IP & Domain Name Newsletter

2026 July

數位發展部
Ministry of Digital Affairs

資策會科技法律研究所
Science & Technology Institute

本期內容

本期電子報持續追蹤 IP/DN 及網際網路治理領域的熱點政策議題。在網際網路基礎設施方面，亞太網路資訊中心（APNIC）近期正式啟用自治系統提供者授權（Autonomous System Provider Authorization, ASPA）支援服務，為防範 BGP 路由劫持與洩漏補上了關鍵的缺口，對維持數位基礎設施的穩健具關鍵意義。在數位治理政策方面，透過近期即將施行的歐盟電子證據規範與英國 Ofcom 最近公布的 OSA 身分驗證指南草案為參照，也能看出多方利害關係人模式與主權國家的政策決策與需求差異。結合法規面的跨境取證挑戰、平台面的數位信任建構，以及技術面的路由防護，期盼能為讀者梳理出宏觀的網際網路治理視野。

目錄

註冊資料揭露政策的缺口：隱私與代理服務

平衡隱私保護與安全防護

網域名稱的隱私與代理（Privacy / Proxy）服務，長期以來是ICANN 治理框架中的核心議題，該政策的精神在於平衡「保護網域註冊人個人隱私」與「維護網路空間信任度及打擊網路犯罪」這兩種對立的公共利益。ICANN 的「隱私與代理服務認證政策（Privacy and Proxy Services Accreditation Issues, PPSAI）」旨在為提供隱私保護的服務商建立一套標準化的認證機制，確保在發生網路犯罪、商標侵權，或散佈惡意軟體等 DNS 濫用行為時，執法單位或智財權人有合法且標準化的管道知悉隱藏在隱私/代理服務背後的真實網域使用者身分。伴隨著註冊資料請求服務（RDRS/SSAD）的持續發展，ICANN 正致力於建立一個既符合全球資料隱私法規，又能滿足維護網路安全之犯罪調查需求的註冊資料存取體系。

隱私與代理服務的濫用風險

從線上安全與網際網路治理的角度，隱私保護若被惡意行為者濫用，將大幅增加追蹤釣魚網站、殭屍網路等 DNS 濫用行為的難度，特別是在 AI 自動化工具蓬勃發展的今日，網路釣魚攻擊與虛假網站能以極快的速度註冊並部署網域，若這些惡意網域隱匿於未經認證的隱私與代理服務之下，將損害網路安全的防護體系，更進一步損害 ICANN 多方利害關係人模式的公信力。

2026 年 6 月 8 日至 11 日於西班牙舉辦的 ICANN86 政策論壇期間，隱私與代理服務及註冊資料存取機制也持續成為跨社群討論的焦

點，尤其直接涉及註冊商驗證網域註冊資料正確性義務的議題。整體而言，社群體認到當前 RDRS 的自願性參與揭露框架在面對 AI 自動化輔助的網路犯罪時顯得過於緩慢，也開始有聲音討論是否應針對「高風險網域（如涉及詐騙或批量註冊）」建立更具強制力的域名實際使用者身分揭露機制。

經銷商（Reseller）合規與穿透義務的侷限性

然而，一個無法忽視的問題仍持續懸而未決，即 ICANN 透過多方利害關係人模式建立的合約義務關係，其拘束力是否能有效傳遞到未與 ICANN 簽訂任何契約的註冊商經銷商（Reseller）身上，又是否具有能有效揭露域名實際使用者真實身分的效力。目前的註冊服務機構認證協議（Registrar Accreditation Agreement, RAA」第 3.12 條規範的穿透義務（pass-through obligation）要求註冊商必須在與經銷商的商業合約中納入特定的合規條款，如必須比照註冊商遵守 RAA 附件的「隱私與代理註冊服務規範（Specification On Privacy And Proxy Registrations）」。

然而 ICANN 缺乏對經銷商合規稽核的權力，前述規範對於在何種條件下必須揭露網域實際使用者真實身分亦未明訂，僅有須公開其揭露政策的透明化規定，保留業者的自主彈性，爰即便未來 PPSAI 政策正式落實，註冊商僅接受經過 ICANN 認證的隱私與代理服務提供

