ISP

张晓伟　金　涛　编著

# 信息安全策略与机制

国家信息化安全教育认证(ISEC)系列教材



机械工业出版社
CHINA MACHINE PRESS

国家信息化安全教育认证(ISEC)系列教材

# 信息安全策略与机制

张晓伟　金　涛　编著

机 械 工 业 出 版 社

本书由浅入深地对信息安全、网络安全进行全方面讲述，并结合一些实际的应用经验，使读者快速掌握信息系统安全策略的具体制订过程。本书共分 13 章，涵盖了当今信息安全中主要的应用技术，也包含了一些安全策略应用的管理经验。本书在第 1 章、第 2 章及第 3 章为读者介绍了安全策略的一些基本概念、安全技术，以及安全策略从制订到实施的整个过程及风险评估；第 4 章至第 13 章，详细介绍了 9 套信息安全策略的具体内容以及策略所涉及的技术机制，也对策略的实施给予了详细的说明。

本书主要面向参加 ISEC 认证考试人员，也可供对信息安全有兴趣的普通读者阅读，同时也是企业管理人员考察自身企业信息安全状况的一本很好的参考书。

**图书在版编目(CIP)数据**

信息安全策略与机制/张晓伟等编著 —北京：机械工业出版社，2004.3
(国家信息化安全教育认证(ISEC)系列教材)
ISBN 7-111-14173-3

Ⅰ.信… Ⅱ.张… Ⅲ 信息系统—安全技术—资格考核—教材
Ⅳ.TP309

中国版本图书馆 CIP 数据核字(2004)第 019287 号

机械工业出版社（北京市百万庄大街 22 号 邮政编码 100037）
责任编辑：丁 诚
责任印制：洪汉军
三河市宏达印刷有限公司印刷·新华书店北京发行所发行
2004 年 4 月第 1 版·第 1 次印刷
787mm×1092mm 1/16 · 8.75 印张 · 208 字
0 001—5 000 册
定价：16.00 元

## 国家信息化安全教育认证(ISEC)专家组

卿斯汉　中国科学院信息安全技术工程研究中心主任　研究员
曲成义　中国航天科技集团公司第710研究所总工　研究员
许榕生　中国科学院高能物理研究所计算中心研究员
贾颖禾　国务院信息化工作办公室网络与信息安全组研究员
曹元大　北京理工大学软件学院院长　博士生导师
杨义先　北京邮电大学信息安全中心主任　博士生导师
林　鹏　国家计算机网络应急技术处理协调中心广东分中心副主任
　　教授级高级工程师
祁　金　公安部公共网络信息安全监察局管理监察处副处长
井乾元　公安部公共网络信息安全监察局安全对策处副处长
万平国　国际信息战略研究中心理事　中网通讯网络有限公司董事长
刘宝旭　中国科学院高能物理研究所计算中心副研究员

## 教材编委会

**主　任:** 宋　玲
**副主任:** 赵小凡　张会生　欧阳满　蔡金荣　沈志工
**成　员:** 洪京一　张宝泰　王　宏　孙论强　彭　澎　张晓伟
　　刘树安　刘　旸　马志谦　胡　铮　宁宇鹏　阎　慧
　　王　伟　薛静锋　辛　阳

# 出版说明

随着信息化在我国的不断深入和发展，信息技术和网络给社会的经济、科教、文化和管理等各个方面注入了新的活力。人们在感受它所带来的新体验、享受它为我们带来高效率的同时，也面临着日益突出的信息安全问题。党和国家领导人多次强调，必须充分认识到做好信息安全保障工作的重要性，大力搞好技术开发和人才培养。

对信息安全专业人才的需求是多层次的。从信息安全基础理论研究到新技术的开发利用，再到各级网络信息系统信息安全保障体系的建设、运行，需要根据不同要求有针对性的进行人才培养。

国家信息化安全教育认证(ISEC)项目是由信息产业部信息化推进司推出的信息安全领域的国家级认证体系。该项目由中国电子商务协会监督，由 ISEC 国家信息化安全教育认证管理中心统一管理与实施。ISEC 国家信息化安全教育认证管理中心以行业为基础、以技术为核心制定了一套面向应用的教育方案。根据工作性质的不同，教育对象被划分为规划决策层、管理运营层和操作层三个层次。认证体系的设计，课程内容及相应的教学考试大纲的编写和指定是针对三个层次人员对信息安全知识和技能的不同需求和理解程度的不同而制定的。确保不同层次，不同需求的各类人员从各自的角度充分掌握和理解信息安全的知识和技能。

