



中华人民共和国国家标准

由化人思

~~GB/T 36958-2018~~

~~Requirements of security~~ Information security technology ~~Technical requirements~~
~~of cyber security~~ management center for classified protection of

发布 2019-07-01 实施 2018-12-28

南京 北京 天津 上海 香港 廣州 汕頭 廈門 福州 煙台 濟南 青島 大連 長春 哈爾濱 瀋陽 西安 蘭州 西寧 昆明 貴陽 成都 重慶 萬縣 宜昌 沙市 漢口 蕪湖 安慶 九江 南昌 杭州 寧波 溫州 紹興 嘉興 湖州 蘇州 無錫 常州 鎮江 揚州 南通 徐州 蚌埠 蕪湖 安慶 九江 南昌 杭州 寧波 溫州 紹興 嘉興 湖州 蘇州 無錫 常州 鎮江 揚州 南通 徐州 蚌埠

1	范围	1	引言	2
1	规范性引用文件	1	1 范围	2
1	术语和定义	1	2 规范性引用文件	2
1	缩略语	1	3 术语和定义	2
2	第二级安全管理中心技术要求	2	4 缩略语	2
2.1	功能要求	2		
2.2	接口要求	2		
2.3	自身安全要求	2		
3	第三级安全管理中心技术要求	3		
3.1	功能要求	3		
3.2	接口要求	3		
3.3	自身安全要求	3		
4	第四级安全管理中心技术要求	4		
4.1	功能要求	4		
4.2	接口要求	4		
4.3	自身安全要求	4		
5	第五级安全管理中心技术要求	5		
5.1	功能要求	5		
5.2	接口要求	5		
5.3	自身安全要求	5		
6	跨定级系统安全管理中心技术要求	6		
6.1	功能要求	6		
6.2	接口要求	6		
6.3	自身安全要求	6		
7	附录A (规范性附录) 网络安全等级保护系统建设要求	7		
7.1	功能要求	7		
7.2	接口要求	7		
7.3	自身安全要求	7		
8	附录B (规范性附录) 网络安全等级保护系统建设要求	8		
8.1	功能要求	8		
8.2	接口要求	8		
8.3	自身安全要求	8		
9	附录C (规范性附录) 网络安全等级保护系统建设要求	9		
9.1	功能要求	9		
9.2	接口要求	9		
9.3	自身安全要求	9		
10	附录D (规范性附录) 网络安全等级保护系统建设要求	10		
10.1	功能要求	10		
10.2	接口要求	10		
10.3	自身安全要求	10		
11	附录E (规范性附录) 网络安全等级保护系统建设要求	11		
11.1	功能要求	11		
11.2	接口要求	11		
11.3	自身安全要求	11		
12	附录F (规范性附录) 网络安全等级保护系统建设要求	12		
12.1	功能要求	12		
12.2	接口要求	12		
12.3	自身安全要求	12		
13	附录G (规范性附录) 网络安全等级保护系统建设要求	13		
13.1	功能要求	13		
13.2	接口要求	13		
13.3	自身安全要求	13		
14	附录H (规范性附录) 网络安全等级保护系统建设要求	14		
14.1	功能要求	14		
14.2	接口要求	14		
14.3	自身安全要求	14		
15	附录I (规范性附录) 网络安全等级保护系统建设要求	15		
15.1	功能要求	15		
15.2	接口要求	15		
15.3	自身安全要求	15		
16	附录J (规范性附录) 网络安全等级保护系统建设要求	16		
16.1	功能要求	16		
16.2	接口要求	16		
16.3	自身安全要求	16		
17	附录K (规范性附录) 网络安全等级保护系统建设要求	17		
17.1	功能要求	17		
17.2	接口要求	17		
17.3	自身安全要求	17		
18	附录L (规范性附录) 网络安全等级保护系统建设要求	18		
18.1	功能要求	18		
18.2	接口要求	18		
18.3	自身安全要求	18		
19	附录M (规范性附录) 网络安全等级保护系统建设要求	19		
19.1	功能要求	19		
19.2	接口要求	19		
19.3	自身安全要求	19		
20	附录N (规范性附录) 网络安全等级保护系统建设要求	20		
20.1	功能要求	20		
20.2	接口要求	20		
20.3	自身安全要求	20		
21	附录O (规范性附录) 网络安全等级保护系统建设要求	21		
21.1	功能要求	21		
21.2	接口要求	21		
21.3	自身安全要求	21		
22	附录P (规范性附录) 网络安全等级保护系统建设要求	22		
22.1	功能要求	22		
22.2	接口要求	22		
22.3	自身安全要求	22		
23	附录Q (规范性附录) 网络安全等级保护系统建设要求	23		
23.1	功能要求	23		
23.2	接口要求	23		
23.3	自身安全要求	23		
24	附录R (规范性附录) 网络安全等级保护系统建设要求	24		
24.1	功能要求	24		
24.2	接口要求	24		
24.3	自身安全要求	24		
25	附录S (规范性附录) 网络安全等级保护系统建设要求	25		
25.1	功能要求	25		
25.2	接口要求	25		
25.3	自身安全要求	25		
26	附录T (规范性附录) 网络安全等级保护系统建设要求	26		
26.1	功能要求	26		
26.2	接口要求	26		
26.3	自身安全要求	26		
27	附录U (规范性附录) 网络安全等级保护系统建设要求	27		
27.1	功能要求	27		
27.2	接口要求	27		
27.3	自身安全要求	27		

