出國報告（出國類別：會議）

出席「網際網路名稱與號碼指配機構」（ICANN）第 79 次會議報告書

服務機關	姓名 / 職稱
數位發展部	曾文方 副司長、陳坤中 高級分析師、姜政男 科長、王文哲 技士
外交部	謝捷帆 薦任科員
內政部警政署刑事警察局	胡正憲 警務正、李榮哲 偵查員
國家資通安全研究院	張元傑 工程師 （線上參加）
數位發展部資通安全署	楊素卿 科長
財團法人台灣網路資訊中心	黃勝雄 董事長、余若凡 執行長、丁綺萍 副執行長、吳國維 國際事務委員會委員、江進容 組長、李曉陽 組長、湯序平 管理師
財團法人中華民國國家資訊基本建設產業發展協進會	梁理旋 副執行長、陳曼茹 經理
網中智庫股份有限公司	賴俞帆 專案經理、孟紅福 研究員、趙郁婷 研究員

派赴國家：波多黎各 聖胡安

會議期間：113 年 3 月 2 日至 3 月 7 日

報告日期：113 年 4 月 16 日

摘 要

一、 第 79 次網際網路名稱與號碼指配機構（ICANN）會議於今（2024）年 3 月 2 日至 7 日以結合線上參與與實體會議的混合模式舉行。

二、 本次 ICANN 大會為社群論壇（Community Forum），議程共 6 天，除了大會議程、公眾論壇，亦包含 ICANN 內部各利害關係團體會議、政策制定（PDP）工作小組會議，以及由技術社群主辦的域名技術研討會等。大會議程討論 New gTLD 註冊管理機構合約中的公眾利益承諾（Public Interest Commitment，PIC）與註冊管理機構自願承諾（Registry Voluntary Commitment，RVC）。

三、 本次會議仍奉前行政院資通安全處指示擴大各部會參與 ICANN 事務，依照前行政院資通安全處指示各參團單位分工合作，分別參加政府諮詢委員會（GAC）、網路安全及穩定諮詢委員會（SSAC）、根伺服器系統諮詢委員會（RSSAC）相關會議，並參與 IP、DN 技術研討會。

四、 其中，GAC 議程包括公共安全小組報告、對董事會提出建議、DNS 濫用討論及 New gTLD 申請政策等議題。會議結束後，GAC 提出 ICANN79 公報。

目次

壹、目的

第 79 次網際網路名稱與號碼指配機構（Internet Corporation for Assigned Names and Numbers，ICANN）會議於本（2024）年 3 月 2 日至 7 日以結合線上參與及實體會議的混合模式舉行。

本次 ICANN 大會為社群論壇（Community Forum），議程共 6 天，議程安排除了大會議程、公眾論壇，亦包含 ICANN 內部各利害關係團體會議、政策制定（PDP）工作小組會議，以及由技術社群主辦的域名技術研討會等。大會議程討論 New gTLD 註冊管理機構合約中的公眾利益承諾（Public Interest Commitment，PIC）與註冊管理機構自願承諾（Registry Voluntary Commitment，RVC）。

我國政府代表由數位發展部主政，並會同外交部、國家資通安全研究院、資通安全署、刑事警察局等單位共 9 人與會，另有財團法人台灣網路資訊中心、財團法人中華民國國家資訊基本建設產業發展協進會及網中智庫股份有限公司 12 人共同組團與會。政府代表主要參與政府諮詢委員會（Governmental Advisory Committee，GAC）會議，亦依照業管屬性參與網路安全及穩定諮詢委員會（Security and Stability Advisory Committee，SSAC）、根伺服器諮詢委員會（Root Server System Advisory Committee，RSSAC）等相關會議，以及各項 IP、DN 技術研討會。本次 ICANN 會議全部議程詳見附件 1，亦可由下述網址獲得：https://icann79.sched.com/。

其中 GAC 會議於 2024 年 3 月 2 日至 7 日召開，計有美國、英國、澳洲、日本、埃及、巴拉圭、千里達及托巴哥等 71 個 GAC 成員及 9 個觀察員參與會議。

GAC 議程包括公共安全小組報告、對董事會提出建議、DNS 濫用討論及 New gTLD 申請政策等議題。會議結束後，GAC 提出 ICANN79 公報。

ICANN80 政策論壇將於盧安達吉佳利舉行，會議時間為 2024 年 6 月 10 日至 13 日。

本報告將介紹 ICANN 組織最新現況，並說明本次參與 ICANN 年度大會各項議程、GAC、GNSO、SSAC、RSSAC 等重要議題及內容，最後就會議內容研提相關建議。

貳、ICANN 簡介

ICANN 是全球性、非營利、共識導向的國際組織（International corporation），1998 年 10 月成立於美國加州，負責監督管理網際網路技術管理功能（Internet technical management functions）、通訊協定參數及通訊埠（Protocol Parameters and Port）之協調、域名系統（Domain Name System，DNS）之管理、IP[1]位址之分配暨指派，以及根伺服器系統（Root server system，RSS）之管理。

ICANN 強調由全球多方利害關係人（multistakeholder）參與（包括政府部門、私人企業、技術社群、個人使用者等）、以由下而上的共識機制為基礎，制定全球域名管理政策，以促進市場競爭機制，維護全球網際網路運作之穩定、可靠、多元及安全為主要使命。

一、 ICANN 組織架構

ICANN 下設有董事會（Board of Directors），基於網際網路由下而上的組織特性，為確保各界聲音與意見都能在網路社群會議中出現，董事會以多方利害關係團體共同組成。成員分別來自以下屬性團體：

1. 支援組織（Supporting Organization，SO）。
2. 諮詢委員會（Advisory Committee，AC）。
3. 網際網路工程任務小組（Internet Engineering Task Force，IETF）。
4. ICANN 組織職員（CEO/Staff）。
5. 提名委員會（Nominating Committee）遴選。

---

[1] 網際網路通信協定（Internet Protocol）容許電腦網路間透過實體鏈路（physical links）快速互相通信。IP 位址以數字表示，網際網路上電腦間的資訊傳輸及連結即藉 IP 位址達成，一般大眾係借用 DNS 以人性化名稱（human-friendly names）來辨識主機位址。

ICANN 多方利害關係人參與架構，可藉由 ICANN 董事會組成理解（如下圖 1）：

圖 1 ICANN 多方利害關係人參與架構圖

ICANN 大會每年召開三次，會議採取開放的參與模式，凡對網路治理有興趣之個人、團體皆可參加，並不侷限於 ICANN 會員。自 2016 年開始，會議模式調整為 A、B、C 三種類型：A 會議為年度第一次會議，會議型態與以往大會相同，但新增跨社群（Cross Community，CC）論壇；B 會議為年度第二次會議，亦稱為政策論壇（Policy Forum），會議主要任務在於 ICANN 內部各工作組織之溝通，以落實政策並促進討論；C 會議為年度第三次會議，會議除各支援組織及諮詢委員會既有議程外，亦增加熱門主題（High Interest Topics，HIT）論壇，以期吸引更多對域名相關議題有興趣的人士參與。與會人士可根據屬性團體性質，參加各利害關係團體討論，或選定感興趣之議題參與討論。

二、 ICANN 組成單位之功能

(一) ICANN 董事會

ICANN 於 2016 年 5 月 27 日通過新組織章程細則（Bylaw）。IANA 功能代管權正式轉移後，該組織章程於 2016 年 10 月 1 日正式生效。依據前揭組織章程，ICANN 董事會係由 16 位具投票權之董事組成，其中 8 位董事由提名委員會選出，位址支援組織（Address Supporting Organization，ASO）、通用名稱支援組織（Generic Names Supporting Organization，GNSO）、國碼名稱支援組織（Country Code Names Supporting Organization，ccNSO）各推舉 2 位，一般使用者諮詢委員會（At-Large Advisory Committee，ALAC）推舉 1 位，ICANN 組織執行長則為當然董事。

依慣例，董事之任期為 3 年，每年改選部分董事，故所有董事之任期交錯，隨時都有新舊董事參與會議討論及投票。

此外，4 位不具投票權之聯絡人則分別由根伺服器系統諮詢委員會（RSSAC）、網路安全及穩定諮詢委員會（SSAC）、網際網路工程任務小組（Internet Eegineering Task Force，IETF）及政府諮詢委員會（GAC）指派。

依據 ICANN 章程，董事會成員有 20 位：

1. **Tripti Sinha**，董事會主席（October 2018 – Annual General Meeting 2024）
2. **Danko Jevtovic**，董事會副主席（October 2018 – Annual General Meeting 2024）
3. **Maarten Botterman**，NomCom（November 2016 – Annual General Meeting 2025）
4. **Sarah Deutsch**，NomCom（November 2017 – Annual General Meeting 2026）
5. **Edmon Chung**，NomCom（October 2021 – Annual General Meeting 2024）
6. **Chris Chapman**，NomCom（September 2022 – Annual General Meeting 2025）

7. **Sajid Rahman**，NomCom（September 2022 – Annual General Meeting 2025）
8. **Catherine Adeya**，NomCom（October 2023 – Annual General Meeting 2026）
9. **Becky Burr**，GNSO（November 2016 – Annual General Meeting 2025）
10. **Chris Buckridge**，GNSO（October 2023 – Annual General Meeting 2026）
11. **Alan Barrett**，ASO（October 2021 – Annual General Meeting 2024）
12. **Christian Kaufmann**，ASO（September 2022 – Annual General Meeting 2025）
13. **Patricio Poblete**，ccNSO（October 2020 – Annual General Meeting 2026）
14. **Katrina Sataki**，ccNSO（October 2021 – Annual General Meeting 2024）
15. **Léon Felipe Sanchez Ambia**，ALAC（November 2017 – Annual General Meeting 2026）
16. **Harald Alvestrand**，IETF 聯絡人（Since 2018）
17. **Sally Costerton**，代理主席暨執行長（Since 2023）
18. **James Galvin**，SSAC 聯絡人（Since 2021）
19. **Wes Hardaker**，RSSAC 聯絡人（Since 2022）
20. **Nico Caballero**，GAC 聯絡人（Since 2023）

(二) ICANN 支援組織

目前 ICANN 下設有 3 個支援組織（SO），分別為 ASO、ccNSO、GNSO，各 SO 均有特定功能，為 ICANN 在各專責領域之主要政策建議來源及諮詢單位。簡介如下：

1. 位址支援組織（ASO）

ASO 負責向 ICANN 提出有關 IP 位址運作、指配及管理之政策性建言，其著重於識別單一 Internet 上各種電腦之 IP 位址系統，如 210.69.99.253；ASO 係 ICANN 與各區域網際網路註冊管理機構(Regional

Internet Registries，RIR）洽簽之 MoU 所設立之組織。目前按區域所設立之 RIR，分別有負責北美洲區域之 ARIN、歐洲區域之 RIPE NCC、拉丁美洲區域之 LACNIC、亞洲區域之 APNIC 及非洲區域之 AFRINIC。一般 RIR 的基本位址分配政策係依區域需要，並視未來一年內位址可能需求情形，來分配位址區塊（Address Block）。

2. 國碼名稱支援組織（ccNSO）

ccNSO 負責向 ICANN 提出有關 ccTLD（如：.us、.it、.tw、.jp 等）與 IDN ccTLD（如：「.台灣」、「.pф」（Russia））之政策性建言，ccNSO 係由 ccTLD 營運方組成，下設理事會（Council）管理相關政策制定流程，於羅馬會議期間（2004 年 3 月 1 日）正式成立。

3. 通用名稱支援組織（GNSO）

GNSO 負責向 ICANN 提出有關通用頂級域名之政策性建言，係由 gTLD 登記註冊管理機構、受理註冊機構、智慧財產權團體、商業團體、網路服務供應商團體、非營利組織團體及非營利使用者團體所組成，下設理事會（Council）管理相關政策制定程序。

(三) ICANN 諮詢委員會

諮詢委員會（AC）為正式諮詢團體，由來自網際網路社群（Community）的代表組成，各種不同社群的人員會依其利害團體性質參與相關諮詢委員會，並在委員會討論後，向 ICANN 提出政策建言。

ICANN 依組織章程設立不同諮詢委員會，諮詢委員會不代表 ICANN 行使職權，惟向 ICANN 董事會提出其研究報告及建言。

目前 ICANN 董事會設有 4 個諮詢委員會，簡介如下：

1. 政府諮詢委員會 （GAC）

GAC 由國家級政府（National Governments）、國際論壇承認之經濟體（Distinct Economies as recognized by International Fora）、多國政府組織（Multinational Governmental Organizations）及條約組織（Treaty Organizations）以會員代表或觀察員身分所組成，功能為向董事會表達政府與公眾事務單位之關切事項。

GAC 以會議方式討論政府之權益及關切議題，包含消費者權益、網際網路之運作對各國影響、各國政府或國際組織所關切之議題；GAC 不代表 ICANN 行使職權，惟向 ICANN 董事會提出其研究報告及建言。依據 ICANN 組織章程規定，董事會做決策時必須參考 GAC 建議。

2. 網路安全及穩定諮詢委員會（SSAC）

SSAC 負責就網域名稱及位址指配系統之安全及完整性向 ICANN 董事會提出建言，包括安全架構之擬定、與網際網路技術社群及重要 DNS 管理者/業者之溝通協調、風險分析評估、各項頂級域名之使用可能產生的系統問題等。

3. 根伺服器諮詢委員會（RSSAC）

RSSAC 負責向 ICANN 董事會提出有關網域名稱根伺服器運作之建言，包含主機硬體容量、作業系統、名稱伺服器軟體版本、網路連結、硬體環境、安全問題及系統效率、可靠度等。

4. 一般使用者諮詢委員會（ALAC）

ALAC 代表網際網路個人使用者向 ICANN 提出建言，其組成成員係來自網際網路之使用社群中，關切 ICANN 運作之人士。

參、過程

一、會議過程：時間、地點、行程與議程

(一)時間：2024 年 3 月 2 日至 7 日

(二)地點：波多黎各聖胡安

(三) 行程：

日期	行程
3 月 2 日	【GAC】起始會議 【GNSO】國際化域名 EPDP 工作會議 【GAC】高階政府會議籌備會議 註冊資料政策實施：過渡期準備
3 月 3 日	【GAC】與 ALAC 聯合會議 【RSSAC】聯合會議：RSSAC 與 SSAC 【SSAC】聯合會議：ALAC 與 SSAC 【GAC】New gTLD 未來回合討論（2 場） 【GAC】戰略規劃討論 【GNSO】CPH DNS 濫用：社群推廣
3 月 4 日	【ccNSO】Tech Day（4 場） 【GAC】與 CPH 聯合會議 【GAC】DNS 濫用討論
3 月 5 日	【GAC】聆聽社群意見 【RSSAC】聯合會議：ICANN 董事會與 RSSAC 【GAC】WHOIS 與資料保護政策及準確性 【GAC】與董事會聯合會議

