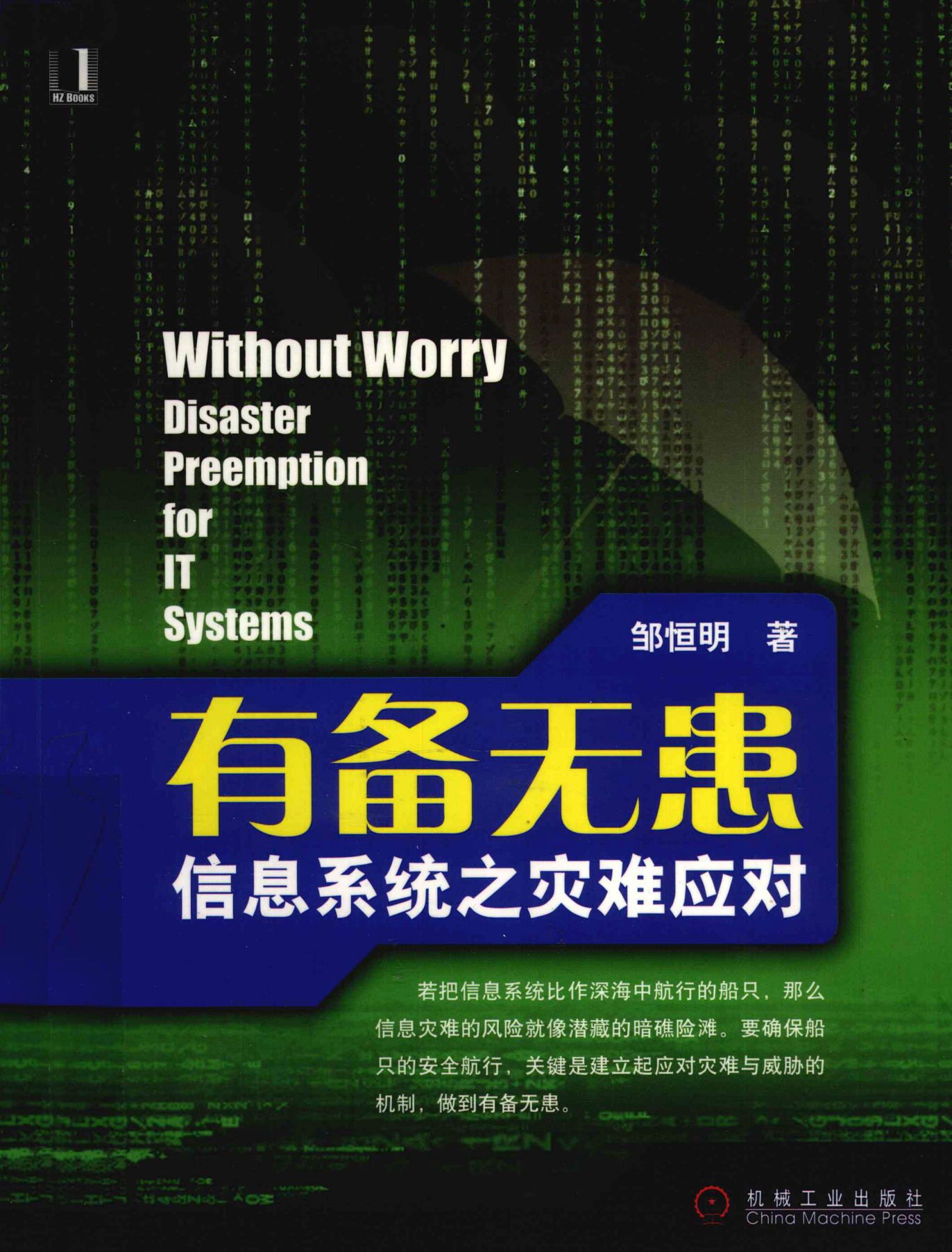

HZ BOOKS
Without Worry
Disaster
Preemption
for
IT
Systems
邹恒明 著
有备无患
信息系统之灾难应对
若把信息系统比作深海中航行的船只，那么信息灾难的风险就像潜藏的暗礁险滩。要确保船只的安全航行，关键是建立起应对灾难与威胁的机制，做到有备无患。
机械工业出版社
China Machine Press


Without Worry
Disaster
Preemption
for
IT
Systems
邹恒明 著
有备无患
信息系统之灾难应对
机械工业出版社
China Machine Press

