

## 计算机联网审计组网模式的建立

廖志芳<sup>1</sup>, 樊晓平<sup>1</sup>, 谢岳山<sup>2</sup>, 杨 玺<sup>1</sup>, 张 恒<sup>1</sup>

(1. 中南大学 信息科学与工程学院, 湖南 长沙 410075; 2. 审计署长沙特派办, 湖南 长沙 410001)  
(zfliao@csu.edu.cn)

**摘 要:**在对众多被审计单位信息化环境及数据分布特征深入调研的基础上,提出了符合我国联网审计实际的三种新型联网审计组网模式,即集中式、分布式以及点到点式组网模式,并利用集中式海关联网审计组网模式对各组网模式的基本组成要素、需解决的关键问题及技术实现进行了深入阐述。该三种组网模式的构建涵盖了国家审计署审计范围内的大部分审计对象,并为联网审计提供了良好的网络平台。

**关键词:**联网审计;组网模式;集中式;分布式;点到点式

**中图分类号:** TP39 **文献标识码:** A

## Research on building audit-online network modes

LIAO Zhi-fang<sup>1</sup>, FAN Xiao-ping<sup>1</sup>, XIE Yue-shan<sup>2</sup>, YANG Xi<sup>1</sup>, ZHANG Hen<sup>1</sup>

(1. School of Information Science and Engineering, Central South University, Changsha Hunan 410075, China;

2. Changsha Resident Audit Office, National Audit Office of P. R. China, Changsha Hunan 410001, China)

**Abstract:** Three novel audit-online network modes which were introduced as central mode, distribute mode and point to point mode were presented according to the analysis on most ministries and commissions, especially on the informatic environment and the data storage methods. Then each mode was introduced in details, including the basic elements, the key problems and the implementation by using the example of CIQ central-mode audit-online network. As a result, the three modes provide an audit network platform for most ministries and commissions quite efficiently.

**Key words:** audit-online; network modes; central mode; distribute mode; P2P mode

计算机联网审计是借助计算机先进的数据处理技术、联网技术、计算机辅助审计软件以及大容量数据库技术,通过远程访问、调用被审计单位的相关电子数据资料来进行审计的一种方法。进行联网审计的前提是要建立良好的计算机联网审计平台,确定合适的联网审计组网模式,方便审计工作。联网审计组网模式主要是指在不影响被审计单位日常工作的情况下,采取合适的技术、方法和手段将被审计单位和审计单位进行联网,在线获取被审计单位数据的组网方法。由于被审计单位信息系统的布局、网络架构、系统结构等方面各不相同,因此对不同的单位采取什么样的组网模式以获取良好的联网审计 QoS,在不同的组网模式下采用何种网络拓扑结构以及在不同的拓扑结构下如何对被审计数据的进行采集、传输、存储以及安全保证等问题的解决方法,构成了计算机联网审计组网模式的主要研究内容。

### 1 计算机联网审计组网模式的选择

对于计算机联网审计系统的组网模式可以依据多种原则进行选择。如依据行业来进行组网,即将同一行业的单位组成一个行业审计专网,其优点是便于横向比较审计数据,可以更好地发现问题,但是存在比较大的数据安全问题;同样也可以通过地域进行组网,将处在同一地域的单位组成一个网络,其优点是便于数据传输,节省硬件费用,但是这种方法在数据管理上比较复杂,不便于数据处理;另外还可以通过数据采集

模式进行组网等,不同的出发点组网模式各有其优越性。但不论采取哪种方法都必须首先进行各个被审计单位的数据采集,因此在确定其组网模式前必须先清楚被审计单位的数据存储类型,并以此为基础来确定组网模式的选择。

#### 1.1 审计数据分布类型的确立

通过对被审计单位广泛的调研与分析,将被审计单位数据按照分布情况分成以下三种类型:

1) 全局集中式数据存储方式,指将本系统中的所有数据全部集中到一个或者少数几个数据中心,也就是所谓的数据大集中。比如工行系统,各地工行营业部将交易数据通过省总行数据中心网关,实时地传送到工行的南方或者北方数据中心,两个数据中心数据互为备份。在我国包括海关、建行、工行、中国银行等部门都已实现了全局的数据大集中。

2) 局部集中数据存储方式,指的是系统的数据存储是分层次的,其数据的存储包括一级、二级甚至多级存储。以农行为例,总行数据中心包含了部分的省行数据,而省行存储了省内各地市的数据。这是典型的二级数据存储方式。我国包括国税、部分商业银行、电信、移动等部门都属于局部数据存储方式。

3) 分散式数据存储,指的是单个单位自行进行数据存储方式的选择,没有与相对应的上级或者下级单位联网,而且在短时间内也没有相应的网络建设计划。这个部分的审计对象主要是国家各部委、大型的国有企业和政府外派单位,它们的

收稿日期:2005-10-20;修订日期:2006-01-13 基金项目:国家 863 计划资助项目(2003AA1Z2330)

**作者简介:**廖志芳(1968-),女,湖南长沙人,副教授,主要研究方向:系统集成、数据挖掘; 樊晓平(1961-),男,浙江绍兴人,教授,博士生导师,主要研究方向:智能信息处理系统、信号处理; 谢岳山(1965-),男,湖南长沙人,高级审计师,主要研究方向:计算机联网审计; 杨玺(1984-),女,江西南昌人,博士研究生,主要研究方向:通信网络、语音处理; 张恒(1983-),男,湖北孝感人,博士研究生,主要研究方向:智能数据处理。

数据特点就是各自独有。

## 1.2 组网模式的选择

从审计数据采集的方便程度看,按照数据存储模式进行组网为最佳。因此在组网模式的确立上,将根据对被审计单位的审计要求,依据不同的数据存储模式,确定数据采集方式以及数据传输方式,来组成不同的联网审计模式。

根据所定义的三种数据存储类型,确定了相对应的三种组网模式:

1) 对于全局集中数据分布类型,通过单一数据采集点的设置,就可以采集到审计所需要的全部数据,称之为集中式组网模式。

2) 对于局部数据分布类型,其数据采集点的设置是分层结构,可能有一级数据采集点,二级数据采集点甚至于多级数据采集点,通过这多级数据采集点才能采集到审计需要的所有数据,称之为分布式组网模式。

3) 对于分散式数据分布类型,其单位的独立性较强,审计所需要的数据可以在一个单位内就可以采集到,称之为点对点的组网模式。

对于审计署所辖的被审计单位,按照数据存储方式都可以按照相应的组网模式联入审计署,进行相关审计。而且按照信息化程度的提高,这三种模式可以进行转换,如分布式组网模式转换为集中式组网模式,因此这三种组网模式的确立涵盖了所有的下属被审计单位。

## 1.3 系统结构

上述三种组网模式要进行完整的联网审计都必须完成以下的工作:首先从被审计单位提取审计数据,经过通信传输将数据传输到审计端并进行存储以及相关处理。将这三个工作过程定义为数据采集、数据传输以及数据存储部分,因此联网审计系统组网模式逻辑结构设计主要包括这三个部分,除此以外还必须要考虑系统的安全设计。

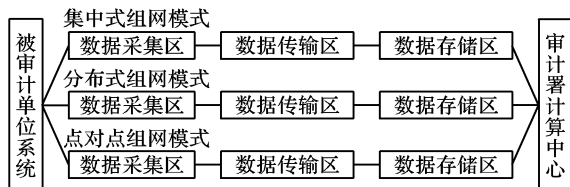


图1 联网审计组网总体框架

综上所述,可以将审计组网的总体框架归纳为图1所示,其总体框架主要由三部分组成:图1左边部分为对被审计单位的数据采集,中间部分表示采集数据的传输,右边部分表示数据在审计署的存储处理。以海关系统为例对联网审计组网模式进行详细说明。

