行政院所屬各機關因公出國人員出國報告書

(出國類別：考察)

網際網路安全管理

(Internet Security and Network Management)

服務機關：財稅資料中心

出　國　人　職　　稱：設計師

姓　　名：蔡芝玉

出國地區：美國

出國期間：八十九年九月二十三日至十月二十二日

報告日期：八十九年元月三十一日

摘　要

本次赴美參訪目的在於蒐集美國各大型電腦公司、企業及政府機構、銀行等在網際網路上的成功發展經驗，尤其是網路的監控、安全管理等最新技術。此外，出國前夕奉　主任秘書指示，順便注意一下國外機關在整合 Intranet 與 Internet 方面如何進行其安全管理。

除此，基於本身負責財政部的網際網路應用規劃及 Intranet 辦公室自動化應用系統整合規劃，因此在參訪行程內容安排不但包括了現行財政部網際網路發展的應用需求，另外也為財稅資料中心八十九年度重要工作之一—五區國稅平台移轉計畫蒐集有關 Internet 與 Intranet 整合相關技術資料。

承蒙美國農業部研究訓練中心(Graduate School, USDA) Ms. Karmen Baretich 的積極聯繫，參訪對象除政府機關資訊中心主管、銀行機構資訊是安管人員、大學電算中心系統管理人員外，還安排了民間網際網路應用軟體開發公司主管及整體規劃顧問公司負責人、技術顧問等資訊專業人士。其中最難得可貴的是有幸參加在喬治亞州亞特蘭大舉行的公元兩千年資訊大展(NetWorld +Interop2000)及拜訪“美國東岸矽谷”—北卡羅來州萊禮的 Research Triangle Park。

由於拜訪行程緊湊且對象層級偏高，為方便對方預先準備妥相關資訊，行前皆委請美國農業部研究訓練中心或當地國際訪客諮詢委員會(Council for International Visitors)先傳真拜訪主題與預定請教問題概要包括：

一、 隨著網際網路應用的普及，要注意哪些安全控管？

二、 如何訂定網際網路安全機制(policy)？遇有衝突時，如何解決？

三、 系統管理人員須具備哪些專業技能？如何培訓？

四、 機密性資料傳輸的安全如何確保？有哪些技術？架構為何？

五、 Internet 與 Intranet 如何整合？

六、 Internet 應用開發最新發展與技術新知。

七、 目前美國網際網路軟體開發工具主流為何？主機平台應選擇 NT、UNIX 或 Linux？

目　錄

壹、目　的

本次出國參訪主題是「網際網路安全與管理」，在主題選定上，主要是考慮到：

一、網際網路已普及，尤其現階段中央政府機關正積極推廣電子化政府，以提升便民服務效能。

二、資訊交流愈來愈偏重網路的傳遞，以加速交換與流通速率。

三、網路的透通性主流即為網際網路，但過度開放必導致安全性降低。

四、資訊的交流互通不能有資料流失、竄改錯誤發生。

五、應用系統的開發技術已從早先集中式主機管理，改向主從二層架構，進而發展為 web-based 三層架構，以因應網際網路線上同步作業需要。

六、機關內部區域網路(LAN)通訊協定已從早期 Novell IPX、IBM NetBIOS 改為 TCP/IP，進而應用規劃也趨向結合網際網路技術，發展 Intranet 群組應用系統。

七、Intranet 適用於機關內部，Internet 主則對外通訊，但對終端使用

者(client users)而言，應整合二者以便利業務執行。

八、網際網路駭客侵犯手段越來越高段且無孔不入，如何做好事先預防勝於事後補救。

由於主題牽涉網路、通訊、安全管理及應用規劃，涵蓋了主機作業系統、資料庫管理系統及開發軟體工具，此外由於財政部、財稅資料中心業務特殊，不論所屬機關規模或資料處理性質與數量，皆較一般企業或政府機關複雜，因此在考察地點、對象及拜訪人員方面，企需具備實質類似豐富經驗或主管整體計畫規劃者。參訪機關及電腦公司包括：(有關詳細行程請參閱附錄一)

