張宏昌（2017），『ccTLDs 在 DNSSEC 建置發展及推動現況之比較』，
中華民國資訊管理學報，第二十四卷，第二期，頁 185-208。

ccTLDs 在 DNSSEC 建置發展及推動現況之比較

張宏昌*
樹人醫護管理專科學校資訊管理科

摘要

在這個資訊網路普及的時代，隨著人們對網際網路的依賴日漸增加，網路的安全性早已是不可忽視的問題。網路攻擊、犯罪手法層出不窮，其中又以「網路釣魚」最為常見，有鑑於此，許多國家紛紛引入具有「資料完整性」、「來源可驗證性」與「可驗證之不存在性」三大特性的 DNSSEC 來解決這樣的問題。雖然 DNSEEC 相較於傳統的 DNS 服務提供了我們更強大的安全性，可是其需要的較高的技術門檻以及缺乏對相關人士的升級部署誘因卻也讓 DNSSEC 在推廣上遇到了不少困難。

為了瞭解全球各頂級國碼域名在 DNSSEC 推動發展狀況，以作為台灣未來在部署、維運 DNSSEC 服務上之重要參考，本研究利用問卷和 E-Mail 的方式與各國相關人士進行訪談，並且同時以於網路上所蒐集的資料輔以佐證，最後再實際透過第三方的測試軟體對所得資訊進行全球不同區域主要頂級國碼域名在 DNSSEC 整體建置推動之驗證、比較與分析研究，希望能夠藉由這些寶貴的經驗與資訊實際瞭解並掌握目前各國在推動 DNSSEC 服務上的發展情形，包括組織編制、實作方法、成本預算、進度與時程以及遭遇困難和解決方法等等。

本研究發現，各國在實作 DNSSEC 方法與推廣、部署過程上都有許多相似的地方，由於現今資訊網路發達，即使是遭受海洋或叢山峻嶺的阻隔，相隔幾千里的國家也能透過 E-Mail 等交談工具以及 RIR 與 ICANN 等組織的協助，輕易學習、分享彼此在部署上的技術與經驗，而造成各國在建設進度上出現落差的原因，除了與可利用的經費有關之外，該國的風土民情也是影響 DNSSEC 部署建設的因素之一。

關鍵詞：DNSSEC、ccTLDs、網路釣魚、DNS

* 本文通訊作者。電子信箱：alex@ms.szmc.edu.tw
2015/01/07 投稿；2015/12/19 修訂；2016/04/17 接受

Chang, H.C. (2017), 'The comparison of DNSSEC development and implementation for ccTLDs', *Journal of Information Management*, Vol. 24, No. 2, pp. 185-208.

The Comparison of DNSSEC Development and Implementation for ccTLDs

Hung-Chang Chang*
Department of Information Management, Shu-Zen Junior College of Medicine and Management

Abstract

Purpose—DNSSEC is the next generation of Internet infrastructure. For a more stable and secure network environment, countries around the world are actively promoting the deployment. In view of this, this paper propose is to survey status of DNSSEC implementation to help technology and promoting staff to do evaluation, promotion DNSSEC deployment easily in Taiwan.

Design/methodology/approach—Detection and Statistics are the most important features of DNSSEC deployment survey. We can use this feature to detect their service to obtain the status of DNSSEC deployment and its environment. We observe the target object, and record their resource record. Then we can analyze these data to estimate the status of deployment of the target objects. Finally, we will refer the results to the relevant personnel.

Findings—DNSSEC deployment issue in recent years have been enthusiastically discussed and implemented. DNSSEC is indispensable role next generation. For this reason, we introduced related knowledge in the first place and proposed an Auxiliary Deployment System for DNSSEC to help our government to more easily promote the deployment lastly.

Research limitations/implications—DNSSEC does not provide confidentiality of DNS responses or communications between DNS clients and servers. It also does not prevent attacks on DNS servers using other parts of the network stack-for instance,

* Corresponding author. Email: alex@ms.szmc.edu.tw
2015/01/07 received; 2015/12/19 revised; 2016/04/17 accepted

implementation of DNSSEC does not protect against distributed denial of service attacks or IP spoofing.

Practical implications－Unlike the majority of Top Level Domains (such as .com and most Asia ccTLDs), .tw does not offer registrations at the second level. The .tw zone is partitioned into 14 second level domains, and the remainder (such as .gov.tw, and mod.tw) are managed within the public sector. In spite of the high level of second level domains, .co.tw is by far the largest of the zones managed by Hinet, accounting for between 92-95% of monthly registrations over the past five years. For a TLD structured into second level domains, like .tw, implementing DNSSEC is more complex than with other TLDs. In reality, this did not introduce DNSSEC to .tw domain name registrants, Only then was it possible for .tw registrars to complete the chain of trust through to individual domains.

Originality/value－Deployment System for DNSSEC greatly reduces the complexity of deployment tasks which has many advantages, including Friendly interface, Real-time information, Integration, and Security. In the future, we will actively use the system in DNSSEC deployment.

Keywords: DNSSEC, ccTLDs, phishing, DNS

壹、緒論

一、研究背景

隨著資訊網路科技的普及與快速發展，其帶給人們更便利的生活，也使得網際網路逐漸成為生活上不可或缺的工具。透過網路的資訊傳遞，我們不僅能夠「秀才不出門，能知天下事」，甚至可以透過網路從事購物、傳送郵件、視訊電話等傳統上較為不方便的事情。然而，網際網路的迅速發展，也提供給犯罪者另一個犯罪的方法與途徑，也就是網路犯罪。「水能載舟，亦能覆舟」，網路詐欺、侵害智慧財產權、網路駭客等皆為透過網路的犯罪行為，這些行為所造成的危害已從虛擬的網路環境轉換至人們現實的生活空間。對於這麼一個無遠弗界、不受時間空間限制且不可預期的犯罪，該如何面對與預防，是現時科技發達的我們所須正視的問題。

根據 Symantec（2006）公佈第十一期全球網路安全威脅研究報告（Internet Security Threat Report）指出，當今網路威脅環境中，最明顯的問題為資料竊取、資料外洩、以及具特定目標的惡意程式碼攻擊數量增多，並且透過這些攻擊手法來竊取機密資料以達到獲取金錢的目的。在資料外洩部份，前 50 大惡意程式碼樣本中佔了 66%，並且在資料竊取（包含使用者名稱與密碼）的攻擊，佔了資料外洩總數的 62%。網路犯罪者不斷改良其攻擊方法，試圖以更為隱匿的方式建立全球合作網路，作為犯罪活動增長的後盾。

人類社會結構複雜的開始，各式各樣的詐騙手法不斷地考驗著人們對信任感的依賴，不論是退稅通知、偽造文件等，所針對的皆為人們對既有的信任程度。近年來，可能曾收過網路銀行所發的客戶通知信函，告知您須登入確認資料之類的內容，而這正是網路釣魚的常見的手法。不需太過專業的技巧，駭客即能透過假造網站的方式來取得有效個人隱私資料，獲取不法利益。根據反網路釣魚工作小組（Anti-Phishing Working Group; APWG）（APWG 2007）調查數據，近一年以來，每一單月已有超過一萬七千件網路釣魚事件發生，其中一月份更刷新記錄，當月回報釣魚事件高達 29930 件。其中，3 月的回報瞄準網路銀行與網路金流服務的佔了全產業的 91.6%。可見金融機構是網路釣魚歹徒的重要目標之一。

