

信息热词检测结果

检测范围 百度百科

检测结论

重复率：43.93454724409449%

互联网+

互联网+概念于2012年11月易观国际董事长兼首席执行官于扬首次提出 并于2015年7月4日 国务院印发了《国务院关于积极推进“互联网+”行动的指导意见》 “互联网+”作为知识社会创新2.0推动下的互联网形态演进 成为了中国互联网发展的新形态和新业态 “互联网+”既是互联网的移动与泛在 促进了传统行业与互联网的融合及应用 将数据、计算、知识三者融合 使创新渗入到各行各业 从而开创了创新驱动发展的“新常态”

三网融合

三网融合又可被称为“数位汇流” 是将电信网、计算机互联网和有线电视网三者互联互通 融合发展 从而为用户提供语音、数据和广播电视等服务 伴随着通信行业加快发展 传统的三网融合已逐渐成为当前互联网发展的趋势

数字城市

数字城市又称“智慧城市” 通过各种信息技术或创新思想 将城市的组成系统和服务集成化 从而提升资源利用效率 优化城市配置和服务 改善人民的生活质量 智慧城市把新一代信息技术充分运用在城市的各个行业中 基于创新2.0的城市信息化程度更加高级智能 逐步实现信息化、工业化与城镇化三者深度融合 有助于进一步缓解常见的“大城市病” 从而提高城镇化质量 以实现可动态的精细化管理

有关智慧城市的定义广泛 目前较为普遍认可的是：智慧城市是创新2.0下的城市新形态 是新一代信息技术基础 推进智慧城市 既是物联网、云计算等新信息技术应用 也是创新2.0的方法论应用 从而构建大众创新、用户创新、协同创新、开放创新为特征的城市可持续创新生态

个人媒体时代

个人媒体时代又称自媒体时代，主要通过个人现代化社交媒体、传播等手段，受众人群是不确定的大多数或确定的单个人，传递规范性和非规范性信息的媒介时代。个人媒体时代依靠其本身的交互性、自主性，使新闻等信息的自由度显著提高，传媒生态发生了前所未有的转变。

在自媒体时代，经济收入增长提高了个体的行动能力，面对灾害的个体自我动员能力也逐步提高。然而其社会组织能力依旧停滞在较低水平，政府与民间互信程度下降。在互联网上，每一个账号，都如同一个小媒体，可以自行发布帖子、转发微博、评论新闻等，由此每一个互联网公民的信息、观点以及态度融入了互联网。例如，目前对自媒体的粗略估计，我国境内的50余家微博客网站中，每天更新帖文一般可达2亿多条。

电子政府

电子政府又称电子政务、数字政府、在线政府等 电子政府是通过数字化技术将政府到公民（政府-公民称为：government and citizens 简称G2C 下同）、政府到企业（government and businesses/Commerce G2B）、政府到员工（government and employees G2E）甚至于政府到政府之间（government and governments /agencies G2G）连接 电子政务的模式一般归纳如下：

G2C (政府到公民 Government to Citizens)

G2B (政府到企业 Government to Businesses)

G2E (政府到员工 Government to Employees)

G2G (政府之间 Government to Governments)

C2G (公民到政府 Citizens to Governments)

其中 数字化主要包括政府管理、信息和通讯技术 (简称：ICT)、企业流程再造 (简称：BPR)和电子公民等 也包括国际、国家、省级、市级各级政府

虚拟现实 (VR)

虚拟现实（英语：virtual reality 缩写VR）简称虚拟技术 也称虚拟环境 通过计算机模拟构造一个三维

空间 在这个三维空间中虚拟世界 从而向用户推送关于视觉等感官的模拟 让用户感觉身在虚拟世界 VR可以支持即时、无限制地观察虚拟空间内的事物 当用户移动位置时 计算机可以马上通过复杂运算 然后向用户传送精确的三维世界影像 从而使用户产生临场感 虚拟技术利用了人工智能、计算机图形、计算机仿真、显示及网络并行处理等技术 **是一种高新技术模拟系统**

增强现实 (AR)

增强现实 (Augmented Reality 简称AR) 有时也翻译为实拟虚境、扩张现实等 AR是指在图像分析技术的基础上 **对摄影机影像的位置和角度进行精确计算 从而使显示屏上的虚拟世界与现实世界场景进行交互的技术** AR于1990年首次提出 **伴随着电子产品运算能力优化 使增强现实的用途变得更广泛**

自媒体

自媒体也称“公民媒体”或“个人媒体”是指私人化、平民化、普泛化、自主化的个体传播者利用现代化、电子化的手段 向不特定的大多数或者特定的单个人传递规范性及非规范性信息的新媒体的总称 意指在网络技术 特别是Web2.0的环境下 由于博客、微博、共享协作平台、社交网络的兴起 使每个人都具有媒体、传媒的功能

有人认为因为自媒体发表容易 所以称为草根媒体 但实际上的草根层次结构较接受的是和自媒体相对的大众媒体 自媒体也是相对传统新闻方式的表述 即具有传统媒体功能却不具有传统媒体运作架构的个人网络行为

互联网数据中心 (IDC)

IDC的服务对象是**互联网内容提供商 (ICP)、企业、媒体和各类网站等** 主要提供的业务是服务器托管、空间租用、网络批发带宽以及ASP、EC等业务 业务特点是大量可靠、安全可信 IDC作为各种模式电子商务安全运作的基础设施 **也可作为企业、商业联盟 (包括分销商、供应商、客户等) 实施价值链管理的支撑平台**

数据中心包含网络、服务两方面概念 **是网络基础资源的组成部分** 主要提供数据传输服务和高速接入服务 给用户综合全面的解决方案 例如 为了使企业和个人更便捷地通过网络开展业务 减少信息技术方面的顾虑 **数据中心为政府、企业上网等提供专业服务**

虚拟专用网络 (VPN)

VPN属于一种通讯方法 常应用于连接团体与团体或中、大型企业或私人网络等 它具有保密性强、信息安全准确等特点 其实现原理是利用隧道协议 (Tunneling Protocol) 以达到以上信息安全效果 在日常使用场景中 即使是通过不安全的网络 (例如: 互联网等) 传输信息 VPN也可以保证信息的安全可靠

其中需要注意的是 是否加密信息是可以人为控制的 例如 **被加密的VPN** 其信息仍旧可能被窃取

办公自动化 (OA)

办公自动化 (Office Automation 简称: OA) 指通过计算机等电子设备和软件 基于数字化技术 从创建到处理乃至传播过程 均通过信息化手段实现

其中 其基本活动是原始数据的存储、电子业务等信息管理 随着数字化信息的发展 相关工作人员之间可实现信息共享、工作协同等 **简化了办公流程 提升了工作效率**

企业资源计划 (ERP)

企业资源计划 (Enterprise resource planning 简称: ERP) 也被称为企业资源规划 在1990年由美国高德纳咨询公司首次提出 企业资源计划最初是指应用软件 (APP) 并且逐渐被国际上的商业企业推广 逐渐发展为现代企业管理理论 作为企业工作流程再造的有力工具

ERP是一个创建在信息技术基础上的系统化管理思想 **为企业决策层及员工提供决策运行手段的管理平台**

二维码

二维码又被称为二维条码 它是由一维条码发展而来 其数据被化成二进制 然后将二进制数据储存在黑白矩形图案中 通过电子设备扫描即可查看

其中 **一维码和二维码的区别是: 一维条码仅在一个方向上 (一般是水平方向) 存储信息** 其垂直方向的高度常为了便于阅读器读取信息 但二维条码在垂直和水平方向均记载着数据 二维码与一维码相比较 二维码多了“定位点”和“容错机制” “定位点”是指二维码上的三个定位角点 **使得扫描设备**

即使从不同方向进行扫描 也可快速读取二维码信息；“容错机制”是指条码部分损坏或污染 其信息仍然能够被还原 并且不同类型的二维码有不一样的容错能力

交互式网络电视（IPTV）

IPTV是通过宽带网络作为电视信号来源的一种宽带电视 其原理是将电视节目信息通过网际协议（Internet Protocol 简称：IP）传送给用户 IPTV服务也常被称为“三合一服务”、“三重服务” 因为IPTV一般需要使用网络 所以服务供应商通常会一并提供联网及IP电话等相关服务

虽然IPTV使用了宽带网络及网际协议 但IPTV也可以不通过互联网进行传输 选择封闭式Intranet（内部网）进行传输

可穿戴设备

可穿戴设备是一种可以穿戴在身上或装饰在人们的衣服、配件上的便携式硬件设备 它是通过软件进行数据交互、云端交互 从而实现广泛的应用 可穿戴设备给我们的生活带来了极大的便捷

共享经济

共享经济建立在不同个体或组织之间 主要对商品、服务等进行有偿或无偿共享 例如 共享汽车、交换住宿等 共享经济通过弱化拥有权 达到强化使用权的目的使物质利用效率尽可能最大化 在共享经济下 目前较为广泛的共享模式是 生产制造可以专门用于“共享”的商品 而不是将闲置资源进行共享 这种共享模式本质上其实是“租赁经济” 一些共享企业为了快速占有市场 利用资本大量投放“共享”商品 反而造成了浪费 甚至产生一些社会问题 例如 大量的共享单车乱停乱放 造成道路拥堵 还被堆成了“共享单车坟墓” 造成了极大的浪费

移动支付

移动支付是指通过移动设备付款的服务 目前较为主流的移动支付方式有以下五种类型：使用短信的转账支付、移动应用支付（APP）、移动账单付款、非接触型支付（NFC）和移动设备网络支付（WAP）

2019年1月24日 交通运输部新闻发言人吴春耕在举行的例行新闻发布会上表示 2019年交通运输部紧紧抓住最直接、最现实人民群众最关心的利益问题 共列出12项民生实事任务的清单 以推动交通运输改革发展成果惠及全体人民 例如 2019年高速公路人工收费车道实现手机移动支付全覆盖 包括260个地级市以上城市交通一卡通互联互通等

智能硬件

智能硬件是指通过软件和硬件结合 改造传统设备 进而让其设备智能化 智能化硬件具有连接能力 可以加载互联网服务 构建“云+端”的架构 可支持大数据等服务 智能硬件移动应用是加载在智能硬件上的应用软件 通过移动应用可以连接智能硬件 便于开发 用户操作简单 支持多种应用功能 为企业获取用户提供了重要入口

智能改造的对象可以是电子设备（例如：手表、电视等其他电器） 也可以是曾经未被电子化的设备 例如：门锁、汽车、茶杯等 智能硬件的应用已经推广到各个领域 例如：智能家居、智能汽车、智能医疗、机器人等领域 常见的智能硬件有：可测温水杯、Google Glass、运动手环、Tesla、智能冰箱等

智能家居

智能家居主要采用安全防范、网络通信、自动控制等先进技术 基于住宅平台 集成了人们的家居生活有关的设施 从而构建智能的住宅设施与家庭事务结合的管理系统 全面提升了家居安全性、舒适性、艺术性和便利性 打造一个环保节能的居住环境

车联网

车联网是通过采集车辆位置、速度和路线等信息构成的交互网络 车联网使用了摄像头、传感器、GPS、RFID等装置 车辆可以完成自身位置和状态信息的采集 例如 日常生活中常用的导航系统 就是所有车辆通过互联网将车辆行驶信息传输到中央处理器 进行信息采集和处理后 从而及时汇报实时路况 计算出不同车辆的最佳路线、安排信号灯周期

工业4.0

工业4.0是基于工业发展阶段进行划分 按照目前的共识 蒸汽机时代划分为工业1.0 电气化时代划分为工业2.0 信息化时代划分为工业3.0 工业4.0则是智能化时代 即基于信息化技术促进产业变革的时代 工业4.0最早于 2013年4月在德国的汉诺威工业博览会上被正式提出 其主要目的是提高德国工业的竞

争力 在新的工业革命中抢占先机 这是德国政府《德国2020高技术战略》（简称：《战略》）中的十大未来项目之一 该《战略》由德国联邦教育局及研究部和联邦经济技术部联合资助 预计投资高达2亿欧元 工业4.0的技术基础是网络实体系统及物联网

在2015年5月 我国国务院正式印发《中国制造2025》 部署全面推进实施制造强国战略 **工业4.0进入了中德合作新时代** 在《中德合作行动纲要》中共有4条工业4.0合作内容 双方一致认为 **两国政府应为企业参与该进程提供政策支持**

零售O2O

O2O（Online To Offline，简称：O2O）最早由美国提出，是指将线下的商务机会与线上互联网结合，让互联网成为线下交易的平台。O2O的概念比较宽泛，同时涉及线上和线下可以通称为O2O。从2013年起，O2O步入了高速发展时期，本地化及移动设备走向整合与完善。O2O商业模式就此衍生，这成为了O2O模式下的本地化分支。

智慧农业

智慧农业是指智慧经济下的农业或者是智慧经济形态在农业中的具体表现 在发展中国家中 **智慧农业成为了智慧经济的主要组成 是发展中国家消除贫困、经济发展的重要途径**

智慧农业从农作物的生产到销售均可涉及 例如 农业生产监测是通过在农田、温室、园林等目标区域的传感节点 实时采集温度、湿度、光照、土壤水分等生态信息 将采集信息并传输到中央控制系统 农业生产人员可通过监测数据对环境进行分析 **开展有针对性地的农业活动** 以实现农业生长环境的智能控制

3D打印

3D打印是以数字模型文件为基础 采用粉末状金属、塑料等可粘合材料作为原始打印材料 通过逐层打印来构造物体的快速成型技术

3D打印常使用数字技术材料打印机 被应用于模具制造、工业设计、工程和施工（AEC）、航空航天、土木工程、牙科和医疗产业、地理信息系统等领域 现在也可被用于产品的直接生产 例如：打印零部件；打印生物实验材料 2019年1月14日 **美国加州大学圣迭戈分校首次利用快速3D打印技术** 制造出模仿中枢神经系统结构的脊髓支架 成功帮助大鼠恢复了运动功能

大数据

大数据（Big data）也被称为巨量资料 是指超出传统数据处理应用软件处理能力的术语 **也可指那些多种数据来源的非结构化或结构化的大量数据** 在学术研究方面 **大数据出现推出了许多主题研究的新颖方案** 这也在一定程度上推动了大数据统计方法的发展 其中 **需要注意的是 大数据只是观察和追踪发生的事情 它并未对数据进行抽样** 因此 大数据包含的数据集大小常常远远超出传统软件在一定时间内处理的能力 随着技术的发展 **发布新数据更加便利** 世界各国政府对数据高透明度的要求 大数据分析在现代研究中愈渐火热

分布式存储

分布式存储是一种通过网络利用企业中的机器上的磁盘空间 并将这些分散的存储资源构建成虚拟的存储设备 将数据分散存储在不同的机器上

数据挖掘

数据挖掘（Data mining）属于跨学科的计算机科学分支 它利用人工智能、统计学、机器学习和数据库的交叉方法 **从较大型的数据集中发现大数据中数据信息呈现的规律性、价值点等** 数据挖掘总目标是从一个庞大数据集中提取价值信息 并将其转换成人们可理解的数据结构 以方便企业等组织进一步利用 **除了对数据的原始分析 它还包括数据库和数据管理方面、数据预处理、兴趣度量、复杂度的考虑、模型与推断方面考量等** 以及收发数据的可视化呈现、在线实时更新等后处理 **数据挖掘是“数据库知识发现”的分析步骤 类似“数据捕鱼”、“数据捕捞”和“数据探测” 这些是指用数据挖掘方法** 可能由于采样过小 导致无法可靠地统计推断出信息的有效性 但可以用来创建新的假设以检验更大数据总体

数据挖掘的基本任务

数据挖掘包括：分类、聚类分析、关联度分析、回归分析、预测、序列分析等

一、分类：

分类是找出一组数据对象的相同特征 再按照一些分类模式将其划分为不同的类 其目的是利用分类模型 将数据项映射给某个类别 分类可以应用在用户特征分类、识别并划分用户属性和用户特征分析、用户的购买趋势预测等 例如 汽车零售商可把不同消费者对汽车的喜好标准划分成不同的消费者类 这样售车人员就可以特定分类的汽车宣传册发放给特定喜好的消费者 实现精准营销

常见的分类算法：决策树算法、神经网络算法、贝叶斯算法等

二、聚类分析：

聚类分析是一种较细的分类方法 它基于一组事例的属性进行分组 聚类后的同一类在某种程度上有一定相似的属性值

聚类分析是将一组数据按照相似性和差异性进行分类 最终使得属于同一类的数据间的相似性尽可能大 不同类的数据间的差异性尽可能大 它同样可以应用到客户群体的分类、客户购买趋势预测、市场的细分等

三、关联度分析：

数据关联是数据库中被发现的一种关联关系 比如 两个或多个变量的取值之间存在某种规律性 就称为关联 这种关联可被分为简单关联、因果关联、时序关联等 关联分析是为了便于找出数据集中隐藏的关联网 有时数据库中数据的关联函数未知或者不确定 因此关联分析生成的规则应该带有可信度 有一个经典案例是 曾经沃尔玛经过大量数据分析 发现购买尿不湿的男人们 为了奖励自己 会额外购买啤酒 因此沃尔玛为了提升啤酒销量 会在尿不湿旁边摆放啤酒

四、回归分析：

回归任务与分类任务有一些相似 但回归分析不查找描述类的模式 它通过查找模式以确定数值 例如 线性回归的结果是一个函数 可以根据输入的值确定输出

回归分析方法常被广泛地应用于解释市场占有率、销售额、品牌偏好及市场营销效果 把两个或两个以上定距或定比例的数量关系用函数形势表示出来 就是回归分析要解决的问题

五、预测：

预测技术采用数列作为输入 表示一系列时间值 然后应用各种能处理数据周期性分析、趋势分析、噪声分析的计算机学习和统计技术来估算这些序列未来的值

六、序列分析：

发现离散序列中的模式 序列由一串离散值（或状态）组成 例如：DNA序列、Web点击的网址序列、购买商品的次序等 序列数据和时间序列数据观察值都是连续的 观察值之间相互依赖 它们的区别在于序列表现为离散的状态 而时间序列表现为连续的数值；序列和关联数据的相似之处是包含一个项集或一组状态 它们的区别是序列模型分析状态转移 而关联模型忽略个体间差异 比如 认为购物篮的每个商品平等且独立 序列认为先买电脑还是先买扬声器是两个不同序列 而关联则认为是相同的 常见的序列分析技术有马尔科夫链等

图论相关知识可用于描述某个新网站的Web点击序列 每个节点就代表一个URL地址 每一条边代表两个URL地址之间的转移 每一个转移用一个权值表示一个URL地址转到另一个URL的概率

七、偏差分析：

偏差分析又被称为比较分析 它将差异性和极端特例进行描述 常被用于揭示事物之间的偏离常规的异常现象

常见的偏差检测方法有：找出观测结果与参照值之间的有效性差别

数据挖掘的基本技术

神经网络方法

神经网络具有良好的鲁棒性、并行处理、分布存储和高度容错等特性 比较适用于数据挖掘 因此近年来越来越受到人们的关注

遗传算法

遗传算法是一种仿生全局优化方法 它基于生物自然选择与遗传机理进行随机搜索 从而找出最优结果 遗传算法具有良好的隐含并行性、模型之间结合性等性质 便于其在数据挖掘领域被加以应用

决策树方法

决策树是一种预测模型算法 它通过对大量数据进行有目的分类 从中找出一些有价值的、潜在的信息

它的主要优点有表示简单、分类速度快 适合于大规模的数据处理

粗集方法

粗集理论是一种研究不精确、不确定知识的数学工具 粗集方法有几个优点：可不用给出额外信息；简化输入信息的表达空间；算法简单 便于操作 粗集处理的对象是类似二维关系表的信息表

覆盖正例排斥反例方法

覆盖正例排斥反例方法利用覆盖所有正例、排斥所有反例的思想 以此来寻找规则 首先在正例集合中任选一个种子 将其带入到反例集合中逐个比较 与字段取值构成的选择子相容则舍去 相反则保留 按此思想循环所有正例种子 将得到正例的规则(选择子的合取式)

统计分析方法

在数据库字段项之间存在两种关系：函数关系和相关关系 对它们的分析可采用统计学方法 即利用统计学原理对数据库中的信息进行分析 可进行常用统计、回归分析、相关分析、差异分析等

模糊集方法

模糊集方法利用模糊集合理论对实际问题进行模糊评判、模糊决策、模糊模式识别和模糊聚类分析 系统的复杂性越高 模糊性越强 一般模糊集合理论是用隶属度来刻画模糊事物的亦此亦彼性的

什么类型的数据可以进行挖掘？

根据信息存储格式，用于挖掘的对象有关系数据库、数据仓库、空间数据库、面向对象数据库、时态数据库、文本数据源、多媒体数据库、异质数据库以及Internet等。

数据可视化

数据可视化是对数据的属性或者关系的研究 利用图或表等人们便于理解的图形化表示方法表示出来 其中 这种表现形式常常被定义为以某种概要形式抽提出来的信息 包括相应信息单位的各种属性和变量

为什么要进行数据预处理？

由于数据库中的数据极易受噪声、丢失数据和不一致数据的侵扰，因为数据库太大（一般在千兆字节乃至以上），并且大多来自于多个异构数据源。低质量的数据信息容易导致挖掘结果不佳，难以获取想要的价值信息。

当前衍生出大量数据预处理技术。例如，数据清理技术，常用来去掉数据中的噪声，纠正数据不一致；数据集成技术，将多个源的数据合并成一致的数据，再对其进行存储。

数据预处理的主要任务

数据清理通过填写缺失值、数据去噪、识别或删除一些离群点 以此解决数据不一致性 达到“清理”数据 如果数据清理不成功得到的数据就是脏数据 使挖掘结果难以具有可信度 并且脏数据可能导致挖掘过程陷入混乱 造成输出结果不可靠 即使大部分挖掘例程都会通过某些过程来处理不完整数据或噪声数据 但它们并非一直是鲁棒的 相反 更应该避免数据被建模函数过分拟合 因此 预处理的关键步骤是使用数据清理例程清洗数据

数据集成是将多个数据库、数据立方体或文件中的数据进行集成 其目的是在分析中使用多个数据源的数据

数据规约可以降低数据集规模 而且不损害数据挖掘结果 最终得到数据集的简化表示 数据规约后的体量更小 经典的数据归约策略有：维归约、数值归约等

数据变换是引导挖掘过程的一种有效的附加预处理过程

数据仓库

数据仓库是一种资讯系统的资料储存理论 它注重利用某些特殊资料储存方式 让数据更加有利于进行数据分析处理 从而获取有价值的信息并依此作决策

存储在数据仓库中的资料 一旦被存入就不再随时间而更动 并且存储的数据具有时间属性 例如 数据仓库中常含有大量的历史性资料 可通过特定分析方式 从其中发掘出价值信息

数据仓库的特点

主题导向 (Subject-Oriented)

主题导向区别于一般业务交易处理 (OLTP) 系统 数据仓库的资料模型设计 它更加看重将数据按意义进行归类 分类后的数据归至相同的主题区 (subject area) 所以被称为主题导向 举例如

Arrangement、Party、Product、Event等

集成性 (Integrated)

该数据来自企业各业务交易处理 (OLTP) 系统 在数据仓库中是集成过且一致的

时间差异性 (Time-Variant)

数据变动可以从数据仓库中通过纪录进行追踪 这样有利于反映出数据随着时间变化的数据变化轨迹

不变动性 (Nonvolatile)

数据一旦被确认写入后 无论数据是否错误 数据均不会被取代或删除

数据仓库的作用

数据仓库主要应用于数据库已大量存在的场景下 为了方便后续的数据挖掘、方便决策需要而产生 它并不是传统意义上的“大型数据库” 建设数据仓库的目的是为前端查询、分析奠定基础 因为数据有较大冗余 所以数据的存储要求也较高

操作数据库系统和数据仓库的区别

数据库和数据仓库在某些方面有一定的相似之处，两者都需要加载数据库软件，通过数据模型来组织、管理数据。两者的区别是，数据库常常关注业务交易处理 (OLTP)，而数据仓库更注重数据分析层面 (OLAP)，由此会导致两者的数据库模型上有较大差异。数据库一般追求交易的速度、完整性和一致性等，在数据库模型上主要遵从范式模型 (1NF, 2NF, 3NF等)，最大程度上减少数据冗余，保证引用完整性，而数据仓库注重效率，包括数据分析效率、查询速度、相关性分析，因此数据仓库更多使用多维模型，以提高数据分析的效率。

数据立方体

数据立方体是为了让用户从多个角度探索和分析数据集 一般同时考虑三个因素 (维度) 它是一类多维矩阵

如果想从一堆数据中提取信息 可以通过工具来找到在不同场景下的有关联的和重要的信息 例如 一份简单的数据报告 大多采用二维表示 即行和列构成的表格 这种情况仅适用于考虑两个因素 但在日常生活中 我们不止面对两个因素 因此需要使用更强大的工具

