南京证券 IPv6 规模部署实践

（南京证券供稿 江苏局指导）

一、概述

为贯彻落实《中国人民银行 中国银行保险监督管理委员会 中国证券监督管理委员会关于金融行业贯彻<推进互联网协议第六版（IPv6）规模部署行动>的实施意见》（银发（2018）343号，以下简称《实施意见》）的相关要求，南京证券股份有限公司（以下简称公司）于2019年启动IPv6网络部署工作，总体工作根据公司实际采用分批次分阶段方式实施。2019年，公司在完成研究并制定IPv6改造技术方案的基础上，率先对互联网门户网站进行了IPv6网络和应用改造，并推动网站成功上线部署，通过基于IPv4/IPv6双栈模式，首批完成对公司及子公司门户网站的IPv6改造与部署，2020年完成面向公众服务的存量互联网应用系统的IPv6改造与部署，2021年完成面向公众服务的新增互联网应用系统IPv6改造与部署。截止目前，公司已完成多套应用系统IPv6改造与部署，实现了IPv6互联网接入线路具备不低于现有IPv4的安全防护能力，且IPv6各项指标均满足“证券期货行业IPv6规模部署情况专项摸排表”中的对应指标要求。

二、加强组织领导

公司对 IPv6 部署工作高度重视，以保障业务连续性为前提，加强 IPv6 规模部署工作的顶层设计，统筹规划，稳妥推进。该项工作由公司分管信息技术工作的总工程师、首席信息官负责领导；金融科技部作为牵头部门，负责 IPv6 规模部署工作的统一规划设计和改造推进；公司各相关部门、分支机构和子公司在金融科技部的统一指导下，负责本部门或本单位应用系统的 IPv6 改造和部署工作。在 IPv6 改造和部署工作推进过程中，公司领导组织各相关部门定期召开 IPv6 工作碰头会，讨论和研究 IPv6 改造计划、技术方案、协调工作过程中遇到的各类相关问题，有力保障了 IPv6 改造与部署工作的顺利开展。

三、落实责任机制

2019 年以来，公司梳理了所有面向公众提供互联网服务的应用系统清单，明确了各相关部门、分支机构和子公司的工作责任，并指定具体工作范围。2019 年起，公司按《实施意见》要求开始规划此专项工作，做好 IPv6 改造相关的年度预算，制定了详细的 IPv6 部署计划，确保 IPv6 部署工作责任到人，稳步推进。2020 年底，公司按计划完成了全部面向公众服务的互联信息系统的 IPv6 改造和部署工作，2021 年以来，公司对照“金融行业 IPv6 规模部署情况专项摸排表”及金融行业 IPv6 监测平台的监测指标，持续开展已完成 IPv6 改造的互联网应用系统的 IPv6 优化工作，进一步提升用户的 IPv6 访问体验。2021 年，公司完

成新增面向公众服务的互联网应用系统的 IPv6 改造与部署。根据监管要求，公司每季度按照“证券期货行业 IPv6 规模部署情况专项摸排表”进行专项摸排并完成监管报送，确保改造后的应用系统的 IPv6 指标符合表中的各项指标要求，并通过金融行业 IPv6 监测平台的线上监测评估。

三、预算资金保障

根据《实施意见》的相关要求，公司积极落实 IPv6 规模部署相关工作。公司在前期做好行业调研和基础设施状况摸底的基础上，充分进行 IPv6 改造技术论证，制定符合公司实际的 IPv6 改造与部署方案，合理规划分期分批实施步骤，并将 IPv6 改造项目的相关费用分别列入 2019-2021 年的每个年度预算方案中，在得到公司董事会及预算委员会审批通过后，按照规划分期分批投入改造费用。在专项资金的保障下，确保 IPv6 改造项目资金充裕，顺利推进并落实了 IPv6 规模部署工作。

四、技术实施方案

公司 IPv6 规模部署总体上采用 IPv4/IPv6 双栈模式，即采用对原在网的 IPv4 站点进行 IPv6 兼容性改造，并充分考虑改造后 IPv6 网络基础架构的标准化和通用性。IPv6 改造具体涉及到的网络与安全基础设施及相关工作，主要包括互联网接入线路、DNS 智能解析设施、负载均衡器、网络防火墙、IPS、Web 应用防火墙、三层交换机、网站主机、CDN 站点、网站应用系统及 IPv6 地址规划和 IPv6 特殊端口报备等多个方面。在互联网 IPv6 接入

线路方面，公司数据中心现有三大运营商（电信、联通和移动）共计数十条 IPv4 线路上同时开启了 IPv6 接入；在 DNS 域名解析设备方面，采用 IPv6 与 IPv4 共用智能 DNS 解析系统，并在智能 DNS 解析系统上配置互联网 IPv6 地址接入，分别为电信和联通 IPv6 线路，实现对 IPv4/IPv6 双栈的智能 DNS 解析，同时支持域名解析 A 记录和 AAAA 记录。

