第 34 章　信息安全知识

34.1　信息系统安全和安全体系

近年来，我国信息化进程不断推进，信息系统在政府和大型行业、企业组织中得到了日益广泛的应用。随着各部门对其信息系统不断增长的依赖性，信息系统的脆弱性日益暴露。由于信息系统遭受攻击使得其运转及运营受负面影响的事件不断出现，信息系统安全管理已经成为政府、行业、企业管理越来越关键的部分。由于如何规范日趋复杂的信息系统的安全保障体系建设，以及如何进行复杂信息系统的安全评估是信息化进程中所面临的巨大挑战。因此，信息系统安全建设是政府、行业和企业必须携手面对的问题。

由于信息系统本身的脆弱性和复杂性，大量的信息安全问题也伴随着计算机应用的拓展而不断涌现，病毒传播、黑客入侵、网络犯罪等安全事件的发生频率逐年升高，危害性也越来越大。如何构建企业信息安全体系，保护企业的利益和信息资产不受侵害，为用户提供可信的服务，已成为各企业当前迫切需要解决的问题。

34.1.1　信息安全需求分析

首先，要对企业信息网络可能面临的安全威胁和安全问题进行系统的分析，形成完整的安全需求，才能构造符合企业实际的、可操作性强的信息安全体系。

1．可能面临的安全威胁

（1）物理安全风险。物理安全风险包括：计算机系统的设备、设施、媒体和信息面临因自然灾害（如火灾、洪灾、地震）、环境事故（如断电、鼠患）、人为物理操作失误，以及不法分子通过物理手段进行违法犯罪等风险。

（2）数据安全风险。数据安全风险包括：竞争性业务的经营和管理数据泄露，客户数据（尤其是大客户资料）泄露、数据被人为恶意篡改或破坏等。

（3）网络安全风险。网络安全风险包括：病毒造成网络瘫痪与拥塞、内部或外部人为恶意破坏造成网络设备瘫痪、来自因特网黑客的入侵威胁等。

（4）业务中断风险。以上这些风险都可能造成企业业务中断，甚至造成企业重大损失和恶劣社会影响，破坏企业品牌和信誉。

2．可能存在的安全问题

（1）信息网络系统建设规划上的不完善。信息网络建设初期，是以保证企业应用的功能和性能为主的，没有将信息安全作为系统的主要功能之一。虽然利用当时的技术手段采取了一些安全措施，但安全保护措施较为零散，缺乏整体性与系统性，对于信息网络的安全保护缺乏统一的、明确的指导思想，这是引发安全问题的主要源头。

（2）技术与设计上的不完善。自计算机诞生和因特网问世以来，技术上的漏洞和设计方面的缺陷就随之而来，这些缺陷存在于计算机操作系统、数据库系统、网络软件和应用软件的各个层次，有可能被恶意用户利用，来获取非法访问权限。这也是引发安全问题的主要原因。

（3）网络互联方面的风险。随着企业业务的扩展，企业信息网同外部信息网的连接关系越来越复杂。在企业的信息网络与外界网络的连接之间，特别是和因特网之间，如果缺乏必要、有效的技术防范措施，那么恶意用户很容易利用漏洞侵入内部网络。

（4）安全管理方面的问题。这方面问题主要表现在：没有建立专门的安全管理组织，信息安全管理制度不健全或贯彻落实不够，人员不到位，安全防范意识不强，或者企业为节约成本，人力投入和实际需要存在矛盾。这些问题使得安全技术和管理措施难以有效实施。

34.1.2　信息安全的体系架构

1．信息安全的总体架构

通过上述分析，根据企业信息安全需求，我们可以提出此方面的总体架构，详见图 34-1，目的是确保信息的机密性、完整性、可用性、可审计性和抗抵赖性，以及企业对信息资源的控制，确保企业经营和业务的不间断运行。

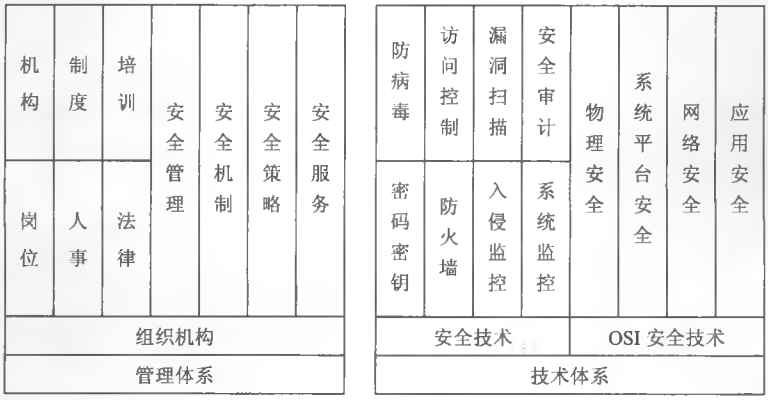

图 34-1　企业信息安全的总体架构图

2．如何构建信息安全的技术体系

（1）物理安全。

保证信息系统物理安全，首先要根据国家标准、企业的信息安全等级和资金状况，

制订适合本企业的物理安全要求，并通过建设和管理达到相关标准。

其次，关键的信息系统资源，包括主机、应用服务器、网络设备、加密机等设备，通信电路，以及物理介质（软/硬磁盘、光盘、磁带、IC卡、PC卡等），应有加密、电磁屏蔽等保护措施，并放在物理上安全的地方。

（2）系统平台安全。

系统平台安全主要是保护主机上的操作系统与数据库系统的安全，它们是两类非常成熟的产品，安全功能较为完善。对于保证系统平台安全，总体思路是先通过安全加固解决企业管理方面的安全漏洞，然后采用安全技术设备来增强其安全防护能力。实施系统平台安全应注意以下几个方面：

- 加强主机操作系统、数据库系统的账户与口令管理，其中：对系统建设过程中可能遗留的无用账户、默认账户和默认口令应注意清查并及时删除；如无法确认，必须修改默认口令；账户口令要符合设置要求，对重要设备的系统级（ROOT）账户口令每个月至少要变更一次，重要操作后要及时变更口令。
- 要建立操作系统、数据库和应用系统的相关应用和端口的对应关系，关闭主机系统上与应用服务无关的端口。
- 企业应用系统对不间断运行的要求较高，如果采用打补丁的方式进行加固，风险大，工作量大，即便是表面看起来很普通的补丁也可能造成整个系统瘫痪。因此，打补丁的最佳时机是在应用系统上线投产前的安装调试阶段；应用上线后，尽量不要采用打补丁加固的方法，如果确实要打补丁，事先要经过严格的测试并做好数据备份和回退措施。
- 如果系统平台中存在较大安全漏洞而无法打补丁加固时，可利用安全保护措施的互补性，在网络边界处采取合适安全保护措施，并加强对主机系统的审计与管理，以弥补该问题遗留的安全隐患。
- 对于企业外公司开发的应用系统，如需要开发公司工程师远程登入查找故障，应贯彻最小授权原则，开放的账户只能给予满足要求的最少权限，并对远程登入时间、操作完成时间、操作事项进行记录，及时关闭开放的用户；有条件的，可打开系统平台自带的审计工具，或配备第三方的监控、审计和身份认证工具。

（3）网络安全。

计算机网络是应用数据的传输通道，并控制流入、流出内部网的信息流。网络安全最主要的任务是规范其连接方式，加强访问控制，部署安全保护产品，建立相应的管理制度并贯彻实施。建设网络安全体系应注意以下几个方面：

- 计算机网络边界的保护强度与其内部网中的数据、应用的重要程度紧密相关，网络安全等级应根据结点的网络规模、数据重要性和应用重要性进行划分并动态调整。
- 可以根据不同数据和应用的安全等级，以及相互之间的访问关系，将内部网络划分为不同的区域，建立以防火墙为核心的边界防护体系。

- 项目规划阶段就要考虑防火墙、漏洞扫描、入侵检测和防病毒等各安全产品之间的互相协作关系，以实现动态防护。

（4）应用安全。

应用安全是指保护应用系统的安全、稳定运行，保障企业和企业用户的合法权益。保证应用系统安全，应加强以下几个方面的建设：

- 建立统一的密码基础设施，保证在此统一的基础上实现各项安全技术。
- 实施合适的安全技术，如身份鉴别、访问控制、审计、数据保密性与完整性保护、备份与恢复等。

为实现以上安全目标，可采用如下安全策略：

- 根据企业应用系统的特点，抽象出应用系统的基本模式，然后建立相应的安全模型，并统一设计同类应用系统的安全功能的实现方法。
- 根据应用系统模式及其传输的业务数据的重要性，为应用系统划分安全等级，针对不同安全等级的应用系统实施不同强度的安全保护功能。

3. 如何构建企业信息安全的管理体系

信息安全不仅是技术问题，更主要的是管理问题。俗话说“三分技术，七分管理”，任何技术措施只能起到增强信息安全防范能力的作用。只有管理到位，才能保障技术措施充分发挥作用。能否对信息网络实施有效的管理和控制是保障信息安全的关键。构建企业信息安全管理体系时，应建立从规划、建设、运行维护到报废的全过程安全管理，建立评估—响应—防护—评估的动态闭环的管理流程。

（1）加强全过程安全管理。

信息系统整个生命周期分为规划、建设、运行维护、报废四个阶段，不同的阶段有不同的安全管理重点和要求。

① 在信息网的规划阶段就要加强对信息安全建设和管理的规划。信息安全建设需要投入一定的人力、物力和财力，由于无论管理工作还是技术建设工作都不可能一步到位，因此要根据企业状况实事求是地确定信息网的安全总体目标和阶段目标，分阶段实施，降低投资风险。

② 在工程建设阶段，建设管理单位要将安全需求的汇总和安全性能、功能的测试列入工程建设各个阶段工作的重要内容，要加强对开发（实施）人员、开发过程中的资料（尤其是涉及各种加密算法的资料）、版本控制的管理，要加强对开发环境、用户和路由设置、关键代码的检查。

③ 在运行维护阶段，要注意以下事项：

- 建立有效的安全管理组织架构，明确职责，理顺流程，实施高效的管理。领导重视是做好信息安全工作的关键，人员落实是做好信息安全工作的保障。
- 制订完善的安全管理制度，加强信息网的操作系统、数据库、网络设备、应用系统运行维护过程的安全管理。
- 要建立应急预案体系，保证业务不间断运行，如主机应急预案、业务应急预案、

网络应急预案、灾备系统等。

- 信息中心要加强对物理场所的安全管理，包括机房人员出入管理、营业场所出入管理、机房物理安全管理、消防安全管理等。
- 加强安全技术和管理培训。针对已发生的犯罪大多是内部人员或内外勾结犯罪的情况，要加强对内部人员的管理（包括技术人员和营业人员）和教育，让相关人员知法懂法。
- 加强执行力度和违规行为的处罚力度。根据以往教训，往往是有章不循而且连续几个环节都没有遵守规章制度，才让犯罪分子有机可乘。

④ 在设备报废阶段，对于过期的保密信息（包括电子文档记录的信息），要及时、集中销毁；对于报废设备，处理时要销毁遗留在设备上涉及安全的信息。

（2）建立动态的闭环管理流程。

企业信息网处于不断的建设和调整中，新的安全漏洞总是不断地被发现，当单纯的静态管理流程不能满足要求时，需要建立动态、闭环的管理流程。动态、闭环的管理流程就是要在企业整体安全策略的控制和指导下，通过安全评估和检测工具（如漏洞扫描、入侵检测等）及时了解信息网存在的安全问题和安全隐患，据此制订安全建设规划和安全加固方案，综合应用各种安全防护产品（如防火墙、防病毒、身份认证、审计等手段），将系统调整到相对安全的状态。

- 对于一个企业而言，由于安全策略是信息安全体系的核心，因此制订明确、有效的安全策略是非常重要的。企业安全组织要根据这个策略制订详细的流程、规章制度、标准和安全建设规划、方案，保证这一系列策略规范在整个企业范围内贯彻实施，从而保护企业的投资和信息资源安全。
- 要制订完善的、符合企业实际的信息安全策略，就必须先对企业信息网的安全状况进行评估。安全评估是指对信息资产的安全技术和管理现状进行评估，让企业对自身面临的安全威胁和问题有全面的了解，从而制订有针对性的安全策略来指导信息安全的建设和管理工作。

34.2　信息系统安全风险评估

在信息技术广泛应用的今天，我们面临着越来越多的信息安全威胁和挑战。传统的信息系统工程并没有把信息安全问题单独提出来考虑，而是在设计中遇到明显的安全问题时设计一个安全应用来解决。然而由于没有系统的归纳和总结，人们经常会有很多疑问：我们的安全控制全面吗？我们的安全控制是否达到了预期效果？安全控制是否有冗余？网络安全是我们信息系统的责任吗？社会工程攻击如何防范？物理隔离应什么时候进行设计？

近两年来，信息安全风险评估问题成为信息安全领域研究的热门话题之一，也是大家都非常关心的一个问题。从国际上的情况来看，也是各国都在探索的一个问题。下面

我们从三个方面来探讨一下信息安全风险评估。

34.2.1　信息安全风险评估的概念

信息系统主要存在两方面的安全风险：一是系统存在着脆弱性，就是我们常说的技术上的漏洞，可以被利用的漏洞；二是人为或自然的威胁，导致一些信息安全事件发生的可能性及其造成的影响，特别是负面影响。也就是说脆弱性和威胁是原因，可能性和影响是结果，当然还有一些其他的要素。信息安全风险评估是指对信息系统及其处理的传输和存储的信息的保密性、完整性和可用性等安全属性进行科学识别和评价的过程，因为人们的认识能力和实践能力，从阶段性来说总是有局限性的。

可以说信息系统存在的脆弱性是不可避免的，经过几十年的研究，大家发现这是由于人为的错误所造成的，对于现在我们所使用的一个庞大的、复杂的技术系统来说，恐怕在长时间内是不可避免的。在现实环境中，人们总是要面临着各种各样的威胁，或者说信息安全风险是必然的。在这种情况下，通过适当的、足够的，有时候是综合的安全措施来控制风险，最终目的是使残余下来的风险可以降低到最低程度。由于任何信息系统都会有安全风险，所以，人们追求的所谓安全的信息系统，实际上是指信息系统在实施了风险评估并做出风险控制后，仍然存在的残余风险可被接受的信息系统。

风险评估是对信息资产面临的威胁、存在的弱点、造成的影响，以及三者综合作用而带来风险的可能性的评估。作为风险管理的基础，风险评估（Risk Assessment）是组织确定信息安全需求的一个重要途径，属于组织信息安全管理体系策划的过程。风险评估的主要任务包括：

- 识别组织面临的各种风险；
- 评估风险概率和可能带来的负面影响；
- 确定组织承受风险的能力；
- 确定风险消减和控制的优先等级；
- 推荐风险消减对策。

在风险评估过程中，有几个关键的问题需要考虑。第一，要确定保护的对象（资产）是什么？它的直接和间接价值如何？第二，资产面临哪些潜在威胁？导致威胁的问题何在？威胁发生的可能性有多大？第三，资产中存在哪些弱点可能会被威胁所利用？利用的容易程度又如何？第四，一旦威胁事件发生，组织会遭受怎样的损失或者面临怎样的负面影响？第五，组织应该采取怎样的安全措施才能将风险带来的损失降低到最低程度？解决以上问题的过程，就是风险评估的过程。