一、政府機關：

(一)亞特蘭大 Fulton 郡稅務局---稅務系統在網際網路上的應用發展。

(二)Charlotte-Mecklenburg 郡政府--- Charlotte-Mecklenburg 郡政府的網際網路安全控管建置及其他安管方案。

(三)北卡萊禮 Research Triangle 基金會---Research Triange Park 科技研究發展現況。

(四)北卡萊禮 Research Triangle 協會---網際網路資訊科技發展現

況。

(五)北卡萊禮市政府資訊中心---北卡萊里市政府的網際網路安全控管建置。

二、學術機關：

(一)史丹福大學 Silicon Valley World Internet Center---富士通公司在網際網路上的發展。

(二)北卡羅萊州州立大學---校園內資訊管理、系統安全監控、網際網路安全機制、網路架構。

(三)杜克大學---校園內資訊管理、系統安全監控、網際網路安全機制、網路架構。

三、銀行機構：

(一)聯邦準備銀行 Richmond 分行---聯邦準備銀行的網際網路安全控管建置。

(二)第一聯邦國家銀行---第一聯邦國家銀行的網際網路安全控管建置。

四、網際網路軟體開發公司：

(一)WebPro 網際網路公司---網際網路開發最新工具、系統安全注意事項。

(二)WebWide 資訊系統公司---網際網路開發最新工具、人員技能培訓。

(三)WebslingerZ 公司---網際網路開發最新工具、人員技能培訓。

五、整體規劃／諮詢顧問公司：

(一) 國際商業機器股份有限公司(IBM)---網際網路安全管理與架構。

(二) Organic 公司---網際網路上分散式資料庫的同步控制與回復、穩定性高的主機選擇。

(三) William Ives 顧問公司---Intranet 與 Internet 整合可行方案。

(四) @stake 公司---各種數位安全服務系統、網際網路安全注意事項。

貳、過　程

為期一個月的研習行程按性質分為前、後二段：前段(第一週)主要參加公元二千年亞特蘭大 NetWorld+Interop2000 資訊展暨研討會 Seminars/Workshops 活動；後段(第二至四週)則是拜訪由美國農業部研究訓練中心或當地國際訪客諮詢委員會(Council for International Visitors)所預先安排之政府機關資訊單位、學術機關、銀行機構、網際網路軟體開發公司、整體規劃／諮詢顧問公司等，平均每日至少一至二個約會，每次約談約二至三小時。

整個拜訪行程地點包括了美國西岸之舊金山及史丹佛大學、東南部的喬治亞州商業中心—亞特蘭大及北卡羅萊州金融中心—夏洛特(Charlotte)、研究發展中心—萊禮(Raleigh)，其中北卡羅萊州的萊禮已逐漸發展為美國東岸的矽谷，最主要原因在於美國幾個高科技大廠包括 IBM、Cisco、Nortel 等都已將其研發中心遷移至此，並且和當地美國排名前十大名校—杜克(Duke)大學及北卡羅萊州州立大學(North Carolina State University)合作發展研究計畫。

由於安排參訪對象實屬機會難得，為把握有限時間蒐集足夠資訊，行程前皆儘量先電請當地國際訪客諮詢委員會之安排人員(program coordinator)傳真所欲研討問題內容及相關主題給拜訪公

司，俾利對方準備妥相關參考資料。另外，自己則儘量抽空至當地市立圖書館、學校圖書館或當地國際訪客諮詢委員會辦公室借用個人電腦，上網閱覽拜訪公司之基本資料及公司服務內容，以利個人更了解對方，同時充實自己與拜訪公司的對話內容。

