银行计算机安全体系研究

中国人民银行
支付与科技司
一九九六年八月

国家“八五”重点科技攻关项目

内部资料
注意保存

银行计算机安全体系研究

曹谷崖　曲成义　刘玉宏　耿　慧
戴　珊　韩国强　张　宏　强群力

前　言

当今世界，以计算机、通信技术为基础的金融电子化系统迅速发展，引起了金融行业的一场革命，促进了金融行业的现代化建设，对提高金融业务的工作效率和准确性、提高信息管理水平和增强科学管理决策能力等起了极为重要的作用。

随着金融电子化建设的深入发展，金融业务处理和科学管理决策对计算机的依附程度越来越大，而与人工处理数据相比，电子数据处理具有更大的风险性，这是由于其数据以及数据处理过程是“不可见”的，数据处理量大，速度快，又由于计算机本身固有的脆弱性，因此容易受到外部环境和人为的有意或无意的危害和攻击。

事实上，金融电子化正面临着严峻的安全挑战：一方面银行计算机系统需要安全、可靠，可抗击各种自然灾害，防范各种故障，抵御各种计算机病毒，避免任何事故给银行的计算机信息系统造成影响、损失；另一方面则面临“计算机犯罪”的严峻威胁。

计算机犯罪属于一种高技术犯罪，由于它的隐蔽性、高获利性和低破案率，直接刺激了它在金融界中的增长。美国金融界每年由于计算机犯罪引起的经济损失近百亿美元。此外，还有人为的破坏和自然灾害；如纽约世界贸易中心的大爆炸和日本的神户大地震都是导致银行计算机系统遭受很大的破坏的原因。我国银行界在电子化建设过程中，采取了不少安全管理和安全技术等措施，收到了不小的成效，但是随着金融电子化建设的迅速发展，我国银行计算机应用逐渐暴露出许多危险的隐患，其安全开始面临更大的风险和挑战，计算机犯罪已明显呈上升的趋势。

为了提高银行电子化系统的安全性和可靠性，保障银行各项业务的有效运行，确保国家、银行和客户的利益免受损失，从安全体系的高度全面研究和布署银行计算机安全和保密工作是非常重要的，它是关系到银行电子化建设健康发展的大事。特别是随着银行计算机网络的不断扩大，银行新兴电子化业务不断扩展，电子资金的流量猛增，这项工作更显得特别重要并具有战略意义。

本研究报告首先对国际计算机安全领域中的计算机犯罪、计算机安全对策、计算机安全标准、计算机安全机制和计算机安全系统进行了研究和评述，以便我们借鉴，使我们的研究工作立足于较高的起点之上；接着对我国银行界的安全现状进行了调查分析，本研究报告采

用了报表统计分析法、现场考察调研法、专家座谈调查法、德尔菲专家评测法等科学的调查方法，对银行电子化安全状况进行了大量的抽样调查，在定量与定性的基础上，获取了大量有价值的科学数据和结论。研究报告最后运用综合集成的系统工程方法对国际计算机发展动向、国内银行计算机安全现状和我国银行计算机发展中的安全需求进行了认真的研究分析，形成了银行计算机安全体系框架，就安全策略、安全管理、安全立法、安全标准、安全机制、安全服务和计算机稽核等七个方面提出了体系结构表，以利于指导银行计算机的安全立项研究、安全规划制定、安全系统的研制、安全管理模式的完善、安全运营机制的改进等。在该研究报告的基础上又提出了对当前“我国银行计算机安全工作的整体规范建议”。

本课题是针对“八五”国家重点科技攻关项目《银行计算机安全保密体系》而开展的，是中国农业银行信息电脑部牵头，由中国农业银行、航天工业总公司710所、中国人民银行、中国工商银行和中国银行等部门共同研究完成的。在研究中得到了金融界和我国计算机安全领域内的大量专家、学者的支持和帮助。

周林影、陈逢吉、陈天晴、杨应辉、仲安妮、王云生、缪道期、吴亚非、赵战生、周禹相、孙康成、邓其沛、张炳成、蒋笑凡、刘云川、杨光、余秀清等同志为本研究报告提供了珍贵的材料和见解。在此，对上述同志表示衷心的感谢。

