ICS 35.040
L 80

中华人民共和国国家标准

GB/T 20987—2007

信息安全技术　网上证券交易系统信息安全保障评估准则

Information security technology—
Evaluation criteria for online securities trading system information security assurance

2007-06-14 发布　　2007-11-01 实施

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会　发布

中 华 人 民 共 和 国
国 家 标 准
信息安全技术 网上证券交易系统
信息安全保障评估准则
GB/T 20987—2007
*
中国标准出版社出版发行
北京复兴门外三里河北街16号
邮政编码:100045
网址 www.spc.net.cn
电话:68523946 68517548
中国标准出版社秦皇岛印刷厂印刷
各地新华书店经销
*
开本 880×1230 1/16 印张 5.75 字数 154 千字
2007年10月第一版 2007年10月第一次印刷
*
书号:155066·1-29960 定价 52.00 元

GB/T 20987-2007

前　言

本标准的附录 A 为规范性附录。

本标准由全国信息安全标准化技术委员会提出并归口。

本标准起草单位：中国信息安全产品测评认证中心。

本标准主要起草人：吴世忠、王海生、陈晓桦、王贵驷、李守鹏、江常青、彭勇、张利、钱伟明、邹琪、李娟、李静、王庆、班晓芳、江典盛、陆丽、姚轶崭、孙成昊、门雪松、杜宇鸽、杨再山。

引　言

0.1　网上证券交易系统信息安全保障的含义

随着互联网技术在证券行业的应用，网上证券交易系统日益成熟。以网络为媒介进行证券交易可满足随时、随地进行快捷交易的需求。信息技术的进步促进了证券市场的发展；证券市场不断发展的需求，也促进了信息技术应用的发展。网络通讯能力的增强、网络安全技术的应用，使得证券公司与其他金融机构之间的业务合作越来越紧密。网上交易的飞速发展一方面突破了证券行业依靠传统营业部"划地为营"的地域性限制，扩大了潜在的用户市场，降低了交易服务成本，提高了服务质量；同时网上交易的出现使得证券公司的经纪业务不再仅仅凭借营业部数量的多少取胜，从规模、地理位置、装修等硬件方面的竞争向价格、服务、品牌等软件方面转化。与传统交易方式相比，网上交易具有安全性高、速度快、财经信息丰富、操作便捷等优势。

信息安全保障问题是网上证券交易系统建设和运行中必须解决的基础和根本性问题，它关系到客户与证券公司的切身利益。网上证券交易系统是一种特定的信息系统（即用于采集、处理、存储、传输、分发和部署信息的整个基础设施、组织结构、人员和组件的总和），它的信息安全保障工作必须结合证券行业的特点，以风险和策略为出发点和核心，即从网上证券交易系统所面临的风险和所处的环境出发制定网上证券交易系统的安全保障策略，在网上证券交易系统的整个生命周期中从技术、工程、管理和人员等方面提出安全保障要求，确保信息的保密性、完整性和可用性特征，实现和贯彻组织机构策略并将风险降低到可接受的程度，达到保护证券公司的信息和信息系统资产，从而保障证券公司业务安全、可靠开展的最终目的。

网上证券交易系统信息安全保障涵盖以下几个方面：

a）网上证券交易系统信息安全保障应贯穿网上证券交易系统的整个生命周期，包括规划组织、开发采购、实施交付、运行维护和废弃五个阶段，以获得网上证券交易系统信息安全保障能力的持续性。

b）网上证券交易系统信息安全保障不仅涉及安全技术，还应综合考虑安全管理、安全工程和人员安全等，以全面保障网上证券交易系统安全。在安全技术上，不仅要考虑具体的产品和技术，更要考虑网上证券交易系统的安全技术体系架构；在安全管理上，不仅要考虑基本安全管理实践，更要结合组织的特点建立相应的安全保障管理体系，形成长效和持续改进的安全管理机制；在安全工程上，不仅要考虑网上证券交易系统建设的最终结果，更要结合系统工程的方法，注重工程过程各个阶段的规范化实施；在人员安全上，要考虑与网上证券交易系统相关的所有人员包括规划者、设计者、管理者、运营维护者、评估者、使用者等的安全意识以及安全专业技能和能力等。

c）网上证券交易系统信息安全保障是基于工程的保障。通过风险识别、风险分析、风险评估、风险控制等风险管理活动，降低网上证券交易系统的风险，从而实现网上证券交易系统信息安全保障。

d）网上证券交易系统信息安全保障的目的不仅是保护信息和资产的安全，更重要的是通过保障网上证券交易系统的安全，保障网上证券交易系统所支持的业务，从而达到实现组织机构使命的目的。

e）网上证券交易系统信息安全保障是主观和客观的结合。通过在技术、管理、工程和人员方面客观地评估安全保障措施，向网上证券交易系统的所有者提供其现有安全保障工作是否满足其

安全保障目的的信心。因此，它是一种通过客观证据向网上证券交易系统所有者提供主观信心的活动，是主观和客观综合评估的结果。

f) 保障网上证券交易系统安全不仅是系统所有者自身的职责，而且需要社会各方参与，包括电信、电力、国家信息安全基础设施等提供的支撑。保障网上证券交易系统安全不仅要满足系统所有者自身的安全需求，而且要满足国家相关法律、政策的要求，包括为其他机构或个人提供保密、公共安全和国家安全等社会职责。

