Broadview
WWW.BROADVIEW.COM.CN

银行行为控制

——银行信息化与安全

屈延文 韩玮玺 王永红 南相浩 林 鹏 王贵驷 等著

Software Behavior

電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
http://www.phei.com.cn

银行行为控制

——银行信息化与安全

屈延文　韩玮玺　王永红
南相浩　林　鹏　王贵驷　等著

電子工業出版社
Publishing House of Electronics Industry
北京 • BEIJING

内 容 简 介

本书是《软件行为学》系列学术著作之一。本书面向银行领域的物理世界风险监管和网络虚拟世界信息化与安全的基本问题，提出了解决问题的理论、模型、方法与方案。它不仅对银行，而且对全国各行业信息化具有实际指导、借鉴和参考意义。本书最为突出的成果是：其一，建立了软件行为学提出的软件与代理组织模式与行为模式体系，实现了软件与代理行为协同、行为控制、行为监管、行为认证在信息化与安全领域中的全面应用。其二，对通信安全方面提出了具有重大改革意义的新的技术体制：公共网络与专用网络的可信接入新机制，将数据客体与伴随代理捆绑在一起，以“活性客体”传输的新型敏感信息处理技术。其三，建立了新的信息化与安全总体方法论框架，包括信息化关键技术领域的互操作性、安全应急、用户技术标准化、技术法规体系、测评认证体系、信息监管/监控体系、信息化配置管理制体系等。

本书面向金融行业的经营者、信息化工作领导与实施的决策人员，以及IT技术人员，也可作为其他各行业信息化建设的参考用书。

图书在版编目（CIP）数据

银行行为控制：银行信息化与安全 / 屈延文等著. —北京：电子工业出版社，2004.11
ISBN 7-121-00413-5

I. 银… II. 屈… III. ①信息技术－应用－银行业务－中国 ②银行业务－现代化管理：安全管理－中国 IV. F832.2-39

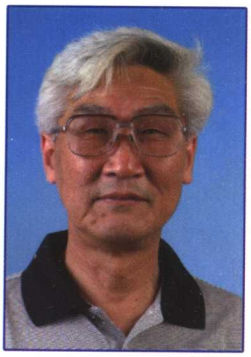
中国版本图书馆CIP数据核字（2004）第100307号

责任编辑：张 毅 zhangyi@phei.com.cn
印 刷：北京东光印刷厂
出版发行：电子工业出版社
北京市海淀区万寿路173信箱 邮编100036
经 销：各地新华书店
开 本：787×1092 1/16 印张：28.5 字数：614千字
印 次：2004年11月 第1次印刷
定 价：180.00元

凡购买电子工业出版社的图书，如有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系。联系电话：（010）68279077。质量投诉请发邮件至 zlts@phei.com.cn，盗版侵权举报请发邮件至 dbqq@phei.com.cn。

屈延文

现任信息产业部太极联合实验室主任，国家金卡工程办公室安全组组长，中国信息产业商会信息安全产业分会常务副理事长，北京大学、武汉大学、北京交通大学兼职教授及中国民生银行顾问。长期从事计算机科学、操作系统、软件工程、系统工程、系统安全和信息化总体技术的研究工作，是中国著名计算机科学学者与专家。他是《形式语义学基础与形式说明》、《实用类型程序设计》、《软件行为学》等著作的作者，是《银行行为监管》和《银行行为控制》著作的主笔，还是《银行计算机信息系统安全技术规范》的主编与执笔。他是软件行为学学科的提出者。



南相浩

现任北京大学兼职教授和中国民生银行顾问等职务，长期从事密码学、信息安全和信息安全系统研究工作，是中国著名密码学专家。他是《网络安全技术概论》著作的作者，是《银行行为监管》和《银行行为控制》著作的副主笔。他是CPK密钥管理算法的提出者。

韩玮玺

现任中国民生银行科技部总经理等职务，从事计算机系统、系统工程和金融电子化与信息化的研究工作。他是《银行行为监管》和《银行行为控制》著作的副主笔。

王永红

现任中国人民银行广州分行科技处处长、广州银行电子结算中心副理事长和广东省金融电子化学会秘书长等职务，从事计算机系统、系统工程和金融电子化与信息化的研究工作。他是《银行行为监管》和《银行行为控制》著作的副主笔。

