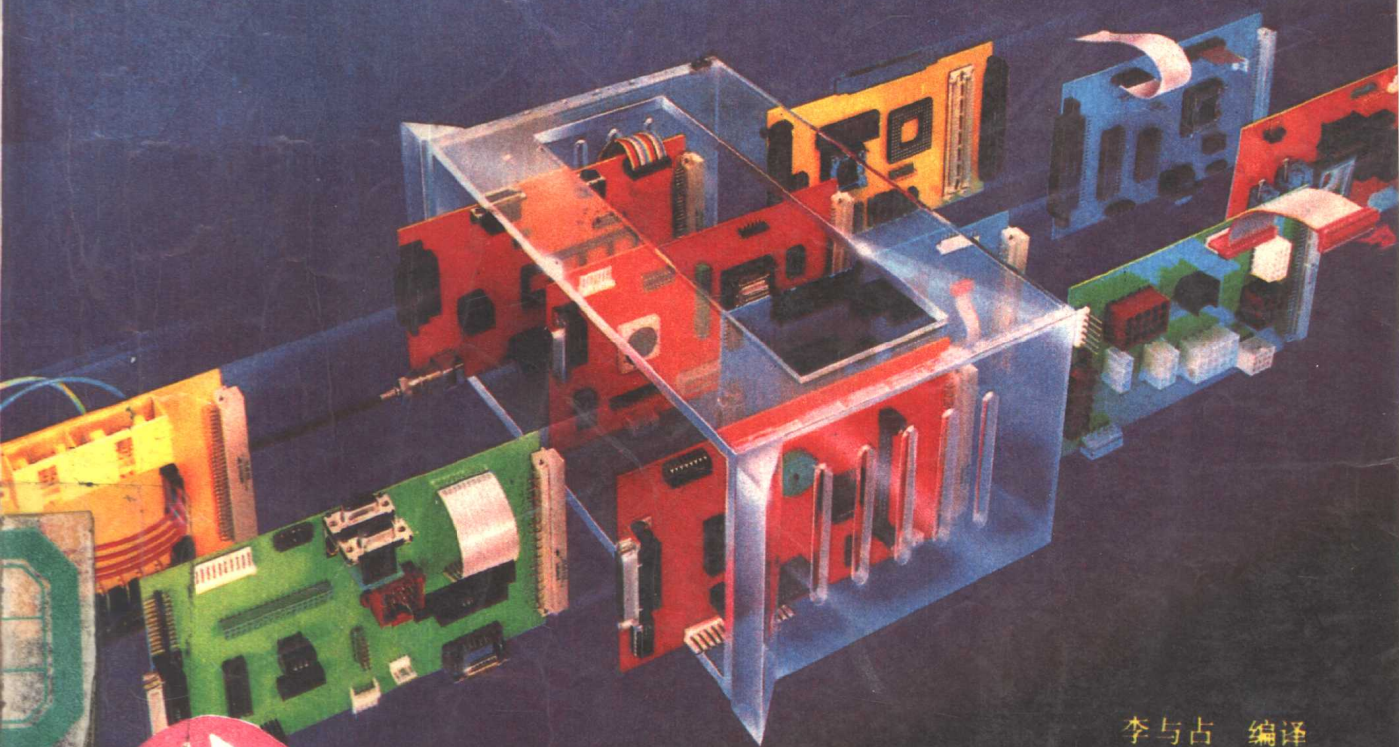


DOS2.0 3.0 3.1 3.2 3.3 4.00 4.01

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 与 占 编译

中国科学院希望电脑公司

一九九一年一月

版权所有
翻印必究

■ 北京市新闻出版局

准印证号: 3317—90317

■ 订购单位: 北京8721信箱资料部

■ 邮 码: 100080

■ 电 话: 2562329

■ 传 真: 01—2561057

■ 乘 车: 320、332、302路

车至海淀黄庄下车

■ 办公地点: 希望公司大楼一楼
往里走101房间

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 编程繁琐、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 Programming 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

前言

第一部分 DOS 2.0 3.0 3.1 3.2 3.3 系统调用	1
---	---

第一章 MS-DOS 系统调用的用法	2
--------------------------	---

首先说明系统调用的步骤与种类	2
分别说明本书使用的四个头文件	2
§ 1.1 何谓系统调用(功能调用)	2
§ 1.2 系统调用的种类	3
§ 1.3 用 COM 模式开发程序	6
① COM 模式的程序格式	6
② 宏定义与头文件	7
③ COM 模式的编译/连接的批处理	8
§ 1.4 本书使用的头文件	8
① STDIO.H(标准 I/O 头文件)	8
③ FILEH. H(文件句柄头)	14
④ MEMORY. H(内存头)	16
memory	

