肖俊良 编著

计算机病毒及其防治技术

中山大学出版社

计算机病毒及其防治技术

肖俊良 编著

中山大学出版社
·广州·

图书在版编目(CIP)数据

计算机病毒及其防治技术/肖俊良编著.—广州:中山大学出版社,1996.9
ISBN 7-306-01179-0

Ⅰ.计…
Ⅱ.肖…
Ⅲ.①计算机病毒 ②防治方法
Ⅳ.TP3

中山大学出版社出版发行
〔广州市新港西路135号〕
广东省农垦总局印刷厂印刷
广东省新华书店经销

787×1092毫米　16开本　14印张　32万字
1996年9月第1版　1996年9月第1次印刷
印数:1—5000册　定价:18.00元

前　言

随着计算机在各项业务中的广泛使用，计算机病毒传播也更为流行。只要使用受病毒感染的磁盘，该机就有可能成为病毒的扩散者，进而感染与之发生读写关系的磁盘，扩散到别的计算机，引起病毒的广泛传播。

计算机病毒多由那些精通计算机的人编制，他们为了显示自己的编程技巧，或者为了开恶意的玩笑等。一般说来，计算机病毒都具有很巧妙的编程技巧，因而具有易传播、隐蔽及能复制自身等特点。

然而，归根到底，计算机病毒也是一种计算机程序，只不过是一种专门利用计算机系统本身的弱点攻击计算机资源的程序。因此病毒本身除了编制巧妙、目的恶劣之外，并没有什么可怕，利用现有的反病毒软件工具，是完全可以发现、清除病毒的。

本书介绍信誉较好的软件出版商的软件产品，其中包括 McAfee Associates 公司，Central Point Software 公司及我国公安部的。

清除计算机病毒的正确步骤应该是，首先利用公安部的 KILL 程序对微机系统进行病毒诊治，以确保当前使用的微机系统（特别是硬盘）没有“国产病毒”，然后才考虑使用国外的病毒清除软件。

本书介绍的软件都是基于微机系统 ROM（只读存储器）中的固化程序是可信的（TRUSTED），这意味着所购买的微机产品是由著名厂家制造的。如果微机产品是由信誉没有保障的厂家制造的，则不能保证 ROM 中的 BIOS（基本输入/输出系统）不包含计算机病毒。

现在我们的最好成果是：《引导扇区（即操作系统）型病毒通用清除软件 －KV－BOOT》、《带知识库的文件寄生型病毒清除软件－KV－FILE》、《通用病毒防御系统》及《可执行文件通用免疫系统》。

林东海高级工程师（教授级）、关朵霏副教授对本书进行了认真的审阅，并提出许多修改意见，在此深表谢意。

由于本人水平所限，不妥之处在所难免，敬请读者赐教。

肖俊良

1996 年 4 月

目　录

第一章　计算机病毒概述

一、计算机病毒的概念

什么是计算机病毒呢？目前尚未有一个公认的定义，不过从本质上来说，计算机病毒实际上是一段程序，只不过它不同于一般的程序，这段程序能够传染其他程序并进行自我复制，能够对计算机系统进行各种干扰和破坏，同生物学中的“病毒”具有相似之处，这也正是这些程序之所以被称为计算机病毒的原因。总结目前出现的各种计算机病毒的共性，我们可以这样说，计算机病毒就是通过某种途径传染并潜伏在计算机存储介质（磁盘）中，当达到某种条件时被激活的，对计算机系统进行干扰和破坏的一段程序或指令的集合。

二、计算机病毒的特性

目前，在世界范围内发现的计算机病毒已超过1000种，在国内已发现的计算机病毒也有几十种，例如：“小球”病毒、“大麻”病毒、“黑色星期五”病毒、“雨点”病毒、“磁盘杀手”病毒、“音乐”病毒等等。尽管这些病毒各自的传染方式、传染目标不一，发作条件各异，干扰和破坏程度不同，但是，它们都有如下共同的特性：

1．传染性

传染性是所有病毒程序都具有的一大特性。通过传染，病毒就可以扩散。病毒程序通过修改磁盘扇区信息或文件内容并把自身嵌入其中的方法达到病毒的传染和扩散。被嵌入到的程序叫做宿主程序。