数据立方体是二维表格的多维扩展 就像几何学中立方体是正方形的三维扩展 “立方体” 可以将其看作是一组类似的互相叠加起来的二维表格 并且数据立方体不仅仅局限于三个维度 大多数在线分析处理 (OLAP) 系统能用很多个维度构建数据立方体 例如 微软的SQL Server 2000 Analysis Services工具 允许维度数高达64个 数据立方体之所以有价值 是因为我们能在一个或多个维度上给立方体做索引

有哪些数据防护技术？

计算机存储的信息日渐庞大，信息的价值也逐渐提升。为保障计算机数据安全，常常会采用许多安全防护技术。目前主流的数据安全防护技术如下：

磁盘阵列

磁盘阵列是将多个类型、容量、接口甚至品牌相同的磁盘或硬盘连接成一个阵列，读写磁盘数据速度更快、准确率更高、更加安全，从而达到数据读取速度和安全性的一种手段。

2) 数据备份

备份管理包括备份的历史记录的保存、可计划性、自动化操作或日志记录。

3) 双机容错

双机容错是为了保证系统数据和服务的在线性，即当某一系统发生故障时，另一个系统发挥作用，以保证正常向网络系统提供数据和服务，使得服务不至于停顿，双机容错能够在一定程度上数据不丢失、系统不宕机。

4) NAS

NAS解决方案通常作为文件服务的设备，由工作站或服务器通过网络协议和应用程序来进行文件访问，大多数NAS链接在工作站客户机和NAS文件共享设备之间进行。这些链接依赖于企业的网络基础设施来正常运行。

5) 数据迁移

数据迁移是指由在线和离线存储设备共同构成，构成了一个可以协调工作的存储系统，该系统存储系统中可支持动态管理数据，使得访问频率高的数据存放于性能较好的在线存储设备中，而访问频

率低的数据存放于较为廉价的离线存储设备中。

6) 异地容灾

以异地实时备份为基础的高效、可靠的远程数据存储，在各单位的IT系统中，必然有核心部分，通常称之为生产中心，往往给生产中心配备一个备份中心，该备份中心是远程的，并且在生产中心的内部已经实施了各种各样的数据保护。但是不管怎么保护，当火灾、地震这种灾难发生时，一旦生产中心瘫痪了，备份中心会接管生产，继续提供服务。

7) SAN

SAN支持服务器在共享存储装置中高速传送数据。其优点是带宽高、可用性高、容错能力强、优化升级更方便、容易进行管理，有助于优化系统的成本情况。

8) 数据库加密

对数据库中数据加密是为增强普通关系数据库管理系统的安全性，提供一个安全适用的数据库加密平台，对数据库存储的内容实施有效保护。它通过数据库存储加密等安全方法实现了数据库数据存储保密和完整性要求，使得数据库以密文方式存储并在密态方式下工作，确保了数据安全。

9) 硬盘安全加密

通过安全加密的故障硬盘，硬盘维修商根本无法查看，保证了内部数据的安全性。硬盘发生故障更换新硬盘时，可支持全自动智能恢复受损坏的数据。一定程度上防止企业内部数据因硬盘损坏、操作错误而造成的数据丢失

有哪些数据安全技术？

对应用系统使用、产生的介质或数据按其重要性进行分类，对存放有重要数据的介质，应备份必要份数，并分别存放在不同的安全地方（防火、防高温、防震、防磁、防静电及防盗），建立严格的保密保管制度。

保留在机房内的重要数据（介质），应为系统有效运行所必需的最少数量，除此之外不应保留在机房内。

根据数据的保密规定和用途，确定使用人员的存取权限、存取方式和审批手续。

重要数据（介质）库，应设专人负责登记保管，未经批准，不得随意挪用重要数据（介质）。

在使用重要数据（介质）期间，应严格按国家保密规定控制转借或复制，需要使用或复制的须经批准。

对所有重要数据（介质）应定期检查，要考虑介质的安全保存期限，及时更新复制。损坏、废弃或过时的重要数据(介质)应由专人负责消磁处理，秘密级以上的重要数据（介质）在过保密期或废弃不用时，要及时销毁。

机密数据处理作业结束时，应及时清除存储器、联机磁带、磁盘及其它介质上有关作业的程序和数据。

机密级及以上秘密信息存储设备不得并入互联网。重要数据不得外泄，重要数据的输入及修改应由专人来完成。重要数据的打印输出及外存介质应存放在安全的地方，打印出的废纸应及时销毁。

数据安全的特点有哪些？

机密性（Confidentiality）

保密性（secrecy）又被称为机密性 是指个人或团体的信息不为其他不应获得者获得 在电脑中 许多软件如邮件应用软件、浏览器等 都有保密性相关的设定 用以维护用户资讯的保密性 并且间谍档案或黑客会引发保密性的问题

完整性（Integrity）

数据完整性指在传输、存储信息或数据的过程中 确保信息或数据不被未授权的篡改或在篡改后能够被迅速发现 是信息安全的三要素之一 在信息安全领域使用过程中 常常和保密性边界混淆 以普通RSA对数值信息加密为例 黑客或恶意用户在没有获得密钥破解密文的情况下 可以通过对密文进行线性运算 相应改变数值信息的值 例如交易金额为X元 通过对密文乘2 可以使交易金额成为2X 也称为可延展性（malleably）为解决以上问题 通常使用数字签名或散列函数对密文进行保护

可用性（Availability）

数据可用性的中心是使用者 其易用性设计的重点在于让产品的设计能够符合使用者的习惯与需求 以

互联网网站的设计为例 希望让使用者在浏览的过程中操作更简单、使用体验更好 基于这个因素 任何有违信息的“可用性”都算是违反信息安全的规定 因此 许多国家如美国、中国均要求保持信息能够不受规限地流通

企业可以通过哪些方法维护数据安全？

备份关键的数据。

备份数据就是在其他介质上保存数据的副本。目前常见有两种备份方法：完整备份和增量备份。完整备份会把所选的数据完整地复制到其他介质。增量备份仅备份上次完整备份以来添加或更改的数据。

通过增量备份扩充完整备份通常较快且占用较少的存储空间。可以考虑每周进行一次完整备份，然后每天进行增量备份。但是，如果要在崩溃后恢复数据，则把花费较长的时间，因为首先必须要恢复完整备份，然后才恢复每个增量备份。如果对此感到担忧，则可以采取另一种方案，每晚进行完整备份；只需使备份在下班后自动运行即可。

通过实际把数据恢复到测试位置来经常测试备份是个好主意。这具有以下作用：确保备份介质和备份数据状况良好、确定恢复过程中的问题、可提供一定程度的信心。

不仅必须确保数据以精确和安全的方式得到备份，而且必须确保在需要进行恢复时，这些数据能够顺利地装回系统中。

建立权限。

操作系统和服务器都可对由于员工的活动所造成的数据丢失提供保护。通过服务器，可以根据用户在组织内的角色和职责而为其分配不同级别的权限。不应为所有用户提供“管理员”访问权，这并不是维护安全环境的最佳做法，而是应制定“赋予最低权限”策略，把服务器配置为赋予各个用户仅能使用特定的程序并明确定义用户权限。

对敏感数据加密。

对数据加密意味着把其转换为一种可伪装数据的格式。加密用于在网络间存储或移动数据时确保其机密性和完整性。仅那些具有工具来对加密文件进行解密的授权用户可以访问这些文件。加密对其他访问控制方法是一种补充，且对容易被盗的计算机（例如便携式计算机）上的数据或网络上共享的文件提供多一层保护。

物联网

物联网（Internet of Things 简写：物联网）属于互联网、传统电信网等信息承载体 可以使独立功能的普通物体实现互联互通 物联网常使用无线网 因为每个个体周围的设备可以达到上千个 所以物联网可能要包含500兆至1000兆个物体 在物联网上 每个人都可以应用电子标签将真实的物体上网联结 在物联网上都可以查出它们的具体位置

通过物联网可以用中心计算机对机器、设备、人员进行集中管理 也可以对家庭设备、汽车进行智能遥控 类似自动化操控系统 并且可以通过收集这些小体量、分散的数据 最终汇聚成大数据 例如 对车辆道路优化以减少车祸、灾害预测与犯罪防治、流行病控制等等社会的重大改变 实现物和物相联

物联网的特性

物联网是物物相连的

物物之间的信息交换和通信

物联网具有行业性

物联网的物物相连是众多物联网终端设备之间的相连

感知中国

“感知中国”就是中国的物联网 是中国发展物联网的一种形象称呼 通过在物体上植入各种微型感应芯片使其智能化 通过无线网络来实现人和物体之间的“对话” 物体和物体之间的“交流”

物联网展示了生活中任何物品都可以变得“有感觉、有思想”的智能图景 被认为是世界下一次信息技术浪潮和新经济引擎

物联网的架构分为哪几层？

目前物联网架构一般分为感知层、网络层和应用层三个层次 当然根据分类标准的不同 也有四层、五

层和七层架构的分法

感知层

感知层是物联网的皮肤和五官 **用于识别物体、感知物体、采集信息、自动控制** 例如 装在空调温度传感器识别到室内温度高于30度 **信息收集后** 空调自动进行制冷；感知层涉及到的是各种识别技术、信息采集技术、控制技术 同时这些技术交叉使用 **有单一的、综合的感知 比如机器人就是整合了各种感知系统** 属于综合感知 这一层最常见的就是各种传感器 用于替代或者延展人类的感官完成对物理世界的感知 也包括常见的RFID、二维码技术

网络层

网络层则主要实现信息的传递、路由和控制 主要分为两大部分：物联网的通信技术、物联网的通讯协议 通讯技术负责把物与物进行物理连接 使其可以进行通信；通讯协议负责建立通信规则和统一格式 通讯技术有着不同的分类标准 从介质上分为：有线网络、无线网络；从通信距离上分为：超短距、近距离、中长距离、超远距离

应用层

应用层基于各种物联网通讯协议 对物联网数据进行宏观分析 并将分析结果反馈到感知层 从而执行一些特定的控制功能 例如 **控制物与物之间的协同 物与环境的自适应性** 人与物的交互协作 应用层可粗略分为两大部分：通用的物联网平台、通用的物联网平台上再产生具体应用 其中 通用的物联网平台被建立在云平台之上 可以是IAAS/PASS/SAAS的一种或者混合 例如 **树根互联、SAP Leonardo、百度云天工、阿里Link物联网平台**；另外一种为通用的物联网平台上再产生具体应用 这些应用类似于手机App 具体应用就是如何具体控制这些物如何收集信息 如何进行控制物

射频识别技术（RFID）

射频识别技术(Radio Frequency Identification 简称：RFID)又称无线射频识别 是一种无线通信技术 可通过无线电信号识别特定目标 **读写相关数据** RFID不需要在识别系统与特定目标之间建立机械或光学接触 **其优点是非接触式识别** 可以穿过雪、雾、冰、涂料、尘垢等恶劣环境阅读标签 阅读速度极快 大多数情况下读取数据时间不超过100Ms

贴有RFID标记的物体若无主动通信能力 不能作为物联网终端设备 因此RFID常被用来进行物体识别 其物联网终端设备通常是RFID读写器或有源RFID设备 一般情况下 RFID的拓扑结构采用一对多方式（一个读写器对应多个贴有RFID标记的物体）

物联网的应用有哪些？

工业领域

工业领域所涵盖的能够联网的事物最丰富 比如印刷设备、车间机械、矿井与厂房 其中 **工业物联网的应用集中在石油天然气与工厂环境** 是目前物联网项目最多的应用领域

例如 **英特尔公司为俄勒冈的一家芯片制造厂安装了200台无线传感器** 用来监控部分工厂设备的振动情况 并在测量结果超出规定时提供监测报告 通过对危险区域/危险源（如矿井、核电厂）进行安全监控 能有效地遏制和减少恶性事件的发生

医疗领域

目前物联网技术在医疗行业中的应用包括人员管理智能化、医疗过程智能化、供应链管理智能化、医疗废弃物管理智能化以及健康管理智能化 例如 美敦力公司去年的一款自动胰岛素泵 MiniMed670G就是物联网传感技术在医疗领域应用实例 **其设备配备了血糖传感器** 释放胰岛素的泵以及能查看数据的显示仪 血糖传感器每5 分钟就会透过皮下软针所接收的血液来测量患者血糖 并将数据传递到胰岛素泵 集成有判断逻辑的泵会基于血糖值来判断是否释放胰岛素、释放多少胰岛素 **这些数据还会同步上传云端** 为后续专业医护人员的介入创造了条件

智能交通与车联网

物联网在智能交通的应用包括实时监控系统、自动收费系统、智能停车系统和实时车辆跟踪系统 支持通过自动检测并报告公路、桥梁的健康状况 并能帮助交通运输业缓解能耗、污染以及拥堵问题 美国交通部提出了“国家智能交通系统项目规划” 预计到2025年全面投入使用 该系统综合运用大量传感器网络 配合GPS系统、区域网络系统等资源 实现对交通车辆的优化调度 并为个体交通推荐实时的、最佳的行车路线

运用物联网技术可以透过感测装置捕捉车辆、驾驶、乘客、周围环境的相关信息 开创更优质的驾车体验 例如 科技巨头Google、特斯拉、宝马等国际重量级车厂 都已纷纷投入智能车、无人驾驶车的开发

智能家居

2018年3月 海尔发布了全球首套由互联互通的智慧家电构成的智慧家庭 让智能家居从梦想落地到现实 各种电器间的相互通信 让生活更舒适、简单 智能家电和用户间的交互 可以根据用户个性化需求 主动提供服务 比如洗碗机可以根据菜谱自动选择相应的洗涤程序

除了海尔智慧家居这种整套操作系统 智能电视、智能音箱等智能硬件也可以当做智能家居的控制中心和枢纽 例如国外的亚马逊Echo、谷歌Home、苹果HomePod等 国内的暴风大耳朵、阿里巴巴天猫精灵等都有此发展趋势 “人工智能+物联网”将掀起改变生活方式的狂潮

智慧物流

智慧物流是把条形码、射频识别技术、传感器、全球定位系统等物联网技术 广泛应用于物流业运输、仓库、配送、包装、装卸等环节 **智慧物流的崛起离不开电商爆发的催化 更离不开物联网技术的加持**

过去物流仓库爆仓和干线压力是头等问题 特别是在双11、双12购物节 在2016年双11前 各大物流企业做出应对措施中就包括不少的智慧物流技术 例如 京东在2016年首次引进智能机器人设备 机器人仓、机器人分拣中心两个自动化设备在双11期间启用 单台自动分拣设备最高处理量可达到2万件/小时 **京东目前在全国范围的自动分拣设备的日均处理量已达到百万件以上**

IPv6

网际协议第6版（Internet Protocol version 6 简称：IPv6）是网际协议（IP）的最新版本 被用于互联网的网络层协议 使用IPv6取代IPv4的目的是解决IPv4地址使用即将殆尽的问题 **在一些性能等其他方面也有所改进**

传感器

传感器（Sensor）被用来侦测环境中所发生事件或变化 并将此消息发送至其他电子设备（如中央处理器） 通常由敏感组件和转换组件组成

遥感技术

遥感（remote sensing）是指用间接手段来获取目标状态信息的方法 例如 从人造卫星或飞机对地面观测 通过电磁波（包括光波）的传播与接收 感知目标的某些特性并加以分析

按遥感平台可分为：机载遥感和星载遥感 其中机载遥感是飞机携带传感器（CCD相机或非数码相机等）对地面的观测 星载遥感是指传感器被放置在大气层外的卫星上；按传感器感知电磁波波长可分为：可见光—近红外（visible – near infrared）遥感、红外遥感及微波遥感等；根据接收到的电磁波信号的来源 遥感可分为主动式（信号由感应器发出）和被动式（信号由目标物体发出或反射太阳光波）

遥感的优点是能够在短时间内取得大范围的数据 将其以图像与非图像方式呈现 以及代替人类前往难以抵达或危险的地方观测 被应用于航海、农业、气象、资源、环境、行星科学等等各领域

无线传感器网络（WSN）

无线传感器网络(Wireless Sensor Networks 简称：WSN)是一种分布式传感网络 通过无线通信方式形成的一个多跳自组织网络 它的末梢是可以感知和检查外部世界的传感器 WSN中的传感器通过无线方式通信 因此网络设置灵活 设备位置可以实时更新 还可以跟互联网进行有线或无线方式的连接

WSN的发展得益于微机电系统(Micro-Electro-Mechanism System MEMS)、片上系统(System on Chip SoC)、无线通信和低功耗嵌入式技术的飞速发展

WSN广泛应用于军事、智能交通、环境监控、医疗卫生等多个领域

第五代通信技术有哪些优势

传输速率更快，5G设备的数据速率为10Gbps，是4G设备的百倍以上，那就意味着，下载一部3GB电影只需5秒左右；

响应延迟更底，5G设备的数据传输延迟在1ms以下，而4G设备的数据传输延迟为50ms。

更高的吞吐量，5G的数据吞吐量每平方公里为100万，大约是4G的几十到上百倍。

5G的发展历程

2013年2月 为了加快5G移动技术的发展 欧盟宣布 将拨款5000万欧元 计划到2020年推出成熟的标准

2013年5月13日 韩国三星电子有限公司宣布 已成功开发第5代移动通信（5G）的核心技术 这一技术预计将于2020年开始推向商业化 该技术可在28GHz超高频段以每秒1Gbps以上的速度传送数据 且最长传送距离可达2公里

在2013年11月6日华为宣布将在2018年前投资6亿美元对5G的技术进行研发与创新 并预言在2020年用户会享受到20Gbps的商用5G移动网络

2014年5月8日 日本电信营运商 NTT DoCoMo 正式宣布将与 Ericsson、Nokia、Samsung 等六家厂商共同合作 预计在2015年展开户外测试 并期望于 2020 年开始运作

2015年3月1日 英国《每日邮报》报道 英国已成功研制5G网络 并进行100米内的传送数据测试 **每秒数据传输高达125GB** 是4G网络的6.5万倍 理论上1秒钟可下载30部电影 并称于2018年投入公众测试 2020年正式投入商用

2015年3月3日 欧盟数字经济和社会委员古泽 奥廷格正式公布了欧盟的5G公司合作愿景 力求确保欧洲在下一代移动技术全球标准中的话语权

2015年9月7日 美国移动运营商Verizon无线公司宣布 将从2016年开始试用5G网络 2017年在美国部分城市全面商用 中国5G技术研发试验将在2016-2018年进行 分为5G关键技术试验、5G技术方案验证和5G系统验证三个阶段实施

2016年3月 工信部副部长陈肇雄表示：5G是新一代移动通信技术发展的主要方向 是未来新一代信息基础设施的重要组成部分 与4G相比 5G不仅将进一步提升用户的网络体验 同时还将满足未来万物互联的应用需求

从用户体验看 5G具有更高的速率、更宽的带宽 预计5G网速将比4G提高10倍左右 只需要几秒即可下载一部高清电影 能够满足消费者对虚拟现实、超高清视频等更高的网络体验需求

从行业应用看 5G具有更高的可靠性 更低的时延 能够满足智能制造、自动驾驶等行业应用的特定需求 拓宽融合产业的发展空间 支撑经济社会创新发展

从发展态势看 5G还处于技术标准的研究阶段 后来几年4G还将保持主导地位 实现持续高速发展 但5G有望2020年正式商用

2016年 诺基亚与加拿大运营商Bell Canada合作 完成加拿大首次5G网络技术的测试 测试中使用了73GHz范围内频谱 数据传输速率为加拿大现有4G网络的6倍

2017年2月9日 国际通信标准组织3GPP宣布了“5G”的官方 Logo

2017年11月15日 工信部发布《关于第五代移动通信系统使用3300-3600MHz和4800-5000MHz频段相关事宜的通知》 确定5G中频频谱 能够兼顾系统覆盖和大容量的基本需求

2017年11月下旬中国工信部发布通知 正式启动5G技术研发试验第三阶段工作 并力争于2018年年底前实现第三阶段试验基本目标

2017年12月21日 在国际电信标准组织3GPP RAN第78次全体会议上 5G NR首发版本正式冻结并发布

2017年12月 发改委发布《关于组织实施2018年新一代信息基础设施建设工程的通知》 要求2018年将在不少于5个城市开展5G规模组网试点 每个城市5G基站数量不少50个、全网5G终端不少于500个

2018年2月23日 在世界移动通信大会召开前夕 沃达丰和华为宣布 两公司在西班牙合作采用非独立的3GPP 5G新无线标准和Sub6 GHz频段完成了全球首个5G通话测试 6

2018年2月27日 华为在MWC2018大展上发布了首款3GPP标准5G商用芯片巴龙5G01和5G商用终端 支持全球主流5G频段 包括Sub6GHz(低频)、mmWave(高频) 理论上可实现最高2.3Gbps的数据下载速率

2018年6月13日 3GPP 5G NR标准 SA（Standalone 独立组网）方案在3GPP第80次TSG RAN全会正式完成并发布 这标志着首个真正完整意义的国际5G标准正式出炉

2018年6月14日 3GPP全会（TSG#80）批准了第五代移动通信技术标准（5G NR）独立组网功能冻结 加之2017年12月完成的非独立组网NR标准 5G已经完成第一阶段全功能标准化工作 进入了产业全面冲刺新阶段

2018年6月28日 中国联通公布了5G部署：将以SA为目标架构 前期聚焦eMBB 5G网络计划在2020年正式商用

2018年8月2日 奥迪与爱立信宣布 计划率先将5G技术用于汽车生产 在奥迪总部德国因戈尔施塔特 两家公司就一系列活动达成一致 共同探讨5G作为一种面向未来的通信技术 能够满足汽车生产高要求的潜力 奥迪和爱立信签署了谅解备忘录 在未来几个月内 两家公司的专家们将在位于德国盖梅尔斯海姆的“ 奥迪生产实验室 ”的技术中心进行现场测试

2018年11月21日 重庆首个5G连续覆盖试验区建设完成 5G远程驾驶、5G无人机、虚拟现实等多项5G应用同时亮相

2018年12月1日 韩国三大运营商SK、KT与LG U+同步在韩国部分地区推出5G服务 这也是新一代移动通信服务在全球首次实现商用 第一批应用5G服务的地区为首尔、首都圈和韩国六大广域市的市中心 以后将陆续扩大范围 按照计划 韩国智能手机用户2019年3月份左右可以使用5G服务 预计2020年下半年可以实现5G全覆盖

2018年12月7日 工信部同意联通集团自通知日至2020年6月30日使用3500MHz-3600MHz频率 **用于在全国开展第五代移动通信（5G）系统试验** **12月10日** 工信部正式对外公布 已向中国电信、中国移动、中国联通发放了5G系统中低频段试验频率使用许可 这意味着各基础电信运营企业开展5G系统试验所必须使用的频率资源得到保障 向产业界发出了明确信号 进一步推动我国5G产业链的成熟与发展

2018年12月18日 AT&T宣布 将于12月21日在全美12个城市率先开放5G网络服务

目前5G的商用情况

国内推动5G发展主要由IMT—20205G推进组牵头，下设在不同工作组推动中国5G标准化，5G的测试试验以及5G知识产权相关的工作。

国际上5G发展最新情况，2018年6月14日5G独立组网标准，就是Rel—15 SA标准已经按期完成，无线接口和核心网接口实现端到端全新的业务承载能力。

5G试验方面，68个国家和地区的154家运营商完成获得许可，同时5G频段39个国家和地区推出频谱规划，其中24个国家和地区明确频谱拍卖或分配时间表，主要是在3.5GHz以及28Ghz试验频段。

5G终端方面，随着SA 5G的标准正式确立，5G商用进入倒计时，产业配套预计在2019年逐步完备，2020将开启全球商用。

云计算

云计算（英语：cloud computing）**是一种基于互联网的计算方式 通过这种方式** 共享的软硬件资源和信息可以按需求提供给计算机各种终端和其他设备

云计算的特征

互联网上的云计算服务特征和自然界的云、水循环具有一定的相似性 根据美国国家标准和技术研究院的定义 云计算服务主要具备以下几条特征：

根据实际需要提供服务

数据访问不受时间、地域、网络设备等限制

可支持多人共同享用数据池

部署迅速 灵活度较高

数据操作可监控 服务可量化

一般认为还有如下特征：

可通过虚拟化技术 快速部署资源或获得服务

减少用户终端的处理负担

降低了用户对于IT专业知识的依赖

云计算有哪些优势？

超大规模。“云”具有相当的规模，Google云计算已经拥有100多万台服务器，亚马逊、IBM、微软和Yahoo等公司的“云”均拥有几十万台服务器。“云”能赋予用户前所未有的计算能力。

虚拟化。云计算支持用户在任意位置使用各种终端获取服务。所请求的资源来自“云”而不是固定的有形的实体。应用在“云”中某处运行，但实际上用户无需了解应用运行的具体位置，只需要一台笔记本或一个PDA就可以通过网络服务来获取各种能力超强的服务。

