ICS 35.040
L 80

中华人民共和国国家标准

GB/T 36958—2018

信息安全技术　网络安全等级保护安全管理中心技术要求

Information security technology—Technical requirements of security management center for classified protection of cybersecurity

2018-12-28 发布　　2019-07-01 实施

国家市场监督管理总局
中国国家标准化管理委员会　发布

目　　次

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:中国电子科技集团公司第十五研究所(信息产业信息安全测评中心)、公安部第三研究所、公安部第一研究所、网神信息技术(北京)股份有限公司。

本标准主要起草人:霍珊珊、任卫红、刘健、张益、董晶晶、刘凯明、郑国刚、陶源、陈广勇、李秋香、卢青、王刚。

引　言

本标准从安全管理中心的功能、接口、自身安全等方面，对 GB/T 25070 中提出的安全管理中心及其安全技术和机制进行了进一步规范，提出了通用的安全技术要求，指导安全厂商和用户依据本标准要求设计和建设安全管理中心。为清晰表示每一个安全级别比较低一级安全级别的安全技术要求的增加和增强，从第二级安全管理中心的技术要求开始，每一级新增部分用“黑体”表示。

安全管理中心是对网络安全等级保护对象的安全策略及安全计算环境、安全区域边界和安全通信网络上的安全机制实施统一管理的平台或区域，是网络安全等级保护对象安全防御体系的重要组成部分，涉及系统管理、安全管理、审计管理等方面。

信息安全技术　网络安全等级保护
安全管理中心技术要求

1　范围

本标准规定了网络安全等级保护安全管理中心的技术要求。

本标准适用于指导安全厂商和运营使用单位依据本标准要求设计、建设和运营安全管理中心。

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/T 5271.8　信息技术　词汇　第8部分：安全

GB 17859—1999　计算机信息系统　安全保护等级划分准则

GB/T 25069　信息安全技术　术语

GB/T 25070　信息安全技术　信息系统等级保护安全设计技术要求

3　术语和定义

GB 17859—1999、GB/T 5271.8、GB/T 25069 和 GB/T 25070 界定的以及下列术语和定义适用于本文件。

3.1

数据采集接口　data acquisition interface

采集网络环境中的主机操作系统、数据库系统、网络设备、安全设备等各监测对象上的安全事件、脆弱性以及相关配置及其状态信息的接口。

3.2

采集器　collector

从网络安全等级保护对象或其所在区域上收集网络安全源数据和事件信息的组件。

3.3

安全管理中心　security management center

对定级系统的安全策略及安全计算环境、安全区域边界和安全通信网络的安全机制实施统一管理的平台或区域。

注：修改 GB/T 25070—2010 定义 3.6。

4　缩略语

下列缩略语适用于本文件。

CPU　中央处理器(Central Processing Unit)

CVE　通用脆弱性及披露(Common Vulnerabilities & Exposures)

DDoS　分布式拒绝服务(Distributed Denial of Service)