計畫編號：NCC-T109-033

110 年委託研究報告

網域名稱涉有違反相關法律之實例研究及處置建議委託研究
期末報告

計畫委託機關：國家通訊傳播委員會

中華民國 110 年 10 月

本報告書僅供

政府機關參考

請勿轉載

計畫編號：NCC-T109-033

110 年委託研究報告

PG11003-0075

網域名稱涉有違反相關法律之實例研究及處置建議委託研究
期末報告

受委託單位

恆業法律事務所

計畫主持人 戴豪君博士

協同主持人 余啟民博士

執行協同主持人 林繼恆主持律師

專案顧問 胡博硯博士

專案經理（計劃聯絡人） 李璨宇律師

研究期程：中國民國 110 年 3 月至 110 年 12 月

研究經費：新台幣 98 萬元

中華民國 110 年 10 月

目次

圖目錄

表目錄

提要

關鍵詞：網域名稱、網域名稱濫用、網域名稱回應政策區域、網域名稱註冊管理機構、網域名稱受理註冊機構、財團法人台灣網路資訊中心、網際網路名稱與數字位址分配機構、馬尼拉原則、網域名稱濫用架構

一、隨著網際網路的蓬勃發展以及網路平臺抒發意見、自行架設網站等模式已完全融入生活中，其所衍生的網路違法事件亦與日俱增。面對眾多的網路違法事件，有人民對相關違法事件之檢舉、有行政機關就其管轄事務向國家通訊傳播委員會（National Communications Commission 下稱：通傳會、NCC）通知，亦有檢警單位為防止犯罪進一步通知業者先行停止解析網域名稱。惟實際進行網域名稱濫用之處置上，卻因現有法規不足，未有明確之行政處分標準作業程序，導致各機關僅以發函通知之方式，通知通傳會處理網域名稱濫用之行為。

二、對此，本研究針對網域名稱涉有違反相關法律之實例進行研究，及提出處置建議。內容包含研析美國、日本、馬來西亞及英國等國外立法例（第四章第二節）；盤點我國針對網路內容或使用者行為之違法態樣，及我國網域名稱註冊管理機構監理法規（第四章第三節）；研析我國利用 DN 跨國追查蒐證及進行行政處分之困境（第二章第一節）；研析網域名稱濫用之自律或他律機制（第二章第二節）；實務網域濫用案例之研析（第三章）；訪談行政機關及業者，並舉行座談會收集利害關係人意見（第五章）後，提出我國面對網域濫用之監理建議（第六章）。

三、本研究研析美國、日本、馬來西亞及英國有關處理網域名稱濫用之處置手段、網域名稱濫用代表案例，及訪談利害關係人，歸納出以下研究發現：

（一） 日本設有專責之民間機構一般社團法人安全網路協會（Safer Internet Association，下稱 SIA）負責認定網域名稱內容濫用之態樣，針對內容態樣區分為「違法內容」及「不當內容」，由 SIA

將上述內容通知特定主管機關、檢警單位、網路平臺業者及內容創作者。除做為檢警單位開啟偵查之手段外，亦希望網路平臺業者及內容創作者透過自律之機制，直接刪除特定內容，以作為對網域名稱涉及內容濫用時之處置。惟對於「特定網域名稱之取消、停止解析」之情況，日本並無法規明文允許行政機關可以對特定網域名稱做出取消或停止解析之行政處分，對涉有技術濫用之網域名稱亦然。是以，日本考慮是否制定相關法規，對於網域名稱技術濫用賦予行政機關為「取消、停止解析網域名稱」處分之權限。

（二） 確保言論自由為美國立國方針，在川普總統上任以來，雖曾出現是否制定對網路內容進行規範管理之法規，惟最後均未成立。是以，針對網域名稱濫用之處置，司法機關做為美國對違法網域名稱濫用之唯一處置主體。其中，美國特有的民事訴訟對物扣押制度可使受不當網域名稱侵害之人在該侵害網域名稱所有人不明之情況下，透過民事對物扣押程序，讓法院以判決之方式要求美國之網域名稱註冊管理機構取消特定網域名稱或對該網域名稱進行停止解析。

（三） 馬來西亞針對網域名稱濫用則給予馬來西亞通訊傳播暨多媒體委員會（Malaysian Communications and Multimedia Commission，下稱 MCMC）極大之權限，甚至在 MCMC 的職責中即提到，「監督及監測通訊傳播及多媒體活動」、「社會管制（Social regulation）」均為其主要任務。為確保 MCMC 管制馬來西亞所有網域名稱濫用之權限，據通訊傳播暨多媒體法（Communications and Multimedia Act 1988，下稱 CMA）概括授權 MCMC 阻隔各類型網域名稱之權利。

（四） 英國於智慧財產領域，依 1988 年英國著作權、設計和專利法第 97A 條，在 ISP（Internet Service Provider，下稱 ISP）業者，實

際上知悉他人利用其提供之網路服務進行侵權行為時，智慧財產權人得請求法院核發禁制令將違法之網域停止解析。又針對網域名稱兒童情色內容濫用問題，其主要仰賴 ISP 業者的自我監控，由非營利機構—網路觀察基金會（Internet Watch Foundation，下稱 IWF）負責協調處理。IWF 會追蹤其網站之註冊地區，若該註冊地區在英國，則會直接向該註冊者發出通知要求刪除該內容，若註冊地區在國外，則會聯繫並與該國之警察合作，以該國之法制或流程刪除該等內容。是以英國針對網域內容濫用主要係依司法機關之禁制令及民間自律。

（五） 透過訪談利害關係人，如我國網域名稱註冊管理機構財團法人台灣網路資訊中心（Taiwan Network Information Center，下稱 TWNIC），知悉註管機構系扮演網路基礎建設者之角色，不宜自行判斷網域名稱濫用與否；及透過訪談網路內容防護機構（Institute of Watch Internet Network，下稱 iWIN），知悉其扮演我國民間第三方機構，專責處理網路內容涉及侵害兒少身心之申訴及後續通報，並有良好的成效。此種民間從下至上之網路監理模式，係可複製用於處理其他網域名稱內容濫用。

四、本研究除利用文獻分析法進行國內外相關法制之研究外，亦透過行政機關訪談、業者代表訪談及舉辦一場座談會，邀請產學界，蒐集來自產業界代表、網域名稱濫用處置之專家學者關於本研究相關議題之建議，以使未來網域名稱濫用處理制度更為務實可行並符合我國國情需求。

五、本研究針對網域濫用提出以下建議：

（一） 針對網域技術濫用依網域名稱濫用框架（DNS Abuse Framework）已針對網域濫用定義五種類型包含：一、惡意軟體（Malware）；二、殭屍網路（Botnets）；三、網路釣魚（Phishing）；四、偽冒嫁接（Pharming）；五、以垃圾郵件之形式達成以上濫用之行為 （Spam），並明確指出註冊管理機構知悉有前述之網

域名稱濫用情形時，註冊管理機構必須有所作為。然而具體作為義務及處置手段於我國法律多未有明文。是以針對網域技術濫用應有法律授權，使主管機關及註冊管理機構得快速進行網域技術濫用的各項處置。

（二） 針對網域內容濫用之監管涉及限制言論自由，基於我國網域名稱註冊管理機關 TWNIC 與網際網路名稱與數字位址分配機構（Internet Corporation for Assigned Names and Numbers ，下稱 ICANN）之註冊管理機構協議，其並無義務負責監督、管理網頁內容，且也無權限審查網頁內容而取消網域名稱，此外目前各國並無由註冊管理機構自行認定內容是否內容違法之前例。故考量內容濫用之類型眾多且事涉專業判斷，宜另由司法或專業機構負責認定。目前我國有關網路內容涉及侵害兒少身心之申訴及處理，係由民間第三方機構 iWIN 負責，處理範圍包含色情、暴力、恐怖、血腥、有害物品、及其他有害兒少身心健康內容等六大類。未來可考量將 iWIN 之處理範圍擴大，或另設專責民間第三方機構以解決如傳染病防治、婚姻媒合、日租套房等網域名稱內容違法不當之通報及處理。此外，盤點我國法規，僅有兩部法規分別是兒童及少年福利與權益保障法第 46 條及動物傳染病防治條例第 38 條之 3，明文授權該管行政機關將經其認定為違法之網域名稱為限制接取、瀏覽及移除等措施。是以本於網域名稱內容違法態樣眾多及主管機關之權責，各目的事業主管機關宜於主管法規內明訂須將網頁內容刪除、停止解析網域名稱之態樣（相關立法方向可參考第陸章第五節），以利第三方機構或行政機關針對網域名稱內容違法不當情事進行審酌，並通知行為人、註冊管理機構、受理註冊機構及 ISP 業者。

Abstract

Keywords: Domain Name, Domain Name Abuse, Domain Name Abuse Framework, DNS RPZ, Domain Name Registry, Domain Name Registrar, TWNIC, ICANN,

1. In recent years, most internet users express their opinions by setting up their own websites and/or leaving messages on various Internet platforms. The development of the Internet has led to an increasing number of illegal Internet incidents. In response to such network violations, in addition to people reporting violations to the administrative agency and the administrative agency's resultant notification to the NCC, prosecutors and police units have taken steps to stop resolving domain names. However, current laws and regulations for the handling of Domain Name Abuse are insufficient, and there is no standard operating procedure for the handling of such matters.
2. Instead of dealing with Domain Name Abuses, various agencies only notify the NCC to deal with those problems. This research will study and analyze the regulatory models of Domain Name Abuse in various countries to reflect on Taiwan's Domain Name Abuse handling mechanism.
3. This research studies Domain Name Abuse cases and the relevant regulations, and will then propose solutions and advice as its conclusion. This research will analyze foreign legislation including regulations from the United States, Japan, Malaysia and the United Kingdom in Chapter 4, Section 2; present case studies in Taiwan regarding illegal behavior and content in the Domain Name Abuse context, and Taiwan's Domain Name registry supervision regulations in Chapter 4, Section 3; demonstrate the difficulty in investigating and administratively resolving cross border cases

in Taiwan in Chapter 2, Section 1; analyze the regulations or self-regulations of the Domain Name community; elaborate on the Domain Name abuse cases in Chapter 4; introduce the service providers', administrative agencies' and other stakeholders' opinions through interviews and a forum in Chapter 5; and finally propose our advice on how to handle Domain Name Abuse issues.

4. This research analyzes the methods used to deal with Domain Name Abuse and important cases in the United States, Japan, Malaysia and the United Kingdom, and has interviewed relevant stakeholders. These research findings can be summarized as following:

   (1) Japan established a non-government organization, Safer Internet Association （"SIA"）, which is responsible for determining the abuse of Domain Name Content (the content is divided into "illegal content" and "inappropriate content"). Once such content is identified, the SIA then notifies specific agencies, police units, online platform operators and content creators of the above content. In addition to serving as a means for police units to initiate investigations, the intention is also that network platform operators and content creators can directly delete specific content through a self-discipline mechanism to achieve immediate disposal of "Domain Name Content". However, Japan has no laws or regulations allowing administrative agency to order the deletion of such content or to stop the resolving of any Domain Name, even when internet virus is found. Therefore, Japan is also considering whether to introduce relevant laws and regulations to give administrative agencies the authority to "remove specific Domain Name and stop Domain Name Resolving".

   (2) After President Trump took office, there have been discussions about whether to introduce specific legislation to control online content;

however, freedom of speech is the foundation of the Constitution of the United States, and Congress ultimately vetoed the above-mentioned bill. Therefore, the United States judiciary remains the only body able to deal with Domain Name Abuse. In particular, a unique civil remedy in the United States allows people who have been infringed by Domain Name to use the “in rem action” process when the owner of the domain is unknown, whereby the court will require the Domain Name Registry to delist or stop resolving a specific domain.

(3) In response to Domain Name Abuse, Malaysia has given the Malaysian Communications and Multimedia Commission （”MCMC”） great authority, and even listed "Supervise and monitor communications and "Multimedia activities" and "Social regulation" as MCMC’s main tasks. In order to ensure that the MCMC controls the abuse of all domains in Malaysia, the Communications and Multimedia Act 1988 generally authorizes the MCMC to block all types of domains.

(4) In the field of intellectual property in the United Kingdom, in accordance with Article 97A of the British Copyright, Design and Patent Act of 1988, intellectual property owners may request the court to issue a prohibition order to stop the resolving of illegal domain, when the Internet Service Provider（”ISP”） knows that others are using the Internet services provided by it to commit infringements. In response to the DNS Abuse of child pornography on the Internet, it mainly relies on the ISP industry’s self-monitoring and is coordinated by the non-profit charity, the Internet Watch Foundation （”IWF”）. IWF will trace the jurisdiction in which the website is registered. If it is registered in the UK, it will directly notify the registrant to delete the image or video. If the registered address is abroad, it will contact

the police of that country to delete the illegal content via the country's legal system or process. Therefore, the handling of domain content abuse in the United Kingdom is mainly based on judicial injunctions and civil self-discipline.

(5) Through interviewing relevant stakeholders - Taiwan Network Information Center for instance - this research suggests that Domain Name Registry is not an appropriate body to determine whether there is Domain Name Abuse. And through interviewing iWIN, this research finds that it is an ideal model to let an independent agency be responsible for handling complaints and reporting content regarding internet content that is harmful to children and adolescents. This "bottom up" internet governance approach should be used in other fields of Domain Name Content Abuse.

5. In addition to the comparative study on foreign legal systems, this research also conducted interviews with administrative agencies, interviews with industry representatives, and held a coordination meeting for research and business communication, inviting industry and academia to collect the relevant topics of this research, so as to make the future domain abuse processing system in Taiwan more practical and feasible and better meet the needs of Taiwan's national conditions.

6. This research initially proposes the following suggestions for domain abuse:

(1.) For domain abuse of technology: five types of domain abuse have been defined: 1. Malware; 2. Botnets; 3. Phishing 4. Pharming; 5. Achieve the above abuse in the form of spam. However, the specific obligations and disposal methods have not been expressly stated in law; Therefore, there should be legal authorization for domain abuse of technology, so that the competent authority and the registration agency can quickly

remove the technology abuse domain and stop the resolving method through RPZ.

(2.) The supervision of the domain abuse of content involves restrictions on freedom of speech. Based on the registry agreement between the domain name registration authority （i.e., TWNIC） and ICANN, it is not obliged to supervise and manage the content. In addition, there is currently no precedent for the registration authority to determine whether the content is illegal. Therefore, considering that there are many types of content abuse, and the matter involves professional judgment, it should be determined by judicial or professional institutions.

(3.) At present, the complaint and handling of online content in our country involving violations of children's bodies and minds is the responsibility of the third-party organization iWIN Internet Content Protection Agency. The scope of processing includes pornography, violence, terror, blood, harmful substances, and other violations harmful to children and teenagers. In the future, the processing scope of the iWIN network content protection agency can be expanded, or to set up a special private third-party organization to handle illegal and improper network content such as infectious disease prevention, marriage matchmaking, and daily rental suites. In addition, the only two laws and regulations in our country are Article 46 of The Protection of Children and Youths Welfare and Rights Act and Article 38-3 of Statute for Prevention and Control of Infectious Animal Diseases, which expressly authorize the administrative agency to determine the content of the website as illegal and then restrict the accessibility and browsing of them. Because of the numerous forms of illegal domain content, the competent authority should clearly stipulate in the competent laws and

regulations that the domain content must be deleted and ceased to be resolved, to facilitate third-party agencies or administrative agencies to deliberate on illegal and improper content of the domain, and to notify the perpetrator, the registration agency, the registration agency, and the ISP.

第一章緒論

第一節 研究背景

隨著網際網路的蓬勃發展以及網路平臺抒發意見、自行架設網站等模式已完全融入生活中，其所衍生的網路違法事件亦與日俱增。面對眾多的網路違法事件，包含違法內容及以網站散播網路病毒等事件，有人民對相關違法事件提出檢舉、有行政機關就其管轄事務向通傳會請求將網站內容刪除或取消網域名稱之通知，亦有檢警單位為防止犯罪進一步通知業者先行停止解析網域名稱。惟實際進行網域名稱濫用之處置上，卻存在法規不足，未有行政處分標準作業程序之情況，導致各機關僅以發函通知之方式，通知通傳會處理網域名稱濫用之行為。為處理現行對網域名稱濫用處理缺乏相關法規之情況，本團隊除會對特定網域名稱作成行政處分之要件進行研析外，亦會參酌各國對網域名稱濫用之規管模式，以利我國於未來建置完善之網域名稱濫用處理機制。

盤點我國所有可用於規範網際網路內容或使用者行為違法態樣之規定，僅有兩條規定明文授權該管行政機關將經其認定為違法之網站內容為限制接取、瀏覽，甚至是移除之措施，上述規定，分別是兒童及少年福利與權益保障法第 46 條之 1 及動物傳染病防治條例第 38 條之 3。是以，如行政機關欲通知網域名稱註冊管理機構就違反其餘規定（諸如：公職人員選舉罷免法、毒品防制條例等實體法）之網域名稱，為限制一般人民閱覽之行政處分時，並無具體法律依據。如涉及刑事犯罪之網路內容或網域名稱，尚得依檢警單位向法院聲請扣押來達到限制接取之目的，惟其餘監理性行政法規，如缺乏刑事法之依據，將欠缺對違法網域名稱濫用行為做出行政處分之法源依據。

由上可知，就網域名稱為處置之技術，作為「違法網路使用行為」之處置手段在我國尚不成熟，方有前述法規命令不完備之情況。是以，本團隊特別選定四個國家之立法例作為參考，分別是日本、美國、英國及馬來西亞。在監理方面，這四個國家針對網域名稱濫用有著不同之監理方式，以及對網路內容處置及言論自由保障有不同權衡態度。其中包含對網路內容規範最為寬鬆之美國，僅司法機關為監理網域名稱之唯一主體；其次為處於監理光譜

中較偏向寬鬆之日本，其雖由第三方機構 SIA 初步審查相關網域名稱濫用行為態樣，惟 SIA 於判斷後僅能通知相關業者、檢警單位，SIA 本身及任何行政機關均無對網域名稱濫用行為，進行網域名稱處置之權限。而最嚴格之監理方式為馬來西亞，依照該國 CMA 之規定，MCMC 有全面阻隔所有網站的權限，從 MCMC 實際封鎖之數量來看，超過 70%之各類型網站均是由 MCMC 封鎖。

本研究於行政處分部分將以現有之兒童及少年福利與權益保障法第 46 條之 1 及動物傳染病防治條例第 38 條之 3 作為基礎；針對司法機構之處置措施，將以我國第一個扣押網域名稱的 110 年度聲扣字第 11 號裁定做為基礎，並輔以國外立法例，包含日本、美國、英國、馬來西亞等各種不同網域名稱濫用規管密度國家之作法，同時於法制面、程序面提出建議，期能研擬出符合我國國情、務實可行、公平有效之網域名稱濫用處置方式，以利通傳會從程序面及法制面向各機關提出建議，及協助建置符合我國的網域名稱濫用處置體系，作為後續法規政策研擬之參考。

第二節 研究方法

本案研究流程圖如下（細部說明詳如後）：

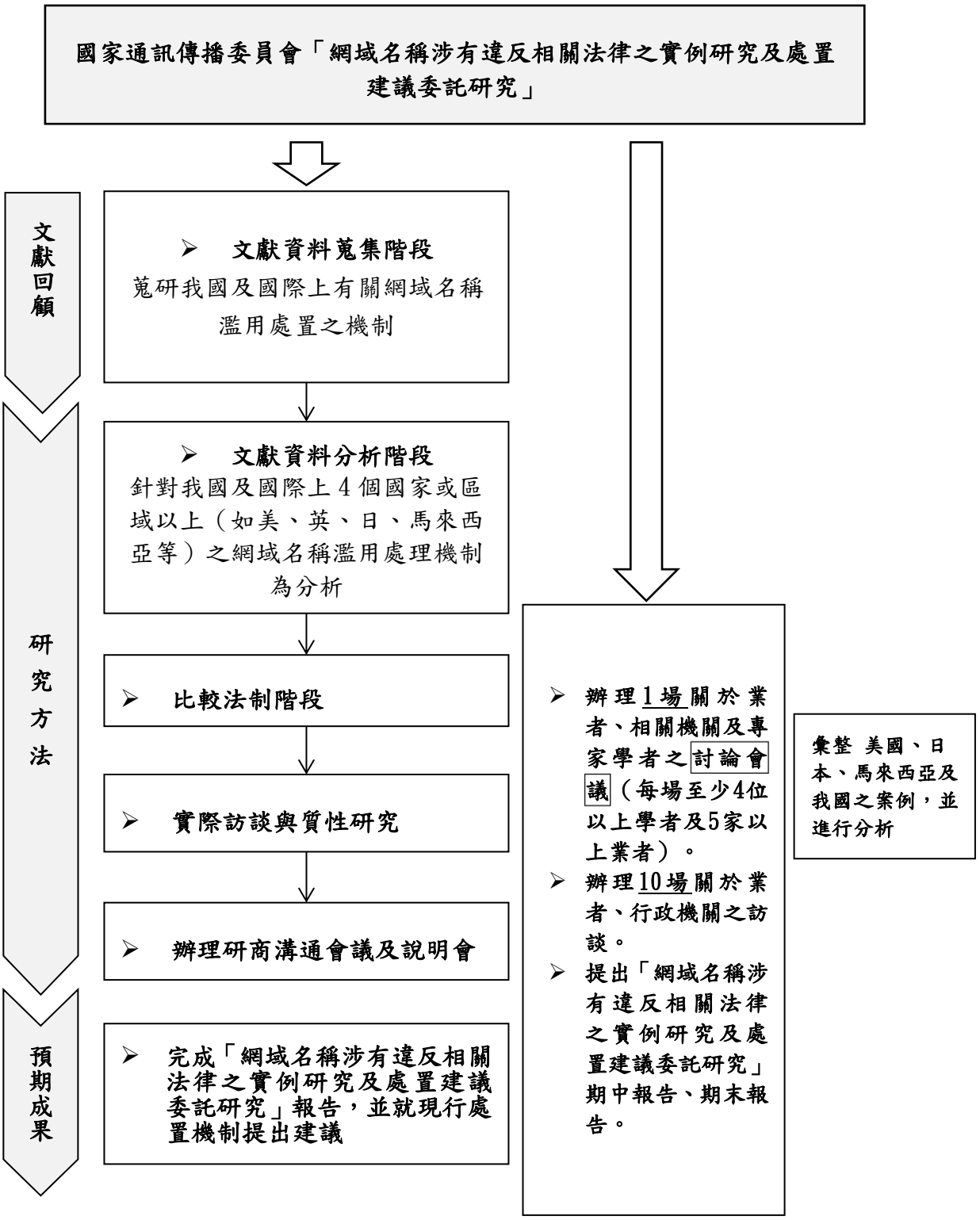


圖 1 研究流程圖

本研究採取以下研究方法（說明詳如後）：

一、 「**文獻分析法**」：進行研究資料蒐集，範圍將包括初級資料（如各國之法制規範、案例或官方文件）與次級資料（如書籍與期刊論文），並將文獻資料進行分析歸納。

二、 「**比較法制研析**」：研析將各國之網域名稱監管機構監督與管理機制、行政措施，並與我國現行法制、案例為比較分析與參採性分析。

三、 「**焦點團體研究法**」：本研究之研究目的係為提出具體之「網域名稱涉有違反相關法律之實例研究及處置建議委託研究」建構建議，故須利用質性研究法中之「焦點團體研究法」，舉辦座談會及訪談，蒐集來自產、官、學界之意見，以實際了解法制現況、產業實務，並協助通傳會、相關行政機關就現行之處置機制提出建議。

第一項　文獻分析法

一、 文獻資料蒐集

（一） **各國網域名稱濫用行為之處理官方網站蒐集**：蒐集我國及各國就網域名稱濫用行為處置機制、相關案例等。

（二） **外國法規資料庫實例蒐集**：例如 Lexis、Westlaw 等，以蒐集各國之相關網域名稱濫用行為處置法規資訊及國際案例。

表 1 資料庫列表

資料庫名稱	簡介	圖示
Lexis	可蒐集美國相關法規。	LexisNexis™
Westlaw	可蒐集各國法規。	Westlaw®

資料庫名稱	簡介	圖示
ICANN 官方網站	查找註冊管理機構協議（Registry Agreements）及註冊管理機構-受理註冊機構協議（Registry-Registrar Agreement）	
一般社団法人セーフィーインターネット協会（SIA）官方網站	可蒐集民間針對網域名稱內容濫用之處理準則	
日本總務省官方網站	可蒐集官方針對網域名稱名濫用之相關政策	
馬來西亞通訊傳播暨多媒體委員會（MCMC）官方網站	可蒐集官方針對網域名稱濫用之相關法規、執掌與政策	 OFFICIAL WEBSITE OF SURUHANJAYA KOMUNIKASI DAN MULTIMEDIA MA MALAYSIAN COMMUNICATIONS AND MULTIMEDIA COMMISS https://www.mcmc.gov.my/en/home
Thomson Reuters PRACTICAL LAW	可蒐集關於馬來西亞 1998 年《通信和多媒體法》（CMA）之法規介紹與實務操作	
美國.US 網域名稱註冊管理機構之官方網站	可蒐集美國註冊管理機構之相關資訊與服務內容。	

二、 文獻資料分析

（一） 分析國際上各國就法制面、組織面就網域名稱濫用行為處置之機制。

（二） 分析我國處理網域名稱濫用行為處置之相關單位，如網域名稱註冊管理機構、衛生福利部（下稱衛福部）：、行政院農業委員會（下稱農委會）等，包含相關機關之組織、通報程序與效力等議題。

（三） 彙整我國及各國處理網域名稱濫用之案例，並針對處置機制、救濟程序、實際處理成效進行分析。

第二項　比較法制研析

一、 針對各國之網域名稱濫用行為處置之發展趨勢、法制現況、組織架構、監督機制及救濟與效力層面為分析。

二、 將各國之網域名稱濫用行為處置機制與我國現行法制為落差分析。將各國及世界重要組織之網域名稱濫用處理機制之作法納入我國之可行性分析（包含政策、立法、專責機構設立、網路環境、國情不同等）。

第三項　質性研究

一、 將各國與我國之網域名稱濫用行為處置案例，針對網域名稱濫用種類、阻擋網域名稱數量、處理方式或其他可供政策規劃內容等進行質性研究。

二、 除以文獻蒐集分析方式彙整各國之網域名稱濫用案例外，可配合通傳會之需求進行「深度訪談」取得行政機關或業者代表處理網域名稱濫用行為相關之書面、正式或非正式的資料，以瞭解業產業內部無法公開或無法呈現的原則與關鍵點等資訊。分析與比較並研提結論建議。

第四項　焦點團體研究法－協調研商溝通會議、說明會

由於本研究係就我國網域名稱濫用行為處置機制，進行現況釐清及就未

來提出具體法制興革建議，透過訪談及舉行座談會方式，讓通傳會、行政院資通安全處、TWNIC、專家學者、業界代表表示意見，並舉辦1場座談會（業者、行政機關及專家學者），14場深度訪談（業者代表、行政機關及民間團體），以讓不同意見之各方代表於座談會上形成意見交流，進而達成意見溝通之效果，俾利後續政策研擬與辦理。

第三節 工作項目與進度說明

一、本研究依本案需求書，期末報告已完成以下工作項目：

（一） 研析我國利用 DN 跨國追查蒐證及進行行政處分之困境及以下概念之釐清：

1. 馬尼拉中介者責任原則（Manila Principles on Intermediary Liability，下稱馬尼拉原則）
2. 網域名稱回應政策區域（Domain Name System Response Policy Zone，下稱 DNS RPZ）
3. 網域名稱濫用框架（DNS Abuse Framework）

就以上內容之說明及研析，詳請本期末報告第二章。

（二） 網域名稱濫用處理案例

研析我國及國際上針對網域名稱內容及技術濫用之處理案例：

技術濫用：

1. 美國微軟對 Conficker 殭屍網路民事訴訟
2. 日本殭屍病毒案例
3. 雪崩（Avalanche）殭屍網路國際犯罪集團案

內容濫用：

1. 美國國土安全部網域名稱暨智慧財產權打擊犯罪行動（Operation in Our Sites）

2. 110 年度聲扣字第 11 號網域名稱扣押案

3. 楓林網影音著作盜版侵權案

4. SWAG 關閉網站案

5. 「安博盒子（Unblock）」侵害著作權案

就以上內容之說明及研析，詳參本期末報告第參章。

（三） 網際網路內容或使用者行為訂有規定之各國及我國立法例

研析美國、日本、馬來西亞及英國等國家/區域之立法例，包含下列項目：

1. 法制面：分析各國網域名稱濫用處理機制之相關規範，包括自律及他律機制。

2. 組織面：分析各國處理作為之行為主體，及網路濫用行為之通報機關。

就以上內容之說明及研析，詳請本期末報告第參章。

（四） 完成以下訪談

1. 訪談行政機關：

(1) 行政院資通安全處

(2) 內政部警政署刑事警察局

(3) 交通部郵電司

(4) 行政院農業委員會動植物防疫檢疫局

2. 訪談業者及機構代表

(1) TWNIC 財團法人台灣網路資訊中心

(2) iWIN 網路內容防護機構

(3) 中華電信數位通信分公司

(4) 新世紀資通股份有限公司

(5) 亞太電信股份有限公司

(6) 鼎嘉數位有限公司

(7) 協志聯合科技股份有限公司

(8) 台灣大哥大股份有限公司

(9) 台灣之星電信股份有限公司

(10) 網路中文資訊股份有限公司

表 2 工作進度查核表

期程	期限規劃		計畫預期成果
第一階段	• 應於契約生效次工作日起 3 個工作日內上網登錄基本資料（GRB 表）。 • **契約生效次工作日起 15 日之內將乙方研究人員約定同意書（格式如附件）送交甲方備查** • 契約生效次工作日起 120 日內提出期中報告初稿中文版本 8 份。		針對各國網域名稱濫用之監督與管理機制之法制面、組織面、營運面及監督面。期中報告內並包含研究方法、進度說明、蒐集之資料、文獻分析、研究發現及建議事項及參考資資料，作為建構我國網域名稱濫用處理機制之參考基礎。
	期中報告：工作項目期限規劃		
	• 完成工作項目一（一）： 蒐集針對網際網路內容或使用者行為訂有規定之立法例（外國立法例 3 件以上；本國立法例 3 件以上），並分析網域名稱註冊管理機構法律責任	120 日內	
	• 完成工作項目一（二）： 研析我國利用 DN 跨國追查蒐證及進行行政處分之困境。	120 日內	
	• 完成工作項目一（三）： 網域名稱濫用（DNS Abuse）之自律或他律機制（馬尼拉原則、DNS RPZ 框架等）之困境及可行性分	120 日內	

期程	期限規劃		計畫預期成果
	析（濫用通知正當流程、技術可行性、比例原則認定等）。		
	• 完成工作項目一（四）： 網域名稱濫用（DNS Abuse）之國內外爭議案例研析（國際案例 2 件以上；國內案例 3 件以上），應與前揭工作項目所研析之法律或自律機制相關，並提出建議。	120 日內	
第二階段	• 應於契約生效次工作日起 240 日內提出期末報告初稿中文版本 8 份(含光碟電子檔 2 份)。 • 再依審查意見於指定期限內修正完畢送交通傳會確認，經通傳會確認無誤後，本團隊再依通傳會指定期限內提出完整期末研究報告中文版本及英文精簡版各 4 份，並提交計畫摘要（中、英文版）、完整研究報告之全文電子檔光碟片 1 式 2 份。		
	期末報告：工作項目期限規劃		
	• 完成工作項目二（一）： 於履約期間訪問相關行政機關（至少 3 家）、網際網路服務業者（至少 7 家），以了解實務上的困難及需求。。	240 日內	透過廣度與深度之訪談，取得網域名稱濫用處理相關之書面、正式或非正式的資料，以瞭解網際網路服務產業內部無法公開或無法呈現的原則與關鍵點等資訊，以利通傳會全面性的瞭解與統計。
	• 完成工作項目二（二）： 邀集相關專家學者至少 4 人、網際網路服務業者至少 5 家，召開討論會議 1 場次	240 日內	就網域名稱濫用及相關研究範圍內之法制議題，進行實務暨學術之研討，協助通傳會針對業者進行網域名稱濫用之監督及管理辦法之說明，以利通傳會推動對網域名稱濫用行為之自律及他律監理。
	• 完成工作項目三（一）：	240 日內	以利通傳會推動網域名稱之自

期程	期限規劃		計畫預期成果
	提出「外國人註冊使用網域名稱(如「.tw」、「.com」)架設網站，其網站內容或網路使用者行為涉違反我國法律時」，我國網域名稱註冊管理機構的應處機制。		律及他律監理措施，俾保障我國民眾充分獲取資訊與自由表達言論之權利。
	• 完成工作項目三（二）： 提出「網際網路內容或網路使用者行為涉及違反我國法律時」我國網域名稱註冊管理機構之處置建議及精進作為。	240 日內	以利通傳會推動網域名稱之自律及他律監理措施，俾保障我國民眾充分獲取資訊與自由表達言論之權利。
	• 完成工作項目三（三）： 提出「本會依電信管理法對於頂級網域名稱註冊管理業務之現行監理機制是否有進行調整之必要性」之分析及整體性專業建議	240 日內	以利通傳會推動網域名稱之自律及他律監理措施，俾保障我國民眾充分獲取資訊與自由表達言論之權利。
	• 完成工作項目四： 於指定時間在本會場地舉辦成果發表會議 1 場次。	240 日內	以利通傳會推動網域名稱之自律及他律監理措施，俾保障我國民眾充分獲取資訊與自由表達言論之權利。

第二章研析跨國進行行政處分之困境及網域名稱國際協定、技術介紹

第一節 研析我國利用網域名稱跨國追查蒐證及進行行政處分之困境

為對網域名稱濫用進行適當處置，檢警及行政機關有對濫用之網域名稱進行追查蒐證，進而進行適當處置之必要。然而隨網路及科技技術的發展，網路匿名及其跨境特性，不論對於司法及警察機關利用網域名稱進行追查犯罪、事證蒐集、特定嫌疑人等皆產生困難；對行政機關而言，進行行政處分時，受處分的當事人究竟為誰、如何履行正當法律程序（如處分之送達及賦予陳述意見機會），亦因跨境網域名稱之性質及管理人之匿名特性致生困擾。以下本文將依序探討利用網域名稱跨國追查蒐證及進行行政處分之目前困境。

第一項 境外網域名稱追查網域名稱註冊人之困境

第一款 面臨之困境

網域名稱資料查詢系統（下稱「WHOIS」）資料庫供註冊人、執法單位、智財及商標權人、企業及個人使用者查詢服務。WHOIS 資料庫係由各網域名稱 IP 位址管理及發放機構，要求註冊人註冊時提供相關資料而建置，其蒐集方式通常是透過與申請註冊者簽訂契約書，同意使用者對於特定網域名稱申請使用時，要求註冊者須先提供相關註冊資訊，同意各該網域名稱受理註冊機構將其註冊資料納入其 WHOIS 資料庫中，並且公開於網際網路上，供公眾以網域名稱或 IP 位址等方式查詢各該網域名稱及 IP 位址註冊者之相關註冊資料[1]。這些資料可能包括網域名稱基本資訊（如註冊日、到期日、狀態等）及註冊人的聯繫方式（如公司名稱、地址、電話、E-mail 等）[2]。WHOIS

[1] Vincent Chen，台灣網民 WHOIS 查詢受 GDPR 之可能影響， https://medium.com/vincent-chen/%E5%8F%B0%E7%81%A3%E7%B6%B2%E6%B0%91whois%E6%9F%A5%E8%A9%A2%E5%8F%97gdpr%E4%B9%8B%E5%8F%AF%E8%83%BD%E5%BD%B1%E9%9F%BF-281624733003（最後瀏覽日：2021 年 6 月 30 日）。

[2] 網路中文，WHOIS 隱私服務，https://www.net-chinese.com.tw/nc/index.php/MenuLink/Index/WHOISPrivacy（最後瀏覽時日：2021 年 6 月 30 日）。

資料庫建置的主要目的可分為三個部分，第一部份為網域名稱及 IP 位址註冊之管理目的[3]，第二部分則為對網路犯罪之打擊、消弭及預防。第三部份則為網路上發生爭端之解決[4]。

然而隨著各國對個人資料保護法的重視，網域名稱追查也面臨如何兼顧個人資料保護之課題。以歐盟一般資料保護規則（General Data Protection Regulation,下稱 GDPR）[5]為例，負責協調管理全球網域名稱系統的 ICANN，也在 GDPR 的影響下修正 WHOIS 資料庫上之公開資訊，不再顯示註冊人的姓名、電話、地址、電子郵件信箱等資訊（但仍會顯示註冊人所在國家、州/省）[6]。

就此議題，通傳會曾於 2018 年 5 月 GDPR 即將生效前，邀集法務部、行政院消費者保護處、經濟部智慧財產局、內政部警政署、資策會、台北律師公會、國家資訊基本建設產業發展協進會、TWNIC 等單位，就即將生效之歐盟 GDPR 對 WHOIS 所造成的影響進行討論，並發布新聞稿說明可能遇到的問題及相關因應措施：「ICANN 的過渡性方案將會在公開查詢 WHOIS 系統時遮蔽（mask）與個人資料相關的欄位資訊，如姓名、住址、電話、電子郵件等。而目前在網際網路上想要處理違法網站、侵害著作權、內容申訴、購買網域名稱等行為，都需要使用 WHOIS 系統以通知相關網站所有人。」[7]。

綜上所述，對於跨國網域名稱追查網域名稱註冊人時，會有因 WHOIS

[3] 如確認該域名是否可註冊、該網站的營運是否為該企業的真實身分，或是出於合法目的而需聯繫域名註冊人。

[4] 同註 1。

[5] Regulation （EU） 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC （General Data Protection Regulation） （Text with EEA relevance）, OJ L 119, 4.5.2016, p. 1–88 .

[6] TWNIC，ICANN 的難題：WHOIS 與 GDPR （下集），https://blog.twnic.tw/2019/05/14/3718/（最後瀏覽日：2021 年 6 月 30 日）。

[7] 通傳會，為加強網域名稱相關個資保護與接軌國際，國家通訊傳播委員會邀集相關機關團體就「域名資料查詢系統（WHOIS）」與即將生效之歐盟一般性個人資料保護規則（GDPR）間之調適處理，說明相關因應作為、影響評估及未來發展，持續促進我國就國際個資保護趨勢之妥善因應-歷史資料，https://www.ncc.gov.tw/chinese/news_detail.aspx?site_content_sn=8&sn_f=39164（最後瀏覽日：2021 年 6 月 30 日）。

資料庫查詢屏蔽個人資料，造成於追查網域名稱註冊人之困難。縱使能快速取得註冊人之個人資料，然而如何將網域名稱違法行為與網域名稱註冊人相連結，以建立因果關係，亦是需要面對之挑戰。

第二款 困境之因應

對於上述情形以下區分該網域名稱為「.tw」或受理註冊機構在我國有總機構或分支機構；及網域名稱為「.tw」以外且受理註冊機構在我國未有總機構或分支機構，兩種類型進行討論。

一、 使用「.tw」網域名稱或受理註冊機構在我國有總機構或分支機構

（一）機關得適用個人資料保護法第 15 條向 TWNIC 或境內之受理註冊機構發函取得網域名稱註冊人之個人資料

受理註冊機構在我國有總機構或分支機構，即適用我國個人資料保護法（下稱:個資法）之情況下，依個資法第 15 條：「公務機關對個人資料之蒐集或處理，除第六條第一項所規定資料外，應有特定目的，並符合下列情形之一者：**一、執行法定職務必要範圍內**。二、經當事人同意。三、對當事人權益無侵害。」是以行政機關於法定職務必要範圍內有蒐集取得網域名稱註冊人之個人資料時，即得依本條向境內之受理註冊機構及 TWNIC，取得註冊人之個人資料。

「執行法定職務」且「必要範圍內」屬於兩獨立不同要件。「執行法定職務」係指具有法律明文職務權限範圍內，如兒童及少年福利與權益保障法第 46 條 3 項「網際網路平臺提供者經目的事業主管機關告知網際網路內容有害兒童及少年身心健康或違反前項規定未採取明確可行防護措施者，**應為限制兒童及少年接取、瀏覽之措施，或先行移除**。」及動物傳染病防治條例第 38 條之 3：「網際網路內容涉及境外應施檢疫物之販賣至國內、輸入或其他檢疫相關事項，經輸出入動物檢疫機關公告者，其廣告刊登者、平臺提供者、應用服務提供者或電信事業，應依輸出入動物檢疫機關之公告，採取下列措施：一、

加註有關宣導防疫或檢疫之必要警語。二、保存刊登者、販賣者或訂購者個人資料，或定期提供予輸出入動物檢疫機關。三、**限制接取、瀏覽或移除相關網頁內容**。」該等法律明文規範，衛福部、農委會針對網站內容違反該等法規時，有請求將限制接取網域名稱、瀏覽或移除相關網頁內容之權限，是以衛福部、農委會發函向 TWNIC 或在境內之受理註冊機構取得違反此兩部法律之網域名稱註冊人之個人資料以作成處分，符合個資法第 15 條第 1 項第 3 款之「執行法定職務」。

「必要範圍內」係指須符合比例原則。經查詢法務部及國家發展委員會之解釋函令並未特別針對「必要範圍內」進行定義，此外，亦因必要範圍之認定往往與具體個案事實相牽連而須併同考量。參考民國 107 年 2 月 12 日法務部法律字第 10703500080 號函之意旨：「本部行政執行署所屬各分署（下稱分署）辦理行政執行案件時，**如執行人員已無從經由其他方式掌握義務人等之行蹤，並經執行人員查知義務人在特定醫療機構有就醫紀錄者，則在符合個資法第 5 條比例原則之前提下，認有向該醫療機構蒐集渠等就醫時所留存之聯絡地址、電話等資料之必要，於執行法定職務必要範圍內向醫療機構查調義務人通訊住址電話，符合個資法第 15 條第 1 款之規定**…按分署為執行公法上金錢給付義務強制執行之法定職務，有依法進行督促義務人等到場履行義務或報告財產狀況（行政執行法第 14 條規定參照）、執行義務人之財產等執行行為之必要。**是以當義務人等遷離戶籍地，甚至戶籍遭逕遷至戶政事務所，或向義務人等已知之住居所送達文件，均遭遷移不明退回，義務人等處於住居所不明之狀態，致分署無法順利進行前揭執行程序，亦無法將相關執行文書合法送達義務人等，俾渠等得以到場陳述意見、或是對於執行名義或執行方法等提出異議，以保障其等合法權益時，分署必須依職權透過各種管道查明義務人等之聯絡方式**。」是以如法律上（如行政程序法第 39 條、102 條）有明文行政機關於作成處分前，有給予當事人陳述意見及文

書合法送達之必要，應符合個資法第 15 條第 1 項第三款之執行「必要範圍內」，故機關為針對濫用之網域名稱之註冊人作成行政處分時，得發函向 TWNIC 或受理註冊機構以取得註冊人之聯繫電話、e-mail 及地址等個人資料。

（二）依 TWNIC 及受理註冊機關之服務合約、申請書等文件，TWNIC 及受理註冊機構應有權限得向行政機關提供註冊人之個人資料

依個資法第 19 條第 1 項：「**非公務機關對個人資料之蒐集或處理，除第六條第一項所規定資料外，應有特定目的，並符合下列情形之一者**：一、法律明文規定。二、與當事人有契約或類似契約之關係，且已採取適當之安全措施。三、當事人自行公開或其他已合法公開之個人資料。四、學術研究機構基於公共利益為統計或學術研究而有必要，且資料經過提供者處理後或經蒐集者依其揭露方式無從識別特定之當事人。**五、經當事人同意**。六、為增進公共利益所必要。七、個人資料取自於一般可得之來源。但當事人對該資料之禁止處理或利用，顯有更值得保護之重大利益者，不在此限。八、對當事人權益無侵害。」是以非公務機關得與透過契約與私人間約定個資之蒐集及處理。

受理註冊機構以中華電信為例，其個人資料蒐集告知條款即有提及「中華電信股份有限公司**基於履行契約義務及行使契約權利；履行法定義務**…，須蒐集您的個人資料」。網域名稱申請同意書第 4 條第 2 項及第 4 項：「（二）基於國際網路社群慣例及維護消費者權益、保護智慧財產權與執行法律等公共利益之考量，**註冊申請人同意本公司將網域名稱之相關資料（包括且不限於網域名稱、申請人姓名、電話、傳真、電子郵件（E-mail）、申請日期、有效日期、DNS 設定資料），公開並提供第三人在各註冊 WHOIS 線上查詢及各項網域名稱實驗計劃使用**。為保護註冊申請人之隱私權，本公司得視註冊申請人所擇定部份中英文資料提供並顯示其相關資料；（四）**本公司將遵**

守相關法律規定，在必要範圍內盡最大努力保護註冊申請人所提供之中英文資料，非正當理由，不提供第三人或其他人使用。」故如果具正當理由，例如將濫用網域名稱之註冊人之聯繫資料交給行政機關應符合受理註冊機構中華電信與註冊人間之約定。

「.tw」註冊管理機構 TWNIC 依個資法第 8 條訂立個人資料保護法應告知事項，其中第 2 條蒐集目的：「提供網域名稱註冊管理及爭議處理相關服務、非公務關依法定義務所進行個人資料之蒐集處理及利用、契約、類似契約或其他法律關係事務、消費者、客戶管理與服務、電信及傳播監理、學術研究、**其他公共部門 包括行政法人、政府捐助財團法人及其他公法人 執行相關業務**、其他經營合於營業登記項目或組織章程所定之業務。」。此外，網域名稱申請同意書第 2 條：「TWNIC 有權基於國際網路社群慣例及維護消費者權益、保護智慧財產權與執行法律等公共利益之考量而設置 WHOIS 查詢介面，**將註冊人所提供之中英文資料（網域名稱、申請人姓名、電話、傳真、電子郵件（E-mail）、申請日期、有效日期、DNS 設定資料），提供外界線上逐筆查詢**。為保護註冊人之隱私權，TWNIC 得視該註冊人為個人或非個人而擇定部份中英文資料，供該註冊人選擇是否顯示提供外界查詢。」；第 4 條：「本同意書第 2 條之中英文資料除提供外界線上逐筆查詢外，TWNIC 將依個人資料保護法及相關法律之規定，保護註冊人所提供之資料。**除依法律規定、法院命令或相關主管機關依法以書面申請，TWNIC 將不會提供與第三人使用**。」是以 TWNIC 亦針對可能蒐集及利用註冊人個資部份於事情取得註冊人同意，並於行政機關依法須取得註冊人個資如聯繫資料等，得發函給 TWNIC，而 TWNIC 亦應提供網域名稱濫用之註冊人聯繫資料。

（三）小結

綜上所述，針對網域名稱為「.tw」者，行政機關有必要取得該濫用網域名稱之註冊人個人資料時，得在符合個資法第 15 條第 1 款

[8]執行法定職務必要範圍內，發函向 TWNIC 或受理註冊機構取得註冊人之聯繫資料。此外網域名稱雖非「.tw」但受理註冊機構在境內有總機構或分支機構者，亦應遵守我國個資法之規定，故行政機關亦得依個資法第 15 條第 1 款執行法定職務必要範圍內，發函向受理註冊機構取得網域名稱註冊人之聯繫資料。

「執行法定職務」多需有法律明文或授權，為保險起見各事項之主管機關應於其主管法規內明文對網域名稱濫用情形之處理，以符合針對網域名稱濫用之註冊人作成行政處分及發函向 TWNIC、受理註冊機構取得網域名稱註冊人聯繫資料，併敘明之。

二、 使用「.tw」以外網域名稱且受理註冊機構在境內無分支機構

WHOIS 為一線上資料庫，可透過輸入網域名稱或是 IP 查詢到網域名稱註冊人之子信箱、電話號碼、地址等個人資料。然而 2018 年歐盟一般資料保護規範（GDPR）施行後，註冊管理機構及受理註冊機構須遵守 GDPR 對個人資料之保護，將網域名稱註冊人之個人資料隱蔽。然而實務上如行政機關或是對網域名稱有爭執之他方仍有取得網域名稱註冊人聯繫資料之需求，故 ICANN 組成快速政策制定程序（Expedited Policy Development Procedure，下稱 EPDP）工作小組，第一階段任務是確認因應 GDPR 之臨時屏蔽註冊人個人資料等條款的內容是否須調整或修正，以合法並符合 ICANN 社群共識；**第二階段的任務則是為具合法、合理目的，需要取得非公開註冊資料的第三方，探討建立標準化流程的需求與必要**[9]。於第二階段報告書中工作小組提出揭露/存取非公開註冊資料的標準化系統（System for Standardized Access/Disclosure to Non-Public Registration Data，下稱 SSAD），透過此一系統之建置，使有需求之機構、機關及個人得快速取得網域名稱註冊人之個人資料。

[8] 個資法第 15 條：「公務機關對個人資料之蒐集或處理，除第六條第一項所規定資料外，應有特定目的，並符合下列情形之一者：一、執行法定職務必要範圍內。二、經當事人同意。三、對當事人權益無侵害。」

[9] TWNIC，EPDP 發布第二階段結案報告，https://blog.twnic.tw/2020/09/05/14860/ （最後瀏覽日：2021 年 9 月 23 日）。

SSAD 有以下特色[10]：一、透過單一窗口提出需求；二、標準化申請表單；三、內建驗證機制；四、標準化審核及回應流程，各分述如下：

（一） 透過單一窗口提出需求

1. 減少請求者追蹤資料所花費的時間及投入的精力。
2. 確保請求可傳達到揭露資訊實體（如受理註冊機構），從而消除請求未妥善接收或傳送至無處理權限之實體而引發不確定因素。
3. 請求和回應可供追蹤，以確定資訊提供符合服務協議。

（二） 標準化申請表單

1. 減少因資訊不充足而遭到拒絕揭露之數量。
2. 提高揭露實體的審核效率。
3. 降低請求者之不確定性，請求者擁有一組標準/統一資料供其在接受揭露請求時提供。

（三） 內建驗證機制

1. 創建通用回應格式。
2. 制定可供揭露方在審核及回復請求時遵循的規則、指南。

（四） 標準化審核及回應流程

1. 允許揭露方創建通用回應格式。
2. 允許制定可供揭露方在審核及回復請求時遵循的規則、指南。
3. 允許採用通用回應審核系統。
4. 允許待定請求者自動處理某些待定請求。

[10] ICANN, gTLD 註冊數據臨時規範快速政策制定流程第 2 階段的最終報告，頁 12。

5. 在某些情況下，可自動揭露資訊。

6. ICANN 可以通過記錄請求和回應來統計揭露次數、識別系統性違規情況及採取相應的強制措施。

SSAD 機制如下圖，請求人取得驗證機構之驗證後，透過單一窗口及匯道提出請求後，集中匯道管理人員審核請求，並區分符合自動化揭露及須人工審核之請求（詳後述），並交由受理註冊機構提出資訊，透過統一之匯道傳送給請求人。

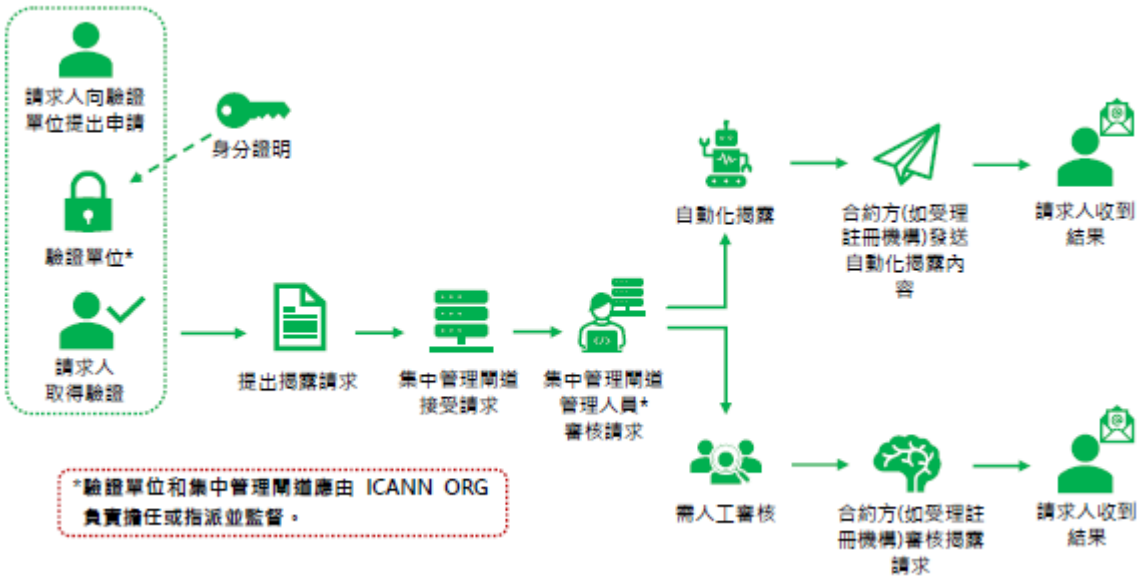


圖 2 SSAD 流程示意圖[11]

以下就 SSAD 機制重要部分具體介紹：

（一） 認證政策及認證要求[12]

SSAD 為使請求人可快速取得網域名稱註冊人聯繫資料及確保個人資料安全，制定政策包含：一、SSAD 僅接受組織或個人所提出，且區分一次性及重複性請求人，而可有不同之驗證方式；二、法人或個人皆可獲得驗證；三、由 ICANN 管理及組成立（或委外）單一處

[11] 參考 GDPR vs. WHOIS：隱私與安全難以兩全？座談會簡報重新繪製。
[12] 同註 10，頁 16-17。

理驗證之機構負責驗證、頒發及持續管理憑證。

驗證機構除須要驗證請求者身分外，亦須確認請求者之驗證上載有包含以下幾點：一、關於請求目的；二、請求之法律依據；三、關於法律合規（如個人資料之處存、保護及處理）；四、聲明出於正當合法目的使用資料；五、關於濫用之預防、爭議解決及投訴流程。

（二） 政府註冊使用 SSAD 機制之資格[13]

國家/地區政府或其授權機構有取得網域名稱註冊人之個人資料，以完成公共政策，包含但不限於以下：民刑事執法機關、數據保護和監管機關、司法機關、依法受政府委託處理公共政策任務之消費者權益組織、依法受政府委託處理公共政策任務之網路安全機構包含如電腦網路危機處理暨協調中心。

（三） 請求揭露標的及內容[14]

請求人為順利取得資訊，請求須要載明以下內容：

1. 欲揭露之網域名稱
2. 標示請求人之簽名/驗證
3. 關於請求者請求之法律權限、合法權益、其他法律依據、請求理由（如合法權益或法律依據為何？為何請求者需要此資訊）
4. 請求者本於善意原則提出請求
5. 請求資訊與達到目的[15]之必要關聯
6. 請求類型，如緊急性及優先與否

（四） 請求之優先程度[16]

於報告中建議至少提供以下三種級別，以供請求人提出請求時選

[13]同註 10，頁 22。
[14]同註 10，頁 23。
[15] 包含但不限於：1.刑事程序、國家或公共安全。2.其他爭訟程序如智慧財產權侵權、網域名稱爭議解決之損害賠償。3.消費者保護、防止濫用和網路安全。4.監管機關權限。
[16]同註 10，頁 26。

擇：

1. 第一優先級—緊急型

   限於可能威脅生命、嚴重人身傷害、破壞重要基礎設施[17]，或剝削兒童等情況[18]。此級別之申請者不限於執法機關。

2. 第二優先級—ICANN 爭訟程序

   此類請求是根據 ICANN 契約要求或是現有具共識之政策如網域名稱爭議解決機制，提出爭訟後取得結果。具申請此類別之請求人限於 ICANN 批准之爭議解決服務機構及其員工。

3. 第三優先級

   第一及第二級以外之其他請求。如請求者能說明該請求涉及消費者保護問題，如網路釣魚、惡意軟體、詐欺等，於前述情況下之請求將優先於其他類型之第三優先級請求。

（五） 自動化揭露及人工審核

如自動化揭露在技術、商業及法律可行下，受理註冊機關應自動化處理揭露決定。目前 GDPR 允許自動揭露範圍包含如[19]：

1. 來自當地執法機關之請求，且符合 GDPR 第 6 條第 1 項 e 款為了公共利益或行使機關權限及任務所必需的；或符合 GDPR 第 2 條豁免條款，即主管機關為預防、調查、偵查或起訴刑事犯罪或執行刑事處罰，包括防範和預防對公共安全的威脅。上述範圍可包含於我國個資法第 16 條第 2 款「為維護國家安全或增進公共利益所必要」。
2. 對違反個人資料保護之行為進行調查
3. 僅提供居住城市之請求以評估請求賠償或出於統計目的

[17] 指重要的物理和網路系統，因一旦此類物理或網路系統功能喪失或遭到破壞，將對人身安全、經濟保障、公共衛生或安全產生重大不利影響。
[18] 此指不需要特別技能即可判斷其影響公共安全。
[19]同註 10，頁 33。

如不符合自動化揭露範圍，即須經由人工審查請求人之請求，並同時考量被揭露人之權益。於評估請求者合法權益時，須考量以下幾點：

1. 請求人主張之權益須具體、真實且不模糊及非單方臆測。
2. 遵守個人資料保護法及其他法律。
3. 合法權益包含：(1) 法律主張之執行、行使或辯護，包含智慧財產權侵權；(2) 防止詐欺和濫用服務；(3) 物理、IT 和網路安全。

此外亦應評估個資主體之權益或基本權和自由未超越請求人之合法權益，受理註冊機構應綜合考量以下因素[20]：

1. 影響評估：考量對個資主體之直接影響及處理個資潛在後果。同時亦須考量到請求人請求之條件及要求揭露之資訊，越接近個資主體時所增加之風險。
2. 資料性質：考量資料之敏感性及資料是否已經公開。
3. 個資主體身分：考量個資主體之身分，如揭露資訊是否會導致其面臨之風險進一步增加，如兒童、尋求庇護者、其他受保護主體等。
4. 請求人資料處理範圍：考量請求人之請求及其他相關資訊，判斷資料是否可妥善保護而不被公開揭露。
5. 個資主體之合理期待：考量個資主體是否合理期待以此種方式揭露資料。
6. 涉及法律框架：考量請求人及個資主體之法律關係，及潛在可能影響。
7. 跨境數據傳輸：考量可能須跨境傳輸之要求。

[20]同註 10，頁 31-32。

EPDP 工作小組提出之第二階段報告於 2021 年 3 月 25 日經 ICANN 董事會決議通過，並指示 ICANN 主席暨執行長對 SSAD 進行評估。ICANN 於 2021 年 7 月 8 日公告 SSAD 實施評估流程問卷，希望藉此判斷 SSAD 潛在使用者的數量，以及 SSAD 啟用後可能收到的請求多寡，以評估 SSAD 建置工程可行性、相關風險、開銷及所需資源[21]。於未來 SSAD 機制正式實施，網域名稱濫用之各主管機關即可註冊加入此機制，取得使用「.tw」以外網域名稱（如.com）且受理註冊機構在境內無分支機構之網域名稱濫用註冊人之聯繫資料，以解決不易取得網域名稱濫用行為人之困境。

第二項　行政處分有效性問題及因應

對於境外網域名稱內容違法，行政機關可否逕要求境外域名註冊管理機構將違法網域名稱取消或停止解析，亦非無疑。綜觀我國現行法律，主要規範限制接取、瀏覽、移除網路內容者為兒童及少年福利與權益保障法第 46 條第 3 項及動物傳染病防治條例第 38 條之 3。依兒童及少年福利與權益保障法第 46 條第 3 項，規範網路平臺提供者經目的事業主管機關告知網際網路內容有害兒童及少年身心健康時，網路平臺提供者有限制瀏覽或移除內容之義務；依動物傳染病防治條例第 38 條之 3，規範網際網路內容涉及境外應施檢疫物之販賣至國內、輸入或其他檢疫相關事項，經輸出入動物檢疫機關公告者，廣告刊登者、平臺提供者、應用服務提供者或電信事業應依公告限制接取、瀏覽或移除相關網頁內容。上述法規適用下，對於境外網域名稱有應移除之內容時，在管轄權無法擴及境外業者下，逕作成行政處分給境外網路服務提供業者或平臺業者，於實務執行上容有困難。是以，行政機關對於該等境外業者並無實質之強制力，因此通常僅能期待其願意自主將網頁內容移除。

對於前述要求使用境外網域名稱內容下架，僅能期待境外業者願意自主將網頁內容移除，故現行行政機關得選擇發函給 TWNIC，透過停止解析該

[21] TWNIC，SSAD 實施評估流程問卷，展開實施評估流程，https://blog.twnic.tw/2021/08/09/19305/ （最後瀏覽日：2021 年 9 月 27 日）。

網域名稱方式，使國人難以接觸該等網域名稱內容，間接達到降低違反兒童及少年福利與權益保障法及動物傳染病防治條例之內容傳遞及散布。

第三項　履行正當法律程序潛在問題及因應

依行政程序法第 102 條規定，行政機關作成限制或剝奪人民自由或權利之行政處分前，除已依第 39 條規定，通知處分相對人陳述意見，或決定舉行聽證者外，應給予該處分相對人陳述意見之機會。然而對於境外網域名稱，除網域名稱註冊人之資訊有取得上之限制外，當受處分之註冊人亦為境外之人時，通知並給予其陳述意見之機會於執行上將有難度。

其次，依行政程序法第 110 條規定，書面之行政處分自送達相對人及已知之利害關係人起；書面以外之行政處分自以其他適當方法通知或使其知悉時起，依送達、通知或使知悉之內容對其發生效力。因此為使行政處分發生效力必須以有效送達受處分人為前提。對於境外網域名稱，如其網域名稱註冊人亦為境外之人時，必須取得網域名稱註冊人之住址，並對之為送達。是以，在涉及境外送達下，做成處分之機關，應如何將處分即時、有效送達註冊人，執行上亦有困難。可能的方式為依同法第 86 條囑託該國管轄機關或駐在該國之中華民國使領館或其他機構、團體將行政處分送達，然而於執行上是否符合成本效益、是否可滿足時效要求，亦非無疑問。

對上述問題可參酌行政程序法第 103 條第 2 款：「情況急迫，如予陳述意見之機會，顯然違背公益者」以因應須立即將網域名稱停止解析或內容下架，以避免情勢更為嚴峻（如散播病毒、釣魚等）；同條第 3 款：「受法定期間之限制，如予陳述意見之機會，顯然不能遵行者。」以因應網域名稱註冊人之聯繫資料顯為造假，致聯繫上註冊人顯有困難，或難以趕上做成處分之期限；同條第 5 款：「行政處分所根據之事實，客觀上明白足以確認者。」以因應網域名稱內容明顯違反相關法律（如網頁內容涉及兒童情色、毒品販賣等）。另外對於處分難以送達問題，可透過立法於相關法規增修「無法查明行為人之送達，得以公告方式為之。」或行政程序法第 78 條基於應為送達之處所不明為公示送達，加以解決此問題，相關具體說明可參見第陸章第五節。

第二節 ICANN 之統一網域名稱爭議解決政策及統一快速暫停系統

統一網域名稱爭議解決政策及統一快速暫停系統係為解決網域名稱自身之商標爭議及搶註問題而制定之機制，為網域名稱發展中最典型之網域名稱濫用類型，以下將依序介紹之。

一、ICANN 之統一網域名稱爭議解決政策：解決網域名稱自身之商標爭議及搶註問題

「網際網路名稱與數字位址分配機構」（ICANN）為一全球性管理網際網路的非營利私人機構。ICANN 於 1998 年在美國加州成立，負責網域名稱系統（DNS）的作業，即負責協調管理特定化的辨識名稱（identifier），以確保每一台電腦在網際網路上的唯一性，並制定有關網域名稱和網際網路位址運作方式的政策[22]。但依據 ICANN 組織章程第 1.1 條之規定，ICANN 並非網域名稱內容之監督者，也無權管理、監督網路內容[23]，更無權將網域名稱移除或阻擋[24]。

於 ICANN 設立之初，即有網域名稱涉及侵害商標權之法律議題，故 ICANN 於 1998 年即諮詢世界智慧財產權組織（World Intellectual Property Organization，下稱 WIPO）。WIPO 於 1999 年提出其建議，ICANN 並於同年制定發布其統一網域名稱爭議解決政策 （Uniform Domain Name Dispute Resolution Policy，下稱「UDRP」）以統一性解決網域名稱之商標爭議。

UDRP 在性質上屬於 ICANN 與註冊管理機構間約定之「強制性機制」，即註冊管理機構有義務依此機制解決註冊管理機構與其客戶（即網域名稱持有人或註冊人）間與第三人（即申訴人）就網域名稱之爭議。惟 UDRP 所訂之適用範圍相當狹義，僅適用於涉及「網域名稱濫用」（如

[22] 劉靜怡、雷憶瑜，國際網路組織介紹，頁 42，https://www.twnic.tw/download/031014.pdf （最後瀏覽日：2021 年 6 月 30 日）。

[23] BYLAWS FOR INTERNET CORPORATION FOR ASSIGNED NAMES AND NUMBERS | A California Nonprofit Public-Benefit Corporation，ICANN official website, https://www.icann.org/resources/pages/governance/bylaws-en/#article1 (last visited Jun. 30, 2021).

[24] ICANN 官方網站，https://www.icann.org/news/blog/icann-doesn-t-take-down-websites （最後瀏覽日：2021 年 6 月 30 日）。

搶註冊）之情況方適用 UDRP 程序，而其他與商標有關之網域名稱爭議類型仍必須以協議、法院命令或仲裁先行解決後，方得採取取消、暫停或轉讓該網域名稱之作法[25]。

適用 UDRP 之網域名稱爭議，應交由 UDRP 核可之爭議解決服務機構解決。該服務機構之判斷得為取消、移轉網域名稱之依據。此外，依據 UDRP 第 3 及第 7 條之規定，註冊管理機構原則上不得撤銷、轉讓、啟動、停用或變更網域名稱註冊的狀態，而僅能於下列情形採取移除、移轉或變更網域名稱：

1. 收受註冊人或其授權人之書面或電子指示。但註冊人不得於（a）UDRP 爭議解決程序中或其結束後 15 日內或（b）法院或仲裁程序開始後（除非得對造書面同意）為之，同時，亦不得請求變更註冊管理機構
2. 收受有管轄權之法院或與仲裁機構之命令
3. 收受 UDRP 爭議解決服務商機構依據 UDRP 程序所作成之決定。

UDRP 並無明確定義「網域名稱濫用」而僅於第 4.a 條規定適用之爭議型態（Applicable Disputes），須同時符合以下情形[26]:

1. 註冊人網域名稱與申訴人之有權利之商標或服務標章一致相同或近似且混淆者
2. 註冊人就其網域名稱無權利或合法利益
3. 註冊人已註冊該網域名稱且正惡意使用中

就惡意使用之解釋，於 UDRP 第 4.b 條列出相關定義，包括（一）主要用於以超過註冊人取得網域名稱之直接成本販售、出租或以其他方法移轉該網域名稱予有該名稱商標權之申訴人或其競爭對手；（二）註冊

[25] 同註 24（最後瀏覽日：2021 年 6 月 30 日）。
[26] 同註 24（最後瀏覽日：2021 年 6 月 30 日）。

人註冊該網域名稱係為避免或阻礙商標權人或標章之所有人取得與其商標或標章相對應的網域名稱，且註冊人過去已有相當類似之行為模式;(三)註冊人係為破壞註冊人之競爭對手而註冊該網域名稱;或(四)註冊人使用該網域名稱是企圖故意吸引網路用戶訪問該網站或其他線上網址，以獲得商業利益，方法是使註冊網站或網站上的產品或服務的來源、贊助商、從屬關係或認與申訴人標記具有相似性從而使人產生混淆。

上述為申訴人得提出之申訴範圍及內容。而註冊人亦得以 UDRP 第 4.c 條證明其網域名稱之權利與合法利益，包括（一）於收到申訴前，註冊人已善意使用或可證明已準備使用該網域名稱或與其相當之名稱，銷售商品或提供服務；（二） 註冊人使用該網域名稱，即便尚未取得該商標或標章，已為一般大眾所熟知；或（三） 註冊人正於合法非商業或合理之使用，而未以混淆、誤導消費者或減損商標或之方式獲取商業利益。

此外，依據 UDRP 第 4.k 條之規定，UDRP 程序並不具排他性。於 UDRP 開始之前或結束後，均不妨礙註冊人或者申訴人得請求有管轄權的法院就爭議進行解決。若 UDRP 爭議解決機制作成不利於註冊人決定後之 10 日內，註冊管理機構未收到註冊人之法院訴訟文件，註冊管理機構將執行取消、移轉該網域名稱之決定。反之，若註冊管理機構於 10 日內收到註冊人之法院訴訟文件，註冊管理機構將不執行裁決並且不會採取進一步的行動，直至收到（i）令註冊管理機構確信雙方已解決爭議的證據；（ii）令註冊管理機構確信註冊人訴訟已被駁回或撤回的證據；或者（iii）由法院發出的駁回註冊人訴訟或者責令註冊人無權再繼續使用註冊人網域名稱的命令副本[27]。

[27]謝銘洋，新通用頂級域名（New gTLD）開放對我國域名管 理機制之影響與因應之研究，財團法人台灣網路資訊中心，資料來源：https://www.twnic.tw/file/1406rp.pdf （最後瀏覽日：2021 年 6 月 30 日）。

二、統一快速暫停系統[28]：加速解決新通用頂級網域名稱自身之商標爭議及搶註問題

統一快速暫停系統（Uniform Rapid Suspension System, 下稱「URS」）是 ICANN 為了因應新通用頂級網域名稱施行的新措施，係一更為快速、經濟的網域名稱爭議解決機制。一旦新通用之頂級網域名稱措施開始施行後，若他人在新通用頂級網域名稱下註冊的網域名稱侵犯商標權時，便可透過 URS 請求暫停該網域名稱之使用。然而在 2013 年 1 月 1 日以前已生效的原通用頂級網域名稱下的網域名稱，並不適用 URS，而仍應回歸 UDRP 處理之。

商標權人如欲主張網域名稱傷害商標權而應予暫停者，應向 URS 的網域名稱爭議解決機構提起投訴。根據 ICANN 所發布之消息，接受投訴的機構有亞洲網域名稱爭議解決中心（Asian Domain Name Dispute Resolution Centre）及美國國家仲裁協會（National Arbitration Forum）。URS 的爭議處理機制完全採「獨任審查員」方式進行。申訴人如擬獲得有利的裁決，則必須證明以下三個要件：

1. 爭議網域名稱與受保護的文字標識相同或混淆性相似。若該文字標示是有效註冊的商標，則必須提出使用證明。若使用證明曾經由商標信息交換機構確認過者，得提交一份聲明及一份目前用於商業用途的樣本即可。
2. 被申訴人對爭議網域名稱不享有合法權益。
3. 被申訴人對爭議網域名稱的註冊和使用具有惡意。

上述三個要件與現行 UDRP 的三個要件大致相同，但其中特別新增申訴人若是依據已註冊的商標提出投訴者，則必須提出使用證據的要求。

在舉證責任方面，申訴人必須舉證證明上列三個要件均成立。然而

[28] 陳彥君，新通用頂級域名爭議解決新機制，資料來源：http://www.winklerpartners.com/?p=4430&lang=zh-hant （最後瀏覽日：2021 年 6 月 30 日）。

因 URS 是比現行 UDRP 更為快速的網域名稱爭議解決機制，為兼顧對造權益，因此投訴人負有比在 UDRP 程序中，更高的舉證責任。現行 UDRP 要求投訴人舉證到「證據優勢」（preponderance of the evidence）的程度即足，亦即依據投訴人所提出的證據可以證明投訴人所主張的事實為真的可能性大於非真實的可能性即可；但 URS 則要求投訴人必須舉出「清晰可信」的證據才足夠（clear and convincing evidence）。

同時 URS 特別指明，即便係出於獲利而買賣網域名稱及為投資目的而大量持有網域名稱，只要不是主要為了高價出售給商標權人或其競爭對手，並不當然構成惡意註冊；即使用爭議網域名稱是否屬於惡意，審查員仍必須依案件具體事證個案判斷。若依案件事證判斷關於被投訴人是否惡意註冊、使用爭議網域名稱，仍存有未臻明確的爭點時，審查員即應駁回投訴人之投訴。

綜上，商標權人仍應先確定爭議網域名稱的通用頂級網域名稱為 2013 年 1 月 1 日以後生效的新通用頂級網域名稱，方可選擇 URS。再者，商標權人若希望取得爭議網域名稱所有權者，則必須選擇現行 UDRP 尋求救濟。但若商標權人面對的是大量惡意註冊，卻又不想取得一大批無用的網域名稱時，則可考量以 URS 尋求救濟，快速凍結大批惡意註冊的網域名稱，同時亦無需負擔該等網域名稱將來的註冊費用問題。

第三節 網域名稱濫用架構、馬尼拉原則、DNS RPZ 之困境及可行性分析

一、網域名稱濫用框架：解決網域名稱技術濫用及特殊網域名稱內容濫用類型（如兒童性虐及販賣鴉片等）

「網域名稱濫用框架」（DNS Abuse Framework）為因應網域名稱濫用，提出基本可供參考之處置方向，並將網域名稱濫用類型分為網域名稱技術濫用及網域名稱內容濫用。網域名稱濫用框架認為網域名稱技術濫用，本於註冊管理機構維護網路基礎設施之角色應有作為義務；而網域名稱內容濫用，基於註冊管理機構不審酌網域名稱內容，故除特殊類

型如兒少性虐待之素材、網路違法販售鴉片、人口販售及具體且可信的煽動暴力，建議採取專業之「受信任之通知者」，以協助濫用控管外，其餘應由投訴人向網站管理者、註冊人或伺服器服務提供尋求移除濫用內容。網域名稱濫用框架為機關、註冊管理機構、網路社群等因應網域名稱濫用最具參考性之原理原則，亦為貫串本研究之重要參考。以下將具體介紹之。

網域名稱濫用框架為 11 國際著名之通用頂級域名（gTLD）與國家頂級域名（ccTLD）註冊管理機構與註冊業者於 2019 年 10 月分發布針對註冊管理機構與註冊業者就於網域名稱濫用之議題所應採取之建議作為，此網域名稱濫用框架並於 2019 年 ICANN 政府諮詢委員會（Government Advisory Committee）蒙特羅年會上被指定為業界潛在最佳守則[29]。自發布實施至今，已有超過 50 餘參與此框架之註冊管理機構與受理註冊機構，其中包括 GoDaddy、PIR, Neustar、Enom 等具國際權威性之註冊管理機構與受理註冊機構[30]。

網域名稱濫用框架之性質為機構與業者之自律框架機制。其目的在於使註冊管理機構與註冊業者遵循一定之定義與程序，以保護網域名稱基礎建設 （DNS Infrastructure）之健全與安全為目的。按網域名稱濫用框架之定義，網域名稱濫用共有 5 種[31]有害類型[32]：

1. 惡意軟體（Malware）

為未經使用者同意所安裝，足以擾亂設備、蒐集機密資訊或存取電腦系統之惡意破壞軟體，包括病毒、間諜軟體、勒索軟體等其他惡意軟體。

2. 殭屍網路（Botnets）

[29] 網域名稱濫用框架官方網頁，2020 年回顧簡介 http://dnsabuseframework.org/dns-abuse-framework-2020-retrospective.html （最後瀏覽日：2021 年 6 月 30 日）。

[30] 同註 29（最後瀏覽日：2021 年 6 月 30 日）。

[31] 皆為網域名稱技術爛用。

[32] Framework to Address Abuse, https://dnsabuseframework.org/media/files/2020-05-29_DNSAbuseFramework.pdf, at 1 (last visited Jun. 30, 2021).

為已受惡意軟體侵入並經由網際網路連結之數個電腦並受外部管理員遠端指使為一定作為或不作為之電腦網絡。

3. 網路釣魚（Phishing）

為一種駭客讓用戶傳送敏感資訊（包括企業或財務資訊）的手法，例如傳送帳戶號碼、帳戶使用者帳號及密碼、身分證號碼等，該手法包括傳送看起來像是來自可信任來源的電子郵件或誘拐用戶連結至一個假冒可信任來源的詐騙網站，或促使用戶安裝貌似可信來源之軟體，但實際上為惡意軟體。

4. 偽冒嫁接（Pharming）

為以綁架 DNS 或 DNS 中毒為手段，嫁接不知情之用戶至詐騙網站或服務。嫁接與網路釣魚較明顯不一樣的地方在於前者涉及改變用戶所輸入之 DNS，而後者則係以詐騙手段使用戶輸入、傳送敏感個資。

5. 以垃圾郵件之形式達成以上濫用之行為（Spam）

此處非指一般單純未經索取之電子郵件，而是指以垃圾郵件之形式達成以上濫用之行為。換言之，若此垃圾郵件屬於網路釣魚之一部份，則屬於此框架所指之垃圾郵件。

網域名稱濫用框架明確指出，**當註冊管理機構知悉有上述之網域名稱濫用情形時，註冊管理機構必須有所作為**，如依據註冊管理機構與 ICANN 之合約維持網域名稱濫用之聯絡窗口以利接收網域名稱濫用之投訴並盡速調查該濫用之情形[33]。惟由於註冊管理機構之型態與其於整體網際網路 DNS 基礎建設之角色，**註冊管理機構能採取之唯一處理措施僅是將使整個網域名稱失效或禁用[34]。但此禁用措施無法精準的移除該網域名稱之濫用部份**，特別是當濫用情形是存在於較廣泛的網域名稱或平臺內，如線上討論區、網路市集等其他多人共用之多功能或面向之

[33] *Id.,* at 3.
[34] *Id.*

網站。

此外，**註冊管理機構無法處理「網域名稱內容」之濫用，因為註冊管理機構依據其與 ICANN 之合約並無義務監督、管理網域名稱之內容且無權限因網域名稱內容而取消網域名稱**。**並且，如以取消網域名稱之方式處理網域名稱內容爭議，往往是不符合比例原則之措施**[35]，**因為取消網域名稱無法精準的移除該網域名稱內容之濫用部份，且一旦取消網域名稱後，整個網站將失效**，包括不屬網域名稱內容濫用之部份以及第 3 級網域名稱，例如該網域名稱之電子郵件。

因此，網域名稱濫用框架僅認定於下列特殊網域名稱內容之情況下，註冊管理機構得於尚未收到法院命令前但收到特定且具有可信度的通知時，採取積極作為：

1. 兒少性虐待之素材 （Child Sexual Abuse Material）
2. 網路違法販售鴉片 （Illegal distribution of opioids online）
3. 人口販售 （Human trafficking）
4. 具體且可信的煽動暴力

在上開特殊情形，註冊管理機構於處理網路內容時應通知受理註冊機構並與其協調合乎比例原則之處理措施，並使受理註冊機構與其用戶辦理處理措施事宜，如將受害網域名稱回復其尚未收侵害之狀態。此外，網域名稱濫用框架並認為直接刪除、禁用網域名稱之處理措施無法避免網域名稱內容濫用之原始者即刻重新註冊另一網域名稱以達相同之違法目的[36]。**網域名稱濫用框架亦建議註冊管理機構與受理註冊機構就上開特殊網域名稱內容考慮使用專業之「受信任之通知者」（Trusted Notifiers），以協助濫用控管並於採取處理措施時之提供諮詢**[37]。

然除上述特殊網域名稱內容之情況外，於一般網域名稱內容濫用之情形，由於註冊管理機構無法直接取消網域名稱內容並為保障該網域名

[35] *Id.*
[36] *Supra* note 32, at 4.
[37] *Supra* note 32, at 5.

