清流月刊中華民國九十八年十一月號

可攜式媒體的安全管理，光賴政策面的強制要求是不夠的，唯有強化使用者本身的認知訓練與自我管理才是重要關鍵。

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為教學使用。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，因為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，為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，稱之為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為重要或具機密性之資料，資產價值較高，容易成為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為嚴重，甚至進入實體隔離網路進行擴散並竊取資料，可視為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為「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為：「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，來達成自行安裝並啟用之程序。

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。當開啟的過程若是一般方式，便會啟動惡意程式，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，並且知道開啟的路徑，便可安全地開啟而不致引爆，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，為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 ; 將開啟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啟的動作，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，直接開啟隨身碟，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，開啟檔案總管，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，於開啟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。

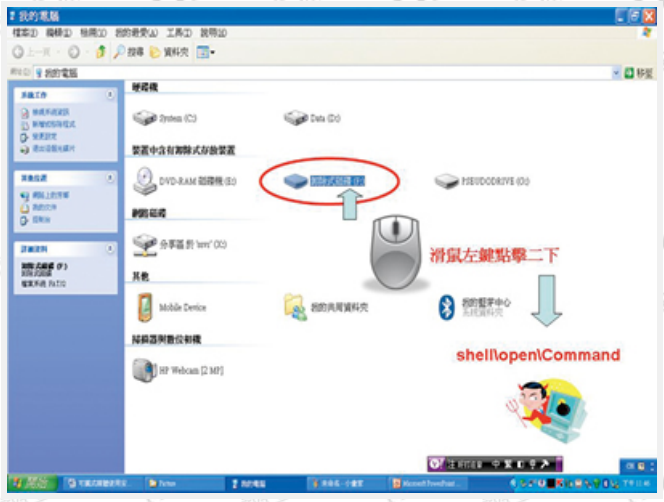

圖1：滑鼠點擊二下開啟USB（資料來源：自行整理）

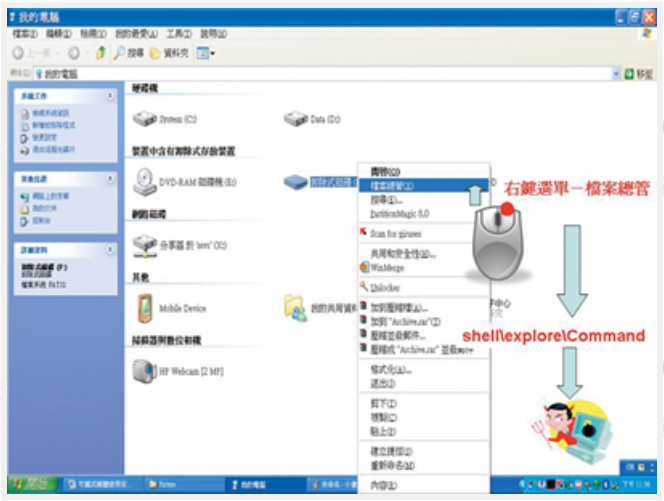

圖2：右鍵選單\檔案總管，開啟USB（資料來源：自行整理）

正確開啟USB的方法

圖1、2大家常用開啟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。那正確的開啟方法又是如何呢？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，因為惡意程式為避免被發現，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。