網路釣魚，除了讓消費者受騙，導致詐欺犯罪的行為外，也影響了一般人繼續使用網路交易的意願，讓網路上正當經營的網站蒙受影響造成損失。

二、研究動機

網路服務、技術不斷地推陳出新，1984 年 Paul Mockapetris 設計出「網域名

稱系統」（Domain Name System; DNS），提供給使用者一個毫無感覺其存在的基礎網路服務，只要使用網路，大多數網路應用需依靠 DNS 的服務來完成。例如，瀏覽網頁、寄發郵件、檔案傳輸等網路服務。DNS 服務主要是提供網域名稱（Domain Name）與網路位址（IP Address）轉換的服務。

2004 年德國少年綁架了 Google.de；2005 年 1 月，ISP-Panix 的網域因網域註冊單位的疏忽而被轉向到位於澳洲的網站等事件頻傳，DNS 技術的翻新，網路詐欺手法從網路釣魚攻擊進階到攻擊 DNS 伺服器的 Pharming 攻擊，攻擊所影響的除了網際網路使用者權益外，連同企業、個人、金融機構，甚至是政府機關，都遭受同樣威脅與侵害，這些問題皆凸顯了網路安全的防護措施與相關稽核機制的重要性。

相對於網路釣魚，另一種較高深的欺騙手法則是針對 DNS 伺服器著手，所使用的技巧包括欺騙網域註冊單位的客服人員及入侵 DNS 主機等。或許 DNS 服務對一般人而言僅是個微不足道的服務，但其順暢安全的運作卻是相當重要的。當攻擊者透過作業系統或應用軟體的弱點進行入侵 DNS 系統，並竄改 DNS 轄區資料時，使用者將被導向至惡意的偽造網站而造成無法預期的損害。

三、研究目的

本研究為瞭解全球各頂級國碼域名在 DNSSEC 推動狀況，以作為相關單位在推動 DNSSEC 建置工作之重要參考；進行全球不同區域主要 ccTLDs 在 DNESEC 整體建置推動之比較與分析研究，以實際瞭解並掌握全球目前推動之現況。

本研究目的為調查全球頂級國碼域名（ccTLDs）在 DNSSEC 之推動現況比較，目標範圍包括以下各項：

1. 以跨區域之方式，針對全球各區域內主要之 ccTLDs 進行 DNSSEC 推動現況之比較。如目前已有 gTLDs 提供 DNSSEC，亦同時進行其推動 DNSSEC 之現況研究。
2. 區域內選擇進行比較之 ccTLDs，應以域名註冊數量及該 ccTLD 其它在政治或經濟層面所具有特殊之影響力為選擇考量。
3. 推動現況之比較應包括：推動 DNSSEC 建置之組織架構、推動建置 DNSSEC 之具體方式、目前受理註冊機構（Registrar）或相關服務商支援 DNSSEC 之現況、已啟動 DNSSEC 之域名比例、提供 DNSSEC 服務之費用及執行 DNSSEC 之相關規範或政策、推動上面臨之問題及解決方案、推動時程。

貳、文獻探討

一、DNS 安全性探討

DNS 當初設計並未考量安全性的問題，主要目的在於提供便利性，讓網路使用者能輕易地經由 DNS 服務將網域名稱轉換為網域位址。DNS 服務對網路使用者而言是個便利的服務；對入侵者而言，DNS 的資訊卻往往是入侵者對目標網域最想取得的第一步，入侵者可藉由網域名稱相關資料瞭解該網域提供的服務及伺服器分佈的情形，入侵者可從 DNS 資訊中獲取該伺服器作業系統平台資訊或 DNS 版本等資訊，藉由這些重要資訊事先了解可從何處著手入侵的程序。

根據 SANS（SysAdmin, Audit, Network, Security）與 FBI 合作之網路安全攻擊目標前二十名漏洞排行榜調查，在跨平台應用程式類，DNS Server 佔漏洞排行榜第六名（SANS 2006）。根據 CVE（Common Vulnerabilities and Exposures）（CVE 2007）與 CAN（Common Vulnerabilities and Exposures candidate）公佈之 BIND 漏洞通報，從 1999 累積至 2007 年共有 52 則。其中，Buffer Overflow 攻擊佔了 13 則。由此可知，DNS 仍是相當脆弱的，其安全性仍待考量。

近年來也有相關研究在討論 DNS 的安全性爭議（Holmblad & GIAC 2003; Pfleger 2003; Carli 2003; Liu 2000; Householder & King 2002），本研究將概略描述各學者所歸納出相關 DNS 弱點或攻擊以及 ISC 所公佈的弱點分佈列表。

Holmblad 與 GIAC（2003）根據了許多文獻，歸納分析之後提出了更詳細的 DNS 弱點，細分為 Spoofing of DNS Responses、Cache Poisoning、Email Spoofing、Exploit of Known Security Related Software Faults、Improper DNS Configuration 以及 High Profile and Successful attacks in DNS Server 等。

Pfleger（2003）研究中指出駭客使用 Cache Poisoning 技術的兩大動機：

1. 阻斷式攻擊（Denial of Service; DoS）攻擊，若「foo.example.net.IN CNAME foo.example.net.」此記錄存在 DNS Cache 中，當使用該網域名稱發出轄區傳送（Zone Transfer）要求時，可能會導致伺服器終止執行，造成 DoS 狀況的發生。
2. 偽裝網站，攻擊者透過偽裝成信任的網站，當使用者在惡意網站中輸入帳號密碼後即完成竊取資訊的程序，為避免被發現此步驟為非正常網站程序所為，再將使用者導向回合法網頁。

Carli（2003）研究中歸納整理 DNS 攻擊分為二大類：

1. 協定的攻擊：區分為 DNS Spoofing、DNS ID Hacking 以及 DNS Cache Poisoning 等三種。名稱伺服器的軟體。
2. 伺服器的攻擊：區分為 DNS 軟體的弱點。例如，緩衝區溢位（Buffer

Overflow）或 DNS 伺服器運作的其他服務以及 DoS 攻擊或濫用發送 ICMP 回應的 Smurfing 攻擊。

Liu（2002）與 Householder 與 King（2002）歸納整理出名稱伺服器攻擊可能有五種：

1. 名稱伺服器的軟體。
2. DoS 攻擊。
3. Spoofing Attacks。
4. 轄區傳送時的資訊外洩。
5. 不知情的參與者（名稱伺服器可能在不知情之下參與攻擊其他網站）。

根據 Aniello Del Sorbo（Del Sorbo 2002）研究中指出 DNS 威脅分為五種：

1. Cache Poisoning。
2. Client Flooding。
3. DNS 動態更新弱點（DNS Dynamic Update Vulnerabilities）。
4. 資訊外洩（Information Leakage）。
5. Compromise of DNS server's Authoritative Data。