稱之延續使用，網域名稱濫用框架**建議由投訴人向網站管理者（Site Operator）、註冊人（Registrant）或伺服器服務提供者（Hosting provider）尋求移除濫用內容之救濟方式，而非向註冊管理機構或受理註冊機構提出取消網域名稱名稱之要求**，如下：圖所示[38]：

圖 3 移除濫用內容之救濟程序

由上可知，網域名稱濫用框架針對網域名稱技術濫用基於註冊管理機構維護網路基礎設施之職責，應有作為義務。對於網域名稱內容濫用則限於兒少性虐待之素材、網路違法販售鴉片、人口販售、具體且可信的煽動暴力等重大違反人權、公益等情事，受專業之「受信任之通知者」後進行適當處置。對此等網域名稱內容濫用情事，於我國兒童及少年福利與權益保障法第 46 條之 1 及第 46 條第 3 項已有明文得限制接取、瀏覽之措施，或先行移除等處置手段（具體說明可參第四章第三節第二項）。

二、馬尼拉中介者責任原則：定位網路仲介者角色及免於因使用者網域名稱內容濫用而負責

馬尼拉中介者責任原則（下稱「馬尼拉原則」）為定位網路仲介者對於網域名稱濫用時所扮演之角色，其核心主張在於保障網際網路之開放與自由，並使網路仲介者免於為網路使用者產生之內容（如網域名稱內容濫用）而負責任。此影響行政機關制定政策因應網域名稱內容濫用時，與網路仲介者間的互動關係應為協力解決網域名稱內容濫用。以下將詳細介紹馬尼拉中介者責任原則。

[38] *Id.*

馬尼拉中介者責任原則是由美國著名非政府組織「電子前哨基金會」（Electronic Frontier Foundation）[39]所領銜倡議之網際網路中介者責任之最低標準。此原則係於 2015 年 3 月由電子前哨基金會等其他國際非政府組織所公布之民間框架倡議文件[40]。馬尼拉原則之訂定係參考「世界人權宣言」、「公民及政治權利國際公約」，和「聯合國工商業與人權指導原則」制訂[41]。綜觀目前之「簽署團體」與「簽署個人」，其公布之總簽署人數約為 111 團體[42]與 400 位個人[43]，為各國之非政府組織或財團法人而無政府機關或組織，屬於台灣之團體與個人有「台灣人權促進會」[44]與極少數我國國民[45]。

馬尼拉原則之主要目的在提供各國政府對於訂定網路中介者相關責任之法律或政策時之原則指引與參考，而其主要精神及目的在於保障網際網路之開放與自由，並以中介者免於為網路使用者產生之內容（User Generated Content，下稱 UGC）而需負擔責任（即除有司法機關之命令不得使網路中介者限制網路之內容）[46]。

依據馬尼拉原則之背景說明文件[47]，如採廣義定義，「中介者」包含「任何能夠實現提供一方通信至另一方之任何實體」，並以經濟合作暨發展組織（Organization for Economic Cooperation and Development，OECD）2015 年「網路中介者之經濟與社會角色」報告書之定義「網際

---

[39] 電子前哨基金會係於 1990 年由美國著名網路創業者 （如蓮花軟體之 Mitch Kapor 先生，昇陽電腦之 John Gilmore 先生，蘋果電腦 Steve Wozniak 先生等人） 在加州舊金山市設立之國際性非政府組織，主旨在於捍衛網路言論自由、網路使用者隱私、網路創新之發展及網路中立 （net neutrality），資料來源：https://www.eff.org/about （最後瀏覽日：2021 年 6 月 30 日。

[40] 電子前哨基金會網頁，https://www.eff.org/press/releases/international-coalition-launches-manila-principles-protect-freedom-expression （最後瀏覽日：2021 年 6 月 30 日）。

[41] 馬尼拉原則官方網站，https://www.manilaprinciples.org/principles（ 最後瀏覽日：2021 年 6 月 30 日）。

[42] 同註 41（最後瀏覽日：2021 年 6 月 30 日）。

[43] 同註 41（最後瀏覽日：2021 年 6 月 30 日）。

[44] 同註 41（最後瀏覽日：2021 年 6 月 30 日）。

[45] 如 「Rebecca Yen」馬尼拉原則官方網站 https://www.manilaprinciples.org/individual-signatories?page=39; 「Ming-Syuan Ho」https://www.manilaprinciples.org/individual-signatories?page=38; 「Poren Chiang」https://www.manilaprinciples.org/individual-signatories?page=29 等人 （最後瀏覽日：2021 年 6 月 30 日）。

[46] 2017 年電子前哨基金會關於網域名稱註冊之白皮書，頁 7，https://www.eff.org/files/2017/08/02/domain_registry_whitepaper.pdf（最後瀏覽日：2021 年 6 月 30 日）。

[47] 2015 年馬尼拉原則背景文件，電子前哨基金會官方網站 https://www.eff.org/files/2015/07/08/manila_principles_background_paper.pdf （最後瀏覽日：2021 年 6 月 30 日）。

網路中介者為促成第三方間之網際網路訊息交換的單位。其提供網路內容之存取、主機、傳輸、索引等服務與產品，或是提供網際網路為基礎之服務予第三人」為馬尼拉原則就「中介者」之主要定義，並包括以下網路服務提供者：網路服務提供者、搜尋引擎、社群網路、雲端服務提供者、電子商務平臺、網路主機公司、網域名稱受理註冊機構、內容整合業者及運作公開 WIFI 或 Tor 節點的個人等[48]。惟中介者之責任免除範圍不包括其自行發布之內容或是其他自身行為所生之責任，例如違約、稅務、詐欺等因自身或業務行為所生之責任[49]。

馬尼拉原則總共有以下六大原則：

1. 原則一: 中介者應免於對第三方內容承擔責任

此原則在建議政府應以法律保障中介者免受第三方 UGC 之法律責任。依據馬尼拉原則 2015 年之「最佳實踐指引」法律規範應包括以下面向[50]：

(a) 任何管理中介者責任的規定必須由法律制定，且務必做到準確、清晰和易懂。

(b) 在中介者沒有參與修改內容的情況下，中介者應該免於對第三方內容承擔責任。

(c) 中介者不得因沒有限制合法內容而被追究責任。

(d) 中介者不得因託管違法的第三方內容被追究無過失責任，也不得在中介者責任制度中要求中介者對內容主動進行監控。

2. 原則二: 沒有司法機關命令，不得要求「中介者」對內容進行限制

依此原則，除非要求內容下架之一方為獨立且公正之司法機關，不得要求中介者在未取得系爭內容上架者同意之情況下，對內容限

[48] 同註 47，頁 6。
[49] 同註 47，頁 8。
[50] 2015 年馬尼拉原則「最佳實踐指引」，頁 2，電子前哨基金會官方網站 https://www.eff.org/files/2015/10/31/manila_principles_1.0.pdf（（最後瀏覽日：2021 年 6 月 30 日）。

制之命令或請求有任何作為[51]。依據馬尼拉原則 2015 年之「最佳實踐指引」法律規範應包括以下面向[52]：

(a) 除非一個獨立且公正的司法機關發布命令認定爭議內容為非法，否則不得要求中介者對內容進行限制。

(b) 對內容進行限制的命令必須：

i. 認定該內容在其管轄區域內屬於非法。

ii. 指出網際網路識別元及非法內容的描述。

iii. 提供充分的證據證明命令的法律依據。

iv. 在適用情況下，指出限制內容的限制期間。

(c) 如果中介者沒有適當地遵守內容限制的命令，中介者所須承擔的一切責任必須與該不當行為合乎比例並直接相關。

(d) 如果內容限制的命令不符合此項原則，中介者不得被要求對沒有遵守該命令負責。

3. 原則三:內容限制請求必須清晰、明確，且依照正當程序

此原則係屬上述原則二之衍生原則，即內容限制要求者須為司法機關，惟當政府行政機關或私人，在尚未請求司法機關作為前，投訴或要求內容限制時，該政府或私人之要求須必須清晰、明確，且依照正當程序[53]。依據馬尼拉原則 2015 年之「最佳實踐指引」法律規範應包括以下面向[54]：

(a) 中介者不得被要求對第三方內容的合法性進行實質性評估。

(b) 針對非法內容的內容限制請求至少必須包含下列項目：

[51] 同註 32，頁 25。
[52] 同註 32，頁 2。
[53] 同註 32，頁 30。
[54] 同註 32，頁 3。

i. 主張該內容為非法的法律依據。

ii. 網際網路識別元及據稱非法內容的描述。

iii. 對使用者內容提供者提供適用的限制、例外，和抗辯判斷基準。

iv. 除法律禁止的情況外，請求檢舉人或其代理人的聯繫方式。

v. 足以證明該請求法律依據的證據。

vi. 所提供資訊正確無誤的善意聲明。

(c) 屬於中介者內容限制政策之內容限制請求，至少必須包含下列項目：

i. 爭議內容違反中介者內容限制政策的原因。

ii. 網際網路識別元及據稱違反內容限制政策情況的描述。

iii. 除法律禁止的情況外，請求發起方或其代理人的聯繫方式。

iv. 所提供資訊正確無誤的善意聲明。

(d) 代管內容的中介者得依法律規定對關於非法內容的內容限制請求作出回應，將合法並符合條件的請求轉發給使用者內容提供者，或者通知投訴人內容不合法之原因。不得要求中介者確保其有能力識別使用者。

(e) 在轉發請求時，中介者必須對使用者內容提供者的權利提供清晰易懂的解釋，包含法律強制中介者對內容進行限制時任何適用之反通知或上訴機制。

(f) 如果中介者基於內容限制請求對他們代管的內容進行限制，他們必須遵守下方關於透明度和問責機制。

(g) 濫用或惡意的內容限制請求應受處罰。

4. 原則四:法律、內容限制命令，和實務作法必須通過必要性和比例原

則的檢驗

依據馬尼拉原則 2015 年之「最佳實踐指引」法律規範應包括以下面向[55]：

(a) 所有內容限制必須局限於特定之爭議內容。

(b) 在對內容進行限制時，必須採用限制性最低的技術手段。

(c) 如果內容是因為在特定地理區域屬於違法而被限制，而中介者針提供因地域而異的服務，那麼內容限制應局限於該地理範圍內。

(d) 如果內容是因為在一定期間內屬於非法而被限制，那麼限制不能持續超過該期間，並應該定期檢視限制命令以確保其仍然有效。

5. 原則五:法律、內容限制政策，和實務做法必須遵循正當程序

承上述原則三關於正當程序之原則，此為馬尼拉原則第二個有關正當程序之原則。本原則五係為使中介者內部政策亦遵循正當程序確保沒有恣意的內容限制並避免政府機關以法律以外之手段施壓中介者自願性的對網路內容予以限制[56]。依據馬尼拉原則 2015 年之「最佳實踐指引」，法律規範應包括以下面向[57]：

(a) 除有特殊情況，否則基於命令或請求而對任何內容進行限制之前，中介者和使用者內容提供者必須被賦予有效的陳述權。在特殊情況下，必須盡快對該命令及其執行進行事後審查。

(b) 任何規範中介者的法律必須賦予使用者內容提供者和中介者對內容限制命令的上訴權。

(c) 使用者內容提供者違反中介者的內容限制政策，中介者應對其提供複查內容限制決定的機制。

[55] 同註 32，頁 4。
[56] 同註 32，頁 40。
[57] 同註 32，頁 4。

(d) 如果使用者內容提供者在根據（b）上訴成功或者根據（c）的複查否決內容限制，中介者應恢復內容。

(e) 中介者不應於沒有司法機關命令時揭露關於使用者的個人識別資訊。中介者責任制度不得要求中介者在沒有司法機關命令時揭露任何個人識別之使用者資訊。

(f) 中介者草擬和執行其內容限制政策時應該尊重人權。同樣地，政府也有義務確保中介者的內容限制政策尊重人權。

6. 原則六:透明度和問責機制必須建立在法律、內容限制政策和實務做法中

此原則主要係為中介者與使用者間之服務條款透明度與問責制度而設，並使中介者對於該服務條款之履行問責[58]。蓋中介者固然得依據其服務條款為內容限制，因此服務條款之透明度與其內建之制度須完整。依據馬尼拉原則 2015 年之「最佳實踐指引」法律規範應包括以下面向[59]：

(a) 政府必須及時以易存取的格式在線上公布所有與中介者責任相關的法律、政策、決定及其他形式的規定。

(b) 政府不得使用非司法措施對內容進行限制。這包括直接或間接強迫更改服務條款，推動或執行所謂「自律」的做法，以及達成限制交易或限制公開傳播內容的協議。

(c) 中介者應該以清楚的語言和易存取的格式在線上公布其內容限制政策，在更動時及時更新，並將變動適時通知使用者。

(d) 政府必須發布透明度報告，提供關於其發給中介者之所有內容命令和請求的特定資訊。

(e) 中介者應該發布透明度報告，提供其所為之所有內容限制的特定資訊，包括對政府請求、法律命令和私人投訴請求採取的行

[58] 同註 32，頁 48。
[59] 同註 32，頁 5。

動，以及內容限制政策的執行情況。

(f) 如果中介者可以在其產品或服務上顯示通知，那麼當使用者試圖存取其中被限制的內容時，中介者必須顯示明確通知，以解釋什麼內容被限制以及這麼做的理由。

(g) 政府、中介者和公民社會應該共同努力建立和維護獨立、透明、公正的監督機制，以確保可對內容限制政策與實務做法進行問責。

(h) 應於中介者責任框架和法律中，要求就規定及指引進行定期、系統性檢視，以確保它們為最新、有效，且不過分繁瑣。這類定期檢視應納入有關其執行情形及影響的證據蒐集機制，並應制定規章，對它們的代價、實質利益，及人權影響進行獨立審查。

三、DNS RPZ：源於解決技術濫用

網域名稱系統回應原則區域機制（下稱 DNS RPZ）為因應網域名稱濫用之重要處置手段，特別是面對境外網域名稱濫用，而無法找到網域名稱註冊人、具急迫性、或無法透過司法互助有效解決時，得有效因應網域名稱濫用之處置技術。DNS RPZ 源於網域名稱技術濫用，然而隨著網域名稱內容濫用越顯嚴重，近年亦有探討是否將此用於因應網域名稱內容濫用，然此將涉及對於網路言論之箝制，進而有是否須法律授權以符合法律保留原則之探討（參第六章第五節）。以下將詳細介紹之。

DNS RPZ[60]係由知名電腦科學家 Paul Vixie 先生於 2010 年鑒於網路惡意網域名稱猖獗情況所發展之技術[61]。由於越來越多惡意程式及殭屍網路利用網域名稱查詢惡意網域名稱的趨勢，透過 DNS RPZ 可即時向資安信譽評等機構訂閱惡意網域名稱黑名單及更新，而達到有效的惡意網域名稱偵測與防護措施[62]。

---

[60] DNS RPZ 官方網站，https://dnsrpz.info/ （最後瀏覽日：2021 年 6 月 30 日）。

[61] Paul Vixie, *Taking Back the DNS*, CircleID (Jul. 30, 2010), http://www.circleid.com/posts/20100728_taking_back_the_dns/.

[62] iThome， DNS 危機解密，https://www.ithome.com.tw/guest-post/106780（最後瀏覽日：2021 年 6 月 30 日）。

簡言之，DNS RPZ 如同網路管理者設定之防火牆[63]。DNS RPZ 的功能範例包括：阻擋使用者連結惡意網站或使其轉向內部安全網域名稱（於該網域名稱內警示使用者關於所欲連結網站屬於惡意網站），或阻擋使用者接取特定已知之惡意網域名稱，以避免惡意網站連結至其網域名稱系統伺服器（Domain Name System Server，下稱 DNS 伺服器）之作用[64]。其簡要功能簡介如下[65]:

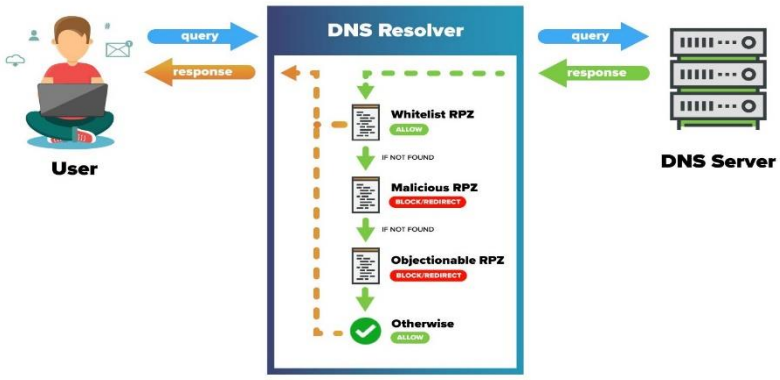


圖 4 DNS RPZ 示意圖

依上圖所示，網路使用者於指令連接至網站時（輸入網站名稱後），藉由網域名稱系統解析器（Domain Name System Resolver，下稱 DNS 解析器）得知 DNS 伺服器之回覆後，同時過濾並處理該網域名稱是否屬於惡意網站，如屬「非惡意網站區域」之名單（Whitelist RPZ），使用者則得連結至該網站，反之，如 DNS 伺服器經過 DNS 解析器過濾後，屬於「惡意網站區域」（Malicious RPZ）或「潛在問題區域」（Objectionable RPZ）名單內，DNS 解析器將自動阻擋該網域名稱或轉接使用者致其他網站或給予警示，以避免使用者連結到惡意網站。

除技術特色外，此機制特別之處在於 RPZ 之阻擋或轉接功能係基於第三方信譽評等機構而來，而此等評等機構之資料來源則非以網路內容而定，且阻擋或轉接之決定並非由註冊管理機構發動。此外，DNS RPZ

63 Omar Santos, *Using DNS RPZ to Block Malicious DNS Requests*, CISCO (Oct. 2, 2013.), https://blogs.cisco.com/security/using-dns-rpz-to-block-malicious-dns-requests.
64 Zvelo, Using DNS RPZ to Protect Against Malicious Threats, https://zvelo.com/using-dns-rpz-to-protect-against-malicious-threats/ (last visited Jun. 30, 2021).
65 *Id.*

機制之原意係為保障使用者受惡意網站之侵入而設（依據資安信譽評等機構訂閱網域名稱系統惡意域名黑名單），並非以網域名稱內容濫用是否存在網站內而過濾。此機制看似符合上述自律與他律機制之限制，且不屬於網域名稱內容之審查或限制。惟目前國際業者間尚無針對 DNS RPZ 之使用有統一之規範或要求。

TWNIC 於 2020 年 9 月 23 日發表其官方 DNS RPZ 簡要說明[66]。TWNIC DNS RPZ 防止國內使用者接取不當或惡意網域名稱，此可能涉及實質上剝奪台灣網路使用者閱覽、轉傳、分享網路資訊，涉及言論自由的限制。因此 TWNIC 以 DNS RPZ 限制惡意或不當網站必須有正當事由。正當事由可分為兩種類型，第一種類型為依據法律及因應法律規定所採取之行動，如兒童及少年福利與權益保障法第 46 條之 1 及動物傳染病防治條例第 38 條之 3 明文授權該管行政機關將經其認定為違法之網站內容為限制接取、瀏覽及移除。因此當有法院判決裁定或行政機關之行政處分時認定該網域名稱有內容濫用時，TWNIC 須配合停止解析該等網域名稱。另外如類型為網域名稱係有資安疑慮且影響資安重大者（技術濫用），即參考網域名稱濫用框架當註冊管理機構知悉有前述之網域名稱濫用情形時，註冊管理機構必須有所作為義務，因此當有危害資安之網域名稱濫用時，TWNIC 即須出面處理。

（一） 限制及困境

綜觀上述註冊管理機構之自律與他律機制，目前無論是 ICANN 之 UDRP 或是 TWNIC 之 TWDRP 機制，其可處理之爭議類型均有限制。若涉及網際網路內容或使用者行為時，則可歸納以下特點:

1. 於註冊管理機構知悉網域名稱有「惡意網站」之情形時，註冊管理機構必須有所作為。惟其能採取之唯一處理措施是將使整個網域名稱取消或停止解析。此措施無法精準移除該網域名稱之濫用部份，而僅能移除系爭網域名稱，包括其內所

[66] TWNIC 官方網站，https://blog.twnic.tw/2020/09/23/15311/ （最後瀏覽日：2021 年 6 月 30 日）。

有合法與非法內容及網域名稱之使用，如使用該網域名稱之電子郵件帳戶。

2. 除於特殊情況下，**國際註冊管理機構間之共識主要是以不介入網路內容或使用者行為之審查與處理**。註冊管理機構並認為移除網路內容之措施應於網站、網域名稱、伺服器服務商與投訴人間協調為之。註冊管理機構僅於有法院之命令之情況下，方須依該命令限制網域名稱內容或採取積極處理措施。

3. 網際網路網域名稱系統基礎建設之服務者，如 ICANN、註冊管理機構、受理註冊機構，均無就網路內容或網路使用者濫用情形之審查或處理之法律與合約依據。惟得依上述框架與原則通知適當之人，例如網站管理者（Site Operator）、註冊人（Registrant）或伺服器服務提供者（Hosting provider）。

4. 依據馬尼拉原則，網路中介人（如社群網站平臺業者，受理註冊機構、內容整合業者、ISP 業者等）應免於對 UGC 負責且不應對 UCG 內容作任何審查或內容限制。

5. 任何對於網路內容或使用者行為之限制，均須合乎比例原則。

因此，目前網域名稱濫用之自律或他律機制，大致上可分為：（一）依 UDPR 及 URS 處理網域名稱涉及商標權之濫用；及（二）依網域名稱濫用框架涉及資安之濫用。原則上，基於網域名稱系統業者與註冊管理機構在網際網路之基礎架構中之角色，**上述機制均無法作為註冊管理機構因網路內容或使用者行為，直接取消網域名稱之依據**，**僅於註冊管理機構收到法院命令時，方得為之**。實務上一般亦認為，無論係因法院命令或其他原因註冊管理機構取消網域名稱，註冊人或使用者亦得立即或事後將相同網域名稱內容或使用者行為複製於新註冊或其他網域名稱。

（二） DNS RPZ 先天限制

由上述 DNS RPZ 之介紹可知，其係阻斷 DNS 快取伺服器之解析功能，惟，並非所有 DNS 快取伺服器均有加入我國 DNS RPZ 之協定，是以，縱 TWNIC 將該網站列為 DNS RPZ 黑名單，只要網路瀏覽者使用其他 DNS 解析器，依然可以順暢連到 DNS RPZ 黑名單之網站。此外，利用網域名稱技術達到之網路遮蔽手段無法進行比例原則之判斷，以臉書（facebook）為例，以網域名稱技術停止該網站之解析僅能一次遮蔽整個網站，如欲就該網站之特定貼文進行遮蔽，僅能採取 DNS 以外之技術為之。

第四節 網域名稱濫用處置手段及方式整理

針對網域名稱濫用之處置手段，可分為以下五種類型：

一、APNIC、TWNIC 取消網域名稱：此手段係指註冊管理機構本於其受理網域名稱登記之權限，自然有能力將網域名稱取消。

二、TWNIC 針對「.tw」網域名稱進行 Server Hold：此手段係指 TWNIC 基於其為「.tw」之註冊管理機構，本於其權限於網域名稱上加入“serverHold”的狀態，則整個 TWNIC 的 DNS 會停止此網域名稱的名稱伺服器，進而使所有 DNS 都停止解析該網域名稱。

三、DNS RPZ 停止解析：此手段係指 TWNIC 與境內 ISP 業者合作，將特定境內及境外網域名稱停止解析，使境內之網路使用人難以接觸至該網域名稱。惟網路使用人使用其他快取主機或 VPN 連線後，仍可閱覽停止解析之網域名稱內容。

四、通知伺服器業者或是平臺業者刪除特定內容：此手段係指違法不當網域內容存放於特定伺服器或平臺業者時，主管機關或第三方機構得通知定伺服器或平臺業者將相關內容刪除。

五、通知業者、創作人刪除特定內容：此手段係指針對違法不當網域名稱內容，主管機關或第三方機構得通知創作人將網域名稱違法不當內容刪除。

六、業者自律：即針對網域名稱濫用行為，行政機關不主動介入通知 TWNIC、ISP 業者將該等網域名稱停止解析或刪除內容，而係透過「民間第三方機構」（如我國 iWIN）通知相關 ISP 業者、平臺業者、創作人之方式，將不當違法內容刪除或是停止解析相關網域名稱。

以下為方便讀者理解各技術及手段之優缺點，以下面表格加以呈現：

表 3 網域名稱濫用處置技術及手段之優缺點

	APNIC、TWNIC 取消網域名稱	TWNIC 針對「.tw」網域名稱進行 Server Hold	DNS RPZ 停止解析	通知伺服器業者或是平臺業者刪除特定內容	通知創作人刪除特定內容	業者自律
優	取消網域名稱後，全世界網路使用人使用任何途徑皆無法瀏覽該網站	對「.tw」網域名稱使用 Server Hold 後，能確保全世界及使用任何途徑都無法瀏覽該網站	1. 適用範圍廣，不論境內、境外網域名稱均可使用。 2.具時效性 3. 不須找到「網域名稱濫用之行為人」即可為之。	就特定內容進行內容下架，能落實「最小侵害」	就特定內容進行內容下架，能落實「最小侵害」	1. 無公權力介入。 2. 無法律保留的疑慮。 3. 具時效性。
缺	1.難確保境外註冊管理機構確實取消網域名稱 2.不具時效性 3.具不可回復性，侵害過大，可能不符合比例原則	1.僅限「.tw」網域名稱 2.侵害過大，不符合最小侵害	1.網路使用人使用其他快取主機或 VPN 連線後，仍有機會閱覽受停止解析之網域名稱內容。 2.僅能停止解析整個網站，當網域名稱僅有部分涉及濫用時，此手段將不符合比例原則。	1.須確認內容存在之網域名稱為伺服器業者依服務規章得將其刪除。 2.除法律有特別明文外，須待司法程序為之，不具時效性	1.須確實找到「網域名稱濫用之行為人」 2.除法律有特別明文外，須待司法程序為之，不具時效性	1. 針對涉及專業之「網域名稱技術濫用」民間機構無通報能力。 2. 民間機關通報之成效難以預期。

又行政機關、司法機關及網路使用關係人面對現行網域名稱濫用，羅列潛在可因應之方式有：

一、**行政處分**：即立法明文主管機關得做成「限制接取、瀏覽或移除相關網頁內容」之處分。

二、**行政執行**：管制性規定存在，主管機關為落實規定而為直接強制、即時強制之手段。

三、**刑事扣押**：刑事實體法明定之各項犯罪行為，並對各項犯罪行為使用到之網域名稱進行扣押。

四、**民事暫時狀態假處分**：依民事訴訟法第 538 條及民法相關規定（如第 18 條人格權保護）或是智慧財產案件審理法第 22 條[67]，對濫用之網域名稱請求將網域名稱停止解析及網域名稱內容刪除。

五、**偵查機關直接通知**：偵查機關本於調查犯罪職權，針對發現網域名稱濫用事實，以不具拘束力之通知，通知各業者請其本於與消費者間契約條款等為適當處置。

六、**民間機構通報**：由民間機關通知各業者，為自律機制，其通報無須法源依據。

上述六種方式各有其優點及無法避免之缺點。故因應網域名稱濫用情事之急迫性及現行法制之齊備與否，而選擇不同之處理方式。如法律已授權而具有社會共識，則機關得以行政處分方式，對濫用之網域名稱進行適當處置。如未有法律授權，惟網域名稱濫用情勢急迫且涉及刑事犯罪，則得採取刑事局通知各業者方式進行處置。非涉及刑事犯罪或其他一般情形，則得採取民間機構通報各業者方式，以迴避潛在干涉言論自由之疑慮。

[67] 智慧財產法院民事裁定 104 年度民暫字第 3 號裁定。

以下為方便讀者理解各因應方式之優缺點，以下面表格加以呈現：

表 4 網域名稱濫用處置方式之優缺點

	行政處分	行政執行	刑事扣押	民事暫時狀態假處分	偵查機關直接通知	民間機構通報
法源依據/法律保留	立法明文或授權主管機關得公告相關措施，如：「限制接取、瀏覽或移除相關網頁內容」。	管制性規定存在，主管機關為落實規定而為直接強制、即時強制之手段。	刑事實體法明定之各項犯罪行為	民事訴訟法第538條 民法相關規定（如第18條人格權保護）	由偵察機關本於調查犯罪職權，通知各業者，請業者本於與消費者間契約條款等為適當處置，為自律機制。	由民間機關通報各業者，為自律機制，通知非行政處分，無違反法律保留疑慮。
優	具時效性，且專責之處分機關具備該領域之專業性	可確實落實各管制性法規之目的	符合程序正義	符合程序正義	最為迅速，可在當日完成	無公權力介入，無違法法律保留的疑慮，具時效性
缺	如行政機關得「限制接取、瀏覽或移除相關網頁內容」之範圍過大，有干涉言論自由之疑慮。	行政執行法第28條直接強制及第36條即時強制並未直接明文「限制接取、瀏覽或移除相關網頁內容」可做為執行之手段，故僅能適用同條之概括規定。如受處分人對行政執行有所疑義，進入法律爭訟，行政機關即須面臨法院審酌執行是否合於比例原則及正當目的。	緩不濟急，且針對找不到犯罪人之情況，無從執行。	需特定相對人，且可能找不到相對人之情況，即無從聲請。	刑事局及調查局有公權力，會有規避法律保留的疑慮	針對涉及專業之「網域名稱技術濫用」民間機構無通報之能力，且民間機關通報之成效難以預期。

第三章研析網域名稱濫用代表性案例

第一節 國內網域名稱濫用（DNS Abuse）案例研析

第一項 網域名稱技術濫用案例－雪崩（Avalanche）殭屍網路國際犯罪集團案

（一） 案例背景

1. 「雪崩（Avalanche）」犯罪集團專門從事散布惡意程式，進行針對性地攻擊網路銀行，其濫用行為之態樣包含殭屍網絡、惡意軟體和勒索軟體之託管和管理系統。估計在德國境內已造成 600 萬歐元的損失，而透過「雪崩」進行的網路駭侵更造成全球的經濟損失，歐洲刑警組織表示，全球所遭受的損失可能高達億萬美元，由於該平臺管理的惡意軟體及家族量太多，具體損失難以統計[68]。

2. 雪崩殭屍網路案歷經四年調查，包含我國調查局人員，全球共有 31 個國家執法機關派員成立專案組研商案情、分配任務，並聯合美國、歐洲刑警組織（Europol）、歐洲檢察官組織（Eurojust）及全球執法機關共同合作採取行動，通過與網際網路服務提供商 ISP 協作[69]。

3. 於西元 2016 年 11 月 30 日全球同步進行搜索扣押，此次行動逮捕人數 5 人，搜索處所 37 處，扣押伺服主機 39 部，強制離線伺服主機 221 部，係有史以來最大型的監控惡意網路流量及打擊殭屍網路行動，總計超過 80 萬個惡意網域名稱受到阻斷，國內（台灣）由法務部調查局協請 TWNIC 同步阻斷 3 萬 3,925 筆惡意網域名稱[70]。

（二） 案例分析

1. 近年來歐洲所面臨的重大安全威脅來自恐怖主義、國際毒品運輸、洗錢、組織性詐騙、偽造歐元與人口販運，因此分別設立了歐洲網路犯罪中心（European Cybercrime Centre, EC3）、歐洲人口販運防治中心

[68] E 安全，全球最大殭屍網絡基礎設施平台—雪崩 Avalanche 已造成億萬美金損失，微文庫 https://www.gushiciku.cn/dc_hk/108488677（最後瀏覽日：2021 年 6 月 30 日）。

[69] 陳念祖，法務部調查局與美國、歐洲刑警組織共同偵破「雪崩」殭屍網路案，台灣 TB 新聞網 http://tbnews.com.tw/society/20161202-12225.html （最後瀏覽日：2021 年 6 月 30 日）。

[70] 同上註。

（European Migrant Smuggling Centre, EMSC）、歐洲反恐中心（European Counter Terrorism Centre, ECTC）與智慧財產犯罪協調辦公室（Intellectual Property Crime Coordinated Coalition, IPC3）等機構，加以因應[71]。本案即在該背景下，成為近年歐盟與我國刑事司法合作之指標案例。

2. 目前歐洲刑警組織對外得與歐盟以外的第三國簽訂兩種合作協議，第一種是策略協議，第二種是行動協議，其差異在於前者不允許交換個人資料，後者則可。歐洲刑警組織的網路犯罪中心與我國司法警察機關有著良好的合作關係[72]，例如於雪崩 Avalanche 殭屍網路國際犯罪集團案中，即與我國法務部調查局合作，成立本案聯合調查團隊，透過我國調查局協請 TWNIC 同步阻斷三萬三千九百廿五筆惡意網域名稱。

3. 參照本案例之成功經驗，**我國未來可考慮與歐洲刑警組織或其他國際組織締結協議，成為合作夥伴**，以共同打擊網路犯罪為目標達成刑事司法互助，逐步深化合作關係。

第二項　網域名稱內容濫用案例－楓林網影音著作盜版侵權案

（一） 案例背景

1. 桃園地方檢察署於 2019 年 11 月 9 日發布新聞稿表示，33 歲陳男與 32 歲莊男經營「楓林網」，自 2015 年起結合大陸人士，在外國租用雲端主機，將未經授權電影、戲劇、影集等擅自下載至網站，或將其他網站檔案連結直接嵌入「楓林網」，供不特定人免費觀看，並在網頁及影片播放中安插廣告藉此牟利。被告等人遭著作權人史坦利國際傳媒公司、三立電視公司、富士電視台公司、采昌國際多媒體公司、華納兄弟娛樂公司等企業蒐證提起刑事告訴[73]。

[71] 鄭文中，淺論歐盟刑事司法合作之歷史發展，台灣國際研究季刊第 14 卷第 3 期，頁 45，2018 年 9 月。
[72] 同上註。
[73] 吳睿騏，楓林網盜版侵權 檢方起訴 2 犯嫌查扣財產 6700 萬，中央社

2. 桃園地檢署除依違反著作權法提起公訴，另查扣價值約 6700 多萬元財產。根據警方公告，破獲的非法網站「楓林網」之網域名稱為（8maple.ru）該網域名稱利用註冊境外主機，架設免費影視頻道，供不特定民眾觀賞。警方查緝楓林網 8 個網址對應 25 臺雲端主機部分已經依法查扣並針對網站主機封網[74]。最近疑似復活的楓林網，應該是分站，因為原本被封鎖的網域名稱只有「8maple.ru」，換一個網域名稱後（https://imaple.tv/），目前網友仍可以瀏覽網站觀賞戲劇[75]。

3. 盜版影音網站存在台灣多年，盜版網站會將伺服器設在國外，或是租用境外網址，並在不同國家多點架設，成立多個備援網站，分散風險，且盜版網站最常使用層層轉址的方式，引導至不同伺服器，使得執法單位難以追查。

圖 5 內政部警政署刑事警察局之網站查禁公告 （圖片來源[1]）

https://www.cna.com.tw/news/firstnews/202011090258.aspx（最後瀏覽日：2021 年 6 月 30 日）。

[74] T 客邦，楓林網被關為什麼 Google 還有「楓林網」存在？而且你依然拿他們沒辦法，遊戲角落，https://game.udn.com/game/story/10455/4477602（最後瀏覽日：2021 年 6 月 30 日）。

[75] 黃瀞儀，楓林網起死回生？網驚曝：時下最夯劇都可以看，中時新聞網 https://www.chinatimes.com/realtimenews/20200813005426-260402?chdtv（最後瀏覽日：2021 年 6 月 30 日）。

（二） 案例分析

1. 經檢視近期各國家法制對於網路侵權責任之相關立法以及實際案例後，可歸納目前近期立法趨勢為透過封鎖境外網站以及課予 ISP 業者監控義務遂行保障網路著作權之目的[76]，少有係直接針對網域名稱進行扣押或其他行政處置手段，過去也常遭遇因伺服器分散各國，若想查封盜版網站，需與他國簽署司法互助協議始有依據進行，然而與我國簽署司法互助協議之國家並不多。而本案件係在此背景下，警方似採取直接針對侵權網站所使用之網域名稱進行扣押，惟經本團隊實際查證，本案並未對網域名稱進行扣押，係於確認侵權人機房之地址後，扣押其所有伺服器以達到限制楓林網繼續運作之結果。

2. 惟本案確實有討論過對網域名稱進行扣押之可能，是以，未來可能的衍生議題為，在著作權侵權案例且侵權人不明的情況下，警方或受侵害之人，亦可聲請將侵權網站之網域名稱扣押，使民眾無法再連結至該網站。對此議題後續有 110 年度聲扣字第 11 號裁定，成功說服法院針對違反著作權之網域名稱，核發扣押命令要求 NameCheap 公司及 GoDaddy 公司暫停網路服務，亦命 TWNIC 將該網域名稱列入 DNS RPZ 停止該網域名稱之解析。

第三項　網域名稱內容濫用案例－SWAG 關閉網站案

（一） 案例背景

1. 知名本土成人影片網站 SWAG 為規避檢警偵查將**伺服器架設於美國。**其後經查發現公司位置實際設立於台北市松山區並由「攻城獅」科技公司經營。刑事局於 3 月接獲檢舉，電信偵查大隊透過付費金流進行追查。於 4 月初刑事局電偵大隊持搜索票至公司進行搜索，並將劉姓負責人、員工、工程師等 35 人帶回偵辦。訊後劉姓負責人

[76] 洪爾謙，著作權法下管制侵權內容之法律研究─以封鎖境外網站為中心，國立清華大學科技法律研究所碩士論文，頁 3，2014 年。

夫婦、員工以及工程師等 5 人依妨礙風化罪嫌送辦，檢方諭令劉姓負責人 30 萬元交保[77]。

2. 警方表示除女優自行拍攝影片外，公司亦會協助找攝影棚。會員支付台幣 1 元購買 30 顆「鑽石」，觀看每部影片需 250 顆「鑽石」，每次觀看時，女優可分紅 30 至 40 顆「鑽石」。因網站不具過濾會員身分機制，而供不特定者瀏覽，涉犯妨害風化罪。**警方共查扣五台電腦，含管理帳號及密碼、直播主會員資料，並取得 SWAG 管理權限，封鎖網站（要求網站暫時關閉）避免持續散布色情內容**[78]。

3. 2021 年 3 月底以來，該網站存在但無法登入觀覽。SWAG 並於 4 月 3 日發出聲明表示，因接獲刑事警察局電偵大隊通知，需調整審查機制及使用者註冊流程以符合當地法規。另為兼顧保護未成年人及提供良好的成人娛樂內容，將持續建立完善的審查機制，以更嚴謹態度杜絕違法內容，並據註冊方式及付費管道，建立使用者年齡門檻，防止未成年人瀏覽[79]。

（二） 案例分析

1. 本件案例之網域名稱內容涉及播放露骨性愛影片，而被刑事局認為有違反刑法第 235 條散布、播送或販賣猥褻影像之罪嫌而移送法辦。此涉及網域名稱內容被認為違反法律時，行政機關可否關閉網站之爭議。

2. 經查 SWAG 網域名稱位置為「https://app.swag.live」。「.live」網域名稱註冊者多為媒體廣播公司、娛樂場所、數位活動提供者、提供線上影片教學的教育單位等具有線上影音串流需求者。註冊.live 可將其指向您位於 Periscope、Blab、Twitch、YouTube、或其他串流應用程式的即時串流頻道[80]。

---

[77] 新頭殼 newtalk，「亞洲最大」成人平台 SWAG 被抄 會員哀嚎擔憂「鑽石」會費要不回，https://newtalk.tw/news/view/2021-04-04/558670 （最後瀏覽日：2021 年 6 月 30 日）。

[78] 聯合新聞網，播台女露點片 色情網 SWAG 被抄，https://udn.com/news/story/7315/5362885（最後瀏覽日：2021 年 6 月 30 日）。

[78] https://hi-in.facebook.com/SWAGRecruitment/posts/256462022883803/

[80] Godaddy，.live 網域名稱，https://tw.godaddy.com/tlds/live-domain （最後瀏覽日：2021 年 6 月 30 日）。

3. 據新聞所述，本案並未直接將網域名稱取消，而係因網域名稱負責人在境內，得透過搜索扣押公司電腦，包含管理帳號及密碼、直播主、會員資料，並取**得 SWAG 網站管理權限，而直接封鎖網站內容，並未將該網域名稱取消，或停止解析該網域名稱**。

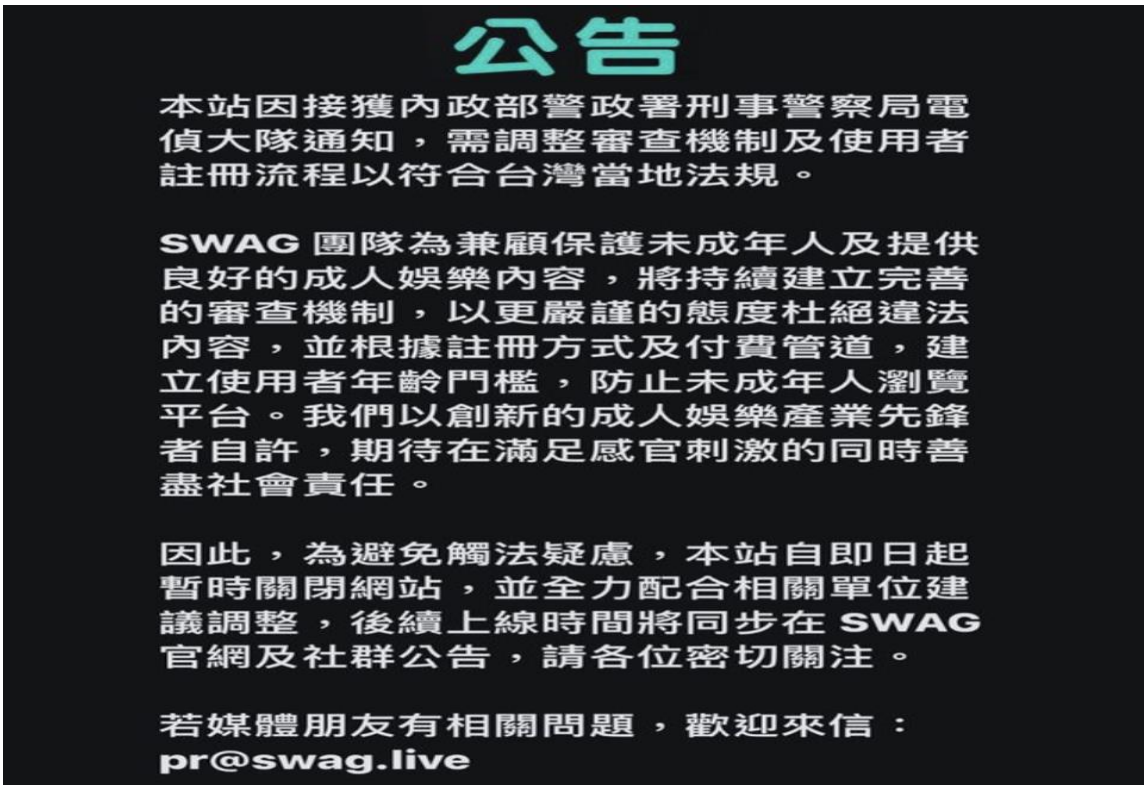


圖 6 SWAG 網站上覆蓋頁面

（三） 本案後續影響

1. 本案為繼楓林網案，以國內查緝到經營者本人後，再進一步將網站內容下架之案例。值得探討部分為「.live」屬國外網域名稱並非 TWNIC 註冊管理機構所管轄。故國外網域名稱內容濫用時，除查緝到經營者本人外，亦有其他方式得處理內容濫用之網域名稱，如參考以 110 年度聲扣字第 11 號裁定命註冊管理機構停止網路服務，及命 TWNIC 將該網域名稱列入 DNS RPZ 以停止該網域名稱之解析。
2. 連結至本案網域名稱「https://app.swag.live」，即可發現網站被重新指向至刑事警察局電偵大隊網站。此種技術與 DNS RPZ 技術之應用無

關，且經本所查證，本案法院有通知相關單位將 SWAG 網站之網域名稱為進一步處置，惟最後因為法院之通知並不明確，而未予執行。

第四項　網域名稱內容濫用案例－小鴨、劇迷等網站網域名稱扣押案

（一） 案例背景

1. 本件犯罪嫌疑人透過國外受理註冊機構 NameCheap 公司及 GoDaddy 公司註冊「.tv」、「.co」、「.to」、「.net」、「.com」、「.cc」等網域名稱，供大眾透過網路得觀看具有著作權之影音，而侵害著作權人之公開傳輸權，並依著作權法第 92 條及第 101 條第 1 項負有刑事責任。

2. 刑事警察局向法院提出 NameCheap 公司及 GoDaddy 公司之通用服務條款協議(下稱服務協議)，及國際組織 ICANN 所提供之 Guidance for Preparing Domain Name Orders, Seizures & Takedowns（網域名稱扣押指引，下稱「扣押指引」）為據，釋明將我國之法院裁判通知 NameCheap 公司及 GoDaddy 公司後，兩間公司即會依據服務協議及扣押指引而限制本件網址之使用、轉讓或其他處分。此外，透過 TWNIC 停止解析該等網站及對應 IP 之方式，使本案所涉網址無法使用，並藉此將本件網域名稱納入我國公權力支配之下，而得為扣押處分。

3. 因上述理由，本件審理法院認為本案涉及之網域名稱依刑事警察局之釋明，足認該網域名稱應得由我國司法機關進行扣押，即以 **110 年度聲扣字第 11 號裁定命** NameCheap 公司及 GoDaddy 公司暫停網路服務，亦命 TWNIC 將該網域名稱列入 DNS RPZ 以停止該網域名稱之解析。

（二） 案例分析

1. 網域名稱得否作為扣押之標的一直為我國司法實務上困擾之事，本件案例應屬第一件具體明確說明網域名稱得作為扣押之標的。

2. 本件法律依據為刑事訴訟法第 133 條第 1 項可為證據或得沒收之物，得扣押之。又扣押之意思表示於到達扣押物之持有人（含所有人），

並將應行扣押之物移入公權力之支配下，其扣押之行為即屬完成[81]。本件犯罪嫌疑人於境內，故並無裁定送達之困難。惟網域名稱是否得為扣押之「物」，及是否得置於「公權力之支配下」非無疑問[82]。依刑法第 38 條第 2 項供犯罪所用、犯罪預備之物或犯罪所生之物，屬於犯罪行為人者，得沒收之。本件網域名稱提供公眾得任意地接觸具著作權之影音，而屬於施行著作權法第 92 條犯罪行為之工具。然而網域名稱並非有體物，因此是否屬於刑法第 38 條第 2 項所稱之「物」，即非無爭議[83]，而對此本件裁定並未詳實說明此部分爭議。

3. 又網域名稱置於「公權力之支配下」，始達成扣押之本旨。本件法院採信聲請人引用 NameCheap 公司及 GoDaddy 公司之服務協議及扣押指引，只要本件具有法院裁定或判決通知兩間公司即會依據服務協議及扣押指引而限制本件網址之使用、轉讓或其他處分。是以本裁定作成後，將會通知 NameCheap 公司及 GoDaddy 公司進行後續程序處理，並透過 TWNIC 停止解析該等網站及對應 IP 之方式使本網址無法使用。

4. 透過 WHOIS 網站查找裁定所扣押之網域名稱，於網域名稱狀態上顯示禁止移轉，且嘗試連結至該網域名稱然顯示無法連上這個網站。故應可認為確實置於「公權力之支配下」而達成扣押之本旨。

（三） 本案後續影響

1. 本件具開創性將網域名稱作為可被扣押之標的。後續是否會有其他裁定採相同見解或是另有其他看法，值得我們關注。

2. 本件網域名稱持有人於境內，故扣押裁定即扣押之意思表示送達至犯罪嫌疑人並不困難。然而有更多時候，基於網路之匿名性無法確知

[81] 參最高法院 71 年度台上字第 2360 號判決。

[82] 如後續法院實務認為網域名稱非得以扣押之物，則僅能可慮是否於著作權法或相關法律中定明「限制我國網路使用者接取、瀏覽之措施、先行移除或使他人無法進入該涉有侵權之內容或相關資訊」，使 TWNIC 得依行政機關作成之處分使用 DNS RPZ 停止解析侵權網域名稱。

[83] 有論者認為金錢、比特幣等非有體物可作為扣押之標的，且刑法第 10 條第 6 項及刑事訴訟法第 122 條有針對電磁紀錄等非有體物進行規範。故網域名稱亦應得作為扣押之標的。

犯罪嫌疑人，此時針對違法濫用之網域名稱是否得逕為扣押非無疑問[84]。

第五項　網域名稱內容濫用案例－「安博盒子（Unblock Box）」侵害著作權案

（一）案例背景

1. 「安博盒子（Unblock Box）」是一種可透過網路收看影音的數位機上盒，因廠牌叫 UNBLOCK（解除封鎖），故得名之。除可透過安博盒子觀看免費的合法播放內容外，並可透過安裝特定 APP 來收看更多的違反著作權法等侵權節目，該行為態樣不只對影視產業造成莫大衝擊，也使得「為內容付費」的觀念難以建立。根據資策會服務創新研究所 2018 年調查，若以全臺 2,642 萬名 4G 用戶估算，經由盜版網站及 APP 觀看影音內容比例高達 79.9%，被侵權的國內外頻道已超過百個，產業的損失一年將達 283 億元[85]。

2. 安博盒子目前在各大台灣電商都可以直接購買到，不只愛爾達遭受盜播影響，其他合法業者也遭受重大損失，東京奧運期間，許多民眾透過觀看轉播東京奧運賽事為台灣選手加油，但卻爆出有公眾人物使用盜版安博盒子收看賽事，引來撻伐，通傳會也於社群軟體上發文呼籲，提醒未經 NCC 型式認證的射頻器材均不得販售，並將持續配合經濟部智慧財產局、刑事警察局電信偵查大隊一同打擊侵權之數位機上盒[86]。

---

[84] 可能的方向為將網域名稱導向刑事警察局網站，透過此方式告知網域名稱持有人，其網站內容可能有違法之虞，請盡快與刑事警察局連繫，作為送達扣押處分方法之一。

[85] 莊伯仲，三招解決盜版的安博盒子，https://tw.sports.yahoo.com/news/%E8%8E%8A%E4%BC%AF%E4%BB%B2-%E4%B8%89%E6%8B%9B%E8%A7%A3%E6%B1%BA%E7%9B%9C%E7%89%88%E7%9A%84%E5%AE%89%E5%8D%9A%E7%9B%92%E5%AD%90-033000491.html?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAAE_0ceb_oNEvNAquXnRFleiZ1lz5yBKU-bboOStCJKgPBlHta_oATMGhn0d5WVwo9NoUGj99JwdPAIYB7PXERCD3e3vHYjtgR5jWuERr5UBZDqWyptUP_DNOnQgBCUc0lwg4WPo_B_sO8TZfEk25Wvxfm9WuF63p189NSI_HYXyG（最後瀏覽日：２０２１年 9 月 20 日）。

[86] 安博盒子看東京奧運爆爭議，非法機上盒看直播免罰、製造販售 3 行為將遭殃，數位時代，https://www.bnext.com.tw/article/64244/ncc-stb-unblocktech（最後瀏覽日：2021 年 9 月 20 日）。

（二） 案例分析

1. 機上盒的審驗機關是通傳會，但這純粹是因機上盒具備 WiFi 或藍牙無線射頻功能，為避免射頻功能過強，影響用戶健康或干擾網路、手機、廣播頻道等電波，或是功能過弱，造成經常斷訊、難以收視，故應依電信管理法第 66 條經核准，始得販賣電信管制射頻器材。由於不肖業者常以通過 NCC 審驗，誤導外界以為內容也是經過合法認證，NCC 經過多次抽驗後，也曾廢止審驗後另以不符規定製品行銷的機上盒之認證。然而上述 NCC 行政措施與打擊盜版並無直接關聯，只是多少影響非法機上盒之行銷而已[87]。

2. 據台灣高等檢察署表示，數位機上盒之典型犯罪手法為盜版非法業者一方面自設串流伺服器機房，擷取重製國內外戲劇節目及重要賽事訊號；一方面與不肖之電腦程式技術業者勾結，由電腦技術業者提供消費者數位機上盒及內建程式（有時提供指引，由消費者另行自行下載），供消費者點選數位機上盒內建之軟體，向串流伺服器機房產生要求，串流伺服器即將壓縮之影音資訊封包傳輸至機上盒轉至電視供消費者收看，完成非法的公開播送及公開傳輸[88]。影音戲劇節目屬於視聽影音著作，原本即受著作權法之保護；至於運動賽事，（包含全程錄影、轉播與球評），實務亦認屬於視聽著作，除在報導之必要範圍內可以合理使用之外，同樣受著作權法之保護，亦即任何人不得擅自以下載重製、擷取直播訊號公開播送、公開傳輸等方法侵害著作權，故前述行為中，提供機房主可能遭依著作權法第 91 條至第 92 條之規定進行追訴，最重五年以下有期徒刑。

3. 我國 2019 年 5 月著作權法新法正式施行，新法中有針對要非法機上盒上游相關產業鏈規範著作權法第 87 條第 8 款「明知他人公開播送或公開傳輸之著作侵害著作財產權，意圖供公眾透過網路接觸該等著作，有下列情形之一而受有利益者：（一）提供公眾使用匯集該等

[87] 章忠信，機上盒侵害著作權之法律防制，著作權筆記，http://www.copyrightnote.org/ArticleContent.aspx?ID=54&aid=2889（最後瀏覽日：2021 年 9 月 20 日）。

[88] 台灣高等檢察署，安博盒子裡的著作權《就像偷水電！全民瘋奧運 機上盒侵權》，https://www.tph.moj.gov.tw/4421/4475/632364/889417/post （最後瀏覽日：2021 年 9 月 20 日）。

著作網路位址之電腦程式。（二）指導、協助或預設路徑供公眾使用前目之電腦程式。（三）製造、輸入或銷售載有第一目之電腦程式之設備或器材。」之規定，目的為阻斷非法機上盒盜版影音來源之問題，是故販賣數位機上盒或程式之業者，則可能違反我國著作權法第87條規範，並依照著作權法第93條規定刑責最重為二年以下有期徒刑。

4. 經濟部智慧財產局表示[89]，依照著作權法，製造、輸入或銷售有連結侵權影音內容的機上盒，最重可處2年以下徒刑和新台幣50萬元罰金，惟依照現行著作權法之規範，確實無法裁罰使用安博盒子之消費者，只能進行道德勸說。

5. 解決芻議:

(1) 執法者加強取締：警政署刑事警察局應和法務部檢調單位、經濟部智慧財產局通力合作，取締此等破解訊號再分享於眾的違法行徑。安博盒子可以收看盜版影音內容，已是眾所皆知，而且隨處可買，何以仍然視若無睹、放任不管？既然多數消費者的使用動機就是侵權，而且相關APP均可公開下載，那麼有關單位應可循線追查，以現今科技水準來看，掃除違法機房在實務上並無困難[90]。

(2) 扣押侵權網站之網域名稱或伺服器：如同前述，過去著作權侵權網站等案例中，多係透過停止解析境外網域名稱以及課予ISP業者監控義務遂行保障網路著作權之目的，惟類似於前述楓林網及110年度聲扣字第11號裁定之案例分析，警方可採取直接針對侵權網站所使用之網域名稱進行扣押，或者扣押犯罪行為人所有之伺服器以達到限制安博盒子背後犯罪手法繼續運作之結果。

[89] 謝佳興，用安博盒子看東奧違不違法？ 經濟部智慧財產局揭曉答案，中央廣播電台，https://www.rti.org.tw/news/view/id/2107266 （最後瀏覽日：2021年9月20日）。

[90] 莊伯仲，解決安博盒子問題的幾點芻議，獨家報導，https://www.scooptw.com/thinktank/media/61898/%E8%A7%A3%E6%B1%BA%E5%AE%89%E5%8D%9A%E7%9B%92%E5%AD%90%E5%95%8F%E9%A1%8C%E7%9A%84%E5%B9%BE%E9%BB%9E%E8%8A%BB%E8%AD%B0/ （最後瀏覽日：2021年9月20日）。

第二節　國際網域名稱濫用（DNS Abuse）案例研析：

第一項　網域名稱技術濫用案例－Microsoft Corp. v. John Does 案

（一） 案例背景

2010 年 2 月，微軟第一次透過技術和法律結合之行動打擊殭屍網路 Waledac[91]。該殭屍網路每天發送 15 億封詐騙郵件，詐騙郵件會安裝惡意軟體在收信者電腦中，藉以竊電腦取使用者的金融和個人資訊。而且該批攻擊行動中，殭屍網路的惡意軟體偽裝成微軟官方軟體，讓用戶電腦不再作微軟官方的安全性升級，反而安裝了殭屍網路給的「防毒軟體」，微軟因此交到數千封客訴，使用者認為這些惡意信件是微軟發送的，並認為是微軟造成電腦故障。

（二） 微軟主張：

1. 實體法請求權：

(1)電腦詐欺及濫用法案(Computer Fraud and Abuse Act,下稱「CFAA」)：

駭客行為或者轉發惡意軟體的行為通常可以 CFAA 起訴。若駭客有未經授權、逾越授權利用他人電腦進行商業交易，而造成他人有五千美金以上之財產損害、醫療資源受損、人身損害或者影響公共衛生與安全時，CFAA 允許當事人請求損害賠償、核發禁制令以及請求損失補償[92]。

微軟指控 Waledac 入侵公司及全球各國客戶的電腦，未經授權地竊取資訊、詐欺並且在傳播惡意軟體時造成損害。

(2)反垃圾郵件法案（The Controlling the Assault of Non-Solicited Pornography And Marketing Act of 2003,下稱「CAN-SPAM」）：

依照 CAN-SPAM 法規定，執法機關或 ISP 業者得對濫發垃圾電郵之人提起民、刑事訴訟，而對於商用電郵之發送，該法亦要求應遵循一定之行為規範，諸如電郵內應提供收件人選擇退出寄送名單的

---

[91] *See* Tim Cranton, Cracking Down on Botnets, OFFICIAL MICROSOFT BLOG （Feb. 24, 2010）, https://blogs.microsoft.com/on-the-issues/2010/02/24/cracking-down-on-botnets/

[92] NACDL, Computer Fraud and Abuse Act （CFAA）, https://www.nacdl.org/Landing/ComputerFraudandAbuseAct （last visited Jun. 30, 2021）.

連結、載明發送人之地址、電郵內容涉及情色成分者則應於標題明確予以提示等[93]。

微軟以 CAN-SPAM Act 主張殭屍網路利用電子郵件進行詐欺，依該法，行為人應負民事賠償及相關責任。

(3)電子通信隱私法（Electronic Communications Privacy Act，下稱 ECPA）

ECPA 是美國國會於 1986 年制定，以延伸原先在電話有線監聽的相關管制（包含透過電腦的電子數據傳遞）。ECPA 修正原先 1968 年的「綜合犯罪防制及街坊安全法第三篇」（Title III of the Omnibus Crime Control and Safe Streets Act）（即有線監聽法），其主要是來防止政府未被允許而去接取監聽私人的電子通訊。ECPA 的 2709 條允許美國聯邦調查局（FBI） 發布國家安全令函給網路服務提供業者（ISP），以命令他們揭露客戶記錄。

微軟另外也以 ECPA 主張殭屍網路攔截並干擾微軟及其客戶的電子郵件傳送。該法案課以刑事責任，同時有民事賠償規定。

(4)入侵他人動產（Trespass to chattels）

此請求權也可以用在以電子方式入侵、未經他人授權適用他人裝置的情形。微軟主張 Waledac 未經授權進入他人電腦、利用他人電腦未經授權傳發電子郵件，並且在世界各地造成損害。

(5)聯邦商標法（The Lanham Act）有關商標淡化與混淆（dilution and false designation of origin provisions）之規定

此請求權基礎在專門在「詐騙信件用錯誤的電子郵件標頭」等案件，並對發送詐騙信件者請求民事追訴之用。微軟主張 Waledac 殭屍網路利用 Microsoft, Window, Hotmail 等標頭造成客戶之混淆與誤導，讓客戶不知道該些信件發送者為何，同時 Waledac 還利用微軟的防毒軟體來發送假的防毒軟體。此舉造成了微軟商標淡化（blurring and dilution by tarnishment）。

[93] 15 USC Ch. 103: CONTROLLING THE ASSAULT OF NON-SOLICITED PORNOGRAPHY AND MARKETING

(6)不當得利（Unjust Enrichment）：

此為習慣法的原則，因為殭屍軟體未經授權利用了微軟及其客戶的電腦、未經授權利用微軟的軟體，而有不當獲利，微軟以此請求殭屍網路應賠償其獲利[94]。

2. 微軟於本案訴訟策略及程序上之主張：

(1)策略目的

微軟在其「Legal Action Plan」指出，用 ICANN 之 UDRP 政策來取消網域名稱太慢，蓋殭屍網路的 C&C 伺服器早已變換網域名稱，故採取民事對物扣押方式處理本案。

(2)一造辯論程序

Conficker 案件係 ICANN 用凍結網域名稱之方式打擊使得殭屍網路之 C&C 伺服器無法運作。微軟用不同的方式。微軟要求地方法院申請核發單方程序（Ex Parte proceeding），程序啟動後有三天時間不會通知被告，以免 C&C 伺服器移動其網域名稱並且讓被告銷毀實體證據。

此做法有前案可參考，2009 年聯邦貿易委員會（FTC）以此方式使得一個有犯罪活動的 ISP 無法運作。該案啟動單方程序也是為了避免被告將犯罪證據銷毀並且逃逸。聯邦民事訴訟程序允許單方程序聽證（Ex Parte proceeding hearings）但是法院會要求原告提出相當證據。

微軟主張，其提出單方程序也係為了避免殭屍網路的網域名稱再度變換，至少需等到該網路的 C&C 伺服器不能運作時再通知被告。微軟依據的案例係 1979 年之 In re Louis Vuitton Et Fils S.A.，該案法院同意原告請求，否則會給被告時間銷毀實體證據。微軟提出向法院提出詳盡的計畫以說服法院。

(3)緊急/臨時禁制令

94 Janine S. Hiller, *Civil Cyberconflict: Microsoft, Cybercrime, and Botnets*, 31 SANTA CLARA HIGH TECH. L.J. 163, 10 (2014).

微軟同時聲請(法院也同意其聲請)緊急臨時禁制令(Emergency Temporary Restraining Order，下稱 TRO）請求法院禁止無名被告不得再控制殭屍網路。同時以預防禁制令(Preliminary Injunction)通知受理註冊機構 VeriSign 公司在確定網域名稱所有人之期間封鎖相關網域名稱。此手段可以讓 C&C 伺服器無法轉移到其他網域名稱，並且讓伺服器不能傳達命令給受感染電腦。

法院同意微軟的臨時禁制令申請，並在後來核發禁制令，蓋法院認為微軟在侵害 CFAA、入侵他人動產、不當得利等請求權基礎有理由。法院給微軟 14 天關閉殭屍網路，微軟並在 48 小時內關閉了殭屍網路，而位在中國的被告收到了法院的訴訟通知，不過其中一些被告經證明是無辜的，針對此類情況，微軟買下這些網域名稱並協助無辜的被告清理其電腦。

(4)一造缺席判決

微軟啟動單方程序、並且請法院核發禁制令，如此便能得到一造缺席判決（Default Judgement），並以此判決將殭屍網路所持有的網域名稱移轉給微軟。微軟也表示，最有效打擊殭屍網路的方式便是將其持有網域名稱剝奪，並且將該網域名稱移轉給可信賴之人，確保未來這些網域名稱不會又落入殭屍網路手中。微軟基於以下幾點事展開此行動的不二人選：微軟有足夠資金、有專業技術去控制這些網域名稱[95]。

（三） 其他微軟對抗殭屍病毒案例

1. Rustock 殭屍網路：

同 Waledac 作法，透過第三方阻擋網域名稱。微軟主張以 All Writs Act 要求法院命令訴外人阻擋網域名稱。另外微軟也聲請扣押伺服器所在位置的電腦、檔案及資訊，法院命法警陪同微軟扣押實體證據。而且因為殭屍網路濫用微軟商標，Lanham Act 本身也讓微軟有請求權基礎可以聲請扣押相關證據。此案中，微軟雙管齊下，同時要求法院命令第

[95] *Id.* at 12.

三阻擋網域名稱（數位），並且扣押證據（實體），同時以數位和實體之方式確保殭屍網路不能運作。

2. Kelihos 殭屍網路

和 Waledac 殭屍網路案相似，但微軟更主張了網域名稱所有人過失之指控。微軟主張網域名稱所有人有過失未注意到其所有的網域名稱被用在惡意用途。此案件有兩個意義：一，縱使被告在美國法院管轄權外，只要該網域名稱之受理註冊機構及註冊管理機構在境內，法院有管轄權。二，網域名稱所有人縱使沒有參與犯罪，仍有注意網域名稱不能被用作犯罪用途的注意義務。

3. Zeus 殭屍網路

微軟主張被告違反反勒索及受賄組織法（Racketeer Influenced and Corrupt Organizations Act，下稱 RICO），因該殭屍網路集團竊取金融帳戶資訊，且動員成員提領並存放竊取之款項。法院核發 TRO 及扣押命令扣押實體證物，並且命令將網域名稱移轉給微軟。

4. Nitol 殭屍網路

微軟主張侵害 CFAA、入侵他人動產、不當得利等，嗣法院核發禁制令及新建網域名稱系統沉洞伺服器（Domain Name System Sinkhole，下稱「沉洞」）使該病毒網域名稱無法續為傳遞違法訊息，除件至沉洞外，整體手段和前開案件類似。

5. Bamital 殭屍網路

手段和前開案件亦差不多。該案中要協助阻擋網域名稱的各種第三方（網域名稱之受理註冊機構及註冊管理機構），不只有美國境內者，還以印度、捷克、南韓、蘭等地區的第三方。（不過法院向該地區之請求沒有強制力）[96]。

6. 聯合 FBI、金融機構和金融資安資訊分享與分析中心（Financial Services Information Sharing and Analysis Center）進行訴訟

[96] *Id.* at 14.

(1) Citadel 殭屍網路：微軟同樣得到法院核發的單方 TRO，並且經由法院命令第三方協助移轉網域名稱，由微軟接管該網域名稱。同時扣押相關實體證據。

(2) ZeroAccess 殭屍網路：該殭屍網路是 P2P 型態網路，因此並無實質上的 C&C 伺服器，又該網路中許多 IP 位址位於國外，因此法院無法命令美國境內的網域名稱註冊管理機構將一些網域名稱移轉給微軟。因此，法院改變方法，命令境內 ISP 業者阻當惡意網域名稱[97]。

第二項　網域名稱內容濫用案例－Operation in Our Sites（下稱「OPS」）行動

（一）案例背景

美國國土安全部（下稱「DHS-ICE」）依據智慧財產資源及機構優先法案（ Pro-IP Act）及民事扣押手段於 2010 年 6 月開始執行大規模之網域名稱暨智慧財產權打擊犯罪行動，此行動稱為 Operation in Our Sites。自 2010 年開始，OPS 行動時常於特殊節日前加強執行，如 2010 年之網購週一節、2011 年之西洋情人節及超級盃等節日，而由於此等類型之非法網站屬國際詐騙集團操控，此等案件之網域名稱之註冊人大多數均無聲請異議或提出抗辯。

（二）解決手段

DHS-ICE 依 Pro-IP Act 之目的持續執行 OPS 及網域名稱扣押。依據 DHS-ICE 統計，於 2017 至 2018 年間，透過美國本土及國際合作，該年有超過 100 萬個網域名稱因涉及違反上述智慧財產權而被扣押[98]。今（2021）年 4 月，馬利蘭州聯邦檢察署（US District Attorney for the District of Maryland）與 DHS-ICE 已經扣押 8 個意圖利用新型冠狀病毒肺炎疫情圖利之網域名稱。其中包括「healthbridgescience.com」及「genobioscience.com」侵害某生技公司之商標權及著作權，「global-

[97] *Id. at* 17.
[98] DHS-ICE，Over a million websites seized in global operation, ICE (Nov. 26, 2018), https://www.ice.gov/news/releases/over-million-websites-seized-global-operation .

pandemic-vaccines.com」販售仿冒疫苗等。依據 DHS-ICE 今年 4 月之新聞稿，DHS-ICE 截至 4 月時已分析超過 78,000 個與新型冠狀病毒肺炎相關之網域名稱[99]。

（三） 案例分析

美國法律因其特殊對物管轄及扣押之英美法法理，允許執法單位基於對物管轄之對物扣押之手段（in rem civil action），即在不知相對人下，仍可為扣押，就涉及特定犯罪或違法行為之網域名稱予以扣押並命令註冊管理機構將原網域名稱網址導向指定網址。此作法雖引起部分學者對於正當法律程序、言論自由管制及財產權保護發出疑慮[100]，惟實務上仍無法院採反對見解[101]。

我國或可參考美國特定法律或措施，惟須注意法理基礎即有根本之不同。美國法下之對物扣押係因其民事訴訟法例早已確定單純對物管轄之法理，反觀我國則無相同原則可類推適用。此外，若欲參考美國法例之對物扣押措施，除宜注意法例上是否有法源或法理依據外，仍應於推動修法（如民事訴訟法）建構類似美國對物管轄法例時，思考相關配套措施。

第三項　網域名稱技術濫用案例－日本以「沉洞」對抗 Vawtrak 殭屍病毒

（一） 案例背景

2015 年（平成 27 年）4 月發生一種被稱為 Vawtrak 的網路病毒在世界各國傳播，控制並感染日本國內約 4 萬 4,000 台電腦及國外約 3 萬 8,000 台電腦。受病毒感染的電腦會非法轉帳受害人網路銀行中的存款。日本石川縣一名女子 2014 年 8 月舉報她遭駭客盜取驗證碼，從戶口盜走 96 萬日圓。警方發現受害者的電腦感染 Vawtrak 病毒，當登入網路銀行後，

[99] DHS-ICE, HSI investigation results in seizure of 3 domain names purporting to be biotechnology company websites with COVID-19 treatments, ICE (Apr 7, 2021), https://www.ice.gov/news/releases/hsi-investigation-results-seizure-3-domain-names-purporting-be-biotechnology-company.

[100] Karen Kopel, *Operation Seizing Our Sites: How the Federal Government Is Taking Domain Names Without Prior Notice*, 28 BERKELEY TECHNOLOGY LAW JOURNAL 860, 861 (2013).

[101] Nicole Kardell, Feds Open The Gates and Seize the Domain Names, Infrah Law (Apr. 28, 2016), https://www.ifrahlaw.com/crime-in-the-suites/feds-open-the-gates-and-seize-the-domain-names/.

畫面出現要求輸入驗證碼的假網站，只要受害人輸入相關資料即在受害人毫不知情的情況下轉帳給第三人[102]。

（二） 解決手段

針對此事，日本警視廳透過分析受感染的電腦，及取得 C&C 伺服器[103]所分配到現已失效的網域名稱，並自行設置「沉洞[104]」伺服器以觀察受感染電腦與 C&C 伺服器間之通信情況，並協助被感染電腦解毒。

為終止殭屍網路，建置「沉洞」伺服器技術，可用於解析 C&C 伺服器及 C&C 伺服器與感染電腦間通信，對於了解事件全貌具有重要意義。如 C&C 伺服器在日本境內，屬日本檢警搜查及管轄範圍內，即可依刑事訴訟法向法院聲請令狀將該伺服器加以扣押並解析。此時可能無須使用「沉洞」方式，即可觀察 C&C 伺服器與感染電腦間之通信情況[105]。

然而另一方面，如 C&C 伺服器在海外，即非屬日本檢警搜查及管轄範圍內，因此原則上僅能透過尋求伺服器所在國之司法互助共同進行搜查。如 C&C 伺服器所使用之網域名稱有「.JP」之網域名稱，為觀察伺服器與感染電腦中之通信，即有尋求「.JP」網域名稱註冊管理機構（Japan Registry Services, JPRS）之協助，以使用「沉洞」技術之需求[106]。根據 2017 年（平成 29 年）網路安全政策會議（サイバーセキュリティ政策会議）報告書提及目前 C&C 伺服器使用「.JP」網域名稱情形算是少見，故現階段尚未有尋求 JPRS 制定出對應措施之必要[107]。

（三） 案例分析

---

[102] 資安趨勢部落格，日逾 8 萬台電腦感染網銀病毒,破解雙重認證,非法轉帳，https://blog.trendmicro.com.tw/?p=12034（最後瀏覽日：2021 年 5 月 19 日）。

[103] C&C 伺服器（又稱 CNC 伺服器）也就是 Command & Control Server，一般是指揮控制僵屍網路 botnet 的主控伺服器，用來和僵屍網路的每個感染了惡意軟體（malware）的宿主機進行通訊並指揮它們的攻擊行為。

[104] DNS 沉洞（DNS sinkhole），又名沉洞伺服器為一種 DNS 伺服器，它對於特定網域名稱給出不同的導向，使網路使用者無法連結到惡意網站。同時藉此方式可以知道內部受保護的網路中有哪些主機受感染，並使得一些大型的殭屍網路無法發揮其效用。

[105] サイバーセキュリティ政策会議，平成 29 年度サイバーセキュリティ政策会議 報告書，頁 8-9。

[106] 同註 105，頁 9。

[107] 同註 105，頁 9。

1. 針對使用「沉洞」技術尚未有明確的法律授權及根據，而為今後須與警察廳、總務省、法務省及 JPRS 共同合作及研議之課題。於報告書中特別提及在美國 FBI 及 Microsoft 針對殭屍網路係作為民事訴訟上之當事人，採行民事訴訟程序解決此類問題；於德國則採用刑事訴訟程序解決此類問題。兩種方式於日本法體系上仍有所扞格，因此無法直接參考兩國之處理程序導入日本法體系內，且對於殭屍網路及網路病毒往往並非單獨一家民間企業能加以面對，於日本係以檢警主導使用「沉洞」技術加以觀察及解決殭屍網路問題。如需尋求「.JP」註冊管理機構 JPRS 協助，其請求之法律基礎為何、採行刑事或民事訴訟程序、JPRS 未有規範框架下任意提供協助之妥當性等皆須逐一考量，並設計出適當之程序[108]。此外，使用「沉洞」技術時並未取得通信雙方當事人之同意即加以進行，因此涉及侵害通信秘密及阻斷通信等問題。故於請求 JPRS、ISP 業者協助時，此點即須加以留意。

2. 從避免殭屍網路感染範圍擴大觀點，亦可由 ISP 業者為主體進行相關措施。如當 ISP 業者發現受感染電腦時，可以利用 walled garden 技術切斷該受感染電腦之網路，以防止感染擴大。ISP 業者對於 DoS 攻擊等伺服器攻擊行為加以應對之措施，即可能涉及違反電氣事業法第 4 條通信秘密保護之規定。故在總務省召開網路利用環境確保檢討會（円滑なインターネット利用環境の確保に関する検討会）討論此等問題，此外網路電信業者亦共同制定出電氣通信事業受網路攻擊之應對及通信秘密相關指引（電気通信事業者におけるサイバー攻撃等への対処と通信の秘密に関するガイドライン）。於指引中羅列各種可能的網路攻擊事例、及 ISP 業者可採行構成正當防衛及緊急避難之措施如阻斷通信等。

[108] 平成 29 年網路政策會議第三回會議紀錄即提及，要求 JPRS 自行判斷涉及殭屍網路之網域名稱有難度，故仍有賴檢警協助處理。此外為使 JPRS 將網域名稱取消、停止解析亦應有相關免除責任之規範。JPRS 可依汎用 JP ドメイン名登録等に関する規則第 29 條如有確定判決可將網域名稱取消，或是依第 22 條無法聯繫到網域名稱註冊人，將網域名稱停止解析。平成 29 年度サイバーセキュリティ政策会議（第３回）発言要旨，頁 6-7。

3. 針對日本網域名稱技術濫用如殭屍網路、網路病毒等並無相對應完善的法規要求 JPRS 及 ISP 業者有配合的義務。惟實務運作上，如殭屍網路之 C&C 伺服器在日本境內屬日本司法管轄範圍內即可透過刑事訴訟法之扣押相關規定加以扣押 C&C 伺服器解決殭屍網路問題。然而如 C&C 伺服器在日本外，除須尋求跨國司法互助外，警方如需要尋求 JPRS、ISP 業者協助，則無明確的相關法制度及框架可供遵循。故運作上可能係透過警方發函給 JPRS、受理註冊機構告知相關網域名稱有散播殭屍網路及病毒問題，再透過受理註冊機構與註冊人間之契約條款終止契約，以達到將該網域名稱取消之目的。又同時警方亦可能發函給 ISP 業者告知相關網域名稱有散播殭屍網路及病毒問題，ISP 業者在遵循電氣通信事業受網路攻擊之對應及通信秘密相關指引下，可將有問題之網域名稱停止解析。

第四章 立法例研析規劃

第一節 網域名稱註冊管理機構及受理註冊機構之間的協議規範

一、 註冊管理機構協議及網域名稱受理註冊機構認可協議

註冊管理機構協議（Registry Agreement，下稱「RA」）是為了規範頂級網域名稱的授權註冊管理機構與 ICANN 組織間之權利義務之正式法律文件，文件中規定任何單位成為註冊管理機構前，必須瞭解、遵循之權利義務及其他協議條款，本研究團隊進一步研析 RA 及其他協議條款可能涉及網域名稱內容監理之條款如下：

（一） ICANN 與 TWNIC 間之 RA[109]

ICANN 與 TWNIC 間之註冊管理機構協議第三條以下規定了 ICANN 及 TWNIC 之權利義務，本研究團隊謹翻譯並節錄如下：

1. 第 3 條 ICANN 之義務

(1) 第 3.2 條 資料數據庫之維護

ICANN 應維護或促使維護一個穩定、安全且經授權的根資料數據庫（本協議中稱為“根數據庫”），其中包含有關根伺服器系統中 TLD 之相關訊息。對於受委託之 ccTLD（即我國之頂級網域名稱「.tw」），根數據庫應至少包含有關發起人實體、管理聯繫人、技術聯繫人和網域名稱伺服器的訊息。

(2) 第 3.3 條 指定行政和技術聯繫人

ICANN 應按附件 A 之約定提供「.tw」行政/技術聯繫等支援服務，在本協議生效期限內，TWNIC 可不定期以書面形式通知 ICANN，要求更改「.tw」之行政或技術聯繫人。

(3) 第 3.4 條 更新網域名稱伺服器信息

[109] ccTLD Sponsorship Agreement (.tw ccTLD)，ttps://www.icann.org/resources/unthemed-pages/sponsorship-agmt-2003-03-26-en.

