信息基础设施应用与管理丛书

信息安全技术与应用

中国石油化工集团公司信息系统管理部　编著

中国石化出版社
HTTP://WWW.SINOPEC-PRESS.COM

信息基础设施应用与管理丛书

信息安全技术与应用

中国石油化工集团公司信息系统管理部 编著

中国石化出版社
HTTP://WWW.SINOPEC-PRESS.COM

内 容 提 要

本书讲述了信息安全的基本知识、相关技术以及中国石化信息安全建设和应用的实践经验，旨在提升信息安全人才队伍建设，提高信息系统运维管理水平。本书共三部分十五章。第一部分介绍了信息安全基础知识、政策法规、信息安全管理体系等。第二部分介绍信息安全技术，从网络安全、系统安全、密码技术、应用与开发以及物理安全等几个方面介绍了相关技术。第三部分介绍中国石化信息安全体系建设，包括信息安全体系框架、信息安全技术应用、安全运维管理、IT 内部控制以及信息安全检查等。希望该书成为各级信息化工作者、信息安全管理人员、技术人员的工具用书。

图书在版编目(CIP)数据

信息安全技术与应用 / 中国石油化工集团公司信息系统管理部编著. —北京:中国石化出版社,2011.5
(信息基础设施应用与管理丛书)
ISBN 978-7-5114-0910-2

Ⅰ.①信… Ⅱ.①中… Ⅲ.①信息系统-安全技术
Ⅳ.①TP309

中国版本图书馆 CIP 数据核字(2011)第 083155 号

中国石化出版社出版发行
地址:北京市东城区安定门外大街 58 号
邮编:100011　电话:(010)84271850
读者服务部电话:(010)84289974
http://www.sinopec-press.com
E-mail:press@sinopec.com
河北天普润印刷厂印刷
全国各地新华书店经销
*
787×1092 毫米 16 开本 12.25 印张 295 千字
2012 年 9 月第 1 版　2012 年 9 月第 1 次印刷
定价:38.00 元

《信息基础设施应用与管理丛书》
编审委员会

《信息基础设施应用与管理丛书》具体编写人员

《信息基础设施应用与管理丛书》分为《网络技术与应用》《服务器技术与应用》《信息安全技术与应用》三个分册，各册由下列人员编写：

《网络技术与应用》：蔡荣生　孙　维　樊晓红　褚军农
黄喆磊　许扬帆　任晓辉　郭建红

《服务器技术与应用》：夏茂森　林　涛　朱　靖　徐　斌
叶传中　李中福　穆　莉

《信息安全技术与应用》：康效龙　刘　茂　郭晓东　吕燕君
赵丽华　孙　晨　郭延玲

总　序

信息化是当今世界发展的大趋势，是推动经济社会变革的重要力量。信息资源日益成为重要生产要素和社会财富；信息网络更加普及；信息安全重要性与日俱增；信息化必将重塑世界政治、经济、社会、文化和军事发展的新格局。大力推进信息化，是我国现代化建设的重要战略举措之一，是贯彻落实科学发展观、构建社会主义和谐社会和建设创新型国家的需要和必然选择。

在集团公司党组的正确领导下，中国石化围绕“建设世界一流能源化工公司”战略发展目标，坚持信息化“六统一”原则，秉承“三结合”理念，大力促进信息化与工业化的融合，信息化建设与应用取得快速发展。尤其是“十一五”期间，中国石化紧紧围绕自身发展战略和主营业务开展信息化工作，逐步使信息化成为公司发展战略的重要组成部分，在公司管理体制创新、经营模式转变等方面发挥了巨大的作用，为集团公司改革发展和建设具有较强国际竞争力的跨国能源化工公司做出了贡献。

作为中国石化信息化发展的重要组成部分，信息基础设施有效地支撑了经营管理、生产运营等业务应用系统的正常运行。为了更好地总结经验、提升运维管理水平，中国石化信息系统管理部组织有关技术人员和专家，经过多次研讨、审定，编写了《信息基础设施应用与管理丛书》，本丛书包括《网络技术与应用》《服务器技术与应用》《信息安全技术与应用》等分册。

