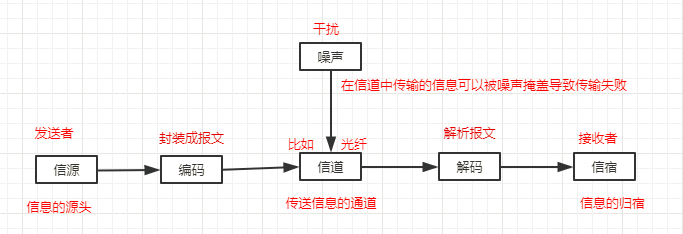
# 信息化与信息系统\*概述

本节课程需要掌握的考点

1. 信息的特征P2（了解）、信息的质量属性p3（掌握）、信息的传输模型P4（掌握）
2. 信息系统的特征 P5（了解）
3. 信息化5个层次 P8、信息化的主体手段途径目标 P8(掌握)
4. 两网、一站、四库、十二金P9 (了解)
5. 信息化六要素及其地位P9-10 (掌握)
6. 信息系统生命周期五个阶段及其内容p10-12(掌握)
7. 信息系统开发方法：结构化、面向对象、原型法、面向服务的方法特征及其优缺点p12-17 （掌握）
8. 计算机网络：OSI协议7层及其作用协议P18、IEEE802协议P18-19、TCP/IP协议4层及其协议作用P19-21、网络交换P21、网络设置及其作用P21-22、无线网络P22、网络存储P33-34、可用性和可靠性P34-35（掌握）

* 信息的质量属性：
  + 1. 精确性 对事物状态描述的精准程度
    2. 完整性 对事物状态描述的全面程度，完整信息应包括所有重要事实
    3. 可靠性 指信息的来源、采集方法、传输过程是可以信任的，符合预期
    4. 及时性 指获得信息的时刻与事件发生时刻的间隔长短
    5. 经济性 指信息获取、传输带来的成本在可以接受的范围之内
    6. 可验证性 指信息的主要质量属性可以被证实或者证伪的程度
    7. 安全性 信息可以被非授权访问的可能性，可能性越低，安全性越高

* 信息技术 核心是传输技术



* 1. 信源：产生信息的实体，信息产生后，由这个实体向外传播、如QQ使用者
  2. 信宿：信息的归宿或接收者，如使用QQ的另一方（当然这一方也是信源），它通过计算机屏幕接收QQ使用者发生的文字
  3. 信道：传播信息的通道，如TCP/IP网络
  4. 编码器：对编码信息进行加密在编码
  5. 译码器：把信道上送来的信号（原始信息与噪声的叠加）转换成信宿能接受的信号
  6. 噪声：干扰，可以来自于信息系统分层结构的任何一次，到噪声携带的信息达到一定程度的时候，在信道中传输的信息可以被噪声掩盖导致传输失败。

## 1.1信息系统与信息化

系统的特性：

1. 目的性 2) 整体性 3)层次性 4)稳定性 5)突变型 6)自组织性 7)相似性 8)相关性 9) 环境适应性

信息系统的特性：开放性、脆弱性、健壮性

* 信息化五个层次：
  + 产品信息化 智能电视、智能灯具
  + 企业信息化 生产制造系统、ERP、CRM、SCM
  + 产业信息化 农业、工业、交通运输、生产制造业、服务业等传统产业
  + 国民经济信息化 金融、贸易、投资、计划、通关、营销等组成一个信息大系统
  + 社会生活信息化 智慧城市、互联网金融
* 信息化
* 主体 全体社会成员、包括政府、企业、事业、互联网金融
* 手段 基于现代信息技术的先进社会生产工具
* 途径 创建信息时代的社会生产力，推动社会生产关系及社会上层建筑的改革
* 目标 使国家的综合实力。社会的文明素质和人民的生活质量全面提升
* 两网、一站、四库、十二金(了解)
  + - 两网 指政务内网和政务外网
    - 一站 政府门户网站
    - 四库 人口、法人单位、空间地位和自然资源。宏观经济等四个基础数据库
    - 十二金

办公业务资源系统、宏观经济管理系统建设

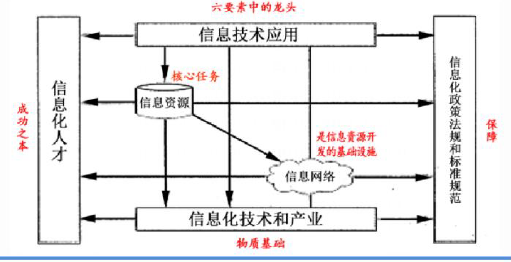
金税、金关、金财、金融监管（含金卡）、金审

金盾、金保、金农、金水、金质

信息化体系六要素

* + 信息技术应用 龙头（主阵地）
  + 信息资源 核心任务
  + 信息网络 基础设施
  + 信息技术和产业 物资基础
  + 信息化人才 成功之本
  + 信息化法规 保障

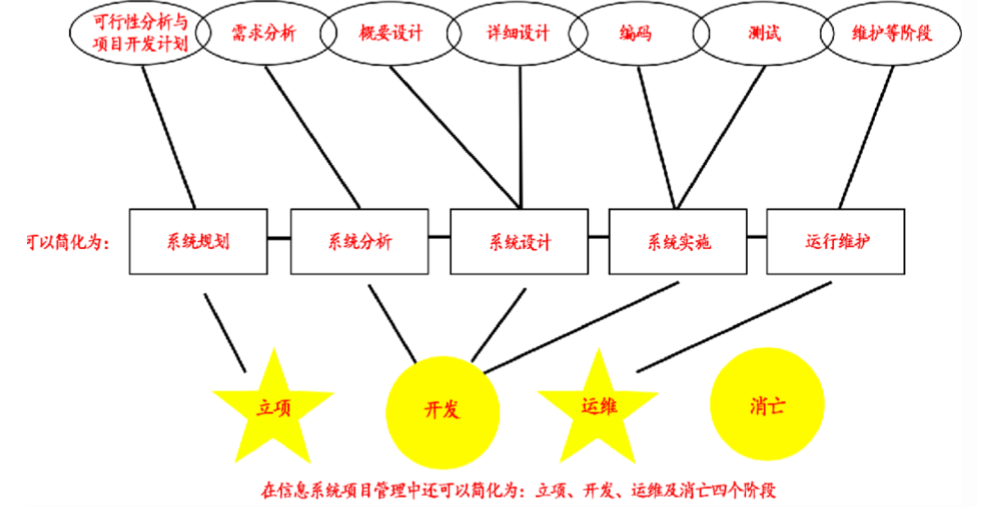
记忆口诀：鹰头、鸡基、人本、法保、织一织热的心、网基



图形记忆口诀：鹰上（应用）、下鸡（技术）、左人（人才）、右龟（规范）

阶段划分：

* 系统规划（可行性分析与项目开发计划）
* 系统分析（需求分析）
* 系统设计（概要设计、详细设计）
* 系统设施（编码、测试）
* 运行维护





记忆技巧：划分即实行，掌握每个阶段的产物

1、系统规划阶段：对组织的环境、目标及现行系统的状况初步调查，根据组织目标和发展战略，确定信息系统的发展战略，对建设新系统的需求做出分析和预测，研究建设新系统的必要性和可能性。给出拟建设的备选方案，写出可行性研究报告

2、系统分析阶段：根据系统设计计划书所确定的范围，对现行系统进行详细调查，描述现行系统的业务流程，指出现行系统的局限性和不足之处，确定新系统的基本目标和逻辑功能需求，即提出新系统的逻辑模型。（做什么）

3、系统设计阶段：根据系统说明书中规定的功能要求，考虑实际条件，具体设计实现逻辑模型的技术方案，也就是设计新系统的物理模型。又称为物理设计阶段，可分为总体设计（概要设计）和详细设计两个阶段。技术文档是系统设计说明书、

4、系统实施阶段：将设计的系统付诸实施的阶段。任务包括计算机等设备的购置、安装和调试、程序的编写和调试、人员培训、数据文件转换、系统调试与转换等、这个阶段的特点是几个相互联系、相互制约的任务同时展开，必须精心安排、合理组织。系统测试之后写出系统测试分析报告。

5、系统运行和维护阶段：系统投入运行后，需要经常进行维护和评价，记录系统运行的情况，根据一定的规则对系统进行必要的修改，评价系统的工作质量和经济效益。

## 1.2信息系统开发方法

**结构化的方法**：

包括结构化方法、面向对象方法、原型化方法、面向服务的方法

精髓是自顶向下、逐步求精和模块化设计

主要特点：

1、开发目标清晰化

2、开发工作阶段化

3、开发文档规范化

4、设计方法结构化

主要缺点：

1、开发周期长

2、难以适应需求变化

3、很少考虑数据结构

**面向对象（OO）方法**:

系统分析、系统设计和系统实现三个阶段之间已经没有“缝隙”

使用结构化方法进行自顶向下的整体划分；然后，自底向上地采用OO方法进行开发

结构化方法和OO方法仍是两种在系统开发领域中相互依存的、不可替代的方法

面向对象的方法

1、面向对象（OO）方法认为，客观世界是由各种对象组成的，任何事物都是对象

2、与结构化方法类似，OO方法也划分阶段，但其中的系统分析、系统设计和系统实现三个阶段之间已经没有“缝隙”。也就是说，这三个阶段的界限变得不明确

3、OO方法使系统的描述及信息模型的表示与客观实体相对应，符合人们的思维习惯，有利于系统开发过程中用户与开发人员的交流和沟通，缩短开发周期。面向对象设计主要有三大特征：封装性、继承性和多态性，使用面向对象方法构建的系统具有更好的复用性