在本協議有效期開始時，「.tw」的網域名稱服務器的主機名和 IP 地址應如附件 A 之約定，TWNIC 可通知 ICANN 要求更改根數據庫中受授權之「.tw」網域名稱伺服器之主機名或 IP 地址。

(4) 第 3.5 條 實施聯繫信息更新

ICANN 根據 TWNIC 提交之請求，在合理確信該請求是真實且符合第 4.4 節要求後 7 天內，ICANN 應修改根數據庫中之聯繫訊息。

(5) 第 3.6 條 發布根區域 WHOIS 協定之訊息

ICANN 應發布或授權發佈在根數據庫中授權的「.tw」數據。發布之數據應至少包括 TWNIC 行政聯繫人和技術聯繫人之名稱、數據元素的指引；發布之方式以及發布更新頻率應按照附件 C 的約定進行。

(6) 第 3.7 條 運行根網域名稱伺服器系統及根區域文件之內容

ICANN 應盡合理的商業努力來協調根網域名稱伺服器系統，以確保其以穩定和安全的方式運行並進行維護。ICANN 在本協議所賦予之權利範圍內履行本網域名稱記錄義務。

2. 第 4 條 TWNIC 之義務

(1) 第 4.1 條 為「.tw」提供網域名稱服務（Name service）

TWNIC 應盡合理及最佳商業努力，以穩定，安全的方式來操作和維護「.tw」之主要和次要網域名稱伺服器，足以解決「.tw」任何子網域名稱 Internet 用戶之管理權限。

(2) 第 4.2 條 確保 ICANN 得訪問「.tw」之區域文件和註冊數據

TWNIC 應確保 ICANN 可以不定時，合理地指定之方式訪問「.tw」，並向 ICANN 持續提供「.tw」之區域文件，以及準確和最新之註冊數據，以驗證和確保「.tw」運行之穩定性。

(3) 第 4.3 條「.tw」註冊表數據託管

TWNIC 應確保註冊數據庫之安全性和完整性，包括建立由 TWNIC 管理之註冊數據庫，並由 TWNIC 託管相關數據，而費用由 TWNIC 承擔。託管數據庫之代理人或鏡像站操作員應取得 TWNIC 和政府機構的核准，並且不受 TWNIC 之控制。

（二） 本研究團隊分析：

經本研究團隊研析，上述規定可視為透過根數據庫之託管及數據分享模式，針對「.tw」網域名稱之使用及授權訂有約束及強制力規範，除上述規定外，並未針對域名使用者行為，或網站言論內容訂有相關約定，亦無規定 ICANN 及 TWNIC 有管制網域名稱濫用之義務。

二、 網域名稱受理註冊機構認可協議（Registrar Accreditation Agreement）

（一） 認可協議有關網域名稱濫用之規定（第 3.18 條 網域名稱受理註冊機構之網域名稱濫用聯繫與調查濫用報告）

1. 第 3.18.1 條 網域名稱**受理註冊機構（下稱「受理註冊機構」）應提供並維持濫用聯繫之方式，以接收涉及註冊名稱的濫用檢舉及通報，包括非法活動報告**。受理註冊機構應在其網站主頁上（或在 ICANN 指定處）發布電子郵件地址以接收此類報告。網域名稱受理註冊機構應採取合理，迅速的步驟，對任何濫用舉報進行調查並做出適當回應。

2. 第 3.18.2 條 **受理註冊機構應建立並維持專門的濫用聯繫方式**，包括專門電子郵件地址和電話號碼，每週 7 天，每天 24 小時進行監控，以接收執法機構、消費者保護、準政府或非政府組織等單位之非法活動報告，涉及之國家或地區之轄區，由受理註冊機構設立及維持辦事處。**有充分根據之非法活動報告必須由受理註冊機構授權之個人在 24 小時內進行審查，該個人有權採取必要和適當的行動。在回應任何此類報告時，不需要受理註冊機構採取任何違反所應適用法律之行動。**

3. 第 3.18.3 條 受理註冊機構應在其網站上發布接收、處理和追蹤濫用報告之程序進度說明。受理註冊機構應記錄對此類報告之接收和答覆紀錄，相關報告記錄保留期限至少為兩（2）年或依照所適用法律允許之最長期限。於保存期間內，受理註冊機構在受合理通知下應向 ICANN 提供此類記錄。

（二） 本研究團隊分析：

經本研究團隊研析，上述規定授權受理註冊機構，若收到有關已註冊網域名稱的投訴，包括但不限於網域名稱濫用、言論內容涉及違法不當等，則受理註冊機構應建立專門舉報機制受理相關報告；受理註冊機構之反濫用部門應負責處理所收到的投訴與舉報。

受理註冊機構之反濫用部門收到投訴或不當使用的舉報之後，應針對投訴內容進行評估。若該舉報經判斷證明為合理者，按照現行實務做法，受理註冊機構將會連絡該網域名稱擁有者（已註冊網域名稱持有人）並請網域名稱持有人執行必要動作以解決問題。若是在嚴重違反使用者條款的情形之下，受理註冊機構有權利可立即停止網路服務[110]。

[110] Webnode 網域名稱規範，https://www.webnode.tw/domain-names-policies/ （最後瀏覽日：2021 年 4 月 25 日）。

若受理註冊機構判定該投訴為不合理，該投訴遭到駁回，或無法對該投訴進行正確評估，則得不採取任何進一步動作，並針對投訴者進行答覆說明，若有必要，則該受理註冊機構得將檢舉函轉介與該管之主管機關。

第二節 各國立法例之研析

第一項 日本

（一） 規範網際網路內容

日本對於網路內容及使用行為之違法及不當與否之認定上並無統一的法規範存在，而係由民間及網路服務業者自發性地於 2013 年成立一般社團法人安全網路協會[111]（SIA）及由電信事業業者共同組成一般社團法人電信服務協會（Telecom Services Association，簡稱 Telesal）[112]下的違法情報等對應連絡會[113]，共同處理網路內容違法不當問題。SIA 與 Telesal 的違法情報等對應連絡會皆訂有相關違法不當態樣的指引規範，兩者指引內容大致相同，但 SIA 之指引於 2019 年 4 月修訂完成，其內容較新且較完整，因此在此主要介紹 SIA 之指引[114]。

SIA 參考相關法規之違法要件及態樣**訂立安全線運用指引**[115]，針對網路內容區分為**內容違法**及**內容不當**。前者係指該內容存在於網路上使公眾得閱覽有違反相關法規；後者係指雖大眾得閱覽之內容雖不違法，但其可能引起違法行為，或是其有為公眾所皆知極重大問題。就「**內容違法**」，**其可分為五大類型**，臚列如下表：

---

111 協會之設立目的等具體介紹將於後詳述。

112 官方網站：https://www.telesa.or.jp/（最後瀏覽日：2021 年 11 月 23 日）。

113 本連絡會成立目的係為使網路通信業者得適當地處理網路上違法不當資訊，而共同組成本連絡會。並有發布相關處理指引，https://www.telesa.or.jp/consortium/illegal_info （最後瀏覽日：2021 年 11 月 23 日）。

114 Telesal 違法情報等對應連絡會訂立之指引主要供網站管理人參考，與 SIA 訂立之指引相似，皆參考各法律規範之違法態樣，訂立出網域名稱內容濫用之態樣。惟 Telesal 違法情報等對應連絡會訂立之指引最後更新日期為 2014 年 12 月，相較於 2019 年 SIA 訂立之指引較舊外，並無規範網域名稱內容不當之態樣。

115 セーフライン運用ガイドライン。

表 5 違法內容列表

類型	違反之具體內容
性表現及性行為	公然陳列猥褻之電磁紀錄[116]
	公然陳列兒童色情相關之電磁紀錄[117]
	引誘性交易[118]
	約會網站違反禁止引誘規範[119]
藥物	藥物犯罪之實行及管制藥品及毒品[120]
	管制藥物（毒品等）之廣告[121]
	指定藥物之廣告[122]
	指定藥物同等或以上之具精神毒性蓋然性高之藥品廣告[123]
	未經許可藥品之廣告[124]
轉帳詐欺	勸誘、引誘轉讓存摺[125]
	勸誘、引誘轉讓手機門號[126]
侵入他人帳號	無故、不當要求輸入帳號密碼[127]
	助長不當侵入他人帳號行為[128]
成為社會問題之違法	以兒童為對象之照片、影音[129]
	情人、配偶間散佈他方情色影音供不特定人閱覽[130]

116 刑法第１７５条第１項。
117 児童ポルノ法第７条第６項。
118 売春防止法第５条第３号及び第６条第２項第３号
119 出会い系サイト規制法第６条。
120 麻薬特例法第９条
121 覚せい剤取締法第２０条の２、麻薬及び向精神薬取締法第２９条の２及び第５０条の１８、大麻取締法第４条第１項第４号。
122 医薬品医療機器等法第７６条の５。
123 医薬品医療機器等法第７６条の６の２第１項。
124 医薬品医療機器等法第６８条。
125 犯罪収益移転防止法第２７条第４項。
126 携帯電話不正利用防止法第２３条
127 不正アクセス禁止法第７条第１号
128 不正アクセス禁止法第５条。
129 刑法 第２３０ 条 、民法第７１０条及び第７２３条。
130 私事性的画像記録の提供等による被害の防止に関する法律第２条及び第３条。

就「**內容不當**」可分為七大類，臚列如下：

表 6 內容不當列表

	類型
一	網路內容直接且明顯與違法行為（槍枝轉讓、爆裂物製造、兒童情色影音提供、偽造公文書、殺人、脅迫等）之要約、引誘、媒介。
二	無法直接判定內容違法（即構成前述表格內之違法內容），但仍相當程度地懷疑其違法
三	尚未管制到或是規避法律之藥品、毒品、合法薄荷等物之仲介、要約、引誘等。 同時符合以下兩要件： 1. 刊載內容「合法薄荷」、「合法粉末」、「合法具香氣菸草」等很高機率暗示為危險藥品、毒品 2. 刊載「賣」、「量販」、「外送」等販賣、轉讓、仲介等意涵之內容。 且符合下列擇一要件： 刊載「拒絕公然買賣」、「人體禁止吸入」等特別強調禁止吸食、公然買賣意涵之內容。 同時販賣菸管、捲紙等，且明顯為引誘吸食。 刊載「鳥取縣無法送達」、「鳥取、石川、和歌山以外全國皆可送達」等。因該等縣市法規禁止危險藥品、毒品製造、買賣、持有、使用，因此拒絕運送至該等地方，即表示為危險藥品、毒品。
四	引誘自殺 1. 刊載對不特定多數人、「想死」、「想自殺」之人，提供執行自殺之「幫助」或「委託」意涵之內容 2. 刊載「一起自殺嗎」、「募集真的想死的人」不僅自己對他人生命亦造成危險之自殺引誘、勸誘等意涵之內容 3. 輔以判斷網站整體即周邊資訊，以判斷是否有真正助長自殺之風險
五	勸誘、引誘以兒童為對象之霸凌 1. 原則由兒童本人或是法定代理人之通報

	2. 刊載內容於不特定多數人可閱覽之部落格、網站 3. 刊載「霸凌吧」、「毆打吧」、「大家無視他」等對特定兒童霸凌之勸誘、引誘意涵之內容
六	刊載被害者遺體、自殺行為影像等明顯傷害遺族感情 1. 原則由遺族通報 2. 可確信該影像為過世之本人 3. 「自殺」、「他殺」、「事故死」、「病死」等影像內容 4. 排除公共性、公益性明顯較優先之情形 5. 不包含動物屍體、殺害動物之影像
七	閱覽人觀看影像後明顯厭惡之遺體、殺害行為之影像 1. 「自殺」、「他殺」、「事故死」、「病死」等影像內容 2. 「頭部分離」、「內臟外漏」、「滿身是血」、「臉部無法判斷人別之慘狀」、「遺體腐爛」等慘不忍睹之遺體及殺害影像 3. 必須不具有公共性及公益性。即例如述說戰爭、恐怖攻擊、事故、生病等文章所連同刊登之圖片影像，及紀錄片、電影、圖片等研究為目的之影像不包含在內 4. 不包含已在閱覽人閱覽前附註注意聲明等防止閱覽人不經意地閱覽內容

綜上所述，日本對於網路內容及使用行為之違法及不當與否之認定，並無統一的法規範存在，而係藉由民間 SIA 等機構作為通報窗口，就違法、不當網路內容透過 SIA 的安全線運用指引，將網路內容可能之違法及不當態樣於指引中羅列出來，以作為接到民眾、網路使用者通報時就內容妥當性與否之判斷標準。

對於詐騙、釣魚、盜用個資及植入木馬等網路使用者行為問題。如網路上釣魚等詐欺行為即可能構成日本刑法第 246 條詐欺罪；侵入網路提供業者之伺服器將保存內容刪除或改寫，即可能違反日本刑法第 234 條之 2 電子計算機損壞等業務妨害罪；而以不當方式手段取得他人帳號及密碼，且侵入伺服器時即可能構成侵入行為禁止

相關法律[131]第 3 條侵入行為禁止之違法。

（二） 政府無權限要求註冊管理機構移除或是停止解析網域名稱

依電氣通信事業法第 39 條之 3 第 1 項明文規定提供網域名稱名之電信通信業者（即註冊管理機構，日本為 JPRS）無正當理由不能拒絕提供網域名稱註冊服務，亦即註冊管理機構有無差別性地提供服務之義務。當註冊管理機構違反前述義務時，依同條第 2 項總務大臣可以在為使用者利益或確保公共利益之必要範圍內，得對註冊管理機構要求進行業務改善及履行相關措施[132]。此外，同法第 3 項註冊管理機構有提出收支狀況及會計財務報表之義務。因此可以看出主管機關總務省對註冊管理機構監管目的在於確保註冊管理機構可以無差別性地提出服務，及確保其能持續營運，屬於低度之管理。

隨著網路普及，於 2014 年時總務省曾組成網域名稱政策委員會，探討如何維持註冊管理機構之信賴性、透明性時，有特別提及要以何種方式管理註冊管理機構以確保註冊管理機構之可信賴性，如由民間及利害關係者主導、國家與註冊管理機構簽訂契約，及以法律之形式管理註冊管理機構。上述三種方式各有其優缺點，為方便表達以表格方式呈現[133]：

表 7 註冊管理機構管理模式

	利害關係人及民間主導	註冊管理機構與國家簽訂契約	法律規範
優點	不會影響社會發展及	不會影響社會發展及	1. 大眾可以清楚知

[131] 不正アクセス行為の禁止等に関する法律。

[132]總務省近期曾於 2019 年曾因舊山梨醫科大學曾使用過的網域名稱名「yamanashi-med.ac.jp」被不符合註冊資格的成人網站所使用，因而發出行政指導，要求 JPRS（.JP 之註冊管理機構）報告本件事情發生之原因及避免再次發生之對策 株式会社日本レジストリサービスに対する「.jp」ドメイン名の管理・運用に係る措置（要請），https://www.soumu.go.jp/menu_news/s-news/01kiban04_02000152.html（最後瀏覽日：2021 年 6 月 30 日）。

[133] 「ドメイン名に関する情報通信政策の在り方」（平成 25 年 10 月 1 日付け諮問第 20 号）に関する情報通信審議会からの答申の公表，答申概要，頁 5。

	民間活力	民間活力	悉規範內容 2. 行政處分流程、依據清楚明確
缺點	管理規範不透明	1. 部分內容無法透過契約方式規範 2. 對國民於透明性上仍有不足	可能過度規範致減損民間活力及社會發展

對於上述三種方式，最終選擇由民間主導即由註冊管理機構自行作成標準及規範，於作成規範時應公開與利害關係者討論標準及規範之設置，並應尊重討論結果以訂立規範。

綜上所述，**總務省對於 JPRS 屬於低度管理，並無得直接要求註冊管理機構移除或是停止解析違法不當網域名稱之相關法律規範**。總務省雖沒有直接說明未訂立相關法律之理由，但由上述低度管理由民間主導並強調不影響民間活力，可知悉如總務省有權直接要求註冊管理機構移除內容或是停止解析將影響網路上之言論自由。此外，由社團法人安全網路協會（SIA），於其安全線運用指引之第一章第一節設立目的即強調網路並非由各國政府所管理，而係由一般市民、企業自治及自助之方式加以維繫其秩序。資訊自由地流通及表現自由作為社會基盤，由民間自主營運及發展具重要性。因此，**在日本對於網域名稱內容違法及不當，主管機關總務省並無法直接介入要求 JPRS 取消或是停止解析網域名稱**。

（三） 認定內容或行為違法之機構

主要接受民眾及網路使用者通報網域名稱內容違法及不當者為 SIA，而非註冊管理機構 JPRS。SIA 於 2013 年 11 月由網路業者共同成立。業者們有感於隨著智慧手機使用之普及網路服務更加便利，然而同時對於潛在可能的危害風險亦隨之升高。兒童情色、毒品及管制藥品販賣、犯罪等違法、不當之資訊內容在網路上流傳，因此有必

要對此問題提出對策。

SIA 對於上述問題講求依據實際情況、考量時效性及減輕被害，欲維護安全的網路環境。其與警方合作建立方便網路使用者通報網路內容違法及不當之熱線。熱線共有兩條，一條於 2013 年 11 月由民間自行運作的「安全線」及另外一條 2016 年 4 月起受警察廳（原文：警察庁[134]）所委託之「網路熱線中心（Internet Hotline Center，下稱 IHC）」。兩條熱線彼此相互分擔業務，警察廳所委託的 IHC 熱線主要處理國內網站內容違法；民間自主運作的安全線主要處理國外網站內容違法及國內外網站內容不當[135]。

為避免兩熱線恣意地處理、認定網站內容違法不當，造成損及網路言論自由，及使網路表現活動之萎靡，因此於 IHC 熱線設置營運委員會及運用指引檢討協議會，而安 SIA 則聘有外部委員（教授、律師等），這些委員會中有法律專家、律師、兒童福祉團體、關係者參與在內，對 SIA 活動狀況及實績等予以評價，並觀察指引運用情況、網路資訊流通狀況等就指引內容予以即時必要之修正[136]。

（四） 認定不法無須需經過法院審核及給予當事人陳述意見機會

對於前述機構 SIA 於收到網路使用者之通報後，會依安全線運用指引判斷內容有無違法及不當。針對違法及不當內容之認定 SIA 期許自己能符合下述三項標準[137]：

1. 可信賴性

對於 ISP 業者及網路內容代管業者等，信賴 SIA 認定「內容違反」之判斷，而願意接受其刪除網頁內容之請求，並期許 SIA 能不論業者與利用者間有無契約與否及契約內容為何，皆不會因為刪除內容、阻止資訊流傳而有法律上責任。因此 SIA 做成之

134 機關功能似我國警政署。
135 違法・有害情報対策活動報告（2019 年 1 月~12 月），頁 3。
136 同註 135，頁 3。
137 同註 115，第三章第一節及第四章第一節。

判斷必須有法院亦會有相同認定之確信。針對「不當內容」SIA 作出該內容不當之判斷後，**交給 ISP 業者及網路內容代管業者作參考，並自行決定刪除與否**。

2. 確保判斷適切

要求作出的判斷必須依造指引且有適當之程序。

3. 快速對應

確保適切判斷的同時，避免違法內容廣泛流傳，使警察、ISP 業者、網頁管理者等快速對應，因此有必要能快速作出判斷。

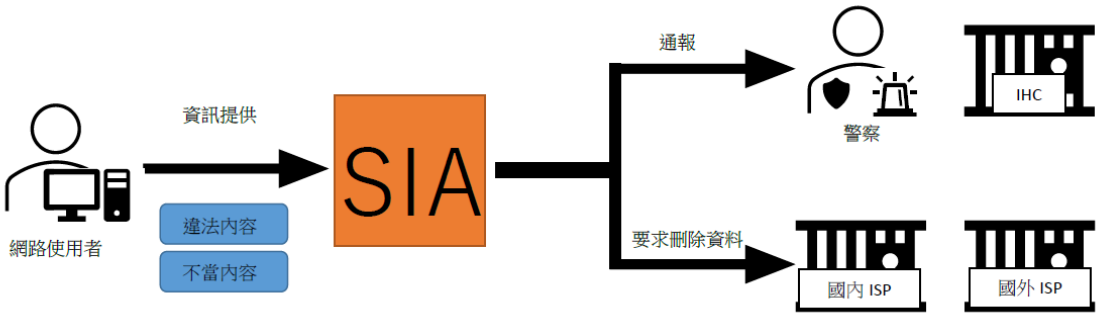


圖 7 SIA 通報流程圖

由上圖及指引所訂立之標準可知在認定違法及不當之過程中，基於快速應對之需求在認定網頁內容違法或不當之前，**並不會給予網頁權利人陳述意見之機會，且判斷過程中亦不會經過法院審酌**，以達到即時性及降低違法不當內容之影響性。

（五） 違法不當內容之判斷對於註冊管理機構無拘束力

SIA 收到網路使用者之申報後會將資訊主要交給警察機關、ISP 業者及網站管理人、關係機關、網路過濾業者等四個主要單位[138]，其具體內容以下申述之：

1. 警察機關

[138] 同註 115，第一章第一節（2）。

內容經 SIA 認定於網路上散布可能違反刑法、特定犯罪關聯之內容（如違禁品買賣相關資訊）、其他犯罪有關內容、自殺相關內容、犯罪搜查及預防、人命保護等相關資訊。

2. 伺服器管理人、網站管理人

經 SIA 認定違法及有害之網站內容，會通知 ISP 業者及網站管理人請求刪除或是避免內容繼續於網路上流傳

3. 關係機關

經 SIA 認定該違法及不當內容資訊交由專門機構及機關處理較為妥當。如毀損名譽及侵害隱私之內容中有重大侵害人權部分時，會將資訊交給法務省人權擁護機關；違法高利貸廣告則交給金融廳處理。

4. 網路過濾業者

網路過濾業者作為接受網路資訊人的守門人，對於違法不當之網頁內容，SIA 會建立資料庫，定期將資訊交給網路過濾業者。

SIA 刪除違法不當之網頁內容及相關防止內容流傳之請求，其相對人係先向部落格或是網頁管理者提出請求，當無法特定部落格及網頁管理者，或是其收到請求後不願意對應刪除網頁內容或執行防止內容流傳之必要措施時，會向伺服器管理人提出請求；無法特定伺服器管理人，或其不願意接受 SIA 之請求時，會向分配 IP 位置給伺服器業者之機構如 ISP 業者提出請求。

通報給註冊管理機構為 SIA 最後的選擇，絕大多數個案在刊載違法不當之網頁管理者或是伺服器管理者、ISP 業者即將網頁內容刪除，以 2019 年為例提出 21,183 件請求 19,540 件網頁內容被刪除（約 92%）[139]。基於 SIA 本質為民間發起的機構，所以提出之請求僅具有建議性質，不論對部落格及網頁管理者、伺服器管理人，及網路服務提供業者等皆無拘束力，且對於違法不當網頁內容之刪除，並不會直

[139] 同註 135，頁 13。

接要求到註冊管理機構協助處理。

（六） 註冊管理機構無權自行認定違法而移除內容拒絕解析

「.jp」為日本的 ccTLD，於 1986 年開始提供網域名稱註冊服務，初期是由日本網路資訊中心（Japan Network Information Center，下稱 JPNIC ）負責。該法人組織隨著「.jp」的網域名稱註冊數量日漸增多，於 2000 年 12 月 22 日經大會決議，決定另行成立日本註冊股份有限公司 JPRS。2002 年 1 月 JPRS 正式被日本政府認可為「.jp」之網域名稱註冊管理機構，並與 JPNIC 簽屬管理權移轉協議書。2002 年 2 月 JPRS 正式被 ICANN 認可為「.jp」之網域名稱註冊管理機構並簽署 ccTLD 合作契約[140]。於 2002 年 4 月由 JPRS 正式接管「.jp」網域名稱的註冊業務[141]。

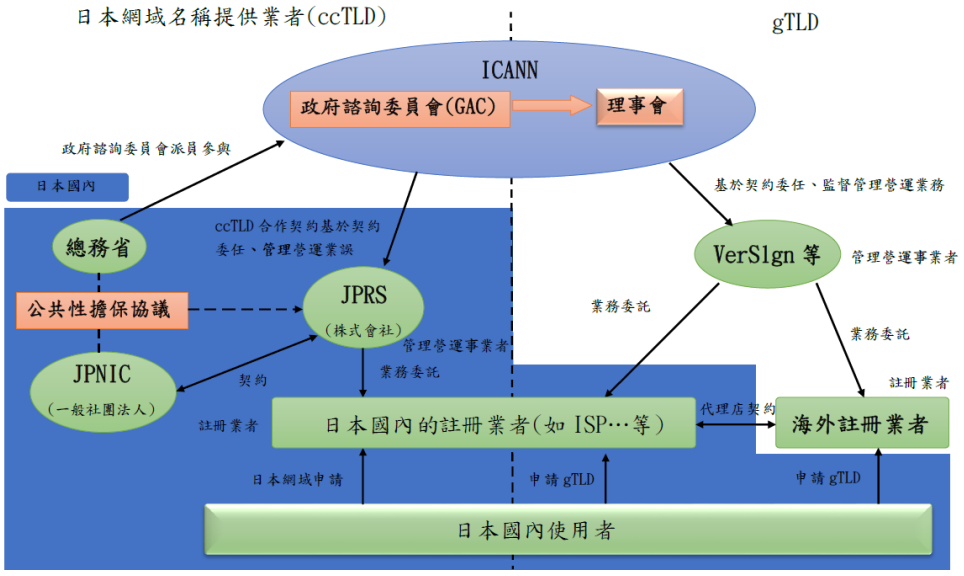


圖 8 JPRS 關係圖

[140] ccTLD Sponsorship Agreement （.jp）.

[141] 財團法人台灣網路資訊中心（編），各國頂級國碼網域名稱管理機制研究計畫，收於：財團法人台灣網路資訊中心委託研究報告，頁 23-24（2013 年）；JPRS 沿革，https://jprs.co.jp/company/history.html（最後瀏覽日：2021 年 6 月 30 日）。

隨著網路時代的來臨，網路上的違法行為漸增，關係機關及政府等對於身為註冊管理機構之 JPRS 能否將違法不當網頁之網域名稱名刪除或是停止解析網頁等方式，使網路使用者得不再接觸到該網站內容。因此於 2015 年 9 月 JPRS 內部之 JP 網域名稱諮詢委員會[142]第 53 次會議中提出議題：身為 JP 網域名稱管理機構對不當使用 JP 網域名稱時可能之對應，並請求委員會能提出相關之見解及方案。此議題經過多次討論後，提出了以下幾點方向：

1. 身為註冊管理機構之 JPRS 應有之定位[143]

JPRS 認為，沒有任何一個政策可以完美處理所有網域名稱濫用行為，且對於個案亦無法以單一政策即加以全面應對。因此有各關係機關一同合作之必要。在日本這些關係機關並不只有警察、法院，包含網域名稱濫用之通報機構及 ISP 業者等需要民間與行政機關一同面對處理。**JPRS 為 JP 網域名稱之註冊管理機構，對於網域名稱名有無濫用與否，以不自己判斷為原則**，但身為網路世界之一員有必要思考有無身為註冊管理機構所能採取之措施。

2. 怎樣的行為會構成網域名稱濫用及個案濫用與否由誰判斷較好[144]

網域名稱濫用行為有很多種，雖有透過法院來停止濫用行為及填補損害，但有些類型及個案較難透過法院解決，且所需之時間過可能造成損害擴大。因此透過 JPRS 與受理註冊機構間合作，以解決網域名稱濫用問題為較妥當。然而 JPRS 對於網域名稱濫用行為是否要停止註冊人使用.JP 網域名稱，此涉及到註冊人權利的剝奪，而由 JPRS 單獨判斷有濫用停止權利之可能。因此對於個案是否濫用網域名稱之判斷，由中立、專門之第三方機

[142] 為確保 JP 網域名稱管理業務的公平性及中立性而特別設立 JP 網域名稱名諮詢委員會。
[143] 第 56 回 JP ドメイン名諮問委員会資料及び議事録，不正行為に使われている JP ドメイン名へのレジストリとしての対応について 答申骨子，頁 2。
[144] 同註 143，頁 2-3。

構定立標準並依循該標準認定網域名稱濫用與否會是較好的方式。

3. JPRS 身為註冊管理機構對於濫用網域名稱能對應之方式[145]

JPRS 身為註冊管理機構，針對網域名稱濫用之情形，可以取消該網站使用之網域名稱，或是透過 DNS 不回傳 IP 位置與 ISP 業者及網路使用人之方式，使大眾再也無法進入該網站。然而如 JPRS 取消該網站使用之網域名稱後，所有使用該網域名稱之網站及信箱皆無法再使用，此手段有可能因過當而違反**比例原則**之虞，且將網域名稱名取消或暫停至整個網路世界無法再接觸該網站，往往要數小時到 1 天的時間，其是否屬於即時、有效之方式，也非無疑問。

從而，**較佳的方式是先請求網站管理人刪除該網頁內容**，及較接近網路使用人負責傳輸與接收網路資訊之伺服器管理者與 ISP 業者協助處理較為妥當。而當前述機構及業者無法解決時，再由 JPRS 考量是否暫停該網域名稱。

上述的討論於 JP 網域名稱諮詢委員會第 56 次之會議中有所結論。對於網域名稱濫用因取消濫用網域名稱名影響過大，因此 **JPRS 會透過不回傳網域名稱之 IP 給 ISP 業者及網路使用人之方式**，使大眾再也接觸不到該網站。對於這樣的處理機制之相關規範會載明於註冊規則中，並與 ISP 業者及受理註冊機構一同協力解決網域名稱濫用問題[146]。

現行 JPRS 之註冊規則，以「泛用 JP 網域名稱註冊規則」[147]為例，其第 29 條規範取消網域名稱註冊之事由，其第 1 項第

[145] 同註 143，頁 3-4。

[146] 第 56 回 JP ドメイン名諮問委員会資料及び議事録，正行為に使われている JP ドメイン名への JPRS におけるレジストリとしての対応の実装検討における留意点。

[147] JP 汎用 JP ドメイン名登録等に関する規則。

4 款規定當收到判決書、和解書、調解書、仲裁判斷或是與前述同一效力之文書時，JPRS 必須將該網域名稱取消；及同條項第 5 款規定，當 JP 網域名稱名之登錄明顯欠缺社會容許性時，JPRS 必須將該網域名稱取消。

協助企業、個人向 JPRS 申請網域名稱之受理註冊機構櫻花公司（さくらインターネット株式会社[148]）為例，於其網域名稱服務條款[149]第 13 條第 1 項規範有下列事由時有權將網域名稱取消、移轉、修正，其中第 3 款事由為當依各國法令規定須將網域名稱名取消、移轉、修正。

此外，同條項第 1 款事由為當網域名稱使用人違反上位規範（如 JPRS 規範）及櫻花公司基本條款時，櫻花公司有權將網域名稱註冊取消、移轉、修正。櫻花公司之基本條款[150]第 15 條第 1 項也列出相關禁止事項如下表：

表 8 櫻花公司禁止事項摘要

款	內容
1.	侵害本公司或第三人之財產、隱私、肖像權、智慧財產權及其他權利
2.	對本公司或第三人誹謗、侮辱、損害名譽、損害信用
3.	銀行帳戶及手機門號違法買賣、詐欺、管制藥物買賣、兒童性交易等違反法令之犯罪行為及其相關行為
4.	刊載或發送猥褻、兒童情色、兒童虐待等影像、文書
5.	對本公司服務下可利用之資訊為竄改或刪除
6.	發送或刊載病毒等有害電腦之程式
7.	侵入通信設備
8.	任意發送對第三人廣告、宣傳、勸誘等目的電子郵件，或是發送第三者感

[148] 該公司之各項條款，https://www.sakura.ad.jp/agreement/?_ga=2.91935647.461501070.1610173974-342210 45.1610173974&fbclid=IwAR2QkpkdOSBDY-rbsrIQzKrluKqT7V8BukXniEhhCyCUwBZS5BjPY00D7No。

[149] ドメインサービス約款，https://www.sakura.ad.jp/agreement/[a]yakkan7_domain.pdf（最後瀏覽日：2021 年 6 月 30 日）。

[150] 基本約款，https://www.sakura.ad.jp/agreement/[a]yakkan0_kihon.pdf（最後瀏覽日：2021 年 6 月 30 日）。

	到嫌惡之電子郵件
9.	違法賭博及其勸誘行為
10.	直接且明顯地要約、仲介、引誘違法行為如轉讓槍砲、提供兒童情色影音、公文書偽造、殺人、脅迫等
11.	刊載或發送殺人現場等血腥內容、虐待動物之內容，及其他社會通念明顯使人感到嫌惡之內容
12.	引誘他人自殺之行為
13.	對其他使用人或第三者明顯造成困擾
14.	違反公序良俗
15.	違法行為
16.	對本公司及第三人之設備利用或營運造成障礙者
17.	使用本公司服務對第三者之通訊造成障礙之行為
18.	妨礙本公司提供服務之行為
19.	行為態樣及目的為刊載該當前述各款事由網站之連結
20.	助長及協助第三人實施前項各款行為
21.	其他本公司認定其行為不恰當者

綜上所述，身為註冊管理機構的 **JPRS 在其註冊規則中有概略規範當 JP 網域名稱名之註冊明顯欠缺社會容許性時，JPRS 有義務將該網域名稱取消**。但該當欠缺社會容許性之態樣則有賴第三方（如前述 SIA 協助認定），並**主要透過受理註冊機構與個人及企業間契約條款之適用，將該違法及不當之網域名稱代管服務暫停或將網域名稱內容刪除**。

（七） 日本網域名稱技術濫用—網路釣魚

網路釣魚（Phishing）係指企圖從電子通訊中，透過偽裝成信譽卓著的公司以獲得如使用者名稱、密碼和信用卡明細等個人敏感資訊的詐騙犯罪行為。詐騙者會傳送偽造電子信件，或設立仿造受信任公司（例如：Yahoo 奇摩、eBay、PayPal 或使用者往來銀行或信用卡

公司）登入頁面的偽造網站，誘使受害人填寫使用者名稱（帳號）和密碼。順利取得帳號和密碼後，詐騙者可使用受害人的個人資訊盜刷信用卡、掏空銀行帳號，並可變更密碼以防止受害人登入線上帳號[151]。

參考「.JP」網域名稱註冊管理機構 JPRS 之 JP 網域名稱名諮問委員會（JP ドメイン名諮問委員会）第 54 次會議提及處理網路釣魚分成以下五個程序[152]：

1. 網路使用人、金融機構、業者等通報
2. JPCERT/CC[153]協助共同確認是否有網路釣魚情形
3. 與該網域名稱受理註冊機構或 ISP 業者聯繫
4. 受理註冊機構或 ISP 業者將網頁內容刪除或解除契約
5. 受理註冊機構無法處理時 JPRS 適時將網域名稱取消

上述 5 個流程，然而實務運作上至多於第 4 步請求受理註冊機構、ISP 業者透過與註冊人間之契約條款加以解決用於網路釣魚之網域名稱，而並無至第 5 步 JPRS 將網域名稱取消之情形。蓋如為網站被盜用作為網路釣魚使用者，由 ISP 業者通知客戶即可快速將釣魚之網頁內容刪除；或是當受理註冊機構或 ISP 業者聯繫註冊人，發現其聯絡資訊不實即可透過契約條款加以解除與註冊人間之契約；或是受理註冊機構或 ISP 業者與註冊人間契約條款多有如「內容不適、用於詐欺」等條款，即可將與註冊人間之契約加以解除[154]。

隨著網路釣魚越顯嚴重，亦有將「.JP」網域名稱用於網路釣魚。

---

[151] Yahoo，我該如何識別網路釣魚網站或電子信件？，https://safety.yahoo.com/TW/Security/IDENTIFY-A-PHISHING-WEBSITE-TW.html（最後瀏覽日：2021 年 5 月 18 日）。

[152] JP ドメイン名諮問委員会事務局，不正行為に使われている JP ドメイン名へのレジストリとしての対応について，第 54 回 JP ドメイン名諮問委員会 参考資料 3，頁 21。

[153] 日本電腦網路危機處理暨協調中心為一非營利之機構，整理資安事件資訊、建立資安預警機制，並致力於提升大眾對於資訊安全議題的重視與瞭解程度。

[154] 同註 152，頁 24。フィッシング対策協議会，NEWS LETTER No. 9:ドメイン名レジストリから見たフィッシング対策，https://www.antiphishing.jp/news/interview/news_letter_no_9.html（最後瀏覽日期 2021 年 5 月 18 日）。

故國內外網路使用者、機構等要求身為「.JP」網域名稱註冊管理機構之 JPRS 將相關網域名稱取消。對此 JPRS 發布答覆書[155]說明其可能的作為：

1. 喚起網路使用人注意

   透過介紹網路釣魚相關案例、提供受害人可能之應對方式，以促使網路使用人注意網路釣魚。

2. 取消網域名稱

   網域名稱註冊管理機構之職責在於公平、中立、不干涉網域名稱使用人之使用前提下受理網域名稱註冊。故關於網域名稱使用之妥當性，不宜逕由 JPRS 加以審查及取消該網域名稱，而應透過受理註冊機構透過與註冊人間之契約關係加以處理，屬較適當的方式。

綜上所述，「.JP」網域名稱註冊管理機構 JPRS 針對用於網路釣魚之網域名稱濫用問題，並不會直接介入將該網域名稱取消，而係透過受理註冊機構、ISP 業者與註冊人間之契約關係，解決技術濫用之網路釣魚問題。

（八） 日本使用 RPZ 停止解析針對兒童情色問題

日本特別重視網路兒童情色問題。在政策方面，於 2009 年 1 月總務省下之網路違法、有害情報對應檢討會[156]，即針對網路兒童情色問題認為「仍是待解決的問題之一，封鎖（blocking）可被期待作為限制瀏覽之手段，但須要關係者間的彼此合作」。2009 年 3 月警察廳下之總和安全對策會議[157]，亦有針對兒童網路情色問題進行討論，會議報告書中提到「封鎖（blocking）於他國已有先例，今後可參考外

[155] JPRS，フィッシング被害防止においてドメイン名レジストリが担うべき活動の方針について，https://jprs.jp/advisory/program/080509.html（最後瀏覽日：2021 年 5 月 18 日）。
[156] インターネット上の違法・有害情報への対応に関する検討会。
[157] 総合セキュリティ対策会議。

國處理方式，並立即進行相關制度之檢討」。2010 年 7 月首相官邸（似我國總統府）下之犯罪對策閣僚會議[158]，由所有內閣成員所組成之會議，於會議中提出「兒童情色排除總和對策[159]」。對策中討論到封鎖（blocking）需考量網路使用者之通信秘密及表現自由所受到的不利影響，並預計於 2010 年中討論 ISP 等相關事業者可以自主實施之對策[160]。

上述歷程並呈現於兒童買春、兒童情色行為等規制及處罰且兒童保護相關法[161]第 16 條之 3，該條文明示「提供網路供不特定人可發送、閱覽訊息之電信服務業者，基於持有、提供兒童情色之行為在網路上流通造成擴大兒童權益之損害，且一旦散布到國內外，將之刪除以回復兒童權益將變得非常困難。有鑑於此業者對於搜查機關之協力，及本於業者所擁有之管理權限，應致力於制定針對散播兒童情色之防免措施」。由此條文可看出針對防止網路散布兒童情色問題，仍是以民間自主為主，政府為輔之方式進行。

從 2011 年 4 月開始 ISP 業者開始自主針對兒童情色網站進行封鎖（blocking）。然而業者須同時考量不對網路使用者之通訊秘密及表現自由造成不當影響。故為促使 ISP 業者能加速處理網路兒童情色問題及確保其成效。現行針對網路兒童情色問題之處理，增加由警察廳及 IHC 等民間團體提供刊載兒童情色網站之資訊給網路內容安全協會（Internet Content Safety Association, ICSA）[162]，經其審查並製作出黑名單交由 ISP 業者進行封鎖[163]。相關流程圖如下：

158 犯罪対策閣僚会議。
159 児童ポルノ排除総合対策。
160 安心ネットづくり促進協議会，児童ポルノ対策の取り組みの経緯 2.国内における政府の動き，https://www.good-net.jp/blocking/prehistory/prehistory_2 （最後瀏覽日：2021 年 6 月 22 日）。
161 児童買春、児童ポルノに係る行為等の規制及び処罰並びに児童の保護等に関する法律
162 インターネットコンテンツセーフティ協会
162 インターネットコンテンツセーフティ協会
163 同註 158，頁 6-7。

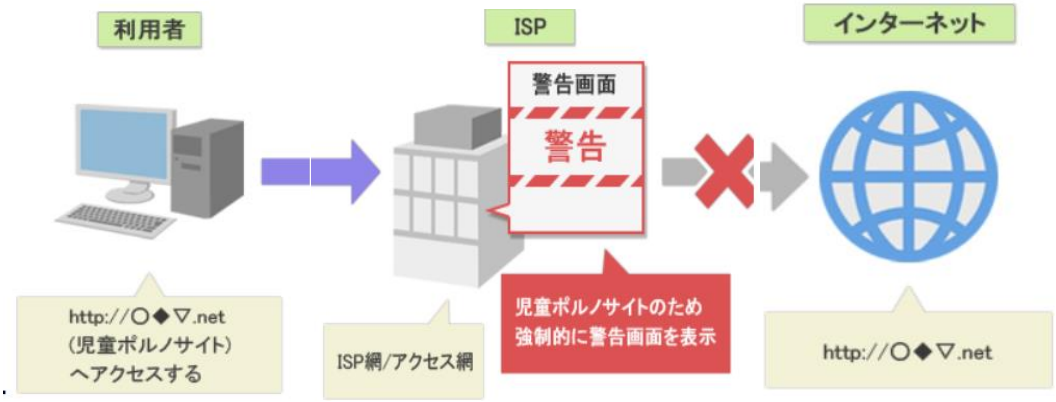


圖 9 網路兒童情色處理示意圖

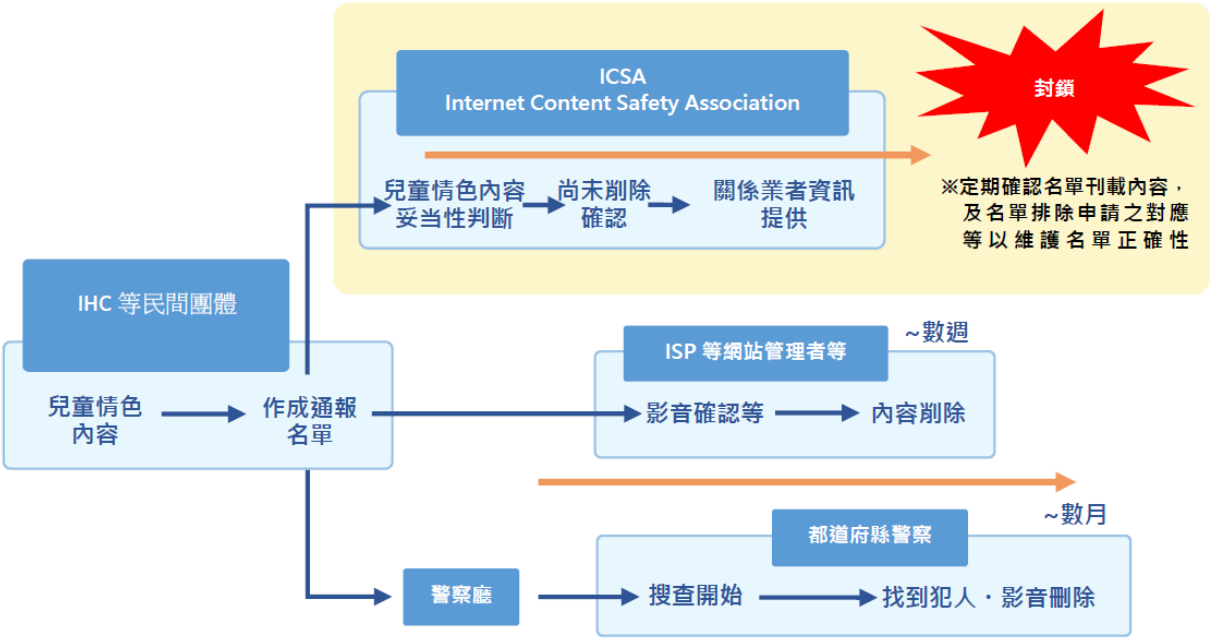


圖 10 網路兒童情色處理流程圖[164]

[164] インターネットコンテンツセーフティ協会，アドレスリスト作成業務について，http://www.netsafety.or.jp/blocking/index.html （最後瀏覽日：2021 年 6 月 22 日）。

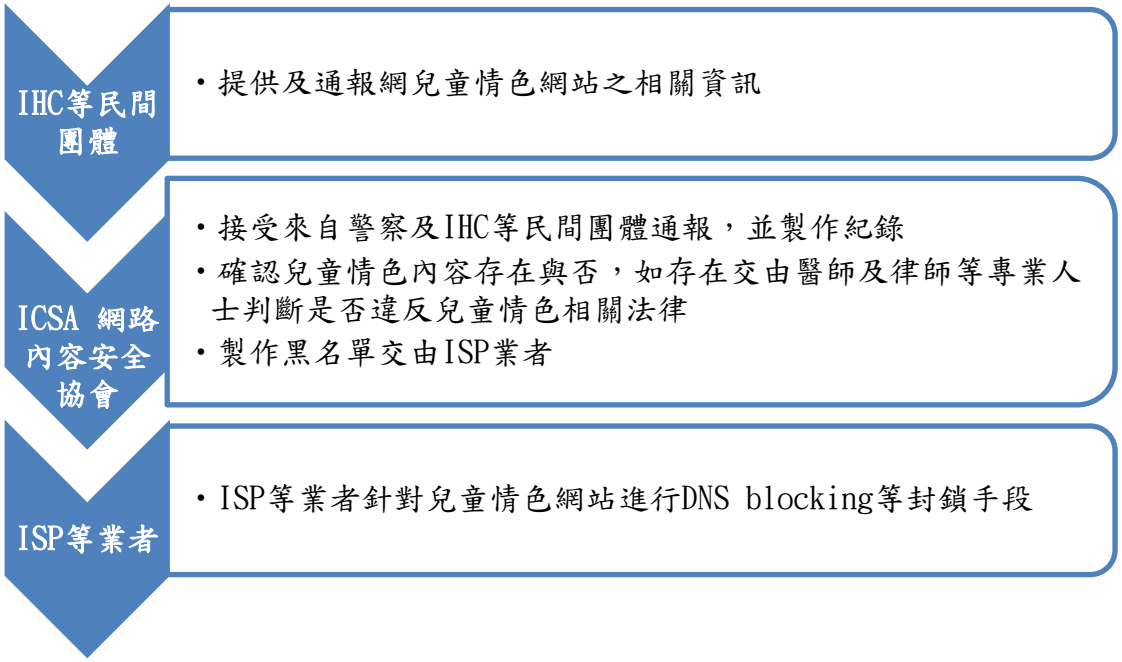


圖 11 兒童情色黑名單製作流程[165]

ICSA 針對作成黑名單有以下判斷標準[166]：

一、 網站架設目的：該網域名所有相關網站之開設目的之全部或一部為兒童情色相關影像，並將其置於網路上流通。

二、 兒童情色影像之數量：該網域名稱下之所有網站中有以下幾點之一者：

（一） 明顯侵害兒童權利之影像存在。

（二） 具有相當數量之明顯侵害兒童權利之影像。

（三） 侵害兒童權利之影像具相當比例存在。

三、 發信者具同一性：

（一） 該網域名稱下有複數網站且各網站的管理人為同一人

（二） 該網域名稱下有複數網站，有管理員以外之第三人於該網域名稱內所設置之留言區、布告欄等發布資訊時

165 同上註。

166 インターネットコンテンツセーフティ協会，DNS ブロッキングにおけるリスト対象ドメイン判定基準

1. 資訊中具有 2 位以上兒童情色影音受害者，且該網站管理者可以判定實質上是發布者之情形。
2. 或是有兒童情色以外之資訊包含在內，但多數的資訊發布者知悉此網站之架設目的為流通兒童情色影音且容忍此情形下發布資訊。

四、 無其他代替手段存在：總和考量上述三點並無其他手段可以代替將該網域名稱之 DNS 封鎖（blocking）。

此外，在總務省之支持下，由電気通信事業者協會、Telesal、日本インターネットプロバイダー協会（JAIPA Japan Internet Providers Association），及日本ケーブルテレビ連盟（JCTA Japan Cable and Telecommunications Association）等四個業界協會共同組成違法情報對應連絡會[167]，並公布違法有害情報對應契約條款範本[168]供公佈欄網站管理員及網路服務提供業者，視情況將範本條文納入與服務使用人間之契約中。範本第 4 條第 1 項即針對網路兒童情色影音之封鎖（blocking）有具體規範，謂「本公司為防止擴大被害兒童權益侵害，本公司或製作兒童情色網站黑名單團體判斷顯著侵害兒童權利之兒童情色影音，可事前不通知，即可在確認該網站存在下，使兒情情色影音無法再行閱覽。」，並參酌違法有害情報對應契約條款範本之解說，「使兒情情色影音無法再行閱覽」係指強制使網路使用人無法再行連接至相關網站，即使用 DNS blocking 之技術，使網站無法再行瀏覽。

綜上所述，日本針對網域名稱濫用問題，係採取民間自主政府為輔之互動模式解決問題。針對特別重視的網路兒童情色影音問題，除在法律上具體說明網路服務業者須共同協助解決外，亦是於民間團體公布之契約範本中具體說明使用到 DNS blocking 之技術解決網域名稱濫用問題。

[167] 違法情報等対応連絡会。
[168] 違法・有害情報への対応に関する契約約款モデル条項。

（九） 日本如何處理境外網域名稱濫用

隨著網路無國界，網頁內容以中文表達，然而其網站管理人或網域名稱註冊人可能使用國外伺服器及網域名稱，放置違反本國法之內容。針對此種情形應如何處理該網域名稱，維護國人權益即為重要議題。

日本針對境外網域名稱內容濫用，亦在 SIA 處理、協助通知之工作範圍內。SIA 業務範圍可參考下圖：

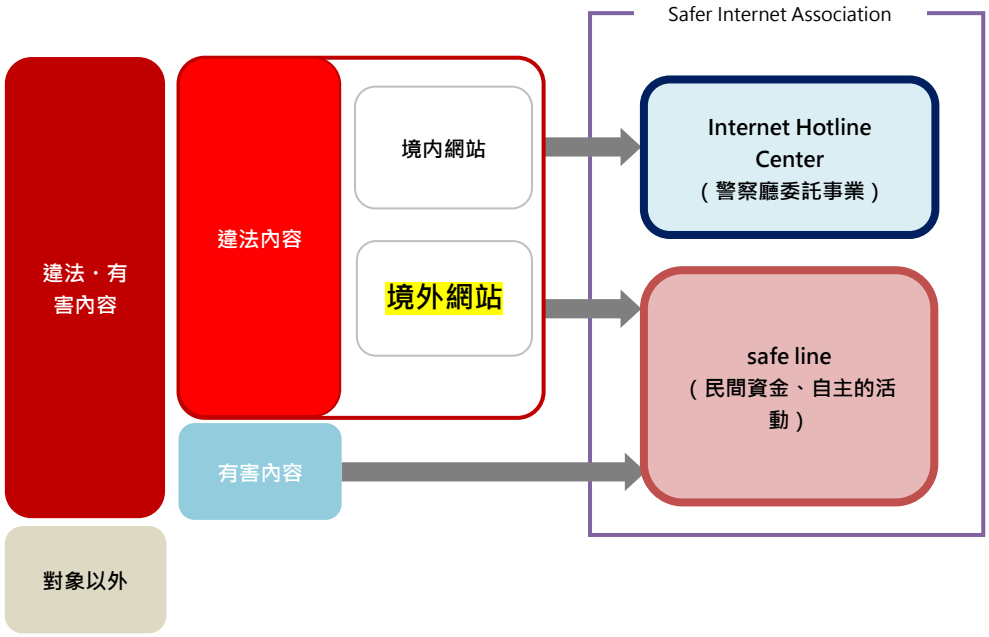


圖 12 SIA 業務範圍[169]

根據 SIA 網站公布之最新 2019 年數據，該年度通報網域名稱放置違法、有害內容共計 47,396 件，其中於日本境內約 10.4%，而高達 89.6%為境外網域名稱，而其中美國占 52%，其次荷蘭占 39%，而法國占 4%[170]。

[169] Safer Internet Association，違法・有害情報対策活動報告（2019），頁 4。
[170] Safer Internet Association，同註 169，頁 10-13。

日本境內網域 10.4%　　日本境外網域 89.6%

圖 13 境內及外網域名稱內容濫用比例

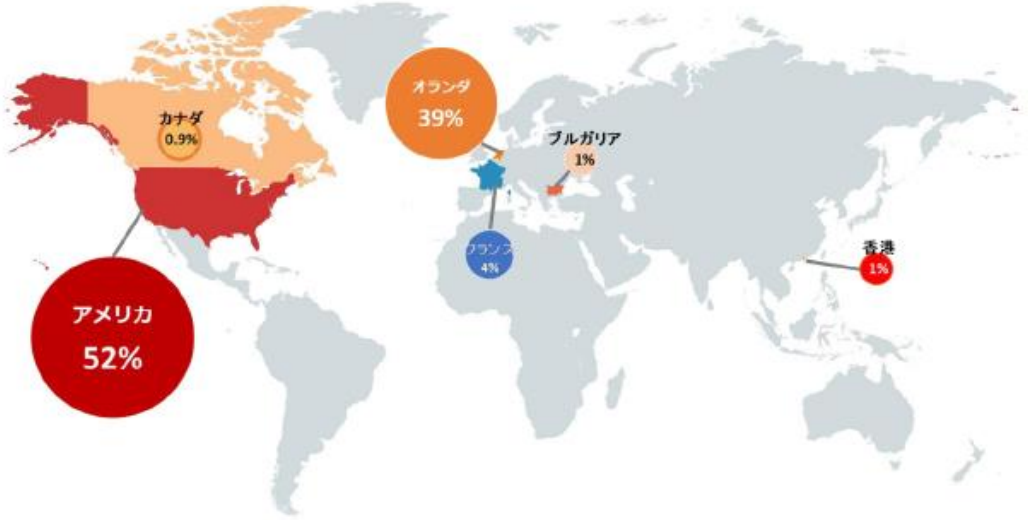


圖 14 違法及有害網域名稱所在國家比例

2019 年 SIA 境內外總計發出 21,183 件請求，請求 ISP 業者或網站管理人刪除違法及有害之內容，當中有 19,540 件成功刪除內容，刪除率約為 92%。雖然有些境外網域名稱內容在日本境內屬違法而在國外並非違法，然而對境內外網域名稱刪除率並無太大影響，境內網域名稱刪除率約為 90%，而境外網域名稱刪除率為 93%[171]。具體各項濫用通報數、請求刪除數及刪除率等境內外比較可參考後面表

[171] Safer Internet Association，同註 169，頁 13-14。

格。SIA 能有高達 92%之刪除成效，源於其由網路業界自組成立外，其專業性及權威受到肯定並同時有營運政府委託之 IHC 熱線，故業者多能尊重 SIA 之判斷，協助刪除相關網域名稱違法及不當之內容。

日本境內刪除率 90%　　日本境外刪除率 93%

圖 15 境內外網域名稱刪除率

第二項　美國

在美國憲法增修條文第 1 條的言論自由保障下，美國對於言論內容之保障相當完整。網路內容即屬使用者之言論，因此其在美國之網路內容或使用者行為規管亦受言論自由之保障。**政府原則上不得事前審查、限制言論內容否則視為違憲[172]。言論內容之事後審查亦僅得於限定之情況下始得限制**。

（一） 通訊端正法（Communication Decency Act）

美國通訊端正法（Communications Decency Act，下稱「CDA」）第 230 條（47 U.S. Code § 230）係於 1996 年訂立。原本立意是為保障兒童在網路上避免取得「猥褻或不端正」（obscene or indecent）資訊而（1）禁止故意運用通訊裝置傳送不端正的內容予未滿 18 歲的未成年人，並（2）以刑罰禁止故意讓未滿十八歲未成年人取得依現今社區標準明顯令人不悅（patently offensive）的方式描述（depict or describe）性行為或器官等（sexual or excretory activities or organs） 資訊[173]。惟本法此部分之規範

[172] 美國最高法院判決：Sable Communications v. FCC, 492 U.S. 115 (1989)

[173] 陳起行，由 Reno v. ACLU 一案論法院予網際網路之規範，歐美研究第 33 卷第 3 期，頁 603（2003 年 9 月）。

最終於美國最高法院 1997 年 Reno v. American Civil Liberties Union（ACLU）案，以過度限制言論自由、規範過廣而違憲。然 CDA 其他部分之規範，仍然有效。其中最重要者為第 230 條之規定[174]。

一般認為 CDA 第 230 條之規定為網際網路服務供應商之「安全港條款」，因為其中規範兩大重點：

1. 免除互動式電腦（interactive computer）系統服務提供者（service provider）或使用者（user）對於任何資訊內容提供者所提供之資訊的發表人或出版者責任[175]。換言之，互動式電腦服務提供者或使用者均不視為該第三人所提供之資訊出版者或發表人。
2. 免除互動式電腦系統服務提供者或使用者對於（a）其主動且善意採取之任何行為限制接觸或取得其認為猥褻、淫亂、骯髒、過度暴力、屬於騷擾或其他令人反感之資訊，無論該等資訊是否受憲法保障及（b）採取任何技術方法限制上述資訊取得之行為之一切民事責任。

而依據 CDA 第 230 條之定義及美國聯邦法院之判例，「互動式電腦系統服務提供者或使用者」包括網站提供者（如 facebook）、網際網路服務者（如中華電信）、網域名稱受理註冊機構（如 GoDaddy）及註冊管理機構（如 GoDaddy Registry）等[176]。因此，**互動式電腦系統服務提供者或使用者，因為僅提供平臺予資訊發表者發表網路內容，因此不會對該內容負責任[177]**。即便系統服務提供者已收到資訊移除通知，但其不移除該第三人所發表之誹謗資訊，仍不受侵權行為之損害賠償責任[178]。再者，部份美國法院認為，系統服務提供者得自行選擇是否審查使用者所發布之資訊，且無論審查與否，均免除其責任[179]。

---

[174] 47 U.S. Code § 230 - PROTECTION FOR PRIVATE BLOCKING AND SCREENING OF OFFENSIVE MATERIAL.

[175] 47 U.S. Code § 230(c)(1) "*Treatment of publisher or speaker: No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider.*"

[176] Kathleen A. Ruane, *How Broad A Shield? A Brief Overview of Section 230 of the Communications Decency Act*, Congressional Research Service (Feb. 21, 2018), https://fas.org/sgp/crs/misc/LSB10082.pdf .

[177] 美國聯邦第 4 巡迴法院 1997 年 Zeran v. American Online 案 129 F.3d 327

[178] 美國聯邦第 9 巡迴法院 2009 年 Barnes v. Yahoo!, Inc. 案 570 F.3d 1096

[179] 美國聯邦第 4 巡迴法院 2003 年 Green v. Am. Online, Inc. 案 318 F.3d 465

CDA 第 230 條之保護雖似全面，但依其規定，此法律不影響或限制任何關於（1）人口性販售、（2）刑法、（3）智慧財產權之法律或（4）1986 年電子通訊隱私法的實施或其執行。因為 CDA 第 230 條之規範，美國系統服務提供者受非常廣泛之免責保護。而受害之當事人，除上述例外情況外較有法律依據向系統服務提供者求償外，僅得依一般侵權行為法或其他法律直接向不法網路內容發表者求償。實務上亦有其他限制：

1. 系統服務提供者已明確同意移除誹謗資訊卻不移除者，則有可能適用禁反言之原則（promissory estoppel）而負損害賠償責任[180]；
2. 若系統服務提供者修改或編輯誹謗或其他有害資訊，而該行為實質加強原第三者所提供之不法資訊時，則屬於資訊之提供之範疇而不受免除責任之保護[181]；
3. 如統服務提供者積極向第三方資訊提供者索取不法或侵權言論資訊並使其發表時，亦失去 CDA 第 230 條之保護[182]。

依照目前美國法院案例，若該不法資訊之發表係依據與系統服務提供者之委任或雇傭關係而產生，系統服務提供者仍有可能負損害賠償責任[183]。

在此原則下，目前所蒐集之美國聯邦法律對於網際網路內容或使用者行為之立法例多屬關於（1）兒少保護、（2）電腦資安、（3）智慧財產權之保護，然其他網路內容或使用者行為，除受侵權行為等民刑法之一般規範外，並無特別之聯邦立法例。

（二） 兒少保護類立法例

1. COPPA/CIPA

美國關於網路及兒少保護之聯邦立法例主要係由「兒童線上隱

[180] 同上註。
[181] 美國聯邦第 9 巡迴法院 2008 年 Fair Housing Council v. Roommates.com, LLC 案, 521 F.3d 1157
[182] 美國聯邦康州法院 2010 年 Doctor's Assocs., Inc. v. QIP Holder LLC 案 2010 WL 669870
[183] 美國加州上訴法院 2006 年 Delfino v. Agilent Tech., Inc.案 52 Cal. Rptr. 3d 376；美國聯邦第 9 巡迴法院 2000 年 Ben Ezra, Weinstein and Co., Inc. v. Am. Online, Inc. 案, 206 F.3d 980

私保護法」（Children's Online Privacy Protection Act，下稱「COPPA」[184]）及「兒童網路保護法」（Children's Internet Protection Act，下稱「CIPA」[185]）。

COPPA 是美國於 1998 年通過、2000 年生效之聯邦法律，COPPA 規定商業網站業者提供之服務如以 13 歲以下之兒童為對象時，應事先告知並取得父母同意後始得蒐集兒童之個資；同時就蒐集、使用、揭露兒童之個人資訊或其用途，業者負有說明義務。COPPA 之主管機關為美國聯邦貿易委員會（FTC），FTC 得依據 COPPA 之授權訂定實施辦法並有核可業者自律機制。雖 COPPA 與 CIPA 並無直接針對網路內容或使用者行為作規範，然而係規範網路業者對於兒童之個資收集與取得家長同意等措施（COPPA），以及受政府補助之學校或圖書館對於兒童取得不適當網路資訊之採取之強制保護措施（CIPA），此部分我國或可參考。**惟 COPPA 及 CIPA 兩法律均無對註冊管理機構之責任做任何規範**，且實務上亦難證明註冊管理機構是否知悉有違反 COPPA/CIPA 之行為存在於其網域名稱內。然可確定是，主張網路業者違反 COPPA 而受有損害者，須經由法律程序向業者主張。

2. SESTA-FOSTA

禁止性拐賣法及允許各州及受害者打擊性拐賣法（SESTA-FOSTA）係於 2018 生效。由於其規範目的在於限縮 CDA 第 230 條之保護，因此法案推出之際即引起捍衛言論自由組織及保守派之抗議並且已經有利害關係人提起聯邦法院訴訟。然而，此法案是目前唯一仍然有效且限制 CDA 第 230 條對於網路業者保護之聯邦法律。

依據 SESTA-FOSTA 之規定，互動式電腦系統服務提供者、所有人、經營者或使用者不得**明知**廣告或促使他人賣淫或性販運，如該等資訊係由他人提供者亦同，否則將有民事及刑事責任。換言之，

[184] 聯邦法典 15 U.S.C. § 6501

[185] 聯邦法典 20 U.S. Code § 9134 及 47 U.S. Code § 254

SESTA-FOSTA 明確排除網路平臺業者之民事責任豁免並且加入了刑罰。目前尚無依據 SESTA-FOSTA 起訴或受罰之網路業者。此外，**SESTA-FOSTA 亦無對註冊管理機構之責任做任何規範**且實務上亦難證明註冊管理機構是否知悉有違反 SESTA-FOSTA 之行為存在於其網域名稱內。然可確定是，主張網路業者違反 SESTA-FOSTA 而受有損害者，須經由法律程序向業者主張。

（三） 電腦資安之立法例

美國聯邦電腦詐欺及濫用防制法（CFAA[186]），係於 1986 年制定並經歷數次修訂之聯邦法律。CFAA 主要所處罰的行為型態是無（越）權使用電腦的行為，包括行為[187]：

1. 禁止間諜行為（Espionage prohibitions）
2. 未獲授權或逾越權限之資訊獲取
3. 侵入政府系統（Trespass on government system）
4. 基於詐騙之意圖（With intent to defraud）
5. 造成損害（Causes damage）之行為
6. 密碼之交易（Password trafficking）
7. 勒索電腦與資料進行勒索（Extortion threat to a computer/data）

CFAA 之性質如同我國刑法第 358 條之入侵電腦罪，惟其構成要件較廣，並課予行為人民事與刑事責任，由受害人或政府調查機關（如 FBI、CIA）經由法院程序起訴之方式向行為人主張權利。然 CFAA 並無對註冊管理機構之法律責任有任何規定。

（四） 保護智慧財產權之相關立法例

美國就註冊管理機構之法律責任，除 CDA 第 230 條外，最為相關之

---

[186] 聯邦法典 18 U.S.C. § 1030

[187] 陳靜慧，2018 年 3 月 5 日「跨境電腦犯罪之司法管轄 與發展趨勢 ～以網路詐欺犯罪為中心」出國報告，https://report.nat.gov.tw/ReportFront/PageSystem/reportFileDownload/C10700108/001 （最後瀏覽日：2021 年 6 月 30 日）。

法律即屬與智慧財產權保護之聯邦法律。其中，最為廣泛適用者屬「數位千禧年著作權法」（Digital Millennium Copyright Act，下稱「DMCA」）以及「反網路侵佔消費者保護法」（Anti-Cybersquatting Consumer Protection Act，下稱「ACPA」）。

1. ACPA

ACPA 係於 1999 年生效之聯邦法律[188]，其主要規範功能在於提供商標權人對付惡意搶註冊者之法律上之請求權基礎，禁止惡意從他人商標或 ACPA 保護之個人名字中獲利，且註冊、買賣、使用相同或近似混淆已是具有特殊性商標之網域名稱，或註冊、買賣、使用相同或近似以混淆或淡化於在註冊時已是著名商標之網域名稱[189]，違反者須負商標權人損害賠償責任。

主張 ACPA 之商標權人，須證明他人搶註係屬「惡意」。而法院判斷是否屬惡意之因素亦訂定於 ACPA 內，且類似 ICANN UDRP 之要件，包括[190]:（1）註冊人於網域名稱有商標或其他智慧財產權、（2）網域名稱是否為註冊人之合法姓名或通常稱呼之註冊人之名稱、（3）註冊人註冊該網域名稱係為避免或阻礙商標權人或標章之所有人取得與其商標或標章相對應的網域名稱，且註冊人過去已有相當類似之行為模式等其他 9 因素。

此外，ACPA 亦明確規定商標權人，除得提起一般法院救濟外，亦得向法院提起對網域名稱之「對物之民事程序」（in rem civil action）並規定對物之法院管轄範圍（註冊管理機構之所在地或註冊文件提交所在地）及送達程序[191]。對物之名民事程序之救濟僅限於對網域名稱之（1）沒收（forfeiture）、（2）撤銷（cancellation）或（3）將其移轉（transfer）至商標權人。

---

188 聯邦法典 15 U.S.C. § 1125(d)

189 楊擴舉，「網域名稱爭議與商標權保護基本問題之研究」，https://www.tipo.gov.tw/tw/cp-182-313838-f9a73-1.html （最後瀏覽日：2021 年 6 月 30 日）。

190 聯邦法典 15 U.S.C. § 1125(d)(1)(B)

191 聯邦法典 15 U.S.C. § 1125(d)(2)(A)至(C)

關於註冊管理機構之法律責任，ACPA 僅規定有限之責任如下[192]:（1）當註冊管理機構收受商標權利人起訴之通知時，註冊管理機構須提交法院一切足以使法院掌控並瞭解該網域名稱之登記與使用情形之資料；(2）除收受法院命令外，不得於訴訟程序中任意移轉、暫停或為任何網域名稱變更之措施；及（3）如收到法院命令而故意不為命令指示之作為或不作為，註冊管理機構須負金錢損害賠償或假處分之責任[193]。

2. DMCA

數位千禧年著作權法係於 1998 年生效之聯邦法律，其主要係針對當時之著作權法予以修訂，增修內容要點有下列幾項：(1）世界智慧財產權組織條約之施行、(2）網際網路侵害著作權責任之規範、（3）暫時性錄製、遠距教學、圖書館與檔案保存處之免責、(4）電腦之維護或修理[194]。

DMCA 主要目的係在於保障著作權，包括網路著作權。除一般著作權之保障外，較特別之處在於其所建立之網路服務提供商（online service providers，包括 ISP）之「避風港條款」[195]。因我國「網路服務提供者之民事免責事由」部份訂定係參考 DMCA 第 512 條之規定，我國著作權法第六章之一「網路服務提供者之民事免責事由」之規定與 DMCA 避風港條款（DMCA 第 512 條）有許多共同之處，在此不重複逐一比較說明。然無論依 DMCA 抑或我國著作權法之規定，註冊管理機構均無需對網路內容或使用者行為須負法律責任。

（五） 美國之網域名稱扣押—In Rem Forfeiture

---

[192] 聯邦法典 15 U.S.C. § 1125(d)(2)(D)

[193] Kaplan, Jason S, *The Anticybersquatting Consumer Protection Act: Will it End the Reign of the Cybersquatter?*, VOL. 8 IS.1 UCLA ENTERTAINMENT LAW REVIEW 43, 4X (2000).

[194] 王琇慧，「千禧著作權法（DMCA）施行之新平台-自由貿易協定（FTA）」，頁 92，2005 年，https://www.tipo.gov.tw/tw/dl-4488-bdb94726bc00408e95fc8604e0e10717.html （最後瀏覽日：2021 年 6 月 30 日_。

[195] 聯邦法典 17 U.S. Code § 512

在美國司法體系下，有三種對物扣押型態。「刑事沒收（Criminal Forfeiture）」為刑事起訴之一部分，其依據對「被告」的管轄（in personam jurisdiction）而通常為犯罪工具或所得。於刑事訴訟程序中，若陪審團裁判被告有罪且犯罪工具或所得是得以扣押者，法院將依據該決定發布扣押命令，故美國法之刑事沒收之性質與我國之刑事沒收性質一致。

另外，「行政扣押」（Administrative Forfeiture）與「民事扣押」（Civil Forfeiture）均係依據對物（in rem jurisdiction）之管轄。行政扣押（Administrative Forfeiture）不須經司法程序即得由行政機關執行扣押，行政機關之法源依據為 1930 斯姆特-霍利關稅法案（The Smoot-Hawley Tariff Act），惟行政扣押之標的均係與進出口管制物品、票據等其他價值不超過美金 50 萬元之相關物品，不包括網站且實務上亦無主張網域名稱得適用關稅法案之案例。美國網域名稱民稱扣案例均係以民事扣押之手段實施。本節將簡介美國對物扣押之依據以及網域名稱扣押之實例。

1. 民事對物管轄與扣押之法源

美國民事扣押（Civil Forfeiture）係依據法院對物之管轄權而生。對物管轄之法理源自於 1877 年美國最高法院 Pennoyer v. Neff 案例[196]。依據 Pennoyer 案，各州對位於其領土內之個人及物品均有管轄權，法院亦同。隨著各州之間貿易發達，美國最高法院於 1945 年 International Shoe Co. v. Washington 案例[197]進一步闡釋對物之管轄法理，使位於不同州之被告若有財產於本州或於本州有任何作為時，即屬於有與本州之「最低接觸」（Minimum Contacts）而使本州法院對於該被告或財產有管轄權。因此，對物之管轄在美國司法體系下已行之有年且廣為適用。

雖美國最高法院至今對於網域名稱是否為「財產」尚無表示，實務上，美國司法部（DOJ）、國土安全部（DHS-ICE）及國家智慧財產權合作中心（IPR Center）已因違反智慧財產權相關法律而對網域

[196] 95 U.S. 714 （1877）
[197] 326 U.S. 310 (1945)

名稱為民事扣押。

此實務做法係依據聯邦法典 18 U.S.C.第 2323 條及 18 U.S.C.第 981 條之規定。其中，18 U.S.C.第 2323 條主要規範「任何用以交易第 2319 條所禁止標的之物品，或是任何用以、或意圖用以犯罪或幫助全部或一部犯罪之財產，均應沒收」並適用民事扣押/沒收之規定[198]。18 U.S.C.第 2319 條即為違反著作權之刑事責任。此外，相關智慧財產權法案有（1）1999 年反搶註消費者保護法（ACPA）及（2）2008 年智慧財產資源及機構優先法案（Prioritizing Resources and Organization for Intellectual Property Act，下稱「Pro-IP Act」）。ACPA 主要規範惡意註冊與他人商標或該法保護之個人名字之民事責任。行為人不得從中獲利，且註冊、買賣、使用相同或近似混淆已是具有特殊性商標及之網域名稱，或註冊、買賣、使用相同或近似以混淆或淡化註冊時已是著名商標之網域名稱。Pro-IP Act 則是加重違反著作、商標、專利等智慧財產權之民刑事責任。兩者均對民事扣押有明文規範。上述法律均係近年美國 DHS-ICE 執行網域名稱扣押之主要依據。

2. 網域名稱扣押之一般程序

美國對物扣押之民事程序適用聯邦刑事訴訟法之規定，屬於單方程序（ex-parte proceeding）[199]。原告或執法單位（如 DOJ、DHS-ICE 等），於搜集相關違法情事證據後（如非法散佈他人著作、販售仿冒品或網域名稱與註冊商標相似且混淆之情況），出具切結書載明犯罪事實並詳列證據後，向管轄法院聲請，法院認定犯罪事實有超過相當理由（probable cause）之依據後，核發扣押命令[200]。取得扣押命令後，原告或執法單位即送達於註冊管理機構，註冊管理機構依命令將網域名稱轉向指定網頁（IP 位置），使欲瀏覽該網站之使用者無法

198 18 U.S. Code § 2323, https://www.law.cornell.edu/uscode/text/18/2323.
199 *Supra* note 100, at 861.
200 陳昱奉，數位時代之犯罪偵查與網路自由及隱私權之保障—從網域名稱（Domain Name）之扣押、沒收談起，臺灣嘉義地方法院檢察署 102 年度自行研究報告，頁 17-20（2014 年 12 月），https://www.cyc.moj.gov.tw/media/136016/551410383574.pdf

以原有網址瀏覽原始內容[201]（如圖 16）。

圖 16 healthbridgescience.com 網域名稱扣押後之畫面

依據美國聯邦法典 18 U.S.C.第 983 條關於民事扣押之規定，一般而言，扣押聲請者為政府時，執法機關應即時通知利害關係人且最遲需於扣押後 60 日為之。受通知人得於收到通知 35 日內提異議救濟，異議後執法機關有 90 天得向法院證明扣押網域名稱之依據。若受通知人並無提出異議或執法機關成功說服法院扣押網域名稱之依據，扣押即成立[202]。反之，若受通知人提出異議，執行機關則得啟動法院扣押程序，如不啟動法院扣押程序，執行機關須回復並交回網域名稱予受通知人（或註冊人）。18 U.S.C.第 983 條亦規定其他關於後續訴訟、當事人適格，訴訟代理人等其他程序規定。

（六） 對於境外網域名稱之處置

有關美國實務境外網站之封鎖，2011 年美國國會曾提出「遏止網路盜版法案」（Stop Online Piracy Act, SOPA），在該法案下，美國司法部得對境外侵權網站取得令狀，要求 ISP 業者、網路廣告業者、

[201] *Supra* note 100, 874- 76.
[202] 18 U.S.C. §983，https://www.law.cornell.edu/uscode/text/18/983.