本系列教材是在国家信息化安全教育认证(ISEC)专家组的指导下，由国家信息化安全教育认证(ISEC)教材编委会组织编写的。始终以 ISEC 国家信息化安全教育认证管理中心制订的各级考试大纲为依据，坚持面向行业用户的需求和侧重技术应用两个基本原则，全面地介绍了信息安全各种主流技术和管理规范，以帮助读者深入了解信息安全本质，并熟练掌握相应的技能，从而建立完备的信息安全观念。本系列教材包括：《网络安全基础》、《防火墙原理与技术》、《入侵检测技术》、《VPN 技术》、《PKI 技术》、《数据备份与灾难恢复》、《网络隔离与网闸》、《信息安全法规与标准》、《信息安全策略与机制》、《信息安全团队构建与管理》，共计 10 本。

在写作过程中，北京正阳天马信息技术有限公司为本系列教材的编写提供了很多宝贵的建议和支持。

# 前　言

目前，计算机网络信息系统的安全性已经引起人们的关注。随着管理信息系统在企业中的普及，各种安全问题与安全隐患不断产生，加上计算机病毒的广泛传播，使计算机信息安全面临着新的课题。

信息安全策略(Security Policy)描述了整体信息系统的安全目标，它详细说明了在信息系统中什么是应该做的，而什么是禁止做的。确定安全策略是一个组织实现安全管理和采取技术措施的前提，否则任何安全措施都将是无的放矢。

本书自成体系，循序渐进，覆盖面比较广，详细介绍了各种信息安全策略，探讨了相关的应用技术和设备。

本书共分为13章。第1章综合描述了信息系统与安全策略，使读者对基本的概念有一个初步的了解。第2章介绍了安全策略的规划、制订与实施的过程，并探讨了安全策略涉及的主要技术。第3章重点介绍了风险评估的具体内容。第4章重点介绍了环境安全与环境安全策略。第5章介绍了数据访问安全策略，描述了数据访问的控制方案。第6章探讨了数据加密与数据备份策略。第7章病毒防护策略，介绍了如何避免病毒的侵扰。第8章系统安全策略，包含了Web安全策略等多项网上应用系统的安全策略。第9章描述了身份认证及授权的安全策略，介绍了如何对权限进行管理。第10章主要介绍了灾难恢复及事故处理、紧急响应等的安全策略。第11章介绍了口令及口令的管理等安全策略与措施。第12章描述了定期审计与复查策略。第13章描述了安全教育策略与安全策略的实施过程。

本书在编写过程中参考了大量资料，并得到了国家信息化安全认证中心有关专家的大力帮助，对此表示衷心感谢。本书由云南大学信息学院计算机科学与工程系副教授张晓伟及金涛同志共同编写。由于作者水平有限，书中错误之处恳请各位专家批评指正。

本书主要适用于参加国家信息化安全教育认证(ISEC)考试人员，也可供大专院校计算机专业学生及各类信息安全爱好者使用。

编　者

2004年2月19日

# 目　录

# 第 1 章　信息系统与安全策略概述

**本章导读：**

本章重点介绍了信息安全策略的基本知识与基本概念，包括系统、信息系统、策略、安全策略等内容。

目前，企事业单位对于发展和完善信息管理系统的计划已经在促使或应该促使企业的管理阶层或组织机构重新调查信息流动或信息系统的安全性是否全面是否完善。在向信息自动化发展的过程中，应该首先强化的是信息系统的安全性，而不是仅仅限于各种问题的解决方案。在过去，安全性措施较为被动，只针对发生的各类事件来反应、处理，很少做到有计划地主动检查是否存在安全隐患，以达到预防一切安全问题发生的目的。这种状况现在应该加以改变，从而适应高速发展的信息技术。信息系统安全性问题一直都直接属于 IT 或相关技术部门的管理范围，但最近也经常可以看到企业中出现专项管理的高层次管理人员，例如安全系统经理或安全系统总监等职位的出现，由此可见互联网的盛行与企业信息管理系统的发展正在逐渐成为新的商业发展方向，伴随其而来的信息系统安全风险问题，也同时成为了受高度重视的重要方面。

