第22章信息系统安全管理

22.1信息系统安全策略

22.1.1信息系统安全策略的概念与内容

信息系统安全策略是指针对本单位的计算机业务应用信息系统的安全风险□安全威胁）进行有效的识别、评估后，所采取的各种措施、手段，以及建立的各种管理制度、规章等。由此可见，一个单位的安全策略一定是定制的，都是针对本单位的“安全风险（威胁）”来进行防护的。安全策略的归宿点□立脚点）就是单位的资产得到充分的保护。安全策略涉及技术的和非技术的、硬件的和非硬件的、法律的和非法律的各个方面。

由于计算机业务应用信息系统安全的事情涉及到单位□企业、党政机关）能否正常运营的大事，必须由单位的最高行政执行长官、部门或组织授权完成安全策略的制定，并经过单位的全员讨论修订。安全策略自从宣布施行之日起，就是单位□企业、党政机关）内部的一个重要法规，任何人不得违反。

安全策略的核心内容就是“七定”，即定方案、定岗、定位、定员、定目标、定制度、定工作流程。“七定”的结果就是确定了该单位组织的计算机业务应用信息系统的安全如何具体地实现和保证。安全策略一定要具有科学性、严肃性、非二义性和可操作性。

按照系统安全策略“七定”要求，系统安全策略首先要解决定方案，其次就是定岗。

目前，国家部级机关的信息中心负责计算机业务应用信息系统的运营。在信息中心设置安全处，配备一名处长和一到两名副处长，科室设置和科员配置各单位均不相同。但明确了单位的信息安全由安全处负责，处长就是单位的CSO (Chief Security Officer)。国内银行系统由科技处负责全行的计算机业务应用信息系统的安全，科技处处长就是银行的CSO。

以上做法虽然简单，但定岗、定位、定员、定目标都得到落实了。然后就要由安全处或科技处负责定制度、定工作流程。在定制度、定工作流程中，还要明确一些关键岗位和人员。CSO之下，国内一般设置以下各种专业化的职能和职位，如机房设备安全管理、主机和操作系统管理、网络和数据库管理、应用和输入输出管理、应用开发管理以及应急事故管理等，相应的职位为各种管理员，如机房设备安全管理员、主机和操作系统管理员等。

有了岗位，就要有责、权、利以及相应的工作制度、工作流程，由此形成各种安全策略，包括机房设备安全管理策略、主机和操作系统管理策略、网络和数据库管理策略、应用和输入输出管理策略、应用开发管理策略、应急事故管理策略、密码和安全设备管理策略、信息审计管理策略等。

22.1.2建立安全策略需要处理好的关系

1．安全与应用的依存关系

安全与应用是矛盾统一的。没有应用，就不会产生相应的安全需求；发生安全问题，就不能更好地开展应用。另外，安全是有代价的，不但会增加系统的开销，也会增加系统建设和运行的费用，同时还会规定对使用的限制，从而给应用带来不便。应用需要安全、安全为了应用。过分强调安全或者应用，都是有失偏颇的，都不是正确的态度。

2．风险度的观点

系统安全是一个动态的过程，今天看来是安全的系统，明天可能就不再安全。因为发现了新的漏洞，或者黑客研究出了新的攻击技术，病毒制造者设计了新的病毒程序，甚至仅仅是由于我们对系统进行了重新配置等。因此把信息系统的安全目标定位于“系统永不停机、数据永不丢失、网络永不瘫痪、信息永不泄密”，是错误的，是不现实的，也是不可能的。系统安全是相对的，是一个风险大小的问题。我们不能一厢情愿地追求所谓的绝对安全，而是要将安全风险控制在合理程度或允许的范围内。这就是风险度的观点。

3．适度安全的观点

怎样才是适度安全，需要运用风险评估的方法才能得出结论。风险评估围绕威胁、资产、脆弱性、安全措施展开分析。在评估时不仅要考虑现有环境，还要考虑近期和远期发展变化趋势。同时，还要评估控制风险所需的安全代价。在此基础上对风险和代价进行均衡，才能确定相应的安全策略。安全风险和安全代价两者之间的关系，可用图22-1表示。

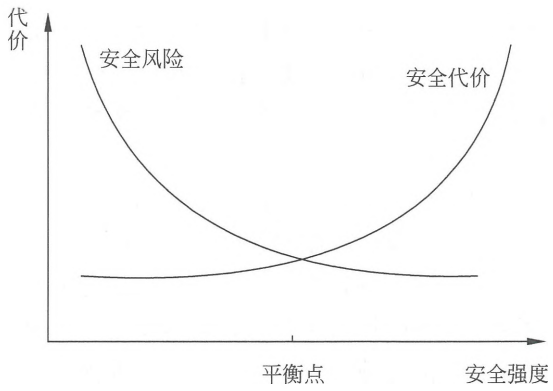


图22-1安全风险和安全代价之间关系

从图中不难看出，安全代价低，显然安全风险肯定很大；反之，安全风险要降得很低，安全的代价也就很大。这个代价不光指资金投入，包括系统性能下降、效率低下等引出的“代价”。一个好的信息安全保障系统的标志就是有效控制两者的“平衡点”，既能保证安全风险的有效控制，又使安全的代价可以接受。这个平衡点对于不同行业、不同单位、不同时间点都不一样，需要实现“动态”控制。三种不同架构的信息安全保障系统和网络信息安全的等级保护等的理念和建设方案，都是适度安全的观点的体现。

4．木桶效应的观点

木桶效应的观点是将整个信息系统比作一个木桶，其安全水平是由构成木桶的最短的那块木板决定的。同时，保护信息系统的各个安全要素是同等重要的，各方面要素均不容忽视。但是要强调的是，安全管理在所有要素中具有极其重要的地位。有人将安全管理的漏洞比作存在于木桶桶底的漏洞。如果安全管理有漏洞，其他安全措施即使投入再大也无济于事。

5．信息系统安全等级保护的概念

《计算机信息系统安全保护等级划分准则》 GB 17859—1999)是建立安全等级保护制度，实施安全等级管理的重要基础性标准，它将计算机信息系统分为以下5个安全保护等级。

第一级用户自主保护级。通过隔离用户与数据，使用户具备自主安全保护的能力。它为用户提供可行的手段，保护用户和用户信息，避免其他用户对数据的非法读写与破坏，该级适用于普通内联网用户。

第二级系统审计保护级。实施了粒度更细的自主访问控制，它通过登录规程、审计安全性相关事件和隔离资源，使用户对自己的行为负责。该级适用于通过内联网或国际网进行商务活动，需要保密的非重要单位。

第三级安全标记保护级。具有系统审计保护级的所有功能。此外，还需提供有关安全策略模型、数据标记以及主体对客体强制访问控制的非形式化描述，具有准确地标记输出信息的能力；消除通过测试发现的任何错误。该级适用于地方各级国家机关、金融单位机构、邮电通信、能源与水源供给部门、交通运输、大型工商与信息技术企业、重点工程建设等单位。

第四级结构化保护级。建立于一个明确定义的形式安全策略模型之上，要求将第三级系统中的自主和强制访问控制扩展到所有主体与客体。此外，还要考虑隐蔽通道。必须结构化为关键保护元素和非关键保护元素。计算机信息系统可信计算机的接口也必须明确定义，使其设计与实现能经受更充分的测试和更完整的复审。加强了鉴别机制；支持系统管理员和操作员的职能；提供可信设施管理；增强了配置管理控制。系统具有相当的抗渗透能力。该级适用于中央级国家机关、广播电视部门、重要物资储备单位、社会应急服务部月、尖端科技企业集团、国家重点科研单位机构和国防建设等部门。

第五级访问验证保护级。满足访问控制器需求。访问监控器仲裁主体对客体的全

部访问。访问监控器本身是抗篡改的；必须足够小，能够分析和测试。为了满足访问监控器需求，计算机信息系统可信计算机在其构造时，排除那些对实施安全策略来说并非必要的代码；在设计和现实时，从系统工程角度将其复杂性降低到最小程度。支持安全管理员职能；扩充审计机制，当发生与安全相关的事件时发出信号；提供系统恢复机制。系统具有很高的抗渗透能力。该级适用于国防关键部门和依法需要对计算机信息系统实施特殊隔离的单位。

不管是企业还是单位机构，应当根据其业务应用信息系统所处理信息的敏感程度、业务应用的性质和部门重要程度，按照国家有关标准分别确定其计算机信息系统的安全保护等级。

信息系统的安全保护等级由两个定级要素决定：等级保护对象受到破坏时所侵害的客体和对客体造成侵害的程度。

一是受侵害的客体。等级保护对象受到破坏时所侵害的客体包括公民、法人和其他组织的合法权益；社会秩序、公共利益；国家安全。

二是对客体的侵害程度。对客体的侵害程度由客观方面的不同外在表现综合决定。由于对客体的侵害是通过对等级保护对象的破坏实现的，因此，对客体的侵害外在表现为对等级保护对象的破坏，通过危害方式、危害后果和危害程度加以描述。等级保护对象受到破坏后对客体造成侵害的程度分为造成一般损害；造成严重损害；造成特别严重损害。因此，信息系统受到破坏后，会对公民、法人和其他组织的合法权益造成损害，但不损害国家安全、社会秩序和公共利益，则为第一级。信息系统受到破坏后，会对公民、法人和其他组织的合法权益产生严重损害，或者对社会秩序和公共利益造成损害，但不损害国家安全，则为第二级。信息系统受到破坏后，会对社会秩序和公共利益造成严重损害，或者对国家安全造成损害，则为第三级。信息系统受到破坏后，会对社会秩序和公共利益造成特别严重损害，或者对国家安全造成严重损害，则为第四级。信息系统受到破坏后，会对国家安全造成特别严重损害，则为第五级。

定级要素与信息系统安全保护等级的关系，如表22-1所示。

表22-1定级要素与安全保护等级的关系

等 级	对 象	侵 害 客 体	侵 害 程 度	监 管 强 度
第一级	一般系统	合法权益	损害	自主保护
第二级		合法权益	严重损害	指导
		社会秩序和公共利益	损害	
第三级	重要系统	社会秩序和公共利益	严重损害	监督检查
		国家安全	损害	
第四级		社会秩序和公共利益	特别严重损害	强制监督检查
		国家安全	严重损害	
第五级	极端重要系统	国家安全	特别严重损害	专门监督检查

22.1.3信息系统安全策略设计原则

我国信息化建设总结出来的宝贵经验有8个总原则和10个特殊原则。

1．8个总原则

(1) 主要领导人负责原则。信息安全保护工作事关大局，影响组织和机构的全局，主要领导人必须把信息安全列为其最关心的问题之一，并负责提高、加强部门人员的认识，组织有效队伍，调动必要资源和经费，协调信息安全管理工作与各部门的工作，使之落实、有效。

(2) 规范定级原则。有关部门或组织根据其信息重要程度和敏感程度以及自身资源的客观条件，应按标准确定信息安全管理要求的相应等级，并在履行相应的审批手续后，切实遵从相应等级的规范要求，制定相应的安全策略，并认真实施。

(3) 依法行政原则。信息安全管理工作主要体现为行政行为，因此必须保证信息系统安全行政主体合法、行政行为合法、行政内容合法、行政程序合法。

(4) 以人为本原则。威胁和保护这两个对立面是信息安全管理工作的主体。实践表明它们在很大程度上受制于人为的因素。加强信息安全教育、培训和管理，强化安全意识和法治观念，提升职业道德，掌握安全技术是做好信息安全管理工作的重要保证。

(5) 注重效费比原则。安全需求的不断增加和现实资源的有限性使安全决策处于两难境地。恰当地把握效费比是从全局上处置好信息安全管理工作的一个平衡点。

(6) 全面防范、突出重点原则。全面防范是信息系统综合保障措施。它需要从人员、管理和技术多方面，在预警、保护、检测、反应、恢复和跟踪等多个环节上采用多种技术实施。同时，又要从组织和机构的实际情况出发，突出自身的信息安全管理重点。不同的部门、不同的信息系统应有不同的信息安全管理重点。

(7) 系统、动态原则。信息系统安全管理的系统特征突出。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，以便能按照“木桶原理”体现信息保护安全管理的系统集成效果。同时，信息保护安全管理又是一种状态和过程，随着系统脆弱性及其强度的时空分布的变化，威胁程度的提高，系统环境的变化以及人员对系统安全认识的深化等，必须及时地将现有的安全策略、风险接受程度和保护措施进行复查、修改、调整以至提升安全管理等级。

(8) 特殊的安全管理原则。在制定和实施安全策略和技术措施时，必须遵循安全管理的10个特殊原则。

2．10个特殊原则

(1) 分权制衡原则。安全管理采取分权制衡的原则，避免操作权力过分集中，否则一旦出现问题就将全线崩溃。

(2) 最小特权原则。对信息、信息系统的访问采用最小特权原则。任何实体□用户、管理员、进程、应用或系统）仅享有该主体需要完成其被指定任务所必须的特权，不应享有任何多余特权。

(3) 标准化原则。安全技术和设备的使用要经有关部门批准，并按有关等级标准使用。

(4) 用成熟的先进技术原则。成熟的技术提供可靠性、稳定性保证，采用新技术时要重视其成熟的程度。如果新技术势在必行，应该首先局部试点然后逐步推广，减少或避免可能出现的损失。

(5) 失效保护原则。系统运行错误或故障时必须拒绝非授权访问，阻断非授权人员进入内部系统，直至必要时以牺牲使用为代价确保安全。

(6) 普遍参与原则。不论信息系统的安全等级如何，要求信息系统所涉及人员普遍参与，共同保障信息系统安全。

(7) 职责分离原则。职责分离是降低意外或故意滥用系统风险的一种方法。为减小未经授权的修改、滥用信息或服务的机会，对特定职责或责任领域的管理和执行功能实施分离。有条件的组织或机构，应执行专职专责。如职责分离比较困难，应附加其他的控制措施，如行为监视、审计跟踪和管理监督。

(8) 审计独立原则。审计独立，才能保证公正。

(9) 控制社会影响原则。非涉密信息的完整性、可用性对社会具有相当重大的影响，同样应针对其风险程度予以保护。

(10) 保护资源和效率原则。风险度的观点和适度安全的观点都是安全策略制定中的具体体现。

22上4信息系统安全方案

1.与信息系统安全方案有关的系统组成因素

系统方案直接影响到信息系统安全实施与效果，因此，建设一个计算机业务应用信息系统时，从信息安全角度考虑，确定一个有利于信息安全的系统组成方案是十分必要的。与系统安全方案有关的系统包括以下组成因素。

(1) 主要硬件设备的选型。

(2) 操作系统和数据库的选型。

(3) 网络拓扑结构的选型。

(4) 数据存储方案和存储设备的选型。

(5) 安全设备的选型。

(6) 应用软件开发平台的选型。

(7) 应用软件的系统结构的确定。

(8) 供货商和集成商的选择等。

(9) 业务运营与安全管理的职责□岗位）划分。

(10) 应急处理方案的确定及人员的落实。

这些全局性组成因素的选定是否科学合理，对以后整个系统的信息安全方案的确定

具有决定的作用。

2.确定信息系统安全方案

确定信息系统安全方案主要包括以下内容。

(1) 首先确定采用MIS+S、S-MIS或S^2-MIS体系架构，不同体系架构差别很大，对后续工作和目标影响很大。

(2) 确定业务和数据存储的方案。业务和数据存储的方案对整个信息系统组成和信息安全方案的确定，影响很大。

(3) 网络拓扑结构。信息安全的主要威胁都是来自网络，因此网络的拓扑结构对信息安全方案的确定，影响也是很大。

(4) 基础安全设施和主要安全设备的选型。这部分是信息安全保障系统的核心，有没有这些设施，选用什么样的安全设备，对信息安全方案的确定起到关键的作用。

(5) 业务应用信息系统的安全级别的确定。根据国家标准GB 17859—1999《计算机信息系统安全保护等级划分准则》，单位可以根据使用的目的要求，确定本单位的计算机业务应用信息系统要确定为哪一等级，一旦你确定了某个安全级别，也就确定了安全的大体方案。

(6) 系统资金和人员投入的档次。这条决定了前几条的选定，因为没有钱，一切设想、计划只能成为幻想。有了钱，没有人也是不可想象的。

我们知道，“信息安全保障系统”是一个在网络上，集成各种硬件、软件和密码设备，以保障其他业务应用信息系统正常运行的专用信息应用系统，以及与之相关的岗位、人员、策略、制度和规程的总和。因此，系统安全方案与系统的安全策略是密不可分的。没有安全策略就没有安全方案；相反，没有安全方案，也就没有安全策略。

22.2信息安全系统工程

22.2.1信息安全系统工程概述

随着国际互联网信息高速公路的畅通和国际化的信息交流，业务大范围扩展，信息安全的风险也急剧恶化。由业务应用信息系统再来解决安全，已经不能胜任。再由操作系统、数据库系统、网络管理系统来解决安全问题，也不能满足实际的需要，于是才不得不建立独立的信息安全系统。信息安全系统是一门新兴的工程实践课题。与国外的同行相比，我们极有必要加大对信息安全系统工程的研究，规范信息安全系统工程建设的过程和提高建设信息安全系统工程的成熟能力。否则，信息安全系统工程建立不合理、不科学、不到位、不标准，势必影响业务应用信息系统的正常运营，阻碍信息化的推进。

信息安全系统工程就是要建造一个信息安全系统，它是整个信息系统工程的一部分，而且最好是与业务应用信息系统工程同步进行，而它主要是围绕“信息安全”的内

容，如信息安全风险评估、信息安全策略制定、信息安全需求确定、信息安全系统总体设计、信息安全系统详细设计、信息安全系统设备选型、信息安全系统工程招投标、密钥密码机制确定、资源界定和授权、信息安全系统施工中需要注意防泄密问题和施工中后期的信息安全系统测试、运营、维护的安全管理等问题。这些问题与用户的业务应用信息系统建设所主要关注的完全不同。业务应用信息系统工程所主要关注的是客户的需求、业务流程、价值链等的企业的业务优化和改造的问题。信息安全系统建设所关注的问题恰恰是业务应用信息系统正常运营所不能缺少的。

为了进一步论述信息安全系统工程，我们需要区分几个术语，并了解它们之间的关系。信息系统、业务应用信息系统、信息安全系统，信息系统工程、业务应用信息系统工程、信息安全系统工程以及信息系统安全和信息系统安全工程之间的关系，如图22-2所示。

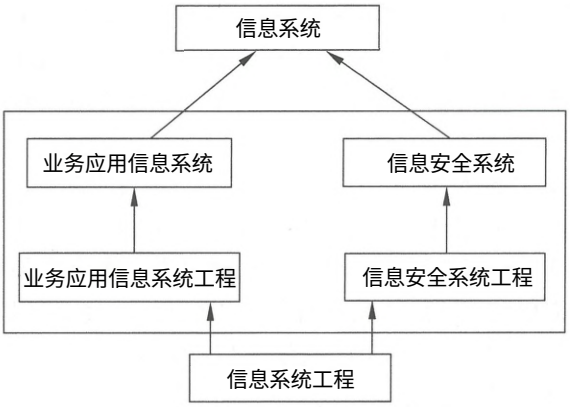


图22-2术语之间的关系

信息系统业界又叫作信息应用系统、信息应用管理系统、管理信息系统，简称MIS (Management Information System)。信息安全系统服务于业务应用信息系统并与之密不可分，但又不能混为一谈。信息安全系统不能脱离业务应用信息系统而存在，比如我们说建立国税信息系统、公安信息系统、社保信息系统等，一定包含业务应用信息系统和信息安全系统两个部分。但二者的功能、操作流程、管理方式、人员要求、技术领域等都完全不同。随着信息化的深入，两者的界限就越来越明显了。

