doi :10.3969/j.issn.1671-1122.2019.02.010

《网络安全等级保护基本要求》（GB/T 22239–2019）标准解读

马力[1]，祝国邦[2]，陆磊[2]

（1. 公安部信息安全等级保护评估中心，北京 100142；2. 公安部网络安全保卫局，北京 100741）

摘　要：《网络安全等级保护基本要求》（GB/T 22239–2019）即将正式实施。文章介绍了《GB/T 22239–2019》的修订背景和进程、与《GB/T 22239–2008》比较发生的主要变化、其安全通用要求和安全扩展要求的主要内容等，目的使用户更好地了解和掌握《GB/T 22239–2019》的内容。

关键词：等级保护对象；安全通用要求；安全扩展要求

中图分类号：TP309　**文献标识码：**A　**文章编号：**1671-1122（2019）02-0077-08

中文引用格式：马力，祝国邦，陆磊 .《网络安全等级保护基本要求》（GB/T 22239-2019）标准解读 [J]. 信息网络安全，2019,19（2）:77–84.

英文引用格式：MA Li, ZHU Guobang, LU Lei. *Baseline for Classified Protection of Cybersecurity*(GB/T 22239-2019) Standard Interpretation[J].Netinfo Security, 2019, 19（2）:77–84.

Baseline for Classified Protection of Cybersecurity (GB/T 22239-2019) Standard Interpretation

MA Li[1], ZHU Guobang[2], LU Lei[2]

(1.*Information Classified Security Protection Evaluation Center of the Ministry of Public Security, Beijing* 100142, *China*; 2.*Cyber Security Department of the Ministry of Public Security, Beijing* 100741, *China*)

Abstract: *Baseline for Classified Protection of Cybersecurity*(GB/T 22239-2019) will be formally implemented soon. This paper introduces the background and process of the revision GB/T 22239-2019, the main changes in comparison with GB/T 22239-2008, the main contents of its security general requirements and security special requirements, etc., so as to enable users to better understand and master the contents of GB/T 22239-2019.

Key words: classified protection object; security general requirements; security special requirements

收稿日期：2019–1–15

作者简介：马力（1963—），男，江苏，副研究员，硕士，主要研究方向为信息技术、网络安全、等级保护；祝国邦（1979—），男，吉林，副研究员，硕士，主要研究方向为信息技术、网络安全、等级保护；陆磊（1976—），女，北京，本科，主要研究方向为信息技术、网络安全、等级保护。

通信作者：马力 mali@cspec.org.cn

0 引言

《信息安全技术 信息系统安全等级保护基本要求》（GB/T 22239-2008）在我国推行信息安全等级保护制度的过程中起到了非常重要的作用，被广泛用于各行业或领域，指导用户开展信息系统安全等级保护的建设整改、等级测评等工作[1]。随着信息技术的发展，已有 10 年历史的《GB/T 22239-2008》在时效性、易用性、可操作性上需要进一步完善。2017 年《中华人民共和国网络安全法》[2] 实施，为了配合国家落实网络安全等级保护制度[3]，也需要修订《GB/T 22239-2008》。

2014 年，全国信息安全标准化技术委员会（以下简称安标委）下达了对《GB/T 22239-2008》进行修订的任务。标准修订主要承担单位为公安部第三研究所（公安部信息安全等级保护评估中心），20 多家企事业单位派人员参与了标准的修订工作。标准编制组于 2014 年成立，先后调研了国际和国内云计算平台、大数据应用、移动互联接入、物联网和工业控制系统等新技术、新应用的使用情况，分析并总结了新技术和新应用中的安全关注点和安全控制要素，完成了基本要求草案第一稿。

