可攜式媒體使用安全守則

◎ 鍾榮翰

民國 96 年 8 月間網路媒體報導：3 月間神奈川縣警方在調查非法入境案時，意外發現一名海上自衛隊士官家中電腦硬碟內有大量神盾艦系統資料，而後案件如滾雪球般擴大。警調單位查出來源可能來自海上自衛隊第一術科學校，校內教官複製神盾艦防空系統以及領導幹部養成等資料作爲教學使用。類似這樣的教學資料在學生之間流傳十分普遍，因此這名士官可能透過學生輾轉拿到這些特別軍事機密的戰艦中樞防空系統資料。

這起案件對於在國防上與美國有密切合作關係的日本來說無疑是項打擊，因爲在美日安保條約中明文規定，關於洩漏美方軍武機密的罰則，視情節嚴重涉案人最高將被判處 10 年有期徒刑，而日本國防部長（防衛相）小池百合子也已因此案下台以示負責。

同年 11 月國內媒體報導：Maxtor 在泰國生產的 3.5 吋、500G 可攜式硬碟，遭植入木馬程式；調查局已於 10 月間先行接獲民眾報案，實地購買同款硬碟送交資安鑑識實驗室分析、測試，證實確有 autorun.inf 及 ghost.pif（惡魔程式）木馬程式。該木馬程式會感染其他插入的隨身碟，並感染 autorun.inf、windows.scr 檔案，且會主動連線及上傳資料到外部網站。使用者只要接上該硬碟，電腦程式就會自動連線某特定網址，電腦資料變成「全都露」。

以上二則報導揭示了可攜式媒體所衍生的資安議題，其涉及層級之高，與影響範圍之廣，甚至可能有損機關或是國家之形象。究竟應如何正確使用及管理可攜式媒體，本文將從技術、操作與管理三個層面分別探討應注意事項，以供讀者參考。

認識 USB

隨著記憶體製作技術之進步，可攜式媒體的體積越來越小，儲存空間卻越來越大，加上「通用串列匯流排 (Universal Serial Bus，就是大家所熟知的 USB)」隨插即用之特性，爲人類生活帶來極大之便利。

USB 目前已是一種標準的連接界面，即插即用(Plug-and-Play)，不必重新配置規劃系統，也不必打開機殼調整界面卡的設定值，電腦會自動識別這些周邊設備，並且配置適當的驅動程式，無需使用者再另外重新設定。該介面目前所支援之周邊設備包含鍵盤、網路通訊、印表機、音效、儲存設備、數位相機及 3G 手機等。它具有「熱插拔」(Hot Attach &Detach)的特性，也就是在作業系統已開機的執行狀態中，隨時可以插入或拔離 USB 裝置，不需有關機之動作，也不會導致設備之毀損。有關此一特性攸關安全地卸除 USB 操作方法，請務必牢記。

使用 USB 隨身碟潛在之風險

使用者習慣將具備 USB 介面之可攜式媒體，稱之爲 USB 隨身碟，可以算是目前最便利的儲存裝置，難怪深受大眾的喜愛，但卻存在著以下的潛在風險：

1. 功能多樣化，在管理政策中難以定義，實際作業不易杜絕員工使用。
2. 外型設計多樣化，容易通過安全檢查，不易偵測。
3. 因其輕便性，易於遺失或遭竊；若內存資料未加密，易遭不當揭露。

4. 存於可攜式設備及儲存媒體的內容多數爲重要或具機密性之資料，資產價值較高，容易成爲有心人士竊取的目標。
5. 有心人士可利用進入機關內部機會，進行不法竊取機密的活動。
6. 可攜式設備及儲存媒體常被共享使用，讓資料的不當存取及病毒擴•散情形更爲嚴重，甚至進入實體隔離網路進行擴散並竊取資料，可視爲另一種型態之社交工程攻擊。
7. 大多數可攜式設備及媒體不會產生事件記錄，無法追蹤其使用過程。
8. 可攜式媒體結合環保軟體的使用，增加非法軟體管制的困難度。

綜整以上各點意見，機關對於 USB 隨身碟之使用，應採取審慎之態度。目前僅有少數具有高度強制力之機關，採行全面禁止使用之方式，於管理政策上宣示：「禁止機關同仁使用隨身碟」。惟絕大部分的機關，於實務上卻必須利用 USB 碟之便利特性，運用於資料交換或重要資料之備份，於是如何正確而安全地使用 USB 隨身碟，便是認知訓練上重要課題，也是本文撰寫之目的。