该研究报告经陈静、杨智慧、周林影、陈天晴、赵战生、张一平、吴维霞、卢小冰、张居兴等诸位专家进行了认真地审查，对他们的宝贵意见再次表示感谢。

该项研究只是一个起步，目的在于推动银行电子化安全工作，以促进我国银行电子化工程更健康和迅速地发展。

目　录

第一章　国际计算机安全概况与探讨

1、各国在计算机安全方面的对策

1.1　广泛开展计算机安全教育

国际信息处理联合会（IFIP）组织的计算机安全年会近两年（SEC、93 及 SEC、94）都在会议上倡导要加强计算机安全教育，阐述这一问题的重要性。

最近，美国成立了“国际强化安全研究所（WISE）”。该研究所的目的在于为工业和政府机构在各种各样的法规方面提供训练和咨询，虽然它关注各个方面的安全，而不仅仅是针对计算机安全问题，但它的成立及其开展的工作，对计算机安全教育是一个良好的促进。

该研究所涉及的领域包括安全、保密、调查和防止损失，它主要提供专业训练、研究和开发，提出安全、保密方面的问题并作为“思想库”提供服务。它还在格林斯博罗校园首开课程，并有计划深入到公司或政府机构中去。所开的课程包括：保护计算机和专有数据、保护文件和专有信息、安全管理等。

1.2　计算机安全法规的制定

当今社会计算机犯罪活动之所以猖獗，其中一个主要原因在于各国的计算机安全立法不健全，尤其没有制定相应的刑法，因此使犯罪活动屡禁不止。正是认识到了这一点，各国政府近几年来纷纷制定计算机安全方面的法律、法规，尤其是意大利，将计算机犯罪与刑法联系起来修改了有关条款，对犯罪者真正做到绳之以法。美国则将此项工作渗透到修改其行政法、刑法、民法及诉讼法等工作中去。我国的第一部计算机安全法规《中华人民共和国计算机信息系统安全保护条例》也是出于同样目的诞生的。如：

（1）美国的《信息自由法》
（2）英国的《数据保护法》
（3）美国和加拿大的《个人隐私法》
（4）经济合作发展组织各成员国政府联合通过的《过境数据流宣言》
（5）美国的《反腐败行径法》
（6）美国的《伪造访问设备和计算机欺骗与滥用法》
（7）美国的《电子通信稳私法》
（8）美国的《计算机欺骗和滥用法》
（9）美国的《计算机安全法》
（10）英国的《计算机滥用法案》
（11）《中华人民共和国信息系统安全保护条例》

一九九四年二月十八日国务院总理李鹏同志签署了147号国务院令，发布《中华人民共和国计算机信息系统安全保护条例》并立即执行。该条例主要有以下六个管理制度：

①安全等级保护制度

②国际联网备案制度

③信息媒体进出境申报制度

④案件强制报告制度

⑤计算机病毒归口管理制度

⑥专用产品销售许可证制度

(12)《中华人民共和国计算机信息网络国际联网管理暂行规定》

为了加强对计算机信息网络国际联网的管理，保障国际计算机信息交流的健康发展，我国制定了本规定。该规定明确要求凡是中华人民共和国境内的计算机信息网络要进行国际联网，均需按此规定办理执行。

另外，我国正在酝酿讨论中的还有一系列有关计算机安全方面的法规，如《计算机信息系统管理规定》、《计算机病毒控制条例》、《计算机信息系统安全检查办法》、《计算机安全技术产品鉴别办法》、《计算机信息系统安全申报注册管理办法》等。

针对银行领域，也有相应考虑与研究，如新出台的《票据法》及正在讨论中的《信用卡法》及《银行卡法》等。

1.3 国外金融计算机安全防范措施

计算机技术在金融领域中的广泛应用，给计算机技术的发展带来了严峻的考验——计算机系统的安全性。为此，计算机系统的安全与否，是其能否在金融领域中生存下去的关键问题。因而，日本针对此问题在金融计算机安全方面制定出了一套严格、全面、具体的安全规范。

1.3.1 设备规范

本规范制定了计算中心及营业网点的建筑和各类设备对自然灾害、非法破坏和设备故障等方面的预防及应急对策方法，确保其可靠安全。

在计算中心方面，制定了计算机机房、数据保管室、电源室、空调室、有关通信设备的安全对策。

对于营业点则由建筑内主要的营业厅、放置CD、ATM的终端室、电源设备、空调设备、有关通信设备的安全对策组成。同时对于设置在企业或穿墙式CD、ATM，可酌情选择相应的对策标准。

