ICS 35.030
CCS L 80

中华人民共和国国家标准

GB/T 43269—2023

信息安全技术
网络安全应急能力评估准则

Information security techniques—
Assessment criteria for cybersecurity emergency capability

2023-11-27 发布　　2024-06-01 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。

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。

本文件由全国信息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、国家计算机网络应急技术处理协调中心浙江分中心、安天科技集团股份有限公司、北京天融信网络安全技术有限公司、国家计算机网络应急技术处理协调中心江苏分中心、北京时代新威信息技术有限公司、中国电子技术标准化研究院、北京数字观星科技有限公司、中国网络安全审查技术与认证中心、国家计算机网络应急技术处理协调中心黑龙江分中心、新华三技术有限公司、国网智能电网研究院有限公司、北京东方通网信科技有限公司、深信服科技股份有限公司、奇安信网神信息技术(北京)股份有限公司、启明星辰信息技术集团股份有限公司、信联科技(南京)有限公司、华为技术有限公司、恒安嘉新(北京)科技股份公司、中电长城网际系统应用有限公司、深圳市腾讯计算机系统有限公司、联想(北京)有限公司、陕西省网络与信息安全测评中心、任子行网络技术股份有限公司、杭州安恒信息技术股份有限公司、华信咨询设计研究院有限公司、浙江鹏信信息科技股份有限公司、北京惠而特科技有限公司、北京辰安科技股份有限公司、上海观安信息技术股份有限公司、北京山石网科信息技术有限公司。

本文件主要起草人：陈悦、云晓春、耿冬梅、舒敏、王文磊、马骏野、赵焕菊、马旸、杨剑、于佳华、王新杰、吴莉莉、郭亮、龙泉、翟亚红、仲思超、闵京华、罗亮、王惠莅、蒋凌云、王秉政、万晓兰、崔婷婷、钱珂翔、叶润国、陈洪波、张璇、陈世俊、刘丙双、陈晓光、姚力、赵承刚、石竹君、高瑞、张胜、白峻、李汝鑫、刘蓝岭、董平、章亮、张帆、孙立立、李世斌、季莹莹、俞政臣、曾宪育、谢江、于俊杰、任协京、林峰。

信息安全技术
网络安全应急能力评估准则

1 范围

本文件规定了网络安全应急能力要求，给出了相应评估流程。

本文件适用于各类组织进行网络安全应急能力建设与评估。

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 20986 信息安全技术 网络安全事件分类分级指南

GB/T 25069 信息安全技术 术语

GB/T 38645—2020 信息安全技术 网络安全事件应急演练指南

3 术语和定义

GB/T 25069 界定的以及下列术语和定义适用于本文件。

3.1

网络安全应急能力 cybersecurity emergency capability

在网络安全事件发生的事前、事中和事后，组织采取网络安全应急响应措施应对突发网络安全事件的能力。

4 概述

本文件将网络安全应急能力分为三个级别，从低到高依次是一级、二级和三级，每个级别的网络安全应急能力要求包括应急组织与人员、应急制度、监测预警、应急处置、预防保障 5 个方面共 15 个部分，如图 1 所示。第 5 章、第 6 章、第 7 章分别规定了一级、二级和三级网络安全应急能力要求，高级别在低一级别的基础上提出增强要求或增加新的条款，并用黑体字标出，各级网络安全应急能力适用场景见附录 A。