NIIEPA presents

ICANN JUNE

ICANN 工作小組每月電子報 2023 年 6 月 30 日 Issue #6

圖片來源：freepik

合約協商更新：改善 DNS 濫用條款

30 MAY 2023

由受理註冊機構利害關係團體（Registrars Stakeholder Group，RrSG）與註冊管理機構利害關係團體（Registries Stakeholder Group，RySG）組成的合約協商代表團，近日結束受理註冊機構驗證協議（Registrar Accreditation Agreement，RAA）及註冊管理機構協議（Registry Agreement，RA）中 DNS 濫用相關條款修訂的協商。

協商修訂後的條款針對註冊管理機構與受理註冊機構（以下簡稱合約方）如何回應 DNS 濫用，列出更明確、更有意義的規定。本修訂後的合約已公告並開放徵詢公眾意見，同時亦發布 ICANN 建議書草案（draft ICANN Advisory），解釋新條款內涵及執行方式。

本次合約協商雙管齊下，一方面透過小範圍、精確的合約修訂，確保合約方履行減緩 DNS 濫用的條約；另一方面，小範圍且聚焦的修訂也提供 ICANN 社群更多機會，評估未來進一步修訂合約、增加條款的需求。若有需求，則將透過 GNSO 公開、透明且基於多方利害關係模式的政策發展流程進行。

公眾意見徵詢結束後，ICANN Org 將分析募集到的社群意見、發布統整報告，並視需要，與合約協商代表團討論進一步調整的可能。定案後的修訂合約須經合約方投票通過後，交付董事會。若一切順利，修訂後的合約條款預計最早於 2024 年第二季生效。

緩解 DNS 濫用是影響全體 ICANN 社群的重要工程。

SALLY COSTERTON

圖片來源：ICANN 網站

聯合國秘書長政策報告：供 ICANN 社群參考

13 JUNE 2023

聯合國秘書長最近針對全球數位契約（Global Digital Compact, GDC）發布第五份政策摘要（Policy Brief 5）。ICANN 下政府暨國際政府組織交流（Government and IGO Engagement, GE）部門發表部落格文章，點出摘要中特別值得 ICANN 社群注意的部分。本文純粹為提供資訊，不代表 ICANN 立場。

以下重點節選特別涉及 ICANN 使命的幾個段落：

> 第 25 點：我們必須保護網際網路及其實體基礎建設。網際網路乃由歷史悠久的多方利害關係機構們治理。雖然不同司法管轄地區的法規可能不同，我們應協力維護政策與技術相容，以及網際網路的互通運作。

脈絡：雖然部分網際網路層面由多方利害關係方組成的組織協調，但聲稱特定數個機構管理網際網路並不精確。網際網路由網路互連組成，範圍從在地、國家、地區到全球，受各種規則及法規管轄，僅仰賴通用技術標準維繫其互通運作。

> 第 56 點：既有的協作機制，特別網路治理論壇（IGF）及世界資訊高峰會（WSIS），及聯合國組織如國際電信聯盟（ITU）、聯合國教科文組織（UNESCO）或聯合國開發計畫署（UNDP）辦公室，都在支援、就共同目標提供知識、分享經驗、促進對話上扮演重要角色。

脈絡：摘要將 IGF 及 WSIS 稱為「協作機制」並不準確。根據 WSIS 突尼斯議程，IGF 是「多方利害關係政策對話的論壇」，使命中從未提及「協作機制」。56 點提到的其他組織架構亦同。

> 附件 1 第 5 點：多方利害關係論壇，尤其是 ICANN 和 IETF。

脈絡：必須澄清這 2 個組織並非論壇，而是各有特定職責及功能的不同實體。

由於此政策摘要並沒有募集回饋，ICANN Org 所能做的僅有分享其中內容，協助 ICANN 社群完整了解摘要，以及未來提案的可行性和潛在後果。

最新 DNS 偵錯工具

31 MAY 2023

如同其他協定，DNS 也會出錯並中斷線上服務，造成網際網路使用者的困擾。要維繫順暢、值得信賴的網際網路，快速有效地解決錯誤是關鍵。以下分享 2 種快速有效偵測並解決 DNS 問題的新方法。

