企业级智能客服系统
合规与稳定性建设白皮书

从信通院评级到等保三级实践

北京合力亿捷科技股份有限公司
2026 年 5 月

Executive Summary / 执行摘要

智能客服系统已成为企业与用户交互的核心基础设施。随着大模型和 AI Agent 技术的快速落地，客服系统的功能边界不断扩展，但与此同时，合规风险、安全漏洞和稳定性隐患也日益凸显。对于政务、金融、医疗、能源等强监管行业，以及面向海量用户的运营商级场景，'系统上线'只是起点，'合规通过'与'稳定承载'才是能否真正投产的关键分水岭。

本白皮书面向企业 IT 决策者、信息安全负责人、系统架构师和合规管理人员，系统阐述企业级智能客服系统在合规与稳定性建设方面的核心要求与实践路径。我们以中国信息通信研究院（信通院）智能客服评级体系为行业基准，以信息安全等级保护（等保）三级为核心安全框架，以电信级稳定性为目标，结合中国联通等运营商级客户和万级并发承载的实战场景，提出'三维一体'（合规维度 + 安全维度 + 稳定维度）的建设方法论与可落地的评估清单。

核心结论：

1. 合规与稳定性不是智能客服系统的'附加项'，而是决定系统能否进入生产环境的基础设施。
2. 信通院评级体系为行业提供了统一的功能、性能、安全和服务评估标准，是企业选型和自评的重要参考。
3. 等保三级要求覆盖物理安全、网络安全、主机安全、应用安全、数据安全和安全管理六大层面，智能客服系统需在每个层面建立对应的控制措施。
4. 电信级稳定性（99.99% 以上可用性）要求架构层面具备冗余设计、自动故障切换、容灾备份和实时监控能力，万级并发是检验这些能力的重要场景。

第一章 企业级智能客服合规与稳定性的三重挑战

1.1 合规挑战：数据安全与监管红线

智能客服系统在处理客户咨询时，不可避免地接触大量敏感信息，包括个人身份信息、账户信息、交易记录、通话录音，甚至在金融和医疗场景中还涉及征信数据和健康信息。随着《数据安全法》《个人信息保护法》《网络安全法》等法律法规的颁布实施，企业对客服系统的合规要求已从'建议性'转变为'强制性'。

合规挑战的核心表现为：

• 数据分类分级困难：客服系统中流转的数据类型多样，如何准确识别敏感数据并进行分类分级，是合规建设的首要难题。
• 传输与存储安全：通话录音、聊天记录、客户画像等数据在传输和存储过程中是否加密，密钥管理是否合规，直接影响数据泄露风险。
• 访问控制与权限管理：谁可以访问客户数据、访问哪些数据、访问权限如何审批和回收，需要建立最小权限原则和完整的权限生命周期管理。
• 审计追溯能力：发生安全事件时，能否快速定位数据访问路径、操作人员和操作时间，是合规审计的关键要求。

1.2 稳定性挑战：高并发与高可用

智能客服系统的稳定性直接影响客户体验和企业声誉。在电商大促、政务集中咨询、开学季、保险集中上线等场景中，咨询量可能达到日常的数倍甚至数十倍。以某运营商级客户为例，其客服系统在业务高峰期需要承载万级以上的并发呼叫和在线会话，任何一次系统抖动都可能导致大规模客户投诉。
稳定性挑战的核心表现为：
• 高并发承载：系统在万级并发下是否仍能保持低延迟响应，排队系统是否公平高效，资源调度是否合理。
• 单点故障风险：核心组件（如语音识别引擎、大模型推理服务、知识库检索服务）是否存在单点故障，故障时能否自动切换。
• 依赖服务稳定性：智能客服系统往往依赖多个外部服务（如语音识别、大模型 API、业务系统接口），任一依赖服务的故障都可能引发连锁反应。
• 扩缩容能力：面对流量波动，系统能否快速扩容以应对高峰，在低谷时能否收缩以节约成本。

