2023

IP&DN

網路位址及網域名稱趨勢電子報

2023年9月號

INTERNET PROTOCOL ADDRESS & DOMAIN NAME

指導單位 | moda 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

本期電子報首先精選國際間重要的網路位址與網域名稱相關新聞；介紹今（2023）年9月12日至14日於日本京都（Kyoto, Japan）舉辦的APNIC 56會議，這是APNIC成立30週年的慶典活動，該會議中特別邀請到歷經APNIC成立初期到穩定發展不同時期的重要代表人物，共同回顧了APNIC三十年的發展歷程；接續摘錄數位發展部近期所舉辦的「WSIS+20到底是什麼？」座談會中專家們會議上的討論重點。最後，專欄文章將簡略介紹「DNS權威主機」的用途、特性，以及所面臨的挑戰，並提供了應對這些挑戰的可能對策。

目錄

IP&DN全球重點新聞

飽受爭議的「.sucks」頂級網域在GoDaddy上架

「.sucks」頂級網域自2014年推出後便飽受爭議，特別是對品牌名稱的高額註冊費，更被ICANN的智慧財產權利害關係方團體批評為掠奪行為。但其註冊管理機構Vox Populi的執行長John Berard卻認為此價格合理，他還提供了品牌方管理自己的brand.sucks 網站的機會。在2015年中完全開放給大眾註冊時，Vox Populi更訂出超過標準值的US$249年費高價，當時獲得了超過6,200筆註冊量，到了2021年更達到最高峰的13,400筆。包括像是針對特定城市名稱的「city-name.sucks」、針對特定電影名稱註冊的「.sucks」網站等，都遭到批評。儘管爭議不斷，「.sucks」在GoDaddy的上架，在業界仍被認為是「.sucks」發展的重大里程碑。

點此查閱更多資訊

亞培試圖以UDRP來解決商標問題，失敗收場

全球性的保健產品製造商亞培（Abbott Laboratories）試圖要利用ICANN的網域名稱爭議處理機制（UDRP），來解決一家品牌是Ensure 販賣燕窩相關食品與護膚品的越南商家的商標爭議。該越南商家的品牌與亞培的安素（Ensure）營養品的商標名稱相同，其販售商品的網站註冊名稱為 ensure-nest.com。該UDRP案件在今年9月中作出判決，亞培並沒有取回該ensure-nest域名。參與此UDRP案件的仲裁員表示，此為商標使用爭議，而非域名濫註的爭議，因此無法透過UDRP機制解決，建議透過法院來解決此爭議。

點此查閱更多資訊

ICANN公布.com註冊商排行榜

點此查閱更多資訊

ICANN公佈.com註冊商排行榜，這些註冊商在2023年4月的.com註冊量如表所列。

排名	註冊商	.com的4月註冊量
1	GoDaddy.com	799,939
2	Namecheap Inc.	281,785
3	Google Inc.	231,422
4	Newfold Digital	186,042
5	Gname.com	165,072
6	Tucows	155,112
7	Alibaba	111,377
8	CentralNic	102,755
9	NameSilo	79,086
10	GMO	74,168

APNIC歡慶三十週年

為歡慶APNIC三十週年，本屆APNIC年度會議特地回到APNIC的創始地日本舉行。會議期間，亦由現任APNIC首席科學家Geoff Huston主持，邀請到歷經APNIC草創成立、初期營運到穩定發展不同時期的重要代表人物，共同回顧APNIC三十年的旅程。

本特別場次的與談人包括當年共同於日本東京成立APNIC的日本網路之父Jun Murai（村井純），以及曾任ICANN技術長、目前為Virtualized網際網路技術與治理顧問的David Conrad。也請到當時Merit Network的專案系統經理Elise Gerich。Merit在1987年承接美國國家科學基金會合約，與IBM、MCI及密西根大學合作，成功連結美國境內多個學術網路，打造當代網際網路的骨幹。

