

# 財團法人台灣網路資訊中心因公出國人員報告書

九十八年十二月二日

報告人 姓名	高境輿、楊禎葆	服務單位及 職稱	TWNIC 工程師
出國期間	九十八年十一月八日至 九十八年十一月十四日	出國地點	日本-廣島
出國事由	參加第七十六次 IETF 日本廣島會議  報告書內容應包含：  一、出國目的  二、考察、訪問過程  三、考察、訪問心得  四、建議意見  五、其他相關事項或資料  (內容超出一頁時，可由下頁寫起)		
授權 聲明欄	本出國報告書同意貴中心有權重製發行供相關研發目的 之公開利用。  授權人： (簽章)		

附一、請以「A4」大小紙張，橫式編排。出國人員有數人者，依會議類別或考察項目，彙整提出報告。

註二、請於授權聲明欄簽章，授權本中心重製發行公開利用。

## 一 出國目的

至日本廣島參加IETF第七十六屆會議，本次會期自九十八年十一月八日（日）至十一月十三日（五），為期六日，主要目地為參與及了解各技術發展WG 的趨勢及討論方向，與會期間並與CNNIC討論CDNC決議事項執行進度與交換意見，本會期IDNABIS及EAI並無議程。

## 二 考察、訪問過程

此次會議雖期程共六天，於會期間均於 ANA 會場飯店參與各相關 WG 並觀察現場環境及設備配置並與 CNNIC 討論 CDNC 決議事項執行進度與交換意見。

## 三 考察、訪問心得

### \*會場環境及設置觀察心得

本次會議於廣島 ANA HOTEL 舉辦,共於 8 個 room 舉行各 SECTION,分於三、四兩樓(三樓七間、四樓一間),場地均為非階梯式並配合 AIR WALL 可打通空間 ,下圖為場地投影機設置及座椅排放情形,左邊為 OPEN MIC 識別投影幕,一為簡報內容投影幕。



(圖一. 場地投影機設置及座椅排放情形)

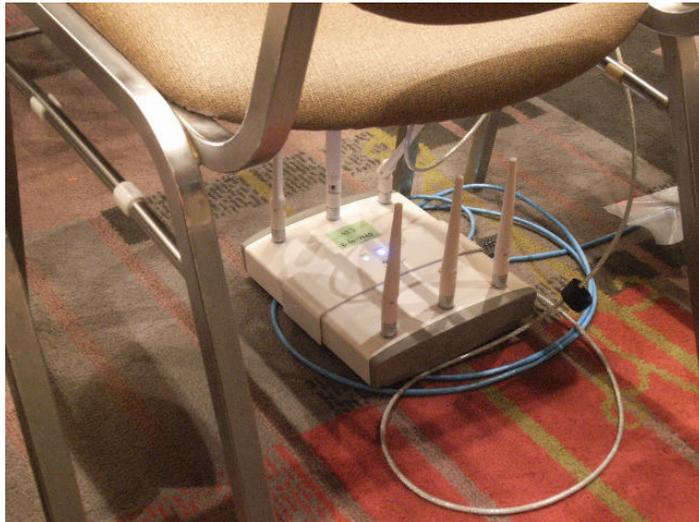
報到台設於三樓電梯入口處,於各 ROOM的正中央,旁邊設置白板資訊看板及兩台

42 吋 LCD 螢幕顯示各 ROOM 議程。



(圖二、圖三. 會場報到臺設置及資訊看板)





(圖四、圖五. 會場無線 AP 設置圖)

無線網路部份會場共有 50 部 CISCO 1252 AP,支援 802.11a、b、g、n 並提供兩路加密連線以 WPA2-PSK 的方式以 AES 加密,並將 CHALLENGES STRING 列在每個 STAND 下方。

ESSID	802.11 Protocol	Band	Security
ietf	b/g/an	2.4GHz 5GHz	NONE
ietf-a	an	5GHz	NONE
ietf-v6ONLY	b/g/an	2.4GHz 5GHz	NONE
ietf.wpa	b/g/an	2.4GHz 5GHz	WPA2-PSK(AES)
ietf-a.wpa	an	5GHz	Security Key hiroshimaJAPAN

NOC team prefers 5GHz band(802.11an) connection.