第二章 MS_DOS 上的重要概念	18
-------------------------	----

§ 2.1 PSP(Program Segment Prefix)	18
① PSP 的结构	18
② 命令行的参数	19
§ 2.2 使用 FCB 的文件处理	19
① FCB 与 DTA	19
② 顺序文件与随机文件	20
③ 文件属性	21
④ 日期/时间的格式	22
§ 2.3 使用文件句柄的文件处理	22
① 文件句柄	22
② 标准文件句柄	23
§ 2.4 磁盘的结构	23
① 磁盘的分配	23
② 目录	25
§ 2.5 内存管理	26

① 段与偏移量	26
② 内存分配	26
§ 2.6 进程	27

第三章 MS-DOS 的隐含中断 29

中断类型 20H	29
中断类型 21H	29
中断类型 22H	30
中断类型 23H	32
中断类型 24H	34
中断类型 25H、26H	37
中断类型 27H	40

第四章 系统调用的详细说明 42

① 标准输入输出	42
② 文件管理(利用文件句柄)	43
③ 目录管理	43
④ 磁盘管理	43
⑤ 进程管理	44
⑥ 内存管理	44
⑦ 设备管理/MS-Networks 管理	45
⑧ 其他	45
⑨ 版本 2.0 以前的系统调用	45
功能 00H	46
功能 01H	47
功能 02H	48
功能 03H	49
功能 04H	52
功能 05H	53
功能 06H	54
功能 07H	56
功能 08H	58
功能 09H	60
功能 0AH	61
功能 0BH	63
功能 0CH	64
功能 0DH	65
功能 0FH	68

功能 10H	70
功能 11H	72
功能 12H	74
功能 13H	75
功能 14H	76
功能 15H	78
功能 16H	80
功能 17H	81
功能 19H	83
功能 1AH	84
功能 1BH	86
功能 1CH	88
功能 21H	90
功能 22H	93
功能 23H	96
功能 24H	97
功能 25H	98
功能 26H	101
功能 27H	102
功能 28H	104
功能 29H	106
功能 2AH	110
功能 2BH	111
功能 2CH	112
功能 2DH	113
功能 2EH	114
功能 2FH	116
功能 30H	117
功能 31H	118
功能 33H	120
功能 35H	121
功能 36H	123
功能 38H	124
功能 39H	127
功能 3AH	129
功能 3BH	131
功能 3CH	133
功能 3D	135
功能 3EH	137
功能 3FH	139

功能 40H	141
功能 41H	143
功能 42H	144
功能 43H	147
功能 44H, 子功能 00H, 01H	149
功能 44H, 子功能 02H~05	152
功能 44H, 子功能 06H, 07H	153
功能 44H, 子功能 08H	155
功能 44H, 子功能 09H, 0AH	156
功能 44H, 子功能 0BH	157
功能 45H	159
功能 46H	160
功能 47H	162
功能 48H	164
功能 49H	167
功能 4AH	169
功能 4BH, 子功能 00H	172
功能 4CH, 子功能 03H	175
功能 4CH	178
功能 4DH	180
功能 4EH	182
功能 4FH	184
功能 54H	186
功能 56H	187
功能 57H	189
功能 58H	190
功能 59H	192
功能 5AH	196
功能 5BH	198
功能 5CH	200
功能 5EH, 子功能 00H	204
功能 5EH, 子功能 02	205
功能 5FH, 子功能 02H	206
功能 5FH, 子功能 03H	207
功能 5FH, 子功能 04H	208
功能 62H	209
第五章 DOS 调用研读资料	211
第二部分 DOS 4.00 4.01 系统调用	268

第六章 DOS4.0 4.01 功能调用	269
§ 6.1 DOS INT 21H 功能总结	269
§ 6.2 DOS INT 21H 扩展错误代码一览	273
§ 6.3 DOS INT 21H 扩展错误类型一览	275
§ 6.4 DOS INT 21H 扩展错误处理一览	275
§ 6.5 DOS INT 21H 扩展错误位置一览	276
§ 6.6 常用功能使用建议	276
00H——程序终止	276
01H——带回显的控制台输入	277
02H——显示输出	277
03H——辅助输入	277
04H——辅助输出	278
05H——打印机输出	278
06H——直接控制台 I/O	278
07H——无回显, 直接控制台输入	279
07H——无回显, 直接控制台输入	279
08H——无回显、控制台输入	279
09H——显示字符串	279
0AH——缓冲键盘输入	280
0BH——检查标准输入状态	280
0CH——清键盘缓冲区、调用键盘功能	281
0DH——磁盘复位	281
0EH——选择磁盘	281
0FH——FCB 打开文件	282
10H——FCB 关闭文件	283
11H——FCB 查找第一目录项	283
12H——FCB 查找下一项	284
13H——FCB 删除文件	285
14H——FCB 顺序读	285
15H——FCB 顺序写	285
16H——FCB 创建文件	287
17H——FCB 重命名文件	288
19H——当前磁盘	288
1AH——置磁盘传送地址	289
1BH——分配表信息	289
1CH——给定设备的分配表信息	290
1FH——取缺省设备参数块	290
21H——FCB 随机读	291