34.2.2　风险评估的意义和作用

（1）风险评估是信息系统安全的基础性工作，它是观察过程中的一个持续的工作。信息安全中的风险评估是传统的风险理论和方法在信息系统中的运用，是科学地分析和

理解信息与信息系统在保密性、完整性、可用性等方面所面临的风险，并在风险的减少、转移和规避等风险控制方法之间做出决策的过程。

由于风险评估将导出信息系统的安全需求，因此，所有信息安全建设都应该以风险评估为起点。信息安全建设的最终目的是服务于信息化，但其直接目的是为了控制安全风险。

只有在正确、全面地了解和理解安全风险后，才能决定如何处理安全风险，从而在信息安全的投资、信息安全措施的选择、信息安全保障体系的建设等方面做出合理的决策。

进一步地说，持续的风险评估工作可以成为检查信息系统本身乃至信息系统拥有单位的绩效的有力手段，风险评估的结果能够供相关主管单位参考，并使主管单位通过行政手段对信息系统的立项、投资、运行产生影响，促进信息系统拥有单位加强信息安全建设。

（2）风险评估是分级防护和突出重点的具体体现。

- 信息安全建设的基本原则包括必须从实际出发，坚持分级防护、突出重点。
- 风险评估正是这一原则在实际工作中的具体体现。
- 从理论上讲，不存在绝对的安全，实践中也不可能做到绝对安全，风险总是客观存在的。
- 安全是风险与成本的综合平衡。
- 盲目追求安全和回避风险是不现实的，也不是分级防护原则所要求的。

要从实际出发，坚持分级防护、突出重点，就必须正确地评估风险，以便采取科学、客观、经济和有效的措施。

（3）加强风险评估工作是当前信息安全工作的客观需要和紧迫需求。

34.2.3 信息安全风险评估的基本要素

信息安全风险评估的基本要素包括前面所说的资产、威胁、脆弱性、风险。其中，资产是指通过信息化建设积累起来的信息系统、信息、生产或服务能力、人员能力和赢得的信誉等。威胁是指一个单位的信息资产的安全可能受到的侵害。威胁由多种属性来刻画：威胁的主体（威胁源）、能力、资源、动机、途径、可能性和后果。脆弱性是指信息资产及其防护措施在安全方面的不足和弱点。脆弱性也常常被称为弱点或漏洞。风险由意外事件发生的可能性及发生后可能产生的影响两种指标来衡量。风险是在考虑事件发生的可能性及其可能造成的影响下，脆弱性被威胁所利用后所产生的实际负面影响。风险是可能性和影响的函数，前者指威胁源利用一个潜在脆弱性的可能性，后者指不利事件对组织机构产生的影响。残余风险是指采取了安全防护措施，提高了防护能力后，仍然可能存在的风险。

由于现在的信息系统可以是一个组织、公司乃至国家完成使命的一种手段，因此它的风险评估必须从使命出发。由于信息化取得了很多的成果，得到了很广泛的应用，所以就产生了资产，我们用信息资产这个概念来描述我们信息化的成果，或者我们在信息

化过程中进行衡量，也许信息资产的概念是最直接的概念，当然它也存在一个量化问题。在信息安全威胁方面，我们当前信息化过程中有来自很多方面的威胁，既有人为的，也有自然的，都可能对我们信息系统造成威胁。根据一般的理解，由于人们只有在具体的事件中才能逐渐认识信息安全的利益所在，所以我们在评估的时候要关注以往发生的事情和别人发生的事情。残余风险不可能完全消除，这是由于信息化的发展，信息系统已经渗透到这个社会生活的各个方面，已经逐渐成为一个谁也离不开的东西。同时它经受着方方面面的危险，因此也许在相当长的时间之内完全消除风险是不现实的，所以必须承认即使我们采取了措施，即使我们加强了保护，即使我们投入了很多的资源，最终我们还是要面临风险。当对我们采取的安全措施再进行评估时，要考虑已有的安全措施是否还有效，是否有待加强。安全措施需要从管理、技术、运行三个方面去考虑。通过安全措施对资产加以保护，对脆弱性加以弥补，从而可降低风险。实施了安全措施后，威胁只能形成残余风险。而这个过程中往往是很多措施共同起作用的。在我们考虑采取措施时，特别是对安全级别要求比较高的系统，往往要采取综合性的措施加以防范。

从对现行信息系统的风险分析入手，采用先进的风险分析方法，明确系统要保护的资产，找出系统的弱点和威胁，度量各种安全风险。

（1）确认最关键的资产。明确保护的资产、资产的位置，以及资产的重要性是安全风险分析的关键。

（2）基于对关键资产的确认，系统管理员、操作者、安全专家对网络脆弱性进行评估，进行风险的识别。采取合适的方法、手段对信息资产的风险进行识别，这些方法、手段包括调查研究、理论分析、会议座谈、工具分析、历史情况分析、雇请工程师进行模拟渗透式攻击等方法，以便尽可能地暴露信息与网络系统的风险点。

（3）风险的度量。明确存在哪些弱点漏洞及这些弱点漏洞的风险级别，分析资产所面临的威胁，以及发生的可能性和一旦出现安全问题可能造成什么样的影响等。对于能够量化的应尽可能地量化，对于不能量化的应进行形式化分析。

34.2.4　风险评估的途径

在风险管理的前期准备阶段，组织已经根据安全目标确定了自己的安全战略，其中就包括对风险评估战略的考虑。所谓风险评估战略，其实就是进行风险评估的途径，也就是规定风险评估应该延续的操作过程和方式。风险评估的操作范围可以是整个组织，也可以是组织中的某一部门，或者独立的信息系统、特定系统组件和服务。影响风险评估进展的某些因素，包括评估时间、力度、展开的幅度和深度，都应与组织的环境和安全要求相符合。组织应该针对不同的情况来选择恰当的风险评估途径。目前，实际工作中经常使用的风险评估途径包括基线评估、详细评估和组合评估三种。

1. 基线评估

如果组织的商业运作不是很复杂，并且组织对信息处理和网络的依赖程度不是很高，或者组织信息系统多采用普遍且标准化的模式，基线风险评估（Baseline Risk Assessment）就可以直接而简单地实现基本的安全水平，并且满足组织及其商业环境的所有要求。

采用基线风险评估，组织根据自己的实际情况（所在行业、业务环境与性质等），对信息系统进行安全基线检查（用现有的安全措施与安全基线规定的措施进行比较，找出其中的差距），得出基本的安全需求，通过选择并实施标准的安全措施来消减和控制风险。所谓的安全基线，是在诸多标准规范中规定的一组安全控制措施或者惯例，这些措施和惯例适用于特定环境下的所有系统，可以满足基本的安全需求，能使系统达到一定的安全防护水平。组织可以根据以下资源来选择安全基线：

（1）国际标准和国家标准，例如 BS 7799-1、ISO 13335-4；

（2）行业标准或推荐标准，例如，德国联邦安全局 IT 基线保护手册；

（3）来自其他有类似商务目标和规模的组织的惯例。

当然，如果环境和商务目标较为典型，组织也可以自行建立基线。

基线评估的优点是需要的资源少，周期短，操作简单，对于环境相似且安全需求相当的诸多组织，基线评估显然是最经济有效的风险评估途径。当然，基线评估也有其难以避免的缺点。比如，基线水平的高低难以设定，如果过高，可能导致资源浪费和限制过度，如果过低，可能难以达到充分的安全。此外，在管理安全相关的变化方面，基线评估比较困难。基线评估的目标是建立一套满足信息安全基本目标的最小的对策集合，它可以在全组织范围内实行，如果有特殊需要，应该在此基础上，对特定系统进行更详细的评估。

2. 详细评估

详细风险评估要求对资产进行详细识别和评价，对可能引起风险的威胁和弱点水平进行评估，然后根据风险评估的结果来识别和选择安全措施。这种评估途径集中体现了风险管理的思想，即识别资产的风险并将风险降低到可接受的水平，以此证明管理者所采用的安全控制措施是恰当的。

详细评估的优点在于：

（1）组织可以通过详细的风险评估而对信息安全风险有一个精确的认识，并且准确定义出组织目前的安全水平和安全需求；

（2）详细评估的结果可用来管理安全变化。

当然，由于详细的风险评估可能是一个非常耗费资源的过程，包括时间、精力和技术，因此，组织应该仔细设定待评估的信息系统范围，明确商务环境、操作和信息资产的边界。

3. 组合评估

基线风险评估耗费资源少、周期短、操作简单，但不够准确，适合一般环境的评估；详细风险评估准确而细致，但耗费资源较多，适合严格限定边界的较小范围内的评估。实践当中，组织多是采用二者结合的组合评估方式。

为了决定选择哪种风险评估途径，组织首先对所有的系统进行一次初步的高级风险评估，着眼于信息系统的商务价值和可能面临的风险，识别出组织内具有高风险的或者对其商务运作极为关键的信息资产（或系统），这些资产或系统应该划入详细风险评估的范围，而其他系统则可以通过基线风险评估直接选择安全措施。

这种评估途径将基线风险评估和详细风险评估的优势结合起来，既节省了评估所耗费的资源，又能确保获得一个全面系统的评估结果。而且，组织的资源和资金能够应用到最能发挥作用的地方，具有高风险的信息系统能够被预先关注。当然，组合评估也有缺点：如果初步的高级风险评估不够准确，某些本来需要详细评估的系统也许会被忽略，最终导致结果失准。

34.3　信息安全策略

在信息安全工程体系中，信息安全策略（Information Security Policy）是指在一个组织内指导如何对包括敏感信息在内的资产进行管理、保护和分配的规则和指示。确定并实施安全策略是组织的一项重要使命，也是组织进行有效安全管理的基础和依据。由于安全策略是信息系统安全保障的核心和起点，因此在构建安全的信息系统之前，制订明确和合理的安全策略就成为关键。信息安全具有相对的概念，安全策略制订工作的主要任务就是收集目标系统的最小安全需求，对其进行形式化处理，整理成一套安全策略的基本原则。在安全策略制订过程中必须考虑可行性和成本效益，也就是说，除了要考虑安全策略的可操作性，还要明确由这些安全策略所带来的附加开销能够得到管理层的理解和支持，以便加强、维护网络和系统的安全。

目前，缺乏良好的安全策略和指导文件是大多数公司所面临的主要安全脆弱性之一。在建设信息系统之初，系统安全人员的大部分时间将花在根据目标系统的业务需求进行风险分析与风险评估的工作上。通常，这些工作可以分成四个步骤：首先，识别目标计算机和网络面临的所有威胁；其次，确定这些威胁的种类和危害程度；再次，根据目标系统的业务需求实行风险评估；最后，推荐行为措施，制订安全措施和安全指导手册。

34.3.1　威胁分析和风险分析

可靠的风险评估的第一步是对风险进行正确的识别。对于信息资产来说，各种不同的对象存在不同的情况，有的资产可能具有较多脆弱性，有的资产可能受到诸多威胁，

有的资产可能目前尚未受到威胁，但是对于风险评估来说属于高重要性对象，等等。由此可见，如何正确对信息资产进行分类，划分不同的等级，正确识别出风险评估的对象是进行风险评估乃至风险管理的一个非常关键的前提条件。造成信息资产的风险的主要因素有三个：脆弱性、威胁和资产的危险程度（也就是重要性），三者对风险的影响如图 34-2 所示。

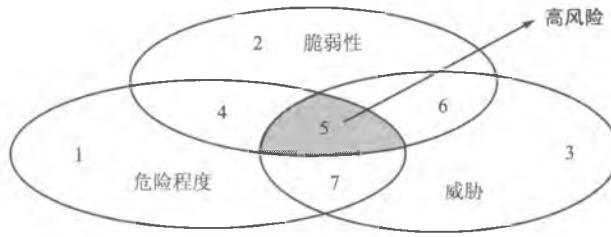

图 34-2　资产风险评估图

信息资产的脆弱性指的是可以通过什么方法来危及、试探、破坏甚至毁坏目标资产；信息资产受到的威胁指的是谁，以及如何能够找到资产的脆弱性；危险程度指的是资产的重要性。如图 34-2 所示，图中的 3 个椭圆区域分别代表脆弱性、威胁和危险程度，3 个椭圆相互重叠，将其并集区域划分为 7 个部分，我们分别用数字 1 到 7 表示。下面我们对这 7 个部分分别代表的含义进行描述：

（1）部分重要资产，包括信息、系统、程序、人员、设备或工具等，它们均不存在脆弱性和威胁；

（2）部分非重要资产，包括系统、程序，人员、设备或工具等，它们均没有已知威胁；

（3）威胁环境，不属于重要资产且不具有脆弱性；

（4）部分重要资产，具有已知脆弱性，但是不具有威胁；

（5）部分重要资产，具有已知脆弱性和威胁，这是最敏感的区域，也就是我们进行风险评估的重点；

（6）部分非重要资产，具有已知脆弱性和威胁；

（7）部分重要资产，无已知脆弱性，但是受到特定的威胁。

风险识别的目标就是对信息资产的脆弱性、威胁和危险程度进行分析，找出风险的大小等级，为确定风险评估的对象奠定基础。风险是信息资产本身的脆弱性、受到的威胁，以及其危险程度共同作用的结果，从数学角度来说，风险是 3 个变量，危险程度、脆弱性和威胁的函数。我们用公式表示为：

$$R=F\ (PV, Pr, C)$$

式中：R 为资产受到某种威胁而具有的风险；PV 为威胁发生的概率；Pr 为脆弱性被利用的概率；C 为资产的危险程度，也就是资产对于风险分析来说具有的重要性。

在进行具体的风险识别时，可以采用风险矩阵的方法来确定风险的大小等级。风险

主要是由威胁发生的概率、脆弱性被威胁利用的概率，以及信息资产的重要程度来确定，我们可以根据这 3 个因素预先设定一个三维风险价值矩阵，称之为“预先价值矩阵（Matrix with Predefined Value）”，然后按照威胁、脆弱性和重要程度的识别与评价方法逐一确定目标信息资产的每一威胁发生的概率、脆弱性被该威胁利用的概率和资产的重要程度，从而可以从风险的预先价值矩阵中查出对应的风险值。下面我们给出一个风险预先价值矩阵的例子。在表 34-1 中：将威胁发生的概率划分为低、中、高三级，分别赋值 0 到 2；将脆弱性被威胁利用的概率也划分为低、中、高三级，分别赋值 0 到 2；将信息资产的重要程度划分为五级，分别赋值 0 到 4；风险值最简单的计算方法是将 3 个参数值相累加。当然，在实际计算信息资产的风险值时可考虑更复杂的计算公式。

表 34-1　风险预先价值矩阵例表

	威胁发生的概率	低（0）			中（1）			高（2）		
	脆弱性被利用的概率	低 0	中 1	高 2	低 0	中 1	高 2	低 0	中 1	高 2
资产重要程度	0	0	1	2	1	2	3	2	3	4
	1	1	2	3	2	3	4	3	4	5
	2	2	3	4	3	4	5	4	5	6
	3	3	4	5	4	5	6	5	6	7
	4	4	5	6	5	6	7	6	7	8

34.3.2　制订安全策略

如前所述，安全策略是为发布、管理和保护敏感的信息资源而制订的一组法律、法规和措施的总和，是对信息资源使用、管理规则的正式描述，是企业内所有成员都必须遵守的规则。根据对信息系统风险分析的结果，结合安全目标和安全需求，提出系统的安全策略，作为安全体系进一步设计的依据和指导。安全策略可能包括物理安全策略、网络安全策略、应用安全策略和管理安全策略等。

在这一环节，我们为目标信息系统制订一个完备且合适的安全策略。根据威胁分析和风险分析得到目标系统的安全级别，在充分考虑成本效益的前提下，要根据安全级别为目标信息系统定义一个完备且合适的安全策略，该策略应根据自身风险和承受能力来包含尽可能多的方面，组织的安全策略的主要内容应包括：

