“智慧政务”通用架构设计的研究
——以A市“智慧政务”平台建设为例

许兴　陈亚成　宋艳　马威　郭竹媛
扬州疾病预防控制中心　江苏　扬州　225002

[摘　要]随着信息化发展、高质量发展的内在驱动，各地方政府陆续新建“智慧政务”平台，实现服务百姓和城市精细化治理的功能。本文将以A市政府“智慧政务”平台建设为例，重点阐述大数据中心、视频共享平台的架构设计，力求从中总结出通用的设计方案，为其他地方政府“智慧政务”建设提供参考。

[关键词]大数据中心；视频共享平台
【DOI】10.12252/j.issn.2096-627X.2021.08.291

1 背景

“智慧政务”是“大平台协同、大数据应用”理念在A市政府的落地，立足A市政府高质量发展的实际需要，满足服务A市政府百姓和城市精细化治理要求，以信息资源整合为手段，以大数据平台为支撑，以大数据治理为核心，促进跨层级、跨系统、跨部门、跨业务的协同管理和服务。通过打造“智慧A市政府一朵云、智慧应用五领域（民生幸福、城市治理、生态文明、产业协同、乡村振兴）、城市管理一中心”的 “151”工程体系，实现A市政府 “创新网格一张网、数据资源一中心、感知设施一主线、应用支撑一朵云、时空数据一张图、移动服务一终端、联动指挥一平台、标准规范一体系、信息安全一标准、运维管理一机制”，让A市政府社会治理更高效、A市政府百姓生活更智能。

2 大数据中心架构设计

2.1 总体架构设计

A市政府大数据中心物理上分为互联网区、公用网区2个区域。

（1）互联网区：承载直接面向互联网用户的业务系统资源区，提供面向公众的访问能力。

（2）公用网区：承载各委办局政务业务系统，如社会治理、智慧水利、智慧工地等业务系统。

2.2 网络架构设计

2.2.1 设计思路

A市政府大数据中心网络架构的总体规划需要遵循安全、可靠的设计理念。针对公用网和互联网的不同网络安全需求、数据中心内管理平面的安全隔离需求，采用“分区+分平面”架构，即从业务应用来看将数据中心平台区划分为公用网区和互联网区；从数据中心管理来看将数据中心内部划分为管理平面、业务平面、存储平面。使网络层次更加清楚、网络性能更优化，网络架构更加可靠。

