



电子科技大学
University of Electronic Science and Technology of China

第4章 信息安全等级保护



章节内容

- ◆ 4.1 概述
- ◆ 4.2 信息系统安全等级保护制度
- ◆ 4.3 信息系统安全等级保护方法
- ◆ 4.4 信息系统的安全等级



4.1 信息系统安全等级保护概述

- 信息安全等级保护：

指对涉及国计民生的基础信息网络和重要信息系统按其重要程度及实际安全需求合理投入，分级进行保护，分类指导，分阶段实施。

➤ 等级保护的核心观念是**保护重点、适度安全**；分等级、按标准进行建设、管理和监督。**综合平衡安全成本和风险**，提高保护成效。



4.1 信息系统安全等级保护概述

- ◆ 美国的军事保密制度（文件保密制度），即“多级安全”（MLS）体系：人员授权和文件都分为**绝密、机密、秘密和公开**4个等级。
- ◆ 主要目的：计算机系统如何实现真实世界的等级保护体系。
- ◆ 《可信计算机系统评估准则》（TCSEC）



4.1 信息系统安全等级保护目的

- ◆ 规范信息安全等级保护管理，提高信息安全保障能力和水平，维护国家安全、社会稳定和公共利益，保障和促进信息化建设。
- ◆ 国家通过制定统一的信息安全等级保护管理规范和技术标准，组织公民、法人和其他组织对信息系统分等级实行安全保护，对等级保护工作的实施进行监督、管理。



4.1 信息系统安全等级保护范围

✓ 运营商和服务提供商

电信、广电等基础信息网络，经营性公众互联网信息服务单位等。

✓ 重要行业

铁路、银行、海关、税务、民航、电力、证券、保险、外交、科技、发展改革、国防科技、公安、财政、审计、商务、水利、国土资源、能源、交通、文化、工商行政管理、邮政等。

✓ 重要机关

市（地）级以上党政机关网站、办公等系统。

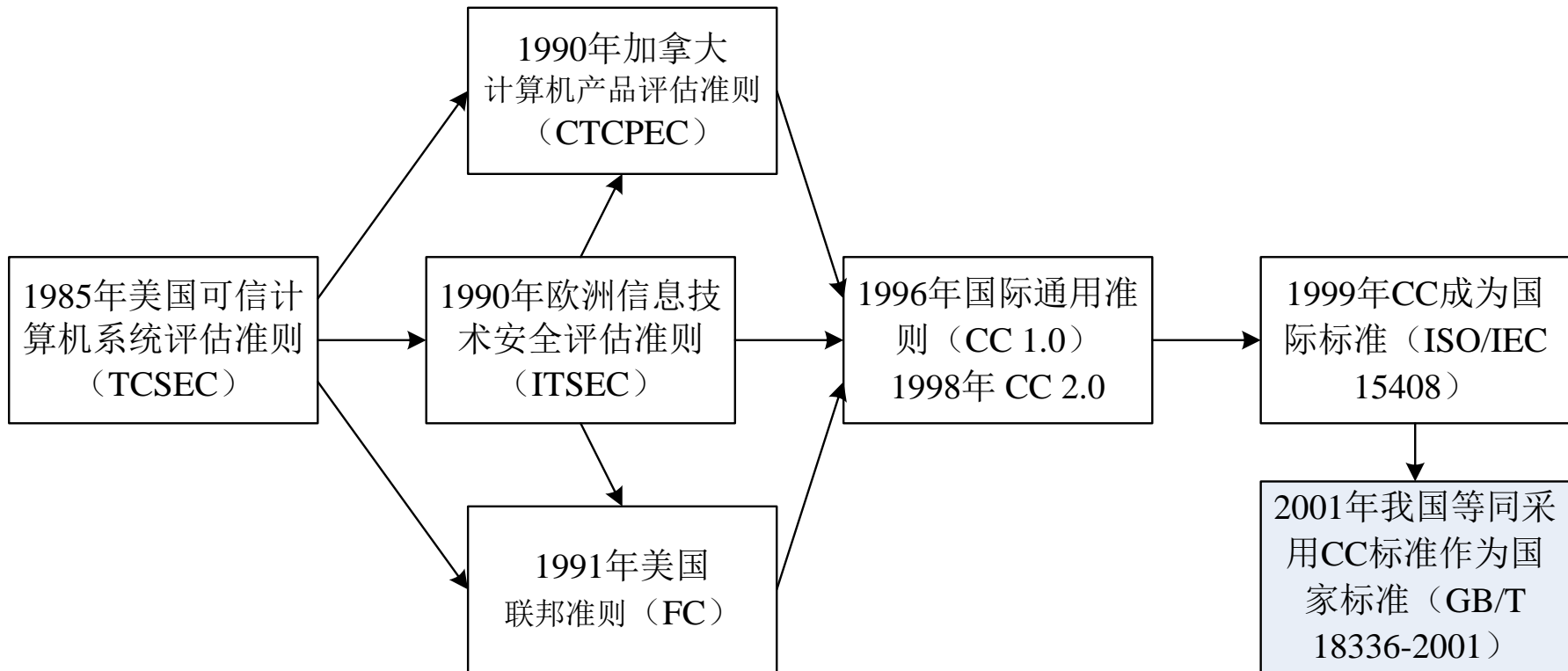
✓ 涉密系统

涉及国家秘密的信息系统。



4.1 信息系统安全等级保护发展

□ 信息安全评估准则的发展





4.1 信息系统安全等级保护发展

1. 《可信计算机系统评估准则》TCSEC

➤ 1985年12月作为国防部标准，称为“橘皮书”

类别	级别	名称	主要特征
A	A1	形式化认证	正式的设计规范来分析、核对
B	B3	安全区域	建立安全审计跟踪，独立安全管理
	B2	结构化保护	可信任运算基础体制、安全体系结构
	B1	强制存取保护	强制访问控制，灵敏度安全标记
C	C2	自主存取控制	单独的可追究性，加强审慎控制
	C1	主存取控制	可信任运算基础体制，机密性相同
D	D1	低级保护	本地操作系统，完全没有保护的网路

安全等级

➤ 偏重测评安全功能，不重视安全保证



4.1 信息系统安全等级保护发展

2. 《信息技术安全评估准则》 ITSEC

欧洲统一的安全评估标准，安全分为功能与评估。

3. 《加拿大计算机产品评估准则》 CTCPEC

吸取ITSEC和TCSEC的优点。

4. 《信息技术安全性评价组合联邦准则》 FC

定义保护框架和安全目标。

《信息技术安全评价通用准则》 CC

- 信息技术安全性评估标准，用来评估信息系统、信息产品的安全性。分为两个方面：安全功能需求和安全保证需求。



4.1 信息系统安全等级保护发展

- 信息安全评估准则的发展

- 2003年12 月，美国通过了《联邦信息和信息系统安全分类标准》（FIPS 199），描述了如何确定一个信息系统的安全类别。
- NIST分别于2004 年6月推出了SP 800-60第一、第二部分《将信息和信息系统映射到安全类别的指南》及其附件。



4.1 信息系统安全等级保护发展

- 信息安全评估准则的发展

➤ NIST的SP 800-53 《联邦信息系统推荐安全控制》为不同级别的系统推荐了不同强度的安全控制集（包括管理、技术和运行类）。SP 800-53还提出了3类安全控制（包括管理、技术和运行），汇集了美国各方面的控制措施的要求。

➤ SP 800系列标准都对我国《信息系统安全等级保护基本要求》（GB/T 22239-2008）等标准有直接的影响。



4.1 信息系统安全等级保护发展

- **第一时期 1994 ~ 2003 年 政策环境营造阶段**
 - ◆ 《中华人民共和国计算机信息系统安全保护条例》
 - ◆ 《国家信息化领导小组关于加强信息安全保障工作的意见》
- **第二时期 2004 ~ 2006 年 等级保护工作开展准备阶段**
- **第三时期 2007 ~ 2010 年 等级保护工作正式启动阶段**
 - ◆ 《信息安全等级保护管理办法》
 - ◆ 《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》
- **第四时期 2010 年至今 等级保护工作规模推进阶段**
 - ◆ 《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》
 - ◆ 《关于进一步推进中央企业信息安全等级保护工作的通知》



4.1 中国等级保护的发展

颁布时间	文件名称	文号	颁布机构	内容及意义
1994年 2月18日	《中华人民共和国计算机信息系统安全保护条例》	国务院147号令	国务院	第一次 提出信息系统要实行等级保护，并确定了等级保护的职责单位，并成为等保的 法律基础 。
1999年 9月13日	《计算机信息系统安全保护等级划分准则》	GB 17859-1999	国家质量技术监督局	将我国计算机信息系统安全保护划分为五个等级，这成为等保的 技术基础和依据 。
2003年 9月7日	《国家信息化领导小组关于加强信息安全保障工作的意见》	中办国办发[2003]27号	中共中央办公厅、国务院办公厅	明确指出“实行信息安全等级保护”，并确定了信息安全等级保护制度的 基本内容 。
2004年 9月15日	《关于信息安全等级保护工作的实施意见》	公通字[2004]66号	公安部、国家保密局、国家密码管理委员会办公室、国务院信息化工作办公室	将等级保护从计算机信息系统安全保护的一项制度提升到国家信息安全保障的一项 基本制度 。
2007年 6月22日	《信息安全等级保护管理办法》	公通字[2007]43号		明确了信息安全等级保护制度的 基本内容、流程及工作要求 ，明确了信息系统运营使用单位和主管部门、监管部门在信息安全等级保护工作中的 职责、任务 。
2009年 10月27日	《关于开展信息安全等级保护安全建设整改工作的指导意见》	公信安[2009]1429号	公安部	指导各地区、部门在等级保护定级工作基础上，开展已定级系统（除涉国家机密）的安全 整改工作 。



4.1 中国等级保护的发展

颁布时间	文件名称	文号	颁布机构	内容及意义
2010年	《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》	公信安[2010]303号	公安部	公安部结合工作实际，及时制定和出台规范性文件，对等级测评体系的建设工作提出明确要求，信息安全等级保护政策基本完备
2013年6月1日	《信息安全技术政府部门信息安全管理基本要求》	GB/T 29245-2012		规定政府部门信息安全管理基本要求，用于指导各级政府部门的信息安全管理工作。保密和密码
2013年8月	《2013年国家信息安全专项有关事项的通知》	发改办高技〔2013〕1965号	发改委	落实《国务院关于大力推进信息化发展和切实保障信息安全的若干意见》（国发〔2012〕23号）的工作部署，针对金融、云计算与大数据、信息系统保密管理、工业控制等领域面临的信息安全实际需要，继续组织国家信息安全专项。
2014年	《关于加强国家级重要信息系统安全保障工作有关事项的通知》	公信安[2014]2182号	公安部、发改委和财政部	加强对47个行业、276家信息系统运营单位，500个涉及国计民生的国家级重要信息系统的安全监管
2015年	《信息安全技术统一威胁管理产品技术要求和测试评价方法》	GB/T 31499-2015		标准规定了统一威胁管理产品的功能要求、性能指标、产品自身安全要求和产品保证要求，以及统一威胁管理产品的分级要求，并根据技术要求给出了测试评价方法。
2016年	《信息安全技术政府部门联网计算机终端安全管理基本要求》	GBT 32925-2016		标准规定了政府部门联网计算机终端的安全要求。



4.1 存在的问题

- 信息安全等级保护制度实施过程中存在的问题：
 - I. 信息安全等级保护定级标准指标较为宏观，需要进一步定量分析，提高准确度。
 - II. 新标准实施后，缺乏相应的软件支撑。



4.1 实施等级保护的意义

- 等级保护制度是国家信息安全保障的**基本制度、基本策略、基本方法**；是我国多年来信息安全工作经验的总结。
- 开展信息安全等级保护工作：
 - 有利于同步建设信息安全设施；
 - 有利于指导和服务；
 - 有利于优化信息安全资源的配置，保障重点；
 - 有利于明确责任；
 - 有利于产业发展。