- 组织拥有并且需要保护的信息资产；
- 组织实施信息安全的组织架构、角色定义和人员责任；
- 组织对内部和外部用户正确使用资源的期望方式；
- 组织对信息资产的防护方针；
- 组织针对安全事件的响应机制。

该安全策略通常来说，至少应具备以下几个特性：机密性、完整性、可用性、可确认性、保障性和可实施性。

（1）机密性。必须控制对系统的信息、服务和设备的访问，以确保敏感信息的机密性。只有需要这些信息和服务的授权人员才能访问系统和数据。

（2）完整性。必须保持目标系统中软硬件和数据的完整性，以确保它们能在网络或公共介质上正确处理、存储和传输。系统中的每个文件或数据集，在其生命周期内都必须具备一个可识别源。

（3）可用性。必须保证系统免受拒绝服务攻击或环境变化等的威胁，例如，断电或温度过高等，但是必须考虑保护措施的成本效益。

（4）可确认性。系统必须能够追踪与系统安全相关的事件，包括违反和企图违反安全策略的子系统或用户。系统必须执行以下规则：访问系统的人员和子系统必须具有唯一标识，在被允许访问敏感信息、服务和设备之前必须具有标识与鉴别机制；每个处理敏感或重要任务的子系统都必须对与安全相关的事件保持审计迹。该审计信息必须能够防篡改，并要保持其能起作用。

（5）可保障性。必须明确目标系统处理的信息、设备、服务，以及需要知情的员工的重要性和敏感性，以确定合理的安全需求。根据安全策略，系统选用的安全措施必须能够提供足够的与数据重要性相称的安全保护。

（6）可实施性。安全策略必须贯彻于系统的整个生命周期。必须对系统安全功能的所有措施，包括那些在子系统级实行的措施进行评估，以确保能够充分满足安全策略的需求。每个平台都必须进行评估，以确保系统配置能够执行声明的安全策略。最后可以生成一份脆弱性评估报告，该评估必须由安全管理员或系统管理员来执行，以决定是否必须修改系统，使其遵循安全策略。

34.3.3　制订详细计划实施安全策略

由于安全策略与组织的安全级别，以及业务需求是密不可分的，因此，安全策略的制订过程也应贯穿于策略的整个执行过程。也就是说，要通过实践来不断调整与完善信息安全策略体系和内容，信息安全策略的实施过程是一项较为长期的反复的过程。可见，任何组织一旦建立起安全策略，就必须创建一个详细的实施计划，逐步、分段地增加和改进信息安全基础设施，以便完备地实施该安全策略。详细的实施计划有助于有效地管理开支计划和控制执行时间。

安全策略实施的整个过程将涉及目标组织各个层次上的多方面人员，包括高级管理层、关键业务部门、IT 部门、用户代表等。其中，获得高层管理层的支持与认可是安全策略得以顺利贯彻落实的关键。

信息安全策略实施计划至少应该包含以下步骤：

- 进行现场勘查，了解每个员工的信息系统的环境现状；
- 与相关人员进行访谈，深入全面了解组织的业务需求，以及相应的安全需求；
- 通过文档审查，了解组织当前的策略制订及部署情况；
- 从最高层次到最低层次分级制订安全策略；

- 通过与相关人员讨论，或者召开讨论会议等形式来完善每项安全策略；
- 通过培训等多种途径，让组织的员工、顾客等获知并理解与其工作有关的安全策略；
- 试实行安全策略时，既可以在整个组织范围内也可以在特定的部门内进行，其中包括购买必需的软硬件设备、雇用必需的员工以及安装和测试软硬件设备等；
- 搜集、分析反馈意见，修订和调整安全策略；
- 由管理层批复，发布正式版《安全策略实施指南》，其内容涵盖各种技术标准、规范和手册、关键的操作程序和管理方针、与信息安全相关的具体的管理制度等；
- 根据《安全策略实施指南》，对组织的员工、顾客等进行安全策略方面的培训；
- 长期执行并维护安全策略。

34.4　密码技术

计算机网络安全的发展是以密码学研究为基础的，信息加密、数字签名、数字印鉴、身份鉴别等安全机制是建立在密码技术的基础之上，是一种主动式防范技术。当前密码技术是解决信息系统安全的一项核心技术，是解决信息安全问题的最有效的手段之一。密码分为三种体制：单钥密码体制、双钥密码体制和混合密码体制。密码体制的安全依赖于密钥的安全。

34.4.1　单钥密码体制

一个加密系统，如果加密密钥和解密密钥相同，或者不相同但可以由其中一个推导出另一个，则是单钥密码体制（又称对称密钥密码体制、秘密密钥密码体制、私钥体制），常见的有著名的 DES（Data Encryption Standard，数据加密标准）算法。

DES 是一种数据分组的加密算法，采用多次换位加密与代替相结合的处理方法，将数据分成长度为 64 位的数据块，其中 8 位做奇偶校验，有效密码长度为 56 位。首先，将明文数据进行初始置换，得到 64 位的混乱明文组，再将其分成两段，每段 32 位；然后，进行乘积变换，在密钥的控制下，做 16 次迭代；最后，进行逆初始变换而得到密文。DES 算法已通过硬件实现，效率非常高。其优点是：具有很高的保密强度；加密后信息没有膨胀；可生成数字印鉴用于数据防篡改。其缺点是：密钥使用一段时间后就必须更换，密钥在传递过程中容易泄露；N 个人要使用 $N(N-1)/2$ 个密钥，密钥管理非常困难；无法解决数字签名验证的问题。

单钥密码体制使用相同的密钥加密和解密，传统密码技术都属于这一类。由于该体制以很高的速度实现加密算法，所以常常用来加密数据含量大的通信消息和文件。其典型实例包括美国开发的 DES、瑞士开发的 IDEA（国际数据加密算法），以及最近颁布

的 AES（高级加密标准）等。单钥密码体制的关键问题是：如何保证与之通信各方的独立密钥的秘密性；如何在发收方之间安全传递密钥；如何管理大量的秘密密钥等。单钥密码体制既可用于数据加密，也可用于信息的认证。

34.4.2 双钥密码体制

如果将一个加密系统的加密密钥和解密密钥分开，加密和解密分别由两个密钥来实现，并且由加密密钥推导出解密密钥（或由解密密钥推导出加密密钥）在计算上是不可行的，这种密码体制称为双钥密码体制（又称非对称密钥密码体制、公开密钥密码体制、公钥体制），采用双钥密码体制的每一个用户都有一对选定的密钥，一个可以公开，一个由用户秘密保存，双钥密码体制的出现是对现代密码学的一个重大突破，它给网络信息的安全带来了新的活力。

双钥密码体制是美国 Diffie 和 Hellman 于 1976 年提出的概念，比较著名的双钥密码体制的实现方案有：Deffie、Iellman 和 Nerkle：双钥交换体制，它的保密性是基于求解离散对数问题的困难性；Rivest、Shamir 和 Adleman 提出的 RSA 双钥体制，它的保密性基于大整数素因子分解的困难性；Merkle 和 Herman 提出的背包双钥体制，它的保密性是基于求解背包的困难性；我国科学家陶仁骥、陈世华提出的有限自动机密码体制，它的保密性是基于构造非线性弱可逆有限自动机弱逆的困难性和矩阵多项式分解的困难性。

经典的 RSA 算法是建立在“大数分解和素数检测”的理论基础上的。2 个大素数相乘在计算机上是容易实现的，但将乘积分解为 2 个大素数因子的计算量却相当巨大，大到甚至在计算机上也不可能实现。

素数检测就是判定一个给定的正整数是否为素数，该算法取用一个合数（该合数为 2 个素数的乘积），而不是取用一个大素数作为其模数，其实现的步骤可分为：设计密钥、设计密文和恢复明文几个过程。

双钥密码体制的加密和解密采用不同密钥。发方利用收方的公开密钥加密密文，收方使用与公开密钥对应的秘密密钥解密密文。由于公钥密码体制只需保密解密密文所需的密钥，所以密钥管理比采用秘密密钥密码体制容易得多。它的优点有：密钥分配简单；密钥的保存量少；可以满足互不相识的人之间进行私人谈话时的保密性要求；可用于数字签名；可实现防否认服务。

双钥密码体制的最大缺陷是加密速度慢。另外，双钥体制建立在未证明的理论之上，不能认为是绝对安全的；双钥体制的时间耗费巨大；双钥必须要求能保护公钥文件的完整性。

34.4.3 混合密码体制

在实际密码通信中常采用混合密码体制的方式，即数据含量大的通信采用高速的对

称密钥密码体制加密，而对称密钥密码体制的密钥，由于其数据含量少，则用公钥密码体制加密传递给收方。

混合密码体制融合了对称密码体制和公钥密码体制的优点，如将 RSA 与 DES 结合构成的混合加密方法称为 RSA 数字信封。BIIC 加密体制是其著名代表，结合了 DES 和 RSA 的优点，兼具了算法的高效率、高保密性、数字印鉴功能和 RSA 的密钥管理简便、数字签名的功能，可用于确定数据文件的完整性及数据来源等。BIIC 加密体制是将 RSA 公开密钥和私有密钥反过来使用，即用私有密钥加密文件，用公开密钥解密，使他人无法涂改或伪造数据文件。混合密码体制已被广泛用于 S/MIME 协议、SSL 协议和 SET 协议。

无论对称密钥密码体制还是公开密钥密码体制，密钥的产生、分发和管理是其关键。随着 Internet 技术的发展，网络信息安全成为 Internet 服务、电子商务、网络银行等各类机构或企业关注的焦点问题。近年来 Internet 上出现了许多新的安全技术和安全规范，公开密钥基础设施（PKI，Public Key Infrastructure）成为其中重要的技术。

34.5　访问控制

34.5.1　访问控制技术

访问控制就是要对访问的申请、批准、执行、撤销全过程进行控制。访问控制决定一个用户或程序是否有权对某一特定资源或协同内容执行一个特定的操作（如共享、修改、签字等），以确保只有合法用户的合法访问才能得到批准，且被批准的访问只能执行授权的操作。有三种权限判定方法：强制法、随意法和角色判定法。

（1）在强制法中，每个用户具有一个安全级，针对每个资源也有相应的安全系数，安全级集合是一个偏序集。也可以采用分类的方法，每个用户不仅有一个安全级，而且在同一级中还要受类别的控制。一般原则是用户有权读取其安全级以下的所有资源，也有权向其安全级以上的资源写入数据。

（2）随意访问控制，用访问矩阵指定每一个用户对每个资源的访问模式（读、写、执行等权限）。随意法灵活，但它不能控制信息流向。

（3）角色判定法，是以用户访问某特定资源时的角色来决定其权限，具体办法是：为每一个资源对象建立一张访问控制列表，表明其对各种角色赋予的权限；也给每个用户赋予一个或几个预定的角色，这种方法具有前两种的特点和优点，而且更加安全和方便。

34.5.2　身份认证技术

身份认证就是确定用户是否合法，有两种身份认证方法：基于令牌的身份验证和 Kerberos。

（1）验证令牌为一次性口令机制，口令仅使用一次，在同一台主机上，用户不同时间所用的口令是不同的。一个用户在注册到网络远程主机之前，必须向主机表明身份并产生一个口令表。有同步和挑战应答两种实现算法：在同步算法中，身份认证服务器 AS 负责管理用户登录，它产生一个 PIN（Personal Identification Number）给用户，当用户使用 PIN 登录时，AS 查找内部的身份认证数据库，若得到与用户令牌中相同的 key，则用户的令牌产生一个序列，通过比较这两个序列是否相同来鉴别用户身份。在挑战应答算法中，AS 也提供一个 PIN 给用户，但它还产生一个随机数，用户将这个随机数送入令牌，令牌将其加密返回一个序列，AS 内部根据用户 PIN，找到其令牌中的 key，也加密那个随机数，如果所得序列与用户令牌所得一致，就为合法用户。

（2）Kerberos 是一种由第三方进行的，基于保密密钥的身份认证算法。Kerberos 作为被信赖的第三方分别与网络上的每一个主体（Server 或 Client）共同持有一个保密密钥。为了能够访问服务器，该用户必须从 Kerberos 处得到一张 ticket，由于这张 ticket 是用该服务器的密钥加密的，所以只有 Kerberos 和服务器能读懂它，因而可确定用户是否合法。

34.5.3　网络安全访问控制

访问控制是网络安全防范和保护的主要策略，它的主要任务是保证网络资源不被非法使用和访问。它是保证网络安全最重要的核心策略之一。访问控制涉及的技术也比较广，包括入网访问控制、网络权限控制、目录级安全控制，以及属性安全控制等多种手段。

1．入网访问控制

入网访问控制为网络访问提供了第一层访问控制。它控制哪些用户能够登录到服务器并获取网络资源，控制准许用户入网的时间和准许他们在哪台工作站入网。用户的入网访问控制可分为三个步骤：用户名的识别与验证、用户口令的识别与验证、用户账号的默认限制检查。三道关卡中只要任何一关未过，该用户便不能进入该网络。对网络用户的用户名和口令进行验证是防止非法访问的第一道防线。为保证口令的安全性，用户口令不能显示在显示屏上，口令长度应不少于 6 个字符，口令字符最好是数字、字母和其他字符的混合，用户口令必须经过加密。用户还可采用一次性用户口令，也可用便携式验证器（如智能卡）来验证用户的身份。网络管理员可以控制和限制普通用户的账号使用、访问网络的时间和方式。用户账号应只有系统管理员才能建立。用户口令应是每个用户访问网络所必须提交的“证件”。用户可以修改自己的口令，但系统管理员应该控制对口令的以下几个方面的限制：最小口令长度、强制修改口令的时间间隔、口令的唯一性、口令过期失效后允许入网的宽限次数。用户名和口令验证有效之后，再进一步履行用户账号的默认限制检查。网络应能控制用户登录入网的站点、限制用户入网的时间、限制用户入网的工作站数量。当用户对交费网络的访问“资费”用尽时，网络还应

能对用户的账号加以限制，用户此时应无法进入网络访问网络资源。网络应对所有用户的访问进行审计。如果多次输入口令不正确，则认为是非法用户的入侵，应给出报警信息。

2. 网络权限控制

网络的权限控制是针对网络非法操作所提出的一种安全保护措施。用户和用户组被赋予一定的权限。网络控制用户和用户组可以访问哪些目录、子目录、文件和其他资源，可以指定用户对这些文件、目录、设备能够执行哪些操作。受托者指派和继承权限屏蔽（irm）可作为两种实现方式。受托者指派控制用户和用户组如何使用网络服务器的目录、文件和设备。继承权限屏蔽相当于一个过滤器，可以限制子目录从父目录那里继承哪些权限。我们可以根据访问权限将用户分为以下几类：特殊用户（即系统管理员）；一般用户，系统管理员根据他们的实际需要为他们分配操作权限；审计用户，负责网络的安全控制与资源使用情况的审计。用户对网络资源的访问权限可以用访问控制表来描述。

3. 目录级安全控制

网络应允许控制用户对目录、文件、设备的访问。用户在目录一级指定的权限对所有文件和子目录有效，用户还可进一步指定对目录下的子目录和文件的权限。对目录和文件的访问权限一般有 8 种：系统管理员权限、读权限、写权限、创建权限、删除权限、修改权限、文件查找权限、访问控制权限。用户对文件或目标的有效权限取决于以下因素：用户的受托者指派、用户所在组的受托者指派、继承权限屏蔽取消的用户权限。一个网络管理员应当为用户指定适当的访问权限，这些访问权限控制着用户对服务器的访问。8 种访问权限的有效组合可以让用户有效地完成工作，同时又能有效地控制用户对服务器资源的访问，从而加强了网络和服务器的安全性。