本书从多个层面对信息灾难的应对理论、技术、手段和工业实践进行讲解，帮助读者揭开信息灾难应对技术与规划的神秘面纱。本书在技术方面的内容包括数据容灾、系统容灾、数据备份、灾难恢复、灾难防止、灾难恢复、灾难锁定、灾难的无害遽止、灾难虚拟化和信息盾等；规划方面的内容包括信息资产分类、信息风险识别、风险分析、灾难恢复战略、数据恢复策略、系统恢复战略、终端用户恢复策略和应急决策。同时，本书对工业界的灾难恢复实践进行了较为系统的论述，内容涵盖智能存储系统、存储架构、光纤协议、CRC 校验、分布式数据库技术、业务连续性解决方案、各种灾难恢复解决方案和灾难恢复技术与产品的主要提供商简介。

本书可以作为设计与维护各种信息系统的技术和管理人员的参考资料。



**图书在版编目（CIP）数据**

有备无患：信息系统之灾难应对/邹恒明著. —北京：机械工业出版社，2009.1

ISBN 978-7-111-25214-6

Ⅰ.有…　Ⅱ.邹…　Ⅲ.信息系统－安全技术　Ⅳ.TP309

中国版本图书馆 CIP 数据核字(2008)第 192344 号

机械工业出版社（北京市西城区百万庄大街 22 号　邮政编码　100037）

责任编辑：王　璐

北京牛山世兴印刷厂印刷

2009 年 1 月第 1 版第 1 次印刷

186mm×240mm · 16 印张

标准书号：ISBN　978-7-111-25214-6

定价：39.00 元

凡购本书，如有倒页、脱页、缺页，由本社发行部调换

本社购书热线：(010) 68326294

*In Pursuit of Absolute Simplicity* 求于至简，归于永恒

# 致　　谢

本书的成书离不开很多人的支持。感谢跟随笔者进行研究的上海交通大学高可靠实验室的人员，他们的部分工作在本书中得到了反映；感谢上海交通大学的尤晋元教授和傅育熙教授，他们对本人的工作给予了多方面的支持；感谢美国 EMC 公司同仁 Dan Arnon、Yuval Ofek 和 Kevin McCarthy，他们对本作者进行的远程数据复制和灾难恢复架构工作提供了很多支持与帮助；感谢密歇根大学(University of Michigan-Ann Arbor)的 Farnam Jahanian 教授，笔者是在其指导下才开始了数据和系统复制的研究。

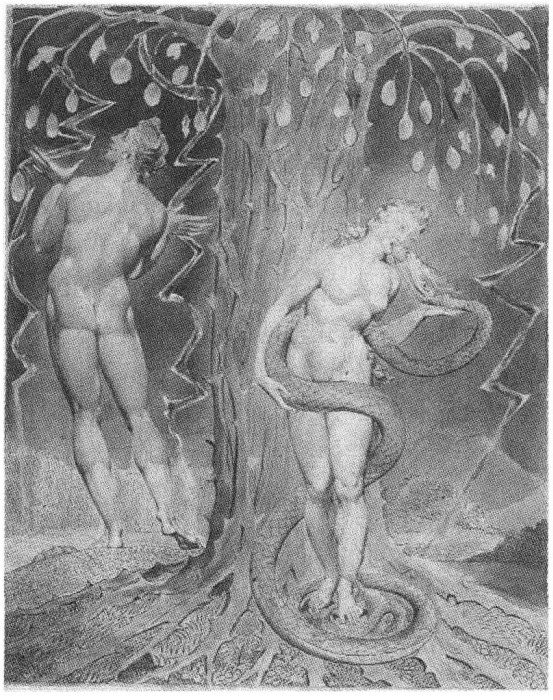
笔者要感谢自己的家人：夫人蕾蕾，女儿雨洁、雨蓉、雨恒和雨宜，她们的持久忍耐和不懈奉献，才使得本人有时间完成本书。

当然，最重要的是，感谢上帝！

# PREFACE 前言

2008年初春，一场历史上规模罕见的冰雪灾害突然席卷了中国南方，造成南方多个省市大面积电力中断，京广线铁路行车瘫痪，京珠高速公路南段全面封闭，数百万铁路公路旅客滞留广州、衡阳等地，成百上千个航班停飞，许多城市陷入一片冰冷与黑暗之中，受灾城市的很多市民靠吃方便面和盒饭度日。此次灾难的受灾总人数约为1.1亿。雪灾给中国南方乃至全国的经济、社会和人民生活造成了严重的影响。此次冰雪灾害持续时间之久、破坏范围之广、受灾人数之多、对各种城市基础设施破坏之严重，前所未有。

