

等级保护新标准2.0

条例解读

刘大伟

目录

Contents

1

等级保护发展历程与展望

2

等级保护2.0标准体系

3

等级保护2.0基本要求解析

4

等级保护2.0扩展要求解析



1 等级保护发展历程与展望

• 等级保护发展历程与展望

等保1.0时代

等保2.0工作

展望

1994-2003
政策环境营造

2004-2006
工作开展准备

2007-2010
工作正式启动

2010-2016
工作规模推进

- 1994年，国务院颁布《中华人民共和国计算机信息系统安全保护条例》，规定计算机信息系统实行安全等级保护。
- 2003年，中央办公厅、国务院办公厅颁发《国家信息化领导小组关于加强信息安全保障工作的意见》（中办发[2003]27号）明确指出“实行信息安全等级保护”。

- 2004-2006年，公安部联合四部委开展涉及65117家单位，共115319个信息系统的等级保护基础调查和等级保护试点工作，为全面开展等级保护工作奠定基础。

- 2007年6月，四部门联合出台《信息安全等级保护管理办法》。
- 2007年7月，四部门联合颁布《关于开展全国重要信息系统安全等级保护定级工作的通知》。
- 2007年7月20日，召开全国重要信息系统安全等级保护定级工作部署专题电视电话会议，标志着信息安全等级保护制度正式开始实施。

- 2010年4月，公安部出台《关于推动信息安全等级保护测评体系建设和开展等级测评工作的通知》，提出等级保护工作的阶段性目标。
- 2010年12月，公安部和国务院国有资产监督管理委员会联合出台《关于进一步推进中央企业信息安全等级保护工作的通知》，要求中央企业贯彻执行等级保护工作。

• 等级保护发展历程与展望

等保1.0时代

等保2.0工作

展望



- 2016年10月10日，第五届全国信息安全等级保护技术大召开，公安部网络安全保卫局郭启全总工指出“**国家对网络安全等级保护制度提出了新的要求，等级保护制度已进入2.0时代**”。
- 2016年11月7日，《中华人民共和国网络安全法》正式颁布，第二十一条明确“**国家实行网络安全等级保护制度……**”。

- 以《GB17859 计算机信息系统安全保护等级划分准则》、《GB/T22239-2008 信息安全技术 信息系统安全等级保护基本要求》为代表的等级保护系列配套标准，习惯称为**等保1.0标准**。
- 2013年，全国信息安全标准化技术委员会授权**WG5-信息安全评估工作组**开始启动等级保护新标准的研究。
- 2017年1月至2月，**全国信息安全标准化技术委员会**发布《网络安全等级保护基本要求》系列标准、《网络安全等级保护测评要求》系列标准等“征求意见稿”。
- 2017年5月，**国家公安部发布**《GA/T 1389—2017 网络安全等级保护定级指南》、《GA/T 1390.2—2017 网络安全等级保护基本要求 第2部分：云计算安全扩展要求》等4个公共安全行业等级保护标准。

● 等级保护发展历程与展望

等保1.0时代

等保2.0工作

展望

等级保护2.0时代，将根据信息技术发展应用和网络安全态势，不断丰富制度内涵、拓展保护范围、完善监管措施，逐步健全网络安全等级保护制度政策、标准和支撑体系。

□ 等级保护上升为法律

《中华人民共和国网络安全法》第21条规定“国家实行网络安全等级保护制度”，要求“网络运营者应当按照网络安全等级保护制度要求，履行安全保护义务”；第31条规定“对于国家关键信息基础设施，在网络安全等级保护制度的基础上，实行重点保护”。

□ 等级保护工作内容将持续扩展

在定级、备案、建设整改、等级测评和监督检查等规定动作基础上，2.0时代风险评估、安全监测、通报预警、案事件调查、数据防护、灾难备份、应急处置、自主可控、供应链安全、效果评价、综治考核等这些与网络安全密切相关的措施都将全部纳入等级保护制度并加以实施。

□ 等级保护对象将不断拓展

随着云计算、移动互联、大数据、物联网、人工智能等新技术不断涌现，计算机信息系统的概念已经不能涵盖全部，特别是互联网快速发展带来大数据价值的凸显，等保保护对象的外延将不断拓展。

□ 等级保护体系将进行重大升级

2.0时代，主管部门将继续制定出台一系列政策法规和技术标准，形成运转顺畅的工作机制，在现有体系基础上，建立完善等级保护政策体系、标准体系、测评体系、技术体系、服务体系、关键技术研究体系、教育训练体系等。



2 等级保护2.0标准体系

• 等级保护2.0标准体系

等保1.0

等保2.0

GB 17859-1999 《计算机信息系统安全保护等级划分准则》

《信息系统安全等级保护定级指南》

《信息系统安全等级保护基本要求》

《信息系统安全等级保护实施指南》

《信息系统等级保护安全技术要求》

《信息系统安全等级保护测评要求》

《信息系统安全等级保护测评过程指南》

• 等级保护2.0标准体系

等保1.0

等保2.0

GB 17859-1999 《计算机信息系统安全保护等级划分准则》

- 正式更名为网络安全等级保护标准;
- 横向扩展了对云计算、移动互联网、工业控制系统的安全要求;
- 纵向扩展了对等保测评机构的规范管理。

(注: 基于2017年等级保护标准系列征求意见稿)

《信息系统安全等级保护定级指南》

《网络安全等级保护基本要求》

第一部分: 安全通用要求

第二部分: 云计算安全扩展要求

第三部分: 移动互联网安全扩展要求

第四部分: 物联网安全扩展要求

第五部分: 工业控制系统安全扩展要求

《网络安全等级保护实施指南》

《网络安全等级保护安全技术要求》

第一部分: 安全通用要求

第二部分: 云计算安全扩展要求

第三部分: 移动互联网安全扩展要求

第四部分: 物联网安全扩展要求

第五部分: 工业控制系统安全扩展要求

《网络安全等级保护测评要求》

第一部分: 安全通用要求

第二部分: 云计算安全扩展要求

第三部分: 移动互联网安全扩展要求

第四部分: 物联网安全扩展要求

第五部分: 工业控制系统安全扩展要求

《网络安全等级保护测评过程指南》

《网络安全等级保护测试评估技术指南》

《网络安全等级保护安全管理中心技术要求》

《网络安全等级保护测评机构能力要求和评估规范》

未变化
修订内容
新增

• 等级保护2.0标准体系

主要标准

内容解析

GB 17859-1999 《计算机信息系统安全保护等级划分准则》

《信息系统安全等级保护定级指南》

《网络安全等级保护基本要求》

第一部分：安全通用要求

第二部分：云计算安全扩展要求

第三部分：移动互联网安全扩展要求

第四部分：物联网安全扩展要求

第五部分：工业控制系统安全扩展要求

《网络安全等级保护实施指南》

《网络安全等级保护安全技术要求》

第一部分：安全通用要求

第二部分：云计算安全扩展要求

第三部分：移动互联网安全扩展要求

第四部分：物联网安全扩展要求

第五部分：工业控制系统安全扩展要求

《网络安全等级保护测评要求》

第一部分：安全通用要求

第二部分：云计算安全扩展要求

第三部分：移动互联网安全扩展要求

第四部分：物联网安全扩展要求

第五部分：工业控制系统安全扩展要求

《网络安全等级保护测评过程指南》

《网络安全等级保护测试评估技术指南》

《网络安全等级保护安全管理中心技术要求》

《网络安全等级测评机构能力要求和评估规范》

● 等级保护2.0标准体系

主要标准

内容解析

□ 公安部已于2017年5月率先发布《网络安全等级保护定级指南》、《网络安全等级保护基本要求 第5部分：工业控制系统安全扩展要求》等4个行业标准。

□ GA/T 1389—2017《信息安全技术 网络安全等级保护定级指南》

在国标《信息安全等级保护定级指南》的基础上细化优化了对客体侵害事项、侵害程度的定义，确定了对基础信息网络、工业控制系统、云计算平台、物联网、采用移动互联技术的信息系统、大数据等对象的定级原则，进一步明确了定级过程中专家审查、主管部门审核、公安机关备案审查等节点的管理要求。

□ GA/T 1390.2—2017《信息安全技术 网络安全等级保护基本要求 第2部分：云计算安全扩展要求》

针对云计算架构的特点，对云计算环境下的物理位置、虚拟化网络、虚拟机、云服务方、云租户、虚拟镜像等技术保护要求，以及云服务商选择、SLA协议、云安全审计等安全管理要求进行了规定。

□ GA/T 1390.3—2017《信息安全技术 网络安全等级保护基本要求 第3部分：移动互联安全扩展要求》

针对移动互联网系统中移动终端、移动应用和无线网络等三个关键要素，明确了无线接入设备的安装选择、无线接入网关处理能力、非授权移动终端接入等技术保护要求，以及应用软件分发运营商选择、移动终端应用软件恶意代码防范等管理要求进行了规定。

□ GA/T 1390.5—2017《信息安全技术 网络安全等级保护基本要求 第5部分：工业控制系统安全扩展要求》

分析了工业控制系统的层次模型、区域模型，提出了工业控制系统安全域划分和保护的主要原则。并从物理提示标志、网络非必要通信控制、系统时间戳等技术方面，以及工控系统管理员/工控网络管理员/工控安全管理员岗位设置、工控设备的版本号漏洞控制等管理方面进行了规定。

• 等级保护2.0标准定级要求

定级要求

新增定级流程

定级对象

① 定级要求

- 重新对部分内容的顺序作了调整，从整体显得更加的合理。
- 增加了新的内容和流程，例如扩展了定级的对象，包括基础信息网络、工业控制系统、云计算平台、物联网、其他信息系统、大数据等；新增加的流程为“定级工作一般流程”，并对旧版本“定级一般流程”更名为“定级方法流程”。

1.0 要求

第三级，信息系统受到破坏后，会对社会秩序和公共利益造成严重损害，或者对国家安全造成损害。

定级一般流程；

2.0 要求

第三级，等级保护对象受到破坏后，会对公民、法人和其他组织的合法权益产生特别严重损害，或者对社会秩序和公共利益造成严重损害，或者对国家安全造成损害；

更名为“定级方法流程”。

新增“定级工作一般流程”。

等级保护2.0标准定级要求

定级要求

新增定级流程

定级对象

原标准

受侵害的客体	对客体的侵害程度		
	一般损害	严重损害	特别严重损害
公民、法人和其他组织的合法权益	第一级	第二级	第二级
社会秩序、公共利益	第二级	第三级	第四级
国家安全	第三级	第四级	第五级

新标准

受侵害的客体	对客体的侵害程度		
	一般损害	严重损害	特别严重损害
公民、法人和其他组织的合法权益	第一级	第二级	第三级
社会秩序、公共利益	第二级	第三级	第四级
国家安全	第三级	第四级	第五级

