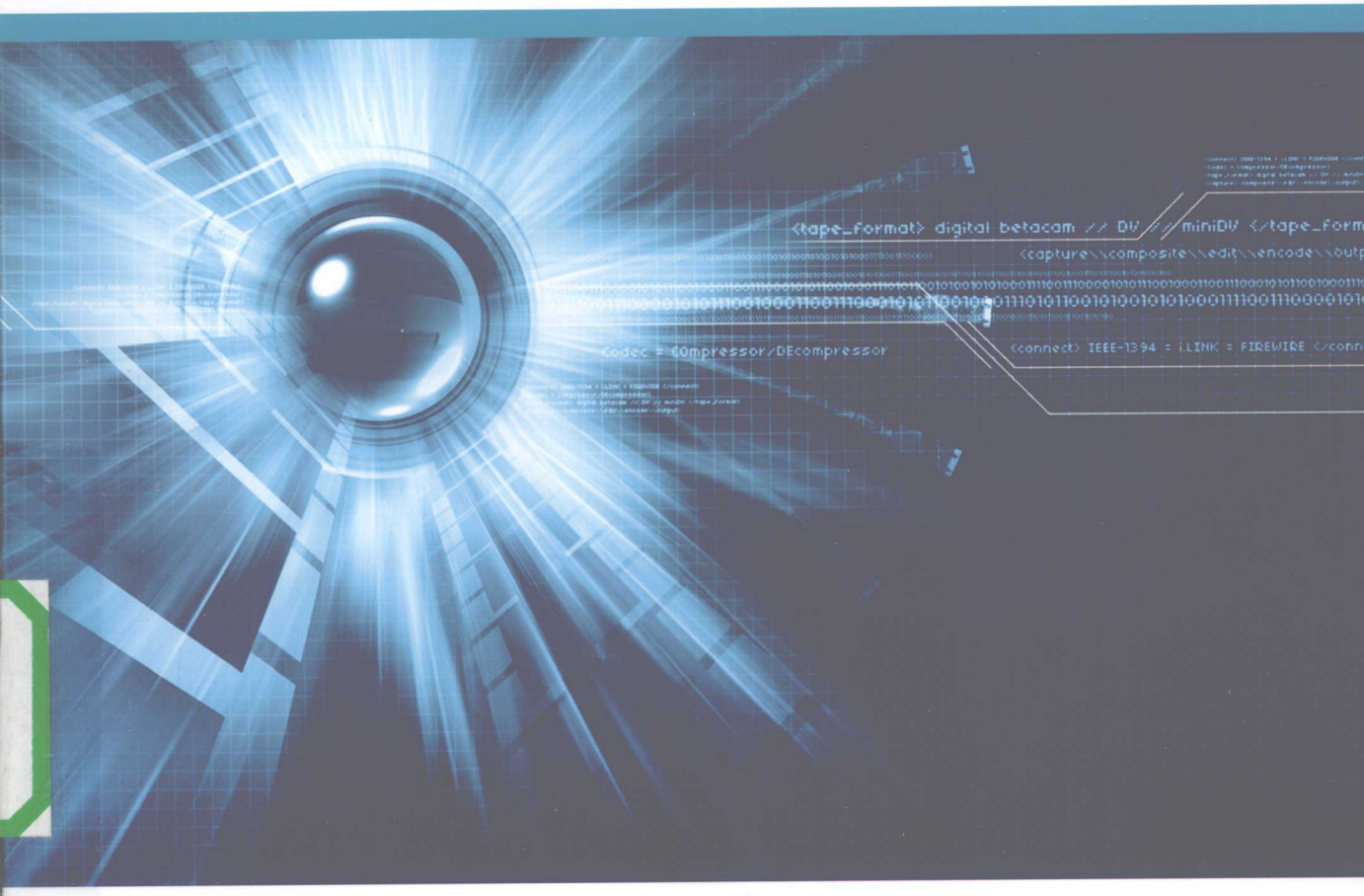
国家信息安全培训丛书

信息系统灾难恢复基础

中国信息安全测评中心　编著



航空工业出版社

国家信息安全培训丛书

信息系统灾难恢复基础

中国信息安全测评中心　编著

航空工业出版社

北京

内 容 提 要

随着信息化程度的增强，信息系统灾难带来的损失日益增大。减少信息系统灾难对社会的危害和人民财产带来的损失，保证信息系统所支持的的关键业务能在灾害发生后及时恢复并继续运作成为信息安全领域的重要研究方向。

