

ICANN NEWSLETTER

Apr. 2026

moda 數位發展部
Ministry of Digital Affairs



stli

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

Table of Contents

重點議題

- ICANN85 GAC 公報政策議題概覽 1

最新消息

- ICANN 將辦理 2026 New gTLD 申請問答研討會 4
- ICANN 啟動 2026 年 RSP 第二輪評估 5
- ICANN 開放 ICANN 87@NextGen 申請 6

公眾意見徵詢

- 社群優先評估指引草案 7

文摘

- 破碎的網路：網路碎片化如何威脅我們的網路世界 8

ICANN85 GAC 公報政策議題概覽

2026 年 3 月在印度孟買舉行 ICANN 85 的會議，政府諮詢委員會（Governmental Advisory Committee, GAC）共有 70 個成員政府及 9 個觀察員組織以實體與線上混合形式出席。GAC 會後發布之公報（Communiqué）聚焦多項核心網路治理議題，其明確支持網域註冊資料緊急請求的 24 小時回應時限，並要求建立執法機關（Law Enforcement Agency, LEA）身分驗證機制。針對 DNS 濫用，GAC 呼籲建立集中式通報入口，並縮短註冊驗證期。此外，GAC 支持 2026 New gTLD 申請人支持計畫（Applicant Support Program, ASP）將受助申請案件數擴充至 75 件，且不得削減原有 85% 的費用減免。

網域名稱註冊資料

GAC 肯定理事會同意將註冊商對執法機關緊急請求的回應時限訂為 24 小時，同時強調此時限必須以「建立執法機關身分驗證機制（Authentication Mechanism）」為前提條件。GAC 反對為此重啟新的政策制定程序（PDP），認為身分驗證的實施應直接納入現行《註冊資料政策（Registration Data Policy）》的執行範疇，以免延誤維護公共安全的進度。

此外，針對理事會決定不採納 18 項 SSAD 建議，改由 GNSO 納入過往兩年的 RDRS 試行經驗，以提出補充建議（Supplemental Recommendations）；GAC 支持此發展路徑，並重申 gTLD 註冊商應強制參與（Mandatory Participation），以確保此一機制的實用性，同時敦促在數個月內盡速完成相關程序。

DNS 濫用防制政策與 PDP1

GAC 肯定「關聯網域檢查 (Associated Domain Checks) 」 PDP1 的正式啟動，並支持縮短整體工作時程。然而，GAC 指出先前的議題報告中有多項政策差距仍待填補，包含報告透明度不足、預測演算法 (Predictive Algorithms) 未充分運用於早期偵測，以及子網域濫用 (Subdomain Abuse) 等問題。

GAC 在公報中指出，若在網域 DNS 解析前完成註冊人聯絡資訊驗證，可減少約 70% 的惡意註冊。因此，GAC 強烈主張應縮短現行 15 天的註冊後驗證期 (Post-registration Verification Period)，並探索包含合約修訂在內的快速推進路徑。此外，GAC 亦建議 ICANN 建立「集中式通報機制 (Centralized Reporting Mechanism)」，要求註冊局與註冊商定期回報投訴數量與處理結果，以提升資料透明度。



圖片來源：Gemini

2026 New gTLD 相關政策

2026 New gTLD 申請將於 2026 年 4 月底啟動，針對 ASP，GAC 支持理事會擴大預算，將受助申請案件數從原規劃的 45 件擴增至 75 件合格申請案，絕不能因既有預算規劃而調降原有的財務支持水準，必須確保每位合格申請人仍能獲得最高 85% 的基本費用減免 (Base Fee Reduction)，確保多元參與政策目標不受損。

為協助成員審查，GAC 要求在 ICANN86 會議前安排專題說明會，指導成員如何透過申請管理系統 (TLD Application

Management System, TAMS) 存取公開申請資訊；系統亦應提供更完善的搜尋與下載功能，以提升政府審查效率。

其他重要議題

除上述三項核心議題外，公報亦涉及其他議題，在統一網域名稱爭議解決政策 (Universal Dispute Resolution Policy, UDRP) 審查方面，GAC 建議參考 WIPO-ICA 聯合報告作為即將啟動之審查的框架；在區域網際網路註冊機構 (Regional Internet Registries, RIRs) 治理方面，GAC 強調相關治理應符合公共利益與多方利益相關者模式；此外，GAC 亦關注根伺服器系統的穩定性與韌性，期望進一步了解事件偵測與通報框架；並將持續參與評審架構改革 (Review of Reviews) 跨社群工作組，追蹤安全穩定韌性及競爭與消費者信任等重要評審的後續安置方式。

