等保2.0标准

一、网络安全法解读

网络安全法的背景和历程

网络安全法时间轴

网络安全法的意义和作用

新时代的网络安全主观

国家战略

网络安全上升为国家战略，成为总体国家安全观的重要组成部分

统一体

将网络安全和信息化工作视为一个统一体，形成了一体两翼、驱动双轮的网络安全观

辩证思维

针对网络安全新形势、新特点、提出了整体、动态、开放、相对、共同的辩证网络安全观

合作共赢

针对全球互联网领域发展不平衡、规划不健全、秩序不合理等问题，提出了互相尊重、相互信任基础上合作共赢的网络安全观

以人为本

将以人民为中心的发展新思想贯穿到网络安全领域，形成“网络安全为人民，网络安全靠人民”的以人为本的网络安全观

网络安全法整体框架

防御、控制、三位一体

第一章 总则	14条规定	简述法律目的，范围，总则，部门职责，总体要求等
第二章 网络安全支持与促进	6条规定	定义国家直属部门、政府在推动网络安全工作上的职责
第三章 网络运行安全	19条规定	定义网络运营者与关键信息基础设施的运行安全规定
第一节 一般规定	10条规定	针对网络运营者的网络运行安全要求与职责规定
第二节 关键信息基础设施的运行安全	9条规定	针对关键信息基础设施的安全规定与保护措施要求
第四章 网络信息安全	11条规定	定义个人信息保护的保护规定
第五章 监测预警与应急处置	8条规定	定义国家网络安全监测预警与汇报机制
第六章 法律责任	17条规定	定义处罚规定
第七章 附则	4条规定	相关名词释义与其他附则

第一章、总则

目标:保障网络安全，维护网络空间主权和国家安全、社会公共利益，保护公民、法人和其他组织的合法权益，促进经济社会信息化健康发展

范围:在中华人民共和国境内建设、运营、维护和使用网络，以及网络安全的监督管理

职责:国家网信部门负责统筹协调网络安全工作和相关监督管理工作。国务院电信主管部门、公安部门和一他有关机关依照本法和有关法律、行政法规的规定，在各自职责范围内负责网络安全保护和监督管理工作

关键点:网络安全与信息化发展并重、网络安全战略、基本要求和主要目标、培养网络安全人才、网络技术研发、标准制定、义务、举报，监测、防御、处置境内外安全风险和威胁，保护关键信息基础设施

第二章、支持与促进

定义国家对网络安全工作支持与推进说明，包括相关标准制定与监督;各级政府单位要支持网络安全;包括信息安全技术、信息安全服务、信息安全测评、信息安全教育与宣传、信息安全人才培养等工作

第三章、网络运行安全

第一节：

国家实行网络安全等级保护制度

网络产品、服务应当符合相关国家标准的强制性要求

网络关键设备和产品应强制取得国家安全标准认证

对网络运营者提供标准的安全职责工作说明

第二节：

针对公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务等重要行业和领域，在网络安全等级保护制度的基础上，实行重点保护

每年至少进行一次检测评估

定期组织安全拥挤演练

第四章、网络信息安全

个人隐私保护、发布信息监管

第五章、监测预警与应急处置

网络安全预警监测、安全风险评估、应急预案、风险发布

第六章、法律责任

最高100万:违反22/27/33/34/36/38/41/42/43，最高100万，主管10万

最高50万:违反22/24/27/37/46/47/69

关键安全预防措施

加强网络入侵防护

关键基础设施一旦被入侵，危害极大，要重点进行网络入侵的防护

对于传统威胁，要做到快速处理、精准的防护；对于该机未知威胁，也要做到智能检测与防护

综上，建设加强入侵防护是网络安全防护的核心关键工作

建设安全态势平台

维护网络安全，首先要知道的风险在哪里，是什么样的风险，正所谓"聪者听于无声，明者见于未形"

综上，感知网络安全态势是网络安全防护中最基本、最基础工作

二、等级保护建设

等级保护背景介绍发展历程

信息安全等级保护是最基本制度、基本国策、基本方法

信息安全等级保护是党中央国务院决定在信息系统安全领域实施的基本国策

信息安全等级保护是国家信息安全保障的基本制度

信息安全等级保护是国家信息安全保障工作的基本方法

2016年10月10日，第五届全国信息安全等级保护技术大会召开，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”。

2017年6月1日，《中华人民共和国网络安全法》正式施行，第二十一条明确“国家实行网络安全等级保护制度...”