被动的在需要时才去寻找解决方案的模式，已经不能适应于现代化的管理体系。通过了解信息管理系统的本质，也可以了解到完善的安全机制必须要起始于制定明确的安全性策略，而且必须做到兼顾考虑目前以至未来在系统运行方面的所有安全因素。而在讨论安全性问题与信息系统运行时，如果出现两者有抵触、制约的情况，以至信息系统数据的存取遭到拒绝时，系统的整体安全设定只能是作出最简单的选择，通过或被拒绝。其实，最安全的系统应该是完全独立的，不与外界接触的系统，然而往往这种系统是达不到信息管理系统的要求的。所以，制订相应的安全策略就是要解决这种现象，即不影响整体系统的正常运行，又可以达到高安全性的目的。

## 1.1　信息系统的安全管理

系统是由相互作用和相互依赖的若干部分结合成的具有特定功能的整体。系统一般包括下列因素：

(1) 一种产品或者组件，例如计算机、所有的外部设备等；

(2) 操作系统、通信系统和其他相关的设备、软件，构成了一个组织的基本结构；

(3) 多个应用系统或软件(财务、人事、业务等等)；

(4) IT 部门的员工；

(5) 内部用户和管理层；

(6) 客户和其他外部用户；

(7) 周围环境，包括媒体、竞争者、上层管理机构。

根据上述系统的含义,可以得出以下的结论:

(1) 系统由若干个具有独立功能的部分组成;

(2) 组成系统的各元素之间相互联系、相互制约;

(3) 系统是一个整体,有明确的目标;

(4) 系统有一定的结构。一个系统是其构成要素的集合,这些要素相互联系,相互制约;

(5) 系统有一定的功能。功能是指系统与外部环境相互联系和相互作用中表现出来的性质、能力和功效。

信息系统指的是实现系统中各实体间数据的传输、交换、转移,并使各实体通过高速信息交换相互协作,提高工作效率的解决方案。信息系统存在于任何一个社会组织中,它渗透到组织中的每一个部分,就像人体组织的神经系统,分布在人体组织中的每一个部分。信息系统是为管理服务的,信息系统不同于其他系统,它不是从事某一具体工作,而是起到关系全局并使系统中各子系统协调一致的作用。信息系统主要由信息资源、硬件系统和软件系统三部分组成,各部分相互作用以达到提供信息的目的。

信息系统的概念包括下面几个方面的含义:

(1) 信息系统的输入与输出目标明确;

(2) 信息系统的输入、处理和输出反映了信息系统的功能和目标;

(3) 信息系统中各功能之间相互联系;

(4) 信息系统中的反馈用于调整或改变输入或处理活动的输出,反馈是对系统进行有效控制的重要手段;

(5) 信息系统并不是特定的指基于计算机的信息系统。

经常会被提到的"安全"是一个广泛的概念,它涉及到许多不同的区域或领域(物理设备、网络、系统平台、应用程序等),和每个区域相关的风险、威胁及解决方法。信息安全指的是在信息传递的过程中,数据被破坏、偷窃或丢失的风险性。讨论信息安全的时候,应该避免只关心黑客和操作系统的某些漏洞,虽然它们是安全中重要的组成部分,但它们也只是安全广义概念中的两个组成部分。

企业对于信息网络的依靠已经越来越紧密,体现在电子商务、内部信息管理系统等在企业中得到的实际应用。对于拥有网络连接并以网络连接作为基础来进行信息交换的企业组织来说风险与威胁是永远存在的。信息安全永远是一个动态发展的过程,它不仅仅是纯粹的技术范畴,仅仅依赖于安全产品的堆积来应对迅速发展变化的各种攻击手段是不能持续有效的。信息安全建设是一项复杂的系统工程,规划、管理、技术等多种因素相结合使之成为一个可持续的动态发展的过程。

既然绝对的信息安全是不存在的,每个网络环境就都有一定程度的漏洞和风险。信息安全问题的解决只能通过一系列的规划和措施,把风险降低到可被接受的程度,同时采取适当的机制使风险保持在此程度之内。当信息系统发生变化时,应当重新规划和实施安全管理来适应新的安全需求。信息系统的安全性往往取决于系统中最薄弱的环节——人。人是信息安全中最关键的因素,同时也应该认识到人也是信息安全中最薄弱的环节。

