ICANN 工作小組電子報

February 20, 2022

財團法人中華民國國家資訊基本建設產業發展協進會
National Information Infrastructure Enterprise Promotion Association

目錄

重要議題

ICANN 發布 SSAD 實施評估結果

通用頂級域名註冊資料臨時條款加速版政策發展流程（Expedited Policy Development Process on the Temporary Specification for gTLD Registration Data，簡稱 EPDP）第二階段於 2020 年 7 月發布結案報告，內容主要針對標準化存取/揭露系統（System for Standardized Access/Disclosure，SSAD）提出政策建議。同年 9 月，GNSO 理事會決議通過 EPDP 第二階段結案報告，提交 ICANN 董事會並開放徵詢公眾意見。

2021 年 3 月 25 日，ICANN 董事會指示 ICANN ORG 就 EPDP 第二階段結案報告中的 SSAD 相關建議，啟動實施評估流程（Operational Design Phase，ODP），分析潛在風險、預期開銷、資源需求、時程規劃、外在因素、全球公共利益及其他考量，供董事會決議時參考。SSAD 的 ODP 已於今（2022）年初結束，並於 1 月 25 日發布實施評估結果（Operational Design Assessment，ODA）。

SSAD ODA 報告中將評估結果分成 12 大項。以下簡要介紹各大項的重點發現：

1	執行準備	本項描述提出資料要求的一方（Requestor，以下稱要求方）應如何於 SSAD 中驗證（verify）並獲得認證（accredited），並列出相關法律考量及風險。簡要而言，ICANN ORG 會將非政府機關代表的身分驗證外包予一個集中化管理的認證單位（Central Accreditation Authority，Central AA）；代表政府單位的 SSAD 使用者，則將由各國內指定的認證主管機關（Accreditation Authority，AA）、經各國自行設計的認證流程取得資格。
2	時程	ICANN ORG 預估 SSAD 的建立及實施總共需耗時五到六年。
3	SSAD 運作	認證單位（AA）將是 SSAD 要求方與 SSAD 系統的唯一對口。AA 會將收到的資料要求轉給全自動化的中央閘道（Central Gateway），由後者轉給相應合約方[1]（Contracted Party，CP）審核並決定是否核准此要求。一旦資料要求經核准，原要求方可透過合約方提供的註冊資料存取協定（Registration Data Access Protocol，RDAP）服務，查詢要求的資料內容。

[1] 註冊管理機構與受理註冊機構。

4	必要系統及工具	為執行 SSAD，必須建立兩套系統：一是包含使用介面網頁和 API，供要求方提出資料要求的「集中化 AA 系統」。二則是「中央化閘道系統」，此系統亦須設置使用介面和 API，供合約方、認證單位、SSAD 濫用監察員及負責管理資料要求的管理人員使用。ICANN 建議兩套系統都外包。
5	廠商及第三方	ICANN ORG 目前列出 7 項須外包予廠商執行的 SSAD 功能：中央化閘道管理、集中化 AA、獨立稽核、SSAD 濫用監察、系統研發、客服，以及推廣宣傳的公關服務。
6	資源及人力	雖然 ICANN ORG 建議將大部分的 SSAD 的研發和執行工作外包，ICANN ORG 仍須為此工作花費大量時間及人力。
7	成本	SSAD 的研發執行成本預估為 2,000 至 2,700 萬美元，開始運作後預估的年度執行成本為 1,400 萬美元至 1 億 600 萬美元。
8	費用	ICANN ORG 建議收取 3 項費用：身分驗證/認證、要求方關係驗證，以及揭露要求。收費目的是回收 SSAD 的研發執行成本，ICANN 預估 SSAD 運作至少 5 年後才能完全回收成本。
9	風險	根據 ICANN ORG 分析，SSAD 與 ICANN 章程或任何現行政策之間並無衝突。但 SSAD 的研發建置仍可能出現諸如運作不敷成本、衍生的法規問題或訴訟糾紛等風險。除此之外，任何大規模、名氣高的系統都更容易成為網路犯罪的目標，SSAD 也不例外。
10	全球公共利益框架	根據 ICANN ORG 的分析，EPDP 第二階段的建議符合公共利益。
11	履約執行	經分析，ICANN 履約部門在 SSAD 運作中，主要責任將會是調查要求方或資料所有人就合約方處置提出的投訴。
12	稽核	SSAD 完全運作前應執行 1 次稽核，運作後 1 至 2 年內，稽核員也應持續監控確認是否有不符規定或特殊事件。

