信息系统安全管理

钱钢 著

东南大学出版社

信息系统安全管理

钱 钢 著

东南大学出版社

内 容 提 要

在信息化建设中进行信息系统安全管理，是一个新的和十分重要的课题，已经引起国家的高度重视。信息系统安全管理不单单是管理体制或技术问题，而是策略、管理和技术的有机结合。从安全管理体系的高度来全面构建和规范我国的信息安全，将有效地保障我国的信息系统安全。

本书围绕信息系统的安全管理这一主线，在国内较早地全面透彻地介绍了信息系统安全管理的基本框架、基本要求及与此相关的知识，力求做到既有理论深度，又有较强的实务性。本书将指导信息系统安全管理者系统准确地把握安全管理的思想，正确有效地运用安全管理的方法、技术与工具。

本书可作为信息化管理者、IT 咨询顾问、IT 技术人员的参考手册和培训教材，也可作为信息管理与信息系统专业、信息安全专业、计算机类专业的本科生及研究生学习和掌握安全管理方面的综合性教材或参考书，对于非专业人员也有很大的参考和使用价值。

图书在版编目(CIP)数据

信息系统安全管理/钱钢著. —南京：东南大学出版社，2004.10
ISBN 7-81089-740-3

Ⅰ.信… Ⅱ.钱… Ⅲ.信息系统-安全管理 Ⅳ.TP309

中国版本图书馆 CIP 数据核字(2004)第 100104 号

东南大学出版社出版发行
(南京四牌楼 2 号 邮编 210096)
出版人：宋增民
江苏省新华书店经销 江苏兴化印刷厂印刷
开本：787mm×1092mm 1/16 印张：18.25 字数：465 千字
2004 年 10 月第 1 版 2004 年 10 月第 1 次印刷
印数：1～2 800 册 定价：28.00 元

(凡因印装质量问题，可直接向我社发行科调换。电话：025-83795801)

前　言

对信息系统安全进行系统化管理具有重要的现实意义，它成为摆脱当前信息安全困境的有效途径。本书是以国家863信息安全应急计划的信息安全系统工程方法研究课题成果为基础，为解决信息系统安全管理中遇到的实际问题提出了一套系统化的管理方法。全书首先对国内外信息安全的现状、信息安全的内涵、信息安全管理模型及标准进行了综述，在对现代信息技术的特点和管理理念进行分析的基础上，以创新观念解决信息安全问题，即通过引入安全系统工程能力成熟模型，构建基于过程的信息系统安全管理的工程化体系，提出了信息系统风险分析和实现安全审计的方法，并对体系的内容作了较深入介绍。最后，针对安全事件发生后的法律诉讼，本书著者作为江苏省目前仅有的两名计算机司法鉴定人之一，特意增加计算机司法鉴定一章，以供读者了解这一新的和十分重要的内容。

本书内容包括四个部分，第一部分介绍了有关信息系统安全管理的基本知识，包括保障信息系统安全的一般技术和国内外信息安全管理标准，提出了信息系统安全管理的工程化体系；第二部分介绍了信息系统安全的风险评估及应用、安全审计技术以及常见操作系统的安全管理。第三部分介绍了电子政务、电子商务的安全管理，并在此基础上介绍了信息系统安全体系的设计和典型应用；第四部分从法律保障的意义上讲述计算机司法鉴定的内容和过程。通过对本书的学习，信息安全及相关行业的从业人员可对风险、安全策略及安全工程的概念有所了解，并明确信息系统安全管理所应包含的内容。

本书是在中国博士后科学基金和东南大学博士后科学基金的资助下完成的，并得到了南京师范大学国家211工程重点项目“信息安全保密技术与相关数学理论研究”的资助。在本书的成书过程中，得到了东南大学信息与通信工程博士后流动站胡爱群教授的悉心指导，他作为国家863计划信息安全技术主题专家，为本书的撰写给予了大力的支持和帮助；魏然博士在百忙之中，抽出宝贵的时间对本书内容做了整体审核并提出许多建设性意见，使我受益匪浅，在此一并表示真诚的感谢。此外，对所有参考文献的作者和其他被引用文献资料的作者表示衷心的感谢，正是由于他们的辛勤劳动才使得本书的内容得以充实。限于时间与水平，不妥之处在所难免，敬请批评指正。

