CHAPTER 3

信息安全管理概述 第3章

3.1 信息安全管理的总体要求和基本原则

3.1.1 总体要求

按照《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号文)的精神,信息安全保障工作的总体要求概括为坚持积极防御、综合防范的方针,全面提高信息安全防护能力,重点保障基础信息网络和重要信息系统安全,创建安全健康的网络环境,保障和促进信息化发展,保护公众利益,维护国家安全。

积极防御就是要坚持用发展的思路辩证地认识和解决信息安全问题,在对信息安全风险进行充分分析和评估的基础上构造安全防护与安全监管结合的保护体系,加强预警、应急处理和灾难备份。

综合防范就是在预防、监控、应急处理、对抗和打击犯罪等环节从法律、管理、技术、人员等方面采用多层次、立体、全面的防护措施,充分发挥国家、社会、组织和个人的作用,全社会共同构筑国家信息安全保障体系。

3.1.2 基本原则

《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号文)指出,信息安全保障工作的基本原则是"立足国情,以我为主,坚持管理与技术并重;正确处理安全与发展的关系,以安全保发展,在发展中求安全;统筹规划,突出重点,强化基础性工作;明确国家、企业、个人的责任和义务,充分发挥各个方面在信息安全保障工作中的积极性"。

"增强国家综合实力,促进经济社会的发展"是信息化的根本目的,信息安全保障为信息化的发展保驾护航。将信息安全问题绝对化,或脱离发展过程的现实而盲目追求信息安全是有害的;同样,只强调信息化应用,忽视信息安全问题则是另一个极端的错误倾向,必须坚持以安全保发展,在发展中求安全的辩证思维。同样,信息安全中的技术与管理也是辩证统一

的。在强调信息安全保障工作中的高技术防护和对抗特点时必须十分重视管理的作用。科学的管理不仅贯穿信息安全保障的全过程，而且是将信息安全技术转化为保证能力的必要条件。

我国信息安全保障中的主要设备和核心技术受制于人的现实，要求我们必须充分发挥政治和制度优势，强化信息安全意识和责任心，坚持以我为主，管理与技术并重的方针。这样做，不仅能有效地在信息安全保障体系中发挥技术与管理的互补性优势，同时也是降低信息安全保障成本的可行办法。必须坚持从本地、本单位的实际出发，根据信息化发展的不同阶段和不同的安全保护目标统筹规划，保障重点，客观分析信息安全与信息化应用的阶段适应性，综合平衡安全风险和安全成本，这是信息安全保障中始终要遵循的原则。

3.2 信息安全管理的范围

3.2.1 信息基础设施

1. 全球信息基础设施

信息基础设施(Information Infrastructure)是(有线和无线)通信网络、计算(机)设备、网络互连设备、外围设备、数据存储设备、动力保障和环境设备的集合，它可以建立在国家或地区之间的广大地域、空域和海域上。

从理论上讲，全球信息基础设施不被单个机构所控制或归其所有，它的“所有权”分布于IT公司、学术单位、政府实体以及个人。因特网(Internet)就是现今使用最为广泛和主流的全球信息基础设施实例，也是全球通信网络平台，大多数对内对外通信的网络都是在这个全球信息基础设施上建立起来的虚拟网、专用网、广域网以及定制的各种网络。

但实际上，由于这样的全球性信息基础设施中的顶级(根)服务器、路由器和域名系统(DNS)的硬件设备都控制在美国及其盟友国，大多基础通信和操作规程(协议或标准、操作系统等)的制定权和修订权以及IP地址、DNS等信息资源的分配权都掌握在由美国政府控制的大型IT企业或组织手中，这就决定了它们对全球信息基础设施资源的垄断或控制地位。

2. 国家信息基础设施

国家信息基础设施(National Information Infrastructure)是一个国家用来处理其(政府的或商业的)业务的信息基础设施，同样是(有线和无线)通信网络、计算(机)设备、网络互连设备、外围设备、数据存储设备、动力保障和环境设备的集合，也可以建立在国家或地区之间的广大地域、空域和海域上。不过，从技术层面讲，国家信息基础设施只是全球信息基础设施的一个子集。

3. 区域信息基础设施

区域信息基础设施(Local Information Infrastructure)是指一个地区、行业或组织为处理其业务所建设和使用的信息基础设施。它是国家信息基础设施的一个子集。

4. 网络边界

网络边界指位于某个国家、区域和组织的物理网络设施与外部物理网络设施之间的一个区域，这个区域往往由一台或一组网络设备(交换机、路由器等)组成，这些网络设备处理不同级别的通信交换或路由信息。与因特网相连的局域网或私有网，其物理边界就在互连

网络设备处，而逻辑边界则与不同级别的信息相关。

3.2.2　信息安全基础设施

信息安全基础设施是指可为密码服务、鉴别服务和访问控制服务等提供基础性和共享性支撑的设备和系统的通称，具体指 PKI(Public Key Infrastructure，公钥基础设施)/CA(Certification Authority，证书机构)、PKI/KMI(Key Management Infrastructure，密钥管理基础设施)和 PKI/PMI(Privilege Management Infrastructure，权限管理基础设施)等各类与公开密钥和身份标识(ID)信息有关的设备和系统，通过使用数字证书，构建网络信任体系，提供支撑性的安全基础服务。这些信息安全基础设施分别(在国家统一规划和技术标准指导下按行业、系统和业务类别)以树形结构从顶(根)至下分层进行部署，将全国大一统网络按层次分类划分为众多的虚拟网络，并按信息级别和使用权限对各类信息资源进行安全有序的访问与操作使用。