经常可以听到这样的新闻:病毒程序给某行业的信息系统造成了严重的破坏,黑客获取了信用卡的信息,大型网站主页被破坏等等。这时,可能普遍的认识是因为企业没有安装安全产

品(如:防火墙、入侵检测系统、防病毒系统等),或因为安全产品没有起到相应的作用,但其实这些问题很大程度上是由于安全管理没有得到有效实施而造成的。

安全管理是企业信息安全的核心,是指针对于企业的信息安全,而制订并审查实施过程的一整套解决方案。安全管理包括风险管理、安全策略和安全教育,这三个组成部分构成了整个企业安全规划体系的基础。风险管理用来识别企业的资产,评估威胁这些资产的风险,评估假定这些风险成为现实时企业所承受的灾难和损失。然后,通过降低风险(如:安装防护措施)、避免风险、转嫁风险(如:买保险)、接受风险(基于投入/产出比考虑)等多种风险管理方式得到的结果来协助管理部门根据企业的业务目标和业务发展特点来制定企业信息安全策略。安全策略是指在一个特定的环境里,为保证提供一定级别的安全保护所必须遵守的规则。根据安全策略的内容,还需要对所有涉及的人员进行安全教育。

根据企业规模、业务发展、安全需求的不同,安全策略可以繁简不同,但是语言描述都应该简单明了、通俗易懂并直接反映主题,避免含糊不清的情况出现。信息安全策略是企业安全的最高方针,由高级管理部门支持,一定要形成书面文档、广泛发布到企业所有员工手中。同时,要对所有相关人员进行安全策略如何实施的培训,对于特殊责任人员要进行特殊的培训,使得安全策略能够真正在企业正常运营过程中得到贯彻、落实、实施。在安全规划实行过程中,管理部门的支持也是非常重要的因素,通过专门负责的管理人员的有效支持,会大大加强安全管理的实施力度。

安全管理通过识别企业的信息资产,评估信息资产的价值,制定和实施安全策略、安全标准、安全方针、安全措施来保证企业信息资产的完整性、机密性、可用性。

## 1.2　企业策略从制订到实施的过程

企业策略是在企业发展的过程中,管理阶层制订的,或管理阶层指定人员制订的,企业中每一位员工都要遵守的准则体系。安全策略是企业策略构成的重要部分,是在企业策略中各方面安全的准则,而信息安全策略又是企业安全策略中最重要的组成部分。

企业策略从制订到实施分为三个阶段,分别是分析阶段、策略制订阶段和执行阶段。企业信息安全策略的制订过程如下。

(1) 分析阶段也可以称为构思阶段,主要指在制订策略前,首先对策略目标进行正确的定位,并结合企业的自身的情况和系统的安全性,作全面的调查并记录、存档的一系列过程。

制订企业策略,或者具体到制订企业信息安全策略,总是从企业的领导阶层发起,直接由一位高层领导负责指出策略制订的主要方向、策略的实施目标,再由指定的人员或部门开始作前期的调查,并记录存档。

(2) 策略制订阶段主要指通过对整个信息系统全面的调查分析后,经过制订、审查并修改,逐步完善整个策略体系。要注意策略在初期制订时,应避免内容过于复杂,或者目标定位不清晰。

对任何一种公司文档来说,制订完成后进行审查是一种惯例。策略是不同于一般类型的文档,审查过程不仅要从技术方面考虑,还要从法律方面进行考虑。在策略被批准执行之前,决策层领导必须要对整个评审过程有清楚的了解。第一次审查可以由作者本人进行,不同的

部门依次进行审查。审查过程将在不同部门间成立的审查委员会监督下进行。策略涉及到的部门或分部的负责人要提出意见。企业如果有律师,也有必要参与这个过程。律师会对策略中的某些部分很熟悉,比如策略的实施以及如何监督策略的执行。

