



# 中华人民共和国国家标准 中华人民共和国

GB/T 36958—2018



信息安全技术 信息安全技术

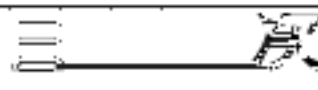
信息安全技术 信息安全技术

requirements of security

Information security technology—Technical require

Level security

management center for classified information



.....	II	引言 .....	2
.....	1	1 范围 .....	2
.....	1	2 规范性引用文件 .....	3
.....	1	3 术语和定义 .....	3
.....	1	4 缩略语 .....	2
5 安全管控中心概述 .....	2	5.1 总体说明 .....	2
5.1 总体说明 .....	2	5.2 功能描述 .....	3
5.2 功能描述 .....	3	6 第二级安全管理中心技术要求 .....	3
6 第二级安全管理中心技术要求 .....	3	6.1 功能要求 .....	3
6.1 功能要求 .....	3	6.2 接口要求 .....	8
6.2 接口要求 .....	8	6.3 自身安全要求 .....	13
6.3 自身安全要求 .....	13	7.1 功能 .....	13
7 安全管理中心技术要求 .....	13	7.2 接口 .....	13
7.1 功能 .....	13	7.3 自身 .....	13
7.2 接口 .....	13	8 第二级安全管理中心技术要求 .....	13
7.3 自身 .....	13	8.1 功能 .....	13
8 第二级安全管理中心技术要求 .....	13	8.2 接口 .....	13
8.1 功能 .....	13	8.3 自身安全要求 .....	21
8.2 接口 .....	13		
8.3 自身安全要求 .....	21		

# 前 言

本标准按照 GB/T 1.1—2009 给出的规则起草。

本标准由

## 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—2018 信息安全技术 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—2010 信息安全技术 术语

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。

术语

3.1

术语和定义

3.2

采集器 collector

3.3

安全管理中心

## 4 缩略语

缩略语适用于本文件。

中央处理器(Central Processing Unit)

下列缩

CPU

集中管理基础设备

集中管

Service

集中管

## IP 互联网协议(Internet Protocol)

IP 互联网协议(Internet Protocol) 是网络层的核心协议，负责将数据包从源主机发送到目的主机。它定义了数据包的格式和传输规则。IP 地址是标识网络中设备的唯一地址，分为 IPv4 和 IPv6 两种版本。IP 地址的表示方法为点分十进制，例如 192.168.1.1。IP 地址的分配由 IANA 负责，分为公有 IP 地址和私有 IP 地址。公有 IP 地址可以在互联网上路由，而私有 IP 地址只能在局域网内使用。IP 地址的分配遵循一定的规则，例如私有 IP 地址的范围是 10.0.0.0/8、172.16.0.0/12 和 192.168.0.0/16。



能够通过管理对象的名称管理員进行再鉴别,并对身份标识信息进行有效鉴别。

6.1.1

6.1.1.2 数据保护

6.1.1.2.1 数据保密性

数据保密性应满足以下要求:

- a) 应在安全管理策略中明确规定管理对象的鉴别信息,并应通过鉴别信息对管理对象进行鉴别;
- b) 应使用加密技术对安全管理策略中鉴别信息进行加密。

6.1.1.2.2 数据完整性

数据完整性应满足以下要求:

2.3 数据备份与恢复

6.1.1.

数据备份与恢复应满足以下要求:

- a) 提供数据本地备份及恢复功能,数据备份应至少每天一次,备份应异地存放;
- b) 应制定数据备份及恢复策略,策略应明确备份数据的范围、备份周期、备份介质、备份位置、备份方式、恢复流程等。

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:

- a) 应支持安全事件实时采集及存储;
- b) 应支持安全事件按策略采集,并能对采集到的安全事件进行关联分析;
- c) 应支持安全事件按策略采集,并能对采集到的安全事件进行关联分析;

安全事件采集应满足以下要求:

- c) 能够对采集的安全事件原始数据进行集中存储。

注:安全事件的属性可参考附录 C。

1.1.3.2 安全事件告警

6.

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。

1.1.3.3 安全事件响应

6.

安全事件响应应满足以下要求:

- a) 应支持安全事件按策略采集,并能对采集到的安全事件进行关联分析;

系统的安全策略... 系统能够安全地... 系统能够安全地... 系统能够安全地...

