

2023

IP & DN

網路位址及網域名稱趨勢 電子報

2023年6月號

I
N
T
E
R
N
E
T
&
D
O
M
A
I
N
A
D
D
R
E
S
S

指導單位 | mod^a 數位發展部
Ministry of Digital Affairs

執行單位 | Nii 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

本期內容

2023年第二季的 ICANN 社群及域名市場熱鬧無比，首先是3月初由美國白宮發布的國家網路安全戰略，已敦促更多域名受理註冊機構積極採納安全措施，減少針對DNS攻擊的機會；Google在5月初將包括 .ZIP 在內的 8 個新頂級網域投入市場開放使用；ICANN的註冊資料查詢服務測試也即將展開。此外，本期電子報也介紹了6月中在華盛頓特區舉行的ICANN 77會議中對New gTLD專屬頂級網域的討論，並收錄由理律法律事務所曾更瑩律師撰稿之DNS濫用專欄文章。最後，本電子報也整理出4月「電信業者VS. 科技巨頭：網路建設由誰來買單？」座談重點，提供讀者閱覽。

目錄

IP&DN 全球重點新聞	2
ICANN77 會議回顧	4
「電信網路業者vs. 科技巨頭：網路建設該由誰買單？」座談會重點回顧	6
專欄文章：DNS Abuse — ICANN 將展新局	9

IP&DN全球重點新聞

📖 美國國家網路安全戰略的域名安全衝擊

📖 RDRS：所有受理註冊機構注意！

📖 .zip和.mov域名的安全風險

美國國家網路安全戰略的域名安全衝擊

美國政府於2023年3月發布[國家網路安全戰略](#)，其中加重對軟體開發業者與國內產業保護自家系統免於駭侵的責任要求；亦強化聯邦調查局與國防部打擊全球駭客及勒索軟體團體的力道。

這個改善美國整體網際網路安全並減少網路威脅的網路安全戰略，可能也將為域名安全帶來正面影響。如美國政府用來偵測、防治網路攻擊的新措施，可能也將間接減少針對域名及域名系統的攻擊。此戰略最起碼也能敦促其他受理註冊機構效仿更重視安全的大規模受理註冊機構，開始採納諸如「了解顧客」（Know Your Customer, KYC）、註冊管理機構鎖（registry lock）或DNS安全擴充（DNS Security Extensions, DNSSEC）等安全做法。

戰略中也談到網際網路和DNS作為基礎建設的重要，如連同戰略發布的白宮〈事實清單〉（White House Fact Sheet）指出：「降低網際網路及數位生態系統中的結構性技術弱點」是強化國家網路安全韌性的關鍵元素。

➡ [點此查閱](#)更多資訊

RDRS：所有受理註冊機構注意！

ICANN正在準備啟動註冊資料請求服務（Registration Data Request Service, RDRS），受理註冊機構利害關係團體鼓勵所有ICANN認證受理註冊機構參與。

RDRS是促進受理註冊機構的註冊資料處理要求符合資料保護法規的重要一步。為確保在保護註冊人個資的同時，具合法需求的第三方仍有辦法取得非公開的註冊資料，ICANN社群建議打造資料存取／揭露標準化系統（SSAD），而RDRS就是為建立SSAD搜集使用資料的試行專案。

受理註冊機構完全可自願選擇是否參與RDRS，但夠多的受理註冊機構參與，才能蒐集到充分資料，準確呈現域名產業內的真實資料請求情形。其他參與RDRS可能帶來的好處包括：標準化資料請求格式、更安全的通報管道、掌握資料請求者身分、搜集實際資料，以及最重要的，共同支持多方利害關係的政策制定治理模型。

➡ [點此查閱](#)更多資訊

.zip和.mov域名的安全風險

Google Registry今年5月初開放8筆new gTLD註冊，包括瞄準博士的.phd和教授的.prof，也有以爸爸為目標客群的.dad。但其中，引起各方關切，尤其許多網路安全專家憂慮的，是.zip和.mov。

.zip和.mov都是大家熟知、常見的檔案名稱。.zip常用於壓縮檔案，.mov則是Apple使用的影片格式。許多人擔心，惡意人士會利用這兩個TLD偽裝成檔案的網址，發動網路釣魚等數位詐騙攻擊。程式也可能因此更容易搞混檔案名稱與網址，擅自在檔案中加入超連結。

