第3章　信息系统安全工程

本章学习目标：

- 了解信息系统安全工程基本概念。
- 了解信息系统安全工程过程。
- 掌握如何基于信息系统安全工程方法开展系统安全工程建设。

3.1　概　　述

信息安全保障问题的解决既不能只依靠纯粹的技术，也不能只靠简单的安全产品的堆砌，它要依赖于复杂的系统工程，即信息安全工程。本章主要介绍由系统工程发展而来，以时间维划定工程元素的方法学——信息系统安全工程。

3.1.1　信息系统安全工程的定义

1993年，美国国家安全局制定的《信息系统安全工程手册》中提出了“信息系统安全工程”(Information Systems Security Engineering，ISSE)的概念，并将其定义为“侧重于信息安全的应用系统工程”。美国国家安全局2000年制定的《国家信息系统安全术语表》(NSTISSI No. 4009)中，将ISSE描述为“在信息系统生命周期过程中为实现和维护系统最优的安全性和持续性所做的各种努力”。现在对ISSE的普遍解释为：“信息系统安全工程是采用工程的概念、原理、技术和方法，来研究、开发、实施与维护信息系统安全的过程，是将经过时间考验证明是正确的工程实践流程、管理技术和当前能够得到的最好的技术方法相结合的过程”。

信息系统安全工程是系统工程在安全空间的映射，它的重点是通过实施系统工程过程来满足信息保护的需求，信息系统安全工程将有助于开发可满足用户信息保护需求的系统产品和过程解决方案，信息系统安全工程的主要目标包括以下6个方面。

(1) 获得对企业安全风险的理解。

(2) 根据已识别的安全风险建立一组平衡的安全需求。

(3) 将安全需求转换成安全的策略，成为信息系统建设基本原则，并落实到项目实施中的各个科目活动、系统配置或运行的定义中。

(4) 通过正确有效的安全机制建立抵御安全威胁和系统正常运营的保证。

(5) 动态监测和判断系统中和系统运行时出现的安全隐患和突发事件，并及时按预先指定的方案，启动紧急事故处理程序进行处理和追踪，遏制危险的发生和蔓延，使系统免除

损失或控制在可控制范围之内。

(6) 将所有科目和专业活动集成为一个具有共识的系统安全可信性工程。

3.1.2 信息系统安全工程与系统工程的关系

系统工程是信息系统安全工程的基础,通常系统工程可以分为发掘需求、定义系统、设计系统和实施系统 4 个阶段,在这 4 个阶段的执行过程中还需要有阶段性评估。信息系统安全工程是系统工程的一部分,是系统工程的基本原理在信息安全领域内的具体应用,它也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 4 个阶段,每个阶段还可以进一步细分,在这 4 个阶段的执行过程中同样还必须有阶段性评估,以保证执行效果。

具体来说,一个信息系统安全工程包括发掘信息保护需求、定义信息保护系统、设计信息保护系统、实施信息保护需求以及评估信息保护系统几个步骤。信息系统安全工程(ISSE)与系统工程(SE)的对应关系如图 3-1 所示。

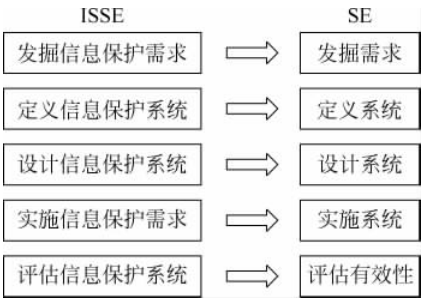

图 3-1 信息系统安全工程与系统工程的对应关系

对系统而言,ISSE 过程和 SE 过程要同步考虑:即在相应的阶段同时考虑信息保护的目标、需求、功能、体系结构、设计、测试与实施,使得信息保护得以优化。它们的具体区别如表 3-1 所示。

表 3-1 SE 过程与 ISSE 过程的区别

SE 过程	ISSE 过程
发掘需求	发掘信息保护需求
系统工程师要帮助客户理解并记录用来支持其业务或使命的信息管理的需求,信息需求说明可以在信息管理模型(Information Management Model,IMM)中记录	信息系统安全工程师要帮助客户理解用来支持其业务或使命的信息保护的需求。信息保护需求说明可以在信息保护策略(Information Protection Policy,IPP)中记录
定义系统	定义信息保护系统
系统工程师要向系统中分配已经确定的需求。应标识出系统的环境,并说明系统功能对该环境的分配。要写出概要性的系统运行概念(Concept of Operations,CONOPS),描述待建系统的运行情况。要建立起系统的基线要求	信息系统安全工程师要将信息保护需求分配到系统中。系统安全的背景环境、概要性的系统安全 CONOPS 以及基线安全要求均应得到确定

续表

SE 过程	ISSE 过程
设计系统	设计信息保护系统
(1) 设计系统体系结构 系统工程师应该分析待建系统的体系结构，完成功能的分析和分配，同时分配系统的要求，并选择相关机制。系统工程师还应确定系统中的组件或要素，将功能分配给这些要素，并描述这些要素间的关系。 (2) 开展详细设计 系统工程师应分析系统的设计约束和均衡取舍，完成详细的系统设计，并考虑生命周期的支持。系统工程师应将所有的系统要求跟踪至系统组件，直至无一遗漏。最终的详细设计结果应反映出组件和接口规范，为系统实现时的采办工作提供充分的信息	(1) 设计系统安全体系结构 信息系统安全工程师要与系统工程师合作，一起分析待建系统的体系结构，完成功能的分析和分配，同时分配安全服务，并选择安全机制。信息系统安全工程师还应确定安全系统的组件或要素，将安全功能分配给这些要素，并描述这些要素间的关系。 (2) 开展详细的安全设计 信息系统安全工程师应分析设计约束和均衡取舍，完成详细的系统和安全设计，并考虑生命周期的支持。信息系统安全工程师应将所有的系统安全要求跟踪至系统组件，直至无一遗漏。最终的详细安全设计结果应反映出组件和接口规范，为系统实现时的采办工作提供充分的信息
实施系统	实施信息保护需求
系统工程师将系统从规范变为现实，该阶段的主要活动包括采办、集成、配置、测试、记录和培训。系统的各组件要接受测试和评估，以确保它们能够满足规范。成功的测试之后，各组件——硬件、软件、固件要进行集成和正确的配置，并作为一个系统接受整体测试	信息系统安全工程师要参与到对所有的系统问题进行的多学科检查之中，并向 C&A 过程活动提供输入，例如检验系统是否已经针对先前的威胁评估结果实施了保护；跟踪系统实现和测试活动中的信息保护保障机制；向系统的生命周期支持计划、运行流程以及维护培训材料提供输入
评估有效性	评估信息保护系统
各项活动的结果要接受评估，以确保系统能够满足用户的需求，系统在一个预期环境中实现了期望的功能，并达到了一个需要的质量标准。系统工程师要检查系统对任务需求的满足程度	信息系统安全工程师要关注信息保护的有效性——系统是否能够为其使命所需的信息提供保密性、完整性、可用性、认证和不可否认性

