# 无锡：筑牢财政信息安全防线

燕霞

2000年以来，无锡财政加快信息化建设，逐步实现了基础设施全贯通、业务软件全覆盖、IT管理全方位，信息化管理水平有了质的飞跃。但在享受信息化发展所带来的便利的同时，也面临着巨大的风险。特别是随着无锡市政务内网改造为政务外网，财政信息系统也随之迁移到政务外网，增加了网络安全风险。面对越来越复杂多变的网络安全威胁和攻击，保证财政信息系统的稳定运行以及数字资产的安全，已经成为财政信息化发展必须要妥善处理的第一要务。为此，无锡财政未雨绸缪，从加强信息安全整体规划入手，设计了“三位一体”的信息安全保障体系，提升财政信息安全防护能力。

## 信息安全存在的问题

一是安全制度亟需完善。缺少制度界定，就无法实现权责明晰化、行为规范化、奖惩有据化，信息安全难以落到实处。无锡财政前几年虽建立了一些信息化管理制度，但对照信息安全等级保护测评对信息安全制度方面的相关要求，仍存在着制度不健全、不完善的问题，信息安全制度建设尚未形成体系化。

二是安全技术有待提升。由于之前财政专网是依托政务内网而建，与互联网物理隔离，所以信息安全防护措施比较单一，安全设备往往仅依靠防火墙、漏洞扫描等设备，对全系统缺乏必要的技术监控手段，存在“管理黑洞”，导致系统管理人员很难细致全面地掌握网络中用户的行为，也难以对外来入侵风险进行有效识别。

三是安全管理仍要加强。各级财政部门对信息化重视程度不一，信息安全工作相对滞后，缺乏统一规划，各自为政；信息化专业队伍技术水平参差不齐，缺少既懂业务又懂信息化的复合型人才；业务操作人员、预算单位用户、县区财政部门的信息安全意识还比较薄弱，对安全管理的重视程度也不够，帐号转借他人、U盘在内外网间随意插拔、未经授权访问和违规操作等现象时有发生。

## 明确财政信息安全建设要求

1.建设原则。财政信息安全保障体系遵循以下建设原则：一是重点保护原则。根据信息系统的重要程度、业务特点，通过划分不同安全保护等级的信息系统，实现不同强度的安全保护，集中资源优先保护涉及核心业务或关键信息资产的信息系统。二是适度安全原则。任何信息系统都不能做到绝对的安全，过多的安全要求必将造成易用性降低和运行的复杂性，因此应在安全需求、安全风险和易用性之间进行平衡和折中。三是分步实施原则。根据信息安全需求紧迫性的顺序，规划信息安全建设的顺序，分布实施信息安全建设。

2.建设目标。以信息系统“三级”安全等要求为标准，构建“三位一体”的财政信息安全体系，从技术上对网络和信息系统进行及时监测及分析，让信息系统的使用有规可循、有据可查，保证整个操作流程清晰可控；保障各种网络资源稳定可靠、受控合法；保障数据在存储、传输、应用过程中的安全；从管理上建立和完善信息安全管理规范和机制。具体来说，就是从安全管理制度、安全管理机构、人员安全管理等方面进行管理体系建设；从物理安全、网络安全、主机安全、应用安全、数据安全等方面进行技术体系建设；从系统建设管理、系统运维管理等方面进行运行体系建设。

3.总体框架。无锡财政从信息安全管理体系、信息安全技术体系和信息安全运维体系三个方面着力构建“三位一体”的财政信息安全体系。

## 循序渐进实施

（一）安全域设计。根据目前无锡财政信息系统部署现状、业务需求以及安全保护要求，从信息系统业务相似性、资产相似性、安全需求相似性、所面临威胁相似性这4个维度，将信息系统划分为计算服务、网络互连、管理支撑三类安全域。

（二）构建信息安全模型。为了精确、形象地描述信息系统的安全属性，准确地描述安全与系统行为的关系，参考WPDRRC信息安全模型，从实际出发，综合考虑安全成本和风险级别，采用PDRR模型进行安全体系方案设计，即从P（保护能力）、D（检测能力）、R（响应能力）、R（恢复能力）四个环节明确应对措施。

（三）明确安全域安全要求。现阶段，单纯的依靠挖掘漏洞，填补漏洞的这种“封堵查杀”的被动式防范已经无法满足安全需求，只有采取主动式预防的措施，以先进的网络攻防技术作为信息安全的矛和盾，才能在信息安全防护上做到攻守兼备、游刃有余。所以，按照PDRR安全模型，针对不同的安全域，明确了网络和边界安全、计算环境安全、管理支撑安全三方面的具体要求。