本书系统地介绍了信息系统灾难恢复的发展过程、定义概念、标准法规和规划实施方法、步骤。本书共分为两个部分，第一部分介绍了信息灾难恢复的发展过程、相关标准法规；第二部分介绍了信息系统灾难恢复的组织管理、建设流程、需求确定、策略制定，以及灾难备份中心的建设等具体操作内容。

本书是中国信息安全测评中心注册信息安全专业人员（CISP）和注册信息安全员（CISM）的正式教材，可作为高等院校信息安全专业的教材，还可作为信息安全培训和从业人员的信息系统灾难恢复的参考用书。

图书在版编目（CIP）数据

信息系统灾难恢复基础/中国信息安全测评中心编著.
北京：航空工业出版社，2009.6
（国家信息安全培训丛书）
ISBN 978-7-80243-342-7

Ⅰ.信… Ⅱ.中… Ⅲ.信息系统—安全管理 Ⅳ.TP309

中国版本图书馆 CIP 数据核字（2009）第 089266 号

信息系统灾难恢复基础
Xinxi Xitong Zainan Huifu Jichu

航空工业出版社出版发行
（北京市安定门外小关东里 14 号 100029）
发行部电话：010-64815615 010-64978486
北京地质印刷厂印刷 全国各地新华书店经售
2009 年 6 月第 1 版 2009 年 6 月第 1 次印刷
开本：787×1092 1/16 印张：9.75 字数：241 千字
印数：1—5000 定价：29.00 元

国家信息安全培训丛书

序

世界正经历一场伟大的信息革命，信息成为一种重要的战略资源。它改变着人们的生活方式和工作方式，形成新的社会形态。

随着我国社会信息化进程的不断发展，计算机网络及信息系统在政府机构、企事业单位及社会团体的工作中发挥着越来越重要的作用。然而，信息化水平的提高在带来巨大发展机遇的同时也带来了严峻的挑战。由于信息系统是一个复杂巨系统，它存在着脆弱性，信息安全问题不断暴露。信息安全关系到国家的经济安全、政治安全、军事安全和文化安全。信息安全已经成为维护国家安全和社会稳定的一个重要因素。

当前，社会对信息安全专业人员的需求逐年增加。发展信息安全技术与产业，关键是人才。培养信息安全领域的专业人才，已成为当务之急。高素质的信息安全人才队伍是保障国家重点基础网络和重要系统安全的基石，是制定信息安全发展战略规划与政策并建设国家信息安全保障体系的骨干力量，是发展我国信息安全产业的排头兵。

目前我国的信息安全教育工作仍相对滞后，信息安全人才十分匮乏，社会需求与人才供给间还存在着很大差距。如何培养信息安全的专业人才，是我国目前面临的重要问题。

《国家信息安全培训丛书》力图涵盖信息安全知识体系的方方面面，蕴含了信息安全保障体系的各个组成部分，是一套很好的信息安全专业人员培训丛书。相信这套丛书的出版，将有利于信息安全专业人员的培养。

何德全

2009 年 5 月

《信息系统灾难恢复基础》编委会

目　录

第一部分　信息系统灾难恢复基础

第二部分 信息系统灾难恢复规划和实施

第一部分

信息系统灾难恢复基础

本部分包含以下章节：

第 1 章　信息系统灾难恢复综述

第 2 章　信息系统灾难恢复相关标准法规

第 1 章　信息系统灾难恢复综述

1.1　信息系统灾难恢复的历史和现状

1.1.1　国外灾难恢复的发展概况

灾难备份和恢复于 20 世纪 70 年代中期在美国起步，源于美国中西部地区对电脑设施进行的备份。灾难恢复行业的历史性标志是 1979 年在美国宾夕法尼亚州的费城（Philadelphia）建立了专业的商业化的灾难备份中心并对外提供服务。在这以后的 10 年里，美国的灾难恢复行业得到了迅猛发展，拥有超过 100 家灾难备份服务商。1989 年以后的 10 年中，灾难备份服务商之间进行了大规模的合并和重组，到 1999 年市场上只剩下 31 家灾难备份服务商，并以每年 15%的速度增长。