網路支付服務業者停止與侵權網站交易，並禁止搜尋引擎顯示侵權網站網址，以達到境內封鎖網站之效力[203]。惟此法案產生箝制網路自由及商業發展之爭議，2012 年該法案便被國會擱置未通過[204]。

至若境外網域名稱扣押方面，美國移民及海關執法局（U.S. Immigration and Customs Enforcement's, ICE）及國土安全調查局（Homeland Security Investigations, HIS）曾經實施「Operation In Our Sites」行動，針對求全販賣仿冒物的網站進行扣押，該行動於 2010 年至 2014 扣押 2550 個網域名稱[205]。若違法網站為美國境內網域名稱，ICE 等執法機關得向法院提出相當合理（probable cause）之證據及說明，由法院核發令狀後，執法機關持該令狀向註冊管理機構要求將網域名稱 IP 位址導向美國政府，此過程中，執法機關無須證明違法網站確實有侵害他人權利或者違反刑事法規[206]。至若違法網站為美國境外網域名稱，由當地網域名稱註冊管理機構扣押並保管。

「Operation In Our Sites」為跨國行動，雖然部分美國境外網域名稱係由當地政府扣押，美國政府對於境外網域名稱理應沒有管轄權限，惟美國當局最終取巧地突破跨境執法之限制。原理在於，因管理.com、.org 和.net 頂級網域名稱註冊管理機構為 VeriSign 公司，又 VeriSign 公司位於美國境內，美國移民及海關執法局表示，只要持法令扣押命令，可要求 VeriSign 執行任何結尾為.com、.org 等網站之扣押，VeriSign 並會將該網域名稱重新導向到美國政府的 IP，告知訪問者該網站已被查封[207]，以上流程不必經由國際司法互助或者訴訟程序便可完成。2012 年 2 月間，於加拿大註冊網域名稱「Bodog.com」

[203] 陳昱奉，同註 200，頁 34-36。
[204] 謝孟珊，網路媒體界群起抗議，美國總統歐巴馬表示反對，SOPA 法案遭到擱置，資策會科技法律研究所，2017 年 1 月，https://stli.iii.org.tw/article-detail.aspx?no=64&tp=1&d=5627。
[205] Newsroom, *international law enforcement agencies seize 706 domain names selling counterfeit merchandise*, U.S. Immigration and Customs Enforcement (Dec. 12, 2017), https://www.ice.gov/news/releases/ice-international-law-enforcement-agencies-seize-706-domain-names-selling-counterfeit
[206] 陳昱奉，同註 200，頁 10-14。
[207] David Kravets, *Uncle Sam: If It Ends in .Com, It's .Seizable*, Wired(Mar. 6, 2012), https://www.wired.com/2012/03/feds-seize-foreign-sites/.。

遭扣押，輸入網址後只見美國司法部及國土安全部之標誌[208]，此即係美國政府向 VeriSign 核發扣押命令完成查封之案件。上述做法之案件，VeriSign 並未透露其已和美國政府合作期間及案件數量，惟可能已透過此方式沒收了大量販賣違禁物、非法串流音樂和電影、以及簽賭博弈網站。

近年來，目前實務上較常出現的情況，被法院以扣押命令沒收的網域名稱，大多是在美國境內註冊，而違反特定目的事業法規者而言，尤其大多數案件係牽涉恐怖主義、被美國制裁國家（例如伊朗）散佈不利美國訊息者，例如未經過外國資產控制辦公室（Office of Foreign Assets Control）註冊便使用美國國內公司註冊網域名稱者，法院便以此境內網域名稱為非法使用之事實核發扣押命令[209]。不過仍疑似有案件係政府機關向 VeriSign 核發命令要求將網域名稱移轉給政府之案例，例如德黑蘭國際聯播網「Press TV」，2019 年期間正值美國對伊朗制裁，PressTV 旗下網域名稱「presstv.com」便被美國政府扣押[210]。惟政府官方新聞稿並未詳細說明本案扣押方式是否類似「Operation In Our Sites」模式。

（七） 近年立法趨勢

綜上所述，美國對於網際網路內容或使用者行為訂有規定之立法例相當少，且多數在於兒少保護、資安保護及智慧財產權保護。按美國註冊管理機構相關立法例，最為重要者即係 CDA 第 230 條之規定，因其免除了網路中介人對於第三方於其網域名稱之內容的民事責任。

近期美國國會提出有關網路內容或使用者行為的法案有 2020 年 3 月之**消除對互動科技的濫用和肆意忽視法案**（Eliminating Abusive

[208] Dan Katz, Bodog.com Domain Name Seized by U.S. Government, Poker News Daily (Feb. 28, 2012), https://www.pokernewsdaily.com/bodog-com-domain-name-seized-by-u-s-government-21299/
[209] Department of Justice, United States Seizes Domain Names Used by Foreign Terrorist Organization, https://www.justice.gov/opa/pr/united-states-seizes-domain-names-used-foreign-terrorist-organization (last visited: Sept. 21, 2021).
[210] Julia Dickson, *U.S. Seizes Websites Tied to Iran*, United States Institute of Peace (Jul. 7, 2021), https://iranprimer.usip.org/blog/2021/jul/07/us-seizes-websites-tied-iran

and Rampant Neglect of Interactive Technologies Act）[211]、2020 年 6 月之**平臺問責與消費者透明度法案**（Platform Accountability and Consumer Transparency Act）[212]。兩法案之目的均在限縮 CDA 第 230 條之保護並且加強政府對於網路平臺之規管能力，惟目前尚未有明確立法程序上之進展。就美國政府方面，時任美國川普總統於 2020 年 5 月 28 日簽屬「防止網際網路審查」行政命令（Executive Order on Preventing Online Censorship）[213]。此行政命令雖名義上似乎在保障網路言論自由，但實際上其內文則是限縮網路平臺業者 CDA 第 230 條之保護，因為它將規範網路業者審查第三方內容之行為、賦予聯邦貿易委員會介入並調查網路平臺業者是否違反其服務條款而為不實廣告。依此行政命令，如網路平臺業者對於第三方所提供之資訊進行編輯或審查（包括將發文標示為可能之不實言論、移除、修改、限制等）時，網路平臺業者即屬於該資訊之發表者而排除適用 CDA 第 230 之保護。然而，此行政命令僅屬政策方向宣導非屬法律，尚待美國司法部長（US Attorney General）依據此行政命令之授權開始草擬相關法案並遞交於立法程序後，才有修改 CDA 第 230 條之法律效力。

CDA 第 230 條之聯邦法律顯示了美國法制對於言論自由保障之程度，並明定網路中介人最大限度之免責條款。相較於其他國家，美國無專一或單獨法律規範網路內容或使用者行為，且依上述美國最高法院案例以及其近期立法經驗，美國目前應傾向不採取如馬來西亞對於網路內容或使用者行為之規範。

第三項　馬來西亞

（一）通訊傳播暨多媒體法介紹—第 233 條與第 263 條網站封鎖（site

[211] 全文於美國國會官方網站 https://www.congress.gov/bill/116th-congress/senate-bill/3398（最後瀏覽日：2021 年 6 月 30 日）。
[212] PLATFORM ACCOUNT ABILITY AND CONSUMER TRANSPARENCY ACT, https://www.schatz.senate.gov/imo/media/doc/OLL20612.pdf (last visited: Jun. 30, 2021).
[213] UPDATE: Section 230 and the Executive Order on Preventing Online Censorship, Congressional Research Service, https://crsreports.congress.gov/product/pdf/LSB/LSB10484 (last visited: Jun. 30, 2021).

blocking）措施

為因應 1990 年代新興匯流通訊傳播與多媒體產業之興起，馬來西亞政府於 1998 年針對通訊傳播及多媒體產業採取匯流之管制模式，並整併原有之 1950 年電信法（Telecommunications Act 1950）與 1988 年廣電法（Broadcasting Act 1988）之法規內容，於 1999 年 4 月 1 日正式頒布 1988 年通訊傳播暨多媒體法（Communications and Multimedia Act 1998，下稱 CMA），做為全新之匯流監理與發照制度之法制基礎[214]。

此外，馬來西亞政府亦為新創立之監理機關—馬來西亞通訊傳播暨多媒體委員會（Malaysian Communications and Multimedia Commission，下稱 MCMC）頒布馬來西亞通訊傳播暨多媒體委員會法（Malaysian Communications and Multimedia Commission Act 1998）[215]。

通訊傳播暨多媒體法共計有 11 篇，適用範圍包含電信、傳播電視及多媒體，其立法架構係以事務管轄為章節主體，即自原有之電信與廣播電視之規範歸納出共通之規定，第 1 篇至第 5 篇主要為管轄與程序性規定以及執照制度，第 6 篇至第 9 篇則將監理架構區分為經濟管制、技術管制、消費者保護與社會管制，至於第 10 篇與第 11 篇則為總則與過渡規定[216]。

有關馬來西亞網站封鎖之法源，則規範於 CMA 總則篇之第 233 條「不當使用網路設施或網路服務等」，其規範內容為：「（1）（a）利用任何網路設施、網路服務或應用程式服務，製造、創造或收集並發起傳播任何猥褻、不雅、虛假、威嚇或意圖滋擾、虐待、威脅、騷擾之評論、要求、建議或其他通訊內容，屬於犯罪（（1）A person who—（a）by means of any network facilities or network service or applications service knowingly —（i）makes, creates or solicits; and（ii）initiates the transmission of, any comment, request, suggestion or other communication which is obscene, indecent, false, menacing or offensive in character with intent to annoy, abuse,

[214] About us-History, MCMC, https://www.mcmc.gov.my/en/about-us/history (last visited: Jun. 30, 2021).
[215] *Id.*
[216] 公務出國報告，出席馬來西亞通訊傳播暨多媒體委員會雙邊交流會議及參訪相關機構，國家通訊傳播委員會，頁 9（104 年 2 月 11 日）。

threaten or harass another person; commits an offence.)。」[217]，此外，「(2)（a）若基於商業目的透過網路服務或應用程式服務提供任何猥褻內容，或（b）允許他人於自己之控制下透過網路服務或應用程式服務用於（a）段所述之活動，屬於犯罪（1）A person who knowingly — （a）by means of a network service or applications service provides any obscene communication for commercial purposes to any person; or （b） permits a network service or applications service under the person 's control to be used for an activity described in paragraph （a）, commits an offence.。」[218]，「(3)任何人犯第 233 條所訂之罪刑，可處最高五萬林吉特（馬幣）與/或一年以下有期徒刑((3） A person who commits an offence under this section shall, on conviction, be liable to a fine not exceeding fifty thousand ringgit or to imprisonment for a term not exceeding one year or to both and shall also be liable to a further fine of one thousand ringgit for every day during which the offence is continued after conviction.」[219]。

此外，CMA 第 263 條規範受許可業者之一般性義務（General duty of licensees):「(1)被許可人應當盡最大努力防止其擁有或者提供之網路設施或其所提供之網路服務、應用服務或內容應用服務用於或與馬來西亞任何法律規定之任何犯罪有關之行為（1） A licensee shall use his best endeavour to prevent the network facilities that he owns or provides or the network service, applications service or content applications service that he provides from being used in, or in relation to, the commission of any offence under any law of Malaysia.)。(2） 應委員會或任何其他主管機關的書面要求，被許可人應協助委員會或其他主管機關阻止根據馬來西亞任何成文法或其他實施之馬來西亞法規規定之犯罪之實施或試圖實施之行為，包括但不限於保護公共利益和維護國家安全((2） A licensee shall, upon written request by the Commission or any other authority, assist the

[217] Section 233 Improper use of network facilities or network service, etc., Communications and Multimedia Act 1998.
[218] *Id.*
[219] *Id.*

Commission or other authority as far as reasonably necessary in preventing the commission or attempted commission of an offence under any written law of Malaysia or otherwise in enforcing the laws of Malaysia, including, but not limited to, the protection of the public revenue and preservation of national security.)。」

因此，受 MCMC 許可之業者在 MCMC 或其他機構的書面要求下，必須在合理必要的範圍內協助 MCMC 或其他機構，防止任何於馬來西亞實施之成文法規定的犯罪或犯罪企圖[220]，亦即，受許可之網路服務提供者有義務阻止利用其所擁有或提供之網路服務、應用服務或與任何實施犯罪有關之行為[221]。而遭屏蔽之網站內容大致可歸納為以下幾個類型：

1. 侵害著作權：依馬來西亞 1987 年著作權法第 41 條，提供非法內容下載連結之網站（如 Pirate Bay）如經舉報或是主管機關調查後，將被屏蔽，而著作權侵害雖屬於馬來西亞國內貿易和消費者事務部的管轄範圍[222]，但就網站內容涉及違反著作權法之情形，著作權人亦得檢具相關資料以及已通知該網站之網路服務提供者之證明，向 MCMC 的消費申訴局（Consumer Complaints Bureau）提出申訴，MCMC 將有權依據著作權人之申訴做出網站屏蔽之行政處分，著作權人也可直接向高等法院聲請針對違反著作權法之網站進行屏蔽之裁定[223]。
2. 涉及賭博：線上賭博網站（如 betfair.com）將依馬來西亞 1953 年公共賭場法第 4（1）條遭到屏蔽[224]。
3. 冒犯性與不雅之內容：由於 CMA 第 233 條之條文內容如「淫穢、不雅、虛假、威脅或冒犯性」、「意圖惹惱、辱罵、威脅或騷擾他人」所

---

[220] Sharon Tan, Zaid Ibrahim and Co., Communications: regulation and outsourcing in Malaysia: overview, https://content.next.westlaw.com/Document/Ib97922b5830011e598dc8b09b4f043e0/View/FullText.html?transitionType=Default&contextData=(sc.Default) (last visited: Jun. 30, 2021).

[221] Site Blocking Global Best Practices, Michael Schlesinger, https://www.ipaj.org/bunkakai/content_management/event/pdfs/20180728/Schlesinger_20180728_2.pdf (last visited: Oct. 7, 2021).

[222] SinarProject, Laws cited for Internet Censorship in Malaysia, https://sinarproject.org/digital-rights/updates/laws-cited-for-internet-censorship-in-malaysia (last visited: Oct. 7, 2021).

[223] Luther, Blocking of Websites Which Contain Copyright Infringing Content in Various Asian Countries, https://www.luther-lawfirm.com/fileadmin/user_upload/WP_Handout_Blocking-of-websites_Asian-countries_V01_270120.pdf. (last visited: Oct. 7, 2021).

[224] *Supra* note 222.

涵蓋之範圍過於廣泛，也使第 233 條是常被 MCMC 引用並廣泛用於屏蔽包含色情（如 pornhub）[225]、政治批評言論（如 Medium.com、Malaysia Chronicle）[226]、新聞媒體（如 Sarawak Report）[227]、LGBT+網站（如 Gay Star News）[228]、宗教討論網站（如 Patheos）[229]、小說網站（如 FanFiction.net）[230]、交友網站（http://adultfriendfinder.com）[231]等。。

4. 違反伊斯蘭教法：依據馬來西亞的某些州伊斯蘭教法，違反伊斯蘭教法規範之法規將會被屏蔽，例如 Khilafah.net 即因違反雪蘭莪州 1995 年伊斯蘭教法罪行第 16 條（出版或傳播任何違反伊斯蘭教法的書籍、文件或錄音）而遭到 MCMC 以 CMA 第 263（2）條要求網站服務提供者屏蔽開網站。然而有論者認為引用州伊斯蘭教法之條文進行網路審查與屏蔽是有爭議的，因網站屏蔽之效果將擴及適用於來西亞任何州的所有馬來西亞人，包含非穆斯林在內。

圖 17 網站因違反雪蘭莪州 1995 年伊斯蘭教法而遭到屏蔽之畫面[232]

[225] OONI, The State of Internet Censorship in Malaysia, https://ooni.org/post/malaysia-report/ (last visited: Oct. 7, 2021).
[226] *Id.*
[227] *Id.*
[228] *Supra* note 222.
[229] *Id.*
[230] *Id.*
[231] *Id.*
[232] *Id.*

（二） 主管機關

馬來西亞通訊傳播暨多媒體委員會（MCMC）係依據通訊傳播馬來西亞通訊傳播暨多媒體委員會法設立，隸屬通訊傳播暨多媒體部（Ministry of Communications and Multimedia Malaysia）[233]，委員由部長任命，包含 1 名主任委員，3 名政府代表委員，2 至 5 名來自產業界之其他代表委員，委員會之人員共約有 700 多人[234]。

MCMC 主要之任務係依據通訊傳播暨多媒體法賦予之權力，對通訊傳播及多媒體產業進行監理，也促進通訊傳播及多媒體產業落實政府的國家政策目標、監理包括電信及廣播電視匯流產業以及建立網際網路活動之新監理架構。此外，隨著 2001 年郵政服務法之公布，MCMC 之監管範圍擴張至監理郵政服務產業，並依據 1997 年數位簽章法對認證中心（Certification Authorities）進行核照[235]。

MCMC 主要任務包含[236]：

1. 就有關通訊傳播及多媒體活動之國家政策目標的所有事務提供建議；
2. 落實及執行通訊傳播暨多媒體法之條款；
3. 監理所有未於通訊傳播暨多媒體法中敘明的與通訊傳播及多媒體活動有關之事務；
4. 考慮並提出對通訊傳播暨多媒體法的改革建議；
5. **監督及監測通訊傳播及多媒體活動；**
6. 鼓勵並促進通訊傳播及多媒體產業之發展；
7. 鼓勵並促進通訊傳播及多媒體產業之自律；
8. 促進及維持在通訊傳播及多媒體產業所有持照者或獲得授權之人的完整性；
9. 提供各種形式的協助，並促進涉及通訊傳播及多媒體活動的人員間

---

233 Legislation, MCMC, https://www.mcmc.gov.my/en/legal/acts （last visited 30 June 2021）.
234 同註 216，頁 7。
235 *Supra* note 233.
236 Our Responsibility, MCMC, https://www.mcmc.gov.my/en/about-us/our-responsibility (last visited Jun. 30, 2021).

的協調合作；

10. 落實公報中部長所指定的任何成文法中的任何功能。

MCMC 之監理角色包含[237]：

1. 經濟管制(Economic regulation)—包含促進競爭及禁止反競爭行為，以及發展和執行接取規範及相關標準。也包括核發執照、執行網路及應用提供者的執照許可條件、確保規則的遵守及效能/服務品質。
2. 技術管制（Technical regulation）—包含有效的頻率頻譜指配、發展和執行技術規範及相關標準，以及管理編碼（numbering）及電子定址（electronic addressing）。
3. 消費者保護（Consumer protection）—強調消費者的賦權，同時確保在爭議解決、服務的可負擔性及可得性等領域有足夠的保護措施。
4. 社會管制（Social regulation）—包含一體兩面的內容發展及內容管制，後者包括禁止攻擊性內容及內容相關議題的公共教育。
5. 郵政管制（Postal regulation）—包含維護郵政服務的提供及促進郵政及快遞市場的競爭。
6. 認證中心管制(Certification Authority regulation)—包含藉由核照及審計機制管控認證中心的營運，以確保其可信賴度。

（三） 認定機構（認定違法）

依據 CMA，MCMC 有權依 CMA 之規範內容實施保護措施以保護消費者，包含透過阻止造訪有害且違反規定之網站。其中色情網站遭封鎖之數量最多，2018 年共有 1,579 個網站。MCMC 表示其採取的措施符合針對網站封鎖之標準流程，且已通過 ISO 9001：2015 認證[238]，而其屏蔽所使用之技術主要為 DNS RPZ 之方式，攔截網路使用者訪問某些網址的請求，以達到屏蔽網站之效果[239]。

---

[237] *Id.*
[238] SHAPING THE DIGITAL LANDSCAPE ANNUAL REPORT, MCMC (2018), at 66, https://www.mcmc.gov.my/skmmgovmy/media/General/pdf/MCMC-2018_ENG.pdf.
[239] *Supra* note 225.

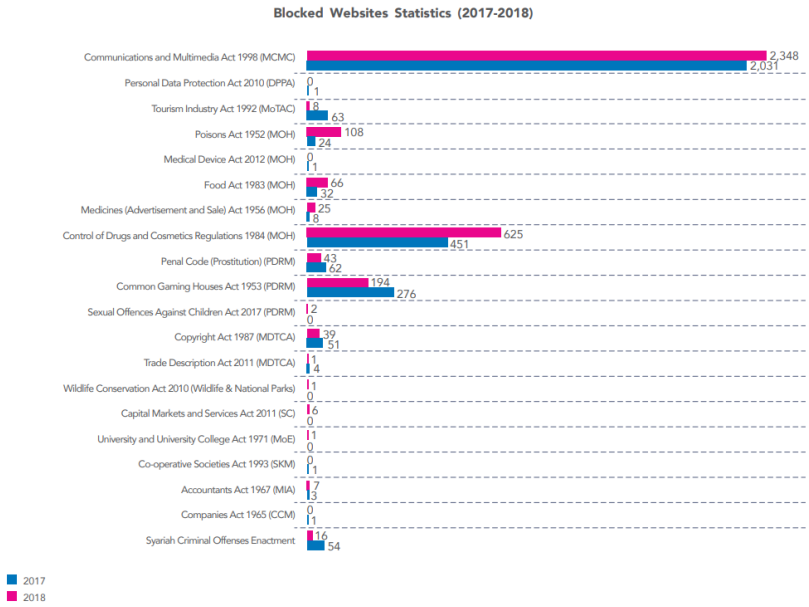


圖 18 MCMC 針對網站封鎖之統計數據（2017-2018）

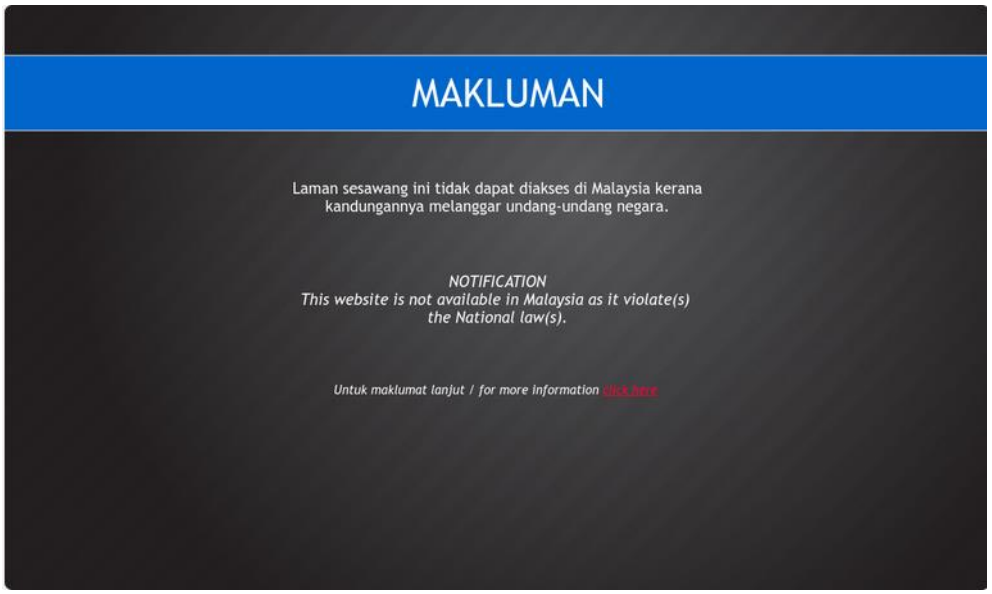


圖 19 網站遭 MCMC 屏蔽之頁面

（四） 境外網域名稱之封鎖

馬來西亞屏蔽境外網域名稱最著名的例子，是於 2015 年時，國外網路媒體報導有關當時首相 Najib 之政權腐敗與批評等相關新聞之事件，在英國調查網站 Sarawak Report[240]發表關於 1Malaysia Development Berhad（1MDB）國家投資基金資源分配不當的文章後，MCMC 命令網路服務提供商屏蔽 Sarawak Report 之網站，部落客平臺 Medium 也因拒絕撤下 Sarawak Report 之文章而遭到屏蔽。於 2016 年香港評論網站 Asia Sentinel 也因發表一篇批評首相 Najib 的文章而被 MCMC 認為「違反國家法律」而遭到屏蔽[241]。雖然 MCMC 以國家安全為由屏蔽上述網站，係根據 CMA 第 233 條之規定，惟有論者認為上述的審查活動不排除是出於政治動機[242]。

（五） 救濟

根據 CMA 的幾種機制，受 MCMC 決定影響的人有權發表意見或提供書面意見，對委員會的決定不服者可以向部長設立的上訴法庭（Appeal Tribunal）提出上訴，以審查作出決定的案情和程序。上訴法庭為臨時召集的，以審查由委員會決定（decision）或指示（direction）的事項，但由委員會裁定（determination）的事項或由部長確定為不得上訴的事項除外。上訴法庭的決定屬終局且具有約束力的決定，不能再提出上訴。

此外，CMA 還規定對部長或委員會的一項決定或其他行動進行司法審查，前提是受該決定或其他行動影響的人已經用盡了 CMA 規定的所有其他補救措施[243]。

（六） 相關案例與評論

從 2018 年 9 月到去年，馬來西亞通訊與多媒體委員會（MCMC）封

---

[240] Sarawak Report, https://www.sarawakreport.org/search/?q=1Malaysia+Development+Berhad+%281MDB%29&lang=en&page=4 (last visited: Oct. 7, 2021).
[241] Freedom House, https://freedomhouse.org/country/malaysia/freedom-net/2019 (last visited: Oct. 7, 2021).
[242] *Supra* note 225.
[243] *Supra note* 168.

鎖了 2,921 個色情網站，以保護該國的本地互聯網用戶[244]，且阻止色情網站訪問的行動仍在積極進行。此外，MCMC 也持續屏蔽涉及盜版、詐騙甚至 LGBT+等網站。在 2008 年至 2017 年間 MCMC 屏蔽了 10,962 個被發現參與網絡欺詐的網站，而為了因應「假新聞」的盛行，MCMC 表示 2016 年和 2017 年有 1,375 個網站因「虛假內容」而被屏蔽[245]。

然而，因 CMA 第 233 條條文規範內容過於廣泛，使得網站內容審查容易流於恣意且不明確，只要有民眾向 MCMC 檢舉或投訴，即有可能因網站內容被 MCMC 認定違反 CMA 第 233 條而遭到屏蔽，此外，亦有論者認為，CMA 第 233 條與第 263 條之規範，容易被執政者濫用以限制少數族群或社群之言論自由或政治批評，而有修法或調整之必要[246]。

（七） 致 MCMC 信件

經研究團隊查詢之結果，目前並無公開資訊公布馬來西亞網域濫用處理之案例，為進一步蒐集瞭解「馬來西亞案例」，本研究已為 貴局發信詢問 MCMC，以充實研究結果。本信件於 110 年 6 月 4 日寄出，茲就本信件函詢 MCMC 之問題及翻譯如下：

Dear Sirs/Madams, 敬啟者： By way of introduction, our firm, Lin and Partners, Attorneys-at-Law, is the government's National Communications Commission （the central government authority responsible for regulating telecommunications and broadcasting services in Taiwan; "NCC"） legal counsel in a regulatory/policy shaping project concerning "Resolution of Domain Name Abuse". 本所為恆業法律事務所，受臺灣之國家通訊傳播委員會（負責監管臺灣電信與廣播業務之中央主管機關，簡稱 NCC）之委託作為法律顧問，辦理有關網域名稱涉有違反相關法律之監管政策之專案研究。

[244] MAHAIZURA ABD MALIK, MCMC: Almost 3,000 pornographic sites blocked since Sept 2018, New Straits time, https://www.nst.com.my/news/crime-courts/2021/01/660369/mcmc-almost-3000-pornographic-sites-blocked-sept-2018 （last visited: Oct. 7, 2021）.

[245] *Supra* note 241.

[246] *Supra* note 222.

It is our understanding that your esteemed Malaysian Communications and Multimedia Commission （"**MCMC**"） is the main official unit in Malaysia committed towards regulations on the field of communication and multimedia.
據本所瞭解，貴單位──馬來西亞通信與多媒體委員會（MCMC）為馬來西亞負責監管通信與多媒體領域之主要政府單位。

Due to recent enacted law, we are currently gathering information on the different mechanisms for the governance on the content abuse of the DNS. Therefore, we write to seek your kind assistance in clarifying our below enquiries regarding Malaysia's site blocking regime under Communications and Multimedia Act 1998.
鑒於臺灣不久前已頒布電信管理之新法，本所正協助蒐集有關網域名稱內容濫用之不同監管機制。因此，本所特以此封信件就以下有關馬來西亞於 1998 年通訊傳播與多媒體法下之網站封鎖制度尋求 貴局之協助與釋疑。

Background 背景介紹

Due to the recent aggravation of the DNS abuse, we have conducted research and compared national governance on the DNS abuse regulatory regimes of selected countries, including Malaysia, for us to assess and develop Taiwan's DNS governance mechanism.
由於近來網域名稱濫用之情形加劇，本所特別針對包含馬來西亞在內之幾個選定國家進行監管法制之研究與比較，以評估與發展臺灣之網域名稱監理機制。

Question 1: Procedures for MCMC to implement site-blocking measures on particular domain name
問題 1：MCMC 針對特定網域名稱實施網站封鎖措施之流程

We note from Communications and Multimedia Act（"CMA"）that MCMC has the authority to decide on implementing the site-blocking measures on the particular domain name with content abuse.
依本所瞭解，依據通訊傳播與多媒體法 MCMC 有權針對內容涉及違法之特定網域名稱實施網站封鎖措施。

Could you please assist in explaining the overall procedures for such implementation including （i） how MCMC detects and investigates on the suspected violation by a website, （ii） what's the standards for determining the content in such website is in violation of Article 233 of the CMA, and （iii） what occasions and how often MCMC would invoke Article 263 of the CMA requesting the licensee in assisting in the implementation of the site blocking?
可否請 貴會協助說明實施該等措施之完整流程，包含（i） 貴會如何探知與調查網站涉嫌違法之情事，（ii）判定該網站之內容涉及違反通訊傳播與多媒體法第 233 條之認定標準為何，以及（iii）MCMC 會在何種情形與多久會援引通訊傳播與多媒體法第 263 條，要求受許可之網路服務提供者協助實施網站封鎖？

Question 2: Remedy mechanism for the site-blocked to appeal against MCMC's decision
問題 2：網站受封鎖之受處分人針對 MCMC 之決定之救濟措施

We note from the CMA that an ad hoc Appeal Tribunal may be established for reviewing the decision or direction of the MCMC but not a determination by the MCMC. Could you please kindly explain that whether the site-blocking implementation of MCMC is categorized as a "decision"/"direction" or "determination" under CMA?
依本所瞭解，依據通訊傳播與多媒體法，臨時性上訴審裁小組可以依情況設立並審查 MCMC 的決定（decision）或指導（direction），但不包含 MCMC 的判定（determination）。可否請 貴會協助說明 MCMC 的網站封鎖措施是屬於通訊傳播與多媒體法下之決定（decision）或指導（direction），或是屬於判定（determination）？

In addition, could you please also kindly explain on the complete remedy mechanism for the site-blocked to seek against MCMC's site-blocking decision, including the administrative appeal mechanism under MCMC and/or judicial review by seeking relief from the court?
另外，可否請 貴會說明網站受封鎖者針對 MCMC 網站封鎖決定之完整救濟機制，包含 MCMC 下之行政上訴救濟機制和/或透過向法院尋求救濟之司法審查？

Question 3: Specific cases and materials
問題 3：相關案例與資料

Would it be possible for MCMC to provide access to any available cases, materials or database of DNS content abuse or the practice of site-blocking for our reference to enhance our research and analysis on Malaysia Site-Blocking mechanism?
可否請 貴會提供有關 DNS 內容濫用或網站封鎖實施情形之任何案例、資料或資料庫，以完善我們對馬來西亞網站封鎖制度之研究？

We acknowledge that perhaps the above questions may not be briefly explained or answered and would be grateful if you could provide guidance as to other available online resources which may further clarify our queries.
我們承認上述所詢之問題可能無法獲得簡要之解釋或回覆，若 貴會能提供有關其他可獲得之線上資源以進一步釐清我們之疑問，我們將不勝感激。

Thank you very much for your time and kind assistance in this matter. Please let us know if you have any questions or comments to the above, or if there is anything that we can be to your assistance.
非常感謝 貴會於此次來函所詢之事項所花費之時間與協助。如果 貴會對上述內容有任何疑問或意見，或有任何我們可以提供幫助之處，歡迎不吝賜知。

Thank you and we look forward to hearing back from you soon.
謝謝，期待很快收到 貴會之回覆。

Yours sincerely,
林上倫律師 Shang-Lun Lin
恆業法律事務所 Lin & Partners Attorneys-at-Law

第四項　英國

（一） 1988年英國著作權、設計和專利法：法院禁制令解決相關往域濫用行為

在英國，在著作權侵權訴訟中法院得核發禁制令命令侵權行為人排除侵害，即命令侵權行為人將侵權內容從網路上下架，此外，著作權人可以依據 1988 年英國著作權、設計和專利法第 97A 條向英國法院申請禁制令，在「網路服務提供者（ISP）實際上知悉他人利用其提供之網路服務進行侵權行為」（where that service provider has actual knowledge of another person using their service to infringe copyright）時，要求網路服務提供者 ISP 進行網域名稱阻擋。在認定 ISP 是否實際上知悉時，法院應考慮在特定情況下它認為相關的所有事項，包含網路服務提供者是否已通過根據《2002 年電子商務（EC 指令）條例》（SI 2002/2013）第 6（1）（c）條提供的聯繫方式收到通知，以及該通知已有記載寄出通知者的全名和地址，與有關侵權的詳細資訊。

於 2010 年 12 月美國電影協會（MPA）應 6 家好萊塢電影製片廠的要求，依 1988 年英國著作權、設計和專利法第 97A 條向法院申請阻擋進入涉及侵權之網站 Newzbin2，並成功使法院核發禁制令屏蔽 Newzbin2。

Newzbin2 是一個僅限會員的網站，整理了大量非法複製材料的連結，包括在 Usenet 討論論壇上找到的電影、音樂和電腦遊戲。嗣後，MPA 亦成功贏得了類似的法院禁制令，例如 2011 年 7 月，高等法院向 BT（英國最大互聯網服務提供商）核發禁制令，2011 年 10 月 BT 被命令在 14 天內屏蔽並阻止訪問 Newzbin2，BT 沒有對禁制令提出上訴，並於 2011 年 11 月 2 日實施屏蔽措施，此外，法院亦向天空英國有限公司 Sky 核發禁制令，要求其實施措施阻止其客戶訪問 Newzbin2，Sky 的相關措施也於

2011 年 12 月完成。2012 年 11 月 28 日，Newzbin 宣布關閉其索引服務[247]。

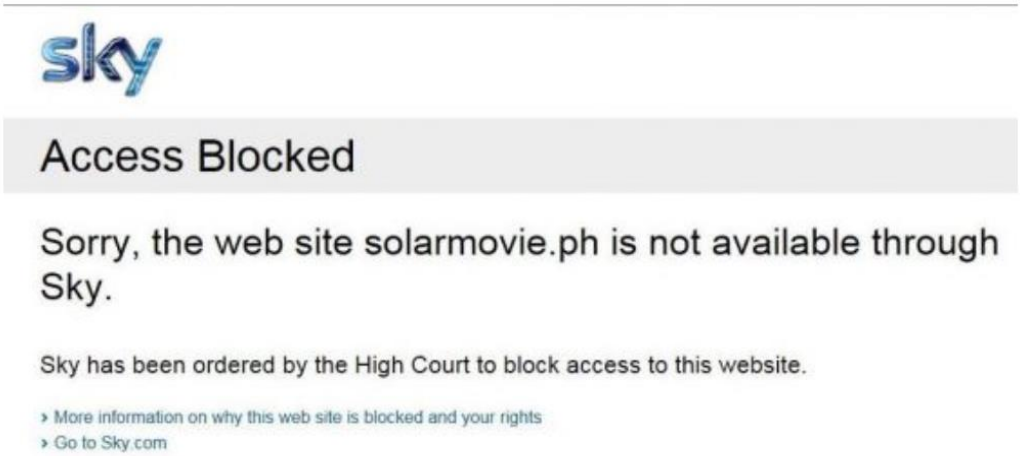


圖 20 英國 ISP 業者 Sky 屏蔽網站之頁面[248]

隨後，2012 年 5 月英國音樂產業跟隨 MPA 的腳步，獲得了高等法院的禁制令裁決，下令多家 ISP 即 Sky、Everything Everywhere、TalkTalk、O2 和 Virgin Media 封鎖海盜灣 The Pirate Bay 網站。海盜灣使用戶能夠搜索和下載受著作權保護的內容，包括音樂和電影。EMI、Sony、Polydor 和其他主要唱片公司，代表英國唱片業協會（BPI）及其所有成員的貿易機構，主張該網站侵犯了他們的著作權，高等法院在該案中也根據英國著作權、設計和專利法第 97A 條發布了禁制令[249]。

表 9 法院禁制令統整[250]

電影公司（film studios）	
1.	2011年10月26日有關Newzbin2的法院禁制令（20C Fox v BT and 20C Fox v BT （No 2））

247 https://www.pinsentmasons.com/out-law/analysis/newzbin2-ruling-sets-precedent-for-online-copyright-infringement (last visited: Oct. 11, 2021).
248 https://www.wiggin.co.uk/insight/site-blocking-an-introduction-and-legal-background/ (last visited: Oct. 11, 2021).
249 https://www.pinsentmasons.com/out-law/news/website-blocking-provisions-to-be-removed-from-digital-economy-act-says-government- (last visited: Oct. 11, 2021).
250 http://www.bailii.org/ew/cases/EWHC/Ch/2003/3354.html (last visited: Oct. 11, 2021).

2.	2013年4月24日有關Movie2K 與 DL4all 的法院禁制令，以及針對Movie2K 改名成Movie 4K 後法院另於2013年7月17日下的禁制令
3	2013年7月1日有關EZTV之法院禁制令
4	2013年10月25日有關YIFY-Torrents 與其他四個網站之3個法院禁制令
5	2013年11月13日有關SolarMovie and Tube+之法院禁制令（Paramount v Sky）
6	2014年2月18日有關Viooz 與其他3個網站之法院禁制令（Paramount v Sky 2）
唱片公司（record companies）	
1	2012年6月13日有關The Pirate Bay（"TPB"）的法院禁制令（Dramatico v Sky and Dramatico v Sky （No 2））
2	2013年2月28日有關Fenopy, H33T and Kat 的法院禁制令 （EMI v Sky）
3	2013年10月8日有關1337X 與其他20個網站的法院禁制令
英國蘭足球超級聯賽（FA Premier League）	
1	2013年7月16日有關FirstRow Sports的法院禁制令 （FAPL v Sky）

此外，著作權人雖可以根據《著作權、設計和專利法》第 97A 條向英國法院申請網站屏蔽，但英國的《商標法》中沒有類似的規定。然而於 2014 年 10 月，高等法院依據歷峰（Richemont）、卡地亞國際（Cartier International）和萬寶龍（Montblanc）之申請[251]，核准向英國主要 ISPs（包含 Sky, BT, EE, TalkTalk and Virgin 發出了針對商標侵權消費品的第一項禁制令，以封鎖六個網域名稱[252]（申請時為七個，其中有一個網域名稱 www.hotcartierwatch.com 已自行撤下）：www.cartierloveonline.com、www.iwcwatchtop.com、www.replicawatchesiwc.co、www.1iwc.com、www.montblancpensonlineuk.com 及 www.ukmontblancoutlet.co.uk.

（二） 2010年數位經濟法第17條、18條（已廢止）

為符合數位時代需求，且考量實務上判斷 ISP 是否實際上知悉著作

[251] https://achristie.com/uk-court-extends-isp-site-blocking-remedy-to-online-trademark-infringement/ (last visited: Oct. 11, 2021).
[252] *Supra* note 250.

權人申請所載之侵權行為之判斷標準仍不清楚，法院之審理程序緩不濟急，使得著作權人之權益無法獲得即時之保障，著作權人在此法院禁制令程序耗費的成本幾乎等同於提起一個侵權行為訴訟，故英國政府於 2010 年 4 月 8 日通過、6 月 8 日施行的數位經濟法案（Digital Economy Bill）中建構了一個新的網站封鎖禁令的框架，由英國國家通訊管理局（Office of Communications, Ofcom）負責處理網路著作權侵害問題（Online infringement of copyright），採取二階段實施方式課予網路服務提供者保護著作權義務。第一階段初始義務（Initial Obligations），ISP 就著作權人提出之侵權通報（Copyright infringement Report），依法負有轉送通知給使用者之義務，以及依照著作權人要求之期間提出侵害列表的義務。第二階段技術義務（Technical Obligation），待第一階段之措施無法有效降低網路著作權侵害問題時，課予 ISP 採取特定技術措施的義務，例如流量限制、斷線等[253]。

數位經濟法第 17 條和第 18 條規定的相關條款適用上比依據英國著作權、設計和專利法第 97A 條所含括的範圍更廣。例如，根據英國著作權法第 97A 條，ISP 必須實際知道他人使用他們的服務侵犯著作權，然而在數位經濟法下，ISP 是否實際知悉不是相關考慮因素，重要的反而是該網站是否「已經、正在或可能被用於或與侵犯著作權的活動有關」[254]。

儘管如此，於數位經濟法實施後，數位文化傳媒和體育部（Department for Digital, Culture, Media and Sport，DCMS）於 2011 年 2 月要求 Ofcom 審查數位經濟法第 17 和 18 節在技術上是否可行，Ofcom 2011 年五月的報告中發現，數位經濟法第 17 條和第 18 條無法預測、成本低且速度不夠快，基於此報告之結論，以及 2011 年 7 月法院第一次依 1988 年著作權、設計和專利法核發禁制令（即前述所提及的 Newzbin2 案），DCMS 乃於 2011 年 8 月 3 日宣布刪除第 17 條和第 18 條，並認為 1988 年著作權、

[253] 經濟部智慧財產局委託研究案「英國著作權法令暨判決之研究」期末報告，頁 12（2021 年 12 月 7 日）。

[254] Ofcom, “Site Blocking” to reduce online copyright infringement; https://www.openrightsgroup.org/publications/copyright-and-web-blocking-in-the-uk/ (last visited: Oct. 11, 2021).

設計和專利法已成功用於阻止以侵犯著作權為由訪問網站[255]。

（三） 2017年數位經濟法（2017 Digital Economy Act）解決情色網域名稱濫用問題

英國復於 2017 年 4 月 27 日通過數位經濟法的修正案，納入 ISP 應過濾並阻擋年齡驗證不充分的色情網站之要求。依數位經濟法第 13 條有關防止未滿 18 歲之青少年訪問色情網站之規定，若 ISP 業者在網站上以商業方式（on a commercial basis）向英國境內之人提供色情素材，則應設置相關措施以避免未滿 18 之人得以隨時或任意造訪該提供色情素材之網站[256]。就一般常見的作法而言，色情網站的首頁會跳出只有年滿 18 歲才能存取的警告視窗，但使用者只要簡單地宣稱自己已滿 18 歲就能進入。然而依據數位經濟法之規定，不論是免費或付費的色情網站，都必須在網站上嵌入年紀驗證機制，強迫造訪者提供信用卡上的詳細資訊，得先證明這些使用者已年滿 18 歲才得以訪問網站[257]。

有關色情網站涉及兒童色情和淫穢之內容，在英國係違反 1978 年的兒童保護法（The Protection of Children Act 1978），依兒童保護法之規定，對於製造、散布及展示 18 歲以下的人的不雅照片，最高處 10 年以下有期徒刑。然而，**在英國，網路上兒童色情與淫穢內容之監管主要是仰賴 ISP 業者的自我監控，由非營利機構──互聯網觀察基金會（IWF）負責協調**。IWF 係由英國通信服務提供商（包括 ISP、移動電話運營商、互聯網貿易協會、搜索引擎、硬體製造商和軟體提供商）自願捐款資助成立，其任務係透過搜索與爬蟲技術，在網絡中識別兒童性虐待或兒童色情等圖像與影片，或透過全國熱線舉報服務受理民眾之舉報，若已識別網站上之內容為兒童性虐待或色情之素材，**IWF 會追蹤其網站之註冊地區，若**

255 “Website blocking provisions to be removed from Digital Economy Act, says Government”, Pinsent Masons, https://www.pinsentmasons.com/out-law/news/website-blocking-provisions-to-be-removed-from-digital-economy-act-says-government- (last visited: Oct. 11, 2021).
256 Section 14(1), 2017 Digital Economy Act.
257 英國政府通過數位經濟法案，色情網站須強制驗證造訪者年齡、嚴禁機器人搶票，https://www.ithome.com.tw/news/115639 （最後瀏覽日：2021 年 10 月 16 日）。

該註冊地區在英國，則 IWF 會直接向該註冊者發出通知要求刪除該圖像或影像，若註冊地區在國外，則 IWF 會聯繫並與該國之警察網絡合作以該國之法制或流程刪除。

由於 IWF 發現之兒童色情圖片或影像大多是英國境外網站提供之內容，因此 IWF 除依上述流程要求刪除兒童色情內容以外，也會將網站網址放在其彙整之 URL 列表中，供其合作之 ISP 業者依其定期更新之 URL 列表阻止英國民眾訪問相關違法網站[258]。

（四） 2021年網路安全法案（Online Safety Bill）解決網路危害內容問題

英國數位文化傳媒和體育部於 2019 年提出網絡危害白皮書，建議政府應就網路危害內容提高監理措施，英國國會遂於 2021 年 5 月 21 日提出「網路安全法案」，課予平臺業者或搜尋引擎審查並移除網路上違法、或者合法但有害內容（以下簡稱危害內容）之義務，並提高主管機關，即 Ofcom 對於網路業者之監督權限[259]。

網路安全法案將網路服務分為「使用者對使用者服務」（user-to-user service）以及「搜尋服務」（search service），「使用者對使用者服務」係指提供使用者製造、上傳或分享內容，並給其他使用者觀覽之服務，例如臉書、Youtube 等網站服務。網路安全法案分為三大類：「1 類服務」、「2A 類服務「2B 類服務」依照網站內容數量，以及危害內容傳播風險加以區別，「1 類服務」例如臉書、推特等全球性社群網站，法案對其監理密度較高；「2B 類服務」則為其他網路服務，例如購物網站、通訊軟體、約會網站等。以上兩類服務分別被課予不同程度之義務，其中 1 類服務等社群龍頭受到的監理密度最高[260]。至於「2A 類服務」則指 Google、Bing 等

[258] URL List, Internet Watch Foundation, https://www.iwf.org.uk/become-a-member/services-for-members/url-list (last visited: Oct. 17, 2021).
[259] Draft Online Safety Bill, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/985033/Draft_Online_Safety_Bill_Bookmarked.pdf
[260] 英國推出《網路安全法》草案，聚焦網路危害內容管理，財團法人電信技術中心，https://www.ttc.org.tw/News/more?id=d3602a80892c4c2999eec94c668ad76d （最後瀏覽日：2021 年 11 月 30 日）。

搜尋引擎或非其他非使用者對使用者之服務。

網路安全法案下，「2A 類服務」及「2B 類服務」應向 Ofcom 登記，並每年應繳交透明度報告，並評估危害之內容、處理有害兒少身心之內容，並落實言論自由保障；至於較受矚目之「1 類服務」監理措施，除以上規至措施之外，法案另外要求服務業者須將有害內容訂立明確標準，並且採取具體措施將危害之內容移除，有害內容例如色情、仇恨言論、鼓勵自殘等。

另外法案規定服務業者應對言論自由採取明確保障措施，尤其針對具有民主重要性之內容（content of democratic importance）有保護義務，例如關於選舉、公投等宣傳或者反對政府政策或政黨之言論，應當予以尊重，並一視同仁對待，不得歧視特定觀點或立場之政治言論。網站並應訂立對於政治性言論的具體條款及政策，並平等落實，例如某政黨以暴力陳抗內容上傳社群網站，雖然暴力內容可能違反群規約，惟該內容若具民主社會辯論之重要性者，網站依照其對政治言論之條款及政策可將該等內容保留[261]。另外法案要求服務業者應具體保障用戶言論自由，倘若用戶發表內容遭到不公平地刪除，嚴重違反言論自由或隱私權時，用戶可直接向 Ofcom 申訴[262]。

在該法案下，若 Ofcom 認為合理適當時，服務業者得使用經認可之技術，直接將特定危害內容迅速刪除。若 Ofcom 認為服務業者未將危害內容刪除，危害內容長期且普遍地存在於網路上時，Ofcom 得對服務業者發布技術警告通知（technology warning notice），或對業者處以 1800 萬英鎊或業者全球年收入的 10%之罰鍰。另外 Ofcom 得向法院申請服務限制令（service restriction order），命令線上金流、廣告之輔助服務（ancillary service）不得再向違法之服務業者提供輔助服務。更甚者，Ofcom 可向法院申請「接取限制令」（access restriction order），限制英國境內使用者接

[261] Landmark laws to keep children safe, stop racial hate and protect democracy online published, Gov.UK(May 12, 2021), https://www.gov.uk/government/news/landmark-laws-to-keep-children-safe-stop-racial-hate-and-protect-democracy-online-published

[262] *Id*。

取該網站服務，使的該網站無法再向英國境內提供服務[263]。

綜上，網路安全法案雖然賦予 Ofcom 幾個新的監管手段，但是整體立法思維乃提高業者自律，尤其是針對全球社群龍頭等網站而言，法案要求社群網站事先訂立明確政策，並清楚說明尊重言論自由之前提下，社群網站對於危害內容應如何處置。網路安全法案目前尚在由上議院及下議院組成之審查委員會進行立法前審議，預計於 2021 年 12 月 10 日提出審查報告[264]。目前對於該法案抱持較為保留態度者認為，社群網站對於如何判定何謂違法內容，例如兒童性虐待影像，固然有較為明確之標準，但是「合法但有害之內容」是棘手之問題，例如網路霸凌言論、假消息，該等內容雖然未必違反任何法規，但是對於網路言論環境具有腐蝕性及破壞性，故社群網站理應對於「合法但有害之內容」作出管制，但是如何認定「有害」因為審查標準不清，有論者認為恐讓社群網站自我審查壓力過大，並讓用戶產生寒蟬效應[265]。不過，有鑑於網路內容生成量之大，比起由主管機關監理，交由最具有資源及技術之業者保護網路言論環境，本為合理且最具效率之模式，故也有建議認為，該法案應當配合網際網路發展而定期更新，且立法者僅規定監理網路內容環境之框架，其餘應交由業者及網路公民自主地維護健全之言論環境[266]。

第三節　我國立法例之研析

第一項　我國與網域名稱濫用相關之立法例

（一）盤點網際網路內容或使用者行為之違法態樣及相關法律責任

經本研究團隊研析，盤點現行法規可用於規範網際網路內容或使用者行為違法態樣之規定及法律責任如下：

---

[263] 同註 260。

[264] What is the Online Safety Bill and why are some people worried about it? Alexander Martin (Oct. 19, 2021), https://news.sky.com/story/what-is-the-online-safety-bill-and-why-are-some-people-worried-about-it-12437427

[265] *Id*.

[266] What the Online Safety Bill means for social media, Sarah Dawood (Nov. 22, 2021), https://www.newstatesman.com/spotlight/cyber/2021/11/online-safety-bill-social-media

表 10 網際網路內容或使用者違法態樣表

不法行為	相關案例	法律責任
刑罰		
發表警告、恐嚇、威脅之言論並要求特定對象行無義務之事	**臺灣苗栗地方法院 108 年度易字第 847 號判決**	**刑法 304 條強制罪：** 以強暴、脅迫使人行無義務之事或妨害人行使權利者，處三年以下有期徒刑、拘役或三百元以下罰金。
發表警告、威脅欲對特定對象不利之言論	**臺灣苗栗地方法院 108 年度易字第 847 號判決**	**刑法 305 條恐嚇危安罪：** 以加害生命、身體、自由、名譽、財產之事，恐嚇他人致生危害於安全者，處二年以下有期徒刑、拘役或三百元以下罰金。
	臺灣高等法院高雄分院 90 年上易字 1580 號刑事判決	**刑法 346 條恐嚇取財罪：** 意圖為自己或第三人不法之所有，以恐嚇使人將本人或第三人之物交付者，處六月以上五年以下有期徒刑，得併科一千元以下罰金。 以前項方法得財產上不法之利益，或使第三人得之者，亦同。
發表或散播批評、誹謗、不實的言論	**臺灣高等法院 105 年度上易字第 1164 號判決**	**刑法 309 條公然侮辱罪：** 公然侮辱人者，處拘役或三百元以下罰金。 **刑法 310 條誹謗罪：** 意圖散布於眾，而指摘或傳述足以毀損他人名譽之事者，為誹謗罪，處一年以下有期徒刑、拘役或五百元以下罰金。 散布文字、圖畫犯前項之罪者，處二年以下有期徒刑、拘役或一千元以下罰金。 對於所誹謗之事，能證明其為真實者，不罰。但涉於私德而與公共利益無關者，不在此限。
使用者製造/散佈電腦病毒，造成他人電磁檔案毀損	**臺灣高等法院 95 年度上訴字第 3830 號判決**	**刑法 360 條** 無故以電腦程式或其他電磁方式干擾他人電腦或其相關設備，致生損害於公眾或他人者，處三年以下有期徒刑、拘役或科或併科三十萬元以下

不法行為	相關案例	法律責任
		罰金。 **刑法 362 條** 製作專供犯本章之罪之電腦程式，而供自己或他人犯本章之罪，致生損害於公眾或他人者，處五年以下有期徒刑、拘役或科或併科六十萬元以下罰金。
公布他人個資，包含人肉搜索等個資侵害個人隱私與資訊	**臺灣臺北地方法院 108 年度訴字第 878 號判決**	**個人資料保護法第 41 條：** 意圖為自己或第三人不法之利益或損害他人之利益，而違反第六條第一項、第十五條、第十六條、第十九條、第二十條第一項規定，或中央目的事業主管機關依第二十一條限制國際傳輸之命令或處分，足生損害於他人者，處五年以下有期徒刑，得併科新臺幣一百萬元 以下罰金。
散布假消息侮辱公務員或公署者	**臺灣高等法院 104 年度上易字第 1326 號判決**	**刑法第 140 條侮辱公署罪：** 於公務員依法執行職務時，當場侮辱或對於其依法執行之職務公然侮辱者，處六月以下有期徒刑、拘役或三千元以下罰金。 對於公署公然侮辱者，亦同。
意圖哄抬物價而囤積民生用品並造謠	**臺灣士林地方法院 110 年度訴字第 183 號判決**	**刑法第 251 條**：「意圖抬高交易價格，囤積下列物品之一，無正當理由不應市銷售者，處三年以下有期徒刑、拘役或科或併科三十萬元以下罰金…。（第一項） 意圖影響第一項物品之交易價格，而散布不實資訊者，處二年以下有期徒 刑、拘役或科或併科二十萬元以下罰金。（第三項） 以廣播電視、電子通訊、網際網路或其他傳播工具犯前項之罪者，得加重其刑至二分之一。（第四項）」
其他特別刑法定有散布不實	**臺灣桃園地方法院 110 年度壢簡字第**	**傳染病防治法第 63 條散布或傳播不實疫情消息罪；**

不法行為	相關案例	法律責任
資訊	**667 號判決** **臺灣高等法院 108 年度金上重更一字第 7 號判決**	**證券交易法第 155 條第 1 項第 6 款、第 171 條第 1 項及第 2 項意圖影響有價證券交易價格而散布流言或不實資料罪；**
境外敵對勢力之滲透干預，危害國家安全及社會安定之滲透行為	**法務部法律字第 10803509450 號要旨：** **法務部就調查局擬蒐集「國家機密人員名冊資料」具有正當性、必要性及合理關聯性等，涉及個人資料保護法等相關規定之說明。**	**反滲透法第 3 條** 任何人不得受滲透來源之指示、委託或資助，捐贈政治獻金，或捐贈經費供從事公民投票案之相關活動。 **反滲透法第 4 條** 任何人不得受滲透來源之指示、委託或資助，為總統副總統選舉罷免法第四十三條或公職人員選舉罷免法第四十五條各款行為。 **反滲透法第 5 條** 任何人不得受滲透來源之指示、委託或資助，進行遊說法第二條所定之遊說行為。
民事侵權		
發表或散播批評、誹謗、不實的言論侵害他人權利、名譽或其他人格權	**最高法院 109 年度台上字第 708 號民事判決**	**民法第 184 條第 1 項一般侵權行為：** 因故意或過失，不法侵害他人之權利者，負損害賠償責任。故意以背於善良風俗之方法，加損害於他人者亦同。 **民法 195 條第 1 項侵害人格權：** 不法侵害他人之身體、健康、名譽、自由、信用、隱私、貞操，或不法侵害其他人格法益而情節重大者，被害人雖非財產上之損害，亦得請求賠償相當之金額。其名譽被侵害者，並得請求回復名譽之適當處分。
在網站上張貼別人著作	**智慧財產法院 98 年度刑智上更（一）字第 48 號刑事判決**	**著作權法第 91 條** 擅自以重製之方法侵害他人之著作財產權者，處三年以下有期徒刑、拘役，或科或併科新臺幣七十五萬元以下罰金。 意圖銷售或出租而擅自以重製之方法侵害他人之著作財產權者，處六月以上五年以下有期徒

不法行為	相關案例	法律責任
		刑，得併科新臺幣二十萬元以上二百萬元以下罰金。 以重製於光碟之方法犯前項之罪者，處六月以上五年以下有期徒刑，得併科新臺幣五十萬元以上五百萬元以下罰金。 著作僅供個人參考或合理使用者，不構成著作權侵害。
搜尋服務提供者（即平臺業者）經著作權人或製版權人通知其使用者涉有侵權行為後，未移除、亦未使他人無法進入該涉有侵權之內容或相關資訊	**臺灣桃園地方法院 99 年度壢智簡字第 25 號刑事簡易判決**	**著作權法第 90-8 條** 有下列情形者，搜尋服務提供者對其使用者侵害他人著作權或製版權之行為，不負賠償責任： 一、對所搜尋或連結之資訊涉有侵權不知情。 二、未直接自使用者之侵權行為獲有財產上利益。 三、經著作權人或製版權人通知其使用者涉有侵權行為後，立即移除或使他人無法進入該涉有侵權之內容或相關資訊。
蒐集、盜用、公布他人個資	**臺灣士林地方法院 107 年度簡上字第 225 號民事判決**	**個人資料保護法 29 條：** 非公務機關違反本法規定，致個人資料遭不法蒐集、處理、利用或其他侵害當事人權利者，負損害賠償責任。但能證明其無故意或過失者，不在此限。
行政秩序罰		
發表或進行任何危害兒童及少年身心健全發展之不當言論或行為	**臺北高等行政法院 104 年度訴字第 1002 號判決**	**兒童及少年福利與權益保障法第 49 條第 2 款：** 任何人對於兒童與青少年不得有「身心虐待」之行為，違者依同法 97 條之規定，處新台幣六萬元以上三十萬元以下罰鍰，並公告其姓名。
侵害個人隱私資料之行政罰	-	**個人資料保護法第 47 條：** 非公務機關有下列情事之一者，由中央目的事業主管機關或直轄市、縣（市）政府處新臺幣五萬元以上五十萬元以下罰鍰，並令限期改正，屆期未改正者，按次處罰之：

不法行為	相關案例	法律責任
		一、違反第六條第一項規定。 二、違反第十九條規定。 三、違反第二十條第一項規定。 四、違反中央目的事業主管機關依第二十一條規定限制國際傳輸之命令或處分。
以不當言論遂行性騷擾	**臺灣臺北地方法院 105 年度簡字第 171 號行政訴訟判決**	**性騷擾防治法第 2 條第 2 款：** 本法所稱性騷擾，係指性侵害犯罪以外，對他人實施違反其意願而與性或性別有關之行為，且有下列情形之一者： 二、以展示或播送文字、圖畫、聲音、影像或其他物品之方式，或以歧視、侮辱之言行，或以他法，而有損害他人人格尊嚴，或造成使人心生畏怖、感受敵意或冒犯之情境，或不當影響其工作、教育、訓練、服務、計畫、活動或正常生活之進行。 **性騷擾防治法第 20 條：** 對他人為性騷擾者，由直轄市、縣（市）主管機關處新臺幣一萬元以上十萬元以下罰鍰。
意圖使人當選或不當選而散布不實資訊	**最高法院 106 年度台上字第 1158 號刑事判決**	**公職人員選舉罷免法第 104 條：** 意圖使候選人當選或不當選，或意圖使被罷免人罷免案通過或否決者，以文字、圖畫、錄音、錄影、演講或他法，散布謠言或傳播不實之事，足以生損害於公眾或他人者，處五年以下有期徒刑。
散布謠言，足以影響公共之安寧者	**臺灣臺北地方法院 108 年度北秩字第 624 號裁定**	**社會秩序維護法第 63 條第 1 項第 5 款：** 有左列各款行為之一者，處三日以下拘留或新臺幣三萬元以下罰鍰： 五、散佈謠言，足以影響公共之安寧者。
網域名稱內容監理性規定		
危害兒童及少年身心健全發	**最高行政法院 100 年度判字第 1520 號判**	**兒童及少年福利與權益保障法第 46 條** 為防止兒童及少年接觸有害其身心發展之網際

不法行為	相關案例	法律責任
展等網路安全之不當言論	**決**	網路內容，由通訊傳播主管機關召集各目的事業主管機關委託民間團體成立內容防護機構，並辦理下列事項...。 **兒童及少年福利與權益保障法第 46 條之 1：** 任何人不得於網際網路散布或傳送有害兒童及少年身心健康之內容，未採取明確可行之防護措施，或未配合網際網路平臺提供者之防護機制，使兒童及少年得以接取或瀏覽。 網際網路平臺提供者經目的事業主管機關告知網際網路內容有害兒童及少年身心健康或違反前項規定未採取明確可行防護措施者，**應為限制兒童及少年接取、瀏覽之措施，或先行移除。** **兒童及少年福利與權益保障法第 94 條：** 網際網路平臺提供者違反第四十六條第三項規定，未為限制兒童及少年接取、瀏覽之措施或先行移除者，由各目的事業主管機關處新臺幣六萬元以上三十萬元以下罰鍰，並命其限期改善，屆期未改善者，得按次處罰。 違反第四十六條之一之規定者，處新臺幣十萬元以上五十萬元以下罰鍰，並公布其姓名或名稱及命其限期改善；屆期未改善者，得按次處罰；情節嚴重者，並得勒令停業一個月以上一年以下。
未依輸出入動物檢疫機關之公告，發布「涉及境外應施檢疫物之販賣至國內」之網際網路內容	**臺灣臺北地方法院 110 年度簡字第 120 號判決**	**動物傳染病防治條例第 38 條之 3：** 網際網路內容涉及境外應施檢疫物之販賣至國內、輸入或其他檢疫相關事項，經輸出入動物檢疫機關公告者，其廣告刊登者、平臺提供者、應用服務提供者或電信事業，應依輸出入動物檢疫機關之公告，採取**「限制接取、瀏覽或移除相關網頁內容」之措施。**

第二項　我國有關「限制接取、瀏覽或移除相關網頁內容」之立法例

經研究團隊盤點我國所有可用於規範網際網路內容或使用者行為違法態樣之規定，僅有兒童及少年福利與權益保障法及動物傳染病防治條例有明

文授權該管行政機關將經其認定為違法之網站內容為限制接取、瀏覽，甚至是移除之措施。

兒童及少年福利與權益保障法第 46 條之 1：「任何人**不得於網際網路散布或傳送有害兒童及少年身心健康之內容**，未採取明確可行之防護措施，或未配合網際網路平臺提供者之防護機制，使兒童及少年得以接取或瀏覽。」，又有害兒童及少年身心健康之範圍從常見避免兒童接觸之情色內容，至賭博、歧視他人、仇恨言論、洩漏或揭漏他人的個人資料等涵蓋範圍廣，具體類型分為以下六大類：

一、情色

整個網站、網路文章或網路影片所呈現出的內容與傳遞的訊息，涉及男性女性的身體裸露、未成年的裸照、未成年遭受性剝削的內容、性行為、性暗示、媒介性交易的資訊或是具有性暗示意涵等內容。

二、暴力

整個網站、網路文章或網路影片所呈現出的內容與傳遞的訊息，涉及性侵害或性虐待他人、殺害或虐待人類/動物、自我傷害（例如直播自殺畫面、張貼割腕自殘的照片等）、或是暴力兇殘的畫面（例如幫派械鬥的畫面）。

三、恐怖

恐怖的前提是要大多數的民眾都會感到心裡不舒服，整個網站、網路文章或網路影片所呈現出的內容與傳遞的訊息，涉及人類/非人類的死亡狀況或屍體狀態、天災人禍等災難現場的狀況且有人類因此受有傷害、或是與鬼怪靈異等超自然現象有關的內容，皆屬恐怖的範疇，並且需要多數人都會有感到驚嚇、不安等心裡不舒服的狀態。

四、血腥

日常生活偶爾會因為受傷而流血，但是不會讓人看得不舒服，因此血腥的前提需要是大多數的民眾都會感到心裡不舒服的內容，才是血腥所要處理的範疇，而當整個網站或網路影片所呈現出的內容，涉及血液，或是身體器官內臟、手腳四肢的受傷、損害等內容皆屬之，依據內容呈現

的強度不同，必須提供不同程度的防護機制。

五、有害物品

生活中有部分物品並不適合未成年的兒少接觸，為了避免引起未成年人接觸的慾望，或是進一步保護未成年人本身，整個網站、網路文章或網路影片所呈現出的內容與傳遞的訊息，涉及菸（例如未成年抽菸）、酒（例如未成年飲酒）、檳榔（例如未成年吃檳榔）、毒品（例如販賣毒品、教導如何吸毒）、管制藥物（例如販售未取得食藥署認證的藥品）、槍械、刀械、爆裂物等內容。

六、其他違反有害兒少身心健康內容

網路上的資訊非常多元，並無法單單用幾種類型就能涵括完畢，此類型所規範的是除了色情、暴力、恐怖、血腥及有害物品外其他內容，以及受理申訴的 iWIN 團隊經常收到的申訴類型，當整個網站、網路文章或網路影片所呈現出的內容與傳遞的訊息，涉及歧視他人、仇恨言論、洩漏或揭漏他人的個人資料（例如電話號碼、地址等）、賭博資訊（例如線上賭博網站），或是其他不適合未成年進行的活動等

對於該等內容未採取適當之防務措施，依同法第 46 條第 3 項網際網路平臺提供者[267]應為限制兒童及少年接取、瀏覽之措施，或先行移除。對此英國亦有相類似立法如英國 2017 年數位經濟法規範 ISP 業者受通知後，應過濾並阻擋年齡驗證不充分的色情網站。網域名稱濫用框架亦有提及如兒童行虐待、網路違法販售鴉片、人口販賣、具體可信的煽動暴力等情事，註冊管理機構得於尚未收到法院命令前，收到特定且具有可信度的通知時，採取積極作為。此外，兒童權利公約第 17 條（e）項即明文應確保兒童可自國內與國際各種不同來源獲得資訊及資料，同時參考第 13 條及第 18 條之規定，鼓勵發展適當準則，以保護兒童免於受有損其福祉之資訊及資料之傷害。由上可知，網路有害兒童身心健康內容應受到規範及管理，而具有高度公益行。

動物傳染病防治條例第 38 條之 3 第 3 項：「網際網路內容涉及境外應施

[267] 依同法第 46 條第 4 項網際網路平臺提供者係指提供連線上網後各項網際網路平臺服務，包含在網際網路上提供儲存空間，或利用網際網路建置網站提供資訊、加值服務及網頁連結服務等功能者。

檢疫物之販賣至國內、輸入或其他檢疫相關事項，經輸出入動物檢疫機關公告者，其廣告刊登者、平臺提供者、應用服務提供者或電信事業，應依輸出入動物檢疫機關之公告，採取下列措施：三、限制接取、瀏覽或移除相關網頁內容。」。是以主管機關得對於違反應施檢疫物之販賣至國內、輸入或其他檢疫相關事項得作成處分要求平臺提供者、應用服務提供者或電信事業進行限制接取、瀏覽或移除相關網頁內容。

動物傳染病防治條例第 38 條之 3 立法背景係有鑑於我國非洲豬瘟疫情嚴峻，政府早已禁止疫區之相關檢疫品輸入國內，惟因電子商務興起，國人於淘寶、蝦皮等網路購物平臺交易頻繁，加以中國大陸為此次非洲豬瘟疫情之重災區，復以兩岸人民交流密切，故如何防範國人於網路購買來自中國大陸之非洲豬瘟相關檢疫品，或以郵包寄遞方式夾藏應檢疫物闖關，實為防堵前述漏洞之首要課題。為強化網路電商販售端的管理，故於 108 年 12 月 13 日新增同法第 38 條之 3 規定，規範網路電商應配合政府防疫檢疫措施之義務與責任，以阻擋民眾下單購買或賣家違規上架販售境外動物檢疫物，減少違規檢疫物以快遞、貨運或郵包寄到國內的機會[268]。

綜上所述，我國相關立法僅有兒童及少年福利與權益保障法及動物傳染病防治條例有明文授權該管行政機關將經其認定為違法之網站內容為限制接取、瀏覽，甚至是移除之措施。是以，未來各主管機關應考量違法態樣、公益性、比例原則等決定是否於主管法規中明文授權機關得採取限制接取、瀏覽，移除之措施，以有對網域名稱濫用行為作出行政處分之法源依據。

第三項　與網域名稱及網域名稱註冊管理機構相關之我國立法例

由於網域名稱屬於新興的領域，雖然各國專家學者咸認為其屬公共財，但對於其法律性質、其管理應如何進行、政府對於網域名稱監理之介入等等問題，都仍然存有相當多的爭議[269]，我國雖由 TWNIC 負責「.tw」網域名稱之註冊管理，但 TWNIC 為何擁有此一權力，其法律依據及是否有調整之必

[268] 李淑瓊，網購或郵寄夾藏中國大陸應施檢疫物闖關所涉罰則之研析，立法院網站，https://www.ly.gov.tw/Pages/Detail.aspx?nodeid=6590&pid=191871（最後閱覽日：2021 年 11 月 24 日）。

[269] 探討 TWNIC 對網域名稱使用涉有違反相關法律之虞時可採行之緊急處置措施，財團法人台灣網路資訊中心委託研究案，2006 年，頁 5。

要，具進一步探討之必要。

1. 電信管理法

我國電信管理法第 71 條規定：「網際網路位址或網際網路頂級網域名稱註冊管理服務，應由法人組織辦理。（第一項）提供網際網路位址或網域名稱註冊管理服務之國家級網際網路位址註冊管理機構或國碼網際網路頂級網域名稱註冊管理機構，應訂定業務規章，並送主管機關備查。（第二項）網際網路頂級網域名稱足以表徵我國者，該網域名稱註冊管理機構應訂定業務規章，供主管機關查核。（第三項）從事第一項業務者之資格、條件、申請程序、方式、業務規章應記載事項、委託辦理註冊業務、行政管理及其他應遵行事項之辦法，由主管機關定之；其相關輔導措施之辦法，由行政院指定機關定之。（第四項）主管機關為辦理網際網路位址及網域名稱註冊管理事項，得與國際組織進行協商及交流合作。（第五項）」，本法為授權主管機關管理網際網路位址或網際網路頂級網域名稱註冊管理服務之規定。

電信管理法第 2 條規定，本法所稱主管機關為通傳會。由上述規範可知，通傳會依法對於網域名稱註冊管理機構之管理，類似於對於社團法人之低度監管模式，網域名稱註冊管理機構應訂定業務規章，供主管機關查核。然而，於在網路愈發達所衍生的網路犯罪及糾紛日益增加，致使我國政府相關單位，例如行政院公平交易委員會、地方政府、內政部警政署常以網域名稱註冊人違反公平交易法、菸害防制法、著作權法、刑法等法律或為偵查犯罪所需，進而要求.tw 網域名稱註冊管理機構之 TWNIC 對該有違反法律之虞之網域名稱進行必要之處置。

依照現行我國立法例，通傳會無權利要求註冊管理機構就個案移除不法內容或取消網域名稱等必要處置。此有賴各機關於主管法規中定明，授權其針對濫用之網域名稱為必要處置，相關修法方向參第六章第五節。

2. 網際網路位址及頂級網域名稱註冊管理業務監督辦法

(1) 網際網路位址及頂級網域名稱註冊管理業務監督辦法(下稱「本辦法」)第 4 條規定：國家級網路位址註冊管理機構或國碼頂級網域名稱註冊管理機構，應檢具下列文件送主管機關備查。

(2) 本辦法第 6 條規定:「頂級域名註冊管理機構或網路位址註冊管理機構從事註冊管理業務，不得有下列行為：一、違反法律或依法律授權之法規。二、危害網際網路之互連或運作。三、危害國家安全或妨害治安。四、妨害公共秩序或善良風俗。(第一項)國碼頂級網域名稱註冊管理機構或國家級網路位址註冊管理機構從事註冊管理業務應確保通信秘密及提供公平服務，違反規定者，應依主管機關通知限期改正。(第二項)」

(3) 本辦法第 7 條規定:「國碼頂級網域名稱註冊管理機構或國家級網路位址註冊管理機構應就其註管業務訂定業務規章...業務規章應訂定公平合理之服務條件，並載明下列事項：...五、網域名稱爭議處理機制。六、其他與註冊人消費權益有關之事項。」

3. 網域名稱註冊管理業務規章

(1) 財團法人台灣網路資訊中心(TWNIC)於 109 年 8 月 27 日修訂新版網域名稱註冊管理業務規章(下稱「本業務規章」)

(2) 本業務規章第 7 條規定:「本中心得委託受理註冊機構代辦本業務。本中心僅對受理註冊機構受委託範圍內之業務負責，客戶與受理註冊機構間非關網域名稱註冊事宜，概與本中心無關。受理註冊機構有關本業務事宜，不得違反電信管理法、監督辦法及本規章。」

(3) 本業務規章第 8 條:「本中心不負查證客戶所填具資料真偽之責任，如客戶提供不實資料致生任何糾紛或法律責任者，由客戶自行負責。

(4) 本業務規章第 26 條：「客戶同意如與第三人就其所註冊之網域名稱產生爭議時，悉依本中心所公布之『財團法人台灣網路資訊中心網域名稱爭議處理辦法』及『財團法人台灣網路資訊中心網域名稱爭議處理辦法實施要點』等相關規定處理。前項之規定，不妨礙客戶或第三人向法院提出有關該網域名稱之訴訟權利。」

(5) 本業務規章第 27 條：「本中心應依網域名稱爭議處理程序規定，根據專家小組所作成之決定，移轉或取消網域名稱。客戶除得依網域名稱爭議處理程序另行提起訴訟暫停決定之執行外，不得對本中心為任何訴訟上請求。

由上述可知，TWNIC 應根據專家小組所作成之決定，移轉或取消網域名稱。但似無義務主動認定網路內容或使用者行為之適法性。

4. 網域名稱申請同意書

(1) TWNIC 於 2015 年 5 月 27 日修正通過「網域名稱申請同意書」(下稱「本同意書」)，係 TWNIC 與.tw 註冊人之間之重要規範，並構成「網域名稱業務規章」之補充性條款之內容。

(2) 本同意書第 2 條：「TWNIC 有權基於國際網路社群慣例及維護消費者權益、保護智慧財產權與執行法律等公共利益之考量而設置 WHOIS 查詢介面，將註冊人所提供之中英文資料（網域名稱、申請人姓名、電話、傳真、電子郵件（E-mail)、申請日期、有效日期、DNS 設定資料)，提供外界線上逐筆查詢。為保護註冊人之隱私權，TWNIC 得視該註冊人為個人或非個人而擇定部份中英文資料，供該註冊人選擇是否顯示提供外界查詢。」

(3) 本同意書第 7 條：「網域名稱註冊使用，須確保其資訊防護措施之完備及安全，如因可歸責網域名稱註冊人之事由，足資影響他人權益或危害網路運作，TWNIC 於接獲相關機關通知後，得視情況暫停所註冊之網域名稱或為其他合理之處置。」

(4) 本同意書第 11 條：「本同意書未盡事宜，概依我國相關法律之規定及網域名稱註冊管理業務規章；法律未規定者，得參考網域名稱註冊管理之國際慣例。」

綜上，依照本同意書第 7 條，**因可歸責網域名稱註冊人之事由，足資影響他人權益或危害網路運作**，TWNIC 於接獲相關機關通知後，得視情況暫停所註冊之網域名稱或為其他合理之處置，以申請人事前同意，作為 TWNIC 依據其他政府機關為必要處置之立法例來源。關於著作權之搜尋服務提供者部分，我國規定和美國法相同，於搜尋服務提供者怠於移除其他使用者之侵權結果時，將使該業者和侵權人成立共同侵權行為，顯見關於著作權內容之侵害，我國目前主要仍以民事契約作為他律規範之手段。

5. **網路內容或使用者行為適法性之通報單位或機構**

(1) iWIN 網路內容防護機構

iWIN 網路內容防護機構（iWIN）係依據我國兒童及少年福利與權益保障法第 46 條第 1 項規定由通傳會召集各目的事業主管機關委託民間團體成立內容防護機構，其任務包含維護兒少網路安全環境、推動業者自律及受理有害兒少內容之申訴。

iWIN 邀集相關主管機關、兒少團體、社會團體、專家學者以及網路服務業者，共同組成任務型「多方利害關係人諮詢會議」協助擬定申訴案件處理等級、分案標準並視執行成效進行檢討；並針對民間通報，提具判斷意見供權責機關審查參考[270]。

