中国金融计算机
信息系统安全管理手册

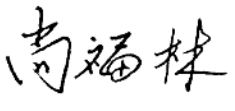
中国人民银行
支付与科技司
一九九七年二月

序　言

改革开放以来，伴随着我国国民经济的发展和金融行业体制改革的不断深入，金融电子化也取得了瞩目的进步，计算机和通信网络等先进信息技术在金融行业得到了普遍应用。目前，银行、保险等金融机构纷纷建立起各自的计算机网络处理系统，绝大多数传统业务已经实现了自动化处理，一些新型的金融服务也开始提供于社会。但是，随着金融行业计算机应用水平的提高，金融行业对计算机信息系统的依赖程度日益加深，金融行业的计算机系统安全建设就显得越来越重要。如何保证计算机信息系统的实体安全？如何保证系统的正常运行？如何防止系统及数据被非法利用或破怀，保证处理过程的完整性及处理结果的准确性？如何保证故障情况下系统不间断运行的能力？如何有效防止计算机犯罪，保证资金的安全？这些都是在金融电子化建设过程中必须认真研究并予以解决的重大问题。为此，我们在“八五”期间组织了科技攻关小组，在吸取国外发达国家或地区安全管理方面先进经验的基础上，加紧对适合我国国情的金融计算机信息系统安全管理方面的研究，取得了《金融电子化系统安全管理规范》和《金融行业计算机系统安全对策规范》两个攻关成果。这两个规范对金融计算机系统安全的系统可靠性、环境与运行安全性、信息的安全保密性以及参与系统运作的人事组织管理提出了具体的要求和约束，并根据金融部门的实际情况，在设备、技术和应用等方面，制定了具体的对策，在一定范围内规范了金融计算机信息系统的安全管理工作。在此，我对全体科技攻关人员的辛勤劳动表示感谢。

今天，我们将两个攻关成果汇编为《中国金融计算机信息系统安全管理手册》(试行)，发布至全国的地市以上的金融机构，要求各级金融机构高度重视此项工作，并以此手册为依据，积极创造条件，加强金融计算机信息系统的安全建设和管理，保证金融电子化系统的健康发展。

中国人民银行副行长



目　录

上　篇　金融电子化系统安全管理规范

下　篇　金融行业计算机系统安全对策规范

上　篇

金融电子化系统安全管理规范

第一部分 总 论

第一章 金融电子化系统及其安全管理

1.1 金融电子化系统的作用与地位

金融电子化系统是指以计算机为基础，采用现代化技术手段对金融信息进行采集、处理、存储、管理、检索和传输，并提供各类金融信息服务的系统。它支撑各类现代金融业务活动，为其进行科学化处理提供可操作的技术平台。

