

GOTOP

電腦病毒 診斷及治療



碁峯資訊 工具軟體系列叢書

張寶源

電腦病毒 之診斷及治療

張寶源

碁峯資訊股份有限公司 印行

目錄

第一章	DOS 的基本觀念	1-1
1-1	軟碟的啓動	1-2
1-2	硬碟的啓動	1-5
1-3	.COM 檔和 .EXE 檔之比較	1-8
1-4	磁片的構造	1-11
1-5	DOS 中斷系統	1-13
1-6	病毒常用的中斷介紹	1-17
第二章	何謂電腦病毒	2-1
2-1	什麼是電腦病毒	2-2
2-2	什麼是病毒感染的目標	2-3
2-3	病毒如何感染程式	2-5
2-4	破壞性程式的種類	2-6
2-5	電腦病毒感染的途徑	2-8
第三章	病毒的分類	3-1
3-1	啓動磁區感染型病毒	3-3
3-2	命令處理器感染型病毒 (COMMAND.COM Virus)	3-8
3-3	檔案型病毒	3-10
3-4	複合感染型病毒	3-14
3-5	特定檔案感染型病毒	3-15
3-6	記憶體常駐型病毒	3-16

第四章	病毒的基礎診斷和治療	4-1
4-1	常見的電腦病毒發作症狀	4-2
4-2	基本的治療方法	4-4
4-3	有效的預防措施	4-6
第五章	進階解毒原理	5-1
5-1	啓動磁區型病毒	5-2
5-2	命令處理器型病毒解毒原理	5-8
5-3	檔案感染型病毒之解毒原理	5-9
5-4	複合型病毒解毒原理	5-22
5-5	特定型病毒解毒原理	5-23
5-6	記憶體常駐型病毒解毒原理	5-26
第六章	流行病毒剖析	6-1
	AIDS	6-2
	Air cop	6-3
	Aircop	6-6
	Airwolf	6-9
	Alabama	6-13
	Alameda	6-15
	Amicga	6-17
	Amstrad	6-18
	Ashar	6-21
	Austrian	6-23
	Barrelona	6-25
	Basic	6-26

Bee	6-29
Bloody	6-34
Brain	6-36
Cascade	6-38
Cascade-B	6-41
Chaos	6-44
Chinese Bomb	6-46
Christmas	6-48
Copy Lock	6-49
Dark Avenger	6-52
Datacrime	6-55
Datacrime II	6-57
dBASE	6-59
Den Zuk	6-62
Devil's Dance	6-64
Disk Killer	6-67
Do-Nothing Virus	6-70
Doom I	6-72
DOOM I-B	6-75
DOOM II	6-78
Doom II -B	6-83
DOS 62	6-88
EDV	6-91
Friday the 13th (13 號星期五)	6-93
Friday The 13th COM	6-98
Friday the 13th-B	6-99
Friday the 13th-C	6-103

Fu Manchu	6-108
Fumble	6-111
Ghost Boot	6-112
Ghost COM	6-114
Golden Gate	6-117
Greensleeves	6-119
Ha! Ha!	6-124
Ha! Ha!-B	6-129
Halloechen	6-134
Hammer	6-137
Hammer 4	6-142
Holland Girl	6-145
I/O port	6-147
Icelandic	6-149
Icelandic-III	6-151
Icelandic II	6-153
Jerusalem	6-154
Jerusalem-B	6-159
JoJo	6-160
Joker	6-163
Joshi	6-165
June, 16	6-168
Lehigh	6-171
Lisbon	6-173
MIX/1	6-176
Music	6-178
Music Bug	6-180

New Aircop	6-182
New Jerusalem	6-184
Ohie	6-189
Oropax	6-191
Payday	6-193
Perfurme	6-198
Pertagon	6-199
Ping Pong	6-201
Ping Pong-B	6-203
Pixel	6-204
Plaetique	6-206
Plastique-27	6-211
Programs Killer	6-216
Red September	6-221
Saratoga	6-226
Search	6-228
SF	6-230
Stoned	6-232
Stoned-B	6-235
Stoned-C	6-238
Stoned II	6-240
Stupid	6-243
Sunday	6-244
Sunday-B	6-249
Sunday-C	6-254
Sunny	6-259
Sunny-B	6-262

