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 网络安全监测基本要求

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

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 …… 5
6.3 自身安全要求 …… 5
7 第三级安全管理中心技术要求 …… 8
7.1 功能要求 …… 8
7.2 接口要求 …… 13
7.3 自身安全要求 …… 13
8 第四级安全管理中心技术要求 …… 15
8.1 功能要求 …… 15
8.2 接口要求 …… 21
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。

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(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

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

[illegible]

3.2

采集器 collector

[illegible]

3.3

安全管理中心 security management center

[illegible]

注：修改 GB/T 25069—2010 定义3.1。

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　通用漏洞披露(Common Vulnerabilities & Exposures)

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

IP　　互联网协议(Internet Protocol)

[redacted]


网
接
入
核心交换

b) 能够对被管理对象的系统管理员进行身份识别，并对身份标识及识别信息进行复杂度检查；

c) 能够对被管理对象的系统管理员进行身份鉴别，并对身份标识及识别信息进行定期更换；

d) 能够对被管理对象的系统管理员进行登录失败处理，如结束会话、限制非法登录次数和当登录连接超时自动退出等措施；

e) 能够对被管理对象的系统管理员进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听；

f) 能够实现被管理对象的系统管理员角色分离，实现基于角色的访问控制。

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：

6.1.1.2.2 数据完整性

数据完整性应满足以下要求：

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：

a) 提供数据本地备份与恢复功能，备份数据备份至少每天一次；

b) 提供异地数据备份功能，支持将重要数据定时备份至异地灾备中心；

c) 提供重要数据处理系统和重要网络设备的配置数据的备份与恢复功能。

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) 应提供对安全事件的采集功能；

b) 应能对采集到的安全事件进行统一格式化；

c) 能够对采集的安全事件原始数据的集中存储。

注：安全事件的属性可参考附录C。

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：

6.1.1.3.4 综合分析报表

综合分析报表应满足以下要求：

a) 能够对资产、威胁、脆弱性、风险、事件、资源监控等信息进行综合分析，并生成报表；

b) 能够按照统计条件和报表生成周期，自动生成报表；

c) 支持报表的导出；

d) 支持手工或者自动生成报表。

6.1.1.4 监测管理

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) 资产管理信息应包括资产名称、资产IP地址、资产类型、资产责任人、资产业务流向、资产重要性等；

c) 支持资产属性的自定义；

d) 支持手工或者自动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) 能够按照统计条件和报表生成周期，自动生成报表；

c) 支持威胁的自定义分类，包括威胁名称、威胁类别、威胁描述等；

d) 支持威胁的导入导出。

6.1.1.4.3 脆弱性管理

脆弱性管理应满足以下要求：

a) 能够对被管理对象的脆弱性进行扫描，并支持手动上传脆弱性扫描文件，能够对扫描结果进行展示；

b) 能够对脆弱性扫描结果进行统计分析，并生成报表；

c) 支持脆弱性的自定义分类，包括脆弱性名称、脆弱性类别、脆弱性描述等；

d) 支持脆弱性的导入导出。

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、资产面临的威胁、资产存在的脆弱性，自动计算资产面临的风险，并能够以直观的方式显示风险计算结果；

b) 支持风险计算模型和计算公式的配置，包括资产价值、威胁发生频率、脆弱性严重程度的赋值；

c) 能够根据风险计算结果，提供风险处置建议；

d) 能够对处置后的风险进行重新评估计算。

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、主机操作系统、数据库、中间件、应用系统等重要性能指标，实现对其运行状态的

6.1.1.5.2 网络拓扑监测

网络拓扑监测应满足以下要求：

6.1.2.1 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

6.1.2.2.3 审计数据采集方式

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

[illegible]

6.2.2 接口安全要求

[illegible]

6.3 身份安全要求

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：

[illegible]

6.3.2 访问控制

[illegible]

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：

[illegible]

6.3.4 软件容错

[illegible]

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。

[illegible]

6.3.6 入侵防范

6.3.7 数据安全

中心技术要求

7 第三级安全管理中

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

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]

