更新日期：2019 年 7 月 25 日

本期電子報內涵

一、重要議題

GDPR/WHOIS：最新進展

EPDP 進展

- **EPDP 第二階段：ICANN65 討論**

ICANN65 期間，EPDP 小組召開兩場實體會議。在合計長達 13 小時的會議中，EPDP 小組的工作重點包括：

- 討論使用者要求存取非公開 gTLD 註冊資料的「使用案例」範本架構。
- 檢視 2 則使用案例。
- 與 ICANN ORG 聯合會議。ICANN ORG 已將技術研究小組完成的統一存取模型（Unified Access Model，UAM）呈予歐盟資料保護委員會（European Data Protection Board，EDPB），會議中由 ICANN ORG 代表向小組簡報後續進展。
- 檢視 EPDP 第二階段專案計畫及時程規劃。

會議期間，EPDP 小組決定將「使用案例」當成討論範本，透過檢視「要求存取非公開 gTLD 註冊資料」的使用者歷程，探討標準化存取/揭露系統（Standardized System of Access/Disclosure）的必要元素與步驟。由於許多團體皆有意願提交新的使用案例，EPDP 小組亦趁會議期間擬定未來提交案例的

範本，主席並要求所有欲提交新案例之團體，必須於 7 月 5 日前完成。

EPDP 小組於 ICANN65 期間討論了 2 則使用案例，分別是「商標所有權人要求存取侵害其商標權的註冊人資料，以採取後續法律行動」，以及「執法機關進行犯罪調查」。於 7 月 5 日收集完所有團體提交的使用案例後，EPDP 小組預計分成 3 個小分組，於 7 月中旬至 8 月中旬分別檢視 3 至 4 個使用案例，並在 8 月底或 9 月初將小分組結論分享給 EPDP 全體成員。

下一次 EPDP 小組實體會議預計於今年 9 月 9 日至 11 日於美國洛杉磯舉行。

- **EPDP 第一階段實施進度**

EPDP 第一階段執行審核小組（Implementation Review Team，IRT）於 5 月組成，本次 ICANN65 會議中，IRT 亦舉行了自成立以來的首次面對面會議。會議由 ICANN ORG 全球域名部門計畫主任，也是 EPDP Phase 1 結案報告的執行專案小組（Implementation Project Team，IPT）的專案經理 Dannis Chang 主持。

IRT 現有 28 名小組成員，38 名觀察員。與 EPDP 不同，IRT 並未限制成員人數，任何有興趣的人都可以加入 IRT。

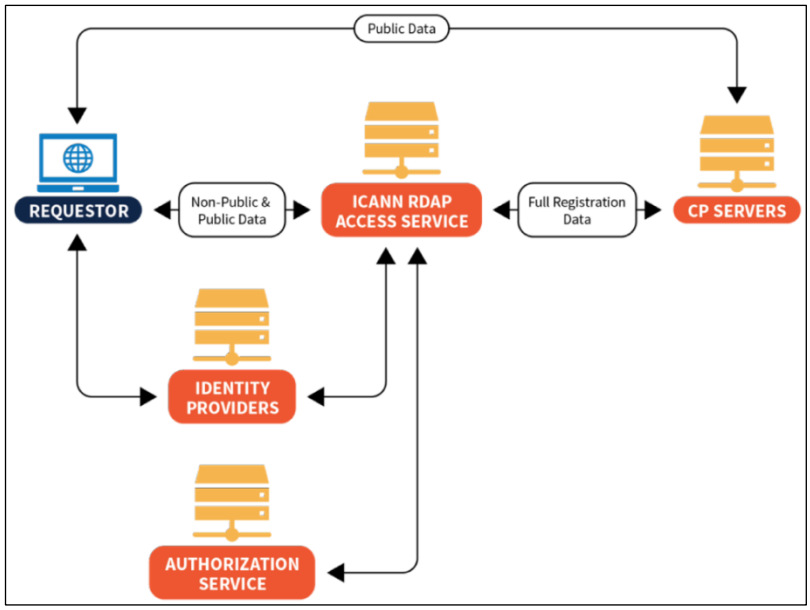
IPT 及 IRT 目前處於「分析 EPDP 第一階段結案報告政策建議」的工作階段。IPT 會就每項建議產出分析文件，文件中包含四部分，分別是 (1) 政策語言；(2) 執行注意事項；(3) 其他可能選項/做法；(4) IRT 審核建議紀錄。最後一部分的主要目的是記錄 IRT 對文件內容提出的建議，並確認 IPT 逐項回應，或因應調整文件內容。而 IRT 的任務是審核 IPT 的工作，並回答 IPT 的問題。