由于互联网应用系统底层所使用的网络与安全基础设施，以及操作系统、中间件等软件均为通用组件，本身已对 IPv6 协议支持较为完善，其 IPv6 改造具有与上层应用软件无关的特点，改造工作利于标准化。2019 年下半年开始，公司在完成网络与安全基础设施 IPv6 改造的基础上，后期重点推进互联网应用系统的应用层 IPv6 改造。公司前期经过技术分析，采用了"先测试-再确认-后改造"的模式，即在预先完成网络与安全基础设施 IPv6 改造的前提下，首先对所有面向公众服务的互联网应用系统，进行全面的应用软件 IPv6 兼容性测试，只在确认应用软件对 IPv6 兼容性存在问题的情况下，公司技术团队和软件开发商一起讨论并制定 IPv6 应用改造的技术方案，同时将该应用的 IPv6 改造列入计划。若应用软件通过全面的测试发现对 IPv6 已经具有较好的兼容性，则无需进行应用层内部 IPv6 改造，直接添加已 IPv6 支持的标识，并按照监管要求对其 IPv6 的各项技术指标进行测试评估。

五、IPv6 运维保障

公司统筹考虑应用系统和软硬件基础设施的 IPv6 改造实施，注重防范集中式改造升级引发的各类可能的安全生产风险。鉴于 IPv6 和 IPv4 网络在安全运维上存在差异，公司首先全面梳理出应用系统相关的软硬件基础设施 IPv6 支持情况并建立清单，根据实际情况推进 IPv6 改造和规模部署工作，并统筹兼顾各种应用系统的特点，分批实施。

在网络管理方面，公司通过修订网络安全管理办法、技术实施方案、应急响应、软件开发管理、监控运维等相关管理流程和制度，明确公司信息网络与应用系统必须支持 IPv6 协议相关要求，建立 IPv6 安全防护体系，并与 IPv4 一样，制定 IPv6 相关的总体安全策略，在工作实施细则中对 IPv6 安全提出明确的要求，进一步加强 IPv6 的安全管理。

在应急管理方面，公司在现有信息安全应急预案的基础上，针对 IPv6 改造实施制定了相应的应急预案，并在每年组织的相关应急演练中包含 IPv6 部分的演练。针对 IPv6 网络制定较为完备的业务连续性方案，并确保定期对相关的预案进行评估修订。确保现有的日志系统可以支持 IPv6 相关网络、系统和应用信息。

六、IPv6 人才建设

通过 IPv6 规模部署工作的开展，公司技术部门引导技术团队的每一位成员主动学习 IPv6 理论知识，积极与同业交流 IPv6 网络部署与运维经验，并参与技术讨论和方案验证等，为公司技

术团队提供一定的 IPv6 技术储备和经验积累，不仅可以进一步提高公司技术团队信息化 IPv6 网络升级改造的能力，还能提升团队成员分工协作、群力群策解决问题的能力。

七、存在的风险与问题

首先，IPv4 和 IPv6 是两种不同的 IP 协议，在技术原理、协议框架、网络配置、日常运维、地址规划等诸多方面，均需要技术团队及时更新知识，对 IPv6 网络的每一项变更操作，对数据中心网络安全来说是均可能存在不确定性的挑战。在 IPv6 改造与部署过程中，虽然技术人员能力和经验随着改造的不断深入而逐步提升，具体方案也是根据公司实际情况而定，但所改造系统上线运行后的负载压力并未显现，因此数据中心 IPv6 网络还需要经过大规模 IPv6 流量的全面考验。

其次，由于 IPv6 改造采用了 IPv6 和 IPv4 协议双栈模式，网络与安全设备需同时开启 IPv4 和 IPv6 协议流量的转发和相关的安全防护，且现网中网络与安全设备在建设之初，并未特别考虑过 IPv6 的性能需求，该模式对网络与安全设备的运行性能与稳定性都提出了较大的挑战；此外，目前市面上主流的网络与安全设备对 IPv6 流量的安全防护能力普遍没有 IPv4 相关技术成熟，且不能覆盖所有 IPv4 的安全防护场景，也未经过大规模生产网络部署的考验；技术团队对 IPv6 相关的安全和运维知识储备相比 IPv4 还存在不足。以上情况均可能对 IPv6 网络的安全稳定运行带来一些不确定性，存在一定程度的安全风险。

八、IPv6 下一步计划

公司将在继续做好面向公众服务的互联网应用系统 IPv6 改造基础上，持续推进互联网应用系统的 IPv6 规模部署工作，及时总结经验并完善方案，持续开展面向不同网络、不同应用和不同终端的 IPv6 升级改造工作，不断健全 IPv6 网络监控运维体系和完善网络安全管理制度与能力。

根据规划，公司下一步将基于 IPv4/IPv6 双栈模式，在保留其原有三层网络架构基础上，对数据中心内网区和骨干网络进行 IPv6 改造，并为确保原有网络稳定，采用独立核心骨干路由承载 IPv6 业务。在核心路由设备上开启 OSPFv3 动态路由协议同步 IPv6 路由，采用 VRRPv3 实现 IPv6 网关设备冗余备份，为后期纯 IPv6 网络提前夯实基础。后期将继续结合网络性能监控与流量回溯等技术手段，对改造后应用系统的 IPv6 指标进行全方位的健康侦测，确保公司的 IPv6 规模部署工作稳扎稳打，少走弯路。