者註冊域名且合約鍊的穿透義務能有效連結，這個機制揭露真實域名使用者的實際成效是否符合打擊網路犯罪的期待與需求仍有待觀察。

延伸閱讀：

1. ICANN86 Seville Communique
2. Registrar Accreditation Agreement

跨境直接取證與合規新挑戰：歐盟電子證據規範

建立直接跨境取證制度

歐盟「電子證據規範（E-Evidence Regulation, Regulation (EU) 2023/1543）」與「電子證據指令（Directive (EU) 2023/1544）」為歐盟內部打擊跨境網路犯罪建立了新的取證通道。過去，歐盟各國執法機關在調閱跨國網路犯罪證據時，必須仰賴曠日廢時的司法互助協定（MLAT）程序，而歐盟 E-evidence 政策的核心精神在於跨過傳統的 MLAT，賦予歐盟各成員國執法機構「直接」向設立於其他歐盟國家（及設立於歐盟境外但有面向歐盟用戶提供服務）的服務提供者（如電信服務、ISP、域名註冊商及與域名隱私與代理註冊服務等）下達資料保全與提交之命令的權力，包括用戶基本資料、網路流量紀錄，甚至是與通訊內容相關的資料。服務提供者在收到命令後，必須在法定時限內（緊急情況下只有 8 小時）做出回應並提供資料。

歐盟 E-evidence 的全面生效對 IP/DN 產業亦帶來了深遠的合規壓力，法規要求有面向歐盟用戶提供服務的受理註冊機構（Registrar）與註冊管理機構（Registry）必須在歐盟境內指定法定代理人或設立單一聯繫窗口，以確保能全天候接收並處理來自全歐盟執法機關的跨境命令。

繞過 ICANN 治理框架

從網際網路治理與多方利害關係人模式的角度來看，這象徵著歐盟成員國政府間達成了彼此擴張其數位管轄權的共識，在刑事犯罪偵

查方面架空了 ICANN 透過多方利害關係人模式形成的註冊資料揭露政策，雖然能提升跨境取證效率，但也大幅提高了業者的合規成本，並將原本司法機關之間承擔的溝通成本轉嫁給了私人企業，中小型 ISP 與域名註冊服務商缺乏應對多語系、跨國法律文書審核的資源也是一大挑戰，可能會需要 AI 自動化審查工具的輔助。

業者的雙重合規壓力

歷經了三年的過渡期，E-evidence 即將於 2026 年 8 月 18 日正式生效並對業者產生拘束力，若未能在即時完成法定代理人的指定與系統對接，業者可能將面臨巨額裁罰（全球年營業額的 2%）。然而 E-evidence 與保障用戶個資隱私的 GDPR 之間存在衝突，產業仍將持續面對兩難的合規挑戰，例如若利用 AI 技術自動化審查 E-evidence 調取命令以降低合規成本，即可能觸及 GDPR 對完全自動化處理個人資料的限制。

延伸閱讀：

1. Regulation (EU) 2023/1543
2. Directive (EU) 2023/1544

強化數位信任：英國發布 OSA 身分驗證指南草案

網際網路治理的長期痛點

在網際網路治理與線上安全維護領域，身分驗證一直是一個難題，ICANN 的諸多治理政策如註冊資料正確性（註冊商驗證註冊人身分）與註冊資料揭露緊急請求的落實，皆在身分驗證的議題遭遇相當的障礙。目前在 ICANN 的治理框架下並沒有對註冊商應驗證註冊人真實身分的要求，僅要求驗證聯絡資訊的準確性與可聯絡性；而面對來自如執法機關的緊急註冊資料揭露請求，註冊商又必須驗證請求來源的真實身分以避免合規風險，而可行的驗證機制目前尚未建立。

英國 OSA 將提供身分驗證工具納入法定義務

而關於身分驗證，被視為全球最具企圖心的網路內容監管架構之一的英國「線上安全法（Online Safety Act 2023, OSA）」，其核心精神也包含了促進數位信任的強化，進而提升整體數位線上環境的安全可靠性，其中就包含了數位平台用戶身分驗證措施的相關規範。2026 年 7 月 10 日，英國通訊管理局（Ofcom）正式發布了針對第一類（Category 1）服務[1]的「使用者身分驗證指南（User Identity Verification Guidance）」草案並展開至 10 月 2 日的公眾諮詢。

