基于电子政务云的网络安全架构治理探讨

王西元　陈　云
（台州复星办公设备有限公司 浙江 台州 318000）

摘　要　随着云计算技术的不断发展，各政府部门也主动将云计算技术应用到电子政务网络系统中，并主动构建了电子政务云系统，这为政府部门的信息处理、公众服务等工作的开展提供了便利，但也对网络安全提出了更高的要求。需要基于电子政务云的实际运行需求，构建电子政务网络安全体系，充分发挥出电子政务云的优势，满足电子政务的需求。文中对基于电子政务的网络安全架构治理体系进行了探究与分析。

关键词： 电子政务云；网络安全；架构治理
中图分类号　TN915.08

Discussion on Network Security Architecture Governance Based on E-government Cloud

WANG Xiyuan and CHEN Yun
（Taizhou Fuxing Office Equipment Co.,Ltd.,Taizhou,Zhejiang 318000,China）

Abstract　With the continuous development of cloud computing technology,various government departments also take the initiative to apply cloud computing technology to the e-government network system,and take the initiative to build an e-government cloud system,which provides convenience for the development information processing and public services of gove rnment departments, but also puts forward higher requirements for cyber security issues. It is necessary to build an e-government cyber security system based on the actual operation requirements of e-government cloud,give full play to the advantages of e-government cloud,and meet the development needs of e-government. This paper explores and analyzes the cyber security architecture governance system based on e-government.

Key words　E-government cloud,Network security,Architecture governance

0　引言

随着数字化技术的不断发展，网络安全在“数字政府”建设中取得了良好的应用效果，各政府部门也主动开始了电子政务云的创建，这对提高政府部门的社会服务能力有着重要意义。但在电子政务云运行期间，网络安全突发事件也在不断增加，一系列安全问题逐渐显露。因此，需从电子政务云的总体框架与安全需求出发，做好网络安全架构工作，强化电子政务云的安全治理工作，发挥出电子政务云的社会服务价值。

1　电子政务云的网络安全需求

1.1　数据安全需求

应用电子政务云能将信息技术与政务办公工作紧密结合在一起，也能充分体现出“数字政府”的建设概念。在电子政务云中，有着重要的政务应用，其存储着大量的政务数据。在网络安全架构中，不仅需要考虑是否具备良好的安全防护体系，还要形成严格的内部管理体系，以保障云政务应用工作的稳定运行，避免用户数据被泄露。只有做好数据安全管理工作，才能保证电子政务云的安全性与稳定性。因此，在探讨网络安全需求时，需要充分考虑电子政务云的数据安全性，减少外界因素对数据的安全威胁，保障电子政务云的运行质量。

电子政务云中存储着大量的政务数据，数据作为生产要素，虽然能提高政务工作的效率，但也存在一定的安全风险。在明确数据的安全防护需求时，应针对数据传输、交换、损毁等数据管理全生命周期做好安全防护工作，还应充分考虑各类数据的备份与灾害恢复问题，提高政务数据的安全管理效果。

1.2　使用边界的安全防护需求

基于电子政务云，公众、政府人员与企业可以通过互联网技术手段直接访问政府应用，但其边界出口还存在较高的安全风险隐患，具体体现在可能出现用户非授权访问、DDos 恶意流量攻击、恶意代码等诸多安全威胁[1]。因此，

作者简介：王西元（1970—），专科，初级助理工程师，研究方向为信息系统；陈云（1979—），专科，研究方向为信息系统。

在电子政务云的安全防护中，可以通过建设互联网业务区的方式，合理布设边界防护设备，对电子政务云的边界进行安全防护，提高电子政务云的安全性。在默认情况下，电子政务云中的政务应用与部署区域之间不允许互相访问，因此在政务应用期间，需通过身份认证、访问控制等方式，做好数据访问环节的安全管理工作。在安全防护需求的搭建中，可以通过安全管理中心实现对威胁情报的应急响应，对漏洞状态进行实时监测，提高安全防护工作的整体水平。

2 安全管理框架的搭建要点

国家及地方政府部门在建设电子政务云的过程中，需以《网络安全登记保护2.0》为指导思想，从安全技术、安全管理等多方面入手，进行电子政务云的安全模型设计工作。在电子政务云安全层次模型的构建中，需构建安全管理体系、安全运维体系、标准与规范体系等，提高电子政务云的安全防护水平。