日期	行程
	New gTLD 未來回合：字串相似性審核規劃 【RSSAC】RSSAC 會議
3 月 6 日	【GAC】與 GNSO 聯合會議 【SSAC】聯合會議：ICANN 董事會與 SSAC 【GNSO】SubPro 補充建議：社群諮詢 【SSAC】公開會議 【GAC】公報撰寫（3 場） 【ccNSO】DNSSEC 與安全工作坊（3 場）
3 月 7 日	【GAC】公報撰寫（2 場） 【GAC】總結會議

會議議程：GAC 議程如附件 2，GAC 公報如附件 3。

二、GAC 會議相關議程

(一)行政會議

1. 高階政府會議籌備會議

高階政府會議（High Level Government Meeting, HLGM）旨在提升高階政府長官對 ICANN 職能及其於網路治理議題上角色的認識。ICANN 訂本（2024）年 6 月 9 日至 13 日在盧安達舉行第 80 次會議，並於第一天舉辦疫後首次高階政府會議（HLGM），邀請 GAC 會員專業部會首長等出席討論重要網路政策議題。

本籌備會議中 GAC 秘書處與盧安達 GAC 代表共同宣布盧方已依據「國際電信聯盟」（International Telecommunication Union, ITU）會員名單寄發邀請函。葡萄牙認為 HLGM 與 ITU 相關不大，對其合作的合理性提出疑問。GAC 主席回應，ICANN 及 ITU 間有持續合作及互邀參與相關會議和活動，此次邀請也為彰顯雙方交流。ICANN 政府及國際政府組織（International Governmental Organization，IGO）參與資深主任 Laurent Ferrali 亦回應，本次 HLGM 亦有邀請其他國際組織，例如 GAC 觀察員世界智慧財產權組織（World Intellectual Property Organization，WIPO）、聯合國教科文化組織（United Nations Educational, Scientific, and Cultural Organization，UNESCO）等其餘逾二十多個國際組織。

2. 戰略規劃討論

GAC 首次制訂 4 年期戰略目標及工作計畫，以決定 GAC 關切議題之優先順序，並強化對 ICANN 組織決策之參與度及影響力，預計於 ICANN 第 80 次會議中定稿。

(1) GAC 策略計畫制定方式

GAC 將策略計畫分成 3 個不同時間層面：

- 長期：策略目標（Strategic Objectives）
- 中期：預期產出/成果（Expected Outcomes）
- 短期：作為項目（Action Items）

(2) GAC 策略計畫制定之時程規劃請參考圖 2。

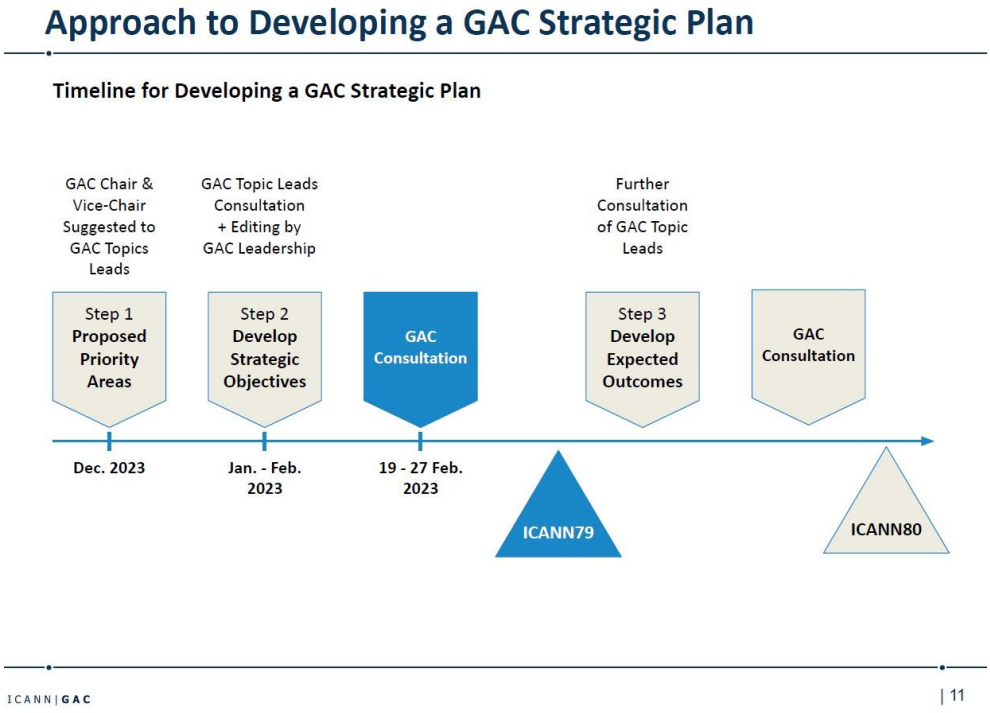

圖 2 GAC 策略計畫制定之時程

(3) 預期本策略計畫將

- 提升 GAC 積極參與 ICANN 討論之立場；
- 提升 GAC 提供即時、有效建議與政策意見；
- 協助與政府高層級 ICANN 利益相關方就 GAC 重要事項進行討

論溝通。

(4) GAC 策略目標提案

目標領域	概述
政府在 ICANN 中之作用	重申政府在 ICANN 多方利益共同體模型中之關鍵作用，並確保政府能透過現行與未來的 ICANN 流程與程序，有效地追求公共政策利益。 尤其是，GAC 將努力評估目前的 ICANN 結構，是否為諮詢委員會（包含 GAC）提供了充分且有意義的機會，來制定、影響與修改政策結果。
GAC 的效力	尋求增加政府參與審議工作，並提高其做為 ICANN 多方利益共同體流程參與者之有效性，以確保政府的聲音得到表達、適當代表並在政策與策略成果中獲得適當考慮。
未來幾輪次之 New gTLD	透過前幾輪次新通用頂級域名（New Generic Top-Level Domain，New gTLD）之經驗（包含成本與效益），努力確保未來幾輪次之 New gTLD： ・ 促進競爭、消費者信任與消費者選擇； ・ 為數位落差做出貢獻，特別是對服務匱乏與代表性不足地區申請人之協助，以及國際化網域名稱之推廣； ・ 納入適當的安全性、穩定性與韌性保障措施； ・ 為 GAC 提供適當之程序與能力，以解決特定或某類申請案引起之意外問題，特別是影響全球公共利益（如地理名稱）之問題。
DNS 濫用	因為涉及政府對 DNS 濫用之疑慮，積極參與 ICANN 社群工作，並針對 ICANN 活動提出建議，以便：

目標領域	概述
	・ 提升 DNS 之安全性、穩定性與韌性； ・ 減少 New gTLD 中 DNS 濫用的發生率與危害； ・ 支持 ICANN 持續改進 DNS 濫用防治與預防標準，並有效執行； ・ 檢視並確定預防與防治 DNS 濫用的最佳實踐，供更廣泛採用。 在此工作中，考慮到 DNS 濫用具有不斷變化之特性，GAC 將向 GAC 成員與觀察員進行調查，更好地了解如何解決該問題，並滿足政府之期望。
網域註冊資料	預計根據所適用之隱私監管框架，與涉及 WHOIS 服務之 GAC 原則，努力確定並推薦作法，以促進並支援網域名稱註冊資料之可持續存取，並提高正確性。 建於 WHOIS 資料之不斷發展，GAC 將與 ICANN 社群合作，確保註冊資料反映並解決目前網域產業之複雜性。此包含確保滿足向受理註冊機構提出之註冊資料合法請求，並能存取有意義之資料。該些資料應清楚闡明參與網域名稱註冊之每個實體所扮演之角色，包含註冊資料之權威來源、網域之最終使用者（如受益之使用者），以避免與其他實體混淆，如隱私與代理服務、經銷商。
普遍適用性	與各國政府及所有利益相關方合作，促進多語系的網際網路發展，並透過確保所有網域名稱（包含新頂級網域、國際化網域名稱與電子郵件位址）得到所有支援網際網路的應用程式、裝置與系統，平等對待並可供他人使用，從而提供普遍性的存取。

目標領域	概述
新興科技對網路獨特識別碼之影響	加深對網際網路獨特識別碼相關新技術挑戰、機會之理解與認識。為此，預計運用 ICANN 社群、政府及其他領域之專業知識，分享資訊並評估潛在影響，以造福 GAC 成員與所有利益相關方。
網路治理	努力確保所有參與者定期了解影響網路獨特識別碼的網路治理生態系統發展。GAC 得協調成員間之努力，為全球網路治理流程做出貢獻，以利支援多方利益共同體模型。

3. 社群意見募集

GAC 社群 Open Mic 工作會議以開放討論形式，聽取 ICANN 各方社群成員提出的建議或問題。GAC 將所有重點記錄下來，並在 ICANN 79 其他會議場次中或未來 ICANN 會議回覆這些問題。

(1) GAC 請求完全保密取得註冊資料

- 非企業利害關係團體（Non-commercial Stakeholder Group ，NCSG）呼籲 GAC 在完全保密的情況下取得註冊人敏感個人資料時，得透過正當程序以及公開透明的方式，以避免造成濫用註冊資料系統、侵犯個人權益的可能性，敦促 GAC 討論尋求解決措施。
- 歐洲高峰會數位發展暨治理部長 Patrick Penninckx 表示也十分關注這項議題。
- 瑞士 GAC 代表回應 GAC 曾經設立人權與國際法工作小組，建議相關事宜未來可以持續討論。

(2) GAC 提名委員會（NomCom）代表

埃及 GAC 提議討論 GAC 是否要派代表參與提名委員會（Nominating Committee，NomCom），以及委派的利益與否。美國 GAC 代表則感謝埃及提出的建議，美國對這件事沒有意見。

(3) 締約方議院聯繫小組

美國 GAC 代表表示 GAC 在規管締約方的協議上具有一定分量，建議可能要討論是否要成立締約方議院聯繫小組。伊朗 GAC 代表表示得留意在討論與締約方議院相關的議題時，會有法律上的問題，因此聯繫小組的必要性、成立時機、工作制定、時程表、義務責任，都必須加以討論。

(4) IPv4 和 IPv6

台灣網路資訊中心（National Network Information Center，TWNIC）國際事務委員會吳委員國維建議 GAC 可以改進相關資訊的交流傳達，並提出透過手機網路改善 IPv6 的個人見解。巴布亞紐幾內亞 GAC 則建議 ICANN 應該持續分享討論區域網際網路註冊管理機構（RIR）相關資訊。

(5) 其他討論

GAC 主席及多國 GAC 代表分享 2024 年即將召開之國際會議資訊，如瑞士與國際電信聯盟（International Telecommunication Union，ITU）共同協助舉辦的 WSIS+20 會議、全球 IGF 論壇將於沙烏地阿拉伯舉行等，我國也分享亞太區域網路治理論壇 2024（Asia Pacific Regional Internet Governance Forum，APrIGF 2024）將於 8 月在臺北舉行。

哥倫比亞與瑞士 GAC 代表建議 GAC 可以建立共同行事曆，或是透過日內瓦網路平臺所建立的公共開放行事曆，讓大家分享上述的會議資訊。

網中智庫（隸屬網路中文受理註冊機構）Hong-Fu Meng 提問 GAC 對於

是否有了 CSAM（Child Sexual Abuse Material）這項議題，或是與其他相關組織合作協助通報，保護下一個世代的安全？英國 GAC 代表對此回應表示未來 GAC 會盡力解決 CSAM 並給予回覆。

(二) 跨社群組織及跨社群工作小組會議

1. 與 ICANN 董事會會議

(1) GNSO 利益聲明（Statement of interest，SOI）

有鑑於近期 GAC 向 ICANN 董事會反映，GNSO 運作原則中允許參與者不揭露其在 ICANN 所代表之資訊一事，GAC 請 ICANN 董事會思考有何方式可使所有 ICANN 社群群體，包含 GNSO，應要求在政策制定及運作活動揭露該資訊。

ICANN 董事會主席認為，此事至關重要並鼓勵所有 ICANN 社群向公開透明的方向前進。

(2) 緊急註冊揭露請求

GAC 樂見 ICANN 董事會對於預期的後續步驟提出意見，以利基於新共識政策對緊急註冊資料揭露請求回應時間達成共識。

ICANN 董事會與 GAC 立場一致，認為此時程不符合申請目的之需求。ICANN 董事會記得於董事會 GAC 互動小組（Board GAC InteractionGroup，BGIG）會議中 GAC 所陳述之執法單位認證問題，ICANN 董事會預期與 GNSO 據此進行討論。

(3) New gTLD 未來回合討論

針對我方關注之新通用頂級域名（New gTLD）開放議題，部分會員提問倘有未獲保留之字詞或申請對於國家或政府而言有文化敏感度的頂級域名（Top-Level Domain，TLD）名稱之情況應如何

處理。ICANN 回覆，倘有未獲保留之字詞，各會員仍可透過提出異議等方式表達意見，惟 ICANN 強調不涉入任何政治爭議。另外，若相關字詞已寫入根域，則難以事後移除。

(4) 申請人支援計畫（ASP）

ICANN 董事會將如何確保申請人支援計畫（Applicant Support Program，ASP）有充裕資金與資源，使其具全球包容性與代表性，確保資源匱乏地區在 ASP 計畫中之優先性、重要性。

- ICANN 組織正在全面性進行規劃，使其有充足資源以提供費用減免及其他協助。
- ASP 中並未對特定區域排有優先性，ICANN 將盡力確保申請人多元化。

(5) New gTLD 未來回合之效益分析

經 GAC 成員審查由 ICANN 製作的有關 New gTLD 未來回合計劃成本和效益的分析概述，GAC 注意到該概述內容似乎未能滿足 GAC 對新一輪的 New gTLD 計劃成本和效益進行客觀和獨立分析的要求。在 GAC 看來，這樣的分析應該包含試圖從全球視角量化所有重大優點和缺點。

按照目前呈現的情況，《概述報告》[2]似乎是對個別問題的評估（例如，競爭和消費者選擇問題的評估）以及一些關於 DNS 濫用的考慮。似乎並未尋求優點與缺點的量化。此外，目前所有文件的輸入都是由 ICANN 利益相關者或 ICANN 組織準備，這些利益相關者或 ICANN 組織本身，無論如何都與先前的 gTLD 輪次或下一輪 gTLD 有關，因此不能被視為客觀或獨立。

[2] https://www.icann.org/en/system/files/files/overview-cost-benefit-analyses-next-round-22jan24-en.pdf

2. 與 GNSO 會議

(1) New gTLD 未來回合

- Small Team Plus 進展更新：ICANN 社群皆同意應禁止同時授權相同拼法之單／複數字詞申請案，以避免混淆情形發生，惟 ICANN 董事會未同意採納 GNSO 提交之建議。
- 拉丁字元附加符號：ICANN 工作人員已針對此議題進行討論，預計四月份會產出相關決議及具體提案。

(2) 可預測性常設委員會（SPIRT）

可預測性常設委員會（Standing Predictability Implementation Review Team，SPIRT）之章程制定小組持續徵求志願者加入，下一場小組會議將於 2024 年 3 月 18 日舉行，該小組工作時程預計為 3 個月，每一至兩週召開一次會議。

