主要内容

- 信息安全基本概念
- 信息安全的现状
- 什么是信息安全工程

安全问题的解决

- 不能只依靠纯粹的技术
- 也不能靠简单的安全产品的堆砌
- 也不能仅靠安全管理体系建设

复杂的系统工程——信息安全工程

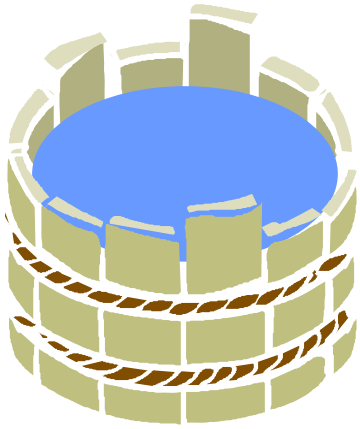
信息安全工程

- 信息安全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践流程、管理技术和当前能够得到的最好的技术方法相结合的过程。

- 信息安全工程是信息安全保障建设的全部问题集

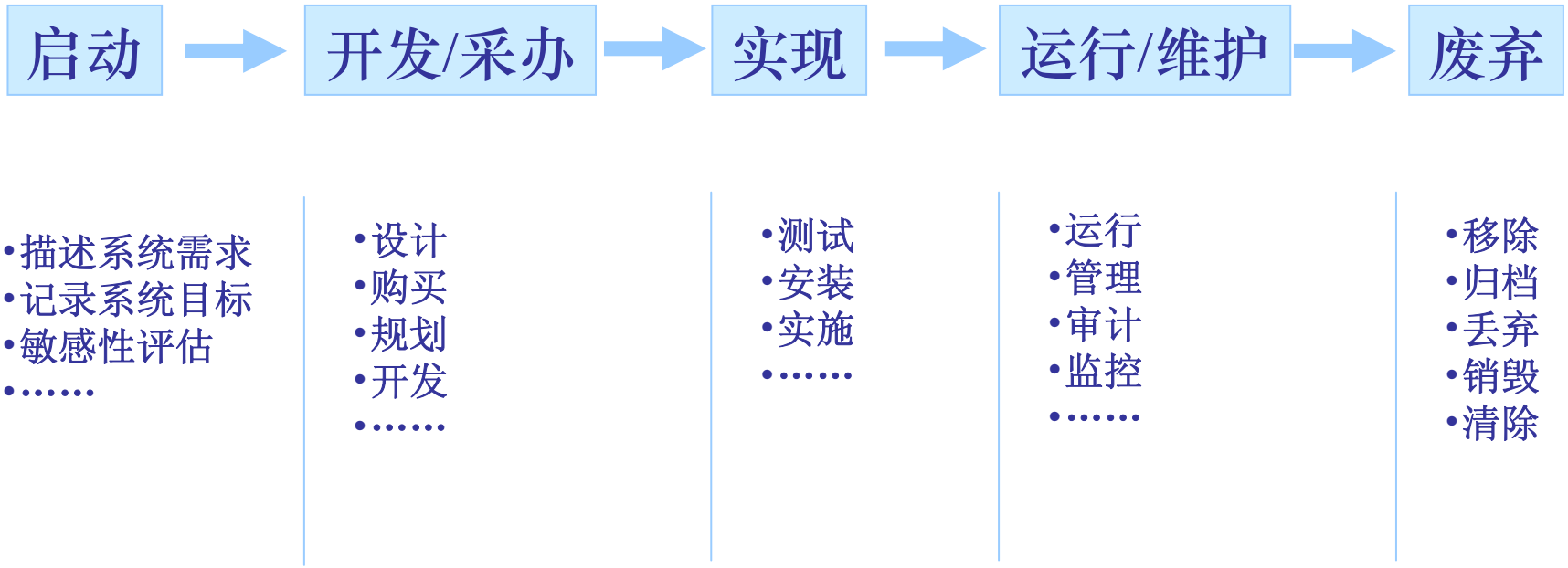
为什么需要信息安全工程?

