

ICANN NEWSLETTER

Aug. 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

- ICANN 公布《2026 New gTLD 字串相似度評估指南》定案版本 1

最新消息

- ICANN 2026 New gTLD 申請窗口正式截止 4
- ICANN 發布 Root Zone KSK 輪替指引 6

公眾意見徵詢

- 技術研究小組關於 gTLD 與替代命名系統整合的初步報告 8
- DNS Abuse Mitigation PDP1《初步報告》公眾諮詢 9

文摘

- 印度 DNS 濫用危機下的受理註冊機構問責缺口 11

ICANN 公布《2026 New gTLD 字串相似度評估指南》定案版本

ICANN 於 2026 年 7 月 30 日正式發布《字串相似度評估指南》(String Similarity Evaluation Guidelines, 簡稱 SSE Guidelines) 及配套之《字串相似度評估資料》(String Similarity Evaluation Data, 簡稱 SSE Data) 定案 1.0 版本, 以供獨立運作之「字串相似度評估小組」(SSE Panel) 執行本輪申請之字串相似度評估作業。此一制度之政策依據源自 GNSO《New gTLD 後續程序政策發展流程最終報告》第 24 章之建議, 並依《國際化域名加速版政策制定流程》(IDN EPDP) 第一階段最終報告之要求, 將比對範圍擴大納入申請字串之變體字串 (variant strings) ; 其核心目的在於防止因核准視覺上相似之頂級域名, 導致使用者混淆、進而損及全球大眾對域名系統之長期信賴, 機制細節則規定於《2026 New gTLD 申請指南》(AGB) 第 7.10 節。

本次機制採取「SSE Data + SSE Tool + SSE Panel」三層架構。第一層 [SSE Data](#) 由各文字系統之語言學專家, 針對根區標籤生成規則 (Root Zone Label Generation Rules, RZ-LGR) 之完整字碼範圍進行視覺相似性分析, 並將相似程度區分為以下五級, 「相同或近乎相同 (同形異義字) , 或 RZ-LGR 中已定義之變體字元」、「高度易混淆」、「相似」、「弱相似」及「明顯不相似」, 其中前三級原則上均視為具視覺相似性。各文字系統專家完成初步比對後, ICANN 再對全部專家資料進行三道整合品管, 包括人工複核語法格式與比對範圍完整性、跨文字系統一致性校對 (協調不同專家對同一組跨文字系統配對之判定歧異) , 以及遞移律 (transitivity) 檢查 (將經比對

鏈間接串連之字碼一併納入同一相似組別)。經此程序後，資料方轉換為供 SSE Tool 運算之機器可讀格式，同時提供人工可查閱之 HTML 版本。

第二層 SSE Tool 則依 AGB 第 7.10.1 節所定範圍，將每一申請字串及其變體字串，與既有 gTLD、前一輪申請中仍在審理之字串、既有 ccTLD、被請求之國際化國碼頂級域名 (IDN ccTLD)、本輪其他申請字串、被封鎖名稱 (Blocked Names)，以及二字元 ASCII 字串等七大類別進行自動化預篩比對，產出「潛在競合集合」

(potential contention sets)，供後續審查。最後，第三層由 SSE Panel 依 SSE Guidelines 進行人工審查並作成最終判斷，小組須附理由方得調整、新增或刪除由第二層工具提出之潛在競合集合；但就少數未能由第二層工具所報告之字串，如變體字串數量逾工具比對上限，或因資料整合技術限制未納入 SSE Data 之特定字碼組合，在缺乏潛在競合集合的情況下，須由 SSE Panel 逐一人工複核；若判斷存在疑義，指引則要求採取較為保守之認定方式，傾向判定為相似。

本次定案版 SSE Data 之建置過程，亦揭露 ICANN 在處理漢字 (Han script) 此一跨國共用文字系統時所採行之作法，對我國具高度參考價值。依《SSE Data Overview》所載，中文 RZ-LGR 涵蓋 19,685 個漢字碼點，韓文 RZ-LGR 則涵蓋 4,758 個，兩者

漢字	碼位	漢字	碼位
青	U+9752	青	U+9751
清	U+6E05	清	U+6DF8
精	U+7CBE	精	U+FA1D
靖	U+9756	靖	U+FA1C
晴	U+6674	晴	U+FA12
請	U+8ACB	請	無
情	U+60C5	情	無
晴	U+775B	晴	無