（1）安全性：

网络架构设计需满足安全等保三级要求，针对A市政府大

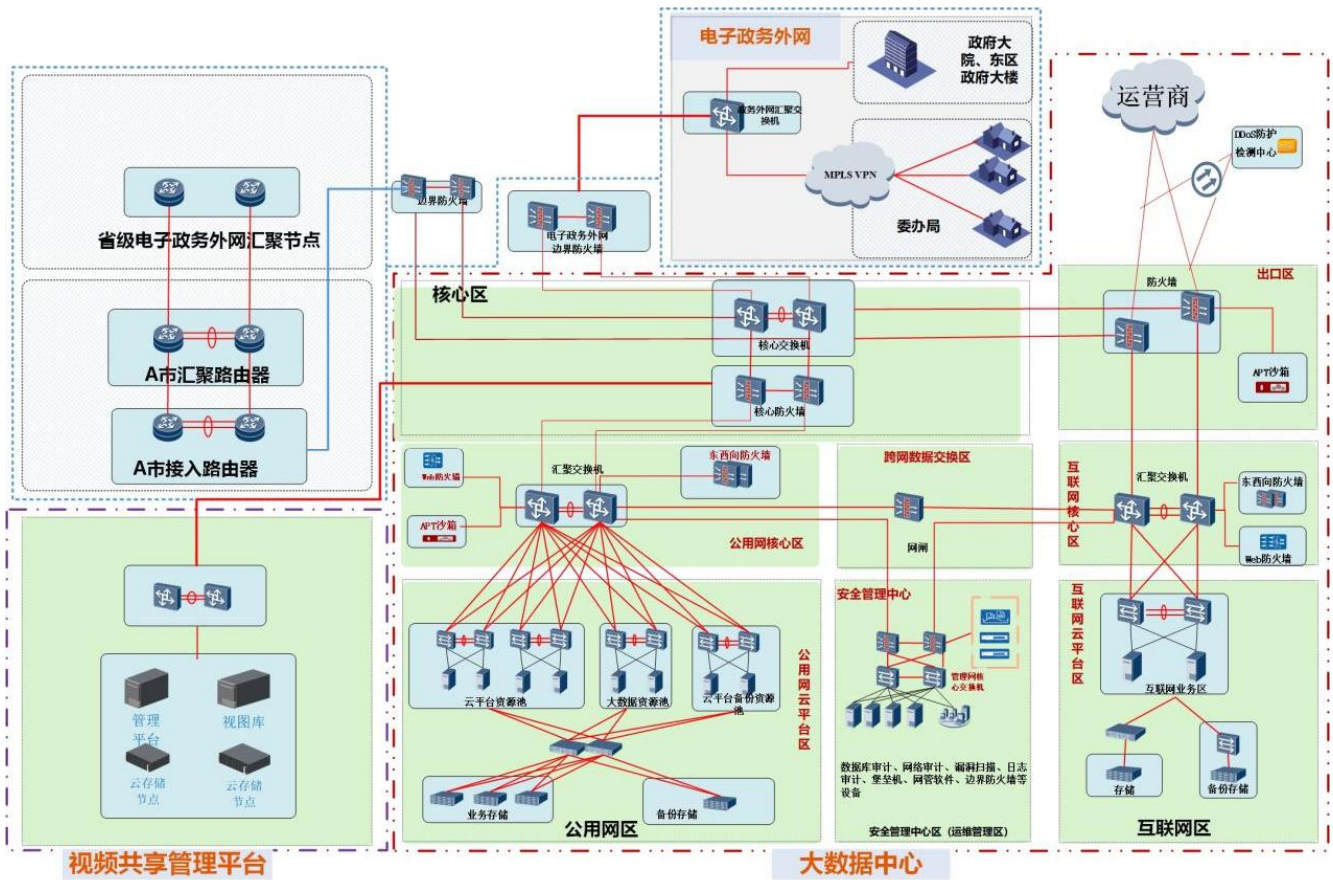

图1 大数据中心网络架构图

数据中心外部网络的不同安全需求，一方面防范来自Internet的各类安全威胁，另一方面提供各委办用户政务类业务安全隔离的诉求。将数据中心划分为两个独立的业务区域：互联网区和公用网区。

针对数据中心内部网络划分为管理、业务、存储三平面，三平面独立组网，物理隔离，使整个A市政府大数据中心的架构具备伸缩性和灵活性，同时也便于安全域的划分和安全防护的设计实施。

（2）可靠性：

A市政府大数据中心结构化设计可靠性体现在设备可靠性、网络冗余性以及业务容灾性设计。从网络设备来看，核心节点交换机具备工业级的超高可靠性，支持不中断业务软件升级，满足用户业务的永续性需求；交换机、防火墙主控板、交换网板、电源、风扇灯关键部件全冗余，所有模块支持热插拔；设备控制平面、数据平面、监控平面完全隔离，提高系统可靠性。

从网络架构来看，A市政府大数据中心网络可靠性设计体现在适当的冗余性和网络的对称性，采用双节点双归属的架构实现网络结构的冗余和对称。核心/接入交换机采用虚拟集群技术，2台设备冗余部署；防火墙采用成对部署，采用双机热备技术，所有表项、会话实时同步；所有连接链路采用链路捆绑，大大提升网络可靠性。