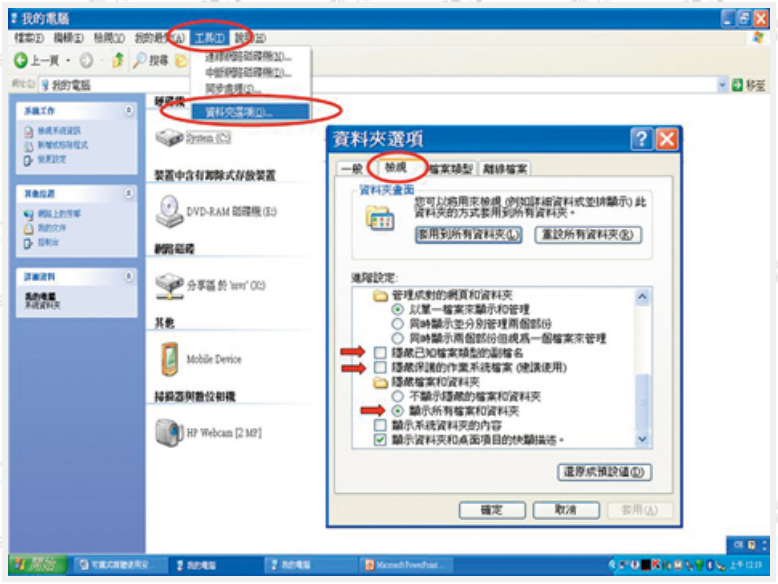

圖3：檢視隱藏檔案（資料來源：自行整理）

接下來在開啟「我的電腦」視窗後，要點選「資料夾」以開啟左側之「資料夾窗格」，一定要從左側窗格中點選USB隨身碟，就可開啟資料夾的內容，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。

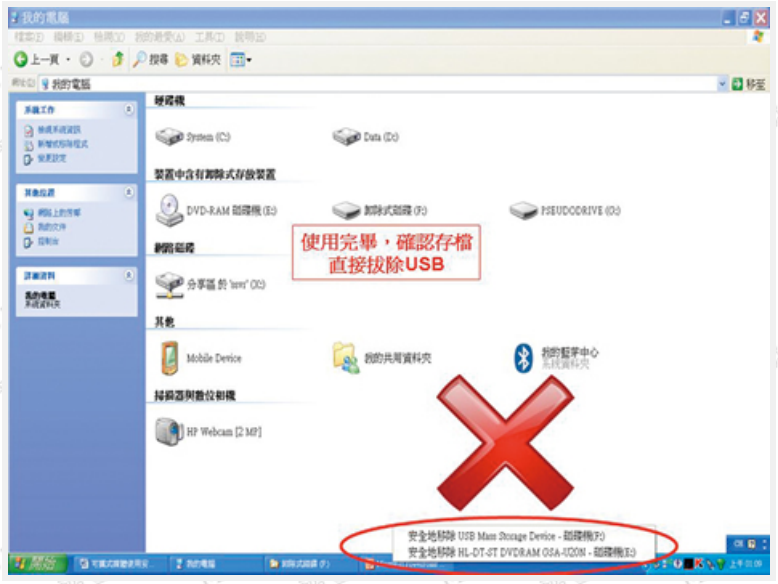

圖4：正確開啟USB隨身碟的方法（資料來源：自行整理）

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，係為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。

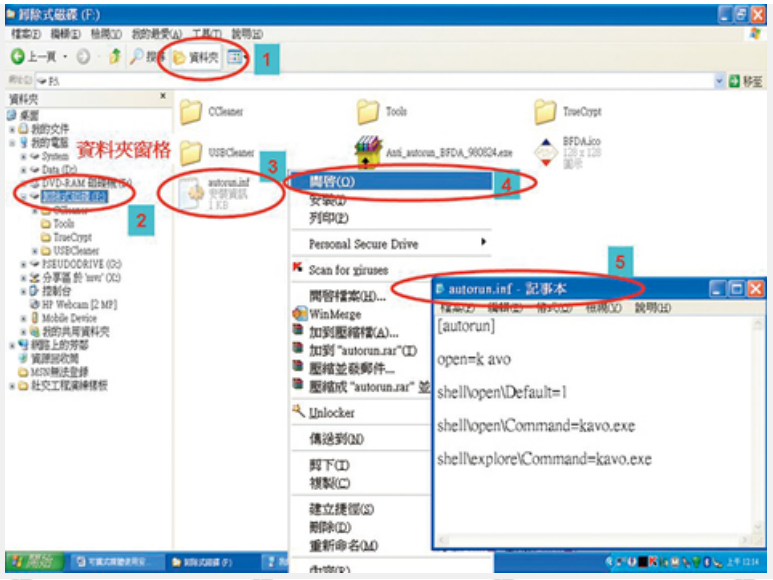

圖5：安全卸載USB的方法（資料來源：自行整理）

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。

▲Top

視覺化的USB惡意程式預警機制，可以比防毒軟體更早一步提醒你是否處於安全環境。

可攜式媒體防護範例介紹

◎鍾榮翰

簡易偵測機制

前文中提要，USB惡意程式會利用Autorun.inf當做地雷的開關，用以引爆炸藥，而對電腦造成危害。請注意！每一個USB隨身碟只有一個正確的位址可以安置開關，而且是僅能有一個開關。如果我們用同樣的模式，預先安置了一個經過巧思設計的開關，並且搭配一支環保程式（或稱之為綠色軟體），就可以變成一組視覺化的偵測機制，讓一般使用者可以眼見為憑，體會原來的操作習慣，會導致惡意程式的入侵。

