GOTOP

電腦病毒診斷及治療

碁峰資訊 工具軟體系列叢書

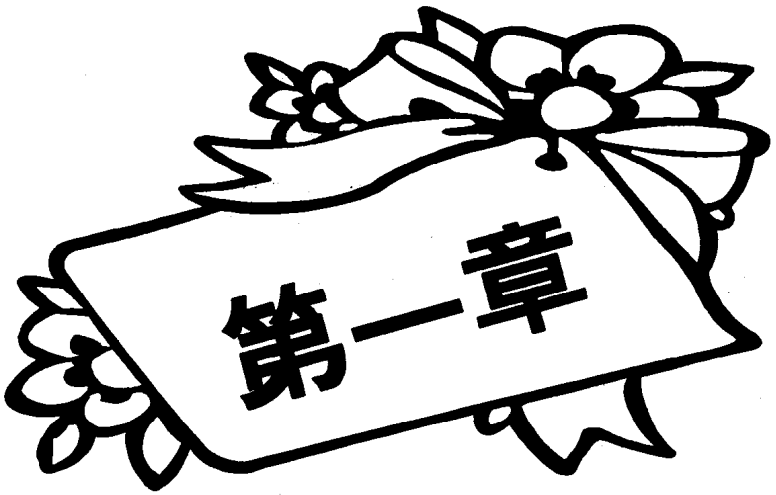
張寶源

電腦病毒之診斷及治療

張寶源

碁峰資訊股份有限公司 印行

目 錄



DOS 的基本觀念

1-1 軟碟的啓動

當電腦開始啓動時，CPU 被 RESET,CS 和 IP 值被設定爲 ROM BIOS 的起始位址，即 CS = FFFF，IP = 0000。該處有一跳躍指令，系統就跳到 START 處開始做一些如 RAM，磁碟機，螢幕，和鍵盤的檢查。接著便讀取磁片之 Boot 磁區，將它載入到 0000:7C00 的地方，此時控制權便交給 Bootstrap。這時 Bootstrap 會檢查根目錄中是否有 IO.SYS 和 MSDOS.SYS 兩個隱藏檔。若有便將 IO.SYS 載入並建立 Disk Base 表，並修改 INT 1EH 的位址。完成初始化之後，便將 MSDOS.SYS 讀入，由 MSDOS.SYS 來做另一階段的初始化。並且開始執行 CONFIG.SYS 檔案，以設定設備驅動程式。完成之後再將 COMMAND.COM 載入,並讀取 AUTOEXEC.BAT 檔案，螢幕上並顯示 DOS 之提示符號 A:>。圖 1-1 說明了上述過程。

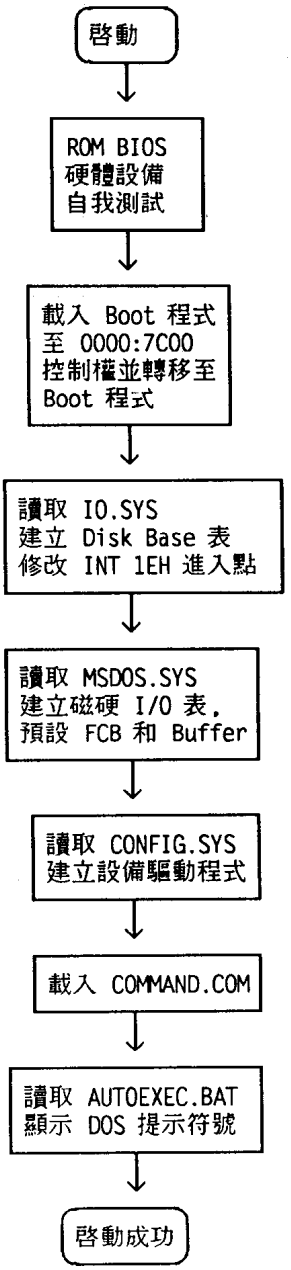

啓動
ROM BIOS
硬體設備
自我測試
載入 Boot 程式
至 0000:7C00
控制權並轉移至
Boot 程式
讀取 IO.SYS
建立 Disk Base 表
修改 INT 1EH 進入點
讀取 MSDOS.SYS
建立磁硬 I/O 表,
預設 FCB 和 Buffer
讀取 CONFIG.SYS
建立設備驅動程式
載入 COMMAND.COM
讀取 AUTOEXEC.BAT
顯示 DOS 提示符號
啓動成功