林 鹏

现任国家计算机网络与信息安全管理中心科技委副主任和广州分中心副主任、中山大学兼职教授和国家金卡工程办公室安全组成员等职务，长期从事密码学、系统工程、信息与系统安全和金融电子化与信息化的研究工作，是中国信息安全专家。他是《银行行为监管》和《银行行为控制》著作的副主笔。

王贵驷

现任中国信息安全产品测评认证中心常务副主任和中国计算机学会常务理事等职务，从事计算机、计算机网络、系统工程、系统安全和信息化总体技术的研究工作，是中国信息安全专家。他是《银行行为监管》和《银行行为控制》著作的副主笔。

著作委员会

委员会名誉主任：	经叔平	中国民生银行董事长
委 员 会 主 任：	董文标	中国民生银行行长
委员会副主任：	洪　崎	中国民生银行副行长
	吴透红	中国民生银行财务总监
	梁玉堂	中国民生银行行长助理
指 导 委 员：	邵　平	中国民生银行行长助理
	毛晓峰	中国民生银行董事会秘书
	赵品璋	中国民生银行首席风险官
顾　　问：	孙　玉	中国民生银行顾问 中国工程院院士
	陈天晴	中国人民银行科技司副司级巡视员
	周林影	中国金融电子化公司总工程师
	吴世忠	中国信息安全产品测评认证中心主任 教授
	方滨兴	国家计算机网络与信息安全管理中心科技委主任 教授
	王志刚	电子工业出版社党委书记 前社长
主　　笔：	屈延文	中国民生银行顾问 教授
副 主 笔：	南相浩	中国民生银行顾问 教授
	韩玮玺	中国民生银行科技部总经理
	王永红	中国人民银行广州分行科技处处长
	林　鹏	国家计算机网络与信息安全管理中心科技委副主任 教授
	王贵驷	中国信息安全产品测评认证中心常务副主任

著 作 委 员 会：

董文标、洪崎、屈延文、南相浩、吴透红、梁玉堂、邵平、毛晓峰、赵品璋、韩玮玺、陈天晴、周林影、王永红、林鹏、王贵驷、戴宇星、穆新宇、贾风军、曹惠彬、吕晓强、武亦文、李宝生、李明生、刘玉林、张瑞兰、饶广军、王洁中、付敏、严立、陈子奇、李宪、邓小四、杨勇刚、严望佳、刘毅、黄奇、贺卫东、章林光、刘兵、刘爱民、董浩然等。

全面提高我国银行监管信息化和信息监管能力，为我国金融业健康发展提供一流服务。

张致祥

二〇〇〇年十一月

序

20世纪80年代以来，国际银行业金融创新风起云涌，其中信息技术已经成为推动银行业创新和发展的原动力。一方面，客户需求的个性化、多样化以及由此带来的银行服务和产品的持续创新，要求银行的业务处理系统、管理系统和监督控制系统都要实现高度的信息化。另一方面，银行的体制创新以及风险管理体系的重新塑造也有赖于先进的信息技术支撑。这就决定了银行业必须占领信息化的制高点，必须充分利用最先进的信息技术，银行业由此也成为在信息技术改造方面表现最抢眼的行业。可以这样说，现代银行业成功实现了信息技术与传统金融服务的有机结合。

中国加入世贸组织就要进一步融合到世界经济一体化之中，而经济一体化必然带来金融的一体化，中国银行业的开放已经纳入明确的日程表。外资银行挟资本雄厚、品牌悠久之势，纷纷抢摊登陆，必将给中国银行业带来冲击和挑战，也将对中国银行业的发展产生深远的促进作用。虽然外资银行在资本规模、企业文化、市场和客户定位方面有所差异，但是充分利用先进的信息技术是外资银行的相通之处。

