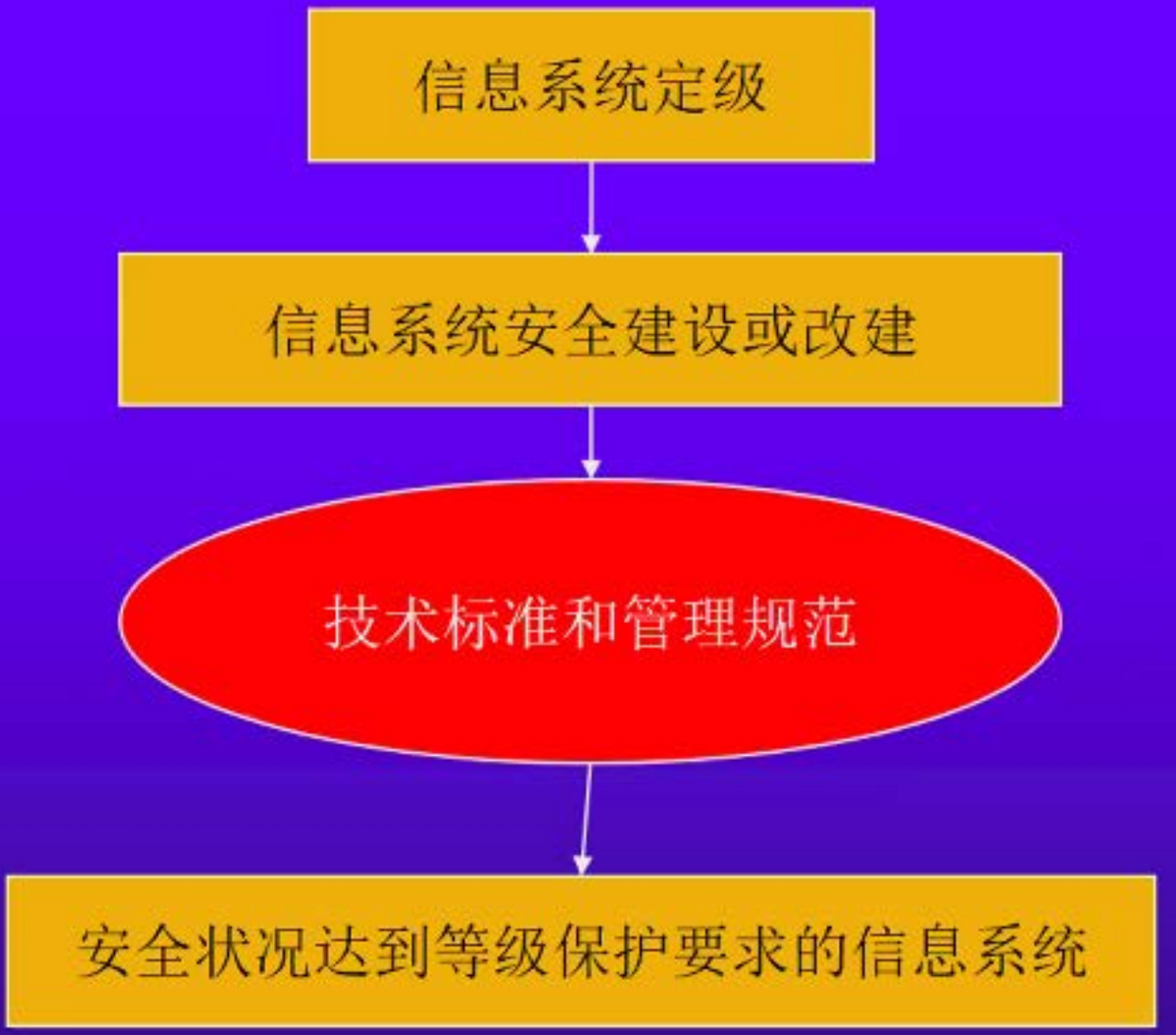
中华人民共和国网络安全法

- 第二十一条 国家实行网络安全等级保护制度。网络运营者应当按照网络安全等级保护制度的要求，履行下列安全保护义务，保障网络免受干扰、破坏或者未经授权的访问，防止网络数据泄露或者被窃取、篡改：
  - （一）制定内部安全管理制度和操作规程，确定网络安全负责人，落实网络安全保护责任；
  - （二）采取防范计算机病毒和网络攻击、网络侵入等危害网络安全行为的技术措施；
  - （三）采取监测、记录网络运行状态、网络安全事件的技术措施，并按照规定留存相关的网络日志不少于六个月；
  - （四）采取数据分类、重要数据备份和加密等措施；
  - （五）法律、行政法规规定的其他义务。

