# 基于云计算的数字政府架构下政务服务的数据安全管理机制研究

曾宇 李慧琳 滕思翰 王松 于浩波

1 内蒙古自治区大数据中心，内蒙古自治区呼和浩特市新城区，010010；

2 内蒙古自治区金融运行监测中心，内蒙古自治区呼和浩特市新城区，010010；

**摘要：**云计算技术深度应用于数字政府建设，重构了政务服务模式且提升了治理效能，但政务数据安全面临跨界融合引发的系统性风险，立足云计算技术特性和政务数据治理需求，本文系统剖析数字政府架构下政务数据安全的现实状况并从技术防护、管理规范、法律保障、协同治理这四个方面构建立体化安全管理机制，研究显示，要以技术创新筑牢安全根基、通过管理优化完善制度框架、靠法治建设明确权责界限、借多元协同凝聚治理力量以构建覆盖数据全生命周期的安全防护体系，为数字政府建设提供可操作的安全治理方案。

**关键词：**云计算；数字政府；政务服务；数据安全

**DOI：**10.69979/3041-0673.25.07.099

## 引言

国家“十四五”数字经济发展规划深入实施，数字政府建设以云计算为核心架构全面推进，由于云计算技术资源虚拟化、服务集约化、部署弹性化，能有效破解政务信息系统“数据孤岛”难题，推动政务服务从“线下分散办理”向“云端协同治理”转型，但政务数据在云端存储、跨域流转、融合应用时，面临着数据主权界定模糊、安全责任划分不清、技术防护体系不健全等新挑战，《“十四五”国家政务信息化规划》明确构建“云网数端”协同的安全防护体系，只有从理论层面厘清云计算环境下政务数据安全核心要素，从实践维度构建适配新型政务架构的数据安全管理机制，才能筑牢数字政府建设安全屏障。

## 1 基于云计算的数字政府架构下政务服务数据安全现状

### 1.1 政策法规体系化构建初具成效

在我国，以《数据安全法》《个人信息保护法》为核心，《关键信息基础设施安全保护条例》《政务信息资源共享管理暂行办法》等相配套的法规体系已形成，明确了数据分类分级保护、跨境流动管理、安全责任追溯等基本制度，并且地方政府根据“一网通办”“一网统管”建设需求出台了《政务数据安全管理办法》《公共数据开放安全规范》等实施细则，建立了数据安全评估、风险监测、应急处置等操作规范，推动政务数据安全管理从原则性规定向精细化治理过渡。

### 1.2 技术防护体系呈现智能化特征

基础设施层靠虚拟化安全技术，用内存隔离、镜像加密等法子保障虚拟环境安全且通过云防火墙、入侵检测系统对网络流量细粒度管控，数据处理层中，动态脱敏技术自动识别敏感字段并变形处理，区块链技术凭借分布式账本让数据操作可追溯且人工智能算法实时分析异常访问行为，应用服务层，零信任架构（Zero Trust Architecture）达成“持续验证、最小授权”的访问控制，联邦学习技术在保护数据隐私的情况下完成跨域协同计算，从而形成覆盖“云-网-端”的立体化技术防护体系。

### 1.3 管理体制机制建设逐步规范

首席数据官（CDO）制度在中央及地方政府被普遍设立，由其统筹数据安全与发展事宜，数据安全管理委员会、跨部门协调小组等议事机构被建立，从而形成“业务部门数据确权-技术部门安全防护-监管部门监督评估”的分工协作机制。制度建设上，数据分类分级指南、安全审计规范、容灾备份标准等配套文件不断出台，政务云平台安全准入、第三方服务商资质审查、数据共享安全评估等管理流程走向标准化且工作人员安全意识培训、数据安全应急演练常态化。

## 2 基于云计算的数字政府架构下政务服务数据安全问题分析

### 2.1 数据存储安全面临多重威胁

云端数据中心存在物理安全风险，如自然灾害会使基础设施损毁且人为操作失误能引发存储系统故障，虚拟化技术有“共享风险”，同一物理服务器的虚拟机可能因隔离机制失灵而出现数据越界访问情况，备份恢复体系存在不足，一些机构未建异地灾备中心且增量备份策略不合理，造成恢复时间目标和恢复点目标不达标，并且历史数据归档与销毁流程缺少规范管理。

### 2.2 数据传输安全存在链路隐患

在网络传输时面临中间人攻击、DNS 劫持、SSL/TLS 协议漏洞等威胁，政务云与第三方平台做数据交互有接口安全风险，并且多云架构下跨服务商进行数据迁移会面临格式不兼容、加密算法冲突等状况，跨境数据流动因各国安全审查标准不同而受限制有合规性风险，物联网设备接入政务云时身份认证机制薄弱可能出现终端劫持事件而成为数据泄露的新入口。

### 2.3 数据访问安全存在管理漏洞

传统用户名/密码认证方式破解起来不难且生物特征识别技术有模板泄露的危险，多因素认证（MFA）在移动端应用的时候会有兼容性方面的问题，基于角色的访问控制（RBAC）权限颗粒度不够且部分业务系统还在用“一刀切”的授权模式而没有做到基于数据标签的动态权限管理，云计算服务商内部人员也许会凭借管理权限获取数据访问日志从而有数据被滥用或者泄露的潜在风险。