2015 年 2 月至 2016 年 7 月，标准编制组在草案第一稿的基础上，广泛征求行业用户单位、安全服务机构和各行业 / 领域专家的意见，并按照意见调整和完善标准草案，先后共形成 7 个版本的标准草案。2016 年 9 月，标准编制组参加了安标委 WG5 工作组在研标准推进会，按照专家及成员单位提出的修改建议，对草案进行了修改，形成了标准征求意见稿。2017 年 4 月，标准编制组再次参加了安标委 WG5 工作组在研标准推进会，根据征求意见稿收集的修改建议，对征求意见稿进行了修改，形成了标准送审稿。2017 年 10 月，标准编制组又一次参加了安标委 WG5 工作组在研标准推进会，在会上介绍了送审稿内容，并征求成员单位意见，根据收集的修改建议，对送审稿进行了修改完善，形成了标准报批稿。

2019 年《信息安全技术 网络安全等级保护基本要求》（GB/T 22239-2019）将正式实施。本文分析《GB/T 22239-2019》相较《GB/T 22239-2008》发生的主要变化，解读其安全通用要求和安全扩展要求的主要内容，以便于读者更好地了解和掌握《GB/T 22239-2019》的内容。

1 总体结构的变化

1.1 主要变化内容

《GB/T 22239-2019》相较于《GB/T 22239-2008》，无论是在总体结构方面还是在细节内容方面均发生了变化[4]。在总体结构方面的主要变化为：

1）为适应网络安全法，配合落实网络安全等级保护制度，标准的名称由原来的《信息系统安全等级保护基本要求》改为《网络安全等级保护基本要求》。

2）等级保护对象由原来的信息系统调整为基础信息网络、信息系统（含采用移动互联技术的系统）、云计算平台 / 系统、大数据应用 / 平台 / 资源、物联网和工业控制系统等。

3）将原来各个级别的安全要求分为安全通用要求和安全扩展要求，安全扩展要求包括云计算安全扩展要求、移动互联安全扩展要求、物联网安全扩展要求以及工业控制系统安全扩展要求。安全通用要求是不管等级保护对象形态如何必须满足的要求；针对云计算、移动互联、物联网和工业控制系统提出的特殊要求称为安全扩展要求。

4）原来基本要求中各级技术要求的“物理安全”、“网络安全”、“主机安全”、“应用安全”和“数据安全和备份与恢复”修订为“安全物理环境”、“安全通信网络”、“安全区域边界”、“安全计算环境”和“安全管理中心”；原各级管理要求的“安全管理制度”、“安全管理机构”、“人员安全管理”、“系统建设管理”和“系统运维管理”修订为“安全管理制度”、“安全管理机构”、“安全管理人员”、“安全建设管理”和“安全运维管理”[5]。

5）云计算安全扩展要求针对云计算环境的特点提出。主要内容包括“基础设施的位置”、“虚拟化安全保护”、“镜像和快照保护”、“云计算环境管理”和“云

服务商选择”等。

6）移动互联安全扩展要求针对移动互联的特点提出。主要内容包括“无线接入点的物理位置”、“移动终端管控”、“移动应用管控”、“移动应用软件采购”和“移动应用软件开发”等。

7）物联网安全扩展要求针对物联网的特点提出。主要内容包括“感知节点的物理防护”、“感知节点设备安全”、“网关节点设备安全”、“感知节点的管理”和“数据融合处理”等。

8）工业控制系统安全扩展要求针对工业控制系统的特点提出。主要内容包括“室外控制设备防护”、“工业控制系统网络架构安全”、“拨号使用控制”、“无线使用控制”和“控制设备安全”等。

9）取消了原来安全控制点的 S、A、G 标注，增加附录 A“关于安全通用要求和安全扩展要求的选择和使用”，描述等级保护对象的定级结果和安全要求之间的关系，说明如何根据定级的 S、A 结果选择安全要求的相关条款，简化了标准正文部分的内容。

10）增加附录C描述等级保护安全框架和关键技术、附录 D 描述云计算应用场景、附录 E 描述移动互联应用场景、附录 F 描述物联网应用场景、附录 G 描述工业控制系统应用场景、附录 H 描述大数据应用场景[6, 7]。