- 由信息安全特性决定
  - 社会性
  - 全面性
  - 过程性或生命周期性
  - 动态性
  - 层次性
  - 相对性

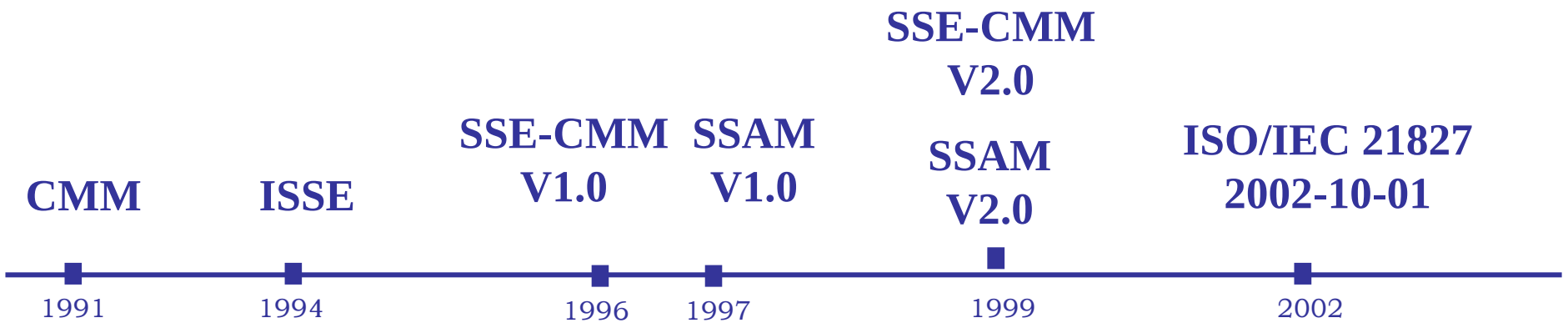


生命周期

系统生命周期通常有以下几个阶段组成：

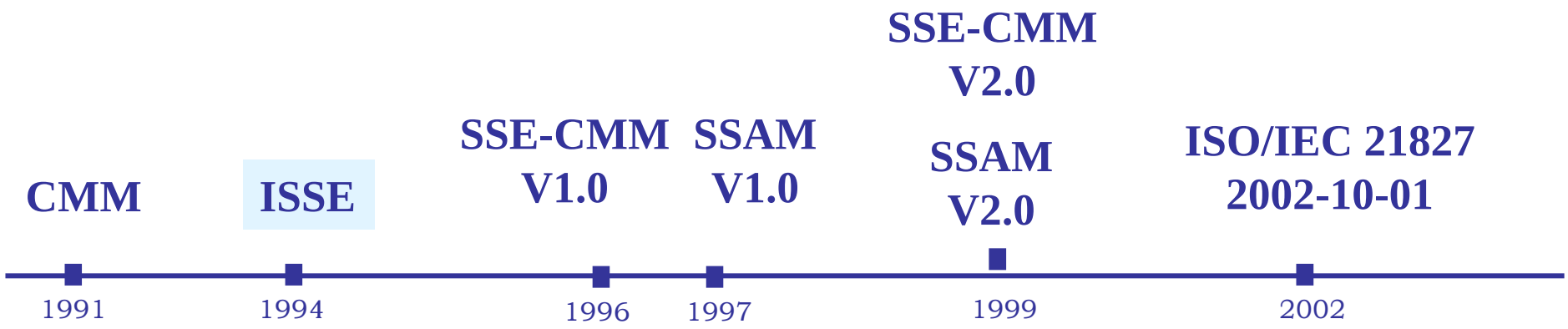


信息安全工程的发展



- ISSE：Information Systems Security Engineering
- SSE-CMM：Systems Security Engineering – Capability Maturity Model
- SSAM：SSE-CMM Appraisal Method

