
DIY
实战
系统恢复
实战手册
数位文化 编著
掌握系统恢复，尽在本书
丰富的病毒检验方法
最强的系统恢复功能
最佳的硬盘数据备份方法
8
中国铁道出版社
CHINA RAILWAY PUBLISHING HOUSE

# 系统恢复

# 实战手册

数位文化　编著

中国铁道出版社
2002年·北京

（京）新登字 063 号

北京市版权局著作权合同登记号：01-2001- 5293 号

## 版 权 声 明



**图书在版编目（CIP）数据**

系统恢复实战手册/数位文化 编著 －北京：中国铁道出版社，2002.1
ISBN 7-113-04501-4
Ⅰ.系… Ⅱ.数… Ⅲ.计算机病毒－防治－手册 Ⅳ.TP309.5-62

中国版本图书馆 CIP 数据核字(2001)第 096764 号

书　　名：系统恢复实战手册
作　　者：数位文化
出版发行：中国铁道出版社（100054，北京市宣武区右安门西街 8 号）
策划编辑：苏　茜　郭毅鹏
特邀编辑：徐煜东
封面设计：孙天昭　杨铭
印　　刷：北京市燕山印刷厂
开　　本：787×1092　1/18　印张：22.5　字数：452 千
版　　本：2002 年 1 月第 1 版　2002 年 1 月第 1 次印刷
印　　数：1～5000 册
书　　号：ISBN 7-113-04501-4/TP・662
定　　价：31.00 元

# 出版说明

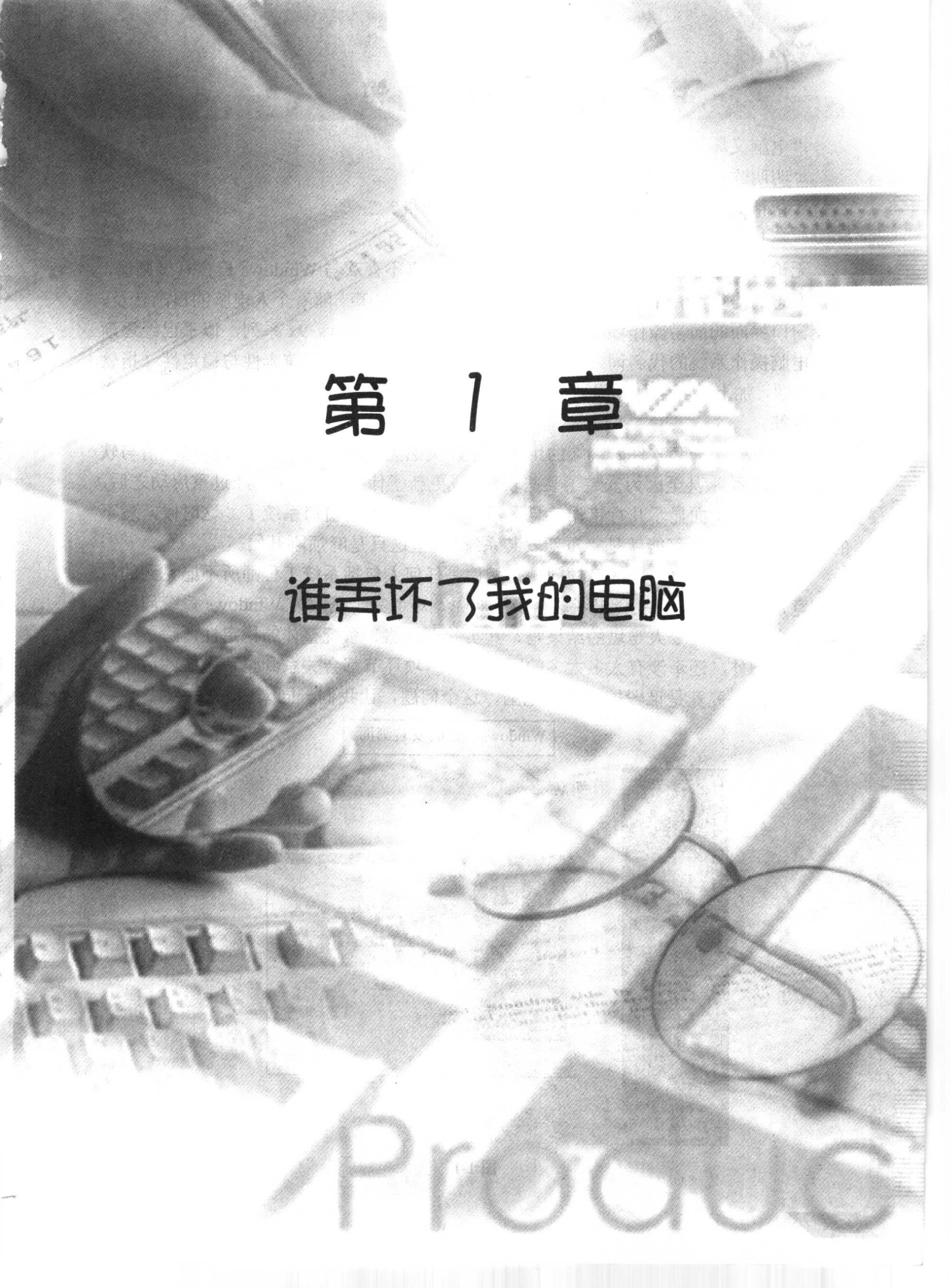
本书以病毒入侵电脑作为切入点，介绍与剖析了电脑病毒到底是什么东西？并且说明如何防止病毒入侵，以及在电脑中建立一个完整的防护网，杜绝电脑病毒上身。

