MS 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

MS-DOS系統呼叫

編譯者：張　德　華
發行人：楊　鏡　秋
出版者：儒林圖書有限公司
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 已經穩固了作爲 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

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

因爲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爲提高。

分別說明本書使用的四個標頭檔案

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

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OMS-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～62 H 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 21 H，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）。

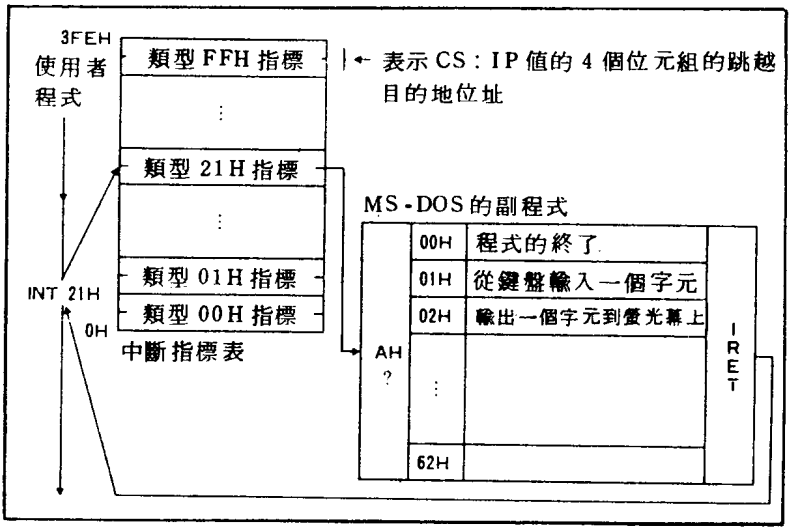

圖1　系統呼叫的概念

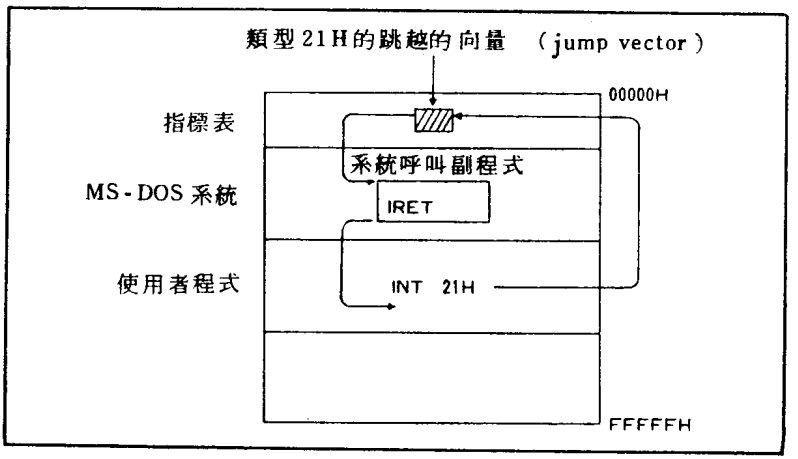

圖2　系統呼叫的記憶體映像

1.2

系統呼叫的種類

8086 在中斷指標表之中保留類型 0 ～ 4 爲特別的中斷。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	檢查第一個脗合的目錄項（FCB）
12H	檢查下一個脗合的目錄項（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-DOS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