政务信息安全管理与应用丛书

政务信息系统灾难恢复实用技术

王宗君　侯海波　毛东军　等　编著

中国质检出版社
中国标准出版社

政务信息安全管理与应用丛书

政务信息系统灾难恢复实用技术

王宗君 侯海波 毛东军 赵章界 李颖涛 张 格
姚 东 龚伟兵 房孝强 李蒙生 张 勇 毛作奎 编著

中国质检出版社
中国标准出版社
北 京

内 容 提 要

本丛书从电子政务的固有特点出发，结合编者单位丰富的实践经验，围绕电子政务信息安全保障的重点领域，介绍了信息安全的实用技术方法。

本书为丛书的灾难恢复分册，对当前实用的灾难恢复技术做了完整、客观的介绍。在给出灾难恢复技术总体框架的基础上，对各种主流灾难恢复技术，包括其技术原理、技术过程、技术特点以及应用的最佳实践等做了详细的介绍。

本书可供各级政府以及安全服务机构、第三方测评机构从事信息化、网络与信息安全的管理和技术人员使用，也可供其他行业相关人员参考。

图书在版编目(CIP)数据

政务信息系统灾难恢复实用技术/王宗君等编著. —北京：中国标准出版社，2012

ISBN 978-7-5066-6644-2

Ⅰ. ①政… Ⅱ. ①王… Ⅲ. ①电子政务—管理信息系统—维护 Ⅳ. ①D035.1-39

中国版本图书馆 CIP 数据核字(2011)第 281480 号

中国质检出版社
中国标准出版社 出版发行

北京市朝阳区和平里西街甲 2 号(100013)
北京市西城区三里河北街 16 号(100045)

网址：www.spc.net.cn
总编室：(010)64275323 发行中心：(010)51780235
读者服务部：(010)68523946
中国标准出版社秦皇岛印刷厂印刷
各地新华书店经销

*

开本 787×1092 1/16 印张 11.5 字数 272 千字
2012 年 3 月第一版 2012 年 3 月第一次印刷

*

定价 **30.00** 元

丛书编委会

丛书序

中国正处在高速发展时期，随着人们生活水平的提高，社会对政府提出了越来越高的要求。利用信息技术对政府拥有的和需要的资源进行使用和管理，提高资源的使用效率和政府的办事效率，是建立服务型和经济型政府的必然选择。目前，我国大到中央政府，小到乡镇街道，都广泛开展了政府信息化应用，应用范围涵盖门户网站、日常行政办公系统、指挥调度系统、决策支持系统、行政审批系统以及网上报税等。这些信息化应用对促进政府职能转变、提高政府工作效率和办事水平、提供优质的政府服务等起到了非常重要的作用。

政府信息化带来巨大效益的同时，人口、交通、卫生、教育、税收、执法、统计等行政管理越来越依赖信息化手段，也使得政府掌握的各类资源面临着更多的威胁。这些威胁来自自然灾难和恶劣的自然环境、信息化设施设备和系统自身的故障以及人为的有意或无意的破坏等。对政府信息系统实施攻击的，不局限于个人，还包括具有强大攻击力的敌对势力，甚至敌对国家。另一方面，信息化应用天生就是不安全的，政府单位在建设信息系统时追求速度和节约成本的动力远远大于对安全的需求，这导致信息系统常常千疮百孔。两方面的因素结合起来，加上针对信息系统的攻击比传统攻击更加低廉和便捷，导致针对政府的信息安全攻击层出不穷。政府网站被黑，政府管理的公民隐私信息泄露，网上缴税系统瘫痪等，严重影响了政府的公信力和行政能力。

我国政府高度重视信息安全和保密工作。早在1994年，我国就发布了《中华人民共和国计算机信息系统安全保护条例》，对计算机信息系统安全等级保护、计算机信息系统安全专用产品销售等做出了具体规定。而2003年的《中共中央办公厅、国务院办公厅转发〈国家信息化领导小组关于加强信息安全保障

