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 网络安全等级保护实施指南

2018-12-28 发布　　2019-07-01 实施

目次

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 5271.8　信息技术　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　信息安全技术　术语

[illegible]

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 [illegible] interface

[illegible]

3.2

采集器　collector

[illegible]

3.3

安全管理中心 [illegible]

[illegible]

4　缩略语

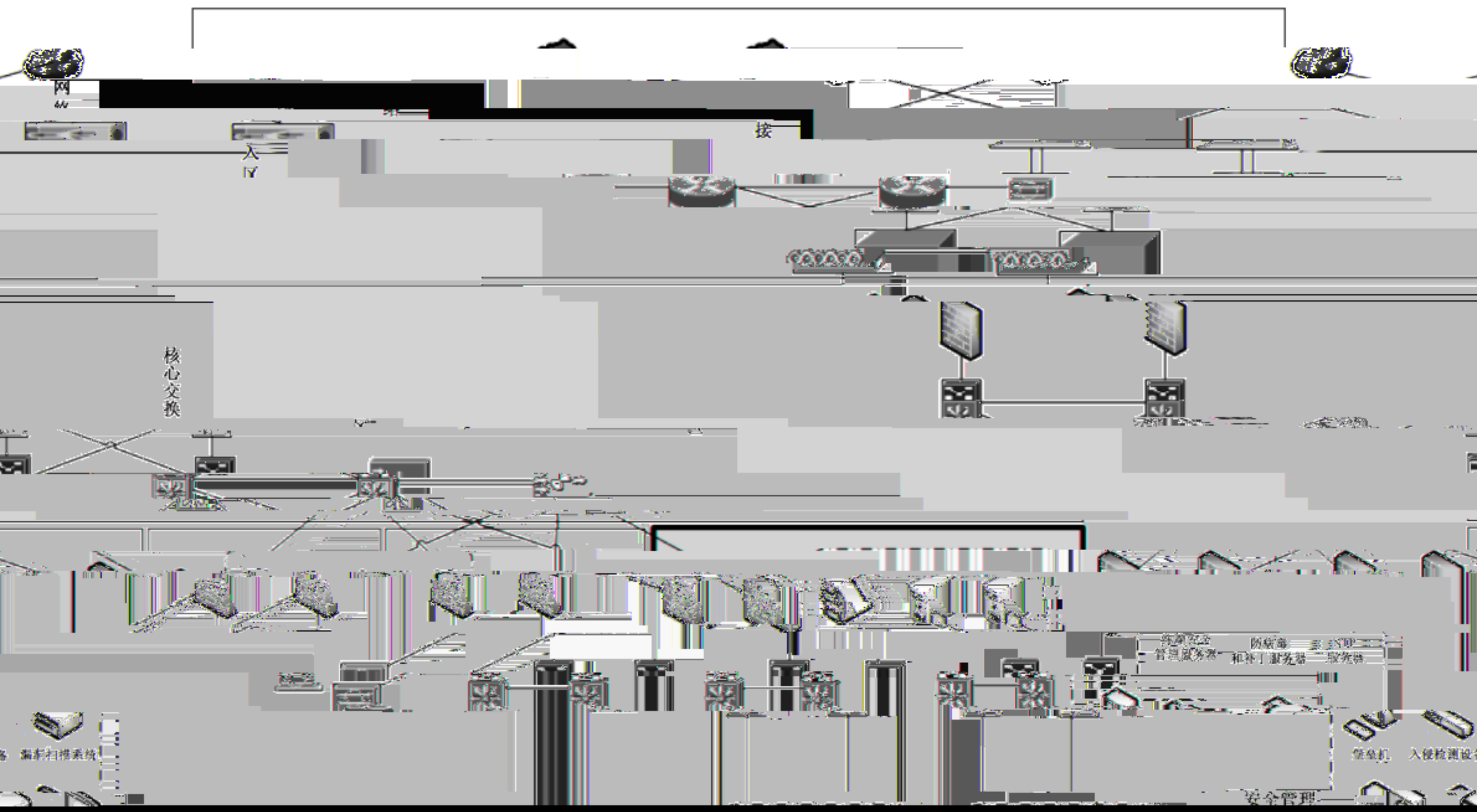
下列缩略语适用于本文件。

CPU　中央处理器(Central Processing Unit)