4、一些大型信息系统的开发，通常是将结构化方法和OO方法结合起来。首先，使用结构化方法进行自顶向下的整体划分；然后，自底向上的采用OO方法进行开发。因此，结构方法和OO方法仍是两种在系统开发领域中相互依存的、不可替换的方法。

**面向对象方法OO：**对象、类、集成、封装、消息、多态。关键点：在于是否建立一个全面、合理、统一的模型既能反应问题域又被计算机系统求解域所接受

1. 面向对象的分析OOA：了解问题涉及的对象、对象的关系与操作，构造问题的对象模型
2. 面向对象的设计OOD：对OOA结果整理
3. 面向对象的程序设计OOP：系统功能的编码。

OO方法的分支：Coad/Yourdon、Booch、OMT(系统分析、系统设计、对象设计和实现)、OOSE

**面向对象概念解析**

--1—什么是对象：只要是客观存在的事物都是对象

--2—什么是类：类是确定对象讲会拥有的特征（属性）和行动（方法），它不是具体客观存在的东西

--3—对象的属性：对象的属性就是对象具备的各种特征，每个对象的每个属性都具有特点的值。

--4—对象的方法就是对象执行的操作，也就是说对象能干什么？这就成为方法。

面向对象和面向过程的区别：

1. 面向对象是将实物高度抽象化
2. 面向过程是一种自顶向上的编程
3. 而面向对象是自下先建立抽象模型然后再使用模型

补充知识点：

**对象**：对象是由数据及其操作所构成的封装体，对象包含三个基本要素，分别是对象标识、对象状态和对象行为；是系统中用来描述客观事物的一个模块，是构成系统的基本单元。用计算机语言来描述，对象是由一组属性和对这组属性进行的操作构成的。

**类**：现实世界中实体的形式化描述，类将该实体的属性（数据）和操作（函数）封装在一起。

类和对象的关系可以总结为：

1. 每一个对象都是某一个类的实例；
2. 每一个类在某一时刻都有零或更多的实例；
3. 类是静态的，对象是动态的
4. 类是生成对象的模板

类和对象的关系可理解为，对象是类的实例，类是对象的模板。如果将对象比作房子，那么类就是房子的设计图纸。

**抽象**：通过特定的实例抽取共同特征后形成概念的过程，对象是现实世界中某个实体的抽象，类是一组对象的抽象。

**封装**：封装是将相关的概念组成一个单元，然后通过一个名称来引用他。面向对象封装是将数据和基于数据的操作封装成一个整体对象，对数据的访问或修改只能通过对象对外提供的接口进行。

补充面向对象的知识点

**继承**：继承表示类直接的层次关系，继承又可分为单继承和多继承，继承自父类的属性特征，不需要在子类中进行重复说明

**多态**：使得在多个类中可以定义同一个操作或属性名，并在每个类中可以有不同的实现。多态使得某个属性或操作在不同的事情可以表示不同类的对象特性。多态，是面向对象的程序设计语言最核心的特性。多态，意味着一个对象有着多重特征，可以在特定的情况下，表现不同的状态，从而对应着不同的属性和方法

**接口**：接口就是对操作规范的说明，其只说明操作应该做什么

**消息**：体现对象间的交互，通过它向目标对象发送操作请求

**组建**：小时软件系统可替换的、物理的组成部分，封装了模块功能的实现。组建应当是内聚的，并具有相对稳定的公开接口。

**模式**：描述了一个不断重复发生的问题，以及该问题的解决方案。其包括特定环境、问题和解决方案三个组成部分。应用设计模式可以更加简单和方便的去复用成功的软件设计和架构，从而帮助设计者更快更好的完成系统设计

**复用**：软件复用是指将已有的软件及其有效成分用于构造新的软件或系统。

**原理**：

系统开发初期，必须明确系统的功能要求，确定系统边界

根据用户初步需求，利用系统开发工具，快速地建立一个系统模型展示给用户，在此基础上与用户交流，最终实现用户需求的信息系统快速开发的方法

**分类**：

**是否实现功能**：

**水平原型**：

也称为行为原型，用来探索预期系统的一些特定行为，并达到细化需求的目的

通常只是功能的导航，但并未真实实现功能

主要用在界面上

**垂直原型**：

也称为结构化原型，实现了一部分功能

主要用在复杂的算法实现上

**最终结果**：

**抛弃式原型**：用在解决需求不确定性、二义性、不完整性、含糊性

**演化式原型**：

为开发增量式产品提供基础，逐步将原型演化成最终系统

必须易于升级和优化的场合，特别适用于Web项目

**特点**：

1. 可以使系统开发的周期缩短，成本和风险降低、速度加快，获得较高的综合开发效益。
2. 以用户为中心来开发系统的，用户参与的程度大大提高，开发的系统符合用户的需求，因而增加了用户的满意度，提高了系统开发的成功率。
3. 由于用户参与了系统开发的全过程，对系统的功能和结构容易理解和接受，有利于系统的移交，有利于系统的允许和维护。

**优点**:

1. 主要在于能有效地确认用户需求
2. 用于那些需求不明确的系统开发
3. 对分析层面难度大、技术层面难度不大的系统，适合于原型开发
4. 而对于技术层面的困难远大于其分析层面的系统，则不宜用原型法

**面向服务的方法**：

1. 进一步将接口的定义与实现进行解耦
2. 提高系统可复用性、信息资源共享和系统之间的互操作性

**OIS模型：**

1. 物理层

该层包括物理连网媒介，如电缆连线连接器。该层的协议产生并检测电压以便发送和接收携带数据的信息。有RS232、V.35、RJ-45、FDDI。

1. 数据链路层

它控制网络层与物理层之间的通信。它的主要功能是将从网络层接收到的数据分隔成特定的可被物理层传输的帧。协议有IEEE802.3/.2、HDLC、PPP、ATM

1. 网络层

其主要功能是将网络地址（例如，IP地址）翻译成对应的物理地址（例如，网卡地址），并决定如何将数据从发送方路由到接收方。有IP、UDP、SPX。

1. 传输层

主要负责确保数据可靠、顺序、无错地从A点传输到B点、如提供建立、维护和拆除传送连接的功能；选择网络层提供最合适的服务；在系统之间提供可靠的透明的数据传送，提供端到端的错误恢复和流量控制、有TCP、UDP、SPX。

1. 会话层

负责在网络中的两节点之间建立和维持通信，以及提供交互会话的管理功能，如三种数据流方向的控制，即一路交互、两路交替和两路同时会话模式。有RPC、SQL、NFS

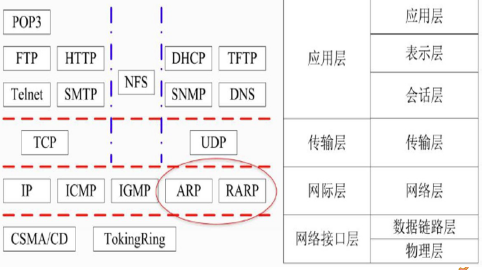
1. 表示层

如同应用程序和网络之间的翻译官，数据将按照网络能理解的方案进行格式化；管理数据的解密和加密、数据转换、格式化和文本压缩。有JPEG、ASCII、GIF、MPEG。

1. 应用层

负责对软件提供接口以使程序能使用网络服务，如事务处理程序、文件传送协议和网络管理等。有HTTP、Telnet、FTP、SMTP。

|  |  |  |  |
| --- | --- | --- | --- |
| 层次 | 名称 | 主要功能 | 主要设备及协议 |
| 7 | 应用层 | 实现具体的应用功能 | POP3、FTP、HTTP、Telnet、SMTP、DHCP、TFTP、SNMP、DNS |
| 6 | 表示层 | 数据的格式与表达、加密、压缩 |
| 5 | 会话层 | 建立、管理和终止会话 |
| 4 | 传输层 | 端到端的连接 | TCP、UDP |
| 3 | 网络层 | 分组传输和路由选择 | 三层交互机，路由器 ARP、RARP、IP、ICMP、IGMP |
| 2 | 数据链路层 | 传送已帧为单位的信息 | 网桥、交换机、网卡 PPTP、L2TP、SLIP、PPP |
| 1 | 物理层 | 二进制传输 | 中继器，集线器 |



TCP/IP协议

1. 应用层
   1. FTP（文件传输协议）

网络上两天计算机传送文件的协议

FTP在客户机和服务器之间需建立两天TCP连接，一条用于传送控制信息（使用21号端口），另一条用于传送文件内容（使用20号端口）

* 1. TFTP（简单文件传输协议，UDP）

用来在客户机与服务器之间进行监督文件传输的协议，提供不复杂、开销不大的文件传输服务。提供不可靠的数据流传输服务

* 1. HTTP(超文本传输协议)

从WWW服务器传输超文本到本地浏览器的传送协议

* 1. SMTP(简单邮件传输协议，TCP)提供可靠且有效的电子邮件传输的协议
  2. DHCP(动态主机配置协议，UDP) 负责IP地址的分配，有固定分配、动态分配和自动分配
  3. Telnet(远程登录协议TCP)允许用户登录进入远程计算机系统
  4. DNS(域名系统) 转换工作称为域名解析转换
  5. SNMP(简单网络管理协议) 网络管理

1. 传输层
   1. TCP 是可靠的，面向连接的、全双工的数据传输服务，输数据量比较少，且对可靠性要求高的场合。
   2. UDP 一种不可靠的、无连接的协议，传输数量大，对可靠性要求不是很高，但要求速度快的场合。
2. 网络层
   1. IP 无连接的和不可靠的，他将差错监测和流量控制之类的服务授权给了其他的各层协议
   2. ICMP（网络控制报文协议） 专门用于发送差错报文协议
   3. IGMP（国际足管理协议） 允许Internet中的计算机参加多播，是计算机用做向相邻多路由器报告多目组成成员的协议
   4. ARP（地址解析协议） IP地址向物理地址的转换。每块网卡都有唯一的地址
   5. RARP（反向地址分析协议）物理地址向IP地址的转换

