

统）、从记录系统到数据仓库的映射、数据模型的规格说明、抽取日志和访问数据的公用例行程序等。

- 粒度：数据仓库的数据单位中保存数据的细化或综合程度的级别。细化程度越高，粒度级就越小；相反，细化程度越低，粒度级就越大。
- 分割：结构相同的数据被分成多个数据物理单元。任何给定的数据单元属于且仅属于一个分割。
- 数据集市：小型的，面向部门或工作组级的数据仓库。
- 操作数据存储（Operation Data Store, ODS）：能支持组织日常的全局应用的数据集合，是不同于DB的一种新的数据环境，是DW扩展后得到的一个混合形式。它具有四个基本特点：面向主题的、集成的、可变的、当前或接近当前的。
- 数据模型：逻辑数据结构，包括由数据库管理系统为有效进行数据库处理提供的操作和约束；用于表示数据的系统。
- 人工关系：在决策支持系统环境中用于表示参照完整性的一种设计技术。

数据仓库是一个面向主题的、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。常见的数据仓库的体系结构如图 2-2 所示。

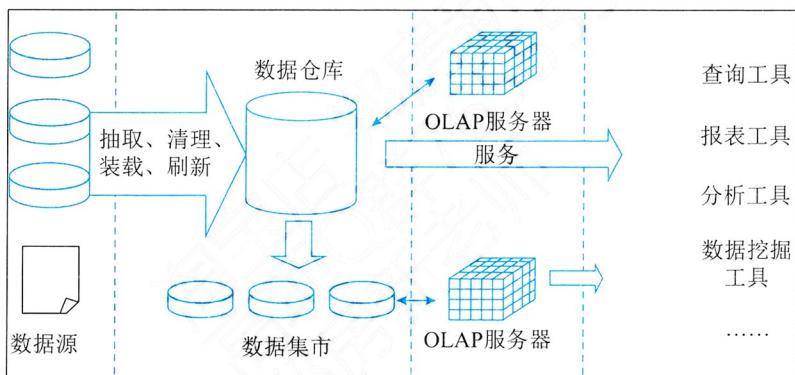


图 2-2 数据仓库体系结构

(1) 数据源。它是数据仓库系统的基础，是整个系统的数据源泉。通常包括组织内部信息和外部信息。内部信息包括存放于关系型数据库管理系统中的各种业务处理数据和各类文档数据。外部信息包括各类法律法规、市场信息和竞争对手的信息等。

(2) 数据的存储与管理。它是整个数据仓库系统的核心。数据仓库的真正关键是数据的存储和管理。数据仓库的组织管理方式决定了它有别于传统数据库，同时也决定了其对外部数据的表现形式。要决定采用什么产品和技术来建立数据仓库的核心，则需要从数据仓库的技术特点着手分析。针对现有各业务系统的数据，进行抽取、清理并有效集成，按照主题进行组织。数据仓库按照数据的覆盖范围可以分为组织级数据仓库和部门级数据仓库（通常称为数据集市）。

(3) 联机分析处理（On-Line Analytic Processing, OLAP）服务器。OLAP 对分析需要的数据进行有效集成，按多维模型予以组织，以便进行多角度、多层次的分析，并发现趋势。其具

体实现可以分为：基于关系数据库的 OLAP（Relational OLAP, ROLAP）、基于多维数据组织的 OLAP（Multidimensional OLAP, MOLAP）和基于混合数据组织的 OLAP（Hybrid OLAP, HOLAP）。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 基本数据存放于关系数据库管理系统（Relational Database Management System, RDBMS）之中，聚合数据存放于多维数据库中。

（4）前端工具。前端工具主要包括各种查询工具、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。其中数据分析工具主要针对 OLAP 服务器，报表工具、数据挖掘工具主要针对数据仓库。

2.1.4 信息安全

常见的信息安全问题主要表现为：计算机病毒泛滥、恶意软件的入侵、黑客攻击、利用计算机犯罪、网络有害信息泛滥、个人隐私泄露等。随着物联网、云计算、人工智能、大数据等新一代信息技术的广泛应用，信息安全也面临着新的问题和挑战。

1. 信息安全基础

信息安全强调信息（数据）本身的安全属性，主要包括以下内容。

- 保密性（Confidentiality）：信息不被未授权者知晓的属性。
- 完整性（Integrity）：信息是正确的、真实的、未被篡改的、完整无缺的属性。
- 可用性（Availability）：信息可以随时正常使用的属性。

信息必须依赖其存储、传输、处理及应用的载体（媒介）而存在，因此针对信息系统，安全可以划分为四个层次：设备安全、数据安全、内容安全、行为安全。

信息系统一般由计算机系统、网络系统、操作系统、数据库系统和应用系统组成。与此对应，信息系统安全主要包括计算机设备安全、网络安全、操作系统安全、数据库系统安全和应用系统安全等。

网络安全技术主要包括：防火墙、入侵检测与防护、VPN、安全扫描、网络蜜罐技术、用户和实体行为分析技术等。

2. 加密解密

为了保证信息的安全性，就需要采用信息加密技术对信息进行伪装，使得信息非法窃取者无法理解信息的真实含义；需要采用加密算法提取信息的特征码（校验码）或特征矢量，并与有关信息封装在一起，信息的合法拥有者可以利用特征码对信息的完整性进行校验；需要采用加密算法对信息使用者的身份进行认证、识别和确认，以对信息的使用进行控制。

发信者将明文数据加密成密文，然后将密文数据送入网络传输或存入计算机文件，而且只给合法收信者分配密钥。合法收信者接收到密文后，实行与加密变换相逆的变换，去掉密文的伪装并恢复出明文，这一过程称为解密（Decryption）。解密在解密密钥的控制下进行。用于解密的一组数学变换称为解密算法。

加密技术包括两个元素：算法和密钥。密钥加密技术的密码体制分为对称密钥体制和非对

称密钥体制两种。相应地，对数据加密的技术分为两类，即对称加密（私人密钥加密）和非对称加密（公开密钥加密）。对称加密以数据加密标准（Data Encryption Standard, DES）算法为典型代表，非对称加密通常以 RSA（Rivest Shamir Adleman）算法为代表。对称加密的加密密钥和解密密钥相同，而非对称加密的加密密钥和解密密钥不同，加密密钥可以公开而解密密钥需要保密。

3. 安全行为分析技术

传统安全产品、技术、方案基本上都是基于已知特征进行规则匹配来进行分析和检测。基于特征、规则和人工分析，以“特征”为核心的检测分析存在安全可见性盲区，有滞后效应、无力检测未知攻击、容易被绕过，以及难以适应攻防对抗的网络现实和快速变化的组织环境、外部威胁等问题。另一方面，虽然大多数的攻击可能来自组织以外，但最严重的损害往往是由内部人员造成的，只有管理好内部威胁，才能保证信息和网络安全。

用户和实体行为分析（User and Entity Behavior Analytics, UEBA）提供了用户画像及基于各种分析方法的异常检测，结合基本分析方法（利用签名的规则、模式匹配、简单统计、阈值等）和高级分析方法（监督和无监督的机器学习等），用打包分析来评估用户和其他实体（主机、应用程序、网络、数据库等），发现与用户或实体标准画像或行为异常的活动所相关的潜在事件。UEBA 以用户和实体为对象，利用大数据，结合规则以及机器学习模型，并通过定义此类基线，对用户和实体行为进行分析和异常检测，尽可能快速地感知内部用户和实体的可疑或非法行为。

UEBA 是一个完整的系统，涉及算法、工程等检测部分，以及用户与实体风险评分排序、调查等用户交换和反馈。从架构上来看，UEBA 系统通常包括数据获取层、算法分析层和场景应用层。

4. 网络安全态势感知

网络安全态势感知（Network Security Situation Awareness）是在大规模网络环境中，对能够引起网络态势发生变化的安全要素进行获取、理解、显示，并据此预测未来的网络安全发展趋势。安全态势感知不仅是一种安全技术，也是一种新兴的安全概念。它是一种基于环境的、动态的、整体的洞悉安全风险的能力。安全态势感知的前提是安全大数据，其在安全大数据的基础上进行数据整合、特征提取等，然后应用一系列态势评估算法生成网络的整体态势状况，应用态势预测算法预测态势的发展状况，并使用数据可视化技术，将态势状况和预测情况展示给安全人员，方便安全人员直观便捷地了解网络当前状态及预期的风险。

网络安全态势感知的关键技术主要包括：海量多元异构数据的汇聚融合技术、面向多类型的网络安全威胁评估技术、网络安全态势评估与决策支撑技术、网络安全态势可视化等。

2.1.5 信息技术的发展

作为信息技术的基础，计算机软硬件、网络、存储和数据库、信息安全等都在不断的发展创新，引领着当前信息技术发展的潮流。

在计算机软硬件方面，计算机硬件技术将向超高速、超小型、平行处理、智能化的方向发展，计算机硬件设备的体积越来越小、速度越来越高、容量越来越大、功耗越来越低、可靠性越来越高。计算机软件越来越丰富，功能越来越强大，“软件定义一切”概念成为当前发展的主流。

在网络技术方面，计算机网络与通信技术之间的联系日益密切，甚至是已经融为一体。作为国家最重要的基础设施之一，5G成为当前的主流，面向物联网、低时延场景的窄带物联网（Narrow Band Internet of Things, NB-IoT）和增强型机器类型通信（enhanced Machine-Type Communication, eMTC）、工业物联网（Industrial Internet of Things, IIoT）和低延时高可靠通信（Ultra Reliable Low Latency Communication, URLLC）等技术，将进一步得到充分发展。

在存储和数据库方面，随着数据量的不断爆炸式增长，数据存储结构也越来越灵活多样，日益变革的新业务需求驱使数据库及应用系统的存在形式愈发丰富，这些变化均对各类数据库的架构和存储模式提出了挑战，推动数据库技术不断向着模型拓展、架构解耦的方向演进。

在信息安全方面，传统计算机安全理念将过渡到以可信计算理念为核心的计算机安全，由网络普及应用引发的技术与应用模式的变革，正在进一步推动信息安全网络化关键技术的创新；同时信息安全标准的研究与制定，信息安全产品和服务的集成和融合，正引领着当前信息安全技术朝着标准化和集成化的方向发展。

2.2 新一代信息技术及应用

信息技术在智能化、系统化、微型化、云端化的基础上不断融合创新，促进了物联网、云计算、大数据、区块链、人工智能、虚拟现实等新一代信息技术的诞生。新一代信息技术与信息资源充分开发利用形成的新模式、新业态等，是信息化发展的主要趋势，也是信息系统集成领域未来的重要业务范畴。

2.2.1 物联网

物联网（The Internet of Things）是指通过信息传感设备，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、监控和管理的网络。物联网主要解决物品与物品（Thing to Thing, T2T）、人与物品（Human to Thing, H2T）、人与人（Human to Human, H2H）之间的互连。另外，许多学者在讨论物联网时经常会引入 M2M 的概念：可以解释为人与人（Man to Man）、人与机器（Man to Machine）或机器与机器（Machine to Machine）。

