ICS 35.100.05，35. 240. 40
L79，A11

IAC
CCSA

中国保险行业协会标准
中国通信标准化协会标准

T/IAC CCSA 32—2019

保险行业云计算场景和总体框架

Insurance industry cloud computing scenario and overall framework

2019- 12-24 发布　　2020- 03- 24 实施

中国保险行业协会
中国通信标准化协会　　发布

目　　次

前　言

本标准按照GB/T 1.1-2009给出的规则起草

本标准由中国保险行业协会、中国通信标准化协会提出并归口

本标准起草单位：中国信息通信研究院、中国人民财产保险股份有限公司、中国太平洋保险（集团）股份有限公司、中国人寿保险股份有限公司、安心财产保险有限责任公司、中国再保险（集团）股份有限公司、阳光保险集团股份有限公司、泰康保险集团股份有限公司、 华为技术有限公司、深圳市腾讯计算机系统有限公司、北京青云科技股份有限公司、云栈科技（北京）有限公司、杭州数梦工场科技有限公司、北京易捷思达科技发展有限公司。

本标准起草人：栗蔚、郭雪、孔松、卫斌、刘震、王龙涛、李玉山、胡罡、顾睿、张宁军、袁红、于希金、李文鹏、张云龙、冯键、成宇、尹琛、廖东升、黄建坤、段红帅、白阳、赵华、符海芳、蒋增增、武献雨、傅帅、张春源、杜建伟、李小庆、宋敬海、刘宏亮、张敏。

引　言

为推进保险行业落地云计算应用，提高保险行业科技创新能力，本标准结合保险行业业务特点和信息系统建设需要，对保险行业云计算场景和总体框架做出规范，为保险机构规划和使用云计算提供指引，同时为云服务提供者和云计算软件厂商能够提供满足保险行业实际需求的云计算服务或软件提供依据。

保险行业云计算场景和总体框架

1 范围

本标准规定了保险行业的云计算场景和总体框架。

本标准适用于保险行业等相关组织对云计算的规划和使用，也可为云计算服务商和云计算软件厂商设计和建设保险行业的云计算提供依据。

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，仅所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 32400-2015 信息技术 云计算 概览与词汇

JR/T 0071-2012 金融行业信息系统信息安全等级保护实施指引

JR/T 0166-2018 云计算技术金融应用规范技术架构

JR/T 0168-2018 云计算技术金融应用规范 容灾

3 术语和定义

下列术语和定义适用于本文件。

3.1

云计算 cloud computing

一种通过网络将可伸缩、弹性的共享物理和虚拟资源池按需自服务的方式供应和管理的模式。

注：资源包括服务器、操作系统、网络、软件、应用和存储设备等。

[GB/T 32400-2015，定义3.2.5]

3.2

云服务提供者 cloud service provider

提供云服务的参与方。

[GB/T 32400-2015，定义3.2.15]

3.3

公有云 public cloud

云服务可被任意云服务客户使用，且资源被云服务提供者控制的一种云部署模型。

[GB/T 32400-2015，定义3.2.33]

3.4

私有云 private cloud

云服务仅被一个云服务客户使用，且资源被该云服务客户控制的一类云部署类型。
[GB/T 32400-2015，定义3.2.32]

3.5

行业云 community cloud

团体云 organization cloud

服务由一组特定的云服务使用者使用和共享,且资源被云服务提供者或使用者控制的一种云部署模式。这组云服务提供者和使用者在监管政策、安全要求等方面相同或高度相似。
[JR/T 0166-2018，定义3.10]

3.6

混合云 hybrid cloud

至少包含两种不同的云部署模型的云部署模型。
[GB/T 32400-2015，定义3.2.23]

3.7

基础设施即服务 infrastructure as a service

为云服务客户提供云能力类型中的基础设施能力类型的一种云服务类别。
[GB/T 32400-2015，定义3.2.24]

3.8

平台即服务 platform as a service

为云服务客户提供云能力类型中的平台能力类型的一种云服务类别。
[GB/T 32400-2015，定义3.2.30]

