Windows 9x / NT (Workstation) / 2000 (Professional)

版本 4.02 SP2

使用说明书

2000年4月17日 第二版发行

开发：安哲洙计算机病毒研究所

技术支持/售后服务 •病毒检举/咨询

邮编： 135-745
地址： 汉城市江南区三星洞144-17三和大厦十层 安哲洙计算机病毒研究所
网址： http://www.ahnlab.com
电话： 82-2-2186-6000 （总机）
82-2-558-7400 （售后服务中心）
82-2-558-7566 （病毒检举中心）
传真： 82-2-2186-6100 （总机）
82-2-558-7567 （售后服务中心专用）

前言

此说明书为购买V3Pro 2000 Deluxe的用户而编。希望您从头到尾读一遍。通过本说明书，您可以熟悉V3Pro 2000 Deluxe的使用方法，同时还可以提高对计算机病毒的应付能力。

说明书构成

此说明书由五个章节构成。第一章介绍售后服务服务及使用程序应预先了解的内容。第二章包括V3Pro 2000 Deluxe的特征和设置方法，第三章介绍简单使用方法，第四章说明熟练使用方法，第五章介绍有用的工具集及网络连接。

使用说明书里的标记及使用说明书的规则

本说明书以尽可能使用中文为原则。但是必要时在括号内使用了英文字母，同时，如果没有可代替的专业用语，则以直接使用英语原词为原则。

本说明书把“安哲洙计算机病毒研究所”简称为“安哲洙研究所”或“研究所”，“计算机病毒”简称为“病毒”，“NT Workstation”简称为“NT(Workstation)”或“NT”。“2000 Professional”简称为“NT(Professional)”或“2000”。

使用说明书的规则

Symbol or Mark	Description
NT/2000	有关NT(Workstation)/2000(Professional)的内容
参考	表示说明或提示，例外事项，快捷执行方法等。
注意	表示对意外情况或对有可能引起重大损失的情况的警告事项。
英语大写字母	表示子目录，路径，文件名等。
粗体字	表示菜单，对话框，选项等。
<Key1>→<Key2>	按<键1>，然后按<键2>。
<Key1> + <Key2>	同时按<键1><键2>。
粗体字1→粗体字2	点击**粗体字1**以后，再点击**粗体字2**。

目录

第一章

开始之前

- *用户登记及售后服务*
- *使用咨询及技术支持*
- *发现新种病毒时*
- *使用V3Pro 2000 Deluxe时的注意事项*

用户登记及售后服务

安哲洙研究所为登记用户提供关于V3系列产品的技术支持、售后服务及病毒咨询等多种服务。

必须进行用户登记

购买V3Pro 2000 Deluxe的用户必须进行用户登记。安哲洙研究所的V3系列产品有别于其它程序，因为新病毒将不断地被发现，所以持续升级将是必需的。因此每周将进行一次升级，并为登记用户提供特别服务。但是，如果无法确认是否进行了用户登记，即使是购买了本产品的正版用户也无法享受售后服务。**因此希望购买以后务必进行用户登记。**

通过网络可以方便地进行在线用户登记

如果使用包含在产品包装的用户登记卡进行登记将会需要一定时间，在此时间内无法得到提供给登记用户的服务。因此利用网络，通过网页进行在线登记，将会缩短登记时间。

利用安哲洙研究所网页（www.ahnlab.com）上的用户专用论坛 - 在线用户登记菜单就可以直接进行登记。但是，如果是无法使用网络的用户则必需在用户登记卡（与产品一起包装）上正确填写姓名、邮编、地址、电话号码及当前使用的四大BBS的ID等用户信息之后，用邮寄或传真（82-2-558-7567）方式传送到本研究所。

售后服务期限为一年（从登记开始计算）

V3系列产品的售后服务期限为一年。在登记并经过一年以后将停止包括每周定期最新引擎升级服务在内的提供给登记用户的所有服务。

对于登记用户将提供多种服务

对于登记用户，在有效期限内将提供以下各种服务。

- 每周定期的最新升级服务
- 利用电子邮件/网络/通讯/邮寄/电话的咨询服务
- 在有效期限内进行升级时，对同一系列产品提供无偿升级服务
- 提供Web 引擎“安哲洙计算机病毒新闻”
- 提供年一回病毒日历®
- 利用电子邮件提供各种新闻
- 可免费参加反病毒研讨会及教育课程

如果用户登记期限到期，请务必进行登记更新。

因杀毒软件的特点，迅速的升级是非常必要的。为此，V3系列产品提供每周一次的迅速升级，此外还要耗资进行持续的研究与开发。因此与别的程序不

同，我产品具有一年的登记有效期限。

在登记过一年以后将中断售后服务，因此系统被新种病毒感染的危险性将会增大。为此，希望登记期限已过的用户务必进行登记更新，以安全保护计算机系统。

所谓登记更新是提供给已购买V3系列产品并已进行登记的用户的一项服务。如果登记用户欲延长一年得到引擎升级服务，则按此项“登记用户优惠制度”，将得到比一般用户低50%的削价优惠。

如欲得到更详细的与登记更新有关的信息，可参考安哲洙研究所网页上的售后服务菜单。

V3Pro 2000 Deluxe 引擎升级方法

对于V3Pro 2000 Deluxe登记用户，我们将用电子邮件或用户提供的地址寄送可以每周(星期三前后)通过用户专用论坛下载最新引擎升级文件的权力。

对于登记用户将用电子邮件每周定期传送升级通知。收到升级通知以后，可利用网络的用户可通过安哲洙研究所网页上的用户专用论坛。利用网络的用户可利用包含在V3Pro 2000 Deluxe软件里的升级魔法师功能直接安装下载升级文件（升级魔法师为利用互联网的自动升级功能。详细内容请参照第五章第一节）

> **参考**：只拥有四大BBS ID的用户申请进行用户登记时，在从安哲洙研究所收到用户登记确认电子邮件的第二天中午12点开始才可利用“用户专用论坛”。

使用咨询及技术支持

使用V3Pro 2000 Deluxe时，如有疑难事项，请先参考本说明书。对于其它的疑难事项，请利用以下电子邮件、网络主页、四大BBS 专用论坛、电话、传真及一般邮件等进行问询。

互联网

安哲洙研究所主页： www.ahnlab.com

售后服务负责人电子邮件 ID

互联网： customer@ahnlab.co.kr

邮寄及电话、传真

135-745
汉城市江南区三星洞144-17三和大厦十层
安哲洙计算机病毒研究所售后服务负责人 （收）

电话：82-2-558-7400（售后服务中心）
传真：82-2-558-7567

用户登记

1 请务必进行用户登记

可用（1）或（2）的方法进行用户登记。

(1) 在线用户登记

连接http:\\www.ahnlab.com，选择“在线用户登记”

(2) 用户登记卡

填写产品包装里的用户登记卡，用传真（82-2-558-7567）或邮件寄送。

参考：不接受用BBS进行的用户登记。

2 必须进行用户登记的重要理由

因为不断有新种病毒被发现

反病毒软件必须在最短周期内进行更新。只有进行用户登记了的用户才能使用V3Pro 2000 Deluxe的引擎升级文件，因此必须进行用户登记才能进行反病毒软件升级。只有最新版才能继续对新种病毒进行查/杀。

3 请务必进行升级

只有进行用户登记了的用户才能下载引擎升级文件

请在（1）、（2）、（3）中选择最方便的方法。

(1) 通过研究所主面下载升级文件

(a) 连接http:\\www.ahnlab.com，选择用户专用论坛的会员菜单。

(b) 输入User Name及Password。

(c) 选择综合引擎下载文件。

(d) 在资源管理器上双击要下载的文件。

(e) 执行V3Pro 2000 Deluxe确认引擎日期是否更新为最新日期。

(2) 利用升级魔法师®功能

(a) 执行V3Pro 2000 Deluxe。

(b) 执行升级魔法师®功能，按开始升级按钮。

(c) 退出V3Pro 2000 Deluxe后重新执行，则升级结束。

参考：升级魔法师®必须在连接互联网时方才有效。

发现新种病毒时

如怀疑发现新种病毒，请与安哲洙研究所联系。

被新种计算机病毒感染或疑心被感染时，或者在利用非V3系列产品杀毒软件发现病毒时，请与安哲洙研究所的病毒检举中心或与售后服务中心联系，并传送相关数据。我们将对被传送的文件，进行迅速分析确认是否被感染。如被感染，我们将以最快的治疗升级支持使受害程度减小到最低。

采集文件病毒（包括宏病毒）和引导型病毒的方法如下。（请参考附录“关于Windows用V3+ Neo”）

文件（宏）病毒采集方法：文件（宏）病毒感染执行文件，因此请把疑心被感染了的文件（宏病毒时为相关Office文件）传送给我们。

采集引导型病毒的方法：如果利用V3Pro 2000 Deluxe提供的引导区备份功能，或使用包含在Windows用V3+ Neo里的引导型病毒采集工具V3BACKUP.EXE（使用例：“C:\V3BACKUP 相关子目录名”），就可以方便地采集引导型病毒。但是使用Windows用程序V3BACKUP.EXE时，必须用干净的DOS盘启动以后才可执行。请把执行后生成的MBS.V3和DBS.V3文件（使用软盘时，生成FBS.V3文件）传送给检举中心负责人。

互联网

安哲洙研究所主页：www.ahnlab.com

病毒检举中心负责人电子邮件 ID

互联网：customer@ahnlab.co.kr

邮寄及电话、传真

135-745
汉城市江南区三星洞144-17三和大厦十层
安哲洙计算机病毒研究所售后服务负责人 （收）
电话：82-2-558-7566（病毒检举/咨询）
传真：82-2-558-7567

使用 V3Pro 2000 Deluxe 时的注意事项

无法检测出没有信息的新种病毒

V3Pro 2000 Deluxe可以查/杀到目前为止在国内所发现的所有计算机病毒和在国内没有发现但具有强大破坏力的外国病毒。但对于新种病毒，因V3Pro 2000 Deluxe没有其有关信息，所以无法检测出来（其它杀毒软件也一样）。对于由此而引起的病毒感染和受害情形，安哲洙研究所将不负任何责任。因此为了防止被病毒感染，不能只依靠杀毒软件，还要并行其它预防方法，如事前把重要文件备份（复制）好后另行保管等。

存在不可治疗文件

用V3Pro 2000 Deluxe治疗被计算机病毒感染的文件时，大部分可恢复到被感染以前的状态。但对于新种变种病毒、重叠病毒、重复感染或被感染的宏文件正在执行中时是无法进行正常治疗的。即一个文件被几个病毒同时感染时致使文件损伤时，或文件被在感染同时进行破坏的重叠病毒感染时，或被感染的宏文件正在执行中时是无法进行治疗的。因此在杀毒以前，请把被病毒感染的文件备份或终止执行以后再进行治疗。

一定要接受每周提供的升级服务

在到目前为止已上市的国内外杀毒软件当中，安哲洙研究所提供的V3系列产品具有最快的升级周期（一周）。考虑到一周内也可出现新的病毒，为迅速应付病毒并使受害程度减小到最低，每周升级是有必要的。登记用户只有接受安哲洙研究所每周提供的升级服务，才能迅速应付新种病毒。

此外，如出现恶性病毒，安哲洙研究所将随时提供紧急升级服务，由此在紧急状况下也可进行迅速对付。

参考： 反病毒软件必须在安装后及时升级为最新版本，才可从新种病毒的威胁下保护自己的计算机系统安全。

参考： 如出现恶性新种病毒，安哲洙研究所将在发现24小时内随时提供紧急升级服务。

第二章

V3Pro 2000 Deluxe 的特征及安装

- *特征*
- *执行环境及组成*
- *安装*
- *删除*

特征

V3Pro 2000 Deluxe是安哲洙研究所开发出的Windows 9x / NT (Workstation) / 2000 (Professional)用计算机杀毒软件（Anti-Virus Program）。在国内外众多杀毒软件中，V3Pro 2000 Deluxe不仅提供最快最强大的查/杀毒功能，而且还可以监视、检测并治疗在网络上收到的各种数据及文件。V3Pro 2000 Deluxe内藏有国际先进的WARP 引擎，因此误诊的可能性极少，并具有出色的文件恢复功能。

V3Pro 2000 Deluxe的特性如下。

彻底防止从网络游入的病毒

网络监视功能与系统监视功能相结合，监视从网络输入的数据是否被病毒感染。如发现病毒，提供完整的检测、治疗功能。

内藏病毒监视、自动解毒功能

采用智能病毒监视（预防）系统。在执行中，如发现病毒，将自动防止病毒流入整个系统，并及时治疗被感染文件。系统监视功能不仅在防毒方面具有卓越功能，而且对系统速度几乎没有影响。这是V3Pro 2000 Deluxe的重要功能。

内藏强有力的 WARP 引擎®

采用了安哲洙研究所独自开发的优秀的WARP 引擎®，不仅对Windows 9x / NT (Workstation) / 2000 (Professional)系统，而且对DOS的内存领域也可进行彻底检查，因此可以安全使用系统。此外。它还提供国内外杀毒软件中最快的检查速度，最完美的解毒率和文件恢复功能。