2.2.2 总体网络

A市政府大数据中心网络方案设计遵循高可靠性、高安全性原则，整体网络架构如下：

A市政府大数据中心的网络设计采用分区+分平面原则，根据业务系统情况将数据中心内部网络划分核心区、互联网区、公用网区、安全管理区和跨网数据交换区。

针对政务业务高安全性要求，区别处理公用网与互联网业务的不同安全威胁，互联网区通过高速链路连接互联网出口区，公用网区通过高速链路连接市政务外网，满足各委办局业务接入公用网与互联网的需求，当互联网区和公用网区数据业务发生交互时，通过跨网数据安全交换区进行交互。

同时，在云平台内部将管理、业务、存储平面完全隔离，各自通过独立交换机组网，避免了各类网络之间的竞争和由此产生的拥塞，有效提升了网络的性能。

2.2.3 核心区网络设计

核心区作为整个A市政府区大数据中心的核心区域，负责全A市政府区电子政务业务流量转发，对于核心设备的性能、稳定性要求极高，故本次配置了2台高性能核心交换机，以A市政府区核心交换机为整个A市政府大数据中心的核心区域，按照上下分别接入不同的网络：

（1）向上

A市政府区核心交换机通过边界防火墙和A市政府区电子政务外网互联互通，满足A市政府区各委办局的安全接入。

（2）向下

部署安全管理中心，和互联网、公用网区的汇聚交换机互联互通，实现对2个区域网络设备的安全管理运维。

（3）向左

A市政府区核心交换机通过出口网关设备，和互联网区、互联网网络实现互联互通，一方面统一A市政府区各委办局、各镇（街道）、园区、村（社区）的互联网出口，另一方面满足其互联网区业务应用的安全访问。

（4）向右

A市政府区核心交换机通过边界防火墙设备，和公用网区、省级政务外网实现互联互通，一方面满足A市政府区各委办局、各镇（街道）、园区、村（社区）接入到省级政务外网，另一方面满足省级政务云对A市政府区大数据中心资源的调取和查阅。

2.2.4 公用网区网络设计

公用网区用于部署政府职能业务，并提供各委办局政务网络的接入，满足政府各部门协同共享办公的需求。

本次公用网区网络采用核心+接入的二层扁平化网络架构，二层扁平化的网络架构可以实现：

核心区用于数据流量的高速转发，网络设计说明如下：

（1）部署两台公用网汇聚交换机之间采用双机虚拟化协议堆叠成一台逻辑主机，达到性能翻倍与相互备份的效果。千兆链路旁路部署东西向隔离防火墙、Web应用防火墙和APT沙箱等安全设备。

（2）与A市政府区核心交换机通过万兆防火墙双链路互联互通，实现公用网区资源安全接入到A市市电子政务外网中，满足省级电子政务对A市政府区政务数据的调取和使用，同时可供A市政府区委办局的安全访问。

（3）部署多台服务器接入交换机，两两一组绑定成双机虚拟机化，两个逻辑交换机通过链路绑定与核心交换机互联，达到设备和链路的性能翻倍，互为备份的效果，为各类信息系统提供不间断计算平台业务支撑。采用双40GE链路上行到公用网区核心交换机。下行采用10GE链路供服务器、存储等设备的接入。

2.2.5 互联网区网络设计

互联网区部署一些面向公共的业务。对于该区域，要进行足够的安全设施部署。互联网区网络说明如下：

（1）互联网核心区：

部署两台互联网汇聚交换机之间采用双机虚拟化协议堆叠成一台逻辑主机，达到性能翻倍与相互备份的效果。千兆链路旁路部署东西向隔离防火墙、Web应用防火墙等安全设备。

（2）互联网云平台区：

部署服务器、存储接入交换机，两两一组绑定成双机虚拟机化，两个逻辑交换机通过链路绑定与核心交换机互联，达到设备和链路的性能翻倍，互为备份的效果，为部署在互联网上的业务系统提供不间断计算平台业务支撑。采用双40GE链路上行到核心交换机。下行采用10GE链路供服务器、存储等设备的接入。