(3) GNSO 利益聲明（Statement of Interest，SOI）

GAC 主席已將透明度議題之信件寄交 ICANN 董事會主席；GNSO 回應，該社群內部尚未就該議題達成共識，後續可能將社群內部各方意見提供參考。

(4) DNS 濫用防治

- 註冊管理機構協議（Registry Agreement，RA）及驗證受理註冊機構協議（Registrar Accreditation Agreement，RAA）契約修訂已由 ICANN 董事會批准，並將於 2024 年 4 月 5 日起生效。
- GNSO 社群預計待契約修訂施行狀況，並蒐集來自 ICANN 履約部分、第三方單位等資訊，以決定後續相關政策制定之範圍及內容。

- GNSO 內部 DNS 濫用小組目前亦等待契約修訂的施行狀況以繼續小組工作。

(5) 註冊資料正確性範圍界定小組（Registration Data Accuracy Scoping Team）

- 該小組工作目前暫停至今（2024）年 8 月，尚待資料處理相關協議之進展，如 ICANN 與締約方之協商提前完成，則該小組工作也將隨之重啟。
- ICANN 已進行相關評估，討論哪類註冊人資料得被用以評估資料正確性，惟該評估認為，ICANN 並無收集相關資料以衡量資料正確性之法律依據。

(6) 其他事項

- 註冊資料緊急請求：該議題目前已進到 ICANN 董事會進行討論，目前尚未得知下一步進展。
- 域名系統安全擴充（Domain Name System Security Extensions，DNSSEC）：關於 DNSSEC 是否能普及至所有網域名稱，GNSO 回應表示目前沒有相關政策正在進行中，惟《RAA》中有條款說明受理註冊機構必須提供 DNSSEC，且 GNSO 政策僅管理受理註冊機構及驗證受理註冊機構，無法擴及至 ISP 業者、經銷商等，故目前無規劃相關政策。
- 隱私代理服務（Privacy Proxy Service）：ICANN 近期通知 GNSO 可開始隱私代理服務之後續相關工作。

3. 與 ALAC 會議

ALAC 報告下一輪次《申請人支援指南》[3]的修訂內容，以及申請人協助相關措施，包含降低申請費用、提供無償協助服務(Pro-bono)、募資計畫等。

「申請人支援計畫（ASP)」旨在透過提供資金性和非資金性的協助來發展 New gTLD，鼓勵全球多元性、市場的公平競爭和強化 DNS 的使用。伊朗評論募資計畫的資金（美金兩百萬元）不足以支援 ASP。

印尼詢問如何保護宗教文化相關的字詞（例如：Islam 伊斯蘭、Halal 清真），ALAC 回應得透過申請人建議、GAC 建議、GAC 預警來保護相關字詞。

加勒比海電信聯盟(Caribbean Telecommunications Union, CTU ）指出得思考 New gTLD 未來回合計劃針對的群體對象為何，以及募資計畫實際上應準備多少的預算。

巴西重視如何確保非資金性協助的成效，ALAC 回應申請人計畫將依照 GNSO 和 ICANN 董事會的決議來判斷，如有相關建議請在施行審查小組階段提出。

(三) 公共政策及重要議題

1. WHOIS/RDRS

(1)註冊資料請求服務及對隱私／代理人服務之衝擊

企業 Verizon 代表 Patrick Flaherty 分享企業用戶使用「註冊資

[3] https://community.icann.org/display/SPIR/ASP+%7C+Applicant+Support+Program?preview=/273448978/302350567/240212_DRAFT%20ASP%20Handbook.pdf

料請求系統（Registration Data Request Service，RDRS）」系統及資料揭露審核的觀察結果，並指出資料揭露的同意標準似無統一規則可循。其舉 Verizon 針對「包含有完整 Verizon 名稱在內」及「自 Verizon 名稱衍生之錯漏字」的侵權域名提出註冊資料請求申請為例，48 件申請件裡只有 12 件獲得資料揭露同意（Approved），2 件為部分同意（Partially Approved），且部分拒絕揭露理由不甚明確（如依適用法律規定不得提供），其他拒絕揭露（Denied）之理由提供的資訊也相當有限（如回覆建議應改正申請理由，卻未再敘明）。Patrick Flaherty 另分享由其他代理商以同樣的侵權域名提出資料揭露申請，從不同受理註冊機構所獲得的審核結果卻不盡相同，再次印證了資料揭露審核標準的不一致。

Patrick Flaherty 在會議現場也透過模板（template）示範遞件流程，並表示遞件模板的建置有助於提交大量請求。其建議與會者也撥冗操作 RDRS 系統，並將使用意見提供 ICANN 參考。

公共安全工作小組代表 Gabriel Andrews 則希望能藉由本次簡報，提升全球公共安全機構與執法機關對 RDRS 的認知與實際使用，並提供建設性之回饋。其認為，最有效也最快速提升公眾對 RDRS 覺察之方式，就是在 WHOIS 系統裡提供 RDRS 的連結，讓偵查者或資料請求者能快速被轉介至資料請求管道，希望這項建議能再獲重視。Gabriel Andrews 也分享其他幾項來自於執法機關的反饋，例如：

- RDRS 系統無法針對隱私／代理人服務的域名資料提出申請，讓 RDRS 所標榜的「一站式」概念出現美中不足之憾；
- 建議將 ccTLD 納入 RDRS 的服務範圍，並透過此平臺將資料請求導向相關受理註冊機構進行揭露決策；

- 建議在 RDRS 的域名搜尋列的輸入字串形式能擴及「子網域」（subdomain），因為在某些情況下，子網域的顯示有助於受理註冊機構識別終端使用者；
- 執法機關期待，經 RDRS 接獲資料請求的受理註冊機構，能先聯繫執法機關釐清狀況，再接續 RDRS 的資料揭露流程。但目前普遍聽聞之實踐方式大多在 RDRS 以外進行，所以將建議 ICANN 是否能建立更細緻之分類，以符合執法機關的業務特性。
- 部分問題內容可能對申請人造成誤會，進而影響請求之遞交：例如被描述為遞件申請必須要件之傳票、法院判決等，事實上並非必要。

Gabriel Andrews 最後依據 ICANN 2024 年 2 月公布的 RDRS 使用情形的量測數據，說明其觀察到的資料請求類別之分布情形，以及審核結果與申請件性質之間關係，作為 RDRS 未來改進方向。

註冊管理機構團體代表由 Sarah Wyld 進行經驗分享，除了部分 RDRS 功能（例如「Pending requestor input」無法實際反映註冊管理機構的處理狀況，建議能建立更加細緻之分類）、使用者介面（讓註冊管理機構能進行更快速的轉介處置）、以及與資料請求者所提供資訊（RDRS 無針對資料請求者進行身份驗證、請求類別選擇有誤、速件標示之合理性）有關之問題外，其表示整體感受十分正面，也認為 RDRS 值得受理註冊機構投入。但 Sarah Wyld 最終仍不忘強調人工審核的重要性，以合理權衡資料請求方與資料主體兩邊之權益。

(2)最新進展

自上屆（ICANN 78）大會結束至今，與 WHOIS 與資料保護政策有關之進展或討論如下：

- 將 RDRS 的「緊急請求」（Urgent Request）功能更名為「速件審理請求」

（Expedited Review Request），並調整其功能描述。

- 於 RDRS 新增供執法機關勾選之保密要求。
- 將「緊急」（Urgent）類別由「速件」（Expedited）類別替換，但其他符合緊急請求申請的收件方式，仍待後續討論。
- 針對參與 RDRS 之受理註冊機構實施系統訓練。

Laureen Kapin 另指出，有高比例的資料請求申請與未參加 RDRS 的受理註冊機構有關，故提升受理註冊機構的參與率也是後續工作之一。

針對「隱私／代理人服務認證議題（Privacy Proxy Services Accreditation Implementation，PPSAI）」，ICANN 近期終於發布政策建議分析報告的工作草案（working draft），為延宕數年的相關政策執行工作帶來新的進展，並提供社群重啟討論與反饋之機會。

(3)資料正確性

根據美國代表團成員 Kenneth Merrill 之報告，GNSO 資料正確性範疇界定工作組目前雖仍處於暫停運作階段，不過 GNSO 近期表示，有意在註冊資料保護規範完成時提前重啟工作組；另外，目前正由 ICANN 技術長辦公室（Office of Chief Technology Officer，OCTO）制定中的報告，將分析網路攻擊的偏好手法，出版後或有助減低發生於頂級網域的惡意攻擊，部分內容也將有助資料正確性的討論。

(4)緊急請求揭露註冊資料

GAC 建議 ICANN 董事會，為因應此類請求相關之重大公眾安全利益，盡速採取行動建立明確的流程與交付時程，以落實網域名稱註冊資料緊急請求政策。此類流程應確保 ICANN 社群，包含 GAC 適當參與。

GAC 重申其公共政策上之疑慮，即對於在特定緊急情況請求註冊資料（稱謂「緊急請求」）之適當回應時間建置一事上缺乏進展。

GAC 回顧指出，2019 年「通用頂級域名註冊資料臨時條款加速版政策制定流程」（Expedited Policy Development Procedure on the Temporary Specification for gTLD Registration Data，EPDP）第一階段建議所提出之特別時程，以回應「『緊急』合理註冊資料揭露請求，又該請求係指有提供證據以表明迫切揭露需求之請求。」實施審核小組制定了緊急請求之嚴格標準，並於最初對於此類緊急請求提出三個工作日之回應時間。

在「註冊資料共識政策草案（Draft Registration Data Consensus Policy）」之公眾評議中，GAC 及其他 ICANN 社群反對 IRT 所提出之「緊急請求」回應時間，因該時程與回應緊急情況之義務不一致，並建議 IRT 重新檢視該回應時間。

2. New gTLD 未來回合討論

頂級域名（Top-Level Domain，TLD）為最高層級之網域名稱，因傳統頂級域名之使用漸趨飽和，ICANN 曾於 2012 年開放新通用級域名（New Generic Top-Level Domain，New gTLD）申請，並為各國政府保留主權字詞（如.taiwan）。為因應新一回合申請需求，ICANN 預計於 2026 年開放下一輪申請。本次會議討論主要聚焦開放政策配套措施等技術議題，其中為各國保留之主權字詞擬延續現行政策。

(1) New gTLD 工作小組進展

為協助 GAC New gTLD 實施審核小組議題主持人（加拿大及瑞士）之工作，GAC 內部目前由我國 TWNIC 國際事務委員會曾委

員更瑩、英國 Rosalind Kennybirch 及哥倫比亞 Thiago Dal Toe 自願加入 GAC 內部協助小組。

(2) New gTLD 實施審核小組（Implementation Review Team，IRT）

下一回合 New gTLD 申請指南（Applicant Guidebook，AGB）目前正在進行公眾評議，評議期至 2024 年 3 月 19 日，工作小組已起草 GAC 建議。目前 New gTLD 下一回合開放時間仍預計落在 2026 年 4 月，依此時程，AGB 應在 2025 年 12 月 25 日前公布。

圖 3 AGB 公眾評議預計排程

(3) New gTLD 成本效益分析

ICANN 組織編制《與 New gTLD 下一回合計劃成本與效益相關的分析概述》（Overview of Analyses Related to Costs and Benefits of the Next Round of the New gTLD Program），惟部分 GAC 成員提出該文件之不客觀、不獨立性，分析應由第三方顧問進行。

(4) 公眾利益承諾（Public Interest Commitments，PICs）／註冊管理機構自願承諾（Registry Voluntary Commitments，RVCs）

- PICs/RVCs 議題目前正進行社群諮詢，第一階段諮詢期至 2024 年 2 月 23 日止，ICANN 79 會議後之第二階段意見收集至 2024 年 3 月 31 日止，GAC 由美國及英國協助意見起草。
- 《ICANN 章程》修訂程序：依序為「ICANN 董事會提出」→「公眾評議程序」→「ICANN 董事會批准」→「賦權社群（Empowered Community）批准程序」（如果批准）→社群論壇。
- 部分 GAC 成員建議，須將此議題進行法律相關分析，並將結果分享給 ICANN 社群，以協助社群討論、判斷是否需要修改《ICANN 章程》。

(5) 申請人支援計畫（ASP）

GAC 建議 ICANN 董事會以下幾點：

- 回顧 ICANN77 GAC 建議，社群要求「改善輪次」的呼聲，確保「申請人支援計畫（Applicant Support Program，ASP）」著重於促進 New gTLD 計畫全球多元化。
- 公告完整詳盡 ASP 溝通與推廣策略，及相關施行計畫，供 ICANN 社群審查與評論，其中包含詳細的成本、詳盡的工作範圍與明確的成功指標，以補充施行計畫中所包含的 New gTLD 未來回合計畫廣溝通規劃。此 ASP 溝通及推廣策略，必須包含建立「全球通用」（Universal Acceptance，UA）及「國際化網域」（Internationalized Domain Names，IDN）意識之細節，並應運用 ICANN 社群關係網確保覆蓋到資源匱乏地區。
- 明確說明 ASP 相關基金將如何專用於協助申請人，並在考慮到上次啟動 ASP 後至今之通膨情況下，評估支撐 ASP 計畫之適當預算及相關溝通與推廣策略。

GAC 強調，促進全球多元化對 ASP 計畫成功之重要性，並請

ICANN 董事會參考 GAC 對資源匱乏地區之定義。GAC 觀點是，全球溝通與推廣對於鼓勵資源匱乏地區組織機構透過 ASP 申請，至關重要。將運營 gTLD 的經濟益處標示出來，將有助於組織機構理解申請 New gTLD 的益處。

此外， GAC 擔心，若 ASP 資金配額依舊如 2012 年輪次，將無法充分保障所有成功申請者都能從 ASP 受益，特別是要考慮到過去十年以來的通膨趨勢。此外，申請費用將增至約 240,600 元美金，自 185,000 美金增加了約三成。據此，ASP 資金至少應等比例增加。

3. DNS 濫用討論

美國聯邦交易委員會(Federal Trade Commission, FTC)代表 Laureen Kapin 分享了「Consumer Sentinel Network」計畫，與聯邦貿易委員會出版的 2023 年度美國詐騙數據報告。根據此報告，內容型詐騙手法以電子郵件形式獲得最多申訴，且由於電子郵件為網路釣魚詐騙的主要載體，與 DNS 濫用防治關聯性高。其他相關載體還包括線上廣告、跳出式廣告、網站與應用程式，造成的金錢損失總數高居第三位，符合 DNS 濫用行為定義的「網路釣魚詐騙（Phishing）」。在去（2023）年間網路釣魚詐騙的申訴總量超過 1,000 筆，損失總金額超過 220 萬美金，其主要手法為冒用企業或政府之名詐騙，並藉機取得受害者個資。