2．寄生性

病毒程序嵌入到宿主程序中，依赖于宿主程序的执行而生存，这就是计算机病毒的寄生性。病毒程序在侵入到宿主程序中后，一般对宿主程序进行一定的修改，使得宿主程序一旦执行，病毒程序就被激活，从而可以进行自我复制和繁衍。

3．破坏性

大多数计算机病毒在发作时都具有不同程度的破坏性，有的干扰计算机系统的正常工作，有的占用系统资源，有的则修改和删除磁盘数据或文件内容。

以上是计算机病毒的三个主要特点，除此之外，计算机病毒还有如下两个特点：

4．隐蔽性

计算机病毒的隐蔽性表现在两个方面，一是传染过程的隐蔽性，大多数病毒在进行传染时速度是极快的，一般不具有外部表现，不易被人发现。二是病毒程序存在的隐蔽性，一般的病毒程序都夹在正常程序之中，很难被发现，而一旦病毒发作出来，往往已

经给计算机系统造成了不同程度的破坏。

5．**潜伏性**

计算机病毒侵入系统后，一般不立即发作，而是具有一定的潜伏期，病毒不同，其潜伏期的长短就不同，有的潜伏期为几个星期，有的潜伏期为几年。在潜伏期中，只要条件许可，病毒程序就会不断地进行自我复制、繁衍和传染。一旦条件成熟，病毒就开始发作，发作的条件依病毒的不同而不同，这一条件是计算机病毒设计人员所设置的。病毒程序在运行时，每次都要检测发作条件。

三、计算机病毒的分类

对于计算机病毒可以从不同的角度来进行分类：

1．**按其破坏的程度划分**

（1）良性病毒

良性病毒危害性小，不破坏系统和数据，只是对系统的正常工作进行一些干扰。如“小球”病毒就属于良性病毒。

（2）恶性病毒

恶性病毒危害性大，这种病毒一旦发作就会修改和删除数据文件的内容，破坏磁盘扇区信息，使系统处于瘫痪状态。例如，“黑色星期五”就属于恶性病毒。

2．**按其寄生方式划分**

（1）操作系统型病毒，也称引导扇区型病毒

这种病毒通过修改磁盘引导记录使自身占据磁盘引导扇区，在启动系统时进入计算机内存并得以执行，这样就使系统处于带毒状态，从而可以进行传染和破坏活动。如“小球”病毒、“大麻”病毒都是操作系统型的病毒。

（2）外壳型病毒，也称文件型病毒

这种病毒程序一般附着在宿主程序的首尾，并修改宿主程序使宿主程序执行时首先执行并激活病毒程序，使病毒程序得以传染、繁衍和发作。例如，“雨点”病毒、“黑色星期五”等就属于外壳型病毒。

（3）入侵型病毒

入侵型病毒在传染时往往对宿主程序进行一定的修改，以使自身嵌入到宿主程序中，而不仅仅是包围在宿主程序的周围。这种病毒一般是针对某些特定的程序而设计的，一旦这种病毒侵入到一个程序之中，要想对该程序进行解毒是比较困难的。

（4）源码病毒

这种病毒在程序被编译之前插入到诸如 Fortran、C、Pascal 等语言编写的源程序中，完成这种工作的病毒程序一般寄生在编译处理程序或连接程序中。

除了上面两种分类之外，按其攻击的机种可分为：攻击微型机的、攻击小型机的、攻击工作站的等等。其中以攻击 IBM PC 机及其兼容机的病毒为最多，这是由于大部分病毒程序都是以 DOS 系统为攻击对象。

四、计算机病毒的一般结构

尽管目前出现的计算机病毒种类繁多，形式各异，但是它们作为一类特殊的计算机

程序，从宏观上来划分，都具有相同的结构，即计算机病毒程序的三大功能模块：引导模块、传染模块和干扰、破坏模块。其中传染模块又可以分为：传染条件判断模块和实施传染模块；干扰、破坏模块又可以分为干扰、破坏条件判断模块和实施干扰、破坏模块。其结构形式如图 1.1。

引导模块的功能是将病毒程序由外存引入内存并使其后面的两个模块处于激活状态。传染模块的功能是，在传染条件满足时把病毒传染到所攻击的对象上。干扰、破坏模块的功能是，在病毒发作条件（干扰、破坏条件）满足时，实施对系统的干扰和破坏活动。需要说明的是，并不是所有的计算机病毒都由这三大功能模块组成，有的可能没有破坏模块，如“巴基斯坦”病毒；而有的病毒在三个模块之间可能没有明显的界线。