注：基于GA/T 1389—2017《网络安全等级保护定级指南》及GB/T 22240—2008《信息系统安全等级保护定级指南》内容对比分析。

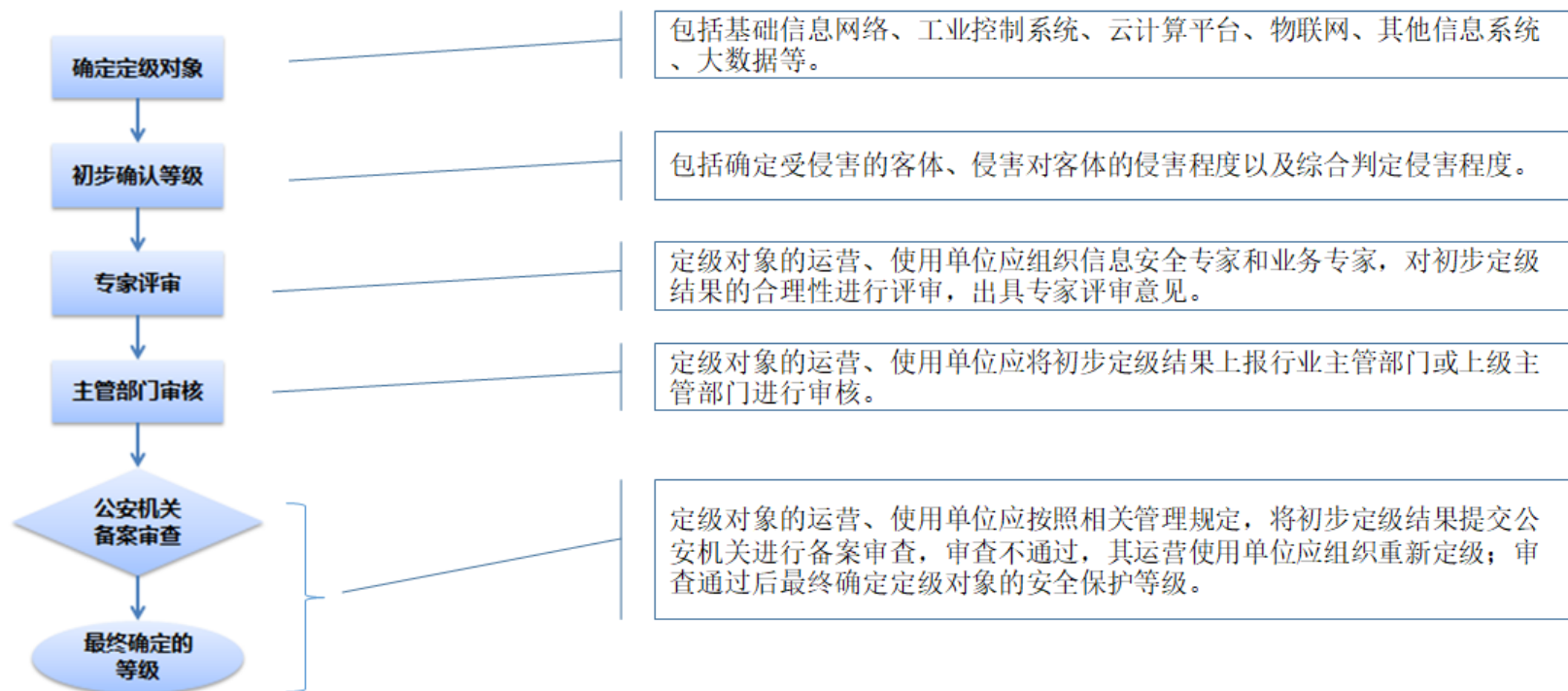
● 等级保护2.0标准定级要求

定级要求

新增定级流程

定级对象

② 新增“定级流程”



注：基于GA/T 1389—2017《网络安全等级保护定级指南》及GB/T 22240—2008《信息系统安全等级保护定级指南》内容对比分析。

等级保护2.0标准定级要求

定级要求

新增定级流程

定级对象

③ 定级对象

- 重新对定级对象进行调整，并进行相应的介绍。
2.0定级对象分为基础信息网络、信息系统和其他信息系统，其中信息系统再细分为工业控制系统、物联网、大数据、移动互联以及云计算平台。

1.0
要求

信息系统

一个单位内运行的信息系统可能比较庞大，为了体现重要部分重点保护，有效控制信息安全建设成本，优化信息安全资源配置的等级保护原则，可将较大的信息系统划分为若干个较小的、可能具有不同安全保护等级的定级对象。

2.0
要求

工业控制系统

工业控制系统主要由生产管理层、现场设备层、现场控制层和过程监控层构成，其中：生产管理层的定级对象确定原则见(其他信息系统)。设备层、现场控制层和过程监控层应作为一个整体对象定级，各层次要素不单独定级。

对于大型工业控制系统，可以根据系统功能、控制对象和生产厂商等因素划分为多个定级对象。

物联网

物联网应作为一个整体对象定级，主要包括感知层、网络传输层和处理应用层等要素。

采用移动互联技术的信息系统

采用移动互联技术的等级保护对象应作为一个整体对象定级，主要包括移动终端、移动应用、无线网络以及相关应用系统等。

大数据

应将具有统一安全责任单位的大数据作为一个整体对象定级，或将其与责任主体相同的相关支撑平台统一定级。

云计算平台

在云计算环境中，应将云服务方侧的云计算平台单独作为定级对象定级，云租户侧的等级保护对象也应作为单独的定级对象定级。
对于大型云计算平台，应将云计算基础设施和有关辅助服务系统划分为不同的定级对象。

基础信息网络

对于电信网、广播电视传输网、互联网等基础信息网络，应分别依据服务类型、服务地域和安全责任主体等因素将其划分为不同的定级对象。
跨省全国性业务专网可作为一个整体对象定级，也可以分区域划分为若干个定级对象。

其他信息系统

作为定级对象的其他信息系统应具有如下基本特征：

- a) **具有确定的主要安全责任单位。**作为定级对象的信息系统应能够明确其主要安全责任单位；
- b) **承载相对独立的业务应用。**作为定级对象的信息系统应承载相对独立的业务应用，完成不同业务目标或者支撑不同单位或不同部门职能的多个信息系统应划分为不同的定级对象；
- c) **具有信息系统的基本要素。**作为定级对象的信息系统应该是由相关的和配套的设备、设施按照一定的应用目标和规则组合而成的多资源集合，单一设备（如服务器、终端、网络设备等）不单独定级。

注：基于GA/T 1389—2017《网络安全等级保护定级指南》及GB/T 22240—2008《信息系统安全等级保护定级指南》内容对比分析。



3 等级保护2.0基本要求解析

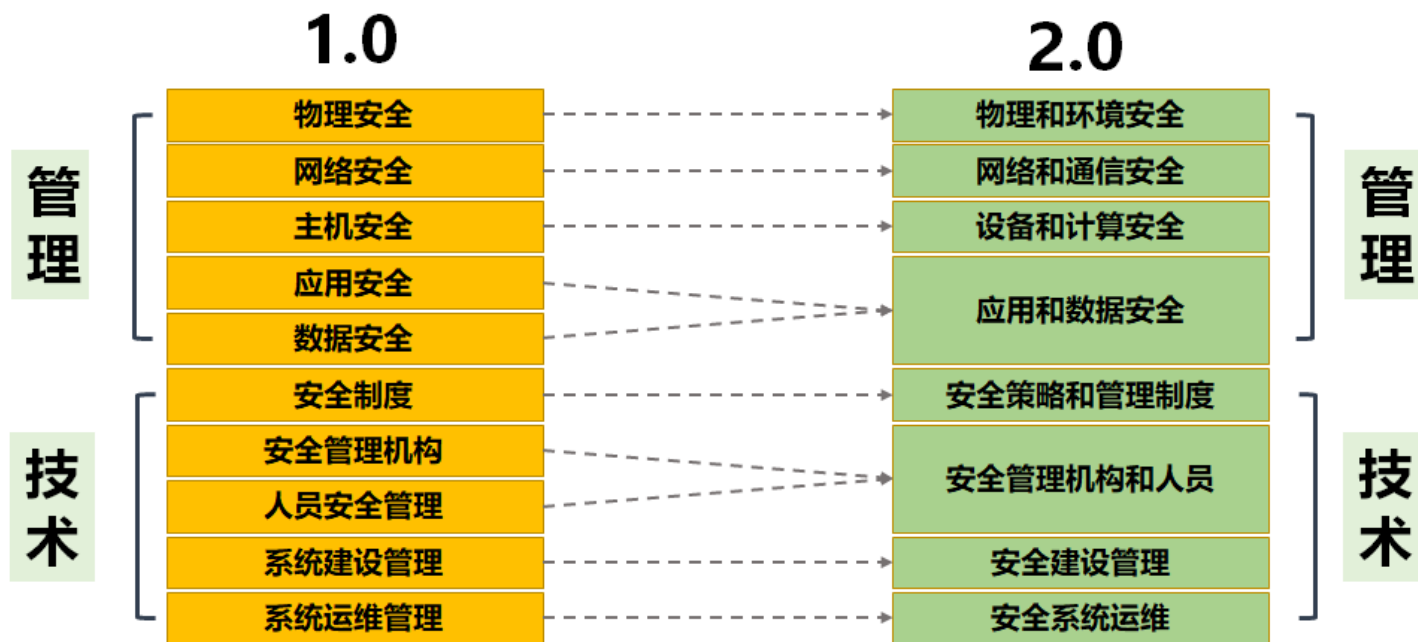
• 等级保护2.0基本要求解析

整体变化

技术

管理

□ 安全控制域划分上有较大变化，原有十个安全域整合为八个，定义上更精确，内涵更为丰富。



注：基于《网络安全保护基本要求 第一部分：通用安全要求》征求意见稿及GB/T 22239《信息安全等级保护基本要求》三级要求对比分析。

等级保护2.0基本要求解析

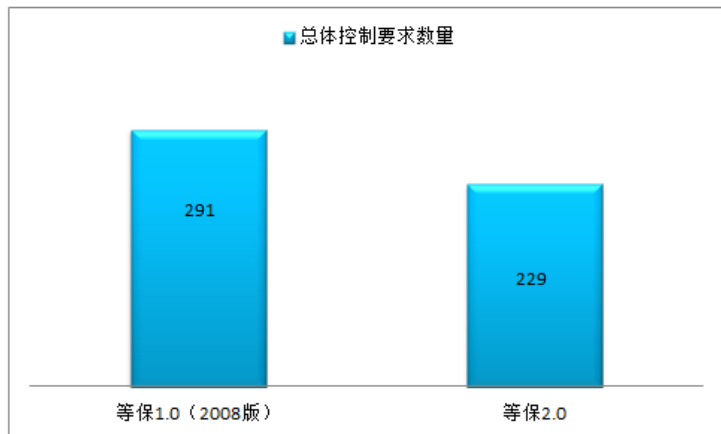
整体变化

技术

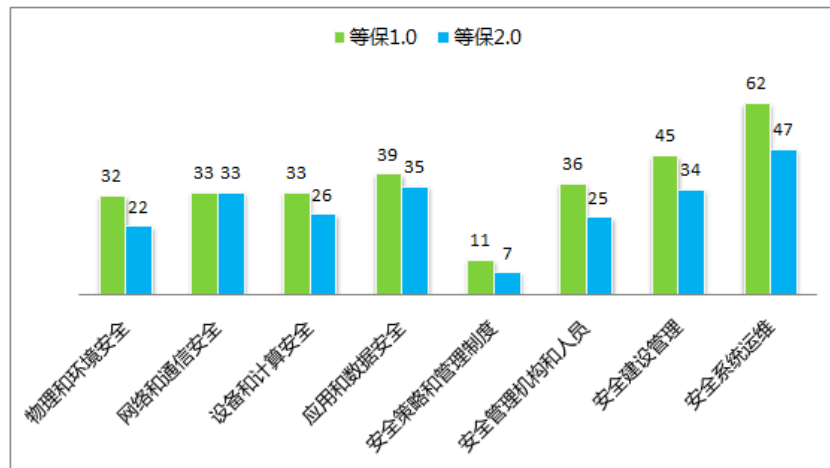
管理

□ 安全控制要求的部分条款被合并，部分条款被删除，同时也有部分新增要求，整体数量有较大降低。

总体安全要求数量对比
(以三级系统为例)