业务应用信息系统支撑业务运营的计算机应用信息系统，如银行柜台业务信息系统、国税征收信息系统等。

信息系统工程即建造信息系统的工程，包括两个独立且不可分割的部分，即信息安全系统工程和业务应用信息系统工程。

业务应用信息系统工程就是为了达到建设好业务应用信息系统所组织实施的工程，一般成为信息系统集成项目工程。它是信息系统工程的一部分。

信息安全系统工程是指为了达到建设好信息安全系统的特殊需要而组织实施的工程。它是信息系统工程的一部分。信息安全系统工程作为信息系统工程的一个子集，其安全体系和策略必须遵从系统工程的一般性原则和规律。信息安全系统工程原理适用于系统和应用的开发、集成、运行、管理、维护和演变，以及产品的开发、交付和演变。这样，信息安全系统工程就能够在一个系统、一个产品或一个服务中得到体现。

我们讲述的是信息安全系统工程，而不是信息系统安全工程。从字面上理解，信息系统安全工程可能会误解为安全地建设一个信息系统，而忽略信息系统中的信息安全问题。因为信息系统可以安全地建设成一个没有信息安全子系统的信息系统，在目前国内仍然存在这样的新建的信息系统——没有考虑信息安全的问题，或没有充分地考虑信息安全的问题，从而留下相当大的隐患。信息安全系统工程就明白无误地确定了，这个工程就是建设一个信息安全系统。

22.2.2信息安全系统

信息安全保障系统一般简称为信息安全系统，它是“信息系统”的一个部分，用于保证“业务应用信息系统”正常运营。现在人们已经明确，要建立一个“信息系统”，就必须要建立一个或多个业务应用信息系统和一个信息安全系统。信息安全系统是客观的、独立于业务应用信息系统而存在的信息系统。

我们用一个“宏观”三维空间图来反映信息安全系统的体系架构及其组成，如图22-3所示。

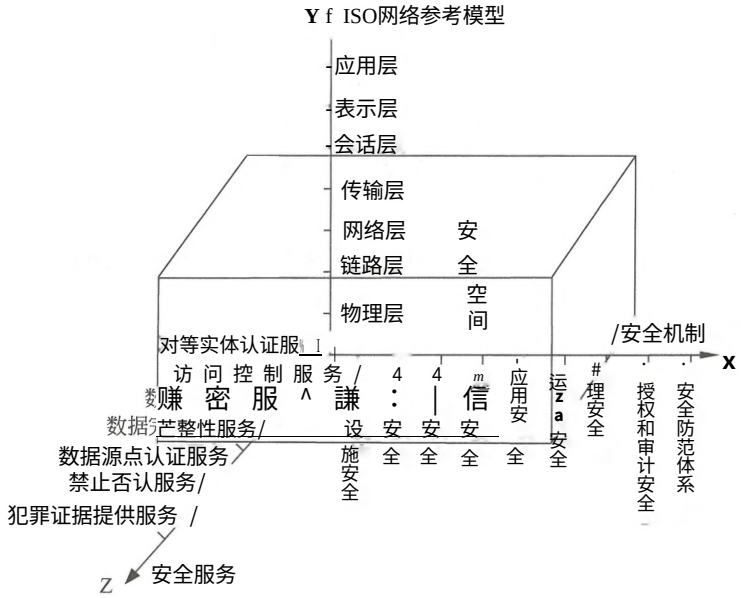


图22-3信息安全空间

X轴是“安全机制”。安全机制可以理解为提供某些安全服务，利用各种安全技术和技巧，所形成的一个较为完善的结构体系。如“平台安全”机制，实际上就是指的安全操作系统、安全数据库、应用开发运营的安全平台以及网络安全管理监控系统等。

Y轴是“OSI网络参考模型”。信息安全系统的许多技术、技巧都是在网络的各个层面上实施的，离开网络，信息系统的安全也就失去意义。

Z轴是“安全服务”。安全服务就是从网络中的各个层次提供给信息应用系统所需要的安全服务支持。如对等实体认证服务、访问控制服务、数据保密服务等。

由X、Y、Z三个轴形成的信息安全系统三维空间就是信息系统的“安全空间”。随着网络逐层扩展，这个空间不仅范围逐步加大，安全的内涵也就更丰富，达到具有认证、权限、完整、加密和不可否认五大要素，也叫作“安全空间”的五大属性。

1.安全机制

第一层：基础设施实体安全

(1) 机房安全，包括机房环境、包括机房环境、温度、湿度、电磁、噪声、防尘、静电和振动等。

(2) 场地安全，包括建筑安全、包括建筑安全、防火、防雷、围墙和门禁系统等。

(3) 设施安全，包括设备可靠性、通信线路安全性和辐射控制与防泄露等。

(4) 动力系统安全，包括电源安全和空调等。

(5) 灾难预防与恢复。

第二层：平台安全

(1) 操作系统漏洞检测与修复，包括Unix系统、Windows系统、Linux系统和网络协议等。

(2) 网络基础设施漏洞检测与修复，包括路由器、交换机和防火墙等。

(3) 通用基础应用程序漏洞检测与修复，包括数据库、Web、FTP、Email、DNS以及其他各种系统守护进程等。

(4) 网络安全产品部署，平台安全的实施需要用到市场上常见的网络安全产品，主要包括防火墙、入侵检测、脆弱性扫描和防病毒产品。

第三层：数据安全

(1) 介质与载体安全保护。

(2) 数据访问控制，包括系统数据访问控制检查、标识与鉴别等。

(3) 数据完整性。

(4) 数据可用性。

(5) 数据监控和审计。

(6) 数据存储与备份安全。

第四层：通信安全

(1) 通信线路和网络基础设施安全性测试与优化。

(2) 安装网络加密设施。

(3) 设置通信加密软件。

(4) 设置身份鉴别机制。

(5) 设置并测试安全通道。

(6) 测试各项网络协议运行漏洞。

第五层：应用安全

(1) 业务软件的程序安全性测试□Bug分析）。

(2) 业务交往的防抵赖测试。

(3) 业务资源的访问控制验证测试。

(4) 业务实体的身份鉴别检测。

(5) 业务现场的备份与恢复机制检查。

(6) 业务数据的唯一性、一致性和防冲突检测。

(7) 业务数据的保密性测试。

(8) 业务系统的可靠性测试。

(9) 业务系统的可用性测试。

第六层：运行安全

(1) 应急处置机制和配套服务。

(2) 网络系统安全性监测。

(3) 网络安全产品运行监测。

(4) 定期检查和评估。

(5) 系统升级和补丁提供。

(6) 跟踪最新安全漏洞及通报。

(7) 灾难恢复机制与预防。系统改造管理。

(8) 网络安全专业技术咨询服务。

第七层：管理安全

包括人员管理；培训管理；应用系统管理；软件管理；设备管理；文档管理；数据管理；操作管理；运行管理；机房管理。

第八层：授权和审计安全

授权安全是指以向用户和应用程序提供权限管理和授权服务为目标，主要负责向业务应用系统提供授权服务管理，提供用户身份到应用授权的映射功能，实现与实际应用处理模式相对应的、与具体应用系统开发和管理无关的访问控制机制。

审计安全是指：

·监控网络内部的用户活动。

·侦察系统中存在的潜在威胁。

·对日常运行状况的统计和分析。

·对突发案件和异常事件的事后分析。

·辅助侦破和取证。

·安全审计是信息安全系统必须支持的功能特性。

第九层：安全防范体系

企业安全防范体系的建立，就是使得企业具有较强的应急事故处理能力，其核心是实现企业信息安全资源的综合管理，即EISRM (Enterprise Information Security Resource Management) □ 企业安全防范体系的建立可以更好地发挥以下六项能力：预警□ Warn) 、保护□ Protect)、检测□ Detect)、反应□ Response)、恢复□ Recover)和反击□ Counter-attack) 6个环节，即综合的WPDRRC信息安全保障体系。

企业可以结合WPDRRC能力模型，从人员、技术、政策□包括法律、法规、制度、管理）三大要素来构成宏观的信息网络安全保障体系结构的框架，主要包括组织机构的建立、人员的配备、管理制度的制定、安全流程的明确等，并切实做好物理安全管理、中心机房管理、主机安全管理、数据库安全管理、网络安全管理、网络终端管理、软件安全管理，授权和访问控制管理、审计和追踪管理，确保日常和异常情况下的信息安全工作持续、有序地开展。

2.安全服务

(1) 对等实体认证服务。对等实体认证服务用于两个开放系统同等层中的实体建立链接或数据传输时，对对方实体的合法性、真实性进行确认，以防假冒。

(2) 数据保密服务。数据保密服务包括多种保密服务，为了防止网络中各系统之间的数据被截获或被非法存取而泄密，提供密码加密保护。数据保密服务可提供链接方式和无链接方式两种数据保密，同时也可对用户可选字段的数据进行保护。

(3) 数据完整性服务。数据完整性服务用以防止非法实体对交换数据的修改、插入、删除以及在数据交换过程中的数据丢失。数据完整性服务分为以下几个部分。

·带恢复功能的链接方式数据完整性。

·不带恢复功能的链接方式数据完整性。

·选择字段链接方式数据完整性。

·选择字段无链接方式数据完整性。

·无链接方式数据完整性。

(4) 数据源点认证服务。数据源点认证服务用于确保数据发自真正的源点，防止假冒。

(5) 禁止否认服务。禁止否认服务用以防止发送方在发送数据后否认自己发送过此数据，接收方在收到数据后否认自己收到过此数据或伪造接收数据，由两种服务组成：不得否认发送和不得否认接收。

(6)犯罪证据提供服务。

3.安全技术

1) 加密技术

加密是确保数据安全性的基本方法。在OSI安全体系结构中应根据加密所处的层次及加密对象的不同，而采用不同的密码。由于有加密技术的存在，必须有密钥管理技术的存在。在网络环境中，密钥管理显得格外重要。

2) 数字签名技术

数字签名是确保数据真实性的基本方法。利用数字签名技术还可以进行报文认证和用户身份认证。数字签名具有解决收发双方纠纷的能力，这是其他安全技术所没有的。

3) 访问控制技术

访问控制按照事先确定的规则决定主体对客体的访问是否合法。当一主体试图非法使用一个未经授权的资源时，访问控制将拒绝这一企图，并将这一事件报告给审计跟踪系统，审计跟踪系统将给出报警并记录日志档案。

4) 数据完整性技术

破坏数据的主要因素有：

数据在信道中传输时受信道干扰影响产生错误或是被非法侵入所篡改，或是被病毒所感染等。

数据完整性技术通过纠错编码和差错控制来应对信道干扰，通过报文认证来应对非法入侵者的主动攻击，通过病毒实时检测来应对计算机病毒。

数据完整性技术包括以下两种方式：数据单元的完整性和数据单元序列的完整性。

5) 认证技术

在计算机网络中认证主要有站点认证、报文认证、用户和进程认证等。多数认证过程采用密码技术和数字签名技术。对于用户身份认证，随着科技的发展，用户生物特征认证技术将得到越来越多的应用。在大型计算机网络中，由于有众多的用户，而且并不是所有的用户都诚实、可信，同时由于设备故障等技术原因造成信息丢失、延迟等，这很可能引起责任纠纷。为了解决这个问题，需要有一个各方都信任的第三者实体以提供公正仲裁。

6) 数据挖掘技术

随着高科技的发展，犯罪和不法之徒的手段也越来越高科技化，直截了当的犯罪我们好查，对于隐蔽的手法就需要新的高科技手段来对付，利用大量的数据积累和经验的积累，数据挖掘技术是及早发现隐患、将犯罪扼杀在萌芽阶段并及时修补不健全的安全防范体系的重要技术。

22.2.3信息安全系统架构体系

信息安全系统大体划分为三种架构体系：MIS+S系统、S-MIS系统和S^2-MIS系统。

1. **MIS+S** 系统

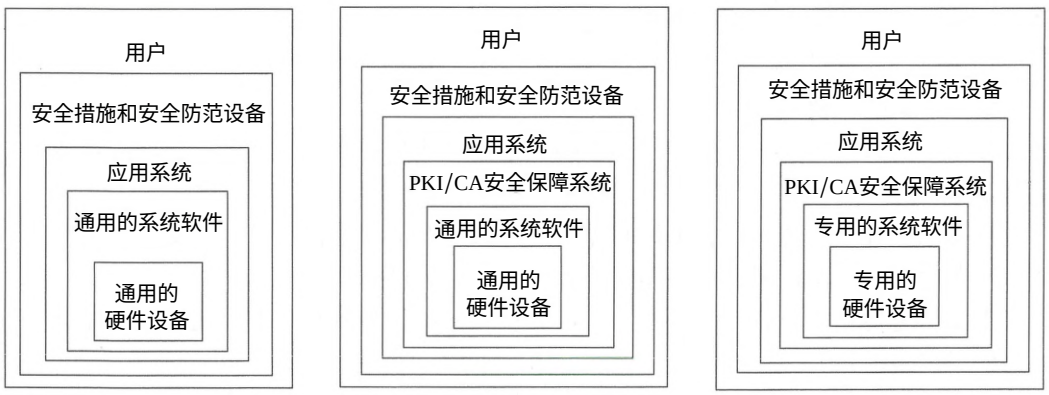
MIS+S (Management Information System+Security)系统为“初级信息安全保障系统”或“基本信息安全保障系统”。顾名思义，这样的系统是初等的、简单的信息安全保障系统。其特点如下。

·业务应用系统基本不变。

·硬件和系统软件通用。

·安全设备基本不带密码。

这里所说的“安全设备”主要是指那些在应用系统之外的信息安全设备，如防火墙、网络隔离、安全路由，以及病毒防治系统、漏洞扫描系统、入侵检测系统、动态口令卡等。不使用PKI/CA的VPN设备也属于这个范畴。这种系统的架构，如图22-4 (1)所示。



(1) MIS+S系统架构 (2) S-MIS系统结构 (3) S^2-MIS系统架构

图22-4系统架构示意图

2. **S-MIS**系统架构

S-MIS (Security- Management Information System)系统为“标准信息安全保障系统”。顾名思义，S-MIS系统一定是涉密系统，即系统中一定要用到密码和密码设备，一定是基于PKI/CA和PMI/AA建立的支撑用户的业务应用信息系统的运营。其特点如下：

·硬件和系统软件通用。

• PKI/CA安全保障系统必须带密码。

·业务应用系统必须根本改变。

·主要的通用的硬件、软件也要通过PKI/CA认证。

业务应用系统必须根本改变就是指业务应用系统必须按照PKI/CA的标准重新编制的全新的安全的业务应用信息系统。这种系统的架构，如图22-4 (2)所示。

3．**S^2-MIS**系统架构

S^2-MIS (Super Security-Management Information System)系统为“超安全的信息安全保障系统”。顾名思义，这样的系统是建立在“绝对的”安全的信息安全基础设施上的。它不仅使用世界公认的PKI/CA标准，同时硬件和系统软件都使用专用的、安全产品。主要的硬件和系统软件需要PKI/CA认证，可以说，这样的系统是集当今所有安全、密码产品之大成。其特点如下。

·硬件和系统软件都专用。

· PKI/CA安全基础设施必须带密码。

·业务应用系统必须根本改变。

这种系统的架构，如图22-4 (3)所示。

三种不同系统架构的信息安全保障系统适用于不同业务应用系统的需要。显然，建立三种不同系统架构的信息安全保障系统所需要的投资和完成的工期将有非常大的差别。建立一个MIS+S系统需要几十万元□RMB)的话，建立一个S-MIS系统需要几百万到几千万元，而建立一个S^2-MIS系统将需要更大的投资。当然，系统的安全保障的能力与效果也将完全不同。

信息安全系统与业务应用信息系统既有区别又有紧密联系。用户的业务应用信息系统生命周期与信息安全系统生命周期的关系几乎是一样的，因为它们是同步进行的。但是，它们在工程实施过程和工程保证过程则完全不同的。其中最大不同点是，信息安全系统从项目启动□立项）开始，需要严格保密的。一般情况下，不允许外单位人员参加。所有参加该项目的人员，不仅需要签订工程建设期间的保密协议，还要签订3~5年不泄密的保密协议。

此外，信息安全系统需要专业知识和技能，涉及到这样的信息系统集成项目，承建单位需要有特殊的资质。还有，从工程要求来看，信息安全系统工程的建设决不能与业务应用信息系统工程建设混为一谈。我们要切记，任何一个信息系统，必定要有两个系统的生命周期并存。虽然两者始终保持并存的关系，或者可能延续到正常运营和维护阶段结束之后，彼此仍然保持“并存”的关系，但是他们之间有明显的主次之分。信息安全保障系统永远是业务应用信息系统中起到支撑保障作用的一个重要组成部分，因此永远处于次要地位。没有了业务应用信息系统，也就没有了信息安全系统。信息安全系统的“天职”就是保障业务应用信息系统的安全。相反，没有了安全，业务应用信息系统也就不能正常地运营了。所以，虽然处于次要地位，确实不可缺少的。

22.2.4信息安全系统工程基础

1.信息安全系统工程与技术工程的关系

信息安全系统的建设是在OSI网络参考模型的各个层面进行的，因此信息安全系统工程活动离不开以下相关工程。

(1) 硬件工程。
(2) 软件工程。
(3) 通信及网络工程。
(4) 数据存储和灾备工程。
(5) 系统工程。
(6) 测试工程。
(7) 密码工程。
(8) 企业信息化工程。

信息安全系统建设是遵从企业/单位（组织）所制定的安全策略进行的。而安全策略由业主与业主的客户、集成商、安全产品开发者、密码研制单位、独立评估者和其他相关组织共同协商建立。因此信息安全系统工程活动必须要与其他外部实体进行协调。也正是因为信息安全系统工程存在着这些与其他工程的关系接口，而这些接口又遍布各种组织且具有相互影响，所以信息安全系统工程与其他工程相比就更加复杂。

2.信息安全系统工程与安全管理的关系

信息安全系统工程应该吸纳安全管理的成熟规范部分，这些安全管理包括：

(1) 物理安全。侧重于保护建筑物和物理场所的安全。
(2) 计算机安全。各种类型计算设备的安全保护。
(3) 网络安全。保护网络联结和数据传输的安全措施，包括网络硬件、软件和协议，以及在网络上传输的信息的安全。
(4) 通信安全。保护有关安全域之间的通信安全，特别是信息在传输介质上传输时的安全。
(5) 输入/输出产品的安全。保护与主机硬件和软件的安全、正常、稳定的连接和运行，防止外来的干扰和破坏。
(6) 操作系统安全。保护操作系统本身安全运营的安全措施和由操作系统提供给使用者的安全措施。
(7) 数据库系统安全。保护数据库管理系统本身安全运营的安全措施和由数据库管理系统提供给使用者的安全措施。
(8) 数据安全。保护在存储、操作和处理中的数据。
(9) 信息审计安全。保证审计信息和审计系统的安全运营，从而获得运行环境安全和安全运行态势维护。
(10) 人员安全。有关人员及其可信度保证，以及安全意识培训教育保证。
(11) 管理安全。有关安全管理和管理该系统的安全。
(12) 辐射安全。控制所有机器设备保证不将未期望的信号发射到安全域外部。