前 言

1—2009 给出的规则起草

本标准按照 GB/T 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 5271.8—2018 信息安全技术 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—2010 信息安全技术 术语

2 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

3.1.1

物理访问接口 physical access interface

物理访问接口是指物理访问设备与物理访问对象的连接接口,用于物理访问设备对物理访问对象进行物理访问。

3.2

3.2.1

采集器 collector

采集器是指用于采集网络安全事件、日志、告警等信息的设备。

3.3

安全管理中心 security management center

安全管理中心是指用于集中管理网络安全事件、日志、告警等信息,并提供集中分析和响应的系统。

3.4

注:修改自GB/T 25069—2010定义。

4 缩略语

下列缩略语适用于本文件。

CPU 中央处理器(Central Processing Unit)

Computer Vulnerabilities Exposures

CVE 通用漏洞编号计划(Common Vulnerabilities and Exposures)

Distributed Denial of Service

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

IP 互联网协议(Internet Protocol)

IP 地址 33350 3340

IP 地址 33350 3340

IP 地址 33350 3340



能够对其管理对象的名录管理信息进行鉴别,并对其进行鉴别信息的有效性验证。

6.1.1

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) 在安全使用环境上,应使管理信息的管理过程,可防止被未授权人员非法访问或篡改;
- b) 应使用密码技术对安全信息进行加密。

6.1.1.2.2 数据完整性

数据完整性应满足以下要求:

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) 将任意的数据备份与恢复功能,应是数据名称与内容,在多个安全场所存储;

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) 应能安全事件按照要求及时发现和采集发生的安全事件;

集的安全事件原始数据的集中存储。

详细可参考附录C。

e) 能够对采

注:安全事件的

告警

6.1.1.3.2 安全事件

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。

安全事件告警

响应

6.1.1.3.3 安全事件

应满足以下要求:

安全事件响应

二六五 雅集詩話的纂修系統之二

6 1 1 2 1 66218

25. 101

2. 1

43

— — — — —

6 1 1 4 1 盜

$$\frac{2}{3} \times 100 = 66\frac{2}{3}\%$$

2

1

1

a) 具备预先定义的威胁分类;

Figure 6. The effect of the initial concentration of the monomer on the polymerization rate.

論三國經義之流傳與經義之變遷

④ 资本风险的计算规则和计算公式能够根据部署环境的实际

10

Figure 1. Schematic diagram of the experimental setup.

1230

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

审计策略集中管理应部署在骨干操作系统、数据库系统、网络设备、安全设备、服务器、主机等配置设备

6.1.2.2 审计数据集中管理

6.1.2.2.1 审计数据采集

5) 支持对全网设备产生的审计数据进行集中采集；

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

笔带型接口和自定义接口以及第三方的插

安全管理中心应支持 SNMP Trap Syslog Web Service

6.3.6 入侵防范

6.3.7 数据安全

安全管理中心应能执行的数据安全应满足以下要求：

- a) 能够检测到被管理对象数据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) 能够对被管理对象数据完整性进行持续监测。