各控制域安全要求数量对比
(以三级系统为例)



注：基于《网络安全保护基本要求 第一部分：通用安全要求》征求意见稿及GB/T 22239《信息安全等级保护基本要求》三级要求对比分析。

等级保护2.0基本要求解析

整体变化

技术

管理

- 整体内容上，对过于细节内容进行精炼或合并，对部分要求进行了删减，同时也新增了部分要求。
- 在操作落实方面更灵活，同时与1.0相比整体安全要求有所降低。

例：整合的内容

网络安全——身份鉴别

- a) 应提供专用的登录控制模块对登录用户进行身份标识和鉴别；
- c) 应提供用户身份标识唯一和鉴别信息复杂度检查功能，保证应用系统中不存在重复用户身份标识，身份鉴别信息不易被冒用；

网络与通信安全——身份鉴别

- a) 应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，鉴别信息具有复杂度要求并定期更换；

例：删减的内容

安全管理机构——人员配备

- c) 关键事务岗位应配备多人共同管理。

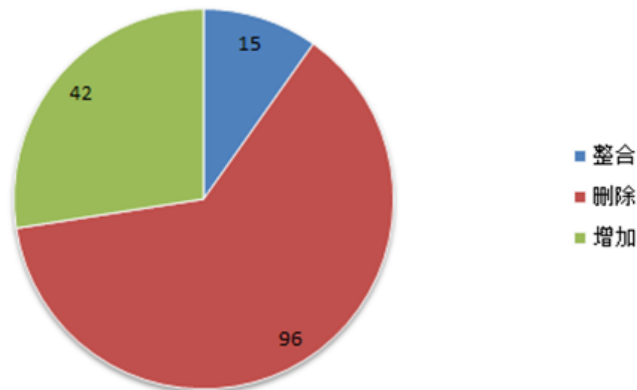
例：增加的内容

网络和通信安全——边界完整性检查

- d) 应限制无线网络的使用，确保无线网络通过受控的边界防护设备接入内部网络。

设备和计算安全——安全审计

- e) 审计记录产生时的时间应由系统范围内唯一确定的时钟产生，以确保审计分析的正确性。



注：基于《网络安全保护基本要求 第一部分：通用安全要求》征求意见稿及GB/T 22239《信息安全等级保护基本要求》三级要求对比分析。

等级保护2.0基本要求解析

整体变化

技术

管理

① 物理和环境安全——实质性变更

- 降低物理位置选择要求，机房可设置在建筑楼顶或地下室，但需要加强相应防水防潮措施。
- 降低了物理访问控制要求，不再要求人员值守出入口，不再要求机房内部分区，不再对机房人员出入进行具体要求。
- 降低了电力供应的要求，不再要求必须配备后备发电机。
- 降低了电磁防护的要求，不再要求必须接地。
- 降低了防盗和防破坏要求，可部署防盗系统或视频监控系统

1.0 要求

- b) 机房场地应避免设在建筑物的高层或地下室，以及用水设备的下层或隔壁。
- a) 机房出入口应安排专人值守，控制、鉴别和记录进入的人员；—
- b) 需进入机房的来访人员应经过申请和审批流程，并限制和监控其活动范围；—
- c) 应对机房划分区域进行管理，区域和区域之间设置物理隔离装置，在重要区域前设置交付或安装等过渡区域；—
- d) 重要区域应配置电子门禁系统，控制、鉴别和记录进入的人员。
- e) 应建立备用供电系统。—
- a) 应采用接地方式防止外界电磁干扰和设备寄生耦合干扰；—
- f) 应利用光、电等技术设置机房防盗报警系统；—
- g) 应对机房设置监控报警系统。—

2.0 要求

- b) 机房场地应避免设在建筑物的顶层或地下室，否则应加强防水和防潮措施。
- 机房出入口应 配置电子门禁系统，控制、鉴别和记录进入的人员。
- c) 应设置机房防盗报警系统或设置有专人值守的视频监控系统。

注：基于《网络安全保护基本要求 第一部分：通用安全要求》征求意见稿及GB/T 22239《信息安全等级保护基本要求》三级要求对比分析。

• 等级保护2.0基本要求解析

整体变化

技术

管理

② 网络和通讯安全——实质性变更1

- 强化了对设备和通信链路的硬件冗余要求。
- 强化了网络访问策略的控制要求，包括默认拒绝策略、控制规则最小化策略和源目的的检查要求。
- 降低了带宽控制的要求，不再要求必须进行QOS控制。
- 降低了安全访问路径、网络会话控制、地址欺骗防范、拨号访问权限限制等比较“古老”的控制要求。

1.0 要求

e) 应在业务终端与业务服务器之间进行路由控制建立安全的访问路径；—

g) 应按照对业务服务的重要次序来指定带宽分配优先级别，保证在网络发生拥堵的时候优先保护重要主机。—

d) 应在会话处于非活跃一定时间或会话结束后终止网络连接；—

e) 应限制网络最大流量数及网络连接数；—

f) 重要网段应采取技术手段防止地址欺骗；—

g) 应按用户和系统之间的允许访问规则，决定允许或拒绝用户对受控系统进行资源访问，控制粒度为单个用户；—

h) 应限制具有拨号访问权限的用户数量。—

2.0 要求

e) 应提供通信线路、关键网络设备的硬件冗余，保证系统可用性

a) 应在网络边界或区域之间根据访问控制策略设置访问控制规则，默认情况下除允许通信外受控接口**拒绝所有通信**；

b) 应删除多余或无效的访问控制规则，优化访问控制列表，并保证访问控制规则数量最小化；

c) 应对源地址、目的地址、源端口、目的端口和协议等进行检查，以允许/拒绝数据包进出；

注：基于《网络安全保护基本要求 第一部分：通用安全要求》征求意见稿及GB/T 22239《信息安全等级保护基本要求》三级要求对比分析。

• 等级保护2.0基本要求解析

整体变化

技术

管理

② 网络和通讯安全——实质性变更2

- 强化了安全审计的统一时钟源要求。
- 强化了对网络行为审计的要求。
- 强化了网络边界的安全控制，特别是无线网络与有线网络的边界控制。
- 强化了对网络攻击特别是“未知攻击”的检测分析要求。
- 强化了对恶意代码和垃圾邮件的防范要求，强调在“关键网络节点”。
- 降低了对审计分析的要求，不再要求必须生成审计报表。

1.0
要求

e) 应能够根据记录数据进行分析，并生成审计报表；

- a) 应在网络边界处对恶意代码进行检测和清除；
- b) 应维护恶意代码库的升级和检测系统的更新。

2.0
要求

d) 审计记录产生时的时间应由系统范围内唯一确定的时钟产生，以确保审计分析的正确性；

e) 应能对远程访问的用户行为、访问互联网的用户行为等单独进行行为审计和数据分析。

a) 应保证跨越边界的访问和数据流通过边界防护设备提供的受控接口进行通信；

d) 应限制无线网络的使用，确保无线网络通过受控的边界防护设备接入内部网络。

c) 应采取技术措施对网络行为进行分析，实现对网络攻击特别是**未知的新型网络攻击**的检测和分析；

b) 应在关键网络节点处对垃圾邮件进行检测和防护，并维护垃圾邮件防护机制的升级和更新。

a) 应在关键网络节点处对恶意代码进行检测和清除，并维护恶意代码防护机制的升级和更新；

注：基于《网络安全保护基本要求 第一部分：通用安全要求》征求意见稿及GB/T 22239《信息安全等级保护基本要求》三级要求对比分析。

• 等级保护2.0基本要求解析

整体变化

技术

管理

② 网络和通讯安全——实质性变更3

□ 特别增加了安全集中管控的要求，建设集中安全管理系统成为必要。

□ 将原有属于网络设备防护的内容移到了“设备和计算安全”部分。

1.0 要求

- a) 应对登录网络设备的用户进行身份鉴别；
- b) 应对网络设备的管理员登录地址进行限制；
- c) 网络设备用户的标识应唯一；
- d) 主要网络设备应对同一用户选择两种或两种以上组合的鉴别技术来进行身份鉴别；
- e) 身份鉴别信息应具有不易被冒用的特点，口令应有复杂度要求并定期更换；
- f) 应具有登录失败处理功能，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；
- g) 当对网络设备进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听；
- h) 应实现设备特权用户的权限分离。

2.0 要求

- a) 应划分出特定的管理区域，对分布在网络中的安全设备或安全组件进行管控；
- b) 应能够建立一条安全的信息传输路径，对网络中的安全设备或安全组件进行管理；
- c) 应对网络链路、安全设备、网络设备和服务器等的运行状况进行集中监测；
- d) 应对分散在各个设备上的审计数据进行收集汇总和集中分析；
- e) 应对安全策略、恶意代码、补丁升级等安全相关事项进行集中管理；
- f) 应能对网络中发生的各类安全事件进行识别、报警和分析。

注：基于《网络安全保护基本要求 第一部分：通用安全要求》征求意见稿及GB/T 22239《信息安全等级保护基本要求》三级要求对比分析。

• 等级保护2.0基本要求解析

整体变化

技术

管理

③ 设备和计算安全——实质性变更1

- 强化了访问控制的要求，细化了主体和客体的访问控制粒度要求。
- 强化了安全审计的统一时钟源要求。
- 强化了入侵防范的控制要求，包括终端的准入要求、漏洞测试与修复。
- 降低了对审计分析的要求，不再要求必须生成审计报表。
- 降低了对恶意代码防范的统一管理要求和强制性的代码库异构要求。
- 提出了采用**可信计算技术**防范恶意代码的控制要求。