3.2　信息系统安全工程过程

3.2.1　发掘信息保护需求

ISSE 的过程始于审视用户的任务需求、相关政策、规定、标准以及用户环境中的信息系统威胁。ISSE 随后要确定信息系统和信息的用户是谁、与其他信息系统和信息进行交互的状态如何，以及在信息保障系统生命周期的每个阶段，它们的角色、职责和授权是什么。信息保障需求应当来自用户的观点，而不应过度受限于信息设计或实施的限制。

发掘信息保护需求要考虑以下方面。

(1) 考虑对所要完成任务的信息保护需求。

(2) 掌握对信息系统的威胁。

(3) 考虑信息保障政策。

发掘信息保障需求过程和主体如图 3-2 所示。

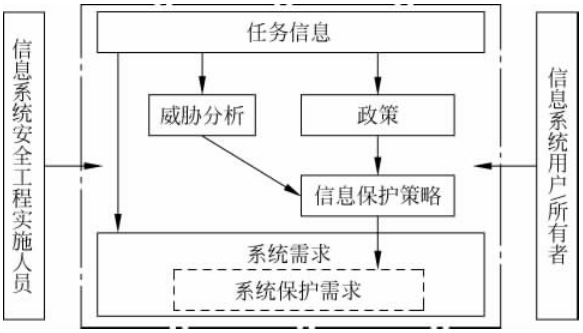

图 3-2 发掘信息保障需求过程和主体

1. 考虑对所要完成任务的信息保护需求

ISSE 首先需要考虑系统任务可能受到的各方面的影响(包括人的因素和系统的因素),以及可能造成的各方面的损失,例如泄密、数据被篡改、服务不可用、操作抵赖等。用户通常都知晓其所需要的任务信息的重要性,但在确定这些信息需要何种保护,以及达到怎样的保护级别时,可能会一筹莫展。为了科学地了解任务的信息保护需求,ISSE 需要做的工作如下。

(1) 帮助用户对信息处理的过程建模。

(2) 帮助用户定义对信息的各种威胁。

(3) 帮助用户确定信息的保护次序和等级。

(4) 制定信息保护策略。

(5) 与用户协调、达成一致。

与用户进行交互是 ISSE 的必不可少的环节,在标识信息系统和信息的具体用户,标识用户与信息系统和信息的交互作用的实质、用户在信息保护生命周期各阶段的角色、责任和权力的基础上,评估信息和系统对任务的重要性,并确保任务需求中包含了信息保护的需求、系统功能中包含了信息保护的功能。

这个环节要达到的目标是:一份满足用户在资金、安全、性能、时间等各方面要求的信息系统保护框架,其中至少要包含以下几个方面。

(1) 被处理的信息是什么?属于何种类型(涉密信息、金融信息、个人隐私信息等)?

(2) 谁有权处理(初始化、查看、修改、删除等)这些信息?

(3) 授权用户如何履行其职责?

(4) 授权用户使用何种工具(硬件、软件、固件、文档等)进行处理?

(5) 用户行为是否需要监督(不可否认)?

在这个环节,ISSE 的工作需要用户的全程参与,共同研究信息系统的角色,使信息系统更好地满足用户的任务要求。

2. 掌握对信息系统的威胁

定义信息面临的威胁是“发掘信息保护需求”的一项关键活动。“威胁”是指可能造成某

个结果的事件或对系统造成危害的潜在事实。对信息管理的威胁，是指可以利用信息系统的脆弱性，可能造成某个有害结果的事件或对信息系统造成危害的潜在事实。

ISSE 需要在用户的帮助下，准确、详尽地定义出信息系统在设计、生产、使用、维护以及销毁的过程中可能受到的威胁，并针对这些威胁提出相应策略。

分析信息系统面临的安全威胁，可以从以下几个方面入手。

（1）检测恶意攻击。指检测人为的、有目的性的破坏行为，这些破坏行为分为主动和被动两种。主动攻击是指以各种方式有选择性地破坏信息，例如欺骗、修改、删除、否决、伪造、信息泄露、拒绝服务、提升权限等；被动攻击是指在不干扰系统正常工作的情况下，进行侦听、截获、窃取、破译等。

（2）了解安全缺陷。指了解信息系统本身存在的一些安全缺陷，包括网络硬件、通信链路、人员素质、安全标准等原因引起的安全缺陷。

（3）掌握软件漏洞。因为软件的复杂性和编程方法的多样性，导致软件中有意或无意留下了一些漏洞，例如操作系统的安全漏洞、TCP/IP 协议的漏洞、网络服务的漏洞等。

（4）分析结构隐患。主要是指网络拓扑结构的安全隐患，因为诸如总线、星状、环状、树状等结构都有各自的优缺点，都存在相应的安全隐患。

分析信息的威胁主体，应该涉及以下几个方面。

（1）威胁主体的动机或意图。

（2）威胁主体的能力。

（3）威胁或攻击的途径。

（4）主体及威胁存在的可能性。

（5）影响或后果。

3. 考虑信息保障政策

在了解了信息保护需求并掌握了系统面临的威胁之后，ISSE 需要考虑信息保障政策，并制定出相关的信息安全策略。

策略是指以正式形式出现的，经管理层同意和批准的，规定了组织行为方向和行为自由程度的途径，或者说策略是管理层对某个主题有关意见的一种陈述形式。信息安全策略是一组规则，这组规则描述了一个组织要实现的信息安全目标和实现这些信息安全目标的途径。

