Houston 主席 Marco Ayala 以及 Honeywell 產品管理主管並創辦「Women in Cybersecurity」的 Saltanat Mashirova 女士。論壇內容將涵蓋最新威脅趨勢、資安強化策略及促進跨產業協作的實務經驗分享，並提供與全球專家交流之機	● **活動資訊** ● **OT 安全**

名稱	資安相關重點	關鍵字
	會。此活動由新加坡 CSA 主辦，最新活動資訊與報名可至官網(www.otcep.gov.sg)查詢[7]。	

3. 歐洲

名稱	資安相關重點	關鍵字
英國	**科學創新暨科技部(DSIT)：** 於 4 月 1 日首次公開《資安與韌性法案》(Cyber Security and Resilience Bill)的政策聲明(Policy Statement)，預告將對現行 2018 年《網路與資訊系統條例》(NIS Regulations)進行修訂並擴大適用範圍、強化供應鏈與資料中心[8]。該法案是《變革計畫》(Plan for Change)的一環，目標是為強化英國對抗網路威脅之能力、保護經濟並提升數位基礎設施韌性。 以下簡述該法案核心立法措施[9]： 1. 將更多實體納入監理範圍： (1)首次納入 900 至 1,100 家管理式服務供應商(MSPs)，並明確定義哪些服務屬於受規範的管理式服務，例如涉及 IT 網路存取、系統管理或資安服務(如 MSSP、SIEM、SOC)者皆納入適用範圍。 (2)強化供應鏈安全與關鍵供應商(Designated Critical Supplier, DCS)指定制度：政府將透過次級立法(Secondary Legislation)，明定關鍵	● **資安政策或法令** ● **關鍵基礎設施** ● **資安治理** ● **供應鏈安全**

名稱	資安相關重點	關鍵字
	服務營運者(Operators of Essential Services, OES)與相關數位服務提供者(Relevant Digital Service Providers, RDSP)在供應鏈資安上的義務，例如納入契約要求、資安審查或備援計畫，以防範供應商成為弱點；監管機關可指定個別高影響力供應商為 DCS，若其中斷將對關鍵服務產生重大衝擊者，則須遵守與 OES 及 RDSP 相當的資安與通報義務；而原本免責的小型與微型 RDSP，若其服務對關鍵服務具關鍵性，也可能被指定為 DCS 納入規範。 2. 賦權監理機關： (1)更新英國網路安全中心(NCSC-UK)的網路評估架構(Cyber Assessment Framework, CAF)，使其與 NIS2 指令更加一致，並成為具約束力的標準。 (2)強化資安事件通報義務，要求 24 小時內須初步通報 NCSC-UK；72 小時內提交事件報告。 (3)提升資訊委員辦公室(ICO)主動監理能力(按：ICO 是 RDSP 的主管機關)，包括提升可主動向 RDSP 索取資訊與強制要求其註冊，以因應大規模數位服務風險。 (4)完善成本回收(Cost Recovery)制度：監理機關可設定收費標準，不再完全依賴政府預算，提升財務獨立與執法效率。	

名稱	資安相關重點	關鍵字
	3. 調整監理架構，引入授權立法(Delegated Powers)彈性，讓科技大臣可在特定保障機制(Certain Safeguards)下直接調整規範，而不須每次皆經國會立法。 4. 其他正在考慮採取的措施，包括：將資料中心納入監理、建立全國資安優先事項聲明，以及賦予科技大臣在國安事件中直接指導業者或監管機關採取行動的權力。 此法案預計於 2025 年底前提交國會審議，是英國為確保關鍵基礎設施、供應鏈與數位經濟安的重要立法，將有助建立更具韌性的網路安全監管架構。	

4. 國際組織

名稱	相關重點	關鍵字
歐盟	**執委會：** 首先，於 4 月 1 日公布《保護歐盟》(ProtectEU)內部安全戰略，目標是為協助成員國並強化歐盟保障公民安全的能力[10]。該戰略指出，在傳統安全及地緣政治變遷之際，歐盟面對外國敵對勢力所發動的混合型威脅、組織犯罪擴張及線上犯罪的增加，都讓歐盟亟需轉變安全應對思維。摘述《保護歐盟》中與資安相關的目標及行動[11]，包括： 1. 建立歐盟內部安全治理架構，包括政策擬定初期的安全評估與備援影響、定期進行安全威脅分析並強	● **國家安全** ● **網路犯罪** ● **關鍵基礎設施** ● **資安政策或法令**

