財團法人台灣網路資訊中心因公出國人員報告書

九十五年十一月二十日

報告人 姓 名	楊禎葆 葉士豪	服務單位及職稱	工程師 工程師
出國期間	九十四年十一月六日至 九十四年十一月一十三日	出國地點	美國-聖地牙哥
出國事由	參加第六十七次 IETF 聖地牙哥會議 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

第六十七次 IETF 會議於九十五年十一月五日至九十五年十一月十日在美國聖地牙哥舉行。此次會議爲期六天，而中心參加之主要目的爲參加 EAI WG (Working Group) 標準討論 EAI (Email Address Internationalization)，及參加 DNS 相關之 WG 會議，並參與會中心之相關議題(DNS/DomainKey/Ecrit) 以了解其發展。

二、考察、訪問過程

此次會議雖期程共六天，行程安排，我們僅參加四天的會議，重點參加必要之 WG，所以共參加了五個 WG 分別爲 DKIM、ECRIT、DNSEXT、EAI、DNSOP。

因所到第一日已深夜零晨，稍做整埋後，次日，正式開始一系列之 Working Group 會議，由於會議是同一時間有多個 WG 同时舉行，故我們僅選擇與中心核心之相關問題參加，故共參加了五場不同之主題。

三、考察、訪問心得

ERRIT (Emergency Context Resolution with Internet Technologies)

此 Working Group 主要探討 Internet 之緊急電話(例如 119/110) 之定址技術，如何以該緊急電話中所帶有之資訊(例如 IP、Number) 得知緊急電話之發話人之地理資訊，尤於現有之 Internet 有許多狀況造成定址上的困難(例如 VPN,DHCP,Tunnel)，故造成許多發話人定址之的問題，由於此類技術的困難性及複雜度頗高，自成立 Working Group 以來雖有許多討論，但尚未形成有效之共識，故會議中每個 topic 或 slice 都有許多的 Comment。

本次會議報告在 Columbia University 舉辦的 “SDO Emergency Services Coordination Workshop” 的狀況，這個 Workshop 主要在實現目前 ECRIT 的 draft 所提出來的各種做法及問題，目前 WG 最主要的工作就是找一個能普遍爲各接受的方案。而這個 Workshop 另一個重點在於 ETSI 及 ITU-T 都參與了這個會議並提供了一些看法，並表示其亦在研究 IP Network 的緊急電話問題，個人認爲這個領域隨著 VoIP 發展會顯得愈來愈重要。

除了 Workshop 的 Issue 外，本次會議的另一個重點是 LoST (A Location-to-Service Translation Protocol) 的 Draft，其主要提到如何用 xml 來表示一些緊急情況下的必要資訊，不過一些細節可能尚需經過更多的討論，故留待 Mailing list 請有意見的人再行提出，因爲內容細節實在是多了些。

WG 另外也討論了使用 DHCP 來進行 Location Awareness，主要在 DHCP 協定在送出 options 時，加入一個關於 Location Information 的項目，並目規定了 Options 中的內容的一些意義。

另外，也有人提出在 VoIP 協議上直接在 UA (User Agent) 上寫上 Location 的資訊，因利受話端(119/110)判讀，這種方式較爲直覺而有效，不過因爲無線技術發展的關係，這個 Location 資訊需要能夠即時更新即較不能符合期望,而這個需求也需要提到相關 VoIP 協議的認可。與會的人認爲這個方法可用而直接，但可能會有他的局限。

DKIM WG (Domain Keys Identified Mail)

DKIM WG 主要在設計一套 Email 認證的方式，以減少 Spam Mail 的判讀問題，這個做法主要在 MTA 端發生，而不影響目前的 MUA，MTA 在發送信件時以自己的 Private key 對表頭 (Mail Header) 加密計算，產生一組簽章，收信的 MTA 在收到信件時，以 DNS 查詢的方式取得發送端的 sha publick key，進行還原處理，處理後與發送端的簽章進行比對是否一致。

這個做法其實和 SPF 有點類似，而 SPF 則直覺許多，DKIM 需要有簽章及驗證動作，可能會使用到較多的系統資源，對於惡意的攻擊容易形成 DOS 狀況，這是目前 DKIM 最大的缺點，而表頭處理確實能有效驗證發送者身份，只要進行 DKIM 的檢查，即可決定對進件的處理行爲是拒收或接收。

會議首先報告了 RFC 4686 的公佈，這篇 RFC 主要由 DKIM WG 所提交的，提到了 DKIM 可能面臨的一些問題，及這些問題處理的建議方法，不過也很明白的指出有些問題是一定需要面對的。

此外，與會的報告中也提到了目前 DKIM 使用 type TXT 做爲目前 DKIM 的查詢類別是不好的，因爲其他太多東西也使用到 TXT 易造成混淆，故建議使用一個新的 TYPE 來供 DKIM 使用，而新的 TYPE 就可以使用 wildcard，在日後 WG 的進程上有會更大的空間。會議上另一個報告重點則是 SPP (Signing Practices Protocol)，它是一個說明 DKIM 政策的一個補充，也就是我這個 Domain 的 DKIM 原則，是第三方 Sign 或是自己 Sing，以及什麼信件是 sign 的，感覺起來這個 Draft 目前共識仍在形成中，尚只是一個概況及做法說明，目前尚無明確的詳細的 Protocol 做法，尚有很大的發展空間。

EAI WG (Email Address Internationalization)