網路安全研究人員已經觀察到惡意行為者策略性購入.zip網址，用來測試發動釣魚攻擊。但也有意見指出，.zip和.mov並不像許多人聲稱的如此危險。現實中已有諸如代理伺服器或訊務管理工具等措施，足以防治上述可能風險。

➡ [點此查閱](#)更多資訊

ICANN 77會議回顧

ICANN77會議中，有多個場次討論 New gTLD 後續開放的相關課題，主要包括專屬通用域名（closed generic gTLDs）、申請人支援（Applicant Support），以及目前 New gTLD 實施進度的說明等。

而所謂的通用類型頂級網域，如大家最熟悉的 .com，是開放任何人採先到先贏的方式來註冊與使用的頂級網域；而所謂的「專屬通用域名」是指，該「通用」類型的頂級網域被其管理機構限制第二層域名註冊情況，例如 .book、.cloud、.disaster 等的通用字不對外開放註冊，僅由獲得授權的申請者專用。在2012年第一次開放 New gTLD 申請階段，其實並未著墨專屬通用類型域名的申請情況，也因此被認為是開放的，GNSO 也提出 ICANN 沒有權責限制申請人對於申請字串名稱使用方式的看法。但隨後代表政府的 GAC 提出建議，認為通用類型的字串名稱若要專用，則應當在符合公共利益的條件下。也因此，ICANN 董事會期望在下一回合開放 New gTLD 申請階段，勢必要把「專屬通用域名」申請的遊戲規則定義清楚，使申請人有所遵循。

惟在過去多年的政策討論階段，此議題一直沒有辦法在社群中達成共識。就在 ICANN 籌備開放 New gTLD 的實施階段之際，為使此議題有進展，ICANN 董事會也要求 GAC 和 GNSO 針對專屬通用域名的申請方式進行對話討論，過程中代表網路使用者的 ALAC 社群也加入討論，形成了由 GAC、GNSO 和 ALAC 代表所組成的促進對話小組。



[Photo by icannphotos on flickr](#)

該小組已就「專屬通用域名」擬出高層次之政策制定條件框架草案（並未涉及細節），作為後續啟動政策制定流程的依據；並在 ICANN77 期間辦理 2 個場次的公開會議，和社群說明框架重點並且尋求社群的回饋意見。若此框架未能順利確認下來，後續有關專屬通用域名的政策制定流程將無法啟動，而 ICANN 董事會也將需要決定在下一回合 New gTLD 開放收到專屬通用域名申請案的處理方式。

GAC在ICANN77期間也有 1 場針對專屬通用域名的討論，其中一個場次就「專屬通用域名框架草案」尋求GAC的意見與想法。在GAC代表提出的意見中，大致可歸納為，政府希望能建立一套可確保專屬通用域名符合公共利益的評估標準，不過政府對於目前不同利害關係人、國家或經濟體對於公共利益的意涵仍然形成共識表達深度的關切。另，為確保該公共利益，GAC在New gTLD 申請評估過程中也應當扮演一定的角色。另外，關於申請人在取得該專屬通用域名後卻無法實踐其承諾事項後的gTLD追回、專屬通用域名可能帶來潛在獨佔風險等問題，也應當在此框架中有所著墨。



公共利益應當是當前討論中最不容易處理的課題；在前述「促進對話小組」的腦力激盪過程中即有相當多對此主題的討論，包括到底公共利益應以全球為範圍，又或者僅需要針對某個特定社群即可？小組選擇了中間的立場，亦即同時允許廣泛性和針對性的公共利益，前提該專屬通用域名符合更廣泛的公共利益。此外，「促進對話小組」也依gTLD不同的生命週期階段，將框架草案內的具體內容區分申請期、評估期及授權後三個區塊，並在每個區塊中描述小組成員認為應該包含在內的標準。GAC所關心可能會造成壟斷的問題，在框架草案中，便併陳了2個選項：申請人必須要證明其在所屬產業或群體的「代表性」，或者申請人須透過合約來承諾不會作出反競爭行為。

