安全体系结构 参考图

# 1.1 CIA三元组

保密性、完整性、可用性（CIA三元组）经常被视为安全基础架构中主要的目标和宗旨。 安全控制评估通常用于评价这三个核心信息安全原则的符合情况。对脆弱性和风险的评估也基于它们对一个或多个CIA三元组原则的威胁。

## 1.1.1 保密性

保密性指为保障数据、客体或资源保密状态而采取的措施。保密性保护的目标是阻止或最小化**未经授权的数据访问**。 保密性在保护授权访问的同时防止泄露。

保密性的（部分）相关概念、条件和特征包括：

* 敏感性：指信息的特性，这种特性的数据一旦泄露就会导致伤害或损失。
* 关键性：信息的关键程度是其关键性的衡量标准。关键级别越高，越需要保持信息的保密性。

## 1.1.2 完整性

完整性是保护数据可靠性和正确性的概念。完整性保护措施防止了**未经授权的数据更改**。 恰当实施的完整性保护措施允许合法修改数据，同时可预防故意和恶意的未经授权的活动（如病毒和入侵）以及授权用户的误操作（如错误或疏忽）。

可以从以下三个方面检验完整性：

* 防止未经授权的主体进行修改。
* 防止授权主体进行未经授权的修改（如引入错误）。
* 保持客体内外一致以使客体的数据能够真实反映现实世界，而且与任何其他客体的关系都是有效的、一致的和可验证的。

针对完整性的攻击包括病毒、逻辑炸弹、未授权访问、编码和应用程序中的错误、恶意修改、故意替换以及系统后门。完整性破坏的原因也包括安全策略中的疏漏或配置有误的安全控制。

预防完整性威胁的措施包括严格的访问控制、严格的身份认证流程、入侵检测、客体/数据加密、哈希值验证、接口限制、输入/功能检查和充分的人员培训。

保密性和完整性相互依赖。没有客体完整性（即，不能保证客体不受未经授权的修改），就无法维持客体保密性。

## 1.1.3 可用性

可用性意味着授权主体被授予实时的、不间断的**客体访问权限**。通常，可用性保护控制措施提供组织所需的充足带宽和实时的处理能力。如果安全机制提供了可用性，它就应该能保证数据、客体和资源可被授权主体访问。 可用性包括对客体的有效的持续访问及抵御拒绝服务攻击的能力。可用性还意味着支撑性基础设施（包括网络服务、通信和访问控制机制）是可用的，并允许授权用户获得授权的访问。

在系统上维护可用性，就必须有适当的控制措施以确保授权的访问和可接受的性能水平，以快速处理通信的中断，提供冗余、维护可靠的备份，并防止数据丢失或受损。

可用性面临的威胁包括设备故障、软件错误和环境问题。聚焦与破坏可用性的攻击形式包括DoS攻击、客体破坏和通信中断。

预防可用性威胁的措施包括正确设计正确设计中转传递系统，有效使用访问控制，监控性能和网络流量，使用防火墙和路由器防止DoS攻击，对关键系统实施冗余机制，以及维护和测试备份系统。大多数安全策略以及业务连续性计划（BCP）关注不同级别的访问/存储/安全（即磁盘、服务器或站点）上的容错特性，目标是消除单点故障，保障关键系统的可用性。

可用性依赖于完整性和保密性。

## 1.1.4 真实性和不可否认性

真实性指的是数据是可信/非伪造的，并源自其声称的来源。这一概念与完整性有关，但相对来说关注的是验证数据是否来自声称的来源。 数据具有真实性时，接收者可以高度确信数据来自其声称的来源，并且在传输（或存储）过程中没有发生变化。

不可否认性确保事件的主体或引发事件的人不能否认事件的发生。不可否认性可以预防主体否认发送过消息、执行过动作或导致某个事件的发生。 标识、身份认证、授权、问责制和审计使不可否认性成为可能。可使用数字证书、会话标识符、事务日志以及其他许多事务性机制和访问控制机制来实施不可否认性。

## 1.1.5 DAD三元组

DAD三元组是与CIA三元组相反的一个概念。DAD三元组由泄露（disclosure）、修改（alteration）和破坏（destruction）组成。它代表CIA三元组中安全保护的失败。

* 当敏感或保密资料被未经授权的实体访问时，就会发生泄露，违反了保密性。
* 当数据被恶意或意外更改时，就会发生修改，违反了可用性。
* 当资源被破坏或授权用户无法访问时（技术上通常称之为拒绝服务），就会发生破坏，违反了可用性。