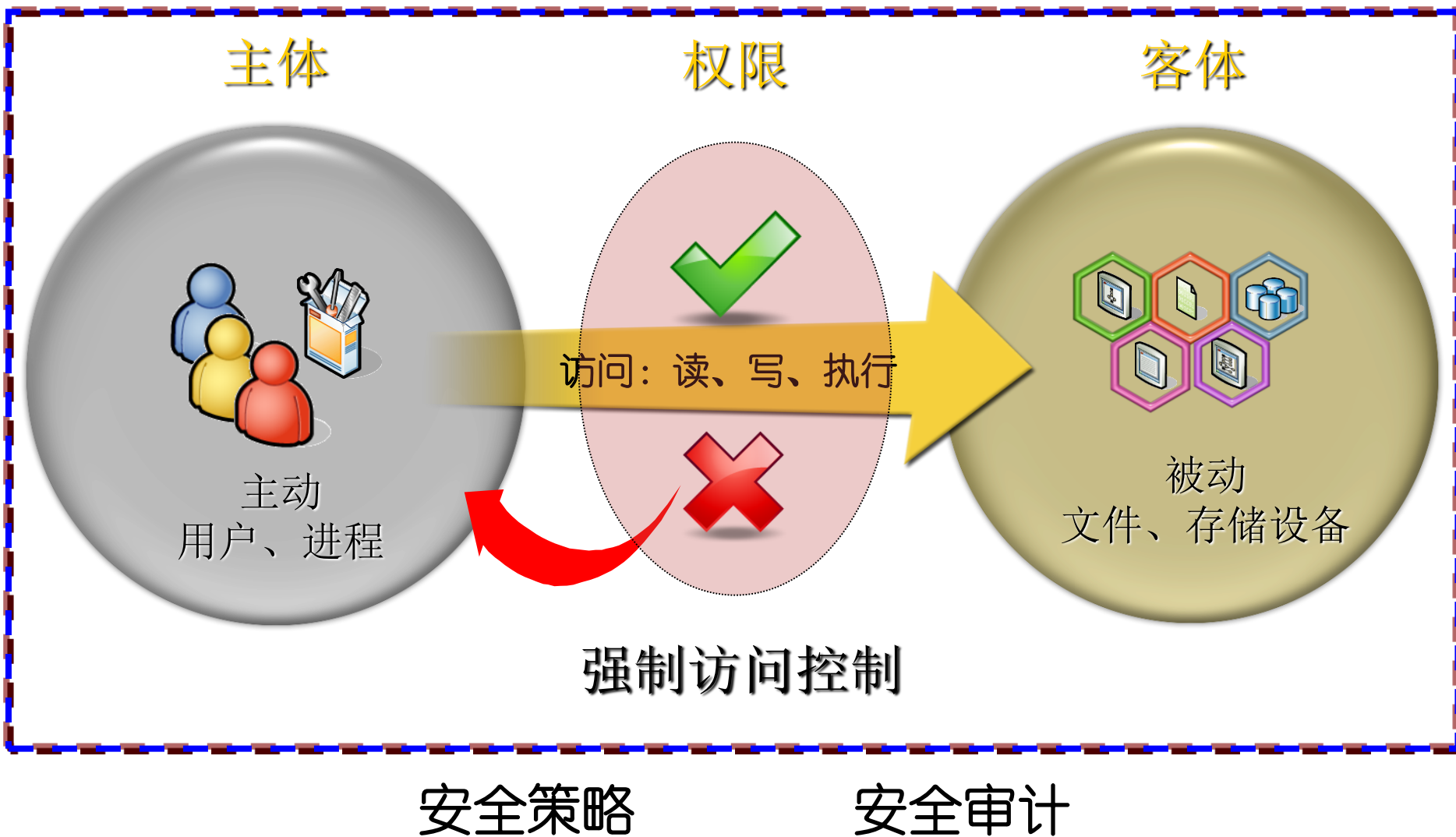


4.1 开展等级保护的要求

- 基础信息网络和重要信息系统，按照“**准确定级、严格审批、及时备案、认真整改、科学测评**”的要求完成定级、备案、整改、测评等工作。
- 公安机关和保密、密码工作部门要及时开展监督检查，**严格审查**信息系统所定级别，**严格检查**信息系统开展备案、整改、测评等工作。
- 对故意将信息系统安全级别定低，逃避公安、保密、密码部门监管，造成信息系统出现重大安全事故的，要追究单位和人员的责任。



4.1 等级保护涉及的基本概念





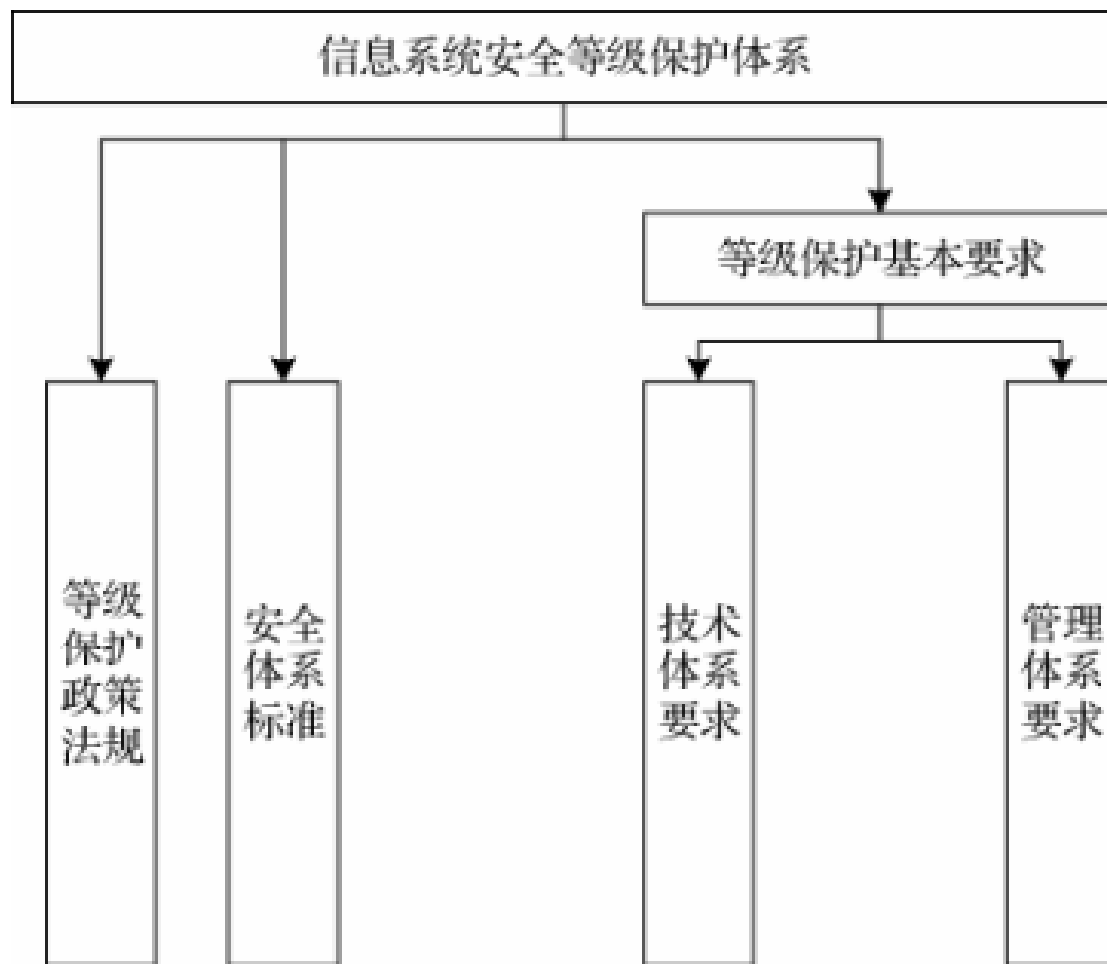
4.2 信息系统安全等级保护制度

□ 信息系统安全等级保护原则

- ① 自主保护原则：自主确定、自行实施；
- ② 重点保护原则：集中资源、关键信息系统；
- ③ 同步建设原则：同步规划和设计安全方案；
- ④ 动态调整原则：因需而变

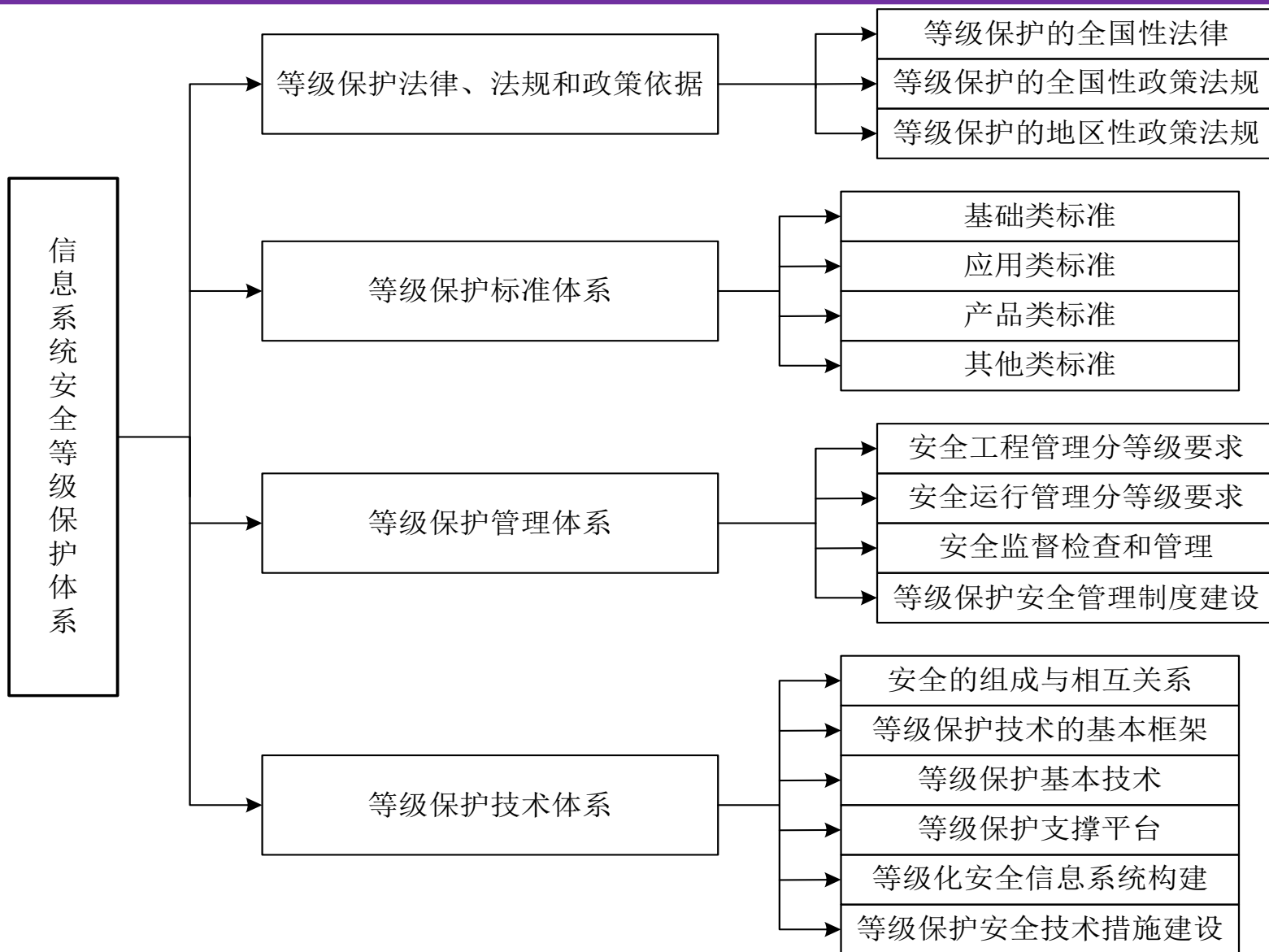


4.2 信息系统安全等级保护体系





4.2 信息系统安全等级保护体系





4.2 信息系统安全等级保护体系

□ 等级保护相关的法律、法规和政策依据

- ◆ 1994 《中华人民共和国计算机信息系统安全保护条例》。
- ◆ 2003年中办发[2003]27号文件《国家信息化领导小组关于加强信息安全保障工作的意见》。
- ◆ 2004年《关于信息安全等级保护工作的实施意见》。
- ◆ 2005年《关于开展信息系统安全等级保护基础调查工作的通知》。
- ◆ 2006年《国务院办公厅转发国家网络与信息安全协调小组关于网络信任体系若干意见的通知》。
- ◆ 2009年《关于印送〈关于开展信息安全等级保护安全建设整改工作的指导意见〉的函》。



4.2 信息系统安全等级保护体系

□ 等级保护标准体系

- 国家已出台70多个国标、行标以及报批标准，从基础、应用、产品、管理、制度等各个方面对等级保护系统提出了要求和建议。
- 四大类：**基础类、应用类、产品类和其他类。**



4.2 信息系统安全等级保护体系

◆ 等级保护标准体系-基础类标准

- 《计算机信息系统安全保护等级划分准则》（GB 17859-1999）
- 《信息系统安全等级保护基本要求》
（GB/T 22239-2008）



4.2 信息系统安全等级保护体系

◆ 等级保护标准体系-应用类标准

➤ 信息系统定级

- 《信息系统安全保护等级定级指南》（GB/T 22240-2008）

➤ 等级保护实施

- 《信息系统安全等级保护实施指南》（GB/T 25058-2010）

➤ 信息系统安全建设

- 《信息系统通用安全技术要求》（GB/T 20271-2006）
- 《信息系统物理安全技术要求》（GB/T 21052-2007）...