## 1.3常规信息系统集成技术

**网络协议：**

局域网协议：IEEE802规范

组成：

802.1（802协议概论）、802.2（逻辑链路控制层LLC协议）

802.3（以太网的CSMA/CD载波监听多路访问/冲突监测协议）

802.4（令牌总线Token Bus协议）、802.5（令牌环Token Ring协议）

802.6（城域网MAN协议）、802.7（FDDI宽带技术协议）

802.8（光纤技术协议）、802.9(局域网上的语音/数据集成规范)

802.10（无线局域网WLAN标准协议）

分类：

|  |  |  |  |
| --- | --- | --- | --- |
| 分类 | 类型 | 传输速度 | 传输介质 |
| IEEE 802.3 | 标准以太网 | 10Mb/s | 细同轴电缆 |
| IEEE802.3u | 快速以太网 | 100Mb/s | 双绞线 |
| IEEE802.3z | 千兆以太网 | 1000Mb/s | 光纤或双绞线 |

广域网协议：

PPP点对点协议、ISDN综合业务数字网、xDSL、DDN数字专线、X.25、FR帧中继、ATM异步传输模式

**网络交换**：

* 物理层交换 如电话网
* 链路层交换 二层交换，对MAC地址进行变更
* 网络层交换 三层交换，对IP地址进行变更
* 传输层交换 四层交换，对端口进行变更，比较少见
* 应用层交换

**网络设备**：

|  |  |  |
| --- | --- | --- |
| 互联设备 | 工作层次 | 主要功能 |
| 中继器 | 物理层 | 对接收信号进行再生和发送，只起到扩展传输距离用，对高层协议是透明的，但是要个数有限（例如，再以太网中只能使用4个） |
| 网桥 | 数据链路层 | 根据帧物理地址进行网络直接的信息转发，可缓解网络通信繁忙度，提高效率。只能够连接相同MAC层的网络 |
| 路由器 | 网络层 | 通过逻辑地址进行网络之间的信息转发，可完成异构网络之间的互联互通，只能连接使用相同网络层协议的子网 |
| 网关 | 高层（第4-7层） | 最复杂的网络互联设备，用于连接网络层以上执行不同协议的子网 |
| 集线器 | 物理层 | 多端口中继器 |
| 二层交换机 | 数据链路层 | 是指传统意义上的交换机，多端口网桥 |
| 三层交换机 | 网络层 | 带路由功能的二层交换机 |
| 多层交换机 | 高层（第4-7层） | 带协议转换的交换机 |

**无线网络的产品**：无线网卡、无线AP、无线网桥和无线路由器

**网络存储技术**：

1、直接附加存储（DAS）

存储设备通过SCSI电缆直接连到服务器

其本身是硬件的堆叠，存储操作依赖于服务器，不带有任何存储操作系统

2、网络附加存储（NAS）

1、通过网络接口与网络直接相连，由用户通过网络访问，支持即插即用

2、NAS存储设备类似于一个专用的文件服务器，去掉了通用服务器的大多数计算功能，而仅仅提供文件系统功能，从而降低了设备的成本

3、支持多种TCP/IP协议，主要是NFS（网络文件系统）和CIFS（通用Internet文件系统）来进行文件访问，性能特点是进行小文件级的共享存取

3、存储区域网络（SAN）

特点： 通过高速光纤连接，极度可扩展型；通过专用交换机将磁盘阵列与服务器连接起来的高速专用子网，它没有采用文件共享存取方式，而是采用块（block）级别存储

分类：

* + - * FCSAN 热插拔性、高速带宽、远程连接、连接设备数量大等
      * IPSAN 基于IP网络实现数据块级别存储方式的存储网络，由于设备成本低，配置技术简单，可共享和使用大容量的存储空间
      * IBSAN 机构设计的非常紧密，大大提高了系统的性能、可靠性和有效性，能缓解各硬件设备之间的数据流量拥塞

**网络接入:**

有线接入：PSTN、ISDN、ADSL、FTTx+LAN和HFC

无线接入：无线电波作为传输媒介

GPRS、3G、4G接入

WiFi和移动互联接入（4G）



高速以太网的宽带技术FTTx+LAN（光纤+局域网）

FTTC（光纤到路边）FTTZ（光纤到小区）FTTB（光纤到楼）FTTF（光纤到流层）FTTH（光纤到户）

**网络工程：**

网络规划：网络需求分析、可行性分析、对现有网络的分析和描述

网络设计：

核心层：通过高速转发通信，提供优化、可靠的骨干传输结构

汇聚层：核心层和接入层的分界面，完成网络访问策略控制、数据包处理、过滤、寻址，以及其他数据处理的任务

接入层：允许终端用户连接到网络

网络实施：

**网络设计工作**：

1. 网络拓扑结构设计 考虑因素有：地理环境、传输介质与距离以及可靠性
2. 主干网络（核心层）设计 根据用户方网络规模大小、网上传输信息的种类和用户方可投入的资金等因素来考虑
3. 汇聚层和接入层设计 汇聚层的存在与否，取决于网络规模的大小
4. 广域网连接与远程访问设计 根据网络规模的大小、网络用户的数据量来选择
5. 无线网络设计 适用于很难布线的地方（比如受保护的建筑物、机场等）或者经常需要变动布线结构的地方（如展览馆等） 对于城市范围的网络接入也能适用，可以设想一个采用无线网络的IS可以为一个城市的任何角落提供高速互联网接入
6. 网络安全设计 网络系统的硬件、软件及其系统中的数据受到保护
7. 设备选型

**数据仓库：**面向主题的、集成的、非易失的、且随时间变化的数据集合，用于支持管理决策

组成：

1、数据源 数据仓库系统的基础，是整个系统的数据源泉

2、数据的存储与管理 是整个数据仓库系统的核心

3、OLAP服务器

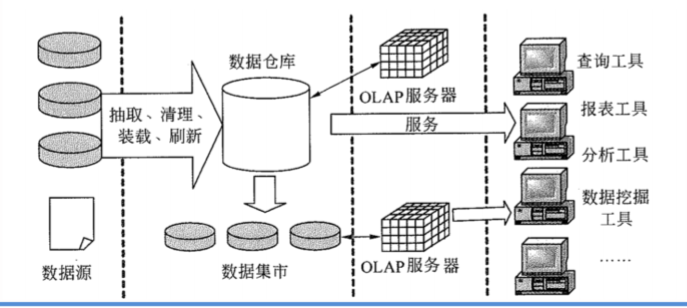
ROLAP：基本数据和聚合数据均存放在RDBMS之中

MOLAP：基本数据和聚合数据均存放于多维数据库中

HOLAP：基本数据存放于RDBMS之中，集合数据存放于多维数据库中

4、前端工具

各种查询工具、报表工具、分析工具、数据挖掘工具以及各种基于数据仓库或数据集市的应用开发工具



**中间件**:

定义： 1、在一个分布式系统环境中处于操作系统和应用程序之间的软件

2、一种独立的系统软件或服务程序，分布式应用软件借助这种软件在不同的技术之间共享资源，中间件位于客户机服务器的操作系统之上，管理计算机资源和网络通信

分类：

底层型中间件：

主流技术有JVM（Java虚拟机）、CLR（公共语言运行库）、ACE（自适配通信环境）、JDBC(Java数据库连接)和ODBC（开放数据库互连）代表产品主要有SUNJVM和MicrosoftCLR

通用型中间件：主流技术有CORBA（公共对象请求代理体系结构）、J2EE、MOM（面向消息的中间件）和COM代表产品主要有IONAOrbix、BEWebLogic和IBMMQSeries

集成型中间件：主流技术有WorkFlow和EAI(企业应用集成) 代表产品有BEAWebLogic 和 IBMWebSphere

应用：

1、为了完成系统底层传输层的集成，可以采用CORBA技术

2、为了完成不同系统的信息传递，可以采用消息中间件产品

3、为了完成不同硬件和操作系统的集成，可以采用J2EE中间件产品

## 1.4软件工程

**分类**：

1、业务需求

反映企业或客户对系统高层次的目标要求，项目投资人、购买产品的客户、客户单位的管理人员、市场营销部门或产品规划部门

2、用户需求 描述用户的具体目标，或用户要求系统必须能完成的任务，描述用户能使用系统来做什么

3、系统需求 从系统的角度来说明软件的需求，包括功能需求、非功能需求和设计约束等，也称为行为需求，规定了开放人员必须在系统中实现的软件功能，用户利用这些功能来完成任务，满足业务需要