(圖六. 本屆無線網路之 SSID 表,於各 AP STAND 下方均有黏貼)

本屆 IETF 於會期由主辦單位發起一個 RFID 的測試實驗,每位與會者除了名牌外另加發一個 RFID TAG,經過報到只至實驗官方網頁開通帳號後,便可將 IETF 報到資料 SELECT 出來,應用方式為在各 WG 的 OPEN MIC 的 STAND 下方以拉鍊袋將 RFID SENSOR 搭配 IPHONE 成爲輸入感應端,於發言時只要將 TAG 感應,便會在前方螢幕 SHOW 出發言者資料。



(圖七、圖八.感應輸入端設備及感應顯示結果)

各 ROOM 的座位設置不足,故多數場次都有與會者站在後方,插座設置數目也較前幾屆為少。



(圖九 因座位安排較少,多數場次都是滿座情形)



(圖十 插座設置圖,插座與人數比率約為 1 比 4,較為不足)





(圖十一、十二、十三 TERMINAL ROOM 分為兩間,每間均可坐約 25-30 人,一間提供彩色印表機,另一間提供黑白印表機,設定資訊均貼於設備上)



(圖十四 每日中午均有販賣餐盒)



(圖十五 本屆 IETF 76 贊助單位之露出看板)

\*參加 section 心得:

## <DNSEXT>

DNSEXT 主要在討論 DNS 之功能發展，例如 DNS 應具備那些功能或新增什麼樣的資源記錄等，皆在於 DNSEXT 工作小組中討論，就中心負責 .tw DNS 運作的角色來說，此工作小組一直是中心參與 IETF 以來，一定會參與的部份。本次會議 DNSEXT 討論僅有兩個主題，即 DNSSEC、DNS TCP transport 為主，主要討論如下：

draft-ietf-dnsext-dnssec-algallocation-00 由 Paul Hoffman 提出，主要做為 IANA 之註冊使用，描述了 DNSKEY 不同的的演算方法代碼，如 DNS Security Algorithm Numbers 5 為 RSA/SHA-1 編碼等，由於目前的 DNSSEC 相關 RFC/Drafts 並未對各數值之代號進行描述，故 Paul 本篇主要透過 IANA 的 DNSKEY Registry 來對各編碼方式，長度等進行代號之描述，以利日後 DNSSEC 相關之表格使用。因本篇內容極為簡單，主要對於 IANA 及 DNSKEY 之代號進行規範，故在主席一在詢問下，與會者皆無意見，相信本篇應直接進行 Last Call。而 WORKING GROUP 所提及之 draft-ietf-dnsext-dnssec-registry-fixes-01 因為內容及精神和 Paul 一樣，故會議上僅進行了簡單的報告。

Dnssec-bis 之修改版本主要著重在對查詢結果的狀況判斷之描寫，在 DNSSEC 的信任架構中，對於回應不對的 DNSKEY 等，在回應值上以 INSECURE/SECURE/BOGUS 等來說明，但作者的描述與會者有許多不同意見，主要在於回應值的狀況描述不足，在某些情況下未考慮，在許多人的質疑下，大家皆同意此文應對此回應值進行更多細分及描寫，以利將來實作上得以判斷。

TCP DNS 主要探討在將來的 DNS 設計上，可使用 TCP 協定，以增加 DNS 的可靠度，因 UDP 封包存在假造及欺騙等問題。故在此 WG 長期以來，一直有些人為 TCP DNS 的設計而努力。以本次會議來說，TCP DNS 存在許多正面與負面之不同看法，例如，支持 UDP DNS 的以 UDP 可以大量回應為主要論點，可以承載較高之查詢壓力等，但 DNS 的先天限定 (RFC1035)，封包不能超過 512bytes 之問題，雖然有 EDNS0 之支援，但仍不完全。支持設計 TCP DNS 者則站在了 TCP 協議不能偽裝、不需要 DNSSEC 即能保證內容，對於封包大小未限定等優點，但也承認 TCP DNS 存在了封包會有 fragmentation 之問題，及存在 SYN 等攻擊風險。而因為在 RFC1123 中寫到 DNS QUERY “MUST” 先以 UDP 傳送，目前討論方向是“不一定”要先送 UDP，會上連續三篇 PRESENTATION 包含前言~說明~及實驗報告證明其可行性，目前想法並非是全改由 TCP 而是希望能支援 TCP，進而有效解決目前臨的問題，而成為完整的 DNS SOLUTION，在會場上發言者大多數皆對 TCP DNS 持正面之看法，但最後主席則裁示這一議題回歸社群及郵件列表上討論，後續將持續觀察其發展及變化。

