

ICANN NEWSLETTER

Sept. 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 發布《推動普遍接受採納指引》，訂定 47 項具體建議與四構面量測架構 1

最新消息

- ICANN Domain Metrics 新增 DNS 濫用緩解時間量測功能 3
- ICANN 公布 New gTLD 申請之保障措施評估服務商 5

文摘

- Project Jake：網域註冊資料揭露的新模式 6
- DNS 濫用檢舉與下架之間的「通報落差」 10

ICANN 發布《推動普遍接受採納指引》，訂定 47 項具體建議與四構面量測架構

ICANN 於 2026 年 9 月 9 日發布由「普遍接受專家工作小組」(Universal Acceptance Expert Working Group, UA EWG) 制定之《推動普遍接受採納指引》(Guidelines for Advancing Universal Acceptance (UA) Adoption)，其核心目標在於解決國際化網域名稱及電子郵件地址長期無法為各類網路應用正確辨識之問題。UA EWG 於 2025 年 8 月 18 日成立，依章程所列 10 項核心問題 (Charter Questions) 研擬相關建議；草案經 2026 年 2 月 23 日至 4 月 13 日公開徵詢意見後，於 8 月 20 日完成定稿，並於 9 月 9 日正式對外發布，ICANN 表示社群普遍支持該指引之方向與架構。

所謂「普遍接受」(Universal Acceptance, UA)，係指所有有效之網域名稱及電子郵件地址，不論採用何種文字系統、語言或字元長度，均應能被網路應用程式、裝置及系統正確接受、驗證、儲存、處理及顯示，與國際化網域名稱 (Internationalized Domain Names, IDNs) 及電子郵件地址國際化 (Email Address Internationalization, EAI) 密切相關。依 [CircleID](#) 報導，電子郵件地址國際化之支援比例雖已由 2021 年之 19.5% 成長至 2026 年之 29.2%，惟多數使用者以本地語言電子郵件地址於網站或社群平台申請帳號時，仍經常遭遇無法正確辨識之情形。指引文件強調，UA 並非個別應用程式或前端介面可獨力解決之問題，而是橫跨 Unicode 標準、作業系統、瀏覽器、身分驗證系統及各類應用程式之「技術堆疊問題」，須由函式庫、DNS 及電子郵件系統等不同技術層級共同支援。

本次[文件](#)共提出 47 項具體建議，逐一對應章程所列 10 項核心問題，依序涵蓋大型科技公司、開源軟體社群、標準制定組織、軟體開發者、系統管理員、DNS 產業、主機與網際網路服務提供者、公部門與政府間組織、學術界，以及量測架構等 10 大面向。就政府角色而言，第 34 項建議明確建議由政府諮詢委員會 (Governmental Advisory Committee, GAC) 之 UA 工作小組接觸各國政府代表，鼓勵各國政府組成在地任務小組，納入國碼頂級網域名稱 (ccTLD) 管理者、技術社群及公部門代表共同參與。為追蹤推動成果，指引另提出認知度 (Awareness)、政策支持 (Policy Support)、實作 (Implementation) 及能力建構 (Capacity Development) 四構面量測架構，分別以活動與媒體宣傳、國家政策與電子化政府整備度、網域與電子郵件註冊及伺服器能力之實際使用數據，以及課程與人才培訓資源為衡量指標，並建議建立 UA 成效儀表板持續呈現採用進展。惟指引本身屬諮詢性質，並未直接對 ICANN 或相關利害關係人創設強制義務。