**分类2**：

1、功能需求 通过系统特性的描述表现出来的，所谓特性指一组逻辑上相关的功能需求，表示系统为用户提供某项功能（服务），使用户的业务目标得以满足

2、非功能需求 系统必须具备的属性或品质，例如，易用性、可维护性、效率等

3、设计约束 限制条件或补充规约，通常是对系统的一些约束说明，例如，必须采用国有自主知识产权的数据库系统，必须运行在UNIX操作系统之下等

**分类3**：

1、常规需求 用户认为系统应该做到的功能或性能，实现越多用户会越满意

2、期望需求 用户想当然认为系统应具备的功能或性能，但并不能正确描述自己想要得到的这些功能或性能需求。如果期望需求没有得到实现，会让用户感到不满意。

3、意外需求 兴奋需求，是用户要求范围外的功能或性能（但通常是软件开发人员很乐意赋予系统的技术特性），实现这些需求用户会更搞笑，但不实现也不影响其购买的决策。

**特点**：无二义性、完整性、一致性、可测试性、确定性、可跟踪性、正确性、必要性

**获取的方法**： 用户访谈、问卷调查、采样、情节串联板、联合需求计划

**SA方法：**

1、核心是数据字典

2、模型  
 1、数据模型 实体联系图（E-R图） 描述实体、属性、以及实体之间的关系

2、功能模型 数据流图（DFD） 从数据传递和加工的角度，利用图形符合通过逐层细分描述系统内各个部件的功能和数据在它们之间传递的情况，来说明系统所完成功能

3、行为模型（状态模型STD） 通过描述系统的状态和引起系统状态转换的事件，表示系统的行为，指出作为特定事件的结果将执行那些动作。

**软件需求规格说明书（SRS）：**

需求开发活动的产物，使项目干系人与开发团队对系统的初始规定有一个共同的理解

内容：1.范围2.引用文件3.需求4.合格性规定5.需求可追踪性6、尚未解决的问题7、注解8、附录

**需求验证：**

1、内容

1、SRS正确的描述了预期的、满足项目干系人需求的系统行为和特征

2、SRS中的软件需求是从系统需求、业务规格和其他来源中正确推导而来的

3、需求是完整的和高质量的

4、需求的表示在所有地方都是一致的

5、需求为继续进行系统设计、实现和测试提供了足够的基础

2、方法 需求评审、技术评审、需求测试

**UML**

**结构：**构造块、规则、公共机制

UML具有的语言特征：

1、不是一种可视化的程序设计语言，而是一种可视化的建模语言

2、不是过程，也不是方法，但允许任何一种过程和方法使用它；

UML适用于迭代式开发过程

**四种关系：**

1、依赖 两个事物之间的语义关系，其中一个事物发生变化会影响另一个事物的语义

2、关联 描述一组对象之间连接的结构关系

3、泛化 一般化和特殊化的关系，描述特殊元素的对象可替换一般元素的对象

4、实现 类之间的语义关系，其中的一个类指定了由另一个类保证执行的契约

**5个系统视图：**

1、逻辑视图 设计视图，表示了设计模型中在架构方面具有重要意义的部分，即类、子系统、包和用例实现的子集

2、进程视图 是可执行线程和进程为活动类的建模，它是逻辑视图的一次执行实例，描述了并发和同步结构

3、实现视图 对组成基于系统的物理代码的文件和构建进行建模

4、部署视图 对构件部署到一组物理节点上，表示软件到硬件的映射和分布结构

5、用例视图 是最基本的需求分析模型

1. 关联 不同类的对象之间的结构关系，它在一段时间内将多个类的实例连接在一起，对象实例之间的关系，而不表示两个类之间的关系
2. 依赖 两个类A和B，如果B的变化可能会引起A的变化，则称类A依赖于类B
3. 泛化 一般事物与该事物中的特殊种类之间的关系，也就是父类与子类之间的关系，继承关系是泛化关系的反关系，也就是说，子类继承了父类，而父类则是子类的泛化。
4. 共享聚集 聚合关系，它表示类之间的整体与部分的关系，部分可能同时属于多个整体，部分与整体的生命周期可以不相同。例如：汽车和车轮是聚合关系，车子坏了，车轮还可以用，车轮坏了，可以换一个新的
5. 组合聚集 组合关系，它也是表示类之间的整体与部分的关系，与聚合关系的区别在于，组合关系中的部分职能属于一个整体，部分与整体的生命周期相同，部分随着整体的创建而创建，也随着整体的消亡而消亡。
6. 实现关系 将说明和实现连续起来，接口是对行为而非实现的说明，而类中则包含了实现的结构。一个或多个类可以实现一个接口，而每个类分别实现接口中的操作

关联：连接模型元素及链接实例，用一条实线来表示。

依赖：表示一个元素以某种方式依赖于另一个元素，用一条虚线加箭头来表示



聚合：表示整体与部分的关系，用一条实现加空心菱形来表示



组合：表示整体与部分的有一关系，用一条实线加实心菱形来表示

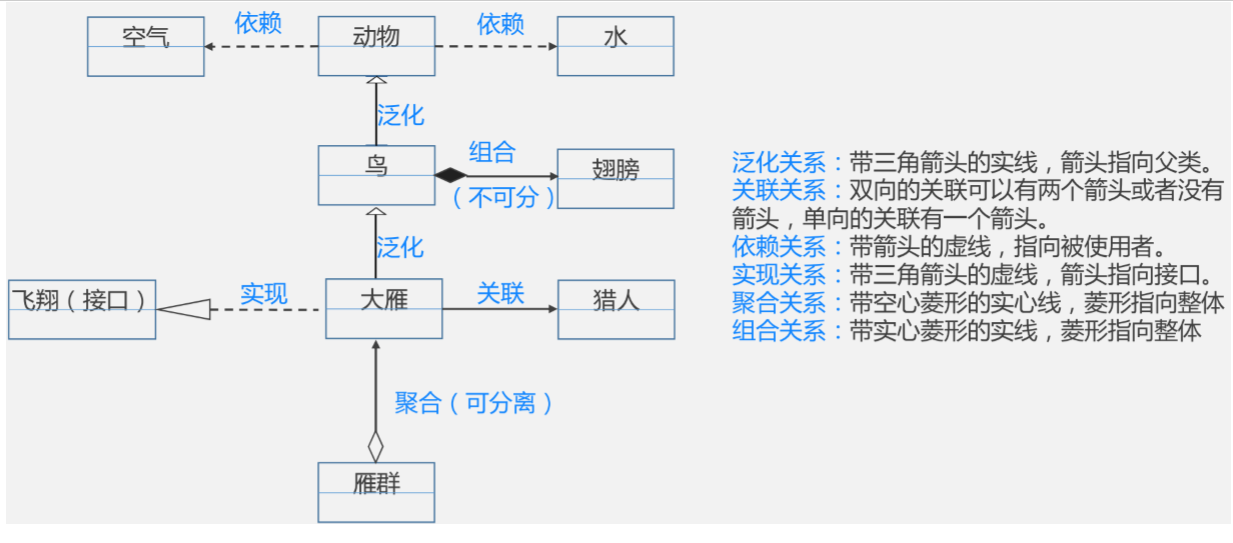


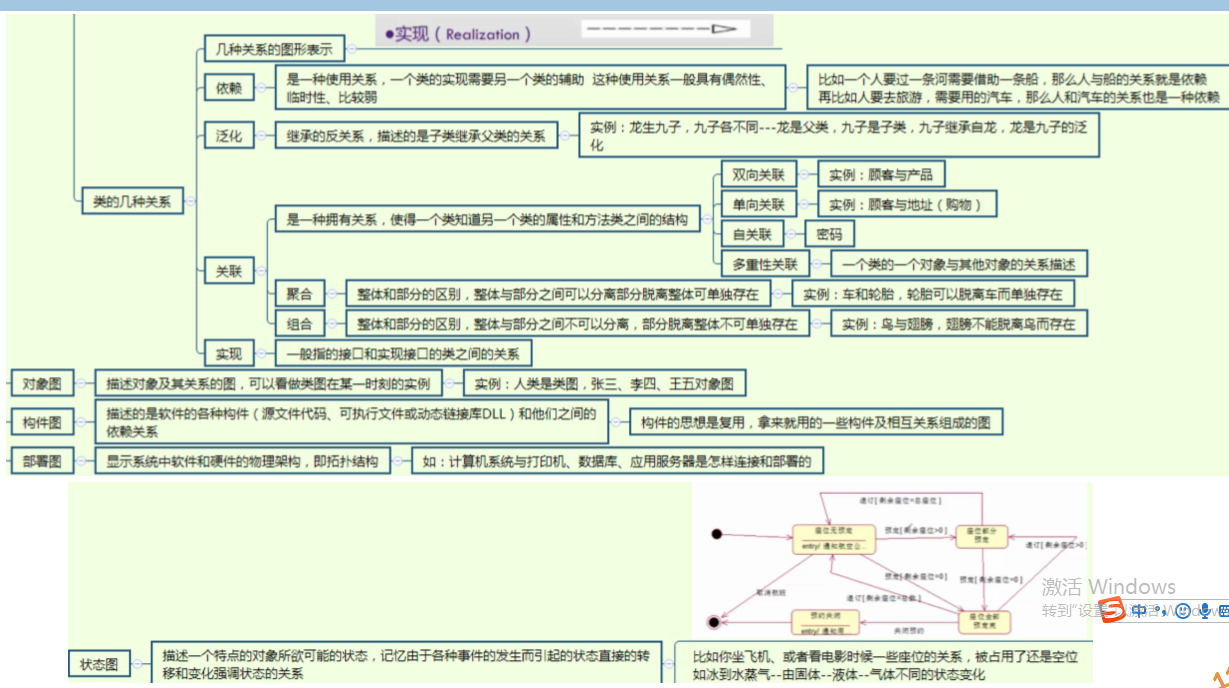
泛化：表示一般与特殊的关系，用一条实线加空心箭头来表示



实现：表示类与接口的关系，用一条虚线加空心箭头来表示







**14种图：**

1. 类图 描述一组类、接口、协作和它们之间的关系，是最常见的图
2. 对象图 描述一组对象以及它们之间的关系，描述了在类图中所建立的事物实例的静态快照
3. 构件图 描述一个封装的类和它的接口、端口、以及由内嵌的构建和连接件构成的内部结构
4. 组合机构图 描述结构化类（例如，构件或类）的内部结构，包括结构化类与系统其余部分的交互点。组合结构图用于画出结构化类的内部内容
5. 用例图 描述一组用例、参与者及它们之间的关系
6. 顺序图（序列图） 一种交互图，展现了一种交互，由一组对象或者参与者以及它们之间可能发送的消息构件
7. 通信图 一种交互图，它强调收发消息的对象或参与者的结构组织，强调的是时序，强调的是对象之间的组织结构（关系）
8. 定时图（计时图） 一种交互图，它强调消息跨越不同对象或参与者的实际时间，而仅仅只是关心消息的相对顺序
9. 状态图 描述一个状态机，它由状态、转移、事件和活动组成
10. 活动图 将进程或其他计算结构展示位计算内部一步步的控制流和数据流
11. 部署图 描述对运行时的处理节点及在其中生存的构建的配置
12. 制品图 描述计算机中一个系统的物理结构。制品包括文件、数据库和类似的物理比特集合
13. 包图 描述由模型本身分析而成的组织单元，以及它们之间的依赖关系
14. 交互概览图 是活动图和顺序图的混合物

