深圳证券交易所
SHENZHEN
STOCK EXCHANGE

# 会员及其他相关单位访问深交所交易系统接入服务技术规范

**（Ver 1.02）**

深圳证券交易所

二〇二〇年三月

# 文档说明

| 文档名称 | 会员及其他相关单位访问深交所交易系统接入服务技术规范 |
|---|---|
| 说明 | 本文档为会员及其他相关单位访问深交所交易系统的接入服务技术规范。 |

| 修订历史 | | |
|---|---|---|
| 日期 | 版本 | 修订说明 |
| 2017-05-16 | Ver1.00 | 创建文档。 |
| 2018-02-08 | Ver1.01 | 对应用安全与管理规范进行完善。 |
| 2020-03-17 | Ver1.02 | 1、将网关监控等同于接入终端进行管理；<br>2、完善网络接入规范，明确期货公司的接入具体要求，强调接入端协同配置规避线路故障；<br>3、系统阐明信息安全规范；<br>4、明确违规的后续措施，如应急处置手段等。 |

# 目 录

# 会员及其他相关单位访问深交所交易系统接入服务技术规范

## 一、前言

为规范各会员及其他相关单位访问深圳证券交易所（以下简称“深交所”）交易系统的接入服务，保障证券市场交易及相关技术系统的安全运行，根据《证券期货业信息安全保障管理办法》、《证券基金经营机构信息技术管理办法》、《深圳证券交易所会员管理规则》及行业自律规范，深交所制定本技术规范。

## 二、应用管理规范

1、会员及其他相关单位只能通过深交所或深交所授权机构许可的应用软件开展业务，所使用的应用软件版本应符合深交所要求，并按深交所要求及时升级所使用的应用软件版本。

2、会员及其他相关单位用于交易、行情等业务的接入终端（包括交易网关、行情网关、文件网关、交易终端、网关监控，下同）等设备应当根据《深圳证券交易所网关部署及接入指引》，确保应用系统的高可用性、完整性和安全性。

3、会员及其他相关单位在接入终端上安装应用软件前应先对应用软件进行评估，并保留评估记录。应对在接入终端上安装的应用软件编制软件清单，向深交所报备评估记录和软件清单。在接入终端上安装的软件清单有变化时，应在变化后的五个工作日内向深交所报备评估记录和软件清单。报备评估记录和软件清单的格式自行制定（至少包括报备负责人的姓名及联系电话和接入终端的操作系统版本），通过邮件发送到 sseyxb@szse.cn。

4、接入终端的软硬件变更管理记录、所有本地和远程操作信息、操作系统及应用软件的日志信息必须保存，严禁删除和篡改，保存时间不少于一年。

5、交易网关、行情网关和文件网关不得重复登录。同一网关号在同一时刻只允许登录一次交易及相关系统。如需热备，应使用不同网关号。

## 三、通信网络接入管理规范

1、会员必须有两个（含）以上能够互为备份的集中运行中心，分别配置访问深交所交易系统接入服务的接入终端和网络。

2、会员及其他相关单位须具备不同运营商（含托管接入）的网络接入线路，分别接入深交所主、备数据中心。通过应用层和网络层的协同配置，确保单一线路或者单一运营商故障时可继续正常开展业务，并定期演练。

3、会员及其他相关单位集中交易、行情业务的通信网络接入应达到以下要求：

- 地面通信线路带宽应满足最低要求：会员 10Mbps，基金公司、资产管理公司、保险公司和期货公司等 6Mbps；
- 在网络调试过程中以及上线投产运行后，与深交所互联接口必须使用路由网络（3 层）端口，不允许使用交换（2 层）端口；
- 在地面通信线路的基础上，至少还应有一路高速单向卫星用作地面行情的备份，可以高速双向卫星作为极端情形下的交易通信备份线路。

