行政院所屬各機關因公出國人員出國報告書

（出國類別：其他）

駐外科技組
資訊服務重整及資安檢測計畫
結案報告

服務機關：行政院國科會

姓名職稱：董湘興高級分析師

出國地點：越南河內

出國期間：100/10/16 至 100/10/23

報告日期：100 年

目　　錄

壹、 考察目的

一、 考察緣起

行政院於民 90 年正式設立「國家資通安全會報」，肩負起政府資通安全防護工作的推動，並要求各政府機關落實執行資安防護工作，尤其對國家外交最前線之各駐外單位提出嚴格資安要求，並指派由國安局定期派員稽核。為因應是項作業，本會資訊小組(以下簡稱本小組)除平常協助各駐外科技組各項資訊業務外，另特別安排於 94~96 年分別派員前往歐洲、亞澳及美加地區駐外科技組實地協助網路建置、資通安全檢核維護、教育訓練等，成效頗為良好。

近接駐美國代表處科技組及駐越南代表處科技組等分別來函，請本小組派員協助重整現行資訊網路架構及相關服務。由於該二個科技組當年係獨立建置其資訊網路架構，並未納入駐地代表處網路架構內，但因近年來資安技術需求日新月異，科技組受限於資訊專業技術人力不足，無法即時調整更新，故亟需本會協助。

因應上述二科技組之需求，本小組已簽奉核可辦理「駐外科技組資訊服務重整及資安檢測計畫」，其工作內容除事前針對科技組作資料之蒐集、分析、模擬外，並需派員赴二科技組駐地進行網路/資訊設備重整、應用系統安裝、資安調整設定、掃毒等工作。

二、 考察行程

日　　期	說　　明
100/10/16 (星期日)	台北 → 越南河內
100/10/17 (星期一)	駐越南科技組工作。
100/10/18 (星期二)	駐越南科技組工作。
100/10/19 (星期三)	駐越南科技組工作。
100/10/20 (星期四)	駐越南科技組工作。
100/10/21 (星期五)	駐越南科技組工作。
100/10/22 (星期六)	假日
100/10/23 (星期日)	越南河內→ 台北

三、 參與人員

- 董湘興(國科會資訊小組高級分析師)
- 周方俊(承商系統管理師)
- 蔡介元(承商系統管理師)

貳、 考察內容

一、 作業程序

(一) 建置維護資訊安全網路架構

1. 個人電腦
   - 解決應用系統問題、及重整補強作業系統
   - 協助更新作業系統修補程式
   - 協助更新 Office 修補程式
   - 協助更新套裝軟體修補程式
   - 安裝常用基本之應用軟體(必須有版權)
   - 經過各項資訊安全掃描確認無任何問題後
   - 製作回復光碟
2. 依外交部資訊安全稽核表，協助檢查資安相關設定。
3. 資訊安全維護
4. 弱點掃描(確認網路及電腦待修補的漏洞)
   - 掃瞄網路，了解科技組現有網路的弱點與漏洞。
5. 建立防護機制（安裝修補程式）
   - 針對各項弱點與漏洞進行修補程式安裝。
6. 掃描與刪除
   - 病毒
   - 手動掃除病毒。
   - 重新設定防毒軟體與排程更新病毒碼與掃描。
   - 惡意程式(後門程式、間諜程式)
   - 透過 3~4 種掃描軟體交錯掃描。
   - 無法辨識的可疑檔案或 log 送回資訊小組進行後續分

析。

- 重新掃描(確認網路及電腦的漏洞已修補完畢)

(二) 資訊安全例行工作

- 更新修補程式
- 更新病毒碼
- 主動掃描後門等惡意程式
- 搜集 log 送回資訊小組
- 作業系統回復光碟操作。

(三) 本會各應用系統教育訓練

- 工作月報管理系統
- 經費管理系統
- 駐外科技組 Intranet 專屬網站
- 新聞剪影管理系統
- 海外學人資料庫
- 公文文書製作操作(含 word 簡易操作)
- 駐外科技組公文管理系統
- 作業系統回復光碟操作。
- 一般 Office 辦公軟體(Word、Excel、Powerpoint、Access、Outlook)