**软件架构**

**核心**：能否达到架构级的软件复用，也就是说，能否在不同的系统中，使用同一个软件架构

**软件架构风格**：

1. 数据流风格 批处理序列架构风格和管道/过滤器
2. 调用/返回风格 主程序/子程序、数据抽象和面向对象，以及层次结构
3. 独立构件风格 进程通信和事件驱动的系统
4. 虚拟机风格 解释器和基于规则的系统
5. 仓库风格 数据库系统、黑板系统和超文本系统

**评估人员关注**：质量属性

**相关名词**：

敏感点：一个或多个构件（和/或构件之间的关系）的特性

权衡点：影响多个质量属性的特性

**评估方式**：

调查问卷（或检查表）的方式

基于场景的方式

最为常用

分类：

架构权衡分析法（ATAM）

软件架构分析法（SAAM）

成本效益分析法（CBAM）

描述方面:

刺激 场景中解释或描述项目干系人怎样引发与系统的交换部分

环境 描述的是刺激发生时的情况

响应 系统是如何通过架构对刺激作出反应的

作用：分析软件架构对场景的支持程度，从而判断该架构对这一场景所代表的质量需求的满足程度。

基于度量的方式

1.5软件设计

设计模式：  
分类：

结构化设计：

一种面向数据流的方法

以SRS和SA阶段所产生的DFD和数据字典等文档为基础

自顶向下、逐步求精和模块化的过程

面向对象设计

原则：

高内聚：模块内部个成分之间的联系程度

低耦合：模块之间联系的程度

区别：

OOD是OOA方法的延续，其基本思想包括抽象、封装和可扩展性，其中可扩展性主要通过继承和多态来实现

目的：可以方便地复用成功的软件设计

要素：模式名词、问题、目的、解决方案、效果、实例代码和相关设计模式

处理范围分：

类模式：处理类和子类之间的关系和静态关系

对象模式：处理对象之间的关系和动态性

目的和用途分：

创建型模式：用于创建对象，包括工程方法模式、抽象工程模式、原型模式、单例模式和建造者模式

结构型模型：用于处理类或对象的组合，包括适配器模式、桥接模式、组合模式、装饰模式、外观模式、享元模式和代理模式

行为型模式：用于描述类或对象的交互以及职责的分配，包括职责模式、命令模式、解释器模式、迭代器模式、中介者模式、备忘录模式、观察者模式、状态模式、策略模式、模板方法模式、访问者模式

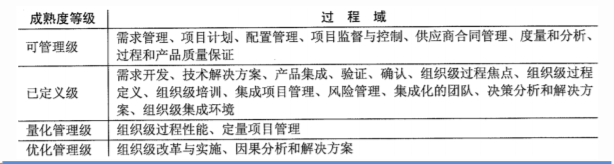
能力成熟度模型集成：

能力成熟度模型集成（CMMI）

定义：继承了CMM的阶段表示法和EIA/IS731的连续式表示法，这两 方法各有优缺点，均采用统一的24个过程域，它们在逻辑上是等价的，对同一个组织采用两种模型分别进行CMMI评估，得到的结论应该是相同的

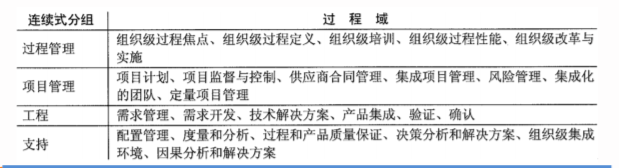
分类：

1、阶段式模式



保持4个成熟等级，但关键过程域做了一些调整和扩充

2、连续式模型



将24个过程域按照功能分为过程管理、项目管理、工程和支持四个过程组

**软件测试**

**测试方法分：**

静态测试：被测试程序不在机器上运行，而采用人工检测和计算机辅助静态分析的手段对程序进行检测，包括对文档的静态测试和对代码的静态测试，对文档的静态测试主要以检查单的形式进行，对代码的静态测试一般采用桌前检查、代码走查和代码审查

**动态测试**：

定义：在计算机上实际运行程序进行软件测试

方法：

白盒测试：结构测试，用软件单元测试中，将程序看作是一个透明的白盒，测试人员完全清楚程序的结构和处理算法，按照程序内部逻辑结构设计测试用例，检测程序中主要执行通路是否能按预定要求正确工作，方法有控制流测试、数据流测试和程序变异测试，使用人工检查代码的方法来检查代码的逻辑问题，逻辑覆盖，语句覆盖、判定覆盖、条件覆盖、条件/判定覆盖、条件组合覆盖、修正的条件/判定覆盖和路径覆盖功能测试

黑盒测试：功能测试，用于集成测试、确认测试和系统测试中，将程序看作是一个不透明的黑盒，完全不考虑程序的内部结构和处理算法，只检查程序功能是否能按照SRS的要求正常使用，程序是否能适当地输入数据并产生正确的输出信息，程序运行过程中能否保持外部信息（如文件和数据库等）的完整性等。方法：等价类划分、边界值分析、判定表、因果图、状态图、随机测试、猜错法和正交试验法

**单元测试**：也称为模块测试，测试的对象是可独立编译或汇编的程序模块、软件构件或OO软件中的类（统称为模块），目的是检查每个模块能否正确的实现设计说明中的功能、性能、接口和其他设计约束等条件，发现模块内可能存在的各种差错。

**集成测试：**检查模块之间，以及模块和已集成的软件之间的接口关系，并验证已集成的软件是否符合设计要求

**确认测试：**

**目的：**主要用于验证软件的功能、性能和其他特性是否用户需求一致

**分类：**

**内部确认测试：**由软件开发组织内部按照SRS进行测试

**Alpha测试：**由用户在开发环境下进行测试

**Beta测试：**由用户在实际使用环境下进行测试，通过后，才能把产品发布或交付给用户

**系统测试**：对象是完整、集成的计算机系统，目的是在真实系统工作环境下，验证完整的软件配置能否和系统正确连接，并满足系统/子系统设计文档和软件开发合同规定的要求

**配置项测试**：对象是软件配置项，目的是检验软件配置项与SRS的一致性

**回归测试**：

目的：测试软件变更之后，变更部分的正确性和对变更需求的符合性，以及软件原有的、正确的功能、性能和其他规定的要求的不损害性

对象：未通过软件单元测试的软件，在变更之后，应对其进行单元测试，未通过配置项测试的软件，在变更之后，首先应对变更的软件单元进行测试，然后再进行相关的集成测试和配置项测试。未通过系统测试的软，在变更之后，首先应对变更的软件单元进行测试，然后再进行相关的集成测试、配置项测试和系统测试。因其他原因进行变更之后的软件单元，也首先应对变更的软件单元进行测试，然后再进行相关的软件测试

**面向对象的测试系统**：

1、封装性 必须考虑到信息隐藏原则对测试的影响，以及对象状态与类的测试序列

2、继承性 必须考虑到继承对测试充分性的影响，以及误用引起的错误

3、多态性 必须考虑到动态绑定对测试充分性的影响、抽象类的测试、以及吴用对测试的影响

**软件调试与测试的区别**：

1、测试的目的是找出存在的错误，而调试的目的是定位错误并修改程序以修改错误

2、调试时测试之后的活动，测试和调试在目标、方法和思路上都有所不同

3、测试从一个已知的条件开始，使用预先定义的过程，有预知的结果；调试从一个未知的条件开始，结束的过程不可预计

4、测试过程可以事先设计，进度可以事先确定；调试不能描述过程或持续时间

**软件测试的管理：**

过程管理**：**

组成：测试活动管理，测试资源管理

要点：软件测试应由相对独立的人员进行。根据软件项目的规模、完整性级别和测试类别，软件测试可由不同机构组织实施

配置管理：将测试过程中产生的各种工作产品纳入配置管理，由开发组织实施的软件测试，应将测试工作产品纳入软件项目的配置管理，由独立测试组织实施的软件测试，应建立配置管理库，将被测试对象和测试工作产品纳入配置管理

**评审工作：**

测试就绪评审：测试执行前对测试计划和测试说明等进行评审

测试评审：测试完成后，评审测试过程和测试结果的有效性，主要对测试记录和测试报告进行评审

**补充**：

1、软件测试是为了发现错误而执行程序的过程，是根据程序开发阶段的规格说明及程序内部结构而精心设计的一批测试用例（输入数据及其预期结果的集合），并利用这些测试用例去运行程序，以发现程序错误的过程。故软件测试应尽可能在实际运行试验环境下进行。软件测试不再只是一种仅在编码阶段完成后才开始的活动，而是应该包括在整个开发和维护过程中的活动，他本身也是实际产品构造的一个组成部分。

