



2020 北京网络安全大会

2020 BEIJING CYBER SECURITY CONFERENCE

《中国DevOps现状调查报告（2020年）》 解读

中国信息通信研究院
云计算与大数据研究所
刘凯铃



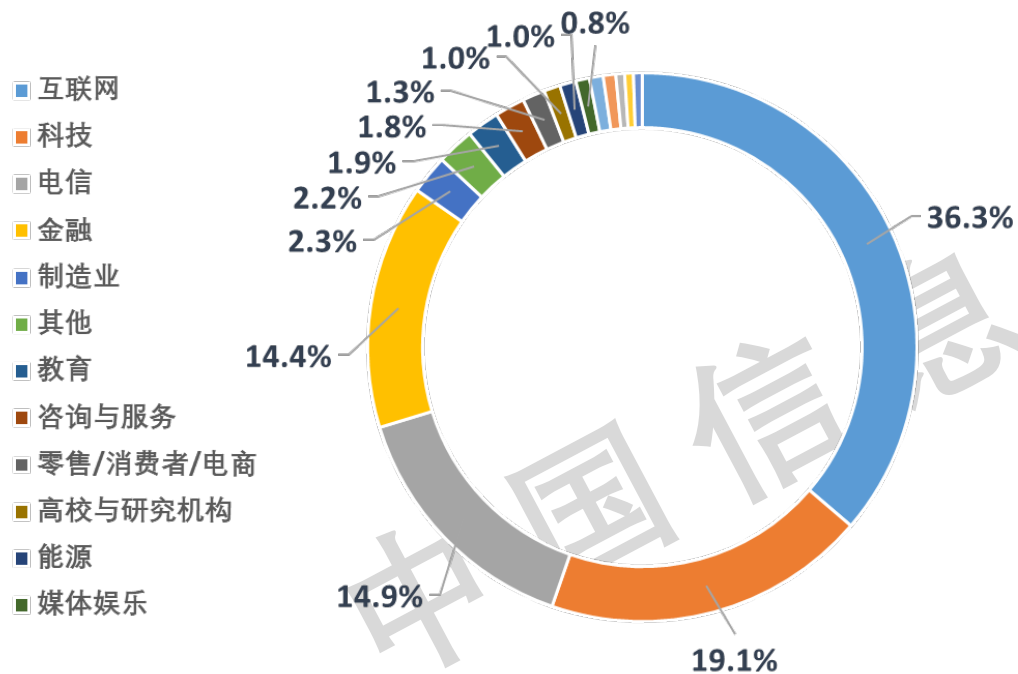
DevOps调查背景





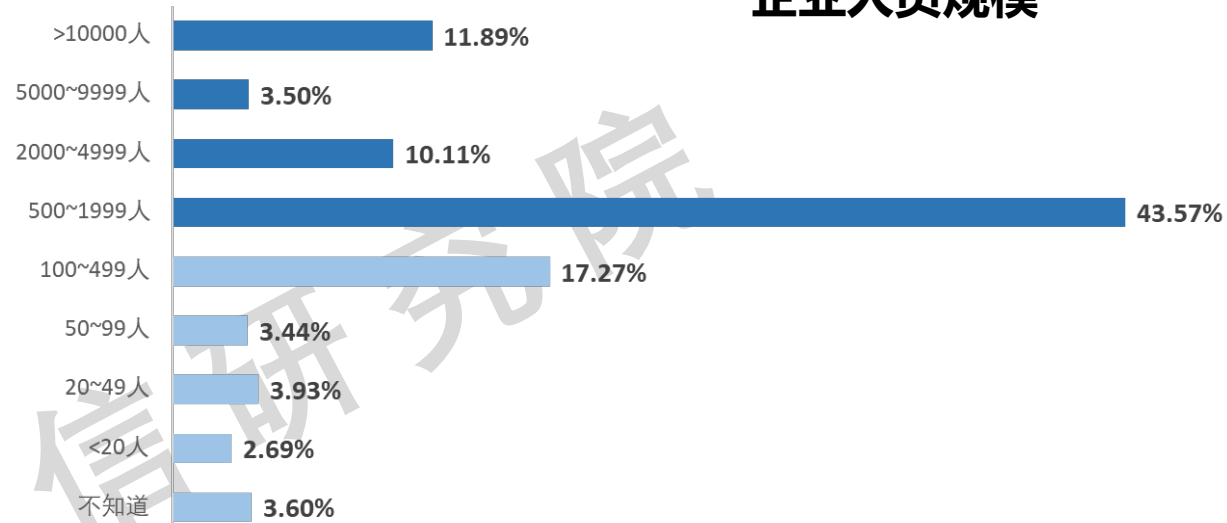
本次调查由中国信息通信研究院联合云计算开源产业联盟、高效运维社区、南京大学、腾讯蓝鲸智云、百度、京东智联云、苏宁消费金融、华为云DevCloud、中国移动通信研究院、中国电信天翼云、中国联通软件研究院、中国农业银行、广东移动、浙江移动、平安科技、云智慧等企业共同发起，各地DevOps实践企业和社会各界也给予了大力支持，在此，谨表示最衷心的感谢。本次调查共收到**1858**份有效问卷，同时也对参与中国DevOps现状调查的企业朋友表示最诚挚的谢意！

