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

前言 …… Ⅰ
引言 …… Ⅱ
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 安全管理中心概述 …… 2
5.1 总体说明 …… 2
5.2 功能描述 …… 3
6 第二级安全管理中心技术要求 …… 3
6.1 功能要求 …… 3
6.2 接口要求 …… 3
6.3 自身安全要求 …… 3
7 第三级安全管理中心技术要求 …… 4
7.1 功能要求 …… 4
7.2 接口要求 …… 8
7.3 自身安全要求 …… 8
8 第四级安全管理中心技术要求 …… 13
8.1 功能要求 …… 13
8.2 接口要求 …… 13
8.3 自身安全要求 …… 13
9 第五级安全管理中心技术要求 …… 15
9.1 功能要求 …… 15
9.2 接口要求 …… 15
9.3 自身安全要求 …… 15

前　言

本标准按照 GB/T 1.1—2009 给出的规则起草。

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

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

[illegible]于本文[illegible]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。

[illegible]GB/T 32918(信息技术 SM2 椭[illegible] 第8部分：安全

GB/T 859—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

3　术语和定义

[illegible]定义适用于[illegible] 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。

[illegible]

3.[illegible]

[illegible]

[illegible]

3.2

采集器　collector

[illegible]

3.3

[illegible]

[illegible]

[illegible]

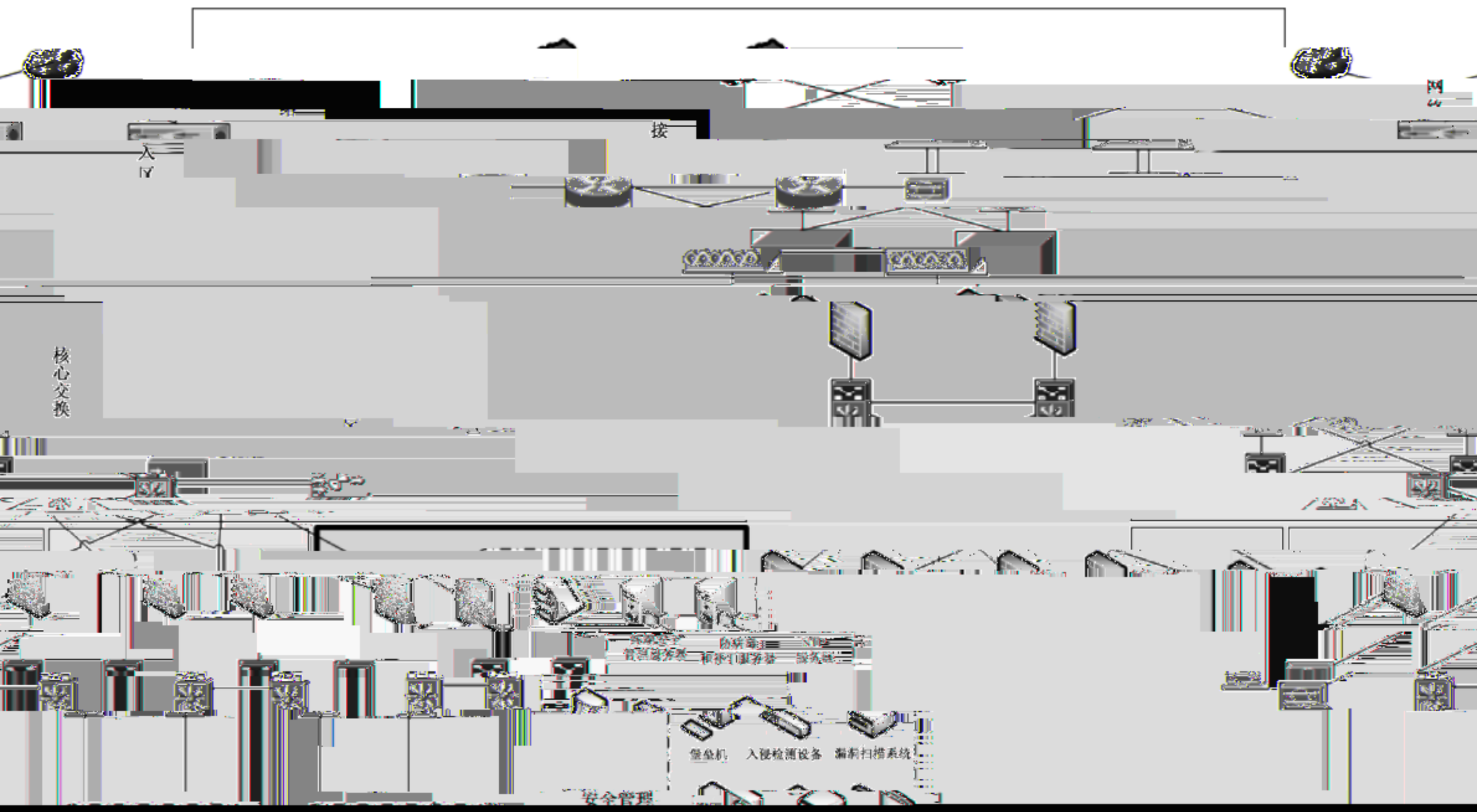
[illegible]