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、路由等信息；

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，在发现异常时可根据预先设定的规则产生告警；

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) [illegible]

c) [illegible]

7.1.1.3.4 事件关联分析

[illegible]

7.1.1.5 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：

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) 支持对网络设备进行在线编辑，允许手工增加或

b) 能够实现当前网络环境中关键设备（包括网络设备

态，如网络流量、网络协议统计分析等指标。

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) 为安全标记采集、传输、使用等环节的系统组件提供安全标记数据接口，支持安全标记的正确

调用和传输；

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

c) 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) 支持对主体和客体进行安全级别的划分，划分结果应

7.1.2.3 设备策略管理

7.1.2.3.1 安全审计策略

应为安全审计组件提供统一的策略配置接口，支持管理员对审计事件、审计记录、审计报表、安全报警等审计策略进行

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

[illegible]

7.1.3.2.4 审计数据关联分析

[illegible]

7.2 接口要求

7.2.1 第三方插件/代理接口协议要求

[illegible]要求：

[illegible]

7.2.2 接口安全要求

[illegible]

[illegible]

7.3 自身安全要求

7.3.1 身份鉴别

[illegible]

7.3.2 访问控制

[illegible]

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；

d) 应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保证管理员的鉴别信息所在的存储空间被释放或重分配给

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：

a) 应提供故障状态监测功能，应能够对系统服务故障、运行异常进行检测和报警；

b) 应提供重启恢复功能，应能够在故障发生后重启并恢复到故障前的状态；

c) 应提供关键数据的备份和恢复功能，应能够对关键数据进行备份和恢复。

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) 应能够对单个管理员账户的多重并发会话进行限制；

c) 应能够对一段时间内未作任何动作，应能够自动结束会话；

d) 应能够对最大并发会话连接数进行限制；

e) 应能够对单个管理员账户的多重并发会话进行限制；

f) 应能够对一段时间内可并发会话连接进行限制；

g) 应能够对一段时间内的资源使用情况进行监测，应能够对异常降低到预先规定的最小值进行检测和报警；

h) 应提供

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；

b) 能够检测到对重要程序的完整性进行破坏，并在检测到完整性

受到破坏后具有恢复措施；

c) 应采用安全审计或其他相关技术实现对系统资源和关键数据访问记录的数据传输完整性

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) 应能够检测到重要数据在传输和存储过程中完整性受到破坏并在检测到完整性

受到破坏时具有恢复措施；

b) 应采用安全审计或其他相关技术实现对系统资源和关键数据访问记录的数据传输完整性

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]

[illegible]

[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]

[illegible]

[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；

b) 在主体对客体进行访问时，应保证数据访问路径上各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：

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

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；

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) 支持通过监测网络设备、主机操作系统、数据库、中间件、应用系统等重要对象的性能指标，

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) 支持自动发现网络节点设备及其连接关系，并以图形化方式呈现，

c) 支持在指定网络范围内发现与监测网络设备可以直接通信的其他网络设备，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/客体的安全标记进行管理，并依据安全标记和强制访问控制规则确定主体对客体的访问权限，