《管理办法》”等级划分和保护“第八条

- 信息系统运营、使用单位依据本办法和相关技术标准对信息系统进行保护，国家有关信息安全职能部门对其信息安全等级保护工作进行监督管理。

技术标准和管理规范的作用



整体要求的管理规范和技术标准

- 《信息安全等级保护管理办法》
- 《计算机信息系统安全保护等级划分准则》（GB17859-1999）
- 《信息系统安全等级保护实施指南》
- 《信息系统安全保护等级定级指南》
- 《信息系统安全等级保护基本要求》
- 《信息系统安全等级保护测评要求》
- 等等

《基本要求》的作用

信息系统安全等级保护基本要求

运营、使用单位
（安全服务商）

主管部门
（等级测评机构）

安全保护

测评检查

《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；

《基本要求》的定位

《基本要求》的定位

基本要求

保护

某级信息系统

基本保护

特殊需求
补充措施

基本保护

测评

基本要求

补充的安全措施
GB17859-1999
通用技术要求
安全管理要求
高级别的基本要求
等级保护其他标准
安全方面相关标准
等等

《基本要求》基本思路

不同级别信息系统

重要程度不同

应对不同威胁的能力(威胁\弱点)

具有不同的安全保护能力

不同的基本要求

不同级别的安全保护能力要求

- 第一级安全保护能力
  - 应能够防护系统免受来自个人的、拥有很少资源（如利用公开可获取的工具等）的威胁源发起的恶意攻击、一般的自然灾难（灾难发生的强度弱、持续时间很短等）以及其他相当危害程度的威胁（无意失误、技术故障等）所造成的关键资源损害，在系统遭到损害后，能够恢复部分功能。
- 第二级安全保护能力
  - 应能够防护系统免受来自外部小型组织的（如自发的三两人组成的黑客组织）、拥有少量资源（如个别人员能力、公开可获或特定开发的工具等）的威胁源发起的恶意攻击、一般的自然灾难（灾难发生的强度一般、持续时间短、覆盖范围小等）以及其他相当危害程度的威胁（无意失误、技术故障等）所造成的重要资源损害，能够发现重要的安全漏洞和安全事件，在系统遭到损害后，能够在一段时间内恢复部分功能。