22.2.5信息安全系统工程体系结构

1. **ISSE-CMM** 概述

ISSE是一门系统工程学，它的主要内容是确定系统和过程的安全风险，并且使安全风险降到最低或使其得到有效控制。

信息安全系统工程能力成熟度模型 Information Security System Engineering Capability Maturity Model，ISSE-CMM)是一种衡量信息安全系统工程实施能力的方法，是使用面向工程过程的一种方法。ISSE-CMM是建立在统计过程控制理论基础上的。统计过程控制理论认为，所有成功企业的共同特点是它们都具有一整套严格定义、管理完善、可测可控的有效业务过程。ISSE-CMM模型抽取了这样一组“好的”工程实施并定义了过程的“能力”。主要用于指导信息安全系统工程的完善和改进，使信息安全系统工程成为一个清晰定义的、成熟的、可管理的、可控制的、有效的和可度量的学科。

ISSE-CMM模型是信息安全系统工程实施的度量标准，它覆盖了：

·整个生命期，包括工程开发、运行、维护和终止。

·管理、组织和工程活动等的组织。

·与其他规范如系统、软件、硬件、人的因素、测试工程、系统管理、运行和维护等规范并行的相互作用。

·与其他组织□包括获取、系统管理、认证、认可和评估组织）的相互作用。

1) ISSE-CMM主要概念

(1) 过程。过程□Process)是指为了达到某一给定目标而执行的一系列活动，这些活动可以重复、递归和并发地执行。

(2) 过程域。过程域 Process Area，PA)是由一些基本实施 Base Practices，BP)组成的，它们共同实施来达到该过程域规定的目标。这些基本实施是强制性的，因为只有它们全部成功地得到执行，才能满足过程域规定的目标。ISSE-CMM包含工程、项目和组织三类过程域。组织类与项目类过程域的差别仅仅是所有权的不同，项目过程域只针对一个特定的产品，而组织过程域则含有一个或多个项目。

(3) 工作产品。SSE-CMM中的工作产品□WorkProduct)系指在执行任何过程中产生出的所有文档、报告、文件和数据。

(4) 过程能力。过程能力 Process Capability)是通过跟踪一个过程能达到期望结果的可量化范围。

一个组织的过程能力可帮助组织预见项目达到目标的能力。位于低能力级组织的项目在达到预定的成本、进度、功能和质量目标上会有很大的变化，而位于高能力组织的项目则完全相反。

2) ISSE-CMM 的组织

ISSE-CMM 主要适用于工程组织 Engineering Organizations)、获取组织 Acquiring Organizations)和评估组织 Evaluation Organizations)。

(1) 信息安全的工程组织。信息安全工程组织包含系统集成商、应用开发商、产品提供商和服务提供商等。工程组织使用ISSE-CMM对工程能力进行自我评估。

(2) 信息安全的获取组织。信息安全的获取组织包含采购系统、产品，以及从外部/内部资源和最终用户处获取服务的组织，他们使用ISSE-CMM来判别一个供应者组织的信息安全系统工程能力，识别该组织供应的产品和系统的可信任性，以及完成一个工程的可信任性。

(3) 信息安全的评估组织。信息安全的评估组织包含认证组织、系统授权组织、系统和产品评估组织等，他们使用ISSE-CMM作为工作基础，以建立被评组织整体能力的信任度。

2. **ISSE**过程

ISSE过程的目的是使信息安全系统成为系统工程和系统获取过程整体的必要部分，从而有力地保证用户目标的实现，提供有效的安全措施以满足客户的需求，将信息系统安全的安全选项集成到系统工程中，去获得最优的信息安全系统解决方案。为了使信息安全系统具有可实现性并有效力，必须把信息安全系统集成在信息系统生命周期的工程实施过程中，并与业务需求、环境需求、项目计划、成本效益、国家和地方政策、标准、指令保持一致性。这种集成过程将产生一个信息安全系统工程□ISSE)过程，这一过程能够确认、评估、消除□或控制）已知的或假定的安全威胁可能引起的系统威胁□风险），最终得到一个可以接受的安全风险等级。在系统设计、开发和运行时，应该运用科学的和工程的原理来确认和减少系统对攻击的脆弱度或敏感性。ISSE并不是一个独立的过程，它依赖并支持系统工程和获取□保证）过程，而且是后者不可分割的一部分。

ISSE过程的目标是提供一个框架，每个工程项目都可以对这个框架进行裁剪以符合自己特定的需求。ISSE表现为直接与系统工程功能和事件相对应的一系列信息安全系统工程行为。

ISSE将信息安全系统工程实施过程分解为：工程过程 Engineering Process)、风险过程 Risk Process)和保证过程 Assurance Process)三个基本的部分，如图22-5所示。它们相互独立，但又有着有机的联系。这三个部分在IS)中的定义与我们面所介绍的完全吻合。粗略地说来，在风险过程中，人们识别出所开发的产品或系统的险，并对这些危险进行优先级排序。针对危险所面临的安全问题，信息安全系统工程过要与其他工程一起来确定安全策略和实施解决方案。最后，由安全保证过程建立起解决案的可信性并向用户转达这种安全可信性。

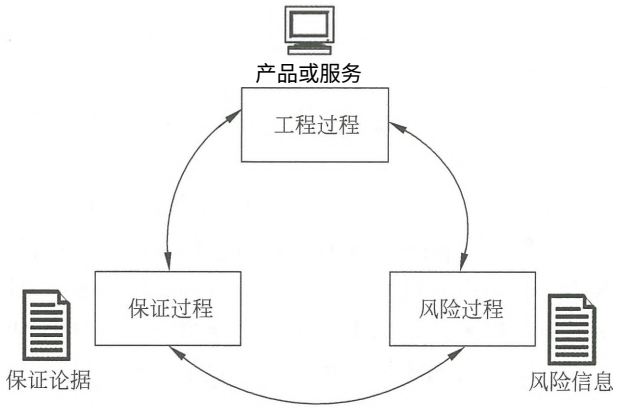


图 22-5 信息安全系统工程过程的组成部分

总的来说，这三个过程共同实现了信息安全系统工程过程结果所要达到的安全目标。

1)信息安全系统的工程过程

信息安全系统工程与其他工程活动一样，是一个包括概念、设计、实现、测试、部署、运行、维护、退出的完整过程，如图22-6所示。在这个过程中，信息安全系统工程的实施必须紧密地与其他的系统工程组进行合作。ISSE-CMM强调信息安全系统工程是一个大项目队伍中的组成部分，需要与其他科目工程的活动相互协调。这将有助于保证安全成为一个大项目过程中一个部分，而不是一个分离的独立部分。

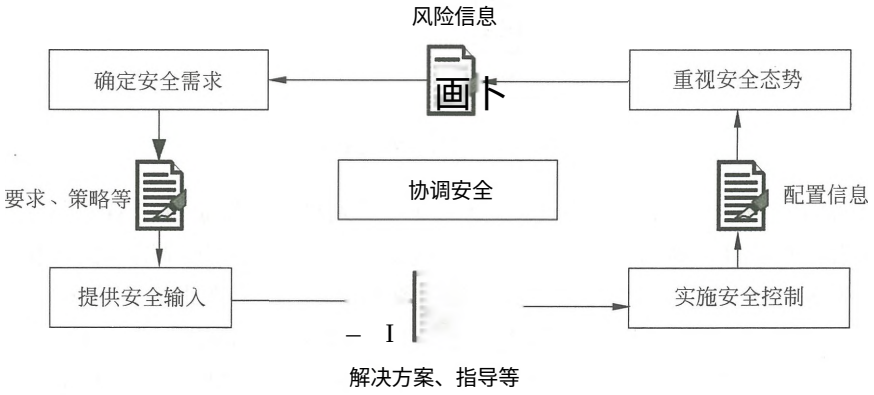


图22-6信息安全系统工程实施过程

使用上面所描述的风险管理过程的信息和关于系统需求、相关法律、政策的其他信息，信息安全系统工程就可以与用户一起来识别安全需求。一旦需求被识别，信息安全系统工程就可以识别和跟踪特定的安全需求。

对于信息安全问题，创建信息安全解决方案一般包括识别可能选择的方案，然后评估决定哪一种更可能被接受。将这个活动与工程过程的其他活动相结合，不但要解决方案的安全问题，还需要考虑成本、性能、技术风险、使用的简易性等因素。

2)信息安全系统的风险过程

信息安全系统工程的一个主要目标是降低信息系统运行的风险。风险就是有害事件发生的可能性及其危害后果。出现不确定因素的可能性取决于各个信息系统的具体情况。这就意味着这种可能性仅可能在某些限制条件下才可预测。此外，对一种具体风险的影响进行评估，必须要考虑各种不确定因素。因此大多数因素是不能被综合起来准确预报的。在很多情况下，不确定因素的影响是很大的，这就使得对安全的规划和判断变得非常困难。

一个有害事件由威胁、脆弱性和影响三个部分组成。脆弱性包括可被威胁利用的资产性质。如果不存在脆弱性和威胁，则不存在有害事件，也就不存在风险。风险管理是调查和量化风险的过程，并建立组织对风险的承受级别。它是安全管理的一个重要部分。风险管理过程，如图22-7所示。

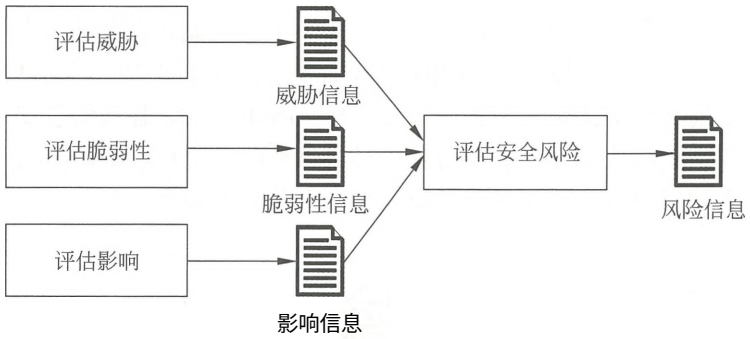


图22-7风险管理过程

安全措施的实施可以减轻风险口安全措施可针对威胁和脆弱性自身。但无论如何，不可能消除所有威胁或根除某个具体威胁。这主要是因为消除风险所需的代价，以及与风险相关的各种不确定性。因此，必须接受残留的风险。在存在很大不确定性的情况下，由于风险度量不精确的本质特征，在怎样的程度上接受它才是恰当的，往往会成为很大的问题。ISSE-CMM过程域包括实施组织对威胁、脆弱性、影响和相关风险进行分析的活动保证。

3)信息安全系统的保证过程

保证过程是指安全需求得到满足的可信程度，它是信息安全系统工程非常重要的产品，保证过程，如图22-8所示。保证的形式多种多样。ISSE-CMM的可信程度来自于信息安全系统工程实施过程可重复性的结果质量。这种可信性的基础是主程组织的成熟性，

成熟的组织比不成熟的组织更可能产生出重复的结果。

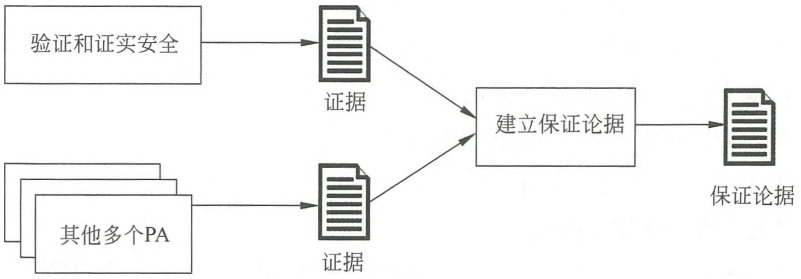


图22-8保证过程

安全保证并不能增加任何额外的对安全相关风险的抗拒能力，但它能为减少预期安全风险提供信心。安全保证也可看作是安全措施按照需求运行的信心。这种信心来自于措施及其部署的正确性和有效性。正确性保证了安全措施按设计实现了需求，有效性则保证了提供的安全措施可充分地满足用户的安全需求。安全机制的强度也会发挥作用，但其作用却受到保护级别和安全保证程度的制约。

3．**ISSE**体系结构

ISSE-CMM的体系结构完全适应整个信息安全系统工程范围内决定信息安全工程组织的成熟性。这个体系结构的目标是为了落实安全策略，而从管理和制度化突出信息安全工程的基本特征。为此，该模型采用两维设计，其中的一维是“域”□Domain)，另一维是“能力”□Capability)。

1）基本模型

域维汇集了定义信息安全工程的所有实施活动，这些实施活动称为过程域。能力维代表组织能力，它由过程管理能力和制度化能力构成。这些实施活动被称作公共特性，可在广泛的域中应用。执行一个公共特性是一个组织能力的标志。通过设置这两个相互依赖的维，ISSE在各个能力级别上覆盖了整个信息安全活动范围。

2）域维/安全过程域

ISSE包括6个基本实施，这些基本实施被组织成11个信息安全工程过程域，这些过程域覆盖了信息安全工程所有主要领域。安全过程域的设计是为了满足信息安全工程组织广泛的需求。划分信息安全工程过程域的方法有许多种。典型的作法之一就是将实际的信息安全工程服务模型化，即原型法，以此创建与信息安全工程服务相一致的过程域。其他的方法可以是识别概念域，它们将识别的这些域形成相应的基本信息安金工程构件模块。

每一个过程域包括一组表示组织成功执行过程域的目标。每一个过程域也包括一组集成的基本实施。基本实施定义了获得过程域目标的必要步骤。

一个过程域：

(1) 汇集一个域中的相关活动，以便于使用。

(2) 就是有关有价值的信息安全工程服务。

(3) 可在整个组织生命周期中应用。

(4) 能在多个组织和多个产品范围内实现。

(5) 能作为一个独立过程进行改进。

(6) 能够由类似过程兴趣组进行改进。

(7) 包括所有需要满足过程域目标的基本实施□BP)。基本实施的特性包括：

·应用于整个企业生命期。

·和其他BP互相不覆盖。

·代表安全业界“最好的实施”。

·不是简单地反映当前技术。

·可在业务环境下以多种方法使用。

·不指定特定的方法或工具。

由基本实施组成的11个安全工程过程域包括：

PA01—实施安全控制；PA02—评估影响；PA03—评估安全风险；PA04—评估威胁；PA05—评估脆弱性；PA06—建立保证论据；PA07—协调安全；PA08—监控安全态势；PA09—提供安全输入；PA10—确定安全需求；PA11—验证和证实安全。

ISSE-CMM还包括11个与项目和组织实施有关的过程域：PA12保证质量；PA13管理配置；PA14管理项目风险；PA15监测和控制技术工程项目；PA16规划技术工程项目；PA17定义组织的系统工程过程；PA18改进组织的系统工程过程；PA19管理产品线的演变；PA20管理系统工程支持环境；PA21提供不断更新的技能和知识；PA22与供应商的协调。

3)能力维/公共特性

通用实施 Generic Practices，GP)，由被称之为公共特性的逻辑域组成，公共特性分为5个级别，依次表示增强的组织能力。与域维基本实施不同的是，“能力”维的通用实施按其成熟性排序，因此高级别的通用实施位于能力维的高端。

公共特性设计的目的是描述在执行工作过程□此处即为信息安全工程域）中组织特征方式的主要变化。每一个公共特性包括一个或多个通用实施。通用实施可应用到每一个过程域□ISSE-CMM应用范畴），但第一个公共特性“执行基本实施”例外。其余公共特性中的通用实施可帮助确定项目管理好坏的程度并可将每一个过程域作为一个整体加以改进。

下面的公共特性表示了为取得每一个级别需满足的成熟的信息安全工程特性。

表 22-2

级 另IJ	公 共 特 性	通 用 实 施
Level 1 一非正规实施级	——执行基本实施	1.**U**: 执 行 过 程
Level 2 ——规划和跟踪级	——规划执行	2.1.1:为执行过程域分配足够资源 2.1.2:为开发工作产品和/或提供过程域服务指定责任人 2.1.3:将过程域执行的方法形成标准化和/或程序化文档 2.1.4:提供支持执行过程域的有关工具 2.1.5:保证过程域执行人员获得适当的过程执行方面的培训 2.1.6:对过程域的实施进行规划
	—-规范化执行	2.2.1:在执行过程域中，使用文档化的规划、标准和/或程序 2.2.2:在需要的地方将过程域的工作产品置于版本控制和配置管理之下
	——验证执行	2.3.1:验证过程与可用标准和/或程序的一致性 2.3.2:审计工作产品□验证工作产品遵从可适用标准和/或需求的情况)
	——跟踪执行	2.4.1:用测量跟踪过程域相对于规划的态势 2.4.2:当进程严重偏离规划时采取必要修正措施
Level 3 —— 充分定义级	——定义标准化过程	3.1.1:对过程进行标准化 3.1.2:对组织的标准化过程族进行裁剪
	——执行已定义的过程	3.2.1:在过程域的实施中使用充分定义的过程 3.2.2:对过程域的适当工作产品进行缺陷评审 3.2.3:通过使用已定义过程的数据管理该过程
	—— 协调安全实施	3.3.1:协调工程科目内部的沟通 3.3.2:协调组织内不同组间的沟通 3_3.3:协调与外部组间的沟通
Level 4 ——里化控制级	——建立可测度的质量目标	4.1.1:为组织标准过程族的工作产品建立可测度的质量目标
	——对执行情况实施客观管理	4.2.1:量化地确定已定义过程的过程能力 4.2.2:当过程未按过程能力执行时，适当地采取修正行动
Level 5 一持续改进级	——改进组织能力	5.1.1:为改进过程效能，根据组织的业务目标和当前过程能力建立量化目标 5.1.2:通过改变组织的标准化过程，从而提高过程效能
	——改进过程的效能	5.2.1:执行缺陷的因果分析 5.2.2:有选择地消除已定义过程中缺陷产生的原因 5.2.3:通过改变已定义过程来连续的改进实施

4)能力级别

将通用实施划分为公共特性，将公共特性划分为能力级别有多种方法。

公共特性的排序得益于对现有其他安全实施的实现和制度化，特别是当实施活动有效建立时尤其如此。在一个组织能够明确地定义、裁剪和有效使用一个过程前，单独执行的项目应该获得一些过程执行方面的管理经验。例如，一个组织应首先尝试对一个项目规模评估过程后，再将其规定为这个组织的过程规范。有时，当把过程的实施和制度化放在一起考虑可以增强能力时，则无须要求严格地进行前后排序。

公共特性和能力级别无论在评估一个组织过程能力还是改进组织过程能力时都是重要的。当评估一个组织能力时，如果这个组织只执行了一个特定级别的一个特定过程的部分公共特性时，则这个组织对这个过程而言：处于这个级别的最底层。例如，在2级能力上，如果缺乏跟踪执行公共特性的经验和能力，那么跟踪项目的执行将会很困难。

如果高级别的公共特性在一个组织中实施，但其低级别的公共特性未能实施，则这个组织不能获得该级别的所有能力带来的好处。评估组织在评估一个组织个别过程能力时，应对这种情况加以考虑。

当一个组织希望改进某个特定过程能力时，能力级别的实施活动可为实施改进的组织提供一个“能力改进路线图”。基于这一理由，ISSE-CMM的实施按公共特性进行组织，并按级别进行排序。

对每一个过程域能力级别的确定，均需执行一次评估过程。这意味着不同的过程域能够或可能存在不同的能力级别上。组织可利用这个面向过程的信息，作为侧重于这些过程改进的手段。组织改进过程活动的顺序和优先级应在业务目标里加以考虑。

业务目标是如何使用ISSE-CMM模型的主要驱动力。但是，对典型的改进活动，也存在着基本活动次序和基本的原则。这个活动次序在ISSE-CMM结构中通过公共特性和能力级别加以定义。

