若公務員不能建立資訊保密的安全共識，再完善的資安規定，都抵不住一個小失誤或蓄意洩漏。

淺談 P2P 潛藏的風險

◎ 王駿傑

由於網路技術的日趨成熟，加上 P2P 程式的積極開發應用，使得人們更容易超越時空的限制，獲取更快、更即時的訊息，例如最受歡迎的 MSN 聊天室、FOXY 網路瀏覽程式等，都是以此技術衍生的。然而，正當大家在享受最新的歌曲、電影的同時，P2P 程式其實正一步一步將大家推向最危險的邊緣。

所謂的「點對點交換技術」(Peer-to-Peer，簡稱 P2P)，又稱「對等網際網路技術」，其設計的概念，就是打破網路原有的伺服器與客戶端的限制，讓所有的網路使用者能夠共同分享硬體資源，包括 CPU 處理能力、硬碟儲存，甚至是網路頻寬，因此，可以讓大家更快、更迅速地分享資訊，下載 MP3、視訊影片等龐大的數位檔案。

然而使用 P2P 程式卻潛藏著極高的風險，務必要加以正視，包括：

1. 病毒攻擊的高度風險

使用 P2P 程式，無非是打開了家中的大門，歡迎任何陌生人隨時進來，當然其中也包括壞人。而且失去伺服器的先行監控，也將使電腦病毒更輕易地潛入使用者電腦中，增加病毒攻擊頻率。

2. 木馬程式的暗藏風險

由於失去了層層的監控防護機制，不法分子與駭客更可利用 P2P 程式，成爲最佳的犯罪利器，將木馬程式、鍵盤側錄軟體等大大方方地植入使用者電腦，不動聲色地竊取使用者的重要資料，造成難以估計的損失與傷害。

3. 機密資料的洩漏風險

只要輸入相關的字元，P2P 程式可以將所有網路使用者的資源與檔案，一網撈盡。因此，如果使用者電腦裡儲存有重要的機敏資訊或私密檔案，在使用 P2P 下載的同時，也將會被駭客一覽無遺，形成安全上的最大漏洞。

4. 智產分享的法律風險

P2P 程式應用時，無法分別合法或非法資訊。當使用者以 P2P 程式下載自己想要的檔案時，擁有者不能拒絕分享檔案，甚至無法發覺自己的電腦已將檔案寄送出去，所以，未來將衍生許多

智慧財產權，以及著作權等等的侵權法律糾紛，擾亂每個人的生活。俗話說：「天下沒有白吃的午餐。」這句話用來形容 P2P 程式，是再貼切不過了。所以，不要爲了貪圖一時的享受而樂極生悲，造成自己更多的損失。基於維護國家整體安全的前提，國人尤其是公務員在使用網路時，更應特別注意，避免因圖一時便利，或輕忽了檔案的重要性與機敏性，使得敵人乘虛滲透入侵，癱瘓網路，破壞國家內部的安全。因此，使用 P2P 程式應有的防護作爲，就是必需養成良好的資安習性，包括：

1. 絕不公務家辦

如把未完成的公務資料攜回家中，使用連接網際網路的電腦作業，將可能遭到暗藏的木馬程式，藉由 P2P 等程式把重要的檔案與秘密，偷偷地傳出，造成洩密的發生。

2. 嚴禁下載非法軟體

利用人們慾望的弱點，非法軟體大部分都會潛藏著木馬、病毒等惡意程式，藉機偷取個人重要資訊，或是讓使用者的電腦成爲犯罪的跳板。所以下載程式或檔案，應選擇合法的官方網站；另外，也要避免遭到網路釣魚的詐騙，造成嚴重的損失。

3. 培養檔案加密習性

不僅在公司，在家中所使用的電腦也應隨時加密，不使用時一定要關機，才不會讓 P2P 程式將電腦裡所有的資訊暴露於網路之中，任人下載窺視，或成爲有心人士的共犯與推手，達成其侵略破壞的目的。

總之，再完善的資安規定，若大家不能建立資訊保密的安全共識，縱有再高階的防火牆、防毒軟體及複雜的數位加密技術，都抵不住人員的一個小失誤與蓄意洩漏。因此，唯有大家依據政府通資部門的政策指導，安裝資安軟體與保密設定，才能由內而外地鞏固資訊安全，確保國家社會的正常運作。