ICS 35.040
L 80

中华人民共和国国家标准

GB/T 36958—2018

目次

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

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

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

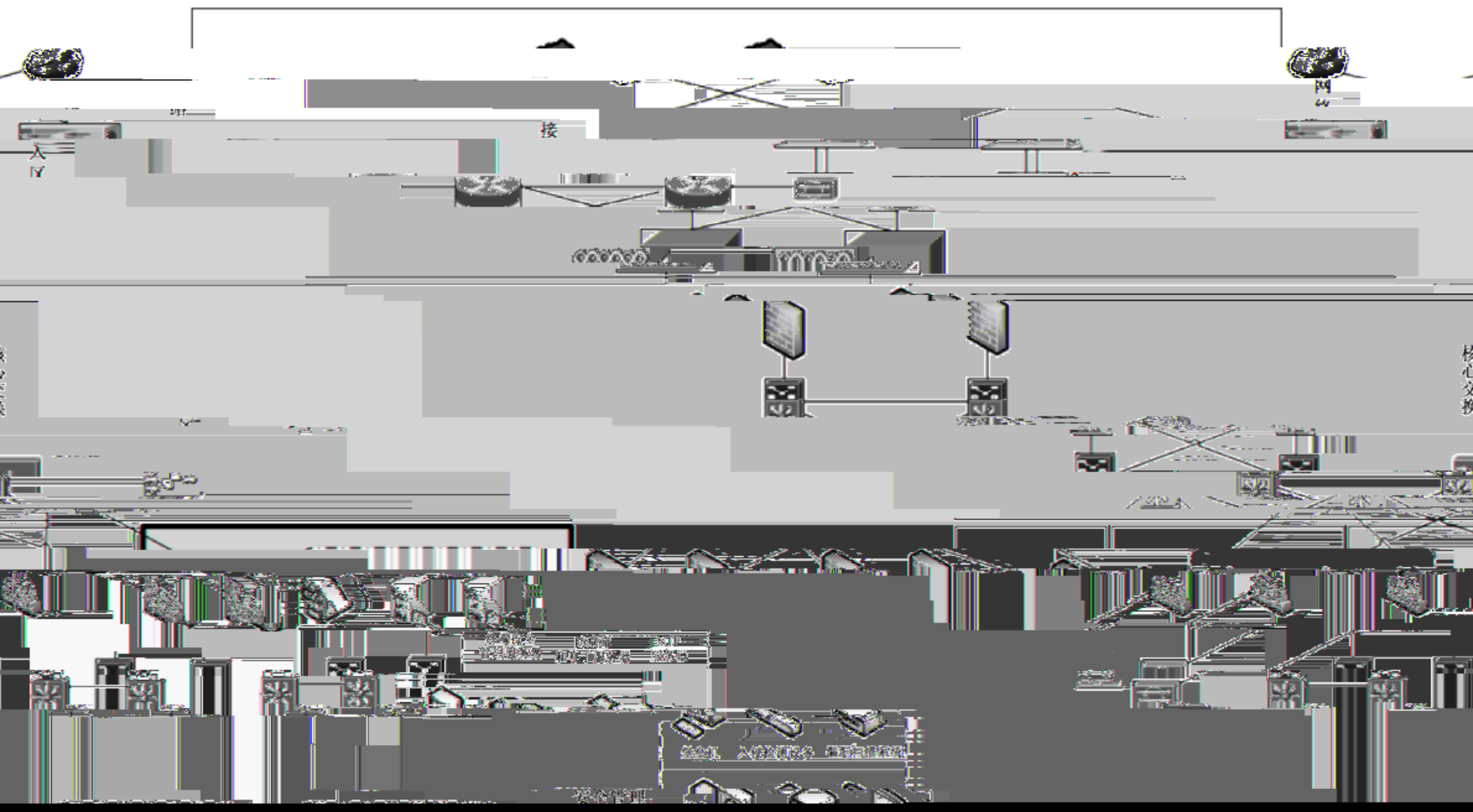
下列缩略语适用于本文件。

CPU　中央处理器(Central Processing Unit)

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

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

IP	互联网协议(Internet Protocol)
[illegible]	[illegible]
IP-6	[illegible]



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

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

应满足以下要求：

[illegible]……能够根据安全事件……或……事件关联……

CVE 编号影响的操作系统等；

[illegible]