名稱	相關重點	關鍵字
	化與安全學院(Security College)及歐盟理事會之交流，並向歐洲議會與理事會定期報告，監督與協助關鍵措施的推動。 2. 透過情報共享提升威脅預警能力，包括：建立定期的歐盟內部安全威脅總覽(Landscape)；增強會員國與歐盟單一情報分析能力(SIAC)[12]的情報共享(Intelligence-Sharing)；強化會員國與歐盟機構之間的資訊交換(Information Sharing)。 3. 強化司法與內政事務(JHA)機構的能力，因多數網路犯罪皆涉及數位資料，合法取用資料成為關鍵。對此，該戰略將擴大歐洲刑警組織(Europol)的職能讓其具備更強的執行力，並加強邊境管理局(Frontex)、歐盟司法合作組織(Eurojust)、歐盟網路安全局(ENISA)等機構合作。此外，建立新的跨境關鍵通訊系統，並制定合法取用數位資料與加密技術的指引路徑圖，同時檢討資料保留(Data Retention)規則以提升執法效率。 4. 強化對混合威脅的韌性：將提升關鍵基礎設施防護、資安與線上威脅的因應能力，包括確保會員國有效落實《關鍵實體韌性指令》(CER Directive)與《網路與資訊安全指令》(NIS2 Directive)；推出新的《資安法》(Cybersecurity Act)，並建立保障雲端與電信服務安全的新措施；採取措施降低對單一外部供應商的依賴，並對高風險供應商調整採購規則；加強運輸樞紐(Transport Hubs)的安全保障，	

名稱	相關重點	關鍵字
	包括《歐盟港口戰略》(EU Ports Strategy)與航空運輸的新通報機制；推出針對化學、生物、放射性與核子(CBRN)威脅的行動計畫。 5. 執法單位將打擊組織犯罪，包括制定新組織犯罪法律，強化偵查權限；推動兒童保護行動計畫；全面落實資產追回與沒收新規則，強化追查金流(Follow the Money)做法。 其次，於 4 月 1 日宣布啟動一項 500 萬歐元的徵案計畫(Call for Proposals)，強化歐洲查核事實網絡(European Network of Fact-Checkers)[13]，以促線上環境的可信度與安全，讓歐洲公民在數位空間中獲得更好的保障。此舉是呼應執委會主席 von der Leyen 在 2024–2029 年政治綱領中所提出的《歐洲民主防護盾》(European Democracy Shield) 倡議。 該倡議將強化歐洲各地事實查核社群的能量，目標是在所有歐盟成員國與官方語言中，皆能提供查核服務。該網絡將以歐洲數位媒體觀察站(European Digital Media Observatory, EDMO)及歐洲事實查核標準聯盟(European Fact-Checking Standards Network, EFCSN)等既有機制為基礎，進一步補充並擴大其效能。最後，本次徵案涵蓋的主要行動包括：推動查核人員反騷擾保護計畫、建立事實查核資料庫、建立面對緊急狀況的查核應變能力等。	● **不實訊息**

二、全球人工智慧資安政策法制焦點

名稱	相關重點	關鍵字
日本	**AI 安全研究中心(JP-AISI)：** 於 3 月 31 日發布兩份與 AI 相關的重要文件。首先是《AI 安全紅隊測試方法指引(第 1.10 版)》(AI セーフティに関するレッドチーミング手法ガイド(第 1.10 版))[14]。該指引最初於 2024 年 9 月發表，本次修訂版則透過實務案例讓讀者更具體理解紅隊測試的實務操作。具體而言，JP-AISI 以使用檢索增強生成(Retrieval-Augmented Generation, RAG)機制的 AI 系統進行紅隊測試，詳細說明紅隊測試的各個步驟，並將測試結果整理成結構化文件以提供更實用參考。 其次是《資料品質管理指引》(データ品質マネジメントガイドブック)[15]，目的是為確保資料品質，以提升 AI 系統的可信任度。這份指引是根據 JP-AISI 於 2 月 7 日發布的草案版本更新而成並開放各界提供意見。	● **人工智慧** ● **AI 治理** ● **AI 安全** ● **參考指引**
國際組織	**國際電信聯盟(ITU)：** 副秘書長 Tomas Lamanauskas 於 4 月 1 日撰文指出，制定 AI 技術標準有助於降低 AI 系統的開發與部署成本、提升可近性，同時確保 AI 發展能符合人權與永續原則，造福所有人群。他強調，在法律調整速度難以因應科技變化之際，技術標準是各國實現政策目標、接軌民間創新的重要工具[16]。 目前，國際電信聯盟（ITU）已發布超過 120 項 AI 相關標準，另有 130 項正在制定中。ITU 並與國際標準	● **人工智慧** ● **AI 治理** ● **AI 安全**