4　缩略语

[illegible]

DNS　分布式域名(Distributed Denial of Service)

IP	互联网协议(Internet Protocol)
[illegible]	[illegible]
[illegible]	[illegible]


核心交换
安全管理
堡垒机
入侵检测设备
漏洞扫描系统

6.1.1.2 数据保护

6.1.1.2.1 数据保密性

6.1.1.2.2 数据完整性

6.1.1.2.3 数据备份与恢复

数据备份与恢复应满足以下要求：

6.1.1.3 安全事件管理

6.1.1.3.1 安全事件采集

安全事件采集应满足以下要求：

6.1.1.3.2 安全事件告警

安全事件告警应具备告警功能，在发现异常时可根据预先设定的阈值产生告警。

6.1.1.3.3 安全事件响应

安全事件响应应满足以下要求：

6.1.1.5.1　可用性监测

可用性监测应满足下要求：

6.1.1.4.3　脆弱性管理

6.1.1.4.4　风险分析

6.1.1.4.2　威胁管理

6.1.1.1　资产管理

6.1.1.5.2 网络拓扑监测

网络拓扑监测应满足以下要求：

6.1.2 审计管理要求

6.1.2.1 审计策略集中管理

6.1.2.2 审计数据集中管理

6.1.2.2.1 审计数据采集

6.1.2.2.2 审计数据采集对象

6.1.2.3 审计数据采集方式

审计数据采集方式应满足以下要求：

a) 支持通过如 Syslog、SNMP 等协议采集各种系统或设备上的审计数据；

b) 通过统一接口，接收被管理对象的安全审计数据。

6.2 接口要求

6.2.1 第三方插件/代理接口协议要求

以及第三方的插 安全管理中心应支持 SNMP Trap、Syslog、Web Service 等常规接口和自定义接口

接口安全要求应满足以下要求：

a) 采用安全的接口协议，保证接口之间交互数据的完整性；

b)

安全要求

6.3 身

份鉴别

6.3.1 身

管理中心控制台的管理员身份鉴别应满足以下要求：

安全管

a) 提供专用的登录控制模块对管理员进行身份标识和鉴别；

b) 提供管理员用户身份标识唯一和鉴别信息重复检查功能，保证不存在重复用户身份标识；

c)

6.3.2 访问控制

安全管理中心控制台的访问控制应满足以下要求：

a)

b)

c)

6.3.3 安全审计

安全管理中心控制台的安全审计应满足以下要求：

a)

b)

c)

d)

6.3.4 软件容错

6.3.5 资源控制

安全管理中心控制台的资源控制应满足以下要求：

a) 对管理员登录地址范围进行限制；

b) 当管理员在一段时间内未作任何动作，应能够自动结束会话；

c) 能够对最大并发会话连接数进行限制；

6.3.6 入侵防范

6.3.7 数据安全

7 第三级安全管理中心技术要求

7.1 功能要求

7.1.1 系统管理要求

7.1.1.1 用户身份管理

用户身份管理应满足以下要求：

7.1.2 数据保护

7.1.2.1 数据保密性

7.1.2.2 数据完整性

7.1.1.2.3 数据备份与恢复

数据备份与恢复应满足以下要求：

a) 提供数据本地备份与恢复功能，完全数据备份至少每天一次，备份介质场地存放；

b) [illegible]

c) [illegible]

7.1.1.2.4 剩余信息保护

[illegible]

