网络安全等级保护2.0要求

王昱镔

公安部第一研究所
THE FIRST RESEARCH INSTITUTE OF THE MINISTRY OF PUBLIC SECURITY OF P.R.C.

目 录

提纲

网络安全等级保护的基本含义

- 对等级保护对象分等级进行安全保护和监管。
- 对网络安全产品的使用实行分等级管理。
- 对网络安全事件实行分等级响应、处置。

网络安全等级保护的工作内涵

将全国的**等级保护对象**按照重要性和受破坏后的危害性分成**五个安全保护等级**（从第一级到第五级逐级增高），定级后第二级以上系统到公安机关备案，公安机关审核合格后颁发备案证明；各单位各部门根据系统等级按照国家标准进行安全建设整改，建设安全设施、落实安全措施、落实安全责任、建立和落实安全管理制度等；聘请测评机构进行安全技术测评；公安机关定期开展监督、检查。

一 网络安全等级保护发展历程

等级保护制度发展历程

网络安全等级保护是国家信息安全保障的基本制度、基本策略、基本方法。开展网络安全等级保护工作是保护信息化发展、维护网络安全的根本保障，是网络安全保障工作中国家意志的体现。

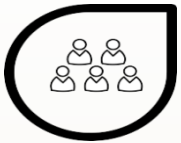
一 网络安全等级保护发展历程

标准体系历程-2014年之后

云计算

移动互联

新技术新应用涌现



大数据

物联网

工业控制系统

标准体系历程-2014年之后

- 等级保护进入2.0时代，根据信息技术发展应用和网络安全态势，不断深入研究、拓展保护范围，逐步健全网络安全等级保护标准体系。
- 公安部自2014年4月开始组织了30余家企事业单位开展云计算、移动互联、物联网、工业控制、大数据等领域的技术研究。
- 2015年初，标委会批准立项。
- 2015年中，标委会批准设计要求修订立项。
- 2016年10月形成征求意见稿。

标准体系历程-2014年之后

- 2017年4月，标委会批准定级指南立项。
- 2017年4月，已立项标准征求意见稿经信安标委会工作组成员单位投票通过，成为送审稿。
- 2017年12月，已立项标准成为报批稿。
- 2019年5月，等保2.0宣贯会召开。

网络安全等级保护2.0-主要标准

- 网络安全等级保护条例（总要求/上位文件）
- 计算机信息系统安全保护等级划分准则（GB 17859-1999）（上位标准）
- 网络安全等级保护实施指南（GB/T25058-2019）
- 网络安全等级保护定级指南（GB/T22240-2020）
- 网络安全等级保护基本要求（GB/T22239-2019）
- 网络安全等级保护设计技术要求（GB/T25070-2019）
- 网络安全等级保护测评要求（GB/T28448-2019）
- 网络安全等级保护测评过程指南（GB/T28449-2018）

等级保护制度发展展望

国家网络安全等级保护制度（基本制度、基本国策，上升为法律）

- 《信息安全等级保护管理办法》从部门规章提升为法律要求。
- 公安部正会同中央网信办、国家保密局、国家密码管理局起草《网络安全等级保护条例》，构造全新的等级保护基本制度体系。
- 目前《网络安全等级保护条例》已经四部委达成一致，报国务院立法部门，拟于年内出台。

二 网络安全等级保护2.0特点

特点1-对象范围扩大

新标准将云计算、移动互联、物联网、工业控制系统等列入标准范围，构成了“安全通用要求+新型应用安全扩展要求”的要求内容

安全通用要求和安全扩展要求的使用场合

- 安全通用要求针对**共性化保护需求**提出，等级保护对象**无论以何种形式出现**，必须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，需要根据安全保护等级和使用的特定技术或特定的**应用场景实现安全扩展要求**。

