信息系统

Disaster Recovery

灾难恢复的规划及实施

主编 王渝次
副主编 王秀 杨淑琴
执行主编 黄伟 熊四皓

北京交通大学出版社
http://press.bjtu.edu.cn

信息系统
灾难恢复
的规划及实施

主编　王渝次
副主编　王秀　杨淑琴
执行主编　黄伟　熊四皓

北京交通大学出版社
·北京·

内容简介

本书通过介绍信息系统灾难恢复的概念、意义和发展，灾难恢复的管理，需求分析，等级划分，策略的制定与实现，预案的制定、落实和管理，实施案例等内容，全面地阐述了信息系统灾难恢复建设和管理的科学体系和方法论。

本书内容符合中国的信息系统灾难恢复现状，具有丰富的内涵和原创性，实用性强，使读者能够通过书中的方法和步骤解决信息系统灾难恢复实际工作中的常见问题，真正有所收益。

本书由国家灾难恢复有关政策的起草者及具有丰富实践经验的灾难恢复专家共同编写。它适用于企事业单位的中高层管理人员、IT相关部门的技术人员，是从事灾难恢复领域的管理和技术人员的必备参考书，也可作为高等院校灾难恢复研究的参考文献。

图书在版编目（CIP）数据

信息系统灾难恢复的规划及实施／王渝次主编. — 北京：北京交通大学出版社，2006.7
ISBN 7-81082-823-1

Ⅰ.信… Ⅱ.王… Ⅲ.信息系统－安全管理 Ⅳ.TP309

中国版本图书馆CIP数据核字（2006）第072725号

责任编辑：井飞　　特邀编辑：张京满
出 版 者：北京交通大学出版社
　　北京市海淀区高梁桥斜街44号　　邮编：100044
印 刷 者：北京嘉业印刷厂
发 行 者：新华书店总店北京发行所
开　　本：787×1092　1/16　　印张：16　　字数：320千字
版　　次：2006年7月第1版　　2006年7月第1次印刷
书　　号：ISBN 7-81082-823-1/TP·292
印　　数：1～5000册　　定价：42.00元

本书如有质量问题，请向北京交通大学出版社质检组反映。
投诉电话：010-51686043；　E-mail：press@center.bjtu.edu.cn

《信息系统灾难恢复的规划及实施》

编 委 会

作者简介

王渝次

现任国务院信息化工作办公室网络与信息安全组组长。先后在中共中央办公厅、中央财经领导小组办公室工作，历任副处长、处长、副局长等职，参与多项重大政策问题调查与研究。1999年至2000年，任山东省威海市副市长。2001年以来，就职国务院信息化工作办公室，先后负责综合协调和网络与信息安全等方面的工作，参与组织中国国家信息安全战略与信息安全主要政策的研究和制定。

王秀

国家税务总局信息中心主任兼国家税务总局信息化工作办公室常务副主任。先后组织领导了税务信息系统一体化建设和金税工程（三期）总体设计工作，参与组织了税务系统南海灾备中心的筹备工作。

杨淑琴

博士研究生。1982年毕业于中国人民大学档案系计算机情报检索专业，1987—1989年在加拿大国家档案馆做访问学者，1992年受聘于中国证券市场研究设计中心，期间，以STAQ系统（法人股交易市场）软件开发组负责人身份设计开发了法人股在线交易、批处理清算过户系统。1992年至今，就职中国证监会。曾任办公厅计算机管理处、信息统计部计算机室、技术监管处处长，现任证监会信息中心副主任。

黄伟

万国数据服务有限公司（GDS）总裁。参与信息系统灾难恢复国家标准的制定工作。同时，作为国内第一家灾难恢复专业服务商的领导者，为国内灾难恢复外包服务树立了市场的典范和信心。

熊四皓

现任国务院信息化工作办公室网络与信息安全组处长。历任信息产业部电信管理局副处长、信息产业部电信研究院研究室主任等职。参与组织制定我国重要信息系统灾难恢复有关政策和标准。1993年毕业于清华大学物理系，获理学学士学位；2004年毕业于挪威管理学院，获管理学硕士学位。

李建彬

1992年毕业于清华大学计算机科学与技术系，中科院软件所客座研究员，1995年就职于国家税务总局信息中心至今。长期从事网络规划设计与工程实施和信息安全管理工作，参与信息系统灾难恢复国家标准的制定工作。

许强

先后毕业于北京理工大学计算机科学与工程系和清华大学经济管理学院。参与或主持设计开发若干管理信息系统，参与信息系统灾难恢复国家标准的制定工作，目前主要业务领域是信息安全保障工作的组织与协调。现就职于证监会信息中心。