企业行业分布



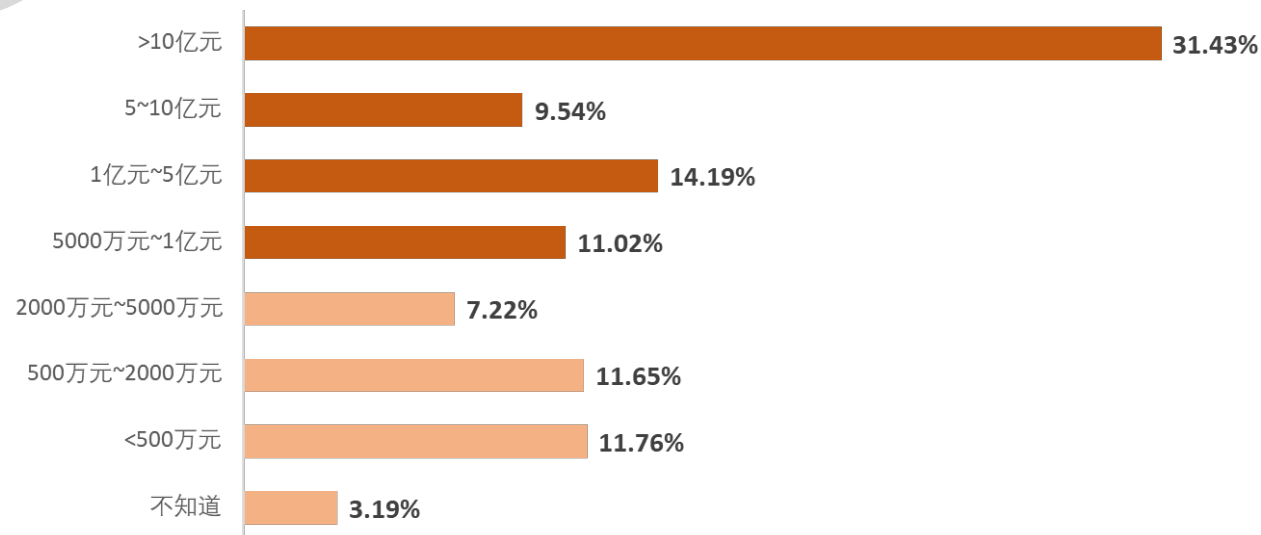
数据来源：中国信息通信研究院

企业人员规模



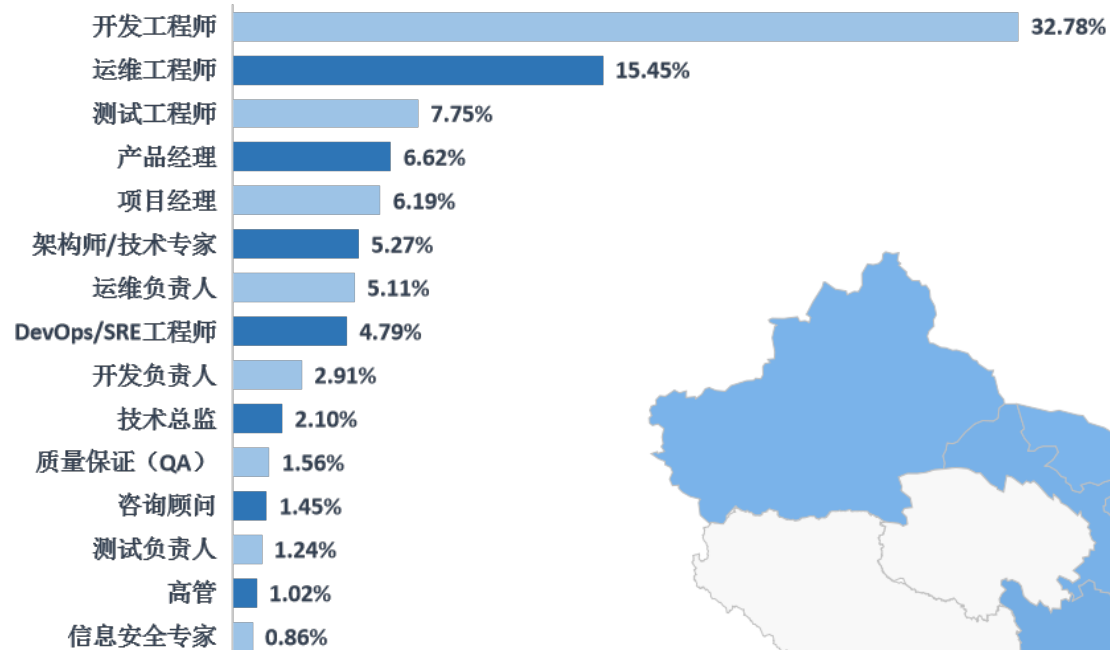
数据来源：中国信息通信研究院

企业资产规模



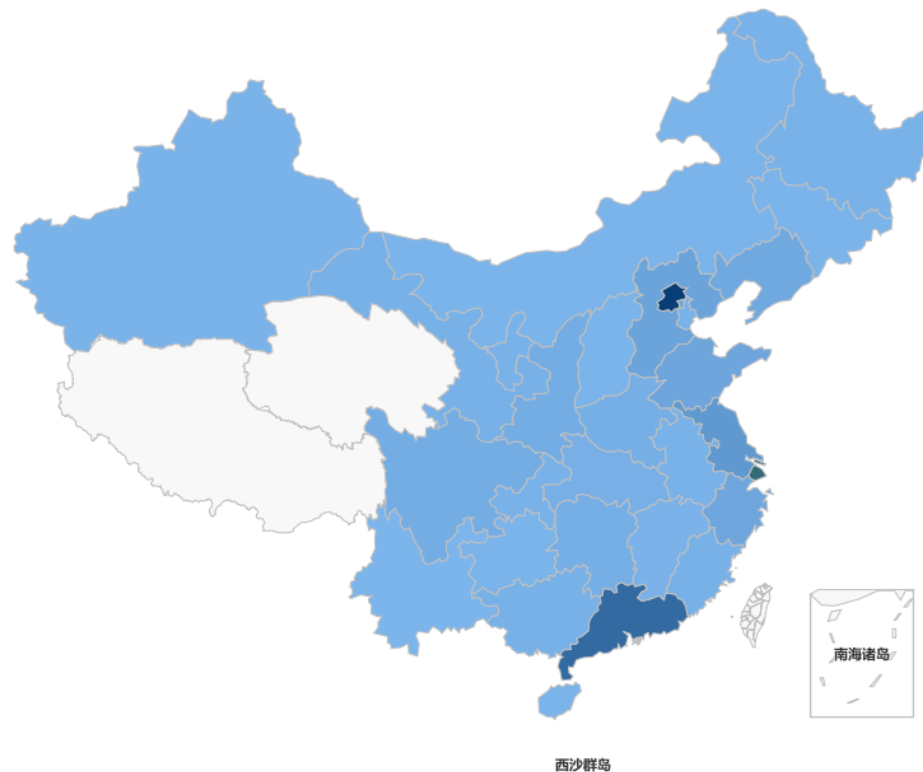
数据来源：中国信息通信研究院

个人职位分布



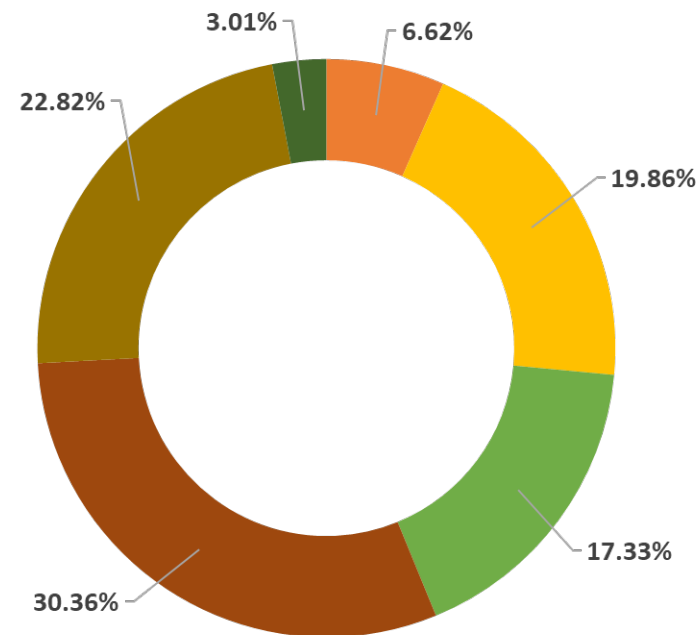
数据来源: 中国信息通信研究院

中国



个人地域分布

个人工作经验



■ <1年 ■ 1-3年 ■ 4-5年 ■ 6-10年 ■ 11-20年 ■ >20年

数据来源: 中国信息通信研究院



DevOps现状

DATA SECURITY

IoT CLOUD

HUMAN PROGRESS

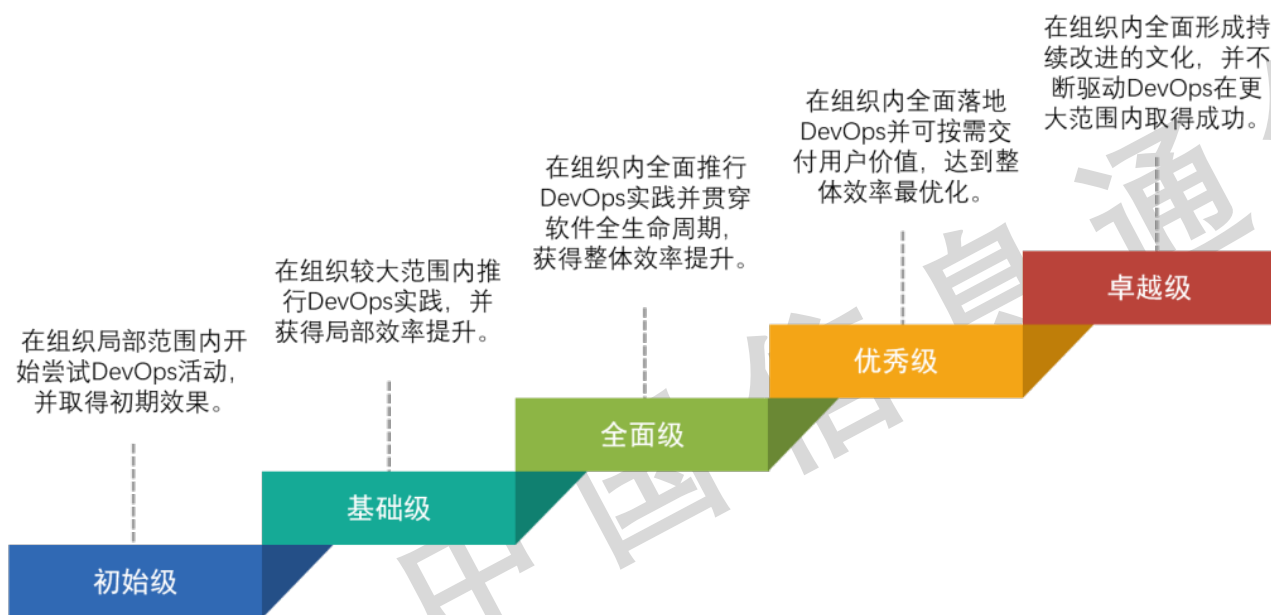
BEHAVIORAL ANAL

TECHNOLOGY

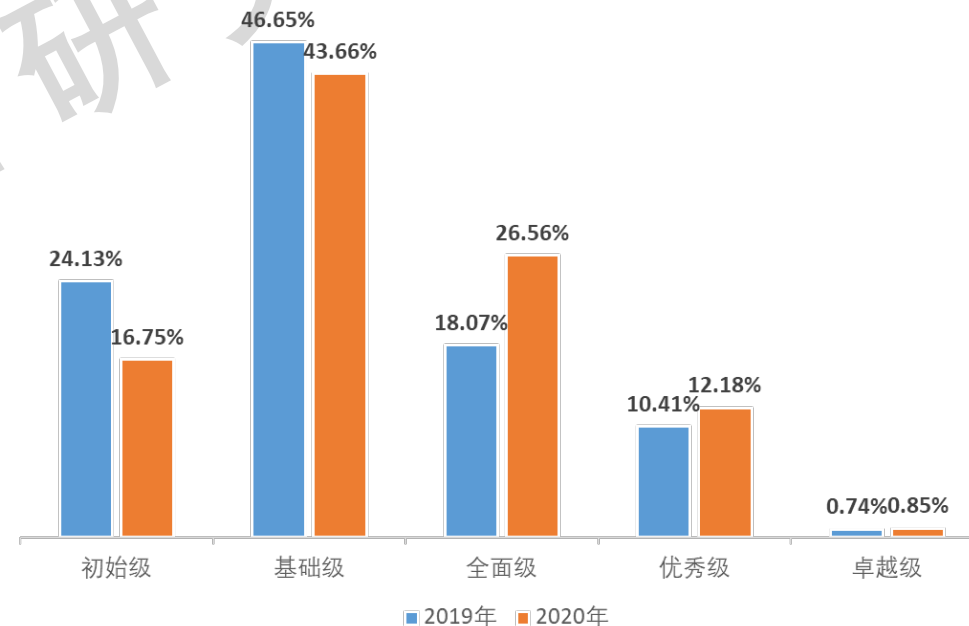
THREAT ANALYSIS RISK MANAGEMENT WEAPONIZATION BIODATA
HYPERCONNECTED BILITIES
VULNERABILITIES ZERO TRUST SERVICES BUSINESS MALWARE DIGITAL
TECHNOLOGY CONTIN
DEVICES HYPERC
DEVSECOPS REALITY
DEFENSE HUNTING HUMAN ACCESS
DEFENSE HUNTING HUMAN ACCESS
HACKERS TA
SUPPLY CHAIN APPLICATIONS GDPR LEARNING IoT TRUST
INFORMATION WORLD APPLICATIONS
ENDPOINT SECURITY DEFENSE ENDPOINT SE
SOFTWARE AI IoT NETWORK HUNTING
CRITICAL INTERNET CLOUD
COMPLIANCE RESPONSE FRAUD
SOFTWARE BEHAVIORAL ANALYTICS
DATA LOSS PREVENTION DEFENSE NETWORK

我们将软件端到端研发运营一体化能力划分为敏捷开发管理、持续交付、技术运营、应用设计、安全及风险管理与系统和工具六个部分，基于此对中国DevOps现状进行调查

中国企业DevOps成熟度逐步向全面级发展。



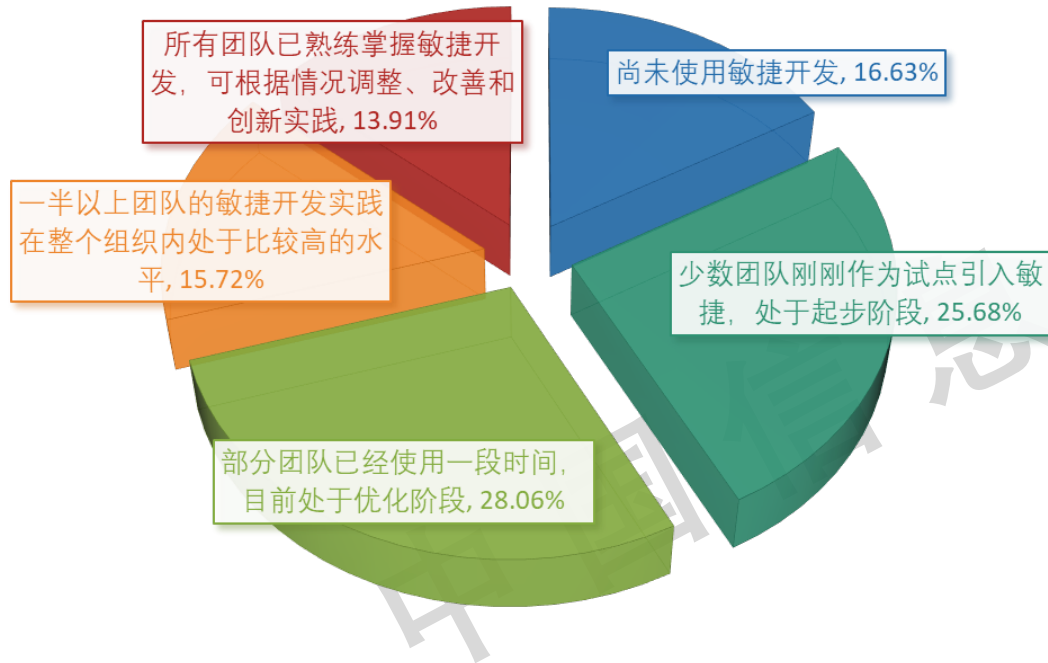
DevOps级别划分



数据来源：中国信息通信研究院

企业DevOps成熟度分布

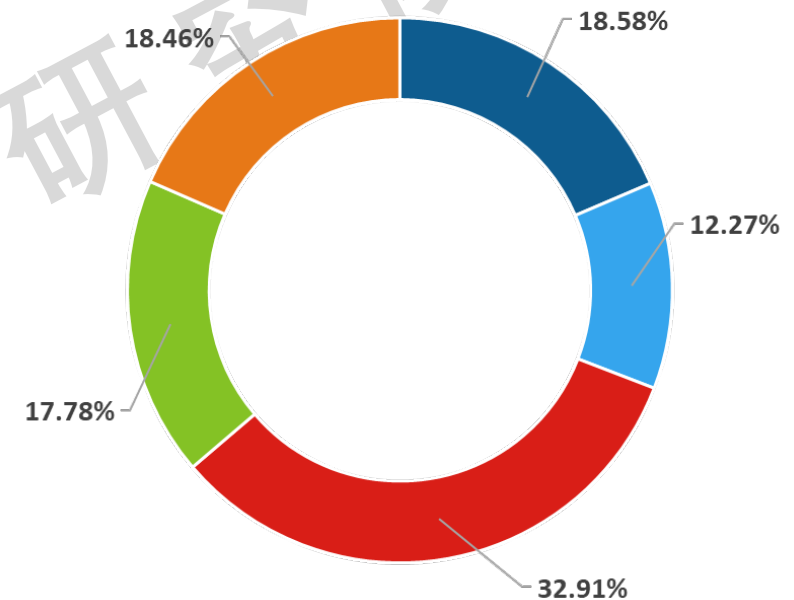
多数团队已实践敏捷开发，并不断优化。



数据来源：中国信息通信研究院

敏捷实践现状分布

近七成企业在项目初期收集高层次需求，在项目过程中逐渐细化、调整需求，以便灵活响应需求变化。



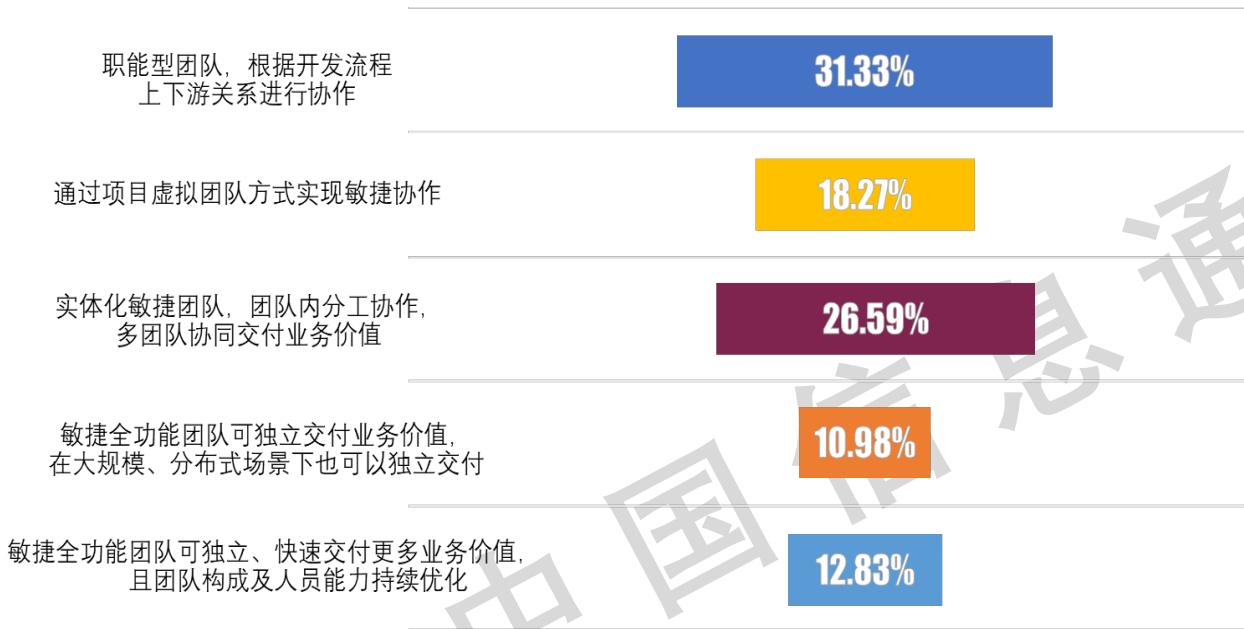
- 项目启动前收集并确认所有需求
- 项目启动前只收集高层次需求用于设计和规划
- 项目初期收集高层次需求，后期在交流中逐步细化需求
- 项目过程中可以定期调整需求顺序和置换需求
- 项目全程随时可以调整需求顺序和置换需求，需求全过程可视化