在研討內容準備方面，主要考量自己現行負責工作—財政部網際網路與內部網際網路 OA 應用系統規劃及整體網路邏輯架構規劃，另外還包括了系統管理人員所需安全管理、防火牆安全機制訂定以及主任秘書臨時交辦之五區國稅平台移植後 Internet 與 Intranet 整合可行方案。綜合上述需求，個人研提了幾點問題列敘如下：

一、 網際網路應用的普及，要注意哪些安全控管？

二、 如何訂定網際網路安全機制(policy)？遇有衝突時，如何解決？

三、 系統管理人員須具備哪些專業技能？如何培訓？

四、 機密性資料傳輸的安全如何確保？有哪些技術？架構為何？

五、 Internet 與 Intranet 如何整合？

六、 Internet 應用開發最新發展與技術新知。

七、 目前美國網際網路軟體開發工具主流為何？主機平台應選擇

NT、UNIX 或 Linux？

另外，在參加 NetWorld+Interop2000 資訊展時，也同時選擇了幾個相關研習主題 Seminars/Workshops 聽講：

一、 VPN Day。

二、 Computer Attacks: Trends and Countermeasuresm。

三、 Network Security: Practical Approaches from the Front Lines。

四、 Deployed and Emerging Security Systems for the Internet。

參、重要心得

以下僅就前述研討問題所蒐集得資料彙整摘述如下：

問題一：隨著際網路應用的普及，要注意哪些安全控管？

說　明：政府機關為便利民眾辦理各項業務申辦例如報稅、繳納展延等事項，已陸續在網際網路上開發全球資訊服務網(World Wide Web)、網路報繳稅、人民申請案件申請受理等應用系統，惟開放後常遭受網路駭客或惡意人士破壞伺服主機，致無法正常提供服務。

方　法：重要觀念『安全是不可妥協』。開放便民措施是善良理念，但為維持作業的正常運作，安全必須嚴格管控，手段包括資料的加密、電子簽章、資料亂碼處理以妨害克截取或竄改資料；使用身分認證以確保資料來源與目的無誤；建置虛擬私人網路(VPN)確保傳輸過程安全；加裝防火牆以多重監管外來者進入等。

問題二：如何訂定網際網路安全機制(policy)？遇有衝突時，如何解決？

說　明：現行政府機關在網際網路上開發應用如 WWW、線上申辦等

服務主要目的皆為便民，但〝方便〞民眾則表示限制越少越好，相反地對政府機關系統管理維護人員而言，卻是惡夢的開始，因為安全漏洞太多，駭客入侵太容易！

方　法：安全管制的鬆緊尺度宜參考應用系統的資料使用及對象來分別訂定管制標準，且並非完全由資訊維護單位負責制定，而是應該由系統的需求提出單位會同資訊部門共同商定，如果有高階首長主持參與，將更有利機制訂定後的強制執行，同時當需求與管理雙方出現意見衝突時，高階首長正可發揮仲裁的角色功能。以美國杜克大學為例，資訊中心(OIT)負責全校網路安全控管，教授、學生會、教職員提出需求時，由 OIT 初審再送校務委員會複審通過後據以執行。

問題三：系統管理人員須具備哪些專業技能？如何培訓？

說　明：由於網路技術太專業，一般政府機關大多委外(outsourcing)辦理網路軟、硬維護，遇有問題也直接呼傳廠商解決，造成技術過度依賴，更令人憂心的是經驗技能不足影響委外需求規格訂定品質降低及內容空洞、缺乏整體規劃與具體管理概念。

