

點對點傳輸，P2P

前言：

相信很多單位都曾收過 P2P 事件侵權的 mail 通知，其中不乏就是呼籲要使用合法軟體並尊重智慧財產權。

當聽到 P2P 就會直覺想到 Foxy、eMule、edonkey 這些傳輸軟體^{註1}！這些軟體本身都是合法的技術，合不合法則是看「分享的檔案」是否有版權。其實 P2P 只是一種對等式網際網路傳輸技術^{註2}，很多研究計畫^{註3}或是常用的 IM^{註4}都是採用 P2P 技術。

它強調的是網際網路架構之下端點(使用者端)對端點(Peer-to-Peer)、程式對程式(Program-to-Program)、電腦對電腦(PC-to-PC)及人與人間(People-to-People)四重直接的關係。

當安裝 P2P 分享軟體後，所有連上網際網路的個人電腦，都可以同時扮演伺服器端及用戶端，可以同時下載資料及與他人分享自己電腦中的資料。

P2P 軟體使用衍生問題：

- P2P 工具包可能被惡意人員放置木馬後門程式或病毒、蠕蟲。
P2P 軟體大多都是免費軟體，技術較高的人員可把這些軟體做逆向工程，夾帶木馬後門程式或惡意程式後，再放於網路上供人下載，如不是在官方網站下載這些軟體，勢必會危害到你的電腦亦或是你在下載的檔案是一支惡意程式而不是原本所想的檔案。
- P2P 軟體本身的漏洞，造成駭客入侵。
P2P 軟體多為免費，相對資金並不是充裕無法做很完善的程式漏洞的安全檢測，有心人士蒐集到這些軟體漏洞，將會對這些使用有漏洞軟體的使用者進行攻擊。
- 使用 P2P 軟體時，誤將本機目錄開放共享。
很多人裝上軟體後，並不會多加設定軟體進階功能，這些軟體本身都會預設幫你開啟分享目錄 My Documents 這些資料夾，這是非常危險。很多人或是編輯文書工具，預設存檔大都存在 My Documents 這資料夾內，重要資料都是在這，跟著 P2P 軟體一起分享出去，進行網路資料交換。許多機密外洩是這樣發生。(警局筆錄外洩事件、軍方演習機密、個人申報所得稅資料)
- 使用 P2P 下載影音檔案，多半為 mp3、mpeg 和 avi... 等檔案，可能造成侵權行為。
擅自以重製之方法侵害他人之著作財產權者，處三年以下有期徒刑、拘役，或併科新臺幣七十五萬元以下罰金。將網路上的文章、圖片、音

樂或影片等著作上傳、下載、轉貼、傳送與儲存都是屬於重製行為，若未經同意進行重製，都將會違犯此條文。

- 使用 P2P 檔案交換嚴重佔用網路頻寬造成單位行政庶務、網路教學無法正常運作。

P2P 軟體使用注意事項：

- 辦公室應嚴禁使用 P2P 軟體工具，避免駭客有入侵的可能機會，也勿使用公務用之筆記型電腦下載 P2P 檔案，以免不慎遭駭客入侵後，擴散至辦公室網路中的其他電腦。
- 下載任何工具軟體，應該從原廠官方網站取得，切勿從入口網站或是論壇網站下載當然亦須留意釣魚網站，如此可避免下載含有惡意程式的 P2P 軟體工具組。
- 使用 P2P 工具時，應縮短暴露在網際網路的時間，下載完畢後，應該立即停止執行 P2P 程式，避免駭客透過 P2P 工具攻擊。
- 使用 P2P 工具所下載回來的檔案，亦須多加留意，最好經過掃毒及後門防範軟體的驗證，確認是安全的，以免您的電腦成為辦公室網路的跳板。

註 1

P2P 軟體：BitTorrent、BitComet、BTspirit、BitTorando、eDonkey、eMule、GnuTella、ezPeer、Mxie、FastTrack、KaZaA、WinMx、Winny、NapMx、Foxy 等，族繁不及備載。

註 2

對等式網際網路傳輸技術：任兩個網路上的電腦彼此可以互相分享資料與頻寬，而不需要利用單一的伺服器來對其他電腦服務。使用者可以透過 P2P 軟體進行直接的互動，使得網路上的溝通變得更為容易、更直接共享與互動。

註 3

研究計畫：Seti@home：尋找外星智慧計畫
Folding@Home：模擬蛋白質折疊的計畫
FightAIDS@Home：協助愛滋病研究
Evolution@Home：模擬物種演進及滅亡
Predictor@Home：預測蛋白質結構

註 4

IM：即時通訊(Instant Message)軟體，如 MSN、skype、yahoo message 等，詳可參閱本中心/資訊安全專區/資安宣導的即時通訊 IM。

多一點確認，少一分損失

參考資料：http://newsletter.ascc.sinica.edu.tw/news/read_news.php?nid=1343

資料提供：國立嘉義大學電算中心