第3章 网络安全管理

目前，世界各国互联网管理大致可分为两类：政府主导模式和政府指导行业自律模式。政府主导模式强调政府在互联网管理中的作用，通过政府立法和网络过滤技术手段对网络进行管理。政府指导行业自律模式倚重互联网业界的自律和规范，在通过立法规范的同时，着重强调业界自身的网络分级制度和从业者的自身规范。无论采用哪种管理模式，政府都在网络管理中起着极其重要的作用，政府通过立法对网络安全进行规范和管理，这是各国管理网络的共识。

中国互联网是开放的，也是依法管理的。网信部门、工信部门、公安部门等依照职责分工进行网络管理。公安部门依照职责负责互联网安全监督，维护互联网公共秩序和公共安全，防范和惩治网络违法犯罪活动。

信息网络安全监督管理是指公安机关网络安全保卫部门运用行政手段，依法管理、检查和指导信息网络安全保护工作，依法查处信息网络领域违法行为，预防信息网络违法犯罪活动，维护网上公共秩序，保障信息网络安全的行政管理活动。信息网络安全监督管理主要就是互联网安全监督管理，是开展网上斗争、维护网络秩序、打击涉网违法犯罪活动的重要基础，是维护网上公共秩序的重要手段。

3.1 网络安全管理概述

3.1.1 新时期中国网络安全管理现状

党的十八大以来，我国信息网络基础设施建设实现了跨越式发展，网络走入千家万户，我国已成为全球网络大国。与此同时，互联网的社会影响力不断提升，网络内容乱象频发，网络安全威胁日益突出，给国家安全带来巨大危险。如何既促进我国互联网快速发展，又有效防止对国家政权安全和政治安全的冲击以及确保社会稳定，成为现实的难题。近年来党中央持续深化互联网管理领导体制改革，形成了党委集中统一领导下的综合治理格局，走出了一条有中国特色的互联网治理道路。现阶段，我国网络安全管理主要体现在以下4方面。

1. 网络安全上升到国家战略高度

2014年2月，习近平总书记在中央网络安全和信息化领导小组第一次会议上指出，“网络安全和信息化对一个国家很多领域都是牵一发而动全身的”“没有网络安全就没有国家安全，没有信息化就没有现代化”“建设网络强国的战略部署要与‘两个一百年’奋斗

目标同步推进”。2016 年 3 月，国民经济“十三五”规划提出了实施网络强国战略，不仅再次明确网络强国的战略定位，而且凸显该战略在整个国民经济发展中的地位。2017 年 10 月，党的十九大报告中提出，“坚持总体国家安全观。统筹发展和安全，增强忧患意识，做到居安思危，是我们党治国理政的一个重大原则。必须坚持国家利益至上，以人民安全为宗旨，以政治安全为根本，统筹外部安全和内部安全、国土安全和国民安全、传统安全和非传统安全、自身安全和共同安全，完善国家安全制度体系，加强国家安全能力建设，坚决维护国家主权、安全、发展利益。”信息安全已成为国家安全体系中重要的组成部分，是国家安全战略的重要内容。

2. 形成了多主体参与的网络综合治理体系

基于对互联网管理重要性的认识，从党的十八大开始，针对我国互联网管理体制存在的多头管理、职能交叉、权责不一、效率不高等弊端，对互联网管理体制进行全面改革。2014 年 2 月，中央网络安全和信息化领导小组成立，这是我国互联网管理的最高领导机构，负责统筹协调涉及经济、政治、文化、社会及军事等各个领域的网络安全和信息化重大问题，开启了以国家意志对网络空间进行统一规划和综合治理的新时代。目前已逐步形成了党委领导、政府管理、企业履责、社会监督、网民自律等多主体参与，经济、法律、技术等多种手段相结合的综合治网格局。

中央网络安全和信息化领导小组的具体办事机构简称“中央网信办”，中央网信办不仅是互联网内容的主管部门，同时负责统筹协调全国网络安全和信息化工作，工信、公安、新闻出版、文化、工商等政府部门分别负责特定领域与互联网相关的事务。

3. 建成了比较完整的网络安全保障体系

2016 年 11 月，《中华人民共和国网络安全法》颁布，于 2017 年 6 月 1 日实施。这是我国网络安全领域首部基础性、框架性、综合性法律。之后相关部门配套出台了一系列部门规章和规范性文件，其中部门规章主要包括《网络安全审查办法》（自 2020 年 6 月 1 日起实施）、《网络信息内容生态治理规定》（自 2020 年 3 月 1 日起施行）、《儿童个人信息网络保护规定》（自 2019 年 10 月 1 日起施行）、《区块链信息服务管理规定》（自 2019 年 2 月 15 日起施行）、《互联网域名管理办法》（自 2017 年 11 月 1 日起施行）、《互联网新闻信息服务管理规定》（自 2017 年 6 月 1 日起施行）、《互联网信息内容管理行政执法程序规定》（自 2017 年 6 月 1 日起施行）。规范性文件主要包括《微博客信息服务管理规定》《互联网新闻信息服务单位内容管理从业人员管理办法》《互联网新闻信息服务新技术新应用安全评估管理规定》《互联网用户公众账号信息服务管理规定》《互联网跟帖评论服务管理规定》《互联网论坛社区服务管理规定》《互联网新闻信息服务许可管理实施细则》。

目前，网络安全法律政策框架基本形成，网络安全管理各项工作已纳入法治化轨道。

4. 推进了全球互联网治理体系变革

网络安全，谁也不能独善其身。党的十八大以来，我国积极参与国际互联网治理，推进全球互联网治理体系改革。2014 年 11 月 19 日至 21 日在中国浙江乌镇召开了首届世界互联网大会，来自全球近 100 个国家和地区的 1000 多位政府官员、互联网领军人物和专家学者围绕国际互联网治理、互联网新媒体、跨境电子商务、网络安全、打击网络恐怖主

义等议题，举行了 10 多场分论坛和高端对话。习近平主席指出要“建立多边、民主、透明的国际互联网治理体系”。乌镇被授予大会永久会址，世界互联网大会每年在此召开一次。

2015 年第二届世界互联网大会，国家主席习近平出席开幕式并发表主旨演讲，提出“尊重网络主权、维护和平安全、促进开放合作、构建良好秩序”的四项原则以及五点主张：①加快全球网络基础设施建设，促进互联互通；②打造网上文化交流共享平台，促进交流互鉴；③推动网络经济创新发展，促进共同繁荣；④保障网络安全，促进有序发展；⑤构建互联网治理体系，促进公平正义。

2016 年第三届世界互联网大会的主题是“创新驱动 造福人类——携手共建网络空间命运共同体”。2017 年第四届世界互联网大会的主题是“发展数字经济 促进开放共享——携手共建网络空间命运共同体”。2018 年第五届世界互联网大会的主题是“创造互信共治的数字世界——携手共建网络空间命运共同体”。2019 年第六届世界互联网大会的主题是“智能互联 开放合作——携手共建网络空间命运共同体”。2020 年 11 月的世界互联网大会·互联网发展论坛的主题是“数字赋能 共创未来——携手构建网络空间命运共同体”。