1. 技术基础

物联网架构可分为三层：感知层、网络层和应用层。感知层由各种传感器构成，包括温度传感器，二维码标签、RFID 标签和读写器，摄像头，GPS 等感知终端。感知层是物联网识别物体、采集信息的来源。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，是整个物联网的中枢，负责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，它与行业需求结合以实现物联网的智能应用。

物联网的产业链包括传感器和芯片、设备、网络运营及服务、软件与应用开发和系统集成。物联网技术在智能电网、智慧物流、智能家居、智能交通、智慧农业、环境保护、医疗健康、城市管理（智慧城市）、金融服务与保险业、公共安全等方面有非常关键和重要的应用。

2. 关键技术

物联网关键技术主要涉及传感器技术、传感网和应用系统框架等。

1) 传感器技术

传感器是一种检测装置，它能“感受”到被测量的信息，并能将检测到的信息按一定规律变换成为电信号或其他所需形式的信息输出，以满足信息的传输、处理、存储、显示、记录和控制等要求。它是实现自动检测和自动控制的首要环节，也是物联网获取物理世界信息的基本手段。

射频识别技术（Radio Frequency Identification, RFID）是物联网中使用的一种传感器技术，在物联网发展中备受关注。RFID 可通过无线电信号识别特定目标并读写相关数据，而无须识别系统与特定目标之间建立机械或光学接触。RFID 是一种简单的无线系统，由一个询问器（或阅读器）和很多应答器（或标签）组成。标签由耦合元件及芯片组成，每个标签具有扩展词条唯一的电子编码，附着在物体上标识目标对象，它通过天线将射频信息传递给阅读器，阅读器就是读取信息的设备。RFID 技术让物品能够“开口说话”。这就赋予了物联网一个特性——可跟踪性，即可以随时掌握物品的准确位置及其周边环境。

2) 传感网

微机电系统（Micro-Electro-Mechanical Systems, MEMS）是由微传感器、微执行器、信号处理和控制电路、通信接口和电源等部件组成的一体化的微型器件系统。其目标是把信息的获取、处理和执行集成在一起，组成具有多功能的微型系统，集成于大尺寸系统中，从而大幅地提高系统的自动化、智能化和可靠性水平。MEMS 赋予了普通物体新的“生命”，它们有了属于自己的数据传输通路、存储功能、操作系统和专门的应用程序，从而形成一个庞大的传感网，使物联网能够通过物品来实现对人的监控与保护。未来，衣服可以通过传感网“告诉”洗衣机放多少水和洗衣粉最经济；文件夹会“检查”人们忘带了什么重要文件；食品蔬菜的标签会向顾客的手机介绍“自己”是否真正“绿色安全”。

3) 应用系统框架

物联网应用系统框架是一种以机器终端智能交互为核心的、网络化的应用与服务。它将使对象实现智能化的控制，涉及 5 个重要的技术部分：机器、传感器硬件、通信网络、中间件和应用。该框架基于云计算平台和智能网络，可以依据传感器网络获取的数据进行决策，改变对象的行为控制和反馈。以智能停车场为例，当车辆驶入或离开天线通信区时，天线以微波通信的方式与电子识别卡进行双向数据交换，从电子车卡上读取车辆的相关信息，从司机卡上读取司机的相关信息，自动识别电子车卡和司机卡，并判断该车卡是否有效和司机卡的合法性，核对车道控制电脑并显示与该电子车卡和司机卡一一对应的车牌号码及驾驶员等资料信息。车道控制电脑自动将通过时间、车辆和驾驶员的有关信息存入数据库中，车道控制电脑根据读到的

数据判断是正常卡、未授权卡、无卡还是非法卡，据此做出相应的回应和提示。另外，家中的老人通过佩戴嵌入智能传感器的手表，在外地的子女可以随时通过手机查询父母的血压、心跳是否稳定。智能化的住宅在主人上班时，传感器自动关闭水电气和门窗，定时向主人的手机发送消息，汇报安全情况。

3. 应用和发展

物联网的应用领域涉及人们工作与生活的方方面面。在工业、农业、环境、交通、物流、安保等基础设施领域的应用，有效地推动了这些方面的智能化发展，使得有限的资源能更加合理地使用分配，从而提高了行业效率、效益；在家居、医疗健康、教育、金融与服务业、旅游业等与生活息息相关领域的应用，通过与社会科学和社会治理的充分融合创新，实现了服务范围、服务方式和服务质量等方面的巨大变革和进步。

2.2.2 云计算

云计算（Cloud Computing）是分布式计算的一种，指的是通过网络“云”将巨大的数据计算处理程序分解成无数个小程序，然后通过由多部服务器组成的系统进行处理和分析这些小程序得到结果并返回给用户。在云计算早期，就是简单的分布式计算，进行任务分发并对计算结果进行合并。当前的云计算已经不单单是一种分布式计算，而是分布式计算、效用计算、负载均衡、并行计算、网络存储、热备份冗余和虚拟化等计算机技术混合演进并跃升的结果。

1. 技术基础

云计算是一种基于互联网的计算方式，通过这种方式将网络上配置为共享的软件资源、计算资源、存储资源和信息资源，按需求提供给网上的终端设备和终端用户。云计算也可以理解为向用户屏蔽底层差异的分布式处理架构。在云计算环境中，用户与实际服务提供的计算资源相分离，云端集合了大量计算设备和资源。

当使用云计算服务时，用户不需要安排专门的维护人员，云计算服务的提供商为数据和服务器的安全做出相对较高水平的保护。由于云计算将数据存储在云端（分布式的云计算设备中承担计算和存储功能的部分），业务逻辑和相关计算都在云端完成，因此，终端只需要一个能够满足基础应用的普通设备即可。

云计算实现了“快速、按需、弹性”的服务，用户可以随时通过宽带网络接入“云”并获得服务，按照实际需求获取或释放资源，根据需求对资源进行动态扩展。

按照云计算服务提供的资源层次，可以分为基础设施即服务（Infrastructure as a Service, IaaS）、平台即服务（Platform as a Service, PaaS）和软件即服务（Software as a Service, SaaS）三种服务类型。

IaaS 向用户提供计算机能力、存储空间等基础设施方面的服务。这种服务模式需要较大的基础设施投入和长期运营管理经验，其单纯出租资源的盈利能力有限。

PaaS 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。PaaS 服务的重点不在于直接的经济效益，而更注重构建和形成紧密的产业生态。

SaaS 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，

SaaS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。

2. 关键技术

云计算的关键技术主要涉及虚拟化技术、云存储技术、多租户和访问控制管理、云安全技术等。

1) 虚拟化技术

虚拟化是一个广义术语，在计算机领域通常是指计算元件在虚拟的基础上而不是真实的基础上运行。虚拟化技术可以扩大硬件的容量，简化软件的重新配置过程。CPU的虚拟化技术可以单CPU模拟多CPU并行，允许一个平台同时运行多个操作系统，并且应用程序都可以在相互独立的空间内运行而互不影响，从而显著提高计算机的工作效率。

虚拟化技术与多任务以及超线程技术是完全不同的。多任务是指在一个操作系统中多个程序同时并行运行，而在虚拟化技术中，则可以同时运行多个操作系统，而且每一个操作系统中都有多个程序运行，每一个操作系统都运行在一个虚拟的CPU或者虚拟主机上。超线程技术只是单CPU模拟双CPU来平衡程序运行性能，这两个模拟出来的CPU是不能分离的，只能协同工作。

容器(Container)技术是一种全新意义上的虚拟化技术，属于操作系统虚拟化的范畴，也就是由操作系统提供虚拟化的支持。目前最受欢迎的容器环境是Docker。容器技术将单个操作系统的资源划分到孤立的组中，以便更好地在孤立的组之间平衡有冲突的资源使用需求。例如：用户创建一个应用，传统方式需要虚拟机，但虚拟机本身就占用了更多的系统资源。又如，应用需要在开发和运维之间转移、协作，当开发和运维的操作环境不同时，也会影响结果。使用容器技术可将应用隔离在一个独立的运行环境中，该独立环境称之为容器，可以减少运行程序带来的额外消耗，并可以在几乎任何地方以相同的方式运行。

2) 云存储技术

云存储技术是基于传统媒体系统发展而来的一种全新信息存储管理方式，该方式整合应用了计算机系统的软硬件优势，可较为快速、高效地对海量数据进行在线处理，通过多种云技术平台的应用，实现了数据的深度挖掘和安全管理。

分布式文件系统作为云存储技术中的重要组成部分，在维持兼容性的基础上，对系统复制和容错功能进行提升。同时，通过云集群管理实现云存储的可拓展性，借助模块之间的合理搭配，完成解决方案拟定解决的网络存储问题、联合存储问题、多节点存储问题、备份处理、负载均衡等。云储存的实现过程中，结合分布式的文件结构，在硬件支撑的基础上，对硬件运行环境进行优化，确保数据传输的完整性和容错性；结合成本低廉的硬件的扩展，大大降低了存储的成本。

在分布式文件系统的支撑下，实现了通过云存储资源的拓展，辅助高吞吐量数据的分析，使得用户可以更加充分、全面地进行数据管理，实现用户上传信息的优化管理，满足了不同平台信息获取需要。另一方面，通过加强对云存储技术中相关数据的安全防护，实现信息存储过

程中的病毒防护和安全监控，确保信息存储应用的安全性。

3) 多租户和访问控制管理

云计算环境下访问控制的研究是伴随着云计算的发展而开始的，访问控制管理是云计算应用的核心问题之一。云计算访问控制的研究主要集中在云计算访问控制模型、基于 ABE 密码体制的云计算访问控制、云中多租户及虚拟化访问控制研究。

云计算访问控制模型就是按照特定的访问策略来描述安全系统，建立安全模型的一种方法。用户（租户）可以通过访问控制模型得到一定的权限，进而对云中的数据进行访问，所以访问控制模型多用于静态分配用户的权限。云计算中的访问控制模型都是以传统的访问控制模型为基础，在传统的访问控制模型上进行改进，使其更适用于云计算的环境。根据访问控制模型功能的不同，研究的内容和方法也不同，常见的有基于任务的访问控制模型、基于属性模型的云计算访问控制、基于 UCON 模型的云计算访问控制、基于 BLP 模型的云计算访问控制等。

基于 ABE 密码机制的云计算访问控制包括 4 个参与方：数据提供者、可信第三方授权中心、云存储服务器和用户。首先，可信授权中心生成主密钥和公开参数，将系统公钥传给数据提供者，数据提供者收到系统公钥之后，用策略树和系统公钥对文件加密，将密文和策略树上传到云服务器；然后，当一个新用户加入系统后，将自己的属性集上传给可信授权中心并提交私钥申请请求，可信授权中心针对用户提交的属性集和主密钥计算生成私钥，传给用户；最后，用户下载感兴趣的数据。如果其属性集合满足密文数据的策略树结构，则可以解密密文；否则，访问数据失败。

