注：

ICS 35.040
L80

中 华 人 民 共 和 国 国 家 标 准

GB/T XXXXX—

信息安全技术 网络安全等级保护安全管理中心技术要求

Information security technology—Techniques requirement of Security Management Center for information system classified protection

（征求意见稿）

2016 年 09 月 28 日

图1 XXXX－XX－XX 发布 XXXX－XX－

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会 发布

目 次

前　言

本标准编制依据国家标准化管理委员会发布的《GB/T 1.1-2009 标准化工作导则 第1部分：标准的结构和编写》的相关要求。

本标准按照GB/T 1.1-2009给出的规则起草。

本标准由全国信息安全标准化技术委员会（SAC/TC 260）提出并归口。

本标准起草单位：信息产业信息安全测评中心、公安部信息安全等级保护评估中心、网神信息技术（北京）股份有限公司

本标准主要起草人：霍珊珊、任卫红、刘健、张益、董晶晶、刘凯明、郑国刚、陶源、孙燕辉、陈广勇、朱震、李学峰

引 言

本标准为设计、研发和部署所需要的安全等级的安全管理中心提出了通用的安全技术要求，主要从网络安全保护等级划分的角度来说明，即为实现GB/T 22239-2008和GB/T 25070-2010的要求对安全管理中心通用安全技术和机制进行了规范，指导安全厂商和用户依据本标准要求进行产品研发、生产和系统设计、部署和集成。

安全管理中心是对信息系统的安全策略及安全计算环境、安全区域边界和安全通信网络上的安全机制实施统一管理的平台，是信息系统安全防御体系的重要组成部分，涉及系统管理、安全管理、审计管理等方面。本标准依据GB/T 22239-2008和GB/T 25070-2010 关于安全管理中心的要求，从安全管理中心的功能要求、接口要求、自身安全性等方面，对安全管理中心的安全要求进行更加具体的描述。

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

本标准规定了适用于不同安全保护等级的信息系统中安全管理中心的技术要求。

本标准适用于不同等级的安全管理中心的建设和配置。

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 17859-1999 计算机信息系统安全保护等级划分准则

GB/T 22239-2008 信息安全技术 信息系统安全等级保护基本要求

GB/T 25070-2010 信息安全技术 信息系统等级保护安全设计技术要求

3 术语和定义

GB 17859-1999、GB/T 5271.8和GB/T 25069-2010界定的以及下列术语和定义适用于本文件。

3.1

安全管理平台 Security Management Platform，SMP

安全管理中心的实体管理控制平台，为信息系统安全管理人员提供统一的安全防护机制和安全管理操作入口的管理平台。

3.2

数据采集接口 Data Acquisition Interface

安全管理中心采集网络环境中的各监测对象上的安全事件、脆弱性信息以及相关配置及其状态的接口。

4 安全管理中心概述

4.1 总体说明

针对信息系统的安全策略及安全计算环境、安全区域边界和安全通信网络三个部分的安全机制，形成一个统一的安全管理中心，实现统一管理、统一监控、统一审计、综合分析且协同防护。本标准将安全管理中心技术要求分为功能要求、接口要求和自身安全性要求三个大类（如图1所示）。其中，功能要求从系统管理、安全管理和审计管理三个方面提出具体要求；接口要求对安全管理中心涉及到的接口协议和接口安全做出规定；自身安全要求对安全管理中心自身安全提出具体要求。