该套丛书阐述了中国石化信息基础设施建设、运维、管理及新技术应用等情况，具有一定的前瞻性和先进性，文字叙述深入浅出，具有良好的可读性；丛书的组织和编写成系列而又不繁杂，选题既重理论更重实用，建设与应用相结合，具有较强的实用性；同时，该套丛书以中国石化信息基础设施的建设和应用为背景，在突出行业特点的同时，很好地兼顾了信息技术本身的通用性，可以说是一套具有技术性、实用性、工具性的信息技术培训教材。希望该套丛书成为信息技术各级管理人员、技术人员的工具用书。

二〇一二年七月

前　言

随着信息技术的飞速发展和广泛应用，信息技术成为人们日常生活和工作的重要组成部分，社会信息化和信息网络化，突破了信息在时间和空间上的障碍，使信息的价值不断提升。但是与此同时，计算机病毒、网页篡改、非法入侵、数据泄密、网站欺骗、拒绝服务等信息安全事件时有发生，尤其对一些大型企业来说，经过多年的信息化发展，其业务开展对信息系统的依赖性越来越强，信息安全的重要性日益显现。信息安全已成为影响国家安全、社会稳定、经济发展、公民利益的重要问题。

就中国石化信息系统而言，加油卡系统、ERP 系统、生产调度指挥系统、资金集中系统、集团门户、生产执行系统(MES)等多个信息系统承载了中国石化经营管理、生产营运的大量核心业务，保障其安全稳定运行关系到中国石化自身的经济利益。因此，中国石化在大力推进应用系统建设的同时，也非常重视信息安全建设，从信息安全体系建设、管理制度以及技术措施等方面做了大量的工作，有效地保障了中国石化信息系统的安全稳定运行。本书正是对中国石化信息安全建设和应用的阶段性总结，旨在提升信息安全人才队伍建设，提高信息系统运维管理水平。

全书分为三大部分：信息安全管理、信息安全技术、中国石化信息安全体系建设。

本书成稿阶段主要的执笔者是康效龙。参与编写的人员有刘茂、郭晓东、吕燕君、赵丽华、孙晨、郭延玲。石化盈科公司为本书的编写提供了大量的背景资料。在此，对所有为本书做出贡献和付出过辛勤劳动的同志表示衷心的感谢。

由于时间和能力有限，难以做到尽善尽美，不当之处在所难免，恳请读者批评指正。

编者

目　录

第一部分　信息安全管理

第二部分　信息安全技术

第三部分 中国石化信息安全体系建设

第一部分　信息安全管理

第1章　信息安全历史、现状与发展趋势

1.1　信息安全的发展史

“计算机安全”的概念最早提出是在1969年。当时美国兰德公司给美国国防部的报告中指出“计算机太脆弱了，有安全问题”——这是首次公开提到计算机安全。在当时和其后的相当一段时间，“计算机安全”的内涵主要是指实体安全，即物理安全。

到了七八十年代，由于各类计算机管理系统开始发展，各种应用开始增多，“计算机安全”开始逐步演化为“计算机信息系统安全”。这时，“安全”的概念已经不仅仅是实体的安全，也包括软件与信息内容等的安全。

到了80年代后期，“网络安全”和“信息安全”才开始逐步被广泛采用。近几年“安全”概念，已经不仅仅是安全防范，而是包含了安全保障的含义，即包括监控、保护、应急处理、恢复等系统性的保障。

这种概念和内涵随着历史发展继续发生变化，纵观中国计算机安全和网络安全的发展，根据法律、标准、管理、技术与市场、应用系统、人才等多个因素衡量，中国的计算机安全和网络安全的发展可以分三个阶段。

（1）宣传启蒙阶段：20世纪80年代末之前

中国计算机安全的起步相对发达国家来说是比较晚的，这与我国计算机及通信技术发展和应用有关。除了通信保密较早外，其他各个方面与发达国家相比还是有不小差距的。在七八十年代一个较长的发展阶段，中国的计算机安全整体都处于“宣传启蒙”期，各方面都比较基础，只有少数院校和研究所开展相关工作。