➤ 等级测评

- 《信息系统安全管理测评》（GA/T 713-2007）...



4.2 信息系统安全等级保护体系

◆ 等级保护标准体系-产品类标准

➤ 操作系统

- 《操作系统安全技术要求》（GB/T 20272-2006）
- 《操作系统安全评估准则》（GB/T 20008-2005）

➤ 数据库

- 《数据库管理系统安全技术要求》（GB/T 20273-2006）
- 《数据库管理系统安全评估准则》（GB/T 20009-2005）

➤ 网络

- 《网络和终端设备隔离部件技术要求》（GB/T 20279-2006）
- 《网络脆弱性扫描产品技术要求》（GB/T 20278-2006）…



4.2 信息系统安全等级保护体系

◆ 等级保护标准体系-产品类标准

➤ PKI

- 《PKI系统安全等级保护评估准则》（GB/T 21054-2007）
- 《公钥基础设施安全技术要求》（GA/T 687-2007）...

➤ 网关

- 《网关安全技术要求》（GA/T 681-2007）

➤ 服务器

- 《服务器安全测评要求》（GB/T 25063-2010）
- 《服务器安全技术要求》（GB/T 21028-2007）

➤ 入侵检测

- 《入侵检测系统技术要求和检测方法》（GB/T 20275-2006）
- 《计算机网络入侵分级要求》（GA/T 700-2007）



4.2 信息系统安全等级保护体系

◆ 等级保护标准体系-产品类标准

➤ 防火墙

- 《防火墙安全技术要求》（GA/T 683-2007）
- 《包过滤防火墙评估准则》（GB/T 20010-2005）...

➤ 路由器

- 《路由器安全技术要求》（GB/T 18018-2007）
- 《路由器安全测评要求》（GA/T 682-2007）...

➤ 交换机

- 《网络交换机安全技术要求》（GB/T 21050-2007）
- 《交换机安全测评要求》（GA/T 685-2007）

➤ 其他产品

- 《虹膜特征识别技术要求》（GB/T 20979-2007）...



4.2 信息系统安全等级保护体系

◆ 等级保护标准体系-其他类标准

➤ 风险评估

- 《信息安全风险评估规范》（GB/T 20984-2007）
- 《信息安全风险管理指南》（GB/Z 24364-2009）

➤ 事件管理

- 《信息安全事件管理指南》（GB/Z 20985-2007）
- 《信息安全事件分类分级指南》（GB/Z 20986-2007）
- 《信息系统灾难恢复规范》（GB/T 20988-2007）



4.2 信息系统安全等级保护体系

◆ 《信息系统安全等级保护基本要求》

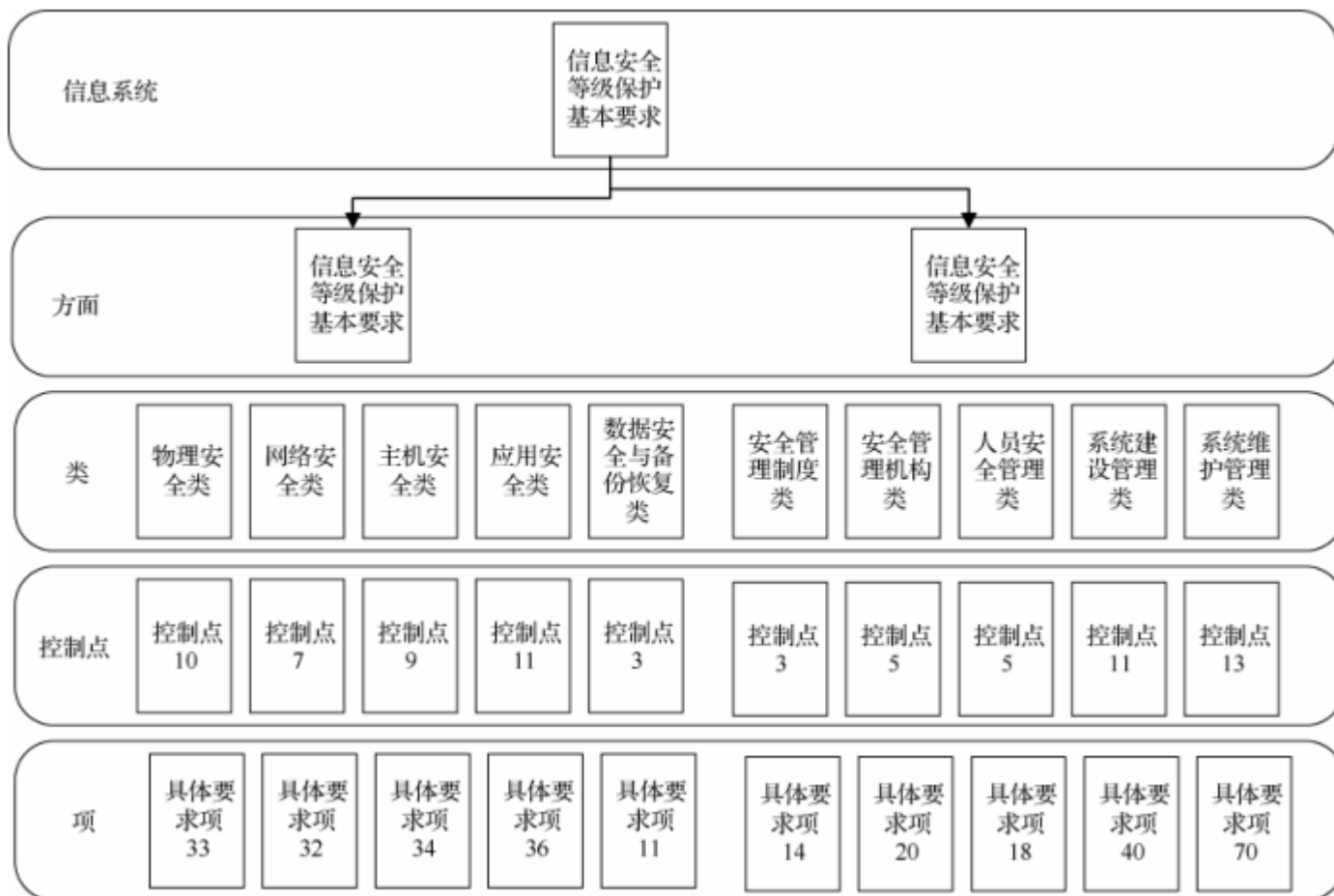
基本要求的组织方式：

- 针对不同安全保护等级信息系统应该具有的基本安全保护能力提出的安全要求。
- 根据实现方式的不同，基本安全要求分为**基本技术要求**和**基本管理要求**两大类。



