



信息安全导论

第十二章 信息安全等级保护与信息系统安全工程

黄 珮



温故：信息安全研究内容

管理规范

法律和法规

管理研究

内容安全

网络与系统安
全

应用研究

密码学

信息隐藏

基础研究



知新

- 等级安全保护
 - 既是管理规范，也有对应的行政法规
 - 同时也有对应的测评标准
 - 安全操作系统与系统安全加固
- 信息系统安全工程
 - 信息安全管理规范



本章内容提要

- 信息安全等级保护综述
- 等级保护的设计与应用
- 信息系统安全工程
- 系统安全工程-能力成熟度模型（SSE-CMM）



引言

- 国家信息化领导小组关于加强信息安全保障工作的意见
 - 我国信息保障工作的纲领性文件
 - 综合平衡安全风险和成本
- 信息系统安全等级保护主要内容
 - 国家对涉及国家安全和社会稳定与安全，公民、法人和其他组织的合法权益的信息系统，按其重要程度和实际安全需求，分级、分类、纵深采取保护措施，保障信息系统安全正常运行和信息安全



信息系统等级安全保护应用指南

- 明确责任，共同保护
- 依照标准，自行保护
- 同步建设，动态调整
- 指导监督，重点保护



等级划分

- 《信息安全等级保护管理办法》
—公安部等四部门，2007年6月发布
- 国家的核心信息系统
—第四、第五级，最高级别安全保护

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



等级安全基本安全保护能力要求描述

- 第一级：应能够防护系统免受来自个人的、拥有很少资源的威胁源发起的恶意攻击，一般的自然灾害，以及其他相当危害程度的威胁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：应能够防护系统免受来自**外部小型组织**的、拥有**少量资源**的威胁源发起的恶意攻击，一般的自然灾害，以及其他相当危害程度的威胁所造成的重要资源损害，能够**发现重要的安全漏洞和安全相关事件**，在系统遭到损害后，能够在**一段时间内**恢复部分功能
- 第三级：应该能在**统一安全策略**下防护系统免受来自**外部有组织**的团体、拥有**较为丰富资源**的威胁源发起的恶意攻击，**较为严重的自然灾害**，以及其他相当危害程度的威胁所造成的主要资源损害，能够**发现安全漏洞和安全相关事件**，在系统遭到损害后，能够**较快恢复绝大部分**功能



等级安全基本安全保护能力要求描述

- 第四级：应该能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、拥有丰富资源的威胁源发起的恶意攻击，严重的自然灾害，以及其他相当危害程度的威胁所造成的资源损害，能够发现安全漏洞和安全相关事件，在系统遭到损害后，能够迅速恢复所有功能
- 第五级：简单地说，是在第四级的安全保护能力的基础上，由访问控制监视器实行访问验证，采用形式化技术验证相应的安全保护能力确实得到实现



等级保护相关法规标准

- 《中华人民共和国计算机信息系统安全保护条例》
—1994年国务院颁布
- 《国家信息化领导小组关于加强信息安全保障工作的意见》
—中办发[2003]27号文件
- 《关于信息安全等级保护工作的实施意见》
—2004年，进一步明确了信息安全等级保护制度的基本内容



等级保护相关法规标准

- 《信息安全等级保护管理办法》
 - 2006年3月，正式实施
- 技术标准
 - 《计算机信息系统安全保护等级划分准则》
 - GB 17859-1999
 - 安全产品的开发、具体标准的制定、安全系统的建设与管理、相关法律法规及其执法提供技术指导和基础
 - 《信息系统安全等级保护基本要求》
 - GB/T 22239-2008
 - 《信息系统等级保护安全设计技术要求》