2.1 安全管理中心搭建

安全管理中心作为开展统一管理的平台，涉及系统管理、安全管理、安全审计、集中管控等多个方面。在安全管理中心中，应做好系统的安全运维管理工作，对于运维区域内的边界设备，应做好与物理资源层的基础设施开展数据交互的管理工作，实现对各类安全数据的集中监测与集中化管理[2]。

在搭建安全管理中心时，通过安全的通信网络，可通过网络接口、API接口、WEB服务接口等，对电子政务云提供的各类计算环境进行综合访问，如基础设施层、服务层等。在控制基层设施层的物理资源时，需参考《网络安全等级保护2.0》中的物理环境安全要求。因为服务层需要为电子政务云提供各种软件与组件，基础设施提供者与政府租户应结合服务模式的差异，划分责任范围。在基于IaaSde的服务中，由政府租户负责网络与主机安全，做好软件平台安全、应用安全与数据安全的管理工作，基础设施提供者则负责虚拟化资源安全层和物理资源安全层。在基于PaaS开展各项服务活动时，应由政府租户做好应用安全与数据安全管理工作[3]。基础设施的提供者需要做好虚拟化资源安全层、物理资源安全层、网络与主机安全、软件平台安全的管理工作。因此，政府租户应负责做好各类数据安全管理工作，让基础设施提供者做好网络与主机安全管理工作，搭建效果良好的安全管理中心。

2.2 安全管理体系搭建

安全管理体系的搭建也是电子政务云网络安全架构中的重要内容，只有做好安全管理体系的搭建工作，才能保障电子政务云与各类云服务均处于持续安全与稳定运行的状态。在安全管理体系的搭建中，相关安全管理部门需基于《网络安全等级保护2.0》中的三级要求，合理选取安全管理技术，为电子政务云业务的顺利开展提供良好的基础[4]。目前，安全管理体系包含网络安全管理制度、人员管理制度、建设管理制度等多个方面的内容。安全运维体系则在项目运维过程中，面向政务应用工作的开展需求，为政府单位提供面向租户的运行管理部门与自服务门户，面向电子政务云子运维人员，优化运维管理水平。通过构建安全管理体系，在标准与规范体系下，能实现各类资源的有序整合，并通过统一的标准与使用规则，提升安全管理工作的整体水平。

3 电子政务云的安全防护体系应用要点

在搭建电子政务云的网络安全防护体系时，主要涉及安全物理环境、安全管理中心与安全管理体系等。

3.1 安全物理环境

在电子政务云的安全防护体系搭建工作中，首先需要构建良好的安全物理环境。良好的安全物理环境是保障电子政务云安全、可靠运行的重要基础，在不间断运行的基础上，应做好机房环境、通信线路、设备实体、存储介质等方面的工作，再基于计算机场地与数据中心建设的具体要求，搭建安全物理环境。在安全物理环境建设工作中，应从位置选择上入手，考虑防雷击、防水防潮等多个方面，做好自然威胁防护工作。针对电子政务云在运行过程中的潜在人为威胁问题，则需要从防盗窃、防破坏两部分入手，做好人为威胁防护工作。

3.2 安全管理中心

安全管理中心包含系统管理、审计管理、安全管理、集中管控等多个方面。在搭建了安全管理中心之后，需要实现对系统运行情况的动态控制，合理设置安全运行参数，做好主客体的标记与授权工作，还需做好审计机制的管理工作。通过设置安全运维区域，可以对电子政务云系统中的网络链路、安全策略、恶意代码等问题进行集中化的监测与管理，并实现对相关系统管理人员与操作人员的身份审计[5]。

为保障通信网络的安全性，可以从网络架构入手，不断提高电子政务云平台的带宽与业务处理能力，并提供设备的冗余部署工作，通过多种技术手段，进一步提升通信工作的保密性与完整性。在搭建可信的网络平台时，也可以借助可信计算技术与公钥基础设施，减少外界攻击对电子政务云平台的影响。

在部署安全区域边界时，可以在互联网出口位置部署抗DDoS系统，以防范各类服务器攻击，如通过部署WEB应用防护系统，能对SQL注入与跨站攻击起到良好的防范效果，实现用户对互联网边界的访问控制。通过部署防火墙系统及恶意代码防护系统，则能对病毒蠕虫、僵尸网络、入侵攻击等起到良好的防护效果。由于电子政务云平台直接关系到各项政务工作的开展，因此在安全防护系统的架构中，需对不同政务应用的重要等级进行分类，根据信息流向的高低来合理部署防火墙与网闸，构建具有针对性的安全防护策略，有效控制电子政务云各类信息流的运行情况。