4. 属性安全控制

当用文件、目录和网络设备时，网络系统管理员应给文件、目录等指定访问属性。属性安全在权限安全的基础上提供更进一步的安全性。网络上的资源都应预先标出一组安全属性。用户对网络资源的访问权限对应一张访问控制表，用以表明用户对网络资源的访问能力。属性设置可以覆盖已经指定的任何受托者指派和有效权限。属性往往能控制以下几个方面的权限：向某个文件写数据、复制一个文件、删除目录或文件、查看目录和文件、执行文件、隐含文件、共享等。

5. 服务器安全控制

网络允许在服务器控制台上执行一系列操作。用户使用控制台可以装载和卸载模块，可以执行安装和删除软件等操作。网络服务器的安全控制包括可以设置口令锁定服务器控制台，以防止非法用户修改、删除重要信息或破坏数据；可以设定服务器登录时间限制、非法访问者检测和关闭的时间间隔。

34.6　用户标识与认证

34.6.1　PKI 概述

公钥基础设施 PKI（Public Key Infrastructure），是一种遵循既定标准的密钥管理平台，它能为所有网络应用提供加密和数字签名等密码服务及所必需的密钥和证书管理体系。简单地说，PKI 技术就是利用公钥理论和技术建立的提供信息安全服务的基础设施。

公钥体制是目前应用最广泛的一种加密体制。在这一体制中，加密密钥与解密密钥各不相同，发送信息的人利用接收者的公钥发送加密信息，接收者再利用自己专有的私钥进行解密。这种方式既能保证信息的机密性，又能保证信息具有不可否认性。为了使公开密码系统得以顺利运作，必须设法将公钥与其持有人紧密结合并证明某一公钥确实为某人或某机构所拥有。利用可信赖的第三方机构——证书机构 CA（Certificate Authority）作为密钥管理与验证机构，以签发数字证书方式证明公钥的效力。此外，所有辅助公开密码系统使用与应用服务的工作，均可视为公开密钥基础设施的一部分。

数字证书是把公钥及公钥的拥有者绑定在一起的数字文件，CA 利用自己的私钥签名用户证书，而 CA 的公钥证书则是广为发布的，从而使用户可以利用公证机关的证书来验证别的用户的证书。证书依据其用户分为两类：用于加密的证书和用于数字签名的证书。当然，也有既用于加密又用于数字签名的证书。

就目前来看，PKI 基础设施是比较成熟、完善的网络安全解决方案。具体说来，PKI 是一个颁发和管理用户密钥的系统，所有的 PKI 都应该具有以下两个基本操作。

（1）发放证书：将公开密钥与个人、组织或其他实体，以及类似于许可证或凭据的信息捆绑在一起。

（2）确认证书：判断一个证书是否可以被正确使用。

34.6.2　基于 X.509 的 PKI

X.509 是目前唯一已经实施的 PKI 系统，下面详细介绍基于 X.509 标准的 PKI 系统。基于 X.509 的 PKI 由以下各部分组成。

认证机关 CA：CA（Certificate Authorization）是证书的签发机构，它是 PKI 的核心。构建密码服务系统的核心内容是如何实现密钥管理。在公钥体制中，由于私钥由持有者秘密掌握，因此密钥管理主要是公钥的管理问题，目前较好的解决方案是引进证书机制。CA 是这样一个可信的机构，它对任何一个主体的公钥（即证书）进行公证，证明主体的身份，以及主体与公钥的匹配关系，并保证该公钥的可靠性、合法性和可用性。

证书库：证书库是证书的集中存放地，它与网上“白页”类似，是网上的一种公共信息库，用户可以从此处获得其他用户的证书和公钥。X.509 PKI 建议采用支持 LDAP 协议的目录系统构造证书库，用户或相关的应用通过 LDAP 来访问证书库。系统必须

确保证书库的安全可靠性和完整性，并防止伪造、篡改证书。

密钥备份及恢复系统：如果用户丢失了用于脱密数据的密钥，则密文数据将无法被脱密，造成数据丢失。为避免这种情况的出现，PKI 应该提供备份与恢复脱密密钥的机制。密钥的备份与恢复应该由可信的机构来完成。值得强调的是，密钥备份与恢复只能针对脱密密钥，签名私钥不能够做备份。

证书作废处理系统：证书作废处理系统是 PKI 的一个重要组件。同日常生活中的各种证件一样，证书在 CA 为其签署的有效期以内也可能需要作废。例如，A 公司的职员 a 辞职离开公司，这就需要终止 a 证书的生命期。为实现这一点，PKI 提供多种作废证书策略机制。

作废证书一般通过将证书列入作废证书表（CRL）来完成。通常，系统中由 CA 负责创建并维护一张及时更新的 CRL，而由用户在验证证书时负责检查该证书是否在 CRL 之列。证书的作废处理必须在安全及可验证的情况下进行，系统还必须保证 CRL 的完整性。

客户端应用接口系统：X.509 PKI 要求客户端应用接口系统，为各种应用提供跨平台、安全、一致、可信的与 PKI 交互的方式，同时要屏蔽密钥管理的细节。

以上各部分集成为一个系统，由相应的权威机构监督和管理，就是人们通常所说的“认证中心”、“证书服务中心”或“CA 中心”等。

34.6.3　X. 509 证书介绍

X. 509 证书标准是目前被广为接受的证书格式。X. 509 证书有两类，一类是身份证书；另一类是凭据证书。

1. X. 509 身份证书

通常所说的“数字证书”、“CA 证书”、“数字标识”多指的是 X. 509 身份证书。该证书类似于身份证明，它能简单地鉴别一个实体（在证书中被称为主体，Subject）和公钥的对应关系，因为其中列出了该实体的公钥。以下介绍 X. 509 身份证书的典型内容。

（1）Version：证书的 X.509 版本号，不同版本的证书格式不同。

（2）Serial Number：序列号，同一 CA 机构签发的证书序列号唯一。

（3）Algorithm Identifier：（或 CA signature algorithm）CA 签名算法的标识符及其必要的参数。

- Algorithm：CA 的签名算法的标识。
- Algorithm Parameters：CA 签名算法的参数。

（4）Issuer：（或 Issuer name）CA 机构的标识信息，即 CA 机构的 X. 500 名字。

（5）Period of Validity：证书有效期。

- Validity：有效期。
- Not Before Date：起始有效期。
- Not After Date：截止有效期。

（6）Subject:（或 Subject name）证书持有人的标识信息，即证书持有人的 X. 500 名字。

（7）Subject's Public Key:（或 Subject public Key Info）证书持有人的公钥，包括公钥值、算法标识名及参数。

- Algorithm：证书持有人的密钥要使用的算法的标识名。
- Parameters：必要的参数（如果有的话）。
- Public Key：证书持有人的公钥值。

（8）Signature：CA 机构对证书的签名。

*Issuer Unique Identifier：用于防止 CA 的 X. 500 名字重名的标识。

*Subject Unique Identifier：字符串，用于防止主体的 X. 500 重名。

（*注：由于后两项实现起来比较困难，具体实现中均采用一些变通的做法。）

此外，X. 509 第 3 版还有证书的许多扩展特性及 CRL 的格式。

2. X. 509 凭据证书

通常讲的证书主要是指身份证书（即公钥证书），主要用于认证和鉴别身份。当把与主体有关的某些属性（如许可证、角色、访问权限等）分离出来，就可以产生另一种证书，称为凭据证书。凭据证书主要用于许可证、角色、访问授权等。与身份证书不同，一个个体可以有多个凭据证书，所有凭据证书都与该主体的公钥相关，凭据证书用于证明主体具有的某些属性。凭据证书将属性值与 X. 509 身份证书捆绑在一起或直接与一个主体名捆绑在一起。

凭据证书包括以下内容。

（1）凭据证书匹配规则。

（2）凭据证书内容，包括颁发者、算法标识符、证书序列号、证书有效期、属性列表和扩展域等。

34.6.4　PKI 证书的作用

PKI 证书可提供下列 4 种重要的安全保证。

（1）机密性（Confidentiality）。文件可以用密钥加解密，以达到机密性。

（2）完整性（Integrity）。文件接收者通过数字签名核对可确保此文件的完整性。

（3）不可否认性（Non-repudiation）。因只有文件发送者知道自己的私有密钥，而且文件具有发送者的数字签名，使其无法否认发送的事实。

（4）鉴别（Authentication）。文件接收者可确认此文件的发送者身份。

PKI 证书所提供的机密性是指发送方将信息经接收方证书的公钥加密后的密文信息，只能由接收方用自己保存的私钥解密，任何其他人要想恢复原先信息，都是非常困难的，从而保证了通信的机密性。在加密应用中，接收者的公钥是完全公开的，任何想给接收者发送保密信息的人都可以公开、自由地得到接收者的公钥；而接收者的私钥则是需要严格保密的，绝对不能泄露给他人。即使加密后的信息在传送过程中被他人截取

或偷听，由于他无法得到接收方的私钥，也不能破解截取或偷听到的信息。机密性是证书最重要、最基本的功能之一。用证书进行加密及解密的过程如图 34-3 所示。

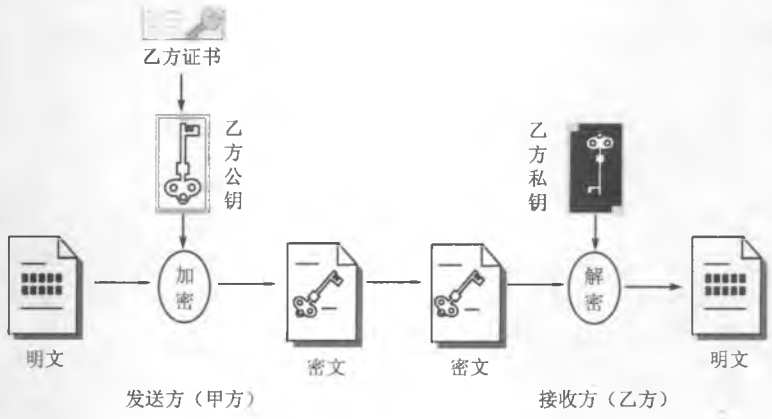

图 34-3　用证书进行加密和解密的过程

数据的完整性是指信息的接受者能够检验收到的信息是否真实可靠。检验的内容包括：信息的内容是否被篡改、信息是否被重放。信息的完整性常通过数字签名技术来实现。数字签名是防止网上交易时进行伪造和欺骗的一种有效手段。发送者在自己要公布或发送的电子文档上“签名”，接收者通过验证签名的真实性来确认文档是否被篡改过。在进行签名时，发送者首先将要签名的文档进行哈希（Hash）运算，然后发送者就可以用自己的签名私钥对 Hash 运算得出的简洁数据进行加密签名；接收者收到签名文档后，用发送者的公钥进行解密，得到解密后的 Hash 运算结果和文档。此时，接收者只需要计算出该文档的 Hash 运算结果并与解密得到的 Hash 运算结果进行比较，即可知道该文档的真伪。在数字签名应用中，发送者的公钥可以很方便地得到，而他的私钥则需要严格的保密。数字签名的过程与加密通信过程很相似，原理如图 34-4 所示。

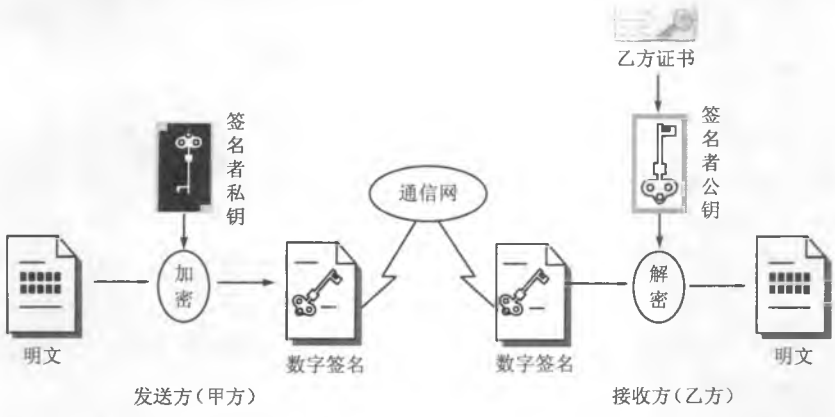

图 34-4　用证书进行数字签名图

为了防止人们否认自己曾经做过的事情，PKI 为此做了安全而有效的防范措施。当你要进行某些机密或重要的活动，PKI 要求你对所做的事情做数字签名，留下“指纹”，留待日后查证，以防事后抵赖。防抵赖从本质上仍然是数字签名技术的一种应用。

身份认证是数字签名技术的另一种应用，基于 CA 证书机构的权威性，其颁发的公钥证书实际上代表了证书持有人的真实身份。从某种意义上说，由于公钥证书是证书持有者的数字化身份证，而证书持有人的私有密钥与证书的公钥是一一对应的，因此用私有密钥对数据进行的加密（即数字签名），毫无疑问就代表了证书持有人对数据进行的加密。任何人收到加密数据以后，如果能够用某人的公钥证书解密数据，则表示该文件是由此证书的持有人所发送的。

PKI 技术是利用公钥理论和技术，以及传统加密技术建立的提供信息安全服务的基础设施，PKI 系统中使用的主要加密算法为：DES，Triple DES，RSA 等；主要签名算法为：MD5，SIIA 等。

34.6.5 PMI 与 PKI

PMI（Privilege Management Infrastructure）即授权管理基础设施或特权管理基础设施，是属性证书、属性权威、属性证书库等部件的集合体。X. 509 定义的属性证书框架提供了一个构建权限管理基础设施（PMI）的基础，这些结构支持类似访问控制的应用。

在过去的几年中，权限管理作为信息安全的一个领域得到快速发展，而且研究的热点集中于基于 PKI 的 PMI 研究。在 PKI 得到较大规模应用以后，人们已经认识到需要超越当前 PKI 提供的身份验证和机密性应用，步入授权应用领域。尽管 PKI 自身可以通过一定的手段提供授权访问控制的机制，但提供信息环境的权限管理还是被从 PKI 中脱离出来，成为了下一个信息安全研究的主要目标。

这是因为 PKI 在实际应用中，存在用户数量大、角色繁多、内容不同、规则多样、策略复杂，以及上下文环境差异等问题，其引起的访问控制和授权趋于复杂及难于管理，需要一种新的信息保护基础设施，能够系统地建立对认证用户的授权，这就是建立在 PKI 基础上的 PMI，它对权限管理进行了较为系统的定义和描述，将权限管理研究推到了应用前沿。

PMI 以资源管理为核心，将对资源的访问控制权统一交与授权机构进行管理，即由资源的拥有者来进行访问控制。换言之，PMI 的目的就是向用户和应用程序提供授权服务管理；向应用系统提供与应用相关的授权服务管理；提供用户身份到应用授权的映射功能；提供与实际应用处理模式相应的、与具体应用系统开发和管理无关的授权和访问控制机制。

PMI 的层次结构与 PKI 的层次结构类似，也是基于树状结构的。一般来说，其结构可分为三级：SOA 中心、AA 中心、AA 代理点。

SOA 中心：是授权管理体系的中心业务节点，是整个 PMI 的最终信任源和最高管理机构。它负责授权管理策略的管理、AA 中心的设立审核及管理，以及授权管理体系

业务的规范化等工作。可通过不同的 SOA 中心之间建立交叉认证信任链加以扩展。

AA 中心：是 PMI 的核心服务节点，与 SOA 中心通过业务协议达成相互信任关系，对属性证书进行签名及发布。它负责应用授权受理 AA 代理点的设立审核、代理点管理等工作。