各种系统备份的技巧，全部都在本书中有完整的介绍，不用担心漏失了什么数据，无论何时何地，您大可以放心地进行电脑重新安装的工作。安装系统其实相当简单，从硬盘的分区、格式化，到 Windows 系统的安装，以一个完整的流程进行介绍。就算是新手，也可以随着书中的步骤独立进行操作，马上成为人人口中的“电脑高手”。

本书由第三波电脑图书股份有限公司提供版权，经中国铁道出版社计算机图书项目中心审选，张瀚文、李自运、马超、陈贤淑、汤小伟、廖康良等同志完成了本书的整稿及编排工作。

2002 年 1 月

# 目　录



# 第 1 章

## 谁弄坏了我的电脑

“电脑又坏了!!!”

“明明昨天还好好的，怎么今天无法开机？”

“帮帮忙？！Windows 重启了一百多次还死机？”

“咦！蓝蓝的天～白白的字～死机画面又出来了...”

无论与手边那台电脑的关系密不密切，无论喜不喜欢与 Windows 日夜耳鬓厮磨，这样熟悉的语句，相信是每一个电脑玩家都曾有过的心声。随着个人电脑的日渐普及，以及窗口界面的简易操作环境的推广，Microsoft 的 Windows 9x 系列，似乎已经逐渐成为电脑操作系统的代名词。只是由于系统内部（指硬件）的兼容性与稳定性（指软件）问题，加上外界各种因素的干扰，使得操作系统经常无故“抛锚”，不免让用户伤透了脑筋。

有些时候，一套软件好端端的用到一半，突然无故地关闭，接着告诉您“请与软件供应商联系”；甚至因为安装了某些软件，或更新了什么系统软件，经过重启动之后，便直接在屏幕上面显示几行错误信息，然后就再也进不去窗口系统了。这时候，剩下的惟一解决途径，可能就是“重新安装系统”，但这只是麻烦刚开始。

一次又一次反复出现的麻烦问题，相信是任何人包括系统工程师所不愿见到的，但究竟是什么原因，系统会出现这么多毛病呢？难道完全是因为 Windows 系统问题太多，才会造成这样令人难堪的结果吗？其实并不尽然！系统整体的稳定性，除了本身软件的影响外，还牵涉有太多太多的因素，每一项环节都会关系到整个系统的运作与流程。因此，究竟是谁毁掉了您的电脑，这个问题，让我们一同来深入探究！

