ICS 35.240.01
CCS L80

DB15

内 蒙 古 自 治 区 地 方 标 准

DB15/T 2196—2021

大数据应用 云服务安全技术指南

Big data application—Technical guide for cloud service security

2021-05-25 发布　　2021-06-25 实施

内蒙古自治区市场监督管理局　　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。

本文件由内蒙古自治区大数据中心提出并归口。

本文件起草单位：内蒙古自治区大数据中心、杭州安恒信息技术股份有限公司、内蒙古工业大学网络空间安全研究所、北京信息安全测评中心。

本文件主要起草人：包瑞林、孙卫、林明峰、田丽丹、梁伟、李媛、王钢、李欢、崔连伟。

大数据应用云服务安全技术指南

1 范围

本文件规定了云服务客户信息系统从迁移上云到退出云计算平台过程中各阶段的安全服务内容与技术要求。

本文件适用于党政机关云计算平台使用单位、云服务商和云服务安全提供商。云安全测评机构也可参考使用。

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 20984 信息安全技术 信息安全风险评估规范

GB/T 22240 信息安全技术 网络安全等级保护定级指南

GB/T 25069 信息安全技术 术语

GB/T 31167 信息安全技术 云计算服务安全指南

GB/T 32400 信息技术 云计算 概览与词汇

3 术语和定义

GB/T 25069界定的以及下列术语和定义适用于本文件。

3.1

云服务商 cloud service provider

云计算服务的供应方。

[来源：GB/T 31167-2014，3.3]

3.2

云服务客户 cloud service customer

为使用云服务而处于一定业务关系中的参与方。

[来源：GB/T 31167-2014，3.4]

3.3

云计算平台 cloud computing platform

云服务商提供的云计算基础设施及其上的服务软件的集合。

[来源：GB/T 31167-2014，3.7]

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。
[来源：GB/T 31167-2014，3.8]

3.5

云服务安全提供商 cloud service security provider

支撑或协助云服务商或云服务客户的安全管理、技术和运维的提供商。

3.6

云服务用户cloud service user

云服务客户中使用云服务的自然人或实体代表。
[来源：GB/T 32400-2015，3.2.17]

4 安全服务过程

4.1 概述

云服务用户迁移信息系统至云计算平台、使用、退出云计算环境过程中，安全服务生命周期包括上云前安全分析与设计、安全建设、安全运维与安全退出四个阶段。云安全服务生命周期各个阶段输入输出文档，见附录A。

针对尚未建设的信息系统（以下简称“新建系统”），安全服务过程如图1所示。在上云前安全分析与设计阶段，完成安全评估与需求分析、安全开发及定级备案；在安全建设阶段，完成安全管理体系建设、安全技术体系建设、安全自测，根据安全自测结果进行整改和加固，最后进行第三方测评；在安全运维阶段，进行安全运维体系建设及落地实施；在安全退出阶段，针对信息系统退出云计算平台的过程开展安全管控。

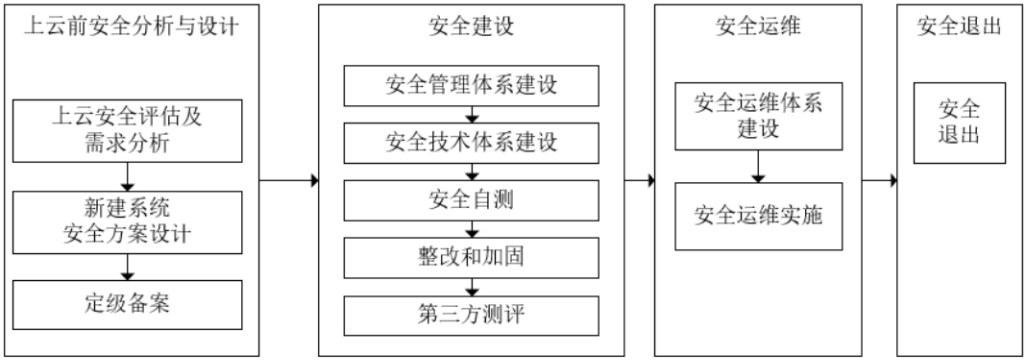

图1 新建信息系统安全服务过程

针对已建信息系统，安全服务过程如图2所示。在上云前安全分析与设计阶段，完成安全评估与需求分析、定级备案；在安全建设阶段，通过安全自测得出差距分析，设计整改方案，开展安全管理体系建设、安全技术体系建设、整改和加固，最后开展第三方测评；在安全运维阶段，进行安全运维体系建设及落地实施；在安全退出阶段，针对信息系统退出云计算平台的过程开展安全管控。