### <YAM& SASL >

在 YAM WORKING GROUP 內數篇 EMAIL 相關 PROTOCAL 的作者,針對目前 IESG,執行作業的做法上進行討論,認為 IESG 於對於推動標準上的程序應有所調整,以目前的作法對於標準之推動不但無法順暢推動,更反而造成阻撓。

於 SASLWORKING GROUP 上以 RFC4752 中內容來檢討本 WG 未來發展的方向,並進行討論,最後並決議將於近期內 CLOSE 本 WORKING GROUP。

### <DNSOP>

在 DNSOP 的 WORKING GROUP 上本屆討論幾個議題,首先是討論依 DSP 的規範下 DNSSEC 的 KEY 的 TIMING 是否適宜,另外來自 NTIA(National Telecommunications and Information Administration)的也於會上介紹 NTIA 的相關資訊及任務內容,包含整理 ICANN 及 VERISIGN 的 DSP..等 DNS SEC 的相關資料,詳細請至 <http://www.ntia.doc.gov/dns/dnssec.html>,另外於 WORKING GROUP 上也討論到在 IDN 的背景前提下對於新 TLD 的開放註冊之相關議題,與會不少人皆表示意見,不過也都了解這是要看 ICANN 的決策,另外在會上也有 CNNIC 報告 IDN TLD IMPLEMENTATION GUIDELINE 與會人士多認為本篇屬於經驗分享性質,會上也發表了 DNS PROXY BYPASS,及建議 IANA 修改 SERVICE NAME 及 FIRE FOX 的 DNSSEC PLUGIN..等議題,均引起與會人士討論及不少迴響。

### <V6OPS>

於 WORKING GROUP 上討論議題有” ISP SIMNARIO”本篇作者表示目前該篇是以資料整合及研究之階段為主,期望能蒐集各 ISP 於 v6 施行之過渡時期作法,本篇目地為拋磚引玉將各種作法加以搜集,並希成爲 BCP,不過與會者多認為本篇應分析至 v6 環境下各 ISP 對不同 SERVICE 的作法,且認為不比較方法之好壞,應一併收錄以確定本文之完整性,也認為本篇不應以 BCP 為期待,應列爲 INFORMATIONAL RFC ,作者表示將再進行修改,也期待各 ISP 的與會者能會後提供研究之資料供其參考,另一篇討論 CGN(Carrier-Grade NAT)的問題,指出在 IPv6 over IPv4 或者 v6 to v4 的狀況下,應考慮 MTU 限制的問題(AT LEAST 1500BYTE),另篇討論 TEREDO EXTENSION 的部份,作者指出在 RFC4380 中應列出更完整的 NAT TYPE,另外也提到在 SERVER LOAD 部份可加以改善,認為在 TRAILER TYPE HANDLEING 部份,只要去分析 TYPE=00 的部份,TYPE==01 的狀況則於其他 TYPE 情形一樣直接忽略,之外也認為 NAT 的狀態 FLASH 應小於 30 秒,另外有作者展示 IPv6 的 APPLICATION PROXY,提出有趣的論點,當 v6 環境下的服務不使用 DNS64 或當爲 v6 ONLY HOST 的情形,則可透過 APPLICATION

PROXY 進行轉譯,而與會者多抱持保留態度,希望作者於本篇後續能有更深入的內容供大家參考。

**\*與 CNNIC 討論情形:**

於會期間與 CNNIC 再次確認 CDNC 決議事項,針對 EAI 決議事項及字表議題進行執行討論及確認,目前執行情形良好。

#### **四 建議意見**

- 1.建議持續關注相關各 WORKING GROUP 動態及相關訊息。
- 2.建議國內 ISP 持續積極投入 IPv6 的佈建,並加強與國際上其他 ISP 討論及分享佈建經驗。
- 3.建議與國外相關單位進行更密切及多元的交流及經驗分享。
- 4.建議分析近幾屆各主辦單位辦理 IETF 各方面作業情形,以為參考。
- 5.DNSSEC 部份應可配合 WORKING GROUP 標準討論方向,逐步進行相關測試。

#### **五 相關資料**

[1] 76th IETF Meeting URL : <http://www.ietf.org/meeting/76/>

[2] 76th IETF Meeting Agenda : <https://datatracker.ietf.org/meeting/76/agenda.html>