1.0
要求

- d) 应能够根据记录数据进行分析，并生成审计报表；—
- b) 主机防恶意代码产品应具有与网络防恶意代码产品不同的恶意代码库；—
- e) 应支持防恶意代码的统一管理。—

2.0
要求

- f) 访问控制的粒度应达到主体为用户级或进程级，客体为文件、数据库表级；
- e) 审计记录产生时的时间应由系统范围内唯一确定的时钟产生，以确保审计分析的正确性。
- c) 应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终端进行限制；
- d) 应能发现可能存在的漏洞，并在经过充分测试评估后，及时修补漏洞；
- a) 应采用免受恶意代码攻击的技术措施或采用可信计算技术建立从系统到应用的信任链，实现系统运行过程中重要程序或文件完整性检测，并在检测到破坏后进行恢复。

注：基于《网络安全保护基本要求 第一部分：通用安全要求》征求意见稿及GB/T 22239《信息安全等级保护基本要求》三级要求对比分析。

• 等级保护2.0基本要求解析

整体变化

技术

管理

③ 设备和计算安全——实质性变更2

□ 强化了将网络设备本身安全看作整体设备和计算安全的一部分，突出了“重要节点”的概念。

1.0
要求

c) 应对重要服务器进行监视，包括监视服务器的CPU、硬盘、内存、网络等资源的使用情况；

e) 应能够对系统的服务水平降低到预先规定的最小值进行检测和报警。

2.0
要求

b) 应提供重要节点设备的硬件冗余，保证系统的可用性；

c) 应对重要节点进行监视，包括监视CPU、硬盘、内存等资源的使用情况；

d) 应能够对重要节点的服务水平降低到预先规定的最小值进行检测和报警。

注：基于《网络安全保护基本要求 第一部分：通用安全要求》征求意见稿及GB/T 22239《信息安全等级保护基本要求》三级要求对比分析。

• 等级保护2.0基本要求解析

整体变化

技术

管理

④ 应用和数据安全——实质性变更

□ 特别增加了个人信息保护的要求。

- 强化了对软件容错的要求，保障故障发生时的可用性。
- 强化了对账号和口令的安全要求，包括更改初始口令、账号口令重命名、对多余/过期/共享账号的控制。
- 强化了安全审计的统一时钟源要求。
- 降低了对资源控制的要求，包括会话连接数限制、资源监测、资源分配控制。
- 降低了对审计分析的要求，不再要求必须生成审计报表。

1.0 要求

d) 应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。

d) 应能够对一个时间段内可能的并发会话连接数进行限制；
f) 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；
g) 应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帐户或请求进程的优先级，根据优先级分配系统资源。

2.0 要求

a) 应仅采集和保存业务必需的用户个人信息；
b) 应禁止未授权访问和使用用户个人信息。

b) 在故障发生时，应能够继续提供一部分功能，确保能够实施必要的措施；

c) 应强制用户首次登录时修改初始口令；

b) 应重命名默认账号或修改这些账号的默认口令；

c) 应及时删除或停用多余的、过期的账号，避免共享账号的存在；

e) 审计记录产生时的时间应由系统范围内唯一确定的时钟产生，以确保审计分析的正确性。

注：基于《网络安全保护基本要求 第一部分：通用安全要求》征求意见稿及GB/T 22239《信息安全等级保护基本要求》三级要求对比分析。

• 等级保护2.0基本要求解析

整体变化

技术

管理

① 安全策略和管理制度——实质性变更

□ 降低了对安全管理制度的管理要求，包括版本控制、收发文管理等，其中不再要求必须由信息安全领导小组组织制度的审定。

1.0
要求

b) 安全管理制度应具有统一的格式，并进行版本控制；
c) 应组织相关人员对制定的安全管理制度进行论证和审定；
e) 安全管理制度应注明发布范围，并对收发文进行登记。

a) 信息安全领导小组应负责定期组织相关部门和相关人员对安全管理制度体系的合理性和适用性进行审定；

2.0
要求

无

注：基于《网络安全保护基本要求 第一部分：通用安全要求》征求意见稿及GB/T 22239《信息安全等级保护基本要求》三级要求对比分析。

• 等级保护2.0基本要求解析

整体变化

技术

管理

② 安全管理机构和人员——实质性变更

- 对安全管理和机构人员的要求整体有所降低，一方面对过细的操作层面要求进行删减，例如记录和文档的操作要求、制度的制定要求等，另一方面对岗位配备、人员技能考核等要求也有实质性的删减。
- 强化了对**外部人员**的管理要求，包括外部人员的访问权限、保密协议的管理要求。

1.0 要求

d) 应制定文件明确安全管理机构各个部门和岗位的职责、分工和技能要求。

e) 关键事务岗位应配备多人共同管理。

d) 应记录审批过程并保存审批文档。

e) 应聘请信息安全专家作为常年的安全顾问，指导信息安全建设，参与安全规划和安全评审等。

d) 应制定安全审核和安全检查制度规范安全审核和安全检查工作，定期按照程序进行安全审核和安全检查活动。

a) 应定期对各个岗位的人员进行安全技能及安全认知的考核；
b) 应对关键岗位的人员进行全面、严格的安全审查和技能考核；
应对考核结果进行记录并保存；

b) 应对安全责任和惩戒措施进行书面规定并告知相关人员，对违反违背安全策略和规定的人员进行惩戒；

c) 应对定期安全教育和培训进行书面规定；

d) 应对安全教育和培训的情况和结果进行记录并归档保存。

2.0 要求

b) 应确保在外部人员接入网络访问系统前先提出书面申请，批准后由专人开设账号、分配权限，并登记备案；

c) 外部人员离场后应及时清除其所有的访问权限；

d) 获得系统访问授权的外部人员应签署保密协议，不得进行非授权操作，不得复制和泄露任何敏感信息。

注：基于《网络安全保护基本要求 第一部分：通用安全要求》征求意见稿及GB/T 22239《信息安全等级保护基本要求》三级要求对比分析。

● 等级保护2.0基本要求解析

整体变化

技术

管理

③ 安全建设管理——实质性变更1

- 对安全建设管理的要求整体有所降低，一方面对过细的操作层面要求进行删减，例如不再要求由专门部门或人员实施某些管理活动、不再对某些管理制度的制定作细化要求；另一方面对安全规划管理、测试验收管理也有实质性的删减。

1.0 要求

a) 应指定专门的部门或人员负责管理系统定级的相关材料，并控制这些材料的使用；—

b) 应指定和授权专门的部门对信息系统的安全建设进行总体规划，制定近期和远期的安全建设工作计划；—

e) 应根据等级测评、安全评估的结果定期调整和修订总体安全策略、安全技术框架、安全管理策略、总体建设规划、详细设计方案等相关配套文件。—

e) 应指定或授权专门的部门负责产品的采购；—

d) 应指定或授权专门的部门或人员负责等级测评的管理。—

e) 应确保选定的安全服务商提供技术培训和承诺，必要的与其签订服务合同。—

e) 应制定工程实施方面的管理制度，明确说明实施过程的控制方法和人员行为准则。—

a) 应委托公正的第三方测试单位对系统进行安全性测试，并出具安全性测试报告；—

e) 应对系统测试验收的控制方法和人员行为准则进行书面规定；—

d) 应指定或授权专门的部门负责系统测试验收的管理，并按照管理规定的要求完成系统测试验收工作；—

e) 应组织相关部门和相关人员对系统测试验收报告进行审定，并签字确认。—

d) 应对系统交付的控制方法和人员行为准则进行书面规定；—

e) 应指定或授权专门的部门负责系统交付的管理工作，并按照管理规定的要求完成系统交付工作。—

注：基于《网络安全保护基本要求 第一部分：通用安全要求》征求意见稿及GB/T 22239《信息安全等级保护基本要求》三级要求对比分析。

• 等级保护2.0基本要求解析

整体变化

技术

管理

③ 安全建设管理——实质性变更2

- 强化了对**服务供应商**管理、系统上线安全测试、工程监理控制的管理要求。
- 强化了对**自行软件开发**的要求，包括安全性测试、恶意代码检测、软件开发活动的管理要求。

无

1.0
要求

2.0
要求

c) 应通过第三方工程监理控制项目的实施过程。

c) 应定期监视、评审和审核服务供应商提供的服务，并对其变更服务内容加以控制。

e) 应确保在软件开发过程中对安全性进行测试，在软件安装前对可能存在的恶意代码进行检测；

g) 应确保开发人员为专职人员，开发人员的开发活动受到控制、监视和审查

b) 应进行上线前的安全性测试，并出具安全测试报告。

注：基于《网络安全保护基本要求 第一部分：通用安全要求》征求意见稿及GB/T 22239《信息安全等级保护基本要求》三级要求对比分析。

• 等级保护2.0基本要求解析

整体变化

技术

管理

④ 安全运维管理——实质性变更1

- 对安全运维管理的要求整体有所降低，一方面对过细的操作层面要求进行删减，例如不再要求由专门部门或人员实施某些管理活动、不再对某些管理制度的制定作细化要求；另一方面对介质管理、设备管理也有实质性的删减。

1.0 要求

b) 应建立资产安全管理制度，规定信息系统资产管理的人员或责任部门，并规范资产管理和使用的行为；

a) 应建立介质安全管理制度，对介质的存放环境、使用、维护和销毁等方面作出规定；

e) 应根据数据备份的需要对某些介质实行异地存储，存储地的环境要求和管理方法应与本地相同；

f) 应对重要介质中的数据和软件采取加密存储，并根据所承载数据和软件的重要程度对介质进行分类和标识管理。

d) 应对存储介质的使用过程、送出维修以及销毁等进行严格的管理，对带出工作环境的存储介质进行内容加密和监控管理，对送出维修或销毁的介质应首先清除介质中的敏感数据，对保密性较高的存储介质未经批准不得自行销毁；

b) 应建立资产安全管理制度，规定信息系统资产管理的人员或责任部门，并规范资产管理和使用的行为；

b) 应建立基于申报、审批和专人负责的设备安全管理制度，对信息系统的各种软硬件设备的选型、采购、发放和领用等过程进行规范化管理；

d) 应对终端计算机、工作站、便携机、系统和网络等设备的操作和使用进行规范化管理，按操作规程实现主要设备（包括备份和冗余设备）的启动/停止、加电/断电等操作；

b) 应指定专人对网络和主机进行恶意代码检测并保存检测记录；

应建立密码使用管理制度，使用符合国家密码管理规定的密码技术和产品。

b) 应建立备份与恢复管理相关的安全管理制度；

e) 应定期执行恢复程序，检查和测试备份介质的有效性，确保可以在恢复程序规定的时间内完成备份的恢复。

注：基于《网络安全保护基本要求 第一部分：通用安全要求》征求意见稿及GB/T 22239《信息安全等级保护基本要求》三级要求对比分析。

● 等级保护2.0基本要求解析

整体变化

技术

管理

④ 安全运维管理——实质性变更2

- 将原有属于监控管理和安全管理中心的内容移到了“网络和通信安全”部分。
- 将原有属于网络安全设备的部分内容移到了“漏洞和风险管理”部分。
- 降低了对网络和系统管理的要求，包括安全事件处置管理、实施某些网络管理活动、网络接入策略控制。