安哲洙研究所以自己固有的技术力量独立开发的WARP 引擎®把病毒检测、治疗和预防技术合为己身的杀毒程序里的核心部分。它有以下优点。

- **及时应付病毒的抗病毒功能** - 对于到目前为止被发现的国产病毒，它具有100%的检测、治疗功能。此外对国外各种病毒，包括最近流入的恶性病毒（如CIH及梅丽沙、Explorer Zip、Back Orifice等），它都提供完美的查/杀功能。
- **出色的文件修复能力** - 治疗被感染文件时，它具有出色的文件修复能力。因此可以使文件受害程度减小到最低。
- **最快的查/杀速度** - 以安哲洙研究所所固有的治疗方法（特征位置检查技术：只捡具有被感染可能性的领域进行检查的跟踪方法）设计，它在目前上市的杀毒产品中具有最快的查/杀速度。
- **对国内尚未发现病毒的检测功能** - 对于在国内尚未发现的一万多种外国产病毒，它也具有检测功能。由此对新种病毒的流入也作好了完备的准备。

获得国内专利及KT Mark的，已充分显示其优秀性的 WARP引擎®名称的由来及含义

WARP 引擎®的“WARP”是从电影“STAR TREK”而来，是搭载在主人公们的联邦宇宙飞船上的超光速推进引擎的名称。根据电影，所谓WARP驱动系统具有可以超光速旅行和空间移动的能量，是被从Alpha Centauri（离太阳系最近的行星）过来的叫Zefram Cochrane的科学家发明的。从“提供世界上最快最正确的治疗（修复）率”的意义上出发，搭载在安哲洙研究所V3系列产品上的反病毒引擎被命名为“WARP：World-class Accelerated Recovery Processor”。安哲洙研究所不断强化WARP 引擎®的如上特性，给广大用户提供有别于其它治疗工具的、以独立技术为基础的治疗方案。

以迅速升级应付新种病毒

包括V3Pro 2000 Deluxe在内，安哲洙研究所的V3系列产品在国内外治疗工具当中具有最快的升级周期（每周一回）。此外，为解除用户手动升级时的不便，在程序内部藏有自动升级系统即升级魔法师®服务。执行升级魔法师®，就可以通过安哲洙研究所主页上的升级服务器自动下载引擎升级文件。

发现病毒时的多种安全可靠的治疗方法

如发现被感染，会及时提供自动治疗以及伴随治疗的安全的应对方法。即根据用户设置的不同选项，为应对可能发生的文件损坏，在进行杀毒之前把文件保存到备份文件夹里。如果是不可解毒文件，将会自动删除以免病毒扩散，并删除以前把文件保存到备份文件夹里。

此外，它还可以在读写软盘或关闭Windows时，检测系统是否被引导型病毒感染，并因此可以彻底预防引导型病毒的流入。

提高防毒及管理效率的多种附加功能

它不仅内藏有包括高可信度病毒分析、基于研究成果的病毒相关信息的病毒信息数据库，而且还内藏有病毒日历，因此对于在年中特定日活动的病毒也具有预防功能。

此外它还提供很多其它功能。如为了用户能够应付病毒感染而提供的检查记录信息，为方便用户而提供的多种环境设置选项，各种有用的工具菜单，在网络上的在线用户登记等。所有这些功能使系统在不同情况下具有不同的防毒及管理能力。

使用NT 工作站及Windows2000时的注意事项！

1. 使用说明书中与引导区有关部分与NT工作站及Windows2000无关。
2. 使用说明书中与SOS软盘制作有关部分与NT工作站及Windows2000无关。
3. 使用说明书中的升级魔法师功能只对NT工作站及Windows2000（专业版）用户中具有管理员权限的使用者有效，且只有在login状态时才能使用。

执行环境及组成

执行环境

V3Pro 2000 Deluxe是Windows 9x / NT (Workstation) / 2000 (Professional)用杀毒软件。为执行V3Pro 2000 Deluxe最低需要如下使用环境。

- Intel Pentium 133MHz以上IBM-PC兼容机
- 64MB以上内存
- VGA以上的图像卡及监视器
- 10MB以上的硬盘剩余空间
- Windows 9x / NT (Workstation) / 2000 (Professional)
- CD-ROM驱动器（24倍速以上推荐）
- 鼠标器

软件的组成

组成软件的文件夹功能如下。

文件夹名	说明
UPDATE	升级文件
BACKUP	用来备份被感染文件的文件夹
TEMP	V3Net临时使用的文件夹
TXT	用来保存从研究所传送过来的信息
SYSTEM	治疗工具所使用的系统文件
LOGWIN	用来储存检查记录的文件夹

产品组成

V3Pro 2000 Deluxe包装盒里有CD-ROM一张，使用说明书，用户登记卡及使用权证书。CD-ROM里存有Windows 9x / NT (Workstation) / 2000 (Professional)用杀毒软件，即V3Pro 2000 Deluxe和DOS版V3+ Neo。DOS用V3+ Neo是为了重新安装操作系统，或在无法正常启动时进行安全的病毒检查而预备的。

与V3Pro 98和V3Web相比较有所改善的功能

1、更快速的检查速度

有效改善其检查过程，提高了检查速度。

2、通过与V3Web合并，安定了网络监视功能

把V3Pro 98和V3Web完全融合起来，不仅提高了系统监视功能，而且对从网络上游入的病毒也可进行彻底的监视。

3、强化升级魔法师®功能

拥有多个升级服务器，因此能够更加快速的接受升级服务。

4、读写软盘时，为封锁引导型病毒源进行自动检查

如果插上被引导型病毒感染的软盘，关闭系统后重新启动时，系统会首先驱动软盘。在此过程当中，引导型病毒将会感染硬盘驱动器。此后，即时拿出软盘也无法解除已流入硬盘驱动器里的引导型病毒引起的损害。为了完全封锁此种病毒的流入，不仅在驱动软盘时增加了检查功能，而且在关闭Windows时，如果发现软盘还插在软驱上，将会自动进行病毒检查，因此使系统能够维持安全的防病毒环境。

5、采用“快捷检查条”，追求检查方法的多样性

可使用户直接输入检查对象进行检查。使系统拥有更具弹性的防御管理功能。

6、对于系统正在使用中的文件也可进行治疗

对于Windows系统正在使用的文件也可进行治疗。V3Pro 2000 Deluxe可强制中断被感染文件的执行并进行治疗。被强制中断的文件无法自动重新执行。如果无法中断，就把执行文件另外复制一份后对其进行治疗，然后在重新启动时，就用被治疗的文件代替原文件。因此，对于正在执行的文件，也可进行安全的治疗。

7、强化备份管理及自动传送功能

把被感染的文件储存到另一备份文件夹里，以防万一。如果是新种病毒，就直接传送到研究所的病毒检举中心，并提供快速的治疗工具升级支持。

8、可追踪杀毒工具的所有活动

事件记录及信息记录本上记录着系统/网络监视、升级执行与否、病毒检查执行与否、从研究所传送到的信息等各项情报，因此可以追踪杀毒工具的所有活动，以便更加安全地管理系统。

9、追加Neo扫描功能

此功能可强制关闭正在执行中的Windows系统，并在用DOS启动后，在执行Windows以前用V3+ Neo检查所有硬盘。特别是对于Windows系统正在使用的文件，用此功能可保证可靠防御管理。

10、追加Web连接及Office Protector功能

追加了能够直接连接安哲洙研究所网页的Web连接功能和对MS Office及 MS网络Explorer 5.0的插件功能.

11. 增加对互联网端口的检查功能

使用互联网时可对互联网端口进行检索，以检查BackDoor软件是否正在执行中，如发现疑为病毒使用中的端口，将显示警告信息。

12. 增加了寄存器治疗引擎

为了对与PrettyPark一样对寄存器等Windows系统部分进行任意改动的病毒进行查杀，可在不执行其它批处理文件的情况下只以V3引擎进行治疗。

13. 增加了对正在使用中的软件的检查功能

为对应象BackDoor一样在软件执行中进行活动的病毒的增长，在进行文件检查之前将首先对正在执行中的程序进行检查。

14. 完美支持Windows2000

强化了系统监视功能，更完美支持Windows2000系统软件。

安装

按Windows 9x / NT (Workstation) / 2000 (Professional)的任务栏上的开始按钮，选择运行。在打开栏上填写CD-ROM驱动器的名称和安装程序名。（一般来讲V3Pro 2000 Deluxe在安装时将会执行自动安装功能。如果您不希望其自动执行，可在按<Shift>键的同时插入CD-ROM即可。）

输入‘D:\setup.exe’，按确认按钮，则V3Pro 2000 Deluxe的安装程序就会执行，并循序显示其安装过程。

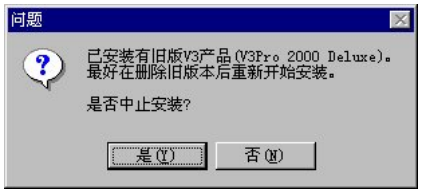
V3Pro 2000 Deluxe 安装过程

1. 显示确认 V3Pro 2000 Deluxe版权的对话窗口。如同意本使用许可协议内容并希望继续安装，请按是(Y)。

2. 安装V3Pro 2000 Deluxe以前会询问是否要检查计算机系统有无病毒。有三种选择：检查所有文件夹，检查系统文件夹，或不检查。若要检查系统有无病毒，请选择相应选择项后按是（Y），则将执行V3Pro 2000 Deluxe里的V3+ Neo。检查结束后关闭DOS窗口，就会回到Windows窗口并继续进行安装。（NT没有以上信息。）

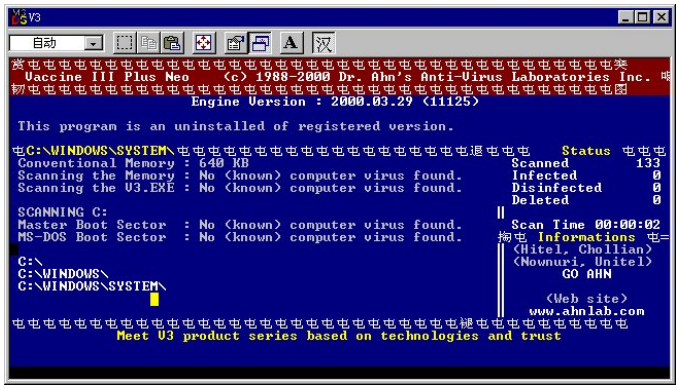
系统存有以前版本或其它杀毒工具时

为了安装V3Pro 2000 Deluxe，需要删除已有的V3系列产品。如存有以前版本，将会显示询问是否要删除的画面。（对于其它杀毒工具也用相同方法检查设置与否）



选择是，删除以以前版本后重新安装。

参考：只有删除已有的其它杀毒软件，才能安全安装V3Pro 2000 Deluxe。



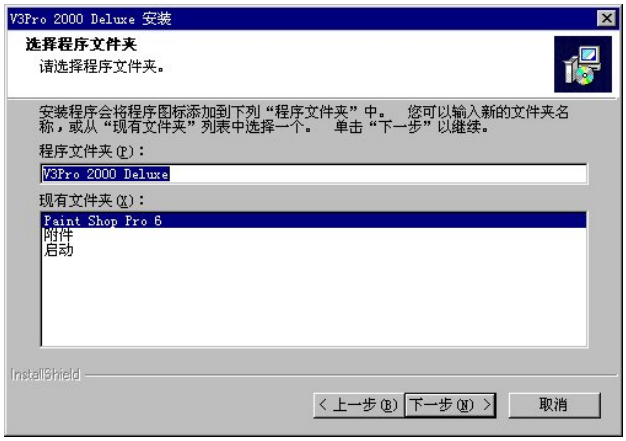
3. 显示确认V3Pro 2000 Deluxe版权的对话窗口。同时显示安装程序以前关闭所有Windows程序的提示。按下一步(N)就会继续执行。如有其它Windows程序正在执行，请先关闭此程序关闭后再重新开始安装。

4. 输入用户信息。输入用户姓名或所属单位名称，公司，序列号（产品号）。序列号就是用户登记卡上的产品号码。

5. 选择用来安装V3Pro 2000 Deluxe的文件夹。默认值为‘C:\Program Files\V3’。若要安装到其它文件夹，可按浏览（R）按钮选择其它文件夹。若选择默认值，就跳到第六步继续安装。

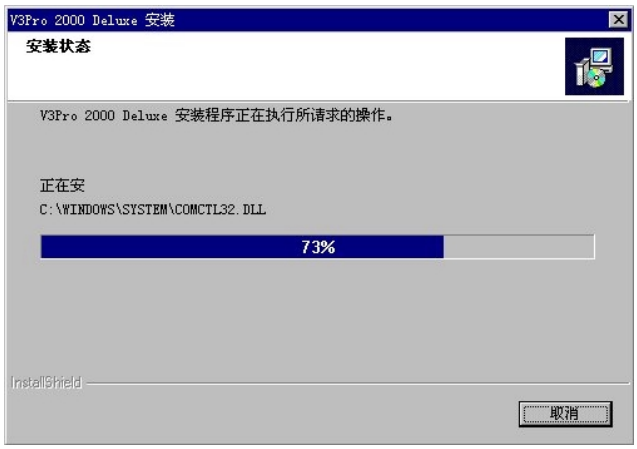
6. 在第四步，按浏览（R）按钮，就可另行选择所要的文件夹。

7. 选择了目标文件夹以后，需要选择程序文件夹。程序文件夹的默认值为V3Pro 2000 Deluxe。输入新的文件夹名或在已有文件夹中选择一个后，按下一步（N）按钮，将继续安装。