数据来源：中国信息通信研究院

需求过程现状分布

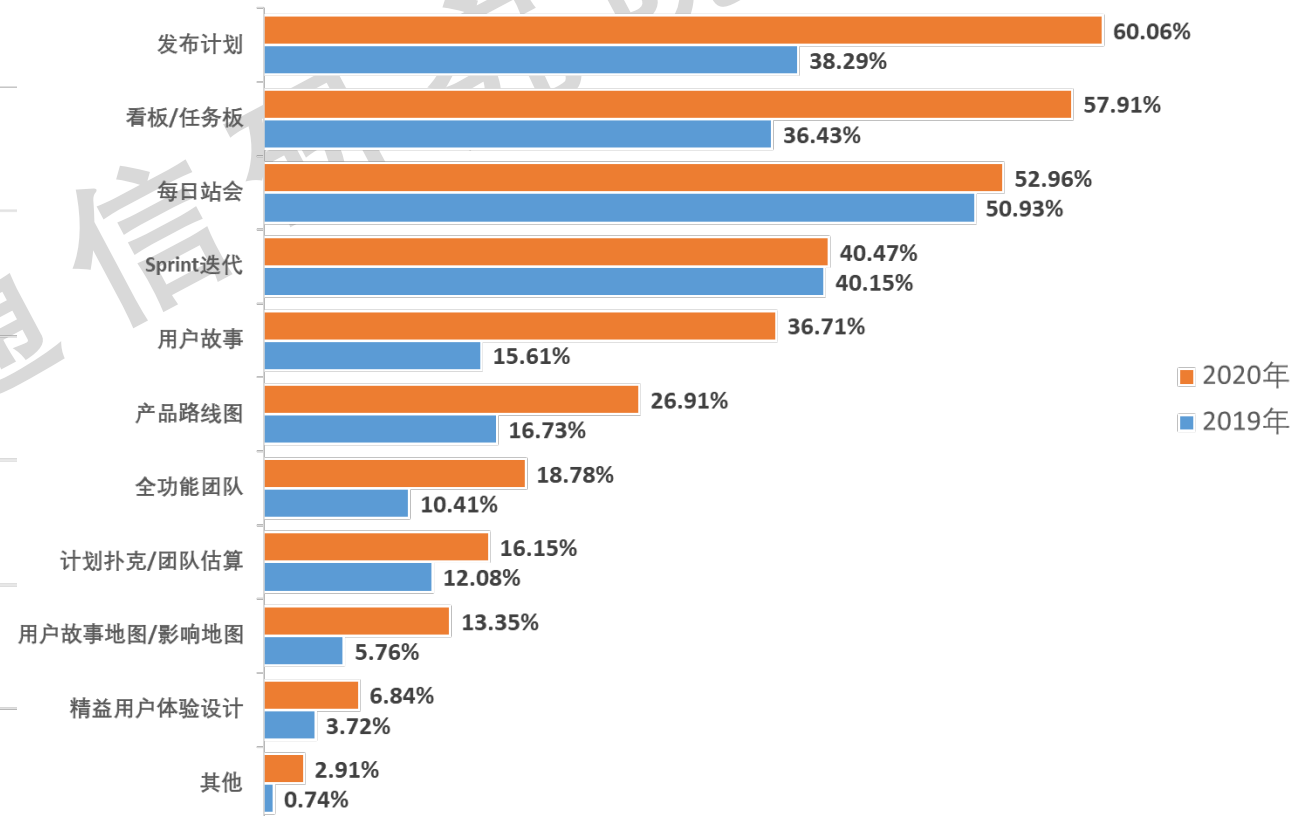
企业多采用实体化敏捷团队及分工协作的管理模式，并以独立交付更多的业务价值为发展方向。

敏捷管理实践的普及率较2019年显著提升。



数据来源：中国信息通信研究院

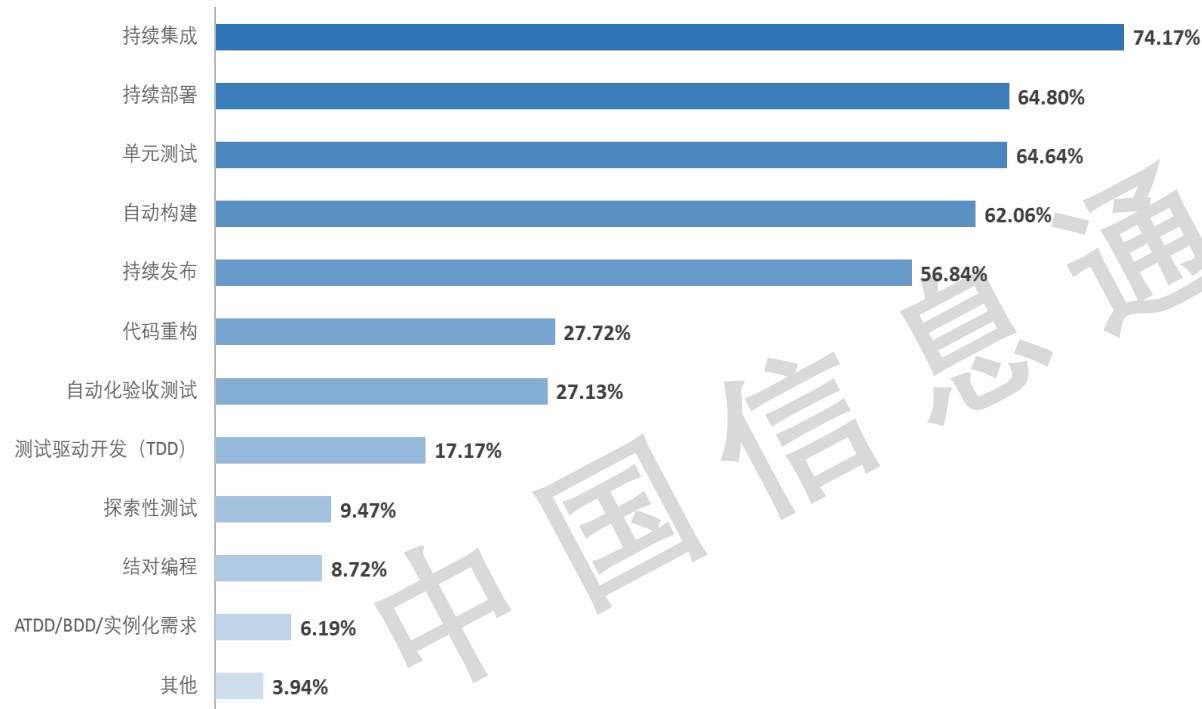
组织结构与协作模式的现状分布



数据来源：中国信息通信研究院

敏捷管理实践的选择分布

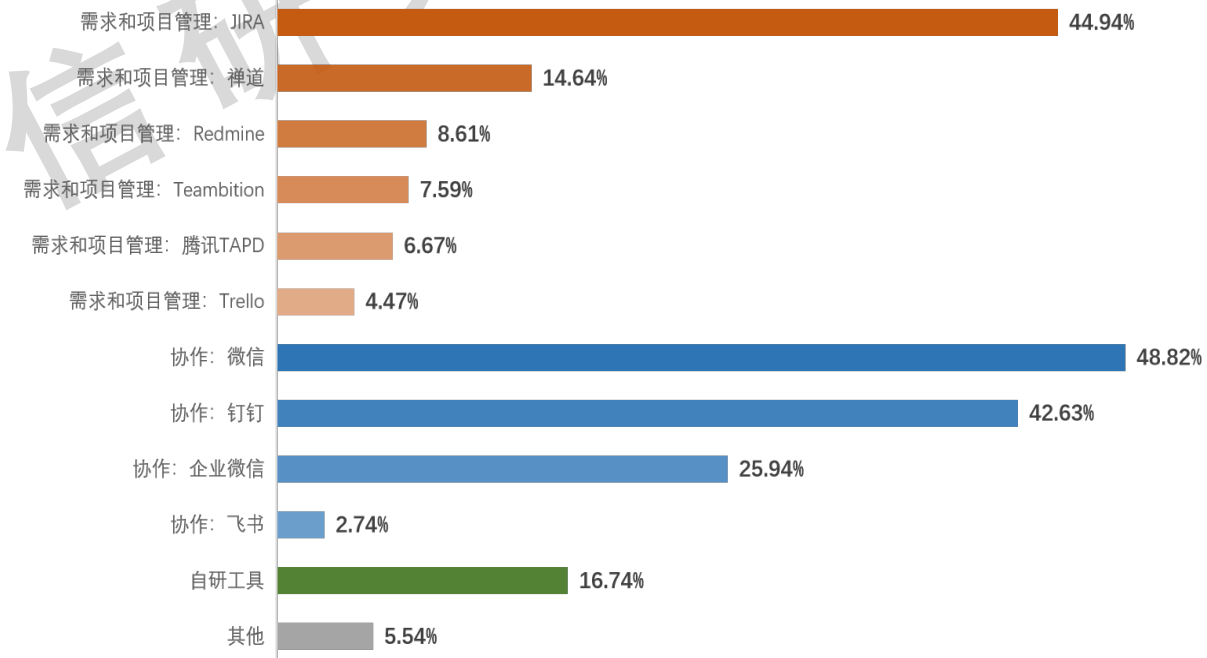
持续集成、持续部署、单元测试、自动构建和持续发布是企业应用最为广泛的敏捷工程实践。



