政务信息安全管理与应用丛书

政府网络与信息安全事件应急工作指南

钱秀槟　毛作奎　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

政府网络与信息安全事件应急工作指南

钱秀槟　毛作奎　毛东军　刘海峰　赵章界　刘国伟
李锦川　闫腾飞　方　星　荣晓燕　黄少青　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。

本书为丛书的应急分册，共分为8章。分别介绍了突发事件的背景，当前针对各类突发事件的应急管理，网络与信息安全应急体系的主要内容，网络与信息安全事件的基础知识及其分类分级，网络与信息事件应急响应的流程，4类最典型事件的应急处置，网络与信息安全事件应急预案的编制方法，网络与信息安全应急的宣传、培训和演练工作。本书还收录了相应的重要文件和部分可参考的范文。

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

政府网络与信息安全事件应急工作指南/钱秀槟等编著. —北京：中国标准出版社，2012

ISBN 978-7-5066-6560-5

Ⅰ. ①政… Ⅱ. ①钱… Ⅲ. ①电子政务—信息安全—研究 Ⅳ. ①D035.1-39

中国版本图书馆CIP数据核字(2011)第229856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 11.75 字数 280千字
2012年1月第一版 2012年1月第一次印刷

*

定价 **32.00** 元

丛书编委会

主　编： 白　新

副主编： 童腾飞　贾　力　毛东军

编　委： （按姓氏笔画排序）

万京平	方　星	毛作奎	水海峰
王　亮	王宗君	王春佳	付征兵
史宜会	刘　云	刘　旭	刘　泰
刘　鹏	刘　霞	刘国伟	刘海峰
刘慧刚	孙永生	孙志谊	成金爱
朱浩东	闫腾飞	齐　宁	张　勇
张　格	张乐东	张晓梅	李　东
李　垚	李　媛	李晨旸	李蒙生
李锦川	李颖涛	陈　平	陈　萍
孟　炎	房孝强	姚建东	胡　冰
荣晓燕	赵章界	徐晓滢	郭子亮
钱秀槟	梁　博	黄少青	

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

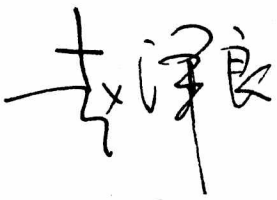
进入21世纪以来，信息感知和获取、无线宽带、移动互联、虚拟计算、网络融合等技术取得新的突破，下一代互联网、云计算等快速发展，工业控制系统、生产调度系统等传统网络同互联网等大众网络互联互通的趋势明显，电网、铁路、公路、桥梁、隧道、大坝、油气管道、城市交通与供水系统等的“数字化”、“网络化”步伐加快，金融、能源、交通、物流、制造等行业的信息化水平持续提高，国民经济和社会对信息系统与网络的依赖性越来越大。由此产生的信息安全问题更加突出，网络信息系统的重大风险和缺陷不断出现，计算机病毒、木马、僵尸网络、间谍软件、钓鱼仿冒网站等盛行，网络攻击、诈骗等犯罪活动甚至网络恐怖主义严重，网络上的淫秽色情内容、虚假有害信息也不同程度地存在，直接影响国家经济安全和社会正常秩序，直接影响企业和个人切身利益。

解决信息安全问题要坚持积极防御、预防为主。但信息安全是一项风险管理工作，不存在绝对的安全，不能做到永远不发生信息安全事故。必须在立足安全防护的同时，高度重视信息安全应急这项工作，认真制定并落实信息安全应急预案。要明确信息安全事件处理的责任分工，明确应急处理流程和权限，落实应急资源和技术支持队伍，一旦出事要能在第一时间响应和处置，坚决防止雪崩效应，最大限度地减少信息安全事件造成的损失。

北京市政务信息安全应急处置中心（北京信息安全测评中心）是北京市网络与信息安全应急的市级专业队伍，在近年首都各项大型活动，尤其是2008年奥运会、残奥会和2009年新中国成立六十周年大庆等重大活动的信息安全保障中发挥了重要的作用，也积累了宝贵的经验。《政府网络与信息安全事件应急工作指南》（以下简称《指