(1) DNS 濫用情形之量測

CleanDNS 專案代表 Alan Woods 表示，DNS 濫用防治不應單純著重在通報數或測得數據的呈現，而是應透過質化分析來評估 DNS 濫用的起因與衝擊，後續再綜合考量締約方組織的意見。其另強調，在處理 DNS 濫用行為時，除了最終手段的「阻斷(stopping)」

外，也可考量「干擾（disrupting）」作為的必要性。Alan Woods 透過下列三點，說明 DNS 濫用防治修訂工作的關鍵：

- 顯現有因應必要之證據（Actionable Evidence）：此項涉及濫用申訴之方式與查核，以及所出具證據在取得與調閱上的一致性。目前的濫用申訴僅顯示案件總數，並未標註是否已獲證實。為量測這項要件，就必須建立申訴標準及最佳實踐。
- 立即行動（Prompt Action）：此項涉及如何定義「立即性」，並予以有效量測。依據 SSAC 115[4]，此要件雖已訂定 96 小時的標準，但仍建議締約方研判事件之嚴重性，縮短因應時間，並記錄、分析影響締約方主觀判斷之因素。
- 阻斷及／或改行干擾（Stop and/or otherwise disrupt）：此項涉及所採取的因應作為是否適當。ALAN WOODS 建議針對締約方的因應決定、採取作為及對受害人的影響進行分析。

Alan Woods 另表示，找出並排除未能積極處理的締約方，縮短 DNS 濫用的「存留時間」（Time to Live），也是 DNS 濫用防治修訂工作的重心。這也是這項工作在分析時不應側重量化、而須兼及質化面向，並從理解締約方的主觀考量與因應實踐上著手之原因。

(2) 後續進展方向

歐盟代表團成員 Martina Barbero 重申 GAC 在 2023 年 7 月 17 日提出的 DNS 濫用防治意見，GAC 成員也針對 ICANN 履約管理部門後續彙報進度之時間點，及對於政策擬定之期待進行討論。

---

4 https://community.icann.org/display/BA/SAC115%3A+SSAC+Report+on+an+Interoperable+Approach+to+Addressing+Abuse+Handling+in+the+DNS

三、ccNSO 相關議程

(一) Tech Day

1. Tech Day 1

(1) LACTLD Anycast Cloud

LACNIC 分享 LACTLD 的 Anycast 雲端架構[5]，該平臺是拉丁美洲區域的非營利協同架構。與商業的 Anycast 產品類似，不同的是該平台是由拉丁美洲的社群自行設計研發。

A. ccTLD 的 DNS 運作機制

說明早期 LACTLD[6]的 ccTLD 運作機制有多個權威伺服器，其中一台為主從架構的主要伺服器,負同步其他的副伺服器以滿足覆載平衡、客戶最短距離與達成堅固與韌性需求。

早期 LACTLD 的 ccTLD 就有非正式的互相支援機制，但難以進行擴充。

B. 升級成 Anycast 服務

透過 Anycast 架構升級舊機制並滿足下列優點：網路使用最佳化、透過 Anycast 完成主從架構的進化、將伺服器以節點的型態隱藏於雲端中、高擴展性與韌性、更適合抵禦阻斷服務攻擊(DoS)。

C. LACTLD Anycast 雲端服務現狀

該 Anycast 雲端服務由 LACTLD 會員共同管理(主要為.br, .cl 與 LACNIC)，除此之外還有一些全球性的 IXP 會運營節點以負責

[5] https://programafrida.net/en/archivos/project/lactld-anycast-cloud

[6]https://www.lacnic.net/3257/47/evento/lactld

全球性的流量。

自 2015 年正式營運後已有 19 個 ccTLDs 加入，共計為 LACTLD 的 61%成員。

D. LACTLD Anycast 雲端服務之架構

共有 18 個正式服務節點，包含一些單一節點與全球節點、目前流量為約每秒 2 萬次查詢，峰值為每秒 3 萬次查詢。

(2) DNSSEC.UA With Knot

Hostmaster.UA 分享透過 Knot 升級 DNSSEC 之心得。

A. 為何使用 Knot

使用 Knot 而非 Bind 原因，包括透過排程更新 ZSK，消除新舊 ZSK 同時存在的問題、可在必要時再更新 RRSIG，Hostmaster.UA 採用每四天更新一次 RRSIG 進行、更有效率的更新模式、與 6connect 整合以達成 Anycast 功能、獲得 CZNIC 的支援(Knot 為 CZNIC 之專案)。

B. 介紹 2023 年時.UA DNSSEC 架構遷移之時間線

主要針對遷移過程中的「事件」進行介紹，講解將檔案匯入 EPP 資料庫中因為 Bind 序號所產生的問題，講者建議使用者在進行此類遷移可在測試環境測試完成後再進行。此外講者也針對遷移的過程中載入 Zone File 可能發生的錯誤與衝突點進行解說。

C. .UA TLD Zone Singer 遷移計畫

- 建立虛擬 Knot 伺服器；
- 設定該伺服器為線上簽章者；
- 複製 KSK/ZSK 至該伺服器；
- 交由 Knot 進行各種自動化更新，包含 ZSK 輪換、RRSIG 與 NSEC3 更新以及進行少量的 IXFR 測試

(3) Registry System Testing 2.0

Registry System Testing (以下簡稱 RST)是為確保註冊管理機構有能力用穩定且安全的手段運營新通用頂級域名所設計之流程。此項目最早在 2012 年由 ICANN 的 Internet Infrastructure Support 所開發。因為以下原因，現在的 RST 被認為是老舊且不適合使用於下一輪新通用頂級域名之營運：

- 手動管理，無法任意擴充；
- 除錯與重試之生命週期過長；
- 範圍未包含新的註冊管理機構服務，如 RDAP。

A. RST 2.0 支援下列新增項目

- 加入現有關鍵功能的測試計畫，例如，新增 RDAP 並移除 Whois 等。
- 更新現有註冊服務供應商評估計畫，包含主要的註冊服務供應商、DNSSEC 服務供應商、DNS 服務供應商與代理人服務供應商。
- 通過 RST 是完成註冊服務供應商評估計畫最終確認。
- 全自動化、自助服務，並提供可操作測試情境與環境（OT&E）。

B. RST-API 相關介紹

RST-API 透過 OpenAPI 格式所開發的規格見 https://icann.github.io/rst-api-spec/ ， Github 連結詳見 https://github.com/icann/rst-test-specs

C. RST 測試計畫

測試計畫包含以下屬性：

- 機器可讀之測試規格
- 階層化結構，一個測試計畫有一個或多個測試套件，一個測試套件有一個或多個測試案例
- 以 YAML 檔案保存所有測試之預期正確結果
- 可產出人類可閱讀之 HTML 格式文件
- 所有的可輸入參數與輸出結果皆以 JSON 格式設計
- 所有錯誤情境皆有一個獨自的編號以便識別

D. 註冊服務供應商評估計畫

依據註冊服務供應商的類別 RST 制定了不同的評估計畫，以對應相關的之角色與功能，如圖 4 所示。

Main RSP	DNS RSP	DNSSEC RSP	Proxy RSP
1. **EPP** a. RFC conformance b. Query and transform commands c. Extensions (e.g., DNSSEC, RGP) d. Data persistence 2. **RDAP** a. RFC conformance b. RDAP profile conformance 3. **IDN** a. IDN Guidelines conformance b. IDN table review c. Variant handling in the TLD and second level 4. **RDE** a. RFC conformance b. Deposit integrity 5. **Rights Protection Mechanisms (TMCH)**	1. **Authoritative DNS** a. RFC conformance b. IPv4/IPv6 reachability c. Zone file conformance	1. **DNSSEC Signing** 2. **Maintenance of Chain of Trust** 3. **DNSSEC Operations** a. ZSK rollover b. KSK rollover c. Algorithm rollover	1. **EPP and RDAP conformance** 2. **Integration with Primary SRS**

圖 4 評估計畫角色與功能對應

E. Pre-Delegation Tests

Pre-Delegation 測試是針對頂級域名之測試，測試內容包含 EPP、IDN、RDAP 等，此外也會對進行整合測試確認系統與其他系統界接無誤。

F. 針對 DNS 與 DNSSEC 的測試計畫

此測試計畫是基於 Zonemaster 所制定，透過測試規格產生剖繪並在系統本地端進行測試。針對 Anycast 架構也會針對資料一致性進行測試。RDAP 測試套件會使用 RDAP 一致性工具進行測試，詳見 https://github.com/icann/rdap-conformance-tool。

(4) DNS Monitoring – Hands-on look at observability for authoritative DNS operators

NetActuate 以權威 DNS 營運人員角度介紹各式監控工具以及實際資料進行手作示範並提供相關的 Playbook 與儀表板工具。

A. AS112

AS112 是用於緩解私人 IP 反查行為導致佔據公用 DNS 資源之專案，該專案使用專門設置的 DNS 服務器，負責處理這些查詢，任何有興趣於此專案的人皆可加入該計畫。

B. 可觀察性

可觀察性的基本定義包含系統是否保留日誌、系統指標以及系統軌跡等。

C. DNS 服務監控可用的商業工具

講者介紹了市面上可用的 DNS 服務之商業工具，包含 Prefops、Globalping 與 RIPE Atlas 等。

D. 針對 Anycast DNS 服務監控可用的工具

Anycast DNS 服務錯誤通常是因為 BGP 路由錯誤所導致，講者推薦下列 BGP 路由監控工具，包含 BGPAlerter、PacketVis 與 bgp.tools 等。

E. 內部 DNS 監控

內部 DNS 監控往往帶有許多雜訊與難以解釋的查詢，應建立起基準值以面對實際的異常進行應對。透過安裝 AS112 的方式進行內部 DNS 監控，並利用 Telegraf 進行資料收集後儲存至 InfluxDB，並透過 Grafana 以儀表板方式呈現。

F. 告警機制

告警機制建立在每個 AS112 節點的基準值上，使用者可以依據自己的需求透過平日基準值建立告警機制。

此外補足 DNS 日誌不足的部份，Netflow/sflow 也可以加入監控告警之考量，以利監控如 DDoS 等事件之發生。

2. Tech Day 2

(1) SSAC Greetings at Tech Day

SSAC 副主席 Tara Whalen 透過 Tech Day 介紹 SSAC 與其角色與職責，包含參與社群互動、分析 DNS 系統可能遭遇的威脅與風險、與其他組織合作，如 IETF、RSSAC 與 RIRs 等、對 ICANN 董事會報告過往活動與關鍵發展進程、根據安全評估與營運專業對 ICANN 社群與董事會提出建議。

此外 SSAC 也希望藉此機會招募 SSAC 會員，以增加心血並提高區域參與的多元性。

(2) ICANN Domain Metrica

Domain Metrica 是由 ICANN CTO 辦公室的 Security, Stability and Resilience 團隊(以下簡稱 SSR 團隊)所提出的新專案，因為現有專案 Domain Abuse Activity Reporting (以下簡稱 DAAR 專案)具有特定目的導致難以新增或擴充功能，團隊提出 Domain Metrica 專

案用來精進網域名稱指標評估。

A. 提高指標品質

藉由新專案的導入，SSR 團隊希望透過以下目標提昇指標品質：

- 資料品質之提昇，如降低誤判；
- 更準確的定義,比如從 SPAM 中細分釣魚與惡意程式派送;
- 考量評量誤差，認知並理解指標之限制；
- 透明且可重複進行，數字可被獨立驗證或方法可在不同的地方使用。

B. ICANN Domain Matrica

ICANN Domain Metrica 包含下列特性：

- 為一個測量平臺，任何可發現或精進之精準評估方法都會加入測量；
- 模組化，隨著時間推移新的 Meta data 都可以透過模組化的方式加入；
- 具有靈活性可依據使用者需求使用,並根據需求進行更新;
- 公開且透明，所有的方法與來源都會被公開，並盡可能的分享資料。

C. 從 DAAR 的經驗中進化

Domain Metrica 將取代 DAAR 給予網域名稱更精準的指標評估，預計會有下列改進：

- 更有用且精確的資料，如註冊服務供應商層級的統計資料並提供互動式的圖表呈現；

- 更容易取得資料，更有善的網頁界面並提供 API 存取；
- 更具擴充性，考量使用者與所需容量的增加，該專案將會是全雲端解決方案。

D. 包含 DNS Abuse 議題之外的範圍

與 DNS 相關的有效數值與指標皆將納入該專案，包含網域熱門指標、近即時惡意與被入侵網域之分類、持續運營時間與安全威脅預警等。此外穩定與安全性相關議題指標也都可以納入該專案。

E. 預計時程

此專案預計在今年第三季發布，使用者可利用 ICANN 帳號進行存取。

(3) eeID: strong contact identification @.ee

.ee 為愛沙尼亞 ccTLD，因為以下原因推動 eeID 以利管理 DNS 註冊服務利害關係人們：

- 有效的身份識別防止濫用；
- 確認外國註冊人之身份；
- NIS2 要求註冊管理機構、註冊機構以及服務供應商必須驗證網域註冊中的聯絡人資訊。

為此.ee 找到了以下解決方案：

- 使用 European eIDs；
- eIDAS；
- RegeID；
- 透過直接接觸確認。

.ee 透過此機會接觸到了 RegeID 專案，於是決定建立一個識別平臺，讓包含國外的註冊服務供應商也能夠方便使用此解決方案，此平台被稱為 eeID。

講者透過線上展示，透過 eeID 存取.ee 相關網域註冊服務，並指出一切都建立在 Personal Id code 這個屬性上。

除了歐洲之外的使用者，eeID 透過整合 Fast Identity Online（FIDO）進行認證

(4) DNSCAPTURE – A DNSSEC Diagnostic Platform

DNSCAPTURE 是用於驗證 DNSSEC 設定與紀錄是否正確的工具，預計包含以下功能：

- Zone 驗證：驗證 Zone 中所有的紀錄包含 NS, MX, A, AAAA, SOA, DNSKEY, DS, NSEC/NSEC3；
- SLD 驗證：從 SLD 層級驗證相關 DNSSEC 紀錄；
- CDN based DNSSEC：針對多層 CDN 架構中使用 CNAME 進行 DNSSEC 驗證之確認；
- Negative Validation：尚未實做之功能，預計用於對特定 Zone 及其所屬 TLD 進行 DNSSEC 驗證。

此外 DNSCAPTURE 預計在今年釋出更多新功能如下：

- PassiveDNSSEC：該功能用於透過時間軸圖表來呈現不同網域/Zone 的 DNSSEC 紀錄變更；
- GRAPH Analysis：類似於 DNSViz 的多層 DNSSEC 視覺化工具；

- 修正建議功能：目前的工具只指出錯誤點而沒有詳細的建議，該工具將透過 rfc8914 進行這方面補強；
- DNSSEC Crawler：建立 DNSSEC 爬蟲獲得資料後建立視覺化。

透過實機演示，講者介紹了 DNSCAPTURE 目前的功能，可以看出該工具還在早期的階段，大多的結果以文字化呈現。

3. Tech Day 3

ICANN79 Tech Day 第三場為 eID 的座談討論，主要針對如何識別註冊人身份進行討論。

(1) Digital Credentials Use Case: .CA Registrant Information Validation (RIV)