因此，iWIN 係目前我國主要協助主管機關針對爭議內容進行審查，提具判斷意見供權責機關審查參考，及通報網路內容或使用者行為是否違反兒童及少年福利與權益保障法之機構，惟 iWIN 並無任何公權力自行判定為違法，僅係於發現不當內容時通知網域

[270] iWIN 目標，iWIN 官方網站，https://i.win.org.tw/about.php#stop6，（最後閱覽日：2021 年 6 月 30 日）。

名稱所有人，如不處理，iWIN 將通知主管機關，實際裁罰或監理手段仍是由主管機關作成。故 iWIN 既僅為「單純之觀念通知」，無須網域名稱申請人陳述意見，即得進行初步判斷，並提供其認定違法之網站供衛福部參考，再由衛福部決定，是否依法對相關網域名稱進行限制接取、瀏覽或刪除內容之處分。

(2) 檢察機關或司法警察機關

如網路內容或使用者行為有違反我國刑法及特別刑法規定者，應主動移送或函送檢察機關或司法警察機關偵辦，故檢察機關或司法警察機關應為初步階段之網路內容或使用者行為適法性之認定機構。惟檢察官如欲將網域名稱進行扣押，依照我國之實務經驗，僅有法院核發之扣押裁定方得扣押網域名稱。

(3) 行政機關得否認定網域名稱之合法性

行政機關如需對網域名稱為一定處置，基本上應有相關法規作為行政處分之法源依據。以我國而言，僅有兒童及少年福利與權益保障法及動物傳染病防治條例有授權衛福部及農委會要求網域名稱註冊管理機構為限制接取及瀏覽之處分。

如無相關法規，實務上亦有受理註冊機構及網路服務提供業者依照刑事警察局、法務部調查局來函之指示，對毒品、賭博”及國際上指示隻病毒網站進行進一步處置，惟在我國對上述處置手段並無法源依據，僅能稱上述網域名稱註冊管理機構及受理註冊機構自發性之行為，在相關領域之法規命令出現前，難謂為行政處分。

(4) TWNIC 並非網路內容或使用者行為適法性之認定單位

依照網域名稱註冊管理機構業務規章之規定，客戶與受理註冊機構間非關網域名稱註冊事宜，與本中心無關；且網域名稱註冊管理機構不負查證客戶所填具資料真偽之責任，如客戶提供不實資料致生任何糾紛或法律責任者，由客戶自行負責。此外，按照網

域名稱申請同意書第 7 條規定， TWNIC 於接獲相關機關通知後，得視情況暫停所註冊之網域名稱或為其他合理之處置。由上述可知，TWNIC 並非網路內容或使用者行為適法性之認定單位。

第四節 小結

各國針對網域名稱濫用按其國情及法體系而有不同的監理手段及力道，以表列比較各國間之差異。

表 11 各國制度比較表

	馬來西亞	日本	美國	英國	我國
非司法之內容認定機構	MCMC （行政機關）	SIA （民間團體）	無	互聯網觀察基金會（Internet Watch Foundation）（民間團體）	衛福部 農委會 偵查機關 iWIN（民間團體）
法源依據	概括授權之立法	無	無	特定領域立法： 1988 年英國著作權、設計和專利法	特定領域立法 1. 兒童及少年福利與權益保障法第 46 條之 1 2. 及動物傳染病防治條例第 38 條之 3
處置手段	行政處分	1. 民間通報 2. 業者自律 3. 刑事扣押	民事扣押	1. 民間通報 2. 業者自律 3. 禁制令	1. 民間通報 iWIN 2. 業者自律 3. 刑事扣押 4. 民事暫時狀態假處分

	馬來西亞	日本	美國	英國	我國
境外網域名稱處理之方式	由 MCMC 命令 ISP 業者屏蔽網站	由 SIA 通報海外 ISP 業者，並無強制力；尋求司法互助	採司法互助，惟.com 之受理註冊機構 VeriSign 為美國境內公司，美國司法部曾函請 VeriSign 要求取消網域名稱	與該國之警察網絡合作以該國之法制或流程刪除	使用 DNS RPZ 停止解析濫用網域名稱
是否符合 DNS Abuse Framework	否 監理「內容濫用」範圍過大，且針對非重大內容無法官保留	是 網路病毒之濫用部分沒有監理性立法，行政機關難以對此作成相關行政處分	是 所有網域名稱濫用均由法院處理，符合法官保留。	是 所有網域名稱濫用均由法院處理，符合法官保留。	否 監理之「內容濫用」範圍超過該架構，且過去多為偵查機關追查犯罪之權責進行處置

第五章 蒐集利害關係人意見及彙整

本章節彙整研究團隊對網域名稱關係人之訪談，希冀透過訪談瞭解網域名稱實務運作及網域名稱濫用應對之策及困境。機關訪談包含行政院資通安全處、刑事警察局電信偵查大隊及交通部郵電司等共計三個；機構則為TWNIC及iWIN；業者為中華電信數位通信分公司、新世紀資通股份有限公司、亞太電信股份有限公司、鼎嘉數位有限公司、協志聯合科技股份有限公司、台灣大哥大股份有限公司、台灣之星電信股份有限公司、網路中文資訊股份有限公司等共計八家，為便於業者接受訪談並回覆研究團隊，除中華電信數位通信分公司為視訊訪談外，其他業者採取書面訪談。此外亦於110年10月22日舉行座談會，邀請業者及專家學者與會，提供寶貴意見。

以下為各訪談對象回覆及座談會之綜合整理，詳細記錄可參考本研究報告附件。

第一節 機關訪談

第一項 行政院資通安全處

一、訪談目的

訪談目的
1. 了解網域名稱回應政策區域 （Domain Name Response Policy Zone, 下稱DNS RPZ）之使用程序及範圍。
2. 兒童及少年福利與權益保障法及動物傳染病防治法有關「內容下架/移除」之意思。
3. 了解建議後續訪談對象為何。

二、會議討論主題

（一） DNS RPZ 之原理、流程及實務使用情形

受訪者意見歸納
1. DNS RPZ 是網域名稱或者 IP 位址的介接技術，例如可以 TWNIC 便開頭擋掉。但是如果要從 TWNIC 阻擋一定要有法律依據，或是過法院裁定。 2. RPZ 技術層面上，最小單位可以阻擋 IP、阻擋網站、阻擋網域名稱都可以。但是不能擋 IP 裡面的特定內容或處理特定網頁。除非該網頁連結到一個被停止的 IP。另外，停止解析的意思是 DNS 不解析，跟 DNS RPZ 不一定一樣，DNS RPZ 是不作網域名稱跟 IP 的對應。我們可以說因為 DNS RPZ 所以停止解析，但是不能反過來說，停止解析就是 RPZ。 3. 至於可使用 RPZ 之主體為何，如果有人有 DNS 技術或許就有那個能力可使用，但身處網路供應鏈最上層的 TWNIC 建置 DNS RPZ 才最有效果。 4. 另外行政院資安處尚有黑名單措施，此與 DNS RPZ 不同，此先由行政院資安處蒐集黑名單，再由國發會將黑名單設置於政府網頁以建置防火牆，藉此阻擋特定網站內容。
研究團隊意見及歸納:
本團隊研究各國政府立法例，取消網域名稱都是最後、最備位的手段。一開始會由受理註冊機構先用使用合約介入、再來才是扣押伺服器、用防火牆擋，盡量不會取消網域名稱。

（二）內容下架之意涵及案例研析

受訪者意見歸納
1. 實體法所謂「下架」會是針對內容刪除，不會是下架網域名稱。因為網域名稱裡面的不只一個網站，又單一網站裡面的內容也很多，若將整個網域名稱取消會牽涉到箝制言論自由的問題。 2. 至於研究團隊問到「雪崩案件」，假設此集團在台灣並無犯罪行為，法院會無法作出裁定取消其網域名稱。這時候可能要從該網站跟 ISP 的契約關係決定是否要停止服務，和法院保留沒關係。總之雪崩案不是用 DNS RPZ 技術，網域名稱取消或移轉這

件事不一定是用 DNS RPZ 的。

3. SWAG 不是用 TWNIC 的 DNS RPZ 技術停止解析網域名稱。網址移轉的不用特別技術就可以做到。從 DNS 上、伺服器上做網址轉接都可以，各種階段來做都可以，網站轉址跟 TWNIC 未必有關係。
4. RPZ 的概念類似「100>>中正區」的關係被拿掉。至於網站找不到的話是「地址某某號，但是查無此號碼」，跟 RPZ 關係不大。網站找不到有兩種，一種是找不到服務，一種是根本沒有網站。因為台灣地區 IP 都是用 TWNIC 在做分配，所以如果 TWINC 阻擋，網站根本無法連到，所以影響最大。

研究團隊意見及歸納:

那麼之後我們的訪談及研究會轉向 DNS RPZ 以外的網站內容下架問題。

（三）制度建議以及接續訪談對象建議

受訪者意見歸納

1. DNS RPZ 理想制度應該要一個平時用、一個緊急用。平時用之程序跟通保法做法一樣，需法院同意。緊急用時可以直接做，但有二十四小時限制。
2. 想知道技術面的部分，建議訪問調查局或者刑事局，因為他們是實際執法單位，會有更多元的看法。國安會也可以，其從國家安全角度，看法也會更不一樣。
3. 建議可以訪談中華電信，因為中華電信是台灣最大的電信業者，可以問他們有關 RPZ 問題。

研究團隊意見及歸納:

謝謝簡處長提供寶貴意見，我們接下來會把執法單位以及中華電信列為訪談對象。

第二項　刑事警察局電信偵查大隊

一、訪談目的

訪談目的
1. 刑事局處理「網域名稱濫用」之程序及案例。
2. 「斷源專案」之端續及法源依據為何?
3. 刑事局是否加入 DNS RPZ 政策?與「斷源專案」之關係
4. 針對影響網路安全之「網域名稱技術濫用」之處置（程序保障與急迫危險之天秤）。
5. 刑事偵查與行政處分之優劣

二、會議討論主題

（一） 刑事偵查措施探討

受訪者意見歸納
1. 刑事偵查方式主要分為三種： (1) 有最高權限會直接接管網域名稱申請，直接扣押網域名稱申請的帳號密碼，電信隊會把密碼改完之後，直接把網址轉向我們設定的網站。swag 和楓林網皆是以此方式，楓林網案件中並無扣押裁定。搜索票會特別寫到應扣押雲端硬碟。 (2) 第二種方式就是通報 TWNIC，請法院通報業者停止解析。DNS RPZ 是資安聯防，請 TWNIC 跟業者合作，達到境內聯防。 (3) 第三種為針對美國的網域名稱或者再上一層的域名要求取消網域名稱。此需要未來的司法互助，由台灣的檢察官通報美國的檢察官才能做到。目前做不太到。 2. TWNIC 負責停止解析有以下問題：第一，TWNIC 要求業者停止解析事實上並無強制力。第二，找民間機關做強制處分有偵查秘密外洩之問題，希望未來有一個公家機構可以負責這個職責。我們認為要有一個部門負責處理 RPZ 的執行，且執行上不再分民事、刑事、行政程序處理，單純負責執行 RPZ。 3. DNS RPZ 宜處理資安問題。但是如果是網路內容有問題，比方賭博、色情、統戰言論，這種情況是不是該用 RPZ，要另外討論。
研究團隊意見及歸納:

我們前面訪談的受訪者沒有談論到電信警察隊提到的偵查洩密問題，基於此脈絡下，RPZ 執行機關的確可能需要為公部門。謝謝電信警察隊提供寶貴意見。

（二） 斷源專案探討

受訪者意見歸納

1. 有關斷源專案：

   早期電信警察隊為了因應電信犯罪氾濫，人頭門號、地下電台等等問題而設，現在轉型到對付詐騙集團。現在其實專案的主管機關是 NCC，斷源專案其實是概括名詞，勉強來說法源為電信法、刑事訴訟法，以及通訊監察法，但沒有明確法源，只是一個行政手段。斷源專案現在已停止。現在給 165 反詐騙專線來做。
2. 我們認為，讓網站違法內容下架未必要用 RPZ，以預防的立場來說，對斷源專案是可以做的，其極具效率，且只是單純防止更多人被害，並沒有要進一步行刑事訴訟程序追究任何人責任。
3. 針對不同種類之違法內容審查，我們認為，不同事務交給不同目的事業主管機關到最後就會沒效率且沒人管。若擔心一個專責機構權限會太大，交給一個民間機構中介處理。比方說 iWIN 作法，其有明確法源基礎且背後有行政機關為後盾。
4. 總結一下，現在的目標是讓網頁內容無法顯示，若採取消網域名稱方式，需要司法互助且程序會拖很久，若採停止解析，其是預防犯罪的動作，是行政處分，不需要發動刑事程序，較有效率。

研究團隊意見及歸納:

謝謝電信警察局提供有關斷源專案之意見。

（三）制度建議

受訪者意見歸納
我們認為，給執法單位一個權限不是真正要讓執法單位用，而是萬一發生平臺不理執法機關時，應該要怎麼處理的問題。建議 NCC 統一來規定取消網域名稱措施之規定，以免該領域主管機關不知道怎麼做，並且建議 NCC 把 TWNIC 的角色再明確化。
研究團隊意見及歸納:
謝謝電信警察局之意見。

第三項　交通部郵電司

一、訪談目的

訪談目的
1. 瞭解目前 ICANN 對個資議題及 WHOIS 資料庫之態度
2. 瞭解網域名稱技術濫用處理方向

二、會議討論主題

（一） 目前 ICANN 對個資議題及 WHOIS 資料庫之態度

受訪者意見歸納
ICANN 對各項議題（含個資及 WHOIS 資料等）之政策擬定形式係採由下而上、及透過多方利益共同體機制進行討論，以期形成共識，最後由董事會做最後決定，且 ICANN 亦遵循各國的法律；而針對個資議題及 WHOIS 資料庫部分，過往 WHOIS 資料係為開放狀態，後因歐盟為保護個資安全而制定歐洲個人資料保護規則（GDPR），故之後大部分 WHOIS 欄位改為封閉狀態，目前 ICANN 對於本項議題之日後開放程度及存取方式，刻正透過快速政策制定流程（EPDP）之三階段討論及評估中。
研究團隊意見及歸納:
謝謝讓團隊瞭解目前 ICANN 針對個資議題討論情況。

（二） ICANN 提出之揭露/存取非公開註冊資料的標準化系統

受訪者意見歸納
依行政院分工，本部並非 gTLD 政策及公共安全（含資料保護）之業務主管機關，且本部也非揭露/存取非公開註冊資料的標準化系統（System for Standardized Access/Disclosure to Non-Public Registration Data，下稱 SSAD ）使用單位，建議洽詢業務主管機關或 SSAD 使用單位之意見。惟建議我國本議題之業務主管機關及使用單位應密切注意 SSAD 系統之相關發展方向及內容，必要時提出意見，以符合我國之實務需求
研究團隊意見及歸納:
謝謝讓團隊瞭解 SSAD 之重要性。

（三） 主管機關對註冊管理機構 TWNIC 之監管態度與世界趨勢

受訪者意見歸納
本部並非「網際網路位址及頂級網域名稱註冊管理業務監督辦法」之業務主管機關，建議洽詢業務主管機關之意見。惟考量個資保護及資安問題，影響國人權益及安全極大，建議主管機關仍應有此類監管之規範為宜。
研究團隊意見及歸納:
謝謝讓團隊注意個資保護之重要性。目前「網際網路位址及頂級網域名稱註冊管理業務監督辦法」第 7 條第 2 項 3 款規範業務規章應訂定公平合理之服務條件，並載明註冊人基本資料利用之限制及條件。是以註冊管理機構依本法第 7 條報請備查時，主管機關得審酌主管機構之業務規章是否符合我國個資法之保護。

（四） 網域名稱技術濫用監理方向

受訪者意見歸納
依行政院分工，本部並非資安業務主管機關，建議洽詢業務主管機關相關意見。惟鑑於目前技術濫用情況不一，為能儘速處理，建議可作適當分工，部分情況可由 TWNIC 直接取消網域名稱，部分則另由業務主管機關決定。
研究團隊意見及歸納:
感謝提供部分涉及緊急情勢之技術濫用可由 TWNIC 逕為處理之監理方向。

第四項　農業委員會動植物防疫檢疫局

一、訪談目的

訪談目的
1.瞭解動植物防疫檢疫局執行動物傳染病防治條例第 38 條之 3 第 3 款有關網路內容涉及境外應施檢疫物之販賣至國內、輸入或其他檢疫相關事項有限制接取、瀏覽或移除相關網頁內容時，所採取之流程。
2.瞭解動植物防疫檢疫局執行上述限制接取、瀏覽或移除相關網頁內容之處理方式及成效。

二、會議討論主題

（一） 防檢局依動物傳染病防治條例第 38 條之 3 第 3 款執行情況

受訪者意見歸納
1. 執行限制接取、瀏覽或移除相關網頁內容之情形： (1.)　認定不當內容之來源有來自人民申訴檢舉、動植物防檢局自行查找 (2.)　將違法之內容以公文函通知「網路平臺業者」及「ISP 業者」請求將內容刪除或停止解析。 (3.)　約 98%在網路平臺業者發生 (4.)　搜查電商平臺刊登違規境外應施檢疫物廣告查獲案件之平均查獲率，自 108 年的每月平均 7.4%降到 110 年的每月平均 0.1% 2. 「網際網路內容涉及境外應施檢疫物販賣至國內或輸入時應採取措施」於今年 7 月 23 日修正公告，係因業者及產業團體屢次透過外國商會等管道向國家發展委員會反映，建議政府瞭解電商平臺特性，針對電商平臺、賣家及電信業者不同的營運模式，建構可歸責之管理措施，制定出符合電商產業環境永續發展的法規。而本局評估並研析業者陳情意見後，在兼顧有效管理電商平臺及邊境阻絕動物疫病的考量，修正該措施。
研究團隊意見及歸納:
感謝提供 貴局告訴研究團隊動物傳染病防治條例第 38 條之 3 第 3 款執行情況，此可作為其他領域如有類似網域名稱濫用處置需求之參考。

（二） 相關處置案例

受訪者意見歸納

1. 提供以下案例：

(1.) A 君平常在家照顧小孩，同時在兩家以上電商平臺開設置帳號，拍賣日韓泰進口零食或其他物件作為收入，其經營模式為買家向 A 君下單後，A 君向自國外網路訂購並以快遞貨物方式寄送予買家，**本次係 A 君刊登日本雞皮餅乾廣告，日本雞皮餅乾屬不得輸入之檢疫物**，經防檢局查察後通知 A 君到案陳述意見，A 君亦以書面陳述意見坦承刊登廣告，依規定受裁處新臺幣 3 萬元罰鍰。

(2.) B 君喜愛出國至泰國旅遊，旅途中發現當地泰國雞皮及炸豬皮餅乾頗受歡迎，B 君自行以旅客方式攜帶入境，並**在電商平臺設置帳號拍賣，泰國雞皮及炸豬皮餅乾均屬禁止輸入之檢疫物**，經查獲後通知 B 君到案陳述意見，B 君亦坦承不諱，然攜帶輸入之餅乾因無人訂購，已自行食用完畢，針對 B 君違規刊登泰國雞皮及炸豬皮餅乾之行為，依規定受裁處新臺幣 3 萬元罰鍰，另對其違規輸入未申報檢疫情節，將另案調查，如查證屬實後則依規定再裁處新臺幣 3 萬元罰鍰。

(3.) C 君為中國大陸籍配偶，因懷念家鄉味而經由淘寶網站訂購中國大陸之泡椒鳳爪及含牛肉火腿腸懶人火鍋等含肉加工食品，為貼補家用**在電商平臺設置帳號拍賣，經防檢局查察後，C 君亦坦承刊登行為**，依規定受裁處新臺幣 3 萬元罰鍰。

研究團隊意見及歸納:

感謝 貴局提供資料。經研究團隊進一步與 貴局聯繫，得知 貴局將先請求電商平臺協助將平臺上之廣告刪除並請求電商提供廣告刊登者的資料（如姓名、住址、聯絡電話、電子郵件及國民身分證統一編號），以進行下一步調查。

第二節 機構訪談

第一項 iWIN 網路內容防護機構

一、訪談目的

訪談目的
1. 瞭解 iWIN 執行兒童、少年網路內容防護之流程。
2. iWIN 任何為確保兒童及少年閱覽之內容，是否應擴大通報範圍?
3. 未來是否參照日本之通報組織「Safer Internet Association」，讓 貴機構成為通報所有網域名稱內容濫用之民間機構?

二、會議討論主題

（一） iWIN 職責介紹及下架違法內容意見

受訪者意見歸納
1. iWIN 職責大抵可以分為四部分：網路行為觀察、處理民眾申訴、推動業者自律（因為 iWIN 無法人格且無強制力，故仰賴業者自律尤其重要）、教育宣導（包含對政府機關，包含司法機關、警政機關，以弭平各機關法規遵循程度之差距）
2. iWIN 另外提供業者自律框架五大原則：1.使用者規範、2.平臺自我審查機制、3.防護措施、4.申訴管道、5.機關連繫窗口。
3. iWIN 原則上不主動去查是否有不當內容。至若民眾申訴內容有違法疑慮，若經過 iWIN 審查過後確認有問題，無論就內境外業者，只要聯絡的到，iWIN 通通會通知。如果業者對於內容防護仍未改善，iWIN 才會將案件後送到法令主管機關。此方法境內業者成效大約在 70-80%，境外業者大約在 50%。
研究團隊意見及歸納:
謝謝讓團隊瞭解 iWIN 目前運行情況。

（二）對於 iWIN 能否擴張業務範圍之意見

受訪者意見歸納
1. 有關停止解析之問題，因為違反兒少法的內容以形式審查即可判斷，但是假消息是需要實質判斷的，所以停止解析未必是最好方法，停止解析比較適合形式判斷的內容。再者，如果 iWIN 的強制力變高，審查過程上勢必會再變慢。 2. iWIN 無法擴張業務，因為法源就是兒少法。但是 iWIN 工作模式可以被複製，故其他主管機關法令可以同樣方式操作，將違法內容下架。只是不同內容需要有不同的制度訂定方式。目前的做法應該是看看有無 iWIN 之外其他單位有興趣承作其他主管機關相關業務。
研究團隊意見及歸納:
贊成交給電腦公會承接其他內容類型的業務。我們需要把 iWIN 組織之績效優點呈現出來，以期能成立其他類似 iWIN 之組織。

第二項　TWNIC 財團法人台灣網路資訊中心

一、訪談目的

訪談目的
1. 了解 DNS RPZ 之使用程序及範圍。
2. 停止網路服務之內涵及實務流程。
3. DNS RPZ 或下架網頁內容之制度建議

二、會議討論主題

（一） DNS RPZ 之流程及實務使用情形

受訪者意見歸納
1. 針對.tw 的部分，我們啟動 DNS RPZ 必須以取得法院判決、或者具有法律依據的行政處分為前提。假如判決文義清晰，我們便會以判決文義執行，目前只有收過兩件。我們收過很多政府機關來函，但是因為法律依據較為不明，所以我們沒有依照函文辦理過。我們也沒有收過民事執行的公文。 2. 我們沒有收過 iWIN 的通報，衛福部通報也沒有，但是假如我們收到通報，因為有

兒少法之法律依據，我們的確可以據以執行。另外如果國安單位要求時，因為此時案件樣態我們無法自己定義，我們會據以執行。

3. ISP 業者幾乎都已經加入 DNS RPZ 的次節點，因為 DNS RPZ 技術有法律依據，業者會以遵守自律規範方式加入節點。
4. DNS RPZ 不是處理違法網域名稱濫用之唯一手段，而是最後手段。此外，ICANN 不處理任何網域名稱取消，他們認為這是各個司法管轄機關的職責。

研究團隊意見及歸納:

謝謝 TWNIC 寶貴意見。

（二）停止網路服務或內容下架之探討

受訪者意見歸納

1. 受理註冊機關要有法律依據才能停止解析，原則上 ISP 業者技術上有辦法停止解析，但是還是要有法律依據之處分或判決。
2. ISP 可以刪除網頁內容。網路接取業者可以針對特定內容進行遮蔽處理。ISP 會比 TWNIC 多一些工具可以管理，例如透過路由器或者防火牆，利用 access control list 控制資料處理。
3. 農委會有來溝通過關於動植物違禁商品下架的事宜，現在有法律但沒有具體 SOP，故目前我們有沒收過來自農委會的行政處分要求取消網域名稱。

研究團隊意見及歸納:

謝謝 TWNIC 寶貴意見。

（三）制度建議

受訪者意見歸納

1. NCC 主要針對有線無線電視廣播以及通信電信監理管理，而我們是處理後者。如果是對特定網路內容，會是比較困難的地方，因為無法界定管裡權責。這裡最好還是回歸每個目的事業主管機關，由他們訂定相關法律。
2. 我們常常收到不同單位公文要求移除網站，這種單純公文往返我們無法處理，現在只有兩個法律有授權可以處理（兒少法、動防法）。因此馬來西亞的管制措施，即以

MCMC 是管制言論的機關，可以任意發行政處分，此方式較不可行，基於法治國原則，我國比較可能採取日本作法，對於網域名稱處置須有法院判決方可為之。

研究團隊意見及歸納:

看來無論是內容下架或者用 DNS RPZ，應請各主管機關制定規範及流程，之後的 SOP 便是取得法院判決及合法之行政處分，再來進行後續處理，會是比較合理的方式。

第三節 業者訪談

第一項 中華電信數位通信分公司訪談

一、訪談目的

訪談目的
1. 了解 DNS RPZ 之使用程序及範圍。
2. 了解 ISP 業者依照使用人條款停止提供網域名稱服務

二、會議討論主題

（一） DNS RPZ 之原理、流程及實務使用情形

受訪者意見歸納

1. TWNIC 的 DNS RPZ 政策是由 TWNIC 判斷網站內容之違法性，業者們再行配合政策將有問題的網域名稱停止解析。其實 RPZ 技術即行之有年。過去我們有配合警方斷源專案，由刑事警察局作為窗口發函給中華電信，
2. 針對違反善良風俗如毒品、色情網站停止解析，斷源專案沒有處理過什麼知名網域名稱，大多是名不見經傳的賭博或掃情網站。
3. 停止解析、取消該網域名稱與 DNS RPZ 阻止使用者進入網站之差別：
   (1) 實施機構不同

   DNS RPZ 主要由 DNS Resolver 快取主機(ISP 業者)及 Authoritative Name Server 權威主機進行處理。

   取消網域名稱主要由網域名稱註冊商及受理註冊機構進行處理。

   (2) 效力範圍不同：

DNS RPZ 需透過 DNS Resolver 快取主機（ISP 業者）參與配合，如未參與 DNS 政策，客戶端仍可透過未配合之 DNS Resolver 快取主機（ISP 業者）連結至該網域名稱。

取消網域名稱是根本作法，即無該網域名稱存在，客戶端無法連結至相關網域名稱。

研究團隊意見及歸納:

謝謝中華電信寶貴意見，我們對於技術層面的問題大致已經釐清，我們接下來應該會訪談執法單位以了解實務操作方法。

（二）內容下架之意涵及案例研析

受訪者意見歸納

1. 中華電信並無能力自行判斷網域名稱內容違法與否，僅會被通知進行停止解析相關網域名稱，網站違法與否多由 TWNIC 或特定主管機關判斷。至於如果有註冊人不付網域名稱註冊費的情形，依序進入贖回期等，最後才取消網域名稱，此是在 ICANN 框架下的 ISP 業者使用人條款下的操作流程。
2. ISP 業者無法刪除客戶之網站內容。因刪除相關內容，需要網站管理之帳戶權限。若主管機關或 TWNIC 告知本公司存在之不當內容，本公司僅能停止提供網路服務，而通常都是採取停止解析網域名稱做為執行之手段。

研究團隊意見及歸納:

謝謝中華電信寶貴意見。

（三）立法建議

受訪者意見歸納

公司法務同仁會比較清楚。至於我們業者比較關心的是，如果停止解析網域名稱是否會造成客訴的問題，例如相關客訴。如能告訴客戶具體因違反何等法律致停止解析網域名稱，較能快速解決客訴問題。

研究團隊意見及歸納:

謝謝中華電信寶貴意見。

第二項　其他業者書面訪談

書面訪談以下業者：新世紀資通股份有限公司、亞太電信股份有限公司、鼎嘉數位有限公司、協志聯合科技股份有限公司、台灣大哥大股份有限公司、台灣之星電信股份有限公司、網路中文資訊股份有限公司等七家業者

一、會議討論主題

（一） 貴公司是否有 TWNIC 之網域名稱回應政策區域政策（DNS RPZ），停止解析任何網域名稱？

1. 需有行政機關之行政處分？抑或機關發函即為已足？抑或民間團體（諸如：iWIN、TWNIC）通報即足？
2. 需有法官刑事扣押裁定？抑或檢、警附帶扣押即為已足？

受訪者回答歸納	
鼎嘉科技	目前沒有收過 TWNIC 主動告知，是用戶主動告知我們才知道一個網站連不上。
協志科技	行政機關通報窗口為 TWNIC，並由 TWNIC 通知我們即可。我們業者這邊不會直接受行政機關通知或者收到法院令狀。
亞太電信	目前有收過 TWNIC 一次電子郵件通知辦理。
台灣大哥大	本公司可配合，且不需要有行政處分或法院令狀為前提。
新世紀資通	本公司願意配合法令停止解析特定網域名稱，惟前提應有法源依據，由特定行政機關依法通知本公司配合辦理。刑事程序部分，停止解析特定網域名稱對於網域名稱使用人及 ISP 業者皆有極大影響，若倉促認定即便事後撤銷，對於網域名稱使用人及 ISP 業者所產生之損害恐難以回復，故應有法官刑事扣押裁定。
台灣之星	未作答。
網路中文	DNS RPZ 起源於 2020 年由 Godaddy、Amazon、Neustar、PIR 等 48 家大型網路註冊機構提出網域名稱濫用框架倡議。 TWNIC DNS RPZ 主要運作是其與國內 ISP 業者建構 DNS RPZ（又稱之 DNS 快取伺服器服務），限制境內外惡意網域名稱或 IP 位址接取，為國

	內網路使用者提供資安防護的第一線防衛措施；網路中文是臺灣第一家獲得 ICANN、TWNIC 認證資格的受理註冊機構（又稱註冊商），本公司非 ISP 業者，主要核心業務為提供網域名稱解析及網域名稱註冊管理服務，故本公司非 TWNIC DNS RPZ 合作商，雖無法配合 DNS RPZ，但仍有配合執行依法規、協議及符合 ICANN 要求的適當處置。
研究團隊意見及歸納:	
1. 亞太電信有收過一次 TWNIC 通知。 2. 業者願意配合 TWNIC 處理。業者認為無須有行政處分或法院另狀即可配合；有認為應有相關法源依據。 3. 現行 TWNIC DNS RPZ 需有法院判決/裁定或是行政機關行政處分，始能針對內容濫用之網域名稱進行停止解析。故未來如欲透過行政處分對網域名稱停止解析，各機關應於主管法規定明相關處置手段，以符合法律保留原則。	

（二） 貴公司是否因影響人民網路使用安全之情況而配合國安單位取消網域名稱或停止解析網域名稱之案例？自「雪崩案件」[271]以後，似乎調查局來函（不須依法為行政處分），各 ISP 業者即須阻斷有資安疑慮之網域名稱。

受訪者回答歸納	
鼎嘉科技	TWNIC 應該保持中立，除非有影響國家安全之情。
協志科技	尚未遇過。
亞太電信	否。
台灣大哥大	否。
新世紀資通	本公司辦理停止解析或取消特定網域名稱之行為皆依相關行政機關通知辦理。
台灣之星	無。
網路中文	本公司尚無案例。 依據本公司與 TWNIC 網域名稱受理註冊授權合約 增補條款第 2.原合

[271] 自由時報，我調查局與 31 國聯手偵破「雪崩」網路犯罪集團，https://news.ltn.com.tw/news/society/breakingnews/1904635 （最後瀏覽日：2021 年 10 月 11 日）。

	約第二條新增之第九項：受理註冊機構於接獲 TWNIC、相關單位、當事人之通知，或於其他情形下知悉註冊者有濫用行為或違法活動，應代理 TWNIC 依照「財團法人台灣網路資訊中心網域名稱申請同意書」第一條第三項以及第九條、相關主管機關之命令或法令規定採行適當執行措施。於採行執行措施之前，得先詢問 TWNIC 意見。因此，若本公司接獲 TWNIC、相關主管機關之命令或法令規定關於「.tw」系列網域名稱之通知，將於執行措施之前，先詢問 TWNIC 意見，再採行適當執行措施。而非「.tw」網域名稱則仍需有法院裁判再執行措施。
研究團隊意見及歸納:	
1. 業者無遇到相關案例。 2. 業者認為可皆依行政機關之通知。另有業者認為若為針對「.tw」網域名稱之通知，將於執行措施之前，可先詢問 TWNIC 意見，再採行適當執行措施。若為「.tw」以外之網域名稱，則現行法下建議仍應有法院判決。	

（三） 是否可能類似設防火牆（如色情守門員、大陸長城），讓所有客戶端無法連結到該網域名稱?此外，是否能參酌中國及時把網路內容下架的做法。

受訪者回答歸納	
鼎嘉科技	否。
協志科技	沒有類似做法。受理註冊商的角色，僅是受理客戶申請網域名稱名稱及管理客戶網域名稱使用權限，並無實權管理戶的網頁內容。此外如何判斷內容濫用執行上亦有困難。
亞太電信	否。
台灣大哥大	否。
新世紀資通	若特定網域名稱已列入 DNS RPZ 執行名單辦理停止解析或下架等措施時，使用國內網域名稱則無法連結至該網域名稱。
台灣之星	目前環境僅能透過 DNS 停止解析網域名稱令用戶無法透過網域名稱連結至目標，並無規劃類防火牆之作法。

網路中文	技術上可設防火牆，但客戶若使用跳板、VPN 將失去效用；管理機制之規劃仍需依法建構。
研究團隊意見及歸納:	
業者無相關機制，僅有將特定網域名稱列入 DNS RPZ 執行名單停止解析	

（四） 除 DNS RPZ 所列之黑名單外，各業者是否有內部之「黑名單網域名稱」？

受訪者回答歸納	
鼎嘉科技	有。
協志科技	無自設黑名單，依 TWNIC 指示配合。
亞太電信	否。
台灣大哥大	否。
新世紀資通	本公司辦理停止解析或取消特定網域名稱之名單皆依相關行政機關通知辦理。
台灣之星	無。
網路中文	本公司內部無網域名稱黑名單。 網域名稱註冊者申請網域名稱有可能會涉及違反網域名稱註冊管理機構所制定之規範、及其所在地區之法令規範、中華民國法律、註冊申請人所在地之法律、ICANN 所訂之規範，致網域名稱遭註冊管理機構拒絕申請或凍結刪除。
研究團隊意見及歸納:	
業者無自設內部黑名單。	

（五） 貴公司是否有依據「網域名稱之使用者協議」停止提供網域名稱服務？如有，所使用之手段為何（取消網域名稱、停止解析網域名稱等……）？ 貴公司停止對使用者提供網域名稱服務後，使用國外 VPN 連接是否仍可瀏覽該網域名稱？

受訪者回答歸納

鼎嘉科技	未作答。
協志科技	尚未遇過。
亞太電信	可以停止解析網域名稱。
台灣大哥大	依據附件網域名稱代管服務契約，若客戶（乙方）未遵守網際網路規範時，我司可以不經用戶同意下停止解析網域名稱服務。終止代管網域名稱時，使用國 VPN 連接無法瀏覽該網域名稱。
新世紀資通	本公司辦理停止解析或取消特定網域名稱之行為皆依相關機關通知辦理。依照 VPN 連接技術，的確可以使用國外 VPN 連接被 DNS RPZ 阻隔之網站。
台灣之星	無。停止解析網域名稱後用戶若使用 VPN 或指定其他 DNS 仍可瀏覽。
網路中文	本公司有依法規及協議進行停止解析的機制，但目前為止沒有案例。
研究團隊意見及歸納:	
1. 台灣大哥大：依據附件網域名稱代管服務契約，若客戶（乙方）未遵守網際網路規範時，我司可以不經用戶同意下停止解析網域名稱服務。 2. 其他業者：無/依 TWNIC 通知處理。	

（六） 承上題，受理註冊機構（諸如:中華電信、網路中文）依照使用人條款停止提供網域名稱服務之端序為何？

1. 需有行政機關之行政處分？抑或機關發函？抑或民間團體（諸如:iWIN）通報即足?
2. 需有法官刑事扣押裁定？抑或檢、警附帶扣押即為已足？
3. 影響網路安全之情況是否亦屬之？
4. 其效果和 DNS RPZ 阻止使用者進入該網站之差別為何？
5. 是否有相關案例？

受訪者回答歸納	
鼎嘉科技	無相關案例。
協志科技	無相關案例。本公司不會收到法院裁定，只要有 TWNIC 通知即可，若

	有影響網路安全時，我們也會先通知客戶自行檢查。
亞太電信	依據服務款約定，如果用戶網域名稱危害他人權益或者影響網路運作，本公司得暫停提供網域名稱服務，目前只發生過一次案例。至於「停止提供網域名稱服務」與「DNS RPZ 阻止使用者進入該網站」二者間之主要差別在於影響範圍的大小。例如：若採停止提供某網域名稱服務，所有連線要去該網站時，皆無法開啟該網站。若採 DNS RPZ 阻止使用者進入該網站方式，則只有客戶端 DNS 設定我方 CDNS IP，才無法開啟該網站。
台灣大哥大	本公司依據法令及契約辦理。
新世紀資通	新世紀資通股份有限公司依照 TWNIC Domain Name Registration Agreement 規定，TWNIC 得於有關機關通知後，有權對已註冊之網域名稱執行暫停或採取必要措施; TWNIC DNS RPZ 與業者 DNS RPZ 為主從架構，因此業者 DNS RPZ 會與 TWNIC DNS RPZ 同步執行停止提供網域名稱服務之程序。
台灣之星	無作答
網路中文	（一）及（二）「.tw」系列網域名稱依 TWNIC 網域名稱受理註冊授權合約及其增補條款，於接獲 TWNIC、相關單位、當事人之通知，或於其他情形下知悉註冊者有濫用行為或違法活動，應代理 TWNIC 依照「財團法人台灣網路資訊中心網域名稱申請同意書」、相關主管機關之命令或法令規定採行適當執行措施。於採行執行措施之前，得先詢問 TWNIC 意見。非「.tw」網域名稱則需有法院裁判較無爭議。 （三）受理註冊機構無權獨斷是否屬影響網路安全之情況。 （四）停止提供服務給註冊者使用與僅不被使用者看見。 （五）暫無案例。
研究團隊意見及歸納:	
業者多以受 TWNIC 通知後，或詢問 TWNIC 意見後，依照使用人條款停止提供網域名稱服務	

（七）根據 110 年度聲扣字第 11 號裁定，法院同時通知受理註冊機構依據服務協議限制該網址之使用，及透過 TWNIC 停止解析該網站，藉此將該網址納入我國公權力支配下而為扣押處分。試問，受理註冊機構依據服務協議限制該網址之使用之具體案例為何？

受訪者回答歸納	
鼎嘉科技	未作答。
協志科技	無，僅接受 TWNIC 通知。
亞太電信	此案亞太電信僅配合 110.03.09 TWNIC 電子郵件通知停止解析 8 個網站。
台灣大哥大	無。
新世紀資通	因本公司並未有相關案例且亦非 110 年度聲扣字第 11 號裁定之當事人，故無法表示意見。
台灣之星	未作答。
網路中文	110 年度聲扣字第 11 號裁定為依法不得公開之案件。 具體案例暫無。
研究團隊意見及歸納:	
1. 亞太電信：此案亞太電信僅配合 110.03.09 TWNIC 電子郵件通知停止解析 8 個網站。 2. 其他業者：無	

（八）如果使用國外 VPN 連接被 DNS RPZ 阻隔之網站，是否仍可以順利瀏覽該網站之內容？

受訪者回答歸納	
鼎嘉科技	未作答。
協志科技	不確定。
亞太電信	是。
台灣大哥大	VPN 大多使用國外 DNS，應仍可順利瀏覽網頁。
新世紀資通	依照 VPN 連接技術，的確可以使用國外 VPN 連接被 DNS RPZ 阻隔之

	網站。
台灣之星	若用戶透過他網之 DNS 進行解析，則仍有機會可順利瀏覽內容。
網路中文	目前 TWNIC 推動之 DNS RPZ 係由國內 ISP 業者阻斷其 DNS 解析，故透過 VPN 連接此網站仍可取得所有資料，若要達到完全阻斷「.tw」系列網域名稱之被瀏覽，其實需由 TWNIC 進行 serverHold 之作業使該網域名稱停止所有運作。
研究團隊意見及歸納:	
依照 VPN 連接技術，的確可以使用國外 VPN 連接被 DNS RPZ 阻隔之網站。	

（九）貴公司是否有將一網站之特定內容進行刪除或阻隔之方式？

受訪者回答歸納	
鼎嘉科技	是。
協志科技	無。僅是受理客戶申請網域名稱及管理客戶網域名稱使用權限.，並無實權管理戶的網頁內容。此外執行上客戶及網域名稱眾多無能力依依判斷網域名稱內容違法不當。
亞太電信	否。
台灣大哥大	否。
新世紀資通	本公司停止解析或取消特定網域名稱等行為皆依相關機關通知辦理，並無主動針對網站之特定內容進行刪除或阻隔。
台灣之星	現行無針對一網站之特定內容進行刪除或阻隔方式。
網路中文	本公司沒有對於網站特定內容及頁面進行刪除或阻隔的方式；從網域名稱端處理則是可以使該網站全體服務受阻隔。
研究團隊意見及歸納:	
業者皆無。	

（十）如果未來要擴大停止解析或取消特定網域名稱之法源依據（諸如：禁止網路上張貼迎娶外籍新娘之廣告、禁止張貼違法日租套房廣告等），貴公司對此之態度為何？

受訪者回答歸納	
鼎嘉科技	此違反言論自由。
協志科技	本公司為受理註冊機構，並無權管客戶網域名稱內容，由主管機關訂立相關規範後配合處理。
亞太電信	本公司將依法辦理。
台灣大哥大	原則上只要有法規依據，本公司均會配合，但取消特定網域名稱需考量實務執行上之可行性。
新世紀資通	本公司願意配合法令停止解析或取消特定網域名稱，惟前提應有法源依據。至於法律具體內容及範圍，本公司尊重立法機關職權。
台灣之星	依法遵辦。
網路中文	依法行政。
研究團隊意見及歸納:	
業者多建議有相關法令後，依法辦理。	

（十一） 針對特定網域名稱濫用行為，建議由民間通報抑或由行政機關通報?針對上述情況 貴公司之立場及立法建議為何?

受訪者回答歸納	
鼎嘉科技	可參考美國做法。
協志科技	如為民間第三方專業機構（如 iWIN），經審查民眾通報後，再行通知公司處理為可行方式。公司接獲通知後，會將相關情形通報 TWNIC，待 TWNIC 通知後，進行下一步處理。
亞太電信	本公司將依法辦理。
台灣大哥大	針對特定網域名稱濫用行為，民間通報可做為行政機關通報之參考依據，但業者執行仍應以行政機關通報為宜。
新世紀資通	在有法源依據之前提下，本公司願意配合法令協助處理網域名稱濫用行為，至於究竟應由何單位通報、通報效果為何等，本公司建議應於法令內明訂，以為遵循依據；又法律具體內容及範圍，本公司尊重立法機關之專業及職權。

台灣之星	皆可由民間或行政機關通報後，交由主管機關裁定並通知電信業者執行。
網路中文	建議依法由行政機關通報。任何判斷或執行均需法源依據，無法以民間業者自律構成。本公司為致力穩定各頂級網域名稱，根據 ICANN 及各註冊商註冊協議（Registry-Registrar Agreement）之要求，遵循網域名稱反濫用，若註冊者有濫用行為，本公司或各網域名稱註冊管理機構有權凍結或刪除網域名稱或終止網路相關服務。 若有法規授權及制定流程並有司法資源協助，則受理註冊機構凍結、刪除網域名稱或終止相關服務時較無爭議且較有能力即時防止更大損害。
研究團隊意見及歸納:	
有相關法源依據下，民間第三方專業機構通報或行政機關通報皆可。但業者執行 DNS RPZ 仍應以主管機關通知為宜。	

第四節 座談會

一、訪談目的

座談會目的
為聽取業者、第三方機構以及專家學者對本研究案之建議，辦理本次座談會，以期能了解業者實務上面對之問題，以及專家學者意見，互相交流以激盪出不同想法。

二、iWIN 意見

iWIN 意見整理
（一） iWIN 處理案件以兒少色情或有害兒少身心健康之內容為主，此種內容可有一定的範圍延伸，比如說詐騙不實訊息。若為農委會、疾病管制言論，則不在 iWIN 管轄範圍內。 （二） iWIN 就內容管理上原則上採取業者自律，業者若認為內容無違法疑慮者，可直接和 iWIN 反映，並無正式異議流程可言。另外自律標準已提供於官網供業者參考。 （三） 未來是否採取停止解析處理違法內容，除須有法律保留外，不同種類違法內

容何時應以停止解析處理，應由不同目的事業主管機關訂定。不過同時須考量機關標準不一致的可能。

（四） 未來是否要擴大 iWIN 職權，原則上是尊重主管機關意見。或可考慮成立多個類似 iWIN 之機構，以免單一機構處理所有內容有權力過大疑慮。

研究團隊意見及歸納

（一） iWIN 主要處理內容違法之案件，不處理技術濫用型案件，且 iWIN 採取業者自律模式為主，為第三方獨立機構。

（二） iWIN 認為，無論是否要以停止解析方式處理內容違法之網域名稱，須有法律保留，並可考慮依照內容類別由不同主管機關立法。另外亦可考慮成立多個類似 iWIN 之機構作為受理內容違法案件之機構。

三、業者意見

業者意見整理	
中華電信	網域名稱封鎖的技術難度小，現行實務較大問題為欠缺法律授權依據。另外請封鎖之情資品質亦重要，以免業者誤判導致合法網域名稱被停止解析。
台灣大哥大	停止解析就技術面而言不成問題，本公司也有在進行黑名單技術。實務問題在於，網路上過多詐騙網站，如果用停止解析的方式管理，會有從嚴認定無效率、從寬決定容易錯殺無辜。
亞太電信	本公司停止解析技術上沒問題，至於情資的品質好壞，則需投入時間去做判斷，業者面對的問題都很類似。
新世紀資通	本公司遭遇之問題為停止解析案件會重複收到來函，來自不同窗口但內容重複，通報流程及窗口建議統一。
網路中文	停止解析應有法源依據，且停止解析對於非 tw 網域名稱效果強烈，未來須考慮建立救濟管道。
鼎家數位	本公司認為立委在立法議題選擇上，會考量議題是否有投資報酬率。

研究團隊意見及歸納

（一）大多數業者均肯定停止解析技術上無問題，實踐上須有法律授權。

（二）多數業者困境為審查案件標準無從定奪，且情資來源不統一，或有情資品質不可靠之問題。

四、學者意見

（一）數位經濟暨產業發展協會 詹婷怡律師

專家意見

（一）若以網域名稱及 RPZ 作為研究對象，須了解層級化網路治理架構以及 Multi-stakeholders 機制，以及 DNS 在網路中之角色。並進一步釐清，DNS RPZ 原係處理技術濫用之手段。接著進一步討論用於處理內容領域之問題。

（二）進入網域名稱內容濫用之討論後，方有所謂立法政策及法院判斷問題。

（三）針對內容濫用進一步繼續討論設立第三方獨立機構審查網域名稱內容濫用，及其可以扮演如何的角色及其功能的有效性（與侷限性），對此 iWIN 具有相當參考價值。

（四）如內容領域得適用 DNS RPZ 停止解析，則是否僅限 RPZ 手段，在非 tw 網域名稱，網域名稱是否可能扣押也可進一步分析。

（五）各該社會、商業等行為所涉法令，各該主管機關法規調適必須同步與時俱進

研究團隊意見及歸納

（一）DNS RPZ 之使用從技術領域擴及討論到內容濫用領域。

（二）討論建置第三方機構處理內容濫用問題時，iWIN 具有參考價值。

（三）該主管機關法規調適必須同步與時俱進以解決網域名稱濫用問題

（二）世新大學 何吉森教授

專家意見

（一）iWIN 為成功典範，且突顯 ICANN 由下而上的業者自律精神，故 iWIN 值得複製借鏡。英國現針對網域名稱監理屬「共管」模式，由第三方機構分擔主管機關審查案件負擔。

（二）技術濫用案件是否交由 iWIN 負責，採保留看法。

（三）同意 RPZ 應作為最後手段，美國法民事扣押制度是否能引進我國，須再觀察。

研究團隊意見及歸納

iWIN 為成功典範，突顯 ICANN 由下而上的業者自律精神，不過不應要求 iWIN 負責技術濫用類案件。

（三）元智大學 葉志良教授

專家意見

（一）第三方機構定位應該為幫助業者自律之角色，且行使職權須有法律依據，內部亦須有檢核制度。

（二）不同種類內容之管制，應採單一立法或個別立法須再進一步觀察。技術濫用及內容違法案件亦應為不同模式處理。同時可考慮訂定急迫及非急迫兩套制度處理網域名稱濫用。

研究團隊意見及歸納

第三方機構應為幫助業者自律的角色，並須有法律依據。並認為不同案件類型應為不同處理方式，並可研擬急迫及非急迫案件處理流程。

（四）科技法律研究所 顧振豪副所長

專家意見

（一）以下整理分析幾個比較法制度：

1. 挪威係以刑事程序沒收（扣押）方式處理網域名稱濫用。
2. 比利時是透過政府機關經濟局，不沒收（扣押）網頁而係在中間跳出警告頁面，作為嚴重侵權案件的最後手段。
3. 英國近年停止網域名稱案件相當多，英國透過其他執法機構向註冊管理機構或是受理註冊機構通報，以網域名稱註冊人與受理註冊機構間契約進行辦理。

（二）關於扣押網域名稱之問題，我國的刑事訴訟法可沒收供犯罪之物，惟在實務上案例較少。ICANN 曾發布網域名稱扣押指引，或許可以做為我國刑事網域名稱扣

押之參考。我國亦可考慮以定暫時狀態假處分等方式扣押網域名稱。

研究團隊意見及歸納

各國針對不同類型之網域名稱濫用，有不能處理方式，可看出多為透過司法、行政或是民間自治方式處理網域名稱濫用問題。扣押網域名稱以我國現行法而言或許可行，惟未來仍待司法實務繼續發展。

（五）高雄科技大學 程法彰教授

專家意見

（一）馬尼拉原則實際上有課與平臺業者審查內容的責任，可考慮由通傳會訂立法律並擬定行政規則，以規範平臺業者。或者，可以行政指導方式，強化業者自律。

（二）認同 DNS RPZ 為最終手段。DNS RPZ 是否要利用在內容管制上，有賴未來司法實務上發展。

研究團隊意見及歸納

業者自律之重要性，並且認為平臺業者也有確保內容符合自律規範之責任。

五、問題與討論

	問題討論	業者/專家學者
一、	是否各領域主管機關要求刪除網域名稱內容或是停止解析時，於相關法規內應明文「限制我國網路使用者接取、瀏覽之措施或移除網頁內容」，以符合法律保留原則？	是，主管機關要求刪除網域名稱內容或是停止解析須符合法律保留
二、	是否各領域主管機關要求刪除技術濫用或是停止解析時須有相關法律，以符合法律保留原則？	1. RPZ 為限制網路接取的技術手段，原始目的為網域名稱系統服務提供的功能之一，以維持網路基

		礎設施運作。 2. ICANN 倡議 DNS Abuse Framework，作為技術之自律規範
三、	是否註冊管理機構（TWNIC）知悉或收受通知面對網域名稱濫用時，應自行認定是否違法？	建議由第三方機構協助認定是否構成網域名稱濫用
四、	以「停止解析」做為「網域名稱濫用」之處置手段應符合比例原則？	DNS RPZ 停止解析應作為網域名稱濫用處立之最後手段
五、	是否網域名稱內容濫用由第三方機構判斷網際網路內容是否存在違法或不當，再將相關資訊彙整通報給各主管行政機關、檢警單位及 ISP 業者？	建議可由第三方機構協助進行初步判斷網域名稱是否構成違法濫用
六、	是否針對停止解析等處分無法查明或難以送達網域名稱註冊人時，以「公告」代替送達？	座談會中無針對此進一步討論
七、	各業者於收到TWNIC停止解析特定網域名稱之指示後，是否有執行上之困難？	多數業者困境為審查案件標準無從定奪，且情資來源不統一，或有情資品質不可靠之問題。

第五節 小結

DNS RPZ 原始目的為網域名稱系統服務提供的功能之一，維持網路基礎設施運作，並多用於網域名稱技術濫用領域以維持網路基礎設施運作。近年討論此種技術是否也可以作為使網域名稱內容濫用之處置手段。從機關、業者及專家學者意見可知，DNS RPZ 用於網域名稱內容濫用屬最後手段，且 TWNIC 或 ISP 業者進行 DNS RPZ 時，基於涉及人民權利限制如為行政機關之來函，應有相關法律之授權；如為司法機關則應有法院裁定或判決。

網域名稱技術濫用基於部分濫用網域名稱可能影響基礎資訊安全或侵害他人權利，故有機關建議可以將 DNS RPZ 作為司法刑事制手段分為平時和緊急兩種制度，平時發動應遵守令狀原則，緊急時參考通訊保障監察法設計，先逕行停止解析，並有 24 小時之限制須補向法院請求裁定。另外按刑事警察局電信偵查大隊之實務經驗，若無法或難以追查刑事犯罪行為人，卻仍有停止解析特定網域名稱之需求，如出於資安考量而非箝制言論內容，可將停止解析程序定調為行政處分，如此可更有效率，且較無侵犯人權疑慮。

網域名稱內容濫用監理上，可分為兩種見解，第一種為建立起一個全權處理所有網域名稱管理及審查，並受理通報之機關；第二種為 iWIN 模式，即透過民間機構通報。多數專家學者肯定 iWIN 由下而上之監理模式，並認同業者自律。

業者表示，民間機構之通報或可做為行政機關處分之參考依據，且若民間機構具有權威性而得確保提供之情資正確性，業者願參考機構之專業判斷通知網域名稱註冊人有網域名稱濫用違法問題。惟若要求業者配合辦理 DNS RPZ，建議仍須有相應之法規命令其參考。除落實法律保留原則已明確業者應盡之作為外，業者亦得向受影響之客戶說明一切均係依法辦理，以杜絕註冊人與受理註冊機構間發生任何爭議。

第六章 網際網路規範觀察及分析建議

第一節 國外網路使用者行為及網域名稱內容濫用時，TWNIC 的應處機制

本章節針對外國人註冊使用網域名稱（如「.tw」、「.com」）架設網站，其網站內容或網路使用者行為涉違反我國法律時，TWNIC 的應處機制進行探討。

網站內容或網路使用者行為涉違反我國法律，現行我國法有移除網頁內容之相關規範，如兒童及少年福利與權益保障法第 46 條第 3 項，規範網路平臺提供者經目的事業主管機關告知網際網路內容有害兒童及少年身心健康時，網路平臺提供者有限制瀏覽或移除內容之義務；動物傳染病防治條例第 38 條之 3，規範網際網路內容涉及境外應施檢疫物之販賣至國內、輸入或其他檢疫相關事項，經輸出入動物檢疫機關公告者，廣告刊登者、平臺提供者、應用服務提供者或電信事業應依公告限制接取、瀏覽或移除相關網頁內容。

以下分析參考 TWNIC、受理註冊機構之與網域名稱註冊人間的合約，並參酌研究團隊訪談 TWNIC，獲悉身為註冊管理機關屬網路基礎設施建置者，無從自行審酌及直接介入網域名稱濫用，且處置手段有限且可能違反比例原則（如取消網域名稱），而使用 DNS RPZ 停止解析內容濫用之網域名稱需有法院判決/裁定或行政處分。又研究團隊訪談受理註冊機構及舉辦座談會，獲悉受理註冊機構皆有參與 TWNIC DNS RPZ 並可配合於接獲 TWNIC 通知後進行相關處置，且技術層面並無問題。以下將區分網域名稱使用「.tw」及「.tw 以外網域名稱」兩部分探討之。

一、 TWNIC 針對使用網域名稱「.tw」之應處機制

網域名稱「.tw」為台灣網域名稱註冊管理機構所受理註冊之網域名稱，因此 TWNIC 對於註冊人得依其服務條款及註冊人受理註冊機構間之合約等處理違反法律之網域名稱。

TWNIC 的網域名稱註冊管理業務規章第 25 條第 2 款註冊人應確

保註冊資料之真實性，且非以不正當目的註冊或使用該網域名稱。本條雖僅概括抽象地說明註冊人不應該有網域名稱濫用之行為，但其可作為 TWNIC 規範網域名稱濫用行為不論是技術或內容濫用之上位規定。相較具體之規範於 TWNIC 網域名稱申請同意書第 7 條規定，網域名稱註冊使用須確保其資訊防護措施之完備及安全，如因可歸責網域名稱註冊人之事由，足資影響他人權益或危害網路運作，TWNIC 於接獲相關機關通知後，得視情況暫停所註冊之網域名稱或為其他合理之處置。因此 TWNIC 有權限在接獲相關機關通知該網域名稱之使用者有如垃圾郵件、網路釣魚、殭屍網路等技術濫用該網域名稱時，TWNIC 有權將註冊網域名稱取消或是不再解析該網域名稱[272]。**然而該條對於網域名稱內容濫用部分之因應機制並未在同意書內定有明文，且「其他合理之處置」亦未於規章中具體明文**。

實際於第一線受理個人、企業註冊之受理註冊機構，其與網域名稱註冊人間亦有契約可為依憑。以 Hinet 的網域名稱委託申請書為例，其於第 1 條即規範網域名稱名申請、續用、移轉、讓渡、爭議等辦法依各註冊管理局規定，如.tw 之註冊管理局 TWNIC。因此本條款可作為與上位 TWNIC 規範之嫁接條文。此外，第 7 條亦**明文註冊申請人保證絕不以申請之網域名稱從事破壞網際網路和諧及違反國家法律之行為**，惟綜觀申請同意書，並無具體說明註冊人違法時可採取之應處措施。

另外參考亞太電信亦為受理註冊機構其『網域名稱/虛擬主機/企業郵件/HackerScan』服務條款之第三章服務使用規範即有網域名稱名濫用之相關規定。第 2 條明文註冊人**應遵守中華民國及國際間資訊、電信、證券交易、金融、專利、商標、著作權及其他相關法規**暨權利所有人在網路上之授權聲明，並自行承擔使用網路資源所衍生之一切

[272] 同意書第 9 條第 2 項規定：「除本同意書另有約定者外，註冊人涉有違反本同意書、網域名稱註冊管理業務規章及其相關規定者，TWNIC 得以書面或電子郵件通知註冊人，要求註冊人以書面敘明理由回覆。若註冊人於接獲通知三十日內，未能以書面檢具事證敘明正當理由或證明其並無違約情事者，TWNIC 得視情況暫停或取消其所註冊之網域名稱，或為其他合理之處置。」惟如對於技術濫用之類型是否需要再給註冊人 30 日陳述意見之機會非無疑問。

法律責任。第 3 條亦明文當註冊人有違反以下事由時亞太電信有權刪除該等內容資訊並終止註冊人之使用：(a)禁止入侵網路上任何系統、(b) 禁止破壞網路系統及各項服務、(c) 禁止擷取、使用、刊登非經所有者正式開放或授權之資源、(d) 禁止從事違反公共秩序、善良風俗、及法律所禁止之行為、(e) 禁止從事不法交易行為或張貼虛假不實、引人犯罪之訊息、(f) 禁止設立任何違反法令之網站或於網站中公然販賣槍枝、毒品、禁藥、盜版軟體或其他違禁物品、(g) 禁止從事涉及誹謗、恐嚇他人及任何不法侵害他人權利之行為、(h) 禁止傳輸或散佈電腦病毒、(i) 禁止提供賭博資訊或以任何方式引誘他人參與賭博。

上述事由幾乎涵蓋所有可能網域名稱濫用行為，因此當註冊人有網域名稱濫用行為時，亞太電信身為受理註冊機構其得終止服務以解決濫用問題，惟實務上，受理註冊機構並不會主動中斷網域名稱之代管服務，均係於接獲 TWNIC 或相關行政單位之指示，依指示停止服務。

綜上所述，註冊管理機構 TWNIC 對於「.tw」網域名稱濫用可以選擇最強烈之手段取消該網域名稱，或是選擇透過不再解析該網域名稱之方式[273]，使網路使用人不再接觸到該網站內容，如 31t.tw 一案即透過不再解析該網域名稱之方式處理[274]。TWNIC 亦可選擇透過通知受理註冊機構之方式，請求機構依其與註冊人間之合約條款解除契約，停止提供服務與註冊人，**惟不論是 TWNIC 或各受理註冊機構，均不會主動在行政機關要求處置特定網域名稱前為任何舉措，是以各領域主管機關於主管法律規範明確訂定處置機制及措施，如：「限制我國網路使用者接取、瀏覽之措施或移除網頁內容」，以符合法律保留原則更顯重要。**

[273] 於後具體討論台灣 DNS RPZ 政策模式。

[274] T.H. Schee，台灣國安單位封鎖 31t.tw 一案，https://blog.schee.info/2019/03/16/%E5%8F%B0%E7%81%A3%E5%9C%8B%E5%AE%89%E5%96%AE%E4%BD%8D%E5%B0%81%E9%8E%96-31t-tw-%E4%B8%80%E6%A1%88/（最後瀏覽日：2021 年 6 年 30 日）。

二、 TWNIC 針對使用網域名稱「.tw 以外網域名稱」之應處機制

ccTLD 種類約有兩百多種，而「.tw 以外網域名稱」如「.jp」或「.cn」等等即非 TWNIC 註冊管理機構所得直接依其規章，或是請求其下之受理註冊機構透過合約能加以解決。因此除請求其他註冊管理機構合作取消該網域名稱，如垃圾郵件、網路釣魚、殭屍網路等技術濫用時得依處理網域名稱濫用框架之相關規範通報 ICANN 以為處理，但對於內容濫用部分基於大部分註冊管理機構除收到具有可信之通知時，將兒少性虐待之素材、網路違法販售鴉片、人口販售，及具體且可信的煽動暴力之內容所使用之網域名稱取消外，則需透過法院命令始得對該網域名稱採取必要措施。因此對於「.tw 以外網域名稱」較有效之應處機制為 DNS RPZ 政策區域（DNS RPZ），是網域名稱系統服務器提供的功能之一，亦可以稱為「DNS 防火牆」。因有越來越多惡意程式及殭屍網路，RPZ 允許以自定義的資訊修改解析的結果後，再回傳給 DNS 客戶端，藉由修改查詢結果的方式，以防止駭客攻擊、或避免使用者訪問惡意網站，可作為資安防護的第一線防衛措施[275]。

RPZ 採取主從架構，當不當網域名稱或 IP 位址寫入主節點 DNS RPZ，所有參與 DNS RPZ 的次級節點會同時限制接取此不當網域名稱或 IP 位址 TWNIC 與國內 ISP 業者共同合作建構全台 DNS RPZ 服務架構，透過 DNS RPZ 服務架構限制接取的網域名稱不限於「.tw」網域名稱，尚包含境外惡意網域名稱[276]。台灣 DNS RPZ 架構如下圖：

[275] TWNIC，回應政策區域（Response Policy Zone, RPZ），https://blog.twnic.tw/2020/07/02/14020/（最後瀏覽日：2021 年 6 月 30 日）。

[276] 黃勝雄，DNS RPZ 摘要說明，https://blog.twnic.tw/2020/09/23/15311/（最後瀏覽日：2021 年 6 月 30 日）。

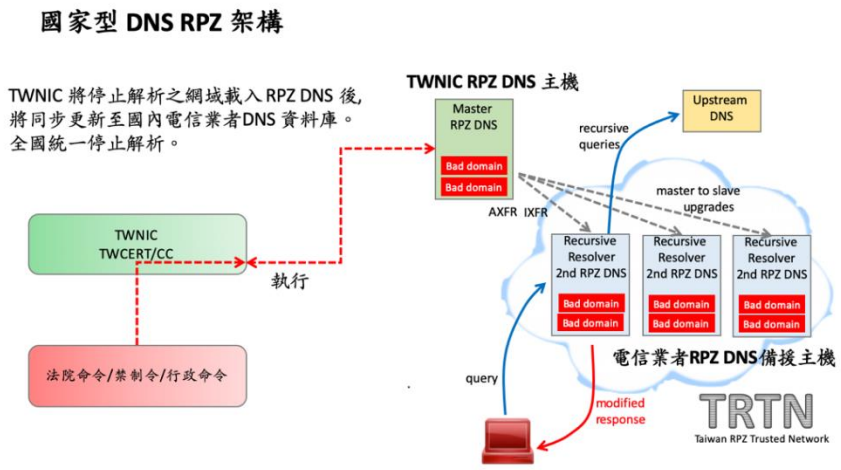


圖 21 國家型 DNS RPZ 架構

TWNIC DNS RPZ 防止國內使用者接取不當或惡意網域名稱，此可能涉及實質上剝奪台灣網路使用者閱覽、轉傳、分享網路資訊，涉及言論自由的限制。因此 TWNIC 以 DNS RPZ 限制惡意或不當網站必須有正當事由。正當事由可分為兩種類型，第一種類型為依據法律及因應法律規定所採取之行動，如兒童及少年福利與權益保障法第 46 條之 1 及動物傳染病防治條例第 38 條之 3 明文授權該管行政機關將經其認定為違法之網站內容為限制接取、瀏覽及移除。因此當有法院判決裁定或行政機關之行政處分時認定該網域名稱有內容濫用時，TWNIC 須配合停止解析該等網域。

另外如類型為網域名稱係有資安疑慮且影響資安重大者（技術濫用），即參考網域名稱濫用框架當註冊管理機構知悉有前述之網域名稱濫用情形時，註冊管理機構必須有所作為義務，因此當有危害資安之網域名稱濫用時，TWNIC 即須出面處理。

DNS RPZ 架構除針對「.tw」之網域名稱外，特別是針對「.tw 以外」之網域名稱名更具有效果，透過停止解析該網域名稱，使境內網路使用者不會再接觸到該違法和不當之網域名稱。惟 **DNS RPZ 技術有其侷限性，僅能限制透過特定快取主機連結網路之網路使用者連結特定網站，如網路使用者使用其他未加入 DNS RPZ 之快取主機（諸**

如：「Google DNS」）時，DNS RPZ 即無法作用，此外，當網路使用者使用國外 VPN 進行網路連結時，該使用者仍可連結上列入 DNS RPZ 之網站。

又是否需有必要另立法規或修法強制要求所有業者加入 TWNIC DNS RPZ，依目前我國實務運作 ISP 業者皆已加入 TWNIC DNS RPZ，並參與其建置。此外，目前我國實務 ISP 業者多同時又身兼受理註冊機構之角色，提供受理網域註冊服務，與 TWNIC 具有協力合作關係。又為符合由下而上之監理，避免行政機關過於介入監管之印象，應無特別另立法規或修法強制要求所有業者加入 TWNIC DNS RPZ 之必要。

第二節 網路內容或網路使用者行為違反我國法，TWNIC 之處置建議

本章節針對網際網路內容或網路使用者行為涉及違反我國法律時，TWNIC 之處置建議及精進作為進行探討。

就網際網路內容或網路使用者行為涉及違反我國法律之議題，應分為兩個層次探討，即一、如何認定網際網路內容/行為是否涉及不法，以及二、.後續如何透過執行手段處理不法網域名稱。研究團隊參酌訪談 TWNIC 獲悉其扮演網路基礎設施建置者角色，無從自行判斷網域名稱違法濫用與否，及參考網域名稱濫用框架，將網域名稱濫用區分為網域名稱技術濫用及網域名稱內容濫用，針對網域名稱技術濫用，註冊管理機構本於網路基礎設施建置者角色應有作為義務。然網域名稱內容濫用事涉專業判斷，建議委由第三方專業機構通知，或採行向網站管理者、註冊人或伺服器服務提供者尋求移除濫用內容之救濟方式，加以解決網域名稱內容濫用問題。參酌前述就一、如何認定網際網路內容/行為是否涉及不法，以及二、後續如何透過執行手段處理不法網域名稱，此二議題提出以下方向：

一、議題一：如何認定內容/行為是否涉及不法：

（一） 原則不應由註冊管理機構自行認定是否違法：

依我國網域名稱註冊管理機關即 TWNIC 與 ICANN 之合約，其並無義務負責監督、管理網域名稱之內容且也無權限審查網域名稱內容而取消網域名稱。此外依 TWNIC 於 2020 年 9 月 23 日發表其官方 DNS RPZ 簡要說明[277]所提到之「TWNIC DNS RPZ 架構」，TWNIC 亦僅限於兩情況時方得取消網域名稱名稱：（一）網域名稱係依法院判決/裁定或行政機關命令移除者及（二）網域名稱有資安疑慮且影響資安重大者；是以 TWNIC 並不自行判斷網際網路內容涉及不法。因此，目前註冊管理機構依法並無認定內容是否違法不當之權限。此外，註冊管理機構有無足夠資源如專業、人力得認定違法不當，亦須加以考量。

目前各國尚無由註冊管理機構自行認定是否內容違法之前例，如我國進一步由不具公權力的註冊管理機構認定網域名稱違法不當，將可能引發相關爭議。考量網域名稱內容濫用涉及多元議題及面向（例如兒少、國安等廣泛議題），宜另由司法、行政機關或專業機構負責認定（詳如下節）。

（二） 如擬由註冊管理機構負責認定違法，也應限縮於以「技術濫用」之違法為限：

如擬由註冊管理機構負責認定違法，則應以被認為有可能直接危害網際網路基礎結構的穩定性與安全性（如垃圾郵件、網路釣魚、殭屍網路等）等者為限（Technical Abuse）。

依網域名稱濫用框架，規定註冊管理機構得於特殊情況下（例如有關兒少性虐待之素材（Child Sexual Abuse Material）、網路違法販售鴉片（Illegal distribution of opioids online）、人口販售（Human trafficking）、煽動暴力）等，雖尚未收到法院命令，但獲得具有可信

[277] TWNIC 官方網站，https://blog.twnic.tw/2020/09/23/15311/ （最後瀏覽日：2021 年 6 月 30 日）。

度的通知時，可採取積極作為。惟目前網域名稱濫用框架所謂「積極作為」，並無明確定義。且此網域名稱濫用框架，並無直接轉化為內國法之效力，其在我國如何落實執行，仍須依循我國法律。考量註冊管理機構在我國尚無法定執法權限，基於法律保留原則，仍不建議逕由註冊管理機構自行認定網際網路內容有無違法。

（三） 於註冊管理機構知悉或合理懷疑網域名稱內容涉及不法情形時，應賦予其通報義務：

網域名稱濫用框架明確指出，當註冊管理機構知悉有上述之網域名稱濫用情形時，註冊管理機構必須有所作為。如採相同邏輯，於註冊管理機構知悉網域名稱內容涉及不法時，其雖不適合自行作成判斷，但也不應撒手不管而無積極作為。是以，建議可考慮賦予其通報義務，通知相關司法或行政機關。

（四） 於相關機構調查過程，可考慮賦予註冊管理機構配合調查或資訊提供之協力義務：

司法或相關行政機關啟動調查，為期能掌握時效及盡早查明事實，可考慮賦予註冊管理機構協力調查或資訊提供義務，如提供網域名稱申請人之個人資料。

（五） 為明確上開事項包含註冊管理機構之通報、協力調查義務，可考慮透過修改電信管理法第 71 條及相關子法、簽訂行政契約或行政指導之方式為之：

此外，就細部事項，則可考慮透過授權 NCC 制定相關行政命令（例如透過修訂網際網路位址及頂級網域名稱註冊管理業務監督辦法等）。此外，亦可考慮由 NCC 與註冊管理機構以簽訂「行政契約」或行政指導之方式，就細部事項為補充。

二、議題二：後續如何透過執行手段處理不法網域名稱：

（一） 註冊管理機構就經認定不法內容，應有配合執法之義務：

雖考量註冊管理機構性質，不宜由其自行認定網際網路內容是否涉及不法，但一旦經法院或專業機構判定內容確實涉及不法後，為確保可即時有效防止不法侵害情形，應賦予註冊管理機構配合執法之義務。

（二） 執行手段應符合比例原則，採取採取侵害較少之方式：

1. 就執法之手段，應考量其違法之情節，而依循比例原則，選擇適當之手段。舉例而言，如以禁用網域名稱之方式處理，在難以精準移除該網域名稱之濫用部份下（例如網路討論區、網路市集等情形），可能必須移除整個網站，甚至使非屬違法部分之內容也遭移除，即可能產生是否有執法過度而違反比例原則之爭議。
2. 是以，在作法上，註冊管理機構應優先考慮其他侵害較少之方式，如先行通知（可請求受理註冊機構協助通知）網域名稱濫用人及網域名稱註冊人請其將內容刪除，如無法聯繫上相關人員或於期限內無回應者，再行採取如拒絕提供解析服務、暫停提供服務、或依契約（例如申請書）通知註冊業者並與其協調等合乎比例原則之處理措施，而移除網域名稱將屬最後手段。
3. 以日本為例，依日本註冊管理機構 JPRS 亦認為，較好的方式是先請求網站管理人刪除該網頁內容，及較接近網路使用人負責傳輸與接收網路資訊之伺服器管理者與 ISP 業者協助處理較為妥當，而當前述機構及業者無法解決時，再由 JPRS 考量是否暫停該網域名稱，以符合比例原則。

（三） 明定註冊管理機構之執法原則（比例原則）及方式：

綜上，為協助註冊管理機構可選擇最適當之手段，即視情節優先採取通知、拒絕提供解析服務、採取暫停提供服務等措施。此外，為期明確，也可考慮在通傳會之網際網路位址及頂級網域名稱註冊管

理業務監督辦法明訂註冊管理機構之執法應符合比例原則，以及可採取之執法手段，俾利相關單位依法行政。

第三節 通傳會對頂級網域名稱註冊管理業務之監理機制調整之必要性

本章節針對通傳會依電信管理法對於頂級網域名稱註冊管理業務之現行監理機制是否有進行調整之必要性進行探討。以下區分兩部分，第一部分先研析目前通傳會對於頂級網域名稱註冊管理業務之監理機制，第二部分對目前監理模式提出調整可行性及調整方向。

第一項 現行監理機制係採低度監理，尊重網路業者自律

（一） 三種監理模式

各國電信管理機關對於註冊管理機構之監理，依監理密度，主要可分為三種模式如下表：

表 12 世界網域名稱內容濫用之監理模式

模式	模式一：利害關係人及民間主導	模式二：註冊管理機構與國家簽訂契約	模式三：透過法律規範
優點	避免政府被認為干預網路及言論自由	避免政府被認為干預網路及言論自由	1. 大眾可以清楚知悉規範內容 2. 行政處分流程、法律依據清楚明確
缺點	管理規範不透明	1. 部分內容無法透過契約方式規範 2. 對國民於透明性上仍可能有所不足	政府可能被認為干預網路及言論自由
監理密度	低	中	高

（二） 依電信管理法第 71 條，我國目前對註冊管理機構監理模式係採「低度監理」（介於模式一至模式二）

依我國現行電信管理法第 71 條規定：「一、網際網路位址或網際網路頂級網域名稱註冊管理服務，應由法人組織辦理。二、提供網際網路位址或網域名稱註冊管理服務之國家級網際網路位址註冊管理機構或國碼網際網路頂級網域名稱註冊管理機構，應訂定業務規章，並送主管機關備查。三、網際網路頂級網域名稱足以表徵我國者，該網域名稱註冊管理機構應訂定業務規章，供主管機關查核。四、從事第一項業務者之資格、條件、申請程序、方式、業務規章應記載事項、委託辦理註冊業務、行政管理及其他應遵行事項之辦法，由主管機關定之；其相關輔導措施之辦法，由行政院指定機關定之。主管機關為辦理網際網路位址及網域名稱註冊管理事項，得與國際組織進行協商及交流合作。」

查通傳會依電信管理法第七十一條第四項，業已訂定「網際網路位址及頂級網域名稱註冊管理業務監督辦法」。惟辦法內容僅規定註冊管理機構應訂定業務規章並報請備查，並未明文規定註冊管理機構對於網際網路不法內容之處理方式。是以，本研究認為，在現行電信管理法之架構下，目前通傳會對於註冊管理機構之監理模式應是介於上揭三種模式之模式一至模式二間，即採低度之監理模式。在保障言論自由為普世共通價值下，通傳會目前之監理方式，應符合法治國原則，且與國際多數國家作法相符。

（三） 依網際網路位址及頂級網域名稱註冊管理業務監督辦法對受理註冊機構進行監管

依網際網路位址及頂級網域名稱註冊管理業務監督辦法第 9 條第 1 項：「頂級域名註管機構得**委託受理註冊機構分配網域名稱予註冊人**；網路位址註管機構得委託網路位址代理發放機構分配網際網路位址予註冊人。」是以註冊管理機構得與受理註冊機構簽訂契約，委由受理註冊機構將網域名稱分配與註冊人。此外，依同條第 2 項：「國碼頂級域

名註管機構應於委託契約生效之次日起十日內，**將受理註冊機構名單報請主管機關備查**。」是以通傳會得掌握註冊管理機構與受理註冊機構間之關係及具體受理註冊機構之家數及名單。