1.2 变化的意义和作用

《GB/T 22239-2019》采用安全通用要求和安全扩展要求的划分使得标准的使用更加具有灵活性和针对性。不同等级保护对象由于采用的信息技术不同，所采用的保护措施也会不同。例如，传统的信息系统和云计算平台的保护措施有差异，云计算平台和工业控制系统的保护措施也有差异。为了体现不同对象的保护差异，《GB/T 22239-2019》将安全要求划分为安全通用要求和安全扩展要求。

安全通用要求针对共性化保护需求提出，无论等级保护对象以何种形式出现，需要根据安全保护等级实现相应级别的安全通用要求。安全扩展要求针对个性化保护需求提出，等级保护对象需要根据安全保护等级、使用的特定技术或特定的应用场景实现安全扩展要求。等级保护对象的安全保护措施需要同时实现安全通用要求和安全扩展要求，从而更加有效地保护等级保护对象。例如，传统的信息系统可能只需要采用安全通用要求提出的保护措施即可，而云计算平台不仅需要采用安全通用要求提出的保护措施，还要针对云计算平台的技术特点采用云计算安全扩展要求提出的保护措施；工业控制系统不仅需要采用安全通用要求提出的保护措施，还要针对工业控制系统的技术特点采用工业控制系统安全扩展要求提出的保护措施。

2 安全通用要求的内容

2.1 安全通用要求基本分类

《GB/T 22239-2019》规定了第一级到第四级等级保护对象的安全要求，每个级别的安全要求均由安全通用要求和安全扩展要求构成。例如，《GB/T 22239-2019》提出的第三级安全要求基本结构为：

8 第三级安全要求

8.1 安全通用要求

8.2 云计算安全扩展要求

8.3 移动互联安全扩展要求

8.4 物联网安全扩展要求

8.5 工业控制系统安全扩展要求

安全通用要求细分为技术要求和管理要求。其中技术要求包括“安全物理环境”、“安全通信网络”、“安全区域边界”、“安全计算环境”和“安全管理中心”；管理要求包括“安全管理制度”、“安全管理机构”、“安全管理人员”、“安全建设管理”和“安全运维管理”。两者合计 10 大类，如图 1 所示。

2.2 技术要求

技术要求分类体现了从外部到内部的纵深防御思想。对等级保护对象的安全防护应考虑从通信网络到区域边界再到计算环境的从外到内的整体防护，同时考虑对其所处的物理环境的安全防护。对级别较高的等级保护对象还需要考虑对分布在整个系统中的安全功能或安全组件的集中技术管理手段。

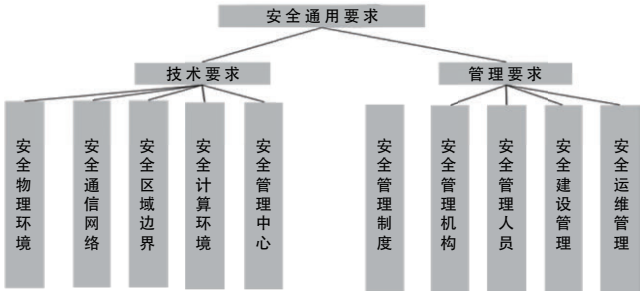

图 1 安全通用要求基本分类

1）安全物理环境

安全通用要求中的安全物理环境部分是针对物理机房提出的安全控制要求。主要对象为物理环境、物理设备和物理设施等；涉及的安全控制点包括物理位置的选择、物理访问控制、防盗窃和防破坏、防雷击、防火、防水和防潮、防静电、温湿度控制、电力供应和电磁防护。

