第 3 章　网络信息安全工程基础知识

互联网技术飞速发展不断推动着人类社会生活和生产方式的不断变革。网络信息安全在理论与实践中都面临挑战。健全、完善和合理运用国家治理网络空间安全的法律法规，熟悉和掌握最新互联网信息技术规律，网络空间合理利用才能为社会进步和人类历史发展提供重要的机遇。

本章系统地介绍了我国网络信息安全有关法律法规以及电力等行业网络信息安全规范规定，论述了大数据、云计算、物联网、电子商务、智能电网、智慧城市、内存计算技术、新一代移动通信技术、全球能源互联网技术的基本概念及特点，讨论了运用网络信息安全工程技术知识，保证网络空间安全的有关问题。

3.1　国家信息安全有关法律法规

本节主要内容包括：最新国家安全法有关信息安全的部分内容，中华人民共和国计算机信息系统安全保护条例，中华人民共和国网络安全法（草案）部分章节。本节还介绍了信息安全等级保护管理办法、工业控制系统信息安全管理及电力监控系统安全防护规定等内容。

3.1.1　国家安全法有关信息安全内容

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了中华人民共和国国家安全法，2016 年 1 月 1 日起执行。国家安全是指国家政权、主权、统一和领土完整、人民福祉、经济社会可持续发展和国家其他重大利益相对处于没有危险和不受内外威胁的状态，以及保障持续安全状态的能力。有关信息安全内容包括：第二章 维护国家安全的任务第二十五条“国家建设网络与信息安全保障体系，提升网络与信息安全保护能力，加强网络和信息技术的创新研究和开发应用，实现网络和信息核心技术、关键基础设施和重要领域信息系统及数据的安全可控；加强网络管理，防范、制止和依法惩治网络攻击、网络入侵、网络窃密、散布违法有害信息等网络违法犯罪行为，维护国家网络空间主权、安全和发展利益。”第四章 国家安全制度第四节审查监管第五十九条“国家建立国家安全审查和监管的制度和机制，对影响或者可能影响国家安全的外商投资、特定物项和关键技术、网络信息技术产品和服务、涉及国家安全事项的建设项目，以及其他重大事项和活动，进行国家安全审查，有效预防和化解国家安全风险”。

根据我国面临的网络安全形势日趋严峻，将坚持“积极利用、科学发展、依法管理、确保安全”的16字方针，加大依法管理网络的力度，不断健全网络安全的保障体系。同时从以下5个方面加强网络信息安全的保护。

一是积极推动网络信息安全立法工作，组织制定信息安全检查、信息安全管理、通信网络安全的防护、互联网安全接入等急需的标准。制定相关法律法规和标准，做到有法可依、依法办事。二是加快完善信息安全审查制度框架，有计划地开展信息安全审查试点，特别是要加强政府部门云计算服务的信息安全管理，组织实施党政机关互联网安全接入工程和重点领域信息安全检查。三是强化信息安全基础设施和技术手段体系化建设，进一步巩固提升电话用户实名登记工作，开展地下黑色产业链等网络安全环境的治理，特别是抓好木马、僵尸等病毒的防范，对钓鱼网站、移动恶意程序等网络攻击威胁的监测和处理工作也要进一步加强。同时，配合公安机关开展源头的打击，实现标本兼治。四是扶持和壮大网络与信息安全产业，重点支持网络与信息安全关键核心技术的突破，加强应用试点示范，发展信息安全产品和服务，构建全产业链协同发展的格局。五是推动网络空间国际交流与合作，在网络安全的技术、信息共享、跨境安全事件处置等方面加强国际合作，加强网络与信息安全的宣传教育，组织开展网络安全宣传周等项活动，来提升全社会网络安全的意识和自我保护能力。

2012年12月28日，第十一届全国人民代表大会常务委员会第三十次会议通过的《全国人民代表大会常务委员会关于加强网络信息保护的决定》规定：国家保护能够识别公民个人身份和涉及公民个人隐私的电子信息。网络服务提供者和其他企业事业单位及其工作人员在有关业务活动中保证公民个人电子信息安全。有关主管部门应当在各自职权范围内依法履行职责，采取技术措施和其他必要措施，防范、制止和查处窃取或者以其他非法方式获取、出售或者非法向他人提供公民个人电子信息的违法犯罪行为以及其他网络信息违法犯罪行为。

3.1.2 中华人民共和国计算机信息系统安全保护条例

1994年2月18日，中华人民共和国国务院令（147号）发布《中华人民共和国计算机信息系统安全保护条例》，有关内容如下。

（1）条例所称的计算机信息系统，是指由计算机及其相关的和配套的设备、设施（含网络）构成的，按照一定的应用目标和规则对信息进行采集、加工、存储、传输、检索等处理的人机系统。计算机信息系统的安全保护，应当保障计算机及其相关的和配套的设备、设施（含网络)的安全，运行环境的安全，保障信息的安全，保障计算机功能的正常发挥，以维护计算机信息系统的安全运行。

（2）计算机信息系统实行安全等级保护。安全等级的划分标准和安全等级保护的具体办法，由公安部会同有关部门制定；计算机机房应当符合国家标准和国家有关规定。在计算机机房附近施工，不得危害计算机信息系统的安全；计算机信息系统的使用单位应当建立健全安全管理制度，负责本单位计算机信息系统的安全保护工作。

（3）公安机关对计算机信息系统保护工作行使下列监督职权。

① 监督、检查、指导计算机信息系统安全保护工作；

② 查处危害计算机信息系统安全的违法犯罪案件；

③ 履行计算机信息系统安全保护工作的其他监督职责。

公安机关发现影响计算机信息系统安全的隐患时，应当及时通知使用单位采取安全保护措施。公安部在紧急情况下，可以就涉及计算机信息系统安全的特定事项发布专项通令。

（4）违反本条例的规定，有下列行为之一的，由公安机关处以警告或者停机整顿。

① 违反计算机信息系统安全等级保护制度，危害计算机信息系统安全的；

② 违反计算机信息系统国际联网备案制度的；

③ 不按照规定时间报告计算机信息系统中发生的案件的；

④ 接到公安机关要求改进安全状况的通知后，在限期内拒不改进的；

⑤ 有危害计算机信息系统安全的其他行为的。

3.1.3　信息安全等级保护管理办法有关部分

2007 年 6 月 22 日，为加快推进信息安全等级保护，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，公安部、国家保密局、国家密码管理局、国务院信息化工作办公室制定了《信息安全等级保护管理办法》。

（1）为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，国家通过制定统一的信息安全等级保护管理规范和技术标准，组织公民、法人和其他组织对信息系统分等级实行安全保护，对等级保护工作的实施进行监督、管理。

（2）等级划分与保护。

国家信息安全等级保护坚持自主定级、自主保护的原则。信息系统的安全保护等级应当根据信息系统在国家安全、经济建设、社会生活中的重要程度，信息系统遭到破坏后对国家安全、社会秩序、公共利益以及公民、法人和其他组织的合法权益的危害程度等因素确定。

信息系统的安全保护等级分为以下 5 级。

第一级，信息系统受到破坏后，会对公民、法人和其他组织的合法权益造成损害，但不损害国家安全、社会秩序和公共利益。

第二级，信息系统受到破坏后，会对公民、法人和其他组织的合法权益产生严重损害，或者对社会秩序和公共利益造成损害，但不损害国家安全。

第三级，信息系统受到破坏后，会对社会秩序和公共利益造成严重损害，或者对国家安全造成损害。

第四级，信息系统受到破坏后，会对社会秩序和公共利益造成特别严重损害，或者对国家安全造成严重损害。

第五级，信息系统受到破坏后，会对国家安全造成特别严重损害。

信息系统运营、使用单位依据本办法和相关技术标准对信息系统进行保护，国家有关信息安全监管部门对其信息安全等级保护工作进行监督管理。

（3）等级保护的实施与管理。

① 信息系统运营、使用单位应当按照《信息系统安全等级保护实施指南》具体实施等级保护工作。跨省或者全国统一联网运行的信息系统可以由主管部门统一确定安全保护等级。

对拟确定为第四级以上信息系统的，运营、使用单位或者主管部门应当请国家信息安全保护等级专家评审委员会评审。信息系统的安全保护等级确定后，运营、使用单位应当按照国家信息安全等级保护管理规范和技术标准，使用符合国家有关规定，满足信息系统安全保护等级需求的信息技术产品，开展信息系统安全建设或者改建工作。

② 在信息系统建设过程中，运营、使用单位应当按照《计算机信息系统安全保护等级划分准则》（GB17859—1999）、《信息系统安全等级保护基本要求》等技术标准，参照《信息安全技术信息系统通用安全技术要求》（GB/T20271—2006）、《信息安全技术网络基础安全技术要求》（GB/T20270—2006）、《信息安全技术 操作系统安全技术要求》（GB/T20272—2006）、《信息安全技术 数据库管理系统安全技术要求》（GB/T20273—2006）、《信息安全技术 服务器技术要求》、《信息安全技术 终端计算机系统安全等级技术要求》（GA/T671—2006）等技术标准同步建设符合该等级要求的信息安全设施。运营、使用单位应当参照《信息安全技术 信息系统安全管理要求》（GB/T20269—2006）、《信息安全技术信息系统安全工程管理要求》（GB/T20282—2006）、《信息系统安全等级保护基本要求》等管理规范，制定并落实符合本系统安全保护等级要求的安全管理制度。

③ 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。第三级信息系统应当每年至少进行一次等级测评，第四级信息系统应当每半年至少进行一次等级测评，第五级信息系统应当依据特殊安全需求进行等级测评。信息系统运营、使用单位及其主管部门应当定期对信息系统安全状况、安全保护制度及措施的落实情况进行自查。第三级信息系统应当每年至少进行一次自查，第四级信息系统应当每半年至少进行一次自查，第五级信息系统应当依据特殊安全需求进行自查。经测评或者自查，信息系统安全状况未达到安全保护等级要求的，运营、使用单位应当制定方案进行整改。

④ 已运营（运行）的第二级以上信息系统，应当在安全保护等级确定后 30 日内，由其运营、使用单位到所在地设区的市级以上公安机关办理备案手续。新建第二级以上信息系统，应当在投入运行后 30 日内，由其运营、使用单位到所在地设区的市级以上公安机关办理备案手续。隶属于中央的在京单位，其跨省或者全国统一联网运行并由主管部门统一定级的信息系统，由主管部门向公安部办理备案手续。跨省或者全国统一联网运行的信息系统在各地运行、应用的分支系统，应当向当地设区的市级以上公安机关备案。

⑤ 公安机关检查发现信息系统安全保护状况不符合信息安全等级保护有关管理规范

和技术标准的，应当向运营、使用单位发出整改通知。运营、使用单位应当根据整改通知要求，按照管理规范和技术标准进行整改。整改完成后，应当将整改报告向公安机关备案。必要时，公安机关可以对整改情况组织检查。

⑥ 第三级以上信息系统应当选择使用符合以下条件的信息安全产品。

- 产品研制、生产单位是由中国公民、法人投资或者国家投资或者控股的，在中华人民共和国境内具有独立的法人资格；
- 产品的核心技术、关键部件具有我国自主知识产权；
- 产品研制、生产单位及其主要业务、技术人员无犯罪记录；
- 产品研制、生产单位声明没有故意留有或者设置漏洞、后门、木马等程序和功能；
- 对国家安全、社会秩序、公共利益不构成危害。

（4）涉及国家秘密信息系统的分级保护管理。

涉密信息系统应当依据国家信息安全等级保护的基本要求，按照国家保密工作部门有关涉密信息系统分级保护的管理规定和技术标准，结合系统实际情况进行保护。

非涉密信息系统不得处理国家秘密信息。涉密信息系统按照所处理信息的最高密级，由低到高分为秘密、机密、绝密三个等级。

涉密信息系统建设使用单位应当在信息规范定密的基础上，依据涉密信息系统分级保护管理办法和国家保密标准 BMB17-2006《涉及国家秘密的计算机信息系统分级保护技术要求》确定系统等级。对于包含多个安全域的涉密信息系统，各安全域可以分别确定保护等级。