对于各类计算中心、营业点，由于地理环境、建筑、设备各异，在实施本标准确有困难时，可以选择变更实施对象的措施。

1.3.2 技术规范

考虑到技术将进一步发展，本技术规范仅对主要功能制定了对策方法。在实施本方法时，则要有实现其功能必须的软、硬件以及适当的运用。

为提高计算机系统的可靠性、安全性，本技术规范针对其构成要素（软件和硬件）制定了系统可靠性和安全性对策规范。

提高系统可靠性，即为减少计算机系统故障，则能快速恢复，减少损失。其对策方法有

以下几个方面：

- 硬件可靠性对策，由预防维修、硬件备份构成；
- 软件安全对策，由保证开发质量、正确维护构成；
- 运行可靠性，由操作简单、自动化操作、检查功能、负载监视功能构成；
- 故障的早期发现、快速恢复，由故障检出、分离、局部化、恢复功能组成。

对于安全防范对策，由数据保护对策和防止非法使用对策组成。数据保护对策，由防止泄密、破坏修改、检出构成。防止非法使用对策，由存取权限及防止非法使用监测等方面内容构成。防止非法程序对策由防御和监测对策构成。

1.3.3 应用规范

本应用规范归纳制定了计算中心和营业网点计算机应用的组织结构、管理体制，审批制度等重要方面。

有关计算中心，制定了设置防灾及防范业务组织、制定规章制度、出入管理、计算机系统有关设备的应用管理、系统开发、变更的确认制度、各种设备管理、应用培训、人事管理、检查等条例。

对于营业网点，也制定了设置防灾、防范业务组织、规章制度应用管理、各类设备管理、应用教育、培训、管理及检查等。

1.4 我国的一些计算机安全防范措施

在我国，随着计算机技术的发展与应用，为了保障计算机系统的安全可靠性，也相应地制定了一些安全规范作为国家标准推广，为计算机安全起着引导和保证的作用。如：

(1)《计算机场地技术条件》 GB2887－89

(2)《计算机场地安全要求》 GB9361--88

(3)《计算机机房用活动地板技术条件》 GB6650－86

(4)《电子设备雷击保护导则》 GB7450－87

(5)《信息技术设备的无线电干扰》 GB9254－88

除此以外，还有一些其他与计算机及其安全有关的国标和军标，均对提高计算机系统的安全可靠性有着很重要的指导作用。

2、世界性的计算机犯罪

2.1 概况

计算机犯罪是一种利用计算机知识和技能进行的对计算机系统及其信息的破坏活动。随着科学技术的发展及人们知识水平的提高，犯罪手段日趋隐蔽和多样，诸如逻辑炸弹、特洛依木马、意大利香肠术等黑客行动，计算机病毒也日益演化成了一种计算机犯罪的常用手段。

在一些计算机技术发达的国家里，利用计算机进行犯罪活动，早在本世纪六十年代末就已出现，在七十年代发案率逐渐上升，到八十年代已是发达国家日益严重的社会问题。进入九十年代以来，世界各国的计算机安全专家和学者逐渐重视并投入相当精力研究这个问题，并且提出了一系列的法规、标准、技术方案及安全模型等，成立了相应组织对犯罪及安全问题进行系统全面的分析与研究。“美国国家计算机安全协会”就是在 Davic Den 博士倡导下成立

的专门从事这方面研究工作的社会组织，尤其对计算机病毒进行了世界性的系统研究。另外，各种国际标准化组织也纷纷颁布或完善有关标准，力争抵御计算机犯罪对计算机系统的破坏，最大限度地降低计算机犯罪造成的不良影响。

计算机犯罪案件的频频发生，严重威胁着利用计算机系统处理敏感数据的部门的利益和安全，甚至产生不可弥补的损失，同时也会给社会造成严重危害。几年前震惊世界的“莫里斯”案件及其后果，相信人们尚记忆犹新，近几年来，计算机系统在金融领域得到广泛使用，政府部门又没有相应强有力的法律法规出台，从而使计算机犯罪活动日益猖獗、经济损失日趋严重，因此我们要研究计算机安全技术必须从分析计算机犯罪着手。

2.2 计算机犯罪的一般描述

2.2.1 计算机犯罪的定义

计算机犯罪不同于传统的犯罪活动，它是一种高技术的犯罪，它侵入的对象也通常是国家要害部门、军事系统和金融领域等，因此它比传统的犯罪更具有威胁性。随着计算机犯罪案件的不断出现，计算机犯罪已成为一种概念，并逐渐形成一门学科。