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：

- a) 能够对被管理对象数据完整性进行持续监测；
- b) 能够对被管理对象数据完整性进行持续监测；
- c) 能够对被管理对象数据完整性进行持续监测；
- d) 能够对被管理对象数据完整性进行持续监测；
- e) 能够对被管理对象数据完整性进行持续监测；
- f) 能够对被管理对象数据完整性进行持续监测；
- g) 能够对被管理对象数据完整性进行持续监测；
- h) 能够对被管理对象数据完整性进行持续监测；
- i) 能够对被管理对象数据完整性进行持续监测；
- j) 能够对被管理对象数据完整性进行持续监测；
- k) 能够对被管理对象数据完整性进行持续监测；
- l) 能够对被管理对象数据完整性进行持续监测；
- m) 能够对被管理对象数据完整性进行持续监测；
- n) 能够对被管理对象数据完整性进行持续监测；
- o) 能够对被管理对象数据完整性进行持续监测；
- p) 能够对被管理对象数据完整性进行持续监测；
- q) 能够对被管理对象数据完整性进行持续监测；
- r) 能够对被管理对象数据完整性进行持续监测；
- s) 能够对被管理对象数据完整性进行持续监测；
- t) 能够对被管理对象数据完整性进行持续监测；
- u) 能够对被管理对象数据完整性进行持续监测；
- v) 能够对被管理对象数据完整性进行持续监测；
- w) 能够对被管理对象数据完整性进行持续监测；
- x) 能够对被管理对象数据完整性进行持续监测；
- y) 能够对被管理对象数据完整性进行持续监测；
- z) 能够对被管理对象数据完整性进行持续监测；

7.1.1.2 数据保护

7.1.1.2.1 数据保密性

数据保密性应满足以下要求：

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数据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) 能够对被管理对象数据完整性进行持续监测；
- c) 能够对被管理对象数据完整性进行持续监测；
- d) 能够对被管理对象数据完整性进行持续监测；
- e) 能够对被管理对象数据完整性进行持续监测；
- f) 能够对被管理对象数据完整性进行持续监测；
- g) 能够对被管理对象数据完整性进行持续监测；
- h) 能够对被管理对象数据完整性进行持续监测；
- i) 能够对被管理对象数据完整性进行持续监测；
- j) 能够对被管理对象数据完整性进行持续监测；
- k) 能够对被管理对象数据完整性进行持续监测；
- l) 能够对被管理对象数据完整性进行持续监测；
- m) 能够对被管理对象数据完整性进行持续监测；
- n) 能够对被管理对象数据完整性进行持续监测；
- o) 能够对被管理对象数据完整性进行持续监测；
- p) 能够对被管理对象数据完整性进行持续监测；
- q) 能够对被管理对象数据完整性进行持续监测；
- r) 能够对被管理对象数据完整性进行持续监测；
- s) 能够对被管理对象数据完整性进行持续监测；
- t) 能够对被管理对象数据完整性进行持续监测；
- u) 能够对被管理对象数据完整性进行持续监测；
- v) 能够对被管理对象数据完整性进行持续监测；
- w) 能够对被管理对象数据完整性进行持续监测；
- x) 能够对被管理对象数据完整性进行持续监测；
- y) 能够对被管理对象数据完整性进行持续监测；
- z) 能够对被管理对象数据完整性进行持续监测；

7.1.1.2.4 剩余信息

A wide panoramic view of a city skyline at night, featuring numerous illuminated buildings and structures along a waterfront. The lights from the buildings create a vibrant contrast against the dark sky and water.

安全事件采集应满足以下要求：

标识: 事件标题, 类型, 结果, IP地址, 端口号等值。c. 安全事件的调查应包括但不限于: 时间, 时

五、公司主要会计数据、财务指标如下：

Figure 1. The effect of the number of trials on the number of correct responses. The number of correct responses was significantly higher for the 10 trials condition than for the 5 trials condition. Error bars represent the standard error of the mean.