南》)是该中心信息安全系列丛书之一,是该中心对历年工作经验的总结。

《指南》面向政府,从理论和实践两个方面分别对信息安全应急工作的概念规则、技术方法进行了阐述,既可让应急工作的管理者了解应急工作的整体思路,也能够指导应急工作的执行者开展具体的各项工作。相信本书的出版发行能够很好地促进政府开展信息安全应急工作,并进一步推动电子政府更上一个新的台阶。



2011 年 10 月

前　言

随着我国信息化，尤其是政府信息化的不断发展，信息化对于政府行使社会管理和公共服务职能的支撑程度也在不断增加，由此带来的问题是，当这些起着支撑作用的网络与信息系统发生故障、遭受攻击或被滥用时，可能对经济发展、社会稳定和人民生活带来负面影响，严重时甚至可能影响到国家安全。

党和政府高度重视网络与信息安全应急工作，自2006年《国家突发公共事件总体应急预案》及2007年《中华人民共和国突发事件应对法》发布实施以来，网络与信息安全领域的专项应急工作也在不断向前发展。2008年12月20日，国务院发布了《国家网络与信息安全事件应急预案》，该预案从国家的高度对网络与信息安全事件应急管理各项工作做出了规定，为网络与信息安全事件应急工作的开展指明了方向。北京市政务信息安全应急处置中心（北京信息安全测评中心）作为北京市政务领域信息安全应急工作的基础性技术支撑单位，在市经济和信息化委员会（原北京市信息化工作办公室）的领导下在信息安全应急相关方面开展了大量的工作，在奥运会、残奥会以及新中国成立六十周年大庆期间发挥了应有的作用。中心自成立以来，得到了国家及北京市信息化主管部门的大力支持，并积极参加了北京市信息安全发展规划、体系建设以及国家、北京市及北京市部分市属单位网络与信息安全事件应急预案的制修订和应急演练工作，通过这些工作积累了一些网络与信息安全应急的经验。为深入贯彻《国家网络与信息安全事件应急预案》的要求，我们基于对网络与信息安全事件应急工作的粗浅认识，组织编写了《政府网络与信息安全事件应急工作指南》（以下简称《指南》），希望《指南》能够对北京市、其他兄弟省市以及各基层政府开展网络与信息安全事件应急工作提供有益的参考。

《指南》共分为8章，其中第1章为绪论，介绍了突发事件的背景，并引出网络与信息安全事件及其特点和趋势；第2章介绍了当前针对各类突发事件的应急管理；第3章介绍了网络与信息安全

应急响应体系的主要内容；第4章介绍了网络与信息安全事件的基础知识及其分类分级；第5章系统地介绍了网络与信息事件应急响应的流程；第6章介绍了4类最典型事件的应急处置；第7章介绍了网络与信息安全事件应急预案的编制方法；第8章介绍了网络与信息安全应急的宣传、培训和演练工作。《指南》还收录了《中华人民共和国突发事件应对法》、《国家突发公共事件总体应急预案》等重要文件和部分可参考的范文。

《指南》是作者所在单位面向政府开展网络与信息安全应急工作经验的总结，适合各级政府从事信息化、网络与信息安全的管理和技术人员的使用，也可供其他行业部门人员参考。

限于作者知识水平，书中难免出现错误之处，恳请读者批评指正。

编　著　者

2011年8月

目　录

第 1 章 绪 论

人类社会的发展历史其实就是一部与各种灾害不断斗争的历史。从远古时期开始，人类为了自身生存就开始不断地同各种自然灾害和非自然的灾难作斗争，并在斗争的过程中积累了许多宝贵经验，人类文明也随着人类社会应对各类灾害能力的增强而不断地发展进步。

1.1 突发事件和网络与信息安全事件

随着社会发展程度的不断提高，人类社会面临的灾害也已经从最初单一的自然灾害变得更为复杂多样，各类直接或间接人为原因造成的事件或事故也越来越成为影响社会发展的重要因素，这些事件和事故与自然灾害一起被统称为突发事件。网络与信息安全事件是随信息化的发生发展而出现的一种突发事件，是信息化革命不可避免的副产品。

