

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 III

引言 IV

1 范围 1

2 规范性引用文件 1

3 术语和定义 1

4 缩略语 2

5 应急响应计划的编制准备 2

5.1 风险评估 2

5.2 业务影响分析 2

5.3 制定应急响应策略 3

6 编制应急响应计划文档 3

6.1 概述 3

6.2 总则 4

6.3 角色及职责 4

6.4 预防和预警机制 5

6.5 应急响应流程 5

6.6 应急响应保障措施 7

6.7 编制计划必需的附件 8

7 应急响应计划的测试、培训、演练和维护 9

7.1 应急响应计划的测试、培训和演练..... 9

7.2 应急响应计划的管理和维护 9

附录 A（资料性附录） 信息安全应急响应计划示例——××大学信息安全应急响应预案 10

附录 B（资料性附录） 业务影响分析(BIA)示例 18

附录 C（资料性附录） 业务影响分析(BIA)模板 20

附录 D（资料性附录） 呼叫树示例和联系人清单表 22

参考文献 24

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。

GB/T 24363—2009

3.5

应急响应计划 emergency response plan

组织为了应对突发/重大信息安全事件而编制的,对包括信息系统运行在内的业务运行进行维持或恢复的策略和规程。

3.6

灾难恢复 disaster recovery

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。

[GB/T 20988—2007]

3.7

风险评估 risk assessment

依据有关信息安全技术与管理标准,对信息系统及由其处理、传输和存储的信息的保密性、完整性和可用性等安全属性进行评价的过程。

[GB/T 20984—2007]

3.8

恢复时间目标 recovery time objective

信息安全事件发生后,信息系统或业务功能从停顿到恢复的时间要求。

[GB/T 20988 —2007]

3.9

恢复点目标 recovery point objective

信息安全事件发生后,系统和数据应恢复到的时间点的要求。

[GB/T 20988 —2007]

4 缩略语

BIA 业务影响分析(Business Impact Analysis)

POC 联系点(Point of Contact)

RTO 恢复时间目标(Recovery Time Objective)

RPO 恢复点目标(Recovery Point Objective)

SLA 服务水平协议(Service Level Agreement)

5 应急响应计划的编制准备

5.1 风险评估

标识信息系统的资产价值,识别信息系统面临的自然的和人为的威胁,识别信息系统的脆弱性,分析各种威胁发生的可能性。风险评估具体内容见 GB/T 20984—2007 的第 5 章风险评估实施和第 6 章信息系统生命周期各阶段的风险评估。

5.2 业务影响分析

5.2.1 概述

业务影响分析(BIA)是在风险评估的基础上,分析各种信息安全事件发生时对业务功能可能产生的影响,进而确定应急响应的恢复目标。

5.2.2 分析业务功能和相关资源配置

对单位或者部门的各项业务功能及各项业务功能之间的相关性进行分析,确定支持各种业务功能的相应信息系统资源及其他资源,明确相关信息的保密性、完整性和可用性要求。

5.2.3 确定信息系统关键资源

对信息系统进行评估,以确定系统所执行的关键功能,并确定执行这些功能所需的特定系统资源。

5.2.4 确定信息安全事件影响

应采用如下的定量和/或定性的方法,对业务中断、系统宕机、网络瘫痪等信息安全事件造成的影响进行评估:

- a) 定量分析——以量化方法,评估业务中断、系统宕机、网络瘫痪等可能给组织带来的直接经济损失和间接经济损失;
- b) 定性分析——运用归纳与演绎、分析与综合以及抽象与概括等方法,评估业务中断、系统宕机、网络瘫痪等可能给组织带来的非经济损失,包括组织的声誉、顾客的忠诚度、员工的信心、社会和政治影响等。

5.2.5 确定应急响应的恢复目标

根据业务影响分析的结果,同时结合 GB/T 22239 和 GB/T 22240,确定应急响应的恢复目标,包括:

- a) 关键业务功能及恢复的优先顺序;
- b) 恢复时间范围,即恢复时间目标(RTO)和恢复点目标(RPO)的范围。

5.3 制定应急响应策略

5.3.1 概述

应急响应策略提供了在业务中断、系统宕机、网络瘫痪等信息安全事件发生后,快速有效地恢复信息系统运行的方法。这些策略应涉及到在业务影响分析(BIA)中确定的应急响应的恢复目标。

5.3.2 系统恢复能力等级划分

系统恢复能力可以划分为基本支持、备用场地支持、电子传输和部分设备支持、电子传输及完整设备支持、实时数据传输及完整设备支持、数据零丢失及远程集群支持等 6 个等级,具体划分遵照 GB/T 20988—2007 的附录 A 灾难恢复能力等级划分。

5.3.3 系统恢复资源的要求

系统恢复资源的要求遵照 GB/T 20988—2007 的 6.3 灾难恢复资源的要求。

5.3.4 费用考虑

信息系统的使用或管理组织(以下简称“组织”)应确保有足够的人员和资金执行所选择的策略。各种类型的备用站点、设备更换和存储方式的费用应与预算限制相平衡。

应保证预算充足,应包括软件、硬件、差旅及运送、测试、计划培训项目、意识培训项目、劳务、其他合同服务以及任何其他适用资源的费用。

组织应进行成本效益分析,以确定最佳应急响应策略。

6 编制应急响应计划文档

6.1 概述

编制信息安全应急响应计划文档是应急响应规划过程中的关键一步。应急响应计划应描述支持应急操作的技术能力,并适应机构需求。应急响应计划需要在详细程度和灵活程度之间取得平衡,通常是计划越详细,其方法就越缺乏弹性和通用性。本标准说明了编制应急响应计划的要点。计划编制者应根据实际情况对其内容进行适当地调整、充实和本地化,以更好地满足组织特定的系统、操作和机构需求。同时可以参考 GB/Z 20985—2007 的第 8 章使用。

应急响应计划应能为信息安全事件中不熟悉计划的人员或要求进行恢复操作的系统提供快速明确的指导。计划应明确、简洁、易于在紧急情况下执行,并尽量使用检查列表和详细规程。

应急响应计划文档包括总则、角色及职责、预防和预警机制、应急响应流程、应急响应保障措施和附件 6 个部分。