从管理角度看，信息安全策略是一个组织关于信息安全的文件，是一个组织关于信息安全的基本指导规则。它通常由组织最高管理层批准，在整个组织内发布。其目标在于减少信息安全事故的发生，将信息安全事故的影响与损失降低到最小。信息安全策略必须由高层管理机构批准并颁布，在策略的贯彻过程中，应该使每个参与者都能够理解策略，并且理解为相同的含义。如果策略在某些地方不能得到贯彻，则一定要让其他参与者都知道这样做的后果。信息安全策略是分层的，一旦制定后，高层的策略一般是不会改变的，而下层的局部策略可以根据具体情况而定，但不能与更高层的信息安全策略及其他有关政策相违背。制定策略的时候需要全面考虑相关的国家政策、法规、标准和惯例等。为达成这个目标，策略制定小组不仅需要系统工程师、ISSE 工程师、用户代表，还需要信用机构、认证机构、设计专家，甚至是政府机构的参与。

信息安全策略中需要具体定义出要保护什么、用什么方法保护、如何保护，需要确定以

下几方面的内容。

(1) 法律和法规。所要遵循的相关法律和法规的要求。

(2) 信息保护的内容和目标。确定要保护的所有信息资源,以及它们的重要性、所面临的主要威胁和需要达到的保护等级。

(3) 信息保护的职责落实办法。明确各组织、机构或部门的信息安全保护的责任和义务。

(4) 实施信息保护的方法。确定保护信息系统中的各种信息资源的具体方法。

(5) 事故的处理。包括应急响应、数据恢复等措施,以及相应的奖惩条款、监督机制等。

3.2.2 定义信息保护系统

ISSE 将定义信息保护系统将要做什么、信息保护系统执行其功能的情况如何,以及信息保护系统的内部和外部接口。定义信息保护系统的活动时,用户对于信息保障需求和信息系统环境的描述要被转换成目标、要求和功能,这一工作是要定义需要建立什么样的信息保障系统、信息保障系统如何实现良性地运行,并定义信息保障系统的内/外部接口,包括以下内容。

(1) 确定信息保障目标。

(2) 描述系统内部关联和环境。

(3) 检查信息保障要求。

(4) 功能分析。

1. 确定信息保障目标

信息保障目标与通常的系统对象具有相同的特性,例如对于信息保护需求的明确性、可测量性、可验证性、可追踪性等。确定信息保护对象,要保证它们的这些有效性度量(Measure of Effectiveness,MoE)性质,在描述每个对象时需要说明以下问题。

(1) 信息保障目标支持系统中的什么任务对象。

(2) 有哪些与信息保护目标和任务相关的威胁。

(3) 失去目标会有什么后果。

(4) 受什么样的信息保护策略或方针的支持。

2. 描述系统内部关联和环境

在信息安全工程中,系统联系对于确定系统边界并实施保护是很重要的,任务目标、任务信息处理、系统威胁、信息安全策略、设备等都极大地影响着系统边界与环境,因此,描述系统内部关联和环境需要做以下工作。

(1) 在系统的任务处理过程、与其他系统和环境之间,确定物理的和逻辑的边界。

(2) 描述信息的输入和输出、系统与环境之间或与其他系统之间的信号与能量的双向流动情况。

3. 检查信息保障要求

ISSE 的系统信息保障要求检查任务是对上述过程中的分析(包括目标、任务、威胁、系统联系等)进行特征检查。当信息保护需求从最初的信息保障的用户愿望,经过充分定义,并演变为一系列的系统保护规范时,信息保护的需求能力可能出现缺失,因此,需要检查信

息保护需求的正确性、完整性、一致性、依赖性、无冲突和可测试性等特征。

4. 功能分析

ISSE 使用许多系统工程工具来理解信息保护功能，并将功能分配给系统中各种信息保护的配置项。在定义信息保护系统中，对功能进行分析，必须分析备选系统体系结构、信息保护配置项，以及信息保护子系统是如何成为整个系统的一部分，这些功能是否能达到原本设定的目标，并理解它们如何才能与整个系统协调工作。

3.2.3　设计信息保护系统

明确目标系统后，将构造信息系统的体系结构，详细说明信息保护系统的设计方案。这时 ISSE 工程师要进行如下工作。

(1) 功能分配。

(2) 信息保护预设计。

(3) 详细信息保护设计。

1. 功能分配

当某种系统功能被定位到人、软件、硬件或固件上后，同时也就附上了相对应的信息保护功能。ISSE 应该为系统制定一个理论和实践上都可行的、协调一致的信息保护系统体系构架。功能分配过程包括以下内容。

(1) 提炼、验证并检查安全要求与威胁评估的技术原理。

(2) 确保一系列的低层要求能够满足系统级的要求。

(3) 完成系统级体系结构、配置项和接口定义。

2. 信息保护预设计

在需求和构架已经确定的前提下，ISSE 进入了信息保护的预设计阶段。在这一阶段，ISSE 工程师将制定出系统建造的规范，其中至少包括以下内容。

(1) 检查、细化并改进前期需求和定义的成果，特别是配置项的定义和接口规范。

(2) 从现有解决方案中找到与配置项一致的方案，并验证是否满足高层信息保护要求。

(3) 加入系统工程过程，并支持认证/认可和管理决策，提出风险分析结果。

3. 详细信息保护设计

进一步完善配置及方案，细化底层产品规范，检查每个细节规范的完整性、兼容性、可验证性、安全风险和可追踪性等。详细设计包括以下内容。

(1) 检查、细化并改进预设计阶段的成果。

(2) 对解决方案提供细节设计资料，以支持系统层和配置层的设计。

(3) 检查关键设计的原理和合理性。

(4) 设计信息保护测试与评估程序。

(5) 实施并追踪信息保护的保障机制。

(6) 检验配置层设计与上层方案的一致性。

(7) 提供各种测试数据。

(8) 检查和更新信息保护的风险与威胁计划。

(9) 加入系统工程过程，并支持认证/认可和管理决策，提出风险分析结果。

3.2.4 实施信息保护需求

这一活动的目标是建立、采购、集成、核实和验证各个信息保障的子系统，包括按照计划更新对于系统信息保障威胁的评估，以及对于系统运作状况的评估；核实系统信息保障要求以及实施解决方案的限制；跟踪、参与和应用信息保障担保机制；考查系统运行过程的进展情况，包括生命周期的支持计划；一套正式的信息保障评估系统；对于验证和鉴定过程的活动进一步增加内容；参与集体的、多学科的综合检查。

具体内容包括以下三个阶段。

(1) 采购部件。

(2) 建设系统。

(3) 测试系统。

1. 采购部件

一般来说，要根据市场产品的研究、偏好和最终的效果，来决定是以购买还是自行生产的方式来取得部件。购买/生产的决定应该通盘考虑安全因素、可操作性、性能、成本、进度、风险等影响。在购买时，对于大量生产且相对低成本的商业现货供应(Commercial off the Shelf，COTS)和由政府机构创建的技术团体开发的政府现货供应(Government off the Shelf，GOTS)等都可作为部件采购的考虑范围。在采购部件时，要注意考虑以下因素。