工作的意见〉的通知》(中办发[2003]27号)则对信息安全工作做出了全面部署。我国各级政府积极落实信息安全等级保护制度,开展网络信任、安全测评、安全预警、容灾备份、应急处置等工作,规范信息安全产品和服务的管理,加强信息安全和保密的监督检查。

作为我国首都,北京市积极贯彻落实国家信息安全和保密管理的政策法规和市委市政府领导的指示精神,努力把自身打造成信息安全一流的可信城市,保障首都安全,促进首都经济发展。北京高度重视信息安全工作的组织领导,成立了北京市网络与信息安全协调小组和北京市通信保障和信息安全应急指挥部;积极开展信息安全监督管理工作,进行多种形式的专项检查和联合检查;加强网络与信息安全应急体系建设,建立快速有效的分等级信息安全应急响应与处置机制;积极推进等级保护工作,加强信息系统建设方案的安全审查和建设完成后的安全测评与定级备案审查;加强基础设施建设,建立了北京市政务网络信任体系、北京市信息安全容灾备份中心、北京市通信保障和信息安全应急指挥平台、北京市政务信息安全监控预警系统等一批信息安全基础设施;完善信息安全法规政策和标准体系,发布了《北京市信息化促进条例》、《北京市公共服务网络与信息系统安全管理规定》等一系列政策法规和标准。北京在信息安全与保密管理方面取得了丰硕成果,为成功举办2008年奥运会与残奥会以及新中国成立60周年大庆做出了重要贡献。

本丛书总结了北京在信息安全基础设施建设和信息安全保障工作方面的理论研究成果和实践经验,希望能对未来北京市政务信息安全保障起到推动作用,同时也能对其他省市有参考和借鉴意义。

2011年11月

序

政务信息化是社会发展的必然趋势，当今我国各级党政机关都在使用现代信息技术进行办公、管理和为社会公众提供服务，信息化过程中产生的一些信息和信息系统已经成为党政机关至关重要的资产，一旦遭到破坏，将严重影响党政机关办事效率，甚至对公众利益和国家安全造成严重伤害。

近年来世界各地频繁发生的火灾、洪灾、地震、飓风、恐怖袭击等灾难直接对信息和信息系统造成毁灭性破坏，单纯依靠本地信息安全防护手段，已经无法保障电子政务信息和信息系统在灾难发生时安全可用。因此，如何建设电子政务信息安全灾难恢复体系，提高抵御灾难的能力，受到党政机关的高度重视。目前，针对这一问题，我国已经发布了一系列文件对信息系统灾难恢复体系建设进行指导和监督。

北京市政务信息化建设起步较早，信息化程度较高，对电子政务信息系统灾难恢复的建设需求尤其迫切。通过开展一系列灾难恢复管理和技术机制的调查研究，北京信息安全测评中心在2010年完成了北京市信息安全容灾备份中心的建设。《政务信息系统灾难恢复实用技术》凝聚了北京信息安全测评中心多年来在容灾备份中心建设中积累的大量研究成果和宝贵经验。

灾难恢复建设是一项复杂工程，需要有科学的管理和先进的技术。同时，各种电子政务信息系统情况不同，灾难恢复需求和灾难恢复等级不同，如何选择合理的灾难恢复技术，是电子政务信息和信息

系统的灾难恢复建设过程中面临的一项挑战。《政务信息系统灾难恢复实用技术》从灾难恢复技术入手，在给出灾难恢复技术总体框架的基础上，对各种主流灾难恢复技术的特点、关键问题、应用实践等做了较全面、客观的介绍，能够帮助读者从自身的需求和现状出发，选择合理的灾难恢复技术和方案。相信本书的出版和发行，能够为电子政务信息系统灾难恢复建设提供指导和借鉴，有力地提升电子政务信息系统容灾抗毁能力。