（四）安全风险分析。对照“三级”安全等要求，从网络安全、主机安全、应用安全、数据安全、管理安全等方面，对财政信息系统进行全方位、多角度的问题排查，以便于信息安全体系建设中真正做到有的放矢。

## 安全解决方案设计

（一）细化管理，筑牢信息安全外围防线。俗话说：“三分技术，七分管理”。光靠信息安全技术（产品）很难实现信息安全的目标，加强信息安全管理才是信息安全的解决之道。组织机构方面，借助于“财政信息化管理工作机制”平台，成立“无锡市财政局信息化工作和网络安全领导小组”，下设办公室，由各处室的一名信息化联络员组成。通过完善组织架构，明确不同角色的定位、职责以及相互关系。人员安全方面，工作中大部分的信息安全控制需要依靠人的自我约束、自我控制和主观能动性。一方面积极开展信息安全宣传，不断加强工作人员的信息安全意识和安全防范意识；另一方面，通过组织各种技术培训，学习安全技能，提升信息安全工作的主动性。制度标准方面，结合相关信息系统安全等级保护要求，对涉及信息系统的各类活动、各个细节均做了明确规范，制定了《信息化工程（项目）施工管理制度》、《外部人员访问重要区域管理制度》、《网络安全管理制度》、《系统安全管理制度》、《安全监控和日志审计管理制度》等18个相关操作层制度。通过不断完善相关制度建设，织密信息安全防线，堵塞管理机制漏洞。

（二）强化技术，练好信息安全内在功夫。必要的安全设施、监控技术、防范策略、溯源手段是支持和保证财政信息安全体系顺利构建的钢筋铁骨。2016年开始无锡财政在充分利用现有资源的基础上，合理部署安全设备，对网络及核心系统进行统一管理和监控，以满足事前可预防、事中可控制、事后可审计的安全防护要求。网络安全方面，无锡财政已建成纵向广域财政专网（实现省、市、县区、乡镇四级财政网络的上下贯通），以及横向城域财政专网（实现国地税、银行、预算单位、非税单位的安全连通）。从过去以系统划分为导向的条线式构建模式，改变为以功能划分为导向的区域式构建模式。按照服务器区、外联区、内联区和安全管理区四个功能区域对现有的网络结构和层次进行调整优化，功能清晰，层次明了。系统和应用安全方面，将所有非核心应用部署在虚拟化平台上，既避免了服务器单点故障时引起业务中断，又实现了硬件设备的高可用。同时，将入侵检测系统、数据库审计、网络日志审计、堡垒机等安全产品有针对地部署在财政内网的各个功能区域，并根据管理要求配置了安全策略。可以严控用户操作、抵御恶意攻击、发生问题快速精确定位和溯源，全面保障财政业务安全。数据安全方面，无锡财政已建成了应用级、网络级和数据级的同城异地容灾备份系统。近几年，为解决现有存储资源无法互补共享、难以统一管理的问题，对财政灾备体系重新进行全局性的整体规划，率先探索采用存储虚拟化镜像技术组建同城异地双活数据中心。并将所有磁盘阵列纳入统一存储资源池，构建财政信息系统云存储平台，将核心系统及虚拟化平台均纳入双活数据中心。这样，即使在存储、网络或服务器任意故障情形下，核心系统及虚拟化平台上的应用服务都可做到业务不中断、数据零丢失，确保财政业务运转连续、稳定安全。

（三）优化运维，确保信息安全落地生根。一是运维管理制度化。通过明确信息系统建设者、使用者、运维者等各方的安全责任，从信息化项目设计规划、建设、交付到运行维护的全流程，都按照制度进行管理，做到“责任到人、有章可循”，确保风险隐患能得到控制和及时整改。二是运维内容明细化。根据技术关联性划分岗位职责，如网络管理岗、应用管理岗、资产管理岗、审计岗等，全面细致地定义每个岗位的运维内容，并针对每个岗位实行AB角制度。运维内容主要包括设备监控、安全策略管理、安全事件预警和通知、安全事件分析和响应、安全事件审计等。三是运维服务流程化。在行政办公系统中集成开发了信息化管理平台，创新性地设计实现了信息化管理工作的全程网上管理，实现了信息流、工作流、业务流的集成统一。建立了分类细致、规范高效的信息系统运维流程，通过流程化、自动化的运维服务加强制度化和标准化的落地，减少人为的矛盾，提高运维效率和质量。

（作者单位：江苏省无锡市财政局）

责任编辑 张蕊