改善對 DNS 錯誤的了解

準確找出 DNS 錯誤的問題所在並採取必要行動並非易事。DNS 錯誤可能以網站連不上、連線速度緩慢、無法傳送電子郵件等形式發生；原因更是五花八門，包括設定錯誤、伺服器連線失敗、軟體或網路問題，甚至是惡意攻擊。

傳統 DNS 錯誤代碼提供的資訊極少，除錯流程也因此變得複雜耗時，而且需要高度專業技能。

最近提出的改善提案「DNS 錯誤擴充」（*Extended DNS Errors*，RFC 8914）協助 DNS 向客戶端及網路營運人員傳達更多錯誤的細節資訊，DNS 除錯流程也因此得益於更多、更詳細的相關資訊。

自動回報 DNS 錯誤

即時、準確發現 DNS 錯誤是採取行動的關鍵。IETF 中的 DNS 運作工作小組（DNS Operations Working Group）正在開發名為「DNS 錯誤通報」（*DNS Error Reporting*）的 DNS 協定擴充，協助 DNS 自動通報錯誤。

此功能將協助分析及調查通報的錯誤，以及通知相關負責單位。此自動通報流程直接利用 DNS 協定，大幅提升發現及解決錯誤的效率，相關單位不會再「看了社群媒體才知道」域名出問題。此協定預計今年底前正式成為「標準」。

圖片來源：freepik

2023 年 ICANN DNS 研討會
將於越南峴港舉行

15 JUNE 2023

2023 年 ICANN DNS 研討會（ICANN DNS Symposium，IDS）將於 9 月 5 日於越南峴港舉辦。ICANN 將邀請講者分享 DNS 安全及與新興技術的整合，探討整合帶來的挑戰和機會。研究人員、開發及維運工程師將齊聚一堂，討論諸如供應鏈、物聯網，以及 DNS 創新使用，如 IP 轉譯位址技術及封鎖名單等各項議題。

IDS 前一天將舉辦「DNS 濫用討論」全天活動，結束後則緊接著有為期 2 天、由 DNS 維運分析及研究中心（DNS Operations Analysis and Research Center，DNS-OARC）主辦的 OARC41 工作坊。

以下為當週活動日程：

- 9 月 4 日：DNS 濫用討論
- 9 月 5 日：ICANN DNS 研討會
- 9 月 6、7 日：OARC 41

研討會提供與會者討論 DNS 相關技術議題的空間，歡迎所有清楚了解 DNS 營運的人，諸如 gTLD 註冊管理機構、受理註冊機構、

gTLD 經銷業者、代管服務供應業者，以及註冊管理服務供應業者參與。

點此前往研討會專屬網站了解更多。

Epik 受害註冊人
紓困支援

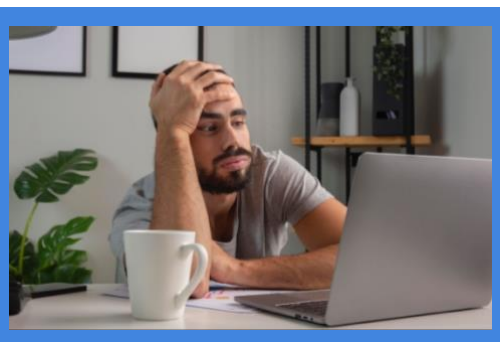
自 2023 年 3 月起，ICANN 持續收到針對受理註冊機構 Epik Inc.（以下簡稱 Epik）的投訴，包括收錢後未即時更新域名、客服及顧客支援緩慢或無效等。ICANN 正積極處理中，亦於今年 6 月 1 日正式向 Epik 發布違規通知。

本文說明註冊人能尋求的救濟資源，以及 ICANN 確保 Epik 履行合約的執行手段。

註冊人救濟：投訴方式及管道

ICANN 驗證受理註冊機構必須服從受理註冊機構驗證協議（RAA）、轉移政策、過期註冊恢復政策及過期域名刪除政策。若註冊人認為受理註冊機構未盡義務，導致自身權益受損，可參考以下資訊：

- 點此了解如何轉移域名。
  - 若註冊人聯絡受理註冊機構後仍無法取得授權資訊代碼（AuthInfo code）或解鎖並轉移域名，可透過此表格向 ICANN 申訴。
- 點此了解如何更新域名。
  - 若註冊人域名過期，聯絡 Epik 試圖更新域名未果，可填寫此表格向 ICANN 申訴。
- 點此瀏覽所有 ICANN 履約申訴表格。
- 點此瀏覽註冊人資源彙整。