6.1.1.4 统计与报表

统计与报表应满足以下要求：

统计与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) 能够进行统计分析和报表生成功能。

6.1.1.4 资产管理

6.1.1.4.1 资产管理

资产管理应满足以下要求：

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；
- 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、资产位置等属性；
- c) 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导入。

6.1.1.4.2 威胁管理

威胁管理应满足以下要求：

威胁管理应满足以下要求：

- a) 具备预定义的安全威胁分类；

威胁管理应支持自定义安全威胁分类，能够将发生的安全事件对应的威胁类型与资产类型的威胁...

6.1.1.4.3 脆弱性管理

脆弱性管理应满足以下要求：

脆弱性管理应支持创建并维护脆弱性检测列表，支持脆弱性列表的合并及更新。

6.1.4 风险分析

6.1.1.4

风险分析应满足以下要求：

风险分析应支持对资产、资产属性、资产类型、资产位置、资产责任人、资产位置等属性进行风险评估。

风险分析应支持对资产、资产属性、资产类型、资产位置、资产责任人、资产位置等属性进行风险评估。

风险分析的计算规则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配置。

风险分析的计算规则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配置。

6.1.1.5 来源监控

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、主机操作系统、数据库、中间件、应用系统等重要性资源的健康状态；



## 6.2 接口要求

### 6.2.1 第三方插件/代理接口协议要求

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以及第三方的插

### 6.2.2 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；

## 6.3 身份鉴别

### 6.3.1 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下要求：

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) 提供管理员账号身份标识唯一性和鉴别信息重复度检查功能，保证不存在重复用户名身份标识。

### 6.3.2 访问控制

安全管理中心控制台访问控制应满足以下要求：

c) 应授权管理员配置访问控制策略，并禁止默认账号的访问。

## 6.3 安全审计

6.3

安全管理中心控制台的安全审计应满足以下要求：

a) 应记录每个管理操作的安全审计数据，记录数据管理应能对重要操作和变更操作进行审计。

b) 应记录每个管理操作的安全审计数据，记录数据管理应能对重要操作和变更操作进行审计。

c) 应提供审计数据的查询、统计、导出、打印、分析等功能，并能生成审计报告。

d) 应提供审计数据的备份、恢复、删除等功能。

### 6.3.4 软件容错

安全管理中心控制台软件容错应满足以下要求：

a) 应支持容错功能，当系统发生故障时，应能够自动恢复。

输入

## 6.3.5 资源控制

6.3.5

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

安全管理中心对操作的数据安全应满足以下要求：

- 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，并在检测完整性错误时采取必要的恢复措施；
- b) 能够检测到被管理对象鉴别信息、配置管理数据在存储过程中完整性受到破坏，并在检测完整性错误时采取必要的恢复措施；
- c) 采用密码技术或其他保护措施实现鉴别信息、配置管理数据在传输和存储过程中的机密性；

中心技术要求

## 7 第三级安全管理中心

### 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：

- 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，并在检测完整性错误时采取必要的恢复措施；
- b) 能够检测到被管理对象鉴别信息、配置管理数据在存储过程中完整性受到破坏，并在检测完整性错误时采取必要的恢复措施；
- c) 采用密码技术或其他保护措施实现鉴别信息、配置管理数据在传输和存储过程中的机密性；

##### 7.1.1.2 数据保护

###### 7.1.1.2.1 数据保密性

数据保密性应满足以下要求：

###### 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，并在检测完整性错误时采取必要的恢复措施；
- b) 能够检测到被管理对象鉴别信息、配置管理数据在存储过程中完整性受到破坏，并在检测完整性错误时采取必要的恢复措施；

到完

到完

### 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，安全数据备份至少每天一次，备份介质异地存放；

### 7.1.1.2.4 剩余信息

### 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) 采集安全事件应覆盖网络安全设备告警和入侵检测系统告警等；
- b) 采集的安全事件应包含事件发生时间、事件类型、结果、IP地址、端口等信息；
- c) 安全事件的采集应符合国家网络安全等级保护基本要求；
- d) 安全事件采集应符合国家网络安全等级保护基本要求；
- e) 安全事件的采集应符合国家网络安全等级保护基本要求；