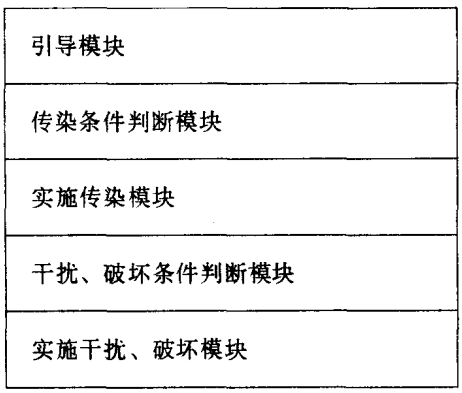

图 1.1　计算机病毒程序结构

五、计算机病毒的作用机制

计算机病毒结构的三大模块各有其自己的作用机制，我们把它们分别叫做引导机制、传染机制和破坏机制。

1. 计算机病毒的引导机制

计算机病毒的寄生目标有两种，一种是寄生在磁盘引导扇区；另一种是寄生在可执行文件（.EXE、.SYS 或 .COM）中。寄生的方法也有两种，一种是采用替代法；另一种是利用链接法。所谓替代法是指，病毒程序用自己的部分或全部指令代码，替代磁盘引导扇区或文件中的全部或部分内容。所谓链接法则是指病毒程序将自身代码作为正常程序的一部分与原有正常程序链接在一起，病毒链接的位置可能在正常程序的首部、尾部或中间。寄生在磁盘引导扇区的病毒一般采取替代法，而寄生在可执行文件中的病毒一般则采用链接法。

对于寄生在磁盘引导扇区的病毒来说，病毒引导程序占有了原系统引导程序的位置，并把原系统引导程序搬移到一个特定的地方。这样系统一启动，病毒引导模块就会被自动地装入内存并获得执行权，然后该引导程序负责将病毒程序的传染模块和干扰、破坏模块装入内存的适当位置，并采取常驻内存技术以保证这两个模块不会被覆盖，接着对该两个模块设定某种激活方式，使之在适当的时候取得执行权。处理完这些工作

后，病毒引导模块将系统引导模块装入内存，使系统在带毒状态下运行。

对于寄生在可执行文件中的病毒来说，病毒程序一般通过修改原有可执行文件，使该文件执行时首先转入病毒程序引导模块，该引导模块完成把病毒程序的其他两个模块驻留及初始化的工作，然后把执行权交给执行文件，使系统及执行文件在带毒的状态下运行。

2．计算机病毒的传染机制

所谓传染是指计算机病毒由一种载体传播到另一个载体，由一个系统进入另一个系统的过程。这种载体一般为磁盘或磁带，它是计算机病毒赖以生存和进行传染的媒介。但是，只有载体还不足以使病毒得到传播。促成病毒的传染还有一定的先决条件。这可分为两种情况，其中一种情况是，用户在进行拷贝磁盘或文件时，把一个病毒由一个载体复制到另外一个载体上；或者是通过网络上的信息传递，把一个病毒程序从一方传递给另一方。这种传染方式叫做计算机病毒的被动传染，另外一种情况是，计算机病毒是以计算机系统的运行以及病毒程序处于激活状态为先决条件。在病毒处于激活的状态下，只要传染条件满足，病毒程序就能主动把病毒自身传染给另一个载体或另外一个系统。这种传染方式叫做计算机病毒的主动传染。对于主动传染而言，病毒传染的过程是这样的：在病毒引导模块将病毒传染模块驻留内存的过程中，通常还要修改系统中断向量入口地址（例如 INT 13H 或 INT 21H），使该中断向量指向病毒程序传染模块。这样，一旦系统执行磁盘读写操作或系统功能调用，病毒传染模块就会被激活，传染模块在判断传染条件满足的条件下，把病毒自身传染给被读写的磁盘或被加载的程序，也就是实施病毒的传染，然后再转移到原中断服务程序执行原有的操作。

