防治病毒软件

CPAV使用指南

福建省凯特新技术联合开发中心　编

福建科学技术出版社

防治病毒软件
CPAV使用指南

福建省凯特新技术联合开发中心　编

（闽）新登字 03 号

防治病毒软件 CPAV 使用指南
福建省凯特新技术联合开发中心编
*
福建科学技术出版社出版、发行
（福州得贵巷 27 号）
福建省新华书店经销
福州 7228 工厂印刷
开本 787×1092 毫米 1/16　8.5 印张 2 插页 196 千字
1993 年 6 月第一版
1993 年 6 月第 1 次印刷
印数 1—8 200
ISBN 7—5335—0662—6　/TP・7
定价：5.80 元

序

我国自从发现首例计算机病毒至今短短几年，病毒正以迅猛的速度传播，计算机受病毒感染情况相当严重，有些重要部门的信息资源已受到不同程度的侵袭和损害。在这种情况下，福建省公安厅计算机安全监察处的3位年轻同志编译了这本《防治病毒软件CPAV使用指南》，率先公开发行，为防治计算机病毒做了一项有益的工作。

他们从事计算机安全监察工作多年，积累了防治计算机病毒的丰富经验，从目前世界上众多的抗病毒软件中，精选出了一个功能很强且较为实用的抗病毒软件——CPAV，推荐给用户。《防治病毒软件CPAV使用指南》不是原作《CPAV使用手册》的简单翻版，而是作者站在用户角度，讲解如何使用CPAV并提出自己见解，通过精心编辑而成。该书读起来通俗易懂，即使是初学者亦能很快掌握，同时对专业人员也有一定启迪作用。它将为您走进CPAV天地提供一条捷径。

福州大学计算机系

何　天　牧

1992年10月

编 者 的 话

本书从使用者这一 角度出发，较详细地阐述了世界著名的抗病毒软件 CPAV V1.2 的使用方法、使用技巧以及使用中遇到的各种问题的解决办法。CPAV 是目前众多的抗病毒软件中功能最强的一种，能检测、清除一千多种病毒，并且有较好的免疫及对未知病毒的前报功能。书中附录还提供许多防治病毒的实用资料。我们编写本书的目的在于让广大计算机用户通过了解、熟悉 CPAV，把它作为防治计算机病毒的一种有力工具，使计算机病毒的破坏作用降到最低程度。本书可供各类院校、机关、科研单位、生产单位、计算机销售部门及家庭计算机用户参考。

本书由黄文同志主编，潘东升、林锐同志参加编写工作。在编写过程中得到福州大学何天牧教授的大力支持，在此表示衷心的感谢！

因为时间较仓促，错误在所难免，望广大读者批评指正。

1992 年 10 月 于福州

目　　录

第一章　计算机病毒概述

近几年来计算机病毒在世界上包括在我国不断出现，且迅速蔓延。随着计算机网络的覆盖面日益扩大，计算机的普及范围不断增加，计算机病毒给我们的科研、生产和工作以至日常生活带来的危害越来越大，使人类社会蒙受了巨大损失。

当计算机遭受到计算机病毒感染后，轻者屏幕显示被干扰，计算机运行速度降低，重者使计算机内软盘和硬盘上保存的文件、数据被改写或丢失殆尽，甚至于使整个计算机系统瘫痪。据国际信息处理联合会总务委员会的报告，自从1984年美国正式公布计算机病毒以来，已知的计算机病毒超过了2000种，现在以每天至少增加两种的速度递增。在我国大陆首次发现的计算机病毒，系1989年3月西南铝加工厂出现的称作“乒乓”的病毒。据报道，在海湾战争期间，美国首次使用计算机病毒为武器破坏伊拉克电脑工作。伊拉克从法国购买了一种用于空防系统的新型电脑打印机，美国间谍把含有计算机病毒的芯片插到这种打印机里，这种病毒会使伊拉克军事指挥中心的主计算机失灵。美国官员说，他们达到了预期的目的。尽管后来人们了解到这个故事只是美国电视记录片的内容，但是着实使美国军方指挥官吓出一身冷汗。因为计算机病毒的受害者如果是美军自己的话，后果不堪设想。