企业管理层对策略的最终版本提出意见——也就是批准过程,批准应该是在策略审查过程之后的。如果管理层不同意这些策略的内容,那就需要重新进行整个过程。

(3) 执行阶段主要指策略制订完成后,对相关人员进行培训并贯彻实施的过程。

在策略批准以后,就必须执行。没有监督措施的策略就会被任意违反,这和法律需要强制执行一样。

## 1.3 信息安全策略概述

### 1.3.1 信息安全策略的特点

安全策略是一种处理安全问题的管理策略的描述。策略要能对某个安全主题进行描绘,探讨其必要性和重要性,解释清楚什么该做,什么不该做。下面为管理拨号进出访问控制的策略描述。

对网络的所有拨号访问应该通过严格的身份认证控制来集中保护。调制解调器应该被配置成拨入或者拨出,不能拨入、拨出都被允许。网络管理员应该提供程序来准许对调制解调器服务的访问。在没有经过审查和同意之前,用户不能在网络的任何地方安装调制解调器。

安全策略应该简明,在生产效率和安全之间应该有一个好的平衡点,易于实现、易于理解。安全策略必须遵循三个基本概念:确定性、完整性和有效性。

另外,安全策略还可能包含一些表面上和上述三个概念没有任何关系的地方。因为整个企业组织的整体安全是最重要的,不能忽略小的方面而影响整体的安全。这包括对设备、数据、电子邮件、互联网等的可接受的使用策略。

信息安全策略是描述程序目标的高层计划。它既不是指导方针或标准,也不是程序或控制。安全策略为一个总体安全程序提供一份计划,使应用者能按照定义好的方式来保证安全。

策略中不应该包含具体的执行程序。程序是指执行的详细步骤,而一个策略是对程序应该实现的目标的有效声明。安全策略使用一般的语言描述,所以并不影响具体的执行过程。有些策略则会有更加详细的执行说明或相关的文件资料,但是这些细节不应该出现在策略本身之中。

### 1.3.2 制定策略的时机与必要性

理想情况下,制定策略的最佳时间是在发生第一起网络安全事故以前。尽早制订安全策略,有利于安全管理人员了解什么需要保护以及可以采取什么措施。而且,为一个发展中的基础设施编写策略总比为配合一个现存的业务运作环境而改编策略要更有效率。

(1) 任何业务动作过程均存在不同程度的风险,所以要及时用安全措施来减少这种风险。安全策略要考虑业务运作过程,应用保护它们的最佳实践措施可以保证系统安全,并且在重要

数据丢失时减轻损失。

(2) 新经济提高了电子信息的价值。电子信息以及存储这些信息的机器和业务动作是密不可分的,所以企业很愿意向保险公司申请为它们投保。保险公司就会向那些要求投保的公司询问安全策略和方法,他们关心的第一个问题也许就是查看安全策略。对于没有安全策略的公司在投保时,大部分保险公司都不予考虑。保险公司会认为,如果没有经历过制定安全策略的过程,这个企业不会知道要保护什么,所以接受它们的投保太冒险了。

(3) 一个包括软件开发策略在内的安全策略对于开发更安全的系统是有指导作用的。通过创建这些指导方针和标准,开发者将会有章可循,测试者可以明了测试的对象,管理员也会清楚需求是什么。自适应型(即无策略)的开发,投资和责任都很大。制定和实施软件开发策略并作为开发者的指南,可以减轻以后的责任。

(4) 在安全事故发生以后再来实施安全策略就像是亡羊补牢,千万不要认为发生过一次的事情就再也不会发生,相反,发生过一次的事情很有可能再次发生。

(5) 当发生一次安全事故以后,在制定策略的时候,不要只把重点放在被攻破的地方。因为那只是许多应该注意的地方中的一处。要从全局考虑问题,永远不要把它们孤立对待。只有这样,才能编写出一个综合而全面的策略。

(6) 拥有一份完备的安全策略可以在一定程度上表明企业在满足客户的需求。在新的客户开发过程中,安全策略给客户的感觉是,对他们所关心的安全问题有很认真的态度。

(7) 政府或机关单位对安全性的要求尽管一直在变化。但是对安全性的需求一直非常重要,有时政府或机关单位会制定一些安全条例,规定为政府服务的企业要照条例遵守,同时还要遵守其他已有的条例。由于越来越多这方面的建议被提出,对安全策略的需求也会增多。当企业为政府或机关单位工作或者合作时,一份安全策略应该是首先要引起注意的事情。