由历届世界互联网大会的主题可以看出，构建网络空间命运共同体，就是要把网络空间建设成造福全人类的发展共同体、安全共同体、责任共同体、利益共同体，实现发展共同推进、安全共同维护、治理共同参与、成果共同分享。

构建网络空间命运共同体应加强政府、国际组织、互联网企业、技术社群、社会组织、公民个人等各主体的沟通与合作，形成立体协同的治理架构。国际社会要本着相互尊重和相互信任的原则，通过积极有效的国际合作，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，推动构建和平、安全、开放、合作的网络空间，建立多边、民主、透明的网络治理体系，携手共建网络空间命运共同体。

3.1.2　网络安全监督管理基本原则

互联网安全监督管理是公安机关的法定职责，在开展网络安全管理的工作中，需遵循以下基本原则。

1. 依法行政原则

对互联网的管理是国家赋予公安机关的事权，公安机关的相关业务工作必须坚持依法行政，按照国家相关法律法规，依法管理、依法监督、依法检查、依法侦查和办案。

中央网信办提出，推进网络空间法治化的要义是发挥法治对引领和规范网络行为的主导性作用，重点是按照科学立法要求加强互联网领域的立法，关键是严格执法，基础是按照全民守法要求，引导网民尊法守法，做“中国好网民”。

通过加强立法、严格执法、依法治网，以维护互联网“虚拟社会”的和谐发展为目标，以互联网的稳定和安全为主要任务，加强管理、夯实基础、扎实工作，采取监督管理和技术防控相结合，建立长效和现代的管理机制，增强公安机关对互联网的掌控能力，为开展网上斗争、维护网络治安秩序、打击网上各类违法犯罪行为提供保障。

2. 责任制原则

信息网络安全，实行“谁主管谁负责，谁建设谁负责，谁使用谁负责，谁管理谁负责，谁经营谁负责”的责任制，分工明确，责任到人。

国家各部门分工明确，工业和信息化部负责互联网的行业管理，网信办负责网上意识形态工作，各单位负责本单位信息系统的建设和安全运行。公安机关则通过建立互联网单位安全管理档案、监督互联网单位建立健全安全管理制度、落实安全保护措施等具体工作，实现对各互联网单位的监督、检查和指导。多部门分工协作，同时调动社会力量，共同参与对互联网的综合治理，共同维护互联网的安全。

3. 重视基础信息建设原则

公安机关网安部门需要开展经常性的基础调查，了解和掌握网络运营、服务、使用单位的基本情况，这是网安部门一项重要的法定职责，也是开展网上工作的重要支撑和基础。

4. 重点保护原则

在网络安全等级保护制度的基础上，对关键信息基础设施实行重点保护。

对要害部门和重点单位，要了解其网络安全现状和结构，建档管理，随时更新，为联动处置突发事件打牢基础。

3.1.3 网络安全监督管理对象

网络安全监督管理的主要工作对象是网络运营者和参与者，包括互联网接入服务单位、互联网数据中心、互联网内容服务单位、互联网联网单位、互联网上网服务营业场所，可统称为联网单位。

互联网接入服务单位（Internet service provider，ISP），是指负责提供互联网接入网络运行的单位，如中国电信、中国移动、中国联通、中国广电等。

互联网数据中心（Internet data center，IDC），是指向企业、商户或网站服务器群提供大规模、高质量、安全可靠的专业化服务器托管、虚拟空间租用、网络带宽出租等业务的平台和云平台。

互联网内容服务单位（Internet content provider，ICP），是指通过互联网开办网站，提供有偿或无偿信息服务的单位，分为非经营性 ICP 和经营性 ICP。非经营性 ICP 主要指政府网站、企事业单位网站、电子报刊等。经营性 ICP 是指通过互联网，向上网用户有偿提供信息或者网页制作、硬盘空间出租等服务活动的网站，经营的内容主要是网上广告、服务器硬盘空间出租、有偿提供特定信息内容、电子商务、网络直播及其他网上应用服务。国家对经营性 ICP 实行许可制度（许可证由各地通信管理部门核发），对非经营性 ICP 实行备案制度。

互联网联网单位，是指以固定光纤、线路拨号、无线等方式接入互联网，作为上网、办公、服务公众、数据传输、生产经营、科研教学、企业管理等网络应用的单位。

互联网上网服务营业场所，是指社区、学校、图书馆、宾馆、咖啡馆、娱乐休闲中心等向特定对象提供上网服务的单位，这些场所也纳入互联网联网单位管理，同时还需要其他一些特有的管理。

3.1.4　网络安全监督管理工作特点

1. 管理对象的广泛性

管理对象包括各种类型的联网单位；多种重要信息系统，不仅包括电力、民航等国家重要基础设施的各种应用系统，还包括金融、证券等重点单位和重要政府部门的内部应用网络系统。

2. 管理方式的复杂多样性

管理方式包括行政管理的一般管理方法，如指导、检查、督促和查处等；公安机关网安部门所特有的特殊管理方式；互联网新型服务以及新的管理对象所带来的新管理方式。

3. 管理措施的强制性

网络安全监督管理是国家赋予公安机关以治安强制措施作为后盾的一种行政管理工作。

4. 管理工作的社会性

社会性主要表现在两个方面：一是工作面向社会公开进行，关系到国家集体和群众方方面面具体的利益；二是工作的组织开展需要依靠社会力量，需要多方共同参与信息网络安全管理。

3.1.5　网络安全监督管理主要任务

(1) 指导、督促互联网单位的备案工作。

(2) 监督、检查互联网单位落实安全管理制度和安全保护技术措施。

(3) 监督、管理互联网上网服务营业场所，严格进行安全审核和日常检查。

(4) 监督、检查、指导重要信息系统的信息安全等级保护和关键信息基础设施重点保护工作。

(5) 处置网上有害信息。

(6) 查处信息网络违法违规行为。

(7) 组织开展计算机病毒等破坏性程序的日常防治管理。

(8) 组织开展重大活动的信息安全保卫工作。

(9) 开展信息网络安全专业技术人员继续教育工作。

3.1.6　网络安全监督管理主要方法

为主动适应新形势下网络安全监督管理工作的需要，全国各地公安网安部门转变管理模式，前置管理岗位，强化警民互动，大力推进网安警务室建设，将网络监管工作融入网站、运营单位的日常运作中，进一步延伸互联网防控触角，以虚拟社会管理基层化、实体化为手段，进一步密切警民关系，加大监管力度，提升网络阵地控制能力，准确把握住涉网问题的源头和关键，带动基础数据采集、安全措施落实、有害信息防治和打击涉网违法犯罪等工作能力水平的整体提高。