4.2 信息系统安全等级保护体系

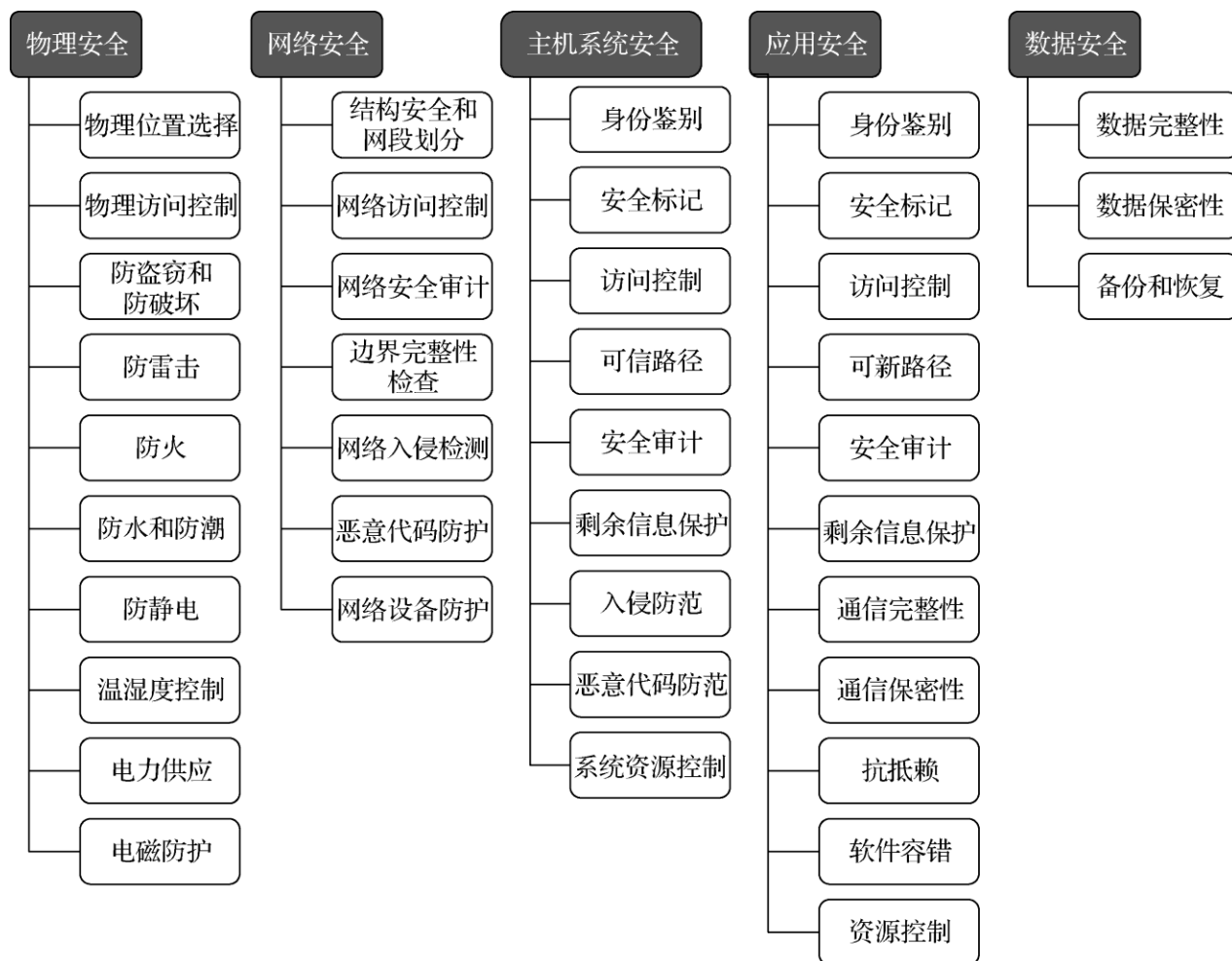
◆ 《信息系统安全等级保护基本要求》





4.2 信息系统安全等级保护体系

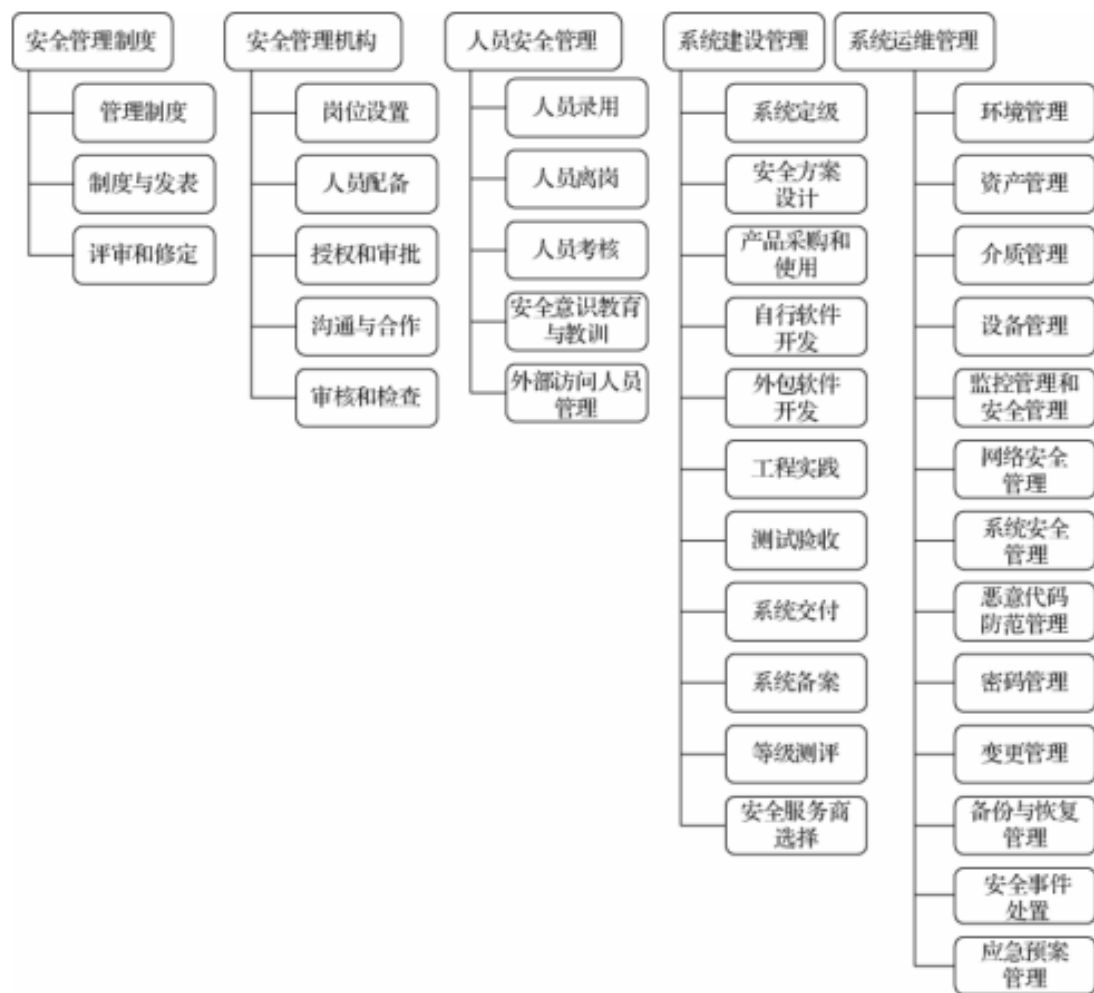
◆ 基本技术要求体系





4.2 信息系统安全等级保护体系

◆ 基本管理要求





4.2 信息系统安全等级保护体系

■ 等级保护管理体系-工程管理分等级要求

➤ 目标：对按照等级保护要求开发的信息安全系统的整个开发过程实施管理，确保所开发的安全系统达到预期的安全要求。包括：

- ◆ 工程管理计划。
- ◆ 工程资格保障。
- ◆ 工程组织保障。
- ◆ 工程实施管理。
- ◆ 项目实施管理。



4.2 信息安全等级保护体系

■ 等级保护管理体系-运行管理分等级要求

➤ 通过对照等级保护要求开发的信息安全系统的运行过程，按照相应的安全保护等级的要求实施安全管理，确保其在运行过程中所提供的安全功能达到预期的安全要求。包括：

- ◆ 系统安全管理计划、管理机构 and 人员配置、规章制度、人员审查与管理、人员培训考核与操作管理、安全管理中心、风险管理、密码管理。



4.2 信息系统安全等级保护体系

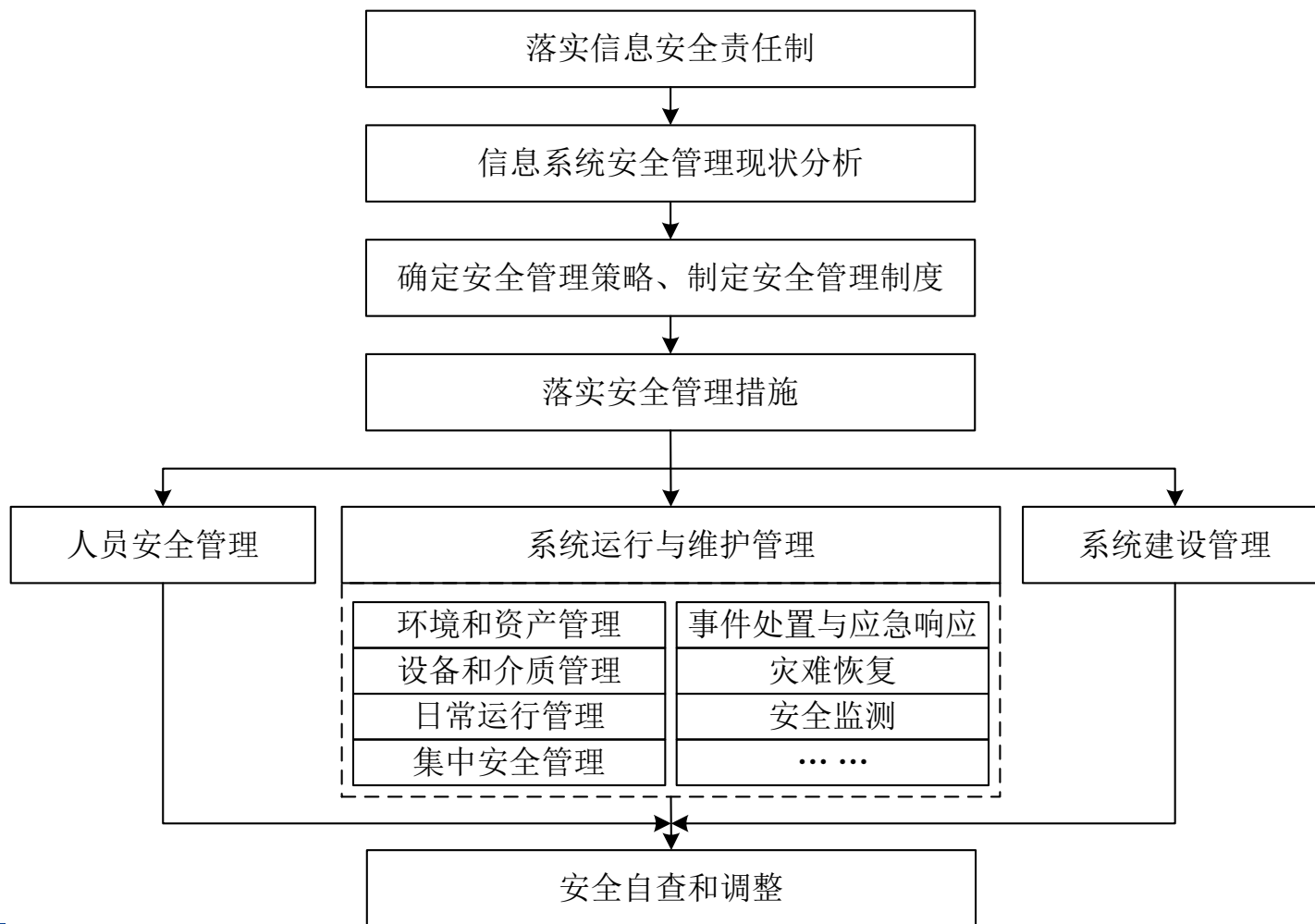
■ 等级保护管理体系-安全监督检查与管理

- 安全产品的监督检查和管理。
- 安全系统的监督检查和管理。
- 长效持续的监督检查和管理。



4.2 信息系统安全等级保护体系

■ 等级保护管理体系-安全管理制度建设





4.2 信息系统安全等级保护体系

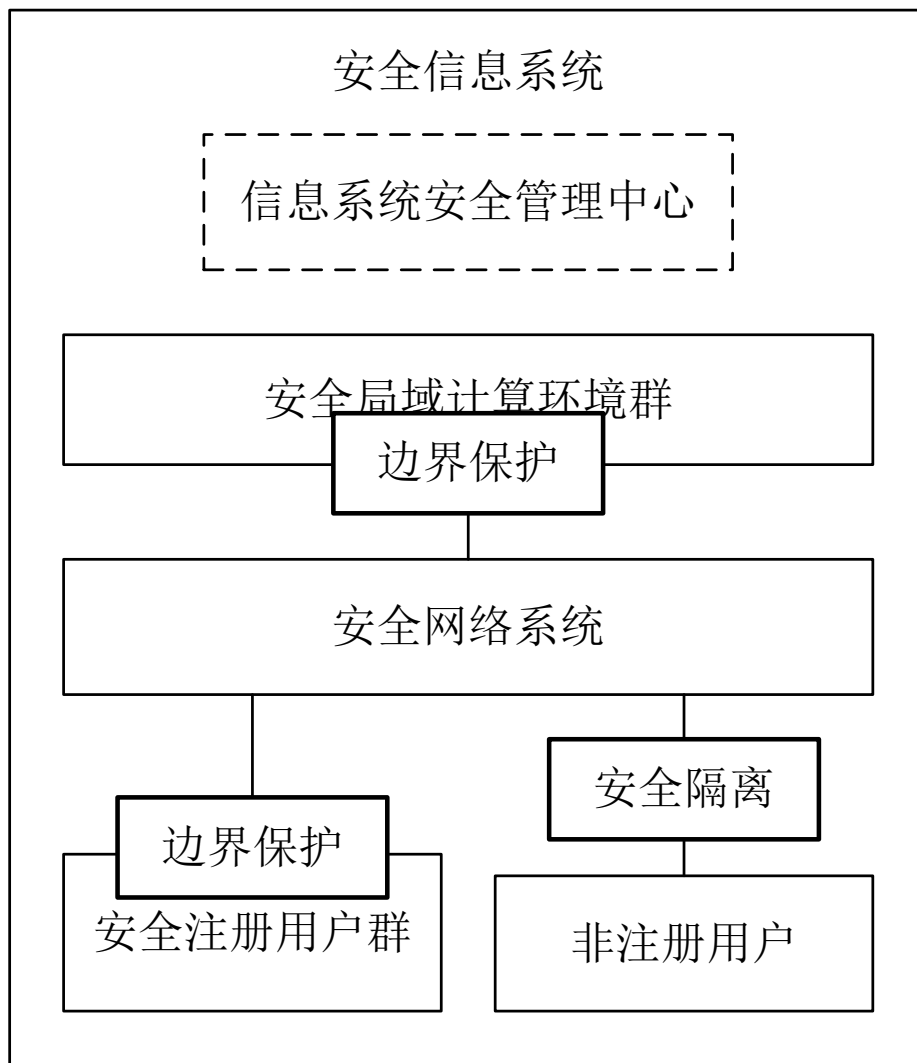
■ 等级保护技术体系-安全组成及相互关系

应用安全 (应用软件安全、支撑软件安全、工具软件安全)	应用管理	安全 管 理
网络安全 (网络软件安全、网络安全协议安全、网络数据传输安全)	系统管理	
系统安全 (操作系统安全、数据库管理系统安全)	网络管理	
物理安全 (计算机硬件安全、网络硬件安全、环境安全)	物理管理	



4.2 信息系统安全等级保护体系

■ 等级保护技术体系-等级保护基本框架





4.2 信息安全等级保护体系

■ 等级保护技术体系-等级保护基本技术

➤ 标识与鉴别技术:

- 口令鉴别
- 生物特征鉴别
- 数字证书鉴别

➤ 访问控制技术:

- 自主访问控制
- 强制访问控制



4.2 信息安全等级保护体系

■ 等级保护技术体系-等级保护基本技术

➤ 存储和传输的数据完整性保护技术：

■ 包括一般的校验码机制（例如奇偶校验、海明校验等）、密码系统支持的校验机制、隐藏信息技术支持的纠错机制等。

■ 访问控制、身份鉴别、边界隔离与防护等实际上也都是与完整性保护有关的安全技术和机制。



4.2 信息安全等级保护体系

■ 等级保护技术体系-等级保护基本技术

➤ 存储和传输的数据保密性保护技术：

■ 包括密码系统支持的加密机制、隐藏信息技术支持的信息保护机制等。

■ 访问控制、身份鉴别、边界隔离与防护等实际上也都是与保密性保护有关的安全技术和机制。



4.2 信息系统安全等级保护体系

■ 等级保护技术体系-等级保护基本技术

➤ 边界隔离与防护技术：

- 包括防火墙、入侵检测、防病毒网关、非法外连检测、网闸、逻辑隔离、物理隔离、信息过滤等，用于阻止来自外部网络的各种攻击行为。

➤ 系统安全运行及可用性保护技术：

- 安全审计技术
- 安全性检测分析技术
- 系统安全监控技术
- 信息系统容错备份与故障恢复技术



4.2 信息安全等级保护体系

■ 等级保护技术体系-等级保护基本技术

➤ 密码技术：

- 包含对称密钥密码、非对称密钥密码和单向函数。
- 密码技术可用于实现数据加密、数字签名、身份认证、权限验证、数据完整性验证等安全需求的场合。



4.2 信息安全等级保护体系

■ 等级保护技术体系-等级保护支撑平台

➤ 信息系统密码基础设施平台：

■ 由密码技术所构成的密码基础设施平台，由基于公钥基础设施（PKI）、授权管理基础设施（PMI）、密钥管理基础设施（KMI）等密码安全机制和授权管理机制等组成，它为安全信息系统实现保密性、完整性、真实性、抗抵赖、访问控制等安全机制提供支持。