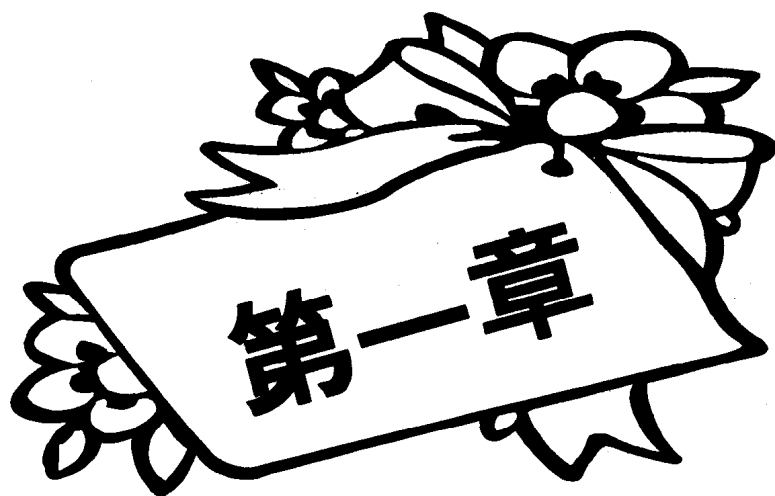
Surviv 1.01	6-265
Surviv 2.01	6-268
Surviv 3.00	6-270
Swap	6-275
Symphony No.40	6-277
SysLock	6-282
The 100 Years	6-284
Traceback	6-286
Traceback II	6-289
Two Tigers	6-292
Typo Boot	6-297
Typo COM	6-299
Vacsina	6-300
Vcomm	6-301
Vienna	6-302
Vienna-B	6-305
Virus-101	6-308
Virus-102	6-310
Virus-90	6-311
W13	6-312
Wolf Man	6-313
Yale	6-318
Yankee Doodle	6-320
Zero Bug	6-326
1181	6-329
1252	6-334
1260	6-339

1280	6-342
1452	6-344
1536	6-349
1554	6-352
1575	6-357
1701	6-362
1704	6-365
1720	6-368
1813	6-371
2900	6-376
2930	6-381
3012	6-384
382	6-389
398 panic	6-390
405	6-392
4096	6-393
512	6-395
5120	6-398
6.4	6-401
648	6-403

第七章 有效的保護措施.....7-1

7-1 限制共享	7-3
7-2 使用密碼	7-5
7-3 保護病毒	7-7
7-4 軟體的保護	7-8
7-5 資料的保護	7-10

7-6	硬體的保護	7-11
7-7	小心的使用 BBS 電子佈告欄	7-12
7-8	有效的防毒技巧	7-13
第八章	常用偵毒和解毒軟體之簡介	8-1
8-1	SCAN	8-2
8-2	CLEAN	8-13
8-3	病毒終結者 III	8-23
8-3-1	電腦捍衛戰士 (PROTPC)	8-23
8-3-2	硬碟防護程式 (HDPROT)	8-24
8-3-3	記憶體顯示器 (RAMMAP)	8-26
8-3-4	病毒掃瞄者 (SCANVIR)	8-29
8-3-5	檔案型病毒獵殺者 (HUNTFILE)	8-35
8-3-6	磁片型病毒獵殺者 (HUNTDISK)	8-37
8-4	Norton Antivirus	8-40
8-4-1	系統安裝	8-41
8-4-2	病毒攔截器 (Virus Intercept)	8-60
8-4-3	病毒診所 (Virus Clinic)	8-65
8-4-4	Norton Antivirus 環境的設定	8-82
8-5	其他解毒軟體	8-91
8-6	各種偵毒及解毒軟體之比較	8-96
第九章	病毒別名參考表	9-1
第十章	結論	10-1
10-1	如何採樣病毒碼	10-1
10-2	防毒程式原理介紹	10-6
附錄	磁片使用說明	A-1