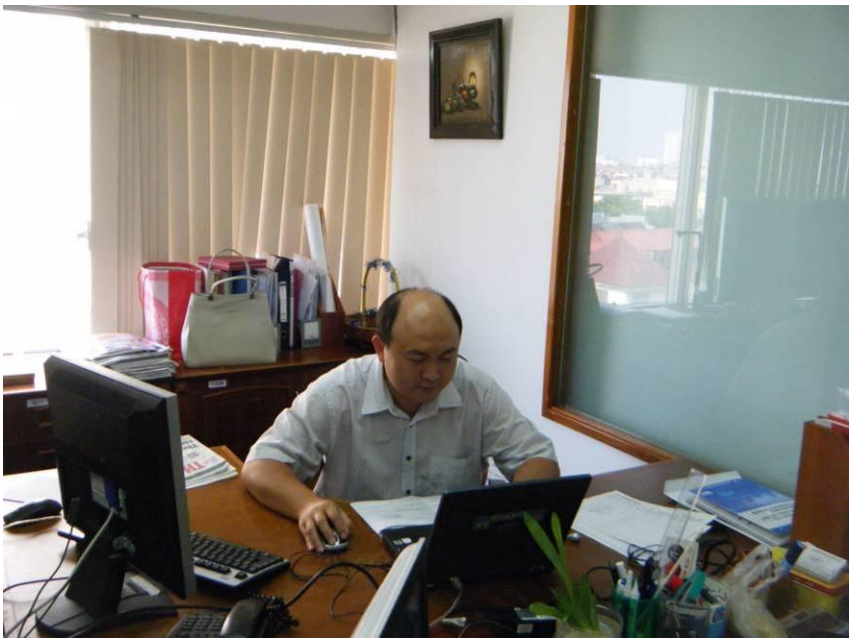
(四) 資訊安全座談會

二、 工作成果

(一) 資訊環境現況與盤點

本次實地盤點資訊相關設備，主要項目計有：個人電腦 7 台、筆記電腦 3 台(含平板電腦)、印表機 3 台等。其中個人電腦 2 台因設備老舊不進行檢修，只做資料移轉。