高可靠性。“云”使用了数据多副本容错、计算节点同构可互换等措施来保障服务的高可靠性，使

用云计算比使用本地计算机更加可靠。

通用性。云计算不针对特定的应用，在“云”的支撑下可以构造出千变万化的应用，同一片“云”可以同时支撑不同的应用运行。

高可伸缩性。“云”的规模可以动态伸缩，满足应用和用户规模增长的需要。

按需服务。“云”是一个庞大的资源池，用户按需购买，像自来水、电和煤气那样计费。

极其廉价。“云”的特殊容错措施使得可以采用极其廉价的节点来构成云；“云”的自动化管理使数据中心管理成本大幅降低；“云”的公用性和通用性使资源的利用率大幅提升；“云”设施可以建在电力资源丰富的地区，从而大幅降低能源成本。

云计算的供货商有哪些？

从全球范围来看 公有云厂商前五名分别是AWS、微软、谷歌、阿里云和IBM 阿里云也是唯一上榜的中国厂商 AWS在四个区域均排在第一 微软在三个区域排在第二 但在亚太地区被阿里云赶超 屈居第三 谷歌在亚太地区的名次也下滑了一位 腾讯云排亚太地区第五

在其他市场 IBM在North America和EMEA Region排第四 Salesforce排第五 而在Latin America（拉丁美洲）市场 Salesforce超越IBM成为第四

双机热备

双机热备因两机高可用在国内使用较多 特指基于高可用系统中的两台服务器的热备（或高可用）故得名双机热备 双机高可用按工作中的切换方式分为：主-备方式（Active-Standby方式）和双主机方式（Active-Active方式）主-备方式即指的是一台服务器处于某种业务的激活状态（即Active状态）另一台服务器处于该业务的备用状态（即Standby状态）而双主机方式即指两种不同业务分别在两台服务器上互为主备状态（即Active-Standby和Standby-Active状态）

云服务的基本层次有哪些？

云计算主要思想是面向服务 从SOA发展而来

云计算包括三个层次的服务：基础架构即服务（IaaS）平台即服务（PaaS）和软件即服务（SaaS）

IaaS的基本功能有哪些？

IaaS通过互联网提供数据中心、基础架构硬件和软件资源 还可以提供服务器、操作系统、磁盘存储、数据库和/或信息资源

PaaS的基本功能有哪些？

PaaS提供了基础架构 软件开发者可以在这个基础架构之上建设新的应用 或者扩展已有的应用 而不必购买开发、质量控制或生产服务器

SaaS的基本功能有哪些？

SaaS是最为成熟、最出名 也是得到最广泛应用的一种云计算 它是一种软件分布模式 在这种模式下 应用软件安装在厂商或者服务供应商那里 用户可以通过某个网络来使用这些软件 通常使用的网络是互联网

虚拟化

虚拟化（技术）或虚拟技术（Virtualization）是将计算机的各种实体资源（CPU、内存、磁盘空间、网络适配器等）虚拟化的一种资源管理技术 通过抽象、转换后 构建成可供分割、组合为一个或多个计算机配置环境 由此 打破实体结构间的不可切割的障碍 使用户可以比原本的配置更好的方式来应用这些计算机硬件资源 这些资源的新虚拟部分是不受现有资源的架设方式 地域或物理配置所限制 一般所指的虚拟化资源包括计算能力和数据存储

数据中心

数据中心也被称为服务器场 意味着安置计算机系统及相关部件的设施 例如 电信和储存系统 数据中心一般包括冗余和备用电源、冗余数据通信连接、环境控制（例如空调、灭火器）和各种安全设备

虚拟化与云计算之间的关系

云计算是一个理论概念，而不适用于特指某种具体技术。虚拟化是一种具体技术，指把硬件资源虚拟化，具有隔离性、可扩展性、安全性、资源可充分利用等特点的技术。CPU虚拟化的技术

：Intel的VT-x，AMD的AMD-V。虚拟化的软件：VMWare，Hyper-V，Xen，KVM，OpenVZ等

目前云计算，大多是依赖虚拟化，通过把多台服务器实体虚拟化后，构成一个资源池，实现共同计

算，共享资源。

大数据存储面临的新问题和新挑战有哪些？

容量问题

这里所说的“大容量”通常可达到PB级的数据规模，因此，海量数据存储系统也一定要有相应等级的扩展能力。与此同时，存储系统的扩展一定要简便，可以通过增加模块或磁盘柜来增加容量，甚至不需要停机。

“大数据”应用除了数据规模巨大之外，还意味着拥有庞大的文件数量。因此如何管理文件系统层累积的元数据是一个难题，处理不当的话会影响到系统的扩展能力和性能，而传统的NAS系统就存在这一瓶颈。所幸的是，基于对象的存储架构就不存在这个问题，它可以在一个系统中管理十亿级别的文件数量，而且还不会像传统存储一样遭遇元数据管理的困扰。基于对象的存储系统还具有广域扩展能力，可以在多个不同的地点部署并组成一个跨区域的大型存储基础架构。

延迟问题

“大数据”应用还存在实时性的问题。有很多“大数据”应用环境需要较高的IOPS性能，比如HPC高性能计算。此外，服务器虚拟化的普及也导致了对高IOPS的需求，正如它改变了传统IT环境一样。为了迎接这些挑战，各种模式的固态存储设备应运而生，小到简单的在服务器内部做高速缓存，大到全固态介质的可扩展存储系统等都在蓬勃发展。

并发访问

一旦企业认识到大数据分析应用的潜在价值，他们就会将更多的数据集纳入系统进行比较，同时让更多的人分享并使用这些数据。为了创造更多的商业价值，企业往往会综合分析那些来自不同平台下的多种数据对象。包括全局文件系统在内的存储基础设施就能够帮助用户解决数据访问的问题，全局文件系统允许多个主机上的多个用户并发访问文件数据，而这些数据则可能存储在多个地点的多种不同类型的存储设备上。

安全问题

某些特殊行业的应用，比如金融数据、医疗信息以及政府情报等都有自己的安全标准和保密性需求。虽然对于IT管理者来说这些并没有什么不同，而且都是必须遵从的，但是，大数据分析往往需要多类数据相互参考，而在过去并不会会有这种数据混合访问的情况，因此大数据应用也催生出一一些新的、需要考虑的安全性问题。

成本问题

成本问题“大”，也可能意味着代价不菲。而对于那些正在使用大数据环境的企业来说，成本控制是关键的问题。想控制成本，就意味着我们要让每一台设备都实现更高的“效率”，同时还要减少那些昂贵的部件。

对成本控制影响最大的因素是那些商业化的硬件设备。因此，很多初次进入这一领域的用户以及那些应用规模最大的用户都会定制他们自己的“硬件平台”而不是用现成的商业产品，这一举措可以用来平衡他们在业务扩展过程中的成本控制战略。为了适应这一需求，现在越来越多的存储产品都提供纯软件的形式，可以直接安装在用户已有的、通用的或者现成的硬件设备上。此外，很多存储软件公司还在销售以软件产品为核心的软硬一体化装置，或者与硬件厂商结盟，推出合作型产品。

数据的积累

许多大数据应用都会涉及到法规遵从问题，这些法规通常要求数据要保存几年或者几十年。比如医疗信息通常是为了保证患者的生命安全，而财务信息通常要保存7年。而有些使用大数据存储的用户却希望数据能够保存更长的时间，因为任何数据都是历史记录的一部分，而且数据的分析大都是基于时间段进行的。要实现长期的数据保存，就要求存储厂商开发出能够持续进行数据一致性检测的功能以及其他保证长期高可用的特性。同时还要实现数据直接在原位更新的功能需求。

数据的灵活性

大数据存储系统的基础设施规模通常都很大，因此必须经过仔细设计，才能保证存储系统的灵活性，使其能够随着应用分析软件一起扩容及扩展。在大数据存储环境中，已经没有必要再做数据迁移了，因为数据会同时保存在多个部署站点。一个大型的数据存储基础设施一旦开始投入使用，就很难再调整了，因此它必须能够适应各种不同的应用类型和数据场景。

云计算的发展历程

1983年 太阳电脑（Sun Microsystems）提出“网络是电脑”（“The Network is the Computer”）

2006年3月 亚马逊（Amazon）推出弹性计算云（Elastic Compute Cloud；EC2）服务

2006年8月9日 Google首席执行官埃里克 施密特（Eric Schmidt）在搜索引擎大会（SES San Jose 2006）首次提出“云计算”（Cloud Computing）的概念 Google“云端计算”源于Google工程师克里斯托弗 比希利亚所做的“Google 101”项目

2007年10月 Google与IBM开始在美国大学校园 包括卡内基梅隆大学、麻省理工学院、斯坦福大学、加州大学柏克莱分校及马里兰大学等 推广云计算的计划 这项计划希望能降低分布式计算技术在学术研究方面的成本 并为这些大学提供相关的软硬件设备及技术支持（包括数百台个人电脑及 BladeCenter与System x服务器 这些计算平台将提供1600个处理器 支持包括Linux、Xen、Hadoop等开放源代码平台）而学生则可以通过网络开发各项以大规模计算为基础的研究计划

2008年1月30日 Google宣布在台湾启动“云计算学术计划” 将与台湾台大、交大等学校合作 将这种先进的大规模、快速将云计算技术推广到校园

2008年2月1日 IBM（NYSE: IBM）宣布将在中国无锡太湖新城科教产业园为中国的软件公司建立全球第一个云计算中心（Cloud Computing Center）

2008年7月29日 雅虎、惠普和英特尔宣布一项涵盖美国、德国和新加坡的联合研究计划 推出云计算研究测试床 推进云计算 该计划要与合作伙伴创建6个数据中心作为研究试验平台 每个数据中心配置1400个至4000个处理器 这些合作伙伴包括新加坡资讯通信发展管理局、德国卡尔斯鲁厄大学 Steinbuch计算中心、美国伊利诺伊大学香槟分校、英特尔研究院、惠普实验室和雅虎

2008年8月3日 美国专利商标局网站信息显示 戴尔正在申请“云计算”（Cloud Computing）商标 此举旨在加强对这一未来可能重塑技术架构的术语的控制权

2010年3月5日 Novell与云安全联盟（CSA）共同宣布一项供应商中立计划 名为“可信任云计算计划（Trusted Cloud Initiative）”

2010年7月 美国国家航空航天局和包括Rackspace、AMD、Intel、戴尔等支持厂商共同宣布“OpenStack”开放源代码计划 微软在2010年10月表示支持OpenStack与Windows Server 2008 R2的集成；而Ubuntu已把OpenStack加至11.04版本中

2011年2月 思科系统正式加入OpenStack 重点研制OpenStack的网络服务

政务云

政务云（Government Cloud）是指通过云计算技术 统筹机房、计算、应用支撑、信息资源等 发挥云计算的虚拟化、高可靠性、高通用性、高可扩展性 使其数据处理快速、按需、弹性服务 为政府行业提供基础设施、支撑软件、应用系统、信息资源、运行保障和信息安全等综合服务平台

建设政务云有什么意义？

避免重复建设、减少财政支出

政务云平台应充分利用目前现有的基础资源，以实现各种资源整合，由平台统一为政府部门提供资源、运维、安全和管理服务，能够提升基础设施利用率，减少运维人员和运维费用，避免重复建设、投资浪费现象。

促进信息共享、实现业务协同

在当今社会，信息赋予了极大的力量，政府作为最大的信息采集者、拥有者。通过建设电子政务等信息化平台，实现政府信息流通和共享，有利于国家整体发展。在政府各个部门之间、政府部门与社会服务部门之间建立“信息桥梁”，极大地提高各级政府机关的整体工作效率。

构筑信息堡垒、保障数据安全

传统模式下，基础的信息安全保障措施不全，缺少灾备中心和应急机制，有的部门甚至连机房等基础环境都不符合安全标准。政务云平台通过顶层设计制定了从技术、架构、产品、运维、管理、制度等一系列的保障措施，保证了部署在平台的应用及数据的安全。另外，通过建立统一的灾备体系，确保在发生灾难的情况下，快速、完整的恢复应用。当前，国家对政务云的安全越来越重视，中央网信办明确要求“要对为党政部门提供云计算服务的服务商，参照有关网络安全国家标准，组织第三方机构进行网络安全审查”，鼓励重点行业优先采购和使用通过安全审查的服务商提供的云计

算服务。通过技术手段和国家强制措施，政务云模式下的信息安全更有保障。

优化资源配置、提升服务能力

通过政务云平台，传统的部门组织朝着网络组织方向发展，打破同级、层级、部门的限制，促使政府组织和职能进行整合，使政府的程序和办事流程更加简明、畅通，使人力和信息资源得到最充分的利用和配置。同时，采用政务云平台集约化模式建设电子政务项目，可以使政府部门从传统的硬件采购、系统集成、运行维护等工作中解脱出来，转而将更多的精力放到业务的梳理和为民服务上来，能够极大提升为民服务的能力和水平，促进政府管理创新和建设服务型政府。

建设政务云的前景

现阶段政务云建设，主要是借助IaaS，实现基础设施资源整合与共享，业务系统基于IaaS进行开发和部署，并没有改变传统应用系统的架构，这个阶段称为政务云1.0阶段。

国发〔2015〕5号文《国务院关于促进云计算创新发展培育信息产业新业态的意见》指出，充分发挥云计算对数据资源的集聚作用，实现数据资源的融合共享，推动大数据挖掘、分析、应用和服务。政务云建设进入一个新的阶段，称之为政务云2.0阶段。政务云2.0阶段，在IaaS基础设施资源整合与共享的基础上，将会实现IaaS/PaaS深度融合，借助云计算技术推动政府大数据的开发与利用，实现跨系统的信息共享与业务协同，推进应用创新。政务云2.0特征是以数据为核心、以IaaS/PaaS深度融合为支撑，以新架构的云应用创新为代表。在2.0阶段，应用对业务连续性和数据安全可靠性保障提出了更高要求。

关键信息基础设施

关键信息基础设施是面向公众提供网络信息服务或支撑能源、通信、金融、交通、公用事业等重要行业运行的信息系统或工业控制系统 且这些系统一旦发生网络安全事故 会影响重要行业正常运行 对国家政治、经济、科技、社会、文化、国防、环境以及人民生命财产造成严重损失

工业互联网的实质

首先是全面互联 在全面互联的基础上 通过数据流动和分析 形成智能化变革 形成新的模式和新的业态 互联是基础 工业互联网是工业系统的各种元素互联起来 无论是机器、人还是系统

互联解决了通信的基本 更重要的是数据端到端的流动 跨系统的流动 在数据流动技术上充分分析、建模 伯特认为智能化生产、网络化协同、个性化定制、服务化延伸是在互联的基础上 通过数据流动和分析 形成新的模式和新的业态

这是工业互联网的基理 比现在的互联网更强调数据 更强调充分的连接 更强调数据的流动和集成以及分析和建模 这和互联网是有所不同的 工业互联网的本质是要有数据的流动和分析

工业互联网生态系统的持续拓展基于Predix以及Predix.io两大基础

工业互联网具有哪些效应？

假设发展情况和互联网大潮时期类似，截至2030年工业互联网革命将为全球GDP带来15万亿美元，相当于在计算全球经济总量时把美国的经济多加了一次。

最令人惊讶的地方在于这一切来源于那些看起来很小的生产力提升。即使是1%的生产效率提升，背后潜藏的上升空间也是没有人可以抵挡的。

工业互联网已经不断应用于各个领域，并且开始潜移默化地改变我们的生活。

工业互联网将智能设备、人和数据连接起来，并以智能的方式利用这些交换的数据。在通用电气的倡导下，AT&T、思科（Cisco）、通用电气（GE）、IBM、英特尔（intel）已在美国波士顿宣布成立工业互联网联盟（IIC），以期打破技术壁垒，促进物理世界和数字世界的融合。

区块链

通常形容区块链为一个大账本 从技术层面上说 是指所有区块链在一起的一个链表结构 类似于C/C++中的单项链表数据结构 只是每个区块保存前一个区块的hash码值 所以从某个区块逆向上溯 最终都会找到创世区块

区块链的特征

去中心化

因为使用分布式核算和存储 没有中心化的硬件或管理机构 任意节点的权利和义务都是同等的 系统中的数据块依靠系统中具有维护功能的节点来进行维护

开放性

系统是开放的 只有交易各方的私有信息被加密 其他的区块链数据对所有人进行公开 任何人均可通过公开的接口查询区块链数据和开发相关应用 因此整个系统信息高度透明

自治性

区块链采用基于协商一致的规范和协议（例如 公开透明的算法）使得整个系统中的所有节点能够在去信任的环境自由安全的交换数据 使得对“人”的信任改成了对机器的信任 任何人为的干预不起作用

信息不可篡改

一旦信息经过验证并添加至区块链 就会永久的存储起来 除非能够同时控制住系统中超过51%的节点 否则单个节点上对数据库的修改是无效的 **因此区块链的数据稳定性和可靠性极高**

匿名性

由于节点之间的交换遵循固定的算法 其数据交互是无需信任的（区块链中的程序规则会自行判断活动是否有效）因此交易对手无须通过公开身份的方式让对方自己产生信任 对信用的累积非常有帮助

区块链的应用价值

跨国支付 目前金融领域应用支付价值最多 因为跨国支付中货币兑换周期较长、时间成本较高、手续繁多等因素 如果使用区块链内的代币来做跨国支付交易 效率将达到最大化

清结算系统 银行、证券等机构每天有大量的清结算账目工作 在区块链中支付即结算的机制 如果清结算转移在区块链中可直接替代当下的清结算系统

供应链系统 区块链中协作效率最大化 可以大大提高比如装修这种长链条行业的供应链管理 或者直接替代短链行业的供应链系统 区块链可以完美做到对于供应链条的问题追责和生产协作

知识产权 区块链中的数据永远保存、全程可追溯、不可篡改等特性 非常适用知识产权的保护 可实时记录更新备案知识产权资产的产权链以及所有权情况 并且转让也很方便

商品防伪 区块链的可溯源特性 应用在商品的防伪和打假工作将是革命式的突破 对于像LV、茅台这种每年花费巨额成本打假的知名品牌是一个大大降低成本的方式

身份管理 区块链的不可篡改以及私钥的安全机制 让身份管理更加容易 可直接应用于选举、政务、房地产交易等繁琐手续的领域 不再需要一大堆的证明文件

物联网、人工智能、云计算等 AI的技术核心算法是深度学习 而机器学习对象都是基于数据 所以对于数据安全一直以来都是技术领域的痛点 **区块链的可溯源、可追溯保证数据的安全** 对于机器智能来说也可以排除机器攻击人类的隐患 对于云端数据来说 也不怕信息泄露 这一点同样也适用于医疗、基因数据管理等高科技领域

游戏 游戏虚拟币与区块链代币的关联整合 基于区块链协作模式的游戏玩法 未来的游戏可探索更多可能性

区块结构包含哪些信息？

一个完整的区块结构主要由以下几部分构成：

数据项字节字段说明 Magic NO4魔数常数 0xD9B4BEF9 Blocksize4 区块大小

用字节表示的该字段之后的区块大小 Blockheader80 区块头组成区块头的几个字段

Transaction counter1-9 交易计数器 该区块包含的交易数量，包含coinbase交易 Transactions

不定交易记录在区块里的交易信息，使用原生的交易信息格式，并且交易在数据流中的位置必须与Merkle树的叶子节点顺序一致

去中心化

去中心化是一种现象或结构 必须在拥有众多节点的系统或拥有众多个体的群中才能出现或存在 节点与节点之间的影响 会通过网络形成非线性因果关系

分布式账本

分布式账本（Distributed ledger）技术是一种应用在资本市场的区块链技术 可以移除市场中效率低下、成本较高的市场基础设施

分布式账本可以支持网络成员之间共享、复制和同步数据库 用于记录网络参与者之间的交易 例如

资产或数据的交换在一定程度上降低了因调解不同账本所产生的时间和开支成本

区块链都有哪几类

“公有链”(Public blockchain)

“私有链”(Private blockchain)

“联盟链”(Consortium blockchain)

三类区块链主要区别是：

公有链：对所有人开放，任何人都可以参与；

联盟链：对特定的组织团体开放；

私有链：对单独的个人或实体开放。

图灵完备

图灵完备是指机器执行任何其他可编程计算机能够执行计算的能力；例如Ethereum虚拟机(EVM)

挖矿

挖矿是获取比特币的勘探方式的昵称。利用电脑硬件计算出币的位置并获取的过程称之为挖矿。

矿工

尝试创建区块并将其添加到区块链上的计算设备或者软件 在一个区块链网络中 当一个新的有效区块被创建时 系统一般会给予区块创建者（矿工）一定数量的代币 作为奖励

矿池

是一个全自动的挖矿平台 使得矿工们能够贡献各自的算力一起挖矿以创建区块 获得区块奖励 并根据算力贡献比例分配利润（即矿机接入矿池—提供算力—获得收益）

主链

主链一词源于主网（mainnet 相对于测试网testnet）即正式上线的、独立的区块链网络

侧链

楔入式侧链技术（pegged sidechains）它将实现比特币和其他数字资产在多个区块链间的转移 这就意味着用户们在使用他们已有资产的情况下 就可以访问新的加密货币系统

比特币

比特币（BitCoin）最早在2009年被中本聪提出 最初设想是发布开源软件 并在其上构建P2P网络 比特币属于P2P形式的数字货币 点对点的传输目的是构建去中心化的支付系统

区块链的发展历程

2008年爆发全球金融危机 当时有人用“中本聪”的化名发表了一篇文章 描述了比特币的模式 与法定货币作比较 比特币是由网络节点的计算生成 没有一个集中的发行方 任何人可以在任意一台接入互联网的电脑上买卖 也有可能参与制造比特币 并且支持在全世界范围内进行流通 比特币交易不受人、地域的限制 在交易过程中外人无法辨认证户身份信息 2009年 比特币诞生 它是由计算机生成的一串串复杂代码组成 随着比特币总量的增加 新币制造的速度减慢 截止2014年总共达到2100万个的总量上限 被挖出的比特币总量超过1200万个

2009年比特币诞生之初 每笔赏金是50个比特币 诞生10分钟后 第一批50个比特币生成了 而此时的货币总量就是50 随后比特币就以约每10分钟50个的速度增长 当总量达到1050万时(2100万的50%) 赏金减半为25个 当总量达到1575万(新产出525万 即1050的50%)时 赏金再减半为12.5个

2014年9月9日 美国电商巨头eBay宣布 该公司旗下支付处理子公司Braintree将开始接受比特币支付 该公司已与比特币交易平台Coinbase达成合作 开始接受这种相对较新的支付手段

2017年1月22日晚间 火币网、比特币中国与OKCoin币行相继在各自官网发布公告称 为进一步抑制投机 防止价格剧烈波动 各平台将于2017年1月24日中午12：00起开始收取交易服务费 服务费按成交金额的0.2%固定费率收取 且主动成交和被动成交费率一致 5月5日 OKCoin币行网的最新数据显示 比特币的价格刚刚再度刷新历史 最高触及9222点高位

智慧城市

什么是智慧城市？

智慧城市（英语：Smart City）是指利用各种信息技术或创新意念 集成城市的组成系统和服务 以提升

资源运用的效率 优化城市管理和服 务 以及改善市民生活质量 智慧城市把新一代信息技术充分运用在城市的各行各业之中的基于知识社会下一代创新（创新2.0）的城市信息化高级形态 实现信息化、工业化与城镇化深度融合 有助于缓解“大城市病” 提高城镇化质量 实现精细化和动态管理 并提升城市管理成效和改善市民生活质量 关于智慧城市的具体定义比较广泛 当前在国际上被广泛认同的定义是 智慧城市是新一代信息技术支撑、知识社会下一代创新（创新2.0）环境下的城市形态 强调智慧城市不仅仅是物联网、云计算等新一代信息技术的应用 更重要的是通过面向知识社会的创新2.0的方法论应用 构建用户创新、开放创新、大众创新、协同创新为特征的城市可持续创新生态 智慧城市通过在人力和社会资本 以及在交通和信息通讯基础设置上的投资来推动可持续经济增长和高生活质量 并且通过参与式的管理对上面的资源及自然资源进行科学的管理 一些智慧城市建设的先行城市也越来越突出以人为本的可持续创新 比如欧盟启动了面向知识社会创新2.0的Living Lab计划 致力于围绕市民需求将城市建设为各方共同参与的开放创新空间 比如维也纳大学对城市体系评价的六个指标 即智慧的经济、智慧的运输业、智慧的环境、智慧的居民、智慧的生活和智慧的管理等六个方面 当前 智慧城市的建设是信息技术、城市规划等领域的热点问题

智慧城市的产生背景

智慧城市的概念最早源于IBM提出的“智慧地球”这一理念 此前类似的概念还有数字城市等 2008年11月 恰逢2007年 - 2012年环球金融危机伊始 IBM在美国纽约发布的《智慧地球：下一代领导人议程》主题报告所提出的“智慧地球”即把新一代信息技术充分运用在各行各业之中