0.2 网上证券交易系统信息安全保障评估准则的编制目的和意义

GB/T 20274《信息安全技术 信息系统安全保障评估框架》是建设、评估信息系统安全保障的基础性和框架性标准，给出了对信息系统安全保障体系的通用要求。本标准是在 GB/T 20274 的基础之上，结合网上证券交易系统的具体特点，给出了网上证券交易系统的信息系统安全保障要求。

制定本标准的意义在于：

a) 为网上证券交易系统信息安全保障的设计、实施、建设、测评、审核提供规范的、通用的描述语言；

b) 有利于网上证券交易系统所有者编制其信息系统的安全保障要求；

c) 有利于网上证券交易系统安全集成商和安全服务提供商提供更为科学规范化的设计和服务，促进信息安全市场的发展；

d) 有利于有关行政管理部门、执法机构、测评认证机构对网上证券交易系统进行安全检查、检测、审计、评估和认证。

目　次

信息安全技术　网上证券交易系统信息安全保障评估准则

1　范围

本标准规定了网上证券交易系统的描述、安全环境、安全保障目的、安全保障要求及网上证券系统信息安全保障目的和安全保障要求的符合性声明。

本标准适用于规范网上证券系统在交易过程中涉及信息安全的评估工作。

2　规范性引用文件

下列文件中的条款通过本标准的引用而成为本标准的条款。凡是注日期的引用文件，其随后所有的修改单(不包括勘误的内容)或修订版均不适用于本标准，然而，鼓励根据本标准达成协议的各方研究是否可使用这些文件的最新版本。凡是不注日期的引用文件，其最新版本适用于本标准。

GB/T 20274(所有部分)　信息安全技术　信息系统安全保障评估框架

3　术语和定义

GB/T 20274 确立的以及下列术语和定义适用于本标准。

网上委托　entrust through Internet

证券公司通过互联网，向在本机构开户的投资者提供用于下达证券交易指令、获取成交结果的一种服务方式。

4　系统描述

4.1　网上证券交易系统概述

网上证券交易系统是一种具有特定使命、技术系统和组织结构的信息系统。信息系统是用于采集、处理、存储、传输、分发和部署信息的整个基础设施、组织结构、人员和组件的总和。在本标准中，所使用的信息系统概述框架见图 1。

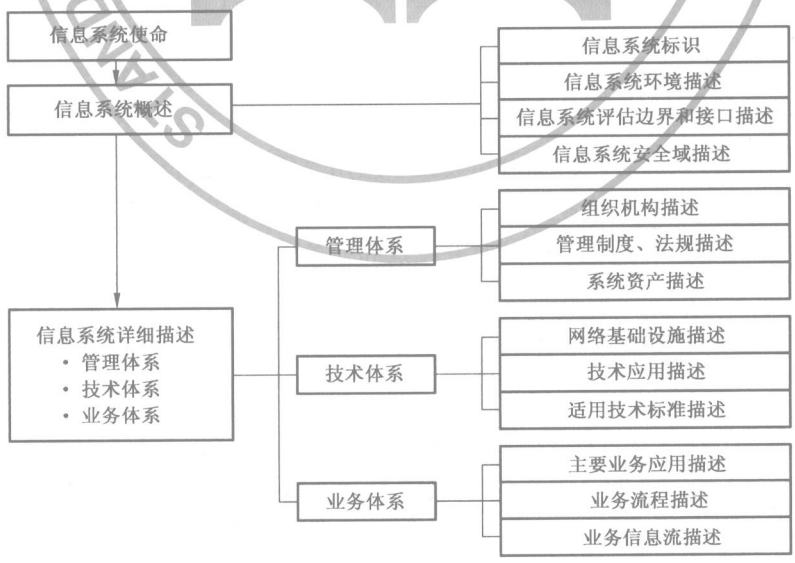

图 1　信息系统框架

整个信息系统描述主要包括三个大类：信息系统使命、信息系统概述和信息系统详细描述，相应的具体描述内容包括：

a) 信息系统使命：即从目的和意义方面对信息系统进行高层描述，它是信息系统根本和本质的要求。

b) 信息系统概述：对所要评估的信息系统进行概括性说明和描述。

1) 信息系统标识：应给出系统的正式名称和标识。系统标识包括其名称、所属的公司及其地点和包含最终用户及其地点等相关信息；

2) 信息系统环境描述：描述的运行环境以及系统开发、集成和维护的环境；

3) 信息系统评估边界和接口描述：描述所要评估系统的边界和相应的外部接口，此描述必须用图表或文字清晰地描述和界定所要评估的系统部件和边界；

4) 信息系统安全域描述：根据系统的关键性（描述系统的关键性以及系统可接受的风险级别）、数据的分类和密级（描述系统所处理的数据类型和机密级别）和系统用户（描述使用系统的用户描述）等方面划分系统的安全域。