能力级别代表工程组织的成熟度级别，如图22-9所示，5个级别的基本内容概述如下。

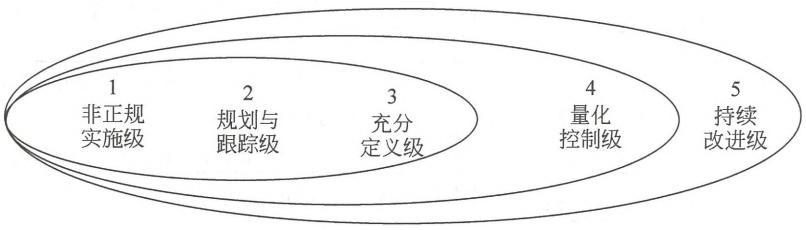


图22-9能力级别代表工程组织的成熟度级别的5级模型

五级能力级别的重点及能力特点如表22-3所示。

表22-3能力级别的重点与能力特点

级 另lj	重　　点	能 力 特 点
1级 —— 非正规实施级	着重于一个组织或项目只是执行了包含基本实施的过程	必须首先做它，然后才能管理它
2级 ——规划和跟踪级	着重于项目层面的定义、规划和执行问题	在定义组织层面的过程之前，先要弄清楚与项目相关的事项
3级 —— 充分定义级	着重于规范化地裁剪组织层面的过程定义	这个级别的能力特点可描述为：用项目中学到的最好的东西来定义组织层面的过程
4级 ——量化控制级	着重于测量。测量是与组织业务目标紧密联系在一起的。尽管在以前的级别上，也把数据收集和采用项目测量作为基本活动，但只有到达高级别时，数据才能在组织层面上被应用	只有知道它是什么，才能测量它和当被测量的对象正确时，基于测量的管理才有意义
5级 —— 持续改进级	从前面各级的所有管理活动中获得发展的力量，并通过加强组织的文明保持这种力量。这一方法强调文明的转变，这种转变又将使方法更有效	持续性改进的文明需要以完备的管理实施、己定义的过程和可测量的目标作为基础

22.3 PKI公开密钥基础设施

22.3.1公钥基础设施□PKI)基本概念

1. **PKI**的总体架构

公钥基础设施PKI (Public Key Infrastructure,公开密钥基础设施）是以不对称密钥加密技术为基础，以数据机密性、完整性、身份认证和行为不可抵赖性为安全目的，来实施和提供安全服务的具有普适性的安全基础设施。其内容包括数字证书、不对称密钥密码技术、认证中心、证书和密钥的管理、安全代理软件、不可否认性服务、时间邮戳服务、相关信息标准、操作规范等。

一个网络的PKI包括以下几个基本的构件。

数字证书：这是由认证机构经过数字签名后发给网上信息交易主体□企业或个人、设备或程序）的一段电子文档。在这段文档中包括主体名称、证书序号、发证机构名称、证书有效期、密码算法标识、公钥和私钥信息和其他属性信息等。利用数字证书，配合相应的安全代理软件，可以在网上信息交易过程中检验对方的身份真伪，实现信息交易双方的身份真伪，并保证交易信息的真实性、完整性、机密性和不可否认性。数字证书提供了 PKI的基础。

认证中心：CA (Certification Authority)是PKI的核心。它是公正、权威、可信的第三方网上认证机构，负责数字证书的签发、撤销和生命周期的管理，还提供密钥管理和证书在线查询等服务。

数字证书注册审批机构：RA (Registration Authority)系统是CA的数字证书发放、管理的延伸。它负责数字证书申请者的信息录入、审核以及数字证书发放等工作，同时，对发放的数字证书完成相应的管理功能。发放的数字证书可以存放于1C卡、硬盘或软盘等介质中。RA系统是整个CA中心得以正常运营不可缺少的一部分。

数字签名：利用发信者的私钥和可靠的密码算法对待发信息或其电子摘要进行加密处理，这个过程和结果就是数字签名。收信者可以用发信者的公钥对收到的信息进行解密从而辨别真伪。经过数字签名后的信息具有真实性和不可否认□抵赖）性。

密钥和证书管理工具：管理和审计数字证书的工具，认证中心使用它来管理在一个CA上的证书。

双证书体系：PKI采用双证书体系，非对称算法支持RSA和ECC算法，对称密码算法支持国家密码管理委员会指定的算法。

PKI的体系架构：宏观来看，PKI概括为两大部分，即信任服务体系和密钥管理中心。

PKI信任服务体系，是为整个业务应用系统□如电子政务、电子商务等）提供基于PKI数字证书认证机制的实体身份鉴别服务，它包括认证机构、注册机构、证书库、证书撤销和交叉认证等。

PKI密钥管理中心 Key Management Center，KMC)提供密钥管理服务，向授权管理部门提供应急情况下的特殊密钥回复功能。它包括密钥管理机构、密钥备份和恢复、密钥更新和密钥历史档案等。PKI的体系架构，如图22-10所示。国家PKI组织结构示意图，如图22-11所示。

2.双证书、双密钥机制

一对密钥□一张证书）应用中的问题：

如果密钥不备份，当密钥损坏□或管理密钥的人员离职时带走密钥）时，以前加密的信息不可解密。

如果密钥不备份，很难实现信息审计。 ■

如果密钥不备份，数字签名的不可否认性很难保证。

两对密钥□两张证书）的客观需求；一对密钥用于签名□签名密钥对），一对密钥用于加密□加密密钥对）。加密密钥在密钥管理中心生成及备份，签名密钥由用户自行生成并保存。

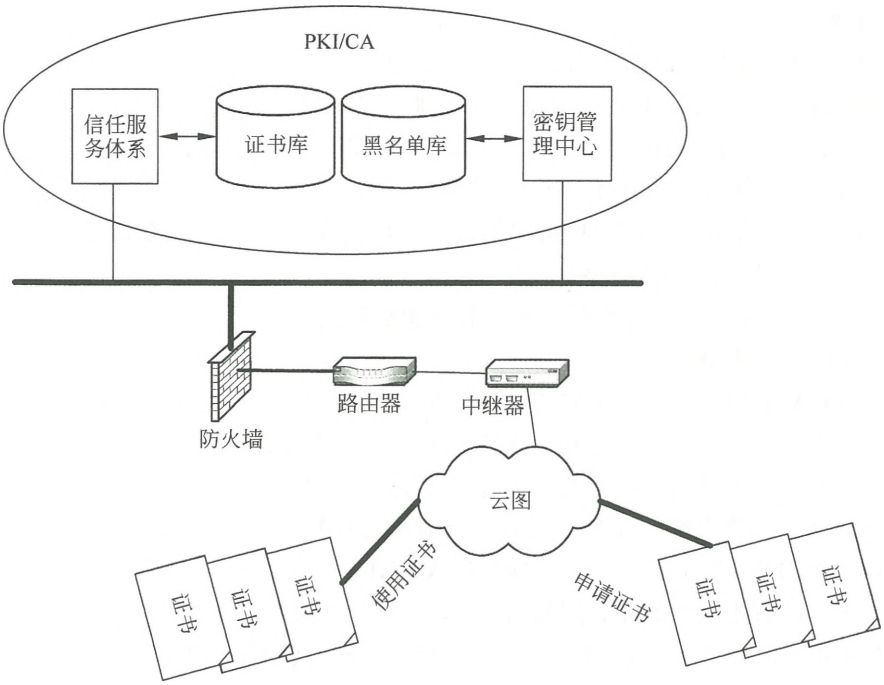


图22-10 **PKI/CA**认证体系架构示意图

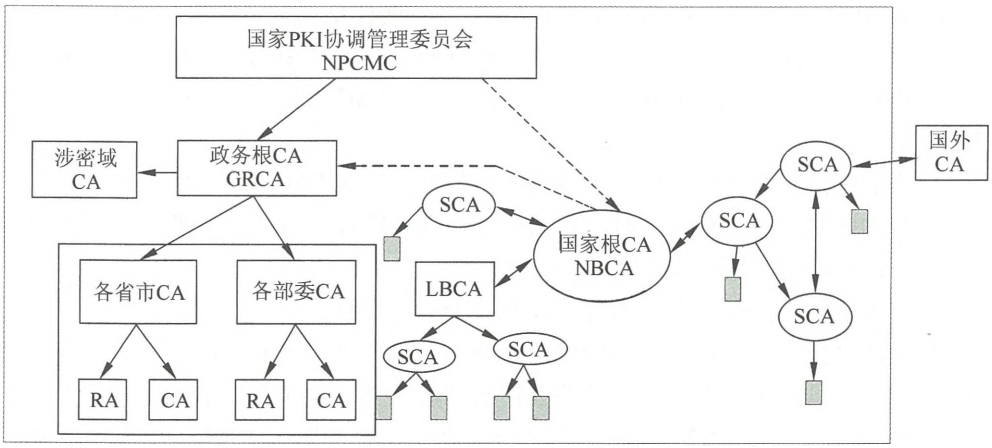


图22-11国家**PKI**组织结构示意图

3.双密钥证书的生成过程

(1) 用户使用客户端产生签名密钥对。

(2) 用户的签名私钥保存在客户端。

(3) 用户将签名密钥对的公钥传送给CA中心。

(4) CA中心为用户的公钥签名，产生签名证书。

(5) CA中心将签名证书传回客户端进行保存。

(6) KMC（密钥管理中心）为用户生成加密密钥对。

(7) 在KMC中备份加密密钥以备以后进行密钥恢复。

(8) CA中心为加密密钥对生成加密证书。

(9) CA中心将用户的加密私钥和加密证书打包成标准格式PKCS#12。

(10) 将打包后的文件传回客户端。

(11) 用户的客户端装入加密公钥证书和加密私钥。

4. X.509证书标准

在PKI/CA架构中，一个重要的标准就是X.509标准，数字证书就是按照X.509标准制作的。本质上，数字证书是把一个密钥对□明确的是公钥，而暗含的是私钥）绑定到一个身份上的被签署的数据结构。整个证书有可信赖的第三方签名。典型的第三方即大型用户群体□如政府机关或金融机构）所信赖的CA。

此外，X.509标准还提供了一种标准格式CRL。

目前X.509有不同的版本，例如X.509V2和X.509V3都是目前比较新的版本，但都是在原有版本□X.509V1)的基础上进行功能的扩充，其中每一版本必须包含下列信息。

(1) 版本号：用来区分X.509的不同版本号。

(2) 序列号：由CA给每一个证书分配唯一的数字型编号，当证书被取消时，实际上是将此证书的序列号放入由CA签发的CRL中，这也是序列号唯一的原因。

(3) 签名算法标识符；用来指定用CA签发证书时所使用的签名算法。算法标识符用来指定CA签发证书时所使用的公开密钥算法和HASH算法，需向国际指明标准组织(如ISO)注册。

(4) 认证机构：即发出该证书的机构唯一的CA的X.500规范用名。

(5) 有效期限：证书有效的时间包括两个日期，即证书开始生效期和证书失效的日期和时间，在所指定的这两个时间之间有效。

(6) 主题信息：证书持有人的姓名、服务处所等信息。

(7) 认证机构的数字签名；以确保这个证书在发放之后没有被改过。

(8) 公钥信息：包括被证明有效的公钥值和加上使用这个公钥的方法名称。

X.509标准第三版在V2的基础上进行了扩展，V3引进一种机制。这种机制允许通过标准化和类的方式将证书进行扩展以包含额外的信息，从而适应下面的一些要求。

一个证书主体可以有多个证书。

证书主体可以被多个组织或社团的其他用户识别。

可按特定的应用名□不是X.500规范用名）识别用户，如将公钥同E-mail地址联系起来。

在不同证书政策和实用下会发放不同的证书，这就要求公钥用户要信赖证书。

5. 公开密钥证书的标准扩展

公开密钥证书并不限于以下所列出的这些标准扩展，任何人都可以向适当的权利机构注册一种扩展。将来会有更多的适于应用的扩展列入标准扩展集中。值得注意的是这种扩展机制应该是完全可以继承的。

公开密钥证书的标准扩展可以分为以下几组。

·密钥和政策信息，包括机构密钥识别符、主体密钥识别符、密钥用途□如数字签字，不可否认性、密钥加密、数据加密、密钥协商、证书签字、CRL签字等）、密钥使用期限等。

·主体和发证人属性，包括主体代用名、发证者代用名、主体检索属性等。

·证书通路约束，包括基本约束，指明其他的证书认证机构。

·与CRL有关的补充。

6. 数字证书的主要内容

数字证书是公开密钥体制的一种密钥管理媒介。它是一种权威性的电子文档，形同网络计算环境中的一种身份证，用于证明某一主体□如人、服务器等）的身份及其公开密钥的合法性。在使用公钥体制的网络环境中，必须向公钥的使用者证明公钥的真实合法性。

因此，在公钥体制环境中，必须有一个可信的机构来对任何一个主体的公钥进行公证，证明主体的身份以及它与公钥的匹配关系。数字证书的主要内容，如表22-4所示。

表22-4数字证书的主要内容

字 段	定 义	举 例
主题名称	唯一标识证书所有者的标识符	**C=CN**，0=**CCB**，**OU=IT**
签证机关名称□**CA**)	唯一标识证书签发者的标识符	**C=CN**，0=**CCB**，**CN**： **CCB**
主体的公开密钥	证书所有者的公开密钥	1024位的**RSA**密钥
CA的数字签名	**CA**对证书的数字签名，保证证书的权威性	用**MD**5压缩过的**RSA**加密
有效期	证书在该期间内容有效	不早于 2000.1.1 19:00:00 不迟于 2002.1.1 19:00:00
序列号	**CA**产生的唯一性数字，用于证书管理	01:09:00:08:00
用途	主体公钥的用途	验证数字签名

在表22-4中，CA的数字签名保证了数字证书□实质是持有者的公钥）的合法性和权威性。主体□用户）的公钥可有两种产生方式。

(1) 用户自己生成密钥对，然后将公钥以安全的方式传送给CA，该过程必须保证用户公钥的可验证性和完整性。

(2) CA替用户生成密钥对，然后将其以安全的方式传送给用户，该过程必须确保密钥对的机密性、完整性和可验证性。该方式下由于用户的私钥为CA生成，故对CA的可信性有更高的要求。

用户A可通过两种方式获取用户B的数字证书和公钥，一种是由B将数字证书随同发送的正文信息一起传送给A,另一种是所有的数字证书集中存放子一个数字证书库中，用户A可从该地点取得B的数字证书。

CA的公钥可以存放在所有节点处，方便用户使用。

表22-4中的“用途”是一项重要的内容，它规定了该数字证书所公证的公钥的用途。公钥必须按规定的用途来使用。一般地，公钥有两大类用途。

(1) 用于验证数字签名。消息接收者使用发送者的公钥对消息的数字签名进行验证。

(2) 用于加密信息。消息发送者使用接收者的公钥加密用于加密消息的密钥，进行数据加密密钥的传递。

相应地，系统中需要配置用于数字签名/验证的密钥对和用于数据加密/解密的密钥对，这里分别称为签名密钥对和加密密钥对。这两对密钥对于密钥管理有不同的要求：

(1) 签名密钥对。签名密钥对由签名私钥和验证公钥组成。签名私钥具有日常生活中公章、私章的效力，为保证其唯一性，签名私钥绝对不能够作备份租存档，丢失后只需重新生成新的密钥对，原来的签名可以使用旧公钥的备份来验证。验证公钥需要存档、用于验证旧的数字签名。用作数字签名的这一对密钥一般可以有较长的生命期。

(2) 加密密钥对。加密密钥对由加密公钥和解密私钥组成，为防止密钥丢失时丢失数据，解密私钥应该进行备份，同时还可能需要进行存档，以便能在任何时候解密历史密文数据。加密公钥无须备份和存档，加密公钥丢失时，只需重新产生密钥对。

加密密钥对通常用于分发会话密钥，这种密钥应该频繁更换，故加密密钥对的生命周期较短。

不难看出，这两对密钥的密钥管理要求存在互相冲突的地方，因此，系统必须针对不同的用途使用不同的密钥对，尽管有的公钥体制算法，如目前使用广泛的RSA，既可以用于加密，又可以用于签名，在使用中仍然必须为用户配置两对密钥、两张数字证书，其一用于数字签名，另一个用于加密。

RA提供CA和用户之间的交互界面，它捕获和确认用户身份并提交数字证书请求给CA。CA决定用户的信任级别，确认过程的质量存放在数字证书中。

22.3.2数字证书及其生命周期

1．**PKI/CA**对数字证书的管理

PKI/CA对数字证书的管理是按照数字证书的生命周期实施的，包括证书的安全需求确定、证书申请、证书登记、分发、审计、撤回和更新。

映射证书到用户的账户是使数字证书的拥有者安全使用制定的应用所必不可少的环节，也是PKI/CA对数字证书管理的重要内容。

CA是一个受信任的机构，为了当前和以后的事务处理，CA给个人、计算机设备和组织机构颁发证书，以证实它们的身份，并为他们使用证书的一切行为提供信誉的担保。

2.数字证书的生命周期

下面分别介绍数字证书的生命周期的各个阶段。

阶段一：安全需求确定。为了确定PKI数字证书的安全需求，必须完成以下工作。

(1) 标识需要证书的应用程序。在单位内部，确定与把信息暴露给非授权的用户相关的风险。例如，当交换机密数据时，一项业务可能正在保护商业伙伴之间的电子邮件消息。

(2) 确定所需要的安全级别。选择所需要的安全级别来保护信息的完整性和保密性需要考虑的因素是私有密钥的长度、加密技术的算法、证书的生命周期和再生周期。例如，使用一个较长的私有密钥和一个较短的证书生命周期来为高价值的信息提供安全性。

(3) 标识需要证书的用户、计算机和服务。标识用户、计算机和服务，它们将参与信息的安全交换。例如，确定来自外部伙伴的哪个用户将访问一个内部存货数据库。

(4) 确定如何保护私有密钥。选择所需要的安全级别来保护私有密钥。选项包括在用户的简档里储存私有密钥，或者为了改善安全性，也包括要求使用智能卡储存私有密钥。

阶段二：证书登记。为了参与一个PKI，用户和计算机必须申请和接收来自CA的证书。申请和接收一个证书的过程称为登记。通常，通过提供独一无二的信息和一个新生成的公开密钥，一个用户启动登记过程。在颁发证书之前，CA使用已提供的信息来验证用户的身份。

申请和颁发一个证书的过程随着CA及其策略的变化而变化，但是总的来说这个过程可以划分为以下步骤。

(1) 生成一个密钥对。申请人制定一个公开和私有密钥对，或者由单位给申请人分配一个密钥对。

(2) 收集登记信息。申请人给CA提供颁发证书所需要的信息。例如，这些信息可能包括用户的名字和电子邮件地址，或者包括一个出生证、指纹、公证文档，或者CA需要确认申请人身份的其他任何信息。

(3) 申请证书申请人发送一个证书申请，它包括用户的公开密钥和另外所需要的信息。

(4) 用CA的公开密钥对申请进行加密，然后把加密的申请发送给CA。

(5) 验证信息。CA使用它所需要的任何策略规则，来确定是否给申请人颁发证书。正如身份验证请求一样，CA的验证策略和程序影响了证书生成的可信度，这些证书是由CA颁发的。

(6) 创建证书。CA创建和签署一个数字文档，此文档包含申请人的公开密钥和其他适当的信息。CA的签署使主体名字和主体公开密钥的结合生效。签署过的文档就是证书。

(7) 发送或邮寄证书。CA发送证书给申请人，或者邮寄证书给申请人。

阶段三：证书分发。当用户向一个企业CA提交证书请求时，请求会立即得到处理，因为企业CA使用活动目录来验证用户。证书请求或者立即被拒绝，或者立即给予批准。如果批准的话，就颁发证书，而且提示用户安装它。