AA 代理点：对应 AA 中心的附属机构，接受 AA 中心的直接管理；有与具体应用用户的接口 PA 及 UPA。PA（Policy Allocator）策略管理系统，用于对权限策略进行管理，UPA（User PA）应用用户管理系统，用于对用户权限进行管理。

属性证书（AC）：X. 509 v4 定义了属性证书，它记录用户的一些易变的信息（如级别等），公钥须与用户公钥证书（PKC）一起使用。PKI 与 PMI 比较如表 34-2 所示。

表 34-2　PKI 与 PMI 的比较

概　念	PKI 实体	PMI 实体
证书	公钥证书	属性证书
证书发行	CA	AA
证书用户	主体	拥有者
证书绑定	主体的名字和公钥	拥有者的名字和权限属性
撤销	CRL 证书撤销表	ACRL 属性证书撤销表
信任域	根 CA 或信任链	SOA（Source of Authority）
下级机构	CA	AA（Attribute of Authority）

目前，关于 PMI 系统的研究和开发还处在验证阶段，并没有统一的标准，很多国外著名的信息安全公司如 RSA，Entrust，Baltimore，IBM 等在 PMI 研究方面进行了大量的工作。政府方面也进行了相应的研究。例如，在 EU 资助下的 PERMIS 项目（Privilege and Role Management Infrastructure Standards Validation）正在进行中，并提出了一些草案，目的是验证 PMI 的适应性和可用性，并尝试标准化电子商务应用中所需的权限，以及制订描述这些权限和 PERMIS API 的 RFC；加拿大对 PMI 的研究也从纸面转向了电子验证。国内对 PMI 的研究已经开始，也已经有类似的产品出现，但是还没有应用实例。

总之，权限管理设施（PMI）是一个通过颁发属性证书来提供灵活的权限管理的基础设施，它的建立独立于 PKI，同时二者又存在着联系，PKI 是 PMI 的基础，而 PMI 则是 PKI 的扩展及补充。

34.7　安全审计与入侵检测

34.7.1　安全审计概述

随着信息技术的广泛应用，人们对信息技术产品和系统的依赖性越来越大，信息安全问题也日益突出。人们十分关注这些由大量的、复杂的部件构造起来的大型信息系统

的安全性到底如何，我们是否可以完全信任它。

目前关于信息技术产品和系统的评价和测量并没有形成形式化的测度理论，但存在着各种各样的安全测度的具体实践方式。目前，业界所有安全测度方式可以大致归结为以下四类：安全审计，包括内审和外审；风险分析；能力成熟模型；安全评测。

（1）安全审计。以审计概念为核心的安全测度思想认为存在关于安全的最佳实践。以通过最佳实践实施与否及其程度来测量 IT 系统的安全性。相关的模型和指南包括：美国信息系统审计和控制协会的 COBIT，德国的 IT 基本安全保护手册，ISO 17799，以及美国审计总署的自动信息系统安全审计手册等。它们主要针对的是信息系统安全措施的落实和安全管理，是一种静态、瞬时的测量方式。

（2）风险分析。风险分析模型是从风险控制角度进行安全测度分析。一般通过调查要保护的信息数据，假设对这些数据存在的安全威胁和漏洞，以及这些威胁和漏洞对数据可能造成的影响进行计算。经过数学的概率统计得出对安全性的测量，大部分以可能产生的损失来量化。从而提出需要进行安全风险控制，降低风险，将安全风险控制在可以接受的范围内。风险管理是一种动态的、反复的测量。

（3）能力成熟模型。能力成熟模型认为通过过程来保证安全。最著名的是 SSE-CMM 系统安全工程能力成熟模型，其思想来源于卡内基梅隆的软件工程能力成熟模型（SW-CMM）。它将安全能力划分为五个等级，从低到高，低等级的是指不成熟的、难以控制的，中等级是指可管理的、可控的，高等级是指可量化的、可测量的。能力成熟模型是一种动态的螺旋式上升的模型，我们将在后面的章节中详细描述。

（4）安全测评。安全测评更多地从安全技术、功能、机制角度来进行安全测量。早期的有美国国防部的橘皮书 TCSEC，但它比较适用于对计算机，特别是操作系统进行安全度量，它对操作系统从 C1 到 A1 的等级划分到现在仍有着相当的影响力。与其类似的还有欧洲的 ITSEC，加拿大的 CTCPEC。但这些标准已经不适合网络化的 IT 安全测量。经过近十年的努力，安全测量的重大标准 ISO 15408 终于产生，建成了通用评估准则 CC。CC 为信息技术、安全技术的测量提供了很好的方法，特别是信息安全产品，但对信息系统的测量仍不够充分。

34.7.2　电子数据安全审计

电子数据安全审计是对每个用户在计算机系统上的操作做一个完整的记录，以备用户违反安全规则的事件发生后，有效地追查责任。电子数据安全审计过程的实现可分成三步：第一步，收集审计事件，产生审计记录；第二步，根据记录进行安全违反分析；第三步，采取处理措施。

电子数据安全审计工作是保障计算机信息安全的重要手段。凡是用户在计算机系统上的活动、上机下机时间，与计算机信息系统内敏感的数据、资源、文本等安全有关的事件，可随时记录在日志文件中，便于发现、调查、分析及事后追查责任，还可以为加强管理措施提供依据。

1. 审计技术

电子数据安全审计技术可分三种：了解系统技术，验证处理技术和验证处理结果。

（1）了解系统技术。审计人员通过查阅各种文件，如程序表、控制流程等来审计。

（2）验证处理技术。这是为了保证事务能正确执行，控制能在该系统中起作用。该技术一般分为实际测试和性能测试，实现方法主要有以下三种。

- **事务选择。**审计人员根据制订的审计标准，可以选择事务的样板进行仔细分析。样板可以是随机的，选择软件可以扫描一批输入事务，也可以由操作系统的事务管理部件引用。
- **测试数据。**这种技术是程序测试的扩展，审计人员通过系统动作准备要进行处理的事务。通过某些独立的方法，可以预见正确的结果，并与实际结果相比较。用此方法，审计人员必须通过程序检验被处理的测试数据。另外，还有综合测试、事务标志、跟踪和映射等方法。
- **并行仿真。**审计人员可通过应用程序来仿真操作系统的主要功能。当给出实际的和仿真的系统相同的数据后，比较它们的结果。仿真代价较高，借助特定的高级语音系统可使仿真类似于实际的应用。

（3）验证处理结果技术。这种技术是指审计人员把重点放在数据上，而不是对数据的处理上。这里主要考虑两个问题。一是如何选择和选取数据。将审计数据收集技术插入应用程序审计模块（此模块根据指定的标准收集数据，监视意外事件）；扩展记录技术为事务（包括面向应用的工具）建立全部的审计跟踪；借用于日志恢复的备份库（如当审计跟踪时，用两个可比较的备份去检验账目是否相同）；通过审计库的记录抽取设施（它允许结合属性值随机选择文件记录并放在工作文件中，以备以后分析），利用数据库管理系统的查询设施抽取用户数据。

二是从数据中寻找什么。当抽取数据后，审计人员可以检查控制信息（含检验控制总数、故障总数和其他控制信息）；检查语义完整性约束；检查与无关源点的数据。

2. 审计范围

在计算机系统中，审计通常作为一个相对独立的子系统来实现。审计范围包括操作系统和各种应用程序。

操作系统审计子系统的主要目标是检测和判定对系统的渗透及识别误操作。其基本功能为：审计对象（如用户、文件操作、操作命令等）的选择；审计文件的定义与自动转换；文件系统完整性的定时检测；审计信息的格式和输出媒体；逐出系统、报警阈值的设置与选择；审计日志记录及其数据的安全保护等。

应用程序审计子系统的重点是针对应用程序的某些操作作为审计对象进行监视和实时记录，并根据记录结果判断此应用程序是否被修改和安全控制，是否在发挥正确作用；判断程序和数据是否完整；依靠使用者身份、口令验证终端保护等办法控制应用程序的运行。

3. 审计跟踪

通常审计跟踪与日志恢复可结合起来使用，但在概念上它们之间是有区别的。主要区别是日志恢复通常不记录读操作。但根据需要，日记恢复处理可以很容易地为审计跟踪提供审计信息。如果将审计功能与告警功能结合起来，就可以在违反安全规则的事件发生时，或在威胁安全的重要操作进行时，及时向安检员发出告警信息，以便迅速采取相应对策，避免损失扩大。审计记录应包括以下信息：事件发生的时间和地点；引发事件的用户；事件的类型；事件成功与否。

审计跟踪的特点是：对被审计的系统是透明的；支持所有的应用；允许构造事件实际顺序；可以有选择地、动态地开始或停止记录；记录的事件一般应包括被审计的进程、时间、日期、数据库的操作、事务类型、用户名、终端号等；可以对单个事件的记录进行指定。

按照访问控制类型，审计跟踪描述一个特定的执行请求，然而，数据库不限制审计跟踪的请求。独立的审计跟踪更保密，因为审计人员可以限制时间，但代价比较昂贵。

4. 审计流程

电子数据安全审计工作的流程是：收集来自核内和核外的事件，根据相应的审计条件，判断是否是审计事件。对审计事件的内容按日志的模式记录到审计日志中。当审计事件满足报警阈值时，则向审计人员发送报警信息并记录其内容。当事件在一定时间内连续发生，满足逐出系统阈值时，则将引起该事件的用户逐出系统并记录其内容。

常用的报警类型有：用于实时报告用户试探进入系统的登录失败报警，以及用于实时报告系统中病毒活动情况的病毒报警等。

审计人员可以查询、检查审计日志以形成审计报告。检查的内容包括：审计事件类型、事件安全级、引用事件的用户、报警、指定时间内的事件，以及恶意用户表等，上述内容可结合使用。

审计可分为人工审计，计算机手动分析、处理审计记录并与审计人员最后决策相结合的半自动审计，依靠专家系统做出判断结果的自动化的智能审计等。为了支持审计工作，要求数据库管理系统具有高可靠性和高完整性。数据库管理系统要为审计的需要设置相应的特性。

34.7.3　安全审计与入侵检测系统

安全审计与入侵检测系统主要用于监视并记录网络中的各类操作，实时地综合分析网络中发生的安全事件和外部事件，如外部入侵行为和内部事件，以及内部人员的文件复制、信息获取、信息发布、资源变迁等；然后根据设置的规则，智能地判断出违规行为，并对违规行为进行记录、报警和阻断。对网络中出现的黑客入侵行为进行实时报警和阻断，可以有效地阻拦来自网络内部和外部，特别是来自因特网的恶意破坏行为。系统自身的数据具备防销毁、防篡改的特性，能够为网络犯罪案件的侦破和取证提供精确、

宝贵的辅助数据。该系统可以在内部局域网上建立完善的安全预警和安全应急反应体系，为信息系统的安全运行提供保障。典型的系统结构如图 34-5 所示，服务网是一个典型的 ICP 服务模式，各类因特网的服务由不同服务主机完成，在需要的主机中装入审计软件，并由一台或几台审计设备对服务网络进行审计；对内部网络的服务器，也是通过形式多样的 Agent，收集安全审计信息，上报给审计中心。

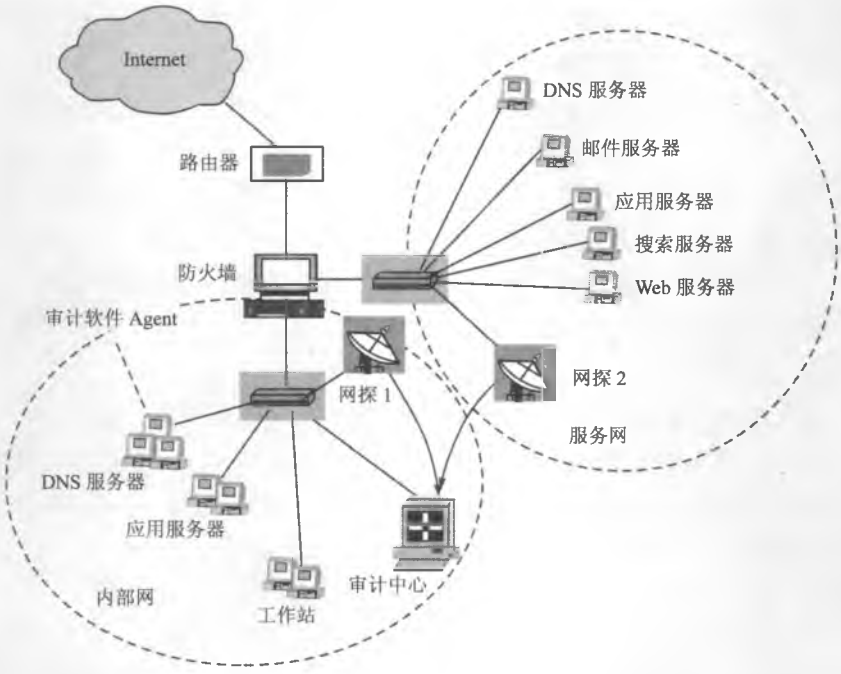

图 34-5　安全审计与入侵检测系统结构图

该系统的主要功能如下：

- 实时组态式的软件系统，与分布式结构紧密配合，灵活方便地重组新系统；
- 具有充当安全产品通用平台的能力，提供各个层次的接口功能，与其他产品很好地协同工作；
- 可充分扩充和升级的监测审计设备，可按用户需求进行定制；
- 系统具有很强的信息捕捉及还原能力，能识别多种非法入侵行为；
- 简洁高效的人机操作界面，配合丰富的说明文档，使用方便；
- 采用并联方式接入网络，对网络进行安全防卫，不影响现有网络效率；
- 灵活多样的安全响应机制，如在提供服务的同时也可抵御网络入侵，不必封堵和停止服务（防火墙通常通过封堵服务来抵御入侵）；
- 强大的事件处理记录功能，实现操作和违规的不可抵赖性，提供与安全有关事件的复查和取证功能；
- 全面监测和防卫能力，不仅能监测和抵御来自外部的入侵，同时能防止来自内

部的威胁；

- 采用分布式体系结构，可同时对多个网络系统进行审计监控。

34.8　信息系统安全的组织管理

信息系统的安全是一个整体的系统工程问题，所以不是通过简单的技术堆积就可以解决的。同时，信息系统安全问题是一个动态的问题，一个随着时间、人员、环境而变化的问题。可见，信息系统安全的设计必须遵循一定的原则，在一定的条件下，将技术措施与管理有机结合，求得最佳的解决方案。

另外，在复杂的信息环境中，使用统一和有效的安全原理开发 IT 解决方案时会遇到很多挑战。例如：集成专门的安全功能到计算机系统的多个组成架构中的复杂性，开发全面兼容的基本安全需求集的困难性。虽然随着国际化标准组织的安全评估通用标准（CC）的产生，使得开发可扩展的 IT 安全架构的困难减少了很多，但在具体过程中仍然存在着很多障碍。

设计信息安全系统的总体目标是“确保受保护目标信息的完整性、正确性和私密性”。由此可见，信息安全系统必须是全方位、综合性的，应由多层次的安全防护层构成一个整体安全框架。通过划分整体安全防御层次，当系统受到入侵时，各安全防御层分级阻止违规行为，实现一体化的安全系统。

34.8.1　设计原则与安全策略

1. 设计原则

信息系统安全体系的设计和实施，应遵从下列原则。

（1）领导负责制原则。信息系统安全工作实行谁主管，谁负责。各级领导务必把信息系统安全列为重要的任务之一，负责加强有关人员的安全意识，配置必要的资源和经费，协调安全管理与各部门工作的关系，抓好信息系统的安全建设，确保安全措施落实、有效。