22H——FCB 随机写	291
23H——FCB 文件尺寸	292
24H——设置相对记录域	293
25H——置中断向量	294
26H——创建新程序段前缀	294
27H——FCB 随机读	295
28H——FCB 随机块写	295
29H——分析文件名	296
2AH——取日期	297
2BH——置日期	297
2CH——取时间	298
2DH——置时间	298
2E00H——复位确认状态	299
2E01H——置确认状态	299
2FH——取盘传送区地址	299
30H——取 DOS 版本号	299
31H——结束并驻留	300
32H——取设备参数块	301
3300H——取 Break 状态	301
3301H——置 Break 状态	301
3305H——取引导驱动器	301
34H——取 DOS 内部标志地址	302
35H——取中断向量	302
36H——取磁盘自由空间	302
3700H——取开关字符	303
3701H——设置开关字符	303
38H——取/置国家信息	304
39H——创建子目录	305
3AH——删除子目录	305
3BH——改变目录	306
3CH——创建一个文件	306
3DH——打开文件	306
3EH——关闭文件句柄	308
3FH——读文件或设备	308
40H——写文件或设备	308
41H——删除一个文件	309
42H——移动文件读/写指针	309
4300H——取文件属性	310
4301H——置文件属性	310
4400H(IOCTL)——取设备状态	310

4401H(IOCTL)——置设备状态·····	311
4402H/4403H (IOCTL)——读/写字符设备·····	312
4404H/4405H(IOCTL)——读/写块设备·····	312
4406H/4407H(IOCTL)——取 I/O 状态·····	312
440AH(IOCTL)——测试句柄为本/远地·····	313
440BH(IOCTL)——设置共享重入重试计数·····	314
440CH/440DH(IOCTL)——句柄/块设备通用 IOCTL 请求·····	314
440EH/440FH(IOCTL)——取/置逻辑驱动器·····	315
45H——复制文件句柄·····	315
46H——强迫复制文件句柄·····	316
48H——分配内存块·····	316
49H——释放内存块·····	317
4AH——修改分配的内存块·····	317
4B00H——执行程序(EXEC)·····	317
4B01H——装入程序·····	318
4B03H——装入覆盖·····	319
4CH——终止进程(Exit)·····	319
4DH——取子进程的返回码·····	320
4EH——查找第一个匹配文件·····	320
4FH——查找下一个匹配文件·····	321
50H——设置活动进程数据块·····	321
51H——取活动进程数据块·····	322
52H——取 DOS 内部值·····	322
54H——取验证状态·····	323
55H——复制 PDB·····	323
56H——重命名/移动文件(重命名目录)·····	324
5700H——取文件日期和时间·····	324
5800H——取分配策略·····	324
5801H——设置分配策略·····	325
59H——取扩展错误信息·····	325
5AH——以唯一名创建文件·····	326
5BH——创建新文件·····	326
5C00H——锁定文件存取·····	327
5C01H——打开文件锁定·····	327
5D00H——DOS 调用服务器·····	328
5D01H——提交所有文件·····	329
5D02H——以名字关闭文件·····	329
5D03H——关闭特定计算机的所有文件·····	329
5D04H——关闭特定进程的所有文件·····	330
5D05H——取打开文件列表项·····	330

5D06H 和 5D0BH——取 DOS 数据区地址	330
5D07H——取打印流状态	331
5D08H——设置打印流状态	332
5D09H——截断打印流	332
5D0AH——设置扩展错误信息	332
5E00H——取机器名字	333
5E01H——设置机器名	333
5E02H——置打印机设置(Set up)	333
50E03H——取打印机设置	334
5E04H——设置打印机模式	334
5E05H——取打印机模式	335
5F00H——取重定向模式	335
5F01H——置重定向模式	335
5F02H——取重定向列表项	336
5F03H——重定向设备	336
5F04H——取消重定向	337
5F05H——取扩展的重定向列表项	337
60H——翻译文件规范	338
62H——取 PSP 地址	338
6300H——取 DBCS 前景字节表	339
6301H——置/复位 Hangeul 模式	339
6302H——取 Hangeul 模式	339
6501H——取扩展国家信息	340
6502H/6504H——取文本/文件大写(UpperCase)表地址	341
6506H——取对照表地址	342
6507H——取 DBCS 向量	342
6520H/6521H/6522H——大写映射功能	343
6523H——YES/NO 检查	343
6600H——取全局(Global)代码页	344
6601H——设置全局代码页	344
67H——设置句柄计数	344
68H——提交文件	345
6900H——取介质 1D	345
6901H——置介质 1D	345
6CH——扩展打开/创建文件	346