(1) 确保考虑了全部相关的安全因素。

(2) 查看现有产品是否能满足系统部件的需求，最好有多种产品可供选择。

(3) 验证一系列潜在的可行性选项。

(4) 考虑将来技术的发展，新技术和新产品如何运用到系统中去。

2. 建设系统

建设系统的过程，是确保已设计出必要的保护机制，并使该机制在系统实施中得以实现。与许多系统一样，信息保护系统也会受到许多因素的影响来加强或削弱其效果，这些因素决定了信息保护对系统的适宜程度。所以，在建设系统中，要重视以下问题。

(1) 部件的集成是否满足系统安全规范。

(2) 部件的配置是否保证了必要的安全特性，以及安全参数能否正确配置以便提供所要求的安全服务。

(3) 对设备、部件是否有物理安全保护措施。

(4) 组装、建造系统的人员是否对工作流程有足够的知识和权限。

3. 测试系统

ISSE 要给出一些与信息保护相关的测试计划和工作流程，还要给出相关的测试实例、工具、软硬件等。这些测试系统的工作包括以下内容。

(1) 检查、细化并改进设计信息安全系统的阶段结果。

(2) 检验解决方案的信息保护需求和约束限制等条件，并实施相关的系统验证和确认机制与决策。

(3) 跟踪实施与系统实施和测试相关的系统保障机制。

(4) 鉴别测试数据的可用性。

(5) 提供安全支持计划,包括逻辑上的、有关维护和培训等方面。

(6) 加入系统工程过程,并支持认证/认可和管理决策,提出风险分析结果。

3.2.5　评估信息保护有效性

ISSE 集中于信息保障系统的有效性,主要是指系统在保密性、完整性、可用性、不可否认性等安全特性方面的有效性。如果系统在这些方面达不到要求,信息系统安全工程的任务则很难达到用户的满意。

有效性评估要注意以下几点。

(1) 系统的互操作安全性,即系统是否通过外部接口正确地保护了信息。

(2) 系统的可用性,即系统是否能给用户提供信息资源与信息保护。

(3) 用户需要接受什么样的培训才能正确地操作和维护信息保护系统。

(4) 人机界面或接口是否有缺陷,从而导致出错。

(5) 建造和维护信息系统的成本是否可以接受。

(6) 确定风险和可能的任务影响,并提供报告。

要在多项活动中评估信息保护的有效性:发掘信息保护需求,定义系统安全要求,定义系统安全体系结构,开展详细的安全设计以及实现系统安全。

3.3　基于 ISSE 的公文流转系统安全解决方案

公文流转系统就是利用网络传送工作文件,将工作流转化为电子信息流,实现发文、收文、签发、审批等行政事务信息化,它的目的在于推进各部门办公自动化、网络化、电子化,通过信息及通信技术的应用,改变目前各部门之间传统的手工公文流转方式,突破时间与地域限制,使成员之间真正通过电子化渠道进行沟通,提高工作效率,从而为进一步实现信息化打下良好基础。

3.3.1　公文流转系统概述

公文管理是各企事业单位最繁杂的一项工作,不仅工作量非常大而且公文种类也很多。它主要包括议案、请示、工作报告、通报、通知、公告、函件、工作总结等。收文管理和发文管理是公文流转系统的核心功能,此安全解决方案主要针对收文管理和发文管理过程中的安全问题展开。

收文管理包括收文登记、收文拟办、核签、审核、批示、批复意见填报、收文办理、归档等工作。收文登记时自动编制收文号,可以选择模板或以附件形式新建公文。根据收文流程自动进行公文流转。收文办理人可以查看正文和历史处理流程、意见,收文流程如图 3-3 所示。

发文管理完成发文工作中的全部业务工作。在发文管理中文件由起草部门进行正式的拟稿,然后通过工作流送交部门负责人复核,在核稿完成后,送交主管领导审批并提交主管领导签发,完毕后返回经办人,由经办人清稿后发给办公室进行分发传阅,全部阅示完毕后文件归档。发文流程如图 3-4 所示。