金融电子化系统的发展水平，是衡量一个国家现代化水平和金融现代化水平的重要标志，它在我国社会主义建设事业中占有十分重要的地位。

金融电子化系统的作用主要表现在以下几个方面：

(1) 利用计算机网络传递金融电子数据，加速资金的运转，提高资金利用率，促进国民经济的发展。

(2) 增强信息的采集、处理和综合利用能力，为科学高效地进行金融业的经营、管理、决策提供依据。

(3) 改变传统的金融作业方式，改善服务质量，方便客户，提高银行的服务水平。

(4) 为加强国际间的经济交往，促进国际金融业务活动提供有效的技术手段和条件。

1.2 金融电子化系统安全管理的对象与范围

金融机构按行业可分为银行、证券、保险、信托等。金融电子化系统由这些金融机构的各种业务处理系统、管理信息系统和决策支持系统所组成。

金融电子化系统安全管理的对象主要包括以下四类：

(1) 实现、运行、维护金融电子化系统的相关人员；

(2) 金融电子化系统内的电子数据及其存储媒体；

(3) 构成金融电子化系统的相关设备、设施及通信线路；

(4) 金融电子化系统的实现方法和相关技术。

上述安全管理对象所构成的集合，形成了金融电子化系统的安全管理范围，它是本规范安全管理的作用域。

1.3 金融电子化系统安全管理的特点

金融电子化系统的安全管理是金融电子化系统建设的重要组成部分，也是系统正常运行

的必要条件和保障。金融电子化系统具有以下特点：

(1) 复杂性

金融电子化系统是一项技术密集、资金密集、大型复杂的人机系统，它面向社会，涉及资金的流动，始终是金融行业内外不法分子攻击的目标。

(2) 保密性

金融是国民经济的命脉，金融电子化系统排斥来自任何原因和任何可能存在的不保密隐患，不给恶意、非法的活动提供可乘之机。

(3) 安全性

金融电子化系统的安全不但涉及国家和金融业的利益，而且还涉及到广大客户的利益。任何不安全因素都可能会造成信息的丢失、资金财产的损失和金融市场的混乱。

(4) 风险性

金融业务是高度风险业务。金融业务由手工处理逐步转为电子化系统处理以后，银行、证券、保险等行业中新型业务的自助服务方式有了很大的增加，接触金融业务系统的人员从银行内部扩大到了社会各界，给金融业务的经营管理带来了新风险和新问题。计算机系统固有的脆弱性又加大了金融业务的风险性。

(5) 实时性

金融电子化系统所处理的信息瞬息万变，要求所有采集、处理的数据必须做到准确、及时、完整、相互关系完全匹配。因此需要速度快，实时性强。

1.4 安全与保密的基本原则

有效地保护计算机信息系统的安全，需要科研、产业、应用、管理等部门的共同努力，需要在立法、行政、技术等方面采取综合的措施。根据目前我国金融业的实际情况，金融电子化系统的安全与保密的基本原则为以下几点：

(1) 安全服从于国家利益

任何部门或机构在实施安全管理时都应当遵循国家有关法规规定，在确保国家利益的前提下保护好本单位的利益，并接受国家相关部门的指导、监督和检查。

(2) 独立自主

在金融电子化系统中，凡涉及安全保密的重要环节，无论在设计、实现、运行、维护和系统配置上，所用技术应立足于国内，不得直接引用未经任何消化改造的境外安全保密技术和设备。

(3) 选用成熟技术

金融电子化系统的各主要组成部分应有完备的安全与保密措施，应尽量采用成熟的新技术。

(4) 注重实效

实施金融电子化系统安全与保密管理应量力而行，不应盲目追求一时难以实现或投资过大的目标。应使投入与所需求的安全功能相适应。

第二章　安全等级及安全管理的重要环节

2.1　安全等级划分方法

为了使金融电子化系统的硬件、软件、信息受到保护，免于因自然的或人为的原因而遭到破坏、更改和泄露，保证系统能连续正常运行，承受合理风险，管理规范应对金融电子化系统进行安全等级的划分。

金融电子化系统安全主要由人员安全、环境安全、运行安全、实体安全和信息安全几个主要方面组成。金融电子化系统安全的主要内容包括系统的保密性和系统的可靠性。保密性是指系统所处理信息涉及到国家秘密和金融行业的商业秘密的程度，可靠性是指系统运行中如果出现毁坏、故障、事故、差错对金融业务正常运作所带来影响的程度。金融电子化系统安全管理是在综合保密性和可靠性的基础上，按照系统所处理信息的重要性来统一进行安全等级划分的。

遵照《中华人民共和国计算机信息系统安全保护条例》，结合我国金融行业的特点，金融电子化系统安全等级共分为五级，级别要求和作用强度的排列顺序是从一级（最高级）到五级（最低级）。

2.2　系统安全等级划分

（1）系统安全一级

存储、处理和传输绝密信息的金融电子化系统。该系统中的信息一旦泄露或损坏，会给国家安全和利益带来特别严重的损害，对金融业造成巨大经济损失。因此，系统应能够确保连续可用，不因局部的毁坏、故障、事故、差错造成系统效率的降低。

（2）系统安全二级

存储、处理和传输机密信息的金融电子化系统。该系统中的信息一旦泄露或损坏，会给国家安全和利益带来严重的损害，对金融业造成很大的经济损失。因此，系统应能连续可用，局部的毁坏、故障、事故、差错虽然可能影响了系统的效率，但仍能正确运行。