从 1982 年到 1998 年的 16 年间，灾难恢复预案经受了大型灾难的考验，业务连续规划（BCP）开始出现，美国灾难恢复行业成功地完成了 582 宗灾难恢复，平均每年约 40 宗。在这些灾难恢复中，44%的案例是由于发生了区域性的灾难使多个灾难备份服务客户同时受到影响，而从来没有出现客户因灾难备份中心资源不够而无法恢复的情况。灾难发生的原因最常见的是停电，其次是硬件损坏和火灾等。这 582 宗灾难分别由遍布全美的 25 个灾难备份中心进行了成功的恢复，灾难恢复服务商充分显示了其在提供专业可靠、低成本灾难备份与恢复服务方面的优势。

2005 年，美国德勤公司针对灾难恢复建设及其驱动力等方面，对 273 个机构（覆盖政府、银行、保险、制造、医疗保险、电力、通信、教育和零售业等）进行了调查，结果显示，建设灾难恢复系统的比例在不断增高，如表 1–1 所示。

表 1–1　美国灾难恢复建设情况

机构灾难恢复建设情况	2004 年	2005 年
全部或部分关键业务建立了灾难恢复系统的机构	74.4%	83.6%
全部关键业务建立了灾难恢复系统的机构	21.7%	41.8%

各机构开展灾难恢复建设的驱动力主要来自于确保业务的持续可用、法律法规的要求、机构决策层对风险管理的责任等。美国德勤公司 2005 年的调查数据如表图 1–1 所示。

9・11 事件后，Globe Continuity Inc. 对美国、英国、澳大利亚及加拿大共 565 个公司使用灾难备份中心的情况进行了调查，发现在拥有或租用了灾难备份中心的公司中，56%使用了商业化的灾难备份服务，29%使用自有的灾难备份中心，15%在商业化灾难备份服务的基础上同时拥有自己的备份设施。两项相加，使用灾难备份服务外包的比例达到了 71%。西方国家灾难恢复建设状况如图 1–2 所示。