1.0 要求

a) 应对通信线路、主机、网络设备和应用软件的运行状况、网络流量、用户行为等进行监测和报警，形成记录并妥善保存；
b) 应组织相关人员定期对监测和报警记录进行分析、评审，发现可疑行为，形成分析报告，并采取必要的应对措施；
c) 应建立安全管理中心，对设备状态、恶意代码、补丁升级、安全审计等安全相关事项进行集中管理。

c) 应根据国家相关管理部门对计算机安全事件等级划分方法和安全事件对本系统产生的影响，对本系统计算机安全事件进行等级划分；
d) 应制定安全事件报告和响应处理程序，确定事件的报告流程、响应和处置的范围、程度，以及处理方法等；
e) 制定防止再次发生的补救措施，过程形成的所有文件和记录均应妥善保存；

d) 应定期对网络系统进行漏洞扫描，对发现的网络系统安全漏洞进行及时的修补；

a) 应指定专人对网络进行管理，负责运行日志、网络监控记录的日常维护和报警信息分析和处理工作
c) 应根据厂家提供的软件升级版本对网络设备进行更新，并在更新前对现有的重要文件进行备份；
e) 应实现设备的最小服务配置，并对配置文件进行定期离线备份；
g) 应依据安全策略允许或者拒绝便携式和移动式设备的网络接入；

a) 应根据业务需求和系统安全分析确定系统的访问控制策略；

注：基于《网络安全保护基本要求 第一部分：通用安全要求》征求意见稿及GB/T 22239《信息安全等级保护基本要求》三级要求对比分析。

● 等级保护2.0基本要求解析

整体变化

技术

管理

④ 安全运维管理——实质性变更3

□ 特别增加了**漏洞和风险管理**、配置管理、外包运维管理的**管理要求**。

□ 强化了对**账号管理**、运维管理、设备报废或重用的**管理要求**。

2.0
要求

a) 应采取必要的措施识别安全漏洞和隐患，对发现的安全漏洞和隐患及时进行修补或评估可能的影响后进行修补；
b) 应定期开展安全测评，形成安全测评报告，采取措施应对发现的安全问题

a) 应记录和保存基本配置信息，包括网络拓扑结构、各个设备安装的软件组件、软件组件的版本和补丁信息、各个设备或软件组件的配置参数等；
b) 应将基本配置信息改变纳入变更范畴，实施对配置信息改变的控制，并及时更新基本配置信息库

a) 应确保外包运维服务商的选择符合国家的有关规定；
b) 应与选定的外包运维服务商签订相关的协议，明确约定外包运维的范围、工作内容；
c) 应确保选择的外包运维服务商在技术和管理方面均具有按照等级保护要求开展安全运维工作的能力，并将能力要求在签订的协议中明确；
d) 应在与外包运维服务商签订的协议中明确所有相关的安全要求。如可能涉及对敏感信息的访问、处理、存储要求，对IT基础设施中断服务的应急保障要求等。

b) 应指定专门的部门或人员进行账号管理，对申请账号、建立账号、删除账号等进行控制；

f) 应严格控制变更性运维，经过审批后才可改变连接、安装系统组件或调整配置参数，操作过程中应保留不可更改的审计日志，操作结束后应同步更新配置信息库；
g) 应严格控制运维工具的使用，经过审批后才可接入进行操作，操作过程中应保留不可更改的审计日志，操作结束后应删除工具中的敏感数据；
h) 应严格控制远程运维的开通，经过审批后才可开通远程运维接口或通道，操作过程中应保留不可更改的审计日志，操作结束后立即关闭接口或通道；

d) 含有存储介质的设备在报废或重用前，应进行完全清除或被安全覆盖，确保该设备上的敏感数据和授权软件无法被恢复重用。

注：基于《网络安全保护基本要求 第一部分：通用安全要求》征求意见稿及GB/T 22239《信息安全等级保护基本要求》三级要求对比分析。



4 等级保护2.0扩展要求解析

• 等级保护2.0扩展要求解析-云计算

定级

责任划分

IaaS

PaaS

SaaS

云计算平台架构

云计算平台由设施、硬件、资源抽象控制层、虚拟化计算资源、软件平台和应用软件等组成。

软件即服务 (SaaS)

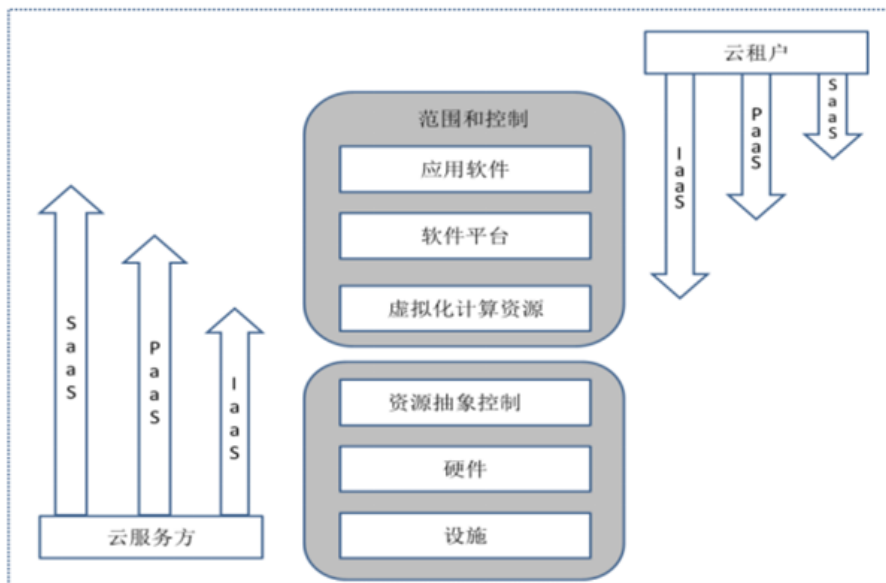
在平台即服务模式，云计算平台包括设施、硬件、资源抽象控制层、虚拟化计算资源和软件平台；

平台即服务 (PaaS)

在平台即服务模式，云计算平台包括设施、硬件、资源抽象控制层、虚拟化计算资源和软件平台；

基础设施即服务 (IaaS)

在基础设施即服务模式，云计算平台由设施、硬件、资源抽象控制层组成；



• 等级保护2.0扩展要求解析-云计算

定级

责任划分

IaaS

PaaS

SaaS

云计算环境

云服务方

在云计算环境中，应将云服务方侧的云计算平台单独作为定级对象定级。

云租户

云租户侧的等级保护对象也应作为单独的定级对象定级。

大型云计算平台

应将云计算基础设施和有关辅助服务系统划分为不同的定级对象。

• 等级保护2.0扩展要求解析-云计算

定级

责任划分

IaaS

PaaS

SaaS

云计算系统与传统信息系统保护对象差异

层面	云计算系统保护对象	传统信息系统保护对象
物理和环境安全	机房及基础设施	机房及基础设施
网络和通信安全	网络结构、网络设备、安全设备、虚拟化网络结构、虚拟网络设备、虚拟安全设备	传统的网络设备、传统的安全设备、传统的网络结构
设备和计算安全	网络设备、安全设备、虚拟网络设备、虚拟安全设备、物理机、宿主机、虚拟机、虚拟机监视器、云管理平台、数据库管理系统、终端	传统主机、数据库管理系统、终端
应用和数据安全	应用系统、云应用开发平台、中间件、云业务管理系统、配置文件、镜像文件、快照、业务数据、用户隐私、鉴别信息等	应用系统、中间件、配置文件、业务数据、用户隐私、鉴别信息等
系统安全建设管理	云计算平台接口、云服务商选择过程、SLA、供应链管理过程等	N/A

