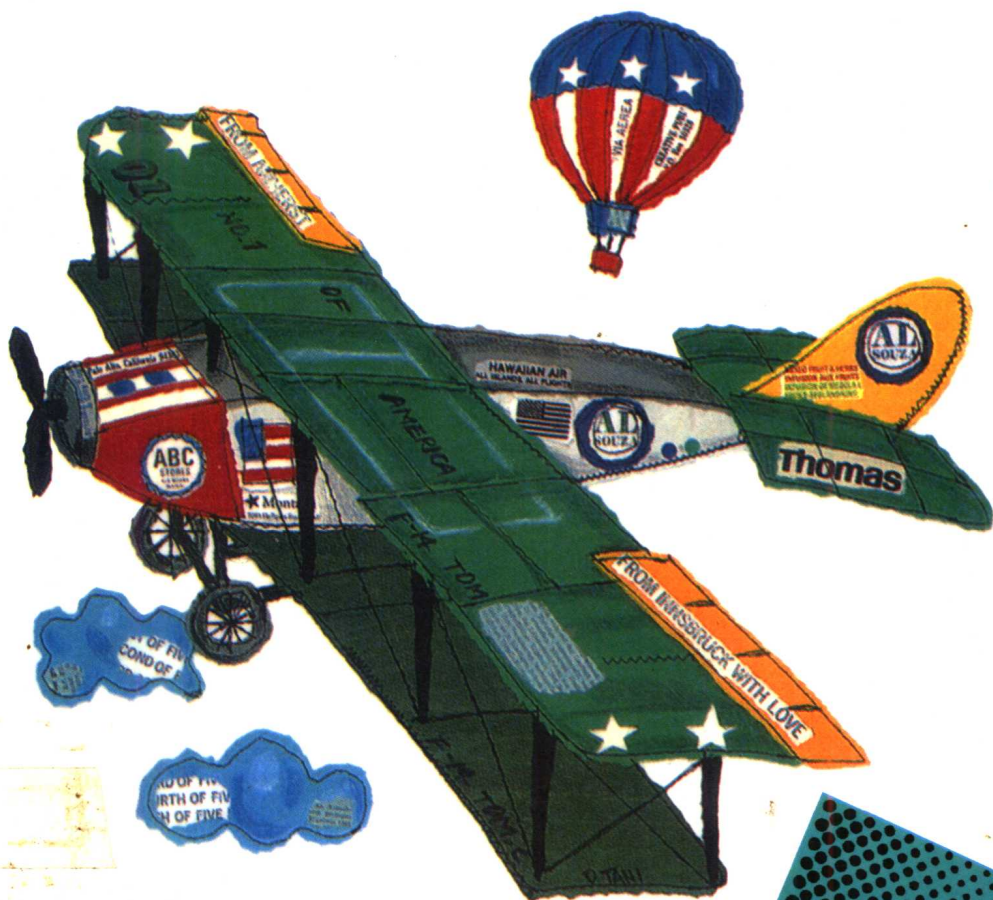


M S DOS

3.1 3.2 3.3

系統呼叫



張德華 編譯

MS DOS

3.1 3.2 3.3

系 統 呼 叫

張德華 編譯

本書程式磁片每片30元

15週年紀念
1973-1988
中南圖書公司

儒林圖書公司 印行

版權所有
翻印必究

MS-DOS 系統呼叫

編譯者：張 德 華

發行人：楊 鏡 秋

出版者：儒 林 園 書 有 限 公 司

地 址：台北市重慶南路一段 111 號

電 話：3118971-3 3144000

郵政劃撥：0106792-1 號

吉豐印刷廠有限公司承印

板橋市三民路二段正隆巷 46 弄 7 號

行政院新聞局局版台業字第 1492 號

中華民國七十六年十二月初版

定價新台幣 220 元正

原 序

MS-DOS 所提供的系統呼叫 (System Call) 的功能大約有 100 種。由於在組合語言層次 (level) 呼叫這些功能，而可以很容易地進行控制台輸入輸出、檔案處理、目錄管理、記憶體管理、行程 (process) 管理等高度技巧的處理。