董事會和 GNSO 理事會將持續討論 SSAD 建議相關議題，董事會亦將開始研議下一步。

最新消息

董事長部落格：1 月董事例行工作會議精華回顧

ICANN 董事會於今（2022）年 1 月 13 至 16 日舉行今年首次董事會例行工作會議。依慣例，董事長 Maarten Botterman 撰寫部落格文章，與社群分享會議重點。

會議第一天聚焦於戰略規劃。首先由董事會內各委員會主席分享關鍵議題，並檢視相關準備工作進度。接著，董事會對照上述議題與戰略計畫，討論是否需調整不同議題及工作的優先順序，依此訂定董事會今年的工作計畫。

第二天，董事會首先檢視 ICANN72 的 GAC 公報，研議如何回覆公報內容。第二個議程聚焦於新通用頂級域名未來政策（gTLD Subsequent Procedure，SubPro）ODP 進展，最後董事會回顧並確認前一天訂定的工作計畫。

15 日第三天的首場議程，是檢視 GNSO 審核所有 gTLD 權利保護機制（Review of all Right Protection Mechanisms in all gTLDs，簡稱 RPM）政策發展流程（PDP）第一階段結案報告的 35 項建議。第二場議程則是安全、穩定及靈活性第二次審核（The second Security, Stability, and Resiliency Review，SSR2）及第三次當責及透明度審核（The third Accountability and Transparency Review Team，ATRT3）的進度更新。

除此之外，董事會也聽取 ICANN 財政年度 2023 至 2027 年（FY23 - 27）執行財政計畫及 FY23 執行計畫暨預算的草案報告。上述計畫已於去年 12 月公告並開放徵詢公眾意見，並於今年 2 月 7 日結束徵詢。

最後一天的董事會議由 SSAD ODP 近況報告揭開序幕，接續展開 2022 年首次正式董事會議。會議中的董事會決議可參考此處。除回應 ICANN72 GAC 公報和 RPM 第一階段結案報告決議外，董事會也就.WEB 的獨立審核流程（Independent Review Process，IRP）結果做出決議。

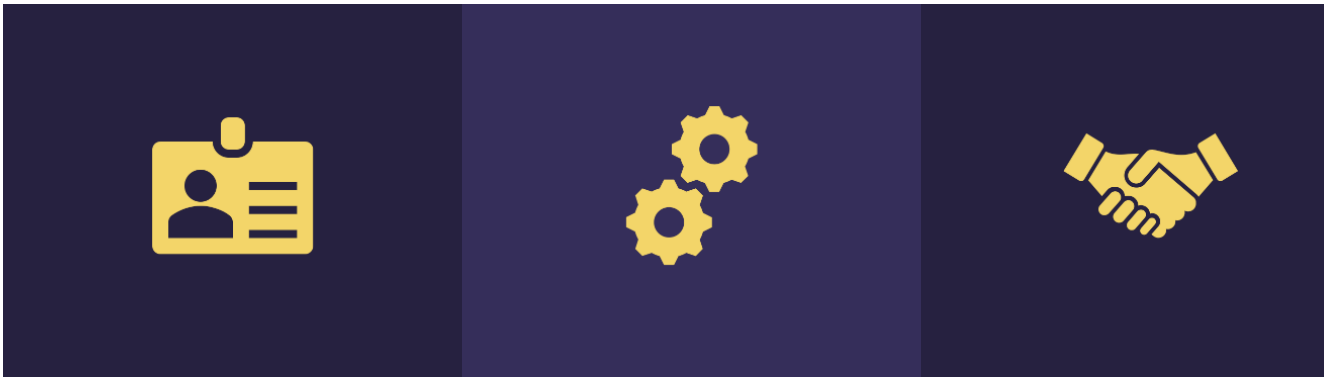
例行工作會議的尾聲，董事會依慣例回顧 4 天的工作會議，反思會議期間哪些議程和方式最有效率，未來又應如何改善會議規劃。相關董事會工作亦將於 ICANN73 會議持續推進。