具体地说“智慧”的理念就是透过新一代信息技术的应用使人类能以更加精细和动态的方式管理生产和生活的状态 通过把传感器嵌入和装备到全球每个角落的供电系统、供水系统、交通系统、建筑物和油气管道等生产生活系统的各种物体中 使其形成的物联网与互联网相联 实现人类社会与物理系统的集成 而后透过超级计算机和云计算将物联网集成起来 即可实现 此后这一理念被世界各国所接纳 并作为应对金融海啸的经济增长点 同时 发展智慧城市被认为有助于促进城市经济、社会与环境、资源协调可持续发展 缓解“大城市病” 提高城镇化质量

智慧城市的现状

2008年 奥巴马就任美国总统后 便对IBM的“智慧地球”概念做出积极回应 将纳入国家战略和应对金融危机的经济新的增长点

随后出于商业目的 IBM提出“智慧的城市在中国突破”的战略 并相继与中国大陆的多个省市签署了“智慧城市”共建协议 使得“智慧地球”、“智慧城市”等新概念引起各界广泛关注 为应对智慧城市建设的趋势 中华人民共和国住房和城乡建设部发布了《国家智慧城市试点暂行管理办法》 工业和信息化部也在酝酿相关标准

截止到2012年 施耐德电气已在全球包括中国、印度、欧洲、美国、南美等国家和地区的200多个城市完进行了智慧城市的建设

2012年12月 中国工程院组织起草并发布的《中国工程科技中长期发展战略研究报告》将智能城市列为中国面向2030年的30个重大工程科技专项之一

智慧城市的构成

智慧城市有助推动城市的可持续发展 令发展与环保之间获取良好平衡 从而打造一个“智慧环境” 在城市规划上 透过网络和遥距监控技术 政府可充分掌握及分析城市的天气状况、资源运用的程度和道路交通状况等数据 因而调节及善用社区的资源 实现节能减排 减低“环境足迹” 提升环境的可持续性

公共交通管理和监测及电子道路收费系统 均能应用于交通繁忙的地区 有助改善和缓解道路挤塞的问题 实践“智慧流动” 公共交通管理和监测能向车主提供实时数据 避免车主将车辆驶入挤塞的路段 提升城市运输效率 电子道路收费系统则是以用者自付原则减低非必要的交通需求 从而改善地区性交通挤塞及空气质量

新型智慧城市“新”在哪里？

“新型智慧城市”相较“智慧城市”而言，主要体现三个“新”，一是新的战略重心——构建一套适应城市特色、行之有效的管理制度体系；二是新的思维理念——从通过上设备、做系统，解决城

市单一或局部的表象问题，到通过合理规划数据流，串联城市运行的方方面面，进而从根本上解决城市问题；三是新的攻关方向——从城市视角出发，以数据驱动为核心，系统性解决城市复杂性问题，提升市民获得感。

智慧城市和数字城市的区别

对比数字城市和智慧城市，可以发现以下六方面的差异。

其一，当数字城市通过城市地理空间信息与城市各方面信息的数字化在虚拟空间再现传统城市，智慧城市则注重在此基础上进一步利用传感技术、智能技术实现对城市运行状态的自动、实时、全面透彻的感知。

其二，当数字城市通过城市各行业的信息化提高了各行业管理效率和服务质量，智慧城市则更强调从行业分割、相对封闭的信息化架构迈向作为复杂巨大系统的开放、整合、协同的城市信息化架构，发挥城市信息化的整体效能。

其三，当数字城市基于互联网形成初步的业务协同，智慧城市则更注重通过泛在网络、移动技术实现无所不在的互联和随时随地随身的智能融合服务。

其四，当数字城市关注数据资源的生产、积累和应用，智慧城市更关注用户视角的服务设计和提供。

其五，当数字城市更多注重利用信息技术实现城市各领域的信息化以提升社会生产效率，智慧城市则更强调人的主体地位，更强调开放创新空间的塑造及其间的市民参与、用户体验，及以人为本实现可持续创新。

其六，当数字城市致力于通过信息化手段实现城市运行与发展各方面功能，提高城市运行效率，服务城市管理和发展，智慧城市则更强调通过政府、市场、社会各方力量的参与和协同实现城市公共价值塑造和独特价值创造。

智慧城市的形成因素

有两种驱动力推动智慧城市的逐步形成 一是以物联网、云计算、移动互联网为代表的新一代信息技术 二是知识社会环境下逐步孕育的开放的城市创新生态 前者是技术创新层面的技术因素 后者是社会创新层面的社会经济因素 由此可以看出创新在智慧城市发展中的驱动作用 清华大学公共管理学院书记、副院长孟庆国教授提出 新一代信息技术与创新2.0是智慧城市的两大基因 缺一不可

智慧城市不仅需要物联网、云计算等新一代信息技术的支撑 更要培育面向知识社会的下一代创新（创新2.0） 信息通讯技术的融合和发展消融了信息和知识分享的壁垒 消融了创新的边界 推动了创新2.0形态的形成 并进一步推动各类社会组织及活动边界的“消融”

智慧城市建设中的难点

其一，数据的整合和协同。

数据资源的整合协调，这是智慧城市的重心所在，则需将各个部门行业，或是不同系统之间的海量数据进行融合，由此形成新的有价值的数据源。智慧城市建设的关键在于数据资源的建设，数据是智慧产生的根源，进一步作出智慧决策。

其二，信息安全是最大难题。

智慧城市建设的前提需要有海量信息的搜集存储，因此信息安全也处在风险当中。由此可见，在智慧城市的建设初期，其信息安全是重点，更是难点。

其三，信息流将成城市运转的“血液”。

在整个智慧城市的建设当中，其中海量数据是基础，硬件是支撑，而数据开发融合则是核心，当然，智慧城市建设最终方向，则是激发城市信息化活力。

其四，在变化中摒弃不正确的政绩观是难点。

智慧城市的建设，既不是表面功夫，也不是用来作秀的舞台，因此政府部门不仅要提高自身的思想认识，在干部选拔任用和考核方面都需进一步完善。干部考核选拔机制也成为新形势下的新课题之一。

其五，智慧城市建设必须了解城市需求。

除了要让百姓满意之外，智慧城市的建设更应该从城市的实际出发，充分了解居民主体的物质文化需求。不仅要依靠已有的建设经验，更要注意吸取其他国家的智慧城市的建设经验。

智慧城市的建设意义

建设智慧城市是实现城市可持续发展的需要

建设智慧城市是信息技术发展的需要

提高我国综合竞争力的战略选择

工业互联网

什么是关键信息基础设施？

关键信息基础设施是面向公众提供网络信息服务或支撑金融、能源、交通、通信等重要行业运行的信息系统或工业控制系统。关键信息基础设施保护工作直接关系到国家安全、国计民生和公共利益。这些系统一旦发生网络安全事故，会影响重要行业的正常运行，对国家经济、政治、文化、科技、国防、社会、环境以及人民生命财产安全造成严重损失。

信息基础设施由什么组成？

信息基础设施的范围包含了诸如通信管网（包括同轴电缆、以太网线、光纤PSTN及其管道资源）、中继设备、无线基站、各级机房以及相关配套的电源、建筑等设施。信息基础设施是国家基础设施的重要内容。国家基础设施（National Information Infrastructure，缩写NII）是在信息基础设施基础上的一个更高水准的目标，可以提供一系列复杂但容易使用的服务。它包括五点内容：

一系列不断扩展的仪器设备，如键盘、摄像机、手机、电视、扫描仪、传真机、计算机、电线、打印机等。

信息本身，可以通过视频、音频等形式体现。

各类应用程序和软件，用户通过应用程序及软件去访问、组织、处理由基础设施提供的信息。

各类网络标准和传输编码，通过它们实现网络间的互连和操作，确保个人信息和网络的安全与可靠。

。

人，人的主要任务是挖掘信息、开发应用程序和服务、组建设备、培训其他人员等。

关键信息基础设施有哪几类？

关键信息基础设施包括以下几类：

网站类：如党政机关网站、企事业单位网站、新闻网站等；

平台类：如网上购物、网上支付、搜索引擎、电子邮件、论坛、地图、等网络服务平台；

生产业务类：如办公系统、工业控制系统、大型数据中心、云计算平台、电视转播系统等。

关键信息基础设施面临的风险分析

目前，互联网已成为我们生活中不可或缺的一部分，已经融入到社会中的方方面面。随之而来的问题是，网络安全威胁和风险也与日俱增，网络空间成为国家间政治、军事、经济、外交斗争的新战场。关键信息基础设施面临的风险分析主要有以下几种：

高危漏洞大量出现，危及市政、能源、制造等领域的关键信息基础设施，权限管理类型的漏洞较多，高危漏洞达到62%。Struts2（基于MVC设计模式的Web应用框架），弱口令（容易被猜解的密码），目录遍历（由于Web服务器或者Web应用程序对用户输入的文件名称的安全性验证不足而导致的一种安全漏洞）等漏洞危害严重，对网站系统造成数据泄露等一系列危害。

新型恶意软件病毒威胁严重，定向攻击、勒索攻击成为攻击关键信息基础设施的新手段。2010年，震网病毒首次被检测出来，它是有史以来最高端的“蠕虫”病毒，感染了全球超过45000个网络，伊朗遭到的攻击最为严重，60%的个人电脑感染了这种病毒。

在万物互联形势下，攻击关键信息基础设施难度降低。在开源社区中，很多关于设备的弱口令信息以及工业控制系统的扫描、探测、渗透方法被公布，这使得对工业系统的入侵难度降低，也进一步加剧了工业控制系统的网络安全风险。

我国关键信息基础设施成为多个APT组织重点攻击目标，面临严重的境外网络威胁。

使用的操作系统、服务器、数据库等产品大多为外国开发，我国对于核心技术的掌握依然劣于外国，在短时间内也没有特别有效的方法进行改变，重要领域的关键核心技术仍然受制于人。

工业互联网应用的主要方向有哪些？

工业互联网应用的主要方向主要有以下三个：

网络化协同制造（异地/跨企业）

利用互联网、大数据和各种集成技术将串行工作变成并行工作，打破时间、空间的约束，将供应链内、供应链间的企业产品设计、制造、运行、维护、管理等各个环节紧密连接，实现产品全生命周期内资源的最充分利用。解决异地、跨企业的设计、生产、维护和经营管理等产品全生命周期并行协同能力问题。

智能制造（企业内部）

将云计算、物联网、大数据等新一代信息技术与产品全生命周期活动的各个阶段相融合，通过各种关键技术实现自主感知制造信息、智能决策、智能执行，从而实现工厂内部生产制造过程的智能化。

云制造（产业链/智能/协同）

将各类制造资源和制造能力虚拟化、服务化，使用户通过终端和网络就能随时按需获取制造资源和服务能力，进而完成制造产品全生命周期的各类活动。融合网络化协同制造和智能制造，实现覆盖制造全产业链和全生命周期的社会化协同制造。

什么是CPS？(物理信息系统)

物理信息系统(CPS Cyber-Physical Systems)是一个综合计算、网络和物理环境的多维复杂系统，通过先进的传感、通信、计算与控制技术，基于数据与模型，驱动信息世界与物理世界的双向交互与反馈闭环；通过3C(Computing、Communication、Control)技术的有机融合与深度协作，实现大型工程系统的实时感知、动态控制和信息服务。CPS主要面向机器设备，包含设备程序自动化编程系统、生产任务管理系统、生产工具管理系统、生产监控管理系统四部分。

工业互联网与CPS的关系

CPS是工业互联网的重要使能，其核心技术支撑了工业互联网实现物理实体世界与虚拟世界的互联互通。CPS与工业互联网的本质都是基于传感器、执行器、云计算、处理器、信息网络、大数据将现实的物理世界映射为虚拟的数字模型，通过基于高级算法的大数据分析，将最优的决策数据反馈给物理世界，优化物理世界运转效率，提升安全水平。从应用领域来看，CPS涵盖工业互联网。工业互联网强调的是对工业生产系统的感知、互联和计算，实现对生产过程和产品服务的优化。CPS在包含工业生产系统之外，还包含对交通、医疗、农业、能源等其它生产生活领域的应用。从技术侧重来看，CPS与工业互联网略有差异。虽然CPS与工业互联网在本质内容和组织要素上是一致的，但从NIST的《愿景申明》中可以看到，CPS特别强调对嵌入式计算、分布式控制系统的应用，工业互联网强调对互联网、云计算平台和大数据技术的应用。因此，在技术侧重方面，CPS与工业互联网略有差异。

工业互联网的应用解决方案有哪些？

工业互联网的应用解决方案主要有以下几种：

基于云平台的智能云工厂解决方案

基于云平台的智能云工厂主要由航天云网平台、企业云、工业互联网、智能产线和数据中心等五部分组成。智能云工厂可以满足用户的个性化定制需求；支持柔性化生产、完成生产调控；设备可以进行自适应调整，降低岗位对工人技术要求。

面向行业应用的行业云解决方案

行业云是面向食品、软件、化工、等重点行业而搭建的平台。行业云有效实现行业内的数据共享及数据活化，提供更好的服务。

面向区域应用的工业云解决方案

工业云是一种新型的网络化制造服务模式，以公共服务平台为载体，通过虚拟化、服务化和协同化汇聚分布、异构制造资源和能力，在制造全生命周期各个阶段提供优质、及时、低成本的服务。

工业控制系统包含什么？

工业控制系统包括数据采集系统（Supervisory Control And Data Acquisition，SCADA）、分布式控制系统（Distributed Control System，DCS）、可编程逻辑控制器（Programmable Logic Controller，PLC）以及其他控制系统。数据采集系统是以计算机为基础的生产过程控制和调度自动化系统，适用于地理环境恶劣无人值守的环境；分布式控制系统属于过程控制系统，适用于流程行业；可编程逻辑控制器属于离散控制系统，适用于制造业。

工业控制系统面临的威胁

工业控制系统面临的威胁主要有三个：

外部威胁——APT、目标攻击等

工业控制系统网络的外部威胁可能与政治敌对势力(如某个民族、国家、恐怖组织或激进黑客)有关，但也可能部分出于工业间谍活动。对手的动机不同，其攻击目的也多种多样。比如说，政治敌对势力更倾向于中断工业控制系统运行或摧毁工业控制系统，而工业间谍更倾向于窃取知识产权。目前，大多数工业部门，尤其是涉及关键基础设施的部门，更容易成为政治动机的攻击目标，目的是造成系统运行中断或摧毁系统。而那些不身处关键基础设施行业的部门也容易被波及到，因为，出于政治动机的网络攻击所利用的漏洞是所有工业行业都可能会用到的技术。所以无可避免地会影响到非目标企业及其工业控制系统。

内部威胁——员工、承包商等

工业网络在风险上与IT网络是大致相当的。雇员、承包商和第三方集成商等都拥有工业控制系统网络的合法访问权，由于大多数工业控制系统网络缺乏身份验证或加密措施来限制用户活动，任何内部人士都能无限制的访问网络设备。

人为失误——可能是工业控制网络最大的威胁

人为失误无法避免，但因此造成的损失可能是巨大的，对很多企业、部门来说，人为失误造成的损失可能比内部威胁更严重。所以，在某些情况下，人为失误可以看作是工业控制系统的最大威胁。人为失误包括配置错误、设置错误、可编程逻辑控制器(PLC)编程错误等，能导致 workflow 中的危险改变。有些人为失误是员工违规操作引起的，比如有时需要远程接入工业控制系统网络，但系统不提供安全连接，这时员工只可能会自己建立未经授权的远程连接，这个未经授权的远程连接就有可能被攻击方利用，攻击系统。更多时候，人为失误造成的漏洞更容易被攻击者利用。

工业控制系统的防护策略

白名单策略：对获得信任的程序实行白名单管理 防止恶意软件或未经许可的软件的执行

补丁管理：对于计算机中的各种软件及操作系统实行补丁管理 维护好每一台计算机设备上的软件信息 包括软件版本及补丁安装历史等 否则 软件中“高危”漏洞有可能给企业造成严重损失

尽量减少拥有域管理或本地管理权限的用户数量：用户在进行低风险操作时应使用普通账户 最好是在临时性的虚拟环境或普通电脑上操作 降低被攻击的风险

屏蔽本地管理员账户：避免攻击者利用被破解的本地管理员账户（入侵企业网络内的其他计算机设备

多重身份认证：在远程登陆计算机、进入数据库或其他敏感信息库以及进行权限操作（如系统管理等）时应该实行多重身份认证 如密码、指纹、物理令牌等信息

网络隔离：在考虑连接需求、用户角色、业务功能、信任界限和信息敏感度等因素 将某个电脑设备与其它电脑设备之间的通讯进行控制 例如 不允许用户电脑间相互通讯 企业还可以限制VPN和远程登陆、无线连接以及员工使用自带的电脑、智能手机等设备

防火墙技术：阻止恶意软件或其它未经许可的通信进入网络 仅允许白名单上的软件向网络外进行通信

设立临时性虚拟操作环境：为读取邮件、网络浏览等不安全操作提供临时性虚拟操作环境 便于由感染状态自动恢复到正常状态 但是这样无法保留入侵痕迹、入侵证据

引入主机入侵检测/防御系统：可有效识别系统异常情况 & 恶意软件 避免误判

集中并同步记录事件日志：自动同步记录并分析所有成功或失败的计算机事件及所有允许和受阻的网络行为 相关日志应保留一定时间

加强工作站应用程序的安全设置：严格对与网络通信的应用程序进行设置 及时关闭不需要的脚本、宏功能及各种插件

用户培训：培训用户识别有风险的内容及不进行各种有风险的操作 养成良好的使用习惯 如不使用弱密码、不泄露私人信息、不使用外带的USB设备或其他IT设备等

计算机配置管理：屏蔽非必需的操作系统功能 如IPv6、自动运行、远程桌面等 保持用户电脑配置管理的一致性

禁止工作站直接访问因特网：为工作站配备一个非路由网络捕捉设备作为缺省路由 避免恶意软件直接与因特网通信

安装防病毒软件：有些防病毒产品已经发展为反恶意软件产品 安装这些软件来及时检测系统安全 防止病毒危害计算机

强制实施强密码措施：对服务账户和其他具有管理权限的账户应实施强密码措施 避免重复使用密码和使字典词语做密码

网络安全篇

信息安全

什么是信息安全？

信息安全是对数据处理系统采取的技术和管理的安全保护 目的是保护计算机硬件、软件、数据不因偶然的或恶意的原因而遭到损坏、修改和泄露 信息安全主要包括以下五个方面的内容：保证信息的真实性、保密性、完整性、未经授权拷贝和所寄生系统的安全性

信息安全是一门涉及计算机科学、通信技术、应用数学、数论、网络技术、密码技术、信息论、信息安全技术等多种学科的综合性学科

什么是网络安全？

网络安全是指网络系统的软件、硬件及其系统中的数据受到保护 不因偶然的或者恶意的原因而遭到损坏、修改和泄露 系统连续、可靠、正常地运行 网络服务不中断 网络安全从广义上来说 凡是涉及到网络信息的保密性、可用性、完整性、可控性和真实性的相关技术和理论都是网络安全的研究领域 从其本质上来就是网络上的信息安全

网络安全是一门涉及计算机科学、通信技术、应用数学、数论、网络技术、密码技术、信息论、信息安全技术等多种学科的综合性学科

安全隐患的产生原因、类型区别有哪些？

安全隐患产生的原因主要有以下五个方面：

网络通信协议的不安全

计算机病毒的入侵

黑客的攻击

操作系统和应用软件的安全漏洞

防火墙自身带来的安全漏洞

安全隐患的类型主要分为主动攻击和被动攻击两大类

主动攻击包含攻击者访问所需信息的故意行为 比如伪造无效 IP 地址去连接服务器 使接受到错误 IP 地址的系统浪费时间去连接到某个非法地址；远程登录到指定机器的端口 找出公司运行的邮件服务器的信息 主动攻击包括拒绝服务攻击、资源使用、欺骗、信息篡改等攻击方法

被动攻击主要是收集信息而不是进行访问 数据的合法用户对这种活动毫无察觉 被动攻击包括嗅探、信息收集等攻击方法 从攻击的目的来看 有拒绝服务攻击(Dos)、获取敏感信息的攻击、获取系统权限的攻击；从攻击的切入点来看 有缓冲区溢出攻击、系统设置漏洞的攻击等；从攻击的纵向实施过程来看 有获取初级权限攻击、提升最高权限的攻击、后门攻击、跳板攻击等；从攻击的类型来看 有对各种操作系统的攻击、对特定应用系统的攻击、对网络设备的攻击等

网络安全的实现目标和主要技术措施

在网络安全领域 攻击随时可能发生 系统随时可能崩溃 仅靠人工完成这些繁重的工作是不可能的 所以 必须借助先进的技术和工具来帮助企业完成如此繁重的劳动 以保证计算机网络的安全

计算机网络的安全性主要包括网络服务的可用性（Availability）、网络信息的完整性（Integrity）和网络信息的保密性（Confidentiality） 下列是几个与之相关的重要网络安全技术：

杀毒软件

与一般的单机杀毒软件相比 杀毒软件的网络版市场更多是技术及服务的竞争 其特点表现在杀病毒技术的发展日益国际化 世界上每天会出现有 13 种到 50 种新病毒 并且60%的病毒均通过互联网传播 病毒发展有日益跨越疆界的趋势 杀病毒企业的竞争也随之日益国际化

防火墙

防火墙技术是网络安全中系统安全产品使用最广泛的技术 即在 Internet 和内部网络之间设一个防火墙 目前在全球连入 Internet 的计算机中约有三分之一处于防火墙保护之下

加密技术

加密技术是网络安全的另一个非常重要的手段 它的核心思想是：既然网络本身并不安全可靠 那么所有重要信息就全部通过加密处理 加密技术主要分两种：单匙技术和双匙技术

信息安全的主要表现形式

信息安全的主要表现形式有蠕虫或病毒扩散、垃圾邮件泛滥、黑客行为、信息系统脆弱性和有害信息的恶意传播等

网络信息传播方式

网络媒体集散信息观点影响社会舆论

无论是信息量，还是观点数量，网络媒体都已超过传统媒体，成为社会舆论的重要发源地。网上不仅有正面信息，也有流言、谣言、假新闻等负面信息，如果不善加管理和引导，会对社会舆论产生负面影响。

网络论坛发酵网民情感引致社会行动

网民在网络论坛中的真实面目和身份被各种符号所代替，具有隐匿性。网民可以毫无顾忌地发表意见，各种观念在网上集合、交汇、碰撞，夹杂着有害的、负面的杂音和噪音。网络论坛成为“意见市场”，帖子成为“意见广告”。在论坛讨论中，兴趣观点比较相近的网民更容易聚集在一起，形成独特的政治场。这种政治场不断放大网民意见，形成“集体狂欢”，出现舆论一边倒的极化现象。网站论坛成为网络舆论发酵器，累积情绪，直至引发社会行动，实现从虚拟政治到现实政治的转换。

网络通讯隐秘传递信息编织社会网络

网络通讯（包括电子邮件和即时通讯）是互联网的重要功能，具有隐秘性、快捷性等特点。电子邮件使用简单、易于保存、投递迅速、全球畅通，可以传播文字、声音、图像等多种资料，可以进行一对一、一对多传递，极大地改变信息传播方式。但是，电子邮件在给人们带来诸多便利的同时，也被境内外敌对势力加以利用。2008年“3.14”事件爆发之前，境外“藏独”分子就通过电子邮件发送《“西藏人民大起义运动”倡议书》和达赖“3.10”讲话等材料，反复煽动人民群众。

网络检索强力搜寻相关信息确定社会角色

百度、谷歌、搜狐等搜索引擎具有强大的信息检索功能，可以在瞬间检索上百亿张网页，搜寻相关信息，给人们的工作、学习、生活、研究等都带来极大便利。

网络博客传播思想观点影响社会思潮

博客是近年来增幅最大的言论载体，个人上网写博客正在形成一个新的文化奇观。Web2.0的推广，实现了“去中心化”的非线性传播，打破了网络出版的限制，消除了网民交流的中间环节，每个网民都可以成为传播发起节点，人人是记者、人人是作家、人人是编辑、人人办刊物。不但各类网站纷纷开设博客频道，而且出现了专门的博客网站。通过博客传播的观点已经并将继续影响社会思潮。

网络站点成为群体社会活动组织平台

交友网站和网络社区使网民出现分众化趋势，为相同兴趣（比如郊游）的网民组织活动提供平台，丰富网民生活。网络站点也成为集体上访等群体行动的组织平台。网络传播信息迅速、高效、广泛，使得集体串联活动十分便捷。

信息安全的基本属性

信息安全的基本属性主要表现在以下5个方面：

保密性（Confidentiality）：保证信息为授权者享用而不泄漏给未经授权者

完整性（Integrity）：保证信息从真实的发信者传送到真实的收信者手中 传送过程中没有被非法用户添加、删除、替换等

可用性（Availability）：保证信息和信息系统随时为授权者提供服务 保证合法用户对信息和资源的使用得到合理授权

可控性（Controllability）：出于国家和机构的利益和社会管理的需要 保证管理者能够对信息实施必

要的控制管理 以对抗社会犯罪和外敌侵犯

不可否认性 (Non-Repudiation) : 人们要为自己的信息行为负责 提供保证社会依法管理需要的公证、仲裁信息证据

建立安全网络的基本策略

引入入侵检测系统

入侵检测是指通过对计算机网络或计算机系统中的若干关键点收集信息并对其进行分析,从中发现网络或系统中是否有违反安全策略的行为和遭到攻击的迹象,同时作出响应。入侵检测作为一种积极主动的安全防护技术,能很好地弥补防火墙的不足。它能够帮助系统对付网络攻击,扩展了系统管理员的安全管理能力(包括安全审计、监视、进攻识别和响应),提高了信息安全基础结构的完整性。

加强加密强度

加密强度取决于三个主要因素:

第一个因素是算法的强度,包括几个因素,例如,除了尝试所有可能的密钥组合之外的任何方法都不能数学的使信息被解密。从我们的角度而言,我们应该使用工业标准的算法,它们已经被加密学专家测试过无数次,任何一个新的或个体的配方将不被信任直到它被商业的认证。

第二个因素是密钥的保密性,一个合乎逻辑但有时被忽略了的方面。如果密钥受到损害,没有算法能够发挥作用。因此,数据的保密程度直接与密钥的保密程度相关。

第三个因素是密钥长度,这是最为人所知的一个方面。根据加密和解密的应用程序,密钥的长度是由“位”为单位,在密钥的长度上加上一位则相当于把可能的密钥的总数乘以二倍,简单的说,构成一个任意给定长度的密钥的位的可能组合的个数可以被表示为2的n次方,这儿的n代表密钥长度。

弥补缺陷漏洞

弱点漏洞是系统在设计过程中留下的问题,也是黑客入侵系统时经常利用的系统漏洞。及时发现、弥补这些先天不足,对保证系统安全尤为重要。人工的测试,费时费力并且不切实际。弱点漏洞分析系统能自动侦测分析系统存在的弱点漏洞,并提出相关问题的解决方案。

网络边界上的安全问题主要有哪几方面?

