電腦輔助建築製圖能力本位訓練教材

偵毒及排除

編號：SCD-A2D0904

編 著 者：吳育昇
審 稿 者：李光華、蔡謀誠
主辦單位：行政院勞工委員會職業訓練局
研製單位：中華民國職業訓練研究發展中心
印製日期：九十年十二月

行 政 院
勞工委員會 職業訓練局

單元 SCD-A2D0904 學習指引

當你學習本單元之前，你必須精通下列的操作：硬體介紹、週邊設備認識、作業系統操作等功能， 同時能說出其功能及意義，假如自認無法勝任此一工作，則請按下列的指示進行學習：

(1) 你全部無法勝任上列之工作，請將本教材放回原位，並取出編號 SCD-A2D0803 教材開始學習，或請教你的老師。

(2) 如果你已經學會硬體介紹了，但不瞭解週邊設備的認識，則請從編號 SCD-A2D0801 教材開始學習，或請教你的老師。

(3) 如果你已經學會硬體介紹、週邊設備認識，但不會作業系統的操作，則請從編號 SCD-A2D0901 教材開始學習，或請教你的老師。

引言

『電腦病毒』的出現震撼了整個世界，在高度電腦化的社會裡它所造成的損失不亞於天災，輕則工商機關辛苦建立的資料毀於一旦，重則造成全國金融、學術通訊網路的全面癱瘓，不可不慎啊！因此本章節將探討有關偵毒及排除操作的活動計有下列幾個方面：即：(1)電腦病毒的定義與有關名詞解釋，(2) 電腦病毒的特性與分類，(3) 電腦病毒感染的途徑與特徵，(4) 掃毒程式的應用。在這幾個方面，第(1)(2)(3)項次係介紹有關電腦病毒的的相關智能，而第(4)項次則是介紹有關電腦病毒的掃毒操作智能，因此在操作之中請熟習各項次的意義與操作，進而應用於防止電腦病毒的入侵與電腦病毒的防治。

請翻至第 2 頁

定義

一般而言偵毒的意義係指偵測出電腦病毒，排除則指排除電腦病毒於電腦之外，因此預防電腦病毒的感染乃是必具的概念，而偵毒及排除則爲必要的操作方法。

請翻至第 3 頁

學習目標

一、 不使用參考資料，你能夠以你自己的話正確地說明電腦病毒的定義與有關名詞解釋。

二、 不使用參考資料，你能夠以你自己的話正確地說出電腦病毒的分類。

三、 不使用參考資料，你能夠以你自己的話正確地說出電腦病毒感染的途徑與如何防制電腦病毒。

四、 不使用參考資料，你能夠以你自己的話正確地操作防毒、偵毒與解毒的步驟。

假如你認爲能夠勝任以上學習目標的能力，請翻至第 41 頁做測驗。假如你需要更多學習的話，請翻到第 4 頁

學習活動

本講義之學習活動分二部份：(1)相關知識，(2)實際操作。在實際作偵毒、解毒操作之前，我們必須事先學習與偵毒、解毒操作有關之知識，你可以由閱讀本教材之第 5 頁至第 26 頁去學習，至於有關偵毒、解毒操作的技巧，則請閱讀本教材之第 27 頁至第 37 頁去學習。

請翻至第 5 頁

本教材的第一個學習目標是：

不使用參考資料，你能夠以你自己的話正確地說明電腦病毒的定義與有關名詞解釋。

把握今天，充實明天，
珍惜現在，創造未來。

請翻至第 6 頁

壹：電腦病毒的定義與有關名詞解釋

有鑑於一般電腦用戶對於電腦病毒仍然『一知半解』，或是飽受電腦病毒侵擾，天天重建資料而苦不堪言，因此筆者在此作一有系統的整理，期能使大家對電腦病毒有更深一層的認識，同時知道如何防毒、偵毒與排除等的操作，以求學會相關防制之道。

現將電腦病毒的定義與有關名詞解釋列述如下：

1、 電腦病毒 (Computer Virus)

乃是指一組被精心設計的程式，具有『自行複製繁殖』的能力，它附著於作業系統的開機磁片或其他軟體程式，以進入電腦記憶體內。在潛伏期間不斷地伺機修改磁片或程式，以進行『感染』的工作，待發作時期一到，便執行某種程序來破壞資料檔案，同時干擾整個電腦系統的運作。

2、 潛伏 (Concealing)

病毒的程式碼存在磁片或程式中，但尚未被使用者或系統將之載入，也可以稱爲『被感染』 (Infected) 。

3、 活化 (Active)

病毒程式被使用者或系統從潛伏部位載入電腦內，開始發揮作用的期間稱之。

4、 感染 (Infecting)

病毒程式對磁片或程式軟體進行修改複製的工作，使之帶有病毒程式碼而成爲帶原者。

5、 蟲 (Bug)

一種造成系統或程式不正常運作現象的錯誤或原因，它可能是硬體上的問題或程式設計上『有意』或『無意』的缺失。Bug 程式與 Virus 病毒程式最大的分別在於 Bug 沒有繁殖傳染的能力，而 Virus 病毒程式有感染的能力。

6、 磁碟片啓動磁區 (Boot Sector)

位於磁碟片最外側第 0 面第 0 軌的第一號磁區，電腦將 Boot Sector 讀入記憶體內，再由 Boot Sector 程式把整個作業系統的其他部份載入。

請翻至第 7 頁

7、 硬碟分割區域管理表 (Hard Disk Partition Table)

簡稱硬碟分區表 (Partition Table),位於硬碟磁盤最外側第 0 面第 0 軌的第一號磁區，記錄著各種作業系統分割區大小、位置與可啓動的分區。

8、 檔案配置表 (File Allocation Table ；FAT)

MS DOS (OS/2)作業系統在磁片或硬碟內所預留的一塊區域，用來指示檔案的空間配置情形，分佈在那些磁區，爲整個儲存媒體(磁碟片、硬碟)最重要的部份之一。FAT 表一旦被毀，整張磁碟片或硬碟內的所有資料將因 DOS 找不到正確的存放位置而無法存取。