文章最後，Botterman 強調，他了解大家都迫不及待想重返實體會議，但觀察全球疫情發展，ICANN73 實在難以混合模式舉行。他承諾即使遠端，董事會仍將致力確保高度互動交流，也感謝社群和 ORG 在此情況下，仍與董事會共同支持 ICANN 使命，期許 2022 年也成果豐碩。

ICANN 發行 RDAP 符合性檢驗工具

ICANN 今年 2 月發行新工具，供註冊管理機構及受理註冊機構確保提供的 RDAP 服務符合網際網路工程任務組（Internet Engineering Task Force，IETF）提出的實施要求，也提供選擇性符合 gTLD RDAP 設置檔的選項。

RDAP 是 IETF 建立的工具，此協定以改善後的標準化形式，傳送域名及號碼資源的註冊資料要求和回應。RDAP 還有很多 WHOIS 沒有的優點，包括支援國際化域名、存取資料安全性，以及容許差別化資料存取。



利用此新發行的 RDAP 符合性檢驗工具，使用者得以查詢域名、實體和域名伺服器的公開註冊資料，並檢驗這些資料是否符合以下文件列出的執行標準：

- RFC 7480
- RFC 7481
- RFC 9082
- RFC 9083
- RFC 7484
- RFC 8605

本工具也提供檢查是否符合 2019 年 2 月 gTLD RDAP 設置檔的選項。gTLD RDAP 設置檔乃基於 gTLD 註冊資料中繼政策要求，提供註冊管理機構和受理註冊機構相關技術指示，確保 RDAP 服務執行的一致性。

總計而言，RDAP 符合性檢驗工具會檢查 212 項業界 RDAP 標準，以及 74 項 gTLD RDAP 設置檔設定。檢查結果將生成報告，檢驗不符的項目會顯示錯誤代碼及內容敘述。更多細節可參考相關說明文件。

通用頂級域名申請政策實施評估流程：工作軌介紹

新通用頂級域名申請政策（SubPro）實施評估流程（ODP）於今年 1 月 3 日啟動，目的是提供分析及參考資料，協助董事會決議 SubPro 結案報告建議是否符合 ICANN 及社群的最佳利益。

SubPro 結案報告產出分為 41 項主題，內容從簡單到複雜的程度不一，涵蓋超過 300 條建議、實施指導原則及確認過去建議或實施做法。即使是最簡單的「維持 2012 年做法」，也必須調整以符合十年後現況。不僅如此，新的隱私保護法規、技術演進、物價上漲、ICANN ORG 的 2012 年教訓，以及結案報告建議的新標準和要求等，皆須逐一納入考量。

ICANN ORG 依功能及相關活動，重新分類 SubPro 結案報告的數百條產出，並依此規劃 ODP 工作。目前已整理出 9 條工作軌，簡介如下：

專案管理

所有專案管理事項，包括風險管理、假設事項、報告及任務標的。

政策發展及實施材料

支援政策實施、建立並更新申請流程、撰寫申請人指南等。

運作準備

聚焦於完善 ICANN ORG 準備度，包括建置支援後續流程的內部實施程序，以及升級現行實施做法以因應未來合約方數量成長。

系統及工具

重視安全、隱私保護及高組織效率之未來申請回合系統的研發、設計及執行。此項下亦包含建置後續維護及改善的相關流程。

“This is a high-level overview of what will be a deep, thorough, and complex endeavor.”

廠商

就特殊專長或其他專業能力招商簽約。此項下工作主要負責擬定廠商合作及合約規範。

傳播推廣

提供專案工作進展，與 ICANN 社群及其他讀者分享相關資訊。

資源、人力及物流管理

設定專案不同階段需要的資源和人力，並依規劃安排相關人力及資源。

財務

管理 SubPro 中涵蓋的所有財務工作，包括成本估算、費率計算、付款及退款流程，以及計畫相關預支請款等。

其他

監控其他不在結案報告中，但可能影響 SubPro 的現行社群或 ICANN ORG 工作，如國際化域名（Internationalized Domain Name，IDN）及域名衝突研究專案。

SubPro ODP 專案小組將於 ICANN73 期間與社群分享最新工作進度，在那之前若有任何其他疑問，也可參考本 ODP 專屬網頁，或寄信至 subpro-odp@icann.org（此信箱的所有信件往來都將公開庫存）。