（2）综合防范原则。以预防为主、综合治理、人员防范与技术防范相结合，逐级建立安全保护体系和责任制，加强制度建设和安全建设，全面加强管理，逐步实现安全工作的科学化、规范化。

（3）动态管理原则。信息系统安全工作要按照系统工程的要求，注意各方面、各层次、各时期的相互协调、匹配和衔接，根据系统环境的变化，以及对系统安全认识的深化，及时复查、修改、调整安全策略。

（4）适度投资原则。信息系统安全管理需要在投资与效益之间加以权衡。安全工作既要充分有效，将系统存在的安全风险造成的危害降低到最小程度；又要适度投资，取得综合最佳的安全效果。

（5）以人为本原则。加强人员的信息安全教育、培训和管理，强化安全意识和法治观念，提升职业道德，掌握安全技术，做好信息安全管理工作。

（6）最小特权原则。为系统资源规定明确的使用权限，对系统的所有人员，按其职责划定必要的最小的授权范围，明确安全责任，通过技术和行政管理措施有效地阻止越权使用行为。

2. 安全策略

安全策略由高级管理部门制订，确保企业的网络系统运行在一种合理的安全状态下。同时，也不妨碍企业员工和用户从事他们正常的工作。安全策略对于企业的网络安全建设起着举足轻重的作用，所有安全建设的后续工作都是围绕安全策略展开的。安全策略的制订是烦琐和复杂的，根据企业的具体需求，可能会包含不同的内容。

信息系统的安全策略从宏观角度反映企业整体的安全思想和观念，作为制订具体策略规划的基础，为其他安全策略标明应该遵循的指导方针。具体的策略可以通过安全标准、安全方针、安全措施来实现。安全策略是基础，安全标准、安全方针、安全措施是安全框架。在安全框架中使用必要的安全组件、安全机制等，提供全面的安全规划和安全架构。

安全标准是强制执行的，它指出了硬件、软件产品应当如何使用。它提供了一种手段来保证企业中应用程序、特定技术等以“规定”的方式执行。安全方针指出了当安全标准中未对不可预料的情形定义时的补充规定。安全措施指出了在操作环境中安全策略、安全标准、安全方针的具体实现步骤。安全标准、安全方针不应该是一个文档，使它们组件化有助于分发和在必要的时候更新。

安全策略中包括了安全框架、安全管理策略、安全技术流程、紧急响应流程、安全评估策略、安全审核策略，以及自身管理人员和用户的安全教育策略。

现代安全体系的建立，是和有效的管理机制无法分离的，单纯的技术手段并不能保障一个系统的安全。而管理体系中，很重要的一个因素是人，内部人员、外部人员、第三方人员，以及外部入侵者等构成了企业信息资产威胁的主要来源，必须有一套良好的管理机制来保障企业系统的安全运作。

由于任何防护手段都无法保障百分之百的安全性，所以在发生安全事件以后，必须有一套紧急响应处理机制。在该机制中明确给出，通过什么途径，由什么人负责，由哪些人参加，按照什么流程，采用什么手段来处理安全事件，同时，也能够保障发生了安全事件以后，将威胁和风险降到最低。

同时，安全策略必须将人的因素考虑进去，技术和管理必须很好地配合。随着信息技术的发展，安全威胁也逐渐增长，新的安全漏洞和威胁也越来越多，对于企业安全管理人员和用户本身的要求也越来越高，只有不断地加强对管理员和用户进行持续的安全教育，才能够有效降低安全风险。当然，企业制订安全策略时应遵守相关的法律条令，有时安全策略的内容和员工的个人隐私相关联，在考虑对信息资产保护的同时，也应该对这方面的内容有一个明确的说明。

34.8.2　安全设计

根据信息安全技术实现上的不同，对应的安全管理可以划分为实物管理、网络管理、主机和系统管理、应用与数据管理四个层次。其中资产管理、人员管理、安全培训和风险管理贯穿整个管理体系，并针对各个层次有着不同的规章制度、培训内容和评估角度。

（1）实物管理。实物管理是指保护计算机设备、设施（含网络），以及其他媒体（如文档、磁盘等）免受非法的实物访问、自然灾害和环境危害（如电磁污染等）的管理措施。涉及环境安全（如物理访问控制、场地安全、交接区域等）、设备安全（如电源保护、设备安置、设备的销毁与处置等）和媒体安全（桌面清理规则、可移动媒体的管理、文档的管理、信息的销毁等）。

（2）网络管理。网络管理是指在网络互联时的安全管理；主要涉及数据传输链路的安全（如线路窃听与干扰等）、网络层的安全（如网络设备安全、网络访问控制、拨号网络安全、网络和链路层数据加密、防火墙应用、病毒防范、入侵检测、安全审计等）、应用层的安全（如身份认证、访问控制、数据保密性和完整性维护、内容审计、记录与抗抵赖等）。

（3）主机与系统管理。主机和系统管理是指通过相关的技术手段和措施，保障系统内部所有相关主机及操作系统、主流应用软件、客户端系统不受恶意攻击和破坏；主要包括操作系统安全（如访问控制、口令管理、用户标识等）、主机系统漏洞检测（如网络扫描、主机扫描、数据库扫描等）和网络病毒防范。

（4）应用与数据管理。应用与数据管理是指对办公自动化系统，以及各种业务应用系统（如电子商务/电子政务平台、CA/PKI 平台、Web 系统、DB 系统等）的安全管理；主要涉及信息加密和完整性、身份认证与授权管理、数据备份与恢复、数据及应用监测。

信息系统安全工程是一项涉及可信产品或者系统整个生命期的安全工程活动，其中包括概念定义、需求分析、设计、开发、集成、安装、运行、维护和终止。系统安全工程过程分为三类：风险过程、工程过程和保证过程。首先，要对威胁、系统脆弱性和事件影响进行分析，并将其引向对系统风险的分析，从而使用安全机制将系统中遗留的风险控制在可接受的范围内。安全工程人员再根据风险分析的结果，以及有关系统需求、可应用的法律法规和方针政策等信息，同客户一起定义和识别系统的安全需求，包括成本、性能、技术风险及使用难易程度等各种因素和各种替代方案，制订解决方案。然后，要保证安全机制配置正确，运行正常，并对系统进行不间断的监测，以控制新风险不致增大到不能接受的地步。最后，要通过对现有系统安全机制正确性和有效性的测试及验证，建立系统安全的证据，保证安全工程的质量。

在组织的信息化过程中，信息需求是组织的激励因素，它给组织带来效益和效率；同时信息安全是需求的保障因素，它虽然从某种意义上来讲并不能提高组织的效率（安全与效率是一对矛盾），但离开安全却是不行的。准确把握信息需求和信息安全的关系，

可保障组织高效和可靠的运作。而在信息安全中，信息安全服务对象的安全需求与信息安全法律法规共同保障了信息安全系统工程的实施。

安全工程包含三类措施：安全技术措施、安全运行措施和安全管理措施。其中安全运行措施包括，网段划分维护、身份鉴别与访问控制、日常入侵监测与安全审计、防病毒跟踪与升级、备份与恢复、应用系统安全、网络中心安全、防火墙维护、日常安全运行计划等多方面的内容。同时组织还需要建立和实施完善的管理制度和方案，包括组织管理、人员管理、技术安全管理、涉密便携机管理、场地设施安全管理等。通过一系列的系统性安全措施，为信息系统提供一套纵深的系统性防御体系。

为了更准确地得出测评结果报表以供选择风险策略和做好安全规划，安全软件应针对不同组织的具体情况，准备各种管理类问询表、技术类检查表并完成调查；同时使用漏洞扫描工具及扫描分析工具检查系统的技术漏洞。通过评测过程进行测评分析，集中分析处理数据，从而减少人为的影响。由国内外现行标准的参照比对，得出的综合性评估结论应考虑技术和管理各方面因素，结论应具有客观性和科学性。

34.8.3　安全工程的实施

在安全体系框架的基础上，考虑实现的安全服务和安全机制，以及要采用的安全技术或安全产品。可能的安全技术为：身份认证技术、数字签名技术、访问授权管理技术、时间戳技术、网络监测技术、隔离技术、阻断技术等。可能的产品为：防火墙、身份认证系统、访问控制系统、VPN 通道、安全监测系统、安全监控系统等。

信息安全工程的实施应该遵从经济、高效与公开、公正、公平的原则。实施方案的选取要严格按照企业统一的安全策略进行审定，建议采用招投标的方式进行。在信息安全工程中，所用到的技术与产品必须经过严格的测试选型，符合企业信息与网络系统安全技术产品的功能规范的要求，符合国家对信息安全方面的法律与规定的要求。

34.8.4　安全工程的监理

工程的实施要实施工程监理制度。安全工程监理主要从工程的规范、流程进度等方面进行监督与检查。安全监理单位或个人必须是第三方中立机构或个人，这样才能保证项目真正按照合理流程与技术标准进行，才能保证工程的招投标过程和项目实施的公正与科学性。

34.8.5　安全教育

安全意识和相关技能的教育是企业安全管理的重要内容，其实施力度将直接关系企业安全策略被理解的程度和被执行的效果。为了保证安全的成功和有效，高级管理部门应当对企业各级管理人员、用户、技术人员进行安全培训。所有的企业人员必须了解并严格执行企业安全策略。在安全教育的具体实施过程中，应该考虑一定的层次性。

（1）主管信息安全工作的高级负责人或各级管理人员，重点应了解、掌握企业信息安全的整体策略及目标、信息安全体系的构成、安全管理部门的建立和管理制度的制订等。

（2）负责信息安全运行管理及维护的技术人员，重点是充分理解信息安全管理策略，掌握安全评估的基本方法，对安全操作和维护技术的合理运用等。

（3）用户的重点是学习各种安全操作流程，了解和掌握与其相关的安全策略，包括自身应该承担的安全职责等。

当然，对于特定的人员要进行特定的安全培训。安全教育应当定期地、持续地进行。在企业中建立安全文化并将其融汇到整个企业文化体系中，才是最根本的解决办法。

34.8.6 安全管理制度

对系统安全的管理不仅仅是购买、部署各种安全产品，而是一个周而复始、螺旋上升的过程。

首先，我们需要利用一些安全工具对具体的系统进行评估，发现系统中每个主要信息资产的弱点与威胁，指出企业现有的安全策略对于确保信息安全是否足够。通过评估，对系统的安全状态和级别有了明确的了解，然后通过部署安全产品、修改现有系统和产品配置等手段对系统进行检测，监视和寻找系统中的可疑活动和入侵企图。同时，修正企业安全策略、修改安全产品的安全规则，对各种已知的威胁进行预防，禁止各种已知的入侵行为。最后，对系统的安全状况进行管理，安装设定的策略管理用户和资产的权限，审计系统的活动，发现新的安全问题。通过审计和管理，可能会发现新的问题。另外，由于 IT 系统的结构变化、应用系统的变化都会导致安全策略的变化。因此，上述过程不是静态的，而是周而复始的过程，该过程在维护系统安全的活动中一直存在。

要对信息网络进行有效的安全管理，必须对系统的使用人员和管理人员的不同角色进行清晰的划分。不同的角色拥有不同的权限和职责，互相制约，共同保障整个系统的安全性。

34.8.7 信息安全管理的国际标准

信息安全作为一个不可避免的问题已经摆在了人们面前。据美国 FBI 统计，美国每年因信息安全问题所造成的经济损失高达 100 多亿美元，且还有日益增加的趋势。追溯原因，发现导致信息安全问题的根源主要有两方面：一是技术，二是管理。也就是说，实现信息安全保障，在研究和发展技术和机制的同时，也要关注安全管理制度的建立、执行和完善。无论多么先进的信息安全技术，都只有在科学的信息安全管理的基础上才能发挥作用。通过技术手段可获得的安全性是有限的，它需要合适的管理和规程给予支持。由此可见，信息安全管理已成为信息安全保障能力的重要基础。

在科学的信息安全管理发展过程中，如果没有标准的、规范化的规程，规模化的信息安全产业就无从谈起。可见，研究国际信息安全管理标准的发展历程和动态趋势，对

指导现阶段我国的信息安全管理体系标准化建设有着重要的意义。

随着信息安全管理重要性地位的日益突出，20 世纪 90 年代后期，ISO 和 IEC 开始研究和制订信息安全管理标准。SC27 是 ISO/IEC 联合技术委员会 JTC1 下设的专门负责信息安全领域国际标准化研究的分技术委员会，它的工作范围和领域是通用的 IT 安全服务和技术的标准化。具体工作内容包括：标识 IT 系统安全服务的一般要求；研究和制订安全技术和机制（包括加密和非加密）；研究和制订安全指南；研究和制订管理支持性文件和标准；研究和制订 IT 系统评估以及 IT 系统、组件和产品认证的准则。

SC27 中的第一工作组 WG1 负责信息安全管理标准研究，负责研究需求、安全服务及指南等内容。工作范围包括：确定应用程序和信息系统的需求，采用相应的技术和机制，研究和制订提供安全服务的相关标准，如鉴别、访问控制、完整性、保密性、管理和审核，以及支撑性解释文档如安全指南、词汇和术语、风险分析等。

经过近十年的需求调研和研究探索，WG1 已经制订了基本涵盖信息安全管理各个领域的标准，这些标准为今后进一步扩展和完善信息安全管理标准奠定了重要的基础。

ISO/IEC 17799：2000 是目前信息安全管理标准中应用最为广泛的一个，来源于英国标准局 BSI 7779 系列标准的第 1 部分，于 2000 年成功转化成 ISO/IEC 标准。该标准从信息安全策略、组织的安全、资产分类和控制、人员安全、物理和环境安全、通信和操作管理、访问控制、系统开发和维护、业务连续性管理和符合性等 10 个方面分别介绍了 36 个信息安全的控制目标及实现这些控制目标的 127 个控制措施。

随着 BS 7799 认证数量在世界范围内的日益增多，很多信息化发达的欧美国家认为，应该从国际上对如何建立信息安全管理体系的问题进行研究，于是 SC27/WG1 于 2002 年启动了信息安全管理体系（ISMS）项目的预研。例如，是否以规划（Plan）、实施（Do）、检查（Check）和持续改进（Act）的 PDCA 过程模型为基础，建立一个包括风险评估、处理和管理、控制措施的选择、风险再评估等题目的 ISMS；调研哪些国际或国家标准可作为 ISMS 标准开发的基础。例如，风险评估标准 ISO/IEC TR13335-3《IT 安全管理指南》CMITS；管理体系标准 ISO 9001：2000、ISO 14000、BS 7799-2：2002、ISO Guide72 和 73；论证 ISMS 的可行性研究报告，并考虑信息安全管理度量机制和测量措施的要求。

2004 年 SC27 全体会议决议通过，以 BS 7799-2：2002 《信息安全管理体系使用指南规范》为基础开发国际 ISMS 标准。国际 ISMS 标准将促进以 PDCA 模型为基础的安全管理过程的应用，并将与信息安全管理实用规则、信息安全风险管理方法学、信息安全管理度量机制和测量措施等一起使用。

从上述标准的分析中可以看出，在目前的信息安全管理国际标准中对同一主题的阐述有所重复。例如，ISO/IEC TR 13335 系列和 ISO/IEC 17799：2000 分别从不同角度说明了如何解决信息安全管理问题，两者都以指导性建议给出了如何实现信息安全管理的框架，虽然思路和出发点各有不同，但同一标准组织中多次出现类似主题的标准可能给用户的使用带来困惑。针对这个问题，国际上启动了信息安全管理标准框架的研究。