#### 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) 告警信息应包含事件发生时间、事件类型、结果、IP地址、端口等信息；
- b) 告警信息应包含事件发生时间、事件类型、结果、IP地址、端口等信息；
- c) 告警信息应包含事件发生时间、事件类型、结果、IP地址、端口等信息；

#### 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，支持基于告警响应的工单管理；
- b) 能够提供安全通告功能，可以创建或导入安全通告；
- c) 能够根据安全通告提示的安全风险等级进行风险评估；

#### 7.1.1.3.4

安全事件分析应满足以下要求：

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：

a) 支持资产属性的自定义；

b) 支持资产归属关系的数据关联和报表生成；

7.1.1.4.2 资产价值评估

资产价值评估应满足以下要求：a) 支持资产价值评估模型的自定义；b) 支持资产价值评估模型与资产属性的关联；c) 支持资产价值评估模型与资产归属关系的关联；d) 支持资产价值评估模型与资产报表的关联。

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

下要求：

风险分析应满足以

a) 支持风险分析模型的自定义；b) 支持风险分析模型与资产属性的关联；c) 支持风险分析模型与资产归属关系的关联；d) 支持风险分析模型与资产报表的关联。

e) 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相应调整；

f) 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相应调整。

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：

...设备、应用系统、应用系统重要性能指标、...

...了解其运行状态、...

...设备运行、故障报警、...

...设备运行、故障报警、...

...设备运行、故障报警、...应能够对...设备运行、故障报警、...指标报警、预警、...

7.1.1.5 网络拓扑监测

以下要求：

网络拓扑监测应满足

...支持在线编辑，允许手工增加或删除监测节点或链路；

a) 支持对网络拓扑

...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

b) 能够呈现当前网

...网络流量统计分析等指标；

态，如网络流量

...在网络运行中出现异常时，能够及时发现当前网络拓扑图中异常设备警告；

7.1.2 安全管理要求

7.1.2.1 安全标记

以下要求：

安全标记应满足

...能够对网络中关键设备(包括网络设备、安全设备、服务器主机等)和链路的运行状

a) 支持对网络拓扑

...能够在网络运行中出现异常时，能够及时发现当前网络拓扑图中异常设备警告；

b) 能够呈现当前网

...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

c) 标记属性应包括安

...安全级别的系统中安全标记与安全属性的单一映射关系。

d) 能够实现对不同安

7.1.2.2 授权管理

以下要求：

授权管理应满足以下要

...所能访问范围的统一管理；

a) 实现对每一个标记

...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

b) 实现主体对客体访

...标记和客体标记安全级别应不同，制定访问控制策略，控制主体对客体的访问

c) 实现根据主体标

理

7.1.2.3 设备策略管

策略

7.1.2.3.1 安全配置

...设备运行、故障报警、...应能够对...设备运行、故障报警、...指标报警、预警、...

设备管理应实现

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

审计数据采集方式应满足以下要求:

- a) 通过数据库审计、Syslog、SNMP等方式采集各系统或设备产生的审计数据;
- b) 通过统一接口采集被管理对象的安全事件数据。

### 7.1.3.2.4 审计数据关联分析

审计数据关联分析方式应满足以下要求:应能对采集到的审计数据进行关联分析,发现异常行为和异常事件,并及时告警。

## 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:

接口协议要求应满足以下要求:应能支持第三方插件/代理接口协议,并能与第三方系统对接。

### 7.2.2 接口安全要求

接口安全要求应

应满足以下要求:

- a) 采用安全协议,保证接口之间交互数据的完整性;
- b) 采用加密技术保证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

安全管理中心控制台的管理人员身份鉴别应满足以下要求:

安全管理中心

应采用符合GB/T 17945-2009要求的身份鉴别技术,并能与第三方系统对接。

应采用符合GB/T 17945-2009要求的身份鉴别技术,并能与第三方系统对接。

### 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) 采用自主可控的身份鉴别技术,并能与第三方系统对接;
- b) 自主可控的身份鉴别技术,并能与第三方系统对接。

应实现特权用户账号限制,应禁止未授权用户对系统进行操作,并能与第三方系统对接。

### 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) 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和安全事件进行的操作；
- 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) 审计记录的结果至少应包含事件发生时间、时间戳、发起者信息、资源、地址