本書針對這些系統呼叫的用法，就其功能一一舉範例程式加以說明，另外又介紹將各系統呼叫 (功能呼叫) 寫成巨集 (macro)，把特別常用的收在標頭檔案 (header file) 之中，以便含入 (include) 使用者的原始檔案中的方法。由此，雖是組合語言，却又像一種高階語言一樣，可進行程式設計，減少設計程式時的負擔。

使用系統呼叫時需要瞭解 PSP (Program Segment Prefix)、FCB (File Control Block)、目錄、檔案頭銜 (file handle)、記憶體配置 (memory allocation)、行程 (process) 等與 MS-DOS 的結構有關的概念。這些概念在第二章介紹，必要時請參考。

MS-DOS 已經穩固了作為 16 位元個人電腦的作業系統的主流地位，所以在此 OS 上執行的軟體逐漸增加。它所提供的系統呼叫雖是用組合語言寫的，但 C、Pascal、Fortran、BASIC 等高階語言也可加以利用。由於這些系統呼叫可隨意使用，使得在 MS-DOS 上開發程式就非常方便。

以系統呼叫這項強而有力的工具，邁進 MS-DOS 的內部世界，應該是打開與一般程式設計方法不同層次的軟體環境的關鍵所在。本書若能幫助讀者進入 MS-DOS 的內部世界，那是作者的一大榮幸。

目 錄

原 序	I
第一章 MS-DOS系統呼叫的用法	1
1.1 何謂系統呼叫 (功能呼叫)	2
1.2 系統呼叫的種類	4
1.3 用 COM 模式開發程式	8
① COM 模式的程式格式	8
② 巨集定義與標頭檔案	9
③ COM 模式的組譯 / 連結的批次檔	10
1.4 本書使用的標頭檔案	12
① STDIO.H (標準 I/O 標頭檔案)	12
② FILE.H (FCB 檔案標頭)	16
③ FILEH.H (檔案頭銜標頭)	17
④ MEMORY.H (記憶體標頭)	19
第二章 MS-DOS 上的重要概念	21
2.1 PSP (Program Segment Prefix)	22
① PSP 的結構	22
② 命令列的參數	23
2.2 使用 FCB 的檔案處理	25
① FCB 與 DTA	25
② 循序檔案與隨機檔案	27

③ 檔案屬性.....	28
④ 日期 / 時刻的格式.....	29
2.3 使用檔案頭銜的檔案處理.....	30
① 檔案頭銜.....	30
② 標準檔案頭銜.....	31
2.4 磁碟的結構.....	32
① 磁碟的配置.....	32
② 目 錄.....	34
2.5 記憶體管理.....	36
① 分段與差距.....	36
② 記憶體配置.....	36
2.6 行 程.....	38
第三章 MS-DOS的預設中斷.....	41
中斷類型 20H ▶ 程式的終了.....	42
中斷類型 21H ▶ 功能呼叫.....	44
中斷類型 22H ▶ 程式終了位址.....	45
中斷類型 23H ▶ < CTRL - C > 中斷處理程式的位址.....	48
中斷類型 24H ▶ 嚴重錯誤的中斷處理程式的位址.....	51
中斷類型 25H、26H ▶ 絕對磁碟讀 / 寫.....	57
中斷類型 27H ▶ 程式結束但仍駐留在記憶體中.....	60
第四章 系統呼叫的詳細說明.....	63
① 標準輸入輸出.....	64

