



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101年2月1日非上班時間，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：

- 隔離電腦未落實隔絕於網際網路之外，專用於公務作業。
- 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。
- 機敏資料存放在對外開放的資訊系統中。
- 隔離電腦未以人工更新防毒程式病毒碼。
- 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。
- 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：

- 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。

- 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。
- 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：

 - 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。
 - 隔離電腦變更為上網電腦或上網電腦變更為隔離電腦時，須先將電腦硬碟格式化、重新安裝作業系統。
 - 資料之加解密須在隔離電腦進行。

- 嚴禁安裝使用 P2P 點對點分享軟體。
- 禁止下載安裝或使用未經授權來路不明之軟體。
- 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。
- 上網電腦禁止瀏覽非法或機關所限制之網站。
- 電腦應避免 24 小時開機，不使用時即關機或離線。
- 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。
- 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。

本署叮嚀

駐外機構人員對資訊保密工作應存有「時時保密」、「處處保密」及「維護機密安全是個人的專業責任」之觀念，尤以當前資訊設備精進，傳遞資訊的速度極快，洩密者或竊密者只要利用資訊設備，即可將所竊取之資訊即時傳遞，進而影響國家安全及利益。因此，對於資訊異常狀況，應保持高度警覺，以避免非相關人員接觸或使用資訊設施或資料，增加洩密之機會，為有效維護資訊安全，應妥採下列作為：

- (一) 人員管理及資訊保密教育訓練；

針對駐外機構人員之品德操守，主管應負起考核責任，瞭解屬員生活作息、交友、家庭、財務等有無異常狀況，適時輔導。調（派）任工作前，應施以保密安全教育，使其了解個人保密安全責任，熟悉有關安全要求與方法，對未依規定者，應適時調整職務，並在決定或提出建議之時，採取隔離措施。

（二）屬行稽核管制措施：

為有效稽核駐外機構電腦作業情形，發現潛存危險因子，資訊單位應對所屬電腦系統實施定期與不定期方式抽檢，並嚴格針對駐外人員於電腦作業時之磁碟暨檔案管理情形、密碼設定、實體隔離、電子郵件實施全面性檢查，確保資訊安全。

（三）緘密資料處理儲存：

電腦資料處理應設定安全防護措施，建立預警功能。在電腦資訊系統未採取任何安全存取控制及保密措施前，任何機敏資料，禁止存放於硬碟。

 **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。