CA(Certification Authority，证书机构)负责制作、分发、撤销、作废证书等管理活动。其基本元素是数字证书，数字证书上有持有者的身份标识、权限属性、密钥信息等基本数据，是网络信任体系用户的“身份证”。

KMI(Key Management Infrastructure，密钥管理基础设施)为鉴别服务和加密服务提供密钥管理，并且提供密钥恢复服务以及存取用户证书的目录。KMI 不直接提供用户所需的安全参数，而是提供被其他安全设备和技术所使用的模块和接口参数。KMI 的主要运行过程包括登记授权使用 KMI 的个体；接受个体的密钥申请；生成对称或非对称密钥；密钥的安全分发；密钥的跟踪审计；密钥泄露和丢失处理，例如删除已泄露的密钥。

由此可知，KMI 可提供 4 个方面的业务：

① 对称密钥的产生和分发；

② 支持非对称密钥以及相应的证书管理；

③ 提供目录服务；

④ 对 KMI 自身的管理。

随着电子政务系统和电子商务系统建设的不断推进，对密钥管理的需求必将不断增长和强化，KMI 技术将被不断完善并广泛应用。

PMI(Privilege Management Infrastructure，权限管理基础设施)是信息安全基础设施中的另一个重要的组成部分。PMI 的主要目的是向用户和应用程序提供权限管理服务，负责向应用系统提供与应用相关的权限管理，提供用户身份到应用权限的映射功能，提供与实际应用处理模式对应的与具体应用系统开发和管理无关的授权和访问控制机制，可以简化具体应用系统中有关安全机制的开发和维护。

PMI 作为信息安全基础设施之一，为用户指定权限属性信息，例如特权、能力和角色等，并采用 X.509 协议所规定的数据格式使用证书。PMI 通过在应用服务中使用用户权限管理支持访问控制服务。

3.2.3　基础通信网络

我国基础通信网络担负着为国家信息化提供互连互通的网络平台服务，以及为与国际联网提供高速信道服务的重任。目前比较有影响的基础通信网络如下：

- 中国科学技术网(CSTNET)；
- 中国教育和科研计算机网(CERNET)；
- 中国电信公用计算机互联(骨干)网(CHINANET)；
- 中国联通互联网(UNINET)；
- 中国移动互联网(CMNET)，等等。

国家对基础通信网络的安全管理要求是在网络交换的链路层和物理层为网络的安全有序和健康运行提供公共平台服务。为此，对基础通信网络的基本安全要求是“具有防止和对抗网络病毒传播与大规模拒绝服务攻击的能力”。

3.2.4 广播电视传输网

各级政府或政府授权的机构利用有线、无线和卫星系统构成的广播电视传输网络担负着以语音、图像和数据为外在形式的公共传媒的重任，为社会提供公共信息和社会控制信息服务。

国家对广播电视传输网的安全管理要求是“对传输信道和媒体的控制，以及防止和对抗系统外的势力对传输信道和媒体的侵占、插入、篡改和干扰，确保传输网络正常运行”。

3.2.5 信息系统

1. 国家重要信息系统

国家重要信息系统是指“关系国家安全、国计民生、经济命脉、社会稳定等方面的数据相对集中的、规模较大的信息系统，其中包括受国家委托或需要受控管理的军事工业企业和研究单位的信息系统”。这些系统通常由政府或其委托的机构负责建立、运行和维护。

2. 电子政务系统

电子政务系统是指“各级政务机关为实现办公自动化、网络化、信息化而建立、运行和维护的公文流转和业务信息系统”。这些系统辅助政府实现：

① 增强为公众、其他部门和其他政府实体提供信息和服务的能力；

② 改进政府管理工作和提升政府形象，包括增强影响力，提高效率和服务质量，以及加速政府机构和管理模式的改革进程。我国的电子政务系统分为各级政府机关的政务信息系统和各级党委机关的党务信息系统，前者原则上运行于电子政务外网上，后者完全运行于电子政务内网上。

3. 电子商务系统

电子商务系统指利用互连网络平台开展商务活动的金融、物资流通和各类交易的信息系统。

4. 企事业信息系统

企事业信息系统指各类企业和事业单位利用互连网络平台或技术所建立起来的集内部办公业务和生产、管理事务以及与社会交互为一体的综合业务信息系统。

5. 其他信息系统

其他信息系统指利用互连网络平台为社会和个人提供除上述信息系统服务功能以外的信息化服务系统，例如网吧、咨询服务和各种社交网络、即时通信、公共电子邮件系统等。

3.3　安全管理在信息安全保障中的地位和作用

安全管理和安全技术是构造信息安全保障体系的两大组成部分，两者具有同等重要的地位和作用。安全技术需要安全管理来规划、设计、实施、调整和维护，安全技术的效能需要安全管理予以激活和提升；安全管理可借助安全技术实现系统化、智能化和决策科学化。安全管理和安全技术互为支持和补充。在一定的条件下，两者可以互相转化。安全管理和安全技术的最佳融合可以提高安全保障体系的功效或绩效比，降低安全成本。

3.4　习题与思考题

1. 积极防御的核心思想是什么？

2. 深刻理解安全管理与安全技术的关系。

3. 电子政务系统是怎样分类的？为什么电子政务系统要运行在两个不同的网络上？

4. 就你知道或熟悉的网络信息系统，举两个例子，将其归类到 3.2.5 节中所述的信息系统中，并说明为什么。

5. 人们常说国际互联网(Internet)是一把“双刃剑”，根据你的理解举例说明之。