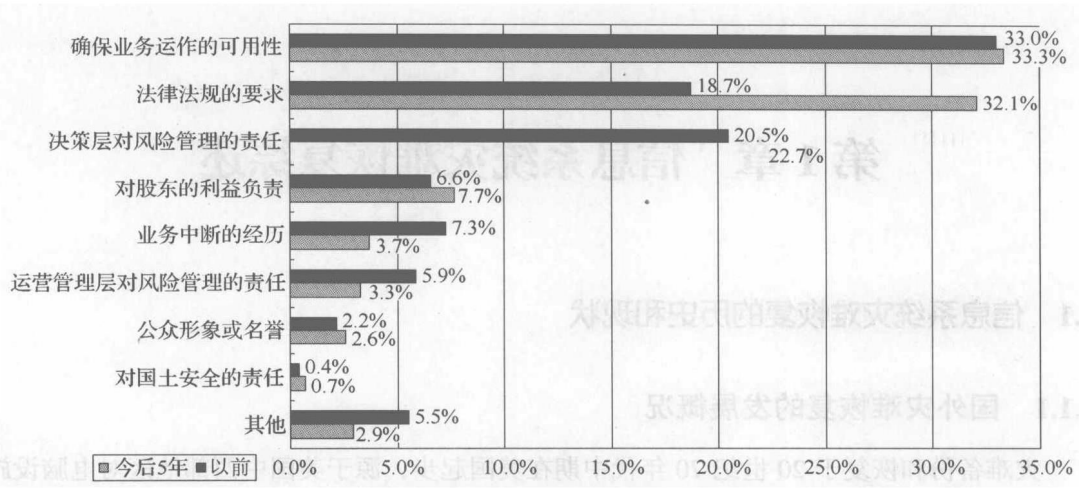


图 1-1　灾难恢复建设的驱动力

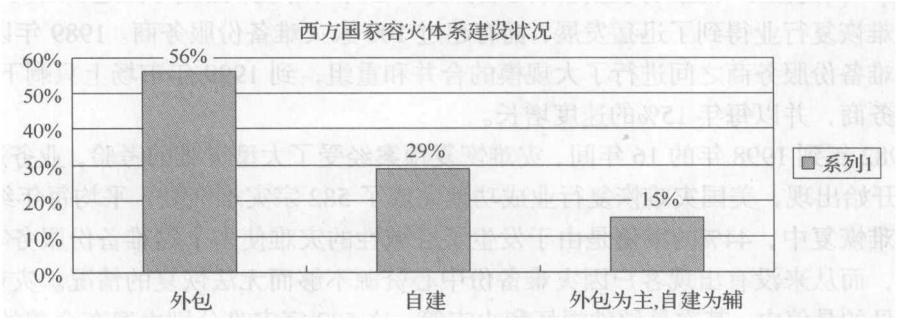


图 1-2　西方国家灾难恢复建设状况

2006 年，IDC 对 40 家企业的业务连续性和灾难备份情况进行抽样调查，其中，自建占 56.8%，外包占 43.2%。调查指出，从 2004 年到 2006 年，公司越来越认同在满足他们的可用性要求方面外包模式比自建模式更加安全可靠。IDC 在 2006 年的调查报告中还指出，2006 年灾难恢复外包建设模式的比例比 2004 年高出 30.5%；自建的成本是外包费用的 3.28 倍。

鉴于灾难恢复建设的重要性，美国、欧洲等西方国家的政府和行业主管部门就重要信息系统的灾难恢复建设制定了相应的监管措施来指导和规范行业的灾难恢复工作。尤其是 9・11 事件发生后，各国监管部门纷纷对其行业的抵抗灾难打击和保证连续运作的能力进行了重新评估，制定了新的规范、指引和工作文件。

从用户的行业划分来看，灾难恢复行业面向的主要客户还是金融业。事实上，有近一半的灾难备份中心是专门为金融行业服务的。据 CPR（Contingency Planning Research）估计，美国灾难恢复行业的年销售额中有 45%来自金融行业。

西方发达国家重要机构都在远离主数据中心的地方拥有一个灾难恢复系统，如美国的 Wells Fargo Bank、法国的法兰西银行、新加坡的 Citibank 等。对于信息系统依赖程度较高的公司往往需要拿出 IT 总预算的 7%～15%用于灾难恢复，每月要支付大约 5 万～10 万美

元的费用，大公司甚至达到每月100万美元。据Meta预测，在全球大公司中，用于业务连续计划的投入将会持续上升，到2007年，这笔投入将平均达到7%。

1.1.2　国内灾难恢复的发展概况

在国内，各行业用户对信息安全的建设越来越重视，其投入也呈现稳定增长的态势，但就单位信息化来说，大部分单位还没有有效的灾难恢复策略，没有建立统一的业务连续管理机制。

20世纪90年代末期，一些单位在信息化建设的同时，开始关注对数据安全的保护，进行数据的备份，但当时，不论从灾难恢复理论水平、重视程度、从业人员数量质量，还是技术水平方面都还很不成熟。

2000年，“千年虫”事件引发了国内对于信息系统灾难的第一次集体性关注，但9·11事件所带来的震动真正地引起了大家对灾难恢复的关注。随着国内信息化建设的不断完善、数据大集中的开展和国家对灾难恢复工作的高度重视，越来越多的单位和部门认识到灾难恢复的重要性和必要性，开展灾难恢复建设的时机已基本成熟。21世纪初，国内灾难恢复专业服务商的出现以及灾难恢复外包和咨询项目的开展标志着国内灾难恢复市场的起步。中国的灾难恢复建设在经历几年的探讨之后，正逐步进入实践阶段。