4.2 信息系统安全等级保护体系

■ 等级保护技术体系-等级保护支撑平台

➤ 信息系统应用安全支撑平台：

利用密码基础设施平台提供的基于PKI/PMI/KMI技术的安全服务，采用安全中间件及一站式服务理论和技术，支持面向业务应用的各种应用软件系统安全机制的设计，实现包括真实性鉴别、访问控制、信息安全交换、数据安全传输以及数据的保密性、完整性保护等应用软件系统的安全功能，是应用软件系统安全支撑平台的设计目标。

- 安全服务要求
- 分等级要求



4.2 信息系统安全等级保护体系

■ 等级保护技术体系-等级保护支撑平台

➤ 信息系统灾难备份与恢复平台：

- 灾难备份
- 灾难恢复
- 分等级要求

➤ 信息系统安全事件应急响应与管理平台：

- 应急响应与管理
- 应急计划
- 联动要求
- 标准化要求



4.2 信息系统安全等级保护体系

■ 等级保护技术体系-等级保护支撑平台

➤ 信息系统安全管理平台：

- 信息系统安全管理平台既是一个管理机构，又具有强烈的技术特色。

- 通过对各种信息安全设备、安全软件、人员角色等进行集中监控与管理，把原本分离的各种信息资源联系成一个有机协作的整体，实现信息安全管理过程中的实时状态监测与风险评估、动态策略调整、综合安全审计、数据关联处理，以及恰当及时的威胁响应，从而有效地提升信息系统的安全保障能力和用户的管理水平。



4. 3等级保护的基本原理和方法

■ 等级保护的基本原理

根据信息系统所承载的业务应用的不同安全需求，采用不同的安全保护等级，对不同的信息系统或同一信息系统中的不同安全域进行不同程度的安全保护，以实现对信息系统及其所存储、传输和处理的数据信息在安全保护方面，达到确保重点，照顾一般，适度保护，合理共享的目标。

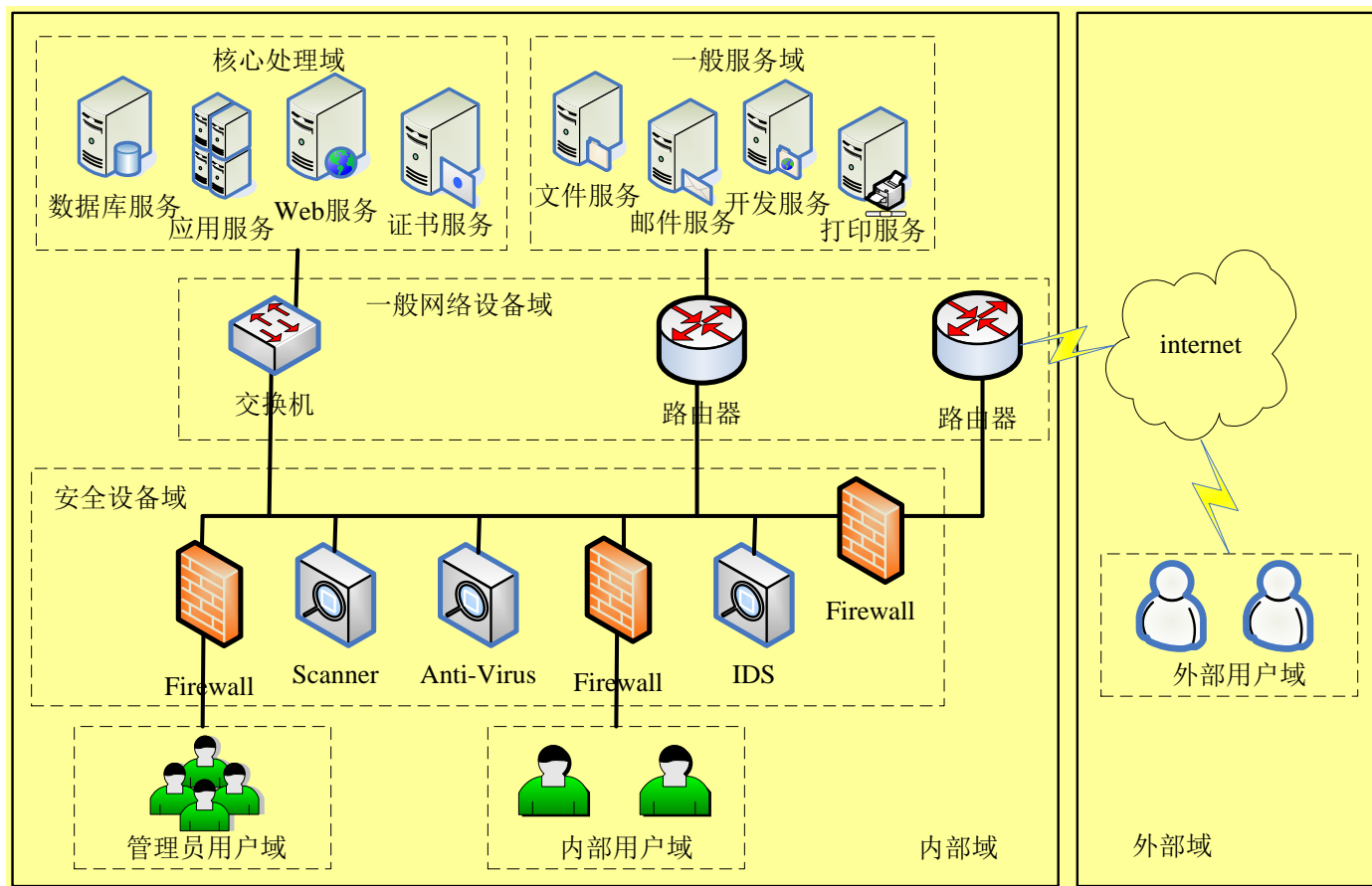


4. 3等级保护的基本原理和方法

- 信息系统安全防护按照边界安全防护、网络环境安全防护、主机安全防护和应用防护4个层次进行防护措施设计。
- 安全域指同一系统内根据信息的性质、使用主体、安全目标和策略等元素的不同来划分的不同逻辑子网或网络。
- 信息系统安全域的划分主要考虑因素：
 - ✓ 业务和功能特性
 - ✓ 安全特性的要求
 - ✓ 参照现有状况



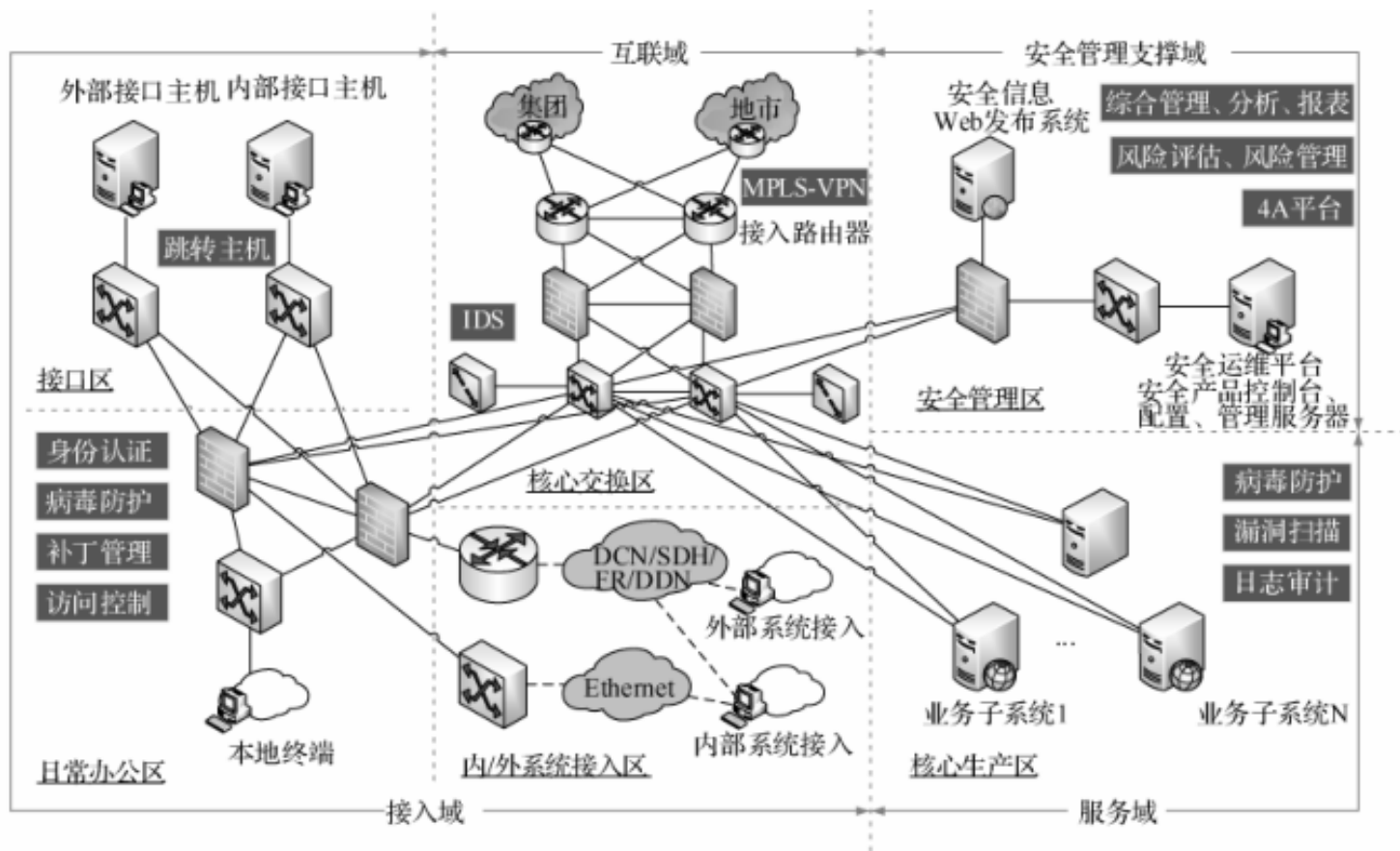
4. 3等级保护的基本原理和方法



安全域划分



4. 3等级保护的基本原理和方法

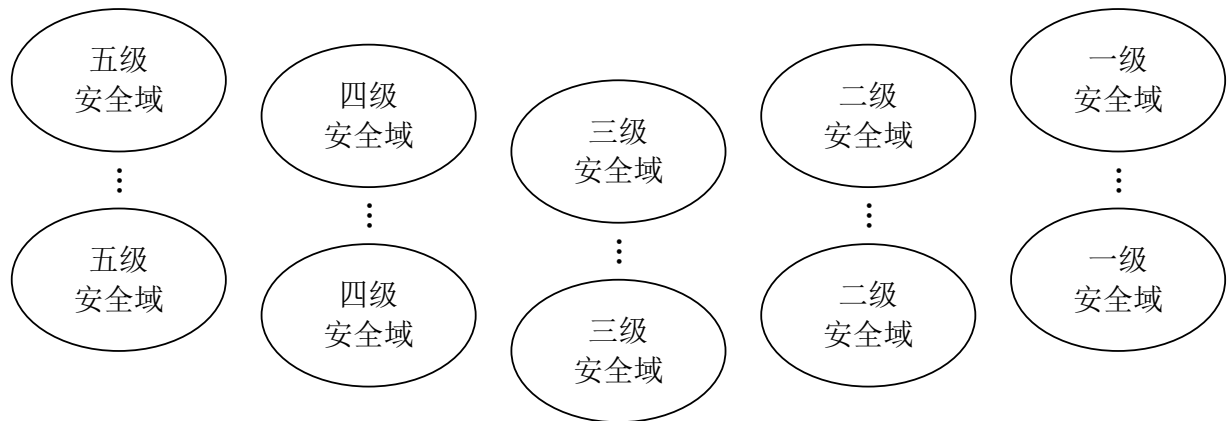
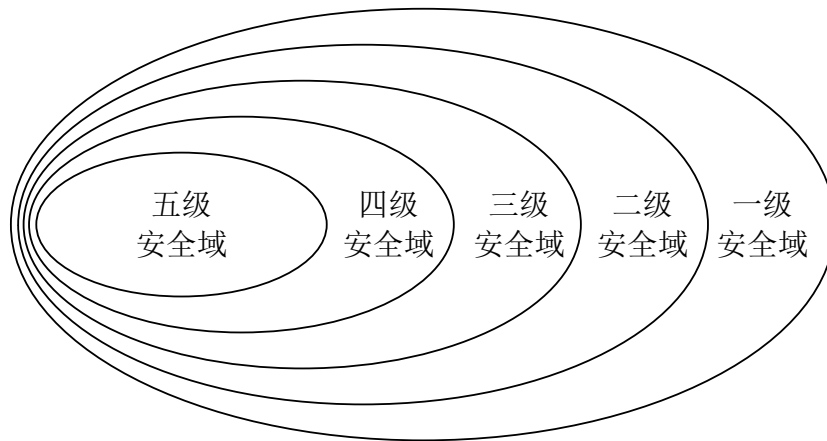