3．计算机病毒的破坏机制

破坏机制在设计原则、工作原理上与传染机制基本相同。它也是通过修改某一中断向量入口地址（一般为时钟中断 INT 8，或与时钟中断有关的其他中断，如 INT 1CH）使该中断向量指向病毒程序的破坏模块。这样，当系统或被加载的程序访问该中断向量时，病毒破坏模块被激活，在判断设定条件满足的情况下，对系统或磁盘上的文件进行破坏活动。这种破坏活动不一定都是删除磁盘文件，有的可能是显示一串无用的提示信息，例如，在用感染了“大麻病毒”的系统盘进行启动时，屏幕上会出现“YOUR PC IS NOW STONED”。有的病毒在发作时，会干扰系统或用户的正常工作，例如“小球”病毒在发作时，屏幕上会出现一个上下来回滚动的小球。而有的病毒，一旦发作，则会造成系统死机或删除磁盘文件。例如，“黑色星期五”病毒在激活状态下，只要判断当天既是 13 号又是星期五，则病毒程序的破坏模块即把当前感染该病毒的程序从磁盘上删除。

六、计算机病毒的预防和消除

不论是良性病毒还是恶性病毒，一旦侵入系统都会给系统带来这样或那样的干扰、破坏活动，特别是通过网络传播的计算机病毒，能在很短的时间内使整个计算机网络处于瘫痪状态，从而造成巨大的损失。因此，预防病毒的侵入、阻止病毒的传播，及时地消除计算机病毒是一项非常重要的工作。而在这些工作中，预防病毒的侵入显得尤为重

要，因为没有病毒的侵入，也就没有病毒的传播，更不需要消除病毒。

1．积极地预防计算机病毒的侵入

计算机病毒的传播需要以软盘或硬盘为媒介，使用一个带毒的软盘或硬盘启动系统或在系统状态下运行一个带毒的软件，都会使系统处于带毒状态。这样在这种状态下使用的磁盘和运行的文件都有可能感染上病毒。为此，预防计算机病毒的侵入要从管理上入手，在以下几个方面加以注意：

（1）系统启动盘要专用，而且要加上写保护，以防病毒侵入。

（2）不要乱用其他来历不明的程序或软件，也不要使用非法复制或解密的软件。

（3）对于外来的机器或软件要进行病毒的检测，在确认无毒的情况下方可使用。

（4）对于带有硬盘的机器最好专机专用或专人专机，以防病毒侵入硬盘。

（5）对于重要的系统盘、数据盘以及硬盘上的重要信息要经常备份，以使系统或数据遭到破坏后能及时得到恢复。

（6）网络上的计算机用户要遵守网络软件的使用规定，不能在网络上随意使用外来的软件。

除了从管理上预防计算机病毒之外，还可以从技术上预防计算机病毒的侵入。从技术上预防计算机病毒的一种方法是：在系统启动盘上的自动批处理文件中加入一个病毒检测程序，该检测程序在系统启动后常驻内存，对启动盘进行病毒的检查，并随时监视系统的异常举动（例如，中断向量被异常地修改，出现异常的磁盘读写操作等），一旦发现有病毒侵入的迹象就进行报警，以提醒用户及时地消除病毒。另外一种技术上的保护措施是：设计一种硬件设备，系统一启动该设备便进行工作，时刻监视系统的各种异常举动并及时报警，以防止病毒的侵入。目前在市场上销售的计算机防病毒卡就是这样的一种设备。

2．及早发现计算机病毒

尽管采取了各种各样的预防措施，往往由于不慎会使计算机病毒乘虚而入。病毒一旦侵入，就会不断地自我复制、传染和破坏。显然，对于一个侵入了计算机病毒的系统来说，应及早地发现病毒以决定消除病毒的方法，从而尽可能地减少病毒造成的损失。

那么怎样才能及时地发现计算机病毒呢？一般来说，不论何种病毒，一旦侵入系统，都或多或少，或隐或显地给系统带来一些不正常的现象，根据这些现象可以及早地发现病毒。根据实践经验，出现以下不正常现象有可能是病毒程序所致：