郭全明

中国人民银行科技司计算机安全管理处处长，工学硕士。从事中国人民银行信息化建设和管理工作，曾承担人民银行金融信息管理中心机房改造、内联网防病毒、防火墙、网络改造、客户端管理、电子认证CA系统等工程建设工作，负责信息安全管理工作，组织实施风险评估、各项网络、信息安全规划、标准与制度建设，参与信息系统灾难恢复国家标准的制定工作，是《计算机世界》评选的2005年度十大“中国信息安全突出贡献奖”获奖者之一。

汪琪

万国数据服务有限公司（GDS）首席灾难恢复和业务连续性专家、咨询与方案总监，中国内地第一位获得DRI International “Certified Business Continuity Professional”认证的业务连续运作专家。负责若干中国银行业、证券业、保险业、基金业及地方政府灾难恢复和业务连续运作咨询和外包项目。信息系统灾难恢复国家标准的主要起草人之一。

刘东红

毕业于北京理工大学，获计算机应用技术专业工学硕士学位。曾负责或参与某省电力公司数据规划等若干重点信息化建设项目，参与信息系统灾难恢复国家标准的制定工作。曾任教于中国矿业大学，现就职于万国数据服务有限公司（GDS）。

康潭云

万国数据服务有限公司（GDS）高级灾难恢复和业务连续性顾问。深交所交易系统实时灾备技术顾问，中国建设银行业务连续性咨询项目负责人，信息系统灾难恢复国家标准的主要起草人之一。

曹铮

万国数据服务有限公司（GDS）高级灾难恢复和业务连续性顾问。多年业务连续领域工作经验，主要负责了深圳发展银行灾难备份系统的建设实施及其业务连续性计划的开发和维护管理工作，以及兴业银行和中国建设银行业务连续性规划咨询工作。

赵庆

1995年加入IBM中国有限公司，就职于全球信息科技服务部。2004年开始担任中国区业务连续和灾难恢复专业服务经理，专注于业务连续和灾难恢复服务产品线的管理，包括市场调研，产品的开发和推广，业务伙伴的开发和合作，市场推广活动，资源和技能的规划。

苏卓

就职于IBM全球信息科技服务部，资深信息系统架构师，负责IBM中国区大型或复杂信息系统的灾难恢复解决方案的规划及实施。

王迪

就职于IBM全球信息科技服务部市场部，负责部门的市场战略规划和相应项目的执行，以确保市场部能够提供部门业务增长所需要的动力。

周西柱

EMC公司中国区副总裁。全国青年科技工作者协会理事，中华全国青年联合会委员，中美商会会员。1990年毕业于清华大学。曾就职于中国电子工业部、Oracle中国公司。参与了金关工程、金税工程、金保工程、金盾工程、金质工程、新华社多媒体数据库、长安集团ERP等若干国家级重点信息化建设项目。

于希国

EMC公司中国区产品和解决方案市场经理，2001年加入EMC公司，先后负责中国区的技术支持、解决方案咨询、市场资讯等工作。曾就职于中国惠普有限公司及中国石油天然气股份有限公司，拥有扎实的理论知识和丰富的实践经验。

序言

随着国民经济和社会信息化的日益推进，网络与信息系统的基础性、全局性地位进一步增强，国民经济和社会发展对网络和信息系统的依赖性越来越紧密。尤其是银行、电力、铁路、民航、证券、保险、海关、税务等行业和部门的信息系统以及电子政务系统已经成为国家重要基础设施。这些信息系统的安全运行直接关系到国家安全和人民利益，更关系到社会的稳定。国内外一系列已经发生的事件表明，如果重要信息系统没有一定的灾难恢复能力，这些系统一旦发生重大事故或遭遇突发事件，不仅遭受无可挽回的经济损失，还将严重影响国民经济的发展和社会稳定。

国家高度重视重要信息系统的灾难备份和灾难恢复工作。2003年《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。

为落实国家信息化领导小组关于加强信息安全保障工作的要求，国务院信息办会同有关部门在大量调查研究的基础上，组织起草了《关于做好重要信息系统灾难备份工作的通知》，对做好国家重要信息系统灾难备份工作的目标、原则和近期任务提出了明确要求。

灾备工作在我国刚起步，一些重要信息系统主管部门和运行单位深感经验不足。2004年10月开始，国务院信息办组织有关单位起草了《重要信息系统灾难恢复指南》（以下简称《指南》）。《指南》的起草既参考了国际有关标准，又结合了我国信息化和信息安全保障的实际情况，其内容覆盖了灾难恢复工作的主要环节。目前，已将《指

南》印发给各基础信息网络和重要信息系统主管部门，供这些部门在开展相关工作中参考。

《指南》指明了做好信息系统灾难恢复工作的基本思路，具体工作的开展还涉及很多非常专业的细节问题。对灾备这项工作还有一个学习认识、结合实际深化提高的过程。《信息系统灾难恢复的规划及实施》围绕《指南》的流程进行编写，同时借鉴了国内外同行在这方面的成功经验，对有关技术和管理人员理解使用《指南》，掌握信息系统灾难恢复的基本知识和实施流程，能提供有益的帮助。希望通过该书的出版，促进我国的信息系统灾难恢复工作的科学开展，为提高我国信息安全保障水平做出贡献。