安全域划分



4. 4等级保护的基本原理和方法

■ 分区域分等级安全保护





4.3等级保护的基本原理和方法

■ 内部保护和边界保护

➤边界保护主要考虑的问题是如何使某个安全等级的网络内部不受来自外部的攻击，提供各种机制防止恶意的内部人员跨越边界实施攻击，以及防止外部人员通过开放门户/隐通道进入网络内部。

➤信息系统边界防护分为外部边界防护和内部边界防护。具体归为信息外网第三方边界、信息内网第三方边界、信息内外网边界、信息内网纵向上下级单位边界及横向域间边界5 类。



4. 3等级保护的基本原理和方法

■ 内部保护和边界保护

- 典型的边界防护可采用防火墙、信息过滤、信息交换控制等。既可以用于最外部边界防护，也可以用于内部各安全域的边界防护。
- 入侵检测、病毒防杀既可以用于边界防护也可以用于内部保护。
- 身份鉴别、访问控制、安全审计、数据存储保护、数据传输保护等是内部保护常用的安全机制，也可用作对用户和信息进/出边界的安全控制。



4.3等级保护的基本原理和方法

■ 边界安全保护

边界类型	边界说明	主要控制实施	产品实现
外网第三方边界	外网与互联网的边界及其他单位通过拨号连接所形成的网络边界	网络访问控制；流量及连接数控制；内容过滤；对外服务安全；入侵检测	防火墙；统一威胁管理（UTM）；入侵检测/防护系统（IDS/IPS）；虚拟专用网络（VPN）
内网第三方边界	内网与企业业务合作伙伴等第三方网络专线连接所形成的边界，如银行	网络访问控制；流量及连接数控制；入侵检测	防火墙；入侵检测/防护系统（IDS/IPS）
内外网边界	信息内网与信息外网连接的边界	逻辑强隔离	专用逻辑强隔离
纵向边界	信息内网纵向上下级单位网络连接的边界以及平级单位间连接的边界	网络访问控制；入侵检测	防火墙；入侵检测/防护系统（IDS/IPS）
横向域间边界	各安全域间的互访边界	域间访问控制；边界入侵检测	防火墙；入侵检测/防护系统（IDS/IPS）；WLAN；ACL



4. 3等级保护的基本原理和方法

■ 网络安全保护

- 目的是防范恶意人员通过网络对应用系统进行攻击，同时阻止恶意人员对网络设备发动的攻击。
- 由**相同安全等级**的服务器组成的安全局域计算环境需要**相应安全等级**的局域网实现连接，由相同安全等级的终端计算机组成的安全用户环境需要相应安全等级的局域网实现连接。

防护对象	主要控制措施	产品实现
网络设备	接入控制；设备安全配置；设备安全加固；安全弱电扫描；配置文件备份；设备安全审计；网络带宽及处理能力保证；设备链路冗余	网络准入控制系统（MAC）；漏洞扫描系统；日志管理分析系统；网管系统
网络业务信息流	网络业务信息流；数据传输加密	入侵检测/防护系统（IDS/IPS）系统；虚拟专用网络（VPN）



4. 3等级保护的基本原理和方法

■ 网络安全保护

➤ 物理安全策略

目的是保护计算机系统、网络服务器、打印机等硬件实体和通信链路免受自然灾害及人为破坏。

➤ 访问控制策略

是网络安全防范和保护的主要策略。

➤ 防火墙控制

是用以阻止网络中的黑客访问某个机构网络的一道屏障，也可以称之为控制进、出两个方向通信的门槛。



4. 3等级保护的基本原理和方法

■ 网络安全保护

➤ 信息加密策略

目的是保护网内的数据、文件口令、控制信息，以及网上传输的数据。

➤ 网络安全管理策略

加强网络的安全管理，制定合理的规章制度。确定安全管理等级和安全管理范围。制定有关规程和制度，应急措施。



4. 3等级保护的基本原理和方法

■ 主机安全保护

- 确保业务数据在进入、离开或驻留服务器时保持**可用性、完整性和保密性**。
- 主机系统安全防护包括对服务器及桌面终端的安全防护。

防护对象		主要控制措施	产品实现
服务器	操作系统	操作系统安全加固；病毒防护；防恶意代码；入侵检测；访问控制；主机弱点扫描；安全补丁更新；系统备份；防止非法外联；安全审计	防火墙；入侵检测/防护系统 (IDS/IPS)；弱点扫描系统；补丁管理系统；日志分析管理系统；防病毒/恶意代码系统；数字证书系统；备份系统
	数据库系统	访问控制；安全审计；管理存储过程；数据安全；数据备份	日志分析管理系统；数字证书系统；备份系统
桌面终端	桌面终端	桌面终端病毒防护；恶意代码防护；补丁管理；桌面主机资产管理；桌面终端安全管理	防病毒/恶意代码系统；终端管理系统；补丁管理系统



4. 3等级保护的基本原理和方法

■ 主机安全保护

从**系统安全**、**文件安全**和**网络安全**三方面来提供保护，共同为主机提供了一个全面的保护环境。

➤ 系统安全

对主机的系统安全保护主要依赖于防火墙、IDS 和操作系统本身固有的安全特性。

➤ 文件安全

存放在主机上的数据。

➤ 网络安全

在主机的网络接口上所做的保护措施。



4. 3等级保护的基本原理和方法

■ 应用保护

保证应用系统自身的安全性，以及与其他系统进行数据交互时所传输数据的安全性；在安全事件发生前发现入侵企图或在安全事件发生后进行审计追踪。

防护对象	主要控制措施	产品实现
应用系统	接入控制；设备安全配置；设备安全加固；安全弱电扫描；配置文件备份；设备安全审计；网络带宽及处理能力保证；设备链路冗余	日志管理分析系统；备份管理系统；数字证书及认证系统
用户接口	用户认证安全；数据完整性检测；数据安全保密	通过应用系统实现
数据接口	接口认证；数据传输加密；数据完整性检测	通过应用系统实现



4.4 信息系统的安全等级

《计算机信息系统安全保护等级划分准则》GB17859-1999

● 第一级 用户自主保护级

用户自主控制资源访问

● 第二级 系统审计保护级

访问行为需要被审计

● 第三级 安全标记保护级

通过标记实现强制访问控制

● 第四级 结构化保护级

可信计算机结构化

● 第五级 访问验证保护级

所有的过程都需要验证



4.4 信息系统的安全等级

- 信息系统的安全保护等级由两个定级要素决定：
 - 等级保护对象受到破坏时所侵害的客体
 - 对客体造成侵害的程度。
- 受侵害的客体（三个方面）
 - 公民、法人和其他组织的合法权益
 - 社会秩序、公共利益
 - 国家安全
- 侵害的程度：
 - 一般损害、严重损害、特别严重损害



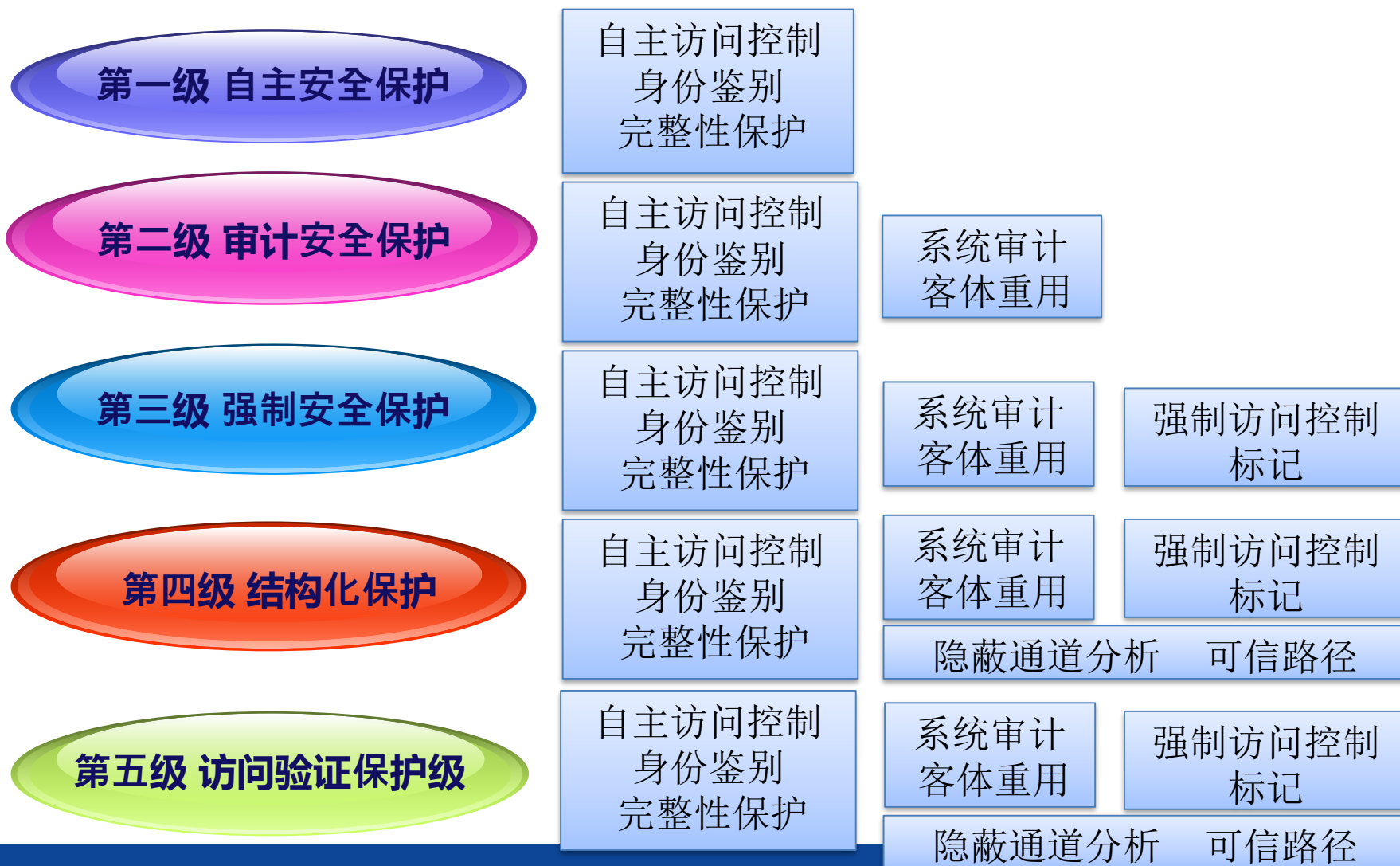
4.4 信息系统的安全等级

等级	对象	侵害客体	侵害程度	监管强度
第一级	一般系统	合法权益	损害	自主保护
第二级		合法权益	严重损害	指导保护
		社会秩序和公共利益	损害	
第三级	重要系统	社会秩序和公共利益	严重损害	监督检查
		国家安全	损害	
第四级		社会秩序和公共利益	特别严重损害	强制监督检查
		国家安全	严重损害	
第五级	极端重要系统	国家安全	特别严重损害	专门监督检查