### 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敏感信息在发生有效会话结束或

### 7.3.5 软件容错

安全管理中心控制台应提供容错能力，当发生异常时，应能自动恢复或报警。

- a) 当管理员在一段时间内未作任何操作时，应能自动结束会话；
- b) 能够对最大并发会话连接数进行限制；
- c) 能够对会话连接数进行实时监控，当连接数达到预设阈值时，应能自动报警。

### 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) 能够对管理员登录地址进行限制；
- b) 当管理员在一段时间内未作任何操作时，应能自动结束会话；
- c) 能够对最大并发会话连接数进行限制；
- d) 能够对会话连接数进行实时监控，当连接数达到预设阈值时，应能自动报警。

### 7.3.7 入侵防范

### 安全管理中心控制台的安全审计应满足以下要求：

### 7.3.8 数据备份

安全管理中心控制台的数据备份应满足以下要求：

## 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；

##### 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：

数据完整性应满足以下要求：

- a) 能够检测到被管理对象中的异常信息，并对管理对象中异常信息的主要特征进行识别和定位，完成由异常信息采取的恢复措施；
- b) 能够对识别到的被管理对象中的异常信息的主要特征进行识别和定位，完成由异常信息采取的恢复措施；
- c) 对重要通信提供专用通信协议或安全通信协议服务，避免来自通用通信协议的攻击破坏。

###### 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：

- a) 提供数据本地备份与恢复功能，完全数据备份至少每五一次，备份介质异地存放。

- b) 提供异地实时备份功能，利用通信网络将数据实时备份至灾难备份中心。

中华人民共和国境内,禁止从境外对接由云计算平台的运维。

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;

## 3 安全事件响应

### 8.1.1.3

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：

支持关联分析事件序列，并能识别和关联异常事件。

支持对事件的正向和反向关联分析。

支持对事件的正向和反向关联分析。

支持对事件的正向和反向关联分析。

支持对事件的正向和反向关联分析。

### 8.1.1.3.5 统计分析报表

统计分析报表应满足以下要求：

支持按时间段、事件类型、设备、用户等进行统计。

支持对统计结果进行分析和报表生成。

### 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：

- a) 支持对资产的分类和定义；
- b) 支持对资产的发现和识别；
- c) 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

支持对资产的分类和定义，支持对资产的发现和识别，支持对资产的自动发现，并能够将其自动添加到资产库中。

#### 8.1.1.4.3 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；

支持对威胁的分类和定义，支持对威胁的发现和识别，支持对威胁的自动发现，并能够将其自动添加到威胁库中。

#### 8.1.1.4.4 脆弱性管理

脆弱性管理应满足以下要求：

支持对脆弱性的发现和识别，支持对脆弱性的自动发现，并能够将其自动添加到脆弱性库中。

8.1.1.4.5 风险分析

风险分析应满足以下要求：

- a) 能够对重要资产的安全威胁、攻击场景的成因和攻击后果进行安全风险评估，并评估对业务的影响；
- b) 能够对安全威胁、攻击场景的成因和攻击后果进行安全风险评估，并评估对业务的影响；
- c) 安全管理系统能够以图形化的方式展现当前资产和安全域的风险等级、当前风险的排名等。

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：

- a) 支持通过探测网络设备、服务器、主机、操作系统、数据库、中间件、应用系统等重要性能指标，

8.1.1.5.2 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) 在网络运行过程中能够实时反映当前网络拓扑图变更；
- c) 能够对网络中断、设备故障、设备下线等异常事件进行告警；
- d) 能够在指定网络范围内进行拓扑发现并自动生成网络拓扑图。

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：

- a) 能够对主/客体的安全标记统一管理，客体标记范围包括用户、代理进程、终端等

8.1.2.2 授权管理

8.1.2.2.1 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；
- c) 实现根据主体标记和客体标记安全级别的不同,制定访问控制策略,控制

权限管理、应用访问

主体对客体的访问,

软件进行授权

8.1.2.3 设备策略管理

8.1.2.3.1 安全配置策略

设备管理应满足以下要求：

- a) 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

策略的统一查询;

8.1.2.3.2 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防

入侵防御的事件采集、接收和命令下发;