專屬通用域名框架草案文件可按此[連結](#)查閱，有關框架草案的意見蒐集期限為7月15日。

「電信網路業者VS. 科技巨頭：網路建設該由誰買單？」座談會重點回顧

「公平分攤」網路建設成本並非嶄新議題，歐洲電信業者於2012年就於國際電信聯盟（ITU）會議遞出相同概念的「發送方付費」（Sending Party Pays）提案，但表決未獲通過。反倒是韓國率先於2020年12月實施俗稱Netflix law的法案，讓ISPs可向大型內容業者收取網路「穩定」費，惟法條文字模糊，Netflix和YouTube迄今仍拒絕付費。此外，美國 FCC 委員 Brendan Carr 去（2022）年9月也表示，美國的網路建設融資模式自1990年的撥接上網時代以來從未改變，而「現在是讓科技巨頭開始『公平分攤』的時刻了」。

以下為2023年4月份所辦理的網路建設成本公平分攤的座談重點，邀請數位部韌性司、台灣網路資訊中心（TWNIC）、台灣電信產業發展協會及 Google 代表，分別從不同利害關係人角度來闡述其觀點。

座談主持人 TWNIC 黃勝雄執行長在引言時提到網路運作關鍵元件之一的海纜，當從容量觀點來看，目前約有六成是由電信業者所提供，四成則是來自於內容業者，但近年平臺或內容業者已逐漸成為海纜與頻寬建設的最重要投資者。



他也提到歐洲的網路費提案源自於電信產業對歐盟監管機構施壓的結果，而內容巨頭 Netflix 對歐洲網路費提案則認為，內容業者在內容方面的投資才是推動電信業者商業模式的助力。黃博士認為，歐盟的提案恐怕會增加消費者成本，並使網路更不穩定，因為內容業者會試圖改變訊務的路由來避免額外成本的發生。

數位部鄭明宗司長認為，政府會認為網路基礎建設是數位國土之延伸，也因此由國內業者自行興建基礎設施為必要，且外資與本土投資比例會有所限制，最後一哩路的建設更是必要。也因此，他認為對網路基礎建設付費使用是值得深究的課題。他也點出目前的爭議點是，電信業者與內容業者對於基礎建設流通的訊務責任歸屬認知差異，前者認為是內容業者提供的服務導致訊務量大增，但內容業者卻認為訊務量增長源自於用戶的需求。此也造成雙邊認為應當由誰來對網路建設成本付費的不同價值觀。

鄭司長進一步說明，目前國際間對此並無統一規範或分攤機制，僅有大型 ISP 會與內容業者就如何分攤成本進行討論；而中小型 ISP 則無對應籌碼，如此一來可能會影響人民通訊傳播使用權利，並影響在地通訊產業發展。最後他提到，在數位應用服務、人工智慧、擴增實境、元宇宙持續發展下，網路用戶數及訊務量預期將持續攀升。為順應國際趨勢，呼應不同產業發展需求，有必要正視網路成本分攤議題。

台灣電信產業發展協會劉莉秋副秘書長則從另一個面向來談網路建設成本的分攤。他認為，國內電信業者努力推動寬頻服務與智慧型裝置普及，進而帶動了數位創新應用服務發展，但電信產業卻因數位經濟崛起導致營收逐年下滑。語音服務被取代、市場以資費為顯學的價格競爭及高管制強度，也讓電信業者缺少多元的營收來源。在肩負基礎設施建設的責任下，電信業者幾乎無法抵擋來自於數位平臺邊際成本趨近於零的運作模式。

劉副秘書長強調，相對於最接近用戶的內容服務業者，在網路建設投入最多、屬於特許行業的電信業者，對於造成社會成本的網路內容，反而要承擔最多的責任。他也認為，國內行動上網吃到飽上網費率是大型科技平臺業者服務得以成功的關鍵，也突顯出產業生態鏈結構失衡的問題。建立共榮生態圈，而非產業廝殺、適者生存的零和問題，這是在現行法制架構下，政府必須思考的本土產業結構問題。



Google 台灣政府事務及公共政策陳幼臻副總經理從數位平臺與電信業者在生態系統中的夥伴關係來探討此議題。他說明數位平臺與電信業者在生態網路系統中應該是夥伴關係，他闡述數位平臺促進了電信業者核心業務成長、提升網路傳輸的技術含量增進電信業者營運效能，以及為電信業者提供新的商機。

陳副總經理進一步引用第三方數據說明電信網路成本與網路流量成長並無直接相關性，並認為收取網路流量費將有損使用者權益；南韓立法允許電信業者收取網路流量費的做法，就已造成如網路品質下降、數位內容多樣性降低，以及數位平臺或內容業者退出南韓市場等負面效果。