等级保护2.0扩展要求解析-云计算

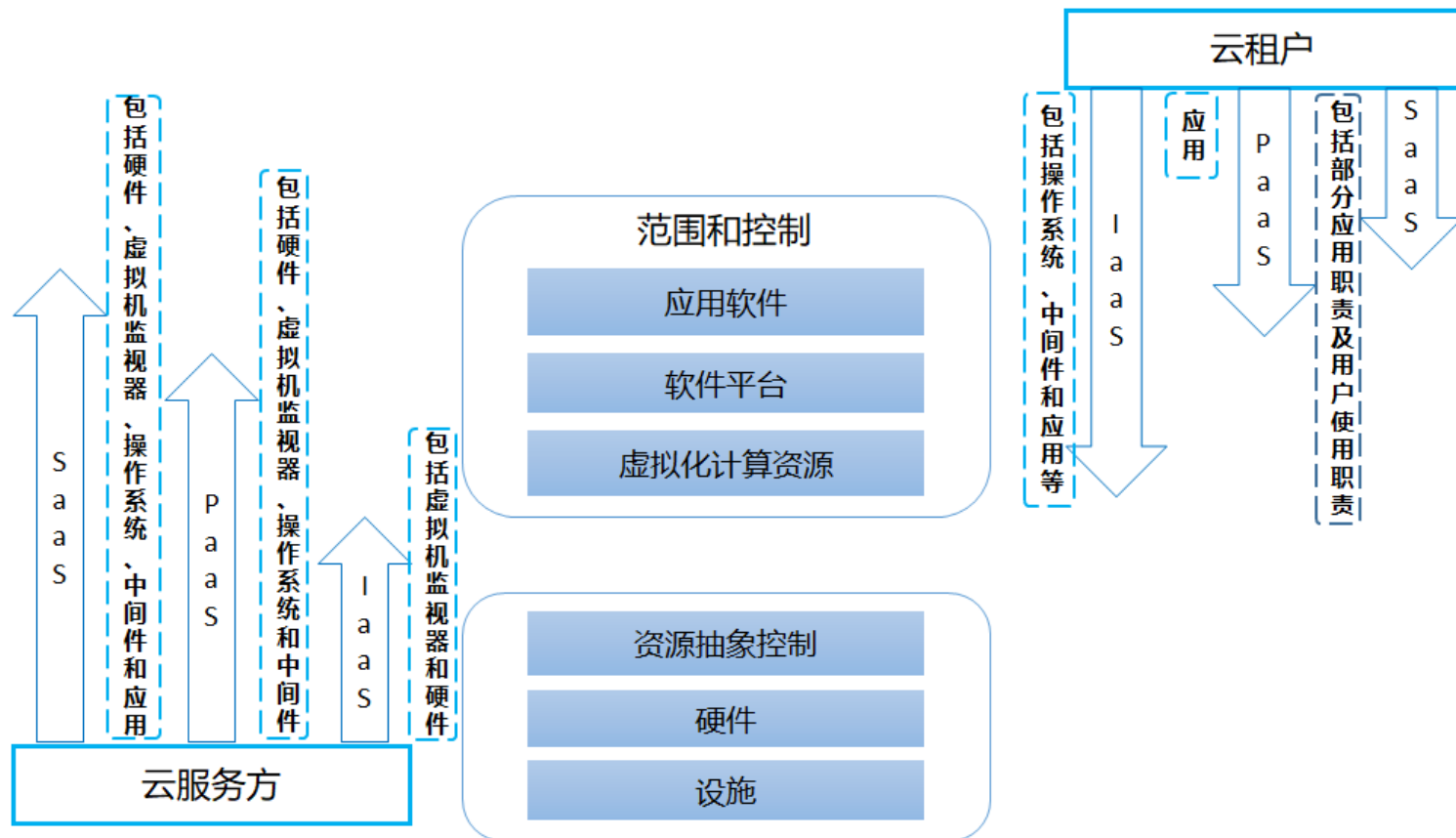
定级

责任划分

IaaS

Paas

SaaS



• 等级保护2.0扩展要求解析-云计算

定级

责任划分

IaaS

Paas

Saas

① 设施——控制要求

应用软件

软件平台

虚拟化计算资源

资源抽象控制

硬件

设施

- 提出物理位置的选择的要求，例如云计算的所有物理设备和数据均存放在国内。
- 提出服务供应商选择和供应链管理的要求，例如选择云服务商和供应商的过程须符合国家的有关要求。

• 等级保护2.0扩展要求解析-云计算

定级

责任划分

IaaS

Paas

Saas

① 硬件——控制要求

应用软件


软件平台

虚拟化计算资源

资源抽象控制

硬件

设施

- 
- 提出身份鉴别的要求，例如设备之间建立双向身份验证机制。
 - 提出访问控制的要求，例如在远程管理设备时不能直接连接其他网络。
 - 提出数据保密性的要求，例如保证设备之间网络通信的保密性。

• 等级保护2.0扩展要求解析-云计算

定级

责任划分

IaaS

Paas

SaaS

① IaaS——控制要求2

□ 特别增加了**镜像和快照保护**的控制要求。

□ 提出了对身份验证机制的控制要求。

□ 提出了对职责与权限划分、数据安全审计、恶意代码检测、虚拟机迁移、资源控制的要求。

应在网络策略控制器和网络设备（或设备代理）之间建立 **双向身份验证机制**。

- a) 当进行远程管理时，防止远程管理设备同时直接连接其他网络；
- b) 确保 只有在云租户授权下，云服务方或第三方 才具有 云租户数据 的管理权限；
- c) 提供云计算平台管理用户权限分离机制，为网络管理员、系统管理员建立不同 账户并分配相应的权限。

- a) 根据云服务方和云租户的职责划分，收集各自控制部分的审计数据；
- b) 保证云服务方对云租户系统和数据的操作可被云租户审计；
- c) 保证审计数据的真实性和完整性；
- d) 为安全审计数据的汇集提供接口，并可供第三方审计；
- e) 根据云服务方和云租户的职责划分，实现各自控制部分的集中审计。

- a) 确保虚拟机迁移过程中，重要数据的保密性，防止在迁移过程中的重要数据泄露；
- b) 支持云租户部署密钥管理解决方案，确保云租户自行实现数据的加解密过程；
- c) 对网络策略控制器和网络设备（或设备代理）之间网络通信进行加密。

- a) 虚拟机对宿主机资源的异常访问，并进行告警；
- b) 虚拟机之间的资源隔离失效，并进行告警；
- c) 非授权新建虚拟机或者重新启用虚拟机，并进行告警。

应能够检测恶意代码感染及在虚拟机间蔓延的情况，并提出告警。

- a) 屏蔽虚拟资源故障，某个虚拟机崩溃后不影响虚拟机监视器及其他虚拟机；
- b) 对物理资源和虚拟资源按照策略做统一管理调度与分配；
- c) 保证虚拟机仅能使用为其分配的计算资源；
- d) 保证虚拟机仅能迁移至相同安全等级的资源池；
- e) 保证分配给虚拟机的内存空间仅供其独占访问；
- f) 对虚拟机的网络接口的带宽进行设置，并进行监控；
- g) 为监控信息的汇集提供接口，并实现集中监控。

- a) 提供虚拟机镜像、快照完整性校验功能，防止虚拟机镜像被恶意篡改；
- b) 采取加密或其他技术手段防止虚拟机镜像、快照中可能存在的敏感资源被非法访问；
- c) 针对重要业务系统提供加固的操作系统镜像。

应确保虚拟机迁移过程中，重要数据的完整性，并在检测到完整性受到破坏时采取必要的恢复措施。

应保证虚拟机所使用的内存和存储空间回收时得到完全清除。

• 等级保护2.0扩展要求解析-云计算

定级

责任划分

IaaS

PaaS

SaaS

② PaaS——控制要求1

- 提出了对数据集中审计的、职责划分的要求。
- 提出了对开发环境访问控制的要求。

- a) 根据云服务方和云租户的职责划分，收集各自控制部分的审计数据；
- b) 保证云服务方对云租户系统和数据的操作可被云租户审计；
- c) 保证审计数据的真实性和完整性；
- d) 为安全审计数据的汇集提供接口，并可供第三方审计；
- e) 根据云服务方和云租户的职责划分，实现各自控制部分的集中审计。

- b) 保证不同云租户的应用系统及开发平台之间的隔离。

• 等级保护2.0扩展要求解析-云计算

定级

责任划分

IaaS

Paas

SaaS

③ SaaS——控制要求1

□ 特别增加了**接口安全**的控制要求。

□ 提出了对应用系统监测、数据备份/存储/迁移/审计的控制要求。

□ 提出了对职责与权限划分、数据安全审计、恶意代码检测、资源控制的要求。

应保证云计算服务对外接口的安全性。

- a) 云租户应在本地保存其业务数据的备份；
- b) 提供查询云租户数据及备份存储位置的方式；
- c) 保证不同云租户的审计数据隔离存放；
- d) 为云租户将业务系统及数据迁移到其他云计算平台和本地系统提供技术手段，并协助完成迁移过程。

a) 能够对应用系统的运行状况进行监测，并在发现异常时进行告警

• 等级保护2.0扩展要求解析-云计算

定级

责任划分

IaaS

Paas

SaaS

③ SaaS——控制要求2

- 特别增加了供应链管理、监控和审计管理的控制要求。
- 提出了对选择服务商、测试验收、平台接口安全、授权审批的控制要求。

a) 确保选择供应商的过程符合国家的有关规定；
b) 确保供应链安全事件信息或威胁信息能够及时传达到云租户；
c) 保证供应商的重要变更及时传达到云租户，并评估变更带来的安全风险，采取有关措施对风险进行控制。

a) 确保信息系统的监控活动符合关于隐私保护的相关政策法规；
b) 确保提供给云租户的审计数据的真实性和完整性；
c) 制定相关策略，对安全措施有效性进行持续监控；
d) 云服务方应将安全措施有效性的监控结果定期提供给相关云租户。

应保证云服务方对云租户业务数据的访问或使用必须经过云租户的授权，授权必须保留相关记录。

云计算平台应提供开放接口或开放性安全服务，允许云租户接入第三方安全产品或在云平台选择第三方安全服务，支持异构方式对云租户的网络、主机、应用、数据层的安全措施进行实施

应验证或评估所提供的安全措施的有效性。

a) 确保选择云服务商的过程符合国家有关规定；
b) 选择安全合规的云服务商，其所提供的云平台应具备与信息系统等级相应的安全保护能力；
c) 满足服务水平协议（SLA）要求；
d) 在服务水平协议（SLA）中规定云服务的各项服务内容和具体技术指标；
e) 在服务水平协议（SLA）中规定云服务商的权限与责任，包括管理范围、职责划分、访问授权、隐私保护、行为准则、违约责任等；
f) 在服务水平协议（SLA）中规定云计算所能提供的安全服务的内容，并提供安全声明；
g) 在服务水平协议（SLA）中规定服务合约到期时，完整地返还云租户信息，并承诺相关信息均已在云计算平台上清除；
h) 与选定的云服务商签署保密协议，要求其不得泄露云租户数据和业务系统的相关重要信息；
i) 对可能接触到云租户数据的员工进行背景调查，并签署保密协议；
j) 云服务商应接受云租户以外的第三方运行监管。

• 等级保护2.0扩展要求解析-移动互联

定级

移动终端

无线网络

移动应用

移动管理

① 定级

移动互联技术的等级保护对象应作为一个整体对象定级，移动终端、移动应用和无线网络等要素不单独定级，与采用移动互联技术等级保护对象的应用环境 and 应用对象一起定级。

• 等级保护2.0扩展要求解析-移动互联

定级

移动终端

无线网络

移动应用

移动管理

② 移动终端——控制要求1

□ 提出了对移动终端 自身安全、移动终端运行环境、移动终端应用管理的控制要求。

- a) 应对移动终端用户登录、移动终端管理系统登录及其他系统级应用登录进行身份鉴别；
- b) 移动终端应具有登录失败处理功能，应配置并启用限制非法登录次数等措施。

- a) 应启用移动终端安全审计功能，对终端用户重要操作及软件行为进行审计；
- b) 审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；
- c) 应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等

- a) 移动终端应安装防恶意代码软件，并定期进行恶意代码扫描，及时更新防恶意代码软件版本和恶意代码库；
- b) 移动终端应支持移动业务应用软件仅运行在**安全容器**内，防止被恶意代码攻击。

- a) 应将移动终端处理访问不同等级等级保护对象的运行环境进行**操作系统级**隔离；
- b) 应将移动终端处理访问等级保护对象的运行环境与非处理访问等级保护对象运行环境进行**系统级**隔离；
- c) 应限制用户或进程对移动终端系统资源的最大使用限度，防止移动终端被提权。

• 等级保护2.0扩展要求解析-移动互联

定级

移动终端

无线网络

移动应用

移动管理

② 移动终端——控制要求2

□ 特别增加了应用管控、移动终端管控的控制要求。

- a) 移动终端管理客户端应具有**软件白名单功能**，应能根据白名单控制应用软件安装、运行；
- b) 移动终端管理客户端应具有应用软件权限控制功能，应能控制应用软件对移动终端中资源的访问；
- c) 移动终端管理客户端应只允许 **等级保护对象** 管理者指定 证书签名的应用软件安装和运行；
- d) 移动终端管理客户端应具有接受移动终端管理服务端推送的移动应用软件**管理策略**， 并根据该策略对软件实施管控的能力。