欧洲经济合作与发展组织认为“在自动数据处理过程中，任何非法的、违反职业道德的未经批准的行为，都是计算机犯罪行为”。

相对准确的是德国人提出的一种观点，认为“计算机犯罪是指针对计算机或把计算机作为工具的任何犯罪行为”。

基于这一观点，我国有关部门也提出自己的定义，即：以计算机为工具或以计算机资源为对象实施的犯罪行为。

无论采用哪一种定义，计算机犯罪是客观存在的，是利用计算机技术和知识等对计算机系统进行的破坏活动，而且正日益威胁着信息系统和社会的安危。

2.2.2 计算机犯罪的特征

计算机犯罪与常规犯罪行为有很大区别。计算机犯罪是一种高技术的犯罪活动，是瞬间可以发生的事件，而且犯罪现场很少留下任何痕迹。由于计算机网络系统的广泛应用，计算机犯罪已成为可以跨越国界的犯罪活动。

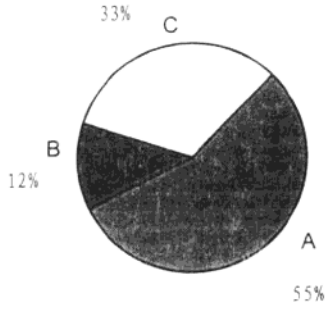
从计算机犯罪行为本身看，计算机犯罪的特征可由以下几方面来描述：

(1) 高技术性：计算机犯罪是伴随着科学技术的进步而发展起来的，其作案工具、手段都是利用科学技术，因此说它具有高技术性。另外从图 1－2－1 的犯罪人员职业分布可以看出，计算机专业人员占比例最大，从而也说明了高技术这一特性。

(2) 瞬时性：常规的犯罪活动是以分钟、小时、天、周和年来计算的，而计算机犯罪常常是短短的一瞬间内发生并完成的，一般只需几毫秒或几秒。这种特性，使得犯罪行为难以发现和取证。

(3) 隐蔽性：象“逻辑炸弹”和“特洛依木马”一样，计算机犯罪行为有很好的伪装和自我保护，它往往隐藏在系统中一段时间，只有当某种条件具备时才进行破坏活动，这也为取证和破获带来很大困难。

(4) 广域性：这是由于计算机网络系统的广泛应用而带来的计算机犯罪的特性，网络系统的建立和发展，使得地理上的界限已不能阻挡计算机犯罪活动的发生，它可以通过网络系统跨国界地进行破坏活动。



A: 计算机专业人员
B: 部门有关人员
C: 其他

图 1—2—1 计算机犯罪人员职业分布图

从计算机犯罪作案人员的角度来看计算机犯罪具有以下特点：

- 犯罪者趋向年轻化；
- 犯罪者趋向专业化；
- 计算机犯罪的共谋作案性；
- 计算机犯罪人员趋向国际化。

2.2.3 计算机犯罪的手段

企图利用计算机系统进行犯罪活动的人，通常采用的都是与计算机技术及知识有关的高新技术，而且作案人本身也往往具有较高的技术水平。通过对计算机犯罪案例的分析，这种利用高技术进行犯罪活动的手段基本可分为四大类，即："黑客"、"病毒"、"泄漏"、"拒绝"，具体如下：

(1) 数据欺骗 (Data diddling)
(2) 特洛依木马 (Trojan horse)
(3) 逻辑炸弹 (Logic bombs)
(4) 意大利香肠术 (Salami techniques)
(5) 超级冲击 (Superzapping)
(6) 活动天窗 (Trabdoors)
(7) 清理垃圾 (Scavening)
(8) 浏览 (Browsing)
(9) 数据泄露 (Data leakage)
(10) 顺手牵羊 (Piggy backing)
(11) 冒名顶替 (Impersonation)
(12) 蠕虫 (Worm)

(13) 核心大战 (Core wars) 等

2.3 计算机犯罪带来的危害

2.3.1 黑客对计算机系统的危害

黑客是指那些非计算机系统的合法用户，而又具有高技术可以采用各种手段进入计算机系统窃取数据的人。

黑客行动是有预谋的犯罪活动，直接并严重地威胁着计算机系统的安全与可靠，也给计算机系统及用户带来了极大的危害。下面列举几个典型案例以示说明黑客对计算机系统造成的危害与损失。