2003年，中共中央办公厅、国务院办公厅下发了《国家信息化领导小组关于加强信息安全保障工作的意见》，明确要求：各基础信息网络和重要信息系统建设要充分考虑抗毁性与灾难恢复，制定和不断完善信息安全应急处置预案。为贯彻落实中央的指示，国务院信息化工作办公室于2004年9月份下发了《关于做好重要信息系统灾难备份工作的通知》，文件强调了“统筹规划、资源共享、平战结合”的灾难备份工作原则。为进一步推动八个重点行业加快实施信息系统灾难恢复工作，国务院信息化工作办公室于2005年4月份下发了《重要信息系统灾难恢复指南》，文件指明了灾难恢复工作的流程、灾难备份中心的等级划分及灾难恢复预案的制定。2007年6月，《重要信息系统灾难恢复指南》经修订完善后正式升级为国家标准，国家质量监督检验检疫总局以国家标准的形式正式发布了《信息安全技术　信息系统灾难恢复规范》（GB/T 20988—2007），该标准于2007年11月正式实施。

北京、上海、深圳、广州和成都等城市都已出台或正在研究电子政务信息系统灾难恢复工作的意见和规划；中国人民银行发布了《中国人民银行关于加强银行数据集中安全工作的指导意见》、《关于进一步加强银行业金融机构信息安全保障工作的指导意见》；银监会发布了《关于印发〈银行业金融机构信息系统风险管理指引〉的通知》，以上文件明确要求银行必须建立相应的灾难备份中心，制定业务连续性计划。中国保险监督管理委员会出台了《加强保险信息安全保障工作的意见》、《关于做好保险业信息系统灾难备份工作的通知》和《保险业信息系统灾难恢复管理指引》（征求意见稿）。中国证券监督管理委员会下发了《关于进一步做好证券期货业信息安全保障工作的意见》和《关于印发〈证券期货业信息安全保障管理暂行办法〉的通知》等。

一些业务对信息化依赖程度极高的政府部门已着手本单位灾难恢复建设。国税总局、海关总署、中国人民银行、商务部等部委均已完成或正在建设灾难备份中心；北京、上海、深圳、广州、杭州等各地政府已建设或启动灾难备份中心建设。政府部门以自建为主，大部分采用了专业化灾难恢复/业务连续性咨询服务。

银行业灾难恢复建设起步早，各单位基本上建立了专门的灾难恢复组织机构，大部分国有银行和大中型商业银行都建设了同城或异地的灾难备份中心，正在实施或有未来 3 年内的异地或同城灾难备份中心建设规划。目前，自建和外包的建设模式并存。工商银行、农业银行、中国银行和建设银行四大国有商业银行以及交通银行、招商银行、兴业银行、民生银行和光大银行等股份制商业银行均采用或计划采用自建模式。国家开发银行选择了同城、远程灾难备份均采用外包模式，以降低管理复杂度，提高专业性。深圳发展银行、广东发展银行、中信银行、华夏银行等股份制商业银行均选择外包模式。

其他信息化程度较高的行业如保险、证券、电力、民航、电信、石化和钢铁等企业正在开展和规划灾难恢复系统的建设。

同时，国内的灾难恢复工作还存在一些问题。部分单位对灾难恢复建设的概念模糊，混淆了数据备份、灾难恢复和业务连续性的区别，存在侥幸心理，缺乏开展灾难恢复工作的积极性；在没有统筹规划的前提下各行业及地方自行建设灾难备份中心，必将产生重复建设的情况，造成社会经济资源的分散和浪费；从事灾难恢复建设和服务的企业良莠不齐，部分企业缺乏专业化能力，所提供的建设方案不能满足灾难恢复的要求，不具备保证灾难恢复和业务连续性能力；灾难备份中心应付灾难的能力必须通过不断的演练来提升和完善，目前已建成的灾难备份中心普遍缺乏严格的演练，灾难备份中心的运营缺乏有效的监管和审计，导致大量的灾难备份中心无法在灾难来临时有效发挥作用。

中国的信息化正逐步进入应用时代，数据量也迅速增长，存储数据的备份与灾难恢复的建设将成为信息化的核心，灾难恢复市场将进入加速发展期。赛迪顾问预测，在未来 3 年中预计灾难恢复市场规模将持续高速增长。来自 IDC 的最近调查结果也表明了这一趋势，在未来 5 年中，中国的灾难恢复业务将发展很快，其综合年增长率将达到 46%。