b) 支持主体或其代表能够修改主/客体的安全标记，并依据强制访问控制规则确定主体是否有权修改这些安全标记，

c) 支持为新创建的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

d) 支持为输出到外部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

e) 支持为输入到内部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

f) 支持为输出到外部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

g) 支持为输入到内部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

h) 支持为输出到外部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

i) 支持为输入到内部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

j) 支持为输出到外部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

k) 支持为输入到内部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

l) 支持为输出到外部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

m) 支持为输入到内部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

n) 支持为输出到外部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

o) 支持为输入到内部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

p) 支持为输出到外部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

q) 支持为输入到内部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

r) 支持为输出到外部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

s) 支持为输入到内部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

t) 支持为输出到外部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

u) 支持为输入到内部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

v) 支持为输出到外部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

w) 支持为输入到内部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

x) 支持为输出到外部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

y) 支持为输入到内部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

z) 支持为输出到外部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

aa) 支持为输入到内部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

bb) 支持为输出到外部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

cc) 支持为输入到内部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

dd) 支持为输出到外部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

ee) 支持为输入到内部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

ff) 支持为输出到外部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

gg) 支持为输入到内部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

hh) 支持为输出到外部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

ii) 支持为输入到内部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

jj) 支持为输出到外部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

kk) 支持为输入到内部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

ll) 支持为输出到外部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

mm) 支持为输入到内部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

nn) 支持为输出到外部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

oo) 支持为输入到内部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

pp) 支持为输出到外部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

qq) 支持为输入到内部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

rr) 支持为输出到外部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

ss) 支持为输入到内部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

tt) 支持为输出到外部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

uu) 支持为输入到内部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

vv) 支持为输出到外部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

ww) 支持为输入到内部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

xx) 支持为输出到外部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

yy) 支持为输入到内部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

zz) 支持为输出到外部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

aaa) 支持为输入到内部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

bbb) 支持为输出到外部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

ccc) 支持为输入到内部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

ddd) 支持为输出到外部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

eee) 支持为输入到内部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

fff) 支持为输出到外部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

ggg) 支持为输入到内部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

hhh) 支持为输出到外部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

iii) 支持为输入到内部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

jjj) 支持为输出到外部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

kkk) 支持为输入到内部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

lll) 支持为输出到外部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

mmm) 支持为输入到内部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

nnn) 支持为输出到外部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

ooo) 支持为输入到内部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

ppp) 支持为输出到外部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

qqq) 支持为输入到内部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

rrr) 支持为输出到外部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

sss) 支持为输入到内部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

ttt) 支持为输出到外部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

uuu) 支持为输入到内部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

vvv) 支持为输出到外部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

www) 支持为输入到内部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

xxx) 支持为输出到外部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

yyy) 支持为输入到内部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

zzz) 支持为输出到外部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

aaaa) 支持为输入到内部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

bbbb) 支持为输出到外部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