信息泄密:网络上的资源是可以共享的,但没有授权的人得到了他不该得到的资源,信息就被泄露了。一般信息泄密有两种方式:

网络内部泄密:指的是攻击者(非授权人员)进入了网络,获取了信息。

网络外部泄密:指的是合法使用者在进行正常业务往来时,信息被外人获得。

入侵者的攻击:互联网是世界级的大众网络,网络上有各种势力与团体。入侵是指有人通过互联网(或其他渠道)进入你的网络,篡改数据或实施破坏行为,造成网络业务的瘫痪。这种攻击是主动的、有目的、甚至是有组织的行为。

网络病毒:与非安全网络的业务互联,可能会在通讯中带来病毒,一旦在被侵入用户的网络中发作,业务将受到极大冲击。病毒的传播与发作一般具有不确定的随机特性。这是“无对手”、“无意识”的攻击行为。

木马入侵:木马的发展是一种新型的攻击行为,它在传播时象病毒一样自由扩散,没有主动的迹象,但进入用户的网络后,便主动与他的“主人”联络,从而让“主人”来控制你的机器,既可以盗用你的网络信息,也可以利用用户的系统资源为他工作。比较典型的就“僵尸网络”。

信息加密的基本概念

信息加密技术是通过数学或物理手段对电子信息在传输过程中和存储体内进行保护以防止泄露的技术

在计算机通讯中采用密码技术将信息隐藏起来再将隐藏后的信息传输出去使信息在传输过程中即使被窃取或截获窃取者也不能了解信息的内容从而保证信息传输的安全

任何一个加密系统至少包括下面四个组成部分:

(1) 明文:指未加密的报文

(2) 密文:指加密后的报文

(3) 加密解密设备或算法

(4) 加密解密的密钥

发送方用加密密钥通过加密设备或算法将信息进行加密后发送出去 接收方在收到密文后 用解密密钥将密文解密 恢复为明文 如果传输中有人窃取 窃取者只能得到无法理解的密文 从而对信息起到保密作用

什么是对称加密？

对称加密指的是需要对加密和解密使用相同密钥的机密算法 由于其速度快 对称性加密通常在消息发送方需要加密大量数据时使用 对称性加密也称为密钥加密 在对称加密(或单密钥加密)中 只有一个密钥用来加密和解密信息 即使单密钥加密是一个简单的过程 双方也都必须完全的相信对方 并都持有这个密钥的备份

什么是非对称加密？

非对称加密算法需要两个密钥：公开密钥（publickey）和私有密钥（privatekey） 公开密钥与私有密钥是一对 一个用于加密 另一个用来解密 如果用公开密钥对数据进行加密 只有用对应的私有密钥才能解密；如果用私有密钥对数据进行加密 那么只有用对应的公开密钥才能解密 因为加密和解密使用的是两个不同的密钥 所以这种算法叫作非对称加密算法

什么是数字签名？

"数字签名"是通过某种密码运算生成一系列符号及代码组成电子密码进行签名 是只有信息发送者才能产生的别人无法伪造的一段数字串 这段数字串同时也有效证明了信息发送者发送信息的真实性的一个有效证明

"数字签名"是目前电子商务、电子政务中应用最普遍、可操作性最强、技术最成熟的一种电子签名方法 它采用规范化的程序和科学化的方法 用于鉴定签名人的身份、对电子数据内容的认可、验证文件的原文在传输过程中有无变动等 确保传输电子文件的真实性、完整性和不可抵赖性

计算机病毒的防范

什么是病毒？

计算机病毒是指编制或在计算机程序中插入的破坏计算机功能或者损坏数据、影响计算机使用、能自我复制的一组计算机指令或者程序代码 通俗的讲 计算机病毒是人为编写的有害代码

计算机病毒特性

破坏性

任何病毒只要侵入系统，都会对系统及应用程序产生不同程度的影响。轻则显示一些画面，发出音乐，弹出一些无用的窗口。重则损坏数据，删除文件，格式化磁盘，有的甚至对计算机硬件也有损坏。

隐蔽性

病毒一般是短小精悍的一段程序，通常潜入到正常程序或磁盘中。在没有防护的情况下，有些病毒是在悄无声息地破坏计算机或者进行自我复制，有些病毒还嵌入到正常的程序中，因此很难被发现。

潜伏性

大部分病毒在侵入系统之后不会马上发作，它可以长时间隐藏在系统之中，在满足其特定条件下才会发作。

传染性

传染是大多数计算机病毒的一个重要特点。它通过修改别的程序，并包含自身的副本，以达到扩散的目的。病毒能将自身的代码强行传染到一切符合其传染条件的未感染文件，而且还可以通过各种可能的渠道感染其他计算机。

不可预见性

从病毒检测技术来看，病毒还有不可预见性。不同种类的病毒，其代码千差万别。有的正常的程序也使用了类似病毒的操作甚至借鉴了某些病毒的技术，甄别起来更是困难。再加上病毒的制作技术也在不断的提高，所以病毒对于反病毒软件来说永远是超前的。

计算机病毒引起的异常情况

计算机中病毒后通常会有一下几种情况：

操作系统无法正常启动；运行速度明显变慢；平时能正常运行的计算机突然经常性无缘无故地死机；平时能正常运行的应用程序经常发生死机或者非法错误；无意中要求对软盘进行写操作；发出一段音乐；产生特定的图象；鼠标自己在动；系统文件的时间、日期、大小发生变化；陌生人发来的电子函件；磁盘空间迅速减少；提示一些不相干的信息；硬盘灯不断闪烁；Windows桌面图标发生变化。

计算机病毒的危害

病毒发作对计算机数据信息的直接破坏作用

大部分病毒在发作的时候直接破坏计算机的重要数据信息 方法有格式化磁盘、破坏CMOS设置、删除重要文件或者用无意义的“垃圾”数据改写文件、改写文件分配表和目录区等

占用磁盘空间和对信息的破坏

寄生在磁盘上的病毒总要非法占用一部分磁盘空间 文件型病毒利用一些DOS功能进行传染 这些DOS功能能够检测出磁盘的剩余空间 将病毒的传染部分写入磁盘的剩余空间中 所以 文件型病毒在传染过程中一般不破坏磁盘中的原有数据 但非法占用了一部分磁盘空间 一些文件型病毒传染速度很快 在短时间内传染大量文件 每个文件都不同程度地增大了 进而造成磁盘空间的严重浪费 引导型病毒的一般传染方式是由病毒本身占据磁盘引导扇区 而把原来的引导扇区转移到其他扇区 **也就是说引导型病毒要覆盖一个磁盘扇区** 被覆盖扇区的数据将会永久性丢失 并且无法恢复

占用系统资源

除VIENNA、CASPER等少数病毒外 其他大多数病毒在动态下都是常驻内存的 这就会占用一部分系统资源 病毒所占用的基本内存长度与病毒本身长度大致相同 病毒占用内存 导致内存减少 一部分软件无法运行

影响计算机运行速度

病毒进驻内存后不但干扰系统运行 还影响计算机速度 主要表现在：

病毒为了判断传染激发条件 需要监视计算机的工作状态 这对于计算机的正常运行状态来说是多余且有害的

有些病毒为了保护自己 不但对磁盘上的静态病毒进行加密 还会对进驻内存后的动态病毒进行加密 CPU每次寻找到病毒位置时要运行一段解密程序 把加密的病毒解密成合法的CPU指令再执行 而病毒运行结束时会再用一段程序对自身重新加密 这样CPU会执行成千甚至上万条多余的指令

病毒在进行传染时同样要插入非法的额外操作 特别是传染软盘时计算机运行速度会明显下降 而且软盘正常的读写顺序被打乱 **发出刺耳的噪声**

计算机病毒的兼容性对系统运行的影响

兼容性是计算机软件的一项重要指标 兼容性差的软件会对运行条件“挑肥拣瘦” 对操作系统和机型等有着严格要求 反之兼容性好的软件则可以在各种计算机环境下运行 病毒的编制者一般不会在各种计算机环境下对病毒进行测试 因此病毒的兼容性较差 常常导致死机

计算机病毒给用户造成严重的心理压力

对于保护计算机安全来说 用户对病毒采取宁可信其有的态度无疑是十分必要的 然而这往往需要付出时间、金钱等方面的代价 许多用户常常只是怀疑磁盘中有病毒就格式化磁盘 这种做法所带来的损失更是难以弥补 不仅是个人单机用户 在一些大型网络系统中也难免为甄别病毒而停机 总之计算机病毒像“幽灵”一样笼罩在广大计算机用户心头 给人们造成巨大的心理压力 极大地影响了现代计算机的使用效率 从而带来难以估量的无形损失

计算机病毒的传播途径

计算机病毒主要是通过运行程序、复制文件、传输文件等手段进行传播 在日常的使用中 有以下几种传播途径：

硬盘：硬盘的存储量大 在利用它传输文件或引导系统时 也很容易传播病毒

软盘：使用外界被感染的软盘造成病毒的传播 例如 使用来历不明的软件、不明渠道获得的系统盘、游戏盘等是最普遍的传播方式

光盘：光盘存储容量大 携带方便 便于传输文件 然而盗版光盘的泛滥却为病毒传播带来了方便 盗版

光盘上的软件未经过严格的病毒检测 难免会携带病毒 即使用户发现病毒也无法清除

网络：随着互联网的普及 人们通过网络来传输文件越来越方便 但是对于网上众多的软件 谁也不能保证其中不携带病毒 由于网络速度快、覆盖面广 更为病毒的快速传播创造了条件 近年来出现的许多新式病毒都是通过网络进行传播的 破坏性极强

国内外知名的反病毒软件有哪些？

国内外常用反病毒软件有：

瑞星杀毒；软件金山毒霸；诺顿（反病毒程序）；360杀毒（整合了五大领先查杀引擎）；腾讯电脑管家（拥有云查杀木马，系统加速，漏洞修复实时防护，网速保护，文档保护等功能）。

U盘、移动硬盘病毒防范

一般U盘一般都是FAT32格式，如果是FAT格式的，格式化成 FAT32。

在U盘的根目录下面，建一个名为：autorun.ini 文件夹，注意这里不是文件，而是新建文件夹，然后在 autorun.ini 里面再建一个 autorun.ini 文件夹，第二个autorun.ini 文件夹里面新建一个 1.txt 全部设为只读模式即可。

不要复制exe格式的文件到U盘里面，把exe文件打包成rar格式再复制进U盘，这样是防止exe格式被感染。

不要在U盘里面建文件夹放东西，因为有的病毒会把文件夹隐藏掉。

对于移动硬盘，格式化成 具有安全设置功能的ntfs 格式。

电子邮件附件病毒防范

第一，不要轻易执行附件中的*.EXE和*.COM文件，这些附件极有可能携带病毒或黑客程序，轻易运行，很可能带来不可预测的结果。对于相识和不相识的朋友发过来的附件都必须检查，确定安全后才可放心使用。

第二，不要轻易打开附件中的文件或文档。对于对方发送过来的电子邮件及相关附件的文档，首先要用“save as”命令保存起来，然后用杀毒软件检查无毒后才可以打开使用。如果直接打开相关的附件文档，计算机会自动启用相关的软件，如有病毒则会立刻传染，不过在运行Office97时，如有“是否启用宏”的提示，那绝对不要轻易打开，否则极有可能传染上邮件病毒，当前的Melissa和Papa病毒就是其中的例子。

第三，对于自己发送的附件，也一定要查看是否有毒，待确认无毒后，才可以发送。虽然电子邮件病毒非常可怕，但是只要不轻易运行和打开附件，是不会传染上病毒的，仍可放心使用。

第四，对付电子邮件病毒，最有效的方法是在运行的计算机上安装实时化的杀毒软件。实时化杀毒软件会时刻监视用户对外的任何操作，如从网上接收电子邮件或下载有关文件、运行有关邮件附件的文档或程序，实时化杀毒软件时刻监视着这些文件是否有病毒，如有，会自动进行报警，并立即清除，不需人为干涉。当然对于这些软件要及时升级，才能取得最佳的效果

网页传播病毒防范

网页病毒防治的关键在于网页病毒防范。网页病毒防范主要是遵循一个原则：尽量不点击不熟悉的或者认为可能有病毒的网站，这样可以减少中毒的可能性。如果中了网页病毒，也不要慌张，可以根据其表现形式逐一解决。因为网页病毒主要是通过网页中嵌入程序脚本语言来修改浏览者系统中的注册表相应的键值，所以可以通过修改注册表的方法来解决。如果注册表也被锁定禁用，那么先要通过一些软件把注册表恢复过来再进行修改。

文档杀手-宏病毒

为了减少用户的重复劳作，例如进行相似的操作，Office提供了一种所谓宏的功能。用户可以通过这个功能把一系列的操作记录下来，作为一个宏。之后只要运行这个宏，计算机就能自动地重复执行定义在宏中的所有操作。虽然这种宏操作方便了普通的计算机用户，但同时也给病毒制造者提供了可乘之机。

宏病毒是一种专门感染 Office系列文档的恶性病毒。1995年，世界上发现了第一个宏病毒Concept。由于宏的编程语言VBA简单易学，因此大量的宏病毒层出不穷，短短两年时间其数量就上升至20000多种！除了感染Word的宏病毒，还出现了感染Amipro、Excel、Access的宏病毒，宏病毒还可以在它们之间相互感染，并由Word感染Windows的虚拟驱动程序，从而造成严重的后果。

0day病毒

0DAY漏洞 最早的破解是专门针对软件的，叫做WAREZ，后来才发展到游戏，音乐，影视等其他内容的。0day中的0表示zero，早期的0day表示在软件发行后的24小时内就出现破解版本，现在我们已经引申了这个含义，只要是在软件或者其他东西发布后，在最短时间内出现相关破解的，都可以叫0day。0day是一个统称，所有的破解都可以叫0day。

互联网时代敲诈者-勒索病毒

勒索病毒是一种新型电脑病毒，是黑客通过锁屏、加密文件等方式劫持用户文件并以此敲诈用户钱财的恶意软件。黑客通过网络钓鱼或利用系统漏洞等方式，向受害电脑或服务器植入病毒，从而加密硬盘上的文档甚至整个硬盘，之后向受害者索要数额不等的赎金后才给予解密。

勒索病毒-事前防范

目前已知的是，Windows 10操作系统只要打开了自动更新，就不会有中毒的风险。而目前国内大量使用的Windows 7甚至Windows XP电脑则比较容易中毒。目前，微软已经为所有的Windows系统紧急发布了系统补丁。

另外，像445这样的高危端口，一般的家用电脑也最好关闭掉。关闭方法为：

打开“控制面板”，点击防火墙

点击“高级设置”

先点击“入站规则”，再点击“新建规则”

勾选“端口”，点击“协议与端口”

勾选“特定本地端口”，填写445，点击下一步

点击“阻止链接”，一直下一步，即可完成

勒索病毒-中毒后应对方法

立即组织内网检测，查找所有开放445 SMB服务端口的终端和服务端，一旦发现中毒机器，立即断网处理。目前看来对硬盘格式化可清除病毒。对于XP、2003等微软已不再提供安全更新的机器，建议升级操作系统版本或使用360“NSA武器库免疫工具”对系统进行检测，查看是否存在漏洞，并关闭受到漏洞影响的端口，以此避免遭到勒索软件等病毒的危害。

一旦发现电脑中毒，立即断网。启用并打开“Windows防火墙”，进入“高级设置”，在入站规则里禁用“文件和打印机共享”相关规则。关闭UDP135、445、137、138、139端口，关闭网络文件共享。

尽快对电脑中的重要文件资料进行备份。

严格禁止使用U盘、移动硬盘等可执行摆渡攻击的设备。

及时更新操作系统和应用程序到最新的版本。

计算机病毒有利的一面

计算机病毒对抗是电子战的新领域，也是近年来C3I对抗中的热门话题。目前世界各国的军事电子领域都竞相开始研究这种全新的电子战“武器”，计算机病毒所攻击的是系统的核心部件，此外，它还具有隐蔽性和传染性的特点，这就为电子对抗提供了崭新的技术手段。

科学家断言：未来战争破坏力最大的已不再是核打击，在电脑已经成为军事指挥、武器控制和国家经济中枢的情况下，“计算机病毒打击”将更直接、更危险。可想而知，随着微电脑技术在军事领域越来越广泛地应用，进攻性的计算机病毒武器将迅速投入战场。计算机病毒武器将成为信息战的杀手锏。

黑客与入侵检测

什么是黑客？

黑客是Hacker的译音 源于Hack 本意为“做了一件非常漂亮的工作”原指一群精力旺盛、专业技能超群、聪明能干、对计算机信息系统进行非授权访问的人员 而现在黑客泛指在计算机技术上有一定特长 掌握一定的技术知识 采用非法手段逃过计算机网络系统的访问控制 而未经授权或非法访问进入计算机网络的人 被认为是网络“攻击者”和“破坏者”

黑客攻击的动机

黑客攻击的动机主要有以下几种：

好奇心：对数据内容、网络系统或网站的好奇 从而进行窥探；
恶作剧：无聊的计算机程序员 通过网络进行戏弄；
贪欲：盗窃或者敲诈重要资料或财物；
宿怨报复：受批评、被降级或被解雇的雇员 或者其他任何认为自己受到不公平对待的人员 利用网络进行肆意报复；
名声显露：通过展示计算机经验与才能来证明自己的能力并获得名气；
仇恨义愤：国家和民族利益和情感因素的原因；
黑客道德：许多构成黑客人物的动机；
获取机密：以军事、政治、商业经济竞争为目的的间谍窃取机密工作

黑客攻击的分类

按攻击的行为主动性分为：

主动攻击、被动攻击

按攻击的位置情况可分为：

远程攻击、本地攻击、伪远程攻击

黑客攻击的过程

黑客常用的攻击步骤可以说变幻莫测 但其整个攻击过程也具有一定规律 一般可以分为“攻击五部曲”：隐藏IP、踩点扫描、获得特权、种植后门、隐身退出

黑客根据实际情况变化也可能进行调整 掌握黑客攻击规律有助于进行有针对性的防范 网络情况复杂 黑客个性各异 其攻击流程也不尽完全相同 这5个攻击步骤是对一般情况而言的 是绝大部分黑客在通常情况下的一般规律

黑客攻击常用的方法

黑客常用的方法有以下几种：

端口扫描

端口扫描往往也成为黑客发现获得主机信息的一种最佳途径。

网络监听

网络监听工具Sniffer (也称嗅探器)和 NetXRay等原本是用于网络检测管理的工具，主要是分析网络的流量，以便找出所关注网络中潜在的问题。但也可以被黑客用于窃听网络，因此也属于一种攻击手段。

网络嗅探

网络嗅探就是使网络接口接收不属于本主机的数据。通常账户和密码等信息都以明文的形式在以太网上传输，一旦被黑客在杂错节点上嗅探到，用户就可能会遭到损害。

网络监听的概念及原理

网络监听工具是利用计算机的网络接口截获目的地为其他计算机的数据报文的一种工具 可以作为能够捕捉网络报文的设备 也可以被理解作为一种安装在计算机上的监听设备 可以用于监听计算机在网络上所产生的多种信息

网络监听的检测

网络监听的威胁

网络监听能够捕获密码 这大概是绝大多数人非法使用监听工具的理由 网络监听还能够捕获专用的或者机密的信息

网络监听的检测方法

在Linux 下对嗅探攻击的程序检测方法比较简单 一般只要检查网卡是否处于混杂模式就可以了；而在Windows 平台中 并没有现成的函数可供实现这个功能 只要可以执行程序检查一下是否有嗅探程序在运行即可 (c:\windows\Drwatson.exe)

网络嗅探的防范对象

对于网络嗅探攻击 可以采取以下一些措施进行防范

(1) 网络分段

(2) 加密

(3) 一次性密码技术

特洛伊木马的攻击原理

特洛伊木马是指隐藏在正常程序中一段具有特殊功能的恶意代码，是具备破坏和删除文件、发送密码、记录键盘和攻击Dos等特殊功能的后门程序。

一个完整的木马系统由硬件部分、软件部分和具体连接部分组成。

使用木马工具进行网络入侵，基本过程可以分为6个步骤。

(1) 配置木马

(2) 传播木马

(3) 运行木马

(4) 泄露信息 收集一些服务端的软硬件信息，并通过E-mail或ICQ等告知控制端用户。

(5) 建立连接 服务端安装木马程序，且控制端及服务端都要在线。控制端可以通过木马端口与服务端建立连接。

(6) 远程控制 通过木马程序对服务端进行远程控制。

缓冲区溢出攻防

缓冲区溢出的原理

缓冲区溢出攻击是指通过往程序的缓冲区写超出其长度的内容，造成缓冲区的溢出，从而破坏程序的堆栈，使程序转而执行其他指令，以达到攻击的目的。造成缓冲区溢出的原因是没有仔细检查程序中用户输入的参数。

最常见的缓冲区溢出攻击手段是通过制造缓冲区溢出使程序运行一个用户shell，再通过shell执行其他命令。如果该程序属于root且有suid权限，攻击者就获得了一个有root权限的shell，可以对系统进行任意操作。

拒绝服务攻击与防范

拒绝服务攻击（Denial of Service，简称DoS）是指黑客利用使网站服务器充斥巨量请求和信息的手段，消耗网络带宽或系统资源，最终导致网络系统难以运行，直至瘫痪而停止提供正常的网络服务的攻击方式。

“拒绝服务”的一种攻击方式为：传送众多要求确认的信息到服务器，使服务器里充斥着大量无用的信息。所有的信息都有需回复的虚假地址，以至于当服务器试图回传时，却无法找到用户。服务器于是暂时等候，有时超过几分钟，然后再切断连接。服务器切断连接时，黑客再度传送新一批需要确认的信息，这个过程周而复始，最终导致服务器瘫痪。经常遭受攻击的主要目标包括：路由器、数据库、Web服务器、FTP服务器和与协议相关的服务。

DDoS攻击防范

分布式拒绝服务攻击(DDoS)是目前黑客经常采用而难以防范的攻击手段。分布式拒绝服务攻击手段DDoS是通过网络进行的多对一的攻击方式。

DDoS攻击实例——目前最流行的DDoS攻击手段SYN Flood攻击。

防范攻击的措施与步骤

防范攻击的措施

1. 提高防范意识
2. 设置安全口令
3. 实施存取控制
4. 加密及认证
5. 定期分析系统日志
6. 完善服务器系统安全性能
7. 进行动态站点监控
8. 安全管理检测
9. 做好数据备份
10. 使用防火墙和防毒软件

防范攻击的步骤

1. 选好操作系统
2. 补丁升级
3. 关闭无用的服务和端口
4. 隐藏IP 地址
5. 查找本机漏洞
6. 选用防火墙软件

入侵检测系统的概念与功能

入侵检测系统 (Intrusion Detection System IDS) 是进行入侵检测监控和分析过程自动化的软件与硬件的组合系统 它处于防火墙之后对网络活动进行实时检测 入侵检测技术IDS是一种主动保护自己免受攻击的一种网络安全技术

入侵检测系统主要功能包括6个方面：

- (1) 监视、分析用户及系统活动；
- (2) 系统构造和弱点的审计；
- (3) 识别反映已知进攻的活动模式并向相关人员报警；
- (4) 异常行为模式的统计分析；
- (5) 评估重要系统和数据文件的完整性；
- (6) 操作系统的审计跟踪管理 并识别用户违反安全策略的行为