因此，为顺应国际银行业发展潮流、迎接外资银行的挑战，中国银行必须加快信息技术的应用。先进信息技术的运用已经成为中国银行业把握历史机遇、发挥后发优势、应对严峻挑战、保持健康发展的致胜关键。

改革开放以来，中国银行业信息化经历了两个阶段：第一阶段是从20世纪80年代到90年代后期，即所谓的电子化阶段；第二阶段是从90年度后期到现在，即所谓的信息化阶段。改革开放的20年，也是我国银行业电子化、信息化从无到有、蓬勃发展的时期。当然，我们也要看到，中国银行业信息化过程中或多或少也出现过一些问题，一个小小的计算机病毒就可能导致银行电脑系统的瘫痪，一张普通的储蓄卡也会成为犯罪分子的工具，这对于中国银行业，对于银行监管当局，都是一个严峻的挑战，因此，中国银行业信息化还任重而道远。

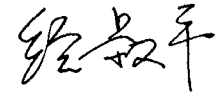
我很高兴看到屈延文、南相浩、韩玮玺等诸位所著的《银行行为监管——银行监管信息化》和《银行行为控制——银行信息化与安全》这两本非常有新意、见解独到的著作，希望能对银行信息化发挥现实的指导意义。

《银行行为监管——银行监管信息化》讨论了银行信息化过程中的风险监管这一世界性的重大课题，提出了建立银行风险监管综合认识体系的新观点。

《银行行为控制——银行信息化与安全》讨论了信息化总体和信息安全方法论的总体框架，特别是提出了信息化问题的基本理念，就是将信息化安全最终建立在行为与内容安全之上。

这两本著作从全局的、总体的高度来讨论银行信息化的问题，涵盖了金融学方法、管理学方法、计算机科学方法和系统工程方法等多个学科，集中了许多方面的重要研究成果，为中国银行信息化的监管信息化提出了许多有价值的建议。书中阐述的信息化总体设计的理论、模型、方法和方案，不仅对银行业，而且对保险、证券等其他金融行业，乃至其他产业的信息化都具有借鉴和参考的价值。

我非常愿意将这两本著作推荐给金融界和IT企业界的朋友们，希望大家开卷有益。



2004年10月12日

前　言

本书面向银行领域的物理世界风险监管和网络虚拟世界信息化与安全的基本问题，提出了解决问题的理论、模型、方法与方案。在信息化领域中，业务与服务走向代理化是信息技术发展的必然之路。信息化安全问题的基本理念最终建立在行为与内容的安全之上，这种行为不仅仅是人在网络中的访问行为，还表现在人类在网络世界中的代理行为，计算机与通信系统的软件与硬件安全最终也要拿出行为及其行为结果：内容作为网络世界中安全的证据，也就是说，信息、计算机系统和通信系统等信息技术领域的安全问题要建立在行为识别基础之上，而不能仅仅建立在模式识别基础之上。本书是一本改变信息化安全认识、理念、研究与实践基础的学术著作，提出了一系列新的理论方法、模型和方案设计。本书是《银行行为监管——银行监管信息化》一书的姊妹篇。

本书的第一个主题是银行信息化总体研究。国家或行业甚至大型企业的信息化都应当摆脱没有总体框架指导的弊端。信息化不等于建立通信系统、计算机系统，信息化本质是推动社会进步、提高生产力、促进生产关系的变革。计算机专家、通信专家和其他信息技术专家并不自然地等于信息化的专家，因为信息化逐步产生出自己固有技术领域，例如互操作性技术、信息化安全技术、用户技术标准化技术、技术法规体系、测评认证技术体系、信息化监管/监控技术体系、信息化配置管理体系等技术领域。建立这些信息化技术领域在于充分利用信息资源、全面地提高信息化的效益、扩展和规范信息化市场、保护和尊重人在信息化中的权益、促进信息产业更大的进步和最大限度地促进信息化应用。在新世纪，任何国家、行业和企业信息化都不能背离信息化发展的客观规律，必须将自己的信息化融入到全球和国家信息化的总体框架之中。研究信息化的总体方法论框架体系是推动信息化总体理论与实践的最核心的内容。

