ICS 35.040
L 80

中华人民共和国国家标准

GB/T 35279—2017

信息安全技术　云计算安全参考架构

Information security technology—Security reference architecture of cloud computing

2017-12-29 发布　　2018-07-01 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:北京大学软件与微电子学院、中国电子技术标准化研究院、中国科学院信息工程研究所信息安全国家重点实验室、中国科学院软件研究所、韶关学院、北京鼎普科技股份有限公司、北京时代新威信息技术有限公司、中国移动通信集团公司、华为技术有限公司、中国电信股份有限公司北京研究院、成都信息工程大学、中金数据系统有限公司、中国银联股份有限公司、阿里云计算有限公司、浪潮(北京)电子信息有限公司、国云科技股份有限公司、上海众人网络安全技术有限公司、东软集团股份有限公司、北京天融信网络安全技术有限公司、新华三技术有限公司、黑龙江省电子信息产品监督检验院、百度在线网络技术(北京)有限公司、汉柏科技有限公司、中国信息安全研究院有限公司、中国信息安全测评中心、中国电子科技集团第 30 研究所、西安电子科技大学、重庆邮电大学、成都电子科技大学、西安未来国际信息股份有限公司。

本标准主要起草人:卿斯汉、王惠莅、刘贤刚、陈驰、谢垂益、季统凯、谈剑峰、李雪莹、王海洋、王新杰、陈雪秀、杨晨、罗锋盈、马文平、柏洪涛、任兰芳、葛小宇、唐洪玉、万国根、崔玲、杨阳、赵江、崔进、龚一斌、史翔宇、方舟、马杰、王智民、刘冬梅、都婧、王强、周启明、陈晓峰、田玲、冯超、路娜、王希忠、沈晴霓、文伟平、徐菲、邹琪、孙松儿、李彦宾、黄永洪。

引　言

云计算是一种以服务为特征的计算模式，它通过对各种计算资源进行抽象，以新的业务模式提供高性能、低成本的持续计算、存储空间及各种软件服务，支撑各类信息化应用，能够合理配置计算资源，提高计算资源的利用率，降低成本，促进节能减排，实现真正的理想的绿色计算。

云计算带来诸多便利与优势的同时也给信息安全带来了多个层面的冲击与挑战。云计算的服务计算模式、动态虚拟化管理方式以及多层服务模式等引发了新的信息安全问题；云服务级别协议所具有的动态性及多方参与的特点，对责任认定及现有的信息安全体系带来了新的冲击；云计算的强大计算与存储能力被非法利用时，将对现有的安全管理体系产生巨大影响等。

在一种云服务中，信息与业务的安全性涉及所有参与该服务的云计算角色。为了清晰地描述云服务中各种参与角色的安全责任，需要构建云计算安全参考架构，提出云计算角色、角色安全职责、安全功能组件以及它们之间的关系。

本标准适用于指导所有云计算参与者在进行云计算系统规划时对安全的评估与设计。

信息安全技术　云计算安全参考架构

1　范围

本标准规定了云计算安全参考架构，描述了云计算角色，规范了各角色的安全职责、安全功能组件及其关系。

本标准适用于指导所有云计算参与者在进行云计算系统规划时对安全的评估与设计。

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

3　术语和定义

GB/T 25069—2010 和 GB/T 31167—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、灵活的物理或虚拟资源池，并可按需自助获取与管理资源的模式。

注：资源实例包括服务器、操作系统、网络、软件、应用与存储设备等。

[GB/T 31167—2014，定义 3.1]

3.2

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]

3.3

云服务客户　cloud service consumer

为使用云计算服务同云服务商建立业务关系的参与方。

[GB/T 31167—2014，定义 3.4]

3.4

云计算环境　cloud computing environment

云服务商提供的云计算平台，及客户在云计算平台之上部署的软件及相关组件的集合。

[GB/T 31167—2014，定义 3.8]

3.5

云审计者　cloud auditor

一般为独立的第三方审计机构，负责审计云服务的供应与使用，覆盖运营、性能与安全。