方　法：委外維護目的在於輔助人力、經驗的不足及專業知識的不夠

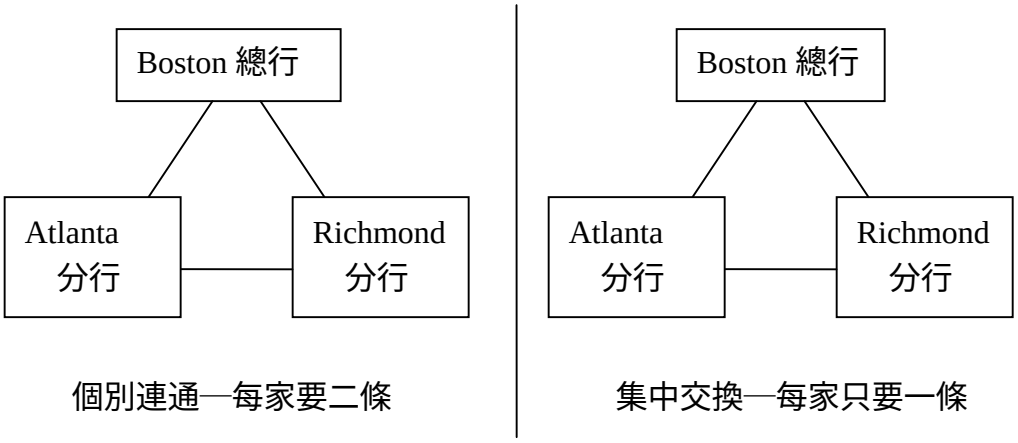
多聞, 絕不可過分依賴. 系統管理人員(system programmer;SP)職責在於“管理”而非〝維護〞，由於 SP 對機關業務需求比維護廠商更了解，才能切實針對業務需求規劃出適當的管理制度. 完整的系統管理內容則應包括系統日誌(system journal)的過濾分析、系統每日執行狀況、資源使用分析、使用者權限、危機預警與應變處理、備援與回復等。因此，SP 基本上應對負責之作業系統功能完全了解，除此系統運作之平台主機及其內執行相關軟體亦應一併了解，有助於異常狀況緊急發生時，可迅速初步辨釐問題歸屬後，再洽詢正確廠商協助解決問題。至於 SP 的培訓方法，一般多採赴外受訓或單位年長人員經驗傳授。以美國 William Ives 顧問諮詢公司為例, 公司內有二十五位工程師, 無法一一派訓, 為節省出差、受訓費用，改採聘僱微軟專業講師到公司為期一週，講授內容並非一般教材講義，而是實機操作解決問題。

問題四：機密性資料傳輸的安全如何確保？有哪些技術？架構為何？

說　明：網際網路係開放供公眾使用，因此機密性資料若不經處理直接透過網際網路傳送，則非常容易被駭客攔截。以財政部而言，遇到金融、股市緊急事故爆發，金融局或證券暨期貨管

理委員會必須即刻報告並提供相關資料供首長參考， 但此類資料必屬機密性，不得為其他人所偷看、竊取或竄改。

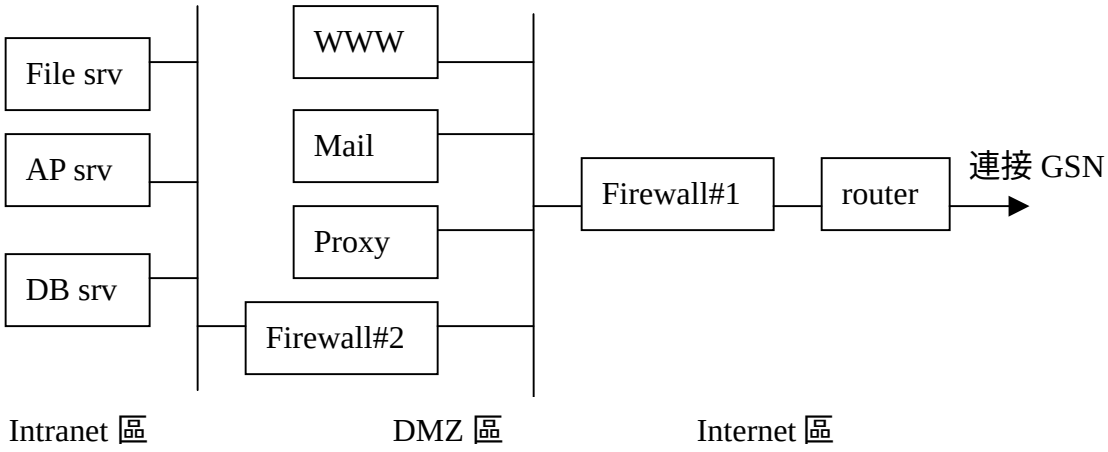
方　法：以美國聯邦銀行 Richmond 分行與其總行及其他分行互傳當日交易金額 財務報表等機密資料為例, 仍採用專線(Leased line)為最保全方法，但為減少專線的租用費用及線路架設，所有分行間的對傳皆以波士頓總行為集中交換據點，並由總行訂定交換機制及負責交換的確認工作(概念架構如下圖)。