沈昌祥

2011 年 12 月

前　言

对信息化社会而言，信息系统的持续运行具有重要的意义，然而信息系统持续运行面临的挑战也越来越大。作为积极应对灾难、建设灾难恢复系统的核心要素，灾难恢复技术受到了越来越多的重视。然而，灾难恢复涉及的技术众多，它们各有特点又需要互为补充，因此，如何选择合理的灾难恢复技术，是许多信息系统管理者面临的一个难题。

本书对当前实用的灾难恢复技术做了一个完整、客观的介绍。在给出灾难恢复技术总体框架的基础上，对各种主流灾难恢复技术，包括其技术原理、技术过程、技术特点以及应用的最佳实践等做了详细的介绍。最后，还对如何选择灾难恢复技术给出了详细的论述，用以帮助读者从自身的需求和现状出发，选择合理的灾难恢复技术和方案。

对刚刚接触灾难恢复技术的读者，建议按照顺序阅读，以便能够对灾难恢复的架构以及灾难恢复技术的机理有一个基础的了解。第4章～第11章是灾难恢复技术的单项描述，分别对高可用性、数据备份、数据快照、数据复制、持续数据保护、应用恢复、网络恢复、数据传输等技术进行了详细的介绍，适合有一定基础的读者进行选择阅读和参考。对于正在进行灾难恢复技术选择的读者，则可以重点阅读第12章，之后再有选择地阅读第4章～第11章的内容。附录给出了灾难恢复的相关法规、部分政务系统灾难恢复实施案例、相关技术对应的厂商和产品等资料，可供随时进行查询和参考。

本书虽然针对政务信息系统提出，但所描述的灾难恢复技术，无论是整体框架，还是具体的各项技术，都具有广泛的适用性。因

此本书对所有信息系统的管理者、决策者都有参考价值。

为了方便读者选择技术和产品，在本书的最后，对灾难恢复技术涉及的相关产品及其提供商尝试性地给出了参考列表。由于每种技术对应的厂商和产品众多，且厂商和产品名称随时可能变更，也限于编者的精力，无法对所有的厂商和产品系列进行收录和核对，因此错误和遗漏在所难免。在此也欢迎读者和厂商予以补充和修正。

由于灾难恢复技术涉及的知识面广、发展迅速，加之作者水平有限，书中错误在所难免，其不当之处，敬请指正。

在本书编写过程中，北京商务中心区通信科技有限公司和北京威泰信息技术有限公司参与了策划、构思、写作、编校、审核等工作，在此表示感谢。

编 著 者

2011 年 11 月

目　录

第 1 章 灾难恢复概述

“未雨绸缪”、“凡事预则立”，信息系统也一样。灾难可能会损坏信息系统的业务数据，可能会导致应用系统的失效和网络中断，甚至会损毁整个数据中心。因此，通过一系列的技术和手段，在信息系统遭受灾难时，尽快恢复业务系统，实现对业务的持续支撑，具有重要的意义。

在详细介绍灾难恢复技术之前，本章先就灾难恢复技术的背景、定位、价值和意义等做一个基本的介绍。

1.1 灾难恢复背景

随着信息化建设，尤其是随着电子政务、电子商务的深入发展，越来越多的政府、企业和各类组织机构的业务系统承载在信息系统之上。各类组织业务的正常开展越来越依赖于其信息系统的持续运行。业务数据的丢失、应用系统的停止、网络的异常带来的不良影响也越来越严重。

玉树地震、南方旱灾、洪灾等自然灾难，以及近期银行、证券业务系统瘫痪事件的发生，使政府和企业的灾难恢复意识越来越强烈。灾难的发生对人民的生活、企业的生产、国家的政治和经济都会产生不可估量的影响，灾难恢复是防灾、减灾的核心，也是信息化社会一个不可缺少的基础安全设施。

近年来，国内外发生的一系列恐怖活动和自然灾害表明，在信息系统越来越复杂、应用和数据越来越集中、其本身的脆弱性越来越高的同时，信息系统面临的威胁也越来越多。有关调查显示，20％的组织平均每五年就会遇到影响其运营的重大意外事件。