云中多租户及虚拟化访问控制是云计算的典型特征。由于租户间共享物理资源，并且其可信度不容易得到，所以租户之间就可以通过侧通道攻击来从底层的物理资源中获得有用的信息。此外，由于在虚拟机上要部署访问控制策略可能会带来多个租户访问资源的冲突，导致物理主机上出现没有认证的或者权限分配错误的信息流。这就要求在云环境下，租户之间的通信应该由访问控制来保证，并且每个租户都有自己的访问控制策略，使得整个云平台的访问控制变得复杂。目前，对多租户访问控制的研究主要集中在对多租户的隔离和虚拟机的访问控制方面。

4) 云安全技术

云安全研究主要包含两个方面的内容，一是云计算技术本身的安全保护工作，涉及相应的数据完整性及可用性、隐私保护性以及服务可用性等方面的内容；二是借助于云服务的方式来保障客户端用户的安全防护需求，通过云计算技术来实现互联网安全，涉及基于云计算的病毒防治、木马检测技术等。

在云安全技术的研究方面，主要包含：

- 云计算安全性：主要是对于云自身以及所涉及的应用服务内容进行分析，重点探讨其相应得安全性问题，这里主要涉及如何有效实现安全隔离，保障互联网用户数据的安全性，如何有效防护恶意网络攻击，提升云计算平台的系统安全性，以及用户接入认证以及相应的信息传输审计、安全等方面的工作。
- 保障云基础设施的安全性：主要就是如何利用相应的互联网安全基础设备的相应资源，有效实现云服务的优化，从而保障满足预期的安全防护的要求。

- 云安全技术服务：重点集中于如何保障实现互联网终端用户的安全服务要求，能有效实现客户端的计算机病毒防治等相关服务工作。从云安全架构的发展情况来看，如果云计算服务商的安全等级不高，会造成服务用户需要具备更强的安全能力、承担更多管理职责。

为了提升云安全体系的能力，保障其具有较强的可靠性，云安全技术要从开放性、安全保障、体系结构的角度考虑。①云安全系统具有一定的开放性，要保障开放环境下可信认证；②在云安全系统方面，要积极采用先进的网络技术和病毒防护技术；③在云安全体系构建过程中，要保证其稳定性，以满足海量数据动态变化的需求。

综上所述，云安全技术是新一代互联网中安全技术构架的核心内容，体现了当前快速发展的云计算的先进性，是未来的信息安全技术发展的必然趋势。随着云计算应用领域的拓展，云安全技术也必然会越来越成熟，能有效全方位保障广大互联网用户的 data 应用安全性，对于云计算的进一步推广与应用具有至关重要的作用。

3. 应用和发展

云计算经历十余年的发展，已逐步进入成熟期，在众多领域正发挥着越来越大的作用，“上云”将成为各类组织加快数字化转型、鼓励技术创新和促进业务增长的第一选择，甚至是必备的前提条件。

云计算将进一步成为创新技术和最佳工程实践的重要载体和试验场。从 AI 与机器学习、IoT 与边缘计算、区块链到工程实践领域的 DevOps、云原生和 Service Mesh，都有云计算厂商积极参与、投入和推广的身影。以人工智能为例，从前面提到的 IaaS 中 GPU 计算资源的提供，到面向特定领域成熟模型能力开放（如各类自然语言处理、图像识别、语言合成的 API），再到帮助打造定制化 AI 模型的机器学习平台，云计算实际上已成为 AI 相关技术的基础。

云计算将顺应产业互联网大潮，下沉行业场景，向垂直化、产业化纵深发展。随着通用类架构与功能的不断完善和对行业客户的不断深耕，云计算自然渗透进入更多垂直领域，成为提供更贴近行业业务与典型场景的基础能力。以金融云为例，云计算可针对金融保险机构特殊的合规和安全需要，提供物理隔离的基础设施，还可提供支付、结算、风控、审计等业务组件。

多云和混合云将成为大中型组织的刚需，得到更多重视与发展。当组织大量的工作负载部署在云端，新的问题则会显现：①虽然云端已经能提供相当高的可用性，但为了避免单一供应商出现故障时的风险，关键应用仍须架设必要的技术冗余；②当业务规模较大时，从商业策略角度看，也需要避免过于紧密的厂商绑定，以寻求某种层面的商业制衡和主动权。

云的生态建设重要性不断凸显，成为影响云间竞争的关键因素。当某个云发展到一定规模和阶段，就不能仅仅考虑技术和产品，需要站在长远发展的角度，建立和培养具有生命力的繁荣生态和社区。另外，云生态需要关注面向广大开发者、架构师和运维工程师的持续输出、培养和影响。只有赢得广大技术人员的关注和喜爱，才能赢得未来的云计算市场。

综上所述，“创新、垂直、混合、生态”这四大趋势伴随云计算快速发展。云计算对 IT 硬件资源与软件组件进行了标准化、抽象化和规模化，某种意义上颠覆和重构了 IT 业界的供应链，是当前新一代信息技术发展的巨大的革新与进步。

2.2.3 大数据

大数据（Big Data）指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。

1. 技术基础

大数据是具有体量大、结构多样、时效性强等特征的数据，处理大数据需要采用新型计算架构和智能算法等新技术。大数据从数据源到最终价值实现一般需要经过数据准备、数据存储与管理、数据分析和计算、数据治理和知识展现等过程，涉及数据模型、处理模型、计算理论以及与其相关的分布计算、分布存储平台技术、数据清洗和挖掘技术、流式计算和增量处理技术、数据质量控制等方面的研究。一般来说，大数据主要特征包括：

- 数据海量：大数据的数据体量巨大，从TB级别跃升到PB级别（ $1\text{PB}=1024\text{TB}$ ）、EB级别（ $1\text{EB}=1024\text{PB}$ ），甚至达到ZB级别（ $1\text{ZB}=1024\text{EB}$ ）。
- 数据类型多样：大数据的数据类型繁多，一般分为结构化数据和非结构化数据。相对于以往便于存储的以文本为主的结构化数据，非结构化数据越来越多，包括网络日志、音频、视频、图片、地理位置信息等，这些多类型的数据对数据的处理能力提出了更高要求。
- 数据价值密度低：数据价值密度的高低与数据总量的大小成反比。以视频为例，一部1小时的视频，在连续不间断的监控中，有用数据可能仅有一二秒。如何通过强大的机器算法更迅速地完成数据的价值“提纯”，成为目前大数据背景下亟待解决的难题。
- 数据处理速度快：为了从海量的数据中快速挖掘数据价值，一般要求要对不同类型的数据进行快速的处理，这是大数据区别于传统数据挖掘的最显著特征。

2. 关键技术

大数据技术作为信息化时代的一项新兴技术，技术体系处在快速发展阶段，涉及数据的处理、管理、应用等多个方面。具体来说，技术架构是从技术视角研究和分析大数据的获取、管理、分布式处理和应用等。大数据的技术架构与具体实现的技术平台和框架息息相关，不同的技术平台决定了不同的技术架构和实现。从总体上说，大数据技术架构主要包含大数据获取技术、分布式数据处理技术和大数据管理技术，以及大数据应用和服务技术。

1) 大数据获取技术

目前，大数据获取的研究主要集中在数据采集、整合和清洗三个方面。数据采集技术实现数据源的获取，然后通过整合和清理技术保证数据质量。

数据采集技术主要是通过分布式爬取、分布式高速高可靠性数据采集、高速全网数据映像技术，从网站上获取数据信息。除了网络中包含的内容之外，对于网络流量的采集可以使用DPI或DFI等带宽管理技术进行处理。

数据整合技术是在数据采集和实体识别的基础上，实现数据到信息的高质量整合。数据整合技术包括多源多模态信息集成模型、异构数据智能转换模型、异构数据集成的智能模式抽取

和模式匹配算法、自动容错映射和转换模型及算法、整合信息的正确性验证方法、整合信息的可用性评估方法等。

数据清洗技术一般根据正确性条件和数据约束规则，清除不合理和错误的数据，对重要的信息进行修复，保证数据的完整性。包括数据正确性语义模型、关联模型和数据约束规则、数据错误模型和错误识别学习框架、针对不同错误类型的自动检测和修复算法、错误检测与修复结果的评估模型和评估方法等。

2) 分布式数据处理技术

分布式计算是随着分布式系统的发展而兴起的，其核心是将任务分解成许多小的部分，分配给多台计算机进行处理，通过并行工作的机制，达到节约整体计算时间，提高计算效率的目的。目前，主流的分布式计算系统有 Hadoop、Spark 和 Storm。Hadoop 常用于离线的复杂的大数据处理，Spark 常用于离线的快速的大数据处理，而 Storm 常用于在线的实时的大数据处理。

大数据分析与挖掘技术主要指改进已有数据挖掘和机器学习技术；开发数据网络挖掘、特征群组挖掘、图挖掘等新型数据挖掘技术；创新基于对象的数据连接、相似性连接等大数据融合技术；突破用户兴趣分析、网络行为分析、情感语义分析等面向领域的数据挖掘技术。

3) 大数据管理技术

大数据管理技术主要集中在大数据存储、大数据协同和安全隐私等方面。

大数据存储技术主要有三个方面。①采用 MPP 架构的新型数据库集群，通过列存储、粗粒度索引等多项大数据处理技术和高效的分布式计算模式，实现大数据存储；②围绕 Hadoop 衍生出相关的大数据技术，应对传统关系型数据库较难处理的数据和场景，通过扩展和封装 Hadoop 来实现对大数据存储、分析的支撑；③基于集成的服务器、存储设备、操作系统、数据库管理系统，实现具有良好的稳定性、扩展性的大数据一体机。

多数据中心的协同管理技术是大数据研究的另一个重要方向。通过分布式工作流引擎实现工作流调度、负载均衡，整合多个数据中心的存储和计算资源，从而为构建大数据服务平台提供支撑。

大数据隐私性技术的研究，主要集中于新型数据发布技术，尝试在尽可能少损失数据信息的同时最大化地隐藏用户隐私。在数据信息量和隐私之间是有矛盾的，目前没有非常好的解决办法。

4) 大数据应用和服务技术

大数据应用和服务技术主要包含分析应用技术和可视化技术。

大数据分析应用主要是面向业务的分析应用。在分布式海量数据分析和挖掘的基础上，大数据分析应用技术以业务需求为驱动，面向不同类型的业务需求开展专题数据分析，为用户提供高可用、高易用的数据分析服务。

可视化通过交互式视觉表现的方式来帮助人们探索和理解复杂的数据。大数据的可视化技术主要集中在文本可视化技术、网络（图）可视化技术、时空数据可视化技术、多维数据可视化和交互可视化等。在技术方面，主要关注原位交互分析（In Situ Interactive Analysis）、数据表示、不确定性量化和面向领域的可视化工具库。

3. 应用和发展

大数据像水、矿石、石油一样，正在成为新的资源和社会生产要素，从数据资源中挖掘潜在的价值，成为当前大数据时代研究的热点。如何快速对数量巨大、来源分散、格式多样的数据进行采集、存储和关联分析，从中发现新知识、创造新价值、提升新能力的新一代信息技术和服务业态，是其应用价值的重要体现。