特点2-分类结构统一

新标准“基本要求、设计要求和测评要求” 分类框架统一，

形成了“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” 支持下的三重防护体系架构

特点3-强化可信计算

新标准强化了可信计算技术使用的要求，把可信验证列入各个级别并逐级提出各个环节的主要可信验证要求

特点4-强化供应链安全，产品和技术网络安全审查

新标准强化对提供网络设计、建设、运维和技术服务的

机构和人员进行安全管理。

特点5-强化安全保护技术措施的落实

新标准强化报送网络安全监测预警信息，报告网络安全案事件。

特点6-强化网络安全监测预警和信息通报工作

新标准变被动防护为主动防护，变静态防护为动态防护，

变单点防护为整体防控，变粗放防护为精准防护。

特点7-强化应急演练和应急处置

新标准强化应急演练和应急处置，加强网络安全协同应急处置。

特点8-强化重要数据和个人信息安全保护要求

新标准采取保护措施，保障数据和信息在收集、存储、

传输、使用、提供、销毁过程中的安全 。

定级

① 定级含义

根据信息、信息系统的重要程度和信息系统遭到破环后对国家安全、社会秩序、公共利益以 及公民、法人和其他组织的合法权益的危害程度，确定信息系统的安全保护等级。系统定级过程实质上是对国家重要信息资产的识别过程。

3.1

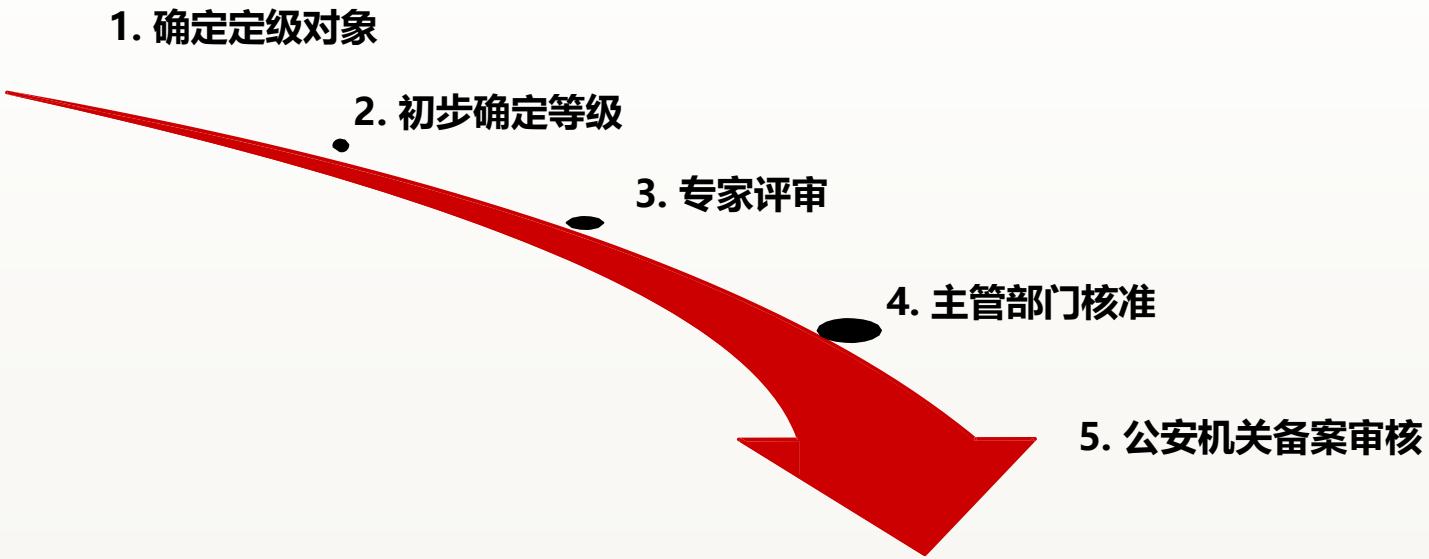
等级保护对象 target of classified security

信息安全等级保护工作直接作用的具体的信息和信息系统。

等级保护对象（修订）

网络安全等级保护工作直接作用的对象， 包括信息系统、通信网络设施和数据资源等。

关键环节



1确定定级对象

定级对象的类型

网络/平台类	信息系统类	数据类 大
电信网	计算机信息系统	数据 数字
广播电视网	工业控制系统	资产 数据
互联网行业专网	移动互联系统	资源
云计算服务平台	物联网系统	
大数据服务平台		
服务	信息和服务	信息

