行政院所屬機關因公出國人員報告書
（出國類別：考察）

「考察日本 VPN(Virtual Private Network)發展現況」
考察報告書

服務機關：行政院國家科學委員會
科學技術資料中心

出國人姓名職稱：林子超先生　助理系統分析師
黃百立先生　程式設計師

出國地點：　日本
出國期間：　民國八十九年十二月十日至十二月十六日

行政院研考會省（市）研考會編號欄

重要活動日程

日期	考察機構
89/12/10	台北→東京
89/12/11	株式会社 InfoCOM 新横濱本社 (NISSHO IWAI INFOCOM Corporation)
89/12/12	株式会社 富士通 (FUJITSU LIMITED) 研究所
89/12/13	株式会社 日立製作所 (HITATCHI LIMITED)
89/12/14	株式会社 PFU (PFU LIMITED) 東京本社 株式会社 INES (NIES Corporation) 東京本社
89/12/15	科学技術振興事業団 開發部 (Japan Science and Technology Corporation (JST))
89/12/16	東京→台北

摘　　要

為瞭解日本虛擬私人網路 VPN(Virtual Private Network)技術在日本國內研發與應用（包括遠距存取、即時加解密、B2B、B2C..等）及網路安全政策之發展現況，本中心特派林子超及黃百立倆位同仁，於民國八十九年十二月十日至十二月十六日赴日本 InfoCOM Corporation 等公司訪問考察。參訪單位及內容分述如下：

1. 株式会社 InfoCOM 新横濱本社(NISSHO IWAI INFOCOM Corporation)：位於新横濱的 INFOCOM 總公司，將網路安全及資訊保護列為公司營運的首要條件之一；為此該公司除了加強建築物的耐震強度及備援電源系統外，另有二十四小時全年無休之網路安全等部門，以利掌握網路狀況。

2. 株式会社 富士通 (FUJITSU LIMITED)：隸屬於富士通集團的富士通研究所，主要負責產品研究及開發；其於商品開發所投入之人力及物力或是理念之堅持，令人印象深刻。

3. 株式会社 日立製作所 (HITATCHI LIMITED)：日立製作所開發之 VPN 商品，有別於傳統之身份認証機制，而改採傳統機制+IC 晶片+終端軟體之 VPN 安全機制，以降低遭受冒用之風險。除了商品之探究外，另提供日立製作所針對網路安全衝擊所擬訂之網路安全政策。

4. 株式会社 PFU (PFU LIMITED) 東京本社：PFU 公司主要在於提供中小企業低成本之 VPN 設備，對於網路安全及 VPN 之使用有著與眾不同之規劃策略。

5. 株式会社 INES (NIES Corporation) 東京本社：INES 公司所開發之 VPN 技術，相當令人矚目，原因在於其所開發之與 IP sec 相容之「光干涉暗號 (WLIC)」加解密運作模式，其除速度較 DES 加解密運作模式快上四倍以上外，編碼位元數更為 DES 之兩倍，也就是 128 位元。

6. 科学技術振興事業団 開發部(Japan Science and Technology Corporation (JST))：定位近似國科會科學技術資料中心的 JST，其主要扮演著國家型網路計畫及政策擬訂之評估與分析。

本報告除簡介各參訪公司及機構所扮演之角色與功能外，並敘述其發展現況。最後就發展現況提出心得與建議，俾提供國內各界參考。

目　　次

壹、 目的

本計畫之考察目的，主要在瞭解日本虛擬私人網路 VPN(Virtual Private Network)技術在日本國內研發與應用（包括遠距存取、即時加解密、B2B、B2C..等）及網路安全政策之發展現況。

貳、 過程及內容

本項考察期間自民國 89 年 12 月 10 日至 89 年 12 月 16 日止共 7 天。透過 JST 及東亞協會安排為期七天之考察活動，期間分別參訪 NISSHO IWAI INFOCOM(InfoCOM)、富士通株式會社、日立製作所、PFU 東京本社、INES 東京本社、JST 開發部等機構。

