国家教育管理公共服务平台

省级数据中心建设指南

教育部教育信息化推进办公室　　发布
教育部教育管理信息中心　　编制
2013 年 4 月

前 言

本指南的附录是技术资料性附录。

本指南由教育部教育管理信息中心提出。

本指南由教育部教育信息化推进办公室负责解释。

目 录

一、 引言

教育管理信息系统建设是《国家中长期教育改革和发展规划纲要(2010-2020年)》以及《教育信息化十年发展规划（2011-2020年)》中确定的重要内容，是支撑教育管理现代化、促进教育改革发展的基础性工程。

国家教育管理公共服务平台建设是“十二五”期间的教育管理信息系统建设的核心任务，是“三通两平台”的重点内容之一。其具体内容是建立覆盖全国各级教育行政部门和各级各类学校的管理信息系统及基础数据库,为加强教育监管、支持教育宏观决策、全面提升教育公共服务能力提供技术和数据支撑。平台按照“两级建设、五级应用”体系进行实施。两级建设是指在教育部和各省级教育行政部门分别建立中央和省两级数据中心，建设数据集中、系统集成的应用环境；五级应用是指各类教育管理信息系统均同步建设中央、省、地市、县、学校五级系统，由教育部统一组织开发，其中中央级系统部署在中央级数据中心，省、地市、县、学校级系统下发并部署在省级数据中心，供中央、各地和学校使用，以上由教育部统一组织开发的国家教育管理信息系统在本指南中简称为国家信息系统。平台将整合各级各类教育管理信息资源和信息化基础设施，建设包含教育机构、学生、教师和学校资产及办学条件等各类教育管理与服务对象，覆盖国家、各地和学校等多层次的共享的教育基础数据库，以及信息整合、业务聚合、服务融合的教育管理信息系统，实现教育行政部门与学校间的数据互通和系统互联，提升教育监管能力与公共服务水平。

国家教育管理公共服务平台建设以各地和学校的相关信息系统和数据作为基础，需要推动国家信息系统在各地和学校的部署与应

用。国家教育管理公共服务平台省级数据中心建设是构建“两级建设和五级应用”、保证国家信息系统在省级部署与应用的关键设施。近几年各省借助教育信息化工程实施建设了所属的数据中心，但是整体上各省级数据中心依然存在着设计不完整，可靠性、可用性、可持续发展能力严重不足，专业化运行维护管理水平需要进一步提高等诸多问题。同时，国家信息系统在各省的部署，需要在设计和运行环境上（如数据库平台、中间件、数据采集、地理信息等公共平台，数据交换、安全体系等互联互通设施）提供相应的框架规范，迫切需要在技术层面上进行规划与指导。

本指南将为各省级教育行政部门在国家教育管理公共服务平台省级数据中心基础设施、公共软件平台、信息安全、技术服务与运行维护体系等各方面的设计和建设提供指导。

二、 建设目标与基本原则

2.1 省级数据中心的建设目标

省级数据中心是为本省提供教育管理信息系统运行的云服务平台，承载和满足国家教育管理公共服务平台在省级教育行政部门的部署和运行；集成和支撑省本级各类教育基础数据库和各类教育管理信息系统；服务于所辖区域内教育行政部门和学校的信息化管理业务应用，带动全省教育信息化发展。

2.2 省级数据中心建设应遵循的原则

省级数据中心建设应遵循“三项原则”。

1．实用性和先进性原则

省级数据中心建设既要充分考虑实用性，始终面向业务应用，又要考虑先进性，保持适度前瞻。在进行架构规划时，不盲目追求设备的超前采购，在充分考虑应用性能的基础上，保护原有投资。同时要采用成熟先进的理念、技术和方法，适应发展潮流。

2．可靠性和稳定性原则

省级数据中心建设要确保系统运行的可靠性和稳定性，要从系统架构、技术措施、设备性能、系统管理、厂商技术支持及维修能力等多方面进行设计规划，确保系统运行的可靠稳定。

3．可扩展性和易维护性原则

省级数据中心建设应充分考虑可扩展性和易维护性，适应系统变化要求，尽量降低电力、人力等各方面资源维护费用。

三、 建设总体要求

3.1 满足应用系统部署和服务的需要

省级数据中心首先要承载国家信息系统的部署运行，也要支撑本省自建应用系统及其他应用系统的部署运行，要采取云服务模式，为本级及所属各级教育行政部门和学校提供信息系统和数据库存储与服务，具体情况如图 1 所示。

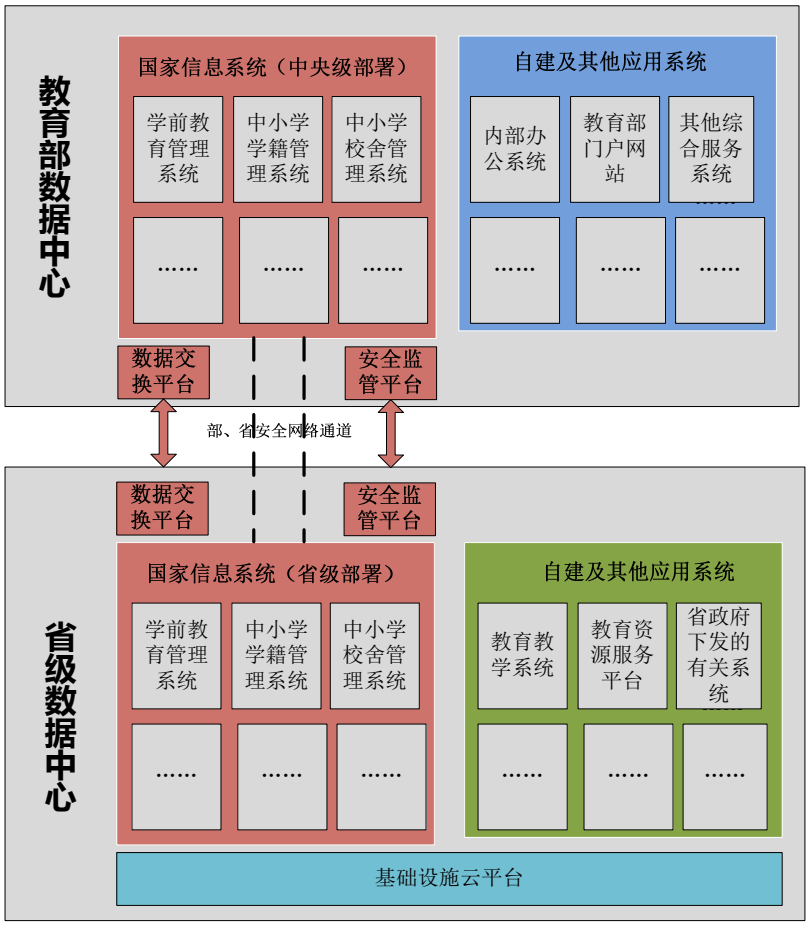

图 1 省级数据中心承载应用系统示意图

3.1.1 承载国家信息系统部署

“教育服务与监管体系信息化建设”项目作为国家教育管理信息化的先导工程，已完成顶层设计。教育部正在统一开发建设一系列与学生、教师、学校资产及办学条件相关的系统，并陆续开始在部（中

央)、省两级投入部署运行（部分信息系统见附录：统一规划的国家信息系统一览表)。省级数据中心必须能够承载这些信息系统的运行，在设计和建设中满足这些信息系统的计算、存储需求。

3.1.2 承载自建及其他应用系统的部署运行

为满足本省教育信息化的应用需求，省级教育行政部门可以建设自己需要的特定应用系统（如教育教学相关信息系统、教育信息服务门户等)。省级数据中心在保证国家信息系统部署运行的基础上，也要考虑本级教育管理和服务信息系统的开发、运行需要。

3.1.3 提供本省教育信息化基础设施云服务

为统筹本省教育信息化基础设施建设，避免基础设施重复建设，省级数据中心在建设时应充分利用云计算技术，搭建云服务平台，为本省教育行政部门和学校提供计算、存储等基础设施云服务。

3.2 形成完善的基础设施环境

省级数据中心要按照国家信息系统的运行要求，构建机房、网络、计算、存储等基础环境和设施；根据业务系统和数据中心运行维护和管理的需要，构建基础软件支撑平台，包括数据库、门户、数据交换和系统管理等平台；建立重要系统和业务数据容灾备份；为应用系统敏感数据建立统一密码安全服务平台，实现敏感数据加密存储和安全访问；建设与教育部数据中心之间的数据交换平台与安全网络通道，保障部、省两级数据中心间的数据传输安全。

3.3 符合国家及教育部信息化有关标准规范

省级数据中心的建设必须严格遵循国家各类信息化标准、规范，采用教育信息化有关标准规范。包括但不限于以下内容。

(1) 《国家电子政务工程建设项目管理暂行办法》

(2) GB 50174-2008 电子信息系统机房设计规范

(3) GB 50462-2008 电子信息系统机房施工及验收规范

(4) GB 50311-2007 综合布线工程设计规范

(5) GB 50312-2007 综合布线系统工程验收规范

(6) GB 50395-2007 视频安防监控系统设计规范

(7) GB 50263-2007 气体灭火系统施工及验收规范

(8) GB 50394-2007 入侵报警系统工程设计规范

(9) GB/T 20269-2006 信息安全技术—信息系统安全管理要求

(10) GB/T 20984-2007 信息安全技术—信息安全风险评估规范

(11) GB/T 22239-2008 信息安全技术—信息系统安全等级保护基本要求

(12) GB/T 22240-2008 信息安全技术—信息系统安全等级保护定级指南

(13) GA/T 388-2002B 计算机信息系统安全等级保护管理要求

(14) 《教育管理信息标准》（教技〔2012〕3 号）

(15) 其他相关技术规范

3.4 建设集中统一的教育基础数据库

省级数据中心要建设省本级教育管理和服务集中统一的教育基础数据库，纵向贯穿学前教育、中小学教育、中等职业教育、高等教育和成人教育等各个教育层次,形成上下一致的教育机构、学生、教师（职工)、学校资产及办学条件基础数据库；横向打通学生、教师（职工)、学校资产及办学条件数据，形成全面整合、集中一致的教育管理和决策基础数据库，为各类业务信息系统提供数据服务。

3.5 构建网络与信息安全保障体系

省级数据中心安全建设，要遵照国家信息安全等级保护相关政策要求和标准规范，遵照教育部有关信息安全的行业要求和标准规范，

形成覆盖技术和管理的整体安全保障体系；建设与教育部数据中心上下级联的安全运行维护、管理、监测与预警的技术和工作管理平台。

3.6 建立运行维护和技术服务体系

建立运行维护保障体系，实现集中的教育信息化基础设施的运行维护；通过制定配套的数据维护、交换、管理制度，实现数据采集、使用的规范化。明确责权明晰的运行维护组织机构，建立信息系统运行维护队伍，实现运行维护和服务流程化、制度化、专业化。

依托数据中心，建设教育管理信息化技术服务体系，采用多种手段为省本级和所属地区的用户（下属教育行政部门和学校）提供网络和应用技术服务、数据采集支持服务。

3.7 规范省级数据中心建设工程管理

省级数据中心建设工程，按照国家电子政务系统建设管理的有关规定，从以下几个方面进行管理。

1. 机构与职责。省级数据中心建设工作明确由本级教育信息化主管部门统筹规划与指导和管理，工程建设实施委托相应的教育信息技术部门承担。

2. 招标管理。省级数据中心建设和相关服务咨询招标应根据《中华人民共和国招标投标法》、《中华人民共和国政府采购法》及有关规定，本着公开、公平、公正的原则进行招标。

3. 实施管理。省级数据中心建设要建立健全项目管理制度，明确责任，规范实施。按照项目审批部门批复的可行性研究报告、初步设计方案和投资概算实施项目建设，详细设计方案报教育部教育管理信息中心审核备案；按照信息系统工程监理的有关规定委托具有相应资质的监理单位进行监理；按照国家有关规定做好项目建设资料的收集、整理和归档工作。

4.资金管理。省级数据中心建设中，按照国家的法律法规及有关部门的财务管理规定使用资金，专账管理、专款专用；加强财务管理与会计核算,规范账务设置,建立健全内部财务管理制度；做好固定资产、软件资产登记与管理工作。

5.**验收管理。**省级数据中心根据《国家电子政务工程建设项目管理暂行办法》规定由立项建设部门组织验收，项目验收前，需由省级教育行政部门和教育部教育管理信息中心组织，对省级数据中心进行符合性评估。

6.运营管理。省级数据中心建成后，各省级教育行政部门明确省级数据中心运行机构，配备相应专业管理和技术人员，制定和完善相应的运行管理制度，落实运行经费,应加强对省级数据中心各系统的日常运行监管、网络和信息安全评估，确保系统的顺利运行。