c) 信息系统详细描述：此部分从管理体系、技术体系和业务体系三个方面分别对信息系统进行详细描述。

1) 管理体系：在管理体系中，需要对信息系统现有的管理组织结构、所使用的相应规章制度和所涉及的重要资产进行描述。

——组织机构描述：信息系统相关的管理、使用、开发、集成、支持组织机构的描述，特别是相关安全保障管理的组织机构的描述；

——管理制度、法规描述：列出同信息系统管理相关的目前使用的相应规章制度和相关法规；

——系统资产描述：信息系统的物理资产（指网上证券交易系统中的各种硬件、软件和物理设施）和信息资产（指在网上证券交易系统计划组织、开发采购、实施交付、运行维护和废弃这一网上证券交易系统生命周期过程中产生的同网上证券交易系统本身相关的有价值的信息以及网上证券交易系统所存储、处理和传输的各种相关的办公、管理和业务等信息）列表。

2) 技术体系：技术体系是信息系统描述的基础，需要对现有的各种应用、相应的网络基础设施和所使用的技术标准进行描述，这些描述将帮助了解用户的信息系统并为进一步描述业务系统提供基础和支持。

——网络基础设施描述：系统的网络层次等网络体系结构说明；

——技术应用描述：用户信息系统的各种应用说明；

——适用技术标准描述：列出相关技术应用等所适用的技术标准。

3) 业务体系：业务体系从业务角度和应用角度出发，基于技术体系，对组织机构的主要业务应用进行分类和描述，并通过业务流程和业务信息流来进一步解释。

——主要业务应用描述：列出组织机构的主要业务应用并进行描述；

——业务流程描述：基于组织机构的管理结构等，描述业务的流程；

——业务信息流描述：描述主要业务应用的接口和相应数据流，数据流描述应包括数据的类型以及数据传送的一般方式。

4.2 网上证券交易系统技术参考模型

为了更好地帮助理解和规范化网上证券交易系统描述，图2列出本规范所建议使用的信息系统技术参考模型。通过此技术参考模型的介绍，帮助用户能以一种更规范、结构化和标准化的方式描述信息技术系统。

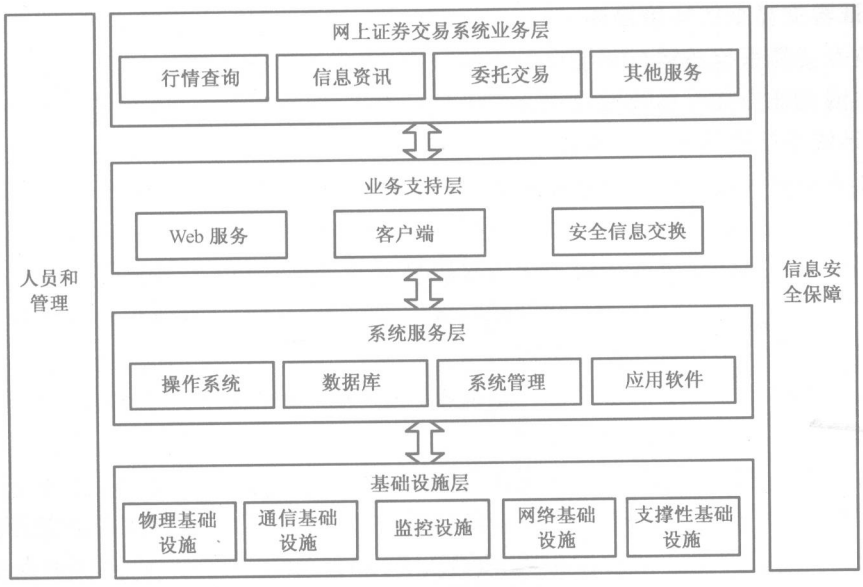

图 2　信息系统技术参考模型

信息系统技术参考模型提供了一个描述和理解信息技术系统的公共词汇表，并定义了信息技术系统通用的服务和接口集合。通过公共词汇表和服务、接口集合的定义，帮助用户以通用、标准化和提高互操作的方式建设、分析和描述信息技术系统。

信息系统技术参考模型主要涉及信息系统描述中的技术体系和业务体系。整个网上证券交易系统技术参考模型分为六个模块：基础设施层、系统服务层、业务支持层、业务应用层、信息安全保障、人员和管理，这六模块分别提供其特定的服务。

a) 基础设施层：向系统服务层提供所需的各种通用网络基础服务，如信息交换服务等；

b) 系统服务层：向业务支持层、业务应用层提供操作系统和数据库等支持；

c) 业务支持层：向业务应用层提供 Web 服务、客户端和安全交换等服务支持；

d) 业务应用层：提供行情查询、信息资讯、委托交易等应用服务技术；

e) 信息安全保障：在各个层面为网上证券交易提供机密性、完整性、可用性、鉴别、抗抵赖等安全服务。主要涉及安全管理、安全协议、加解密、签名与认证、密钥管理、安全测评、公钥基础设施等；

f) 人员和管理：为各个层面提供法律、法规、政策、标准、管理等支持。

4.3　网上证券交易系统描述

4.3.1　网上证券交易系统使命概述

证券公司建设网上证券交易系统，应依据国家相关标准，从具体情况出发，分析实际需求，确定系统所要实现的功能，明确系统与统一网络平台的接口，在保证安全的前提下促进系统的互联互通和系统资源的综合利用；分析系统运行中存在的威胁，从技术、管理、工程三方面实现安全保障。通过建立一个符合标准、功能完善、安全可靠的网上证券交易系统，安全、可靠、快捷的提供网上交易服务。