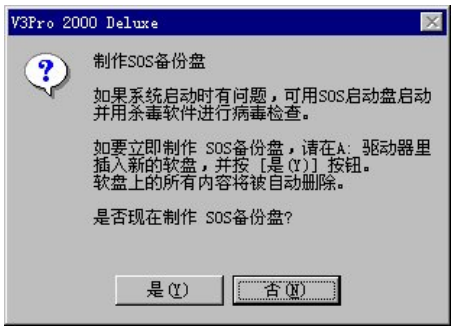


8. 设置V3Pro 2000 Deluxe以前，先确认到目前为止的设置内容。若要检讨或变更已设置内容，请按上一步（B）按钮，若满意，请按下一步（N）按钮。

9. 开始安装V3Pro 2000 Deluxe。



10. 结束安装以前，询问是否要制作SOS盘。

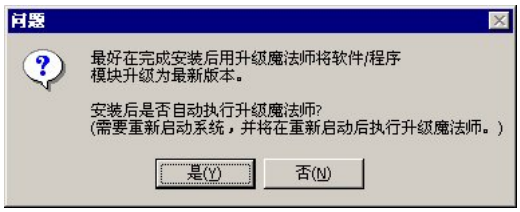


若要制作SOS盘，在A驱动器里插上软盘后按是（Y）按钮，就会显示出格式化窗口。指定格式化形式并其它选择项后按开始（S）按钮，则开始格式化。结束后按关闭（C）按钮，就可开始制作SOS盘。格式化时，软盘上的所有已存数据都会被删除，所以事先请务必进行软盘确认。（NT：若为NT则没有询问过程。）

11. 安装V3Pro 2000 Deluxe过程结束。若要使用‘Windows启动时即开始系统监视功能’，‘使用鼠标器右键快捷菜单检查功能’等功能，可按完成按钮。如果不直接使用，请选择相应设定后按完成按钮。

12. 按结束按钮，V3Pro 2000 Deluxe安装结束。

13. 安装结束后将询问是否执行升级魔法师功能，并升级到最新版本。

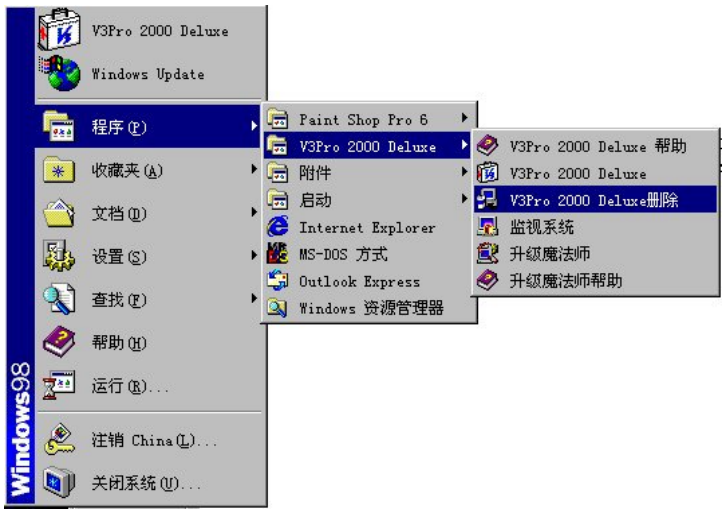


删除

若要在已安装V3Pro 2000 Deluxe的文件夹上重新安装V3Pro 2000 Deluxe，则只有删除旧版软件才能安全进行新版软件的安装。V3Pro 2000 Deluxe包含删除安装工具，因此可以方便的删除旧版软件。

V3Pro 2000 Deluxe 的删除过程

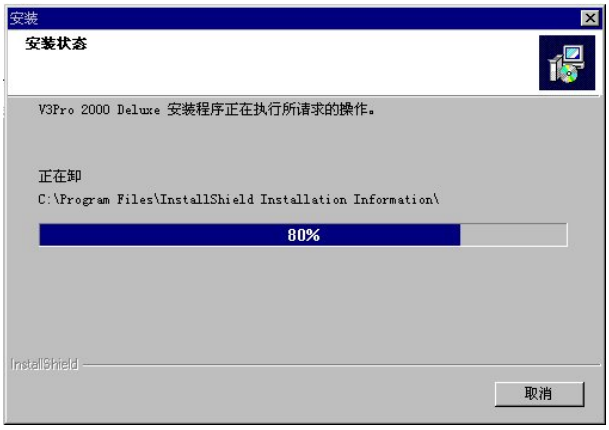
1. 首先在V3Pro 2000 Deluxe程序文件夹里执行V3Pro 2000 Deluxe删除。



用鼠标按开始后按程序→V3Pro 2000 Deluxe→V3Pro 2000 Deluxe删除的顺序移动鼠标指针。

2. 对以下询问，选择是（Y）按钮，开始删除。

3. 显示以下删除过程画面，逐个删除V3Pro 2000 Deluxe的各个组成部件直到删除结束。


安装
安装状态
V3Pro 2000 Deluxe 安装程序正在执行所请求的操作。
正在卸
C:\Program Files\InstallShield Installation Information\
80%
InstallShield
取消

第三章

浏览V3Pro 2000 Deluxe

- *执行*
- *基本画面构成*
- *初试检查及杀毒治疗功能*

执行

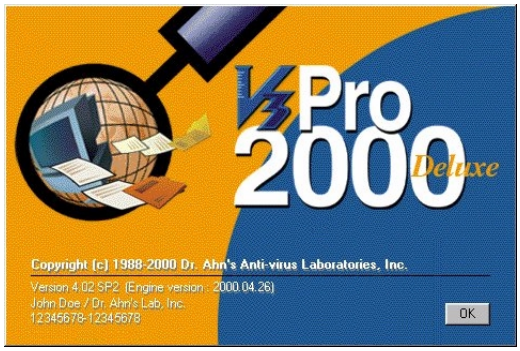
按视窗98/95及NT的任务栏上的开始按钮，将鼠标指针移到程序上。画面将显示子目录形式的程序组，将鼠标指针移到标有V3Pro 2000 Deluxe的子目录中，选择V3Pro 2000 Deluxe，则系统将执行V3Pro 2000 Deluxe。因安装后开始程序组中将自动生成V3Pro 2000 Deluxe执行图标，因此可直接按此图标以执行程序。

V3Pro 2000 Deluxe将在安装后自动在开始程序组中生成执行图标，因此可直接单击此处以执行程序。

用鼠标按 开始→程序→V3Pro 2000 Deluxe→ V3Pro 2000 Deluxe 的顺序移动鼠标指针。

基本画面构成

执行V3Pro 2000 Deluxe后将会瞬间显示信息画面，而后显示V3Pro 2000 Deluxe初始画面、即手动检查画面。



V3Pro 2000 Deluxe的菜单窗口基本由手动检查，检查状态，查看信息，查看记录，备份管理及传送至检举中心，工具，Web连接等构成。

基本构成及各要素名称、功能如下。

- **工具栏** - 是把V3Pro 2000 Deluxe常用功能集合在一起的工具栏。
- **快捷检查条** - 直接输入所要检查对象进行检查的功能。
- **菜单条** - 含有V3Pro 2000 Deluxe各种功能菜单。
- **菜单窗口** - 是V3Pro 2000 Deluxe命令菜单窗口。
- **工作窗口** - 根据各个菜单，显示其工作内容。
- **查看记录窗口** - 随着工作窗口的进行，显示其各种记录。

系统监视功能

V3Pro 2000 Deluxe的系统监视功能可在系统启动时一起启动，并在操作系统层次上24小时监视系统运作，防止病毒从外部的侵入，同时在发现被病毒感染的文件时自动采取治疗、删除、备份等措施，可在任何情况下保护系统于病毒的侵入。

在操作系统层次上对病毒进行实时检查。

NT：NT系统监视由服务程序支持。

菜单窗口内的菜单说明

- **手动检查** - 为V3Pro 2000 Deluxe执行后显示的初始画面。可指定要检查的对象单位是驱动器还是文件夹。设置完检查对象后按‘开始检查‘按钮进行对指定对象的检查。
- **检查状态** - 可看到与系统监视、Internet监视、预约检查、执行屏幕保护程序后进行检查、鼠标右键检查等环境设置状态有关的内容。
- **显示信息** - 可得到病毒日历、病毒信息、信息笔记菜单等各种有用的信息。
- **显示记录** - 显示系统及互联网的监视情况，发现病毒时的检查记录，记录功能升级的成功与否等的事件记录，以及检查结果内容。
- **备份管理与传送至检举中心** - 发现病毒时可将感染文件还原到任意文件夹，如发现新种病毒可利用此功能将可疑文件传送到病毒检举中心。
- **工具** - 提供升级魔法师、Neo扫描、引导区备份、SOS软盘制作、Office Protector等功能，使 V3Pro 2000 Deluxe成为功能更加强大的病毒防治软件。适当利用这些功能可给自己的计算机系统提供更加强大的病毒防治环境。（NT：NT的工具栏没有引导区备份及SOS软盘制作功能。）
- **Web连接** - 利用此功能可直接连接到安研究所主页（安研究所主页、安研究所新闻、新种病毒、病毒问答、WebJin病毒新闻、在线登记等）。

检查、治疗功能浏览

在仔细学习V3Pro 2000 Deluxe功能之前让我们先粗略了解发现病毒时的检查及治疗方法。

病毒检查

执行V3Pro 2000 Deluxe后，在手动检查画面上选择要检查的驱动器，则该驱动器的图标变成深色。选择检查对象后按开始检查按钮进行对该驱动器的病毒检查（如果要检查的驱动器只有一个，则可用鼠标双击该驱动器图标以开始病毒检查）。如果要同时选择多个驱动器，则可拖动鼠标一次完成多个驱动器的选择。

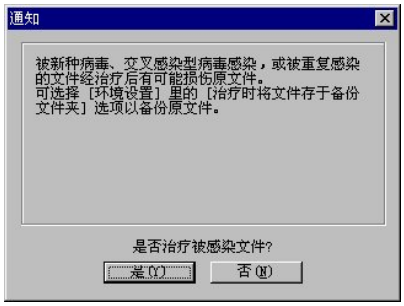
病毒的发现及治疗

如果在检查中发现计算机病毒，系统将发出警告音（‘哔’声）并显示被病毒感染的文件名、文件夹名、检查日期、病毒名称、状态、检查方法等信息。此后则可按用户选择的选项设置（环境设置里的一般设置）进行治疗。

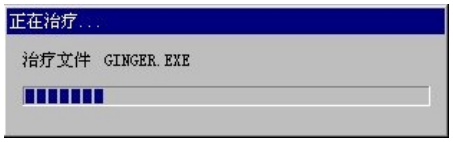
- **治疗所有目录项** – 要治疗病毒治疗窗口内显示的所有病毒项时。
- **治疗选择目录项** – 只治疗用户指定的目录内文件。

如果在治疗目录内的所有项目，选择治疗所有目录项（A）， 如果要治疗目录内指定的部分目录项，选择治疗选择目录项 （C）进行治疗。

显示以下画面时按是（Y） 则开始治疗被病毒感染的文件。



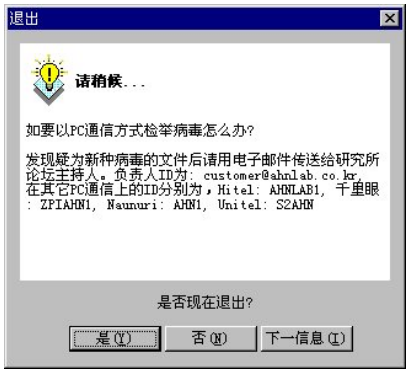
按是（Y）即开始治疗被感染文件。



治疗结束后显示以下信息以提供治疗结果。

退出

如要退出V3Pro 2000 Deluxe，可选择菜单的文件-退出，或按画面右上角的关闭按钮。每次退出都将显示请稍候… 对话框。



本对话框以短小篇幅及向导形式提供病毒相关信息。请参考提供内容后选择退出窗口的是（Y），则退出V3Pro 2000 Deluxe。

> 参考：退出V3Pro 2000 Deluxe后系统监视功能将继续工作。此功能需另行退出。

查看帮助

在V3Pro 2000 Deluxe的使用中如有疑难事项，可选择菜单的帮助-帮助项，或选择标准按钮上的帮助即可。

按病毒治疗窗口提供的状态信息进行治疗

检查病毒后病毒治疗窗口将显示以下状态信息。状态信息分结束治疗、可治疗、新种病毒、可执行压缩文件、压缩文件、无法治疗等。

可治疗

为V3Pro 2000 Deluxe可彻底治疗的文件，将被自动予以治疗。在可治疗文件中显示以下信息时请采取相关措施。

- 因病毒文件被损伤，按设置选项进行处理。
- 请解除Word文件口令后进行治疗。
- 请解除Excel文件口令后进行治疗。
- 请解除Power Point文件口令后进行治疗。
- 文件被损坏或为恶性编码，因此予以删除。
- 请在删除原文件后删除Windows的SYSTEM文件夹里的WSOCK32.DLL文件，并将WSOCK32.SKA文件改名为WSOCK32.DLL。