資料來源：Wikipedia

共 4,744 個重疊字碼點。由於待比對之漢字碼點數量龐大，中文文字系統專家於 2025 年公眾諮詢完成後，另採用人工智慧輔助分析，結合卷積神經網路 (CNN)、筆畫結構分析、Zernike 矩，以及格狀直方圖等四種核心演算法，額外辨識出 1,612 組相似案例，並基於保守原則，一併納入中文、日文、韓文三語系之 SSE 資料。此一作法顯示，SSE Data 之建置係以人工智慧輔助專家分析，而非交由演算法逕行判定；依 SSE Guidelines 第 8 節結論，字串相似度評估之最終決定權亦仍屬 SSE Panel，而非 SSE Tool 或人工智慧本身。

2024 年 2 月 SSE Guidelines 草案發布之初，即有曾參與 New gTLD 政策基礎架構制定工作之資深政策顧問提出[質疑](#)，指出自動化預篩工具與演算法比對模型可能構成一道欠缺透明度之「不透明守門機制」，並援引 2012 年之「.africa」字串爭議為例，主張評估機制若欠缺公開可受檢驗之判準與申訴途徑，恐重蹈治理失靈之覆轍。對此，定案版指引雖未新增獨立之申訴救濟章節，但如前段所述，明確賦予人工判斷最終地位，並要求 SSE Panel 就每一項偏離工具建議之決定附具理由，以此作為對外界疑慮之部分回應；此一設計是否足以完全化解申請人疑慮，仍待後續觀察。

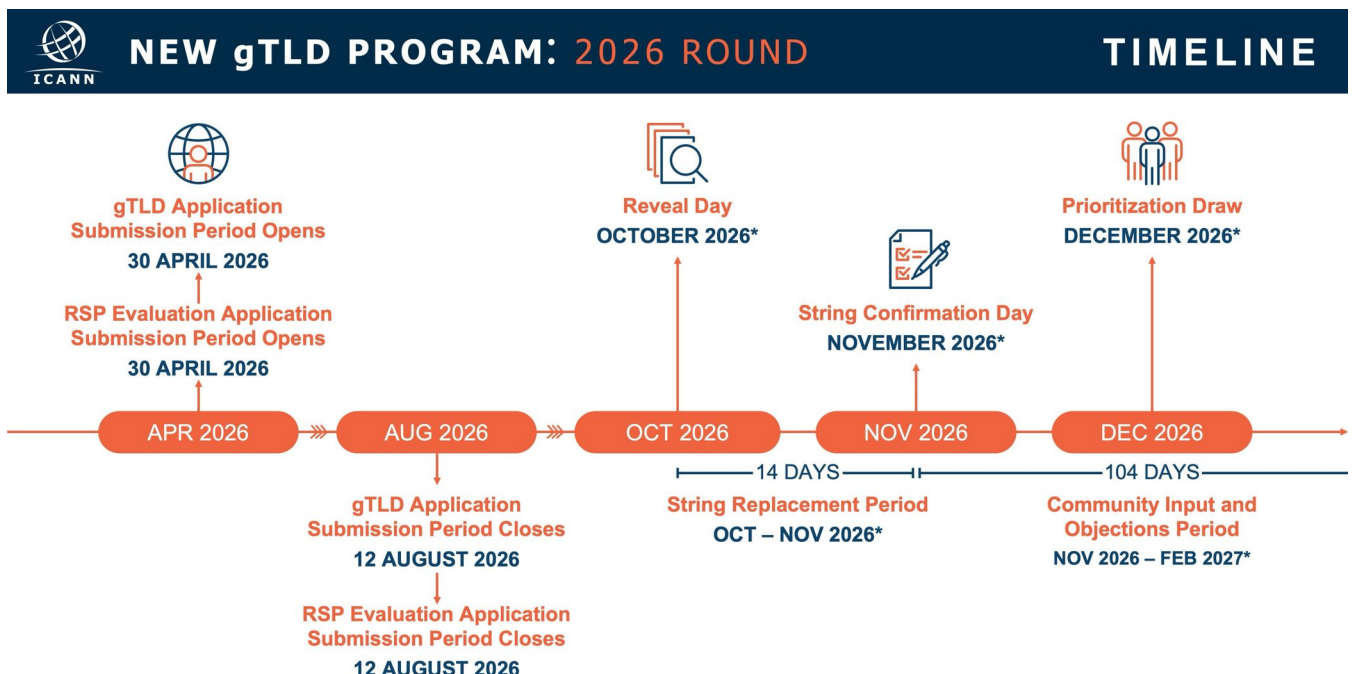
整體而言，鑑於本輪逾 1,600 件申請、涵蓋 27 種文字系統，加以本次 SSE Data 中日韓三語系資料之建置過程，已直接處理中文漢字碼點之視覺相似性判定，此一議題對於已提交中文或其他 CJK 相關字串申請之單位，將直接關係其申請字串於後續評估階段是否面臨競合認定；對持續關注本輪後續發展及未來輪次政策設計之研究者而言，亦具有實質參考價值。