Photo by APNIC on flickr

Image Credit:APNIC Blog

除此之外，JPNIC首席政策官、曾任APNIC執行委員會（Executive Committee，EC）主席超過12年（2003至2016年）的Akinori Maemura（前村昌紀），2016至2023年擔任EC主席的Gaurab Raj Upadhay，以及APNIC總經理Paul Wilson皆列席與談。

與談人自東京草創APNIC談起，乃至搬遷到澳洲布里斯本的決定，共同回顧APNIC成長至今日服務全球最多人口、會員數量持續增加、穩健營運的非營利組織。不僅是APNIC作為組織，參與亞太網路維運討論的社群亦每年迎來新血，面對當代網際網路技術演進呈現的機會與挑戰，與談人共勉在座所有世代持續參與、持續發生，共同維護心中理想的網際網路。

點此觀看座談影片

合作特別興趣小組：強化路由安全

合作特別興趣小組（Cooperation SIG）希望提供一個平臺，供社群討論關乎APNIC利益但範疇較廣，同時涉及其他如政府、其他組織或社群等多方利害關係團體的公共政策或網路治理議題。透過合作SIG的討論，社群成員也可就公共政策議題，研議並確立APNIC社群的正式立場。APNIC秘書處會定期向合作SIG報告APNIC本身進行的對外交流和推廣活動，並尋求SIG對這些活動的建議和指導方向。

本屆合作SIG場次的主題是「強化路由安全：最佳實踐及合作提升網路韌性」，廣邀包括工程師、公司總裁、政策制定者及其他網路安全相關機構與政府單位等背景多元的與談人，共同探索多方利害關係方如何攜手合作，共同促進並提升路由安全。

組織章程修訂

因應2023年3月收到針對APNIC執行委員會（EC）選舉的社群意見，APNIC在7月啟動組織章程修訂的社群諮詢流程，並於9月APNIC56京都會議召開特別會員大會，就組織章程修訂提案投票。

Photo by APNIC on flickr

修訂提案主要目的為增訂APNIC EC候選人的參選條件，如新增規定確保EC的獨立性及地區多元代表性、禁止與APNIC處於官司對造之個人參選、限制外部組織對EC成員的控制、新增選舉委員會等，以改善彌補EC選舉流程的弱點。所有修訂提案皆於2023年9月14日特別會員大會中表決通過。

「今年網路治理最熱門議題—WSIS+20到底是什麼？」座談重點回顧

史上首屆資訊社會世界高峰會（World Summit on the Information Society，WSIS）分為兩階段，分別於2003年日內瓦及2005年突尼斯舉行。其中，突尼斯議程為「網路治理」寫下定義，就此啟動自2006年起，每年舉辦的網路治理論壇（Internet Governance Forum，IGF）。

本場活動將簡介 WSIS 發展至今的重要里程碑，包括多邊模式與多方利害關係模式在網路治理歷史中的角力，以及今明兩年的WSIS+20回顧流程。座談則邀請到國內利害關係人代表，共同探討 WSIS+20 的核心議題，亦即當前全球所面對包括網路安全、DNS濫用、數位不平等待解決議題。

臺灣網路治理論壇理事長吳國維首先回顧了網路治理的演進。他提到了三份重要的歷史文件，即Ira C. Magaziner的《建立全球電子商務框架》白皮書、2005年的網路治理工作小組報告、以及聯合國2005年的突尼斯議程。

2005年的突尼斯議程提出了多方利害關係人模式的採用，並啟動了聯合國網路治理論壇（IGF）。吳理事長指出，縱然IGF取代了2005年後的WSIS功能，但網路社群對ITU（國際電信聯盟）負責管理網際網路仍持懷疑態度，反對在ITU討論網路治理議題。不幸的是，臺灣無法參與WSIS和IGF活動，因為它們屬於聯合國的領域。