根據 ISC（Internet Software Consortium）（ISC 2007）所公告的 BIND DNS 弱點分佈列表中，最常見的弱點攻擊為 DoS、DNS Cache poisoning 以及緩衝區溢位等。DNSSEC 機制於 BIND 第 8 版即被提出，在 BIND 第九版才真正完全實作完成。可見，DNS 伺服器的使用需隨時配合為弱點做修補或更換至較新版版的軟體，才能強化 DNS 協定上的弱點以及保障使用者的網路使用安全。

二、DNSSEC 概述

際網路廣泛用以名稱解析用途的網域名稱系統（Domain Name System, DNS）原是一個缺乏安全性設計的分散式架構，所以歷年來存在著各種轉稼（Pharming）、偽裝（Spoofing）、快取下毒（Cache Poison）與阻絕服務（Denial of Service）等攻擊手法，其中涵蓋著 DNS 區域傳送的安全性問題、動態更新的安全性問題，偽裝資料和快取記錄污染等問題，所以 IETF（Internet Engineering Task Force）為了解決 DNS 服務本身設計所帶來的各種安全性問題，從 90 年代後期就陸續研究並發表了一連串的安全性保護機制。

DNSSEC 乃是透過一種延伸的方法來達成 DNS 安全性的目的，並沒有修改現存 DNS 的運作模式，亦即既有的 DNS 查詢與回應的處理流程並沒有任何變更，只是在每一種運作下新增了資料驗證機制，本文將著重說明如何透過 DNSSEC 來加強既有 DNS 服務的安全性保護之內涵與技術。

（一）DNSSEC 的安全目標

DNSSEC 雖然是 DNS 服務的安全性加強與延伸機制，但並非如萬靈丹一般可以解決所有 DNS 服務目前所面臨的有安全性問題，DNSSEC 的設計乃是透過數位簽章（Digital Signature）的技術來冀望達成下列的安全性目標為：

1. 驗證 DNS 資料來源的真實性（origin authentication of DNS data）。
2. 完整性的確保（Integrity assurance）。
3. 不存在的驗證（authenticated denial of existence）。

另一方面，DNSSEC 並無法提供下列二項安全性服務：

1. 私密性（Confidentiality）：DNS 請求與回應的資料無法避免被竊聽。
2. 可用性（Availability）：阻絕服務（Denial of Service）的攻擊仍可能有效。

換言之，DNSSEC 這項技術僅不過著重於允許用戶端驗證 DNS 回應資料的正確性與完整性。

（二）數位簽章（Digital Signature）

想要理解 DNSSEC 技術運作，您必需先從認識公開金鑰加密技術、數位簽章的產生與確認技術以及信任鏈的概念開始，因為數位簽章可說是 DNSSEC 的關鍵技術。

數位簽章是目前最重要的數位資料防偽技術，電子簽章（Electronic Signature）可取代傳統的簽名或蓋章，但須確保資料在網路傳輸過程中未被竄改，並且能夠鑑別傳輸者之身分，防止其事後否認傳輸之事實。目前網路電子簽章的使用皆是基於數位簽章（Digital Signature），而數位簽章早已廣泛被應用於電子公文、電子契約、電子支票、軟體防偽和網路報稅等各種網路交易平台中。

換言之，利用數位簽章的技術，可提供三項安全性服務與目的：

1. 驗證傳送的來源（Authenticate）。
2. 完整性（Integrity），即確保資料不被竄改。
3. 來源的不可否認性（Non-Repudiation of Origin）。

數位簽章的產生與檢驗須用到兩種密碼學演算法：單向雜湊函數演算法（Hash：MD5、SHA-1）與公開金鑰演算法（RSA），做法是先將電子文件以雜湊演算法計算以產生一固定長度之摘要值（Digest），然後再以簽署人之私密金鑰（Private key）對其加密，形成電子簽章，並得以日後公開金鑰（Public key）加以驗證者。

詳言之，產生數位簽章的一般過程或步驟如下：

1. 將原始訊息利用雜湊演算法（例如 MD5、SHA）計算予以濃縮成一個不可逆且固定長度的摘要值。
2. 利用傳送者的私密金鑰並使用公開金鑰演算法（例 RSA）並將上一步驟所

算出的摘要值予以加密而產生簽章。

3. 將原始訊息和二層加密所得的簽章經由網路一併傳送給接收者。

由上述的步驟過程可知，數位簽章是由雜湊編碼加上一層加密（雜湊與非對稱性演算法）技術所產生的，產生的過程如圖 1 所示。

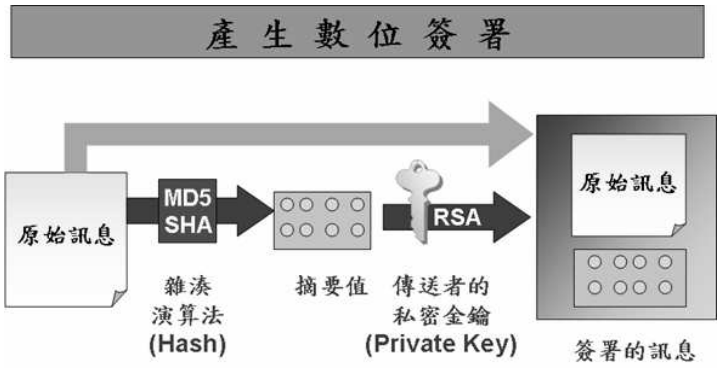

圖 1：數位簽章的產生過程

另一方面如圖 2，一旦接收者收到訊息與數位簽章後，如何驗證數位簽章的真偽，做法及步驟為：

1. 首先取出原始傳送的訊息，並利用相同的雜湊演算法計算出文件的摘要值。
2. 取出簽章並利用傳送者的公開金鑰還原原傳送者所計算的摘要值。
3. 將步驟一接收端所自行計算的摘要值與還原的傳送者所計算的摘要值作一比較，若二者相同則驗證了文件並未被篡改過且傳送的來源具備不可否認性。

由上述的步驟過程可知，接收者是利用傳送者的公開金鑰驗證其真偽。

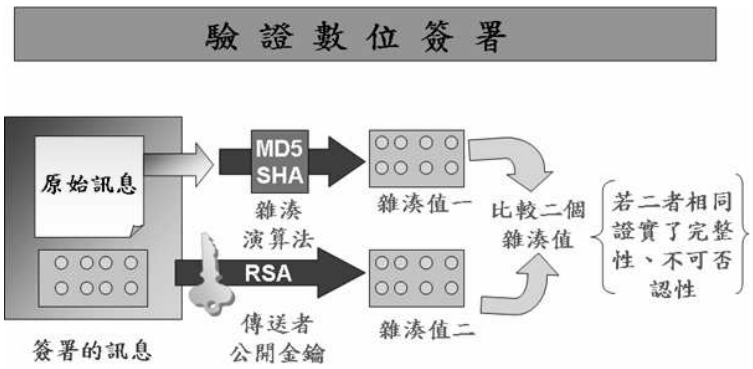

圖 2：數位簽章的驗證架構

一般數位簽章的使用均會透過 PKI 架構，由可信賴的憑證管理中心簽發的憑證來作為公開金鑰信任的來源，利用電子郵件所使用的 S/MIME，報稅所使用的自然人憑證均是，但 DNSSEC 並不使用 PKI，所以數位簽章與公開金鑰等資料以及金鑰的信任鏈就必須由 DNS 區域內的特殊記錄類型來建立。