② 檔案管理 (利用檔案頭銜)	65
③ 目錄管理	65
④ 磁碟管理	66
⑤ 行程管理	67
⑥ 記憶體管理	67
⑦ 裝置管理 / MS-Networks 管理	68
⑧ 其 他	68
⑨ 版本 2.0 以前的系統呼叫	69
功能 00H ▶ 程式的終了	70
功能 01H ▶ 輸入一個字元	72
功能 02H ▶ 輸出一個字元	74
功能 03H ▶ 從輔助輸入裝置輸入一個字元	76
功能 04H ▶ 輸出一個字元到輔助輸出裝置	80
功能 05H ▶ 輸出一個字元到列表機	82
功能 06H ▶ 直接控制台輸入輸出	84
功能 07H ▶ 直接控制台輸入	88
功能 08H ▶ 直接控制台輸入	91
功能 09H ▶ 輸出字串	94
功能 0AH ▶ 緩衝式輸入字串	97
功能 0BH ▶ 檢查輸入狀態	101
功能 0CH ▶ 將緩衝區清成空的之後等待輸入	103
功能 0DH ▶ 磁碟的重置	105
功能 0EH ▶ 磁碟的選擇	107
功能 0FH ▶ 打開檔案	110
功能 10H ▶ 關閉檔案	113
功能 11H ▶ 搜尋第一個匹配的目錄項	116
功能 12H ▶ 搜尋下一個匹配的目錄項	119

功能 13H ▶ 刪除檔案	122
功能 14H ▶ 循序讀取	124
功能 15H ▶ 循序寫入	127
功能 16H ▶ 新建立檔案	130
功能 17H ▶ 改變檔案名稱	133
功能 19H ▶ 取得目前磁碟	136
功能 1AH ▶ 設定 DTA	138
功能 1BH ▶ 取得預設磁碟機的資訊	141
功能 1CH ▶ 取得指定磁碟機的資訊	144
功能 21H ▶ 隨機讀取	147
功能 22H ▶ 隨機寫入	151
功能 23H ▶ 取得檔案大小	156
功能 24H ▶ 設定相對記錄	157
功能 25H ▶ 設定中斷向量	160
功能 26H ▶ 建立新的 PSP	164
功能 27H ▶ 隨機區段讀取	165
功能 28H ▶ 隨機區段寫入	168
功能 29H ▶ 分析檔案名稱	171
功能 2AH ▶ 取得日期	175
功能 2BH ▶ 設定日期	177
功能 2CH ▶ 取得時刻	179
功能 2DH ▶ 設定時刻	181
功能 2EH ▶ 設定檢驗旗號	183
功能 2FH ▶ 取得 DTA 位址	186
功能 30H ▶ 取得 MS-DOS 版本號碼	188
功能 31H ▶ 程式結束但仍駐留在記憶體中	190
功能 33H ▶ < CTRL - Break > 檢查的設定 / 取得	192

功能 35H ▶ 取得中斷向量	195
功能 36H ▶ 取得磁碟的剩餘空間	197
功能 38H ▶ 設定 / 取得國家資訊	200
功能 39H ▶ 建立目錄	204
功能 3AH ▶ 刪除目錄	207
功能 3BH ▶ 改變目前目錄	210
功能 3CH ▶ 建立檔案頭銜	213
功能 3DH ▶ 頭銜檔案的打開	217
功能 3EH ▶ 頭銜檔案的關閉	221
功能 3FH ▶ 讀取頭銜檔案	223
功能 40H ▶ 寫入頭銜檔案	227
功能 41H ▶ 刪除檔案	230
功能 42H ▶ 移動檔案指標	232
功能 43H ▶ 檔案屬性的設定 / 取得	236
功能 44H, 副功能 00H、01H ▶ IOCTL 資料的設定 / 取得	240
功能 44H, 副功能 02H ~ 05H ▶ IOCTL 間的資料傳遞	244
功能 44H, 副功能 06H、07H ▶ 取得輸入 / 輸出狀態	246
功能 44H, 副功能 08H ▶ 檢查是否為可抽換的磁碟機	249
功能 44H, 副功能 09H、0AH ▶ local / remote 的檢查	251
功能 44H, 副功能 0BH ▶ IOCTL 重試的設定	253
功能 45H ▶ 檔案頭銜的複製	255
功能 46H ▶ 將指定頭銜複製到指定頭銜	258
功能 47H ▶ 目前目錄的取得	262
功能 48H ▶ 記憶體配置	265
功能 49H ▶ 釋放配置記憶體	269