（5）信息安全等级保护的密码管理。

国家密码管理部门对信息安全等级保护的密码实行分类分级管理。根据被保护对象在国家安全、社会稳定、经济建设中的作用和重要程度，被保护对象的安全防护要求和涉密程度，被保护对象被破坏后的危害程度以及密码使用部门的性质等，确定密码的等级保护准则。信息系统运营、使用单位采用密码进行等级保护，应当遵照《信息安全等级保护密码管理办法》、《信息安全等级保护商用密码技术要求》等密码管理规定和相关标准。

信息系统运营、使用单位应当充分运用密码技术对信息系统进行保护。采用密码对涉及国家秘密的信息和信息系统进行保护的，应报经国家密码管理局审批，密码的设计、实施、使用、运行维护和日常管理等，应当按照国家密码管理有关规定和相关标准执行；采用密码对不涉及国家秘密的信息和信息系统进行保护的，须遵守《商用密码管理条例》和密码分类分级保护有关规定与相关标准，其密码的配备使用情况应当向国家密码管理机构备案。

运用密码技术对信息系统进行系统等级保护建设和整改的，必须采用经国家密码管理部门批准使用或者准于销售的密码产品进行安全保护，不得采用国外引进或者擅自研制的密码产品；未经批准不得采用含有加密功能的进口信息技术产品。

各级密码管理部门可以定期或者不定期对信息系统等级保护工作中密码配备、使用和管理的情况进行检查和测评，对重要涉密信息系统的密码配备、使用和管理情况每两年至少进行一次检查和测评。在监督检查过程中，发现存在安全隐患或者违反密码管理相关规

定或者未达到密码相关标准要求的，应当按照国家密码管理的相关规定进行处置。

3.1.4 加强工业控制系统信息安全管理有关规定

2011 年 9 月 29 日，经国务院同意，工业和信息化部下发关于加强工业控制系统信息安全管理的通知。

1．充分认识加强工业控制系统信息安全管理的重要性和紧迫性

数据采集与监控（SCADA）、分布式控制系统（DCS）、过程控制系统（PCS）、可编程逻辑控制器（PLC）等工业控制系统广泛运用于工业、能源、交通、水利以及市政等领域，用于控制生产设备的运行。一旦工业控制系统信息安全出现漏洞，将对工业生产运行和国家经济安全造成重大隐患。随着计算机和网络技术的发展，特别是信息化与工业化深度融合以及物联网的快速发展，工业控制系统产品越来越多地采用通用协议、通用硬件和通用软件，以各种方式与互联网等公共网络连接，病毒、木马等威胁正在向工业控制系统扩散，工业控制系统信息安全问题日益突出。我国工业控制系统信息安全管理工作中仍存在不少问题，主要是对工业控制系统信息安全问题重视不够，管理制度不健全，相关标准规范缺失，技术防护措施不到位，安全防护能力和应急处置能力不高等，威胁着工业生产安全和社会正常运转。

2．明确重点领域工业控制系统信息安全管理要求

加强工业控制系统信息安全管理的重点领域包括核设施、钢铁、有色、化工、石油石化、电力、天然气、先进制造、水利枢纽、环境保护、铁路、城市轨道交通、民航、城市供水供气供热以及其他与国计民生紧密相关的领域。各地区、各部门、各单位要结合实际，明确加强工业控制系统信息安全管理的重点领域和重点环节，切实落实以下要求。

1）连接管理要求

（1）断开工业控制系统同公共网络之间的所有不必要连接。

（2）对确实需要的连接，系统运营单位要逐一进行登记，采取设置防火墙、单向隔离等措施加以防护，并定期进行风险评估，不断完善防范措施。

（3）严格控制在工业控制系统和公共网络之间交叉使用移动存储介质以及便携式计算机。

2）组网管理要求

（1）工业控制系统组网时要同步规划、同步建设、同步运行安全防护措施。

（2）采取虚拟专用网络（VPN）、线路冗余备份、数据加密等措施，加强对关键工业控制系统远程通信的保护。

（3）对无线组网采取严格的身份认证、安全监测等防护措施，防止经无线网络进行恶意入侵，尤其要防止通过侵入远程终端单元（RTU）进而控制部分或整个工业控制系统。

3）配置管理要求

（1）建立控制服务器等工业控制系统关键设备安全配置和审计制度。

（2）严格账户管理，根据工作需要合理分类设置账户权限。

（3）严格口令管理，及时更改产品安装时的预设口令，杜绝弱口令、空口令。

（4）定期对账户、口令、端口、服务等进行检查，及时清理不必要的用户和管理员账户，停止无用的后台程序和进程，关闭无关的端口和服务。

4）设备选择与升级管理要求

（1）慎重选择工业控制系统设备，在供货合同中或以其他方式明确供应商应承担的信息安全责任和义务，确保产品安全可控。

（2）加强对技术服务的信息安全管理，在安全得不到保证的情况下禁止采取远程在线服务。

（3）密切关注产品漏洞和补丁发布，严格软件升级、补丁安装管理，严防病毒、木马等恶意代码侵入。关键工业控制系统软件升级、补丁安装前要请专业技术机构进行安全评估和验证。

5）数据管理要求

地理、矿产、原材料等国家基础数据以及其他重要敏感数据的采集、传输、存储、利用等，要采取访问权限控制、数据加密、安全审计、灾难备份等措施加以保护，切实维护个人权益、企业利益和国家信息资源安全。

6）应急管理要求

制定工业控制系统信息安全应急预案，明确应急处置流程和临机处置权限，落实应急技术支撑队伍，根据实际情况采取必要的备机备件等容灾备份措施。

3．建立工业控制系统安全测评检查和漏洞发布制度

（1）加强重点领域工业控制系统关键设备的信息安全测评工作。全国信息安全标准化技术委员会抓紧制定工业控制系统关键设备信息安全规范和技术标准，明确设备安全技术要求。重点领域的有关单位要请专业技术机构对所使用的工业控制系统关键设备进行安全测评，检测安全漏洞，评估安全风险。工业和信息化部会同有关部门对重点领域使用的工业控制系统关键设备进行抽检。

（2）建立工业控制系统信息安全检查制度。工业控制系统运营单位要从实际出发，定期组织开展信息安全检查，排查安全隐患，堵塞安全漏洞。工业和信息化部适时组织专业技术力量对重点领域工业控制系统信息安全状况进行抽查，及时通报发现的问题。

（3）建立信息安全漏洞信息发布制度。开展工业控制系统信息安全漏洞信息的收集、汇总和分析研判工作，及时发布有关漏洞、风险和预警信息。

4．加强工业控制系统信息安全管理工作

要将工业控制系统信息安全管理作为信息安全工作的重要内容，按照“谁主管谁负责、谁运营谁负责、谁使用谁负责”的原则，建立健全信息安全责任制。各级政府工业和信息

化主管部门要加强对工业控制系统信息安全工作的指导和督促检查。有关行业主管或监管部门、国有资产监督管理部门要加强对重点领域工业控制系统信息安全管理工作的指导监督，结合行业实际制定完善相关规章制度，提出具体要求，并加强督促检查确保落到实处。有关部门要加快推动工业控制系统信息安全防护技术研究和产品研制，加大工业控制系统安全检测技术和工具研发力度。国有大型企业要切实加强工业控制系统信息安全管理的领导，健全工作机制，严格落实责任制，将重要工业控制系统信息安全责任逐一落实到具体部门、岗位和人员，确保领导到位、机构到位、人员到位、措施到位、资金到位。

3.1.5 电力监控系统安全防护规定部分

2014 年 8 月 1 日，中华人民共和国国家发展和改革委员会下发《电力监控系统安全防护规定》，自 2014 年 9 月 1 日起施行。

为了加强电力监控系统的信息安全管理，防范黑客及恶意代码等对电力监控系统的攻击及侵害，保障电力系统的安全稳定运行，根据《电力监管条例》、《中华人民共和国计算机信息系统安全保护条例》和国家有关规定，结合电力监控系统的实际情况，制定本规定。

电力监控系统安全防护工作应当落实国家信息安全等级保护制度，按照国家信息安全等级保护的有关要求，坚持“安全分区、网络专用、横向隔离、纵向认证”的原则，保障电力监控系统的安全。电力监控系统是指用于监视和控制电力生产及供应过程的、基于计算机及网络技术的业务系统及智能设备，以及作为基础支撑的通信及数据网络等，包括电力数据采集与监控系统、能量管理系统、变电站自动化系统、换流站计算机监控系统、发电厂计算机监控系统、配电自动化系统、微机继电保护和安全自动装置、广域相量测量系统、负荷控制系统、水调自动化系统和水电梯级调度自动化系统、电能量计量系统、实时电力市场的辅助控制系统、电力调度数据网络等。

1．技术管理

发电企业、电网企业内部基于计算机和网络技术的业务系统，应当划分为生产控制大区和管理信息大区。生产控制大区可以分为控制区（安全区 I）和非控制区（安全区Ⅱ）；管理信息大区内部在不影响生产控制大区安全的前提下，可以根据各企业不同安全要求划分安全区。根据应用系统实际情况，在满足总体安全要求的前提下，可以简化安全区的设置，但是应当避免形成不同安全区的纵向交叉连接。

电力调度数据网应当在专用通道上使用独立的网络设备组网，在物理层面上实现与电力企业其他数据网及外部公用数据网的安全隔离。电力调度数据网划分为逻辑隔离的实时子网和非实时子网，分别连接控制区和非控制区。生产控制大区的业务系统在与其终端的纵向连接中使用无线通信网、电力企业其他数据网（非电力调度数据网）或者外部公用数据网的虚拟专用网络方式（VPN）等进行通信的，应当设立安全接入区。

在生产控制大区与管理信息大区之间必须设置经国家指定部门检测认证的电力专用横向单向安全隔离装置。生产控制大区内部的安全区之间应当采用具有访问控制功能的设

备、防火墙或者相当功能的设施，实现逻辑隔离。安全接入区与生产控制大区中其他部分的连接处必须设置经国家指定部门检测认证的电力专用横向单向安全隔离装置。在生产控制大区与广域网的纵向连接处应当设置经过国家指定部门检测认证的电力专用纵向加密认证装置或者加密认证网关及相应设施。

安全区边界应当采取必要的安全防护措施，禁止任何穿越生产控制大区和管理信息大区之间边界的通用网络服务。生产控制大区中的业务系统应当具有高安全性和高可靠性，禁止采用安全风险高的通用网络服务功能。依照电力调度管理体制建立基于公钥技术的分布式电力调度数字证书及安全标签，生产控制大区中的重要业务系统应当采用认证加密机制。

电力监控系统在设备选型及配置时，应当禁止选用经国家相关管理部门检测认定并经国家能源局通报存在漏洞和风险的系统及设备；对于已经投入运行的系统及设备，应当按照国家能源局及其派出机构的要求及时进行整改，同时应当加强相关系统及设备的运行管理和安全防护。生产控制大区中除安全接入区外，应当禁止选用具有无线通信功能的设备。

2．安全管理

电力监控系统安全防护是电力安全生产管理体系的有机组成部分。电力企业应当按照“谁主管谁负责，谁运营谁负责”的原则，建立健全电力监控系统安全防护管理制度，将电力监控系统安全防护工作及其信息报送纳入日常安全生产管理体系，落实分级负责的责任制。

电力调度机构负责直接调度范围内的下一级电力调度机构、变电站、发电厂涉网部分的电力监控系统安全防护的技术监督，发电厂内其他监控系统的安全防护可以由其上级主管单位实施技术监督。

电力调度机构、发电厂、变电站等运行单位的电力监控系统安全防护实施方案必须经本企业的上级专业管理部门和信息安全管理部门以及相应电力调度机构的审核，方案实施完成后应当由上述机构验收。接入电力调度数据网络的设备和应用系统，其接入技术方案和安全防护措施必须经直接负责的电力调度机构同意。

建立健全电力监控系统安全防护评估制度，采取以自评估为主、检查评估为辅的方式，将电力监控系统安全防护评估纳入电力系统安全评价体系。建立健全电力监控系统安全的联合防护和应急机制，制定应急预案。电力调度机构负责统一指挥调度范围内的电力监控系统安全应急处理。当遭受网络攻击，生产控制大区的电力监控系统出现异常或者故障时，应当立即向其上级电力调度机构以及当地国家能源局派出机构报告，并联合采取紧急防护措施，防止事态扩大，同时应当注意保护现场，以便进行调查取证。