（三）DNSSEC 相關資源記錄

為了讓 DNS 用戶端可以驗證 DNS 回應資料的正確性與完整性，用來保護用戶端免於受到偽造或竄改的 DNS 資料相關的攻擊，所以 DNSSEC 的回應採用了數位簽章（Digital Signature）技術，透過數位簽章可讓用戶端檢查收到的訊息是否完整及正確的授權來源，不過為了確保公開金鑰的正確性，還需要建立完整階層式的信任鏈（chain of trust），而這整個設計的核心就是必須在 DNS 區域內新增一些可用來存放金開金鑰與簽章的特殊資源記錄類型，這即是 RRSIG、DNSKEY、NSEC 以及 DS 等記錄，此外，DNSSEC 還新增了 AD 與 CD 這二個位元旗標來決定是否執行 DNSSEC 資料確認。因此如果將這些新增的 DNSSEC 資源記錄整合入原來的 DNS 遞迴查詢過程中，一部 DNSSEC 用戶端查詢主機記錄時，伺服器就需要在每一層的解析查詢過程中回覆更多用來驗證簽章所的這些資源記錄，如圖 3 顯示為了提供回覆資料簽章驗證能力，所以 DNSSEC 伺服器需要比傳統的 DNS 回覆時新增驗證所需的 DNSKEY、RRSIG 和 DS 記錄：

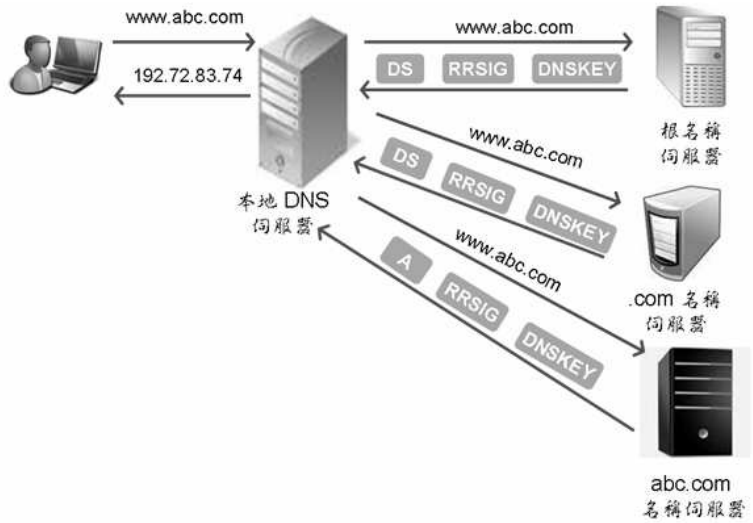

圖 3：用戶端查詢記錄時，與伺服器的溝通過程

驗證資源記錄數位簽章過程時，需要使用到 DNSKEY 的公開金鑰，但問題是當用戶端從網路上取得傳回的公開金鑰時，如何確認這是一把正確沒有問題的公開金鑰，而非有心人士假造或篡改的金鑰，這就牽涉到信任鏈的建立過程，整

個 DNSSEC 信任鏈的設計途徑是先由根域名伺服器的 DS 記錄來確認第一層 DNSKEY 的真偽，再由第一層的 DS 記錄來確認第二層的 DNSKEY 的真偽，最後第二層的 DNSKEY 再確認用戶所收到的記錄數位簽章是否正確無誤，亦即最終確保用戶端所收到的記錄正確無誤，而絕非有心人士篡改或偽造的記錄。

如圖 4 所示，簡單而言，上層 DS 指向下層的 DNSKEY 為信任鏈的基礎。

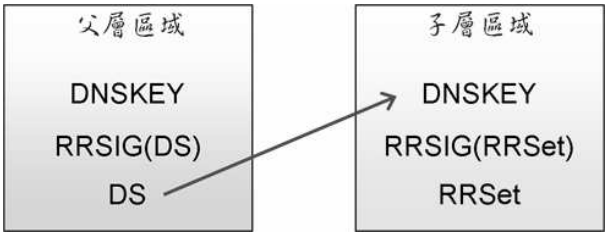

圖 4：DNSSEC 的信任鏈關係

完整的信任鏈如圖 5，將會由 DNS 階層式結構的根網域利用 DS 記錄來指向第一層的公開金鑰開始，再到第二層域 DS 指向第三層的 DNSKEY，第三層……，依此類推，如下圖所示，Root 網域根據下層的.com、.net、.org……第一層網域管理員登錄的公開金鑰來建立 DS 記錄指向其 DNSKEY，而第一層的.com 網域又根據下層的 d1.com、d2.com……網域管理員登錄的公開金鑰來建立 DS 記錄指向其更下層的 DNSKEY。

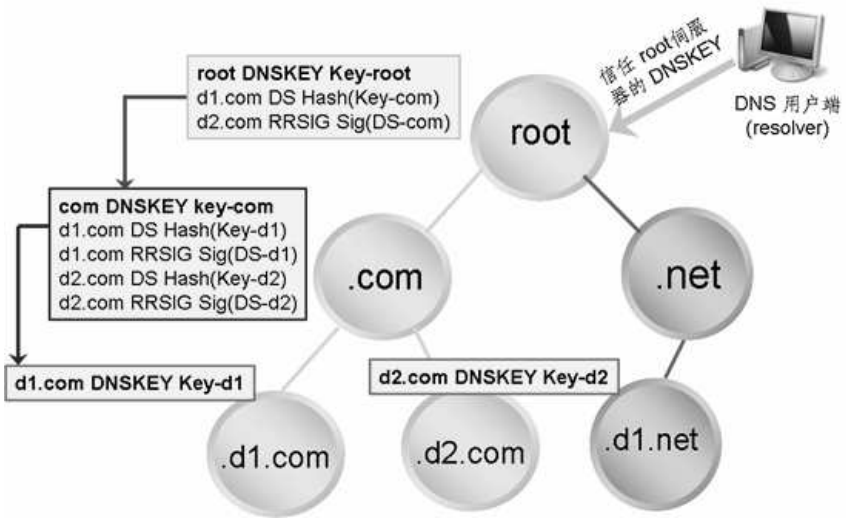

圖 5：DNSKEY 在階層式網域結構之關係

總而言之，DNSSEC 信任鏈的建立並不使用大家所熟知的公開金鑰基礎結構（PKI），信任鏈乃是由緊鄰的 Parent Zone 區域到 Child Zone 區域，亦即只有區域的 Parent Zone 可以擔保他的金鑰正確無誤。