4、会员集中运行中心托管在深圳证券通信有限公司数据中心时，应使用互为冗余的通信线路接入交易行情托管网。

5、使用卫星接入的会员及其他相关单位必须遵守国家的相关法律、法规，与当地无线电管理部门保持联系，办理无线电台执照，并向当地无线电管理部门报备相关内容。

6、为保证交易及相关业务正常运行，会员及其他相关单位有义务配合深交所及深交所授权的单位对通信网络升级、建设、测试等工作。

## 四、信息安全规范

1、会员及其他相关单位建设、运行、维护与深交所交易及相关系统连接的接入终端和网络时，应当符合《深圳证券交易所会员管理规则》中“交易及相关系统管理”要求。

2、深圳证券通信网络为行业专网，会员及其他相关单位接入通信网络后，接入终端应当遵循：

- 不得将接入终端的 IP 地址（包括 NAT 地址转换后的 IP 地址）直接暴露于 Internet 等其他公众网络；

- 具备有效的身份鉴别措施，包括对登录的用户进行身份标识和鉴别等措施；
- 实施有效的访问控制措施，诸如由授权主体配置访问控制策略，访问控制策略规定主体对客体的访问规则等；访问控制的粒度应达到主体为用户级或进程级，客体为文件、数据库表级。
- 具备有效的入侵防范措施，包括遵循最小安装原则，仅安装必需的组件和应用程序等；
- 确保接入终端上深交所应用软件的完整性和数据传输的安全性，不得通过内存注入、数据包篡改或其他手段破坏软件本身、运行时的内存数据和网络数据包的完整性；
- 不得通过直接或间接手段影响深交所应用软件的运行，包括对软、硬件及网络环境的度量等，也不得通过直接或间接手段干扰深交所应用软件的数据包在网络上的正常传输。

3、会员及其他相关单位接入深圳证券通信专网后，互联的网络设备以及与接入终端连接的网络设备，应当遵循：

- 网络设备不得与 Internet 等其他公众网络直接互联；
- 应对网络边界、重要网络节点加强访问控制，遵守权限最小化原则；
- 应对进出网络的数据流实现基于应用协议和应用内容的访问控制；
- 具有攻击和入侵的检测与响应能力，在关键网络节点处检测、防止或限制从内外部发起的网络攻击行为。当检测到攻击行为时，记录攻击源 IP、攻击类型、攻击目标、攻击时间，在发生严重入侵事件时应提供报警；
- 禁止扫描深交所交易系统服务器 IP 地址（包括 NAT 地址转换后的 IP 地址）。

4、会员及其他相关单位作为深圳证券通信专网的重要一环，在日常运营和管理中，应当遵循：

- 应对安全策略、恶意代码、补丁升级等安全相关事项进行集中管理；
- 划分出特定的管理区域，对分布在接入终端到深圳证券通信专网上所有的网络设备、服务器、安全设备或安全组件进行管控和集中监测；
- 对网络边界、重要网络节点以及分散在各个设备上的审计数据进行收集汇总，对发生的各类安全事件进行识别、分析和告警。

5、对于已完成网络安全等级保护定级备案的系统，应定期开展等保测评工作。

## 五、其它事宜

1、本规范由深交所负责解释。

2、会员及其他相关单位应及时向深交所报告对深交所交易系统有安全隐患的异常行为。若发现瞒报、缓报异常信息，并被作为跳板攻击深交所交易系统，一经查实，将视为违反本技术规范。

3、根据《网络安全等级保护基本要求》，当深交所交易系统面临网络攻击等重大安全隐患时，深交所可采取暂停会员及其他相关单位网络接入等应急处置手段。

4、根据《深圳证券交易所会员管理规则》相关规定，深交所可对会员及其他相关单位的接入终端进行监督检查。

5. 未达到或违反本技术规范的会员及其他相关单位，将按照《深圳证券交易所会员管理规则》的规定，采取相应的自律监管措施或纪律处分。

6、本规范自发布之日起施行。

7、技术咨询电话：（0755）82083510（接入终端软件报备和使用咨询）

（0755）83182222（网络接入咨询）