2006年5月于北京

前言

自从有了信息技术以来，信息系统面临的各种灾难和故障就从来没有停止过。随着信息系统的重要程度和关键性的提高，如何保障信息系统对关键应用的服务等级和服务品质，成为日益急需解决的问题，为此，灾难恢复工作已刻不容缓。信息系统灾难恢复的目的是提高信息系统抵御灾难和重大事故的能力，减少灾难打击和重大事故造成的损失，减轻对单位和社会带来的不良影响，保证信息系统所支持的关键业务功能在灾难发生后能及时恢复和继续运作。

“居安思危，思则有备，有备无患。”事实证明，各类灾难的到来通常具有突发性和偶然性，但只要能够进行行之有效的灾难恢复工作，就可以将损失降到最小。

随着科学技术的进步、经验的积累，信息系统灾难恢复的建设和管理已经形成了完整的科学体系和方法论。从探索和实践的过程中，我们也积累了一些国内灾难恢复工作的经验，逐步形成了完善的灾难恢复方法论。尤其是《重要信息系统灾难恢复指南》，它是对做好重要信息系统灾难恢复规划和准备工作的具体规范和指导，为科学实施信息系统灾难恢复提供指导性的流程和方法，对我国的灾难恢复工作具有很强的指导意义。

本书对《指南》的内容进行了解读和有益的补充，对相对成熟的理论和方法进行了全面的介绍。可以说，它是对我们开展灾难恢复工作具有较强指导性和可操作性的一本书。

本书的内容主要由以下九个部分组成。

1．信息系统灾难恢复的概念及意义：讲述了信息系统灾难恢复的基础知识和灾难恢复工作的意义。

2．信息系统灾难恢复的发展：讨论了国内外信息系统灾难恢复的发展概

况，包括国内外主管机构对灾难恢复的监管和灾难恢复、业务连续性标准组织或协会。

3．灾难恢复的管理：介绍了灾难恢复管理的目标、灾难恢复对组织机构的管理要求、灾难恢复的外部协助、IT管理与信息系统灾难恢复、灾难恢复建设的生命周期、灾难恢复建设的基本原则。

4．灾难恢复的需求分析：介绍了风险分析和业务影响分析的方法和内容，从而确定最终用户需求和灾难恢复目标。

5．灾难恢复等级的划分：对《指南》中规定的灾难恢复等级和要素做进一步的描述。

6.灾难恢复策略的制定：叙述了灾难恢复策略的内容、制定原则、成本效益模型、制定方法、制定过程以及必要的支持；同时，对灾难恢复系统的建设模式和灾难恢复服务提供商的选择等问题进行了探讨。

7．灾难恢复策略的实现：依据《指南》中的灾难恢复七要素，说明灾难恢复策略实现的具体内容和要求。

8．灾难恢复预案的制定、落实和管理：讨论灾难恢复预案的制定、落实和管理的过程和注意事项，以及灾难恢复预案的教育、培训和演练。

9．附录：包括《重要信息系统灾难恢复指南》的全文和国内典型的灾难恢复案例。

在本书的编写过程中，得到了许多“无名英雄”的大力支持和帮助，尤其是杨红、于健、高勇、顾海崖、顾宏伟等，在此对他们表示特别的感谢。

编者

2006年5月

目录

第1章

信息系统灾难恢复的概念及意义

“居安思危，思则有备，有备无患。”出自《春秋左传·襄公十一年》。

持续的提供产品和服务是单位存在的基础。单位通过提供持续的产品和服务获得持续盈利的能力，而为公众和特定人群提供特定的服务和支持也是其存在的必要性之一。随着社会的进步和科学技术的发展，单位的运作对信息系统的依赖性越来越大，而信息系统作为电子、信息产品，有其特有的脆弱性，在各种自然灾害和人为灾难面前难免会遭受到毁灭性的打击，进而直接影响产品服务的持续提供，对单位、社会生产环境、人民群众生命财产安全造成巨大的威胁。

本章主要讲述了信息系统灾难恢复的基础知识和灾难恢复工作的意义，对灾难、灾难恢复、灾难恢复规划、灾难备份、数据备份、业务连续规划和业务连续管理等主要概念进行了解释和比较分析，可使读者深入地了解灾难恢复的含义和目标，认识开展灾难恢复工作的必要性和重要性。

1.1 信息系统灾难恢复概述

1.1.1 灾难的定义

灾难是一种具有破坏性的突发事件，如图 1-1 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。