保护等级划分依据



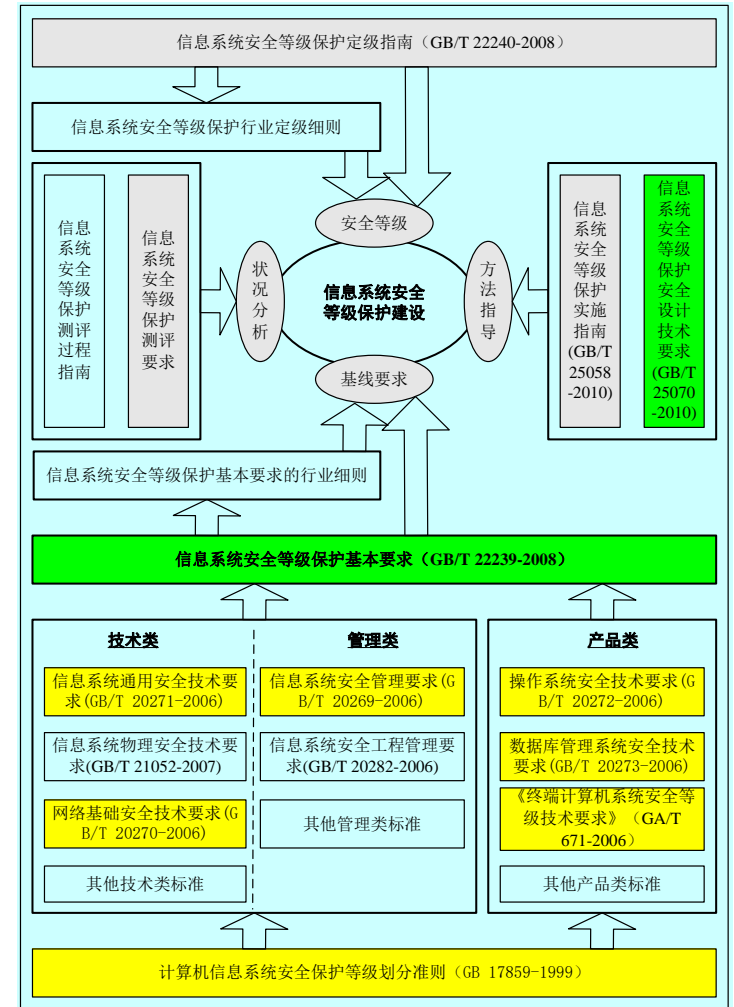
4.4 信息系统的安全等级





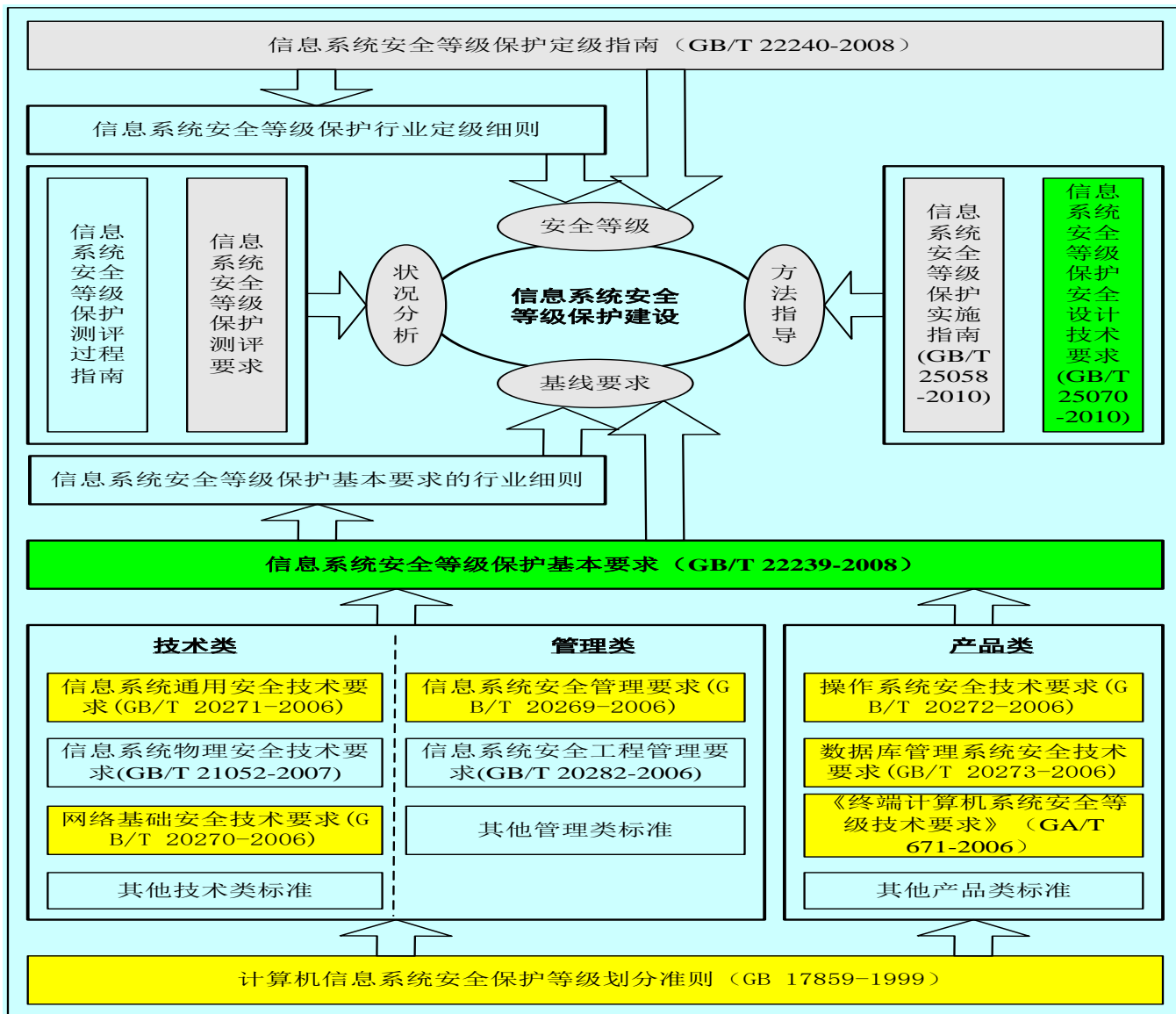
4.4 信息系统的安全等级

- 信息系统安全建设是根据《信息系统安全等级保护基本要求》（GB/T 22239-2008），在不同阶段、针对不同技术活动参照相应的标准规范进行。





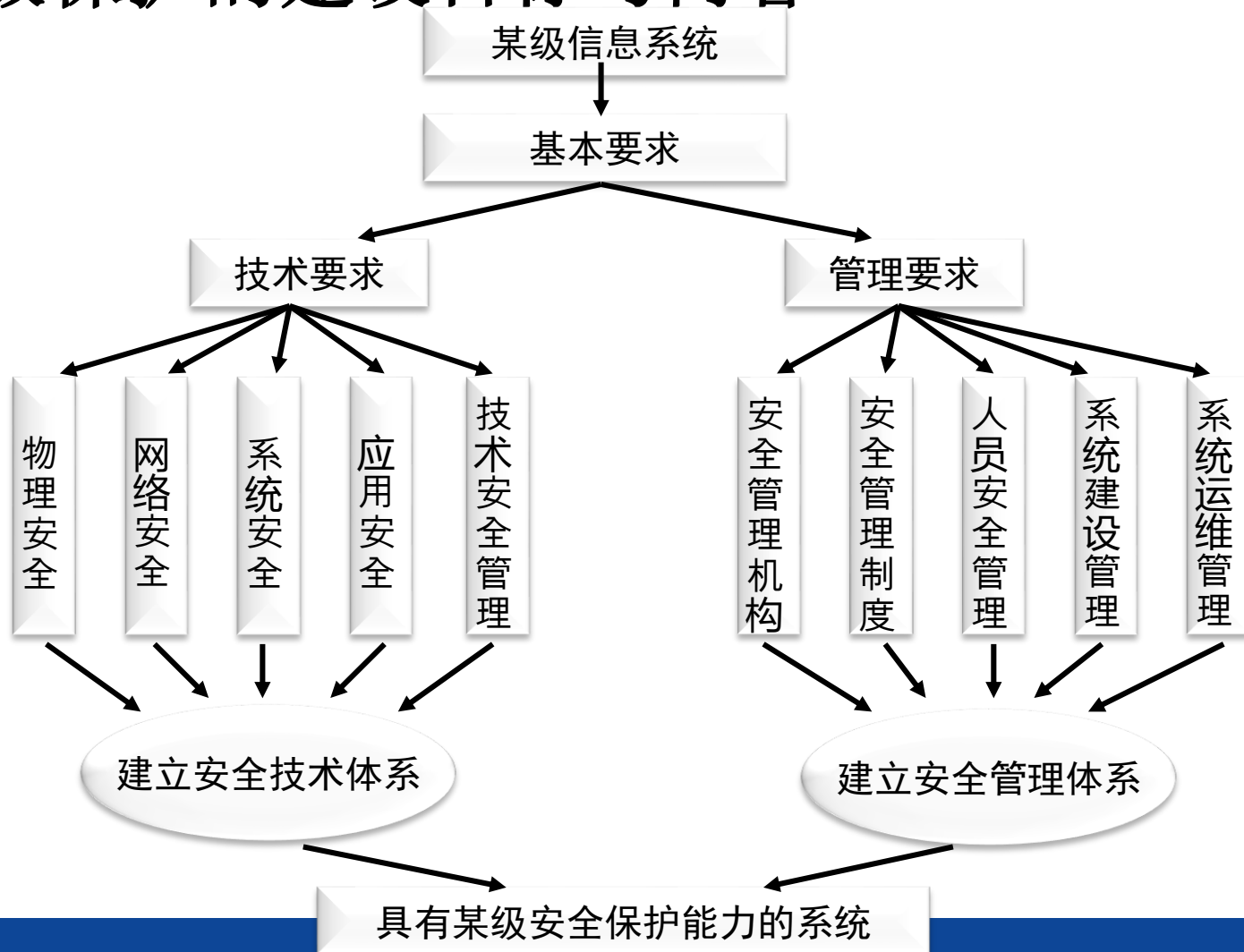
4. 4 信息系统的安全等级





4.4 信息安全定级

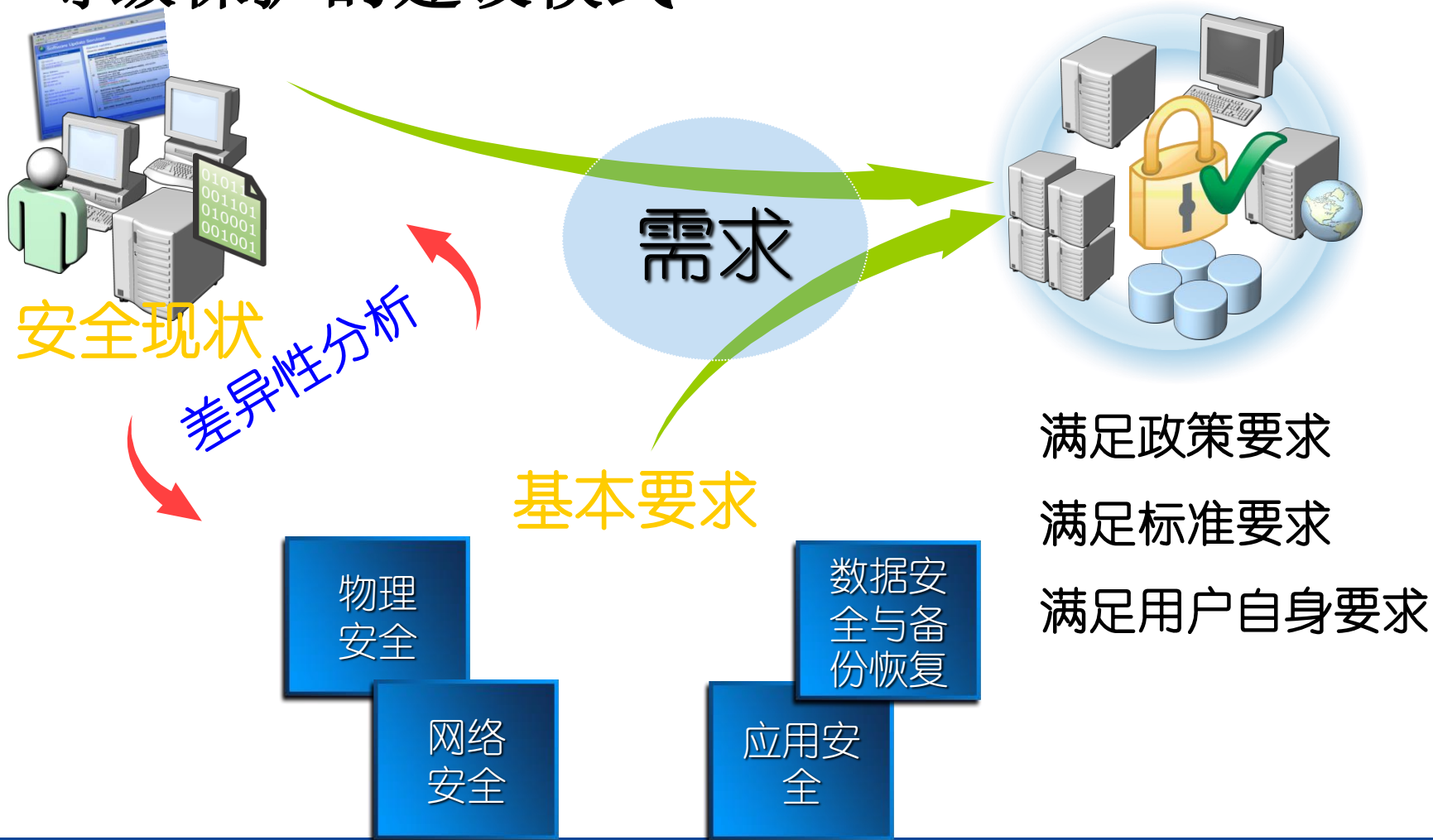
等级保护的建设目标与内容





4.4 信息安全定级

等级保护的建设模式





4.4 信息安全定级

等级保护的建设流程



等保整改



等保建设



达标等保体系



4.4 信息安全定级

等级保护的整改流程

1. 信息系统定级



2. 等保建设立项



3. 信息安全风险评估



4. 等保方案设计



5. 安全体系部署



6. 等保体系测评



7. 等保整改建设完成



4.4 等级保护建设工作

□ 信息系统定级

➤ 按资产价值和威胁的方式定级

■ **第一步：** 根据确定信息系统的总体安全需求等级过程中对信息和信息系统安全保护需求的分析，明确信息系统的安全保护需求是否需要进一步划分安全域。

■ **第二步：** 对目标信息系统（安全域）及其相关设施的资产价值及该信息系统（安全域）可能受到的威胁进行综合评估与审计，确定其相应的资产价值级别和威胁级别，并据此确定目标信息系统（安全域）应具有的安全保护等级。



