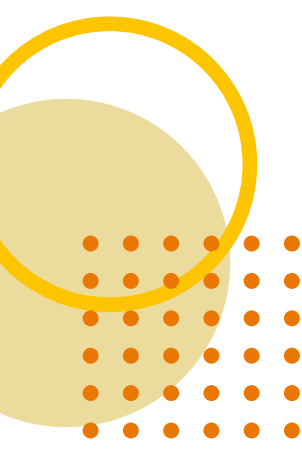




2025.MAR

ICANN NEWSLETTER



2025



Table of Contents

重點議題

1

- ASO AC發布 ICP-2 擬定原則問卷報告

最新消息

2

- ICANN提供New gTLD推廣素材隨選翻譯，助力全球社群參與
- ICANN關注AFRINIC治理危機並支持其恢復穩定運作
- ICANN82 公共論壇重點回顧

公眾意見諮詢

5

- 第二屆IANA命名職能審查小組初步報告

文摘

6

- 被武器化的網路空間
- 失效的域名恐將成為網路犯罪溫床

重點議題

ASO AC發布 ICP-2 擬定原則問卷報告

位址支援組織（Addressing Supporting Organization，ASO）位址委員會（Address Council，AC）已完成更新《建立新地區網際網路註冊管理機構準則》（Criteria for Establishment of New Regional Internet Registries，ICP-2）擬定原則的問卷資料分析與摘要，該項問卷調查係在2024年10月8日至12月6日由號碼資源組織（The Number Resource Organization，NRO）以區域網際網路註冊管理機構（Regional Internet Registry，RIR）社群為對象進行，並同步展開ICANN公眾意見徵詢，期間共收到298份意見回饋，當中以亞太地區最為踴躍，共計提出154份，占比超過五成。

NRO所發布的摘要報告中概述了收到的意見內容，另外也公布了問卷回應的原始資料供參。針對各項擬定原則，受訪者可以透過五個等級選項（強烈同意、同意、中立、不同意、強烈不同意）表達其認同程度；此外，亦可針對各項原則發表評論並在問卷最末提出其他意見。



圖片來源：[FREEPIK.COM](https://www.freepik.com)

調查中的提議原則獲得大多數社群的支持與認可，但仍有少數成員提出提醒與建議，主要關注原則的細節、執行方式及可能影響。例如，需要在NRO執行委員會（Executive Council，EC）與ICANN之間維持權力平衡，並納入其他利害關係人的意見；另有部分疑慮，包括NRO EC的角色需更明確，否則可能存在成為「守門人」的風險；現有RIR在新RIR的建立過程中可能產生利益衝突；此外，若賦予ICANN最終決定權，可能影響RIR的獨立性，使ICANN掌握過多權力。

後續ASO AC將考量本次問卷調查的結果，以及ICANN公眾意見徵詢所收到的意見，以制定ICP-2下一版草案。

最新消息

ICANN提供New gTLD推廣素材 隨選翻譯，助力全球社群參與

為促進域名空間的多樣性，並積極提升全球對於New gTLD的認識，ICANN已開發簡報、資料摘要等多項推廣素材，協助推廣者與更多社群互動。基於多方請求希望將推廣素材翻譯為當地語言，ICANN推出新的隨選翻譯流程「您的語言版New gTLD 計畫」（New gTLD Program In YOUR Language）。

此計畫結合人工智慧與神經機器翻譯（neural machine translation）技術，可將推廣素材翻譯為ICANN六種官方語言以外的其他語言，透過應用程式介面（application program interface，API），即可快速、低成本翻譯推廣文件的簡化版本。

對於此計畫感興趣的個人或組織，可聯繫ICANN區域聯絡人請求翻譯特定文件。語言服務團隊確認可支援該語言後，將使用AI翻譯並將草稿上傳至社群Wiki供志願者審查，確保內容準確無誤。

完成審查後，最終版本將以PDF格式發布，惟需留意，這些文件非屬ICANN官方翻譯，因此須包含法律免責聲明。

「您的語言版New gTLD 計畫」使ICANN能夠以更具意義的方式向弱勢族群介紹New gTLD 所帶來的機會，如有其他請求或需要了解翻譯流程的資訊，請參閱「您的語言版New gTLD 計畫」Wiki 頁面。

資料來源：

<https://www.icann.org/en/blogs/details/icann-offers-on-demand-translation-for-next-round-outreach-material-05-03-2025-en>

