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 网络安全等级保护安全设计技术要求

Information security technology—Technical requirements of security design of 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

目 录

前言 …… II
引言 …… III
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 …… 7
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
附录A（资料性附录）安全管理中心技术要求分级表 …… 23
附录B（资料性附录）安全事件分类 …… 27

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

[illegible]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。

[illegible]GB/T 27818—信息技术　词汇　第8部分：安全

[illegible]GB/T 859—1999　计算机信息系统　安全保护等级划分准则

[illegible]GB/T 25069　信息安全技术　术语

[illegible]

3　术语和定义

[illegible]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。

[illegible]

[illegible]

3.2

采集器　collector

[illegible]

[illegible]

3.4

[illegible]

[illegible]

4　缩略语

[illegible]下列缩略语适用于本文件。

[illegible]中央处理器(Central Processing Unit)　CPU

[illegible]　CPE

[illegible]　IDS

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

网
接
入
核心交换
防病毒
和补丁服务器
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

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：

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：

6.1.1.4 综合管理

6.1.1.4.1 资产管理

6.1.1.4.2 威胁管理

6.1.1.4.3 脆弱性管理

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

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

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

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

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；

b) 采用加密技术或安全协议对接口交互数据进行加密；

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：

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) 提供管理员用户身份标识唯一和鉴别信息复杂度检查功能，保证系统中存在的用户身份标识是唯一的，并符合口令复杂度要求；

6.3.2 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) 提供管理员角色划分功能，并为管理员分配不同的角色；

b) 提供基于管理员角色或者用户的访问控制策略，并默认阻断账户的访问；

6.3 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) 提供覆盖每个管理员的安全审计功能，对管理员的重要操作（如添加、删除、修改安全策略等）、安全事件的处理等进行审计记录，并保证审计记录不可被删除、修改或覆盖（可以设置存储空间阈值，当存储空间达到阈值时，采取报警甚至停止审计记录的策略）；

b) 审计记录应包括事件的日期、时间、发起者信息、类型、描述和结果等；

c) 提供审计记录数据的备份和恢复的功能。

6.3.4 软件容错

数据格式或协议符合系统设计要求

输入

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

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]

7.1.1.3.1 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) [illegible]

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) 能够提供安全通告功能，可以创建或导入安全风险通告，通告中应包括通告内容、描述信息[illegible]

c) [illegible]

d) [illegible]

7.1.1.3.4 安全事件分析

安全事件分析应满足以下要求：

a) [illegible]

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：

7.1.1.4.3 威胁管理

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：

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

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) 采用安全传输协议，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：

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、描述

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) 应对管理员登录操作进行限制；

b) 应能够自动结束会话；

c) 应能够对最大并发会话连接数进行限制；

d) 应对一个时间段内可以同时登录的管理员数量进行限制；

e) 应能够对一个时间段内可以同时进行通信的节点数量进行限制；

f) 应能够对单个账户的多重并发会话进行限制；

g) 应能够对一个访问账户或一个请求进程占用的资源分配最大限额和最小限额；

h) 应能够对系统服务水平降低到预先规定的最小值进行检测和报警；

i) 应提供重要节点设备的硬件冗余，保证系统的高可用性。

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：

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]

8.1.1.2.2 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]

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) 在对主体的重要操作时间点，能够请求建立可信路径实体主体之间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；

c) 能够对安全事件进行过滤，出仅显示指定层面源于同一或特定主体的满足特定条件的安全事件；

d) 安全事件的内容应包括日期、时间、主体标识、客体标识、类型、描述、地址、端口、协议、应用程序接口、安全事件严重级别、处置建议、数据项、安全事件分类、网络拓扑、系统拓扑、资产信息、脆弱性信息、威胁情报信息等。

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) 告警方式应能够包括但不限于短信、邮件、页面提示、声音等多种方式的组合；

c) 告警信息应能够包括但不限于事件名称、事件级别、事件发生时间、事件类型、事件描述、处置建议等内容。

8.1.1.3 安全事件响应

安全事件响应应满足以下要求：

a) 具备安全事件处置流程，对安全事件进行分析并采取响应措施；

b) 具备安全事件记录与报告功能，可自动生成安全事件处置报告；

c) 具备安全事件处置流程的定期评估与改进机制。

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

[redacted]

[redacted]

[redacted]

权限管理、应用访问

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、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

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

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

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：

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

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 IP

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；

c) 各接口之

8.3 自身安全要求

8.3.1 身份鉴别

安全管理中心

a) 提供专用

8.3.2 访问控制

8.3.3 可信路径

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：

8.3.5 剩余信息保护

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：

8.3.7 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：

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：

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]

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：

[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	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
资产业务依赖关系管理	—	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
安全管理功能要求	6.1.1.5.1	7.1.1.5.1	8.1.1.5.1
集中管控	6.1.1.5.2	7.1.1.5.2	8.1.1.5.2
资源监控	—	7.1.2.1	8.1.2.1
网络拓扑监测	—	7.1.2.2	8.1.2.2
安全标记	—	7.1.2.3	8.1.2.3
授权管理	—	7.1.2.4	8.1.2.4
集中管控	—	7.1.2.5	8.1.2.5
基于安全标记的强制访问控制	—	7.1.2.6	8.1.2.6
设备管理	—	7.1.2.7	8.1.2.7

表 B.1（续）

安全管理接口设计要求	6.3.1	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
	6.3.3	7.3.3	8.3.4
安全[illegible]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
[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[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

版权专有 侵权必究