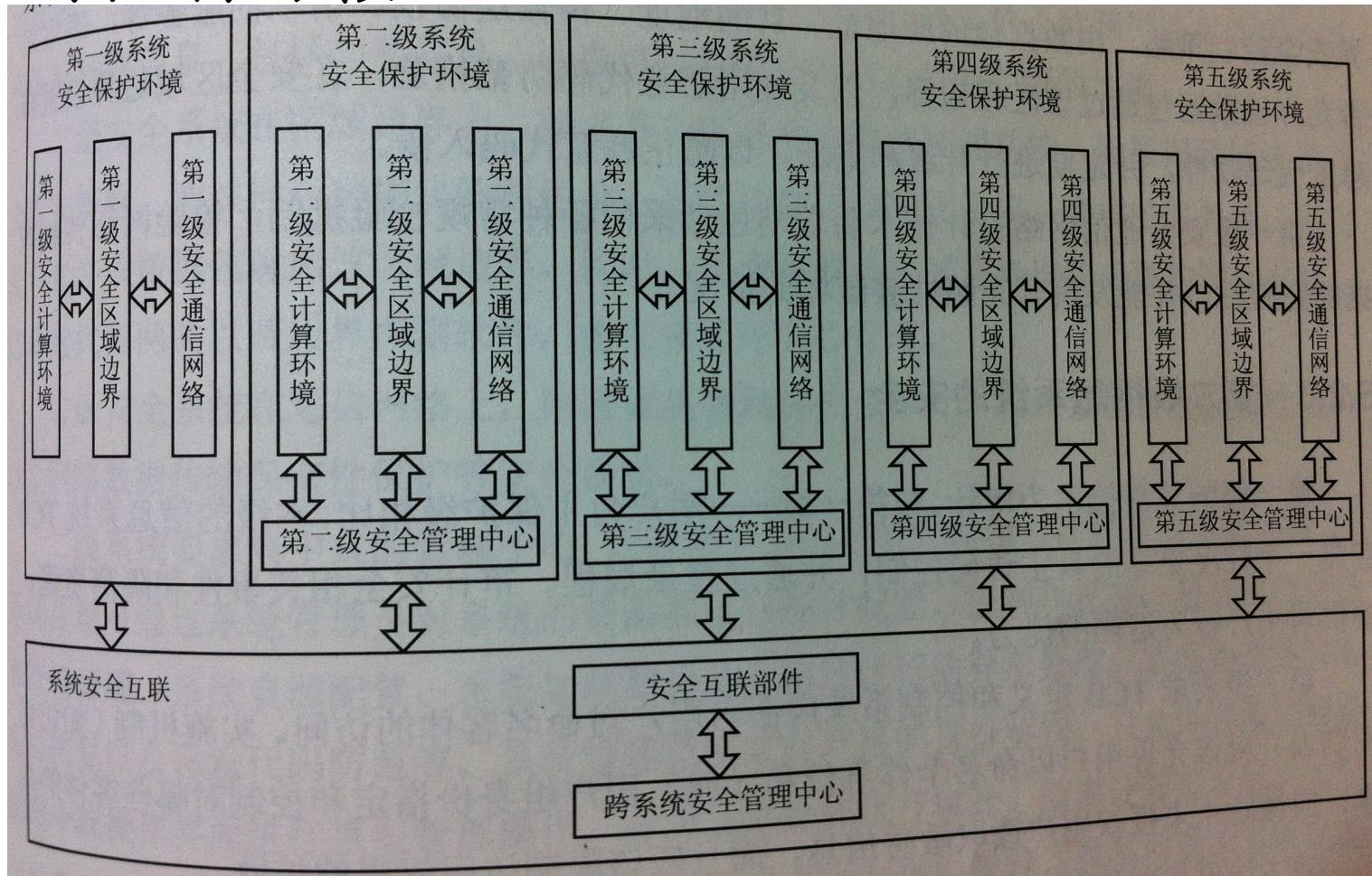
信息系统安全等级保护基本要求

- 基本技术要求
 - 物理安全、网络安全、主机安全、应用安全和数据安全
- 基本管理要求
 - 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



信息系统等级保护安全设计技术要求

• 访问控制为核心





等级保护的技术要求细节

- 等级保护安全技术要求在可信计算基（TCB）上实现
 - 系统的安全机制作为可信计算基的一部分，应考虑在操作系统层面实现
- 一个中心、三层纵深防御体系
 - 安全管理中心
 - 安全计算环境、安全区域边界及安全通信网络



第一级信息系统的安全

- 用户自主保护级
 - 自主访问控制
- 安全计算环境
 - 一般性的口令鉴别、主体粒度为用户/用户组、客体粒度为文件和数据库表的自主访问控制机制、采用常规校验方法的用户数据完整性保护机制、恶意代码防范软件
- 安全区域边界
 - 区域边界包过滤技术、恶意代码防范软件
- 安全通信网络
 - 常规校验机制