受理註冊機構與註冊管理機關之權利義務，則依雙方簽訂之契約為依循。以 TWNIC 網域名稱受理註冊授權合約為例，其明定雙方之權利義務關係，及 TWNIC 對受理註冊機構有監督權限，第 3 條第 6 項明文要求受理註冊機構於合約期間應維持中立、公正及專業之形象，不得有任何有損於註冊管理機構及受理註冊機構聲譽之行為，亦不得有任何破壞網路秩序之行為。此外第 11 條明文 TWNIC 之考核權限，第 11 條第 1 項明文：「TWNIC 得不定時針對受理註冊機構進行抽檢，若其條件不符時，應要求其提出書面改善報告，且須於三十日內完成改善。若屆時仍無法改善，方得解除或終止合約，收回所有註冊者之相關資料，並得請求損害賠償」；第 3 項明文：「TWNIC 考核結果發現瑕疵時，受理註冊機構應依 TWNIC 指示，於限期內改正。如有嚴重瑕疵，致影響受理註冊機構或 TWNIC 業務之執行者，TWNIC 得即時暫停受理註冊機構之授權，限期改正。逾期不改正，甲方得終止合約。」。

由上可知，通傳會對於受理註冊機構屬於低度監理，將受理註冊機構名單予以備查。具體對受理註冊機構之監管，則為由受理註冊機構與註冊管理機關雙方簽訂之契約為依循。

第二項　目前監理模式調整可行性之思考方向

研究團隊參酌網域名稱濫用框架（詳細說明見第二章第三節），及研析外國法制知悉日本面對網域名稱內容濫用之監理，主要透過民間第三方機構 SIA 進行接受民間通報，自行審酌網域名稱涉有違法、不當，轉交業者進行後續處置。此種民間由下而上之自治模式，深受座談會與會專家學者肯認。

此外研究團隊透過訪談我國民間第三方機構 iWIN，知悉其透過接

受民間通報轉送業者、行政機關之模式，有效解決我國有害兒童身心之網域名稱內容濫用，且其模式係可被複製使用於其他網域名稱內容。

又研究團隊透過訪談 TWNIC 及座談會與會專家學者之意見，知悉 DNS RPZ 源係用於處理網域名稱技術濫用，而近年被討論是否得用於處理網域名稱內容濫用，而作為網域名稱內容濫用之處置手段，因涉及箝制網路言論之疑義，故由法院之判決/裁定，或是行政機關經法律授權作成行政處分，加以啟動 DNS RPZ 機制更顯重要。由上述分析及研究，提出以下之思考方向：

1. 參考日本作法，針對網域名稱內容濫用由第三方機構判斷內容是否存在違法或不當，再將相關資訊彙整通報給各主管行政機關、檢警單位及 ISP 業者等，並由各機關自行判定及處置：

以日本為例，即係由第三方之專業機構 SIA 負責接受民眾及網路使用者通報網域名稱內容違法及不當者為，而非註冊管理機構 JPRS，亦非通訊傳播之主管機關。此外，SIA 係依相關法規之違法要件及態樣訂立「安全線運用指引」[278]，針對網路內容區分為內容違法及內容不當。「內容不法」係指該內容存在於網路上使公眾得閱覽有違反相關法規；「內容不當」係指雖大眾得閱覽之內容雖不違法，但其可能引起違法行為，或是其有為公眾所皆知極重大問題。上述透過先由專業機構認定網域名稱內容濫用之作法，除可確保有較足夠之人力及專業進行第一線審查，並立即通報平臺業者、伺服器業者及 ISP 業者，使其可盡速聯繫網域名稱註冊人或立即為相關處置。其後再由行政機關進行第二線審查及追蹤，對違反相關法律之行為人進行行政裁罰及警檢調查。SIA 運作成效以 2019 年為例，SIA 提出 21,183 件請求 19,540 件網頁內容被刪除（約 92%）絕大多數個案在刊載違法不當之網頁管理者或是伺服器管理者、網路平臺業者即將網頁內容刪除。

[278] 同註 115。

目前我國有關網路內容涉及侵害兒少身心之申訴及處理，係由 iWIN 負責，其處理範圍涵蓋六大類，並依內容呈現程度設有不同之標準，六大類別茲羅列如下[279]：

a 色情

整個網站、網路文章或網路影片所呈現出的內容與傳遞的訊息，涉及未成年的裸照、未成年遭受性剝削的內容、性行為、性暗示、媒介性交易的資訊或是具有性暗示意涵等內容，皆屬色情的範疇。

b 暴力

整個網站、網路文章或網路影片所呈現出的內容與傳遞的訊息，涉及性侵害或性虐待他人、殺害或虐待人類/動物、自我傷害（例如直播自殺畫面、張貼割腕自殘的照片等）、或是暴力兇殘的畫面（例如幫派械鬥的畫面）等，這些都屬於暴力的範疇。

c 恐怖

恐怖的前提是要大多數的民眾都會感到驚嚇、不安等心裡不舒服的狀，整個網站、網路文章或網路影片所呈現出的內容與傳遞的訊息，涉及人類/非人類的死亡狀況或屍體狀態、天災人禍等災難現場的狀況且有人類因此受有傷害、或是與鬼怪靈異等超自然現象有關的內容皆屬恐怖的範疇。

d 血腥

血腥的係指大多數的民眾都會感到心裡不舒服的內容，才是血腥所要處理的範疇，而當整個網站或網路影片所呈現出的內容，涉及血液，或是身體器官內臟、手腳四肢的受傷、損害等內容皆屬之。

[279] iWIN 網路內容防護機構，申訴類型說明，https://i.win.org.tw/appeal.php?Target=3 （最後瀏覽日：2021 年 10 月 6 日）。

e　有害物品

生活中有部分物品並不適合未成年的兒少接觸，為了避免引起未成年人接觸的慾望，或是進一步保護未成年人本身，整個網站、網路文章或網路影片所呈現出的內容與傳遞的訊息，涉及菸（例如未成年抽菸）、酒（例如未成年飲酒）、檳榔（例如未成年吃檳榔）、毒品（例如販賣毒品、教導如何吸毒）、管制藥物（例如販售未取得食藥署認證的藥品）、槍械、刀械、爆裂物等內容，皆屬有害物品的範疇。

f　其他違反有害兒少身心健康內容

網路上資訊非常多元，無法單用幾種類型就能涵括完畢。此類型所涵蓋色情、暴力、恐怖、血腥及有害物品外其他內容，以及受理申訴的 iWIN 團隊經常收到的申訴類型，如當整個網站、網路文章或網路影片所呈現出的內容與傳遞的訊息，涉及歧視他人、仇恨言論、洩漏或揭漏他人的個人資料（例如電話號碼、地址等）、賭博資訊（例如線上賭博網站），或是其他不適合未成年進行的活動等，皆屬之。

未來可考慮進一步擴張 iWIN 之業務範圍及權能，或另外新設專業機構認定傳染病防治、婚姻媒合、日租套房等網域名稱內容違法不當問題。此外，如認有網域名稱涉及違法時，可逕通知檢警進行調查。

2. 面對網域名稱技術濫用，建議有明確立法授權以便行政機關及註冊管理機構處理濫用網域名稱

網域名稱濫用框架已針對網域名稱濫用定義五種類型包含：一、惡意軟體（Malware）；二、殭屍網路（Botnets）；三、網路釣魚（Phishing）；四、偽冒嫁接（Pharming）；五、以垃圾郵件之形式達成以上濫用之行為（Spam），而幾乎涵蓋所有技術濫用類型。此外，網域名稱濫用框架明確指出，當註冊管理機構知悉有前述之網域名

稱濫用情形時，註冊管理機構必須有所作為，如依據註冊管理機構與 ICANN 之合約維持網域名稱濫用之聯絡窗口以利接收網域名稱濫用之投訴並盡速調查該濫用之情形。是以註冊管理機構針對技術濫用網域名稱有作為義務，然而作為義務及處置手段於我國法多未有明文。

又技術濫用多涉及無故輸入他人帳號密碼、破解使用電腦之保護措施或利用電腦系統之漏洞，而入侵他人之電腦或其相關設備者，可構成妨礙電腦使用罪章之相關犯罪，而啟動刑事偵查程序。然而檢、警單位多係於接獲通報後方開始進行偵辦，此時多已有實害發生，可能緩不濟急。此外，網路犯罪嫌疑人及機房等往往所在不明，故時常無法比照刑事扣押處分方式避免第三人受害。

由上可知，實有需要針對網域名稱技術濫用有法律授權使主管機關及註冊管理機構得快速取消技術濫用網域名稱及透過 RPZ 停止解析手段，使國人免於成為網域名稱技術濫用下之受害者。相關立法方向如於「資通安全管理法」增訂：「網際網路平臺提供者，經目的事業主管機關告知資通系統及資通服務有違反資通安全政策或保護措施失效之狀態發生，影響資通系統機能運作，構成資通安全政策之威脅，應為限制我國網路使用者接取、瀏覽之措施，或先行移除。」，具體請詳見本章第五節網域名稱技術濫用表格。

3. 各領域主管機關應於其主管法規內，針對網域名稱內容涉及違法情事訂立「限制接取、瀏覽之措施，或先行移除」，以符合法律保留原則。

盤點我國目前可用於規範網際網路內容或使用者行為違法態樣之規定，僅有兩條規定明文授權該管行政機關將經其認定為違法之網站內容為**限制接取、瀏覽，甚至是移除之措施，上述規定，**分別是**兒童及少年福利與權益保障法第 46 條之 1 及動物傳染病防治**

條例第 38 條之 3[280]。是以，如行政機關欲通知網域名稱註冊管理機構就違反其餘規定（諸如：公職人員選舉罷免法、毒品防制條例）等實體法之網域名稱為限制一般人民閱覽之行政處分時，並無明確之法律依據。

網域名稱內容違法態樣眾多如婚姻媒合、日租套房、傳染病防治等，而相關事業主管機關多會發函請求通傳會將相關網域名稱內容移除。然而除發函之機關請求將網域名稱內容移除或停止解析無明確之法律依據外，各主管機關應參考動物傳染病防治條例第 38 條之 3 或是兒童及少年福利與權益保障法第 46 之執行模式，由相關目的主管機關逕發函通知行為人、註冊管理機構、受理註冊機構及 ISP 者，以達到權責相符。

4. 綜上，為兼顧網域名稱註冊者權益及言論自由保障，及遵循馬尼拉原則、網域名稱濫用框架等國際共通之網域名稱爭議處理準則，提出上述三個監理方向，供未來網域名稱濫用之監理制度設計，以期待能兼顧並保護網域名稱註冊者、網路使用人之權益。

第四節 網路內容或網路使用者行為違法，機關對 TWNIC 做成行政處分之程序及要件

如行政機關擬依職權針對網域名稱註冊管理機構以作成行政處分之方式作為監管手段，為符合依法行政及正當法律程序原則，建議應就以下事項納入評估

一、 行政機關作成行政處分之法源依據：

（一）依行政程序法第 92 條：本法所稱行政處分，係指行政機關就公法上具體事件所為之決定或其他公權力措施而對外直接發生法律效果之單方行政行為。目前通傳會對於網域名稱之管理，主要

[280] 該法規範廣告刊登者、平臺提供者、應用服務提供者或電信事業加註有關宣導防疫或檢疫之必要警語，保存刊登者、販賣者或訂購者個人資料，或定期提供予輸出入動物檢疫機關，並針對違法內容要求限制接取、瀏覽或移除相關網頁內容。

係見於電信管理法第 71 條，並搭配同法第 80 條第 1 項第 12 款之罰則。

（二）依目前法律規範，除兒童及少年福利與權益保障法及動物傳染病防治條例外，並無其他條文具體明確授權行政機關得就網際網路內容或網路使用者行為違法時作成任何處置。是以，未來應區分各行政機關管轄之內容，以法規分別授權各主管機關為行政處分之法源依據。

（三）此外，在法律明確性原則之要求下，建議一併就行政機關得作成行政處分之違法態樣、條件等一併敘明，搭配相關技術性、細節性事項授權行政機關制定行政命令以為補充。

二、 網域名稱註冊人陳述意見機會：

（一）依行政程序法，作成處分前，原則應先給予受處分所影響者陳述意見機會（行政程序法第 102 條）。行政程序法第 102 條規定：「行政機關作成限制或剝奪人民自由或權利之行政處分前，除已依第三十九條規定，通知處分相對人陳述意見，或決定舉行聽證者外，應給予該處分相對人陳述意見之機會。但法規另有規定者，從其規定」。

（二）依上，未來如行政機關就網際網路內容/行為是否不法作成行政處分，則須踐行上開行政程序法第 102 條之規定。雖從形式以觀，註冊管理機構或受理註冊機構為負責執行限制接取行為者，故網站所有人或內容之創作者並非直接處分對象，僅屬利害關係人。但本研究認為，從實際網站受限制接取之移除者來看，行政處分之對象應為網站所有人或內容之創作者，至於為限制接取行為之註冊管理機構或受理註冊機構，則僅為行政助手，如按此解釋，則在處分作成前似應給予「網站所有人或內容之創作者」陳述意見機會。

（三）惟針對影響網路使用安全之帶有病毒網域名稱之急迫情況，以

及網域名稱註冊人位於國外，顯然不能遵行陳述意見程序之情形下，對此可參酌行政程序法第 103 條第 2 款：「情況急迫，如予陳述意見之機會，顯然違背公益者」以因應須立即將網域名稱停止解析或內容下架，以避免情勢更為嚴峻(如散播病毒、釣魚等)；同法第 3 款：「受法定期間之限制，如予陳述意見之機會，顯然不能遵行者。」以因應網域名稱註冊人之聯繫資料顯為造假，致聯繫上註冊人顯有困難，或難以趕上做成處分之期限；同條第第 5 款：「行政處分所根據之事實，客觀上明白足以確認者。」以因應網域名稱內容明顯違反相關法律（如網頁內容涉及兒童情色、毒品販賣等)。

三、 送達及通知行政處分決定

（一）依行政程序法第 100 條：「書面之行政處分，應送達相對人及已知之利害關係人；書面以外之行政處分，應以其他適當方法通知或使其知悉。一般處分之送達，得以公告或刊登政府公報或新聞紙代替之。」。依上，因網域名稱註冊人為行政處分之相對人，依法亦應就書面結果告知該利害關係人。

（二）容有疑問者，為在網路高度匿名、無國界之特性下，如何知悉利害關係人之身分，以及如何執行後續之通知送達。為解決此部分問題，在執行面上，通傳會可要求註冊管理機構及受理註冊機構在與網域名稱註冊人之同意書上，同意以受理註冊機構作為送達代收人，一經送達即生效力。或是可透過立法於相關法規增修「無法查明行為人之送達，得以公告方式為之。」以解決此問題，相關具體說明可參見第陸章第五節。

第五節 網域名稱濫用監理機關，各領域增修立法例

研究團隊透過訪談 TWNIC 及座談會與會專家學者之意見，知悉 DNS

RPZ 源係用於處理網域名稱技術濫用，而近年被討論是否得用於處理網域名稱內容濫用，而作為網域名稱內容濫用之處置手段，因涉及箝制網路言論之疑義，故由法院之判決/裁定，或是行政機關經法律授權作成行政處分，加以啟動 DNS RPZ 機制更顯重要。

我國目前可用於規範網際網路內容或使用者行為違法態樣之規定，僅有兩條規定明文授權該管行政機關將經其認定為違法之網站內容為限制接取、瀏覽，甚至是移除之措施，上述規定，分別是兒童及少年福利與權益保障法第 46 條及動物傳染病防治條例第 38 條之 3。是以，如行政機關欲通知網域名稱註冊管理機構就違反其餘實體法規定（諸如：公職人員選舉罷免法、毒品防制條例等），而以要求刪除內容、取消網域名稱或是停止解析等行政處分或第三方機構進行受理通報及處理時，並無明確之法律依據。各法規主管機關可依下流程圖檢視主管法規有無修正之必要：

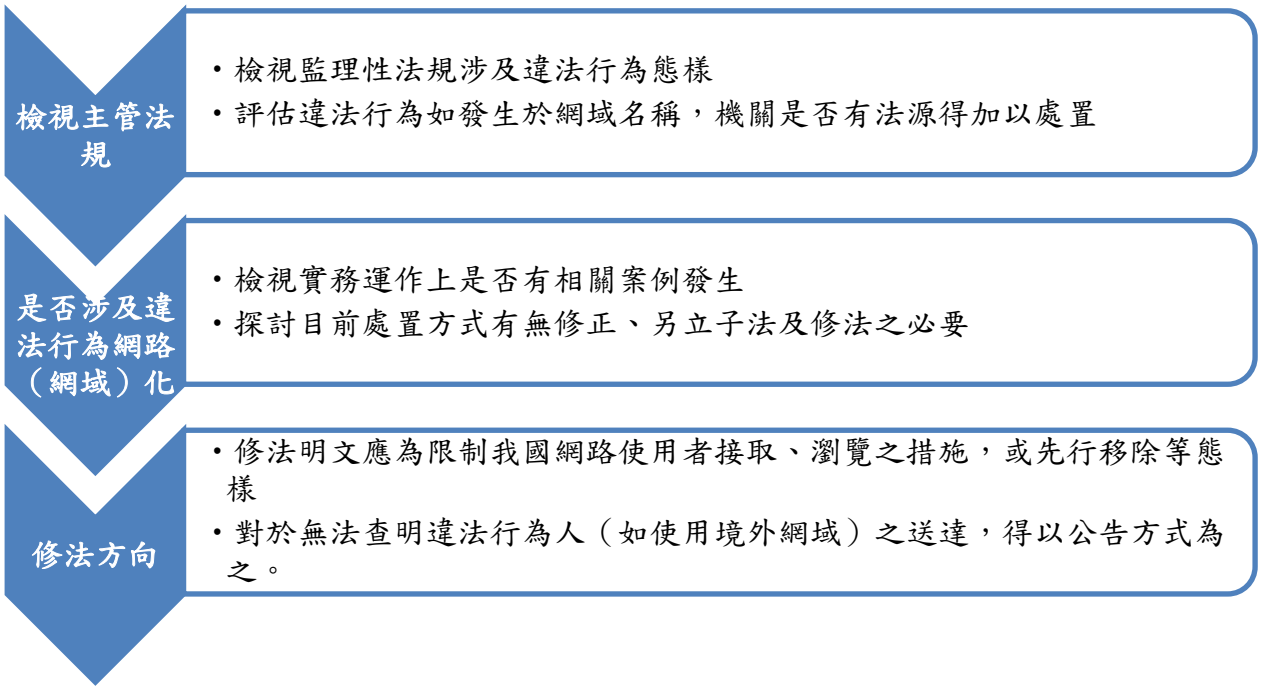


圖 22 主管法規檢視流程圖

此外，於特定領域具平臺業者，則可參考動物傳染病防治條例第 38 條之 3 的立法模式，要求平臺業者加註必要警語，保存刊登者個人資料。又對於經認定屬違法濫用之網域名稱及內容，未配合協助主管機關進行限制接

取、瀏覽或移除相關網頁內容之措施者，得參考兒童及少年福利與權益保障法及動物傳染病防治條例之立法方式課予網路業者罰鍰。此時罰鍰具怠金性質，即督促未配合之業者進行限制接取、瀏覽或移除內容等作為，而非針對網域名稱內容濫用之出現而處罰網路業者，故非使網路業者須對網路使用者產生之內容負擔責任，併敘明之。

以下整理相關常見網域名稱濫用情形、涉及對言論限制情事及其相對應的法規，並以表格呈現方便讀者閱讀：

一、網域名稱技術濫用

	現行	**增訂規定**
主管機關	檢、警單位之刑事調查	行政院資通安全處 參酌網域名稱技術濫用犯罪之目的係以獲取網路使用者之個人資料，爰於「資通安全管理法」增訂如下規定。
實體規定	刑法妨礙電腦使用罪章	於「資通安全管理法」增訂：「平臺提供者、應用服務提供者或電信事業，經目的事業主管機關告知資通系統及資通服務有違反資通安全政策或保護措施失效之狀態發生，影響資通系統機能運作，構成資通安全政策之威脅，應為限制我國網路使用者接取、瀏覽之措施，或先行移除。」
程序規定	刑事訴訟程序	行政機關所為行政處分應符合行政程序法，惟考量違法病毒網站所有人不明之情況下，於「資通安全管理法」增訂「對於無法查明違反資通安全政策之行為人之送達，得以公告方式為之。」
困境暨解決方式	檢、警單位係於接獲通報後方開始進行偵辦，多已有實害發生。	1. 由行政機關作成行政處分，針對情況急迫程度，及是否屬於境外網域名稱，考量使用 DNS RPZ 技術停止解

	犯罪人不明，無法比照刑事扣押處分避免第三人受害。	析該違法網站，以解決網域名稱技術濫用問題。 2. 基於病毒散播之快速及量大，非由行政機關所能一一作成處分。故得立法授權註冊管理機構、受理註冊機構或 ISP 等業者自行處置，並報主管機關備查。 3. 對於同時構成犯罪之網域名稱技術濫用，亦可考慮於警察職權行使法中授權警察得即時為相對應之處置。
違憲風險	<u>無</u>違憲風險，本團隊建議訂定，理由如下： • 網域名稱技術濫用不涉「言論自由」之表達 • 確保安全之網路使用環境之公益性極高	

二、刑事規定之犯罪行為：著作、商標

	現行	**增訂規定**
主管機關	檢、警單位之刑事調查	經濟部智慧財產局 參酌美國「Operation in Our Sites」，就違反商標、著作權之違法網站，迅速以民事程序下架。
實體規定	著作權法、商標法之刑事罰則	於「著作權法」增訂： 「平臺提供者、應用服務提供者或電信事業，經著作權人、製版權人或目的事業主管機關通知其使用者涉有侵權行為後，應立即為限制我國網路使用者接取、瀏覽之措施、先行移除或使他人無法進入該涉有侵權之內容或相關資訊。」 於「商標法」增訂： 「平臺提供者、應用服務提供者或電信事業，經商標權人或目的事業主管機關通知其使用者涉有侵權行為後，應立即為限制

		我國網路使用者接取、瀏覽之措施、先行移除或使他人無法進入該涉有侵權之內容或相關資訊。」
程序規定	刑事訴訟程序	行政機關為行政處分應符合行政程序法，惟考量違法網站所有人不明之情況下，於「著作權法」、「商標法」增訂「對於侵害著作權／商標權之行為人之送達，得以公告方式為之。」
困境暨解決方式	檢、警單位係於接獲通報後方開始進行偵辦，多已有實害發生。 犯罪人不明，無法比照刑事扣押處分避免第三人受害。	1. 目前我國著作權法第 90 條之 4 以下訂有網路服務提供者之避風港條款，故業者多願意配合將違反著作權之內容刪除。惟對於境外網域名稱難以要求配合刪除違法內容等情事發生時，有使用 DNS RPZ 停止解析之需求。 2. 另外對於商標法並無如同著作權法有避風港等相關規範，為避免侵害商標權內容持續呈現於網路上，有使用 DNS RPZ 停止解析之需求。 3. 透過立法修訂行政機關為行政處分，得及時以 DNS RPZ 技術封鎖該違法網站，解決現行無法規允許 TWNIC 將特定違法內容網站以 DNS RPZ 遮蔽之行為。
違憲風險	違憲風險**低**，本團隊建議訂定，理由如下： • 違反刑事法規，縱涉及「保障之言論」，亦為低價值言論 • 我國已有違反著作權法而扣押「特定網站」之案例 • 參酌美國法「Operation in Our Sites」，有類似規定	

三、刑事規定之犯罪行為：賭博、猥褻

	現行	增訂規定
主管機關	檢、警單位之刑事調查	衛生福利部
實體規定	刑法賭博罪章	現行得依照「兒童及少年福利與權益保障法」第 46 條第 3 項之規定停止該網域名稱之解析。故毋庸增訂實體規範。
程序規定	刑事訴訟程序	所為行政處分應符合行政程序法，惟考量違法網站所有人不明之情況下，於「兒童及少年福利與權益保障」增訂「對於無法查明散布有害兒童及少年身心健康行為人之送達，得以公告方式為之。」
困境暨解決方式	檢、警單位係於接獲通報後方開始進行偵辦，多已有實害發生。 犯罪人不明，無法比照刑事扣押處分避免第三人受害。	由行政機關為行政處分，得及時以 DNS RPZ 技術封鎖該違法網站，得解決現行無法規允許 TWNIC 將特定違法內容網站以 DNS RPZ 遮蔽之行為。
違憲風險	違憲風險**低**，本團隊建議訂定，理由如下： • 違反刑事法規，縱涉及「保障之言論」，亦為低價值言論 • 我國已有違反著作權法而扣押「特定網站」之案例 • 針對「兒童色情內容」，日本亦以遮蔽網域名稱之方式進行處理。	

四、不涉及刑事犯罪：動物傳染病防治

	現行	增訂規定
主管機關	行政院農業委員會	行政院農業委員會
實體規定	動物傳染病防治條例	現行得依照「動物傳染病防治條例」第 38 條之 3 第 3 項之規定停止該網域名稱之解析。故無庸增訂。

程序規定	行政程序法	所為行政處分應符合行政程序法，惟考量違法網站所有人不明之情況下，於「動物傳染病防治條例」增訂「對於無法查明發布境外應施檢疫物之販賣至國內行為人之送達，得以公告方式為之。」
困境暨解決方式	針對非使用境內網際網路平臺等難以取得廣告刊登者之個人聯繫資料時，內容刪除及停止解析網域名稱之處分將難以送達廣告刊登者	由行政機關為行政處分，得及時以 DNS RPZ 技術封鎖該違法網站，得解決現行無法規允許 TWNIC 將特定違法內容網站以 DNS RPZ 遮蔽之行為。
違憲風險	違憲風險**低**，本團隊建議訂定，理由如下： • 縱無涉及刑事法規，商業性言論亦屬低價值言論 • 保障國民之健康，公益性極高	

五、不涉及刑事犯罪：婚姻媒合

	現行	**增訂規定**
主管機關	內政部移民署	內政部移民署
實體規定	入出國及移民法第 58 條	於「入出國及移民法」增訂： 「網際網路平臺提供者，經目的事業主管機關通知其使用者涉有廣告物、出版品、廣播、電視、電子訊號、電腦網路或以其他使公眾得知之方法，散布、播送或刊登跨國（境）婚姻媒合廣告，應立即為限制我國網路使用者接取、瀏覽之措施、先行移除或使他人無法進入該涉有侵權之內容或相關資訊。」
程序規定	行政程序法	所為行政處分應符合行政程序法，惟考量違法網站所有人婚姻媒合廣告行為人之送達，得以公告方式為之。」

困境暨解決方式	同前	由行政機關為行政處分，得及時以 DNS RPZ 技術封鎖該違法網站，得解決現行無法規允許 TWNIC 將特定違法內容網站以 DNS RPZ 遮蔽之行為。
違憲風險	違憲風險**中**，本團隊建議訂定，理由如下： • 縱無涉及商業性法規，商業性言論亦屬低價值言論 • 婚姻不得計價原則及善良風俗之確保，惟公益性較低 • 容易違反比例原則，DNS RPZ 技術無法單純遮蔽違法廣告 • 律師倫理法開放以廣告推廣業務	

六、不涉及刑事犯罪：日租套房違反廣告

	現行	**增訂規定**
主管機關	交通部觀光局	交通部觀光局
實體規定	發展觀光條例第 55 條第 4 項	於「發展觀光條例」增訂： 「網際網路平臺提供者，經目的事業主管機關通知其使用者涉有未依本條例領取營業執照而經營觀光旅館業務、旅行業務或觀光遊樂業務者或領取登記證而架設網站或刊登廣告，應立即為限制我國網路使用者接取、瀏覽之措施、先行移除或使他人無法進入該涉有侵權之內容或相關資訊。 」
程序規定	行政程序法	所為行政處分應符合行政程序法，惟考量違法網站所有人非法日租套房廣告行為人之送達，得以公告方式為之。」
困境暨解決方式	處分送達問題	由行政機關為行政處分，得及時以 DNS RPZ 技術封鎖該違法網站，得解決現行無法規允許 TWNIC 將特定違法內容網站以 DNS RPZ 遮蔽之行為。
違憲風險	違憲風險**略高**，本團隊建議訂定，理由如下：	

	• 縱無涉及商業性法規，商業性言論亦屬低價值言論 • 確保旅客安全之公益性高 • 容易違反比例原則，DNS RPZ 技術無法單純遮蔽違法廣告

七、假消息

	現行	增訂規定（不建議增訂）
主管機關	檢、警單位之刑事調查	行政院內政部
實體規定	誹謗罪、妨害信用罪、妨害工商交易罪、意圖使候選人當選或不當選罪、違反商業競爭秩序罪、傳染病防治法第 63 條散布疫情不實訊息、行政秩序維護法	刑事法中不適合加入行政手段，爰將遮蔽謠言網站之規定於「社會秩序維護法」，增訂內容如下： 「網際網路平臺提供者，經目的事業主管機關通知其使用者涉有散佈謠言之行為後，應立即為限制我國網路使用者接取、瀏覽之措施、先行移除或使他人無法進入該涉有侵權之內容或相關資訊。」
程序規定	刑事訴訟程序、行政裁罰	行政機關所為行政處分應符合行政程序法，惟考量違法網站所有人不明之情況下，於「社會秩序維護法」增訂「對於散布不實謠言之行為人之送達，得以公告方式為之。」
困境暨解決方式	對不實言論為即時處理，屬行政處分之範疇，宜於行政法規中訂定之	由行政機關為行政處分，得及時以 DNS RPZ 技術封鎖該違法網站，得解決現行無法規允許 TWNIC 將特定違法內容網站以 DNS RPZ 遮蔽之行為。
違憲風險	違憲風險**高**，本團隊不建議訂定，理由如下： • 「散布不實言論」之定義過於模糊，違反法明確性原則 • 縱違反刑事法規，按照近期言論，被認定為假消息多屬「高價值」之「政治性」言論 • 不實言論多為刑事法規，不適宜放入「即時停止解析」之規定 • 此規定方式勢必會面臨「過度侵害言論自由」之評價	

八、監理性法規法律分析綜合整理

	網路安全領域	刑事實體法已規定之犯罪行為	不涉刑事犯罪之行為			爭議領域
			傳染病防治	婚姻媒合	日租套房	假消息
雙階理論	無價值言論	賭博、毒品、猥褻、盜版（包含商標及著作）等言論均屬「低價值言論」	多涉及「商業性言論」，雖為低價值言論，但仍有違憲疑慮			縱已有刑事規定，此類言論常涉及「政治性言論」，屬高價值言論
事前或事後管制	事前	事後	事後	事後	事後	事後
比例原則	必定符合最小侵害	多符合最小侵害	多符合最小侵害	有不符合最小侵害之疑慮	有不符合最小侵害之疑慮	不符合最小侵害
公益性	高	高	高	中	中	難以判定
對言論自由侵害性	不涉言論自由	低	次低	中	中	高

第六節 研究結論及建議

本研究係針對網域名稱涉有違反相關法律之實例進行研究，及提出處置建議。內容包含研析美國、日本、馬來西亞及英國等國外立法例（第四章第二節）；盤點我國針對網路內容或使用者行為之違法態樣，及我國網域名稱註冊管理機構監理法規（第四章第三節）；研析我國利用 DN 跨國追查蒐證及進行行政處分之困境（第二章第一節）；研析網域名稱濫用（DNS Abuse）之自

律或他律機制如馬尼拉原則、DNS RPZ 框架（第二章第二節）；實務網域名稱濫用案例之研析（第三章）；訪談行政機關及業者，並舉行座談會收集利害關係人意見（第五章）後，提出我國面對網域名稱濫用之監理建議（第六章）。

網域名稱濫用框架為因應網域名稱濫用，提出基本可供參考之處置方向具參考價值，並將網域名稱濫用類型分為網域名稱技術濫用及網域名稱內容濫用。網域名稱濫用框架認為網域名稱技術濫用，本於註冊管理機構維護網路基礎設施之角色應有作為義務；而網域名稱內容濫用，基於註冊管理機構不審酌網域名稱內容，故除特殊類型如兒少性虐待之素材、網路違法販售鴉片、人口販售及具體且可信的煽動暴力，建議採取專業之「受信任之通知者」，以協助濫用控管外，其餘應由投訴人向網站管理者、註冊人或伺服器服務提供尋求移除濫用內容。網域名稱濫用框架為機關、註冊管理機構、網路社群等因應網域名稱濫用最具參考性之原理原則，亦為貫串本研究之重要參考。

研究團隊透過訪談 TWNIC 及座談會與會專家學者之意見，知悉 DNS RPZ 為因應網域名稱濫用之重要處置手段，特別是面對境外網域名稱濫用，而無法找到網域名稱註冊人、具急迫性、或無法透過司法互助有效解決時，得有效因應網域名稱濫用之處置技術。DNS RPZ 作為一個限制網路接取的技術手段，原始目的為網域名稱系統服務提供的功能之一，多用於技術濫用之處置手段，以維持網路基礎設施運作。然而隨網域名稱濫用類型及範圍之擴大，近年對 DNS RPZ 是否亦可作為網域內容濫用之處置手段提出討論，此時因涉及箝制網路言論之疑義，故由法院之判決/裁定，或是行政機關經法律授權作成行政處分，加以啟動 DNS RPZ 機制更顯重要。

又網域名稱濫用處理手段可分為以下六種：一、行政處分：即立法明文主管機關得做成「限制接取、瀏覽或移除相關網頁內容」之處分；二、行政執行：管制性規定存在，主管機關為落實規定而為直接強制、即時強制之手段；三、刑事扣押：刑事實體法明定之各項犯罪行為，並對各項犯罪行為使用到之網域名稱進行扣押；四、民事暫時狀態假處分：依民事訴訟法第 538 條及民法相關規定（如第 18 條人格權保護），對濫用之網域名稱請求將網域名稱內容刪除；五、刑事局、調查局直接通知：警察機關本於調查犯罪職權，

針對發現網域名稱濫用事實，以不具拘束力之通知，通知各業者；六、民間機關通報：由民間機關通知各業者，為自律機制，無須法源依據。

上述六種方式各有其優點及無法避免之缺點。故因應網域名稱濫用情事之急迫性及現行法制之齊備與否，而選擇不同之處理方式。如法律已授權而具有社會共識，則機關得以行政處分方式，對濫用之網域名稱進行適當處置。如未有法律授權，惟網域名稱濫用情勢急迫且涉及刑事犯罪，則得採取刑事局通知各業者方式進行處置。非涉及刑事犯罪或其他一般情形，則得採取民間機構通報各業者方式，以迴避潛在干涉言論自由之疑慮。

以下針對網域名稱技術濫用及網域名稱內容濫用兩種分類，提出以下結論及建議：

一、網域名稱技術濫用

技術濫用不涉及網路言論自由，因此「網域名稱濫用框架」已針對網域名稱濫用定義五種類型包含：一、惡意軟體（Malware）；二、殭屍網路（Botnets）；三、網路釣魚（Phishing）；四、偽冒嫁接（Pharming）；五、以垃圾郵件之形式達成以上濫用之行為（Spam），並明確指出註冊管理機構受行政機關、第三方通知，而知悉有前述之網域名稱濫用情形時，註冊管理機構必須有所作為，如依據註冊管理機構與 ICANN 之合約，維持網域名稱濫用之聯絡窗口以利接收網域名稱濫用之投訴並盡速調查該濫用之情形。

然而註冊管理機構具體作為義務及處置手段於我國法多未有明文。是以針對網域名稱技術濫用應有法律授權，使主管機關及註冊管理機構得快速取消技術濫用網域名稱及透過 RPZ 停止解析手段，使國人免於成為網域名稱技術濫用下之受害者，具體立法方向可參見第陸章第五節。

二、網域名稱內容濫用

研究團隊參酌網域名稱濫用框架（詳細說明見第二章第三節），及研析外國法制知悉日本面對網域名稱內容濫用之監理，主要透過民間第三方機構 SIA 進行接受民間通報，自行審酌網域名稱涉有違法、不當，轉交業者進行

後續處置。此種民間由下而上之自治模式，深受座談會與會專家學者肯認。

此外，研究團隊透過訪談我國民間第三方機構 iWIN，知悉其透過接受民間通報轉送業者、行政機關之模式，有效解決我國有害兒童身心之網域名稱內容濫用，且其模式係可被複製使用於其他網域名稱內容濫用。

網域名稱內容濫用之監管涉及限制言論自由，因此對應國情及法體系，各國有不同之監理機制。如馬來西亞概括授權單一行政機關進行網域名稱濫用之監理，亦有如美國基於言論自由之保障，將網域名稱濫用情形交由法院進行判斷，或如同日本基於避免進行言論審查之疑義及網域名稱濫用情況之申訴量大，而委由民間第三方機構接受網路使用人通報，並進行審查後將濫用情形回報給伺服器業者及 ISP 業者，請求將違法不當之內容刪除，於處理流程中通訊傳播主管機關並不介入網域名稱濫用之個案審查。目前我國依電信管理法第七十一條第四項，業已訂定「網際網路位址及頂級網域名稱註冊管理業務監督辦法」，該辦法主要針對註冊管理機構進行監督，規範註冊管理機構應訂定業務規章並報請備查，而並未明文規定註冊管理機構對於網際網路網域名稱內容濫用之處理方式。是以，通傳會目前之監理方式，應符合法治國原則，且與國際多數國家作法相符。

針對內容濫用個案之判斷，基於我國網域名稱註冊管理機關（即 TWNIC）與 ICANN 之註冊管理機構協議，其並無義務負責監督、管理網域名稱之內容且也無權限審查網域名稱內容而取消網域名稱，此外目前各國並無由註冊管理機構自行認定是否內容違法之前例。故考量內容濫用之類型眾多且事涉專業判斷，宜另由司法或專業機構負責認定。惟 TWNIC 對於網域名稱內容濫用應有相關協力義務如協助調查、資訊提供、及配合法院及行政處分執行 DNS RPZ 停止解析內容濫用之網域名稱。相關協力義務可考慮透過修改電信管理法第 71 條及相關子法、簽訂行政契約或行政指導之方式為之。

目前我國有關網路內容涉及侵害兒少身心之申訴及通報，係由民間第三方機構 iWIN 負責，處理範圍包含色情、暴力、恐怖、血腥、有害物品、及其他違反有害兒少身心健康內容等六大類。未來可考量將 iWIN 之處理範圍

擴大，或另設專責民間第三方機構以解決如傳染病防治、婚姻媒合、日租套房等網域名稱內容違法不當之通報及處理。

此外，盤點我國法規，僅有兒童及少年福利與權益保障法第 46 條及動物傳染病防治條例第 38 條之 3，明文授權該管行政機關將經其認定為違法之網站內容為限制接取、瀏覽及移除等措施。是以，如行政機關欲通知網域名稱註冊管理機構就違反其餘規定（諸如：公職人員選舉罷免法、毒品防制條例）等實體法之網域名稱為限制一般人民閱覽之行政處分或交由第三方機構受理通報及處理時，並無明確之法律依據。是以本於網域名稱內容違法態樣眾多及主管機關之權責，各目的事業主管機關宜於主管法規內明訂須將網域名稱內容刪除、停止解析之態樣（相關立法方向可參考第陸章第五節），以利第三方機構或行政機關針對網域名稱內容違法不當情事進行審酌，並通知行為人、註冊管理機構、受理註冊機構及 ISP 者。

三、面對網域名稱濫用之監理提出以下建議：

（一）TWNIC 針對使用網域名稱「.tw」之應處機制用可以選擇最強烈之手段取消該網域名稱、選擇使用 DNS RPZ 停止解析該網域名稱，或透過通知受理註冊機構之方式，請求機構依其與註冊人間之合約條款解除契約，停止提供網路服務與註冊人等方式，使網路使用人不再接觸到該網域名稱濫用之網站內容；「.tw 以外網域名稱」即非 TWNIC 註冊管理機構所得直接依其規章，或是請求其下之受理註冊機構透過合約能加以解決。是以 DNS RPZ 停止解析內容濫用之網域名稱更顯重要（第陸章第一節）。現行僅有動物傳染病防治[281]及兒少領域[282]有相關針對我國網路使用者「限制接取、瀏覽之措施或移除網頁內容」之相關規範，為符合法律保留原則各領域主管機關宜於相關主管法律、規範明確訂定處置機制及措施。

（二）面對網域名稱技術濫用，依網域名稱濫用框架註冊管理機構有所作為義務，以避免危害網際網路基礎結構的穩定性與安全性。然而對於內

[281] 動物傳染病防治條例。

[282] 兒童及少年福利與權益保障法。

容濫用部分，基於世界潮流及註冊管理機構多無足夠資源如專業、人力得認定違法不當，故宜另由司法、行政機關或專業機構負責認定。惟註冊管理機構應有發現網域名稱濫用之通報行政及司法機關、協助行政及司法機關取得網域名稱註冊人個人資料，並依法配合行政、司法機關之通知執行 DNS RPZ 停止解析濫用之網域名稱。又註冊管理機構知悉網域名稱濫用時，其處置手段應符合比例原則，如先行通知（可請求受理註冊機構協助通知）網域名稱濫用人及網域名稱註冊人請其將內容刪除，如無法聯繫上相關人員或於期限內無回應者，再行採取如拒絕提供解析服務、暫停提供服務、或依契約（例如申請書）通知註冊業者並與其協調等合乎比例原則之處理措施，而移除網域名稱將屬最後手段。

（三）現行通傳會依「網際網路位址及頂級網域名稱註冊管理業務監督辦法」監理 TWNIC，其主要監管係以註冊管理機構訂定業務規章報請備查之方式進行監管，屬低度之監理模式。在保障言論自由為普世共通價值下，通傳會目前之監理方式，應符合法治國原則，且與國際多數國家作法相符。又為維持低度之監管模式，建議參考日本由下而上之監理架構，針對網域名稱內容濫用由第三方機構判斷網際網路內容是否存在違法或不當，再將相關資訊彙整通報給各主管行政機關、檢警單位及 ISP 業者等，並由各機關自行判定及處置。現行我國已有 iWIN 針對已有立法（兒童及少年福利與權益保障法）之兒少領域進行網域名稱濫用之通報，未來可考慮進一步擴張 iWIN 之業務範圍及權能，或另外新設專業機構認定傳染病防治、婚姻媒合、日租套房等網域名稱內容違法不當問題。

（四）針對行政機關基於網域名稱濫用對註冊管理機構作成行政處分，雖形式上係由註冊管理機構執行限制接取，然從實際網站受限制接取或移除之情況來看，行政處分之對象應為網站所有人或內容之創作者。是以，限制接取行為之註冊管理機構或受理註冊機構僅為行政助手。按上述程序，特定行政機關在處分作成前似應給予「網站所有人或內容

之創作者」陳述意見機會，惟針對「影響網路使用安全（如帶有病毒網域名稱等急迫情況，或網域名稱註冊人位於國外之情形）」或「網域名稱註冊人位於國外，顯然不能遵行陳述意見程序」之情形下，可參酌行政程序法第 103 條第 2 款：「情況急迫，如予陳述意見之機會，顯然違背公益者」；同法第 3 款：「受法定期間之限制，如予陳述意見之機會，顯然不能遵行者。」同條第 5 款：「行政處分所根據之事實，客觀上明白足以確認者。」之規定，不給予網域名稱註冊人陳述意見，以避免已發生之網路安全侵害結果進一步擴大（如散播病毒、釣魚等）。此外，基於網路之匿名性，實務上常發生難以聯繫或將行政處分送達特定網域名稱註冊人之情況，本團隊建議可於相關法規增修「無法查明行為人之送達，得以公告方式為之。」之規定，以解決此問題。

綜上所述，希冀未來透過各主管機關與立法者共同努力，針對各領域網域名稱濫用之「限制接取、瀏覽之措施或移除網頁內容」於主管法規中立法或授權制定子法，以符合法律保留原則。並透過民間第三方專業機構協助認定網域名稱濫用情事，建立由下而上之監理方式，以解決網域名稱濫用問題。

附錄一 對行政機關之訪談

一、 行政院資通安全處

網域名稱涉有違反相關法律之實例研究及處置建議委託研究採購案

專家訪談-行政院資安處簡宏偉處長

時　　間：110 年 5 月 24 日下午 3 時 30 分

地　　點：因應新冠肺炎疫情改為遠端會議

出席人員：簡處長宏偉、恆業法律事務所團隊（戴豪君博士、余啟民教授、簡佑霖律師、林上倫律師）

記　　錄：簡佑霖律師

本次訪談過程如下：

一　財團法人台灣網路資訊中心（下稱 TWNIC）使用網域名稱回應政策區域（Domain Name Response Policy Zone, 下稱 DNS RPZ）之端緒為何？ （一） 需有行政機關之行政處分？抑或機關發函即為已足？ （二） 需有法官刑事扣押裁定？抑或檢、警附帶扣押即為已足？ （三） 影響資安之重大情況如何定義？自「雪崩案件」[283]以觀，似乎調查局來函（不須依法為行政處分），TWNIC 即以 DNS RPZ 技術全面下架有資安疑慮之網站。 是否有民事相關案例，諸如民事執行法院依判決執行?
林律師： 現行 RPZ 技術的程序大概是如何？網路黑名單的作法跟 RPZ 技術是否相同？ 簡處長： DNSRPZ 是網域名稱或者 IP 位址的介接技術，例如可以 TWNIC 便開頭擋掉。但是如果要從 TWNIC 阻擋一定要有法律依據。 因此也需要明確授權，不管是來自行政機關或法院，說明某個網域名稱確實有危害，經過法院裁定之後，再交由 TWNIC 阻擋。 實務上有些情形例如假訊息，可以先暫時把東西下架。德國做法是（行政機關）會先要求平臺把網域名稱下架 24 小時，等待法院裁定是否准許下架，若法院不允許下架，要重新回復網站。TWNIC 有類似做法，但是案例少之又少。總之依法很重要，一定要有法院的裁定授權。 黑名單的做法，GSN 是防堵惡意網站的方式之一。但是這種阻隔方法跟 TWNIC

[283] 同註 271。

不一樣。由行政院資安處蒐集黑名單，再由國發會將黑名單設置於政府網頁（Government Service Network，下稱 GSN）以建置防火牆，是以，利用 GSN 防火牆阻擋網站和 TWNIC 無關。行政院資安處對於哪些網站是釣魚網站、惡意網站的掌握較清楚。可以把政府想像成一間公司，以上政府作為不會擴及到一般民眾。

林律師：
簡處長的講法有應證我們研究。我們研究看各國政府立法例，網域名稱下架都是最後、最備位的手段。一開始會由受理註冊機構先用使用合約介入、再來才是扣押伺服器、用防火牆擋，盡量不會下架網域名稱。

簡處長：
這很合理，因為言論自由本來就是民主國家的精神。下架網域名稱考慮言論自由問題，要有法源依據以及法院裁定。

林律師：
另外請問一下，目前我國兩個法源，一個是傳染病防制法，一個是兒少法針對硬蕊色情內容，這是哪一種阻擋方法？因為法條上是講說要下架內容，所以可以用伺服器下架或者網域名稱下架，想問這樣應該用哪種方式？還是說實體法裡面有隱含了可以用網域名稱下架的意思？

簡處長：
比較法一定很少這樣規定。因為一個網站裡面的一樣內容不合適，不代表其他內容不合適；同理，一個網域名稱裡面有很多的網站，又一個網站內容不合適不代表其他網站不合適。實體法下架會是針對內容下架，不會是下架網域名稱。因為網域名稱裡面的不只一個網站。單一網站裡面的內容也很多。此又會牽涉到言論自由問題。

簡處長：
我想好奇問一下，為何問雪崩這個案例？

林律師：
因為這個案子特別針對網域名稱進行查扣。是直接接獲調查局通知就下架，沒有經過法院程序，我們對於這種沒有經過法院保留的案子有興趣想了解其細節。

簡處長：
這是國際案件，是警察體系才能處理。

	假設此集團在台灣並無犯罪，但是集團散佈在世界各國，必須要國際合作，各國都同步切斷該網路才能有效。正因該集團在台灣未必有犯罪行為，法院會無法作出裁定。比方該集團可能在台灣有設定釣魚網站，跟台灣 ISP 有簽契約，但是在台灣沒有犯罪，這時候可能要從該網站跟 ISP 的契約關係決定是否要下架網站。這裡跟法院保留沒關係。總之雪崩案不是用 DNSRPZ 技術下架。網域名稱刪除這件事不一定是用 DNSRPZ 的。 戴老師： 最後想再問簡處長，RPZ 最理想的程序應該為何？ 簡處長： 我認為應該要一個平時、一個緊急。平時程序跟通保法做法一樣，需法院同意。緊急時可以直接做，但有二十四小時限制。
二	停止解析與 DNS RPZ 阻止使用者進入網站之差別為何？是否 DNS RPZ 還有將原網域名稱轉移連接至他位址之功能？
	林律師： 那想問說停止解析的概念，他跟 RPZ 的關聯是什麼？ 簡處長： 停止解析的意思是 DNS 不解析，跟 RPZ 不一定一樣。DNS RPZ 是不做網域名稱跟 IP 的對應。我們可以說因為 RPZ 所以停止解析，但是如果反過來說，停止解析就是 RPZ，這樣講就不對了。 林律師： 用 RPZ 和刪除網路的差異究竟何在？可以回復嗎？ 簡處長： 要回復網站，限制條件解除就可以回復，這個在技術面都不是問題，重點是法律流程要如何處理。 至於說效果差異何在，因為網站上是一層一層下來的，假設有個域名在台灣連不上，在國外可能連得上，因為 RPZ 是透過 TWNIC 讓台灣連不上的。 至於如果叫 ICANN 把網域名稱移除，需要透過該該機構的政策決定。
三	使用 DNS RPZ 之主體是否限於 TWNIC？抑或電信警察大隊或行政院資安處是否也有自己的 DNS RPZ 系統？
	林律師： RPZ 有其他機關可以使用嗎？還是只有 TWNIC？ 簡處長：

	TWNIC 是台灣最上層。但是如果有人有 DNS，或許就有那個能力，但身處網路供應鏈最上層的 TWNIC 建置 DNS RPZ 才最有效果。
四	依照 TWNIC 官方對 DNS RPZ 之說明，該技術係阻止使用者進入特定網域名稱，惟該技術得否進一步就該網域名稱之特定內容進行阻隔？
	林律師： RPZ 會阻擋網站還是網域名稱？ 簡處長： 技術面上都可以。最小單位是阻擋 IP，阻擋 IP、阻擋網站、阻擋網域名稱都可以。但是不能擋 IP 裡面的特定內容，不能處理到特定網頁。除非，該網頁連結到一個被停止的 IP。
五	如果使用國外 VPN 連接被 DNS RPZ 阻隔之網站，是否仍可以順利進入？
	林律師： 那想問一下，如果說有個域名被 RPZ，但是如果用 VPN 的話，是不是可能還是連得到該網域名稱？ 戴老師： 我舉個例子說明，假如有個網站是在新加坡註冊，在台灣被 RPZ 處理，如果台灣人可以連接到新加坡的 DNS 的話，還是可以翻過去連上。 林律師： 那這和 GNS 黑名單一樣嗎？黑名單網站國外可能都還是可以看得到？ 簡處長： 效果類似。
六	近期 SWAG 網站及 110 年度聲扣字第 11 號刑事扣押裁定是否使用 DNS RPZ 技術？根據新聞報導[284]，刑事局與九大電信業者合作，啟用 DNS RPZ 的手法，阻隔一般人進入網站瀏覽，惟目前觀察，現在登入 SWAG 網站僅有「該網站正在配合調查」之提醒，並無新聞所述不得進入網站之情形。試問，資訊警察大隊對於 SWAG 網站之處斷是否包含 DNS RPZ 之技術？
	林律師： 還是想要理解一下，使用 DNS RPZ 跟單純下架網站，各種不同手段的實質性差異？例如 SWAG 之前的處理是不是用 DNS RPZ 技術？ 簡處長： SWAG 那個不是。並不是用 TWNIC 的 DNS RPZ 技術。

[284] 報導者，從 SWAG 被抄，看數位情色產業大躍進下的法律衝撞、直播主的勞動現場，https://www.twreporter.org/a/taiwan-erotic-industry-swag-sex-work

其實網址移轉的不用特別技術就可以做到。從 DS 上、伺服器上做網址轉接都可以，各種階段來做都可以。網站轉址跟 TWNIC 未必有關係。

林律師：
最近一個比較有名的刑事扣押案件是小鴨影音，我們可以發現點進去是 not found 的黑白頁面，這個是怎麼做成的？

簡處長：
這是 http 標準的定義，這是「沒有這個網頁」的意思，這也跟 TWNIC 沒關係。

林律師：
那如果今天是 DNS RPZ 處置的話會長什麼樣子？

簡處長：
會根本連找都找不到，Routing 都 Routing 不到。

余老師：
「404」的意思就是網站找不到，這有可能是 ISP 擋掉。

戴老師：
這是 ENS server 讓 IP 對應不到。

簡處長補充戴老師：
RPZ 的概念類似「100>>中正區」的關係被拿掉。至於網站找不到的話是「地址某某號，但是查無此號碼」，跟 RPZ 關係不大。
網站找不到有兩種，一種是找不到服務，一種是根本沒有網站。

簡處長：
因為台灣地區 IP 都是用 TWNIC 在做分配，所以如果用 TWINC 阻擋，網站根本就連不到。所以影響最大。

戴老師：
林律師提到的兩個下架網站的法律，應該不是用 RPZ 吧？ 主管機關會先叫網站自己下架，從 TWNIC 下架應該是最後手段吧？

林律師：
想請簡處長看一下兩張圖片。一張圖片是「此網域名稱已遭封鎖」，一張是「無法連上網站」。

簡處長：
兩張圖不一樣，第一張圖就是 RPZ。
第二張圖片，跟前者無關，可能原因有很多。可能因為對應不到 IP，或者電腦防火牆自己把他阻擋掉。光是這張圖片是看不出來是哪一個階段造成連不上。

七	日本 sinkhole 技術和台灣是否為台灣所採用?

林律師：
最後想再問 sink hole，技術上大概是怎麼樣子？

簡處長：
Sink hole 主要針對 DDoS。DDoS 是用有瑕疵或者錯誤的 quory 讓伺服器負擔過重，讓網站掛掉。Sink hole 就是查知有這種 Quory 的時候，把他們導到一個無底洞，藉此阻擋 DDoS 攻擊。DDoS 的對抗方式也不只一種。這麼技術並沒有特別說誰才可以做。如果你想知道日本警方是怎麼用 sink hole 的，要知道我們和日本的網路結構可能是不一樣的，如果我國希望有類似效果，可能有其他做法。

林律師：
了解，謝謝簡處長。

八	未來建議訪談對象?

余老師：
最後想問簡處長，還會建議訪問哪些單位？

簡處長：
技術面的部分，會建議訪問調查局或者刑事局，因為他們是實際執法單位，會有更多元的看法。國安會也可以，其從國家安全角度，看法也會更不一樣。也可以問中華電信，因為中華電信是台灣最大的電信業者，可以問他們有關 RPZ 問題。
至於法制面的部分，可以訪問羅秉成羅政委老師。

二、 刑事警察局電信偵查大隊

網域名稱涉有違反相關法律之實例研究及處置建議委託研究採購案

專家訪談-電信偵查大隊第一隊莊隊長明雄

時　　間：110 年 8 月 24 日上午 10 時 00 分

地　　點：刑事警察局電信警察隊

出席人員：莊隊長明雄、恆業法律事務所團隊（戴豪君博士、余啟民教授、簡佑霖律師、林上倫律師）

記　　錄：簡佑霖律師

本次訪談過程如下：

一、針對　貴局管轄之業務，就「網域名稱類型犯罪」提問如下？ （一） 刑事犯罪之偵查過程中，是否伴隨對網域名稱之處置? （二） 刑事警察局是否維護「網路安全、資訊安全」？ （三） 是否因接獲「民間團體（iWIN）」或主管機關（衛生福利部）之通知而開啟犯罪偵查或其他處置? （四） 可否提供代表性案件及範例供本團隊參考？ （五） 除「網域名稱處置」外，是否有其它處理網域名稱內容及技術濫用之手段？（直接扣押犯罪人 Web server、遮擋網站內特定內容、刪除網路伺服器內之內容等）
莊隊長： 主要有三種方式： 第一種，有最高權限會直接接管網域名稱申請，直接扣押網域名稱申請的帳號密碼，電信隊會把密碼改完之後，直接把網址轉向我們設定的網站。swag 和楓林網皆是以此方式，楓林網案件中並無扣押裁定。搜索票會特別寫到應扣押雲端硬碟。 第二種方式就是通報 TWNIC，請法院通報業者停止解析。DNS RPZ 是資安聯防，請 TWNIC 跟業者合作，達到境內聯防。 有關兒少法的通報，衛福部的通報係有法律依據的，如果臉書接收到通報，其自己看了內容可以根據自己社群守則下架，此實際上就是網路自律的行為。 第三種做不太到，比方說針對美國的網域名稱或者再上一層的域名要求下架網域名稱。此需要未來的司法互助，由台灣的檢察官通報美國的檢察官才能做到。

前面三種方法，通常第一種有用就不會用其他的。不過如果遇到比方說 gimy 的情況，封了一個網站還會有其他網站，這樣無法一次解決。

找 TWNIC 有幾個問題，第一，TWNIC 要求業者停止解析事實上並無強制力。第二，找民間機關做強制處分有偵查秘密外洩之問題，我們會希望未來有一個公家機構可以負責這個職責。

老師發問：為何覺得民間單位執行不好？
回答：在起訴之前偵查秘密外洩之問題，給民間機構執行 RPZ 不好。目前是還沒有發生偵查機密外洩，但不能排除這種風險。

林律師問題：感覺可以分成行政管制和刑事裁罰，後者感覺才會有前述的問題。

關於現行法規沒有跟上科技的問題，比方說扣押電磁紀錄要怎麼扣的問題，刑事訴訟法沒有規定，現在的做法是用網路封包扣押。但是法官會希望警察扣押到實體物件。再舉個例子，詐騙犯罪集團有大量財產，有土地，該如何凍結？拿扣押裁定去戶政事務所扣押。網域名稱裁定類似，不影響網域名稱所有權，但是讓網站無法出現。

日本的模式可以參考，日本會以協會名義對執法單位行使告訴權利。

我認為 DNS RPZ 對付者為資安問題。但是如果是網路內容有問題，比方賭博、色情、統戰言論，這種情況是不是該用 RPZ，要另外討論。

網路犯罪可分為三大層次，第一層次是工具派，比方用 Line 或者 Skype 進行詐騙，第二層是網站類，比方色情、賭博網站、第三層是目標類，比方駭客攻擊、DDoS、木馬程序、加密軟體等侵害電腦的犯罪。RPZ 比較針對第二層第三層的犯罪。我是認為針對內容問題的犯罪可以利用 RPZ 技術建立一道長城，不過當然我們會換個名稱。

老師發問：如果要建立長城，法源依據何在？主管機關為何？
回答：未來可以用電信管理法，主管機關可能為數位發展部或者資安署，總之要有一個部門負責處理 RPZ 的執行，此不會再分民事刑事行政程序，我們需要一個中介機構。未來如果要認真執 RPZ 技術，我認為不應該找 TWNIC，畢竟他只是民間機構。

斷源專案

二、針對「斷源專案」之內容及執行流程，提問如下？

（一） 開啟「斷源專案」之端續為何？刑事偵查或第三方機構通知？
（二） 「斷源專案」之執行由何機關決定（警察、檢察官、法官）？
（三） 何種犯罪態樣會採用「斷源專案」來「停止解析」特定網域名稱?
（四） 「斷源專案」屬刑事訴訟中何種強制屬分？
（五） 「斷源專案」之法源依據為何？
（六） 可否提供代表性案件及範例供本團隊參考？
（七） 除「斷源專案」外，是否有其它處理網域名稱濫用之手段？
（八） 是否會對 BET365 及九州娛樂等網站進行斷源?

早期電信警察隊為了因應電信犯罪氾濫，人頭門號、地下電台等等問題。斷源專案現在轉型到對付詐騙集團。現在其實專案的主管機關是 NCC。斷源專案其實是概括名詞，沒有法源，只是一個行政手段。勉強來說只有電信法跟刑事訴訟法是法源，還有通訊監察法。但是整個做法之法律依據其實都很不清楚。斷源專案現在已停止。現在給 165 反詐騙專線來做。

DNS RPZ 處置措施

三、刑事警察局與財團法人台灣網路資訊中心（下稱 TWNIC）之「網域名稱回應政策區域 （Domain Name Response Policy Zone, 下稱 DNS RPZ)」之關係？
（一） 開啟「DNS RPZ」之端序為何？刑事偵查或第三方機構通知？
（二） 何種犯罪態樣會採用「DNS RPZ」來「停止解析」特定網域名稱?
（三） 「DNS RPZ」屬刑事訴訟中何種強制屬分？
（四） 「DNS RPZ」之法源依據為何？
（五） 現在刑事局有無採用「DNS RPZ」措施？未來「DNS RPZ」是否會取代「斷源專案」？
四、針對國內網域名稱及境外網域名稱處置手段是否不同？
五、除「斷源專案」及「DNS RPZ」外，是否有其它處理網域濫用名稱之手段？諸如：遮擋網站內特定內容、刪除網路伺服器內之內容等？

我不認為一定要做 RPZ，因為一件事情是犯罪預防，一個是抓到之後要走刑事程序。以預防的立場來說對斷源專案是可以做的，其只是單純防止更多人被害，並沒有要進一步到刑事訴訟程序。有鑑於斷源專案有效率，而且萬事皆求法官他們案件會太多，我覺得斷源專案的作法應該繼續延續。

我們也應該要思考應該給哪個中介機構處理，這邊講一個之前遇到的問題，博弈廣告的管理是教育部，教育部建議說這種事情在很多領域都會發生，比方說不法投資網站，應該給一個專責主管機關。不同事務交給不同目的事業主管機關到最後就會沒效率且沒人管。至於說如果要擔心一個專責機構權限會太大，應該再交給一個民間機構中介。或者再舉個例子，比方銀行凍結帳戶，銀行公會可以自己討論出一個方式交給主管機關。網路管制可以採同樣方式創造出管理方式
。

iWIN 最近有越做越好，他有公家機關的權力，但是沒有政府的味道。比方說色

情內容外洩，iWIN 協助臉書、谷歌下架，iWIN 背後有 NCC 而且有法源依據可以要求下架。

網域名稱技術濫用

六、就網路病毒事件「殭屍」、「釣魚」、「蠕蟲」等，是否會對上述網域名稱進行處置?如有，處置內容為何?（停止解析或下架網域名稱）

七、針對網域名稱病毒事件之處置是否有法源依據?

八、網域名稱下架或停止解析之手段是否構成直接強制或即時強制?

針對技術濫用問題，我覺得停止解析跟下架實效性是一樣的。因為下架的實際上要辦到不可能，但是兩者的處理都是讓網頁內容無法顯示。下架網域名稱還要司法互助，程序會拖很久。停止解析是預防犯罪的動作，是行政處分，不需要發動刑事程序。

資安案件方面，NCC 有個緊急應變中心，專門管網路病毒。

立法及行政政策

九、如果未來要增加網路言論處理之法源依據，貴公司是否有立法建議?網路病毒這部分是否有立法之需求?

十、經行政機關通知，台灣民眾可以瀏覽境外博弈網站，貴局是否建議訂定法規，以行政處分之方式下架博弈網站?

十一、刑事局發函通知、申請法院扣押網域名稱及以行政處分下架網域名稱，三者所需時間差別?

林律師：非法婚姻、外勞仲介、博弈、詐騙、假投資等內容，這樣有預防犯罪之需求嗎？

回答：非法婚姻仲介跟我們無關，其他是金管會管理。

我認為，我們給執法單位一個權限不是真正要讓執法單位用，而是萬一發生平臺不理執法機關時，應該要怎麼處理的問題。舉個例子，澳洲政府之前不准臉書播放政府不准的廣告，澳洲政府就關閉臉書。這種做法可以值得我們參考。另外針對境內人民連上國外違法網站的問題，其實也類似 RPZ 的概念，不管你國外網站怎麼樣，進來台灣就是要加入聯防機制。另外也可以參考一下美國雲端法案。

最後想問一下問題十一。發函通知可以一天完成，內部有開會決議來發函，例如電信警察局和 NCC 召開的電信諮詢小組會議。

法院扣押時間要比較久，令狀申請要至少一天，執行要一個禮拜。小鴨影音案件第一次申請還被駁回。

行政處分的話，TWNIC 通知業者轉向。真正執行者是電信業者。

老師發問：有沒有東西不是 NCC 管理的？有新機構的話跟 NCC 為何關係？

回答：如果是刑事案件不一定要 NCC。可以建議 NCC 把 TWNIC 的角色再明確化。

老師發問：網域名稱下架行政措施應該誰來管？
回答：其實可以由 NCC 統一來做。以免該領域主管機關不知道怎麼做，或者不知道法律依據。

三、交通部郵電司

網域名稱涉有違反相關法律之實例研究及處置建議委託研究採購案

專家訪談-

時　　間：110 年 10 月 26 日

地　　點：書面訪問

訪談內容如

一、貴單位立於第一線參與 ICANN 會議，目前 ICANN 對個資議題及 WHOIS 資料庫之態度為何?
ICANN 對各項議題（含個資及 WHOIS 資料等）之政策擬定形式係採由下而上、及透過多方利益共同體機制進行討論，以期形成共識，最後由董事會做最後決定，且 ICANN 亦遵循各國的法律；而針對個資議題及 WHOIS 資料庫部分，過往 WHOIS 資料係為開放狀態，後因歐盟為保護個資安全而制定歐洲個人資料保護規則（GDPR），故之後大部分 WHOIS 欄位改為封閉狀態，目前 ICANN 對於本項議題之日後開放程度及存取方式，刻正透過快速政策制定流程（EPDP）之三階段討論及評估中。
二、貴單位對於目前 ICANN 提出之揭露/存取非公開註冊資料的標準化系統（System for Standardized Access/Disclosure to Non-Public Registration Data，下稱 SSAD ）有何想法？是否足以因應我國取得網域名稱註冊人個人資料之需求?
依行政院分工，本部並非 gTLD 政策及公共安全（含資料保護）之業務主管機關，且本部也非 SSAD 使用單位，建議洽詢業務主管機關或 SSAD 使用單位之意見。惟建議我國本議題之業務主管機關及使用單位應密切注意 SSAD 系統之相關發展方向及內容，必要時提出意見，以符合我國之實務需求。
三、目前我國依「網際網路位址及頂級網域名稱註冊管理業務監督辦法」對註冊管理機構（如 TWNIC）進行監管，於該法中主要監管手段為規定註冊管理機構應訂定業務規章並報請備查（第 7 條），屬於低度監管，此種低度監管方式是否符合 ICANN 態度及世界潮流?
本部並非「網際網路位址及頂級網域名稱註冊管理業務監督辦法」之業務主管機關，建議洽詢業務主管機關之意見。惟考量個資保護及資安問題，影響國人權益及安全極大，建議主管機關仍應有此類監管之規範為宜。
四、針對資安事件（網域名稱技術濫用），是否宜由行政院資安處當主管機關，亦或依循 ICANN 之規範，由 TWNIC 直接下架有「網域名稱技術濫用」之網站?
依行政院分工，本部並非資安業務主管機關，建議洽詢業務主管機關相關意見。惟鑑於目前技術濫用情況不一，為能儘速處理，建議可作適當分工，部分情況可由 TWNIC 直接下架，部分則另由業務主管機關決定。

五、兒童及少年福利與權益保障法第 46 條之 1 及動物傳染病防治條例第 38 條之 3 針對網站內容違法為限制接取、瀏覽，甚至是移除之措施之規定，針對其他違法情事於網域名稱內容發生（如賭博、傳染病防治、日租套房等違法情事），是否建議亦應有相對應之立法? 有無建議之領域亦應有相關之立法?
本部並非題旨之業務主管機關，建議洽詢業務主管機關之意見。
六、DNS RPZ 即網域名稱停止解析機制目前是業者自發性加入，貴單位認為是否有強制業者加入之需求?
本部並非題旨之業務主管機關，建議洽詢業務主管機關之意見。

四、農委會動植物防疫檢疫局

網域名稱涉有違反相關法律之實例研究及處置建議委託研究採購案

專家訪談-農委會動植物防疫檢疫局

時　　間：110 年 10 月 7 日

地　　點：書面訪問

訪談內容如下

一、針對 貴機關負責之限制接取、瀏覽或移除相關網頁內容業務，提問如下？
（一） 貴機關認定之不當內容，係來自人民之申訴檢舉、貴機關自行查找? 答：均有。
（二） 境外網域名稱如網域名稱為.tw，其內容有違法或不當時，是否仍在貴機關之限制接取、瀏覽或移除相關網頁內容範圍內? 答：是。
（三） 貴機關判斷特定內容違反動物傳染病防治條例，而須依動物傳染病防治條例第 38 條之 3 第 3 款公告限制接取、瀏覽或移除相關網頁內容，其內部決定公告之流程為何? 答：違規案件依照「網際網路內容涉及境外應施檢疫物販賣至國內或輸入時應採取措施」、行政程序法等規定辦理，經查獲之違規案件，如調查之證據確實，則依動物傳染病防治條例相關規定，以公文書方式通知違規業者。
（四） 貴機關係將認定違法之內容直接通報給「網路平臺業者」、「ISP 業者」或「檢、警機關」?該通報之流程為何？ 答：依據動物傳染病防治條例第 38 條之 3 及「網際網路內容涉及境外應施檢疫物販賣至國內或輸入時應採取措施」規定，本局將違法之內容以公文函通知「網路平臺業者」及「ISP 業者」。
（五） 貴機關是否有對「判斷為違反動物傳染病防治條例」之內容做出行政處分？可否提供代表性案件及範例供本團隊參考？ 答：是。因裁處案涉及個資，本局可去識別化後提供。
（六） 除通知業者自行下架內容外，是否有通報 TWNIC 進行限制接取（DNS RPZ）？ 答：已提供相關案例與 TWNIC
（七） 「網際網路內容涉及境外應施檢疫物販賣至國內或輸入時應採取措施」於今年 7 月 23 日修正公告，修正之原因為何? 答： 1. 因業者及產業團體屢次透過外國商會等管道向國家發展委員會反映，

建議政府瞭解電商平臺特性，針對電商平臺、賣家及電信業者不同的營運模式，建構可歸責之管理措施，制定出符合電商產業環境永續發展的法規。 2. 本局評估並研析業者陳情意見後，在兼顧有效管理電商平臺及邊境阻絕動物疫病的考量，修正該措施。
二、案例檢討
（一） 貴機關是否有依動物傳染病防治條例第 38 條之 3 公告而須採取相關措施之案例。 答：是。
（二） 承一，是否有公告並要求廣告刊登者、平臺提供者、應用服務提供者或電信事業，依動物傳染病防治條例第 38 條之 3 第 3 款限制接取、瀏覽或移除相關網頁內容？ 答：是。
（三） 承二，若有公告通知廣告刊登者、平臺提供者、應用服務提供者或電信事業配合採取 限制接取、瀏覽或移除相關網頁內容， 其成效如何？ 答：本局搜查電商平臺刊登違規境外應施檢疫物廣告查獲案件之平均查獲率，自 108 年的每月平均 7.4%降到 110 年的每月平均 0.1%。
（四） 是否有違反動物傳染病防治條例第 38 條之 3 而依同法第 45 條進行裁罰之案例。 答：是。因裁處案涉及個資，本局可去識別化後提供。
三、立法及行政政策
（一） 如果未來要增加網路言論處理之法源依據， 貴機構是否有立法建議?擴大應「限制接取、瀏覽之措施，或先行移除」之內容? 答：其他領域之網路言論非本局權管，本局無建議。

附錄二　對機構及業者代表訪談

一、TWNIC 財團法人台灣網路資訊中心

網域名稱涉有違反相關法律之實例研究及處置建議委託研究採購案

業者代表訪談-財團法人台灣網路資訊中心

時　　間：110 年 6 月 16 日上午 9 時 30 分

地　　點：因應新冠肺炎疫情改為遠端會議，

出席人員：黃勝雄執行長、林志鴻組長、恆業法律事務所團隊（戴豪君博士、余啟民教授、林上倫律師、簡佑霖律師）

記　　錄：簡佑霖律師

本次訪談過程如下：

一、財團法人台灣網路資訊中心（下稱 TWNIC）停止解析或移除特定網域名稱之端序為何之端序為何？ （一） 需有行政機關之行政處分？抑或機關發函即為已足？抑或民間團體（諸如:I WIN）通報即足? （二） 需有法官刑事扣押裁定？抑或檢、警附帶扣押即為已足？ （三） 影響資安之重大情況如何定義？自「雪崩案件」[285]以觀，似乎調查局來函（不須依法為行政處分），TWNIC 即阻斷有資安疑慮之網站。
黃執行長： 基本原則要是法院判決，或者具有法律依據的行政處分。假如判決文義清晰，便會以判決文義執行。目前收到的公文很多種，法院判決的只有收過兩個，政府機關來函很多，但是因為法律依據較為不明，所以我們沒有處理過。以上是針對.tw 的部分。 小鴨影音是境外網站，所以是第二題的問題。因為該網站是境外網站，境外網站用 DNS RPZ 解決。 林律師： 有移除特定網域名稱之案例？ 黃執行長： 沒有，只是停止註冊人的網路解析服務。他的智慧財產還是在。此外，檢警單位之扣押命令對 TWNIC 無效，僅有法院扣押裁定才有效方屬有效。 另外針對民事程序，本公司未收過民事執行之公文。
二、財團法人台灣網路資訊中心（下稱 TWNIC）停使用網域名稱回應政策區域（Domain Name Response Policy Zone, 下稱 DNS RPZ）之端序為何？ （一） 需有行政機關之行政處分？抑或機關發函即為已足？抑或民間團體（諸

[285] 同註 271。

如:I WIN）通報即足?

（二） 需有法官刑事扣押裁定？抑或檢、警附帶扣押即為已足？

（三） 影響資安之重大情況如何定義？自「雪崩案件」[286]以觀，似乎調查局來函（不須依法為行政處分），TWNIC 即阻斷有資安疑慮之網站。

黃執行長：

我們沒有收到過 iWIN 的通報，衛福部通報也沒有，他們可能已經透其他管道處理了。如果真的收到通報，因為兒少法已經有法律依據了，該通報是有依據的，我們的確可以據以執行。

惟另外有特殊情況，就是有國安需求的情形，此時我們會配合國安單位要求。此時案件樣態我們無法自己定義，是否為國安問題須由發文機關定義，TWNIC 只是執行單位。總之，任何處置行為一定都需要法律依據。

至於網路安全等資安這部分，我們沒處理過類似案件。

三、停止解析、下架該網域名稱與 DNS RPZ 阻止使用者進入網站之差別為何？

黃執行長：

停止解析、下架、屏蔽、DNS RPZ，以上都是習慣用語，需要依據情境而定。兩者彼此之間有一定差距。比較標準的名稱應該是停止解析。

四、使用 DNS RPZ 之主體是否限於 TWNIC？

黃執行長：

TWNIC 是實施者，其他主體，例如國內電信業者，算是次節點，也可以算是同步實施的單位。

林律師：

有沒有加入次節點的業者嗎？

黃執行長：

幾乎都加入了。因為 DNSRPZ 是有法律依據的，所以業者都有加入。

林律師：

那同意加入這部分，當初也寫進 TWNIC 和受理註冊機構的契約裡嗎？

黃執行長：

沒有，這是屬於自律規範的層面，業者自願參與的。

五、DNS RPZ 是否為針對境外特定網域名稱之有效處置手段？有無其他處置方式？

林律師：

DNS RPZ 是否為處理違法網域名稱濫用之唯一手段？

黃執行長：

不是，很多工具都可以處理。例如司法互助、法律合作、司法犯罪調查、布達佩斯協定、聯絡境外主機代理業者等等。DNS RPZ 算是很後端、不得已的處置方式（最後手段）。我們會希望走到最後一步之前，應該把其他方法都先走完。

此外，ICANN 不處理任何域名下架，他們認為這是各個司法管轄機關的職責。針對「.com」網域名稱為下架處置，需找 VeriSign 公司，或者去美國向法院訴訟；而針對網站之特定內容，TWNIC 沒辦法做比例原則的判斷，憑 DNS RPZ，僅能一次對整著網域名稱做處理。

[286] 同註 271。

六、如果使用國外 VPN 連接被 DNS RPZ 阻隔之網站，一般人是否仍可以順利進入？
黃執行長： 沒錯，等於是從國外連接網路。RPZ 不是百分百全封鎖。
七、近期 SWAG 網站是否使用 DNS RPZ 技術？根據新聞報導[287]，刑事局與九大電信業者合作，啟用 DNS RPZ 的手法，阻隔一般人進入網站瀏覽，惟目前觀察，現在登入 SWAG 網站僅有「該網站正在配合調查」之提醒，並無新聞所述不得進入網站之情形。是否 DNS RPZ 還有轉移連接至他網站之功能？
黃執行長： SWAG 案件之判決文義不清，TWNIC 無從據以執行。此外，調查局之前就先聯繫個別業者下架，所以這個是業者自己之行動，和 DNS RPZ 無關。 林律師： SWAG 目前的作法是業者自己轉連結嗎？ 黃執行長： 我們沒處理，但是我們判斷是這樣。
八、受理註冊機構（諸如:中華電信、網路中文）依照使用人條款停止提供網域名稱服務之端序為何？ （一） 需有行政機關之行政處分？抑或機關發函？抑或民間團體（諸如:I WIN）通報即足? （二） 需有法官刑事扣押裁定？抑或檢、警附帶扣押即為已足？ （三） 影響網路安全之情況是否亦屬之？ （四） 其效果和 DNS RPZ 阻止使用者進入該網站之差別為何？ （五） 是否有相關案例？
黃執行長： 受理註冊機關要有法律依據才能停止解析，原則上 ISP 業者技術上有辦法停止解析，但是還是要有法律依據之處分或判決。 如 ISP 業者與網域名稱申請人間有其他私自約定，此時若有爭議即屬於民事司法爭議之範疇。
九、ISP 業者如何就特定網站之內容為刪除？對境外網站可否為之？
黃執行長： 可以刪除。網路接取業者可以針對特定內容進行遮蔽處理。ISP 會比 TWNIC 多一些工具可以管理，例如透過路由器或者防火牆，利用 access control list 控制資料處理。
十、根據 110 年度聲扣字第 11 號裁定，法院同時通知受理註冊機構依據服務協議限制該網址之使用，及透過 TWNIC 停止解析該網站，藉此將該網址納入我國公權力支配下而為扣押處分。TWNIC 是否有依法院之扣押裁定對下述網站為停止解析?
黃執行長： gimy 劇迷和小鴨影音都是 DNS RPZ，SWAG 是業者自己的控制措施在處理。
十一、動植物違禁商品下架，農委會有無和 TWNIC 溝通過？（本計畫戴老師於訪談

[287] 同註 284。

時之提問）
黃執行長：農委會有前來溝通過，現在有法律但是還沒有具體 SOP。目前我們有沒收過來自農委會的行政處分。
十二、對 NCC 未來的立法計畫或網域名稱濫用處置方式有何建議？（本計畫戴老師於訪談時之提問）
黃執行長： 通傳會主要是有線無線電視廣播以及通信電信監理管理。基本上我們是處理後者。 如果是對特定網路內容，會是比較困難的地方，因為無法界定管裡權責。這裡最好還是回歸每個目的事業主管機關，由他們訂定相關法律。即便之後 NCC 新設置數位部，該部對於網域名稱濫用處理這一塊，仍沒有職掌之權限。 林律師： 馬來西亞的管制措施，係以 MCMC 是管制言論的機關，可以任意發行政處分。日本的話，要有法院判決才有辦法對網域名稱為處置。請問黃執行長認為何種立法例較適合我國？ 黃執行長： 我們常常收到不同單位公文要求移除網站，這種單純公文往返我們無法處理，現在只有兩個法律有授權可以處理（兒少法、動防法）。所以馬來西亞的模式台灣不太可能走。日本比較有可能，因為才有法治國的正當程序。

二、 iWIN 網路內容防護機構

網域名稱涉有違反相關法律之實例研究及處置建議委託研究採購案

專家訪談-iWIN

時　　間：110 年 9 月 22 日上午 9 時 30 分

地　　點：遠距訪談

出席人員：iWIN 團隊（劉昱均執行秘書、韓昊雲組長、郭芊欣專員、張芳慈專員）、恆業法律事務所團隊（余啟民教授、林上倫律師、簡佑霖律師）

記　　錄：簡佑霖律師

本次訪談過程如下：

一、針對　貴機構負責之內容防護業務，提問如下：

（一） 貴機構認定之不當內容，係來自人民之申訴檢舉、 貴機構自行查找?