6.1.1.3.4 统计分析报表

统计分析报表应满足以下要求：

a) 能够按照时间、事件类型等条件对安全事件进行查询；

b) 能够提供统计分析和报表生成功能。

6.1.1.4 风险管理

6.1.1.4.1 资产管理

资产管理应满足以下要求：

a) 实现对被管理对象资产的管理，提供资产的添加、修改、删除、查询与统计功能；

b) 资产管理信息应包含资产名称、资产IP地址、资产类型、资产责任人、资产重要性等信息[illegible]；

c) 支持资产属性的自定义；

d) 支持手工录入资产信息或基于指定模板的批量资产导入。

6.1.1.4.2 威胁管理

威胁管理应满足以下要求：

a) 具备预定义的安全威胁分类；

b) 支持用户对安全威胁分类[illegible]，能够[illegible]安全事件[illegible]威胁等。

6.1.1.4.3 脆弱性管理

脆弱性管理应[illegible]，支持漏洞的[illegible]及更新。

6.1.1.4.4 风险分析

风险分析应满足以下要求：

a) 能够根据资产的重要性、资产当前面临的安全威胁和资产的脆弱性计算资产的安全风险；

b) 安全风险的计算周期和计算公式能够根据部署环境的实际需要通过修改配置的方式进行调整；

c) [illegible]

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：

a) 支持通过监测网络设备、安全设备、主机、数据库等的[illegible]，实时了解其可用性状况；

b) [illegible]

[illegible]

6.1.1.5.2 网络拓扑监测

网络拓扑监测应满足以下要求：

[illegible]

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够查看主机操作系统、数据库系统、网络设备、安全设备的审计策略配置[illegible]

[illegible]

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：

[illegible]

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：

[illegible]

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

第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 Service

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]

[illegible]

7.1.1.3 [illegible] 7.1.1.3 安全事件管理

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]

[illegible]

[illegible]

[illegible]

b) [illegible]

[illegible]

c) 安全事件描述应包括时间[illegible]

[illegible]

d) [illegible]

[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：

[illegible]

[illegible]

[illegible]

[illegible]

[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) [illegible]

[illegible]

c) [illegible]

[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]

7.1.3.5 统计分析报表

险管理

7.1.1.4 风险

资产管理

7.1.1.4.1 资

理应满足以下要求：

资产管理

7.1.1.4.3 威胁管理

威胁管理应满足以下要求：

a) 支持自定义安全威胁分类；

b) 支持自定义安全威胁分类，如将已发生的安全事件对应的威胁设置为资产面临的威胁。

7.1.1.4.5 风险分析

风险分析应满足以下要求：

b) 安全风险的计算周期和计算公式能够根据部署环境的实际需要通过修改配置的方式调整；

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：

c) 支持对监测网络设备、安全设备、主机操作系统、数据库系统等重要组件进行监测，实时了解其运行状态；

[illegible]

[illegible]

7.1.1.5.1 [illegible]

工业控制系统中应能够对工业控制系统设备的可用性和安全性进行实时监测，可以对监控指标设置告警阈值，触发告警并记录。

7.1.1.5.2 网络拓扑监测

网络拓扑监测应满足以下要求：

a) 支持对网络拓扑图进行在线编辑，允许手工添加或删除监测节点或链路；

b) 能够展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、网络资源统计分析等指标；

c) 在网络运行出现异常时，能够展现当前网络拓扑图中的告警信息；

[illegible]

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) [illegible]

[illegible]

b) 安全标记信息[illegible]

[illegible]

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) [illegible]

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[illegible]

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

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)

b)

7.3 自身安全要求

7.3.1 身份类别

安全管理中心控制台的管理员身份类别应满足以下要求:

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:

a)

b)

c)

d) 实现特权用户的权限分离,应将系统

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、描述和结果；

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保证管理员的鉴别信息所在的存储空间被释放或再分配给

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：

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；

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

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) 应采用校验技术保证重要数据在传输过程中的完整性，包括但不限于鉴别数据、重要业务数据、

b) 应采用密码技术保证重要数据在存储过程中的完整性，包括但不限于鉴别数据、重要业务数据、

c) 应采用密码技术保证重要数据在传输过程中的保密性，包括但不限于鉴别数据、重要业务数据、

d) 应采用密码技术保证重要数据在存储过程中的保密性，包括但不限于鉴别数据、重要业务数据、

e) 应对重要数据提供备份和恢复措施，实时备份重要业务系统数据、业务数据库系统数据、审计数

f) 应提供重要数据处理系统的热冗余，保证系统的高可用性；

g) 应提供关键网络设备、通信线路和数据处理系统的硬件冗余，保证系统的高可用性；

h) 应提供主要网络设备、通信线路和数据处理系统的软件冗余，保证系统的高可用性；

i) 应提供重要计算节点设备的硬件冗余，保证节点的高可用性；

j) 应提供重要网络设备的虚拟冗余，保证网络的高可用性；

k) 应提供重要存储设备的冗余阵列，保证存储的高可用性；

l) 应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地；

m) 应提供重要数据处理系统的异地灾难恢复功能，当本地系统发生重大灾难事件时，可以在异地

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

8.1.1.2.4 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；

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：

e) 支持资产属性的自定义；

d) 支持手工录入资产记录或基于指定模板的批量资产导入；

e) 支持对资产的自动发现，并能够将其自动添加到资产库中。

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：

a) 具备预定义的安全威胁分类；

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

[redacted]