用户可以使用证书申请向导来申请一个证书。证书申请向导允许用户根据用户的访问权力在不同的证书类型中进行选择。

阶段四：证书撤回。当一些与安全有关的事情，如解除与其他公司的合伙关系，在这种情形下某个证书继续有效是不合适的，那么就需要撤回那个证书。

如果发生以下情况时，需要撤回证书：

·破坏了颁发证书的CA的安全。

·证书的接受者离开了单位，或者接受者的雇用状态已发生重大变化。

·破坏了证书的私有密钥□例如，一个丢失的智能卡）。

·通过欺骗的方式得到一个证书。

·证书颁发给某个人，但是此人不再是一个受信任的伙伴。

需要强调一点：CRL不会撤回客户机上的所有的证书，仅仅撤回CRL中指定的证书。

CA证书服务支持使用行业标准的CRLs来公布关于撤回的证书的信息。认证机构在网络上公布CRL列表，或把它存储在活动目录中，用户和计算机都能够检索它；然后用户和计算机把CRL储存在他们当地的高速缓冲存储器中。

公布CRL列表必须在需求和冲突之间建立平衡。需求是指尽可能及时地公布CRL信息，而冲突是指公布CRL列表增加了网络通信量和服务器的负载。频繁的CRL公布使证书状态的变化能够很快地被人知道，但是也增加了服务器的负载，网给通信也受到影响。因为每当CRL到期和重新公布时，客户都需要下载CRL，注意：如果不能够得到CRL，那么就不能够验证证书，而且访问也将会被拒绝。‘

阶段五：证书更新。所有的证书，包括那些颁发给CA和用户的证书，都有一个有限的生命周期。当一个证书达到它的截止日期时，它自动变得无效，而且不能够再使用。需要用有效的日期重新颁发或更新一个到期的证书。

(1) 规划CA证书的生命周期。当CA给一个用户或计算机颁发一个证书时，CA确保新证书的有效期在CA自己证书的有效期内。这意味着，如果CA证书的有效期只剩六个月，那么CA颁发的新证书的最长有效期是六个月。

用户必须确保CA证书有一个足够长的生命期，这样就不需要太频繁地更新CA颁发的证书。过多的更新证书可能会给用户添加额外的负担。不论证书在何时到期，用户都需要与CA联系，申请一个新的证书，因为用户需要获得已经更新的证书。

(2) 规划证书更新。– 个发行CA直接给用户颁发证书，而不是颁发给其他CA发行的CA负责管理更多的证书，这些证书比一个只给CA颁发证书的CA管理的证书还多。通常用一个新的密钥频繁地更新一个CA的证书，对任何一个密钥的攻击，对攻击

者的价值就降低，对单位PKI的伤害就更少。

阶段六：证书审计。使用审计来监控活动，这些活动与证书服务器上证书的颁布有关。

每个CA维护一个审计踪迹，可以在认证机构管理控制台□MMC)上观察这个踪迹。审计踪迹记录了所有的证书请求，也记录了已经颁发了的而目前仍然有效的证书。审计踪迹记录所有的事务处理，包括失败的请求，也包括所有的信息，这些信息包含在每个已经颁发的证书中。认证机构MMC控制台有能力撤回证书，并且把撤回的证书添加到撤回列表中。

一个审计踪迹可能需要满足CA和单位的安全义务。用户能够查询审计踪迹，从而定位和查看有关的信息，这些信息是关于任何证书申请的信息或CA已颁发的任何证书的信息。例如，如果把已颁发的证书用于非法活动或欺诈性的事务，那么可能需要用户向安全人员或法律人员提供活动的记录。

除此之外，用户也可能需要用审计踪迹记录来监控破坏网络安全的行为。例如，用户能够观察审计踪迹，从而探测失败的证书申请，或确定某人是否用不正确的方法获得证书的。

注意：经过授权，用户能够通过使用认证机构网络接口来查看CA证书服务日志和数据库的内容。

3.映射证书到用户的账户

证书映射为使用者使用数字证书进行实际的应用操作提供了安全的、实际的“交接认证”工作。没有使用数字证书时，使用者进行应用操作时，通过用户ID和口令进入应用程序，但那不能使用PKI提供的安全性，此安全性是以用户对一个有效身份验证的证书的所有权为基础的。证书到用户账户的映射可以分为一对一映射和多对一映射。

单位可能需要支持外部用户的身份验证。这些用户在活动目录中没有账户。以用户对一个有效身份验证的证书的所有权为基础，此证书是从单位外部获得的。证书映射允许单位给用户提供访问权。

当启用证书映射时，根据那些映射的证书的权限在活动目录中对用户进行身份验证并且根据身份验证，授予用户特权和权限。可以用以下方法来配置证书映射。

·把一个证书映射到一个用户账户中。

·使用映射的用户账户对用户进行身份验证。

·用户接受由用户账户允许的特权和权限。

一对一映射创建从个人证书到相应的应用里用户账户的关系。能够把证书映射到用户的账户中，这样就能够授予证书持有者特权和权限。在一对一证书映射中可以在由一个用户所拥有的个人证书与相应的应用里一个相应的用户账户之间，创建一种关系。在证书被映射到相应的应用的用户账户中后，根据已映射的相应的应用的用户账户，对证书的持有者进行身份验证。身份验证之后，给用户授予得到映射的用户账户允许的特权

和权限。

与管理多对一的映射相比，手工管理里一对一的映射将需要完成更多的管理工作。当客户数目相对很小时，使用一对一映射。

如果对很多客户使用一对一的映射，那么考虑通过使用有效服务器页□ASP)技术来开发顾客Web登记页，以自动管理映射过程。

多对一映射为所有的证书创建从一个特定CA到一个应用的用户账户的关系。能够把多个证书映射到一个用户的账户中，这样就能够授予证书持有者对资源的特权和权限。

(1) 把由一个CA颁发的所有证书映射到一个用户账户中。

(2) 使用映射的用户账户对用户进行身份验证。

(3) 用户接受经过用户账户允许的特权和权限。

多对一的证书映射把来自一个CA的所有证书映射到相应的应用中的一个用户账户中。对于接受了来自CA的证书的任何一个用户，多对一映射允许给他们授予访问权，此访问权分配给相应的应用的用户账户。

有些用户可能需要访问网络上的一个给定的资源，例如内部Web站点。当对许多这样的用户进行身份验证时，多对一的映射是很有用的。必须把给那些用户颁发证书的CA安装成自己站点、域、组织单元□0U)或目录树上的一个可信任的根，然后设置规则，此规则把由CA颁发的所有的证书都映射到相应的应用中的一个用户账户中。

设置映射规则，此规则检查包含在用户证书中的信息，例如用户的单位和发行CA，从而确定信息是否与规则中的标准相匹配。当用户证书中的信息与规则相匹配时，把用户映射到一个指定的用户账户中。设置在用户账户上的权限将应用与所有的用户，这些用户拥有由受信任的CA所颁发的证书。

对那些可能需要访问用户网络上资源的不同的群体，可以使用不同的多对一证书映射。可以配置用户账户，使其根据客户对有效证书的所有权而授予不同的特权和权限，那些有效证书与映射规则相匹配，例如，可以把单位雇员映射到一个用户账户，它只允许雇员阅读整个Web站点。然后，把顾问和商业伙伴的雇员映射到其他的用户账户，此账户只允许他们访问非机密的信息和经过选择的专有信息。

22.3.3信任模型

1.信任的概念

X.509规范中给出了适于我们目标的定义：如果实体A认为实体B严格地按A所期望的那样行动，则A信任B。因此，信任涉及假设、预期和行为。这明确地意味着信任是不可能被定量测量的，信任是与风险相联系的，而且信任的建立不可能总是全自动的。然而信任模型的概念是有用的，因为它显示了 PKI中信任最初是怎样建立的，允许人们对基础结构的安全性以及被这种结构所强加的种种限制进行更详尽的推理，以确定PKI的可信任程度。在PKI上下文中，前面的定义能够如下应用：如果一个终端实体假设

CA能够建立并维持一个准确地对公钥属性的绑定□例如，准确地指出发给对方-证书-实体的身份），则该实体信任该CA，或者说该CA是可信任的CA。

词语“信任”同样还通过另一种有用的方式频繁使用，PKI文献经常提到所谓的可信公钥。这个短语并不描述关于行为的假设和预期，它是前面语义的推理结果。比如，Alice相信某一公钥/私钥正当、有效，并能确定是被某一特定的实体所拥有，则Alice就可说该公钥是可信的。该实体的名字或鉴别的信息是在证书中与公钥一起出现的，但是Alice也可以通过其他方式知道该名字，例如，它可以是根CA的身份，而Alice是被该根CA初始化进入PKI的用户。

2. **PKI/CA**的信任结构

1)层次信任结构

认证机构□CA)的严格层次结构可以描绘为一倒转的树，根在顶上，树枝向下伸展，树叶在下面。在这倒转的树上，根代表一个对整个PKI域内的所有实体都有特别意义的CA，通常被叫作根CA，其作为信任的根或“信任锚”。在根CA的下面是零层或多层中间CA（也被称作子CA，因为它们是从属于根的），这些CA由中间节点代表，从中间节点再伸出分支。与非CA的PKI实体相对应的树叶通常被称作终端实体或简称为终端用户，如图22-12所示。

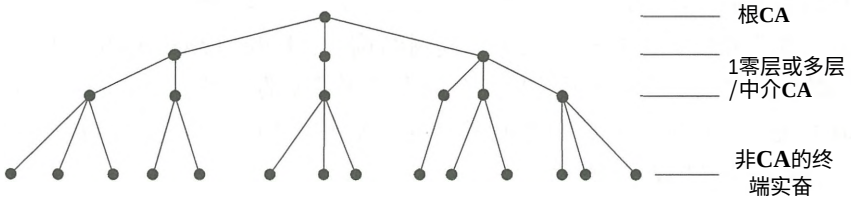


图22-12 **CA**的严格的层次模型

术语“根”通常被想象为在图22-12中作为一个具有众多分支和树叶的树形结构的始点，但实际上其描绘了一些更基本的内容。根不仅是网络、通信或子结构的始点，它还是信任的始点。在这个系统中的所有的实体□终端实体和所有的子CA)都以根CA的公钥作为它们的信任锚，也就是它们对所有证书验证决策的信任始点或终点。

在这个模型中，层次结构中的所有实体都信任唯一的根CA，这个层次结构按如下规则建立。

(1) 根CA直接为它下面□零层）的CA认证□更准确地说是为其创建和签署证书）。

(2) .每个零层CA都认证零个或多个直接在它下面的子CA。

(3) 倒数第二层的CA认证终端实体□非CA的终端实体）。

在层次结构中的每个实体□包括中介CA和终端实体）都必须拥有根CA的公钥，该公钥的安装是在这个模型中为随后进行的所有通信进行证书处理的基础。因此，它必

须通过一种安全的传递方式来完成。例如，一个实体可以通过物理途径如□纸的）信件或电话来取得这个密钥，也可以选择通过电子方式取得该密钥，然后再通过其他方式确认它。例如，可以把密钥的“指纹”□密钥的SHA-f散列结果）由信件发送、公布在报纸上或者通过电话告知。

注意，在一个多层的严格层次结构中，终端实体被直接在其上面的CA认证□更准确地说是颁发证书），但是这些终端实体的信任锚是根CA。对没有子CA的较浅的层次结构，终端实体来的根和证书颁发者是相同的，这种层次结构被称作可信颁发者层次结构。

2)分布式信任结构

与在PKI系统中的所有实体都信任唯一 CA的严格层次结构相反，分布式信任结构把信任分散到两个或更多个□或许是很多个）CA上。更准确地说，Alice把CA1的公钥作为她的信任锚，而Bob可以把CA2的公钥作为他的信任锚，因为这些CA的密钥都作为信任锚，因此相应的CA必须是整个PKI群体的一个子集所构成的严格层次结构的根CA(CA1是包括Alice在内的层次结构的根，CA2是包括Bob在内的层次结构的根）。

如果这些层次结构都是浅层的可信颁发者层次结构，那么该总体结构被称作“完全同位体结构” Fully Peered Architecture),因为所有的CA实际上都是相互独立的同位体(在这个结构中没有子CA)。另一方面，如果现有的层次结构都是多层结构(Multi Level Hierarchy)，那么最终的结构就被叫作“满树结构” Fully Treed Architecture)。注意根CA之间是同位体，但是每个根又是一个或多个子CA的上级。混合结构(Hybrid Treed Architecture)也是可能的□具有一个或多个可信任颁发者层次结构和一个或多个多层树型结构），该结构如图22-13所示。

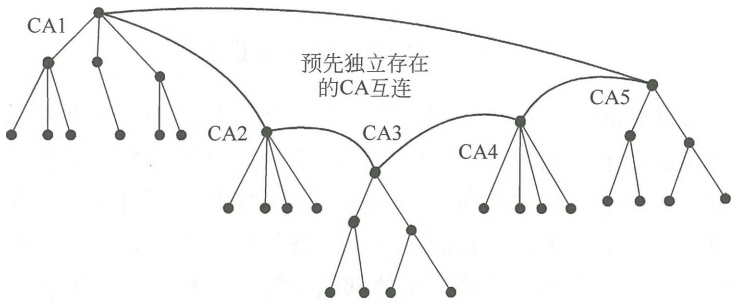


图 22-13 分布式信任结构模型

一般地□但并不总是），完全同位体结构在单一的组织范围内□如在单一公司内）实施，而满树结构和混合结构则是对在不同的组织范围内已经存在的相互独立的PKI进行互联的结果。

端点是许多在企业范围内自选实施的PKI，并且这些PKI不必是源自同一个根CA。

这些孤立的PKI系统可以按照不同的方式诸如严格层次结构、完全同位体结构等来配置。

3) Web模型

Web模型依赖于流行的浏览器，例如Netscape公司的Navigator和Microsoft公司的Internet Explorer,与PKI/CA的严格层次结构模型相似。在这种模型中，许多CA的公钥被预装在正在使用的标准浏览器上。这些公钥确定了一组CA，浏览器用户最初信任这些CA并把它们作为证书检验的根。

Web模型在方便性和简单互操作性方面有明显的优势，然而在一定的环境下做出实施决策时，这个模型的安全问题应该考虑。例如，因为浏览器的用户自动地信任预安装的所有公钥，所以即使这些根CA中有一个是“坏的”□例如，在认证实体时没有尽到应尽的努力），安全性也将完全被破坏。因此，Alice必将相信任何声称是Bob的证书都是Bob的合法证书，即使它实际只是由其公钥嵌入浏览器中“坏的” CA签署的挂在Bob名下的Eve的公钥，所以，Alice就可能无意间向Eve透露机密或接受Eve伪造的数字签名，这种假冒能够成功的原因是Alice 一般不知道一个给定的引入证书是由哪一个根密钥验证的。在嵌入到其浏览器中的20或更多个根密钥中，Alice可能只认可所给出的一些CA对其他的根密钥并不了解。然而在这个模型中，其软件平等而无任何疑问地相互信任，造成它们中的任何一个所签署的证书都毫无疑问地被彼此接受。

在某些其他信任模型中也可能出现类似情况。例如，在分布式结构中，Alice或许不能认可一个特定的CA，但是在保证其软件在相关的交叉认证是有效的、可信任的情况下，可以信任它的密钥。然而，Web模型可能比这更为糟糕。在分布式信任结构中，Alice在PKI安全方面明确地相信她的局部CA就是可信任的；而在Web模型中，Alice通常因为与安全无关的多种原因而获得了一个特定的浏览器。因此，她也没有任何理由假定这个浏览器持有可信任的“正确的” CA密钥□从她的安全角度来看）。

另一个潜在的与Web模型有关的安全考虑是没有实用的机制来撤销嵌入到浏览器中的根密钥。如果发现一个根密钥是“坏的”或者与根□公开）密钥相应的私钥被泄密了，那么使全世界数百万个浏览器都有效地废止那个密钥的使用是不可能的，这部分是因为每个站点都要得到一个适当的消息实际上是很困难的，部分是因为浏览器软件本身并没有设计成可以理解这些消息。因此，从浏览器中去除坏密钥要求全世界的每个用户都需要有明确的行动，要求全世界立即采取这个行动，否则一些用户将是安全的，而另一些用户仍处于危险之中。

4) 以用户为中心的信任模型

在一般被称作以用户为中心的信任模型中，每个用户都对决定依赖哪个证书和拒绝哪个证书直接完全地负责。尽管最初的可信密钥集可能是包括一个特定用户个人认识的朋友、家人或同事的密钥集合。

以用户为中心的信任用著名的安全软件程序PrettyGoodPrivacy (PGP)可以说明，特别是对它的密钥更新实现，更可以看出这种模型的弱点。

因为对用户行为和决策的依赖，以用户为中心的信任模型在高技术性和高利害关系的群体中可能是可行的，但是对一般的群体□它的许多用户有极少的或者没有安全方面的知识或PKI的概念）是不现实的。而且，这种模型一般在公司、金融或政府环境下是不适合的。因为在这些环境下通常希望或需要对用户的信任实行某种控制□更准确地说，这些环境可能希望在组织的基础上使特定的一个密钥或一组密钥有效或无效）。这样的组织信任策略在以用户为中心的信任模型中不能用任何一种自动的和可实施的方式来实现。

3.实体命名□**DN**)信任机制

数字证书是把一个密钥对□明确的是公钥，而暗含的是私钥）绑定到一个身份上的被签署的数据结构。但是，身份必须是唯一的与一个特定的PK实体相联系的并且它必须在使用的上下文中是有意义的。否则，安全通信是不可能实现的。Alice为了加密给Bob的数据或验证Bob的签名使用一个证书，但如果该证书实际上是□Alice并不知道）与某个其他实体相联系的，安全实际上是被破坏了。

依赖于域的大小，身份的唯一性可能简单或很难实现。在一个小的、封闭的环境里，唯一性实质上可以“免费”出现，甚至名字就能够区别所有的实体。然而，当环境变大时，唯一性就较难保证了，在互联网的规模上，主张全球名称的唯一性实际上是不可能的。

从理论方面考虑，全球实体名称的唯一性通过X.500加可识别名机制是完全可以实现的。这是一个根在顶部而命名机构在每个节点□它的唯一目的是保证它下面节点的唯一性）的层次命名结构。如果用这种方法命名的每个实体都正式地由适当的命名机构注册并且接受它被赋予的名字，DN机制就保证了唯一性，这种方法正用于现在的互联网协议 Internet Protocol，IP)和RFC822 (E-mail)的实体命名上，并成为现代电子通信中寻址和路由的基础。

最后，值得注意的是，即使全球唯一性的实现是困难的□也许是不可能的），实体名字也总是有局部意义的。更准确地说，它们在局部环境下是有意义的。因此，把一个密钥对绑定在一个特定实体名字的某种形式上是很有用的。一般而言，一个有用的实现依赖于身份已经有效存在而且权威的命名管理登记工作机构已经建立。

22.3.4应用模式

在信息安全保障系统的架构体系中，PKI/CA是S-MIS和S^2-MIS的安全基础平台。新的应用必须建立在PKI/CA的安全技术框架之内，让新的应用充分享受PKI/CA所提供的所有安全成果。PKI/CA和PMI/AA，都是在业务应用信息系统的“底层一核心层”，充分体现了信息安全保障系统的“定义”，它的运营就是要保障其他业务应用信息系统健康、正常的运行。

1.电子商务

电子商务的参与方一般包括买方、卖方、银行和作为中介的电子交易市场。买方通过自己的浏览器上网，登录到电子交易市场的Web服务器并寻找卖方，当买方登录服务器时，互相之间需要验证对方的证书以确认其身份，这被称为双向认证。