刚刚出现计算机病毒时，人们谈“毒”色变，经过一段时间的接触，人们有了一定认识，心理上也有了一定的承受力。为了预防计算机病毒，广大计算机用户要树立计算机安全管理意识，制定严格的制度，做到以防为主，以“治”为辅。不用来历不明的磁盘，外来的软件要先经过检查后再用，计算机让他人使用或维修过也要确认没有病毒才能投入正常工作。计算机病毒的数量日益增多，花样不断翻新，攻击性越来越强。可是我们没有必要杞人忧天，正如人类自身都是处在各种各样病毒包围的环境中，经历了无数次的大瘟疫，通过顽强地抗争至今仍然健康地生活一样。只要共同努力，我们所处于的信息社会应当会不断地发展前进。

1、计算机病毒定义。计算机病毒是1984年在一次国际计算机安全学术会议上提出的，目前还没有公认的定义。作者理解为计算机病毒是一种具有隐蔽性、传染性（自我复制）以及破坏性的计算机程序段（指令段）。

2、计算机病毒分类。计算机病毒主要有3类：一是引导型病毒，如“大麻”、“6.4”病毒以及1992年3月间引起全世界广泛关注的“米开朗基罗”病毒；二是文件型病毒，如“1575（毛毛虫）”、“黑色星期五”病毒；三是混合型病毒（具有引导型与文件型双重性），如“1253”病毒等。

3、计算机病毒传播途径。可经由使用者、存贮介质及计算机网络等多种途径传染。计算机病毒的主要来源有：新来的磁盘、电子邮件、外人使用过的机器。

4、计算机病毒触发条件。计算机病毒的触发（激活）是有条件的，如特定的日期、时间、

开关机次数、敲某些键或输入某个 DOS 命令等。

5、计算机病毒组成部分。计算机病毒通常是由 3 部分组成的，它们是：传染部分、激活部分和任务部分。

6、计算机病毒工作的机理。计算机病毒工作的机理是由某个载体先将病毒代码安装（传染）到计算机存储介质，然后潜伏下来一旦满足某些条件，甚至是随机条件病毒被激活并由任务部分产生不良后果或破坏作用。

7、计算机病毒产生原因。计算机病毒的产生原因大致有这么几种：一是恶作剧，大部分是学生干的；二是软件研制者对非法拷贝的痛恨；三是所谓“能人”要自我表现；四是政府、军方对敌人的破坏；五是对现实不满而产生报复行为。

8、计算机病毒破坏作用。计算机病毒破坏作用有良性与恶性之分。良性的一般只干扰屏幕显示，键盘反应变慢，计算机运行速度降低；恶性的使计算机磁盘上保存的文件被改写或删除，磁盘空间等资源被无故占用，甚至于掌握计算机中断等控制权导致整个计算机系统死锁，使硬盘不能启动。

计算机病毒具体的感染部位：感染硬盘分区表、硬盘主引导扇区、软盘引导扇区、覆盖文件、.EXE 文件、.COM 文件（包括 COMMAND. COM 文件）这么几种。

9、计算机病毒防治。防治计算机病毒可分 3 个步骤：防毒、侦毒、解毒。防毒即预防计算机病毒，在计算机病毒传染之前报警，拒病毒于计算机之外。现已有防病毒卡或软件对计算机的磁盘、文件等进行免疫。这种对计算机病毒主动出击，积极预防的方针是防治病毒的主要方向。侦毒是查清计算机是否感染上病毒，若有，应查明属何种病毒以便对症下“药”。解毒是利用诊治计算机病毒软件来清除病毒，或者用其他方法消除病毒以恢复正常。有些计算机病毒采用了加密技术使消毒变的更为困难。消除病毒只是一种补救措施，因为计算机被病毒感染，可能病毒已经产生了破坏作用，这时也许用户还未察觉。

