第 24 章 信息系统安全和安全体系

信息系统安全三维空间	信息系统安全架构体系	信息系统安全支持背景	信息安全保障系统定义
信息系统安全三维空间 Y 轴：OSI（开放式系统互连）网络参考模型 X 轴：安全机制 Z 轴：安全服务 X、Y、Z 三个轴形成空间就是信息系统的“安全空间”，这个空间具有五个要素：认证、权限、完整、加密和不可否认。 1、 安全机制 第一层：基础设施实体安全 机房安全、场地安全、设施安全、动力系统安全、灾难预防与恢复 第二层：平台安全 操作系统、网络设施、应用程序、安全产品 第三层：数据安全 介质和载体安全、数据访问控制、数据完整性、 数据可用性、数据监控和审计、数据存储和备份 第四层：通信安全 第五层：应用安全 安全性测试、防抵赖测试、安全验证测试、身份鉴别测试、恢复机制检查、保密性测试、可靠性测试、可用性测试 第六层：运行安全 第七层：管理安全 人员管理、培训管理、应用系统管理、软件管理、设备管理、 文档管理、数据管理、操作管理、 运作管理、机房管理 第八层：授权和审计安全 第九层：安全防范体系 核心：实现企业信息安全资源的综合管理 即 EISRM 六项能力：预警、保护、检测、反应、恢复和反击 WPDRRC 能力模型：从**人员、技术和政策**三大要素来构成宏观的信息网络安全保障体系结构的框架 2、 安全服务 对等实体认证服务、数据保密服务、数据完整性服务、数据源点认证服务、禁止否认服务 3、 安全技术 加密技术、数据签名技术、访问控制技术、数据完整性技术、认证技术	1、 MIS+S：初级信息安全保障系统 特点：⊙应用基本不变 ⊙软硬件通用 ⊙安全设备不带密码（不使用 PKI/CA） 2、 S-MIS：标准信息安全保障系统 特点：⊙软硬件通用 ⊙PKI/CA 安全保障系统必须带密码 ⊙应用系统必须根本改变（即按照 PKI/CA 的标准重新编制的应用信息系统） 3、 S^2-MIS 特点：⊙软硬件专用 ⊙PKI/CA 安全保障系统必须带密码 ⊙应用系统必须根本改变（即按照 PKI/CA 的标准重新编制的应用信息系统） ⊙主要硬件和系统软件需要 PKI/CA 认证		