9、 系統中斷向量表 (System Interrupt Vector Table)

位於位址 0000 : 0000 ~ 0000 :03FF，存放許多重要的硬體介面處理程式或軟體處理程式的進入點。絕大多數病毒以修改此處達到控制 PC 的目的。

10、 常駐記憶體程式 (Terminated and Stayed Resident ； TSR Program)

一種進入記憶體後可留存下來的程式，經使用者以熱鍵(Hot Key)或軟體中斷來啓動此程式，發揮該特殊功能服務，或改進擴充整個作業系統的功能。

請翻至第 8 頁

學習評量一：

一、請不要用參考資料或書籍，試解釋下列各相關名詞。

1. 潛伏(Concealing)：
2. 感染 (Infecting) ：
3. 蟲 (Bug)：
4. 磁片啓動磁區(Boot Sector)：
5. 檔案配置表(File Allocation Table ；FAT)：

請翻至第 9 頁

筆 記 欄

請翻至第 10 頁

學習評量─答案：

一、請不要用參考資料或書籍，試解釋下列各相關名詞。

1. 潛伏(Concealing)：
2. 感染 (Infecting) ：
3. 蟲 (Bug)：
4. 磁片啓動磁區(Boot Sector)：
5. 檔案配置表(File Allocation Table ；FAT)：

(你的答案請參考本書第 6 頁至第 7 頁的說明。)

請翻至第 11 頁

本教材的第二個學習目標是：

不使用參考資料，你能夠以你自己的話正確地說出電腦病毒的分類。

請翻至第 12 頁

壹：電腦病毒的分類

一、 美國病毒防治協會將所有電腦病毒的種類大致區分爲下列數種：

(一)、啓動磁區感染者 (Boot Sector Infector)

潛伏在啓動磁區的病毒。當使用者用已中毒的磁碟片開機時，啓動磁區的程式因爲已遭病毒修改，會把病毒程式先載入記憶體內，使病毒活化，開始發揮作用。

(二)、程式檔病毒 (Program Infector)

是潛伏在程式中，當使用者執行了已中毒的程式，便使病毒活化，開始作怪。例如『十三號星期五病毒』即屬之。例如(c)Brain 大腦病毒、 Disk Killer 磁碟殺手 、Stoned Virus 石頭病毒 …等均屬之。

(三)、作業系統感染者 (System Infector)

潛伏在作業系統程式中 (如 MS – DOS 的 IO.SYS MSDOS.SYS 與 COMMAND.COM 開機檔案) 的病毒。著名的有專門感染 COMMAND.COM 檔的 Lehigh 病毒。

(四)、混合型感染者 (Mixed Infector)

病毒同時修改磁片的啓動磁區與程式檔案，增加電腦中毒的機會。例如『塑膠炸彈 (Plastque Bomb) 病毒 』 (俗稱 『大榔頭』 病毒)。

此外，磁片的 Boot Sector 或程式同時被兩種以上的病毒入侵，這兩種(以上)的病毒並不互相衝突時，使得中毒的磁片一開機或中毒的程式一執行，此時 N 種病毒同時進入電腦內，彼此各感染各的互不侵犯，這種感染方法稱爲多重感染(Multilayer Infecting)，我們也可以稱這些病毒爲『複合病毒』(Complex and Combined Virus)。

請翻至第 13 頁

二、 若依病毒的破壞性大體上可分爲下列數種：

(一)、良性病毒：

這種病毒大多只具有感染與複製的能力，可能是病毒設計者『做試驗用的』，看看它能傳播多遠多廣。

(二)、頑皮性病毒：

大體上而言這一型的病毒並沒有任何破壞力，只不過會開開使用者的玩笑，妨礙使用者的工作；如『兩隻老虎』在發作時會不斷地哼著『走音』的『兩隻老虎』的音樂。

(三)、惡性病毒：

這些病毒可不好惹。它會先潛伏一段時間，等待時機成熟後就開始突擊，殺得使用者措手不及。至於惡性病毒的破壞威力可分下列四種程度：

1. 干擾系統運作，破壞使用者使用電腦的信心。

2. 針對某些特定對象，作『重點式』的破壞。
例如著名的『十三號星期五』病毒發作時，它將會殺掉你正要執行的程式。

3. 毀掉整張磁片或整部硬碟的資料。
例如著名的『Disk Killer』入侵你的電腦 48 小時之後，就顯示一段 Disk Killer V1.0 PROCESSING 的訊息，然後你硬碟內所有資料就全部被毀了。

4. 破壞毀損硬體週邊設備或減少它們的壽命。
或許有的人認爲軟體不可能破壞硬體，但事實並非如此，許多可程式設定的硬體，光是人爲操作的不當或軟體設計的錯誤，就可導致硬體的損毀，又何況『精心設計』的電腦病毒程式呢?

請翻至第 14 頁

貳：電腦病毒傳播的媒介

前面提到美國病毒防治協會將所有電腦病毒的種類大致區分爲下列四種：

一、啓動磁區感染者 (Boot Sector Infector)

二、程式型病毒 (Program Infector)

三、作業系統感染者 (System Infector)

四、混合型感染者 (Mixed Infector)

第一種『開機型病毒』的感染媒介是磁碟片 (正確的說法應是磁碟片上的 Boot Sector，因爲一張磁碟片上只有一個 Boot Sector，所以磁片開機型病毒只對該磁片做一次感染的動作。)

第二種『程式型病毒』的感染媒介是程式，病毒會主動或被動地感染未中毒的程式，一張磁碟片中若存在好幾個程式，就可能都被感染了。

第三種『作業系統感染者病毒』與第四種『混合型感染病毒』的感染媒介可能是磁碟片或是程式，甚至於兩者一起來。

參：電腦病毒入侵的步驟與解決之道

一、 啓動磁區感染的開機型病毒 (Boot Sector Infector)