除了用抗病毒软件或防病毒卡进行消除病毒外，用户可以借助 DOS 命令进行消毒工作。首先把染毒的机器电源关闭，用干净的贴有写保护的 DOS 软盘重新冷启动。对于引导型病毒用户可以对磁盘进行格式化来消除，若是硬盘主引导扇区被感染，还要进行低级格式化。对于文件型病毒最简便的消毒方法是用干净的文件覆盖受感染文件。特别需要提醒用户注意的是，无论用何种方法进行清除，工作之前都要把文件、数据备份起来，再好的产品总有失误的时候，否则因操作不当或其它因素造成数据丢失，后果不堪设想。

第二章　CPAV 简介

CPAV 是 Central Point Anti—Virus 的缩写。它是 Central Point 软件公司继著名的 PCTOOLS 软件之后推出的一种检测、清除与免疫计算机病毒的集成软件。CPAV V1.2 能够检测和清除病毒超过 1000 种之多。CPAV V1.0 与 Pctools V7.0 是于 1991 年 5 月一起推出的，1992 年 2 月又推出 CPAV V1.2 版。CPAV 不仅能够对已知的病毒进行处理，而且具有对未知的病毒进行检测的能力。CPAV 完全适用于 Windows 这种窗口软件的环境，使该软件更易于操作。同时它还提供了文件的免疫功能，任何企图在可执行的文件中加入一小段程序都会被报告出来。截止到 1992 年 2 月，CPAV 收集保存的病毒名称清单包括各种各样病毒及变种已达到 1009 种，其中每一种类型的病毒都有较为详细的说明信息。对新出现的病毒还可以自行更新病毒清单。CPAV 能够适用于多种机型，有着非常丰富的联机帮助功能，用户可以不必借助《使用手册》就能运用自如。CPAV 充分吸收了 PCTOOLS 软件的优点如用户界面非常友好，需要选择输入的地方以高亮度字母作显示一目了然。显示的信息若多于一屏时，窗口旁边附有标尺让用户随时可以了解到目前所浏览的信息处于什么位置。

CPAV 不仅从诊治病毒入手，而且从预防病毒这一角度出发，下了较大的功夫。把被动的检查病毒变为主动地对病毒出击，进行免疫与预防。CPAV 所提供联机安全控制机制，能够在任何时候被病毒入侵时自动产生报警，并提醒用户把病毒删除掉。在开机自动处理文件（AUTOEXEC.BAT）中加入 VSAFE.COM，使之常驻内存随时对系统进行监视。VSAFE 还具有探测网络安全能力，设置相应的参数后，每当遇到网络访问时，它都会提供安全检测。CPAV 靠 VSAFE 提供 8 个方面的安全与监视功能，可以任选其中几项或全部。8 个安全监视功能是：

(1) 硬盘低级格式化；
(2) 常驻内存程序；
(3) 全面的写保护；
(4) 检查可执行文件；
(5) 引导扇区病毒；
(6) 保护硬盘引导扇区；
(7) 保护软盘引导扇区；
(8) 保护可执行文件。

CPAV 中的 BOOTSAFE 命令文件在开机时运行之，会检测内存、分区表、主引导扇区等信息的完整性，一旦发现病毒就会立即告。在 INSTALL 安装实用程序中，除了正常的安装过程、参数配置及显示方式的选择等功能外，它还特别提供了应急软盘的制作。应急软盘的制作是把硬盘的分区表、主引导扇区以及 CMOS 参数等信息备份到软盘上，一旦硬盘受到严重损坏

(包括病毒以外其它原因的损坏)时用应急软盘来恢复硬盘的内容。特别是CPAV对毒性极大的DIR II病毒能够有效地抑制、清除。甚至可以消除交叉感染的病毒,如一个文件同时被DIR Ⅱ与1591病毒感染。CPAV V1.2还有其它众多的功能,将在以后各章介绍。