无独有偶，冰雪灾害后不久，2008年5月12日下午2点28分，一场几十年不遇的8.0级强烈地震撼动了四川汶川地区，全国20多个省市有明显震感，震区的许多房屋倒塌，地震夺去了近7万人的生命。在社会各界关注震区人民生命和财产损失时，却鲜有人注意到位于灾区的重要机构的信息系统均遭摧毁，其造成的损失将是难以弥补的。



夏娃听从蛇的唆使吃下禁果

蛇对女人说，神岂是真的说，不许你们吃园中所有树上的果子吗？

女人对蛇说，园中树上的果子，我们可以吃，惟有园当中那棵树上的果子，神曾说，你们不可吃，也不可摸，免得你们死。

蛇对女人说，你们不一定死，因为神知道，你们吃的日子眼睛就明亮了，你们便如神能知道善恶。

于是女人见那棵树的果子好作食物，也悦人的眼目，且是可喜爱的，能使人有智慧，就摘下果子来吃了。又给她丈夫，她丈夫也吃了。

——摘自《圣经·旧约·创世纪》

自从亚当和夏娃听从撒旦的挑唆，违背神的旨意偷吃禁果后，灾难便来到世界上，贪婪、嫉恨、饥饿、疾病、杀戮等各种灾难一直与人类为伴。为了应对这些灾难，人类进行了不遗余力的探索和努力。从某种程度上说，人类在创造历史的过程中一直与灾难进行着抗争。为了应对疾病这一灾难，人类研究出医学；为了应对饥饿这一灾难，人类发明了狩猎、耕种和食物保存的技术；为了应对自相残杀这个灾难，人类设立了政府、国家、法律等机制；为了应对贪婪和嫉恨，人类制定了各种道德规范；为了应对战争这个灾难，人类成立了联合国和各种和平协作组织；为了应对环境破坏的灾难，人类又建立了各种国际组织并缔结了各种国际公约。

然而，不管人类如何尽力，灾难却始终无法从人类的生活中根除，灾难随着人类生活方式的每一次变迁而变迁。每次人类认为消除了一种灾难时，新的灾难随即降临。人类克服了饥饿和贫穷的灾难，却带来了环境恶化的灾难；人类发明了信息技术，给人类的生活带来了意义深远的变化，但灾难也再次蜕变，化作各种各样的信息灾难如病毒和攻击，继续困扰着人类。由于对外围物质条件的极度依赖，信息时代的人类已经变得更加脆弱。人类生活对信息技术和信息系统的依赖是如此之强，一场重大的信息灾难很有可能将整个人类社会退步几十年，甚至改变人类的思维方式和生活哲学。

随着时间推移，除非人类对物质享受的追求发生重大改变，人类对信息技术的依赖将与日俱增，直至人的生命直接与信息技术相连。就像风靡全世界、拥有数百万参与者的游戏《第二生命》(Second Life)中所演示的，人的第二生命就在信息系统的虚拟世界里面。对于某些游戏玩家来说，这个虚拟的游戏世界甚至是他们的第一生命，这些玩家的收入、地位和荣誉都来自于位于美国加利福尼亚州的数千台服务器和存储器系统。因此，保障人类赖以生存和繁荣的信息基础平稳运行是一件十分重要的事情，这一重要性无论如何强调都不过分。如何保障人类的信息系统在天灾和人祸的打击下平滑运转是摆在各个国际组织、国家、政府、机构、企业、学校，甚至个人面前的严峻挑战。

本书就是从这个角度出发，试图对信息系统的灾难应对这个课题进行技术上的探讨。撰写这本书对作者来说既是一种探索，也是一种超越。

探索指的是市场上类似的书籍数量稀少，虽然市场上包含有“灾难恢复”4个字的书有近十种，这些书的一个共同特点就是，从国外引进，内容着重从商业化的角度进行灾难恢复规划，如智能存储系统、数据镜像技术、主动复制技术、分布式容灾技术、系统容灾技术、光纤协议网、系统转出与转入技术等并无论及。国外情况也类似，虽然有一些零零碎碎的灾难恢复网络论坛，但看不到系统性讨论灾难应对基础和技术等方面的书籍或资料。