1. 落实网上公开执法措施

互联网的安全监督管理工作，就是要落实好“虚拟社区”和“虚拟人”的管控工作，以网管网。虚拟社会现实化，对互联网依法实施公开管理。

具体措施包括公安机关设立网上执法形象和执法标志，建立网上报警服务网站，在论坛、聊天室和拍卖网站等网上复杂场所和有害信息高发部位设立“报警岗亭”等。“虚拟警察”在网上公开亮相值勤，与网民实时互动，随时接受群众举报，提供求助和法律咨询服务，发现网上违法信息和违法行为，根据具体情况，依法公开警告、劝阻或制止，情节严重的要依法查处。2015 年 6 月，首批 50 个省市公安机关统一标识为“网警巡查执法”的微博、微信和百度贴吧账号集中上线。网警的定时巡查、报警图标的设定等作为新型的接警渠道，在很大程度上消除了网络管理过程中在时间和空间上的盲点，扩大了网警的监管时段和范围，更提高了网民的维权意识和自律意识。

2. 开展涉网单位基础调查

基础调查是公安机关网安部门一项经常性和基础性的工作，是了解和掌握信息网络运营、服务和使用单位基本情况的重要手段。

通过基础调查，在公安机关和被管理的互联网单位之间建立纵向的信息交流和传输渠道，实行案事件报告制度、情况数据定期上报和数据变更及时上报等制度，全面掌握本地 ISP、IDC、ICP 等联网单位的基本情况，为制定管理计划和措施提供支持。

3. 建立网络安全监督管理制度

依照国家有关法律法规，结合安全管理工作实际，制定和完善一整套针对性强，责、权明确的网络安全管理规章和制度，对重要信息系统单位、重点要害部位、上网服务场所、互联网联网单位、安全产品进行全面规范化管理。

4. 落实网络安全保护技术措施

按照《互联网安全保护技术措施规定》（公安部令第 82 号，2005 年 12 月发布）的要求，监督管理互联网服务提供者、联网使用单位落实互联网安全保护技术措施。采取的互联网安全保护技术措施应当具有符合公共安全行业技术标准的联网接口，并保障互联网安全保护技术措施功能的正常发挥。

5. 开展网络与信息安全信息通报

2004 年 8 月，“国家网络与信息安全信息通报中心”正式建立，挂靠公安部公共信息网络安全监察局。2015 年，在《关于加快推进网络与信息安全信息通报机制建设的通知》（公信安〔2015〕21 号）中提出，建立部省市三级、100 个重要行业部门、横纵通畅的立体化网络安全通报预警体系（3 层 100 纵）。网络与信息安全信息通报中心主要有以下职能：建立与协调小组信息通报渠道；组织分析、研判和评估；掌握网络安全信息；研判结果及时报告政府，必要时向社会发布预警信息等。信息通报工作原则：第一时间发现问题、第一时间通报处置、第一时间侦查调查和第一时间督促整改。

6. 建设社会支撑力量弥补警力不足

“专群结合、依靠群众”是确保信息网络安全监督管理工作顺利进行的重要保障，通过发动、组织社会力量参与信息网络安全防范和管理工作，可以有效弥补公安机关警力不足，将违法犯罪行为置于群众和社会的监督之下。

公安部设立了网络违法犯罪举报网站，网址：www.cyberpolice.cn/wfjb。

7. 加强行政执法力度，做好宣传教育

公安机关在查办案件过程中可执行“一案双查”制度：针对涉网违法犯罪案件调查中发现的互联网服务提供者不履行网络安全责任义务的行为，同步开展调查处置工作，既惩戒犯罪分子，又整治网络平台，查处为网络犯罪“输血供电”的利益链条，以及不履行网络安全管理义务的网络运营者，持续净化网络环境。

同时加强日常网络安全知识宣传，通过互联网站或者通过印制宣传书籍、画册的形式开展互联网日常安全的教育宣传活动，宣传国家法律法规，指导开展信息网络安全防范，传播正能量；专项行动期间还应配合工作需要进行专题的宣传教育。网安部门在日常管理执法工作中，有针对性地宣传法律法规，督促落实安全保护制度和技术措施，提高被管理单位和个人的安全意识。

2020 年 6 月，广西贵港网安部门在检查中发现，覃塘区网民何某珍和韦某南联网备案的个人网站因未采取防范计算机病毒和网络攻击、侵入的技术措施，导致黑客利用网站漏洞植入涉淫秽色情、赌博违法有害信息。发现情况后，贵港市公安局覃塘分局网安大队立即开展调查。经查，何某珍和韦某南二人的个人网站分别于 2017 和 2018 年联网 ICP 备案到期未注销，同时一直未到公安机关备案，也未对个人运营的网站采取相应网络安全防范技术措施，未落实网络安全监测职责，网络安全责任意识淡薄、联网备案制度和网络安全等级保护制度落实不到位，致使个人开设的网站被黑客植入涉黄、涉赌违法有害信息。根据调查结果，覃塘分局网安大队依据《中华人民共和国网络安全法》第二十一条、第五十九条之规定，分别对何某珍、韦某南予以警告处罚，并责令限期整改。

通过整合网上治安防控工作的各种力量，综合采用多种工作方法，有效维护网上治安秩序。

3.2　互联网安全监督管理工作

互联网安全监督管理通过备案管理、落实安全管理规章制度、落实安全技术保护措施等一系列具体工作来实现。

3.2.1　备案管理

备案是互联网安全管理的基础。备案制度的实施，可以增强联网单位的安全管理意识，建立健全安全管理制度，督促其依法履行社会责任。通过备案管理，可以有效防止和控制危害我国国家利益的有害信息流入和涉及我国国家机密的重要信息流出。

1. 设定依据

《计算机信息网络国际联网安全保护管理办法》(公安部令第33号,1997年12月16日发布)第十二条规定,“互联单位、接入单位、使用计算机信息网络国际联网的法人和其他组织(包括跨省、自治区、直辖市联网的单位和所属的分支机构),应当自网络正式联通之日起三十日内,到所在地的省、自治区、直辖市人民政府公安机关指定的受理机关办理备案手续。”

2. 备案对象

凡中华人民共和国境内的互联网运营单位(包括ISP、IDC)、互联网信息服务单位(ICP)、互联网联网单位、互联网上网服务营业场所和个人联网用户均为备案对象。

3. 备案材料

备案登记需要提供的材料如下。

(1)《计算机信息网络国际联网备案表》一式两份(加盖公章)。

(2)《网站基本情况表》(有网站的填写)。

(3)证件复印件:经营性互联网站需提交通信管理部门核发的《电信与信息服务业务经营许可证》、工商部门核发的《营业执照》副本复印件。个人网站需提交有效身份资料证照复印件。