7.1.1.3 安全审计

7.1.1.3.1 安全事件采集

安全事件采集应满足以下要求：

a) [illegible]

b) [illegible]

c) 安全事件的内容应包括日期时间、主体标识、客体标识、类型、结果、IP地址、端口等信息；

d) [illegible]

e) [illegible]

7.1.1.3.2 安全事件告警

安全事件告警应满足以下要求：

a) 具备告警功能，在发现异常时可提供[illegible]

b) [illegible]

c) [illegible]

7.1.1.3.3 安全事件响应

安全事件响应应满足以下要求：

a) 能够提供工单管理的功能，支持基于告警响应动作创建工单的流转流程；

b) 能够提供安全通告功能，可以创建或导入安全风险通告，通告中应包括通告内容、描述信息[illegible]

c) [illegible]

d) 能够根据生成的安全风险通知的操作系统，提供通知的软件资产列表；

e) [illegible]

7.1.1.3.4 事件关联分析

事件关联分析应满足以下要求：[illegible]

7.1.1.3.5 统计分析报表

7.1.1.4 风险管理

7.1.1.4.1 资产管理

资产管理应满足以下要求：

7.1.1.4.3 威胁管理

威胁管理应满足以下要求：

7.1.1.4.5 风险分析

风险分析应满足以下要求：

7.1.1.5 资源监控

7.1.1.5.1 可用性监测

可用性监测应满足以下要求：



7.1.1.6.2 网络拓扑监测

网络拓扑监测应满足以下要求：

a) 支持对网络拓扑进行自动发现，绘制网络拓扑图，自动识别网络设备、安全设备、服务器主机等关键设备，以及设备之间的连接关系；

b) 能够实现当前网络环境中关键设备（包括网络设备、安全设备、服务器主机等）和链路的运行状态、如网络流量、网络协议统计分析等信息；

c) 支持网络运行状态异常时，能够根据预先配置的网络拓扑图，自动定位异常设备或链路，并以醒目的方式在网络拓扑图中进行标记；

d) 支持网络拓扑图的编辑，允许手工添加或删除监测节点或链路；

e) 支持对网络拓扑图进行自动布局，以及手工调整布局。

7.1.2 安全管理要求

7.1.2.1 安全标记

安全标记应满足以下要求：

a) 能够支持为主体/客体（或其他资源）创建安全标记，并能够维护（如增加、修改或删除）主体/客体安全标记所包含的信息；

b) 安全标记应具有唯一性，能够在强制访问控制/多级安全系统中为安全属性具有唯一确定的含义和删除的能力；

c) 标记属性应包括安全级别、安全范围等信息，安全级别应可排序进行高低判断，安全范围应可进行是否包含判断；

d) 能够实现对不同安全级别的系统中安全标记与安全属性的单一映射关系。

7.1.2.2 授权管理

授权管理应满足以下要求：

a) 实现对每一个标记所能访问范围的统一管理；

b) 实现主体对客体访问权限的统一管理，包括主机访问权限管理、网络访问权限管理、应用访问权限管理；

c) 实现根据主体标记和客体标记安全级别的不同，动态调整访问控制策略，控制主体对客体的访问。

7.1.2.3 设备策略管理

7.1.2.3.1 安全配置策略

设备管理应实现对主机操作系统、数据库系统、网络设备、安全设备的安全配置策略的统一查询、部署和下载。

7.1.2.3.2 入侵防御

入侵防御应满足以下要求：

a) 提供统一接口，实现对网络入侵防御和主机入侵防御的事件采集、接收和指令下发；

计：应通过运维审计系统对管理员的运维行为进行安全审计；应通过租户隔离机制，确保审计数据隔离的有效性；

7.1.3.2.3 审计数据采集方式

7.1.3.2.4 审计数据关联分析

7.2 接口要求

7.2.1 第三方插件/代理接口协议要求

接口协议要求应满足以下要求：

7.2.2 接口安全要求

接口安全要求应满足以下要求：

a) 采用安全的接口协议，保证接口之间交互数据的完整性；

b) 采用加密技术实现接口之间交互数据的保密性。

7.3 自身安全要求

7.3.1 身份鉴别

安全管理中心监控台的管理员身份鉴别应满足以下要求：

a)

