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

前　言

—2009 给出的规则起草。

本标准按照 GB/T 1.1

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 37718　信息技术　词汇　第8部分：安全

GB/T 17859　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/T 37718、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

4　缩略语

下列缩略语适用于本文件。

CPU　中央处理器(Central Processing Unit)

DNS　域名解析服务(Domain Name System/Service)

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


网
络
入
口
接
核心交换
防病毒
和补丁服务器
NTP
服务器
堡垒机
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

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

6.1.1.3.2 安全事件告警

6.1.1.3.3 安全事件响应

6.1.3.4 资产分类

6.1.3.4.1 资产管理

6.1.3.4.1.1 资产管理

6.1.3.4.1.1.1 资产管理

6.1.3.4.1.1.2 资产分类

6.1.3.4.1.1.3 资产标识

6.1.3.4.1.1.4 资产管理

6.1.3.4.1.1.5 资源供给

6.1.3.4.1.1.5.1 可用性监测

可用性监测应满足以下要求：

6.1.3.4.2 威胁管理

6.1.3.4.3 脆弱性管理

6.1.3.4.4 风险分析

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

以及第三方的插 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

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发送的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

7.1.1.3 安全

7.1.1.3.1 安全事件

安全事件采集应

7.1.1.3.2

安全

9

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：

[illegible]管理员掌握网络设备、安全设备、主机操作系统、数据库、应用系统等重要性能指标，实时了解其[illegible]状态；

[illegible]

c) [illegible]工业控制系统设备[illegible]进行实时监控[illegible]

[illegible]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、网络频宽统计分析等信息；

c) 在网络运行出现异常时，能够展现当前网络拓扑图中[illegible]告警信息；

d) [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) 能够对节点的安全标记[illegible]，包括[illegible]网络设备等；

b) 安全标记应具有唯一性，能够[illegible]标记的创建、修改和删除等操作；

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) 实现根据主体标记和客体标记安全级别[illegible]，制定访问控制策略，控制主体对客体的访问。

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

集方式 7.1.3.2.3 审计数据采

关联分析 7.1.3.2.4 审计数据

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：

应满足以下要求： 接口安全要求

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。

要求 7.3 自身安全

7.3.1 身份鉴

心控制台的管理员身份鉴别应满足以下要求： 安全管理中

控制 7.3.2 访问

理中心控制台的访问控制应满足以下要求： 安全管

a) 实现特权用户的权限分离，为每个系统用户分配完成各自承担任务所需的最小权限，并在管

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) 应提供对控制台操作的安全审计功能，安全管理中心控制台的安全审计应独立于被审计系统，并能对控制台操作的全过程进行审计；

b) 应能对控制台操作的所有用户操作进行审计，审计记录应包括事件的日期、时间、类型、主体标识、客体标识和结果等；

c) 应能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；

d) 应能对审计记录进行备份，避免审计记录对控制台存储空间造成影响；

e) 应能对审计进程进行保护，防止未经授权的中断。

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保证管理员的敏感信息所在的存储空间被释放或重新分配给其他用户前得到完全清除，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) 应提供软件容错机制，保证软件系统连续可靠正常运行；

b) 应提供故障自动恢复功能，在故障发生时能够保证系统及时恢复；

c) 应提供关键业务数据的备份和恢复功能，保证在故障发生后能够恢复业务数据。

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) 应能够对管理员登录的最长会话连接时间进行限制；

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；

d) 能够对管理员登录的最长会话连接进行限制；

e) 应提供对重要资源状态的监测功能，能够对服务水平降低到预先规定的最小值进行检测和报警。

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) 应能够对入侵事件进行记录。

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) 应能够检测到重要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；

b) 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检测到完整性错误时采取必要的恢复措施。

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]

8.1.1.2.3 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) 在对主体的身份鉴别询问、鉴别评判结果返回等信息与其他信息在传输时应能够建立一条安全的信息传输

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：

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

8.1.1.5 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、安全设备

8.1.1.5.2 网络拓扑监测

网络拓扑监测应满足以下要

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

限管理、应用访问

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；

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：

8.1.2.3.2 入侵防御

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：

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 地址、端口等信息；

b) [illegible]

c) [illegible]

d) [illegible]

e) [illegible]

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) 支持对网络设备（如交换机、路由器等）[illegible]的审计数据采集；

b) 支持对主机设备（如服务器、操作系统等）、应用支撑[illegible]（如台式电脑、笔记本电脑[illegible]等）终端以及安全管理系统所使用的设备上的审计数据采集；

c) 支持对数据库的审计数据采集；

d) 支持对安全设备（如防火墙、入侵检测系统[illegible]）、[illegible]系统、工业控制系统[illegible]安全设备[illegible]等系统和设备的审计数据采集；

e) 支持对各类应用[illegible]的审计数据采集；

f) [illegible]

g) [illegible]

h) 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、服务器、操作站等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 等协议采集各种系统或设备上的审计数据；

b) 通过统一[illegible]审计数据[illegible]；

c) 支持[illegible]

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断网期间采集的数据。

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；

b) 采用[illegible]

c) 各接口之间进行通信时，应通过身份验证机

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

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：

8.3.4 安全审计

8.3.5 剩余信息保护

8.3.6 软件容错

8.3.8 入侵防范

8.3.9 数据安

[illegible]

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：

[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
数据保护	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
融合信息保护	—	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
安全事件响应	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	6.1.1.5.1	7.1.1.5.1	8.1.1.5.1
网络拓扑监测	6.1.1.5.2	7.1.1.5.2	8.1.1.5.2
安全标记	—	7.1.2.3	8.1.2.3
授权管理	—	7.1.2.2	8.1.2.2
集中管理	6.1.2.1	7.1.3.1	8.1.3.1
集中审计	6.1.2.2	7.1.3.2	8.1.3.2
安全策略	—	—	8.1.3.3
系统管理	6.1.3.1	7.1.3.3	8.1.3.4
安全管理	6.1.3.2	7.1.3.4	8.1.3.5
集中管控	6.1.3.3	7.1.3.5	8.1.3.6
审计管理	6.1.3.4	7.1.3.6	8.1.3.7
安全管理	6.1.3.5	7.1.3.7	8.1.3.8
集中管控	6.1.3.6	7.1.3.8	8.1.3.9

表 B.1（续）

技术要求	第一级	第二级	第三级
安全管理接口设计要求	6.3.1.1	7.3.1	8.3.1
安全接口要求	6.3.2	7.3.2	8.3.2
身份鉴别	6.3.1	7.3.1	8.3.1
访问控制	6.3.2	7.3.2	8.3.2
可信路径	—	—	8.3.3
安全审计	6.3.3	7.3.3	8.3.4
剩余信息保护	—	7.3.4	8.3.5
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
7		
8		
9		
10		
11	事件内容	事件原始信息
12		
13		
14		
15		
16		
17		
18		
19		
20		

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