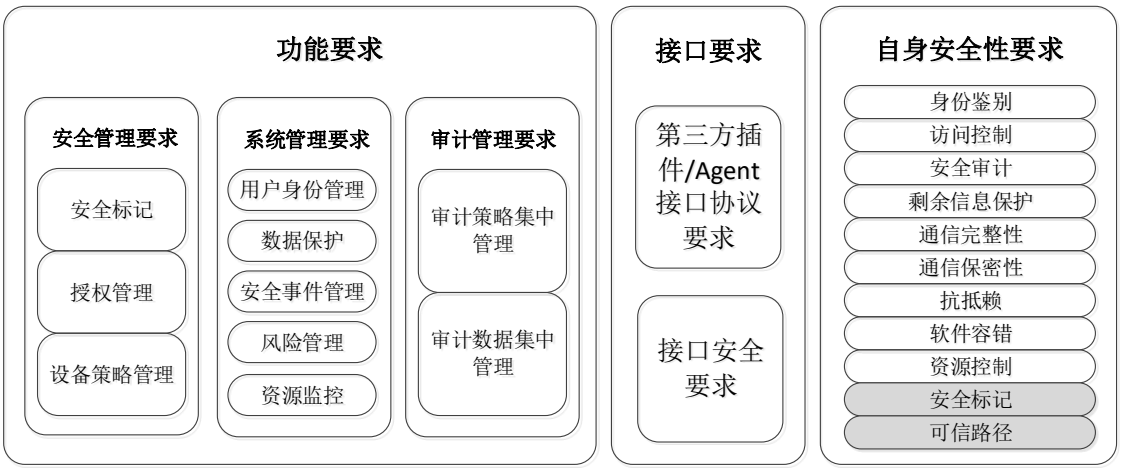

图 1 安全管理中心技术要求框架图

4.2 功能描述

统一管理是指对被保护系统和安全管理中心的主体和客体进行统一标记和基于标记授权管理，对安全管理中心涉及的相关软硬件产品在统一的管理界面进行策略配置，确保组织的安全管理策略得到贯彻和下发。

统一监控是指对被保护系统和安全管理中心自身的运行状态进行监控，对于运行过程中的异常情况及时提供告警，并通过安全事件管理等模块协助实施应急响应机制。

统一审计是指对被保护系统和安全管理中心的相关重要安全事件和用户操作行为进行审计，确保用户行为的可追溯性，提供自动化的审计分析手段，及时发现异常的安全行为，同时为综合分析提供数据支撑。

综合分析是指通过智能分析模块，针对监控数据和审计数据进行关联分析，把握被保护系统的安全运维态势，对可能出现的安全事件进行预警，对组织的安全策略制定和配置管理策略的统一调整提供指导意见。

协同防护是指针对统一监、统一审计和综合分析结果，由管理员及时对相关的安全策略配置进行调整，实现对信息系统安全的动态防护。

4.3 安全等级

本标准按照GB 17859-1999、GB/T 22239-2008和GB/T 25070-2010，分两个等级对安全管理中心的功能要求、接口要求和自身安全性提出详细要求。为清晰表示每一个安全等级比较低一级安全等级的安全技术要求的增加和增强，在第六章的描述中，每一级新增部分用“宋体加粗”表示。

5 基本级安全管理中心技术要求

5.1 功能要求

5.1.1 系统管理要求

5.1.1.1 用户身份管理

用户身份管理应满足以下要求：

a) 能够对系统中的主体和客体身份进行标识；
b) 能够对登录客体的主体身份进行鉴别；
c) 身份标识及鉴别信息应具有不易被冒用的特点；
d) 具有登录失败处理措施，可采取结束会话、限制非法登录次数和当网络登录连接超时自动退出等措施；
e) 采用两种或两种以上组合的鉴别技术对主体进行身份鉴别。

5.1.1.2 数据保护

5.1.1.2.1 数据保密性

数据保密性应满足以下要求：

a) 在通信双方建立连接之前，应用系统应利用密码技术进行会话初始化验证；
b) 对通信过程中的整个报文或会话过程进行加密；
c) 采用加密或其他保护措施实现系统管理数据、鉴别信息和重要业务数据存储保密性。

5.1.1.2.2 数据完整性

数据完整性应满足以下要求：

a) 能够检测到系统管理数据、鉴别信息和重要业务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) 能够检测到系统管理数据、鉴别信息和重要业务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。

5.1.1.2.3 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，增量数据备份至少每天一次，备份介质场外存放；
b) 备份数据应至少包含：安全管理中心采集的原始数据、主/客身份标识数据、主/客体安全标记数据、安全管理中心自身审计数据等；
c) 提供主要网络设备、通信线路和数据处理系统的硬件冗余，保证系统的高可用性。

5.1.1.2.4 剩余信息保护

剩余信息保护应满足以下要求：

a) 保证主体的鉴别信息所在的存储空间被释放或再分配给其他主体前得到完全清除，无论这些信息是存放在硬盘上还是在内存中；
b) 保证系统内的文件、目录和数据库记录等客体所在的存储空间被释放或重新分配给其他主体前得到完全清除。

5.1.1.3 安全事件管理

5.1.1.3.1 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) 能够提供与第三方信息系统的接口，发送或接收安全事件；
c) 支持对安全事件的归一化处理，将不同来源、不同格式、不同内容组成的原始事件转换成标准

