ICS 35.040
L 80

中华人民共和国国家标准

GB/T 36958—2018

引言 ……

1 范围 ……

2 规范性引用文件 ……

3 术语和定义 ……

4 缩略语 ……

5 [illegible]

5.1 总体说明 ……

5.2 功能描述 ……

6 第二级安全管理中心技术要求 ……

6.1 功能要求 ……

6.2 [illegible]

6.3 自身安全要求 ……

[illegible]

7.1 功能要求 ……

7.2 接口要求 ……

7.3 自身安全要求 ……

[illegible]

8.1 功能要求 ……

8.2 [illegible]

8.3 自身安全要求 ……

[illegible]

前　言

本标准按照 GB/T 1.1—2009 给出的规则起草。

[illegible]

[illegible]

[illegible]

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

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 32918(所有部分)　信息技术　SM2椭圆曲线公钥密码算法

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

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

3.2

采集器　collector

3.3

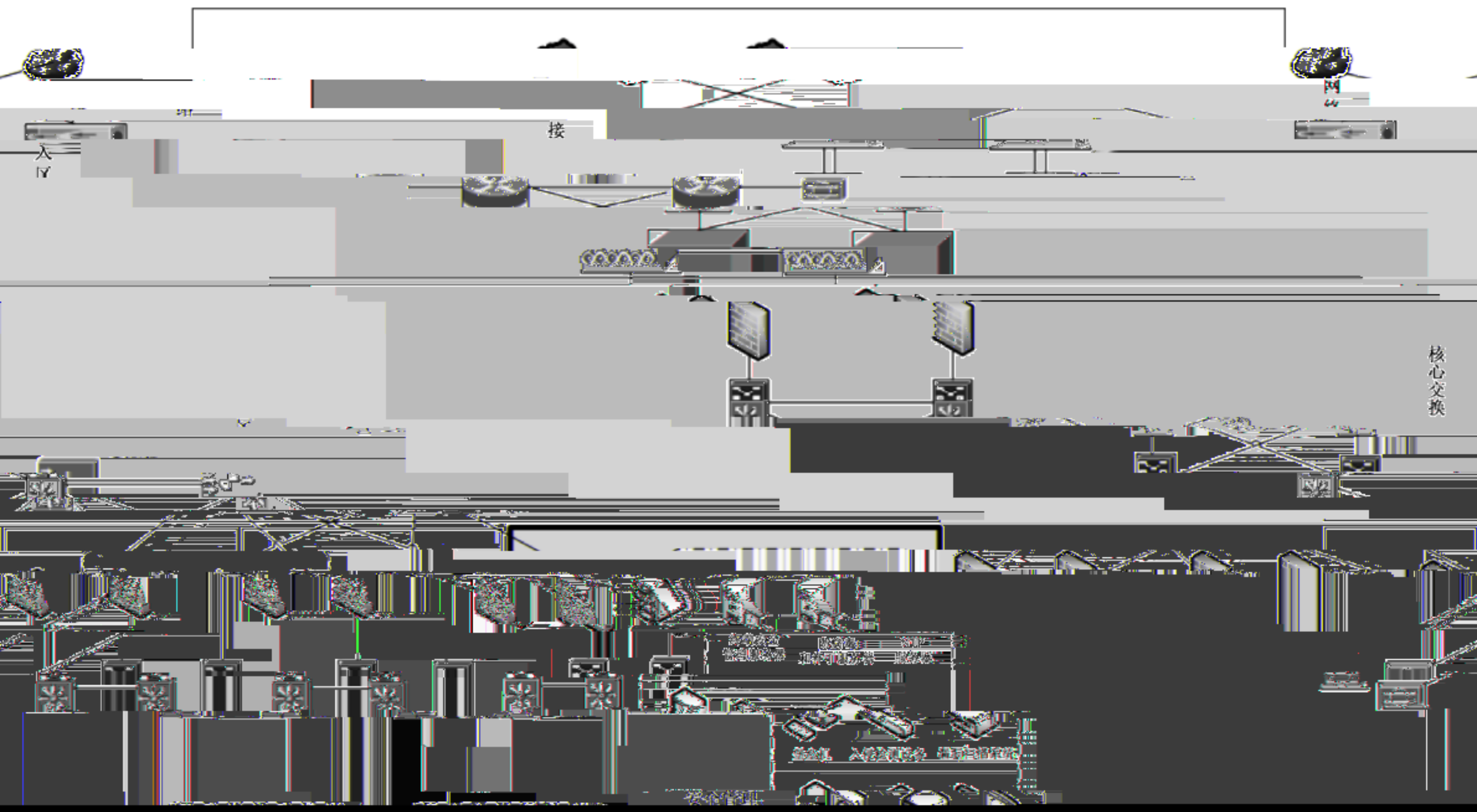
安全管理中心　security management center

4　缩略语

下列缩略语适用于本文件。

CPU　中央处理器(Central Processing Unit)

IP	互联网协议(Internet Protocol)
[illegible]	[illegible]
IP-6	互联网协议第六版(Internet Protocol Version 6)


接
入
网
核心交换

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

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：

6.1.1.4.2 威胁管理

6.1.1.4.3 脆弱性管理

6.1.1.4.4 风险分析

6.1.1.5 资源监控

6.1.1.5.1 可用性监测

可用性监测应满足以下要求：

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

审计策略集中管理应能查看主机操作系统、

6.1.2.2 审计数据集中管理

6.1.2.2.1 审计数据采集

审计数据采集应满足以下要求：

6.1.2.2.2 审计数据采集对象

审计数据采集对象应满足以下要求：

d) 支持安全设备（如防火墙、入侵检测系统、流量控制

6.1.2.2.3 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

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

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：

7.1.1.2 数据保护

7.1.1.2.1 数据保密性

7.1.1.2.2 数据完整性

数据完整性应满足以下要求：

a) 能够检测到被管理对象鉴别信息、配置管理数据在传输过程中完整性受到破坏，**并在检测到完整性错误时采取必要的恢复措施**；

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 [illegible]