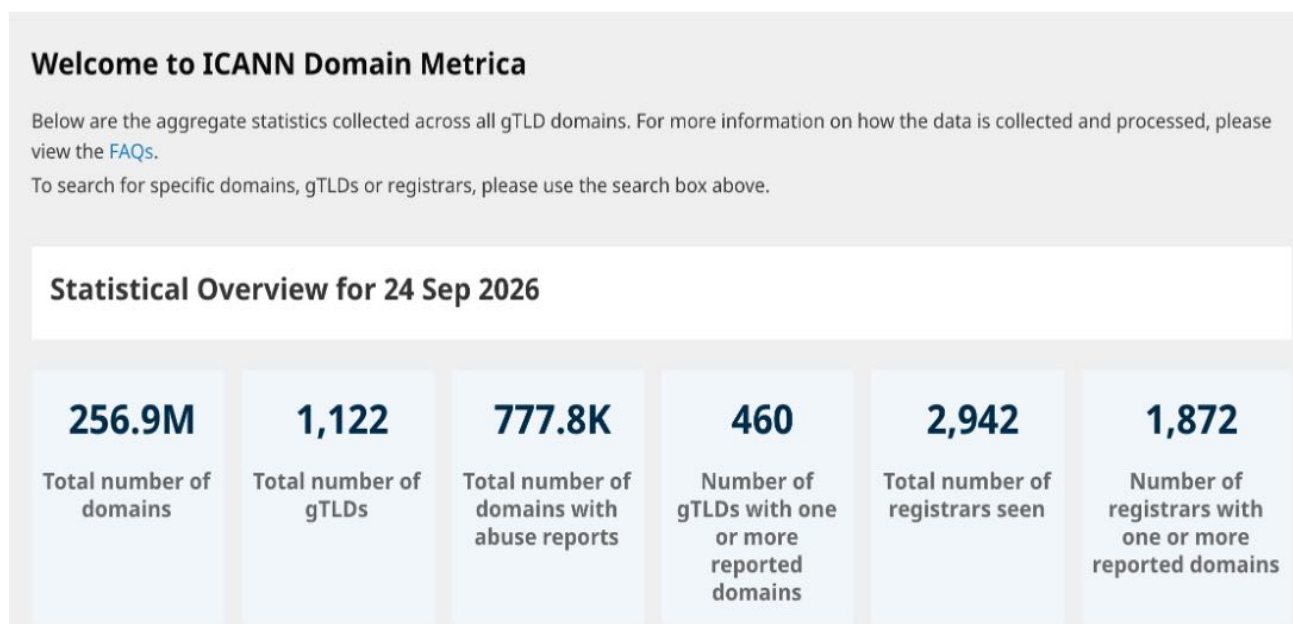
隨 2026 年 New gTLD 計畫持續推進，若多文字網域名稱及對應電子郵件地址無法在各類應用環境中被正確接受，新增之國際化字串在實務上將無法充分展現其價值；如何將 UA 從理念性倡議工作，轉為未來實際可用的基礎建設，仍有待後續觀察。對我國而言，公部門系統檢測與採購規範，以及未來若參與相關在地推動任務小組，均可參考指引所列具體建議。

[資料來源連結](#)

[指引](#)

ICANN Domain Metrics 新增 DNS 濫用緩解時間量測功能

ICANN Domain Metrics 係用於彙整網域名稱註冊趨勢及潛在 DNS 濫用相關資料的平台，可協助 ICANN 社群、研究人員及其他利害關係人觀察網域名稱生態系統的活動與長期趨勢。ICANN 於 2026 年 9 月 3 日宣布，於 ICANN Domain Metrics 新增網域正常運作時間 (uptime) 量測功能，以進一步觀察被列入信譽封鎖清單 (reputation blocklist) 的網域名稱，在被通報可能涉及網域名稱濫用後，其 DNS 持續正常解析及後續緩解所需的時間。



資料來源：ICANN Domain Metrics

本次更新的核心為「緩解所需時間」(Time to Mitigation, TTM) 指標，用以估算被通報網域自首次至最後一次成功 DNS 解析之間的時間，以觀察相關網域仍可透過 DNS 連線的期間。除 TTM 外，使用者亦可查看目前監測狀態、首次及最後一次成功 DNS 解析時間，以及可取得時的緩解結果。相關功能已整合至 Domain

Metrica 的 Domain Search，使用者可直接查詢個別被通報網域的監測資料。

ICANN 表示，本次更新是後續一系列 DNS 濫用緩解量測功能的第一階段。未來預計進一步擴充視覺化資訊、針對受理註冊機構及註冊管理機構的專屬檢視，以及應用程式介面 (API) 存取功能，使 DNS 濫用緩解時間更容易進行比較與分析。

[資料來源連結](#)

ICANN 公布 New gTLD 申請之保障措施評估服務商

ICANN 於 2026 年 8 月 20 日宣布，經 2025 年 12 月啟動之公開徵求建議書 (Request for Proposal, RFP) 程序，選定顧問與評估機構 Mirror Group LLC 擔任 2026 年 New gTLD 申請計畫「保障措施評估」 (Safeguard Assessment) 服務商。

保障措施評估屬於 New gTLD 字串評估 (String Evaluation) 階段之一環，其重點並非判斷申請人能否取得特定字串，而是確認申請字串是否因涉及消費者保護、敏感用途或受監管產業等風險類別，而須於「2026 年基礎註冊管理機構協議」 (2026 Base Registry Agreement) 中納入特定之保障性公共利益承諾 (specific safeguard public-interest commitments)，作為取得該 gTLD 後之額外契約義務。ICANN 表示，評估程序將著重公平性、一致性及客觀性，以適用於來自不同地區及背景之申請人。

[資料來源連結](#)

Project Jake：網域註冊資料揭露的新模式

文章出處：[CircleID](#)