（二） 境外網域名稱之不當內容是否在 貴機構之防護範圍?

（三） 貴機構判斷特定內容違反兒少法第 46 條之流程為何?

（四） 貴機構係將認定違法之內容直接通報給「衛福部」或直接通報給「網路平臺業者」、「ISP 業者」或「檢、警機關」?該通報之流程為何？

（五） 貴機構或「衛福部」是否有對「判斷為違反兒少法」之內容做出行政處分？可否提供代表性案件及範例供本團隊參考？

（六） 除通知業者、創作者自行下架內容外，是否有通報 TWNIC 進行限制接取（DNS RPZ）？

（七） 目前防護內容之標的為何？除色情、暴力等不適合兒童及少年觀看之內容外，是否包含「博弈網站」？

（八） 余老師補充提問：希望可以了解，假設應依法行政有法院令狀，iwin 是否可以擴張執掌，在兒少保障之外，還為其他的處置？業務量是否可以承擔？

劉昱均執行秘書：

（一）iWIN 係根據兒少法第 46 條成立，因為並無單一部會之量能可單獨承擔相關業務，所以係以跨部會方式，由各大機關出資成立。出資之六大部會組成，係有鑑於當時部分重大事件及輿論和此六大部會有關。iWIN 的工作是任務型執行計畫，只是計畫辦公室，並非法人。

iWIN 職責大抵可以分為四部分：網路行為觀察、處理民眾申訴、推動業者自律（因為 iWIN 無法人格且無強制力，故仰賴業者自律尤其重要）、教育宣導（包

含對政府機關，包含司法機關、警政機關，以弭平各機關法規遵循程度之差距）因為自律防護必定會勝過事後救濟裁罰手段，故業者自律有其重要性，比方日本業者，業者會考量到自己的商業信譽便愛惜羽毛。我國就此出現兩個問題：台灣業主會自律嗎？如何落實境外業者自律？

為了落實自律，iWIN 就有害兒少身心內容訂定自律共同標準。為了定義何謂有害兒少身心，以及何謂適當防護措施，iWIN 針對此二抽象概念作具體研究，將有害身心內容分為六大類：色情、暴力、恐怖、血腥、危險物品、其他有害內容。

另外有鑑於「內容分級制度」在網路內容管制上比較有困難，目前是採取四個層級做處理：1.警示性防護 2.阻攔性防護（彈跳出提示詢問是否為 18 歲） 3.嚴格年齡限制（如果單純問是否滿 18 歲，只能算是阻攔性防護，必須問出生年月，或者透過信用卡來做年齡驗證） 4.禁止表現（此部分因為限制言論自由，所以需要有法令規範，比方兒少色情，兒少色情沒有灰色地帶，法令規定一律禁止表現）。對於限制性內容，在 iWIN 網站有詳細定義。

iWIN 另外提供業者自律框架五大原則：1.使用者規範（此係為了讓使用者明白使用該平臺的規定，幫助業者能夠有效管理平臺內容，另外這種使用者規範有參考境外業者的標準，以符合境內外業者公平對待）、2.平臺自我審查機制（平臺若自身有產製內容，應該訂定自我審查機制，避免誤觸兒少法 46-1 條受罰）、3.防護措施、4.申訴管道（使用者對業者）、5.機關連繫窗口。

（二）iWIN 原則上不主動去查是否有不當內容。iWIN 會先主動通知業者改善，如果未改善會轉案。

林律師提問：針對兒少法第 46 或 69 條情形，有直接下架措施嗎？

劉執秘答：目前無論是境內或者境外域名，iWIN 沒有過下架的案件，主要還是要靠業者自律。

（三）民眾申訴內容有違法疑慮，若經過 iWIN 審查過後確認有問題，無論境內境外業者，只要聯絡的到，iWIN 通通會通知。如果業者對於內容防護仍未改善，iWIN 才會將案件後送到法令主管機關。此方法境內業者成效大約在 70-80%，境外業者大約在 50%，但是兒少法方面的案件，例如兒少色情內容案件，業者大多都會主動把內容下架，因為業者會在意自己的名聲，例如 Facebook 或 Twitter，這兩個品牌不會想要跟兒少色情沾上邊。

（四）參考問題（三）回答。

（五）參考前一題回答，iWIN 作法並非行政處分，主要是在凝聚業者共識並推動自律。

（六）一個域名被下架之後，業者還是可以繼續去產生一個新域名，我們成效有限，因此我們對停止解析採保留態度。我們也沒看過有任何國內成功把業者下架的案例，只有國外案例，亦即透過 app store 把應用程式下架。以上談到的甚至包含兒少性剝削網站，我們也沒有成功封掉過。

因為一個網站使否被下架需要實質內容判斷，若其中只有 1%的內容違法，其餘

內容和兒少保護無關，例如政治性言論，若將其下架便會有箝制言論自由的問題，操作上會出現爭議。

（七）目前我們沒有刑事警察局斷源專案的做法。

（八）見到下述三、四題之回答

案例檢討

二、近期 SWAG 網站是否使用是否與　貴機構之通報有關？

答：SWAG 在 107 年起有接受 iWIN 自律輔導，但中間有漸漸較少聯繫，但只要一有相關新聞有出現，就會主動聯繫 iWIN，希望我們提供自律改善建議。

後來因被偵辦的緣故，檢察官要求 SWAG 要建立防護機制，後續我們便持續協助盤點平臺機制，目前的模式也逐步建立了默契與信任。

立法及行政政策

三、如果未來要增加網路言論處理之法源依據，　貴機構是否有立法建議?擴大應「限制年接取、瀏覽之措施，或先行移除」之內容?

四、是否仿照日本 SIA（Safer Internet Association）之模式，擴大　貴機構通報內容之範圍?

林律師問：是否會擴大範圍給其他領域？例如接受農委會、經濟部主管之違法內容下架？

劉執秘答：iWIN 無法擴張業務，因為法源就是兒少法。但是 iWIN 工作模式可以被複製，故其他主管機關法令可以同樣方式操作，將違法內容下架。只是不同內容需要有不同的制度訂定方式。目前的做法應該是看看有無 iWIN 之外其他單位有興趣承作其他主管機關相關業務。

余老師：贊成交給電腦公會承接其他內容類型的業務。我們需要把 iWIN 組織之績效優點呈現出來，以期能成立其他類似 iWIN 之組織。至若緊急案件應對機制，我認為不必在各部會成立新的組織，應以 NCC 提供的架構下自行附加法源基礎。

答：再回到有關停止解析之問題，因為違反兒少法的內容以形式審查即可判斷，但是假消息是需要實質判斷的，所以停止解析未必是最好方法，停止解析比較適合形式判斷的內容。再者，如果 iWIN 的強制力變高，審查過程上勢必會再變慢。

三、 中華電信數位通信分公司

網域名稱涉有違反相關法律之實例研究及處置建議委託研究採購案

業者代表訪談-中華電信數位通信分公司

時　　間：110 年 6 月 17 日下午 3 時 30 分

地　　點：因應新冠肺炎疫情改為遠端會議，

出席人員：駱建宇股長、林方傑工程師、恆業法律事務所團隊（戴豪君博士、余啟民教授、林上倫律師、曹廷豪律師）

記　　錄：曹廷豪律師

本次訪談過程如下：

一、講解域名生態圈
請參考本次域名生態 word 檔案。（此部分再請林工程師檢附相關資料與本團隊。）
二、財團法人台灣網路資訊中心（下稱 TWNIC）使用網域名稱回應政策區域（Domain Name Response Policy Zone, 下稱 DNS RPZ）之端序為何？ （一） 需有行政機關之行政處分？抑或機關發函即為已足？抑或民間團體（諸如:I WIN）通報即足? （二） 需有法官刑事扣押裁定？抑或檢、警附帶扣押即為已足？ （三） 影響資安之重大情況如何定義？自「雪崩案件」[288]以觀，似乎調查局來函（不須依法為行政處分），TWNIC 即阻斷有資安疑慮之網站。
林上倫律師： 中華電信有無收到法院裁定或行政處分後進行 DNS 的停止解析？ 林方傑工程師： 1. TWNIC 的 DNS RPZ 政策主要是各業者 由 TWNIC 判斷網站內容之違法性，業者們再行配合政策將有問題的網域名稱停止解析。 2. 在 TWNIC 主導 RPZ 政策前，RPZ 技術即行之有年。過去配合警方斷源專案，針對違反善良風俗如毒品、色情網站停止解析。 余啟民教授： RPZ 會議參與成員有誰? 目前決議前是否採用 RPZ 政策與斷源專案雙軌進行；是否有著名案例可供參考? 林方傑工程師： 1. 由 TWNIC 發開會通知，除 TWNIC 的執行長參與外，NCC 長官及 ISP 業者大部

[288] 同註 271。

分都有被邀請參與會議。

2. TWNIC 開始討論 RPZ 政策後，目前尚未收到斷源專案之來函。但在 RPZ 政策實施前，如有相關來函會配合辦理。
3. 斷源專案來函要求停止解析的網域名稱多是名不見經傳的網域名稱，且多是賭品及色情。

林上倫律師：
不是法院命令，僅是檢警的通知函就執行停止網域名稱解析嗎?

林方傑工程師：
由警方來函，函文中如說明違法刑法等法律，並說明欲停止解析之 DNS。

余啟民教授：
是否除了刑事警察局外，其他單位也有相關專案?如保智大隊、電信警察是否也會發函?

林方傑工程師：
斷源專案統一由刑事警察局作為窗口發函給中華電信。

林上倫律師:
是否能提供本團隊去識別化之來函以供研究參考?

林方傑工程師：
建議透過刑事警察局管道取得。

三、停止解析、下架該網域名稱與 DNS RPZ 阻止使用者進入網站之差別為何？

林方傑工程師：
1.實施機構不同：

- DNS RPZ 主要由 DNS Resolver 快取主機（ISP 業者）及 Authoritative Name Server 權威主機進行處理。
- 下架網域名稱主要由網域名稱註冊商及受理註冊機構進行處理。

2. 效力範圍不同：

- DNS RPZ 需透過 DNS Resolver 快取主機（ISP 業者）參與配合，如未參與 DNS 政策，客戶端仍可透過未配合之 DNS Resolver 快取主機（ISP 業者）連結至該網域名稱。
- 取消網域是根本作法，即無該網域名稱存在，客戶端無法連結至相關網域名稱。

林上倫律師：
是否可能類似設防火牆，讓所有客戶端無法連結到該網域名稱?此外，是否能參酌中國及時把網路內容下架的做法。

駱建宇股長：
1. 與客戶端設定有關，此為獨立於 DNS 解析之外的技術。
2. 建立類似守門員機制阻擋連結相關網域名稱越來越困難，因現行許多網站多採

取 Https 架構使網站內容保密，故守門員無法知悉該網域名稱內容為何，進而封鎖連結該等網域名稱。

3. 大陸長城要求網站提供商不能使用 Https 架構，且不能將內容加密及不能使用 VPN。現今除大陸政府外，無人知悉具體長城技術及作法為何，僅有推測可能封包存取等方式，知悉並阻擋連結相關網域名稱，但實際執行上需花費大量資源。此外，大陸架設網站需要申請相關執照，如網站違法可透過申請資料，找到網站負責人。以台灣民情，大陸長城不適合用於台灣。

四、使用 DNS RPZ 之主體是否限於 TWNIC？

林方傑工程師：

自不同角度觀之，DNS RPZ 之施行主體會有所不同：

1. 將特定網域名稱列入 DNS RPZ 之權限以觀，TWNIC 即屬施行主體。TWNIC 得確認網站是否違法不當，並使配合參與 RPZ 政策之業者一起停止解析特定網域名稱。其中，參與 RPZ 政策之業者眾多，建議取得相關會議記錄確認參與業者。
2. RPZ 為技術之一種，故具有此方面專業之人均可以實行，在此角度下，多數具有快取主機之 ISP 業者均為 RPZ 之施行主體。除加入 DNS RPZ 政策外，特定業者亦可以外購網域名稱黑名單加入該業者之快取主機，以達到停止特定網站解析之目的。

駱建宇股長：

1. 中華電信不會主動介入及阻擋客戶連線至相關網域名稱，除非具有正當原因，如機關發函要求阻擋客戶連線至釣魚網站。
2. 業者自行購買黑名單阻擋客戶連線至該等網域名稱，此一般情況為加值服務且事前皆須取得客戶同意。

五、DNS RPZ 是否為針對境外特定網域名稱之有效處置手段？有無其他處置方式？

林方傑工程師：

以 DNS RPZ 技術而言，該網域名稱為境內或境外並不影響網域名稱停止解析之運作。

目前較擔心為可能誤停止解析境外網域名稱，蓋停止解析部分 DNS 可能影響其他合法之網域名稱使用者。以 FB 為例，「facebook」網站中之一篇貼文被認為是違法言論，如 DNS RPZ 停止解析「facebook」網站，可能使其他合法之內容一併受到影響。

林上倫律師：

目前中華電信有提供租用權威主機之服務，或透過與租用人之契約或因實質掌控權威主機進而將相關網頁內容刪除嗎?

林方傑工程師：

原則上不會介入用戶使用，實務上亦無發生介入租用人使用之情形。ISP 業者不會對網路使用者之內容進行任何處置。

林上倫律師：
經 TWNIC 黃執行長之說明，會針對「.tw」之網域名稱使用 serverHold 技術以達到該網站的全面停止解析，請問中華電信是否可以直接阻斷客戶連結到相關網域名稱，以達到類似「sever hold」的效果?

駱建宇股長：
第一次聽到 serverHold，基於本單位之認知，最有效阻斷任何人看到特定網站內容的方法仍是請求平臺業者或是網路內容創作者自行刪除內容。

六、如果使用國外 VPN 連接被 DNS RPZ 阻隔之網站，一般人是否仍可以順利進入？

林方傑工程師：
一般而言，外國之 VPN 會有自己的快取主機，而這些快取主機不會加入 DNS RPZ 政策，是以，使用 VPN 連線之網路使用者仍可順利進入列為 DNS RPZ 名單之網站。

七、近期 SWAG 網站是否使用 DNS RPZ 技術？根據新聞報導[289]，刑事局與九大電信業者合作，啟用 DNS RPZ 的手法，阻隔一般人進入網站瀏覽，惟目前觀察，現在登入 SWAG 網站僅有「該網站正在配合調查」之提醒，並無新聞所述不得進入網站之情形。是否 DNS RPZ 還有轉移連接至他網站之功能？

林方傑工程師：
實際網站是否被阻擋要看 land page。SWAG 目前應該沒有使用到 RPZ 停止解析技術。且轉移連接至他網站之功能和 DNS RPZ 無關，應為該網站之所有人配合檢警單位調查所進行之內部設定。

林上倫律師：
停止解析的網域名稱不明確時，是否有要求提供更明確的資料?

林方傑工程師：
TWNIC 的 RPZ 政策仰賴 TWNIC 審查申請停止解析相關網域名稱之資料是否齊全及符合 RPZ 政策規範。業者收到清單後會再確認一次。
斷源專案實務上有以技術原因告知警方無法配合處理。如該網域為泛用型網域名稱，不僅是有問題網域名稱會使用，正常用戶亦會使用到。故此類型網域名稱即無法配合停止解析。

八、依照 TWNIC 官方對 DNS RPZ 之說明，當不當網域名稱或 IP 位址寫入主節點 DNS RPZ 時，所有參與 DNS RPZ 的次級節點會限制接取此不當網域名稱或 IP 位址。所謂參與「DNS RPZ 的次級節點係指所有「網際網路服務提供業者」?」有無未參與 DNS RPZ 的次級節點?（致使成為 DNS RPZ 之阻隔漏洞）

林方傑工程師：
中華電信只是次級節點之一。TWNIC 目前邀請所有業者參與，此提問建議詢問

[289] 同註 284。

TWNIC 可得到更具體說明。

九、DNS RPZ 得否進一步就該網域名稱之特定內容進行阻隔？

林方傑工程師：
DNS RPZ 無法針對網頁之部分內容進行阻隔。

十、受理註冊機構（諸如:中華電信、網路中文）依照使用人條款停止提供網域名稱服務之端緒為何？
（一） 需有行政機關之行政處分？抑或機關發函？抑或民間團體（諸如:I WIN）通報即足?
（二） 需有法官刑事扣押裁定？抑或檢、警附帶扣押即為已足？
（三） 影響網路安全之情況是否亦屬之？
（四） 其效果和 DNS RPZ 阻止使用者進入該網站之差別為何？
（五） 是否有相關案例？

林方傑工程師：
中華電信並無能力自行判斷網域名稱內容違法與否，故僅是被通知進行停止解析相關網域名稱。網站違法與否多由 TWNIC 或主管特定事物之行政機關判斷。

林上倫律師：
註冊人不付網域名稱註冊費，是否可依雙方契約終止使用網域名稱權限?

林方傑工程師：
不付註冊費，依序進入贖回期等，最後註銷網域名稱等，皆是在 ICANN 框架下，訂立使用人條款。

十一、ISP 業者如何就特定網站之內容為刪除？對境外網站可否為之？

林方傑工程師：
ISP 業者無法刪除客戶之網站內容。因刪除相關內容，需要網站管理之帳戶權限。是以針對主管機關或 TWNIC 告知本公司存在之不當內容，本公司僅能停止提供網路服務，而通常都是採取停止解析網域名稱做為執行之手段。

十二、根據 110 年度聲扣字第 11 號裁定，法院同時通知**受理註冊機構依據服務協議限制該網址之使用**，及**透過 TWNIC 停止解析該網站**，藉此將該網址納入我國公權力支配下而為扣押處分。TWNIC 是否有依法院之扣押裁定對下述網站為停止解析?

林上倫律師：
被扣押的網站有些顯示 404，理由為何?

林方傑工程師：
顯示 404 為 Http 架構下表示錯誤即該網頁內容不存在。顯示 404 代表 DNS 工作已完成找出 IP ，並連結到網頁，僅是網頁內容不存在。小鴨等因網域名稱註冊簡單，故難以徹底解決盜版問題。
今日再就上述網站為觀察，均已成為 DNS RPZ 之管制名單。

十三、如果未來要增加網路言論處理之法源依據，貴公司是否有立法建議?

林方傑工程師：

此問題需另外請教公司法務同仁。法務同仁較關注程序面完整 （如有無公文或正式來函，及受理函文對象明確等）。

余啟民教授：

法務指總公司法務嗎?總公司法務也會參與嗎?

林方傑工程師：

1. 主要由數據公司法務同仁處理。但出席 TWNIC RPZ 會議，總公司法務也有一起配合出席，並由法務同仁討論後統一由總公司對外說明。
2. 目前較關心的是如果停止解析網域名稱是否會造成客訴的問題。會續有相關客訴，如能告訴客戶具體因違反何等法律致停止解析網域名稱，較能快速解決客訴問題。

余啟民教授：

斷源專案未有明確的法律授權。這可能與 TWNIC 要求法律明確授權有所衝突。此部分於 TWNIC 舉行的會議中和刑事警察局討論此問題，始更完善 RPZ 執行授權問題。請問針對前述問題刑事警察局有列席會議嗎?

林方傑工程師：

沒有注意到刑事警察局有無出席會議。

四、 新世紀資通股份有限公司

業者訪談大綱—新世紀資通

一、 貴公司是否有配合財團法人台灣網路資訊中心（下稱 TWNIC）之網域名稱回應政策區域政策（Domain Name Response Policy Zone, 下稱 DNS RPZ），停止解析任何網域名稱？

（一） 需有行政機關之行政處分？抑或機關發函即為已足？抑或民間團體（諸如：iWIN、TWNIC）通報即足?

說明：本公司願意配合法令停止解析特定網域名稱，惟前提應有法源依據，由特定行政機關依法通知本公司配合辦理。

（二） 需有法官刑事扣押裁定？抑或檢、警附帶扣押即為已足？

說明：停止解析特定網域名稱對於網域名稱使用人及 ISP 業者皆有極大影響，若倉促認定即便事後撤銷，對於網域名稱使用人及 ISP 業者所產生之損害恐難以回復，故應有法官刑事扣押裁定。

二、 貴公司是否因影響人民網路使用安全之情況而配合國安單位下架網域名稱或停止解析網域名稱之案例？自「雪崩案件」[290]以觀，似乎調查局來函（不須依法為行政處分），各 ISP 業者即須阻斷有資安疑慮之網域名稱。

說明：本公司辦理停止解析或下架特定網域之行為皆依相關行政機關通知辦理。

三、是否可能類似設防火牆（如色情守門員、大陸長城），讓所有客戶端無法連結到該網域名稱?此外，是否能參酌中國及時把網路內容下架的做法。

說明：若特定網域名稱已列入 DNS RPZ 執行名單辦理停止解析或下架等措施時，使用國內網域名稱則無法連結至該網域名稱。

四、除 DNS RPZ 所列之黑名單外，各業者是否有內部之「黑名單網域名稱」？

說明：本公司辦理停止解析或下架特定網域名稱之名單皆依相關行政機關通知辦理。

五、 貴公司是否有依據「網域名稱之使用者協議」停止提供網域名稱服務？如有，所使用之手段為何（下架網域名稱、停止解析網域名稱等……）？

貴公司停止對使用者提供網域名稱服務後，使用國外 VPN 連接是否仍可瀏覽該網域名稱?

說明：本公司辦理停止解析或下架特定網域名稱之行為皆依相關機關通知辦理。

依照 VPN 連接技術，的確可以使用國外 VPN 連接被 DNS RPZ 阻隔之網站。

六、承上題，受理註冊機構（諸如:中華電信、網路中文）依照使用人條款停止提供網域名稱服務之程序為何？

（一） 需有行政機關之行政處分？抑或機關發函？抑或民間團體（諸如:I WIN）通報即足?

（二） 需有法官刑事扣押裁定？抑或檢、警附帶扣押即為已足？

（三） 影響網路安全之情況是否亦屬之？

290 同註 271。

（四） 其效果和 DNS RPZ 阻止使用者進入該網站之差別為何？

（五） 是否有相關案例？

說明：新世紀資通股份有限公司依照 TWNIC Domain Name Registration Agreement 規定，TWNIC 得於有關機關通知後，有權對已註冊之域名執行暫停或採取必要措施; TWNIC DNS RPZ 與業者 DNS RPZ 為主從架構，因此業者 DNS RPZ 會與 TWNIC DNS RPZ 同步執行停止提供網域名稱服務之程序。

七、根據 110 年度聲扣字第 11 號裁定[291]，法院同時通知**受理註冊機構依據服務協議限制該網址之使用**，及**透過 TWNIC 停止解析該網站**，藉此將該網址納入我國公權力支配下而為扣押處分。試問，**受理註冊機構依據服務協議限制該網址之使用**之具體案例為何？

說明：因本公司並未有相關案例且亦非 110 年度聲扣字第 11 號裁定之當事人，故無法表示意見。

八、如果使用國外 VPN 連接被 DNS RPZ 阻隔之網站，是否仍可以順利瀏覽該網站之內容？

說明：依照 VPN 連接技術，的確可以使用國外 VPN 連接被 DNS RPZ 阻隔之網站。

九、貴公司是否有將一網站之特定內容進行刪除或阻隔之方式？

說明：本公司停止解析或下架特定網域名稱等行為皆依相關機關通知辦理，並無主動針對網站之特定內容進行刪除或阻隔。

十、如果未來要擴大停止解析或下架特定網域名稱之法源依據（諸如：禁止網路上張貼迎娶外籍新娘之廣告、禁止張貼違法日租套房廣告等），貴公司對此之態度為何？

說明：本公司願意配合法令停止解析或下架特定網域名稱，惟前提應有法源依據。至於法律具體內容及範圍，本公司尊重立法機關職權。

十一、針對特定網域名稱濫用行為，建議由民間通報抑或由行政機關通報?針對上述情況　貴公司之立場及立法建議為何?

說明：在有法源依據之前提下，本公司願意配合法令協助處理網域名稱濫用行為，至於究竟應由何單位通報、通報效果為何等，本公司建議應於法令內明訂，以為遵循依據；又法律具體內容及範圍，本公司尊重立法機關之專業及職權。

[291] 台灣台北地方法院 110 年度聲扣字第 11 號刑事裁定

五、 亞太電信股份有限公司

業者訪談大綱—亞太電信

一、 貴公司是否有配合財團法人台灣網路資訊中心（下稱 TWNIC）之網域名稱回應政策區域政策（Domain Name Response Policy Zone, 下稱 DNS RPZ），停止解析任何網域名稱？

ANS :是。

（一） 需有行政機關之行政處分？抑或機關發函即為已足？抑或民間團體（諸如：iWIN、TWNIC）通報即足?

ANS :目前僅有依 110.03.09 TWNIC 電子郵件通知執行過乙次。

（二） 需有法官刑事扣押裁定？抑或檢、警附帶扣押即為已足？

ANS :目前僅有依 110.03.09 TWNIC 電子郵件通知執行過乙次。至於其他案件，本公司將依據相關法律規定辦理。

二、 貴公司是否因影響人民網路使用安全之情況而配合國安單位下架網域名稱或停止解析網域名稱之案例？ 自「雪崩案件」[292]以觀，似乎調查局來函（不須依法為行政處分），各 ISP 業者即須阻斷有資安疑慮之網域名稱。

ANS :否。

三、是否可能類似設防火牆（如色情守門員、大陸長城），讓所有客戶端無法連結到該網域名稱?此外，是否能參酌中國及時把網路內容下架的做法。

ANS :否。

四、除所列之黑名單外，各業者是否有內部之「黑名單網域名稱」？

ANS :否。

五、 貴公司是否有依據「網域名稱之使用者協議」停止提供網域名稱服務？如有，所使用之手段為何（下架網域名稱、停止解析網域名稱等……）？

ANS :停止解析網域名稱。

貴公司停止對使用者提供網域名稱服務後，使用國外 VPN 連接是否仍可瀏覽該網域名稱?

ANS :是。

六、承上題，受理註冊機構（諸如:中華電信、網路中文）依照使用人條款停止提供網域名稱服務之端序為何？

（一） 需有行政機關之行政處分？抑或機關發函？抑或民間團體（諸如:I WIN）通報即足?

（二） 需有法官刑事扣押裁定？抑或檢、警附帶扣押即為已足？

（三） 影響網路安全之情況是否亦屬之？

（四） 其效果和 DNS RPZ 阻止使用者進入該網站之差別為何？

[292] 同註 271。

（五） 是否有相關案例？

ANS：

（一） 本公司依據亞太電信『網域名稱/虛擬主機/企業郵件/HackerScan』服務條款，提供及辦理提供使用人網域名稱服務有關事宜。

（二） 依據亞太電信『網域名稱/虛擬主機/企業郵件/HackerScan』服務條款第4.2.g條約定:「網域名稱註冊使用，須確保其資訊防護措施之完備及安全，如因可歸責甲方（使用人）之事由，足資影響他人權益或危害網路運作，WEBCC 及乙方（亞太電信）於接獲相關機關通知後，得視情況暫停甲方（使用人）所註冊之網域名稱或為其他必要之處置。」

（三） 【停止提供網域名稱服務】與【DNS RPZ 阻止使用者進入該網站】二者間之主要差別在於影響範圍的大小。例如：若採停止提供某網域名稱服務，所有連線要去該網站時，皆無法開啟該網站。若採 DNS RPZ 阻止使用者進入該網站方式，則只有客戶端 DNS 設定我方 CDNS IP，才無法開啟該網站。

（四） 目前亞太電信僅有依 110.03.09 TWNIC 電子郵件通知執行過停止解析任何網域名稱乙次，沒有其他相關案例。

七、根據 110 年度聲扣字第 11 號裁定[293]，法院同時通知**受理註冊機構依據服務協議限制該網址之使用**，及**透過 TWNIC 停止解析該網站**，藉此將該網址納入我國公權力支配下而為扣押處分。試問，**受理註冊機構依據服務協議限制該網址之使用**之具體案例為何？

ANS：此案亞太電信僅配合 110.03.09 TWNIC 電子郵件通知停止解析 8 個網站。

八、如果使用國外 VPN 連接被 DNS RPZ 阻隔之網站，是否仍可以順利瀏覽該網站之內容？

ANS：是。

九、 貴公司是否有將一網站之特定內容進行刪除或阻隔之方式？

ANS：否。

十、如果未來要擴大停止解析或下架特定網域名稱之法源依據（諸如：禁止網路上張貼迎娶外籍新娘之廣告、禁止張貼違法日租套房廣告等），貴公司對此之態度為何？

ANS：本公司將依據相關法律規定辦理。

十一、 針對特定網域名稱濫用行為，建議由民間通報抑或由行政機關通報?針對上述情況 貴公司之立場及立法建議為何 ？

ANS：本公司將依據相關法律規定辦理。

[293] 同註 291。

六、 鼎嘉數位有限公司

業者訪談大綱—鼎嘉數位科技

一、 貴公司是否有配合財團法人台灣網路資訊中心（下稱 TWNIC）之網域名稱回應政策區域政策（Domain Name Response Policy Zone, 下稱 DNS RPZ），停止解析任何網域名稱？

有

（一） 需有行政機關之行政處分？抑或機關發函即為已足？抑或民間團體（諸如：iWIN、TWNIC）通報即足?

Twnic 之前都沒有通知我們，就直接把網址處理了。我們都是後來客人與我們反映，才知道網址被拿走了。

（二） 需有法官刑事扣押裁定？抑或檢、警附帶扣押即為已足？

目前沒有接觸這樣的客人

二、 貴公司是否因影響人民網路使用安全之情況而配合國安單位下架網域名稱或停止解析網域名稱之案例？自「雪崩案件」[294]以觀，似乎調查局來函（不須依法為行政處分），各 ISP 業者即須阻斷有資安疑慮之網域名稱。

TWNIC 不能有裁判功能，因該保持中立，即使被國際警察，或是中華明國政府裁定，TWNIC 藥效訪國際 .ORG 註冊局，有許多 https://thepiratebay.org/ 是無法被取消的網址，即使有多少次的裁定是盜版網站，但是他的網址依舊正常使用，它 2004 註冊到現在，網站也活得好好的。

如果這些都是商業行為，不至於國家及安全，如果是中國或是它國（俄羅斯，北韓的攻擊 DDoS） 成為國家安全，twnic 才有可能考慮介入，商業攻擊，不關 twnic 的事。詐騙只是商業行為而已，不是國家級攻擊。

各 ISP 不因該接受商業犯罪的裁定而阻斷了網路服務，網路犯罪也只是商業犯罪之一，沒有流血，也沒有死人，只是帳面上的損失。

如果今天是駭客攻擊核電廠的電腦，飛機機場，這是可以臨時停止服務，因為這個會死人。

唯有小政府，台灣網路才會進步。如:425+1=426，與其他公然侮辱的法律已讓台灣網路環境動彈不得，台灣人必須要有言語的自由，才不會被有力人士把語言當作武器，我們看到了反送終，人民無法用自己的語言表達心裡的意識，台灣的公然侮辱罪，有可能就是為來的中國的國安法的起源。

三、是否可能類似設防火牆（如色情守門員、大陸長城），讓所有客戶端無法連結到該網域名稱?此外，是否能參酌中國及時把網路內容下架的做法。

不會

四、除所列之黑名單外，各業者是否有內部之「黑名單網域名稱」？

[294] 同註 271。

yes
五、　貴公司是否有依據「網域名稱之使用者協議」停止提供網域名稱服務？如有，所使用之手段為何（下架網域名稱內容、停止解析網域名稱等……）？　貴公司停止對使用者提供網域名稱服務後，使用國外 VPN 連接是否仍可瀏覽該網域名稱? yes
六、承上題，受理註冊機構（諸如:中華電信、網路中文）依照使用人條款停止提供網域名稱服務之端序為何？ （一）　需有行政機關之行政處分？抑或機關發函？抑或民間團體（諸如:I WIN）通報即足? （二）　需有法官刑事扣押裁定？抑或檢、警附帶扣押即為已足？ （三）　影響網路安全之情況是否亦屬之？ （四）　其效果和 DNS RPZ 阻止使用者進入該網站之差別為何？ （五）　是否有相關案例？no
七、根據 110 年度聲扣字第 11 號裁定[295]，法院同時通知**受理註冊機構依據服務協議限制該網址之使用**，及**透過 TWNIC 停止解析該網站**，藉此將該網址納入我國公權力支配下而為扣押處分。試問，**受理註冊機構依據服務協議限制該網址之使用**之具體案例為何？
八、如果使用國外 VPN 連接被 DNS RPZ 阻隔之網站，是否仍可以順利瀏覽該網站之內容？
九、　貴公司是否有將一網站之特定內容進行刪除或阻隔之方式？ yes
十、如果未來要擴大停止解析或下架特定網域名稱之法源依據（諸如：禁止網路上張貼迎娶外籍新娘之廣告、禁止張貼違法日租套房廣告等），貴公司對此之態度為何？ 這違反了語言自由
十一、針對特定網域名稱濫用行為，建議由民間通報抑或由行政機關通報?針對上述情況　貴公司之立場及立法建議為何? 言語自由因該是受到憲法保證的最上層，可以效仿美國

[295] 同註 291。

七、 協志聯合科技股份有限公司

業者訪談大綱—協志聯合科技

一、 貴公司是否有配合財團法人台灣網路資訊中心（下稱 TWNIC）之網域名稱回應政策區域政策（Domain Name Response Policy Zone, 下稱 DNS RPZ），停止解析任何網域名稱？

（一） 需有行政機關之行政處分？抑或機關發函即為已足？抑或民間團體（諸如：iWIN、TWNIC）通報即足?

目前以 TWNIC 通知即可。此外 TWNIC 為 RPZ 通報窗口，故行政機關發函通知對象應為 TWNIC。

（二） 需有法官刑事扣押裁定？抑或檢、警附帶扣押即為已足？

不需要。此外法院裁定原則上本公司不會知情，且通知窗口應為 TWNIC。

二、 貴公司是否因影響人民網路使用安全之情況而配合國安單位下架網域名稱或停止解析網域名稱之案例？ 自「雪崩案件」[296]以觀，似乎調查局來函（不須依法為行政處分），各 ISP 業者即須阻斷有資安疑慮之網域名稱。

尚未遇到

三、是否可能類似設防火牆（如色情守門員、大陸長城），讓所有客戶端無法連結到該網域名稱?

目前沒有。若有這類要求須依 TWNIC 通知各家討論。

此外，是否能參酌中國及時把網路內容下架的做法。

無法。受理註冊商的角色，僅是受理客戶申請網域名稱及管理客戶網域名稱使用權限.，並無實權管理戶的網頁內容。此外如何判斷內容濫用執行上亦有困難。

四、除 DNS RPZ 所列之黑名單外，各業者是否有內部之「黑名單網域名稱」？

五、無自設黑名單，依 TWNIC 指示配合。

六、 貴公司是否有依據「網域名稱之使用者協議」停止提供網域名稱服務？

如有，所使用之手段為何（下架網域名稱內容、停止解析網域名稱等……）？

尚未遇到。

貴公司停止對使用者提供網域名稱服務後，使用國外 VPN 連接是否仍可瀏覽該網域名稱?

不確定。

七、承上題，受理註冊機構（諸如:中華電信、網路中文）依照使用人條款停止提供網域名稱服務之端序為何？

（一） 需有行政機關之行政處分？抑或機關發函？抑或民間團體（諸如:I WIN）通報即足?

目前以 TWNIC 通知即可。

（二） 需有法官刑事扣押裁定？抑或檢、警附帶扣押即為已足？

法院裁定原則上本公司不會知情。遇此情況會先行通知 TWNIC 確認，待

[296] 同註 271。

收到 TWNIC 回覆後處理。

（三） 影響網路安全之情況是否亦屬之？

亦是先行通知 TWNIC 確認，並發信提醒客戶請客戶檢查，並待 TWNIC 進一步通知。

（四） 其效果和 DNS RPZ 阻止使用者進入該網站之差別為何？

不確定。

（五） 是否有相關案例？

無。

八、根據 110 年度聲扣字第 11 號裁定[297]，法院同時通知**受理註冊機構依據服務協議限制該網址之使用**，及**透過 TWNIC 停止解析該網站**，藉此將該網址納入我國公權力支配下而為扣押處分。試問，**受理註冊機構依據服務協議限制該網址之使用**之具體案例為何？

無，僅接受 TWNIC 通知。

九、如果使用國外 VPN 連接被 DNS RPZ 阻隔之網站，是否仍可以順利瀏覽該網站之內容？

不確定。

十、貴公司是否有將一網站之特定內容進行刪除或阻隔之方式？

無。僅是受理客戶申請網域名稱及管理客戶網域名稱使用權限.，並無實權管理戶的網頁內容。此外執行上客戶及網域名稱眾多無能力依依判斷網域名稱內容違法不當。

十一、 如果未來要擴大停止解析或下架特定網域名稱之法源依據（諸如：禁止網路上張貼迎娶外籍新娘之廣告、禁止張貼違法日租套房廣告等），貴公司對此之態度為何？

本公司為受理註冊機構，並無權管客戶網域名稱內容，由主管機關訂立相關規範後配合處理。

十二、 針對特定網域名稱濫用行為，建議由民間通報抑或由行政機關通報?針對上述情況 貴公司之立場及立法建議為何?

如為民間第三方專業機構（如 IWIN），經審查民眾通報後，再行通知公司處理為可行方式。公司接獲通知後，會將相關情形通報 TWNIC，待 TWNIC 通知後，進行下一步處理。

[297] 同註 291。

八、 台灣大哥大股份有限公司

業者訪談大綱—台灣大哥大

一、 貴公司是否有配合財團法人台灣網路資訊中心（下稱 TWNIC）之網域名稱回應政策區域政策（Domain Name Response Policy Zone, 下稱 DNS RPZ），停止解析任何網域名稱？

本公司配合 TWNIC RPZ 政策。

（一） 需有行政機關之行政處分？抑或機關發函即為已足？抑或民間團體（諸如：iWIN、TWNIC）通報即足?

依法令規範配合辦理

（二） 需有法官刑事扣押裁定？抑或檢、警附帶扣押即為已足？。

依法令規範配合辦理

二、 貴公司是否因影響人民網路使用安全之情況而配合國安單位下架網域名稱或停止解析網域名稱之案例？自「雪崩案件」[275] 以觀，似乎調查局來函（不須依法為行政處分），各 ISP 業者即須阻斷有資安疑慮之網域名稱。

目前未曾接獲國安單位來函。

三、是否可能類似設防火牆（如色情守門員、大陸長城），讓所有客戶端無法連結到該網域名稱?此外，是否能參酌中國及時把網路內容下架的做法。

N/A。

四、除 DNS RPZ 所列之黑名單外，各業者是否有內部之「黑名單網域名稱」？

N/A。

五、 貴公司是否有依據「網域名稱之使用者協議」停止提供網域名稱名稱服務？如有，所使用之手段為何（下架網域名稱內容、停止解析網域名稱等……）？ 貴公司停止對使用者提供網域名稱服務後，使用國外 VPN 連接是否仍可瀏覽該網域名稱?

依據附件網域名稱代管服務契約，若客戶（乙方）未遵守網際網路規範時，我司可以不經用戶同意下停止解析網域名稱服務。終止代管網域名稱時，使用國外 VPN 連接無法瀏覽該網域名稱。

六、承上題，受理註冊機構（諸如:中華電信、網路中文）依照使用人條款停止提供網域名稱服務之端序為何？

（一） 需有行政機關之行政處分？抑或機關發函？抑或民間團體（諸如:I WIN）通報即足?

依法令規範及契約辦理

（二） 需有法官刑事扣押裁定？抑或檢、警附帶扣押即為已足？

依法令規範及契約辦理

[275] 同註 271。

（三） 影響網路安全之情況是否亦屬之？

依法令規範及契約辦理

（四） 其效果和 DNS RPZ 阻止使用者進入該網站之差別為何？

如透過停止網域名稱服務，該網域名稱即無法被瀏覽。而 DNS RPZ 只能影響我司 DNS 服務的客戶端，第三方 DNS 不受影響。

（五） 是否有相關案例？

N/A

七、根據 110 年度聲扣字第 11 號裁定[276]，法院同時通知受理註冊機構依據服務協議限制該網址之使用，及透過 TWNIC 停止解析該網站，藉此將該網址納入我國公權力支配下而為扣押處分。試問，受理註冊機構依據服務協議限制該網址之使用之具體案例為何？

N/A

八、如果使用國外 VPN 連接被 DNS RPZ 阻隔之網站，是否仍可以順利瀏覽該網站之內容？

VPN 大多使用國外 DNS，應仍可順利瀏覽網頁。

九、貴公司是否有將一網站之特定內容進行刪除或阻隔之方式？

N/A

十、如果未來要擴大停止解析或下架特定網域名稱之法源依據（諸如：禁止網路上張貼迎娶外籍新娘之廣告、禁止張貼違法日租套房廣告等），貴公司對此之態度為何？

原則上只要有法規依據，本公司均會配合，但下架特定網域名稱需考量實務執行上之可行性

十一、針對特定網域名稱濫用行為，建議由民間通報抑或由行政機關通報?針對上述情況　貴公司之立場及立法建議為何?

針對特定網域名稱濫用行為，民間通報可做為行政機關通報之參考依據，但業者執行仍應以行政機關通報為宜

[276] 同註 291。

九、 台灣之星電信股份有限公司

業者訪談大綱—台灣之星

一、 貴公司是否有配合財團法人台灣網路資訊中心（下稱 TWNIC）之網域名稱回應政策區域政策（Domain Name Response Policy Zone, 下稱 DNS RPZ），停止解析任何網域名稱？

（一） 需有行政機關之行政處分？抑或機關發函即為已足？抑或民間團體（諸如：iWIN、TWNIC）通報即足?

（二） 需有法官刑事扣押裁定？抑或檢、警附帶扣押即為已足？

二、 貴公司是否因影響人民網路使用安全之情況而配合國安單位下架網域名稱或停止解析網域名稱之案例？自「雪崩案件」[277] 以觀，似乎調查局來函（不須依法為行政處分），各 ISP 業者即須阻斷有資安疑慮之網域名稱。

無。

三、是否可能類似設防火牆（如色情守門員、大陸長城），讓所有客戶端無法連結到該網域名稱?此外，是否能參酌中國及時把網路內容下架的做法。

目前環境僅能透過 DNS 停止解析網域名稱令用戶無法透過網域名稱連結至目標，並無規劃類防火牆之作法。

四、除 DNS RPZ 所列之黑名單外，各業者是否有內部之「黑名單網域名稱」？

無。

五、 貴公司是否有依據「網域名稱之使用者協議」停止提供網域名稱服務？如有，所使用之手段為何（下架網域名稱內容、停止解析網域名稱等……）？ 貴公司停止對使用者提供網域名稱服務後，使用國外 VPN 連接是否仍可瀏覽該網域名稱?

無。停止解析網域名稱後用戶若使用 VPN 或指定其他 DNS 仍可瀏覽。

六、承上題，受理註冊機構（諸如:中華電信、網路中文）依照使用人條款停止提供網域名稱服務之端序為何？

（一） 需有行政機關之行政處分？抑或機關發函？抑或民間團體（諸如:I WIN）通報即足?

（二） 需有法官刑事扣押裁定？抑或檢、警附帶扣押即為已足？

（三） 影響網路安全之情況是否亦屬之？

（四） 其效果和 DNS RPZ 阻止使用者進入該網站之差別為何？

（五） 是否有相關案例？

七、根據 110 年度聲扣字第 11 號裁定 [278]，法院同時通知**受理註冊機構依據服務協議限制該網址之使用**，及**透過 TWNIC 停止解析該網站**，藉此將該網址納入我國公權力支配下而為扣押處分。試問，**受理註冊機構依據服務協議限制該網址之使用**之具體案例為何？

八、如果使用國外 VPN 連接被 DNS RPZ 阻隔之網站，是否仍可以順利瀏覽該網站之

[277] 同註 271。

[278] 同註 291。

內容？ 若用戶透過他網之 DNS 進行解析，則仍有機會可順利瀏覽內容。
九、　貴公司是否有將一網站之特定內容進行刪除或阻隔之方式？ 現行無針對一網站之特定內容進行刪除或阻隔方式，
十、如果未來要擴大停止解析或下架特定網域名稱之法源依據（諸如：禁止網路上張貼迎娶外籍新娘之廣告、禁止張貼違法日租套房廣告等），貴公司對此之態度為何？ 依法遵辦。
十一、針對特定網域名稱濫用行為，建議由民間通報抑或由行政機關通報?針對上述情況　貴公司之立場及立法建議為何? 皆可由民間或行政機關通報後，交由主管機關裁定並通知電信業者執行。

十、 網路中文資訊股份有限公司

業者訪談大綱—網路中文

一、 貴公司是否有配合財團法人台灣網路資訊中心（下稱 TWNIC）之網域名稱回應政策區域政策（Domain Name Response Policy Zone, 下稱 DNS RPZ），停止解析任何網域名稱？

（一） 需有行政機關之行政處分？抑或機關發函即為已足？抑或民間團體（諸如：iWIN、TWNIC）通報即足?

（二） 需有法官刑事扣押裁定？抑或檢、警附帶扣押即為已足？

DNS RPZ 起源於 2020 年由 Godaddy、Amazon、Neustar、PIR 等 48 家大型網路註冊機構提出網域名稱濫用框架倡議（DNS Abuse Framework）。

TWNIC DNS RPZ 主要運作是其與國內 ISP 業者建構 DNS RPZ（又稱之 DNS 快取伺服器服務），限制境內外惡意網域名稱或 IP 位址接取，為國內網路使用者提供資安防護的第一線防衛措施；網路中文是臺灣第一家獲得 ICANN、TWNIC 認證資格的受理註冊機構（又稱註冊商），本公司非 ISP 業者，主要核心業務為提供網域名稱解析及網域名稱註冊管理服務，故本公司非 TWNIC DNS RPZ 合作商，雖無法配合 DNS RPZ，但仍有配合執行依法規、協議及符合 ICANN 要求的適當處置。

二、 貴公司是否因影響人民網路使用安全之情況而配合國安單位下架網域名稱或停止解析網域名稱之案例？自「雪崩案件」[298]以觀，似乎調查局來函（不須依法為行政處分），各 ISP 業者即須阻斷有資安疑慮之網域名稱。

本公司尚無案例。

依據本公司與 TWNIC 網域名稱受理註冊授權合約 增補條款第 2.原合約第二條新增之第九項：受理註冊機構於接獲 TWNIC、相關單位、當事人之通知，或於其他情形下知悉註冊者有濫用行為或違法活動，應代理 TWNIC 依照「財團法人台灣網路資訊中心網域名稱申請同意書」第一條第三項以及第九條、相關主管機關之命令或法令規定採行適當執行措施。於採行執行措施之前，得先詢問 TWNIC 意見。

因此，若本公司接獲 TWNIC、相關主管機關之命令或法令規定關於 TW 系列網域名稱之通知，將於執行措施之前，先詢問 TWNIC 意見，再採行適當執行措施。而非 TW 域名則仍需有法院裁判再執行措施。

三、是否可能類似設防火牆（如色情守門員、大陸長城），讓所有客戶端無法連結到該網域名稱?此外，是否能參酌中國及時把網路內容下架的做法。

技術上可設防火牆，但客戶若使用跳板、VPN 將失去效用；管理機制之規劃仍需依法建構。

四、除 DNS RPZ 所列之黑名單外，各業者是否有內部之「黑名單網域名稱」？

本公司內部無網域名稱黑名單。

[298] 自由時報，我調查局與 31 國聯手偵破「雪崩」網路犯罪集團 https://news.ltn.com.tw/news/society/breakingnews/1904635

網域名稱註冊者申請網域名稱有可能會涉及違反網域名稱註冊管理機構所制定之規範、及其所在地區之法令規範、中華民國法律、註冊申請人所在地之法律、ICANN 所訂之規範，致網域名稱遭註冊管理機構拒絕申請或凍結刪除。

五、貴公司是否有依據「網域名稱之使用者協議」停止提供網域名稱服務？如有，所使用之手段為何（下架網域名稱內容、停止解析網域名稱等……）？　貴公司停止對使用者提供網域名稱服務後，使用國外 VPN 連接是否仍可瀏覽該網域名稱?

本公司有依法規及協議進行停止解析的機制，但目前為止沒有案例，若被我們停止解析之後，無人可瀏覽該網域名稱。

六、承上題，受理註冊機構（諸如:中華電信、網路中文）依照使用人條款停止提供網域名稱服務之端序為何？

（一）需有行政機關之行政處分？抑或機關發函？抑或民間團體（諸如:I WIN）通報即足?

（二）需有法官刑事扣押裁定？抑或檢、警附帶扣押即為已足？

（三）影響網路安全之情況是否亦屬之？

（四）其效果和 DNS RPZ 阻止使用者進入該網站之差別為何？

（五）是否有相關案例？

（一）及（二）

TW 系列網域名稱依 TWNIC 網域名稱受理註冊授權合約及其增補條款，於接獲 TWNIC、相關單位、當事人之通知，或於其他情形下知悉註冊者有濫用行為或違法活動，應代理 TWNIC 依照「財團法人台灣網路資訊中心網域名稱申請同意書」、相關主管機關之命令或法令規定採行適當執行措施。於採行執行措施之前，得先詢問 TWNIC 意見。非 TW 網域名稱則需有法院裁判較無爭議。

（三）受理註冊機構無權獨斷是否屬影響網路安全之情況。

（四）停止提供服務給註冊者使用與僅不被使用者看見。

（五）暫無案例。

七、根據 110 年度聲扣字第 11 號裁定[299]，法院同時通知**受理註冊機構依據服務協議限制該網址之使用**，及**透過 TWNIC 停止解析該網站**，藉此將該網址納入我國公權力支配下而為扣押處分。試問，**受理註冊機構依據服務協議限制該網址之使用**之具體案例為何？

110 年度聲扣字第 11 號裁定為依法不得公開之案件。

具體案例暫無。

八、如果使用國外 VPN 連接被 DNS RPZ 阻隔之網站，是否仍可以順利瀏覽該網站之內容？

目前 TWNIC 推動之 DNS RPZ 係由國內 ISP 業者阻斷其 DNS 解析，故透過 VPN 連接此網站仍可取得所有資料，若要達到完全阻斷 TW 系列網域名稱之被瀏覽，其實需由 TWNIC 進行 serverHold 之作業使該網域名稱停止所有運作。

[299] 台灣台北地方法院 110 年度聲扣字第 11 號刑事裁定

九、貴公司是否有將一網站之特定內容進行刪除或阻隔之方式？ 本公司沒有對於網站特定內容及頁面進行刪除或阻隔的方式;從域名端處理則是可以使該網站全體服務受阻隔。
十、如果未來要擴大停止解析或下架特定網域名稱之法源依據（諸如：禁止網路上張貼迎娶外籍新娘之廣告、禁止張貼違法日租套房廣告等），貴公司對此之態度為何？ 依法行政。
十一、針對特定網域名稱濫用行為，建議由民間通報抑或由行政機關通報?針對上述情況　貴公司之立場及立法建議為何? 建議依法由行政機關通報。 任何判斷或執行均需法源依據，無法以民間業者自律構成。 本公司為致力穩定各頂級網域名稱，根據 ICANN 及各註冊商註冊協議（Registry-Registrar Agreement）之要求，遵循網域名稱反濫用，若註冊者有濫用行為，本公司或各網域名稱註冊管理機構有權凍結或刪除網域名稱或終止網路相關服務。 若有法規授權及制定流程並有司法資源協助，則受理註冊機構凍結、刪除網域名稱或終止相關服務時較無爭議且較有能力即時防止更大損害。

附錄三　座談會會議記錄

「網域名稱涉有違反相關法律之實例研究及處置建議委託研究」 期末座談會議

會議紀錄

時　　間：110 年 10 月 22 日（星期五）上午 10 時至 12 時

地　　點：線上會議

主　　席：計畫主持人 戴豪君老師

出席人員：

恆業法律事務所團隊：

戴豪君教授、余啟民教授、林繼恆律師、胡博硯教授、林上倫律師、曹廷豪律師、簡佑霖律師、鄭淵仲律師

NCC：

林永裕科長、林秉豐科員

專家學者：

數位經濟暨產業發展協會	詹婷怡律師
世新大學	何吉森教授
高雄科技大學	程法彰教授
元智大學	葉志良教授
資策會科技法律研究所	顧振豪副所長

業者：

iWIN	劉昱均執行秘書
網路中文	劉莘相董事長
網路中文	杜敏蓉執行長
網路中文	魏駿光資深經理
網路中文	賴欣昀業務經理

網路中文	賴俞帆總經理特助
網路中文	陳宛萱執行秘書
網路中文	劉家榮網路分析師
網路中文	謝銘仁研究員
網路中文	徐子欣
台灣大哥大	胡政嘉資深主任工程師
台灣大哥大	莊雅婷資深主任管理師
中華電信	駱建宇股長
中華電信	林方傑工程師
中華電信	詹雅然管理師
新世紀資通	顧信弘經理
新世紀資通	饒大忠技術副理
新世紀資通	黃惠中技術副理
新世紀資通	廖鈺鳴資深專員
亞太電信	李建勳經理
鼎家數位	李鼎嘉負責人
鼎家數位	楊于怡
鼎家數位	黃珮珍

報 告 人：林上倫律師

記　　錄：簡佑霖律師

壹、主席致詞

謝謝大家參與今天「網域名稱涉有違反相關法律之實例研究及處置建議委託研究」的期末座談會，感謝大家蒞臨與指導。這裡以會議主持人身份向大家介紹與會來賓（下略），並請林上倫律師進行今天座談會報告。

貳、研究團隊報告（略，參見報告投影片）

參、綜合討論

業者發言部分

一、 戴豪君教授：

謝謝林上倫律師的報告，就以下討論主題，請各位來賓分享意見與建議：

（一）是否各領域主管機關要求刪除網域名稱內容或是停止解析時，於相關法規內應明文「限制我國網路使用者接取、瀏覽之措施或移除網頁內容」，以符合法律保留原則？

（二）是否各領域主管機關要求刪除技術濫用或是停止解析時，以符合法律保留原則？

（三）是否註冊管理機構（TWNIC）知悉或收受通知面對網域名稱濫用時，應自行認定是否違法？

（四）以「停止解析」做為「網域名稱濫用」之處置手段應符合比例原則？

（五）是否網域名稱內容濫用由第三方機構判斷網際網路內容是否存在違法或不當，再將相關資訊彙整通報給各主管行政機關、檢警單位及 ISP 業者？

（六）是否針對停止解析等處分無法查明或難以送達網域名稱註冊人時，以「公告」代替送達？

（七）各業者於收到 TWNIC 停止解析特定網域名稱之指示後，是否有

執行上之困難？

二、 iWIN 劉昱均執行秘書：

（一）iWIN 不只處理兒少色情，也會處理有害兒少身心健康之內容，此種內容有一定的範圍，比如說像是詐騙不實訊息仍在我們管理範疇下，但至於像農委會或者疾病管制等言論，就不會是在我們的處理範圍裡面。

（二）我們對於業者原則上都是採取業者自律的模式，如果我們對於業者發出通知，業者不會有所謂的異議管道，但會直接跟我們討論，業者的自律標準我們也很清楚地在官網上提供給業者。

（三）至於停止解析的部分，我們認為必須以台灣法律有明確規定者為限，亦即法律明文規定網路上不可以出現的內容。我們認為違法內容應該以不同目的事業主管機關來訂定，決定是否要停止解析。不過這樣有一個可能的缺點，就是有每個機關停止解析的標準可能不一樣的問題。

（四）至於是否要擴大 iWIN 職權，我們原則上是尊重主管機關意見。不過 iWIN 編制不大，又兒少規範範圍已經很多。我們也認為說如果假設不同的處理內容，有不同的類似 iWIN 的單位其實也還蠻好的，以避免所有的內容都集中在同一個機構裡，而導致這個機構可能在某個程度來講權力過大。

三、 中華電信林方傑工程師：

我這裡代表中華電信以技術角度發言。域名封鎖的技術難度小，這個單純要執行的話很容易。現在是制度面問題，域名封鎖需要有法源依據。同時通報濫用之情資的品質也很重要，以免誤判，導致合法的內容被下架。

四、 台灣大哥大胡政嘉資深主任工程師：

停止解析的技術不是問題。我們發現詐騙網站很多，如果用停止解析的

方式管理，採取從嚴認定的話，時間會很久，擋掉一個會再出現一個；從寬認定的話速度會快很多，但是會有錯殺的風險。

五、 亞太電信李建勳經理：

停止解析技術上沒問題，現況手動執行也沒問題，至於情資的品質好壞，則需投入時間去做判斷，這個我們跟前面台灣大哥大意見相同，所以業者大家面對的問題都很類似。

六、 新世紀資通顧信弘經理：

我們遇到的問題大抵上就是停止解析案件我們會重複收到公文，或者來函可能來自不同窗口，內容有重複性，通報稍嫌凌亂，因此我們希望通報窗口可以單一。

七、 網路中文劉莘相董事長：

（一）依法行政有其重要性，停止解析必須要有法律授權。

（二）我們不認為民間團體可以在沒有法源下作決定。

（三）透過 RPZ 停止解析最有影響力者為並非「.tw」系列網域名稱，RPZ 效力主要適用境外網域名稱之停止解析。

（四）我們認為對於境外網站而言，有一個救濟管道是很重要的。以免衍生其他法律後續糾紛。

八、 鼎家數位李鼎嘉負責人：

我想從經濟學的角度發表意見，我們臺灣有 113 個立法委員，每一個立法委員選上大概要 3000 萬到一億的錢，這錢立委要回收。因此立委在議題選擇上他要看到議題有投資報酬率。

專家學者發言部分：

一、數位經濟暨產業發展協會 詹婷怡律師：

（一）我這裡不會針對議題一一回應，而是希望協助受託單位釐清架構以及建議。我覺得太多的人因為不理解網路治理的架構，所以在討論很多議題的時候，邏輯沒有處理清楚讓很多的議題都糊在一起。

（二）我具體建議研究分為幾個層次：既然我們的研究對象應該是網域名稱，並且我們手段希望用 RPZ，因此我們要了解域名在層級化網路治理架構以及 Multi-stakeholders 機制，以同時提升各方資訊及網路素養。接著我們才能理解 RPZ 對網路治理裡面扮演何種角色。RPZ 是一個限制網路接取的技術手段，原始目的為域名系統服務提供的功能之一，以維持網路基礎設施之運作。後來 ICANN 以及 Internet Society 對於域名濫用之討論，以及相關機構倡議提出之 DNS abuse framework 作為 Norm 形式的技術自律規範，針對技術濫用類型分為：惡意軟體、殭屍網路、網路釣魚、偽冒嫁接、垃圾郵件形式濫用等，加上網路中介者在 RPZ 技術手段上之協力。

（三）再來才必須了解，因為網路從開始發展的時候，最重要的任務是要能夠互通互聯，而且要能夠達到穩定，然後再延伸到具有韌性。而因為 DNS 是個可控的節點，所以會被用以犯罪。所以 DNS 本來是技術濫用的問題。

（四）DNS 以前是技術濫用問題，現在還有營運模式跟內容的問題。故 RPZ 技術是否以及如何延伸至內容領域的範圍，有關法律保留以及各該主管機關之法規適用問題須依靠立法以及法院判斷。所以技術的 RPZ 跟內容的 RPZ 是不一樣的，不能混在一起講之後然後說我們需要一個第三方機構。

（五）衍生到下一個層次，接下來我們才會討論到中介者是誰，中介者

是否該審查內容、該如何承擔責任。我們不能直接說要找一個第三方，因為無論是要找 ISP 業者或 iWIN，定位跟屬性會很不一樣，同時也要注意第三方獨立機構的侷限性。

（六）最後才會討論到，RPZ 以外有沒有其他手段？比方說網路中文有提到，非 tw 域名其實有其他方法可以處理。或者扣押域名，雖然現在美國法上比較可行，其他國家幾乎不可行，可是其實我們有沒有考慮到在司法上面怎麼去做這個部分的修法？接下來要延伸到內容管制的時候，可能因為涉及到與單純技術層次不一樣的問題，比方說言論自由等，再進一步作討論。

（七）至於說 iWIN，我覺得 iWIN 是個非常成功的典範，他是第一線快速回應的機制，處理很多內容，並且很快地跟很多單位合作，比方衛福部、警政署、社會局。不過我們要搞清楚這個典範是在上述研究邏輯架構下的位置。同時各個目的事業主管機關法令必須配合與時俱進。

二、世新大學何吉森教授：

（一）有關各領域主管機關分別制定法規的問題，我想特別提到兒少法方面，很高興 iWIN 被大家信任。我認為 iWIN 可以再做得更多。

（二）有關網域名稱的規範，可看到兒少法第 46 條第 3 項內容，大抵是符合 ICANN 的由下而上、業者自律的精神。未來其他事務領域應該要記得這種制度精神。

（三）至於第三題說有沒有可能讓 TWNIC 自行認定內容有無違法，我過去在新聞局廣播電視事業處當處長時，我們曾經就討論過電信業者是否能向電信協會成立一個第三方機構，並由第三方機構認定內容是否違法。我們還可以看到英國的部分，就內容管理或兒少保護是分開由不同機構管理，他們很強調「共管」。我是認為主管機關沒那麼多時間，前端還是需要一個機構幫忙。

（四）iWIN 他符合 ICANN 由下而上的精神，但是至於說他的職權是否

要擴大到技術濫用的部分，我會有所保留。

（五）我同意 RPZ 應該作為最後手段。至於剛剛詹律師提到美國法的對物扣押，在台灣能否變成真正的法律，我也認為需要再觀察。

三、元智大學 葉志良老師：

（一）我很認同詹律師的看法，RPZ 一開始是技術面跟網路資安的管理方法，且現在網域名稱都是以自律為主。依我過去處理網路著作爭議的經驗，發現業者協力不夠完整，另外法制面上也應有依據，讓第三方機構做出任何決定有所依循。

（二）再來是第三方機構的定位，應該是自律角色。另外第三方機構作決定時，其內部應如何執行、是否有內部檢核動作，都需要建立完整制度。

（三）單一立法或者個別立法也要好好思考。內容違法在行政層面或者第三方機構會比較不好處理，因此內容類跟技術類案件可能要分開來處理。急迫及非急迫性網域名稱濫用於制度上也必須分開處理。

（四）我最後也想提到共管，我是認為台灣目前業者自律都還做得不夠好，共管的話可能還無法討論。

四、科技法律研究所 顧振豪副所長：

（一）我們科法所這裡算是長期處理域名爭議，這裡整理幾個案例分享。針對網域名稱濫用挪威適用刑事程序沒收（扣押）方式；比利時是透過政府機關經濟局，不是沒收（扣押）網頁而是在中間跳出警告頁面，作為嚴重侵權案件的最後手段；英國比較特殊，近年停止域名案件相當多，英國透過其他執法機構向註冊管理機構或是受理註冊機構通報，以網域名稱註冊人與受理註冊機構間契約進行。

（二）至於我國的刑事訴訟法，本來就可以沒收功犯罪之物，只是在實

物上較少案例。ICANN 之前有一個域名扣押指引，或許可以做為我國刑事域名扣押之參考。至於我國我覺得可以參考看看我國是否要使用定暫時狀態假處分方式進行。

五、高雄科技大學 程法彰教授：

（一）我首先想討論平臺業者部分。歐盟數位服務法有強化中介平臺責任，尤其是有關內容處理，如果平臺業者自己就有一套遊戲規則，應該考慮是不是就可以讓業者先去做。當然我們要考慮言論自由的問題，不同的言論涉及到言論自由之限制也不同。

（二）我會傾向不要用各部會立法的模式，我傾向集中式管理，先作原則性規範，例如先由通傳會訂立法律，在擬定行政規則，去規範平臺業者。這種方式符合馬尼拉原則規範平臺業者自治之精神。

（三）DNS RPZ 我也認同是最終手段。DNS RPZ 是否要利用在內容管制上，也要看未來司法實務上會怎麼做。

（四）iWIN 模式是要求業者加入的自律機制，或許我們可以以行政指導之方式達到由下而上之自治精神。

六、網路中文補充：

網域名稱濫用具跨國性，我們認為網域名稱價格太過低廉會助長濫用情況。至於資安的部分，其實有一個全球統一的通報框架正在擬定中，各國可以參考之，就不必各自為政。以上補充說明。

網路中文並於會議後補充如下：

（一）網域名稱濫用影響具有全球性，DNS 的運作也具有跨國管轄權的特性，因此，在面對這個議題時，ICANN 會議中所討論的網域名稱濫用，技術手段的介入點是在 Registry 和 Registrar。只有 Registry 和 Registrar 才能真正有效的在全球的範圍內遏止濫用行為，但也因為影響性太大，很容易受到比例原則、言論自由的挑戰。

（二）《ICANN 章程》雖然限制了 ICANN 制訂政策採取更積極的 DNS

濫用防治行動，但 ICANN 本身並沒有限制社群內部形成自律機制，在這次 ICANN72 會期預計有幾項自律機制會在締約方通過。

（三）在全球政府方面，GAC 也十分重視這項議題，如日本政府也曾經在會議上強烈指出著作權侵害對其帶來的損害以及 Registrar 濫用窗口失聯的情況；GAC 也在討論過程中重新檢視 ICANN 整體政策，指出「網域名稱的註冊政策」與「定價策略」，也是導致 DNS 濫用的源頭之一。

（四）負責全球網路安全與穩定 SSAC 也提出《SAC115》一文，嘗試提供 ICANN 社群一個可相容之方法來解決 DNS 濫用通報問題。

（五）以上說明，補充國際最新發展供參。

附錄四　成果發表會

時　　間：110 年 11 月 16 日（星期二）上午 10 時至 12 時

地　　點：線上會議

主　　席：射頻與資源管理處 林永裕科長

主講單位：恆業法律事務所研究團隊

議　　程：

議程	時間
報到	10:00 ~ 10:30
主席/長官致辭	10:30 ~ 10:40
網域名稱國際協定及技術介紹	10:40 ~ 10:50
各國對「網域名稱濫用」之立法例 代表性「網域名稱濫用」案例	10:50 ~ 11:30
就網域名稱濫用之態樣，研擬監理性法規	11:30 ~ 11:45
Q&A	11:45 ~ 12:00

成果發表會簡報如下（為求版面統一，另啟新頁）：

致
國家通訊傳播委員會

網域名稱涉有違反相關法律之實例研究及處置建議委託研究採購案
--成果發表會

LIN & PARTNERS 恆業法律事務所

民國110年11月16日

計畫主持人　戴豪君博士

協同主持人　余啟民博士　/ 執行協同主持人　林瓊恆主持律師
專案顧問　胡博硯博士　/專案經理　辜琬宇合夥律師

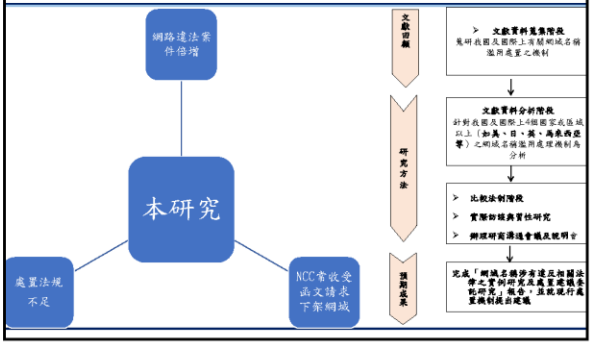
1

目錄

2

第一章 本研究案緣起

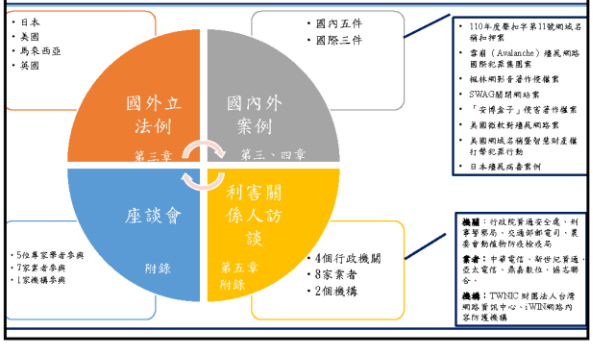
研究案緣起(1)



3

第一章 本研究案緣起

研究案緣起(2)



4

第一章 本研究案緣起

研究案緣起(3)

法源不足

- 僅有兩條法規明文授權該管行政機關將經其認定為違法之網站內容為限制接取、瀏覽，甚至是移除之措施。分為別：
  兒童及少年福利與權益保障法第 46 條之1
  動物傳染病防治條例第38-3條

斷源專案處理網域濫用

- 過去警方使用斷源專案發函給業者方式解決網域濫用問題

第三方民間機構iWIN網路內容防護機構

- 目前我國第三方民間機構iWIN網路內容防護機構，協助通報「有害兒少身心健康」之「網路內容」給業者

5

第一章 本研究案緣起

研究案緣起(4)　（同第七章結論與建議）

網域技術濫用

- 「網域名稱濫用框架」指出該管機構知悉網域名稱技術濫用時，該管機構必須有所作為
- 該管機構具體作為義務及處置手段於我國法多未有明文。
- 建議針對網域技術濫用應有法律授權，使主管機關及該管機構得快速下架或停止解析技術濫用網域

網域內容濫用

- 就網域內容濫用，並無由該管機關自行認定是否內容違法之前例。建議由司法或專業機構負責認定
- 涉及侵害兒少身心之申訴及處理由民間第三方機構iWIN負責，但其他領域，尚無機構負責。
- 可考慮擴大iWIN處理範圍，或另設專責民間第三方機構以處理其他網域濫用問題。
- 我國法規僅有兒童及少年福利與權益保障法及動物傳染病防治條例，授權該管行政機關將違法之網站內容為限制接取、瀏覽及移除。建議其他法律也應增設類似規範，以符合法律授權。

6

目錄

7

網域名稱濫用綜覽

網域技術濫用 → 網域濫用 ← 網域內容濫用

1. 惡意軟體（Malware）
2. 殭屍網路（Botnets）
3. 網路釣魚（Phishing）
4. 偽冒嫁接（Pharming）
5. 以垃圾郵件之形式造成以上濫用之行為（Spam）

1. 兒少性虐待之素材
2. 網路違法販售鴉片
3. 人口販售
4. 具體且可信的煽動暴力
5. 兒童及少年福利與權益保障法第46條
6. 動物傳染病防治條例第38-3條

8

網域名稱國際協定及技術介紹—處理網域名稱濫用框架 (DNS Abuse Framework)

(1) 處理網域名稱濫用框架（DNS Abuse Framework)(自律)

- 網域名稱濫用框架之性質為機構與業者之自律框架機制。其目的在於使註冊管理機構與受理註冊機構遵循一定之定義與程序。自發布實施至今，已有超過50餘參與此框架之註管機構與受理註冊機構，其中包括 GoDaddy, PIR, Neustar, Enom等具國際權威性之註管機構與業者。

域名技術濫用類型

1. 惡意軟體 (Malware)
2. 殭屍網路 (Botnets)
3. 網路釣魚 (Phishing)
4. 偽冒嫁接 (Pharming)
5. 以垃圾郵件之形式造成以上濫用之行為 (Spam)

特殊網域內容濫用

1. 兒少性虐待之素材
2. 網路違法販售鴉片
3. 人口販售
4. 具體且可信的煽動暴力。

業界共識

- 由於註管機構之型態與其於整體網際網路DNS基礎建設之角色，無義務監督、管理網域之內容且無權限因網域內容而禁用網域名稱。註管機構無法處理「網域內容」之濫用，但針對技術濫用有作為義務。
- 註管機構能採取之唯一處理措施僅是將使整個網域名稱失效或禁用 。但此禁用措施無法精準的移除該網域之濫用部份，往往是各國不符合比例原則之措施

處理網域名稱濫用框架之建議:

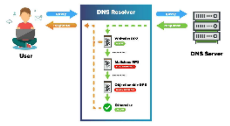
- 註冊管理機構與受理註冊機構就上開「特殊網域內容」考慮使用專業之「受信任之通知者」(Trusted Notifiers)， 以協助濫用控管並於採取處理措施時之提供諮詢。於其他情形，應由投訴人向網站管理者 (Site Operator)、註冊人 (Registrant)或伺服器服務提供者 (Hosting provider)尋求移除濫用內容之救濟方式，而非向註管機構或受理註冊機構提出取消網域名稱名稱之要求。

9

網域名稱國際協定及技術介紹—DNS回應原則區域機制(RPZ)

(2) DNS回應原則區域機制(RPZ)

RPZ作為一個限制網路接取的技術手段，原始目的為域名系統服務提供的功能之一，作為技術濫用之因應措施，以維持網路基礎設施運作。近年討論此技術用於網域內容濫用



DNS RPZ 主要功能

- 藉由DNS解析器得知DNS伺服器之回覆後，透過第三方資安信譽評等機構所提之名單過濾。
- DNS解析器將自動限制惡意網域名稱或IP位址接取，以避免使用者連結到惡意網站。

目前國際業者間尚無針對DNS RPZ之使用有統一之規範或要求：

10

就網域濫用之態樣，研擬管制性規定—處置技術整理

	APNIC、TWNIC下架網域	TWNIC針對「.tw」網域進行Server Hold	DNS RPZ停止解析	通知伺服器業者或是平台業者刪除特定內容	通知創作人刪除特定內容
優	下架網域後，能確保全世界及使用任何途徑都無法瀏覽該網站	對「.tw」網域使用後，能確保全世界及使用任何途徑都無法瀏覽該網站	1.適用範圍廣，不論境內、境外均可使用 2.具時效性 3.不須找到「網域濫用之行為人」即可為之。	就特定內容進行內容下架，能落實「最小侵害」	就特定內容進行內容下架，能落實「最小侵害」
缺	1.難確保境外註管機構確實下架，以我國為例，至今並無任何下架網域之案例 2.不具時效性 3.侵害過大，不符合比例原則	1.僅限「.tw」網域網域 2.侵害過大，不符合最小侵害	1.使用其他快取主機連線後即可閱覽停止解析內容。 2.僅能停止解析整個網站，當網域僅有部分涉及濫用時此手段將不符合比例原則。	1.須確認內容存存之網域為伺服器業者依服務規章將將其刪除。 2.除法律有特別明文外，須待司法程序為之，不具時效性	1.須確實找到「網域濫用之行為人」 2.除法律有特別明文外，須待司法程序為之，不具時效性

11

目錄

12

第三章 各國對「網域名稱濫用」之立法例

日本(1)

項目	說明
規範網路內容之立法例	■ **社團法人安全網路協會（Safter Internet Association 簡稱SIA），參考相關法規之違法要件及態樣訂立安全線運用指引，指引規範網路內容違法及不當** ■ 違法類型包含五大類：性表現及性行為、藥物、轉帳詐欺、侵入他人帳號、成為社會問題之違法（兒童照片及影音、情人及配偶間散布他方情色影音） ■ 不當類型包含： 1.違法行為之要約、引誘、媒介。 2.無法直接判定內容違法，但仍相當程度地懷疑其違法 3.尚未管制到底是脫法之藥品、毒品、合法藥劑等物之仲介、要約、引誘 4.引誘自殺 5.勸誘、引誘以兒童為對象之霸凌 6.刊載被害者遺體、自殺行為影像等明顯傷害遺族感情 7.閱覽人觀看影像後明顯厭惡之遺體、殺害行為之影像
認定為違法/不當之效果	■ SIA收到網路使用者之申報後會將資訊主要交給警察機關、ISP業者、網站管理人、關係機關、網路過濾業者等 ■ SIA本質為民間機構，提出之請求僅具有建議性質並無拘束力