Magaziner的白皮書則強調了網際網路對民主的重要性，但也預見了一些問題，如隱私、內容管制、跨國稅收和版權保護。

最後，吳理事長提到了2016年將IANA功能轉移給ICANN的重要時刻，這是多方利害關係人模式的里程碑。然而，聯合國、ITU和政府組織一直試圖擴大網路治理權限。隨著WSIS二十年回顧（WSIS+20）即將來臨，網路社群和臺灣都將面臨新的挑戰和討論。

理律法律事務所合夥人曾更瑩律師認為WSIS+20是檢討多方利害關係人模式的機會，特別關注ICANN的權責和功能是否會受到影響。她強調政府在ICANN的政府諮詢委員會（GAC）中仍有一定份量，並且GAC的建議受到董事會的重視，這維持了多方利害關係人模式的平衡。

資訊工業策進會楊仁達副執行長指出，網路已成為現代社會不可或缺的一部分，但一般民眾對於網路的管理和本質知之甚少。他表示，若無法釐清網路的本質，如何有效管理它將成為一個問題。

數位經濟暨產業發展協會詹婷怡副理事長分享了她的經歷，強調WSIS聚焦於網路治理，但治理不僅僅是一個機制，還牽涉到一套遊戲規則。她提到了最近由聯合國提出的全球數位盟約（Global Digital Compact，GDC），正就各種關鍵網路治理議題徵詢全球社群意見中，值得我們持續關注。詹副理事長認為，WSIS中我們最需關注的，是機制與議題之間的角力。

TWNIC黃勝雄執行長表示目前針對WSIS+20的討論，聚焦於2025年WSIS會不會變更網路治理框架，他認為答案是肯定的。ITU從WSIS+10就野心勃勃，可能會試圖加強政府的控制力，但要取代現有的多方利害關係人模式則難以實現。他強調「管理」和「治理」之間的區別，並指出多方利害關係人模式的事實地位在網路治理中扮演了重要角色。

如前所述，無論IGF或WSIS都是聯合國主辦活動，臺灣無法參與。吳理事長詢問與談人是否有任何突破限制的創意參與方案。曾律師分享自身經驗，的確在許多國際場域難以用「臺灣」身份參與討論。但她強調，只要有足以分享、借鏡的經驗和知識，還是會吸引別人主動來取經和交流。

其他與談人皆同意上述論點，如楊仁達副執行長提出應實質發揮影響力，創造典範生態；詹副理事長則建議在正視困境的同時，善用各種不同的管道、論壇和國際大會，正面突破並積極參與。黃執行長則沿用井田制比喻，指出此類參與付出和回收不成正比，但仍期待各位共襄盛舉。