All Rights Reserved by NIEPA



圖片來源：[FREEPIK.COM](https://www.freepik.com)



最新消息

ICANN關注AFRINIC治理危機 並支持其恢復穩定運作

ICANN 持續關注非洲網路資訊中心（African Network Information Centre，AFRINIC）的治理危機，並在可能的範圍內提供支持與建議。

根據模里西斯（Mauritius）最高法院破產部門於2025年2月12日發布的命令，任命 Gowtamsingh Dabee 取代原 AFRINIC 官方接管人，並要求 Dabee 加快腳步於2025年4月25日前規劃及舉行董事會選舉，目的在於確保 AFRINIC 資產的安全，且根據 AFRINIC 章程重組其董事會。



Dabee 是在模里西斯具備25年以上專業經驗的破產管理人，ICANN 深知接管人在修復 AFRINIC 治理方面的重要性，並已主動向 Dabee 提供協助。未來 ICANN 也將持續關注後續事態發展，並將根據 Dabee 的請求提供必要支援，以恢復 AFRINIC 的治理與運作。

資料來源：

<https://www.icann.org/en/announcements/details/icann-update-on-afrinic-receiver-appointment-09-03-2025-en>

<https://afrinic.net/fr/notice-of-appointment-of-receiver-pursuant-to-section-187-of-the-insolvency-act-2009>



圖片來源：FREEPIK.COM



最新消息

ICANN 82 公共論壇重點回顧

ICANN82會議於2025年3月8日至3月13日在美國西雅圖舉行，會議的最後一天舉行了一場公共論壇 (Public Forum)，由董事會主席Tripti Sinha擔任主持人，該論壇開放所有社群成員參加，使來自不同背景的參加者能有機會針對ICANN關注的核心議題發表看法，並討論可行的應對措施。

其中有關New gTLD政策的意見包括：當前的政策可能導致市場壟斷，因為某些企業已經獲得特定關鍵字的獨家控制權，限制其他競爭者的申請機會，進而影響市場公平性；此外，建議ICANN應重新考慮私人拍賣機制，因為這項機制在2012年New gTLD開放申請時，有效解決了競爭者之間的衝突。

對此，ICANN表示未來將持續監測New gTLD申請與市場發展情況，以確保其運作符合公平競爭原則；關於私人拍賣機制，先前內部討論後認為其與ICANN的價值觀不符，因此不再採用。儘管如此，ICANN仍然開放討論如何優化New gTLD申請過程，並鼓勵社群成員提供意見，以確保未來的申請機制能夠平衡市場需求與公平性。

在DNS濫用方面，與會者建議ICANN應採取更積極的措施來保護可信任的網域，例如建立可信任網域的認證機制，以便與惡意網域區分，減少濫用風險。ICANN表示將審視其可行性，但現階段尚無具體計畫，目前主要的應對措施是透過修訂DNS濫用相關的締約方合約義務來加強規範。ICANN認可DNS濫用問題的複雜性，並鼓勵社群持續提出建議，以共同探討更有效的應對方案。



資料來源：

[ICANN82 Public Forum Zoom Webinar Archive](#)
All Rights Reserved by NIEPA

圖片來源：[FREEPIK.COM](#)

公眾意見徵詢

第二屆IANA命名職能審查小組初步報告

網際網路號碼指配機構（Internet Assigned Numbers Authority，IANA）命名職能審查（Naming Function Review，IFR），是ICANN為確保IANA命名職能的執行品質、透明度與問責性所設立的定期審查機制。根據《ICANN章程》[第18條](#)規定，此項審查應至少每5年辦理一次，以助於社群監督與持續改善IANA命名職能的運作。

第一屆審查於2018年9月啟動，審查小組負責評估由公共技術識別碼（Public Technical Identifiers，PTI）執行的命名職能是否符合契約規範與社群需求；第二屆審查則由ICANN董事會於2023年9月正式啟動。

第二屆IANA IFR小組的初步報告已發布，並公開徵求社群意見，重點關注IANA命名職能契約中域名系統安全擴充（Domain Name System Security Extensions，DNSSEC）政策細節的納入、契約修正的透明度與可取得性，以及審查頻率，並提出若干附帶性調查結果。