因此，撰写本书没有现成模板可以套用，也没有一个行业标准来规范。虽然信息工业界发

表过数据备份、灾难恢复方面的白皮书、最佳实施方案等文档，但本书并不是一本介绍最佳实施方案的技术报告，在内容上与这些白皮书等存在很大区别。因此，撰写本书是本作者的一次探索，能否被读者接受尚需要时间的检验。

超越指的是本作者知识水平有限、经验有限，因此，对于本人来说，撰写本书着实是一个巨大的挑战，也是对本人学识和认知的一种超越。

本书旨在抛砖引玉，以作者的一家之言，探讨信息灾难的来源、影响和应对。从多个层面对信息灾难的应对理论、技术、手段和工业实践进行讲解，帮助读者揭开信息灾难应对技术和手段的神秘面纱。本书从信息灾难的来源与定义开始讲起，在解释了数据容灾、备份、镜像、复制这些基础知识后，再阐述灾难恢复的技术、架构和规划。技术方面的内容包括数据容灾、系统容灾、数据备份、灾难恢复、灾难防止、灾难的自动恢复、灾难锁定、灾难的无害遽止、灾难虚拟化和信息盾技术。规划方面的内容包括信息资产分类、信息风险识别、风险分析、灾难恢复战略、数据恢复策略、系统恢复战略、终端用户恢复策略和应急决策。同时，本书对信息工业界的灾难恢复实践进行了较为系统的论述，内容涵盖智能存储系统、存储架构、光纤协议、CRC校验、分布式数据库技术、业务连续性解决方案、各种灾难恢复解决方案和灾难恢复技术与产品的主要提供商简介。

本书共分5篇13章。5篇分别为背景篇、基础篇、技术篇、规划篇和高级篇。13章分别为灾难应对背景、容灾的基本概念、数据容灾技术、系统容灾技术、分布式数据库容灾技术、数据备份与数据恢复、灾难恢复技术、存储系统架构、灾难恢复规划、灾难恢复解决方案、灾难恢复案例分析、灾难应对的最新发展趋势和结语。具体内容简介如下。

## 背景篇

背景篇包括灾难应对背景和容灾的基本概念两个部分。第1章灾难应对背景部分的内容包括全球信息化浪潮、灾难的内涵与外延、天灾和人为灾难的介绍、灾难损失分析、灾难实例举证、灾难的变化趋势和灾难虚拟化趋势。第2章容灾的基本概念探讨缺陷、错误、系统失效、系统失效描述、系统可用性和灾难应对级别等。

## 基础篇

本篇包括数据容灾技术、系统容灾技术和分布式数据库容灾技术三个部分。第3章数据容灾技术的内容包括容灾机理简介、主动容灾技术、数据编码技术、CRC校验技术、RAID技术和数据镜像技术。第4章系统容灾技术的内容包括时空冗余技术、分布处理技术、分布式操作系统、系统防卫技术、设备保护策略、系统复制技术和复合复制技术。第5章分布式数据库容灾技术的内容包括分布式数据库概览、分布式数据库容灾机理、分布式数据库战略、分布式数据库选择策略、数据分配策略、分布式数据库架构、分布式管理系统和分布式数据库历史等。

## 技术篇

技术篇包括数据备份与数据恢复、灾难恢复技术和存储系统架构三个部分。第6章数据备份技术的内容包括主动和被动备份、在线和离线备份、实时和延时备份、等分和差分备份、增量备份技术、分裂和并列备份、差分增量备份技术、近程与远程备份、磁带和磁盘备份技术、数据恢复技术、数据取证技术，并选取了一个数据备份实例——安全自备份数据存储系统来进行分析。第7章灾难恢复技术的内容包括灾难恢复的历史、数据镜像技术、系统恢复技术、灾难恢复过程、网络和用户恢复技术、数据迁移技术和灾难恢复技术实例分析，这里列举的是EMC Celerra灾难恢复技术。第8章存储系统架构的内容包括内置式存储设备、直连式存储器、网络接入的存储器、智能存储设备、存储区域网、存储网络结构、NSA-SAN组合存储和灾难恢复的架构设计。