34.9 信息系统安全工程

34.9.1 信息系统安全工程概述

信息系统安全工程（Information System Security Engineering ，ISSE）是对信息系统建设中涉及的多种要素，按照系统论的科学方法进行的一种安全工程。随着我国近年对电子政务、电子商务的大力建设，信息安全建设问题越来越突出，如何评价资产？如何分析风险和如何选择安全产品等一系列问题摆在面前。同时人们也越来越认识到，一个中型或大型系统的安全建设不只是安全产品的简单堆叠，而是信息安全保障问题，需要综合考虑系统中存在的人、管理、技术和运行等因素和环节。于是，人们提出要用系统安全工程的思想来解决安全问题。

系统安全工程是一个非常复杂的过程，技术性和政策性都非常强。按照信息安全工程的思想来保证信息系统的安全，就要从安全体系的构成、安全基线的划分、安全风险的评估、安全策略的制订、安全工程的实施，以及安全系统管理等方面入手来解决各种问题。在这种情况下，需要有规范的方法和标准来指导系统安全的整个开发过程，于是引发了系统安全工程这一新兴学科的蓬勃发展。对信息安全的建设必须在ISSE的理论基础上实施人们已经形成了共识，但是在一个具体的安全工程中，如何应用ISSE却是一个比较大的难题。这是因为ISSE只是从系统论的角度指明了一个框架和范围，而实施的细节却依赖于已有的经验和积累。ISSE 规定了在五个阶段中应该达到的目的，也就是输入输出关系，并没有规定具体的工具和方法。比如，在需求分析阶段，如何选择一种合理的风险分析方法就是个难题。可见，与其说ISSE是一种方法，不如说是一种理念。

ISSE 是 IATF 中的一个重要组成部分。IATF 是由美国政府和工业界联合提出的信息保障技术框架。它全面地概括了与信息系统安全问题相关的所有方面，包括：系统工程、骨干网、本地计算环境、边界连接和支持系统等。ISSE 为 IATF 框架的其他部分提供了工程实现保障，是整个框架得以正确、完整实施的基础。

作为一种系统工程技术，ISSE 不仅可以用来设计、实现独立的软硬件系统，还可以为集成的计算机系统的设计和重构提供服务。它可以与设计者和工程人员提供的设计要素，以及面向开发者、管理者、用户的接口相结合，在投资额度的限制下，使整体系统获得最大的安全性能。

ISSE 的工作范围包括：寻找与安全有关的设计要素，进行安全系统的预设计，设计安全系统规范，辅助详细设计，检查详细设计文档，评估方案与安全规范的一致性，推荐满足安全条件的部件，检查系统安装、设置的疏漏，以及性能测试等。

IATF 从工程实践的角度，对系统工程和信息系统安全工程（ISSE）过程给予描述，认为 ISSE 过程是系统工程过程的扩展，它们都拥有共同的阶段：发掘需求、系统功能定义、系统设计、系统实现、系统有效性评估。另外，IATF 还解释了其他与 ISSE 有关

的过程，如系统采购、风险管理、认证和认可、生命周期支持。IATF 对使用通用准则（CC）支持 ISSE 过程也提供了建议。以信息系统安全工程为基础，可确保安全解决方案的有效性。

ISSE 是系统工程（Systems Engineering）中的一部分。它分为发掘信息保护需求、定义信息保护系统、设计信息保护系统和实施信息保护系统四个阶段。

1. 系统工程

通常系统工程包括发掘业务需求、定义系统功能、系统分析、系统设计和有效性评估五个过程。

系统工程过程原理将问题与解决方案加以区分。问题代表限制、风险、政策和其他解决问题的局限性。解决方案代表要完成的活动和需要建造的用以满足用户需求的产品。但需要一个评估体系来评估解决方案是否可以解决存在的问题，而这些评估又是对问题和解决方案做出必要修正的基础。

2. ISSE 过程

发掘信息保护需求：ISSE 过程开始于对用户的任务需求，相关政策、规定和标准，以及用户环境中的信息系统威胁进行调查。ISSE 随后确定信息系统和信息的用户与其他信息系统和信息进行交互的状态，以及在信息保护系统生命期的每个阶段，他们的角色、职责和授权。信息保护需求来自用户，而不会过度受信息设计或实施的限制。

定义信息保护系统：在定义信息保护系统时，用户对信息保护的需求和信息系统环境的说明被转换成目标、要求和功能，信息保护系统的内/外部接口也得到定义；内容包括信息保护目标、系统内部联系和环境、信息保护要求和功能分析。

设计信息保护系统：在设计信息保护系统时，ISSE 将进行功能分配，构造系统的结构，确定详细的设计方案。

实施信息保护系统：实施信息保护系统的目标是建立、采购、集成、核实和验证信息保护的子系统，具体包括采购、建设和测试三个阶段。

有效性评估：有效性评估的焦点是信息保护系统的有效性。ISSE 强调系统对其所处理的信息必须提供适当级别的保密性、完整性、可用性和抗抵赖能力，否则任务的成功就面临危险。有效性评估将涉及互操作性、可用性、培训、人-机界面和代价等。

3. ISSE 过程与其他过程的关系

（1）系统获取过程：系统获取过程与系统工程及 ISSE 过程并行发生。系统获取阶段包括：需求定义阶段、概念发掘阶段、工程实施阶段生产和运行支持阶段。ISSE 需要明白任务需求、任务环境、政策限制，以及系统信息保护需求。要对已得到的信息及特定的时间、成本、技术和风险估计进行判断，以确保每一个信息保护子系统都是满足要求的。

（2）风险管理：风险管理从初始的系统开发开始应用，贯穿开发和获取过程的始终。一旦系统开始建设，风险管理过程需调整与相应系统设计和配置的变化、操作环境

的变化，以及支持任务的变化。这些因素在开发、采购和安装的过程中随时间而变化时，还要定期地对风险进行考虑。

风险管理是一个循环的过程，始于对任务和信息保护目标和需求的理解，体现任务当前的风险状态，体现可能的完成任务的阻碍。ISSE 的目的就是要采取一些措施减轻风险。对于特定的用户系统，通常不可能靠实施一套技术或非技术的对策来完全使用户满意。任务的性质也许对操作能力和功能要求与对降低风险的要求正好相反。由此可见，应当使用风险管理方法决定是否需实施一套信息保护系统。风险管理要完成的任务是理解任务目标、理解信息保护需求、描述风险特征、描述什么可以做、决定做什么和执行决策。

（3）生命期支持：系统生命期通常包括概念和需求定义、系统功能设计、系统开发和获取、系统实现和测试、系统维护操作支持，以及最终的系统处理几个阶段。

经验告诉我们，一旦系统开发完成后，就难以改变安全解决方案。由此可以看出，当发掘需求和定义系统时，一定要考虑安全需求。为有效地将安全措施和控制集成进系统工程过程，设计人员和开发人员需要修正原有的过程模式，以形成一个可重复的系统开发生命期，并集中在安全控制和保护机制上。

生命周期支持活动包括：建立生命期管理计划、建立系统工程管理计划、建立配置控制程序、建立安全计划、建立维护计划、建立意外事故和持续操作计划、建立系统处理计划。

（4）认证和认可：认证和认可定义为对技术性和非技术性安全特性的综合评估。通过建立准则，使得特定的设计和实施符合一系列特定的安全要求，并且由 DAA 宣布，只允许系统在可接受的风险程度内运行。

初始的认证任务包括：系统结构分析、软件设计分析、网络连接规则一致性分析、集成产品的完整性分析和生命周期管理分析与脆弱性评估。

最终的认证任务包括：安全测试和评估、渗透性测试、TEMPEST 和 Red-Black 验证、COMSEC 符合性确认、系统管理分析、站点认可调查、意外事故计划评估、基于风险的管理检查。

34.9.2 基于能力成熟度模型（SSE-CMM）的方法

1. 基于能力成熟度模型的开发思想

过去人们在开发安全产品过程中往往只重视产品本身的标准化问题，却忽视了开发过程本身的标准化。如何提高开发过程的能力，如何能使过程本身标准化、规范化，引起了人们的重视。目前大部分产品开发采取的组织形式是矩阵式的管理模式，即平时按一般组织形式管理，一旦有项目就由组织各部门人员组成项目小组。项目的成败是由小组成员的能力决定的，这是一种基于个人能力的组织管理模式。这种管理模式的不足之处在于，一旦项目组的主要成员中途离开就可能造成整个项目拖延甚至使项目停止运

作。整个项目的运行过程对于开发商来说近乎黑箱运作。当这个项目成功后，开发商难以让其他成员共享他们的经验，因为开发过程主要靠人的思维活动，而人的思维是不断变化的，即使同一个人两次开发同一个项目，也会有所不同。为了改变这种状况，一个不同于以往的概念逐渐被接受，即一个单位的开发和生产能力取决于该单位的过程能力。这种过程能力是整体的能力而不是个人的能力。要建立一个规范的过程并通过政策保证过程的执行，从而使项目的执行不再是一个黑箱子，项目管理者可以清楚地知道项目是按规定的过程进行的。其中所设定的过程可能有缺陷，但存在的问题可以在执行的过程中反映出来，在该过程执行一段时间后，可根据反映出来的问题不断完善这个过程。周而复始就能使这个过程逐渐完善和成熟。伴随着过程的成熟，开发商的能力也不断成熟。

2．SSE-CMM 模型的提出

基于上述的思想，美国国家安全局（NSA）于 1993 年 4 月提出了一个专门应用于系统安全工程的能力成熟度模型的构想。在美国国家安全局、美国国防部、加拿大通信安全局的号召和推动下，汇聚了 60 多个厂家，集中了大量的人力、物力和财力对该构想进行了开发实施，并于 1996 年 10 月出版了系统安全工程能力成熟度模型（SSE，CMM，Systems Security Engineering Capability Maturity Model）的第一个版本。第一个版本发布后，标准制订者随即选择了 5 家公司对该模型进行了长达一年的试用，并根据试用中积累的经验和教训对模型进行了几次更新，并于 1997 年 4 月出版了评定方法的第一个版本，1999 年 4 月发布了 SSE-CMM 的 2.0 版本。目前，该模型已经提交国际标准化组织申请作为国际标准。

3．SSE-CMM 的基本思想

SSE-CMM 的基本思想是建立和完善一套成熟的、可度量的安全工程过程。该模型定义了一个安全工程过程应有的特征，这些特征是完善安全工程的根本保证。这个安全工程对于任何工程活动均是清晰定义的、可管理的、可测量的、可控制的，并且是有效的。SSE-CMM 及其评定方法汇集了业界范围内常见的实施方法，提供了一套包括政府及产业的标准度量体系，确保了在处理硬件、软件、系统和组织安全问题的工程实施活动后，能够得到一个完整意义上的安全结果。在以下安全活动过程中，SSE-CMM 已成为公认的标准规范。这些活动包括：

（1）整个工程的生命周期过程，包括开发、运行、维护和结束。

（2）整个组织过程，包括各种管理、组织和工程活动。

（3）与其他工程规范和标准的交流，包括其他系统、软件、硬件、人的因素和检测工程规范等。

（4）与其他组织的交流活动，包括信息获取、系统管理、认证、授权和评价等活动。

此外，SSE-CMM 还用于改进安全工程实施的现状，以达到提高安全系统、安全产品和安全工程服务的质量和可用性，并降低成本的目的。

34.9.3　SSE-CMM体系结构

1. SSE-CMM中包含的过程域

为了将安全工程思想变为一种有效的工程规范，在SSE-CMM模型中，定义了22个安全方面的过程域PA（Process Areas），并将每个过程域按其能力由低到高分为0～5共6个级别，在每个过程域中提出了要控制和达到的目标。为了实现这些目标，在每个过程域中又包括许多具体的基本实施BP（Basic Practice）。这些基本实施规范了工作流程，是保证过程目标有效控制的重要手段。按照解决问题的不同，过程域可以分为三类：一类是工程过程域（PA），包括11个过程；一类是项目过程域（PA），包括5个过程；还有一类是组织过程域（PA），包括6个过程。

工程过程域中包括的主要内容如表34-3所示。在项目过程域中包括5个过程，它们分别为：PA12——质量保证，PA13——配置管理，PA14——项目风险管理，PA15——技术成果的监控，PA16——技术成果的计划。在组织过程域中包括6个过程，它们分别为：PA17——定义与组织系统工程过程，PA18——提高组织系统工程过程，PA19——产品线进展管理，PA20——系统安全工程支持环境管理，PA21——提供在研的技术和知识，PA22——与供应商协调。这两类过程域虽然并不直接同系统安全相关，但它们通过和安全过程域的协调来保证安全工程的实施。

表34-3　SSE-CMM工程过程域内容表

有关项目 / 过程域标号	过程域名称	过程域目标	过程域描述	基本实施个数
PA01	安全机制控制	正确使用和设定安全控制机制	将系统应有的安全功能综合到设计过程中	包括4个BP
PA02	影响评估	识别和描述出系统安全的影响因素	评估影响的可能性，包括有形和无形的损失	包括6个BP
PA03	安全风险评估	达到对风险的正确理解，并对风险因素进行优先级排序	确认和评估风险发生的可能性，其中风险来自威胁、脆弱性和影响	包括6个BP
PA04	威胁评估	确定出对系统安全的威胁因素	找出威胁的特点和性质	包括6个BP
PA05	脆弱性评估	正确理解在一定环境下的系统脆弱性	进行系统分析，找出系统的具体脆弱性并对其进行整体评估	包括5个BP
PA06	安全证据建立	提供满足客户安全需求的证据	安全证据是一系列安全保证目标的组合	包括5个BP
PA07	安全协调	所有的成员都要加入到安全工程中，与安全有关的决策要及时交流和沟通	安全活动不能孤立地进行，必须使各方通过有效的手段进行协调	包括4个BP

续表

有关项目 / 过程域标号	过程域名称	过程域目标	过程域描述	基本实施个数
PA08	安全势态监视	与安全有关的内外事件都要检测出来，根据安全需要改变安全状况	保证系统可能存在的威胁安全的缺陷和错误都被检测和报告出来	包括 7 个 BP
PA09	提供安全输入	所有的问题都要从安全的角度来考察，确定安全输入方案	为系统结构、设计者、执行者和用户提供安全信息	包括 6 个 BP
PA10	确定安全需求	使包括客户在内的各方取得安全方面的共识	将安全需求具体化，为了满足政策、法律和标准等而确定基本需求	包括 7 个 BP
PA11	安全测试与验证	使方案满足系统安全需求和客户操作安全需求	通过对安全需求和体系结构及设计方法的分析、论证和审核来证实和确认安全	包括 5 个 BP

2. SSE-CMM 系统安全工程

在工程进行中可以根据不同的目标确定采用不同的过程域，通过提高过程的能力来保证系统、产品或服务的安全性。SSE-CMM 将系统安全工程分为三类，它们是风险过程、安全过程和信任度过程。其中，风险过程是指对要实施安全工程的系统进行风险分析，分析各种可能对系统构成威胁的影响因素、系统本身的脆弱性，以及如果威胁因素起作用可能对系统造成的影响。工程过程是指工程队伍根据风险分析的结果、有关系统需求、可应用的法律法规和方针政策等信息，同客户一起识别和定义系统的安全需要，在综合考虑包括成本、性能、技术风险和使用难易程度等各种因素和各种替代方案之后创建出解决方案，然后用该方案指导安全系统的开发和建设，并对系统进行不间断的监测，以保证风险不至于增大到不能接受的程度。信任度过程是指对安全工程过程和质量结果进行测试和验证，从而得出系统安全是否可信的结果。随着这三个过程的不断执行，工程队伍的过程能力也不断成熟。