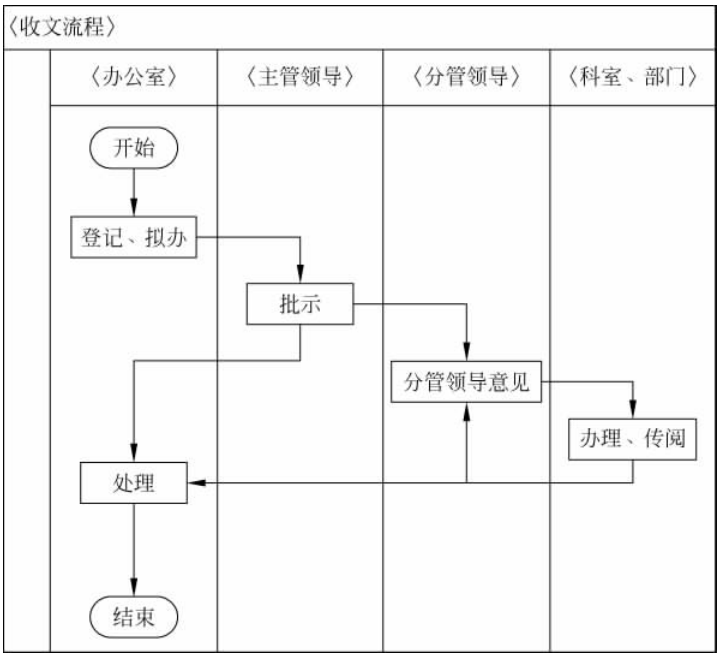

图 3-3　收文流程

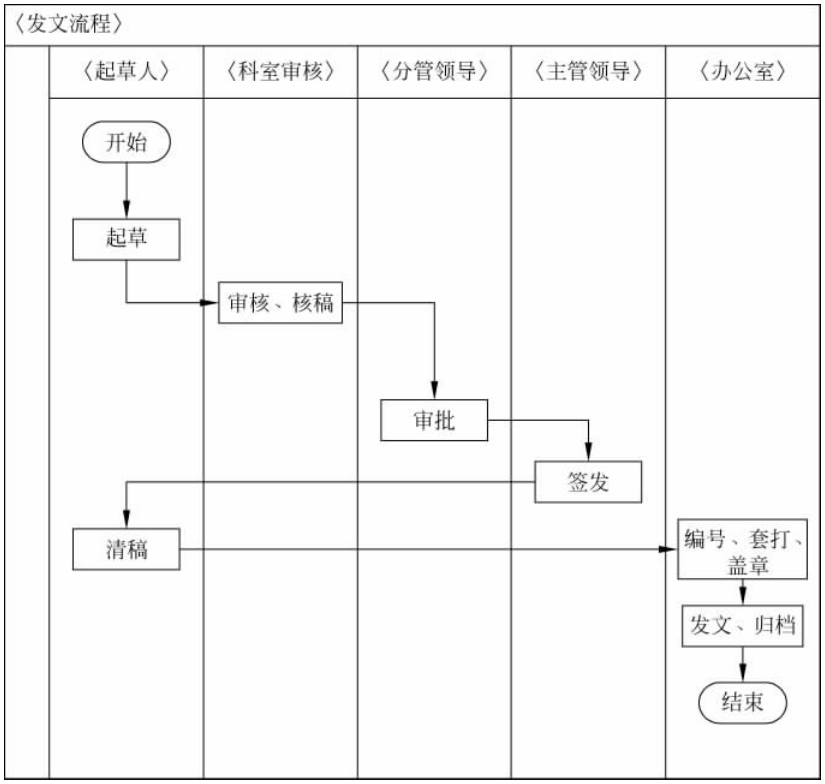

图 3-4　发文流程

从发文管理与收文管理的具体流程不难发现，公文流转强调一级一级处理的流程，不能越级也不能回转，因此访问控制是流程正常运行的关键；公文流转需要参与角色具有相应的权限才能进行既定的操作，由此可见身份认证也是一个必不可少的环节，此外，公文传输过程中的安全问题，也是一个不容忽视的环节。

3.3.2　安全需求分析

1. 公文流转系统的特点

公文流转系统包括了公文的上传、审批、下达、查阅等环节，是一种特殊的管理信息系统。公文流转系统能根据用户提出的公文流程，对整个工作流程进行实时跟踪，对修改审核的信息进行记录，并能根据有关规定自动地报告公文在流转过程中的状态。其特点主要体现在以下几个方面。

(1) 公文流转系统处理的是公文，涉及的往往是一些非结构化数据，没有结构、类型等方面的规定，不同的公文有不同的处理流程。

(2) 公文流转系统是集中式与分布式的混搭。公文集中存储在服务器上，在应用程序驱动下，在公文处理的各个环节流转。关于公文处理终端功能，有些需要能支持在本地进行扫描、编辑等公文处理，应用分布式，有些只需要支持批阅公文，需要集中式。

(3) 公文流转系统中公文的安全级别不同。公文流转系统应用于许多的办公部门，每个部门的工作人员的权限应该是不同的。公文流转过程中针对不同层次、级别的办公人员而言，公文的保密程度不同。

(4) 公文流转系统是一种综合性的管理系统，人员之间的协同工作在系统处理过程中表现尤为重要，公文流转过程中每个经手的人员或者部门的权限应该不同。用户可以预先定义公文的处理流程及相应权限，只有具有相应权限的人员才可以进行公文的在线处理。

2. 确定威胁类别及所带来的影响

威胁分析是安全需求挖掘中有决定意义的一步，只有确定威胁的种类，才能针对特定的威胁种类定义出特定的安全策略，制定有效的安全方法。对于整个公文流转系统，所受的威胁主要来自于以下两个方面。

1) 使用网络访问的人

(1) 来自系统内部人员的威胁。一方面，可能由于员工对于系统的安全操作要求不达标，从而导致系统运行无法达到安全标准，还有用户的不安全的使用习惯导致的系统的不安全；另一方面，可能由于员工有意恶意操作导致系统的不安全。