(4)单位计算机信息网络安全组织成员名单(包括本单位网络安全主管领导、两名信息网络安全专业技术人员名单及联系方式)。

(5)单位计算机信息网络安全管理制度。

(6)互联网信息网络安全技术措施解决方案。

(7)单位网络结构拓扑图(标明内部IP使用情况)。

(8)提供虚拟主机服务、托管主机服务的信息服务单位,除提交以上材料外,还必须提交使用本单位虚拟主机服务的所有用户及托管主机的所有用户的基本情况,包括URL(域名)、负责人、联系方式。

(9)从事刊载新闻网站除提交以上材料外,还必须提交新闻管理部门的批准文件。

(10)系统维护权落于外地、服务器托管于本地的网站,除提交以上材料外,还必须提交其系统维护权所在地主管公安机关出具的备案证明。

单位的联网方式、IP地址变更、提供网络服务内容等发生变化时,应重新填写《计算机信息网络国际联网备案表》和《网站基本情况表》,到原办理备案手续的网安部门进行变更登记。

网安部门负责对备案材料进行审核,建立备案档案,进行备案统计,并按有关规定逐级上报。还要进行定期审核。

4. 备案管辖

各地级以上(含地级)人民政府公安机关网安部门对物理位置在本行政区划内与互联网相连接的计算机信息系统(服务器)或维护人员都具有备案管辖权。

网站系统维护管理权属位于本地、服务器位于外地的,首先要到本地网安部门备案,

然后还要到服务器托管地的主管部门备案登记。

5. 备案流程

互联网单位根据备案程序，将备案所需材料提交给对本单位具有管辖权的公安机关网安部门进行备案登记。在此过程中，网安部门需要完成受理备案材料、核实检查备案两方面工作。

1）公安机关网安部门受理备案材料工作流程

第一步，调查摸底：掌握本地互联网单位的数量；发现未掌握的本地互联网联网单位。

第二步，指导备案：通知联网单位进行备案，告知备案表领取地址或下载电子表格的网址，并指导备案单位准备好所需材料。

第三步，接收备案材料：①备案表一式两份（盖备案单位公章）；②安全组织成员名单；③信息网络安全专业技术人员继续教育证书复印件；④计算机信息网络安全保护管理制度；⑤计算机信息网络安全保护技术措施；⑥网络拓扑图；⑦按照法律法规要求提交相关管理部门颁发的证照的复印件。

第四步，备案初审：①初审不合格，如果备案表填写错误或备案材料不齐全，退还备案材料，告知备案单位备案不受理的原因；②初审合格，如果备案表填写正确，备案材料齐全，窗口正式受理备案材料，发予备案单位回执及备案表副本。

第五步，备案复审：窗口将受理的备案材料汇总后转交相关业务科室对备案材料进行复审，并对备案单位进行现场检查，核实材料内容。在规定时间（15 个工作日）内未能审核完毕的，应向备案单位说明原因。

2）公安机关网安部门核实检查备案工作流程

第一步，检查准备：①安排检查人员（两人以上），进行工作部署；②了解被检查单位名称、地址、电话、联系人及网络等情况；③准备检查证、检验笔录、联网单位备案资料、互联网联网单位安全检查表、责令限期整改通知书、询问笔录、印油等相关物品。

第二步，检查告知：①出示执法身份证件，表明身份；②联系单位负责人或安全管理责任人，说明检查目的；③要求被检查单位安排两名安全管理人员配合检查。

第三步，检查内容：①检查安全组织和安全保护工作制度；②测试安全保护技术措施；③检查机房的实体安全措施；④核查网络结构、拓扑图、IP 资源；⑤核实其他备案材料。检查过程中填写《互联网联网单位安全检查表》，要求被检查单位安全管理人员核实无误后署名。

第四步，检查结果：检查不合格，现场对安全管理责任人进行询问，制作笔录，当场采集证据，并出具责令限期整改通知书，要求被检单位限期整改；经现场检查合格的单位，在规定的 15 个工作日内发予备案证书；在规定时间内未能审核完毕的，应向备案单位说明原因。

第五步，整改验收：整改期限到期后，进行现场复查、验收。整改合格，继续进行备案，备案审核时限从整改完成之日起重新计算；整改不合格，责令继续整改。经过两次整改仍未能达到整改要求或坚决不整改的单位，给予行政处罚。将检查情况和整改情况录

入信息系统。

3）联网备案流程

互联网站通过“全国互联网安全管理服务平台”(www.beian.gov.cn)进行联网备案，如图 3-1 所示。

图 3-1　全国互联网安全管理服务平台

(1) 提交申请。用户注册、登录，开办主体管理，新办网站备案申请。已完成备案的网站，如备案信息需要变更，应及时登录备案网站进行变更。

(2) 初步审核。录入主体信息时所填写的信息必须真实、有效才能审核通过；网站如不涉及前置审批内容，不要在选项内容中打钩。

(3) 预约检查。非交互式网站初步审核完成后即完成备案；交互式网站需要进行面审或实地检查。

(4) 备案完成。在完成以上审核后，公安机关将核发公安备案编号。需要将备案编号放置在网站首页下端；可将网站备案代码增加在网站首页的代码中。

6. 备案罚则

对不按规定履行备案义务的单位或个人，不落实安全管理制度和措施的，按照《中华人民共和国计算机信息系统安全保护条例》第二十条和《计算机信息网络国际联网安全保护管理办法》第二十三条之规定，由公安机关责令限期改正，给予警告，有违法所得的，没收违法所得；在规定限期内未改正的，对单位主管负责人员和其他直接责任人员可以并处五千元以下的罚款，对单位可以并处一万五千元以下的罚款；情节严重的，可以给予六个月以内的停止联网、停机整顿的处罚，必要时可以建议原发证、审批机构吊销经营许可证或者取消联网资格。

3.2.2　落实安全管理规章制度

根据《公安机关互联网安全监督检查规定》的第十条，公安机关应当根据互联网服务

提供者和联网使用单位是否制定并落实网络安全管理制度和操作规程进行监督检查。网络安全管理制度主要包括以下内容。

1. 信息发布审核、登记制度

联网单位应建立信息发布、审核和登记制度，所有上网信息必须“先审后发”，遵循“谁主管，谁主办，谁负责”的原则。已发布信息的原始资料应及时分类存档，做到有案可查。

2. 信息监视、保存、清除和备份制度

联网单位的网络管理部门应当对本单位的网络使用情况进行监督、检查，杜绝访问境内外反动、黄色网站，不阅览、传播各类反动、黄色信息；应当保证单位计算机内日志文件及其他重要数据的完整性、真实性，并做好备份工作，配合各类安全检查；各部门信息文档要及时备份；发现本单位计算机存有各类反动及不健康信息，应当及时清除，情节较重的应及时上报。

3. 病毒检测和网络安全漏洞检测制度

联网单位的网络管理部门应对进入本网络的信息、所有对外发布的信息进行有效的病毒检测，以防止病毒的扩散，对于新发现的病毒要及时备份染毒文件，并追查病毒来源。查到病源和感染体，则进行隔离杀毒，必要时需要重装操作系统；应随时检查防火墙、在线病毒检测等网络安全技术措施的配置，以防止网络安全漏洞造成的后果扩散；应对网络进行有效的网络安全配置，及时报告已发现的网络安全漏洞；应采用合理的技术手段对网络运行安全进行有效的监控。