（3）系统安全三级

存储、处理和传输秘密信息的金融电子化系统。该系统中的信息一旦泄露或损坏，会使国家安全和利益遭受损害，对金融业造成一定的经济损失。因此，要求系统在局部出现毁坏、故障、事故、差错时，能够在最短时间内得到排除、纠正和恢复；在系统排除、纠正和恢复过程中，应有某种替代措施维持业务工作的进行。

（4）系统安全四级

存储、处理和传输不属国家密级，但属于金融业内部掌握、具有敏感性信息的金融电子

化系统。该系统中的信息一旦泄露或损坏，会使银行、证券交易商、保险公司及其客户陷入困境，甚至造成损失，使其社会声誉受到损害。因此，系统应具有对局部毁坏、故障、事故、差错在短时间内得到排除、纠正和恢复的能力。

(5) 系统安全五级

存储、处理和传输不属于以上保护级别信息的金融电子化系统。该系统的毁坏、故障、事故、差错可能会造成某些金融业务的停顿，影响某些金融业务的效率，但经济损失不大。

2.3 安全管理的几个重要环节

金融电子化系统安全管理的几个重要环节是：

(1) 规范

金融电子化系统的设计、实现、运行应在本规范指导下进行，不得盲目开发、自由设计、无章操作。

(2) 预防

按照 2.2 的条款，系统应具备保障安全性所需要的相关功能，在系统的规划、设计、选购、集成、安装中应该同步考虑系统的安全策略和选定的安全等级。

(3) 安全机制

确保具有安全等级的运行系统具备与该系统相应的安全机制，并且能够正常工作。

(4) 检查

定期检查维护系统，尽可能采用远程或联机诊断技术。

(5) 应急

系统应具有安全恢复机制和应急措施。

(6) 监督核查

在制定管理制度中，要明确按时间或按业务处理周期定期进行有关环节及内容的稽核，并要制度化、责任化。

2.4 安全管理的基本要求

金融电子化系统安全管理基本要求是：

(1) 系统必须安全运行

不允许无安全保证的系统投产运行。

(2) 系统必须高度保密

确保存储在系统中和在网络上传输的电子信息安全。

(3) 系统必须具有数据完整性保护的措施和能力

不允许没有相应保护措施和能力的系统投产。

(4) 系统必须有独立的严密的安全管理控制机制

要求有针对性地使用密码技术、鉴别技术、访问控制技术、信息流控制技术、审计控制技术、数据保护技术、软件保护技术、信息泄漏防护技术等，建立独立的、严密的安全管理控制机制。

(5) 系统信息交换应具有有效性和合法性

信息的有效性是金融电子化系统应用的前提，重要信息交换的有效性、合法性需要国家法律意义上的确认。特别是在出现争议时，在法律意义上能够做出公证或仲裁。目前，金融电子化系统应当力求为今后立法执法提供电子信息凭据。