的事件格式；

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、结果、IP 地址、端口等信息；

e) 安全事件采集的范围应涵盖主机设备、网络设备、数据库、安全设备、各类中间件、机房环境控制系统等；

f) 支持对采集的安全事件原始数据的集中存储。

5.1.1.3.2 告警及响应

告警及响应应满足以下要求：

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) 在产生告警时，应能够触发预先设定的事件分析规则，执行预定义的告警响应动作，如：控制台对话框告警、控制台告警音、电子邮件告警、手机短信告警、创建工单、通过 Syslog 或 SNMP Trap 向第三方系统转发告警事件等；

c) 具有对高频度发生的相同安全事件进行合并告警，避免出现告警风暴的能力。

5.1.1.3.3 统计分析

统计分析应满足以下要求：

a) 能够按照时间、事件类型等条件对安全事件进行查询；

b) 提供统计分析和报表生成功能。

5.1.1.3.4 办公协同

办公协同应满足以下要求：

a) 能够提供工单管理的功能，支持创建工单的流转流程；

b) 支持基于告警响应动作的工单管理功能；

c) 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、CVE、BUGTRAQ 编号、影响的操作系统等。安全管理中心可以根据通告提示的安全风险影响的操作系统，提供受影响的被保护资产列表；

d) 支持向第三方系统发送工单信息、安全告警、安全预警、综合风险、资产信息、安全通告等数据；

e) 支持从第三方系统接收工单信息、安全告警、安全预警、综合风险、资产信息、安全通告等数据。

5.1.1.3.5 事件关联分析

事件关联分析应满足以下要求：

a) 提供单一事件源的事件关联分析功能，并能够提供告警；

b) 针对常见的攻击行为和违规访问提供相应的关联分析规则，如针对主机扫描、端口扫描、DDOS 攻击、蠕虫、口令猜测、跳板攻击等的关联分析规则。

5.1.1.4 风险管理

5.1.1.4.1 资产管理

资产管理应满足以下要求：

a) 实现对信息系统资产的管理，提供资产的添加、修改、删除、查询与统计功能；

b) 资产管理信息应包含资产名称、资产 IP 地址、资产类型、资产责任人、资产业务价值以及资产的机密性、完整性、可用性赋值等资产属性；
c) 支持资产属性的自定义；
d) 支持手工录入资产记录或基于指定模板的批量资产导入。

5.1.1.4.2 资产业务价值评估

资产业务价值评估应满足以下要求：

建立资产业务价值评估模型，能够依据资产类型、资产重要性、损坏后造成的影响、涉及的范围等参数形成资产业务价值等级。

5.1.1.4.3 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；
b) 支持自定义安全威胁分类，如将已发生的安全事件设置为资产面临的威胁。

5.1.1.4.4 脆弱性（安全漏洞）管理

脆弱性管理应满足以下要求：

a) 允许创建并维护资产脆弱性（安全漏洞）列表；
b) 支持漏洞列表的合并及更新。

5.1.1.4.5 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（安全漏洞）及资产面临的安全威胁，计算目标资产的安全风险的安全风险；
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相应调整；
c) 安全管理系统能够以图形化的方式展现当前资产的风险级别、当前风险的排名统计等。

5.1.1.5 资源监控

5.1.1.5.1 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，实时了解这些对象的可用性状态；
b) 支持对关键指标（如：CPU 使用率、内存使用率、磁盘使用率、进程占用资源、交换分区、网络流量等方面）设置阈值，触发阈值时产生告警。

5.1.1.5.2 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、网络协议数据分析等指标；
c) 在网络运行出现异常时，能够展现在当前网络拓扑图中并相应产生告警；

d) 能够发现并阻断非授权设备的外联及接入。

5.1.2 安全管理要求

5.1.2.1 安全标记

安全标记应满足以下要求：

a) 实现对主/客体的安全标记统一管理，主体标记范围包括用户、进程、终端等，客体标记范围包括文件、目录、数据库表、磁盘、设备等；
b) 安全标记应具备唯一性，能够准确反映主/客体在定级系统中的安全属性，并且具有防止篡改和删除的能力；
c) 标记属性应包括安全级别、安全范围等敏感信息，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) 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。

5.1.2.2 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) 实现对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，不同标记的主/客体间的访问策略进行统一管理。