一般而言，只要不用中了開機型病毒的磁碟片開機，開機型病毒就無法進入電腦內潛伏，伺機感染其他磁片；那麼中了開機型病毒的磁碟片又該如何復原呢?在此提供下列三種方式供作參考：

1. 將該磁碟片上仍可使用的檔案備份下來，然後重新 Format (當然你必須確定電腦內部沒有任何病毒，且 Format.com 也沒問題才行)。

2. 研究該開機型病毒，把原來的 Boot Sector 讀出來，寫回正確位置，順便將病毒所做出來的 Bad Clusters (損壞磁區集合)改爲自由使用(可用 DEBUG、SYMDEB 或 TD 等偵錯工具程式執行)。

請翻至第 15 頁

3. 利用 DOS 的外部指令 SYS，製造一份新的 Boot Sector 寫回去。

註：以上第 2、3 項方法稱爲『砍頭法』，只要將正確的 Boot Sector 寫回正確位置，也就是說把病毒的 Boot Sector 給蓋掉，病毒的載入部份被毀，自然失去作用。

★ 解決開機型病毒的注意事項：

1. 市面上一般治療開機型病毒的解毒程式，就是利用上述第二道步驟，如果你的磁片中了變種病毒或新病毒，原本的 Boot Sector 存放位置就不一樣，而解毒程式笨笨的讀一個磁區就寫回去，導致磁片解毒後將無法開機的窘境，請多加注意。

2. 有些解毒程式會對磁碟片的 Boot Sector 做一 Virus Label，萬一遇到病毒要感染時，一檢查到有它的 Label，就以爲該磁碟片已感染過了，於是不再感染，而使該磁碟片逃過一劫，這種『欺騙式的防毒疫苗』遇到新病毒或變種病毒時還是無效，而較差一點的解毒程式一檢查到該磁碟片上的『病毒疫苗記號』時，還真以爲中了病毒，而隨便依照公式將某一磁區當 Boot 磁區寫回去，不是解壞了就是不斷顯示該磁片已中毒，不斷的重覆解毒動作而把磁碟片磨壞了，請謹慎小心。

★ 解決開機型病毒的參考步驟：

1. 若中了開機型病毒時，先檢查該中毒磁片上有沒有原始 Boot Sector 的備份，有的話直接以備份的 Boot Sector 寫回，如果沒有原始 Boot Sector 備份的話，就請參考第二項的操作。

2. 以復原中毒磁碟片的第二種方法依已知的病毒種類逐一檢查，若有發現開機型病毒時，此時解毒程式將詢問你，要不要爲這一磁碟片製造一個新且正確的 Boot Sector 並寫回去(此時通常回答『要』)，最後還幫你磁碟片上的啓動磁區做一備份，不但能完全解毒，亦不怕新的開機型病毒入侵。

請翻至第 16 頁

二、 程式型病毒 (Program Infector)

程式型病毒顧名思義就是附著在可執行程式檔案中的病毒，在 MS-DOS 中，可執行程式檔分爲兩種：第一種是 COM 檔，第二則是 EXE 檔。

一般而言，除非程式型病毒要刻意破壞程式，或爲了不增加中毒程式的長度，將病毒程式碼直接覆蓋到受害程式的本體，不然通常程式型病毒會保留原程式的一部份，所以只要 COM 檔被病毒感染，一般而言其長度一定變大。

★ 解決程式型病毒的參考步驟：

1. 只要不執行中毒的程式，程式型病毒也無法溜進電腦內，而去感染其他的程式。

2. 至於中了毒的程式該如何復原呢?

(1). 若你有針對該程式有作備份的檔案，此時可在確定電腦沒有中毒的情況下 COPY 回去。

(2). 以解毒程式針對該中毒檔案進行還原的工作，不過因爲遇到該病毒的變種機會也不小，還原公式也有所變動，套用原先的公式會出錯，再加上有些病毒感染某程式檔時已破壞了一部份，這種毒發身亡的程式是救也救不回來乾脆予以 Delete 掉。通常解毒程式治療程式型病毒的成功率在 95%~70%之間，其治癒率會隨程式出來的時間增長而慢慢降低。

(3). Internal Overlay 的 EXE 檔萬一感染到程式型病毒時，則在第一份模組之後的第二份模組會被病毒碼覆蓋而毀損，所以 Internal Overlay EXE 檔一旦中毒是鐵定無解的，只能 Delete 掉並重新拷貝原版的程式檔。

請翻至第 17 頁

三、 作業系統病毒 (System Infector)和混合型病毒 (Mixed Infector)

像 System Infector 與 Mixed Infector 型病毒，其感染方式與上述兩者一致，不是感染 Boot Sector 就是 COM 與 EXE 檔，其解毒步驟亦需雙管齊下，同時還原中毒的 Boot Sector 與程式才行，此處就不多說了。

請翻至第 18 頁

學習評量二：

一、請不要用參考資料或書籍，試述美國病毒防治協會將所有電腦病毒的種類大致區分爲那幾種。

二、請不要用參考資料或書籍，試述若從病毒的破壞性來區分，電腦病毒的種類大致可區分爲那幾種。

三、請不要用參考資料或書籍，試述惡性病毒的破壞威力可分爲那四種程度。

請翻至第 19 頁

筆 記 欄

請翻至第 20 頁

學習評量二答案：

一、 請不要用參考資料或書籍，試述美國病毒防治協會將所有電腦病毒的種類大致區分爲那幾種。

(你的答案請參考本書第 12 頁的說明。)

二、 請不要用參考資料或書籍，試述若從病毒的破壞性來區分，電腦病毒的種類大致可區分爲那幾種。

(你的答案請參考本書第 13 頁的說明。)

三、 請不要用參考資料或書籍，試述惡性病毒的破壞威力可分爲那四種程度。

(你的答案請參考本書第 13 頁的說明。)