### 2.4 数据共享开放存在治理困境

统一安全标准在跨部门数据共享方面是缺乏的，并且 XML/SOAP 之类的传统数据交换协议有安全方面的不足，全链路加密在 API 接口调用时并未达成，在公共数据开放进程里，静态脱敏技术应对不了由动态组合查询引发的隐私泄露问题且数据开放平台的访问流量监控和异常行为预警机制需要完善，数据共享中的主权归属、利益分配、责任追溯等问题界定得不够清晰，“不敢共享、不愿共享、不会共享”这种现象依旧存在。

### 2.5 服务商安全管理存在信任鸿沟

ISO27001 等安全认证不全、漏洞扫描不及时、应急响应团队缺位等问题在部分中小云计算服务商中存在，并且政府部门与服务商之间安全责任划分不清晰，数据主权归属、跨境流动规则、违约赔偿机制等合同核心条款存在法律盲区，服务商持续监管机制缺失，安全能力评估仅停留在准入阶段，动态风险评级与退出机制尚未建立。

表 1 数据安全风险分类与具体描述

| 数据安全风险分类 | 具体风险描述 |
| --- | --- |
| 数据存储安全风险 | 云端数据中心物理灾害/人为故障风险、虚拟化环境数据隔离失效、备份恢复策略不完善 |
| 数据传输安全风险 | 网络攻击导致数据篡改窃取、多云架构兼容性问题、跨境数据流动合规性风险 |
| 数据访问安全风险 | 身份认证缺陷、权限管理粗放、服务商内部人员权限滥用 |
| 数据共享开放安全风险 | 跨部门共享机制缺失、开放数据隐私泄露、数据主权与责任界定模糊 |
| 云计算服务商安全风险 | 技术漏洞管理滞后、安全管理能力参差、服务合同责任条款缺失 |

## 3 基于云计算的数字政府架构下政务服务数据安全管理机制构建

### 3.1 技术机制：构建主动防御的安全技术体系

#### 3.1.1 全链路数据加密机制

存储环节里，结构化数据字段用国密算法（SM4）来加密且非结构化数据的版权信息靠数字水印技术嵌入，传输环节中，部署国密 SSL 证书让 HTTPS 加密传输得以实现且应用层运用安全断言标记语言（SAML）达成跨域身份验证，密钥管理方面，硬件安全模块（HSM）使密钥生命周期自动化管理得以实现并且还建立密钥使用审计日志与异常熔断机制。

#### 3.1.2 智能访问控制体系

构建“认证-授权-审计”三位一体架构：多因子认证技术（像生物特征、动态令牌、设备指纹等）被融合进身份认证里以实现登录场景的风险自适应评估，权限管理采用基于属性的访问控制（ABAC）模型并通过结合数据标签、用户行为轨迹来实施动态授权，访问审计利用大数据分析建立用户行为基线以实时识别异常访问模式并触发预警。

#### 3.1.3 弹性容灾备份体系

构建起“本地备份+异地灾备+云端归档”的三级架构，核心数据利用实时复制技术保证 RPO 为 0 且重要业务系统凭借灾备演练达成 RTO 不多于 15 分钟，运用数据去重与压缩技术削减存储成本并制订有差异的备份策略（每周进行一次全量备份，每小时进行一次增量备份），建立历史数据分级销毁制度以使数据生命周期

处于可管控状态。

3.1.4 动态安全监测机制

云安全态势感知平台被部署，集成威胁情报共享、漏洞扫描、入侵检测等功能且通过机器学习算法实现安全事件的智能关联分析。数据流动监测模型被建立，负责跨域数据交互的流量监控、协议分析、内容审计并实时识别数据泄露、越权访问等安全事件且自动阻断。

## 3.2 管理机制：建立全生命周期的制度规范体系

3.2.1 数据分类分级管理机制

《政务数据分类分级指南》被制定出来，数据被划分为核心政务数据（像涉密文件）、重要业务数据（像公民个人信息）、一般共享数据（像政策解读文件）这三类且相应设置绝密、机密、秘密这三级安全防护等级，数据资产清单被建立并明确每类数据的责任主体、存储位置、共享范围和安全防护措施，从而达成“一数一标、一标一策”的精准管理。

3.2.2 安全管理制度闭环

全周期管理体系涵盖“规划-建设-运行-评估”，构建这个体系时，项目规划阶段要同步设计安全方案并进行安全合规性评审，建设阶段得落实“三同步”原则即安全设施与主体工程同步设计、同步实施、同步使用，运行阶段需建立安全巡检日志、事件处置台账、定期评估报告制度，评估阶段要引入第三方机构开展安全成熟度测评并建立问题整改闭环管理机制。

3.2.3 人员安全管理体系

数据安全“三员”（系统管理员、安全管理员、审计管理员）管理要实施起来并且岗位分离与相互制衡机制也要建立，分级分类培训得开展起来并且新入职人员得通过数据安全准入考试且关键岗位人员每个季度都要接受专项培训，若年度安全意识考核不合格则数据访问权限就得暂停，离职人员数据权限回收机制要建立起来并且离职前 48 小时内得把账号注销掉且权限也得回收，重要岗位要进行脱密期管理。

