



mod^a

數位發展部
Ministry of Digital Affairs

ICANN AUGUST NEWSLETTER

2024

TABLE OF CONTENTS

01

頭條新聞

亞太網路治理學院擴展計畫

02

最新消息

ICANN公告2024年國際化域名報告

ICANN公告新DNSSEC錨點

2024年亞太DNS論壇：人際交流、互助
合作及教學相長

03

公眾意見徵詢

註冊管理機構與受理註冊機構資料處理條款
無參考用LGR的gTLD IDN參照表審核流程
涉及ICANN獎助計畫的組織章程修訂
轉移政策審核初步報告

04

文摘

一舉奪金：強健網際網路韌性的重要
中介方的崛起

頭條新聞

亞太網路治理學院擴展計畫

亞太治理網路學院（Asia Pacific Internet Governance Academy，APIGA）是以亞太地區18至35歲的年輕人為主要對象，聚焦於網路治理的知名人才培育計畫。根據統計資料，每4名APIGA畢業學員中，就有1名持續參與本地、地區或全球網際網路活動。第八屆APIGA也於今年7月於韓國釜山圓滿落幕。

ICANN今年8月宣布推出APIGA擴展計畫，將APIGA延伸至本地層級。2024年總計將有4場當地規模的APIGA活動。ICANN與共同主辦方韓國網路振興院（Korea Internet and Security Agency，KISA）認為，「本地APIGA」（Local APIGA）將有效補強在韓國舉辦的年度區域APIGA，於本地APIGA脫穎而出的優秀學員，將可直接參與區域APIGA。



這個擴展計畫希望彌補APIGA高競爭、低錄取率的遺憾，增加本地年輕族群體驗APIGA課程的機會。不僅如此，本地APIGA以當地語言進行，也幫助非英文母語的年輕學子更加輕易、深入學習網路治理。

今年4月由NII產業發展協進會於臺北舉辦的「亞太網路治理學院－臺灣研習營」，作為史上首屆本地APIGA獲得巨大成功。包括尼泊爾、印尼及澳洲也計畫於今年2024年舉辦本地APIGA，更多相關資訊可參考[ICANN網站](#)。

最新消息

ICANN公告2024年國際化域名報告

ICANN發布的2024年6月國際化域名（Internationalized Domain Name, IDN）報告中，包含頂級域名及第二層域名的IDN概況總覽，以及ICANN Org與社群自2023年1月至2024年6月完成的IDN相關工作。[點此閱讀](#)報告全文。

有了IDN，全世界的使用者、企業和政府因此能使用本地語言和文字域名。這也是確保數位包容、多語言網際網路的關鍵。為達成[ICANN戰略計畫](#)「推廣IDN與全球通用」的目標，ICANN Org持續與社群合作，在協助全球多語言人口以母語使用DNS的同時，維護DNS的安全與穩定。

ICANN Org每年發布IDN報告，追蹤IDN進展並記錄亮眼成績。這些報告聚焦於四大主題：發配與註冊統計資料、ICANN社群制定的IDN政策、ICANN Org進行的IDN相關專案，以及已實施運行的IDN成果。本次報告亮點包括IDN頂級域發配及第二層域名註冊統計數字、GNSO與ccNSO相關政策工作進展，以及ICANN Org在支援IDN政策制定及實踐運行上的各項專案。

更多IDN相關資訊可參考ICANN網站中的[IDN專屬網頁](#)。



**IDNs and UA continue
to be a strategic
focus for the ICANN
organization.**

ICANN公告新DNSSEC錨點

ICANN 最近透過網際網路指派號碼機構（Internet Assigned Numbers Authority, IANA）功能，公告新域名系統安全擴充（Domain Name System Security Extensions, DNSSEC）安全錨點。

DNSSEC安全錨點是DNSSEC系統的最終信任點。DNSSEC驗證域名資料為真、避免遭第三方仿冒假造，並藉此保護DNS安全。信任錨點的更新，需要網際網路基礎建設營運方之間密切謹慎的合作，確保無縫轉移，才能維護DNS的安全與穩定。