编　者

2003年11月于南京

目　录

第一章　信息系统安全综述

1.1 影响系统安全的因素

1.1.1 信息系统安全的重要性

信息系统的安全之所以重要，其原因在于：

1. 信息系统的重要应用成为受威胁和攻击的目标。因为信息系统存储和处理有关国家安全的政治、经济、军事情况及一些部门、组织的机密信息或个人的敏感信息，因此成为国外敌对国家情报部门和一些组织或个人威胁和攻击的目标。

2. 信息系统本身的脆弱性成为不安全的内在因素。由于信息系统本身的脆弱性以及硬件和软件的开放性，加之缺乏完善的安全措施，容易给犯罪分子以可乘之机。

3. 随着计算机功能的日益完善和运行速度的不断提高，系统组成越来越复杂，其本身存在的隐患就成为不安全因素。另外，随着计算机网络的迅速发展，规模也越来越庞大，更增加了隐患和被攻击的区域及环节。

4. 随着应用的需要，计算机使用的场所逐渐从条件优越的机房转向工业、野外、海上、天空、宇宙、核辐射环境，其气候、力学、电磁和辐射等应力都比机房恶劣，恶劣的环境条件会导致计算机出错概率和故障的增加，其可靠性和安全性便受到影响。

5. 随着信息系统的广泛应用，应用人员队伍不断扩大，各层次的应用人员增多，人为的某些因素，如操作失误的概率增加，会威胁信息系统的安全。

6. 安全是针对某种威胁而言的，对信息系统来说，许多威胁和攻击是隐蔽的，防范对象是广泛的、难以明确的，即潜在的。

7. 信息系统安全涉及到许多学科，既包含自然科学和技术，又包含社会科学。就技术而言，信息系统安全涉及计算机技术、通信技术、存取控制技术、验证技术、容错技术、诊断技术、加密技术、防病毒技术、抗干扰技术和防泄漏技术等，因此它是一个综合性很强的问题，并且其技术、方法和措施还要根据外界不断变化的威胁和攻击情况而不断变化，这就增加了保证信息系统安全的难度。

1.1.2 影响信息系统安全的因素

影响信息系统安全的因素，可以分为两大类：一类是自然因素，一类是人为因素。

1. 自然因素

自然因素是指因自然力造成的地震、水灾、火灾、风暴、雷击等，它可以破坏信息系统实体，也可以破坏信息。自然因素可以分为自然灾害、自然损坏、环境干扰等因素。

(1)自然灾害：各种自然灾害造成的事故和损失，如失火、地震灾害、风暴灾害、洪水灾害、雷电灾害、静电等。

(2)自然损坏:自然损坏是指因系统本身的脆弱性而造成的威胁。例如,元器件失效、设备(包括计算机、外围设备、通信及网络、供电设备、空调设备等)故障、软件故障、设计不合理、保护功能差和整个系统不协调等。

(3)环境干扰:环境干扰如高低温冲击、电压降低、过压或过载、振动冲击、电磁波干扰和辐射干扰等因素。

2. 人为因素

人为因素分为无意损坏和有意损坏两种。

(1)无意损坏:无意损坏是过失性的,是因人的疏忽大意造成的。例如,操作失误、错误理解、无意造成的信息泄露或破坏。

(2)有意破坏:有意破坏是指直接破坏设备、盗窃资料及信息、非法使用资源、施放病毒或使系统功能改变等,这是应该引起特别注意的。

1.2 信息系统安全策略

1.2.1 安全策略的一般原则

1. 需求、风险、代价综合平衡原则

一个信息系统的安全,要根据系统的实际情况(包括系统任务、功能、环节及工作状况等)、需求、威胁、风险和代价进行定性和定量相结合的分析,找出薄弱环节,制定规范。具体措施往往是上述因素相互平衡、折中的结果。

2. 综合性、整体性原则

对信息系统的安全对策,应该用系统工程的观点进行综合分析,贯彻整体性原则。一个信息系统包括人、设备、软件、数据、网络以及运行等环节。这些环节在一个系统安全中的地位、作用及影响,只有从系统综合、整体角度去分析,才能对可能采取的措施的有效性、可行性得出恰当的结论。另外,一种安全技术可以有多种措施,并且可能是多种措施综合使用的结果,而各种措施的代价、效果对不同的系统并不一定相同。因此,综合性、整体性分析是非常需要的。