表 1 给出了安全物理环境控制点 / 要求项的逐级变化。其中数字表示每个控制点下各个级别的要求项数量，级别越高，要求项越多。后续表中的数字均为此含义。

表 1 安全物理环境控制点 / 要求项的逐级变化

序号	控制点	一级	二级	三级	四级
1	物理位置的选择	0	2	2	2
2	物理访问控制	1	1	1	2
3	防盗窃和防破坏	1	2	3	3
4	防雷击	1	1	2	2
5	防火	1	2	3	3
6	防水和防潮	1	2	3	3
7	防静电	0	1	2	2
8	温湿度控制	1	1	1	1
9	电力供应	1	2	3	4
10	电磁防护	0	1	2	2

承载高级别系统的机房相对承载低级别系统的机房强化了物理访问控制、电力供应和电磁防护等方面的要求。例如，四级相比三级增设了“重要区域应配置第二道电子门禁系统”、“应提供应急供电设施”、“应对关键区域实施电磁屏蔽”等要求。

2）安全通信网络

安全通用要求中的安全通信网络部分是针对通信网络提出的安全控制要求。主要对象为广域网、城域网和局域网等；涉及的安全控制点包括网络架构、通信传输和可信验证。

表 2 给出了安全通信网络控制点 / 要求项的逐级变化。

表 2 安全通信网络控制点 / 要求项的逐级变化

序号	控制点	一级	二级	三级	四级
1	网络架构	0	2	5	6
2	通信传输	1	1	2	4
3	可信验证	1	1	1	1

高级别系统的通信网络相对低级别系统的通信网络强化了优先带宽分配、设备接入认证、通信设备认证等方面的要求。例如，四级相比三级增设了“应可按照业务服务的重要程度分配带宽，优先保障重要业务”，“应采用可信验证机制对接入网络中的设备进行可信验证，保证接入网络的设备真实可信”，“应在通信前基于密码技术对通信双方进行验证或认证”等要求。

3）安全区域边界

安全通用要求中的安全区域边界部分是针对网络边界提出的安全控制要求。主要对象为系统边界和区域边界等；涉及的安全控制点包括边界防护、访问控制、入侵防范、恶意代码防范、安全审计和可信验证。

表 3 给出了安全区域边界控制点 / 要求项的逐级变化。

表 3 安全区域边界控制点 / 要求项的逐级变化

序号	控制点	一级	二级	三级	四级
1	边界防护	1	1	4	6
2	访问控制	3	4	5	5
3	入侵防范	0	1	4	4
4	恶意代码防范	0	1	2	2
5	安全审计	0	3	4	3
6	可信验证	1	1	1	1

高级别系统的网络边界相对低级别系统的网络边界强化了高强度隔离和非法接入阻断等方面的要求。例如，四级相比三级增设了“应在网络边界通过通信协议转换或通信协议隔离等方式进行数据交换”，“应能够在发现非授权设备私自联到内部网络的行为或内部用户非授权联到外部网络的行为时，对其进行有效阻断”等要求。

4）安全计算环境

安全通用要求中的安全计算环境部分是针对边界

内部提出的安全控制要求。主要对象为边界内部的所有对象，包括网络设备、安全设备、服务器设备、终端设备、应用系统、数据对象和其他设备等；涉及的安全控制点包括身份鉴别、访问控制、安全审计、入侵防范、恶意代码防范、可信验证、数据完整性、数据保密性、数据备份与恢复、剩余信息保护和个人信息保护。

表 4 给出了安全计算环境控制点 / 要求项的逐级变化。

表 4 安全计算环境控制点 / 要求项的逐级变化

序号	控制点	一级	二级	三级	四级
1	身份鉴别	2	3	4	4
2	访问控制	3	4	7	7
3	安全审计	0	3	4	4
4	入侵防范	2	5	6	6
5	恶意代码防范	1	1	1	1
6	可信验证	1	1	1	1
7	数据完整性	1	1	2	3
8	数据保密性	0	0	2	2
9	数据备份与恢复	1	2	3	4
10	剩余信息保护	0	1	2	2
11	个人信息保护	0	2	2	2