以下的示範非常簡單，首先要將電腦之自動播放功能開啟，並需要一支綠色軟體，亦即不需安裝，可以存放在USB隨身碟中，就可以在任一的電腦中執行；藉由執行的結果，模擬惡意程式的行為，達到視覺化的效果，訓練使用者養成正確操作的好習慣。請依據以下步驟實施：

1. 下載CCleaner程式 http://www.ccleaner.com/download
2. 安裝CCleaner程式（這是免費且支援中文化的電腦清理程式），預設路徑為C:\Program Files\CCleaner
3. 將上述路徑之CCleaner資料夾，複製到USB隨身碟
4. 以上係利用綠色軟體之特性，複製到隨身碟後毋須安裝即可執行
5. 開啟附屬應用程式—記事本
6. 編寫autorun.inf檔案

```
[autorun]
open=CCleaner
shell\open\Default=1
shell\open\Command=CCleaner\ccleaner.exe
shell\explore\Command=CCleaner\ccleaner.exe
```

7. 將檔案另存成autorun.inf並儲存於USB根目錄下，如圖1所示。

以上偵測機制的功能，是利用與USB惡意程式同樣的方法，但是可以達到視覺化的效果，以提示使用者操作方式是否正確！如圖2所示。

於上圖中，當使用者點選卸除式磁碟F:\，直接以滑鼠左鍵點擊二下，便會觸發Shell\open\Command，而啟動CCleaner程式，便會產生視覺化之效果，提示我們已經觸發地雷了，其執行結果與USB惡意程式之執行雷同，也就是說：如果以上之USB隨身碟中藏有惡意程式，則以上使用者的開啟方式，已經啟動惡意程式而遭感染了。

利用以上的簡易偵測機制，可以用來訓練使用者，讓他嘗試著用各式各樣的方法來開啟USB隨身碟，看看是否會觸發CCleaner程式，了解以往的認知式錯誤的，進而養成正確操作的好習慣。