新种病毒（请将相关文件寄送到研究所）

为虽可诊断但以当前版本还无法治疗的文件。此时可将感染文件寄送安哲洙研究所的病毒检举中心。

可执行压缩文件（请在解压缩后重新进行检查）
压缩文件（请在解压缩后重新进行检查）

如在环境设置里选择可执行压缩文件或压缩文件检查选项后进行病毒检查，则系统将可检查出压缩文件所带的病毒，但是对此并不进行治疗。请用户在对该文件进行解压缩后再行治疗。

无法治疗（重复感染，感染交叉型病毒）

发现无法进行正常治疗的病毒时将显示以上信息。当一个文件被几个病毒同时感染导致文件损伤时，或被交叉型病毒 - 即在感染文件同时亦损伤文件的病毒所感染时，或治疗病毒后文件长变为0字节时，或治疗宏病毒而该文件带有口令或为被打开文件时，或在治疗被写保护了的软盘上时都会显示以上状态信息。

第四章

使用方法

- *利用菜单条的执行功能*
- *用快捷检查条直接进行检查*
  - *系统监视*
  - *手动检查*
  - *检查状态*
  - *查看信息*
  - *查看记录*
  - *环境设置*
- *备份管理及传送至检举中心*

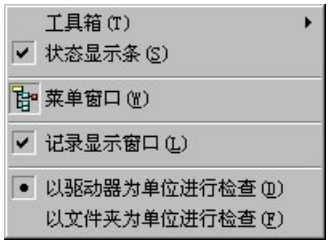
利用菜单条的执行功能

为利用菜单条的功能说明。文件部分的菜单将因菜单窗内容不同而稍有不同。下面是缺省值为手动检查画面景显示的菜单条内容。

文件

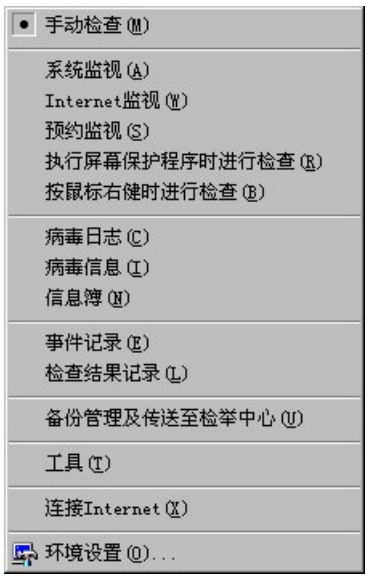
- **检查** - 检查在手动检查里设置的检查对象。
- **删除** - 删除选择目录或对象。
- **创建新对象目录** - 创建用户定义的检查对象。
- **登记信息** - 显示被指定为对象目录的文件夹等的信息。
- **升级魔法师** - 通过互联网获取升级服务。
- **退出** - 退出V3Pro 2000 Deluxe。

显示



- **工具栏** - 显示或隐藏工具栏。
- **状态显示条** - 显示状态显示条。
- **菜单窗口** - 显示菜单窗。
- **记录显示窗** - 显示记录显示窗。
- **以驱动器为单位进行检查** - 以驱动器为单位进行检查。
- **以文件夹为单位进行检查** - 以文件夹为单位进行检查。

作业



- **手动检查** - 设置手动检查。
- **系统监视** - 设置系统监视。
- **Internet监视** - 设置Internet监视。
- **预约检查** - 设置预约检查。
- **执行屏幕保护程序时进行检查** - 设置执行屏幕保护程序时进行检查选项。
- **按鼠标右键进行检查** - 设置按鼠标右键时进行检查选项。
- **病毒日历** - 将具有特定发作日期的病毒标于日历上以作预警。
- **病毒信息** - 为病毒分析信息数据库。
- **信息簿** - 安研究所提供的信息内容。
- **事件记录** - 系统/Internet监视与否，检查记录，功能升级的成功/失败记录等。
- **检查结果记录** - 显示检查结果。
- **备份管理及传送至检举中心** - 将发现的病毒保管于备份文件夹或传送到安研究所病毒检举中心。
- **工具** - 提供升级魔法师，Neo扫描，引导区备份，SOS软盘备份，Office Protector等各种工具。
- **连接Internet** - 连接安研究所主页。
- **环境设置** - 设置与各检查功能相关的选项。

帮助

- **帮助项** - 显示帮助。
- **V3Pro 2000 Deluxe信息** - 可确认用户名，产品序列号及版本日期等。

有用的热键!

热键	说明
F1	显示帮助
F2	在‘手动检查’窗口‘开始检查’
F3	转换为‘快捷检查条’
F5	‘信息簿’，‘事件记录’，‘检查结果记录’里的‘升级’
F6	转换到下一窗口
Shift + F6	转换到前一窗口

用快捷检查条直接进行检查

快捷检查条在以下位置上。

可在此处直接设置检查对象。

在用快捷检查条进行检查项的输入时文件夹的区分符号为空格。输入几个文件夹名时用空格进行区分，长文件夹名或带空格的文件夹名用“ ”进行区分。（请注意检查指定对象文件夹时并不包含子文件夹，因此如要包含子文件夹请设置 /s选项。）

项目	说明
选项帮助	/?
以驱动器为单位进行检查	C:
以文件夹为单位进行检查	C:\windows
检查多个文件夹	C:\windows, “c:\program files” d: /s
检查子文件夹	C:\windows /s
检查所有文件	C:\windows /a
检查压缩文件	C:\windows /c /s
以文件为单位进行检查	C:\windows\win.com
检查网络共享文件夹	\\ahn4\t\（输入时用\\进行区分。）

系统监视

系统监视功能在操作系统层次上监视系统运作，防止病毒从外部的侵入。如果没有在V3Pro 2000 Deluxe安装时或环境设置菜单时特别取消相关设置，则此一功能将在Windows 98/95或NT系统启动时一起启动。

执行此功能则在Windows的任务栏右侧产生一系统监视图标，将鼠标指针置于此图标上按右键，则显示三个功能如下。

- **打开** - 执行V3Pro 2000 Deluxe程序。
- **暂停** - 将暂时中止系统监视功能的执行。此时图标形状有变，如要重新执行只需选择本功能予以解除。
- **结束** - 结束系统监视程序的执行。

如要在Windows上直接执行系统监视功能，只需选择开始 - 程序 - V3Pro 2000 Deluxe - 系统监视即可。

手动检查

如要进行手动检查

为设置检查对象以进行病毒检查的菜单。同时因显示记录窗口提示软件版本日期与设置的选项等，因此可方便地查看用户设置的内容。

V3Pro 2000 Deluxe自动识别与系统连接的所有磁盘驱动器，作业窗口显示这些驱动器的图标，并兼有检查对象的设置与解除作业窗口的功能，因此可直接将各图标指定为检查对象或解除之。

用鼠标按各图标，则该图标显为深色，该图标所代表的区域将被指定为病毒检查对象。反之如要从检查对象中解除，则用鼠标单标已被选为检查对象的图标即可。

在检查对象设置窗里设置检查对象后按开始检查，则开始对用户设置的检查对象进行病毒检查。也可在检查对象设置窗里双击相关驱动器直接开始检查。

如果检查结果未有发现病毒，则显示信息将表明没有病毒，如果发现病毒，则在检查结束后自动显示治疗窗口开始进行治疗。

新对象目录

可指定用户定义的新对象目录。利用此功能可对用户特别指定的文件夹或驱动器进行单独检查，因用户可按不同环境指定需要特别关注的检查对象，因此可减低检查整个驱动器时的低效率，节约检查时间，特别是对使用大容量硬盘的用户。

选择手动检查作业窗口的创建新对象目录，则可打开设置用户定义检查对象窗口。左侧分窗为选择对象目标，右侧分窗为检查对象目录。选择需要的项目后进行追加。

以文件夹为单位进行检查/以驱动器为单位进行检查

作为缺省设置，第一次执行V3Pro 2000 Deluxe后检查窗口将显示以驱动器为单位进行检查的画面。如要以文件夹为单位进行检查，则选择以文件夹为

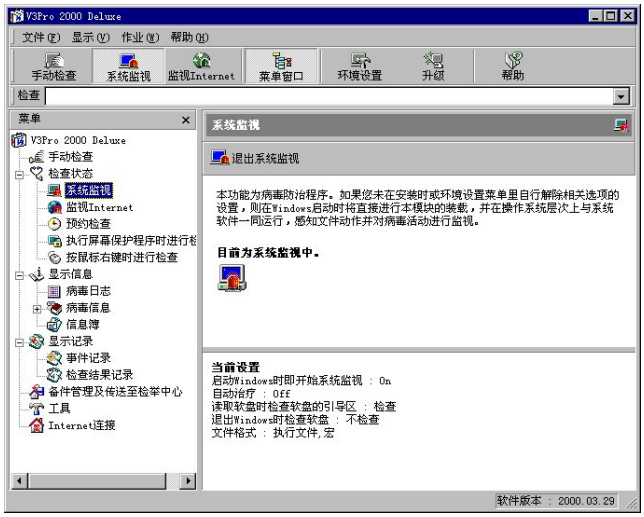
单位进行检查并以文件夹为单位设置检查对象。

如要重新以驱动器为单位进行检查，则选择以驱动器为单位进行检查即可。

检查状态

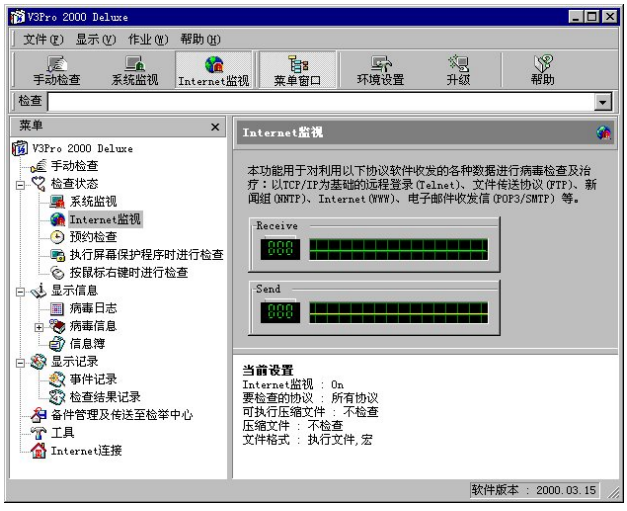
系统监视

可查看系统是处于监视状态下还是暂时中止状态下。如果没有在安装时或环境设置菜单时特别取消相关设置，则此一功能将在Windows启动时一起启动，并在操作系统层次上监视系统运作， 自动检查病毒。