第七章 DOS 4.00 功能调用实例	348
---------------------	-----

第八章 设备的输入/输出控制(IOCTL)编程实例	415
---------------------------	-----

第三部分 BIOS 扩充 扩展内存中断调用	433
-----------------------	-----

附录 A IBM ROM BIOS 所提供的服务	434
--------------------------	-----

INT 05H (5) 打印屏幕	434
------------------	-----

INT 10H (16) 视频显示	434
-------------------	-----

AH=00H (0) 设置视频显示方式	435
---------------------	-----

AH=01H (1) 设置光标大小	436
-------------------	-----

AH=02H (2) 设置光标位置	436
-------------------	-----

AH=03H (3) 读取光标位置	437
-------------------	-----

AH=04H (4) 读取光笔位置	437
-------------------	-----

AH=05H (5) 设置工作显示页	437
--------------------	-----

AH=06H (6) 窗口向上卷动	438
-------------------	-----

AH=07H (7) 窗口向下卷动	438
-------------------	-----

AH=08H (8) 读取字符和特性	439
--------------------	-----

AH=09H (9) 写出字符和特性	439
--------------------	-----

AH=0AH (10) 写出字符	439
------------------	-----

AH=0BH (11) 设置彩色调色板	440
---------------------	-----

AH=0CH (12) 显示一个像素	441
--------------------	-----

AH=0DH (13) 读取像素	441
------------------	-----

AH=0EH (14) 以 TTY 方式写出字符	441
--------------------------	-----

AH=0FH (15) 获得当前显示方式	442
----------------------	-----

INT 11H (17) 仪器	442
-----------------	-----

INT 12H (18) 内存大小	443
-------------------	-----

INT 13H (19) 磁盘	443
-----------------	-----

AH=00H (0) 重设磁盘系统	444
-------------------	-----

AH=01H (1) 取得磁盘状态	444
-------------------	-----

AH=02H (2) 读取磁盘扇区	445
-------------------	-----

AH=03H (3) 写入磁盘扇区	445
-------------------	-----

AH=04H (4) 验证磁盘扇区	446
-------------------	-----

AH=05H (5) 格式化磁盘磁道	447
--------------------	-----

INT 14H (24) 通讯	447
-----------------	-----

AH=00H (0) 设置串行口的起始值	448
----------------------	-----

AH=01H (1) 送出一个字符	449
-------------------	-----

AH=02H (2) 接收一个字符	449
-------------------	-----

AH=03H (3) 获得串行口状态	450
--------------------	-----

INT 15H (21) 录音机	450
------------------	-----

AH=00H (0) 开启录音机马达	451
--------------------	-----

AH=01H 关闭录音机马达	451
----------------	-----

AH=02H (2) 读数据段	451
-----------------	-----

AH=03H 写数据区段	452
INT 16H (22) 键盘	452
AH=00H (0) 读取下一个键盘字符	452
AH=01H (1) 检查字符是否准备好了	452
AH=02H (2) 获得功能转换状态	453
INT 17H 打印机	453
AH=00H (0) 输出字符到打印机	454
AH=01H (1) 启动打印机	454
AH=02H (2) 取得打印机状态	454
INT 18H (24) BASIC	455
INT 19H (25) 重新启动	455
INT 1AH (26) 时钟	455
AH=00H 读取目前计时器数值	456
AH=01H (1) 设置目前计时器数值	456
附录 B 扩展内存规范参考	458
§ B.1 EMS 功能一览表	458
§ B.2 EMS 错误信息一览表	469
§ B.2.1 检测 EMS 支持	470
§ B.2.2 EMS 编程注意点	471
附录 C 扩充内存规范参考	472
§ C.1 XMS 功能一览表	472
§ C.2 XMS 错误码一览表	476
§ C.2.1 测试 XMS 支持	477
§ C.2.2 XMS 编程建议	478
附录 D 硬件中断	479
INT 00H(0) 除以零	479
INT 01H(1) 单步执行	479
INT 02H (2) NMI	479
INT 03H (3) 断点	479
INT 04H (4) 溢出	479
INT 08H (8) 计时器脉冲	480
INT 09H (9) 按下键盘	480
INT 0BH (11) 串行口 1	480
INT 0CH (12) 串行口 0	480

INT 0DH (13) 硬盘驱动器.....480

INT 0EH (14) 软盘驱动器.....480

INT 0FH (15) 打印机.....481

INT 1DH (29) 显示起始表.....481

INT 1EH (30) 磁盘驱动器参数表.....481

INT 1FH (31) 图形表格.....481

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）。