5.1.2.3 设备策略管理

5.1.2.3.1 设备管理

设备管理应满足以下要求：

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的统一查询。

5.1.2.3.2 入侵防御

入侵防御应满足以下要求：

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。

5.1.2.3.3 恶意代码防范

恶意代码防范应满足以下要求：

a) 对恶意代码防范产品统一升级监控和管理；
b) 对恶意代码防范情况的数据采集；
c) 统一的消息上报。

5.1.3 审计管理要求

5.1.3.1 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，包括策略是否开启、参数设施是否符合安全策略等；

b） 提供预定义响应行为管理功能，能够启用或关闭针对不同的安全审计日志的响应行为。

5.1.3.2 审计数据集中管理

5.1.3.2.1 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） 支持设定查询条件进行审计数据查询；

c） 能够对采集的原始审计数据进行集中存储；

d） 严格限制审计数据的访问控制权限，限制管理用户对审计数据的访问，实现管理用户和审计用户的权限分离，避免非授权的删除、修改或覆盖；

e） 支持对各种审计数据按规则进行过滤处理；

f） 支持对数据采集信息按照特定规则进行合并。

5.1.3.2.2 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、流量管理、负载均衡等网络基础支撑设备）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平台和桌面电脑、笔记本电脑、手持终端等终端用户访问信息系统所使用的设备）的审计数据采集；

c） 支持对数据库（如 Oracle、My SQL、MSSQL Server 等）的审计数据采集；

d） 支持对安全设备（如防火墙、入侵监测系统、抗拒绝服务攻击设备、防病毒系统、应用安全审计系统、访问控制系统等与信息系统安全防护相关的各种系统和设备）的审计数据采集；

e） 支持对各类中间件的审计数据采集；

f） 支持对机房环境控制系统（如空调、温度、湿度控制、消防设备、门禁系统等）的审计数据采集；

g） 支持对其他应用系统或相关平台的审计数据采集。

5.1.3.2.3 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） 通过统一接口，接收被监测系统或设备的安全审计数据。

5.1.3.2.4 审计数据关联分析

审计数据关联分析应满足以下要求：

应支持将来自不同采集对象的审计数据在一个分析规则中进行分析。

5.2 接口要求

5.2.1 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/IPv6混合环境）；

b) 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件或者 Agent 的接口实现各组件之间、与第三方平台之间的数据交换。

5.2.2 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设计，确保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。

5.3 自身安全性要求

5.3.1 身份鉴别

身份鉴别应满足以下要求：

a) 提供专用的登录控制模块对登录安全管理平台的用户进行身份标识和鉴别；
b) 对同一用户采用两种或两种以上组合的鉴别技术实现用户身份鉴别；
c) 提供用户身份标识唯一和鉴别信息复杂度检查功能，保证安全管理平台中不存在重复用户身份标识，身份鉴别信息不易被冒用；
d) 提供登录失败处理功能，可采取结束会话、限制非法登录次数和自动退出等措施；
e) 启用身份鉴别、用户身份标识唯一性检查、用户身份鉴别信息复杂度检查以及登录失败处理功能，并根据安全策略配置相关参数。

5.3.2 访问控制

访问控制应满足以下要求：

a) 提供自主访问控制功能，依据安全策略控制用户对文件、数据库表等客体的访问；
b) 自主访问控制的覆盖范围应包括与信息直接相关的主体、客体及它们之间的操作；
c) 由授权主体配置访问控制策略，并禁止默认账户的访问；
d) 实现安全管理平台特权用户的权限分离，应授予不同账户为完成各自承担任务所需的最小权限，并在它们之间形成相互制约的关系。

5.3.3 安全审计

安全审计应满足以下要求：

a) 提供覆盖到每个用户的安全审计功能，记录所有用户对安全管理平台重要操作和安全事件进行审计；
b) 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、描述和结果等；
d) 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；
e) 根据统一安全策略，提供集中审计接口。

5.3.4 剩余信息保护

剩余信息保护应满足以下要求：

a) 保证用户的鉴别信息所在的存储空间被释放或再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；
b) 保证系统内的文件、目录和数据库记录等资源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。

5.3.5 通信完整性

通信完整性应满足以下要求：
利用密码技术保证通信过程中数据的完整性。

5.3.6 通信保密性

通信保密性应满足以下要求：
a) 在通信双方建立连接之前，安全管理平台应利用密码技术进行会话初始化验证；
b) 对通信过程中的整个报文或会话过程进行加密。

5.3.7 抗抵赖

抗抵赖应满足以下要求：
a) 具有在请求的情况下为数据原发者或接收者提供数据原发证据的功能；
b) 具有在请求的情况下为数据原发者或接收者提供数据接收证据的功能。

5.3.8 软件容错

软件容错应满足以下要求：
a) 提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的数据格式或长度符合系统设定要求；
b) 提供自动恢复功能，当故障发生时能够恢复工作状态。

