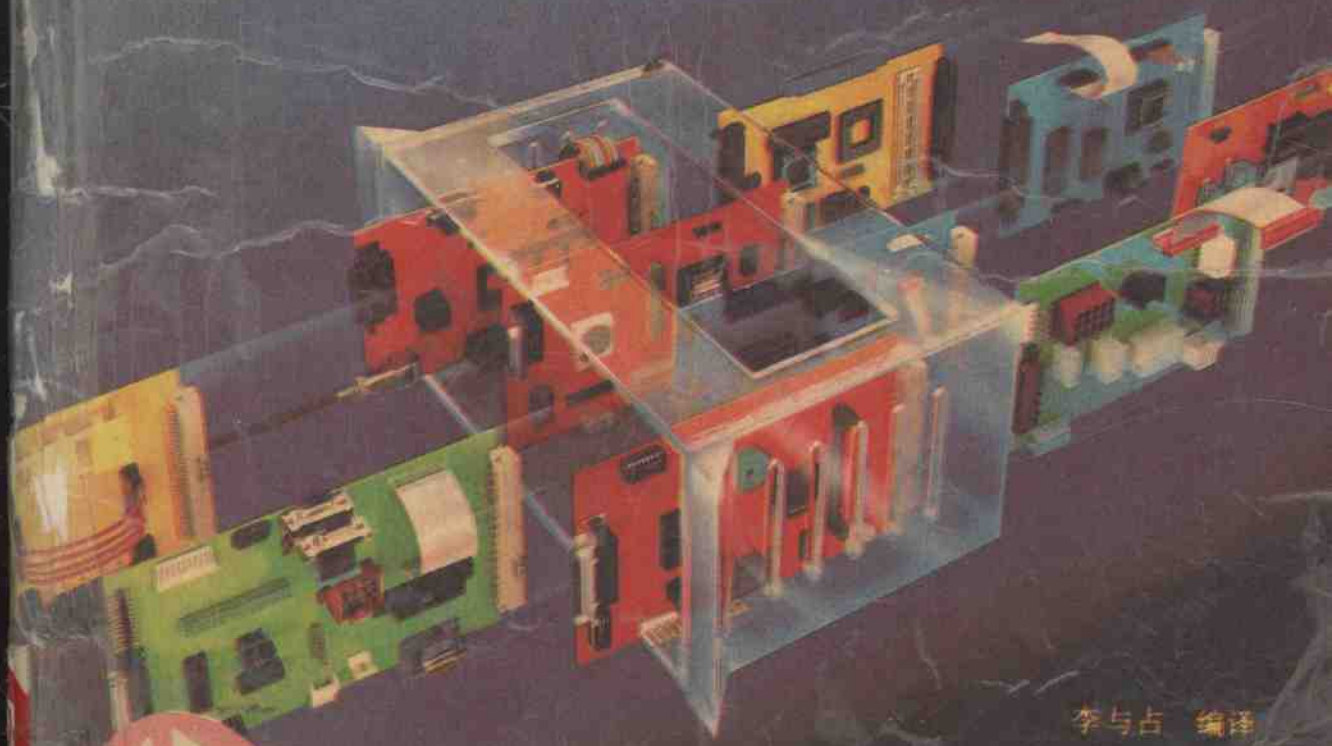
3.0 3.1 3.2 3.3 4.00 4.01

系统调用大全

DOS

系统调用·调用汇编宏·调用实例·所有数据结构·BIOS扩充和扩展内存调用方法等



李与占 编译

HOPE 中国科学院希望高级电脑技术公司

DOS 2.0 3.0 3.1 3.2 3.3 4.00 4.01

系统调用大全

李 宁占 编译

中国科学院希望电脑公司

一九九一年一月

前 言

DOS BIOS 系统调用是 IBM 个人计算机的核心，因为 PC 的操作系统就是由 ROM BIOS、IBMBIO(对 MS-DOS 而言是 IO.SYS)、IBMDOS(对 MS-DOS 而言是 MSDOS)和命令解释程序 COMMAND 组成，而 DOS BIOS 系统调用(即服务子程序)是构成上述各部分的基本元素。

