Note

0x01 网络与信息安全概述

信息安全的基本要素

机密性
完整性
可用性
可控性
可审查性

还扩展为 可鉴别性、不可抵赖性、可靠性

信息安全的目标和功能

为了实现上述的五个基本目标，网络应具备防御、监测、应急、恢复等基本功能

信息安全理论基础

通用理论基础： 数学、信息理论、计算理论
特有理论基础： 访问控制理论、博弈论、密码学

信息系统安全层次

设备安全、数据安全、内容安全、行为安全

信息安全管理

信息安全管理要素：
网络管理对象、网络脆弱性、网络威胁、网络风险、网络保护措施等

信息安全管理流程：
识别安全管理对象 > 识别价值威胁脆弱性 > 构建防范措施 > 实施措施 > 安全运维

系统可靠性涉及的概念

1. 常见概念：平均无故障时间、平均修复时间、平均失效间隔、失效率。

2. 系统可靠性：串联系统、并联系统、模冗余系统。
3. 容错技术： 软件容错、硬件容错、数据容错。
4. 容灾：目的是保持信息系统的业务持续性。

网络安全等级保护

等级保护中的安全等级，主要是根据 ***受侵害的客体*** 和 ***对客体的侵害程度*** 来划分的
等级保护工作分为五个阶段：

- 定级(又分为五步)
  - 确定定级对象
  - 用户初步定级
  - 组织专家评审
  - 行业主管部门审核
  - 公安机关备案审核
- 备案
- 等级测评
- 安全整改
- 监督检查

等保2.0 新特点

> 总体设计思路： 一个中心，三重防护
> 增加了 “可信验证” 控制点　一级到四级逐步增加
>
> 各级技术要求：安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心
>
> 各级管理要求：安全管理制度、安全管理机构、安全管理人员、安全建设管理、安全运维管理

0x02 法律法规

安全法规

> 侵入国家事务、国防建设等信息系统 三年以下
> 获取数据严重的三年以下，特别严重的 三年以上七年以下
> 对原有系统功能进行增删改查导致不能运行的 严重处 五年以下，特别严重处五年以上有期徒刑。
>
> 帮助信息网络犯罪活动罪： 三年以下有期徒刑或拘役

信息系统安全保护等级划分

- 用户自主级

自主访问控制、身份鉴别、数据完整性

- 系统审计保护级

自主访问控制、身份鉴别、客体重用、审计、数据完整性

- 安全标记保护级

自主访问控制、强制访问控制、标记、身份鉴别、客体重用、审计、数据完整性

- 结构化保护级

自主访问控制、强制访问控制、标记、身份鉴别、客体重用、审计、数据完整性、隐蔽信道分析、可信路径

- 访问验证保护级

自主访问控制、强制访问控制、标记、身份鉴别、客体重用、审计、数据完整性、隐蔽信道分析、可信路径、可信恢复