透過.ca（加拿大）註冊人資訊驗證來分享數位憑證的使用案例，.ca 並未針對所有新註冊的網域註冊人進行資訊驗證，而是選擇在被回報為濫用的時候進行此項驗證，他們將此流程稱為 RIV。

目前的作法是.ca 要求所有的網域註冊人必須是加拿大居民或者擁有加拿大商標。一旦調查啟動，稽核團隊會透過電子郵件的方式要求被請求方提供護照、駕照或出生證明的影本，但這產生了兩個問題：

- 隱私權問題，要求註冊人提供上述資料對隱私權有一定程度的侵害；
- 稽核團隊無法驗證憑證之真實性。

因此.ca 決定轉用數位憑證進行驗證，新版的驗證程序將會沿

用上述流程，僅將實體的身份憑證改為線上的數位憑證。實際作法是透過具有身份驗證的功能的支付系統(電子錢包)進行身份驗證，再將相關的驗證資訊以數位簽章的方式進行傳輸，團隊僅需要驗證該資訊是否是正確簽章過得資訊即可。

但此作法產生的僅能驗證該註冊人提供了正確簽章的數位憑證，而無法驗證該數位憑證與註冊人之連結，如惡意使用者偽冒他人的身份。目前.ca 的作法是將此確認轉嫁給發行該數位憑證的發行者，如確認該發行者本身已進行過驗證，則認為此憑證與註冊人之身份是一致的。

(2) Domain Ownership digital credentials

European Digital Identity Wallet 即將實施，屆時所有歐盟公民將可以用數位或實體的方式儲存自己的身份證明，其中包含身份 ID、大學文憑與駕照等。

.cz（捷克）提出了將 Domain ownership digital credentials 放入歐盟電子錢包的概念，執行方無論是註冊管理機構或註冊機構皆可。

一旦此憑證發布後，註冊管理機構或註冊機構可透過自動化的方式每日對該網域擁有者的電子錢包進行身份驗證，以達到持續驗證的目的。

(3) Electronic identification and verification – simple, good and necessary

eeID 講者針對個人識別碼進行更詳細的分享，講者認為該識別碼是數位身份的重要關鍵。由於歐洲國家中有因為歷史原因不願

意針對公民進行編號，也有國家將此識別碼是為隱私資訊，因此該資訊往往被用其他方式再處理過，如將編號分段等。在不同的情境下，審核方可能會在同一個人身上得到不同的個人識別碼，因此講者建議用混合式的方法進行身份識別，如同 eeID 現在所有的架構一樣。

(4) .th Registrant Verification and Authentication

.th（泰國）分享他們的註冊人的驗證與認證方式，驗證策略為針對所屬所有網域註冊人進行驗證，因為.th 會提供免費的泰文網域給個人使用，所以會分為個人與團體(公司/機構/政府單位)兩大類。

A. 個人部份

驗證註冊人的身份證件，如駕照或者數位身份證，驗證是否本人的部份則交由可信賴的執法單位執行。

B. 團體部份(公司/機構/政府單位)

驗證註冊人的文件，同時也會透過可信賴的執法單位協助確認。

.th 目前以文件的方式進行驗證，但泰國以有數位身份證平台，個人會有國名身份證 ThaID，尚未支援非自然人，所以團體的部份還需要等待建置。

講者分享透過數位身份證驗證個人網域註冊人之機制，其機制名為 ndid，該機制是透過區塊鍊技術所建置，其中也整合了銀行提供 Idp 服務進行驗證，並在註冊人同意後對權威機構請求註冊人資料進行驗證。

鑑於 ndid 價格問題，.th 目前考慮將此項目轉移到 ThaID 並與

其他政府服務進行整合。

因提供民眾使用泰文電子郵件導致無法在許多只接受英文作為電子郵件帳號之平台使用，.th 也設計了一個專門為泰文設計的認證平臺。

(5) 互動討論環節

由與會專家進行座談討論。

A. .swiss（瑞士）分享數位認證作法以及經驗

.swiss 有近 2 萬個法人網域，其認證方式是在紀錄中放入公司 ID 來作為身份認證的基礎，所以要取得.swiss 域名就要取得公司 ID，目前此這個作法並沒有任何偽冒的情形，即便註冊的過程需要花費更多的時間，但也確保了安全。但現在碰到的問題是 DNS EPP 中中並沒有欄位可以放置這類公司 ID 或識別 ID 的欄位，但在 RDAP 中有一個欄位稱為公共 ID 目前通常僅用於 RDAP 中識別 IANA 註冊商 ID，該欄位有未來可以利用的機會。

B. RegeID 與歐盟 eIDAS

RegeID 計劃目的在將所有歐洲電子身份證整合到註冊流程中。然而，由於 eIDAS 的作業方式，歐洲各國在數據交換標準方面存在差異，尤其是在組織數據方面。目前歐洲僅有一些國家提供給組織的數位身份。新的歐洲數位電子錢包可能會提供更適用於私營部門的框架。至於域名產業中目前還沒有太多的註冊管理機構或註冊機構參與其中，但隨著 NIS2 規定的實施，對數位 ID 的關注可能會增加。

C. .th 心得分享

.th 頂級域名強調了對每個註冊者進行驗證的重要性，以確保

使用該域名的是合法的實體。目前正在實施一個名為 NDAD 的平台，但使用該服務的人數仍然較少。但隨著數位化進程的加速和成本的降低，更多需要驗證註冊者的頂級域名可能會考慮實施類似的服務。

D. CIRA 與可信賴註冊

CIRA 認為可信賴註冊重點在於可信任註冊管理局。可信賴註冊目前正由 Linux 基金會的 Trust over IP 組織進行相關的工作。他們致力於定義信可信賴註冊相關協議，並在 IETF 進行相關工作。他們的目標是制定標準，使 DNS 和 DNSSEC 能夠發現發行者與註冊管理局之關聯，並建立信任。

E. OpenID Foundation 與 Open Wallet Foundation

CZNIS 參與了 OpenID Foundation 和 Open Wallet Foundation，目前致力於開發開源軟體，可能用於構建電子錢包。在歐洲，ETSI 是一個非常重要的組織，因為歐洲的法規只能參考 ETSI 或 ISO 標準，無法參考 IETF 標準。因此，許多 IETF 標準都轉變為 ETSI 標準以便於在電子錢包中使用。目前有數個標準競爭中，如 W3C 的可驗證憑證和 IETF 的可驗證憑證替代方案，以及 ISO 的 MDL 標準。這些標準具有不同的特性，因此需要確定哪個標準將勝出，或者哪個標準將被修改以滿足所有需求。目前正努力使所有錢包之間實現互操作性。

4. Tech Day 4

(1) .PR（波多黎各） Tech Day Presentation

講者分享推廣.pr 的策略與經驗。包含為了提高與.com 競爭的優勢推出優惠的價格，以及免費提供在地使用者一折優惠等。外國

商家落地波多黎各也可以透過文件證明後申請一年的免費.pr 網域，此外他們也提供了客戶端的 Portal 讓使用者可以針對自己的網域進行管理。

此外他們還有推薦計畫，讓其他代理商也可以透過分成的方式販賣.pr 網域。

(2) Auction: fair method for releasing domains @.ee

.ee（愛沙尼亞）分享為何他們覺得網域拍賣是最好釋出網域名稱的方式，原因如下：

- 防止域名搶註，減少域名蟑螂
- 公平的取得權
- 提高網域的價值
- 降低註冊服務的負擔

.ee 嘗試過使用隨機的釋出網域、限制存取次數防止機器人等方式，但因此必須隱藏或延遲 WHOIS 資訊。這種方式導致發布不實訊息的問題，所以最終在抽獎與拍賣中間選擇了網域拍賣。

因分享拍賣推動之初遭到大大的反彈，講者認為溝通是關鍵點，比須讓相關資訊傳達給相關的註冊機構以及大眾，並了解對方的觀點且公開不預設立場。

接著分享網域拍賣的經驗，講者認為「先到先得」並不適用於網域拍賣，尤其在 Registrar-Registry-Registrar（RRR）模式下並不公平，於是採用了預約機制並使用盲拍（Blind auction）模式。競標者需要在一定的時間內提出適當的價格競標網域名稱，中間可以

做任何修改，截止後價高者得。得標者必須在 7 天內付款並在 30 天內註冊該網域，若連續違反相關規定 3 次則會加入黑名單。

此外他們也透過了 AI 的幫助來排序競標，讓更受歡迎的網域更容易被競標者所看到，就跟電子商務網站的推薦系統一般。

(3) Measuring Domain Abuse

分享更有效的域名濫用評估方法,講者認為現有的域名濫用評估方法並不有效,單純的數字統計並無法呈現每個濫用案例的目的性與衝擊程度，因此提出了新的評估方式。

A. 評估域名濫用之生命週期

透過追蹤域名濫用之生命週期可以測量該惡意行為所帶來的衝擊持續時間。量測該指標不僅可以提高降低域名濫用持續時間,且可藉此降低其生命週期，達到減少受害者之目的。

B. 損害導向分析

分析域名濫用所造成的損失,藉此判斷惡意行為的危害程度。此舉可以協助處理大量的域名濫用時找出必須被優先處理之事件。

C. 損害報告之現狀

講者認為在現有機至中損害報告屬於極度不足的情形，大多數的線上攻擊都是針對特定小部份人群且受限於使用者必需自願提出損害報告，目前全球範圍內只有少於 2%的線上攻擊有提供損害報告。

D. 提高線上攻擊之門檻

講者分享提高線上攻擊之門檻手法及相對應的缺點，如單純的提高網域註冊價格門檻無法阻止線上攻擊的發生,因為回報更為巨大。近期出現許多惡意使用者利用假身分或竊取的身分來註冊網域，也無法阻止他們透過中間商購買網域。此外服務供應商往往是商業競爭關係,彼此之間

不會互相交換線上攻擊之資訊，於是切換供應商就可以閃避大多數的偵測。針對新帳號的審查與延遲開通也可以有效降低線上攻擊發生的時間與頻率。此外對惡意來源的網路架構進行關聯，如找出指向惡名昭彰(Bad Reputation)的 IP 地址或 DNS 伺服器之網域也是提高攻擊門檻的方法。

(4) Applying the DNS/DNSSEC/DANE Protocol Stack to Digital Emblems

數位徽章（Digital Emblem）概念最早是由國際紅十字會（ICRC）因需要可被密碼學驗證的數位標章而來，PCH 講者分享透過 DNS 相關的防護機制來作為數位徽章之應用。

A. 使用案例

透過數位徽章作為密碼學可驗證的標誌來標記數位資產，例如網站、電子郵件伺服器和靜態數據。此外也可以與 QR 碼或 RFID 結合使用，以允許驗證實體物件的真實性。

B. 數位徽章與 DNS

數位徽章的之密碼學驗證是透過 DANE 中的數位憑證與其他 DNSSEC 簽章結合。透過 DNS 記錄與帶有徽章的實體關聯，如顯示徽章使用的核可人、地理位置等。目前 IETF 正在進行 DNS 圖形標記和位置記錄研究的相關工作。利用 DNS 允許分層分散管理，例如國際紅十字會和國家紅十字會分層標記。同時使用動態 DNS 和 DANE 允許安全快速的更改或撤銷。

C. 數位徽章與 DNS 運用

PCH 正與國際紅十字會和其他機構（JHUAPL）合作，開發具彈性、動態和安全設計的數位徽章。正在進行的工作使用現有的 IETF RFC（包括 DANE、TXT、LOC），並開發數位徽章之原型以用於使用案例中展示。目前工作已達到里程碑。

(二) Internet Fragmentation

本場次由 ccNSO Internet Governance Liaison Committee（IGLC）規劃，主要討論網路分裂（Internet fragmentation）對 ccTLD 的影響。

一般對於網路分裂的討論常常混淆在一起，定義也很發散，網路治理論壇確認網路分裂的三個層面包含使用者體驗層面、技術層面以及治理層面。Elena Plexida （ICANN org, Vice President for Government and IGO Engagement）表示，網路內容已是分裂的現況，不是所有人、所有地方都可以接取網路內容，這是限制或規管造成的分裂呈現，例如家長監護措施，或是歐盟的 NIS 2 修正案。就技術層面來說，尚未有分裂的呈現，但隨網路技術的發展，或許可能出現另一套 DNS 或 IP 協議取代現行的標準，而造成分裂的情況。而另一個分裂的原因則是在治理層面的國家主權政治因素，例如地緣政治的緊張關係或各國開始立法規管 DNS 等，這是網路分裂目前最被關注的層面。

Bruna Martins dos Santos 介紹 IGF 的網路分裂政策（Policy Network on Internet Fragmentation ，PNIF），歷經 2022-2023 二年的討論，PNIF 主要目標是(1)提供一個系統化、全面性的架構來定義網路分裂、及其造成的原因與影響；(2)案例收集及分析；(3)提供相關原則或建議，以維護網路開放、互連互通的本質，防止網路的分裂，PNIF 從三個面項進行討論並提供可能的建議作為: User Experience、Tech Layer，Internet Governance and Coordination。

相關內容可參閱 https://www.intgovforum.org/en/content/policy-network-on-internet-fragmentation。

之後由.za（南非）、.br（巴西）及 AFTLD 分享網路分裂的案例。.za（南非）簡述該國過多及不連貫立法所造成網路分裂情況，以及 One

Internet 對國家主權的潛在威脅。.br （巴西）認為須處理網路分裂的確切定義及分類，避免犯下日後無法修正的錯誤。AFTLD 以 Internet Shutdown 為例，說明主權國家是造成網路分裂的原因之一，自 2022 年來非洲計有 7 個國家政府關閉 9 次網路，特別是在發生重大政治事件期間，據估計，2022 年非洲因關閉網路造成高達 2.61 億美元的損失，網路關閉時間總計 9,532 小時，影響 1.322 億人。約有超過 4 成（42%）的非洲 ccTLD 是受到各國政府監管的，這也可能是造成網路分裂的生存威脅。

(三) Policy Gap Discussion

這場次討論是由於一件特殊的.lb(黎巴嫩)暫時接管事件而引發的。在前次會議時，IANA 報告由於表列在 IANA 資料庫的. lb 管理代表人過逝，且無人取代，僅由幾位非正式職位的熱心人士暫時協助. lb 的維運。IANA 經相關事件調查，並與 ccNSO、GAC 及相關單位商議後，在 ICANN 的同意下，暫時接管擔任.lb 管理代表人，以「Caretaker Operations」取代原管理代表人名字，直到.lb 新的管理代表人出現。目前大多數的政策或程序都假定 ccTLD 管理單位都會依規定，主動向 IANA 來維護或更新資料，但.lb 這個案例及 IANA 的臨時性措施所呈現出的現實，已引發 ccNSO 的關注，並著手進行相關政策或方案的討論，以因應未來可能出現的問題。本場次即在討論目前 ccNSO 政策框架中與 ccTLD 授權（delegation）、移轉（transfer）、撤銷（revocation）及移除（retirement）實務程序可能出現的差距。