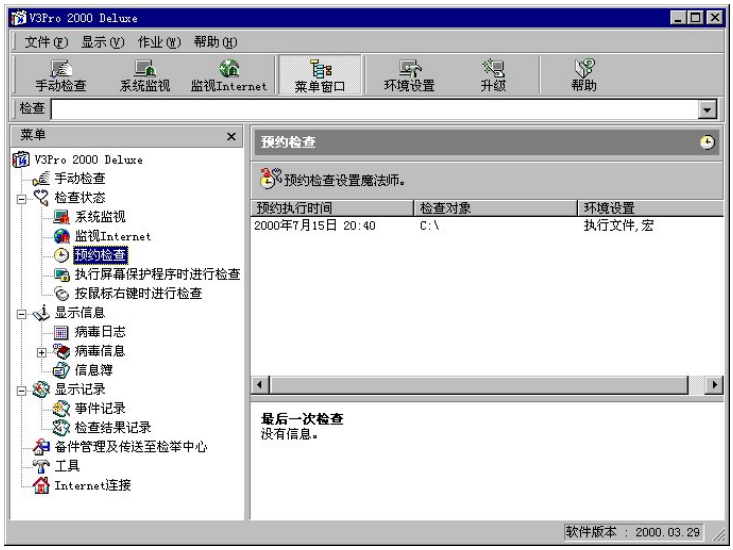
Internet 监视

可通过图象画面查看出入互联网的数据状态。如果要检查以TCP/IP为基础的所有协议，请选择所有协议，如只需检查特定协议，则可在环境设置菜单指定相关协议。



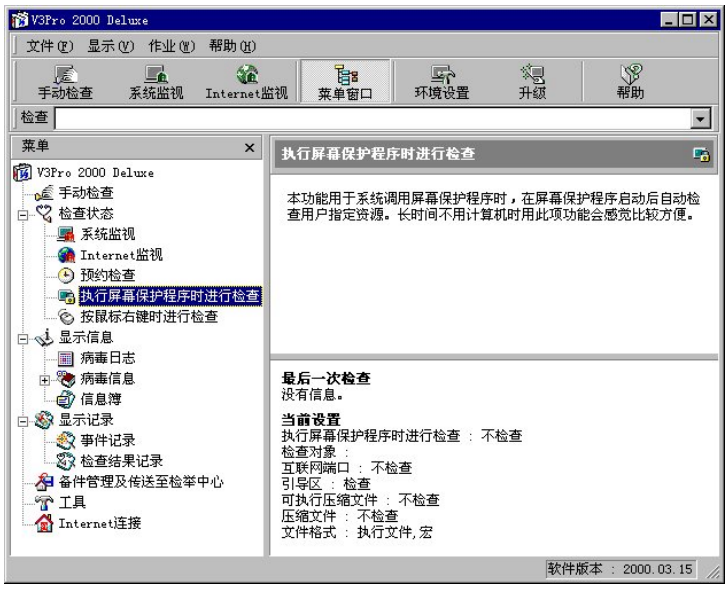
预约检查

可查看等待中的预约检查状态。如果要追加预约检查，可单击预约检查设置魔法师设置您所需的预约时间。



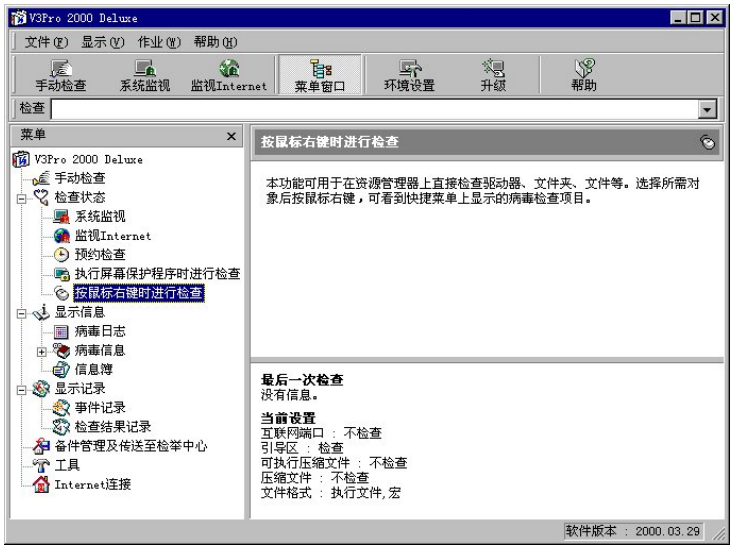
执行屏幕保护程序时进行检查

可查看与执行屏幕保护程序时进行检查相关的设置状态。如果设置了此选项，则当屏幕保护程序时系统将在自动检查用户指定的检查对象。可在长时间不用计算机时利用此功能。



按鼠标右键进行检查

可查看按鼠标右键进行检查时的设置状态与检查状态。



利用按鼠标右键进行检查功能可在资源管理器等上直接对驱动器、文件夹或文件等进行检查。选择一对象后按鼠标右键，可在显示的快捷菜单上看到病毒检查菜单项。

按此处可在资源管理器上直接对检查对象进行检查。

选择快捷菜单上的用V3进行病毒检查，则可直接检查相关检查对象。

查看信息

病毒日历

可通过病毒日历®查看在特定日期发作的病毒信息。

有些计算机病毒通过测试系统的日期与时间，在特定日期发作以为害用户，此为特定日期发作病毒。

这些病毒中比较有代表性的有：在米开朗基罗的生日3月6日发作的米开朗基罗病毒，有在13日与星期五相叠的日子发作的耶路撒冷病毒，在12月25日发作的圣诞节问候病毒等。虽然特定日期发作病毒在整个病毒中所占比例并不高，但利用此病毒日历可对此种病毒早作提防，并可唤起对病毒的注意。

病毒日历®的病毒信息窗口中有当前月份日历及每日发作病毒目录等。以下半部还可看到相关病毒信息。如选择Filp.2153病毒名称，则可看到与该病毒的特征（种类、感染方法、感染位置、症状）有关的信息。

另外可按需要选择不同年度的月历，选择不同日期以查看在该日期发作的病毒信息等。可利用日历上端的方向按钮以一年或一月为单位查找特定日期发作病毒的发作日期。

按方向按钮翻动日历，则显示相关年度月份的日历，日期则固定在现在状态上。如果要查看在某特定日期发作的病毒，可翻动日历到需要的年度月份后将，鼠标指针置于该日期上并单击之。

病毒信息

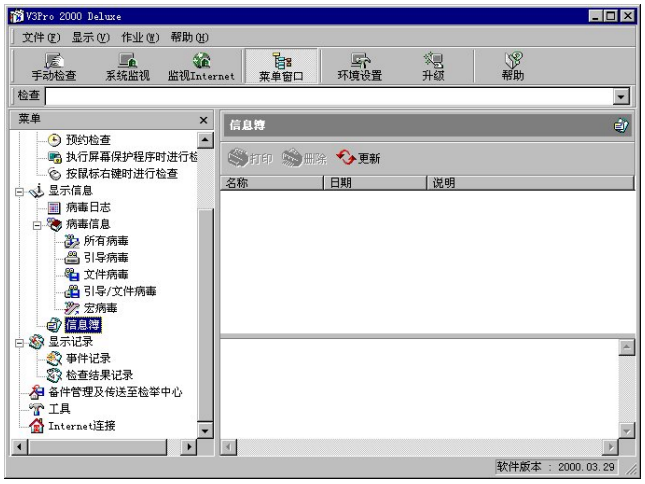
按类显示可诊断/治疗病毒的详细分析信息。可查看所有病毒、引导病毒、文件病毒、引导/文件病毒、宏病毒等的分析资料。

- **所有病毒** – 所有种类的病毒
- **引导** – 专门感染引导区的病毒
- **文件** – 感染文件的病毒
- **引导/文件** – 既感染引导扇区又可感染可执行文件的病毒
- **宏** – 利用宏功能传染的病毒

选择用户想要了解的病毒种类，则显示病毒信息窗口。病毒信息窗分7个菜单，用鼠标选择各个病毒以查看相关信息。

信息簿

可查看安研究所进行软件功能升级时发送给用户的文本文件。该文本文件包含与追加的病毒，新种病毒，其它病毒等有关的信息。



查看记录

事件记录

显示系统及互联网的监视情况，发现病毒时的检查记录，功能升级的成功与否记录等。（NT：NT系统不记录事件日志。该记录将在V3Pro 2000 Deluxe的检查记录/事件记录中。）

- **全部删除** - 删除所有当前记录。
- **更新** - 如果有新内容，则显示变更了的内容。

检查结果记录

V3Pro 2000 Deluxe在病毒检查后如发现病毒将保存检查记录以供用户参考，检查结果记录即提供此一功能。选择检查结果记录，可查看到最近为止的所有病毒记录。‘文件名’及‘文件夹名’显示被确认为感染了病毒的文件名及该文件所属的文件夹路径名，‘病毒名称’显示感染了的病毒名称。‘状态’栏则显示与是否完成治疗有关的结果记录。

环境设置

V3Pro 2000 Deluxe提供多种环境设置选项。善用V3Pro 2000 Deluxe提供的环境设置菜单可构筑更强有力的病毒防治环境。按标准按钮的环境设置或选择菜单的作业-环境设置，则可对一般、手动检查、系统/Internet监视、预约检查、执行屏幕保护程序时进行检查、用鼠标右键进行检查等进行设置，这里包括以下选项。

治疗设置

执行环境设置-一般以进行一般检查选项的设置。

- 治疗时将文件备份保管于备份文件夹
- 处理无法治疗的文件
- 发现病毒时发出警告音-
- 只在发现病毒时显示检查结果
- 保存检查记录 / DMZ设置

检查设置

设置要检查的区域及检查对象。

- **检查引导区** - 检查系统的引导区
- **检查可执行压缩文件** - 检查DIET、LZEXE、PKLITE等可执行压缩文件。
- **检查压缩文件** - 检查扩展名为ZIP、ARJ、RAR、JAR、CAB、LHA、UUEN/DECODE、ZOO、MIME等的压缩文件。
- **检查双重压缩文件** - 检查双重压缩文件。

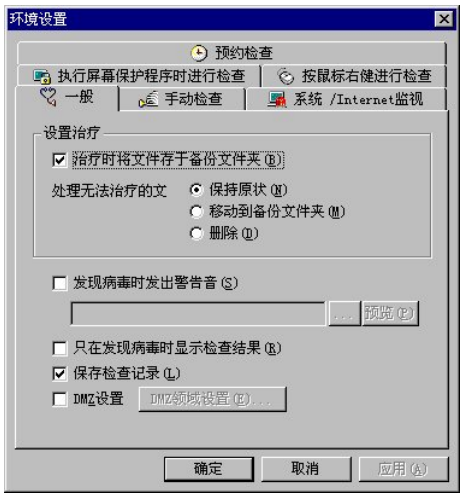
要检查的文件格式

设置要检查的文件格式。

- **检查所有文件** - 检查宏、可执行文件、压缩文件、一般文本文件等所有格式的文件。
- **检查可执行文件** - 检查扩展名为COM、EXE、OVL、DLL、BIN等可以执行的文件。
- **检查宏** - 检查可被宏病毒感染的文件。
- **检查用户定义文件** - 检查带有用户指定扩展名的文件。

一般设置

选择环境设置一般将显示进行各种检查时的选项设置画面。



在各种检查时指定检查对象的选项。对治疗时将文件备份保管于备份文件夹、处理无法治疗的文件等可在治疗时指定对指定文件的处理方法。同时发现病毒时发出警告音、只在发现病毒时显示检查结果、保存检查记录、DMZ设置等也有相关选项（DMZ显示‘不检查的区域’。）

治疗时将文件备份保管于备份文件夹

这是为了防止在治疗过程中损伤原文件而引起数据丢失，把发现有病毒而欲治疗的文件在治疗前先进行备份。如DATA.COM文件感染病毒时将在备份过程中产生一个扩展名为V3B的DATA.V3B文件。

处理无法治疗的文件

利用此功能，可以在发现无法正常清除的病毒时，将相关文件移动/保存到用户指定的文件夹或加以删除。默认值设为‘保持原状’，也可按用户意愿将不可解毒之文件移动到备份文件夹或直接加以删除。

- **保持原状** - 将文件原样放置。
- **移动到备份文件夹** - 将文件移动到备份文件夹中。
- **删除** - 删除该文件。

发现病毒时发出警告音

可在此指定发现病毒时通过扬声器发出的警告音。可变更WAV文件选择用户喜欢的警告音。

保存检查记录

设置‘保存检查记录’，则在检查病毒后生成每日一份的LOG文件记录检查结果。

> **参考**：事件日志为自动记录项。

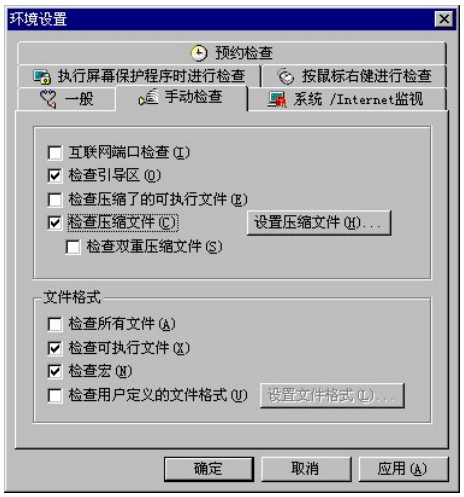
DMZ 设置

意为‘设置不需检查的区域’，对大容量磁盘用户尤其有用。如果用户认为某文件夹绝对不会有病毒，检查该文件夹属时间浪费，则可以将该文件夹设为不需检查的区域。进行DMZ设置时需注意的是，调用V3Pro 2000 Deluxe的任何查毒方法都不会检查用DMZ设置了的区域。

> **注意：**非熟练用户最好不要设置‘DMZ设置’。

手动检查

在V3Pro 2000 Deluxe的初始画面上选择驱动器或文件夹，并按开始检查按钮进行查毒时将用到手动检查选项。缺省值为只检查引导区、可执行文件及宏文件。

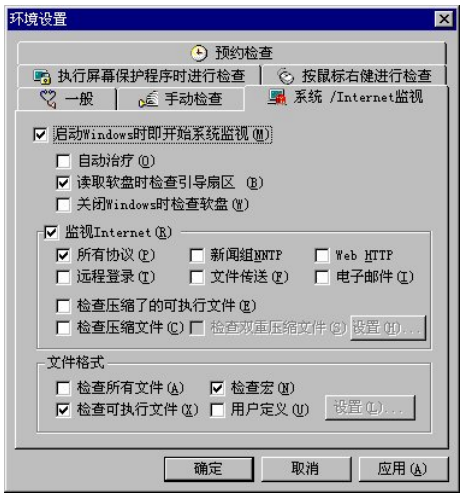


系统/Internet 监视

系统/Internet监视程序将在Windows的系统层次上防止病毒文件的执行。V3Pro 2000 Deluxe建议用户在安装本系统时即设置本监视功能，这样只要安装了V3Pro 2000 Deluxe软件，监视程序就会在后台工作，保护系统安全。

可在Windows 9x / NT (Workstation) / 2000 (Professional)的任务栏右角看到系统监视设置图标。此图标显示系统监视程序正在工作中。