一个著名的例子是关于“意大利香肠术”袭击的，即一个程序员把 1 分以下舍去的小数部分转移到自己的银行帐号中去，结果积成了一笔可观的数额。

1983 年哥伦比亚发生了一起轰动一时的计算机盗窃案，这是一个通过计算机网络系统进行国际化金融犯罪的典型例子，损失金额 1350 万美元。

利用信用卡的犯罪活动也十分严重，德国的四名罪犯利用计算机改变信用卡的磁条密码，一次骗走十万马克而被捕。

另一起是涉及美国、英国、欧洲的一起关于五万美元的信用卡诈骗案。手段是非法收集信用卡号码，然后出售。

在 AT&T 系统协会上，75 个用户提出了同样的问题，这就是由于黑客的骚扰，使公司的电话费用一个月内增加了三倍。

据英国报纸《保卫者》报道，1991 年英国伦敦计算机犯罪诈骗金额已达到 10 亿英磅，是上一年的两倍还多。

信息高速公路技术的发展，为黑客犯罪提供了新的场所。在美国，人们发现黑客正在对信息高速公路的设想构成威胁。通过“特洛依木马”偷窃用户的口令，用以进入 Internet 上的的其它网络。据推测，这个黑客可能已经窃取了联在 Internet 上的数以千计的用户口令。

政府部门、军事系统也是黑客们猎取的主要目标，近几年来时常有这方面的犯罪报道。如美国的 ARPANET、国家宇航局的 SPAN 及美国国防部的计算机系统都曾不同程度地遭受过黑客的入侵，造成不同程度的破坏与损失。

在海湾战争中，以色列某年轻黑客，打入了五角大楼的计算机控制系统，读出并拷贝有关“爱国者”导弹防御系统和美国国防部的其它绝密程序，因而被称为“爱国者”黑客而被拘留。

在我国，每年计算机犯罪带来的损失也是很大的，某地区自 1987 年首例犯罪案件以来，至今已有 10 多起，总计直接损失 140 多万元人民币。

在金融领域，计算机犯罪问题更为严重，早在 1986 年我国即发生了第一起计算机犯罪案件，案犯陈某利用女友是某银行营业所柜员的条件，了解客户的帐号及余额，然后伪造存折，并利用在另外银行所开的帐户一周内提出港币 3 万元，人民币 2 万元，并专业化地毁灭了证据。

1994 年我国又发生了第一起利用计算机网络系统进行犯罪活动的案件。案犯是某证券公司电脑部的经理，精通计算机软件，利用证券交易系统初上马使用、在安全防范上未加考虑的漏洞，通过软件商为维护软件应用系统而留下的陷井，登录进入到其它证券商的系统中，

通过网络系统非法取回大量客户信息到他自己设计的数据库中，然后经过一定时间的分析与试验，虚增已卖空的帐户中的数额，然后进入股票市场，哄抬他自己购买但正处于赌本状态的那几种股票的市场价格，并伺机卖掉他自己的股票，第一次就获利 1.1 万元，第二次做案获利 0.4 万元。

另外，在银行系统也有虚设帐户、虚存实取、私设程序、修改金额等犯罪案件的发生，严重威胁着金融业务的正常开展。

时至今日，计算机黑客已形成组织或集团，联合进行计算机犯罪活动。

由此可见，世界性的黑客活动正日益危害着各行各业的正常工作，是我们必须足够重视并致力于解决的重要问题。

2.3.2 计算机病毒对计算机系统的危害

计算机犯罪的另一方面——计算机病毒更是一个全球性的问题。无论在我国还是在国际上，自从第一例病毒发现以来，它就以强大的生存繁衍能力在全世界范围内蔓延开来，至今尚没有很好的根治办法。尤其在中国，由于人们习惯于共享软件，又没有良好的管理措施和工作习惯，因此传播更快，危害更大。

在国外自 1983 年发现首例病毒发展到今天，又出现了两类新型病毒，一类是“隐蔽型”的计算机病毒，又称其为隐形飞机式病毒 (stealth virus)，目前已发展到 200 多种。另一类是变形病毒，又有人称为“千面人病毒”，以对比病毒码方式根本查不到这种病毒的病毒码，这类病毒目前越来越多。