（3）出口区：

部署2台出口安全网关，向上租用运营商链路接入到互联网，向下双万兆链路和互联网汇聚交换机对接，满足互联网区业务的对外发布；向左双千兆链路和A市政府区核心交换机互联，作为A市政府区下属区委办局、区政府大楼的互联网的统一出口。出口安全网关主要实现NAT功能，并提供应用层的安全过滤。同时设备上开启防病毒功能，实现安全区域隔离和访问控制。另外也作为互联网接入用户（手机或PC）的VPN网关，完成从移动人员互联网到公用网的准入。

部署1套防DDos流量攻击设备，负责针对DDos流量的检测和过滤，通过分光器千兆链路旁挂在出口链路上。通过运用大数据分析技术，针对60多种网络流量进行抽象建模，秒级攻击响应速度和超百种攻击的全面防御。

部署一台安全沙箱设备，针对来自互联网的未知威胁攻击进行防护，千兆链路旁挂在防火墙上。

部署一台Web应用防火墙设备，对面向互联网的网站进行安全防护，千兆链路旁挂在防火墙上。

2.2.6 安全管理中心区设计

按照《信息安全技术网络安全等级保护基本要求》第三

级安全要求，设置安全管理中心，可以准确了解系统的运行状态、设备的运行情况，统一部署安全策略。从系统管理、审计管理、安全管理、集中管控4个维度进行设计。安全管理中心说明如下：

本次A市政府大数据中心项目中，数据中心内部所有主机、管理数据中心内部所有主机、服务器、网络设备、存储设备都会通过BMC管理网口上联到BMC管理交换机上。公用网区、互联网区的通过不同的BMC管理交换机汇聚后，接入到A市政府大数据中心的安全管理中心，实现互联网区、公用网区的管理实现隔离，部署统一网管平台对数据中心内服务器、存储、网络设备等进行管理。本次部署设备如下：

（1）部署日志审计设备：统一收集设备日志，对网络中发生的任何信息进行集中式存储，做到有源可溯。

（2）部署数据库审计设备：对本地数据中心的数据库访问行为进行严格的记录和管控。

（3）部署运维堡垒机：对安全审计员进行严格的身份鉴别，并只允许其通过特定的命令或界面进行安全审计操作。

（4）部署漏洞扫描：通过深度主机服务探测、Web智能化爬虫、SQL注入状态检测、主机配置检查以及弱口令检查等技术，提供Web漏洞扫描、系统漏洞扫描、数据库漏洞扫描、基线安全检查与口令猜解的功能。

（5）部署网络管理软件系统：对系统的资源和运行进行配置、控制和管理。

（6）部署云安全资源池，采用SDN与服务链技术的结合，安全控制器可实现网络、安全资源的一体化管理与调度，云租户部署所需的安全资源分配、业务流量调度、安全策略部署得以集中交付，轻松实现安全业务的自动化部署。

（7）部署态势感知控制平台，采用最新大数据分析和机器学习技术，用于抵御APT攻击。它从海量数据中提取关键信息，通过多维度风险评估，采用大数据分析方法关联单点异常行为，从而还原出APT攻击链，准确识别和防御APT攻击；同时威胁联动安全设备、终端设备处置闭环，云端信誉共享，做到安全态势实时感知，PB级数据秒级检索溯源，避免核心信息资产损失。

（8）部署云平台业务流实时分析系统，基于大数据分析技术，为用户提供无处不在的网络应用分析与可视化呈现，打通应用和网络的边界。通过Telemetry技术采集海量真实业务报文，提供数据中心内部应用和网络的关联分析，实时呈现应用地图及网络质量，快速识别故障，并在业务产生影响前主动识别风险。

（9）部署数据安全管理平台，实现对数据进行脱敏、加密、水印等安全保障功能。

3 视频共享平台架构设计

3.1 总体架构设计

按照A市政府要求，把现代化的智能手段引入城市管理，将城市各个管理区块都要纳入信息化管理的范畴；同时强化智能监控和信息化手段的运用，实现动态化、全覆盖、无死角的有效管理。

“智慧政务”视频共享平台的建设，通过进一步利用视频联网技术，提升社会治理水平，更好地服务A市政府百姓。通过加强对数据、信息的管理与分析，通过信息化，将互联网技术渗透到社会治理的方方面面，从而提高政府服务百姓、社会治理等方面的效率。