請翻至第 21 頁

本教材的第三個學習目標是：

不使用參考資料，你能夠以你自己的話正確地說出電腦病毒感染的途徑與如何防制電腦病毒。

請翻至第 22 頁

壹：電腦病毒感染的途徑與如何防制電腦病毒

由於電腦病毒的多樣化及多變化，造成電腦使用者人人自危，也造成電腦使用者不小的損害，因此瞭解電腦病毒傳播感染的路徑及如何防制電腦病毒實為首要之務，現茲將一般電腦病毒感染的路徑暨如何防制電腦病毒的方法列示如下：

▼ 一般電腦病毒感染的路徑：

一、 使用中毒或來路不明的磁碟片開機(Boot Sector Infector ；開機磁片型病毒)。

二、 執行了帶毒或來路不明的程式軟體(Program Infector ；程式型病毒)。

三、 連接區域性網路(Local Area Network ；LAN)的個人電腦因某一部 PC 中毒，彼此傳遞程式，而導致整個網路上每部 PC 皆感染中毒。

四、 部份程式遭『有心人士』修改，再加入病毒之後散佈出去，而這些程式又被他人拷貝輾轉流傳到使用者手上，這也是助長病毒擴散的原因之一。

五、 有些軟體設計師為了防止他們的心血遭人『剽竊』(尤其是專愛破解保護的高手)，為維護自身的利益與懲罰這種不尊重『智慧財產權』的非法複製行為，在寫入程式時便加入了病毒；一旦使用者私自複製給別人使用或進行破解的工作，程式就會將病毒釋放出去，破壞盜拷者或破解者的電腦，這也是助長病毒擴散的原因之一。

▼ 如何防制電腦病毒的方法：

為剋制電腦病毒，軟體公司紛紛推出解毒軟體(包括防止病毒入侵的偵測程式與解毒程式)，然而新的病毒或變種病毒肯定會一直出現，因此使用者應保持警覺、小心，並留意電腦內不尋常的舉動，若是要期待一種能防止所有病毒入侵的疫苗與解所有病毒的萬靈丹，則是一種不可能也不實際的想法。因此個人提供下列方法供作防制電腦病毒的參考：

請翻至第 23 頁

一、 尊重智慧財產權，使用原版合法軟體，不使用盜拷或來路不明的軟體。

二、 平時磁碟片不存入資料時，請設定在防止寫入的狀態或貼防寫貼紙。

三、 極爲重要的程式、資料，請常做『備份』，不怕一萬，只怕萬一。

四、 預備兩三片確定無毒的系統開機片，並貼上防寫貼紙。當你覺得目前系統有問題時，請關掉電源，重新以這些磁片開機，並將 DOS 重新安裝到硬碟上。
如：
A:>SYS C:
A:>COPY COMMAND.COM C:\

五、 請多留意磁片的 Boot Sector 、FAT 表；程式檔之 (*.COM & *.EXE) 檔案長度、建檔日期、時間及檔案屬性是否有異常變動，若有此情況請提高警覺。

六、 請多留意電腦運作的狀況，對異常現象須特別留意，如電腦執行速度變慢，讀寫磁片或硬碟的速度慢了，磁臂有異常拉動的現象或螢幕突然消失、反白，甚至出現不該有的訊息，萬一發生了，請先熟記發作情形，然後迅速『關機』 (不可以只按 Reset 鍵或按 Ctrl – Alt – Del 重新啓動)，重新以無毒磁片啓動。

七、 請隨時檢查目前 PC 記憶體分佈情形，注意是否有不明的程式佔用。

八、 對於有問題的程式，最好先在只有軟碟的 PC 上執行幾次看看，或使用工具程式將硬碟設爲防寫或隔離。

請翻至第 24 頁

九、 購買原版合法的偵測防毒與解毒的工具程式，以求有備無患。

十、 隨時留意雜誌等傳播媒體有關最新病毒的報導，以提早防範。

請翻至第 25 頁

學習評量三：

一、請不要用參考資料或書籍，試述電腦病毒傳播感染的途徑有那幾種。

二、請不要用參考資料或書籍，試舉出五種防制電腦病毒的方法。

請翻至第 26 頁

學習評量三答案：

一、請不要用參考資料或書籍，試述電腦病毒傳播感染的途徑有那幾種。
(你的答案請參考本書第 22 頁的說明。)

二、請不要用參考資料或書籍，試舉出五種防制電腦病毒的方法。

(你的答案請參考本書第 22 頁至第 24 頁的說明。)

請翻至第 27 頁

本教材的第四個學習目標是：

不使用參考資料，你能夠以你自己的話正確地操作防毒、偵毒與解毒的步驟。

請翻至第 28 頁

壹：MS-DOS 的防毒功能

由於電腦病毒的感染所造成的損失愈來愈爲嚴重，因此預防電腦病毒的工作更是大意不得，因此 MS-DOS 版提供了 Microsoft Anti-Virus(簡稱 MSAV)的防毒程式，包括 MSAV.EXE(DOS 版)及 MWAV.EXE(MSAV 的 Windows 版)二個程式外，MS-DOS 尚提供 VSafe 的輔助程式，讓使用者不必添購其他防毒軟體，即已具有掃毒、防毒的利器了。同時市面上亦有其他掃毒防毒軟體不勝枚舉，諸如 ZLOCK、 PC - CILLIN……等軟體均屬之，現茲將 MS-DOS 提供防治病毒的方式簡述如下，務期受知名或不知名病毒感染的機率降至最低，同時使你的電腦可以得到更多一層的保障。