[資料來源連結](#)

ICANN 2026 New gTLD 申請窗口正式截止

2026 New gTLD 的申請窗口已於 2026 年 8 月 12 日 23:59 (UTC) 正式關閉。在為期 15 週的申請窗口期間內，ICANN 總共收到超過 1,600 件主要申請案 (Primary Applications)，其中有 1,100 多件另附有替代字串 (replacement strings) 申請，此類申請官方稱為「次要申請」 (Secondary Applications)。相較 2012 年 1,930 件申請，本輪件數略減約 300 件。

ICANN 特別提醒，依規定申請人須於評估規費 (每案 22.7 萬美元) 發票開立後七日內完成繳費，以 8 月 14 日開立之發票為例，繳費期限即為 8 月 21 日；在全數規費入帳確認前，目前公布之申請件數仍屬暫定性質。



*Projected timeline based on 2,000 applications received. Estimations will be updated once the number of applications is publicly shared. Several factors may impact the timeline.

資料來源：ICANN

後續重要時程：行政審查與「揭露日」

申請窗口截止後，ICANN 將針對所有收到的 New gTLD 申請案展開行政審查 (Administrative Check)。完成行政審查後，ICANN 將於「揭露日」 (Reveal Day) 當天，公開已通過行政審查之申請案中，供公眾檢視的部分內容；屆時，申請人與網際網路社群將能掌握各字串的申請狀態，並得知哪些字串之間可能存在相互競合 (in contention) 之情形。

除有特殊情形外，ICANN 預計於申請窗口截止後 9 週內 (即 2026 年 10 月中旬前)，在揭露日當天正式公布通過行政審查之申請案完整清單。ICANN 並預計於 2026 年 9 月中旬，進一步向社群宣布揭露日的確切日期，以及後續各階段關鍵時程。

依 AGB 規定，揭露日後申請案將進入以下三大後續階段：公眾意見與異議程序 (Community Input，含公眾意見及正式異議)、競合集合解決程序 (Contention Set Resolution，其中特別明文禁止申請人私下協議解決字串競合，須循 ICANN 既定程序如拍賣等方式處理)、以及申請人暨申請案評估程序 (Applicant and Application Evaluation)。

[資料來源連結](#)

ICANN 發布 Root Zone KSK 輪替指引

為確保全球網際網路安全更新順利進行，ICANN 於 2026 年 7 月 27 日發布更新版「根區 KSK 輪替期間應注意事項」(What to Expect During the Root KSK Rollover) 指引，此文件係接續 2018 年首次發布之版本修訂而成。該指引旨在協助技術社群及網路生態系統營運者，為預定於 2026 年 10 月 11 日進行的「根區金鑰簽署金鑰」(Root Zone Key Signing Key, KSK) 輪替做好準備。屆時，新一代金鑰 KSK-2024 (Key Tag 38696) 將正式接替現行金鑰 KSK-2017，成為域名系統安全擴充 (Domain Name System Security Extensions, DNSSEC) 信任鏈中後續驗證的核心根金鑰；此為 ICANN 史上第二次執行根區 KSK 輪替 (首次為 2018 年)。KSK-2024 已自 2025 年 1 月起預先發布於根區，提供約 21 個月準備期，供各驗證解析器透過自動信任錨更新機制完成準備。



資料來源：ICANN

Root KSK 位於 DNSSEC 信任鏈的最上層，負責驗證 DNS 資訊的真實性與完整性，確保使用者獲得正確的解析結果而非遭竄改的欺詐資料。ICANN 指出，對於已正確配置並更新信任錨點 (Trust Anchor) 的驗證遞迴解析器 (validating recursive resolver)，此次輪替作業原則上不會產生感知的影響；然而，若系統未正確配置新