3．保密管理

电力监控系统相关设备及系统的开发单位、供应商应当以合同条款或者保密协议的方式保证其所提供的设备及系统符合本规定的要求，并在设备及系统的全生命周期内对其负责。电力监控系统专用安全产品的开发单位、使用单位及供应商，应当按国家有关要求做

好保密工作，禁止关键技术和设备的扩散。对生产控制大区安全评估的所有评估资料和评估结果，应当按国家有关要求做好保密工作。

3.1.6 中华人民共和国网络安全法（草案）部分

为了保障网络安全，维护网络空间主权和国家安全、社会公共利益，保护公民、法人和其他组织的合法权益，促进经济社会信息化健康发展，坚持网络安全与信息化发展并重，遵循积极利用、科学发展、依法管理、确保安全的方针，推进网络基础设施建设，鼓励网络技术创新和应用，建立健全网络安全保障体系，提高网络安全保护能力。积极开展网络空间治理、网络技术研发和标准制定、打击网络违法犯罪等方面的国际交流与合作，推动构建和平、安全、开放、合作的网络空间。

1．网络安全战略、规划与促进

国家制定网络安全战略，明确保障网络安全的基本要求和主要目标，提出完善网络安全保障体系、提高网络安全保护能力、促进网络安全技术和产业发展、推进全社会共同参与维护网络安全的政策措施等。

国务院通信、广播电视、能源、交通、水利、金融等行业的主管部门和国务院其他有关部门应当依据国家网络安全战略，编制关系国家安全、国计民生的重点行业、重要领域的网络安全规划，并组织实施。

国家建立和完善网络安全标准体系。国务院标准化行政主管部门和国务院其他有关部门根据各自的职责，组织制定并适时修订有关网络安全管理以及网络产品、服务和运行安全的国家标准、行业标准。

国家支持企业参与网络安全国家标准、行业标准的制定，并鼓励企业制定严于国家标准、行业标准的企业标准。

国务院和省、自治区、直辖市人民政府应当统筹规划，加大投入，扶持重点网络安全技术产业和项目，支持网络安全技术的研究开发、应用和推广，保护网络技术知识产权，支持科研机构、高等院校和企业参与国家网络安全技术创新项目。

2．网络运行安全一般规定

国家实行网络安全等级保护制度。网络运营者应当按照网络安全等级保护制度的要求，履行下列安全保护义务，保障网络免受干扰、破坏或者未经授权的访问，防止网络数据泄露或者被窃取、篡改。

（1）制定内部安全管理制度和操作规程，确定网络安全负责人，落实网络安全保护责任；

（2）采取防范计算机病毒和网络攻击、网络入侵等危害网络安全行为的技术措施；

（3）采取记录、跟踪网络运行状态，监测、记录网络安全事件的技术措施，并按照规定留存网络日志；

（4）采取数据分类、重要数据备份和加密等措施；

（5）法律、行政法规规定的其他义务。

网络产品、服务应当符合相关国家标准、行业标准。网络产品、服务的提供者不得设置恶意程序；其产品、服务具有收集用户信息功能的，应当向用户明示并取得同意；发现其网络产品、服务存在安全缺陷、漏洞等风险时，应当及时向用户告知并采取补救措施。

网络关键设备和网络安全专用产品应当按照相关国家标准、行业标准的强制性要求，由具备资格的机构安全认证合格或者安全检测符合要求后，方可销售。国家网信部门会同国务院有关部门制定、公布网络关键设备和网络安全专用产品目录，并推动安全认证和安全检测结果互认，避免重复认证、检测。

网络运营者为用户办理网络接入、域名注册服务，办理固定电话、移动电话等入网手续，或者为用户提供信息发布服务，应当在与用户签订协议或者确认提供服务时，要求用户提供真实身份信息。国家支持研究开发安全、方便的电子身份认证技术，推动不同电子身份认证技术之间的互认、通用。

网络运营者应当制定网络安全事件应急预案，及时处置系统漏洞、计算机病毒、网络入侵、网络攻击等安全风险；在发生危害网络安全的事件时，立即启动应急预案，采取相应的补救措施，并按照规定向有关主管部门报告。

任何个人和组织不得从事入侵他人网络、干扰他人网络正常功能、窃取网络数据等危害网络安全的活动；不得提供从事入侵网络、干扰网络正常功能、窃取网络数据等危害网络安全活动的工具和制作方法；不得为他人实施危害网络安全的活动提供技术支持、广告推广、支付结算等帮助。

3．关键信息基础设施的运行安全

国家对提供公共通信、广播电视传输等服务的基础信息网络，能源、交通、水利、金融等重要行业和供电、供水、供气、医疗卫生、社会保障等公共服务领域的重要信息系统，军事网络，设区的市级以上国家机关等政务网络，用户数量众多的网络服务提供者所有或者管理的网络和系统（以下称关键信息基础设施），实行重点保护。

国务院通信、广播电视、能源、交通、水利、金融等行业的主管部门和国务院其他有关部门（以下称负责关键信息基础设施安全保护工作的部门）按照国务院规定的职责，分别负责指导和监督关键信息基础设施运行安全保护工作。

建设关键信息基础设施应当确保其具有支持业务稳定、持续运行的性能，并保证安全技术措施同步规划、同步建设、同步使用。

关键信息基础设施的运营者还应当履行下列安全保护义务。

（1）设置专门的安全管理机构和安全管理负责人，并对该负责人和关键岗位的人员进行安全背景审查；

（2）定期对从业人员进行网络安全教育、技术培训和技能考核；

（3）对重要系统和数据库进行容灾备份；

（4）制定网络安全事件应急预案，并定期组织演练；

（5）法律、行政法规规定的其他义务。

关键信息基础设施的运营者采购网络产品和服务，应当与提供者签订安全保密协议，明确安全和保密义务与责任。可能影响国家安全的，应当通过国家网信部门会同国务院有关部门组织的安全审查。

关键信息基础设施的运营者应当在中华人民共和国境内存储在运营中收集和产生的公民个人信息等重要数据；因业务需要，确需在境外存储或者向境外的组织或者个人提供的，应当按照国家网信部门会同国务院有关部门制定的办法进行安全评估。应当自行或者委托专业机构对其网络的安全性和可能存在的风险每年至少进行一次检测评估，并对检测评估情况及采取的改进措施提出网络安全报告，报送相关负责关键信息基础设施安全保护工作的部门。

国家网信部门应当统筹协调有关部门，建立协作机制。对关键信息基础设施的安全保护可以采取下列措施。

（1）对关键信息基础设施的安全风险进行抽查检测，提出改进措施，必要时可以委托专业检验检测机构对网络存在的安全风险进行检测评估；

（2）定期组织关键信息基础设施的运营者进行网络安全应急演练，提高关键信息基础设施应对网络安全事件的水平和协同配合能力；

（3）促进有关部门、关键信息基础设施运营者以及网络安全服务机构、有关研究机构等之间的网络安全信息共享；

（4）对网络安全事件的应急处置与恢复等，提供技术支持与协助。

4．网络信息安全

网络运营者应当建立健全用户信息保护制度，加强对用户个人信息、隐私和商业秘密的保护。

网络运营者收集、使用公民个人信息，应当遵循合法、正当、必要的原则，明示收集、使用信息的目的、方式和范围，并经被收集者同意。不得收集与其提供的服务无关的公民个人信息，不得违反法律、行政法规的规定和双方的约定收集、使用公民个人信息，并应当依照法律、行政法规的规定或者与用户的约定，处理其保存的公民个人信息。

网络运营者应当采取技术措施和其他必要措施，确保公民个人信息安全，防止其收集的公民个人信息泄露、毁损、丢失。在发生或者可能发生信息泄露、毁损、丢失的情况时，应当立即采取补救措施，告知可能受到影响的用户，并按照规定向有关主管部门报告。

公民发现网络运营者违反法律、行政法规的规定或者双方的约定收集、使用其个人信息的，有权要求网络运营者删除其个人信息；发现网络运营者收集、存储的其个人信息有错误的，有权要求网络运营者予以更正。

任何个人和组织不得窃取或者以其他非法方式获取公民个人信息，不得出售或者非法向他人提供公民个人信息。依法负有网络安全监督管理职责的部门，必须对在履行职责中知悉的公民个人信息、隐私和商业秘密严格保密，不得泄露、出售或者非法向他人提供。

网络运营者应当加强对其用户发布的信息的管理，发现法律、行政法规禁止发布或者

传输的信息的，应当立即停止传输该信息，采取消除等处置措施，防止信息扩散，保存有关记录，并向有关主管部门报告。

电子信息发送者发送的电子信息，应用软件提供者提供的应用软件不得设置恶意程序，不得含有法律、行政法规禁止发布或者传输的信息。电子信息发送服务提供者和应用软件下载服务提供者，应当履行安全管理义务，发现电子信息发送者、应用软件提供者有前款规定行为的，应当停止提供服务，采取消除等处置措施，保存有关记录，并向有关主管部门报告。

国家网信部门和有关部门依法履行网络安全监督管理职责，发现法律、行政法规禁止发布或者传输的信息的，应当要求网络运营者停止传输，采取消除等处置措施，保存有关记录；对来源于中华人民共和国境外的上述信息，应当通知有关机构采取技术措施和其他必要措施阻断信息传播。

3.2　网络信息安全工程技术知识

本节主要内容包括云计算、云资料中心及云安全、互联网与物联网、全球能源互联网及其关键技术知识，介绍国家信息安全法规和保障体系框架设想，探讨抓住网络空间发展与网络信息安全机遇，网络强国必须强化掌控网络信息安全力问题。

3.2.1　抓住网络空间发展与网络信息安全机遇

1．经略网络空间，打造新的战略机遇期

（1）网络空间与现实社会交织互动，为人类社会提供新的发展空间。网络打破地域疆界，改变社会经济形态和传统生产方式，电子政务、电子商务、网络社交、文化娱乐、信息消费，“无所不有”；政治、经济、军事、文化、外交，“一网打尽”。同时，网络又不断挑战人类社会对信息技术、网络社会和信息化的认知极限。大到国际秩序和公认准则、中到国家管理和社会关系，小到人际交往和生活方式，一次次面临颠覆和重构。网络将人类带入了一个全新的空间，信息化成为不可逆转的潮流。网络空间既是一个虚拟的存在，也是一个继海、陆、空、天之后，人类“同呼吸、共命运”的新空间，成为各个大国争夺的新边疆，各种力量博弈较量的新战场。

（2）网络空间蕴含巨大发展红利，为中国提供新的战略机遇。中国经历改革开放三十多年，利用互联网 20 年，已成功地将网络发展转化为先进生产力和正能量，极大地促进了国家经济、政治、文化、社会等各个方面的发展。中国信息化建设成就斐然、世界瞩目。中国凭借独特的理论优势、道路优势和制度优势以及信息化进程的后发优势，一跃成为当今世界第二大经济体。对中国而言，网络空间最大限度地激发了信息化高速发展的活力，蕴含着新一轮技术革命的丰厚能量。可以说，网络空间为维护、延长中国的战略机遇期赢

得了新的发展机会，又为中国开拓新的发展空间创造了历史条件。

（3）用心经略网络空间，促进国家治理能力现代化。习近平总书记将网络视为联系群众的新纽带，维护社会稳定的新阵地，实现中国梦的新机遇以及维护国家安全的新边疆。赋予网络“牵一网而动全局”的新的历史意义。要开启中国从网络大国走向网络强国的新历程，要实现“两个一百年”的宏伟目标和中华民族伟大复兴“中国梦”的伟大理想，就必须以更宽的视野、更大的胆识和更新的智慧，精心经略网络空间，就是要牢牢把握十八届三中全会改革开放的总目标和四中全会依法治国的大格局，聚焦国家总体安全，全面可持续提升网络空间蕴含的生产力、文化力、国防力，推动实现国家网络空间治理体系和治理能力现代化。