3.9

软件即服务 software as a service

为云服务客户提供云能力类型中的应用能力类型的一种云服务类别。
[GB/T 32400-2015，定义3.2.36]

3.10

同城可用区 availability zone in the same region

能够抵御因供电供水中断、水淹、火灾、网络故障、硬件损毁、交通中断等灾难同时影响的两个可用区互为同城可用区。一般情况下两同城可用区之间地理距离为数十公里。
[JR/T 0168-2018，定义3.10]

3.11

异地可用区 availability zone in the different region

能够抵御因战争、洪水、海啸、台风、地震等大范围区域性灾害同时影响的两个可用区互为异地可用区。一般情况下两异地可用区之间地理距离为数百公里以上。

[JR/T 0168-2018，定义3.11]

3.12

敏感数据 sensitive data

敏感数据是指一旦泄露可能会对用户或金融机构造成损失的数据，包括但不限于：

a) 用户敏感数据，如用户口令、密钥等；

b) 系统敏感数据，如系统的密钥、关键的系统管理数据；

c) 其他需要保密的敏感业务数据；

d) 关键性的操作指令；

e) 系统主要配置文件；

f) 其他需要保密的数据。

[JR/T 0071-2012，定义3.1]

4 保险行业云计算需求

4.1 新建保险机构信息系统建设

中小型保险企业在筹建初期，面临自建机房耗时耗力、业务规模难以准确预估、信息技术人才储备不足等问题，全业务部署行业云或公有云，发展信息科技面临的财力、人力压力可以得到极大减轻，从而使其集中投入发展核心业务。

对于在筹建初期有能力搭建私有云的保险企业，在全面预估未来发展趋势后，可自建私有云平台，以更有力的保证信息与资金安全。

4.2 构建新型系统

保险企业新型服务层出不穷，各种互联网保险产品开发、上线、迭代速度越来越快，利用云计算，可以提升服务系统的灵活性，实现系统快速交付，有效应对市场和客户的需求变化。

4.3 优化灾备环境

保险企业自建灾备中心存在IT设备资源利用率较低、维护成本高等问题。将灾备环境部署在行业云，能够有效降低运维成本和人力成本。

4.4 已有信息系统上云

4.4.1 总则

根据涉及敏感数据的数量、数据加解密方案可靠性、系统架构云化改造难度等方面，保险行业信息系统可分为如下四类，如图1所示。四类系统说明如下：

——不涉及或涉及较少的敏感数据的信息系统，具体包括：移动系统、IM系统、办公系统、培训系统、呼叫中心、积分系统、网点管理、公示信息查询、机房运维管理和短信平台等系统，若数据加解密方案可靠性很高，系统架构可平滑完成云化部署，可考虑首先上云；

——涉及部分敏感数据的信息系统，具体包括：网上投保、第三方支付、电子支付、自助查询系统、监管报送、电信反欺诈、经营分析、费控、资金、单证系统、绩效考核和邮件系统等，若数据加解密方案可靠性较高，云化时主要面临接口模式或数据对接类改造，可考虑其次上云；

——涉及较多敏感数据的信息系统，具体包括：统一客户信息、客户关系系统、营销系统、审计、智能风控、财务管理、人力资源、反洗钱、智能双录、事后监督和统一监控等，若数据加解密方案可靠性一般，云化时面临分布式改造、信息安全等方面问题，可考虑下一阶段上云；

——承载保险行业核心业务的信息系统，具体包括：核心业务系统、收付系统、管理策略平台、平台配置、单点登录、准备金和偿付能力等，敏感数据数量庞大，若数据加解密方案可靠性较低，一旦故障，企业、用户将面临巨大损失，可考虑最后阶段上云。