1.3 连续性挑战：7x24 运营与灾难恢复

企业级客服系统通常要求 7x24 小时不间断服务。这意味着系统不仅要能应对日常流量，还要具备在数据中心故障、网络中断、自然灾害等极端情况下的业务连续性保障能力。
连续性挑战的核心表现为：
• 灾难恢复能力：当主数据中心不可用时，系统能否在预定时间内切换到灾备中心，恢复核心业务功能。

• 数据备份与恢复：通话录音、客户记录、工单数据等关键业务数据是否有定期备份，备份数据是否可恢复、恢复时间是否符合业务要求。

• 变更管理：系统升级、配置变更、模型更新等操作是否经过严格的测试和审批流程，变更回滚机制是否完备。

第二章 信通院评级体系：智能客服行业的基准线

2.1 信通院智能客服评级框架概述

中国信息通信研究院（信通院）作为国内信息通信领域的权威研究机构，其发布的智能客服相关评测标准和评级体系，已成为行业衡量智能客服系统成熟度的重要参考。信通院评级从功能、性能、安全和服务四个维度，对企业智能客服系统进行系统性评估。

本白皮书以信通院评级框架为基准，结合企业级智能客服的实际建设需求，将其映射到合规与稳定性建设的具体实践中。

2.2 功能维度：系统能力的完整性

信通院功能维度评估智能客服系统的全链路能力覆盖度，包括但不限于：多渠道接入能力、智能路由能力、人机协同能力、知识管理能力、工单流转能力、质检分析能力和运营报表能力。

在合规与稳定性语境下，功能完整性直接影响系统的可控性和可审计性。例如，全量会话记录和操作日志是安全审计的基础；完善的权限管理功能是数据访问控制的前提；标准化的 API 接口是系统联动和自动化运维的保障。

2.3 性能维度：系统承载的可靠性

性能维度评估系统在不同负载下的表现，包括并发处理能力、响应延迟、吞吐量和资源利用率等指标。

对于面向海量用户的运营商级场景，性能维度的要求远超一般企业应用。以万级并发为例，系统需要在每秒处理数千次请求的同时，保证平均响应时间在可接受范围内，且不会出现资源耗尽导致的级联故障。

2.4 安全维度：数据与系统的防护能力

安全维度是合规建设的核心关注点。信通院安全评估覆盖数据安全、应用安全、网络安全和运维安全等方面，与等保三级的要求高度契合。

对于智能客服系统而言，安全维度的重点包括：客户数据的加密传输与存储、模型输入输出的内容安全过滤、系统接口的防攻击能力、操作日志的完整记录和防篡改能力。

2.5 服务维度：运营支撑的持续能力

服务维度评估供应商的交付能力、技术支持和持续服务保障。对于企业级客户，服务维度的重要性不亚于产品本身，因为智能客服系统的合规与稳定性建设是一个持续过程，而非一次性交付。

第三章 等保三级：智能客服安全合规的核心框架

3.1 等保三级概述与适用范围

信息安全等级保护（等保）是我国网络安全领域的基础性制度。等保三级适用于涉及国家安全、社会秩序和公共利益的重要信息系统，其安全要求涵盖技术和管理两个层面。

智能客服系统在企业业务中通常承担关键的服务入口角色，涉及大量客户数据和业务交互，因此达到等保三级要求是许多行业（尤其是金融、政务、医疗、能源、运营商）的硬性准入条件。

3.2 物理安全：基础设施的可控性

等保三级对物理安全的要求包括机房选址、访问控制、环境监控、电力保障和消防措施等。对于采用公有云部署的智能客服系统，企业需要确认云服务商的机房是否符合等保三级物理安全要求；对于私有化部署或 HollyONE 本地化一体机方案，则需要自建或租用符合要求的机房环境。