USB 惡意程式之運作模式

坊間討論或是媒體報導，常見將利用隨身碟進行入侵之惡意程式稱之爲「USB 病毒」，但是從鑑識實務中分析發現，此類 USB 病毒具備有電腦病毒(Virsus)的感染能力，也具備蠕蟲(Worm)的擴散能力，入侵之後更會如間碟軟體(Spyware ）般地竊取受駭者的機敏資訊，更近一步會如木馬程式（Trojan Horses）般地掌控受害者的電腦，故嚴謹的名稱應稱之爲：「USB 惡意程式」；它們都有一個共同的特徵，就是利用可攜式媒體的自動執行功能，來達到入侵的目的。

USB 惡意程式與一般電腦病毒類似，只是此種類型的惡意程式通常會搭配 Autorun.inf 檔案，並從 USB 隨身碟感染電腦。原本 Autorun.inf 檔案是希望電腦在存取外接式媒體時，作業系統會先尋找 Autorun.inf 檔案，並執行指定的程式指令，達到便捷之目的；很多的多媒體教學光碟便是利用這項功能，來達成自行安裝並啓用之程序。

USB 惡意程式也是利用此種方式，將對應的 Autorun.inf 檔案及惡意程式寫入 USB 隨身碟並加以隱藏，所以就算使用者從本機電腦的「我的電腦」資料夾中，查詢 USB 隨身碟資料，也不一定能查覺出問題。當開啓的過程若是一般方式，便會啓動惡意程式，而達到入侵之目的。

一、惡意程式組成

USB 的惡意程式猶如地雷，主要由二部分所組成，第一部分是引爆的開關，也就是 Autorun.inf 檔案；第二部分是具有爆炸威力的 TNT 炸藥，也就是實際上的惡意程式，必須這二部分結合，才會發生作用，若是移去了開關，TNT 炸藥只會安定地存在，而不構成危害。故當有人誤觸了開關，便會引爆炸藥，近一步導致人員傷亡或是財產損失。反之，若是熟知開關的位置，並且知道開啓的路徑，便可安全地開啓而不致引爆，以確保人員財產的安全。

二、Autorun.inf 語法剖析

上述開關到底有何玄妙之處，爲何會讓不知情的使用者束手無策呢？以下我們便來解析它的語法，進而了解它運作的機制：

它的典型語法由以下 5 行指令所構成

[autorun]；宣告自動執行功能

open=XXXX；地雷名稱

shell\open\Default=1；將下列指令對應至右鍵選單之位置

•shell\open\Command=File\XXXX.exe；將開啓指令對應至炸藥存放的路徑

•shell\explore\Command=File\XXXX.exe；將檔案總管對應至炸藥存放的路徑

若將含有上述開關組成的 USB 隨身碟插入電腦中，作業系統便會依據使用者開啓的動作，執行對應的指令，並會將指令對應至右鍵選單中。

一般的使用者習慣在視窗中使用滑鼠左鍵點二下，直接開啓隨身碟，此時便是執行了 shell\open\Command，作業系統就會去找到炸藥的藏身之處將其引爆，如圖 1 所示。

若是按滑鼠右鍵選單，開啓檔案總管，此時便是執行了 shell\explore\Command，作業系統同樣會去找到炸藥的藏身之處將其引爆，如圖 2 所示。

感染的時機

1. USB→PC：當已遭感染之 USB 連接上 PC，於開啓 USB 之過程中，因操作程序觸動了地雷的開關，因而將炸藥引爆，導致 PC 遭感染。
2. PC→USB：當已遭感染之 PC 插入 USB 隨身碟時，感染時機有二，早期利用連接 USB 隨身碟之當下，立即進行感染，較易被發現；近期則利用「安全地移除硬體」功能，於移除 USB 的時候進行感染，以避免被發現。