（1）屏幕上出现的异常现象

屏幕上出现莫名其妙的提示信息、特殊字符、闪亮的光斑、异常画面。

（2）系统运行时出现的异常现象

① 系统启动时的速度变慢，或系统运行的速度变慢。

② 在进行磁盘文件读写时速度变慢。

③ 系统上的设备无故不能使用，例如系统不承认C盘。

④ 系统在运行时莫名其妙地出现死机现象。

⑤ 喇叭无故发出声音。

⑥ 中断向量被无故地修改。

⑦ 内存容量异常地突然变小。

(3) 程序运行时出现的异常现象

① 程序装入的时间比平常长。

② 原来能正常执行的程序在执行时出现异常或死机。

③ 程序的长度变长。

(4) 磁盘及磁盘驱动器的异常现象

① 磁盘上莫名其妙地出现坏的扇区。

② 一些程序或数据莫名其妙地被删除或修改。

③ 在进行其他操作时系统无故地读写磁盘。

(5) 打印机打印速度变慢或打印异常字符

出现上面所列的各种现象，应及时关机，然后用一个确认没有病毒的系统盘重新引导系统，以便在无毒的情况下检测和消除磁盘上的病毒。

3. 及时消除计算机病毒

如果发现系统感染了病毒，就要及时地检测和诊断病毒，以决定病毒的类型和种类以及其所在的文件和磁盘，为进一步消除病毒作准备。就目前所发现的各种计算机病毒来看，病毒传染的目标分为两种：一是传染磁盘引导扇区（BOOT），一是传染 .EXE 和 .COM 文件。要检测和诊断病毒，首先要观察系统所出现的症状和异常特征，结合事先了解的各种病毒的特征初步判定病毒的类型和种类，然后借助于一定的软件工具进行针对性的检测和诊断，确定病毒的类型及所在，最后利用解毒工具或软件消除病毒。检测和消除计算机病毒有两种方法：

(1) 人工检测和消毒

这种方法是通过使用工具软件 DEBUG 和 PCTOOLS 等，在掌握病毒原理的基础上，对带毒的磁盘或软件进行检测和消毒，适合于病毒侵入范围较小的情况下。DEBUG 是一个能够监督和控制可执行文件，跟踪其执行过程的工具性软件，是分析和消除病毒程序最有力的工具之一。PCTOOLS 也是一个实用的软件工具包，它的 F 命令可以在整个文件中或整个磁盘中搜索一个字符串，这在检测病毒的特征字符串时非常有用。此外，它的 E 命令可以直接对磁盘或可执行文件（.EXE 或 .COM）进行修改，所以它也是检测和消除计算机病毒的最有力的工具之一。

(2) 软件检测和消毒

这种方法是采用现成的软件自动地对病毒进行检测和消除，适合于病毒传播范围较大情况下。目前，在国内流行的病毒检测软件如 CV.EXE、SCAN.EXE 等，可以对多达 1000 种的计算机病毒进行检测。在解毒软件方面，“SOS 反病毒系统”可以对软、硬盘上的“小球”病毒、“大麻”病毒、“黑色星期五”病毒等多种计算机病毒进行诊断、消除和免疫。此外，用户可以在掌握某种病毒程序的基础上，有针对性地自行编写检测和解毒软件。

就两种方法相比较而言，人工检测和消毒操作难度大、技术复杂，它需要操作人员有一定的软件分析经验以及对操作系统有一个深入的了解。而软件检测和消毒的方法操作简单，使用方便，适合于一般的计算机用户学习使用。但是，由于计算机病毒的种类

较多，程序复杂，再加上不断有新的变种，所以软件消毒方法不可能消除所有的病毒。

七、计算机病毒的免疫及其局限性

我们知道，计算机病毒的传染模块一般包括传染条件判断和实施传染两个部分，在病毒被激活的状态下，病毒程序通过判断传染条件满足与否，以决定是否对目标对象进行传染。一般情况下，病毒程序在传染完一个对象后，都要给该被传染对象加上传染标识，传染条件的判断就是检测被攻击的对象是否存在这种标识，若存在这种标识，则病毒程序不对该对象进行传染；若不存在这种标识，则病毒程序就对该对象实施传染。由于这种原因，人们自然会想到是否能在正常对象中加上这种标识，就可以不受病毒的传染，起到免疫的作用呢？我们说这种方法只能在一定的条件下，对一定范围内的有限的几种病毒起到免疫作用。也就是说，这种免疫方法有一定的局限性，它的局限性表现在以下几个方面：

1．对于不设感染标识的病毒不能达到免疫的目的。有的病毒程序只要在激活的状态下，会无条件的把病毒传染给被攻击的对象，而不论这种对象是否已经被病毒感染过或者是否具有某种标识。