图22-14为电子商务中电子支付运行示意图，图中PPT表示支付验证信息，PRT表示供货信息，CAC/CAR表示确认/订购信息，PACK电子支付认证工具包。在双方身份被互相确认以后，建立起安全通道，并进行讨价还价，之后向商场提交订单。订单里有两种信息：一部分是订货信息，包括商品名称和价格：另一部分是提交银行的支付信息，包括金额和支付账号。买方对这两种信息进行“双重数字签名”，分别用商场和银行的证书公钥加密上述信息。当商场收到这些交易信息后，留下订货单信息，而将支付信息转发给银行。商场只能用自己专有的私钥解开订货单信息并验证签名。同理，银行只能用自己的私钥解开加密的支付信息，验证签名并进行划账。银行在完成划账以后，通知起中介作用的电子交易市场、物流中心和买方，并进行商品配送。整个交易过程都是在PKI所提供的安全服务之下进行，实现了安全、可靠、保密和不可否认性。

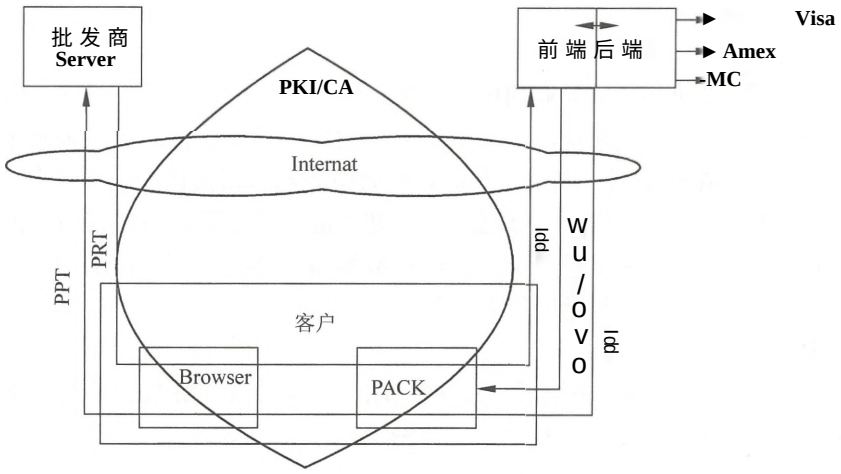


图22-14电子支付示意图

2.电子政务

电子政务包含的主要内容有网上信息发布、办公自动化、网上办公、信息资源共享等。按应用模式也可分为G2C、G2B和G2G。PKI在其中的应用主要是解决身份认证、数据完整性、数据保密性和不可抵赖性等问题。

例如，一个保密文件发给谁或者哪一级公务员有权查阅某个保密文件等，这些都需要进行身份认证，与身份认证相关的还有访问控制、权限管理。认证通过数字证书进行，而访问控制通过属性证书或访问控制列表□ACL)完成。有些文件在网络传输中要加密以保证数据的保密性，有些文件在网上传输时要求不能被丢失和篡改，特别是一些保密

文件的收发必须要有数字签名等。只有PKI提供的安全服务才能满足电子政务中的这些安全需求。

3．网上银行

网上银行是指银行借助于互联网技术向客户提供信息服务和金融交易服务。银行通过互联网向客户提供信息查询、对账、网上支付、资金划转、信贷业务与投资理财等金融服务。网上银行的应用模式有B2C个人业务和B2B对公业务两种。

网上银行的交易方式是点对点的，即客户对银行。客户浏览器端装有客户证书，银行服务器端装有服务器证书。当客户上网访问银行服务器时，银行端首先要验证客户端证书，检查客户的真实身份，确认是否为银行的真实客户；同时服务器还要到CA的目录服务器，通过LDAP协议 Lightweight Directory Access Protocol，轻量级目录访问协议）查询该客户证书的有效期和是否进入“黑名单”；认证通过后，客户端还要验证银行服务器端的证书。双向认证通过以后，建立起安全通道，客户端提交交易信息，经过客户的数字签名并加密后传送到银行服务器，由银行后台信息系统进行划账，并将结果进行数字签名返回给客户端。这样就做到了支付信息的保密和完整以及交易双方的不可否认性。

4．网上证券

网上证券广义地讲是证券业的电子商务，它包括网上证券信息服务、网上股票交易和网上银证转账等。– 般来说，在网上证券应用中，股民为客户端，装有个人证书：券商服务器端装有Web证书。在线交易时，券商服务器只需要认证股民证书，验证是否为合法股民，是单向认证过程。认证通过后，建立起安全通道。股民在网上的交易提交同样要进行数字签名，网上信息要加密传输：券商服务器收到交易请求并解密，进行资金划账并做数字签名，将结果返回给客户端。

5．其他应用

其他应用如网上看病、网上学习、网上联合开发、网上游戏、网上点播等。PKI/CA为虚拟社会的正常运营提供了安全保障，网上应用层出不穷。

22.4 PMI权限□授权）管理基础设施

PMI (Privilege Management Infrastructure)即权限管理基础设施或授权管理基础设施。PMI授权技术的核心思想是以资源管理为核心，将对资源的访问控制权统一交由授权机构进行管理，即由资源的所有者来进行访问控制管理。

我们知道没有PKI就没有信息安全系统，但是只有PKI也没法对信息系统的资源进行合理有效的管理。PMI几乎完全按照PKI的体系架构建立，外形很相像，但内容却完全不同。

PMI建立在PKI基础上，以向用户和应用程序提供权限管理和授权服务为目标，主

要负责向业务应用信息系统提供授权服务管理：提供用户身份到应用授权的映射功能；实现与实际应用处理模式相对应的、与具体应用系统开发和管理无关的访问控制机制；能极大地简化应用中访问控制和权限管理系统的开发与维护；减少管理成本和复杂性。

22.4.1 PMI与PKI的区别

PMI主要进行授权管理，证明这个用户有什么权限，能干什么，即“你能做什么”。PKI主要进行身份鉴别，证明用户身份，即“你是谁”。

它们之间的关系如同签证和护照的关系。签证具有属性类别，持有哪一类别的签证才能在该国家进行哪一类的活动。护照是身份证明，唯一标识个人信息，只有持有护照才能证明你是一个合法的人。

1. **PMI与PKI**逐项比较

PMI与PKI的逐项比较见表22-5。

表22-5 **PMI**与**PKI**比较

概　念	**PMI**实体	**PKI**实体
证书	属性证书	公钥证书
证书签发者	属性证书管理中心	认证证书管理中心
证书用户	持有者	主体
证书绑定	持有者名和权限绑定	主体名和公钥绑定
撤销	属性证书撤销列表□**ACRL**)	证书撤销列表□**CRL**)
信任的根	权威源□**SOA**)	根**CA**/信任锚
从属权威	属性管理中心**AA**	子**CA**

2.属性证书及其管理中心

AC (Attribute Certificate),即属性证书，表示证书的持有者□主体）对于一个资源实体□客体）所具有的权限，它是由一个做了数字签名的数据结构来提供的，这种数据结构称为属性证书，由属性证书管理中心AA签发并管理。

公钥证书是对用户名称和他/她的公钥进行绑定；而属性证书是将用户名称与一个或更多的权限属性进行绑定。在这个方面，公钥证书可被看为特殊的属性证书。

数字签名公钥证书的机构被称为CA (Certification Authorities)，签名属性证书的机构被称为 AA (Attribute Authorities)。

PKI信任源有时被称为根CA，而PMI信任源被称为权威源SOA。

CA可以有它们信任的次级CA。次级CA可以代理鉴别和认证。同样，SOA可以将它们的权利授给次级AA。

如果用户需要废除他/她的签字密钥，则CA将签发一个证书撤销列表□CRL)。与之类似，如果用户需要废除授权，AA将签发一个属性证书撤销列表 ACRLh

22.4.2属性证书定义

对一个实体权限的绑定是由一个被数字签名了的数据结构来提供的，这种数据结构称为属性证书，由属性证书管理中心签发并管理。一些应用使用属性证书来提供基于角色的访问控制。

1.属性证书的格式

属性证书的格式，如表22-6所示。

表22-6属性证书格式

版本号	属性证书的版本号
持有者	属性证书持有者信息
颁发者	属性证书颁发者信息
签名算法	属性证书使用的签名算法
序列号	属性证书序列号
有效期	属性证书生效和失效曰期
属性	属性证书持有者的属性信息
扩展项	定义诸如无撤销信息、证书颁发者密钥标识符、CRL分布点、角色定义证书标识符及其他信息
签名信息	属性证书签发者对属性证书的签名

2. 属性证书的特点

公钥证书将一个身份标识和公钥绑定，属性证书将一个标识和一个角色、权限或者属性绑定□通过数字签名）；和公钥证书一样，属性证书能被分发、存储或缓存在非安全的分布式环境中；不可伪造，防篡改。同时，属性证书具有以下特点。

·分立的发行机构。

·基于属性，而不是基于身份进行访问控制。

·属性证书与身份证书的相互关联。

·时效短。

一个人可以拥有好几个属性证书，但每一个都会与唯一的身份证书关联。几个属性证书可以来自不同的机构。

3. 属性证书的使用

属性证书的使用有两种模式，如图22-15所示。

第一种是推模式，当用户在要求访问资源时，由用户自己直接提供其属性证书，即用户将自己的属性证书“推”给资源服务管理器。这意味着在客户和服务器之间不需要建立新的连接，而且对于服务器来说，这种方式不会带来查找证书的负担，从而减少了开销。

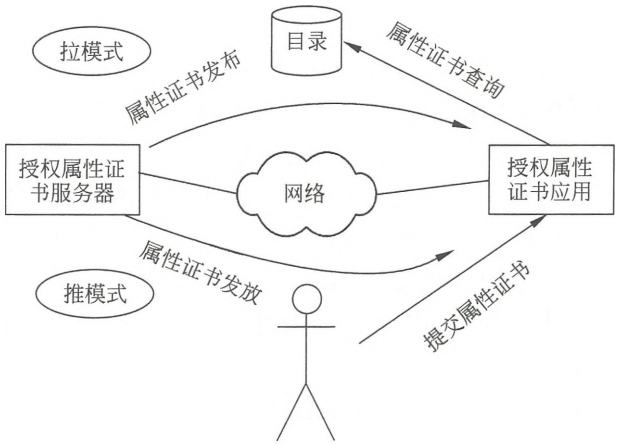


图22-15属性证书的使用

第二种是拉模式，是业务应用授权机构发布属性证书到目录服务系统，当用户需要用到属性证书的时候，由服务器从属性证书发放者□属性权威AA)或存储证书的目录服务系统“拉”回属性证书。这种“拉”模式的一个主要优点在于实现这种模式不需要对客户端以及客户-服务器协议做任何改动。这两种模式可以根据应用服务的具体情况灵活应用。

22.4.3访问控制

1. 访问控制的基本概念

访问控制是信息安全保障机制的核心内容之一，是实现数据保密性和完整性的主要手段之一。访问控制是为了限制访问主体□或称为发起者，是一个主动的实体，如用户、进程、服务等）对访问客体□需要保护的资源）的访问权限，从而使计算机信息应用系统在合法范围内使用；访问控制机制决定用户以及代表一定用户利益的程序能做什么及做到什么程度。

访问控制有两个重要过程。

(1) 认证过程，通过“鉴别□authentication)”来检验主体的合法身份。

(2) 授权管理，通过“授权□authorization)”来赋予用户对某项资源的访问权限。

访问权限随不同的业务应用有不同的规范，一般至少包括读取数据、更改数据、运行程序和发起网络连接等基本操作。

2. 访问控制机制分类

因实现的基本理念不同，访问控制机制可分为强制访问控制 Mandatory Access Control, MAC)和自主访问控制 Discretionary Access Control, DAC)两种。

1） 强制访问控制

系统独立于用户行为强制执行访问控制□MAC),用户不能改变他们的安全级别或对象的安全属性。这样的访问控制规则通常对数据和用户按照安全等级划分标签，访问控制机制通过比较安全标签来确定的授予还是拒绝用户对资源的访问。

在强制访问控制系统中，所有主体□用户，进程）和客体□文件，数据）都被分配了安全标签，安全标签标识一个安全等级。即主体□用户，进程）被分配一个安全等级，客体□文件，数据）也被分配一个安全等级。

访问控制执行时对主体和客体的安全级别进行比较，确定本次访问是否合法。

2） 自主访问控制

自主访问控制□DAC)机制允许对象的属主来制定针对该对象的保护策略。通常DAC通过授权列表(或访问控制列表)来限定哪些主体针对哪些客体可以执行什么操作。这样可以非常灵活地对策略进行调整。

自主访问控制中，用户可以针对被保护对象制定自己的保护策略。每个主体拥有一个用户名并属于一个组或具有一个角色。每个客体都拥有一个限定主体对其访问权限的访问控制列表□ACL)，每次访问发生时都会基于访问控制列表检查用户标志以实现对其访问权限的控制。

3.访问控制安全模型

1) Bell-LaPadula访问控制安全模型

1973年，David Bell和Len LaPadula提出第一个正式的访问控制安全模型——Bell-LaPadula（BLP)。该模型基于强制访问控制系统，以敏感度来划分资源的安全级另IJ，将数据划分为多安全级别与敏感度。

数据和用户由低到高被划分为以下安全等级：公开□Unclassified) —受限□Restricted) —秘密□Unfidential)—机密□Secret)—高密 Top Secret)。

BLP保密模型基于两种规则来保障数据的机密度与敏感度。

上读□NRU):主体不可读安全级别高于它的数据。

下写□NWD):主体不可写安全级别低于它的数据。

假如一个用户，他的安全级别为“高密”，想要访问安全级别为“秘密”的文档，他将能够成功读取该文件，但不能写入；而安全级别为“秘密”的用户访问安全级别为“高密”的文档，则会读取失败，但他能够写入。这样，文档的保密性就得到了保障。

2) Biba完整性模型

20世纪70年代，Ken Biba提出Biba访问控制模型，该模型对数据提供分级别的完整性保证，类似于BLP保密性模型，Biba模型也使用强制访问控制系统。

Biba完整性模型是对主体和客体按照强制访问控制系统的模型。数据和用户被划分为以下安全等级：公开□Unclassified)—受限□Restricted)—秘密□Confidential)—机密□Secret)—高密 Top Secret)。

Biba模型基于两种规则来保障数据的完整性的保密性。

下读□NRU)属性：主体不能读取安全级别低于它的数据。

上写□NWD)属性：主体不能写入安全级别高于它的数据。

从这两个属性来看，我们发现Biba与BLP模型的两个属性是相反的，BLP模型提供保密性，而Biba模型对于数据的完整性提供保障。

Biba模型的一个应用例子是对Web服务器的访问过程，如图22-16所示。定义Web服务器上发布的资源安全级别为“秘密”；Internet上用户的安全级别为“公开”。依照Biba模型，Internet上的用户只能读取服务器上的数据而不能更改它，因此，任何Paste操作将被拒绝。Web服务器上数据的完整性将得到保障。

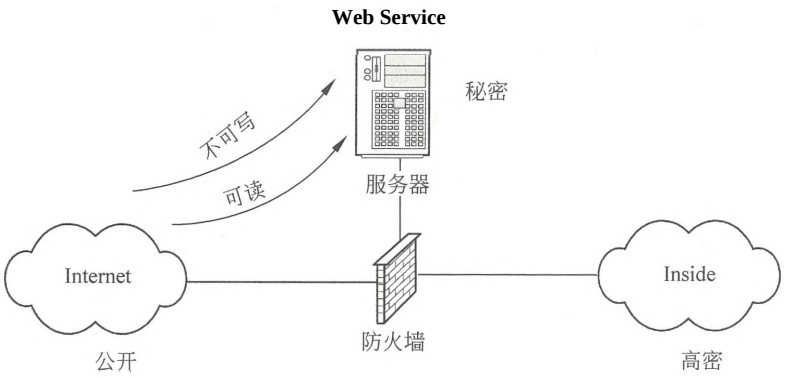


图22-16 **Biba**模型的应用示意图

另一个例子是对系统状态信息的收集。网络设备作为对象，被分配的安全等级为“机密”，网管工作站的安全级别为“秘密”，那么网管工作站只能使用SNMP的get命令来收集网络设备的状态信息，而不能使用set命令更改该设备的设置。这样，网络设备的配置完整性就得到了保障。

22.4.4基于角色的访问控制

20世纪90年代以来，出现的一种基于角色的访问控制RBAC（Role-Based Access Control)技术，有效地克服了传统访问控制技术中存在的不足之处。

用户不能自主地将访问权限授给别的用户，这是RBAC与DAC的根本区别所在。

RBAC与MAC的区别在于：MAC是基于多级安全需求的，而RBAC不是。因为军用系统中主要关心的是防止信息从高安全级流向低安全级，即限制“谁可以读/写什么信息”。而基于角色控制的系统中，主要关心的是保护信息的完整性，即“谁可以对什么信息执行何种动作”。角色控制比较灵活，根据配置可以使某些角色接近DAC，而某些角色更接近于MAC。

基于角色的访问控制中，角色由应用系统的管理员定义。角色成员的增减也只能由应用系统的管理员来执行，即只有应用系统的管理员有权定义和分配角色；而且授权规定是强加给用户的，用户只能被动接受，不能自主地决定。用户也不能自主地将访问权限传给他人，这是一种非自主型访问控制。基于角色的访问控制的运行机理，如图22-17所示。

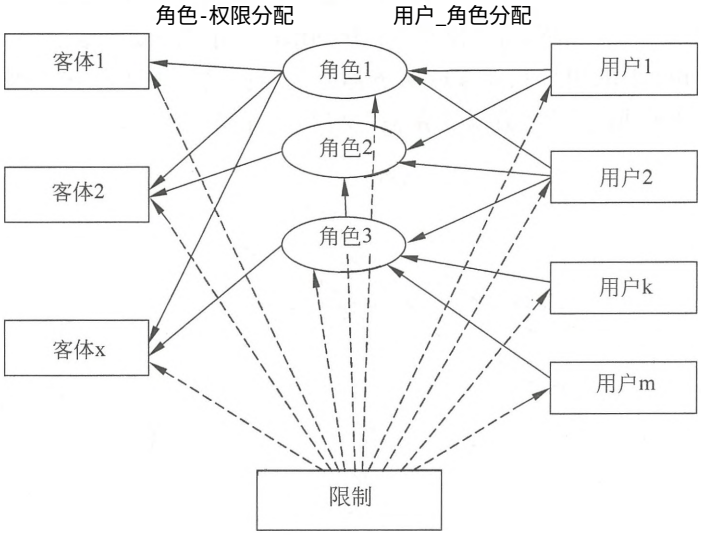


图22-17基于角色的访问控制示意图

需要指出的是角色和组的区别。组通常仅仅是作为用户的集合，而角色一方面是用户的集合，另一方面又是权限的集合，作为中间媒介将用户和权限连接起来。当然角色可以在组的基础上实现，这样就对保持原有系统非常有利。此时角色就成为一个策略部件，与组织的授权、责任关系相联系，而组成为实现角色的工具，两者间是策略与实现机理的关系。

22.4.5 PMI支撑体系

1．**PMI**平台

权限管理、访问控制框架、策略规则共同构成权限管理和访问控制实施的系统平台，或者说构成了属性证书应用支撑框架系统□PMI平台）。

1)策略规则

策略规则是PMI真正发挥在访问控制应用方面的灵活性、适应性和降低管理成本的关键。策略应当包括一个企业/组织将如何将它的人员和数据进行分类组织管理。这种组织管理方式必须考虑到具体应用的实际运行环境，如数据的敏感性，人员权限的明确划分，以及必须和相应机构层次相匹配的管理层次等因素。