1.1.1 突发事件概述

突发事件，也称为“突发公共事件”、“紧急事件”、“公共紧急状态”等，从名称上理解，就是指突然发生的，可能对人们正常的生产和生活带来一定负面影响的事件。

在现实情况下，由于社会文化、自然环境的不同，人们对突发事件的理解和认识甚至是表述也有所差别。例如美国对突发事件的定义为：由美国总统宣布的，在任何场合、任何情景下，在美国的任何地方发生的需联邦政府介入并提供补充性援助以协助州和地方政府挽救生命、确保公共安全及财产安全，或减轻、转移灾难所带来威胁的重大事件。欧洲人权法院则认为，公共紧急状态是一种特别的、迫在眉睫的危机或危险局势，它影响全体公民，并对整个社会的正常生活构成威胁。

我国是个突发事件多发的国家，仅自 2000 年以来每年因自然灾害、事故灾难和社会安全事件等突发事件造成的人员伤亡已逾百万，经济损失高达 6 500 亿元，约占全国 GDP 的 6%。表 1-1 列出了近 3 年来发生在我国大陆地区的部分特别重大突发事件。

表 1-1 2008 年以来我国发生的特别重大突发事件

发生时间	发生地点	事件类别	事 件 后 果
2008-01-10—2008-02-12	长江流域、西部地区	自然灾害	冰雪低温灾害，波及 21 个省(自治区、直辖市、兵团)，因灾死亡 107 人，失踪 8 人，紧急转移安置 151.2 万人，铁路公路滞留人员 192.7 万人；农作物受灾面积 1.77 亿亩，绝收 2 530 万亩；森林受损面积近 2.6 亿亩；倒塌房屋 35.4 万间；因灾直接经济损失 1111 亿元人民币
2008-03-14	西藏拉萨	社会安全事件	打砸抢烧，直接造成 18 人死亡，破坏拉萨市的商店铺面、银行通讯和单位学校等 900 多家，直接经济损失 2.8 亿元人民币。此外，境外藏独分子和支持者还打砸抢烧我国 40 多个驻外使馆和领事馆等机构，并在伦敦、巴黎、旧金山等城市抢夺奥运火炬，冲击奥运圣火传递活动，企图破坏 2008 年北京奥运会，极大地损害了我国在国际上的形象和威信，造成了极其恶劣的影响

表 1-1(续)

发生时间	发生地点	事件类别	事 件 后 果
2008-03	河北三鹿	公共卫生事件	截至2008年9月21日,因使用婴幼儿奶粉而接受门诊治疗咨询且已康复的婴幼儿累计39 965人,正在住院的有12 892人,已治愈出院1 579人,死亡4人
2008-04-28	胶济铁路	事故灾难	交通事故,造成72人死亡、416人受伤
2008-05-12	四川汶川	自然灾害	特大地震,造成69 227人遇难,374 643人受伤,17 824人失踪,直接经济损失达8 451亿元人民币
2008-09-08	山西襄汾	事故灾难	尾矿库溃坝,造成277人死亡、4人失踪
2008-09-13	四川巴中	事故灾难	交通事故,造成51人死亡
2009-07-05	乌鲁木齐	社会安全事件	暴乱,造成197人死亡,直接经济损失达6 895万元人民币
2010-04-14	青海玉树	自然灾害	造成617人死亡,失踪313人,9 110人受伤,其中970人重伤,估计损失约8 000亿元人民币
2010-08-07	甘肃舟曲	自然灾害	死亡702人,失踪1 042人,重伤42人
2010-11-15	上海	事故灾难	死亡58人,经济损失约5亿元人民币

党和政府也对突发事件的应急工作高度重视,通过总结应对各类突发事件的经验,不断丰富完善对突发事件的理解。2003年5月9日公布施行的《突发公共卫生事件应急条例》是我国突发事件应对工作的重要里程碑。该条例对突发公共卫生事件进行了定义,确定突发公共卫生事件是指突然发生,造成或者可能造成社会公众健康严重损害的重大传染病疫情、群体性不明原因疾病、重大食物和职业中毒以及其他严重影响公众健康的事件。随后,国务院于2006年1月8日发布的《国家突发公共事件总体应急预案》对突发事件的概念进行了界定,认为突发事件是指突然发生,造成或者可能造成重大人员伤亡、财产损失、生态环境破坏和严重社会危害,危及公共安全的紧急事件。2007年8月30日,第十届全国人民代表大会常务委员会第二十九次会议审议通过了《中华人民共和国突发事件应对法》,这部法律作为我国首部突发事件应对综合性法律文件,对突发事件应对各方面内容进行了说明。其中第一章第三条明确规定:"本法所称突发事件,是指突然发生,造成或者可能造成严重社会危害,需要采取应急处置措施予以应对的自然灾害、事故灾难、公共卫生事件和社会安全事件。"