这个阶段的典型特征是国家尚没有相关的法律法规，没有较完整意义的专门针对计算机系统安全方面的规章，安全标准也很少，谈不上国家的统一管理，只是在物理安全及保密通信等个别环节上有些规定；企业用户基本没有意识到计算机安全的重要性，只在个别企业的少数有计算机安全意识的人们中开始在初步摸索。

在此阶段，计算机安全的主要内容就是实体安全；80年代后期开始了防计算机病毒和计算机犯罪的工作，但都没有形成规模。

（2）开始阶段：20世纪80年代末至90年代末

从80年代末以后，随着我国计算机应用的迅速发展，信息安全问题开始显现。除了此前已经出现的病毒问题，内部信息泄漏和系统宕机等成为企业不可忽视的问题。此外，90年代初，世界信息技术革命使许多国家把信息化作为国策，美国“信息高速公路”等政策也让中国意识到了信息化的重要性，在此背景下我国信息化开始进入较快发展期，中国的计算机安全事业也开始起步。

在这个阶段，计算机安全的法律法规、标准规范开始出现。1994年，公安部颁布了《中华人民共和国计算机信息系统安全保护条例》，这是我国第一个计算机安全方面的法律，较

全面地从法规角度阐述了关于计算机信息系统安全相关的概念、内涵、管理、监督、责任。与此同时，信息安全标准的制定工作也有许多进展，对产品的质量检测、销售管理、产品认证等管理制度也相继出台。但是，从整体上来讲，这个阶段国家还没有一个整体的规划来论述总的指导原则及相关实施细则和管理方法。

在这个阶段，中国计算机安全的产品、技术、市场开始明显发展，同时国外信息安全企业开始进入中国市场。我国有些企业意识到这个新兴领域广阔的前景，逐渐开始在该领域投入人力、物力。产品技术也从单一的加密、物理安全转入更宽阔的领域，如访问控制（含防火墙）、网络病毒防范，并且在入侵检测、认证识别等方面开始拥有具有自主知识产权的成果。

另一个中国安全产业起步的重要标志是，在这个时期中，许多企事业单位开始把信息安全作为系统建设中的重要内容之一，加大了投入，某些重要行业开始建立专门的信息安全部门来开展信息安全工作，如金融与税务行业——可以说，这些行业对信息安全的重视推动了整个信息安全发展。

此外，在90年代，一些学校和研究机构开始将信息安全作为大学课程和研究课题，信息安全人才的培养开始起步，这也是中国安全产业发展的重要标志。

（3）逐渐走向正轨阶段：20世纪90年代末至今

从1999年前后到现在，中国信息安全产业进入快速发展阶段，并逐步走向正轨。

标志走向正轨的最重要特征是国家出台了一系列重要政策、措施。1999年国家计算机网络与信息安全管理协调小组和2001年国务院信息化工作办公室成立专门的小组负责网络与信息安全相关事宜的协调、管理与规划，这都是国家信息安全走向正轨的重要标志。与此同时，国家在信息安全的法律、规章、原则、方针上都有对应措施，发布了一系列文件。

同时，这个阶段信息安全产业和市场开始迅速发展，增长速度明显加快。1998年中国信息安全市场销售额仅4.5亿元人民币左右，之后十年间以惊人的速度发展，至2007年，市场接近80亿人民币。其中，中国自主研发、自主生产的安全设备发展较快，品种也逐步健全。在企事业单位的应用和管理方面，除加大了投入外，用户也逐渐成熟，要求更加合理和理性。

1.2　信息安全的发展趋势

虽然经过了20多年的发展，信息安全产业仍存在不少的问题。在法律法规方面，虽然制定和发布了一系列信息安全法律、法规、标准等，但仍需要完善；从技术、市场方面看，一些核心技术及产品来自国外，自主产权的技术及产品难以满足需要；从实际应用方面看，对信息安全的认识、投入、管理及人才方面也需大力加强。