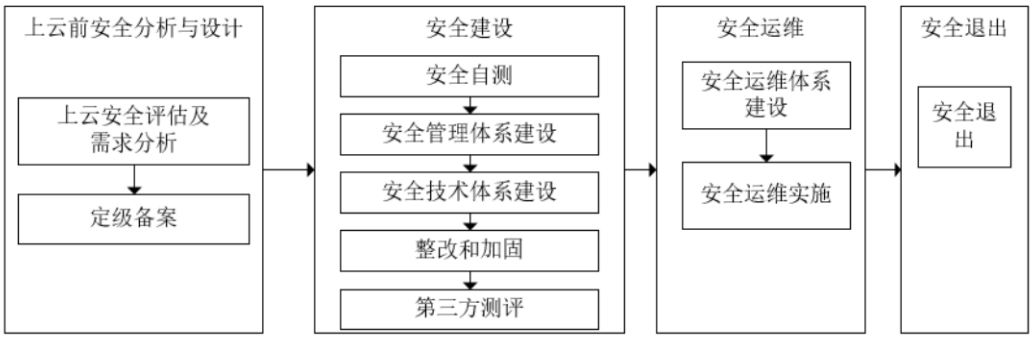

图2　已建信息系统安全服务过程

4.2　上云前安全分析与设计

信息系统迁移至云计算平台（以下简称“上云”）前，完成上云前安全需求分析及定级备案。针对新建系统，根据信息系统安全需求，设计系统安全开发方案，实现软件安全开发生命周期管理。

4.3　安全建设

信息系统迁移至云计算平台后，开展安全管理体系设计及落地、安全技术体系的设计和实施、安全自测、整改加固以及第三方测评，以提升信息系统在云上的安全防护能力。

4.4　安全运维

信息系统完成安全建设后，需开展安全运维活动，包括了安全运维体系的建设以及安全运维实施。在识别、防护、检测、预警、响应、处置等环节，通过团队、技术平台、运维三要素的密切协同，持续性开展安全运维，形成安全闭环。

4.5　安全退出

信息系统退出云计算平台（以下简称“下线”）过程需进行安全退出管理，主要确保业务数据得到有效保护，在系统下线的过程中不造成信息的泄露。

5　上云前安全分析与设计

5.1　上云安全评估及需求分析

对于适合上云的信息系统，安全需求分析重点是合规性需求以及安全风险的可控。通过上云评估及安全需求分析，发现待上云信息系统的安全风险，挖掘信息系统的合规性要求和安全需求，完成信息系统上云前的安全准备工作。具体内容包括：

a）　调研系统业务，包括调研信息系统的业务功能、系统用户、安全保护等级，梳理信息系统资产，根据业务数据的敏感程度以及系统功能，判断信息系统是否适合上云；
b）　调研云计算平台是否已通过云计算服务安全评估；
c）　调研上云前是否存在对信息系统的安全测试要求以及通过情况；
d）　调研系统网络架构及 IP 地址，包括调研信息系统的网络架构、外联线路情况、IP 地址划分、VLAN 划分、业务高峰期流量峰值以及业务流向情况，梳理信息系统架构和业务数据流向；
e）　调研信息系统安全现状，包括安全能力现状及其安全策略；
f）　调研运维终端设备情况，包括设备的安全策略、主机防病毒情况；

g) 调研数据及备份情况，包括信息系统配置信息、业务数据信息、备份策略。
h) 评估信息系统安全风险，对信息系统所面临的安全风险以及上云后面临的安全风险进行风险分析，提出应对建议；
i) 分析系统上云信息系统安全需求。

5.2 定级备案

针对尚未定级备案的信息系统开展定级备案工作。定级备案的措施包括：

a) 依据GB/T 22240要求，确定定级对象，确定受损害的客体以及侵害程度，从业务信息及系统服务两个方面最终确定信息系统安全保护等级；
b) 编写定级报告及备案表；
c) 根据专家评审意见进行修订，完成信息系统备案工作。

5.3 新建系统安全方案设计

对新建信息系统设计安全开发过程。具体措施包括：

a) 在安全需求阶段，应考虑信息系统的安全需求，细化安全需求并完成安全需求确认；
b) 在安全设计阶段，根据安全需求进行安全设计，制定安全编码规范；
c) 在安全开发阶段，根据安全编码规范进行安全开发，编码完成后开展代码审计，并根据审计结果进行整改；
d) 在安全测试阶段，开展安全功能测试及交互式安全测试，并根据测试结果进行整改。

6 安全建设

6.1 安全自测

6.1.1 概述

依据信息系统的安全需求，对信息系统进行安全自测，找出信息系统与安全需求之间的安全差距。

6.1.2 漏洞扫描

对信息系统及云上环境进行漏洞扫描，通过技术手段以及人工验证等手段发现漏洞，包括但不限于WEB应用漏洞、主机操作系统漏洞、数据库漏洞、逻辑缺陷、弱口令、信息泄露及配置不当等脆弱性问题。