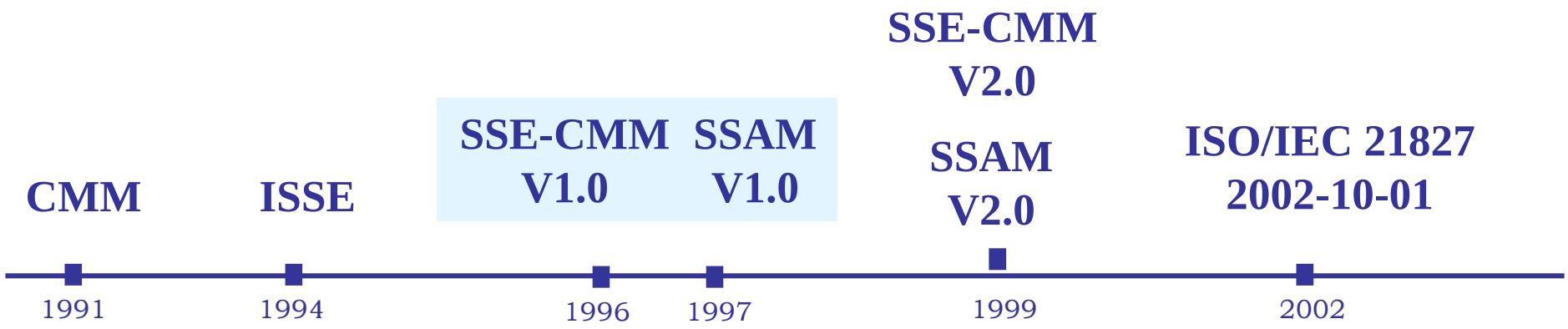
信息安全工程的发展



ISSE

- 由系统工程（SE）发展而来
- 以时间维划定工程元素的方法学

信息安全工程的发展



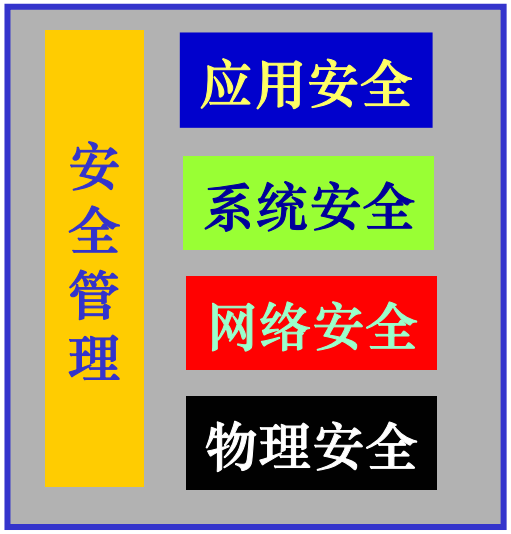
■ SSE-CMM

- 由能力成熟度模型（CMM）发展而来