4. 违法案件报告和协助查处制度

联网单位应教育本单位终端使用者自觉遵守网络法规，严禁利用计算机从事违法犯罪行为；对于本单位发生的计算机违法犯罪行为及所遭受到的攻击，单位网络安全管理员应当及时制止，同时做好系统保护工作；各接入终端使用者有义务接受本单位网络管理部门和上级主管部门的监督、检查，并应积极配合做好违法犯罪事件的查处工作；网络管理部门应及时掌握网内各接入终端使用者的网络违法情况，定期向网络主管领导和上级主管部门报告，并应协助主管部门做好查处工作。

5. 账号使用登记和操作权限管理制度

联网单位的账号使用登记和操作权限管理制度适用于单位建设和管理的、基于角色控制和方法设计的各信息系统，以及以用户口令方式登录的网络设备、网站系统等；信息系统用户、角色、权限的划分明确，不同角色职责清晰；用户、权限和口令设置由专门部门全面负责，须采用实名制管理模式，杜绝一人多账号登记注册；用户管理、口令管理、账号审计、应急管理等措施完善。

6. 安全管理人员岗位工作职责

网络安全管理员主要负责本单位网络（包含局域网、广域网）的系统安全性，负责日常操作系统、网管系统、邮件系统的安全补丁、漏洞检测及修补、病毒防治等工作；协助机房管理人员进行机房管理，严格按照机房制度执行日常维护；加强对本单位的信息发布的审

核管理工作，杜绝违反《计算机信息网络国际互联网安全保护管理办法》的内容出现；接受并配合公安机关的安全监督、检查和指导，如实向公安机关提供有关安全保护的信息、资料及数据文件，协助公安机关查处通过国际联网的计算机信息网络的违法犯罪行为。另外，网络安全管理员应经常保持对最新技术的掌握，实时了解互联网的动向，做到预防为主。

7. 安全教育和培训制度

联网单位的安全教育和培训制度主要如下。

（1）定期组织本单位网络管理员学习《计算机信息网络国际互联网安全保护管理办法》《网络安全管理制度》及《信息审核管理制度》，提高工作人员维护网络安全的警惕性和自觉性。

（2）负责对本网络用户进行安全教育和培训，使用户自觉遵守和维护《计算机信息网络国际互联网安全保护管理办法》，使其具备基本的网络安全知识；杜绝发布违反《计算机信息网络国际互联网安全保护管理办法》的信息内容。

（3）不定期地邀请公安机关有关人员进行信息安全方面的培训，加强对有害信息、特别是影射性有害信息的识别能力，提高防范能力。

8. 其他与安全保护相关的管理制度

3.2.3 落实安全技术保护措施

根据《互联网安全保护技术措施规定》第十六条之规定，“公安机关应当依法对辖区内互联网服务提供者和联网使用单位安全保护技术措施的落实情况进行指导、监督和检查。公安机关在依法监督检查时，互联网服务提供者、联网使用单位应当派人参加。公安机关对监督检查发现的问题，应当提出改进意见，通知互联网服务提供者、联网使用单位及时整改。”不同类型联网单位需要落实的安全保护措施主要包括以下方面。

1. 互联网服务提供者和联网使用单位应当落实的基本互联网安全保护技术措施

这类措施主要包括：①防范计算机病毒、网络入侵和攻击破坏等危害网络安全事项或者行为的技术措施；②重要数据库和系统主要设备的冗灾备份措施；③记录并留存用户登录和退出时间、主叫号码、账号、互联网地址或域名、系统维护日志的技术措施；④法律、法规和规章规定应当落实的其他安全保护技术措施。

2. 提供互联网接入服务的单位应当落实的安全保护技术措施

在上述第 1 条措施的基础上，还需要增加下列安全保护技术措施：①记录并留存用户注册信息；②使用内部网络地址与互联网网络地址转换方式为用户提供接入服务的，要能记录并留存用户使用的互联网网络地址和内部网络地址对应关系；③记录、跟踪网络运行状态，监测、记录网络安全事件等安全审计功能。

3. 提供互联网信息服务的单位应当落实的安全保护技术措施

在上述第 1 条措施的基础上，还需要增加下列安全保护技术措施：①在公共信息服

务中发现、终止传输违法信息，并保留相关记录；②提供新闻、出版以及电子公告等服务的，要能记录并留存发布的信息内容及发布时间；③开办门户网站、新闻网站、电子商务网站的，要能防范网站、网页被篡改，被篡改后能够自动恢复；④开办电子公告服务的，要具有用户注册信息和发布信息审计功能；⑤开办电子邮件和网上短信息服务的，要能防范、清除以群发方式发送伪造、隐匿信息发送者真实标记的电子邮件或者短信息。

4. 提供互联网数据中心服务的单位和联网使用单位应当落实的安全保护技术措施

在上述第 1 条措施的基础上，还需要增加下列安全保护技术措施：①记录并留存用户注册信息；②在公共信息服务中发现、终止传输违法信息，并保留相关记录；③联网使用单位使用内部网络地址与互联网网络地址转换方式向用户提供接入服务的，要能记录并留存用户使用的互联网网络地址和内部网络地址对应关系。

5. 提供互联网上网服务的单位应当落实的安全保护技术措施

在上述第 1 条措施的基础上，还应当安装并运行互联网公共上网服务场所安全管理系统。

3.2.4　监督、管理互联网上网服务营业场所

互联网上网服务营业场所，是指通过计算机等设备装置向公众提供互联网上网服务的网吧、计算机休闲室等营业性场所。

公安机关每年应对申请设立的网吧进行安全审核，包括安全管理制度和安全保护措施的建立健全。在监督网吧建立相关制度后，采取定期或不定期的方式对网吧进行检查，指导、督促网吧经营者落实相关制度。同时在对网吧的安全审核中，认真审核网吧备案资料，对网吧情况有变动的，都要到现场进行实地查看，为搞好网上案件侦破工作奠定基础。

根据公安部《关于加强互联网上网服务营业场所安全管理工作的通知》的规定，公安机关安全审核的主要内容包括：①经营人员应具有合法的身份证明；②营业场地应符合消防安全有关规定；③营业场地面积、终端数量符合规定要求；④无“撤销批准文件”的记录；⑤有专职或兼职的安全管理人员；⑥有相应的防病毒、防有害信息传播等安全技术措施；⑦有经安全检测合格的“网吧”安全管理软件；⑧符合国家现行法律、法规的规定。