由于各省的基本情况不同，省级数据中心的建设模式和规模可能不尽相同，但无论是自建或租赁数据中心，都必须满足本指南的建设总体要求。

四、 建设内容

4.1 省级数据中心分类

为使省级数据中心的建设更有针对性和可操作性，按学生总数将省级数据中心分为A类和B类。学生总数在500万人以上的省份的是A类数据中心，小于500万学生的省份数据中心为B类数据中心。各省数据中心分类参考如下表所示（可根据实际学生数量调整）。

表 1　省级数据中心分类参考表

西部地区	分类	中部地区	分类	东部地区	分类
内蒙古自治区	B	山　西　省	A	北　京　市	A
广西壮族自治区	A	吉　林　省	B	天　津　市	A
重　庆　市	B	黑龙江省	B	上　海　市	A
四　川　省	A	安　徽　省	A	江　苏　省	A
贵　州　省	A	江　西　省	A	浙　江　省	A
云　南　省	A	河　南　省	A	福　建　省	A
西藏自治区	B	湖　北　省	A	山　东　省	A
陕　西　省	B	湖　南　省	A	广　东　省	A
甘　肃　省	B	河　北　省	A		
青　海　省	B	辽　宁　省	B		
宁夏回族自治区	B	海　南　省	B		
新疆维吾尔自治区	B				
新疆生产建设兵团	B				

A 类数据中心的机房面积不低于 350 平方米； B 类数据中心的机房面积不低于 250 平方米。

4.2 机房设施

数据中心机房建设可根据当地的实际情况，采用自建或租用方式，安全上要求满足国家信息安全等级保护相关技术要求。

省级数据中心建设依据《电子信息系统机房设计规范》（GB 50174-2008）将机房建设成为A级电子信息系统机房。

省级数据中心机房设施建设内容应包括：机房布局设计、电气子系统、防雷接地子系统、不间断电源子系统、空调新风子系统、安防子系统、环境监控子系统、综合布线子系统、消防子系统、机房机柜设备、KVM子系统等。

1. 机房布局设计

按照功能布局分为：数据交换区、数据存储区、数据备份区、数据服务器区及监控区等。

2. 电气子系统

(1) 各省级数据中心机房设备用电和动力供电分开。电源采用双路供电，动力供电的设备包括空调、照明、维修插座等。

(2) 机房内强电走线为下走线方式，桥架均作接地连接。

3. 防雷接地子系统

(1) 依据机房配电的实际情况，机房防雷按照 IEC 标准进行安全的二级配合保护。

(2) 机房内金属天花板、地板、管槽等都要做接地保护，并就近连接到配电箱 PE 排上。

(3) 镀锌钢管、金属软管、金属接线盒、金属线槽外壳等均应进行可靠接地，避免因电源波动较大而干扰设备的正常工作。

(4) 各省级数据中心机房建设工程在大楼外挖沟埋桩、焊接地排，使接地电阻小于 1Ω。

4. 不间断电源子系统

按照机房设备用电量配备UPS设备。

5. 空调新风子系统

各省级数据中心机房建设工程应采取主机房设置精密空调，部分区域设置商用空调的形式。机房内空调采用N台使用加1台备用机的方式。

6. 安防子系统

(1) 安防子系统包括门禁系统和监控系统。

(2) 门禁系统主要是在重要的区域设置门禁，对进出人员进行管理登记。

(3) 监控系统是指在重要的区域安装摄像头，做到监控无死角，对机房进行实时监控录像。

7. 环境监控子系统

各省级数据中心机房建设工程环境监控系统是对机房的温湿度、消防、UPS主机、精密空调、配电、漏水等子系统进行全面集中监控，并要做到准确定位。应具有本地声音报警、短信告警功能，支持实时显示、智能查询、报表、存储功能。支持远程访问，并要将门禁及监控系统统一平台界面。

8. 综合布线子系统

各省级数据中心机房建设工程每台服务器机柜至网络机柜，承担信息业务的传输介质应采用光缆或六类及以上等级的对绞电缆，传输介质各组成部分的等级应保持一致，并应采用冗余。双绞线连接到机柜后侧的配线架上。同时可以在地板下预留弱电线槽，或者采用机柜上走线方式。

9.消防子系统

各省级数据中心机房应配备有效灭火装置。消防工程所采用的器材和设备必须是经国家指定的检测中心确认合格的产品。消防系统的设计施工及验收必须经消防检测中心确认及验收。

10. 机房机柜设备

各省级数据中心机房网络机柜和服务器机柜采用符合国家有关标准的设备。

11. KVM 子系统

各省级数据中心机房建设工程中所配备的KVM系统应具备主要服务器的集中操作控制等功能。

4.3 省级教育管理云平台

4.3.1 总体架构

省级数据中心的核心基础设施采用云技术构建，通过云服务模式进行运行，称为省级教育管理云平台。在平台上是公共软件平台与应用层。总体架构如图2所示。

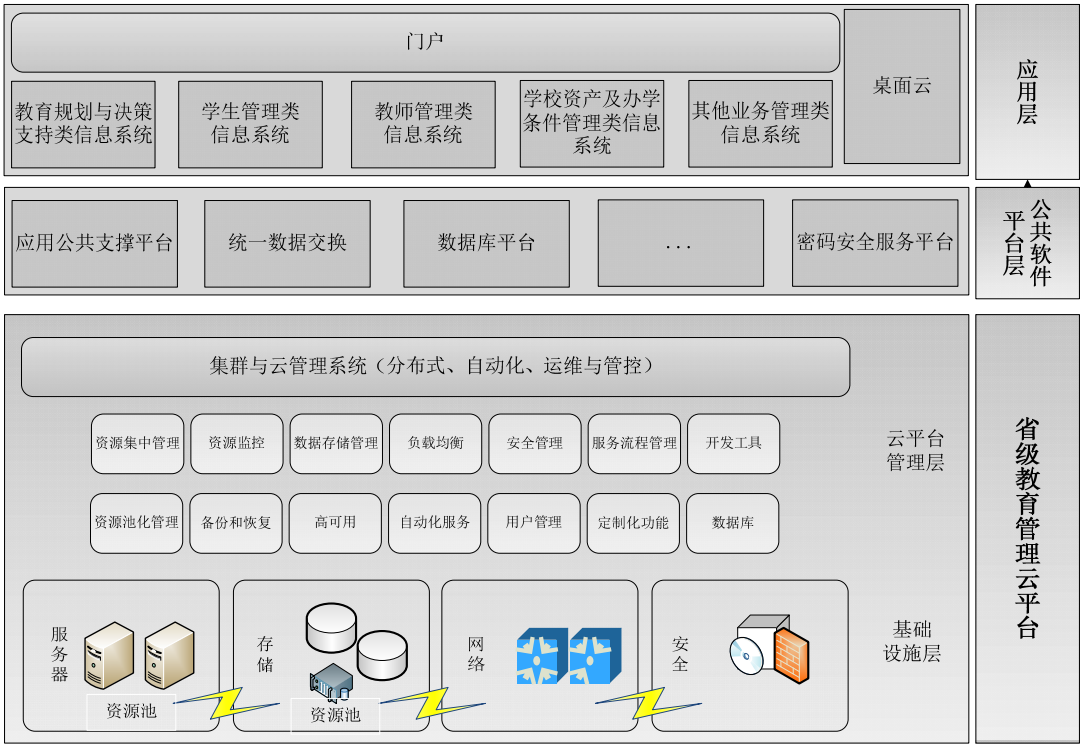

图 2　省级数据中心的整体架构图

省级教育管理云平台要使用符合业界标准的产品来设计，包括硬件、软件和应用规格化来提供简单可靠、易于部署和管理、便于扩展和升级的 IT 基础架构，满足云平台新建、升级扩容以及统一管控的

需求，通过整合资源，统一规划，为各地教育信息化业务应用与拓展提供重要支撑。

省级教育管理云平台架构包括基础设施层和云平台管理层。基础设施层包含网络、服务器、存储备份、容灾备份等。云平台管理层包含虚拟化管理系统、硬件管理系统、运行维护系统、监控系统等，对下提供精细化管理，对上实现统一界面和业务入口。

省级教育管理云平台至少要满足下列功能和性能要求：

1. 能够为国家信息系统部署、本省的信息系统运行、本地的信息系统应用扩展提供基础环境；

2. 具有足够可以动态调配的计算、存储资源，满足各类信息系统不同高峰时段的业务需求；

3. 能够为本省内教育行政部门和学校提供动态和自动的资源使用云服务；

4. 保证各类用户访问国家信息系统的速度，建议功能使用反应（等待）时间小于3秒；

5. 安全保障措施满足国家信息安全等级保护三级要求，保障本省自建信息系统的安全。

4.3.2 基础设施层

4.3.2.1 网络系统

网络系统要符合国家相关技术要求，提供足够网络带宽容量，承载所有的应用系统运行，同时为数据中心运行维护服务管理提供足够的工具支持。

考虑数据中心的安全性，省级数据中心网络拓扑可以参考图3进行优化。在教育部、省之间建立VPN隧道，保障数据传输安全。

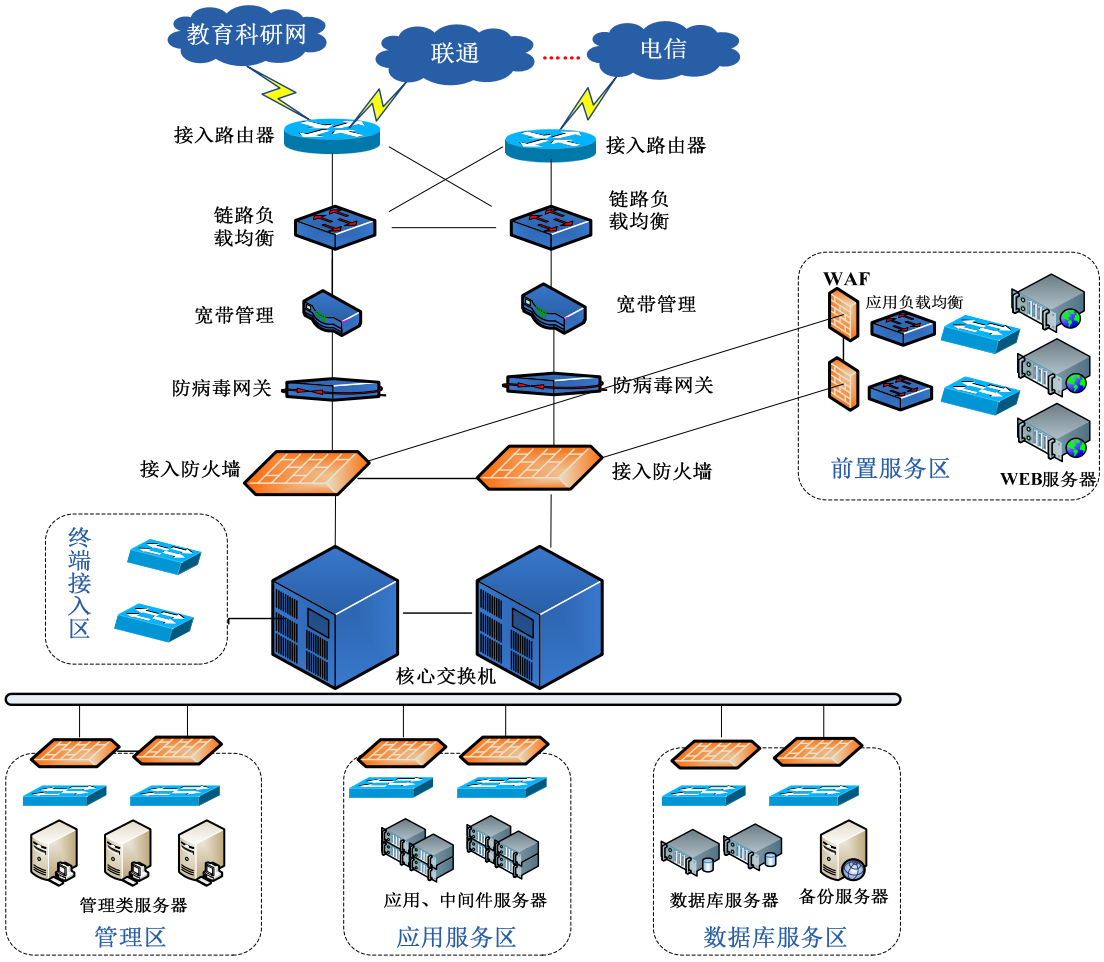

图3　省级数据中心网络拓扑示意图

关于网络结构设计的说明：

1. 互联网边界区

基于各省级数据中心已有的网络出口，主要实现网络出口及出口的安全管理、带宽管理、负载均衡控制。

2. 核心交换区

采用核心交换设备保障核心交换能力。可采用双核心交换设备，以保证核心交换网络的高可用性。

3. 终端接入区

省级教育行政部门使用教育信息系统，通过内部网络端口接入数据中心运行环境，使用终端接入区，通过终端接入区经防火墙进入网络内部。

4. 前置服务区

提供Web服务的服务器被放置在前置服务区，可以增加整个网络的安全性。在前置服务区配合WAF、SSL VPN等设备，加强网络安全。在前置服务区配置应用负载均衡设备实现整个网络的负载均衡。