入侵检测系统的组成及特点

入侵检测系统组成

通常IDS由传感器 (Sensor) 与控制台 (Console) 两部分组成

传感器主要包括事件发生器、事件分析器和事件数据库等 负责采集数据 (网络包、系统日志等)、分析数据并生成安全事件

控制台包括发现入侵、响应单元和作出相应等部件/模块 主要起到中央管理的作用 商品化的IDS通常提供图形界面的控制台

入侵检测系统的特点

入侵检测技术是动态安全技术的最核心技术之一 入侵检测被认为是防火墙之后的第二道安全闸门 提供对内部攻击、外部攻击和误操作的实时保护
信息系统测评

黑客

黑客(Hacker)源于Hack 本意为“干了一件非常漂亮的事” 原指一群专业技能超群、聪明能干、精力旺盛、对计算机信息系统进行百授权访问的人员 现通常将泛指的黑客认为是在计算机技术上有一定特长 并凭借掌握的技术知识 采用非法手段 逃过计算机网络系统的访问控制 而进入计算机网络进行未授权或非法访问的人 认为是网络“攻击者”和“破坏者”

黑客的动机

随着时间的变化 黑客攻击的动机变得越来越多样化 主要有以下几种：

- (1) 好奇心：对网络系统、网站或数据内容的好奇而窥视；
- (2) 贪欲：偷窃或者敲诈财物和重要资料；
- (3) 恶作剧：无聊的计算机程序员 通过网络进行戏弄；
- (4) 名声显露：显示计算机经验与才智 以便证明自己的能力和获得名气；
- (5) 宿怨报复：被解雇、受批评或者被降级的雇员 或者其他任何认为其被不公平地对待的人员 利用网络进行肆意报复；
- (6) 黑客道德：这是许多构成黑客人物的动机；
- (7) 仇恨义愤：国家和民族利益和情感因素的原因；
- (8) 获取机密：以政治、军事、商业经济竞争为目的的间谍窃取机密 工作

黑客攻击的分类

按攻击的行为主动性分为：

主动攻击、被动攻击

按攻击的位置情况可分为：

远程攻击、本地攻击、伪远程攻击

黑客攻击的过程

黑客常用的攻击步骤可以说变幻莫测 但其整个攻击过程也具有一定规律 一般可以分为“攻击五部曲”：隐藏IP、踩点扫描、获得特权、种植后门、隐身退出

黑客根据实际情况变化也可能进行调整 掌握黑客攻击规律有助于进行有针对性的防范 网络情况复杂 黑客个性各异 其攻击流程也不尽完全相同 这5个攻击步骤是对一般情况而言的 是绝大部分黑客在通常情况下的一般规律

黑客攻击常用的方法

黑客常用的方法有以下几种：

端口扫描

端口扫描往往也成为黑客发现获得主机信息的一种最佳途径。

网络监听

网络监听工具Sniffer (也称嗅探器)和 NetXRay等原本是用于网络检测管理的工具，主要是分析网络的流量，以便找出所关注网络中潜在的问题。但也可以被黑客用于窃听网络，因此也属于一种攻击手段。

网络嗅探

网络嗅探就是使网络接口接收不属于本主机的数据。通常账户和密码等信息都以明文的形式在以太网上传输，一旦被黑客在杂错节点上嗅探到，用户就可能会遭到损害。

网络监听的概念及原理

网络监听工具是利用计算机的网络接口截获目的地为其他计算机的数据报文的一种工具 可以作为能够捕捉网络报文的设备 也可以被理解为一种安装在计算机上的监听设备 可以用于监听计算机在网络上所产生的多种信息

网络监听的检测

网络监听的威胁

网络监听能够捕获密码 这大概是绝大多数人非法使用监听工具的理由 网络监听还能够捕获专用的或者机密的信息

网络监听的检测方法

在Linux 下对嗅探攻击的程序检测方法比较简单 一般只要检查网卡是否处于混杂模式就可以了；而在Windows 平台中 并没有现成的函数可供实现这个功能 只要可以执行程序检查一下是否有嗅探程序在运行即可 (c:\windows\Drwatson.exe)

网络嗅探的防范对象

对于网络嗅探攻击 可以采取以下一些措施进行防范

- (1) 网络分段
- (2) 加密
- (3) 一次性密码技术

特洛伊木马的攻击原理

特洛伊木马是指隐藏在正常程序中的一段具有特殊功能的恶意代码 是具备破坏和删除文件、发送密码、记录键盘和攻击Dos等特殊功能的后门程序

一个完整的木马系统由硬件部分、软件部分和具体连接部分组成

使用木马工具进行网络入侵 基本过程可以分为6个步骤

- (1) 配置木马
- (2) 传播木马
- (3) 运行木马
- (4) 泄露信息 收集一些服务端的软硬件信息 并通过E-mail或ICQ 等告知控制端用户
- (5) 建立连接 服务端安装木马程序 且控制端及服务端都要在线 控制端可以通过木马端口与服务端建立连接
- (6) 远程控制 通过木马程序对服务端进行远程控制

缓冲区溢出攻防

缓冲区溢出的原理

缓冲区溢出攻击是指通过往程序的缓冲区写超出其长度的内容，造成缓冲区的溢出，从而破坏程序的堆栈，使程序转而执行其他指令，以达到攻击的目的。造成缓冲区溢出的原因是没有仔细检查程序中用户输入的参数。

最常见的缓冲区溢出攻击手段是通过制造缓冲区溢出使程序运行一个用户shell，再通过shell 执行其他命令。如果该程序属于root 且有suid 权限，攻击者就获得了一个有root 权限的shell，可以对系统进行任意操作。

拒绝服务攻击与防范

拒绝服务攻击（Denial of Service，简称DoS）是指黑客利用使网站服务器充斥巨量请求和信息的手段，消耗网络带宽或系统资源，最终导致网络系统难以运行，直至瘫痪而停止提供正常的网络服务的攻击方式。

“拒绝服务”的一种攻击方式为：传送众多要求确认的信息到服务器，使服务器里充斥着大量无用的信息。所有的信息都有需回复的虚假地址，以至于当服务器试图回传时，却无法找到用户。服务器于是暂时等候，有时超过几分钟，然后再切断连接。服务器切断连接时，黑客再度传送新一批需要确认的信息，这个过程周而复始，最终导致服务器瘫痪。经常遭受攻击的主要目标包括：路由器、数据库、Web 服务器、FTP 服务器和与协议相关的服务。

DDoS攻击防范

分布式拒绝服务攻击(DDoS)是目前黑客经常采用而难以防范的攻击手段。分布式拒绝服务攻击手段DDoS是通过网络进行的多对一的攻击方式。

DDoS 攻击实例——目前最流行的DDoS 攻击手段SYN Flood 攻击。

防范攻击的措施与步骤

防范攻击的措施

1. 提高防范意识
2. 设置安全口令
3. 实施存取控制
4. 加密及认证
5. 定期分析系统日志
6. 完善服务器系统安全性能
7. 进行动态站点监控
8. 安全管理检测
9. 做好数据备份
10. 使用防火墙和防毒软件

防范攻击的步骤

1. 选好操作系统
2. 补丁升级
3. 关闭无用的服务和端口
4. 隐藏IP 地址
5. 查找本机漏洞
6. 选用防火墙软件

入侵检测系统的概念与功能

入侵检测系统（Intrusion Detection System IDS）是进行入侵检测监控和分析过程自动化的软件与硬件的组合系统 它处于防火墙之后对网络活动进行实时检测 入侵检测技术IDS是一种主动保护自己免受攻击的一种网络安全技术

入侵检测系统主要功能包括6个方面：

- (1) 监视、分析用户及系统活动；
- (2) 系统构造和弱点的审计；
- (3) 识别反映已知进攻的活动模式并向相关人员报警；
- (4) 异常行为模式的统计分析；

(5) 评估重要系统和数据文件的完整性；

(6) 操作系统的审计跟踪管理 并识别用户违反安全策略的行为

入侵检测系统的组成及特点

入侵检测系统组成

通常IDS由传感器（Sensor）与控制台（Console）两部分组成

传感器主要包括事件发生器、事件分析器和事件数据库等 负责采集数据（网络包、系统日志等）、分析数据并生成安全事件

控制台包括发现入侵、响应单元和作出相应等部件/模块 主要起到中央管理的作用 商品化的IDS通常提供图形界面的控制台

入侵检测系统的特点

入侵检测技术是动态安全技术的最核心技术之一 入侵检测被认为是防火墙之后的第二道安全闸门 提供对内部攻击、外部攻击和误操作的实时保护

信息系统测评

为什么要进行系统测评

政策要求

信息安全等级保护管理办法（公通字[2007]43号）第十四条：信息系统建设完成后，运营、使用单位或者其主管部门应当选择符合本办法规定条件的测评机构，依据《信息系统安全等级保护测评要求》等技术标准，定期对信息系统安全等级状况开展等级测评。

中央财政资金电子政务建设项目建设单位向审批部门提出项目竣工验收申请时，要提供备案证明、测评报告风、险评估报告。（发改高技[2008]:2071号）

内部需求

确定当前安全保护能力水平。

找出差距，为后续工作提供依据。

等级保护测评职责分工

国家信息安全等级保护协调小组办公室负责隶属国家信息安全职能部门和重点行业测评机构受理；各省等保办负责本省测评机构的受理；公安部信息安全等级保护评估中心负责测评机构的能力评估和培训。

等级保护测评机构业务职能

国字头、职能部门测评机构可在全国范围内开展业务，到地方时应提前告知属地等保办；行业测评机构原则上是开展本行业测评，到地方时，应与属地省级等保办协调；地方测评机构原则上是在本地开展测评，也可到异地开展测评工作，但需提前与当地等保办协调。

等级保护测评机构的业务范围

可以开展的业务：包括等级保护测评和等级保护整改方案的设计。

不允许开展的业务：包括生产安全产品和承担安全项目的集成、实施。

系统等级组合差异

安全等级信息系统保护要求的组合第一级S1A1G1第二级

S1A2G2，S2A2G2，S2A1G2第三级S1A3G3，S2A3G3，S3A3G3，S3A2G3，S3A1G3第四级

S1A4G4，S2A4G4，S3A4G4，S4A4G4，S4A3G4，S4A2G4，S4A1G4注：

业务信息安全类（S）

系统服务保障类（A）

通用安全保护类（G）

等级保护测评相关标准

相关标准主要有：

《信息系统安全等级保护基本要求》

《信息系统安全等级保护测评要求》

《信息系统安全等级保护测评过程指南》

等级保护基本要求

安全要求类层面一级二级三级四级技术要求物理安全9193233网络
安全9183332主机安全6193236应用安全7193136数据
安全及备份恢复24811管理要求安全管理制度371114安全管理机构
492020人员安全管理7111618系统建设管理20284548系
统运维管理18416270合计/85175290318级差//9011528

等级保护基本要求的核心

等级保护基本要求的核心是安全保护能力，即需要达到的基本安全状态。等级保护测评的重点就是信息系统的安全保护能力。安全保护能力可分为恢复能力和对抗能力。

安全保护能力要求

第一级安全保护能力(自主)

经过安全建设整改，信息系统能够抵御一般性的攻击，具有防范常见的计算机病毒和恶意代码危害的能力；系统遭到破坏后，还可以恢复系统的主要功能。

第二级安全保护能力（指导）

经过安全建设整改，信息系统具有抵御小规模、强度较弱的恶意攻击的能力，防范一般性计算机病毒和恶意代码危害的能力，抵御一般的自然灾害的能力，检测常见的攻击行为并对安全事件进行记录的能力。系统遭到破坏后，还可以恢复系统的正常运行状态。

第三级安全保护能力（监督）

经过安全建设整改，信息系统在统一的安全保护策略下具有抵御大规模、较强恶意攻击的能力，防范计算机病毒和恶意代码危害的能力，抵御较为严重的自然灾害的能力，对系统资源、用户、安全机制等进行集中控管的能力，检测、发现、报警、记录入侵行为的能力，对安全事件进行响应处置并能够追踪安全责任的能力。在系统遭到破坏后，还可以较快地恢复正常地运行状态。对于服务保障性要求高的系统，能够快速恢复正常的运行状态。

等级保护测评内容

单元测评：包括测评指标（依照基本要求）、测评实施（描述测评过程中使用的具体测评方法、涉及的测评对象）、结果判定（分为符合、不符合、部分符合、不适用）。

整体测评：是在单元测评的基础上，通过进一步分析信息系统的整体安全性，对信息系统实施的综合安全测评

等级保护测评方法

基本测评方法有以下三种：

访谈（Interview）：是通过引导信息系统相关人员进行有目的的或有针对性的交流以帮助测评人员理解、分析或取得证据的过程，从而了解信息系统的全局性。

检查（Examine）：对文档、机制、设备等进行检查，包括评审、核查、审查、观察、研究和分析等方式。

测试（Test）：借助特定工具，如扫描检测工具、攻击工具、渗透工具、网络协议分析仪等，对机制和设备进行测试，包括功能/性能测试、渗透测试等。

基础篇

计算机基础

电子计算机的发展历程

第1代：电子管数字机（1946—1958年）

世界上第一台电脑硬件方面 逻辑元件采用的是真空电子管 主存储器采用汞延迟线、阴极射线示波管静电存储器、磁鼓、磁芯；外存储器采用的是磁带 软件方面采用的是机器语言、汇编语言 应用领域以军事和科学计算为主

特点是体积大、功耗高、可靠性差、速度慢（一般为每秒数千次至数万次）、价格昂贵 但为以后的计算机发展奠定了基础

第2代：晶体管数字机（1958—1964年）

硬件方的操作系统、高级语言及其编译程序 应用领域以科学计算和事务处理为主 并开始进入工业控制领域

特点是体积缩小、能耗降低、可靠性提高、运算速度提高（一般为每秒数10万次 可高达300万次）、性能比第1代计算机有很大的提高

第3代：集成电路数字机（1964—1970年）

硬件方面 逻辑元件采用中、小规模集成电路（MSI、SSI）主存储器仍采用磁芯 软件方面出现了分时操作系统以及结构化、规模化程序设计方法

特点是速度更快（一般为每秒数百万次至数千万次）而且可靠性有了显著提高 价格进一步下降 产品走向了通用化、系列化和标准化等 应用领域开始进入文字处理和图形图像处理领域

第4代：大规模集成电路机（1970年至今）

硬件方面 逻辑元件采用大规模和超大规模集成电路（LSI和VLSI）软件方面出现了数据库管理系统、网络管理系统和面向对象语言等

1971年世界上第一台微处理器在美国硅谷诞生 开创了微型计算机的新时代 应用领域从科学计算、事务管理、过程控制逐步走向家庭

计算机的类型

计算机是一种能够按照事先存储的程序 自动、高速地进行大量数值计算和各种信息处理的现代化智能电子设备 计算机传统上分为三类：

大型主机：一般为高性能的并行处理系统 存储容量大事物处理能力强可为众多用户提供服务

小型机：具有一定的数据处理能力提供一定用户规模的信息服务作为部门的信息服务中心

微型机：一般指在办公室或家庭的桌面或可移动的计算系统体积小价格低具有工业化标准体系结构兼容性好

现在大致分为以下五大类：

超级计算机：通常是指由数百数千甚至更多的处理器（机）组成的、能计算普通PC机和服务器不能完成的大型复杂课题的计算机 超级计算机是计算机中功能最强、运算速度最快、存储容量最大的一类计算机 是国家科技发展水平和综合国力的重要标志

网络计算机：包括服务器、工作站、集线器、交换机和路由器等

工业控制：主要类别有IPC（PC总线工业电脑）、PLC（可编程控制系统）、DCS（分散型控制系统）、FCS（现场总线系统）及CNC（数控系统）五种

个人电脑：包括台式机、电脑一体机、笔记本电脑、掌上电脑和平板电脑

嵌入式系统：是一种以应用为中心、以微处理器为基础 软硬件可裁剪的 适应应用系统对功能、可靠性、成本、体积、功耗等综合性严格要求的专用计算机系统

计算机的特点及应用领域

计算机大致有以下五大特点：

运算速度快、精度高 现在普通的微机每秒可执行几十万条指令 而巨型机则可达每秒几十亿次甚至几百亿次 随着科技发展 此速度仍在提高

具有存储与记忆能力 计算机的存储器类似于人的大脑 可以“记忆”（存储）大量的数据和计算机程序

具有逻辑判断能力 具有可靠逻辑判断能力是计算机能实现信息处理自动化的重要原因 能进行逻辑判断 使计算机不仅能对数值数据进行计算 也能对非数值数据进行处理 使其应用于如信息检索、图形识别以及各种多媒体应用领域等

自动化程度高 利用计算机解决问题时 人们启动计算机输入编制好的程序以后 计算机可以自动执行 一般不需要人直接干预运算、处理和控制过程

具有很高的计算精确度

在科学的研究和工程设计中 对计算的结果精确度有很高的要求 一般的计算工具只能达到几位数字 而计算机对数据处理结果精确度可达到十几位、几十位有效数字 根据需要甚至可达到任意的精度 由于计算机采用二进制表示数据 因此其精确度主要取决于计算机的字长 字越长 有效位数越多 精确度也越高

计算机应用领域：

计算机应用分为数值计算和非数值应用两大领域 数值应用主要指科学研究和工程设计应用；非数值

应用包括数据处理、知识处理 例如信息系统、工厂自动化、办公室自动化、家庭自动化、专家系统、模式识别、机器翻译等领域

软件

软件（中国大陆及香港用语 台湾称作软体 英文：Software）是一系列按照特定顺序组织的计算机数据和指令的集合 国家标准中对软件的定义为：与计算机系统操作有关的计算机程序、规程、规则以及可能有的文件、文档及数据 简单来说软件就是程序加文档的集合体 一般来讲软件被划分为系统软件、应用软件和介于这两者之间的中间件 软件是用户与硬件之间的接口界面 用户主要是通过软件与计算机进行交流

软件开发

软件开发是根据用户要求建造出软件系统或者系统中的软件部分的过程 它包括需求捕捉、需求分析、设计、实现和测试 需求捕捉是与用户沟通获取用户的需求信息的过程；需求分析是对用户的需求信息进行过滤 去粗取精 去伪求真 准确找出用户的真正需求 然后把它用需求规格说明书表达出来的过程 设计分为概要设计和详细设计两个阶段 概要设计的主要任务是给出软件的模块结构 用软件结构图表示；详细设计的主要任务是设计模块的程序流程、算法、数据结构及数据库设计 实现是把设计的模块转换成计算机可以接受的程序 即以源代码实现功能 测试是在规定的条件下对程序进行操作 以发现程序错误和漏洞 并对其是否能满足设计要求进行评估的过程 简单来说 软件开发就是一系列最终构建出软件产品的活动

程序设计语言

程序设计语言是用于书写计算机程序而人为设计的符号语言 用于对计算进行描述、组织和推导 语言的基础是一组记号和一组规则 根据规则将记号构成的记号串的集合就是语言 在程序设计语言中 这些记号串就是程序

程序设计语言为程序员写出一个好的程序提供了所需的抽象机制、组织原则以及控制结构 常用的程序设计语言有C语言、C++、Java、Python、PHP、VB等 根据其特点不同使用情况也不同 例如 PHP专门用来显示网页 C语言被广泛用于操作系统和编译器的开发

语言处理程序

语言处理程序是为用户设计的编程服务软件 其作用是将高级语言源程序翻译成计算机能识别的目标程序 以便计算机能够运行

语言处理程序一般是由汇编程序、编译程序、解释程序和相应的操作程序等组成 汇编程序的任务是将汇编语言编写的源程序翻译成机器指令程序 编译程序（也称编译器）的任务是将源程序编译成目标语言程序 解释程序（也称解释器）有两种 一种是直接解释执行源程序的解释程序 另一种是将源程序翻译成某种中间代码再执行的解释程序

计算机程序的执行过程

程序是由指令组成的 指令是机器所能识别的一组特定格式的代码串 它要求机器在一个规定的时间段即一个指令周期内 完成一组特定的操作 计算机程序的工作过程为：取指令 分析指令 执行指令 再取下一条指令 循环执行此过程 直到程序结束

以下介绍第一条指令的执行过程 程序执行过程即循环第一条指令的执行过程

取指令阶段：

将程序计数器PC的内容（00H）送至地址寄存器AR 记为PC AR

程序计数器PC的内容自动加1变为01H 为取下一个指令字节作准备 记为PC+1 PC

地址寄存器AR将00H通过地址总线送至存储器 经地址译码器译码 选中00号单元 记为AR M

CPU发出"读"命令

所选中的00号单元的内容B0H读至数据总线DB 记为（00H）DB

经数据总线DB 将读出的B0H送至数据寄存器 记为DB DR

数据寄存器DR将其内容送至指令寄存器IR 经过译码 控制逻辑发出招待该条指令的一系列控制信号 记为DR IR IR ID、PLA 经过译码 CPU"识别"出这个操作码就是MOV A 03指令 于是 它"通知"控制器发出执行这条指令的各种控制命令

执行指令阶段：

经过对操作码B0H译码后 CPU就"知道"这是一条把下一单元中的立即数取入累加器A的指令 所以 **执行第一条指令就必须把指令第二字节中的立即数取出来送至累加器A** 取指令第二字节的过程为：

PC AR 即将程序计数器的内容01H送至地址器AR

PC+1 PC 即将程序计数器的内容处动加1变为02H **为取下一条指令作准备**

AR M 即地址寄存器AR将01H通过地址总线送至存储器 经地址译码选中01H单元

CPU发出"读"命令

(01H) DB 即选中的01H存储单元的内容03H读至数据总线DB上

DB DR 即通过数据总线 把读出的内容03H送至数据寄存器DR

DR A 因为经过译码已经知道读出的是立即数 并要求将它送到累加器A 故数据寄存器DR通过内部数据总线将03H送至累加器A

算法

算法 (Algorithm) 是指解决方案的准确而完整的描述 在计算机中表现为指令的有序序列 并且每条指令表示一个或多个操作 **算法代表着用系统的方法描述解决问题的策略机制** 简单来说 **算法就是为了解决某个问题** 而制定了一系列步骤

算法的基本要素

数据对象的运算和操作：计算机可以执行的基本操作是以指令的形式描述的一个计算机系统能执行的所有指令的集合 成为该计算机系统的指令系统 一个计算机对数据对象的基本运算和操作有如下四类：

算术运算：加、减、乘、除等运算

逻辑运算：与、或、非等运算

关系运算：大于、小于、等于、大于等于、小于等于等运算

数据传输：输入、输出等运算

算法的控制结构：一个算法的功能结构不仅取决于所选用的操作 而且还与各操作之间的执行顺序有关 **算法的控制结构给出了算法的框架** 决定了各操作的执行顺序 算法的控制结构有顺序结构、选择结构、循环结构

数据结构的逻辑结构

数据的逻辑结构指的是反映数据元素之间的逻辑关系的数据结构 逻辑结构包括：

集合结构：数据结构中的元素之间除了“同属一个集合”的相互关系外 别无其他关系 即集合结构里面的元素关系是孤立的；

线性结构：数据结构中的元素存在一对一的相互关系；

树形结构：数据结构中的元素存在一对多的相互关系；

图形结构：数据结构中的元素存在多对多的相互关系

数据结构的存储结构

数据的存储结构指的是数据的逻辑结构在计算机中的存储形式 存储结构有两种：

顺序存储结构：把数据元素存放在地址连续的存储单元里 其数据间的逻辑关系和物理关系是一致的

链式存储结构：把数据元素存放在任意的存储单元里 这组存储单元可以是连续的 也可以是不连续的

操作系统

什么是操作系统？

操作系统 (Operating System 缩写：OS) 是管理计算机硬件与软件资源的计算机程序 为计算机程序提供公共服务 操作系统需要处理各种事务 如决定系统资源供需的优先次序、控制输入与输出设备、操作网络与管理文件系统、管理与配置内存等基本事务 操作系统提供一个让用户与系统交互的操作界面

现在主流的操作系统有哪些？

DOS系统

磁盘操作系统 (Disk Operating System , 缩写：DOS) 是一个基于磁盘管理的操作系统。 DOS系统靠输入命令来进行人机交互，通过命令的形式把指令传给计算机，以实现各种操作。

Windows系统

Microsoft Windows是美国微软公司研发的一套操作系统，于1985年推出。Windows采用图形化模式GUI，比起从前的需要以命令实现各种操作的DOS系统更为人性化，操作更便捷。

Unix / Linux 操作系统

UNIX操作系统是一个强大的多用户、多任务的操作系统，支持多种处理器架构。最早由KenThompson、Dennis Ritchie和Douglas McIlroy于1969年在AT&T的贝尔实验室开发。

Linux是一套完全免费的类Unix操作系统，是一个以POSIX和UNIX为基础的，多任务、多用户、多CPU、支持多线程的操作系统。Linux同Unix一样以网络为核心，是一个性能稳定的多用户网络操作系统。