[審查小組的Wiki頁面](#)提供關鍵文件與資源，包括任務說明書、工作計畫、會議紀錄及相關資料，以供社群參考。

進度時程

開放徵詢 20 March 2025
結束徵詢 28 April 2025
社群意見統整報告 12 May 2025

提案內容

[Second IANA Naming Function Review - Initial Report](#)

提交意見 >



文摘

被武器化的網路空間

文章出處：[CircleID](#)

原文作者：Wolfgang Kleinwächter



2025年慕尼黑安全會議（Munich Security Conference，MSC）傳遞了一項令人不安的訊息——網路空間將受地緣政治衝突規則支配，成為21世紀的戰場。與會者熱烈討論數位服務的軍民交互影響，數位革命不僅改變溝通、商業與娛樂，也影響國家衝突解決方式。若世界從合作轉向對抗，將影響資訊社會的發展。2025年WSIS+20前夕，國際社會須思考如何在武器化的網路空間中推進和平的數位合作。

數位與傳統戰爭界線模糊難辨

2025年慕尼黑安全會議展現出數位戰爭的本質轉變，隨著數位軍事與民用行動的界限模糊，國家、駭客組織與犯罪集團的行為越來越難以區分。網路攻防已成為獨立戰場，九成軍事監視與偵察基礎設施由私營企業掌控，讓軍事決策權游移於政府與企業之間。

數位革命提升了傳統武器的效能，人工智慧則帶來無人載具與自主武器，使戰爭成本嚴重失衡。如今，500美元的無人機足以摧毀價值500萬美元的坦克車，顛覆了傳統戰爭的經濟邏輯。國際社會雖嘗試透過聯合國機制建立信任措施，然而成效有限。美國政府更傾向透過雙邊談判解決數位衝突，而非依賴多邊協議。

全球南方崛起引領數位新勢力

本次會議也凸顯全球南方在數位治理中的崛起。印度外交部長強調，印度不會捲入數位強權的對抗，但也不會回歸不結盟政策，而是採取「多邊結盟」，靈活應對全球局勢。印度憑藉其AI發展戰略與科技實力，正逐步成為新興數位強權；同樣的，沙烏地阿拉伯、巴西與南非等國也在全球數位秩序中扮演越來越重要的角色。

圖片來源：[FREEPIK.COM](#)

文摘

被武器化的網路空間

美國代表批評歐盟數位法規，引發歐洲代表不滿，而印度的參加者則指出，歐洲對全球南方的態度同樣帶有雙重標準，顯示數位治理仍充滿權力競爭。

本文作者認為，數位治理需要全球合作，政府、企業與公民社會必須共同參與。今年的WSIS+20會議將成為關鍵考驗，數位時代的全球秩序正在重塑，未來如何平衡各方利益仍是未解的難題。

數位監管立場各異爭論難解

美國代表批評歐盟的數位法規，延續他在巴黎AI峰會上對《歐盟AI法案》（EU AI Act）的反對立場；而Ursula von der Leyen在2019年出任歐盟執委會主席時就曾強調：歐洲不能成為數位規則的「接受者」，而是要成為「制定者」。

儘管歐盟自2019年以來陸續通過《數位服務法》（Digital Services Act，DSA）、《數位市場法》（Digital Market Act，DMA）、《歐盟AI法案》等法規，試圖主導數位治理，但卻缺乏真正的數位產業領導者。歐盟企業對監管負擔感到壓力，新任歐盟委員Henna Virkkunen承諾不再新增法規，並將簡化現行監管。然而，她並未正面談論「簡化監管」與美國推動的「去管制」是否能相互調和，僅表示將刪減重複法條，但不會放棄監管。



與此同時，美國總統在2025年2月23日簽署的備忘錄中批評，歐盟法規限制美國企業，強調美國不會成為歐洲的財政來源，措辭近似經濟威脅，這反映出歐美在數位治理上的根本衝突。正如法國哲學家 Henri Lacordaire所言，「強者與弱者之間，自由帶來壓迫，法律帶來解放」，歐洲的數位未來正面臨動盪時期。

圖片來源：[FREEPIK.COM](https://www.freepik.com)

文摘

失效的域名恐將 成為網路犯罪溫床

文章出處：[SIDN](#)