5. 应用服务区

应用服务区主要承载运行环境内的应用服务器，包括中间件服务器等。核心区通过独立的防火墙设备接入应用服务区。

6. 数据库服务区

数据库服务区承载了运行环境下所有应用系统的数据库。数据库区包含一系列的数据库服务器及存储设备。在该区内承载的数据库服务建议采用高可用集群设计；在该区域保存的数据，建议在存储设备上保存一份冗余实例，实现数据服务的高可用性。数据库服务区通过独立的防火墙接入核心交换区。

7. 网络管理区

网络管理区用于网络和服务器、安全设备、存储等设施的管理操作设施。该区内包括网络设备，管理用服务器，以及网络和设备管理软件平台。

4.3.2.2 服务器系统

省级教育管理云平台的各类服务器建议采用服务器虚拟化平台设计，利用虚拟化整合物理服务器，形成各自的服务器计算池，将业务迁移到云平台上，通过资源共享实现资源的动态调度，达到利用最大化，节约硬件投资和维护成本。

1．服务器系统框架

服务器系统架构以三层架构为主，即由Web服务器、应用服务器、数据库服务器组成，同时配置辅助管理类服务器。

使用负载均衡技术，是实现服务器架构的可用性和可扩充性的主要手段。这样服务器数量可以根据信息系统和用户的增加逐步扩充，每层架构上均配置多台服务器，将单个信息系统的计算分散到多个服务器（或虚拟机），根据用户数量进行动态调整，以及故障切换。当应用系统增加、负载增大时，可以通过层内横向的服务器扩充，满足应用的服务器资源需求，可以实现服务器系统“统一规划、分步扩充”的战略，提高资金使用效果。

2．服务器系统的规模和性能

服务器的数量和单台计算能力是 A 类数据中心与 B 类数据中心的主要差异化指标之一。同类数据中心的服务器配置也会不同。可参考本指南附录一进行测算。

服务器系统至少要满足下列云服务的功能和性能要求：

（1） 单台服务器、整体服务器都要分别有足够的虚拟化容量，能够实现应用的集群和负载均衡，提供业务应用系统高峰的扩展能力，以及系统的动态迁移能力；

（2） 数据库服务器具备超大记录数据库的大访问量实时处理能力。

3．服务器系统设计

省级数据中心将承载国家信息系统运行，同时还将承载本地区信息系统的运行和服务，以及数据中心管理平台、应用支撑平台及数据库平台。服务器系统主要设计部署于以下区域：

(1)　前置服务区（DMZ，Demilitarized　Zone）

所有对外提供服务的Web服务器都放置在DMZ区。一般Web服务器采用虚拟机（服务器）方式提供服务。在DMZ区将服务器群配置成为一定数量的虚拟化服务器。对于不同处理能力需要的业务系统，分配不同数量的虚拟化服务器，适应并发访问数量的需求。可对特定时间的用户访问量变化进行虚拟化服务器使用数量的调整，实现服务器资源的最优化使用。

(2)　应用服务区

应用服务器主要负责承载应用系统的业务逻辑层计算，采用虚拟化服务器方式可有效提高服务器资源利用率。对于不同业务处理能力的业务系统，将分配不同格式的虚拟化服务器，以满足计算量要求。

(3)　数据库服务区

数据库服务区中将放置数据库服务器，根据业务系统处理能力的不同，为不同业务系统分配不同资源，包括配置不同处理能力的物理服务器，建立不同级别的数据库服务。

(4)　运行维护服务管理区

数据中心运行维护服务管理区将包括运行维护服务器，以及相应的管理平台。

4.Web 服务器

Web服务对服务器主机的文件访问或会话数有较大要求，通常Web 服务对主机CPU的总体要求比较低，可通过“虚拟机＋负载均衡集群”的方式提高系统的运行效率和可靠性，实现资源的完整利用和资源的动态调配。

Web服务器的操作系统根据国家信息系统部署要求选用Linux或Windows平台。

5.应用、中间件服务器

应用、中间件服务器与web服务器一样，以物理主机虚拟出的虚拟主机提供应用和中间件服务，采用“虚拟机＋负载均衡集群”的方式提高系统的运行效率和可靠性，实行资源的完整利用和资源的动态调配。

应用、中间件服务器操作系统根据国家信息系统部署要求选用Linux或windows平台。

6.数据库服务器

数据库服务器根据应用情况通过数据库本身提供的集群软件实现数据库的高可用。按应用需求可分核心应用和普通应用、大负载和小负载，并可利用负载均衡技术提高应用服务器的数量以提高系统的运行能力。对数据库平台的选择，业内以TPC-C的benchmark值为参考依据，总体思想体现在CPU的缓存大、系统内存高、并发任务能力强、机器内部的I/O和总线带宽大。数据库服务器采用独立的物理机部署。

数据库服务器操作系统根据国家信息系统部署要求选用Linux或windows平台。

建议选择八路机架服务器或四路机架服务器作为数据库服务器，分别用于大记录数据库和一般数据库。

7.管理类服务器

管理类服务器主要用于虚拟化管理平台、安全管理平台、身份认证系统、网管、运行维护、备份系统等平台的部署。针对管理类系统部署在同一区域，采用“虚拟机＋负载均衡集群”的方式提高系统的运行效率和可靠度性，达到资源的完整利用和资源的动态调配。

数据备份服务器，由于使用区域和功能的不同，建议使用物理机。

4.3.2.3 存储备份系统

1．存储的数据类型与规模

存储设备是云服务架构的基础，需满足各类应用需求。数据中心存储容量的估算应包括结构化数据存储容量、非结构化数据存储容量、虚拟服务器资源池存储容量，同时按照在线、高可用冗余、本地备份、远程容灾复制等所需要的存储容量。存储容量的测算参照本指南附录一进行测算。应满足以下基本功能与性能要求：

（1） 规划A类数据中心存储数据量至少为100TB，规划B类数据中心存储数据量至少为70TB；

（2） 配置相应的本地备份设备；

（3） 具备存储资源池的共享和适时调度功能；

（4） 要求设备具有良好的扩展能力，便于存储容量的升级能力。

2．存储的类型配置与原则

存储根据数据和使用类型进行配置。存储介质的性能选择应遵循以下原则：

(1) 结构化数据的数据存储应采用高性能存储介质；

(2) 虚拟服务器存储池应采用高性能存储介质；

(3) 本地高可用性磁盘镜像复制应采用高性能存储介质；

4.3.2.4 容灾备份系统

容灾备份系统分为数据备份级别和应用容灾级别，可分为本地备份和异地备份。

1.数据库数据备份设计选择

数据库容灾备份体系结构设计应遵循以下两点要求：

(1)　确保数据的随时可用性及活动备份；

(2)　降低成本。

针对上述两点要求，建议采用以下拓扑模式及技术实现数据库系统数据备份。

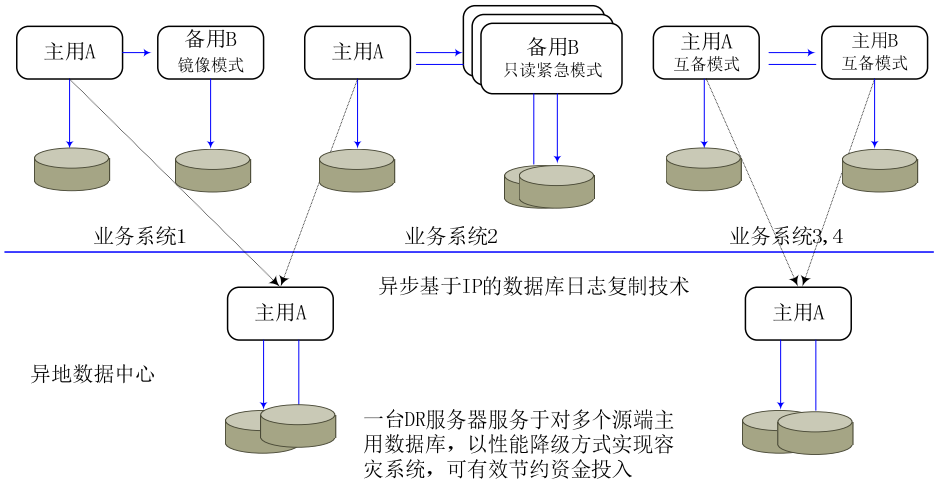

图 4　省级数据中心容灾备份系统部署示意图

2. 其他系统的数据备份考虑

其他系统的数据备份考虑如下：

(1)　WEB 虚拟机可基于 IP 网络或磁盘阵列系统的能力，复制原始镜像到异地；

(2)　应用服务器虚拟机可基于 IP 网络或磁盘阵列系统的能力，复制原始镜像到异地；

(3)　非结构化文件系统可基于 IP 网络或磁盘阵列系统的能力，复制全部或部分数据到异地；

(4)　其它暂不考虑数据备份设计。

3. 应用容灾

在异地建立各类应用系统和数据的完整、实时备份，作为更加完整的容灾系统建设，建议逐步完成。

4.3.3 云平台管理层

云平台管理层包含虚拟化软件，虚拟化管理系统、硬件管理系统、运行维护系统、监控系统等，对下提供精细化管理，对上实现统一界面和业务入口，成为云数据中心统一管理平台。云数据中心统一管理平台至少满足以下功能和性能要求：

（1）对底层服务器的计算、存储等资源池和虚拟化软件进行管理，实现资源供应与自服务，提供按需获取，按量计费的可信赖资源服务；

（2）针对管理和运行维护的实际需要，实现云计算服务的交付、云数据中心用户和流程的管理以及数据中心的监控；可以对虚拟资源和物理资源进行实时的监控和性能查看，并且记录历史数据；

（3）与省本级综合门户、应用支撑服务平台等无缝集成和融合；用户可以通过自助式服务门户，自助的申请资源，在配额范围内系统可以自动审批并创建该资源；

（4）业务运营与计费，维护用户的资源使用信息和业务的运营情况，提供报表等数据给用户参考整个云平台的资源使用情况；

（5）自动化分析与调优，动化分析与调优则是基于资源综合管理系统的数据，通过自学习算法，自适应算法等综合系统，去判断系统的性能瓶颈并给出合理化建议，在提前配置的前提下，可以进行一些自动的性能调优。

云平台管理平台的底层可以是开放式的第三方的虚拟化系统或者存储系统，也可以是国产的虚拟化系统，通过这些底层系统将物理的计算资源，存储资源和网络资源整合起来，进行池化和资源管理。

云数据中心统一管理平台功能参考如表下表所示。

表 2　云数据中心统一管理平台功能参数

概述	详细描述
综合门户、运行维护、应用支撑服务支持	与省级综合门户、运行维护平台、应用支撑服务平台等无缝集成和融合
广泛的平台支持	支持当前主流厂商的 x86 服务器产品，虚拟机支持当前主流的 Windows、Linux 32/64 位操作系统及系统之上的各种应用。
多租户机制	基于策略的用户控制技术和虚拟交换机的网络隔离技术，可以保持多租户环境下的安全性和可靠性。
资源服务按需获取	终端用户可以通过 Web 界面的方式在线自助申请所需的计算、存储、网络资源，实现资源的按需获取。
资源服务按量计费	多层次实时的资源使用情况统计，让用户精确掌控自身资源和费用使用情况。
资源弹性扩充	资源可以根据需要实现多级别的动态扩充，上到资源池虚拟数据中心的资源扩充，下到虚拟机的 CPU 和内存的动态扩充，都可以实现无缝动态的资源弹性扩充。
服务全生命周期管理	系统可以涵盖服务提供所需的各个环节，通常包括服务的申请和流程管理；服务的交付和回收；服务的使用统计和计费；服务的运行监控。
多层次的安全保护	系统实现从底层虚拟化平台的安全(锁定模式防止通过网络以根用户访问虚拟化平台)，网络安全（多模式的虚拟交换机配置）到管理节点的安全。
资源池化	通过虚拟数据中心的形式为用户提供资源。通过以逻辑方式将计算、存储和网络容量组合成资源池，利用服务的交付和提供环节之间的完全抽象化，更高效地管理资源。
多级的资源池	通过将虚拟数据中心细分为提供者虚拟数据中心和组织虚拟数据中心，实现了将 IT 服务的消费与交付相分离，从而更有效的管理资源。
准确的监控告警	对物理资源及虚拟资源的状态进行实时监控，自动触发告警，通知管理员对问题设备进行处理，提高了数据中心的运行维护管理效率。
丰富的报表统计	提供多层次详细的报表数据，方便用户概览资源运行情况和使用