2．提高忧患意识，确保当前的网络信息安全

（1）要清醒认识“大而不强”的基本现状。中国以最大的网民数量、最大的网站数量、最大的手机用户数量和最快的发展速度成为信息化大国。网络已经成为“治国理政”的重要平台、经济发展的重要支撑、社会稳定的重要动力和国家安全的重要屏障。但我国仍是一个发展中的国家，且处于社会主义的初级阶段，大而思强、乐不忘忧是我们前进路上必须牢记的信条。审视我国网络和信息化发展的进程，潜在的脆弱性和安全隐患，时时在敲响“大而不强”的警钟。发展的历史阶段和基本国情使我们在信息安全上面临着特殊的“难处”、“苦处”和“痛处”。“难处”在于，国民经济的发展和社会的运行与稳定，对信息技术和信息化的依赖越来越大，复杂到传统管理方式远远不能适应，敏感到一个漏洞和一线风险都能引发“千里之堤、溃于蚁穴”的严重后果。“苦处”在于，信息技术、核心设备受制于人，信息化建设的“砖头瓦片”大量来自国外，不能自主，难以自控。“温水煮青蛙”的形势短期内难有大的改观。“痛处”在于，中国改革开放进入全面深化的特殊阶段，安全挑战与发展风险巨大。安全形势多元复杂，各种矛盾风险叠加，都在网络上反映出来。而在管理上，缺乏规范有序的管理机制和技术手段，“九龙治水”的管理体制常常导致监管的错位、越位和缺位，一定程度上削弱了治理能力，抵消了体制优势。以上基本现状，一定程度上决定了我国网络信息安全问题的性质和特点。

（2）应牢牢抓住内容安全与技术安全两大重点。我们当前面临的网络安全挑战既有全球共性问题，如系统漏洞、网络窃密、计算机病毒、网络攻击、垃圾邮件、虚假有害信息和网络违法犯罪等；更有意识形态渗透、社会文化冲击和技术受制受控等特殊具体问题。在网络颠覆与技术控制并存、网络博弈日趋激烈的情况下，我们必须以“两手抓，两手都要硬”的原则，抓好内容安全和技术安全。信息内容安全事关政治安全和政权安全，不能有丝毫松懈。在意识形态和网络内容领域，我们长期面临一场看不见又极端尖锐的斗争。近年来，网络舆情持续高发、网络群体性事件接连不断、网络乱象势头猛增，网上多元思潮交锋对抗，网络成为滋生传播负能量的集散地。同时，反动势力利用网络煽动闹事，宣扬极端恐怖主义。“我们能否顶得住、打得赢，直接关系我国意识形态安全和政权安全”。信息技术安全事关经济发展和社会稳定，来不得半点马虎。我国的关键信息基础设施和重要网络系统，自身漏洞风险和安全隐患重重，又身处在国际网络攻击对抗的风口浪尖。目

前，大量在用的芯片、操作系统、数据库、路由器、交换机等核心产品依赖进口，短期内仍难根本改变。电子政务系统、金融系统、能源供应和大量工业控制系统均存在程度不一的安全隐患和技术风险，国家信息安全保障体系亟待加固和升级。

（3）要着力构建三大核心能力。“打铁还需自身硬”，网络信息安全工作需要强有力的实力支撑。一是防御保障能力。即要确保国家重要的网络系统安全、高效地运行。这需要政府、企业、社会方方面面齐心协力，通过技术与管理手段，不断强化信息安全保障体系，构筑坚固的网络长城。二是预警感知能力。即要预知、预防、预止网络上的各种风险，防止误解、误判、误导，及时、全面掌握网络空间威胁和隐患，做到安全“胸中有数、心中有底”。这需要有专门的国家力量。三是反制打击能力。在网络霸权客观存在的情况下，为防止军事讹诈，必须要有网络反制能力。但网络空间的威慑能力宜少而精。一手构筑“防火墙”，一手打造“杀手锏”，是网络强国的应有之义。

（4）应妥善处理四对“辩证关系”。一是发展与安全的关系。十年前我们讲“在发展中求安全”，十年后则提“以安全保发展”。这一思维转变，诠释了网络安全与信息化建设“一体之两翼，驱动之双轮”的辩证关系。安全问题不解决，发展必然会受到制约。二是技术与管理的关系。网络和信息安全问题的解决，需要技术和管理双管齐下，综合施策。有的管理难题，用技术的方式较好解决；反之，有的技术困境，用管理的方法反而简捷有效。要克服技术万能或者一管就灵的偏颇思想。三是政府与市场的关系。明确政府与市场的责任分担，充分发挥政府的主导作用和市场的决定性作用，针对网络空间创新性强、参与方多和管控度低等特点，以“柔性监管”方式最大限度地激发技术创新和产业发展。四是独立自主与国际合作的关系。找准差距、加大投入，加强关键技术的自主可控，是实现网络强国的根本途径。同时扩大开放、合作，以安全审查制度和测试评估机制等确保供应链的安全可信，是成为网络强国的必然选择。

（5）要重点应对五大风险和威胁。目前，我国需要高度关注的安全风险主要表现为以下 5 个方面：一是政治渗透是最大的风险，反映在内容安全上；二是窃密和泄密是最突出的风险，窃泄密案件逐年激增；三是网络犯罪是最现实的风险，金融诈骗、个人隐私泄露层出不穷；四是技术隐患是长期的风险，大量信息技术靠引进，脆弱性大量存在，被不法利用，损失巨大；五是军事威慑是潜在的风险，网络军备竞赛愈演愈烈，恐怖主义在网络空间抬头。

而在网络空间的主要威胁源方面，应重点应对的也有 5 个：一是国家层面。“斯诺登”事件已向世人昭示，有些国家可以组织专门力量，针对其他主权国家，长期进行渗透颠覆和窃密监控活动，破坏力很大，威慑性极强。二是恐怖组织。民族分裂分子和恐怖势力纷纷上网，他们组成复杂，活动隐蔽，行动突发，防不胜防。三是犯罪团伙。此类威胁受高利益驱使，针对企业、团体和个人，攻击方式多，受害主体广，社会危害大。四是黑客团体。这是网络空间的一支新生力量，在各种复杂的社会经济关系与黑色产业链的影响下，良莠不齐，他们组织松散、目标随意，战法参差，很难防范。五是极端个人。他们能力强、掌握资源多，奉行自由主义、反对国家权威。阿桑奇、斯诺登等就是实例，个人利用网络挑战一个国家乃至世界的现象，不容小视。

3.2.2 网络强国必须强化掌控网络信息安全力

“发展是硬道理，安全是总要求”，要实现“网络强国”的新目标和新愿景，就必须兼顾国内、国际两个大局，以强化网络信息安全掌控力为核心，从以下 5 个方面提高我国的网络空间治理能力。

（1）强化治理体系和战略规划。习总书记已先后就国家治理、总体安全、网络空间、深化改革和依法治国等一系列重大问题做出了高瞻远瞩的战略部署，特别是亲自担纲中央网络安全和信息化领导小组的工作，对信息化时代的网络治理提出了更为明确具体的要求。这本身就是国家治理体系和治理能力现代化的伟大实践。近一年来，中央网信办采取了卓有成效的管理举措。加强统一指挥和综合协调，使全国网络安全与信息化工作的领导和管理体系日益清晰；净化网络空间，清理恐怖视频，打击伪基站，传递正能量，网络思想文化生态正在好转；主办世界互联网大会，在伦敦会议、达沃斯论坛等国际场合，积极表达主张、公开宣示立场，让国际社会耳目一新，反响热烈，网络空间的大国形象和“中国信心”开始显现。一系列实招和实策让我们实实在在地感受到了网络治理方面的明显变化。当务之急，一是要进一步强化国家集中统一管理的网络空间制度安排，以组织落实尽快扭转“九龙治水”、政出多门的管理局面，形成统一指挥协调、多方配合支持的治理格局；二是要尽快提出网络空间国家战略，将中央在网络空间治理上的战略意图转化为国家的战略意志和发展规划，指导各行各业的信息化发展和网络治理实践。

（2）完善网络空间法治体系。以法治破解网络治理面临的各种难题，既是必经之途，更是必由之路。当前，关键是要抓住历史机遇，系统周密地推进和部署网络法制建设，破除“法必言外”的错误认识，解决“法难入网”的现实困难，形成“良法良治”的严格规范，营造“遵纪守法”的网络环境，将“依法治网”、“依法管网”作为我国网络空间治理的主线，以法治保障网络空间的长治久安。

（3）推进技术创新和产业发展。“自主可控、安全可靠”是网络的安全之道。自主，就是在关键的、重要的、核心的问题上摆脱受制于人的局面。可控，就是技术、产品未必是自己的，但能够管控住它。安全可靠，则是靠得住、信得过。当前条件下可按照“服务接管”、“产品替代”、“自主创新”的优先顺序和制度安排，围绕国家的发展需求，通过战略、规划、政策、技术进步等举措，逐步增强国家网络和信息安全可控能力，逐步形成自主可控的产业核心竞争力。

（4）增强网络正能量和全民安全意识。将网络作为联系群众的新纽带，体现了新一届党和国家领导人借网络凝聚中国力量的决心和信心。只要我们理解好网络，充分利用好网络，网络就是我们的播种机和宣传队，就能发挥“壮大主流思想舆论，弘扬主旋律，传播正能量，激发全社会团结奋进的强大力量”的效用，进而形成具有中国特色的网络文化。形成全民化的网络安全意识，才能使民众真正拥有和享受网络发展的红利，让民众、民智介入到信息化的发展进程当中。

（5）加强国际合作，贡献中国智慧。习总书记指出，互联网真正让世界变成地球村，

让国际社会越来越成为你中有我、我中有你的命运共同体。在这个开放的大格局中，“开放始终是发展的命根子”，也是网络空间安全战略的本质所在。在和平、发展、合作、共赢的世界潮流下，以促进多极化发展为目的，处理好中美新型大国关系，与世界其他国家相互包容，互惠互利，构建网络空间的“命运共同体”和“利益共同体”，营造和平与发展的国际网络大环境。刚刚举办的 APEC 会议和世界互联网大会，都显示中国的大国责任越来越多，话语权也越来越多。我们需要充分用好国际规则，主动平衡责权利关系，在确保国家主权和根本利益的前提下，积极主动地参与网络空间的国际共治，不断扩大话语权、参与权和主导权，为国际网络治理贡献中国力量和中国智慧，体现全球网络空间的中国担当。

3.2.3　国家信息安全法规和保障体系框架设想

20 世纪 80 年代以前，人们认为信息安全就是通信保密，采用的保障措施是加密和基于计算机规则的访问控制，这个时期被称为通信保密（COMSEC）时代。到了 20 世纪 90 年代，人们的认识加深了，大家逐步意识到数字化信息除了有保密性（保证信息不泄漏给未经授权的人）需要外，还有信息的完整性（防止信息被未经授权的篡改，保证真实的信息从真实的信源无失真地达到真实的信宿）、信息和信息系统的可用性（保证信息及信息系统确实为授权使用者所用，防止由于计算机病毒或其他人为因素造成的系统拒绝服务，或为敌手可用）需求。因此，明确提出了信息安全（INFOSEC）就是要保证信息的保密性、完整性和可用性，这就进入了信息安全时代。20 世纪 90 年代后期到现在，认识进一步加深，在原来的基础上增加了信息和系统的可控性（对信息及信息系统实施安全监控管理）、信息行为的不可否认性（保证信息行为人不能否认自己的行为）。同时被动的保护不能保障安全，还需要相应地增加系统脆弱性检测、入侵检测、安全事件的响应和损毁系统的恢复等，形成了包括保护、检测、反应、恢复 4 个环节的信息保障（IA）的概念，称为 PDRR 模型，这就宣告了信息安全保障时代的到来。

我国信息安全保障的国家战略目标是：保证国民经济基础设施的信息安全，抵御有关国家、地区、集团可能对我国实施“信息站”的威胁和打击国内外的高技术犯罪，保障国家安全、社会稳定和经济发展。信息安全战略防御的重点任务是：保护国民经济中的国家关键基础设施，包括金融、银行、税收、能源生产储备、粮油生产储备、水电气供应、交通运输、邮电通信、广播电视、商业贸易等国家关键基础设施。