数据来源：中国信息通信研究院

企业对敏捷工程实践的选择

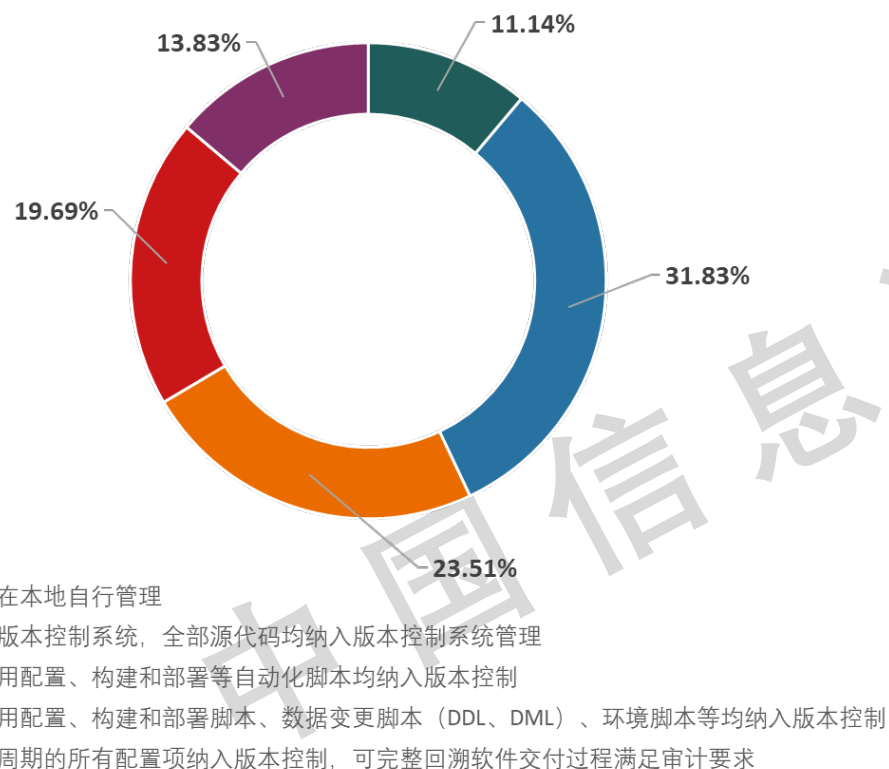
企业采用需求和项目管理工具以及协作工具共同提升研发效率与质量。



数据来源：中国信息通信研究院

企业对敏捷研发管理工具的选择

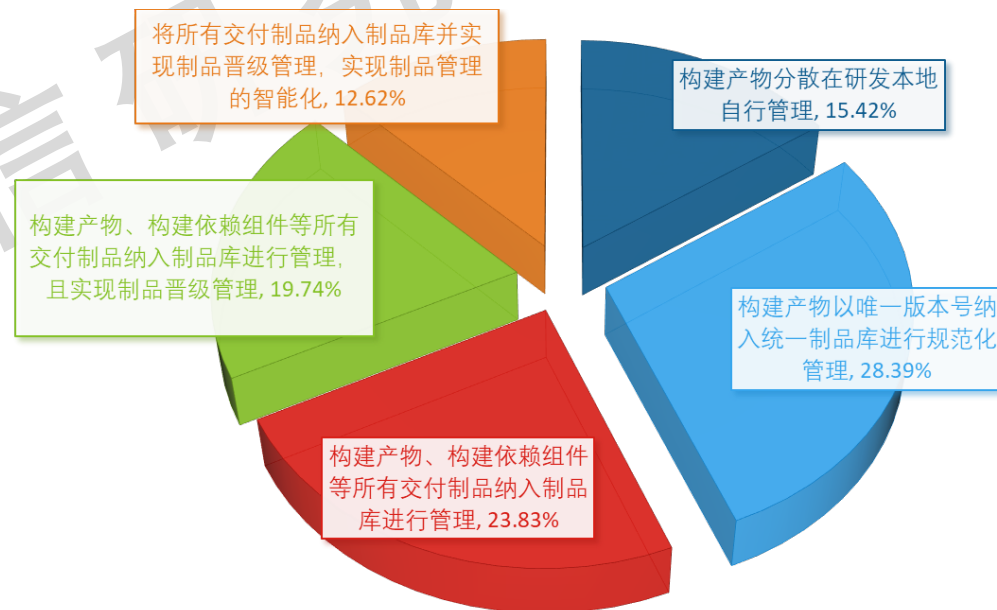
企业普遍将全部源代码纳入版本控制系统管理。



数据来源：中国信息通信研究院

版本控制现状分布

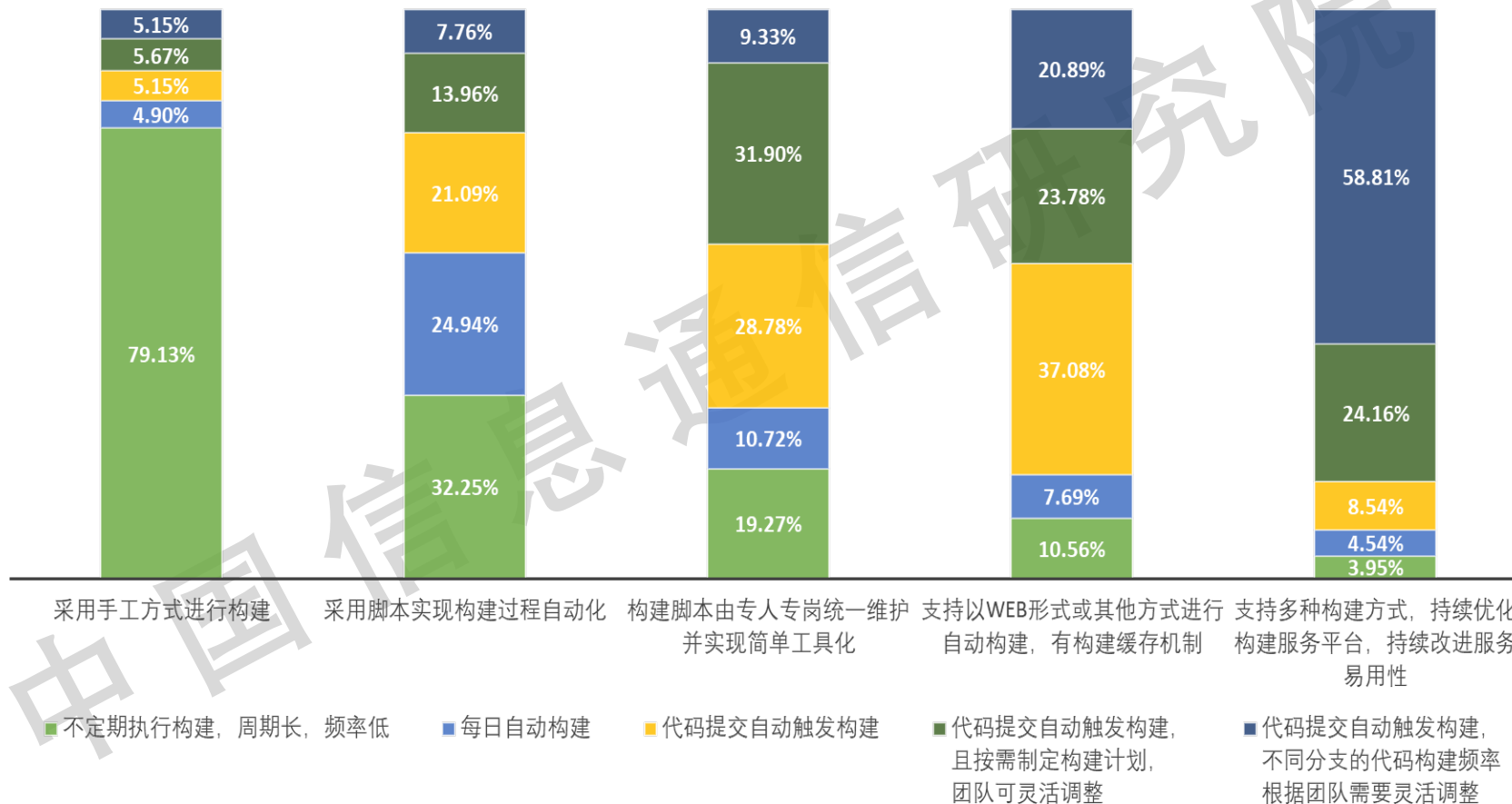
超八成企业将构建产物纳入制品库进行规范管理，但对构建依赖组件的管理、制品晋级管理等仍有待加强。



数据来源：中国信息通信研究院

制品管理现状分布

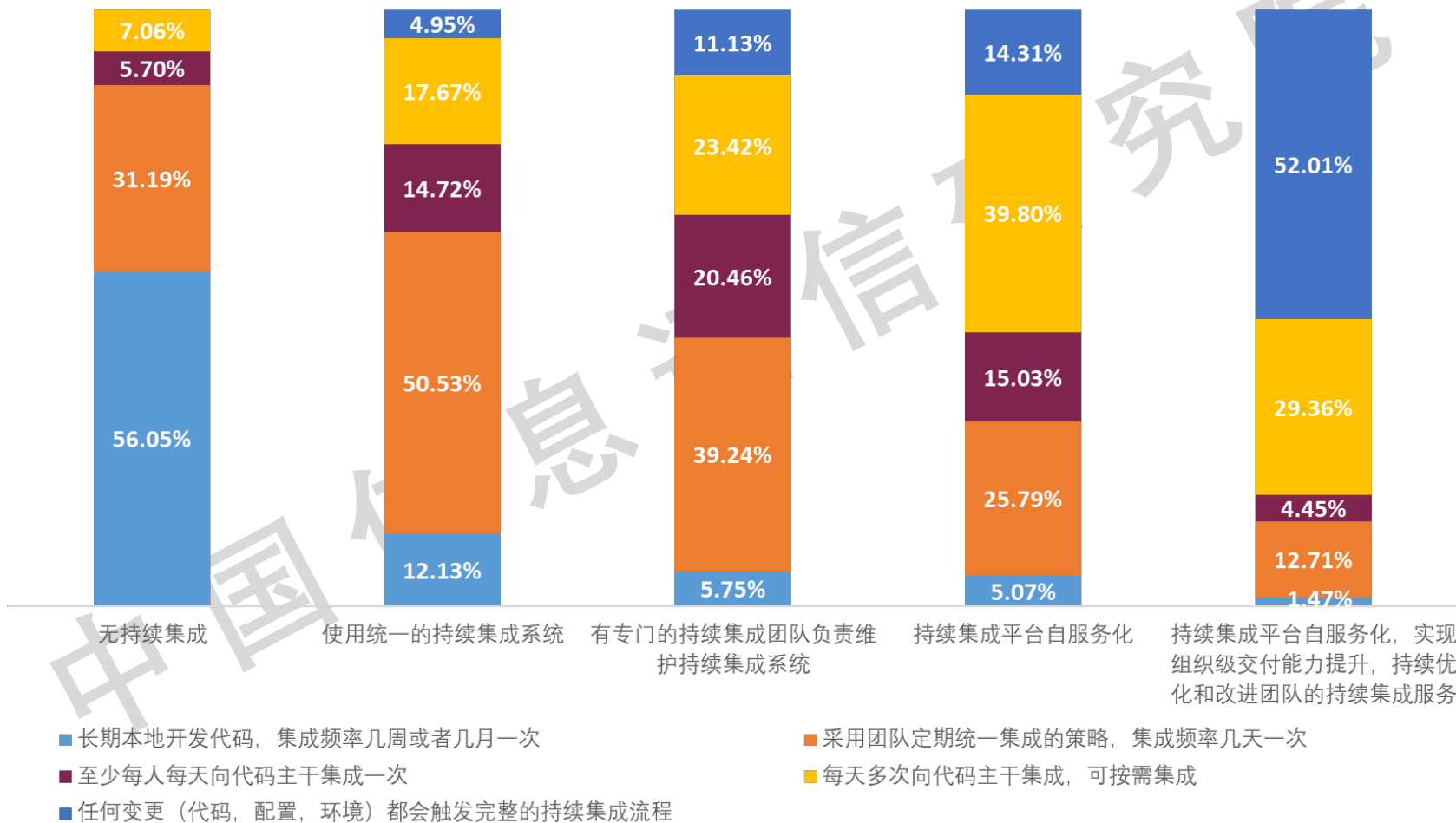
构建频率与构建方式自动化程度总体呈正比，构建频率较高的企业普遍实现了代码提交即构建。



数据来源：中国信息通信研究院

构建频率与构建方式分布对比

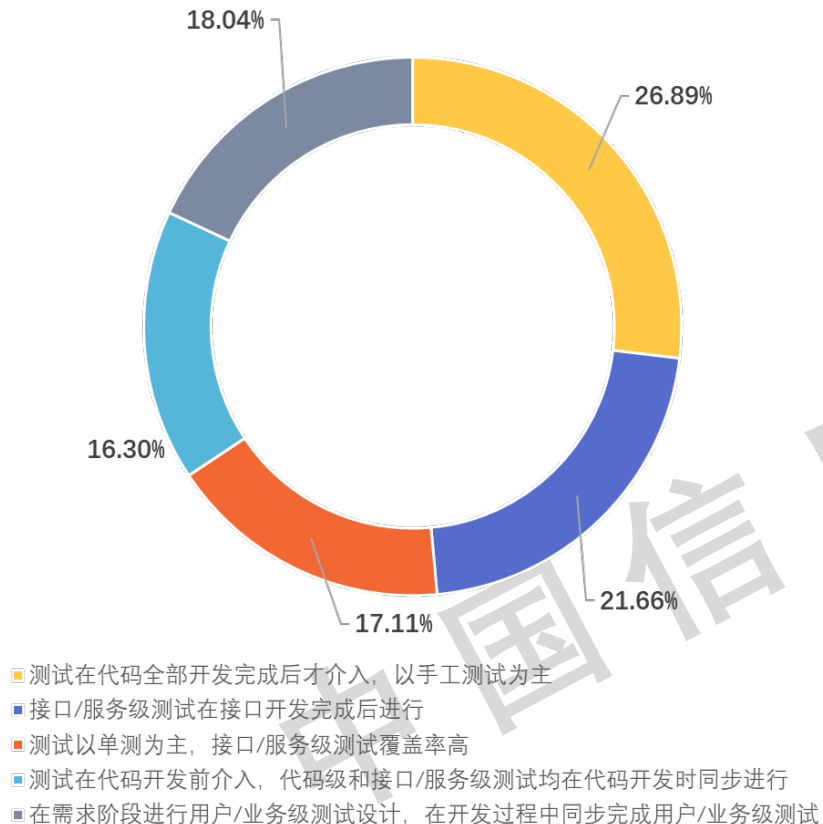
实现集成平台自服务化的企业大多支持持续、按需集成，集成频率与平台成熟度总体呈正比。