3.2.5　组织开展计算机病毒等破坏性程序的防治管理

根据《计算机病毒防治管理办法》，公安部网络安全保卫局主管全国的计算机病毒防治管理工作。

1. 计算机病毒防治的管理规定

计算机病毒防治的管理规定主要如下。

(1) 任何单位和个人不得制作计算机病毒。

(2) 任何单位和个人不得有下列传播计算机病毒的行为：①故意输入计算机病毒，

危害计算机信息系统安全；②向他人提供含有计算机病毒的文件、软件、媒体；③销售、出租、附赠含有计算机病毒的媒体；④其他传播计算机病毒的行为。

(3) 任何单位和个人不得向社会发布虚假的计算机病毒疫情。

(4) 从事计算机病毒防治产品生产的单位，应当及时向公安部网络安全保卫局批准的计算机病毒防治产品检测机构提交病毒样本。

(5) 计算机病毒防治产品检测机构应当对提交的病毒样本及时进行分析、确认，并将确认结果上报公安部公共信息网络安全监察部门。

(6) 对计算机病毒的认定工作，由公安部公共网络安全保卫局批准的机构承担。

(7) 计算机信息系统的使用单位在计算机病毒防治工作中应当履行下列职责：①建立本单位的计算机病毒防治管理制度；②采取计算机病毒安全技术防治措施；③对本单位计算机信息系统使用人员进行计算机病毒防治教育和培训；④及时检测、清除计算机信息系统中的计算机病毒，并备有检测、清除的记录；⑤使用具有计算机信息系统安全专用产品销售许可证的计算机病毒防治产品；⑥对因计算机病毒引起的计算机信息系统瘫痪、程序和数据严重破坏等重大事故，要及时向公安机关报告，并保护现场。

(8) 任何单位和个人在从计算机信息网络上下载程序、数据或者购置、维修、借入计算机设备时，应当进行计算机病毒检测。

(9) 任何单位和个人销售、附赠的计算机病毒防治产品，应当具有计算机信息系统安全专用产品销售许可证，并贴有“销售许可”标记。

(10) 从事计算机设备或者媒体生产、销售、出租、维修行业的单位和个人，应当对计算机设备或者媒体进行计算机病毒检测、清除工作，并备有检测、清除的记录。

(11) 任何单位和个人应当接受公安机关对计算机病毒防治工作的监督、检查和指导。

2. 计算机病毒防治的管理职责

公安机关对计算机病毒防治的管理职责如下。

(1) 监督、检查、指导信息系统运营或使用单位建立并落实计算机病毒等破坏性程序的防治管理制度和安全保护技术措施。

(2) 督促从事计算机设备或者媒体生产、销售、出租、维修行业的单位及个人做好计算机设备或者媒体的病毒检测、清除工作。

(3) 开展本地计算机病毒疫情调查，并举办各种计算机病毒等破坏性程序防范的宣传活动。

(4) 督促取得从事计算机病毒防治产品生产资格的单位进行审批、备案，加强对计算机病毒防治产品的监管。

(5) 督促计算机病毒防治产品研制、生产、销售单位，安全服务机构和用户对发现的计算机病毒提取样本，报送公安机关网络安全保卫部门。

(6) 建设网络安全监控系统。在骨干网、支网、用户网等不同层次上建设网络安全监控系统，实时检测网络病毒传播情况，及时发现病毒源，发布预警信息。

(7) 将接收的计算机病毒样本上报上级公安机关网安部门。

(8) 指导组织社会技术支撑力量对发现的计算机病毒及时进行处置,对用户级的计算机病毒控制与处置工作提供技术支持。包括提取计算机病毒样本,交付指定计算机病毒防治机构进行解剖、分析后,形成计算机病毒疫情分析报告和解决方案。

(9) 利用行政管理手段,严格控制病毒传播源,严厉处罚各类病毒传播行为和传播人。

3.2.6　开展信息网络安全专业技术人员继续教育工作

2006 年 5 月,公安部办公厅、人事部办公厅联合发布了《关于开展信息网络安全专业技术人员继续教育工作的通知》(公信安〔2006〕526 号),将信息网络安全专业技术人员继续教育工作作为一项长期工作,纳入公安机关信息网络安全监督管理工作之中。

1. 目标任务

通过继续教育,使信息网络安全专业技术人员及时更新法律法规、管理和技术知识,提高政治素质和职业道德水平,逐步建立一支与公安机关密切配合、维护信息网络安全的社会力量。

2. 继续教育内容和方式

(1) 继续教育内容。信息网络安全专业技术人员继续教育分为信息网络安全管理、信息网络安全技术和网吧等公共上网场所安全管理这 3 类,其培训内容以近三年来涉及信息安全的国家法律法规,国家信息安全保障工作政策措施,信息安全管理技术发展动态,防范网络攻击、计算机病毒和有害信息传播的管理技术措施为重点,每年结合新出台的信息安全法律法规以及信息安全管理和技术发展情况,对继续教育内容进行调整。

(2) 继续教育方式和培训时间。信息网络安全专业技术人员继续教育培训要结合各地实际情况,采取集中培训、自学、研修、网络等多种有效、简便的培训方式方法。有条件的地方要组织信息网络安全专业技术人员进行一定时间的集中培训,并要注重质量和效果。每年各种形式的继续教育时间累计不少于 12 天或 72 学时。

(3) 培训与考试。相关专业技术人员经过继续教育后参加由公安、人事部门组织开展的考试。考试合格者,由公安部公共信息网络安全监察局和人事部专业技术人员管理司统一颁发“信息网络安全专业技术人员继续教育证书”。

3.2.7　开展专项治理工作

根据不同时期的网络发展状况和工作重点,开展专项治理工作,监督检查网络运营者履行网络安全职责,提升网络安全管理能力和水平。

例如,2019 年中央网信办、工业和信息化部、公安部、国家市场监管总局联合开展的 App 违法违规收集使用个人信息专项治理工作取得了积极进展,包括制定印发了《App 违法违规收集使用个人信息行为认定方法》《App 违法违规收集使用个人信息自评估指南》等政策规范,成立了专项治理工作组,受理网民有效举报信息 12000 余条,针对 2300 余款 App 开展深度评估、问题核查,对用户规模大、问题突出的 260 款 App,有关部门采取了公开曝光、约谈、下架等处罚措施。通过专项治理工作,公众常用 App 存在的无隐私

政策、捆绑授权和强制索权、超范围收集使用个人信息等典型问题得到明显改善，这些运营者履行个人信息保护责任义务的能力和水平得到有效提升。

3.3 网络安全等级保护和关键信息基础设施重点保护

我国实行网络安全等级保护制度，对网络实施分等级保护、分等级监管。网络安全等级保护是指对存储、传输、处理国家重要信息、法人和其他组织及公民的专有信息或公开信息的网络分等级实行安全保护，对信息系统中使用的信息安全产品实行按等级管理，对信息系统中发生的信息安全事件分等级响应、处置。

网络安全等级保护是国家信息安全保障的基本制度、基本策略、基本方法，是保护信息化发展、维护国家信息安全的根本保障，这也是当今发达国家保护关键信息基础设施、保障信息安全的通行做法。

