

银行计算机信息系统 安全技术规范

中国人民银行

中國人民銀行



電子工業出版社

Publishing House of Electronics Industry
URL: <http://www.phei.com.cn>

银行计算机信息系统 安全技术规范

中国人民银行

电子工业出版社

Publishing House of Electronics Industry

北京 · Beijing

内 容 提 要

本规范系统地阐述了信息系统的安全问题、安全概念、安全原则、安全标准、安全策略、安全结构、安全服务和系统管理等方面总体技术要求,提出金融信息系统安全是面向空间、时间、功能和人员的全方位的动态安全概念。强调金融信息系统安全是在尽可能地提高防护能力的同时,加强信息系统对自身漏洞和攻击的检测、管理、监控和处理能力,形成对信息系统安全事件的快速反应能力。本规范可以作为金融系统进行信息系统安全建设和管理的工作指南和工作手册。

图书在版编目(CIP)数据

银行计算机信息系统安全技术规范 / 屈延文编. - 北京: 电子工业出版社, 2001. 3
ISBN 7-5053-6553-3

I. 银... II. 屈... III. 银行 - 信息系统 - 安全技术 - 规范 IV. F830.49-65

中国版本图书馆CIP数据核字(2001)第10422号

书 名: 银行计算机信息系统安全技术规范

著 者: 中国人民银行

责任编辑: 徐津平

特约编辑: 陈崇连

印 刷 者: 北京天竺颖华印刷厂

出版发行: 电子工业出版社 URL: <http://www.phei.com.cn>

北京市海淀区万寿路173信箱 邮编: 100036 电话: 68279077

开 本: 787 × 1092 1/16 印张: 14.25 字数: 356千字

版 次: 2001年7月第2次印刷

书 号: ISBN 7-5053-6553-3
TP·3618

定 价: 78.00元

凡购买电子工业出版社的图书,如有缺页、倒页、脱页者,请向购买书店调换。
若书店售缺,请与本社发行部联系调换。

《银行计算机信息系统安全技术规范》

编 委 会

主 任：陈 静

副 主 任：李 龙
陈天晴

主 编：屈延文

副 主 编：周林影
李 宪

编 委：（按姓氏笔划排序）

马蔚彦	王子中	王红兵	王欣环	史奇中	阳 江
李 龙	李 宪	向蓉美	宋江秋	陈天晴	陈 静
张文军	张永福	杨兰平	周全军	周林影	范平清
郑丘海	屈延文	赵一惠	姜云兵	曹艳阳	程晓阳

审 核：（按姓氏笔划排序）

文海明	王贵驷	朱 勇	刘 信	刘爱民	刘恩煜
李世京	余林生	张如辰	张兴耆	张素伟	陈国钦
陈 捷	侯凯涛	侯靖晖	胡秀红	高 杨	顾忠勋
翁正军	黄仲孚	潘宇东			

目 录

前言	1
第1章 引言	3
第2章 范围	5
2.1 适用的系统	5
2.2 防护的对象	5
2.3 银行信息系统安全建设的国家性、行业性和企业性	6
2.4 说明	6
2.4.1 一般说明	6
2.4.2 如何阅读本规范	7
第3章 概述	9
3.1 什么是信息系统安全	9
3.2 信息安全是核心	10
3.3 信息系统安全是信息安全的保障	10
3.4 信息与信息系统安全的基本方法	10
3.4.1 安全防护的基本方法	11
3.4.2 安全检测的基本方法	11
3.4.3 安全事件反应的基本方法	12
3.5 信息系统安全要落实在信息系统建设和运营的全过程中	12
3.6 人是信息系统安全的关键要素	12
3.7 提高信息系统安全 PDR 综合能力	13
3.8 信息系统安全是基于时间的	13
3.9 银行信息系统安全建设的内容和技术要求	14
3.9.1 银行信息系统安全建设要区别新建和已建系统	14
3.9.2 银行信息系统安全建设内容和技术要求	15
3.9.3 银行信息系统安全技术的总体方案	16
3.9.4 用户安全、站点安全和平台安全	18
3.9.5 银行信息系统安全监控网络和安全监控中心	19
3.10 信息安全产品的测评和认证	19
3.10.1 国外信息产品的安全测评和认证	19
3.10.2 我国信息安全的测评和认证	23
3.10.3 信息技术安全的测评认证方法 (CEM)	26
3.10.4 安全信息系统能力成熟模型 (CMM)	26
3.10.5 信息技术安全的测评认证和 PDR 安全方案模型的关系	26