(二) 個人電腦、週邊設備現況與處理



- 個人電腦共 5 台未更新病毒碼，已協助更新。

  說明：主要因實體隔離平時未連上網路，所以無法更新病毒碼，現場已透過手動的方式下載病毒碼，並執行完整掃描。

- 個人電腦 5 台、筆記型電腦 3 台未更新作業系統修補程式(Hotfix)，已協助更新。

  說明：個人電腦 5 台因實體隔離平時未連上網路，所以無法更新病毒碼，現場已透過手動的方式下載病毒碼，並執行完整掃描。

  筆記型電腦 3 台因為作業系統預設自動安裝的時間設定為 AM3:00，但該時段並非辦公時間電腦並不會開機，所以普遍未安裝修補程式。

  處理方式：先手動安裝全部的修補程式 hotfix 後，設定自動更新時間於每週四中午 12 點。

- 發現個人電腦 4 台、筆記型電腦 2 台都未設定密碼。

  說明：已於資訊安全座談會中，特別說明密碼的使用規則、如何建立強建的密碼、密碼的更換週期，以及妥善保存個人密碼的方式。

- 完成個人電腦 3 台汰舊換新。

說明：已由國內攜帶之三台新電腦進行更換。

- 完成 5 台離線共用行事曆軟體安裝。

說明：安裝免費的 Rainlendar-Lite-2.9-32bit 行事曆軟體。

- 完成 4 台辦公室系統軟體安裝

說明：組長與僱員的電腦各安裝一套 ABBYY PDF Transformer 轉換大師 3.0 中文盒裝版。

2 位僱員的電腦各安裝一套自然輸入法 9.0 專業版。

- 完成 2 台電腦公文文書製作軟體安裝。

說明：更新組長、僱員公務電腦公文文書製作軟體(機關代碼)。

- 完成 1 台電腦駐外會計系統軟體安裝架設檔案伺服器。
- 完成登入 INTRA 憑證的更新。

說明：加強人員控管，落實資訊安全標準作業規範。

(三) 協助資訊作業環境調整，落實實體隔離政策

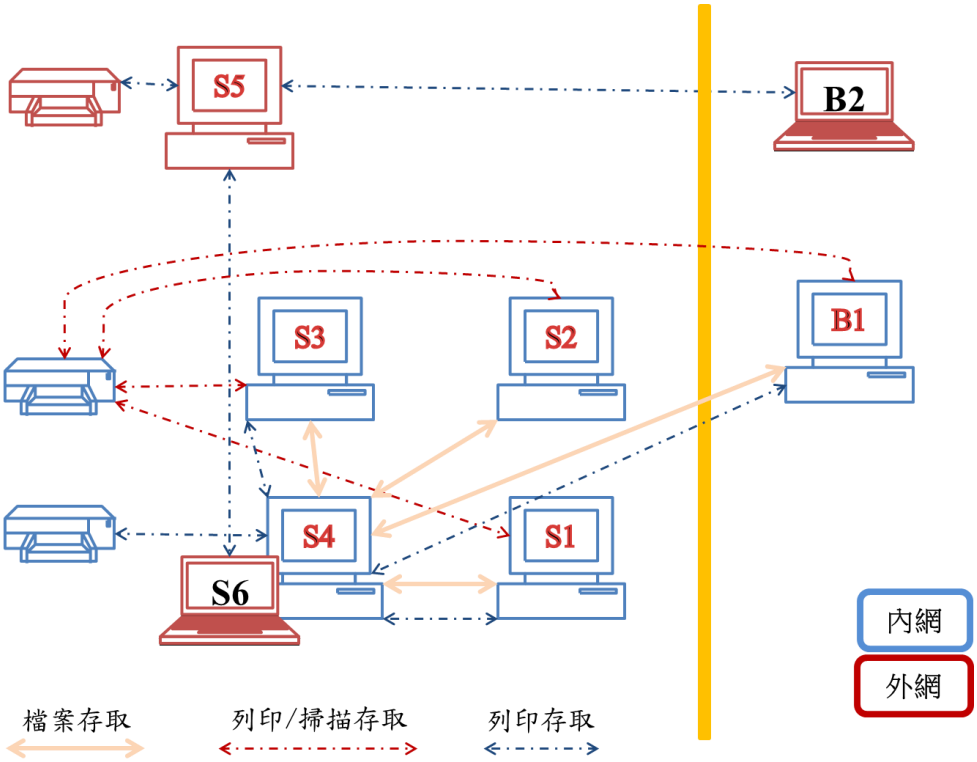
資訊作業環境透過 Hub 區分為內網及外網(詳如下圖)，各環境獨立運作，內網&外網間資料禁止也無法互通共享，若有需要，唯有透過乾淨 USB 外接碟。

內網：由 B1、S1、S2、S3、S4 等五台 PC(含 NB)形成內網，均必須輸入帳號及密碼方得登錄使用，無法連上網際網路使用，其中 S4 具備檔案伺服器及印表機伺服器功能。

- 提供各級人員(B1、S1、S2、S3)將公務相關資料集中存放，個人僅限存取自己的目錄，僅組長(或授權)得存取所有人員的目錄。
- 提供各級人員(B1、S1、S2、S3)透過網路直接分享 HP 多功能事務機等設備。

- 提供各級人員(B1、S1、S3)透過印表機伺服器，分享 CANON 印表機設備。
- 針對特定電腦提供不斷電服務。

外網：由 B2、S5、S6 等三台 PC(含 NB)形成外網，均必須輸入帳號及密碼方得登錄使用，可連上網際網路使用，若需進入國科會網站，尚需提供磁碟憑證密碼，其中 S5 兼具印表機伺服器功能，提供 B2、S5、S6 等得共享 HP 多功能事務機等設備。