(四) ccPDP4 Community Update

ccPDP4 IDN 工作小組已完成相關建議報告草案，並預告後續相關工作時程。最終版報告於今（2024）年 2 月 23 日公告，包含 4 個部份：Part O - Introducing the Final Report and Policy Recommendations；Part A

- The Policy Recommendations；Part B - Advice to IDNccTLD Managers；及 Part C - Annexes。Part A 為工作小組提出的 5 大類 13 項政策建議。而 IDN Tables 及 IDN 註冊原則等二議題不在本次政策建議範圍內，列在 Part B，作為 IDN ccTLD 管理單位的參考。

相關內容可參閱：https://ccnso.icann.org/en/workinggroups/ccpdp4-final-report-23feb24-en.pdf。

四、SSAC 相關議程

SSAC 負責就網域名稱及位址分配系統的安全性及完整性，向 ICANN 董事會提出建議，包括運作問題（如正確、可靠的運行根區 DNS）、管理問題（如位址分配及 IP 分配）、註冊問題（如註冊管理機構與受理註冊機構提供之服務）、安全架構之擬定、重要 DNS 管理者與業者之溝通協調、風險分析評估，以及各項頂級網域名稱之使用可能產生之系統問題等。SSAC 目前有 33 位成員，由 ICANN 董事會指派。

(一) SSAC 與 ALAC 聯合會議

本場次係 ICANN 的一般使用者諮詢策員會（ALAC）與網路安全及穩定諮詢委員會（SSAC）之聯合會議，議程進行討論更安全的網路活動、緊急請求的後續進展、SAC123[7]簡報（SSAC 關於網路域名解析演進的報告結論）等。

1. 與更安全的網路

透過調查指出最關心的常見安全風險點是網路釣魚事件（Phishing）。我們嘗試實驗進行推廣最終用戶教育，策劃和傳播最具影響力的 DNS 安全訊息，考慮在每個地區最有效資訊宣傳方法組合，或執行類似「全球通用(Universal Acceptance，UA)日」邀請全球網路社群參加活動。

2. 緊急要求揭露註冊資料

僅限於對生命、嚴重身體傷害、關鍵基礎設施或兒童剝削構成迫在眉睫的威脅的情況，以及在對抗或解決這種威脅時需要披露資料的

[7] https://itp.cdn.icann.org/en/files/security-and-stability-advisory-committee-ssac-reports/sac-123-15-12-2023-en.pdf

情況。

(1) SSAC 的主要關注點

缺乏針對緊急請求的具體提交機制，依賴一般揭露請求流程，反應時間「一般」在 24 小時內，最多可延長 7 天，對於描述為「對生命構成迫在眉睫的威脅」或嚴重傷害的情況來說，反應時間被認為不足夠。

(2) SSAC 檢視該政策的四個方面，以確定其不符合目的：

- 適用性：目前政策可能無法充分滿足快速揭露的迫切需求。
- 透明度：政策用語和基本原則含糊不清（需要明確）。
- 聲譽：對 ICANN 在緊急情況回應方面的形像有潛在的負面影響。
- 流程：現有流程在有效處理緊急揭露請求方面所面臨的挑戰。

(3) SAC122[8]建議

該政策必須提供額外的結構，以便以適當加快的方式處理緊急請求並確保處理回應時間符合目的，且 ICANN 組織應獲取並記錄有關緊急請求的資料，向社群提供進階資訊。

(4) 緊急請求

「合法披露的緊急請求」僅限於對生命、嚴重身體傷害、關鍵基礎設施或兒童剝削構成迫在眉睫的威脅的情況，以及在對抗或解決這種威脅時需要披露數據的情況。

8 https://community.icann.org/display/BA/SAC122%3A+SSAC+Report+on+Urgent+Requests+in+the+gTLD+Registration+Data+Policy?preview=/292421745/292978690/sac-122-en.pdf

3. 建議的私人使用頂級域名對最終用戶的影響

本場次針對現有政策是否符合全球公共利益進行討論，如 RDRS 回應資料要求的規定時限過長，不符使用者需求等問題。

(1) SAC123

SSAC 關於私人使用 TLD 的諮詢報告，包含「私人使用 TLD 的使用範例」（例如 .home、.corp、.mail、.internal）。

(2) SSAC 建議 ICANN 董事會確保使用第 4.1 節中指定的標準來識別字串，並在頂層保留該字串供私人使用。這個特定的字串絕不能被委託。SSAC 提出了以下字串選擇標準：

- 有效的 DNS 標籤。
- 尚未在根區域中進行委派。
- 與現有的 TLD 不存在令人混淆的相似之處。
- 內容比較短，容易記住，且有意義。

4. 公眾意見

建議私人使用的頂級網域字串。

(1) 網際網路號碼指配機構 (IANA) 已做出臨時決定，應保留「.INTERNAL」供私人使用和內部網路應用程式使用。

(2) 在 ICANN 董事會審核和批准此保留之前，我們正在尋求有關該選擇是否符合 SAC113[9]指定程序的回饋，以及任何其他認為該字串不適合此目的選擇的意見。

[9] https://community.icann.org/display/BA/SAC113%3A+SSAC+Advisory+on+Private-Use+TLDs?preview=/218466759/240616395/sac-113-en.pdf

5. 對最終用戶的影響

SSAC 已選出下一屆的主席與副主席，分別為 Rom Mohan 與 Tara Whalen，任期為 2024 年的 1 月 1 日至 2026 年的 12 月 31 日。

(1) 潛在好處

透過明確區分公有和私有命名空間來提高安全性，降低與潛在 gTLD 的域名衝突風險，增強用戶在瀏覽網路時信任度和可靠性。

(2) 潛在挑戰(潛力)

使用者可能不知道「.INTERNAL」或輕易採用它，導致潛在的混淆或繼續使用非指定域名。

6. SSAC 和 ALAC 的角色

SSAC 提供有關實施和安全影響的技術專業知識和指導。ALAC 倡導最終用戶利益，重點關注可用性、可訪問性和認知度。

7. 不斷發展的網際網路域名解析空間

(1) SAC123 報告：SSAC 關於網路域名解析演進的報告，不斷變化的需求刺激具有不同原理和功能的替代命名系統的開發，此報告探討替代命名系統的影響。

(2) 改變網際網路域名解析的動機：變革的動機，包含速度增強、隱私問題、去中心化治理等，為使替代系統被廣泛接受，需要提供功能或克服 DNS 的某些技術限制。

(3) 現今使用的替代命名系統：許多替代命名系統與特定應用程式捆綁在一起，這些應用程式通常會繞過管理員控制的設定和任何預先配置的 DNS 設定。如 Multicast DNS、Tor(.Onion)、以太坊域名服務、

不可阻擋的領域及 Gnu 域名系統。

(4) SSAC 建議 ICANN 應追蹤並定期提供的更新：利用域命名空間的替代協議，努力創建緩解措施並減少多個命名空間和協議共存的風險。另應透過新興識別碼技術小組等方式讓 ICANN 社群及時了解新的發展動態。

(二) 與董事會會議

本場次係 ICANN 董事會（ICANN Board）與網路安全及穩定諮詢委員會（SSAC）之聯合會議，會前已就 NCAP 有初步的交流，議程進行討論域名衝突分析專案（NCAP）、SSAC 研究 2 最終報告草案[10]等相關議題。

1. 什麼是域名衝突？

將網域域名想像成地址，如果兩棟房子共用相同地址，郵件應該發送到哪一棟？如果被傳送到錯誤的位址，也會有安全性問題。在 DNS 系統中，最常見的當全球 DNS 命名空間中使用的網域也在企業內部使用時，就會發生域名衝突，使用者、軟體或其他功能可能發生嚴重的問題。

2. 為什麼域名衝突評估具有相關性？

首先我們發現出乎意料後果的風險。企業使用標籤作為內部的 TLD，域名可能會洩露到全球網際網路。

- 新通用頂級域名 （gTLD）引入時，增加更多域名衝突的可能性。潛在域名池越大，gTLD 字串就越有可能無意中與專用網路或內部命名系統

[10] https://itp.cdn.icann.org/en/files/name-collision/name-collision-analysis-project-study-two-report-draft-17-01-2024-en.pdf

中已使用的域名重疊。

- 由於技術和網路基礎設施的發展，測量域名衝突很困難。尤其是 DNS 的隱私增強，以及替代域名系統使 DNS 環境變得更加複雜，測量也更加困難。
- 關注衝突字串案例分析：域名衝突造成負面影響的可能性增加，並發現關鍵診斷測量有助於預測域名衝突所帶來的影響，且洩露衝突字串與授權 TLD 查詢不同，DNS 服務發現協定和蒐尋清單是主要問題。
- 不存在 TLD 的 DNS 查詢的調查研究：就根伺服器資料有益部分，任何根伺服器資料就足夠了，透過蒐集 DNS 遞迴解析資料進行域名衝突優劣的評價。
- 新 gTLD 衝突根本原因分析：這實際上集中在 ICANN 自 2012 年以來收到的 47 份報告，透過域域名衝突實測資料的強力支持，指出主要的衝突問題實際上是從 2,012 個 gTLD 字串的授權中觀察到的。今後需要從風險管理的角度來處理名稱衝突的發現。

3. 建議流程

- 第 0 階段：預申請，鼓勵申請人透過審查公開資料來主動評估潛在的域名衝突。有助於儘早識別潛在的衝突。
- 第 1 階段：初始風險，評估技術審核團隊 (TRT) 審核公開資料以評估域名衝突的初始風險，如果“高風險：”TRT 向 ICANN 董事會提交建議，或者申請人可以提出緩解計畫供 TRT 審查，其他申請進入第二階段。
- 第 2 階段：域名衝突評估，ICANN 暫時將 TLD 字串授權給根區域。TRT 進行以下一項或多項評估，包含：不間斷、受控中斷、明顯的干擾可見的中斷與通知。
- 第 3 階段：董事會決策，TRT 向 ICANN 董事會提交風險建議；申請人可提出緩解計畫供 TRT 審查，ICANN 董事會就批准申請，或可能將該

字串分配到衝突字串清單做出最終決定。

4. 技術評審組研究技術評審組(TRT)

技術評審組研究技術評審組建議建立高技術審查團隊，監督域名衝突評估的評估。

- TRT 資格：需豐富的 DNS 管理經驗，對網路基礎設施有深入的了解，熟練處理歷史和即時資料以進行趨勢分析和預測建模、精通風險管理。
- TRT 職能角色：評估域名衝突的可見性，記錄資料、調查結果和建議，評估緩解和補救計畫以及緊急應變建議。

5. 資料收集：不能簡單地重複使用 2012 年使用的碰撞偵測方法。

上一輪實施的受控中斷不適用於 IPv6，根伺服器和解析器操作員現在的資料比 2012 年少得多。另由於技術和監管變化，要嚴謹分析域名衝突，則必須從各種來源收集資料。ICANN 組織對某些提議的資料蒐集方法的隱私和機密性風險表示擔憂。

6. 時間軸

預計 2024 年 4 月 7 日 NCAP 討論小組向 SSAC 發送最終研究 2 報告，並於 2024 年 5 月 1 日 SSAC 向 ICANN 董事會傳送 NCAP 研究 2 報告及其有關域名衝突的任何建議。

(三) DNSSEC 工作坊

1. 場次一

本場議題著重在數位信任（Digital Trust）上，並以座談的方式進行。

(1) Digital Trust Panel

生成式 AI 導致數位信任在近年受大重大的威脅，各式各樣的解決方式被提出，講者分享以下幾種：

- 使用網域名稱作為識別。
- 利用 X.509 作為數字識別信息。
- W3C DIDs[11] 作為去中心化之可驗證憑證（Verifiable Credentials）。
- 使用 DNSSEC 進行識別。

A. 加入監管機制

這些方式都提供了相同的手段，那就是加密與簽章，但也都缺乏一個關鍵要素是監管的真實性。講者認為現有的憑證發行者、持有者和驗證者三角模式中需要增加一個監管機制，以確保可信賴度。

B. 確認可信賴之要素

- 機密性：確保通訊不可被觀測
- 真實性：確保參與的各方是他們所聲稱的人
- 隱私性：確保分享的信息受到尊重並不會被非法分享

C. 數位公共基礎設施（Digital Public Infrastructure，DPI）

DPI 之目的在從平台轉向由協議驅動的開放網絡。21 世紀數字公共基礎設施應包括五個基本類別需被滿足：

- 識別和登記
- 數據共享和人工智慧/機器學習模型
- 建立可信任設施
- 可透過開放通訊協定或 API 發現和實現服務存取
- 支付，使交易更便捷

[11] https://www.w3.org/TR/did-core/

(2) C2PA 與 CAI

Adobe 人員介紹並展示該公司所開發的 CAI 功能以及 C2PA 組織，其中 CAI（Content Authenticity Initiative）是一個由 Adobe 等公司領導的聯合倡議，目的在對抗數字內容的不實造假問題。它致力於發展技術，通過數字簽名和元數據來驗證媒體內容的真實性和來源。

而 C2PA（Coalition for Content Provenance and Authenticity）是一個組織，其目的在開發標準和技術以確保媒體內容的可信度和真實性。該聯盟由主要的科技公司、新聞機構和其他相關利益相關方組成，致力於解決數字內容造假問題。

(3) 信任註冊管理機構（Trust Registries）

互聯網上存在著一個缺失的信任層，導致我們無法驗證網站或實體的真實身份。信任註冊管理機構可以解決這個問題，它是一個由特定領域的權威機構管理的註冊管理機構，其中包含可驗證的數據和對實體身份的聲明。信任註冊管理機構可以用於各種目的，包括驗證數字憑證、內容真實性、以及其他信任相關的應用。信任註冊管理機構是互聯網信任的關鍵組成部分，可以幫助我們構建一個更加安全可靠的數字世界。現實世界中已有許多使用案例：

- 黃頁：列出本地企業的名稱、地址和電話號碼。
- 國際民用航空組織（International Civil Aviation Organization,ICAO）：管理能夠發行旅行證件的所有機構的主列表。
- 去中心化識別符（DID）：用於在區塊鏈等分散式系統中識別實體。

有了信任註冊管理機構可以達到以下目的：

- 驗證數字憑證：確保數字憑證是由其聲稱的實體發行的。
- 內容真實性：驗證內容的真實性和完整性。
- 訪問控制：控制誰可以訪問特定資源。
- 數據完整性：確保數據未被篡改。