因此，提高防范意识，积极建设灾难恢复系统，对各类组织而言，具有越来越重要的价值。灾难恢复应该成为各类组织持续发展战略的一部分。

随着政务系统信息化的深入开展，政务信息系统的持续发展更是成为关系到国家安全、社会稳定、经济发展的重要问题。《国家信息化领导小组关于加强信息安全保障工作的意见》(中办发[2003]27 号)、《关于做好重要信息系统灾难备份工作的通知》(信安通[2004]11 号)等对政务信息系统的安全和持续发展提出了具体的要求。2007 年发布的 GB/T 20988—2007《信息安全技术　信息系统灾难恢复规范》还对重要信息系统灾难恢复的规划和建设给出了具体的规范和指导。

我国相关部门表示，制定强制性的灾备建设规范，完善灾备标准体系，以促进政府相关部门、行业用户、企业灾难恢复保障体系的发展，已经成为信息化工作的一项重点工作。

1.2 灾难恢复相关术语

在 GB/T 20988—2007 中，对灾难、灾难恢复和灾难备份定义如下：

灾难是指“由于人为或自然的原因，造成信息系统严重故障或瘫痪，使信息系统支持的业务功能停顿或服务水平不可接受、达到特定的时间的突发性事件。通常导致信息系统需要切换到灾难备份中心运行。”

灾难恢复(DR，Disaster Recovery)是指“为了将信息系统从灾难造成的故障或瘫痪状态恢

复到可正常运行状态，并将其支持的业务功能从灾难造成的不正常状态恢复到可接受状态，而设计的活动和流程。”

灾难备份是指“为了实现灾难恢复而对数据、数据处理系统、网络系统、基础设施、专业技术支持能力和运行管理能力进行备份的过程。”

由此可见，灾难恢复是目的，灾难备份是必要的手段。

灾难恢复体系包括管理和技术两个方面，即管理体系和技术系统。

灾难恢复管理体系包括了实现灾难恢复的设计、建设、维护、应急操作等全过程，是一项复杂的系统工程。在将信息系统恢复到正常状态的过程中，一方面要依赖相应的管理操作，另一方面，不可或缺的就是灾难恢复技术系统。

灾难恢复技术系统，即通常所讲的灾难恢复系统，包括实现灾难恢复所必需的一系列灾难恢复技术和相应的软硬件设施。

灾难恢复技术是灾难恢复系统建设的基础。灾难恢复系统的建设、运维和操作，都是围绕着灾难恢复技术而展开的。因此，建设合理的灾难恢复体系，确保灾难恢复的合理实现，关键在于采用合理的灾难恢复技术。

1.3　灾难恢复与信息安全

确保信息的保密性、完整性、可用性是信息系统的基本安全要求，信息安全已经成为信息系统基础架构不可或缺的组成部分。长期以来，信息安全技术一直集中在防病毒、入侵检测、防火墙等方面。这些传统信息安全技术的应用，在一定程度上保障了信息系统的安全运行。然而，尤其是美国“9·11 事件”之后，人们发现，尽管传统的信息安全技术可以控制和消减一部分信息系统安全运行面临的风险，但我们的信息系统仍旧无法应对许多不可控制的风险和威胁，例如地震、洪水、战争等。这些灾难通常会完全破坏我们的信息系统——从数据到应用，从软件到硬件，从设备到场地——当然，也包括传统的信息安全措施。

不仅如此，传统的信息安全技术也无法彻底抵御和完全消除病毒、黑客攻击等所造成的信息系统非正常停机后果。当由于以上事件导致系统的停机时间达到一定的程度之后，就需要启用灾难恢复手段，来保证信息系统的持续运行。因此，灾难恢复不仅是现有信息系统信息安全保护手段的延伸，更是信息系统安全的最后防线。与传统的信息安全技术一样，灾难恢复已经成为 IT 基础架构的一部分，见图 1-1。