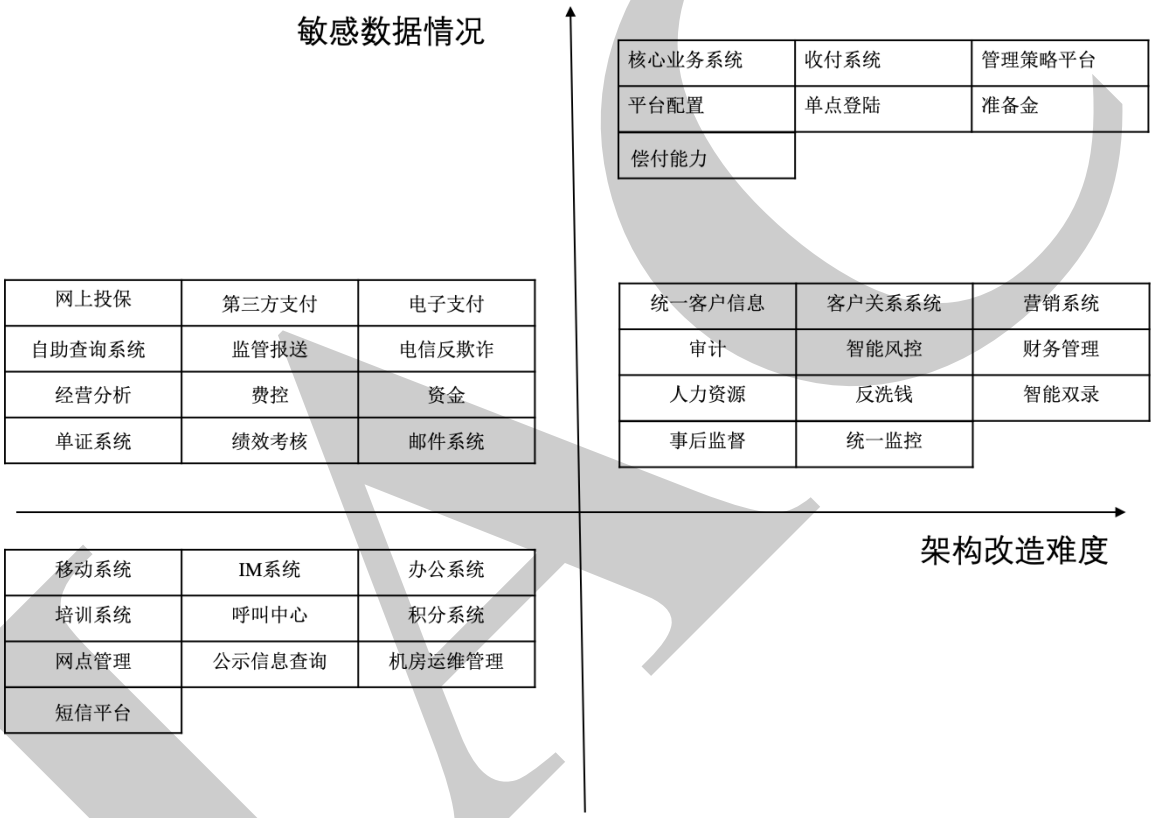

图1　保险业信息系统分类

4.4.2　敏感数据情况决定部署模式

敏感数据情况是对涉及敏感数据的数量以及数据加解密方案可靠性的综合考量。敏感数据数量较少，数据加解密方案可靠性较高的系统，可优先上云选择；对于涉及敏感数据较多的系统，可根据数据加密存储方案的可靠性，审慎选择云计算部署模式。

4.4.3　技术架构确定是否上云

已有信息系统的实现技术能够平滑云化时，适合优先上云。

对于系统架构云化改造较困难、涉及敏感数据较多且数据加密存储方案可靠性较低的的信息系统，若云化后具有较大性能提升或明显优势时可选择上云。优势包括但不限于：

——支撑业务爆发增长：支持快速的资源弹性扩展，满足突发海量交易的需求；

——并发访问：提高系统的请求承受能力，满足投保、查保等系统面临的数据存取与访问要求；
——快速开发迭代：实现系统快速交付，有效应对市场和客户的需求变化；
——降低运维成本：使用云服务，保险企业可降低配备IT专业运维人员的数量，同时可实现自动化运维功能，降低运维成本。