高级别系统的计算环境相对低级别系统的计算环境强化了身份鉴别、访问控制和程序完整性等方面的要求。例如，四级相比三级增设了“应采用口令、密码技术、生物技术等两种或两种以上组合的鉴别技术对用户进行身份鉴别，且其中一种鉴别技术至少应使用密码技术来实现”，“应对主体、客体设置安全标记，并依据安全标记和强制访问控制规则确定主体对客体的访问”，“应采用主动免疫可信验证机制及时识别入侵和病毒行为，并将其有效阻断”等要求。

5）安全管理中心

安全通用要求中的安全管理中心部分是针对整个系统提出的安全管理方面的技术控制要求，通过技术手段实现集中管理。涉及的安全控制点包括系统管理、审计管理、安全管理和集中管控。

表 5 给出了安全管理中心控制点 / 要求项的逐级变化。

高级别系统的安全管理相对低级别系统的安全管理强化了采用技术手段进行集中管控等方面的要求。

表 5 安全管理中心控制点 / 要求项的逐级变化

序号	控制点	一级	二级	三级	四级
1	系统管理	2	2	2	2
2	审计管理	2	2	2	2
3	安全管理	0	2	2	2
4	集中管控	0	0	6	7

例如，三级相比二级增设了“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”，“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”，“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，并保证审计记录的留存时间符合法律法规要求”，“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”等要求。

2.3 管理要求

管理要求分类体现了从要素到活动的综合管理思想。安全管理需要的“机构”、“制度”和“人员”三要素缺一不可，同时还应对系统建设整改过程中和运行维护过程中的重要活动实施控制和管理。对级别较高的等级保护对象需要构建完备的安全管理体系。

1）安全管理制度

安全通用要求中的安全管理制度部分是针对整个管理制度体系提出的安全控制要求，涉及的安全控制点包括安全策略、管理制度、制定和发布以及评审和修订。

表 6 给出了安全管理制度控制点 / 要求项的逐级变化。

表 6 安全管理制度控制点 / 要求项的逐级变化

序号	控制点	一级	二级	三级	四级
1	安全策略	0	1	1	1
2	管理制度	1	2	3	3
3	制定和发布	0	2	2	2
4	评审和修订	0	1	1	1

2）安全管理机构

安全通用要求中的安全管理机构部分是针对整个管理组织架构提出的安全控制要求，涉及的安全控制点包括岗位设置、人员配备、授权和审批、沟通和合作以及审核和检查。

表 7 给出了安全管理机构控制点 / 要求项的逐级

变化。

表 7 安全管理机构控制点 / 要求项的逐级变化

序号	控制点	一级	二级	三级	四级
1	岗位设置	1	2	3	3
2	人员配备	1	1	2	3
3	授权和审批	1	2	3	3
4	沟通和合作	0	3	3	3
5	审核和检查	0	1	3	3

3）安全管理人员

安全通用要求中的安全管理人员部分是针对人员管理模式提出的安全控制要求，涉及的安全控制点包括人员录用、人员离岗、安全意识教育和培训以及外部人员访问管理。

表 8 给出了安全管理人员控制点 / 要求项的逐级变化。

表 8 安全管理人员控制点 / 要求项的逐级变化

序号	控制点	一级	二级	三级	四级
1	人员录用	1	2	3	4
2	人员离岗	1	1	2	2
3	安全意识教育和培训	1	1	3	3
4	外部人员访问管理	1	3	4	5

4）安全建设管理

安全通用要求中的安全建设管理部分是针对安全建设过程提出的安全控制要求，涉及的安全控制点包括定级和备案、安全方案设计、安全产品采购和使用、自行软件开发、外包软件开发、工程实施、测试验收、系统交付、等级测评和服务供应商管理。