原文作者：Klaus Stoll

WHOIS 自 1980 年代起使所有註冊資料公開可查，卻缺乏安全防護及一致的資料格式，濫用情形（垃圾郵件、詐欺）日增。2000 年代起要求資料保密之呼聲漸強，並因 2018 年歐盟 GDPR 上路而加速。未經同意而全面公開個資使資料持有人暴露於法律責任之下，完全封閉又損及執法等合法監督需求，因而使資料持有人陷入兩難的困局。

對既有資料持有人及當前 New gTLD 的申請人而言，妥善處理客戶資料隱私，將成為市場差異化之關鍵，也將促使註冊人提供真實資料而非虛假資訊。基於此，市場上需要一套符合特定條件之揭露機制，既能支援既有及未來政策、以分散式多方治理運作，使申請人明確知悉可取得資料範圍、使資料持有人得評估請求正當性而免除責任風險，並兼顧易用性、效率與經濟永續，同時與既有框架保持互通，且可漸進式導入、將干擾降至最低。

Project Jake 正為此應運而生，由 Edgemoor Research Institute (ERI) 所推動。旨在建立申請人 (Requestors) 與資料持有人 (Data Holders) 間自願性、群組對群組 (group-to-group) 之網域註冊資料揭露框架，透過四級敏感度量表，由資料持有人自行決定揭露範圍與條件，藉以化解註冊人隱私保護與執法機關、研究人員、企業等合法資料存取需求間之緊張關係。

行政框架與核心協議

Project Jake 架構建立在兩個相互關聯的要素之上，其一為定義利害關係人互動方式的行政框架（Administrative Framework），其二為由資料持有人定義在何種情況下願意釋出何種資料的協議（Agreement）。

行政框架區分申請人與資料持有人兩大陣營，雙方均得組成各自之群組（申請人群組 / 資料持有人群組），由對應之群組管理者代表成員治理群組、審核成員資格，並對外締結協議；資料持有人（即受理註冊機構、註冊管理機構等）則始終保留決定向何人、在何種條件下揭露何種資料之最終權限。

釋出資料的協議架構則採「分層設計」，以解決隱私與安全之間的衝突。該協議以「請求範本」的形式規定揭露條款，其中載明目的、身分驗證標準、允許之用途、最高敏感度層級以及其他參數。資料持有人依自身規則及所在司法管轄等因素，依「敏感度框架」將資料分為公開（Public）、私人（Private）、更私密（More Private）、受保護（Protected）四級，其分類標準完全由資料持有人決定，框架本身不作統一規範，同一群組內之不同資料持有人亦得有不同歸類。締約層級上，則分為連結雙方群組管理者之主協議，以及個別成員與所屬群組間之協議。透過此種「群組對群組」而非逐案協商之模式，可大幅提升具共同需求機構間之締約效率；而群組成員與群組之間的協議，則規範了各別群組內的個人成員身分，並使參與者受規則、安全義務及責任風險之約束。

Project Jake 的運作

Project Jake 提供「Jake 應用套件」，內含 Jaddar (供申請人查詢及送出請求)、Jareg (供資料持有人提供 RDAP 資料、執行揭露與 redaction)、Jadmin (供申請人群組管理)、Jaremin (供資料持有人群組與協議範本管理) 四項工具，已於 2026 年 6 月 ICANN 86 展示測試，並以開放原始碼透過 GitHub 提供下載。

THE JAKE APPLICATIONS SUITE
MANAGE • AUTHORIZE • PROTECT • DISCLOSE
Trusted access to Internet domain registration data

Tool	Icon	Function
Jaddar	Search icon	QUERY APPLICATION Search, look up data and submit requests
Jareg	Database icon	DATA HOLDER Provide RDAP data, policy and redaction, and request review
Jadmin	Users icon	REQUESTOR MANAGER Manage requestor groups, users and subscription requests
Jaremin	Group icon	GROUP ADMIN Manage data holder groups, agreement templates and subscription review

THE JAKE APPLICATIONS SUITE | Powering responsible data stewardship across the Internet.

資料來源：CircleID

實際運作上，資料持有人先建立客製化揭露協議範本，經申請人群組管理者比對需求後，由雙方管理者完成締約並啟用。申請人須加入相應之申請人群組取得會員憑證，始得依範本提出非公開資料請求，資料持有人核實申請人身分及授權層級、確認請求符合協議後決定揭露範圍（並保有揭露少於協議上限之裁量權）。全程以「群組對群組」協議取代逐案協商，藉此提升締約與請求處理效率。

Project Jake 已開發並目前正在測試該框架 (Framework) 與 Jaddar 套件 (Jaddar Suite) 的 Alpha 版本。現正邀請早期採用者測試該框架與協定 (Protocols)，其可透過託管服務或下載方式取得。Beta 版本將於 2026 年底或 2027 年初提供，以進行更廣泛的傳播與採用。值得注意的是，ERI 已與 TWNIC 簽署三年期合作協議，共同研發以 RDAP 為基礎、用於蒐集及揭露網域註冊資料之系統，目標於 2027 年第一季推出基礎可用系統；此一合作使我國成為觀察 Project Jake 揭露機制能否實際落地運作之場域之一。