	情况。

4.3.4 桌面云服务

桌面云是云计算的一种应用形态，通过集中化桌面管理，可提高资源利用率，降低整体拥有成本。将个人桌面环境所需的计算、存储资源集中于中央服务器上，取代了客户端的本地计算、存储资源；中央服务器的计算、存储资源同时也是共享、可伸缩的，使得不同个人桌面环境资源按需分配、交付，总体上降低硬件资源需求。

桌面云解决方案在云计算硬件资源和云资源管理及调度、虚拟化平台的基础上，提供了云终端、接入控制、桌面会话管理等主要组件，以及一体化的云平台和桌面业务管理维护系统，整体架构如图 5 所示。

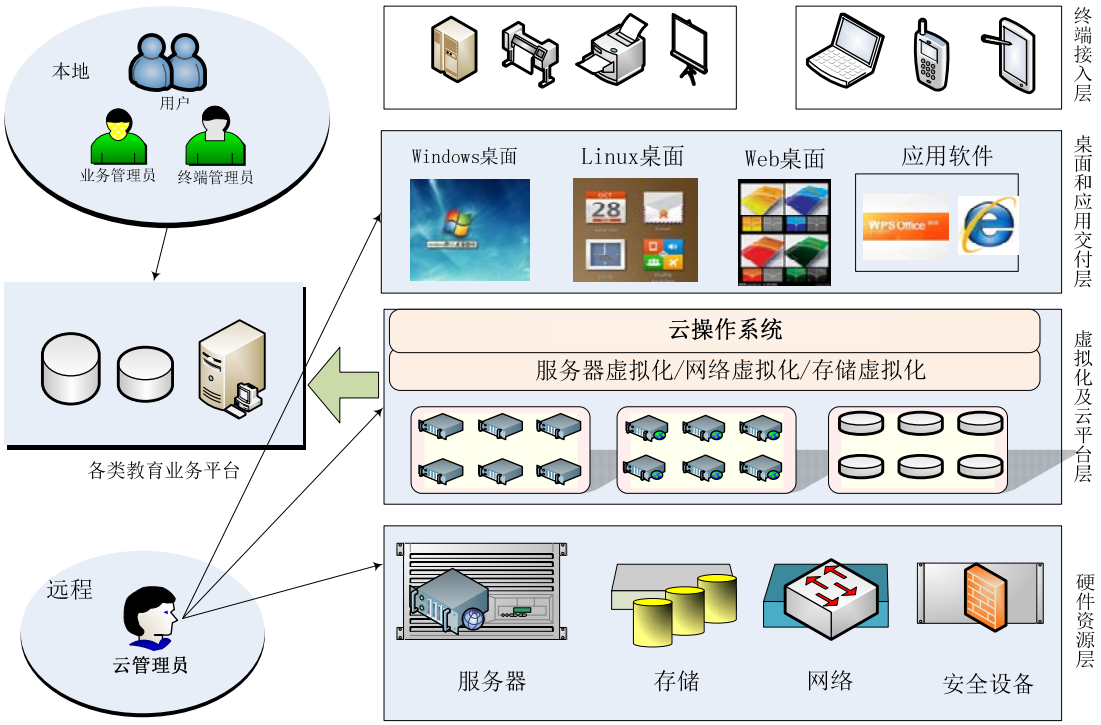

图 5 桌面云架构图

虚拟桌面管理系统的主要构成如下：

(1) “终端接入层”将远程桌面输出到显示器，以及将键盘鼠标输入传递到虚拟桌面。

(2) “桌面和应用交付层”接入网关主要提供两个功能，一是对 Web Interface 节点的访问提供负载均衡，保障可靠性；另一个功能是对远程桌面连接协议 ICA(Independent Computing Architecture)进行加密和转发。

(3) “桌面管理系统”用于对用户的虚拟机生命周期管理以及连接管理，例如创建虚拟机、分配虚拟机等。

(4) “虚拟化及平台层”采用业界先进的虚拟化软件，在保证物理资源充分利用的同时，可提供高可靠性，打造高效、灵活、安全的云平台。

(5) “硬件资源”是云平台的基础，云平台的硬件主要包括服务器、存储、网络以及安全设备。

4.4 公共软件平台

4.4.1 应用公共支撑平台

应用公共支撑平台层包括以下几个方面。

1.综合门户

实施省级综合门户建设，建设省级教育管理公共服务门户和教育信息公共服务门户。省级教育管理公共服务门户要集成省级各应用系统并集成展示教育基础数据，实现省级单点登录。省级教育信息公共服务门户要实现公共用户的数据查询和访问服务。

2.数据交换与共享

由教育部提供数据交换平台，统一部署，实现部、省两级数据中心的数据交换。

基础数据库信息共享使用教育部提供的教育基础信息数据库管理与服务系统平台。

3. 应用系统支撑平台

教育部提供与业务信息系统配套的应用系统支撑平台，为各省的业务信息系统提供全局统一基础性支撑服务，使各应用系统能够进行有效的整合与协同，形成各省信息系统统一的公共支撑环境，与国家信息系统一并部署，可提供省级应用涉及的应用集成、技术支撑、安全服务、运行监控等领域的软件服务集合，应用系统支撑平台有关内容另行作为技术规范印发。由各省负责应用系统支撑平台的实施与集成工作。

4.教育基础信息数据库管理与服务系统

教育部提供教育基础信息数据库管理与服务系统，由各省负责实施与集成工作。通过该系统建设和实施，建立省级教育基础信息数据库，为业务系统提供权威、准确、完整有效的数据。教育基础信息数据库管理与服务系统包括五个方面内容：元数据管理，支持对数据资源目录的管理；主数据管理，支持主数据的建设与管理；数据质量管理，支持对教育基础信息数据库的质量管理与评估；数据服务，提供接口、工具支持数据资源的共享与应用；数据安全管理，控制数据存取和访问，对教育基础信息数据库的运行状态进行监控和分析。

5.公共中间件

公共中间件包括应用服务器中间件、目录服务、商业智能、内容管理、地理信息系统、报表工具、即时消息等，在此基础上构建统一的应用软件基础运行支撑环境。教育部提供部分中间件的使用授权（具体见表5）。

4.4.2 数据库平台

建设数据库平台是为了实现对数据中心各类资源的合理配置和有效使用，数据库管理系统选用Oracle和SQL Server。

数据库平台属于省级数据中心的核心平台，为省级及以下教育行政部门、学校和各个应用提供高度安全、可靠的数据平台，利用数据库平台，可以帮助各级教育行政部门在可信的平台上自如地进行伸缩，提高管理和开发的工作效率。建立于数据中心平台之上的应用系统数据库，对结构化数据的存储主要包括以下需求要素：

表 3　省级数据中心结构化数据存储需求因素

编号	标　准		说　明
D1	初始数据容量		系统初创的初始化数据量，迁移已有系统的数据容量
D2	数据年增量		每年新增的数据量
D3	数据生命周期	在线存储数据量	可以根据数据库中需要保留最近多少年的数据进行推算
D4		近线存储(NearStore)数据量	数据超出年限迁移出在线数据库，其中哪些年份的数据应能快速导回在线数据库以备数据查询
D5		离线存储数据量	超过哪些年份的数据基本已不再使用，可以被离线存储归档
D6		可清除数据量	哪些数据量不再需要存储归档，可以进行删除处理
D7	数据恢复	可容忍丢失的最大数据量	系统发生意外情况时，允许损失多长时间内的数据，称为数据恢复的RPO(Recovery Point Objective)
D8		可容忍的最长数据恢复时间	允许在多长时间内完成达到RPO要求的数据恢复，称为数据恢复的RTO(Recovery Time Objective)
D9		数据备份的保留期	保留多长时间内的数据备份副本，或保留最近多少个数据备份副本

数据库平台应支持多个逻辑处理器，并有效地利用一流硬件供应商的多核技术体系，保证数据库平台的高性能和可伸缩性，为整合更多数据源和充分利用硬件资源提高保障。

4.4.3 密码安全服务平台

为解决各应用系统对其核心敏感数据信息进行统一加密的需求，保证重要数据的机密性、完整性、认证等安全特性，省级数据中心需按照教育部的统一要求配备部署密码安全服务平台，实现对应用系统敏感数据信息的加密处理，支持国家标准密码算法，为应用系统提供数据加密/解密、数字签名/验证签名、密钥管理、访问控制、密码设备统一管理等密码安全服务。

4.5 信息安全保障体系

4.5.1 信息安全保障体系总体要求

1. 安全保障体系框架

根据数据中心的总体安全保障机制，结合国家信息安全等级保护基本要求，与数据中心整体技术框架相配合，建立相配套的安全保障体系框架，如图 6 所示。

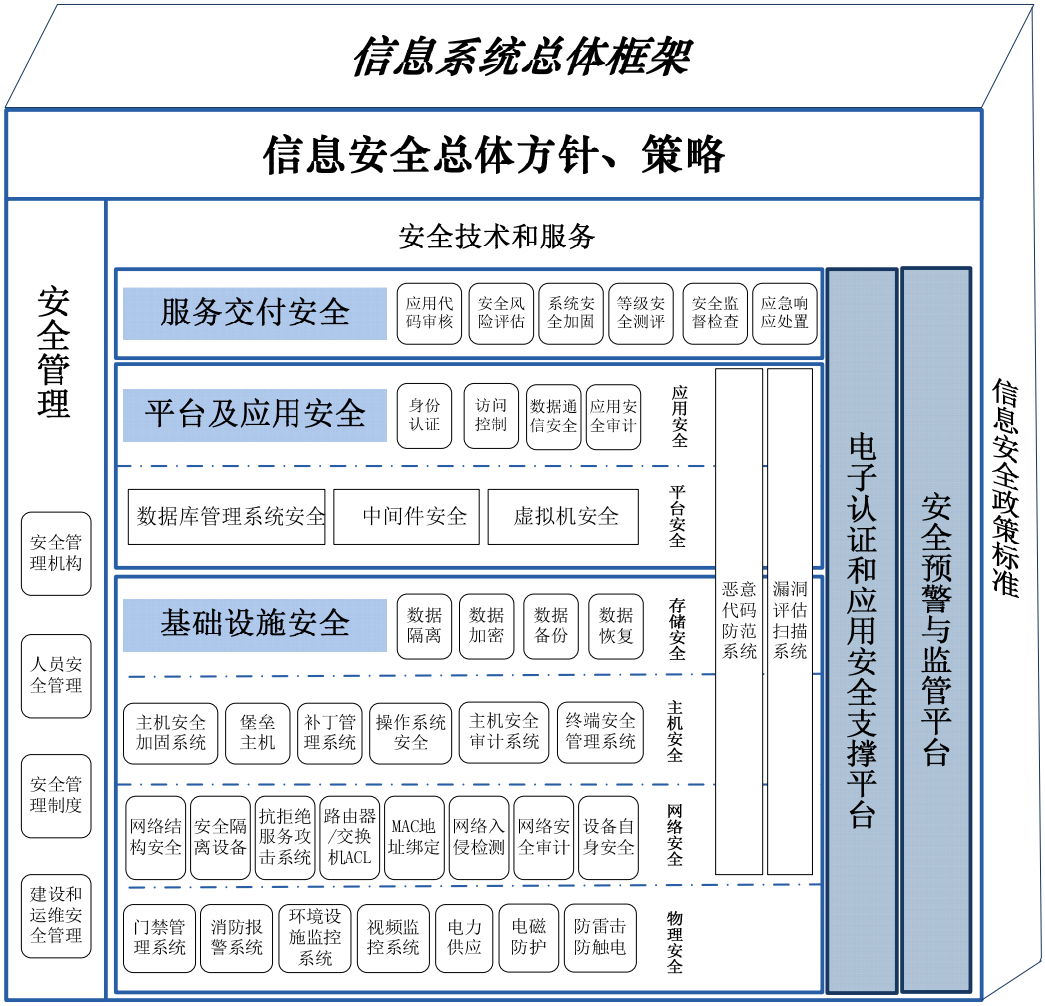

图 6　省级数据中心安全保障体系框架

2. 总体安全保障机制

数据中心建设应采用纵深防御的安全保障机制，确保核心数据资源的安全保护。核心数据要建立核心存储区域，该区域位于纵深防御的最里层，逐级建立数据库服务区、应用服务区、前置服务区和对外服务器区等安全区域，根据总体的信息安全策略，从基础设施、平台应用和服务交付等各层面综合保障数据中心的安全。