第二级信息系统的安全

- (强) 审计
 - 审计加强的自主访问控制
- 安全计算环境
 - 受保护客体的访问审计轨迹完整性保护、细粒度审计
- 安全区域边界
 - 协议识别与过滤机制
- 安全通信网络
 - 网络安全审计、网络数据传输完整性保护以及网络数据传输保密性保护等
- 集中式的安全管理中心



第三级信息系统的安全

- 高安全级别信息系统
 - 强制访问控制
 - 安全策略模型、数据标记以及主体对客体强制访问控制的非形式化描述
 - 系统管理员、安全管理员和审计管理员三权分立
- 免疫恶意代码
 - 以BLP模型为例
 - 即使可写入恶意代码，但无法将秘密信息偷走
 - 不应安装第三方安全防护软件
 - 不符合Biba模型，安装后反而会引入漏洞



第四级信息系统的安全

- 结构化保护级
 - 安全功能要求与第三级基本相同，但在安全保障上有所加强
 - 防止来自系统内部的攻击
- 最小化授权原则



第五级信息系统的安全

- 访问验证保护级
 - 访问监控器
 - 基于形式化验证技术
 - 在第四级安全保护的基础上，实现访问监控器，仲裁主体对客体的访问



小结 (1/2)

- 信息安全等级保护制度是国家在国民经济和社会信息化的发展过程中，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健康发展的一项重要制度
- 等级保护不仅是对信息安全产品或系统的检测、评估及定级，更重要的是，它是围绕信息安全保障全过程的一项基础性管理制度



小结 (2/2)

- 第一级保护
 - 普通个人电脑、小流量网站、非重要网站
 - 第二级保护
 - 大流量网站、学校招生网站
 - 第三级保护
 - 电子政务网站
 - 第四级保护
 - 第五级保护
- 银行数据中心、军队数据中心。。。。



本章内容提要

- 信息安全等级保护综述
- 等级保护的设计与应用
- 信息系统安全工程
- 系统安全工程-能力成熟度模型（SSE-CMM）



第一级安全保护环境主要产品类型及功能

表 6-2 第一级系统安全保护环境主要产品类型及功能

使 用 范 围	安 全 功 能	产 品 类 型
安全计算环境	用户身份鉴别	操作系统、数据库管理系统等
	自主访问控制	
	用户数据完整性保护	
	恶意代码防范	主机防病毒软件*等
安全区域边界	区域边界包过滤	防火墙、网关等
	区域边界恶意代码防范	防病毒网关*等
安全通信网络	网络数据传输完整性保护	路由器等

注：其中带“*”的项表示其设备的功能可在信息系统安全设计技术方案中统一考虑。



第二级安全保护环境主要产品类型及功能

表 6-3 第二级系统安全保护环境主要产品类型及功能

使 用 范 围	安 全 功 能	产 品 类 型
安全计算环境	用户身份鉴别	操作系统、数据库管理系统、安全审计系统*、身份鉴别系统等
	自主访问控制	
	系统安全审计	
	用户数据完整性保护	
	用户数据保密性保护	
	客体安全重用	
安全区域边界	恶意代码防范	主机防病毒软件*等
	区域边界协议过滤	防火墙、网关等
	区域边界安全审计	
	区域边界恶意代码防范	防病毒网关*等
安全通信网络	区域边界完整性保护	防非授权外联系统、入侵检测系统等
	网络安全审计	VPN、加密机*、路由器等
	网络数据传输完整性保护	
安全管理中心	网络数据传输保密性保护	
	系统管理	安全管理平台
	审计管理	

注：其中带“*”的项表示其设备的功能可在信息系统安全设计技术方案中统一考虑。



第三级安全保护环境主要产品类型及功能

表 6-4 第三级系统安全保护环境主要产品类型及功能

使用范围	安全功能	产品类型
安全计算环境	用户身份鉴别	操作系统、数据库管理系统、安全审计系统*、终端安全管理*、身份鉴别系统等
	自主访问控制	
	标记与强制访问控制	
	系统安全审计	
	用户数据完整性保护	
	用户数据保密性保护	
	客体安全重用	
安全区域边界	系统可执行程序保护	操作系统等
	区域边界访问控制	安全隔离与信息交换系统、安全网关等
	区域边界协议过滤	
	区域边界安全审计	
安全通信网络	区域边界完整性保护	
	网络安全审计	VPN、加密机*、路由器等
	网络数据传输完整性保护	
	网络数据传输保密性保护	
安全管理中心	网络可信接入	
	系统管理	安全管理平台
	安全管理	
	审计管理	