點此觀看完整活動影片

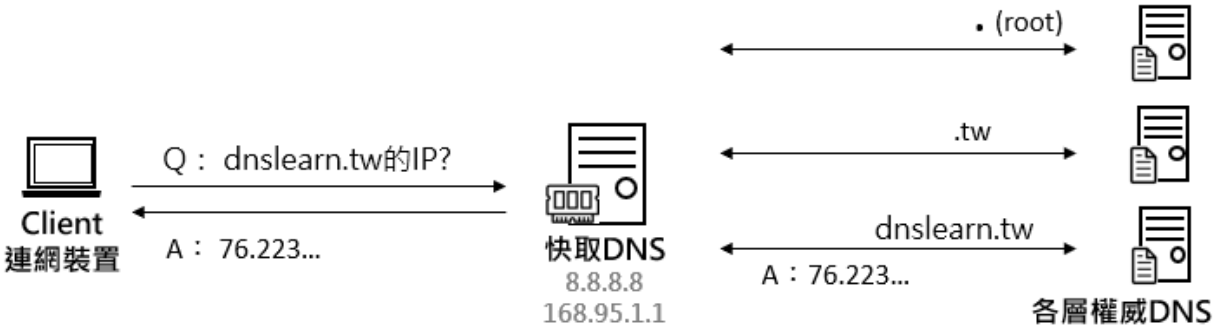
專欄文章｜當代DNS權威主機的挑戰與對策

作者：林方傑｜中華電信網路技術分公司 股長

什麼是DNS權威主機？

Domain Name System（以下簡稱DNS）是網路運作的關鍵基礎之一，負責域名與IP等資料的對應。DNS可簡單分為「快取」與「權威」兩類。前者（或稱「resolver」）負責面對用戶端（以下簡稱clients）、受理其任何域名任何DNS紀錄的查詢，並尋找域名DNS紀錄的資料源頭，從而取得答案再回饋給clients。8.8.8.8、168.95.1.1皆屬此類。而所謂「域名DNS紀錄的資料源頭」即所謂DNS權威主機（authoritative name server，以下簡稱權威DNS）。

每個域名會有其權威DNS處理其DNS紀錄的管理與發布，並回應快取DNS的資料需求。這也代表著在權威DNS的query log中，所記載的來訪IP其實屬於幫忙解析的快取DNS而非真正對DNS紀錄有需求的clients。另外，權威DNS也不宜限制服務對象，否則所轄的域名對部分clients而言會變得無法解析。有別於快取DNS可能由其建置/維護者限縮client來源（比如電信業者只服務其客戶），權威DNS的開放性（理應服務任何快取DNS）是特色也是維護的挑戰。



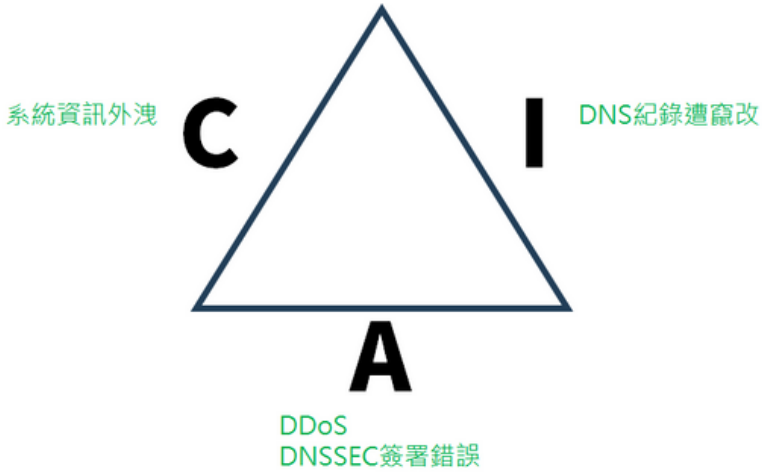
圖｜DNS分類與互動／林方傑繪製

DNS權威主機面臨哪些挑戰？

我們用資安CIA三角來盤點權威DNS所面臨的挑戰。關於機密性（Confidentiality），雖然DNS紀錄屬公開資料、權威DNS的query log也不涉及client上網行為與隱私，但權威DNS的運作環境細節（如伺服器與網路設備的規格、帳密權限、軟體組態、系統架構等）都該被妥善保護。