视频共享平台系统是以开放式视频云架构为基础，以A市政府公安视频专网为核心进行资源整合；同时通过技术手段连通公安视频专网、互联网、政务外网，在满足高安全性要求和网络带宽承载能力的同时，能够做到不同网络的视频和数据，统一汇聚到A市政府公安视频专网，实现对所有视频资源和结构化信息的统一接入和存储，为A市政府政务网共享平台提供视频、图片、数据等基础信息服务。此外，本次政务网新建的平台除具备弹性扩容能力以外，还具备集成开放能力，满足各部委办局的实际应用需求。

3.2 详细架构设计

3.2.1 系统架构设计

（1）视频接入层

视频接入层主要是全区的视频前端，包括公安一类视频资源、政府部门和社会面的二三类视频资源等，并充分利用运营商资源通过专线和互联网资源进行整合。

视频接入层除了整合已建视频资源，还需汇聚以公安、水利、社会治理、校园、工地等应用为主的人脸抓拍、车辆抓拍、智能识别等智能化资源。为后端提供数据来源支撑。

（2）视频管理层

视频管理层主要涉及对于前段采集来的数据进行存储，分析以及数据碰撞等。本次建设中，需要强化视频图像汇聚、分析、处理和管理能力，加强对视频图像解析服务、视频图像行业应用以及运营指挥等系统的支撑

（3）应用层

视频应用层基于API网关提供的视频基础服务、大数据分析服务、智能解析服务，为政府用户提供基础通用应用和业务专用应用。同时，视频应用层根据不同的应用场景分别提供Web应用门户、客户端应用门户以及移动应用门户。

3.2.3 网络架构设计

主要涉及互联网、公安视频专网、电子政务网三网内的资源，横向打通，实现三网内三套平台数据的汇聚、共享以及应用。

（1）互联网社会面资源接入平台

互联网平台主要用于汇聚无法直接接入公安视频专网的视频资源或者已部署在互联网的设备，此类设备可通过互联网链路接入到互联网接入平台，互联网接入平台在通过安全边界，与A市公安局视频专网平台实现上下级联，以补充视频专网资源接入的盲区。

（2）A市政府公安视频专网共享平台

A市政府公安分局视频专网共享平台主要用于汇聚各部委办局的数据信息，包括视频数据、卡口数据、人脸数据。实现对于数据的统一管控。同时，A市政府公安会通过安全边界，将数据共享到电子政务网平台，以供各部委办局对于数据的调阅。

（3）A市政府政务网视频共享平台

在A市政府政务网内建设A市政府政务网视频共享平台，主要利用A市政府视频专网推送过来的数据，在政务网内实现数据的整理汇总，实现可视化展示。并且可以根据个业务部门的需求进行统一的视频资源管控。

4 结语

本文根据A市“智慧政务”平台建设实践，总结出地市级“智慧政务”平台的通用设计，细化为大数据中心、视频共享两大平台设计，为其他地方政府“智慧政务”建设提供参考。

本文结合各地方政府普遍需求，分解为大数据中心、视频共享平台两方面阐述，其中大数据中心设计按照“集约高效、共享开放、安全可控、按需服务”的原则，以“云网合一、云数联动”为构架，通过构建弹性灵活的计算资源池和存储资源池，以高性能计算能力和大规模共享存储的基础，面向地市政府各部门提供云计算、云存储、云安全等服务，实现各部门基

础设施共建共用、信息系统整体部署、业务应用有效协同，为政府的公共服务提供有力支持，提高为民服务水平，提升政府现代治理能力，夯实信息化基础设施；同时视频共享平台设计以公共安全视频监控建设应用为核心，统筹共建并整合城管、公安、生态、水利、综治等政府视频监控资源和社会化视频监控资源，提升公安、交通、城管、生态、自然资源、水利、教体等部门在动态化、信息化条件下的预警预测、综合防控、视频侦查、现场处置和指挥保障能力，为跨地区、跨部门信息共享提供全景式视频信息服务，为应急指挥、城市管理、社会治理提供可视化信息支撑，构建核心支撑能力。

