北京希望电脑公司计算机病毒防治技术丛书

DOS系统维护及计算机病毒防治工具手册

吴万钊 刘中历 吴万铎 宋涵 编著

海洋出版社

北京希望电脑公司计算机病毒防治技术丛书

DOS 系统维护及
计算机病毒防治工具手册

吴万钊 刘中历 吴万铎 宋涵 编著

海洋出版社

1992年·北京

内容简介

本书是一本 DOS 系统维护和防治计算机病毒的工具书，全书分为三篇。

第一篇为系统篇，详细介绍了 DOS 系统的基本结构、引导过程，硬盘结构和系统中断文件管理及内容管理，DOS 加载程序的过程及 EXE 型和 COM 型文件的特点等内容。使读者能基本掌握计算机系统的结构和系统的启动过程。

第二篇为工具篇。详细介绍了三个系统维护工具。它们是：DEBUG，PCTOOLS 6.0 和 NORTON 5.0 。这些系统工具对系统测试，检查和维护及防治计算机病毒是非常有用的。灵活运用这些工具，将会给用户很大的帮助。

第三篇为实用解毒软件篇，介绍了几个最新版本的防治计算机病毒防治的软件，详细说明了它们的各自功能和使用方法，并针对目前流行最广的三种类型的病毒，即系统引导型、文件型、系统引导和文件引导复合型病毒。从它们各自的特点、引导方式、传播过程进行了详细地分析，并对每种类型的病毒给出了具体的诊断和清除的基本思想和办法。

在附录中列出了目前已发现的 700 种病毒的特点，供读者检查和分析病毒作参考。本书是一本实用的系统，护工具和防治病毒的工具书，可以作为大、中专学生和广大计算机用户的参考资料。

购书请与北京 8721 信箱联系，电话：2562329，邮政编码：100080

(京)新登字 087 号

责任编辑　刘莉蕾

*

DOS 系统维护及
计算机病毒防治工具手册

吴万钊　刘中历　吴万铎　宋涵　编著
希　望　审校

*

海洋出版社出版　（北京市复兴门外大街 1 号）
海洋出版社发行　兰空印刷厂印刷
开本：787×1092　1/16　印张：34.17　字数：756 千字
1993 年 10 月第二版　1993 年 10 月第二次印刷
印数：4000 — 8000 册

*

ISBN 7-5027-2405-2/TP・37　定价：19.50元

前　言

微型计算机已经在各行各业中普及，并开始逐步进入家庭。计算机与人们的日常生活日益紧密联系起来。DOS 系统是微机使用最广泛的操作系统。在 DOS 系统下有众多的系统软件、工具软件及应用软件。正是这些软件使用户的系统能发挥出其应有的效能，为人们做出很多的工作。如何使用好这些软件，维护系统的正常运行，仍然是一个摆在广大用户面前的重要问题。

伴随着计算机的发展，在这个高科技的领域中，又出现了计算机病毒，它时刻在对用户的计算机系统构成威胁。

因此，对广大的计算机用户来说，维护系统的正常运行，预防和消除计算机病毒的干扰和破坏，保护系统数据的安全，是他们需要尽快掌握的技能和迫切需要解决的问题。

本书就是根据这样的指导思想来编写的。它包括三篇共八章。

在第一篇中，较详细地介绍了 DOS 系统的结构、系统中断、文件管理、内存管理及 DOS 加载文件等方面的基础知识。这些知识是用户维护系统、防治计算机病毒所必备的。

在第二篇中，详细地介绍了 DOS 系统的两个实用工具软件，PC TOOLS 6.0 版本和 NORTON5.0 版本。这两个系统工具软件，一方面可以帮助用户分析诊断系统的运行情况，另一方面帮助用户恢复系统软硬盘中丢失的数据，它们对消除、诊断计算机病毒也非常有用。灵活、巧妙地使用这些工具，将会给用户很大的帮助。

在第三篇中介绍了三个实用的解毒软件。这些解毒软件可以有效地诊断和防治系统引导型病毒，对已知的文件型病毒也可以有效地诊断和防治。详细地分析了目前出现的几类计算机病毒的特点，为用户提供了诊断和防治计算机病毒的基本思想和方法。如果与 DOS 系统工具配合，则可以更有效地分析、防治各类计算机病毒。