2．对已改变其标识的病毒不能达到免疫的作用。例如，“黑色星期五”病毒对.COM文件传染的条件是，判断该文件的最后五个字节是否为“MsDos”，若是则不对该文件进行传染。根据这种道理，我们可以给某一文件的末尾加上这样的字符串，从而达到免疫的目的。但是，如果有一种“黑色星期五”的变种病毒，不以该字符串为传染标识，这种办法就不起作用了。

3．由于病毒的种类较多，又由于技术上的原因，不可能对一个对象加上各种病毒的免疫标识，这就使得该对象不能对所有的病毒具有免疫的作用。

综上所述，计算机病毒的出现，给计算机系统造成严重的威胁，也给计算机的应用带来了巨大的困难，要消除计算机的病毒，减少计算机病毒的危害，需要做长期的、艰苦的工作。

第二章　计算机病毒解析技术基础

第一节　磁盘的基本知识

一、概述

1．面、道、柱面和扇区、簇

磁盘分为两种：软盘（Floppy Disk）和硬盘（Fixed Disk）。

磁头（Head）对应的磁盘区域称为面（side）。软盘驱动器有两个磁头（0－1头），故软盘有2面（0面及1面）；硬盘一般有4个磁头（0－3头），对应4面（0－3面）。以转轴中心为圆心，把磁盘表面划分为数个半径不等的同心圆，称作磁道（track）。5.25″软盘（道密度为48 TPI）有40磁道，从外往内依次编号为0到39；20M硬盘共614磁道，从外往内依次编号为0到613。不同面上相同直径的磁道构成的圆筒，称为柱面（Cylinder）。硬盘面数较多，“柱面”一词十分形象，柱面数等于磁道数。对同一磁道，又以索引孔与圆心连线为起点逆时针地把圆周分为数个夹角相等的扇区（sector），每扇区可存取512字节（byte）。5.25″软盘一般分为9扇区/道，硬盘为17扇区/道。簇（cluster）是磁盘空间分配的最小单位。一个簇由顺序访问的几个扇区组成，每簇扇区数量与盘的类型以及DOS版本有关。5.25″软盘的一簇由2扇构成，大小是1 KB。20 M硬盘用DOS 2.0或2.1版本格式化后，每簇有8扇区，共4KB；用DOS 3.0或更高版本格式化后，每簇4扇区，大小2 KB。

2．物理扇区及逻辑扇区

磁盘的扇区定位可通过两种方式：物理扇区及逻辑扇区。

物理扇区由驱动器号、面（头）号、柱面（道）号及扇区号四个参数确定，是某个扇区在磁盘上的绝对地址。驱动器号为盘片所在驱动器标识符对应的一个参数，A为0，B为1，C为2（在Debug规定为2，在磁盘中断服务程序中规定为80h）……，以此类推。在同一磁盘上，第一个物理扇区为0面0道1扇区，最后一个扇区为1面39道9扇区（软盘），或3面613柱面17扇区（硬盘）。磁头在访问磁盘时是按先访问完同道（柱面）、同面的所有扇区后再访问下一面的所有扇区，然后才移到下一柱面（道）。

逻辑扇区是以DOS区域起始的物理扇区为逻辑0扇区，按扇区的访问顺序进行连续编址的扇区阵列。例如软盘上DOS区域从物理扇区0面0道1扇区开始，该扇区为逻辑0扇区，与它相邻的0面0道2扇区为逻辑1扇区，等等。硬盘因涉及DOS分区，其DOS区域起点与软盘不同。用DOS 3.0以下版本分区的硬盘，DOS分区从0面0柱面2

扇区开始，对应为逻辑 0 扇区；用 DOS 3.0 以上（含 DOS 3.0）的版本分区硬盘，DOS 分区起点从 1 面 0 柱面 1 扇区开始，对应为逻辑 0 扇区。可见硬盘的逻辑 0 扇区对应的物理扇区因 DOS 版本的不同而存在差异，除此之外，逻辑扇区的编址方法与软盘完全相同。

3．DOS **磁盘结构**

DOS 格式化磁盘由四个区域组成：引导扇区（Boot Area）（硬盘含主引导扇区）、文件分配表（FAT）、根目录表（FDT）和文件数据区（Data Area）。其中第二、三区的长度因磁盘类型的不同而不同。下表列出了软盘和硬盘的区域分布。