本階段完成後，IPT 將根據分析結果，整理出後續執行計畫的預計開銷、範圍及完整的執行時程，並公告及開放徵詢公眾意見。

- **草莓小組（Strawberry Team）**

草莓小組（Strawberry Team）是 ICANN ORG 中負責 GDPR/EPDP 相關事務的專案小組，成員包括擔任「政府交流」（government engagement）一職的 Elena Plexida，以及法務專員 2 名、技術長辦公室職員 1 名、GDD 技術服務職員 1 名、MSSI 職員 2 名。

草莓小組的主要任務是與歐盟執委會、資料保護機關交流溝通，將 ICANN 社群的工作成果呈予對方，確認政策或存取模型是否合法/可行。草莓小組最近一次呈現給歐盟執委會相關人士的成品，是由 TSG 建立的技術模型 TSG01，如下圖：



如圖可見，在此模型中，除原本就公開的註冊資料外，合約方（CP Servers）僅需於收到要求時，提供 ICANN RDAP 服務完整的註冊資訊。ICANN ORG 主張，根據此模型，由於合約方不涉及「決定要求方是否符合資格」的決策流程，因此推斷合約方無須負擔「揭露」[1]資料的法律責任。

Plexida 解釋，ICANN ORG 在布魯塞爾的遊說工作目的有二：一是取得 EDPB 的指導，二則是向歐盟執委會展現 ICANN 社群設法符合 GDPR 的努力。EPDP 小組成員提議，既然 ICANN ORG 已決定繼續進行草莓小組工作，未來草莓小組應與 EPDP 小組保持密切交流，形式可採定期會議報告或指派草莓小組駐 EPDP 聯絡人等。

TOP

[1] 根據 GDPR 第四章，「資料處理」包括資料的蒐集、紀錄、管理、結構化、儲存、改編或變更、檢索、查閱、使用，透過傳播、散布或其他方式予以揭露，比對或結合，限制使用、刪除或銷毀等。

原文： 'processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

二、最新消息

DNS 與物聯網：機會、風險與挑戰

ICANN 安全與穩定諮詢委員會（Security and Stability Advisory Committee，SSAC）最近發布了 SAC105 ，一份說明域名系統（DNS）與物聯網（Internet of Things，IoT）關係作用的報告。與以往 SSAC 發布的報告不同，SAC105 並未向 ICANN 董事會提出任何建議；報告主要目的是提供資訊，希望促進 ICANN 社群成員對此議題的關心及討論。

物聯網將我們的實體生活與上億的感測器及裝置連結，企圖創造更便利、更無縫的生活體驗。物聯網中的資訊交換，與過去我們熟悉的電子郵件或上網瀏覽等傳統網路應用不同，往往是在使用者不知情的情境中被動發生。物聯網裝置持續不間斷地與 DNS 互動，無論運作或更新都須仰賴 DNS，互相影響的型態也更多樣。SSAC 認為 DNS 社群必須了解 IoT 對 DNS 的影響，IoT 製造商也必須了解 DNS 乃 IoT 生態系統保持健全的關鍵。

SAC105 重點發現：機會、風險及挑戰

IoT 裝置直接感應實體環境並做出回應，這種網路應用對安全、穩定及透明度有全新的需求，對可以滿足這些需求的 DNS 而言，未嘗不是個大好機會。DNSSEC 就是個很好的例子，這個技術可以確保智慧門鎖只在收到真正使用者的指令時解鎖。