34.9.4　SSE-CMM 的过程能力水平

过程能力由一组通用实施（GP）来衡量，通用实施是对所有工程过程都通用的工程实践。按照工程队伍对通用实施的执行情况，可以将每个过程域按能力的高低分成 6 个级别，即从第 0 级到第 5 级。

0 级能力水平指非执行能力级。非执行能力级的过程没有共同特征（CF）和通用实践（GP），在开发过程中没有安全工程思想的应用。在这一级的过程水平中也能够完成一些工作，但是当工程队伍中的关键人物不在或者当工程本身变得越来越复杂时，就难以保证任务的完成。

1 级能力水平指非正常执行的能力水平。所有的基本实施在一定程度上都能被执

行，然而对过程能力缺少连续的计划和跟踪。过程的完善能力仍然取决于个人的知识和努力程度。产品质量和生产效率由工程队伍的所有人员的出色工作来保证。由于过程的执行还主要靠经验，对执行结果无明确要求，所以执行活动的能力是不可重复和被其他过程所借鉴的。

2 级能力水平指具有计划与跟踪的能力水平。由于组织的过程能力取决于安全工程基本实施的效率，因此与基本实施有关的工作过程可以被总结和控制。它与 1 级能力水平不同之处在于，此过程中的基本实施是可以重复和被其他组织借鉴的。

3 级能力水平指完好定义的能力级水平。过程中的所有基本实施应按照完善定义的规范来进行，这些规范是工程队伍根据长期经验总结出来的。它与 2 级能力水平不同之处在于定义了一个被接受的标准规范，基本的实施可以反映出过程的特征，过程的能力可以直接转到其他工程活动中。

4 级能力水平指定量控制级水平。对每个已定义的过程和相联系的工作都设定了可度量的过程目标，可以对工程队伍和工程的进展进行定量的预测和控制。

5 级能力水平指持续完善的能力水平。从过程能力的角度看它是最高水平，在此水平下已经建立了对过程效率的定性和定量的目标，而且可以准确度量过程持续改善所获得的效益。

具体实施安全工程的工程队伍的能力直接影响安全工程本身的质量和安全可靠程度。SSE-CMM 模型通过以上的“过程能力”指标对工程队伍的能力进行评估。“过程能力”是通过执行工程过程所得质量结果的变化范围。所得结果的质量变化范围越小，表明执行该过程的队伍越“成熟”，反之亦然。一个工程队伍既可以通过该模型自我评估能力级别，也可以通过第三方来实施评定。

通过以上介绍可以看出，SSE-CMM 模型是目前针对信息系统安全问题而提供的具有较高可靠性的解决方法。它既可用于对一个安全系统或安全产品的信任度测量和改善，也可用于对一个工程队伍的能力进行评定或自我改善，提高系统安全工程队伍自身的能力，从而最大限度地保证系统的相对安全性。

34.9.5　SSE-CMM 的应用

SSE-CMM 模型本身并不是安全技术模型，但它给出了信息系统安全工程需考虑的关键过程域，可指导安全工程从单一的安全设备配置转向系统地解决整个工程的风险评估、安全策略形成、安全方案提出、实施和生存周期控制等问题。

SSE-CMM 可应用于以下几个主要方面：

（1）评估组用来评估一个企业在安全工程过程方面的能力和弱点，指导企业一个等级接一个等级地去提高它们的安全工程过程能力水平。

（2）评估组用来评估安全工程发包方在选择承包商和管理合同时，由于选择不同承包商所造成的风险。

（3）项目管理者和参加者用来制订和实施组织的过程改进计划时，判断什么是必需的。

（4）安全工程过程组织用来指导他们制订和改进安全工程的行为。

执行具体项目时，首先根据风险过程进行风险分析和评估，实施队伍必须根据风险分析的结果和有关系统要求，同客户一起定义系统的保护框架（PP，Protection Profile）和安全目标（ST，Security Target），这也是 PA10 过程。一般由用户定义系统的 PP，详细说明其系统的保护需求。而工程队伍依据 PP 文件制订系统的 ST，阐述系统安全功能及信任度并与用户的保护框架相对比，以证明该系统满足用户的需要。安全目标 ST 必须用具体语言和有力的论据来说明保护框架 PP 中的抽象描述怎样逐条地在所评价的系统中得到满足。在综合考虑包括成本、性能，以及使用难易程度等各种因素和各种替代方案之后，问题的解决方案得以创建出来（PA09 过程）。同时产生一个可用于过程管理的安全基线，并尽量提高其精确度。安全基线是一个系统至少需要满足的安全目标。安全基线的实施是模型的 PA01 过程的工程化途径。此外，还必须通过基线库状况对系统进行不间断的监控，以保证新风险不至于增大到不能接受的程度（PA08 过程）。最后对实施结果进行评定（PA11 过程），确认它的安全信任度（PA06 过程）。

34.9.6　SSE-CMM 的应用前景

目前，SSE-CMM 已经成为西方发达国家政府、军队和要害部门组织和实施系统安全工程的通用方法，是系统安全工程领域里的成熟方法体系，在理论研究和具体实践中具有举足轻重的作用。SSE-CMM 已经被信息技术安全评估国际标准的公共准则 CC 看成是最有希望采用的替代安全技术。在模型的应用方面，Texas Instruments 公司和参与规范制订的一些公司采用该模型指导安全工程活动与传统方法相比，可以在提高过程能力的同时有效地降低成本，从而在开发方法上保证信息系统的安全。

在国内，SSE-CMM 的研究与实施工作正处于起步阶段，国家及军队信息安全测评认证中心已经将系统安全工程能力需求模型作为我国安全产品和信息系统安全性检测和认证的标准之一，目前已经发布了标准草案，少数部门的信息系统正在实施基于该标准的系统安全工程。其中 SSE-CMM 在中国工程技术信息网中得到了成功应用。由于 SSE-CMM 模型本身并不是安全技术模型，它提供的是信息系统安全工程需要考虑的关键过程域，所以，这些过程域可指导信息系统安全工程从单一的安全设备安装转向系统地解决安全工程的管理、组织、设计、实施和验证等问题。但在具体应用方面，该模型缺乏工程化，可操作性差，尤其在我国对于信息系统安全工程的研究并不很成熟，而信息系统安全工程又具有重要的现实意义、特殊性和迫切性。随着我国国防、政府、企业、社会信息化程度的急剧提高，信息系统安全问题对我们的挑战将越来越严峻，对 SSE CMM 做分析与评价，并结合我国实际情况进行改进和完善，对其进行工程化、实用化研究，对指导我国信息系统安全工程的发展，具有十分重要的意义。基于上述分析可以看出，对于 SSE-CMM 模型的开发和应用在我国有着广阔的发展前景。

34.9.7　ISSE 方法概述

NSA 在开发 ISSE 过程中使用了 SSE-CMM 模型，帮助 ISSE 用户确认合格的 ISSE 服务提供商，并提高通信过程的服务质量。ISSE 包括如下的几个过程。

1. 发掘信息系统安全需求

该部分是信息系统建设的前导，涉及以下的工作内容。

① 分析组织的任务。
② 确定信息和任务的关系，以及重要性。
③ 界定法律和法规的要求。
④ 界定威胁的类别。
⑤ 确定影响。
⑥ 界定安全服务。
⑦ 形成信息保护文件。
⑧ 形成安全管理角色和责任的文件。
⑨ 界定设计限制。
⑩ 评估信息保护的有效性。该项包括如下几个方面。

- 为客户提供/介绍信息保护文件；
- 与客户合作完成信息保护需求；
- 支持系统认证/认可（C/A）；
- 指定满意的权威机构/认可者；
- 界定认证当局/认可者；
- 界定客户的认证/认可和获取过程；
- 保证认证/认可者在信息保护方面的合作。

2. 确定系统安全要求

- 开发系统安全的相互关系；
- 确定系统边界和与安全工程（SE）的界面；
- 形成目标系统和外部系统安全分配的文件；
- 界定目标系统和外部系统之间的数据流和与这些数据流有关的保护需求；
- 开发运行的安全概念；
- 开发系统安全要求基线；
- 确定系统安全要求；
- 确定系统运行安全模式；
- 确定系统安全性能度量方法；
- 评审设计约束；
- 评估信息保护的有效性；

- 为客户提供/介绍安全关系、安全运行概念和系统安全要求；
- 在系统安全关系、安全运行概念和安全要求诸方面得到客户的合作；
- 支持认证/认可；
- 保证在系统安全关系、安全运行概念和系统安全要求诸方面得到认证/认可者的合作。

3. 设计系统安全体系

- 实现功能分析和分配；
- 分析备选系统体系结构；
- 把安全服务分配给体系结构；
- 选择机制类型；
- 提供评估用的安全体系结构；
- 修正安全体系结构；
- 选择最终安全体系结构；
- 评估信息保护的有效性；
- 保证所选择的安全机制能够提供所要求的安全服务；
- 向客户说明安全体系结构是如何满足安全要求的；
- 产生风险预测；
- 得到客户的合作；
- 支持认证/认可；
- 准备送交风险分析的最终体系结构文件；
- 与认证/认可者同时提出风险分析结果。

4. 详细安全设计

- 保证遵从安全体系结构；
- 实现折中研究；
- 确定系统安全设计要素；
- 把安全机制分配给安全要素；
- 界定商业产品现货（COTS）和政府产品现货（GOTS）；
- 界定定制的安全产品；
- 限定安全设计要素和系统内外接口；
- 向客户说明安全设计是如何满足安全要求的；
- 以文件的形式向客户说明设计的剩余风险；
- 得到客户的合作；
- 支持系统认证/认可；
- 准备和递交风险分析的详细设计文件；
- 与认证/认可者同时展示风险分析结果。

5. 实现系统

- 支持安全实现和集成；
- 参与实现规划；
- 鉴别安全工具和机制的互操作性；
- 核实是否已经按安全设计实现；
- 核实安全产品/组件已经用所选择的评估标准评估；
- 参与组件的集成并保证它们的集成在满足系统安全规范的同时不改变组件的规范；
- 参与组件的配置，保证必要的安全特性，以及安全参数能正确配置以便提供所要求的安全服务；
- 保证形成系统和组件的配置文件，并由配置管理控制；
- 支持测试和评估；
- 建立测试和评估战略（演示、观测、分析和测试）；
- 鉴别测试和评估数据的可用性；
- 支持测试和评估程序的开发；
- 支持测试和评估活动；
- 评估信息保护的有效性；
- 监控安全设计的正确实现；
- 确定风险和可能的任务影响并提出忠告；
- 支持认证/认可；
- 保证客户和客户的认证/认可者能得到完整的认证/认可文件；
- 支持安全培训。

6. 评估系统

本部分需要对前面几个部分进行有效性评估，一般由建立方组织完成。

34.9.8 ISSE体系结构

ISSE的体系结构是一个顺序结构（如图34-6所示），前一项的结果是后一项的输入，具有严格的顺序性，违背这种顺序性将导致系统建设的盲目性，最终导致一系列“豆腐渣”工程。发掘需求是至关重要的环节，甚至可以说是根本性的环节，其影响因素也很多，决定需求的因素很多，如图34-7所示，需要在用户代表的参与下仔细评判上述决定因素，并合理地排序。

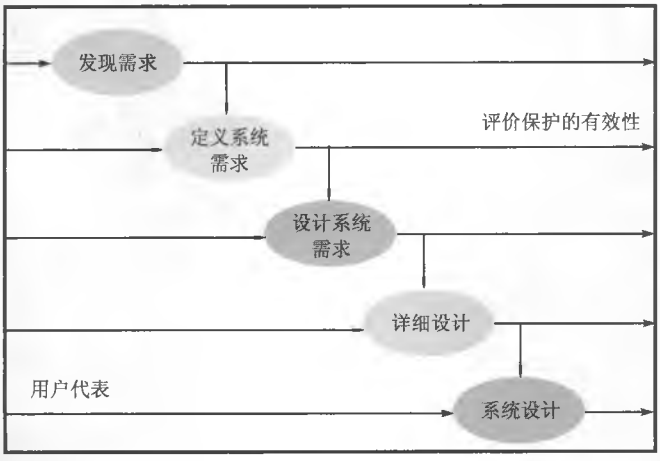

图 34-6　ISSE 体系结构图

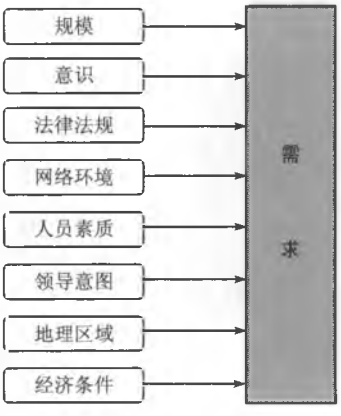

图 34-7　需求因素图

安全需求分析的第一步是获得系统中的资产价值并获得资产的排序。第二步是分析系统面临的各种风险。将风险对资产的威胁进行某种组合分析。一般情况下会形成一个二维的矩阵，在此二维矩阵中可以抽取出值得保护的资产，并进行排序，根据情况的轻重缓急制订出系统的保护策略。在上述风险分析过程中，由于涉及对信息资产的评估，而我们知道，影响信息资产的因素也很多，比如一个笔记本，在裸机时的价值和安装了操作系统的价值不一样；硬盘放置数据对不同人又有不同的价值诱惑力，有些硬盘资源具有时效特征，如预算信息在被审批以前具有相当大的价值，需重点保护。一旦审批完毕就可以公开，其资产价值降为一般。因此，信息资产不仅仅是信息衍生所花费的函数，而且是时间、场合、不同人的函数，这些函数往往是非线性的，各种因素的耦合也是千差万别，目前还没有一个很好的模型能够对此进行很好的表征。由此可见，即使是最好的风险分析家也不一定会得出一个令所有人满意的方案。目前有关风险分析的方法不下 20 多种，主要分为定性和定量两大类方法。

在需求分析基础上是定义系统安全要求。信息安全的基本要求包括机密性、完整性、不可否认性、可用性、可审查性等，需要在上述风险分析的基础上确定系统具体的安全要求。

设计系统体系是核心的环节，是信息安全保障体系思想的集中体现。目前在安全领域中，存在两大保障体系理念，一种是以欧洲为代表的信息安全管理系统（ISMS）的思想，该思想以风险管理为手段和目的；另一种以美国的信息保障体系（IATF）为代表，以纵深防御体系设计作为安全理念的核心。我国目前广泛采用后一种安全理念，其纵深防御体系表现在两个方面，一个是以管理、技术和运行三位一体的纵深防御，另一个纵深是技术层面的纵深，从网络基础设施、边界保护、计算环境保护到应用环境保护的纵深防御。

详细设计的关键是对安全设备和产品的部署。需要在信息保障体系所制订的框架和范围基础上实施具体的产品和技术，以及制订相关的人员措施和运行措施，其中应急响应机制是目前备受关注的技术措施。

系统实施过程需要按照详细设计的内容分阶段、分节点、分步骤地进行设施。

在上述的五个阶段中，均需要用户进行参与，同时要对每一个阶段的有效性进行评估，最终形成一个循环改进的过程。

综上所述，ISSE从系统工程开始，全程地参与了系统的调研、设计、实施和维护，能够对系统提供全方位的安全保护。中间任何环节的疏漏都有可能为最终系统留下安全隐患。信息系统安全工程在国内尚未得到足够的重视，在实际操作的过程中，通常很难保证上述的ISSE流程能够完整地得到实施。实践证明，ISSE是一种十分有效的工程方法，对信息安全系统的建设具有独到的指导意义，是值得我们学习和重视的。