2、软件测试有如下几个原则：

1、软件开发人员即程序员应当避免测试自己的程序（单元测试除外）

2、应尽早的和不断地进行软件测试

3、用测试用例要正确的态度：第一，测试用例应当由测试输入数据和预期输出结果这两部分组成；第二，在设计测试用例时，不仅要考虑合理的输入条件，更要注意不合理的输入条件。

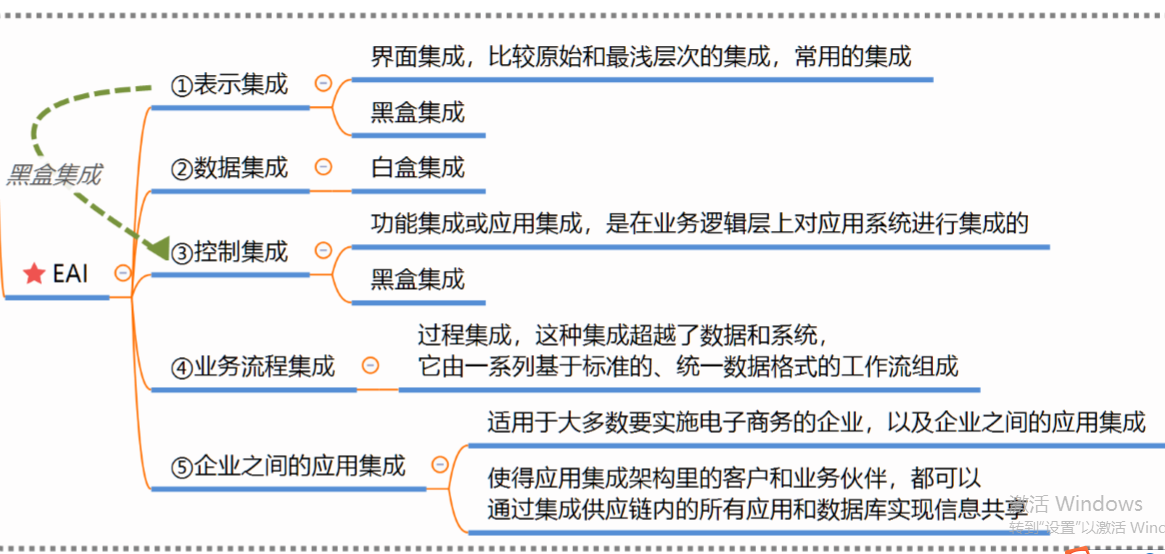
4、要充分注意软件测试中的群集现象，也可以认为是“80-20原则”。不要以为几个错误并且解决这些问题之后，就不需要测试了。反而这里是错误群集的地方，对这段程序要重点测试，以提高测试投资的效益。

5、严格执行测试计划，排除测试的随意性，以避免发生疏漏或者重复无效的工作、

6、应当对每一个测试结果进行全面检查

7、妥善保存测试用例、测试计划、测试报告和最终分析报告，以备回归测试及维护之用。

**EAI**：



## 1.5新一代信息技术

大数据 (Big Data)、云计算(Cloud Service)、物联网（Internet of things）、互联网+(Internet +)、智慧城市(Smart city)、移动互联网(Mobile Internet)、智能制作2025(Intellignet Manufacturing 2025)、人工智能AI(Artificial intellingence)、区块链(Block chain)

新一代信息技术产业包括：

* + 加快建设宽度、泛在、融合、安全的信息网络基础设施，推动新一代移动通信、下一代互联网核心设备和智能终端的研发及产业化，加快推进三网融合，促进物联网、云计算的研发和示范应用。
  + 着力发展集成电路、新型显示、高端软件、高端服务器等核心基础产业。
  + 大力发展数字虚拟等技术，促进文化创意产业发展
  + 大数据、云计算、互联网+、物联网、智慧城市等是新一代信息技术与信息资源充分利用的全新业态，是信息化发展的主要趋势，也是信息系统集成行业今后面临的主要业务范畴。
  + 我国在“十三五”规划纲要中，将培育人工智能、移动智能终端、第五代移动通信（5G）、先进传感器等作为新一代信息技术产业创新重点发展

数以万亿计新设备将接入网络，形成海量数据，应用爆发性增长，促进生产活动和社会管理方式进一步向智能化、精细化、网络化方向转变。

**物联网**

定义： 通过信息传感设备，按约定的协议，将任何物品与互联网相连接，进行信息交换和通信，以实现智能化识别、定位、跟踪、监控和管理的一种网络，主要解决物品与物品、人与人之间的互连，在物联网应用中有两项关键技术，分别是传感器技术和嵌入式技术。

技术：

RFID（射频识别）：是物联网中使用的一种传感器技术，通过无线电信标识识别特定目标并读写相关数据，而无需识别系统与特定目标直接建立机械或光学接触，识别工作无须人工干预，防水、防磁、耐高温。使用寿命长、读取距离大、标签上数据可以加密、存储数据容量更大、存储信息更加自如。更容易地附着在不同的产品上

嵌入式技术：综合了计算机软硬件、传感器技术、集成电路技术、电子应用技术为一体的复杂技术

传感和识别技术：工业和信息化深度融合的关键技术之一

编码技术、标识技术、解析技术、安全技术和中间件技术

架构：

感知层：由各种传感器构成，包括温湿度传感器、二维码标签、RFID标签和读写器、摄像头、GPS等感知终端。

网络层：由各种网络，包括互联网、广电网、网络管理系统和云计算平台等组成，是整个物联网的中纽，赋值传递和处理感知层获取的信息

应用层：是物联网和用户的接口，它与行业需求结合，实现物联网的智能应用

应用：1、智能微尘2、智能电网3、智慧物流4、智能家居5、智能交通6、智慧农业7、环境保护8、医疗健康9、城市管理10、金融服务保险业11公共安全

**云计算**

定义：一种基于并高度依赖于Internet，用户与实际服务提供的计算资源相分离，集合了大量计算设备和资源，并向用户屏蔽底层差异的分布式处理架构

特性：动态易于扩展、虚拟化

主要特点：

1、宽带网络连接 用户需要通过宽带网络接入“云”中并获得有关的服务，“云”内节点之间也通过内部的告诉网络连接

2、快速、按需、弹性的服务 用户可以按照实际需要迅速获取或释放资源，根据需要对资源进行动态扩展

服务类型：

1. IaaS(基础设施即服务) 向用户提供计算机能力、存储空间等基础设施方面的服务，需要较大的基础设施投入和长期运营管理经验，单纯出租资源，盈利能力有限
2. PaaS(平台即服务) 向用户提供虚拟的操作系统、数据库管理系统、Web应用等平台化的服务，重点不在直接的经济效益，而更注重构建和形成紧密的产业生态
3. SaaS(软件即服务) 向用户提供应用软件（如CRM、办公软件等）、组件、工作流等虚拟化软件的服务，一般采用Web技术和SOA架构，通过Internet向用户提供多租户、可定制的应用能力，大大缩短了软件产业的渠道链条，减少了软件升级、定制和运行维护的复杂程度，并使软件提供商从软件产品的生产者转变为应用服务的运营者

结构：

资源池：集群管理的各种基础硬件资源，如CPU、存储和网络宽度

云操作系统：通过虚拟化技术对资源池中的各种资源进行统一调度管理

云平台接口：用户调用计算机资源的接口

分类：

公有云：第三方提供商用户能够使用的云，一般可通过Internet使用，可能是免费或成本低廉的

私用云：为一个客户单独使用而构建的

混合云：将公有、私有两种模式结合起来，根据需要提供统一服务的模式

**大数据**

定义：无法在一定时间范围内用常规软件工具进行捕捉、管理和处理的数据集合，是需要新处理模式才能具有更强的决策力、洞察发现力和流程优化能力的海量、高增长率和多样化的信息资产

特征：5个VVolume（大量）、Variety(多样)、Value(价值)、Velocity(高速)、Veracity(真实性)，体量大、结构多样、时效性强，需要采用新型计算架构和智能算法等新技术

过程：数据准备、数据存储与管理、计算处理、数据分析、知识展现

作用：实现数据的“增值”，数据之和的价值远大于数据的价值之和

技术：大规模并行处理（MPP）数据库。数据挖掘电网、分布式文件系统、分布式数据库、云计算平台、互联网和可扩展的存储系统

数据挖掘：

数据集成：将多个数据源中的数据合并并存放在一个一致的数据仓库中

数据交换：将数据转换或统一成适合挖掘的形式

数据清洗：将重复、多余的数据筛选清除，将缺失的数据补充完整，将错误的数据纠正或者删除，最后整理成为我们可以进一步加工、使用的数据

数据归约：在尽可能保持数据原貌的前提下，最大限度地精简数据量

**移动互联网**

定义：核心是互联网，在桌面互联网的补充和延伸，应用和内容仍是移动互联网的根本，移动互联网与PC互联网协调发展，共同服务经济社会，而不是替代PC互联网

特点：1、终端移动性 2、业务使用的私密性3、终端和网络的局限性4、业务与终端、网络的强关联性

新特点：1、重视对传感技术的应用2、有效地实现人与人的连接3、浏览器竞争及孤岛问题突出

**智慧城市**

主要部分：1、通过传感器或信息采用设备全方位地获取城市系统数据2、通过网络将城市数据关联、融合、处理、分析为信息3、通过充分共享、智能挖掘将信息信息变成知识4、结合信息技术，把知识应用到各行各业形成智慧