数据来源：中国信息通信研究院

集成频率与集成方式分布对比

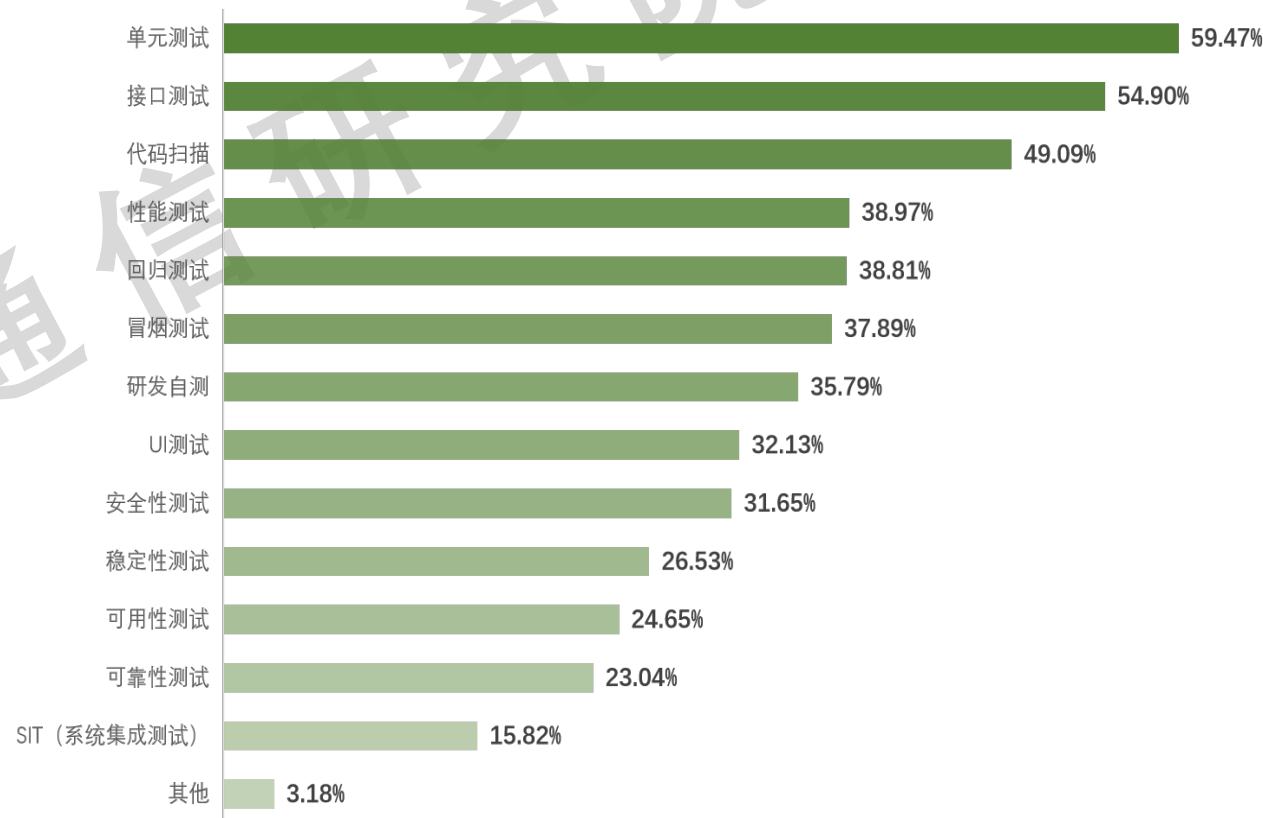
多数企业能够实现在接口开发完成后即介入相关测试，测试阶段逐步左移。



数据来源：中国信息通信研究院

测试过程现状分布

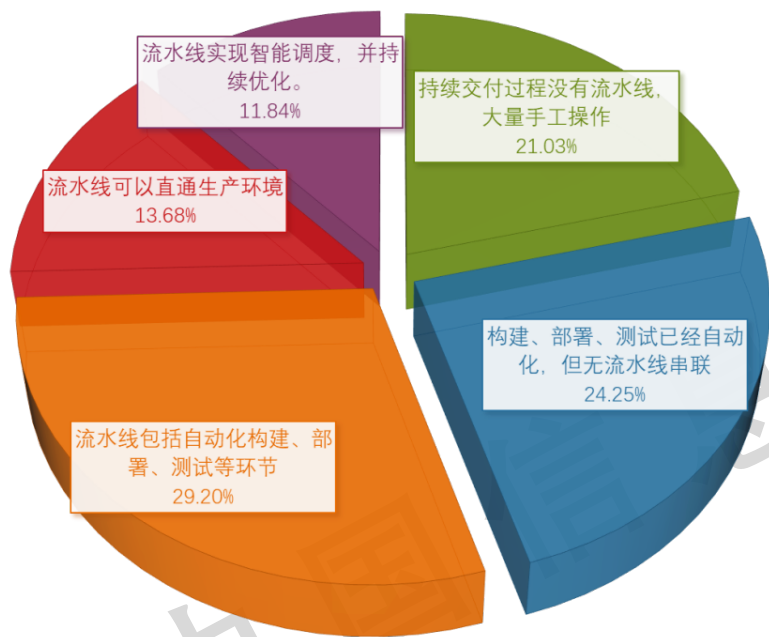
超半数企业实现单元测试与接口测试自动化，而集成测试、可靠性测试及可用性测试的自动化程度仍有较大提升空间。



数据来源：中国信息通信研究院

测试自动化比率分布

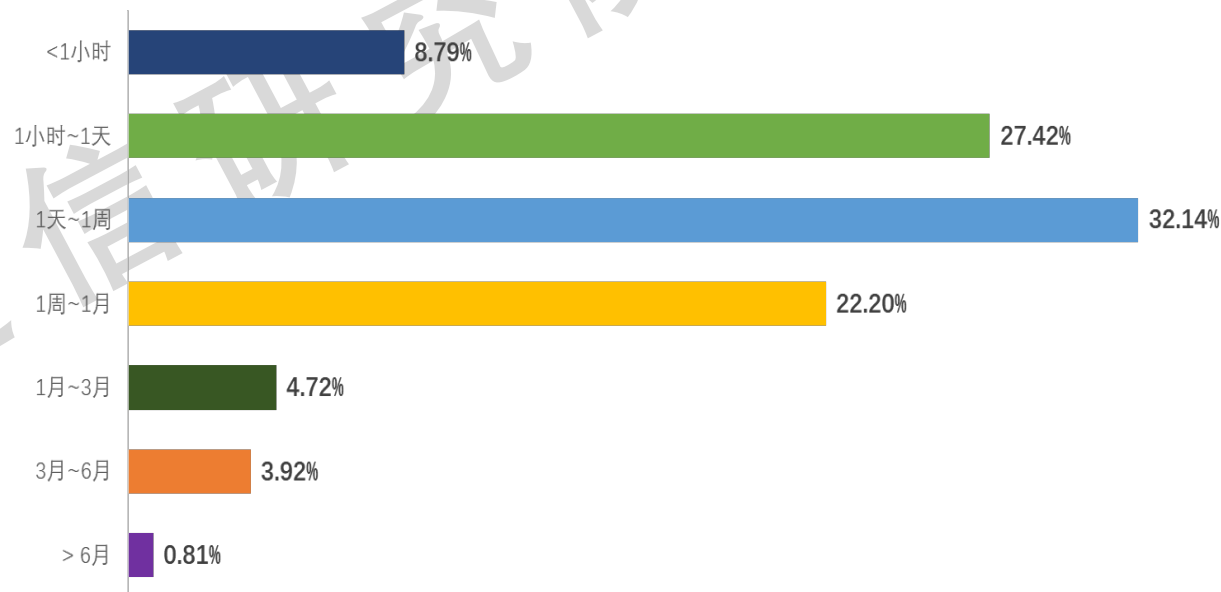
超半数企业采用持续交付流水线打通开发、测试和运维等多个环节。



持续交付流水线现状分布

数据来源: 中国信息通信研究院

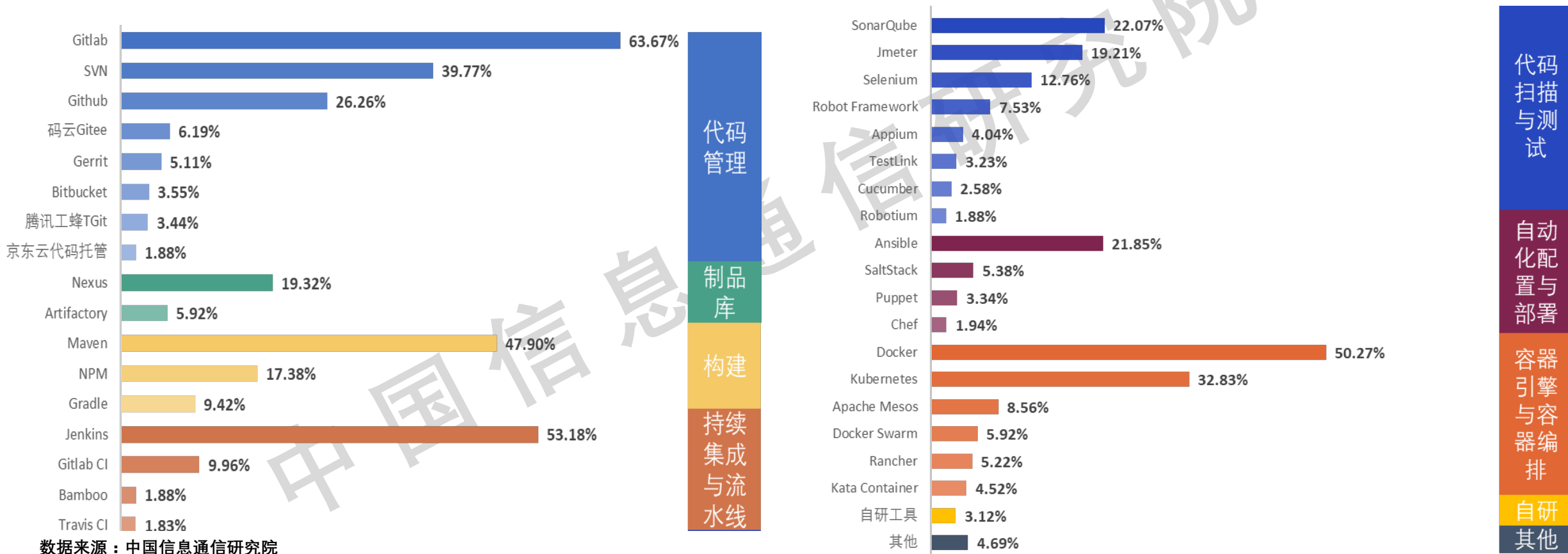
超九成的企业变更前置时间不超过1个月。



变更前置时间现状分布

数据来源: 中国信息通信研究院

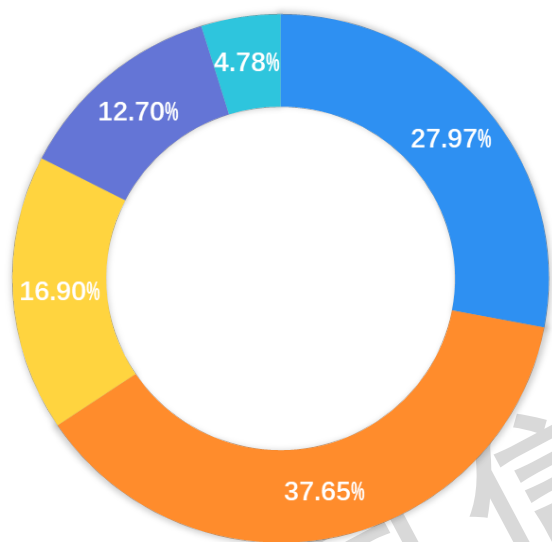
代码管理工具Gitlab、持续集成与流水线工具Jenkins和容器引擎 Docker是企业应用最普遍的三种持续交付工具。



数据来源：中国信息通信研究院

持续交付工具的使用

多数企业的监控管理范围已覆盖至系统、应用与接口日志等，但距离智能化监控管理还存在一定差距。

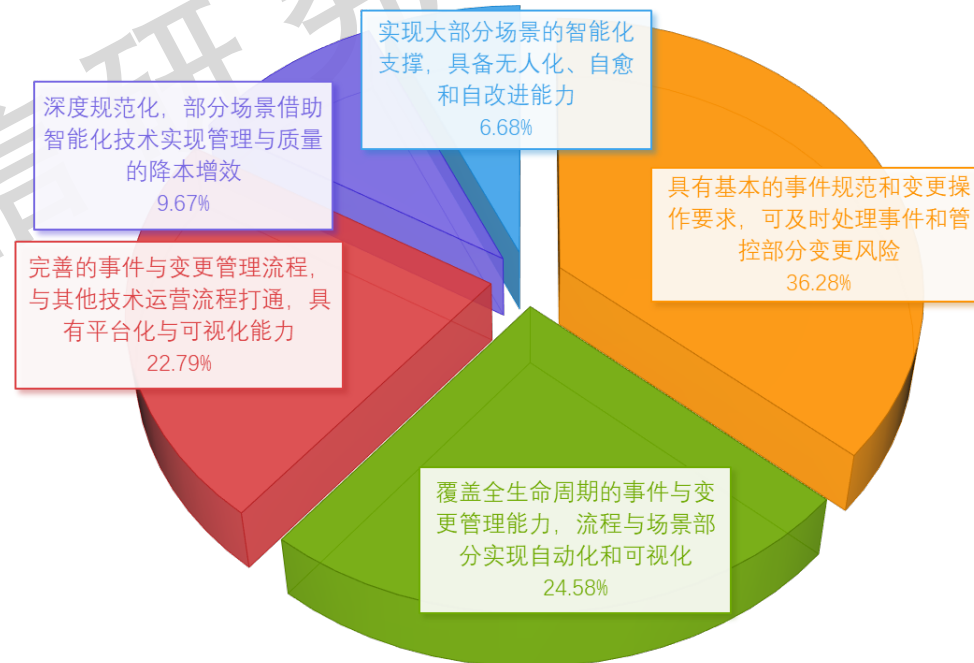


- 有基础的监控，能满足对系统级（CPU等）的监控需求
- 覆盖系统、应用与接口日志监控，具有告警度量、告警收敛与监控数据关联分析能力
- 具有面向应用场景的告警与可视化平台，可实现常见故障自愈
- 监控管理实现阈值动态调整等初步智能化，全网数据秒级上报，可实现自动化决策
- 智能决策、推荐等高度智能化