公眾意見徵詢

域名衝突分析專案（NCAP）研究二文件

開始日期	2022 年 1 月 27 日	結束日期	2022 年 3 月 18 日
簡介	域名衝突分析專案（Name Collision Analysis Project，NCAP）研究二（Study 2）的目標，是了解 DNS 不同層級量測結果涵蓋的域名衝突，並了解域名衝突的影響。目前 NCAP 已完成兩份文件，希望募集社群的意見反饋。兩份文件分別為： • 不存在頂級域名之 DNS 查詢的前瞻性研究：本文件探究 DNS 域名衝突在 DNS 層級內的分布狀況，並提出關於如何、從何處搜集評估 DNS 資料的洞見。 • 域名衝突字串的案例研究：利用 A 和 J 根伺服器的 DNS 查詢資料，針對 .corp、.home、.mail、.internal、.lan 和.local 的案例研究。本研究強調 DNS 查詢內容隨時間演進產生的變化，以及 DNS 演進衍生的訊務改變。		
網頁連結	https://www.icann.org/en/public-comment/proceeding/name-collision-analysis-project-ncap-study-2-documents-27-01-2022		

ICANN 組織章程修訂：第 10 章及附錄 B 內容

開始日期	2022 年 1 月 21 日	結束日期	2022 年 3 月 2 日
簡介	國碼域名支援組織（Country Code Names Supporting Organization，ccNSO）提議調整 ICANN 組織章程第 10 章及附錄 B，此內容調整乃因應 ccNSO 第二次組織審核改善建議，特別是允許 IDN 國碼頂級域名管理方依自身意願成為 ccNSO 成員。調整內容包括 ccNSO 成員定義，以及同一國家有多名 ccTLD 管理方的投票資格。 ICANN 董事會收到 ccNSO 要求後，同意啟動組織章程第 25 章 25.1 節中訂定的組織章程修訂標準流程，依 25.1 節條文規定，在董事會同意修訂組織章程前，修訂提案應先公開並徵求公眾意見。		
網頁連結	https://www.icann.org/en/public-comment/proceeding/icann-bylaws-amendments-ccnso-proposed-changes-to-article-10-and-annex-b-21-01-2022		

文摘

APNIC：科技巨頭及電信業者使用 NAT 將阻礙網路創新

資料來源：The Register

內容摘要：

亞太網路資訊中心（Asia Pacific Network Information Centre，APNIC）首席科學家 Geoff Huston 今年 1 月於 APNIC 部落格發表長文〈2021 年 IP 位址〉，闡述 2021 年的 IPv4 及 IPv6 使用情形，並在結論指出電信商和科技巨頭不願更改使用 IPv4 搭配網路位址轉譯（Network Address Translation，NAT）技術的保守心態，是 IPv6 發展積弱不振的主因，也不利網際網路的未來發展。

2021 年間 IPv4 和 IPv6 使用情形的重點包括：雖然 IPv4 位址交易數量成長，但早已面臨耗盡的 IPv4 位址仍持續減少。另一方面，IPv6 部署率僅成長 3%，這也意味著沒有任何具影響力的企業在去年啟用 IPv6。Huston 指出，由於業者不願改變慣用的 NAT 技術，當代網際網路主要仍以 IPv4 為基礎。這是從上述統計數字看不出的事實。若進一步思考這對網際網路未來發展的意涵，前景並不光明。

「我們看到的，是一個不再以技術創新、開放和多元作為主要發展動力的產業。」Huston 寫道：「因為在 IPv4 中使用 NAT 的業界慣例，網際網路的技術基礎始終停留在僅使用傳輸控制協定（Transmission Control Protocol，TCP）和用戶資料報協定（User Datagram Protocol，UDP）、非常侷限的用戶端/伺服器互動模型。也因此，擁有充分通訊彈性的開放網路模式在今日網路已不復見。」

目前寡占市場的大企業，是導致現況的罪魁禍首。Huston 批評：「業者只想要保全規模和地位，大家都袖手旁觀 IPv4 轉移 IPv6 的漫長過程，創新和創業精神早已不受重視。」