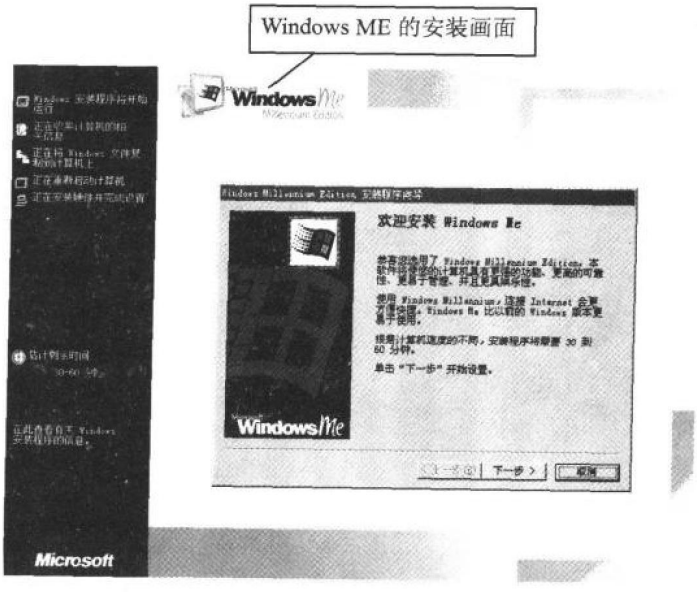



图 1-1

**补充说明**

*Windows 9x 系列*

Windows 系统可区分为 Win9x 与 WinNT 系列，9x 系列则泛指 Windows 95、95OSR2、98、98SE、ME 这些版本；不过 ME 是 9x 系列的最终版本，因为微软合并 9x 与 NT 成为新一代的“Windows XP”。

## 1-1 不听话的 Windows 系统

还记得在 Microsoft Windows 系列前期的 95 版本面市后，因为极度的不稳定引起了很多的争议，这个话题一直喧扰不下。当时有一位专业老师曾经跟课下的学生说过这么一段话，“Windows 95 为什么要叫 95，不是因为它在 1995 年出版的，而是平均每隔 95 天就必须要重新安装一次而得名……”，依此类推，升级到 98 大概也就只能多撑三天？这个说法或许稍嫌夸张，不过想来这确实是许多电脑用户的共同心声，因为在实际操作过程中间，会碰到的形形色色问题，并不亚于“到底是先有鸡或先有蛋”之类的争论。在这里列举出一些在 Windows ME 系统（如图 1-1）当中经常会出现的典型现象。

### 程序发生错误

别的暂且不谈，“程序发生错误”的信息（如图 1-2），相信使用过 Windows 9x 的人一定不陌生，或许当中所出现的文字随着版本和发生的状况而有所不同，但相同的结局是，在这个画面出现之后，很可能之前正在辛苦进行的文件数据突然消失不见，这样的惨痛经验，相信令很多人难忘。

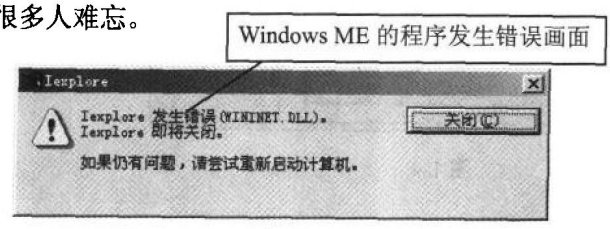



图 1-2

### 蓝屏死机 BSOD ( Blue Screen of Death )

讲到蓝屏死机（如图 1-3），可能有人尚未反应过来这是什么东西。如果换一种讲法，这就是 Windows 死机时出现的“蓝底白字”画面，大概就无人不知无人不晓。当系统负荷超重，或是过多的程序执行错误造成系统资源混乱时，这个经典画面就会登