100

1) 能够提供安全逃生功能,可以创建或已入安全网络逃生,逃生中应勾括逃生内容,逃生信息。

4. 每段以 1 厘米为限，每段以 1 厘米为限，每段以 1 厘米为限。

9

及时了解其运行状态。

设备运行异常时,能及时发现并告警。

告警处理要求:

控制系统应能够对控制系统设备可用性、安全性和完整性进行实时监控,可以对设备故障告警、通信故障告警、设备告警等进行记录。

指标

设备故障监测:应能对设备故障进行监测。

7.1.1.5.2 网络

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、网络故障统计分析等指标;

当在网络运行中出现故障时,能够展现在当前网络拓扑图中产生报警告。

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:

应能够对网络中的安全设备进行安全标记,并能够根据安全标记对设备进行安全策略管理。

应包含设备属性:

- a) 安全标记应具有唯一性,能够准确反映设备在网络中的安全属性,并且具有防止篡改和删除的特性;

- b) 标记属性应包括安全级别、安全范围等信息,安全级别应能够进行高低判断,安全范围应可进行是否包含判断;

- c) 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;

应能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。

7.1.2.3 设备策略管理

7.1.2.3.1 安全配置策略

应能对设备策略进行配置和管理。

应能对设备策略进行配置和管理,包括设备策略、网络设备、安全设备的配置策略等。

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

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

记录准确完整。

7.1.3.2.3 审计数据采集方式

审计数据采集应至少满足以下要求:

- a) 通过被审计系统 Syslog 等方式采集;
- b) 通过统一接口采集被审计对象的审计

7.1.3.2.4 审计数据关联分析

审计数据关联分析应至少满足以下要求:

7.2 接口要求

7.2.1 第三方插件

第三方/代理接口协议要求

接口协议要求应满足以下要求:

接口协议应满足以下要求:

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) 采用加密技术保证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人员身份鉴别应满足以下要求:

安全管理中心控制台应支持多种鉴别方式,至少应支持用户名/密码鉴别或智能卡鉴别。

以上鉴别方式应同时使用,且应强制使用。

鉴别失败时,应记录鉴别失败原因,并应限制连续失败次数,超过限制次数后,应暂时锁定鉴别功能。

鉴别失败次数应可配置。

鉴别失败次数应至少为 5 次,且应至少为 1 次。鉴别失败次数应至少为 1 次,且应至少为 1 次。

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:

应满足以下要求:

应满足以下要求:

应满足以下要求:

应满足以下要求:

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) 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发生时间、时间、发起者信息、资源、描述和结果等；

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鉴别信息所有存储在解密过程中或分配给

其他管理员用户前都彻底清除，无论这些信息是存储在磁介质还是在内存中。

7.3.5 软件容错

安全管理中心控制台应提供软件容错产品以满足要求。

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) 对管理员登录地址进行限制；
- 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；

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) 能够检测和记录服务器、网络设备和安全设备行为异常行为，并在发生异常行为

- b) 应关闭不需要的各组件系统服务和端口；

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) 应制定数据备份和恢复计划，并定期执行；
- b) 应制定数据恢复计划，并定期执行；
- c) 应制定数据恢复计划，并定期执行；

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；

1) 能够记录系统内所有主体的身份信息，包括系统管理员、系统用户、系统设备、系统组件等，并能记录其身份信息的变化情况；

2) 能够对系统内所有主体的身份信息进行验证；

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：

1) 能够对系统内所有数据

进行分类，并根据分类结果对数据进行加密、解密、脱敏、删除等操作；

2) 能够对系统内所有数据的访问权限进行控制，防止数据泄露；

3) 能够对系统内所有数据

进行备份，并在备份过程中对数据进行加密、解密、脱敏、删除等操作；

4) 能够对系统内所有数据的完整性进行校验，防止数据篡改；

5) 能够对系统内所有数据

进行审计，并记录审计结果；

8.1.1.2.2 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及敏感信息、配置管理

完整性受损时采取必要的恢复措施；

- b) 能够检测到被管理对象及敏感信息、配置管理

完整性受损时采取必要的恢复措施；

1) 能够对系统内所有数据

- a) 对重要通信提供专用通信协议或安全通信协

议；

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：

1) 备份至少每天一次，备份介质异地存放；

- a) 提供数据备份与恢复功能，支持数据

备份与恢复，支持数据备份与恢复策略配置，支持数据备份与恢复策略执行；

b) 提供数据备份与恢复功能，支持数据

备份与恢复，支持数据备份与恢复策略配置，支持数据备份与恢复策略执行；

c) 提供数据备份与恢复功能，支持数据

备份与恢复，支持数据备份与恢复策略配置，支持数据备份与恢复策略执行；

d) 提供数据备份与恢复功能，支持数据

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;

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;

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;

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;