(1) 在互联网行业，网络的广泛应用和社交网络已深入到社会工作、生活的方方面面，海量数据的产生、应用和服务一体化。每个人都是数据的生产者、使用者和受益者。从大量的数据中挖掘用户行为，反向传输到业务领域，支持更准确的社会营销和广告，可增加业务收入，促进业务发展。同时，随着数据的大量生成、分析和应用，数据本身已成为可以交易的资产，大数据交易和数据资产化成为当前具有价值的领域和方向。

(2) 在政府的公共数据领域，结合大数据的采集、治理和集成，将各个部门搜集的信息进行剖析和共享，能够发现管理上的纰漏，提高执法水平，增进财税增收和加大市场监管程度，大大改变政府管理模式、节省政府投资、增强市场管理，提高社会治理水平、城市管理能力和人民群众的服务能力。

(3) 在金融领域，大数据征信是重要的应用领域。通过大数据的分析和画像，能够实现个人信用和金融服务的结合，从而服务于金融领域的信任管理、风控管理、借贷服务等，为金融业务提供有效支撑。

(4) 在工业领域，结合海量的数据分析，能够为工业生产过程提供准确的指导，如在航运大数据领域，能够使用大数据对将来航路的国际贸易货量进行预测分析，预知各个口岸的热度；能够利用天气数据对航路的影响进行分析，提供相关业务的预警、航线的调整和资源的优化调配方案，避免不必要的亏损。

(5) 在社会民生领域，大数据的分析应用能够更好地为民生服务。以疾病预测为例，基于大数据的积累和智能分析，能够透视人们搜索“流感、肝炎、肺结核和未病”的发病时间和地点分布，结合气温变化、环境指数、人口流动等因素建立预测模型，能够为公共卫生治理人员提供多种传染病的趋势预测，帮助其提早进行预防部署。

2.2.4 区块链

“区块链”概念于 2008 年在《比特币：一种点对点电子现金系统》中被首次提出，并在比特币系统的数据加密货币体系中成功应用，已成为政府、组织和学者等重点关注和研究的热点。区块链技术具有多中心化存储、隐私保护、防篡改等特点，提供了开放、分散和容错的事务机制，成为新一代匿名在线支付、汇款和数字资产交易的核心，被广泛应用于各大交易平台，为金融、监管机构、科技创新、农业以及政治等领域带来了深刻的变革。

1. 技术基础

区块链概念可以理解为以非对称加密算法为基础，以改进的默克尔树（Merkle Tree）为数据结构，使用共识机制、点对点网络、智能合约等技术结合而成的一种分布式存储数据库技术。区块链分为公有链（Public Blockchain）、联盟链（Consortium Blockchain）、私有链（Private

Blockchain) 和混合链 (Hybrid Blockchain) 四大类。

一般来说，区块链的典型特征包括：

- 多中心化：链上数据的验证、核算、存储、维护和传输等过程均依赖分布式系统结构，运用纯数学方法代替中心化组织机构在多个分布式节点之间构建信任关系，从而建立可信的分布式系统。
- 多方维护：激励机制可确保分布式系统中的所有节点均可参与数据区块的验证过程，并通过共识机制选择特定节点将新产生的区块加入到区块链中。
- 时序数据：区块链运用带有时间戳信息的链式结构来存储数据信息，为数据信息添加时间维度的属性，从而可实现数据信息的可追溯性。
- 智能合约：区块链技术能够为用户提供灵活可变的脚本代码，以支持其创建新型的智能合约。
- 不可篡改：在区块链系统中，因为相邻区块间后序区块可对前序区块进行验证，若篡改某一区块的数据信息，则需递归修改该区块及其所有后序区块的数据信息，然而每一次哈希的重新计算代价是巨大的，且须在有限时间内完成，因此可保障链上数据的不可篡改性。
- 开放共识：在区块链网络中，每台物理设备均可作为该网络中的一个节点，任意节点可自由加入且拥有一份完整的数据库拷贝。
- 安全可信：数据安全可通过基于非对称加密技术对链上数据进行加密来实现，分布式系统中各节点通过区块链共识算法所形成的算力来抵御外部攻击、保证链上数据不被篡改和伪造，从而具有较高的保密性、可靠性和安全性。

2. 关键技术

从区块链的技术体系视角看，区块链基于底层的数据基础处理、管理和存储技术，以区块数据的管理、链式结构的数据、数字签名、哈希函数、默克尔树、非对称加密等，通过基于P2P网络的对称式网络，组织节点参与数据的传播和验证，每个节点均会承担网络路由、验证区块数据、传播区块数据、记录交易数据、发现新节点等功能，包含传播机制和验证机制。为保障区块链应用层的安全，通过激励层的发行机制和分配机制，在整个分布式网络的节点以最高效率的方式达成共识。

1) 分布式账本

分布式账本是区块链技术的核心之一。分布式账本的核心思想是：交易记账由分布在不同地方的多个节点共同完成，而且每一个节点保存一个唯一、真实账本的副本，它们可以参与监督交易合法性，同时也可以共同为其作证；账本里的任何改动都会在所有的副本中被反映出来，反应时间会在几分钟甚至是几秒内，记账节点足够多，理论上除非所有的节点被破坏，所有整个分布式账本系统是非常稳健的，从而保证了账目数据的安全性。

分布式账本中存储的资产是指法律认可的合法资产，如金融、实体、电子的资产等任何形式的有价资产。为了确保资产的安全性和准确性，分布式账本一方面通过公私钥以及签名控制账本的访问权；另一方面根据共识的规则，账本中的信息更新可以由一个、一部分人或者是所

有参与者共同完成。

分布式账本技术能够保障资产的安全性和准确性，具有广泛的应用场景，特别在公共服务领域，能够重新定义政府与公民在数据分享、透明度和信任意义上的关系，目前已经广泛应用于金融交易、政府征税、土地所有权登记、护照管理、社会福利等领域。

2) 加密算法

区块数据的加密是区块链研究和关注的重点，其主要作用是保证区块数据在网络传输、存储和修改过程中的安全。区块链系统中的加密算法一般分为散列（哈希）算法和非对称加密算法。

散列算法也叫数据摘要或者哈希算法，其原理是将一段信息转换成一个固定长度并具备以下特点的字符串：如果某两段信息是相同的，那么字符也是相同的；即使两段信息十分相似，但只要是不同的，那么字符串将会十分杂乱、随机并且两个字符串之间完全没有关联。

本质上，散列算法的目的不是为了“加密”而是为了抽取“数据特征”，也可以把给定数据的散列值理解为该数据的“指纹信息”。典型的散列算法有 MD5、SHA-1/SHA-2 和 SM3，目前区块链主要使用 SHA-2 中的 SHA256 算法。

非对称加密算法由对应的一对唯一性密钥（即公开密钥和私有密钥）组成的加密方法。任何获悉用户公钥的人都可用用户的公钥对信息进行加密与用户实现安全信息交互。由于公钥与私钥之间存在的依存关系，只有用户本身才能解密该信息，任何未受授权用户甚至信息的发送者都无法将此信息解密。常用的非对称加密算法包括 RSA、Elgamal、D-H、ECC（椭圆曲线加密算法）等。

3) 共识机制

在区块链的典型应用——数字货币中，面临着一系列安全和管理问题，例如：如何防止诈骗？区块数据传输到各个分布式节点的先后次序如何控制？如何应对传输过程中数据的丢失问题？节点如何处理错误或伪造的信息？如何保障节点之间信息更新和同步的一致性？这些问题就是所谓的区块链共识问题。

区块链共识问题需要通过区块链的共识机制来解决。在互联网世界，共识主要是计算机和软件程序协作一致的基本保障，是分布式系统节点或程序运行的基本依据。共识算法能保证分布式的计算机或软件程序协作一致，对系统的输入输出做出正确的响应。

区块链的共识机制的思想是：在没有中心点总体协调的情况下，当某个记账节点提议区块数据增加或减少，并把该提议广播给所有的参与节点，所有节点要根据一定的规则和机制，对这一提议是否能够达成一致进行计算和处理。

目前，常用的共识机制主要有 PoW、PoS、DPoS、Paxos、PBFT 等。根据区块链不同应用场景中各种共识机制的特性，共识机制分析可基于：

- 合规监管：是否支持超级权限节点对全网节点、数据进行监管。
- 性能效率：交易达成共识被确认的效率。
- 资源消耗：共识过程中耗费的CPU、网络输入输出、存储等资源。
- 容错性：防攻击、防欺诈的能力。

3. 应用和发展

当前，TCP/IP 协议是全球互联网的“牵手协议”。将“多中心化、分布式”理念变成了一种可执行的程序，并在此基础上派生出了更多的类似协议。然而，回顾互联网技术的发展，当前的互联网技术成功实现了信息的多中心化，但却无法实现价值的多中心化。换句话说，互联网上能多中心化的活动是无需信用背书的活动，需要信用做保证的都是中心化的、有第三方中介机构参与的活动。因此，无法建立全球信用的互联网技术就在发展中遇到了障碍——人们无法在互联网上通过多中心化方式参与价值交换活动。

从区块链技术研究角度看：①在共识机制方面，如何解决公有链、私有链、联盟链的权限控制、共识效率、约束、容错率等方面的问题，寻求针对典型场景的、具有普适性的、更优的共识算法及决策将是研究的重点；②在安全算法方面，目前采用的算法大多数是传统的安全类算法，存在潜在的“后门”风险，算法的强度也需要不断升级；另外，管理安全、隐私保护、监管缺乏以及新技术（如量子计算）所带来的安全问题需要认真对待；③在区块链治理领域，如何结合现有信息技术治理体系的研究，从区块链的战略、组织、架构以及区块链应用体系的各个方面，研究区块链实施过程中的环境与文化、技术与工具、流程与活动等问题，进而实现区块链的价值，开展相关区块链的审计，是区块链治理领域需要核心关注的问题；④在技术日益成熟的情况下，研究区块链的标准化，也是需要重要考虑的内容。

(1) 区块链将成为互联网的基础协议之一。本质上，互联网同区块链一样，也是个多中心化的网络，并没有一个“互联网的中心”存在。不同的是，互联网是一个高效的信息传输网络，并不关心信息的所有权，没有内生的、对有价值信息的保护机制；区块链作为一种可以传输所有权的协议，将会基于现有的互联网协议架构，构建出新的基础协议层。从这个角度看，区块链（协议）会和传输控制协议/因特网互联协议（TCP/IP）一样，成为未来互联网的基础协议，构建出一个高效的、多中心化的价值存储和转移网络。

(2) 区块链架构的不同分层将承载不同的功能。类似 TCP/IP 协议栈的分层结构，人们在统一的传输层协议之上，发展出了各种各样的应用层协议，最终构建出了今天丰富多彩的互联网。未来区块链结构也将在一个统一的、多中心化的底层协议基础上，发展出各种各样应用层协议。