场和您打招呼。一般来说，碰上这个画面时，通常就表示情况已经不太妙了。

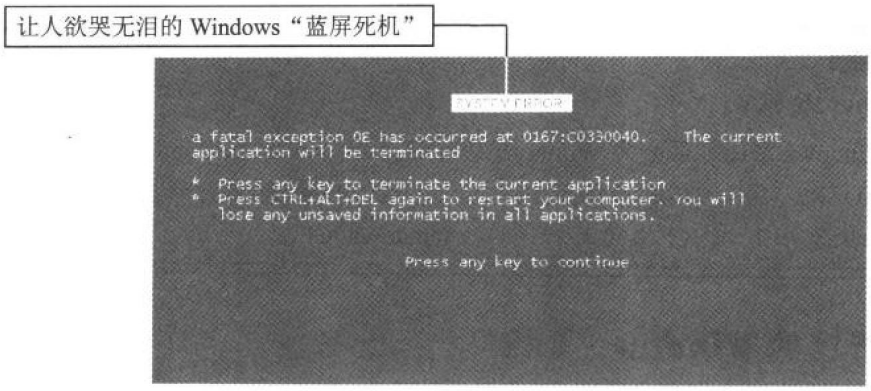



图 1-3

## 注册表错误

如图 1-4 所示。

注册表在 Windows 当中占有很重要的地位，它记录着每个程序安装的相关信息，以及系统软硬件组件设置，少了它电脑根本就成了一堆废物的组合而已。但由于整个系统的核心部分都在这里，若是发生错误时，小则出现错误信息，大则造成系统崩溃。Windows 98/ME 系统当中提供了“系统注册表检查程序”的功能，可以进行登录文件的维护与备份，但是当整个系统登录已经严重错乱时，可能依旧是“孤臣无力可回天”的悲惨下场。

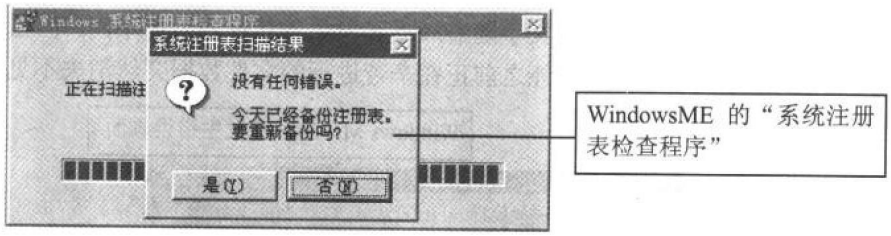



图 1-4

## 1-1-1 系统不稳定的原因

您可能会埋怨 Microsoft 搞出了一套不够稳定的操作系统，其实反过来想，同样一套 Windows 系统就能用得很方便的大有人在，甚至一两年都不需要重新安装，难道人家买的 Windows 比较好吗？当然不可能！所以除了系统本身的问题以外，应该定下心想一想，自己在操作上是不是出了什么问题，否则为什么自己的 Windows 永远都这么不听话呢？

因此这里整理出除系统本身之外，容易造成的不稳定的一些因素：

## 用户操作不当与电脑放置环境不佳

用户在操作上若没有良好的习惯，或是使用电脑的地方环境不佳，这些状况都会对电脑产生相当程度的伤害。比如“不按照正常方式关机”、“在使用过程中移动电脑”、“在电脑周围吃东西”等，这些或许不过是一些细微的小操作，短时间内也感觉不出来有什么影响，但长期来看，对电脑的运作以及系统的稳定性所造成的影响却远远超乎我们预料之外。

## 缺乏系统维护的工作

车子跑久了，都需要回厂维修。同样的道理，电脑使用久了，也需要通过一些工具软件来进行维护保养的工作，这样才能够加强系统的稳定性并修补漏洞。这些日常的保养，或许看似多余，实际上却是非常重要。电脑系统的毁坏，通常不会是一朝一夕所造成，通常这些漏洞往往是一点一滴地累积而扩大，直到破坏到某一程度，最后阻碍系统运作甚至死机，此时再做任何抢救的操作，往往都已经太迟了。

## 安装过多的软件

由于 Windows 系列的高度普及性，从商用软件、文书工具一直到游戏软件，几乎所有类型的工作都会开发可供 Windows 平台使用的软件。虽然如此，若是在同一系统当中安装了过多的软件，将会极度加重系统的负荷。增加了系统的负担、降低系统处理性能，严重者甚至让系统内部错乱而造成系统崩溃。因此，依据本身需求安装真正常用的软件，对于系统的稳定性会有不小的帮助。

## 硬件故障

电脑死机，并不见得全是软件方面的责任，硬件上发生问题的机率其实也相当高。一般而言，CPU 产生问题的几率并不高；通常内存（RAM）和主板（MainBoard）较可能是造成系统不稳定的主要原因。当这些组件成为故障的祸源时，便会影响到整台电脑的运作，进而造成系统极度不稳定。另外，当硬盘出现坏道时，对系统而言也是极大的伤害，甚至可能连文件都会损坏，因此对于硬盘的保护绝对是非常重要的。