7.3.2 访问控制

安全管理中心监控台的访问控制应满足以下要求：

a)

b)

c)

d) 实现特权用户的权限分离，应授予不同账户为完成各自承担任务所需的最小权限，并在它们之

7.3.3 安全审计

安全管理中心控制台的安全审计应满足以下要求：

a) 应提供覆盖到每个管理员的安全审计功能，记录所有管理员对重要操作的安全事件进行审计；

b) 保证无法单独中断审计进程，无法删除、修改或覆盖审计记录；

c) 审计记录的内容至少应包括事件的日期、时间、发起者信息、类型、描述和结果；

d) 提供对审计记录数据进行统计查询分析及生成审计报表的功能。

7.3.4 剩余信息保护

安全管理中心控制台的剩余信息保护应满足以下要求：

a) 确保鉴别信息所在的存储空间被释放或重新分配给其他用户前得到完全清除，无论这些信息是存放在硬盘上还是内存中；

b) 确保安全标记所在的存储空间被释放或重新分配给其他用户前得到完全清除，无论这些信息是存放在硬盘上还是内存中。

7.3.5 软件容错

安全管理中心控制台的软件容错应满足以下要求：

a) 应提供故障检测、故障报警和故障恢复的功能；

b) 应提供关键组件的热冗余或冷备份。

7.3.6 资源控制

安全管理中心控制台的资源控制应满足以下要求：

a) 应对登录超时进行限制；

b) 当管理员在一段时间内未作任何动作，应能够自动结束会话；

c) 能够对最大并发会话连接数进行限制；

d) 能够对单个管理员或者单个发会话进行限制；

e) 能够对一个时间段内可能的并发会话连接数进行限制；

f) 能够对一个管理员或者一个发会话进行限制；

g) 能够对一个时间段内可能的并发会话连接数进行限制。

7.3.7 入侵防范

安全管理中心控制台的入侵防范应满足以下要求：

a) 能够检测到对重要服务器、网络设备和安全设备进行已知攻击，并在检测到已知攻击时提供报警；

b) 应关闭不必要的系统服务和高危端口；

c) 应关闭不必要的系统服务和高危端口。

7.3.8 数据安全

安全管理中心控制台的数据安全应满足以下要求：

a) 能够检测到重要数据被篡改，并在检测到完整性受到破坏后能够及时采取必要的恢复措施；

b) 应关闭不必要的系统服务和高危端口。

8 第四级安全管理中心技术要求

8.1 功能要求

8.1.1 系统管理要求

8.1.1.1 用户身份管理

用户身份管理应满足以下要求：

a) 能够对被管理对象环境中的主体进行标识；

[illegible]

8.1.1.2 数据保护

8.1.1.2.1 数据保密性

数据保密性应满足以下要求：

[illegible]

8.1.1.2.2 数据完整性

数据完整性应满足以下要求：

[illegible]

8.1.1.2.3 数据备份与恢复

数据备份与恢复应满足以下要求：

[illegible]

中华人民共和国境内，禁止从境外对境内云计算平台的运维

可信路径

可信路径应满足以下要求：

a) 在对主体进行身份鉴别时，应能够建立一条安全的信息传输路径；

b) 在主体对客体进行访问时，应保证数据访问路径上各个实体之间能够建立一条安全的信息传输路径。

8.1.1.2.5 剩余信息保护

8.1.1.3 安全事件管理

8.1.1.3.1 安全事件采集

安全事件采集应满足以下要求：

a) 支持安全事件监测采集功能，及时发现和采集发生的安全事件；

b) 能够提供与第三方系统的数据采集接口，发送或接收安全事件；

8.1.1.3.2 安全事件告警

安全事件告警应满足以下要求：

a) 具备告警功能，在发现异常时可根据预先设定的阈值产生告警；

8.1.1.3.3 安全事件响应

安全事件响应应满足以下要求：

8.1.1.3.4 事件关联分析

事件关联分析应满足以下要求：

8.1.1.3.5 统计分析报表

统计分析报表应满足以下要求：

8.1.1.4 风险管理

8.1.1.4.1 资产管理

资产管理应满足以下要求：

8.1.1.4.2 资产业务价值评估

8.1.1.4.3 威胁管理

威胁管理应满足以下要求：

8.1.1.4.4 脆弱性管理

脆弱性管理应满足以下要求：

8.1.1.4.5 风险分析

风险分析应满足以下要求：

a) 能够根据资产的业务价值、资产当前的脆弱性及资产面临的安全威胁，计算目标资产的安全风险和资产所在整个安全域的安全风险；

[redacted]