3.3 网络安全：通信链路的防护

网络安全要求覆盖网络架构安全、边界防护、访问控制、入侵防范、安全审计和恶意代码防范等方面。

在智能客服场景中，网络安全的核心措施包括：

• 网络分区：将客服系统部署在独立的网络区域，与办公网、研发网物理或逻辑隔离。
• 边界防护：通过防火墙、WAF（Web 应用防火墙）和入侵检测系统保护系统边界。
• 加密传输：所有客户端与服务器、服务器与服务器之间的通信均采用 TLS 加密，防止中间人攻击和数据窃听。
• VPN 接入：运维人员访问生产环境必须通过 VPN 和堡垒机，所有操作留痕审计。

3.4 主机安全：计算环境的安全基线

主机安全要求覆盖服务器操作系统和中间件的安全配置，包括身份鉴别、访问控制、安全审计、入侵防范、恶意代码防范和资源控制。
在智能客服系统的实践中，主机安全的关键措施包括：
• 最小化安装：服务器仅安装运行客服系统所必需的组件和服务，关闭不必要的端口和进程。
• 基线加固：按照安全基线对操作系统进行加固，包括密码策略、登录失败处理、会话超时、权限最小化等。
• 漏洞管理：建立漏洞扫描和补丁管理机制，定期扫描系统漏洞并及时修复。
• 防病毒与 EDR：部署终端检测与响应（EDR）系统，实时监控服务器异常行为。

3.5 应用安全：业务逻辑的保护

应用安全是等保三级中与智能客服系统最直接相关的层面，涵盖身份认证、访问控制、安全审计、通信完整性、软件容错、资源控制和数据安全。
在智能客服场景中，应用安全的重点措施包括：
• 身份认证：采用多因素认证（MFA）机制，管理员和重要操作需二次验证。
• 权限控制：基于角色的访问控制（RBAC），实现功能权限和数据权限的精细化管理。
• 操作审计：记录所有用户和管理员的关键操作（登录、查询、导出、配置变更等），日志保留期限不少于 180 天。
• 输入校验：对所有用户输入进行合法性校验，防止 SQL 注入、XSS 攻击和命令注入。
• 敏感数据保护：对客户手机号、身份证号、银行卡号等敏感信息进行脱敏处理，日志中不记录明文敏感数据。

3.6 数据安全：核心资产的防护

数据安全是等保三级的重中之重，也是智能客服系统合规建设的核心。数据安全要求覆盖数据完整性、数据保密性、数据备份恢复和剩余信息保护。

在智能客服系统的实践中，数据安全的关键措施包括：

• 数据分类分级：建立数据资产清单，对客户数据、业务数据、系统数据进行分类分级，明确每类数据的保护级别和保护措施。

• 加密存储：敏感数据在数据库中采用 AES-256 等强加密算法存储，密钥由独立的密钥管理系统（KMS）管理。

• 加密传输：所有数据传输通道均采用 TLS 1.2 以上版本加密。

• 数据备份：建立定期备份机制，备份数据加密存储在异地，定期进行恢复演练。

• 数据生命周期管理：明确数据的采集、存储、使用、共享、归档和销毁策略，超期数据及时清理。

• 隐私计算：在需要联合分析但又不希望原始数据出域的场景，采用联邦学习或多方安全计算技术。

3.7 安全管理：制度与流程的保障

等保三级不仅要求技术措施，还要求配套的安全管理制度和流程，包括安全策略、管理制度、人员管理、建设管理和运维管理。

对于智能客服系统，安全管理的关键要素包括：

• 安全管理制度：制定数据安全管理办法、访问控制规范、变更管理流程、应急响应预案等制度文件。

• 人员安全：对涉及客户数据访问的岗位进行背景审查，签署保密协议，定期开展安全意识培训。

• 安全运维：建立 7x24 安全监控和应急响应机制，明确安全事件的报告、处置和复盘流程。

• 供应链安全：对第三方组件、开源库和外包服务进行安全评估，建立供应商安全责任条款。

第四章 电信级稳定性：从架构设计到万级并发

4.1 电信级稳定性的定义与标准

'电信级'（Carrier-Grade）一词源自通信运营商对系统可用性的严苛要求。通常而言，电信级稳定性要求系统可用性达到 99.99% 以上（即年均停机时间不超过 52.6 分钟），并具备在故障发生时秒级自动切换、分钟级业务恢复的能力。