## 硬件系统超频

许多玩家喜欢利用超频来满足追求速度的快感，但是超频过后并不一定会令人心满意足，因为它对系统的稳定性而言绝对是个极大的威胁。这样的做法对于硬件来说容易造成过大的负荷，让系统温度不正常升高而无法正确地进行处理操作，做出错误的响应造成系统死机。一般并不建议大家去作这种尝试，因为 CPU 在出厂之前，便已测试出该组件的最佳运作时间，若是通过超频方式去增强它的性能，会造成系统因高

温而导致的不稳定，就是其加速的必然代价。

在这里，大概将可能造成系统不稳定的致命杀手列出来，让大家有所警惕；后面的章节，还会更深入地去探讨关于各类与系统稳定相关的使用习惯与概念。

## 1-1-2 黑客入侵

在这个信息快速膨胀的时代，要保持电脑系统的稳定性，除了自己要多加维护之外，更要提防外界的潜在威胁。一些不断通过网络进行破坏，以及窃取他人电脑文件的有心人士，很可能正蠢蠢欲动的准备下一拨的攻击行动，下手的目标或许就是您的电脑。他们就是我们所俗称的——“网络黑客”（Hacker）。

其实说到所谓的“黑客”，必须跟大家澄清一个概念：真正的黑客是一群进行创造与解决问题的人，至于那些在网络上搞破坏与窃取他人文件行径的这些不速之客，并不是真正的“Hacker”，充其量他们只能够称之为“刽客”或“怪客”（Cracker）。但是由于一般人都已经接受了入侵者就等于“黑客”的说法，所以我们也不做太多的解释，在此仅以简单的一句定义来区分两者的差异性：

- **黑客（Hacker）：**

  黑客是有益的，他们创造东西、解决问题，并以共享的态度分享出他们所作的一切研究内容。

- **刽客（Cracker）：**

  刽客是有害的，他们破坏系统、入侵电脑，实际上并没有太大的贡献。

如果您有兴趣深入了解“黑客”与“刽客”的来源与关系，可以参考相关的黑客书籍。在这边提到这个内容，只是希望大家能够得到正确的概念。不过为了符合一般大众的习惯，在本书中我们还是继续使用“黑客”的字眼。

回到主题来，由于 Windows 9x 系列的安全防护问题与漏洞，通过网络，黑客可以很轻易入侵他人的电脑，并进行窃取文件或破坏系统的工作。最常见的做法，就是在被入侵的电脑当中植入“病毒”或“特洛依木马”程序，通过这些程序，进行远程破坏或远程遥控等的操作，换句话说，他们就像是接管了该台电脑一般，可以任意地寄信、散播病毒，想想这样的行为会有多么可怕的后果？

黑客使用“病毒”与“特洛依木马”程序有各自不同的目的，这里分别来做个简单的说明：

- **病毒（Virus）：**

  相信大家对“电脑病毒”这个名词应该并不会陌生，甚至很多人都会“闻毒色变”。病毒的基本功能，不外乎就是破坏电脑文件、瘫痪系统运作与占用网络资源。许多黑客将自己所制作的病毒程序通过网络传递出去，进而破坏他人电脑系统，造

成极大的恐慌。他们的原意各不相同，有些是想要证明自己的实力，有些则是要陷害某些特定对象，或是要将自己的观点想法通过这种方式传递出去。

**特洛依木马（Trojan Horse）：**

木马程序这个名词的由来，取材自古代著名的“木马屠城记”故事。其主要的特性，就是会一声不响的偷偷潜入被黑者的电脑，作为黑客远程操纵的遥控工具。通过木马程序，黑客可以任意进行“远程遥控”、“窃取密码”、“修改系统”等不法勾当－此时自己的电脑成为黑客手下的待宰羔羊，真令人极度的不舒服。

## 1-2 浩劫下的最后抢救

“天有不测风云，电脑也有旦夕祸福”，如果真的那么不幸，电脑遭遇到黑客攻击或系统毁坏的悲惨浩劫时，千万不要气得无所适从。别忘了，我们辛苦搜集建立的文件全部都在硬盘里面，学校的报告、公司的文件....怎么能就这样付诸流水呢？当然不行！所以就算遇到了再大的麻烦，都要把握住最后仅存的一线生机，对电脑系统做最后的抢救工作！

