ICS 35.040
L 80

中华人民共和国国家标准

GB/T 20985.2—2020

信息技术　安全技术　信息安全事件管理　第2部分：事件响应规划和准备指南

Information technology—Security techniques—Information security incident management—Part 2: Guidelines to plan and prepare for incident response

(ISO/IEC 27035-2:2016,MOD)

2020-12-14 发布　　2021-07-01 实施

国家市场监督管理总局
国家标准化管理委员会　发布

目　　次

前　言

GB/T 20985《信息技术　安全技术　信息安全事件管理》分为以下部分：

——第1部分：事件管理原理；

——第2部分：事件响应规划和准备指南。

本部分为GB/T 20985的第2部分。

本部分按照GB/T 1.1—2009给出的规则起草。

本部分使用重新起草法修改采用ISO/IEC 27035-2：2016《信息技术　安全技术　信息安全事件管理　第2部分：事件响应规划和准备指南》。

本部分与ISO/IEC 27035-2：2016的技术性差异及其原因如下：

——关于规范性引用文件，本部分做了具有技术性差异的调整，以适应我国的技术条件，调整的情况集中反映在第2章“规范性引用文件”中，具体调整如下：

- 用等同采用国际标准的GB/T 29246—2017代替了ISO/IEC 27000。

——范围一章增加了“经验总结”阶段的用途和要点（见第1章）。

本部分还做了下列编辑性修改：

——补充了缩略语“ICT”和“UTC”（见3.2）；

——增加了资料性引用文件GB/Z 20986—2007（见6.4的注和6.5的注）；

——将B.3.2中的脚注改为注（见B.3.2）；

——补充了参考文献ISO 22301和ISO 22313（见参考文献）。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别这些专利的责任。

本部分由全国信息安全标准化技术委员会（SAC/TC 260）提出并归口。

本部分起草单位：中电长城网际系统应用有限公司、中电数据服务有限公司、中国电子技术标准化研究院、国家计算机网络应急技术处理协调中心、北京奇虎科技有限公司、公安部第三研究所、国家信息中心、西安丁度网络科技有限公司、陕西省网络与信息安全测评中心、北京江南天安科技有限公司。

本部分主要起草人：闵京华、周亚超、王惠莅、上官晓丽、舒敏、陈悦、张屹、王艳辉、陈长松、杜佳颖、刘蓓、李怡、魏玉峰、陈冠直。

引　言

GB/T 20985 属于信息安全管理体系(ISMS)系列标准的延伸,聚焦于信息安全事件管理,GB/T 22080—2016 将其确定为信息安全管理体系的关键成功因素之一。

组织的事件计划与该组织确信已做好事件准备之间可能存在很大差距。因此,GB/T 20985 的本部分提供指南,以增强组织对信息安全事件响应做好实际准备的信心。为此,本部分关注于事件管理相关的策略和计划,以及如何建立事件响应小组并通过经验总结和评价不断改进其成效。

信息技术　安全技术　信息安全事件管理
第2部分：事件响应规划和准备指南

1　范围

GB/T 20985的本部分基于GB/T 20985.1—2017中给出的“信息安全事件管理阶段”模型的“规划和准备”阶段和“经验总结”阶段，给出了规划和准备事件响应以及事后总结经验和改进的指南。

“规划和准备”阶段的要点包括：

——信息安全事件管理策略和最高管理者的承诺；

——在公司层面以及系统、服务和网络层面都要更新的信息安全策略，其中包括与风险管理相关的信息安全策略；

——信息安全事件管理计划；

——事件响应小组(IRT)的建立；

——建立与内部和外部组织的关系和联络；

——技术及其他方面(包括组织和运行方面)的支持；

——信息安全事件管理的意识教育和培训；

——信息安全事件管理计划的测试。

“经验总结”阶段的要点包括：

——经验教训的总结；

——信息安全的总结和改进；

——信息安全风险评估和管理评审结果的总结和改进；

——信息安全事件管理计划的总结和改进；

——IRT表现和有效性的评价。

本部分给出的原理是通用的，适用于任何类型、规模或性质的组织。组织可根据其业务的类型、规模和性质，关联信息安全风险状况，调整本部分给出的指南。本部分也适用于提供信息安全事件管理服务的外部组织。

2　规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本(包括所有的修改单)适用于本文件。

GB/T 20985.1—2017　信息技术　安全技术　信息安全事件管理　第1部分：事件管理原理(ISO/IEC 27035-1：2016，IDT)

GB/T 29246—2017　信息技术　安全技术　信息安全管理体系　概述和词汇(ISO/IEC 27000：2016，IDT)

3　术语和定义、缩略语

3.1　术语和定义

GB/T 29246—2017、GB/T 20985.1—2017界定的以及下列术语和定义适用于本文件。