> **参考：**因Internet监视功能包含于系统监视功能之内，因此中断系统监视即同时中断Internet监视。



系统监视选项

- **启动Windows即开始系统监视** - 安装时可对此选项进行选择设置。解除此项目的选择即可改变设置。
- **自动治疗** - 执行或打开病毒感染文件时即自动治疗相关文件，使得系统只能执行或打开正常文件的强力反病毒功能，可从根本上保护系统于文件病毒及宏病毒的感染。
- **读取软盘时检查引导扇区** - 为了防止从软盘上感染引导型病毒，可设置本选项以在使用软盘时对引导扇区进行检查。
- **关闭Windows时检查软盘** - 在退出Windows对软盘进行检查，彻底防止病毒从软盘的侵入。

文件格式

- **检查所有文件** - 检查所有格式的文件。
- **检查宏文件** - 检查可能被宏病毒感染的文件。
- **检查可执行文件** - 检查扩展名为COM、EXE、OVL、DLL、BIN等的可执行文件。
- **用户定义** - 检查扩展名为用户指定之文件。

如果只考虑系统的安全，当然要选择‘检查所有文件’。但因大部分病毒主要感染可执行文件及可被宏病毒感染的文件，因此选择检查宏文件及可执行文件可以缩短系统检查时间。

监视 Internet

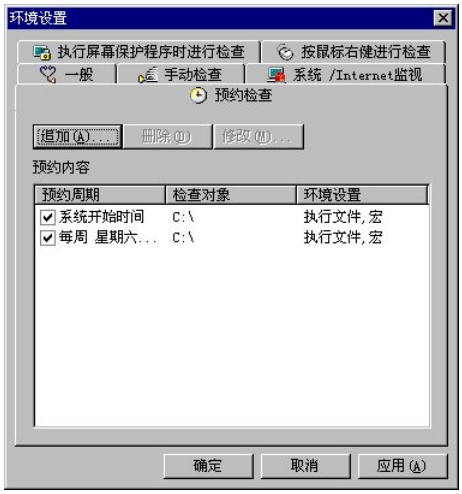
- **所有协议** - 监视所有协议。
- **新闻组NNTP** - 监视NNTP。
- **Web HTTP** - 监视HTTP。
- **远程登录** - 监视TELNET。
- **文件传送** - 监视FTP。
- **电子邮件** - 监视POP3及SMTP。
- **检查可执行压缩文件** - 检查DIET、LZEXE、PKLITE等压缩可执行文件。

- **检查压缩文件** - 检查扩展名为ZIP、ARJ、RAR、CAB、LHA、UUEN/DECODE、ZOO等的压缩文件。
- **检查双重压缩文件** - 检查被双重压缩了的文件。

设置预约检查

可与‘执行屏幕保护程序时进行检查’功能并行使用，可在长时间闲置系统时在指定时间对指定区域进行检查。

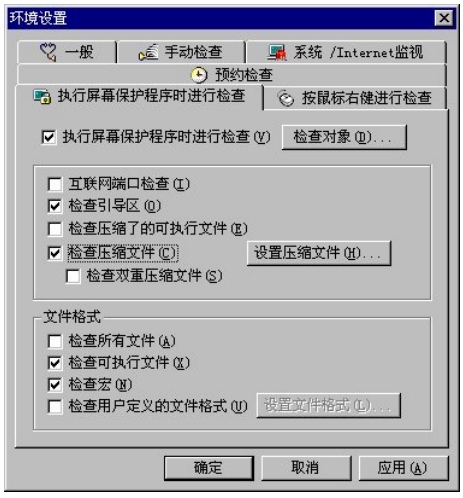
预约检查为非缺省设置项，通过设置预约周期，可在系统启动时，或每日、每周、每月在特定时间对设为检查对象的驱动器或文件夹进行检查。



按追加按钮则执行预约检查设置魔法师，显示检查周期设置画面，对此进行设置后可指定预约检查时要用到的检查方法及文件格式。

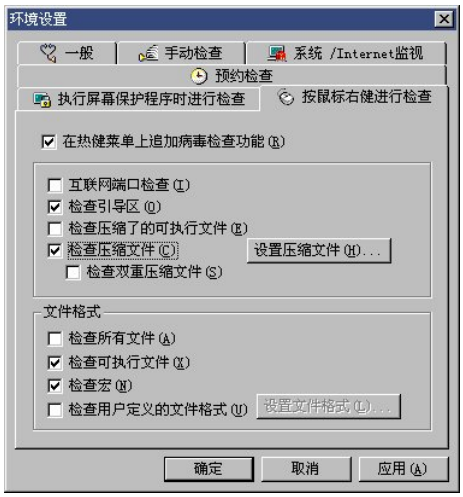
执行屏幕保护程序时执行检查

可利用此功能，在执行屏幕保护程序时对系统进行检查。缺省值为非设置状态。



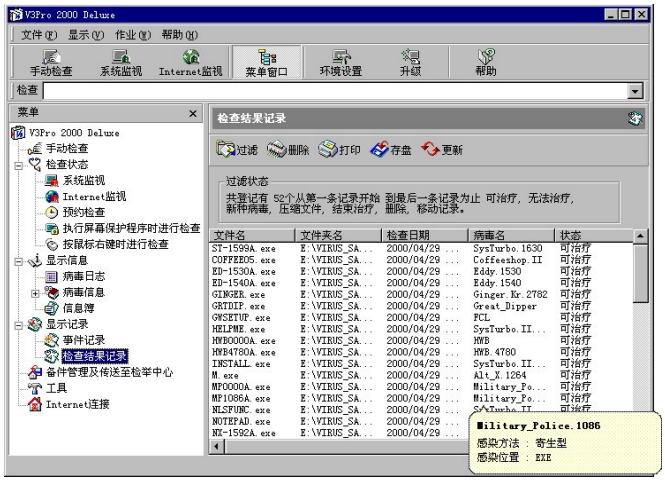
按鼠标右键进行检查

可设置是否利用鼠标右键对特定区域（驱动器/文件/文件夹）进行检查。V3Pro 2000 Deluxe建议用户在安装时即设置本功能，如要解除本功能，可在环境设置菜单里取消对‘在热键菜单上追加病毒检查功能’选项的设置。



可在检查记录窗口里查看病毒信息

将鼠标指针移到检查记录窗口里的病毒名上，则可在提示形式的帮助上看到有关该病毒的相关信息。



如以上画面，将鼠标指针移到Win-Trojan/Back-Orifice，则可看到提示形式的帮助上显示的关于该病毒的简要信息。相关病毒的详细信息可利用病毒信息菜单。

备份管理及传送至检举中心

如果用户的计算机系统可连接互联网，用户可在需要对病毒进行咨询或检举新种病毒时连接研究所提供的网站（www.ahnlab.com）直接发送电子邮件进行询问，或将可疑文件传送至检举中心。进行研究所的主页，连接病毒检举中心后选择病毒检举表，按此表进行询问可使用户更快得到回复。

在菜单窗选择备份管理及传送至检举中心即可直接连到研究所互联网主页内的病毒检举中心。

- **还原** - 将文件还原到原文件夹。因为是感染了病毒的文件，请小心使用此功能。
- **还原到任意文件夹** - 将相关文件移动到别的文件夹。
- **传送至检举中心** - 将染毒文件传送至检举中心。只可传送新种病毒或无法清除的病毒。
- **删除** - 删除指定对象。
- **登记信息** - 可查看备份前的文件信息。

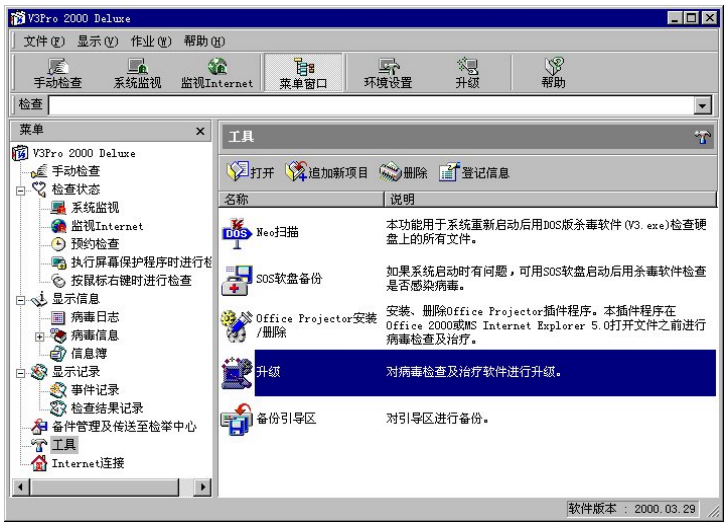
第五章

工具及Web连接

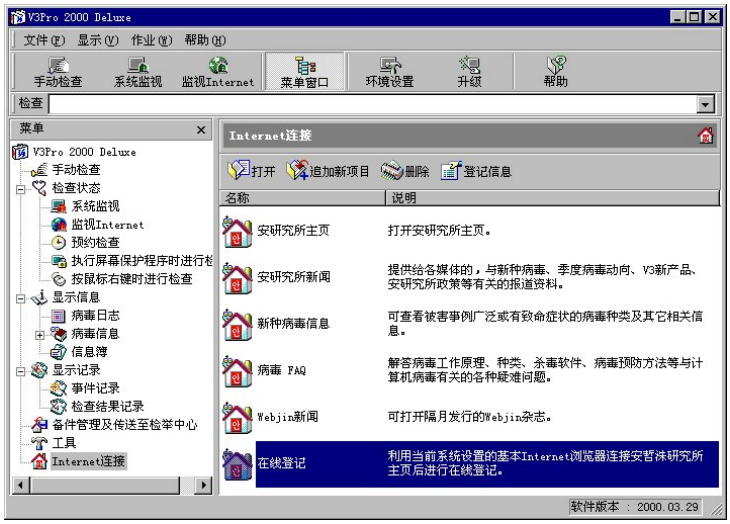
- *升级魔法师*
- *Neo扫描*
- *引导区备份*
- *SOS软盘制作*
- *Office Protector*
- *Web连接*

V3Pro 2000 Deluxe的工具及连接Internet上有升级魔法师、Neo扫描、引导区备份、SOS软盘制作及连接安哲洙研究所主页的功能（安研究所主页、安研究所新闻、新种病毒、病毒问答、WebJin病毒新闻、在线登记），这些功能使得V3Pro 2000 Deluxe成为更加强力的反病毒软件。有效利用这些功能可使自己的系统更安全。

工具菜单



连接 Internet 菜单



升级魔法师

什么叫升级魔法师

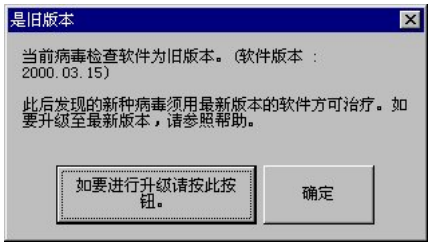
升级魔法师（Smart Update）™作为安哲洙研究所开发的引擎自动升级服务功能，可以通过安哲洙研究所主页上的升级服务器自动下载引擎升级文件及研究所发给用户的通知信息。

升级魔法师™服务支持自动及手动模式，可按用户要求随时为用户提供最新杀毒引擎。

升级方法

1. 选择作业窗口的**工具-升级魔法师**，或工具栏的升级，或菜单的文件-升级魔法师，则可执行升级魔法师®工具。

2. 用户可按自己的系统环境选择要升级的引擎种类及服务器，按开始升级按钮，将显示以下画面。按开始引擎升级按钮，即可升级为最新引擎升级文件。



3. 引擎升级文件夹的缺省值是V3Pro 2000 Deluxe的安装文件夹下的UPDATE

子文件夹。如果目前安装的V3Pro 2000 Deluxe引擎是一个月以前的版本，则在执行V3Pro 2000 Deluxe后将显示以下画面以自动通知用户需要进行引擎升级。