## 规划篇

规划篇包括灾难恢复规划和灾难恢复解决方案两个部分。第9章灾难恢复规划的内容包括灾难恢复规划的环境、灾难恢复规划的流程、灾难风险分析、信息生命周期、数据恢复规划、灾难恢复规范的策略、数据恢复策略、系统恢复策略、终端用户恢复策略、应急决策机制和规划的维护和测试。第10章灾难恢复解决方案的内容介绍了低端、中端、高端的灾难恢复方案，另外还介绍了全球主要灾难恢复方案供应商。

## 高级篇

高级篇包括案例分析和最新研究两个部分。第11章灾难恢复案例分析的内容包括某国际著名投资银行在9·11中的灾难恢复过程、某城市热线灾难恢复解决方案、某国有大型银行灾难恢复解决方案、某城市地铁X号线灾难恢复解决方案、某电信公司灾难恢复解决方案、某新闻社灾难恢复解决方案、某软件公司灾难恢复解决方案、某医院灾难恢复解决方案、某保险公司灾难恢复解决方案和某银行大火的灾难恢复过程。第12章灾难应对的最新趋势则对信息灾难应对的最新研究进行介绍，重点介绍了灾难防止技术、灾难的自动恢复技术、灾难锁定技术、灾难的无害遽止技术、灾难虚拟化技术、灾难堆积理论和信息盾技术。第13章是全书总结。

本书既可以为致力于信息灾难应对的研究人员提供有益的学术参考，又可以为有兴趣涉猎信息灾难应对的大学本科生或研究生打下知识基础；本书既可以成为设计、制定、实施和运行各种不同的信息灾难应对系统的人员的参考资料，也可以作为信息工业界的企业管理者在灾备中心建设和信息灾难应对建设方面的决策依据。

本书内容涵盖了传统的数据和系统容错，当前流行的数据备份、灾难恢复，灾难防止、无害遽止、差分增量合成与分解、信息盾技术工业实践与最新的研究。本书力求理论与技术并重，

现实与前沿齐举，规划与实践同步，通过讲原理、举实例、谈规划，将目前最佳的业界方案与将来的最新研究结合，希望读者在阅读完本书后，达到如下几个效果：

- 认识信息灾难威胁的严峻性。
- 掌握灾难应对的基本方法。
- 学会灾难风险分析与灾难恢复规划。
- 学会评估灾难恢复解决方案的优劣。
- 了解当前最新研究和业界动态。

需要指出的是，本书有许多概念和技术是第一次出现，有的技术还处于实验阶段，未投入实际应用。当然，本书的大部分内容描述的都是现实中可以使用的技术与方法。

本书力求覆盖本领域里的所有重要概念。限于本作者水平和阅历，书中错误及疏漏在所难免，有的论述或许会失之偏颇。当今的信息存储工业界和信息灾难恢复领域正处于迅速的变化和发展之中，对于不同的人许多概念、技术和手段可能意味着不同的东西，新概念、新技术、新方案、新标准随时有可能出现。因此本书的某些阐述不一定契合所有人的理解，而有的新概念在本书中也没有全部涵盖，恳请读者谅解。

最后，恳请学术界和工业界同行及各位读者不吝批评指正，本作者不胜感激。本作者的联系方式为：zou@ sjtu. edu. cn 或 zou@ umich. edu。

邹恒明

2008 年 4 月于上海莘庄

免责声明：

1. 本书中所表达的思想、理论或技术方案纯属作者个人观点，不代表上海交通大学、本书出版社或任何其他人员和机构的立场或观点。

2. 本书力求做到概念精确，技术方案可行。但本作者不保证书中列出的方案必能够直接应用到特定机构或企业的特定情形。如有使用本书中方案效果不彰者，本作者不负责任。

3. 书中所列出的公司名如 EMC、IBM、HP 等，产品名如 Symmetrix、Clariion、SureStore 等，皆属于相应公司所有，如 Symmetrix 属于 EMC 公司注册的产品商标。由于本书提到的公司及产品名称众多，在这里不一一列出。读者自可分辨。