5 保险行业云计算部署模式

5.1 公有云/行业云

保险行业的公有云或行业云从应用接入、数据处理和服务处理等层面，深入满足保险行业业务需求，提供符合监管要求的数据安全与灾备能力，保障保险系统的高可用、高安全、高可靠性。

保险行业应严格遵守国家和监管部门关于信息化工作外包的法律法规与要求，建立有效的评估审核流程与监督管理机制，定期对云服务提供方技术实力、安全资质、风险控制水平、诚信记录、财务状况等方面进行审查与评估。

公有云/行业云应主要满足如下要求：
——计量准确性；
——迁移性，云平台技术、架构体系应无厂商锁定。在保险行业终止或变更服务时，应用、数据应能够采用行业通用打包与加密格式便捷的迁移到其他云平台，同时也应支持迁移到本地的实体机环境。

5.2 私有云

保险行业基于自身技术能力条件搭建私有云平台。在搭建私有云平台时，可以向云计算软件厂商购买计算虚拟化产品、存储虚拟化产品、网络虚拟化产品、虚拟化管理平台产品等软件产品和驻场运维支持服务，同时也可购买基础硬件设施与设备，包括机房等基础设施以及计算、存储、网络等设备。

私有云应主要满足如下要求：
——采用统一、规范的架构体系；
——各公司可根据自身业务情况考虑，进行资源预留；
——支持资源高效交付，提升信息系统稳定性；
——容灾备份应至少保证同城双中心，可自主选择建设异地数据级灾备中心，可根据自身业务需求评估是否建设双活数据中心；
——构建运维安全审计系统，建立完善的合规审查机制，以满足保险行业监管机构等机构的监督检查。

5.3 混合云

不同保险业务具有不同组网要求，保险行业可根据需求搭建混合云架构。混合云的应用场景主要包括：流量突增业务的负载扩充，灾难恢复，数据备份，开发测试生产环境部署和应用部署。其中应用部署主要分为两种情况，核心应用部署在私有云而非核心应用部署在公有云/行业云，或前台应用部署在公有云/行业云而核心数据仍保留在私有云中，以保证核心数据安全可控。

混合云应主要满足如下要求：
——网络联通，支持专线、裸光纤等网络接入方式实现公有云/行业云和私有云的联通；
——可管理性，包括资源管理、监控管理、告警管理、用户管理、虚拟私有云管理等；
——统一的混合云管理平台，实现混合云环境的集中监控，告警和运维。构建统一的API网关，实现不同云提供统一的接口进行管理。

6 保险行业云计算架构特性

6.1 合规性

云平台的建设和管理，从硬件、机房、网络、系统运维、安全等方面均应满足保险行业监管机构的监管要求。

6.2 高弹性

云平台应具有较强的弹性伸缩能力。在保险行业业务需求高峰增长时应具备无缝增加云资源（如计算、存储、网络等）的能力，在业务需求下降时应具备自动减少云服务器实例以节约成本的能力。

6.3 高可靠性

云平台服务具有高可靠性。单点或多点发生故障时，能迅速恢复至可用状态，以确保保险行业日常业务能够连续运行，不出现中断。

6.4 强部署性

云平台支持大规模部署、自动部署，具有一键部署功能。能够实时跟踪部署流程进度，快速定位部署异常，以提高生产效率、降低出错可能。

6.5 开放性

满足保险企业多重业务对接需求。具有开放的API接口，可以实现与第三方管理软件工具结合或二次开发。

6.6 安全性

具有完善的数据安全等安全风险管理体系，满足保险行业各项安全防护需求。

7 保险行业云计算应用场景

7.1 总则

云计算在保险行业的典型应用场景可分为开发测试云、生产云和灾备云，保险企业可自行选择并应用。生产云与开发测试云之间应至少支持逻辑隔离。

注：以下云计算在保险行业的典型应用场景，对于部署在同一个云上或多个云上不做限制要求。

7.2 开发测试云

保险行业测试业务多、开发项目较为独立，存在资源分配难、资源利用率低、资源调配灵活度低、运维响应慢等问题。开发测试环境上云可有效解决上述问题。开发测试云应具备如下功能：