环境设置

一般环境设置

对进行升级后是否自动打开升级后信息及是否将系统用作升级服务器进行设置。

如果指定升级后自动打开信息选项，则可在升级后自动打开相关文件。

如果指定将本系统用作升级服务器选项，则可将该系统用作升级服务器。

Internet 设置

可利用以下升级服务器进行升级。

- Kornet服务器
- Shinbiro服务器
- Bora Net服务器
- I-Net服务器

请在以上服务器中选择使用最快的互联网服务器。这功能只在系统可连接互联网时方才有效。如果使用代理服务器，可选择使用代理服务器选项，并输入代理服务器的地址及端口。

通过 V3Net 进行升级

可通过服务器软件包V3Net接受升级服务。

安装在网络同一区域上的的服务器版V3软件包可利用V3Net进行升级。因此如果没有V3Net或系统未连接互联网，则此升级方法无效。

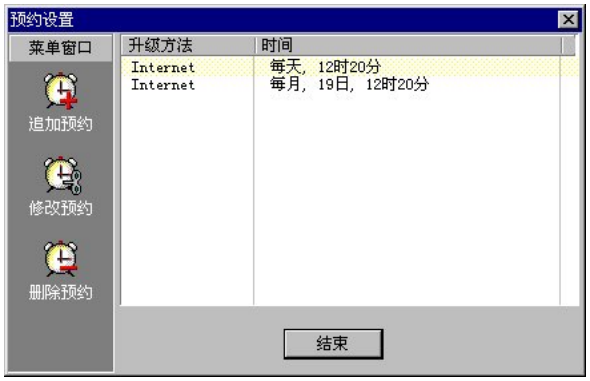
利用共享文件夹进行升级

输入要共享的文件夹名以完成设置。

可直接在存有引擎升级文件的网络驱动器的共享文件夹上直接进行升级，或指定本地盘（A:，C: 等）或本地盘上的文件夹以进行升级。

预约设置

可指定升级方法及预约日期。



追加

按追加预约按钮指定升级方法及预约日期。升级方法可选择Internet，V3Net，共享文件夹等。预约日期可选择每日、每周、每月、用户选择等选项。

修改

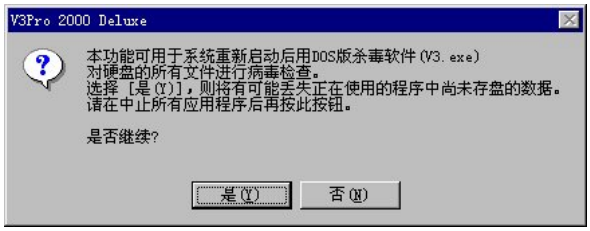
在选择想要修改的预约检查项后按修改预约按钮，将显示预约检查设置画面。在对想要修改的项目进行修改后按确认按钮退出。

删除

选择想要删除的预约检查项后按删除预约按钮。

Neo 扫描

利用Neo扫描功能为了从根本上封锁病毒的侵入先自动强行退出Windows系统。然后在重新启动为DOS状态并用DOS版杀毒软件V3+ Neo进行硬盘检查。特别是Windows系统正在使用的文件被病毒感染时这一方法更加有效。



按是（Y）即执行Neo扫描。

引导区备份

为了对付可疑的新引导区病毒，或因应引导区数据分析需要，此功能将对引导区进行备份（存盘）。

利用引导区备份程序，可在系统感染新型引导型病毒时对病毒进行取样。也可把正常的系统引导区域备份下来，以便引导区被病毒破坏时用作系统修复的参考资料。

按V3Pro 2000 Deluxe的工具-引导区备份按钮，显示引导区备份窗口。

引导区备份窗口可分为两个分窗，可在左窗口选择在备份的文件夹，在右窗口选择要存放的文件夹。因备份驱动器设为C缺省值，因此要存放的文件夹可选软盘驱动器A。如果要备份文件夹软盘的引导区，可在软盘驱动器图标的左侧用鼠标加一标识，反之如果不欲对研究的引导区进行备份，则可解除硬盘驱动器图标的设置。同理，如要存放的文件夹也可按此方法进行指定或解除指定。设置要存放引导区域的驱动器与文件夹后，请按开始备份 （B）按钮进行备份，最后将显示执行结果。

此时按确定钮，并按引导区备份窗品的返回按钮，即回到之前画面。

引导区的备份可在主菜单上选择作业-工具-引导区备份即可进行。

SOS 软盘制作

选择工具-SOS软盘制作菜单即可制作启动引导盘以备急需。插入A驱动器的软盘将被格式化，因此请先查看该软盘上是否有不可丢失数据。

在格式化窗里按开始（S）按钮，格式化结束后请选择关闭（C）按钮。则系统信息将复制到软盘上。

另外在制作的SOS软盘上可发现V3RESCUE.EXE文件。

这个程序可将备份在SOS软盘上的相关硬盘之引导区自动复制到硬盘上，以修复被病毒损伤的硬盘引导区数据。（NT：NT没有SOS软盘制作功能。）

注意： 制作SOS软盘后如果因硬盘格式化作业使得系统引导区数据发生变化，则此时硬盘引导区的数据与SOS软盘制作当时的系统（系统变更前）引导区数据将不再一样。如果无视这种情况，用含有旧引导区数据的SOS软盘修复当前系统，则系统将有可能发生致命错误。因此在使用V3RESCUE.EXE程序前务请加以确认。

Office Protector

可用来查杀通过MS Office 2000或MS Internet Explorer 5.0等的打开文件、下载、打开OLE文件等任务而传染的病毒。

如要安装或删除MS Office 2000或MS Internet Explorer 5.0插件程序，可双击该项并在显示出的以下画面中回答是安装还是删除。

如要安装插件，选择安装，如要删除，选择删除。

Web 连接

在菜单窗里有通过选择连接Internet连到安哲洙研究所网站的工具。提供安研究所主页，安研究所新闻，新种病毒，病毒问答，WebJin病毒新闻，在线登记等菜单。

- **安研究所主页** - 连接安哲洙研究所主页。
- **安研究所新闻** - 可看到从新种病毒、病毒动向到V3软件包、安研究所决策等提供给各传媒的报道资料。
- **新种病毒** - 提供与主页新种病毒警报所提病毒有关的信息。可看到被害事例广泛或症状严重的病毒种类及相关信息。
- **病毒FAQ** - 在此用户可得到与计算机病毒有关的各种问题解答。提供从病毒的工作原理、种类，到与杀毒软件的关系，病毒预防方法等方面的各种知识。
- **WebJin病毒新闻** - 可通过WebJin显看安哲洙研究所发生的隔月刊“安哲洙计算机病毒新闻”。
- **在线登记** - 为了方便用户注册，提供在线登记功能。

附录

- *病毒预防五项守则*
- *病毒用语说明*
- *FAQ（常见问答）*
- *关于DOS版V3+Neo*

病毒预防五项守则

只靠杀毒软件无法完美防范日益增多的新种计算机病毒。更重要的不是感染病毒后的杀毒，而是预防病毒的感染。如能遵守以下守则，则可预防大部分的计算机病毒。

1. 只使用正品，不使用盗版。
2. 重要程序及数据应随时备份（备份）。
3. 使用新程序时请使用最新版本的杀毒软件进行检查。并定期对系统进行检查。
4. 如使用共享或公开软件，则最好在熟悉本软件的计算机人士处下载该文件。
5. 请在未被病毒感染的干净DOS盘上加上写保护，以备非常时刻预备。

病毒用语说明

计算机病毒

可定义为“背着用户，将自身复制到其它程序的程序代码”。更精确的定义是“把计算机程序或把其它可执行部分变形以后，在那里复制自己或自己的变形的程序代码”。

命名为病毒是因为就像生物学里的病毒含有自我复制的遗传基因一样，电脑病毒也含有自我复制的程序代码。因此，“计算机病毒”的更精确的表达应为“计算机病毒程序（Computer Virus Program）”。

特洛伊木马（Trojan Horse）

这是“没有自我复制能力，以引起副作用为其目的而编写的程序代码”。更精确的定义是“背着用户在电脑程序里故意隐藏的没有自我复制能力的程序代码”。

特洛伊木马程序含有故意的一面，这一点有别于因程序编写员失误而造成的错误（Bug）。此外，它不把自己复制在其它程序里，这一点又有别于计算机病毒。举个例子，如果在执行一个文件时，虽然删除硬盘里的所有文件，但并不把自己复制到其它程序里，那么它就是特洛伊木马而不是电脑病毒。

原始型病毒（Primitive Virus）

也叫做第一代电脑病毒，结构非常简单。石头（Stoned）病毒，耶路撒冷（Jerusalem）病毒等属于此类。

密码型病毒（Encryption Virus）

为了不被解毒软件诊断，把病毒程序的一部分或大部分使用密码储存的病毒。瀑布（Cascade）病毒，漫步（Slow）病毒等属于此类。

隐蔽型病毒（Stealth Virus）

为了隐蔽自己并给用户或解毒软件提供错误情报，使用各种各样的方法。即，储存在记忆体中并假示被其感染文件大小没有变化，当解毒软件欲读被感染部分时，它显示被感染以前的内容，以此隐瞒解毒软件或用户。Brain病毒，Joshi病毒，512病毒，4096病毒等属于此类。

千面人病毒（Polymorphic Virus）

虽然它是密码形病毒的一种，但它随着每次被感染，其病毒码也跟着改变的一种可怕的病毒。有一种千面人病毒能变形一百万次以上，因此能引起很大混乱。

巨集病毒 （也叫宏病毒，Macro Virus）

巨集病毒是从去年开始在全世界范围内迅速扩散的一种病毒。它是利用MS公司出品的办公程序里的巨集功能而制造的，在世界各地相继传出其危害事件，更加重了其危害性。

引导型病毒

引导型病毒隐藏在硬盘的第一个扇区，即我们平常所说的引导区。在全世界最初被发现的病毒即Brain病毒和米开朗基罗病毒等都属于此类。

文件型病毒

这是感染一般文件的病毒。此时被感染的程序有COM，EXE等可执行文件，Overlay文件，周边器驱动程序等。

引导型/文件型病毒

这是感染引导区和文件的病毒，包括Natas病毒，One_Half病毒，Tequila病毒等都属于此类。

寄生虫病毒（Parasitic Virus）

它是不破坏原程序，而储存在程序前后的一种病毒。被此类病毒感染的文件里，原程序和病毒程序共存。当执行此文件时，先执行病毒程序而后再执行原程序，因此很难被发现。大部分文件型病毒属于此类。

重叠型病毒（Overwriting Virus）

这是病毒程序重叠在原程序上的一种病毒。一般的重叠型病毒处在文件的前面。当执行此文件时，病毒程序代替原程序被执行，而且原程序已被破坏，因此解毒软件也很难对原程序进行还原。但是，当此病毒储存在程序里不使用的领域时，对原程序的执行没有任何影响，可用解毒软件复原。

产卵型病毒（也叫伴随型病毒，Spawning Virus）

它不直接感染EXE文件，而另制一份相同名称的COM文件，并把病毒文件存进去。当这相同名称的COM文件和EXE文件存于同一子目录时，输入文件名并执行文件就会先执行COM文件，因此其症状与被文件型病毒感染时相同。其中最有名的是AIDS II病毒。

连接型病毒（Linking Virus）

它不直接感染程序，而把储存在子目录领域里的程序起始地址变更到病毒程序起始地址。当执行程序时，先执行病毒程序而后再执行原程序，因此很难发现。其典型例子为Byway病毒。

非驻留型病毒

此类病毒被执行一次以后，就从记忆体里消失。台湾病毒，维也纳病毒属于此类。

驻留型病毒

这是一直储存在记忆体里，并继续感染文件的一种病毒。耶路撒冷病毒，黑暗复仇者（Dark_Avenger）病毒属于此类。

黑客（hacker）

原是对那些热衷于对电脑系统的内部结构和动作原理的研究，并具有对电脑及通讯相当实力的人们的称呼，但是，90年初开始专门指那些非法入侵他人电脑并对其内部文件进行武断阅览，变更，破坏的入侵者。最近，黑客也用于对那些在以Internet为主舞台的假想空间上能够进行许多犯罪活动的有很大潜力的人们的通称。

Back Door

这是利用被系统设计者或管理者故意留下来的系统保安上的漏洞，入侵到应用程序或操作系统里的程序代码。即Back Door可使人们不通过对用户的认证等正常手续而能够接近应用程序或系统。留下保安上的漏洞并非都是恶意的。根据情况，以现场服务技术人员或负责系统供给者的维护人员使用为目的，可以把允许一些特殊标识的程序代码编写到操作系统或应用程序里。当进行调试（Debuging）时，利用Back Door可缩短认证及设置时间。但是，这些Back Door如果被不良编程员利用或开发结束之后未删除的Back Door被其他用户发现时，将会引起非常严重的后果。

逻辑炸弹

将隐蔽的逻辑单元加入到正常程序里，当满足逻辑条件时，就会执行逻辑单元内的指令。例如，按指定时间改变电脑计算利息的方法或利率，并把余额存进恶意行为者的银行账户里即属此类。又如，在一定条件下，删除电脑运行所必需的基本文件使电脑停止运作，或当在互联网上与自己有敌对关系的用户使用电脑时，删除他的电脑里的所有文件等。

背洞（Back Orifice: 简称BO）

背洞是美国叫做‘Cult of Dead Cow（对死牛的崇拜：简称cDc）’的黑客集团制作并发行的程序，是利用Internet（TCP/IP）遥控对方电脑的黑客工具。

使用背洞可远距离控制电脑文件，并且比电脑用户具有更多的权限，因此需要特别注意。此外，它不仅操作文件（文件删除，复制,移动，寻找文件或子目录，子目录生成，删除，文件压缩和解压缩等）或得到系统情报，而且

可以偷窥用户输入的内容或密码并将它储存以后转移到黑客电脑里。它还能重新启动被遥控电脑。

背洞虽然不像病毒具有自我复制能力，但如果不注意会引起很大损失。为此，在V3系列品把它分类为特洛伊木马（称为‘Back Orifice Trojan’）进行查杀。

伪病毒

用实际上不存在的病毒或特洛伊木马程序进行警告，并使他人把收到的信件尽量多地传送给别人的一种‘幸运信件’式的愚弄信件（Hoax）。信件的内容大体上类似于如收到特定题目的信件，系统的所有内容就会被删除等的威胁性内容。例如千万不能读以“Returned or Unable to Deliver”，“Penpal Greetings！”为题目的信件等等。这些信件引用许多技术用语，写的有板有眼，但充其量不过是儿戏。因此，收到此类信件时，可直接删除。