功能 4AH ▶ 改變所配置的記憶體區段	273
功能 4BH, 副功能 00H ▶ 程式的執行	277
功能 4BH, 副功能 03H ▶ 程式的載入	282
功能 4CH ▶ 行程的終了	286
功能 4DH ▶ 取得子行程的傳回值	289
功能 4EH ▶ 搜尋第一個匹配的檔案名稱	292
功能 4FH ▶ 搜尋其次匹配的檔案名稱	295
功能 54H ▶ 檢驗旗號的檢查	298
功能 56H ▶ 改變檔案名稱	300
功能 57H ▶ 檔案日期、時刻的設定 / 取得	303
功能 58H ▶ 記憶體配置策略的設定 / 取得	306
功能 59H ▶ 取得延伸錯誤碼	309
功能 5AH ▶ 建立暫時檔案	315
功能 5BH ▶ 新建立檔案	318
功能 5CH ▶ 檔案記錄的鎖定 / 解鎖	322
功能 5EH, 副功能 00H ▶ 取得局部性終端機名稱	327
功能 5EH, 副功能 02H ▶ 設定列表機	329
功能 5FH, 副功能 02H ▶ 取得重新導向串列的項	331
功能 5FH, 副功能 03H ▶ 設備的重新導向	333
功能 5FH, 副功能 04H ▶ 取消重新導向	335
功能 62H ▶ 取得 PSP 位址	337
附 錄	339

第一章

MS-DOS系統呼叫的用法

首先說明系統呼叫的步驟與種類

因為本書的程式完全是用 COM 模式寫的，所以也一併說明程式的開發方法。

由於將控制台輸入輸出、檔案處理、記憶體管理等基本處理寫成巨集，並當作標頭檔案含入，使得設計組合語言程式的效率大為提高。

分別說明本書使用的四個標頭檔案

[`STDIO.H`]、[`FILE.H`]、[`FILEH.H`]、[`MEMORY.H`]。

2 MS-DOS 系統呼叫

1.1

何謂系統呼叫(功能呼叫)

在組合語言層次寫作控制台輸入輸出或檔案處理等應用程式時，使用者必須各自提供所需的基本處理。在MS-DOS上(其他OS上也同樣)將一些基本處理當作副程式內建於MS-DOS的系統內，讓使用者可加以呼叫，這叫做系統呼叫。MS-DOS提供了大約90種的副程式。

MS-DOS的系統呼叫(功能呼叫)的方式是將功能碼00H~62H存入暫存器AH中，而將所需的參數(也可能沒有)存放在暫存器CX、DX等上，然後進行軟體中斷INT 21H，就可執行功能碼所規定的功能。呼叫的格式如下：

```
MOV  AH, 功能碼  
    [ 各暫存器←參數 ]  
INT  21H
```

在經過INT 21H的系統呼叫之後，暫存器的內容除了暫存器AX等(不一定只有AX，可能還用到其它的暫存器，端視那一個系統呼叫而定)存放傳回的資訊之外，其他的原封不動傳回。

8086的軟體中斷(Interrupt)的格式如下：

```
INT  n
```

n可指定0~FFH(255)。動作是，一旦產生INT n的中斷，就參考從記憶體位址0開始設定的「中斷指標表」的第n個指標(每個指標佔4個位元組)，然後轉向到第n個指標所表示的中斷

服務程式 (interrupt service routine) 等中斷處理結束之後由 IRET 回到原來轉向位置。MS-DOS 的系統呼叫係使用這個中斷類型 21H。