1.2 信息系统灾难恢复有关术语

1.2.1 灾难的定义

灾难是一种具有破坏性的突发事件，如图 1-3 所示。我们所关注的是灾难对单位的正常运营和社会的正常秩序造成的影响，其中最明显的影响是信息服务的中断和延迟，致使业务无法正常运营。信息系统停顿的时间越长，单位的信息化程度越高，损失就越大。

《信息安全技术　信息系统灾难恢复规范》（GB/T 20988—2007）将灾难定义为：由于人为或自然的原因，造成信息系统运行严重故障或瘫痪，使信息系统支持的业务功能停

顿或服务水平不可接受，通常导致信息系统需要切换到备用场地运行的突发事件。典型的灾难事件包括自然灾害，如火灾、洪水、地震、飓风、龙卷风和台风等，还有技术风险和提供给业务运营所需服务的中断，如设备故障、软件错误、通信网络中断和电力故障等；此外，人为的因素往往也会酿成大祸，如操作员错误、植入有害代码和恐怖袭击等。各事件造成的灾难统计数据比例如图 1–4 所示。

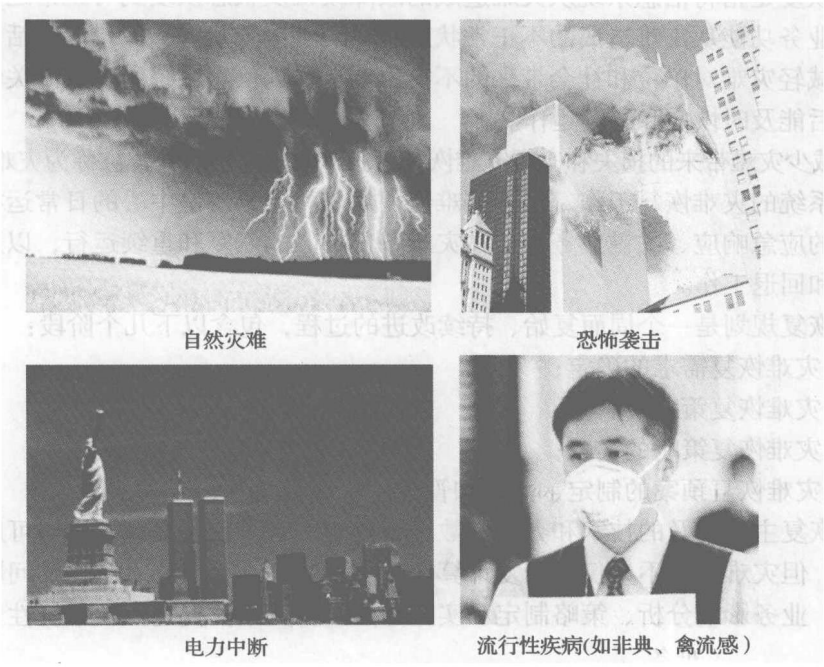


图 1–3　常见灾难图示

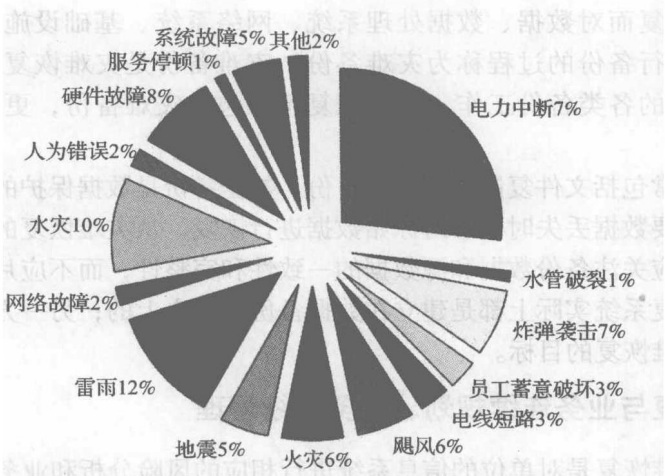


图 1–4　各事件造成的灾难统计数据比例示意图