▼ 以 Vsave 來監督程式是否不正常地常駐，並建立各程式檔之 CHECKSUM，以檢查程式檔是否被更動。

▼ 以 Vsave 可防止硬碟被寫入，以抑制不知名病毒的傳染；Vsafe 還可以防止硬碟被低階格式化、限制啓動磁區被更改，以防止病毒之發作及感染。

▼ 以 MSAV 程式利用病毒識別碼掃瞄並清除已知的各類型病毒。

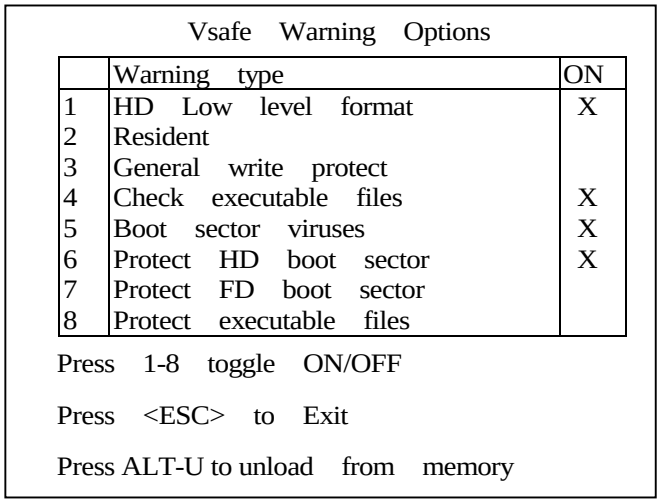
貳：Vsafe 偵毒、防毒程式

Vsafe 是一個常駐的防毒程式，Vsafe 常駐後，每當程式執行時，Vsafe 就會檢查該程式檔是否遭病毒感染。在防範不知名病毒方面，其功能算是相當完備，包括：防止低階格式化、監督程式常駐、磁碟防寫保護、檢查可執行檔等，乃至平常 COPY 檔案時，Vsafe 都會將被 COPY 的檔案一一過濾以檢查是否有病毒存在。

Vsafe 的使用相當簡單，只要在 DOS 下直接執行 Vsafe 即可，使用者可以由 CONFIG.SYS 以 INSTALL=C:\DOS\VSAFE.COM 或在 AUTOEXEC.BAT 中執行之，使得每

次開機後 Vsafe 即已常駐，以提供更徹底的病毒防護系統，當 Vsafe 常駐時，你只要按下 Alt V ，則 Vsafe 立即顯示出如下圖 0904-1 的視窗：

請翻至第 29 頁



Vsafe Warning Options

	Warning type	ON
1	HD Low level format	X
2	Resident	
3	General write protect	
4	Check executable files	X
5	Boot sector viruses	X
6	Protect HD boot sector	X
7	Protect FD boot sector	
8	Protect executable files	

Press 1-8 toggle ON/OFF

Press <ESC> to Exit

Press ALT-U to unload from memory

圖 0904-1

在此視窗中使用者可以按數字鍵 1-8 來選用 Vsafe 的八項主功能，被選用的功能會在 ON 的項目下會顯示 X 的符號。現將此八項主功能的用途簡述如下：

一、HD Low level format 防止硬碟被低階格式化(預設爲 ON)

當病毒企圖以低階格式化摧毀硬碟時，Vsafe 會將其攔截，並顯示：”Program is trying to format Hard disk”(此程式企圖格式化硬碟)以詢問使用者是否要停止(Stop)、繼續(Continue)或重新開機(Boot)。

二、Resident 監督程式常駐(預設爲 OFF)

當任何程式要常駐時(病毒或一般常駐程式如：中文系統)，Vsafe 會顯示訊息，並詢問使用者要停止(Stop)、繼續(Continue)或重新開機(Boot)。

三、General Write Protect 磁碟防寫(預設爲 OFF)

當程式企圖寫入軟硬碟時，Vsafe 會詢問使用者是否要讓此寫入動作繼續，若使用者不允許而選擇停止(Stop)，則系統會顯示 Write Protect(防寫)之訊息，且此寫入動作會失敗。本功能可用以防止未知病毒的傳染，但在執行一些會寫入硬碟的程式時(如 Windows)會產生錯誤，此時必須將此功能設爲 OFF。

四、Check executable files 檢查可執行檔(預設爲 ON)

本功能是用於設定可執行檔在以其他方式開啓時，像 COPY、MOVE 時是否要檢查。

設爲 ON，則在 COPY 等過程中，發現該檔案被病毒感染，會顯示警告訊息並出現詢問窗，讓使用者決定是否要進行此 COPY 動作。

請翻至第 30 頁

五、Boot sector viruses 檢查啓動區是否有病毒(預設爲 ON)

此項功能設定爲 ON 時，Vsafe 會找機會檢查啓動磁區是否有病毒，例如執行 DIR 命令時，Vsafe 會趁機檢查啓動磁區是否感染了病毒，磁碟啓動磁區的檢查也是使用比對病毒特徵碼的原理，因此設此選項爲 ON 會使磁碟讀取的速度降低，而且已知的病毒特徵碼愈多，磁碟的速度就愈慢。

六、Protect HD boot sector 保護硬碟啓動磁區(預設爲 ON)

防止硬碟啓動磁區被其他程式寫入。本功能亦能在程式企圖寫入硬碟分割表時，顯示訊息詢問使用者是否要將其制止。

七、Protect FD boot sector 保護軟碟啓動磁區(預設爲 ON)

防止軟碟的啓動磁區被寫入。

八、Protect executable files 保護可執行檔(預設爲 ON)

每當執行檔被更動時，Vsafe 就會警告使用者，並詢問是否要繼續；本功能並非能百分之一百保護檔案，許多非法手段仍能更改檔案。

▼ 如何解除 Vsafe 的常駐

按下 Alt V 顯示 Vsafe 功能設定視窗後，我們可以按下 Alt U 將 Vsafe 由記憶體中移除，即解除 Vsafe 的常駐。

▼ Vsafe 的命令列參數

按下 Alt V 顯示 Vsafe 的八大功能，亦可由命令列來設定，其格式如下所述：

VSAFE / 參數

其中參數的內容與功能如下所述：

- / 1[±] ~ / 8[±] 設定第 1-8 項功能爲 ON(加號)或 OFF(減號)，例如設 1、3、5、7 項功能爲 ON，2、4、6、8 項爲 OFF，則應執行

Vsafe /1+ /2- /3+ /4- /5+ /6- /7+ /8- 按下<Enter>鍵

- /NE 不使用擴展記憶體(Expanded Memory)