参考模型：

功能层：1.物联感知层2、通信网络层3、计算与存储层4、数据及服务支撑层5、智慧应用层

支撑体系：1、安全保障体系2、建设和运营管理体系3、标准规范体系

**互联网+**

作用：互联网+行动可以助推传统产业的转型升级，传统制造业企业采用移动互联网、云计算、大数据、物联网等，信息通信技术，改造原有产品及研发生产方式、互联网+各个传统行业、提升制造业数字化、网络化、智能化水平

重点： 智能制造、大规模个性化定制、网络化协调制造、服务型制造

发展：工业换联网通过系统构建网络、平台、安全三大功能体系，打造人、机、物全面互联的新型网络基础设施，形成智能化发展的新兴业态和应用模式

**智能制造2025**

人工智能核心：CPS：信息物理系统

工作：促进两化深度融合，加快从制造大国转向制造强国，需要电子信息产业有力支撑，大力发展新一代信息技术，加快发展制造和工业互联网，制订“互联网+”行动计划，推动移动互联网、云计算、大数据、物联网等应用，需要产业密切跟踪信息技术变革趋势，探索新技术、新模式、新业态，构建以互联网为基础的产业新生态体系

**补充说明（人工智能AI）**

AR终端： 营造虚拟和现实交织的新场景，提升效率效益和效果，硬件升级和融合发展是方向

VR终端：构建虚拟世界中沉浸式体验，全景虚拟和交互是特色，VR终端和平台争夺是焦点

AI（人工智能）：引领智能时代，让人类生产和生活更智能化，小企业也有机会抢占市场，如智能语音，视觉识别，医疗和养老领域智能专家系统，无人驾驶，无人机等，技术突破和市场潜力发掘是成功关键。

特征：

感知能力：感知外部世界、获取外部信息的能力

记忆和思维能力：能够存储感知到的外部信息及由思维产生的知识，对信息进行分析、计算、比较、判断、联想、决策

学习能力和自适应能力：与环境的相互作用，不断学习积累知识，能够适应环境变化

行为决策能力：对外界的刺激做出反应，形成决策并传达响应的信息

发展：

2020年 产业成为新的重要经济增长点

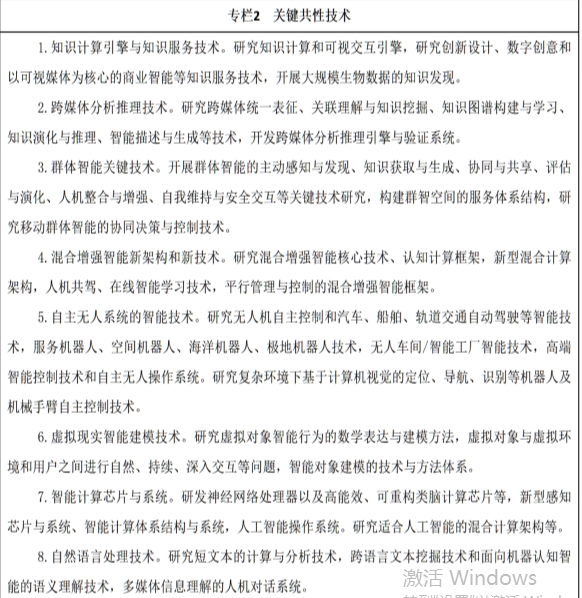
2025年 基础理论实现重大突破，部分技术与应用达到世界领先水平

2030年 理论、技术与应用总体达到世界领先水平

人工智能（Artificial Intelligence）,英文缩写为AI。它是研究、开发用于模拟、延伸和扩展人的智能的理论、方法、技术及应用系统的一门新的技术科学。

人工智能领域的研究包括机器人、语言识别、图像识别、自然语言处理和专家系统等

实际应用：机器视觉，指纹识别，人脸识别，视网膜识别，虹膜识别，掌纹识别，专家系统，自动规划，智能搜索，定理证明，博弈，自动程序设计，智能控制，机器人学，语言和图形理解，遗传编程等。



**IW**

使科幻成为现实，方便随身的智能助手，医疗健康养生养老潜力大，多功能转化和专业化成为两大方向

**区块链**

特征:分布式数据存储、点对点传输、共识机制、加密算法等计算机技术的新型应用模式，所谓共识机制是区块链系统中实现不同节点之间建立信任、获取权益的数学算法去中心化、公开透明，让每个人均可参与数据库记录

概念：

交易：一次操作，导致账本状态的一次改变，如添加一条记录

区块：记录一段时间内发生的交易和状态结果，是对当前账本状态的一次共识

链：由一个个区块按照发生顺序串联而成，是整个状态变化的日志记录

应用：比如比特币、分布式账本

层次：

数据层：封装了底层数据区块及相关的数据加密和时间戳等基础数据和基本算法

网络层：包括分布式组网机制、数据传播机制和数据验证机制

共识层：封装网络节点的各类共识算法

激励层：将经济因素集成到区块链技术体系中来，主要包括经济激励的发行机制和分配机制

合约层：主要封装各类脚本、算法和智能合约，是区块链可编程特性的集成

应用层：封装了区块链的各种应用场景和案例

所谓区块链技术，简称BT（Blockchain technology）,也被称为分布式账本技术，是一种互联网数据库技术，其特点是去中心化、公开透明，让每个人均可参与数据库记录。

最早是比特币的基础技术，目前世界各地均在研究，可广泛应用于金融等领域，区块链的基本原理理解起来并不难。基本概念包括：

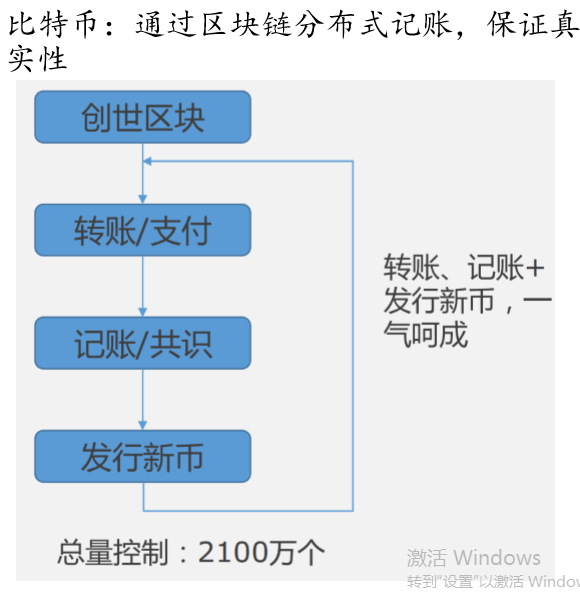
1、交易（Transaction）:一次操作，导致账本状态的一次改变，如添加一条记录；

2、区块（Block）：记录一段时间内发生的交易和状态结果，是对当前账本状态的一次共识；

3、链（Chain）:由一个个区块按照发生顺序串联而成，是整个状态变化的日志记录。

4、如果把区块链作为一个状态机，则每次交易就是试图改变一次状态，而每次共识生成的区块，就是参与者对于区块中所以交易内容导致状态改变的结果进行确认。

用通俗的话阐述：如果我们把数据库假设成一本账本，读写数据库就可以看做一段时间内找出记账最快最好的人，由这个人来记账，然后将账本的这一页信息发给整个系统里的其他所有人、这也就相当于改变数据库所有的记录，发给全网的其他每个节点，所有区块链技术也称为分布式账本



区块链是分布式数据存储、点对点传输、共识机制、加密算法等计算机技术的新型应用模式

区块链（Block chain）是比特币的一个重要概念，它本质上是一个去中心化的数据库，同时作为比特币的底层技术。

区块链的一些领域可以是：智能合约、证券交易、电子商务、物联网、社交通讯、文件存储、存在性证明、身份验证、股权众筹

特征：去中心化、开放性、自治性、信息不可篡改、匿名性

区块链的进化方式是

区块链1.0------------数字货币

区块链2.0------------数字资产与智能合约

区块链3.0------------各种行业分布式应用落地

区块链分为三类：

公有区块链（Public Block Chains）:世界上任何个体或者团体都可以发送交易，且交易能够获得该区块链的有效确认，任何人都可以参与其共识过程。

联合（行业）区块（Consortium Block Chains）:由某个群体内部指定多个预选的节点为记账人，每个块的生成由所有的预选节点共同决定（预选节点参与共识工程），其他接入节点可以参与交易，但不过问记账过程（本质上还是托管记账，只是变成分布式记账，预选节点的多少，如何决定每个块的记账这成为该区块链的主要风险点），其他任何人可以通过该区块链开发的API进行限定查询

私有区块链（private Block Chains）：仅仅使用区块链的总账技术进行记账，可以是一个公司，也可以是个人，独享该区块链的写入权限，本链与其他的分布式存储方案没有太大区别。

**特别联网（adhocnet working）**

指具有动态自组织能力的短距离无线通信联网，一种特殊的无线移动通信网络，网络中所有节点的地位平等，无需设置任何中心控制节点，具有很强的抗毁性，网络中的节点不仅具有普通移动终端所需要的功能，而且具有报文转发能力，当通信源节点不在直接通信范围之内，可以通过中间节点转发报文进行通信

## 1.6信息系统安全技术

**信息安全相关概念**

**信息安全属性**

1. 秘密性 信息不被未授权者知晓的属性
2. 完整性 信息是正确的、真实的、未被篡改的、完整无缺的属性
3. 可用性 信息可以随时正常使用的属性

**设备的安全**

1. 稳定性 在一定时间内不出故障的概率
2. 可靠性 在一定时间内正常执行任务的概率
3. 可用性 随时可以正常使用的概率

**行为安全**

1. 密码性 行为的过程和结果不能危害数据的秘密性。必要时，行为的过程和结果也应是秘密的
2. 完整性 行为的过程和结果不能危害数据的完整性，行为的过程和结果是预期的
3. 可控性 当行为的过程出现偏离预期时，能够发现、控制或纠正