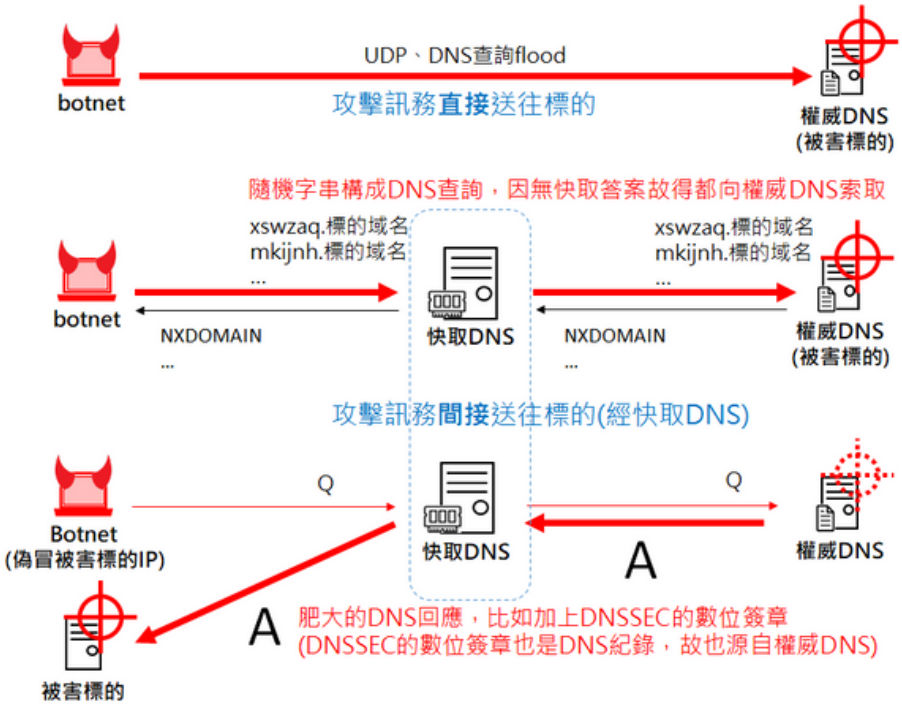
若這些機敏資訊遭洩漏，則系統弱點被發現被利用等風險將大幅提高。若權威DNS遭駭，則所轄域名之DNS紀錄將面臨嚴重的完整性（Integrity）威脅。因權威DNS是域名DNS紀錄的源頭，若落入駭客手中，則駭客就算不發動「快取汙染」（cache poisoning）也能誤導clients，效果甚至更廣更好。對於可用度（Availability）最大的威脅則非DDoS莫屬。

DNS DDoS的分類方式五花八門（註1），有冠上協定名稱的UDP洪水攻擊（User Datagram Protocol floods）、有形容攻擊特徵的「放大攻擊」、「反射攻擊」等。筆者建議從攻擊流量的路徑開始理解。從權威DNS的觀點，筆者將DDoS攻擊流量路徑略分為直接與間接兩種。前者如殭屍電腦鎖定著被害標的直接發送異常且大量的UDP或DNS查詢封包；後者則好比「借刀殺人」，簡述已知手法如下：