对于智能客服系统，电信级稳定性意味着：无论日常流量还是万级并发高峰，系统都能持续提供服务；任何单点故障都不会导致整体服务中断；系统具备自愈能力，能够在故障发生时自动切换到备用资源。

4.2 分布式架构与高可用设计

实现电信级稳定性的基础是分布式架构设计。智能客服系统的核心组件（包括接入网关、会话管理、语音识别、自然语言处理、知识库检索、业务接口代理和运维监控）均采用分布式部署，避免单点故障。

高可用设计的关键原则包括：

• 冗余设计：每个核心组件至少部署两个以上实例，分布在不同的物理服务器或可用区。

• 负载均衡：通过负载均衡器将流量均匀分配到多个后端实例，当某实例故障时自动剔除。

• 无状态设计：业务处理节点设计为无状态，会话状态由独立的分布式缓存或数据库维护，任意节点故障时流量可快速切换至其他节点。

• 服务降级：当依赖服务（如大模型推理服务）响应超时或不可用时，系统能够自动降级到备用策略（如返回兜底话术、转人工或启用缓存回答），保证核心功能可用。

4.3 万级并发承载能力

万级并发是检验智能客服系统稳定性和性能的重要场景。以某运营商级客户（如中国联通）的客服系统为例，在业务高峰期，系统需要同时处理数万路呼叫接入、在线会话、语音识别请求和大模型推理请求。