由于信息安全保障是一个复杂的社会系统工程，基于此概念，必须建立一个国家信息安全保障的框架，主要包括如下几部分。

（1）要加快信息安全立法、建立信息安全法制体系，这样才能做到有法可依，有法必依。

（2）要建立国家信息安全组织管理体系，加强国家信息安全机构及职能，建立高效能的职，职责分工明确的行政管理和业务组织体系，建立信息安全标准和评价体系。

（3）要建立国家信息安全技术保障体系，使用科学技术，实施安全的防护保障。

（4）在技术保障体系下，要建立国家信息安全保障基础设施，其中包括：建立国家重要的信息安全管理中心（风险管理、入侵检测、内容安全与监管等）和密码管理中心（KMI/PKI），建立国家安全事件应急响应中心（病毒、安全事件、国际协同等）；建立数据备份和灾难恢复设施；在国家执法部门建立高技术刑事侦查队伍，提高对高技术犯罪的预防和侦破能力；建立国家信息安全认证机构，对产品和资质进行认证。

（5）要建立国家信息安全经费保障体系，加大信息安全投入。

（6）要高度重视人才培养，建立信息安全人才培养基地。

信息系统的信息保障技术层面分为以下 5 个部分。

（1）应用环境：包括局域网内所使用的主机、服务器、应用程序和数据操作系统、数据库等的安全防御。

（2）应用区域边界：通过部署边界保护措施和监控对内部局域网的访问，实现局域网在这一层连到广域网是安全的。

（3）网络和电信传输：包括实现局域网互连过程的安全，旨在确保通信的机密性，防止使通信能力中断的拒绝服务攻击。

（4）安全管理中心：用于保护、分析和响应本地、地区和国家级非法访问、入侵和网络攻击。

（5）密码管理中心：提供一种通用的联合处理方式，以便安全地创建、分发和管理公钥证书和传统的对称密钥，使它们能够为网络传输、应用区域边界和应用环境提供安全服务。

应尽快开展以下几个方面的工作。

（1）统一认识，加强领导。我们应该积极吸收发达国家对信息保障集中管理的经验，树立国家信息化领导小组统一指挥的绝对权威，进行信息安全保障的重大决策，制定发展政策，协调各方关系，加强对信息安全的宏观筹划和控管力度。在此基础上，针对当前信息安全工作存在的职能交叉、多头管理、重复建设、资源浪费等问题，科学合理地对编制体制进行调整重组，尽快理顺管理体制，实施科学分工，明确各自职责。

（2）抓紧制定信息安全保障体系框架。目前和今后相当长时期内，我国的战略重点是发展国家经济，但是霸权主义和恐怖主义时刻威胁着人类的和平，为了保障我国的安全，确保国家信息化建设顺利进行，实现跨越式发展，有必要制定与我国发展战略相适应的信息安全保障体系的纲领性文件。我们要借鉴别国的有关经验，但决不能刻意消防。

（3）把信息系统的安全作为“系统工程”统筹规划，加强一体化建设。信息安全保障体系建设是一个复杂的系统工程。国内外经验证明，“信息系统的安全保障问题只能作为一个整体来通盘加以解决”。这有两层含义：其一，安全信息系统不可缺少的有机组成部分，应在规划、开发信息系统之初，同时全面、协调地研究、设计系统的安全，这样才能使之具有最大安全互操作性、最好保密互通能力和最高通信效率，而不能按照以前“先建源系统（即安全系统）”的不科学做法；其二，不能“各自为政”，即不能分别孤立地设计、开发各个信息子系统的安全，而应综合规划整个信息大系统的安全事宜。根据我国信息系统发展现状，信息安全保障体系建设面临着非常繁重的任务。其中包括对已建计算机

网络进行信息安全体系配套改造，加快在建网络的安全体系同步建设进程，逐步做到在建网络系统与信息安全系统同步规划、同步论证、同步实施。

（4）加大对信息安全保障体系建设经费的投入。加大对信息安全保障体系建设经费的投入重点是加大科研投入和产业发展的投入。国家应有一个统一规划的科研经费投资计划，从而可以集中力量，突破技术难关，避免重复投资。国家还要增加对信息安全产业发展的资金投入，鼓励风险投资，创造良好的融资环境。

（5）重视人才培养。信息保障体系的建设对人才培养和使用提出了全新的要求。培育和形成信息保障人才资源优势，必须确立新的人才观，进一步深化人才队伍、干部队伍培养使用机制改革。人才是全方位的，除了要培养信息网络安全专家外，还要有信息安全的法律和管理专家。要重视优秀高科技人才的使用和领导干部队伍的年轻化、知识化建设，通过各种途径培养高学历的人才群体，依靠他们实现观念更新的跨越，以及思维和谋略的创新。

3.2.4　云计算、云数据中心及云安全

1．狭义云计算

云计算是并行计算（Parallel Computing）、分布式计算（Distributed Computing）和网格计算（Grid Computing）的发展。云计算是虚拟化（Virtualization）、效用计算（Utility Computing）、IaaS（基础设施即服务）、PaaS（平台即服务）、SaaS（软件即服务）等概念混合演进并跃升的结果。提供资源的网络被称为“云”。

2．广义云计算

“云”是一些可以自我维护和管理的虚拟计算资源，通常为一些大型服务器集群，包括计算服务器、存储服务器、宽带资源等。云计算将所有的计算资源集中起来，并由软件实现自动管理，无须人为参与。这使得应用提供者无须为烦琐的细节而烦恼，能够更加专注于自己的业务，有利于创新和降低成本。

（1）用户所需的资源不在客户端而来自网络。这是云计算的根本理念所在，即通过网络提供用户所需的计算力、存储空间、软件功能和信息服务等。

（2）服务能力具有分钟级或秒级的伸缩能力。如果资源结点服务能力不够，但是网络流量上来，这时候需要平台在一分钟或几分钟之内，自动地动态增加服务结点的数量，如从 100 个结点扩展到 150 个结点。能够称之为云计算，就需要足够的资源来应对网络的尖峰流量，流量下来了，服务结点的数量再随着流量的减少而减少。现在有的传统互联网数据中心自称也能提供伸缩能力，但需要多个小时之后才能提供给用户。问题是网络流量是不可预期的，不可能等那么久。

（3）具有较之传统模式 5 倍以上的性能价格比优势。看了上面一条，有些读者可能在想，没关系，多配一些机器，流量再大也应付得了。但这不是云计算的理念。还有个性能

价格比指标。云计算之所以是一种划时代的技术，就是因为它将数量庞大的廉价计算机放进资源池中，用软件容错来降低硬件成本，通过规模化的共享使用来提高资源利用率。国外代表性云计算平台提供商达到了惊人的 10～40 倍的性能价格比提升。国内由于技术、规模和统一电价等问题，暂时难以达到同等的性能价格比，我们暂时将这个指标定为 5 倍。拥有 256 个结点的云计算平台已经达到了 5～7 倍的性能价格比提升，其性能价格比随着规模和利用率的提升还有提升空间。

3．云数据中心

云数据中心是一种为提供云计算服务而建设的数据中心。与传统 IDC（互联网数据中心）和 EDC（企业数据中心）的区别在于所应对的业务模式不同。传统 IDC 多数是支撑电信运营商数据业务，并有明确的跨网和区域性限制。EDC 更多地支持了以商业软件为平台的特定应用信息系统，因此其规模、等级、变量相对固定。而云计算所需要的数据中心来源于互联网，但又向集成化平台演进，因此，云计算数据中心从基础设施到计算与应用是连续和整体的，并相互关联和可适应。

4．云安全

云安全通过网状的大量客户端对网络中软件行为的异常进行监测，获取互联网中木马、恶意程序的最新信息，推送到服务端进行自动分析和处理，再把病毒和木马的解决方案分发到每一个客户端。云安全的策略构想是：使用者越多，每个使用者就越安全，因为如此庞大的用户群，足以覆盖互联网的每个角落，只要某个网站被挂马或某个新木马病毒出现，就会立刻被截获。

云安全的核心思想是建立一个分布式统计和学习平台，以大规模用户的协同计算来过滤垃圾邮件：首先，用户安装客户端，为收到的每一封邮件计算出一个唯一的“指纹”，通过比对“指纹”可以统计相似邮件的副本数，当副本数达到一定数量，就可以判定邮件是垃圾邮件；其次，由于互联网上多台计算机比一台计算机掌握的信息更多，因而可以采用分布式贝叶斯学习算法，在成百上千的客户端机器上实现协同学习过程，收集、分析并共享最新的信息。反垃圾邮件网格体现了真正的网格思想，每个加入系统的用户既是服务的对象，也是完成分布式统计功能的一个信息结点，随着系统规模的不断扩大，系统过滤垃圾邮件的准确性也会随之提高。用大规模统计方法来过滤垃圾邮件的做法比用人工智能的方法更成熟，不容易出现误判假阳性的情况，实用性很强。反垃圾邮件网格就是利用分布互联网里的千百万台主机的协同工作，来构建一道拦截垃圾邮件的“天网”。

3.2.5 互联网与物联网及其主要特点

互联网（Internet）又称网际网路或音译为因特网、英特网，是网络与网络之间所串连成的庞大网络，这些网络以一组通用的协定相连，形成逻辑上的单一巨大国际网络。这种

将计算机网络互相联接在一起的方法可称作“网络互联”，在这基础上发展出覆盖全世界的全球性互联网络称为“互联网”，即“互相联接在一起的网络”。互联网并不等同万维网（World Wide Web，WWW），万维网只是一建基于超文本相互链接而成的全球性系统，且是互联网所能提供的服务其中之一。

物联网（Internet of Things）指的是将无处不在的末端设备和设施，包括具备“内在智能”的传感器、移动终端、工业系统、楼控系统、家庭智能设施、视频监控系统等和“外在使能”的，如贴上 RFID 的各种资产、携带无线终端的个人与车辆等“智能化物件或动物”或“智能尘埃”，通过各种无线/有线的长距离/短距离通信网络实现互联互通、应用大集成，以及基于云计算的 SaaS 营运等模式，提供安全可控乃至个性化的实时在线监测、定位追溯、报警联动、调度指挥、预案管理、远程控制、安全防范、远程维保、在线升级、统计报表、决策支持、领导桌面（集中展示的 Cockpit Dashboard）等管理和服务功能，实现对“万物”的“高效、节能、安全、环保”的“管、控、营”一体化。

简单地讲，物联网是物与物、人与物之间的信息传递与控制，和传统的互联网相比，物联网有其鲜明的特征。

首先，它是各种感知技术的广泛应用。物联网上部署了海量的多种类型传感器，每个传感器都是一个信息源，不同类别的传感器所捕获的信息内容和信息格式不同。传感器获得的数据具有实时性，按一定的频率周期性地采集环境信息，不断更新数据。

其次，它是一种建立在互联网上的泛在网络。物联网技术的重要基础和核心仍旧是互联网，通过各种有线和无线网络与互联网融合，将物体的信息实时准确地传递出去。在物联网上的传感器定时采集的信息需要通过网络传输，由于其数量极其庞大，形成了海量信息，在传输过程中，为了保障数据的正确性和及时性，必须适应各种异构网络和协议。

还有，物联网不仅提供了传感器的连接，其本身也具有智能处理的能力，能够对物体实施智能控制。物联网将传感器和智能处理相结合，利用云计算、模式识别等各种智能技术，扩充其应用领域。从传感器获得的海量信息中分析、加工和处理出有意义的数据，以适应不同用户的不同需求，发现新的应用领域和应用模式。

根据其实质用途可以归结为以下三种基本应用模式。

（1）对象的智能标签。通过二维码，RFID 等技术标识特定的对象，用于区分对象个体，例如在生活中人们使用的各种智能卡、条码标签的基本用途就是用来获得对象的识别信息；此外通过智能标签还可以用于获得对象物品所包含的扩展信息，例如智能卡上的金额余额，二维码中所包含的网址和名称等。

（2）环境监控和对象跟踪。利用多种类型的传感器和分布广泛的传感器网络，可以实现对某个对象的实时状态的获取和特定对象行为的监控，如使用分布在市区的各个噪声探头监测噪声污染，通过二氧化碳传感器监控大气中二氧化碳的浓度，通过 GPS 标签跟踪车辆位置，通过交通路口的摄像头捕捉实时交通流程等。