有別於專為保障未成年人免於觸及有害內容的「高度有效的年齡保證措施」（僅驗證用戶是否成年，不及於身分屬性，但對有效性的

[1] 指用戶規模大、內容傳播速度快致潛在風險最高，並經 Ofcom 依據認定標準宣告之「使用者對使用者服務」，例如 Facebook。<查看詳情>

要求更高），OSA 第 64 條規範的身分驗證措施是一種「使用者賦權」，用戶可以自行決定是否通過平台驗證其身分屬性來提升個人在網際網路空間上的身分可信度，進而促進整體網際網路數位信任的提升，爰要求在網際網路具有高度影響力的 Category 1 服務提供成人用戶能驗證其身分屬性（例如法定姓名、電子郵件、居住地、雇主、網域、年齡、在其他平台上的使用者名稱…等）的選項，驗證流程的設計須全面落實關聯性（驗證身分的目的及相關的身分屬性）、可靠性（獨立來源證據比較、降低使用者偽造、規避驗證及資料過時風險的合理措施等）、包容性（如不能僅依賴單一官方證件做驗證）與清晰度（如充分說明身分驗證的意義、流程與隱私保護政策）等四大原則。

此外，由於身分驗證的過程會涉及大量的個人資料蒐集與處理，指南也提醒業者在設計與執行驗證時必須完全遵守相關的個人資料保護法規（如 GDPR）。

延伸閱讀：

1. Consultation: Giving users more choice, control and trust in their online experience
2. Draft User Identity Verification Guidance

提升路由安全：APNIC 正式啟用 ASPA 支援

提升 BGP 路由安全

自治系統提供者授權（Autonomous System Provider Authorization, ASPA）是繼路由來源的宣告與驗證（ROA/ROV）之後，最關鍵的密碼學防護機制升級。長期以來，邊界閘道協定（BGP）缺乏內建的安全認證導致路由劫持與路由洩漏（Route Leaks）的發生。ROA 解決了「來源驗證（誰有權廣播這個 IP 網段）」的問題，但無法防止惡意者竄改資料傳輸的路徑。ASPA 則補足了這一點，它允許網路營運商透過資源公鑰基礎設施（RPKI）以密碼學方式明確宣告其授權的「傳輸供應商（Provider ASN）」，使路由器能夠逐節點驗證路由的合理性，進一步提升 BGP 路由路徑的安全性，且 ASPA 並不需要改變 BGP 協定本身，也不強求硬體路由器進行複雜的密碼運算，而是將商業營運關係編入 RPKI 體系中。

補齊亞太地區的路由安全拼圖

2026 年 7 月，亞太網路資訊中心（APNIC）已正式於其管理平台上線並啟用了 ASPA 支援服務，亞太區的網路營運商現在可以與歐洲及北美同步，開始創建並發布 ASPA 物件來保護自身的路由路徑安全，補齊了全球最活躍的網際網路成長區域的路由安全拼圖。

ASPA 的啟用對產業及全球網際網路基礎設施具有決定性的戰略重要性。對於資料中心、ISP 與 AI 雲端運算服務等依賴穩定網路傳輸的業者而言，路由洩漏或劫持不僅會導致連線中斷，更可能使機密的資料或用戶指令被導向惡意伺服器進行側錄。又從網際網路治理的觀點，ASPA 是透過網際網路工程任務組（IETF）制定標準，並由各區域網際網路註冊管理機構（RIRs）協同推動，展現了技術社群透過多方利害關係人模式自主解決全球網路安全危機的能力，即便目前全球發布 ASPA 紀錄的 ASN 比例尚不足 2.5%，且雖然主要 RIR 皆已佈建了 ASPA 的基礎設施（LACNIC 與 AFRINIC 尚未啟用），但網路硬體設備與路由軟體的支援度仍是一大挑戰，業界也需要持續推動軟硬體預設啟用 ASPA 驗證，才能有效發揮其保護路由安全的功能。

延伸閱讀：

1. ASPA at APNIC: Strengthening BGP path validation
2. Hurricane Electric (HE) RPKI & ASPA Adoption Report