## 3.3 法律机制：完善权责清晰的法治保障体系

3.3.1 专项立法与标准建设

《政务数据安全条例》应被推动出台，在云计算环境下明确数据收集的“最小必要”原则、数据共享的“分类授权”规则、数据开放的“分级脱敏”标准，且配套文件如《政务云服务商安全准入规范》《跨部门数据共享安全技术标准》等也需制定，从而构建起“法律-行政法规-部门规章-技术标准”四级规范体系以解决当下制度供给碎片化的问题。

3.3.2 多元主体责任界定

政府部门作为数据主权主体要明确管理责任并建立数据安全责任清单，云计算服务商身为数据处理者需承担技术保障、风险报告、违约赔偿等义务且在服务合同里细化数据泄露违约责任（像按照数据资产价值的一定比例设定赔偿标准），数据使用方得遵循“目的限定”“使用留痕”原则并建立第三方合作安全评估机制以防范合作过程中的二次泄露风险。

3.3.3 执法监管能力建设

跨部门数据安全监管联盟要组建起来并且“双随机一公开”抽查机制得建立，重点对数据跨境流动备案、重要数据出境安全评估等落实情况加以检查，全国统一的政务数据安全监管平台要建设从而实现安全事件的实时监测、智能分析、快速处置，违法违规行为联合惩戒机制得建立且将服务商安全失信行为纳入信用体系以提高数据安全违法成本。

## 3.4 协同机制：打造多元共治的生态治理体系

3.4.1 政府部门内部协同

跨部门数据安全联席会议制度由政务数据主管部门牵头建立，网信、公安、保密等部门参与其中，统筹协调数据共享安全规则制定、重大安全事件处置等工作；跨层级安全协同平台被建设起来，实现国家、省、市三级安全策略的自动同步与联动响应，施行疫情数据共享、应急指挥等场景中的安全协同管控。

3.4.2 政企合作治理机制

“监管沙盒”试点机制被建立起来，服务商被允许在受控环境里测试新型安全技术（像隐私计算、零信任架构）等技术成熟之后将其纳入政务云安全技术目录，安全能力共享平台被构建起来，服务商的威胁情报、漏洞库、应急资源被整合从而形成“政府监管+企业服务+技术创新”的良性互动，安全责任共担模式（Shared Responsibility Model）被推行，政府负责数据分类与权限管理、服务商负责基础设施安全被明确从而形成“边界清晰、责任明确”的协同防护格局。

3.4.3 社会力量参与机制

公众数据安全投诉举报平台得建立起来且“12345”热线、政务邮箱等反馈渠道要畅通并对有效举报予以奖

励，行业协会要被引导着去制定数据安全自律公约、开展服务商安全能力星级评定以促使市场择优机制形成，借由“数据安全宣传周”“政务开放日”等活动向公众普及数据安全知识来提升个人信息保护意识并构建“政府主导、企业主责、社会参与”的共治生态。

表 2 数据安全管理机制与具体措施

| 数据安全管理机制 | 具体措施 |
| --- | --- |
| 技术机制 | 智能访问控制方面有 ABAC 模型和动态权限管理并且全链路加密涵盖国密算法应用与密钥生命周期管理，弹性灾备包含三级备份架构和演练机制，还有态势感知中的智能监测和威胁关联分析。 |
| 管理机制 | 分类分级（构建三分类三级防护体系）以实现制度闭环（涵盖全周期管理与合规性评审），在人员管理方面设有三员制度和培训考核体系。 |
| 法律机制 | 专项立法包含条例和标准体系且责任界定涉及主权主体、处理者和使用者的权责且执法监管涵盖联合监管与信用惩戒。 |
| 协同机制 | 内部有联席会和跨层级平台的协同、政企有监管沙盒与责任共担的协同、社会有公众参与和行业自律的协同。 |

## 5 结论与展望

数字政府深度融合云计算技术，使得数据安全管理不再是单一技术防护而走向体系化治理。本文构建的技术、管理、法律、协同四维机制能够应对云计算环境下数据安全特殊挑战且符合政务数据治理现实需求。未来研究可聚焦探索区块链技术用于数据主权确权、共享溯源的路径、研究量子计算给现有加密体系带来的潜在威胁与应对策略以及构建基于安全成熟度模型（SMM）的政务云安全评估体系等方向，持续完善安全管理机制能给数字政府建设营造“安全可控、开放共享”的发展环境从而有助于国家治理体系和治理能力现代化。

## 参考文献

[1]徐晓林,明承瀚,陈涛.数字政府环境下政务服务数据共享研究[J].行政论坛,2018,25(1):10.DOI:10.3969/j.issn.1005-460X.2018.01.009.

[2]董倩.数字政府背景下政务数据共享机制优化研究[J].中文科技期刊数据库（文摘版）社会科学，2024(2):0109-0112.

[3]敖道恒.基于网络空间安全保障下"数字政府"政务云建设研究分析[J].2021.