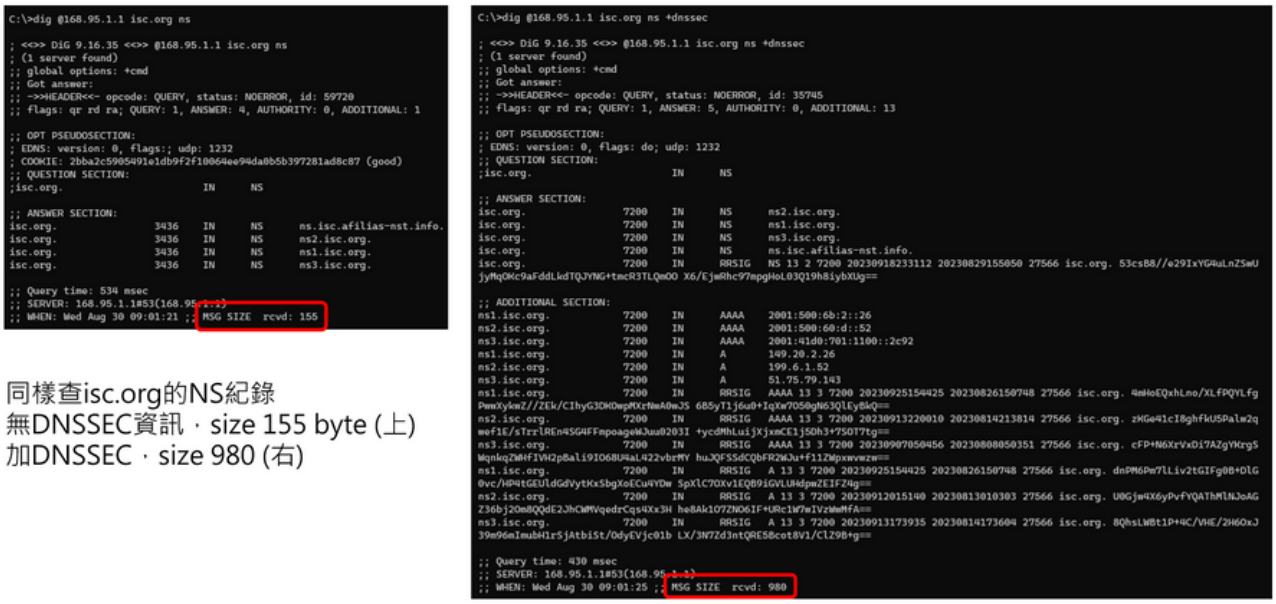
圖｜權威DNS的挑戰／林方傑繪製

- 殭屍電腦先掌握標的權威DNS所轄的域名，再向快取DNS查詢這些域名的DNS紀錄。由於快取DNS必須從域名的權威DNS取得DNS紀錄內容，普通的DNS查詢便可觸發快取DNS向標的權威DNS發送流量。若再以隨機字串搭配域名組成DNS查詢（快取DNS的記憶體難有現成答案），將迫使快取DNS向權威DNS索取更多回應、耗費標的的量能（此即「NXDomain attack」）。
- 攻擊方偽冒攻擊標的之IP向快取DNS提出DNS查詢。當快取DNS回覆解析結果時，便會將DNS回應封包送往被偽冒的IP。如果再搭配回應封包肥大的DNS查詢，就可更高效率地耗費攻擊標的頻寬，構成「DNS reflection/amplification attack」（註2）。雖然此攻擊手法中權威DNS不見得是攻擊標的，但已有報告指出「Domain Name System Security Extensions（以下簡稱DNSSEC）」可能遭濫用成發動放大攻擊的現成素材（註3），這提高了權威DNS被捲入攻擊的機率。



圖｜DNS DDoS手法與路徑／林方傑繪製

DNSSEC是種保護DNS紀錄在傳輸過程中的資料完整性之安全協定（註4），原理是賦予DNS紀錄數位簽章供解析時查驗（也因此會加大DNS回應封包的size成為放大攻擊的現成素材）。也必須注意的是，DNSSEC數位簽章的產製與維護程序有相當的複雜度，若出錯將導致域名被判定為DNSSEC簽署有問題而無法解析，反而成為可用度威脅。