- 以工程域维和能力维来诠释信息安全工程过程的方法学

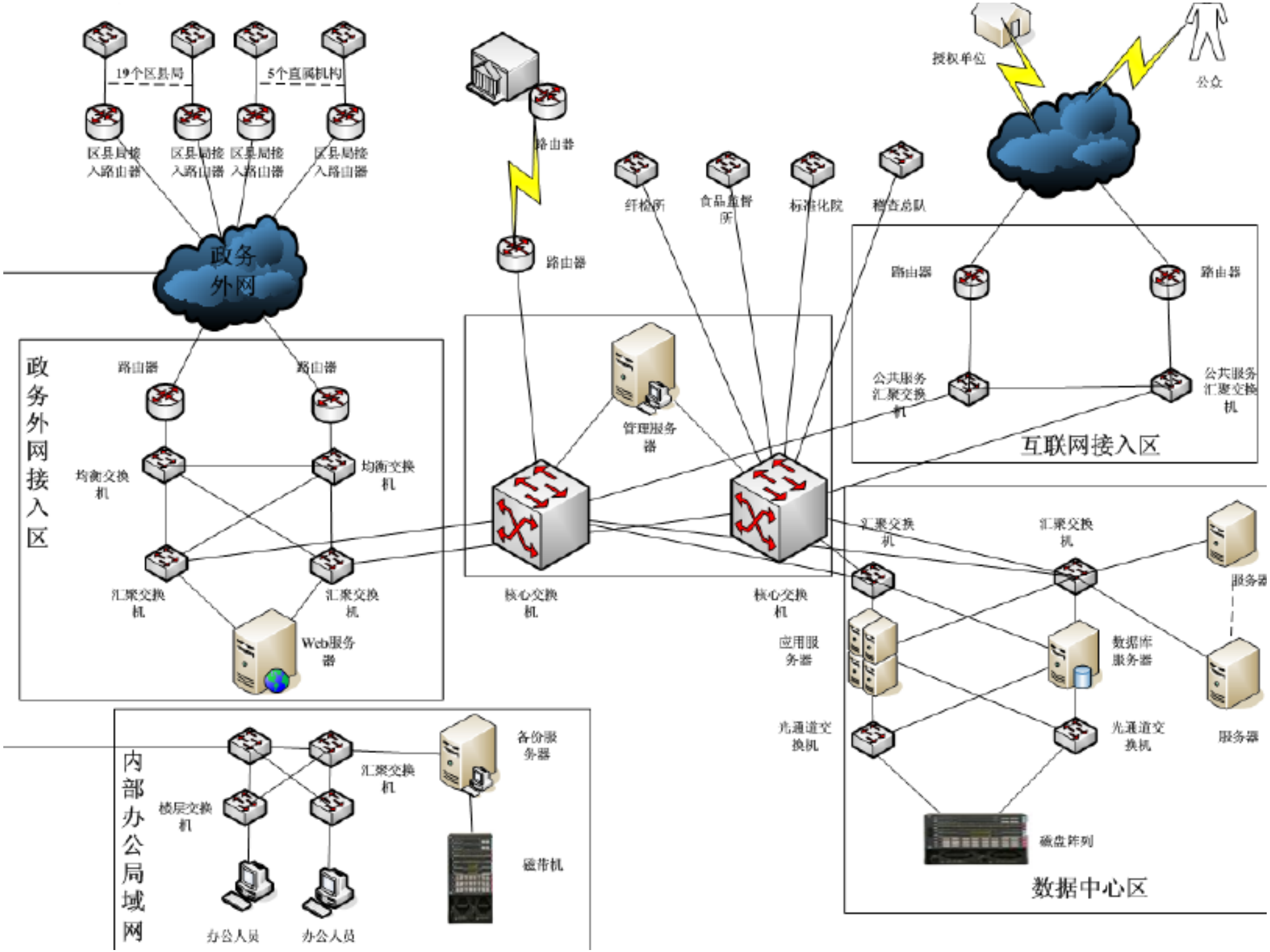
主要应用领域

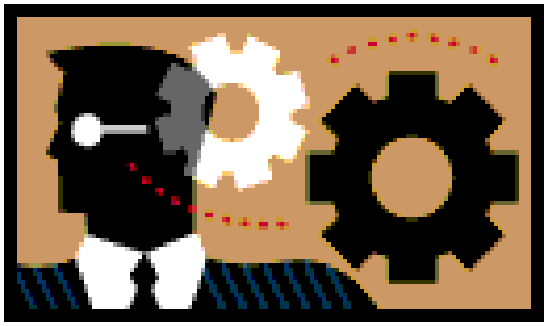
- 政府职能部门
- 电信、电力、交通等基础设施
- 金融、证券、电子商务
- 制造业
- 科教文卫
- 个人

