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 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

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 …… 7
6.3 自身安全要求 …… 8
7 第三级安全管理中心技术要求 …… 8
7.1 功能要求 …… 13
7.2 接口要求 …… 13
7.3 自身安全要求 …… 15
8 第四级安全管理中心技术要求 …… 15
8.1 功能要求 …… 21
8.2 接口要求 …… 21
8.3 自身安全要求 …… 23
9 第五级安全管理中心技术要求 …… 24
9.1 第五级安全管理中心技术要求 …… 24
9.2 第五级安全管理中心技术要求 …… 27

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(所有部分)　信息安全技术　SM2椭圆曲线公钥密码算法

GB/T 36959—2018　信息安全技术　网络安全等级保护　测评机构管理要求

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

4　缩略语

下列缩略语适用于本文件。

CPU　中央处理器(Central Processing Unit)

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]


接
核心交换
入侵检测设备
漏洞扫描系统
安全管理

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

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：

注：安全审计的信息可参考附录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：

[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 [illegible]

6.1.1.4.1 资产管理

[illegible]

a) 支持资产属性的自定义；

d) 支持手工录入资产信录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) [illegible]

6.1.1.4.3 脆弱性管理

[illegible]

6.1.1.4.4 风险分析

风险分析应满足以下要求：

a) 能够根据资产的业务价值、资产当前的脆弱性或资产面临的安全威胁[illegible]风险；

b) 安全风险的计算思想和计算公式能够根据部署环境的实际需要通过修改配置调整；

[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、主机操作系统、数据库、中间件、应用系统等重要性能指标[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：

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

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：

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

[illegible]

6.2.2 接口安全要求

[illegible]

6.3 自身安全要求

6.3.1 身份鉴别

[illegible]

6.3.2 访问控制

[illegible]

6.3.3 安全审计

[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

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；

7.1.1.2.4 剩余信息保护

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：

7.1.3.2 安全事件告警

安全事件告警应满足以下要求：

7.1.3.3 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；

7.1.3.4 事件关联分析

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：

c) 支持资产属性的自定义；

7.1.1.4.2 资产业务价值评估

7.1.1.4.3 威胁管理

威胁管理应满足以下要求：

a) 支持

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：

网络拓扑监测 7.1.1.5.2

网络拓扑监测应满足以下要求：

a) 支持对网络拓扑进行在线编辑，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、流量、网络流量、网络协议统计分析等功能；

安全管理要求 7.1.2

安全标记 7.1.2.1

7.1.2.2 授权管理

授权管理应满足以下要求：

a) 实现对每

b) 实现主体

权限管理

策略管理 7.1.2.3 设备

全配置策略 7.1.2.3.1 安全

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；

[illegible]

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

接口协议要求应满足以下要求：

[illegible]

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：

[illegible]

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) [illegible]

b) [illegible]

c) [illegible]

d) 实现特权用户的权限分离，应将予不同账户为完成各

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) 应对审计记录进行保护，避免受到未预期的删除、修改或覆盖等；

e) 应对审计进程进行保护，避免受到未预期的中断。

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) 应保证管理员鉴别信息所在的存储空间被释放或再分配给其他管理员前得到完全清除，无论这些信息是存放在硬盘上还是在内存中；

b) 应保证用于存储敏感信息的存储空间被释放或重新分配给其他管理员前得到完全清除，无论这些信息是存放在硬盘上还是在内存中。

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) 应提供故障检测功能，保证能够检测到系统的故障，并向管理员报警；

b) 应提供故障恢复功能，保证能够在故障发生后恢复到故障发生前的状态；

c) 应提供故障记录功能，保证能够记录故障发生时间、故障内容等。

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) 应限制管理员登录地址范围；

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用户的最大并发会话进行限制；

e) 应提供对重要资源的监测功能，能够对重要资源的最小剩余空间进行检测和报警；

f) 应提供资源分配策略，保证能够对资源进行合理分配。

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) 应能够检测到对重要服务器进行入侵的行为，能够记录入侵的源IP、攻击类型、攻击目的、攻击时间，并在发生严重入侵事件时提供报警；