EAI 乃是我們此次參加最重要的任務，由於整個解決方案的架構已定，所以本次的討論主要集中在 Open issue。首先是已經在 Mailing List 上面 Last Call 的 Framework，相關的問題都不會影響到整體的架構，會議結束後會將修改過的版本再做一次 Last Call，但此次不再接受新的問題提出，只是文字與編輯上的調整，預計在明年一月之前可以送至 IESG Review。

接著則是 core document 的進度報告及問題討論，在 Extension 的部份最重要的是 extension identifier 確認爲 UTF8SMTP，還有則是在 DSN 的部份須再增加相關敘述，而在這個部份也提到了新的 Encapsulation Draft，由於 DSN 將會需要，所以將會加入 WG 的工作項目中。

而在 Header 這一篇中確定了 ALT-ADDR 的表示方式將使用”<”與”>”來做分隔 (ex: <utf8@utf8 <ascii@ascii>>)，解決了之前可能造成與 domain-literal 混淆的問題；在 UTF8 是否允許出現在 MIME header 的問題，由於在 downgrade 將會較難處理，但原則上必須要支援，才是完整的 internationalization，將會在下一版加入相關的敘述；最後 Header-Type (之前爲 UTF8SMTP) 的新 header 的存在是否必要再次被提出來討論，會議上一致認同該 header 可能會淪於與 MIME-version: 1.0 一樣被忽略的命運，因次可能會考慮移除，將會丟到 Mailing List 上面再做最後的確認。而上在我們實作 testbed 的經驗中，亦發現開發者很容易忽略該 header，直接檢查郵件是否有 UTF8 的存在，反而能讓系統比較強壯，目前這個問題還需要後續討論。

而在 downgrade 這一部分主要確定的方向是使用 header by header 轉換，其餘的討論較爲發散，而 IMAP/POP3 則是依賴 downgrade 相當多，因此目前的狀態是 pending 中。Mailing list draft 則因爲先前的作者無法繼續參與，該篇的編輯將會轉由 Randall Gellens 擔任。時程方面較先前排定的延遲了一些，整體來說時程可能會延後六個月。

DNSOP WG (DNS operation)

Domain Name System Operations WG，這個 WG 主要的工作是建立 DNS Sever 的運作的相關準則，像是 Zone File、Root Server、Resolver 等等，另外 IPv6 DNS 以及 DNSSEC 的運作相關標準，也是此一 WG 的工作項目。

首先是 RFC 4697(Observed DNS Resolution Misbehavior)的發布，主要是講到一些 DNS 常見的問題以及建議的處理方式。其他相關 draft 中 draft-huston-6to4-reverse-dns-07.txt 已送到 IESG 處理，而 draft-ietf-dnsop-serverid-07.txt、draft-ietf-dnsop-default-local-zones-00.txt 與 draft-ietf-dnsop-reflectors-are-evil-02.txt 則是在 WGLC 中，並沒有太多的問題。而在 draft-otis-spf-dos-exploit-01.txt 這篇則是分析了 SPF 對 DNS Server 造成的影響，由於 SPF 有 Redirect 的功能，而在 email 寄送的時候可能會對所有的 domain 作查詢，造成對 DNS 有 dos 的可能。另外還有 AS112、RFC2317bis 與 DNS search path 等相關的問題在討論中。

DNSEXT WG (DNS extension)

DNSEXT 主要專注於 dns extension 之發展，例如 DNS 延伸版本、DNSSEC、NOTIFY、EDNS0、TSIG、IXFR/AXFR，但目前討論的部分大多是 DNSSEC 的範圍。首先是 WG 的狀態報告，已經發布爲 RFC 的標準有 RFC4471 (Derivation of DNS Name Predecessor and Successor)、RFC4592 (Wildcard Clarify)、RFC4635 (HMAC SHA TSIG algorithm Identifiers) 和

RFC4701(DHCID)，而 MDNS 則是在 RFC Editor queue。而其他大多爲 DNSSEC 相關的 draft，關，在這邊則不多作介紹。與中心比較相關的則是在 DNAME(RFC2672bis)部份的討論，提到了目前 DNAME 在許多相關的 RFC 中並沒有做對應的修改，及 Wildcard DNAME 不可使用，NS、MX 與 DNAME 之間相互的關係，還有 CIDR 的反解部分及 IPv6 等等問題，可以作爲中心推動 IPv6 時應該要注意的項目。除此之外，還有一些新的 draft 被討論，包刮有 draft-eastlake-dnsext-cookies 、 draft-stjohns-dnssec-sigonly 、 draft-austein-dnsext-relax-gratuitous-tsig 和 draft-hubert-dns-anti-spoofing，而其中較有趣的有 DNS Cookie，提出了一個新的概念，讓 resolver 和 DNS server 在 DNS packet 中放入一些訊息，可以達到簡單的認證機制，不用用到肥大的 TSIG。

四、建議意見

1. 建議持續追蹤 EAI 發展，並配合相關標準的修改建置測試系統，以利後續開發及討論的參考。
2. Domain Key 的架構並不能有效阻擋 SPAM，但可以知道這個信件即是這個 Domain 發出的。
3. ECRIT WG 目前討論的仍有很大的空間，只是做法及方案太多，感覺起來稍複雜。
4. DNSOP 與 DNSEXT 與中心核心業務直接相關，建議持續關注。

五、其他相關事項或資料

有關第六十七次 IETF 會議議程及相關會議資料請參考(Agenda/ Session/ Presentations)：

http://www.ietf.org/meetings/IETF-67.html