8.1.2.3.3 恶意代码防范

8.1.2.4 密码保障

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：

- a) 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情况,有权策略且不
- b) 能够查看对主机操作系统、数据库系统、网络设备、安全设备的审计策略的统一配置管理

8.1.3 审计管理要求

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) 与审计对象相关的信息流、业务流、数据流、控制流、管理流、决策流、异常流、告警流、事件流、日志流、操作流、配置流、策略流、策略集、策略规则、策略引擎、策略执行、策略验证、策略更新、策略备份、策略恢复、策略迁移、策略分发、策略同步、策略冲突检测、策略冲突解决、策略冲突预防、策略冲突告警、策略冲突日志、策略冲突报告、策略冲突处理、策略冲突预防、策略冲突告警、策略冲突日志、策略冲突报告、策略冲突处理

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 等协议采集各种系统或设备上的审计数据；

b) 支持通过 SNMP 或设备代理的方式采集网络设备上的审计数据。

8.1.3.2.4 数据收集组件要求

数据收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，能够在数据收集组件对数据进行本地缓存，当网络连通恢复以后，信息收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 审计数据关联分析

分析应满足以下要求：

审计数据关联分

应提供附加连接规则自定义功能；

在工业控制系统中，网络路由器应能安全且准确地识别出最小的、或最

行安全预警。

## 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) 采用安全的接口协议,保证接口之间交互数据的完整性；

间进行通信时,应通过身份验证机制相互验证对方的可信性,确保可信连接。

c) 各接口之

## 8.3 自身安全要求

### 8.3.1 身份鉴别

本控制台的管理员身份鉴别应满足以下要求：

本台的登录控制模块对管理员进行身份标识和鉴别,对同一管理员用户采用两种或两种

因素鉴别技术鉴别,且至少有一种是采用构造的复杂认证技术鉴别

安全管理中心

a) 提供专用

实现

### 8.3.2 访问控制

### 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

安全管理中心控制台对管理员进行身份鉴别时，应能够记录一条安全的信息传输路径。

### 8.3.4 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) 提供覆盖到各个管理对象的安全审计功能并记录所有管理对象重要操作和安全事件相关信息；
- 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) 审计记录的数据至少应包括事件源、事件类型、发生时间、发生地点、操作类型、操作结果等；
- d) 提供对审计记录数据进行统计、查询分析及生成审计报告的功能。

### 8.3.5 剩余信息保护

### 8.3.6 软件容错

应满足以下要求：

安全管理中心控制台的软件容错应满足以下要求：

- b) 提供自动保护功能，当故障发生时自动保护当前所有状态；
- c) 提供自动恢复功能，当故障发生时自动恢复到故障前的状态。

### 8.3.7 资源控制

应满足以下要求：

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；

对安全会话连接数进行限制；

c) 能够对最

对管理员账户的多重并发会话进行限制；

d) 能够对单

### 8.3.8 入侵防范

控制台的入侵防范应满足以下要求：

安全管理中心控制

对服务器、网络设备和安全设备进行入侵的行政事并在发生严重入侵事件时提供

能够检测到及

报警

对终端输入IP地址或网络地址范围对通过网络进行管理的管理终端进行限制

b) 能够通过设

### 8.3.9 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) 能够检测到管理数据和鉴别信息在传输和存储过程中被篡改或破坏，并在检测到篡改或破坏

及时采取必要的补救措施。

9 第五级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) 能够实施统一的安全策略，能够对跨定级系统安全管理中心提供多级跨定级系统应用；
- b) 能够对跨定级系统之间的数据流进行实时监控与审计；
- c) 能够实时监控各下级系统的安全事件，并能对安全事件进行统一分析和处理。