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。

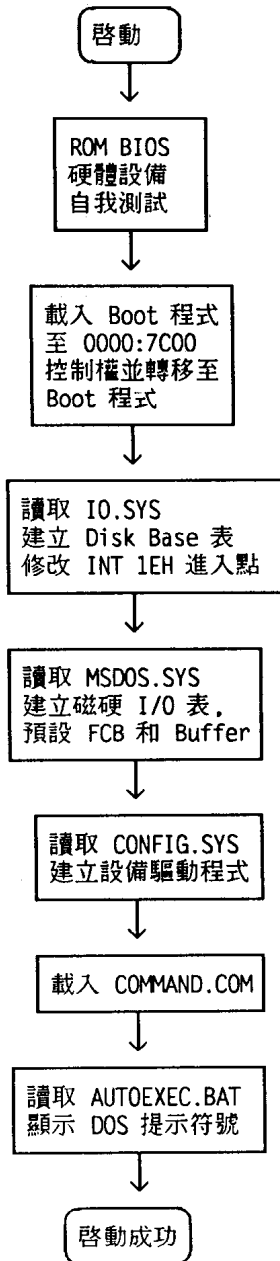


圖 1-1 軟碟啟動流程圖

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 為 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	馬達啟動時間

圖 1-2 Disk Base 表之內容

1-2 硬碟的啟動

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啟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。這個磁軌一般通稱為 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 為每個 partition Table 之內容。

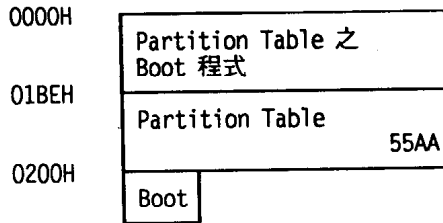


圖 1-3 第一磁軌之結構

Offset	意義
0	啟動編號(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 是否為 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。

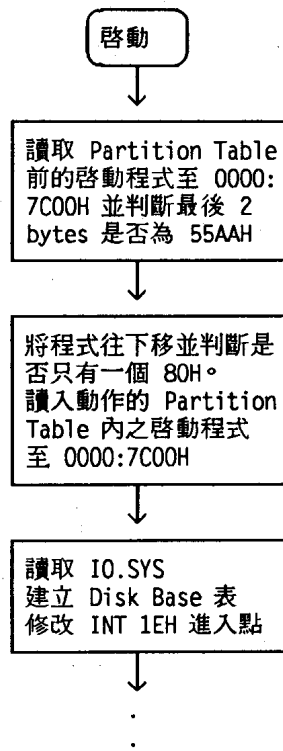


圖 1-5 硬碟啓動之流程圖

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。

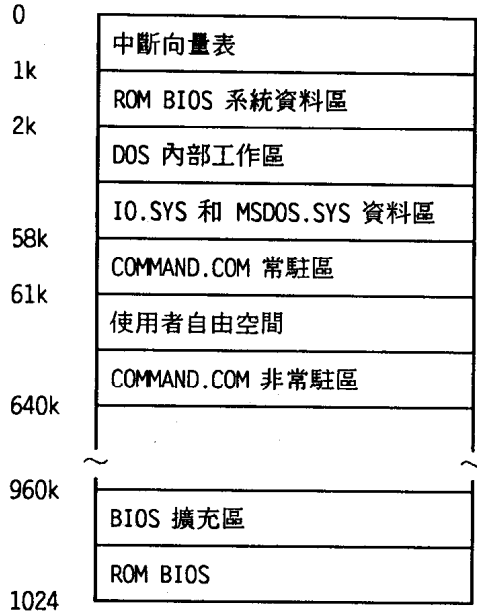


圖 1-6 PC 記憶體分佈圖