圖片來源：freepik

在提出申訴前，請確認投訴的域名為 gTLD 而非 ccTLD。ICANN Org 並不會驗證 ccTLD 受理註冊機構或訂定 ccTLD 政策。如遇到 ccTLD 相關問題，請聯絡該 ccTLD 管理方，或點此查看聯絡資訊。

ICANN 職權

ICANN 能對 Epik 採取的行動必須基於RAA及相關共識政策，包括其中列出 gTLD 域名的更新及取回條款。若 Epik 顧客對 RAA 外的服務有疑慮（如款項問題或透過 Epik 拍賣網站的買賣行為），請自行尋覓法律意見。

公眾意見徵詢

基礎 gTLD 註冊管理機構協議及受理註冊機構協議修訂：DNS 濫用義務條款調整

類別	其他	提案人	ICANN Org	時程進度（UTC）

本案就 gTLD 註冊管理機構協議（RA）及受理註冊機構驗證協議（RAA）（以下併稱協議）中 DNS 濫用條款修訂徵求公眾意見。修訂內容包括：

- 合約方網站上必須列明濫用通報聯絡方式，收到通報後必須傳送回條。
- 合約方可使用網路表格而非電子郵件信箱作為濫用通報聯絡方式。
- DNS 濫用定義（惡意軟體、殭屍網路、釣魚網站、惡意嫁接，以及用來達成上述濫用行為的垃圾郵件）。
- 合約方若取得可採取行動的 DNS 濫用證據，必須及時採取適當行動。
- 容許合約方根據情況，自行選擇並執行適當的濫用緩解行為。
- 明確認證受理註冊機構與註冊管理營運方的不同職權。

提案內容：

- Proposed Global Amendment to the Registrar Accreditation Agreement
- Proposed Clean 2013 Registrar Accreditation Agreement
- Proposed Global Amendment to the Base gTLD Registry Agreement
- Proposed Redline Base gTLD Registry Agreement
- Proposed Redline 2013 Registrar Accreditation Agreement
- Proposed Clean Base gTLD Registry Agreement