CPAV作为一个纯软件产品不像硬件防病毒卡那样需要占用主机的一个扩展槽,而且今后更新升级非常方便。作者对国内流行的数十种病毒用CPAV进行了检测都能很好地报警。CPAV毕竟是舶来品,对国内的有些新病毒还缺乏行之有效的清除方法,如XqR/NewCentury(新世纪病毒),但是CPAV不失为是一个对病毒进行检测、清除与免疫的优秀集成软件。若将CPAV与公安部推广的最新检测病毒软件SCAN V3.1(检测超过500种病毒)、KILL V46.01(杀46种病毒)配合使用,效果就会更好。

CPAV是由20多个文件组成的抗病毒软件,装在一张1.2MB 13.44cm(5.25英寸)软盘上发行。在PC机及其兼容机上均可运行,运行时大致需占用450KB内存。至少要在DOS 3.0以上版本使用CPAV。在原软件提供的病毒清单中有些错误,如病毒总数按统计只有988种(可能是原软件输入时出错)。本书对软件中说明有错误的地方都进行了订正。CPAV由下列程序组成:

INSTALL	EXE	189248	—— 安装文件
AVINST	HLP	81257	—— 安装帮助文件
CPSMAIN	FNT	16385	—— PC Tools V7.X 的源文件
CPSHELP	OVL	29828	—— 帮助覆盖文件
CPAV	EXE	181286	—— 主文件,可单独执行
CPAV	HLP	58075	—— CPAV 帮助文件
CPAV	ICO	766	—— CPAV.EXE 调用
CPAV	GRP	2531	—— CPAV.EXE 调用,有关 WINDOWS 鼠标控制
CPAV	PIF	545	—— CPAV.EXE 调用,有关 VSafe、VWatch 和 WNTSRMAN.EXE 使用
BOOTSAFE	EXE	26513	—— 引导扇区、分配表及 CMOS 安全机制
VSAFE	COM	30334	—— 监测运行环境;保护文件、磁盘、内存的可执行程序
VWATCH	COM	27792	—— 监测运行环境的可执行程序
VSAFE	SYS	57728	—— 监测运行环境,保护文件、磁盘、内存的驱动模块
VWATCH	SYS	29728	—— 监测运行环境的驱动模块
ISCPSTSR	EXE	3486	—— 网络支撑模块,检测 VSAFE 是否常驻内存
WNTSRMAN	EXE	15440	—— Windows TSR 支撑模块
WNTSR	DLL	21712	—— Windows TSR
WNGRAPHC	DLL	25952	—— Windows GRAPHIC
EXCEPT	CPS	408	—— 指定免疫例外文件清单
VIRULIST	CPS	28416	—— 病毒清单,供 CPAV 调用
VIRLIST	DOC	2192	—— 有关新增加病毒清单的说明
README	EXE	59182	—— 阅读实用程序
README	TXT	31221	—— CPAV V1.2 新特色供 README.EXE 调用

以下是 CPAV 安装后生成或者可以更改的文件与目录：

ACTIVITY	CPS	4900	—— 各种活动报告文件
CPAV	INI	602	—— CPAV 与 INSTALL 选择项设置开关
CPAV	TXT	39	—— 由用户自己编辑用于 CPAV 带/N 时调用，屏蔽原来显示界面
CPAV	RPT	311	—— 报告文件
CHKLIST	CPS	54	—— 记录磁盘可执行文件的属性、大小、时间、日期
CPSCOLOR	DAT	5492	—— 键盘、鼠标速度、每屏行数和色彩等数据
REPORTS	<DIR>		—— 存放检测到病毒感染的报告

第三章 CPAV使用

使用CPAV既可以全功能菜单或图示菜单形式来执行，也可以用命令行形式运行。在使用前要说明一下，Tab键与控制光标键经常用于各窗口或各输入选择项间移动时使用。在程序中所有单词以高亮度显示的字母都表示要选择该项时可按该字母确认执行。用户对某个命令或选择项不理解，只要移动光标到不理解的地方并按一下F1键，都能得到相应的帮助。按回车键是确认所选择的项目。