信任註冊管理機構是具有前景的技術，可以幫助我們解決互聯網的信任問題。它可以應用於各種場景，並有可能在未來發揮重要作用。

2. 場次二

(1) Root Zone KSK Update

講者分享透過硬體安全模組(HSM)進行 KSK 更新，以及加密演算法的更新。

A. HSM 與 KSK 更新計畫

講者分享因為 HSM 停止支援後更換新的 HSM 供應商過程的經驗分享，包含：選擇新供應商之標準及更新後的 HSM 與 KSK 更換之時程。

B. 演算法更新計畫

講者演算法更新計畫並認為在根網域上將有以下考量：

- 對於不存在的域名查詢(50%的查詢)，可能會切換到 TCP；
- 為了減輕運營負荷，預計暫時將 RSA ZSK 的長度降低，如降至 1536 位元；
- 將制定完整的操作計劃；
- 需要對軟件和流程進行更新；
- 更新所有驗證解析的信任錨點；
- 預計對算法選擇進行社群諮詢；

- 如欲遵循理想化的 3 年 KSK 生命周期，則在 2029 年進行更新。

(2) Implementation Status of DNSSEC Bootstrapping

講者分享正在制定中的 IETF DNSSEC 啟動程序草案。

A. 以註冊人為中心設定方式

需要透過子網域啟動,有以下缺點:效能不佳且容易發生錯誤、需產生對外流量、無法有效驗證。因此此流程需要被自動化，讓註冊人無須進行額外的操作，但依舊無法進行有效的驗證。

B. CDS/CDNSKEY Processing from Insecure Child

現有的 CDS/CDNSKEY 的處理方式採用 Trust on fisrt use 的方式(簡稱 TOFU)，這方法未解決無法有效驗證的問題，草案提出了以下解決方法。實際作法為透過父網域發布子網域的 CDS 或 CDN 的金鑰記錄的副本，並使用網域伺服器所在區域之密鑰對其進行簽名。因此可以預先建立的信任鏈來建立對子網域中首次見到的簽章紀錄進行的驗證，解此達到驗證。

C. 協定草案之現狀

此草案在 IETF 之現狀：

- 以在 IETF DNSOP 工作小組進入最後請求階段；
- 父網域相關實做已在.ch 與.li 進行；
- 子網域相關實做已有 Cloudflare, Glauca HexDNS, deSEC 等廠商進行支持，並預計在 Knot DNS 3.3.5 與 PowerDNS 4.9.0-beta2 更新此功能。

(3) Do Not Go Insecure（please）

講者說明在 ICANN 70 有人提出了一項暫時取消網域簽章以應對 DNSSEC 演算法滾動所帶來之挑戰。該策略目的在簡化操作、提高穩定性，特別適用於缺乏軟體自動化的情況。但講者認為不應該這樣做，原因如下：

- 安全與穩定性並不衝突
- 軟體自動化不足並非捨棄安全性之理由
- 短暫的移除簽章依舊可以造成危害
- 光靠 TLS 與其他應用層協議並不足以保護安全
- 造成 DANE 機制失效
- 導致服務中斷

講者認為隨意的停用簽章不僅有以上危害還可以導致不利 DNSSEC 的推動。

(4) Two Trendy Ways to Hang Your DNS Cache

DNSSEC 中所有的金鑰都有一個金鑰編號（Key number），該編號為 16 位元的一補數核對和（One's Complement Checksum），導致惡意使用者可以透過偽冒大量帶有相同金鑰編號之金鑰對伺服器發出請求，藉此佔用系統資源以進行阻斷服務式攻擊，此種方法被稱為 Keystrap。

目前相關的緩解措施以備實施，包括：更新所有主要的金鑰快取、BIND 將驗證金鑰轉換到單獨的執行序上，並進行限制 Unbound 以及設定錯誤上限為 8 次。

在修復此漏洞的同時中又發現在 NSEC3 的另外一個漏洞。

NSEC3 是 DNSSEC 中的一種延伸套件用於增強 DNS 的安全性。NSEC3 通過將 DNS 紀錄進行雜奏以防止惡意使用者進行網域列舉。這種方法提高了 DNSSEC 的安全性，使得攻擊者更難進行網絡攻擊。

但同樣的惡意使用者也可以透過此機制送出多階的網域名稱來消耗伺服器的運算資源，進而達到阻斷服務式之目的。

緩解方式與 Keystrap 類似，將相關運算移至單獨的執行序並進行限制並設定嘗試上限等。

(5) Verisign's Transition to Elliptic Curve DNSSEC

Verisign 分享轉換 DNSSEC 演算法之經驗分享，包含如何進行準備、時程之考量、錯誤之考量與現有排程說明等。

A. 截斷（Truncation）問題

針對因解析錯誤發生，而採用雙重簽章機制，導致回應長度過長，而產生截斷問題進行分享。

B. 轉換 EDU 網域之流量觀察

在演算法更新過程中起始時前後時間點觀測到大量流量，隨後發現只是第三方的 DDoS 攻擊。且發現比預期更多的 UDP 與 NXDOMAIN 之發生。

C. 轉換 NET 網域之流量觀察

NET 網域轉換後與 EDU 特徵相同，但規模更大且有更多的 UDP 截斷發生。

D. 轉換 COM 網域之流量觀察

情況與 EDU 及 NET 相同，此外所有的 UDP 與 NXDOMAIN 皆發生截斷，這結果比預期還高。

E. 執行總結

- TCP 流量如預期增加
- UDP 截斷增加則超出預期
- 部份伺服器在處理 NXDOMAIN 時遇到困難
- 沒有發現用戶端解析失敗的狀況

3. 場次三

(1) DNSSEC, DANE & RPKI Deployments Around the World

講者分享各區域 DNSSEC 相關佈署情況，歐洲與南美洲佈署密集度很高而北美洲稍微低一些，密度最低的地方則是非洲和亞洲。

從 DNSSEC 的整體結構來看可以發現在二階域中 DNSSEC 執行率很高，但之後就隨著階層的增加而減少。即便如此依舊可以觀察到近年來佈署情況不斷增長，尤其是在 COVID-19 疫情期間開始加速。

此外 DNSSEC 在電子郵件部份已是一個成功的案例，根據最新數據有超過 40% 的電子郵件服務提供商正在進行 DNSSEC 驗證。MX 與 DANE 記錄已開始快速增長。

全球 RPKI 佈署情況不受保護的 IPv4 前綴數量正逐漸接近有效路由來源授權(ROA)之數量，無效數據的數量則有所下降。

總結來說這些都是網際網路公共識別空間保護方面的成功案例。

(2) DNSSEC “event” measurement

講者分享規劃中的 DNSSEC 事件量測方法，該方法屬於早期階段而非完成狀態，其目的是了解 DNSSEC 中斷時實際發生什麼事情，研究問題分為三個方面，包括什麼是真正的 DNSSEC 中斷、

檢測中斷的方法及如何確認結果。

A. DNSSEC 中斷的定義

DNSSEC 中斷是指若點到點的 DNS 解析和處理路徑上啟用了 DNSSEC 的情況下發生故障便屬於 DNSSEC 中斷。相關的中斷不僅僅是驗證失敗，還包含系統或軟體組件導致的解析差異。

B. 檢測中斷的方法

目前以檢測資源紀錄數位簽章（Resource Records digital Signatures，RRSIG）過期作為範例，透過資料庫操作搜尋所有最後線上時間大於到期時間之紀錄。講者分享相關近期數據後表示相關議題還有許多問題帶解決後結束。

(3) The Road ahead: Integrating Competing Namespace Mapping Systems

傳統的 DNS 系統在分配網域名稱時遵循的是最終一致性原則(Eventually Consistency)。每個域名只會指向單一內容持有者，即便這個獲取過程可能存在延遲。

近年來隨著其他獨立的網域名稱解析系統興起，讓使用們可以獨立將域名映射到不同的內容。

A. 區塊鏈命名系統 （BNS）

區塊鏈命名系統（BNS）號稱提供「真正去中心化」的域名解析系統，滿足 Zooko's Triangle 之特性：

- 人類可理解性：提供有意義且易於記憶的網域名稱給使用者。
- 安全性：惡意實體能造成的破壞應盡可能降低。
- 去中心化：域名解析過程無需中央伺服器。

此時產生了一個問題，那就是 DNS 和 BNS 系統的資源持有

者應該永遠一致嗎？或者說如果資源持有者在兩個不同系統中相同，對應的內容是否應該完全分開？

B. 延伸之問題與討論

講者透過範例的方式討論不同的解析系統間須考量的問題，如下：

- 名稱分配和內容解析的一致性：在不同的域名解析系統中，同一個名稱是否應對應到相同的資源持有者與相同的內容，以確保一致性。
- 解析優先順序：當在不同的名稱映射系統中存在相同名稱但不同內容時，是否需要考慮解析這些名稱時應該遵循一定的優先順序以確保用戶獲得一致的結果。
- 系統間的同步性：當同一個名稱在不同的系統中可能被不同的人擁有時，需要思考如何確保跨系統之間的資源分配和域名解析保持同步以避免出現混亂或衝突。

透過上述分享，講者表示研究處於初步階段，此時正在結構化相關評估與研究，並徵求意見和合作夥伴。

(4) SAC123: SSAC Report on the Evolution of Internet Name Resolution

針對 SAC123 進行報告，該報告主題在網路名稱解析之進化。

A. 網路名稱解析的更多應用

人們希望找出網路名稱解析更多的延伸應用，主要原因如下：

- 已建立的用戶熟悉度：使用者以習慣網域名稱格式，使用者容易識別和記住網站地址。

- 兼容性需求：通過遵循 DNS 格式語法，替代命名系統可以在其應用程式中與傳統 DNS 共同運行。

B. 變更現有網路名稱解析機制

此外，也有許多動機希望能改變現有的網路名稱解析機制，如提高解析速度、隱私權考量、強化身份驗證、去中心化管理、不受審查制度所影響等。

C. 總結

講者指出了隨著替代名稱解析系統的興起，名稱解析的內容變得越來越重要，同時也帶來了混淆的問題。新興趨勢包括基於查詢的解析，根據用戶位置等因素提供不同的功能或 IP 地址。

現今的名稱解析系統使得解析名稱時的內容和結果變得不明顯可能導致誤用或混淆。IETF 和 ICANN 提出了新的頂級域和命名空間，如.alt 和.internal 目的在解決名稱解析系統中的問題。

五、RSSAC 相關議程

本場次以 RSSAC 的角度，討論政府和潛在法規的可能影響。

(一) 安全事件和報告工作小組

- RSSAC058 A.1.1.1 規定根伺服器系統治理結構（RSS GS）必須包括網路事件監督和揭露義務的規定，並將根伺服器營運方（Root Server Operator，RSO）和 RSS GS 之間的安全威脅和漏洞資訊共享入法，RSSAC 安全事件報告工作小組向 RSS GS 提供更正式的建議，通知影響根伺服器系統的有效安全威脅。
- RSSAC 在研究安全事件報告[12]，向網際網路名稱及號碼指配機構（ICANN）董事會以及更廣泛的網路社群提出的建議，透過透明和揭露來增強對根服務系統的信任的方法與公眾相關的安全事件。RSO 曾非正式地發布有關安全威脅和事件的資訊。本文件的目的是推薦一種更正式的資訊傳播流程。
- 有關前項安全報告的保密性和日誌匿名化（4.4 保密性），討論 IP 位址被視為個人識別資訊（PII），因此包含 IP 位址並將其與查詢域名相關聯的封包擷取和日誌檔案應被視為機密。未經授權暴露非匿名 DNS 查詢日誌或資料包捕獲及未經授權洩露企業營運安全所需的機密資訊應報告 RSO。

(二) DNS 根伺服器系統

世界各地有許多組織關注涉及網路治理之立法及監管。RSSAC 主席想向非技術者解釋「我們在做什麼」，透由介紹 DNS 根伺服器系統，讓非技術專家的 ICANN79 新人需要瞭解 DNS 的工作原理、根伺服器系統在其中扮演的角色，並瞭解根伺服器系統的相對重要性，以便他們能做出正確的決定。

---

[12] https://docs.google.com/document/d/1NvSw7PoLGYhXPuMEjiBgqjCtp_khTGGEh0DaHkNJdds/edit

(三) 域名衝突分析專案（NCAP）

域名衝突分析專案（Name Collision Analysis Project，NCAP）[13]旨在瞭解大多數域名衝突的根本原因，研究提出域域名衝突風險評估框架，以保護 DNS 免受域名衝突造成的潛在破壞。

1. 風險評估架構的主要特點

- 綜合風險評估：將域名衝突評估加入新通用頂級域名（New gTLD）字串申請審核流程。
- 技術審核團隊（TRT）：引進專門團隊進行評估，基於實證分析提出 gTLD 字串。
- 增強資料蒐集：鼓勵收蒐額外的定量資料以及來自公開資料集的定性資料，以進行更全面的風險評估。
- 多種評估方法：提供四種蒐集分析方法評估風險的資料。

2. 建議域名衝突風險評估架構的目標

目標 1 在確保可以評估域名衝突，對潛在域名衝突進行實證分析需要根區授權。目標 2 則為 ICANN 提供評估已識別域名衝突的緩解和補救計畫的流程。

3. 建議域名衝突風險評估架構中的初始工作流程。

4. 技術審查團隊評估字串的工作流程，表示取消臨時授權的緊急變更流程，NCAP 建議如果評估流程會對網路服務造成不可接受的風險，則建立取消臨時授權的流程。在定義緊急變更流程時可能需要諮詢

[13] https://community.icann.org/display/NCAP

RSSAC。

5. 更新的域名碰撞評估方法

NCAP 建議開發並實施評估潛在域名衝突的改進方法，納入根伺服器以外的資料以進行更全面的評估。可能需要 RSO 參與來提供來自根伺服器的資料以支援改進的域名衝突評估。

六、其他議題

(一) 國際化域名 EPDP 工作會議

本會議為國際化域名加速版政策制定流程（EPDP - IDN）工作會議，本場討論聚焦於 gTLD 註冊管理機構管理的第二層域名（second-level domain，SLD）國際化域名（Internationalized Domain Name，IDN）異體字參照表（IDN variant table）之間的協調（harmonization），防止使用部分相同字母的不同文本之間，因使用的 IDN 異體字參照表不同，而出現域名指向錯誤或無法解析的問題。

與頂級域名（Top-level Domain，TLD）必須參照 ICANN 發布之根區標籤生成規則（Root Zone Label Generation Rules，RZ-LGR）不同，註冊管理機構有權決定如何管理轄下 SLD，包括制定 SLD 的 IDN 異體字參照表。

ICANN Org 也有發布第二層域名標籤生成規則（Label Generation Rules，LGR）[14]，乃參照根區標籤生成規則（Root Zone Lable Generation Rules，RZ-LGR）訂定。但誠如前述，註冊管理機構有權訂定自己的 SLD 參照表，所以 ICANN 版本也稱為「參考用 LGR」（Reference LGRs）。

IDN EPDP 第二階段目前已幾乎完成研議，僅剩「SLD IDN 異體字參照表之間的協調」的議題，在工作小組內始終無法達成共識。

此議題主要癥結在於 ICANN Org 希望強制要求 gTLD 註冊管理機構使用「參考用 LGR」訂定轄下 SLD 的 IDN 異體字參照表，但代表 gTLD 註冊管理機構的團體（Registry Stakeholder Group，RySG）認為此要求超出 ICANN 政策規定範圍，主張註冊管理機構管理轄下 SLD 的自主權。