(2) 来自系统外部人员的威胁。由于系统内部的有些公文具有一定的价值，导致系统外部人员对系统发起攻击，从而对系统安全造成威胁。

人员威胁分析如图 3-5 所示。

2) 系统问题

(1) 软件故障。由于系统内部软件发生异常，致使内部公文丢失、损坏、泄密等情况发生，从而对系统安全构成威胁。

(2) 硬件故障。由于系统硬件发生故障，致使内部公文丢失、损坏、泄密等情况发生，从而对系统安全构成威胁。

(3) 恶意代码。由于用户操作过程中被提交了恶意代码，致使系统内部公文丢失、损

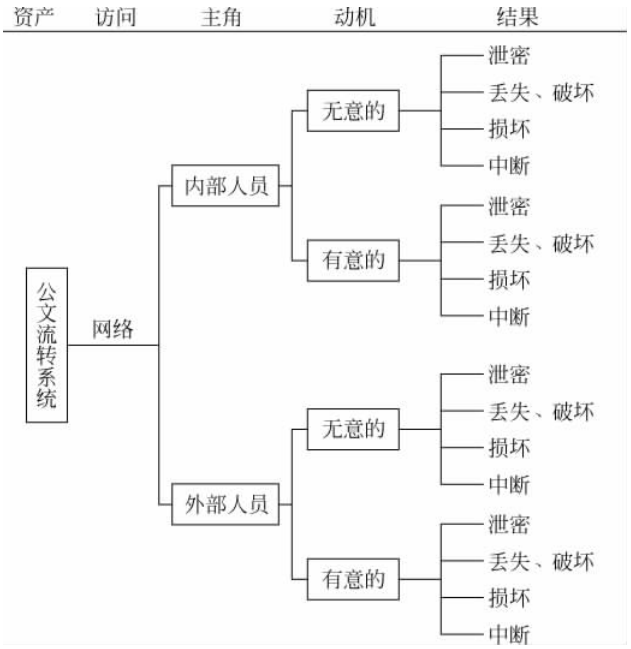

图 3-5　人员威胁分析

坏、泄密等情况发生，从而对系统安全构成威胁。

（4）系统崩溃。由于系统不稳定引起的崩溃，致使系统内部公文丢失、损坏、泄密等情况发生，从而对系统安全构成威胁。

系统威胁分析如图 3-6 所示。

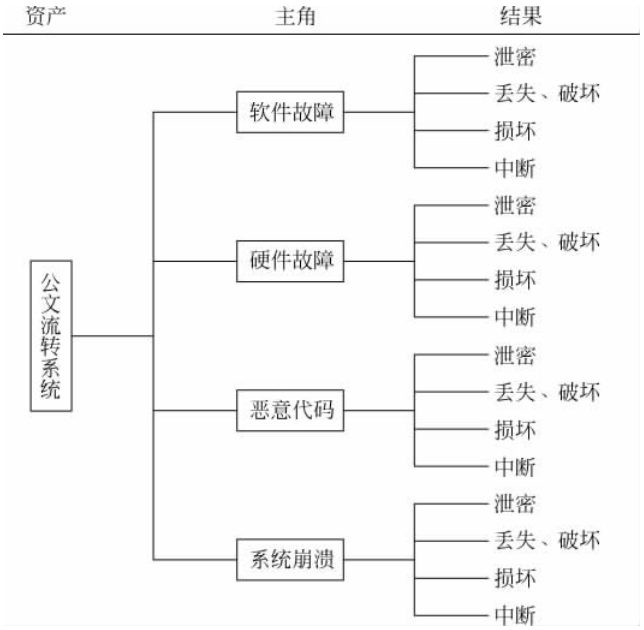

图 3-6　系统威胁分析

3. 确定安全需求

针对威胁分析与威胁分析可能造成的后果，确定了以下安全需求。

(1) 认证需求。提供某个实体的身份认证，保证只有合法用户才能访问到系统内资源。

(2) 访问控制需求。涉密公文必须得到严格的访问控制，确保非法访问者无法访问。

(3) 保密需求。涉密公文必须加密存放、加密传输。

(4) 数据完整性需求。公文必须得到严格的完整性保护，以防止未经授权的增加、删除、修改和代替。

(5) 不可否认需求。公文必须得到严格的防抵赖保护，确保公文的收发都无法抵赖。

(6) 可用性需求。为防止设备故障，软件故障发生引发的一系列问题，对数据进行备份，确保有据可查。

3.3.3　定义信息保护系统

1. 确定信息保护目标

针对以上分析得到的公文流转系统安全需求，本章提出了如下的信息保护目标。

(1) 保密性。信息不能被未授权的个人、实体或者过程利用所获知。

(2) 完整性。保护公文、信息准确和完整。

(3) 可用性。根据授权实体的要求可访问和利用指定的资源。

(4) 真实性。保证主体或资源的确是其所声称的身份、角色。

(5) 可核查性。确保实体行为能被有效跟踪和记录。

(6) 不可否认性。一个已发生的事件可被确认证明，在事后不能否认这个事件或者行为的发生。

2. 信息保护系统功能分析

该信息保护系统应实现对用户的身份认证和访问控制功能，同时应该实现对用户的主要操作进行日志记录，并提供日志审计功能。系统应该通过实现以上安全措施达到对系统中信息的保护，使得系统中的信息具有较强的保密性、不可篡改性和可追溯性。这样，系统中的机密信息才会得以保护，并且即使系统中的信息被非法篡改，也可以通过查阅日志记录追溯到嫌疑人并且对其追究相应的责任，其信息保护功能分析如下。

1) 用户认证功能

由于公文处理工作具有保密性、严肃性的特点，因而公文流转系统必须使用与之相适应的身份认证技术，并基于此形成完备的用户访问控制体系。

该部分功能的实现能满足真实性的信息保护目标。

2) 访问控制功能

访问控制是通过某种途径显式地准许或限制访问能力及范围的一种方法，是针对越权使用系统资源的防御措施；通过限制对关键资源的访问，防止非法用户的侵入或因为合法用户的不慎操作而造成的破坏。

该部分功能的实现能满足可用性的信息保护目标。

3) 数字签名与传输加密功能

公文流转过程中严格的保密性是公文流转系统基本的要求之一，所以一个成熟的公文流转系统必须使用数字签名技术，并在其基础上对数据传输进行加密。数字签名技术也是识别用户身份，确定公文责任的主要技术。

该部分功能的实现能满足保密性、完整性及不可否认性的信息保护目标。

4）审计功能

通过日志审计系统，企业管理员可以随时了解整个 IT 系统的运行情况，及时发现系统异常事件；另外，通过事后分析和丰富的日志系统，管理员可以方便、高效地对系统进行有针对性的安全审计。遇到特殊安全事件和系统故障，日志审计系统可以帮助管理员进行故障快速定位，并提供客观依据进行追查和恢复。

在公文流转系统中，日志记录主要包括记录用户操作，如登入、查看、审核和修改文件，文件当前的状态，如在审核中、审核完毕、归档等。

该部分功能的实现能满足可核查性的信息保护目标。

3.3.4 设计信息保护系统

根据以上分析，公文流转信息保护系统由四个安全功能模块组成，分别是用户认证模块、访问控制模块、安全审计模块和内容保护模块。每个模块均有各自的功能，负责实现不同的安全服务。并且，各个模块之间相互协调运作，对系统安全的保护起到重要的作用。安全保护系统功能模块如图 3-7 所示。

图 3-7 安全保护系统功能模块图

1. 用户认证设计

本系统采用 PKI/CA（Public Key Infrastructure/Certificate Authority）的方式进行用户认证。用户注册后，将从 CA 处获取数字证书。当用户登录时，需提交数字证书进行身份验证。用户身份认证流程如图 3-8 所示。

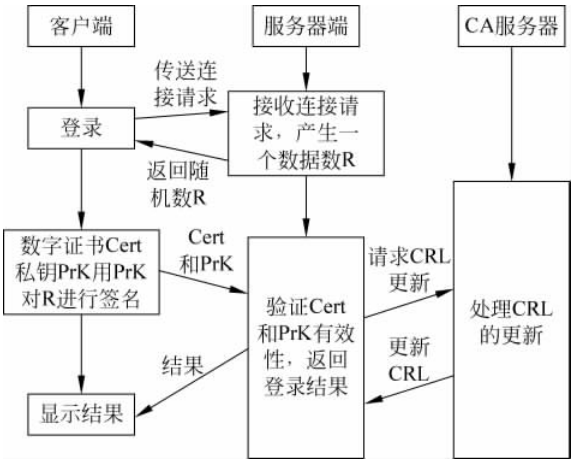

图 3-8 用户身份认证流程

2. 访问控制设计

由于公文流转系统本质上是一种工作流系统，并且一次流转流程中，存在诸多权限不同的用户，使用基于角色的访问控制可以很好地实现。但是基于角色的访问控制（Role-Based Access Control，RBAC）模型对于授权访问是静态的，对动态的公文流转没有良好的解决方法，这里对 RBAC 模型进行扩展。将公文分为静态公文和动态公文，动态公文的访问控制由关系定义进行补充。使用 RBAC 模型和关系约定，可以很好地实现公文流转中的访问控制。