(3) 区块链的应用和发展呈螺旋式上升趋势。如同互联网的发展一样，在发展过程中会经历过热甚至泡沫阶段，并以颠覆式的技术改变融合传统产业。区块链作为数字化浪潮中下一个阶段的核心技术，其发展周期将比预想得要长，影响的范围和深度也会远远超出人们的想象，将会构建出多样化生态的价值互联网，从而深刻改变未来商业社会的结构和个人的生活。

2.2.5 人工智能

人工智能是指研究和开发用于模拟、延伸和扩展人类智能的理论、方法、技术及应用系统的一门技术科学。这一概念自 1956 年被提出后，已历经半个多世纪的发展和演变。21 世纪初，随着大数据、高性能计算和深度学习技术的快速迭代和进步，人工智能进入新一轮的发展热潮，

其强大的赋能性对经济发展、社会进步、国际政治经济格局等产生了重大且深远的影响，已成为新一轮科技革命和产业变革的重要驱动力量。

1. 技术基础

人工智能从产生到现在，其发展历程经历了6个主要阶段：起步发展期（1956年至20世纪60年代初）、反思发展期（20世纪60年代至20世纪70年代初）、应用发展期（20世纪70年代初至20世纪80年代中）、低迷发展期（20世纪80年代中至20世纪90年代中）、稳步发展期（20世纪90年代中至2010年）、蓬勃发展期（2011年至今）。

从当前的人工智能技术进行分析可知，其在技术研究方面主要聚焦在热点技术、共性技术和新兴技术三个方面。其中以机器学习为代表的基础算法的优化改进和实践，以及迁移学习、强化学习、多核学习和多视图学习等新型学习方法是研究探索的热点；自然语言处理相关的特征提取、语义分类、词嵌入等基础技术和模型研究，以及智能自动问答、机器翻译等应用研究也取得诸多的成果；以知识图谱、专家系统为逻辑的系统化分析也在不断地取得突破，大大拓展了人工智能的应用场景，对人工智能未来的发展具有重要的潜在影响。

2. 关键技术

人工智能的关键技术主要涉及机器学习、自然语言处理、专家系统等技术，随着人工智能应用的深入，越来越多新兴的技术也在快速发展中。

1) 机器学习

机器学习是一种自动将模型与数据匹配，并通过训练模型对数据进行“学习”的技术。机器学习的研究主要聚焦在机器学习算法及应用、强化学习算法、近似及优化算法和规划问题等方面，其中常见的学习算法主要包含回归、聚类、分类、近似、估计和优化等基础算法的改进研究，迁移学习、多核学习和多视图学习等强化学习方法是当前的研究热点。

神经网络是机器学习的一种形式，该技术出现在20世纪60年代，并用于分类型应用程序。它根据输入、输出、变量权重或将输入与输出关联的“特征”来分析问题。它类似于神经元处理信号的方式。深度学习是通过多等级的特征和变量来预测结果的神经网络模型，得益于当前计算机架构更快的处理速度，这类模型有能力应对成千上万个特征。与早期的统计分析形式不同，深度学习模型中的每个特征通常对于人类观察者而言意义不大，使得该模型的使用难度很大且难以解释。深度学习模型使用一种称为反向传播的技术，通过模型进行预测或对输出进行分类。强化学习是机器学习的另外一种方式，指机器学习系统制订了目标而且迈向目标的每一步都会得到某种形式的奖励。

机器学习模型是以统计为基础的，而且应该将其与常规分析进行对比以明确其价值增量。它们往往比基于人类假设和回归分析的传统“手工”分析模型更准确，但也更复杂和难以解释。相比于传统的统计分析，自动化机器学习模型更容易创建，而且能够揭示更多的数据细节。

2) 自然语言处理

自然语言处理（Natural Language Processing, NLP）是计算机科学领域与人工智能领域中的一个重要方向。它研究能实现人与计算机之间用自然语言进行有效通信的各种理论和方法。自

然语言处理是一门融语言学、计算机科学、数学于一体的科学。因此，这一领域的研究将涉及自然语言，即人们日常使用的语言，所以它与语言学的研究有着密切的联系，但又有重要的区别。自然语言处理并不是一般地研究自然语言，而在于研制能有效地使用自然语言通信的计算机系统，特别是其中的软件系统。因而它是计算机科学的一部分。

自然语言处理主要应用于机器翻译、舆情监测、自动摘要、观点提取、文本分类、问题回答、文本语义对比、语音识别、中文OCR等方面。

自然语言处理（即实现人机间自然语言通信，或实现自然语言理解和自然语言生成）是十分困难的，困难的根本原因是自然语言文本和对话的各个层次上广泛存在着各种各样的歧义性或多义性。自然语言处理解决的核心问题是信息抽取、自动文摘/分词、识别转化等，用于解决内容的有效界定、消歧和模糊性、有瑕疵的或不规范的输入、语言行为理解和交互。当前，深度学习技术是自然语言处理的重要技术支撑，在自然语言处理中需应用深度学习模型，如卷积神经网络、循环神经网络等，通过对生成的词向量进行学习，以完成自然语言分类、理解的过程。

3) 专家系统

专家系统是一个智能计算机程序系统，通常由人机交互界面、知识库、推理机、解释器、综合数据库、知识获取等6个部分构成，其内部含有大量的某个领域专家水平的知识与经验，它能够应用人工智能技术和计算机技术，根据系统中的知识与经验，进行推理和判断，模拟人类专家的决策过程，以便解决那些需要人类专家处理的复杂问题。简而言之，专家系统是一种模拟人类专家解决领域问题的计算机程序系统。

在人工智能的发展过程中，专家系统的发展已经历了三个阶段，正向第四代过渡和发展。第一代专家系统以高度专业化、求解专门问题的能力强为特点。但在体系结构的完整性、可移植性、系统的透明性和灵活性等方面存在缺陷，求解问题的能力弱。第二代专家系统属于单学科专业型、应用型系统，其体系结构较完整，移植性方面也有所改善，而且在系统的人机接口、解释机制、知识获取技术、不确定推理技术、增强专家系统的知识表示和推理方法的启发性、通用性等方面都有所改进。第三代专家系统属多学科综合型系统，采用多种人工智能语言，综合采用各种知识表示方法和多种推理机制及控制策略，并运用各种知识工程语言、骨架系统及专家系统开发工具和环境来研制大型综合专家系统。

当前人工智能的专家系统研究已经进入到第四个阶段，主要研究大型多专家协作系统、多种知识表示、综合知识库、自组织解题机制、多学科协同解题与并行推理、专家系统工具与环境、人工神经网络知识获取及学习机制等。

3. 应用和发展

经过60多年的发展，人工智能在算法、算力（计算能力）和算料（数据）等方面取得了重要突破，正处于从“不能用”到“可以用”的技术拐点，但是距离“很好用”还存在诸多瓶颈。实现从专用人工智能向通用人工智能的跨越式发展，既是下一代人工智能发展的必然趋势，也是研究与应用领域的重大挑战，是未来应用和发展的趋势。

(1) 从人工智能向人机混合智能发展。借鉴脑科学和认知科学的研究成果是人工智能的一

一个重要研究方向。人机混合智能旨在将人的作用或认知模型引入到人工智能系统中，提升人工智能系统的性能，使人工智能成为人类智能的自然延伸和拓展，通过人机协同更加高效地解决复杂问题。

(2) 从“人工+智能”向自主智能系统发展。当前人工智能领域的大量研究集中在深度学习，但是深度学习的局限是需要大量人工干预，比如人工设计深度神经网络模型、人工设定应用场景、人工采集和标注大量训练数据、用户需要人工适配智能系统等，非常费时费力。因此，科研人员开始关注减少人工干预的自主智能方法，提高机器智能对环境的自主学习能力。

(3) 人工智能将加速与其他学科领域交叉渗透。人工智能本身是一门综合性的前沿学科和高度交叉的复合型学科，研究范畴广泛而又异常复杂，其发展需要与计算机科学、数学、认知科学、神经科学和社会科学等学科深度融合。借助于生物学、脑科学、生命科学和心理学等学科的突破，将机理变为可计算的模型，人工智能将与更多学科深入地交叉渗透。

(4) 人工智能产业将蓬勃发展。随着人工智能技术的进一步成熟以及政府和产业界投入的日益增长，人工智能应用的云端化将不断加速，全球人工智能产业规模在未来10年将进入高速增长期。“人工智能+X”的创新模式将随着技术和产业的发展日趋成熟，对生产力和产业结构产生革命性影响，并推动人类进入普惠型智能社会。

(5) 人工智能的社会学将提上议程。为了确保人工智能的健康可持续发展，使其发展成果造福于民，需要从社会学的角度系统全面地研究人工智能对人类社会的影响，制定完善人工智能法律法规，规避可能的风险，旨在“以有利于整个人类的方式促进和发展友好的人工智能”。

2.2.6 虚拟现实

自从计算机创造以来，计算机一直是传统信息处理环境的主体，这与人类认识空间及计算机处理问题的信息空间存在不一致的矛盾，如何把人类的感知能力和认知经历及计算机信息处理环境直接联系起来，是虚拟现实产生的重大背景。如何建立一个能包容图像、声音、化学气味等多种信息源的信息空间，将其与视觉、听觉、嗅觉、口令、手势等人类的生活空间交叉融合，虚拟现实的技术应运而生。

1. 技术基础

虚拟现实（Virtual Reality, VR）是一种可以创立和体验虚拟世界的计算机系统（其中虚拟世界是全体虚拟环境的总称）。通过虚拟现实系统所建立的信息空间，已不再是单纯的数字信息空间，而是一个包容多种信息的多维化的信息空间（Cyberspace），人类的感性认识和理性认识能力都能在这个多维化的信息空间中得到充分的发挥。要创立一个能让参与者具有身临其境感，具有完善交互作用能力的虚拟现实系统，在硬件方面，需要高性能的计算机软硬件和各类先进的传感器；在软件方面，主要是需要提供一个能产生虚拟环境的工具集。

虚拟现实技术的主要特征包括沉浸性、交互性、多感知性、构想性（也称想象性）和自主性。随着虚拟现实技术的快速发展，按照其“沉浸性”程度的高低和交互程度的不同，虚拟现实技术已经从桌面虚拟现实系统、沉浸式虚拟现实系统、分布式虚拟现实系统等，向着增强式

虚拟现实系统（Augmented Reality，AR）和元宇宙的方向发展。

2. 关键技术

虚拟现实的关键技术主要涉及人机交互技术、传感器技术、动态环境建模技术和系统集成技术等。

1) 人机交互技术

虚拟现实中的人机交互技术与传统的只有键盘和鼠标的交互模式不同，是一种新型的利用VR眼镜、控制手柄等传感器设备，能让用户真实感受到周围事物存在的一种三维交互技术，将三维交互技术与语音识别、语音输入技术及其他用于监测用户行为动作的设备相结合，形成了目前主流的人机交互手段。