4.3.2　网上证券交易系统概述

网上证券交易系统概述，即对所要评估的信息系统进行概括性说明和描述。它主要包括：网上证券交易系统标识、网上证券交易系统环境描述、网上证券交易系统评估边界和接口描述以及网上证券交易系统安全域描述。

4.3.2.1　网上证券交易系统标识

网上证券交易系统应给出系统的正式名称和标识，在系统标识中应标明以下内容：

——名称：×××公司网上证券交易系统；

——所属公司；

——地点：×××公司。

4.3.2.2 网上证券交易系统环境描述

描述网上证券交易系统的运行环境以及系统开发、集成和维护的环境。在网上证券交易系统信息安全保障目的中网上证券交易系统的使用方应给出其所被评估的网上证券交易系统的详细环境描述。

4.3.2.3 信息系统评估边界和接口描述

信息系统评估边界和接口描述应根据所需评估的系统的实际情况，综合考虑安全域等原则进行边界划分，用图表和文字清晰地说明和界定所要评估的系统部件和边界。

图 3 中的例子用于概念化说明如何用图表对边界划分进行描述，此例为集中转发式网上交易系统实例，实际情况中可能主站点位于证券公司内部，仅作为参考。用户应在其信息安全保障目的文件中根据其所要评估信息系统的实际情况加以描述。

此例假设为某个网上证券交易系统的评估边界，其同外部系统的边界点和边界部件为：

——同公众网之间的逻辑隔离设备；

——评估边界为主站点、总部、下属营业部(可对营业部进行抽样)。主站点包括行情服务器、交易服务器等，总部包括转发前置机、安全隔离模块、转发后置机，营业部包括柜台前置机等；