請翻至第 31 頁

• /NX　不使用延伸記憶體(Extended Memory)

• /AK 、 /CK　設定熱鍵以顯示 Vsafe 的八大功能設定。其中 K 爲我們所要指定的按鍵，系統預設爲 Alt V ，例如想更改爲 Alt F 則加入 /AF 的參數；若想設爲 Ctrl V 則加入 /CV 參數。

• /D　不檢查 checksum，即不開啓 chklist.ms 或增加其內容。

• /N　執行 Vsafe 後會載入網路驅動程式，則需使用此參數。

• /U　解除 Vsafe 常駐；按下 Alt V 叫出 Vsafe 設定視窗，再按下 Alt U 亦可解除 Vsafe 的常駐。

▼ Vsafe 的注意事項

一、 Vsafe 防止病毒低階格式化的先決條件，是必須在病毒被載入記憶體常駐之前啓動才有效，如果遇到開機型病毒，且一啓動就開始低階格式化，此時 Vsafe 是無法制止的。

二、若先執行 Vsafe 後，再執行倚天中文系統，按下 Alt V 顯示功能表設定視窗的熱鍵有時會失效，但 Vsafe 仍保持其警戒狀態。若是先執行倚天中文系統再執行 Vsafe 的話，在中文模式下，按下熱鍵後再將中文系統切到英文模式(按 ctrl alt a)，Vsafe 的功能設定視窗才會出現。

三、在 CONFIG 檔以 INSTALL=C:\DOS\VSAFE.COM 的方式執行 Vsafe 的話，因爲此時

Vsafe 是比 command.com 檔更早執行，所以在 COMMAND.COM 未結束前則是無法

解除 Vsafe 的常駐，但 COMMAND.COM 檔是永遠不會結束的，所以 Vsafe 就不可

能解除常駐了。

請翻至第 32 頁

參：MSAV 掃毒、解毒程式

MSAV.EXE 能對整個磁碟進行病毒的偵測與清除，除此之外還附有病毒名冊，使用者可查知所有已知病毒的名單及其感染的大概症狀，要執行 MSAV 只要在 DOS 下鍵入如下的字串即可：

C:\>MSAV　按下 ENTER 鍵

螢幕上立即顯示 MSAV 的視窗，如圖 0904-2 所示，同時進行工作目錄結構的掃瞄，MSAV 共有五大功能選項，分別是 Detect、Detect & Clean 、Select new drive 、Options 及 Exit，現茲將各選項功能敘述如后：

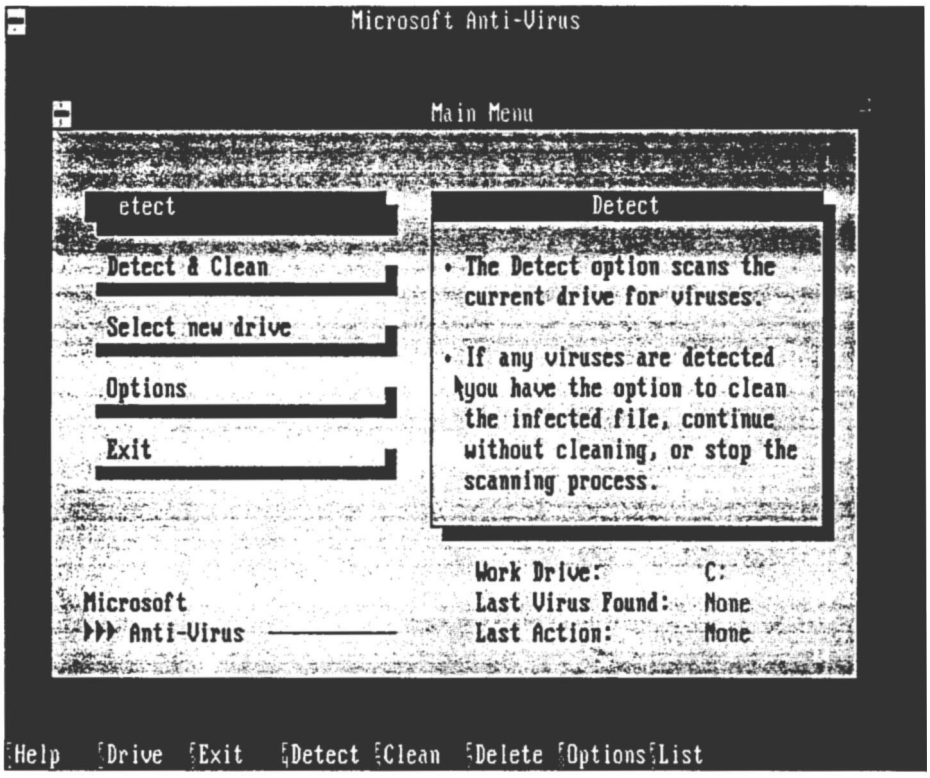


圖 0904-2

一、Detect F4 ：偵測目前工作磁碟上的病毒

當執行 MSAV 的防毒偵測時，首先會先偵測記憶體，看有無病毒存在，且會顯示完成的百分比。開始偵測時，也會顯示所完成目錄個數的比例及目錄中已偵測檔案的比例，如圖 0904-3 所示的畫面。