[illegible]

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

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


网
接
入
核心交换
防病毒
和补丁服务器
堡垒机
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：

[illegible]……CVE编号、影响的操作系统等。

[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 风险管理

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、资产价值等；[illegible]

c) 支持资产属性的自定义；

d) 支持手工录入资产信息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) 支持用户自定义安全威胁分类，[illegible]

6.1.1.4.3 脆弱性管理

脆弱性管理应允许创建并维护脆弱性列表，支持脆弱性的补充及更新。

6.1.1.4.4 风险分析

风险分析应满足以下要求：

a) 能够根据资产价值、资产面临的威胁、资产存在的脆弱性等[illegible]计算资产的安全风险；

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修改配置的方式进行调整；

c) [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]

[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：

[illegible]

6.1.2 审计管理要求

6.1.2.1 审计策略集中管理

[illegible]

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：

[illegible]

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：

[illegible]

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，保证接口之间交互数据的保密性。

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

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) 提供管理员权限最小化的职责划分，实现管理员用户权限的分离；

b) 授权管理员配置访问控制策略，规定主体对客体访问的权限；

c)

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)

b)

c) 提供覆盖到每个用户的安全审计功能，对重要用户行为和重要安全事件进行审计；

d)

e)

f)

6.3.4 软件容错

输入

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。

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 安全审计 7.3.3.8 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) 支持安全事件的自动采集功能，能够采集操作系统、数据库、网络设备、安全设备、虚拟化平台、应用系统等对象的安全事件；

b) 支持对安全事件进行过滤，能够过滤掉不感兴趣的安全事件；

c) 安全事件的内容应包括日期时间、主体标识、客体标识、事件类型、结果、IP地址、MAC地址等信息；

d) 支持以标准格式（如SYSLOG、SNMP Trap）将采集到的安全事件发送给第三方系统；

e) 支持对采集到的安全事件进行备份，并能够对备份的安全事件进行查询、统计、导出等操作。

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) 能够对安全事件进行实时告警，告警方式至少包括短信、邮件、页面提示等多种方式；

b) 能够对不同的安全事件进行分级告警，并可以根据安全事件的级别进行过滤；

c) 能够对安全事件告警进行配置，包括告警触发条件、告警接收人、告警方式等；

d) 能够对安全事件告警进行屏蔽，屏蔽后不再对该安全事件进行告警。

7.1.1.3.3 安全事件响应处置

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、受影响的操作系统、受影响的软件和硬件产品列表；

c) 能够对安全事件处置过程进行记录，形成处置报告。

7.1.1.4 安全事件分析 7.3.3.9 安全审计报表

安全事件分析应满足以下要求：

7.1.1.4.4 统计分析报表

7.1.1.4.2 资产监控

7.1.1.4.3 威胁管理

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：

7.1.1.4.5 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) 应限制管理员的最大并发会话连接数；

b) 应能够在空闲时间内自动结束会话；

c) 应能够对最大并发会话连接数进行限制；

d) 应能够对一个时间段内可以同时新建的会话连接数进行限制；

e) 应能够对一个时间段内可以同时新建的并发进程进行限制；

f) 应能够对一个时间段内可以同时新建的并发线程进行限制。

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，在发生严重入侵事件时应提供报警；

b) 应能够对重要程序的完整性进行检测，并在检测到完整性受到破坏后具有恢复的措施；

c) 应能够对重要可执行程序的完整性进行检测，并在检测到完整性受到破坏后具有恢复的措施。

7.3.8 数据完全

安全管理中心控制台的数据完全应满足以下要求：

a) 应能够检测到重要数据在传输过程中完整性受到破坏，并具有恢复的措施；

b) 应能够检测到重要数据在存储过程中完整性受到破坏，并具有恢复的措施。

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 [illegible]