安全体系一般构成



UPS备用电源
数字证书
Web保护
防火墙
IP-SEC VPN
保密协议
漏洞扫描
防病毒系统
SSL VPN
主机审计
消防系统
监控与报警系统
风险评估
IDS IPS
防垃圾邮件
网闸
门禁系统
网管系统
安全培训
系统升级与补丁更新
内容监管
通信线路保护
网络安全审计
安全管理机构
电子签章
系统安全配置


19个区县局
5个直属机构
区县局接入路由器
区县局接入路由器
区县局接入路由器
区县局接入路由器
政务外网
路由器
路由器
均衡交换机
均衡交换机
汇聚交换机
汇聚交换机
Web服务器
政务外网接入区
路由器
纤检所
食品监督所
标准化院
稽查总队
管理服务器
核心交换机
核心交换机
授权单位
公众
路由器
路由器
公共服务汇聚交换机
公共服务汇聚交换机
互联网接入区
汇聚交换机
汇聚交换机
服务器
应用服务器
数据库服务器
光通道交换机
光通道交换机
服务器
磁盘阵列
数据中心区
内部办公局域网
核层交换机
汇聚交换机
备份服务器
磁带机
办公人员
办公人员



Q&A

关于DNS系统面临严重安全漏洞风险的紧急公告

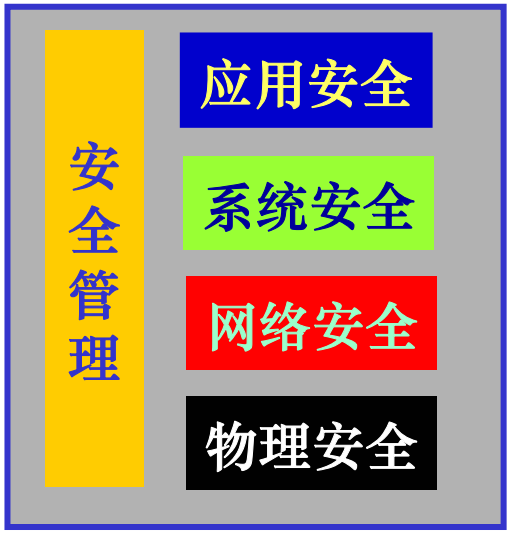
- 漏洞描述：

2008年7月9日以来，思科、微软、ISC等互联网域名解析服务软件厂商纷纷发布了安全公告，称其DNS软件存在高危漏洞，攻击者可以通过猜测DNS解析过程中的报文序列号来伪造DNS权威服务器的应答，从而达到“污染”高速缓存（Cache）中的记录的目的，即将错误的域名指向信息注入DNS服务器，最终导致受到污染的DNS服务器将对外提供错误的解析结果。该种攻击方式可造成域名劫持攻击，使得公众在不知情的情况下通过域名访问到黑客指定的网站，面临网络钓鱼和网页木马等一系列严重的安全威胁。

7月22日，针对该漏洞的探测程序被发布，7月23日，针对该漏洞的完整攻击程序被发布，并随后广泛流传。我中心经过初步测试后发现，在带宽良好情况下，该攻击程序对存在漏洞的DNS服务器只需数分钟就可完成攻击，受攻击目标会瞬时接到大量攻击报文，容易被误判为“query flood”方式的拒绝服务攻击。

