



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	V
引言	VI
1 范围	1
2 规范性引用文件	1
3 术语和定义	1
4 概述	2
4.1 评估原则	2
4.2 评估内容	3
4.3 评估证据	3
4.4 评估实施过程	3
5 系统开发与供应链安全评估方法	5
5.1 策略与规程	5
5.2 资源分配	6
5.3 系统生命周期	7
5.4 采购过程	8
5.5 系统文档	9
5.6 安全工程原则	10
5.7 关键性分析	10
5.8 外部信息系统服务及相关服务	11
5.9 开发商安全体系架构	12
5.10 开发过程、标准和工具	13
5.11 开发商配置管理	15
5.12 开发商安全测试和评估	17
5.13 开发商提供的培训	19
5.14 防篡改	20
5.15 组件真实性	20
5.16 不被支持的系统组件	21
5.17 供应链保护	22
6 系统与通信保护评估方法	25
6.1 策略与规程	25
6.2 边界保护	26
6.3 传输保密性和完整性	28
6.4 网络中断	29
6.5 可信路径	29
6.6 密码使用和管理	30
6.7 协同计算设备	30
6.8 移动代码	30

6.9	会话认证	31
6.10	移动设备的物理连接	32
6.11	恶意代码防护	32
6.12	内存防护	34
6.13	系统虚拟化安全性	34
6.14	网络虚拟化安全性	37
6.15	存储虚拟化安全性	37
7	访问控制评估方法	39
7.1	策略与规程	39
7.2	用户标识与鉴别	40
7.3	设备标识与鉴别	41
7.4	标识符管理	41
7.5	鉴别凭证管理	42
7.6	鉴别凭证反馈	44
7.7	密码模块鉴别	44
7.8	账号管理	45
7.9	访问控制的实施	46
7.10	信息流控制	47
7.11	最小特权	48
7.12	未成功的登录尝试	49
7.13	系统使用通知	50
7.14	前次访问通知	50
7.15	并发会话控制	51
7.16	会话锁定	51
7.17	未进行标识和鉴别情况下可采取的行动	52
7.18	安全属性	52
7.19	远程访问	53
7.20	无线访问	54
7.21	外部信息系统的使用	54
7.22	信息共享	55
7.23	可供公众访问的内容	56
7.24	数据挖掘保护	56
7.25	介质访问和使用	57
7.26	服务关闭和数据迁移	58
8	配置管理评估方法	59
8.1	策略与规程	59
8.2	配置管理计划	59
8.3	基线配置	60
8.4	变更控制	61
8.5	配置参数的设置	63
8.6	最小功能原则	64
8.7	信息系统组件清单	65

9	维护评估方法	67
9.1	策略与规程	67
9.2	受控维护	67
9.3	维护工具	68
9.4	远程维护	69
9.5	维护人员	70
9.6	及时维护	71
9.7	缺陷修复	71
9.8	安全功能验证	72
9.9	软件、固件、信息完整性	73
10	应急响应与灾备评估方法	74
10.1	策略与规程	74
10.2	事件处理计划	74
10.3	事件处理	75
10.4	事件报告	76
10.5	事件处理支持	77
10.6	安全警报	78
10.7	错误处理	78
10.8	应急响应计划	79
10.9	应急培训	81
10.10	应急演练	81
10.11	信息系统备份	82
10.12	支撑客户的业务连续性计划	84
10.13	电信服务	84
11	审计评估方法	85
11.1	策略与规程	85
11.2	可审计事件	86
11.3	审计记录内容	86
11.4	审计记录存储容量	87
11.5	审计过程失败时的响应	87
11.6	审计的审查、分析和报告	88
11.7	审计处理和报告生成	89
11.8	时间戳	90
11.9	审计信息保护	90
11.10	不可否认性	91
11.11	审计记录留存	92
12	风险评估与持续监控评估方法	92
12.1	策略与规程	92
12.2	风险评估	93
12.3	脆弱性扫描	93
12.4	持续监控	95
12.5	信息系统监测	96

12.6	垃圾信息监测	98
13	安全组织与人员评估方法	98
13.1	策略与规程	98
13.2	安全组织	99
13.3	安全资源	100
13.4	安全规章制度	100
13.5	岗位风险与职责	101
13.6	人员筛选	101
13.7	人员离职	102
13.8	人员调动	103
13.9	访问协议	104
13.10	第三方人员安全	104
13.11	人员处罚	105
13.12	安全培训	106
14	物理与环境安全评估方法	107
14.1	策略与规程	107
14.2	物理设施与设备选址	107
14.3	物理和环境规划	108
14.4	物理环境访问授权	109
14.5	物理环境访问控制	110
14.6	通信能力防护	112
14.7	输出设备访问控制	112
14.8	物理访问监控	113
14.9	访客访问记录	114
14.10	电力设备和电缆安全保障	114
14.11	应急照明能力	115
14.12	消防能力	116
14.13	温湿度控制能力	117
14.14	防水能力	118
14.15	设备运送和移除	118
	参考文献	119

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]