数据来源：中国信息通信研究院

监控管理现状分布

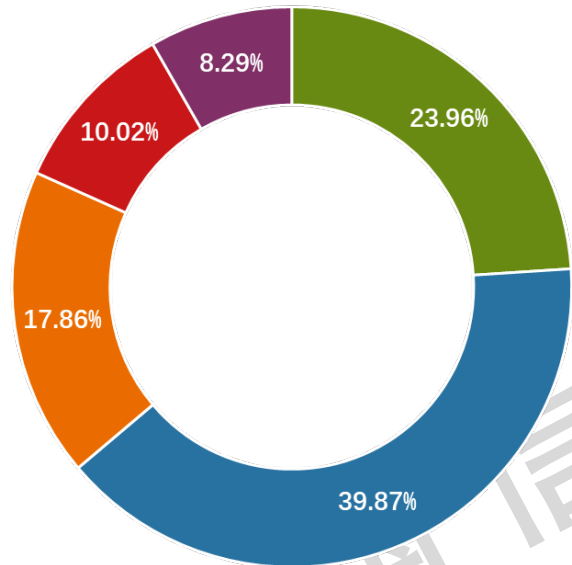
流程与场景的自动化、可视化能力不足是造成事件与变更管理能力较弱的主要原因。



数据来源：中国信息通信研究院

事件与变更管理现状分布

多数企业具有统一的配置管理系统，但自动化能力有待提升，缺乏智能识别配置对象关联关系的能力。

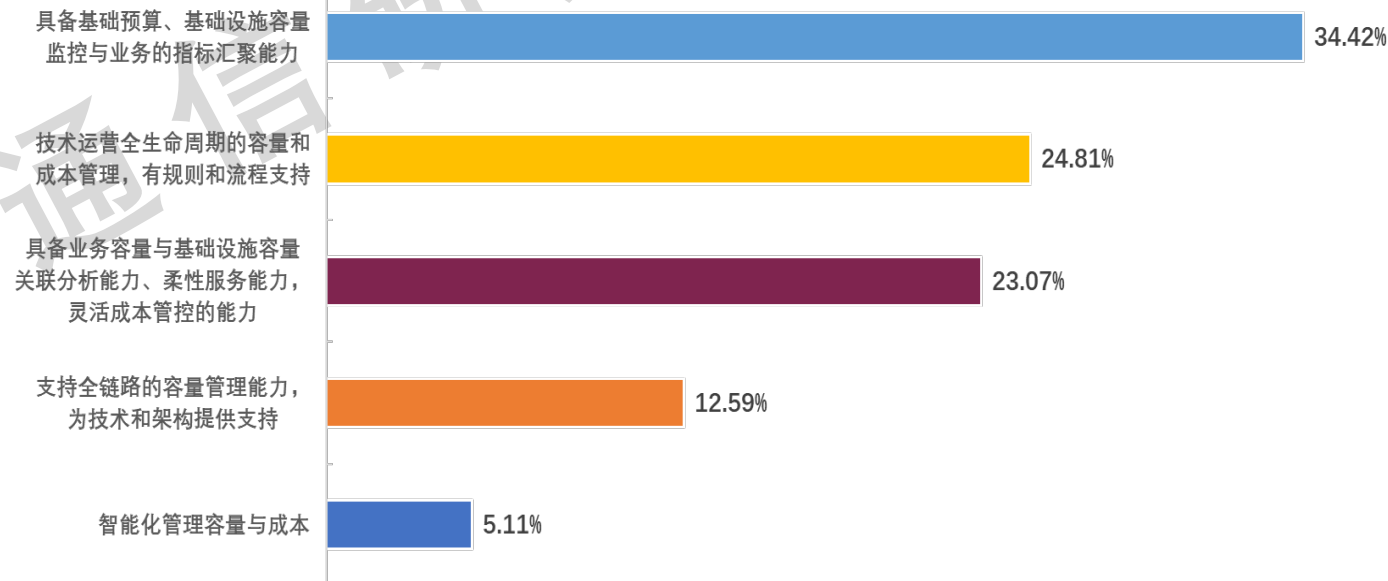


- 依靠人工保障配置记录的管理
- 统一的配置管理系统，全生命周期的管理技术运营相关的对象，有规则和流程支持配置变更
- 自动化配置管理平台，支持自动发现、灵活扩展和关联分析
- 智能识别配置对象的关联关系，配置信息能为技术运营活动提供决策支持
- 智能化配置管理，支持场景智能生成配置对象的关联规则和提供准确的决策依据

数据来源：中国信息通信研究院

配置管理现状分布

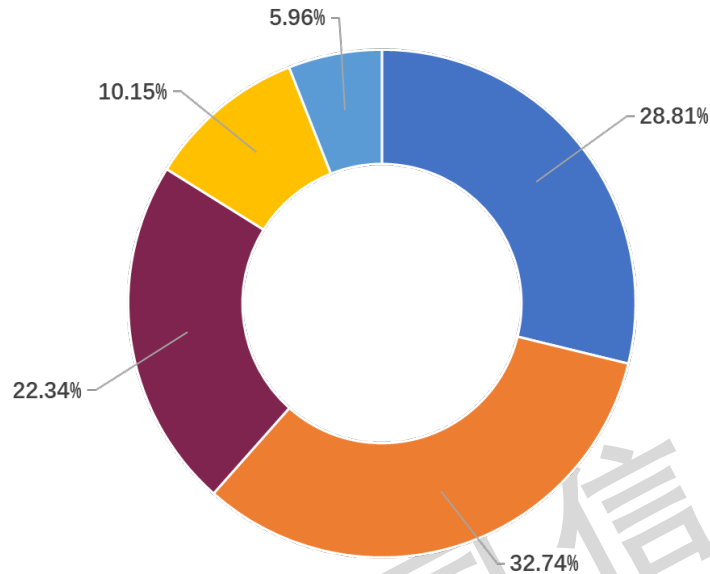
超六成企业支持全生命周期的容量和成本管理，但管控能力缺乏灵活性。



数据来源：中国信息通信研究院

容量与成本管理现状分布

应用服务间调用关系治理平台帮助企业快速有效定位故障，自动扩缩容能力亟待加强。

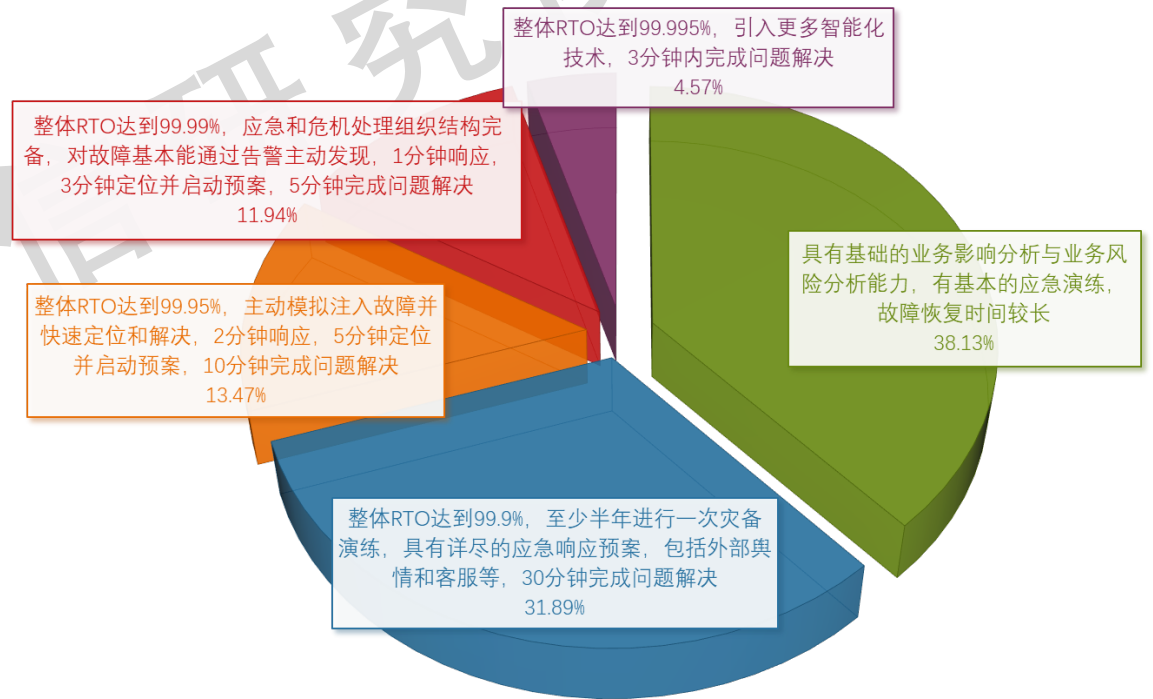


- 支持流量切换，硬件故障能及时回复，数据库备份可靠
- 具有应用服务间调用关系治理平台、IT系统有效打通，故障定位快、数据库读写分离，主备实施同步，同城多机房备份
- 自动化动态扩容，采用分布式缓存、分表分库、跨库事务等技术，同城多机房实时数据备份，异地数据备份
- 结合监控自动扩容缩容，系统拓扑结构自动梳理
- 实现全面自动化和智能化的高可用管理，并持续改进