在美国总统顾问信息技术委员会（PITAC）的《网际安全——优先权危机》中，对信息安全的发展方向进行了阐述，值得我们借鉴。

（1）主要任务。构建可信系统，建立可信的网络秩序，为公众提供可信服务，从被动防御为主的安全转到主动管理为主的安全。为此，PITAC在几百个项目中遴选出十大优先发展的研究项目。

（2）主要课题。规模化认证技术是首要课题，从以脆弱性分析为主的课题转变到以真实

性判别为主的课题。PITAC 提出的目标是要解决数十亿规模的认证。

（3）主要原则。网际安全遵循的原则是“互相怀疑”；从“出于好意”的信息安全观转变到主体鉴别为主的新的网际安全观。

（4）主要应用。网际安全时代，主要应用不局限在信息系统本身，而要包括与之相连的所有空间，如通信协议（防止非法接入）、软件工程（保证计算环境的可信性）、整体解决方案、网络管理等国家重要基础设施的相关领域。

1.3　信息安全在大型企业信息化建设中的作用和意义

企业信息化建设初期，往往注重网络基础设施、应用系统等方面的建设和投入，没有注意到信息安全整体的重要性，或者难以顾及。随着信息系统的建设和广泛应用，信息系统结构和功能越来越复杂，信息化应用贯穿企业生产、管理、运营的各个环节，信息系统成为企业生存发展的重要因素。与此同时，信息安全问题凸现，倍受关注。

有关统计显示，2009 年全球 75% 的企业曾遭受网络攻击，40% 的企业表示，与自然灾害、恐怖袭击和传统犯罪相比，预防网络攻击更为重要。整体而言，大型企业信息系统的风险主要来源于四个方面：

（1）边界安全风险，主要包括黑客攻击、垃圾邮件等；

（2）内网安全风险，主要包括主机系统漏洞、服务配置不当等；

（3）应用风险，主要包括 Web 服务器、文件服务器安全风险等；

（4）管理安全风险，主要包括安全策略不完善、人员安全意识淡薄等。

企业应从战略高度重视信息安全，将信息安全建设视为企业发展的促进因素，变“被动防御”为“主动防御”，保障和促进信息化健康发展。

信息安全是一个整体的系统工程，就像一个“木桶”，整体的安全状况取决于最薄弱的一个环节，即使其它方面做得都很完善，只要留下一个漏洞，便可能被他人利用，而导致一起重要的安全事件。因此，信息安全不是简单的“技术积木”，而是技术与管理的结合体，信息安全建设应逐步由“产品孤立”向“集中管理”过渡、从“单一防御”到“整体防御”深入。

此外，信息安全状况的不断变化，决定了信息安全工作是一个循序渐进、动态管理的长期工作，信息安全体系建设不能一蹴而就，而应循序渐进、不断完善，通过定期的安全评估，注重各层次、各方面、各时期的相互协调、匹配和衔接，形成不断完善、提高信息安全水平的长效机制。

1.4　本 章 小 结

计算机安全由来已久，但是相对于计算机发展来说，却又年轻了不少，在中国尤为如此。中国信息安全九十年代才真正开始发展，面对复杂的信息安全环境，需要广大的信息安全从业人员加倍努力。本章通过对信息安全发展史的回顾，就信息安全的发展趋势、信息安全在大型企业信息化建设中的作用和意义进行了探讨。

第2章　信息安全基础

2.1　信息安全的定义

信息安全是指信息网络的硬件、软件及其系统中的数据受到保护，不因偶然的或者恶意的原因而遭到破坏、更改、泄露，系统连续、可靠、正常地运行，信息服务不中断。

信息安全是一门涉及计算机科学、网络技术、通信技术、密码技术、信息安全技术、应用数学、数论、信息论等多种学科的综合性学科。

2.2　信息安全的重要性

信息作为一种资源，它的普遍性、共享性、增值性、可处理性和多效用性，使其对于人类具有特别重要的意义。信息安全的实质就是要保护信息系统或信息网络中的信息资源免受各种类型的威胁、干扰和破坏，即保证信息的安全性。根据国际标准化组织的定义，信息安全性的含义主要是指信息的完整性、可用性、保密性和可靠性。信息安全是任何国家、政府、部门、行业都必须十分重视的问题，是一个不容忽视的国家安全战略，更是一个大型企业应该重点关注的企业安全战略。

