ICS 35.040
L 80

中华人民共和国国家标准

GB/T 24363—2009

信息安全技术
信息安全应急响应计划规范

Information security technology—
Specifications of emergency response plan for information security

2009-09-30 发布　　2009-12-01 实施

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会　发布

目　　次

前　言

本标准的附录A、附录B、附录C、附录D为资料性附录。

本标准由全国信息安全标准化技术委员会提出并归口。

本标准起草单位：中国科学院研究生院国家计算机网络入侵防范中心、中国电子技术标准化研究所。

本标准主要起草人：张玉清、付安民、肖晖、游双燕、刘奇旭、宋杨、陈深龙、许玉娜、上官晓丽。

引　言

本标准根据《中华人民共和国计算机信息系统安全保护条例》，参照 GB/Z 20985—2007《信息技术　安全技术　信息安全事件管理指南》、GB/T 20988—2007《信息安全技术　信息系统灾难恢复规范》、GB/Z 20986—2007《信息安全技术　信息安全事件分类分级指南》、GB/T 20984—2007《信息安全技术　信息安全风险评估规范》、GB/T 22240《信息安全技术　信息系统安全等级保护定级指南》、GB/T 22239《信息安全技术　信息系统安全等级保护基本要求》以及 NIST SP 800-34《信息技术系统应急规划指南》和 NIST SP 800-61《计算机安全事件处理指南》等标准的有关部分，结合《国家通信保障应急预案》和《上海市网络与信息安全事件专项应急预案》以及相关行业技术发展和实践经验制定而成。

信息系统容易受到各种已知和未知的威胁而导致有害程序事件、网络攻击事件、信息破坏事件、信息内容安全事件、设备设施故障和灾害性事件等信息安全事件的发生。虽然很多信息安全事件可以通过技术的、管理的、操作的方法予以消减，但没有任何一种信息安全策略或防护措施，能够对信息系统提供绝对的保护。即使采取了防护措施，仍可能存在残留的弱点，使得信息安全防护可能被攻破，从而导致业务中断、系统宕机、网络瘫痪等突发/重大信息安全事件发生，并对组织和业务的运行产生直接或间接的负面影响。因此，为了减少信息安全事件对组织和业务的影响，应制定有效的信息安全应急响应计划，并形成预案。

信息安全应急响应计划的制定是一个周而复始、持续改进的过程，包含以下几个阶段：

a）　应急响应计划的编制准备；

b）　编制应急响应计划文档；

c）　应急响应计划的测试、培训、演练和维护。

信息安全技术
信息安全应急响应计划规范

1 范围

本标准规定了编制信息安全应急响应计划的前期准备，确立了信息安全应急响应计划文档的基本要素、内容要求和格式规范。

本标准适用于包括整个组织、组织中的部门和组织的信息系统（包括网络系统）的各层面上的信息安全应急响应计划。

本标准为负责制定和维护信息安全应急响应计划的人员提供指导。

2 规范性引用文件

下列文件中的条款通过本标准的引用而成为本标准的条款。凡是注日期的引用文件，其随后所有的修改单（不包括勘误的内容）或修订版均不适用于本标准，然而，鼓励根据本标准达成协议的各方研究是否可使用这些文件的最新版本。凡是不注日期的引用文件，其最新版本适用于本标准。

GB/T 20984—2007 信息安全技术 信息安全风险评估规范

GB/Z 20985—2007 信息技术 安全技术 信息安全事件管理指南

GB/Z 20986—2007 信息安全技术 信息安全事件分类分级指南

GB/T 20988—2007 信息安全技术 信息系统灾难恢复规范

GB/T 22239—2008 信息安全技术 信息系统安全等级保护基本要求

GB/T 22240—2008 信息安全技术 信息系统安全等级保护定级指南

3 术语和定义

下列术语和定义适用于本标准。

3.1

信息系统 information system

由计算机及其相关的和配套的设备、设施（含网络）构成的，按照一定的应用目标和规则对信息进行采集、加工、存储、传输、检索等处理的人机系统。

[GB/Z 20986—2007]

3.2

信息安全事件 information security incident

由于自然或者人为以及软硬件本身缺陷或故障的原因，对信息系统造成危害，或在信息系统内发生对社会造成负面影响的事件。

[GB/Z 20986—2007]

3.3

业务影响分析 business impact analysis

对业务功能及其相关信息系统资源进行分析，评估特定信息安全事件对各种业务功能的影响的过程。

3.4

应急响应 emergency response

组织为了应对突发/重大信息安全事件的发生所做的准备，以及在事件发生后所采取的措施。