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) 能够担任工单管理的功能,支持工单管理流程,包括工单创建、工单分配、工单处理、工单关闭、工单评价等;
- b) 能够根据工单内容,自动推送相关的安全事件信息;

8.1.1.3.4 事件关联分析

事件关联分析应满足以下要求：

a) 支持事件关联分析功能，能够根据事件发生的时间、地点、类型等信息，自动关联相关事件，并生成事件关联图；

b) 支持事件关联分析功能，能够根据事件发生的时间、地点、类型等信息，自动关联相关事件，并生成事件关联图；

c) 支持事件关联分析功能，能够根据事件发生的时间、地点、类型等信息，自动关联相关事件，并生成事件关联图；

8.1.1.3.5 统计分析报表

统计分析报表应满足以下要求：

a) 支持统计分析报表功能，能够根据事件发生的时间、地点、类型等信息，自动生成统计分析报表；

b) 支持统计分析报表功能，能够根据事件发生的时间、地点、类型等信息，自动生成统计分析报表；

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：

a) 支持资产管理功能，能够对资产进行登记、分类、维护、查询等操作；

b) 支持资产管理功能，能够对资产进行登记、分类、维护、查询等操作；

c) 支持资产管理功能，能够对资产进行登记、分类、维护、查询等操作；

d) 支持资产管理功能，能够对资产进行登记、分类、维护、查询等操作；

e) 支持资产管理功能，能够对资产进行登记、分类、维护、查询等操作；

f) 支持资产管理功能，能够对资产进行登记、分类、维护、查询等操作；

8.1.1.4.2 资产业务价值评估

a) 支持资产业务价值评估功能，能够对资产进行价值评估，并生成评估报告；

b) 支持资产业务价值评估功能，能够对资产进行价值评估，并生成评估报告；

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；

b) 支持威胁管理功能，能够对威胁进行登记、分类、维护、查询等操作；

c) 支持威胁管理功能，能够对威胁进行登记、分类、维护、查询等操作；

8.1.1.4.4 脆弱性管理

脆弱性管理应满足以下要求：

a) 支持脆弱性管理功能，能够对脆弱性进行登记、分类、维护、查询等操作；

b) 支持脆弱性管理功能，能够对脆弱性进行登记、分类、维护、查询等操作；

c) 支持脆弱性管理功能，能够对脆弱性进行登记、分类、维护、查询等操作；

[illegible][illegible]

- [illegible]

-

 Springer

4. <http://www.fishbase.org>

用耕除田庄地以下重稅

- 用耕除田庄地以下重後

-

8.1.1.5.2 网络拓扑监测

网络拓扑监测应满足以下要求

- 网络拓扑监测应满足以下要求

兼下里田園市三品及

- 兼下里田園市三品及

Copyright © 2006 by John Wiley & Sons, Inc.

8.1.2.2 授权管理

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；

访问权限管理、网络访问权限管理、应用访问

访问权限管理、网络访问权限管理、应用访问

访问权限管理、网络访问权限管理、应用访问

理

8.1.2.3 设备策略管

策略

8.1.2.3.1 安全配置

以下要求：

设备管理应满足

以下要求：

以下要求：

8.1.2.3.2 入侵防御

入侵防御应满足以下要求：

入侵防御应满足以下要求：

入侵防御应满足以下要求：

入侵防御应满足以下要求：

入侵防御应满足以下要求：

入侵防御应满足以下要求：

入侵防御应满足以下要求：

入侵防御应满足以下要求：

8.1.2.3.3 恶意代码防范

恶意代码防范应满足以下要求：

恶意代码防范应满足以下要求：

恶意代码防范应满足以下要求：

恶意代码防范应满足以下要求：

8.1.2.4 密码保障

密码保障应满足以下要求：

密码保障应满足以下要求：

密码保障应满足以下要求：

密码保障应满足以下要求：

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：

审计策略集中管理应满足以下要求：

审计策略集中管理应满足以下要求：

审计策略集中管理应满足以下要求：

审计策略集中管理应满足以下要求：

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

图 1-3-2-1 统计数据库设计

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:

- ② 支持对主机设备(如服务器操作系统等)使用支撑终端(即终端)访问信息系统所使用的设备(如数据库采集设备)支持对数据库的实时数据采集。
- ③ 支持安全设备(如防火墙、入侵检测设备等)抗攻击系统、应急响应系统、审计系统、系统安全审计设备。