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

级	技术要求			第二级	第三级	第四级
6.1.1.1			用户身份管理	6.1.1.1	7.1.1.1	8.1.1.1
6.1.1.2			数据保密性	6.1.1.2.1	7.1.1.2.1	8.1.1.2.1
6.1.1.3			数据完整性	6.1.1.3.1	7.1.1.3.1	8.1.1.3.1
6.1.1.2.3.1	7.1.1.2.3.1	8.1.1.2.3.1	数据保护	6.1.1.2.3.1	7.1.1.2.3.1	8.1.1.2.3.1
		8.1.1.2.4				可信路径
	7.1.1.0.4	8.1.1.0.4				融合信息保护
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
6.1.1.3.3	7.1.1.3.3	8.1.1.3.3				系统管理
6.1.1.3.4	7.1.1.3.4	8.1.1.3.4				安全管理
6.1.1.4.1	7.1.1.4.1	8.1.1.4.1				系统管理
6.1.1.4.2	7.1.1.4.2	8.1.1.4.2				安全管理
6.1.1.4.3	7.1.1.4.3	8.1.1.4.3				风险管理
6.1.1.4.4	7.1.1.4.4	8.1.1.4.4	脆弱性管理	6.1.1.4.4	7.1.1.4.4	8.1.1.4.4
6.1.1.4.5	7.1.1.4.5	8.1.1.4.5	风险分析	6.1.1.4.5	7.1.1.4.5	8.1.1.4.5
6.1.1.5.1	7.1.1.5.1	8.1.1.5.1				资源监控
6.1.1.5.2	7.1.1.5.2	8.1.1.5.2				网络拓扑监测
7.1.2.1	8.1.2.1					安全标记
7.1.2.2	8.1.2.2					授权管理
7.1.2.3	8.1.2.3					个人信息保护
7.1.2.4	8.1.2.4					个人信息保护
7.1.2.5	8.1.2.5					个人信息保护
7.1.2.6	8.1.2.6					个人信息保护
7.1.2.7	8.1.2.7					个人信息保护
7.1.2.8	8.1.2.8					个人信息保护
7.1.2.9	8.1.2.9					个人信息保护
7.1.2.10	8.1.2.10					个人信息保护
7.1.2.11	8.1.2.11					个人信息保护
7.1.2.12	8.1.2.12					个人信息保护
7.1.2.13	8.1.2.13					个人信息保护
7.1.2.14	8.1.2.14					个人信息保护
7.1.2.15	8.1.2.15					个人信息保护
7.1.2.16	8.1.2.16					个人信息保护
7.1.2.17	8.1.2.17					个人信息保护
7.1.2.18	8.1.2.18					个人信息保护
7.1.2.19	8.1.2.19					个人信息保护
7.1.2.20	8.1.2.20					个人信息保护
7.1.2.21	8.1.2.21					个人信息保护
7.1.2.22	8.1.2.22					个人信息保护
7.1.2.23	8.1.2.23					个人信息保护
7.1.2.24	8.1.2.24					个人信息保护
7.1.2.25	8.1.2.25					个人信息保护
7.1.2.26	8.1.2.26					个人信息保护
7.1.2.27	8.1.2.27					个人信息保护
7.1.2.28	8.1.2.28					个人信息保护
7.1.2.29	8.1.2.29					个人信息保护
7.1.2.30	8.1.2.30					个人信息保护
7.1.2.31	8.1.2.31					个人信息保护
7.1.2.32	8.1.2.32					个人信息保护
7.1.2.33	8.1.2.33					个人信息保护
7.1.2.34	8.1.2.34					个人信息保护
7.1.2.35	8.1.2.35					个人信息保护
7.1.2.36	8.1.2.36					个人信息保护
7.1.2.37	8.1.2.37					个人信息保护