cccc) 支持为输入到内部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

dddd) 支持为输出到外部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

eeee) 支持为输入到内部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

ffff) 支持为输出到外部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

gggg) 支持为输入到内部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

hhhh) 支持为输出到外部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

iiii) 支持为输入到内部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

jjjj) 支持为输出到外部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

kkkk) 支持为输入到内部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

llll) 支持为输出到外部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

mmmm) 支持为输入到内部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

nnnn) 支持为输出到外部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

oooo) 支持为输入到内部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

pppp) 支持为输出到外部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

qqqq) 支持为输入到内部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

rrrr) 支持为输出到外部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

ssss) 支持为输入到内部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

tttt) 支持为输出到外部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

uuuu) 支持为输入到内部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

vvvv) 支持为输出到外部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

wwww) 支持为输入到内部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

xxxx) 支持为输出到外部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

yyyy) 支持为输入到内部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

zzzz) 支持为输出到外部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

aaaaa) 支持为输入到内部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

bbbbb) 支持为输出到外部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

ccccc) 支持为输入到内部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

ddddd) 支持为输出到外部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

eeeee) 支持为输入到内部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

fffff) 支持为输出到外部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

ggggg) 支持为输入到内部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

hhhhh) 支持为输出到外部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

iiiii) 支持为输入到内部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

jjjjj) 支持为输出到外部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

kkkkk) 支持为输入到内部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

lllll) 支持为输出到外部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

mmmmm) 支持为输入到内部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

nnnnn) 支持为输出到外部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

ooooo) 支持为输入到内部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

ppppp) 支持为输出到外部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

qqqqq) 支持为输入到内部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

rrrrr) 支持为输出到外部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

sssss) 支持为输入到内部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

ttttt) 支持为输出到外部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

uuuuu) 支持为输入到内部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

vvvvv) 支持为输出到外部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

wwwww) 支持为输入到内部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

xxxxx) 支持为输出到外部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

yyyyy) 支持为输入到内部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

zzzzz) 支持为输出到外部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

aaaaaa) 支持为输入到内部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

bbbbbb) 支持为输出到外部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

cccccc) 支持为输入到内部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

dddddd) 支持为输出到外部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

eeeeee) 支持为输入到内部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

ffffff) 支持为输出到外部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

gggggg) 支持为输入到内部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

hhhhhh) 支持为输出到外部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

iiiiii) 支持为输入到内部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

jjjjjj) 支持为输出到外部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

kkkkkk) 支持为输入到内部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

llllll) 支持为输出到外部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

mmmmmm) 支持为输入到内部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

nnnnnn) 支持为输出到外部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

oooooo) 支持为输入到内部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

pppppp) 支持为输出到外部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

qqqqqq) 支持为输入到内部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

rrrrrr) 支持为输出到外部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

ssssss) 支持为输入到内部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

tttttt) 支持为输出到外部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

uuuuuu) 支持为输入到内部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

vvvvvv) 支持为输出到外部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

wwwwww) 支持为输入到内部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

xxxxxx) 支持为输出到外部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

yyyyyy) 支持为输入到内部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

zzzzzz) 支持为输出到外部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