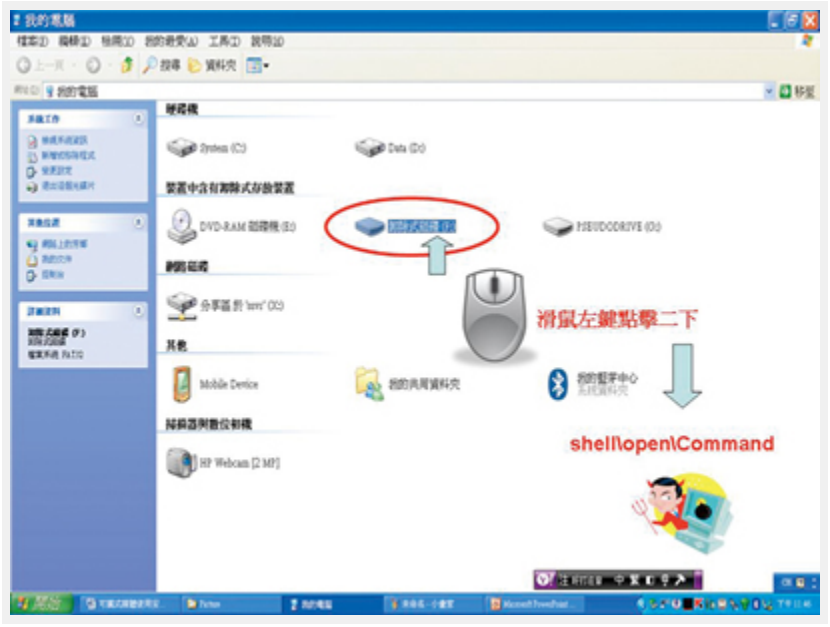

圖 1：滑鼠點擊二下開啓 USB（資料來源：自行整理）

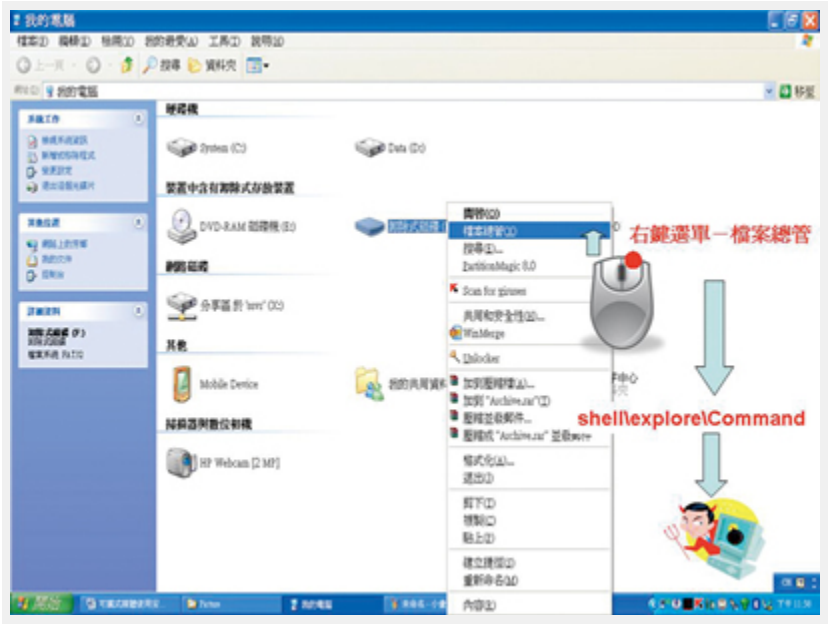

圖 2：右鍵選單\檔案總管，開啓 USB（資料來源：自行整理）

正確開啓 USB 的方法

圖 1、2 大家常用開啓 USB 的方法竟然就是惡意程式所設下的陷阱，等著你自投羅網。那正確的開啓方法又是如何呢？是不是每個人都可以學的會？真的很容易操作嗎？以下將介紹的操作方法，應可防範 USB 惡意程式的感染。

首先我們需要更改一下設定，以顯示所有隱藏檔，因爲惡意程式爲避免被發現，會將自己隱藏起來，所以需要將資料夾選項中，取消隱藏已知檔名類型副檔名，並顯示所有隱藏檔案與資料夾，如圖 3 所示。