数据来源：中国信息通信研究院

高可用管理现状分布

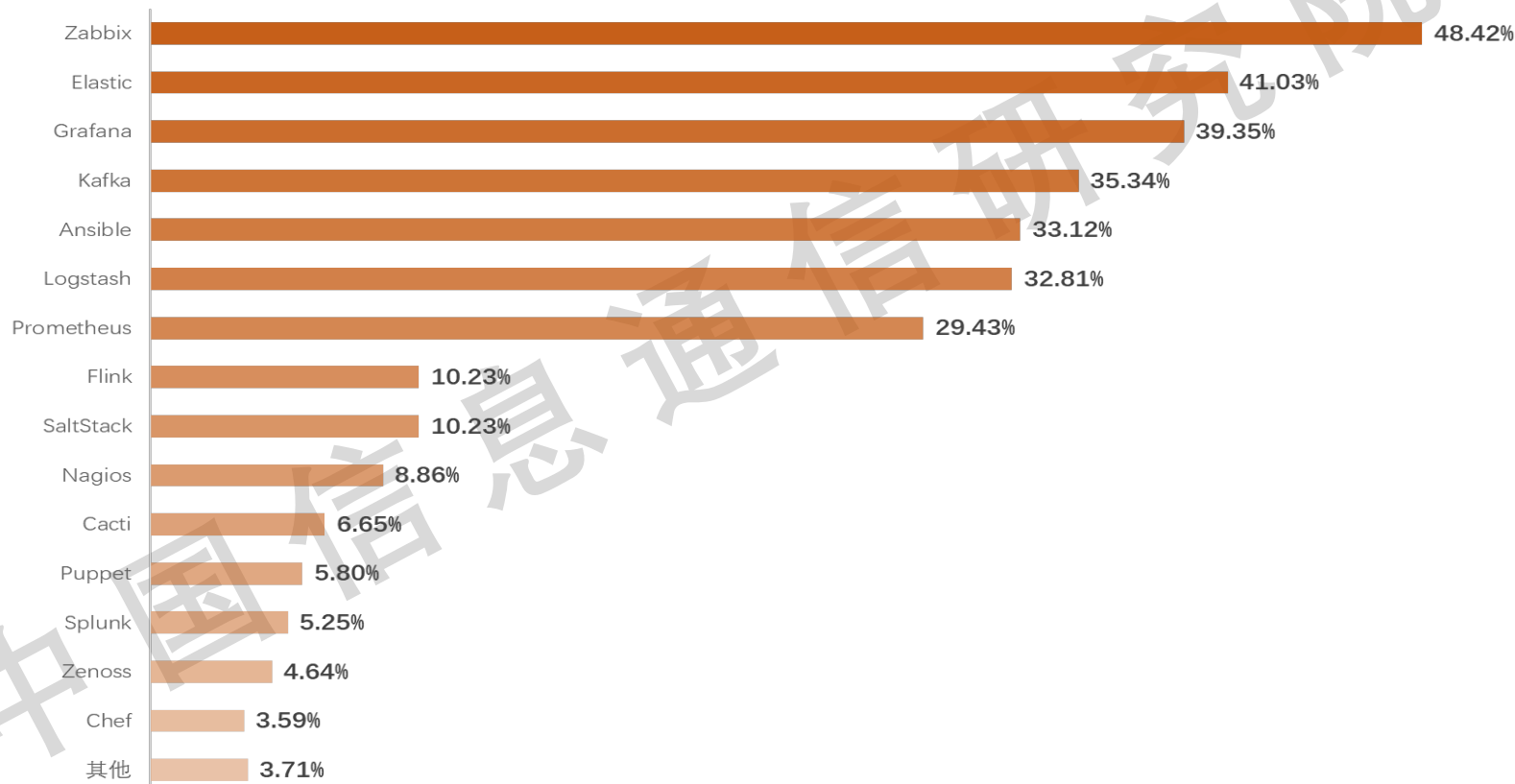
六成以上的企业整体RTO能达到99.9%以上，需健全应急和危机处理能力。



数据来源：中国信息通信研究院

业务连续性管理现状分布

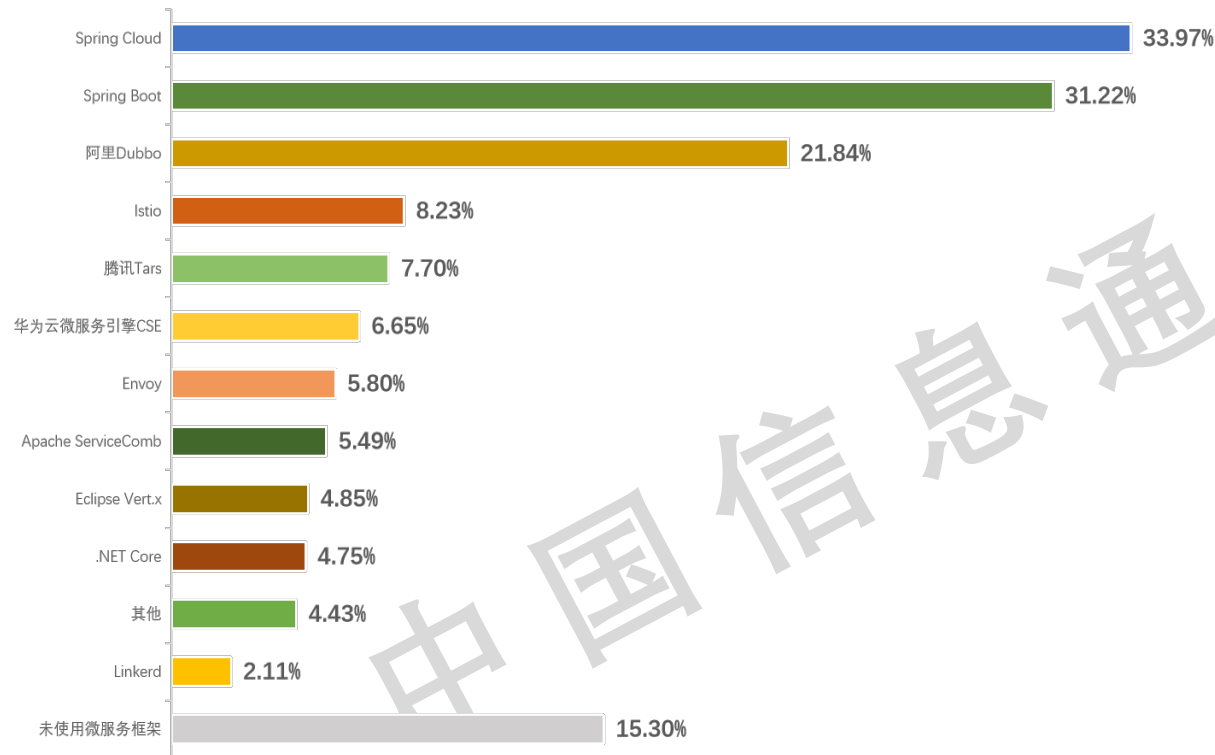
市场已具备较为成熟的自动化运维工具，帮助企业高效率、高质量地完成监控、分析、流处理等工作。



数据来源：中国信息通信研究院

自动化运维工具选择分布

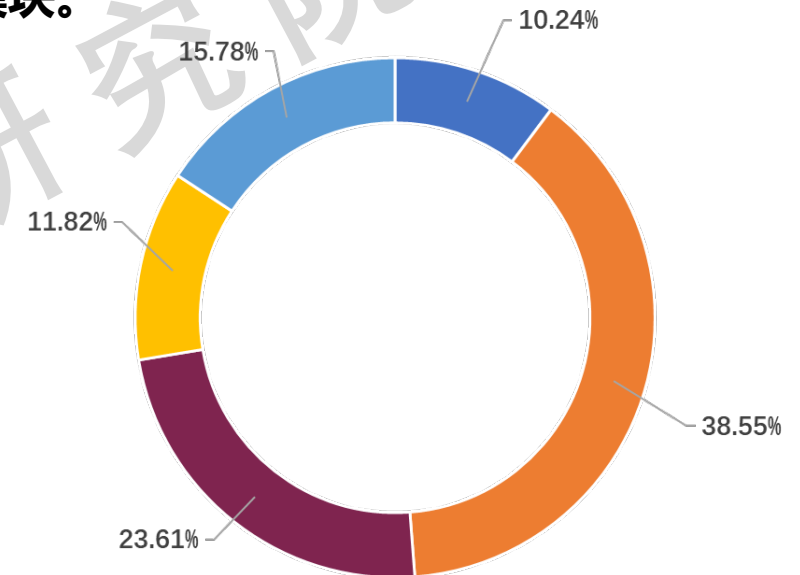
Spring Cloud与Spring Boot是企业当前主要选择的微服务相关技术。



数据来源：中国信息通信研究院

微服务相关技术选择分布

近半数企业的应用架构能做到由专业人士设计，但仍有少部分企业采用巨石架构，所有功能归于一个模块。

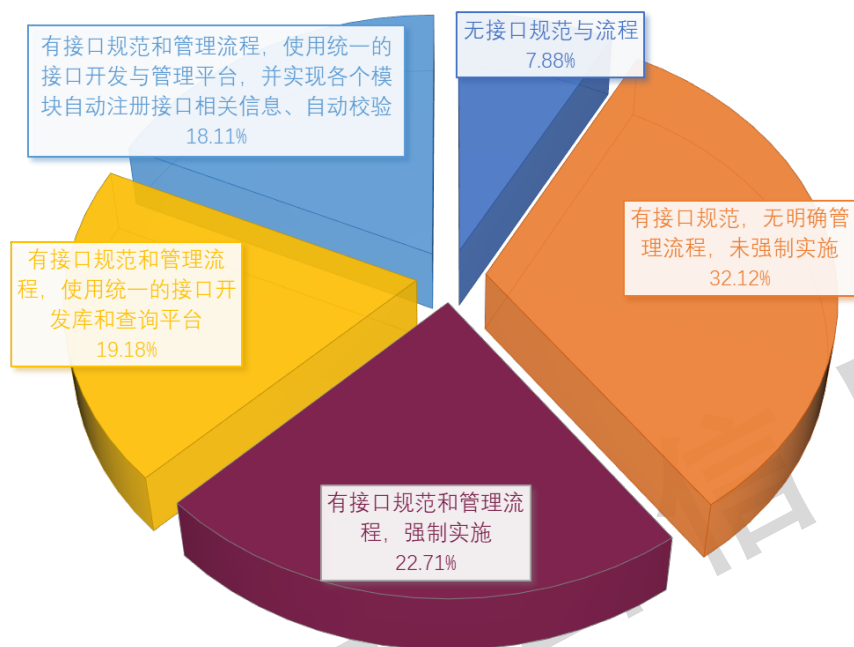


- 应用架构采用巨石架构，所有功能归于一个模块
- 应用架构按经验简单拆分成若干功能独立的模块，各模块可独立开发和部署
- 应用架构由专业人士进行设计和模块拆分
- 应用架构专人设计，对设计质量有明确的度量流程
- 应用架构专人设计，系统复杂度降到最低，对应用架构拆分情况形成持续反馈与改进

数据来源：中国信息通信研究院

应用架构设计现状分布

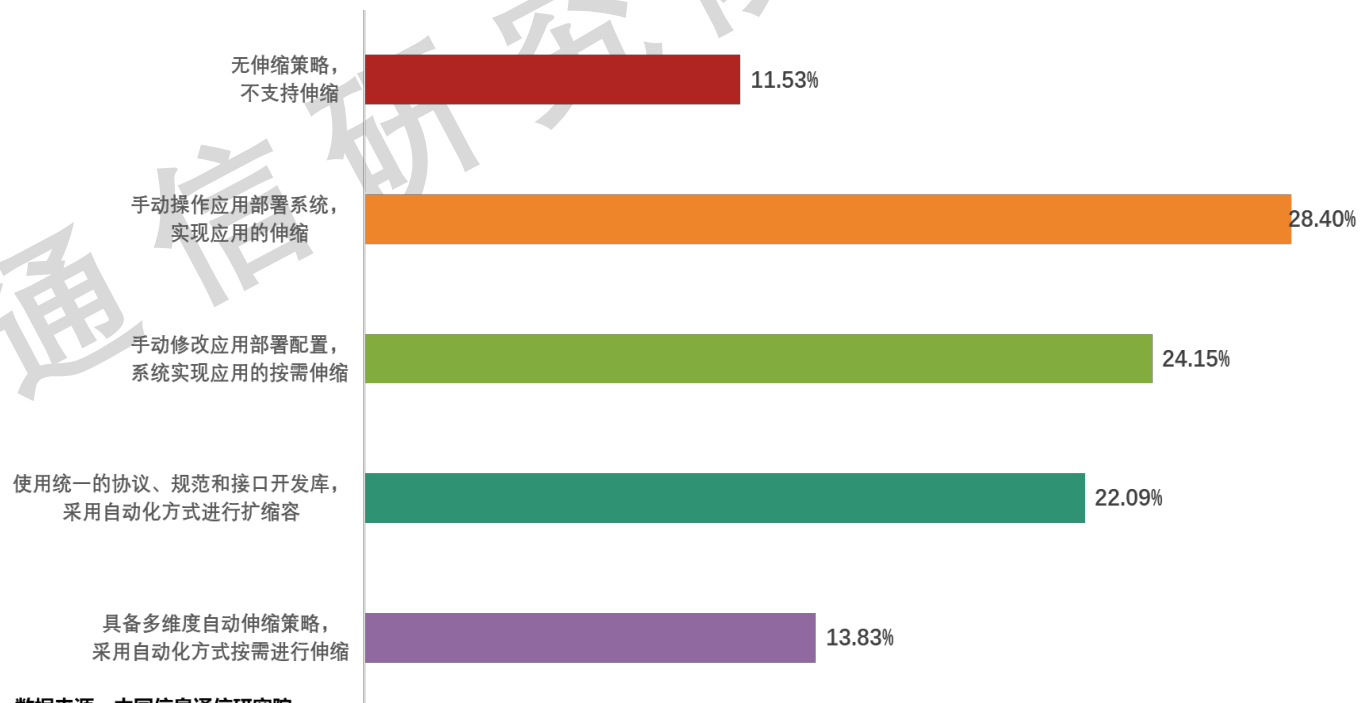
大部分受访企业已有应用接口管理规范，但缺少统一的接口开发与管理平台。



数据来源：中国信息通信研究院

应用接口管理规范现状分布

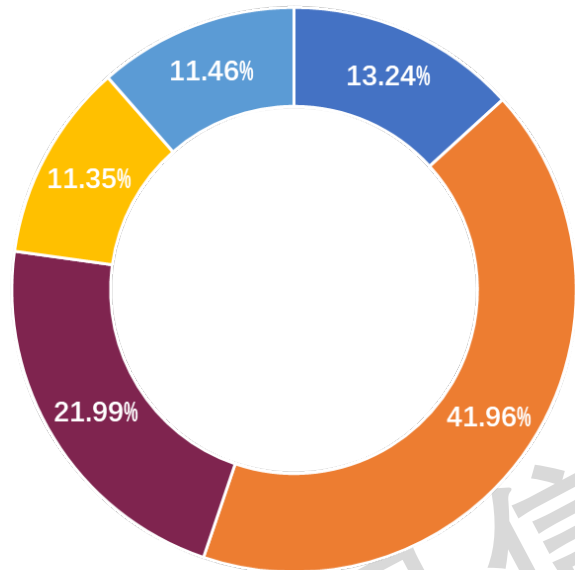
应用可伸缩性的自动化程度较低，仅一成企业具备多维度自动化的应用可伸缩性。



数据来源：中国信息通信研究院

应用可伸缩性现状分布

应用故障修复缺乏统一平台，自动化、智能化处理能力较弱。

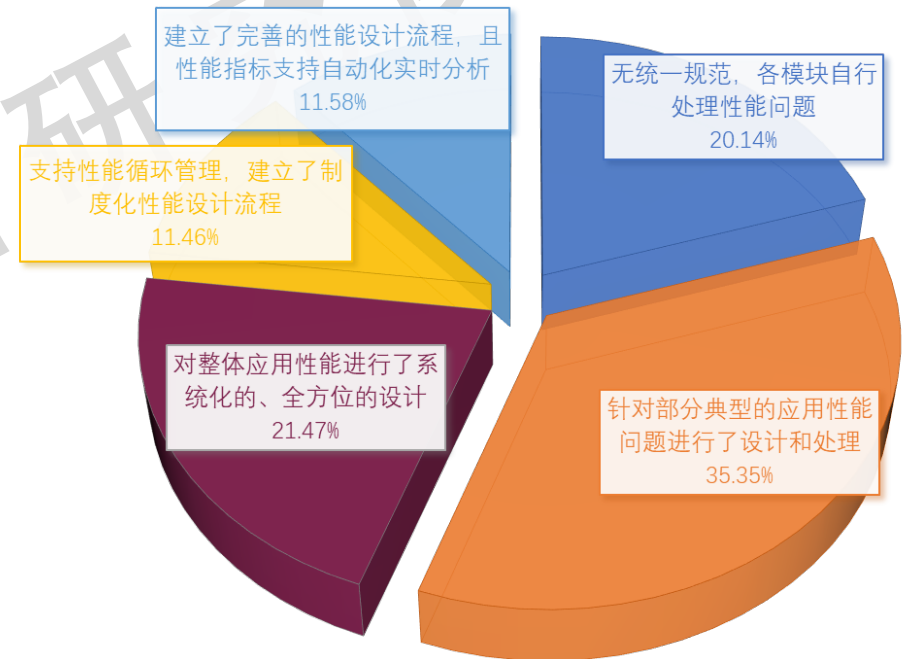


- 无统一日志规范，系统运行状态无法获取，无故障处理能力
- 统一日志规范，人工分析系统运行状态，应用独自提供故障处理能力
- 统一日志规范，统一故障修复平台，利用工具辅助分析故障
- 应用日志支持全链路追踪，单个应用系统可自动处理部分故障
- 应用日志支持图形化展示全链路追踪信息，实现自动预警、故障定位和故障自动修复