本次公告更新乃新增加密金鑰，預計於2026年開始使用此新信任錨點，簽署DNS根區。ICANN鼓勵軟體供應商及系統封裝廠商現在就開始準備相關流程。

ICANN計畫於2025年1月11日於DNS事先發布新加密金鑰，如此一來，到2026年10月預訂金鑰汰換（Rollover）日期為止，有近兩年的準備期間。所有金鑰汰換實務運作相關消息，都會於 [root-dnssec-announce](#) mailing list公告。社群討論則建議前往[ksk-rollover mailing list](#)。

2024年亞太DNS論壇： 人際交流、互助合作及教學相長

第三屆亞太DNS論壇於2024年7月23至24日於印尼峇里島圓滿落幕。根據論壇期間的非正式統計，幾乎所有與會者都藉此盛會認識了新朋友、學到新東西，也不不少人發現了新的機會。

亞太DNS論壇創立的初衷，是打造亞太社群專屬的交流合作常設平臺。今年的論壇除了主場次外，還有4場帶來加值體驗的場邊會議，包括：

- 亞太地區政府諮詢委員會（Governmental Advisory Committee, GAC）能力建構。
- 以印尼當地技術講師人才為對象、聚焦於DNS和DNSSEC的講師教育訓練。
- 針對峇里語、爪哇語、洋涇浜英語（Pegon）及巽他語，印尼當地社群共同討論制定第二層域名的標籤生成規則。
- 國際商標協會（International Trademark Association, INTA）主辦，討論品牌及商標保護的活動。

其他值得一提的亮點包括：

- 所有與會者在開幕座談中，共同討論出國際網路面臨的當地挑戰與機會。關鍵教訓是我們發現，網路自發明以來，僅在「便宜、快速、良好」鐵三角中的前兩項有長足進展。如今我們必須轉移目標，集中於推動包括安全、隱私及加值網路服務的「良好」。
- 論壇期間深入探討「信任通報」機制，亦有中介服務業者在論壇期間簽署雙邊信任通報協議。
- 域名產業的發展與機會，包括鼓勵、確保當地社群可使用母語電子郵件和域名，以促進數位包容。針對即將於2026年展開的New gTLD未來回合，討論則集中於數位資產管理策略、申請與否考量因素等。

[點此觀賞論壇場次錄影。](#)



公眾意見徵詢

註冊管理機構與受理註冊機構資料處理條款

針對將納入ICANN註冊管理機構協議及受理註冊機構驗證協議的資料處理條款（Data Processing Specifications, DPS），目前徵求社群意見中。本條款乃根據gTLD註冊資料臨時條款加速版政策發展流程第一階段結案報告中第19、20項建議，由ICANN及合約方協調後制定。

提案內容

- Draft Registrar Data Processing Specification
- Draft Registry Data Processing Specification

時程進度

開放徵詢
29 July 2024
結束徵詢
09 September 2024
社群意見統整報告
23 September 2024

提交意見



涉及ICANN獎助計畫的組織章程修訂

本提案針對ICANN組織章程的第四章4.2及4.3節，將明文規定禁止個人利用獨立審核流程（Independent Review Process, IRP）或其他ICANN重審機制（統稱「當責機制」），挑戰ICANN獎助計畫的補助對象決定。

提案內容

- Draft Proposal on Fundamental Bylaws Amendment

時程進度

開放徵詢
07 August 2024
結束徵詢
16 September 2024
社群意見統整報告
23 September 2024

提交意見

公眾意見徵詢

無參考用標籤生成規則的gTLD 國際化 域名 (IDN) 參照表審核流程

參考用標籤生成規則 (Reference Label Generation Rules, Ref. LGRs) 適用於第二層域名，透過ICANN Org與相關語言文字社群密切合作產出。參考用LGR的主要用途是審核gTLD註冊管理機構提交的IDN參照表。

目前已完成的參考用LGR共有26份。然而，還有161種萬國碼 (Unicode) 標準容許的文字缺乏適用的參考用LGR。ICANN因此制定此情境下的審核流程提案，並徵求社群指教意見。

提案內容

- Proposed Process to Review gTLD IDN Tables Without Reference Label Generation Rules