国家对关键信息基础设施，在网络安全等级保护制度的基础上，实行重点保护。

3.3.1 网络安全等级保护工作发展历程

1994 年，《中华人民共和国计算机信息系统安全保护条例》规定，“计算机信息系统实行安全等级保护”。1999 年，《计算机信息系统安全保护等级划分准则》(GB 17859—1999) 发布。

2003 年 9 月，《国家信息化领导小组关于加强信息安全保障工作的意见》(中办发〔2003〕27 号)明确指出：实行信息安全等级保护。要重点保护基础信息网络和关系国家安全、经济命脉、社会稳定等方面的重要信息系统，抓紧建立信息安全等级保护制度，制定信息安全等级保护的管理办法和技术指南。2004 年，公安部、国家保密局、国家密码管理局、国信办联合印发了《关于信息安全等级保护工作的实施意见》(公通字〔2004〕66 号)。

2007 年，公安部、国家保密局、国家密码管理局、国信办联合制定了《信息安全等级保护管理办法》(公通字〔2007〕43 号)、《关于开展全国重要信息系统安全等级保护定级工作的通知》(公通字〔2007〕861 号)以及《信息安全等级保护备案实施细则》(公通字〔2007〕1360 号)。《信息安全等级保护管理办法》的正式发布，标志着“等级保护 1.0”的正式启动。“等级保护 1.0”规定了等级保护需要完成的“规定动作”，即定级备案、建设整改、等级测评和监督检查。为了指导用户完成等级保护的“规定动作”，在 2008 年至 2012 年期间国家陆续发布了等级保护的一些主要标准，构成“等级保护 1.0”的标准体系。

2017 年 6 月 1 日，《中华人民共和国网络安全法》正式实施。这是我国自 1994 年发布实施《中华人民共和国计算机信息系统安全保护条例》将“等级保护”明确为我国计算机安全保护的根本制度以来，首次将其写入了法律，网络安全等级保护制度已经上升为法律规定的强制义务。《网络安全法》明确“国家实行网络安全等级保护制度”(第二十一条)、对“一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生、公共利益的关键信息基础设施，在网络安全等级保护制度的基础上，实行重点保护”(第三十一条)。

上述要求为网络安全等级保护赋予了新的含义。重新调整和修订“等级保护 1.0”标准体系，配合《网络安全法》的实施和落地，指导用户按照网络安全等级保护制度的新要求，履行网络安全保护义务的意义重大。这也标志着“等级保护 2.0”的正式启动。

公安部 2018 年 6 月发布《网络安全等级保护条例（征求意见稿）》（以下简称《保护条例》），明确规定，为加强网络安全等级保护工作，提高网络安全防范能力和水平，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，对在中华人民共和国境内建设、运营、维护、使用网络，开展网络安全等级保护工作以及监督管理，个人及家庭自建自用的网络除外。

2019 年 5 月 13 日，国家市场监督管理总局、国家标准化管理委员会联合召开新闻发布会，“等级保护 2.0”相关的《信息安全技术 网络安全等级保护基本要求》（GB/T 22239—2019）、《信息安全技术 网络安全等级保护测评要求》（GB/T 28448—2019）、《信息安全技术 网络安全等级保护安全设计技术要求》（GB/T 25070—2019）等国家标准正式发布，并于 2019 年 12 月 1 日开始实施。这 3 个标准是指导用户开展网络安全等级保护建设整改、等级测评等工作的核心标准，是顺利开展网络安全等级保护工作的前提。

“等级保护 2.0”或“等保 2.0”是一个约定俗成的说法，指按新的等级保护标准规范开展工作的统称。等保 2.0 标准注重全方位主动防御、动态防御、整体防控和精准防护，实现了对云计算、大数据、物联网、移动互联和工业控制信息系统等保护对象全覆盖，以及除个人及家庭自建网络之外的领域全覆盖。

3.3.2　网络安全等级保护工作

1. 基本原则

1）坚持分等级保护、突出重点

根据网络（包含网络设施、信息系统、数据资源等）在国家安全、经济建设、社会生活中的重要程度，以及其遭到破坏后的危害程度等因素，科学确定网络的安全保护等级，实施分等级保护、分等级监管，重点保障关键信息基础设施和第三级（含）以上网络的安全。

2）坚持积极防御、综合防护

按照法律法规和有关国家标准规范，充分利用人工智能、大数据分析等技术，积极落实网络安全管理和技术防范措施，强化网络安全监测、态势感知、通报预警和应急处置等重点工作，综合采取网络安全保护、保卫、保障措施，防范和遏制重大网络安全风险、事件发生，保护云计算、物联网、新型互联网、大数据、智能制造等新技术应用和新业态安全。

3）坚持依法保护、形成合力

依据《网络安全法》等法律法规规定，公安机关依法履行网络安全保卫和监督管理职责，网络安全行业主管部门（含监管部门）依法履行本行业网络安全主管、监管责任，强化和落实网络运营者主体防护责任，充分发挥和调动社会各方力量，协调配合、群策群力，形成网络安全保护工作合力。

2. 职责分工

对网络安全等级保护工作中各部门职责进行如下划分。

中央网络安全和信息化领导机构统一领导网络安全等级保护工作。国家网信部门负责网络安全等级保护工作的统筹协调。

国务院公安部门主管网络安全等级保护工作，负责网络安全等级保护工作的监督管理，依法组织开展网络安全保卫。

国家保密行政管理部门主管涉密网络分级保护工作，负责网络安全等级保护工作中有关保密工作的监督管理。

国家密码管理部门负责网络安全等级保护工作中有关密码管理工作的监督管理。

国务院其他有关部门依照有关法律法规的规定，在各自职责范围内开展网络安全等级保护相关工作。

县级以上地方人民政府依法开展网络安全等级保护工作。

网络运营者应当依法开展网络定级备案、安全建设整改、等级测评和自查等工作，采取管理和技术措施，保障网络基础设施安全、网络运行安全、数据安全和信息安全，有效应对网络安全事件，防范网络违法犯罪活动。

行业主管部门应当组织、指导本行业、本领域落实网络安全等级保护工作。

3. 定级对象

需要进行等级保护的单位类型如下。

(1) 党政机关和事业单位，例如各大部委、省级机关、各地市县(区)级的党委、政府机关以及各类行政事业单位等。

(2) 金融行业，例如金融监管机构、各大银行、证券、保险公司等。

(3) 电信行业，例如各大电信运营商、服务商等。

(4) 能源行业，例如电力公司、石油公司、烟草公司等。

(5) 教育行业，各大高等教育院校(普通高等教育、成人高等教育)，中等教育学校(包含全日制普通中学、中等职业学校、中等师范学校等)。

(6) 企业单位，例如大中型国有企业、央企、上市公司等。

(7) 广电行业。

(8) 卫生行业。

网络安全等级保护工作直接作用的对象，主要包括信息系统、通信网络设施和数据资源等，其中信息系统包括云计算平台/系统、物联网、工业控制系统、使用移动互联技术的系统等。当安全责任主体相同时，大数据、大数据平台/系统宜作为一个整体定级，当安全责任主体不同时，大数据应独立定级。