注：其中带“*”的项表示其设备的功能可在信息系统安全设计技术方案中统一考虑。



第四级安全保护环境主要产品类型及功能

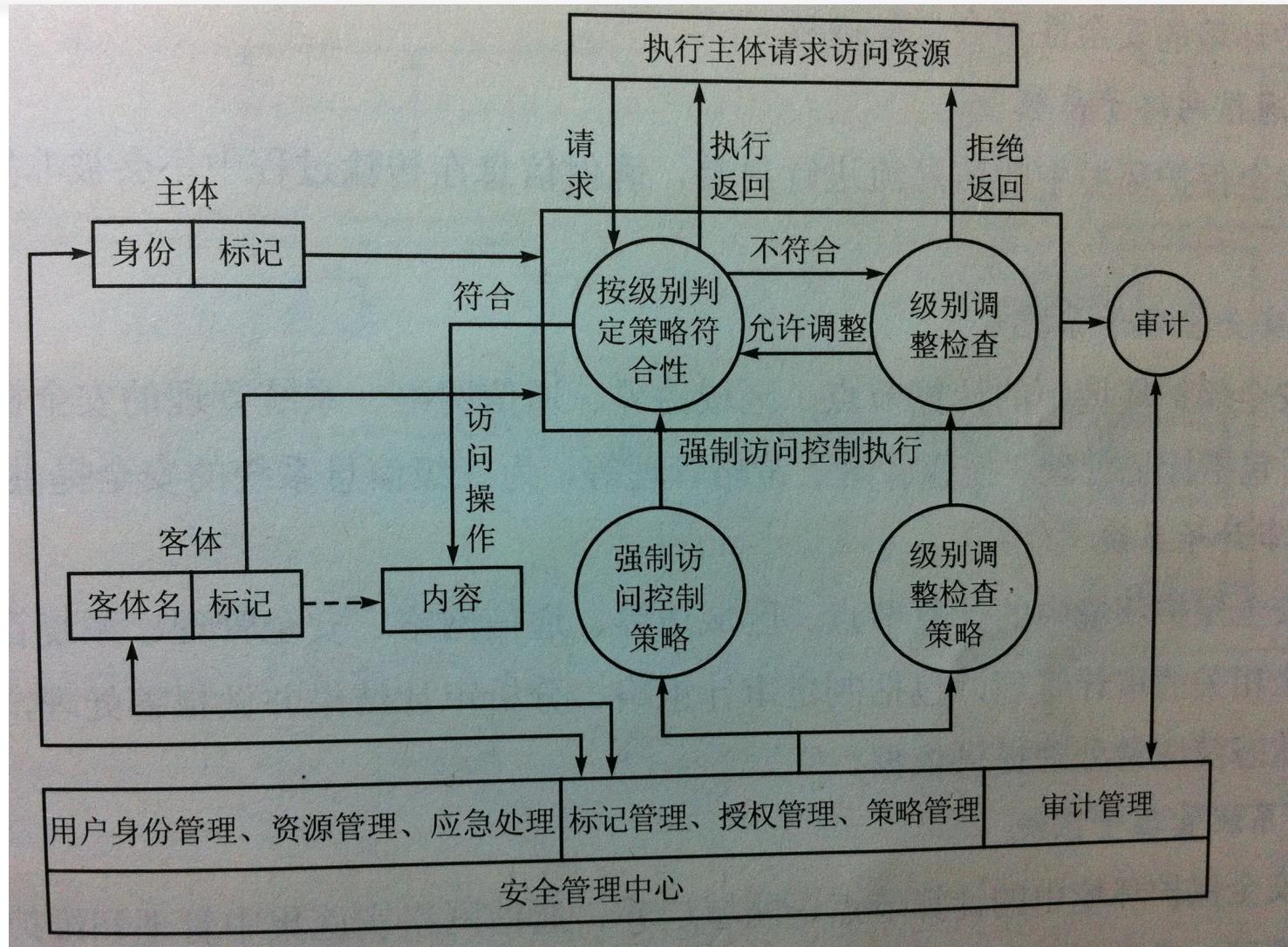
表 6-5 第四级系统安全保护环境主要产品类型及功能

使用范围	安全功能	产品类型
安全计算环境	用户身份鉴别	操作系统、数据库管理系统、安全审计系统*、终端安全管理*、身份鉴别系统等
	自主访问控制	
	标记与强制访问控制	
	系统安全审计	
	用户数据完整性保护	
	用户数据保密性保护	
	客体安全重用	
安全区域边界	系统可执行程序保护	操作系统等
	区域边界访问控制	安全隔离与信息交换系统、安全网关等
	区域边界协议过滤	
	区域边界安全审计	
安全通信网络	区域边界完整性保护	
	网络安全审计	VPN、加密机*、路由器等
	网络数据传输完整性保护	
	网络数据传输保密性保护	
安全管理中心	网络可信接入	
	系统管理	安全管理平台
	安全管理	
	审计管理	