数据完整性应满足以下要求：

a) 能够检测到被管理对象的鉴别信息、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；

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

c) 对重要通信提供专用通信协议或安全通信协议服务，避免来自基于通用通信协议的攻击破坏 [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：

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，备份介质场外存放；

[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；

c) 能够对安全事件进行过滤，过滤策略应支持不同粒度下的事件的屏蔽或放行；

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、操作结果等信息；

e) 安全事件应能够被查询和统计分析，查询和统计分析的条件应包括日期、时间、主体标识、客体标识、类型、描述、地址、操作结果等信息。

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) 告警方式应支持多样化，能够通过发送短信、发送邮件、在页面输出等方式实现告警，告警方式应支持自定义组合；

c) 告警信息应能够发送给指定的用户。

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) 应能够根据预先设定的响应策略，自动执行响应动作，响应动作应包括记录日志、告警、切断网络连接、阻断会话、修改防火墙访问控制策略、降低流量带宽等；

b) 应能够根据预先设定的响应策略，自动执行响应动作，响应动作应包括记录日志、告警、切断网络连接、阻断会话、修改防火墙访问控制策略、降低流量带宽等；

c) 应能够根据预先设定的响应策略，自动执行响应动作，响应动作应包括记录日志、告警、切断网络连接、阻断会话、修改防火墙访问控制策略、降低流量带宽等；

d) 应能够根据预先设定的响应策略，自动执行响应动作，响应动作应包括记录日志、告警、切断网络连接、阻断会话、修改防火墙访问控制策略、降低流量带宽等；

e) 应能够根据预先设定的响应策略，自动执行响应动作，响应动作应包括记录日志、告警、切断网络连接、阻断会话、修改防火墙访问控制策略、降低流量带宽等。

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、资产当前的脆弱性和资产面临的安全威胁，计算资产的安全风险，[illegible]

b) [illegible]

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级别、当前风险的排名等。[illegible]

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、主机操作系统、数据库、中间件、应用系统等重要性能指标，[illegible]

b) [illegible]

c) [illegible]

d) [illegible]

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) [illegible]

c) [illegible]

d) [illegible]

e) 支持在指定网络范围内进行自动发现，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，主体标记范围包括用户、代理进程、终端等，客体标记范围[illegible]

b) [illegible]

c) [illegible]

d) [illegible]

e) [illegible]

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

略的统一查询；

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

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：

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，包括策略是不

是启用、参数设置是否符合安全策略等；

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

8.1.3.2 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 IPv

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
系统管理安全审计要求	6.1.1.5.1	7.1.1.5.1	8.1.1.5.1
集中管理	6.1.1.5.2	7.1.1.5.2	8.1.1.5.2
资源监控	6.1.2.1	7.1.2.1	8.1.2.1
网络拓扑监测	6.1.2.2	7.1.2.2	8.1.2.2
安全标记	6.1.2.3	7.1.2.3	8.1.2.3
授权管理	6.1.2.4	7.1.2.4	8.1.2.4
集中管理	6.1.2.5	7.1.2.5	8.1.2.5

表 B.1（续）

管理接口设置要求	6.3.1.1	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
自身	6.3.3	7.3.3	8.3.4
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
7	事件数量	相同事件的数量
8	事件发生时间	事件发生时间
9	事件类别	事件类别
10	事件级别	事件级别
11	事件原始信息	事件内容
12	事件名称	事件名称
13	事件类型	事件类型
14	源 IP	事件的源地址
15	源端口	事件的源端口
16	源设备名称	源设备名称
17	源 MAC	事件的源 MAC 地址
18	源组织机构	事件的源组织机构
19	目的 IP	事件的目的地址
20	目的端口	事件的目的端口
21	目的设备名称	目的设备名称
22	目的 MAC	事件的目的 MAC 地址
23	目的组织机构	事件的目的组织机构
24	协议	事件的协议

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