表 2.1　磁盘的组成区域

逻辑扇区号	对应扇区	起始物理扇区			逻辑扇区号	对应扇区
		面号	柱面号	扇区号		
0	BOOT 区	0	0	1		主引导区
1—4	FAT 表	1	0	1	0	BOOT 区
5—11	根目录表	1	0	2	1—82	FAT 表
12—719	数据区	1	1	16	83—114	根目录表
		3	1	14	115—41598	数据区

360K 软盘分布　　20M 硬盘分布

主引导扇区位于硬盘的 0 面 0 柱面 1 扇区，是硬盘上的第一物理扇区。由主引导程序（位移量 000H－1 BDH）和分区表（Partition Table）（位移量 1BEH－1FFH）两部分组成，最后两字节（位移量 1 FEH －1 FFH）“55AA”为主引导区结束标记。主引导程序用于硬盘启动时将系统控制转移给用户指定的并在分区表中登记了的某个操作系统；分区表用于指明硬盘划分情况，含四个可能的分区，每个分区的记录占用 16 字节，DOS 由 FDISK 程序建立。下图显示了仅有一个 DOS 分区（0 面 0 柱面 2 扇区 － 3 面 98 柱面 145 扇区）的分区表内容。

```
0DA1：02BE                                                    00  00
0DA1：02C0 00  00  00  00  00  00  00  00  -  00  00  00  00  00  00  00  00
0DA1：02D0 00  00  00  00  00  00  00  00  -  00  00  00  00  00  00  00  00
0DA1：02E0 00  00  00  00  00  00  00  00  -  00  00  00  00  00  00  80  00
                                                              —   —
                                                              ①
0DA1：02F0 02  00  01  03  91  62  01  00  -  00  00  4B  A2  00  00  55  AA
           ——  —   ——————  ——————————————  ——————————————  ——————
           ②   ③   ④       ⑤               ⑥               ⑦
```

①——引导指示符（80h 为引导分区，00h 为非引导分区）；

②——分区开始地址（面号，扇号，柱面号）；

③——OS指示符（01h为12比特/FAT项的DOS系统，04h为16比特/FAT项的DOS系统）；

④——分区结束地址（面号，扇号，柱面号）；

⑤——该分区之前的扇区数；

⑥——该分区占用扇数；

⑦——分区结束符。

每个DOS格式化的磁盘，其最初部分是引导扇区，其中包括一张称为BIOS参数块（Bios Parameter Block，简称BPB）的表格，表中的参数与引导扇区的其他参数一起描绘了整个磁盘的使用情况（图2.1）。从DOS的角度出发，磁盘空间可分为两大部分：系统占用部分及文件正文存贮部分（图2.2）。系统占用部分包括隐藏扇区、保留扇区、FAT占用扇区及目录占用扇区。隐藏扇区及保留扇区可由引导扇区中查出，后两者可由公式计算求得。

FAT占用扇区 = FAT个数×每个FAT占用的扇区

目录占用扇区 = [（根目录项数×20H + 1FFH）÷每扇字节数]

其中，20H是每个目录项占用的字节数，加1FFH是为了在总字节数不够一扇（200H）时补足一扇，[]是取整操作。

这样，系统占用的总扇区数也即DOS文件正文区起始逻辑扇区为：

正文区起始逻辑扇区 = 隐藏扇区 + DOS保留扇区 + 目录占用扇区

相应地，

正文区总扇数 = 磁盘总逻辑扇区数 - 正文区起始逻辑扇区

FAT表中的每一项对应正文区的一个簇，记录该簇的使用情况，因此FAT表的项数就是正文区的簇数，计算公式为：

正文区总簇数 = FAT表的项数 = 正文区总扇数÷每簇扇数

当其值>0FF0H时，FAT表每项占2个字节，否则占1.5字节。通过修改FAT表中某项的值，就可以改变对应簇的使用情况。

要想读取正文区某簇的内容，只有簇号是不够的，还必须将其转化为磁盘的物理磁头号、磁道号及扇区号，取得这些值的第一步是将簇号转换为对应的逻辑扇区号，公式如下：

逻辑性扇区号 =（簇号 - 2）×每簇扇数 + 正文起始逻辑扇区

由此可得：

头号 = [逻辑扇区÷每道扇数] Mod 头数

道号 = [[逻辑扇区÷每道扇数] ÷头数]