鉴于该安全事件形势严峻且发展迅速，为确保我国互联网的运行安全，请各相关单位迅速采取适当措施，对所运行的DNS服务器进行必要的安全加固，并加强异常监测和处置。

安全体系



UPS备用电源

数字证书

Web保护

防火墙

IP-SEC VPN

漏洞扫描

保密协议

防病毒系统

SSL VPN

主机审计

消防系统

风险评估

监控与报警系统

IDS IPS

门禁系统

网闸

防垃圾邮件

系统升级与补丁更新

安全培训

网管系统

网络安全审计

通信线路保护

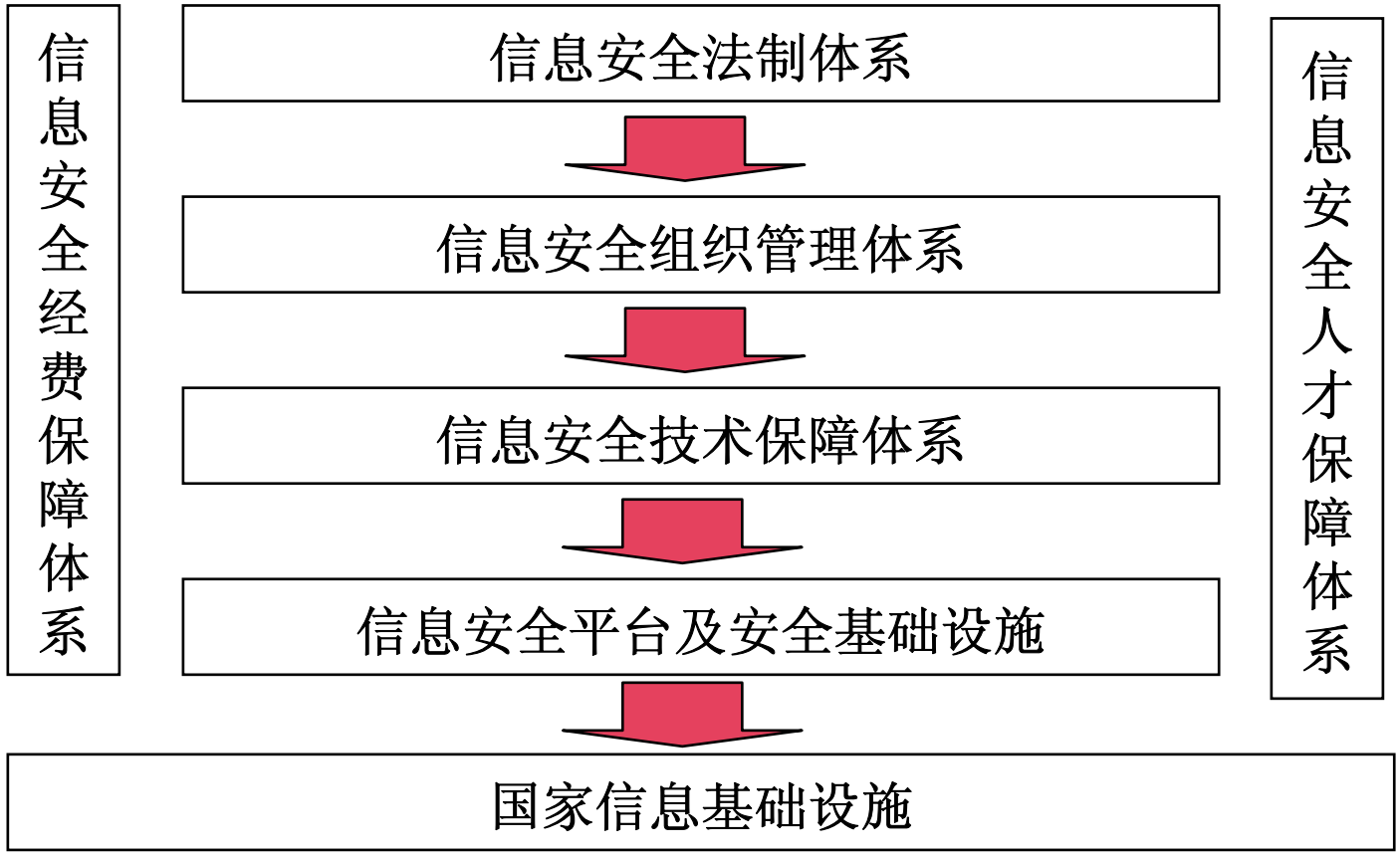
内容监管

安全管理机构

电子签章

系统安全配置

我国信息安全保障体系的基本构架



四个层面，两个支撑，一个确保