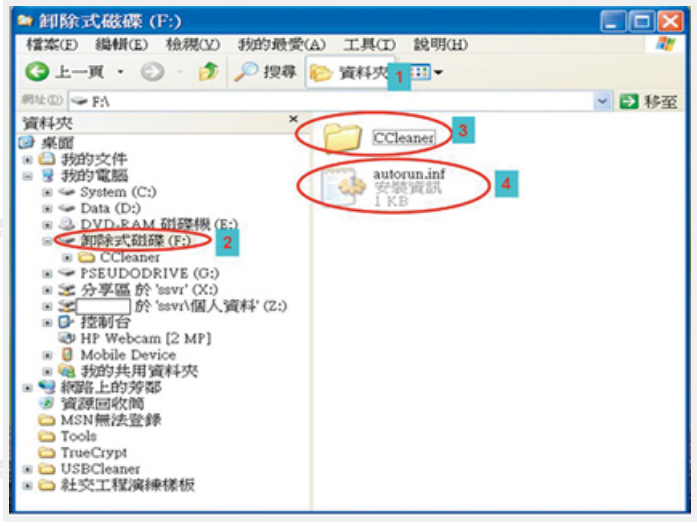

圖1：簡易偵測機制檔案存放位置（資料來源：自行整理）

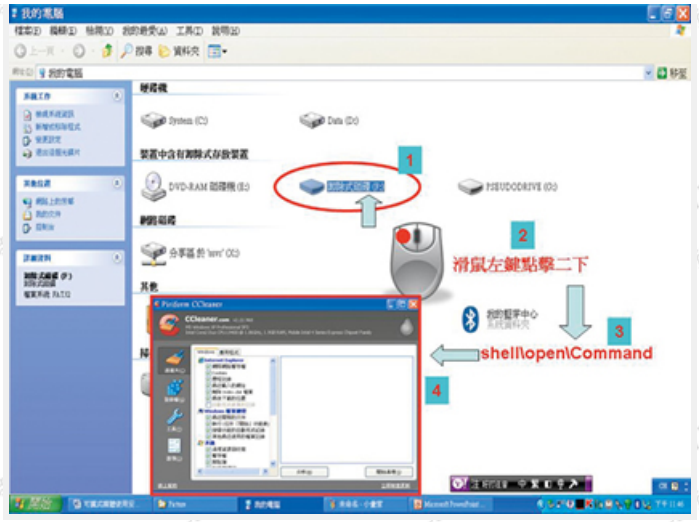

圖2：簡易偵測機制示範（資料來源：自行整理）

進階偵測機制

接下來將要示範進階的偵測機制，可以更直接更快速地判定電腦是否已經遭到此類USB惡意程式的感染，進而採取必要的防護措施。延續上一小節的示範，需要改寫Autorun.inf，請依據以下步驟實施：

改寫autorun.inf檔案

```
[autorun]
label=CClearner ; 將USB磁碟賦予一個標籤
icon=CCleaner\ccleaner.exe ；提供一個圖示以供顯示之用
open=CCleaner
shell\open\Default=1
shell\open\Command=CCleaner\ccleaner.exe
shell\explore\Command=CCleaner\ccleaner.exe
```

完成存檔後，將USB隨身碟拔出後再重新插入，將會發現在「我的電腦」視窗中，新插入的USB隨身碟有了新的標籤，而且有一個視覺化的圖示，如圖3所示。

圖3所示的進階偵測機制，在開啟的過程中和簡易偵測機制有著同樣的功能，但卻新增了更簡易且更迅速的偵測機制，可以立即藉由圖示的存在與否，來判斷USB隨身碟或電腦是否已經遭到此類惡意程式的感染。

進一步說明之前，我們再來複習一下重要的觀念：

1. 每一個USB隨身碟只有一個正確的位址可以安置Autorun.inf開關，而且是僅能有一個開關。
2. 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。
3. 近期則利用「安全地移除硬體」功能，於移除USB之時候進行感染，以避免被發現。

根據以上的重要觀念，我們把已經製作完成的USB隨身碟，插入一台已經遭受感染的電腦，此時會有什麼現象發生呢？如果是採第一種感染方式，於連接USB之當下，立即進行感染，則惡意程式會置換掉我們所編寫的Autorun.inf檔，原設計的標籤與圖示將會消失，我們就可以合理懷疑已經遭受感染。

但實務中遇到的情形，有越來越多的案例是採第二種感染方式，所以我會刻意地啟用「安全地移除硬體」功能，誘使惡意程式來感染USB隨身碟；拔除之後，立即再插入電腦之中，如果已經遭到感染，則原設計的標籤與圖示將會消失。反之，若是原設計的標籤與圖示依舊存在，則可以判定該電腦並未遭受USB惡意程式的感染，可以安心地進行作業。

以上所述的USB隨身碟若是已遭感染，則可點選Autorun.inf，按右鍵開啟，此一動作只會將這個開關打開，並不會觸發內部的指令，不必擔心，根據開關內的指令，按圖索驥便可以找到炸藥的藏身之處，直接將它刪除即可。