- a) 应保证移动终端只用于处理与 等级保护对象 相关业务；
- b) 应保证移动终端安装、 注册 并 运行 终端管理客户端软件；
- c) 移动终端应接受 等级保护对象 移动 终端管理服务端 的设备 生命周期 管理、 设备远程控制、设备安全管控。

• 等级保护2.0扩展要求解析-移动互联

定级

移动终端

无线网络

移动应用

移动管理

③ 无线网络——控制要求1

□ 特别增加了网络设备防护、无线通信完整性和保密性的控制要求。

□ 提出了对无线网络设备在无线设备接入、无线设备自身安全、通信安全、网络边界安全的控制要求。

- a) 应保证无线接入网关的处理能力满足业务高峰期需要；
- b) 应保证无线接入设备的带宽满足业务高峰期需要；
- c) 无线接入设备应开启接入认证功能，并支持采用**认证服务器或国产算法**进行加密。

- a) 应在有线网络与无线网络边界根据访问控制策略设置访问控制规则，默认情况下，除允许通信外，受控接口**拒绝所有通信**；
- b) 应对来自移动终端的数据流量、数据包和协议等进行检查，以允许/拒绝数据包通过；
- c) 应在无线接入网关上对进出无线网络的数据进行**内容过滤**；

- a) 应能够检测、记录、定位非授权无线接入设备；
- b) 应能够对**非授权移动终端**接入的行为进行检测、记录、定位；
- c) 应具备对针对无线接入设备的网络扫描、DoS 攻击、密钥破解、中间人攻击和欺骗攻击等行为进行检测、记录、分析定位；

- a) 应能发现系统移动终端、无线接入设备、无线接入网关设备可能存在的漏洞，并在经过充分测试评估后，及时修补漏洞；
- b) 应**禁用**无线接入设备和无线接入网关存在风险的功能，如：SSID广播、WEP认证等；
- c) 应禁止多个AP使用同一个鉴别密钥。

• 等级保护2.0扩展要求解析-移动互联

定级

移动终端

无线网络

移动应用

移动管理

④ 移动应用——控制要求1

□ 特别增加了软件审核与检测的控制要求。

□ 提出了对移动应用系统自身安全、代码完整性、通信安全、备份恢复管理的控制要求。

- a) 使用口令登录时，应强制用户**首次登录时修改初始口令**，对用户的鉴别信息进行复杂度检查；
- b) 用户身份鉴别信息丢失或失效时，应采用鉴别信息重置或其他技术措施保证系统安全；
- c) 移动应用软件应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，鉴别信息具有复杂度要求；
- d) 移动应用软件应提供并启用登录失败处理功能，多次登录失败后应采取必要的保护措施；
- e) 应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。

- a) 移动应用软件应采用密码技术保证通信过程中数据的完整性；
- b) 移动应用软件应采用校验技术或密码技术保证重要数据存储时的完整性，并在检测到完整性错误时采取必要的恢复措施；
- c) 移动应用软件应采用校验技术保证代码的完整性。

- a) 移动应用软件应采用密码技术保证**重要数据在本地存储时的保密性**；
- b) 应确保移动应用软件之间的重要数据**不能被互操作**；
- c) 应确保移动应用软件数据文件所在的存储空间，被释放或重新分配前可得到完全清除；
- d) 移动应用软件应对通信过程中的敏感信息字段或整个报文进行密码加密。

应保证等级保护对象业务移动应用软件开发后上线前经专业测评机构安全检测。

• 等级保护2.0扩展要求解析-移动互联

定级

移动终端

无线网络

移动应用

移动管理

⑤ 移动管理——管理要求1

□ 提出了对管理制度的制定、岗位职责设定、日常操作管理、技能培训的管理要求。

- a) 应建立等级保护对象移动互联安全管理制度，并纳入等级保护对象安全管理安全制度；
- b) 应对管理人员或移动终端操作人员执行的日常管理操作建立操作规程；
- c) 应在等级保护对象管理制度中建立移动终端管理服务端操作使用管理规定。

- a) 应将移动互联管理纳入等级保护对象管理员职责；
- b) 应设立移动互联信息安全管理工作的职能部门，并制定各负责人的职责；
- c) 应为移动终端管理服务端设置专职管理员、操作员，并纳入职能部门职责。

应保证移动终端管理服务端配备专职管理员、操作员和审计员

- a) 应根据各个部门和岗位的职责明确移动互联管理授权审批事项、审批部门和批准人；
- b) 应针对移动互联系统变更、重要操作、物理访问和系统接入等事项执行审批过程；
- c) 应保证移动终端管理服务端设置专职管理员、操作员权限由审批部门或批准人批准。

- a) 应对各类人员进行移动互联管理安全意识教育和岗位技能培训，并告知相关的安全责任和惩戒措施；
- b) 应对移动终端管理服务端设置专职管理员、操作员进行专项安全意识教育和岗位技能培训，并告知相关的安全责任和惩戒措施

• 等级保护2.0扩展要求解析-移动互联

定级

移动终端

无线网络

移动应用

移动管理

⑤ 移动管理——管理要求2

□ 提出了对软件开发活动、产品采购、工程实施、方案设计、系统交付活动、服务商选择的管理要求。

- a) 应根据等级保护对象的安全保护等级选择移动互联基本安全措施，依据风险分析的结果补充和调整安全措施；
- b) 应根据等级保护对象的安全保护等级进行移动互联安全方案设计，并纳入系统总体方案设计；
- c) 应组织相关部门和安全专家对系统移动互联安全方案设计进行论证和审定，经过批准后才能正式实施。

- a) 应确保移动互联信息安全产品采购和使用符合国家的有关规定；
- b) 相关密码产品使用应符合国家密码管理相关规定。

应指定或授权专门的部门或人员负责系统移动互联工程实施过程的管理。
应对系统的移动互联部分进行安全性测试验收。

- a) 应根据交付清单对所交接的移动互联设备、移动应用程序和文档等进行清点；
- b) 应对负责系统移动互联运行维护的技术人员进行相应的技能培训
- c) 应确保提供移动互联建设过程中的文档和指导用户进行系统运行维护的文档；
- d) 应确保提供移动终端管理服务端建设过程中的文档和指导用户进行系统运行维护的文档。

- a) 应要求对移动业务应用程序开发者进行资格审查；
- b) 应确保开发移动业务应用程序的签名证书合法性；
- c) 应要求移动应用程序开发完提供软件设计文档、使用指南及软件源代码；
- d) 应要求应用程序开发使用的工具来源可靠；
- e) 自行开发移动应用程序,应确保开发环境与实际运行环境物理分开，测试数据和测试结果受到控制；
- f) 自行开发移动应用程序,应制定软件开发管理制度，明确说明开发过程的控制方法和人员行为准则；
- g) 自行开发移动应用程序,应确保具备软件设计的相关文档和使用指南，并对文档使用进行控制；
- h) 自行开发移动应用程序,应确保对程序资源库的修改、更新、发布进行授权和批准，并严格进行版本控制。

- a) 应确保移动互联安全服务商的选择符合国家的有关规定；
- b) 应与选定的移动互联安全服务商签订与安全相关的协议，明确约定相关责任；
- c) 应与选定的服务供应商签订相关协议，明确整个服务供应链各方需履行的信息安全相关义务；
- d) 应选择安全可靠 应用程序分发 运营商

等级保护2.0扩展要求解析-移动互联

定级

移动终端

无线网络

移动应用

移动管理

⑤ 移动管理——管理要求3

□ 特别增加了应用软件来源管理和监控和审计管理的要求。

□ 提出了对资产管理、漏洞评估与修复、恶意代码检测、版本管理、备份恢复管理、事件处置的管理要求。

- a) 应编制并保存与等级保护对象相关的移动终端资产清单，包括资产责任部门、重要程度和使用人等内容；
- b) 应根据资产的重要程度对移动终端进行标识管理，根据其价值选择相应的管理措施。

- a) 应对各种移动互联设备（包括无线接入设备及移动终端）维护纳入等级保护对象进行管理；
- b) 应确保移动终端在报废或重用前应进行完全清除或被安全覆盖，确保该设备上的敏感数据和授权软件无法被恢复重用；
- c) 应在移动终端设备丢失后进行远程数据擦除。

应采取必要的措施识别移动互联安全漏洞和隐患，对发现的安全漏洞和隐患及时进行修补或评估可能的影响后进行修补。

- a) 应对移动终端应用软件恶意代码防范要求做出规定，包括防恶意代码软件的授权使用、恶意代码库升级、恶意代码的定期查杀等；
- b) 应对截获的恶意代码进行及时分析处理；
- c) 应保证移动终端管理服务端将移动应用软件运行策略推送给移动终端。

- a) 移动终端管理服务端应记录和保存移动终端基本配置信息，包括操作系统、软件组件版本、移动终端各种设备或软件组件的配置参数等；
- b) 移动终端管理服务端应将移动终端基本配置信息改变纳入系统变更范畴，实施对配置信息改变控制，并及时更新基本配置信息库；
- c) 应建立合法无线接入设备和合法移动终端配置库，用于对非法无线接入设备和非法移动终端的识别。

- a) 应识别需要定期备份的移动终端中的重要业务信息、系统数据及软件系统等；
- b) 应规定备份信息的备份方式、备份频度、存储介质、保存期等；
- c) 应根据数据的重要性和数据对系统运行的影响，制定数据的备份策略和恢复策略、备份程序和恢复程序等。

- a) 应报告所发现的移动互联安全弱点和可疑事件；
- b) 应明确安全事件的报告和处置流程，规定安全事件的现场处理、事件报告和后期恢复的管理职责；
- c) 应针对移动互联系统发生的安全事件制定应急处置预案。