具体来说，策略包含：

(1) 应用系统中的所有用户和资源信息。

(2) 用户和资源信息的组织管理方式。

(3) 用户和资源信息之间的权限关系。

(4) 保证安全的管理授权约束。

(5) 保证系统安全的其他约束。

2) 权限管理

PMI使用属性证书表示和容纳权限信息。对权限生命周期的管理是通过管理证书的生命周期实现的。属性证书的申请、签发、注销、验证等流程对应权限的申请、发放、撤销、使用验证的过程，而且使用属性证书来管理权限，使得权限的管理不必依赖某个具体的应用，而且有利于权限管理实现分布式的应用。

绝大多数的访问控制应用都能抽象成一般的权限管理模型，其中包括3个实体：对象、访问者和权限验证者。

(1) 对象。对象可以是被保护的资源。在一个访问控制应用中，受保护资源就是对象，如数据库，网页等。对象又称为“客体”。

(2) 访问者。访问者也就是权限声明者，声称拥有某种权限，并要求访问受保护对象。访问者可以是人、程序或设备等。访问者又称为“主体”。

(3) 权限验证者。权限验证者对访问者的访问动作进行验证和决策，以决定访问者的权限对于使用内容来说是否充分。

权限验证者根据以下4个条件决定访问通过还是失败。

·访问者的权限。

·权限策略。

·当前环境变量□如果有的话）。

·对象方法的敏感度□如果有的话）。

访问控制的抽象模型，如图22-18所示。

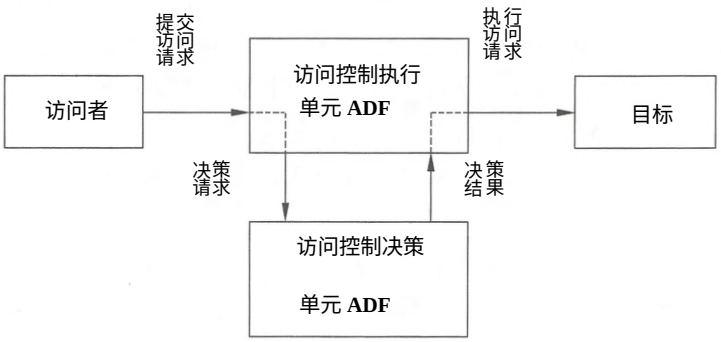


图22-18访问控制抽象模型

2.访问控制的应用

1) 访问控制授权方案

目前我们使用的访问控制授权方案，主要有以下4种。

(1) DAC（Discretionary Access Control)自主访问控制方式：该模型针对每个用户指明能够访问的资源，对于不在指定的资源列表中的对象不允许访问。

(2) ACL (Access Control List)访问控制列表方式：该模型是目前应用最多的方式。目标资源拥有访问权限列表，指明允许哪些用户访问。如果某个用户不在访问控制列表中，则不允许该用户访问这个资源。

(3) MAC (Mandatory Access Control)自主访问控制方式，该模型在军事和安全部门中应用较多，目标具有一个包含等级的安全标签□如：不保密、限制、秘密、机密、绝密）；访问者拥有包含等级列表的许可，其中定义了可以访问哪个级别的目标：例如允许访问秘密级信息，这时，秘密级、限制级和不保密级的信息是允许访问的，但机密和绝密级信息不允许访问。

(4) RBAC（Role-Based Access Control)基于角色的访问控制方式：该模型首先定义一些组织内的角色，如局长、科长、职员；再根据管理规定给这些角色分配相应的权限，最后对组织内的每个人根据具体业务和职位分配一个或多个角色。

2) 访问控制决策的基本因素

访问控制决策的基本因素有。

(1) 访问者。应用中支持哪些用户——确定了用户的范围。

(2) 目标。策略要保护的是哪些目标——确定了受保护的资源的范围。

(3) 动作。应用中限定访问者可以对目标设施的操作——确定了权限的范围。

(4) 权限信任源。应用信任什么机构发布的权限信息。

(5) 访问规则。访问者具有什么权限才能够访问目标。

3) 基于角色的访问控制

在PMI中主要使用基于角色的访问控制。其中，角色提供了间接分配权限的方法。在实际应用中，个人被签发成某个角色，并分配证书使之具有一个或多个对应的角色。而每个角色具有的权限通过角色定义来说明，而不是将权限放在属性证书中直接分配给个人。这种间接的权限分配方式，使得角色权限更新时，不必撤销每一个属性证书，极大地减小了管理开销。PM1应用结构逻辑关系，如图22-19所示。

访问者。访问者是一个实体□该实体可能是人，可能是其他计算机实体），它试图访问系统内的其他实体□目标）。

策略。策略是一个信息库，包含着策略决策所需要的所有信息，如：应用系统中的所有用户和资源信息，用户和资源信息的组织管理方式，用户和资源信息之间的权限关系，保证安全的管理授权定义，保证系统安全的其他规定等。

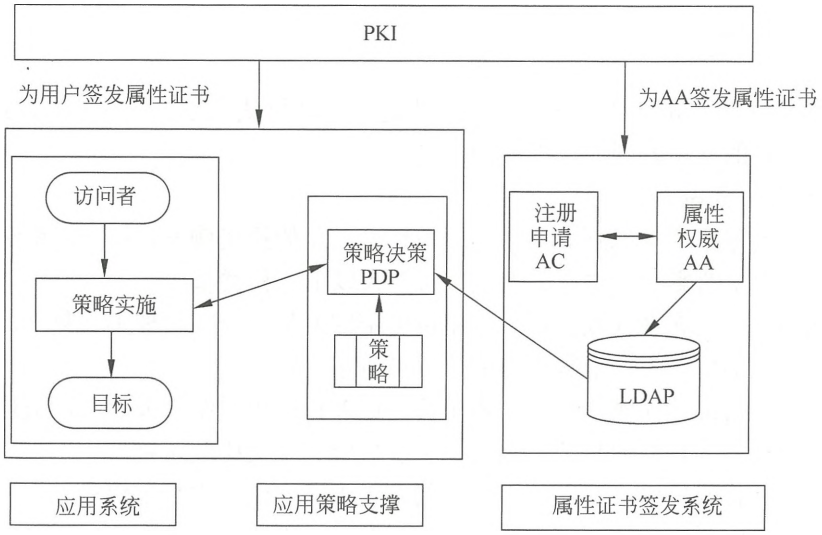


图22-19 **PMI**应用结构的逻辑关系

策略决策。策略决策 Policy Decision Point，PDP)也称作授权策略服务器，它接收和评价授权请求，根据具体策略做出不同的决策。

策略实施。策略实施 Policy Enforcement Points，PEPs)也称作PMI激活的应用。对每一个具体的应用，策略实施可能是不同的。如在某个具体的应用中，策略实施点可能是应用程序内部中进行访问控制的一段代码，也可能是安全的应用服务器□如在Web服务器上增加一个访问控制插件），或者是进行访问控制的安全应用网关。

PMI应用整体结构，如图22-20所示。

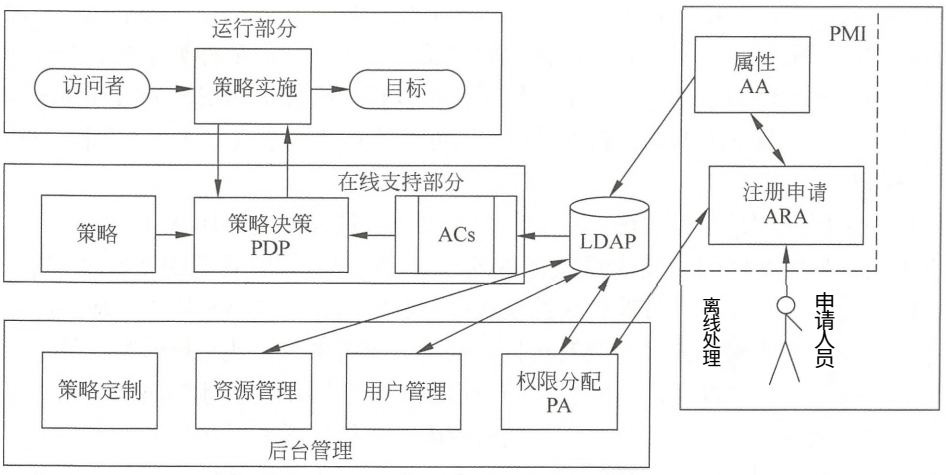


图22-20 **PMI**应用的整体架构

22.4.6 PMI 实施

单位/组织实施PMI，建议采取的步骤为建立属性权威，制定授权策略，进行授权、访问控制和审计的程序编制与应用实施。

1. 建立属性权威

属性权威的建立要考虑到系统的管理方便性，总的投资额度，用户和资源的数量以及更新对AA效率的影响。建立属性权威可分为以下三种类型：

(1) 使用嵌入式属性权威管理。本单位内部的人员和权限管理不太复杂，数据的敏感度也不是太高的情况下，由数据库的管理员直接代管。

(2) 在单位内部建立属性权威。本单位内由多种应用系统组成，用户数量以及资源数量较大，人员结构和管理复杂，人员职位和权限的变化比较频繁。

(3) 建立属性权威中心。在一个更大的范围内的安全应用数量较多，有相同的访问群体，并且这些应用有整体的安全管理规定和要求。投资相对较大，但是能够进行全局的权限管理，能够覆盖区域内的所有用户和应用，管理能力最强，有利于制定全局统一的安全管理模式和策略。

2. 制定授权策略

制定授权策略可以针对安全域内的人员和资源的组织进行分析入手，抓住业务应用的需要，制定系统的授权策略。

以公安“金盾工程”为例，根据公安业务的管理规定和保密的要求，公安部可以制定出保证所有公安系统应用需要的统一基本授权策略，对公安应用的基本角色、基本权限和访问控制原则进行约束和定义，形成“金盾工程”的授权策略。这种策略不是针对具体系统定义的，也不是针对具体哪一个人的，只是规定所有应用系统必须遵守的全局性的安全准则。如，规定总共定义多少种基本的全局角色，每个角色对不同的资源能够具有的最大的权限等。例如，对其他警种的科长是否允许访问某种类型的资源等。

在全局授权策略的基础上，各个应用系统可以根据被保护的资源的具体情况和访问系统的人员情况定制本地的局部授权策略；还可以针对某一个具体应用，定制授权策略。

3. 授权

授权和访问控制是具体实现已经制定好的“授权策略”主要环节。

由于属性权威是资源的权威源/资源的拥有者，可以根据它管理的“用户”信息进行授权。比如，一个人可能同时拥有属性权威中心颁发的属性证书和嵌入式属性权威颁发的属性证书，来证明他是公安系统的科长，同时在应用系统内他是机密数据处理员。有了这样的授权，他就可以直接访问指定的应用系统。应用系统从他的属性证书中，验证发证机关的权威性，并提取与该应用相关的权限，进行判断和操作。

不同规模和级别的属性权威的安全性是不同的。嵌入式的属性权威管理员可以根据需要比较灵活的处理证书的发放和撤销。但是AA中心对证书的管理必须具有更严格的

管理程序和安全性，以保证权威性，并避免失误带来的损害。即使区域型的AA中心一个不负责任签发的属性证书，就会给信任该属性权威的所有应用带来无法估计的损失。而嵌入式的属性权威造成的损害只是发生在单位内部。因此，AA中心的授权实施管理是十分重要的安全管理内容。

4. 访问控制

应用PMI平台建立访问控制系统的工作相对简单，只需针对具体的应用类型定制策略实施点，并安装相关的策略服务器、资源服务器及相应的服务程序即可。

5. 审计

PMI平台提供独立于应用的访问操作审计能力和系统中管理事件的审计，可以在PMI平台中根据需要选择审计内容，不必在开发应用系统前制定。通过标准的审计接口，可以定制将审计结果输出到日志、数据库或其他文件，甚至为入侵检测系统提供数据采集接口，支持基于应用的入侵检测系统。

6. **PMI**实施的工作流程

一般PMI实施采用以下工作流程。

(1) 使用用户管理工具注册应用系统用户信息。

(2) 使用资源管理工具注册资源信息。

(3) 使用策略定制工具制定应用系统的权限管理和访问控制策略。

(4) 便用权限分配工具签发策略证书、角色定义证书。

(5) 属性权威针对用户签发属性证书。

(6) 启动策略实施点，使用指定的策略和相关信息初始化策略决策服务器。

(7) 用户登录时，策略实施点验证用户身份，并根据下一个步骤获取权限信息。

(8) 如果是推模式，直接从用户提供的属性证书中获得权限信息；如果是拉模式，根据用户身份信息从属性证书库中检索，并返回用户的权限信息。

(9) 对每个访问请求，策略实施点根据权限、动作和目标信息生成决策请求。

(10) 策略实施点向策略决策点发出决策请求。

(11) 策略决策点根据策略对请求进行判断，返回决策结果。

(12) 策略实施点根据结果决定是否进行访问。

(13) 如果要停止运行，就关闭策略实施点，由策略实施点通知策略决策服务器停止。

22.5信息安全审计

22.5.1安全审计概念

1.安全审计

安全审计 Security Audit)是记录、审查主体对客体进行访问和使用情况，保证安

全规则被正确执行，并帮助分析安全事故产生的原因。

安全审计是信息安全保障系统中的一个重要组成部分，是落实系统安全策略的重要机制和手段，通过安全审计，识别与防止计算机网络系统内的攻击行为，追查计算机网络系统内的泄密行为。安全审计具体包括两方面的内容。

(1) 采用网络监控与入侵防范系统，识别网络各种违规操作与攻击行为，即时响应（如报警）并进行阻断。

(2) 对信息内容和业务流程进行审计，可以防止内部机密或敏感信息的非法泄漏和单位资产的流失。

安全审计系统采用数据挖掘和数据仓库技术，对历史数据进行分析、处理和追踪，实现在不同网络环境中终端对终端的监控和管理，必要时通过多种途径向管理员发出警告或自动采取排错措施。因此信息安全审计系统被形象地比喻为“黑匣子”和“监护神”。

(1) 信息安全审计系统就是业务应用信息系统的“黑匣子”。即使在整个系统遭到灭顶之灾的破坏后，“黑匣子”也能安然无恙，并确切记录破坏系统的各种痕迹和“现场记录”。

(2) 信息安全审计系统就是业务应用信息系统的“监护神”，随时对一切现行的犯罪行为、违法行为进行监视、追踪、抓捕，同时对暗藏的、隐患的犯罪倾向、违法迹象进行“堵漏”、铲除。

安全审计系统属于安全管理类产品。安全审计产品主要包括主机类、网络类及数据库类和业务应用系统级的审计产品。各类安全审计系统可在日常运行、维护中，对整个计算机网络应用系统的安全进行主动分析及综合审计。

2.安全审计的作用

一个安全审计系统，主要有以下作用。

(1) 对潜在的攻击者起到震慑或警告作用。

(2) 对于已经发生的系统破坏行为提供有效的追究证据。

(3) 为系统安全管理员提供有价值的系统使用日志，从而帮助系统安全管理员及时发现系统入侵行为或潜在的系统漏洞。

(4) 为系统安全管理员提供系统运行的统计日志，使系统安全管理员能够发现系统性能上的不足或需要改进与加强的地方。

网络安全审计的具体内容如下。

(1) 监控网络内部的用户活动。

(2) 侦察系统中存在的潜在威胁。

(3) 对日常运行状况的统计和分析。

(4) 对突发案件和异常事件的事后分析。

(5) 辅助侦破和取证。

3.安全审计功能

CC（即Common Criteria ISO/IEC 17859)标准将安全审计功能分为6个部分：安全审计自动响应功能；安全审计自动生成功能；安全审计分析功能；安全审计浏览功能；安全审计事件选择功能；安全审计事件存储功能。

1) 安全审计自动响应功能

安全审计自动响应□AU_APR)定义在被测事件指示出一个潜在的安全攻击时做出的响应，它是管理审计事件的需要，这些需要包括报警或行动。例如包括实时报警的生成、违例进程的终止、中断服务、用户账号的失效等。根据审计事件的不同，系统将做出不同的响应，其响应的行动可做增加、删除、修改等操作。

2) 安全审计数据生成功能

安全审计数据生成□AU_GEN)功能要求记录与安全相关的事件的出现，包括鉴别审计层次、列举可被审计的事件类型，以及鉴别由各种审计记录类型提供的相关审计信息的最小集合。系统可定义可审计事件清单，每个可审计事件对应于某个事件级别，如低级、中级、高级。产生的审计数据有以下几方面。

(1) 对于敏感数据项□如口令等）的访问。

(2) 目标对象的删除。

(3) 访问权限或能力的授予和废除。

(4) 改变主体或目标的安全属性。

(5) 标识定义和用户授权认证功能的使用。

(6) 审计动能的启动和关闭。

每一条审计记录中至少应所含的信息有：事件发生的日期〔时间、事件类型、主题标识、执行结果□成功、失败）、引起此事件的用户的标识以及对每一个审计事件与该事件有关的审计信息。

3) 安全审计分析功能

安全审计分析□AU_SAA)功能定义了分析系统活动和审计数据来寻找可能的或真正的安全违规操作。它可以用于入侵检测或对安全违规的自动响应。当一个审计事件集出现或累计出现一定次数时可以确定一个违规的发生，并执行审计分析。事件的集合能够由经授权的用户进行增加、修改或删除等操作。审计分析分为潜在攻击分析、基于模板的异常检测、简单攻击试探和复杂攻击试探等几种类型。

(1) 潜在攻击分析。系统能用一系列的规则监控审计事件，并根据规则指示系统的潜在攻击。

(2) 基于模板的异常检测。检测系统不同等级用户的行动记录，当用户的活动等级超过其限定的登记时，应指示出此为一个潜在的攻击。

(3) 简单攻击试探。当发现一个系统事件与一个表示对系统潜在攻击的特征事件匹配时，应指示出此为一个潜在的攻击。

(4)复杂攻击试探。当发现一个系统事件或事迹序列与一个表示对系统潜在攻击的特征事件匹配时，应指示出此为一个潜在的攻击。

4) 安全审计浏览功能

安全审计浏览□AU_SAR)功能要求审计系统能够使授权的用户有效地浏览审计数据，它包括审计浏览、有限审计浏览、可选审计浏览。

(1) 审计浏览。提供从审计记录中读取信息的服务。

(2) 有限审计浏览。要求除注册用户外，其他用户不能读取信息。

(3) 可选审计信息。要求审计浏览工具根据相应的判断标准选择需浏览的审计数据。

5) 安全审计事件选择功能

安全审计事件选择□AU_SEL)功能要求系统管理员能够维护、检查或修改审计事件的集合，能够选择对哪些安全属性进行审计。例如，与目标标识、用户标识、主体标识、主机标识或事件类型有关的属性，系统管理员将能够有选择地在个人识别的基础上审计任何一个用户或多个用户的动作。

6) 安全审计事件存储功能

安全审计事件存储□AU_STG)功能要求审计系统将提供控制措施；以防止由于资源的不可用丢失审计数据。能够创造、维护、访问它所保护的对象的审计踪迹，并保护其不被修改、非授权访问或破坏。审计数据将受到保护直至授权用户对它进行的访问。它可保证某个指定量度的审计记录被维护，并不受以下事件的影响。