3.11	最可信赖的是信息拷贝	27
3.12	依靠法律强化信息系统安全建设	27
第4章	安全标准	29
4.1	强制标准概念	29
4.2	信息处理安全标准	29
4.2.1	计算机安全标准	29
4.2.2	操作系统服务安全标准	29
4.2.3	应用软件实体安全标准	30
4.2.4	应用平台安全标准	30
4.3	信息传输标准	32
4.3.1	终端系统安全标准	32
4.3.1.1	主机安全标准	32
4.3.1.2	安全算法	32
4.3.1.3	安全协议	32
4.3.1.4	评估准则安全性标准	33
4.3.2	网络安全标准	34
4.4	信息模型化和信息安全标准	35
4.5	人机接口安全标准	35
4.6	金融业务安全标准	36
4.6.1	银行业务报文鉴别标准	36
4.6.2	银行业务加密算法标准	36
4.6.3	个人识别号 (PIN) 标准	36
4.6.4	银行业务数字签名标准	37
4.6.5	银行业务密钥管理标准	37
4.6.6	银行信用卡业务安全标准	37
4.6.7	银行电子商务安全标准	37
4.6.8	银行网络支付安全标准	39
4.6.9	银行信息保密等级标准	39
4.6.10	银行信息完整性等级标准	40
第5章	安全策略与模型	41
5.1	信息安全环境	41
5.1.1	信息系统安全假设	41
5.1.2	信息系统安全威胁	41
5.1.3	信息系统安全策略	42
5.2	信息系统安全目标	43
5.2.1	信息系统安全的一般目标	43
5.2.2	信息系统安全目标的说明	43
5.3	信息系统的安全需求	44

5.3.1 IT环境的安全需求	44
5.3.2 安全功能需求	44
5.3.3 安全认证需求	44
5.3.4 安全需求的说明	44
5.4 计划安全系统	44
5.5 安全策略执行和人员	45
第6章 系统安全结构	47
6.1 银行信息系统安全总体结构框架	47
6.1.1 金融信息系统平台（金融信息基础设施公共操作环境 COE）体系结构	48
6.1.2 FII COE 安全服务体系结构框架	49
6.1.3 银行信息系统平台安全防护总体结构框架	50
6.1.4 银行信息系统安全检测总体结构框架	51
6.1.5 银行信息系统安全反应总体结构框架	51
6.2 通信系统安全结构	52
6.2.1 通信系统安全防护结构	52
6.2.1.1 通信系统物理安全	52
6.2.1.2 通信系统防泄露和防截获	53
6.2.1.3 通信系统加密	53
6.2.1.4 通信系统抗拒绝服务	53
6.2.2 通信系统安全检测结构	54
6.2.2.1 通信信道断路检测	54
6.2.2.2 通信连接检测	54
6.2.3 通信系统安全反应结构	54
6.3 计算机网络系统安全结构	55
6.3.1 计算机网络系统安全防护结构	55
6.3.1.1 计算机网络物理安全和加密	55
6.3.1.2 计算机网络安全路由器	56
6.3.1.3 计算机网络安全防火墙	56
6.3.1.4 计算机网络安全网关	58
6.3.1.5 计算机网络代理服务器	58
6.3.1.6 计算机网络安全（访问控制）服务器	59
6.3.1.7 服务器软件防火墙	60
6.3.1.8 在网络设备的操作系统上设置网络安全防护服务套件	60
6.3.1.9 IP的安全结构	60
6.3.2 计算机网络系统安全检测结构	60
6.3.2.1 计算机网络布线系统检测	61
6.3.2.2 TCP/IP 网络协议和网络服务已知漏洞检测	61
6.3.2.3 WEB 服务器已知漏洞检测	61
6.3.2.4 防火墙、代理服务器和访问控制服务器已知漏洞检测	62