名稱	相關重點	關鍵字
	化組織(ISO)及國際電工委員會(IEC)合作推動「世界標準合作」(World Standards Cooperation)機制，確保標準制定過程具透明性、包容性，並納入人權與多元利害關係人的觀點。ITU 也與聯合國人權事務高級專員辦公室合作，將國際人權法的核心原則融入 AI 技術規範中。 針對 AI 可能對環境造成的衝擊，ITU 推出「綠色數位行動」(Green Digital Action)，呼籲業界將 AI 發展與氣候目標接軌。該倡議於 COP29 氣候大會中促成《綠色數位行動宣言》(Declaration on Green Digital Action)，獲得逾 80 國與 2,000 個組織支持，並與法國與 UNEP 共同成立永續 AI 聯盟(Coalition for Sustainable AI)，致力於推動綠色運算與 AI 節能技術。 此外，ITU 也聚焦於消弭全球 AI 技術與技能落差，透過 AI 技能聯盟(AI Skills Coalition)建立線上課程平台、推動基礎建設投資倡議，協助因應發展中國家的數位落差與基礎設施資金缺口。 在應用面上，ITU 與多個聯合國機構合作推動 AI 在垂直領域的應用，例如與世界衛生組織(WHO)、世界智財權組織(WIPO)共同發展 AI 健康倡議(Global Initiative on AI for Health)，與聯合國糧農組織(FAO)合作推動數位農業 AI 應用，並與聯合國歐洲經濟委員會(UNECE)合作研發 AI 道路安全(AI and Road Safety)方案。ITU 也持續投入 AI 於災害預警、氣候韌性與資	

名稱	相關重點	關鍵字
	訊真實性等方面的標準制定，強化其在國際 AI 治理中的技術支柱角色。	

貳、我國資安暨人工智慧政策法制動態

相關重點	關鍵字
國家安全會議： 於 4 月 8 日正式公布《國家資通安全戰略 2025——資安即國安》[17]，指出台灣正面臨國家支持的駭客行動、AI 與量子科技的潛在威脅、勒索軟體攻擊與智財間諜等網路犯罪的挑戰。戰略強調「漸進式改變已難以因應迫切危機」，呼籲大幅提升資安應變目標、能力與韌性，並強化與國際夥伴的鏈結及主動防禦。 戰略主體以「四大支柱」為核心，包括：全社會防衛韌性、國土防衛與關鍵基礎設施、關鍵產業與供應鏈、AI 應用與安全；橫向輔以「資安治理與防護」、「戰略夥伴鏈結」兩大準則，並建立「國家資安戰情協同應變中心」與「強化國家資通安全會報及資訊資安預算正規化」兩大基石，整合六塊基礎聯防體系、跨部會協防體系及戰略夥伴國際合作的運作架構。 具體措施包括：推行零信任架構、部署後量子密碼、擴大國際聯防、建置資安菁英團隊、提升全民資安意識、盤點關鍵基礎設施之風險、提升 AI 應用於資安防護並確保 AI 本身的安全性與可信度，以達成「打造一個堅韌、安全且可信賴的智慧國家」願景。	● **資安政策或法令**
數位發展部數位產業署： 為協助臺灣 AI 產業擴大規模並進軍國際市場，向行政院國家發展基金申請新臺幣 100 億元，推動為期 10 年的「加強投資 AI 新創實施方案」。該方案透過與民間投資人(如金融機構、創投、加速器、企業創投等)合作，共同投資國內具	● **人工智慧** ● **產業扶植措施**