2019年5月13日网络安全等级保护2.0正式发布，同年12月1日施行。

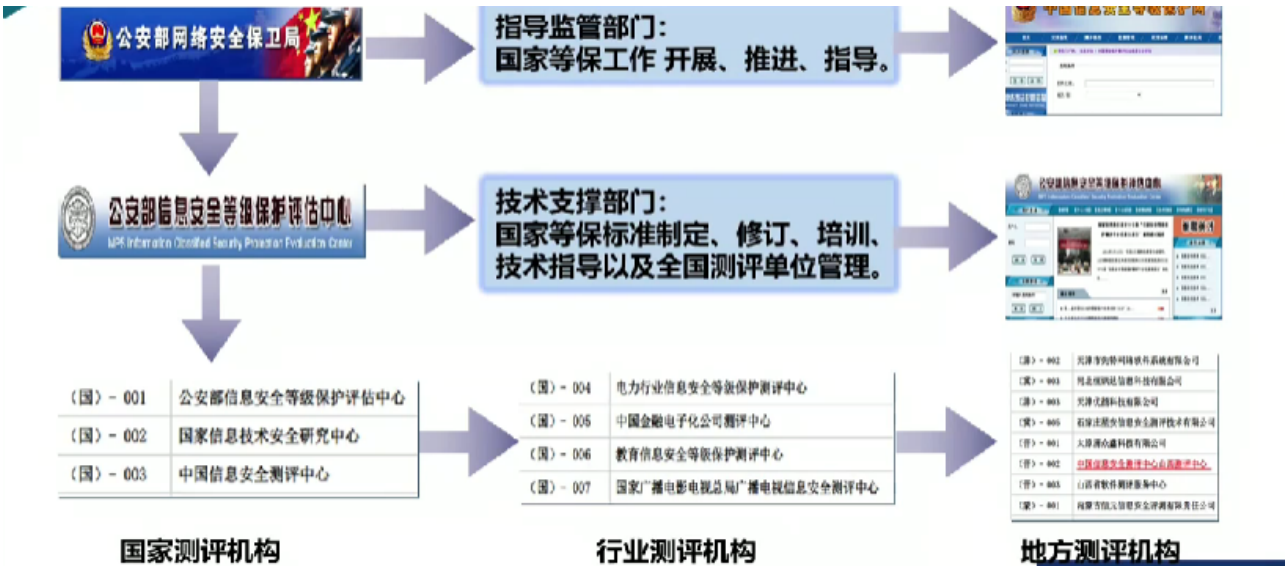
以《GB17859计算机信息系统安全保护等级划分准则》、《GB/T22239-2008信息安全技术信息系统安全等级保护基本要求》为代表的等级保护系列配套标准，习惯称为等保1.0标准。

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。

2019年5月13日《GB/T2239-2019信息安全技术网络安全等级保护基本要求》

等级保护管理组织



等级保护主要工作流程

监督检查是保护能力不断提高的保障

一、定级

定级是等级保护的首要环节

二、备案

备案是等级保护的核心

三、建设整改

建设整改的是等级保护工作落实的关键

四、等级测评

等级测评是评价安全保护状况的方法

网络安全等级保护定级建议

《GB/T 22240-2008信息安全技术网络安全等级保护定级指南》现行标准;

《GB/T 22240-2020信息安全技术网络安全等级保护定级指南》2020年11月1日正式实施。

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

网络安全等级保护定级流程

确定定级对象

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

初步确认的等级

包括确定受侵害的客体、侵害对客体的侵害程度以及综合判定侵害程度。

专家评审

定级对象的运营、使用单位应组织信息安全专家和业务专家，对初步定级结果的合理性进行评审，出具专家评审意见。

主管部门审核

定级对象的运营、使用单位应将初步定级结果上报行业主管部门或上级主管部门进行审核。

公安机关备案审查、最终确定的等级

定级对象的运营、使用单位应按照相关管理规定，将初步定级结果提交公安机关进行备案审查，审查不通过，其运营使用单位应组织重新定级;审查通过后最终确定定级对象的安全保护等级、