但 IoT 也可能在 DNS 上製造過度壓力，這是 DNS 必須面對的風險。最近的量測研究顯示，IoT 殭屍網路（botnet）可以快速感染上千種裝置，包括燈泡、相機，甚至是門鈴，然後利用這些裝置對網路基礎建設展開大型分散式阻斷服務（Distributed Denial of Service ，DDoS）攻擊。由於每種裝置會需要專用的掃毒程序，而且裝置通常在使用者不知情下運行或更新，一舉剷除 IoT 殭屍網路非常困難。

針對如何取得先機、迴避風險，SAC105 中整理出幾項挑戰，也可視為給 DNS 社群的功課。其中一項是建立 DNSSEC 驗證及其他 DNS 安全功能的資料庫，並開放給 IoT 軟體工程師使用。另一項則是建立所有 DNS 維運方自動即時分享殭屍網路情報的機制，如此一來，維運方也能迅速因應新的殭屍網路及 DDoS 攻擊。

SSAC 在文件中也提出幾個比較激進的問題，希望社群起而迴響，一同思考未來對策。SSAC 強烈推薦大家閱讀 SAC105，並將回饋意見寄至 ssac-staff@icann.org。

TOP

主席部落格：ICANN65 重點回顧

ICANN65 馬拉喀什會議已於上個月結束，ICANN 董事會主席 Cherine Chalaby 依照慣例，於會後發表部落格文章，向社群簡介董事會於 ICANN65 期間的重要活動。

董事會例行會議

在 ICANN65 開始前，董事會於馬拉喀什舉行了 3 天的例行會議。會議中除了董事會公開議程、董事會會計年度 2019 重點項目進度報告，還包括許多準備 ICANN65 政策論壇的前置會議。在董事會公開議程中，董事會通過以下決議：

- 考慮 SSAC 就域名註冊資料存取提出的建議（SAC101）
- 採納 ICANN 會計年度 2021-2025 戰略計畫
- 採納必辦審核實施原則
- 接受 SSAC 第二次組織審核的結案報告暨初步實施計畫可行性評估
- GNSO 受理註冊機構團體章程修正

Cherine Chalaby 感謝社群的努力，促成 ICANN 會計年度 2021-2025 戰略計畫的誕生。為了未來能實際達成戰略目標，ICANN ORG 已於數月前開始規劃實施方案，並計畫於未來幾個月內產出 5 年執行暨財務計畫，以持續協助維護 ICANN 社群的多方利害關係治理模式。Cherine Chalaby 鼓勵大家積極參與 ICANN 未來 5 年計畫的討論，自 6 月 14 日起開放的「財政年度 2021-2025 執行暨財務計畫：財務預測與執行規劃」公眾意見徵詢，將於 8 月 5 日截止，社群成員應把握時間提出建議及反饋。

多方利害關係精神獎

來自支援組織與諮詢委員會的遴選委員代表決定將多方利害關係精神獎頒給 Kurt Pritz，感謝他對 ICANN 多方利害關係治理模式的奉獻，亦表彰他在抱持多方歧見的各團體中，盡力異中求同的傑出能力。身為 EPDP 前主席，Kurt Pritz 帶領 EPDP 小組完成第一階段，解決 ICANN 史上最棘手的難題之一，成功產出一套新的註冊目錄服務政策。恭喜 Kurt Pritz！

TOP

當責與透明度審核：進度更新及徵求社群意見

當責與透明度審核（Accountability and Transparency Review，ATRT）為 ICANN 組織章程細則（第四章 4.6 節）規定的必辦審核之一，主要目的是檢視 ICANN 履行使命的效率、強化募集社群意見的機制、加強 ICANN 當責及透明度，進一步確保 ICANN 決策反映公共利益，且對整體網路社群當責。

ATRT2 結束至今已超過 5 年，是時候展開 ATRT3。ATRT3 不僅涉及 ICANN 社群最重視的「當責」議題，本次審核更是 IANA 監管權轉移後，首次由社群自發性實施，其時代意義不言可喻。ATRT3 審核小組於 2018 年 12 月 20 日正式成立，共有 18 名成員。根據 ICANN 組織章程細則規定，必辦審核小組成員應由 SO/AC 共同推舉，確保審核小組的專業及多元性。