- 二) 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、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

4. 数据收集组件要求

信息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。

01225_ 审计数据关联分析

在滿足以下要求:

④ 应提供用户失败则自定义功能。

⑤ 在工业控制系统中,应能接收在远端主入口主站中从并联合站接收最小量,或接收规定的

求
方插件/代理接口协议要求

8.2 接口要求

8.2.1 第三方

议要求应满足以下要求:

接口协议

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)。

a) 安全

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) 接口间通信应使用安全协议,如 TLS、SSL 等。

机制相互验证对方的可信性,确保可信连接。

② 各接口之间进行通信时,应通过身份验证

8.3 自身安全要求

8.3.1 身份鉴别

足以下要求:

安全管理中心控制台的管理人员身份鉴别应满足

身份标识和鉴别,对同一管理员用户采用两种或两种

a) 提供专用的登录控制模块对管理员进行身

鉴别,其中至少有一种是采用构造的复杂且难以被技术来破

法在组合的鉴别技术来鉴别,且应满足

实现。

访问控制

8.3.2 访

安全管理中心控制台的访问控制应满足以下要求:

安全

① 应能对访问控制策略进行配置,并能对策略进行实时监控。

② 应能对访问控制策略进行配置,并能对策略进行实时监控。

③ 应能对访问控制策略进行配置,并能对策略进行实时监控。

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:

① 应能对可信路径进行配置,并能对可信路径进行实时监控。

安全管理中心控制台对管理员进行身份鉴别时,应能够记录一条安全的信息传输路径;

安全管理中心控制台应能够对安全信息传输路径进行实时监控;

安全管理中心控制台应能够对安全信息传输路径进行记录。

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:

应支持进行审计;

a) 应保证覆盖到每个管理员的安全审计功能;记录所有管理员的重要操作和安全

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) 审计而记录的事件至少应包括登录的日期、时间和发起紧急事件类型、描述和系

d) 提供按时间而记录数据进行统计、查询、分析及生成审计报告的功能。

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:

安全管理中心控制台应能够在发生故障时,能够自动恢复系统运行。

安全管理中心控制台应能够在发生故障时,能够自动恢复系统运行。

安全管理中心控制台应能够在发生故障时,能够自动恢复系统运行。

安全管理中心控制台应能够在发生故障时,能够自动恢复系统运行。

附录 A (规范性附录)
术语和缩略语

附录 B (规范性附录)
测试方法

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) 能够对最大并发会话连接数进行限制;

c) 能够对最大并发会话连接数进行限制;

d) 能够对单个管理员账户的多重并发会话进行限制;

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:

入侵事件时提供;

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政;并在发生严重

报警;

b) 能够通过设定终端接入方式或网络地址范围对通过网络进行管理的管理教

c) 能够通过设定终端接入方式或网络地址范围对通过网络进行管理的管理教

设备;能够通过设定终端接入方式或网络地址范围对通过网络进行管理的管理教

设备;能够通过设定终端接入方式或网络地址范围对通过网络进行管理的管理教

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:

安全管理中心控制台应能够在发生故障时,能够自动恢复系统运行。

及时采取必要的恢复措施。

数据完整性和保密性

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。

第五级

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：

- a) 能够实施统一的安全策略，能够对跨定级系统安全管理中心进行识别、鉴别、授权、审计、访问控制、资源保护等安全管理。
- b) 能够识别跨定级系统之间的数据流和交互行为，并能进行安全审计和日志记录。
- c) 能够识别跨定级系统之间的安全策略，并能进行安全策略的制定、发布、执行、审计和日志记录。

附录 A
(规范性附录)

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

见表 A.1。

安全管理中心与网络安全等级保护对象等级对应关系

表 A.1 安全管理中心与网络安全等级保护对象等级对应关系

表 A.1 安全管理中心与网络安全等级保护对象等级对应关系

级别	网络安全等级保护对象等级	安全管理中心等级
第二级	第二级	第二级
第三级	第三级	第三级
第四级	第四级	第四级
第五级	第五级	第五级

附录 B

(规范性附录)

主 编 王 人 等 理 由 人 社 科 学 出 版 社 分 编 主

[illegible]

表 B.1 (续)