网络安全等级保护定级对象

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

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

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

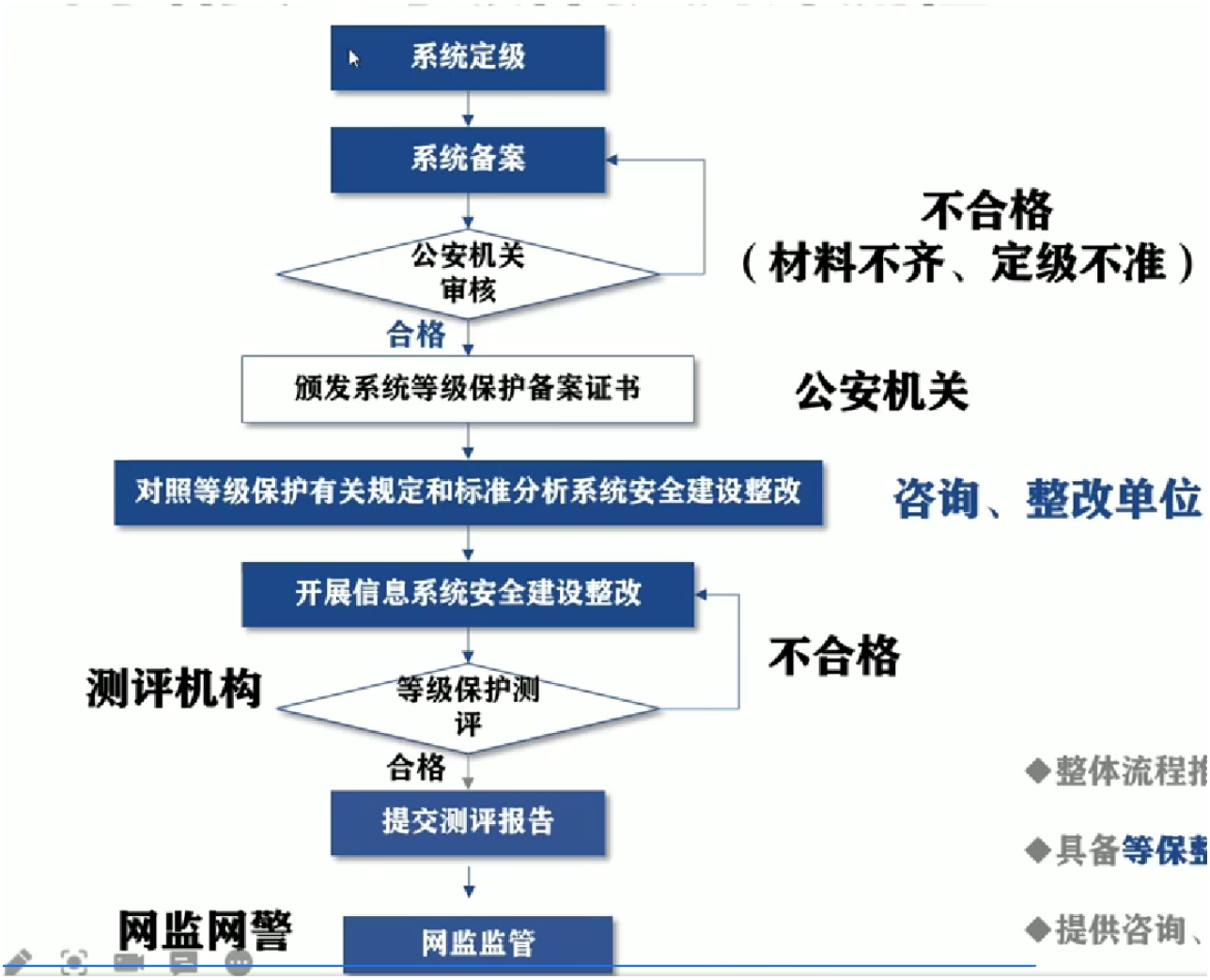
作为定级对象的其他信息系统具有如下基本特征

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;

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;

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样关的和配套的设备、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