3. 信息系统安全重点工作内容

省级数据中心和本省运行的信息系统要按照国家信息系统安全等级保护制度和教育部相关文件要求进行定级；从管理和技术两个角度进行本省网络与信息安全保障体系建设；设置网络与信息安全职能部门和岗位，进行人员安全培训和技能培训，落实信息安全人员持证

上岗；按照教育信息系统安全等级保护政策要求和技术规范，由教育信息安全等级保护测评中心实施，定期开展信息系统等级测评；建立定期安全检查机制并配合主管部门和当地公安部门做好监督检查。

省级数据中心应按照第三级信息系统的安全保护要求进行建设。二级系统可通过建立二级系统区域合理裁剪安全控制。为保障国家信息系统整体安全，省级数据中心应建立安全预警与监管中心，建设与部级上下级联的安全运行维护管理平台、应用安全监测与预警平台和安全工作管理平台。

信息系统在设计规划、建设和运行的整个生命周期中应根据国家信息安全等级保护制度，同步开展信息系统安全等级保护定级、备案、等级测评、建设整改和监督检查等工作，并根据《信息系统安全等级保护基本要求》（GB/T 22239-2008）等国家及行业相关标准规范进行安全保障体系建设。

4.5.2 信息安全方针策略

省级数据中心应结合整体信息安全需求，实现“积极防御、主动防护”，并建立符合国家信息安全等级保护三级要求的总体安全策略，实现信息安全的机密性、完整性、可用性、可控性和不可否认性的安全目标。

4.5.3 安全技术体系

4.5.3.1 基础设施安全

1.物理安全

应根据数据中心机房的总体要求、国家《电子信息系统机房设计规范》（GB 50174-2008）等相关标准进行安全建设，采取门禁、消

防报警、环境动力设施监控管理、视频监控、防雷击和防静电等措施，做好符合要求的电力供应，关键基础设施、设备和磁介质应通过部署防电磁屏蔽机柜等措施建立电磁防护机制。

2.网络安全

(1) 网络结构安全。省级数据中心应根据承载数据的规模、应用系统的重要程度、数据中心的业务和服务功能等划分不同的安全域。安全域应包括应用服务器区域、数据库服务器区域、数据存储区域、前置服务器区域、网络安全管理区域和对外服务区域等，根据“业务资产重要程度相似、业务风险等级相似”等原则进行安全域划分。

(2) 网络核心安全。数据中心网络核心应确保网络数据的处理性能和业务连续性，保障核心业务数据的网络资源冗余，并具有硬件冗余备份机制。

(3) 网络汇聚安全。在网络汇聚安全中应通过 ACL、防火墙实现访问控制机制，确保重要服务器区域之间的安全访问，建立与业务逻辑访问关系相一致的网络访问控制策略，并针对三级区域汇聚边界设置网络入侵检测、网络安全审计等配套安全措施。

(4) 网络接入安全。

① 互联网接入。互联网边界应建立具备冗余机制的边界隔离措施，例如防火墙、防病毒网关、入侵防御等，或具备综合防护能力的统一安全网关。同时根据互联网可能发生的安全威胁合理部署抗 DOS 攻击、负载均衡、带宽管理等措施。

② 教育系统专网接入。教育系统专网包括教育城域网、教育科研网的专网接入应至少部署防火墙、入侵检测和网络安全审计等措施。

③ 第三方接入。其他第三方接入应根据接入的重要程度形成统

一的第三方安全解决区域，部署网络接入边界的防火墙、入侵检测和网络安全审计等措施。

④ 内部服务器和终端接入。在每个网络接入边界应部署用户安全接入系统，控制远程用户的安全接入，并确保与远程接入系统服务之间的安全传输和访问。

(5) 网络传输安全

省级数据中心承载的三级信息系统通过互联网进行远程传输时，应根据实际情况，采用适当的通信传输加密措施，确保网络传输过程的安全性。在部省两级数据中心之间进行数据传输时，应通过IPSEC VPN技术措施进行传输加密，在数据中心服务器与应用终端之间进行数据传输时，应通过SSL VPN技术措施进行传输加密。

(6) 其他安全内容

省级数据中心承载国家信息系统时应设置单独的网络区域，确保系统和数据的安全性，但整体安全应与本省自建及其他应用系统共同搭建信息安全保障体系。

3.主机安全

数据中心服务器主机应建立备份冗余机制，保障系统的持续稳定运行，针对核心重要信息系统应采用主机安全加固系统，建立“三权分立”的访问控制机制，确保系统最小化的访问控制配置实现。

核心服务器应确保采用两种以上的身份鉴别机制，与PKI/CA系统进行结合，运行维护管理可配合堡垒主机，确保实现细粒度的访问控制、敏感信息加密以及日志审计功能。

各类服务器应采用系统补丁管理和防病毒系统提高系统的防护能力，并通过系统配置优化减少自身的安全隐患。对于操作和使用

服务器的业务终端应进行统一的管理，确保业务终端的专业程度，加强终端的自身安全性，包括系统配置优化、防病毒、补丁管理等措施。

4.存储安全

重要数据应采用数据隔离机制，确保数据存储区域的安全性、访问的严格控制和数据的严格使用。

关键和重要业务数据、鉴别信息和重要管理数据要采用加密存储的方式，确保数据的安全性。

数据存储要建立符合数据中心信息系统服务级别的备份恢复机制，确保数据能够在所要求的时限内及时恢复。数据中心三级信息系统的备份恢复要建立异地数据级备份中心或采用第三方异地备份服务，确保每日数据的全备份、异地存储。

4.5.3.2 平台及应用安全

1.平台安全

(1) 数据库系统安全。数据库系统安全是指数据库管理系统的安全性，应采用符合整体信息系统数据支撑的数据库系统，能够承载大型数据的结构化处理和存储。数据库管理系统要实现两种以上的身份鉴别机制，对数据库用户进行权限划分，强制职责分离，实现严格的访问控制，并对敏感数据进行加密处理和存储，同时启动数据库的日志审计功能，保障数据安全。

(2) 中间件安全。业务支撑的中间件系统应启动自身安全配置，并采用漏洞扫描等技术方法对中间件进行评估，能够发现潜在的安全隐患并及时进行加固处理，确保中间件系统的自身安全。保障中间件的原厂商能够支持中间件版本的升级，持续提供确保其安全性和稳定性的服务。

(3) 虚拟主机安全。虚拟机的体系结构本身可以增强虚拟域操作系统的安全性，应当进行合理的设计，通过虚拟机的管理系统加强虚拟机的隔离机制，并配置支持虚拟化的防病毒、入侵检测等机制。

虚拟主机操作系统的运行维护管理要采用两种以上的身份鉴别机制，严格的访问控制和日志审计功能。

2.应用安全

应用系统要设计身份鉴别、访问控制、敏感数据加密、抗抵赖和日志审计等安全功能，符合数据中心的整体技术架构，具体安全技术要求可参见有关教育管理信息化建设应用系统开发安全规范。

应用系统进行数据采集时，应用系统的数据上报终端，应采用SSLVPN、终端认证Key及CA认证证书相结合的方式，保障终端用户的授权认证及数据传输加密，并实现SSLVPN与应用系统的用户身份认证、数据上报安全控制和其他功能的集成。

4.5.3.3 服务交付安全

数据中心在进行应用交付和系统服务时，应采用必要的安全服务机制，确保交付和服务的安全性，包括信息安全风险评估、安全加固、应用代码审计、等级保护安全测评和应急响应等。

在信息系统的建设和运行维护过程中，要通过信息安全风险评估、安全加固和应用代码审计等服务对系统进行安全分析，降低系统自身的脆弱性，提升系统的安全保护能力；同时在出现异常问题和事件时，能够通过应急响应的方式及时进行处理和恢复。

4.5.3.4 电子认证和应用安全支撑系统

应采用电子认证系统，与重要应用系统的身份认证、访问控制、通信安全以及日志审计功能相结合，逐步建立起统一的教育系统信任体系。电子认证和应用安全支撑系统应根据应用系统的实际

安全需求，配置必要的电子证书，同时结合数字签名技术实现抗抵赖机制。通过部署RA中心和本地认证网关，实现PKI/CA系统的措施应用，设置单独的安全区域部署相关的系统设备。

1.电子认证系统

应按照教育部的统一部署，在教育部电子认证系统（CA系统）基础上，建设省级电子认证系统（省级RA系统）。省级电子认证系统通过建设数字证书注册系统方式实现，并通过教育部电子认证系统（CA系统）签发数字证书，二者逻辑关系如图7所示。

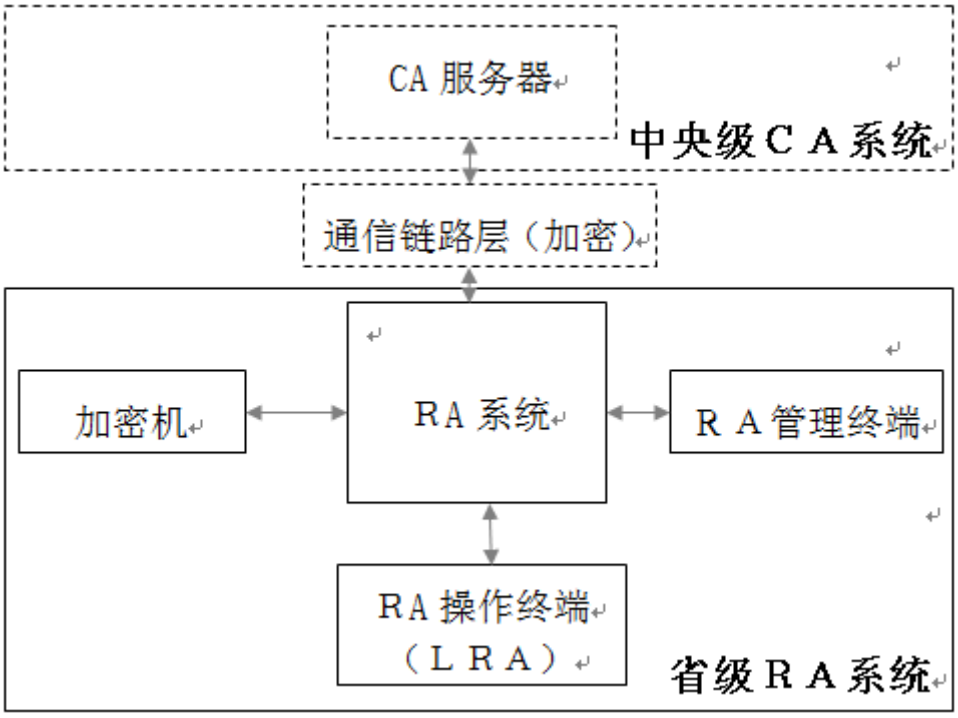

图7 CA系统体系框架

省级RA系统为省级信息系统用户实现证书签发和管理，与应用系统的身份认证、访问控制、通信安全以及日志审计功能相结合，逐步建立起统一的教育系统信任体系。

教育部和省级数据中心进行证书签发的通信网络应采用加密的方式，确保证书签发和资源访问的安全性。

基于省级电子认证系统的证书申请、发放、变更、审核等管理工作应当设置必要的RA操作员、管理员和审核员，全面做好系统的运行维护管理工作，确保系统的安全性。

2.数字证书应用支撑系统

省级信息系统根据实际安全需求，配置数字证书，同时结合数字签名技术实现身份认证和抗抵赖。

通过部署本地身份认证认证网关、签名验证设备、SSL网关等设备，实现PKI/CA系统的措施应用，设置单独的安全区域部署相关的系统设备。

4.5.3.5 安全预警与监管平台

1.安全运行维护管理

省级数据中心结合三级信息系统的安全管理要求，应建立统一的安全运行维护管理平台，能够实现本地计算环境、设备、资源的统一安全监控、告警、安全事件分析、风险管理、综合日志审计和工单管理，能够与中央级安全运行维护管理平台相对接，实现联动，及时上报信息安全事件发生和处理情况。另外，通过统一的安全预警机制，能够及时对信息安全事件提出响应和处置建议。

2.应用安全监测与预警

省级数据中心应配备应用安全监测与预警平台，实现事前漏洞监测，进行实时挂马监测、关键字监测、可用性监测、事后篡改监测，实现安全事件自动通告、安全势态自动跟踪等功能，能够与中央级应用安全监测与预警平台对接，实现联动，及时上报应用安全漏洞、事件发生和处理情况。