(1) 审计存储空间用尽。

(2) 审计存储故障。

(3) 非法攻击。

(4) 其他任何非预期事件。

审计系统能够在审计存储发生故障时采取相应的动作，能够在审计存储即将用尽时采取相应的动作。

22.5.2建立安全审计系统

在计算机网络环境下，建立信息安全审计系统是一个全方位、多层次的复杂系统工程，要深入到计算机应用的每一个领域与技术核心。它按一定规则，在不同层次获取并分析各种记录、日志、报告等信息资源，以如实反映系统安全情况和那里发生的所有事件。其中，事关网络、系统信息安全的网络与主机信息监测审计、应用系统信息监测审计、网络安全系统设备信息审计和系统安全评估报告应作为安全审计系统的主体，而物理安全日志记录则主要为重要场所提供直接的现场审计记录和监控，可作为安全审计系统的辅助系统。

建设安全审计系统的主体方案一般包括利用网络安全入侵监测预警系统实现网络与主机信息监测审计；对重要应用系统运行情况的审计和基于网络旁路监控方式安全

审计等。

1.基于入侵监测预警系统的网络与主机信息监测审计

网络安全入侵监测预警系统基本功能是负责监视网络上的通信数据流和网络服务器系统中的审核信息，捕捉可疑的网络和服务器系统活动，发现其中存在的安全问题，当网络和主机被非法使用或破坏时，进行实时响应和报警；产生通告信息和日志，系统审计管理人员根据这些通告信息、日志和分析结果，调整和更新己有的安全管理策略或进行跟踪追查等事后处理措施。所以，在这个层次上的入侵监测和安全审计是一对因果关系，前者获取的记录结果是后者审核分析资料的来源，或者说前者是手段而后者是目的，任何一方都不能脱离另一方单独工作。作为一个完整的安全审计需要入侵监测系统实时、准确提供基于网络、主机□服务器、客户端）和应用系统的审核分析资料。

入侵监测是指为对计算机和网络资源上的恶意使用行为进行识别和响应的处理过程。它不仅检测来自外部的入侵行为，同时也检测内部用户的未授权活动。

从安全审计的角度看，入侵检测采用的是以攻为守的策略，它所提供的数据不仅可用来发现合法用户是否滥用特权，还可以为追究入侵者法律责任提供有效证据。

1)系统配置拓扑结构

网络安全入侵监测系统由一台安全审计、控制中心和若干台网络探测器组成，采用集中管理的分布式体系结构，具体结构，如图22-21所示。

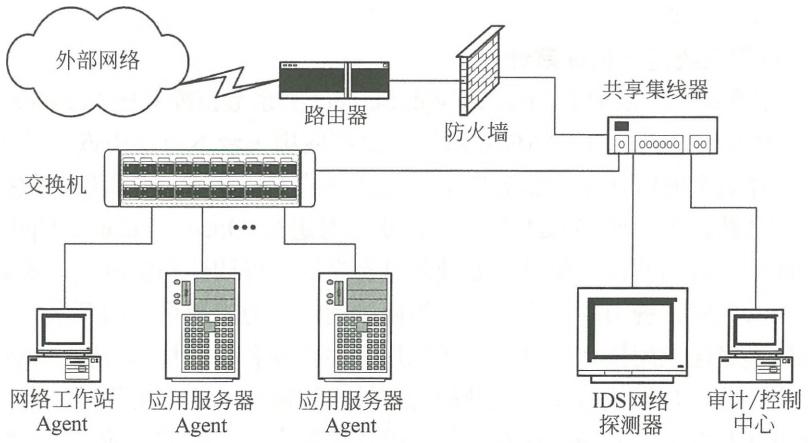


图22-21基于网络和主机监测的安全审计架构示意图

2)工作原理及连接配置

探测器负责监视通过网络相连的计算机主机，即按照指定的安全规则监视网络数据流，发现网络攻击、网络违规行为或迹象的时候，按照即定安全策略实施实时响应，如：向安全控制中心发送报警和网络活动信息，实时阻断非法的网络连接等。探测器设置在网络的敏感部位，如内部网络的入口处或担负重要任务、具有重要数据的服务器的周围

等。安全控制中心负责通过与探测器通信来控制它们的运行，加载安全规则、接收报警信息，产生报警日志和全网的安全审计报告并进行实时与事后分析。

探测器应与被监测的主机或网络处于一个共享的以太网环境内。这是因为探测器的工作原理依赖于以太网的物理特性，探测器与被监控网络的连接有以下4种方式：

(1) 探测器连接在集线器的一个端口上。

(2) 若网络环境中只有交换设备，可以将探测器连接在交换设备的监视□Probe)端口上。

(3) 在交换机上定义一个VLAN使其包含该交换机上所有需要监视的端口。

(4) 特意地构造一个局部的共享总线式的以太网环境，使应被监视的主机或网络能够与探测器处于一个共享的以太网环境内。

安全控制中心原则上可以连接在网络的任何部位。同时，要保证到各探测器的物理网络通路。但由于安全控制中心担负着重要的管理任务，应将其放置在网络中的安全部位，如置于防火墙保护之内并关闭所有Internet服务与文件共享服务，删除所有不必要的用户。当安全控制中心与探测器之间存在防火墙时，应在防火墙中为安全控制中心与探测器通信设置端口过滤规则。

为了进一步保证探测器和控制中心运行安全并与某些交换机工作匹配，也可将探测器设置为双网卡结构。一块用于监听，采集网络数据，不设置IP地址，对网络透明；另一块用于与控制中心通信。

2.重要应用系统运行情况审计

目前，应用系统平台主要有Oracle SQL Server（关系数据库系统）、Lotus的Domino/Notes（全文数据库、应用电子邮件系统），这些应用平台本身都内嵌有较为完备的信息审核机制，作为全面审计跟踪服务器上一切活动的工具，它可以实现在数据库的表、视图、目录、文档、列□域field)等不同层次，对进行Open、Create、Update Delete等细粒度访问操作时的监控。但是，要使其具有良好的可读性和实时性，还需应用程序开发人员做大量耗时、费力的工作。这是很困难的，因为应用系统的开发、销售商一般不会把审核机制底层应用接口提供给具体应用程序开发者。在技术力量不足的情况下，最便捷的解决方法还是寻找可靠、成熟的现有技术解决，以使应用程序开发人员能够专心于程序可用性开发上，而减少在难度较大的程序安全性方面的劳动，达到缩短开发周期、快速投入应用的目的。

截止到目前，从已知的现有技术分析，主要有4种解决方案。

1)基于主机操作系统代理

数据库操作系统□如Oracle、SQLServer)、电子邮件系统□如Microsoft Exchange)在启动自身审计功能之后自动将部分系统审核数据□如用户登录活动、对象访问活动）传送到主机系统审计日志。然后，再通过运行于主机操作系统下一个实时监控代理程序来读取并分析系统审计日志中的相关数据。此方案与应用系统编程无关，所以通用性、

实时性好，但审计粒度较粗，并且对确认的违规行为不能实现阻断控制。原理如图22-22所示。

2)基于应用系统代理

此种解决方案与基于主机操作系统代理不同之处在于：

(1) 首先根据不同应用，设计开发不同的应用代理程序，并在相应应用系统内运行。

(2) 应用系统产生的审计数据不是直接传送给主机操作系统审核，而是首先由应用代理程序接收，再由其传送给主机操作系统审核，也可直接传送给主机操作系统实时监控代理程序处理。

此方案优点是实时性好，且审计粒度由用户控制，可以减少不必要的审核数据。缺点在于要为每个应用单独编写代理程序，因而与应用系统编程相关，通用性不如前者好。原理如图22-23所示。

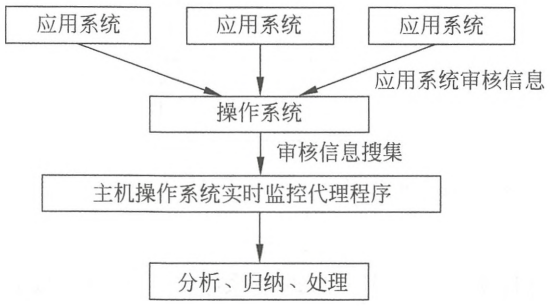


图22-22主机操作系统代理型审计示意图

图22-23基于应用系统代理审计示意图

3)基于应用系统独立程序

在应用系统内部嵌入一个与应用服务同步运行专用的审计服务应用进程，用以全程跟踪应用服务进程的运行。以数据库系统为例，审计人员通过它建立一个监视文档库，作用如下。

·指定需要监视的数据库。

·指定需要监视的数据库的某个域□记录）。

·选择需要记录的数据库对象操作行为□OPEN、CREATE、UPDATE、DELETE)。

·选择需要记录的用户级行为□登录、创建、删除、授权）。

·选择审计日志产生后，通知审计人员的方式□人工查看、电子邮件、寻呼）。

此方案与应用系统密切相关，每个应用系统都需开发相应的独立程序，通用性、实

时性不好，价格将会较高。但审计粒度可因需求而设置，并且用户工作界面与应用系统相同。

现在最为有效的应用系统审计程序，已经解决了实时性问题，即在审计程序内增加一个能够和外部监控台保持实时通信的代理进程□Agent)，外部监控台的作用一是在网络上实时监控若干个应用系统审计进程的运行，二是实时接受、处理各Agent传送过来的审计数据。这种解决方案实际上是基于应用程序代理方案的扩充。原理如图22-24所示。

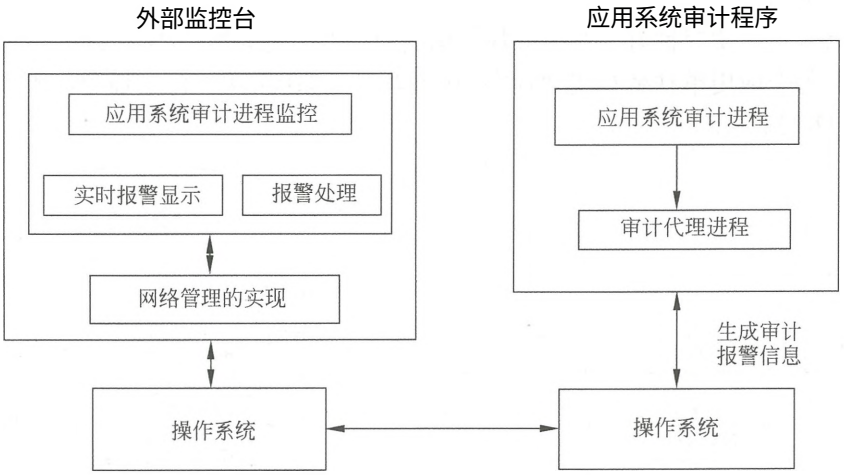


图22-24基于应用程序代理示意图

4)基于网络旁路监控方式，

(1) 工作原理。此方式与基于网络监测的安全审计实现原理及系统配置相同，仅是作用目标不同而已，其系统结构由网络探测器和安全控制中心组成。

① 网络探测器从网上获得用户访问应用系统的指令数据包，根据预先设置的规则分析数据包，进行应用操作的还原，经过数据处理后把实际的操作数据按一定格式提交给安全控制中心。

② 安全控制中心对获得的数据情报进行智能分析，当发现有可疑的操作时，自动进行记录入库、报警、阻断等操作。

③ 安全控制中心的控制台负责设置系统的各项工作参数；进行规则匹配设定以确定哪些操作是违法的，并且起到实时监视、响应的作用。

(2) 主要优点。

①能够有选择地记录任何通过网络对应用系统进行的操作并对其进行实时与事后分析和处理□如：报警、阻断、筛选可疑操作以及对审计数据进行数据挖掘等），无论系统采用的是C/S模式还是B/W/DB模式。

② 能够记录完整的信息，包括操作者的IP地址、时间、MAC地址以及完整的数据操作□如数据库的完整SQL语句）。

③ 审计系统的运行不对应用系统本身的正常运行产生任何影响，不需要占用数据库主机上的CPU、内存和硬盘。

④ 能够对审计数据进行安全的保存，能够保证记录不被非法删除和篡改。

原理如图22-25所示。

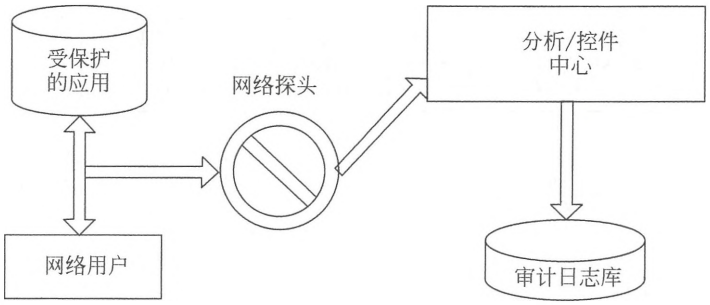


图22-25基于网络监测的安全审计示意图

22.5.3分布式审计系统

网络安全审计系统是对网络系统多个层次上的全面审计。对于一个地点分散、主机众多、各种连网方式共存的大规模网络，网络安全审计系统应该覆盖整个系统，即网络安全审计系统应对每个子系统都能进行安全审计，这样才能保证整体安全。因此，网络安全审计系统不但是一个多层次审计系统，还是一个分布式、多Agent结构的审计系统。多层次审计是指整个审计系统不仅能对网络数据通信操作进行底层审计□如网络上的各种Internet协议），还能对系统和平台□包括操作系统和应用平台）进行中层审计，以及为应用软件服务提供高层审计。

分布式审计系统由审计中心、审计控制台和审计Agent组成。网络安全审计系统结构，如图22-26所示。

1．审计中心

审计中心是对整个审计系统的数据进行集中存储和管理，并进行应急响应的专用软件，它基于数据库平台，采用数据库方式进行审计数据管理和系统控制，并在无人看守情况下长期运行。

2．审计控制台

审计控制台是提供给管理员用于对审计数据进行查阅，对审计系统进行规则设置，实现报警功能的界面软件，可以有多个审计控制台软件同时运行。

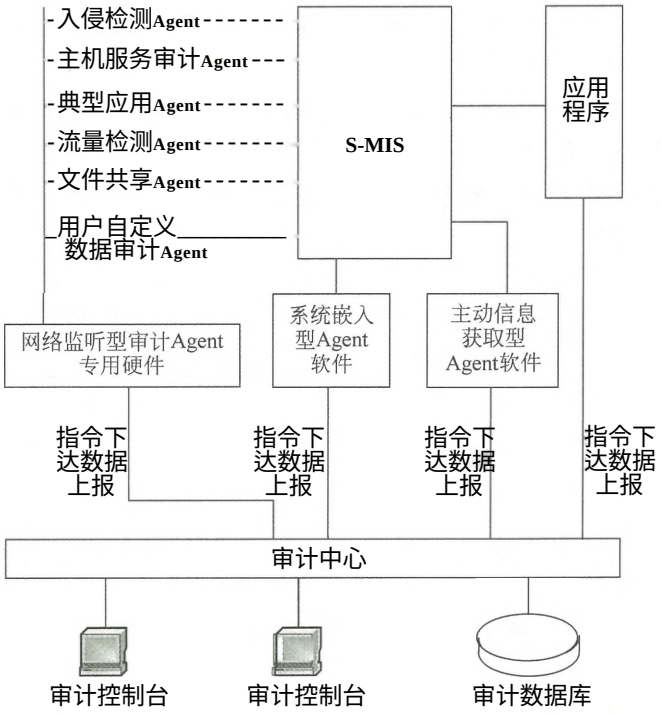


图22-26网络安全审计系统结构如

3.审计 **Agent**

审计Agent是直接同被审计网络和系统连接的部件，不同的审计Agent完成不同的功能。审计Agent将报警数据和需要记录的数据自动报送到审计中心，并由审计中心进行统一的调度管理。

审计Agent主要可以分为网络监听型Agent、系统嵌入型Agent、主动信息获取型Agent 等。

1) 网络监听型Agent

对于网络监听型的审计Agent，需要运行在一个网络监听专用硬件平台上，在系统中，该硬件被称为网探。根据所处的网络平台的不同，网探分为百兆网探、千兆网探等。

根据实际网络的需求，可以在每一个网探上配置实现不同应用的Agent。例如，在内部网的环境中可以适当配备文件共享Agent和用户自定义审计Agent等，在外部网的环境中可以配备入侵检测Agent、典型应用Agent和流量检测Agent。目前实现的网络监听型审计Agent有以下类型。

(1) 入侵检测Agent:主要实现对已知入侵手段的检测功能。

(2) 典型应用Agent:实现在Telent、HTTP、FTP、SMTP、POP3上的应用审计功能。

（3） 流量检测Agent:主要实现对实时和历史流量的检测功能。

（4） 文件共享Agent:主要实现对Windows环境中的基于Netbios Over TCP/IP的文件共享审计功能。

（5） 用户自定义数据审计Agent:实现对用户自定义服务的审计功能。

（6） 主机服务审计Agent:实现对网络上的主机所开放的服务端口进行审计的功能。

2） 系统嵌入型Agent

系统嵌入型Agent是安装在各个受保护的主机上的安全保护软件，这些软件实现基于主机的安全审计和监管。主要实现以下的功能。

（1） 收集系统日志信息，并根据规则判断异常事件的发生。

（2） 对系统内部产生的重要事件〔并不一定产生系统日志）进行收集。

（3） 对主机的资源和性能□包括CPU、内存占用、硬盘占用等）进行例行的监视和记录，发现主机异常运转，并适时杀除异常进程。

(4) 发现主机中存在的异常代码□例如特洛伊木马程序、后门程序、DDOS程序、Proxy程序等）。

（5） 对电子邮件进行审查□针对邮件服务器），发现垃圾邮件中转情况，并中止垃圾邮件的发送□针对垃圾邮件源头主机），发现含有非法内容的邮件，发出报警信息。

（6）Web浏览和发送内容过滤□例如对于Web方式的BBS)，自动删除含有不良内容的张贴文章。

（7） 实现系统强制型的审计□无法通过设置系统参数而绕过审计）。

在软件设计上可以借鉴和部分采用Wrapper技术。Wrapper技术是目前国际上兴起的新技术之一，它的主要思想是在己有的操作系统或应用平台外包裹一层安全增强功能，可以实现附加的网络访问控制、身份验证、审计、加密等功能，并且它对于原有的应用透明，能够兼容传统的应用。

系统嵌入型Agent主要针对一些主流操作系统和应用软件，例如，SUN Solaris操作系统、HP_UX操作系统、Linux操作系统 Windows NT Windows 2000操作系统，Apache Web Server IIS Web Server Sendmail 邮件系统 Exchange 邮件系统 Lotus Notes 邮件系统等。

3） 主动信息获取型Agent

主动信息获取型Agent主要实现针对一些非主机类型的设备的日志收集，如防火墙、交换机、路由器等。这些设备一般以硬件和固化型的软件提供应用，不支持在其操作系统上进行软件开发和嵌入软件模块，所以针对这些设备的日志收集需要采用主动信息采集的方法。

主动信息获取型的审计Agent以软件形式运行在相应的主机上，通过网络 Console 等方式同被审计设备进行交互，收集设备产生的日志或者定时轮巡一些参数，自己根据需求生成日志信息。

主动信息获取型的Agent主要采用以下的手段进行信息获取。

(1) 通过SNMP的TRAP方式。

(2) 通过定时的MIB轮巡，获取关键参数。

(3) 通过定时的Telnet script获取数值。

(4) 通过Console 口定时运行操作终端script来获取参数。

(5) 通过管理接口，如HTTP方式的管理来获取参数。

(6) 通过一些联动接口，如OPSEC接口获取参数。

(7)通过syslog server的方式获取日志信息。

主动信息获取型Agent将根据预先设置的script和运行参数，对收集的信息进行过滤、格式化，以提供统一的日志格式。