在美国影响最大的是米开朗基罗病毒，每年发生一次，造成的损失无法估计。另外还有一种叫“炸弹虫”的病毒，在华盛顿非常流行，这是一种变形病毒，专门设计用来击败 CPAV 和 SCAN 等病毒扫描软件，因此不但扫描无效反而会加剧病毒的传播。

在各种各样的计算机病毒中，给计算机系统及社会造成危害最为严重的要首推网络病毒，又称蠕虫 (Worm)。过去几年来，已在世界上几种常用而重要的网络系统上发现了 Worm，并给这些网络系统造成不同程度的危害。如：

(1) IBM“圣诞卡”病毒就是一种网络上蠕虫爬行蔓延的病毒，它造成了 IBM 专用电子邮件网的 35 万台终端被堵塞的现象。

(2) PC—VAN 病毒，它是一种“特洛依木马”。在这次病毒事件中，有 13 个合法用户的密码被盗，虽然范围不大，也没有造成太大的危害，但在日本也引起了很大震动。

(3) Internet 网络病毒，轰动全球的“莫里斯”案件也是一起严重的 Worm 侵入计算机网络系统的事件。它是利用 UNIX 系统中电子邮件的弱点而入 Internet 网络，并在其中不断自我复制的。至使 6200 台 DEC 的 VAX 小型机及运行 UNIX 的 SUN 工作站都染上了病毒，计算机用户的损失约 9200 万美元。

(4) 3′com 校园网受到病毒侵害，关闭长达数小时，所有九个局域网都不能正常运行。

3、计算机安全组织机构与标准

3.1 现状

早在60年代，国外已有许多政府部门和军事部门广泛使用计算机系统，并用其处理大量保密的、敏感的数据。这客观上使得政府部门不得不对安全问题加以重视，并在60年代末就开始集中精力进行计算机安全方面的研究工作。

最早的研究是美国国防部（DOD）发起并领导的，制定了一系列计算机安全的策略和标准。

其次是由美国国家标准局（NBS）在70年代末进行的，它组织了许多会议和工作组，为计算机系统的安全定义标准。

这些工作的开展和进行，使得美国国家安全局（NSA）担负起了计算机安全的责任，并于1981年成立了DOD的计算机安全中心（CSC），该中心于1985年改名为现在的国家计算机安全中心（NCSC），专门从事计算机安全标准方面的研究。

随着人们对计算机安全问题的迫切要求，从事其标准研究的组织机构越来越多，这些机构及其标准领导着计算机系统安全技术的发展。

目前，国际上从事计算机及其有关安全标准研究的组织机构主要有：

- ISO：(International Standard Organization)
国际标准化组织
- CCITT：(International Telegraph and Telephone Consultative Committee)
国际电报和电话咨询委员会
- DOD：　(U.S Departmant of Defense)
美国国防部
- ECMA：　(European Computer Manufacturers Assiciation)
欧洲计算机制造商协会
- NBS：　(National Bureau of Standards)
国家标准局
- NCSC：　(National Computer Security Center)
国家计算机安全中心
- NSA：　(National Security Agency)
国家安全局
- DARPA：　(Defense Advanced Research Projects Agency)
国防高级研究规划局
- NIST：　(National Institute of Standard Technics)
国家标准技术研究所
- IFIP：　(International Federation for Information Procession)
国际信息处理联合会
- IEEE：　(Institute of Electrical and Electronics Engineers)
电气与电子工程师学会

· X/OPEN：X/开放组织

· CEN/CENELEC：欧洲标准化组织

3.2 ISO

ISO 是一个业务性的非条约组织，成立于 1946 年，其成员是 89 个国家的标准化组织，其中包括美国的 ANSI、英国的 BSI、法国的 AFNOR、德国的 DIN。ISO 公布的标准涉及众多学科，拥有约 200 个技术委员会，每个委员会涉及一个专题，它们的名称是根据其建立的先后顺序编号而成。这里我们介绍的 ISO7489－2 和一些金融标准，涉及 TC97 和 TC68。

3.2.1 ISO/TC97

TC97 是制定“计算机和信息处理”有关标准的技术委员会，ISO7489－2 是一个关于网络安全体系结构的标准，它是 ISO7489 开放系统互连基本参考模型标准的第二个附件，是建立在 OSI 基本参考模型之上的一个安全框架。