本书的第二个主题是银行信息化安全总体研究。国家网络国土安全也必须建立总体发展的框架，信息化安全总体方法学理论是信息化方法理论与实践体系中的重要组成部分，为信息化发展的总体目标服务。银行电子化、信息化和网络化的安全问题十分突出，建设任务同样十分艰巨和迫切。各行各业的信息化离不开信息化安全建设。传统信息化安全概念是指数据与系统的加密、防泄露、防篡改、防非授权破坏、防计算机病毒、防非法入侵、防攻击等。在新世纪，信息化安全不仅仅要求防护信息语法范畴数据和网络物理世界的软硬件安全，更要关注信息的语义范畴和网络虚拟世界的行为安全；信息化安全逐步走向综合治理，这种综合不仅仅实现信息安全系统之间的互动与协同，而且考虑与网络管理、系统管理、数据管理、应用管理、数字证书管理、安全管理、代理管理以及标准化控制等诸多方面融合，构成更加广义的信息技术安全体系；信息化安全在总体结构上不仅仅要求在

一个企业或一个部门中实现，而是要求在全球范围、国家范围内实现一体化体系建设。本书提出的在国家范围内建立安全保障、安全监管、安全应急和安全威慑体系，就是在这种认识上提出的安全总体框架。上述的信息技术安全体系结构虽然对于银行界仅仅是开始，但这些体系的建设直接关系到银行生存与发展的大事，意义重大。

本书的两个主题集中地表达了作者在新世纪“大范围网络环境、超海量数据与对象、高智能应用与管理”的时代特点下对信息化的态度和观点，也集中表现了作者关注行为与内容安全的新安全理念和认识。

本书提出了许多的新的概念和模式，其中最为突出的成果是：其一，实现软件行为学提出的软件与代理组织模式与行为模式体系。这个模式体系针对独立存在和伴侣存在的软件与代理，实现了软件与代理行为协同、行为控制、行为监管、行为认证、行为对抗在信息化与安全领域中的全面应用。其二，对通信安全方面提出了具有重大改革意义的新技术体制，提出了公共网络与专用网络的可信接入新机制和将发送数据客体与伴随代理捆绑在一起的“活性客体”的新型敏感信息的传输、处理技术。把这种伴随保密信息的伴侣代理形象地称为“邮差”代理或“信使”代理。在公共网络环境中，利用代理技术建立一个代理控制的、具有防护与监管功能的临时可信信道。这种邮差模式的传送、处理与存储保密信息客体伴侣代理的方法和建立临时代理控制的可信信道机制，为在公共网络环境安全通信创建了新机制和新模式，为保密通信和安全专用网络的一些基本技术体制提出了从未有过的改进，表现在通信从传输信息到传输代理。其三，建立了新的信息化总体安全方法论框架。本书研究了信息化总体技术关键的互操作性技术、信息化安全技术、用户技术标准化技术、技术法规体系、测评认证技术体系、信息化监管/监控技术体系、信息化指导和控制技术体系等理论、方法和结构；提出在国家范围内建立安全保障、安全监管、安全应急和安全威慑体系基础之上的信息化安全总体框架。其四，本书提出了完整的银行信息化总体方案指南和银行信息化安全总体方案指南。面对信息化为管理层次扁平化和时间空间汇聚与聚焦化，针对银行信息化数据与应用集中，提出了要求银行技术组织体系和业务组织体系变革的新型的集中运营管理模式，指出了在中国实现银行信息化建设的发展道路与技术路线；同时，提出了面对银行信息化，跨银行、跨企业、跨国际边界的要求。除上述显著成果之外，为信息化全面推进代理化也提供了许多可以借鉴的经验。

