文章编号：1005-8451（2020）09-0042-05

铁路云计算安全标准研究与实践

纪　方，田海波，刘鹏宇
（中国铁路信息科技集团有限公司，北京　100844）

摘　要：为促进铁路云计算安全的合规性，对网络安全等级保护（简称：等级保护）2.0制度进行了深入研究，分析了等级保护制度中云服务商与云用户的相互关系。对中国国家铁路集团有限公司主数据中心云平台的等级保护测评情况进行了分析研究，为铁路云计算安全标准合规工作提供参考。

关键词：云计算安全；网络安全；等级保护；测评
中图分类号：U29：TP393　**文献标识码：**A

Research and practice of railway cloud computing security standards

JI Fang, TIAN Haibo, LIU Pengyu
(China Railway Information Technology Group Co. Ltd., Beijing　100844, China)

Abstract: In order to promote the compliance of railway cloud computing security, this article studied the network security level protection (hereinafter referred to as level protection) 2.0 system deeply, and analyzed the relationship between cloud service providers and cloud users in the hierarchical protection system. The article also analyzed and studied the classified protection evaluation of the cloud platform of the master data center of China Railway, so as to provide reference for the compliance of railway cloud computing security standards.

Keywords: cloud computing security；network security；classified protection；evaluation

云计算自2006年提出至今，已成为各国信息化建设的首选。随着云计算的发展，相应的安全性问题逐渐引起关注。为进一步提升安全风控能力，各国标准化组织和机构都展开了云计算安全标准化工作。本论文重点研究了我国网络安全等级保护（简称：等级保护）中的云计算安全扩展要求，阐述了铁路云计算安全实践情况和中国国家铁路集团有限公司（简称：国铁集团）主数据中心云平台的等级保护测评情况。

1　云计算安全标准研究概况

1.1　国外云计算安全标准研究概况

2011年，美国国家标准与技术研究院在NIST SP800-53的基础上，根据云计算的特点制定了《Fed-RAMP安全控制措施》，给出了云计算环境下需增强的安全控制措施[1]。2012年，欧洲网络与信息安全局（ENISA）发布了《云计算–信息安全收益、风险和建议》，整理了云计算面临的安全风险，并在同年发布了《云计算合同安全服务水平监测指南》，制定了反应服务等级协议运行情况的8项指标[2]。2015年，国际标准化组织ISO下设技术委员会发布了《ISO-27017：2015云服务信息安全管理体系》[3]，提出了7个针对云服务的控制措施。同年，云安全联盟（CSA）发布了云安全控制矩阵CCM 3.0，其中包含16个控制域，136条控制措施，并于2017年发布了《云计算关键领域安全指南V4.0》，对云计算安全中的14个关键领域进行了详细描述[4]。

1.2　国内云计算标准研究概况

近几年，国内云计算安全的宏观政策环境已逐渐完善。2014年，针对政府部门的云计算安全需求，中央网络安全和信息化委员会办公室发布了《信息安全技术 云计算服务安全指南》[5]，制定了使用云计算服务时的安全管理要求；并针对云服务商发布了《信息安全技术 云计算服务安全能力要求》[6]，制定了云服务商应具备的安全能力要求。

2019年5月，国家标准化管理委员会正式发布了《信息安全技术 网络安全等级保护基本要求》，

收稿日期：2020-03-27
基金项目：中国铁路总公司科技研究开发计划课题（P2018S001）
作者简介：纪　方，高级工程师；田海波，工程师。

标志着等级保护正式进入2.0时代。该标准已于2019年12月开始正式实行。

2　等级保护研究

2017年《中华人民共和国网络安全法》正式颁布实施，其中，第二十一条和第三十一条均明确了等级保护制度的适用范围

2.1　等级保护1.0与2.0的对比

新发布的等级保护2.0在10年前的1.0版本基础上进行了优化，提出了面向云计算等新技术的安全扩展要求；从被动防御向事前防御、事中响应、事后审计的动态保障体系转变；用可信计算等新的防护要求，取代了过时的测评项。等级保护2.0与1.0版本相比主要有以下3个特点。

（1）将云计算等新兴技术的安全扩展要求列入了标准范围。云计算扩展要求与安全通用要求有较多的重合子项，但也有其独有的条例，如图1所示。

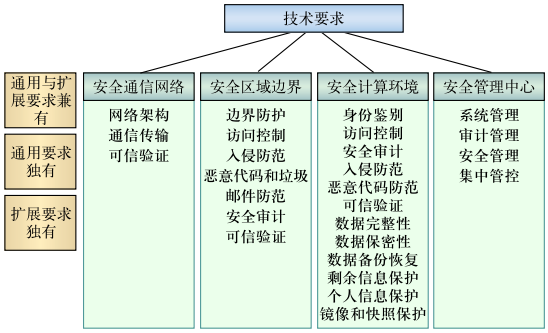

图1　云计算等级保护技术要求

（2）依据等级保护标准，分层面采取“一个中心，三重防御”的体系架构，同时，应考虑构建纵深的防御体系，采取互补的安全措施，保证一致的安全强度，建立统一的支撑平台，进行集中安全管理的总体性要求[7]，保证等级保护对象的整体安全防护能力。

（3）等级保护2.0中强化了对可信验证技术的使用要求，把其加入到等级保护的各个级别中，如表1所示，并提出了在各个关键环节的可信验证要求[8]。不同等级保护级别的可信验证对应不同的监管要求、保护级和可信保障。

结合以上3个要求，从技术和管理两方面进行安全设计，做到可信、可控、可管。

表1　等级保护可信验证技术要求

等级	按级监管	保护级	可信保障
一级	自主保护	自主访问	基础软件可信
二级	指导保护	审计（自主访问）	应用程序验证
三级	监管检查	标记（强制访问）	执行动态度量
四级	强制监督检查	结构化保证	实时关联感知
五级	专门监督检查	实时监控	实时处置

2.2　第三级云计算安全扩展要求研究

云计算安全扩展要求是等级保护2.0的重要内容之一[9]。等级保护2.0明确了云计算的定义和应用场景，基于基础设施即服务（IaaS，Infrastructure as a Service）、平台即服务（PaaS，Platform as a Service）和软件即服务（SaaS，Software as a Service）3种不同的服务模式，提出云服务客户和云服务商的控制范围和安全责任边界，并针对其安全责任边界提出相应的安全要求。

等级保护有5个不同的安全级别，本文主要研究等级保护第三级的安全要求，原因有以下两点：

（1）等级保护中要求“应根据云平台承载或将要承载的等级保护对象的重要程度确定其安全保护等级，原则上应不低于其承载的等级保护对象的安全保护等级”[10]。第三级云平台可满足大多数云平台应用的安全要求。

（2）在等级保护云计算安全扩展要求中，第四级和第三级的主要差异在于，第四级业务应用系统应划分独立的资源池，承载第四级应用的云系统应为独立系统，采取独立的防护机制。其他安全要求与第三级相比无过多增加。

第三级云计算安全扩展要求中包括7个安全类、16个安全控制点和46个测评项，如表2所示。

与通用要求相比，技术安全类仍是“一个中心，三重防御”的体系架构。管理安全类则缩减为两个，主要对云服务商选择提出相应要求。

在具体测评项中，针对云计算特性增加了保护对象，包括云平台、虚拟网络、虚拟网络边界、虚拟机、宿主机、虚拟机镜像和快照等。

结合等级保护附录D中的责任分担模型可知，云服务商与云用户有着各自的安全责任边界，在不同云服务模式下，两者的控制范围和安全责任边界如图2所示。

表2 第三级云计算安全扩展要求指标

扩展类型	安全类	安全控制点	测评项数
技术类要求	安全物理环境	基础设施位置	1
	安全通信网络	网络架构	5
	安全区域边界	访问控制	2
		入侵防范	4
		安全审计	2
	安全计算环境	身份鉴别	1
		访问控制	2
		入侵防范	3
		镜像和快照保护	3
		数据完整性和保密性	4
		数据备份恢复	4
		剩余信息保护	2
	安全管理中心	集中管控	4
管理类要求	安全建设管理	云服务商选择	5
		供应链管理	3
	安全运维管理	云计算环境管理	1
安全扩展要求指标数量统计			46

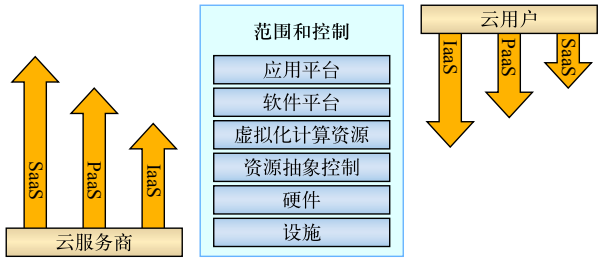

图2 云计算服务模式与控制范围的关系

扩展要求中提出云服务商应对云用户在安全上进行必要的帮助，包括：协助进行业务迁移，支持自行加解密，提供接口或开放性安全服务。同时，对云服务商的操作在安全上进行了一定的限制，规定应通过审计、双向验证等手段确保云服务商对云用户进行敏感操作的安全性和不可抵赖性。

3 铁路云计算安全等级保护进展情况

3.1 铁路云计算安全现状

铁路行业云计算安全经过多年建设，初见成效，主要体现在以下两方面。

（1）云计算安全防护能力不断提升。2018 年，铁路业务网络安全一体化保障工程（简称：铁网护栏工程）开始实施，其中包含面向云计算环境的应用安全保障系统模块，主要用于提升云计算安全防护能力。

（2）等级保护工作稳步推进。国铁集团目前已经完成国铁集团主数据中心（简称：主数据中心）云平台的定级、备案、测评工作。

3.2 铁路云计算安全建设情况

主数据中心于 2018 年 6 月开始设计、建设，采用云计算架构，其云平台定为等级保护第三级。

根据分区、分域原则，结合铁路信息系统的实际网络情况，构建了主数据中心安全架构，如图 3 所示。主数据中心网络可分为业务区和管理区。外部服务网与互联网之间做边界防护。内部服务网与铁路局间网络做边界防护。内外部服务网之间由内外网安全平台进行边界防护。

3.3 铁路云计算安全等级保护测评情况

国铁集团在 2019 年遵循等级保护制度，完成了对主数据中心云平台的等级保护定级、备案和测评等工作。主数据中心云平台针对其面临的主要安全风险，采取相应的安全控制措施，基本满足了等级保护第三级中的安全要求[11]。

（1）基础环境方面。主数据中心云平台所在机房具有防风、防雨、防震等基本能力，机房配备有视频监控系统、自动消防系统、电力供应系统等安全防护措施。网络、主机层面采取充分的冗余措施，网络设备、安全设备、服务器等均在上线前按照要

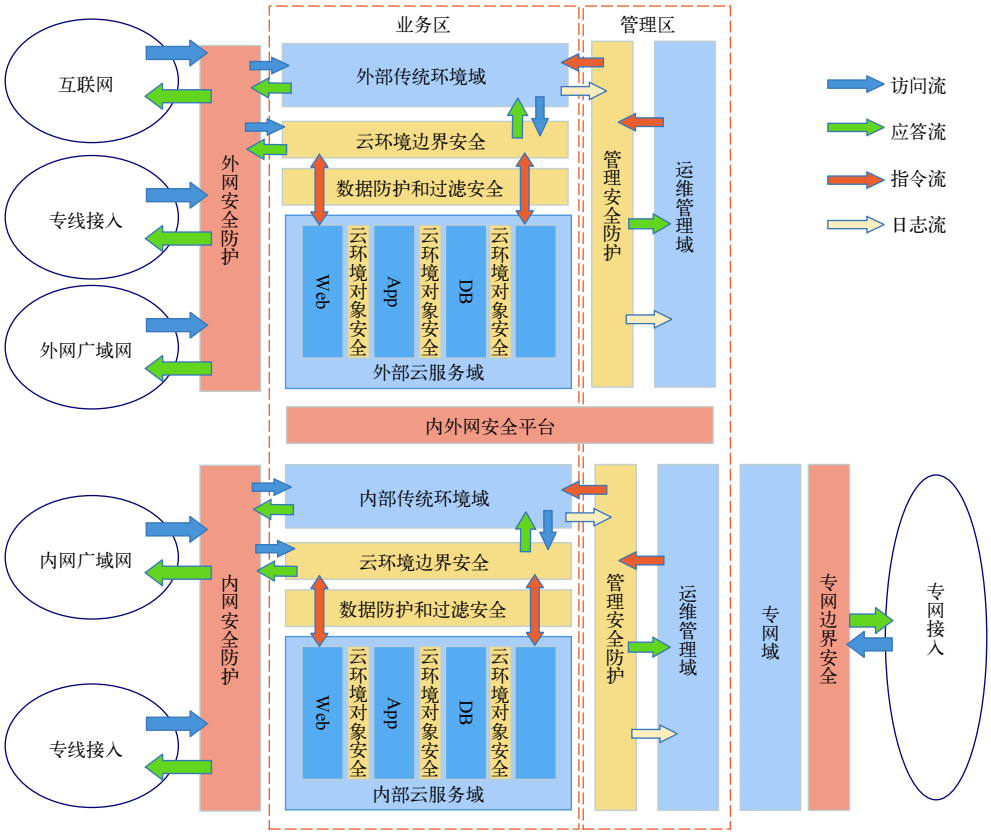

图3　主数据中心安全架构

求统一进行基线配置核查和漏洞扫描，并根据检查结果进行安全加固。

（2）安全控制措施方面。主数据中心云平台按照等级保护责任分担模型，在基础结构安全中部署有终端安全防护、主机安全防护、补丁管理系统、日志审计等安全控制措施；在纵深防御体系中部署有边界网络安全设备、虚拟化网络安全设备、主机防病毒、运维审计、漏洞扫描等安全措施；在积极防御体系中部署有态势感知平台、集中安全管理平台。符合等级保护中“一个中心，三重防御”的安全要求。

（3）安全责任制方面。主数据中心云平台的安全管理机构较为完善，责任明确，成立了网络安全和信息化领导小组，制定了《信息安全方针策略》，明确定义部门及各个工作岗位的职责[12]。

（4）管理制度体系方面。建立了由安全策略、管理制度、操作规程等构成的安全管理制度体系，制定了信息安全工作的总体方针和安全策略，确定了机构安全工作的总体目标、范围、原则和安全框架等[13]。制度涵盖岗位配置与职责、人员管理与培训考核、软件开发、工程实施、资产介质管理、备份与恢复管理、变更与应急管理等。

（5）系统规划与建设方面。制定了《中国铁路总公司主数据中心项目信息系统集成工程施工图》，包含云平台的安全设计方案及工程实施方案，内容覆盖云平台基础环境、网络、主机、应用、数字证书等方面。

4　结束语

本文分析了国内外云计算安全标准的研究情况，并对我国新发布的等级保护制度中的云计算安全扩展要求进行了重点研究。基于等级保护第三级要求，研究了云服务商与云用户的相互关系，结合主数据中心云平台实际情况，对基础环境、安全控制措施、安全责任、管理制度体系等方面进行了全面分析与论述。

目前，本文只研究了主数据中心云平台的测评情况，根据等级保护定级的要求，主数据中心云平台承载的信息系统同样需要满足等级保护的相应要

求。未来可结合具体的铁路信息系统，对云用户端等级保护的建设和测评情况进行深入研究，为铁路云计算安全合规性建设提供参考。

参考文献

[1] 王惠莅，杨　晨，杨建军. 美国国家标准和技术研究院信息安全标准化系列研究(十三) 美国NIST云计算安全标准跟踪及研究 [J]. 信息技术与标准化，2012（6）：49-52.

[2] 姚　远，左晓栋. 云计算安全国家标准研究 [J]. 电子技术应用，2014，40（8）：4-6，9.

[3] 陈兴蜀，杨　露，罗永刚，等. 国内外云计算安全标准研究 [J]. 信息安全研究，2016，2（5）：424-428.

[4] Security Guidance for Critical Areas of Focus in Cloud Computing-v4.0[EB/OL].[2017-07-26].https://cloudsecurityalliance.org/artifacts/security-guidance-v4/.

[5] 全国信息安全标准化委员会.云计算安全服务指南：GB/T 31167-2014[S]. 北京：中国标准出版社, 2014.

[6] 全国信息安全标准化委员会.云计算服务安全能力要求：GB/T 31168-2014[S]. 北京：中国标准出版社, 2014.

[7] 袁　慧. 网络安全等级保护2.0制度的研究和探讨 [J]. 信息与电脑(理论版)，2020，32（1）：223-224.

[8] 马　力. 网络安全等级保护2.0标准体系介绍[EB/OL].[2020-05-20]. http://www.djbh.net/webdev/web/HomeWebAction.do?p=getGzjb&id=8a818256721b693f01723014d841000a.

[9] 张振峰，张志文，王睿超. 网络安全等级保护2.0云计算安全合规能力模型 [J]. 信息网络安全，2019（11）：1-7.

[10] 全国信息安全标准化委员会.信息安全技术网络安全等级保护基本要求：GB/T 22239-2019[S]. 北京: 中国标准出版社, 2019.

[11] 汤　飞，张　彦. 云计算环境下信息系统安全防护 [J]. 铁路计算机应用，2015，24（2）：71-75.

[12] 全国信息安全标准化委员会.信息安全技术网络安全等级保护测评要求：GB/T 28448-2019[S]. 北京：中国标准出版社，2019.

[13] 全国信息安全标准化委员会.信息安全技术网络安全等级保护测评过程指南：GB/T 28449-2018[S]. 北京：中国标准出版社，2019.

责任编辑　李依诺