BIOS 调用管理了 PC 机的硬件特性，把与硬件相关的繁琐的管理与控制以子程序的方式提供；DOS 调用在 BIOS 调用的基础上，把 BIOS 子程序进一步“累积”，变成用户使用更为方便的子程序。BIOS 对 PC 机的控制最为全面，而 DOS 则次之，但 BIOS 的编程比 DOS 编程繁锁、难度大。

BIOS 不仅提供所有标准设备驱动程序，而且支持装载和初始化系统，DOS 提供应用编程接口(API)层，这包括设备支持(键盘、显示器、打印机和通讯口)以及文件支持，大多数功能可以通过 INT 21H 应用编程接口(Application Propgramming Interface 简写 API)访问，21H 中断提供很多不同的子功能，其它功能可通过 INT 25H、INT 26H、INT 2FH API 访问。

DOS 也包括文件分配表(FAT)文件系统。一个文件系统是一组子程序，也就是所说的存取方法，即在支持的介质上，把应用程序对数据的引用转换成物理的地址。FAT 术语的意思是文件分配表，正是具有象 FAT 的文件系统，才使得应用程序不需了解数据如何物理地存储在介质上，不需处理设备参数，如磁柱、磁头和扇区，取而代之的是应用程序只处理称之为文件的有名字的数据集。文件存储在称为目录的文件组里。由于具有象 FAT 的文件系统，允许 DOS 支持对已存在的应用程序不起或极少起作用的更新的更大的介质。例如 DOS 4.0 引进了大于 32MB 介质的支持。除了一少部分工作在介质物理级的磁盘实用程序外，现存的应用程序可以在没有任何改变的情况下存取这些大磁盘。

应用程序是建立在 PC 操作系统之上的，系统调用是应用程序完成所需功能的工具。本书讨论了 DOS 2.0 3.0 3.1 3.2 3.3 4.0 4.01 的系统调用，调用汇编宏，调用实例。介绍了几乎所有 DOS 的数据结构如 PSP、FCB、EXE COM 头结构、环境块、DTA、中断矢量表、日期和时间格式等。还介绍了 BIOS 扩充和扩展内存调用的方法，专论了 IOCTL 的用法。

本书在编译时得到了占卫兵的热忱帮助，在此表示感谢。

编者

1991 年 1 月

目　录

第一部分

DOS 2.0 3.1 3.2 3.3

系统调用

第一章　MS-DOS 系统调用的用法

首先说明系统调用的步骤与种类

因为本书的程序完全是用 COM 模式写的，所以也一并说明程序的开发方法。

由于将控制台输入输出、文件处理、存贮管理等基本处理写成宏，并当作头文件嵌入，使得设计汇编语言程序的效率大为提高。

分别说明本书使用的四个头文件

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

§1.1　何谓系统调用（功能调用）

在汇编语言层次编写控制台输入输出或文件处理等应用程序时，使用者必须各自提供所需的基本处理。在 MS-DOS 上（其他 OS 上也同样）将一些基本处理当作子程序内建于 MS-DOS 的系统内，让使用者可加以调用，这叫做系统调用。MS-DOS 提供了大约 90 种子程序。

MS-DOS 的系统调用（功能调用）的方式是将功能码 00H－62H 存入寄存器 AH 中，而将所需的参数（也可能没有）存放在寄存器 CX、DX 等上，然后进行软件中断 INT 21H，就可执行功能码所规定的功能。调用的格式如下：

```
MOV  AH,  功能码
[各寄存器←参数]
INT  21H
```

在经过 INT 21H 的系统调用之后，寄存器的内容除了寄存器 AX 等（不一定只有 AX，可能还用到其它的寄存器，根据那一个系统调用而定）存放返回的信息之外，其他的原封不动返回。

8086 的软件中断（Interrupt）的格式如下：

```
INT n
```

n 可指定 0～FFH（255）。动作是，一旦产生 INT n 的中断，就引用从内存位址 0 开始设定的[中断指针表]的第 n 个指针（每个指针占 4 个字节），然后转到第 n 个指针所表示的中断服务程序（interrupt service routine），等中断处理结束之后由 IRET 回到原来转向位置。MS-DOS 的系统调用系使用这个中断类型 21H。