審核小組 ICANN65 前便已公告小組權責範圍（terms of reference）及工作計畫，供社群與董事會參考。也因為及時於會前完成了這兩項重點工作項目，小組得以利用 ICANN65 期間推進工作進度；除了繼續蒐集、分析資料外，小組也與社群成員、其他團體進行充分交流。除此之外，小組也持續關注可能與 ATRT3 審核內容重疊的其他社群工作，如「ICANN 多方利害關係治理模式進化」的社群熱門話題、加強 ICANN 當責第二階段的實施狀況等。

小組預計於未來幾周完成資料蒐集，期間也計畫進行問卷調查，取得社群對小組審核重點及目前發現的意見與反饋。若有任何建議指教，小組也隨時歡迎大家寄信到 input-to-atrt3@icann.org。

依規定，ATRT3 需於一年內（即 2020 年 4 月為止）完成審核工作。審核小組目前進度皆依規劃，預計將準時達成目標。ATRT3 下一次的實體工作會議將於 10 月在新加坡舉行。

TOP

三、公眾意見徵詢

「IGO-INGO 修復式權利保護機制」政策建議

- **開放日期：**2019 年 7 月 11 日 23:59 UTC
- **關閉日期：**2019 年 8 月 20 日 23:59 UTC
- **目的：**在董事會決議前，徵求社群對 「IGO-INGO 修復式權利保護機制」政策建議的意見。
- **下一步：**本公眾意見徵詢結束後，董事會將就是否通過政策建議召開會議。
- **說明：**
  - GNSO 理事會於 2014 年 6 月決議通過啟動政策發展流程（Policy Development Procedure，PDP），檢視是否應考量國際政府組織（International Governmental Organization，IGO）及國際非政府組織（International Non-governmental Organization，INGO）的特殊需求及情形，(1) 修正 gTLD 修復式權利保護機制，或 (2) 根據既有的修復式權利保護機制架構，建立一個新的、IGO 及 INGO 專用的爭議解決流程。
  - 工作小組於 2018 年 7 月將結案報告交給 GNSO 理事會。2019 年 4 月，GNSO 理事會決議通過結案報告中第 1 至 4 項建議，報告中第 5 項建議則將留待「審核所有 gTLD 權利保護機制」PDP 第二階段處理。
  - GNSO 理事會通過的 4 項建議已呈予董事會。根據 ICANN 組織章程細則，董事會考慮 PDP 最終建議前須開放徵求社群意見，以確保社群充分發聲的時間與機會。
  - 通過的 4 項建議可歸納為以下 3 個重點：
    - 既有的權利保護機制毋須為 INGO 大幅修正；
    - 不必為 IGO 特別建立新的爭議解決流程；
    - 有關 IGO 提出投訴的現行流程，應撰寫更清楚明瞭的政策指導說明。
- **相關資料：**
  - IGO-INGO Access to Curative Rights Protection Mechanisms PDP WG Final Report
  - PDP Charter
  - PDP Wiki
- **意見提送網址：**
  https://www.icann.org/public-comments/igo-ingo-crp-recommendations-2019-07-11-en

TOP

域名衝突定義提案暨計畫研究範疇

- **開放日期：** 2019 年 7 月 2 日 23:59 UTC
- **關閉日期：** 2019 年 8 月 12 日 23:59 UTC
- **目的：**SSAC 希望就域名衝突分析計畫（Name Collision Analysis Project，NCAP）中的「域名衝突定義」及「計畫研究範疇」徵求社群意見。
- **下一步：**NCAP 討論小組完整檢視並考量社群意見後，會確立「域名衝突」的定義及計畫未來的研究範疇。
- **說明：**
  - 董事會於 2017 年 11 月通過決議（2017.11.02.29 – 2017.11.02.31），要求 SSAC 研究現有的資料、

分析數據及各家看法後，提供董事會以下事項的專業建議：

- ♦ 域名衝突（name collision）的定義；
- ♦ 判定未發配字串是否展現「衝突」(也就是「衝突字串」）的衡量標準；
- ♦ 判定「衝突字串」是否可發配的衡量標準；
- ♦ 判定可否從「衝突字串」清單中移除特定未指配字串的衡量標準。