注：其中带“*”的项表示其设备的功能可在信息系统安全设计方案中统一考虑。



强制访问控制流程





本章内容提要

- 信息安全等级保护综述
- 等级保护的设计与应用
- 信息系统安全工程
- 系统安全工程-能力成熟度模型（SSE-CMM）

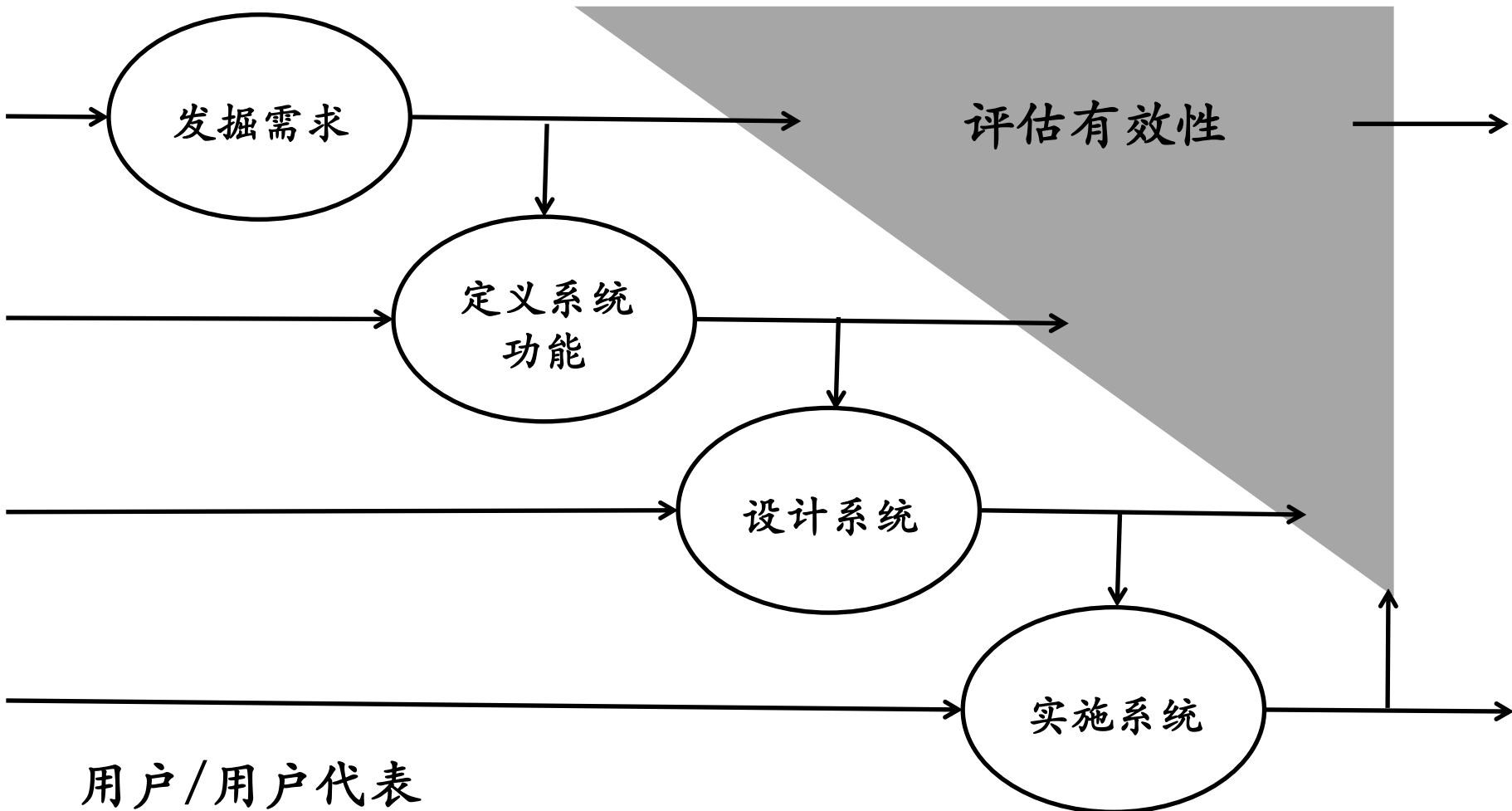


引言

- 信息安全保障问题的解决既不能只依靠纯粹的技术，也不能简单的安全产品的堆砌
—它要依赖于复杂的系统工程——信息安全管理工程
- 信息安全管理工程是采用工程的概念、原理、技术和方法，来研究、开发、实施与维护企业级信息系统安全的过程，是将经过时间考验证明是正确的工程实施流程、管理技术和当前能够做到最好的技术方法相结合的过程



信息系统安全工程基础——系统工程过程





发掘需求

- 信息安全就是为信息化保驾护航，从而能使信息化最终推动组织的任务/业务
 - 微软的SDL



- 信息系统的资产、风险、威胁等要素之间的关系
 - 如果没有价值（资产），不会招来威胁
 - 信息系统安全工程的需求分析就是要找出系统中的所有待保护资产
 - 无形资产、无形资产



定义系统功能

- 目标
 - 有效性 (MoE) 度量
 - 明确、可测和可验证
- 系统背景/环境
 - 系统的物理边界和逻辑边界
 - 系统输入/输出的一般特性
 - 例如：Web软件的系统环境分析



定义系统功能

- 要求 (需求)
 - 功能、性能
 - 质：多好？
 - 量：数量，每个系统的成本多大？
 - 适用范围：Windows? Linux? 版本?
 - 合时性：使用频度，响应度？
 - 有备性：可靠性、可维护性、可用性、可生产性
 - 要求跟踪矩阵 (RTM)
- 功能分析
 - 分析功能之间或功能与环境之间的联系