7.1.2.38	8.1.2.38					个人信息保护
7.1.2.39	8.1.2.39					个人信息保护
7.1.2.40	8.1.2.40					个人信息保护
7.1.2.41	8.1.2.41					个人信息保护
7.1.2.42	8.1.2.42					个人信息保护
7.1.2.43	8.1.2.43					个人信息保护
7.1.2.44	8.1.2.44					个人信息保护
7.1.2.45	8.1.2.45					个人信息保护
7.1.2.46	8.1.2.46					个人信息保护
7.1.2.47	8.1.2.47					个人信息保护
7.1.2.48	8.1.2.48					个人信息保护
7.1.2.49	8.1.2.49					个人信息保护
7.1.2.50	8.1.2.50					个人信息保护
7.1.2.51	8.1.2.51					个人信息保护
7.1.2.52	8.1.2.52					个人信息保护
7.1.2.53	8.1.2.53					个人信息保护
7.1.2.54	8.1.2.54					个人信息保护
7.1.2.55	8.1.2.55					个人信息保护
7.1.2.56	8.1.2.56					个人信息保护
7.1.2.57	8.1.2.57					个人信息保护
7.1.2.58	8.1.2.58					个人信息保护
7.1.2.59	8.1.2.59					个人信息保护
7.1.2.60	8.1.2.60					个人信息保护
7.1.2.61	8.1.2.61					个人信息保护
7.1.2.62	8.1.2.62					个人信息保护
7.1.2.63	8.1.2.63					个人信息保护
7.1.2.64	8.1.2.64					个人信息保护
7.1.2.65	8.1.2.65					个人信息保护
7.1.2.66	8.1.2.66					个人信息保护
7.1.2.67	8.1.2.67					个人信息保护
7.1.2.68	8.1.2.68					个人信息保护
7.1.2.69	8.1.2.69					个人信息保护
7.1.2.70	8.1.2.70					个人信息保护
7.1.2.71	8.1.2.71					个人信息保护
7.1.2.72	8.1.2.72					个人信息保护
7.1.2.73	8.1.2.73					个人信息保护
7.1.2.74	8.1.2.74					个人信息保护
7.1.2.75	8.1.2.75					个人信息保护
7.1.2.76	8.1.2.76					个人信息保护
7.1.2.77	8.1.2.77					个人信息保护
7.1.2.78	8.1.2.78					个人信息保护
7.1.2.79	8.1.2.79					个人信息保护
7.1.2.80	8.1.2.80					个人信息保护
7.1.2.81	8.1.2.81					个人信息保护
7.1.2.82	8.1.2.82					个人信息保护
7.1.2.83	8.1.2.83					个人信息保护
7.1.2.84	8.1.2.84					个人信息保护
7.1.2.85	8.1.2.85					个人信息保护
7.1.2.86	8.1.2.86					个人信息保护
7.1.2.87	8.1.2.87					个人信息保护
7.1.2.88	8.1.2.88					个人信息保护
7.1.2.89	8.1.2.89					个人信息保护
7.1.2.90	8.1.2.90					个人信息保护
7.1.2.91	8.1.2.91					个人信息保护
7.1.2.92	8.1.2.92					个人信息保护
7.1.2.93	8.1.2.93					个人信息保护
7.1.2.94	8.1.2.94					个人信息保护
7.1.2.95	8.1.2.95					个人信息保护
7.1.2.96	8.1.2.96					个人信息保护
7.1.2.97	8.1.2.97					个人信息保护
7.1.2.98	8.1.2.98					个人信息保护
7.1.2.99	8.1.2.99					个人信息保护
7.1.2.100	8.1.2.100					个人信息保护