4.4 等级保护建设工作

□ 信息系统定级

■ **第三步：**按照确定的安全保护等级，从等级保护的相关标准中选取对应等级的安全措施（包括技术措施和管理措施），用系统化方法设计具有相应安全保护等级的安全子系统，并对设计好的安全子系统的脆弱性进行评估。

■ **第四步：**用风险分析的方法对已经设计好安全子系统的目标信息系统（安全域）的资产价值、安全威胁和脆弱性进行评估，确定该信息系统（安全域）具有的剩余风险。



4.4 等级保护建设工作

□ 信息系统定级

■ **第五步：** 再根据安全措施的调整情况，对照等级保护的相关标准中不同安全保护等级的安全技术和安全管理的要求，确定目标信息系统（安全域）的最终安全保护等级。



4.4 等级保护建设工作

- 案例1：某省政府网站系统ZFWZ，用于发布政务公开信息、地方行政法规和管理措施、政府办事流程、新闻发布、政府公告、举报投诉、省内经济形势介绍、下载等信息，服务对象主要是省内企业和市民。
- 该信息安全被破坏可能对社会秩序造成一定影响；由于网站的访问量并不很大，信息被篡改可能造成的不良社会影响不会很大，因此对社会秩序的侵害程度为一般损害；查表知ZFWZ系统的业务信息安全保护等级为第二级，如下表所示。

业务信息安全被破坏时所侵害的客体	对相应客体的侵害程度		
	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



4.4 等级保护建设工作

- 案例2：某省电力集团公司的省级电力实时监控系統，主要运行调度自动化控制系统和能量管理系统（SCADA/EMS）DDZDH，负责省级超高压输电变电站的调度控制和数据采集。
- 调度控制指令或调度程序被修改，可能造成的停电事故会影响几乎所有行业的正常生产和工作，其所侵害的客体为**社会秩序和公共利益**；调度控制指令或调度程序被修改可能造成全省范围大面积停电、人员伤亡和巨额财产损失，同时对其它行业的生产和工作造成非常严重的影响，因此对社会秩序和公共利益的侵害程度为特别严重损害；

业务信息安全被破坏时所侵害的客体	对相应客体的侵害程度		
	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



4.4 等级保护建设工作

□ 等保建设立项

➤ 信息系统等级保护建设，经过信息系统的运营、管理部门以及有关政府部门的批准，并列入信息系统运营单位或政府计划的过程。



4.4 信息系统的安全等级

附件 2:

备案表编号:

[illegible]

信息系统安全等级保护
备案表

备 案 单 位: _____ (盖章)

备 案 日 期: _____

受理备案单位: _____ (盖章)

受理日期: _____

中华人民共和国公安部监制



4.4 信息系统的安全等级

附件3:

涉及国家秘密的信息系统分级保护备案表

单位名称:	
涉密信息系统名称:	
系统密级(保护等级):	<input type="checkbox"/> 绝密 <input type="checkbox"/> 机密 <input type="checkbox"/> 秘密
系统联网范围:	<input type="checkbox"/> 局域网 <input type="checkbox"/> 城域网 <input type="checkbox"/> 广域网(跨____省或地)
系统安全域划分和安全域密级确定:	<input type="checkbox"/> 未划分安全域 <input type="checkbox"/> 划分安全域(共有____, 其中绝密级____, 机密级____, 秘密级____, 内部级____)
系统主要承建单位:	
系统投入使用时间:	
系统运行管理部门:	
系统安全保密管理部门:	
系统分级保护实施情况:	<input type="checkbox"/> 已经实施 <input type="checkbox"/> 正在实施 <input type="checkbox"/> 计划____年实施

填报日期: 年 月 日

填报单位: (盖章)

填表说明:

1. “系统密级”依据《涉及国家秘密的信息系统分级保护管理办法》和国家保密标准 BMB17-2006 确定。
2. 涉密信息系统一般应划分安全域, 同一系统内的不同安全域根据所处理信息的重要程度, 可分别确定密级。
3. 表中“□”用“√”确认。
4. 填报多个涉密信息系统, 可复印此表。

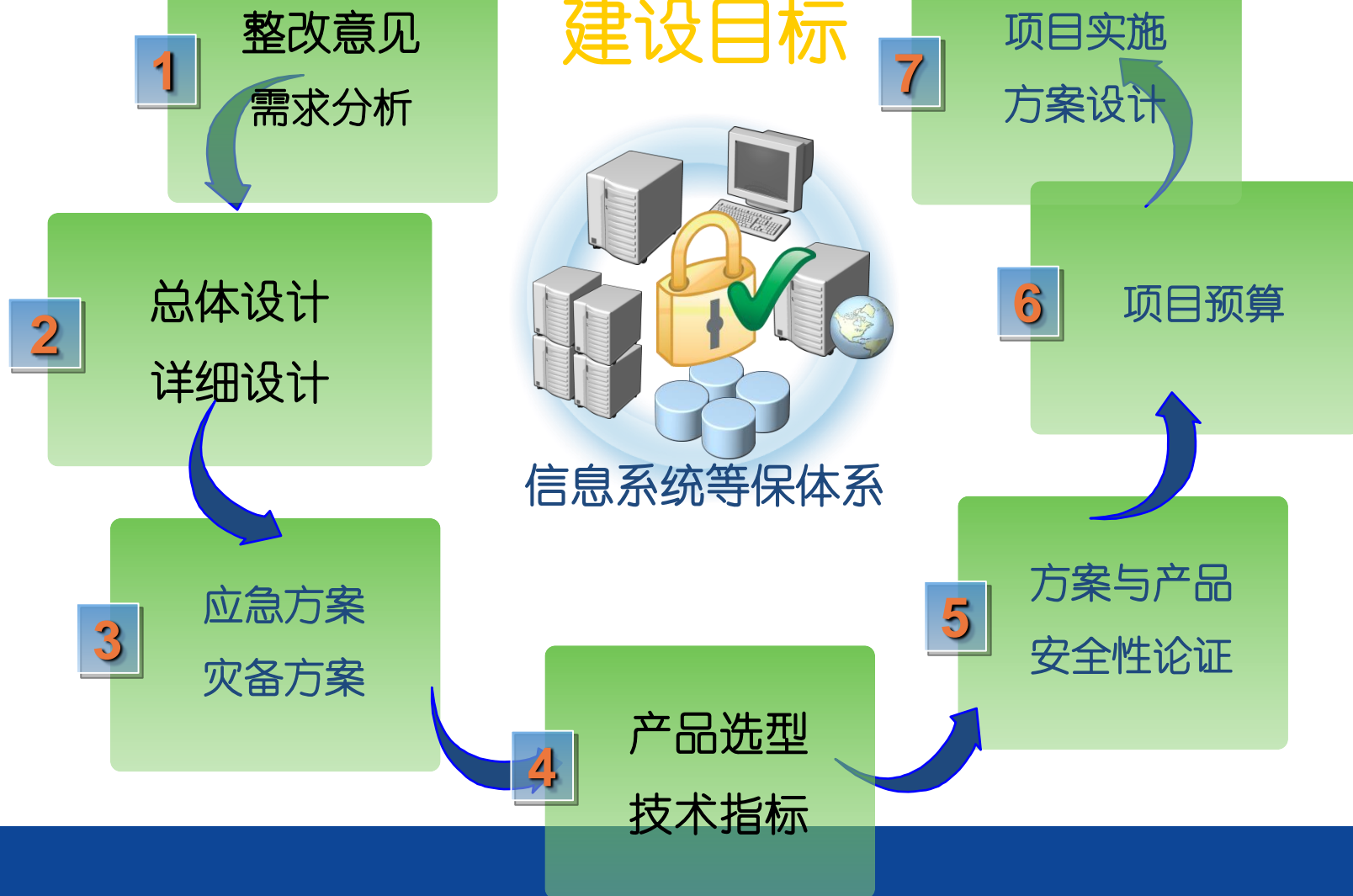
国家保密局制



4.4 等级保护建设工作

□ 等级保护的整改流程-等保方案设计

建设目标






4.4 等级保护建设工作

□ 等级保护的整改流程-等保方案设计

- 一、项目背景
- 二、安全需求分析
- 三、方案总体设计
- 四、等保技术体系设计
- 五、等保物理安全设计
- 六、等保管理安全设计
- 七、应急与灾备设计
- 八、产品选型与技术指标
- 九、方案与产品安全性论证
- 十、项目预算

A large, stylized green bubble graphic composed of many overlapping circles, located on the right side of the slide. It contains the text '经过信息安全等级保护专家论证通过'.

经过信息安全等级保护专家论证通过



4.4 等级保护建设工作

□ 等级保护的整改流程-等保体系测评

- 相应的政策、标准为基准，对等保体系进行风险评测，从面临的威胁、存在的弱点、造成的影响，以及三者综合作用角度，分析信息系统的等保体系是否达标。
- 请相应级别、具有资质的测评中心进行等保测评。
- 等保测评完成后出具《测评报告》和《整改意见》。



差异性

	SSE-CMM	等级保护
出发点	系统安全工程领域中具体应用，为安全工程的结果提供有效的评估手段	以国家安全、社会秩序和公共利益为出发点，指导全国的信息安全工作的一个基本制度，目的是构建国家整体的信息安全保障体系。
对象	安全工程实施的标准。分布于整个安全工程生命周期中各个环节。应用于安全产品开发者、安全系统开发者及集成者，还包括提供安全服务与安全工程的组织	完整信息系统：整体对象和具体对象
侧重点	细化过程来规避掉可能存在的系统不安全因素	通过已知的系统情况找出可能存在的风险和管理漏洞，



共性

	SSE-CMM	等级保护
目标	尽可能的减少风险产生的几率，增加系统的抵御能力，让系统更安全。	尽可能的减少风险产生的几率，增加系统的抵御能力，让系统更安全。
等级划分	5个能力级别	5个等级



本章总结

- 等级保护的核心观念是保护重点、适度安全，即分级别、按需要重点保护重要信息系统，综合平衡安全成本和风险，提高保护成效。
- 在等级保护的基本方法中要注意分区域分等级安全保护、内部保护和边界保护和网络安全保护。
- 根据GB 17859《计算机信息系统安全保护等级划分准则》，我国计算机信息系统安全保护划分为5个等级。
- 在信息系统安全等级保护建设中，一定要按照《信息系统安全等级保护基本要求》，参照相关标准和规范要求开展工作。



课堂作业

- 1、什么是信息安全等级保护？
- 2、实行信息安全等级保护的意義有哪些？
- 3、信息安全等级保护的原则是什么？
- 4、简单描述信息系统安全等级保护体系。
- 5、等级保护的基本原理是什么。
- 6、我国信息系统安全等级是如何划分的，简述每一级的内容。
- 7、简要概述信息安全定级的步骤。