金鑰，可能於輪替後 48 小時內（依相關記錄之存活時間, Time To Live, TTL 而定）開始出現 DNS 解析失敗的風險。

本次更新指引詳述了輪替過程中的預期情境及營運者應採取的準備措施。ICANN 特別提醒各驗證解析器營運者（包含 ISP 與企業網管），應立即確認系統的信任錨點設定中已包含 KSK-2024（Key Tag 38696），不應逕自假設自動更新機制必能成功運作。若驗證失敗已實際發生，指引亦提供應急做法：可暫時關閉 DNSSEC 驗證功能，或依 RFC 7646 設定「否定信任錨」（negative trust anchor）以使服務立即恢復正常，並儘速安裝 KSK-2024 後重新啟用驗證功能。指引並特別說明，本次輪替僅更換金鑰本身，其簽署演算法（RSA/SHA-256）維持不變；下一次預計於 2029 年完成之輪替，始會一併變更為橢圓曲線數位簽章演算法（Elliptic Curve Digital Signature Algorithm, ECDSA）。

Root KSK 輪替是維護全球 DNS 長期穩定、安全性與韌性的重要維運程序。透過「網際網路號碼指配組織」（Internet Assigned Numbers Authority, IANA）的嚴謹作業與定期舉行的公開 KSK 金鑰儀式（KSK Ceremonies），ICANN 持續確保根金鑰的安全管理與社群透明參與。ICANN 呼籲技術社群提前檢視指引並完成系統核對，以確保在 2026 年 10 月的關鍵轉換期內，全球 DNS 服務能維持正常運作。

[資料來源連結](#)

技術研究小組關於 gTLD 與替代命名系統整合的初步報告公眾意見徵詢

ICANN 就技術研究小組 (Technical Study Group, TSG) 提出的「gTLD 與替代命名系統整合初步報告」公開徵求社群意見。近年部分 gTLD 註冊管理機構及 2026 年新 gTLD 計畫申請人，希望將全球域名系統中的 gTLD 與替代命名系統 (Alternative Naming Systems, ANS) 中的相同字串建立關聯。由於此類服務可能涉及 DNS 之安全與穩定，ICANN 遂成立 TSG 進行整體技術評估。

TSG 在初步報告中指出兩者整合原則上具有可行性，但必須確保相同字串在不同系統中始終由同一控制者管理，即「相同字串 + 相同控制者」 (string+controller integration) 原則。此原則的核心目的在於處理 Web3 域名與傳統 DNS 的連結，避免同一名稱在不同系統中指向不同控制者，造成混淆、詐欺及其他安全風險。

報告提出兩種模式：第一種透過「共用註冊系統」 (Shared Registration System, SRS) 運作，由現有 DNS 註冊框架同步管理替代端；第二種為分散式模式，透過「統一真實來源」 (Unified Source of Truth, USoT) 確保各處名稱與控制者資訊一致。無論採取何種模式，申請機構均須證明其設計不會對網際網路安全造成風險。

此外，報告亦將名稱的生命週期管理納入考量，包括名稱啟用、停用、暫停及保留等不同狀態，要求一旦名稱在任一整合命名系統中被配置，相關狀態原則上應能在其他整合系統中維持一致；若整合關

係無法繼續維持，則應具備安全的終止機制（turn-down plan），避免不同系統間產生不一致狀態。

本次公眾意見徵詢主要徵詢社群對報告所提出技術要求是否足以維護 DNS 之安全與穩定，以及對初步報告其他內容之意見。

進度時程：

開放徵詢：10 Aug. 2026

結束徵詢：21 Sep. 2026

社群意見統整報告：5 Oct. 2026

[提案內容連結](#)

DNS Abuse Mitigation PDP 1 《初步報告》公眾意見徵詢

ICANN 就「DNS 濫用防制政策制定小組（DNS Abuse Mitigation PDP 1, DNSAM PDP1）」所完成之《初步報告》展開公眾意見徵集，於 8 月 18 日開啟，預計 9 月 28 日截止，為期 40 天。DNSAM PDP1 係由 GNSO 理事會授權成立，為 2025 年 12 月發布之《DNS 濫用減輕最終議題報告》中兩項 DNS 濫用減輕政策發展流程之第一項任務，其核心內容係研議是否應課予受理註冊機構一項義務：於確認客戶帳戶或註冊人名下至少一個網域涉及《受理註冊機構驗證協議》（RAA）所定義之 DNS 濫用行為時，須進一步調查與該帳戶或註冊人相關聯之其他網域，此即所謂「關聯網域檢查」