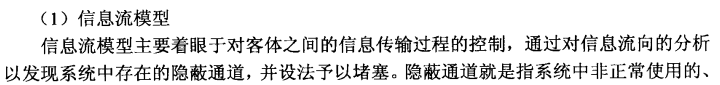
安全模型

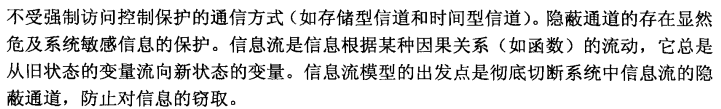
2.1.1 主体和客体

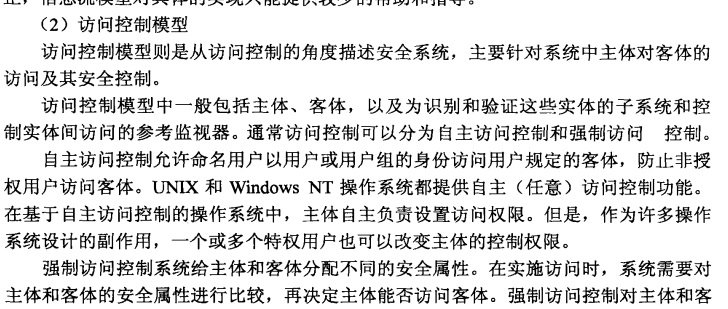
对安全系统中任何资源的访问控制都涉及两个实体：

* 主体：发出资源请求的主动实体。
* 客体：主体想要访问的被动实体。

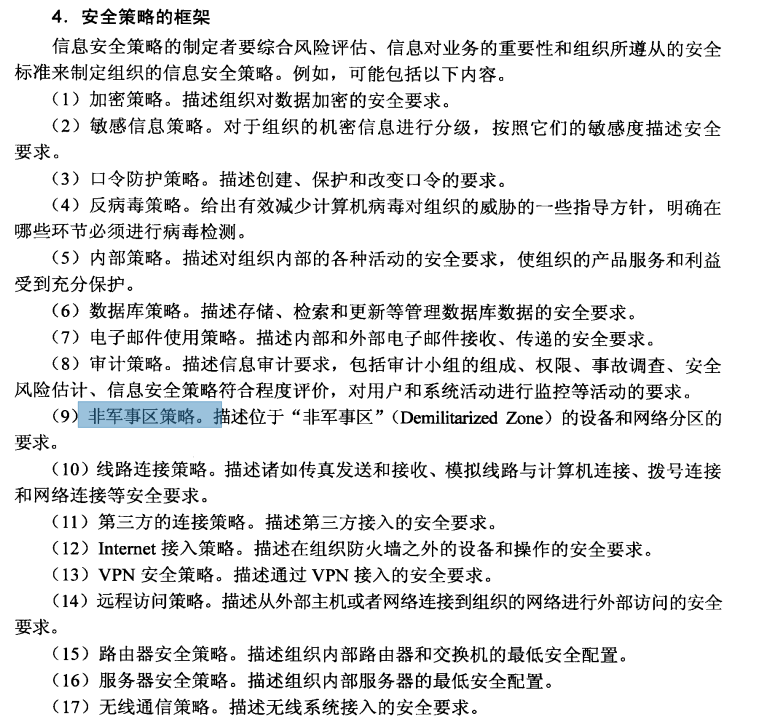
访问是主体和客体之间的一种关系，可能包括读、写、更改、删除等活动。



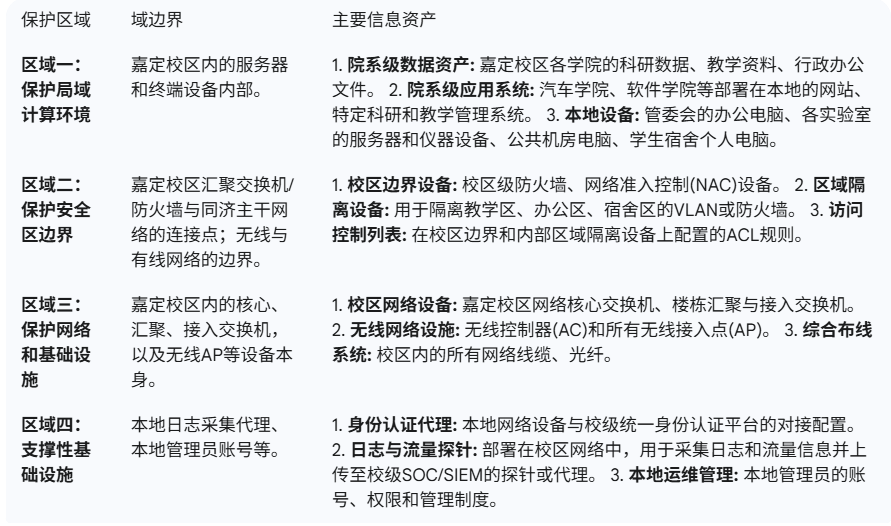




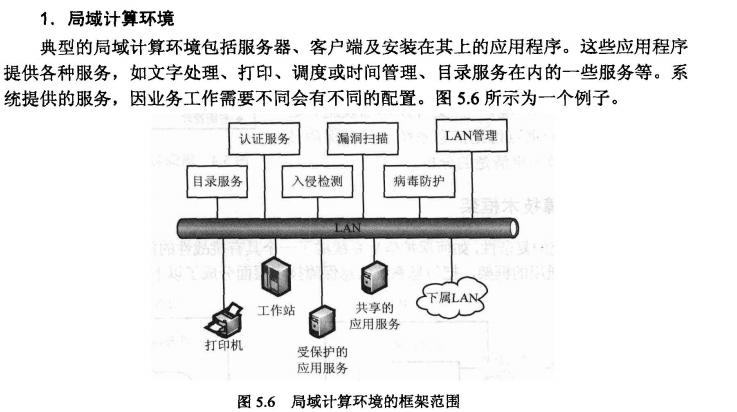
安全策略



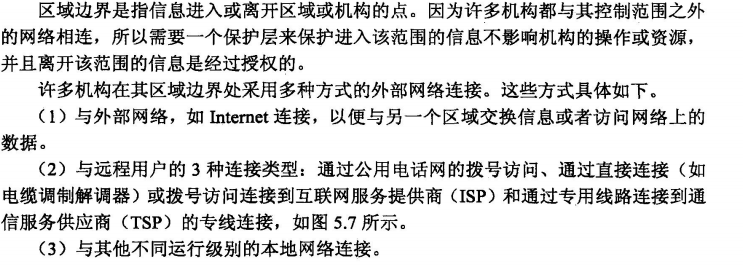
IATF 信息安全保障框架 “三保卫一支撑”