6.3.2.5	Intranet 网络已知漏洞检测	62
6.3.2.6	网络攻击实时监控	63
6.3.2.7	网络数据流的实时监控	63
6.3.2.8	网络检测服务套件	64
6.3.3	计算机网络系统安全反应结构	64
6.4	计算机硬件系统安全结构	64
6.4.1	计算机硬件系统安全防护结构	64
6.4.2	计算机硬件系统安全检测结构	65
6.4.3	计算机硬件系统安全反应结构	65
6.5	计算机操作系统安全结构	65
6.5.1	计算机操作系统安全防护结构	65
6.5.1.1	操作系统相当于 C2 级 TCB	66
6.5.1.2	操作系统相当于 B 级 TCB	66
6.5.1.3	操作系统安全加固套件	66
6.5.2	计算机操作系统安全检测结构	67
6.5.2.1	相当于 C 级操作系统已知安全漏洞检测	67
6.5.2.2	相当于 B 级操作系统已知安全漏洞检测	67
6.5.2.3	操作系统攻击实时监控	67
6.5.3	计算机操作系统安全反应结构	68
6.6	数据库与应用系统安全结构	68
6.6.1	数据库与应用系统安全防护结构	68
6.6.1.1	相当于 C2 级数据库与应用系统安全应用开发	69
6.6.1.2	相当于 C2 级协同工作软件安全应用开发	69
6.6.1.3	相当于 B 级数据库与应用系统安全应用开发	69
6.6.1.4	相当于 B 级协同工作软件安全应用开发	69
6.6.1.5	应用软件安全防护服务套件	70
6.6.2	数据库与应用系统安全检测结构	70
6.6.2.1	相当于 C2 级数据库系统已知安全漏洞检测	70
6.6.2.2	相当于 B 级数据库系统已知安全漏洞检测	70
6.6.2.3	数据库系统攻击实时监控	70
6.6.3	数据库与应用系统安全反应结构	71
6.7	信息加密和完整性结构	71
6.7.1	加密算法	71
6.7.2	信息完整性、抗抵赖技术——数字签名	72
6.7.3	加密软件	72
6.7.4	加密设备	72
6.7.5	密钥管理	73
第 7 章	系统安全服务和过程	75
7.1	安装	75

7.2	配置管理	75
7.3	鉴别	75
7.3.1	一次性口令	75
7.3.2	Kerberos 鉴别系统	76
7.3.3	DCE 分布式计算系统	76
7.3.4	SESAME 鉴别系统	76
7.4	保密性	76
7.5	完整性	76
7.6	访问控制	77
7.7	授权和用户管理	77
7.8	审计	77
7.9	检测和监控	77
7.10	安全事件处理	77
7.11	安全备份	78
7.12	安全管理服务软件系统	78
第 8 章	系统安全事件处理	79
8.1	系统安全事件处理计划	79
8.1.1	系统安全事件处理目标	79
8.1.2	系统安全事件处理优先级	80
8.2	记录系统安全事件	80
8.3	系统安全事件核实与判断	80
8.3.1	核实系统安全事件真实性	80
8.3.2	判断系统安全事件类型和范围	81
8.3.3	判断系统安全事件危害性	82
8.4	系统安全事件现场处理方案选择	82
8.4.1	克制态度	82
8.4.2	紧急消除	82
8.4.3	紧急恢复	82
8.4.4	切换	82
8.4.5	监视	83
8.4.6	跟踪	83
8.4.7	报警	83
8.4.8	权力机关的反击	83
8.5	系统安全事件处理服务和过程	83
8.6	系统安全事件后处理	84
8.6.1	事件后消除	84
8.6.2	事件后恢复	84
8.6.3	修补和弥补系统的脆弱性	84
8.6.4	分析原因	84

8.6.5	总结教训	85
8.6.6	完善安全策略、结构、服务和过程	85
8.6.7	系统安全事件责任	85
8.6.8	系统安全事件处理通报	85
第 9 章	系统管理、安全和操作人员	87
9.1	安全员、管理人员和操作人员	87
9.1.1	系统安全员	87
9.1.2	网络安全员	87
9.1.3	系统管理员	88
9.1.4	网络管理员	88
9.1.5	操作人员	88
9.2	安全员、管理人员和操作人员的职责	88
9.2.1	信息系统安全员的职责	88
9.2.2	网络安全员的职责	88
9.2.3	系统管理员的职责	88
9.2.4	网络管理员的职责	89
9.2.5	操作人员的职责	89
9.3	安全员、管理人员和操作人员的工作内容	89
9.3.1	信息系统安全员 (ISSO) 的工作内容	89
9.3.2	网络安全员的工作内容	90
9.3.3	系统管理员的工作内容	90
9.3.4	网络管理员的工作内容	90
9.3.5	操作员的工作内容	91
附录 A	安全问题	93
A.1	信息系统安全脆弱性和可腐败性	93
A.1.1	信息系统安全脆弱性是体制性的	94
A.1.2	信息系统安全模型的不完备性	95
A.1.3	信息系统安全问题判断的复杂性	95
A.1.4	信息系统安全的防护和检测机制	96
A.2	信息系统安全威胁	96
A.2.1	非授权注册和访问	97
A.2.2	篡改或破坏信息	98
A.2.3	侵入攻击	98
A.2.4	拒绝服务攻击	98
A.2.5	信息犯罪	98
A.2.6	信息恐怖分子	99
A.2.7	信息战争	99
A.2.8	信息系统的攻击机制	99