圖 1 是系統呼叫的概念圖，圖 2 是系統呼叫的記憶體映像 (image)。

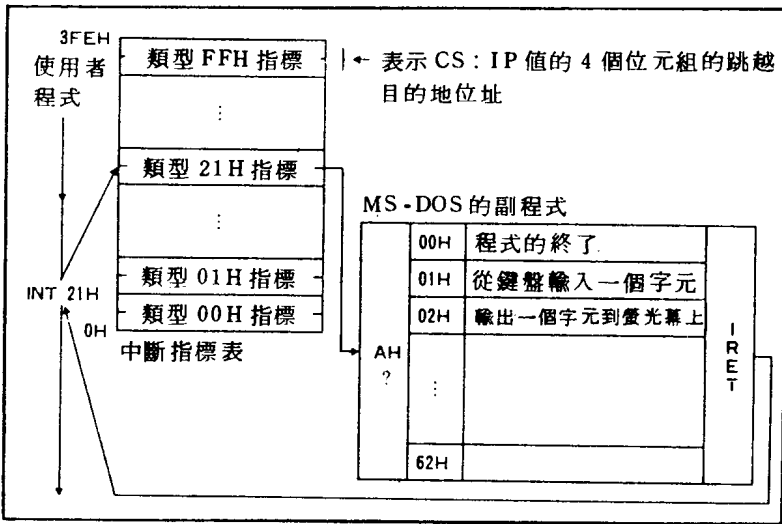


圖 1 系統呼叫的概念

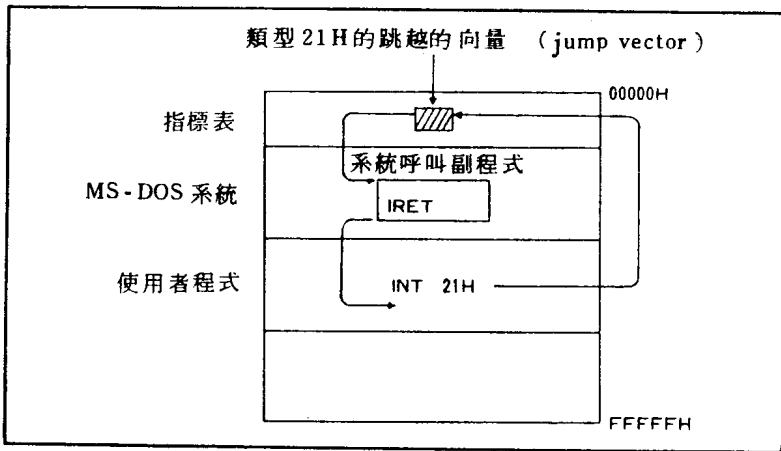


圖 2 系統呼叫的記憶體映像

1.2

系統呼叫的種類

8086 在中斷指標表之中保留類型 0 ~ 4 為特別的中斷。MS-DOS 則保留 20H ~ 3FH 的中斷類型。

表 1 8086 保留的中斷

中斷類型	功 能
00H	除法錯誤 (除以 0 時)
01H	Single step (逐步執行)
02H	NMI 中斷 (不可遮罩中斷)
03H	中斷點 (Break point instruction)
04H	溢位 (overflow) 中斷

表 2 MS-DOS 保留的中斷

中斷類型	功 能
20H	程式的終了
21H	功能呼叫
22H	程式終了位址
23H	<CTRL-C> 的中斷位址
24H	嚴重錯誤的中斷位址
25H	絕對磁碟讀取
26H	絕對磁碟寫入
27H	程式結束但仍駐留在記憶體中
28H ~ 3FH	保留給 MS-DOS 使用

廣義的系統呼叫，是指類型 20H 到類型 27H 的 MS-DOS 保留的中斷。而類型 21H 的中斷根據暫存器 AH 的功能碼可執行大約 90 種的功能，這叫做功能呼叫。狹義的系統呼叫就是指這個功能呼叫。