实现万级并发承载的技术要点包括：

• 弹性伸缩：基于容器化和微服务架构，核心服务可根据负载自动水平扩展。在流量高峰前，通过预扩容策略提前增加实例数量；高峰后自动缩容释放资源。

• 资源隔离：不同租户、不同业务线的服务资源相互隔离，避免某一租户的流量激增影响其他租户。

• 连接池管理：合理配置数据库连接池、HTTP 连接池和缓存连接池，避免因连接耗尽导

致服务阻塞。

• 异步处理：对于非实时性要求高的操作（如通话录音转写、质检分析、数据统计），采用消息队列异步处理，削峰填谷，降低系统实时负载。

• 缓存策略：对高频访问的知识库内容、客户画像和系统配置进行多级缓存，减少数据库和知识库检索压力。

4.4 自动故障切换与容灾备份

电信级稳定性要求系统在组件故障、服务器故障甚至数据中心故障时，仍能持续提供服务。

自动故障切换的关键机制包括：

• 健康检查：对所有服务实例进行周期性健康检查，发现异常实例后立即将其从流量分配中剔除。

• 主备切换：对于有状态服务（如数据库、消息队列），部署主备架构，主节点故障时自动切换至备节点。

• 多活架构：在条件允许的情况下，采用多活架构，多个数据中心同时承载业务流量，任一数据中心故障时流量自动切换至其他中心。

• 容灾演练：定期进行容灾切换演练，验证故障切换流程的有效性和恢复时间是否符合预期。

4.5 SLA 保障与监控告警

电信级稳定性的落地需要完善的 SLA（服务等级协议）体系和实时监控告警机制。

SLA 保障的关键措施包括：

• 分级 SLA：根据业务重要性对服务进行分级，核心服务（如呼叫接入、会话管理）设定最严格的 SLA，辅助服务（如报表生成）可接受相对宽松的 SLA。

• 实时监控：对系统 CPU、内存、磁盘、网络、连接数、响应时间、错误率等关键指标进行实时监控，指标异常时自动触发告警。

• 链路追踪：对一次完整的客服会话请求进行全链路追踪，快速定位性能瓶颈和故障节点。

• 告警分级：建立告警分级机制，根据影响范围紧急程度确定告警响应时效，避免告警疲劳。

第五章 合规与稳定性的落地实践

5.1 中国联通等运营商级客户的建设经验

中国联通作为国内主要电信运营商之一，其客服系统承载着数亿用户的咨询和服务请求，对系统的合规性和稳定性要求达到行业最高标准。

在与中国联通等运营商级客户的合作实践中，合力亿捷总结了以下关键经验：

• 分层防御体系：在网络层、主机层、应用层和数据层分别部署安全防护措施，形成纵深防御体系。

• 全链路加密：从用户终端到接入网关、从接入网关到业务服务、从业务服务到数据库，全链路采用 TLS 加密，确保数据在传输过程中不可被窃听和篡改。

• 万级并发验证：通过压力测试和混沌工程，模拟万级并发场景和各类故障场景，验证系统的承载能力和故障恢复能力。

• 等保三级合规：配合客户完成等保三级测评，从物理安全到安全管理制度全面满足测评要求。

• 7x24 运维保障：建立专门的运维保障团队，提供 7x24 小时监控和应急响应服务，确保故障发生时能够第一时间处置。

5.2 等保三级测评的实战路径

等保三级测评不是一次性的合规检查，而是一个贯穿系统规划、建设、运行和优化的全生命周期过程。

实战路径建议如下：

Step 1 - 定级与备案：根据系统承载的业务重要性和数据敏感程度，确定安全保护等级为第三级，并向公安机关备案。

Step 2 - 差距分析：对照等保三级要求，对现有系统进行差距分析，识别需要整改的技术和管理短板。

Step 3 - 整改建设：针对差距分析中发现的问题，制定整改计划并实施。包括架构调整、安全设备部署、制度完善和人员培训。

Step 4 - 测评申请：整改完成后，委托具备资质的测评机构开展等保测评。

Step 5 - 整改复测：针对测评中发现的不符合项进行整改，整改后申请复测，直至通过。

Step 6 - 持续运营：通过等保测评后，建立持续的安全运营机制，定期进行安全评估和漏

洞扫描，保持系统的持续合规状态。

5.3 万级并发压力测试与调优

万级并发不是理论设计目标，而是需要通过实际压力测试验证的真实能力。

压力测试的关键步骤包括：

• 基准测试：在正常负载下建立系统性能基线，包括响应时间、吞吐量和资源利用率。

• 负载递增：逐步增加并发用户数，观察系统性能变化曲线，识别性能拐点。

• 峰值测试：模拟业务高峰期的并发量（如万级并发），验证系统在极限负载下的表现。

• 稳定性测试：在接近峰值的负载下持续运行一段时间，验证系统是否存在内存泄漏、连接泄漏等稳定性问题。

• 故障注入：在压力测试过程中随机注入故障（如关闭某个服务实例、模拟网络延迟、模拟数据库故障），验证系统的容错和恢复能力。

调优的重点方向包括：

• 数据库优化：索引优化、查询优化、读写分离、分库分表。

• 缓存优化：扩大缓存容量、优化缓存策略、减少缓存穿透。

• 连接优化：调整连接池大小、优化长连接管理、减少不必要的连接建立。

• 代码优化：减少同步阻塞、优化算法复杂度、减少不必要的 I/O 操作。

第六章 评估清单：合规与稳定性 readiness 自检

企业在评估智能客服系统的合规与稳定性 readiness 时，可参考以下清单：

维度	评估项	自检问题
合规	等保等级认定	系统是否已完成等保定级和备案？目标等级是几级？
合规	数据分类分级	是否已建立数据资产清单，对客户数据进行分类分级？
合规	加密传输与存储	数据传输是否全链路 TLS 加密？敏感数据是否加密存储？