本书由屈延文教授总负责，确立了全书的内容结构，并且由他执笔完成了第一篇、第二篇。第三篇由屈延文、南相浩、王永红和林鹏执笔起草，孙玉院士提供了有关信息基础设施方面的建议与相关内容。附录 A 由孙玉执笔完成。附录 B 由屈延文、林鹏、王贵驷、付敏共同参与执笔并修改。通稿由屈延文、南相浩、王永红、韩玮玺、林鹏、王贵驷和严力等负责整理和修改。孙玉、南相浩、周林影、陈天晴、吴世忠、方滨兴负责对全书的审核工作。戴宇星、曹惠彬、李宝生、李明生负责本书编写过程的组织和支持工作。最后由屈延文教授负责全面定稿工作。本书得到中国民生银行的董文标行长、洪崎副行长、科技部和财务部等的大力支持。同时，还得到中国人民银行、中国银监会、中国人民银行广州

分行和中国人民银行广州分行韶关中心支行的支持与热情帮助。中国信息安全产品测评认证中心、国家计算机网络应急技术处理协调中心、中国电子科技集团五十四研究所的网络事业部、信息产业部太极联合实验室、北京江南科友科技有限公司、广东科达信息技术有限公司、北京启明星辰信息技术有限责任公司、中国人民解放军国防科技大学也为本书的编写提供了许多支持和帮助。感谢《网络安全技术与应用》杂志、《金融电子化》杂志以及电子工业出版社对于我们的帮助。在这里，我们特别感谢周仲义教授提出的宝贵意见，还要特别感谢刘玉林女士和《网络安全技术与应用》的武亦文女士在组稿和编辑工作中的努力，感谢《金融电子化》杂志常务副主编王洁中女士在本书出版与宣传方面给予的支持与帮助。

屈延文　韩玮玺　王永红　南相浩　林鹏　王贵驷

2004 年 9 月 28 日

本书概述

本书是一部面向银行乃至整个金融行业信息化建设的专著，对整个银行信息化建设具有实际指导意义，对全国各行业也具有借鉴和参考意义。期望本书能够指导银行监管信息化10年以上的时间，所以，将本书的长期概念，例如银行信息化概念、理论方法、结构概念、体系概念等作为主体写作；而短期概念，例如发展综述、技术概念、产品概念、工具概念等作为副体编写。全书从逻辑上划分为如下三篇和附录共四个部分：

第一篇分两个部分。第一部分讲述了信息化总体技术领域的互操作性技术、信息化安全技术、用户技术标准化技术、技术法规体系、测评认证技术体系、信息化监管/监控技术体系、信息化配置管理技术体系等，阐述了建立运营管理模式、系统体系结构和技术体制在总体设计中的作用。第二部分讲述了在国家范围内建立安全保障、安全监管、安全应急和安全威慑体系的安全总体框架和信息技术安全理论方法和模型。

本篇第一部分第 1 章阐述了信息化总体设计的原则，明确了信息化规划、系统工程总体和项目总体定义与区别；同时，在书中倡导成熟发展战略和公共技术。第 2 章阐述系统工程体系结构的概念，宣传采用 IEEE 610.12 成熟的体系结构概念，规范描述运营体系结构、系统体系结构和技术体系结构；提倡使用 UML 语言描述系统，并根据作者多年的研究与实践经验，提出信息化总体技术领域。第 3 章的内容是信息化总体的前导技术领域，是信息化平台建设好坏成败的关键。第 4 章中阐述了建立用户信息技术标准化体系，指出这个标准化体系区别于企业的产品与技术标准，而强调建立互操作性、安全性和服务高技术化的标准；同时也强调指出建立技术法规，维护用户技术标准体系顺利开展的重要性。第 5 章信息化测评认证与监管/监控是信息化总体的后卫技术。第 6 章信息化配置管理体系是信息化总体的引擎技术和方向控制技术，提供互操作性与安全性的标准化控制、测评认证和配置管理的网络服务。

本篇第二部分的第 7 章阐述了信息化安全问题、要求的提出方法，谈到银行信息化安全总体结构必须融入到国家基础设施安全建设的总体框架之中。银行必须推进信息化用户技术标准和行业技术法规的建立，全面开展银行信息化的测评认证和信息化安全监管工作。第 8 章深入地讨论信息安全健壮性模型、PDR 模型、多代理主动模型和生存性分析的方法体系。第 9 章讨论了银行公共渠道信息化安全总体概念，比较详细地研究了具有安全定位、防护、发现、攻击、追踪等功能的代理结构与系统，提出了专用网络的可信接入新机制和“活性客体”的新型敏感信息传输、处理技术。并认为保密通信和安全专用网络的一些基本技术体制将发生从传输信息到传输代理体制变革的。第 10 章阐述了银行维护可靠性、业务连续性和应急响应的国际通行的模型与分析方法。第 11 章比较详细地介绍了行为可信性、有效性、完整性、保密性和内容可信性等特性的监管代理系统与结构。第 12 章指出了国家