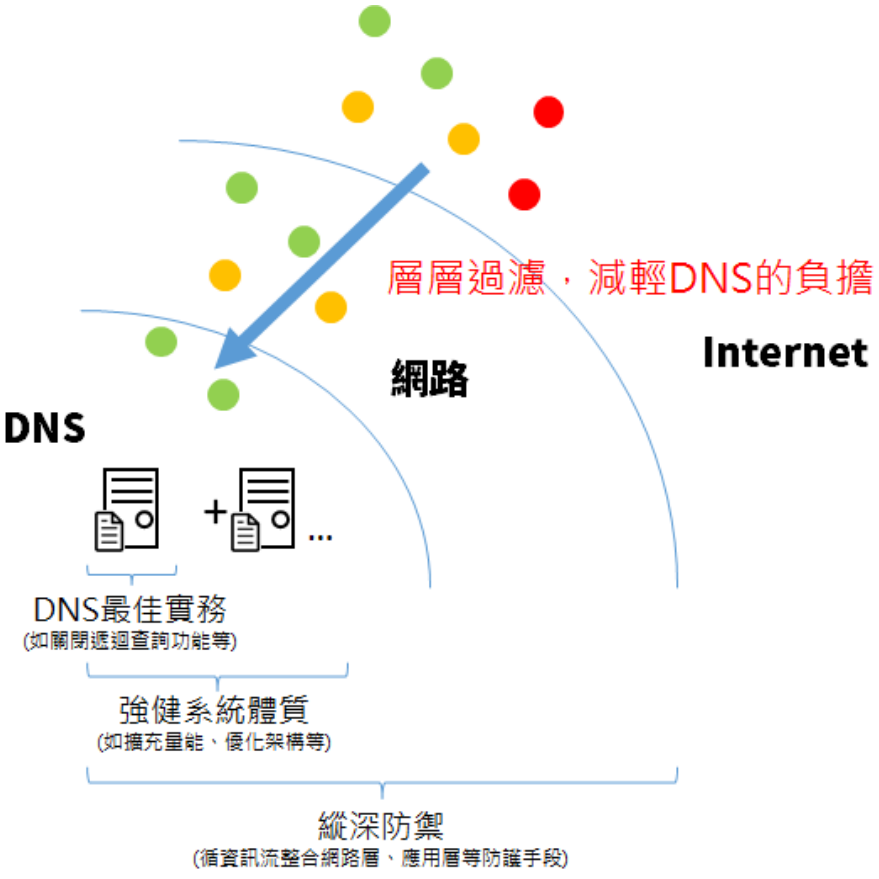
圖｜DNSSEC加大DNS回應封包size／林方傑繪製

有哪些對策可強化權威DNS的安全？

那麼，該如何強化權威DNS的安全呢？可參考下列方向：

1. 遵循最佳實務：各位可優先關注ICANN的「KINDNS」倡議（註5），該倡議旨在為DNS制定一個清晰的營運最佳實務框架（註6），https://kindns.org/提供許多關於DNS部署、設定的詳細建議與指引。
2. 強健系統體質：比如藉增購/汰換設備、優化架構、導入外部資源等以擴充量能、提高韌性。另外建立監測與告警機制可加速緊急處理程序的觸發。
3. 應用縱深防禦策略：建議循資訊流，將DNS主機前所經環節也納入防護機制的部署範圍。不管是使用網路或資安設備、甚至資安服務，若能先濾除明顯異常的封包，多少能提高從攻擊存活的機率。

限於篇幅無法詳述細節，謹以本篇的示意圖與文字簡述分享筆者對權威DNS安全的想法，並與各位共勉。



圖｜強化權威DNS安全的方向／林方傑繪製

| 註解 |

1. 李宗翰 (2014)。DNS DDoS攻擊的類型。IThome。檢自：https://www.ithome.com.tw/tech/87818 (May., 2014)
2. Ben April (2013)。消除DNS反射阻斷式攻擊 (Denial-of-Service Attacks)。資安趨勢部落格 (trendmicro.com.tw)。檢自：https://blog.trendmicro.com.tw/?p=4289
3. Marcin Nawrocki (2022)。Tracing the DDoS attack ecosystem from the Internet core。APNIC Blog。檢自：https://blog.apnic.net/2022/04/28/tracing-the-ddos-attack-ecosystem-from-the-internet-core/?fbclid=IwAR2c6k-gfS8q_wVl4vD_bxTxQRDgf0ZpotqsXHczcyH5uWOEyUqCW3Xn2Pc
4. TWCERT (2019)。TWCERT-電子報-資安小知識-DNS資安(下)。檢自：https://www.twcert.org.tw/newepaper/cp-92-4485-1b51f-3.html
5. ICANN (2022). KINDNS 首頁。ICANN。檢自：https://kindns.org/ (Sep., 2022)
6. 美通社 (2022)。ICANN 倡議促進互聯網安全最佳實踐。digitimes.com.tw。檢自：https://www.digitimes.com.tw/tech/dt/n/shwnws.asp?id=0000644389_WKR24V4W9HSMZR8KLGGES

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/QSGbX8S7reEvJk7m8