開放徵詢

2023 年 5 月 29 日

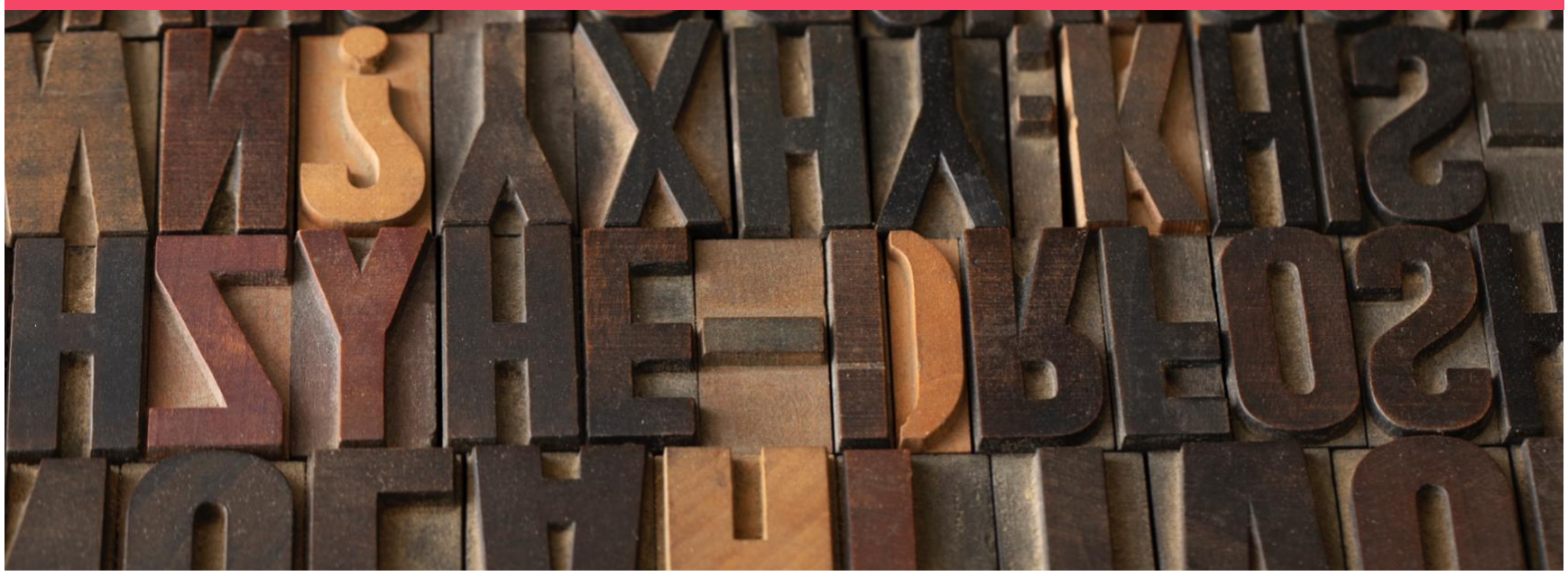
結束徵詢

2023 年 7 月 13 日 | 23:59

募集意見統整報告

2023 年 8 月 1 日 | 23:59

提交意見



圖片來源：freepik

ICANN 的合約管理和執行：大哉問

文章出處：INTERNET GOVERNANCE PROJECT

ICANN77 期間有一場針對 ICANN 權責範圍的激烈辯論：一方認為 ICANN 應有更多權力執行註冊管理機構自願承諾（Registry Voluntary Commitment, RVC），一方則指出為達成此目的，對方提議的做法將危及網路上的言論自由，並傷害 ICANN 的多方利害關係政策制定流程。

背景介紹

ICANN 透過與域名註冊管理機構與受理註冊機構簽約以管理 DNS。網路社群支持這種以私人企業為基礎的合約體制，因為這樣的架構不受政府司法管轄限制，就像網際網路及 DNS 一樣全球適用。

ICANN 的管理權力來自其作為 DNS 根守門人的身分。註冊管理機構僅能透過與 ICANN 簽約取得 gTLD，他們必須遵守合約及若干規定，並定期向 ICANN 繳費。

這些合約來自於 ICANN 政策，政策則由多方利害關係社群制定。ICANN 身為根守門人，基本上壟斷 DNS。如前所述，註冊管理機構必須與 ICANN 簽約才能取得並經營 gTLD，而與壟斷產業核心服務的對象（ICANN）簽訂合約以從事生意，幾乎算是不平等條款，因為這等於對方得以任意訂定條約規範。這也是為什麼 ICANN 政策必須來自由下而上的多方利害關係模式。

自 ICANN 成立，對單一組織集中管理 DNS 可能導致不當管制網際網路內容、服務或應用程式的憂慮始終不斷。而訂定精確、範圍限縮且可執行的使命，是解決此合理顧慮的唯一手段。如同美國《權利法案》或歐盟《基本權利憲章》規範其政府的權力，ICANN 組織章程（bylaws）規範 ICANN 組織的合約權力。

受理註冊機構自願承諾（RVC）

隨著 ICANN 開始準備開放下一回合 new gTLD 申請，受理註冊機構希望他們能在合約中自由添加「受理註冊機構自願承諾」（RVC），並確保 ICANN 有權要求他們履約。

New gTLD 申請人面對許多競爭。他們希望取悅政府、智財權所有人，或任何潛在反對者，順利獲得自己申請的字串。為了達到此目的，他們希望利用 RVC 承諾滿足反對者需求，如為了避免冒犯保守宗教團體，申請人可能在 RVC 中承諾不容許任何瀆神的域名註冊。申請人也可能為了進入中國市場，在 RVC 中規定不准任何域名註冊提及天安門事件或香港雨傘運動。

在自由的域名市場中，gTLD 註冊管理機構的確可以隨意許下承諾，自行遵守承諾。但現在的問題是他們希望 ICANN 透過合約，強制他們遵守承諾。若 ICANN 真的這麼做，等於踏入內容或服務管制的領域，徹底違背其刻意限縮的使命，違反 ICANN 的組織章程。