觀察與結論

從實質內容而言，相較於目前 ICANN 以 SSAD 補充建議與註冊資料請求服務 (RDRS) 推進之集中式、共識導向路徑，Project Jake 代表由下而上、可先行試驗之自願性替代方案。在申請人身分驗證與分類機制上，兩者路徑截然不同，SSAD 係透過單一 (或搭配各國政府平行介面之混合式) 認證權威 (Accreditation Authority) 與中央閘道 (Central Gateway) 統一驗證申請人身分，且申請人僅粗分為自然人 / 法人與政府或政府間組織兩大類；Project Jake 則無任何中央權威，申請人之分類與資格審核完全交由資料持有人群組與申請人群組雙邊自行議定，理論上可依職業別 (如執法機關、資安研究人員、智財權利人等) 更細緻地劃分申請人群組。換言之，Project Jake 以分散式、可自訂之群組取代 SSAD 之集中式單一認證，兩者代表兩種不同之治理哲學，而非同一路徑之變體。不過，其四級敏感度架構雖有提供共通語彙，實際判準仍完全委由各資料持有人自行決定，未來究竟能形成統一共識，或變成多頭馬車，或仍待進一步發展與觀察。

DNS 濫用檢舉與下架之間的「通報落差」

文章出處：[CircleID](#)

原文作者：Garv Chauhan

一件釣魚網站的檢舉從送出到真正下架之間，多數延遲並非因無人處理，而是負責處置的體系本身積壓案件過多，提出檢舉最多的一群人卻對處理進度毫無可見度。作者 Garv Chauhan 引用反釣魚工作小組 (Anti-Phishing Working Group, APWG) 統計，2026 年第一季共記錄 971,181 起釣魚攻擊，較前一季 853,244 起成長 13.8%，此一長期上升趨勢，其增長速度已超出任何單一受理註冊機構濫用處理團隊所能實際跟上的範疇；此外，特定受理註冊機構在這些數據中出現的頻率也高得不成比例，而呈現一種集中化的現象。

數據觀察

就 ICANN 合規執法數據觀察，2024 年 4 月至 2026 年 4 月間，ICANN 合約遵循部門就 DNS 濫用防制要求開立約 530 件調查案，有四分之一調查案在結案時，濫用行為並未真正停止。此外，有超過 25,000 個濫用網域是透過 ICANN 直接調查而進行處理，並有數十萬個問題網域是在部分受理註冊機構於遭調查後，才另行採行系統性改善措施。這表示多數網域濫用的遏止，並非仰賴個別檢舉逐案處理，而是受理註冊機構遭查獲及承擔後果後，才改變其營運方式所致，執法對已被觸及之受理註冊機構具嚇阻效果，但對正在提出檢舉之個別受害人而言，則未必是快速回應機制。

檢舉機制

作者另以印度之釣魚網站檢舉為例，說明「落差」實際所在。個別網域濫用的檢舉會先進入該受理註冊機構自身之內部處理排序，處理的效率則取決於該受理註冊機構是否設有可正常運作之濫用聯絡窗口。依受理註冊機構認證協議（RAA）第 3.18 條，受理註冊機構須於首頁公開濫用聯絡方式，且檢舉表單不得要求登入始能提交。但實際上，使用者若找不到檢舉入口，網域濫用的處置將無法成案，更談不上成為統計數據。至於所謂「24 小時下架」政策，通常僅適用於執法機關以自身證據直接聯繫受理註冊機構之情形；對一般使用者來說，則視受理註冊機構之配合程度、檢舉文件完整度而定，配合度低的受理註冊機構，甚至可能拖延數週才處理。

作者提及 ICANN 合規團隊觀察到檢舉量雖持續逐月成長，但其中惟具備充分事證可受理之檢舉比例則偏低。這並非執法失靈，而是檢舉流程過於複雜，一般使用者難以提出受理註冊機構或 ICANN 所期待的證據，如截圖、時間戳記、郵件標頭紀錄。

觀察與結論

文章結論指出，現有執法體系並非無效，對其所觸及之網域確有成效；問題在於，當濫用行為發生時，相關檢舉資訊往往未能及時透過檢舉機制，讓具處置權限者獲得足以採取行動之依據。真正之課責落差不在於檢舉通過門檻之後如何處理，而是有更多的檢舉根本未能通過門檻，因此使檢舉更容易有效提出與改善回應速度，比單純強化執法機制本身更為關鍵。