當 MSAV 發現病毒時，則會出現如下的對話盒，如圖 0904-4 所示的畫面。

請翻至第 33 頁

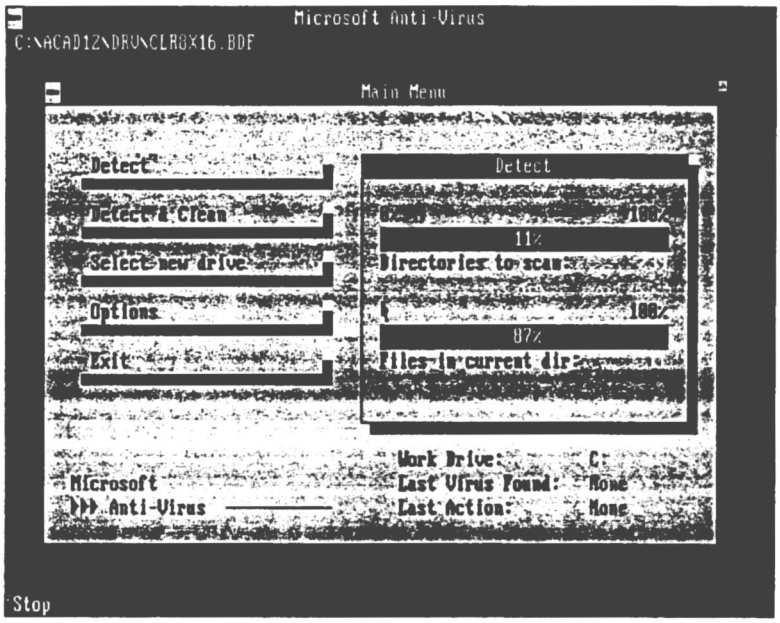


圖 0904-3

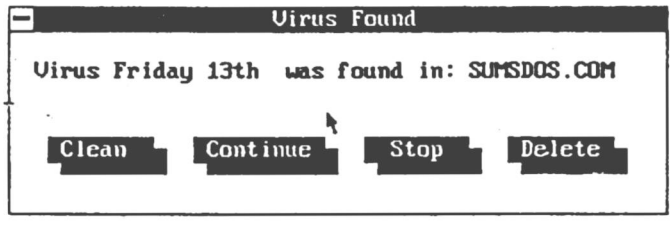


圖 0904-4

此時使用者可選擇如下的功能：

(一)、Clean ：清除病毒。

(二)、Continue ：不清除病毒而繼續偵測的動作。

(三)、Stop ：停止本次的偵測動作。

(四)、Delete：刪除該中毒檔案。

當 MSAV 發現檔案的屬性日期時間大小或 Checksum 不合的話，則會出現如下的對話盒，如圖 0904-5 所示的畫面：

請翻至第 34 頁

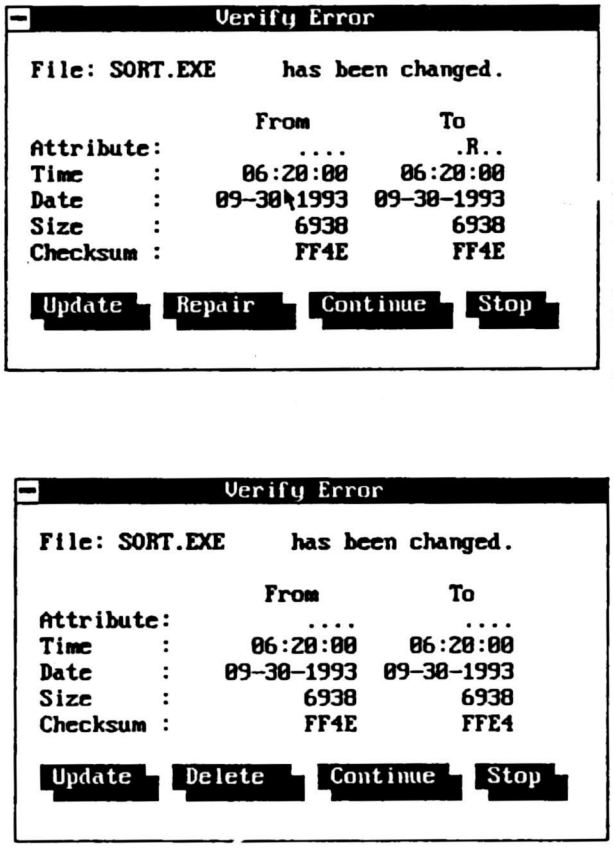


圖 0904-5

此時使用者可選擇如下的功能：

(一)、Update：若使用者確認這個改變是合法的，可選 Update 將 CHKLIST.MS 檔的內容更新。

(二)、Repair：若只是屬性日期時間的改變，可選 Repair 將之修復。

(三)、Delete：若是有其他的變化則可能是已遭病毒感染，此時的 Repair 作用鈕會變成 Delete 鈕，此時無法修復該檔而只能刪除該檔案。

(四)、Continue：繼續偵測。

(五)、Stop ：立即停止偵測行動。

二、Detect & Clean F5 ：偵測並清除工作磁碟上的病毒

此功能與 Detect 功能相似，但若偵測到電腦病毒時，此時會立即將該病毒予以除掉，而不像 Detect 還會顯示詢問訊息，且無論是否有發現病毒均會顯示報告畫面。