2) 传感器技术

VR技术的进步受制于传感器技术的发展，现有的VR设备存在的缺点与传感器的灵敏程度有很大的关系。例如VR头显（即VR眼镜）设备过重、分辨率低、刷新频率慢等，容易造成视觉疲劳；数据手套等设备也都有延迟长、使用灵敏度不够的缺陷，所以传感器技术是VR技术更好地实现人机交互的关键。

3) 动态环境建模技术

虚拟环境的设计是VR技术的重要内容，该技术是利用三维数据建立虚拟环境模型。目前常用的虚拟环境建模工具为计算机辅助设计（Computer Aided Design，CAD），操作者可以通过CAD技术获取所需数据，并通过得到的数据建立满足实际需要的虚拟环境模型。除了通过CAD技术获取三维数据，多数情况下还可以利用视觉建模技术，两者相结合可以更有效地获取数据。

4) 系统集成技术

VR系统中的集成技术包括信息同步、数据转换、模型标定、识别和合成等技术，由于VR系统中储存着许多的语音输入信息、感知信息以及数据模型，因此VR系统中的集成技术显得越发重要。

3. 应用和发展

(1) 硬件性能优化迭代加快。轻薄化、超清化加速了虚拟现实终端市场的迅速扩大，开启了虚拟现实产业爆发增长的新空间，虚拟现实设备的显示分辨率、帧率、自由度、延时、交互性能、重量、眩晕感等性能指标日趋优化，用户体验感不断提升。

(2) 网络技术的发展有效助力其应用化的程度。泛在网络通信和高速的网络速度，有效提升了虚拟现实技术在应用端的体验。借助于终端轻型化和移动化5G技术，高峰值速率、毫秒级的传输时延和千亿级的连接能力，降低了对虚拟现实终端侧的要求。

(3) 虚拟现实产业要素加速融通。技术、人才多维并举，虚拟现实产业核心技术不断取得突破，已形成较为完整的虚拟现实产业链条。虚拟现实产业呈现出从创新应用到常态应用的产业趋势，在舞台艺术、体育智慧观赛、新文化弘扬、教育、医疗等领域普遍应用。“虚拟现实+商贸会展”成为后疫情时代的未来新常态，“虚拟现实+工业生产”是组织数字化转型的新动

能，“虚拟现实+智慧生活”大大提升了未来智能化的生活体验，“虚拟现实+文娱休闲”成为新型信息消费模式的新载体等。

(4) 元宇宙等新兴概念为虚拟现实技术带来了“沉浸和叠加”“激进和渐进”“开放和封闭”等新的商业理念，大大提升了其应用价值和社会价值，将逐渐改变人们所习惯的现实世界物理规则，以全新方式激发产业技术创新，以新模式、新业态等方式带动相关产业跃迁升级。

2.3 本章练习

1. 选择题

(1) 关于信息技术的描述，不正确的是_____。

- A. 信息技术是研究如何获取信息、处理信息、传输信息和使用信息的技术
- B. 信息技术是信息系统的前提和基础，信息系统是信息技术的应用和体现
- C. 信息、信息化以及信息系统都是信息技术发展不可或缺的部分
- D. 信息技术是在信息科学的基本原理和方法下的关于一切信息的产生、信息的传输、信息的转化应用技术的总称

参考答案：D

(2) _____关键技术主要涉及传感器技术、传感网和应用系统架构等。

- A. 物联网
- B. 云计算
- C. 大数据
- D. 人工智能

参考答案：A

(3) _____关键技术主要涉及机器学习、自然语言处理、专家系统等技术。

- A. 物联网
- B. 云计算
- C. 大数据
- D. 人工智能

参考答案：D

(4) 关于云计算的描述，不正确的是_____。

- A. 云计算可以通过宽带网络连接，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高速网络相连
- B. 云计算可以快速、按需、弹性服务，用户可以按照实际需求迅速获取或释放资源，并可以根据需求对资源进行动态扩展
- C. 按照云计算服务提供的资源层次，可以分为基础设施即服务和平台即服务两种服务类型
- D. 云计算是一种基于并高度依赖 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

参考答案：C

(5) 区块链有以下几种特性：多中心化、多方维护、时序数据、智能合约、开放共识、安全可信和_____。

- A. 可回溯性
- B. 不可篡改
- C. 周期性
- D. 稳定性

参考答案：B

(6) 虚拟现实技术的主要特征包括：沉浸性、交互性、多感知性、构想性和_____。

- A. 自主性
- B. 抗否认性
- C. 可审计性
- D. 可靠性

参考答案：A

2. 思考题

(1) 请概述云计算的主要服务模式有哪些。

参考答案：略

(2) 请简述大数据的技术架构是什么。

参考答案：略

(3) 请简述区块链的共识机制。

参考答案：略

第3章 信息系统治理

信息系统治理（IT 治理）是组织开展信息技术及其应用活动的重要管控手段，也是组织治理的重要组成部分，尤其在以数字化发展为重要关注点的新时代，组织的数字化转型和组织建设过程中，IT 治理起到重要的统筹、评估、指导和监督作用。信息技术审计（IT 审计）作为与 IT 治理配套的组织管控手段，是 IT 治理不可或缺的评估和监督工具，重点承担着组织信息系统发展的合规性检测以及信息技术风险的管控等职能。

3.1 IT 治理

新时代的信息技术与各领域发展进入到了深度融合的发展新阶段，成为各类组织实现治理体系与能力现代化，构建敏捷运行管理体系，打造高质量的生产与服务系统，洞察社会与市场变化等高质量发展的必要过程。组织如何从其信息系统投资中获得真正的价值；如何将信息技术战略与组织战略相融合；如何从组织治理的高度，对组织数字化能力做出制度安排；如何从战略投资、组织管理变革的角度，降低 IT 的风险；如何利用国内外信息技术开发利用的最佳实践和重要成果，加快组织的信息化、数字化工作推进等。这些都是 IT 治理所关注的问题。

3.1.1 IT 治理基础

IT 治理是描述组织采用有效的机制对信息技术和数据资源开发利用，平衡信息化发展和数字化转型过程中的风险，确保实现组织的战略目标的过程。

1. IT 治理的驱动因素

组织信息系统建设和运行需要制订总体规划，但制订 IT 资源统一规划存在很多问题：①信息系统应用已有相当的基础，但多年来分散开发或引进的信息系统，形成了许多“信息孤岛”，缺乏共享的、网络化的信息资源，系统集成难题一直无法解决；②信息资源整合目标空泛，没有整合“信息孤岛”的措施，数据中心建设和数据集中管理等规划缺乏可操作性，尤其是缺少数据标准化建设方面的建设规划。这些问题的出现，表明组织在 IT 资源方面没有做到有效统一规划，如何解决这些问题成为了组织发展的一个重要课题。

IT 资产作为组织资产的重要组成部分，IT 治理自然就是组织治理结构中不可分割的一部分。IT 治理是指组织在开发利用信息技术过程中，为鼓励组织所期望的组织行为而明确决策权归属和责任担当的框架，其目标是通过 IT 治理的决策权和责任影响组织所期望的组织行为。随着新时代的发展，数字特征成为组织发展的一项关键特征，组织的高质量发展对 IT 的依赖越来越强，IT 治理对组织愈发重要，为确保 IT 治理的有效，组织高层管理者需要投入越来越多的时间和精力。

随着组织在 IT 方面的投资越来越大，组织的 IT 战略要与组织战略相一致，才能确保组织核心竞争力的建设与保持；要尽可能地保持开放性和长远性，以确保系统的稳定性和延续性；

要认真分析组织的战略与IT支撑之间的影响度，并合理预测环境变化可能给组织战略带来的偏移，在规划时留有适当的余地。组织目标变化太快，很难保证IT与组织目标始终保持一致，因此需要多方面的协调，保证IT治理继续沿着正确的方向走，这也是IT投资者真正关心的问题。IT治理要从组织目标和数字战略中抽取信息需求和功能需求，形成总体的IT治理框架和系统整体模型，为进一步系统设计和实施奠定基础，保证信息技术开发应用符合持续变化的业务目标。

高质量的IT治理能够使组织的IT管理和应用决策与组织期望的行为和业务目标相一致，这就需要组织IT治理机构对组织IT发展进行科学规划并确保其有效实施。驱动组织开展高质量IT治理因素包括：①良好的IT治理能够确保组织IT投资有效性；②IT属于知识高度密集型领域，其价值发挥的弹性较大；③IT已经融入组织管理、运行、生产和交付等各领域中，成为各领域高质量发展的重要基础；④信息技术的发展演进以及新兴信息技术的引入，可为组织提供大量新的发展空间和业务机会等；⑤IT治理能够推动组织充分理解IT价值，从而促进IT价值挖掘和融合利用；⑥IT价值不仅仅取决于好的技术，也需要良好的价值管理，场景化的业务融合应用；⑦高级管理层的管理幅度有限，无法深入到IT每项管理当中，需要采用明确责权利和清晰管理去确保IT价值；⑧成熟度较高的组织以不同的方式治理IT，获得了领域或行业领先的业务发展效果。

IT治理的内涵主要体现在5个方面：①IT治理作为组织上层管理的一个有机组成部分，由组织治理层或高级管理层负责，从组织全局的高度上对组织信息化与数字化转型做出制度安排，体现了治理层和最高管理层对信息相关活动的关注；②IT治理强调数字目标与组织战略目标保持一致，通过对IT的综合开发利用，为组织战略规划提供技术或控制方面的支持，以保证相关建设能够真正落实并贯彻组织业务战略和目标；③IT治理保护利益相关者的权益，对风险进行有效管理，合理利用IT资源，平衡成本和收益，确保信息系统应用有效、及时地满足需求，并获得期望的收益，增强组织的核心竞争力；④IT治理是一种制度和机制，主要涉及管理和制衡信息系统与业务战略匹配、信息系统建设投资、信息系统安全和信息系统绩效评价等方面的内容；⑤IT治理的组成部分包括管理层、组织结构、制度、流程、人员、技术等多个方面，共同构建完善的IT治理架构，达到数字战略和支持组织的目标。

2. IT治理的目标价值

组织治理驱动和调整IT治理。同时，IT治理能够提供关键的输入，成为战略计划的一个重要组成部分，是组织治理的一个重要功能。IT治理将帮助组织建立以组织战略为导向、以实现IT与业务匹配为重心、以价值交付为成果、以绩效管理为控制手段的IT管理体制，正确定位IT团队在整个组织的作用，最终能够针对不同业务发展要求，统一规划IT资源、整合信息资源、有效规避风险、制定并执行组织发展战略。IT治理就是要明确有关IT决策权的归属机制和有关IT责任的承担机制，以鼓励IT应用的期望行为的产生，以联接战略目标、业务目标和IT目标，从而使组织从IT中获得最大的价值。组织实施IT治理的使命通常包括：保持IT与业务目标一致，推动业务发展，促使收益最大化，合理利用IT资源，恰当理清与IT相关的风险等。