图 1 是系统调用的概念图，图 2 是系统调用的内存映像（image）。

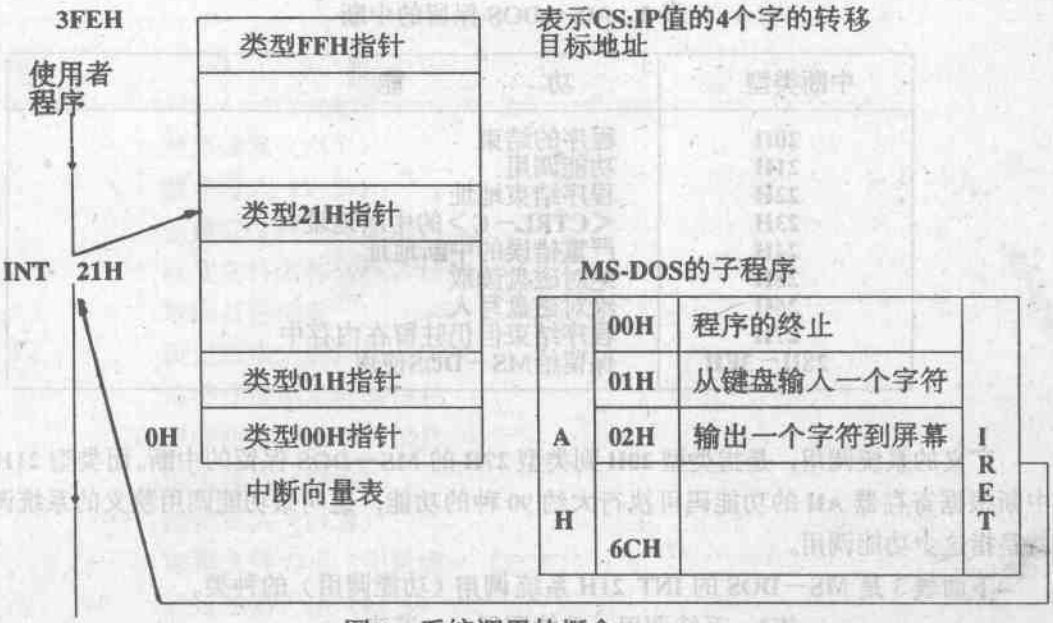


图 1　系统调用的概念

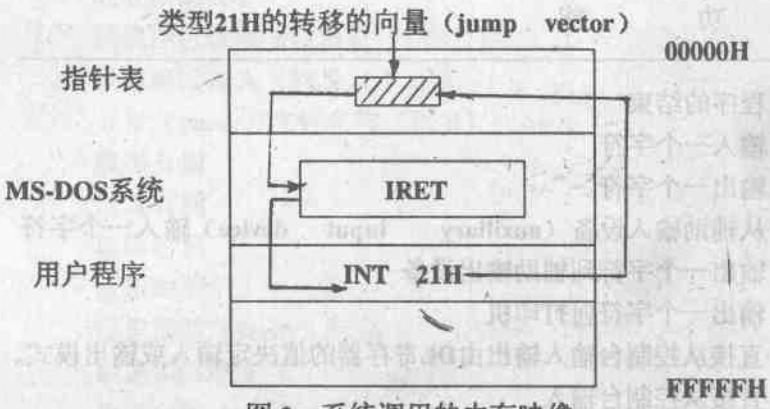


图 2　系统调用的内存映像

§ 1.2　系统调用的种类

8086 在中断指针表之中保留类型 0～4 为特别的中断。MS-DOS 则保留 20H－3FH 的中断类型。

表 1　8086 保留的中断

中断类型	功　　能
00H	除法错误（除以0时）
01H	Single step（单步执行）
02H	NMI中断（不可屏蔽中断）
03H	断点指令中断（Break point instruction）
04H	溢出（overflow）中断