我国的改革开放带来了各方面信息量的急剧增加，并要求大容量、高效率地传输这些信息。为了适应这一形势，通信技术发生了前所未有的爆炸性发展。目前，除有线通信外，短波、超短波、微波、卫星等无线电通信也正在越来越广泛地应用。与此同时，国外敌对势力为了窃取我国的政治、军事、经济、科学技术等方面的秘密信息，运用侦察台、侦察船、卫星等手段，形成固定与移动、远距离与近距离、空中与地面相结合的立体侦察网，截取我国通信传输中的信息。

从文献中了解一个社会的内幕，早已是司空见惯的事情。在1950年以后，从社会所属计算机中了解一个社会的内幕，正变得越来越容易。不管是机构还是个人，正把日益繁多的事情托付给计算机来完成。敏感信息正经过脆弱的通信线路在计算机系统之间传送；专用信息在计算机内存储或在计算机之间传送；电子银行业务使财务账目可通过通信线路查阅；执法部门从计算机中了解罪犯的前科；医生们用计算机管理病历，所有这一切，最重要的问题是不能在对非法(非授权)获取(访问)不加防范的条件下传输信息。

传输信息的方式很多，有企业局域网、互联网和分布式数据库；有蜂窝式无线、分组交换式无线、卫星电视会议、电子邮件及其它各种传输技术。信息在存储、处理和交换过程中，都存在泄密或被截收、窃听、窜改和伪造的可能性。不难看出，单一的保密措施已很难保证通信和信息的安全，必须综合应用各种保密措施，即通过技术的、管理的、行政的手段，实现信源、信号、信息三个环节的保护，方可达到保护信息安全的目的。

2.3　信息安全基本属性

信息安全目标就是要保证信息资源的5个基本安全属性得以实现，即机密性、完整性、可用性、抗抵赖性和可控性。通俗地说，信息安全的目标就是实现信息系统的可用、可控和可信。

2.3.1　机密性

机密性是指信息资源不泄露给非授权的用户、实体或程序，能够防止用户非授权获取信息资源。例如网络系统上传递的信息有些属于重要信息，一旦攻击者通过监听手段获取到，就有可能危及网络系统整体安全。例如：网络管理账号口令信息泄露将会导致网络设备失控。

2.3.2　完整性

完整性是指信息或系统未经授权不能进行更改的属性。例如：电子邮件信息在存储或传输过程中保持不被删除、修改、伪造、插入等。

2.3.3　可用性

可用性是指授权的用户能够按照系统所提供的途径访问相应的信息资源或服务。例如：网站服务受到拒绝服务攻击时，其可用性将降低或破坏。

2.3.4　抗抵赖性

抗抵赖性是指防止网上实体否认其已经发生的行为。这一特性保证了网上信息的来源及信息发布者的真实可信。例如：通过网络审计，可以记录访问者在网络系统中的活动。

2.3.5　可控性

可控性是指网络具有可管理性，能够根据授权对网络进行监测和控制，使得管理者有效地控制网络用户的行为和网上信息的传播。

2.4　信息安全模型

2.4.1　PDR模型

PDR是防护(Protection)、检测(Detection)和响应(Response)的缩写。三者构成了一个首尾相接的环，也即“防护——→检测——→响应——→防护”的一个循环，如图2-1所示。

图2-1　PDR模型

PDR模型建立了一个所谓的基于时间的可证明的安全模型，定义了：防护时间Pt(黑客发起攻击时，保护系统不被攻破的时间)、检测时间Dt(从发起攻击到检测到攻击的时间)和响应时间Rt(从发现攻击到作出有效响应的时间)。当Pt > Dt + Rt的时候，即认为系统是安全的，也就是说，如果在黑客攻破系统之前发现