5.3.9 资源控制

资源控制应满足以下要求：
a) 对安全管理平台的管理员登录地址进行限制；
b) 当安全管理平台中的通信双方中的一方在一段时间内未作任何响应，另一方应能够自动结束会话；
c) 能够对安全管理平台的最大并发会话连接数进行限制；
d) 能够对单个账户的多重并发会话进行限制；
e) 能够对一个时间段内可能的并发会话连接数进行限制；
f) 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；
g) 提供对其自身运行状态的实时监测，应能够对安全管理平台服务水平降低到预先规定的最小值进行检测和报警；
h) 提供服务优先级设定功能，并在安装后根据安全策略设定访问账户或请求进程的优先级，根据优先级分配系统资源。

5.3.10 入侵防范

入侵防范应满足以下要求：
a) 能够检测到对安全管理平台各服务器、网络设备和安全设备进行入侵的行为，并及时更新入侵事件特征库；
b) 能够记录入侵的源 IP、攻击的类型、攻击的目的、攻击的时间，并在发生严重入侵事件时提供报警；
c) 能够对安全管理平台各服务器上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；

d) 安全管理平台各服务器操作系统应遵循最小安装的原则，仅安装需要的组件和应用程序，并通过设置升级服务器等方式保持系统补丁及时得到更新；
e) 安全管理平台各数据库系统、网络设备及安全设备补丁应及时得到更新。

5.3.11 数据安全

数据安全应满足以下要求：
a) 能够检测到管理数据和鉴别信息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) 采用加密或其他有效措施实现管理数据和鉴别信息的数据传输保密性；
c) 能够检测到管理数据和鉴别信息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；
d) 采用加密或其他保护措施实现管理数据和鉴别信息的数据存储保密性。

6 增强级安全管理中心技术要求

6.1 功能要求

6.1.1 系统管理要求

6.1.1.1 用户身份管理

用户身份管理应满足以下要求：
a) 能够对系统中的主体和客体身份进行标识；
b) 能够对登录客体的主体身份进行鉴别；
c) 身份标识及鉴别信息应具有不易被冒用的特点；
d) 具有登录失败处理措施，可采取结束会话、限制非法登录次数和当网络登录连接超时自动退出等措施；
e) 采用两种或两种以上组合的鉴别技术对主体进行身份鉴别，**并且身份鉴别信息至少有一种是不可伪造的**。

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：
a) 在通信双方建立连接之前，系统应利用密码技术进行会话初始化验证；
b) 对通信过程中的整个报文或会话过程进行加密；
c) 采用加密或其他保护措施实现系统管理数据、鉴别信息和重要业务数据存储保密性；
d) **基于硬件化的设备对重要通信过程进行加解密运算和密钥管理；**
e) **对重要通信提供专用通信协议或安全通信协议服务，避免来自基于通用协议的攻击破坏数据保密性。**

6.1.1.2.2 数据完整性

数据完整性应满足以下要求：
a) 能够检测到系统管理数据、鉴别信息和重要业务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) 能够检测到系统管理数据、鉴别信息和重要业务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：
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；
b) 备份数据应至少包含：安全管理中心采集的原始数据、主/客身份标识数据、主/客体安全标记数据、安全管理中心自身审计数据等；
c) **提供异地实时备份功能，利用通信网络将数据实时备份至灾难备份中心；**
d) 提供主要网络设备、通信线路和数据处理系统的硬件冗余，保证系统的高可用性。

6.1.1.2.4 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，应保证在被访问的客体与主体之间应能够建立一条安全的信息传输路径。**

6.1.1.2.5 剩余信息保护

剩余信息保护应满足以下要求：
a) 保证主体的鉴别信息所在的存储空间被释放或再分配给其他主体前得到完全清除，无论这些信息是存放在硬盘上还是在内存中；
b) 保证系统内的文件、目录和数据库记录等客体所在的存储空间被释放或重新分配给其他主体前得到完全清除。

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) 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) 能够提供与第三方信息系统的接口，发送或接收安全事件；
c) 支持对安全事件的归一化处理，将不同来源、不同格式、不同内容组成的原始事件转换成标准的事件格式；
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、结果、IP 地址、端口等信息；
e) 安全事件采集的范围应涵盖主机设备、网络设备、数据库、安全设备、各类中间件、机房环境控制系统等；
f) 支持对采集的安全事件原始数据的集中存储。

6.1.1.3.2 告警及响应

告警及响应应满足以下要求：
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) 在产生告警时，应能够触发预先设定的事件分析规则，执行预定义的告警响应动作，如：控制台对话框告警、控制台告警音、电子邮件告警、手机短信告警、创建工单、通过 Syslog 或 SNMP Trap 向第三方系统转发告警事件等；
c) 具有对高频度发生的相同安全事件进行合并告警，避免出现告警风暴的能力。