在本书的附录中介绍了目前已发现的近 700 种计算机病毒的特点，这为广大的计算机用户分析、诊断和防治和计算机病毒，判断其类型和特点提供了较详细的资料。

这是一本非常实用的工具书。其中部分内容曾在一些学习班中讲授，深受学员的欢迎。这次编辑成书，献给广大计算机用户，希望对他们有所帮助。

本书在编写过程中参考了大量的系统工具书和有关的中外文资料，在此仅向译作者致谢。

由于编写的时间促，加之作者水平有限，书中错误和遗漏之处在所难免，敬请读者和计算机同行们批评指正。

作者

1992 年 3 月 于长春

目　录

第一篇 系统篇

第一章　DOS 系统分析

第二篇 工具篇

第二章 动态调试程序 DEBUG 的使用方法

第三章 Norton Utilities 5. 0 使用方法

第三篇 实用解毒软件篇

第一篇　系统篇

第一章　DOS 系统分析

目前，世界上 90% 的计算机病毒是攻击 PC 机的，而这些病毒程序都十分巧妙地利用了 PC 机使用的磁盘操作系统（即 DOS 系统）的各种强大功能及其面向用户的开放性特点，实现了对病毒程序本身的隐藏，对其他系统的传染和破坏等目的。这些病毒程序的编制水平都非常高，它们充分利用了 DOS 系统的资源。足以见得，病毒程序的编制者对 DOS 系统的深刻了解程度。

我们要检查、分析和消除侵蚀计算机系统的这些病毒程序，当然也必须对 PC 机使用的 DOS 系统有充分的了解。通过详细剖析 DOS 系统的结构及各个组成部分的特点，系统启动时 DOS 的各个模块的运行过程，系统中断向量的设置和功用以及 DOS 加载和管理文件的方式等，就可以从本质上认识计算机病毒的侵入方式和传播过程，以及对计算机系统的干扰、破坏形式。当我们彻底了解了病毒程序赖以生存的系统环境时，就为分析和消除各种类型的计算机病毒奠定了坚实的基础。

本章从以下诸方面 对 DOS 系统的结构作较详细的介绍。

① DOS 系统常用的命令简介
② DOS 系统的环境配置
③ DOS 系统模块的结构
④ DOS 系统的软盘启动
⑤ DOS 系统的引导记录
⑥ 硬盘的结构
⑦ DOS 加载程序的过程
⑧ DOS 文件的管理机制
⑨ DOS 管理文件的方式
⑩ DOS 内存分配方式
⑪ DOS 系统中断

第一节　DOS 系统常用的命令简介

DOS 系统启动成功后，出现提示符“>”。此时系统处在开工阶段，等待用户键入一个 DOS 命令或者执行一个应用程序的命令行。

DOS 命令是 DOS 操作系统提供给用户使用的各种系统管理功能。这些功能分为两类，即 DOS 的内部命令和外部命令。

表 1－1 和表 1－2 给出了所有的 DOS 内部命令和外部命令（3.0 以上版本）。

表 1—1 DOS 内部命令

命 令 字	命 令 的 含 义
BATCH	执行一批文件
BREAK②	关断 DOS 开关
BUFFERS②	置 DOS 缓冲区
CD	改变当前操作目录
CLS	清除显示器屏幕
COPY	拷贝磁盘文件
COUNTRY②	指定国别格式
CTTY	改变主控制台
DATE	输入系统日期
DEL	删除指定磁盘文件
DEVICE②	安装设备驱动程序
DIR	列磁盘文件名清单
ERASE	删除指定磁盘文件
ECHO①	置命令显示开关
FOR①	重执行命令
FCBS②	置打开的 FCB 数
FILES②	置打开的文件数
GOTO①	控制转向标号
IF①	条件执行命令
LASTDRIVE	置最后驱动器
MD	建立一子目录
PATH	建立搜索路径
PAUSE	暂停系统运行
PROMPT	设置系统提示符
REM①	显示注释信息

续表

命 令 字	命 令 的 含 义
REN①	重新命名文件名
RD	删除指定子目录
SET	设置系统运行环境
SHIFT	移位替换参数
SHELL	装载外壳程序
TIME	输入系统时间
TYPE	显示 ASCII 文件内容
VER	显示 DOS 版本号
VERIFY	校验写盘数据
VOL	显示磁盘卷标

注：①表示是批处理命令；

②表示是系统配置命令；

③表示为 DOS 3.0 以上版本有效。

表 1—2 DOS 外部命令

命 令 字	命 令 的 含 义
ASSIGN②	分派驱动器请求
ATTRIB②	置文件只读属性
BACKUP	磁盘文件转储（备份）
CHKDSK	检验磁盘状态
COMMAND	加载命令处理程序
COMP	比较磁盘文件
DEBUG	DOS 调试程序
DISKCOMP	比较两个软盘
DISKCOPY	复制整张磁盘
EDLIN	DOS 编辑程序