ISO7489 描述了开放系统互连（Open Systems Interconection）的“基本参考模型”，该模型的建立用于协调系统互联的标准开发框架。OSI 的目标是使异种机系统之间互联，从而达到应用进程之间的有效通信，而在任何时候，为了保护应用进程之间交换的各种信息，必须建立保证信息安全的安全机制，该机制可以使获取或修改数据所花代价比实现该机制的内在代价更大，或者窃取数据所需用的时间超过数据有效期。ISO7489－2 正是为此提供了一个一致的途径。它从体系结构角度描述了 OSI 基本参考模型之间的安全通信所必需提供的安全服务以及安全机制，并且说明了安全服务及其相应机制在安全体系结构上的关系，从而扩展了 ISO7489 的应用范围，建立了开放互联的安全体系结构的框架。

注意，该国际标准讨论的安全是在 OSI 环境中数据处理/数据通信安全的一个方面，如果要使得 OSI 环境下的安全保护措施有效，那么就要求这些措施应该同 OSI 范围以外的措施共同作用，否则安全性不能保证。

3.2.1.1 安全服务及安全机制

ISO7489－2 中描述了 OSI 安全体系中所需的基本安全服务以及实现这些服务的机制，为了满足安全策略和用户要求，不仅可以应用于 OSI 体系结构中适当的功能层次上，而且还可以用于非 OSI 体系结构之中，但要附加一些特殊的安全机制来实现。在实际建立的安全系统中，为了直接引用的方便，可以使用这些基本安全服务的某些特定组合。

ISO7489－2 在 OSI 参考模型的框架中提供了下面五种可选的安全服务：

（1）鉴别（Authentication）

该服务实现需要两部分鉴别信息，用来鉴别而存储在发送地的信息和经过通信在发送方得到的数据凭证等两部分。安全服务在通信过程中提供两种鉴别，对等实体鉴别和数据源鉴别。

前者在连接建立或者数据传送阶段的某时刻使用，以便确认一个或多个连接实体的身份，防止冒充或连接的非授权重建；后者提供对数据单元的来源提供确认（Corroboration），但不提供对数据单元的重发或篡改的保护。

（2）访问控制（Access Control）

该服务用于防止非授权地使用 OSI 协议可存取的资源，其中包括 OSI 资源以及非 OSI 资源。该服务可分别应用于各种不同类型资源的访问，如通信资源的使用、信息资源的存取及

修改、处理资源的调用执行等，也可应用于所有资源的访问，但应该注意同各种安全策略协调一致。

（3）数据保密（Data Confidentiality）

该服务提供数据的保护，防止非授权的泄露。依据网络通信机制的类型（基于连接或基于非连接）和用户需求又可分为：

- 连接保密
- 无连接保密
- 选择字段保密
- 信息流保密

（4）数据完整性（Data Integrity）

该服务用于抵抗主动威胁，采用下面五种形式：

- 带恢复的连接完整性
- 无恢复的连接完整性
- 选择字段连接完整性
- 无连接完整性
- 选择字段无连接完整性

（5）抗否认（Non－reputation）

包括带数据源证据的抗否认和带有移交证据的抗否认。

ISO7489--2 为提供上述五种安全服务，对应列出了下面特定的安全机制，它们可以设置在 OSI 参考模型框架的适当层次上。

（1）加密机制（Encipherment）

加密能为数据提供机密性，保护通信信息流的有关信息，它能单独作为一种机制运行，也能成为后面其它机制的一部分，起到补充的作用。

（2）数字签名机制（Digital Signature Mechanisms）

该机制的实质在于对特定数据单元的签名，并且只有从形成该签名的那个机密信息中产生出来，机密信息的持有者唯一，因此，当该签名得到检验之后，能够在任何时候向第三方即仲裁人提供证明签名人的证据。

（3）访问控制机制（Access Control Mechanisms）

该机制包括基于规则策略的存取控制方式和基于存取身份的访问控制方式两种，具体手段有：

- 访问控制信息库
- 鉴别信息
- 权标
- 安全标记

此外，还有访问的时间、访问的路径或访问持续的时间等手段。

（4）数据完整性机制（Data Integrity Mechanisms）

数据完整性有两个方面，单个数据单元或字段的完整性和数据单元流或字段流的完整性。

（5）鉴别交换机制（Authentication Mechanisms）

鉴别交换机制设置在网络适当层次上以提供对等实体鉴别，在鉴别实体时得到否定结果，