IT治理主要目标包括：与业务目标一致、有效利用信息与数据资源、风险管理。

(1) 与业务目标一致。IT治理要从组织目标和数字战略中抽取信息与数据需求和功能需求，形成总体的IT治理框架和系统整体模型，为进一步系统设计和实施奠定基础，保证信息技术开

发利用跟上持续变化的业务目标。

(2) 有效利用信息与数据资源。目前信息系统工程超期、IT客户的需求没有满足、IT平台不支持业务应用、数据开发利用效能与价值不高、信息技术与业务发展融合深度不够等问题突出，通过IT治理对信息与数据资源的管理职责进行有效管理，保证投资的回收，并支持决策。

(3) 风险管理。由于组织越来越依赖于信息网络、信息系统和数据资源等，新的风险不断涌现，例如，新出现的技术没有管理，不符合现有法律和规章制度，没有识别对IT服务的威胁等。IT治理重视风险管理，通过制定信息与数据资源的保护级别，强调对关键的信息与数据资源，实施有效监控和事件处理。

3. IT治理的管理层次

IT治理要保证总体战略目标能够从上而下贯彻执行，治理层主要集中在最高管理层（如董事会）和管理执行层。然而，由于IT治理的复杂性和专业性，治理层必须依赖组织的基层来提供决策和评估所需要的信息。基层依据组织总体目标采用相关的原则，提供评估业绩的衡量方法。因此，好的IT治理实践需要在组织全部范围内推行。管理层次大致可分为三层：最高管理层、执行管理层、业务与服务执行层。

最高管理层的主要职责包括：证实IT战略与业务战略是否一致；证实通过明确的期望和衡量手段交付IT价值；指导IT战略、平衡支持组织当前和未来发展的投资；指导信息和数据资源的分配。执行管理层的主要职责包括：制定IT的目标；分析新技术的机遇和风险；建设关键过程与核心竞争力；分配责任、定义规程、衡量业绩；管理风险和获得可靠保证等。业务及服务执行层的主要职责包括：信息和数据服务的提供和支持；IT基础设施的建设和维护；IT需求的提出和响应。

3.1.2 IT治理体系

IT治理用于描述组织在信息化建设和数字化转型过程中是否采用有效的机制使得信息技术开发利用能够完成组织赋予它的使命。IT治理的核心是关注IT定位和信息化建设与数字化转型的责权利划分，如图3-1所示。IT治理体系的具体构成包括IT定位：IT应用的期望行为与业务目标一致；IT治理架构：业务和IT在治理委员会中的构成、组织IT与各分支机构的IT权责边界等；IT治理内容：投资、风险、绩效、标准和规范等；IT治理流程：统筹、评估、指导、监督；IT治理效果（内外评价）等。

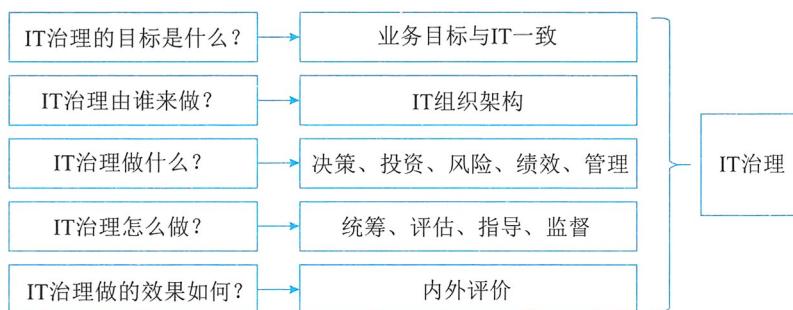


图3-1 IT治理体系的构成

1. IT 治理关键决策

有效的 IT 治理必须关注五项关键决策，如图 3-2 所示，包括 IT 原则、IT 架构、IT 基础设施、业务应用需求、IT 投资和优先顺序。IT 原则驱动着 IT 整体架构的形成，而 IT 整体架构又决定了基础设施，这种基础设施所确定的能力又决定着基于业务需求应用的构建，最后，IT 投资和优先顺序必须为 IT 原则、整体架构、基础设施和应用需求所驱动。然而，这些决策中又有独特问题，即 IT 治理需要确定每个决策由谁来负责输入，以及由谁来负责做出决策。

| IT 原则的决策 | | 组织高层关于如何使用 IT 的陈述 |
|--|--|--|
| IT 架构的决策 | 业务应用需求决策 | IT 投资和优先顺序决策 |
| 组织从一系列政策、关系以及技术选择中捕获的数据、应用和基础设施的逻辑，以达到预期和商业、技术的标准化和一体化 | 为购买或内部开发 IT 应用确定业务需求 IT 基础设施决策 集中协调、共享 IT 服务可以给组织的 IT 能力提供基础 | 关于应该在 IT 的哪些方面投资以及投资多少的决策，包括项目的审批和论证技术 |

图 3-2 关键的 IT 治理决策

IT 决策过程中，需要关注各类关键问题，如图表 3-1 所示。

表 3-1 IT 决策的关键问题

| 关键决策 | 关键问题 |
|------------|---|
| IT 原则 | 组织的运行模型是什么？IT 在业务中的角色是什么？IT 期望行为是什么？如何投资 IT |
| IT 架构 | 组织的核心业务流程是什么？它们之间有什么样的关系？哪些信息在驱动着这些核心流程？数据必须如何整合？哪些技术性能应当在组织范围内得到标准化，以支持 IT 效率，方便流程标准化和整合？哪些行为应当在组织范围内标准化以支持数据整合？哪些技术选择能够指引组织 IT 新计划的方法 |
| IT 基础设施 | 哪些基础设施对实现组织的战略目标来说是最关键的？对于每个能力集，哪些基础设施服务应该在组织级实现，这些服务的水平需求是什么？应当如何定价基础设施服务？如何保持基础技术的不断更新？哪些基础设施服务应当外包 |
| 业务应用需求 | 新业务应用的市场和业务流程机会是什么？如何设计实验以评估业务应用成功与否？如何在架构标准上满足业务需求？应当在什么时候将一个业务需求从例外转换为标准？谁拥有每个项目的成果并且发起组织变革以确保其价值 |
| IT 投资和优先顺序 | 哪些流程变革或者强化对组织来说在战略上是最重要的？当前的以及在提议中的 IT 投资组合是如何分配的？这些投资组合同组织的战略目标一致吗？组织级的投资相对于业务单位的投资哪个更重要？实际投资情况会影响它们的相对重要性吗 |

2. IT 治理体系框架

IT 治理体系框架是实现组织 IT 治理的有效保障，缺乏良好的 IT 治理体系框架，IT 治理的过程将会变得盲目和无序。IT 治理体系框架以组织的战略目标为导向，架起了组织战略与 IT 的

桥梁，实现了 IT 风险的全面管理以及 IT 资源的合理利用。IT 治理体系框架具体包括：IT 战略目标、IT 治理组织、IT 治理机制、IT 治理域、IT 治理标准和 IT 绩效目标等部分，形成一整套 IT 治理运行闭环，如图 3-3 所示。



图 3-3 IT 治理体系框架

(1) IT 战略目标。IT 战略目标是指为实现 IT 价值和目标，使组织从 IT 投入中获得最大收益，而针对 IT 与业务关系、IT 决策、IT 资源利用、IT 风险控制等方面制定的目标。

(2) IT 治理组织。IT 治理组织是界定组织中各相关主体在各自方面的治理范围、责权利及其相互关系的准则，它的核心是治理机构（如 IT 治理委员会等）的设置和权限的划分。各治理机构职权的分配以及各机构间的相互协调，它的强弱直接影响到治理的效率和效能，对 IT 治理效率起着决定性的作用。

(3) IT 治理机制。IT 治理机制是 IT 治理决策机制、执行机制、风险控制机制、协调机制的综合体，各机制之间是相辅相成、相互促进的关系。有效的决策机制能保障 IT 决策与组织的业绩目标和战略目标相匹配；有效的执行机制能保证 IT 治理的良好运作，有效的风险控制机制能降低 IT 活动的风险，实现信息技术开发利用的价值效益；有效的协调机制能有力地发挥 IT 治理的协调效应。

(4) IT 治理域。IT 治理域是在 IT 治理的规则之下，对组织的 IT 资源进行整合与配置，根据 IT 目标所采取的行动。以科学、规范的做法交付面向业务的高质量 IT 服务，确保信息化“高效做事情”、数字化“敏捷的决策”。IT 治理域内容包括 IT 信息系统的计划、构建、运维与监控等。

(5) IT 治理标准。IT 治理标准包括 IT 治理基本规范、IT 治理实施参照、IT 治理评价体系和 IT 治理审计方法等方面，作为组织实施 IT 治理最佳实践和对标依据。

(6) IT 绩效目标。IT 绩效目标关注 IT 价值的实现，评价 IT 规划与 IT 构建过程中是否满足业务需求以及构建过程中的工期、成本、质量是否达到目标。

3. IT 治理核心内容

IT 治理本质上关心：①实现 IT 的业务价值；②IT 风险的规避。前者是通过 IT 与业务战略

匹配来实现的，后者通过在组织内部建立相关职责来实现。两者都需要相关资源的支持，并对其绩效进行有效度量。IT 治理的核心内容包括六个方面：组织职责、战略匹配、资源管理、价值交付、风险管理、绩效管理，如图 3-4 所示。

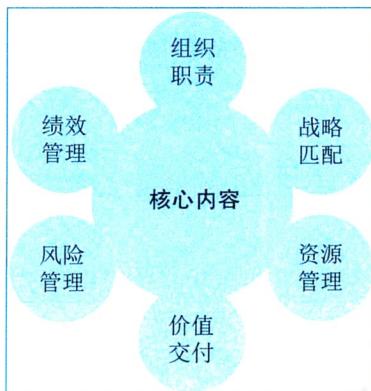


图 3-4 IT 治理核心内容

(1) 组织职责。组织职责指组织参与 IT 决策与管理的所有人员的集合，明确组织信息部门和业务部门之间的关系和责任，正确划分信息系统的所有者、建设者、管理者和监控者。

(2) 战略匹配。IT 治理的一个重要内容，是使组织的 IT 建设与组织战略相匹配，也就是通常所说的“战略匹配”。而战略匹配是 IT 为组织贡献业务价值的重要驱动力。

(3) 资源管理。资源管理的主要功能是确保用户对组织的应用系统和基础设施都有良好的理解和应用，优化 IT 投资、IT 资源（人、应用系统、信息、基础设施）的分配，做好人员的培训、发展计划，以满足组织的业务需求。

(4) 价值交付。通过对 IT 项目全生命周期的管理，确保 IT 能够按照组织战略实现预期的业务价值。重点是对整个交付周期成本的控制和 IT 业务价值的实现，使 IT 项目能够在预算时间、成本范围内，按预定的质量要求完成。价值交付即是创造业务价值。

(5) 风险管理。风险管理是 IT 治理中非常重要的内容。风险管理是确保 IT 资产的安全和灾难的恢复、组织信息资源的安全以及人员的隐私安全。风险管理即是保护业务价值。