自身		接口		第三方	
要求	6.2.1	7.2.1	8.2.1		
要求	6.2.2	7.2.2	8.2.2		
	6.3.1	7.3.1	8.3.1		
	6.3.2	7.3.2	8.3.2		
			8.3.3		
自身	6.3.4	7.3.4	8.3.4		
要求	6.3.5	7.3.5	8.3.5		
资源控制	6.3.6	7.3.6	8.3.6		
入侵防范	6.3.7	7.3.7	8.3.7		
数据安全	6.3.8	7.3.8	8.3.8		

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

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	设备类型
5	设备名称	设备名称
6	接收事件时间	接收事件时间
7	事件源信息	事件源信息
8	事件内容	事件内容
9	事件类型	事件类型
10	事件等级	事件等级
11	事件发生时间	事件发生时间
12	事件发生地点	事件发生地点
13	事件发生设备	事件发生设备
14	事件发生主机	事件发生主机
15	事件发生端口	事件发生端口
16	事件发生协议	事件发生协议
17	事件发生语言	事件发生语言
18	事件发生平台	事件发生平台
19	事件发生系统	事件发生系统
20	事件发生应用	事件发生应用
21	事件发生组件	事件发生组件
22	事件发生模块	事件发生模块
23	事件发生接口	事件发生接口
24	事件发生库	事件发生库
25	事件发生函数	事件发生函数
26	事件发生方法	事件发生方法
27	事件发生类	事件发生类
28	事件发生包	事件发生包
29	事件发生框架	事件发生框架
30	事件发生环境	事件发生环境
31	事件发生网络	事件发生网络
32	事件发生设备	事件发生设备
33	事件发生主机	事件发生主机
34	事件发生端口	事件发生端口
35	事件发生协议	事件发生协议
36	事件发生语言	事件发生语言
37	事件发生平台	事件发生平台
38	事件发生系统	事件发生系统
39	事件发生应用	事件发生应用
40	事件发生组件	事件发生组件
41	事件发生模块	事件发生模块
42	事件发生接口	事件发生接口
43	事件发生库	事件发生库
44	事件发生函数	事件发生函数
45	事件发生方法	事件发生方法
46	事件发生类	事件发生类
47	事件发生包	事件发生包
48	事件发生框架	事件发生框架
49	事件发生环境	事件发生环境
50	事件发生网络	事件发生网络
51	事件发生设备	事件发生设备
52	事件发生主机	事件发生主机
53	事件发生端口	事件发生端口
54	事件发生协议	事件发生协议
55	事件发生语言	事件发生语言
56	事件发生平台	事件发生平台
57	事件发生系统	事件发生系统
58	事件发生应用	事件发生应用
59	事件发生组件	事件发生组件
60	事件发生模块	事件发生模块
61	事件发生接口	事件发生接口
62	事件发生库	事件发生库
63	事件发生函数	事件发生函数
64	事件发生方法	事件发生方法
65	事件发生类	事件发生类
66	事件发生包	事件发生包
67	事件发生框架	事件发生框架
68	事件发生环境	事件发生环境
69	事件发生网络	事件发生网络
70	事件发生设备	事件发生设备
71	事件发生主机	事件发生主机
72	事件发生端口	事件发生端口
73	事件发生协议	事件发生协议
74	事件发生语言	事件发生语言
75	事件发生平台	事件发生平台
76	事件发生系统	事件发生系统
77	事件发生应用	事件发生应用
78	事件发生组件	事件发生组件
79	事件发生模块	事件发生模块
80	事件发生接口	事件发生接口
81	事件发生库	事件发生库
82	事件发生函数	事件发生函数
83	事件发生方法	事件发生方法
84	事件发生类	事件发生类
85	事件发生包	事件发生包
86	事件发生框架	事件发生框架
87	事件发生环境	事件发生环境
88	事件发生网络	事件发生网络
89	事件发生设备	事件发生设备
90	事件发生主机	事件发生主机
91	事件发生端口	事件发生端口
92	事件发生协议	事件发生协议
93	事件发生语言	事件发生语言
94	事件发生平台	事件发生平台
95	事件发生系统	事件发生系统
96	事件发生应用	事件发生应用
97	事件发生组件	事件发生组件
98	事件发生模块	事件发生模块
99	事件发生接口	事件发生接口
100	事件发生库	事件发生库

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

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11月第一版

*

书号: 155066 · 1-61703

版权专有 侵权必究



GB/T 36958-2018