ICS 35.030
CCS L 80

中华人民共和国国家标准

GB/T 31168—2023
代替 GB/T 31168—2014

信息安全技术
云计算服务安全能力要求

Information security technology—
Security capability requirements for cloud computing services

2023-05-23 发布　　2023-12-01 实施

国家市场监督管理总局
国家标准化管理委员会　发布

目　　次

前　言

本文件按照GB/T 1.1—2020《标准化工作导则　第1部分:标准化文件的结构和起草规则》的规定起草。

本文件代替GB/T 31168—2014《信息安全技术　云计算服务安全能力要求》,与GB/T 31168—2014相比,除结构调整和编辑性改动外,主要技术变化如下:

a) 更改了本文件的适用范围(见第1章,2014年版的第1章);

b) 增加了对GB/T 32400—2015和GB/T 35273—2020的规范性引用(见第3章、9.1.1);

c) 更改了部分术语和定义(见第3章,2014年版的第3章);

d) 增加了“缩略语”一章(见第4章);

e) 将“云服务模式”更改为“云能力类型”(见5.1);

f) 增加了高级要求,每类安全要求分别对应一般要求、增强要求和高级要求(见5.4);

g) 删除了“本文件的结构”(见2014年版的4.7);

h) 删除了原各类要求分别对应的策略与规程,整合至第14章的“策略与规程”(见14.1,2014年版的5.1、6.1、7.1、8.1、9.1、10.1、11.1、12.1、13.1和14.1);

i) 增加了“安全管理功能的通信保护”(见7.14);

j) 增加了“WEB访问安全”“API访问安全”(见8.21、8.22);

k) 增加了“数据保护”一章,提出数据安全要求,确保客户迁移数据过程中的业务连续性和数据完整性(见第9章);

l) 将“维护”一章的名称更改为“维护管理”(见第11章,2014年版的第9章);

m) 更改了“机房设计”的内容(见第16章,2014年版的第14章)。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由全国信息安全标准化技术委员会(SAC/TC 260)提出并归口。

本文件起草单位:中电数据服务有限公司、四川大学、杭州安恒信息技术股份有限公司、中国科学技术大学、中国电子技术标准化研究院、中国网络安全审查技术与认证中心、国家信息技术安全研究中心、中国信息安全测评中心、中国信息通信研究院、北京信息安全测评中心、国家工业信息安全发展研究中心、中国软件评测中心、中国移动通信集团有限公司、中电长城网际系统应用有限公司、神州网信技术有限公司、深信服科技股份有限公司、宁夏西云数据科技有限公司、三六零数字安全科技集团有限公司、蚂蚁科技集团股份有限公司、合肥高维数据技术有限公司、上海市方达(北京)律师事务所、北京中测安华科技有限公司、中电和瑞科技有限公司、阿里云计算有限公司、武汉理工大学、四川发展大数据产业投资有限责任公司、南方电网数字传媒科技有限公司、上海观安信息技术股份有限公司、中科锐眼(天津)科技有限公司。

本文件主要起草人:周亚超、罗永刚、左晓栋、陈兴蜀、李世锋、张建军、闵京华、杨建军、李斌、伍扬、王惠莅、张弛、单博深、许皖秀、崔占华、王启旭、杨苗苗、张明天、刘佳良、胡华明、丁晓、史大为、卢夏、李媛、何延哲、刘俊河、王强、陈雪鸿、杨帅锋、柳彩云、胡振泉、耿贵宁、邵江宁、韦韬、郭亮、贾依真、叶润国、田辉、尹云霞、杜宇鸽、安兆彬、吴复伟、张滨、江为强、刘雨桁、杨婷、李安伦、肖广娣、程军军、王坤、张峰、邱勤、艾青松、龙毅宏、张大江、黄少青、果靖、郑珂雪、陈清明、王永基、郑赳、杨勃、王朝栋、张照龙、蒋韬、赵洪宇。

本文件及其所替代文件的历次版本发布情况为:

——2014年首次发布GB/T 31168—2014;

——本次为第一次修订。

引　言

本文件与GB/T 31167—2023《信息安全技术　云计算服务安全指南》构成了云计算服务安全管理的基础文件。GB/T 31167—2023提出了客户采用云计算服务的安全管理基本原则，给出了采用云计算服务的生命周期各阶段的安全管理和技术措施；本文件面向云服务商，描述了提供云计算服务时应具备的安全技术能力。

参照GB/T 31167—2023，本文件分为一般要求、增强要求和高级要求。根据云计算平台上的数据敏感度和业务重要性的不同，云服务商具备的安全能力也各不相同。

信息安全技术
云计算服务安全能力要求

1 范围

本文件规定了云服务商提供云计算服务时应具备的安全能力。

本文件适用于对云计算服务能力的建设、监督、管理和评估。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；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—2022 信息安全技术 术语

GB/T 31167—2023 信息安全技术 云计算服务安全指南

GB/T 32400—2015 信息技术 云计算 概览与词汇

GB/T 35273—2020 信息安全技术 个人信息安全规范

GB 50174 数据中心设计规范

3 术语和定义

GB/T 25069—2022、GB/T 31167—2023 和 GB/T 32400—2015 界定的以及下列术语和定义适用于本文件。

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。

3.2

云计算服务 cloud computing service

使用定义的接口，借助云计算(3.1)提供一种或多种资源的能力。

3.3

云服务商 cloud service provider

提供云计算服务(3.2)的参与方。

3.4

云服务客户 cloud service customer

为使用云计算服务而处于一定业务关系中的参与方。

注 1：业务关系不一定包含经济条款。

注 2：本文件中云服务客户简称客户。