時程進度

開放徵詢	01 August 2024
結束徵詢	12 September 2024
社群意見統整報告	26 September 2024

提交意見

轉移政策審核初步報告

轉移政策審核政策發展流程初步報告內容涵蓋gTLD轉移相關議題，並提出許多修訂現行轉移政策的建議。工作小組誠邀社群建議與指教。

提案內容

- Initial Report on the Transfer Policy Review Policy Development Process

時程進度

開放徵詢	01 August 2024
結束徵詢	30 September 2024
社群意見統整報告	28 October 2024

提交意見

文摘



一舉奪金：強健網際網路韌性的重要

文章出處：ISOC Blog

原文作者：Kelly O'Hara

一旦獲選成為奧運主辦城市，大型基礎建設更新工程便必須隨之展開，準備迎接上千運動選手及上百萬觀賽民眾的到來。如果事前規劃不足，奧運為主辦城市帶來的人潮，很可能嚴重干擾當地交通，甚至是當地居民的日常生活。

那麼，「數位交通」呢？自宣布巴黎將主辦2024年奧運，每當有新的公告、比賽門票開賣、競技開始時，2024年巴黎奧運官方網站的**訊務**都會飆升。

當地網路的韌性確保強健的全球網際網路

雖然網際網路的關鍵根基全球一致，但其效能和使用者體驗仍受各種因素影響。諸如基礎建設、安全、效能和市場準備度，都是用來評量特定地區內網際網路韌性的標準。

確保法國境內的網際網路韌性，足以在奧運期間抵擋（故意或無意地）連線不穩定、提供遊客可靠連線，維持效能而不受激增使用者用量影響，是關鍵課題。尤其今年7月底法國境內數條通訊纜線遭刻意破壞的**事件**，更彰顯此間重要。

網際網路韌性的全球重要性？

奧運期間全球網際網路的重要性絕不亞於巴黎境內。全世界的運動迷需要透過各種管道參與這場盛事：在社群媒體平臺上討論、追蹤新聞、關心獎牌統計數據，以及即時或事後觀賞賽事播映等。然而，住在哪裡可能左右一個人能否為喜歡的選手或隊伍加油。

舉例而言，田徑是最多人看的奧運賽事。奪牌選手可能來自任何地方，但歷史統計數據而言，來自衣索比亞、牙買加、肯亞和美國的選手通常稱霸此領域。住在美國的人能輕鬆透過網路線上觀賽，但衣索比亞的居民可能無法同樣輕易觀賞賽事直播。

目前衣索比亞境內**沒有**任何網際網路交換中心（Internet Exchange Points, IXP），當地網路連線、網路速度和使用經驗因此仍亟需改善。衣國境內的網路覆蓋率也仍不高（雖然近年來有顯著進步），即使可以上網，由於當地停電及網路斷線事件頻傳，網路費用仍高昂且品質不穩定。

網際網路韌性是團隊運動

就像所有奪金的隊伍，攜手合作才能確保最佳網路。區域內鄰近國家的合作，能改善彼此的網路韌性並確保連線；即使發生**海纜損壞**等可能引發大規模網路斷線的事件，也能儘速改道並重新連線。

網際網路凝聚人心的力量就如奧運，也都需要我們的合作支持才能持續成長茁壯。

文摘



中介方的崛起

文章出處：DNS Research Federation

原文作者：Mark McFadden

中介方（Intermediary）作為網路上各種資源與使用者之間協調溝通的中間人，扮演形塑網際網路使用經驗的關鍵角色。這些中介方包含內容傳遞網路（Content Delivery Network，CDN）、惡意軟體偵測業者、隱私保護工具等，發揮提升網速、安全及使用者隱私等功能。