——基于主流技术架构，避免被单一厂商锁定；

——支持资源的快速调配，提高资源利用率，降低开发测试成本；

——开发测试协同。

7.3 生产云

保险企业可根据信息系统所承载数据的敏感程度、业务的重要性等因素综合考量后，将系统生产环境迁移到云计算平台，把保险行业中自行构建的高风险高成本的系统服务替换为云平台上的高可靠低成本服务。生产云应具备如下功能：

——基于主流技术架构，避免被单一厂商锁定；

——应用迁移：云计算产品或服务应具备较好的兼容性，保证保险行业能够自主或在厂商技术人员提供一定支持的情况下完成已有应用的迁入。在保险行业不再使用云计算产品或服务时，保证应用、数据等的迁出。

7.4 灾备云

信息科技系统灾备建设对保险行业来说至关重要，必须要有一个可靠的容灾系统在灾难到来时保障业务稳定运行。保险行业自建灾备中心投入大，建设周期长，使用灾备云能有效降低建设成本和人力成本。保险行业灾备云应满足如下要求：

——基于主流技术架构，避免被单一厂商锁定；

——容灾备份应至少保证同城双中心，可自主选择建设异地灾备中心，可根据自身业务需求评估是否建设双活数据中心；

——分支机构系统应可以切换成直接与灾备中心相连通信；

——支持通过专线接入的方式连接保险行业的自有机房，保障数据完整性和安全性；

——云灾备环境所属数据中心机房建设遵从保险行业监管机构的合规要求；

——针对不同类别信息系统，云灾备环境应满足相应灾难恢复能力等级要求。

8 架构体系

云平台总体架构可以分为基础设施、资源抽象与管理、基础设施即服务、平台 即服务、软件即服务、统一管理和信息安全等部分，具体体系架构图见图 2：

——基础设施：构建云平台的整套设施，包括数据中心及灾备中心等基础设施以及计算、存储、网络等设备，数据中心网络内部应采用高可靠，可拓展的整体架构，应支持异地多活的跨数据中心的网络架构。构建云平台的硬件设施应该满足体系架构开放、安全可控等要求；

——资源抽象与管理：利用虚拟化技术，将云基础资源以虚拟机的方式进行组织。应支持统一管理多种虚拟技术，可相互转化虚拟资源与物理资源等基本要求。关键技术包括计算虚拟化、存储虚拟化、网络虚拟化和虚拟化管理等；

——基础设施即服务：提供虚拟计算机、存储、网络等计算资源，提供访问云基础设施的服务接口，用户可在这些资源上部署或运行操作系统、中间件、数据库和应用软件等。包括但不限于云主机服务、存储服务、负载均衡服务、云备份服务；

——平台即服务：云服务提供方向保险行业提供运行在云基础设施之上的软件开发和运行平台，如：标准语言与工具、数据访问、通用接口等。包括但不限于中间件服务、容器服务、数据库服务、微服务架构等。云计算使用者可基于平台即服务进行系统研发、测试、运行、生产和维护等工作；

——软件即服务：提供软件和应用服务。用户购买服务而非软件版次，可利用不同设备上的用户端（如 WEB 浏览器）或程序接口通过网络访问和使用应用软件。在提供服务时，应满足保险领域相应类型的信息系统在服务外包、信息安全和业务流程等方面的监管要求。服务包括但不限于核心服务，渠道服务，产品服务，管理信息，客户服务，风险管理等；

——统一管理：能够对基础设施和 IT 服务进行统一管理。基础设施云管理包括用户层云管理与资源池管理；IT 服务管理应包括集中监控、运维操作、运维分析、配置管理、服务流程管理和研发运营一体化等；