參、研究方法

一、網路資料蒐集

透過搜尋引擎查詢方式瞭解現階段各國頂級國碼域名之 DNSSEC 建置推動之正式文獻及報導，以瞭解此一主題在全球各國現階段的發展趨勢，並深入了解網路管控良好的國家，如圖 6，為日本推行 DNSSEC 的現況報導在網路管控上有何影響等，以便作為本研究的參考。

圖 6：日本推行 DNSSEC 的現況報導

二、E-Mail 問卷分析

透過利用 E-Mail 問卷現況調查的方式，將主要問題議題及現況回覆方法寄發至各管理頂級國碼域名之管理組織（如各國 NIC 等），並針對以下問題協請各頂級國碼域名之管理組織回覆：

1. 推動 DNSSEC 建置之組織架構。
2. 推動建置 DNSSEC 之具體方式。
3. 目前受理註冊機構（Registrar）或相關服務商支援 DNSSEC 之現況。
4. 已啟動 DNSSEC 之域名比例。
5. 提供 DNSSEC 服務之費用及執行 DNSSEC 之相關規範或政策。
6. 推動上面臨之問題及解決方案。
7. 推動時程。

三、DNSSEC 安全性測試

透過現有已開發成熟之 DNSSEC 測試平台及工具，根據 DNSSEC 新增的 DNSKEY、RRSIG、DS、NSEC 等四種安全性記錄格式，本研究採用容易使用的兩種第三方 DNSSEC 驗證工具：DNSSEC Analyzer（如圖 7）與 DNSViz（如圖 8），來協助本研究者確認 DNSSEC 功能是否正確運作。DNSSEC Analyzer 能迅速得知驗證結果，而 DNSViz 以圖形介面顯示信任鏈驗證過程，能以更直覺的方式協助管理者除錯。來測試 DNSSEC 建置之完整性及安全性，並與 E-Mail 問卷回覆及蒐集之網路資料交叉確認。分析啟用與未啟用 DNSSEC 機制之後，可以從存放轄區資料的檔案看到其檔案大小增加了六倍之多。為確保查詢的網址為俱有不可否認性，以 DNS 工的指令來進行查詢網址。

（一）DNSSEC Analyzer

- http://dnssec-debugger.verisignlabs.com/
- DNSSEC Analyzer 為 VERISIGN 公司旗下的實驗室所開發的一套專門用來測試給定的域名是否支援 DNSSEC 服務的工具。其基於 Web 平台運行所開發，因此具備高度的易用性，使用者只需要輸入域名或任一個網址，系統即會從該網域的 Root-zone 開始一層一層地往下驗證下去，用以確保 DNSSEC 的信任鏈能夠完整地在該網域下運作，並且對發現到的問題給予使用者警示訊息。
- DNSSEC Analyzer 的輸出乃是以文字條列的方式列出信任鏈的驗證結果
- 優點：
  (1) 分析速度較 DNSViz 快。
  (2) 若只想知道驗證結果是否正確，從表格裡的 icon 即能迅速得知結果。
- 缺點：
  (1) 驗證細節以條列式顯示，與 DNSViz 圖形介面相比較不直覺。
  (2) DNSKEY/DS 的資訊不如 DNSViz 詳細。

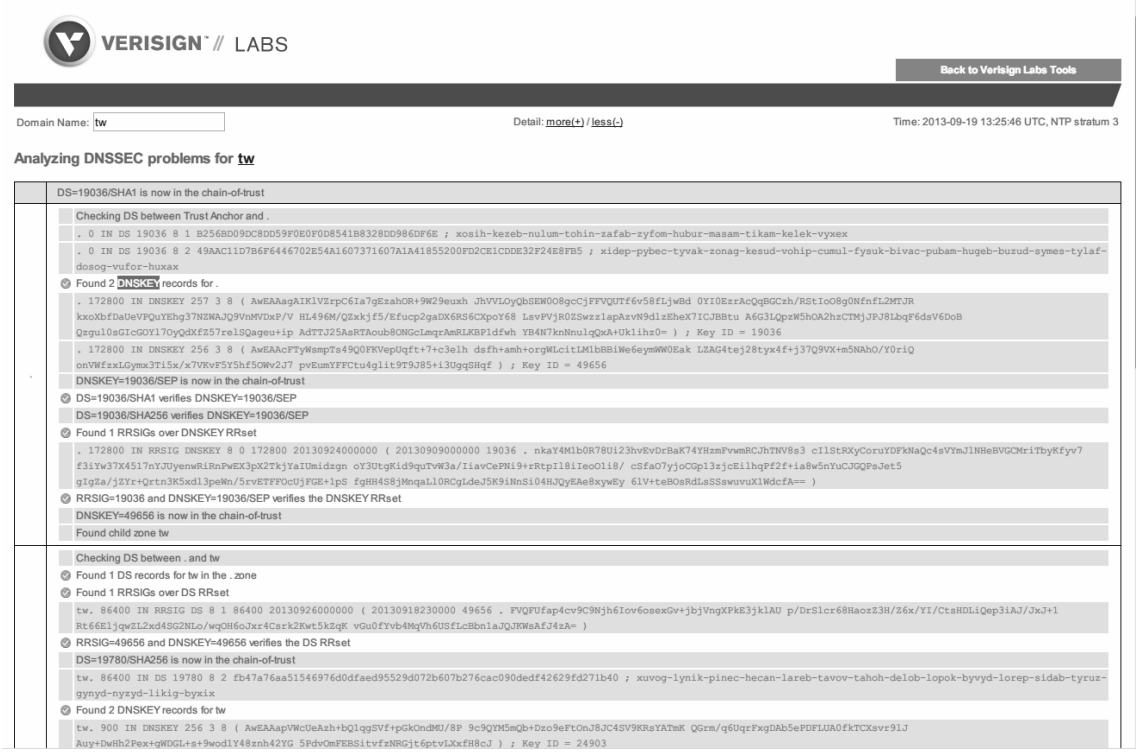

圖 7：Verisign Labs 網站

（二）DNSViz

- http://dnsviz.net/
- DNSViz 為 Sandia 公司設計開發的一套用來視覺化 DNS zone 狀態的分析工具。DNSViz 被設計用來幫助使用者瞭解與解決在 DNSSEC 部署上遇到的問題，它提供了 DNSSEC 驗證鏈中的域名與 DNS 命名空間的解析路徑之可視化分析，並且還列出了它所檢測到的錯誤。
- 網頁會以圖表顯示信任鏈驗證結果。
- 優點：