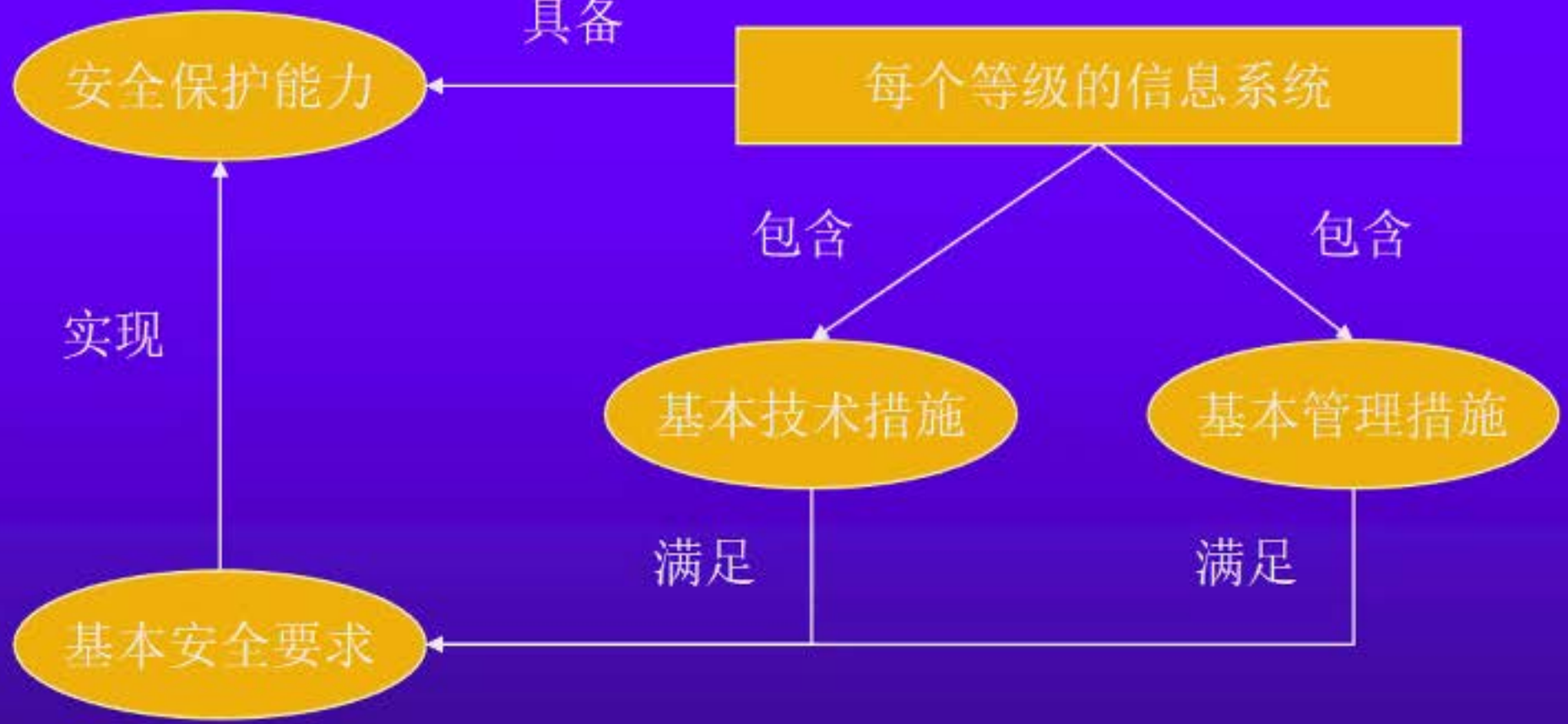
不同级别的安全保护能力要求

- 第三级安全保护能力
  - 应能够在统一安全策略下防护系统免受来自外部有组织的团体（如一个商业情报组织或犯罪组织等），拥有较为丰富资源（包括人员能力、计算能力等）的威胁源发起的恶意攻击、较为严重的自然灾难（灾难发生的强度较大、持续时间较长、覆盖范围较广等）以及其他相当危害程度的威胁（内部人员的恶意威胁、无意失误、较严重的技术故障等）所造成的主要资源损害，能够发现安全漏洞和安全事件，在系统遭到损害后，能够较快恢复绝大部分功能。
- 第四级安全保护能力
  - 应能够在统一安全策略下防护系统免受来自国家级别的、敌对组织的、拥有丰富资源的威胁源发起的恶意攻击、严重的自然灾难（灾难发生的强度大、持续时间长、覆盖范围广等）以及其他相当危害程度的威胁（内部人员的恶意威胁、无意失误、严重的技术故障等）所造成的资源损害，能够发现安全漏洞和安全事件，在系统遭到损害后，能够迅速恢复所有功能。

不同级别的安全保护能力要求

- 第三级安全保护能力
  - 应能够在统一安全策略下防护系统免受来自外部有组织的团体（如一个商业情报组织或犯罪组织等），拥有较为丰富资源（包括人员能力、计算能力等）的威胁源发起的恶意攻击、较为严重的自然灾难（灾难发生的强度较大、持续时间较长、覆盖范围较广等）以及其他相当危害程度的威胁（内部人员的恶意威胁、无意失误、较严重的技术故障等）所造成的主要资源损害，能够发现安全漏洞和安全事件，在系统遭到损害后，能够较快恢复绝大部分功能。
- 第四级安全保护能力
  - 应能够在统一安全策略下防护系统免受来自国家级别的、敌对组织的、拥有丰富资源的威胁源发起的恶意攻击、严重的自然灾难（灾难发生的强度大、持续时间长、覆盖范围广等）以及其他相当危害程度的威胁（内部人员的恶意威胁、无意失误、严重的技术故障等）所造成的资源损害，能够发现安全漏洞和安全事件，在系统遭到损害后，能够迅速恢复所有功能。

各个要素之间的关系



《基本要求》核心思路

各级系统的保护要求差异（宏观）

- 安全保护模型PPDRR

各级系统的保护要求差异（宏观）

一级系统	防护
二级系统	防护/监测
三级系统	策略/防护/监测/恢复
四级系统	策略/防护/监测/恢复/响应

各级系统的保护要求差异（宏观）

一级系统	通信/边界（基本）
二级系统	通信/边界/内部（关键设备）
三级系统	通信/边界/内部（主要设备）
四级系统	通信/边界/内部/基础设施（所有设备）

2022/5/5

各级系统的保护要求差异（宏观）

一级系统	计划和跟踪（主要制度）
二级系统	计划和跟踪（主要制度）
三级系统	良好定义（管理活动制度化）
四级系统	持续改进（管理活动制度化/及时改进）

各级系统的保护要求差异（宏观）

- 安全保护模型IATF

成功的完成业务

信息保障

深度防御战略

人

操作

技术

防御网络与基础设施	防御飞地边界	防御计算环境	支撑性基础设施

对对象的分解：一个中心三个重点

- 安全管理中心
- 安全通信网络
- 安全区域边界
- 安全计算环境
- 安全物理环境

2022/5/5