6.1.3 配置核查

对信息系统及云上环境进行配置核查，采用人工检查用表、脚本程序或基线扫描工具进行配置核查，针对主机系统、数据库、中间件等方面，检查系统策略配置、服务配置、保护措施、系统及软件升级更新情况以及是否存在后门等内容。

6.1.4 代码审计

对具有代码审计安全需求的信息系统，以审计工具或人工分析方式，系统化分析程序代码的弱点，发现用户输入错误的可能情况，评估可能产生的衍生问题。

6.1.5 应用渗透测试

通过应用渗透测试，找出目前信息系统存在的代码缺陷和漏洞，具体措施包括：

a) 通过工具扫描与人工测试、分析的手段，以模拟黑客入侵的方式对信息系统进行模拟入侵测试；
b) 评估信息系统是否存在 SQL 注入、跨站脚本攻击、跨站伪造请求、弱口令、明文传输、文件包含、目录浏览、不安全的跳转、溢出、上传漏洞、不安全的数据传输、未授权的访问等脆弱性问题,识别信息系统存在的安全风险。

6.2 安全管理体系建设

梳理信息安全管理组织现状、信息安全管理制度及落地情况，依据信息安全管理体系要求、制度和标准，结合信息安全管理现状以及安全管理过程中存在的安全痛点和安全需求，设计满足合规性要求及信息系统安全需求的安全管理体系，开展安全管理体系落地。

6.3 安全技术体系建设

依据安全需求、差距分析报告或风险评估报告，对云服务客户信息系统面临的安全风险进行总结分析，设计安全技术方案并实施。具体内容包括：

a) 根据云计算平台以及云安全资源，结合信息系统的安全需求及差距分析，设计安全技术方案；
b) 将安全技术方案的实现方法落实到具体的产品功能或措施，使信息系统达到相应的安全能力要求；
c) 合理划分信息系统安全区域，制定安全产品配置策略以及安全基线；
d) 完成安全产品的安全配置，按照安全基线对操作系统、数据库及其他组件进行安全加固。

6.4 整改和加固

应根据安全自测的差距分析的结果，对信息系统进行整改和安全加固。

6.5 第三方测评

根据云服务客户的安全需求进行第三方测评。第三方测评内容包括但不限于：网络安全等级保护测评，依据GB/T 20984进行的风险评估等。

7 安全运维

7.1 安全运维体系建设

建立安全运维体系，实现安全自身工作的运作机制。结合团队、技术平台、运维流程三要素，运维团队借助技术平台持续开展标准化、流程化的安全运维活动和开展精细化、数字化的运维管理，实现日常安全运维、基于风险监测事件触发的安全运维、基于场景的安全运维。

7.2 安全运维实施

7.2.1 日常安全运维

应定期进行常规性安全检查，包括以下要求。

a) 安全巡检：对信息系统进行安全巡检，包括漏洞扫描、配置核查、应用渗透测试，并提交巡检报告；
b) 安全监控：自动化安全监控平台结合人工监控，详见 7.2.2 章节内容；
c) 安全值守：人员驻场值守。

7.2.2 安全监测

安全监测包括日志监测、安全策略调整、安全事件分析与处理三方面。

a) 日志监测的措施包括：
   1) 对日志数据进行梳理和分类；
   2) 根据攻击模型分析关联数据情况，监测数据的异常变化；
   3) 基于监测结果评估是否受到攻击。
b) 安全策略调整的措施包括：
   1) 根据互联网发生的安全事件以及威胁情报数据，进行影响性评估；
   2) 调整安全设备的安全策略。
c) 安全事件分析与处理的措施包括：
   1) 利用日志监测及策略变更情况，通过观察数据生命周期，进行系统化分析，找出安全事件发生的原因；
   2) 安全加固，规避或降低类似安全事件的发生。

7.2.3 安全通告

定期发布安全预警通告，遇紧急高危漏洞或重大信息安全事件即时通告预警，具体要求包括：

a) 安全通告的内容包括但不限于系统漏洞信息、病毒信息、预警信息、信息安全事件、最新安全技术；
b) 通过多种方式进行通告，包括但不限于电子邮件、电话、信息推送。