(四) 完成檔案伺服器規劃建置

說明：

a. 目錄管理:採三層式架構,第一層為使用者代碼(如 hong、hue、hanh..)，第二層為年度(如 2011、2012..)，第三層細分為已完成及進行中。

b. 權限管理：個人僅限存取自己的目錄，僅組長(或授權)得存取所有人員的目錄。

c. 資料備份：作業應定期由專人進行，完成後備份硬碟須交由組長或授權人保管，及辦理異地存放，確保資料安全無虞。

d. 病毒碼更新：作業應定期由專人進行，操作方式同病毒碼更新程序。

e. 故障排除：

- ✓ 若檔案伺服器無法開啟，請檢查電源線有無鬆脫？若電源線鬆脫，請接回。
- ✓ 若檔案伺服器無法讓使用連線存取資料，請檢查網路線是否脫落？若網路線脫落，請接回。
- ✓ 若檔案伺服器當機或無法登入操作，請重新開機。
- ✓ 若重新開機仍無法登入系統，請更換備援機。

f. 備援方案：步驟如下

- ✓ 使用備援機替換故障的檔案伺服器。
- ✓ 將外接硬碟上的備份資料還原至備援機 D 槽。
- ✓ 確認防毒軟體名稱
- ✓ 透過 USB 外接碟，更新檔案伺服器的病毒碼後，請立即執行掃毒。

(五) 協助建立 PC 或 NB 系統還原機制

說明：

a. 使用時機：電腦速度變慢、異常

b. 系統還原步驟

- ✓ 請先確認作業系統類型(如 MS Windows XP、MS Windows 7)
- ✓ 進行還原
- ✓ 確認防毒軟體名稱
- ✓ 透過 USB 外接碟，更新電腦的病毒碼，完成後請立即執行掃毒。

(六) 協助建立病毒碼更新及掃毒程序

說明：每週定期由專責人員上網下載各類病毒碼，再交由個人自行更新病毒碼。上網電腦及檔案伺服器均應有專

人負責更新病毒碼。

(七) 協助撰寫駐越南科技組資安標準作業規範

說明:提供各項資訊作業相關注意事項,以及標準作業程序。

(八) 應用系統教育訓練

說明：提供簡報說明及實機操作。

(九) 資訊安全座談會

說明：提供簡報說明、經驗分享及實機操作。

(十) 其他協助工作

- 設定網路印表機功能，提供科技組同仁分享列印使用。

  說明：依科技組需求，設定網路印表機功能提供科技組列印使用，停用電腦分享列印功能，避免同仁請假電腦未開機而無法列印。

- 設定網路掃瞄器功能，提供科技組同仁分享掃瞄使用。

  說明：依科技組需求，設定網路掃瞄器功能提供科技組列印使用，避免同仁請假無法開啟電腦而無法掃瞄。

三、 改善建議

1. 因為實體隔離電腦無法上網，故發現修補程式與病毒碼無法更新。

   建議：可上網區的電腦更新修補程式與病毒碼後，再下載離線修補程式與病毒碼給實體隔離電腦更新，且應定期執行。

2. 落實帳號密碼使用規定。

   建議：已於資訊安全座談會中，特別說明密碼的使用規則、如何建立強建的密碼、密碼的更換週期，以及妥善保存個人密碼的方式。

3. 加強資料控管。

   建議：檔案伺服器已架設完成，依據『資訊安全標準作業規範』落實隨時將公務資料存放於檔案伺服器，檔案伺服器的資料每週一次備份到外接式硬碟，進行異地存放。

4. 加強資訊安全之觀念，落實資安標準作業規範。

   建議：依據『駐越南科技組資安標準作業規範』落實資訊安全相關作業。

參、 心得與建議

在瞬息萬變的國際情勢中，如何取得即時國際資訊，如何快速因應國際情勢的變化，資訊科技的有效運用實不可或缺，然而各駐外單位與國內機關在資訊環境比較上，不論在資訊人力、設備、技術等各方面均有明顯落差，為期國家外交事務推動順暢，在資訊科技運用方面，除落實資通安全政策、加強資訊相關設備更新等,不定期派員赴各駐外單位,實地提供稽核、檢測、維運、教育訓練、技術支援等，應為目前最具體、實際的作為。