设计系统

- 短板效应
 - 系统设计必须满足功能、性能、接口、互操作和设计要求在内的一系列要求
- 功能分配
 - 资源计划与调配、配置管理
- 概要设计
- 详细设计



实施系统

- 目的是为所设计的系统开发并集成全部组件
- 主要内容
 - 采购
 - 建设
 - 测试



有效性评估

- 系统是否达到了任务的需求
- 系统是否能够依照组织所期望的方式操作
- 其他因素
 - 互操作性
 - 可用性
 - 训练
 - 人机接口
 - 成本



本章内容提要

- 信息安全等级保护综述
- 等级保护的设计与应用
- 信息系统安全工程
- 系统安全工程-能力成熟度模型 (SSE-CMM)



系统安全工程——能力成熟度模型

- SSE-CMM
 - Systems Security Engineering - Capability Maturity Model
 - 满足信息安全工程过程能力的改进与评估
 - 信息 安全 的 持续 对抗 本 质
 - 衡量 和 不断 改进



SSE-CMM 历史

- SSE-CMM 的基础是CMM
- CMM的1.0版本在1991年8月由卡内基梅隆大学软件工程研究所发布
- 1993年启动研究，1996年10月发布1.0版本
- 1999年4月发布SSE-CMM 2.0版本
- 2003年6月发布SSE-CMM 3.0版本



SSE-CMM的范围

- 可信产品或安全系统的整个生命周期内的安全工程活动
 - 概念定义、需求分析、设计、开发、集成、安装、运行、维护和终止
- 安全产品开发商、安全系统开发商和集成商，以及提供安全服务和安全工程的组织
- 所有类型和大小的安全工程组织，如商业组织、政府组织和学术组织
- SSE-CMM是开放性的，可以向其中不断添加新的安全工程过程及其他相关的过程



