ICS 35.040
L 80

中华人民共和国国家标准

GB/T 20985.1—2017/ISO/IEC 27035-1:2016
代替 GB/Z 20985—2007

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

Information technology—Security techniques—Information security incident management—Part 1:Principles of incident management

(ISO/IEC 27035-1:2016,IDT)

2017-12-29 发布　　2018-07-01 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

GB/T 20985《信息技术　安全技术　信息安全事件管理》分为三个部分：

——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；

——第3部分：事件响应操作指南。

本部分为GB/T 20985的第1部分。

本部分按照GB/T 1.1—2009给出的规则起草。

本部分代替GB/Z 20985—2007《信息技术　安全技术　信息安全事件管理指南》，与GB/Z 20985—2007相比主要技术变化如下：

——由指导性技术文件改为推荐性国家标准，并拟分为三个部分；

——删除了“业务连续性规划”的术语和定义（见2007年版的3.1）；

——增加了“信息安全调查”“信息安全事件管理”“事件处理”“事件响应”和“联系点”的术语和定义（见3.1、3.5～3.8）；

——将术语“信息安全事件响应组（ISIRT）”改为“事件响应小组（IRT）”，并修改了其定义（见3.2，2007年版的3.4）；

——修改了术语“信息安全事态”和“信息安全事件”的定义（见3.3和3.4，2007年版的3.2和3.3）；

——将“规划和准备”“使用”“评审”和“改进”四个信息安全事件管理过程调整为“规划和准备”“发现和报告”“评估和决策”“响应”和“经验总结”五个信息安全事件管理阶段，并相应调整了其中的主要活动（见第5章，2007年版的5.2和第7章～第10章）。

本部分使用翻译法等同采用ISO/IEC 27035-1:2016《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》。

与本部分中规范性引用的国际文件有一致性对应关系的我国文件如下：

——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）

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：中国电子技术标准化研究院、中电长城网际系统应用有限公司、中国信息安全研究院有限公司。

本部分主要起草人：上官晓丽、闵京华、周亚超、许玉娜、蔡一鸣。

本部分所代替的历次版本发布情况为：

——GB/Z 20985—2007。

引　言

关于 ISO/IEC 27035

仅靠信息安全策略或控制不能保证信息、信息系统、服务或网络得到完全保护。即使采取了控制，仍可能存在残留的脆弱性，使信息安全效果降低，使信息安全事件易于发生，对组织的业务运行存在直接和间接的潜在负面影响。此外，以前未识别的新威胁将不可避免发生。若组织对处理这种事件未做好充分准备，将使任何响应的效果变差，却使对业务的潜在负面影响增加。因此，对于任何期望具有强健信息安全计划的组织，采用结构化和有计划的方法来开展如下活动十分必要：

——发现、报告和评估信息安全事件；

——响应信息安全事件，包括启动适当的控制来防止和降低影响并从中恢复；

——报告信息安全脆弱性，以便对其进行评估和适当处理；

——从信息安全事件和脆弱性中汲取经验教训，建立预防性控制，并改进整体信息安全事件管理方法。

为实现这种有计划的方法，ISO/IEC 27035 的如下部分在信息安全事件管理方面提供相应指南：

——ISO/IEC 27035-1 给出了信息安全事件管理的基本概念和阶段，以及如何改进事件管理。这部分将这些概念与结构化方法的原理相结合来发现、报告、评估和响应事件，并进行经验总结。

——ISO/IEC 27035-2 描述如何规划和准备事件响应。部分涵盖了 ISO/IEC 27035-1 中所给事件管理模型的“规划和准备”和“经验总结”阶段。

与其他标准的关系

ISO/IEC 27035 旨在对其他给出信息安全事件调查及调查准备指南的标准和文件进行补充。ISO/IEC 27035 并不是全部指南，而是某些基本原理的参考，旨在确保选择适当的工具、技术和方法并用于所需目的。

ISO/IEC 27035 涵盖信息安全事件管理的同时，也涵盖了信息安全脆弱性的某些方面。ISO/IEC 29147 和 ISO/IEC 30111 分别对脆弱性披露和供应商处理脆弱性提供了指南。

对于需要确定呈现在其面前的数字证据可靠性的决策者，ISO/IEC 27035 还意在提供指导。它适用于那些需要保护、分析和展示潜在数字证据的组织。它与创建和评价数字证据相关规程的策略决策机构相关，这些机构通常作为更大证据机构的组成部分。

有关调查类标准的进一步信息，参见附录 A。

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

1　范围

GB/T 20985的本部分提出了信息安全事件管理的基本概念和过程阶段,并将这些概念与结构化方法的原理相结合来发现、报告、评估和响应事件,以及进行经验总结。

本部分给出的事件管理原理是通用的,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。

ISO/IEC 27000　信息技术　安全技术　信息安全管理体系　概述和词汇(Information technology—Security techniques—Information security management systems—Overview and vocabulary)

ISO/IEC 27035-2　信息技术　安全技术　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)

3　术语和定义

ISO/IEC 27000界定的以及下列术语和定义适用于本文件。

3.1

信息安全调查　information security investigation

为帮助理解**信息安全事件**(3.4)而进行的检查、分析和解释。

[ISO/IEC 27042,定义3.10,做了修改:将“事件”替换为“信息安全事件”]

3.2

事件响应小组　incident response team

IRT

由组织中具备适当技能且可信的成员组成的团队,负责在事件生存周期中处理事件。

注:IRT通常被称为CERT(计算机应急响应小组)和CSIRT(计算机安全事件响应小组)。

3.3

信息安全事态　information security event

表明一次可能的信息安全违规或某些控制失效的发生。

3.4

信息安全事件　information security incident

与可能危害组织资产或损害其运行相关的、单个或多个被识别的**信息安全事态**(3.3)。