[redacted]

[redacted]

授权管理应满足以下要求：

a) 实现对每一个标记所能

b) 实现主体对客体访问权
权限管理；

c) 实现根据主体标记和客

要求：

访问范围的统一管理；

限的统一管理，包括主机访问权限管理、网络访问权限管理、应用访问

体标记安全级别的不同，制定访问控制策略，控制主体对客体的访问，

设备管理应满足以下

a) 实现对主机操作

8.1.2.3.2 入侵防御

入侵防御应满足以下要求：

8.1.2.3.3 恶意代码防范

8.1.2.4 密码保障

8.1.3 审计管理要求

8.1.3.1 审计策略集中管理

审计策略集中管理应满足以下要求：

8.1.3.2 审计数据集中管理

8.1.3.2.1 审计数据采集

审计数据采集应满足以下要求：

a) 能够实现审计数据的归一化处理，内容应涵盖日期、时间、主体标识、客体标识、类型、结果、IP

8.1.3.2.2 审计数据采集对象

审计数据采集对象应满足以下要求：

a) 支持对网络设备、主机设备、业务应用系统、数据库管理系统、中间件、终端操作系统、安全设备、虚拟化平台、大数据组件、云资源管理平台等设备的审计数据采集；

b) 支持对数据库的审计数据采集；

c) 支持对安全设备（如防火墙、入侵检测系统、抗拒绝服务设备、防病毒系统）的安全审计；

d) 支持对控制系统（包括系统安全软硬件、系统和设备的审计数据）采集；

e) 支持对现场控制设备、网络安全设备、网络设备、服务器、操作站等在工业控制系统中应用的网络安全事件信息进行集中管理；

f) 支持对工业控制系统网络安全监控和报警设备的网络安全监控和报警等。

8.1.3.2.3 审计数据采集方式

审计数据采集方式应满足以下要求：

a) 支持通过如 Syslog、SNMP 等协议采集各种系统或设备上的审计数据；

8.1.3.2.4 数据采集组件要求

数据采集组件应支持本地缓存和断点续传，在网络通信发生故障时，能够在数据采集组件对数据进行本地缓存，当网络连通恢复以后，信息采集组件重新恢复向安全管理中心上报断网期间采集的数据。

8.1.3.2.5 审计数据

8.2 接口要求

8.2.1 第三方插件/代理接口协议要求

接口协议要求应满足以下要求：

a) 安全管理中心应实现对 IPv4 及 IPv6 双协议环境的支持(包括 IPv4 环境、IPv6 环境及 IPv4/

8.2.2 接口安全要求

接口安全要求应满足以下要求：

a) 采用安全的接口协议，保证接口之间交互数据的完整性；

b) 采用[illegible]

8.3 自身安全要求

8.3.1 身份鉴别

安全管理中心控制台的管理员身份鉴别应满足以

a) 提供专用的登录控制模块对管理员进行身份

8.3.3 可信路径

8.3.4 安全审计

8.3.5 剩余信息保护

8.3.6 软件容错

8.3.7 资源控制

8.3.8 入侵防范

8.3.9 数据安全

[redacted]

全管理中心技术要求另行制定。

10 跨定级系统安全管理中心技术要求

跨定级系统安全管理中心应满足以下要求：

[redacted]