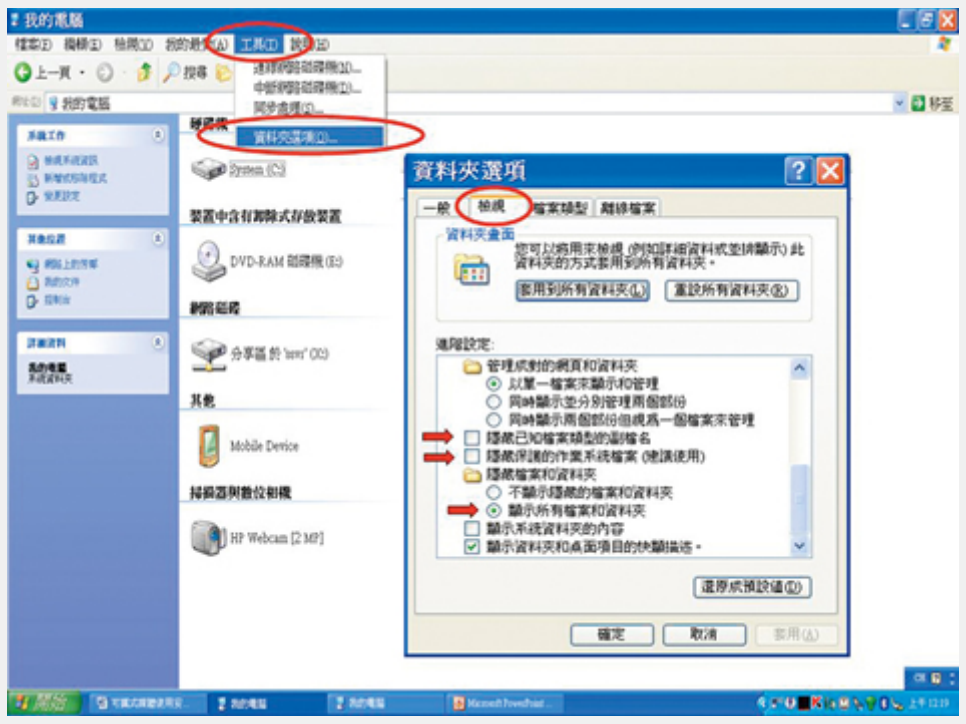

圖 3：檢視隱藏檔案（資料來源：自行整理）

接下來在開啓「我的電腦」視窗後，要點選「資料夾」以開啓左側之「資料夾窗格」，一定要從左側窗格中點選 USB 隨身碟，就可開啓資料夾的內容，不致誤觸開關而引爆炸藥。

若 USB 隨身碟已遭感染，在根目錄下可以發現有 Autorun.inf 的開關藏身其中，直接將它刪除即可，如圖 4 所示，或是將 USB 隨身碟直接格式化，也是個快速清除地雷的好方法，但請記得要將裡面的資料備份出來，相關細節可以請教機關內之資訊人員。