13

第三章 各國對「網域名稱濫用」之立法例

日本(2)

項目	說明
機關有無權限要求註管機構移除或是停止解析網域	■ 總務省對於日本.jp註管機構(Japan Registry Services，下稱JPRS)屬於低度管理，並**無得直接要求註管機構移除或是停止解析違法不當網域之相關法律規範** ■ SIA於指引即強調網路並非由各國政府所管理，而係由自治方式加以維繫
是否有第三方內容認定機構	■ 現行JPRS之註冊規則，以「适用JP網域註冊規則」為例，其第29條規範刪除網域註冊之事由，其第1項第4款規定當**收到判決書、和解書、調解書、仲裁判斷或是與前述同一效力之文書時，JPRS必須將該網域註冊刪除**；及同條項第5款規定，可見無行政機關可要求JPRS對網域進行處置。 ■ SIA於2013年11月由網路業者共同成立接受民眾及網路使用者通報網域內容違法及不當。 ■ 不法及不當之熱線共有兩條，一條於2013年11月由民間自行運作的「安全線」及另外一條2016年4月起受警察廳所委託之「網路熱線中心（簡稱IHC）」。兩條熱線彼此相互分擔業務。
當事人陳述意見機會	■ 基於快速應對違法及不當網路內容，依SIA指引不會給予網頁權利人陳述意見之機會，且過程中不會經過法院審酌 ■ 違法及不當內容之認定SIA期許自己能符合三項標準可信賴性、確保判斷適切、快速對應

14

第三章 各國對「網域名稱濫用」之立法例

日本(3)

- SIA公布2019年數據通報網域放置**違法、有害內容共計47,396件**，其中於日本**境內約10.4%，而高達89.6%為境外網域**
- 2019年SIA**境內外總計發出21,183件請求**，當中有**19,540件成功刪除內容，刪除率約為92%**。，境內網域刪除率約為90%，而境外網域刪除率為93%

通報比例：日本境內 10.4%
刪除率：日本境內90%

通報比例：日本境外 89.6%
刪除率：日本境外93%

15

第三章 各國對「網域名稱濫用」之立法例

日本(4)

日本網域內容濫用—兒童情色

- 針對網路兒童情色問題認為「仍是待解決的問題之一，封鎖(blocking)可被期待作為限制瀏覽之手段，但須要關係者間的彼此合作
- 2011年4月以來，警察及IHC等民間團體通報給**網路內容安全協會(Internet Content Safety Association，簡稱ICSA)，復由ICSA確認並製作黑名單給ISP業者**，最終由ISP業者自主針對兒童情色網站進行DNS停止解析。

法律依據

- **兒童買春、兒童情色行為等規制及處罰並兒童保護相關法第16條之3**：「提供網路供不特定人可發送、閱覽訊息之電信服務業者，基於持有、提供兒童情色之行為在網路上流通造成擴大兒童權益之損害，且一旦散布到國內外，將之刪除以回復兒童權益將變得非常困難。**有鑑於此業者對於搜查機關之協力，及本於業者所擁有之管理權限，應致力於制定針對散播兒童情色之防免措施**」
- 條文可看出針對防止網路散布兒童情色問題，仍是以民間自主為主，政府為輔之方式進行

立法例分析：仍無法規授權行政機關對JPRS下達註銷網域之行政處分

- 即使是「兒童色情」之最嚴重之網域名稱內容濫用態樣，日本仍非以強制公權力手段處理，仍是回歸業者自律。
- DNS RPZ停止解析於日本已有先例，非我國獨有。

16

第三章 各國對「網域名稱濫用」之立法例

日本(5)

日本網域技術濫用—網路釣魚

濫用方式

網路釣魚（Phishing）係指企圖從電子通訊中，透過偽裝成信譽卓著的公司以獲得如使用者名稱、密碼和信用卡明細等個人敏感資訊的詐騙犯罪行為。詐騙者會傳送偽造電子信件，或設立仿造受信任公司(例如Yahoo奇摩、eBay、PayPal 或使用者往來銀行或信用卡公司)登入頁面的偽造網站，誘使受害人填寫使用者名稱（帳號）和密碼。

解決措施：JP網域名諮問委員會第54次會議提及處理網路釣魚處理流程

1. **網路使用人、金融機構、業者等通報**
2. **JPCERT/CC(日本電腦網路危機處理暨協調中心)協助共同確認是否有網路釣魚情形**
3. **與該網域名稱受理註冊機構或ISP業者聯繫**
4. **受理註冊機構或ISP業者將網頁內容刪除或解除契約**
5. 受理註冊機構無法處理時JPRS逕將將網域名稱註銷

立法例分析：仍無法規授權行政機關對JPRS下達註銷網域之行政處分

1. 實務運作上至多於第4步請求受理註冊機構、ISP業者透過與註冊人間之契約條款加以解決用於網路釣魚之網域，而並無至第5步JPRS將網域名稱註銷之情形。
2. 「.jp」網域註冊管理機構多次聲明：「JPRS針對用於網路釣魚之網域濫用問題，並不會直接介入將該網域註銷刪除」

17

第三章 各國對「網域名稱濫用」之立法例

日本(6)

日本以「DNS sinkhole(沉洞)」對抗Vawtrak殭屍病毒

案例背景

Vawtrak的網路病毒在世界各國傳播，控制並感染日本國內約4萬4,000台電腦及國外約3萬8,000台電腦。受病毒感染的電腦會非法轉移受害人網路銀行中的存款。

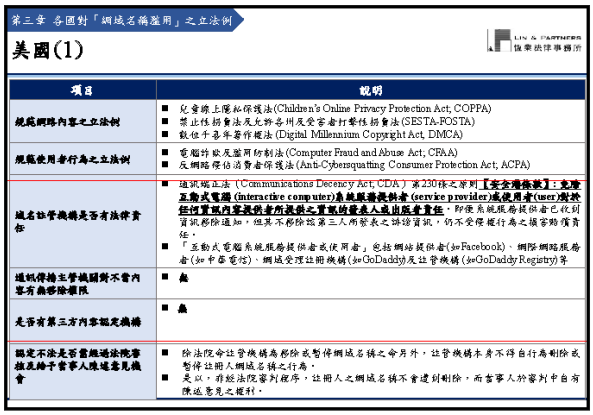
解決措施

為終止殭屍網路，日本各別採取3種手段：

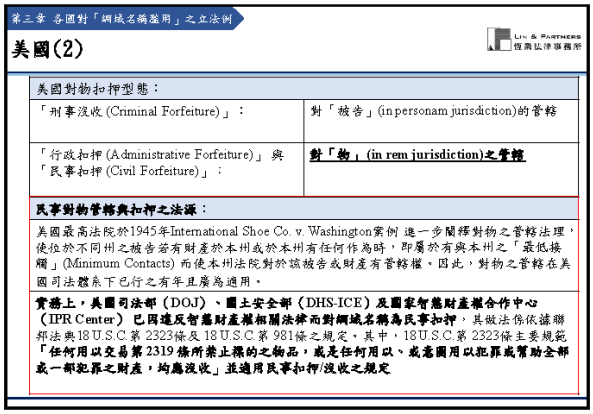
1. 如C&C伺服器在日本境內，可依刑事訴訟法向法院聲請令狀將該伺服器加以扣押並解析。
2. 如C&C伺服器在海外，原則上僅能透過尋求伺服器所在國之司法互助共同進行搜查。
3. 如C&C伺服器在海外，但有有「.jp」之網域名稱，即有尋求「.jp」網域註冊管理機構JPRS之協助，以使用「沉洞」技術解決病毒

尋求「.JP」註冊管理機構JPRS使用「沈洞」技術，**涉及侵害通信秘密及阻斷通信等問題，且其請求不存在法律基礎，有違反「法律保留原則」之可能**

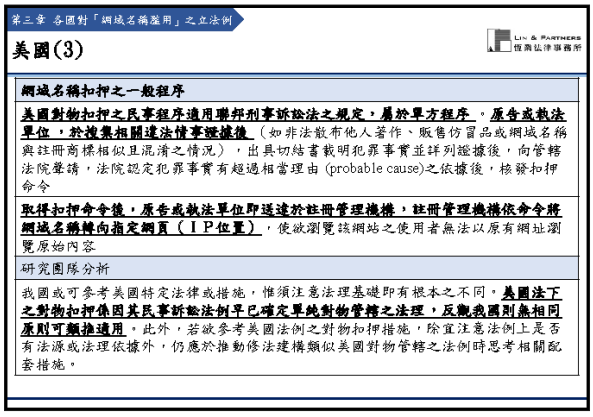
18



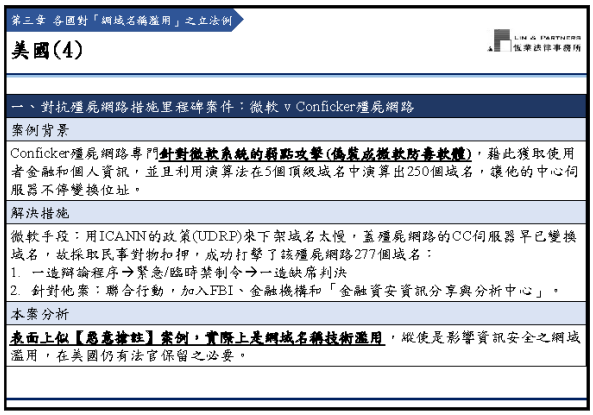
19



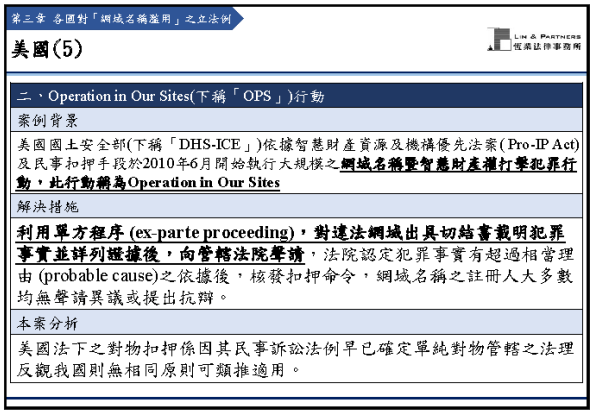
20



21



22



23

24

第三章 各國對「網域名稱濫用」之立法例

馬來西亞(2)

LIN & PARTNERS 恆業法律事務所

違反各法律，依CMA第263條處理網域名稱內容

MCMC進行網站內容審查

- 違反各州伊斯蘭法
- 冒犯性或不雅內容：CMA第233條
- 涉及賄賂：1953年公共賄賂法第4(1)條
- 侵害著作權：1987年著作權法第41條

25

第三章 各國對「網域名稱濫用」之立法例

馬來西亞(3)

LIN & PARTNERS 恆業法律事務所

網站遭屏蔽之頁面	網站因違反雪蘭莪州 1995 年伊斯蘭教法而遭到屏蔽之畫面
	

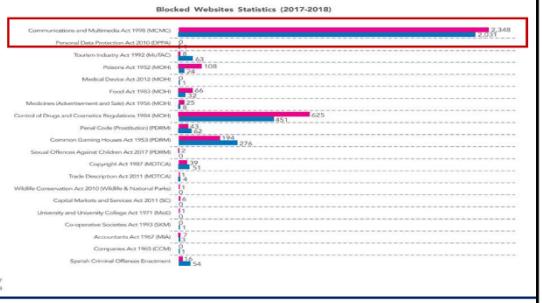
26

第三章 各國對「網域名稱濫用」之立法例

馬來西亞(4)

LIN & PARTNERS 恆業法律事務所

2017-2018馬來西亞網站屏蔽類型數量統計



27

第三章 各國對「網域名稱濫用」之立法例

英國(1)

LIN & PARTNERS 恆業法律事務所

1988年英國著作權、設計和專利法：法院禁制令

- **著作權人可以依據1988年英國著作權、設計和專利法第97A條向英國法院申請禁制令，在「網路服務提供者（ISP）實際上知悉他人利用其提供之網路服務進行侵權行為」時，要求網路服務提供者ISP進行網域阻擋。**
- 在認定ISP是否實際上知悉時，法院應考慮之事項包含ISP者是否已遵循根據《2002 年電子商務（EC 指令）條例》（SI 2002/2013）第 6(1)(c) 條提供的聯繫方式收到通知，以及該通知已有記載考出通知者的全名和地址，與有關侵權的詳細資訊。

第一件英國法院依第97A條核發之禁制令：Newzbin2案

- Newzbin2 是一個僅限會員的網站，整理了大量非法複製材料的連結，包括在 Usenet 討論論壇上找到的電影、音樂和電腦遊戲。
- **於 2010 年 12 月英國電影協會(MPA)應6家好萊塢電影製片廠的要求，以英國ISP業者BT、Sky為相對人，向法院聲請核發禁制令，要求ISP業者實施措施阻止其客戶訪問 Newzbin2。**
- BT與Sky陸續於2011年11月、12月完成屏蔽措施，其後於2012 年 11 月 28 日，Newzbin 2宣布關閉其索引服務。

第一件針對商標侵權核發之禁制令

然而於2014 年 10 月，高等法院依據塵嘩(Richemont)、卡地亞國際(Cartier International)和萬寶龍(Montblanc)之申請，核准向英國主要 ISPs（包含Sky, BT, EE, TalkTalk and Virgin發出了針對商標侵權商貨品的第一項禁制令，以封鎖六個域名。

28

第三章 各國對「網域名稱濫用」之立法例

英國(2)

LIN & PARTNERS 恆業法律事務所

英國ISP業者Sky屏蔽網站之頁面

電影公司(film studies)	
1.	2011年10月26日有關Newzbin2的法院禁制令（20C Fox v BT and 20C Fox v BT (No 2)）
2.	2013年4月24日有關Movie2K 與 DL4all 的法院禁制令，以及針對Movie2K 改名成Movie 4K 後法院另於2013年7月17日下的禁制令
3	2013年7月1日有關EZTV之法院禁制令
4	2013年10月25日有關YIFY-Torrents 與其他四個網站之3個法院禁制令
5	2013 年 11 月 13 日 有 關 SolarMovie and Tube+ 之 法 院 禁 制 令（Paramount v Sky）
6	2014年2月18日有關Viooz 與其他3個網站之法院禁制令(Paramount v Sky 2)
唱片公司(record companies)	
1	2012 年 6 月 13 日 有 關The Pirate Bay（"TPB"）的 法 院 禁 制 令（Dramatico v Sky and Dramatico v Sky (No 2)）
2	2013年2月28日有關Fenopy, H33T and Kat 的法院禁制令（EMI v Sky）
3	2013年10月8日有關1337X與其他20個網站的法院禁制令
英國超級聯賽(FA Premier League)	
1	2013年7月16日有關FirstRow Sports的法院禁制令(FAPL v Sky)

29

第三章 各國對「網域名稱濫用」之立法例

英國 (3)

LIN & PARTNERS 恆業法律事務所

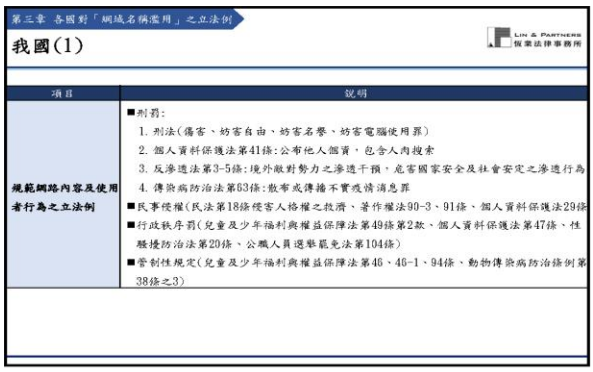
2010年數位經濟法第17條、18條：法院禁制令（已廢止）

- 採取二階段實施方式賦予ISP保護著作權義務：**第一階段ISP就著作權人提出之侵權通報（Copyright Infringement Report），依法負有轉送通知給使用者之義務**，以及依照著作權人要求之期間提出侵害列表的義務。**若第一階段無法有效降低網路著作權侵害問題時，第二階段ISP應採取特定技術措施的義務，例如流量限制、斷線等**
- 然而因於2011年7月法院第一次依1988 年版權、設計和專利法**核發禁制令（Newzbin2案）成功阻止不特定人訪問侵犯著作權之網站，數位文化傳媒和體育部乃於2011 年 8 月 3 日宣布刪除第 17 條和第 18 條**

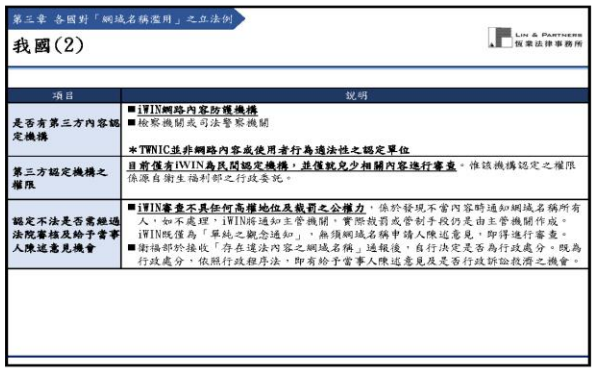
2017年數位經濟法（2017 Digital Economy Act）

- 依2017年數位經濟法第13條，若ISP業者在網站上以商業方式(on a commercial basis)向英國境內之人提供色情素材，則應設置相關措施以**避免未滿18之青少年得以隨時或任意造訪該提供色情素材之網站**
- **兒童色情與淫穢內容之監管主要是仰賴ISP業者的自我監控，由非營利慈善機構——互聯網觀察基金會（Internet Watch Foundation，簡稱IWF）負責協調**。IWF係由英國通信服務提供商（包括ISP、移動電話運營商、互聯網貿易協會、搜索引擎、域名製造商和軟體提供商）自願捐款資助成立
- IWF透過搜索與爬蟲技術，在網路中識別兒童性虐待或兒童色情等圖像與影片，或透過全國無線舉報服務受理民眾之舉報。
- 若已識別網站上之內容為兒童性虐待或色情之素材，**IWF會追蹤其網站之註冊地區，若該註冊地區在英國，則會直接向該註冊者發出通知要求刪除該圖像或影像，若註冊地區在國外，則會聯繫並與該國之警察網絡合作以該國之法制或流程刪除。**由於IWF發現之兒童色情圖片或影像大多是英國境外網站提供之內容，因此也會將**網站網址放在其彙整之URL列表中，供其合作之ISP業者依其定期更新之URL列表阻止英國民眾訪問相關違法網站。**

30



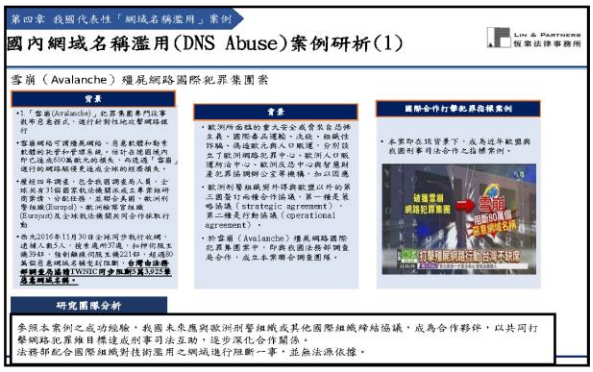
31



32

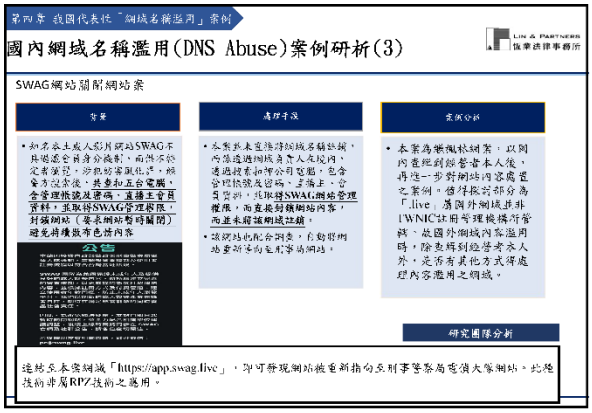
33

34

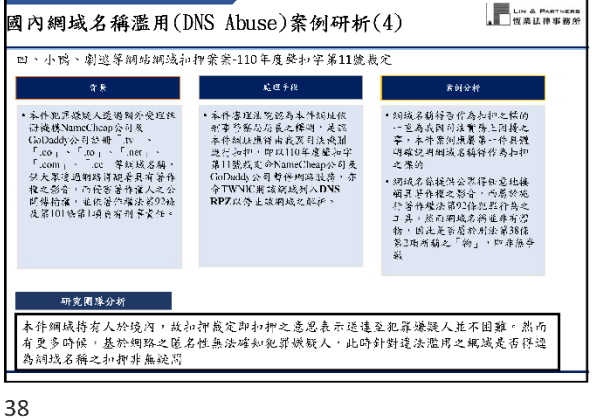


35

36

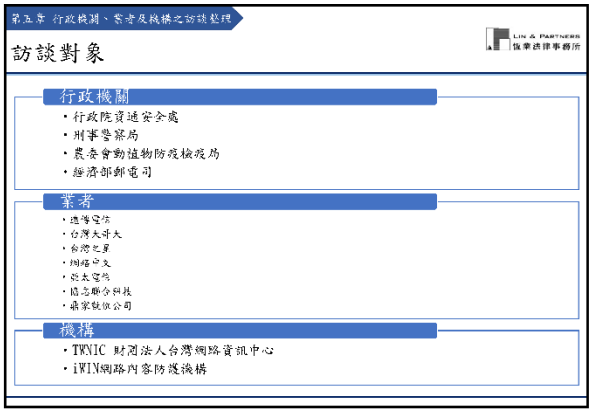


37

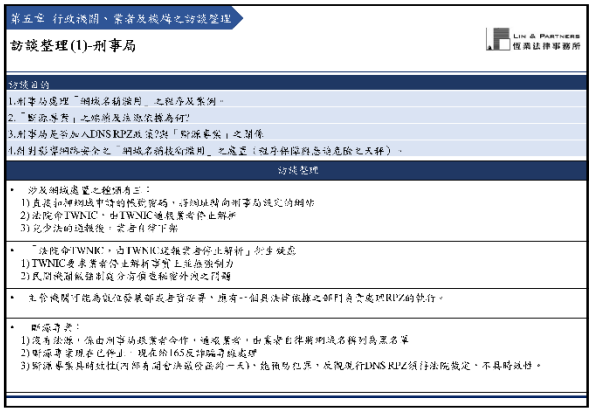


38

39



40



41

42

第五章 行政機關、業者及機構之訪談整理

訪談整理(3)-iWIN 網路內容防護機構

LIN & PARTNERS 恆業法律事務所

訪談目的

1. 瞭解iWIN執行兒童、少年網路內容防護之流程。
2. 瞭解iWIN通報範圍
3. 對日本之通報組織「Safer Internet Association」看法，及對貴機構成為通報所有網域內容濫用之民間機構看法

訪談整理

- 執行情形：
  1) iWin認定之不當內容，係來自人民之申訴檢舉，因案件量大iWin之判斷不會經過委員會，而由承辦專員各自負責，如有判斷上困難，再開研討會議討論。
  2) 國內之網路平台或「.tw」網域大多數會配合iWin之通報。部分境外網域或平台會配合iWin之通報下架內容或其他行為(粗估下架比率約為50%)。
  3) iWin認定內容違法後，會先通知業者自行下架，並告知如不下架，會將違法情狀後送目的事業主管機關及警察機關。目前未曾有遇行政機關接獲iWin通知而停止解析任何網域之行政處分。
- 擴張iWIN業務：
  1) iWIN無法擴張業務，因為法源是兒少法。但是iWIN工作模式可以複製，故其他主管機關得訂立相關法令，採同樣模式處理網域內容濫用。
  2) 違反兒少法的內容以形式審查即可判斷，適合採取停止解析。

43

第六章 就網域濫用之態樣，研擬管制性規

就網域濫用之態樣，研擬管制性規(1)—網域濫用處理手段分析

LIN & PARTNERS 恆業法律事務所

	行政處分	行政執行	刑事扣押	民事暫時狀態假處分	刑事局、調查局直接通知	民間機關通報
法源依據	立法明文主管機關得「限制接取、瀏覽或移除相關網頁內容」之措施。	管制性規定存在，主管機關為落實規定而為直接強制、即時強制之手段。	刑事實體法明定之各項犯罪行為	民事訴訟法第538條 民法相關規定(如第18條人格權保護)	由警察機關通知各業者，為自律機制，無須法源依據。	由民間機關通知各業者，為自律機制，無須法源依據。
優	具時效性，且專責之處分機關具備該領域之專業性	可確實落實各管制性法規之目的	符合程序正義	符合程序正義	最為迅速，可在當日完成	無公權力介入，無違法法律保留的疑慮，具時效性
缺	如行政機關得「限制接取、瀏覽或移除相關網頁內容」之範圍過大，有違憲疑慮	「停止解析網域」作為執行手段侵害過大，不符合比例原則。	緩不濟急，且針對找不到犯罪人之情況，無從執行。	需特定相對人且可能找不到相對人之情況，即無從聲請。	刑事局及調查局有公權力，會有規避法律保留的疑慮	針對涉及專業之「網域技術濫用」民間機構無通報之能力，且民間機關通報之成效難以預期。

46

第五章 行政機關、業者及機構之訪談整理

訪談整理(4)-中華電信

LIN & PARTNERS 恆業法律事務所

訪談目的

1. 了解DNS RPZ之使用程序及範圍。
2. 了解ISP業者依照使用人條款停止提供網域服務

訪談整理

- **DNS RPZ業者角色**
  1) 由TWNIC統一受理(網路業者不會收到來函)，經審核後再透過RPZ機制將符封鎖標的(如域名)通知給參與單位執行(各ISP業者)。
  2) 過去刑警局就會致函給ISP業者要求針對違反善良風俗的網域進行追蹤(斷源專案)。實施DNS RPZ機制後，目前尚未收到斷源專案之來函，但如有相關來函預設應會照往例配合辦理。
- DNS RPZ技術介紹
- 停止解析主要實作於「DNS resolver (或稱DNS快取主機)」，DNS RPZ是一種停止解析、中間攔截的機制。DNS resolver服務提供者除了ISP以外，也不乏國際知名公司如Google、Cloudflare等，是以，如未參與RPZ機制，客戶端仍可透過該DNS Resolver快取主機完成網域解析，連結至對應網站。
- 業者比較關心的是，如果停止解析網域是否會造成客訴的問題，例如相關客訴。如能告訴客戶具體跟違反何等法律致停止解析網域，較能快速解決客訴問題。

44

第六章 就網域濫用之態樣，研擬管制性規

就網域濫用之態樣，研擬管制性規(2)—領域整理

LIN & PARTNERS 恆業法律事務所

	網路安全領域	刑事實體法已規定之犯罪行為	不涉刑事犯罪之行為			爭議領域
			動物傳染病防治	婚姻媒合	日租套房	假消息
雙階理論	無價值言論	賭博、毒品、猥褻、盜版（包含商標及著作）等言論均屬「低價值言論」	多涉及「商業性言論」，雖為低加值言論，但仍有違憲疑慮			縱已有刑事規定，此類言論常涉及「政治性言論」，屬高價值言論
事前或事後管制	事前	事後	事後	事後	事後	事後
比例原則	必定符合最小侵害	多符合最小侵害	符合最小侵害	有不符合最小侵害之疑慮	有不符合最小侵害之疑慮	不符合最小侵害
公益性	高	高	高	中	中	難以判定
對言論自由侵害性	不涉言論自由	低	次低	中	中	高

47

目錄

45

第六章 就網域濫用之態樣，研擬管制性規

就網域濫用之態樣，研擬管制性規(3)

LIN & PARTNERS 恆業法律事務所

各法規主管機關可依下流程圖檢視主管法規有無修正之必要

檢視主管法規
- 檢視管制性法規涉及違法行為態樣
- 評估該等行為以網路、網域作為媒介上發生之可能性

是否涉及違法行為網路（網域）化
- 檢視實務運作上是否有相關案例發生
- 探討目前處置方式有無修正、另立子法及修法之必要

修法方向
- 修法明文應為限制我國網路使用者接取、瀏覽之措施，或先行移除等態樣
- 對於無法查明違法行為人（如使用境外網域）之送達，得以公告方式為之。

48

第六章 就網域濫用之態樣，研擬管制性規

就網域濫用之態樣，研擬管制性規(4)
網域名稱技術濫用領域

	現行	增訂規定
主管機關	檢、警單位之刑事調查	行政院資通安全處 參酌網域名稱技術濫用犯罪之目的係以獲取網路使用者之個人資料，爰於「資通安全管理法」增訂如下規定。
實體規定	刑法妨礙電腦使用罪章	於「資通安全管理法」增訂： 「平臺提供者、應用服務提供者或電信事業，經目的事業主管機關告知資通系統及資通服務有遭反資通安全政策或保護措施失效之狀態發生，**影響資通系統機能運作，構成資通安全政策之威脅，應為限制我國網路使用者接取、瀏覽之措施，或先行移除**。」
程序規定	刑事訴訟程序	行政院所為行政處分應符合行政程序法，惟考量違法病毒網站所有人不明之情況下，於「資通安全管理法」**增訂「對於無法查明違反資通安全政策之行為人之送達，得以公告方式為之。」**
跨境暨解決方式	檢、警單位係於接獲通報後方開始進行偵辦，多已有實害發生。 犯罪人不明，無法以照刑事扣押處分避免第三人受害。	1.由行政機關作成行政處分，針對情況急迫程度，及是否屬於境外網域，考量使用DNS RPZ技術停止解析該違法網站，以解決網域技術濫用問題。 2.基於病毒散播之快速及量大，非由行政機關所能一一作成處分。故得立法授權註冊管理機構、受理註冊機構或ISP等業者自行處置，並報主管機關備查。
違憲風險	**無**違憲風險，本團隊建議訂定，理由如下： • 網域名稱技術濫用不涉「言論自由」之表達 • 確保安全之網路使用環境之公益性極高	

第六章 就網域濫用之態樣，研擬管制性規

就網域濫用之態樣，研擬管制性規(5)
刑事規定之犯罪行為（著作、商標）

	現行	增訂規定
主管機關	檢、警單位之刑事調查	經濟部智慧財產局 參酌美國「Operation in Our Sites」，就違反商標、著作權之違法網站，迅速以民事程序下架。
實體規定	著作權法、商標法之刑事罰則	於「著作權法」增訂： 「平臺提供者、應用服務提供者或電信事業，經著作權人或目的事業主管機關通知其使用者涉有侵權行為後，應立即為限制我國網路使用者接取、瀏覽之措施，先行移除或使他人無法進入該涉有侵權之內容或相關資訊。」 於「商標法」增訂： 「平臺提供者、應用服務提供者或電信事業，經商標權人或目的事業主管機關通知其使用者涉有侵權行為後，應立即為限制我國網路使用者接取、瀏覽之措施，先行移除或使他人無法進入該涉有侵權之內容或相關資訊。」
程序規定	刑事訴訟程序	行政院所為行政處分應符合行政程序法，惟考量違法網站所有人不明之情況下，於「著作權法」、「商標法」增訂「對於侵害著作權／商標權之行為人之送達，得以公告方式為之。」
跨境暨解決方式	同前	1.目前我國著作權法第90條之4以下訂有網路服務提供者之避風港條款，故業者多願意配合將違反著作權之內容刪除。惟對於境外網域難以要求配合刪除違法內容等情事發生時，有使用DNS RPZ停止解析之需求。 2.另外對於商標法並無如同著作權法有避風港等相關規範，為避免侵害商標權內容持續呈現於網路上，有使用DNS RPZ停止解析之需求。 3.透過立法修訂行政機關為行政處分，得及時以DNS RPZ技術封鎖該違法網站，解決現行無法規允許TWNIC將特定違法內容網站以DNS RPZ遮蔽之行為。
違憲風險	違憲風險**無**，本團隊建議訂定，理由如下： • 違反刑事法規，縱涉及「保障之言論」，亦為低價值言論 • 我國已有違反著作權法而扣押「特定網站」之案例 • 參酌美國法「Operation in Our Sites」，有類似規定	

第六章 就網域濫用之態樣，研擬管制性規

就網域濫用之態樣，研擬管制性規(6)
刑事規定之犯罪行為（賭博、猥褻內容）

	現行	增訂規定
主管機關	檢、警單位之刑事調查	衛生福利部
實體規定	刑法賭博罪章	現行得依照「兒童及少年福利與權益保障法」第46條第3項之規定停止該網域名稱之解析。故毋庸增訂實體規範。
程序規定	刑事訴訟程序	所為行政處分應符合行政程序法，惟考量違法網站所有人不明之情況下，於「兒童及少年福利與權益保障」增訂「對於無法查明散布有害兒童及少年身心健康行為人之送達，得以公告方式為之。」
跨境暨解決方式	同前	由行政機關為行政處分，得及時以DNS RPZ技術封鎖該違法網站，得解決現行無法規允許TWNIC將特定違法內容網站以DNS RPZ遮蔽之行為。
違憲風險	違憲風險**低**，本團隊建議訂定，理由如下： • 違反刑事法規，縱涉及「保障之言論」，亦為低價值言論 • 我國已有違反著作權法而扣押「特定網站」之案例 • 針對「兒童色情內容」，日本亦以遮蔽網域名稱之方式進行處理。	

目錄

第七章 結論與建議

（四）結論

網域技術濫用

- 「網域名稱濫用框架」指出註管機構知悉網域名稱技術濫用時，註管機構必須有所作為
- 註管機構具體作為義務及處置手段於我國法多未有明文。
- 建議針對網域技術濫用應有法律授權，使主管機關及註管機構得快速下架或停止解析技術濫用網域

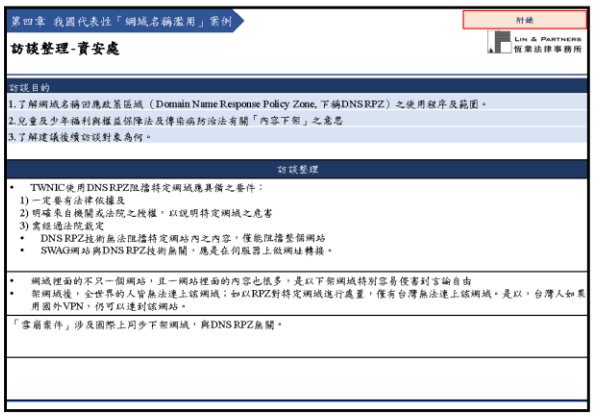
網域內容濫用

- 就網域內容濫用，並無由註管機關自行認定是否內容違法之前例。建議由由司法或專業機構負責認定
- 涉及侵害兒少身心之申訴及處理由民間第三方機構IWIN負責，但其他領域，尚無機構負責。
- 可考慮擴大IWIN處理範圍，或另設專責民間第三方機構以處理其他網域濫用問題。
- 我國法規僅有兒童及少年福利與權益保障法及動物傳染病防治條例，授權該管行政機關將違法之網站內容為限制接取、瀏覽及移除。建議其他法律也應增設類似規範，以符合法律授權。

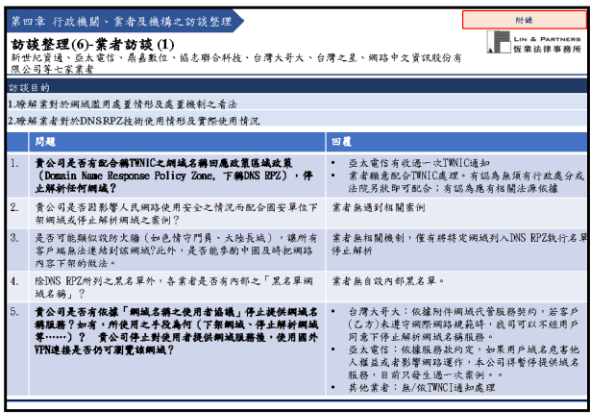
Q&A

55

58

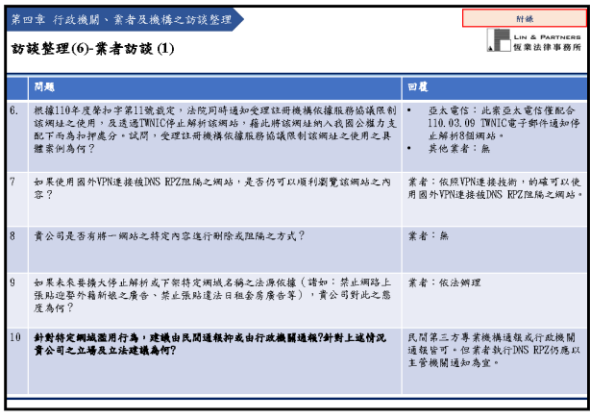


56



59

57



60

第四章 行政機關、業者及機構之訪談整理

附錄

LIN & PARTNERS 恆業法律事務所

10月22日座談會整理(1)

座談會目的

為聽取業者、第三方機構以及專家學者對本研究案之建議，辦理本次座談會，以期能了解業者實務上面對之問題，以及專家學者意見，互相交流以激盪出不同想法。

與會機構與業者	與會專家學者
iWIN網路內容防護機構、	詹婷怡律師
中華電信	何吉森教授
台灣大哥大	程法彰教授
亞太電信	葉志良教授
新世紀資通	顏振豪副所長
網路中文	

61

第四章 行政機關、業者及機構之訪談整理

附錄

LIN & PARTNERS 恆業法律事務所

10月22日座談會整理(2)

	問題討論	業者/專家學者
一	是否各領域主管機關要求刪除網域內容或是停止解析時，於相關法規內應明文「限制我國網路使用者接取、瀏覽之措施或移除網頁內容」，以符合法律保留原則？	是，主管機關要求刪除網域內容或是停止解析須符合法律保留
二	是否各領域主管機關要求刪除技術濫用或是停止解析時須有相關法律，以符合法律保留原則？	1. RPZ為限制網路接取的技術手段，原始目的為域名系統服務提供的功能之一，以維持網路基礎設施運作。 2. ICANN係以 DNS Abuse Framework，作為技術之自律規範
三	是否註管機構(TWNIC)知悉或收受通知面對網域濫用時，應自行認定是否違法？	建議由第三方機構協助認定是否構成網域濫用
四	以「停止解析」做為「網域名稱濫用」之處置手段應符合比例原則？	DNS RPZ停止解析應作為網域濫用處立之最後手段
五	是否網域內容濫用由第三方機構判斷網際網路內容是否存在違法或不當再將相關資訊彙整通報給各主管行政機關、檢警單位及ISP業者？	建議可由第三方機構協助進行初步判斷網域是否構成違法濫用
六	是否針對停止解析等處分無法查明或難以送達網域註冊人時，以「公告代替送達？	座談會中無針對此進一步討論
七	各業者於收到TWNIC停止解析特定網域之指示後，是否有執行上之困難？	多數業者因境為審查案件標準無統定奪，且情資來源不統一，或有情資品質不可靠之問題。

62

第四章 行政機關、業者及機構之訪談整理

附錄

LIN & PARTNERS 恆業法律事務所

座談會問題與討論(1)

	問題	目前國際趨勢及我國作法	本研究分析/建議
1	是否各領域主管機關要求刪除網域內容或是停止解析時，於相關法規內應明文「限制我國網路使用者接取、瀏覽之措施或移除網頁內容」，以符合法律保留原則？	• 現行我國法有移除網頁內容之相關規範，僅有兒童及少年福利與權益保障法第46條第3項及動物傳染病防治條例第38-3條 • TWNIC針對網域內容濫用執行DNS RPZ停止解析網域需有法院判決/裁定或行政機關處分 • TWNIC針對網域名稱係有資安疑慮且影響資安重大者可執行DNS RPZ停止解析網域	• 建議事業主管機關於管轄法規內明文「限制我國網路使用者接取、瀏覽之措施或移除網頁內容」。 • 相關立法方向可參見第五章。
2.	是否註管機構(TWNIC)知悉或收受通知面對網域濫用時，應自行認定是否違法？	• TWNIC未針對網域濫用是否違法進行認定 • ICANN與TWNIC間之註冊管理機構協議並無賦予TWNIC管制網域名稱內容濫用之權利及義務 • 目前各註管機構並無負責認定內容濫用之前例 • 網域名稱濫用框架已針對網域濫用定義五種類型包含：一、惡意軟體；二、殭屍網路；三、網路釣魚；四、偽冒螺接；五、以垃圾郵件之形式達成以上濫用之行為 ，網域名稱濫用報架明確指出，當註管機構知悉有前述之網域名稱濫用情形時，註管機構必須有所作為，然而作為義務及處置手段於我國法多未有明文 • 依法院判決/裁定或是行政機關行政處分，執行DNS RPZ，停止解析濫用網域	• 不應賦予TWNIC自行判斷網域濫用之權利及義務，如有須應限於技術濫用， • 於TWNIC知悉或合理懷疑網域名稱內容涉及不法情形時，應賦予其通報義務 • 於相關機構調查過程，可考慮賦予TWNIC配合調查或資訊提供之協力義務(諸如：提供網域申請人之個人資料) • 於法有明文下，收受行政機關或專業第三方判定濫用時應配合執行DNS RPZ停止解析網域，及配合調查提供相關資訊 • 為明確上開事項，可考慮透過修改電信管理法第71條及相關子法或簽訂政策約之方式為之

63

第四章 行政機關、業者及機構之訪談整理

附錄

LIN & PARTNERS 恆業法律事務所

座談會問題與討論(2)

	問題	目前國際趨勢及我國作法	本研究分析/建議
3.	以「停止解析」做為「網域名稱濫用」之處置手段應符合比例原則？	• 各國均有將「停止解析」作為處置手段，舉例而言，馬來西亞對於外國網域名稱之封鎖均採此技術。日本對於「兒童色情」之內容有採用「停止解析」技術進行處理。 • 惟自「比例原則」以觀，另創作人或業者就特定內容自行下架，最能符合「最小侵害」原則。	• 執行DNS RPZ停止解析網域雖以維準移除該網域名稱之濫用部份下(例如網路討論區、網路市集等情形)，可能必須移除整個網站，使非屬違法部分之內容也遭移除 「停止解析」應為最後手段，需確認該網域名稱無法透過其他方式處置(例如先行通知)時方採用之。
4.	是否網域內容濫用由第三方機構判斷網際網路內容是否存在違法或不當，再將相關資訊彙整通報給各主管行政機關、檢警單位及ISP業者？	• 目前我國有關網路內容涉及侵害兒少身心之申訴及處理，係由iWIN網路內容防護機構負責，其處理範圍涵蓋色情、暴力、恐怖、血腥、有害物品及其他有害兒少身心健康內容等六大類 • 日本第三方民間機構SIA依相關法規之違法要件及態樣訂立「安全維運用指引」，負責接受及審查網路使用者通報網域名稱內容違法及不當	• 可考慮進一步擴張iWIN之業務範圍及權能，或另外新設第三方專業機構收受網路使用人申報及審查停止病治、婚姻媒合、日組委等網域內容違法不當問題。

64

第四章 行政機關、業者及機構之訪談整理

附錄

LIN & PARTNERS 恆業法律事務所

座談會問題與討論(3)

	問題	目前國際趨勢及我國作法	本研究分析/建議
5.	是否針對停止解析等處分無法查明或難以送達網域註冊人時，以「公告」代替送達？	• 行政程序法第100條以書面送達對人為原則 • 動物傳染病防治條例第38條之3第3款明文「網際網路內容涉及境外應施檢疫物之販賣至國內輸入或其他檢疫相關事項，**經輸出入動物檢疫機關公告者，其廣告刊登者、平臺提供者、應用服務提供者或電信事業，應依輸出入動物檢疫機關之公告，限制接取、瀏覽或移除相關網頁內容。**」	• 通傳會可參來註管機關及受理註冊機構在與網域名稱註冊人之同意書上，同意以受理註冊機構作為送達代收人，一經送達即生效力。 • 可透過立法於相關法規增修「無法查明行為人之送達，得以公告方式為之。」以解決此問題。
6.	各業者於收到TWNIC停止解析特定網域之指示後，是否有執行上之困難？	• 目前各業者收到TWNIC通知停止解析網域後，多可配合處理。	• 依研究團隊收到業者書面問卷之回覆，業者可配合處理。

65

第五章 就網域濫用之態樣，研擬管制性規

附錄

LIN & PARTNERS 恆業法律事務所

就網域濫用之態樣，研擬管制性規範—行政執行

1. 依行政執行法第28條「直接強制」、行政執行法第36條「即時強制」進行「網域名稱之停止解析」
2. 適用案例：積微機關對觸犯加值型及非加值型營業稅法第52條規定之電商業者處以停止營業處分一事，為停止營業處分後，是否得以「網域名稱之停止解析」做為執行手段？
3. 此涉兩種立法模式思考

法規明文，應為「限置接取、下架網域」之處分	於法規明文禁止特定行為（諸如：停止營業等）
直接依法為限置接取之行政處分	為落實行為人之行為不行為義務，以強制方法執行之
檢討該法規是否違憲	檢討執行行為是否符合行政程序法之規定（諸如：有無不當聯結、比例原則等）
違憲審查會議審酌	法院審酌

4. 不建議採取行政執行之立法模式。

66

第五章 就網域濫用之態樣，研擬管制性規 附錄

就網域濫用之態樣，研擬管制性規—
不涉及刑事犯罪（動物傳染病防治）

	現行	增訂規定
主管機關	衛生福利部	行政院農業委員會
實體規定	行政管制法規	得依照「動物傳染病防治條例」第38-3條第3項之規定停止該網域名稱之解析
程序規定	行政程序法	所為行政處分應符合行政程序法，惟考量違法網站所有人不明之情況下，於「動物傳染病防治條例」增訂「對於無法查明發布境外應施檢疫物之販賣至國內行為人之送達，得以公告方式為之。」
困境暨解決方式	同前	由行政機關為行政處分，得及時以DNS RPZ技術封鎖該違法網站，得解決現行無法規允許TWNIC將特定違法內容網站以DNS RPZ遮蔽之行為。
違憲風險	違憲風險**低**，本團隊建議訂定，理由如下： • 縱無涉及刑事法規，商業性言論亦屬低價值言論 • 保障國民之健康，公益性極高	

67

第五章 就網域濫用之態樣，研擬管制性規 附錄

就網域濫用之態樣，研擬管制性規—
不涉及刑事犯罪（婚姻媒合）

	現行	增訂規定
主管機關	內政部移民署	內政部移民署
實體規定	入出國及移民法第58條	於「入出國及移民法」增訂： 「網際網路平台提供者，經目的事業主管機關通知其使用者涉有廣告物、出版品、廣播、電視、電子訊號、電腦網路或以其他使公眾得知之方法，散布、播送或刊登跨國（境）婚姻媒合廣告，應立即為限制我國網路使用者接取、瀏覽之措施、先行移除或使他人無法進入該涉有侵權之內容或相關資訊。」
程序規定	行政程序法	所為行政處分應符合行政程序法，惟考量違法網站所有人婚姻媒合廣告行為人之送達，得以公告方式為之。」
困境暨解決方式	同前	由行政機關為行政處分，得及時以DNS RPZ技術封鎖該違法網站，得解決現行無法規允許TWNIC將特定違法內容網站以DNS RPZ遮蔽之行為。
違憲風險	違憲風險**中**，本團隊建議訂定，理由如下： ▪ 縱無涉及商業性法規，商業性言論亦屬低價值言論 ▪ 婚姻不得計價原則及善良風俗之確保，惟公益性較低 ▪ 容易違反比例原則，DNS RPZ技術無法單純遮蔽違法廣告 ▪ 律師倫理法開放以廣告推廣業務	

68

第五章 就網域濫用之態樣，研擬管制性規 附錄

就網域濫用之態樣，研擬管制性規—
不涉及刑事犯罪（日租套房違反廣告）

	現行	增訂規定
主管機關	交通部觀光局	交通部觀光局
實體規定	發展觀光條例第55條第4項	於「發展觀光條例」增訂： 「網際網路平台提供者，經目的事業主管機關通知其使用者涉有未依本條例領取營業執照而經營觀光旅館業務、旅行業務或觀光遊樂業務者或領取登記證而架設網站或刊登廣告，應立即為限制我國網路使用者接取、瀏覽之措施、先行移除或使他人無法進入該涉有侵權之內容或相關資訊。」
程序規定	行政程序法	所為行政處分應符合行政程序法，惟考量違法網站所有人非法日租套房廣告行為人之送達，得以公告方式為之。」
困境暨解決方式	處分送達問題	由行政機關為行政處分，得及時以DNS RPZ技術封鎖該違法網站，得解決現行無法規允許TWNIC將特定違法內容網站以DNS RPZ遮蔽之行為。
違憲風險	違憲風險**略高**，本團隊建議訂定，理由如下： ▪ 縱無涉及商業性法規，商業性言論亦屬低價值言論 ▪ 確保旅客安全之公益性高 ▪ 容易違反比例原則，DNS RPZ技術無法單純遮蔽違法廣告	

69

第五章 就網域濫用之態樣，研擬管制性規 附錄

就網域濫用之態樣，研擬管制性規—
假消息

	現行	增訂規定
主管機關	檢、警單位之刑事調查	行政院內政部
實體規定	詐欺罪、妨害信用罪、妨害工商交易罪、意圖使候選人當選或不當選罪、違反商業競爭秩序罪、散布疫情假訊息罪、社會秩序維護法	刑事法中不適合加入行政手段，爰將遮蔽謠言網站之規定於「社會秩序維護法」，增訂內容如下： 「網際網路平台提供者，經目的事業主管機關通知其使用者涉有散佈謠言之行為後，應立即為限制我國網路使用者接取、瀏覽之措施、先行移除或使他人無法進入該涉有侵權之內容或相關資訊。」
程序規定	刑事訴訟程序、行政裁罰	行政院所為行政處分應符合行政程序法，惟考量違法網站所有人不明之情況下，於「社會秩序維護法」增訂「對於散布不實謠言之行為人之送達，得以公告方式為之。」
困境暨解決方式	對不實言論為即時處理，屬行政處分之範疇，宜於行政法規中訂定之	由行政機關為行政處分，得及時以DNS RPZ技術封鎖該違法網站，得解決現行無法規允許TWNIC將特定違法內容網站以DNS RPZ遮蔽之行為。
違憲風險	違憲風險**高**，本團隊不建議訂定，理由如下： ▪ 「散布不實言論」之定義過於模糊，違反法明確性原則 ▪ 縱違反刑事法規，按照近期言論，被認定為假消息多屬「高價值」之「政治性」言論 ▪ 不實言論多為刑事法規，不適宜放入「即時停止解析」之規定 ▪ 此規定方式勢必會面臨「過度侵害言論自由」之評價 ▪ 僅有馬來西亞有相關規範	

70

附錄五　中英對照表

（英國） 接取限制令	access restriction order
反網路侵佔消費者保護法	Anti-Cybersquatting Consumer Protection Act
亞洲域名爭議解決中心	Asian Domain Name Dispute Resolution Centre
商標淡化	Blurring and dilution by tarnishment
殭屍網路	Botnets
馬來西亞 1988 年廣電法	Broadcasting Act 1988
兒少性虐待之素材	Child Sexual Abuse Material
兒童網路保護法	Children's Internet Protection Act
兒童線上隱私保護法	Children's Online Privacy Protection Act
清晰可信	clear and convincing evidence
美國通訊端正法	Communication Decency Act
通訊傳播暨多媒體法	Communications and Multimedia Act 1988
馬來西亞 1988 年通訊傳播暨多媒體法	Communications and Multimedia Act 1998
電腦詐欺及濫用法案	Computer Fraud and Abuse Act
馬來西亞 MCMC 消費申訴局	Consumer Complaints Bureau
一造缺席判決	Default Judgement
英國數位經濟法案	Digital Economy Bill
數位千禧年著作權法	Digital Millennium Copyright Act
網域名稱濫用框架	DNS Abuse Framework
網域明曾受理註冊機構	Domain Name Registrar
網域明曾受理註冊機構	Domain Name Registrar
網域名稱註冊管理機構.	Domain Name Registry
網域名稱註冊管理機構.	Domain Name Registry
網域名稱系統解析器	Domain Name Resolver
網域名稱濫用框架	Domain Name System Abuse Framework
網域名稱回應政策區域	Domain Name System Response Policy Zone
網域名稱系統伺服器	Domain Name System Server
域名稱系統沉洞伺服器	Domain Name System Sinkhole
電子前哨基金會	Electronic Frontier Foundation
消除對互動科技的濫用和肆意忽視法案	Eliminating Abusive and Rampant Neglect of Interactive Technologies Act
緊急臨時禁制令	Emergency Temporary Restraining Order
歐洲反恐中心	European Counter Terrorism Centre
歐洲反恐中心	European Counter Terrorism Centre-ECTC
歐洲網路犯罪中心	European Cybercrime Centre
歐洲網路犯罪中心	European CybercrimeCentre-EC3

歐洲人口販運防治中心	European Migrant Smuggling Centre
歐洲人口販運防治中心	European Migrant Smuggling Centre-EMSC
單方程序聽證	Ex Parte proceeding hearings
「防止網際網路審查」行政命令	Executive Order on Preventing Online Censorship
快速政策制定程序	Expedited Policy Development Procedure
金融資安資訊分享與分析中心	Financial Services Information Sharing and Analysis Center
一般資料保護規則	General Data Protection Regulation, GDPR
ICANN 政府諮詢委員會	Government Advisory Committee
網域名稱扣押指引	Guidance for Preparing Domain Name Orders, Seizures & Takedowns
國土安全調查局	Homeland Security Investigations
伺服器服務提供者	Hosting provider
伺服器服務提供者	Hosting provider
人口販售	Human trafficking
網路違法販售鴉片	Illegal distribution of opioids online
民事對物扣押	In rem action
民事對物扣押	In rem action
對物扣押之手段	In rem civil action
網路內容防護機構	Institute of Watch Internet Network
智慧財產犯罪協調辦公室	Intellectual Property Crime Coordinated Coalition
智慧財產犯罪協調辦公室	Intellectual Property Crime Coordinated Coalition-IPC3
網路內容安全協會	Internet Content Safety Association
日本網路熱線中心	Internet Hotline Center
網際網路服務供應商	Internet Service Provider
網路觀察基金會	Internet Watch Foundation
網際網路名稱與數字位址分配機構	Internet Corporation for Assigned Names and Numbers
日本網路供應商協會	JAIPA Japan Internet Providers Association
日本網路資訊中心	Japan Network Information Center
日本網域名稱註冊管理機構	Japan Registry Services Co., Ltd
日本有線電視協會	JCTA Japan Cable and Telecommunications Association
馬來西亞通訊傳播暨多媒體委員會	Malaysian Communications and Multimedia

	Commission
馬來西亞通訊傳播暨多媒體委員會	Malaysian Communications and Multimedia Commission
馬來西亞通訊傳播暨多媒體委員會法	Malaysian Communications and Multimedia Commission Act 1998
惡意軟體	Malware
馬尼拉中介者責任原則	Manila Principles on Intermediary Liability
馬來西亞通訊傳播暨多媒體部	Ministry of Communications and Multimedia Malaysia
美國國家仲裁協會	National Arbitration Forum
通訊傳播委員會	National Communications Commission
英國國家通訊管理局	Office of Communications
英國網路安全法案	Online Safety Bill
經濟合作暨發展組織	Organization for Economic Cooperation and Development
經濟合作暨發展組織	Organization for Economic Cooperation and Development
偽冒嫁接	Pharming
網路釣魚	Phishing
平臺問責與消費者透明度法案	Platform Accountability and Consumer Transparency Act
預防禁制令	Preliminary Injunction
證據優勢	preponderance of the evidence
反勒索及受賄組織法	Racketeer Influenced and Corrupt Organizations Act
註冊人	Registrant
網域名稱受理註冊機構認可協議	Registrar Accreditation Agreement
註冊管理機構協議	Registry Agreements
註冊管理機構-受理註冊機構協議	Registry-Registrar Agreement
一般社團法人安全網路協會	Safer Internet Association
（英國） 服務限制令	service restriction order
網站管理者	Site Operator
以垃圾郵件之形式達成以上濫用之行為	Spam
揭露/存取非公開註冊資料的標準化系統	System for Standardized Access/Disclosure to Non-Public Registration Data
揭露/存取非公開註冊資料的標準化系	System for Standardized Access/Disclosure to

統	Non-Public Registration Data
財團法人台灣網路資訊中心	Taiwan Network Information Center
（英國） 技術警告通知	technology warning notice
日本電信服務協會	Telecom Services Association
馬來西亞 1950 年電信法	Telecommunications Act 1950
反垃圾郵件法案	The Controlling the Assault of Non-Solicited Pornography And Marketing Act of 2003
電子通信隱私法	The Electronic Communications Privacy Act
聯邦商標法	The Lanham Act
英國兒童保護法	The Protection of Children Act 1978
綜合犯罪防制及街坊安全法第三篇	Title III of the Omnibus Crime Control and Safe Streets Act
入侵他人動產	Trespass to chattels
受信任之通知者	Trusted Notifiers
美國移民及海關執法局	U.S. Immigration and Customs Enforcement's
統一域名爭議解決政策	Uniform Domain Name Dispute Resolution Policy
統一快速暫停系統	Uniform Rapid Suspension System
美國國土安全部	United States Department of Homeland Security
不當得利	Unjust Enrichment
馬利蘭州聯邦檢察署	US District Attorney for the District of Maryland
網路使用者產生之內容	User Generated Content
網路使用者產生之內容	User Generated Content
世界智慧財產權組織	World Intellectual Property Organization

參考書目

一、中文參考文獻

（一）期刊文獻

1. 陳昱奉，數位時代之犯罪偵查與網路自由及隱私權之保障—從網域名稱（Domain Name）之扣押、沒收談起，臺灣嘉義地方法院檢察署 102 年度自行研究報告，2014 年。
2. 陳起行，由 Reno v. ACLU 一案論法院予網際網路之規範，歐美研究第 33 卷第 3 期，，2003 年。
3. 鄭文中，淺論歐盟刑事司法合作之歷史發展，台灣國際研究季刊第 14 卷第 3 期，2018 年 9 月。

（二）學位論文

1. 洪爾謙，著作權法下管制侵權內容之法律研究—以封鎖境外網站為中心，國立清華大學科技法律研究所，2014 年。

（三）其他文獻與資料

1. 2017 年電子前哨基金會關於網域名稱註冊之白皮書，頁 7，https://www.eff.org/files/2017/08/02/domain_registry_whitepaper.pdf。
2. DNS RPZ 官方網站，https://dnsrpz.info/。
3. E 安全，全球最大殭屍網絡基礎設施平臺—雪崩 Avalanche 已造成億萬美金損失，https://www.gushiciku.cn/dc_hk/108488677
4. Godaddy，.live 網域名稱，https://tw.godaddy.com/tlds/live-domain
5. ICANN 官方網站，https://www.icann.org/news/blog/icann-doesn-t-take-down-websites

6. ICANN，gTLD 註冊數據臨時規範快速政策制定流程第 2 階段的最終報告。
7. iThome, DNS 危機解密，https://www.ithome.com.tw/guest-post/106780
8. iWIN 目標，iWIN 官方網站，https://i.win.org.tw/about.php#stop6
9. T.H. Schee，台灣國安單位封鎖 31t.tw 一案，https://blog.schee.info/2019/03/16/%E5%8F%B0%E7%81%A3%E5%9C%8B%E5%AE%89%E5%96%AE%E4%BD%8D%E5%B0%81%E9%8E%96-31t-tw-%E4%B8%80%E6%A1%88/
10. TWNIC 官方網站，https://blog.twnic.tw/2020/09/23/15311/。
11. TWNIC，EPDP 發布第二階段結案報告，https://blog.twnic.tw/2020/09/05/14860/
12. TWNIC，ICANN 的難題：WHOIS 與 GDPR （下集），https://blog.twnic.tw/2019/05/14/3718/
13. TWNIC，SSAD 實施評估流程問卷，展開實施評估流程，https://blog.twnic.tw/2021/08/09/19305/
14. TWNIC，回應政策區域（Response Policy Zone, RPZ），https://blog.twnic.tw/2020/07/02/14020/
15. T 客邦，楓林網被關為什麼 Google 還有「楓林網」存在？而且你依然拿他們沒辦法，https://udn.com/news/story/7088/4477602
16. Vincent Chen，台灣網民 WHOIS 查詢受 GDPR 之可能影響， https://medium.com/vincent-chen/%E5%8F%B0%E7%81%A3%E7%B6%B2%E6%B0%91whois%E6%9F%A5%E8%A9%A2%E5%8F%97gdpr%E4%B9%

8B%E5%8F%AF%E8%83%BD%E5%BD%B1%E9%9F%BF-281624733003。

17. Webnode 網域名稱規範，https://www.webnode.tw/domain-names-policies/
18. WHOIS 隱私服務，https://www.net-chinese.com.tw/nc/index.php/MenuLink/Index/WHOISPrivacy
19. Yahoo，我該如何識別網路釣魚網站或電子信件？，https://safety.yahoo.com/TW/Security/IDENTIFY-A-PHISHING-WEBSITE-TW.html 。
20. 公務出國報告，出席馬來西亞通訊傳播暨多媒體委員會雙邊交流會議及參訪相關機構，國家通訊傳播委員會，2015 年。
21. 王琇慧，2005 年，「千禧著作權法（DMCA）施行之新平臺-自由貿易協定（FTA）」，第 92 頁，https://www.tipo.gov.tw/tw/dl-4488-bdb94726bc00408e95fc8604e0e10717.html
22. 台灣網民 WHOIS 查詢受 GDPR 之可能影響，https://medium.com/vincent-chen/%E5%8F%B0%E7%81%A3%E7%B6%B2%E6%B0%91whois%E6%9F%A5%E8%A9%A2%E5%8F%97gdpr%E4%B9%8B%E5%8F%AF%E8%83%BD%E5%BD%B1%E9%9F%BF-281624733003
23. 安博盒子看東京奧運爆爭議，非法機上盒看直播免罰、製造販售 3 行為將遭殃，數位時代，https://www.bnext.com.tw/article/64244/ncc-stb-unblocktech。
24. 自由時報，我調查局與 31 國聯手偵破「雪崩」網路犯罪集團 https://news.ltn.com.tw/news/society/breakingnews/1904635

25. 吳睿騏，楓林網盜版侵權 檢方起訴 2 犯嫌查扣財產 6700 萬，https://www.cna.com.tw/news/firstnews/202011090258.aspx
26. 英國政府通過數位經濟法案，色情網站須強制驗證造訪者年齡、嚴禁機器人搶票，https://www.ithome.com.tw/news/115639
27. 財團法人台灣網路資訊中心（編），各國頂級國碼網域名稱管理機制研究計畫，收於：財團法人台灣網路資訊中心委託研究報告，頁 23-24（2013 年）；JPRS 沿革，https://jprs.co.jp/company/history.html
28. 馬尼拉原則官方網站，https://www.manilaprinciples.org/principles。
29. 探討 TWNIC 對網域名稱使用涉有違反相關法律之虞時可採行之緊急處置措施，財團法人台灣網路資訊中心委託研究案，2006 年。
30. 探討 TWNIC 對網域名稱使用涉有違反相關法律之虞時可採行之緊急處置措施，財團法人台灣網路資訊中心委託研究案，2006 年。
31. 章忠信，機上盒侵害著作權之法律防制，著作權筆記，http://www.copyrightnote.org/ArticleContent.aspx?ID=54&aid=2889。
32. 莊伯仲，三招解決盜版的安博盒子，https://tw.sports.yahoo.com/news/%E8%8E%8A%E4%BC%AF%E4%BB%B2-%E4%B8%89%E6%8B%9B%E8%A7%A3%E6%B1%BA%E7%9B%9C%E7%89%88%E7%9A%84%E5%AE%89%E5%8D%9A%E7%9B%92%E5%AD%90-

033000491.html?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAAE_0ceb_oNEvNAquXnRFleiZ1lz5yBKU-bboOStCJKgPBlHta_oATMGhn0d5WVwo9NoUGj99JwdPAIYB7PXERCD3e3vHYjtgR5jWuERr5UBZDqWyptUP_DNOnQgBCUc0lwg4WPo_B_sO8TZfEk25Wvxfm9WuF63p189NSI_HYXyG。

33. 莊伯仲，解決安博盒子問題的幾點芻議，獨家報導，https://www.scooptw.com/thinktank/media/61898/%E8%A7%A3%E6%B1%BA%E5%AE%89%E5%8D%9A%E7%9B%92%E5%AD%90%E5%95%8F%E9%A1%8C%E7%9A%84%E5%B9%BE%E9%BB%9E%E8%8A%BB%E8%AD%B0/。

34. 陳念祖，法務部調查局與美國、歐洲刑警組織共同偵破「雪崩」殭屍網路案， http://tbnews.com.tw/society/20161202-12225.html

35. 陳彥君，新通用頂級域名爭議解決新機制，http://www.winklerpartners.com/?p=4430&lang=zh-hant

36. 陳靜慧，2018 年 3 月 5 日「跨境電腦犯罪之司法管轄 與發展趨勢 ～以網路詐欺犯罪為中心」出國報告，https://report.nat.gov.tw/ReportFront/PageSystem/reportFileDownload/C10700108/001

37. 報導者，從 SWAG 被抄，看數位情色產業大躍進下的法律衝撞、直播主的勞動現場，https://www.twreporter.org/a/taiwan-erotic-industry-swag-sex-work

38. 黃勝雄，DNS RPZ 摘要說明，https://blog.twnic.tw/2020/09/23/15311/

39. 黃瀞儀，楓林網起死回生？網驚曝：時下最夯劇都可以看，中時新聞網 https://www.chinatimes.com/realtimenews/20200813005426-260402?chdtv

40. 新頭殼 newtalk，「亞洲最大」成人平臺 SWAG 被抄 會員哀嚎擔憂「鑽石」會費要不回，https://newtalk.tw/news/view/2021-04-04/558670。

41. 楊擴舉，「網域名稱爭議與商標權保護基本問題之研究」，https://www.tipo.gov.tw/tw/cp-182-313838-f9a73-1.html

42. 經濟部智慧財產局委託研究案「英國著作權法令暨判決之研究」期末報告。

43. 資安趨勢部落格，日逾 8 萬台電腦感染網銀病毒,破解雙重認證,非法轉帳，https://blog.trendmicro.com.tw/?p=12034

44. 電子前哨基金會網頁，https://www.eff.org/press/releases/international-coalition-launches-manila-principles-protect-freedom-expression。

45. 團法人台灣網路資訊中心，新通用頂級域名（New gTLD）開放對我國域名管 理機制之影響與因應之研究，https://www.twnic.tw/file/1406rp.pdf

46. 網域名稱規範，Webnode，https://www.webnode.tw/domain-names-policies/

47. 網域名稱濫用框架官方網頁，2020 年回顧簡介 http://dnsabuseframework.org/dns-abuse-framework-2020-retrospective.html。

48. 網路中文，WHOIS 隱私服務，https://www.net-chinese.com.tw/nc/index.php/MenuLink/Index/WHOISPrivacy

。

49. 臺灣高等檢察署，安博盒子裡的著作權《就像偷水電！全民瘋奧運 機上盒侵權》，https://www.tph.moj.gov.tw/4421/4475/632364/889417/post

50. 遠見雜誌，盜版網站好難抓，楓林網「域名」成查扣把柄，科技新報 https://technews.tw/2020/04/25/domain-name-8maple/

51. 劉靜怡、雷憶瑜，國際網路組織介紹，https://www.twnic.tw/download/031014.pdf

52. 聯合新聞網，播台女露點片 色情網 SWAG 被抄，https://udn.com/news/story/7315/5362885

53. 謝佳興，用安博盒子看東奧違不違法？ 經濟部智慧財產局揭曉答案，中央廣播電台，https://www.rti.org.tw/news/view/id/2107266

54. 謝孟珊，網路媒體界群起抗議，美國總統歐巴馬表示反對，SOPA 法案遭到擱置，資策會科技法律研究所，2017 年 1 月，https://stli.iii.org.tw/article-detail.aspx?no=64&tp=1&d=5627。

55. 謝銘洋，新通用頂級域名（New gTLD）開放對我國域名管理機制之影響與因應之研究，財團法人台灣網路資訊中心，資料來源：https://www.twnic.tw/file/1406rp.pdf。

二、英文參考文獻

（一）期刊文獻

1. Hiller, Janine and Clara, S. Santa, *Civil Cyberconflict: Microsoft, Cybercrime, and Botnets*, 31 Santa Clara High Tech. L.J. 163, 10 HIGH TECHNOLOGY LAW JOURNAL, （2015）.
2. Kopel, Karen, *Operation Seizing Our Sites: How the Federal Government Is Taking Domain Names Without Prior Notice*, 26 BERKELEY TECHNOLOGY LAW JOURNAL, （2013）.

（二）其他文獻與資料

1. About us-History, MCMC, https://www.mcmc.gov.my/en/about-us/history
2. BYLAWS FOR INTERNET CORPORATION FOR ASSIGNED NAMES AND NUMBERS | A California Nonprofit Public-Benefit Corporation，ICANN official website, https://www.icann.org/resources/pages/governance/bylaws-en/#article1
3. Dan Katz, Bodog.com Domain Name Seized by U.S. Government, Poker News Daily （Feb. 28, 2012）, https://www.pokernewsdaily.com/bodog-com-domain-name-seized-by-u-s-government-21299/
4. David Kravets, *Uncle Sam: If It Ends in .Com, It's .Seizable*, Wired（ Mar. 6, 2012）, https://www.wired.com/2012/03/feds-seize-foreign-sites/.
5. Department of Justice, United States Seizes Domain Names Used by Foreign Terrorist Organization, https://www.justice.gov/opa/pr/united-states-seizes-domain-

names-used-foreign-terrorist-organization

6. DHS-ICE, HSI investigation results in seizure of 3 domain names purporting to be biotechnology company websites with COVID-19 treatments, https://www.ice.gov/news/releases/hsi-investigation-results-seizure-3-domain-names-purporting-be-biotechnology-company
7. DHS-ICE，Over a million websites seized in global operation, https://www.ice.gov/news/releases/over-million-websites-seized-global-operation
8. DNS Response Policy Zones, https://dnsrpz.info/.
9. Freedom House, https://freedomhouse.org/country/malaysia/freedom-net/2019
10. Julia Dickson, *U.S. Seizes Websites Tied to Iran*, United States Institute of Peace （Jul. 7, 2021）, https://iranprimer.usip.org/blog/2021/jul/07/us-seizes-websites-tied-iran
11. Kaplan, Jason S., The Anticybersquatting Consumer Protection Act: Will it End the Reign of the Cybersquatter?, https://escholarship.org/uc/item/8gm0v417
12. Kathleen A. Ruane, “How Broad A Shield? A Brief Overview of Section 230 of the Communications Decency Act”, https://fas.org/sgp/crs/misc/LSB10082.pdf
13. Legislation, MCMC, https://www.mcmc.gov.my/en/legal/acts
14. Luther, Blocking of Websites Which Contain Copyright Infringing Content in Various Asian Countries, https://www.luther-

lawfirm.com/fileadmin/user_upload/WP_Handout_Blocking-of-websites_Asian-countries_V01_270120.pdf

15. MAHAIZURA ABD MALIK, MCMC: Almost 3,000 pornographic sites blocked since Sept 2018, New Straits time, https://www.nst.com.my/news/crime-courts/2021/01/660369/mcmc-almost-3000-pornographic-sites-blocked-sept-2018

16. NACDL, Computer Fraud and Abuse Act （CFAA）, https://www.nacdl.org/Landing/ComputerFraudandAbuseAct.

17. Newsroom, *international law enforcement agencies seize 706 domain names selling counterfeit merchandise*, U.S. Immigration and Customs Enforcement （Dec. 12, 2017）, https://www.ice.gov/news/releases/ice-international-law-enforcement-agencies-seize-706-domain-names-selling-counterfeit

18. Nicole Kardell, Feds Open The Gates and Seize the Domain Names, https://www.ifrahlaw.com/crime-in-the-suites/feds-open-the-gates-and-seize-the-domain-names/

19. Ofcom, “Site Blocking” to reduce online copyright infringement; https://www.openrightsgroup.org/publications/copyright-and-web-blocking-in-the-uk/

20. Omar Santos, Using DNS RPZ to Block Malicious DNS Requests, https://blogs.cisco.com/security/using-dns-rpz-to-block-malicious-dns-requests

21. OONI, The State of Internet Censorship in Malaysia, https://ooni.org/post/malaysia-report/

22. Our Responsibility, MCMC,

https://www.mcmc.gov.my/en/about-us/our-responsibility

23. Paul Vixie, Taking Back the DNS, July 30, 2010, http://www.circleid.com/posts/20100728_taking_back_the_dns/

24. Pinsent Masons, https://www.pinsentmasons.com/out-law/news/website-blocking-provisions-to-be-removed-from-digital-economy-act-says-government-

25. PLATFORM ACCOUNT ABILITY AND CONSUMER TRANSPARENCY ACT, https://www.schatz.senate.gov/imo/media/doc/OLL20612.pdf

26. Regulation （EU） 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC （General Data Protection Regulation） （Text with EEA relevance）, OJ L 119, 4.5. （2016）.

27. Sarawak Report, https://www.sarawakreport.org/search/?q=1Malaysia+Development+Berhad+%281MDB%29&lang=en&page=4

28. SHAPING THE DIGITAL LANDSCAPE ANNUAL REPORT 2018, MCMC, https://www.mcmc.gov.my/skmmgovmy/media/General/pdf/MCMC-2018_ENG.pdf.

29. Sharon Tan, Zaid Ibrahim and Co., Communications: regulation and outsourcing in Malaysia: overview, https://content.next.westlaw.com/Document/Ib97922b5830011e598dc8b09b4f043e0/View/FullText.html?transitionType=Default&contextData=（sc.Default）

30. SinarProject, Laws cited for Internet Censorship in Malaysia, https://sinarproject.org/digital-rights/updates/laws-cited-for-internet-censorship-in-malaysia

31. Site Blocking Global Best Practices, Michael Schlesinger, https://www.ipaj.org/bunkakai/content_management/event/pdfs/20180728/Schlesinger_20180728_2.pdf

32. The Manila Principles on Intermediary Liability Background Paper.

33. Tim Cranton, Cracking Down on Botnets, OFFICIAL MICROSOFT BLOG, https://blogs.microsoft.com/blog/2010/02/24/cracking-down-on-botnets/

34. UPDATE: Section 230 and the Executive Order on Preventing Online Censorship, Congressional Research Service, https://crsreports.congress.gov/product/pdf/LSB/LSB10484

35. URL List, Internet Watch Foundation, https://www.iwf.org.uk/become-a-member/services-for-members/url-list

36. Zvelo, Using DNS RPZ to Protect Against Malicious Threats, https://zvelo.com/using-dns-rpz-to-protect-against-malicious-threats/

三、日文文獻

（一）書籍

1. Safer Internet Association，違法・有害情報対策活動報告（2019）。
2. ドメイン名に関する情報通信政策の在り方（平成 25 年 10 月 1 日付け諮問第 20 号）に関する情報通信審議会からの答申の公表，答申概要。
3. サイバーセキュリティ政策会議，平成 29 年度サイバーセキュリティ政策会議 報告書。
4. セーフライン運用ガイドライン第三章第一節及第四章第一節。
5. 違法・有害情報対策活動報告（2019 年 1 月~12 月）。

（二）其他文獻與資料

1. JP 汎用 JP ドメイン名登録等に関する規則。
2. JPRS，フィッシング被害防止においてドメイン名レジストリが担うべき活動の方針について，https://jprs.jp/advisory/program/080509.html。
3. JP ドメイン名諮問委員会事務局，不正行為に使われている JP ドメイン名へのレジストリとしての対応について，第 54 回 JP ドメイン名諮問委員会 参考資料 3，。
4. JP ドメイン名諮問委員会事務局，不正行為に使われている JP ドメイン名へのレジストリとしての対応について，第 54 回 JP ドメイン名諮問委員会 参考資料 3。フィッシング対策協議会，NEWS LETTER No. 9:ドメイン名レジストリから見たフィッシング対策，https://www.antiphishing.jp/news/interview/news_letter_no_9.html。
5. インターネットコンテンツセーフティ協会，アドレスリスト作

成業務について，http://www.netsafety.or.jp/blocking/index.html。

6. ドメインサービス約款，Sakura Internet，https://www.sakura.ad.jp/agreement/[a]yakkan7_domain.pdf。
7. 安心ネットづくり促進協議会，児童ポルノ対策の取り組みの経緯 2.国内における政府の動き，https://www.good-net.jp/blocking/prehistory/prehistory_2。
8. 株式会社日本レジストリサービスに対する「.jp」ドメイン名の管理・運用に係る措置（要請），總務省，https://www.soumu.go.jp/menu_news/s-news/01kiban04_02000152.html。
9. 基本約款，Sakura Internet，https://www.sakura.ad.jp/agreement/[a]yakkan0_kihon.pdf。
10. 第 56 回 JP ドメイン名諮問委員会資料及び議事録，正行為に使われている JP ドメイン名への JPRS におけるレジストリとしての対応の実装検討における留意点。
11. 第 56 回 JP ドメイン名諮問委員会資料及び議事録，不正行為に使われている JP ドメイン名へのレジストリとしての対応について 答申骨子。
12. 平成 29 年度サイバーセキュリティ政策会議（第３回）発言要旨。
13. 約款，Sakura Internet，https://www.sakura.ad.jp/agreement/?_ga=2.91935647.461501070.1610173974-34221045.1610173974&fbclid=IwAR2QkpkdOSBDY-rbsrIQzKrluKqT7V8BukXniEhhCyCUwBZS5BjPY00D7No。