[redacted]

8.1.1.5 资源监控

8.1.1.5.1 可用性监测

可用性监测应满足以下要求：

[redacted]

8.1.1.5.2 网络拓扑监测

网络拓扑监测应满足以下要求：

[redacted]

8.1.2 安全管理要求

8.1.2.1 安全标记

安全标记应满足以下要求：

[redacted]

访问权限管理、网络访问权限管理、应用访问

理

策略

以下要求：

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

b) 支持通过 agent 等方式采集各种操作系统、数据库、中间件、应用系统等的审计数据；

c) 支持对网络设备、安全设备、服务器、操作站等

d) 在工业控制系统中，应对工业控制现场控制设备、网络安全设备、网络设备的网络安全监控和报警、网络安全日志信息进行集中管理。

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

8.1.3.4 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。

8.1.3.5 审计数据关联分析

审计数据关联分析应满足以下要求：

求

方插件/代理接口协议要求

议要求应满足以下要求：

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 接口要

接口协议

a) 安全

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]接口之间的[illegible]；

c) 各接口之间进行通信时，应通过身份验证

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

a) 提供专用的登录控制模块对管理员进行身

实现；

足以下要求：

身份标识和鉴别，对同一管理员用户采用两种或两种

问控制

8.3.3 可信路径

安全管理中心控制台的可信路径应满足以下要求

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

误时采取必要的恢复措施。

[illegible]

[illegible]

[illegible]

9 第五级系统安全管理中心技术要求

第五级安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：

a) [illegible]

b) [illegible]

c) [illegible]

[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
数据完整性	6.1.1.2.2	7.1.1.2.2	8.1.1.2.2
数据保护	6.1.1.2.3	7.1.1.2.3	8.1.1.2.3
数据备份与恢复	—	—	8.1.1.2.4
可信路径	—	7.1.1.2.4	8.1.1.2.5
剩余信息保护	6.1.1.3.1	7.1.1.3.1	8.1.1.3.1
安全事件采集	6.1.1.3.2	7.1.1.3.2	8.1.1.3.2
安全事件告警	—	7.1.1.3.3	8.1.1.3.3
集中关联分析	—	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	监控性检测	6.1.1.5.1	7.1.1.5.1
	网络拓扑监测	6.1.1.5.2	7.1.1.5.2
安全标记	—	7.1.2.1	8.1.2.1
授权管理	—	7.1.2.2	8.1.2.2
安全管理策略	—	7.1.3.1	8.1.3.1
集中管控	安全策略管理	—	7.1.3.2
	终端接入控制	—	8.1.3.2
密码保障	—	7.2.1	8.2.1
可信验证	6.2.2.1	7.2.2.1	8.2.2.1
可信数据采集	—	—	8.2.3.1
可信数据传输	—	—	8.2.3.2
可信数据处理	—	—	8.2.3.3
可信数据交换	—	—	8.2.3.4

表 B.1（续）

技术要求	第一级	第二级	第三级
与管理接口的设要求	6.3.1.1	7.3.1	8.3.1
要求	6.3.2	7.3.2	8.3.2
	6.3.1	7.3.1	8.3.1
	6.3.2	7.3.2	8.3.2
	—	—	8.3.3
自身 要求	6.3.3	7.3.3	8.3.4
安全 机制策略的动态管理	—	—	8.3.5
要求 软件容错	6.3.4	7.3.4	8.3.6
资源控制	6.3.5	7.3.5	8.3.7
人侵防范	6.3.6	7.3.6	8.3.8
数据安全	6.3.7	7.3.8	8.3.9

第一级	第二级	第三级
接口	第三方软件	
要求	接口安全要	
身份鉴别		
访问控制		
可信路径		
安全审计		

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	产生该事件的设备的设备类型
5	设备名称	设备名称
6	事件采集时间	接收事件时间
[illegible]	[illegible]	[illegible]
11	事件内容	事件原始信息
[illegible]	[illegible]	[illegible]
14	[illegible] IP	[illegible]
15	[illegible]	[illegible]
16	目的主机名	[illegible]
[illegible]	[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