扇区号 =（逻辑扇区 Mod 每道扇数）+ 1

其中 Mod 是取余数操作。

	3字节	转移到引导程序的JUMP指令	+0
	8字节	OEM名字及版本	+3
BPB	字	每扇字节数	+B
	字节	每簇扇数	+D
	字	保留扇数	+E
	字节	FAT个数	+10
	字	根目录项数	+11
	字	逻辑扇区总数	+13
	字节	磁盘特征（表明磁盘的类型，如360K）	+15
	字	FAT占用扇数	+16
	字	每道扇数	+18
	字	磁头数	+1A
	字	隐藏扇区数	+1C

图2.1 引导扇区格式

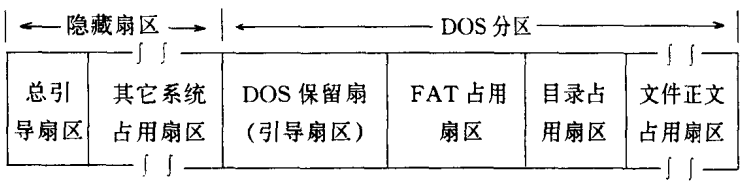

图2.2 磁盘存储示意图

4．磁盘中断服务程序

int 13h是ROM BIOS软中断，其中断向量（地址00：4C - 00：4F）由ROM BIOS在启动时填入。其调用号AH可以有00 - 05六个值，我们感兴趣的是AH=2和AH=3的读/写磁盘扇区功能。与此相关的几个参数为：

AH——调用号（读为02H，写为03H）

AL——读/写扇区数（软盘≤8，硬盘≥128）

DH——磁头号（软盘0 - 1，硬盘0 - 7）

DL——驱动器号（软盘0 - 3，硬盘80 - 87H）

CH——扇区号（软盘1 - 9，硬盘1 - 17）

ES：BX——读/写缓冲区地址

如下的程序用于读出A盘0面0道1扇区的BOOT引导扇区到缓冲区BUF（地址CS：0400）

```
0DB6：0100 8CC8          MOV AX，CS
```

```
0DB6：0102 8EC0          MOV ES，AX
0DB6：0104 BB0004        MOV BX，0400      ；送 BUF 地址→ES：BX
0DB6：0107 B001          MOV AL，1         ；读 1 扇
0DB6：0109 B200          MOV DL，0         ；读 A 盘
0DB6：010B B600          MOV DH，0         ；0 面
0DB6：010D B500          MOV CH，0         ；0 道
0DB6：010F B101          MOV CL，1         ；1 扇区
0DB6：0111 B402          MOV AH，2         ；读功能
0DB6：0113 CD13          INT 13            ；调 INT 13H
0DB6：0115 CD20          INT 20            ；正常退出
```

第二节　DOS 有关知识

一、.COM 文件及 .EXE 文件的装入

.COM 文件和 .EXE 文件是 DOS 的两种二进制代码的可执行文件。COM 文件中的程序代码只在一个段内运行，文件长度不超过 64K 字节，其结构比较简单。.EXE 文件则不同，它可使用多个段，文件长度可大于 64K，在装入内存时涉及重定位问题，因而其结构较复杂。

.EXE 文件由文件头（Header）和重装入模块（Load Module）两大部分组成。文件头又由格式化区（Format Area）和重定位表（Relocation Table）组成。前者长 28 字节，如表；后者紧接格式化区之后，长度不定，重定位项数等于程序段数，在格式化区位移量为 06－07h 处指出。装入模块为程序代码部分，从偏移量 512 字节开始。

由于 COM 文件与 .EXE 文件在结构上的不同，它们在调入执行时也有很大差别。

COM 文件在调入时，DOS 将全部可用内存分配给用户程序。四个寄存器 DS（DataSegment 数据段），CS（Code Segment 代码段），SS（Stack Segment 堆栈段）和 ES（ExtraSegment 附加段）全部指向程序段前缀（PSP，由 DOS 建立，是 DOS、用户程序及命令行之间的接口）的段地址。指令指针 IP 置为 0100h，从程序的第一条指令开始执行；栈指针 SP 置为程序段的末尾。

.EXE 文件在申请内存后，把装入模块读入内存指定区域（尽量装入内存高地址）。DS、ES 指向程序段前缀 PSP 而不是指向用户程序的数据段和附加段；CS，IP，SS，SP 由用户程序的文件头的格式化区域确定并通过再定位调整。

了解 .COM 文件及 .EXE 文件的结构与执行过程将有助于分析一类“执行文件型病毒”。