一、命令行形式

命令行形式允许用户把CPAV.EXE命令加到AUTOEXEC.BAT文件，在启动过程中执行检测病毒的任务。

格式：CPAV [[Drive:] [Drive:] [Drive:] [PATHNAME] /options]
CPAV [[驱动器] [驱动器] [驱动器] [路径名] /选择项]

有效的选择项：

/S — Scan disk and files for viruses (On by default).
扫描磁盘和文件病毒（缺省的）

/C — Scan & Clean disk and files for viruses.
扫描并清除磁盘和文件病毒

/I — Scan, Clean & Immunize disk and files.
扫描、清除与免疫磁盘和文件

/R — Switch the Report option ON.
置“报告选择”开

/A — Scan all drives except A and B.
扫描除A：和B：以外的所有驱动器

/E — Express Menu
以图示菜单显示

/L — Scan all local drives except A and B.
扫描除A：和B：以外的所有本地驱动器

/N — Suppress interface information. Display text in CPAV.TXT file, if any
屏蔽显示界面信息。若存在CPAV.TXT文件以其内容显示出来，否则显示

Working...

/P — Display command—line interface in place of graphic interface.
以命令行界面代替图形界面显示

/F — Suppress names of files scanned. Valid only with /N or /P.
屏蔽所扫描的文件名，仅在使用/N 或/P 时有效

/VIDEO — Display the video command line options
显示视频命令行选择项，即会提示屏幕参数与鼠标参数

/? — Display this help.
显示这个帮助信息

屏幕参数：

/25 — Set screen display to 25 lines (default)
设置屏幕为 25 行显示（缺省值）

/28* — Set screen display to 28 lines (VGA only)
设置屏幕为 28 行显示（仅供 VGA 使用）

/43 — Set screen display to 43 lines (VGA & EGA)
设置屏幕为 43 行显示（供 VGA 和 EGA 使用）

/50 — Set screen display to 50 lines (VGA only)
设置屏幕为 50 行显示（仅供 VGA 使用）

/60 — Set screen display to 60 lines (Video 7 only)
设置屏幕为 60 行显示（仅供视频方式 7 使用）

/IN — Run program in color even if color monitor is not detected
即使彩色监视器没有检测到也以彩色方式运行程序

/BW — Use black and white color scheme (black and white monitor)
使用黑白图像（黑白监视器）

/MONO — Use monochrome color scheme (IBM monochrome)
使用单色图像（IBM 单色监视器）

/LCD — Use LCD color scheme (LCD only, usually laptop)
使用液晶图像（仅在使用 LCD 显示）

/FF — Speed up display — causes snow on some monitors (CGA only)
加速显示，有些监视器会出现雪花点（仅供 CGA 使用）

/BF — BIOS font (use if graphics don't display properly)
使用 BIOS 字符（如果图形不能很好地显示时使用之）

/NF — No fonts — don't use graphics characters
不使用图形符（若图形字符不能使用）

/BT — Allow graphics mouse in Windows, allow graphics fonts with Desqview or UltraVision
在 Windows 中允许使用图形鼠标，允许用超级版本的图形字符

鼠标参数：

/NGM — No graphics mouse — use default mouse character instead
不用图形鼠标——用缺省的鼠标字符代替

/LE — Left—handed mouse — exchange left and right mouse buttons
左手鼠标 —左右鼠标按钮对调

/IM — Disable mouse in PC Tools programs
禁止在 PCTools 程序中使用鼠标

/PS2 — Reset mouse hardware (use if mouse disappears or freezes)
复位鼠标（如果鼠标不出现或死机）

某几个参数可同时组合使用。屏幕与鼠标参数实际上也相当于选择项，跟随在 CPAV 命令后面使用。例如：

C>CPAV /50　　设置屏幕为 50 行显示

二、菜单形式

如果运行 CPAV 时不带选择项与参数，就会以菜单形式出现。

1、全功能菜单

C>CPAV

Central Point Anti—Virus		2.31p
Scan Option Configure Help		
C: \		
File Information Selected Dirs: 17 Selected Files: 15	Virus Information Last Virus Found:	Last Action: Action: Date: 10/12/92
Directory Tree	Files in Current Directory	
C: \ —BAS —CPAV REPORTS —DEMO —PM	AUTOEXEC. BAT　PKZIP. EXE CHKLIST. CPS　ZIP2EXE. EXE COMMAND. COM CONFIG. SYS DEC. BAT IO. SYS MSDOS. SYS PC. EXE PKUNZIP. EXE	