7.2.4 应急预案及演练

为应对信息系统遭遇网络入侵、大规模病毒爆发、拒绝服务攻击等突发安全事件，需提前针对相关事件进行应急预案的编制和演练，具体内容包括：

a) 编制应急预案，组织应急演练的开展；
b) 完成应急预案和演练后，形成报告。

7.2.5 应急响应

应急响应的安全服务措施包括：

a) 对突发安全事件快速应急响应；
b) 对已发生的安全事件在事中及事后进行过程取证、分析及处理。

7.2.6 重大活动安全保障

在重大活动期间制定信息安全保障方案，加强网络监测力度，提高响应效率。重大活动安全服务措施包括：

a) 实时监测攻击态势；
b) 安全保障手段包括但不限于漏洞扫描、配置检查、渗透测试、安全值守、日志分析、应急响应。

7.2.7 专项安全检查

针对云服务客户信息系统的特殊安全需求，进行专项安全检查，包括但不限于弱口令检查、入侵痕迹检查、专项漏洞检查、钓鱼邮件检查等方面。

7.2.8 安全意识及培训

定期开展信息安全培训，根据不同的岗位人员进行有针对性的培训内容。

8 安全退出

应依据GB/T 31167规定的退出服务实施退出，确保在系统下线的过程中不会造成信息的泄露。退出评估实施的措施包括：

a) 对业务系统下线过程进行监管；
b) 评估下线过程的安全风险，梳理并评估业务数据重要性，以及评估对其他信息系统的影响；
c) 制定下线过程的安全防范措施，应在退出云计算平台后再变更相关安全防护措施，防止下线过程中数据泄露；
d) 制定针对性的信息系统安全下线流程。

附 录 A
（资料性）
各阶段输入输出物

安全服务过程的四个阶段输入输出物见表A.1。

表A.1 阶段输入输出物

阶段	输入文档	输出文档
5 上云前安全分析与设计		
5.1 上云安全评估及需求分析	《信息系统安全现状调研表》 《信息系统风险评估工作流程》 《信息系统业务调研表》 《信息系统网络架构及IP地址调研表》	《信息系统信息安全调研报告》 《信息系统信息安全风险评估及安全需求报告》
5.2 定级备案	《信息系统业务调研表》 《信息系统信息安全调研报告》	《信息系统保护等级定级报告》 《信息系统保护等级备案表》
5.3 新建系统安全方案设计	《信息系统信息安全调研报告》 《信息系统信息安全风险评估及安全需求报告》	《软件安全开发生命周期安全需求说明书》 《软件安全开发生命周期安全设计》 《安全编码规范》 《安全测试报告》
6 安全建设		
6.1 安全自测		《差距分析报告》 《漏洞扫描报告》 《安全配置检查报告》 《代码审计报告》 《信息系统渗透测试报告》
6.2 安全管理体系建设	《信息安全管理制度现状清单》 《信息安全管理调研表》 《信息安全管理现状调研报告》	《标准信息安全管理体系文件集》
6.3 安全技术体系建设	《云平台基本情况表》 《安全资源情况表》 《云上系统安全建设方案》	《信息系统云安全实施方案》 《信息系统云安全策略配置及安全加固报告》
6.4 整改和加固	《差距分析报告》	《信息系统安全整改和加固报告》
6.5 第三方测评		《测评报告》
7 安全运维		
7.1 安全运维体系建设	《信息安全管理制度现状清单》 《信息安全管理调研表》 《信息安全管理现状调研报告》	《安全运维体系建设方案》

表A.1表阶段输入输出物（续）

阶段	输入文档	输出文档
7.2　安全运维实施		
7.2.1　日常安全运维		《日程运维报告》
7.2.2　安全监测		《安全日志分析报告》 《安全加固策略》 《安全事件分析报告》 《周期安全风险报告》
7.2.3　安全通告		《安全事件通告》 《安全事件预警》 《安全事件解决方案》
7.2.4　应急预案及演练	《信息安全管理制度现状清单》 《信息安全管理调研表》 《信息安全管理现状调研报告》	《应急演练预案》 《应急演练报告》
7.2.5　应急响应	《安全日志分析报告》	《应急响应分析报告》
7.2.6　重大活动安全保障	《重要时期保障方案》	《重要时期保障报告》
7.2.7　专项安全检查	《专项安全检查方案》	《专项安全检查报告》
7.2.8　安全意识及培训	《安全意识及培训方案》	《安全意识及培训报告》
8　安全退出	《待下线信息系统数据残留情况及业务处理流程计划》	《下线处理安全流程准则》 《信息系统残留风险评估报告》

参 考 文 献

[1] GB/T 31168信息安全技术　云计算服务安全能力要求

[2] CSA 0001.1-2016　云计算安全技术要求 第1部分：总则

[3] CSA 0001.2-2016　云计算安全技术要求 第2部分：Iass安全技术要求

[4] CSA 0001.3-2016　云计算安全技术要求 第3部分：Pass安全技术要求

[5] CSA 0001.3-2016　云计算安全技术要求 第4部分：Sass安全技术要求

[6] 关于加强党政部门云计算服务网络安全管理的意见 中网办发文〔2014〕14号

[7] 国家互联网信息办公室 国家发展和改革委员会 工业和信息化部 财政部关于发布《云计算服务安全评估办法》的公告 2019年 第2号