A.2.8.1 管理类攻击机制	99
A.2.8.2 系统类攻击机制	99
A.3 生存性问题	100
A.3.1 多样性	100
A.3.2 分布性	100
A.3.3 备份性	100
A.3.4 恢复性	100
A.3.5 自主性	101
A.3.6 可控性	101
A.3.7 时代性	101
A.3.8 可用性	101
A.3.9 经济性	101
A.4 计算机安全问题	102
A.4.1 可信计算机系统	102
A.4.1.1 可信计算机硬件系统	102
A.4.1.2 可信(安全)操作系统	103
A.4.1.3 可信计算机外部设备	103
A.4.2 保密性	103
A.4.3 数据完整性	103
A.4.4 行为完整性	104
A.4.5 安全核与可信计算基	104
A.4.5.1 主体	104
A.4.5.2 客体	104
A.4.5.3 引用监控器	104
A.4.5.4 抗篡改性	105
A.4.5.5 访问控制的非旁路性	106
A.4.5.6 可测试与可分析性	107
A.4.6 自主访问控制	107
A.4.6.1 授权	108
A.4.6.2 口令	108
A.4.6.3 文件访问控制	108
A.4.6.4 访问控制表	109
A.4.6.5 用户帐号	109
A.4.7 强制访问控制	109
A.4.8 安全标识	111
A.4.8.1 安全标识的类型与完整性	112
A.4.8.2 安全级	112
A.4.8.3 安全范畴	112
A.4.8.4 完整性级别	112

A.4.8.5 完整性范畴	113
A.4.8.6 可信主体	113
A.4.9 客体重用	113
A.4.10 识别与鉴别	113
A.4.11 审计	114
A.4.12 可信通路	114
A.4.13 系统完整性	114
A.4.14 可信设施管理	115
A.4.15 可信恢复	115
A.4.16 隐蔽通道	116
A.4.16.1 隐蔽存储通道	116
A.4.16.2 隐蔽时间通道	116
A.4.17 安全测试	116
A.4.18 可信文档	117
A.4.19 系统漏洞检测	117
A.4.20 系统漏洞消除	117
A.4.21 系统攻击检测	117
A.4.22 系统攻击反应	117
A.5 计算机数据库与应用系统安全问题	117
A.5.1 可信数据库系统	118
A.5.2 数据库保密性	118
A.5.3 数据库数据的完整性	118
A.5.4 TCB 子集	118
A.5.5 TCB 子集可信依赖关系	119
A.5.6 数据库访问控制	119
A.5.7 数据库漏洞检测	120
A.5.8 数据库漏洞消除	120
A.5.9 数据库攻击检测	120
A.5.10 数据库攻击反应	120
A.6 通信与计算机网络安全问题	120
A.6.1 要求安全的业务	121
A.6.1.1 共享业务需要	121
A.6.1.2 交换业务需要	121
A.6.1.3 协同业务需要	121
A.6.1.4 控制业务网络化的需要	121
A.6.2 可信网络	122
A.6.2.1 可信网络结构	122
A.6.2.2 可信网络设备	122
A.6.2.3 安全网络协议	123

A.6.2.4 安全网络服务	123
A.6.2.5 网络安全机制	123
A.6.3 网络安全鉴别	124
A.6.4 网络信息的保密性	124
A.6.5 网络的完整性	125
A.6.6 网络的抗抵赖性	125
A.6.7 网络访问控制	125
A.6.7.1 分布网络访问控制	126
A.6.7.2 集中网络访问控制	126
A.6.8 传输安全和线路安全	127
A.6.9 路由安全	127
A.6.10 网络安全检测	128
A.6.10.1 网络系统漏洞安全检测	128
A.6.10.2 网络系统被攻击安全检测	128
A.6.11 网络安全反应	128
A.6.11.1 网络漏洞消除	128
A.6.11.2 网络被攻击反应	128
A.7 安全信息资源	128
A.7.1 信息安全机构	129
A.7.2 信息安全站点	129
A.7.3 安全反应机构	129
附录 B 基于时间的 PDR 安全模型	131
B.1 经典信息安全模型	131
B.2 过时的防护思想	132
B.3 教训	132
B.4 基于时间的 PDR 安全模型	132
B.5 系统暴露时间	134
B.6 TBS 和 I&A	135
B.7 TBS 和 DoS	136
B.8 TBS 和加密	136
B.9 TBS 和访问控制	136
B.10 时间表	136
附录 C 中国国家信息安全测评认证	139
C.1 中国国家信息安全测评认证中心简介	139
附录 D 彩虹系列	141
附录 E ITSEC 文档结构	149