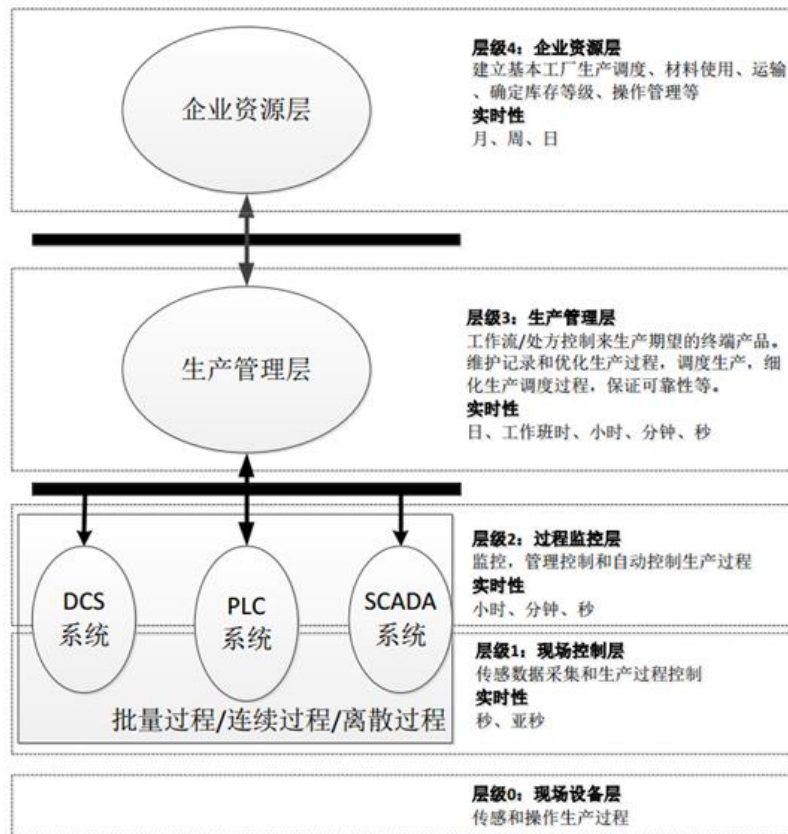
- a) 应保证移动终端安装、运行的应用软件来自等级保护对象管理者指定证书签名或可靠分发渠道；
- b) 应保证移动终端安装、运行的移动应用软件由经审核的开发者开发。
- a) 应确保移动终端管理服务端对移动终端状态、资源使用、软件运行等进行监控和审计；
- b) 应对上线后的业务移动应用软件进行监测

等级保护2.0扩展要求解析-工业扩展

生产管理-功能模型

工业控制系统安全

功能层次模型



● 等级保护2.0扩展要求解析-工业扩展

生产管理-控制要求

□ 提出了对网络区域防护、设备硬件冗余、访问控制策略管理、审计管理的控制要求。

- a) 应避免将重要网络区域部署在网络边界处且没有边界防护措施;
- b) 应提供通信线路、关键网络设备的硬件冗余, 保证系统的可用性。

- a) 对一个可配置的时间或事件序列, 应支持主管手动超驰当前人员用户授权;
- b) 应通过手动或在一个可配置非活动周期后系统自动启动会话锁定防止进一步访问。会话锁定应一直保持有效, 直到拥有会话的人员用户或其它授权的人员用户使用适当的身份标识和鉴别规程重新建立访问;
- c) 应在一个可配置非活动时间周期后自动地, 或由发起会话的用户手动地终止远程会话;
- d) 应在网络边界或安全域之间根据访问控制策略设置访问控制规则, 默认情况下除允许通信外受控接口拒绝所有通信;
- e) 应删除多余或无效的访问控制规则, 优化访问控制列表, 并保证访问控制规则数量最小化。

- a) 应能生成安全相关审计记录, 包括:访问控制、请求错误、操作系统事件、备份和恢复事件、配置改变、潜在的侦察活动和审计日志事件。单个审计记录应包括时间戳、来源(源设备、软件进程或人员用户帐户)、分类、类型、事件 ID 和事件结果;
- b) 应能集中管理审计事件并从系统多个组件收集审计记录, 系统范围(逻辑或物理)的时间相关审计踪迹。应能按照工业标准格式输出这些审计记录, 用于商业日志分析工具进行分析, 例如, 安全信息和事件管理(SIEM);
- c) 根据一般公认的日志管理和系统配置的建议, 系统应设置足够的审计记录存储容量。系统应提供审计机制来减少超出容量的可能性;
- d) 当分配审计记录存储值达到最大审计记录存储容量的配置比例时, 系统应能发出警告; 当容量超出时, 支持覆盖;
- e) 在审计事件的处理失败时, 系统能对人员进行警示并防止丧失基本服务和功能。根据普遍接受的工业实践和建议, 系统应能在审计处理失败的情况下, 采取恰当响应行动;
- f) 在审计记录生成时, 系统应提供时间戳;
- g) 应在可配置的频率下, 对系统时钟进行同步;
- h) 应保护审计信息和审计工具(如有), 防止其在未授权情况下被获取、修改和删除;

• 等级保护2.0扩展要求解析-工业扩展

生产管理-控制要求

- 特别增加了应用软件来源管理和监控和审计管理的要求。
- 提出了对资产管理、漏洞评估与修复、恶意代码检测、版本管理、备份恢复管理、事件处置的管理要求。

- a) 应对控制网络和非控制网络的边界，以及控制系统内安全域和安全域之间的边界，进行监视和控制区域边界通信；
- b) 应在控制网络和非控制网络的边界，以及控制系统内安全域和安全域之间的边界，默认拒绝所有网络数据流，允许例外网络数据流；
- c) 应在控制网络和非控制网络的边界，以及控制系统内安全域和安全域之间的边界上，阻止任何通过的通信；
- d) 应在控制网络和非控制网络的边界防护机制失效时，能阻止所有边界通信（也称）故障关闭；但故障关闭功能的设计不应干扰安全相关功能的运行；应在控制系统内安全域和安全域之间的边界防护机制失效时，及时进行报警，并保障不影响关键设备通讯；
- e) 应能够对非授权设备联到内部网络的行为进行限制或检查；
- f) 应能够对内部用户未经授权联到外部网络的行为进行限制或检查；
- g) 应确保无线网络通过受控的控制网络和非控制网络的边界，以及控制系统内安全域和安全域之间的边界时，边界防护设备接入（有线）网络；
- h) 应能识别控制网络和非控制网络上的边界通讯入侵行为，并有效阻断；

- a) 应在关键网络节点处对恶意代码进行检测和清除，并维护恶意代码防护机制的升级和更新；
- b) 应在关键网络节点处对垃圾邮件进行检测和防护，并维护垃圾邮件防护机制的升级和更新。

- a) 应利用会话完整性机制，保证会话完整性；
- b) 应对通信过程中的敏感信息字段或整个报文进行加密

- a) 应对所有参与无线通信的用户（人员、软件进程或者设备）提供唯一性标识和鉴别；
- b) 根据普遍接受的安全工业实践，应对无线连接的授权、监视以及执行使用进行限制；

- a) 应在有效的补救条件下，识别和处理错误状况。在此过程中，不应暴露任何可被攻击者利用以攻击信息安全管理系统的信息，除非透露这一信息对于及时排除故障是必要的；
- b) 应禁止传输、接收私人消息；
- c) 应在关键网络节点处检测、防止或限制从外部发起的网络攻击行为；
- d) 应在关键网络节点处检测和限制从内部发起的网络攻击行为；
- e) 应采取技术措施对网络行为进行分析，实现对网络攻击特别是未知的新型网络攻击的检测和分析；
- f) 当检测到攻击行为时，记录攻击源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件时应提供报警。

● 等级保护2.0扩展要求解析-工业扩展

生产管理-控制要求

- 特别增加了**应用软件来源管理和监控和审计管理**的要求。
- 提出了对**资产管理、漏洞评估与修复、恶意代码检测、版本管理、备份恢复管理、事件处置**的管理要求。

a) 应能唯一地鉴别和认证全部人员用户。应在所有接口上执行标识和鉴别。当有人用户访问时，应根据适用的安全策略和规程实施职责分离和最小权限；

b) 应能对所有使用人员用户实施多因子鉴别；

c) 应能对所有设备提供唯一性标识和鉴别。应在进行系统访问时，使所有接口根据适用的安全策略和规程支持最小权限，实施标识和鉴别。

d) 应支持用户、组、角色或者接口的标识符管理功能；

e) 应能初始化鉴别器内容；系统一经安装完成，立即改变所有鉴别器的默认值；改变或者刷新所有的鉴别器；当存储或者传输的时候，要保护鉴别器免受未经授权的泄露和修改；

f) 对于使用设备的用户，应通过硬件机制保护相关鉴别器；

g) 对于使用口令鉴别机制的设备，设备应能通过设置最小长度和多种字符类型，实现强制配置口令强度；

h) 设备应防止任何已有的用户账户重复使用同一批口令。此外，设备应加强用户口令的最大和最小有效期的使用。这些能力应符合一般公认的安全产业实践要求；

i) 应根据通用的可以接受的安全行业实践和建议，通过硬件机制来保护相关的私钥；

j) 应能够隐藏鉴别过程中的鉴别信息反馈；

k) 应针对任何用户（人员、软件进程或设备）在可配置时间周期内，对连续无效的访问尝试进行可配置次数限制。当限制次数超出后，应在规定的周期内拒绝访问或者直到管理员解锁。对于代表关键服务或者服务器运行的系统账户，不应允许交互式登录；

l) 在进行鉴别之前，应能显示系统提示信息。使用提示信息应可通过授权人进行配置；

m) 当进行远程管理时，应采取必要措施，防止鉴别信息在网络传输过程中被窃听。

a) 应能支持授权用户管理所有帐户，包括添加、激活、修改、禁用和删除帐户；

b) 应能支持统一账户管理；

c) 应在一个可配置非活动时间周期后自动地，或由发起会话的用户手动地终止远程会话；

d) 对于所有接口，应根据职责分离和最小权限对特定用户（人员、软件进程或设备）实施控制系统的控制使用授权；

e) 应能使授权用户或角色可对所有人员用户的许可到角色映射进行规定和修改；

f) 应能在日常维护时，进行安全功能操作的验证和报告异常事件；

g) 应限制默认账户的访问权限，重命名系统默认账户，修改默认口令；

h) 应及时删除多余的、过期的账户，避免共享账户的存在。

• 等级保护2.0扩展要求解析-工业扩展

生产管理-控制要求

□ 特别增加了应用软件来源管理和监控和审计管理的要求。

□ 提出了对资产管理、漏洞评估与修复、恶意代码检测、版本管理、备份恢复管理、事件处置的管理要求。

- a) 应能对可能造成损害的移动代码技术执行使用限制，包括：防止移动代码的执行；对于代码的来源要求适当的鉴别和授权；限制移动代码传入/传出系统；监视移动代码的使用；
- b) 应能允许代码执行之前验证移动代码完整性；
- c) 应能应用保护机制，防止、检测、报告和减轻恶意代码或未经授权软件的影响。应能更新防护机制；
- d) 应在所有入口和出口提供**恶意代码防护**机制；
- e) 应能管理恶意代码防护机制；
- f) 可采用**可信计算技术**建立从系统到应用的信任链，实现系统运行过程中重要程序或文件完整性检测，并在检测到破坏后进行恢复

- a) 在不影响当前安全状态下，系统应能切换至和切换出应急电源的供应；
- b) 应对重要节点进行监视，包括监视 CPU、硬盘、内存等资源的使用情况；
- c) 应能够对重要节点的服务水平降低到预先规定的最小值进行检测和报警。

- a) 无论在信息存储或传输时，都应对有明确读授权的信息提供保密性保护；
- b) 在进行加密时，应按照国家相关保密部门要求采用合适的加密算法、密钥长度和机制。



感谢各位的观看！

邮箱：liudawei824@126.com