(6) 针对系统的安全管理

对不同业务处理系统要按照有限授权原则、全面确认原则、安全跟踪原则，实施相应的安全管理。

对同城或异地清算系统、电子联行、电子汇兑系统要增强访问控制技术和密押控制手段，增强客户身份识别技术和管理手段，完善核算手续和制度。

对国际清算系统要加强标准化管理，按国际标准与惯例与国际接轨，要增强密押控制与授权人签字管理技术手段。

与境内侨资、外资金融机构或境外金融机构联网通信需经国家安全权力机关审查批准，并经过规定的接口界面实现通信，不允许直接连接。

对金融外汇业务，要在外汇统计业务、外汇管理业务、外汇市场业务的主要处理环节上强化系统安全管理。

对于证券业务，要在保证“公开、公平、公正”的原则下，确保交易的正常进行。

第三章　本规范使用的术语

本规范使用的术语主要引自《金融电子化系统标准化总体规范》，本规范根据需要仅作了少量的补充。

1. **规范**：对设计、施工、制造、检验等技术事项所作的一系列统一规定。属于标准的范畴。

2. **环境安全**：机房、场地的防火、防水、防震、防雷击、防电磁干扰与电磁泄漏以及防盗与防其他人为破坏。

3. **运行安全**：保证系统能连续、正常地运行。

4. **实体安全**：保护计算机和存储媒体的安全。

5. **软件安全**：保护软件不被篡改、非法复制及失效。

6. **信息安全**：保障信息的保密性、完整性、可用性、可控性，保证信息在采集、存储、处理、传输的过程中不被泄漏、修改、失控，数据不被非法使用、修改、复制。

7. **金融报文**：包含金融信息的一次通信。

8. **明文**：未经加密的信息。

9. **加密**：数据通过密码转换生成密码文本的过程。

10. **密文**：已加密的信息。

11. **解密**：一个可逆加密过程的逆过程。

12. **密码算法**：用于加密或解密的、具有抗攻击能力的一组变换函数构成的运算规则。

13. **密码体制**：用特定的密码算法和密钥管理方法构成的密码规则。

14. **密码设备**：具有完成密码功能（加密、解密、数字签名、鉴别、认证、密钥管理）的装置。

15. **密码装置**：执行密码功能（加密、解密、数字签名、鉴别、认证、密钥管理）的设备。

16. **密码编码**：为了隐藏信息内容，防止信息被篡改和非授权使用而对信息进行变换的原则、途径和方法。

17. **密码分析**：在对原始加密算法和使用密钥的信息掌握不足的情况下试图将密文变换成明文的方法和步骤。

18. **抗攻击能力**：对抗密码分析的能力。

19. **密钥**：一个用于控制密码算法的具有变化量的、在保密条件下外人难以预测的参数。

20. **密钥管理**：在应用密码保障信息安全时，对所用密钥生命周期的全过程（产生、存储、分配、使用、废除、归档、销毁）实施的安全保密管理。

21. **文件加密**：将存储在媒体的文本文件进行加密的操作。

22. 数据加密：将存储在媒体的数据进行加密的操作。

23. 通信加密：在通信过程中，对传输报文实施的加密保护。

24. 对称算法：对于加密、解密及认证、校验双方，采用同样密钥的密码算法。

25. 非对称算法：完成加密和解密使用一对密钥，构成非对称密钥集的密码算法。

26. 序列密码：在密钥和密码算法的工作中产生密码序列流，对明文序列采用逐位变换方式（通常运用模二加方法）完成密码变换的密码体制。

27. 分组密码：把明文分成固定长度的二进制数据组，在密钥控制下经过多次迭代逐组进行密码变换的密码体制。

28. 公开密钥密码：密钥的拥有者把密钥分成两个，一个作为加密密钥，一个作为解密密钥，其中一个公开，供要进行密码通信者使用，一个由拥有者保密使用，完成密码变换的密码体制。其密码变换方式也是用分组方式进行。

29. 认证：报文发送双方用于确保数据完整和提供数据来源确认的过程。

30. 数字签名：对报文的部分或全部内容及来源进行确认的数值，一般用非对称密码算法产生和校验数字签名，在某些领域，它也可提供认证服务。

31. 报文验证码：报文发送与接收双方用于确认报文来源和部分或全部报文内容的一种编码，该编码是双方商定的计算的结果。

32. 确认：检验一个报文全部或部分数据完整性的过程。

33. 安全审计：系统记录并激活为测试系统控制充分性的一个独立的检查和测试，用以确保与建立的策略和操作规程的一致性，并据以指出控制、策略和规程中的任何变化。

34. 口令（通行字）：用于鉴别一个用户、一个特定信息或存取方式的一个字或一串符号。

35. 物理安全：为保证信息安全和系统安全可靠运行而对设备、设施、环境、人员等采取的安全措施。

36. 软件：与计算机系统的操作有关的计算机程序、过程、规则以及有关的文件及数据。

37. 文档：与程序开发、维护和使用有关的说明资料，它是软件的重要组成部分。

38. 测试：由人工或自动方法来执行或评价系统或系统组成成分的过程，以验证它是否满足规定的需求、或者识别出期望的结果和真正结果之间有无差别。

39. 系统测试：测试整个硬件和软件系统的过程。以验证系统是否满足规定的需求。

40. 系统确认：在软件开发过程结束时对软件进行评价，以确认它和软件需求是否相一致的过程。

41. 系统验证：确定软件开发周期中的一个给定阶段的产品是否达到前阶段期间确立的需求过程。

42. 验收测试：确定一系统是否符合其验收准则，使客户能确定是否验收新系统的正式测试。

43. 数据库：按照一定的数据结构，在计算机存储设备中存放的相互具有关联的数据集，某一数据集的部分或全体，它至少包括足够为一给定目的或组定数据处理系统使用的一个文卷。