附件 F	ISO/IEC 15408 IT 安全评估准则	153
F.1	安全功能类别	154
F.2	安全认证类别	161
F.3	TOE 评估认证级别类别	165
F.4	预评估类别	167
F.5	公共评估方法	167
附录 G	有关安全方面的 RFC	171
	STD 索引	195
附录 H	缩写词汇表	203

前 言

为加强银行系统计算机安全管理,防范利用计算机进行金融犯罪,防范、控制和化解现代金融风险,维护银行稳定运行,人民银行2000年1月在北京召开了全国银行系统计算机安全工作会议,对全国银行系统计算机安全工作开辟了新时代。在这次会议上颁发了《国家金融信息系统安全总体纲要》,并在全中国试行。经过一年的试行,取得了经验,并进一步对纲要进行修改和完善,改名为《银行计算机信息系统安全技术规范》,于2001年正式发行,在全国银行系统推行。

本规范系统地阐述了信息系统的安全问题、安全概念、安全原则、安全标准、安全策略、安全结构、安全服务和系统管理等方面总体技术要求,提出金融信息系统安全是面向空间、时间、功能和人员的全方位的动态安全概念。强调金融信息系统安全是在尽可能地提高防护能力的同时,加强信息系统对自身漏洞和攻击的检测、管理、监控和处理能力,形成对信息系统安全事件的快速反应能力。本规范发行目的在于规范金融信息系统安全建设,加强信息系统安全的防范意识,提高我国信息系统安全建设的水平,健全和提高金融系统的管理制度和人员素质。本规范可以作为金融系统进行信息系统安全建设和管理的工作指南和工作手册。

本规范的制定,确定了标准原则、实践性原则、全过程原则、人是信息系统安全的关键因素的原则、信息系统安全是基于时间的原则、信息产品的安全评测和认证原则和自主可控原则。并采用承认系统漏洞存在;正视信息系统安全威胁和攻击;实施尽可能的适度防护原则;加强信息系统安全检测;落实信息系统安全事件快速反应;建立打击金融信息犯罪威慑的技术方针。

本规范是由人民银行组织,商业银行、国家外汇管理局参加,由信息产业部电子15所屈延文教授起草执笔,由人民银行组织银行及社会上有关领导、专家进行评审后修改完成的。在此,对组织该规范编写工作的人民银行成都分行科技处表示感谢,对人民银行广州分行以及民生银行广州分行成功进行示范工程表示感谢,对何德全、蔡吉人、吴世忠、陈晓桦、林鹏及为编写本规范付出辛勤劳动及对本规范提出宝贵修改意见的同志表示感谢。

本规范中肯定存在缺点和不足,希望银行系统的同志们结合银行系统业务工作和安全工作的实际,提出宝贵意见。

《银行计算机信息系统安全技术规范》编委会

2001年2月

第1章 引言

银行计算机信息系统安全技术规范从以下两个方面提出了安全技术规范的总体要求：以维护国家主权，建立我国自己的信息威慑力量、对抗信息战威胁、保障国家信息安全为战略目标来制定本规范。

以保守国家金融信息秘密，保护银行资产、提供银行完整服务、维护客户利益和隐私、打击金融信息犯罪等为战术目标来制定本规范。

本规范在重视与金融信息系统生存性相关的安全问题的基础上，重点指明了如何防范金融信息系统犯罪。

本规范提出在进行信息系统安全建设时采取的总方针为：

- 1、承认存在系统漏洞
- 2、正视信息系统安全威胁和攻击
- 3、实施尽可能适度的防护原则
- 4、加强信息系统安全检测
- 5、落实信息系统安全事件快速反应
- 6、建立打击金融信息犯罪威慑

本规范参照了国际标准、国家标准和军用标准，是结合信息系统安全出现的新问题和我国金融领域的实际编制的。

银行信息系统安全建设是国家金融风险防范的重要工作，银行信息系统安全规范是银行系统进行信息系统安全建设和管理的工作指南和工作手册。