下面表 3 是 MS-DOS 的 INT 21H 系統呼叫（功能呼叫）的種類。

表 3 系統呼叫（功能呼叫）一覽表

號 碼	功 能
00H	程式的終了
01H	輸入一個字元
02H	輸出一個字元
03H	從輔助輸入裝置 (auxiliary input device) 輸入一個字元
04H	輸出一個字元到輔助輸出裝置
05H	輸出一個字元到列表機
06H	直接從控制台輸入輸出。由 DL 暫存器的值決定輸入或輸出模式。
07H	直接從控制台輸入
08H	直接從控制台輸入 (讀取鍵盤) (同 07H , 但會檢查 Ctrl-C)
09H	輸出字串
0AH	輸入字串
0BH	檢查鍵盤狀況
0CH	使鍵盤緩衝區變成空的之後，等待輸入
0DH	重置 (reset) 磁碟
0EH	選擇磁碟
0FH	打開檔案 (FCB)
10H	關閉檔案 (FCB)
11H	檢查第一個脛合的目錄項 (FCB)
12H	檢查下一個脛合的目錄項 (FCB)

號 碼	功 能
13H	刪除檔案 (FCB)
14H	循序讀取 (FCB)
15H	循序寫入 (FCB)
16H	新建立檔案 (FCB)
17H	改變檔案名稱 (FCB)
19H	取得目前磁碟
1AH	設定磁碟傳遞位址 (DTA)
1BH	取得預設磁碟機的資訊
1CH	取得指定磁碟機的資訊
21H	隨機讀取 (FCB)
22H	隨機寫入 (FCB)
23H	取得檔案大小 (記錄數) (FCB)
24H	設定相對記錄 (FCB)
25H	設定中斷向量
26H	建立新的 PSP
27H	隨機區段讀取 (FCB)
28H	隨機區段寫入 (FCB)
29H	分析 (parse) 檔案名稱 (FCB)
2AH	取得日期
2BH	設定日期
2CH	取得時刻
2DH	設定時刻
2EH	設定檢驗 (verify) 旗號
2FH	取得 DTA 位址
30H	取得 MS-DCS 版本號碼
31H	程式結束但仍駐留在記憶體中
33H	<CTRL-C> 檢查的設定 / 取得
35H	取得中斷向量
36H	取得磁碟的可用空間 (free space)
38H	國家資訊的設定 / 取得
39H	建立目錄
3AH	刪除目錄

號 碼	功 能
3BH	改變目前目錄
3CH	建立頭銜 (以 handle 的方式)
3DH	打開頭銜
3EH	關閉頭銜
3FH	讀取頭銜
40H	寫入頭銜
41H	刪除檔案
42H	移動檔案指標 (以 handle 的方式)
43H	檔案屬性的設定 / 取得
44H	針對裝置的 IO 控制
45H	檔案頭銜的複製
46H	強行複製到指定頭銜
47H	取得目前目錄
48H	記憶體的配置
49H	釋放配置記憶體
4AH	改變所配置的記憶體區段
4BH	程式的載入 / 執行
4CH	行程的終了
4DH	取得從子行程的傳回碼 (return code)
4EH	搜尋最初匹配的檔案名稱
4FH	搜尋其次匹配的檔案名稱
54H	檢查檢驗旗號
56H	改變檔案名稱
57H	檔案日期時刻的設定 / 取得
58H	記憶體配置策略 (strategy) 的設定 / 取得
59H	取得延伸錯誤碼 (Extended Error Code)
5AH	建立暫時檔案
5BH	建立新的檔案
5CH	檔案記錄的鎖定 / 解鎖
5EH	局部性 (local) 機器名稱的取得 / 列表機的設定 (set up)
5FH	重新導向 / 串列 (redirection/list) 項 (entry) 的取得 / 建立 / 刪除
62H	取得 PSP 位址