3. 易操作性原则

信息系统的许多安全措施需要人去完成,如果措施过于复杂,以致对完成安全操作的人要求很高,这样将降低安全性。例如,密钥的使用,如果要求人进行过多的记忆,则会带来许多问题。

4. 适应性和灵活性原则

信息系统的安全措施要能比较容易地适应系统的变化(需求变化、威胁与风险变化),或用较小代价即可适应变化。在安全措施中,一定要考虑出现不安全情况时可采取的措施,例如系统应急措施、快速恢复措施、隔离措施等,以限制不安全状态的扩展。

5. 可评估性原则

对信息系统采取的安全措施应能评价,应有相应的评价规范和准则。

1.2.2 安全策略的职能

信息系统安全的实质就是安全策略、安全管理和安全技术的实施。安全策略的职能可以

概括成三个方面:限制、监视和保障。

1. 限制

限制那些非法的、偶然的和非授权的信息活动,支持正常的信息活动。

2. 监视

监视系统的运行,发现异常的信息活动或设备(硬件和软件)故障,进行必要的、法律的、行政的或技术的处理。

3. 保障

保障系统资源(硬件、软件)和各类数据及信息的完整性、保密性和可用性。

1.2.3 安全策略的措施

从概念上讲,信息系统的安全包含两方面的含义:一是安全,二是保密。为此,应采取的对策主要包括四个方面:法律保护、行政管理、人员教育和技术措施。

1. 法律保护

有关信息系统的法规大体上可以分成两类:一类是社会规范;另一类是技术规范。

(1)社会规范:社会规范是调整信息活动中人与人之间的行为准则。要结合专门的保护要求定义合法的信息实践,不正当的信息活动要受到民法或刑法的限制或惩处。发布相应的法律法规,明确用户和系统人员应履行的权利和义务,包括保密法、数据保护法、计算机安全法、计算机犯罪法等。

所谓合法的信息实践是指在一定的人—机环境条件下,符合社会规范和技术规范要求,并满足系统或用户应用目标的信息活动。合法的信息实践受到法律保护。

(2)技术规范:技术规范是调整人与自然界之间关系的准则,其内容包括各种技术标准和规程,如计算机安全标准、网络安全标准、操作系统安全标准、数据和信息安全标准、电磁兼容性标准、电磁泄漏极限等。这些法律和标准是保证信息系统安全的依据和主要的保障。

2. 行政管理

行政管理是依据系统的实践活动,为维护系统安全而建立和制定的规章制度和职能机构。这些制度主要有:

(1)组织及人员制度。包括机构、人员的安全意识和技术培训及人员选择,严格的操作守则,严格的分工原则。严格区分系统管理员、终端操作员和系统设计人员等角色,不允许工作交叉。

(2)运行维护和管理制度。包括设备维护制度、软件维护制度、用户管理制度、机房保卫制度、密钥管理制度、出入门管理、值班守则、操作规程、行政领导定期检查和监督等制度。

(3)计算机处理的控制与管理制度。包括编程控制、程序和数据的管理,拷贝及移植、存储介质的管理,文件的标准化及通信和网络的管理。重要计算机要专机专用,不允许兼作其他用机。终端操作员因事离开终端时,必须将终端退回到登陆界面,避免其他人员使用该终端进行非法操作。

(4)对各种资料要妥善保管,严格控制。各类人员所掌握的资料要与其身份相适应。例如,终端操作员只能阅读终端操作手册,系统管理员只能阅读和使用系统手册。

重要信息系统的安全组织机构包括安全审查机构、安全决策机构、安全管理机构和领导机构等。安全管理机构必须由安全、审计、保安、系统分析、软硬件技术人员、通信等有关方面的

人员组成。其中安全管理、保安和系统管理人员的职责是：

① 安全管理人员具体负责本系统区域内的安全策略的实现，保证安全策略的长期有效；负责安全设备安装维护、日常操作监视，应急条件下安全措施的恢复和风险分析等；以及对系统修改的授权，对特权和口令的授权，对违章报告、报警记录、控制台记录的审阅和安全人员的培训，遇到重大问题时及时向主管领导报告等。