## 2 集中式联网审计组网模式实例

海关系统为全国联网,其数据存储为数据大集中方式,也就是所定义的全局集中的数据存储方式,因此其组网模式为集中式组网模式。按照审计流程,将海关集中式组网模式的组成定义为:被审计端数据采集局域网,数据传输局域网以及审计端数据存储局域网。

### 2.1 被审计端数据采集局域网

#### 2.1.1 数据采集方式的确立

数据采集是各种联网审计组网模式中一个重要初始环节,它为联网审计所提供的初始数据的好坏直接影响到审计的成功与否。该部分的主要功能是将被审计单位的数据(例如财务报表、总账数据等)按照一定的审计要求和计划,导入到审计部门的数据系统中,并经过整理和转化,形成便于审计

人员分析和查询的数据格式。这部分需解决的关键问题包括数据采集点的确定,数据采集方式以及安全性措施。数据采集主要采用两种方法,即使用数据采集机和不使用数据采集机。

采用数据采集机的方式是将相关设备设置为数据采集机,放置在被审计单位局域网内,定时地从被审计单位原始数据库中提取与审计相关的审计增量数据,存放在数据采集机本地数据库中,并定时将所采集的审计数据通过数据传输局域网传输到审计署数据中心。这种方法的特点是降低了被审计单位数据安全风险,降低了对网络性能的要求,同时节约了网络资源以及审计数据中心存储空间。该方法可以适用于三种组网模式。

而不采用数据采集机的方式主要集中在数据量小的单位,该方法可以是利用相关设备直接将被审计单位原始数据库不经转换,通过网络完全传输到审计网内数据中心进行数据存储,审计署直接对这些数据进行计算机审计。或者不进行数据传输,审计人员通过审计网络,直接对被审计单位数据库进行审计。这种方法的特点是组网简单,成本较低,但是数据安全风险大,一般这种方法适用于小数据量的对安全要求不是很高的被审计单位。

由于海关采取的是数据大集中存储方式,其系统数据主要集中在南北两个数据中心的,并且数据互为备份,因此其审计数据可全部从任一数据中心获取,考虑到海关数据量巨大,采取了在海关数据中心设置数据采集前置机的方式进行数据采集。

#### 2.1.2 海关被审计端局域网

考虑到网络容灾问题,分别在北方数据中心以及南方数据中心设立了数据采集点,但是以其中的一个为主采集点,另外一个作为备份,一旦主采集点出现故障,其备份采集点将进行工作,这样来保证数据采集的实时性,完备性与安全性。本次数据采集的组网模式是相似的,其结构均如图2所示。利用一台微型服务器作为数据采集机,通过物理开关直接连接海关数据中心。物理开关为自主设计的单刀双置开关,在进行数据采集时,开关打向海关数据中心,在进行数据传输时,开关打向审计署数据中心,以此保证海关数据中心和外界的物理隔离。数据采集完毕,通过交换机、防火墙以及路由器进行数据传输。同时本地审计人员也可以在数据采集局域网中进行实地审计。

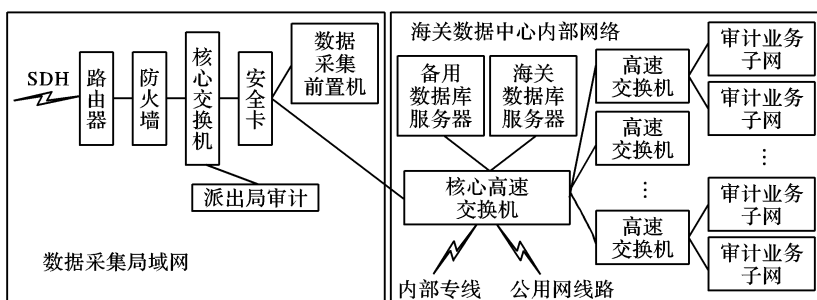


图2 数据采集组网模式

## 2.2 数据传输

### 2.2.1 数据传输方式的选择

经过数据采集后,需要将所采集的审计数据传输到相应的审计数据中心内,这部分工作将由数据传输完成。该部分的主要功能包括建立审计单位服务器与被审计单位组网中的前置机的线路对接、身份认证、数据加密和解密、传输控制以及实时通讯等,其目的是建立一条安全可靠、稳定通畅的数据传输通道,保证审计数据传输的保密性和高效性。大数据量的数据传输可以采用多种方式进行传输,其中比较典型的包括DDN、ATM、SDH、X.25及FR等方式。在集中式组网模