表 9 给出了安全建设管理控制点 / 要求项的逐级变化。

表 9 安全建设管理控制点 / 要求项的逐级变化

序号	控制点	一级	二级	三级	四级
1	定级和备案	1	4	4	4
2	安全方案设计	1	3	3	3
3	安全产品采购和使用	1	2	3	4
4	自行软件开发	0	2	7	7
5	外包软件开发	0	2	3	3
6	工程实施	1	2	3	3
7	测试验收	1	2	2	2
8	系统交付	2	3	3	3
9	等级测评	0	3	3	3
10	服务供应商管理	2	2	3	3

5）安全运维管理

安全通用要求中的安全运维管理部分是针对安全运维过程提出的安全控制要求，涉及的安全控制点包括环境管理、资产管理、介质管理、设备维护管理、漏洞和风险管理、网络和系统安全管理、恶意代码防范管理、配置管理、密码管理、变更管理、备份与恢复管理、安全事件处置、应急预案管理和外包运维管理。

表 10 给出了安全运维管理控制点 / 要求项的逐级变化。

表 10 安全运维管理控制点 / 要求项的逐级变化

序号	控制点	一级	二级	三级	四级
1	环境管理	2	3	3	4
2	资产管理	0	1	3	3
3	介质管理	1	2	2	2
4	设备维护管理	1	2	4	4
5	漏洞和风险管理	1	1	2	2
6	网络和系统安全管理	2	5	10	10
7	恶意代码防范管理	2	3	2	2
8	配置管理	0	1	2	2
9	密码管理	0	2	2	3
10	变更管理	0	1	3	3
11	备份与恢复管理	2	3	3	3
12	安全事件处置	2	3	4	5
13	应急预案管理	0	2	4	5
14	外包运维管理	0	2	4	4

3 安全扩展要求的内容

安全扩展要求是采用特定技术或特定应用场景下的等级保护对象需要增加实现的安全要求。《GB/T 22239-2019》提出的安全扩展要求包括云计算安全扩展要求、移动互联安全扩展要求、物联网安全扩展要求和工业控制系统安全扩展要求。

3.1 云计算安全扩展要求

采用了云计算技术的信息系统通常称为云计算平台。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。云计算平台中通常有云服务商和云服务客户 / 云租户两种角色。根据云服务商所提供服务的类型，云计算平台有软件即服务（SaaS）、平台即服务（PaaS）、基础设施即服务（IaaS）3 种基本的云计算服务模式。在不同的服务模式中，云服务商和云服务客户对资源拥有不同的控制范围，控制范围决定了安全责任的边界。

云计算安全扩展要求是针对云计算平台提出的安全通用要求之外额外需要实现的安全要求。云计算安全扩展要求涉及的控制点包括基础设施位置、网络架

构、网络边界的访问控制、网络边界的入侵防范、网络边界的安全审计、集中管控、计算环境的身份鉴别、计算环境的访问控制、计算环境的入侵防范、镜像和快照保护、数据安全性、数据备份恢复、剩余信息保护、云服务商选择、供应链管理和云计算环境管理。

表 11 给出了云计算安全扩展要求控制点 / 要求项的逐级变化。

表 11 云计算安全扩展要求控制点 / 要求项的逐级变化

序号	控制点	一级	二级	三级	四级
1	基础设施位置	1	1	1	1
2	网络架构	2	3	5	8
3	网络边界的访问控制	1	2	2	2
4	网络边界的入侵防范	0	3	4	4
5	网络边界的安全审计	0	2	2	2
6	集中管控	0	0	4	4
7	计算环境的身份鉴别	0	0	1	1
8	计算环境的访问控制	2	2	2	2
9	计算环境的入侵防范	0	0	3	3
10	镜像和快照保护	0	2	3	3
11	数据安全性	1	3	4	4
12	数据备份恢复	0	2	4	4
13	剩余信息保护	0	2	2	2
14	云服务商选择	3	4	5	5
15	供应链管理	1	2	3	3
16	云计算环境管理	0	1	1	1