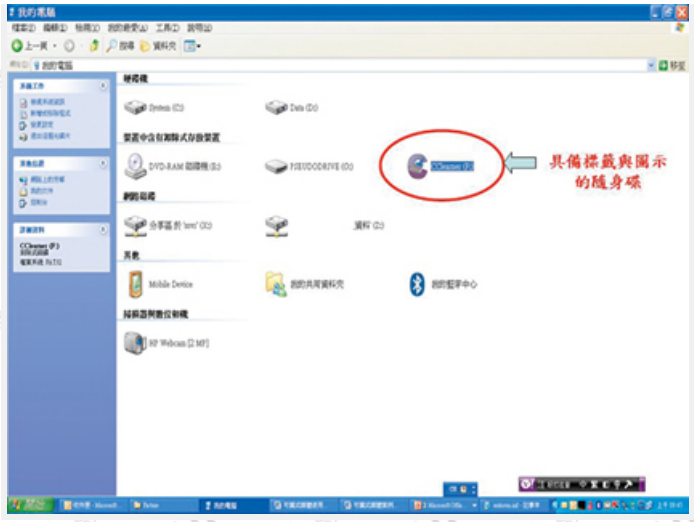

圖3：進階之圖示範例（資料來源：自行整理）

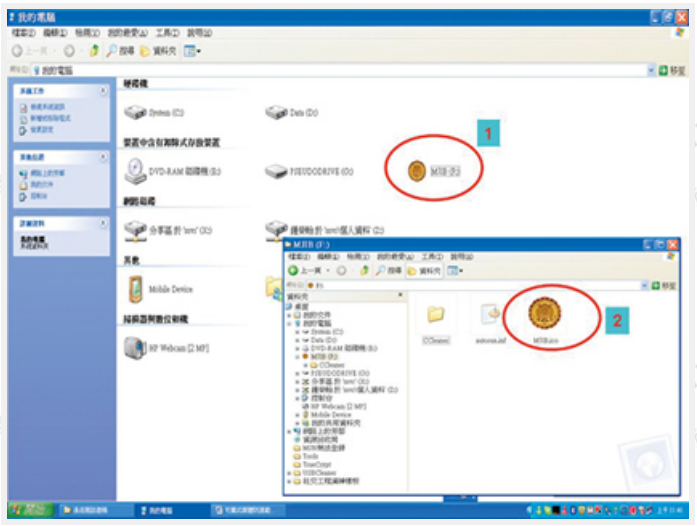

圖4：客製化圖示（資料來源：自行整理）

偵測機制演化

一、客製化磁碟

以上之偵測機制亦可以加以客製化，製作符合機關或是個人特質的標籤與圖示，以達偵測與識別之目的。其方法很簡單，首先找到足以代表機關或是個人的圖片，將之製作成圖示(Icon)，改寫autorun.inf檔案：

```
[autorun]
label=MJIB ; 將USB磁碟賦予一個「MJIB」標籤
icon=MJIB.ico ；提供一個MJIB圖示以供辨識之用
open=CCleaner
shell\open\Default=1
shell\open\Command=CCleaner\ccleaner.exe
shell\explore\Command=CCleaner\ccleaner.exe
```

具有以上圖示功能的USB隨身碟，將更會提醒使用者，要隨時注意正確操作，養成良好習慣。同樣也可針對個人製作具個人識別之圖示，強化個人之識別度，以建立正確的資安認知。

二、加密化磁碟

實務上有使用USB隨身碟者，基於資訊交換或是資料備份之需要，通常會將重要的檔案存放其中；試想若是不慎遺失，重要敏感資訊遭不當揭露，恐為害機關或是個人之安全；惟實務中卻鮮少見到先將檔案加密後再儲存於USB隨身碟中，確有必要加以保護。

以下範例與TrueCrypt加密軟體結合，它是免費的開放源碼磁碟加密軟體（Free open-source disk encryption software），並且提供中文化之套件，相關的軟體與套件，可於以下的網址下載：

TrueCrypt http://www.truecrypt.org/downloads.php

中文化套件http://www.truecrypt.org/localizations.php

（註：業務範圍若涉及國家機密者，所採用之加密軟體應經主管機關核定始可使用，以上範例所採用之加密軟體，僅建議個人或非涉及國家機密業務範圍內使用）

有關TrueCrypt軟體之使用，讀者請自行上網查閱

首先改寫autorun.inf檔案：

```
[autorun]
label=TrueCrypt USB
icon=TrueCrypt\TrueCrypt.exe
action=掛載 TrueCrypt 加密區
open=TrueCrypt
shell\open\command=TrueCrypt\TrueCrypt.exe
shell\explore\Command=TrueCrypt\TrueCrypt.exe
shell\start=掛載 TrueCrypt 加密區
shell\start\command=TrueCrypt\TrueCrypt.exe /q background /lS /e /m rm /v "SecureData"
shell\dismount=卸除TrueCrypt 加密區
shell\dismount\command=TrueCrypt\TrueCrypt.exe /q /d
shell\clean=清除殘存資訊
shell\clean\command=CCleaner\CCleaner.exe
```