——数据管理：应对用户数据进行全生命周期的严格保护，保证数据在采集，传输，处理，交换，存储，销毁的过程中的完整性。

——信息安全：保险行业对数据安全、信息系统可靠性具有较高要求，云平台应提供管理、数据、中间件、应用、虚拟化、系统、网络、物理等方面的安全支持能力。

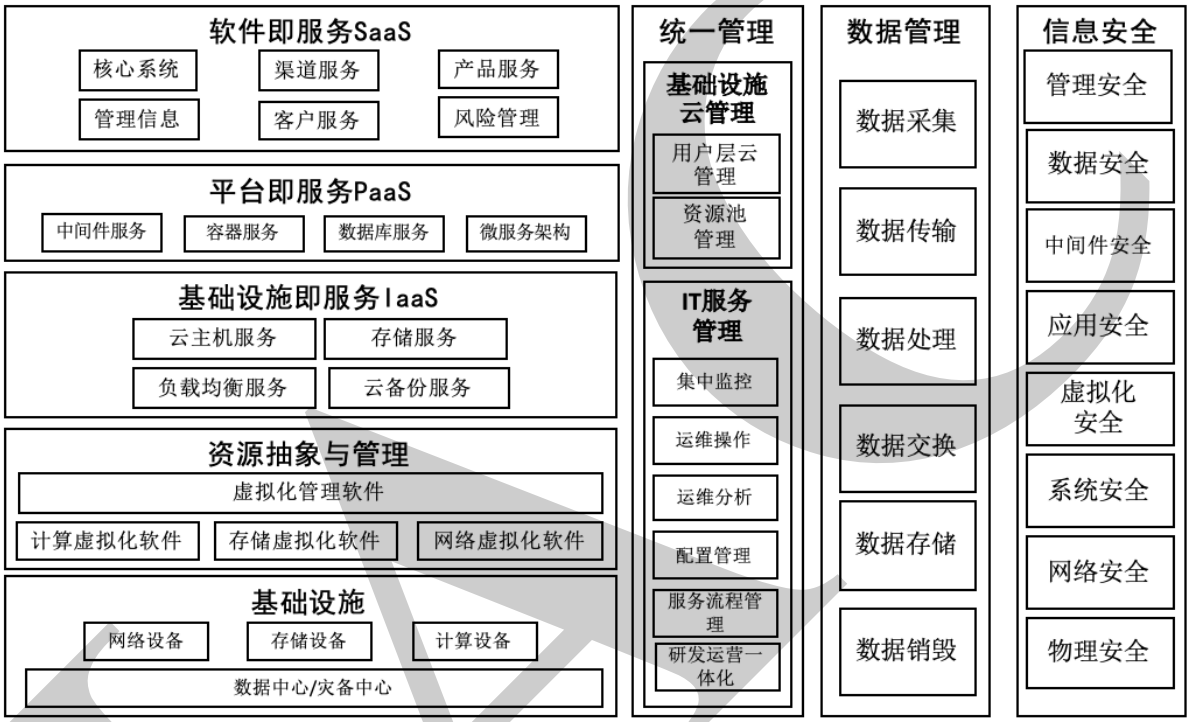

图 2　保险行业云平台体系架构图

参 考 文 献

[1] GB/T 22080-2008 信息技术 安全技术 信息安全管理体系要求
[2] GB/T 22081-2008 信息技术 安全技术 信息安全管理实用规则
[3] GB/T 31167-2014 信息安全技术 云计算服务安全指南
[4] GB/T 31168-2014 信息安全技术 云计算服务安全能力要求
[5] GB/T 31496-2015 信息技术 安全技术 信息安全管理体系实施指南
[6] GA/T 1390.2-2017 信息安全技术 网络安全等级保护基本要求 第 2 部分：云计算安全扩展要求
[7] JR/T 0071-2012 金融行业信息系统信息安全等级保护实施指引
[8] JR/T 0072-2012 金融行业信息系统信息安全等级保护测评指南
[9] JR/T 0073-2012 金融行业信息安全等级保护测评服务安全指引
[10] JR/T 0167-2018 云计算技术金融应用规范 安全技术要求
[11] ISO/IEC TR 27015:2012 信息技术 安全技术 金融服务信息安全管理指南