(6) 绩效管理。没有绩效管理 IT 治理中任何一个域都不可能有效地进行管理。绩效管理主要是追踪和监视 IT 战略、IT 项目的实施、信息资源的使用、IT 服务的提供以及业务流程的绩效。绩效管理所采用的工具，如平衡积分卡，可以将组织的战略目标转化成各个职能部门或团队具体的业务活动的目标，从而保证组织战略目标的实现。

4. IT 治理机制经验

建立 IT 治理机制的原则包括：①简单。机制应该明确地定义特定个人和团体所承担的责任和目标。②透明。有效的机制依赖于正式的程序。对于那些被治理决策所影响或是想要挑战治理决策的人来说，机制如何工作是需要非常清晰的。③适合。机制鼓励那些处于最佳位置的个人去制定特定的决策。

影响力高且具有挑战性的 IT 治理机制，如表 3-2 所示。

表 3-2 影响力高且具有挑战性的 IT 治理机制

| 机制 | 目标 | 期望行为 | 不期望行为 |
|----------------|--------------------------------|---------------|-----------------------------|
| 执行层和高级管理委员会 | 对业务包括 IT 的整体观念 | 整合 IT 的无缝管理 | IT 被忽略 |
| 架构委员会 | 明确战略技术和标准是否被执行 | 业务驱动的 IT 决策制定 | IT 限制和延迟 |
| 有 IT 人员参与的流程团队 | 有效地运用 IT 视角 | 端对端的流程管理 | 功能性技能的停滞和分散的 IT 基础设施 |
| 资金投资批准和预算 | 把 IT 看作另一种业务投资 | 对于不同投资类型的不同方法 | 分析瘫痪小项目，避开了正式批准 |
| 服务水平协议 | 对于 IT 服务的详细说明和衡量 | 专业的供应和需求 | 管理服务水平协议而不是业务需求 |
| 费用分摊机制 | 从业务中补偿 IT 成本 | IT 的可靠应用 | 关于收费和歪曲的需求的争论 |
| IT 业务价值的正式追踪 | 衡量 IT 投资，并通常运用平衡记分卡计算其对业务价值的贡献 | 使目标、利益和成本透明化 | 将 IT 同其他资产相分离，只关注资金流，而不关注价值 |

IT 治理可以从众多最佳实践中学习的经验主要包括：

- IT 指导委员会要吸纳有才干的业务经理，使之负责组织范围的 IT 治理决策，并在 IT 原则中加入严格的成本控制；
- 谨慎管理组织的 IT 架构和业务架构，以降低业务成本；
- 设计严格的架构例外处理流程，使昂贵的例外最小化，并可以从中不断学习；
- 建立集中化的 IT 团队，用以管理基础设施、架构和共享服务；
- 应用连接 IT 投资和业务需求的流程，既可以增加透明度，又可以权衡中心和各运营部门或团队的需求；
- 设计需要对 IT 投资进行集中协作和核准的 IT 投资流程；
- 设计简单的费用分摊和服务水平协议机制，以明确分配 IT 开支等。

3.1.3 IT 治理任务

组织的 IT 治理活动定义为统筹、指导、监督和改进。统筹现在和未来的 IT 战略和组织规划、管理和绩效的实施计划、策略；指导 IT 管理实施、绩效考评、风险控制和业务合规；监督 IT 与业务的一致性、符合性及 IT 应用的合规性；改进 IT 战略规划、组织策略、信息系统全生命周期管控和数据治理。组织开展 IT 治理活动的主要任务聚焦在如下五个方面。

(1) 全局统筹。统筹规划 IT 治理的目标范围、技术环境、发展趋势和人员责权利。组织需要适应当前信息环境和未来发展趋势，保证利益相关者理解和接受 IT 的战略、目标和发展方向。组织需要把 IT 治理作为组织治理的组成部分，建立 IT 治理机构，并明确组织负责人对 IT 治理工作负责。组织还需要关注 IT 发展的规划、实施、检查和改进全过程，重点包括①制订满足可持续发展的 IT 蓝图；②实施科学决策、集约管理的策略，实现横向的业务集成和纵向的业

务管控；通过内外部的监督，确保 IT 与业务的一致性和适用性；③建立适应内外部信息环境变化的持续改进和创新机制。

(2) 价值导向。价值导向包括基于实现有效收益，确保预期收益清晰理解，明确实现收益的问责机制。组织需要建立 IT 投资的价值框架，确保在可承担成本和可接受风险水平的基础上，实现 IT 的战略目标。确保 IT 治理符合组织治理的价值导向，明确战略投资方向，以及由投资产生的 IT 服务、资产和其他资源。组织需要建立价值递送规则，确保利益相关者明确相应的权利和义务，包括：①认可信息技术、信息系统和数据在组织中的价值；②识别投资目录，并以相应的方式进行评估和管理；③对关键指标进行设定和监督，并对变化和偏差做出及时回应；④权衡实施成本与预期效益，并随组织内外部环境的变化及时调整。

(3) 机制保障。机制保障是指组织应对自身 IT 发展进行有效管控，保证 IT 需求与实现的协调发展，并使 IT 安全和风险得到有效的识别、管理、防范和处置。组织需要建立适合组织特点的机制保障方法，满足疏漏互补、协同发展、监督改进和安全风险可控的原则，避免扭曲决策目标方向。组织需要明确管理责任，明晰上下左右权利关系，落实责任制和各项措施。组织可以根据相关法律法规、行业管理和上级监管机构发布的规范文件要求，制定本组织的信息技术治理制度并实施，重点聚焦在：①指导建立规范过程管理和痕迹管理，并向利益相关者公开质量设定举措；②评审 IT 管理体系的适宜性、充分性和有效性；③审计 IT 完整性、有效性和合规性；④监督由审计和管理评审，提出改进内容的实施。

(4) 创新发展。创新发展是指利用 IT 创新开拓业务领域，提升管理水平，改进质量、绩效和降低成本，确保实现战略目标的灵活性和对环境变化的适应性。组织需要通过建立围绕知识资产的创新体系，支撑组织的技术进步、管理提升和业务模式变革。组织可以持续保持管理团队的创造技能，并指导培养各级成员的发问、观察、交际和实验能力。组织可以建立支持创新的人员、技术、制度、资金、风险、文化和市场需求的机制体系，包括：①创造基于业务团队与 IT 团队的深度沟通以及对内外部环境感知和学习的技术创新环境；②确保技术发展、管理创新、模式革新的协调联动；③对组织创新能力进行评估，并对关键创新要素进行分析和评价；④通过促进和创新有效抵御风险，并确保创新是组织文化的组成部分。

(5) 文化助推。文化助推是指组织与利益相关者沟通 IT 治理的目标、策略和职责，营造积极向上、沟通包容的组织文化。组织需要引导组织人员适应 IT 建设所带来的变革、遵循道德和职业规范、端正态度和规范行为。组织可以要求各级管理层把符合信息技术战略发展的文化建设作为其职责的一部分。按照文化营造、实施和改进的生命周期，保障利益相关者的沟通和透明，包括：①建立与 IT 发展相适应的组织文化发展策略；②营造包括知识、技术、管理、情操在内的积极向上的文化氛围；③根据组织内部环境的变化，评估并改进组织文化的管理。

3.1.4 IT 治理方法与标准

考虑到 IT 治理对组织战略目标达成的重要性，国内外各类机构持续研究并沉淀 IT 治理相关的最佳实践方法、定义相关标准，这里面比较典型的是我国信息技术服务标准库（ITSS）中 IT 治理系列标准、信息和技术治理框架（COBIT）和 IT 治理国际标准（ISO/IEC 38500）等。

1. ITSS 中 IT 服务治理

我国 IT 治理标准化研究是围绕 IT 治理研究范畴，为 IT 过程、IT 资源、信息与组织战略、组织目标的连接提供了一种机制。通过指导、实施、管理和评价等过程，确保 IT 支持并拓展组织的战略和目标。在 IT 治理目标和边界确定的情况下，IT 治理围绕决策体系、责任归属、管理流程、内外评价四个方面，通过相关框架体系的研究，规范和引导组织的 IT 治理完成“做什么”“如何做”“怎么样”“如何评价”等问题，如图 3-5 所示。

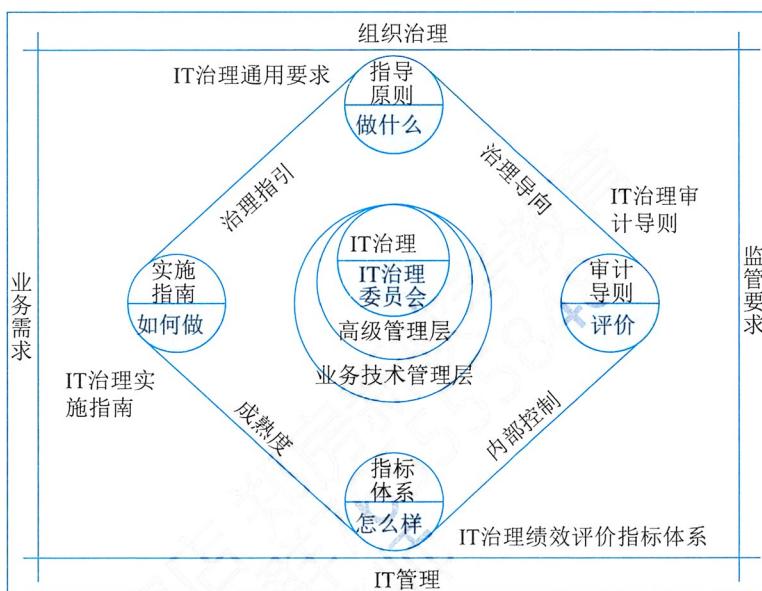


图 3-5 ITSS-IT 治理标准化的逻辑关系图

1) IT 治理通用要求

GB/T 34960.1《信息技术服务 治理 第 1 部分：通用要求》规定了 IT 治理的模型和框架、实施 IT 治理的原则，以及开展 IT 顶层设计、管理体系和资源的治理要求。该标准可用于：①建立组织的 IT 治理体系，并实施自我评价；②开展信息技术审计；③研发、选择和评价 IT 治理相关的软件或解决方案；④第三方对组织的 IT 治理能力进行评价。各级各类信息化主管部门可根据法律法规、部门规章的要求，使用该标准对所管辖各类组织的 IT 治理提出要求，并进行评估、指导和监督。

该标准定义的 IT 治理模型包含治理的内外部要求、治理主体、治理方法，以及信息技术及其应用的管理体系，如图 3-6 所示。

治理主体以组织章程、监管职责、利益相关方期望、业务压力和业务要求为驱动力，建立评估、指导、监督的治理过程并明确任务。治理主体通过信息技术战略和方针，指导管理者对信息技术及其应用的管理体系进行完善，并对信息技术相关的方案和规划进行评估，对信息技术应用的绩效和符合性进行监督。组织结合治理原则和模型，在 IT 治理实施的过程中，开展自我监督、自我评估和审计工作，并持续改进。