参考文献

[1]中国国家标准化管理委员会，GB/T 21061-2007 电子政务网络技术和运行管理规范，2011-01-21，中国标准出版社

[2]胡广伟，司文峰，市级政府智慧政务之路——“互联网+政务服务”应用实践，2019-10-01，科学出版社

[3]张毅，政务大数据应用方法与实践，2021-07-01，中信出版社

[4]中国行政体制改革研究会，数字政府建设，2021-05，人民出版社

[5]沈大风，电子政务发展前沿，2014-06-01，中国经济出版社

作者简介:

许兴（1985-），男，江苏扬州人，工程师，硕士；研究方向：卫生信息化。

通讯作者：陈亚成（1990-），男，江苏扬州人，助理工程师，学士；研究方向：卫生信息运维。

（上接第451页）

处理措施：（1）加强地下水的监测，加强对抽水时含砂率的控制，以免过度降水；（2）引孔时加强管理，减少钻孔中造成的扰动；（3）引孔作业与沉桩施工密切配合，随引随沉，并在同一台班完成；（4）对引孔中出现的塌孔范围及时进行回填。

2.部分沉桩长度不足设计要求

在现场管桩施工时，部分桩沉桩最后三阵贯入度达到要求，直至部分桩出现爆桩情况下，沉桩长度仍不能满足设计最小长度 12m 的要求。原因分析：（1）勘探资料不够详细，对工程地质情况不明；（2）勘探工作是以点带面，对局部硬夹层不可能全部了解清楚，尤其在复杂的工程地质条件下。

处理措施：（1）在问题管桩附近补桩，但仍有补桩不满足长度要求；（2）对长度不足的桩增加进行桩基检测，后续检测表明承载力及桩身完整性均满足设计要求；（3）后续沉桩施工时加长引孔长度，保证引孔穿透卵石层。

3.部分桩出现桩顶上涌情况

在现场管桩施工时，部分桩沉桩完成后，后续施工出现桩顶上涌情况，桩间土标高上浮。原因分析：（1）沉桩时，由于桩身附近土层被压密并挤开，使土体产生垂直方向的隆起，造成临近完成桩产生上浮；（2）沉桩施工方法与施工顺序不当；（3）管桩复打不到位。

处理措施：（1）后续施工自楼栋中间向四周对称施打；（2）加强对管桩复打；（3）加强管桩施工中标高检测，在沉桩到位、整栋楼管桩施工完毕、复打完成、管桩检测前分别进行桩顶标高检测，发现问题及时处理。

结语

综上，随着经济的高速发展和城市建设的扩张，预应力混凝土管桩因其在安全质量控制简便，施工速度快，建设成本低等方面的优势，在工程建设中将继续广泛使用。在今后的应用中，要不断创新和改革，进一步加强新型预应力混凝土管桩材料的研发，新型管桩设备的应用，新型建筑仪器的辅助，提高管桩结构耐久性，降低对周围环境的影响，优化流程，规范施工，提高桩基安全稳定，确保工程牢固可靠。

参考文献

[1]黄成，赵庆鑫.预应力高强度混凝土管桩在复合地基设计中的应用——以太原市南中环-西中环立交工程为例 [J].城市道桥与防洪，2018（05）

[2]朱麟敏.先张法预应力混凝土管桩在公路复合地基中的应用[J].福建建设科技，2011（04）

[3]GB13476-2009.先张法预应力混凝土管桩[S].北京：中国标准出版社，2009

[4]GB50007-2011.建筑地基基础设计规范[S].北京：中国建筑工业出版社，2011

[5]GB50202-2018.建筑地基基础工程施工质量验收标准规范[S].北京：中国计划出版社出版，2018

[6]JGJ106-2014.建筑桩基检测技术规范[S].北京：中国建筑工业出版社，2014.