云计算相关定级对象

云租户 → 采用云服务的业务系统单独定级

云服务商 → 云计算平台通常单独定级

云服务商 → 较大规模的云计算平台可以依据功能或服务划分为多个定级对象。

第二讲 定级关键环节

物联网

物联网主要包括**感知、网络传输和处理应用**等特征要素，应将以上要素**作为一个整体**对象定级，各要素不单独定级。

移动互联系统

采用移动互联技术的信息系统主要包括**移动终端、移动应用、无线网络**等特征要素，可作为一个整体独立定级或与有线网络一起定级，各要素不应单独定级。

三 定级指南解读

工控

现场采集/执行、现场控制和过程控制等要素**应作为一个整体对象定级**，各要素不单独定级；生产管理要素可单独定级。

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

大数据

应将具有单一安全责任单位的大数据作为**一个整体对象定级**。

三 定级指南解读

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（含二级）**。

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核准**。

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核。

三 定级指南解读

	等保1.0	等保2.0
名称	信息系统安全等级保护	网络安全等级保护
顶层文件	《中华人民共和国计算机信息系统安全保护条例》行政法规	《中华人民共和国网络安全法》 《中华人民共和国保守国家秘密法》法律
核心文件	《信息安全等级保护管理办法》部门规范性文件	《网络安全等级保护条例》行政法规
对象	信息和信息系统	等级保护对象（信息系统、通信网络设施和数据资源等）
安全要求	安全基本要求	安全通用要求+安全扩展要求
定级原则	自主定级、自主保护、监督指导	明确等级、增强保护、常态监督
定级流程	直接根据定级要素与安全等级关系定级	确定定级对象、拟定等级、专家评审、主管部门审核、公安机关备案审查
定级对象基本特征	具有唯一确定的安全责任单位；具有信息系统的基本要求；承载单一或相对独立的业务应用	具有确定的主要安全责任主体;承载相对独立的业务应用;包含相互关联的多个资源
备案时限	等级确定或新建系统投入使用30日内	等级确定后10个工作日内

《基本要求》的定位

- 是系统安全保护、等级测评的一个基本“标尺”，同样级别的系统使用统一的“标尺”来衡量，保证权威性，是一个达标线；
- 每个级别的信息系统按照基本要求进行保护后，信息系统具有相应等级的基本安全保护能力，达到一种基本的安全状态；
- 是每个级别信息系统进行安全保护工作的一个基本出发点，更加贴切的保护可以通过需求分析对基本要求进行补充，参考其他有关等级保护或安全方面的标准来实现。