在优化安全计算环境的过程中，因为电子政务云在运行中面临的安全风险隐患类型较多，因此需结合网络安全设备的运行状态，在政务应用的重要节点与环节，搭建可信的安全计算环境。在建立安全计算环境时，可以通过身份鉴别与安全审计，做好这些关键节点部位的安全防护工作，这也是构建网络安全防护体系的重要内容。

3.3 安全管理制度

电子政务云在运行期间会受到多种人为因素的干扰，在人为操作不规范的情况下，也会诱发一系列的安全风险问题，导致数据丢失、被篡改等情况，对电子政务云系统的正常运行造成一定的阻碍。因此，在电子政务云的网络安全架构中，需要对现有的安全管理制度进行创新与优化。在现有的安全管理制度中，应针对机构管理、人员管理、运维管理等，对操作人员的日常操作进行规范化管理，在第一时间处理违规操作行为[6]。这样能让电子政务云的相关操作人员规范自身的操作，避免操作行为问题对电子政务云的安全性造成的影响。通过优化现有安全管理制度的方式，能强化电子政务云的一体化管理，充分发挥出数字化技术在政府工作中的应用价值，提高电子政务的管理效率与社会服务质量。需要注意的是，在电子政务云的运行过程中，可以结合运行场景的各项保护需求，建立基于云计算的防护体系，针对安全风险，应及时补充安全防护措施，提升安全防护工作的水平。

4 电子政务云的安全治理优化策略

4.1 构建全过程的安全治理体系

为强化电子政务云的安全治理水平，需要基于政务信息的全生命周期，构建完善的安全治理体系，通过开展评价、指导、监督等一体化的安全评价体系的方式，将安全风险与威胁控制在可接受的范畴内，为电子政务云与各项政务活动的稳定开展提供良好的环境。只有构建全生命周期的安全治理体系，才能更好地应对新型应用环境下的安全风险与安全挑战，获得良好的政务应用建设效果。

4.2 提高安全支撑能力

随着数字化时代的到来，人们对数字化政务服务工作提出了更高的要求，各级政府部门对政务云的需求也在不断增加。在电子政务云的运行中，需持续开展云网安全扩容与改造工作，避免安全资源使用量不足的问题发生。因此，在电子政务云安全治理期间，需要在不断提高基础服务能力的基础上，不断完善电子政务云管理平台，实现各类资源的集约化利用与动态调整，进一步提高其弹性与安全服务能力。

4.3 构建一体化的安全管理制度

在电子政务云平台安全治理活动中，应主动从制度、机构、人员、建设、运维等多方面入手，建立一体化的安全管理制度。在电子政务云应用中，需不断创新与完善安全管理流程，在政务应用预验收过程中，则可以选择云审查的方式，通过配置检查、漏洞扫描、代码审查等多种模式，判断政务应用的安全建设情况，确保安全建设能与安全设计保持一致。

5 结语

互联网技术与云计算技术的快速发展，为我国电子政务的应用和推广提供了良好的技术支撑，提升了政府部门的电子政务能力。但是，在应用电子政务云的过程中，还存在一定的安全隐患，因此需要做好安全防护管理工作，基于电子政务云的运行特点与需求，合理搭建网络安全架构，减少外界因素对其的影响。只有这样，才能充分发挥出电子政务云的社会服务价值，提升政府部门的线上服务能力。

参考文献

[1] 晁艳锋.新型电子政务基础设施安全监管体系建设研究[J].信息系统工程，2020(12)：83-84，87.

[2] 曹晖.基于云计算的电子政务应用研究[J].科学与信息化，2019(19)：47，49.

[3] 王斌，范松豪.基于电子政务云的网络安全架构治理探讨[J].电子产品可靠性与环境试验，2022，40(5)：7-11.

[4] 李晓明.基于等级保护2.0标准的电子政务云平台网络安全架构探析[J].网络安全技术与应用，2022(8)：73-76.

[5] 刘迎仙，李季伦，樊则胜.云时代下传统电子政务网络安全域的应用划分[J].网络安全技术与应用，2020(10)：131-133.

[6] 孙础辉.基于云计算的电子政务网络安全风险探析[J].电脑爱好者(普及版)(电子刊)，2021(3)：105.