  (1) 驗證細節以圖形介面顯示，能迅速理解驗證過程。

  (2) 將滑鼠游標移至 DNSKEY/DS icon 即能得知相關詳細資訊。
- 缺點：

  (1) 分析速度較 DNSSEC Analyzer 慢。

  (2) 因圖形介面需要較大版面，且需理解圖形所代表的意義，故無法像 DNSSEC Analyzer 能迅速得知驗證結果是否正確。

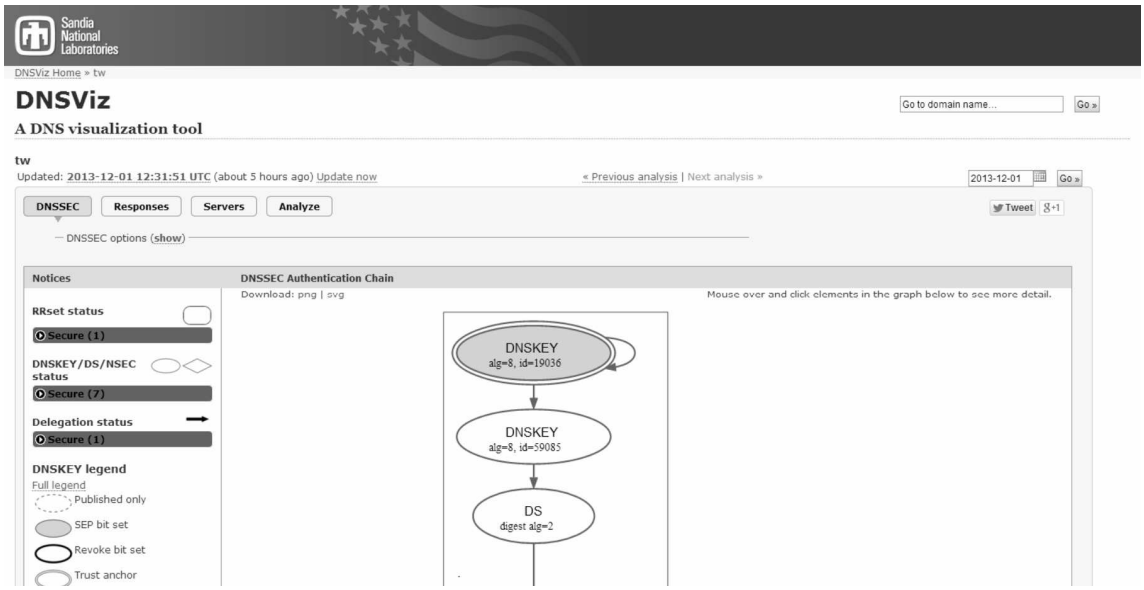

圖 8：DNSViz 網站

肆、研究內容

一、各國現況及問卷調查

為了解決傳統 DNS 在安全方面的問題，自 2009 年開始，許多的國家頂級網域便開始著手進行 DNSSEC 的相關實驗，並在經過一年以上的實驗測試後，於 2011 年正式陸續導入 DNSSEC 的營運。

根據本研究針對目前全球部署建置 DNSSEC 的現況調查及問卷回覆結果及第二節的安全性及網路測試結果如下：

1. 扣除重複性國家頂級網域後，共發出 EMAIL 問卷共 253 份，共收到有效問卷 83 份回覆，無效問卷回覆 23 份，無回應之問卷共 147 份。
2. 連同台灣在內總共有 32 個國家回覆詳細建置過程及經驗分享，詳細國家別為阿富汗、比利時、波札那、智利、中國、哥斯大黎加、捷克、德國、愛沙尼亞、西班牙、芬蘭、法國、香港特別行政區、曼島、約旦、立陶宛、冰島、日本、南韓、蒙古、尼日、奈及利亞、紐西蘭、巴布亞新幾內亞、盧安達、所羅門群島、斯洛文尼亞、臺灣、、蘇聯、泰國、東加、英國等國。
3. 捷克：為 IPV6 滲透率是全球之首，主要的捷克網際網路服務供應商所組成的非營利協會以及聯合捷克政府訊息部簽署協議，民間聯合政府共同推

廣 IPV6

4. 中國：封閉型共產國家之代表，目前中國僅在極少數的部份地區提供支援 DNSSEC 的服務，在隱私方面，中國 CNNIC 方面承諾在不涉及到司法、行政時，會確保個人資訊與機密的訊息不會被洩漏給第三方知道。在部署遇到的困難時，中國認為在金鑰的保護、資料的傳輸以及服務的驗證上是比較棘手的，針對這些問題，中國未來將會積極升級現有設備來進行改善。
5. 如表 1 所示，得知目前根網域（root domain）全部 13 台伺服器已經完全支援 DNSSEC，在 generic TLD 通用型網域名稱部分，即「.com」、「.net」、「.org」等，也已有 9 個網域支援 DNSSEC，至於國家頂級網域（Country Code Top-Level Domains; CCTLD）的部分，目前則有 87 個國家頂級網域有支援 DNSSEC，另有 4 個國家可部分支援，佔全部 253 個還在使用中的網域的 34.39%。

表 1：DNSSEC 部署狀況

Domain 類別	總數量	支援數量	百分比
root domains	13	13	100%
gTLDs	26	9	35%
ccTLDs	253	87	34.39%

二、各國現況彙整

根據上節調查結果，下面我們將針對已回覆問卷及幾個重要的國家或地區在推廣 DNSSEC 的工作現況予以概述，並且在此進行比較與分析：

從收到的問卷進行統計，我們整理出部分已知國家的 DNSSEC 普及率如表 2 所示：

表 2：回收問卷之各國 DNSSEC 普及率

國家	普及率總數量
捷克	27.9%
法國	3.5%
所羅門群島	1%
哥斯大黎加	1%
南韓	<1%

蘇聯	<1%
智利	<1%
泰國	<1%
德國	0.08%
斯洛文尼亞	0.045%
比利時	0.04%
日本	0.03%
紐西蘭	0.018%
立陶宛	0.00437%

依照網路蒐集與實際測試結果，我們整理出世界各大洲對 DNSSEC 的相對支援比例如圖 9 所示：

圖 9：各洲 DNSSEC 普及率

三、各洲別區域現況比較

綜合以上兩節調查結果，我們發現世界各國對 DNSSEC 的部署與否和其經濟發展有著顯著相關，而經濟發展又與地域有著密不可分的關係，圖 10 即為

DNSSEC 在世界各地的部署分佈圖，下面我們將針對不同洲別的發展狀況進行分析：

資料來源：dnssec-deployment.org

圖 10：DNSSEC 在世界的部署分佈圖

（一）亞太地區

亞太地區的 DNSSEC 發展以東亞附近地區最為成熟，包括日本、韓國、中國、泰國以及我們台灣等等，都是經濟發展相對較好，基礎設施建置完善的國家。

而在中東附近戰亂及落後的國家則多沒有部署及建置 DNSSEC。

此地區會定期舉辦 DNSSEC Workshop，讓各國的網域管理單位可以分享經驗、交流技術。並有一網路發展組織 APNIC（Asia Pacific Network Information Centre）居中提供培訓與部署上的支援。

APNIC 為五大 RIR（Regional Internet Registries）之一，是一個開放性會員制的非營利組織，其成立的目的為促進區域網路建設發展，並確保 IP 位址與相關的資源能夠被平均地分配。其中不包含俄羅斯與中東國家在內，在 56 個亞洲與太平洋經濟區中共有超過 2700 個會員。