（3）对象的智能控制。物联网基于云计算平台和智能网络，可以依据传感器网络用获取的数据进行决策，改变对象的行为进行控制和反馈。例如，根据光线的强弱调整路灯的

亮度，根据车辆的流量自动调整红绿灯间隔等。

3.2.6 全球能源互联网及其关键技术

能源互联网指的是横向实现电、气、热、可再生能源等“多源互补”，纵向实现“源-网-荷-储”各环节高度协调，生产和消费双向互动，集中与分布相结合的能源服务网络。从互联网观念出发，能源互联网的主要特征体现在开放、互联、对等、分享；而从能源供应网络出发，能源互联网主要体现在：从就地控制到区域控制，再到全局控制的逐步发展、扩充与完善过程。能源互联网及其关键技术如下。

（1）一带一路。“一带一路”（One Belt And One Road，OBAOR；或 One Belt One Road，OBOR；或 Belt And Road，BAR）是“丝绸之路经济带”和“21 世纪海上丝绸之路”的简称。“一带一路”必将促进我国与俄罗斯、哈萨克斯坦、土库曼斯坦等邻国在石油、天然气、电力和新能源等能源领域的广泛深入合作，因此“全球能源互联网”是结合“一带一路”发展战略打开能源领域的全球视野。

（2）一极一道。从世界清洁能源资源分布来看，北极圈及其周边地区（“一极”）风能资源和赤道及附近地区（“一道”）太阳能资源十分丰富，简称“一极一道”。集中开发北极风能和赤道太阳能资源，通过特高压等输电技术送至各大洲负荷中心，与各洲大型能源基地和分布式电源相互支撑，提供更安全、更可靠的清洁能源供应，将是未来世界能源发展的重要方向。

（3）清洁替代。清洁替代，是指在能源开发上，以清洁能源替代化石能源，走低碳绿色发展道路，逐步实现从化石能源为主、清洁能源为辅向清洁能源为主、化石能源为辅转变。清洁替代将从根本上解决人类能源供应面临的资源约束和环境约束问题，是实现能源可持续利用的战略举措，也是未来全球能源发展的必然趋势。

（4）电能替代。电能替代，是指在能源消费上，以电能替代煤炭、石油、天然气等化石能源的直接消费，提高电能在终端能源消费中的比重。随着电气化进程加快，电能将在终端能源消费中扮演日益重要的角色，并最终成为最主要的终端能源品种，实现更加清洁、便捷、安全的能源利用。

（5）全球能源观。全球能源观是遵循能源发展规律，适应能源发展新趋势形成的关于全球能源可持续发展的基本观点和理论。全球能源观的核心是坚持以全球性、历史性、差异性、开放性的观点和立场来研究和解决世界能源发展问题，更加注重能源与政治、经济、社会、环境的协调发展，更加注重各种集中式（基地式）与分布式清洁能源的统筹开发，要求以“两个替代”为方向，以全球能源互联网为载体，统筹全球能源资源开发、配置和利用，保障世界能源安全、清洁、高效、可持续供应。

（6）国家泛在智能电网。国家泛在智能电网是全球能源互联网的基本组成单元，广泛连接国内能源基地、各类分布式电源和负荷中心，并与周边国家的能源互连互通，承接全球能源互联网跨国跨洲配置的清洁能源。国家泛在智能电网应坚持坚强与智能并重的发展原则，在发挥大电网和坚强网架作用的基础上，有效解决清洁能源发电随机性、间歇性问

题，实现各地集中式电源与泛在分布式电源的优化接入和高效消纳，更可靠地保障能源供应。

（7）电源技术。以清洁能源为主导，以电为中心的能源格局，决定了电源技术在未来能源发展中的关键性作用。其核心是不断提高清洁能源的开发效率和经济性，重点领域包括风力发电、太阳能发电、海洋能发电及分布式电源技术等。这些技术突破是构建全球能源互联网的动力之源，对推动全球能源开发清洁化、低碳化十分重要。

（8）电网技术。以电为中心、全球配置的能源发展格局，决定了电网技术在未来能源发展中的关键性作用，需要不断提高电网输送能力、配置能力和经济性，重点围绕电力系统各环节，加快智能电网技术全面创新，主要领域包括特高压输电技术和装备、海底电缆技术、超导输电技术、直流电网技术、微电网技术和大电网运行控制技术等。这些技术突破是构建全球能源互联网的重要基础。

（9）储能技术。储能技术发展是保障清洁能源大规模发展和电网安全经济运行的关键。储能技术可以在电力系统中增加电能存储环节，使得电力实时平衡的“刚性”电力系统变得更加“柔性”，特别是平抑大规模清洁能源发电接入电网带来的波动性，提高电网运行的安全性、经济性、灵活性。储能技术一般分为热储能和电储能，未来应用于全球能源互联网的主要是电储能。

（10）信息通信技术。信息通信技术是实现电网智能化、互动化和大电网运行控制的重要基础，被认为是 21 世纪社会发展和世界经济增长的重要动力，是多种技术的融合，以及与多种产业的跨界融合，正在带来深刻的产业革命。要适应全球能源互联网的发展、信息通信的内容快速增长、信息通信的范围大幅扩张，就要对信息通信的安全性、实时性、可靠性要求更加严格，这迫切需要在信息通信技术领域有更大的创新和突破。

3.3　信息化工程最新应用技术

本节主要介绍新一代移动通信技术、内存计算技术、智慧城市新技术，海量大数据及智能电网有哪些特点，电子商务的概念及应用。

3.3.1　新一代移动通信技术的主要特点及应用情景

1．移动通信技术的发展历程

第一代（1G）移动通信系统的主要特征是采用模拟技术和频分多址（FDMA）技术，有多种制式。我国主要采用 TACS，其传输速率为 2.4kb/s，由于受到传输带宽的限制，不能进行移动通信的长途漫游，只是一种区域性的移动通信系统。

第二代（2G）移动通信系统采用的技术主要有时分多址（TDMA）和码分多址（CDMA）两种技术，它能够提供 9.6～28．8kb/s 的传输速率。全球主要采用 GSM 和 CDMA 两种制

式，我国采用的主要是 GSM 这一标准。第二代移动通信系统具有保密性强，频谱利用率高，能提供丰富的业务，标准化程度高等特点，可以进行省内外漫游。

第三代（3G）移动通信系统在国际上统称为 IMT-2000，是国际电信联盟（ITU）在 1985 年提出的工作在 2000MHz 频段的系统。与第一代模拟移动通信和第二代数字移动通信系统相比，第三代的最主要特征是可提供移动多媒体业务。

第四代（4G）移动通信系统也称为广带接入和分布网络，具有超过 2Mb/s 的非对称数据传输能力，对高速移动用户能提供 150Mb/s 的高质量的影像服务，并首次实现三维图像的高质量传输。它包括广带无线固定接入、广带无线局域网、移动广带系统和互操作的广播网络（基于地面和卫星系），是集多种无线技术和无线 LAN 系统为一体的综合系统，也是宽带 IP 接入系统。

2．新一代 4G 移动通信系统的主要特点

1）通信速度更快

第一代模拟式仅提供语音服务；第二代数位式移动通信系统传输速率也只有 9.6kb/s，最高可达 32kbp/s；而第三代移动通信系统数据传输速率可达到 2Mb/s；第四代移动通信系统可以达到 10Mb/s 至 20Mb/s，甚至最高可以达到 100Mb/s 的速度传输无线信息，这种速度相当于 2009 年最新手机的传输速度的一万倍左右。

2）网络频谱更宽

4G 通信达到 100Mb/s 的传输速率，必须在 3G 通信网络的基础上，进行大幅度的改造和研究，使 4G 网络在通信带宽上比 3G 网络的蜂窝系统的带宽高出许多。每个 4G 信道会占有 100MHz 的频谱，相当于 W-CDMA 3G 网络的 20 倍。

3）通信更加灵活

4G 手机是一部小型计算机，人们可以想象的是，眼镜、手表、化妆盒、旅游鞋，以方便和个性为前提，任何一件能看到的物品都有可能成为 4G 终端。4G 通信使人们不仅可以随时随地通信，更可以双向下载传递资料、图画、影像，当然更可以和从未谋面的陌生人在网上联线对打游戏。

4）智能性能更高

第四代移动通信的智能性更高，不仅表现于 4G 通信的终端设备的设计和操作具有智能化，更重要的是 4G 手机可以实现许多难以想象的功能。4G 手机可以把电影院票房资料，直接下载到 PDA 之上，这些资料能够把售票情况、座位情况显示得清清楚楚，大家可以根据这些信息来进行在线购票，用来看体育比赛之类的各种现场直播。

5）兼容性能更平滑

要使 4G 通信尽快地被人们接受，除了要考虑它的功能强大外，还应该考虑到现有通信的基础，第四代移动通信系统具备全球漫游、接口开放、能与多种网络互联、终端多样化以及能从第二代平稳过渡等特点。

6）提供各种增值服务

3G 移动通信系统是以 CDMA 为核心技术，而 4G 移动通信系统技术则以正交多任务

分频技术（OFDM）为基础，可以实现例如无线区域环路（WLL）、数字音讯广播（DAB）等方面的无线通信增值服务；第四代移动通信系统不仅采用 OFDM 一种技术，CDMA 技术会在第四代移动通信系统中，与 OFDM 技术相互配合以便发挥出更大的作用，甚至会有新的整合技术 OFDM/CDMA 产生两种技术的结合。

7）实现更高质量的多媒体通信

尽管第三代移动通信系统也能实现各种多媒体通信，而第四代移动通信系统提供的无线多媒体通信服务包括语音、数据、影像等大量信息透过宽频的信道传送出去，为此第四代移动通信系统也称为“多媒体移动通信”。

8）频率使用效率更高

第四代移动通信技术在开发研制过程中使用和引入许多功能强大的突破性技术，例如，一些光纤通信产品公司为了进一步提高无线因特网的主干带宽宽度，引入了交换层级技术，这种技术能同时涵盖不同类型的通信接口，也就是说第四代主要是运用路由技术为主的网络架构。由于利用了几项不同的技术，所以无线频率的使用比第二代和第三代系统有效得多。

3.3.2　海量大数据及其主要特点

大数据技术（Big Data），或称巨量资料，指的是所涉及的资料量规模巨大到无法通过目前的主流软件工具，在合理的时间内达到撷取、管理、处理并整理成为帮助企业经营决策更积极目的的信息。

1．大数据的 4V 特点

大数据具有 4V 特点：Volume（大量）、Velocity（高速）、Variety（多样）、Value（价值）。第一，数据体量巨大，从 TB 级别跃升到 PB 级别。第二，数据类型繁多，如网络日志、视频、图片、地理位置信息等。第三，要求实时性强，处理速度快，1 秒定律。物联网、云计算、移动互联网、车联网、手机、平板电脑、PC 以及遍布地球各个角落的各种各样的传感器，无一不是数据来源或者承载的方式，可从各种类型的数据中快速获得高价值的信息。第四，各行各业均存在大数据，但是众多的信息和资源是纷繁复杂的，需要搜索、处理、分析、归纳、总结其深层次的规律。

2．大数据的采集

科学技术及互联网的发展，推动着大数据时代的来临，各行各业每天都在产生数量巨大的数据碎片，数据计量单位已从 B、KB、MB、GB、TB 发展到 PB、EB、ZB、YB 甚至 BB、NB、DB 来衡量。大数据时代数据的采集也不再是技术问题，只是面对如此众多的数据，我们怎样才能找到其内在规律?