[14] https://www.icann.org/resources/pages/second-level-lgr-2015-06-21-en

RySG 同意必須達成「協調」的結果，但強調註冊管理機構有權自行決定如何達成此結果，反對強制規定註冊管理機構遵循既定規則以確保「協調」。

雙方立場實際上並沒有根本性的差異，僅需更多時間討論以琢磨出工作小組全員皆同意的具體文字。惟本次工作會議僅 60 分鐘，難以在時限內解決此問題。主席因此要求 RySG 與 ICANN Org 代表私下協商後提出建議文字，供小組討論定案。

(二) CPH DNS 濫用：社群推廣

首先由受理註冊機構團體（Registrar Stakeholder Group，RrSG）代表 Reg Levy 簡報註冊管理機構協議及驗證受理註冊機構協議的 DNS 濫用相關條款修訂進度。自合約方（gTLD 註冊管理機構與受理註冊機構）於 2022 年底向 ICANN Org 提出修訂合約協商要求，至 2023 年底修正條款提案由合約方表決通過，預計今（2024）年 4 月 5 日修訂後條款便將實行生效。

Levy 表示，整個流程在約一年之內完成，展現合約方重視 DNS 濫用、積極因應社群回饋的強烈決心。他也強調，修訂後條款是「基本條件」，並非「最高規格」。接下來必須花上一段時間積極蒐集資料，觀察合約執行成效，方能決定下一步。

本場次邀請多位利害關係團體代表，包括非商業利害關係團體（Noncommercial Stakeholder Group，NCSG）代表 Farzaneh Badiei、RySG 代表 Dennis Tan、智財權團體（Intellectual Property Constituency，IPC）代表 John McElwaine、企業團體（Business Constituency，BC）代表 Mason Cole，以及 GAC 代表 Susan Chalmers。除社群成員，ICANN Org 履約執行部門資深主任 Leticia Castillo 亦受邀請參與座談。

主席首先請 Castillo 說明修訂條款上路後，ICANN Org 的履約執行規劃。Castillo 分享，ICANN Org 內部相關工作主要分成 3 個面向：團隊能力建構、網路表格更新，以及投訴案件處理系統。首先，更新內部資料和教育課程，培訓職員了解新規定及執行規範。其次，更新網路表格以容許使用者針對違反新 DNS 濫用條款或潛在濫用情形，向 ICANN Org 提出投訴。最後，則是更新內部案件處理系統，以搜集製作履約執行報告需要的資料。未來 ICANN Org 將以每 12 個月的間隔發布 DNS 濫用履約執行報告。

若干 gTLD 受理註冊機構不約而同指出，新條款上路後，ICANN 收到的投訴無論在數量或內容上都將與過往大相徑庭。以前最常使用投訴系統的頂多是域名註冊人，之後任何人都可能利用 ICANN Org 的投訴系統通報 DNS 濫用，或針對特定受理註冊機構的 DNS 濫用處置提出投訴。他們希望 ICANN Org 已對此做好準備，未來在篩選資料、製作報告時，也應為呈現資料提供更多脈絡化的說明。

主席請社群代表分享，修訂條款上路後，最希望看到的改善情形。

NCSG 代表 Farzaneh Badiei 強調，不能以收到的投訴或結案的投訴數量作為修訂後條款是否成功的指標。成功指標必須仰賴質化資料，若僅著眼數量，最壞的情況可能導致濫權執法、危害人權等風險。她也強調未來 DNS 濫用相關條款的履約執行必須謹守技術分界，不得涉入管制網頁服務或網站內容。

IPC 代表 John McElwaine 認為最重要的是有效的雙向溝通，尤其必須確保投訴方和合約方對合約條款中「可採取行動的證據」的理解一致。BC 代表 Mason Cole 則提出 3 點，分別是有意義的量測指標，以及能指向進一步改善行動，如大規模對應 DNS 濫用的新政策制定流程，最後則

是有效的履約執行。

GAC 代表 Susan Chalmers 介紹 GAC 內 DNS 濫用的議題負責人，分別是她自己、歐盟代表 Martina Barbero 和日本代表 Nobuo Shigata，並解釋自己在此分享的是 GAC 集體觀點，而非個人立場。修訂條款上市後，GAC 最希望看到的就是 DNS 濫用數量顯著下降。另一方面，GAC 也將持續於 2024 年在可著手之處推動 DNS 濫用情形的進一步改善，並重申下一回合 New gTLD 開放前，必須見證 DNS 濫用明顯改善的立場。

(三) New gTLD 未來回合：字串相似性審核規劃

本場次主要介紹未來 New gTLD 申請的字串相似性指南草案[15]，並徵詢社群意見。指南主要描述申請字串視覺相似性問題，內含也涵蓋 GNSO 的 IDN EPDP 第 1 階段結案報告內容，以及申請字串對於其他申請字串、已授權 TLD 字串、 保留字或異體字的審核詳細資訊。後續 ICANN Org 將根據字串相似性審核指南，確認後續執行所需的開發工作；因目前 ICANN 董事會尚未審議 IDN EPDP 第一階段報告，預定在董事會審議後，ICANN Org 再更新與發布指南，並再針對最後版本開放公眾意見徵詢。

ICANN Org 的 Sarmad Hussain（Senior Director, IDN and UA Programs, ICANN Org）介紹，字串相似性指南草案是為了提供決定相似性的考量因素。由於相似性審查須考量的因素非常廣泛，指南提議採取兩階段審查，第一階段以機器預先過濾，第二階段再進入人工審查。

接續由指南草案主要撰稿者 Michel Suignard 說明指南內容。

Suignard 依指南章節依序說明，首先從混淆性（Confusability）、相

[15] https://itp.cdn.icann.org/en/files/strategic-initiatives/string-similarity-review-guidelines-07-02-2024-en.pdf

似性（Similarity）及異體字（Variant）等基本觀念開始。他解釋，「混淆性」是指即使兩個標籤互換，使用者也不會察覺；易混淆（Confusable）則指兩個標籤彼此混淆的程度，超過某個事先定義的門檻。在指南中，此門檻是根區標籤生成規則（Root Zone Label Generation Rules，RZ-LGR）。

字串相似性（String Similarity）則是因為外觀或視覺相似，導致兩個標籤之間混淆。Suignard 也強調相似性通常在根區並不常見，且會隨著使用者介面的字型而發生改變；這也是相似字和異體字之間的最大差異。例如西里爾字母小寫 i 標準寫法  與任何的拉丁字母都不同，但當以斜體字呈現時會變成  ，看起來像小寫的拉丁字母 u。事實上，在拉丁字母 RZ-LGR 中，已將此排除為異體字，不過在某些情況下，有可能讓視覺相似的標籤成為一體。

異體字中，大多數會認為異體字標籤實際上是相同的，且不限於視覺相似性，可能發生在跨文字（script）情況，可根據視覺外觀，也可以根據意義或語義以及發音來判斷。最典型的案例是簡體與繁體中文。

Suignard 接續說明字串相似性審核考量的不同因素，例如編碼位置（code points）的相似性類型、大小寫對混淆性的影響、易混淆序列（Confusable Sequences）、文字相似性等。在流程部分，他提到因為不同因素的組合過多且無窮盡，未來將採取兩步驟程序：首先利用機器篩選需進一步確認的標籤；第二步驟再由專家小組來做出最後決定。

字串審查的結果主要是「通過」（代表不會造成混淆）、「不通過」，或「有爭議」（代表該標籤僅與另一個申請的標籤混淆，需要進一步處理與解決）。未來預期審查小組至少配置 3 名審查委員，這些人員須熟悉語言文字且對 DNS 有基本理解；所有審查過程必須留下紀錄，並說明最終

決策的原因與依據。

有與會者提問如何在 New gTLD 開放前這麼短的時間內就訂出相似性程度的給分標準，因為過往拉丁文字生成小組（Latin Generation panel）曾為決定是否為異體字時就花了約五年時間；Suignard 回應將會利用先前專家們的研究成果，不會從零開始。

另有與會者提醒目前指南並未考量「下底線」議題，大部分的網頁瀏覽器、文件處理軟體在呈現網址時會自動加入下底線，此可能會對例如拉丁文字 o 也有加上底線的符號產生混淆。Suignard 回應對於加入下底線沒有異議；但他也提到目前指南中也未納入單數與複數的棘手課題。

來自於 Google Registry 的與會者也提醒單複數的混淆性問題，他認為非英語系國家用戶因為其使用的文字並無單複數差異，而不會認知到單複數的差異，此便容易產生風險。另外他也提出不同語言相同單字拚法的問題，例如英式 colour 與美式 color 兩個同意字若同時被授權，也可能造成混淆，他詢問是否此也算是字串相似性要處理課題。Suignard 回應 colour 與 color 的例子還有數百萬種可能，而字串相似性審查指南沒有辦法包含全部情境，因此在機制中除利用既有準則進行預先篩選外，最後還會有專家小組判斷的步驟。

(四) SubPro 補充建議：社群諮詢

本場次目的為說明 GNSO 理事會成立的衍伸小組（Small Team Plus），針對 ICANN 董事會未通過的 SubPro 政策建議，討論修訂後提出的補充建議（Supplemental Recommendations），並向社群徵詢意見。首先由小組主席 Paul McGrady 簡介工作進展及 6 個未通過議題（包括主題 9、17、18、22、24 及 32）內涵，再接受社群提問。

McGrady 首先說明衍伸小組成立背景及工作進度，表示希望在 4 月

的 GNSO 理事會審議 SubPro 補充建議。接續逐項說明每個未通過議題，以及延伸小組的相應補充建議重點。

主題 9 註冊管理機構自願性承諾（RVCs）／公共利益承諾（PICs）議題方面，董事會主要擔憂若允許申請人可豁免有關 RVC／PIC 的規定（合約規範 11 (3)(a) 和 (3)(b)），會導致無法處理單一註冊人情境中（亦即品牌 TLD）的第二層域名（SLD）註冊濫用行為。補充建議中調整此豁免為須申請取得（原本是自動生效），而取得豁免的條件是，所有註冊域名均由註冊管理機構或其附屬註冊機構註冊或控制，且註冊管理機構也會採取有效措施識別與緩減 DNS 濫用活動。

主題 17 則關於申請人支援。董事會主要針對「ICANN 應考慮提供符合資格的申請人申請費以外支援」的建議，擔心若無劃定支援界線，可能衍生財務問題。延伸小組的期待是盡量爭取越多申請人支援越好，因此並未就此把建議改成僅減免或減少申請費。針對董事會所擔憂部分，小組因應修正是將原本建議中提到「申請書撰寫費」、「律師費」等具體用字，以更廣泛的用字（一系列對能力建構、規劃、申請、評估、授權前和授權後等階段有用的資源）取代。

主題 24 是有關字串相似性，董事會主要關注 2 項議題，其一是 ICANN 應在 TLD 授權後審查「預期用途」（intended use），而此檢查內容超出 ICANN 使命範圍；其二則是字串相似性的檢查擴展到視覺相似性以外的檢查，包括單複數。對此，小組建議刪除有關預期用途的文字，並增加額外建議：當申請案屬於「品牌」類型時，保留同時申請單複數字串的可能；針對字串混淆相似性的檢查，則加入字典以外的其他公認語言來源。

主題 18 是關於條款與條件，包含 2 個子議題。其中之一是，SubPro

原本建議 ICANN 只有在符合《申請人指南（AGB）》或特定法律要求條件下，才能拒絕申請案。ICANN 董事會認為此建議不當地限制 ICANN 拒絕申請案的自由裁量權。小組的調整建議將原本拒絕申請案須敘明理由，改成 ICANN 拒絕申請案時須說明理由。

另一個董事會關心的子題是，不滿意的申請人或異議者可據此政策建議主張「不起訴協議」無效。延伸小組因此建議取消「不起訴協議」和具體提及挑戰和上訴機制的相關文字。

主題 32 是有關有限度的挑戰／上訴機制，董事會對此的主要擔憂是，目前並無法確定是否可在不造成過多、不必要成本或延誤等結果之前提下，設計出一個由 ICANN 或第三方供應商所提供，針對申請案初始或進階評估決定提出挑戰／上訴的機制。延伸小組因此建議著重於挑戰方（而非挑戰／上訴機制可行性），僅允許提出一次挑戰，且不允許不斷挑戰。

肆、心得與建議

一、持續協助我國相關民間組織擴大參與 ICANN 事務，以提升我國能見度

我民間機構代表積極出任 ICANN 其他主要社群要職，並於相關會議分享我國專業網路技術經驗，頗獲 ICANN 及其他 GAC 會員重視。且 TWNIC 向於 ICANN 會議期間舉辦晚宴洽邀 ICANN 高層及各國公私部門代表等出席，係我團與會期間重要交流活動之一。民間參與對我國在 ICANN 影響力允具重要性。建議持續協助我國相關民間組織擴大參與 ICANN 事務，以提升我國能見度及拓展友我人脈，並展現我國可為國際網路政策及技術發展作出貢獻，增進各國對我在 ICANN 參與之認同感。

二、New gTLD 未來回合討論進展

數位主權概念在近年網際網路及數位科技快速發展下日益重要，且受各國高度關注，網路域名除具備主權識別之意涵外，亦涉及重大商業利益及防範遭受濫用之資安範疇，我國允宜提早布局。目前我國 GAC 成員 TWNIC 國際事務委員會曾委員更瑩擔任 GAC 新通用級域名議題領袖，有助我掌握相關政策發展及擴大話語權。

三、DNS 濫用

打詐、防詐已成世界各國政府施政重點之一，數位發展部去（2023）年已推出 111 簡訊平臺，透過認驗證發送方，確保簡訊發送端無誤；未來 NCC 也將與金管會等單位合作，提供商用短碼簡訊。

又針對濫發商業電子郵件防治一事，數位發展部業以資安情資分享方式提供給相關 ISP 業者，並透過 TWCERT/CC、N-ISAC 與國內、外分享情資，透過跨域整合聯防，共同防治。為加強防詐作為，應持續觀察國際間網

路詐騙手法的趨勢，針對新型態手法預為因應，同時借鏡他國作法，或是與他國交流我國經驗。

參考國際間對 DNS 濫用或資安事件的量測方法及觀點的轉變，同時了解相關利益方（或業者）的實務考量與可能負擔，讓我國相關工作能更加細緻有效。

四、Tech Day

這次的 Tech Day 不僅僅聚焦於傳統的 DNS 技術，還特別強調了網路身份認證與內容驗證的重要性。隨著數位化的普及和生成式 AI 的發展，對於這些需求的重視將會日益增加。這提醒我們在數位世界中，確保身份的真實性和內容的可信度至關重要，而技術的發展和應用將在這個領域發揮關鍵作用。

圖 5 我國代表團合影

伍、附件

1. ICANN 79 波多黎各聖胡安會議議程
2. GAC ICANN 79 會議議程
3. GAC ICANN 79 會議公報