➡ 點此觀看完整[活動影片](#)

專欄文章 | DNS Abuse — ICANN 將展新局

Ⓜ 作者：曾更瑩 | 理律法律事務所 合夥律師

DNS Abuse（域名濫用）一詞係在ICANN社群中，對於與域名有關的濫用行為之泛稱，其中囊括與資訊安全，網路攻擊有關的諸多行為。ICANN社群經過多次討論，將DNS Abuse定義為以下五種行為：malware, botnet, phishing, pharming, 以及spam (用以作為前述四種行為之媒介者)。在廣義的資訊安全一詞之下，DNS Abuse是諸多影響資訊安全的行為中，某些特定跟域名系統有關的濫用行為。

DNS Abuse之產生與防止，涉及域名生態系中各個扮演不同角色之成員；而DNS Abuse通常不止發生在參與ICANN的機構所能掌控的場域，也發生在其他ICANN社群以外的場域；例如某些域名濫用的情狀，也可能係發生在網站內容之層次。ICANN僅能對其社群發揮影響力與拘束力，對於在其他階層所發生的DNS Abuse無法直接處理，特別是針對網路內容層所發生的DNS Abuse，受限於ICANN By Laws之規定，採取消極的態度。然而，與域名有關的網路攻擊或其他資安事件不斷地發生，ICANN與社群受到強大的壓力，特別是來自政府部門以及執法單位之強力要求，必須提出更有效的處理方法。

今（2023）年5月24日，ICANN 與 TWNIC在臺灣合辦 Engagement Forum，大會舉行了一場由ICANN各社群發言與討論DNS Abuse議題的討論會。與會的講者分別從品牌保護、Registrar註冊服務、ICANN 管理者、國家CERT協力等角度，提出各自社群對於防止DNS Abuse的努力與未來期許。本次討論會中點出幾點重要的未來發展方向。

第一、ICANN預計在下半年推出Registration Data Request Service (RDRS) 的先遣實驗計劃。這是自2018年5月，ICANN原本的WHOIS 資料庫，因為被控違反GDPR而處於幾乎關閉的狀態以來，ICANN為解決各方利害關係人欲取得域名註冊人之資訊所踏出的第一步。ICANN並不強制，但鼓勵域名註冊商參與RDRS實驗計畫，希望透過實作儘快解決目前無法取得域名註冊個人的資料的僵局。預計系統上線以後，對於處理DNS Abuse時，需要取得域名註冊人的資料的部分，會有很大的幫助。

第二、ICANN的By-Law雖然表明ICANN的任務，不在處理網路內容層所發生的問題，也不管轄網路內容，但是ICANN也並不禁止，甚至鼓勵社群依照自身之需求，參與對於網路內容相關議題的處理。

第三、ICANN Contracted Parties House為進一步防止DNS Abuse，已經展開與Registrar/Registry之合約條款修正，在合約中要求註冊商應採取之最低標準。

以上Registrar/Registry之合約條款修正內容，ICANN已於今年五月底公布，且在六月舉行的ICANN77會議中，成為眾所矚目的焦點。依照ICANN所公布的修約草案條文，未來Registrar/Registry將有下列義務：

1. 建立DNS Abuse的聯繫Registrar/Registry管道，以便各界針對DNS Abuse能儘速向有關Registrar/Registry通報，Registrar/Registry在接到通報以後，應向通報人確認已收到通報。

2. 如果Registrar/Registry基於「得採取行動之證據（actionable evidence）」，「合理」地決定有DNS Abuse的情況，Registrar/Registry即有義務立即（promptly）對於發生濫用行為的網域名稱採取行動。

3. Registrar/Registry可以直接對於發生濫用之域名採取行動時，例如停止解析、禁止移轉域名註冊商等。但如採取直接手段將因此造成其他附隨的傷害（collateral damage），例如某個域名只有其中幾個網頁有濫用的情事，此時應改以通知網站所有人、經營者以下架網頁之方式為之。

ICANN正就以上合約修正草案公開徵求意見，如草案順利成為合約正式條文，將增加Registrar/Registry處理DNS Abuse的壓力與誘因，預計應可有效減少域名濫用，各界可以再關注合約未來修正的狀況。

感謝您的閱讀，歡迎透過問卷將您對於本期電子報的意見回饋給我們！
問卷連結：<https://forms.gle/B2M4j3Av9K6xpvGN6>