➢ 決議中，董事會也要求 SSAC 進行本研究計畫時應快速、有條理，開銷和時程適當公開，隨時供社群及董事會檢驗。

➢ 在董事會要求之下展開工作的 SSAC，於 2018 年完成了域名衝突分析計畫（Name Collision Analysis Project，NCAP）提案。為回應董事會要求，提案中列出三個階段性研究計畫。

➢ ICANN 董事會於 2019 年 3 月核准了第一階段研究計畫，計畫內容包括

(1) 檢視所有關於域名衝突的歷史研究，並產出重點整理報告，供後續計畫新成員參考；

(2) 整理一份歷史研究使用過的資料清單，並確認是否有缺漏。同時應列出未來研究計畫需要的額外資料；

(3) 第一階段研究計畫完成後，小組應具備足夠的資料，判斷是否需繼續第二及第三階段研究。

➢ NCAP 目前已完成第一階段研究計畫的工作筆記（Statement of Work），其中列出預計研究重點、工作時程，以及工作方法等。同時，NCAP 完成了工作筆記中的第二項標的：域名衝突的定義及研究計畫預計蒐集的資料，並公告徵求社群意見。

● **相關資料：**

➢ Proposed Definition of Name Collison and Scope of Inquiry for the Name Collision Analysis Project: https://community.icann.org/display/NCAP/NCAP+Working+Documents?preview=/79437474/111387704/Definition%20of%20Name%20Collision%20and%20Scope%20of%20Work%20for%20the%20NCAP.pdf

➢ Past Research and Studies on Name Collision:

(1) SAC045: Invalid Top Level Domain Queries at the Root Level of the Domain Name System (https://www.icann.org/en/committees/security/sac045.pdf)

(2) SAC057: SSAC Advisory on Internal Name Certificates (https://www.icann.org/en/system/files/files/sac-057-en.pdf)

(3) Name Collision in the DNS (https://www.icann.org/en/system/files/files/name-collision-02aug13-en.pdf)

(4) New gTLD Collision Risk Mitigation (https://www.icann.org/en/system/files/files/new-gtld-collision-mitigation-05aug13-en.pdf)

(5) Name Collision Occurrence Management Framework (https://www.icann.org/en/system/files/files/name-collision-framework-30jul14-en.pdf)

(6) Mitigating the Risk of DNS Namespace Collisions (https://www.icann.org/en/system/files/files/name-collision-mitigation-final-28oct15-en.pdf)

● **意見提送網址：**

https://www.icann.org/public-comments/proposed-definition-name-collisions-2019-07-02-en

TOP

四、相關文摘

「無協議」脫歐後，Leave.EU 或許仍能保住域名？

原文標題：Leave.EU may keep name after no-deal Brexit if ownership handed to EU citizen

資料來源：The Guardian（原文）

內容摘要：

歐盟執委會今年 3 月曾宣布，若英國無協議脫歐，所有位於英國的.EU 註冊人必須放棄.EU 域名。歐盟執委會近日修正了這項決定：即使在無協議脫歐後，註冊人也能夠保有.EU 域名——前提是註冊人必須為歐盟公民。

2006 年推出的.EU 頂級域名，原意是希望認同歐洲的企業或組織在線上擁抱歐洲身分，不須再使用美國營運的.COM、.NET 和.ORG 等頂級域名。但自開放至今超過 10 年，最有名的.EU 網站，卻是擁護脫歐的英國團體申請的 Leave.eu。

根據.EU 註冊管理機構規定，企業或個人如欲註冊.EU，必須登記執業或定居於歐盟或歐洲經濟區（EEA）。目前持有.EU 頂級域名的英國國民約 34 萬人，若真面臨無協議脫歐，這些人都將失去註冊域名。然而，註冊.EU 的不只有英國國民，還有許多旅居英國的歐盟公民。在這些歐盟公民的抗議下，歐盟執委會提出解套方案：未定居於 EEA 境內的歐盟公民若在 2019 年 10 月 19 日前驗證公民身分，便能保有.EU 域名。