苹果Mac OS系统

Mac OS是一套运行于苹果Macintosh系列电脑上的操作系统。Mac OS是首个在商用领域成功的图形用户界面操作系统。Mac系统是基于Unix内核的图形化操作系统，由苹果公司自行开发。

Windows操作系统的简介

Microsoft Windows是美国微软公司研发的一套操作系统，它问世于1985年，起初仅仅是Microsoft-DOS模拟环境，后续的系统版本由于微软不断的更新升级，不但易用，也慢慢的成为家家户户人们最喜爱的操作系统。

Windows采用了图形化模式GUI，比起从前的DOS需要键入指令使用的方式更为人性化。随着电脑硬件和软件的不断升级，微软的Windows也在不断升级，从架构的16位、16+32位混合版（Windows9x）、32位再到64位，系统版本从最初的Windows 1.0到大家熟知的Windows 95、Windows 98、Windows ME、Windows 2000、Windows 2003、Windows XP、Windows Vista、Windows 7、Windows 8、Windows 8.1、Windows 10和Windows Server服务器企业级操作系统，不断持续更新，微软一直在致力于Windows操作系统的开发和完善。现在最新的正式版本是Windows 10。

Windows操作系统有哪些特点？

直观、高效的图形用户界面：Windows采用了图形化模式GUI，操作简单，容易使用。

用户界面统一：Windows应用程序大多符合IBM公司提出的CUA (Common User Access)标准，所有的程序拥有相同或相似的外观，用户学会了一个软件的操作使用，就很容易学会其他软件。

丰富的设备无关的图形操作：提供丰富的图形操作函数，可以绘制出各种几何图形，如线、圆、矩形等，支持各种输出设备，并且在不同设备上可以显示相同的效果。

多任务：允许用户同时运行多个应用程序，或在一个程序中同时做几件事情。

Unix操作系统的简介

UNIX操作系统是一个强大的多用户、多任务操作系统，支持多种处理器架构，按照操作系统的分类属于分时操作系统。1969年，UNIX的第一版在AT&T的贝尔实验室产生，其前身是MULTICS（多路存取计算机系统）。1975年，AT&T开始向商业和政府用户提供许可证，是第一个在贝尔实验室以外广泛流传的UNIX系统。70年代中期，加州大学伯克利分校及其他大学也开发了相应的UNIX版本，称为BSD UNIX，其增加了Vi编辑器、c shell等。1983年，贝尔实验室发布第一个商业版本的UNIX系统V的版本1，即SVR1。UNIX操作系统由三部分组成：内核、shell和工具及应用程序。内核为UNIX操作系统的核心，指挥调度UNIX机器的运行，直接控制计算机的资源；shell为UNIX内核和用户的接口，是UNIX的命令解释器，也是一种解释性高级语言；UNIX提供了很多工具软件 and 应用程序供用户使用，如vi编辑器、文件查找等等。

Unix操作系统有哪些特点？

UNIX系统是一个多用户、多任务的分时操作系统。

UNIX系统源代码大部分是由C语言编写的，使得系统易读，易修改，易移植。

UNIX系统提供了丰富的、精心挑选的系统调用，整个系统的实现十分紧凑，简洁。

UNIX系统提供了功能强大的可编程的Shell语言（外壳语言）作为用户界面，具有简洁、高效的特点。

UNIX系统采用树状目录结构，具有良好的安全性、保密性和可维护性。

UNIX系统采用进程对换的内存管理机制和请求调页的存储方式，实现了虚拟内存管理，大大提高了

内存的使用效率。

UNIX系统提供多种通信机制，如：管道通信，软中断通信，消息通信，共享存储器通信，信号灯通信。

UNIX系统网络功能强，作为Internet网络技术基础的TCP/IP协议就是在UNIX上开发出来的。UNIX系统是Internet上各种服务器的首选操作系统。

UNIX系统对各种数据库，特别是关系型数据库管理系统提供了强大的支持能力。

macOS操作系统的介绍

macOS 是一套由苹果公司自行开发的运行于苹果 Macintosh 系列电脑上的操作系统。Mac系统是基于Unix内核的图形化操作系统，简单易用且功能强大，一般情况下在普通PC上无法安装。现行的最新的系统版本是macOS 10.14，且网上也有在PC上运行的Mac系统，简称 Mac PC。

另外，疯狂肆虐的电脑病毒几乎都是针对Windows的，由于MAC的架构与Windows不同，而且用户比较少，所以很少受到病毒的袭击。

macOS可以被分成操作系统的两个系列：（1）老旧且已不被支持的“Classic” macOS，它是一个100%的图形操作系统，完全没有命令行模式。但是它几乎没有内存管理、协同式多任务和对扩展冲突敏感。（2）新的macOSX，它结合BSD Unix、OpenStep和Mac OS 9的元素，它以Unix为基础，其代码被称为Darwin，实行的是部分开放源代码。

macOS操作系统有哪些特点

全屏模式：一切应用程序均可以在全屏模式下运行，减少多个窗口带来的困扰。

任务控制：整合了Dock和控制面板，并可以窗口和全屏模式查看各种应用。

快速启动面板：其工作方式与iPad完全相同，它以类似于iPad的用户界面显示电脑中安装的一切应用，并通过App Store进行管理。

应用商店：当用户从应用商店购买一个应用后，Mac电脑会自动将它安装到快速启动面板中，使用户无需对应用进行管理。

Office办公软件的简单介绍

Microsoft Office是一套由微软公司开发的办公软件套装 它为 Microsoft Windows 和 Mac OS X而开发 常用组件有 Word、Excel、Power point等 **最新版本为Office 365(Office 2019)**

该软件最初出现于九十年代早期 最初是一个推广名称 指一些以前曾单独发售的软件的合集 当时主要的推广重点是购买合集比单独购买要省很多钱 最初的 Office 版本只有 Word、Excel 和 Power point；另外一个专业版包含 Microsoft Access；经过不断发展 **Office 应用程序逐渐整合** 共享一些特性 例如拼写和语法检查、OLE 数据整合和微软 Microsoft VBA（Visual Basic for Applications）脚本语言

Office的组成及用途

Office由以下软件组成：

Microsoft Office Word

Microsoft Office Word 是文字处理软件 给用户提供了用于创建专业而优雅的文档工具 帮助用户节省时间 并得到优雅美观的结果 Word 提供了许多易于使用的文档创建工具 同时也提供了丰富的功能集 供创建复杂的文档使用

Microsoft Office Excel

Microsoft Office Excel 是电子数据表程序 方便用户制作出各种电子表格 使用公式和函数对数据进行复杂的运算；利用各种图表来表示数据直观明了；利用超级链接功能 用户可以快速打开局域网或 Internet 上的文件 与世界上任何位置的互联网用户共享工作簿文件

Microsoft Office PowerPoint

Microsoft Office PowerPoint 是微软公司设计的演示文稿软件 用户不仅可以在投影仪或者计算机上进行演示 也可以将演示文稿打印出来 制作成胶片 以便应用到更广泛的领域中 利用 Powerpoint 不仅可以创建演示文稿 还可以在互联网上召开面对面会议、远程会议或在网上给观众展示演示文稿

Microsoft Office Outlook

Microsoft Office Outlook是个人信息管理程序和电子邮件通信软件 可以用它来收发电子邮件、管理联系人信息、记日记、安排日程、分配任务

Microsoft Office FrontPage

Microsoft Office FrontPage是微软公司推出的一款网页设计、制作、发布、管理的软件 集成了编辑、代码、预览三种模式于一身 能够与Microsoft Office各软件无缝连接 具有良好的表格控制能力 还继承了Microsoft Office产品系列的良好易用性 它提供数据库接口向导功能可以替用户产生在线数据库所需要的一切功能 包含数据库的建立、窗体以及所需的各种页面 此外 FrontPage 2002还允许用户设定数据库的交互功能 利用该功能 用户可以设置让指定的访问者通过浏览器来编辑数据库中的记录 或者在数据库中新增记录 查看已有的资料等

Microsoft Office Onenote

Microsoft Office OneNote是一套用于自由形式的信息获取以及多用户协作工具 使用户能够捕获、组织和重用便携式计算机、台式计算机或Tablet PC上的便笺 **为用户提供了一个存储所有便笺的位置** 并允许用户自由处理这些便笺 OneNote 2003还帮助用户以多种方式捕获信息 **然后根据需要组织和使用它**

Microsoft Office Access

Microsoft Office Access是由微软发布的关联式数据库管理系统 它可以用来进行数据分析 利用access的查询功能 可以方便地进行各类汇总、平均等统计 并可灵活设置统计的条件 它还可以用来开发软件 其最大的优点是易学 非计算机专业的人员 也能学会 低成本地满足了那些从事企业管理工作的人员的管理需要 通过软件来规范同事、下属的行为 推行其管理思想 此外 它还可以存储数据 可处理字段、关系和规则的复杂计算 可创建和运行旧数据库

Microsoft Office Publisher

Microsoft Office Publisher是微软公司发行的桌面出版应用软件 它可以提供比Microsoft Word更强大的页面元素控制功能 但比起专业的页面布局软件 比如说Adobe公司的InDesign以及Quark公司的Quark XPress来还略逊一筹 Publisher的大部份替代品 除Adobe PageMaker外 都不提供导入Publisher的功能 ; 但是 Publisher可以导出成 EMF (Enhanced Meta file)格式 它可以被其它软件支持

Microsoft Visio

Microsoft Visio是Windows操作系统下运行的流程图和矢量绘图软件 负责绘制流程图和示意图 帮助用户创建具有专业外观的图表 以便理解、记录和分析信息、数据、系统和过程

Microsoft Office Picture Manager

Microsoft Office Picture Manager是一个基本的图片管理软件 使用 Picture Manager 用户可以一次性处理多张图片 也可以每次只编辑一张图片 并且可以对图片进行编辑

Microsoft Photo Draw

Microsoft Photo Draw是一个简单易用的程序 它独一无二地提供了照片或图形编辑和实例来帮助 Microsoft Office 和小商业用户在PowerPoint、Word、Publisher和Web中创建自定义外观的照片或图形 PhotoDraw包括了专业设计模板、预设的默认设置和自动更正功能

Microsoft Project

Microsoft Project是专案管理软件程序 该程序协助项目经理发展计划、为任务分配资源、跟踪进度、管理预算和分析工作量

Microsoft SharePoint Designer

Microsoft SharePoint Designer 2007是Frontpage 2003的下一个版本 它提供了多种专业工具 利用这些工具 用户在 SharePoint 平台上无需编写代码即可生成交互解决方案、设计自定义 SharePoint 网站以及使用报告和托管权限维护网站性能

Microsoft InfoPath

Microsoft InfoPath是用来开发XML为本用户表格的应用程序 它可透过MSXML与SOAP工具包利用XML Web Services连接到外部系统 并且后端和中间层系统可设定来利用Web Services标准如SOAP UDDI 以及WSDL来沟通 另外 因为InfoPath文件是基于XML的 它可从外部数据库资源调用资料绑定到表格控制元件而非InfoPath本身

Lync

Microsoft Lync是一个配合Microsoft Lync Server一同使用 又随同Office 365与Live@EduLync Online附送的即时通信客户端 Lync在相同的用户界面和后台架构中提供了企业语音、即时通信和web/音频/视频会议等工具 新增了即时动态、通讯录名片变更和720p高清视频通话

Office 助手

Office助手是从Office 97开始具有的新功能 至Office 2003 都有Office 助手 这个特性是提供不同的搜索功能的程序帮助系统的入口

什么是WPS？

WPS Office是由金山软件股份有限公司自主研发的一款办公软件套装 可以实现办公软件最常用的文字、表格、演示等多种功能 具有内存占用低、运行速度快、体积小巧、强大插件平台支持、免费提供海量在线存储空间及文档模板

WPS与Office区别在哪里？

在开发者方面，Office是微软公司开发的软件，采用统一的风格；WPS是中国金山公司开发的办公软件，外观设计、UI设计更符合国人的使用习惯。

在收费方面，Office是收费的，WPS具有免费版和收费版。

在大小方面，Office大概在1G左右，而WPS只有几十兆，占用空间很小。

在功能方面，Office功能较强大，具有多种组件，比如Word、Excel、Powerpoint、Access、FrontPage、Outlook等，而WPS只提供Word、Excel、Powerpoint这三种常用的组件。

在适用范围方面，Office更职业化，适合工作使用，而WPS适合在家庭使用。

Windows操作系统的常用快捷方式

基础快捷键：

Ctrl+C (Ctrl+Insert)：复制选中项目

Ctrl+X：剪切选中项目

Ctrl+V (Shift+Insert)：粘贴选中项目

Ctrl+Z：撤销

Ctrl+Y：重做

Delete (Ctrl+D)：删除选中项目至回收站

Shift+Delete：直接删除选中项目

Ctrl+A：全选

Win键相关的快捷键：

Windows徽标：“开始”菜单

Windows徽标+D：显示桌面

Windows徽标+M：最小化窗口

Windows徽标+E：开启资源管理器

Windows徽标+F：查找文件或文件夹 查找文件目录 在硬盘内查找文件

Windows徽标+F1：启动系统帮助程序

Windows徽标+R：启动运行对话框

SHIFT+Windows 徽标+M：撤消全部最小化

CTRL+Windows 徽标+F：查找计算机

CTRL+Windows 徽标+TAB：将焦点从“开始”菜单移动到“快速启动”工具栏或系统任务栏（使用右箭头键或左箭头键可将焦点移动到“快速启动”工具栏和系统任务栏中的项目）

Windows 徽标+TAB：在任务栏按钮之间循环

Windows 徽标+Break：“系统属性”对话框

Windows操作系统使用时的注意事项

定期清理注册表

电脑中的注册表是电脑最重要的组成部分之一，但有不少注册表对使用电脑是有害的，所以必须定期清理一下，在清理之前做好备份，防止出现误删除有用的注册表。

更新杀毒软件

Windows系统中电脑的杀毒软件是必须装备的，而且要定期的更新，更新杀毒软件能更有效的保护电脑，对账户安全也是必要的。

少用管理员账户登录

windows可以支持多用户使用，在油外部的硬盘和U盘访问计算机的时候最好不要使用管理员账户登录，这样可以降低电脑被病毒入侵的几率。

不随意安装软件

在上网的时候常会有很多的恶意软件，所以对来历不明的软件一定不要随意安装，对一些没把握的软件，可以上网先搜一下看是否是病毒类软件。

整理磁盘

磁盘是电脑的重要组成部分，在电脑使用久了以后磁盘中会有很多碎片，这严重影响电脑的运行速度，所以定期整理磁盘是很有必要的。

定期清理垃圾文件

电脑在上网和使用的过程中会产生很多无用的垃圾文件，这些文件会严重占用电脑的内存空间，所以需要定期的清理垃圾文件。

数据库

什么是数据库？

数据库（Database）是以一定方式储存在一起、能与多个用户共享、具有尽可能小的冗余度、与应用程序彼此独立的数据集合 简单来说 **数据库是按照数据结构来组织、存储和管理数据的仓库** 形象化来说 **数据库可以看做电子化的文件柜 是存储电子文件的处所 用户可以对文件中的数据进行新增、截取、更新、删除等操作**

为什么需要使用数据库？

在日常工作中会产生大量数据，我们常常需要把这些数据放进一个专门管理它们的“仓库”里，并根据管理的需要对其进行相应的处理。而且，随着数据的不断增多，存储空间增大、无效数据增多、查询效率变低的问题日益凸显。而数据库的出现有效地解决了这些问题，使用数据库可以减少数据冗余度，从而大大节省了数据的存储空间。此外，使用数据库可以对成千上万数据进行批量处理，提高查询效率与管理质量。

关系型数据库

关系数据库（Relational Database）是建立在关系模型基础上的数据库 借助于集合代数等数学概念和方法来处理数据库中的数据 关系模型就是指二维表格模型 关系型数据库中的表格为二维行列表格 表格之间具有关联关系 彼此之间可通过某一元素相互联接起来 简单来说 关系型数据库就是由二维表及其之间的联系组成的一个数据组织 在关系型数据库的基础上 美国国家标准局ANSI确立了标准数据查询语言SQL（Structured Query Language）用于对关系型数据库中的数据进行存储、查询、更新等操作 当前主流的关系型数据库有Oracle、DB2、PostgreSQL、Microsoft SQL Server、Microsoft Access、MySQL、浪潮K-DB等

非关系型数据库

非关系型数据库 又被称为NoSQL（Not Only SQL）顾名思义 不仅仅是SQL 随着互联网web 2.0网站的兴起 数据集合规模急剧增大、数据种类增多等多重性问题接踵而来 为了解决大规模数据集合多重数据种类带来的挑战 尤其是大数据应用难题 非关系型数据库迅速发展

NoSQL存储的是大量结构化数据 根据存储结构及应用场合的不同 主要可以将NoSQL分为以下几类：
键值(Key-Value)存储数据库

这类数据库主要会使用到一个哈希表 该表中有一个特定的键和一个指针指向特定的数据 其优势在于简单、易部署 **该类数据库主要有：Redis Voldemort Oracle BDB Amazon's Dynamo**

列（Column-Oriented）存储数据库

该类数据库存储结构为列式结构 这种结构会让很多统计聚合操作更简单方便 使系统具有较高的可扩展性 该类数据库主要有：HBase Cassandra Hypertable BigTable

文档（Document）型数据库

该类数据库的存储结构与键值存储非常相似 也是每个Key分别对应一个Value但是这个value是以文档形式存储 该类数据库主要有：CouchDB MongoDB

图形(Graph)数据库

该类数据库使用图形模式 虽然使存储更为灵活 但也使其变得更为复杂 当数据之间是紧密联系的 使

用图形数据库是最好的选择 该类数据库主要有：Neo4J InfoGrid Infinite Graph

Oracle 数据库

Oracle Database 又名Oracle RDBMS 或简称Oracle 是美国ORACLE公司（甲骨文）推出的一种关系型数据库管理系统 是目前世界最流行的关系型数据库之一 该数据库系统可移植性好、使用方便、功能强大 效率高、可靠性好 适用于各类大、中、小、微机环境 Oracle数据库的适应性好 只要在一种机型上学习了Oracle数据库的所有知识 在其他机型上也同样可以使用 Oracle数据库最新版本为Oracle Database 12c

Oracle数据库逻辑存储结构由至少一个表空间和数据库模式对象组成 模式为对象的集合 模式对象包括表、视图、序列、存储过程、簇等结构 其物理存储结构是由一些多种物理文件组成 主要有数据文件、日志文件、参数文件、警告文件等 此外 其强大的数据恢复功能保证了数据库内容的可靠性和正确性

SQL Server数据库

SQL Server数据库是美国Microsoft公司推出的一种关系型数据库管理系统 是一个可扩展的、高性能的、为分布式客户机/服务器计算所设计的数据库管理系统 它最初由Microsoft、Sybase 和Ashton-Tate三家公司共同开发 在Windows NT推出后 Microsoft与Sybase对于SQL Server的开发开始趋于不同的方向 Microsoft将SQL Server移植到Windows NT系统上 注重开发SQL Server的Windows NT 版本 Sybase 则更注重SQL Server在UNIX操作系统上的应用 SQL Server数据库最新版本为Microsoft SQL Server 2018 SQL Server数据库的逻辑存储结构为文件组、区、数据页 SQL Server将数据库映射成为一组文件 文件类型为主数据文件、次要数据文件和日志文件 数据与日志信息不混合存放在一个文件中 而且一个文件只由一个数据库使用

SQL Server数据库充分利用了Windows NT的优势 其系统管理先进 支持Windows图形化管理工具 支持本地和远程的系统管理和配置；SQL Server数据库具有强壮的事务处理功能 采用各种方法保证数据的完整性；此外 SQL Server数据库具有自主的SQL语言 SQL语句可以用来执行各种各样的操作 如对数据库数据进行增、删、改、查 目前 绝大多数流行的关系型数据库管理系统 如Oracle Sybase Microsoft SQL Server Access等都采用了SQL语言标准

MySQL数据库

MySQL数据库是瑞典 MySQL AB 公司推出的一种开放源代码的关系型数据库管理系统 目前属于Oracle 公司 是目前世界最流行的关系型数据库之一 MySQL数据库最新版本为MySQL 8.0 从逻辑结构看 MySQL数据库的所有数据被存放在表空间中 表空间由段、区、页组成 存储结构采用B树结构 从物理结构看 MySQL数据库由共享表空间、日志文件组、表结构定义文件组成 数据库之中的每个表将独立地产生一个表空间文件 MySQL使用结构化查询语言SQL 可以运行于多种系统上 并且支持多种语言 如C C++ Python Java PHP等语言；MySQL 支持大型的数据库 支持5000万条记录的数据仓库；MySQL数据库采用GPL协议 用户可以根据需要修改其源代码 定制自己的MySQL数据库 MySQL数据库因为其速度、可靠性和适应性而备受关注 大多数人都认为在不需要事务化处理的情况下 MySQL是管理内容最好的选择

南大通用GBASE数据库

GBase 是由南大通用数据技术有限公司推出的数据库产品，目前在国内数据库市场具有较高的品牌知名度。GBase系列产品包括：分析型数据管理系统GBase 8a、大规模分布式并行数据库集群系统GBase 8a MPP Cluster、内存数据库管理系统GBase 8m等。

GBase系列数据库都具有自己鲜明的特点，GBase 8a具有独特的列存储，透明自适应压缩，智能索引等优点，在技术上体现出高性能、高性价比、高可用性；GBase 8a MPP Cluster在GBase 8a列存储的基础上经过开发，可支持TB到PB级别结构化数据存储查询，在技术上体现出高性能、高可用性、高扩展性；GBase 8m将数据存储于内存介质并加以管理，性能可以达到传统磁盘数据库性能的10倍以上，并且提供高效的数据库访问机制，极大地提高了事务并发处理能力。根据其特点不同，各数据库的应用领域也不同：GBase 8a分析型数据管理系统重点应用于海量数据分析领域；GBase 8a MPP Cluster以TB到PB级的海量数据计算规模为目标市场，重点应用于政府、军事部门、电信、金融、互联网等拥有海量业务数据的行业；GBase 8m主要应用于对于数据处理性能要求极高的领域、大规模

用户访问的领域、实时处理领域等，如电信行业的计费系统、金融行业指数分析系统等。

人大金仓数据库

北京人大金仓数据库管理系统KingbaseES，简称金仓数据库，是北京人大金仓信息技术股份有限公司自主研发开发的具有自主知识产权的通用关系型数据库管理系统，它还是入选国家自主创新产品目录的唯一数据库产品。该数据库是面向事务处理类、兼顾分析类应用领域的新数据库产品，致力于解决高并发、高可靠数据存储计算问题，是一款为企事业单位管理信息系统、业务系统量身打造的承载数据库。该数据库可保证数据不丢失、服务不中断、错误不蔓延，具有错误隔离机制，设有3种灾备解决方案，保证业务连续性；支持DB2、SQL Server、Sybase、MySQL、Excel等数据源中的数据迁移；界面体验良好。

金仓分析型数据库Kingbase Analytics DB，简称KADB，采用分布式集群部署和在线动态扩容技术、大规模并行处理（MPP）技术、无共享存储（shared-nothing）技术、行/列混合存储技术、多种压缩技术、资源负载管理技术、库内挖掘分析及安全控制技术等，具有高性能、高扩展的特点，可广泛应用于政府、军队、金融、电信等行业，满足企业对数据采集、存储、挖掘和分析的应用需求。

神通数据库

神通数据库是一款计算机数据库 分为标准版、企业版、安全版

神通数据库标准版提供了大型关系型数据库通用的功能 功能适用 稳定可靠 性价比较高 可以满足中小企业的总体需求

神通数据库企业版是天津神舟通用数据技术有限公司拥有自主知识产权的企业级、大型通用关系型数据库管理系统 它采用关系数据模型作为核心数据模型 支持SQL通用数据库查询语言 提供标准的ODBC、JDBC、OLEDB/ADO和.Net DataProvider等数据访问接口 并具有海量数据管理和大规模并发处理能力 与标准版相比 企业版功能更完备 数据库系统的稳定性、可靠性以及处理事务的效率比标准版也有所提高 可以更好的满足大型企业的业务需求

神通数据库安全版在企业版的基础上 集成多项先进安全技术 增加了高强度身份认证、基于标签的强制访问控制、数据加密存储、可信任路径、独立审计中心等关键安全特性 大大提高了系统的安全性 更好地满足了航天、政府、金融、电信等高安全性行业应用需求