3.3.3 等级保护主要标准的框架和内容

等保 2.0 标准体系主要标准包括：《网络安全等级保护条例》(总要求/上位文件)、《计算机信息系统 安全保护等级划分准则》(GB 17859—1999)(上位标准)、《信息安全技术 网络安全等级保护实施指南》(GB/T 25058—2019)、《信息安全技术 网络安全等级保护定级指南》(GB/T 22240—2020)、《信息安全技术 网络安全等级保护基本要求》(GB/T 22239—2019)、《信息安全技术 网络安全等级保护安全设计技术要求》(GB/T 25070—2019)、《信息安全技术 网络安全等级保护测评要求》(GB/T 28448—2019)和《信息安全

技术 网络安全等级保护测评过程指南》(GB/T 28449—2018)。

等级保护对象的安全保护需要同时落实安全通用要求和安全扩展要求提出的措施。

1. 安全通用要求

《信息安全技术 网络安全等级保护基本要求》《信息安全技术 网络安全等级保护测评要求》和《信息安全技术 网络安全等级保护安全设计技术要求》这 3 个标准采取了统一的框架结构。例如,《信息安全技术 网络安全等级保护基本要求》采用的框架结构如图 3-2 所示。

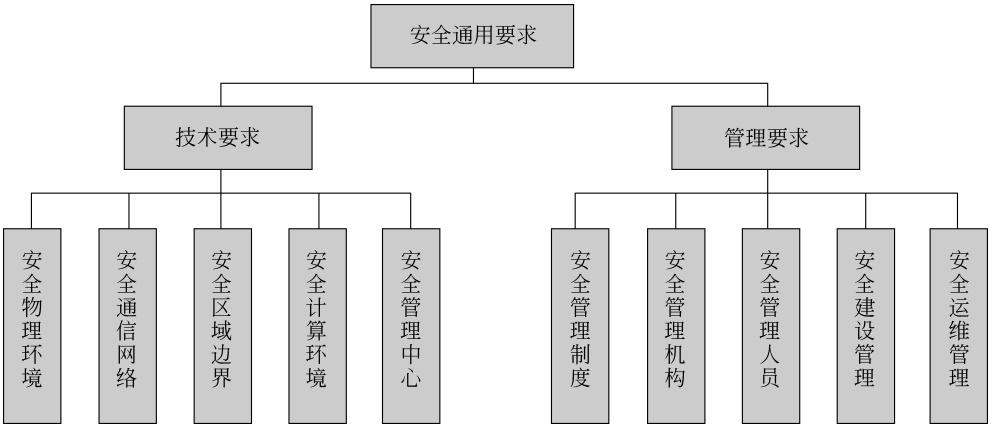

图 3-2　《信息安全技术 网络安全等级保护基本要求》框架

安全通用要求细分为技术要求和管理要求。安全通用要求针对共性化保护需求提出,无论等级保护对象以何种形式出现,都需要根据安全保护等级实现相应级别的安全通用要求。

1) 安全物理环境

针对物理机房提出的安全控制要求,主要对象为物理环境、物理设备和物理设施等。

2) 安全通信网络

针对通信网络提出的安全控制要求。主要对象为广域网、城域网和局域网等,涉及的安全控制点包括网络架构、通信传输和可信验证。

3) 安全区域边界

针对网络边界提出的安全控制要求。主要对象为系统边界和区域边界等,涉及的安全控制点包括边界防护、访问控制、入侵防范、恶意代码防范、安全审计和可信验证。

4) 安全计算环境

针对边界内部提出的安全控制要求。主要对象为边界内部的所有对象,包括网络设备、安全设备、服务器设备、终端设备、应用系统、数据对象和其他设备等;涉及的安全控制点包括身份鉴别、访问控制、安全审计、入侵防范、恶意代码防范、可信验证、数据完整性、数据保密性、数据备份与恢复、剩余信息保护和个人信息保护。

5) 安全管理中心

针对整个系统提出的安全管理方面的技术控制要求。通过技术手段实现集中管理,涉及的安全控制点包括系统管理、审计管理、安全管理和集中管控。

6）安全管理制度

针对整个管理制度体系提出的安全控制要求。涉及的安全控制点包括安全策略、管理制度制定和发布以及评审和修订。

7）安全管理机构

针对整个管理组织架构提出的安全控制要求。涉及的安全控制点包括岗位设置、人员配备、授权和审批、沟通和合作以及审核和检查。

8）安全管理人员

针对人员管理提出的安全控制要求。涉及的安全控制点包括人员录用、人员离岗、安全意识教育和培训以及外部人员访问管理。

9）安全建设管理

针对安全建设过程提出的安全控制要求。涉及的安全控制点包括定级和备案、安全方案设计、安全产品采购和使用、自行软件开发、外包软件开发、工程实施、测试验收、系统交付、等级测评和服务供应商管理。

10）安全运维管理

针对安全运维过程提出的安全控制要求。涉及的安全控制点包括环境管理、资产管理、介质管理、设备维护管理、漏洞和风险管理、网络和系统安全管理、恶意代码防范管理、配置管理、密码管理、变更管理、备份与恢复管理、安全事件处置、应急预案管理和外包运维管理。

2. 安全扩展要求

安全扩展要求针对个性化保护需求提出，等级保护对象需要根据安全保护等级、使用的特定技术或特定的应用场景实现安全扩展要求。《信息安全技术 网络安全等级保护基本要求》提出的安全扩展要求包括云计算安全扩展要求、移动互联安全扩展要求、物联网安全扩展要求和工业控制系统安全扩展要求。

（1）云计算安全扩展要求是针对云计算平台提出的安全通用要求之外额外需要实现的安全要求。主要内容包括“基础设施的位置”“虚拟化安全保护”“镜像和快照保护”“云计算环境管理”“云服务商选择”等。

（2）移动互联安全扩展要求是针对移动终端、移动应用和无线网络提出的安全要求，与安全通用要求一起构成针对采用移动互联技术的等级保护对象的完整安全要求。主要内容包括“无线接入点的物理位置”“移动终端管控”“移动应用管控”“移动应用软件采购”“移动应用软件开发”等。

（3）物联网安全扩展要求是针对感知层提出的特殊安全要求，与安全通用要求一起构成针对物联网的完整安全要求。主要内容包括“感知节点的物理防护”“感知节点设备安全”“网关节点设备安全”“感知节点的管理”“数据融合处理”等。

（4）工业控制系统安全扩展要求主要是针对现场控制层和现场设备层提出的特殊安全要求，它们与安全通用要求一起构成针对工业控制系统的完整安全要求。主要内容包括“室外控制设备防护”“工业控制系统网络架构安全”“拨号使用控制”“无线使用控制”“控制设备安全”等。