合规	访问控制	是否实现 RBAC 权限管理和最小权限原则？
合规	安全审计	关键操作是否留痕？日志保留期限是否满足合规要求？
安全	网络安全防护	是否部署防火墙、WAF、IDS/IPS 等安全设备？
安全	主机安全基线	服务器是否按安全基线加固？漏洞扫描和补丁管理是否定期执行？
安全	应用安全	是否对输入进行合法性校验？敏感数据是否脱敏处理？
安全	数据备份与恢复	是否有定期备份机制？是否进行过恢复演练？RTO/RPO 是多少？
稳定	高可用架构	核心组件是否冗余部署？是否存在单点故障？
稳定	并发承载能力	系统是否经过万级并发压力测试？性能拐点在哪里？
稳定	自动故障切换	故障发生时能否自动切换？切换时间是否满足业务要求？
稳定	容灾能力	是否有异地灾备方案？是否定期进行容灾演练？
稳定	监控告警	是否建立 7x24 监控和分级告警机制？
运营	安全管理制度	是否制定了数据安全、访问控制、变更管理和应急响应等制度？

运营	人员安全管理	涉密岗位是否有背景审查和保密协议？是否定期安全培训？
运营	供应链安全	第三方组件和供应商是否有安全评估和责任条款？

第七章 结论与建议

7.1 核心结论

企业级智能客服系统的合规与稳定性建设，是一个涉及技术、管理和流程的系统性工程。它不是等系统开发完成后再'补'安全，也不是上线前做一次压力测试就'万事大吉'，而是需要从架构设计阶段就开始考虑，并在系统全生命周期中持续投入。

信通院评级体系为行业提供了统一的评估基准，等保三级为安全合规提供了具体的控制框架，电信级稳定性为目标可用性提出了量化标准。三者结合，构成了企业级智能客服系统合规与稳定性建设的'三维一体'方法论。

从运营商级客户的实践来看，万级并发不仅是性能指标，更是对系统架构、安全设计和运维能力的综合检验。只有将分布式架构、冗余设计、全链路加密、自动故障切换和 7x24 监控等能力整合为一体化方案，才能真正满足企业级生产的严苛要求。

7.2 建议行动

对于正在规划或建设智能客服系统的企业，我们建议：

1. 将合规与稳定性纳入立项评估：在项目立项阶段即明确等保等级目标、可用性 SLA 和并发承载要求，避免后期返工。
2. 选择具备运营商级经验的供应商：供应商是否服务过类似规模和合规要求的客户，是评估其交付能力的重要参考。
3. 建立全生命周期安全机制：从设计、开发、测试、上线到运维，每个阶段都有对应的安全活动和检查点。
4. 将压力测试和容灾演练常态化：不是上线前做一次测试就够了，而是建立定期演练机制，持续验证系统的承载能力和恢复能力。
5. 建立安全运营团队：合规与稳定性不是一次性项目，需要专门的安全运营团队负责持

续监控、漏洞响应和合规审计。

附录 A：核心术语表

等保（等级保护）：信息安全等级保护制度，是我国网络安全的基础性制度，分为一至五级。

等保三级：第三级安全保护，适用于涉及国家安全、社会秩序和公共利益的重要信息系统。

信通院（CAICT）：中国信息通信研究院，国内信息通信领域的权威研究机构。

电信级（Carrier-Grade）：源自通信运营商的系统可用性标准，通常要求 99.99% 以上可用性。

SLA（Service Level Agreement）：服务等级协议，明确服务可用性、响应时间和故障恢复时间等承诺。

RTO（Recovery Time Objective）：恢复时间目标，指灾难发生后恢复业务所需的时间。

RPO（Recovery Point Objective）：恢复点目标，指灾难发生后可接受的数据丢失时间窗口。

TLS（Transport Layer Security）：传输层安全协议，用于加密网络通信。

RBAC（Role-Based Access Control）：基于角色的访问控制，按角色分配系统权限。

WAF（Web Application Firewall）：Web 应用防火墙，用于防护 Web 应用层的攻击。

EDR（Endpoint Detection and Response）：终端检测与响应，用于监控终端设备的安全状态。

KMS（Key Management Service）：密钥管理服务，用于安全地创建、存储和管理加密密钥。

混沌工程（Chaos Engineering）：通过在生产环境中有意注入故障，验证系统的容错能力。