ISSN:2661-3719(Print);2661-3727(Online)

基于网络安全等级保护 2.0 背景下城建档案政务云安全应用的研究

孔家聪
广州市城市建设档案馆　广东广州　510030

摘　要：网络安全等级保护 2.0 的发布标志着我国网络安全等级保护工作进入一个崭新的阶段。本文主要介绍了等保 2.0 的变化和特点，并阐述了等保 2.0 测试的意义，分析了网络信息安全建设的发展趋势。重点探索了网络安全等级保护 2.0 背景下城建档案政务云安全的应用，以广州市城市建设档案馆政务云安全应用为例，对在等保 2.0 背景下城建档案政务云安全建设、运维、云计算等应用能力进行剖析和研究。
关键词：网络安全等级保护 2.0；城建档案；政务云；网络安全应用

Research on Cloud security Application of urban construction archives government affairs under the background of Network security Level Protection 2.0

Jiacong Kong
Guangzhou Urban Construction Archives Guangzhou 510030

Abstract: The release of network security level protection 2.0 marks that our network security level protection has entered a new stage. This paper mainly introduces the changes and characteristics of equal insurance 2.0, expounds on the significance of the equal insurance 2.0 test, and analyzes the development trend of network information security construction. This paper focuses on the application of the cloud security of urban construction archives under the background of network security level protection 2.0. Taking the cloud security application of government affairs in Guangzhou Urban Construction Archives as an example, this paper analyzes and studies the cloud security construction, operation and maintenance, cloud computing, and other application capabilities of urban construction archives under the background of equal security 2.0.
Key Words: Network Security Level Protection2.0; Urban construction archives; Government Cloud; Network security application

引言

网络安全等级保护制度是国家网络安全领域的基本国策、基本制度和基本方法。随着信息技术的快速发展，伴随着网络安全形势的不断变化，等保 2.0 在 1.0 的基础上，注重全方位主动防御、动态防御、整体防控和精准防护，实现了对云计算、大数据、物联网、移动互联和工业控制信息系统等保护对象全面覆盖。

一、网络安全等级保护 2.0 的变化和特点

（一）等保 2.0 的变化

从等保 1.0 到等保 2.0，主要体现在体系框架和保障思路的变化、定级对象和测评的变化、等保要求的组合变化、控制点和要求项的变化。等保 1.0 中规定的安全要求在等保2.0中修改为安全通用要求和安全扩展要求，将云计算、移动互联、物联网、工业控制系统等列入标准范围，构成了“安全通用要求+新型应用安全扩展要求”的要求内容。

（二）等保 2.0 的特点

等保 2.0 标准创新性地提出安全保护通用要求，实现了对新技术、新应用安全保护对象和安全保护领域的全面覆盖。2.0 新标准突出技术思维和立体防范，注重全方位主动防御、动态防御、整体防控和精准防护，进一步强化了“一个中心，三重防护”的安全保护体系。等级保护 2.0 新标准强化了密码技术和可信计算技术的使用，把可信验证列入各个级别并逐级提出各个环节的主要可信验证要求，强调通过密码技术、可信验证、安全审计和态势感知等建立主动防御体系。

二、网络安全等级保护 2.0 测评的意义和网络安全建设趋势

（一）等保 2.0 测评的意义

网络安全等级保护 2.0 标准扩展了等级保护对象，将网络基础设施、云计算平台、大数据平台、物联网、工业控制系统纳入保护范围，并在通用要求的基础上，补充提出了云计算安全、移动互联网安全、物联网安全和工业控制系统安全的扩展要求。一方面，等保 2.0 指明了我国关键信息基础设施安全保障的原则、方法与手段，成为我国未来十年关键信息基础设施安全保障最基础、最核心、最重要的一部权威标准规范。另一方面，等保 2.0 可以作为以主动防御为目标、以技术保障为基础、管理运营为核心、以监测预警为支撑的网络安全防御体系框架性指导标准和规划建设指南。