aaaaaaa) 支持为输入到内部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

bbbbbbb) 支持为输出到外部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

ccccccc) 支持为输入到内部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

ddddddd) 支持为输出到外部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

eeeeeee) 支持为输入到内部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

fffffff) 支持为输出到外部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

ggggggg) 支持为输入到内部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

hhhhhhh) 支持为输出到外部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

iiiiiii) 支持为输入到内部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

jjjjjjj) 支持为输出到外部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

kkkkkkk) 支持为输入到内部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

lllllll) 支持为输出到外部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

mmmmmmm) 支持为输入到内部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

nnnnnnn) 支持为输出到外部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

ooooooo) 支持为输入到内部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

ppppppp) 支持为输出到外部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

qqqqqqq) 支持为输入到内部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

rrrrrrr) 支持为输出到外部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

sssssss) 支持为输入到内部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

ttttttt) 支持为输出到外部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

uuuuuuu) 支持为输入到内部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

vvvvvvv) 支持为输出到外部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

wwwwwww) 支持为输入到内部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

xxxxxxx) 支持为输出到外部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

yyyyyyy) 支持为输入到内部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

zzzzzzz) 支持为输出到外部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

aaaaaaaa) 支持为输入到内部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

bbbbbbbb) 支持为输出到外部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

cccccccc) 支持为输入到内部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

dddddddd) 支持为输出到外部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

eeeeeeee) 支持为输入到内部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

ffffffff) 支持为输出到外部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

gggggggg) 支持为输入到内部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

hhhhhhhh) 支持为输出到外部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

iiiiiiii) 支持为输入到内部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

jjjjjjjj) 支持为输出到外部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

kkkkkkkk) 支持为输入到内部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

llllllll) 支持为输出到外部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

mmmmmmmm) 支持为输入到内部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

nnnnnnnn) 支持为输出到外部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

oooooooo) 支持为输入到内部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

pppppppp) 支持为输出到外部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

qqqqqqqq) 支持为输入到内部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

rrrrrrrr) 支持为输出到外部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

ssssssss) 支持为输入到内部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

tttttttt) 支持为输出到外部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

uuuuuuuu) 支持为输入到内部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

vvvvvvvv) 支持为输出到外部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

wwwwwwww) 支持为输入到内部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

xxxxxxxx) 支持为输出到外部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

yyyyyyyy) 支持为输入到内部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

zzzzzzzz) 支持为输出到外部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

aaaaaaaaa) 支持为输入到内部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

bbbbbbbbb) 支持为输出到外部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

ccccccccc) 支持为输入到内部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

ddddddddd) 支持为输出到外部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

eeeeeeeee) 支持为输入到内部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

fffffffff) 支持为输出到外部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

ggggggggg) 支持为输入到内部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

hhhhhhhhh) 支持为输出到外部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

iiiiiiiii) 支持为输入到内部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

jjjjjjjjj) 支持为输出到外部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

kkkkkkkkk) 支持为输入到内部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

lllllllll) 支持为输出到外部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

mmmmmmmmm) 支持为输入到内部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

nnnnnnnnn) 支持为输出到外部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

ooooooooo) 支持为输入到内部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

ppppppppp) 支持为输出到外部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

qqqqqqqqq) 支持为输入到内部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

rrrrrrrrr) 支持为输出到外部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

sssssssss) 支持为输入到内部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

ttttttttt) 支持为输出到外部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