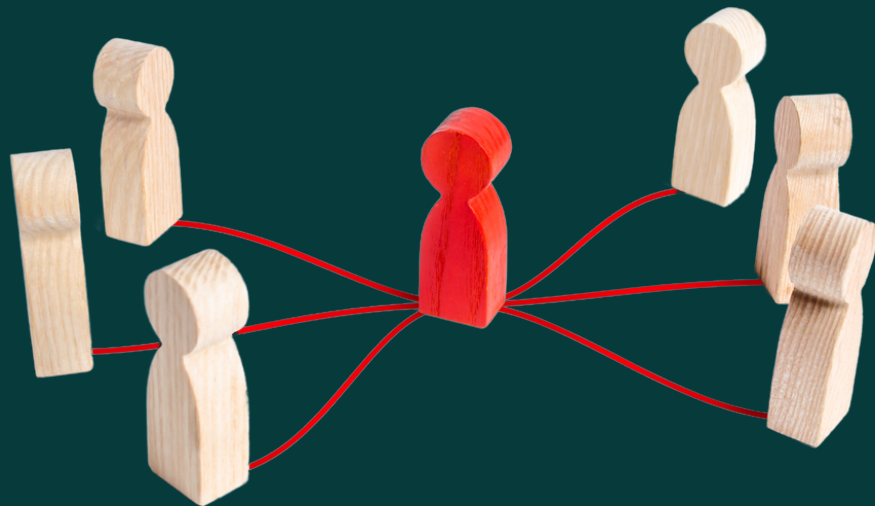
在網際網路基礎建設的脈絡中，中介方也促成更具韌性、更使用者友善的線上環境。雖然使用者不一定知情，但他們直接受惠於中介方提供的網速提升、安全強化及使用者隱私等功能。

隨著網際網路持續進化，中介方的角色在面對新興挑戰、解決使用者需求上，也將日益關鍵。

3種關鍵中介方

內容傳遞網路（CDN）透過策略性將伺服器部署於分散式網路上，就近提供終端使用者快取內容，確保網站內容瀏覽體驗更即時順暢。惡意軟體偵測工具會即時掃描網站、檔案下載及電子郵件附件等，以發現並封鎖潛在危險。

隱私保護工具如虛擬隱私網路（virtual private network，VPN）和匿名代理伺服器服務等，則以安全頻道路由網際網路訊務，確保使用者匿名、保護敏感資訊並防止潛在監控。



IETF的中介方和標準

從標準的觀點來看，隱私保護工具饒富興味。多年來，網路工程任務組（Internet Engineering Task Force，IETF）始終大力宣導安全隱私。現在所有IETF發布的新RFC都必須涵蓋「安全考量」（Security Considerations）章節，雖然此章節中不一定會包含「隱私考量」（Privacy Considerations），但IETF和網際網路架構委員會（Internet Architecture Board，IAB）始終致力發展隱私保護協定。

文摘

網際網路架構委員會（IAB）立場

IAB有一份使用中介方保護隱私的**介紹草稿**。這份草稿仍未正式以RFC形式發布，內容解釋代理服務（proxy）的歷史用法，並檢視使用中介方作為隱私工具的4種不同協定，以及最重要的，使用中介服務的限制。

Privacy Pass

你有在進入某個網站時，被要求從組圖中**選出腳踏車**的經驗嗎？這工具是為了分辨人類使用者與機器人，但應該有不那麼惱人的其他方式。IAB文件提到的隱私通行證（**Privacy Pass**）就是其中一種。簡單來說，隱私通行證利用加密技術而非拼圖來達到辨別機器與人類的目的。除此之外，隱私通行證也容許使用者要求取得資源時無需洩露隱私資訊。

回想一下參加啤酒博覽會的經驗：你透過線上購票憑證在入場時換到一個手環及兩張試飲券。攤位人員看到手環會知道你有買票，但事後無法透過試飲券追蹤你的身分。隱私通行證的實際運作就是這個概念，只是在網際網路上發生：它連接內容使用者與內容提供方，但雙方被隔離，使用者因此在交易中保有一定隱私。

IETF正在準備以RFC發布此**協定及架構**，Cloudflare也已經為**Firefox**和**Chrome**開發擴充程式，以利用支援此協定的網站。Apple的隱私存取通行證（**Private Access Tokens**）也是實作範例。

這很重要嗎？

網際網路的架構初衷是「端對端」，網路邊緣才是情資真正的所在地，中心的用途單純僅為傳輸，沒有任何其他服務。此初衷如今已不再。因為中介服務IETF協定研發出現有趣的演變：過去IETF僅專注於兩個終端之間的協定，如今協定是想著中間人在設計。

但如果協定開始**內建對中介服務的依賴**，將導致網路與經濟的集中化透過協定被進一步實現固化。我們必須持續關注此議題的其他面向。