1.分类结构的变化

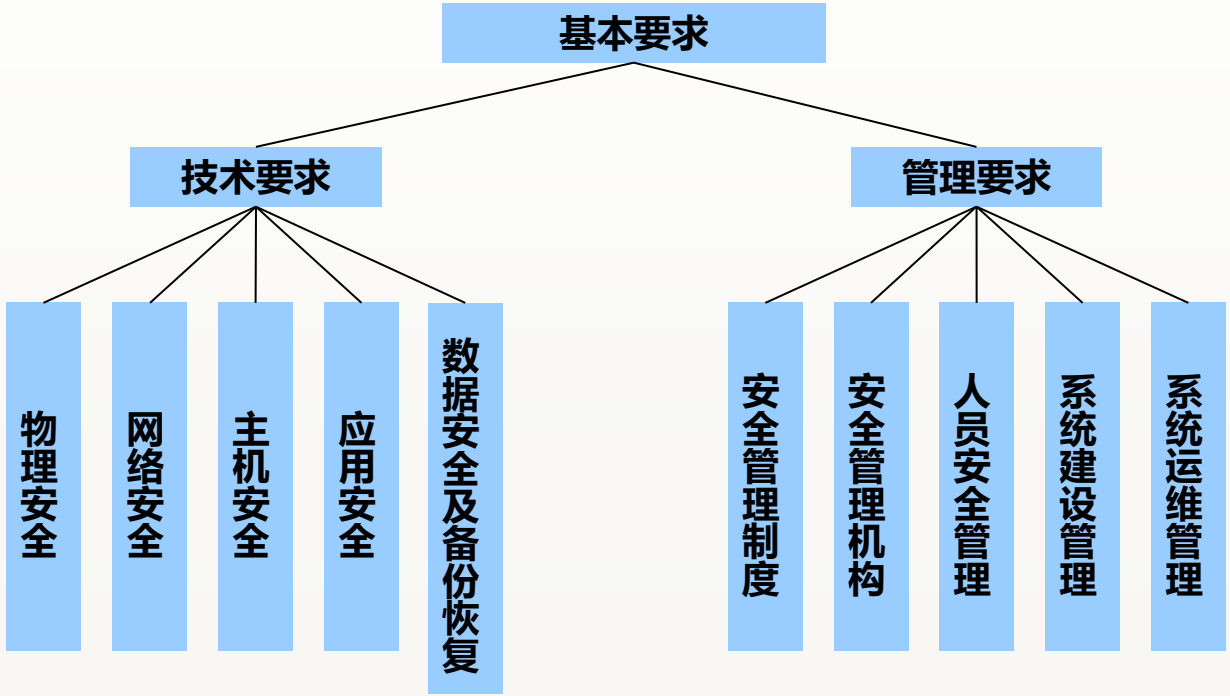
- 技术部分：

  □安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心

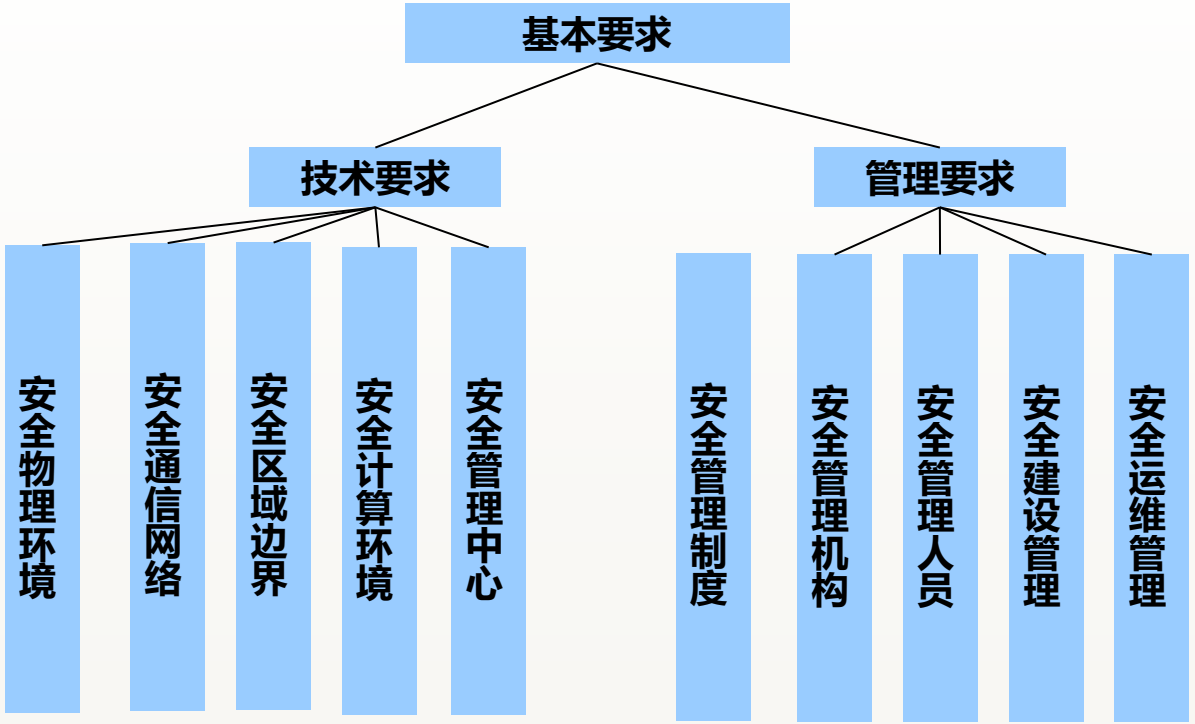
- 管理部分：

  □安全管理制度、安全管理机构、安全管理人员、安全建设管理、安全运维管理

基本要求文档结构（1.0）


基本要求
技术要求
管理要求
物理安全
网络安全
主机安全
应用安全
数据安全及备份恢复
安全管理制度
安全管理机构
人员安全管理
系统建设管理
系统运维管理

基本要求文档结构（2.0）


基本要求
技术要求
管理要求
安全物理环境
安全通信网络
安全区域边界
安全计算环境
安全管理中心
安全管理制度
安全管理机构
安全管理人员
安全建设管理
安全运维管理

2.增加了云计算安全扩展要求

- 云计算安全扩展要求章节针对云计算的特点提出特殊保护要求。

  对云计算环境主要增加的内容包括“基础设施的位置”、“虚拟化安全保护”、“镜像和快照保护”、“云服务商选择”和“云计算环境管理”等方面。

云计算安全扩展要求的主要思想

- 云计算平台（采用云计算技术的系统）**自身安全防护要求**
- 云计算平台**向其上租户系统**提供安全防护的能力要求

云计算安全扩展要求-一些原则性要求

- 应保证云计算平台**不承载高于其安全保护等级**的业务应用系统
- 应保证云计算**基础设施位于中国境内**
- 云计算平台的**运维地点应位于中国境内**，境外对境内云计算平台实施运维操作应遵循国家相关规定

3.增加了移动互联安全扩展要求

- 移动互联安全扩展要求章节针对移动互联的特点提出特殊保护要求。对移动互联环境主要增加的内容包括“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”等方面。

移动互联安全扩展要求使用要点

- 针对采用移动互联技术的等级保护对象其**移动互联部分**提出特殊保护要求。移动互联部分通 常由**移动终端、移动应用和无线网络**三部分组成。

4.增加了物联网安全扩展要求

- 物联网安全扩展要求章节针对物联网的特点提出特殊保护要求。