6.1.1.3.3 统计分析

统计分析应满足以下要求：
a) 能够按照时间、事件类型等条件对安全事件进行查询；
b) 提供统计分析和报表生成功能。

6.1.1.3.4 办公协同

办公协同应满足以下要求：
a) 能够提供工单管理的功能，支持创建工单的流转流程；
b) 支持基于告警响应动作的工单管理功能；
c) 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、CVE、BUGTRAQ 编号、影响的操作系统等。安全管理中心可以根据通告提示的安全风险影响的操作系统，提供受影响的被保护资产列表；
d) 支持向第三方系统发送工单信息、安全告警、安全预警、综合风险、资产信息、安全通告等数据；
e) 支持从第三方系统接收工单信息、安全告警、安全预警、综合风险、资产信息、安全通告等数据。

6.1.1.3.5 事件关联分析

事件关联分析应满足以下要求：
a) 支持将来自不同事件源的事件在一个分析规则中进行分析，从而能从海量事件中过滤出有逻辑关系的事件序列，据此给出相应的告警；
b) **提供多事件源事件关联、时序关联、统计关联以及针对慢攻击的长时间窗口的关联等关联分析功能，并能够提供告警；**
c) 针对常见的攻击行为和违规访问提供相应的关联分析规则，如针对主机扫描、端口扫描、DDOS 攻击、蠕虫、口令猜测、跳板攻击等的关联分析规则；
d) **提供自定义关联规则编辑功能。**

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) 实现对信息系统资产的管理，**以安全域等方式组织资产，**提供资产的添加、修改、删除、查询与统计功能；
b) 资产管理信息应包含资产名称、资产 IP 地址、资产类型、资产责任人、资产业务价值以及资产的机密性、完整性、可用性赋值等资产属性；
c) 支持资产属性的自定义；
d) 支持手工录入资产记录或基于指定模板的批量资产导入；
e) **支持对资产的自动发现，并能够将其自动添加到资产库中。**

6.1.1.4.2 资产业务价值评估

资产业务价值评估应满足以下要求：

建立资产业务价值评估模型，能够依据资产类型、资产重要性、损坏后造成的影响、涉及的范围等参数形成资产业务价值等级。

6.1.1.4.3 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；
b) 支持自定义安全威胁分类，如将已发生的安全事件设置为资产面临的威胁。

6.1.1.4.4 脆弱性（安全漏洞）管理

脆弱性管理应满足以下要求：

a) 允许创建并维护资产脆弱性（安全漏洞）列表；
b) 支持漏洞列表的合并及更新；
c) **支持通过特定代理程序或扫描器获取的相关设备或系统的漏洞和脆弱性信息的导入；**
d) **能够根据漏洞和脆弱性信息，自动生成所涉及的信息资产清单。**

6.1.1.4.5 风险分析

风险分析应满足以下要求：

a) 能够根据应能够根据资产的业务价值、资产当前的脆弱性（安全漏洞）及资产面临的安全威胁，计算目标资产的安全风险**和资产所在安全域**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相应调整；
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、当前风险的排名统计等。

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，实时了解这些对象的可用性状态；
b) 支持对关键指标（如：CPU 使用率、内存使用率、磁盘使用率、进程占用资源、交换分区、网络流量等方面）设置阈值，触发阈值时产生告警**，执行预定义的响应动作**。

6.1.1.5.2 网络拓扑监测

网络拓扑监测应满足以下要求：

a) **支持在指定网络范围内进行拓扑发现并自动生成网络拓扑图；**
b) 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；
c) 能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、网络协议数据分析等指标；
d) 在网络运行出现异常时，能够展现在当前网络拓扑图中并相应产生告警；
e) 能够发现并阻断非授权设备的外联及接入。

6.1.2 安全管理要求

6.1.2.1 安全标记

安全标记应满足以下要求：

a) 实现对主/客体的安全标记统一管理，主体标记范围包括用户、进程、终端等，客体标记范围包括文件、目录、数据库表、磁盘、设备等；
b) 安全标记应具备唯一性，能够准确反映主/客体在定级系统中的安全属性，并且具有防止篡改和删除的能力；
c) 标记属性应包括安全级别、安全范围等敏感信息，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) 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；
e) **实现安全标记的自定义。**

6.1.2.2 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) 实现对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，**针对不同安全层次、**不同标记的主/客体间的访问策略进行统一管理。

6.1.2.3 设备策略管理

6.1.2.3.1 设备管理

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；
b) **实现对主机操作系统、数据库系统、网络设备、安全设备等设备配置策略的统一制定和下发。**