访问控制的主要任务就是保证公文资源不被非法使用和访问，所以所指定的访问控制安全策略应该根据客体的属性而设定。由于客体分为动态客体（即流转中的公文）与静态客体（即归档后公文），所以安全策略也应该分为动态策略和静态策略。由于在发文管理和收文管理中，其对象主要是动态客体，所以这里设计部分只考虑动态策略的构建。

1）收文流程

收文是指由办公室进行接收，并指定特定权限的角色传阅。在这个流程中，为了防止公文被篡改，设置所有角色只对公文基本内容有“读”权限。基于角色的权限控制具体策略如下。

（1）在收文流程中，按照三元组的定义，只有角色（收文员、相关管辖、办公）才享有创建动态公文客体的权限，即首次收文并将公文转入流程系统的权限，并对公文进行初始化如下。

① 当前阶段为“签收”。

② 当前激活区域为公文基本信息（公文编号、公文标题、公文内容等）。

③ 初始化当前控制者。

④ 前处理者为无。

（2）公文流转阶段的规则。除非处理过程完成，即阶段为“处理”，否则只能按照规定的流程进行流转。如果需要多次交互，则有控制流程权限的用户可以做适当的调整，指定公文流转的下一个用户。这些交互过程由逻辑值决定是否转入新的流转阶段。

（3）如果当前阶段为 a1，当前控制者为 user1，则当 user1 完成现阶段操作后，将客体向下一个阶段流转时，需要完成以下任务。

① 修改当前阶段的值，并且下一个阶段的值要满足公文流转阶段的规则。

② 设定下一个控制者的角色，并且下一个控制者的角色的值必须满足授权接手公文的角色。

（4）当用户 user1 成为协办方时，需要完成修改“公文——协办者”关系，将 ID 加入关系中。

（5）用户 user1 对流转中的公文的访问权限，即具体可执行的基本操作，按照下列策略规定。

① 如果用户为动态客体的“当前控制者”，并已有登记信息，就可以对公文执行当前阶段角色允许的操作；如果用户是“前处理者”，则只对公文的基本信息拥有读的权限；如果用户既不是控制者、协办者，也不是前处理者，则对公文没有任何访问权限。

② 如果角色中有公文反馈权限，则可以将不满意的公文设置相应的逻辑值为 False，并将流程返回给最后一位“前处理者”进行重新批阅，这称作一次交互。交互流转时，其他与交互过程无关的用户只有读权限。

③ 如果当前控制者所处的角色中，有调整流转流程的权限，则可以对公文流转的过程进行自定义规定，同时记录控制信息到公文临时信息中。

④ 当公文处理阶段完成之后，一次收文流程完成，这时，公文转变为静态客体，所有角色对其都只有读权限。

2）发文流程

发文是公文流转系统中又一个重要的部分，通过发文流程，可以完成将动态客体转变为静态客体的过程。具体的访问控制策略与收文流程相同。

（1）在发文流程中，按照角色定义，有角色（起草人、相关管辖、办公）负责发文流转过程中动态公文的创建，并填写公文基本信息、访问信息、临时信息等初始化工作。起草阶段完成后，可以获得一份粗略的动态客体。

（2）由发文流程可知，在发文流转中，不存在收文流程中的交互过程，即不存在动态公文被打回去的情况。

（3）如果当前阶段为 a1，当前控制者为 user1，则当 user1 完成现阶段操作后，将客体向下一个阶段流转时，需要完成以下的任务。

① 修改当前阶段的值，并且下一个阶段的值要满足公文流转阶段的规则。

② 设定下一个控制者的角色，并且下一个控制者的角色的值必须满足授权接收公文的角色。

（4）当用户 user1 成为协办方时，需要完成修改“公文——协办者”关系，将 ID 加入关系中。这时，用户对公文基本内容有读权限，对公文临时信息部分有读写权限。

（5）用户 user1 对流转中的公文的访问权限，即具体可执行的基本操作，按照下列策略规定。

① 如果用户为动态客体的“当前控制者”，并已有登记信息，就可以对公文执行当前阶段角色允许的操作；如果用户是“前处理者”，则只对公文的基本信息拥有读的权限；如果用户既不是控制者、协办者，也不是前处理者，则对公文没有任何访问权限。

② 如果当前控制者所处的角色中，有调整流转流程的权限，则可以对公文流转的过程进行自定义规定，同时记录控制信息到公文临时信息中。

③ 当公文处理阶段完成之后，一次收文流程完成，这时，公文转变为静态客体，所有角色对其都只有读权限。

（6）由发文流程可知，最终文档的整合由办公人员完成，即公文的编号、盖章、发文、归档的授权角色。

（7）当公文归档后，一次发文流转完成，动态公文转换为静态公文，这时，所有角色对静态公文都只有读权限。

3. 安全审计设计

日志是记录系统中硬件、软件和系统问题的信息，同时还可以监视系统中发生的事件。用户可以通过它来检查错误发生的原因，或者寻找受到攻击时攻击者留下的痕迹。经过规范化、过滤、归并和警告分析等处理后，以统一格式的日志形式进行集中存储和管理，结合丰富的日志统计汇总及关联分析功能，实现对信息系统的全面审计。

在公文流转系统中，日志记录主要包括记录用户操作，如登录、查看、审核和修改文件，文件当前的状态，如在审核中、审核完毕、归档等。

1）用户登录

用户登录的日志记录应该包含事件编号、用户名、用户登录 IP 地址、登录是否成功、登

录时间、退出时间、日志类别。

(1) 事件编号。用户登录事件的编号。

(2) 用户名。用户登录名。

(3) 用户登录 IP 地址。用户登录地点的 IP 地址。

(4) 登录是否成功。用户是否登录成功。

(5) 登录时间。用户登录的时间。

(6) 退出时间。用户退出的时间。

(7) 日志类别。日志记录属于哪一个类别。若属于用户类别,则日志记录的是用户登录的事件;若属于文件处理,则记录的是用户处理文件的记录。

用户登录日志如表 3-2 所示。

表 3-2　用户登录日志

事件编号	用户名	用户登录 IP 地址	登录是否成功	登录时间	退出时间	日志类别
0001	Sa	1.1.1.1	是	2018-12-19	2018-12-19	用户
0002	Admin	127.0.0.1	是	2018-12-19	2018-12-19	用户