3.2 移动互联安全扩展要求

采用移动互联技术的等级保护对象，其移动互联部分通常由移动终端、移动应用和无线网络 3 部分组成。移动终端通过无线通道连接无线接入设备接入有线网络；无线接入网关通过访问控制策略限制移动终端的访问行为；后台的移动终端管理系统（如果配置）负责对移动终端的管理，包括向客户端软件发送移动设备管理、移动应用管理和移动内容管理策略等。

移动互联安全扩展要求是针对移动终端、移动应用和无线网络提出的特殊安全要求，它们与安全通用要求一起构成针对采用移动互联技术的等级保护对象的完整安全要求。移动互联安全扩展要求涉及的控制点包括无线接入点的物理位置、无线和有线网络之间的边界防护、无线和有线网络之间的访问控制、无线和有线网络之间的入侵防范，移动终端管控、移动应用管控、移动应用软件采购、移动应用软件开发和配置管理。

表 12 给出了移动互联安全扩展要求控制点 / 要求项的逐级变化。

表 12 移动互联安全扩展要求控制点 / 要求项的逐级变化

序号	控制点	一级	二级	三级	四级
1	无线接入点的物理位置	1	1	1	1
2	无线和有线网络之间的边界防护	1	1	1	1
3	无线和有线网络之间的访问控制	1	1	1	1
4	无线和有线网络之间的入侵防范	0	5	6	6
5	移动终端管控	0	0	2	3
6	移动应用管控	1	2	3	4
7	移动应用软件采购	1	2	2	2
8	移动应用软件开发	0	2	2	2
9	配置管理	0	0	1	1

3.3 物联网安全扩展要求

物联网从架构上通常可分为 3 个逻辑层，即感知层、网络传输层和处理应用层。其中感知层包括传感器节点和传感网网关节点或 RFID 标签和 RFID 读写器，也包括感知设备与传感网网关之间、RFID 标签与 RFID 读写器之间的短距离通信（通常为无线）部分；网络传输层包括将感知数据远距离传输到处理中心的网络，如互联网、移动网或几种不同网络的融合；处理应用层包括对感知数据进行存储与智能处理的平台，并对业务应用终端提供服务。对大型物联网来说，处理应用层一般由云计算平台和业务应用终端构成。

对物联网的安全防护应包括感知层、网络传输层和处理应用层。由于网络传输层和处理应用层通常由计算机设备构成，因此这两部分按照安全通用要求提出的要求进行保护。物联网安全扩展要求是针对感知层提出的特殊安全要求，它们与安全通用要求一起构成针对物联网的完整安全要求。

物联网安全扩展要求涉及的控制点包括感知节点的物理防护、感知网的入侵防范、感知网的接入控制、感知节点设备安全、网关节点设备安全、抗数据重放、数据融合处理和感知节点的管理。

表 13 给出了物联网安全扩展要求控制点 / 要求项的逐级变化。

3.4 工业控制系统安全扩展要求

工业控制系统通常是可用性要求较高的等级保护对象。工业控制系统是各种控制系统的总称，典型的

表 13 物联网安全扩展要求控制点 / 要求项的逐级变化

序号	控制点	一级	二级	三级	四级
1	感知节点的物理防护	2	2	4	4
2	感知网的入侵防范	0	2	2	2
3	感知网的接入控制	1	1	1	1
4	感知节点设备安全	0	0	3	3
5	网关节点设备安全	0	0	4	4
6	抗数据重放	0	0	2	2
7	数据融合处理	0	0	1	2
8	感知节点的管理	1	2	3	3

如数据采集与监视控制系统（SCADA）、集散控制系统（DCS）等。工业控制系统通常用于电力，水和污水处理，石油和天然气，化工，交通运输，制药，纸浆和造纸，食品和饮料以及离散制造（如汽车、航空航天和耐用品）等行业。