  对物联网环境主要增加的内容包括“感知节点的物理防护”、“感知节点设备安全”、“感知网关节点设备安全”、“感知节点的管理”和“数据融合处理”等方面。

物联网安全扩展要求使用要点

- 物联网系统通常从架构上可分为三个逻辑层，即感知层、网络传输层和处理应用层。物联网安全扩展要求 **针对感知层部分**提出特殊保护要求，**网络传输层和处 理应用层使用安全通用要求条款**

5.增加了工业控制系统安全扩展要求

- 工业控制系统安全扩展要求章节针对工业控制系统的特点提出特殊保护要求。对工业控制系统主要增加的内容包括“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”等方面。

工业控制系统安全扩展要求使用要点

- 工业控制系统安全扩展要求主要针对现场控制层和现场设备层提出特殊安全要求，其他层次使用安全通用要求条款
- 对工业控制系统的保护需要根据实际情况使用基本要求，具体安全通用要求和安全扩展要求的使用方法比较复杂。

6.增加了应用场景的说明

- 增加附录C 描述等级保护安全框架和关键技术 ，增加附录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（安全扩展要求）。

关于“可信验证控制点”

- 从一级到四级均在“安全通信网络”、“安全区域边界”和“安全计算环境”中**增加了“可信验证”控制点**。

关于“安全管理中心”

□从二级以上在技术上开始增加了“安全管理中心”要求。

二级需要有“系统管理”和“审计管理”；三级以上需要有完整的“系统管理”、“审计管理”和“安全管理”，并且实现“集中管控”。

测评结论-2.0

优

- 被测对象中存在安全问题，但不会导致被测对象面临中、高等级安全风险，且系统综合得分90分以上（含90分）。

良

- 被测对象中存在安全问题，但不会导致被测对象面临高等级安全风险，且系统综合得分80分以上（含80分）。

中

- 被测对象中存在安全问题，但不会导致被测对象面临高等级安全风险，且系统综合得分70分以上（含70分）。

差

- 被测对象中存在安全问题，而且会导致被测对象面临高等级安全风险，或被测对象综合得分低于70分。

敬请批评指正！