3.安全工作管理

各省级教育行政部门应建立安全工作管理平台，实现对信息系统的安全定级备案、差距分析、整改建设、等级测评、监督检查、系统废止等各项工作的全面管理，支持多种方式的查询、分析和统计，并能够与中央级安全工作管理平台对接，实现联动。

4.5.4 安全管理体系

1. 安全管理机构

省级数据中心安全组织应遵循层次化设计原则，分别为信息安全决策层、信息安全管理层和信息安全执行层。设立信息系统安全机制集中管理机构，接受信息安全工作职能部门领导，配备必要的管理和技术人员；负责信息系统安全的集中控制管理，行使防范与保护、监控与检查、响应与处置职能，统一管理信息系统的安全，统一进行信息系统安全机制的配置与管理；适时汇集各种安全机制所获取的与系统安全运行有关的信息；根据应急处置预案作出快速处理；应对安全事件和处理结果进行管理；建立安全管理控制平台，完善管理信息系统安全运行的技术手段；负责接受和配合政府有关部门的信息安全监管工作。

2. 人员安全管理

对于省级教育行政部门内部人员和外部人员，必须结合各省级教育行政部门人力资源管理的实际情况，按照等级保护相关要求进行人员安全管理。重点考虑以下两个方面：

（1） 内部人员安全管理。内部人员管理从人员录用、人员管理、人员考核、保密协议、培训、离岗离职等多个方面都要制定相应的管理制度和规定。建立安全教育和培训制度，定期进行技能考核。

（2） 外部人员安全管理。对于外来人员管理，应包括软件开发商、产品供应商、系统集成商、设备维护商和服务提供商等外来人员，

以及临时因业务洽谈、技术交流、提供短期和不频繁的技术支持服务而临时来访的“第三方”人员。而非临时“第三方”人员指因从事合作开发、参与项目工程、提供技术支持或顾问服务，必须在省级教育行政部门临时工作的“第三方”人员，应制定相应包含访问、安全要求等管理制度。

3. 安全管理制度

结合各类安全管理要求和数据中心面临的实际安全风险，省级数据中心应制定必要的信息安全总体方针、策略、安全管理制度和技术规范，内容覆盖安全管理机构、安全管理制度、人员安全管理、系统建设安全管理和系统运行维护安全管理等相关内容。具体可参考图8。

图 8　省级数据中心安全管理体系框架

4.信息系统建设安全管理

信息系统建设安全管理应当与整体的工程管理相结合，落实“同步规划、同步建设、同步运营”的原则，制定信息系统规划、立项、需求分析、设计、建设、测试、集成等方面的安全管理规定。同时要结合信息系统的开发和部署制定相配套的信息系统安全开发和部署的规范，确保信息系统和数据中心建设过程中的安全。

信息系统建设过程中必须要加强信息安全等级保护工作，通过对信息系统进行定级、备案、等级测评和监督检查等工作落实具体的信息安全等级保护内容。

信息系统正式启动和运行前，必须经过专项安全评估并得到专家或程序的认可，才能正式投入使用。现有信息系统或子系统、信息系统设备需要终止运行的，应采取必要的安全措施，进行数据和软件备份，对终止运行的设备进行不可恢复的数据清除，如果存储设备损坏则必须采取销毁措施，并得到相应领导和技术负责人认可才能正式终止运行。

5.运行维护安全管理

信息系统的运行维护安全管理要实现运行维护管理体系化，对环境、资产、介质、设备进行综合监控管理，对支撑重要信息系统的资源进行监控保护。对于信息系统安全运行维护所需要的密码保护、病毒扫描、变更等事件，必须按照定义好的安全管理策略措施，建立一套运行维护管理制度，并通过培训等方式全面落实。还应通过建立统一的安全预警与监管中心，实现省本级计算环境、设备、资源、应用系统和信息安全工作的统一管理、监控与预警，能够与教育部安全预警与监管平台对接，实现联动，及时上报信息安全漏洞和事件发生和处理情况。

4.6 运行维护与技术服务体系

4.6.1 机构和职责

教育部数据中心、全国集中部署的国家信息系统和中央级部署的国家信息系统的工作统筹和组织管理由教育部教育信息化推进办公室负责；工程实施和运行维护工作由教育部教育管理信息中心负责；业务维护由业务司局负责。

省级数据中心、省级部署的国家信息系统和各省自建系统的工作统筹和组织管理由省级教育信息化主管部门负责，工程实施和运行维护工作由省级教育信息中心（暂无教育信息中心的，明确教育信息技术部门承担）负责，业务维护由业务部门负责。

通过部省两级数据中心运行维护服务体系的建设，构建中央级和省级国家信息系统的统一运行维护服务体系，通过实现运行维护监控平台的对接，整体上形成国家信息系统运行维护一体化体系，具体如图 9 所示。

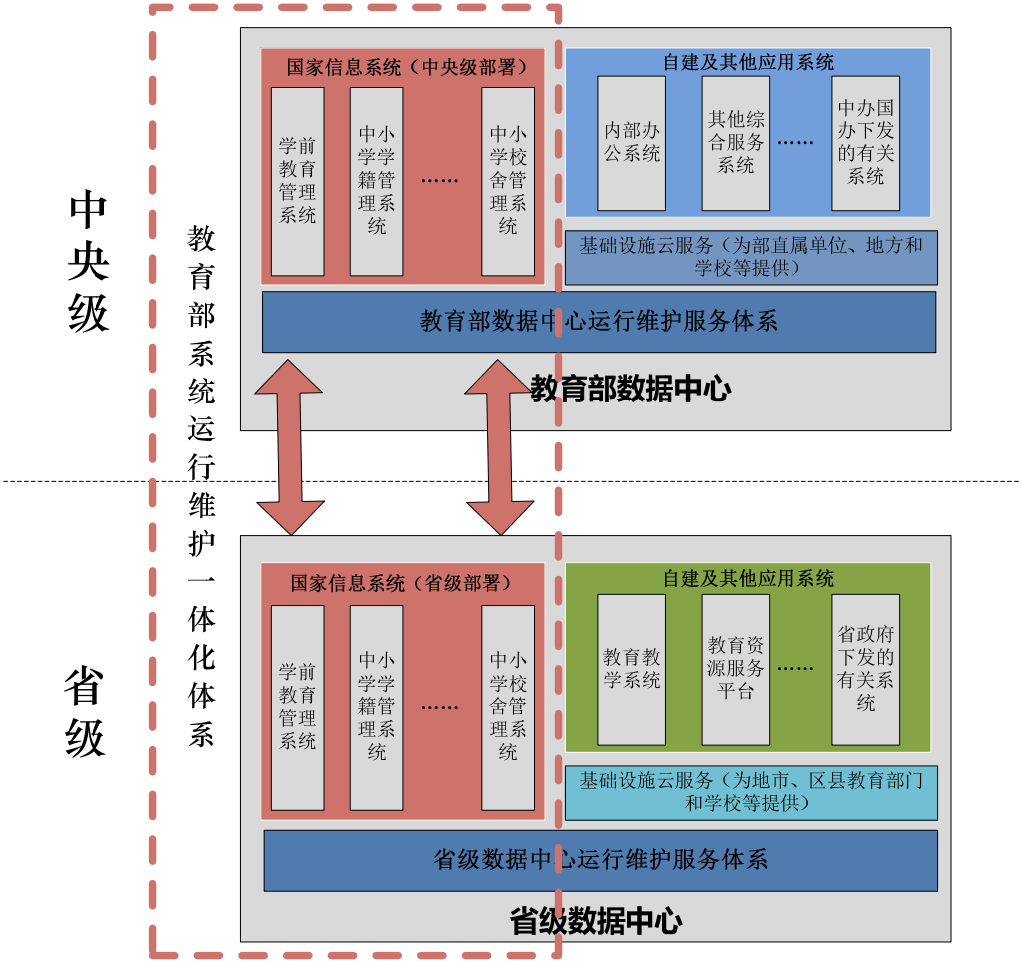

图 9　国家信息系统运行维护一体化体系示意图

4.6.2 运行维护服务体系总体架构

运行维护服务体系由运行维护服务制度、运行维护服务流程、运行维护服务组织、运行维护服务队伍、运行维护技术服务平台以及运行维护对象六部分组成，涉及制度、人、技术、对象四类因素。制度是规范运行维护管理工作的基本保障，也是流程建立的基础。运行维护服务组织中的相关人员遵照制度要求和标准化的流程，采用先进的运行维护管理平台对各类运行维护对象进行规范化的运行管理和技术操作。

1. 运行维护服务制度

根据管理内容和要求制定一系列管理制度，覆盖各类运行维护对象，包括从投产管理、日常运行维护管理到下线管理以及应急处理的

各个方面。此外，为实现运行维护服务工作流程的规范化和标准化，还需要制定流程规范，确定各流程中的岗位设置、职责分工以及流程执行过程中的相关约束。

2.运行维护服务工作流程

应依据管理环节、管理内容、管理要求制定统一的运行维护工作流程，实现运行维护工作的标准化、规范化。其环节包括事件管理、问题管理、变更管理和配置管理。

3.运行维护服务组织和队伍

省级运行维护管理部门应根据其运行维护服务工作的内容和流程确定各项工作中的岗位设置和职责分工，并按照相应岗位的要求配备所需不同专业、不同层次的人员，组成专业分工下高效协作的运行维护队伍。

4.运行维护技术服务平台

运行维护技术服务平台包含实施运行维护和技术服务的各种手段和工具，通过技术手段固化标准化的流程、积累和管理运行维护知识并开展主动性运行维护工作。

4.6.3 运行维护服务体系建设内容

1.运行维护管理制度建设

省级运行维护管理部门应总结现有的运行维护管理经验，遵照国内外相关运行维护标准，结合目前的实际情况，统一制定运行维护管理制度和规范。通过定期和不定期的检查，促进各项制度规范在省级数据中心的贯彻落实，从而建立起统一、规范的运行维护管理工作方式。制度体系内容要涵盖机房管理、网络管理、资产管理、主机和应用管理、存储和备份管理、技术服务管理、安全管理、文档管理以及

人员管理等类别。各类制度具体内容因实际需求而定，至少应包含如下制度：

（1）网络管理制度：包括网络的准入管理制度、网络的配置管理制度、网络的运行/监控管理制度等。

（2）系统和应用管理制度：包括对主机、数据库、中间件、应用系统的配置管理制度、运行/监控管理制度、数据管理制度等。

（3）安全管理制度：包括网络、主机、数据库、中间件、应用软件、数据的安全管理制度及安全事故应急处理制度。

（4）存储备份管理制度：包括备份数据的管理制度和备份设备的管理制度。

（5）故障管理制度：包括对故障处理过程的管理制度、故障处理流程的变更管理制度、故障信息利用的管理制度及重大故障的应急管理制度等。

（6）技术支持工具管理制度：包括对日常运行维护平台、响应中心、运行维护流程管理平台、运行维护知识库、运行维护辅助分析系统等的使用、维护的有关制度。

（7）人员管理制度：包括对运行维护人员的能级管理制度、奖惩制度、考核制度、外部人力资源使用的管理制度等。

（8）考核制度：制定相关制度，对以上各类制度的执行情况进行考核。

（9）其他制度。

随着整个信息化应用内容的不断发展，一些旧的运行管理制度势必不能适应新发展的要求，必须进行不断的改进和完善，并制定相适应的新管理制度，逐步完善管理机制。

2.运行维护管理流程

省级数据中心的运维管理部门依据运行维护管理环节、管理内容、管理要求制定统一的运行维护工作流程，实现运行维护工作的标准化、规范化和自动化。通过建立运行维护管理流程，可以使日常的运行维护工作流程化，职责角色更加清晰，从而使解决问题的速度和质量得到有效提高，实现知识积累和知识管理，并可以帮助运行维护部门进行持续的服务改进，提高服务对象的满意度。运行维护流程包含的环节主要有事件管理、问题管理、变更管理及配置管理。

（1）事件管理。事件是指发生的对运行服务体系某一环节运行造成影响的事件，包括系统崩溃、软件故障、任何影响用户业务操作和系统正常运作的故障、以及影响业务流程的情况，也包括一个用户的请求。对日常性运行维护工作中出现的突发事件（即日常运行维护服务平台自动发现并产生的告警事件）和由用户/维护人员报告的事件会转入事件管理流程。

（2）问题管理。问题是指导致事件产生的原因。问题管理流程着重于消除事件或减少事件发生，确定事件的根本原因，其流程如下：首先，定期分析事件，找出潜在问题，调查问题以找出其原因，制定解决方案、变通方法或提出预防性措施，以消除产生原因，或在重发时使其影响力最小化。其次，记录解决方案、变通方法、预防性措施，根据需要添加到知识库中。再次，提出变更请求，对问题的解决方案进行评估，通过提出变更请求以对该方案进行测试和实施。最后，问题必须进行事后回顾以找出改进机会或总结预防性措施，包括改进事件监测、找出技能差距和文档资料改进等。