从以上对突发事件的描述上可知,无论在具体细节上有什么不同,突发事件区别于非突发事件的两个显著特点是突发性和危害性,如表1-2所示。

表 1-2 突发事件的界定

事件	突发性	危 害 性	是否属突发事件
2008年南方冰雪灾害	1个月左右	因灾死亡107人,失踪8人, 直接经济损失1 111亿元人民币	是
第四纪冰期	至今二百万年	危害不能预计	否
无人区长期干旱	几个月	无危害	否
2010年西南旱灾	几个月	造成返贫人口200多万,经济损失超350亿元	是

第一是突发性，即事件发生在时间上有突然性，事件发生的时间周期较短。如2008年年初在我国长江流域和西部地区发生的大范围冰雪低温灾害，事件发生时间较短，持续时间约1个月；相比较而言，第四纪冰期从二百万年前开始直到现在仍未结束并可能再持续百万年，虽然最终也可能有所危害，但就不能称为突发事件。

第二是危害性，即突发事件已经或可能对人们的正常生产生活造成危害。例如2010年我国西南地区大范围旱灾造成200多万已脱贫的人口返贫、经济损失超过350亿元的重大危害，而无人区同样时间长度的干旱因不对社会造成损失，则不在突发事件范围之内。

通常情况下，根据突发事件发生和发展的过程，可以划分为四个时期，分别是潜伏期、爆发期、持续期、消除期，如图1-1所示。

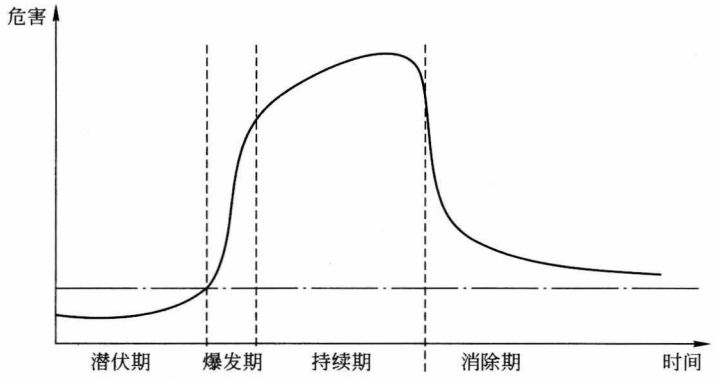


图1-1 突发事件的生命周期

(1) 潜伏期

潜伏期即突发事件发生前的阶段。突发事件的发生均有其内在原因，当条件达到一定程度后，可以造成可见的危害时，突发事件即发生。因此当人们能够识别并监测可引发某类突发事件的要素时，则可以及时采取有效的措施防范事件的发生或发布预警做好应对准备，降低事件可能造成的损失。

(2) 爆发期

爆发期是突发事件全面造成危害的时期。在这一时期，引发事件发生的条件在积聚到一定程度后，在短时间内突然爆发，并造成严重的损失。

(3) 持续期

持续期是指事态急剧扩大的势头已停止或受到限制，但破坏性仍维持在较高的水平上，事件尚未得到有效控制。如果应急准备充分，则这一时期会因应对迅速而得以缩短。

(4) 消除期

当事态已经得到控制时，事件所造成的危害和影响并不立即消失，而是会持续一段时间，这段时间即为消除期。需要指出的是，突发事件的影响往往分为两个部分：直接影响和间接影响。在消除期，直接影响得以消除，但间接影响可能才刚刚出现，如美国的“9·11”事件带给公众心理阴影的消除，则可能需要很长的时间。