（二）歐洲地區

歐洲地區由於網路基礎建設較早，國民平均所得也普遍高於他州各國，因此

歐洲地區的國家大多已經完成 DNSSEC 的部署，而尚未部署及建置 DNSSEC 的國家則多集中於在南歐，究其原因，應與近年的歐洲經濟危機導致無經費或資源可提供建設有所關聯。

該地區負責分配 IP 位址的組織為 RIR 中的 RIPE NCC（Réseaux IP Européens Network Coordination Centre），其總部在阿姆斯特丹，受到荷蘭法律的保護。RIPE NCC 在全球超過 70 個國家中，包括俄羅斯、中東以及中亞部分地區在內，共有超過 7000 個會員，成員有 ISP 業者、電信機構、監管單位、政府、教育機構以及大型企業等等，任何組織或個人都可以成為 RIPE NCC 的會員。

（三）美洲地區

美洲地區只有幾個經濟規模較大的國家完成 DNSSEC 部署，其他在加勒比海與拉丁美洲幾個落後國家中則較無多餘資源可供利用。

美洲負責分配 IP 位址與相關網路資源的 RIR 機構有二，一為負責北美與部分加勒比海地區的 ARIN（American Registry for Internet Numbers），二為負責拉丁美洲與部分加勒比海地區的 LACNIC（Latin American and Caribbean Internet Address Registry）。

（四）非洲地區

非洲僅有幾個大國推動部署及建置 DNSSEC，大多數的國家可能因為基礎發展較為落後，未能有所行動。

非洲負責分配 IP 位址與相關網路資源的管理機構為同樣屬於五大 RIR 組織的 AFRINIC（African Network Information Center），其總部位於模里西斯的埃本城。在 AFRINIC 尚未成立之前，非洲的 IP 位址是由 APNIC、ARIN 與 RIPE NCC 所分配。

（五）小結

由於現今資訊網路發達，即使是受海洋阻擋，相隔幾千里的國家也能透過 E-Mail 與 Skype 等工具輕易分享彼此在部署上的技術與經驗，加上有 RIR 與 ICANN 的協助，我們發現各國在實作方法與推廣過程上都有許多相似的地方，而造成其它各國的建設進度出現落差的原因，除了與可利用的經費有關之外，該國的風土民情也是影響 DNSSEC 部署建設的因素之一，例如中東的國家可能因為宗教或戰爭的因素相對保守，或者是歐洲某些很少傳出有重大資安攻擊事件的國家可能就對部署 DNSSEC 較無法產生共鳴。

四、DNSSEC 安全性及網路測試

綜合第參、三節所提到的 DNSSEC 安全性測試方法，根據 DNSSEC 新增的 DNSKEY、RRSIG、DS、NSEC 等四種安全性記錄格式，本研究採用容易使用的兩種第三方 DNSSEC 驗證工具：DNSSEC Analyzer 與 DNSViz，來協助本研究者確認 DNSSEC 功能是否正確運作。DNSSEC Analyzer 能迅速得知驗證結果，而 DNSViz 以圖形介面顯示信任鏈驗證過程，能以更直覺的方式協助管理者除錯。

綜合前面所提到的測試方法，我們以 DNSSEC Analyzer 和 DNSViz 對各國的頂級網域進行測試，在 DNSKEY 驗證的部分，從圖 11 的統計分布資料中可以看到有 6%的 ccTLDs 沒有使用 DNSKEY，代表其安全性也是有疑慮，無法確認資料的完整性，發揮不了 DNSSEC 的安全性優勢，其它 ccTLDs 皆有使用到 2 組以上的 DNSKEY，以確保 DNSSEC 防護性。

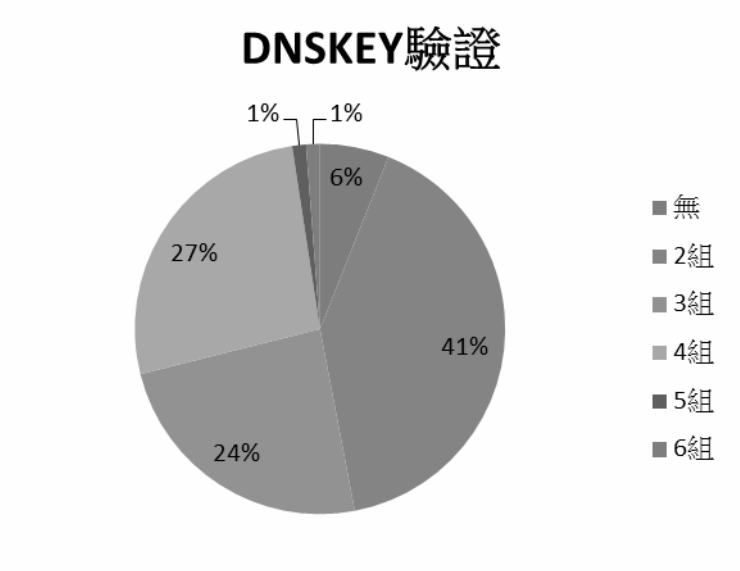

圖 11：DNSKEY 使用數量統計圖

在上層 DS（Delegation Signer）驗證部分，如圖 12，也有 6%的 ccTLDs 沒有使用此驗證功能，無法保證 Child Zone 之 DNSKEY 確實是正確且未經竄改，容易造成來源可驗證的功能。

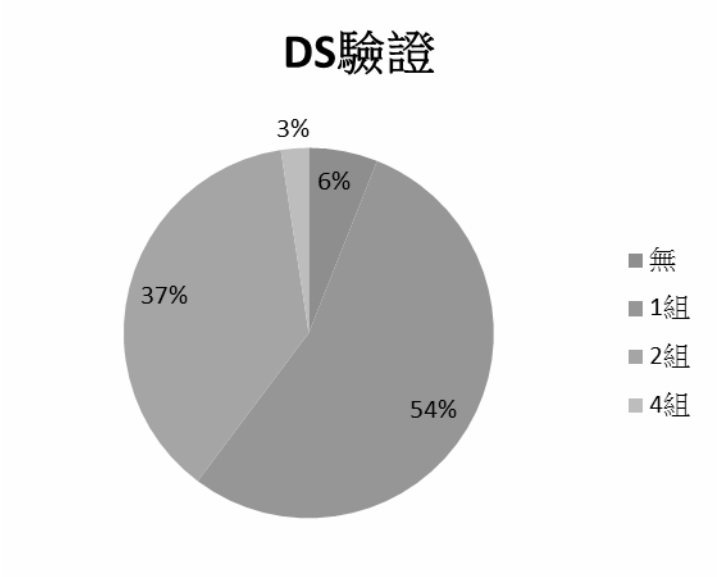

圖 12：DS 使用數量統計圖

用於驗證 DNSSEC 之不存在性的 NSEC 記錄部分，本研究也加以測試統計，如圖 13 所示，結果跟 DNSKEY 的測試結果相同，有 6%的 ccTLDs 沒有 NSEC 記錄功能，無法進行不存在性的驗證。