附 录 A
（规范性附录）
安全管理中心与网络安全等级保护对象等级对应关系

安全管理中心与网络安全等级保护对象等级对应关系见表 A.1。

表 A.1 安全管理中心与网络安全等级保护对象等级对应表

安全管理中心级别	网络安全等级保护对象等级
第二级	第二级
第三级	第三级
第四级	第四级
第五级	第五级

附 录 B
（规范性附录）

安全管理中心技术要求分级表

表 B.1 安全管理中心技术要求分级表

技术要求		第二级	第三级	第四级
系统管理	系统监测	6.1.1.1.1	7.1.1.1.1	8.1.1.1.1
	系统告警	6.1.1.1.2	7.1.1.1.2	8.1.1.1.2
	系统资源分析	—	—	8.1.1.1.3
	系统配置管理	6.1.1.1.3	7.1.1.1.3	8.1.1.1.4
审计管理	审计数据采集	6.1.1.2.1	7.1.1.2.1	8.1.1.2.1
	审计数据存储管理	6.1.1.2.2	7.1.1.2.2	8.1.1.2.2
	审计数据分析	—	—	8.1.1.2.3
	审计数据关联分析	—	—	8.1.1.2.4
	审计报表	6.1.1.2.3	7.1.1.2.3	8.1.1.2.5
	审计报表定制	—	—	8.1.1.2.6
	审计数据备份与恢复	6.1.1.2.4	7.1.1.2.4	8.1.1.2.7
	审计数据保护	6.1.1.2.5	7.1.1.2.5	8.1.1.2.8
安全管理	安全管理策略	—	—	8.1.1.3.1
	安全管理角色	—	—	8.1.1.3.2
	安全管理权限分离	—	—	8.1.1.3.3
	安全管理操作审计	—	—	8.1.1.3.4
集中管控	设备管理	6.1.1.4.1	7.1.1.4.1	8.1.1.4.1
	设备监测	6.1.1.4.2	7.1.1.4.2	8.1.1.4.2
	设备告警	6.1.1.4.3	7.1.1.4.3	8.1.1.4.3
	设备配置管理	6.1.1.4.4	7.1.1.4.4	8.1.1.4.4
	设备资产管理	6.1.1.4.5	7.1.1.4.5	8.1.1.4.5
	设备软件升级	6.1.1.4.6	7.1.1.4.6	8.1.1.4.6
	设备运行状态管理	6.1.1.4.7	7.1.1.4.7	8.1.1.4.7
	设备安全策略管理	—	—	8.1.1.4.8
资源监控	性能监测	6.1.1.5.1	7.1.1.5.1	8.1.1.5.1
	网络拓扑监测	6.1.1.5.2	7.1.1.5.2	8.1.1.5.2
安全标记		—	7.1.2.1	8.1.2.1
授权管理		—	7.1.2.2	8.1.2.2
集中管控	安全策略管理	—	—	8.1.2.3
	安全策略冲突检测	—	—	8.1.2.4
密码保障		—	7.1.2.4	8.1.2.4
审计管理	审计数据采集	6.1.2.3	7.1.3.2.1	8.1.3.2.1
	审计数据存储管理	6.1.2.3	7.1.3.2.2	8.1.3.2.2
	审计数据分析	—	—	8.1.3.2.3
	审计数据关联分析	—	7.1.3.2.4	8.1.3.2.4

表 B.1（续）

技术要求		第一层	第一层	第一层	合作伙伴
管理接口设置要求	6.2.1	7.2.1	8.2.1	接口	第三方插件
要求	6.2.2	7.2.2	8.2.2	要求	接口安全要
	6.3.1	7.3.1	8.3.1		身份鉴别
	6.3.2	7.3.2	8.3.2		访问控制
	—	—	8.3.3		可信路径
	6.3.3	7.3.3	8.3.4		安全审计
8.3.5					
8.3.6					
8.3.7					
8.3.8					
8.3.9					
自身安全要求	剩余信息保护	—		7.3.4	
	软件容错	6.3.4		7.3.5	
	资源控制	6.3.5		7.3.6	
	入侵防范	6.3.6		7.3.7	
	数据安全	6.3.7		7.3.8	

注："—"表示不具有该项要求，"+"表示具有更高的要求。

附 录 C
（资料性附录）
归一化安全事件属性

归一化安全事件属性见表 C.1。

表 C.1 归一化安全事件属性

序号	属性	描述
1	采集器 IP	事件的采集器地址
2	采集器名称	事件的采集器名称
3	设备 IP	产生该事件的设备地址
4	设备类型	该设备的设备类型
5	设备名称	设备名称
6	接收事件时间	事件采集时间
7	归并数量	归并事件的次数
8	事件级别	事件级别
9	事件源信息	11	事件内容
10	事件目的信息	12	事件原始日志
13	事件类别	14	事件名称
15	协议	16	事件处理结果
17	事件处理时间	18	事件处理人
19	事件处理人	20	事件处理单位
21	事件处理单位	22	事件处理备注

中华人民共和国
国家标准
信息安全技术 网络安全等级保护
安全管理中心技术要求
GB/T 36958—2018
*
中国标准出版社出版发行
北京市朝阳区和平里西街甲2号(100029)
北京市西城区三里河北街16号(100045)
网址:www.spc.org.cn
服务热线:400-168-0010
2019年1月第一版
*
书号:155066·1-61703

版权专有 侵权必究