(8) 企业也许要向客户展示其运作过程是符合质量控制标准的。国际标准化组织(ISO)9001 规定了一个验证质量控制的标准,该标准适用于所有商业运作过程。对于质量控制标准所要求的可评价的安全程序来说,安全策略可以作为该程序实施的指导方针。

### 1.3.3　怎样进行开发策略

在编写策略文档之前,应当先确定策略的总体目标,是为了保护公司以及公司和客户之间的往来,还是保护整个系统的数据流的安全性。首先要做的是确定要保护什么以及为什么要保护它们。

策略可以涉及到硬件、软件、访问、用户、连接、网络、通信以及实施等各个方面。在编写之前,要确定什么系统和过程对于公司的业务来说是重要的,这会有助于确定需要哪些种类型的策略,需要哪些策略来完成任务。总而言之,策略制订前的目标是,必须保证已经把所有可能需要策略的地方都考虑到。

**1. 确定策略的结构**

信息安全策略并不一定只在一份文档内完成,也可以由多份文档组织形成。正如本书的组织结构一样,它可以分割成许多相关的章节,而不是从头讲到尾。因此应该避免只编写一份策略文档,最好写成许多独立的文档,把这些独立的文档定义为信息安全策略的章节。这将使策略易于理解,易于分配,也给个人提供了培训机会,因为每个策略都有自己负责的区域。对

策略分区也有利于日后的修改和更新。

对于业务范围内的每一个系统和责任范围内的每一个子系统，都应当定义一个策略文档。可以把电子邮件策略从互联网使用策略中独立出来，一种常见的错误是试图用一种大纲类型的格式写出一份综合式的策略。这样做的结果就是一份冗长、混乱的文档，缺乏可读性，也不会得到其他人的支持。应使策略文档尽可能的简洁、重点突出、阐述清楚、组织有逻辑性和界面整洁，使其更具有可读性，而且尽量不要用一些专业术语来向读者描述。

**2. 风险评估/分析或者审计**

作为风险评估的一部分，企业也许会作一些安全方面的穿透性测试。这个测试要同时在内部和外部网络上执行，对每一个已知的访问点进行测试，以发现所有未知的访问点。这种广泛的评估为了解网络配置提供了必要的信息，这些信息可以用来决定配置、访问以及制订其他策略，也可以明确网络是如何支持公司业务的。

管理人员可能会发现他们自己就可以浏览整个信息系统，确定系统风险并管理企业的物资清单。也许管理人员确实可以完成这些工作，但最好还是请非企业内部的专业安全人员来做这些事情。主要的原因是因为这些专业人员不了解整个系统、已经有的最佳安全措施或者其他的内部信息，这使得在评估的时候不会带有偏见。专业人员可以从一个黑客的角度来观察你的系统是否有潜在的漏洞，并确定这些漏洞带来的后果，这样就可以很快发现系统中的漏洞、弱点和其他的问题。

## 1.4 制订信息系统安全策略的构想

当企业的一位高级管理人员明确了整个企业的信息安全策略的范围及目标后，已经指派好的部门或人员就会开始对策略整体提出一些具体的构想，并且进行逐步完善。

### 1.4.1 制订信息安全策略的原则

在制订信息安全策略时，要遵循以下的原则：

(1) 先进的网络安全技术是网络安全的根本保证。用户对自身面临的威胁进行风险评估，决定其所需要的安全服务种类，选择相应的安全机制，然后集成先进的安全技术，形成一个全方位的安全系统。

(2) 严格的安全管理是确保安全策略落实的基础。各计算机网络使用机构、企业和单位应建立相应的网络安全管理办法，加强内部管理，建立合适的网络安全管理系统，加强用户管理和授权管理，建立安全审计和跟踪体系，提高整体网络安全意识。

(3) 严格的法律、法规是网络安全保障的坚强后盾。计算机网络是一种新生事物。它的好多行为无法可依，无章可循，导致网络上计算机犯罪处于无序状态。面对日趋严重的网络犯罪，必须建立与网络安全相关的法律、法规，使非法分子不会轻易发动攻击。

### 1.4.2 信息安全策略的设计范围

一套信息安全策略应该全面地保护信息系统整体的安全，在设计策略的范围时，主要应考虑以下几个方面。