SSE-CMM的体系结构——基本模型

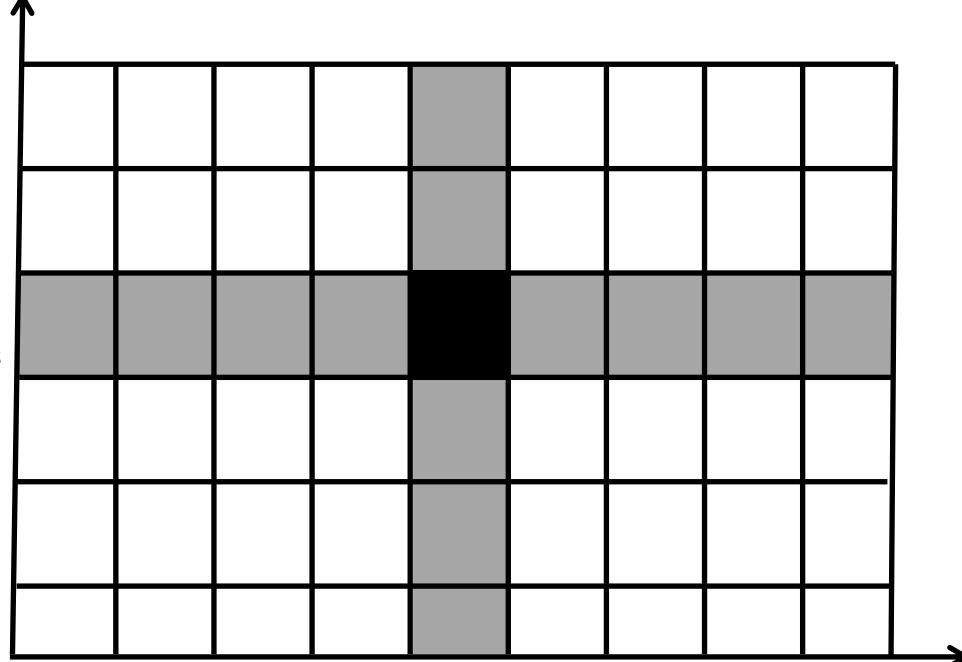
• 两维体系

—域、能力

- 回答了所有交叉点的问题之后，客户便可获知一个安全工程组织的总体工程能力

你的组织在查找系统安全脆弱性时，是否具备必要的资源？

能力维
(通用实施)
Generic Practice



基本实施

由所有定义安全工程的工程实施活动组成

通用实施

组织对过程的管理和制度化能力。这是基本实施过程中必须完成的活动，例如“分配资源”要求



SSE-CMM的体系结构——基本实施及过程域

- SSE-CMM 3.0包含了61个基本实施过程
 - 被归入了11个安全工程过程域 (PA, Process Area)
 - 来源于大量的文献资料、实践经验及专家知识
- SSE-CMM选择的是对安全工程来说非常根本和重要的过程实施行为
 - 应用于企业的整个生命周期
 - 与其他的BP不相互覆盖
 - 代表了安全界的“最好的实施”
 - 不能只简单地反映最新技术
 - 可在多种业务环境下以多种方法运用
 - 不指定具体的方法或工具



SSE-CMM的11个过程域

- | | |
|------------|--------------|
| (1) 管理安全控制 | (7) 协调安全 |
| (2) 评估影响 | (8) 监视安全态势 |
| (3) 评估安全风险 | (9) 提供安全输入 |
| (4) 评估威胁 | (10) 确定安全需求 |
| (5) 评估脆弱性 | (11) 验证与确认安全 |
| (6) 建立安全论据 | |