相關重點	關鍵字
潛力的 AI 新創企業及數位經濟相關產業。目前已公布首批 10 家「搭配投資人」，包括台安生物科技、台灣智慧雲端服務、宇航管理顧問、安發天使投資、能率亞洲資本、國聯創業投資管理顧問、創世投創、斯伯克國際創業投資、華陽中小企業開發及臺企銀管理顧問。此外，數產署將舉辦 6 場投資說明會及 4 場媒合會，首場說明會預計於 4 月 10 日舉行，首場媒合會則訂於 5 月 28 日，相關資訊可洽 AI 百億投資方案網站查詢[18]。	

參考資料：

[1] CCCS, Joint guidance on fast flux, available at: https://www.cyber.gc.ca/en/news-events/joint-guidance-fast-flux.

[2] 將 Fast Flux 網域的流量導到安全的伺服器上，以觀察並找出中毒裝置。CCCS, Fast Flux: A National Security Threat, available at: https://media.defense.gov/2025/Apr/02/2003681172/-1/-1/0/csa-fast-flux.pdf.

[3] 封鎖與低信譽網域或 IP 的來回流量，特別是已知涉及 Fast Flux 的惡意來源。同前註。

[4] 包括提升 DNS 與網路流量的日誌記錄與監控能力；建立自動化警示機制以快速應對 Fast Flux 模式。同前註。

[5] MSIT, MSIT Unveils 2024 Internet Usage Trends, available at: https://www.msit.go.kr/eng/bbs/view.do?sCode=eng&mId=4&mPid=

2&pageIndex=&bbsSeqNo=42&nttSeqNo=1098&searchOpt=ALL&searchTxt=.

[6] NIS, 국정원, 국민 생명과 직결된 의료시스템 보호에 주력, available at: https://www.nis.go.kr/CM/1_4/view.do?seq=344.

[7] CSA, Operational Technology Cybersecurity Expert Panel Forum 2025, available at: https://www.csa.gov.sg/news-events/events/operational-technology-cybersecurity-expert-panel-forum-2025.

[8] DSIT, New cyber laws to safeguard UK economy and secure long-term growth, available at: https://www.gov.uk/government/news/new-cyber-laws-to-safeguard-uk-economy-secure-long-term-growth.

[9] DSIT, Cyber security and resilience policy statement, available at: https://www.gov.uk/government/publications/cyber-security-and-resilience-bill-policy-statement/cyber-security-and-resilience-bill-policy-statement.

[10] European Commission, Commission unveils ProtectEU – a new European Internal Security Strategy, available at: https://ec.europa.eu/commission/presscorner/detail/en/ip_25_920.

[11] EU, COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS on ProtectEU: a European Internal Security Strategy, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52025PC0148.

[12] SIAC 是歐盟專門整合各國情報、進行威脅研判的分析單位，負責提供歐盟層級的戰略情勢評估，由歐盟情報中心(EU INTCEN)與歐盟軍事參謀部情報部門(EUMS Intelligence)共同組成。EEAS, Impetus #28, available at: https://www.eeas.europa.eu/eeas/impetus-28_en.

[13] European Commission, Commission Launches €5 Million Call to Strengthen European Fact-Checking Network, available at: https://digital-strategy.ec.europa.eu/en/news/commission-launches-eu5-million-call-strengthen-european-fact-checking-network.

[14] JP-AISI, AI セーフティに関するレッドチーミング手法ガイド(第 1.10 版)の公開, available at: https://aisi.go.jp/effort/effort_information/250331_1/.

[15] JP-AISI, データ品質マネジメントガイドブック, available at: https://aisi.go.jp/effort/effort_information/250331_2/.

[16] ITU, Standards help unlock trustworthy AI opportunities for all, available at: https://www.itu.int/hub/2025/04/standards-help-unlock-trustworthy-ai-opportunities-for-all/.

[17] 總統府，國家資通安全戰略 2025-資安即國安，查詢網址：https://www.president.gov.tw/File/Doc/9d056651-e4a0-4d51-adeb-5fee5ee71299。

[18] 數位發展部數位產業署，「百億助攻 AI 新創」 公私協力共同投資 AI 數位產業！，查詢網址: https://moda.gov.tw/ADI/news/latest-news/15758。