3．大数据的挖掘和处理

大数据必然无法用人脑来推算、估测，或者用单台的计算机进行处理，必须采用分布

式计算架构，依托云计算的分布式处理、分布式数据库、云存储和虚拟化技术，因此，大数据的挖掘和处理必须用到云技术。

4．大数据的应用

大数据可应用于各行各业，将人们收集到的庞大数据进行分析整理，实现资讯的有效利用。这就需要采用大数据技术，进行分析比对，挖掘主效基因。

大数据分析包括以下 5 个基本方面。

（1）可视化分析。大数据分析的使用者有大数据分析专家，同时还有普通用户，但是他们二者对于大数据分析最基本的要求就是可视化分析，因为可视化分析能够直观地呈现大数据的特点，同时能够非常容易地被读者所接受，就如同看图说话一样简单明了。

（2）数据挖掘算法。大数据分析的理论核心就是数据挖掘算法，各种数据挖掘的算法基于不同的数据类型和格式才能更加科学地呈现出数据本身具备的特点，也正是因为这些被全世界统计学家所公认的各种统计方法（可以称之为真理）才能深入数据内部，挖掘出公认的价值。另一个方面也是因为有了这些数据挖掘的算法才能更快速地处理大数据，如果一个算法得花上好几年才能得出结论，那大数据的价值也就无从说起了。

（3）预测性分析能力。大数据分析最重要的应用领域之一就是预测性分析，从大数据中挖掘出特点，通过科学地建立模型，之后便可以通过模型带入新的数据，从而预测未来的数据。

（4）语义引擎。大数据分析广泛应用于网络数据挖掘，可从用户的搜索关键词、标签关键词或其他输入语义，分析、判断用户需求，从而实现更好的用户体验和广告匹配。

（5）数据质量和数据管理。大数据分析离不开数据质量和数据管理，高质量的数据和有效的数据管理，无论是在学术研究还是在商业应用领域，都能够保证分析结果的真实和有价值。大数据分析的基础就是以上 5 个方面，当然要更加深入大数据分析的话，还有很多很多更加有特点的、更加深入的、更加专业的大数据分析方法。

3.3.3 智慧城市的含义及其新技术

智慧城市就是把信息技术与城市建设融合在一起，将城市信息化推向更高阶段。它基于互联网、云计算、大数据、物联网、社交网络等工具和方法，实现全面透彻的感知、宽带泛在的互联和智能融合的应用。智慧城市将成为一个城市的整体发展战略，作为经济转型、产业升级、城市提升的新引擎，达到提高民众生活幸福感、企业经济竞争力、城市可持续发展的目的，体现了更高的城市发展理念和创新精神。伴随着网络帝国的崛起、移动技术的融合发展以及创新理念的广泛普及，知识社会环境下的智慧城市是继数字城市之后信息化城市发展的高级形态。

智慧城市包含智慧技术、智慧产业、智慧（应用）项目、智慧服务、智慧治理、智慧人文、智慧生活等内容。对智慧城市建设而言，智慧技术的创新和应用是手段和驱动力，智慧产业和智慧（应用）项目是载体，智慧服务、智慧治理、智慧人文和智慧生活是目标。

具体说来，智慧（应用）项目体现在：智慧交通、智能电网、智慧物流、智慧医疗、智慧食品系统、智慧药品系统、智慧环保、智慧水资源管理、智慧气象、智慧企业、智慧银行、智慧政府、智慧家庭、智慧社区、智慧学校、智慧建筑、智能楼宇、智慧油田、智慧农业等诸多方面。

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。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）。信息通信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”。创新形态由生产范式向服务范式转变，也带动了产业形态、政府管理形态、城市形态由生产范式向服务范式的转变。如果说创新 1.0 是工业时代沿袭的面向生产、以生产者为中心、以技术为出发点的相对封闭的创新形态，创新 2.0 则是与信息时代、知识社会相适应的面向服务、以用户为中心、以人为本的开放的创新形态。

建设智慧城市，也是转变城市发展方式、提升城市发展质量的客观要求。通过建设智慧城市，及时传递、整合、交流、使用城市经济、文化、公共资源、管理服务、市民生活、生态环境等各类信息，提高物与物、物与人、人与人的互连互通、全面感知和利用信息能力，从而能够极大提高政府管理和服务的能力，极大提升人民群众的物质和文化生活水平。建设智慧城市，会让城市发展更全面、更协调、更可持续，会让城市生活变得更健康、更和谐、更美好。

对比数字城市和智慧城市，可以发现以下 6 个面的差异。

（1）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。

（2）数字城市通过城市各行业的信息化提高了各行业的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。

（3）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。

（4）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。

（5）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。

（6）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。

智慧城市不但广泛采用物联网、云计算、人工智能、数据挖掘、知识管理、社交网络等技术工具，也注重用户参与、以人为本的创新 2.0 理念及其方法的应用，构建有利于创新涌现的制度环境，以实现智慧技术高度集成、智慧产业高端发展、智慧服务高效便民、以人为本持续创新，完成从数字城市向智慧城市的跃升。智慧城市将是创新 2.0 时代以人为本的可持续创新城市。

3.3.4 内存计算技术及其应用案例

1．内存计算技术的基本原理

在软件、硬件系统协同配置环境下，将数据库及数据仓库移到内存中进行的运算，突破 I/O 瓶颈限制，采用高效并行处理技术，基于内存的高效数据读取和处理以及智能数据字典等高效的数据压缩机制，支持行存储和列存储的内存数据库，支持同时提供 OLTP 交易系统和 OLAP 分析系统。利用虚拟数据模型，实现内存数据仓库数据的高效率计算功能，减少冗余的数据，应用内置的计算引擎，将原来在应用层进行的运算转移到数据库层面处理，对数据密集型运算，优化应用层和数据库层之间的数据交互，从而从整体上提升系统的效率。

2．内存计算技术的主要特点

1）基于内存的高效数据读取和处理

从数据库中读取数据因为磁盘 I/O 的性能限制而成为瓶颈，原因是传统数据库实际上是将数据以文件的形式存储在磁盘上并为应用提供访问数据的接口，从数据库中读取数据的本质是从磁盘上读取文件。在过去几十年的硬件发展中，内存和 CPU 的性能始终在飞速提升，只有磁盘 I/O 的性能提升并不明显。从磁盘上读取数据的速度是毫秒级，而从内存中读取数据的速度是纳秒级，基于内存的数据读取比基于磁盘的数据读取性能要快 100 万倍。所以当基于数据仓库进行报表分析时，如果从传统数据库中读取海量数据需要数十分钟的时间，那么从 SAP HANA 中读取同样的数据只需要不到一秒钟的时间。

2）行存储和列存储的混合模式

传统关系型数据库是按照行的方式存储数据的，能够为交易系统即 OLTP 应用提供高效的支持。例如，一个零售商每当客户购买产品时，需要在业务系统中创建一条数据记录销售的时间、地点、客户、金额、地址等字段数据，当前端完成数据的录入并提交后台系统后，在数据库中会在数据表中插入一行记录，这条记录中会包含本次销售业务操作相关的数据。然而，基于行存储的数据库在支持数据分析应用即 OLAP 应用时则显得低效和力不从心。

同样的例子，假设这家零售公司在传统数据库中保存了三亿条记录，并且需要基于这些销售记录分析单笔销售的平均金额，则需要首先读取所有这三亿条记录，并取出其中的

销售金额这一个字段，然后再进行平均值计算。这意味着实际进行分析的数据（消费金额字段）只占总体数据的 5%（假设每条数据 20 个字段）。显然这是非常低效的方式。而在基于列存储的机制中，这三亿条记录实际上是按照列进行存储，即总共只有 20 条记录（20 个字段，每个字段一条记录）。在进行同样的分析时，只需要取出销售金额这一列的记录并计算平均值即可，与基于行存储的机制相比，在这个示例的应用场景下，数据处理的效率提高了 50 倍。

3）高效的并行处理机制

近几年，硬件服务器的处理器主频提升并不明显，但是单台服务器开始配置更多的 CPU，并且每个 CPU 包含更多的内核。提升并行处理的能力，才能够在新的硬件发展趋势下保证系统的性能能够持续提升。

SAP HANA 支持多服务器、多处理器的高效并行处理，能够最高效、充分地利用多处理器的并发能力。能够拆解数据模型，分成可以并行执行的步骤，也能够将数据处理和运算拆分并部署到多个处理器。例如，计算引擎可以将数据模型拆解，将一些 SQL 脚本拆分成可以并行执行的步骤。这些操作将递交给数据库优化器来决定最佳的访问行存储和列存储的方案。

4）高效的数据压缩优化内存利用

SAP HANA 的基本机制是将数据全部存储到内存中，以进行高效的数据访问和运算。虽然硬件包括内存的价格日趋低廉，但相比磁盘而言，内存仍是较贵的存储设备。而在企业系统中数据增长迅速，达到数 TB 甚至数十 TB 的情况下，将所有数据原封不动地导入内存仍将带来较大的硬件投资。为了帮助企业节省这一部分投资，SAP HANA 中采取了基于智能数据字典等高效的数据压缩机制，能够将数据压缩 5～20 倍，从而充分节约硬件投资。

5）虚拟建模减少数据冗余

在 SAP HANA 中，将源数据导入内存后，在 HANA 中的虚拟建模，一个属性视图可以被看作为一个数据立方体，属性视图不存储任何数据，数据存储在列存储表中，系统只保存这些数据模型内表的构际关系以及数据的运算逻辑，当前端提交分析请求时，HANA 会根据虚拟数据模型进行数据的计算并将结果提交给前端。这意味着 HANA 中不会存在冗余的数据，从而大大节约了硬件的投资和维护成本。

另外，虚拟模型可以进行灵活的创建、修改、删除，从而满足业务的需求变化，而无须担心对整体数据仓库数据结构的影响。在传统数据仓库中，通过 ETL 方式抽取数据并加载到数据模型中往往需要数小时甚至更长的时间，而在 HANA 的架构下，后端数据处理和加载的时间将大大缩短，从而减少 IT 部门运维系统投入的时间和精力，并为前端数据处理提供更长的时间窗口，减少数据不一致性发生的可能。

6）在数据库层面进行数据密集型运算

SAP HANA 除了提供完善的数据库功能外，其内置的计算引擎可以将原本在应用层进行的运算转移到数据库层面进行处理，这在数据密集型运算的场景中，能够优化应用层和数据库层之间的数据交互，从而从整体上提升系统的效率。传统上，数据密集型运算包括

计划、预测、模拟等，在 HANA 中首先将计划（Planning）引擎植入计算引擎中，从而使得基于 HANA 的计划应用的性能得到极大提升。

7）与 SAP ERP 紧密整合提供实时的数据可视性

SAP HANA 能够和 SAP ERP 紧密集成，将 ERP 中的数据利用 SLT（SAP Landscape Transformation）技术实时地复制到 HANA 的内存中，并基于这些数据建立数据分析的应用，从而为业务带来几个主要的好处：一是充分利用 HANA 的内存计算技术，基于大数据量进行高效、高速的数据分析和处理；二是减少传统的在 ERP 中直接分析这些数据给 ERP 系统带来的额外性能压力；三是利用基于 HANA 上的 BI 工具可以进行灵活的数据分析；四是基于实时数据进行分析，带来实时的业务洞察力；五是利用触发机制将 SAP ERP 中的数据能够实时同步到 HANA 中。

8）与 BOBJ Data Service 整合提升数据质量

SAP HANA 和 BOBJ Data Service 紧密整合，从第三方系统获取数据。Data Service 中提供可视化的数据抽取、清洗、加载以及数据质量管理的功能，能够保证进入 HANA 的数据都是高质量的数据，从而确保基于 HANA 进行数据分析的准确性，为业务决策提供更好的支持。

3．主要应用成果

在对辽宁电力 SAP HANA 实现了 10 类业务 36 个场景的验证中，速度平均提升 36 倍，普遍提升 20 倍左右，最高可达到 863 倍。在同一场景下，数据量越大，提升效率越明显。在已知的零售业验证中，报表的查询与执行速度提升了 1000 倍；物资项目管理从 15 小时降低到 4.8 秒；订单到付款分析，从 30 天降低到 28 秒。在 IT 领域有了重要突破。举例说明如下。

场景 1：公司账卡物一致率分析

在验证查询所有（36 个）ERP 上线单位的全部资产和设备（9.86GB）的条件下，使用 HANA 查询时间为 9s，使用 ERP 前台查询超时，通过后台作业查询时间为 7 769s（2.16 小时）（ERP 测试系统），性能提升 863 倍。使用 ERP 实时正式运行系统，查询时间为 5 574s（1.58h），性能提升 619 倍。