uuuuuuuuu) 支持为输入到内部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

vvvvvvvvv) 支持为输出到外部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

wwwwwwwww) 支持为输入到内部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

xxxxxxxxx) 支持为输出到外部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

yyyyyyyyy) 支持为输入到内部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

zzzzzzzzz) 支持为输出到外部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

aaaaaaaaaa) 支持为输入到内部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

bbbbbbbbbb) 支持为输出到外部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

cccccccccc) 支持为输入到内部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

dddddddddd) 支持为输出到外部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

eeeeeeeeee) 支持为输入到内部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

ffffffffff) 支持为输出到外部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

gggggggggg) 支持为输入到内部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

hhhhhhhhhh) 支持为输出到外部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

iiiiiiiiii) 支持为输入到内部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

jjjjjjjjjj) 支持为输出到外部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

kkkkkkkkkk) 支持为输入到内部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

llllllllll) 支持为输出到外部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

mmmmmmmmmm) 支持为输入到内部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

nnnnnnnnnn) 支持为输出到外部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

oooooooooo) 支持为输入到内部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

pppppppppp) 支持为输出到外部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

qqqqqqqqqq) 支持为输入到内部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

rrrrrrrrrr) 支持为输出到外部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

ssssssssss) 支持为输入到内部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

tttttttttt) 支持为输出到外部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

uuuuuuuuuu) 支持为输入到内部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

vvvvvvvvvv) 支持为输出到外部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

wwwwwwwwww) 支持为输入到内部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

xxxxxxxxxx) 支持为输出到外部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

yyyyyyyyyy) 支持为输入到内部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

zzzzzzzzzz) 支持为输出到外部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

aaaaaaaaaaa) 支持为输入到内部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

bbbbbbbbbbb) 支持为输出到外部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

ccccccccccc) 支持为输入到内部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

ddddddddddd) 支持为输出到外部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

eeeeeeeeeee) 支持为输入到内部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

fffffffffff) 支持为输出到外部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

ggggggggggg) 支持为输入到内部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

hhhhhhhhhhh) 支持为输出到外部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

iiiiiiiiiii) 支持为输入到内部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

jjjjjjjjjjj) 支持为输出到外部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

kkkkkkkkkkk) 支持为输入到内部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

lllllllllll) 支持为输出到外部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

mmmmmmmmmmm) 支持为输入到内部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

nnnnnnnnnnn) 支持为输出到外部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

ooooooooooo) 支持为输入到内部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

ppppppppppp) 支持为输出到外部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

qqqqqqqqqqq) 支持为输入到内部的主/客体设置安全标记，并依据强制访问控制规则确定主体是否有权设置这些安全标记，

rrrrrrrrrrr) 支持为输出到外部的主/客体设置安全标记，并依据强制访问控制规则确

问权限管理、网络访问权限管理、应用访问

定访问控制策略，控制主体对客体的访问，

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；

c） 实现根据主体标记和客体标记安全级别的不同，制

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略的统一查询；

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：

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，包括策略具不具备

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：

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故障期间采集的数据。

8.1.3.2.5 审计数据关联分析

审计数据关联分析应满足以下要求：

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：

8.3 自身安全要求

8.3.1 身份鉴别

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

.6 软件容错 8.3

8.3.7 资源控制

8.3.8 入侵防范

8.3.9 数据安全

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：

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

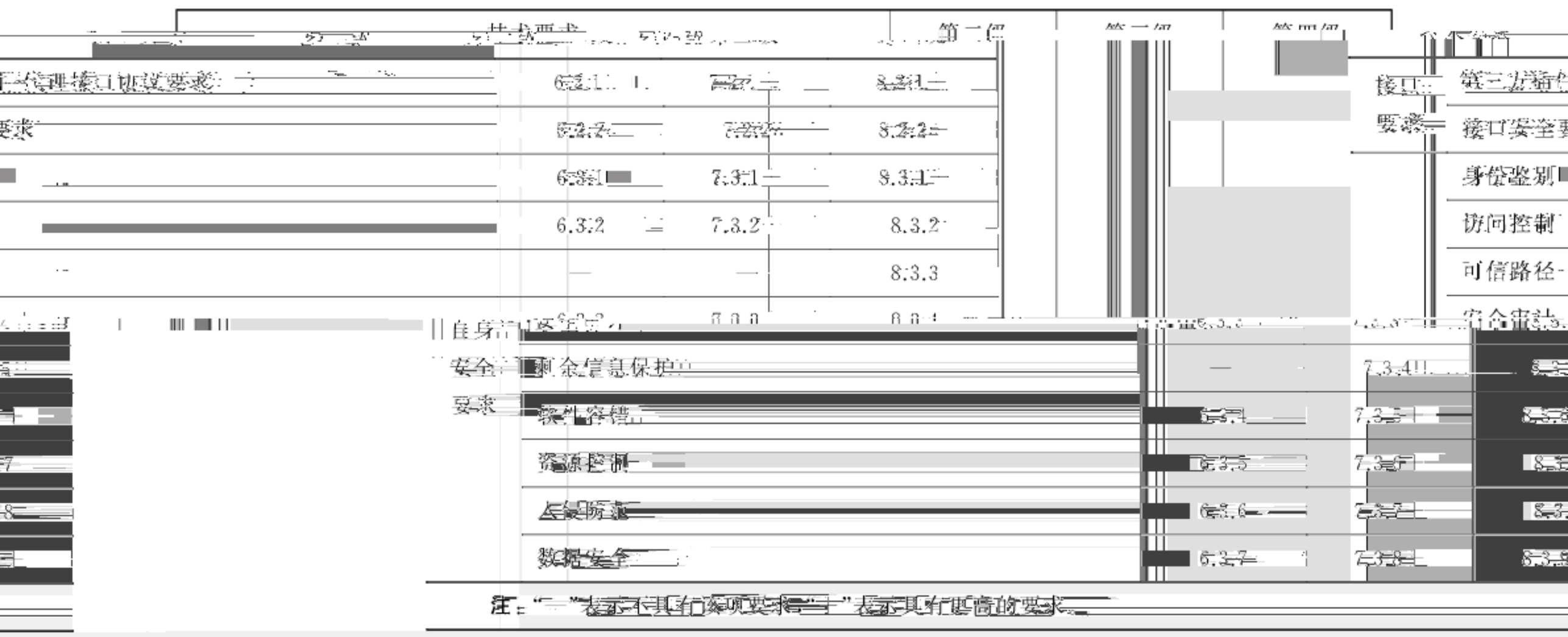
附 录 B
（规范性附录）

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
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
安全事件处置	—	7.1.1.3.3	8.1.1.3.3
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	—	7.1.2.3	8.1.2.3
安全策略管理	—	7.1.2.3.1	8.1.2.3.1
策略冲突检测	—	7.1.2.3.2	8.1.2.3.2
策略优化	—	7.1.2.3.3	8.1.2.3.3
密码保障	—	7.1.2.4	8.1.2.4
集中数据管理	—	7.1.2.5	8.1.2.5
监控数据采集	6.1.2.1	7.1.2.5.1	8.1.2.5.1
监控数据处理	6.1.2.2	7.1.2.5.2	8.1.2.5.2
监控数据关联分析	6.1.2.3	7.1.2.5.3	8.1.2.5.3

表 B.1（续）



注："—"表示不具有该项要求，"√"表示具有该项的要求。

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	事件采集时间	接收事件时间
7	归并事件的次数	归并数量
8	事件发生时间	事件发生时间
9	事件类别	事件类别
10	事件原始信息	事件内容
11	事件内容	事件内容
12	协议	协议类型
13	源端口	源端口号
14	源地址	源地址名称
15	源地址	源地址
16	目的地址名	目的地址名称
17	目的地址	目的地址
18	目的端口	目的端口号

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