② 保安人员主要负责非技术性的常规工作，如信息系统场地的警卫、办公室的安全、验证出入管理的手续和各项规章制度的落实。

③ 系统管理人员的主要任务是安装和升级系统，控制系统的操作、维护和管理，使系统处于可靠的运行状态。

3. 人员教育

对信息系统工作人员，如操作员、系统管理员、系统设计人员，因为他们对系统的功能、结构比较熟悉，对系统威胁很大，需进行全面的安全、保密教育，进行职业道德和法制教育，对于从事国家机密、军事机密、财政金融或人事档案等重要信息系统工作的人员更应重视教育，并挑选素质好、品质可靠的人员担任。

4. 技术措施

技术安全措施是信息系统安全的重要保证。实施安全技术，不仅涉及计算机和外部设备及其通信和网络等实体，还涉及到数据安全、软件安全、网络安全、运行安全和防病毒以及结构和工艺技术。安全技术措施应贯彻于系统分析、设计、运行和维护及管理的各个阶段。

信息系统安全策略的措施是系统的有机组成部分，应以系统工程的思想、系统分析的方法，对系统的安全需求、威胁、风险和代价进行综合分析，从整体上综合最优考虑，采取相应对策。只有这样才能建立起一个有一定安全保障的信息系统。

1.3 信息系统安全保障

1.3.1 信息系统的安全需求

信息系统的安全就是为保证信息系统资源的完整性、可靠性、保密性、安全性、有效性和合法性，维护正当的信息活动而建立和采取的措施和方法的总和，以保证系统的硬件、软件和数据不因偶然的或人为的因素而遭受破坏、泄漏、修改或复制。信息系统的安全需求主要包括：保密性、安全性、完整性、可靠性和可用性以及信息的有效性和合法性。

1. 保密性

保密性是利用密码技术对信息进行加密处理，以防止信息泄漏。这就要求系统能对信息的存储、传输进行加密保护，所采用的加密算法要有足够的强度，并有有效的密钥管理措施，在密钥的产生、存储、分配、更换、保管、使用和销毁全过程中，密钥要难以被窃取，即使被窃取了也没有用。此外，还要能防止因电磁泄漏而造成信息泄密。

2. 安全性

这里主要是指信息系统的实体安全。它包括物理安全、人事安全、过程安全等方面。物理安全是指对计算机设备与设施的防护措施(如防护围墙、警卫人员、安装防电磁泄漏的屏蔽设施等)；人事安全是指对某人参与信息系统工作和接触敏感信息是否合适，是否值得信任的一

种审查;过程安全包括准许某人对计算机设备进行访问、处理信息的 I/O 操作、装入软件、连接终端用户和其他日常管理工作等。

3. 完整性

完整性是指程序和数据等信息的完整程度,它是防止信息系统内程序和数据被非法删改、复制和破坏,并保证其真实性和有效性的一种技术手段,完整性分为软件完整性和数据完整性两个方面。

(1)软件完整性:为了防拷贝,软件要具有唯一标识,还要拒绝动态跟踪;为了防修改,软件要具有抗分析能力和完整性检验手段。

(2)数据完整性:是保证存储或传输的数据不被非法删改或意外事件的破坏,保持数据的完整。

4. 可靠性和可用性

可靠性即保证系统硬件和软件无故障或差错,以便在规定条件下执行预定算法的能力,可用性即保证合法用户能正确使用而不出现拒绝访问或使用,并且要防止非法用户进入系统访问、窃取系统资源和破坏系统,也要防止合法用户对系统的非法操作或使用。因此,要使用可靠性保证和故障诊断技术、识别与验证技术和访问控制技术等。

5. 信息的有效性和合法性

信息交换的双方应能对对方的身份进行鉴别,以保证收到的信息是由确认的对方送过来的。信息接收方应能证实它收到的信息的内容和顺序都是真实的,信息的发送方可以要求对方提供回执,但不能否认从未发过何种信息并声称该信息是接收方伪造的;信息的接收方不能对收到的信息进行任意修改或伪造,也不能抵赖收到的信息。

