ICS 35.030
CSS L 80

中华人民共和国国家标准

GB/T 39204—2022

信息安全技术
关键信息基础设施安全保护要求

Information security technology—
Cybersecurity requirements for critical information infrastructure protection

2022-10-12 发布　　2023-05-01 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：中央网信办网络安全协调局、公安部网络安全保卫局、中国电子技术标准化研究院、中国信息安全测评中心、国家信息技术安全研究中心、国家计算机网络应急技术处理协调中心、公安部第三研究所、公安部第一研究所、北京赛西科技发展有限责任公司、中国信息安全研究院有限公司、国家工业信息安全发展研究中心、中国网络安全审查技术与认证中心、中国互联网络信息中心。

本文件主要起草人：杨建军、郭启全、郭涛、姚相振、王惠莅、祝国邦、范春玲、陈亮、宋璟、孙晓丽、周亚超、孙军、任卫红、李秋香、江典盛、袁静、宫月、任泽君、张新跃、上官晓丽、杨晨、王凤娇、程娜、马力、刘志磊、于东升、陈翠云、刘志宇、任望、魏军、黄元飞、王博、王姣、王秉政。

引　言

为落实《中华人民共和国网络安全法》《关键信息基础设施安全保护条例》关于保护关键信息基础设施运行安全的要求，在国家网络安全等级保护制度基础上，借鉴我国相关部门在重要行业和领域开展网络安全保护工作的成熟经验，吸纳国内外在关键信息基础设施安全保护方面的举措，结合我国现有网络安全保障体系等成果，从分析识别、安全防护、检测评估、监测预警、主动防御、事件处置等方面，提出关键信息基础设施安全保护要求，采取必要措施保护关键信息基础设施业务连续运行，及其重要数据不受破坏，切实加强关键信息基础设施安全保护。

信息安全技术
关键信息基础设施安全保护要求

1 范围

本文件规定了关键信息基础设施分析识别、安全防护、检测评估、监测预警、主动防御、事件处置等方面的安全要求。

本文件适用于指导运营者对关键信息基础设施进行全生存周期安全保护，也可供关键信息基础设施安全保护的其他相关方参考使用。

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 20984 信息安全技术 信息安全风险评估方法

GB/T 25069 信息安全技术 术语

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

关键信息基础设施 critical information infrastructure

公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务、国防科技工业等重要行业和领域，以及其他一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生、公共利益的重要网络设施、信息系统等。

3.2

供应链 supply chain

将多个资源和过程联系在一起，并根据服务协议或其他采购协议建立连续供应关系的组织系列。

注：其中每一组织充当需方、供方或双重角色。

3.3

关键业务链 critical business chain

组织的一个或多个相互关联的业务构成的关键业务流程。

4 安全保护基本原则

关键信息基础设施安全保护应在网络安全等级保护制度基础上，实行重点保护，应遵循以下基本原则。

——以关键业务为核心的整体防控。关键信息基础设施安全保护以保护关键业务为目标，对业务所涉及的一个或多个网络和信息系统进行体系化安全设计，构建整体安全防控体系。