蠕虫（Worm）

这是对电脑里的其它系统不引起直接危害，但在许可范围内不断进行自我复制的程序代码。

其中典型的有HLLC.AIDS_II，HLLC.Even_Beeper，HLLC.Laufwerk。最近出现了利用Internet 电子邮件传播自己的新型网络蠕虫（I-Worm），引起人们的关注。执行网络蠕虫程序，不象其它蠕虫或病毒传播到其它文件夹或文件里，而是利用Internet 电子邮件把自己传播出去，因此其危害性是相当严重的。

Possible病毒

在有些主板上，若要进行低级格式化或硬盘就会出现“possible virus”信息。这是因为在CMOS设置时，把有关“Boot sector virus protection”的选项设置为Enable。此选项是当病毒入侵到引导扇区时提供给用户的警告用选项，因此有外部因素若要变更引导扇区就会告知用户。把此选项设置为'Disable'或'Normal'，就不再出现此信息。

Excel 宏病毒

这是利用Excel程序里的巨集（宏）功能制作的感染Excel文件的病毒。典型的有Laroux，Excel宏.Extras和Excel97宏.VCX，Excel 宏.Compat等。

Word 宏病毒

这是感染MS Word文件的病毒。属于此类的Word97宏.CLASS病毒使用了多样性和隐蔽手法，并在Word作业结束时显示信息。

Windows病毒

这是基于Windows操作系统的病毒。除了1992年第一次发现的Windows病毒 - WinVir以外，Boza，Tentacle，Marburg，CIH病毒也属于此类。

Windows病毒比DOS病毒更难医治。在Windows环境下，对正在执行的被感染文件无法进行治疗，只有关闭程序以后才可进行安全治疗。

黑客版本（Hacking Version）

黑客版本是指那些制作者（社）从来没有制作的程序或计算机指令。黑客版本会用删除程序，硬盘格式化等非正常运行给用户带来危害。为了不使V3系列受到黑客版本的侵害，请务必确认以下事项。

只能在各通讯网（Chollian，Nownuri，Hitel，Unitel）上的研究所专栏资料室里进行下载。如果有比公开资料室里的非登记版V3更高版本的V3，则此V3软件是黑客版本。

除了PKZIP以外，请不要使用用RAR或ARJ等压缩工具压缩的V3+。

对PKZIP文件进行解压缩时，请确认随着-AV检查，是否在最后一行出现以下信息，如果不出现，请不要使用该V3软件。同时请把该文件的出处举报给安研究所。（注：用WINZIP解压缩则不会出现此信息。）

“Authentic files Verified! # SUR710

Dr.Ahn’s Anti-Virus Laboratories，Inc.”

FAQ（常见问答）

Q ***1. 使用V3Pro 2000 Deluxe时，选择“无法治疗时删除”选项后，被删除的文件是否留在拉圾箱里？***

A 选择“无法治疗时删除”选项后，被删除的文件不留在拉圾箱里而是被彻底删除。有时候，通过此选项被删除后还留有文件名。这是因为要删除的文件正在使用中或有密码，此时文件无法还原。如果留有备份文件，请利用此文件进行治疗后再使用。

Q ***2. 在V3Pro 2000 Deluxe的快捷检查条里直接输入文件夹名进行检查时，无法正常进行检查。***

A 请确认输入格式是否正确。在输入快捷检查条时，区分文件夹的记号是空格。输入几个文件夹时也用空格来区分。对于长的文件夹名或含有空格的文件夹名，利用“ ”来区分。（参考：对象文件夹并不包括子文件夹。若要包括，请利用/s选项进行设置。）

Q ***3. 现正在使用V3Pro 2000 Deluxe正版软件。除此软件以外还有加入某网络程序会员后无偿下载的V3+ Neo。请问应使用那套程序，应怎样使用？***

A V3+ Neo为DOS用防毒工具软件。V3Pro 2000 Deluxe正版软件内包括DOS用V3+ Neo登记版，因此用户只要使用正版发行软件即可。在网络下载的V3+ Neo是共享软件，与正版相比较缺少一些网络驱动器诊断功能和巨集(Macro)病毒治疗功能等部分功能。

Q ***4. 把V3Pro 2000 Deluxe光盘插入驱动器后不能正常进行自动安装。光盘含有AUTORUN.INF文件，但为什么不能自动安装呢？***

A V3Pro 2000 Deluxe具有自动安装功能，即AUTORUN功能。如果无法执行AUTORUN，请确认以下事项。在Windows窗口上，点击我的电脑后按一下鼠标右键。然后依次点击属性→设备管理器→CDROM，在此可看到设置了的驱动器名。双击该驱动器名后再次点击属性→设置菜单，确认“自动插入通告”功能是否被激活。如果没有，任何CD-ROM，包括V3Pro 2000 Deluxe在内，都无法执行AUTORUN。选择“自动插入通告”功能选项以后重新启动电脑，就可正常执行AUTORUN。此外，如果不愿使用AUTORUN，请在按<Shift>键的同时插入CD-ROM即可。

Q ***5. 执行工具→Neo搜寻，进行病毒检查后，无法回到Windows窗口。***

A 这是因为为了Neo搜寻而暂时使用的autoexec.bat和autoold.bat两个文件互相反复执行而引起的。开机以后，请在执行Neo搜寻之前按<Ctrl-C>键或<Ctrl-Break>键，不让BAT文件执行，然后把autoexec.bat和autoold.bat两个文件改名或储存到其它文件夹后删除，即可正常开机。

6. 引擎升级时，显示“没有安装V3产品”的信息。

执行引擎升级时，有时候在V3引擎升级窗口上会显示“没有安装V3产品”的信息。这是因为含有用户及防毒工具路径等信息的C:\V3AHN.CFG文件被删除或内部受损，使得引擎升级无法执行而造成的。确认方法是：执行V3Pro 2000 Deluxe，选择帮助→V3Pro 2000 Deluxe信息(A)...，就会在显示用户和产品序号的位置上显示文件受损的信息。如果利用Windows的删除(UnInstall)功能无法删除已安装的防毒工具，就得以手动方式把安装有防毒工具软件的文件夹删除，并重新新进行安装。

7. 利用V3+ Neo解毒时，显示“无法进行写盘操作”的错误信息，并且无法进行治疗。

Windows 98/95系统被引导型病毒感染时，欲用V3+系列进行解毒就会出现此信息。这是因为Windows 98/95系统本身管理开机领域的数码而引起的，并因此导致无法正常治疗。此时，请用没有被引导型病毒感染的干净的DOS版本6.2以下的启动盘进行引导并重新启动之后再行治疗。

8. 系统基本内存容量不等于640Kbyte，是否说明已被引导型病毒感染？

一般情况下，电脑的基本内存容量等于640Kbyte。被引导型病毒感染时，大部分情形下基本内存容量会变小。但是，没有被引导型病毒感染，其基本内存的容量也有不等于640Kbyte的情况。一些使用AMI BIOS的电脑的基本内存容量是639Kbyte，还有许多奔腾PCI机种的基本内存是637Kbyte。此外，根据Windows环境的不同，其基本内存容量也会发生变化。

9. V3BACKUP.EXE的用途是什么？

V3BACKUP.EXE文件是可以用来简单采集引导区样本的工具。一般情况下，电脑的基本内存不等于640Kbyte，许多人就怀疑是否被引导型病毒感染。其实，有一个简单的方法可以确认是否被感染 - 即用干净的软盘启动后比较一下基本内存容量。如果相同，就可安心使用。如果不相同，就有被病毒感染的嫌疑。此时，请使用V3BACKUP.EXE，把启动领域里的数码编成文件后传送给安研究所。执行方法是指定驱动器并执行V3BACKUP.EXE即可，（如：V3BACKUP c:），可在执行了V3BACKUP.EXE的文件夹里发现生成的以下文件。

- MBS.V3 - 硬盘主引导区
- DBS.V3 - 硬盘DOS引导区
- FBS.V3 - 软盘引导区

如果疑心硬盘引导区被感染，可把MBS.V3和DBS.V3传送给安研究所；如果是软盘引导区，则传送FBS.V3。

10. 怎样治疗宏病毒（也称巨集病毒，Macro Virus）？

在全世界范围内陆续发现利用MS公司办公程序里的宏功能而制造的宏病毒。到目前为止，已发现2000多种此类病毒，并且估计其将继续增多。已被发现的大部分宏病毒是Word宏病毒和Excel宏病毒两类，估计将来会出现更多的变形病毒。被宏病毒感染时，把相应宏命令删除，就可能完成杀毒。但如内存也被感染且未进行杀毒，或继续共享被感染文件时，病毒继续扩散的可能性是相当大的。

Q ***11. 病毒名称以数字形式出现，这是为什么？***

A 利用V3系列产品检测病毒时有时会出现这种现象。这是因为安装了V3系列产品的文件夹里或执行V3.EXE文件的磁盘里没有V3WARPN.V3D文件而引起的。有些人在磁盘里只复制DOS用程序V3.EXE即付使用，而这是错误的。一定要同时复制V3WARPN.V3D，V3WARPD.V3D，V3WARPA.V3等文件才可正常使用。

Q ***12. 设置V3Pro 2000 Deluxe时制作了SOS盘。而用这张软盘启动他人PC时发生了异常。***

A SOS软盘含有制作SOS盘的PC硬盘信息。当发生无法认知硬盘的紧急状况时，此SOS盘可供启动使用。为此，在SOS盘上一定要进行写保护。用SOS软盘启动他人PC时，若执行V3RESCUE.EXE，则此SOS盘内的本人系统的硬盘引导区数码会自动复制到他人硬盘上，造成他人PC的引导区数码变更，此种情况下他人PC有可能无法正常启动。

Q ***13. 被Back Orifice Trojan病毒感染时，无法治疗。***

A 象Back Orifice Trojan一样，病毒名称里含有Trojan的病毒是不感染其它文件的。它是只引起妨碍用户作业等问题的特洛伊木马程序。为了防止因此种程序引起的损害，可用V3系列产品对此程序进行检测删除。此外，以HLLC打头的产卵型病毒也不感染其它文件，因此发现此类病毒时可以直接删除以进行杀毒。

关于 DOS 用 V3+ Neo

构成

V3+ Neo内含有V3.EXE，V3BACKUP.EXE程序。V3.EXE是对于到目前为止在国内发现的电脑病毒的查/杀程序，V3BACKUP.EXE是用来采集被引导型病毒感染的引导区样品的工具。

V3.EXE 的使用方法

基本使用方法

V3.EXE是对国内外电脑病毒的诊断/治疗用程序。例如，若要检查C驱动器，在DOS提示符下，按以下方法输入即可。

C:\>V3

选项的选择（OPTION）

执行V3.EXE时可用的选项如下。

V3[驱动器][路径][文件][选项]

(选项) /L 使用语言

/L:E 英语

/L:K1 组合型韩语

/L:K2 完成型韩语

/F 检查多张软盘

/S 检查子目录

/A 检查所有文件

/U 自动杀毒

/? 显示使用法

不使用任何选项或只使用/？选项时，一般在进行对内存的查/杀了和自我检测/治疗后，显示使用格式。只指定了驱动器时，先执行对内存的检查/治疗和自我检测/治疗。如果所选的驱动器是软盘，检查引导区；如果是硬盘，则检查主引导区和DOS引导区。并在此后检查所有目录内的可执行文件。

指定了路径名(path name)时检查其目录内的可执行文件。路径名可以是包括主目录的完整路径，也可以是以当前子目录为基准的相对路径。

指定文件名时，只检查该文件。文件名及扩展名中可以使用“？”或“*”标识。

V3BACKUP.EXE 的使用方法

关于采集引导型病毒

V3BACKUP.EXE可用来进行磁盘信息备份及引导型病毒采集。被新的引导型病毒感染时，请先用干净的软盘启动后，再用V3BACKUP.EXE把被感染的引导区烈军属成文件，并把此文件传送给安哲洙研究所。

即使没有被感染，也可用V3BACKUP.EXE把引导区备份焉，以供日后还原引导区时使用。

使用方法

在DOS提示符状态下，按以下方法输入，就可将指定驱动器(A:，B:，C:)的主引导区及DOS引导区编成文件储存在当前目录里。

C:\>V3BACKUP C:

执行V3BACKUP.EXE时，可供使用的选项只有/？选项。没有指定驱动器或选择/？选项时，显示使用格式。如要采集引导区，一定要指定相关驱动器。所采集的文件按以下文件名存入磁盘。

- 软盘引导区： FBS.V3
- 硬盘主引导区：MBS.V3
- 硬盘DOS引导区：DBS.V3

此外，指定RAM驱动器、光盘驱动器，网络驱动器等无法启动的驱动器时，会显示故障信息，并且不会生成文件。

안철수컴퓨터바이러스연구소
DR.AHN'S ANTI-VIRUS LABORATORIES, INC.

安哲洙计算机病毒研究所进行对杀毒、防火墙、有害信息防护网等软件产品的开发及销售，并开展对计算机相关犯罪的预防、打击及与保安有关的宣传活动。