续表

命 令 字	命 令 的 含 义
EXE2BIN	转换 EXE 文件
FDISK	硬盘分区程序
FIND	查找指定字符串
FORMAT	格式化磁盘
GRAFTABL	装入附加图符表
GRAPHICS	屏幕拷贝图形
JOIN①	连接驱动器目录
KEYBYY①	装入键盘替换程序
LABEL①	设置磁盘卷标名
LINK	DOS 连接程序
MODE	设置设备操作方式
MORE	过滤屏幕显示
PRINT	假脱机打印文件
RECOVER	恢复磁盘文件
RESTORE	复原磁盘文件
SELECT①	选择国别代码
SHARE①	装入文件共享程序
SORT	文件排序过滤
SUBST①	驱动器替换路径
SYS	传送系统隐含文件
TREE	显示树型目录路径

注：①表示 DOS 3.0 以上版本有效

执行 DOS 命令时，必须注意以下几点：

1）所有内部命令在 DOS 常驻内存后的任何时刻，均可发出并执行。

2）所有外部命令包含在扩展名为 .COM 和 EXE 的独立文件中。发出命令时，这些文件应存储在缺省或指定驱动器的磁盘中。这样 DOS 系统的命令解释程序 COMMAND.COM 才能找到该命令并解释执行之。

3）各种 DOS 命令必须紧跟在 DOS 提示符“>”之后，输入完毕后，要按 RETURN

键。如果在 DOS 提示符再次出现之前，没有显示出错信息，则表示发出的命令执行成功。

4）命令之后可以跟一个或多个参数，系统按指定的参数执行相应的功能。若未给定参数，则系统按缺省处理。

5）输入的命令、参数既可用大写或小写字母，也可以大、小写字母混合使用。

6）输入的命令及参数之间需要用间隔符隔开，如空格、逗号、分号、等号等 。通常都是用空格把命令与参数和参数与参数之间分隔开。

这些 DOS 内部命令和外部命令的详细含义及使用方法，请读者自行参考一些 DOS 的有关书籍，这里就不赘述。

在 DOS 系统下，DOS 有一 些专用的功能键表示特定的意义，如表 1－3 所示。

表 1－3　DOS 专用键

键　组　合	特　殊　含　义
Ctrl＋Alt＋Del	重新启动系统
Ctrl＋Break（或 Ctrl＋C）	终止命令运行
Shift＋PrtSc	当前屏幕打印
Ctrl＋PrtSc	打印机联机开关
Ctrl＋NumLock（或 Pause）	暂停命令执行，按任意键恢复运行
F1 或 →	从 DOS 最后一行起，一次一个地显示字符
F2	显示最后一行 DOS 中指定字符之前的所有字符
F3	显示最后一行 DOS 行
F4	显示保留行中指定字符之后的所有字符
F5	当前显示行变为保留行
F6	文件结束符 Ctrl＋Z

第二节　DOS 系统的环境配置

DOS 系统启动时，通常以缺省值来建立自己的系统环境和配置。但从 DOS 2.0 版本开始，DOS 都提供一个系统配置文件 CONFIG.SYS 和 SET 命令，来为用户构造所希望的系统环境和配置，以适应用户应用程序的需要。

每当启动 DOS 系统时，DOS 搜索驱动器的根目录，查找 CONFIG.SYS 文件。若找到，则读取该文件并解释执行文件中的每一条命令，否则按每条命令的缺省值执行之。

SET 命令可安排在 AUTOEXEC.BAT 批文件或用户应用程序的批文件中。

利用 SET 命令可设置系统的环境块。该块包含一系列字符串信息。系统或用户应用

程序可利用环境块从父进程向子进程传递有用的信息。

系统配置文件可提供 8 种类型的命令，包括设置 ①Ctrl＋Break 的检查，②磁盘缓冲区的数量，③系统的日期和时间格式的选择，④装入设备驱动程序，⑤由 FCB 打开的文件数，⑥同时可打开的句柄文件数，⑦可允许访问的最后驱动器名，⑧指定用户外部命令处理程序 。

下面详细叙述系统配置文件的设置和功用以及系统环境的概念和设置。

一、系统配置文件

系统配置文件 CONFIG. SYS 仅在系统启动时由 DOS 解释和执行。在该文件中新增加的或改变原有配置的命令不能立即产生作用，而需要在下一次 DOS 启动后才生效。