（3）变更管理。变更请求通常由于问题的解决方案中需要对生产环境进行某些改变而产生，变更请求来源于问题管理环节或由用户提交。变更管理通过一个单一的职能流程来控制和管理整个信息系统

运行环境中的一切变更，范围可包括软件、硬件、网络设备和文档等的变更，其流程如下。

①由用户或问题管理环节的维护人员提出变更申请，由运行维护负责人检查和完善其内容，并进行风险等级、优先级的初步评估。

②通过分类，确定是否为重大变更、紧急变更，如果是常规变更请求，则由运行维护负责人安排实施；如果是风险等级为“重大”的变更请求，则应上报变更管理小组。

③根据特定的变更请求成立特定的变更管理小组，成员包括对该变更申请有批准权的人员、对该变更的评估和批准提供参考意见的技术人员和管理人员。评估内容包括变更的技术可行性、对系统性能的影响、对现有服务的影响、对资源的需求等。

④变更管理小组评估后决定是否批准变更申请。变更请求得到批准后，运行维护负责人安排相应资源进行变更的计划、测试，并制定实施方案，确定实施时间表，分配相应资源，通知请求人。

⑤相应岗位实施变更，运行维护负责人监视实施过程，并在必要时进行协调。

⑥定期回顾变更管理流程以提高效率和效能，在实施变更流程不久之后，可以进行第一次回顾，以确保流程得到正确实施并达到预期目的。对发现的问题必须追根溯源并尽快解决，之后可以定期举行回顾。

（4）配置管理。配置管理是服务管理的一个核心流程，能确保应用系统及其运行环境中所有设备/系统及其配置信息得到有效完整的记录和维护，包括各设备/系统之间的物理和逻辑关系，从而为实现有效服务管理奠定基础。

配置管理流程着重于管理生产环境中所有必须控制的组成元素，并为其他相关流程(如事件管理等)提供信息，使这些流程更有效地运行，从而确保应用系统环境的完整性和稳定性，其主要流程内容如下：

①识别和维护配置元素：确定需要进行配置管理的元素及所有必需的配置属性，并指明与生产环境中其他配置元素之间的关系。对配置管理数据库提供日常维护。

②配置状态汇总：根据需要定期产生配置管理报表，并能使相关人员进行相关配置的提取、查询，定期产生配置项的状态报告，并能反映配置项的版本和变动历史。

③审计和确认：定期审核全部或部分配置数据库中的配置项，确认其和物理环境的一致性，从而确保配置信息的完整性。

④计划、回顾和改进：定期制定计划(如半年)，以明确下阶段配置管理工作；定期回顾流程和审核结果，找出需要改进的配置项。

⑤配置管理数据库（CMDB）：配置管理数据库由配置识别活动来定义，配置识别活动不但要定义配置项，还需定义配置结构及配置项的相互关系。

（5）其他服务管理。

3.运行维护组织和队伍建设

（1）组织管理。设置运行维护管理部门，负责总体运行维护管理；设置应用服务部门，负责国家信息系统的日常运行和用户服务；设置数据服务部门，负责国家信息系统的采集服务、分析服务。另外，可以外包部分服务，请各承建单位（包括集成商、软件开发商、设备供应商以及其他相关单位）在负责履行售后服务期后，提供运行维护技术支持。

（2）人员管理。对各级运行维护人员尤其是高级运行维护人员的管理，应制定一套切实可行的管理办法，包括人员配置、职责划分、人才库建立、人员培训、人员考核、人员待遇等。通过科学的管理办法和有效的激励机制，充分调动各级运行维护人员的工作积极性和责任心，为做好信息系统运行维护工作打好基础。

4.运行维护技术服务平台

运行维护技术服务平台应由运行维护监控平台、运行维护流程管理服务系统和运行维护辅助分析系统等构成。

（1）运行维护监控平台。建立统一集中的监控平台，将数据中心的基础设施、数据库、信息系统的监控整合在一个平台之上，实现告警显示、告警统计的统一。监控平台也为各信息系统提供监控服务，也可以订阅其业务相关的各种监控报警，通过邮件、短信等形式在第一时间获取业务服务状态的变化。省级数据中心运行维护监控平台要能够实现与中央级运行维护监控平台对接并实现相关数据的报送。

（2）运行维护流程管理服务系统。运行维护流程管理服务系统的建立，一方面可以使日常的运行维护工作有序化，职责角色清晰化，能够有效地提高解决问题的速度和质量，使运行维护部门内的相关支持信息更为畅通、透明、完整，实现知识的积累和管理，更好地进行量化管理和设定优化指标，进行持续地服务改进，最终提高整个运行维护工作的效率和质量。另一方面可以提供所属地区的用户技术服务、本地区的数据采集技术服务。

（3）运行维护辅助分析系统。以运行维护监控平台和运行维护流程管理系统为基础，通过统计分析，了解运行维护服务能力与服务质量的现状，并可以进行趋势分析，为运行维护管理决策提供支持。

附录一　规划内容与测算方法及参考案例

（一）省级数据中心配置测算方法

1.省级数据中心配置测算

表 4　省级数据中心配置测算表

序号	设备类型	每学校/学生所需性能估算	系统规模	同时在线用户数	设备配置总体需求	备 注
1	带宽	0.1MB/学校	N所学校	N×20%	0.02×N MB	2 条链路相互备份，可以采用相同带宽
2	存储系统	20 MB/学生	N万学生		0.2×N TB	
3	备份系统	80 MB/学生	N万学生	N×1%	0.8×N TB	备份系统容量一般为存储系统的4倍
4	数据库服务器	182.85 TPM/学校	N所学校	N×20%	N×36 TPM	采用国际流行的 TPC-C 基准估算
5	中间件服务器	182.85 TPM/学校	N所学校	N×20%	N×36 TPM	参照数据库服务器
6	管理服务器					CPU：2个vCPU 内存：16GB
7	应用服务器		N所学校	N×20%	根据实际需要配置	CPU：4个vCPU 内存：32GB 虚拟机部署

2.服务器需要的处理能力需求计算

假设某省学校规模为1万所，按20%的比例，估算参数：

（1） 单个系统同时在线用户数为2000个（U1）；

（2） 平均每个用户每分钟发出2次业务请求（N1）；

（3） 系统发出的业务请求中，更新、查询、统计各占1/3平均每次更新业务产生3个事务（T1）；

（4） 平均每次查询业务产生8个事务（T2）；

（5） 平均每次统计业务产生13个事务（T3）；

（6） 一天内忙时的处理量为平均值的5倍；

（7） 考虑服务器保留30％的冗余；

（8） 经验系数为1.6(实际工程经验)。

服务器需要的处理能力为：

TPC-C=U1*N1*（T1+T2+T3）/3*经验系数/冗余系数

数据库服务器的处理性能估算为：

TPC-C= 2000*2*（3+8+13）/3*5*1.6/0.7= 365714 TPM

平均每所学校所需的TPC-C值为：365714/2000=182.85 TPM

3.服务器内存估算

该服务器内存主要由操作系统占用内存、数据库系统占用内存、并发连接占用内存等几部分组成。估计参数为：

(1) 操作系统占用约 400MB 内存空间；

(2) 数据库系统占用内存 800MB；

(3) 每个并发连接占用 10MB；

考虑服务器内存保留30％的冗余；

则单台服务器的内存估算为：

Mem=(400MB+ 800MB+ 2000*10MB)/(1-30%)=30GB

（二）按照 500 万学生规模数据中心配置参考示例

本案例包括内容仅含满足国家信息系统部署的配置需求，不含省自建系统和其他系统的运行环境需求。

1．省级数据中心与应用体系总体拓扑结构图

省级数据中心拓扑结构图如下：

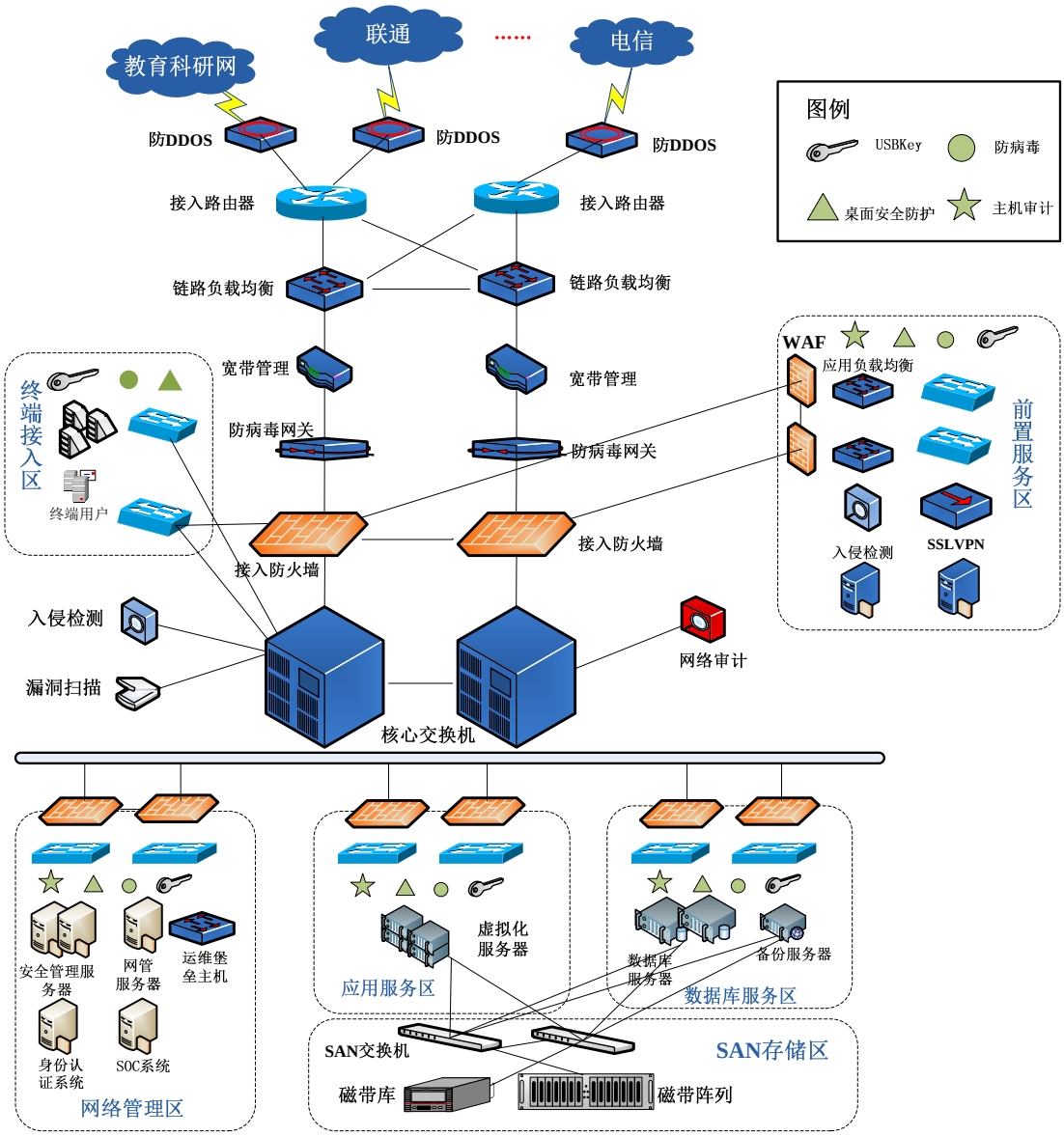

图 10　省级数据中心参考拓扑结构图

2. 工程和设备参考配置

表 5 省级数据中心参考配置清单

序号	类别名称	性能、功能要求	部署位置	数量
一	**基建工程**			
1	机房装修	含机房吊顶、地面、墙面、隔墙、门、辅材等材料费及人工费、机械费	机房	
2	机房电气	含配电柜、电缆、管材、UPS（120KVA）、辅材等材料费及人工费、机械费	机房	
3	机房防雷接地	含避雷器、管线、铜带、辅材等材料费及人工费、机械费	机房	