b) 应能够对恶意代码进行检测和报警，并保存检测记录。

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) 应能够检测到完整性受到破坏，并在发生严重完整性破坏事件时采取恢复措施；

b) 应能够检测到重要数据在传输过程中完整性受到破坏，并在发生严重完整性破坏事件时采取恢复措施；

c) 应能够检测到重要数据在存储过程中完整性受到破坏，并在发生严重完整性破坏事件时采取恢复措施。

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]

[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[illegible]

[illegible]

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，应保证该访问的客体与主体之间[illegible]输路径；

8.1.1.2.5 剩余信息保护

[illegible]

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；

c) 能够对安全事件进行[illegible]

[illegible]

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；

b) [illegible]

[illegible]

8.1.1.3.3 安全事件响应

安全事件响应应满足以下要求：

a) [illegible]

[illegible]

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：

c) 支持资产属性的自定义；

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

8.1.2.2 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，制定访问控制策略，控制主体对客体的访问，

[illegible]

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；

[illegible]

8.1.2.3.2 入侵防御

入侵防御应满足以下要求：

[illegible]

8.1.2.3.3 恶意代码防范

[illegible]

8.1.2.4 密码保障

[illegible]

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[illegible]

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：

a) 采用安全的接口协议，保证接口之间交互数据的完整性；

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，对同一管理员用户采用两种或两种

8.3.2 访问控制

8.3 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

[illegible]

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：

[illegible]

8.3.5 剩余信息保护

[illegible]

8.3.6 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：

[illegible]

8.3.7 资源控制

[illegible]

8.3.8 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：

[illegible]

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：

[illegible]

[illegible]

9 第五级安全管理中心技术要求

行制定。

第五级安全管理中心技术要求另行

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：

[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
数据保密性	6.1.1.2.1	7.1.1.2.1	8
数据保整性	[illegible]	[illegible]	[illegible]
数据保护		数据备份与恢复	
		可信路径	
		融合信息保护	
		安全事件采集	
		安全事件告警	
安全事件管理	6.1.1.3.3	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		网络拓扑监	
安全标记			
授权管理			
中个安全管理			
要求	设备策略管理		
恶意代码防御			
密码保障	—	7.1.2	
[illegible]		7.1	

表 B.1（续）

技术要求		第一级	第二级	第三级	第四级
安全管理	接口设置要求	6.3.1.1	7.3.1	8.3.1	9.3.1
	接口安全要求	6.3.2	7.3.2	8.3.2	9.3.2
	身份鉴别	6.3.1	7.3.1	8.3.1	9.3.1
	访问控制	6.3.2	7.3.2	8.3.2	9.3.2
	可信路径	—	—	8.3.3	9.3.3
	安全审计	6.3.3	7.3.3	8.3.4	9.3.4
安全要求	软件容错	6.3.4	7.3.5	8.3.6	9.3.6
	资源控制	6.3.5	7.3.6	8.3.7	9.3.7
	入侵防范	6.3.6	7.3.7	8.3.8	9.3.8
	数据安全	6.3.7	7.3.8	8.3.9	9.3.9

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	开始时间	事件发生时间
9	结束时间	事件结束时间
10	原始信息	事件原始信息
11	事件内容	事件内容
12	事件级别	事件级别
13	事件类型	事件类型
14	事件名称	事件名称
15	事件类别	事件类别
16	事件子类别	事件子类别
17	事件处理状态	事件处理状态
18	事件处理结果	事件处理结果
19	事件处理人	事件处理人
20	事件处理时间	事件处理时间
21	事件处理方法	事件处理方法
22	事件处理描述	事件处理描述
23	事件处理附件	事件处理附件
24	事件处理备注	事件处理备注
25	事件处理扩展	事件处理扩展

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