达梦数据库

达梦数据库管理系统 简称DM 是达梦公司推出的具有完全自主知识产权的高性能数据库管理系统 达梦数据库管理系统的最新版本是为DM7

DM7是基于成熟的关系型数据模型和标准的接口 是一个跨越多种软硬件平台、具有大数据管理与分析能力、高效稳定的数据库管理系统 它具有以下几个特点：

通用性

达梦数据库管理系统与多种硬件系统均兼容 可运行于X86、X64、SPARC、POWER等硬件体系之上；支持多种主流操作系统 如Windows Linux Unix Kylin等；支持多种主流集成开发环境 如PowerBuilder、Delphi、Visual studio、.NET、C++Builder、Qt、Jbuilder、Eclipse、Zend Studio等；支持多种主流系统中间件 如Weblogic、Websphere、Tomcat、Jboss、东方通TongWeb、金蝶Apusic、中创InfoWeb等；支持多种数据库开发接口 包括OLE DB、ADO、ODBC、OCI、JDBC、Hibernate、PHP、PDO、DB Express以及.Net DataProvider等；系统支持多种网络协议 包括IPV4协议、IPV6协议等；完全支持Unicode、GBK18030等常用字符集

高性能

达梦数据库管理系统 支持列存储、数据压缩、物化视图；可通过表级行存储、列存储选项技术 在同一产品中提供对联机事务处理和联机分析处理业务场景的支持；支持2000个以上的高并发处理；具有对数据分区管理能力 支持对表进行范围分区、哈希分区、列表分区、垂直分区的分区机制 支持多级分区机制；支持分区并发数据处理；支持100TB级数据处理能力

高可用

可配置数据守护系统 自动快速故障恢复 具有强大的容灾处理能力；具有强大的备份、恢复机制 支持逻辑备份恢复和物理备份恢复 并且备份文件可以跨windows和linux、32位和64位等不同的操作系统平台

跨平台

支持windows、Linux、中标麒麟、银河麒麟等操作系统 支持多种主流标准接口

高可扩展

支持拓展软件包和多种工具 可实现海量数据分析处理、支持多种扩展功能

星环数据库

星环数据库是由星环信息科技（上海）有限公司推出的数据库产品，是一款优秀的国产数据库。其主要包括星环科技产品企业级一站式大数据综合平台Transwarp Data Hub、新一代智能大数据云平台Transwarp Data Cloud、分布式闪存数据库Transwarp ArgoDB、分布视图数据库Transwarp StellarDB等。

随着大数据技术在企业中应用得越来越广泛深入，用户的需求也变得越来越复杂，但传统的大数据架构并不能很好的满足这些新需求，需要用到多种架构和产品，导致平台复杂性急剧增加，系统响应时间变慢，各种成本上升。分布式闪存数据库Transwarp ArgoDB针对解决这种问题，以分布式计算引擎和分布式存储引擎，管理组件包括Transwarp Container Operating System、Transwarp Manager和Transwarp Guardian为核心，可以替代Hadoop+MPP混合架构，一站式满足企业对大数据平台的各种诉求。

分布视图数据库Transwarp StellarDB主要针对快速查找数据间的关联关系的问题，它具有强大的图算法分析能力、实时的数据查询、快速的复杂关系查找等功能，可以实现快速查询多层关系。同时，Transwarp StellarDB克服了海量关联图数据存储的难题，它具有灵活而丰富的存储模型、强大的存储容量，通过自定义图存储格式和集群化存储，实现了传统数据库无法提供的低延时多层关系查询，在社交网络、公安、金融领域都有巨大应用潜力。

计算机网络

什么是计算机网络？

计算机网络（computer networks）也称计算机通信网 广义上来说 它是利用通信线路将地理位置不同的、具有独立功能的计算机系统和通信设备按不同的形式连接起来 **以功能完善的网络软件及协议实现资源共享与信息传递的系统 最简单的计算机网络就只有两台计算机和连接它们的一条链路** 从需求来说 **计算机网络是由大量独立的、但相互连接的计算机来共同完成计算机任务的网络** 简单来说 **计算机网络就是一些相互连接的、以共享资源为目的的、自治的计算机的集合**

计算机网络拓扑结构

计算机网络的拓扑结构 **是指将计算机组成的网络之间设备的分布情况以及连接状态以图的形式表现出来** 这个图称为拓扑图 将计算机、设备及传输媒介形成的结点与线的物理连接构成模式 该结点包括两类：转接节点 用来转换和交换信息 包括交换机、集线器、终端控制器等；访问节点 包括主机、终端等 线代表各种传输媒介 包括有线和无线形式

计算机网络性能指标

速率（网速）：主机在数字通信上传送数据的速率，其单位为比特（bit）。

带宽：在计算机网络中，带宽指网络的通信线路传送数据的能力，即单位时间内从网络中的某一点到另外一个点所能通过的“最高数据率” 其单位为比特每秒（bit/s）。一条通信链路中，带宽越宽，最高数据率也越高。

吞吐量：单位时间内通过某个通信线路或接口的数据量。吞吐量受制于带宽或者网络的额定速率。

时延：数据从网络的一端发送数据帧（包含传递的数据包和一些必要的信息）到另一端所需要的时间。时延分为：发送时延、传播时延、处理时延、排队时延。总时延等于所有时延之和。

高速网络链路：提高数据的发送速率，减少数据的发送时延，但不是提高比特在链路上的传播速率。

时延带宽：时延带宽=传播时延*带宽，表示一条链路上传播的所有比特，其单位为比特（bit）。

往返时间（RTT）：从数据的发送开始，到发送方接收到来自接收方的确认信息总共经历的时延。

利用率：利用率包括信道利用率和网络利用率。信道利用率指某信道有百分之几的时间是被利用的即有数据通过。网络利用率指全网络的信道利用率的加权平均值。信道利用率或者网络利用率过高会产生非常大的时延。

计算机网络层次的划分

计算机网络的体系结构是网络协议的层次划分与各层协议的集合，同一层中的协议根据该层所要实现的功能来确定。各对等层之间的协议功能由相应的底层提供服务完成。为了使不同的计算机厂家生产的计算机能够相互通信，以便在更大的范围内建立计算机网络，国际标准化组织（ISO）在1978年提出了“开放系统互联参考”模型（Open System Interconnection/Reference Model），即著名的OSI/RM模型。它将计算机网络体系结构的通信协议划分为七层，自下而上依次为：物理层（Physics Layer）、数据链路层（Data Link Layer）、网络层（Network Layer）、运输层（Transport Layer）、会话层（Session Layer）、表示层（Presentation Layer）、应用层（Application Layer）。除了标准的OSI七层模型以外，常见的网络层次划分还有TCP/IP的四层协议以及TCP/IP的五层协议。对于TCP/IP的四层模型，其自下而上依次为：网络接口层（对应OSI/RM模型中的物理层、数据链路层）、网络层、传输层、应用层（对应OSI/RM模型中的会话层、表示层、应用层）。对于TCP/IP的五层模型，其自下而上依次为：物理层、数据链路层、网络层、传输层、应用层（对应OSI/RM模型中的会话层、表示层、应用层）。

计算机网络七层模型（ISO OSI/RM）

OSI七层模型为网络的标准层次划分，其自下而上依次为：物理层（Physics Layer）、数据链路层（Data Link Layer）、网络层（Network Layer）、运输层（Transport Layer）、会话层（Session Layer）、表示层（Presentation Layer）、应用层（Application Layer）。各层次功能如下：

物理层（Physics Layer）：激活、维持、关闭通信端点之间的机械特性、电气特性、功能特性以及过程特性。物理层确保原始数据可在各种物理媒介上传输，为上层协议提供了一个可靠传输数据的物理媒介。

数据链路层（Data Link Layer）：将来自网络层来的数据可靠传输到相邻节点的目标机网络层，为网络层提供可靠数据传输。

网络层（Network Layer）：实现端到端系统之间透明传输数据，它的功能包括寻址和路由选择、连接的建立、保持和终止等。此外，网络层还可以实现拥塞控制、网际互连等功能。

传输层（Transport Layer）：传输层负责将上层数据分段并提供端到端的、可靠的或不可靠的传输，以及处理端到端的差错控制和流量控制问题。

会话层（Session Layer）：会话层管理主机之间的会话进程，即负责建立、管理、终止进程之间的会话，还可以利用在数据中插入校验点来实现数据的同步。

表示层（Presentation Layer）：表示层负责对上层数据或信息进行变换以保证一个主机应用层信息可以被另一个主机的应用程序理解。

应用层（Application Layer）：为操作系统或网络应用程序提供访问网络服务的接口。

计算机网络硬件

计算机网络硬件包括用于通信的硬件和用于客户端的设备。

通信设备：

网络适配器（Network Adapter）

网络适配器用于把计算机连接到电缆上，传输从计算机与电缆媒介间的数据。

集线器(Hub)

集线器的主要功能为对接收到的信号进行再生整形放大，以扩大网络的传输距离，同时把所有节点集中在以它为中心的节点上。有些集线器仅仅把在任何一条电缆上接收到的信号向所有其他的电缆重新广播；另一些较为高级的集线器可以确定包的目的地址，并重新把信号仅仅发送到相应的电缆上，这些集线器就称之为交换式集线器或者交换机；还有一些高级集线器的特性包括错误诊断与隔离、流量监控及远程管理。

中继器（RP repeater）

中继器可从一个局域网上获取信号，对信号进行放大和提升功率后发向另一个局域网。它能够精确地重发信号，对衰减的信号进行放大，保持与原数据相同。

网桥（Bridge）

网桥也称桥接器，主要用于连接两个或多个局域网，并在它们之间传递封装的数据包。使用网桥可

以连接两个或多个相同类型的网络，允许每个网络使用不同的协议，网桥根据各个局域网上是否使用相同的协议，自动决定并完成所传输的数据包的协议格式的转换。

路由器（Router）

路由器的作用与网桥类似，但其功能要比网桥强，它具有网桥的全部功能，此外，它还具有选择传输路径的功能，以实现负载均衡。

网关（Gateway）

网关可以实现不同网络间不同协议的转换，使协议不同的网络通过网关连成一个网络。

传输介质（Transmission Medium）

传输介质决定网络的传输率、局域网的最大长度、传输的可靠性以及网络适配器的复杂性。常见的传输介质有：双绞线、同轴电缆、光缆等。

用户端设备：

服务器（server）

服务器是网络通信的中心结点。网络上的其他计算机依靠服务器储存数据，验证登录请求；服务器与其他计算机均连接到网络上，但服务器的不同之处是服务器软件比其他计算机上的更强大。

客户机（Client）

客户机又称用户工作站，是用户与网络打交道的设备，客户计算机执行用户程序并直接与用户进行交互。

对等机（Peers）

对等机，即对等式计算机，它不仅仅执行用户程序并直接与用户进行交互(类似于客户机)，而且也能向网络中的其他计算机共享自己的硬盘空间与打印机(类似于服务器)，但与服务器不同的是，对等式计算机并不验证其他计算机的文件，并且存储在对等机中的文件偶尔对网络中的其他计算机可用。

计算机网络软件

计算机网络软件包括通信支撑平台软件、网络应用支撑平台软件、网络应用系统、网络服务支撑平台软件、用于特殊网络站点的软件及网络管理系统等。从网络体系结构模型可知，通信软件和各层网络协议软件是这些网络软件的基础和核心。

通信软件

用以监督和控制通信工作的软件。它是计算机网络软件的基础组成部分，还可以实现计算机与自带终端或附属计算机之间的通信。

协议软件

它是网络软件的重要组成部分。在计算机网络的体系结构模型中，各层的协议大都由软件实现（物理层除外）。每层协议软件通常由一个或多个进程组成，来完成相应层协议所规定的功能，以及向上、下层的接口功能。

应用系统

应用系统的任务是实现网络总体规划所规定的各项任务，提供网络服务和资源共享。网络应用系统分为通用型应用系统和专用型应用系统。通用型应用系统适用于较广泛的行业领域，如数据收集系统、数据库查询系统、数据转发系统等。专用型应用系统只适用于特定的行业领域，如铁路控制、银行核算、军事指挥等。

网络IP地址

网络IP地址是指互联网协议地址（Internet Protocol Address）。IP地址是IP协议提供的一种统一的地址格式，用来为互联网上的每一个网络和每一台主机分配一个逻辑地址，以消除物理地址的差异。简单来说，IP地址相当于给互联网上的计算机一个唯一的编号，假如把互联网上的计算机比作一台电话，那么IP地址就相当于电话号码。

域名系统

域名系统（Domain Name System 缩写：DNS）是互联网的一项服务 它可以实现将域名和IP地址相互映射 能够使用户更方便地访问互联网 域名可将一个IP地址关联到一组有意义的符号串上去 用户访问一个网站的时候 既可以输入该网站的IP地址 也可以输入其域名 对访问而言 两者是等价的 网站的

IP地址都是唯一的 但这样也使得访问不同网站时 容易忘记或记混其IP地址 但是每个网站的域名都与网站内容相关联 方便用户记忆 比如 百度的IP地址为14.215.177.38 其域名为www.baidu.com 相比之下 其域名更容易记忆 方便用户访问

3W服务 (WWW)

WWW(World Wide Web)服务是一种建立在超文本基础上浏览、查询因特网信息的方式。它以交互方式查询并访问存放于远程计算机的信息，其核心技术为超文本传输协议和超文本标记语言。由于www服务使用的是超文本链接 (HTML)，可以很方便的从一个信息页转换到另一个信息页。它不仅能查看文字，还可以欣赏图片、音乐、动画，为用户获取信息资源提供了便利条件。

文件传输 (FTP)

文件传输协议 (File Transfer Protocol 缩写：FTP) 是用于在网络上进行文件传输的一套标准协议 它使用客户端/服务器 (C/S) 模式 能操作任何类型的文件而不需要进一步处理 但是FTP的延时很高 也就是说 从开始请求到第一次接收需求数据之间的时间会很长 而且用户需要不时地执行一些冗长的登录过程

TCP/IP协议

TCP/IP 也称为TCP/IP协议族 是基于 TCP 和 IP 这两个最初的协议之上的不同的通信协议的集合 包括传输控制协议 (TCP协议)、网际协议 (IP协议)、超文本传输协议 (HTTP协议)、FTP (文件传输协议)、DHCP (动态主机配置协议) 等 IP 协议用于计算机之间的通信 负责在因特网上发送和接收数据包 TCP协议用于从应用程序到网络的数据传输控制 负责在传送数据前将它们分割为 IP 包 然后在它们到达的时候将它们重组为原数据包 TCP/IP协议提供点对点的链接机制 将数据应如何封装、定址、传输、路由以及在目的地如何接收都加以标准化

DNS协议

DNS是域名系统(Domain Name System)的缩写 该系统用于命名组织到域层次结构中的计算机和网络服务 域名是由圆点分开一串单词或缩写组成的 在互联网上域名与IP地址之间具有一一对应关系 例如百度的IP地址为14.215.177.38 其域名为www.baidu.com DNS就是进行域名解析的服务器 DNS是互联网的一项核心服务 它可以将域名和IP地址之间进行相互映射

DHCP协议

动态主机设置协议 (Dynamic Host Configuration Protocol 缩写：DHCP) 是一个局域网的网络协议 使用UDP协议工作 该协议用于内部网或网络服务供应商自动分配IP地址以及给用户或内部网络管理员作为对所有计算机进行中央管理 DHCP协议通常被应用在大型的局域网络环境中 主要用于集中管理、分配IP地址 使网络环境中的主机可以动态地获得IP地址、网关地址、DNS服务器地址等信息 能够提升地址的使用率

国家信息化政策规划篇

国家信息战略规划

《国家信息化发展战略纲要》

2016年7月27日由中共中央办公厅、国务院办公厅印发 本战略纲要主要是根据新形势对《2006 - 2020年国家信息化发展战略》的调整和发展 是规范和指导未来10年国家信息化发展的纲领性文件 是国家战略体系的重要组成部分 是信息化领域规划、政策制定的重要依据

《“十三五”国家信息化规划》

2016年12月15日由国务院印发 本规划旨在贯彻落实“十三五”规划纲要和《国家信息化发展战略纲要》 是“十三五”国家规划体系的重要组成部分 是指导“十三五”期间各地区、各部门信息化工作的行动指南

《“十三五”信息领域科技创新专项规划》

由中华人民共和国科学技术部印发，主要制定“科技创新2030-重大项目”实施方案，新一代人工智能重大项目启动实施，天地一体化信息网络、大数据等重大项目稳步推进，启动物联网与智慧城市、宽带通信和新型网络等重点专项。

《国家集成电路产业发展推进纲要》

2014年由国务院印发 集成电路产业是信息技术产业的核心 是支撑经济社会发展和保障国家安全的战

略性、基础性和先导性产业 当前和今后一段时期是我国集成电路产业发展的重要战略机遇期和攻坚期 **为加快推进我国集成电路产业发展 特制定本纲要**

《促进大数据发展行动纲要》

2015年8月31日由国务院印发 重点加快政府数据开放共享 推动资源整合 提升治理能力；推动产业创新发展 培育新兴业态 助力经济转型；强化安全保障 提高管理水平 促进健康发展

《大数据产业发展规划（2016-2020年）》

2016年12月18日由工业和信息化部印发，主要是为了贯彻落实《中华人民共和国国民经济和社会发展的第十三个五年规划纲要》和《促进大数据发展行动纲要》，加快实施国家大数据战略，推动大数据产业健康快速发展。

《关于积极推进“互联网+”行动的指导意见》

2015年07月04日由国务院印发，主要围绕“互联网+”进行讲述如何把互联网的创新成果与经济社会各领域深度融合，进一步促进社会发展。

《中国制造2025》

2015年5月19日由国务院正式印发 坚持“创新驱动、质量为先、绿色发展、结构优化、人才为本”的基本方针 坚持“市场主导、政府引导 立足当前、着眼长远 整体推进、重点突破 自主发展、开放合作”的基本原则 通过“三步走”实现制造强国的战略目标：第一步 到2025年迈入制造强国行列；第二步 到2035年中国制造业整体达到世界制造强国阵营中等水平；第三步 到新中国成立一百年时 综合实力进入世界制造强国前列

信息安全相关的法律法规

我国信息安全法律法规简介

信息安全法是指维护信息安全，狭义上是指预防信息犯罪的刑事法律规范的总称。广义上的“信息安全法的调整范围应当包括网络信息安全应急保障关系、信息共享分析和预警关系、政府机构信息安全管理、通信运营机构的安全监管、ISP的安全监管、ICP(含大型商业机构)的安全监管、家庭用户及商业企业用户的安全责任、网络与信息安全技术进出口监管、网络与信息安全标准和指南以及评估监管、网络与信息安全研究规划、网络与信息安全培训管理、网络与信息安全监控等十二个方面”。

《工业控制系统信息安全防护指南》

2016年10月由工业和信息化部印发 《工业控制系统信息安全防护指南》是国家网络和信息安全的重要组成部分 主要是为了推动中国制造2025、制造业与互联网融合发展的基础保障 指导工业企业开展工控安全防护工作

我国网络安全立法体系架构

我国网络安全法规大体可以分为三个层面：国家法律、地方法规、行业管理办法。网络安全法需确立“防御、控制与惩治”三位一体的立法架构，以“防御和控制”性的法律规范替代传统单纯“惩治”性的刑事法律规范，从多方主体参与综合治理的层面，明确各方主体在预警与监测、网络安全事件的应急与响应、控制与恢复等环节中的过程控制要求，防御、控制、合理分配安全风险，惩治网络空间违法犯罪和恐怖活动。

法律界定了国家、企业、行业组织和个人等主体在网络安全保护方面的责任，设专章规定了国家网络安全监测预警、信息通报和应急制度，明确规定“国家采取措施，监测、防御、处置来源于中华人民共和国境内外的网络安全风险和威胁，保护关键信息基础设施免受攻击、入侵、干扰和破坏，依法惩治网络违法犯罪活动，维护网络空间安全和秩序”，已开始摆脱传统上将风险预防寄托于事后惩治的立法理念，构建兼具防御、控制与惩治功能的立法架构。

《刑法》

2015年8月29日 十二届全国人大常委会第十六次会议表决通过刑法修正案（九） 修改后的刑法自2015年11月1日开始施行 **这也是继1997年全面修订刑法后通过的第九个刑法修正案**

刑法是规定犯罪、刑事责任和刑罚的法律 有广义与狭义之分 广义刑法是一切刑事法律规范的总称 狭义刑法仅指刑法典 在我国即《中华人民共和国刑法》 **与广义刑法、狭义刑法相联系的 刑法还可区分为普通刑法和特别刑法** 普通刑法指具有普遍使用效力的刑法 **实际上即指刑法典** 特别刑法指仅

使用于特定的人、时、地、事（犯罪）的刑法在我国 也叫**单行刑法和附属刑法**

《保护国家秘密法》

于1988年9月5日第七届全国人民代表大会常务委员会第三次会议通过《中华人民共和国保守国家秘密法》，2010年4月29日第十一届全国人民代表大会常务委员会第十四次会议修订通过，现将修订后的《中华人民共和国保守国家秘密法》公布，自2010年10月1日起施行。其作用是为了保守国家秘密，维护国家安全和利益，保障改革开放和社会主义建设事业的顺利进行。

《国家安全法》

中华人民共和国国家安全法的实施细则 于1994年5月10日国务院第十九次常务会议通过 1994年6月4日中华人民共和国国务院令157号发布 自发布之日起施行

2017年11月22日 **《中华人民共和国反间谍法实施细则》自公布之日起施行 1994年6月4日国务院发布的《中华人民共和国国家安全法实施细则》同时废止**

《全国人大常委会关于维护互联网安全的决定》

2000年12月28日在第九届全国人民代表大会常务委员会第十九次会议上通过了**《全国人民代表大会常务委员会关于维护互联网安全的决定》** 主要为加快我国国民经济、科学技术的发展和社会服务信息化进程 保障互联网的运行安全和信息化安全

《中华人民共和国计算机信息系统安全保护条例》

最早在1994年2月18日 **《计算机信息系统安全保护条例》** 由中华人民共和国国务院令147号发布 根据 2011年01月08日《国务院关于废止和修改部分行政法规的决定》修正 自2011年1月8日起实施 **《计算机信息系统安全保护条例》** 是为了保护计算机信息系统的安全 促进计算机的应用和发展 保障社会主义现代化建设的顺利进行而制定的法规

《计算机信息网络国际联网安全保护管理办法》

1997年12月11日国务院批准通过**《计算机信息网络国际联网安全保护管理办法》** 公安部于1997年12月16日公安部令（第33号）发布 于1997年12月30日实施 根据2011年1月8日《国务院关于废止和修改部分行政法规的决定》修订 主要是为了加强对计算机信息网络国际联网的安全保护 维护公共秩序和社会稳定

《互联网电子公告服务管理规定》

根据中华人民共和国工业和信息化部令第28号《工业和信息化部关于废止和修改部分规章的决定》的规定 2000年10月8日中华人民共和国信息产业部令第3号公布的《互联网电子公告服务管理规定》自2014年9月23日起废止 《互联网电子公告服务管理规定》一般指互联网（即广域网、局域网及单机按照一定的通讯协议组成的国际计算机网络）电子公告服务管理规定（互联网电子公告服务管理规定）

《中华人民共和国国家安全法》

2015年7月1日 第十二届全国人民代表大会常务委员会第十五次会议通过新的国家安全法 国家主席习近平签署第29号主席令予以公布 **法律对政治安全、国土安全、军事安全、文化安全、科技安全等11个领域的国家安全任务进行了明确 共7章84条 自2015年7月1日起施行**

中华人民共和国国家安全法 是为了维护国家安全 保卫人民民主专政的政权和中国特色社会主义制度 保护人民的根本利益 保障改革开放和社会主义现代化建设的顺利进行 实现中华民族伟大复兴 根据《中华人民共和国宪法》 制定的法规

《中华人民共和国电子签名法》

2004年8月28日在第十届全国人民代表大会常务委员会第十一次会议中通过了《中华人民共和国电子签名法》 自2005年4月1日起施行 当前版本为2015年4月24日第十二届全国人民代表大会常务委员会第十四次会议修正

中华人民共和国电子签名法是为了规范电子签名行为 确立电子签名的法律效力 维护有关各方的合法权益而制定的法律

《互联网信息服务管理办法》

2000年9月20日经中华人民共和国国务院第31次常务会议通过**《互联网信息服务管理办法》** 2000年9月25日公布施行 该《办法》共二十七条 自公布之日起施行 该办法是为了规范互联网信息服务活动

促进互联网信息服务健康有序发展

《信息安全等级保护管理办法》

根据《中华人民共和国计算机信息系统安全保护条例》等有关法律法规 制定了《信息安全等级保护管理办法》 由四部委下发 公通字200743号文 该办法是为了规范信息安全等级保护管理 提高信息安全保障能力和水平 维护国家安全、社会稳定和公共利益 保障和促进信息化建设

计算机信息系统安全保护的基本制度

1994年2月18日中华人民共和国国务院令第147号现发布了《中华人民共和国计算机信息系统安全保护条例》，自发布之日起施行。该条例为了保护计算机信息系统的安全，促进计算机的应用和发展，保障社会主义现代化建设的顺利进行。

计算机信息网络进行国际联网的原则

1996年2月1日国务院令第195号发布《中华人民共和国计算机信息网络国际联网管理暂行规定》，根据1997年5月20日《国务院关于修改<中华人民共和国计算机信息网络国际联网管理暂行规定>的决定》进行了修正。目的是为了加强对计算机信息网络国际联网的管理，保障国际计算机信息交流的健康发展。