4	空调新风	含机房专用空调（制冷量 60KW）、新风机、线缆、阀门、辅材等材料费及人工费、机械费	机房	
5	机房安防	含门禁系统、闭路监控系统、半球摄像机、硬盘录像机、线缆辅材等材料费及人工费、机械费	机房	
6	环境监控	含机房供配电监控、UPS 监控、精密空调监控、漏水监控、温湿度监控等材料费及人工费、机械费	机房	
7	机房布线	含超五类线缆、管材、辅材等材料费、人工费、机械费	机房	
8	消防	含感烟探测器、声光报警器、气体灭火控制盘、火灾报警控制器、辅材等材料费及人工费、机械费	机房	
9	KVM	含 8 口、16 口或 32 口 KVM	机房	
二	**硬件设备**			
（一）	**网络设备**			
1	路由器	交换容量 400Mbps，转发性能 200Mpps，双主控板，千兆电口 4 个，千兆光口 4 个，冗余电源	数据中心接入路由器	2
2	核心交换机	整机交换容量 2Tbps，万兆光口 8 个，千兆光口 24 个，千兆电口 48 个，冗余主控板，冗余电源	数据中心核心交换机	2
3	汇聚交换机	交换容量 200Gbps，千兆光口 24 个，千兆电口 24 个，冗余电源	前置服务区、应用服务区、数据库服务区、网络管理区等	10
4	链路负载均衡设备	硬盘 80 GB；设备标配 4 个千兆电口；双电源； ATX 自动切换；TCP 并发会话数 6M,L7 RPS 2M,单向吞吐量 5G,L4 CPS 300K	接入链路上	2
5	应用负载均衡设备	吞吐量 1Gbps，硬件 SSL 加密，内存 4G，千兆电口 4 个，千兆广口 2 个	前置服务区	1
6	IPSec VPN 设备	吞吐量 5G,并发连接 200 万，5000 个 vpn 隧道，冗余电源	与教育部数据中心通信网络边界	2
7	SSL VPN 设备	千兆设备，支持 5000 用户并发	前置服务区	1
8	终端认证 Key	集成实现 SSLVPN 证书、用户认证证书	配发至各应用终端用户	30
9	带宽管理系统	吞吐量 2G，并发 200 万，2 个千兆光口，4 个千兆电口	接入链路上	2
（二）	**服务器和计算机设备**			
1	服务器 1	4 路或八路(每颗 8 核/10 核，双线程，大缓存)，128G 内存，配置 512MB Cache，独立 8 通道 SAS RAID 卡，RAID10+热备盘、RAID5，硬盘 5 块 600G,配置 4 个千兆以太网口,HBA 卡 8GB 两块，支持虚拟化技术 扩展卡：双端口 8Gb 光纤通道 HBA 卡，双端口 40GbInfiniBand 接口卡等可选，支持热插拔	web、应用、中间件等	25

2	服务器 2	4 路或 8 路 CPU,（每颗 CPU 为 8 核/10 核，双线程，大缓存），256G 内存，配置 512MB Cache，独立 8 通道 SAS RAID 卡，RAID10+热备盘、RAID5，硬盘 5 块 600G，配置 4 个千兆以太网口，HBA 卡 8GB 两块，支持虚拟化技术 扩展卡：双端口 8Gb 光纤通道 HBA 卡，双端口 40GbInfiniBand 接口卡等可选，支持热插拔	数据库服务器	6
3	服务器 3	1 路 4 核，4G 内存，硬盘 3 块 500G，RAID 卡，配置 4 个千兆以太网口	认证、管理、备份等	8
（三）	**存储备份设备**			
1	存储主机	双控制器、配置 8Gbps 光接口 4 个、支持 70T 存储容量	应用、中间件、数据库、备份	1
2	光纤交换机	16 个光口，8Gbps 光模块 16 个	存储区域	2
3	带库	双控制器、配置 8Gbps 光接口 4 个、支持 300T 存储容量	应用、中间件、数据库、备份	1
（四）	**安全设备**			
1	防火墙	吞吐量 10G，千兆设备，4 个千兆电口，4 个千兆光口，支持万兆口	各区域边界互联网接入链路	8
2	防 DDOS 设备	2U,含交流冗余电源模块,1*RJ45 串口,4*GE 电口（Bypass），2*SFP 插槽。25 IP 许可证	接入链路上	2
3	防病毒网关	HTTP 吞吐率 400Mbps，6 个 10/100/1000M 自适应电口，4 个 SFP 光口插槽（不含模块），1 个 RJ-45 串口，内置 2 路硬件 Bypass	接入链路上	2
4	应用防火墙	千兆高端 WEB 应用防火墙系统，网络吞吐量为 4Gbps，HTTP 新建 连接数大于 10000/s，HTTP 并发连接数 80 万，冗余电源，标准配置 6 个千兆 SFP 插槽，6 个 10/100/1000M 自适应电 口，1 个 Console 口，2 个 USB 口	前置服务区	2
5	网络审计系统	旁路部署，千兆引擎、1U 上架专用设备、2 千兆电口监听、4 个 SFP 千兆插槽、1 个千兆管理口，最大支持 4 个监听口、需配置相应授权及 SFP 模块支持电口或光口，支持 Oracle、SQL-Server、网络邻居、Telnet、FTP、HTTP 等协议的网络审计	部署在服务区的汇聚交换机上	2
6	入侵检测设备	具备 1 个管理口电口、可用于监听的有 4 个 GE 口和 4SFP 插槽；默认为 1 个监听口授权，最大可扩展到 4 个监听口授权一台，网络引擎软件一套，控制中心软件一套	部署在核心交换机上	2
7	漏洞扫描设备	授权可扫描总数量为无限 IP 地址或域名,含交流单电源,一个 100M/1000M 自适应以太网电口，一个管理口，并发 60IP 扫描	部署在核心交换机上	1
8	认证系统	支持制作、发放证书等功能，支持与应用系统进行访问控制联动	管理区	1
9	堡垒主机	30 台服务器以上授权，适用于对 IT 管理人员远程服务器运行维护操作的审计管理。包括身份认证、授权和操作审计等	管理区	1
三	**软件**			

（一）	**系统软件**			
1	操作系统			
（1）	Linux		数据库服务器	40
（2）	Windows Server		web、中间件、应用、管理与备份服务器	30
2	公用软件			
（1）	应用服务器中间件	为复杂应用提供了一个简便、快速的开发和运行平台，对于分布式的企业级应用，提供了易扩展、可伸缩和高安全性等特性。包含J2EE基本服务（JNDI,JTA,JDBC,RMI/IIOP）及Web服务;JCA，EJB，Web Services，JMS;管理控制台（配置、监控等）。国家信息系统采用Weblogic。		
（2）	综合门户	省级教育管理公共服务门户要集成省级各应用系统并集成展示教育基础数据，实现省级单点登录。	由各省定制开发	
（3）	目录服务		教育部配发	
（4）	数据交换与共享平台	数据交换与共享平台实现部、省两级间的数据交换，实现省内教育基础信息数据库与业务系统应用数据库间的数据共享。	教育部配发	1
（5）	应用系统支撑平台	提供基础服务支撑，包括业务支撑服务、安全支撑服务、数据支撑服务、技术服务组件、运行支撑平台，促进各应用系统进行有效的整合和协同。	教育部配发	1
（6）	教育基础信息数据库管理与服务系统		教育部配发	1
（7）	报表工具	提供报表服务，统计分析、打印、打印预览、数据导出等功能，还提供独有的报表查询	教育部配发	
3	工具软件			
（1）	备份软件	支持50个操作系统、2个数据库、40个应用、2个阵列、2个带库驱动器	存储区域	1
（2）	虚拟化和云计算管理软件	虚拟化和云计算管理软件	web、应用、中间件等服务器	1
	运行维护监控软件	运行维护监控		
4	数据库软件			
	数据库软件	具有完整的数据管理功能,完备关系的产品，实现了分布式处理功能，支持实时应用集群 Oracle MS SQL Server	数据库服务器	2
5	应用系统软件			
	应用系统软件	20个主要信息系统部署和实施，扩展升级开发		20
（二）	**安全软件**			
1	主机审计系统	支持100台服务器，漏洞库3年升级服务	web、应用、中间件等服务器	1
2	防病毒系统	网络版防病毒系统，支持100台服务器，病	web、应用、中	1

		毒库 3 年升级服务	间件、管理、备份等服务器	
3	统一安全运行维护管理平台	支持网络、安全、主机等设备的综合统一管理、系统运行情况监控等 ，支持 200 个节点	网络管理区	1
4	信息安全工作管理平台	实现对信息系统的安全定级备案、差距分析、整改建设、等级测评、监督检查、系统废止等各项工作的全面管理，并能够与部级安全管理工作信息化平台相衔接，实现数据上报	应用服务器区	1
5	远程安全监测系统	实现对重要网站和信息系统的远程安全监测，重点监测各类安全漏洞和篡改、暗链、断链等安全事件，做到实时预警。	网络管理区	1
6	桌面系统应急响应系统	实现操作系统崩溃启动排除故障、系统清洗、自动排除故障、系统盘木马病毒清除等功能，支持 100 个 PC 端和 16 个服务器端。	web、应用、中间件、管理、备份等服务器	1
7	密码安全服务平台	密码安全服务平台由两部分组件构成： 密码安全服务平台软件 1 套，用于与应用系统进行接口开发与密钥管理； 加密设备 2 台，采用冗余的模式实现数据加密。		1
8	SSLVPN 集成开发	实现 SSLVPN 与省级系统的用户身份认证、数据上报安全控制和其他功能的集成		1

3．建设经费估算

表 6 省级数据中心参考经费预算

单位：万元

序号	费用名称	投资概算	合 计	说 明
总 计		4770		
（一）	基建工程	**200**		
（二）	硬件设备购置费			
1	网络设备	330		
2	服务器设备	700		
3	存储设备	350		
4	安全设备	250		
	小计	**1630**		
（三）	软件购置费			
1	系统软件	800		
2	安全及其他软件	500		
3	应用、数据与门户集成， 应用系统软件开发改造	700		
	小计	**2000**		
（四）	网络系统集成费(二、三)	**200**		
（五）	安全服务与等级测评费			
1	安全咨询服务费	100		
2	等级测评费	100		

	小计	**200**		
（五）	其他工程和费用			
1	建设管理费	60		
2	设计费	60		
3	招投标费	60		
4	工程监理费	120		
5	培训费	60		
6	其他	80		
	小计	**440**		
（六）	项目预备费	**100**		

4．运行维护经费测算

运行维护经费是省级数据中心可靠运行的重要保障。本指南根据业界的测算标准，结合教育系统实际需求和实际情况，省级数据中心运行维护经费测算如表 7 所示。供各省在建设过程中参考。

表 7 省级数据中心运行维护经费测算

项目	标准	金额（元）	说明
人员经费	100000 元/人年	2500000	含福利费用，工作人员为 25 人
办公经费	1000 元/人月	300000	办公经费按 1000 元/人月测算，
设备维修与配件	投资额×1.5%	240000	设备总投资额为 1630 万元
服务外包与系统软件升级	投资额×4%	800000	系统软件购置费用为 2000 万元
应用系统升级	投资额×5%	350000	应用系统总投资额为 700 万元
安全评估加固与等级测评费	按照服务量估算	1200000	安全评估加固 60 万元，等级测评费按照复测整体打包价 60 万进行估算。
硬件设备更新	投资额×3%	480000	设备总投资额为 1630 万元
线路租赁费	180000 元/条	360000	线路租赁费用按 2 条，每条年租金 18 万元
培训费	投资额×0.4%	190000	按建设总费用 4770 万元的 0.4%计算
电费	设备台（套）*1KW*1 元/KW*365*24	550000	共 63 台设备
合计		6970000	

附录二　统一规划的国家信息系统一览表

大类	信息系统
EIS01 教育规划与决策支持类信息系统	EIS0101 教育规划与建设地理信息系统
	EIS0102 教育统计信息系统
	EIS0103 教育决策支持系统
EIS02 学生管理类信息系统	EIS0201 学前教育学生管理信息系统
	EIS0202 中小学生管理信息系统
	EIS0203 中等职业学校学生管理信息系统
	EIS0204 高等教育学生管理信息系统
	EIS0205 学生资助管理信息系统
	EIS0206 学生体质健康标准数据管理与分析系统
EIS03 教师管理类信息系统	EIS0301 教师管理信息系统
	EIS0302 教师专项业务管理信息系统
EIS04 学校资产及办学条件管理类信息系统	EIS0401 学前教育机构资产及办学条件管理信息系统
	EIS0402 中小学学校资产及办学条件管理信息系统
	EIS0403 中等职业学校资产及办学条件管理信息系统
	EIS0404 高等教育学校资产及办学条件管理信息系统
EIS05 其他业务管理类信息系统	EIS0501 涉外管理信息系统
	EIS0502 语言文字工作管理与服务平台
	EIS0503 科技评价与专利服务系统
	EIS0504 国家教育考试考务管理与安全保障系统
	EIS0505 教育政务系统