F 1 Help F 2 Drive F 3 Exit F 4 Detect F 5 Clean F 6 Immune F 7 Log F 8 Express F 9 List F 1 0 Menu

图 3—1

全功能菜单屏幕显示 6 部分信息分别在下面介绍。

(1) 软件全称与目前机器内部时间；
(2) 一级命令菜单区；
(3) 驱动器以及选择驱动器（A，B，C，D.....）与扫描时显示当前目录文件；
(4) 信息区（被选择的文件与目录数量、病毒信息、最后一次活动与时间）；
(5) 目录树区与目录下的文件区；
(6) 功能键：

F1	Help	帮助（所有的 CPAV 使用与安装帮助信息都可以通过 F1 显示出来）
F2	Drive	选择新驱动器
F3	Exit	退出 CPAV
F4	Detect	检测文件、内存中的病毒与文件的变更
F5	Clean	检测并清除文件、内存的病毒与文件的变更
F6	Immune	对文件进行免疫
F7	Log	显示活动报告
F8	Express	将全功能菜单转换成图示菜单
F9	List	显示病毒清单
F10	Menu	将光标移到一级命令菜单区

2、图示菜单

C>CPAV /E

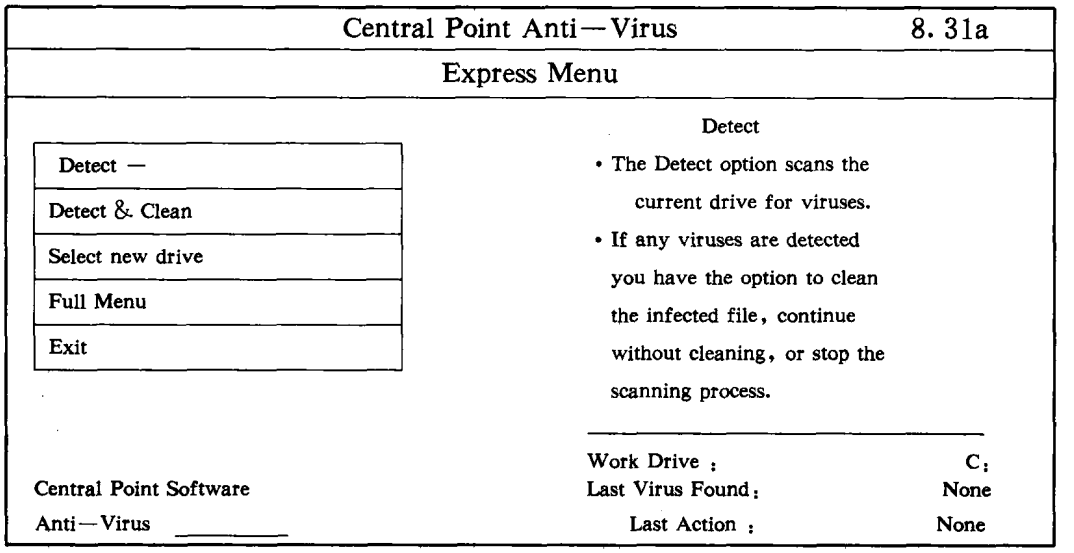


图 3—2

图示菜单屏幕显示 5 个部分信息分别在下面介绍。
(1) 软件全称与目前机器内部时间；
(2) 图示菜单；
(3) 图示命令区和命令解释；

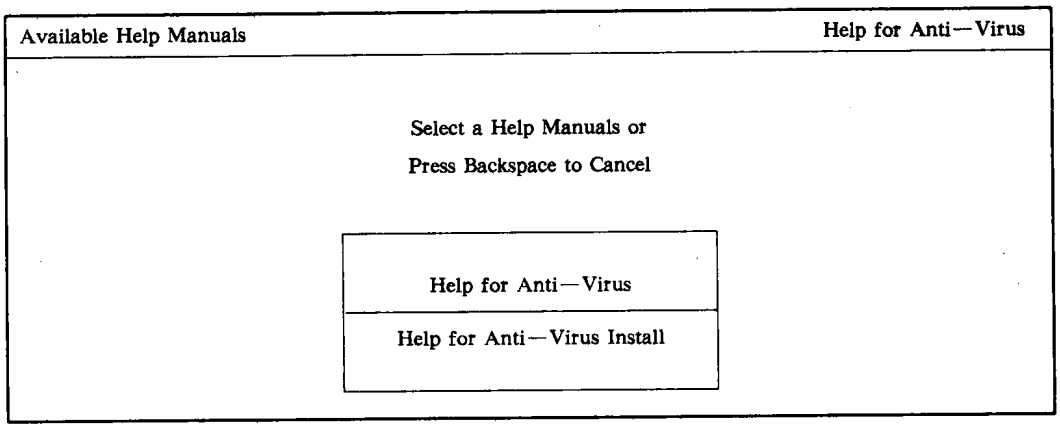
(4) 工作驱动器、最后一次发现病毒名称和最后一次活动信息区；

(5) 功能键：

F1	Help	帮助
F2	Drive	选择新驱动器
F3	Exit	退出 CPAV
F4	Detect	检测文件、内存中的病毒与文件的变更
F5	Clean	检测并清除文件、内存中的病毒与文件的变更
F6		未定义
F7	Log	显示活动报告
F8	Menus	将图示菜单转换成全功能菜单
F9	List	显示病毒清单
F10		未定义

三、帮助信息

在任何地方只要按下 F1 都能得到帮助。如果进入 CPAV 后想得到各种帮助信息，按 F1 键然后再按 F9（Manuals）键，屏幕显示：