問題五：Internet 與 Intranet 如何整合？

說　明：Internet 對外，Intranet 對內。由於內、外使用者不同，一般機關為確保內部資源設備安全，通常會採取二個網路完全分開獨立作業。但是，對於內部同仁要與外部聯繫互通時，則常要切換啟動連線程式或使用不同機器處理，造成作業上非常不方便。

方　法：以美國 IBM 研發公關主管建議採用雙重防火牆區隔內、網路(概念架構如下圖)，外部使用者透過 Internet 欲使用 WWW、Mail 時，須先通過第一道防火牆的過濾，如要再進入使用內部資源，則要再通過第二道防火牆的過濾。過濾條件則可以利用身分認證、密碼或 IP 等處理之。



問題六：Internet 應用開發最新發展與技術新知。

說　明：網際網路應用系統開發技術已從早期集中式(centralized)轉變為主從架構(Client/Server)之 fat client，目前市場開發主流則為 web-based 設計與瀏覽器(browser)介面組合之 thin client。設計方法採物件導向, 透過 ODBC 與資料庫管理系統互通擷取資料，但其撰寫仍嫌冗長、麻煩，且設計者亦須了解資料庫管理系統德處理方式。

方　法：以美國 WebPro 公司為例，頃於公元二０００年六月引進日本新開發之 OMNIS 套裝軟體，並立即使用為客戶開發新網際網路 B2B 網站，獲得很高的評價與讚賞。據該公司表示，此 OMNIS 優點/特色絕對優於當今網際網路開發主流 Java，二者功能比較如下：

(一) OMNIS 與 Java 同樣具有很高的跨平台可攜性，支援 DB2、Oracle、Informix、SQL Server、Sybase 等資料庫管理系統及 NT、UNIX 及 Linux 等作業系統。

(二) 速度方面快約八倍；費用方面僅需約八分之一；安全方面比 Java 更嚴謹。

(三) 同樣設計一個 tree list，Java 約需 10,000 行程式，OMNIS 僅需一頁程式。

(四) 同樣設計一個應用系統，Java 約需十二至十五個月，OMNIS 僅需三至四個月。

(五) OMNIS 符合物件導向設計，但 Java 沒有。

(六) 程式設計人員訓練所需時間方面，Java 至少需要三至四個月，而且還要有 C 語言基礎；OMNIS 則採用 drag-

and-drop 操作方法，不須有經驗設計人員，而且僅需一至二週即可熟練操作。

問題七：目前美國網際網路軟體開發工具主流為何？主機平台應選擇 NT、UNIX 或 Linux？

說　明：財政部現有網路主機作業系統平台有 NT、UNIX、Novell、Linux 等，群組軟體也有 Exchange 及 Notes，網際網路開發語言 ASP、Visual Basic、PHP、Delphi、Java 等。整體而言，環境內平台複雜，軟體種類眾多，不易整合、管理及維護。