——主站点是网上证券系统的对外联系“窗口”，主要负责实现接受用户的各类服务请求；接受、存储、发布行情信息；对用户的交易指令进行预处理，并转发给证券公司；

——位于总部的服务器通过广域网向营业部分发交易指令；接收交易所发送的卫星行情和资讯信息，并发送给托管机房服务器；监控、统计、分析各营业部的交易数据等；

——位于营业部的柜台前置机负责接收总部发送过来的交易数据；对交易数据进行加、解密；并将交易数据转换为柜台系统能够识别的格式发送给柜台系统处理。

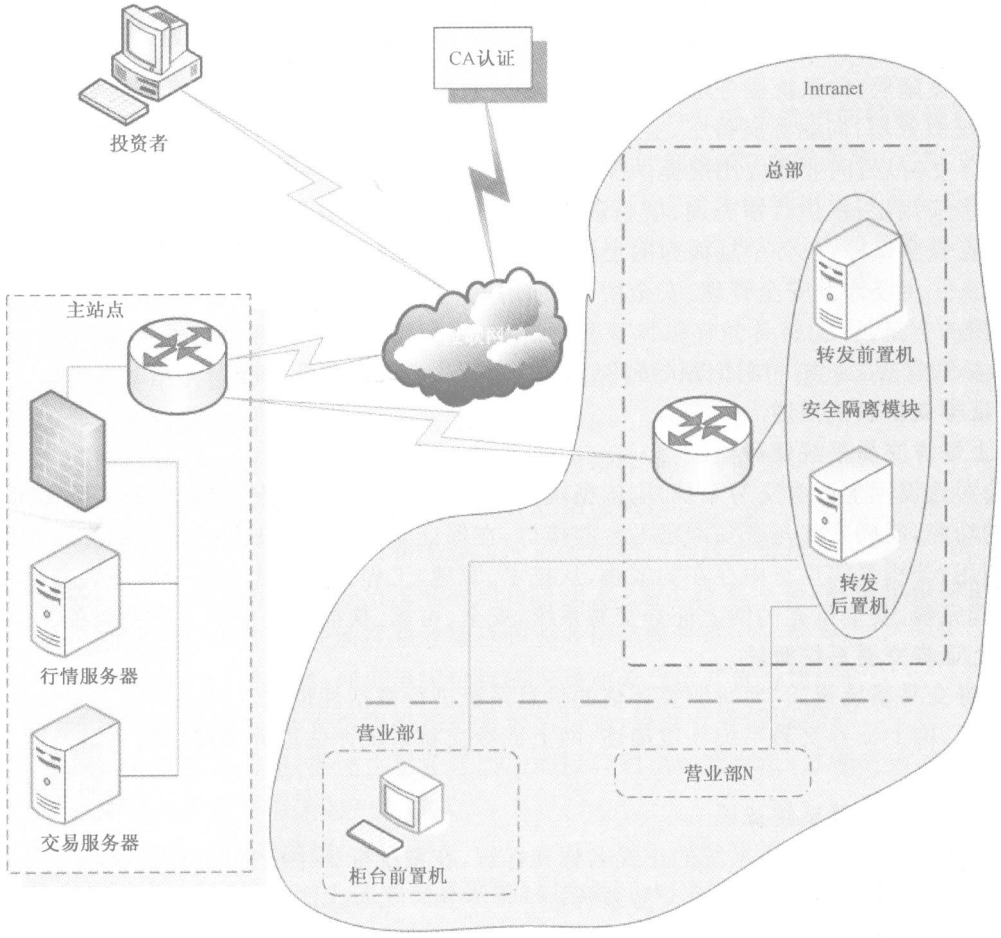

图 3 网上证券交易系统评估边界界定示意图

4.3.2.4 网上证券交易系统安全域描述

网上证券交易系统是一个涉及不同用户对象、数据敏感程度等的一个复杂网络。在网上证券交易系统的安全保障目的中，应根据用户对象、数据敏感程度等划分安全域。通过不同安全域的描述和界定，就能更好对网上证券交易系统进行描述。

网上证券交易系统的网络系统结构包括根据用户对象的不同以及所涉及的信息敏感程度的不同而进行的分类。如表1。

表1 网上证券交易系统用户和信息敏感程度描述

	网上证券交易系统		
用户对象	普通公众	投资者	证券公司人员
信息敏感程度	—	商业秘密	内部信息

4.3.3 网上证券交易系统详细描述

从管理体系、技术体系和业务体系三方面分别对网上证券交易系统进行描述。

4.3.3.1 网上证券交易系统管理体系

管理体系：在管理体系中，需要对网上证券交易系统现有的管理组织结构、所使用的相应规章制度和所涉及的重要资产进行描述。

4.3.3.1.1 组织机构

在网上证券交易系统组织机构概述中，应包括同网上证券交易系统相关的管理、使用、开发、集成、支持组织机构的描述，特别是相关安全保障管理的组织机构的描述。

4.3.3.1.2 管理制度和法规

管理制度、法规描述部分要求列出同网上证券交易系统管理相关的目前使用的相应规章制度和相关法规，在网上证券交易系统信息安全保障目标中用户应给出其所评估的网上证券交易系统管理中所使用的国家、部门、行业和内部的相关管理制度和法规。

4.3.3.1.3 系统资产

资产是网上证券交易系统所要保护的对象，所有威胁都必须针对资产才能产生影响，所有威胁只有通过资产这个载体才能影响网上证券交易系统的最终目标——网上证券交易系统的使命。

在网上证券交易系统中，资产分为物理资产和信息资产。

4.3.3.1.3.1 物理资产

物理资产是指网上证券交易系统中的各种硬件、软件和物理设施。例如：系统的各种网络设备和软件资产。在网上证券交易系统信息安全保障目标中，应详细列出所评估的特定网上证券交易系统中的所有重要资产。下面仅列出在网上证券交易系统中所包含的部分物理资产示例，作为参考：

a) 物理设施

物理设施包括场地、机房、电力供给(负荷量及冗余、备份、净化)、灾难应急(防水、火、地震、雷击等)、文档及介质存储。

b) 硬件资产

硬件资产包括：

1) 计算机：包括大、中、小型计算机，个人计算机；

2) 网络设备：包括交换机、集线器、网关设备或路由器、中继器、桥接设备、调制解调器/Modem池、配线架；

3) 中间件设备：作为交易中间件使用的后台转换机、柜台处理机、委托成交转换机、单向卫星接收机、双向卫星接收机、报盘机以及行情处理等专用微机或工作站；

4) 传输介质及转换器：包括同轴电缆(粗/细)、双绞线、光缆/光端机、卫星信道(收/发转换装置)、微波信道(收/发转换装置)；

5) 输入/输出设备：包括键盘、电话机、传真机、扫描仪、打印机(激光/针式/喷墨)、显示器、终端(数据/图像)；

6) 存储介质：包括纸介质、磁盘、磁光盘、光盘(只读/一次写入/多次擦写……)、磁带、录音/录像带；

7) 监控设备：包括摄像机、监视器、电视机、报警装置。

c) 软件资产

软件资产包括：

1) 计算机操作系统：包括 Unix、Windows NT/2000、HP-UX、其他计算机操作系统；

2) 网络操作系统：包括 IOS、Novell Netware、SNA、其他专用网络操作系统；

3) 通用应用软件：包括 Notes/MS Word、E-mail、Web 服务/发布与浏览软件、其他服务软件；

4) 网络管理软件：包括 SNMP、HP Openview、Netview、其他网络管理软件；

5) 数据库管理软件：包括 Oracle、Sybase、SQL Server、其他数据库管理软件；

6) 业务应用软件：包括网上交易客户端软件、交易主机应用服务软件、交易转发软件、行情服务、行情发送及行情接收软件、SSL 安全网关软件、物理隔离软件等。

4.3.3.1.3.2 信息资产

信息资产是指在网上证券交易系统计划组织、开发采购、实施交付、运行维护和废弃这一网上证券交易系统生命周期过程中产生的同网上证券交易系统本身相关的有价值的信息以及网上证券交易系统所存储、处理和传输的各种相关的办公、管理和业务等信息。例如：系统的网络配置信息、各种维护升级记录、各种业务应用信息等。下面仅列出在网上证券交易系统中所包含的部分信息资产示例，作为参考：