2) 处理文件

处理文件的日志记录,包含文件编号、文件名、处理人员、处理方式、处理部门、处理时间、日志类别、安全级别。

(1) 文件编号。文件自动进行编号。

(2) 文件名。文件名字。

(3) 处理人员。对文件进行处理的人员。

(4) 处理方式。用户对文件进行的操作,例如收文登记、收文拟办、核签、审核、批示、批复意见填报、收文办理、归档。

(5) 处理部门。对文件进行处理的人员的部门。

(6) 处理时间。文件处理的时间。

(7) 日志类别。日志记录属于哪一个类别。若属于用户类别,则日志记录的是用户登录的事件;若属于文件处理,则记录的是用户处理文件的记录。

(8) 安全级别。分为安全、警告、危险。安全级别表示用户登录操作或文件处理在用户权限之内,没有越权情况发生;警告级别表示用户频繁登录,登录 IP 地址变化频繁,对文件提出异常处理请求或文件处理异常;危险级别表示用户对文件进行越权访问。

用户收文过程日志如表 3-3 所示。

表 3-3　用户收文过程日志

文件编号	文件名	处理人员	处理方式	处理部门	处理时间	日志类别	安全级别
1001	公文 1	办公室 1	处理	办公室	2018-12-1	文件处理	安全
1002	公文 2	主管领导 1	批示	主管部门	2018-12-2	文件处理	安全
1002	公文 2	分管领导 1	审阅	分管部门	2018-12-2	文件处理	安全
1004	公文 4	科员 1	办理	科室	2018-12-3	文件处理	安全
1004	公文 4	办公室 1	登记	办公室	2018-12-5	文件处理	安全

用户发文过程日志如表 3-4 所示。

表 3-4 用户发文过程日志

文件编号	文件名	处理人员	处理方式	处理部门	处理时间	日志类别	安全级别
1001	公文 1	起草人 1	起草	科室 1	2018-12-1	文件处理	安全
1001	公文 1	科员 1	审核	科室 1	2018-12-2	文件处理	安全
1001	公文 1	分管领导	审批	分管部门	2018-12-2	文件处理	安全
1001	公文 1	主管领导	签发	主管部门	2018-12-3	文件处理	安全
1001	公文 1	办公室 1	编号,发文	办公室	2018-12-5	文件处理	安全
1001	公文 1	起草人	结稿	科室 1	2012-12-4	文件处理	安全

3）日志文件的保护

日志文件的查看权限：需要管理员权限才可查看日志记录文件；日志文件的修改和删除应设置为本地管理员登入才可处理。

4. 内容保护设计

公文流转过程中，主要有三种情况的文件传送。

（1）一对多的公开明文发送。只需要以明文的方式发送公文，如校长办公室发送给全校的放假通知。

（2）多对一的公文发送。如下级部门的公文，需要发给上级签字。公文需要以密文的方式发送，并且需要保证公文被正确的人签字。

（3）一对一的公文发送。如领导发送给各部门主管的重要通知，必须以密文形式发送，以免被他人截获，从而泄露公司秘密。

此案例采用非对称密码体制来保证公文内容的安全。

3.3.5 实施信息保护系统

基于 ISSE 的设计理念，可以将公文流转系统的实施部分划分为 3 个模块，如图 3-9 所示。

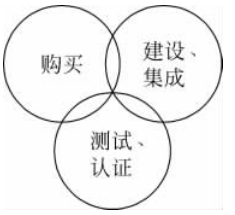

图 3-9 实施信息保护系统的 3 个模块

1. 购买

根据系统设计部分的要求，购买搭建公文流转系统所必需的服务器设备（网站服务器、数据库服务器、VPN 设备），硬件防火墙，路由器等。如有必要，相应的软件服务也需购买。

2. 建设、集成

根据系统设计部分的各个模块需求，集成收文管理和发文管理的两大基本功能。其中收文管理集成了收文登记、收文拟办、核签、审核、批示、批复意见填报、收文办理、归档等功能；发文管理集成了文件拟稿、文件复核、主管领导复核、领导签发、经办人分发传阅、文件归档等功能。最终建设出具备用户认证和访问控制功能，同时对用户的主要操作具备日志记录和日志审计功能的公文流转系统。

3. 测试、认证

按照 ISSE 的标准测试所构建的公文流转系统能否满足用户需求，是否具备用户认证和访问控制功能，是否具备对用户的主要操作有日志记录和日志审计的功能，且能满足用户和认证员的要求。

3.3.6　评估信息保护有效性

该项目主要是实现公文流转系统上的用户验证、访问控制、信息保密性、数据完整性、不可否认性、建立起一套完善的公文流转系统安全保障体系。评估信息保护的有效性主要集中于该信息保障系统的有效性，即系统在保密性、完整性、可用性、不可否认性等安全特性方面的有效性。

项目主要从 5 个方面进行了有效性评估。

1. 实体鉴别

登录系统的用户需要通过身份认证，只有合法的用户才可以访问系统，执行操作。而系统也要提供系统证书，防止有第三者假冒系统。

2. 权限控制

用户新建公文或者审核公文的时候，都需要相应的权限验证，确保该用户有权力访问所要求的公文，进行所要求的操作。

3. 数据保密性

保证公文在前一环节的用户到下一环节之间的传输不被窃听，只有指定的用户才能阅读指定的公文。只有的得到文件服务器的权限才可以访问文件服务器。

4. 不可否认性

公文的提交方不能否认在公文上载明的时间提交过这份公文，接受方不能否认在载明的时间接受过该公文。

5. 数据完整性

公文在传输过程不被插入、修改、更改顺序或者重放。

3.4　小　　结

总的来说，信息系统安全工程规定了在各个阶段应该达到的目的，但没有规定具体的工具和方法，只是从系统论的角度指明了一个框架和范围，实施的细节依赖于已有的经验和积累。信息系统安全工程沿袭了系统工程以时间维划定工程元素的方法学，暴露出一些不足。首先，很多安全要求应该贯彻在整个工程过程之中，尤其是信息安全的保证要求，而信息系统安全工程对其缺乏有针对性的讨论。其次，信息安全的内容极其庞杂，一次完整的信息安全工程过程，往往会涉及多个复杂的安全领域，而有些领域的时间过程性却不明显，以时间维为线索的描述方式不适合反映这些内容。因此，后来在信息安全工程方法的发展上，出现了第二种思路：过程能力成熟度的方法。

习　题

1. 如何发掘信息系统的安全需求？
2. 简述信息系统安全工程的过程。
3. 试比较 ISSE 与 SE。
4. 什么是威胁？一个普通的信息管理系统经常面临什么样的威胁？