式中,由于数据传输方式要与国家电子政务系统中的应用相吻合,因此数据传输方式采用 SDH 方式。分布式组网模式数据传输相对复杂,考虑到其具有多级数据采集点的特点,不同级别数据采集的数据传输方式可能不同。对一级数据采集点所采集的数据可以采用 DDN、ATM 及 SDH 等方式传输到审计署数据中心,对二级数据采集点所采集的数据可以采用 ADSL、ISDN、DDN、ATM 及 SDH 等方式传输到审计特派办数据中心,然后利用审计内网将数据传输至审计署数据中心。而对低级的数据采集点应该根据情况采用相适应的多种方式进行数据传输,如拨号、租用线路等。对于点对点组网模式,由于被审计单位的多样性,具体的数据传输网络选择差异很大,所以在该部分的设计时要考虑所有可能的情况。

### 2.2.2 海关数据传输局域网

在海关联网审计组网模式中,由于海关数据传输量巨大而且对实时审计的发展要求很高,另外也由于国家电子政务平台的通信基础线路为 SDH 光通信专线,因此在数据传输中采用 SDH 作为连接审计单位到海关数据中心的数据传输线路。

### 2.3 审计端数据存储局域网

#### 2.3.1 审计端数据存储方式

数据存储是联网审计组网模式中的一个重要环节,它为联网审计提供初始数据的处理和存储方案,其好坏不仅仅影响到审计的成功与否,而且直接关系到国家的信息安全。因此,这部分的设计主要考虑数据存储方式、数据库服务器对于海量数据的访问与存储的速度、稳定性要求以及数据的安全性要求。该局域网将接收被审计单位不同格式的数据并按照一定的审计要求和计划进行整理及转化,以形成相对统一的数据格式。在数据存储的设计中,无论是哪种组网模式其存储方式是一致的,经过分析决定采取 SAN 进行数据的存储,其构架主要包括群集服务器、光交换设备和数据分区管理设备、数据存储磁盘阵列。

由于审计数据是从不同部门、不同地点采集而来的,而且这些数据的目的、处理方式有所差异,为了提高数据存储的效率,必须采用存储介质分区的方法,将海量数据存储到不同的介质区域中。一般对数据分区的方法有两种:第一种是按照应用来分,就是将不同部门的数据采集到一起,例如国家工商总局的数据集中放在某个区域中,海关总署的数据集中存放在某个区域中。第二种是按照数据特征来分,就是按照数据的特征类型进行分区,例如将刚刚采集得到的原始数据存放在一个区域中,已经处理完毕的数据存放在另外一个区域中。

在联网审计组网模式数据存储方案设计中,将采用两种分区方法结合的办法,首先按照应用进行划分,然后在应用内部按照数据特征进行划分,这样能够保证单个应用的访问速度,又能够使整个系统逻辑清楚,管理方便。

#### 2.3.2 海关联网审计审计端数据存储局域网

审计端数据存储局域网由两部分组成(图3),上面一部分是审计署中心内部网络,下面一部分是联网审计数据存储局域网;图中存储局域网主要由光纤通道交换机、本地磁盘阵列、备份磁带库及远程容灾磁盘阵列组成 SAN 系统,建立一个可扩展、易管理、能够灵活地适应不可预见的存储需要的网络存储环境。传输线路采用双线路备份的方式,两个数据库服务器系统只有一条线路能够接入中心内部网络,但各有一条线路接出审计网络中心;局域网内设两块硬件防火墙,分