工业控制系统从上到下一般分为 5 个层级，依次为企业资源层、生产管理层、过程监控层、现场控制层和现场设备层，不同层级的实时性要求有所不同，对工业控制系统的安全防护应包括各个层级。由于企业资源层、生产管理层和过程监控层通常由计算机设备构成，因此这些层级按照安全通用要求提出的要求进行保护。

工业控制系统安全扩展要求是针对现场控制层和现场设备层提出的特殊安全要求，它们与安全通用要求一起构成针对工业控制系统的完整安全要求。工业控制系统安全扩展要求涉及的控制点包括室外控制设备防护、网络架构、通信传输、访问控制、拨号使用控制、无线使用控制、控制设备安全、产品采购和使用以及外包软件开发。

表 14 给出了工业控制系统安全扩展要求控制点 / 要求项的逐级变化。

表 14 工业控制系统安全扩展要求控制点 / 要求项的逐级变化

序号	控制点	一级	二级	三级	四级
1	室外控制设备防护	2	2	2	2
2	网络架构	2	3	3	3
3	通信传输	0	1	1	1
4	访问控制	1	2	2	2
5	拨号使用控制	0	1	2	3
6	无线使用控制	2	2	4	4
7	控制设备安全	2	2	5	5
8	产品采购和使用	0	1	1	1
9	外包软件开发	0	1	1	1

4 结束语

《GB/T 22239-2019》在结构上和内容上相较于《GB/T 22239-2008》均发生了较大变化，这些变化给网络安全等级保护的建设整改、等级测评等工作均带来了一定的影响。如何基于新标准形成安全解决方案，如何基于新标准开展等级保护测评等，都需要仔细研读新标准，基于新标准找到开展网络安全等级保护工作的新思路和新方法。（责编 马珂）

参考文献：

[1] QU Jie, FAN Chunling, CHEN Guangyong, et al. Research on Establishment of Network Security Service Ability System for A New Era[J].Netinfo Security,2019,19(1):83-87.
曲洁，范春玲，陈广勇，等. 新时代下网络安全服务能力体系建设思路 [J]. 信息网络安全，2019,19（1）：83-87.
[2] Cybersecurity Law of the People's Republic of China [EB/OL]. http://www.npc.gov.cn/npc/, 2016-11-7.
中华人民共和国网络安全法 [EB/OL].http://www.npc.gov.cn/npc/, 2016-11-7.
[3] JI Hui. Controlling Information System Risk by Information Security Service[J]. Netinfo Security,2010,10(5):17-18.
季辉. 通过信息安全服务实现信息系统风险可控 [J]. 信息网络安全，2010，10（5）:17-18.
[4] GUO Qiquan, et al. Training Course on Cybersecurity Law and Classified Protection of Cybersecurity[M].Beijing: Publishing House of Electronics Industry,2018.
郭启全，等. 网络安全法与网络安全等级保护制度培训教程 [M]. 北京：电子工业出版社，2018.
[5] GB/T 22239-2008.Information Security Technology-Baseline for Classified Protection of Information System Security[S]. Beijing: Standards Press of China,2008.
GB/T 22239-2008.信息安全技术 信息系统安全等级保护基本要求 [S]. 北京：中国标准出版社，2008.
[6] National Information Security Standardization Technical Committee. Information Security Technology—Baseline for Classified Protection of Cybersecurity(Draft)[EB/OL]. https://www.tc260.org.cn/,2018-10-31.
全国信息安全标准化技术委员会. 信息安全技术 网络安全等级保护基本要求（征求意见稿）[EB/OL]. https://www.tc260.org.cn/,2018-10-31.
[7] National Information Security Standardization Technical Committee. Information Security Technology—Evaluation Requirement for Classified Protection of Cybersecurity(Draft)[EB/OL]. https://www.tc260.org.cn/,2018-10-31.
全国信息安全标准化技术委员会. 信息安全技术 网络安全等级保护测评要求（征求意见稿）[EB/OL]. https://www.tc260.org.cn/,2018-10-31.