场景 2：购电充值卡统计分析与查询性能分析

在营销系统中，在 HANA 系统中，各个单位可以随时、实时地查看数据；不仅节省了操作流程，而且查询的时候，只有初始刷新数据时需要等待 5s，随后更换查询条件的时候，一单击，报表立刻就运行出来，不需要等待时间，所以报表整体性能的提升远大于 181 倍。

3.3.5 智能电网及其主要特点

智能电网是以包括各种发电设备、输配电网络、用电设备和储能设备的物理电网为基

础，将现代先进的传感测量技术、网络技术、通信技术、计算技术、自动化与智能控制技术等与物理电网高度集成而形成的新型电网，它能够实现可观测（能够监测电网所有设备的状态）、可控制（能够控制电网所有设备的状态）、完全自动化（可自适应并实现自愈）和系统综合优化平衡（发电、输配电和用电之间的优化平衡），它以充分满足用户对电力的需求和优化资源配置、确保电力供应的安全性、可靠性和经济性、满足环保约束、保证电能质量、适应电力市场化发展等为目的，实现对用户可靠、经济、清洁、互动的电力供应和增值服务。

智能电网是应用信息通信技术，实现电能从电网公司到用户的传输、分配、管理和控制，以达到节约能源和成本，实现对电力资源、电力客户、电力资产、电力运营、电力交易的产业链全过程的持续监视，利用“随需应变”的信息提高电网公司的管理水平、工作效率、电网可靠性和服务水平的新一代电力网络。

与传统电网比，智能电网进一步扩展对电网的监视范围和监视详细程度，整合各种管理信息和实时信息，为电网运行和管理人员提供更全面、完整和细致的电网状态视图，并加强对电力业务的分析和优化，改变过去那种基于有限的、时间滞后的信息进行电网管理的传统方式，利用电网实时信息和综合管理信息，与企业决策信息互相交换，促进电网企业实现更精细化和智能化的运行和管理。

1．数据采集

在实时数据采集上，智能电网大大扩展了监视控制与数据采集系统（Supervisory Control And Data Acquisition，SCADA）的数据采集范围和数量，提高了电网的“可视化”。

2．数据传输

智能电网需要采集大量的设备状态数据和客户计量数据。这两类数据的特点是：数据量大，采集点多且分散，对实时性要求比电网实时运行数据低，数据需要被多个系统和业务部门使用。

3．信息集成

众多的自动化系统和管理信息系统，积累了大量的数据。但是，长期以来条块分割和部门壁垒已经成为实现“数字化电网、信息化企业”的主要障碍。

4．动态作业管理

动态作业管理使得数据在传感器、控制中心和作业人员之间能够及时有效地流动，提高运维工作的效率和准确性。能够从各种电压、电流传感器、智能表计、设备状态监测传感器和线路监视传感器中，获得更多准确、及时的数据。通过这些数据，能够预测故障，在故障发生时，能够显示故障的位置和可能的故障原因。另外，动态作业管理能够降低作业成本，减少管理费用。

5．基于 IP 通信的 SCADA

采用标准的 Internet 通信协议，摆脱了对不同设备制造商提供的私有通信协议的依赖。IP SCADA 为智能电网中的传感器、智能表计和手持移动设备（PDA）等提供数据通信支持，能够有效降低通信成本 20%以上。其主要优点如下。

以客户为中心：提供更多样化的电力产品给客户选择，建设更好的渠道与用户实现互动，提供高附加值的服务，实现灵活的需求管理，降低电力价格。

支持分布式和可再生资源的接入：坚强的电网架构可以支持各类的非传统电源的接入，减少网损和污染气体排放。

负载和电源的本地交互：用户可以优先使用附近的分布式能源，减轻骨干电网的负担，提高供电可靠性。

高级自动化和分布式智能：以普遍使用的智能化设备为基础，电网具备自动识别和处理电网事故的能力。

灵活的电网运行：运行需求侧响应和管理，能灵活适应电网结构和电力供求变化，保障电力供应。

面向服务的架构：以面向服务的架构为基础，建设灵活开放的信息系统，实现各种服务的有效整合。

更可靠、安全的电力供应：提高电网输送容量和发电容量，改善电力供应的可靠性和质量，实现更灵活的电能存储。

其重要意义体现在以下几个方面。

（1）具备强大的资源优化配置能力。我国智能电网建成后，将实现大水电、大煤电、大核电、大规模可再生能源的跨区域、远距离、大容量、低损耗、高效率输送，区域间电力交换能力明显提升。

（2）具备更高的安全稳定运行水平。电网的安全稳定性和供电可靠性将大幅提升，电网各级防线之间紧密协调，具备抵御突发性事件和严重故障的能力，能够有效避免大范围连锁故障的发生，显著提高供电可靠性，减少停电损失。

（3）适应并促进清洁能源发展。电网将具备风电机组功率预测和动态建模、低电压穿越和有功无功控制以及常规机组快速调节等控制机制，结合大容量储能技术的推广应用，对清洁能源并网的运行控制能力将显著提升，使清洁能源成为更加经济、高效、可靠的能源供给方式。

（4）实现高度智能化的电网调度。全面建成横向集成、纵向贯通的智能电网调度技术支持系统，实现电网在线智能分析、预警和决策，以及各类新型发输电技术设备的高效调控和交直流混合电网的精益化控制。

（5）满足电动汽车等新型电力用户的服务要求。将形成完善的电动汽车充放电配套基础设施网，满足电动汽车行业的发展需要，适应用户需求，实现电动汽车与电网的高效

互动。

（6）实现电网资产高效利用和全寿命周期管理。可实现电网设施全寿命周期内的统筹管理。通过智能电网调度和需求侧管理，电网资产利用小时数大幅提升，电网资产利用效率显著提高。

（7）实现电力用户与电网之间的便捷互动。将形成智能用电互动平台，完善需求侧管理，为用户提供优质的电力服务。同时，电网可综合利用分布式电源、智能电能表、分时电价政策以及电动汽车充放电机制，有效平衡电网负荷，降低负荷峰谷差，减少电网及电源建设成本。

（8）实现电网管理信息化和精益化。将形成覆盖电网各个环节的通信网络体系，实现电网数据管理、信息运行维护综合监管、电网空间信息服务以及生产和调度应用集成等功能，全面实现电网管理的信息化和精益化。

（9）发挥电网基础设施的增值服务潜力。在提供电力的同时，服务国家“三网融合”战略，为用户提供社区广告、网络电视、语音等集成服务，为供水、热力、燃气等行业的信息化、互动化提供平台支持，拓展及提升电网基础设施增值服务的范围和能力，有力推动智能城市的发展。

（10）促进电网相关产业的快速发展。电力工业属于资金密集型和技术密集型行业，具有投资大、产业链长等特点。建设智能电网，有利于促进装备制造和通信信息等行业的技术升级，为我国占领世界电力装备制造领域的制高点奠定基础。

与现有电网相比，智能电网体现出电力流、信息流和业务流高度融合的显著特点，其先进性和优势主要表现在以下几个方面。

（1）具有坚强的电网基础体系和技术支撑体系，能够抵御各类外部干扰和攻击，能够适应大规模清洁能源和可再生能源的接入，电网的坚强性得到巩固和提升。

（2）信息技术、传感器技术、自动控制技术与电网基础设施有机融合，可获取电网的全景信息，及时发现、预见可能发生的故障。故障发生时，电网可以快速隔离故障，实现自我恢复，从而避免大面积停电的发生。

（3）柔性交/直流输电、网厂协调、智能调度、电力储能、配电自动化等技术的广泛应用，使电网运行控制更加灵活、经济，并能适应大量分布式电源、微电网及电动汽车充放电设施的接入。

（4）通信、信息和现代管理技术的综合运用，将大大提高电力设备使用效率，降低电能损耗，使电网运行更加经济和高效。

（5）实现实时和非实时信息的高度集成、共享与利用，为运行管理展示全面、完整和精细的电网运营状态图，同时能够提供相应的辅助决策支持、控制实施方案和应对预案。

（6）建立双向互动的服务模式，用户可以实时了解供电能力、电能质量、电价状况和停电信息，合理安排电器使用；电力企业可以获取用户的详细用电信息，为其提供更多的

增值服务。

3.3.6 一种现代商业方法——电子商务

电子商务是指采用数字化电子方式进行商务数据交换和开展商务业务活动。电子商务主要包括利用电子数据交换（EDI）、电子邮件（E-mail）、电子资金转账（EFT）及 Internet 的主要技术在个人间、企业间和国家间进行无纸化的业务信息的交换。

在现代信息社会中，电子商务可以使掌握信息技术和商务规则的企业和个人，系统地利用各 种电子工具和网络，高效率、低成本地从事各种以电子方式实现的商业贸易活动。从应用和功能方面来看，可以把电子商务分为三个层次或 3S，即 Show、Sale、Serve。

Show（展示）就是提供电子商情，企业以网页方式在网上发布商品及其他信息，以及在网上做广告等，通过 Show，企业可以树立自己的企业形象，扩大企业的知名度，宣传自己的产品的服务，寻找新的贸易合作伙伴。

Sale（交易）即将传统形式的交易活动的全过程在网络上以电子方式来实现，如网上购物等。企业通过 Sale 可以完成交易的全过程，扩大交易的范围，提高工作的效率，降低交易的成本，从而获取经济和社会效益。

Serve（服务）指企业通过网络开展的与商务活动有关的各种售前和售后服务，通过这种网上的 Serve，企业可以完善自己的电子商务系统，巩固原有的客户，吸引新的客户，从而扩大企业的经营业务，获得更大的经济效益和社会效益。企业是开展电子商务的主角。

电子商务对社会经济产生的影响如下。

（1）电子商务将改变商务活动的方式。传统的商务活动最典型的情景就是“推销员满天飞”，“采购员遍地跑”，“说破了嘴、跑断了腿”，消费者在商场中筋疲力尽地寻找自己所需要的商品。现在，通过互联网只要动动手就可以了，人们可以进入网上商场浏览，采购各类产品，而且还能得到在线服务，商家们可以在网上与客户联系，利用网络进行货款结算服务，政府还可以方便地进行电子招标、政府采购等。

（2）电子商务将改变人们的消费方式。网上购物的最大特征是消费者的主导性，购物意愿掌握在消费者手中，同时消费者还能以一种轻松自由的自我服务的方式来完成交易，消费者主权可以在网络购物中充分体现出来。

（3）电子商务将改变企业的生产方式。由于电子商务是一种快捷、方便的购物手段，消费者的个性化、特殊化需要可以完全通过网络展示在生产商面前，为了取悦顾客，突出产品的设计风格，制造业中的许多企业纷纷发展和普及电子商务，如美国福特汽车公司在 1998 年 3 月将全世界的 12 万个计算机工作站与公司的内部网连接起来，并将全世界的 1.5 万个经销商纳入内部网，福特公司的最终目的是实现能够按照用户的不同要求，做到按需供应汽车。

（4）电子商务将给传统行业带来一场革命。电子商务是在商务活动的全过程中，通过人与电子通信方式的结合，极大地提高商务活动的效率，减少不必要的中间环节。传统的

制造业借此进入小批量、多品种的时代，“零库存”成为可能；传统的零售业和批发业开创了“无店铺”“网上营销”的新模式；各种线上服务为传统服务业提供了全新的服务方式。

（5）电子商务将带来一个全新的金融业。由于在线电子支付是电子商务的关键环节，也是电子商务得以顺利发展的基础条件，随着电子商务在电子交易环节上的突破，网上银行、银行卡支付网络、银行电子支付系统以及电子支票、电子现金等服务，将传统的金融业带入一个全新的领域。

（6）电子商务将转变政府的行为。政府承担着大量的社会、经济、文化的管理和服务的功能，在电子商务时代，当企业应用电子商务进行生产经营，银行金融电子化，以及消费者实现网上消费的同时，将同样对政府管理行为提出新的要求，电子政府或称网上政府，将随着电子商务发展而成为一个重要的社会角色。

总而言之，作为一种商务活动过程，电子商务将带来一场史无前例的革命，其对社会经济的影响远远超过商务的本身。除了上述这些影响外，它还将对就业、法律制度以及文化教育等带来巨大的影响，电子商务会将人类带入信息社会。