[資料來源連結](#)

ICANN 將辦理 2026 New gTLD 申請問答研討會

2026 New gTLD 的申請將於 4 月 30 日啟動，為確保希望參與該計劃的人都做好準備，除了提供各種[支援資源](#)外，ICANN 將舉辦一系列新的網路研討會，專門回答有關 TLD 應用管理系統 (TAMS) 及 2026 年 New gTLD 申請流程相關的問題。TAMS 是申請人、ICANN 員工和評估小組成員用來管理、處理和提交 New gTLD 申請的線上系統。ICANN 於 4 月 21 日 ([16:00 UTC](#) 、 [23:00 UTC](#)) 、 5 月 12 日 ([16:00 UTC](#)) 、及 5 月 26 日 ([16:00 UTC](#)) 舉辦四場網路研討會，研討會的重點將放在如何使用 TAMS，也會邀請潛在申請人提出有關 New gTLD 申請和評估流程等各方面的問題。

[資料來源連結](#)

ICANN 啟動 2026 年 RSP 第二輪評估

2026 New gTLD 的註冊管理服務供應商 (Registry Service Provider, RSP) 評估計畫的第二輪申請期間將自 2026 年 4 月 30 日開始，並於 2026 年 8 月 12 日截止。RSP 評估計畫目的是簡化 New gTLD 申請的評估流程，將營運的技術層面評估與 gTLD 字串的申請評估分離；RSP 的技術服務包括 DNS 服務、執行 DNS 安全性擴充加密操作，以及透過註冊資料存取協定 (Registration Data Access Protocol, RDAP) 提供註冊資料等，RSP 評估計畫旨在確保 RSP 具備營運 gTLD 後端所需的適當技術資格。

所有 New gTLD 申請者必須指定至少一家已通過過 RSP 評估計畫的 RSP，當申請者進入 gTLD 授權階段時，申請者應與該 RSP 完成服務契約的簽署。在特殊情況下，RSP 可能與潛在申請者是同一實體，註冊管理機構也可以選擇將服務外包給第三方 RSP。

[資料來源連結](#)

ICANN 開放 ICANN 87@NextGen 申請

NextGen@ICANN 計畫旨在擴大青年世代對網際網路治理生態系的參與，ICANN 並將其視為永續發展的關鍵策略。該計畫的核心宗旨是透過識別並培育尚未接觸相關領域的青年學子（18-30 歲），引導其理解網際網路底層運行的「自下而上」多方關係人模式（Multistakeholder Model），並期許在完成學業後，能轉化為長期貢獻於區域及全球網路決策的社群成員，確保全球網路治理能持續融入新世代的多元觀點。



圖片來源：ICANN

在執行機制上，該計畫為 ICANN 會議所在地之區域學生，提供包含專業指導、差旅補助與結構化課程的完整支持。透過參與正式的 ICANN 會議，獲選學子能在專家導師的引領下，循序漸進地從觀察者成長為貢獻者，以為全球網際網路的韌性與未來發展培育具備專業素養的新一代領導人才。

ICANN 將於 2026 年 10 月 17 日至 22 日在阿曼馬斯喀特舉行的 ICANN 87 年度大會，NextGen 申請開放時間為 2026 年 3 月 23 日至 2026 年 5 月 1 日。成功入選的候選人將於 2026 年 7 月 7 日在 ICANN 網站上公布。

[資料來源連結](#)

社群優先評估指引草案

ICANN 於 2026 年 3 月 24 日發布社群優先評估 (Community Priority Evaluation, CPE) 的評估指引草案，並開放公共評論。本指引係配合 2026 年 New gTLD 計畫所制定，旨在為受託執行 CPE 的評估供應商提供評分標準、流程規範及報告要求等操作指引。

CPE 是 ICANN New gTLD 計畫中解決字串爭議 (string contention) 的機制之一。當多個申請人競爭同一頂級域名字串，如其中至少有一個申請人自稱為『社群型申請』，且該申請人選擇參與 CPE 時，將透過獨立第三方評估小組判斷該社群型申請是否符合優先資格。本指引定義了評估供應商應如何依據《申請人指南》 (Applicant Guidebook, AGB) 中的四項標準進行評分，是 CPE 制度運作的關鍵操作文件。

ICANN 已於 2026 年 3 月 18 日[宣布](#)選定 Analysys Mason Limited 為 2026 年 New gTLD 計畫的 CPE 供應商，本評估指引草案即為 ICANN 與該供應商合作產出的評估操作規範。