使用编辑程序（如 EDLIN）或 DOS 的 COPY 命令可建立 CONFIG. SYS 文件。下面给出用 COPY 命令建立配置文件的步骤。

① 输入命令

C>COPY CON CONFIG. SYS ↵

② 键入指定的配置命令，每键入一条命令后按 Enter 键；

③ 键入完所有命令后，按 F6 键再按 Enter 键。

执行完上述步骤后，就在 C 盘上建立起一个 CONFIG. SYS 文件。

下面分别说明系统配置文件允许的 8 条配置命令的含义。

1. 中止请求的设置

(1) 格式

BREAK＝ON|OFF

(2) 用途

用该命令置 BREAK＝ON，在此状态下，一旦按 Ctrl＋Break 键，DOS 就响应中止请求。在编译或执行一个程序时，若出现错误或死循环，就可以按下 Ctrl＋Break 键令其停止，返回到 DOS。

开机缺省值是 BREAK＝OFF 状态。此时，仅当 DOS 或应用程序执行下述的操作时：

①标准输入设备操作（键盘）

②标准输出设备操作（显示屏幕）

③标准列表设备操作（打印机）

④标准辅助设备操作（串行通讯口）

DOS 才响应 Ctrl＋Break 键的中止请求。

2. 磁盘缓冲区数量的设置

(1) 格式

BUFFERS＝x

(2) 说明

x 是 1～99 中的任一数，缺省值为 2。

(3) 用途

该命令用来设置系统开工使用的磁盘缓冲区数量。

磁盘缓冲区是 DOS 用于存放磁盘读取或写入磁盘的数据的一块内存空间。每个缓冲

区的容量为 528 个字节，其中 512 字节存放磁盘读写最小单位 1 个扇区的内容，另 16 个字节作为存取标记供 DOS 检测用。例如，当某次要求从磁盘读出 100 个字节时，DOS 就把整个一扇区存放到 1 个 缓冲区中，并取出 100 个字节送入应用程序指定的内存区，然后对该缓冲区置"最近已访问"标记。当下一次再发出读取另一批数据的请求时，DOS 就设法使用另一个缓冲区。这样，所有缓冲区将保留最近刚访问过的数据。在 DOS 请求读取或写入一个记录时，若该记录的大小不为扇区大小的整倍数，DOS 就检查含有那个记录的扇区是否已在缓冲区。如果不在，则向磁盘发出请求并取出所需要的数据。如果数据已在缓冲区中，DOS 就简单地将在缓冲区中的记录传送到实际应用的内存区中，或将所写入的记录插入到缓冲区后再向磁盘发出写盘请求。因此，缓冲区的设置对记录的读或写不仅节省了时间，而且由于访问磁盘的次数减少而延长了磁盘和磁头的使用寿命。

某些应用程序（如 BASIC 程序或数据库管理程序）读写记录是以随机方式为主，在这种情况下，如果设置许多缓冲区，那么直接找到所需数据的机率就大。这不仅加快了存取速度，而且大大改善了应用程序的性能。对以顺序读写记录为主的应用场合（如存取整个文件），分配太多的缓冲区并无多少好处，相反，DOS 在所有缓冲区中检索某个记录所花费的时间可能要比直接从磁盘中读出该记录更长。

对于不同的应用场合，无法给出缓冲区数量的最佳值。合适的缓冲区数目通常要通过实际使用来确定。以下两个方面可作为给定缓冲区数目的依据：

① 应用程序常用的读写类型；

② 系统配置的内存容量。

对于装有硬盘的系统，推荐最少的缓冲区数目为 3～4 个。

3. 设置同时打开的文件句柄数

(1)格式

FILES＝x

(2)说明

x 是 8～255 中任意一个数，缺省值为 8。

(3) 用途

本命令设置 DOS 允许同时打开的文件句柄数。系统允许的最大值为 20，其中包括 DOS 为标准 I/O 设备预留的 5 个文件句柄：

① 标准输入设备；

② 标准输出设备；

③ 标准错误设备；

④ 辅助输入输出设备；

⑤ 标准列表设备 。

因此，为用户开放的前台任务（如 COMP 和 CHKDSK 程序）和后台任务（如 PRINT 程序和网络应用程序）中所使用的文件句柄一次至多为 15 个。DOS 为每一个句柄在 DOS 常驻区中增加 48 个字节。在系统开工时，由本命令的设置值来确定 DOS 在常驻区内预留若干个 48 字节（DOS 2.0 版本为 39 字节）的内存空间。显然，该值愈大，同时访问的磁盘文件数就愈多，但可利用的内存空间就相应减少。