a) 客户信息：包括客户资料、资金数据和交易数据等，这些均属于商用加密信息类别；

b) 交易信息：是主要的业务数据，包括委托数据、成交回报数据等；

c) 行情信息：包括行情查询数据、行情分析数据、现行行情和历史行情信息数据等；

d) 信息资讯：主要是证券相关信息，如新闻、综合报道、专家观点、机构股评、资料、快讯新闻和股评等内容通过信息发布系统提供给投资者参考；

e) 密码信息：包括秘密密钥、私钥、公钥、证书等；

f) 系统维护管理信息：包括系统运行日志、系统审计日志、系统监督日志、入侵检测记录、系统口令、系统权限设置、数据存储分配、内部网络地址、系统配置数据、网络设备的配置信息、路由信息、IP 地址分配信息、设备采购信息、设备维护及升级记录、布线图纸、布线系统维护及升级记录、通信线路参数、以及其他信息等。

4.3.3.2 网上证券交易系统技术体系

技术体系是信息系统描述的基础，需要对现有的各种应用、相应的网络基础设施和所使用的技术标准进行描述，这些描述将帮助了解用户的信息系统并为进一步描述业务系统提供基础和支持。技术体系描述包括网络基础设施描述、技术应用描述和适用技术标准描述。

4.3.3.2.1 网络基础设施描述

网络基础设施结构图将描述网上证券交易系统的网络层次等网络体系结构说明，图 4 给出网上证券交易系统的网络基础设施结构概念性说明。用户应基于此图，在信息系统安全保障目标文档中给出网上证券交易系统的详细网络结构图。

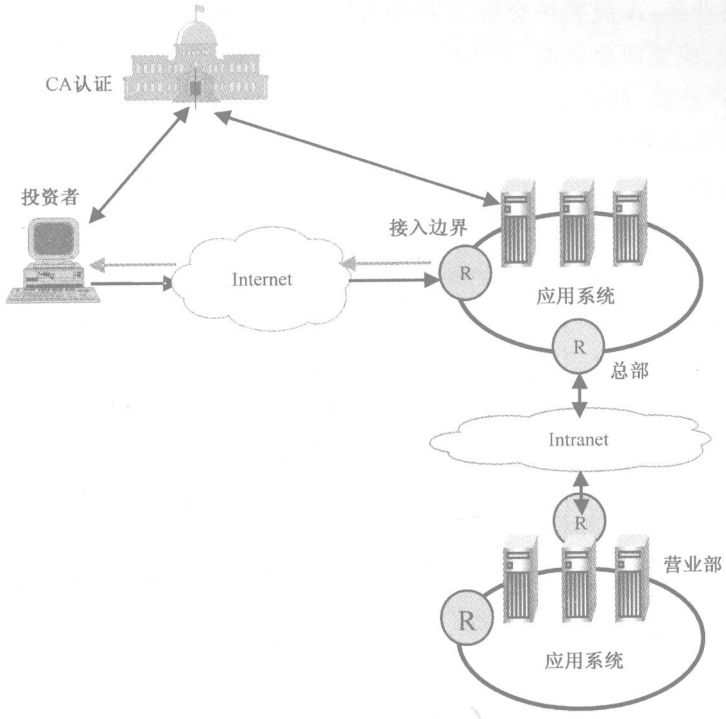

图 4　网上证券交易系统网络体系结构

本系统提供如下安全服务：

a)　确保投资者交易数据的机密性、完整性和准确性；

b)　正确识别网上投资者身份，防止假冒投资者或证券公司身份；

c)　防止交易双方事后否认该事情发生过；

d)　确保网上证券交易系统和其他业务在技术上隔离，禁止通过网上证券交易系统直接访问任何证券公司内部系统；

e)　保证本系统安全性和可用性。

4.3.3.2.2　技术应用描述

描述用户信息系统的各种应用说明。在网上证券交易系统信息安全保障目标中，应详细描述网上证券交易系统的各种应用系统，并进行详细描述。

4.3.3.2.3　适用技术标准描述

列出相关技术应用等所适用的技术标准。在网上证券交易系统信息安全保障目标中，应列出网上证券交易系统的各种应用系统所遵循的标准。

4.3.3.3　网上证券交易系统业务体系

业务体系描述即从业务角度和应用角度出发，基于技术体系，对组织机构的主要业务应用进行分类和描述，并通过业务流程和业务信息流来进一步解释。业务系统描述包括主要业务应用描述、业务流程描述和业务信息流描述。

4.3.3.3.1　主要业务应用描述

列出组织机构的主要业务应用并进行描述。在网上证券交易系统信息安全保障目标中，应对网上证券交易系统进行详细描述，此描述应包含系统的功能结构图、系统的输入数据、数据操作以及输出的产品。