SSE-CMM的体系结构——通用实施与公共特征

- 通用实施被归入了12个不同的逻辑域，称为“公共特征”（Common Feature）
 - 分为5个能力级别，代表了依次增长的安全工程能力

能力级1

➤ 1.1 执行基本实施

能力级2

➤ 2.1 规划执行

➤ 2.2 规范化执行

➤ 2.3 验证执行

➤ 2.4 跟踪执行

能力级3

➤ 3.1 定义标准过程

➤ 3.2 执行既定的过程

➤ 3.3 协调过程

能力级4

➤ 4.1 建立可测量的质量目标

➤ 4.2 客观地管理执行

能力级5

➤ 5.1 改进组织的能力

➤ 5.2 改进过程的有效性



通用实施、公共特征、能力级别的关系



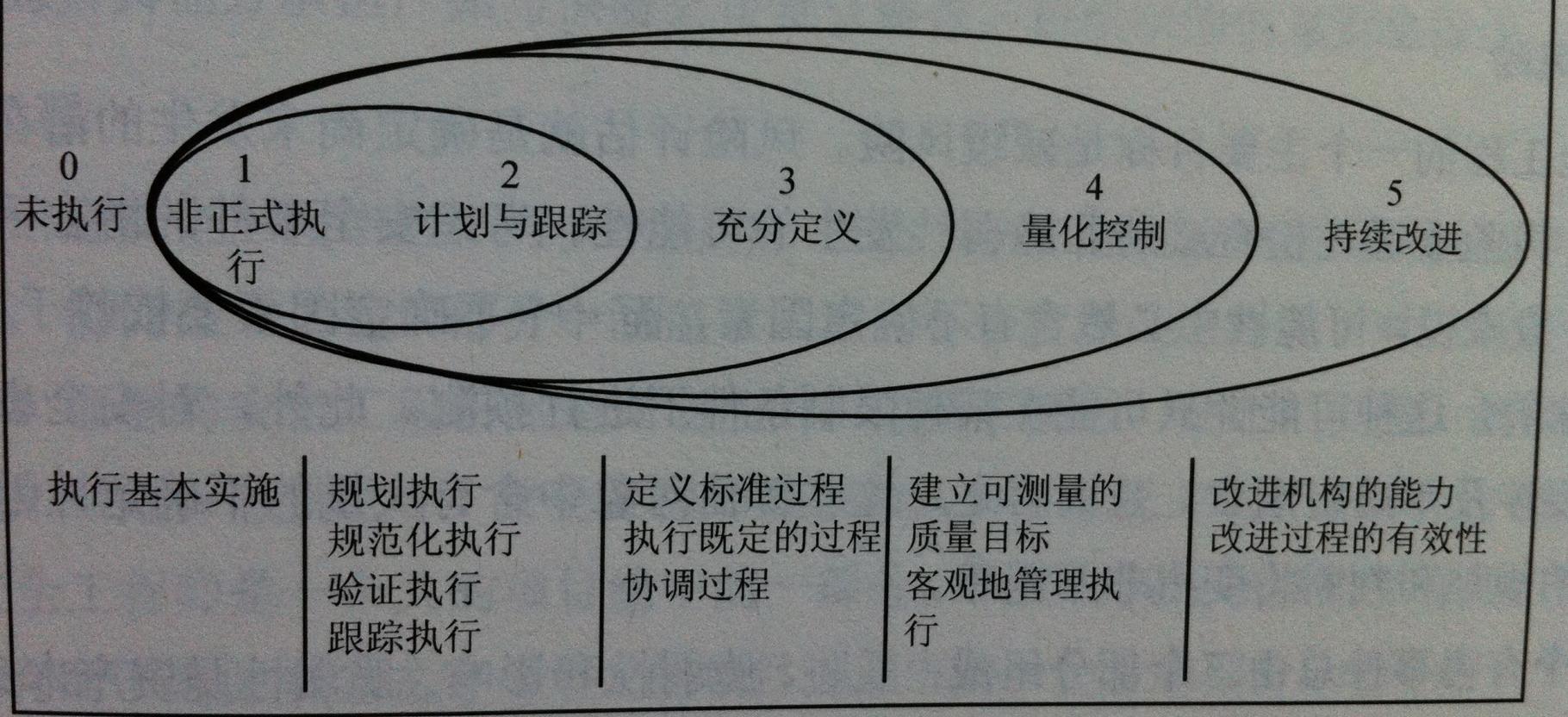
以实施或制度化为手段来提高工程过程的实施能力

通用实施的集合，每一集合中的公共特征面向的是同一类过程的管理和制度化问题

若干个（第1级是一个）公共特征的组合，显示了安全工程过程的实施能力级别



SSE-CMM的五个能力级别及其包含的公共特征





安全工程过程的三个主要部分

风险过程将标识出所开发的产品或系统中存在的危险并将这些危险进行优先级排序

针对危险所可能导致的问题，安全工程过程要与其他工程方法一起合作，确定并实施解决方案

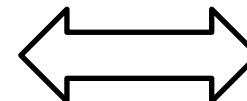
安全保证过程将为解决方案建立起信任度，并将这种信任转达给客户

产品或服务

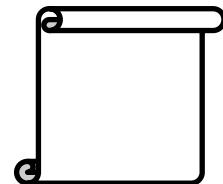


工程过程

机制



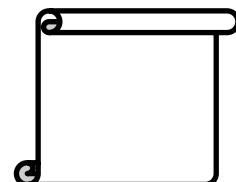
保证过程



测试

风险过程

策略



保证论据

风险信息