圖 1-1 軟碟啓動流程圖

當系統載入 IO.SYS 時，IO.SYS 會修改 11 個位元組的 Disk Base 表及 INT 1EH 中斷向量。圖 1-2 爲 11 個位元組之 Disk Base 表內容。

Offset	意　義
0	步進馬達速率及磁頭無載時間
1	磁頭載入時間及 DMA 模式旗標
2	馬達等待時間
3	每個磁區之位元組數目
4	每個磁軌之磁區數目
5	讀寫每個磁區之間隔長度
6	資料長度
7	Format 時每個磁區之間隔長度
8	Format 時所要填寫的位元數目
9	磁頭之穩定時間
A	馬達啓動時間

圖 1-2 Disk Base 表之內容

1-2 硬碟的啓動

硬碟由於其容量較大，故可以將磁碟劃分成許多區域，故通常執行硬碟規劃時會在啓動程式的前面保留一個磁軌的空間來存放硬碟規劃的資料。這個磁軌一般通稱爲 partition Table。其結構如圖 1-3 所示。

每個 partition Table 包含 16 bytes，其位址是在相對於該磁區 1BEH 處。圖 1-4 爲每個 partition Table 之內容。

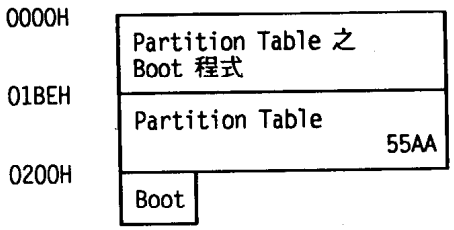


圖 1-3 第一磁軌之結構

Offset	意　義
0	啓動編號(動作者為 80H，不動作者為 00H)
1	起始磁頭號碼
2-3	起始磁區和磁軌號碼
4	系統編號
5	結束磁頭號碼
6-7	結束磁區和磁軌號碼
8-11	第一個磁區的號碼
12-15	分割的磁區總數

圖 1-4 Partition Table 之內容

於是硬碟啓動時 ROM BIOS 硬體測試完畢時先讀取 Partition Table 前面的啓動程式，將它載入到 0000:7C00H 的地方，並判斷該磁區之最後 2 個 bytes 是否爲 55AAH，之後便將程式本身往下移，這時順便檢查是否有一個以上的 80H。若只有一個 80H，系統便將動作的 Partition Table 內的啓動磁區讀至 0000:7C00H，控制權就交給啓動程式，以後的動作便與軟碟相同。圖 1-5 爲硬碟啓動的過程。

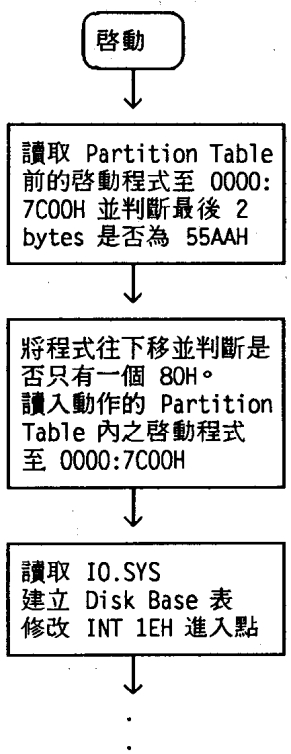


圖 1-5 硬碟啓動之流程圖

當 DOS 啓動成功後對於相關的檔案都已完成記憶體規劃。圖 1-6 爲開機後的記憶體分配圖。

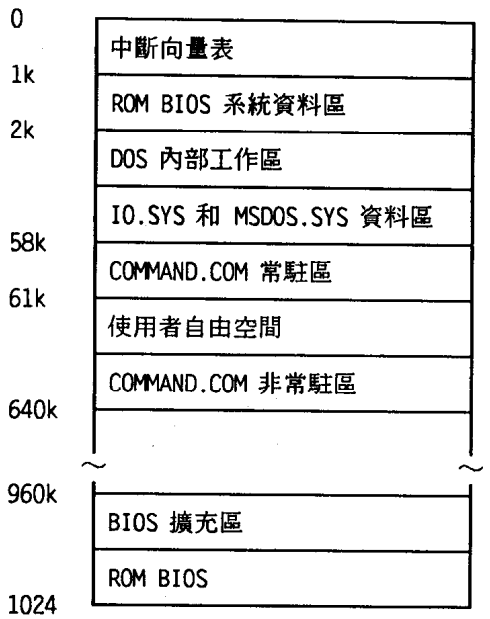


圖 1-6 PC 記憶體分佈圖