6.1.2.3.2 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；
b) **实现对主机操作系统、数据库、网络设备、安全设备入侵防御措施的联动和管理。**

6.1.2.3.3 恶意代码防范

恶意代码防范应满足以下要求：

a) 对恶意代码防范产品统一升级监控和管理；
b) 对恶意代码防范情况的数据采集；
c) 统一的消息上报。

6.1.3 审计管理要求

6.1.3.1 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，包括策略是否开启、参数设施是否符合安全策略等；
b) 提供预定义响应行为管理功能，能够启用或关闭针对不同的安全审计日志的响应行为；
c) **提供自定义响应行为管理功能；**
d) **能够实现对主机操作系统、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。**

6.1.3.2 审计数据集中管理

6.1.3.2.1 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) **能够并根据设定的报表模版生成相应的审计报告；**
c) 支持设定查询条件进行审计数据查询；
d) 能够对采集的原始审计数据进行集中存储；
e) 严格限制审计数据的访问控制权限，限制管理用户对审计数据的访问，实现管理用户和审计用户的权限分离，避免非授权的删除、修改或覆盖；
f) 支持对各种审计数据按规则进行过滤处理；
g) 支持对数据采集信息按照特定规则进行合并。

6.1.3.2.2 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、流量管理、负载均衡等网络基础支撑设备）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平台和桌面电脑、笔记本电脑、手持终端等终端用户访问信息系统所使用的设备）的审计数据采集；
c) 支持对数据库（如 Oracle、My SQL、MSSQL Server 等）的审计数据采集；
d) 支持对安全设备（如防火墙、入侵监测系统、抗拒绝服务攻击设备、防病毒系统、应用安全审计系统、访问控制系统等与信息系统安全防护相关的各种系统和设备）的审计数据采集；
e) 支持对各类中间件的审计数据采集；
f) 支持对机房环境控制系统（如空调、温度、湿度控制、消防设备、门禁系统等）的审计数据采集；
g) 支持对其他应用系统或相关平台的审计数据采集。

6.1.3.2.3 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 协议采集各种系统或设备上的审计数据；
b) **支持基于文件的日志数据采集方式获得被监测系统或设备的审计数据文件；**
c) **支持通过部署软件代理的方式采集特定系统的审计数据；**
d) 通过统一接口，接收被监测系统或设备的安全审计数据。

6.1.3.2.4 **数据采集组件要求**

数据采集组件要求应满足以下要求：

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监控数据。

6.1.3.2.5 审计数据关联分析

审计数据关联分析应满足以下要求：

a) 应支持将来自不同采集对象的审计数据在一个分析规则中进行分析；

b) **应提供审计关联规则自定义功能。**

6.2 接口要求

6.2.1 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/IPv6混合环境）；

b) 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件或者Agent的接口实现各组件之间、与第三方平台之间的数据交换；

c) **提供外部接口实现不同平台之间的同步或异步的数据交互；**

d) **支持通过编写并加载配置文件的方式，实现对第三方设备、系统的接入管理。**

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设计，确保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；

c) **各安全接口之间进行通信时，应通过可信验证机制相互验证对方的可信性，确保可信连接。**

6.3 自身安全性要求

6.3.1 身份鉴别

身份鉴别应满足以下要求：

a) 提供专用的登录控制模块对登录安全管理平台的用户进行身份标识和鉴别；

b) 对同一用户采用两种或两种以上组合的鉴别技术实现用户身份鉴别，**其中一种是不可伪造的；**

c) 提供用户身份标识唯一和鉴别信息复杂度检查功能，保证安全管理平台中不存在重复用户身份标识，身份鉴别信息不易被冒用；

d) 提供登录失败处理功能，可采取结束会话、限制非法登录次数和自动退出等措施；

e) 启用身份鉴别、用户身份标识唯一性检查、用户身份鉴别信息复杂度检查以及登录失败处理功能，并根据安全策略配置相关参数。

6.3.2 安全标记

安全标记应满足以下要求：

应提供为主体和客体设置安全标记的功能并在安装后启用。

6.3.3 访问控制

访问控制应满足以下要求：

a) 提供自主访问控制功能，依据安全策略控制用户对文件、数据库表等客体的访问；

b) 自主访问控制的覆盖范围应包括与信息直接相关的主体、客体及它们之间的操作；
c) 由授权主体配置访问控制策略，并禁止默认账户的访问；
d) 实现安全管理平台特权用户的权限分离，应授予不同账户为完成各自承担任务所需的最小权限，并在它们之间形成相互制约的关系；
e) 通过比较安全标记来确定是授予还是拒绝主体对客体的访问。

