公務機密維護　錦囊 第 3 號

~「駐外機構資訊保密之道」

前言

駐外機構為我國外交打拼的最前線，其工作環節容易受到敵對勢力的刺探、蒐集，且隨著資訊科技日新月異，網路上的駭客攻擊手法也不斷翻新，部分駐外機構屢遭網路駭客惡意攻擊，蒐集公務機密資料或侵擾其行政運作，網路安全與資安管理面臨嚴峻的挑戰。若相關人員未能提高警覺，極易因疏忽而洩漏相關資訊，加上事後追查不易，致使機敏資料外洩時有所聞。

任何一個能夠上網的裝置或電腦，都很容易被網路上的惡意活動影響，因此，駐外機構人員應嚴格遵守相關資訊安全規定，以降低資通安全威脅，提高電腦資訊使用風險承受能力，並妥善使用公務電腦，避免機敏資料外洩，以確保國家安全及利益，實為駐外機構資訊機密維護的重要課題。

案例摘要

- 駐○○代表處○○組所屬電腦於非上班時間，發生大量資訊封包傳送至外部特定電腦情事，經查係該組乙類雇員林○○使用之外網電腦及實體隔離電腦。據瞭解林員以更新電腦病毒碼為由，私自將內網連接外網電腦，傳送大量資訊封包至外部特定電腦，有洩密之虞。林員所使用之 2 臺電腦硬碟，經查共計 26 件機敏資料外洩，違反資訊安全規

定情節嚴重。案經○○委員會召開專案小組會議，決議將林員解聘。

問題分析

- 系統遭入侵：未經授權之使用人（駭客）入侵資訊系統進行攻擊、竊取或竄改資料等非法破壞情事。例如，「社交工程」(Social engineering) 郵件設計愈來愈精巧可信，不知情的收儲，一旦開啟郵件附件，或點擊郵件內的惡意網站連結，任何一個動作都會讓電腦感染病毒。
- 未落實資訊安全規定：
  一、隔離電腦未落實隔絕於網際網路之外，專用於公務　作業。
  二、個人電腦之使用者識別碼及密碼，未妥善保存或交付他人使用，及未定期更換。
  三、機敏資料存放在對外開放的資訊系統中。
  四、隔離電腦未以人工更新防毒程式病毒碼。
  五、非經權責主管核准，個人電腦擅自下載軟體或變更硬體規格。
  六、遇有資安異常事件發生，未即時向資訊單位反映處理。
- 維護措施不足：
  一、可攜式設備或媒體（如筆記型電腦、行動硬碟、隨身碟等）應妥為保管，非因公務需要並經主管核准，不得攜出辦公處所，攜回時應進行掃毒或系統還原。
  二、對於電腦發生異常情事，未有警示系統，俾及時採取有效的防範措施。
  三、重要機敏檔案之備份媒體，未嚴密管制或由專人管制。

- 稽核功能不彰：未依機關資訊安全環境，實施資訊稽核，致未能即時發現缺失。
- 使用人違規使用：經授權之使用人明知違規而使用，致系統資料外洩等情事。

策進作為

- 網路流量監控、分析及管制：

  為防範系統遭駭客入侵，防火牆建置後，網管人員應隨時對資訊網路進行流量監控、分析及管制，俾利及時因應處理。

- 加強教育宣導：

  辦理駐外人員資訊安全教育訓練，建立正確的資安共識，以避免發生違規使用電腦及公務資訊之情事，其宣導重點如下：

  一、隔離電腦應隔絕網際網路並專用於公務作業，禁止私接；上網電腦連接網際網路並專用於上網瀏覽資訊或收發一般電子郵件。兩者不得混用，並於電腦設備明顯處張貼區別用途之識別標籤。

  二、隔離電腦變更用途為上網電腦或上網電腦變更用途為隔離電腦時，須先將電腦硬碟格式化、重新安裝作業系統。

  三、資料之加解密須在隔離電腦進行。

  四、嚴禁安裝使用 P2P 點對點分享軟體。

  五、禁止下載安裝或使用未經授權來路不明之軟體。

  六、避免開啟來路不明的電子郵件及檔案，以避免駭客病毒入侵。

  七、上網電腦禁止瀏覽非法或機關所限制之網站。

八、電腦應避免 24 小時開機，不使用時即關機或離線。

九、機密性或敏感性資料須以主管機關認可之加密機制加密後儲存於光碟、磁片、外接式硬碟等可攜性媒體或隔離電腦硬碟中，並予以妥善保存。

十、禁止使用上網電腦處理機密性或敏感性公務。

落實機關資訊安全稽核：

為機先發掘資安漏洞，同時檢視駐外機構人員實際執行保密情形，各駐外館處應定期、不定期或遇有重大洩密案件之虞時，執行資安稽核或保密檢查，除改善缺失漏洞並提高防火牆功能以防駭客入侵外，同時據以檢討策進，以建立同仁機密資訊維護的正確認知。

結語

駐外機構資訊機密維護工作，是否落實，攸關國家安全及利益，為確保資訊機密的安全，除了必要的資訊安全機制外，最重要的還是需要使用者的保密素養，因為資訊的掌握者、運用者都是「人」，唯有「人」對於資訊安全與保密工作能夠做好，才是維護資訊機密的根本之道；再者，唯有使用者都具備健全的觀念與知識，體認資訊機密安全的重要性，資訊安全政策才能落實。