网络安全等级保护评测流程



整体流程推动主要由经验丰富的系统集成商把握

具备等保整改资质单位为建设权威

提供咨询、协助备案、预测评、整改支持

等级保护建设核心思想

信息系统的安全设计应基于业务流程自身特点，建立“可信，可控、可管”的安全防护体系，使得系统能够按照预期运行，免受信息安全攻击和破坏。

可信

即以可信认证为基础，构建一个可信的业务系统执行环境，即用户、平台、程序都是可信的，确保用户无法被冒充、病毒无法执行、入侵行为无法成功。可信的环境保证业务系统永远都按照设计预期的方式执行，不会出现预期的流程，从而保障了业务系统安全可信。

可控

即以访问控制技术为核心，实现主体对客体的受控访问，保证所有的访问行为均在可控范围之内进行，在防范内部攻击的同时有效防止了从外部发起的攻击行为。对用户访问权限的控制可以确保系统中的用户不会出现越权操作，永远都按系统设计的策略进行资源访问，保证了系统的信息安全可控。

可管

即通过构建集中管控、最小权限管理与三权分立的管理平台，为管理员创建一个工作平台，使其可以进行技术平台支撑下的安全策略管理，从而保证信息系统安全司管。

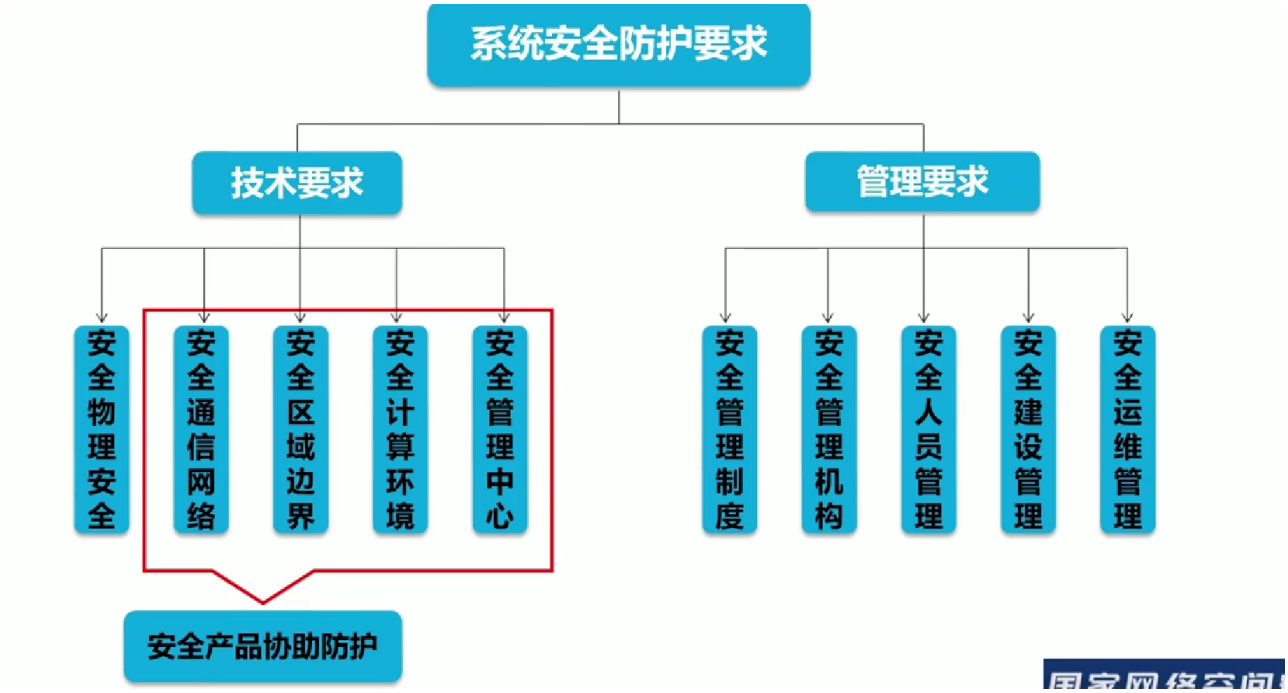
等级保护防护框架

建设“一个中心“管理、“三重防护”体系，分别对计算环境、区域边界、通信网络体系进行管理，实施多层隔离和保护，以防止某薄弱环节影响整体安全

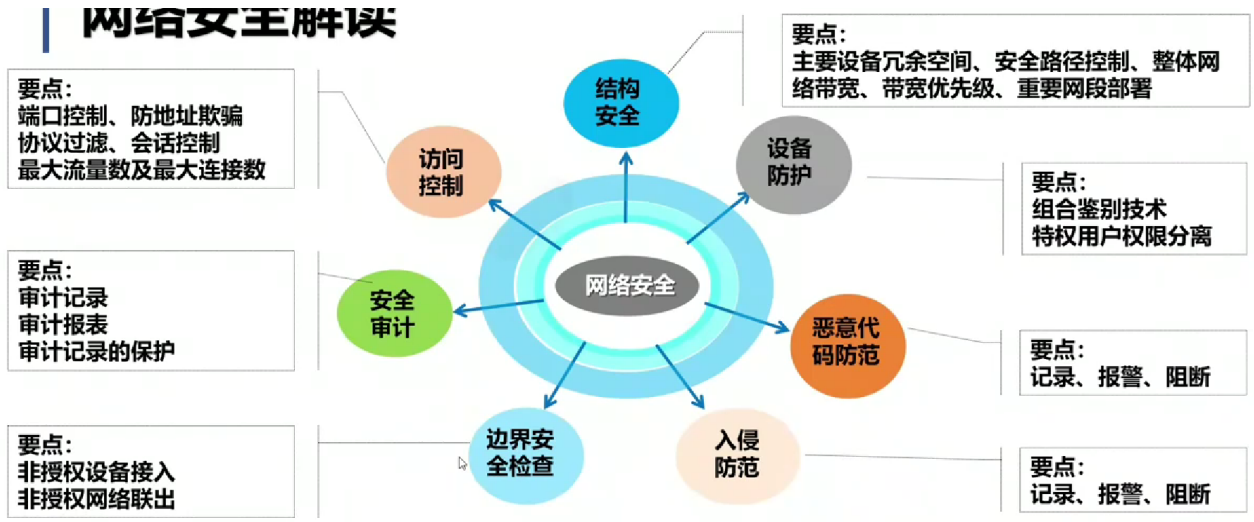
重点对操作人员使用的终端、业务服务器等计算节点进行安全防护，控制操作人员行为，使其不能违规操作，从而把住攻击发起的源头，防止发生攻击行为