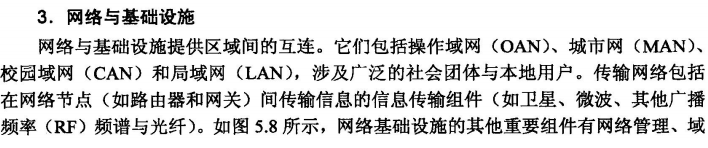


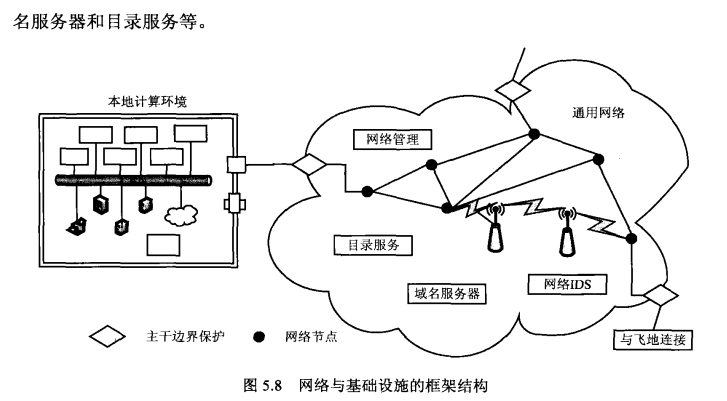
**1.局域计算环境**



**2.区域边界**





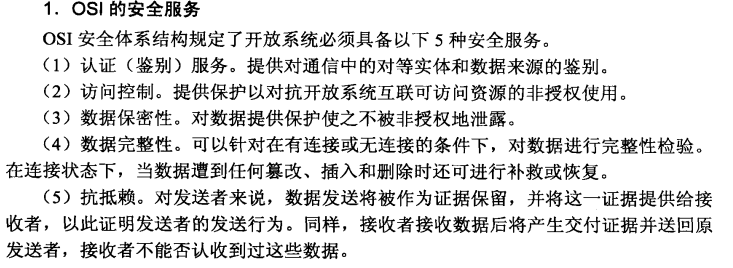


**4.支撑性基础设施**

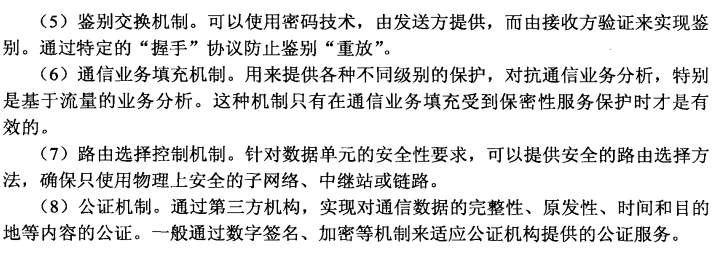