网上交易系统从功能上主要划分为实时委托交易子系统、行情查询与分析子系统和资讯服务子系

统，分别包括如下业务：

a) 实时委托交易业务：A股委托交易、B股委托交易、新股申购、基金及债券业务、资金余额查询、股份余额查询、成交回报查询、历史成交记录查询、撤单、保证金对账单查询、个人信息查询、盈亏计算、总资产核算、修改交易密码、储蓄余额查询、从保证金转款到储蓄、从储蓄转款到保证金、计算市值、批量委托、交割单、对账单查询等；

b) 行情查询与分析业务：实时行情查询、大盘走势、个股行情、行情分析（支持分时走势，F5日线图，F8周线、月线、分钟线的查询）服务等；支持离线浏览和数据下载；支持各种画线功能图，支持自选股设置；支持板块定义及分析，综合排名功能，紧急公告功能；支持股票模糊查询、拼音查询等功能；

c) 资讯服务业务：提供深沪交易所信息、个股资料信息、提供部分研究报告服务及投资建议、特别报道、紧急公告功能、信息咨询服务、投资研究服务、投资建议等服务。

网上证券交易系统的应用业务是为证券公司现有客户和潜在客户提供安全、高效的网上证券交易，使客户方便快捷地查询个人信息资源，并能通过该系统接受行情分析、信息咨询等服务。

4.3.3.3.2 业务流程描述

基于组织机构的管理结构等，描述业务的流程。在网上证券交易系统信息安全保障目标中，根据业务应用结合组织机构的业务流程进行详细描述。

4.3.3.3.2.1 委托交易流程

委托交易子系统由客户端、物理隔离机、加解密安全网关、交易主机应用服务器、交易分发服务器和营业部交易前置机几部分组成。

首先，投资者亲自到开户营业部签署开通网上交易的协议同时获得数字身份证明文件（CA证书），以此通过客户端程序或Internet进入网上交易系统。

在正式开始交易前，客户端软件和服务器软件之间要先进行“握手”，在握手过程中通过数字身份证明文件（CA证书）互相鉴别身份。

其次为第二个阶段——数据传输过程，也就是实际的数据传输过程，这个过程发生在握手过程结束后。在正式交易过程中，客户的交易请求信息由客户端软件加密后把加密后的信息发给加解密安全网关服务器，继而发给交易主机应用服务器，然后转发给总部交易分发服务器，分发服务器根据客户不同的需求将交易信息发送到相对应的营业部交易前置机。再由前置机将加密后的交易请求信息经解密再提交给营业部柜台系统的中间件服务器，最后由营业部柜台系统做相应的处理，并将最终的交易结果按原路反馈给客户。

4.3.3.3.2.2 行情查看流程

行情分析子系统由行情客户端、行情服务器、行情接收系统及行情发送程序几部分组成。

投资者需要查看行情时，只需通过行情客户端输入想要查询的证券代码。客户端即将查询请求发送给行情服务器，在收到客户端的请求后，行情服务器从行情数据库中提取相应的证券信息反馈给行情客户端。