將上述之Autorun.inf檔及TrueCrypt、CCleaner資料夾複製至USB隨身碟中，除了具備前述之偵測機制，更具備有加密之功能，可以更正確且安全地使用USB隨身碟，詳見三所示。

三、清除殘存資訊

接下來本文將說明偵測機制中搭配CCleaner之目的。電腦使用過程中為了效率或是復原之目的，經常會留下許多的暫存檔，包括上網瀏覽之記錄、近期內開啟之文件等，很可能因而揭露了個人的業務活動；相關之資安管理規範或指引，通常會提示應定期加以刪除，以免揭露業務之活動。CCleaner便是基於這樣的目的所發展的工具程式，可以協助我們檢查電腦中的暫存檔，並且很有效率地清除。如圖6所示。

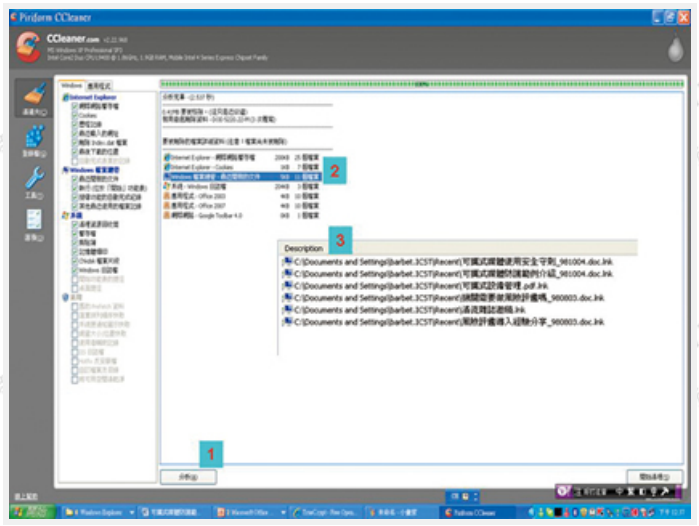

圖5：TrueCrypt軟體示範（資料來源：自行整理）

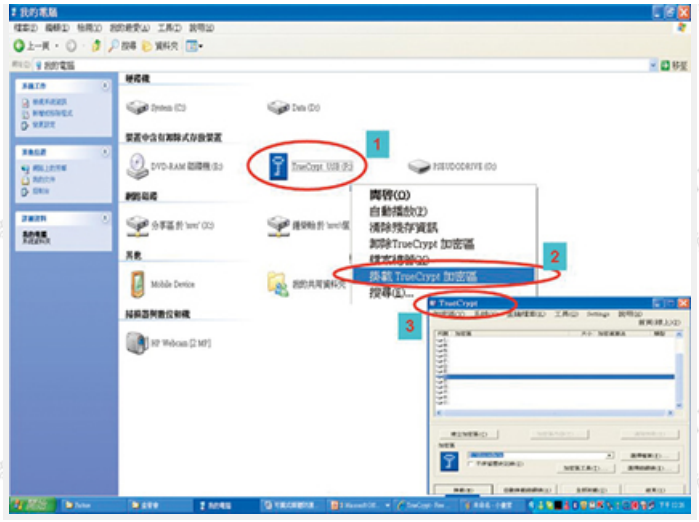

圖6：CCleaner軟體示範（資料來源：自行整理）

結　論

每當有重大隨身碟惡意程式流行之際，經常可見媒體報導，呼籲讀者應小心謹慎，亦常有專家現身說法，教導一般使用者應注意之事項，然確不乏有謬誤之處。以上所述便可驗證習得之方法，是否確具成效。

在本質上USB惡意程式的議題，應屬於個人操作習慣的問題，通常不容易發展出有效之技術解決方案；實務當中固有不同之技術設定，可以阻斷自動執行的功能，但是養成良好之使用習慣，才可以在任何時間、任何地點，使用任何電腦均確保使用安全。

本文所陳述的，主要是利用操作性控制措施，以達避免風險之目的，並廣泛運用視覺促進（Visio Promoting）技術，強化認知訓練之效果；由於實際教學成效卓著，特將此與清流之讀者分享。

（作者是國家資通安全會報技術服務中心經理）

▲Top