請翻至第 35 頁

三、Select new drive F2 ：選擇新工作磁碟機

選擇本功能會在螢幕左上方顯示磁碟機的名稱供使用者選用，選定新磁碟機後，MSAV 便會讀取新磁碟的資料，並設爲工作磁碟。

四、Options F8 ：設定偵測病毒時的各種執行狀態

選擇此功能項時會出現一狀態選項對話盒，如下圖 0904-6 所示之畫面：

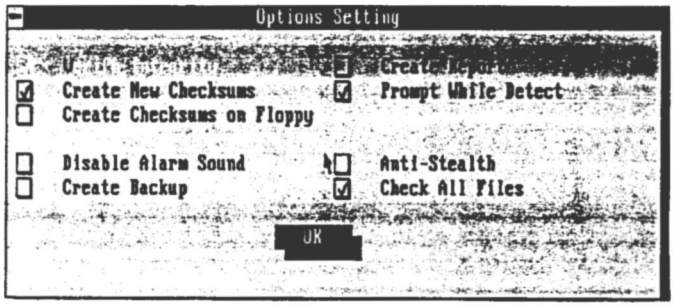


圖 0904-6

現茲將各功能選項的內容簡述如下：

(一)、Verify Integrity ：

當本項功能設定爲 ON 時，每次偵測病毒時就會將執行檔與 CHKLIST.MS 檔記載的內容作比較，以確定檔案的完整性，有助於防範不知名病毒。

(二)、Anti – Stealth ：

當本選項與前項功能均設爲 ON 時，MSAV 會以較複雜的演算法來查驗檔案是否遭隱藏型病毒所感染，如此偵測所花的時間也會較久，但更爲精確。

(三)、Create New Checksums ：

每次執行偵測後就建立新的 CHKLIST.MS 檔。

(四)、Create Checksums on Floppy：

設定在偵測軟碟時，亦建立 CHKLIST.MS 檔，MSAV 的預設是只在硬碟上執行才建立。

請翻至第 36 頁

(五)、Check All Files ：

設定要檢查所有的檔案，若此選項被設定爲 OFF 的狀態，則 MSAV 只偵測可執行檔，只要副檔名符合以下其中之一，即被視爲可執行檔：如 EXE、COM、 DLL、OVL、OVR、OV?、SYS、BIN、APP、PGM、PRG、DRV、386、FON 及 CMD。

(六)、Disable Alarm Sound ：

當 MSAV 發現到病毒或是檔案的 Checksum 與 CHKLIST.MS 檔所記載的不同時，就會發出一串警告聲音及一對話盒，以詢問使用者要採用何種步驟。

若本功能項被設定爲 ON 時，則發生上述情形時則只會顯示該對話盒而不會發出聲音。

(七)、Create Backup ：

MSAV 在發現檔案被病毒感染時，會設法將該病毒消滅，使檔案恢復原狀，則該檔會被 MSAV 所破壞而無法使用。若本功能設爲 ON，則會將檔案以.VIR 爲副檔名預存一份，當 MSAV 把檔案修壞時，使用者可用 REN 命令將.VIR 改回原來的副檔名以救回檔案。但使用者千萬要記得，這些.VIR 檔案極可能是含有劇毒的檔案，確定 MSAV 修復的檔案可正常執行後，儘快將.VIR 的檔案刪除。

(八)、Create Report ：

讓 MSAV 在每次執行後都在磁碟根目錄中建立 MSAV.RPT 報告檔，這個報告檔只記載該磁碟最近一次執行 MSAV 的時間及偵測到的開機型病毒、檔案型病毒名稱、被感染的檔案名稱、消滅掉的數量。只要將這個選項設定爲 ON，則執行 MSAV 的各項主要功能時，便會建立 MSAV.RPT 這個檔，並存於工作磁碟的根目錄下，使用者可自行以文書編輯程式來觀察 MSAV.RPT 的內容。

(九)、Prompt while Dected ：

設定 MSAV 在偵測到病毒或是發現 checksum 有問題時，是否要顯示對話盒供使用者選擇。若設 OFF 的話，當我們發現病毒時，此時使用者無法選擇 Continue、Stop 之類的處理行動。

四、Exit F3 ：離開 MSAV

每次以 ESC F3 等方式離開 MSAV 時，MSAV 都會提示如下圖 0904-7 的對話盒：

請翻至第 37 頁

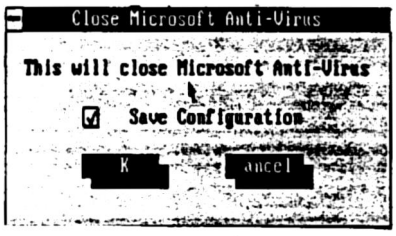


圖 0904-7

其中的 Save Configuration 選項設爲 ON 時(可按 S 鍵切換)表示要將目前的設定存起來，下次進入時，MSAV 即會依此設定來進行其偵測動作，設定好後再按 ENTER 或選 OK 鈕確認離開 MSAV。

▼ MSAV 的命令列參數

MSAV 亦可由命令列來設定，其格式如下所述：

MSAV [磁碟機名] [路徑名稱] [參數]

其中參數的內容與功能如下所述：

- /S 掃瞄所指定的磁碟或路徑中的檔案是否感染病毒。
- /C 偵測並清除所指定的磁碟或路徑中的檔案。
- /R 設定要產生 MSAV.RPT 報告檔。
- /A SCAN 除了 A: B:之外的所有磁碟(含網路磁碟)。
- /L SCAN 除了 A: B:之外的所有 Local drive。
- /N 抑制畫面顯示，使用此參數時只會看到 Working …的訊息及正被偵測中的檔案名稱。
- /P 加上此參數時不會進入 MSAV 畫面，只會以文字來顯現所有的訊息。
- /F 本參數需與 N 或 P 參數合用，使用此參數會連正被偵測中的檔名都不顯示。
- /VIDEO 列出 MSAV 各種顯示模式參數。

請翻至第 38 頁

學習評量四：

一、請不要用參考資料或書籍，試簡述 MSAV 解毒的五項功能內容。

二、請不要用參考資料或書籍，試簡述 Vsafe 的八大功能項目內容。

請翻至第 39 頁

筆 記 欄

請翻至第 40 頁

學習評量四答案：

一、請不要用參考資料或書籍，試簡述 MSAV 解毒的五項功能內容。
(你的答案請參考本書第 32 頁至第 37 頁的說明。)

二、請不要用參考資料或書籍，試簡述 Vsafe 的八大功能項目內容。

(你的答案請參考本書第 28 頁至第 30 頁的說明。)

請翻至第 41 頁

學後評量

一、請不要用參考資料或書籍，試解釋下列各相關名詞。

1. 電腦病毒(Computer Virus)：
2. 硬碟分割區域管理表 (Hard Disk Partition Table) ：
3. 活化 (Active)：
4. 系統中斷向量表 (System Interrupt Vector Table)：
5. 常駐記憶體程式 (Terminated and Stayed Resident ； TSR Program)：

二、請不要用參考資料或書籍，試述解決開機型病毒的參考步驟：

三、請不要用參考資料或書籍，試舉出五種防制電腦病毒的方法。

四、請不要用參考資料或書籍，試簡述 MSAV 解毒的五項功能內容。