**保障信息安全的技术**

1. 硬件系统安全技术、操作系统安全技术 信息系统安全的基础
2. 数据库安全技术、软件安全技术
3. 网络安全技术 是关键技术，防火墙、VPN、防病毒、身份认证、数据加密、安全审计、网络隔离
4. 密码技术 是关键技术
5. 恶意软件防治技术、信息隐藏技术、信息设备可靠性技术

**信息系统的安全保护等级**

第一级 个人合法权益造成损害

第二级 个人合法权益严重损害，或社会利益遭到损害

第三级 公共利益造成严重损害或国家安全造成损害

第四级 公共利益造成特别严重损害国家安全造成严重损害

第五级 国家安全造成特别严重损害

**计算机系统安全保护能力的五个等级**

用户自主保护级

系统审计保护级

安全标记保护级

机构化保护级

访问验证保护级

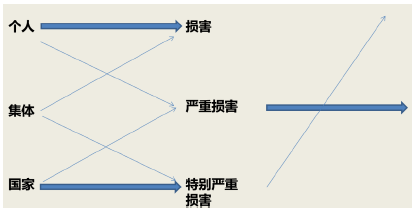
主审计划问（户籍全解放）：

1. 用户自主保护级（普内网用户）
2. 系统审计保护级（商务活动非重要单位）
3. 安全标记保护级（地方各级）
4. 结构化保护级（中央级）
5. 访问验证保护级（国防关键部门或特殊隔离单位）

**人员管理**

首先要求加强人员审查

信息安全教育对象 与信息安全相关的所有人员，领导和管理人员，工程技术人员，一般用户



**加密技术**

对称密钥算法 加密和解密采用相同的密钥，加密速度快，一般用来加密大量数据（SDBI、IDEA（128位）、RC4、DES（64位）、3DES（128位））

非对称密钥算法 加密和解密采用不同的密码，发送者用接收者的公钥（可以公开的密钥）加密，接收者收到信息后要用自己的私钥解密。加密速度较慢，一般用在少量数据的加密中，基于大合数因子分解困难性的RAS密码类、基于离散对数问题困难性的ELGamal密码类

**数字签名**

作用 证明当事者的身份和数据真实性的一种信息

条件

1. 签名者事后不能抵制自己的签名
2. 任何其他人不能伪造签名
3. 如果当事的双方关于签名的真伪发生争执，能够在公正的仲裁者面前通过验证签名来确认其真伪。

方法 利用RSA密码可以同时实现数字签名和数据加密

**认证**

作用 鉴别、确认，它是证实某事是否名副其实或是否有效的一个过程

和加密的区别 加密用以确保数据的保密性，阻止对数的被动攻击，如截取、窃听等，认证用以报文发送者和接收者的真实性以及报文的完整性，防止对手的主动攻击，如冒充、篡改、重播等。

和签名技术区别

1. 认证总是基于某种收发双方共享的保密数据来认证被鉴别对象的真实性，而数字签名中用于验证签名的数据是公开的
2. 认证允许收发双方互相验证其真实性，不准许第三者验证，而数字签名允许收发双方和第三者都能验证
3. 数字签名具有发送方不能抵赖、接收方不能伪造和具有在公证人前解决纠纷的能力，而认证则不一定具备。

**计算机设备安全**

内容

计算机实体

信息的

**完整性**

**机密性**

**抗否认性** 能保障用户无法在事后否认曾经对信息进行的生成、签发、接收等行为的特性，通过数字签名来提供抗否认服务

**可用性**

**可审计性** 利用审计方法，可用对计算机信息系统的工作过程进行详尽的审计跟踪，同时保存审计记录和审计日志，从中可以发现问题

**可靠性**

包含

物理安全 场地安全（环境安全）主要是场地与机房

设备安全 包括设备的防盗和防毁，防止电磁信息泄露，防止线路截获、抗电磁干扰及电源的包含

储存介质安全 介质本身和介质上存储数据的安全，介质的防盗；介质的防毁、如防霉和防砸

可靠性技术 采用容错系统实现，冗余设计来实现，已增加资源换取可靠性

**防火墙**

一种较早使用，实用性很强的网络安全防御技术，它阻挡对网络的非法访问和不安全数据的传递，使得本地系统和网络免于收到许多网络安全威胁

在网络安全中，防火墙主要用于逻辑隔离外部网络与受保护的内部网络

防火墙主要是实现网络安全的安全策略，而这种策略是预先定义好的，所以是一种静态安全技术

在策略中涉及的网络访问行为可以实施有效管理，而策略之外的网络访问行为则无法控制

防火墙的安全策略有安全规则表示

**入侵检测与防护**

入侵检测系统

注重的是网络安全状况的监管，通过监视网络或系统资源，寻找违反安全策略的行为或攻击迹象，并发出报警，大多数IDS系统都是被动的

入侵防护系统

倾向于提供主动防护，注重对入侵行为的控制，预先对入侵活动和攻击性网络流量进行拦截，避免其造成损失，通过直接嵌入到网络流量中实现这一功能的，即通过一个网络端口接收来自外部系统的流量，通过检查确认其中不包含异常活动或可疑内容后，再通过另外一个端口将它传送到内部系统中。这样一来，有问题的数据包，以及所有来自同一数据流的后续数据包，都能在IPS设备中被清除掉。

**VPN(虚拟专用网络)**

在公用网络中建立专用的、安全的数据通信通道的技术，可以认为是加密和认证技术在网站传输中的应用，连接由客户机、传输介质和服务器三部分组成、不是采用物理的传输介质，而是使用称之为“隧道”的技术作为传输介质，这个隧道是建立在公共网络或专用网络基础之上的

常见的隧道技术有：点对点隧道协议（PPTP）、第2层隧道协议（L2TP）和IP安全协议（IPSec）

**安全扫描**

漏洞扫描、端口扫描、密码类扫描（发现弱口令密码），扫描器的软件来完成，是最有效的网络安全检查工具之一，它可以自动检测远程或本地主机、网络系统的安全弱点以及所存在可能被利用的系统漏洞。

**蜜罐技术**

主动防御技术，是入侵检测技术的一个重要发展方向，也是一个“诱捕”攻击者的陷阱，蜜罐系统是一个包含漏洞的诱骗系统，它通过模拟一个或多个易受攻击的主机和服务，给攻击者提供一个容易攻击的目标。攻击者往往在蜜罐上浪费时间，延缓对真正目标的攻击，可以对入侵的取证提供重要的信息和有用的线索，便于研究入侵者的攻击行为。

**无线网络安全技术**

无线公开密钥802基础设施（WPKI）、有线对等加密协议（WEP）、Wi-Fi网络安全接入（WPA/WPA2）、无线局域网鉴别与保密体系（WAPI）、802.11i(802.11工作组为新一代WLAN指定的安全标准)

**按行为分**

1. 切断 对可用性的威胁，系统的资源被破坏或变得不可用或不能用，如破坏硬盘、切断通信线路或使文件管理失效
2. 截取 对机密性的威胁，未经授权的用户、程序或计算机系统获得了对某资源的访问，如在网络中窃取数据及非法拷贝文件和程序
3. 篡改 对完整性的攻击，未经授权的用户不仅获得了对某资源的访问，而且进行篡改，如修改数据文件中的值，修改网络中正在传送的消息内容
4. 伪造 对合法性的威胁，未经授权的永久将伪造的对象插入到系统中，如非法用户把伪造的消息加到网络中或向当前文件加入记录

**安全威胁**

1. 计算机病毒
2. 逻辑炸弹
3. 特洛伊木马
4. 后门 嵌在操作系统中的一段非法代码，渗透者可以利用这段代码侵入系统，安装后面就是为了渗透。
5. 隐蔽通道 系统中不受安全策略控制的、违反安全策略、非公开的信息泄露路径。

**分类**

1. 身份认证机制 实施强认证方法，比如口令、数字证书等
2. 访问控制机制 实施细粒度的用户访问控制，细化访问权限等
3. 数据保密性 对关键信息，数据要严加保密
4. 数据完整性 防止数据系统被恶意代码破坏，对关键信息进行数字签名技术保护
5. 系统的可用性 操作系统要加强应对攻击的能力，比如防病毒，防缓冲区溢出攻击等。
6. 审计 一种有效的保护措施，在一定程度上阻止对计算机系统的威胁，并对系统检测，故障恢复方面发挥重要作用。

**数据库系统安全**

可以认为是用于存储而非传输的数据的安全问题

方法：

数据库访问控制技术

数据库加密技术

多级安全数据库技术

数据库的推理控制问题

数据库的备份与恢复

**应用系统安全**

以计算机设备安全、网络安全和数据库安全为基础

Web威胁防护

威胁：

可信任站点的漏洞；浏览器和浏览器插件的漏洞；终端用户的安全策略不健全；携带恶意软件的移动存储设备；网络钓鱼；僵尸网络；带有键盘记录程序的木马

技术

1. WEB访问控制技术

IP地址、子网或域名；用户名/口令;公钥加密体系PKI（CA认证）

1. 单独登录（SSO）技术
   1. 一点登录，多点单位
   2. 具有数字证书的加密和数字签名技术，基于统一的策略的用户身份认证和授权控制功能，对用户实现集中统一的管理和身份认证
2. 网页防篡改技术
   1. 时间轮询技术
   2. 核心内嵌技术
   3. 事件触发技术
   4. 文件过滤驱动技术
3. Web内容安全
   1. 电子邮件过滤
   2. 网页过滤
   3. 反间谍软件

## 1.7信息化发展与应用