方　法：目前網際網路應用市場內的確主要有二大主流：微軟的 NT/Windows2000 及開放系統 UNIX。此外，二十世紀末新興起一個評論家預估將成為二十一世紀市場的三分天下：紅帽(Red Hat)公司的 Linux。參據受訪諮詢顧問公司提供資料，目前美國主要大公司企業使用 SUN Solaris 主機(UNIX 大廠牌)以求較高穩定性及安全性，但投資成本動輒數百萬美金以上；中小企業發展 WWW 及 OA 系統則選擇小而美的微軟 NT(但目前皆已提升至 Windows2000 版)，因為容易與微軟所開發之 BackOffice 系列軟體工具整合；至於學校、研究單位則較多使用 Linux，因為原始碼(source code)公開，易於研

究、創新設計，最重要是可自網站上免費下在安裝使用。開發工具方面則受限於使用之平台相容性、可攜性，例如 UNIX 上一般使用 Java、Perl、Visual C++；NT/Windows 上使用 ASP、Visual Basic、CGI；Linux 上則工具更少，目前僅有 C++、PHP、Java 等。

肆、結論與建議

此次研習時間為期一個月，較一般出國考察時間長，因此能有較充足的時間與更多電腦公司進行意見交流及資料蒐集，整體而言收獲確實很多，尤其是一般透過個人聯繫很難安排到的政府機關、銀行及學校。所蒐集到的資料與實用經驗，對個人或現任職務執行皆非常有幫助。

綜合前章所述重要心得，個人歸納出以下幾點結論與建議：

一、作業系統方面

UNIX 投資成本昂貴但是穩定性高，適合 critical mission 及 mass production 作業；微軟 Windows2000 對 client 端使用者親合性高、易學習、操作；Linux 的原始碼太公開、易取得，造成其安全性被懷疑，美國不少公司都已退卻、暫緩使用。以財政部現行狀況，若要選擇作業環境之桌面整合，以微軟 Windows2000 較適合。

二、稽核系統方面

主要搭配系統管理建立稽核系統，以協助檢核管理有否漏洞或缺失待加強改進。建議使用專業稽核軟體，並請教廠商協助修改

(customization)，以適用個別機關環境特別需要。

三、 使用者端介面整合方面

二層式 fat client 主從架構已不適用，宜調整為 client/AP server(or middleware)/DB server 三層式主從架構或 web-based+瀏覽器之 thin client 方式，以簡化 client 端作業環境，對 AP 開發人員而言僅需維護主機內應用程式乙套即可。

四、 五區局 Internet 與 Intranet 整合可行案方面

有關五區局 Internet 與 Intranet 整合透通後，其資料機密、安全性可採專線(leased line)、Frame Relay(虛擬分封線路)、Extranet(VPN)、SSL(Secure Socket Layer)、IPSEC(IP Security)、PGP(Pretty Good Privacy)等方法加以處理。

五、 網際網路應用開發工具方面

除傳統 3GL 的程式語言設計外，可考慮購買由 thiry party 所開發之套裝軟體例如 OMNIS，更易開發、易維護、低成本、縮短訓練時間，但是唯一較大缺點是產品為專屬(proprietary)，功能更新、價格易受開發廠商牽制。

上述心得部分除已於歸國後項主管口頭報告過，另外也蒙主管支持，已將 Windows2000 及 VPN 列入財政部財稅資料中心駐部資訊作業小組九十年度重要工作計畫，並將成立專案小組專案研究。

伍、參考資料

一、各受訪公司之產品目錄、網站資訊及研討紀錄。

二、NetWorld+Interop 資訊展參展產品目錄。

三、NetWorld+Interop Workshop 講義包括：

(一)VPN Day。

(二)Computer Attacks: Trends and Countermeasuresm。

(三)Network Security: Practical Approaches from the Front Lines。

(四)Deployed and Emerging Security Systems for the Internet。

四、NetWorld+Interop General Conference Notes。

五、財政部 Internet 及 Intranet 整體網路架構圖。

六、財政部稅資料中心五區國稅局平台移植計畫。

七、 網路資訊雜誌。