然而，若域名註冊人是團體或法人，則不適用此規定。非立案於 EEA 境內的法人若想保住域名，唯一方法是把域名轉移到歐盟公民名下。還記得最有名的 Leave.eu 嗎？根據註冊管理機構 eurid.eu 提供的 WHOIS 資料，這筆域名的註冊人是 LEAVE.EU GROUP LIMITED，看起來不像是歐盟公民。如果 Leave.eu 未來想持續為脫歐造勢發聲，大概只能選擇「在歐盟立案登記」或「將域名轉移給歐盟公民」。

雖然很多人認為這個方案其實是提供英國公民一個漏洞可鑽，但至少英國政府並未公開鼓勵大家利用這個漏洞。事實上，英國數位文化媒體及體育部還是建議國內註冊人趕快註冊其他新域名，以「為無協議脫歐做好準備」。

TOP

重新檢討 DoH 討論

原文標題：Recalibrating the DoH Debate

資料來源：Circle ID（原文）

內容摘要：

DNS over HTTPS（DoH）儼然是最近網路熱門話題之一。不僅 ICANN 於馬拉喀什特別為此舉行跨社群議程，英國網路服務供應商協會（Internet Service Provider Association，ISPA）也在今年因為 Mozilla 計畫於瀏覽器 Firefox 支援 DoH，而提名後者為「2019 網路惡棍」，與美國總統川普並列[2]。

DoH 之所以成為爭議焦點，是因為它將改變自網際網路創立以來的域名解析機制。傳統的 DNS 解析

[2] 在 Mozilla 澄清反駁後，ISPA 已於今年 7 月 9 日取消 Mozilla 的提名。

符合網際網路「互信」的初衷，所有 DNS 查詢的傳輸及回應都沒有加密。然而，隨著網路擴展至現在的規模，在這個「資料是金」的年代，大眾對隱私保護也益發重視。DoH 的誕生便是回應使用者對資料保護的需求。

顧名思義，DoH 是要利用安全超本文傳輸協定（HyperText Transfer Protocol Secure，HTTPS）解析 DNS，這也表示 DNS 查詢從使用者端到回應端都被加密，使用者的隱私因此受到保障，免於被監聽或操控的風險。

支持 DoH 的論點強調它的安全及保護隱私，但反對者認為 DoH 不但沒有更安全，而且 DoH 於瀏覽器端解析 DNS 的方式，只會進一步惡化網路巨頭獨大的現況。現於牛津資訊實驗室（Oxford Information Labs）任職網路安全顧問，同時也積極參與 ICANN、IETF 等網路社群的 Stacie Hoffmann 近日於 CircleID 撰文評論，認為目前對 DoH 的討論陷入對立僵局，應重頭檢視、並廣邀多方利害關係人參與討論。

Stacie Hoffmann 舉出兩個 DoH 利弊夾雜的特點。首先，雖然 DoH 的「點到點加密」措施能防止監聽，因此能保護生活在極權國家的使用者，但她也指出「加密」不等於「保障隱私」。她認為 DoH 並沒有解決隱私問題，因為所謂的「加密傳輸」無法防止資料蒐集，而蒐集資料才是隱私被侵犯的起點。

再者，DoH 將安全工具及使用者保護措施集中於應用層（也就是使用者端）的方式，雖然可能有「迴避當地司法干預」的好處，但也可能反讓攻擊者輕易鎖定目標，或造成「一點失效，全面癱瘓」的後果，很難判斷是好是壞。

作者認為，現在最重要的工作應該是搞清楚 DoH 可能的問題，並舉出可實際受惠於 DoH 技術的使用案例。她強調，轉向如何解決資料濫用、網路分層逐漸合併、安全考量的取捨等討論，會比兩極化、缺乏交集的對話更有建設性。

長久以來，網路標準的討論似乎只限於技術社群，雖然 IETF 開放所有人參與，但公民社會、學界、政策制定者似乎都缺乏參與討論的意願或能力。IETF 作為技術社群，本就相對缺乏公共政策、人權議題等方面的人才，但這並不表示網路標準的討論便可免於這些重要議題。作者呼籲，現在正是多方利害關係人互相加深理解、參與的關鍵時刻，希望大家積極參與 DoH 討論。

TOP