6.3.4 可信路径

可信路径应满足以下要求：

a) 在安全管理平台对用户进行身份鉴别时，应能够建立一条安全的信息传输路径；
b) 在用户通过应用系统对资源进行访问时，安全管理平台应保证在被访问的资源与用户之间应能够建立一条安全的信息传输路径。

6.3.5 安全审计

安全审计应满足以下要求：

a) 提供覆盖到每个用户的安全审计功能，记录所有用户对安全管理平台重要操作和安全事件进行审计；
b) 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、描述和结果等；
d) 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；
e) 根据统一安全策略，提供集中审计接口。

6.3.6 剩余信息保护

剩余信息保护应满足以下要求：

a) 保证用户的鉴别信息所在的存储空间被释放或再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；
b) 保证系统内的文件、目录和数据库记录等资源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。

6.3.7 通信完整性

通信完整性应满足以下要求：
利用密码技术保证通信过程中数据的完整性。

6.3.8 通信保密性

通信保密性应满足以下要求：

a) 在通信双方建立连接之前，安全管理平台应利用密码技术进行会话初始化验证；
b) 对通信过程中的整个报文或会话过程进行加密；
c) 基于硬件化的设备对重要通信过程进行加解密运算和密钥管理。

6.3.9 抗抵赖

抗抵赖应满足以下要求：

a) 具有在请求的情况下为数据原发者或接收者提供数据原发证据的功能；
b) 具有在请求的情况下为数据原发者或接收者提供数据接收证据的功能。

6.3.10 软件容错

软件容错应满足以下要求：

a) 提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的数据格式或长度符合系统设定要求；

b) 提供自动保护功能，当故障发生时自动保护当前所有状态；

c) 提供自动恢复功能，当故障发生时能够恢复工作状态。

6.3.11 资源控制

资源控制应满足以下要求：

a) 对安全管理平台的管理员登录地址进行限制；

b) 当安全管理平台中的通信双方中的一方在一段时间内未作任何响应，另一方应能够自动结束会话；

c) 能够对安全管理平台的最大并发会话连接数进行限制；

d) 能够对单个账户的多重并发会话进行限制；

e) 能够对一个时间段内可能的并发会话连接数进行限制；

f) 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；

g) 提供对其自身运行状态的实时监测，应能够对安全管理平台服务水平降低到预先规定的最小值进行检测和报警；

h) 提供服务优先级设定功能，并在安装后根据安全策略设定访问账户或请求进程的优先级，根据优先级分配系统资源。

6.3.12 入侵防范

入侵防范应满足以下要求：

a) 能够检测到对安全管理平台各服务器、网络设备和安全设备进行入侵的行为，并及时更新入侵事件特征库；

b) 能够记录入侵的源 IP、攻击的类型、攻击的目的、攻击的时间，并在发生严重入侵事件时提供报警；

c) 能够对安全管理平台各服务器上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；

d) 安全管理平台各服务器操作系统应遵循最小安装的原则，仅安装需要的组件和应用程序，并通过设置升级服务器等方式保持系统补丁及时得到更新；

e) 安全管理平台各数据库系统、网络设备及安全设备补丁应及时得到更新。

6.3.13 数据安全

数据安全应满足以下要求：

a) 能够检测到管理数据和鉴别信息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) 采用加密或其他有效措施实现管理数据和鉴别信息的数据传输保密性；

c) 能够检测到管理数据和鉴别信息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；

d) 采用加密或其他保护措施实现管理数据和鉴别信息的数据存储保密性；

e) 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

数据完整性和保密性。

附 录 A
（资料性附录）
安全管理中心与信息系统等级对应关系

安全管理中心与信息系统等级对应关系见表A.1。

表A.1 安全管理中心与信息系统等级对应表

安全管理中心级别	信息系统等级
基本级	二级、三级
增强级	四级

附 录 B
（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B.1。

表 B.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	事件发生时间	事件在安全设备的发生时间
9	事件类型	事件类别
10	事件名称	事件名
11	事件内容	事件原始信息
12	应用协议	事件相关的协议名
13	严重级别	事件的严重级别
14	目的IP	事件的目的地址
15	目的端口	事件的目的端口
16	目的主机名	事件目的主机名称
17	源IP	事件的源地址
18	源端口	事件的源端口

序号	属性	描述
19	源主机名	事件源主机名称
20	多个自定义属性	用户根据需要自己定义的属性