進度時程：

開放徵詢：24 Mar. 2026

結束徵詢：4 May 2026

社群意見統整報告：18 May 2026

[提案內容連結](#)

破碎的網路：網路碎片化如何威脅我們的網路世界

文章出處：[CircleID](#)

原文作者：Prince Zutah

International Online Safety Corp.的總裁 Prince Zutah 近日在 CircleID 撰文探討網路碎片化，其指出網際網路正處於關鍵轉折點，原先以開放、全球互連及技術互通為核心的設計模式，正因地緣政治競爭、商業鎖定誘因及政策干預而承受巨大壓力。網路碎片化（Internet Fragmentation）並非單一突發事件，而是由於政府、企業及技術參與者的決策，導致網路普遍性（Universality）與可靠性逐漸侵蝕的累積過程。

網路碎片化的三種型式

一、技術碎片化

技術碎片化源於互通性（Interoperability）的弱化，網際網路的價值建立在 IETF 等機構制定的通用協議與開放標準之上，當特定國家或機構強制實施專有網路架構、非標準的 DNS 根目錄或封閉式基礎設施設計時，將直接破壞跨系統的



圖片來源：Gemini

連動性。技術變革本身不必然導致碎片化，關鍵在於實施方式是選擇「維護相容性」還是「建立技術壁壘」。

二、政府或政策碎片化

此型式表現為審查制度、網路封鎖、過濾及資料在地化要求，儘管各國政府以維護主權與網路安全作為正當化理由，但單方面且缺乏協調的政策會切斷跨境連結，形成與全球網路脫鉤的數位孤島。數據顯示，網路中斷事件已創 2016 年以來新高，且全球網路自由度已連續十五年下降，反映出行政干預正逐漸成為國家治理的常態工具。

三、商業碎片化

這種隱性碎片化源於主導平台在身分識別、支付、通訊及應用程式分發領域建立的「封閉生態系統」。企業透過提高轉移成本與退出門檻實施用戶鎖定，使互通性變為可選而非必要。這種環境雖然維持連網狀態，實質卻限制了資料可攜性。其結果與政策干預相似，不僅削弱網路開放性，更對依賴開放市場競爭的新創企業構成嚴重的創新阻礙。

網路碎片化透過技術標準不相容、政府中斷網路及審查與商業封閉生態，逐漸削弱全球網路的互通性。網路碎片化不僅導致貿易成本上升與公民權利受損，更產生「安全悖論」（Security Paradox），即當政府為求控制而追求中心化架構時，反而破壞了網路原有的冗餘（Redundancy）與分佈式韌性，使系統在面對攻擊時更顯脆弱。

應對網路碎片化的治理措施

面對網路碎片化的威脅需要透過精確的治理、技術領導力及國際協調來應對。

一、強化多方利益關係人模式，透過網路治理論壇（Internet Governance Forum, IGF）、ICANN 及技術社群在維持全球互通性

中的戰略地位，並結合國家、私部門與公民社會的力量進行協同治理，多方參與模式是維持全球安全與互通網路的基石。

二、推行智慧治理，而非盲目追求數位主權，在保護隱私、網路安全與消費者權益的同時，亦應維護網路的全球架構與互通性。政策制定者應評估法律是否對跨境資料流動或標準相容性造成非必要障礙。

三、支持開放標準與互通的技術基礎設施，持續推動 IETF 等機構制定的自願性標準，確保創新在不破壞網路核心結構的前提下進行。

四、提升數位能力與包容性，透過基礎設施投資、在地技術培育及提升數位素養，確保偏遠地區能實質參與全球網路，防止因數位落差產生的物理性碎片化。



圖片來源：WA.gov.au

五、落實透明度與問責制，涉及命名、路由、資料流及平臺互通的決策不應在黑箱中進行，強化審視機制能及早發現具風險的技術授權或緊急措施，防止其演變為永久性的障礙。

觀察與結論

網路的未來不會僅由技術決定，治理政策亦是塑造網際網路世界的重要因素。作者強調，碎片化並非不可避免，但避免它需要紀律、戰略遠見與領導力。政府需以精準方式監管，企業需在不製造封閉的前提下創新，技術社群需持續捍衛互通性作為公共財，開發中國家則

需在全球數位治理中在場、發聲且具有影響力，確保未來的網路不僅由最有力的行為者設計。如碎片化持續的發生，我們不會一次性失去網路，而將是逐層、逐個地失去特定部分，直到曾經連結全人類的網路，變成個別封閉的數位領土。