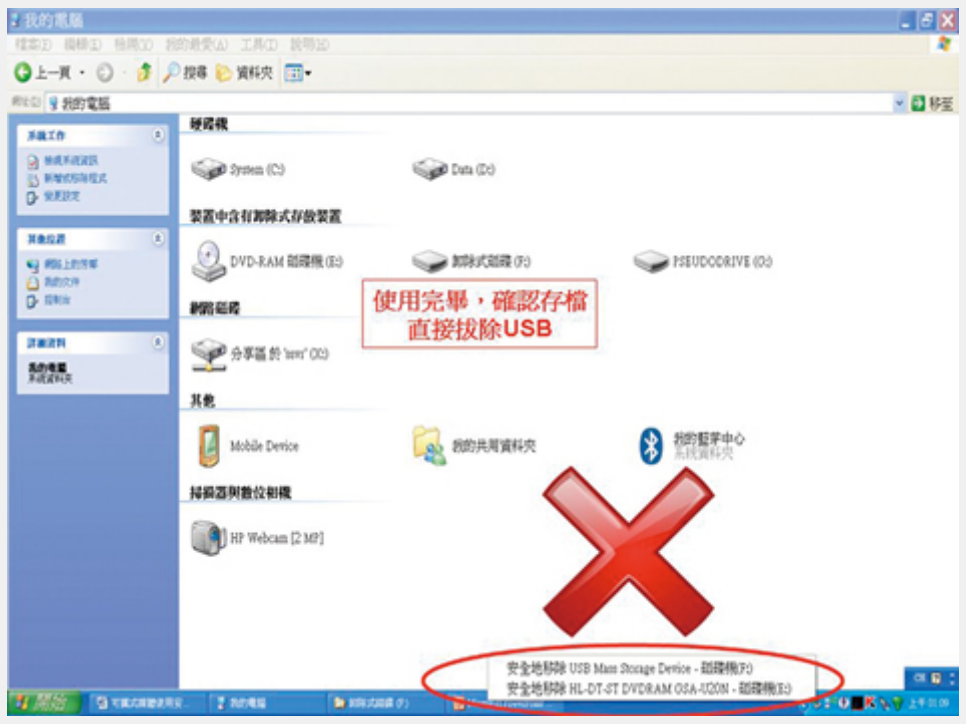

圖 4：正確開啓 USB 隨身碟的方法（資料來源：自行整理）

使用完畢正確退出 USB 之方式，建議於確認 USB 已存檔後，直接拔除，切勿再使用「安全的移除硬體」功能。原 windows 作業系統提供之「安全地移除硬體」功能，係爲避免資料於存取過程中，USB 設備遭移除，而導致資料存取毀損；現在之入侵手法便是利用使用者按下移除功能時才進行感染動作，這點與以往大家所認知的好習慣有所不同，往往擔心是否會損壞硬體。其實 USB 具熱插拔功能，直接拔除並不會損壞硬體，但務必要確認檔案讀取動作已完成，如圖 5 所示。

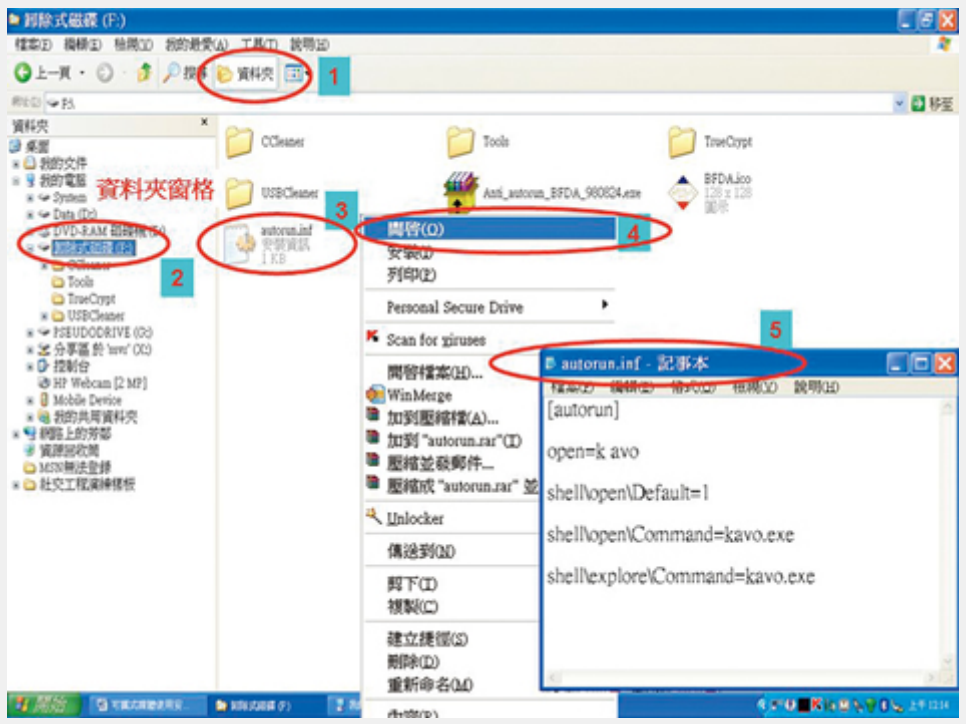

圖 5：安全卸載 USB 的方法（資料來源：自行整理）

結　論

可攜式媒體的安全管理，光是仰賴政策面的強制要求是不夠的，遺憾的是在技術面迄今仍沒有完善的解決方案；然而惡意程式雖是一直演化，但是入侵感染的方式卻極少變動，這是典型的運用操作性控制措施以達其迴避風險的目的。唯有強化使用者本身的認知訓練與自我管理，確保任何時間、任何地點、使用任何電腦，都可以養成本文所介紹之好習慣，才是落實可攜式媒體安全管理的重要關鍵。