1.3.2 信息系统的安全设计原则

为了保证信息系统的安全,防止非法入侵对系统的威胁和攻击,要根据系统安全需求进行安全设计。这里我们提出了 19 条设计原则,可作为设计依据和参考。

(1)成本效率原则:应使系统安全效率最高而成本最低。

(2)简易性原则:简单易行的控制比复杂控制更有效和更可靠,也更受人欢迎,而且省钱。

(3)应急控制原则:一旦控制失灵(紧急情况下)时,要采取预定的应急控制措施和方法步骤。

(4)公开设计与操作原则:保密并不是一种强有力的安全方式,过分信赖可能会导致控制失灵。对控制的公开设计和操作,反而会使信息保护得以增强。

(5)最小特权原则:只限于需要才给予这部分特权。

(6)分工独立性原则:控制、设计、执行和操作不应该是同一人。

(7)设置陷阱原则:在访问控制中设置一种易入的“漏洞”,以引诱某些人进行非法访问,然后将其抓获。

(8)接受能力原则:如果各种控制手段不能为用户所接受,控制则无法实现。因此,采取的控制措施应使用户能够接受。

(9)承受能力原则:应该把各种控制设计成既可适应最常见的威胁,同时也能适应那些很少遇到的威胁。可以抵御最危险的用户企图、容忍最差的用户能力以及其他可怕的用户错误。

(10)检查能力原则:要求各种控制手段产生充分的证据,以显示已完成的操作是正确无误

的。

(11)多层次防御原则:要建立多重控制的强有力系统,如信息加密、访问控制和审计跟踪等。

(12)审计原则:无论谁进入系统后,对其所作所为要负责,系统要予以详细记录。

(13)分割原则:把受保护的系统分割为不同的安全域,并分别加以保护,以增强其安全性。

(14)规范化原则:控制设计要规范化,成为"可论证的安全系统"。

(15)错误拒绝原则:当控制出错时,必须能完全地关闭系统,以防受攻击。

(16)参数化原则:控制能随着环境的改变予以调节。

(17)人为干预原则:在每个危急关头或作重大决策时,为慎重起见,必须有人为干预。

(18)隐蔽性原则:对职员和受控对象能隐蔽控制手段或记录其操作的详情。

(19)安全印象原则:在公众面前应保持一种安全、平静的形象。

1.3.3 信息系统的安全技术

信息系统的安全技术,主要包括以下几个方面:

1. 实体安全

信息系统实体安全主要是指为保证计算机设备和通信线路及设施(建筑物等)的安全,预防地震、水灾、雷击、火灾,满足设备正常运行环境的要求(如供电、机房温度和湿度、灰尘要求,电磁屏蔽要求)而采用的技术和方法;为维护系统正常运行而采用的监测、报警维护等设备和技术;为防止电磁辐射泄漏而采取的低辐射产品、屏蔽或反辐射技术和各种设备的备份等。

2. 数据安全

数据安全主要是指为保证信息系统中数据库(或数据文件)免遭破坏、修改、泄露和窃取等威胁和攻击而采用的技术方法,包括各种用户识别技术、口令验证技术、存取控制技术和数据加密技术,以及建立备份、异地存放、妥善保管等技术和方法。

3. 软件安全

软件安全主要是指为保证信息系统中的软件免遭破坏、非法拷贝、非法使用而采用的技术和方法,包括各种口令的控制与鉴别技术、软件防拷贝和防动态跟踪技术等。

4. 网络安全

网络安全是指为保证网络及其结点安全而采用的技术和方法。它主要包括报文鉴别技术;数字签名技术;访问控制技术;数据加密技术;密钥管理技术;保证线路安全、传输安全而采用的安全传输介质;网络监测、跟踪及隔离技术;路由控制和流量分析控制技术等。

5. 运行安全

运行安全包括安全运行与管理技术;系统的使用与维护技术;随机故障维修技术;软件可靠性与可维护性保证技术;操作系统的故障分析与处理技术;机房环境的监测与维护技术;设备运行状态的记录及统计分析技术等,以便及时发现运行中的异常情况,及时报警,同时提示用户采取适当措施。

6. 防病毒

计算机病毒威胁信息系统安全,已成为一个重要问题。要保证系统安全运行,除了通常安全运行与管理的技术措施之外,还要用各种病毒扫描和消除工具,定期地检测、诊断和消除系统中的病毒,并采取预防方法,防止病毒再入侵。