表 B.1 (续)

要求	6.3.1	7.3.1	8.3.1	接口要素	第三方安全要素
代理接口协议要求	+	+	+		
要求	6.3.2	7.3.2	8.3.2		
	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	8.3.3		安全审计
安全可信连接要素					
要求					
软件容错	6.3.4	7.3.5	8.3.6		
资源控制	6.3.5	7.3.6	8.3.7		
入侵防范	6.3.6	7.3.7	8.3.8		
数据安全	6.3.7	7.3.8	8.3.9		

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

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	事件源 IP	事件源 IP 地址
8	事件源名称	事件源名称
9	事件源地址	事件源地址
10	事件源端口	事件源端口
11	事件源 IP 地址	事件源 IP 地址
12	事件源 IP 地址	事件源 IP 地址
13	事件源 IP 地址	事件源 IP 地址
14	事件源 IP 地址	事件源 IP 地址
15	事件源 IP 地址	事件源 IP 地址
16	事件源 IP 地址	事件源 IP 地址
17	事件源 IP 地址	事件源 IP 地址
18	事件源 IP 地址	事件源 IP 地址
19	事件源 IP 地址	事件源 IP 地址
20	事件源 IP 地址	事件源 IP 地址
21	事件源 IP 地址	事件源 IP 地址
22	事件源 IP 地址	事件源 IP 地址
23	事件源 IP 地址	事件源 IP 地址
24	事件源 IP 地址	事件源 IP 地址
25	事件源 IP 地址	事件源 IP 地址
26	事件源 IP 地址	事件源 IP 地址
27	事件源 IP 地址	事件源 IP 地址
28	事件源 IP 地址	事件源 IP 地址
29	事件源 IP 地址	事件源 IP 地址
30	事件源 IP 地址	事件源 IP 地址
31	事件源 IP 地址	事件源 IP 地址
32	事件源 IP 地址	事件源 IP 地址
33	事件源 IP 地址	事件源 IP 地址
34	事件源 IP 地址	事件源 IP 地址
35	事件源 IP 地址	事件源 IP 地址
36	事件源 IP 地址	事件源 IP 地址
37	事件源 IP 地址	事件源 IP 地址
38	事件源 IP 地址	事件源 IP 地址
39	事件源 IP 地址	事件源 IP 地址
40	事件源 IP 地址	事件源 IP 地址
41	事件源 IP 地址	事件源 IP 地址
42	事件源 IP 地址	事件源 IP 地址
43	事件源 IP 地址	事件源 IP 地址
44	事件源 IP 地址	事件源 IP 地址
45	事件源 IP 地址	事件源 IP 地址
46	事件源 IP 地址	事件源 IP 地址
47	事件源 IP 地址	事件源 IP 地址
48	事件源 IP 地址	事件源 IP 地址
49	事件源 IP 地址	事件源 IP 地址
50	事件源 IP 地址	事件源 IP 地址
51	事件源 IP 地址	事件源 IP 地址
52	事件源 IP 地址	事件源 IP 地址
53	事件源 IP 地址	事件源 IP 地址
54	事件源 IP 地址	事件源 IP 地址
55	事件源 IP 地址	事件源 IP 地址
56	事件源 IP 地址	事件源 IP 地址
57	事件源 IP 地址	事件源 IP 地址
58	事件源 IP 地址	事件源 IP 地址
59	事件源 IP 地址	事件源 IP 地址
60	事件源 IP 地址	事件源 IP 地址
61	事件源 IP 地址	事件源 IP 地址
62	事件源 IP 地址	事件源 IP 地址
63	事件源 IP 地址	事件源 IP 地址
64	事件源 IP 地址	事件源 IP 地址
65	事件源 IP 地址	事件源 IP 地址
66	事件源 IP 地址	事件源 IP 地址
67	事件源 IP 地址	事件源 IP 地址
68	事件源 IP 地址	事件源 IP 地址
69	事件源 IP 地址	事件源 IP 地址
70	事件源 IP 地址	事件源 IP 地址
71	事件源 IP 地址	事件源 IP 地址
72	事件源 IP 地址	事件源 IP 地址
73	事件源 IP 地址	事件源 IP 地址
74	事件源 IP 地址	事件源 IP 地址
75	事件源 IP 地址	事件源 IP 地址
76	事件源 IP 地址	事件源 IP 地址
77	事件源 IP 地址	事件源 IP 地址
78	事件源 IP 地址	事件源 IP 地址
79	事件源 IP 地址	事件源 IP 地址
80	事件源 IP 地址	事件源 IP 地址
81	事件源 IP 地址	事件源 IP 地址
82	事件源 IP 地址	事件源 IP 地址
83	事件源 IP 地址	事件源 IP 地址
84	事件源 IP 地址	事件源 IP 地址
85	事件源 IP 地址	事件源 IP 地址
86	事件源 IP 地址	事件源 IP 地址
87	事件源 IP 地址	事件源 IP 地址
88	事件源 IP 地址	事件源 IP 地址
89	事件源 IP 地址	事件源 IP 地址
90	事件源 IP 地址	事件源 IP 地址
91	事件源 IP 地址	事件源 IP 地址
92	事件源 IP 地址	事件源 IP 地址
93	事件源 IP 地址	事件源 IP 地址
94	事件源 IP 地址	事件源 IP 地址
95	事件源 IP 地址	事件源 IP 地址
96	事件源 IP 地址	事件源 IP 地址
97	事件源 IP 地址	事件源 IP 地址
98	事件源 IP 地址	事件源 IP 地址
99	事件源 IP 地址	事件源 IP 地址
100	事件源 IP 地址	事件源 IP 地址

GB/T 36958—2018

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

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11月第一版

\*

书号: 155066·1-61703

版权专有 侵权必究



GB/T 36958-2018