PROP 系统接入安全技术指引

（结算参与人版　2011 年）

第一章　总则

第一条　为规范结算参与人（以下简称参与人）接入中国证券登记结算公司上海分公司（以下简称本公司）参与人远程操作平台（以下简称 PROP 系统），保障 PROP 系统运行安全，特制定本指引。

第二条　本指引适用于接入 PROP 系统的证券经营机构、托管银行、结算银行、基金管理公司等结算参与机构。

第二章　通讯链路安全

第三条　参与人应至少通过两条不同运营商的 SDH 通讯链路接入，保证 PROP 系统接入的网络带宽满足业务高峰期要求并具备一定的冗余空间。主用链路的带宽应保证可在半小时内完成历史峰值交易量下所有结算数据的下载，备用链路带宽不低于主用链路的 80%。

第四条　参与人应绘制与当前运行情况相符的网络拓扑结构图，有相应的网络配置表，包含设备 IP 地址等主要信息，与当前运行情况相符，并及时更新。

第五条　参与人应在 PROP 系统网络边界部署访问控制设备，启用访问控制功能，应能够对未通过准许私自连接到 PROP 网络的行

为进行检查。

第六条　参与人应对网络设备的管理员登录行为进行控制，应对网络设备的管理员登录地址进行限制，口令应有复杂度要求并至少每季度更换一次，应具有登录失败处理功能，当对网络设备进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。

第三章　主机安全

第七条　参与人应至少配备 PROP 生产网关机、本地备份网关机和异地备份网关机三套系统。

第八条　参与人应对网关机操作系统用户进行身份标识和鉴别，口令应有复杂度要求并至少每季度更换一次，应具有登录失败处理功能，当对网关机设备进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。

第九条　参与人应限制默认账户的访问权限，重命名操作系统默认账户，修改这些账户的默认口令；参与人应定期清理网关机操作系统用户，及时删除多余的、过期的用户，避免共享用户的存在。

第十条　网关机应专机专用，参与人应定期检查用户终端（含网关机）操作系统，遵循最小安装的原则，仅安装需要的组件和应用程序，并在经过充分的评估后对必要补丁进行及时更新。

第十一条　参与人应为用户终端（含网关机）安装恶意代码防

范软件，并确保恶意代码特征库得到及时更新。如用户终端（含网关机）发生恶意代码侵入现象，应立即中止接入，并尽快通知本公司。

第十二条　参与人应通过设定终端接入方式、网络地址范围等条件限制终端登录网关机，应根据安全策略设置登录终端（含网关机）的操作超时锁定。

第十三条　用户终端(含网关机)应实现与互联网的有效隔离。

第四章　应用与数据安全

第十四条　参与人可使用如下两种方式接入 PROP 系统:

（一）通过本公司正式发布的 PROP 客户端软件直接接入 PROP 系统;

（二） 通过本公司正式发布的 PROP 通用接口等接入软件间接接入 PROP 系统。

第十五条　参与人使用 PROP 通用接口接入 PROP 系统的，视同参与人已知悉和承诺下列使用规范和安全责任:

（一）严格按照本公司的要求管理和使用 PROP 通用接口系统，并由专人负责该系统的使用和维护。对于因操作不当而引起系统故障和不良后果由参与人承担全部责任。

（二）参与人对 PROP 通用接口的读写权限管理、访问安全控制以及安装通用接口的机器设备的安全管理承担全部责任。

（三）参与人向 PROP 通用接口提交的数据全部是真实有效和生

效的业务数据。

（四）对使用 PROP 通用接口的应用软件（包括参与人自主开发或第三方软件），应通过必要的、完备的系统测试。

第十六条　参与人负责自身应用数据的完整性、保密性和安全性，并定期进行备份。

第五章　用户及权限管理

第十七条　参与人应确保所有操作员接入 PROP 系统前均得到授权和批准，并根据最小权限原则为不同操作员分配权限，形成相互制约的关系。

第十八条　参与人 PROP 系统管理员和操作员用户的口令应有复杂度要求并至少每季度更换一次。

第十九条 参与人应定期清理 PROP 系统操作员用户，及时删除多余的、过期的用户，避免共享用户的存在。

第六章　密钥安全

第二十条　参与人必须使用本公司（或本公司授权的第三方）提供的加密设备，严禁在 PROP 系统中使用外来加密设备。

第二十一条　参与人应指派专人负责密钥的日常管理，备份密钥应独立保存，已经作废的密钥应由专人负责物理销毁。

第二十二条　参与人应严格控制的密钥的使用，未经许可，不得将密钥带出工作场所，不得将密钥送出维修。

第七章　安全运维管理

第二十三条　参与人应对接入 PROP 系统相关的网络、主机、应用系统与密钥分别指定专人负责管理，定义各管理人员的职责并对关键活动建立审批流程。

第二十四条　各管理人员应依据 PROP 系统用户手册对系统进行使用与维护，严禁进行未经授权的操作。

第二十五条　参与人应定期（每月至少一次）对 PROP 网关机备机的可用性进行检查，定期（每年至少两次）进行 PROP 网关机主备机切换测试。

第二十六条　参与人应对相关管理员与用户进行安全意识教育、岗位技能培训和相关安全技术培训，告知人员相关的安全责任和惩戒措施，并对违反安全策略和规定的人员进行惩戒。

第二十七条　参与人应指定人员对系统管理、维护与运行日志进行分析和处理，应及时向本公司报告所发现的 PROP 系统的安全弱点和可疑事件。任何情况下均不得利用该弱点进行危害 PROP 系统安全性的操作。

第二十八条　参与人应对涉及 PROP 应用的重要系统变更制定详细的变更方案、失败回退方案、专项应急预案。当参与人 PROP 系统接入链路发生变更时，应及时通知本公司。

第八章　应急处置

第二十九条　参与人应建立与本公司的应急联络机制，并通过PROP系统中的“联系人信息自助维护”功能向本公司提供和及时更新指定地及异地结算业务和技术应急联络人信息，联络信息应至少包括姓名、手机和E-Mail。

第三十条 参与人应针对接入PROP系统的物理环境、网络、主机、应用与数据等环节制订相应的应急预案，对相关人员进行应急处置培训，定期组织应急演练，并按要求参加本公司组织的应急演练。

第三十一条　当PROP接入链路发生故障时，参与人应尽快切换到备用链路使用，并向主用链路运营商报修。当PROP生产网关机发生故障时，参与人应尽快切换到备份网关机，并拨打PROP技术支持热线报修，联系电话为021-62321666。

第三十二条　对于参与人因技术系统或通讯线路故障而无法接收业务数据的，应立即与本公司系统运行部联系，联系电话为021-58889056。本公司将视情况采取临时允许使用PROP软证书、数据文件加密后Email发送或人工方式交换数据等应急措施。

第九章　附则

第三十三条　本指引由本公司负责解释。

第三十四条　本指引自发布之日起实施。