此外，在开市期间，行情接收程序会实时地从行情发送程序获取行情信息并将其转存到行情数据库中，以便用户得到最新的信息。

行情发送程序通过隔离机把读取的交易所的实时行情转发给行情采集接收程序，保存在行情数据库中供行情服务器调用。

行情查看流程如图5所示。

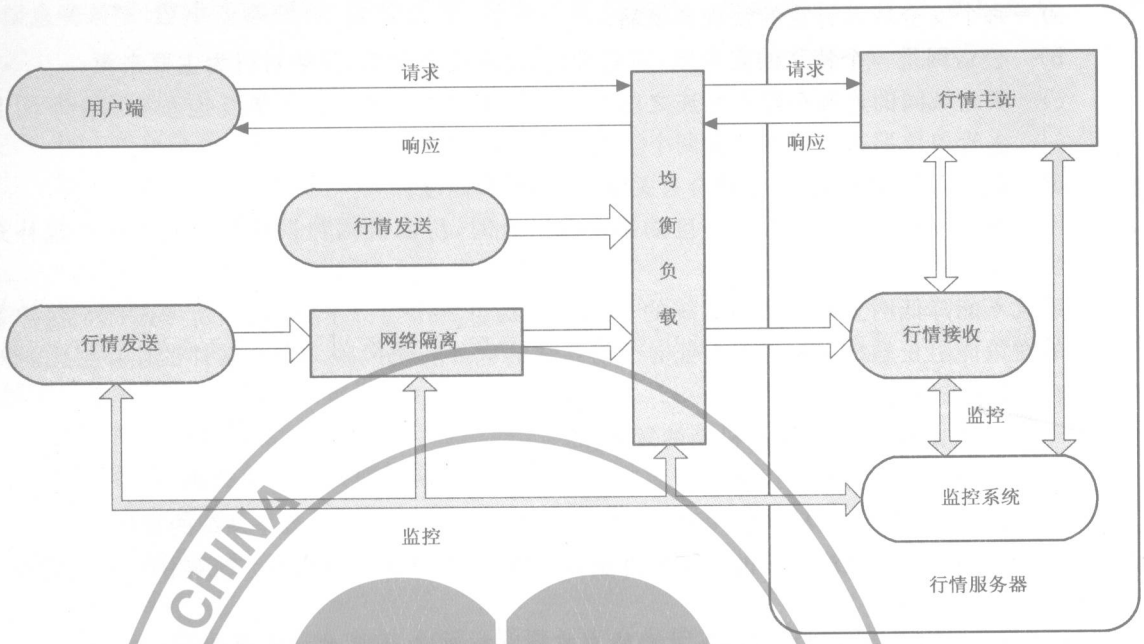

图 5 行情查看流程图

4.3.3.3.2.3 信息资讯流程

投资者可以通过浏览器访问证券网站或通过客户端程序直接查阅所需信息。信息资讯查看流程与行情查看流程完全相同。

4.3.3.3.3 业务信息流描述

描述主要业务应用的接口和相应数据流。数据流描述应包括数据的类型以及数据传送的一般方式。在网上证券交易系统中存在两种类型的信息流:投资者到券商的信息流、券商到投资者的信息流。在网上证券交易系统信息安全保障目标文档中应根据具体情况,并参考本准则中所提出的信息流分类方法进行详细描述。

5 安全环境

5.1 假设

假设是建立在对网上证券交易系统环境预期的应用环境和使用方式的基础上。假设按 A-1、A-2……A-N 编号,假设一般分两类:

a) 关于网上证券交易系统开发和运行环境的一般假设(包括与系统交互的人员、内部互连和物理控制的陈述);

b) 网上证券交易系统中描述系统角色的假设。

5.1.1 网上证券交易系统环境安全假设

环境安全假设有:

A-1 可用性可能依赖于从通信线路提供商提供的通信质量和能力。自然或人为灾难对通信可用性产生的扰动是在系统之外的。通信线路是作为系统一部分的。系统必须提供足够的保护以降低拒绝服务攻击达到一个可接受的水平。

A-2 网上证券交易系统的开发应采用不断持续改进的方法。

A-3 网上证券交易系统能使用不可信任的通信网络来建设通信能力。

5.1.2 网上证券交易系统安全服务假设

网上证券交易系统安全服务假设有:

A-4 网上证券交易系统存在以下不同的安全域:

a) 每个安全域具有它的管理和策略；

b) 公众网是一个特殊的安全域，它有管理，没有安全策略，是敌对行为主要来源；

c) 安全域间的连接在建立互连之前要求上级主管单位授权。如果互连系统属于不同上级主管单位那么互连必须由两个上级主管单位批准；

d) 连接及使用公众网，应符合有关法令、规范和制度。

A-5 网上证券交易系统安全实行深度防御。在适合时，协调机构和系统管理者可以实现补充保护机制。

A-6 系统不能降低网上证券交易系统的全部安全状态。作为一个整体，必须考虑优于保护系统的对策能阻止系统引入对网上证券交易系统的额外安全风险。安全域外的连接必须针对潜在的风险进行检查。

a) 推动通用策略、过程和机制的发展；

b) 这些保护的运行可以分配给协调机构；

c) 符合网上证券交易系统特定的或唯一的脆弱性的策略和对策是系统的责任。

A-7 在检测到的涉及执法机构的安全事件里，协调机构为网上证券交易系统提供单方的意见。

5.2 威胁

在安全环境中的资产部分描述了网上证券交易系统所需保护的资产对象客体，在本条的威胁描述中将描述在网上证券交易系统安全环境中对这些资产的所有相关威胁，这些资产是在网上证券交易系统或其环境内需要特定保护的。值得注意的是，并非所有的在环境中可能遇到的威胁都必须列出，只有那些与网上证券交易系统的安全运行相关的威胁才需要列出。

威胁是一个具备一定攻击能力的特定攻击源利用特定脆弱性对特定资产进行某种方式攻击所产生某种程度影响的可能性。因此，威胁应通过已确定的攻击源、脆弱性、资产、攻击方式和可能影响的程度进行描述。

5.2.1 威胁的分类

威胁是由多个威胁要素组成的，因此从不同角度来看，威胁有不同的分类方式。

5.2.1.1 根据威胁源主体的威胁分类

从威胁源主体来分，威胁分为：

——人员威胁：由人产生或其激活的威胁，例如无意行动（偶然的数据访问、误操作等）或有意的行动（基于网络的攻击、恶意软件上传和机密数据的非授权访问等）；

——自然威胁：洪水、地震、龙卷风、山崩、雪崩、电力风暴以及其他此类事件；

——环境威胁：长期电力故障、污染、化学和液体泄漏。

5.2.1.2 根据攻击方式的威胁分类

从攻击方式来分，威胁分为：

——内部人员攻击；

——被动攻击；

——主动攻击；

——物理临近攻击；

——分发攻击。

各种攻击方式具体解释如下：

a) 内部人员攻击

内部人员攻击往往由内部合法人员造成，他们具有对网上证券交易系统的合法访问权限。内部人员攻击分为恶意和非恶意两种，即恶意攻击和非恶意攻击。

恶意攻击是内部人员出于各种目的，对所使用的信息系统实施的攻击。

非恶意攻击是由于内部合法人员的无意行为造成了对网上证券交易系统的攻击，他们并非故意要