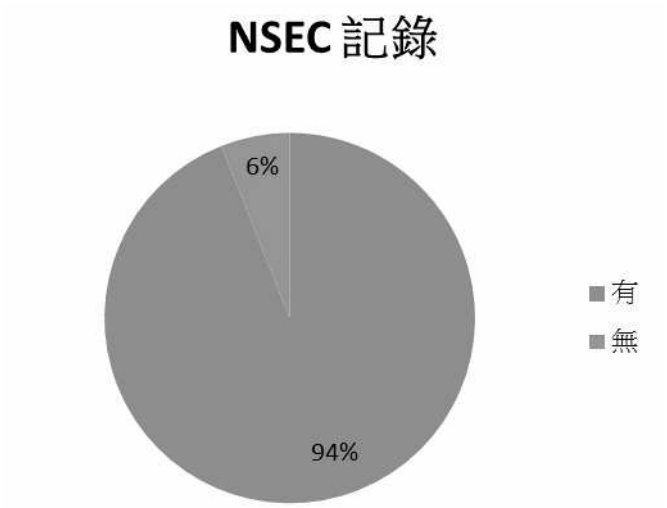

圖 13：DS 使用數量統計圖

伍、分析與結論

一、比較與分析

綜合上一章節所提到的各國現況，我們從調查與收到的反饋當中可以發現各國在部署 DNSSEC 上的進度普遍都比較緩慢，如法國與日本兩個國家皆是從 2009 年就開始著手 DNSSEC 的部署計劃，但發展至今，支援 DNSSEC 的比例才分別達到佔該地區所有網域的 3.5%與 0.03%，這樣的情況和 IPv6 的升級推廣有點類似，其原因分析如下：

1. DNSSEC 的部署有其技術難度，包括網路基礎建設、部署維運、金鑰管理、驗證與除錯等，皆需要相當的時間學習與熟悉。
2. DNSSEC 的部署不像當初在部署光纖網路基礎設施時，有可以被明顯感受到的成果，加上目前 DNS 並沒有立即危害的風險，在大環境不景氣，產品銷售薄利化的現在，相關單位往往把這類有關資訊安全的建設計劃的工作優先權順序降低。
3. 缺乏誘因。如同國內發展 3G 行動上網與 4G 行動上網所面臨的問題，雖然 DNSSEC 明顯優於傳統的 DNS，可以解決目前極為氾濫的網路釣魚等駭客攻擊，但有關產業可能礙於升級成本，不願首先投入人力與資源。

針對上述幾個原因，從 2008 年即開始部署 DNSSEC 的捷克給了我們一個很好的經驗，捷克不僅於基層積極推廣 DNSSEC，爭取一般民眾對於資訊安全議題的重視，在政策方面也採取了和註冊機構聯合營銷的規劃；為了增加誘因，法國於 2013 年 10 月中旬起，亦對有關工作花費給予獎勵性質的補貼，除此之外，為了統一標準與降低作業的複雜度，法國也針對不同的技術環境給予技術指導，以上種種措施都是對推廣 DNSSEC 的部署有一定的幫助。

雖然世界各國在推動 DNSSEC 的部署上遇到許多困難，但我們從各國的推動時程與政策中可以發現，在人們對資安意識愈趨重視的當下，各國對相關的建設所投入的心力可說是愈趨積極，預計在未來 10 年內，DNSSEC 會快速地在全球各地完成部署，並且逐步取代現有的 DNS。

二、對台灣推動 DNSSEC 的建議

即使 DNSEEC 相較於傳統的 DNS 提供我們更強大的安全性，可令人遺憾的是一般的使用者對這方面的知識普遍都不是很瞭解，甚至對於資安議題也沒有特別地重視，在使用者缺乏興趣的背景下，相關的發展、服務與註冊機構也就不願意編列預算升級部署 DNSSEC 所需要的相關設施。這樣的情況不只在台灣發生，各國在發展 DNSSEC 上大都也面臨到這樣的困難，其肇因不安全的資訊環境所帶

來的傷害通常不是可以被立即看見的，尤其目前 DNS 仍在正常運作當中，人們往往會認為沒有迫切需要，而忽略了其中可能帶來的巨大風險，甚至還有部分的人認為，在 DNS 上所被發現的緩存中毒攻擊只是一項可能的風險，而不是一個絕對的理論。

有鑑於此，政府應該效法日本等國，於各地方積極辦理資安講座與工作論壇，用以提升國人對於網路安全的認識；對於一般的發展、服務與註冊機構，也應該透過技術顧問與出版作業準則等方式降低 DNSSEC 的複雜性，以增加民眾對 DNSSEC 操作的信心與透明度，並且可以考慮參考法國在推動 DNSSEC 的政策，對有關於推動 DNSSEC 部署的活動給予適當補助以鼓勵基層加速辦理 DNSSEC 的升級部署，以增加其對於升級 DNSSEC 的誘因。在部署的優先順序上，可先從政府機關與需要較高安全性的金融產業界著手，用以達到示範之功效。

部署 DNSSEC 的工作並非一蹴可幾，需要長時間投入人力與資源，因此政府在 DNSSEC 推動上應該要有耐心，按部就班而不可躁進，確實穩當地將相關的基礎建設建置妥當，並參考及汲取世界各國推動經驗，方是臺灣網路資訊安全發展的長遠之計。

參考文獻

賽門鐵克（2006），第十一期全球網路安全威脅研究報告－資料遭竊與洩漏日益普遍，駭客針對特定目標進行攻擊從中獲利，http://www.symantec.com/zh/tw/about/news/release/article.jsp?prid=20070320_01（存取日期 2013/10/6）。

Anti-Phishing Work Group (APWG) (2007). 'Phishing Activity Trends—Report for the Month of January', available at http://www.antiphishing.org/reports/apwg_report_january_2007.pdf (accessed 8 October 2016).

Carli, F. (2003). 'Security Issues with DNS'. VA, USA: SANS Institute.

Del Sorbo. A. (2002). 'Network Security Sk-DNSSEC: an alternative to the Public Key scheme Syncfiles: a secure file shareing service for Linux'. ITALY.

Holmblad, J. and GIAC, S. (2003). 'The Evolving Threats to the Availability and Security of the Domain Name Service'. VA, USA: SANS Institute.

Householder, A. and King, B. (2002). 'Securing an Internet Name Server'. PA, USA: Software Engineering Institute.

Internet Systems Consortium (2003). 'BIND Vulnerabilities'. available at http://www.isc.org/index.pl?/sw/bind/bind-security.php (accessed 22 May 2007).

Internet Systems Consortium. (2007).http://www.isc.org (accessed 06 April 2017).

Liu, C. (2000)，DNS and BIND（3 版），蔣大偉（編譯），美商歐萊禮股份有限公

司台灣分公司，台北。

Pfleger, J. (2003). 'DNSSEC Resolver Algorithm'. Unpublished master dissertation, University of Disponível, Wien, Austria.

SANS (2006). 'SANS Top-20 Internet Security Attack Targets'. available at http://www.sans.org/top20/ (accessed 12 March 2007).