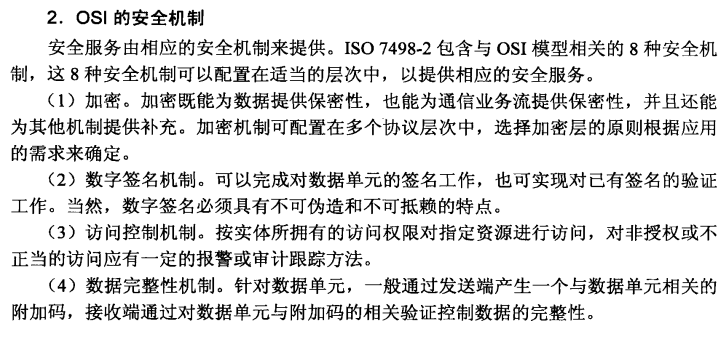


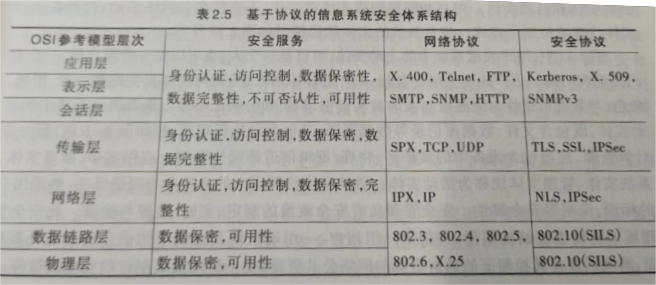
OSI安全体系结构

5类安全服务

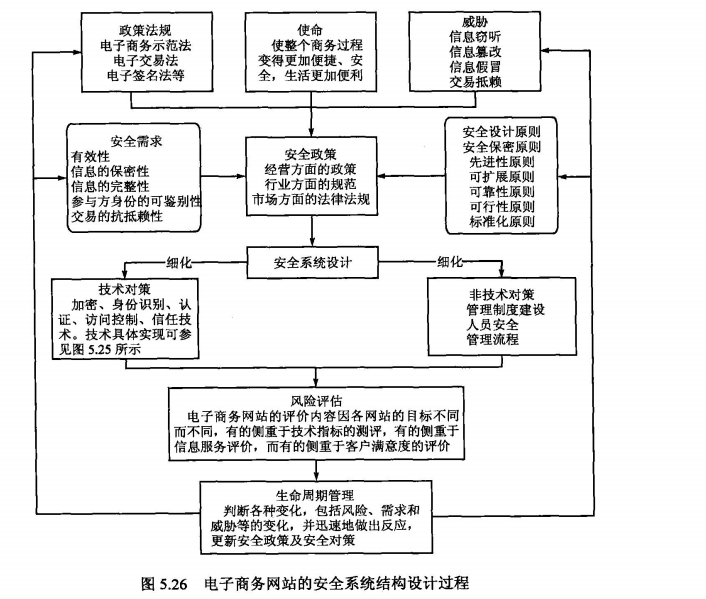


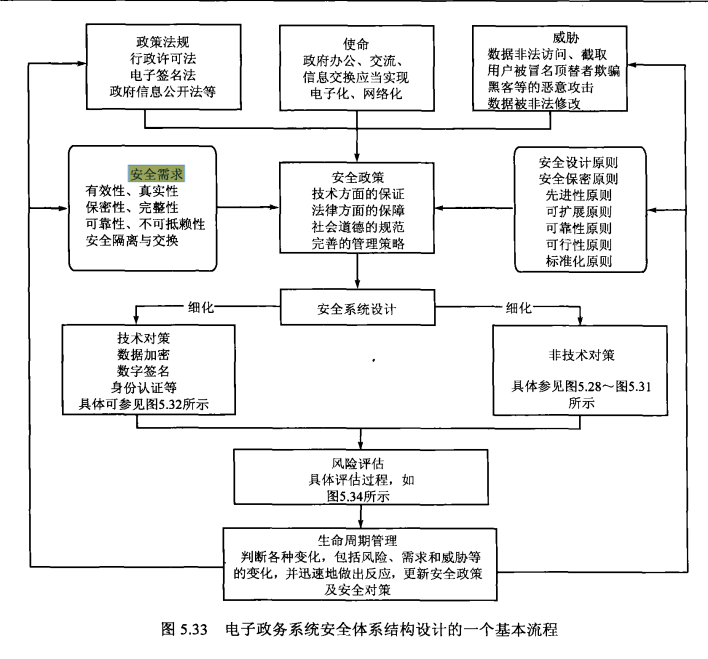
8类安全机制







安全体系结构设计



网络拓扑图

