



# 中华人民共和国国家标准

GB/T 38561—2020

---

## 信息安全技术 网络安全管理支撑系统技术要求

Information security technology—  
Technical requirements for cybersecurity management support system

2020-03-06 发布

2020-10-01 实施

---

国家市场监督管理总局 发布  
国家标准化管理委员会

# 目 次

前言 .....	I
1 范围 .....	1
2 规范性引用文件 .....	1
3 术语和定义 .....	1
4 缩略语 .....	1
5 概述 .....	1
6 系统功能要求 .....	2
6.1 安全目标管理 .....	2
6.2 应急预案管理 .....	2
6.3 对象管理 .....	2
6.4 信息安全事件监测 .....	2
6.5 运行监测 .....	2
6.6 流程处理 .....	3
6.7 统计分析 .....	3
6.8 考核管理 .....	3
6.9 发布与展示 .....	3
6.10 采集与处理 .....	3
6.11 数据交换 .....	4
6.12 备份与恢复 .....	4
7 自身安全性要求 .....	4
7.1 身份鉴别 .....	4
7.2 访问控制 .....	4
7.3 权限管理 .....	4
7.4 数据安全 .....	4
7.5 安全审计 .....	5
8 安全保障要求 .....	5
8.1 配置管理保障 .....	5
8.2 开发 .....	5
8.3 测试保障 .....	5
8.4 交付与运维保障 .....	5
8.5 指导性文档 .....	5
8.6 脆弱性分析 .....	6
8.7 生命周期支持 .....	6

## 前 言

本标准按照 GB/T 1.1—2009 给出的规则起草。

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这些专利的责任。

本标准由全国信息安全标准化技术委员会(SAC/TC 260)提出并归口。

本标准起草单位：浙江远望信息股份有限公司、公安部第一研究所、浙江省委办公厅信息化管理中心、浙江省公安厅科技通信管理局、浙江省高级人民法院信息中心、浙江省信息化推进服务中心、杭州市公安局科技信息化局、中电长城网际系统应用有限公司、北京江南天安科技有限公司。

本标准主要起草人：傅如毅、吴文、宣以广、殷云飞、毛林斌、栗红梅、周春燕、邵森龙、蒋行杰、马洪军、陈冠直、金江焕、周征宇、姚龙飞、蒋先浩、刘京玲、王雪玲。

# 信息安全技术

## 网络安全管理支撑系统技术要求

### 1 范围

本标准规定了网络安全管理支撑系统的技术要求,包括系统功能要求、自身安全性要求和安全保障要求。

本标准适用于网络安全管理工作的支撑系统的规划、设计、开发和测试。

### 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/Z 20986—2007 信息安全技术 信息安全事件分类分级指南

### 3 术语和定义

GB/Z 20986—2007 界定的以及下列术语和定义适用于本文件。

#### 3.1

**网络安全管理支撑系统** cybersecurity management support system

基于组织的安全目标、对象、流程等,支撑组织开展网络安全管理工作的系统。

#### 3.2

**对象** object

网络安全管理中的实体。

注:主要包括硬件资产、软件资产、数据资产、组织人员等。

### 4 缩略语

下列缩略语适用于本文件。

CPU:中央处理器(Central Processing Unit)

DB:数据库(Data Base)

FTP:文件传输协议(File Transfer Protocol)

HTTP:超文本传输协议(HyperText Transfer Protocol)

IP:互联网协议(Internet Protocol)

MAC:媒体访问控制(Media Access Control 或 Medium Access Control)

SNMP:简单网络管理协议(Simple Network Management Protocol)

### 5 概述

网络安全管理支撑系统(以下简称支撑系统)是支撑组织开展网络安全管理工作的系统,实现对组