4. 鉴于存储工业界和灾难恢复技术处于飞速的发展和变化时期，有些陈述无从考究是何人或何公司首先作出，因此无法注明出处，请谅解。如果读者知晓，请不吝告知。

5. 为将某些概念阐述清楚，本书列举了不少实例和案例。这些举例仅仅为了演示概念，不代表本书赞成或推荐这些系统、办法、模型或方案。

6. 为维护商业秘密，本书在保持完整性的前提下对很多案例进行了裁剪，望读者理解。

# 目 录 CONTENTS

## 第三篇 技术篇

## 第四篇 规划篇

CHAPTER 1

# 第 1 章　灾难应对背景

2002 年 6 月的一个午后，在太平洋深处的公海上，一个由航空母舰、导弹驱逐舰组成的联合编队正在进行演习。该演习将对安装在导弹驱逐舰上的 Agies 舰载区域导弹防卫系统进行测试。到下午两点时，一架从航空母舰起飞的战机径直向导弹驱逐舰飞来，这架战机很快就被驱逐舰的导弹防卫系统锁定，防卫系统按照演习计划成功加载了导弹，看上去一切都正常。正当演习人员以为演习已达到预期目的，宣布“演习成功”时，悲剧发生了：防卫系统没有遵从预定指令退出锁定和攻击模式，而是准备自行发射导弹攻击战机。这时舰上的工作人员施展了浑身解数，也无法取消导弹防卫系统的错误指令，只能眼睁睁地看着导弹向假想的敌机发射。驾驶“敌机”的飞行员不得不放弃价值昂贵的战机跳伞逃生。战机被击落坠毁，损失巨大(见图 1-1)。

图 1-1　由于软件锁定造成的导弹误发

事后，相关人员对事故进行了调查，得出的结论是“整个导弹防卫系统被锁仅仅源于系统控制软件的一个小小的设计失误”。此后设计人员对该部分重新进行了设计……

## 引子

如果上面的故事让我们觉得遥不可及，那么下面的事件则是和我们的生活息息相关了。

1995 年 12 月，美国航空公司(American Airlines)的一架喷气式客机在南美洲哥伦比亚的卡里(Cali)机场降落时不幸撞上山峰，造成机上 159 人全部遇难。通过事故后的调查发现，撞山原因是飞行管理软件系统运转不稳定，出现灾变，向飞行员提供了不实的、片面的甚至是相互冲突的信息，飞行员无法对这些信息作出正确判断，导致事故发生。

诸如此类的信息系统故障和灾难造成的物损人亡的事故数不胜数。随着信息系统的普及，信息化已成为必然的趋势，并深入生活的方方面面。大到与国家政府所需的飞船发射和国家防卫，中到与机构企业默契相连的电力调度、海关报单、电子商务和企业信息化，小到与普通大众日常生活休戚相关的交通管理、证券交易、银行服务和电子邮件，似乎一切都离不开信息技术。信息化浪潮的汹涌澎湃，在改变了我们过去的生活模式的同时，也造就了新的思维定式。

## 1.1 信息化浪潮的特点

回首过去，我们发现信息化浪潮具有许多鲜明的特点：一是数据量极大，且数据规模呈加速上升的趋势。1999 年美国 EMC 公司委托加州大学伯克利分校(UC-Berkeley)进行了一项人类数据量增长需求研究。该研究结果表明：自人类诞生以来到 1999 年为止，人类总共积累了大约 12EB 的数据量。而从 1999 年到 2002 年的三年间，人类积累的数据量就达到了 12EB。由此可见人类积累的数据量以惊人的速度急剧增长。

各种统计数据显示，大多数企业的数据年增长率为 70% ~ 100%。这些数据增长的来源包括数据拷贝、多媒体数据以及大型文件。被财富杂志评出的全球营销额处于前 1000 位的公司的数据库容量以 TB 计，而中等规模公司的数据库容量通常在 400 ~ 700GB 之间。

信息化浪潮的第二个特点是数据的种类不断增多。在古代和近代人类所积累的数据通常是文字和图像，而今天积累的数据种类还包括视频、音频等。如何对这些新型数据进行安全、高效和可靠的存放与处理是人类面临的新课题，也是信息技术所面临的更新、更复杂的挑战。

信息化浪潮的第三个特点是数据的存放分散。这里的分散存放不是分布式存放，而是没有关联的杂乱散布。由于计算机技术的普及，拥有计算机或信息系统的机构和个人越来越多，使得数据的产生源也变得越来越多。有统计表明，人类产生的数据中约 55% 保存在个人电脑里，而这些数据间不存在什么有机的联系。

信息化浪潮的第四个特点是越来越多的关键系统依赖信息技术的控制与支持。如现代武器系统大都需要计算机芯片和相应的软件来进行控制；交通控制、航空航天、宇宙探索和重症医疗监护等也依赖计算机及其软件来确保正常运行；电网调度基本上靠计算机控制来进行；银行