问题是，面对一个几乎崩溃的系统，要如何进行文件抢救与系统恢复的工作呢？废话不多说，先来了解一些抢救的基本措施。

### 1-2-1 培养备份文件的习惯

文件备份的工作，在一般人来说，或许会觉得是多此一举。但是当系统崩溃时，这些备份的文件，将可能会成为救命仙丹。因为在遭遇问题的情况下，并不能保证系统能够支撑到做完文件保存操作，或许中途就死机了，那岂不就等于宣告死刑了吗？所以在平时若能培养这种正确的习惯，就不需要等到没救时再来后悔。

至于备份，一般而言可以通过下面几种方法来完成：

**备份至“其他分区”：**

在一台电脑中，可能只有安装一个硬盘，但是在硬盘当中或许会有许多的磁盘分区，比如说有C盘、D盘、E盘等。一般系统的文件都是放置在C盘，因此可以另外使用D、E或是其他的分区，做文件备份的空间。

**备份至“其他硬盘”：**

备份到其他分区其实有小小的缺点，若是该硬盘发生故障或存在坏道时，可能整个硬盘都会无法使用，那么就算存有备份的文件内容也是枉然。能够同时安装多个硬盘，便可以将备份文件保存到其他硬盘，以作为紧急抢救之用。

**备份至“光盘”：**

在刻录机愈来愈普及的今日，利用光盘做文件备份操作，也是非常不错的选择，

不但保存容易，而且文件不易损坏，惟一的缺点就是文件写入后便不能修改。因此若要进行长期性的备份，会花费较高的成本。

## 1-2-2 重建家园的途径

当我们面对混乱不堪的系统时，当然不免会怅然所失。毕竟辛苦维护的系统，就这样被破坏或消失了，心中当然会有所不甘。其实，要重建那个属于我们自己的的系统家园，只要通过正确的恢复方式，便可以很快速地完成。当然，这必须建立在平时有做好的文件备份的 前提下。

要进行系统的恢复工作，基本上依照情形可分为下面几种途径：

### 系统未完全崩溃

在系统只是小型错误需要修正的情况下，其实不需要将整个系统做重新安装的操作，只要对必须修正的部分做还原工作即可。如此一来，不但可以确保文件的完整性，还可维持个性化的操作环境。

**使用“系统还原”工具：**

如果系统是在安装完某些软件后，发生注册表错误而系统死机的情形，这时便可使用 Windows ME 所提供的“系统还原”功能，将之前所记录的系统状态还原，如此便可恢复到未安装该软件之前的系统状态，如图 1-5 所示。

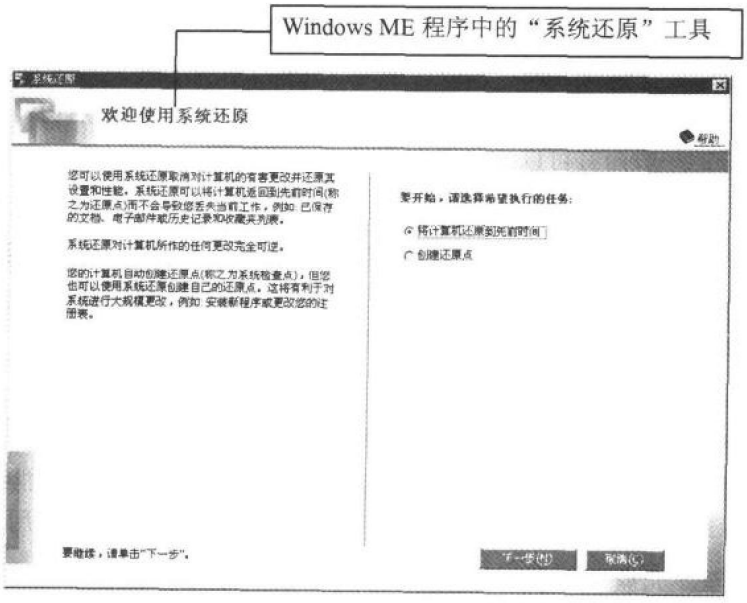



图 1-5