F1Help F2Index F3Exit F4Topics F5GoBack F6Print F7Prev F8Next F9Manuals F10

图 3—3

若选择“Help for Anti—Virus”可按 F8（Next）键一直阅读直到最后响铃结束。同样也可按空格键再按回车键选择" Help for Anti—Virus Install"（CPAV 安装信息）。

F1	Help	显示帮助
F2	Index	显示帮助系统的索引
F3	Exit	退出帮助返回到 CPAV 或 INSTALL
F4	Topics	显示帮助系统的标题
F5	GoBack	回到最早的显示窗口
F6	Print	打印当前帮助窗口信息
F7	Prev	显示前一个窗口信息
F8	Next	显示下一个窗口信息

F9　Manuals 显示 CPAV 与安装帮助供选择

F10　未定义

四、退出 CPAV

若你什么都不想干，请按 F3 或按 ESC 键退出，退出之前会显示：

Central Point Anti－Virus
This will close Central Point Anti－Virus [] (S) ave Configuration (O) K　(C) ancel

图 3－4

直接按回车键或按 O 键退出 CPAV 返回到 DOS 状态。

在使用 CPAV 菜单或安装菜单的任何命令状态，只要按下 Alt＋空格键会出现

Version
Close Alt＋F4

选择 Version 看版本信息

选择 Close 关闭 CPAV 或 INSTALL

在使用 CPAV 菜单或安装菜单的任何命令状态，只要按下 Alt＋F4 键会出现(图 3－4)，用于快速退出。

第一节　扫描菜单

进入 CPAV 全功能菜单后，按 S 键出现扫描菜单窗口：

(D) etect (C) lean (I) mmunize (R) emove Immunization
Delete Checklist (F) iles (V) irus List (U) pdate Virus List
(A) ctivity Log Re (p) ort
E (x) it

检测 清除 免疫 去除免疫
删除检验列表文件 病毒清单 更新病毒清单
活动报告 报告
退出

注：( ) 是作者加上的表示高亮度显示，下同　　中文对照

图 3－5