一、 株式会社 InfoCOM 新横濱本社

http://www.infocom.co.jp

內容：InfoCOM 公司主要之業務為提供與網路相關之軟硬體設備及商業訊息之傳遞與新聞發佈，由於新聞業務首重真實性，因此 InfoCOM 將網路安全設定為公司營運之首要條件之一。有鑑於此，該公司之軟硬體設備均以確保資料安全為基礎設計理念。

硬體設備方面：除了本身之建築物採取了可耐震八級以上之防震結構外，電力供應系統亦有分別隸屬於不同電力公司之電力系統，並外加發電機組及不斷電統。

軟體方面：分佈於全球各地之分公司及服務據點均以 VPN 與新橫濱本社互相連接，並設立了二十四小時全年無休之網路安全監控及客

服中心等部門，以求資訊安全及服務品質。

二、 株式会社 富士通 (FUJITSU Ltd.)

http://www.fujitsu.co.jp

內容：此次參觀之富士通研究所之人機介面實驗室，主要之業務為研究及開發新的電腦應用商品，或是人對於電腦應用之理念及想法予以實現；由其展示之作品不難看出，其為了實現以人為本之設計理念，所投入之心力與成本，令人印象深刻。

三、 株式会社 日立製作所(HITATCHI Ltd.)

http://www.hitachi.co.jp

內容：日立製作所對於 VPN 之網路安全機制及政策訂定相謹慎，特別是對於使用者之身份辯識及使用者不可否認性，採用了多重認証機制。

所謂之身份多重認証機制，包括了帳號、密碼、終端軟體及日立公司開發身份辯識專屬之 IC 晶片，由於 IC 晶片複製不易；因此經過此機制認証過後之 B2B 或是 B2C 等網路商業行為，將具有相當程度的不可否認性，此舉將能有效提升使用者對於網路安全之信賴，及消除使用者害怕身份遭人冒用之恐懼。

值得注意的是，日立公司投入的相當程度的成本於網路安全政策的訂定，原因在於透過網路安全政策的訂定，才是落實網路安全的最

佳方法，此外透過安全政策訂定之推演，亦有助於實體網路安全線路之規劃及最佳化。

附帶提及的是：完整的網路安全規劃，尚須要相關配套之法令來約束，其整體效益才能完全的彰顯出來。

四、 株式会社 PFU (PFU Ltd.) 東京本社

http://www.pfu.co.jp

內容：PFU 公司由別於日立製作對於 VPN 之網路安全機制及政策訂定思維，特別是對於中小型企業、個人工作室或一般家庭之使用者之 VPN 網路規劃，採用基礎網路安全之認証機制與行銷策略。

所謂基礎網路安全之認証機制與行銷策略，基本理念其實就是將網路安全之觀念予以推廣，並深植於每一位網路使用者；因為 PFU 深信，網路是集合式或分散式的使用架構，也就是說：單方向的網路安全機制是不夠的，網路安全應該是全面性的推廣施行才有意義，因為其將行銷策略定位在成本低廉的 VPN 設備上。儘管成本較低，但這並不意味著其 VPN 網路安全就會相對的打折，相反的，透過低成本 VPN 網路安全設備的普及，卻很有可能帶來最大的安全效益。

五、 株式会社 INES (NIES Corporation)東京本社

http://www.ines.co.jp

內容：有別於其他的發展 VPN 軟硬體設備公司，INES 公司選擇了軟硬體設備外的第三種選擇，也就是 VPN 網路之加解密演算法。

所有的 VPN 網路都會有加解密的過程，但是傳統常用的 56 位元之 DES 加解密演算法，隨著硬體設備的創新與性能的提升，遭第三者成功解密的可能性將愈來愈高。根本的解決之道就是提高加解密演算法的位元數。但是高的加解密演算法位元數，雖然可以增加第三者解密所需之時間，但是同時亦將會增加使用者之使用時間，因此如何在兩者間取得一個平衡點，將是一大難題。