分析应用系统的流程，确定用户(主体)和访问的文件（客体)的级别(标记)，以此来制定访问控制安全策略,由操作系统、安全网关等机制自动执行，从而支撑应用安全

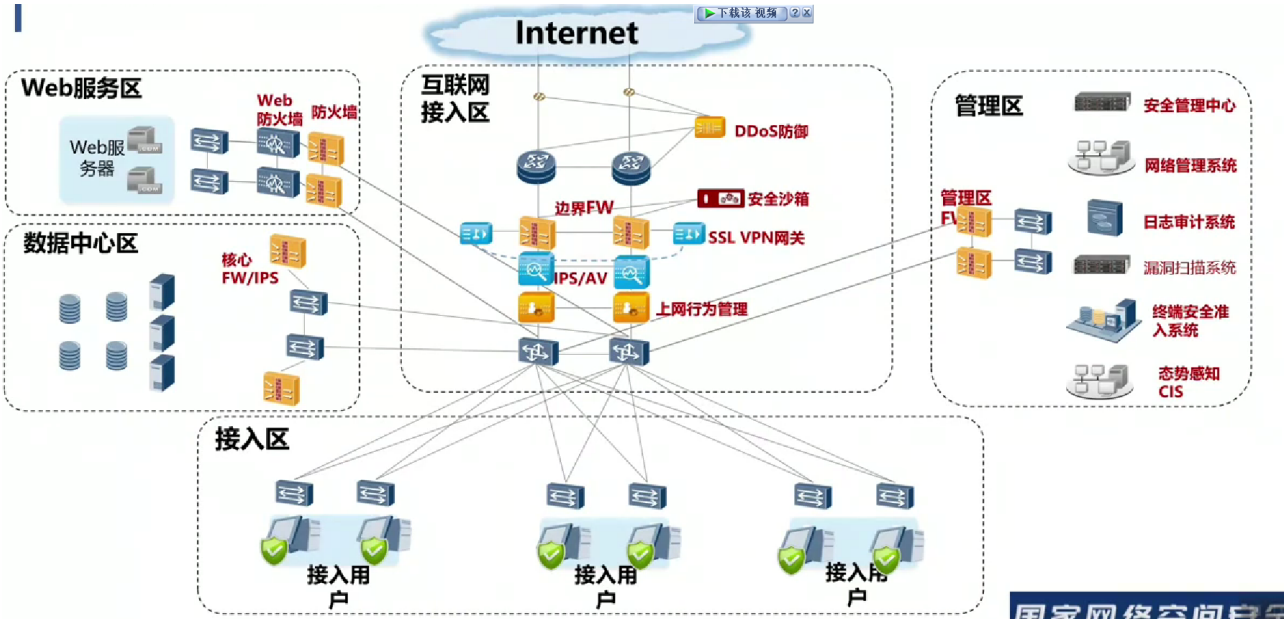
等级保护基本框架要求



网络安全解读



等级保护安全技术方案



等级保护二、三级关键点

二级

技术方面

安全审计、边界完整性检查、入侵防范、资源控制以及通信保密性等控制点

网络安全

不仅要满足网络安全运行基本保障，同时还要考虑网络处理能力要满足业务极限时的需要

加强了网络边界的防护，增加了安全审计、边界完整性检查、入侵防范等控制点-

对网络设备的防护不仅局限于简单的身份鉴别，同时对标识和鉴别信息都有了相应的要求。

三级

是等级保护二级要求的扩展加强

三级要求主干链路冗余，设备性能有冗余

技术方面

网络恶意代码防范、剩余信息保护

如访山控制增加了对重要信对身份鉴别、访问控制、安全审计、数据完整性、数据保密性等均有更进一步的要求息资源设置敏感标记等

网络安全

-对网络处理能力增加了“优先级”考虑，保证重要主机能够在网络拥堵时仍能够正常运行

-网络边界的访问控制扩展到应用层，网络边界的其他防护措施进一步增强，不仅能够被动的“防”，还应能够主动发出一些动作，如报警阻断等，网路设备的防护要求两种身份鉴别技术综合使用

三级等级保护实施方案（通用）

三级系统安全保护环境基本要求与对应产品

使用范围	基本要求	产品类型举例
安全计算环境	网络结构（VLAN划分）	三层交换机（防火墙）MPLS VPN
	访问控制（权限分离）	主机核心加固系统
	入侵防范（检测告警）	主机入侵检测产品（HIDS）
	备份恢复（数据备份）	设备冗余、本地备份（介质场外存储）
	数据完整性、保密性	VPN设备
	剩余信息管理	终端综合管理系统
	身份认证（双因素）	证书、令牌、密保卡
	恶意代码防范（统一管理）	网络版主机防病毒软件
安全区域边界	区域边界访问控制（协议检测）	防火墙（IPS）
	资源控制（优先级控制）	带宽管理、流量控制设备
	区域边界入侵检测	IDS
	区域边界恶意代码防范	防病毒网关，沙箱
	区域边界完整性保护	终端综合管理系统
安全通信网络	通信网络安全审计	上网行为管理
	数据传输完整性、保密性保护	VPN设备
安全管理中心	系统管理	安全管理中心

三、新等级保护差异变化

新环境下等保的变革

等保2.0

国家标准GB/T 22239—2008《信息安全技术信息系统安全等级保护基本要求》在开展信息安全等级保护工作的过程中起到了非常重要的作用，被广泛应用于各个行业和领域开展信息安全等级保护的建设整改和等级测评等工作，但是随着信息技术的发展，GB/T 22239—2008在时效性、易用性、可操作性上需要进一步完善。

为了适应移动互联、云计算、大数据、物联网和工业控制等新技术、新应用情况下信息安全等级保护工作的开展，GB/T 22239—2019的思路和方法是针对移动互联、云计算、大数据、物联网和工业控制等新技术、新应用领域做出扩展的安全要求。

新等保系列目前主要有六个部分

GB/T 22239.1信息安全技术网络安全等级保护基本要求第1部分安全通用要求;

GB/T 22239.2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安全要求;

GB/T 22239.3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;

GB/T 22239.4 信息安全技术网络安全等级保护基本要求第4部分物联网安全扩展要求;

GB/T 22239.5信息安全技术网络安全等级保护基本要求第5部分工业控制安全扩展要求;

GB/T 22239.6信息安全技术网络安全等级保护基本要求第6部分大数据安全扩展要求;