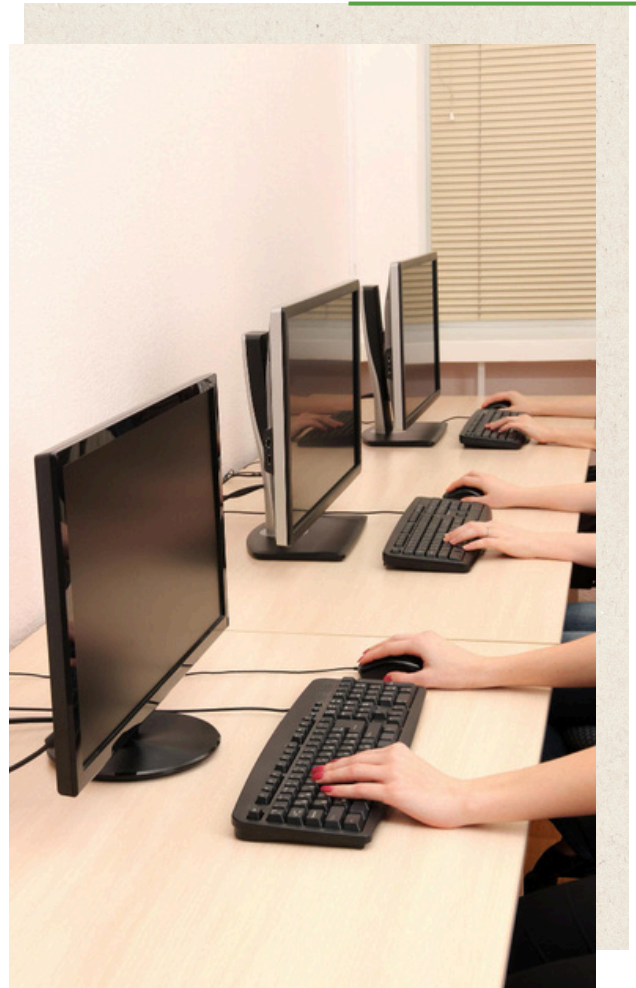
原文作者：SIDN

ICANN於2025年1月發布警告，指出有網路犯罪分子正在營運「流氓」（Rogue）WHOIS伺服器，令業界感到不安。此項犯罪手法，係在合法的域名失效後，將其註冊用於模仿合法的WHOIS伺服器，以攻擊使用者或竊取其身分資料。

WHOIS伺服器是用於存放域名註冊資料的資料庫，並向公眾提供查詢服務，例如註冊者聯絡方式。這類資訊對於簽發傳輸層安全性（Transport Layer Security，TLS）憑證、轉讓網域名稱或發送刪除通知（notice-and-take-down request）等機構極為重要。



圖片來源：[FREEPIK.COM](#)



圖片來源：[FREEPIK.COM](#)

過去，所有通用頂級域名註冊管理機構都需要提供WHOIS服務，然而，自2024年開始，提供註冊資料存取協議（Registration Data Access Protocol，RDAP）服務的註冊管理機構，不再被強制要求營運WHOIS伺服器，導致許多機構關閉其服務，甚至註銷相關域名。在此情況下，不法分子得以重新註冊這些失效的域名，並營運流氓WHOIS伺服器，藉此獲取偽造的SSL憑證，進行網路釣魚攻擊，嚴重威脅網路安全。

文摘

失效的域名恐將成為網路犯罪溫床



資安專家Benjamin Harris在2024年發表一項嚴重的風險，他成功註冊已失效的dotmobiregistry.net，該域名曾是.mobi頂級域名的官方WHOIS伺服器。Harris設立了一個假的WHOIS伺服器，並填入假資料，最終成功簽發偽造的HTTPS憑證，攔截通訊並模仿合法網站。這項研究促使ICANN發布警告，強調流氓WHOIS伺服器的安全風險。

這起事件令人擔憂的地方在於，註冊管理機構理應比任何人都更了解註銷敏感域名的風險，但此案例顯示，許多受理註冊機構與憑證管理機構（Certificate Authorities，CA）仍持續查詢已下線的WHOIS伺服器，且未發現異常，顯示業界在資安意識上仍有不足，域名資料管理及相關流程也仍有很大的改進空間。

老舊的WHOIS協議無法提供與RDAP相同的結構化存取機制，加上RDAP支援身分驗證與存取控制，可提升安全性。作者呼籲各界應盡快由WHOIS過渡至RDAP。此外，重要的域名即使已不再使用於任何活動或服務，也切勿讓域名失效，因為一旦被不法分子重新註冊後，可能會被用於網路犯罪，帶來嚴重的安全風險。