别用于两条审计数据输出的线路上,以保证数据传输的安全性。海关审计数据存储在其中某一个应用服务器中,并根据需要进行相关备份,保证数据的完整性。

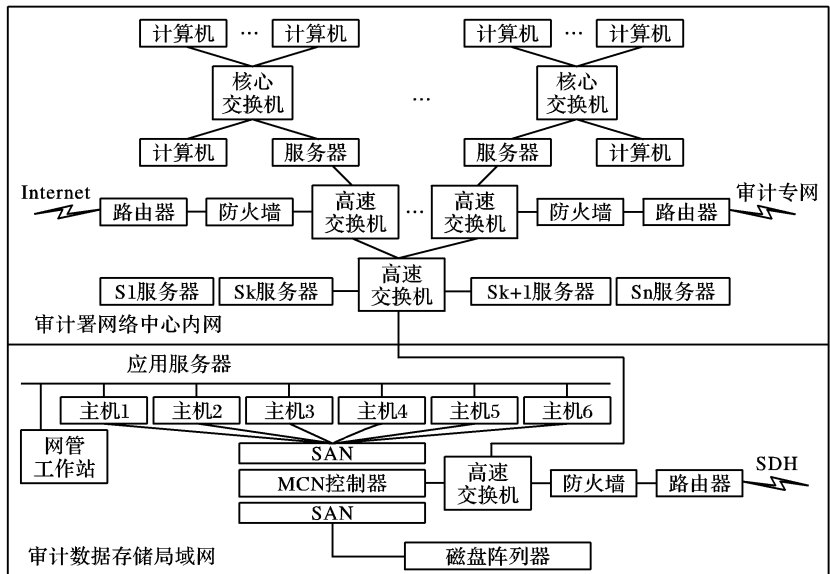


图3 审计端数据存储局域网

### 2.4 系统安全性设计

安全设计主要包括数据采集安全设计、数据传输安全设计和审计数据存储的安全设计。其中数据采集安全设计主要采用了数据采集物理安全卡、审计数据采集身份认证与授权、审计数据采集冗余设计以及审计数据完备性设计等来保证这部分的安全。数据传输主要采用信息传输加密,传输通道加密以及VPN等相关技术来保证其安全性,审计数据存储安全设计主要是要保证审计数据的连续性、共享性和可使用性,同时要保证审计署内外数据的安全隔离。利用SAN专门为审计数据建立了单独的联网审计数据库,以此和审计署本身内部数据库系统隔离。各个审计数据分别存储在不同的数据服务器,并保证数据至少有一个备份。因此在出现故障的情况下,可以保证审计数据的持续工作。同时还可以通过划分区域、各个区域加密保护、审计人员授权以及身份认证和对数据操作的限定等措施,保证只有被授权的审计人员才能调用审计数据。

## 3 结语

本文提出了符合我国联网审计实际的三种组网模式,并以海关集中式联网审计模式为例,对各组网模式基本要素及技术实现的研究成果进行了深入阐述。这三种组网模式的设计涵盖了审计署审计范围内的大部分审计对象,包括金融、海关、国税、国家各部委、大型国有企业、科研院所、高校等;不同的组网模式适用于不同的审计对象。同时这三种组网模式的设计提供了异地审计的平台,使得审计工作更灵活方便。本文的部分研究成果目前已在联网审计试点环境中得到应用。

#### 参考文献:

- [1] 陈峰,董永强. 联网审计模式初探[J]. 中国审计, 2003, (5): 63 - 64.
- [2] 潘立亚. 互联网时代审计新概念: 网络审计[J]. 经济师, 2004, (3): 229 - 229.
- [3] CANCELA H, ROBLEDO F. Gerardo Rubino Network design with node connectivity constraints[A]. Proceedings of the 2003 IFIP/ACM Latin America conference on Towards a Latin American agenda for network research[C]. 2003.
- [4] 张悠慧, 郑邦民. 基于网络附属对象设备的集群存储体系结构[J]. 软件学报, 2003, 14(2).