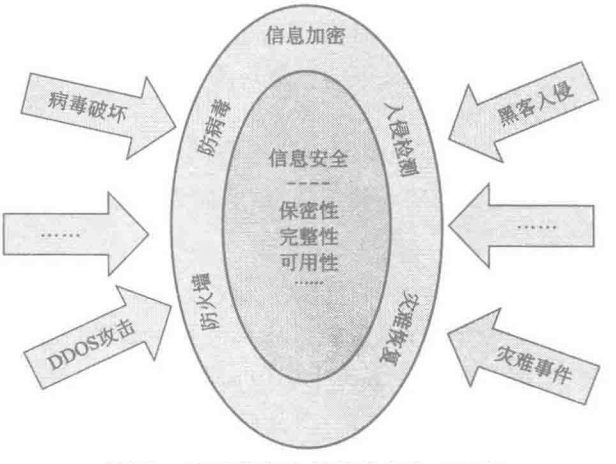

图1-1　灾难恢复与传统信息安全技术

实际上，信息安全技术的内涵和外延也在不断地变化。随着信息安全技术的关注点从最初简单的信息保密要求，扩展到信息保护和现在的信息保障体系，灾难恢复在信息安全中的重要性也越来越高。2007 年，我国发布的国家标准 GB/T 20988—2007 就明确地将灾难恢复归为信息安全技术的一部分。

1.4 灾难恢复建设的价值

在业务系统的正常运营高度依赖信息系统持续运行的信息化时代，灾难恢复在降低灾难造成的损失和不良影响、确保组织持续生存和发展、满足相关法规要求等方面具有重要的价值和意义。

灾难，例如火灾、爆炸、地震、水灾、雷击或线路故障等自然原因以及供电中断、机器故障、人为破坏等非自然原因引起的灾难，通常会导致重要数据丢失或损坏、业务无法正常进行，造成的损失不可估量。

根据有关机构统计，对关键业务运行要求最高的银行业，每次计算机系统宕机导致的损失平均为 1 000 万美元，同时还会导致对公司声誉无法估量的无形损失，而采取灾难恢复方案总共花费平均只有 100 万美元。各行业遭受灾难的损失估算见表 1-1。

表1-1 各行业遭受灾难的损失估算列表

行业	业务	停机每小时的损失	行业	业务	停机每小时的损失
金融	经纪业务运营	6 450 000 美元	交通	预定航班	90 000 美元
	信用卡授权	2 600 000 美元	媒体	电子票务销售	69 000 美元
媒体	付费收看	150 000 美元	金融	ATM 费用	14 500 美元
零售	居家购物(TV)	113 000 美元	政府	劳动部关键业务	有待评估
	目录销售	90 000 美元			

事实上，进行灾难恢复建设，不仅是为了降低损失，而且还关系到组织在灾难后能否持续生存和发展。在业务系统和信息资料高度依赖信息系统的今天，信息系统的不可恢复往往意味着业务系统无法恢复，从而使得各类组织不得不面对信息系统无法恢复带来的严重考验。

IDC 的统计数据表明，美国在 2000 年之前的十年间发生过灾难的公司，有 55%当时倒闭，剩下的 45%中，因为数据丢失，有 29%也在两年之内倒闭，生存下来的仅占 16%。Gartner Group 的数据也表明，在经历大型灾难而导致系统停运的公司中有 2/5 再也没有恢复运营，剩下的公司中也有 1/3 在两年内破产。

由此可见，业务系统的中断可能会使一个企业就此倒闭。灾难恢复是保证组织业务持续运行的基础。灾难恢复建设的实质就是为企业的核心业务系统构筑最后的防线，为组织的健康、持续发展提供保障。

各类组织信息系统的失效对社会带来的影响也越来越大。其中，政务系统是国家政治、经济等各方面正常运转的必要保证，政务系统的正常运行对国民经济具有重要意义。国内外一系列已经发生的灾难事件表明，如果没有应对灾难的准备和一定的恢复能力，重要信息系统一旦发生重大事故或者遭遇突发事件，将会严重影响国民经济的发展和社会的稳定。因此，信息系统的灾难恢复建设是保证国家安全、减少对国民经济不良影响的需要。