44. 计算机通信网：以共享资源为目的，通过数据通信线路将多台计算机互连而成的系统。资源共享包括共享网络中的计算机硬件、软件和数据。多台计算机通常在地理上是广为分布的，或者分布在一个城市范围，或者分布在更局部的范围（例如一群建筑物范围内），相应地将计算机通信网分为广域网（WAN）、城域网（MAN）和局域网（LAN）。

45. 信道：系统中一条数据的通路。

46. 接口：两个不同系统的交接部分。例如，两种硬设备之间的接口装置，两个程序块的接口程序，OSI 参考模式两个相邻功能层之间的接口等。

47. 计算机违法犯罪：因恶意原因而引起电子化系统的硬件、软件、数据遭受破坏、更改、显露或系统不能连续正常运行的行为。违法犯罪类别：

(1) 为获利修改数据文件；

(2) 为获利修改程序文件；

(3) 偷窃硬件或信息；

(4) 越权非法进行存取；

(5) 破坏数据或程序文件；

(6) 破坏硬件；

(7) 泄露信息；

(8) 制造或者有意扩散计算机病毒。

48. 故障：因可靠性而引起的电子化系统的硬件、软件、数据遭到破坏、更改、显露或系统不能连续正常运行的事件。故障类别：

(1) CPU 故障；

(2) 输入输出设备故障；

(3) 电源及空调故障。

49. 事故：因工作人员失误或能力所不及而引起电子化系统的硬件、软件、数据遭受破坏、更改、显露或系统不能连续正常运行的事件。事故的原因主要有以下几类：

(1) 缺少技术骨干；

(2) 编程错误；

(3) 输入错误；

(4) 操作错误；

(5) 理解错误；

(6) 数据无意清除；

（7）组织管理机构不健全；

（8）无意向外泄露信息；

（9）管理不善引起火灾。

50. 天灾：因不可避免的自然灾害引起电子化系统的硬件、软件、数据遭受破坏、更改、显露或系统不能连续正常运行的事件。天灾类别：

（1）地震；

（2）洪水；

（3）山体滑坡；

（4）雷击；

（5）四邻发生火灾或爆炸。

51. 安全监察：各级金融机构的公安（保卫）处（科），按照本规范内容对本单位的电子化系统实施检查和督促，及时发现问题，分清性质，严厉打击各种犯罪活动，提出改进措施，提高电子化系统安全性的一系列活动。

52. 个人识别号（PIN）：PIN 是 Personal Identification Number 的缩写，是一个用于鉴别电子支付系统中各种银行卡持有者身份的秘密代码。

53. 磁条卡：磁介质金融交易卡。它有不安全因素，主要是卡片可能被盗，卡片信息可能被复制，输入非保密终端的信息可能被窃收，卡片信息或 PIN 信息可能被窃取。

54. 智能卡：将一个微处理器嵌在一张塑料卡片上，使识别或鉴别运算直接在卡片上进行。客户的主要帐户信息可存储在卡片中，用作储蓄卡时其作用与银行存折相同。

55. 信用卡：是银行或一些公司签发给那些资信状况良好人士的一种特殊信用凭证。持卡人可凭卡在指定场所进行非现金交易的消费结算活动。也可以在发卡机构所属代办网点提取现金或转帐结算。我国的信用卡是先存款后消费，并允许在一定程度上善意透支。

56. 储蓄卡：是一种能提供存、取款功能的银行交易卡。它与信用卡不同，不允许透支。

57. 稽核：监督的一种形式。它是金融机构内部设立的专门机构或聘请第三者对所属单位和本身的经济活动的真实性、合法性和准确性用专门的方法进行监督检查的行为。它包括监督检查、揭露问题、评价金融机构经营状况、对存在问题提出建议或处理意见、书写稽核报告等过程。

58. 可靠性：在规定的时间内和指定的条件下，系统完成其应有功能的能力。