ICS 35.030
CCS L 80

中华人民共和国国家标准

GB/T 20985.2—2026/ISO/IEC 27035-2:2023
代替 GB/T 20985.2—2020

网络安全技术　网络安全事件管理 第2部分:事件响应规划和准备指南

Cybersecurity technology—Cybersecurity incident management—Part 2:Guidelines to plan and prepare for incident response

(ISO/IEC 27035-2:2023,Information technology—Information security incident management—Part 2:Guidelines to plan and prepare for incident response,IDT)

2026-07-02 发布　　2027-02-01 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

本文件按照GB/T 1.1—2020《标准化工作导则　第1部分:标准化文件的结构和起草规则》的规定起草。

本文件是GB/T 20985《网络安全技术　网络安全事件管理》的第2部分。GB/T 20985已经发布了以下部分:

——第1部分:原理和过程;

——第2部分:事件响应规划和准备指南。

本文件代替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》,与GB/T 20985.2—2020相比,除结构调整和编辑性改动外,主要技术变化如下:

a)　增加了网络安全策略更新(见第5章);

b)　增加了组织的推荐过程相关内容(见6.7);

c)　更改了与脆弱性管理相关的内容(见第6章,2020年版的第6章);

d)　增加了新的角色及其职责,包括事件管理小组和事件协调员(见7.2、7.3)。

本文件等同采用ISO/IEC 27035-2:2023《信息技术　信息安全事件管理　第2部分:事件响应规划和准备指南》。

本文件做了下列最小限度的编辑性改动:

——将标准名称更改为《网络安全技术　网络安全事件管理　第2部分:事件响应规划和准备指南》;

——增加了缩略语“ICT”和“IT”;

——附录B的表格增加了表编号。

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专利的责任。

本文件由全国网络安全标准化技术委员会(SAC/TC 260)提出并归口。

本文件起草单位:国家计算机网络应急技术处理协调中心、中国电子技术标准化研究院、北京青囊风华文化传媒有限公司、杭州安恒信息技术股份有限公司、国家信息中心、北京天融信网络安全技术有限公司、长扬科技(北京)股份有限公司、中国移动通信集团有限公司、北京时代新威信息技术有限公司、公安部第三研究所、中国信息通信研究院、蚂蚁科技集团股份有限公司、北京江南天安科技有限公司、司法鉴定科学研究院、北京东方通网信科技有限公司、海南大学、陕西省网络与信息安全测评中心、启明星辰信息技术集团股份有限公司、北京源堡科技有限公司。

本文件主要起草人:王文磊、崔牧凡、闵京华、吴莉莉、周亚超、王惠莅、刘蓓、王龑、张亚京、陈长松、邱勤、白晓媛、陈冠直、王连强、胡月、魏玉峰、梁露露、周成胜、王隆娟、郭弘、王秉政、崔婷婷、冯霞、潘文博。

本文件及其所代替文件的历次版本发布情况为:

——2020年首次发布为GB/T 20985.2—2020;

——本次为第一次修订。

引　言

GB/T 20985《网络安全技术　网络安全事件管理》为GB/T 22081中事件管理控制提供了指南，指导组织根据面临的网络安全风险实施GB/T 22081中的控制。GB/T 20985拟由四个部分构成。

——第1部分：原理和过程。目的在于提出网络安全事件管理的原理和流程。

——第2部分：事件响应规划和准备指南。目的在于给出事件响应规划和准备以及事件响应经验总结的指南。

——第3部分：ICT事件响应操作指南。目的在于给出ICT安全运营中的网络安全事件响应指南。

——第4部分：协同。目的在于给出多个组织协同处理网络安全事件的指南。

仅靠网络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。即使采取了控制措施，仍可能存在残留脆弱性，降低网络安全效果，导致网络安全事件易发生，对组织的业务运行产生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，进而使业务的潜在负面影响增加。因此，对于任何期望具有强健网络安全计划的组织，采用结构化和有计划的方法来开展如下活动十分必要：

——规划和准备网络安全事件管理，包括策略、组织、计划、技术支持、意识和技能培训等；

——发现、报告和评估网络安全事件以及与事件有关的脆弱性；

——响应网络安全事件，包括启动适当的控制来防止和降低影响并从中恢复；

——适当处理所报告的与事件有关的网络安全脆弱性；

——从网络安全事件和脆弱性中汲取经验教训，实施和验证预防性控制，并改进整体网络安全事件管理的方法。

GB/T 20985(所有部分)旨在对其他给出网络安全事件调查及调查准备指南的标准和文件进行补充。GB/T 20985(所有部分)并不全部是指南，而是某些基本原理和已定义过程的参考，旨在保证选择适当的工具、技术和方法并用于所需目的。

GB/T 20985(所有部分)涵盖网络安全事件管理的同时，也涵盖了网络安全脆弱性的某些方面。ISO/IEC 29147和ISO/IEC 30111分别为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，GB/T 20985(所有部分)也能提供指导。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有关，这些机构通常作为更大证据机构的组成部分。

网络安全技术　网络安全事件管理
第2部分:事件响应规划和准备指南

1　范围

本文件基于GB/T 20985.1—2026中5.2和5.6给出的“网络安全事件管理阶段”模型的“规划和准备”阶段和“经验总结”阶段,给出了事件响应规划和准备以及事件响应经验总结的指南。

规划和准备阶段关键点包括:

——网络安全事件管理政策及高层管理者承诺;

——网络安全政策,包括与风险管理相关的政策,需在组织层面以及系统、服务和网络层面同步更新;

——网络安全事件管理预案;

——事件管理小组(IMT)的组建;

——与内外部机构建立合作关系与联络渠道;

——技术及其他支持(含组织支持与运营支持);

——网络安全事件管理意识宣贯与培训。

经验总结阶段关键点包括:

——识别待改进领域;

——确定并实施必要的改进措施;

——事件响应小组(IRT)的绩效评估。

本文件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,关联网络安全风险状况,调整本文件给出的指南。本文件也适用于提供网络安全事件管理服务的外部组织。

2　规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中,注日期的引用文件,仅该日期对应的版本适用于本文件;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—2026　网络安全技术　网络安全事件管理　第1部分:原理和过程(ISO/IEC 27035-1:2023,IDT)

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)

注:GB/T 29246—2023　信息安全技术　信息安全管理体系　概述和词汇(ISO/IEC 27000:2018,IDT)

3　术语、定义和缩略语

3.1　术语和定义

GB/T 20985.1—2026和ISO/IEC 27000界定的术语和定义适用于本文件。

ISO和IEC维护的用于标准化的术语数据库网址如下: