ICS 35.040
L 80

中华人民共和国国家标准

GB/T 34942—2017

信息安全技术
云计算服务安全能力评估方法

Information security technology—The assessment method for security capability of cloud computing service

2017-11-01 发布　　2018-05-01 实施

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会　发布

目　　次

前　言

本标准按照 GB/T 1.1—2009 给出的规则起草。

本标准由全国信息安全标准化技术委员会(SAC/TC 260)提出并归口。

本标准起草单位:中国电子技术标准化研究院、国家信息技术安全研究中心、中国信息安全测评中心、中国电子科技集团第 30 研究所、中国信息安全研究院有限公司、上海市信息安全测评认证中心、中国信息安全认证中心、中电长城网际系统应用有限公司、四川大学、华东师范大学、国家信息中心、神州网信技术有限公司、浪潮(北京)电子信息有限公司、华为技术有限公司、阿里云计算有限公司、深圳赛西信息技术有限公司、北京工业大学、中标软件有限公司、西安未来国际信息股份有限公司、中金数据系统有限公司、北京软件产品质量检测检验中心、重庆邮电大学、成都信息工程大学、北京邮电大学、西安电子科技大学、桂林电子科技大学、河南科技大学、北京航空航天大学、中国传媒大学。

本标准主要起草人:高林、王惠莅、李京春、何延哲、任望、梁露露、刘贤刚、范科峰、上官晓丽、杨晨、都婧、张玲、王强、徐御、周民、徐云、陈晓桦、吴迪、闵京华、马文平、何道敬、赵丹丹、刘俊河、梁满、刘虹、赵江、黄敏、陈雪秀、徐宁、崔玲、万国根、陈晓峰、杨力、裴庆祺、唐一鸿、蔡磊、叶润国、伍前红、黄永洪、杨震、李刚、陈小松、王勇、张志勇、毛剑、姜正涛。

引　言

GB/T 31168—2014《信息安全技术　云计算服务安全能力要求》对云服务商提出了基本安全能力要求，反映了云服务商在保障云计算环境中客户信息和业务的安全时应具备的基本能力。GB/T 31168—2014 将云计算服务安全能力要求分为一般要求和增强要求，增强要求是对一般要求的补充和强化。在实现增强要求时，一般要求应首先得到满足。有的安全要求只列出了增强要求，一般要求标为“无”。这表明具有一般安全能力的云服务商可以不实现此项安全要求。在具体的应用场景下，云服务商也可采用删减、补充、替代等多种方式对安全要求进行调整。

本标准是 GB/T 31168—2014 的配套标准，对应于 GB/T 31168—2014 的第 5 章～第 14 章规定的要求，本标准也从第 5 章～第 14 章给出了相应的评估方法。本标准主要为第三方评估机构开展云计算服务安全能力评估提供指导。第三方评估机构可采用访谈、检查、测试等多种方式，制定相应安全评估方案，并实施安全评估。

信息安全技术
云计算服务安全能力评估方法

1 范围

本标准规定了依据GB/T 31168—2014《信息安全技术　云计算服务安全能力要求》,开展评估的原则、实施过程以及针对各项具体安全要求进行评估的方法。

本标准适用于第三方评估机构对云服务商提供云计算服务时具备的安全能力进行评估,云服务商在对自身云计算服务安全能力进行自评估时也可参考。

本标准适用于对政府部门使用的云计算服务进行安全管理,也可供重点行业和其他企事业单位使用云计算服务时参考。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件,仅注日期的版本适用于本文件。凡是不注日期的引用文件,其最新版本(包括所有的修改单)适用于本文件。

GB/T 25069—2010　信息安全技术　术语

GB/T 31167—2014　信息安全技术　云计算服务安全指南

GB/T 31168—2014　信息安全技术　云计算服务安全能力要求

3 术语和定义

GB/T 25069—2010、GB/T 31167—2014和GB/T 31168—2014界定的术语和定义适用于本文件。为了便于使用,以下重复列出了GB/T 31167—2014中的术语和定义。

3.1

云计算　cloud computing

通过网络访问可扩展的、灵活的物理或虚拟共享资源池,并可按需自助获取和管理资源的模式。

注:资源实例包括服务器、操作系统、网络、软件、应用和存储设备等。

[GB/T 31167—2014,定义3.1]

3.2

云计算服务　cloud computing service

使用定义的接口,借助云计算提供一种或多种资源的能力。

[GB/T 31167—2014,定义3.2]

3.3

云服务商　cloud service provider

云计算服务的供应方。

注:云服务商管理、运营、支撑云计算的计算基础设施及软件,通过网络交付云计算的资源。

[GB/T 31167—2014,定义3.3]