而 INES 公司所研發之與 IP sec 相容之「光干涉暗號(WLIC)」加解密運作模式，似乎為此難題找到了些許解答。

在同以 30MB 的資料量，分別以 DES 及 WLIC 加解密演算法測量其作業速度，最後求得之時間分別為：DES 加解密演算法 45 秒、WLIC 加解密演算法則只有 10 秒，而且其加解密之速度亦不會因為檔案變大而變慢，相當特殊。

深入瞭解「光干涉暗號(WLIC)」加解密運作模式後發現，其處理速度不會因為檔案大小而變化的原因為：其採用了串流技術(stream)並且成功的應用於加解密運作模式。

「光干涉暗號(WLIC)」加解密運作模式，其有著兩倍於 DES 加解密演算法之 128 位元加解密演算法，加解密之運作速度，在同樣的設備環境下，亦快於 DES 加解密演算法四倍以上，且相容於 IP SEC 之標準，更有著 Stream 功能，如果此產品順利推廣於網路安全之應用上，將會為需要 stream 技術之多媒體網路安全帶來革命性的影響。

六、 科学技術振興事業団 開發部

(Japan Science and Technology Corporation (JST))

http://www.jst.go.jp

內容：於日本定位近似國科會科學技術資料中心的科学技術振興事業団，其主要的業務為：

一、 科學技術情報的流通

二、 科學技術的基礎研究

三、 優良的研究成果之技術轉移

四、 產官學研及海外研究領域之研究交流

五、 國家實驗及研究機構之研究支援

六、 國民之科學技術之推廣與體驗

由於 JST 主要任務包括科學技術情報的流通及國家實驗及研究機構之研究支援等業務，因此建構類似全國性網路安全機制等國家型計畫時，其始終積極的扮演著幕僚及協調的角色，值得借鏡。

參、心得

一.對日本企業界或網路服務公司而言，虛擬私人網路 VPN(Virtual Private Network)之技術早已落實於網路安全架構上，雖然以現行之技術與成本尚無法完全滿足使用者對於 VPN 之期許，故多數的公司最終仍會因受到經費或是安全政策的考量，及業務需求或資訊流通與交換等主客觀因素，而選擇截然不同的 VPN 方案，如此一來將使得多樣化之 VPN 網路服務配套措施更為殷切。

二.虛擬私人網路 VPN(Virtual Private Network)技術或產品之優劣除在於安全功能是否完整外，資料加解密之技術與速度、產品之操作與維護成本等亦相當重要。但除了上述幾項評估要點外，最重要的還是在於 VPN 產品的連結相容性；到目前為止，在實際的應用上，不同廠牌的 VPN 產品仍常會有連結上無法完全相容的問題，但未來的 VPN 產品則均會以 IETF 所公佈的 IPsec 協定為標準，來作為彼此資料加解密、傳輸的依據。

三.在 VPN 技術快速成長及資訊網路全球化擴展影響下，將使得提供數據專線承租服務之 ISP 業者遭受到前所未有之衝擊，同時也宣告了無國界競爭時代的來臨；目前國內 VPN 設備多數均依靠國外進口，因此對於本土化 VPN 網路基礎架構技術之研發、網路服務技術之研發等，仍有相當的成長空間。本團於日本 InfoCOM 等公司實地考察七天，對日本民間企業在 VPN 及先端加解密技術之開發與應用方面之努力倍感欽佩，值得我們的借鏡。

四.隨著網際網路及網路安全之快速成長，日本企業對企業(B to B)使用電子資料交換之營業額也跟著快速的成長，從 1998 的 9 兆日元迅速的增加至 2000 之 19 兆日元，成長了約 110%，究其主要原因在於 B to B 能有效將低事務成本，一般企業僅需利用現有之公眾網路，外加相當程度的