去（2021）年 12 月 APNIC 和拉丁美洲網路資訊中心（Latin American Network Information Center，LANIC）共同發布的報告，也表達類似隱憂。報告指出，科技巨頭的自有網路負責全球巨量網路訊務，Google 和 Facebook 因此對全球網際網路架構握有驚人影響力。

Huston 文中亦延伸此議題，指出「無論是網路中立、切割電信網路和服務業者、對基礎建設的投資風險和回報評估，以及網路本身的開放程度，都嚴重受當代網路產業組成所左右。」

鑑於網路產業的經濟規模，要維持有效、完全開放且鼓勵競爭的環境本身已是個挑戰。隨著基礎架構中根本元素的 IP 位址面臨枯竭，這個挑戰因此更多重艱鉅。文章最後，Huston 提到，現在大家似乎都期待政府出手，透過法規框架限制巨頭企業的擴張，但他也不諱言，很難看出這種方式究竟是否會成功。

歐盟希望打造內建過濾機制的 DNS 基礎建設

資料來源：The Record
內容摘要：

歐盟有意打造自有的 DNS 服務，歐盟機構和一般民眾都可免費使用此名為 DNS4EU 的服務。目前 DNS4EU 仍在規劃階段，歐盟已公告招標，尋求打造此基礎建設的廠商。

歐盟官方代表指出，他們發現 DNS 市場集中於少數非歐洲營運方，這促使歐盟開始探索建立位於歐洲的中央化 DNS 服務的可能。招標公告中指出，目前全球 DNS 解析集中於少數企業，若任一主要供應商發生嚴重事故，DNS 解析過程將因此受到波及。DNS4EU 的建置就是為了因應這個問題。

諸如網路安全、資料保護等議題，也是歐盟決定打造 DNS4EU 的原因。

歐盟表示，DNS4EU 會內建過濾功能，阻擋不良域名（如惡意軟體、釣魚網站或其他網路安全威脅）的 DNS 解析。此過濾功能將仰賴可信的資訊來源，如歐盟各國電腦網路危機處理團隊（Computer Emergency Response Team，CERT），防護歐洲機關免於常見的惡意攻擊。目前尚不清楚是否將強制所有歐盟及歐洲國家政府單位使用 DNS4EU，若如此，則如歐盟 CERT 等大型組織將更有力量，也能提升偵測防制網路攻擊的機動力。

除此之外，歐盟官方也意圖利用 DNS4EU 的過濾系統，封鎖其他法院命令禁止的內容。雖然官方說明並未觸及細節，但一般猜測可能以兒童性暴力和盜版內容為主。

DNS4EU 將需要符合所有資料保護法律，如通用資料保護規則（General Data Protection Regulation，GDPR），確保域名解析的資料處理位於歐洲境內，並禁止任何個人資料的買賣營利行為。在技術細節上，DNS4EU 需支援所有當代 DNS 標準和技術，諸如域名安全擴充（DNS Security Extensions，DNSSEC）、DNS over TLS（DoT）、DNS over HTTPS（DoH），並適用 IPv6。

網路服務供應商 Open-Xchange 的政策創新主任 Vittorio Bertola 受訪時同意，DNS4EU 是數位主權戰略的重要一步。他認為除了 Google 和其他非歐洲業者主導的網路服務外，歐洲人的

確需要一個位於歐洲的免費公共解析服務。他也指出，鑑於最近《雲端法》（CLOUD act）和其他資料跨國傳輸的歐美判例，對許多歐盟企業，尤其是公家機關而言，為了遵守 GDPR，已益發難以使用科技巨頭提供的網路服務。

然而，DNS4EU 禁止利用使用者資料營利，且 DNS4EU 將導致其他歐洲網路營運業者的利潤降低，產業毫無推廣 DNS4EU 的誘因。也因此，DNS4EU 如何自立營運仍存疑。Bertola 更指出，全球解析器以不服從任何國家封鎖命令為原則（如不會因歐洲法院命令而封鎖 Pirate Bay 或 SciHub），事實上，很多使用者就是為了上非法網站而不用當地 ISP 服務，所以 DNS4EU 遲早仍須面對這個問題。

可以想見 DNS4EU 的招標案件將吸引許多廠商投標，然而未來 DNS4EU 到底將如何建設，又是否真能帶來歐盟期望的影響，則仍待後續觀察。