(Associated Domain Checks, ADC)。工作小組於 ICANN85 開始進行討論，本初步報告即為工作小組歷經逾 30 次會議後，對 PDP 章程所列問題之回應與成果。

本次公開徵詢的《初步報告》共提出 8 項初步建議與 5 項實施指引，並同步完成人權影響評估、全球公共利益檢核表、資料隱私議題考量，以及對現行 ICANN 共識政策衝擊評估等多項配套研究。

為利各界精準對應意見與具體建議或指引項目，工作組特別採用「引導式意見提交表單」，使評論人得逐項針對各建議或指引提出看法，並須就整體意見提交摘要說明；該表單雖有助於結構化意見蒐集，惟不限制評論範圍，各界仍可就《初步報告》任何面向自由表達意見。

進度時程：

開放徵詢：18 Aug. 2026

結束徵詢：28 Sep. 2026

社群意見統整報告：16 Oct. 2026

[提案內容連結](#)

印度 DNS 濫用危機下的受理註冊機構問責缺口

文章出處：[CircleID](#)

原文作者：Garv Chauhan

CircleID 於 2026 年 7 月 24 日刊登印度國家鑑識科學大學網路安全領域學生 Garv Chauhan 之文章，探討印度數位公共基礎建設（Digital Public Infrastructure, DPI）快速發展下，惡意網域名稱所造成的 DNS 濫用（DNS abuse）問題，以及網域名稱受理註冊機構（registrar）在其中應負擔的問責責任。

作者以其參與 NGO 活動時遇到的一名印度少女為例。該少女曾差點在仿冒政府求職入口網站上提供家人的印度生物識別身分證號（Aadhaar）、手機號碼及家庭資料；該假網站在版面、語言及表單欄位上均與官方網站高度相似，僅網域名稱存在一個字母的差異。由於網路中斷，少女最終未送出資料。作者認為，這類事件的責任不應只聚焦於受害者與攻擊者之間，更應正視扮演「基礎設施入口」角色的網域受理註冊機構。

就受理註冊機構集中程度而言，Forescout 針對 2024 年 12 月至 2025 年 6 月期間觀察到的 11,894 個惡意軟體通訊網域進行分析，發現前 10 大受理註冊機構占全部惡意網域的 54%，前 100 大則占逾 90%，這顯示 DNS 濫用高度集中於少數受理註冊機構。作者據此認為，若針對主要業者施加問責壓力，可能具有較大的治理效果。

作者同時指出，ICANN 於 2024 年修訂受理註冊機構驗證協議（RAA）及通用頂級域名標準註冊管理機構協議（RA），已為受理

註冊機構及註冊管理機構增訂明確之 DNS 濫用緩解義務（依 ICANN 官方說明，即於取得可採取行動的證據後，應採取適當且合理必要之措施停止或干擾 DNS 濫用）。此外，DNS 研究聯盟



資料來源：DNSRF

（DNS Research Federation, DNSRF）資料顯示，惡意網域名稱於 24 小時內完成緩解處理（mitigation）的比例，已由 2024 年 9 月的 13% 提高至 2025 年初的 20%；惟仍有約八成惡意網域超過 24 小時後仍處於活躍狀態。

作者認為，印度的問題具有特殊性，一方面，印度數位公共基礎建設快速將政府服務及各類計畫入口數位化，使相關網站成為高度集中的仿冒目標；使用者對政府服務的信任及取得服務的急迫性，也容易遭相似網域利用。另一方面，印度電腦緊急應變小組（Computer Emergency Response Team-India, CERT-In）的通報流程預設使用者具備一定程度的數位素養，使部分較脆弱的使用者可能難以有效提出通報。

因此，作者主張印度應建立能反映 DPI 攻擊面的受理註冊機構問責框架，包括強化財務制裁、建立具有實質後果的 DNS 濫用處理時限，以及改善低數位素養使用者的通報機制；對於涉及政府服務或計畫入口網站的相似網域，則應進一步思考受理註冊機構的審查及減害責任。文章最終將問題從單一惡意網域的處理，提升至「誰應承擔 DNS 濫用所產生的治理成本」的制度性問題，值得觀察 ICANN 既有 DNS 濫用緩解義務與印度 DPI 發展之間如何進一步銜接。