而有些人現在主張，為了避免 ICANN 違反組織章程，應該修改組織章程內容，而非不要訂定莫名其妙的 RVC。

避開多方利害關係政策制定

執行 RVC 將為多方利害關係政策流程帶來糟糕的連帶效應。若 ICANN 決定執行受理註冊機構單方面決定的規則，代表多方利害關係流程失去對政策的掌控，無法再透過制定政策規範合約方的行為。ICANN 政策和合約將淪為 ICANN 與合約方之間討價還價的產物，而不再受由下而上、共識決、多方利害關係方共同制定的統一政策規範。

值得慶幸的是，ICANN 若想執行任何規範內容的 RVC 都將違反其組織章程，要為這修改組織章程，也幾乎確定會因工程浩大且公益性低而失敗。但未來的事情很難說，大家還是應該密切持續關注此議題進展，齊力阻止特定團體為自身利益，為多方利害關係流程帶來難以復原的傷害。

圖片來源：freepik

歐盟網路韌性法案激起開源及網路安全疑慮

資料來源：EFF

歐盟現正修訂網路韌性法（Cyber Resilience Act, CRA）草案，此法希望強化歐洲對網路攻擊的防禦能力，並改善未來產品安全。此法含括歐盟消費者可能接觸的多種產品，包括物聯網裝置、桌上型電腦及智慧型手機，並針對上述產品的製造、流通，以及弱點通報、安全事件法律責任等訂定規定。

網路人權倡議團體電子先鋒基金會（Electronic Frontier Foundation, EFF）雖樂見 CRA 意圖，但認為法案內容將導致開源開發人員因收受報酬而無端受罰。法案中要求製造商向執法機關通報遭濫用、尚未修補之弱點的規定，可能引發消息廣傳、更多惡意人士得知並利用弱點發動攻擊，導致受害人數增加的風險。

圖片來源：freepik

對開源軟體的威脅

開源軟體是當代網際網路的骨幹。開發工程師使用如 Linux 和 Apache 等開源專案寫出的免費程式，早已整合進五花八門的產品中，被全球數十億人使用。若沒有個人捐款、基金資源和贊助，這些都不可能發生。這個軟體開發與資金的生態循環，是確保這個軟體驅動的當代世界持續運轉的關鍵。

將具弱點產品送入市場的商業行為，在 CRA 規定下必須負擔法律責任。雖然 CRA 草案中註明非營利行爲可豁免上述條款，但問題在於法規對商業行為的定義過於廣泛，導致許多受贊助的開源產品服務被排除在外。

通常開源貢獻者是基於善意、互惠而開放免費使用，但在 CRA 草案下，就連收到使用者的自主捐款，都將導致開源貢獻者在軟體被發現弱點時蒙受觸法風險。

弱點揭露規定將導致網路安全威脅

草案第 11 章規定製造商必須在 24 小時內向歐盟網路安全機構（European Union Agency for Cybersecurity, ENISA）通報遭濫用中的弱點，後者則必須將相關細節轉知所有歐盟成員國的電腦資安事件應變小組（Computer Security Incident Response Team, CSIRT）與市場監察當局。規定看似立意良好，但對真正在乎安全、希望徹底修補弱點的公司而言，可能會有反效果。

許多重視安全的公司發現弱點後會選擇保密，在完整修補、所有產品都已安裝新補丁後，才分享此消息。這是因為分析、檢驗弱點的根因並發展修補方案需要時間，有時長達數月。法規的緊迫時間線，可能導致公司沒有時間探索從根因解決的完整修補，而在時間壓迫下僅做到表面功夫。

另一方面，通報要求也會讓很多人在短時間內得知消息，因此大幅提升有心人士風聞、藉機利用弱點攻擊的風險。更進一步而言，政府知道太多製造商方面的弱點和安全漏洞，也可能導致國家間的駭侵、間諜行為。通報的製造商不會知道政府怎麼處理他們得到的資訊，若政府決定轉而利用弱點向他國發動網路攻擊，他們身為平民也無力阻止。

不只如此，法規雖要求即時通報，卻未要求向大眾公開弱點。消費者有知的權利。EFF 呼籲修改規定，所有弱點應在完整修補後才通報 ENISA。

良好的第一步

網路韌性法的目標是強化歐洲整體的網路安全。然而，EFF 指出，若不調整上述規定內容，結果可能反其道而行。