政法和军事部门参与保卫国家网络国土的必要性和重要性。

第二篇共分六章。第 13 章是银行信息化总体概述。第 14 章是银行信息化总体技术要求，提出了满足跨银行企业信息化要求，满足与国际连接的跨边界信息化特点和适应“大范围网络环境，超海量的数据与对象，高智能应用与管理”的时代要求。提出银行信息化对技术组织和业务组织体系的变革要求，指明信息化提出的管理扁平化概念为银行信息化带来的风险。第 15 章讲述了银行信息化应用系统分类与组成。第 16 章讨论了银行应用系统运营体系结构注意的问题。重点在第 17 章，详细描述了银行信息化系统总体体系结构（FII COE）、银行信息化应用平台与系统总体体系结构、银行数据共享工程总体体系结构（FII SHADE）、银行信息基础设施平台总体体系结构、银行人机界面平台与系统总体体系结构、银行信息安全、风险监管与管理平台系统的总体体系结构和银行计算网格平台与系统总体体系结构等重要体系结构概念。第 18 章最后讨论了银行信息化技术体系结构概念。

第三篇分三个部分。第一部分依照银行企业、网络服务、电子商务、银行公共渠道通信、银行领域和监管当局划分章节，共分 7 章。其中的第 19 章是信息化安全保障体系概述，包括阻止对关键基础设施信息系统的攻击、消除或减少国家基础设施针对攻击的脆弱性、面对攻击实现快速恢复，提高业务连续性水平。第 20 章是本书的重点内容之一，主要就银行应用系统安全、数据库管理系统（数据共享工程）的安全、计算环境安全、围域边界安全、信息基础设施安全和认证与密钥管理系统等进行了描述；还特别介绍了测评认证的框架。第 21 章主要对银行内部采用的代理服务提出安全要求，包括银行员工个人助理服务代理系统的安全保障，网络服务发布、发现、交互代理系统的安全保障，银行已有业务信息系统的互操作性服务代理系统的安全保障和银行信息系统测试代理系统的安全保障。第 22 章是本书另一个重点，强调电子银行与公共网络环境或大客户网络连接的安全问题。重点就银行分支行柜员系统、网络银行系统、银行卡系统、银行自助设备系统、银行呼叫中心系统、电话银行系统、手机银行系统、银行电子票据信息系统、银行认证信息系统和银行大客户渠道电子商务系统等的安全保障系统进行描述。第 23 章是本书一个创新点，介绍可信接入内部专用网络和网络传输“活性客体”新机制。第 24 章明确指出安全建设目标、银行领域的安全应急和银行领域的安全威慑的建设问题。第 25 章通过借鉴国外类似标准（例如 JTA）提出了银行信息安全技术体制的新结构。

本篇第二部分共分 4 章。第 26 章阐述可靠性与业务连续性的原因。第 27 章主要阐述了银行运营工作中心应急系统的建设。第 28 章阐述了银行灾备中心建设的要求、结构。第 29 章讨论了建立应急支援体系的重要性和建设原则与方法。

本篇第三部分共分 3 章。其中的第 30 章说明了银行（企业）的监管中心由系统管理中心、网络管理中心、安全管理中心和风险监管中心等组成。第 31 章介绍了数据与应用管理、系统管理、网络管理、安全管理和风险监管等系统。第 32 章讨论了系统管理平台、网络管理平台、安全管理平台和综合管理平台等内容。

本书还包含三个附录。附录 A 是信息基础设施总体框架；附录 B 是信息化代理科学与技术；附录 C 列举了书中的英文缩写字及其中文对照。

目　录