（二）网络安全建设的新趋势

安全保障对象已扩展为基础设施和业务应用。等保 2.0 在继承了等保 1.0 中以资产防护为目标的成功实践基础上，结合近些年网络与信息技术的新变化，补充提出了对云计算、物联网、移动互联网和工业控制系统的安全防护要求。等保 2.0 扩展安全防护要求的提出，体现了基础设施和业务应用的发展是安全保障体系创新的第一驱动力，也充分反映了我国以基础设施和业务应用为核心的安全保障思想。随着等保 2.0 扩展安全防护要求的提出，广州市城市建设档案馆不仅运用云计算技术（广州市政务云）进行政务外网之间的相互通信，同时还利用物联网技术（城建档案 RFID 应用和档案库房密集架应用）、移动互联网技术等进行局域网、政务网、互联网之间的互联互通。不仅需要增加额外安全合规投入，而且还需要考虑传统网络与信息系统与云计算、物联网、移动互联网和工业控制系统如何建立协调、统一的安全保障机制，满足等保 2.0 对于安全监测、通报预警、应急处置、态势感知、安全运营的要求。未知威胁与安全分析成为安全建设能力目标。无论是等保 1.0 还是等保 2.0，监测预警都是安全技术体系的重点，等保 2.0 标准对新型攻击分析、网络内部攻击、用户行为分析等高级威胁提出了要求。这些未知威胁与潜在威胁监测预警的能力要求，充分体现了等保 2.0 主动防御、动态防御的核心思想。对未知威胁的检测，一方面可以通过威胁情报关联分析进行；另一方面可以通过异常检测进行，包括网络异常、行为异常、状态异常等；潜在威胁利用关联分析、行为建模、异常分析将那些远离合法和正常行为进行多维度长周期分析，从而达到检测业务欺诈、敏感数据泄露、内部恶意用户、有针对性攻击等潜在高级威胁的目的。分析研判与追踪溯源成为主动安全防御趋势。网络安全的本质在于攻防对抗，等保 2.0 所提倡的主动防御、动态防御的思想，其目的也是在攻防对抗中能够占得先机。只有有效地融合威胁检测、安全预警、分析研判、追踪溯源能力，使之相辅相成、互为补充，才能构成了完整的主动安全防御能力，达到主动安全防御的目的与效果。集中统一的安全运营管理成为安全建设核心。广州市政务云的建设是统一安全运营管理是积极防御体系的典型应用，可以消除各个安全系统孤岛，有效的将平台、人员、制度、流程有机的结合起来，实现安全运营工作的集中化、平台化、自动化，极大地提高安全运营的效果和效率。

三、网络安全等级保护 2.0 下的网络安全应用研究（以广州市城市建设档案馆政务云应用为例）

广州市政务云平台经过一期（2014 年）和二期（2017 年）的建设，已覆盖委办局大部分信息系统和数据，支撑着广州市的政务业务版块的正常运转。广州市城市建设档案馆作为广州市档案系统第一个政务云迁移单位，于 2014 年城建档案信息系统和数据整体迁移至政务云（电信节点），后在 2015-2016 年对政务云配置进行优化完善，在 IAAS 服务基础上扩展提供云平台 PaaS 服务（数据库服务、中件间服务、移动应用支撑服务）、容灾备份服务、信息安全服务、业务应用组件服务、大数据服务等服务内容。借助我馆信息安全提升和整改信息化建设项目，在强大的政务云计算和存储资源基础上，我馆丰富了安全即服务范围，配备了虚拟防火墙、主机漏洞检测、防病毒、应用层防火墙（WAF）、防篡改服务等虚拟化、主机安全服务，在基础备份能力（磁带备份）基础上增加了数据容灾服务能力，虚拟磁带库和备份一体机，随着城建档案信息化的分布式部署和应用，扩充了软件和硬件级负载均衡服务。

（一）等保 2.0 下对政务云计算要求更高

在构建广州市城市建设档案馆等保 2.0 安全体系过程中，我们选择云计算安全服务的内容变得尤为重要。作者认为，云计算安全除了满足网络架构、访问控制、入侵防范、安全审计、集中管控、身份鉴别、数据安全性、数据备份恢复等通用要求之外，还应满足基础设施位置、镜像和快照保护、供应链管理及云计算环境管理等扩展要求。云服务商所提供的云计算平台不但要实现自身的安全防护，还应具备向云租赁客户提供系统安全防护的能力。如：通过登录堡垒机远程管理政务云平台设备时，管理终端和云平台之间应建立双向身份验证机制；应能检测到对虚拟网络节点的网络攻击行为和云服务客户发起的网络攻击行为，并能记录攻击类型、攻击时间、攻击流量等。新标准无疑给安全管理人员和安全运维人员提出了更高的要求。

（二）政务云服务方与使用单位责任划分清晰明确

等保 2.0 下云计算平台需自身先通过等保测评，且云平台不得承载高于其保护等级的业务应用系统。比如，广州市政务服务数据管理局统建的政务云平台（电信节点和联通节点）通过定级专家评审、备案、测评一系列环节定为等保三级，可以承载广州市城市建设档案馆所有二级的信息系统应用业务。此外，云服务方（政务云建设单位）和云服务客户（政务云使用单位）之间有了更加清晰的安全责任边界，根据政务云提供的服务类型

和级别（IaaS/PaaS/SaaS），划分网络安全责任范围，让云服务方和云服务客户负起各自的主体安全责任。

（三）政务云服务方与使用单位安全能力要求提升

等保体系并不强制要求保护对象满足所有要求，传统等保 60 分即达到基本符合，但在等保 2.0 中测评达到 70 分以上才算基本符合，这意味着等保对象的“及格线”拔高，对各单位的网络安全能力提出更高要求。要求建议在安全资源池、安全监测能力、数据安全能力、安全管理中心等多维度做安全规划和全面考虑，这些建设点是过去被动安全防护理念中容易被忽视的点。单位安全能力的建设和提升要以国家网络安全法为指导，以网络安全等级保护技术标准为基础，满足自身安全防护所需，符合公安部、网信办等监管部门审查要求。等级保护 2.0 的到来，为政务云安全建设相关方提出更高的要求，防御手段融合了更多新技术，如态势感知、可信计算。在安全管理上，政务云相关方都应构建完备的安全管理体系，“机构”、“制度”和“人员”三要素全面提升，缺一不可，同时还应对安全整改过程、运行维护过程的重要活动实施控制和管理。

四、结束语

没有网络安全就没有国家安全，等保 2.0 的安全要求是我们维护网络安全的有力武器。认真地解读每一条要求是我们深入开展网络安全工作的前提，这样才能真正地将等保 2.0 运用到实际系统设计、建设、运维工作中。只有通过不断的学习和研究，持续地提高网络安全意识，并在网络安全管理和运维中严格落实各项要求，才能真正实现将安全事件防患于未然，为我国的网络安全事业保驾护航。

参考文献：

[1] 吴蒙 . 网络安全管理与网络安全等级保护制度研究 [J]. 网络安全技术与应用 ,2022(06):164-166.

[2] 阎育斌 . 网络安全等级保护 2.0 下的安全体系建设思路探析 [J]. 网络安全技术与应用 ,2021(01):166-167.

[3] 黄元培 . 网络安全等级保护 2.0 下的安全体系建设研究 [J]. 无线互联科技 ,2020,17(08):32-33.

[4] 张立强 . 网络安全等级保护 2.0 时代的可信性测评探讨 [A]. 公安部第三研究所、江苏省公安厅、无锡市公安局 .2019 中国网络安全等级保护和关键信息基础设施保护大会论文集 [J]. 公安部第三研究所、江苏省公安厅、无锡市公安局 :2020:4.

[5] 何占博 , 王颖 , 刘军 . 我国网络安全等级保护现状与 2.0 标准体系研究 [J]. 信息技术与网络安全 ,2021,38(03):9-14+19.