7.1.3.1 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、路径等信息；

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) [illegible]

b) [illegible]

c) 具备高级定制安全事件告警规则、告警级别、告警方式的能力；

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，通告内容应包括通告内容、描述信息[illegible]

c) [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：

7.1.1.3 [illegible]

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：

[illegible]

7.1.1.4.2 [illegible]

7.1.1.4.3 威胁管理

威胁管理应满足以下要求：

[illegible]

7.1.1.4.5 风险分析

风险分析应满足以下要求：

[illegible]

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：

[redacted]

[redacted]

[redacted]

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

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

7.2.2 接口安全要求

接口安全要求应满足以下要求:

7.3 自身安全要求

7.3.1 身份识别

安全管理中心控制台的管理员身份鉴别应满足以下要求:

7.3.2 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:

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) 应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、

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：

7.3.5 软件容错

安全管理中心控制台

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；

d) 能够对单个管理员账户的多重并发会话进行限制；

e) 应提供对审计记录的监测，应能够对排序查询或者审计记录的最小值、最大值进行检测和报警。

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) 能够检测到对各服务器、网络设备和安全设备进行入侵的行为，并在发生严重入侵事件时提供报警；

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：

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]

8.1.1.2.3 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；

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

b) 能够提供与第三方系统的数据采集接口，发送或接收安

8.1.1.3.2 安全事件告警

安全事件告警应满足以下要

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

问权限管理、网络访问权限管理、应用访问

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；

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

[redacted]

审计数据采集应满足以下要求：

[redacted]

[redacted]

[redacted]

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)

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

a) 提供专用的登录控制模块对管

8.3.2 访问控制

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

[illegible]

第五级安全管理中心技术要求另行制定。

[illegible]理中心技术要求

[illegible]理中心应满足以下要求：

[illegible]跨定级系统安全管理

[illegible]

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

级别	网络安全等级保护对象等级	安全管理中心
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）

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
用户身份管理	6.1.1.1	7.1.1.1	8.1.1.1
数据保密性	6.1.1.2.1	7.1.1.2.1	8.1.1.2.1
数据保护	6.1.1.2.2	7.1.1.2.2	8.1.1.2.2
数据备份与恢复	6.1.1.2.3	7.1.1.2.3	8.1.1.2.3
可信路径	—	—	8.1.1.2.4
剩余信息保护	—	7.1.1.2.4	8.1.1.2.5
安全事件采集	6.1.1.3.1	7.1.1.3.1	8.1.1.3.1
安全事件告警	6.1.1.3.2	7.1.1.3.2	8.1.1.3.2
事件关联分析	—	7.1.1.3.4	8.1.1.3.4
统计分析报表	6.1.1.3.4	7.1.1.3.5	8.1.1.3.5
资产管理	6.1.1.4.1	7.1.1.4.1	8.1.1.4.1
资产业务价值评估	—	7.1.1.4.2	8.1.1.4.2
威胁管理	6.1.1.4.2	7.1.1.4.3	8.1.1.4.3
脆弱性管理	6.1.1.4.3	7.1.1.4.4	8.1.1.4.4
风险分析	6.1.1.4.4	7.1.1.4.5	8.1.1.4.5
资源监控	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
安全策略管理	—	7.1.2.3	8.1.2.3
密码保障	—	7.1.2.4	8.1.2.4
集中管控	—	7.1.2.5	8.1.2.5
审计数据采集	6.1.2.2.1	7.1.3.2.1	8.1.3.2.1
审计数据存储保护	6.1.2.2.2	7.1.3.2.2	8.1.3.2.2
审计分析	6.1.2.2.3	7.1.3.2.3	8.1.3.2.3
审计浏览	6.1.2.2.4	7.1.3.2.4	8.1.3.2.4
审计数据关联分析	—	7.1.3.2.5	8.1.3.2.5

表 B.1（续）

技术要求		第一级	第二级	第三级
安全管理接口设置要求	6.3.1.1	7.3.1.1	8.3.1.1	接口
安全要求	6.3.2.1	7.3.2.1	8.3.2.1	要求
身份鉴别	6.3.1	7.3.1	8.3.1	身份鉴别
访问控制	6.3.2	7.3.2	8.3.2	访问控制
可信路径	—	—	8.3.3	可信路径
安全审计	6.3.3	7.3.3	8.3.4	安全审计
剩余信息保护	—	—	8.3.5	剩余信息保护
通信完整性	6.3.4	7.3.4	8.3.6	通信完整性
通信保密性	6.3.5	7.3.5	8.3.7	通信保密性
抗抵赖	6.3.6	7.3.6	8.3.8	抗抵赖
数据安全	6.3.7	7.3.7	8.3.9	数据安全

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	设备类型
5	设备名称	设备名称
6	接收事件时间	接收事件时间
7	[illegible]	[illegible]
8	[illegible]	[illegible]
9	[illegible]	[illegible]
10	[illegible]	[illegible]
11	[illegible]	[illegible]
12	[illegible]	[illegible]
13	[illegible]	[illegible]
14	[illegible]	[illegible]
15	[illegible]	[illegible]
16	[illegible]	[illegible]
17	[illegible]	[illegible]
18	[illegible]	[illegible]
19	[illegible]	[illegible]
20	[illegible]	[illegible]
21	[illegible]	[illegible]

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

2018年12月第一版

*

书号:155066·1-61703

版权专有 侵权必究