網路安全設備即可輕易達成；且日本政府對於經過網路安全設備認證過後之相關商業行為，亦訂定有相關之配套法律來約束與保障，此舉將對於提升網路商業之普及，有相當大之助益。

五.因應多媒體時代的來臨，INES 在虛擬私人網路 VPN(Virtual Private Network)之研究中之加解密架構，有別於以往採取區塊為單位之方式，而改採用 Stream 為基礎之加解密方式。以 Stream 取代傳統 Block，則加解密資料之提供型態將更為廣泛(包括文字、語音、影像...等，或影像擴展至影片)；以逐步達成由文字傳送之應用轉型為語音、影像及影片等大量資料之 VPN 應用。

四、檢討與建議

一.由於網際網路之電子商務應用已然蔚為風潮，但攸關電子商務成敗之網路安全設備及配套之律法卻才剛起步；因此與電子商務有關之機構及企業，除可加強投注人力於此相關技術領域之研討及文獻蒐集外，同時亦須強化同仁對於網路安全之的認知，並儘速辦理網路安全相關資訊之彙整，積極進行相關配套律法及政策之制訂及建言，期能應付將來社會大眾對於電子商務交易頻繁後，所衍生之相關問題。

二.有關 VPN 等網路安全課題，應加強對使用者之觀念宣導及互動並朝以下方向努力：

1.對於尚未有 VPN 等相關網路安全設備之電子商務業者與準業者，應確實落網路安全宣導，務必使其清楚瞭解，電子商務推行之成敗，關鍵在於各階層之使用者之網路交易過程均受到適當的保障,且此舉將有助營造國家電子商務之大環境，而民眾對於電子商務則將不再怯步。

2.對於已據備 VPN 等相關軟硬體設備之電子商務業者，將可透過跨部會組成之專案編組，與現行之電子商務業者就應用、執行、法律等層面進行座談,以解決目前因網路交易無國界所衍生之多重前所未有之法律問題，並可藉機修正國家電信基礎建設之方向。主動替業者解決環境障礙並提供相關資訊之諮詢，使有心之業者有跡可循，此舉將有效提升電子商務之普及。

三.國內有許多資訊科學領域有相關之電子期刊、館藏圖書及資料庫..等引進及系統開發之政府機構及公司，向來致力於國內外科技新知之整合與提供，若能將目前急迫且未來勢必成為主流之電子商務、網路安全等相關議題加強導入於現有之資訊蒐集範疇之中，則此舉一方面可以滿足民眾

對於電子商務或網路安全等相關訊息之需求，另一方面亦可將資料彙集整理，並予以加值分析，可謂一舉數得。現正值商務電子化萌芽之際，建議除引用電子商務與網路安全相關研究人員外，積極加強推廣網路安全觀念亦是當務之急。

四.日本在網路安全議題向來相當重視，因此相關領域之書籍與文獻及報告甚多，若有同仁欲瞭解但無法順利閱讀者，除建議中心鼓勵同仁進修日文外，更可聘請些許日文系工讀生，加以初步解譯供同仁選讀。

五.為有效提昇國人對於網路安全觀念之認知，建議可仿效 HITACHI 公司，定期為各營運部門進行網路安全宣導及檢測，其檢測之規模遍及全球，目的除在於落實網路安全觀念外，可進一步修正公司之安全政策，值得我們借鏡。

五、結語

虛擬私人網路 VPN(Virtual Private Network)與網路安全觀念密不可分，唯有確實落實正確的網路安全觀念，才可以在公眾上享有隱私權；縱使虛擬私人網路 VPN 相關的技術一直在推陳出新，但是其為國人所帶來的相關電子商務商機及機制卻才剛萌芽。

原因在於成功的電子商務，有許多的環節相扣缺一不可；但國人仍習慣著眼於較高利益之環節，因而缺乏基礎環節之涵養。反觀日本，以對於虛擬私人網路 VPN(Virtual Private Network)之發展為例，由於各環節均有人力投入，所以才使其得以營造完整的電子商務環境，此精神值得國人深思。