数据来源：中国信息通信研究院

应用故障处理现状分布

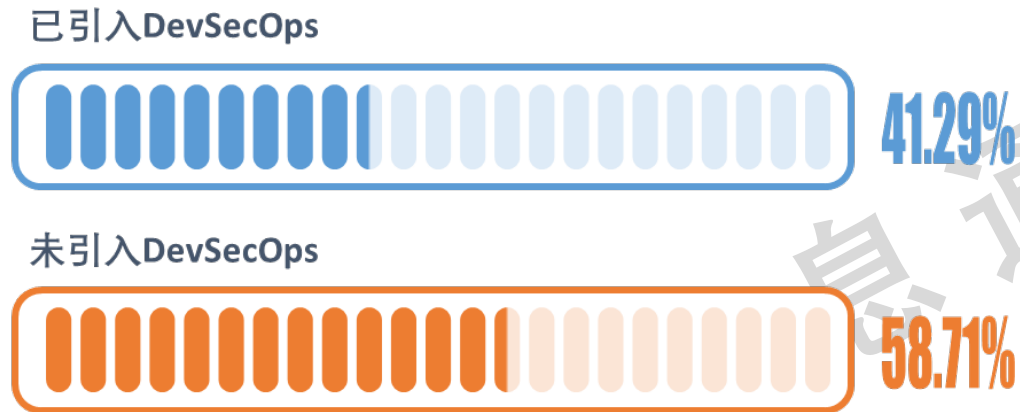
半数以上企业缺乏系统化、全方位的应用性能管理。



数据来源：中国信息通信研究院

应用性能管理现状分布

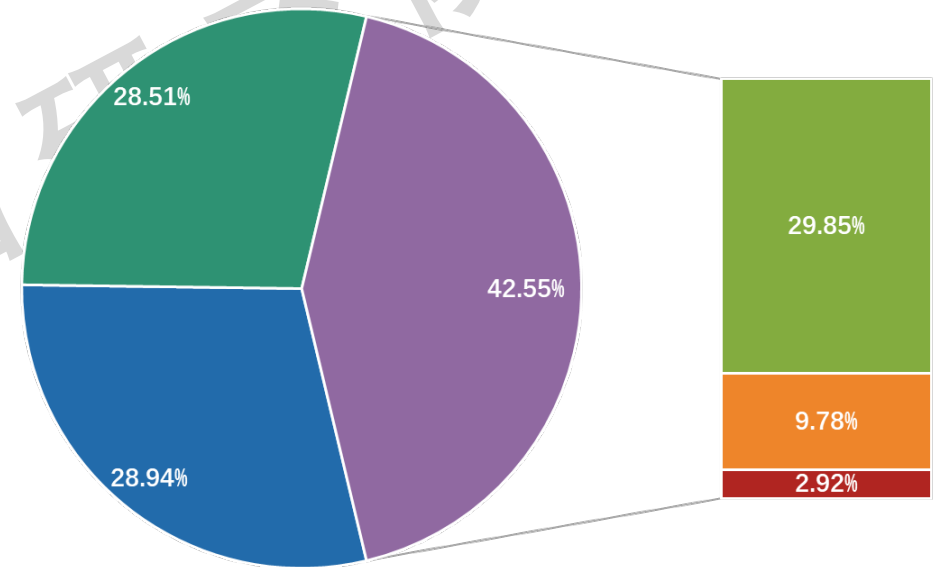
超四成的企业引入了DevSecOps。



数据来源：中国信息通信研究院

DevSecOps引入现状

四成以上企业有专业的安全团队，较去年增长显著，安全投入得到企业重视并迅猛发展。



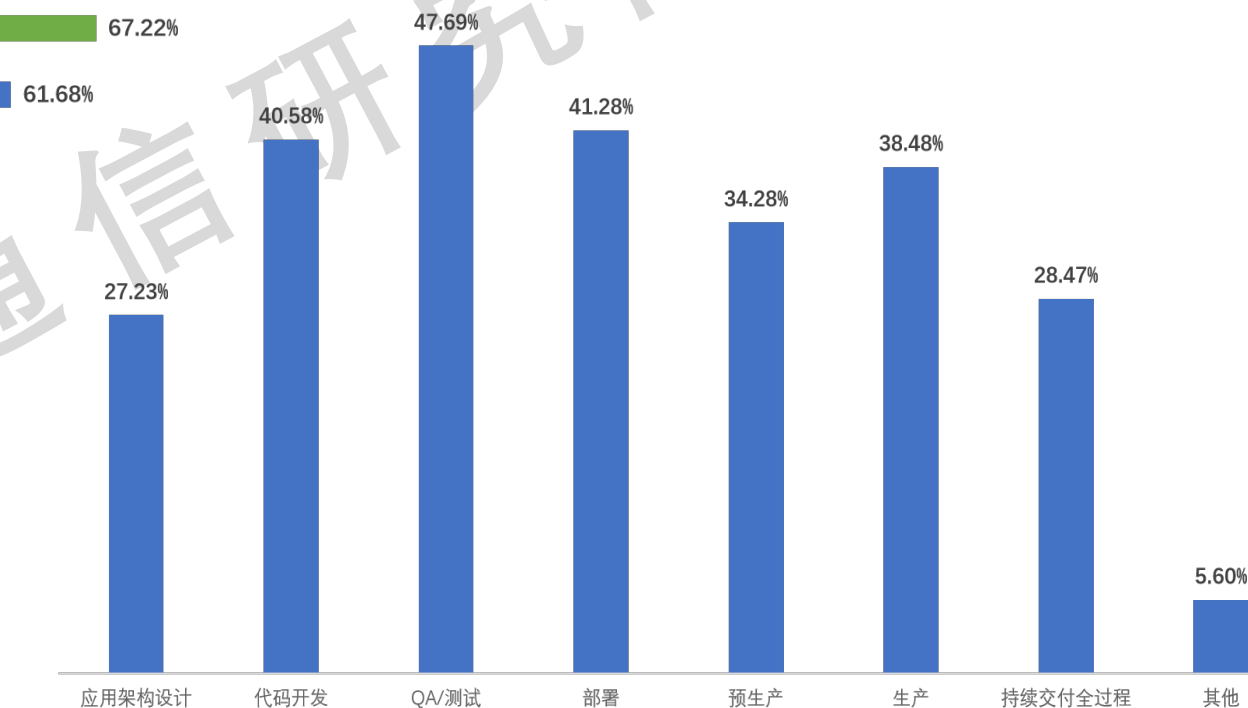
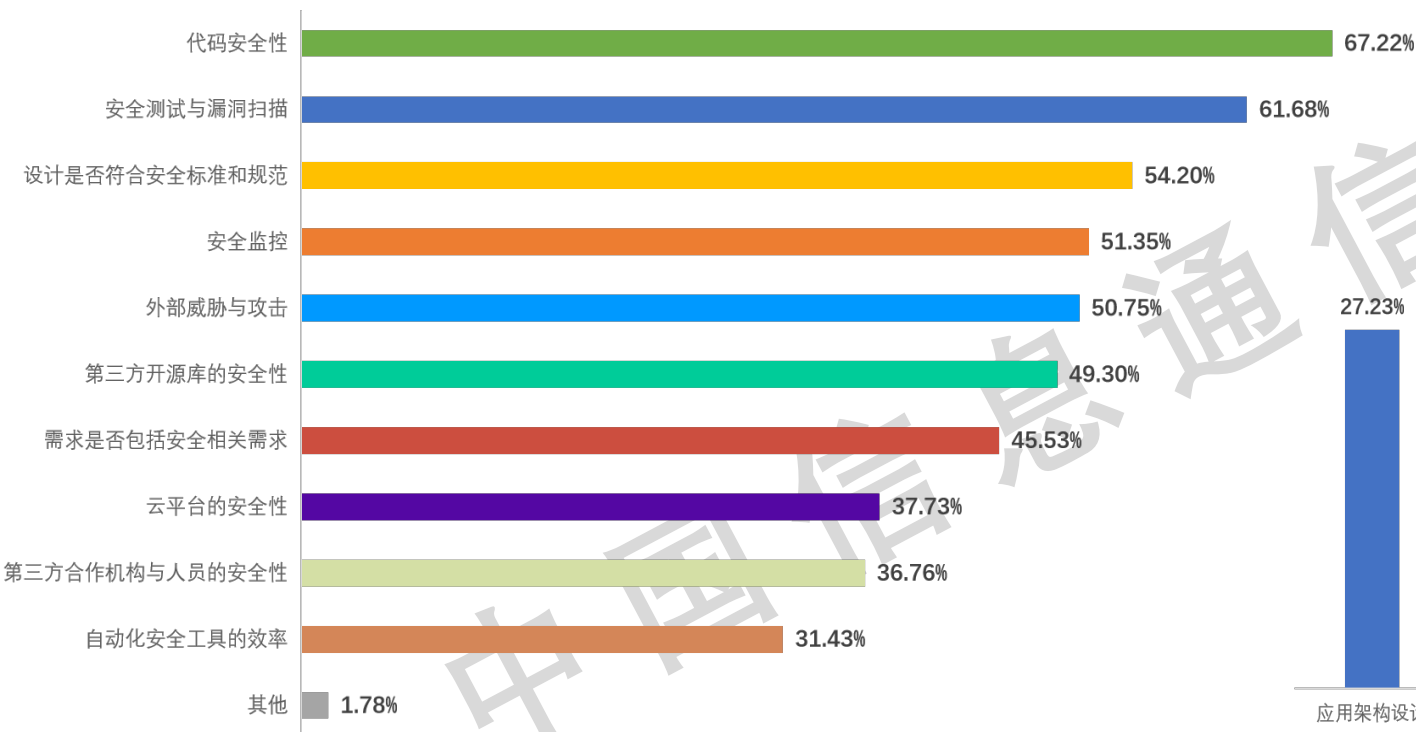
- 否，没有专业的安全团队
- 否，没有专业的安全团队，但有安全管理岗位与人员
- 是，有专门的安全管理团队与安全主管
- 是，有高级别的安全管理组织与技能完善的安全专家团队
- 是，安全专家团队对行业具有突出贡献

数据来源：中国信息通信研究院

专业安全团队现状

代码安全性、安全测试与漏洞扫描等安全内容备受企业关注。

自动化安全测试逐步向全流程覆盖，能够帮助企业尽早发现和解决安全问题。



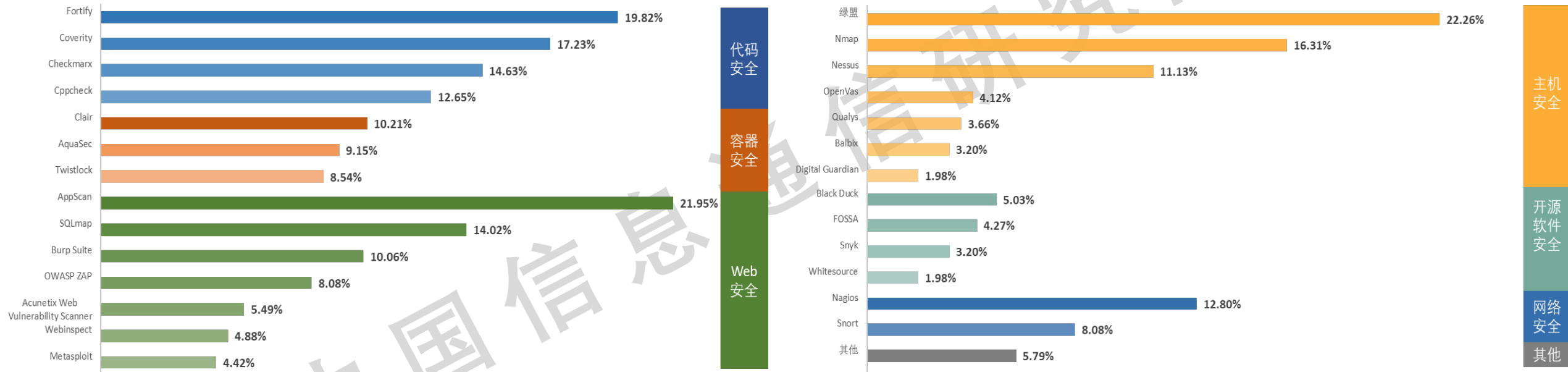
数据来源：中国信息通信研究院

数据来源：中国信息通信研究院

企业关注的安全内容现状

自动化安全测试阶段

安全工具应用情况呈多样性，其中容器及网络安全相关工具的普及率有待提升。

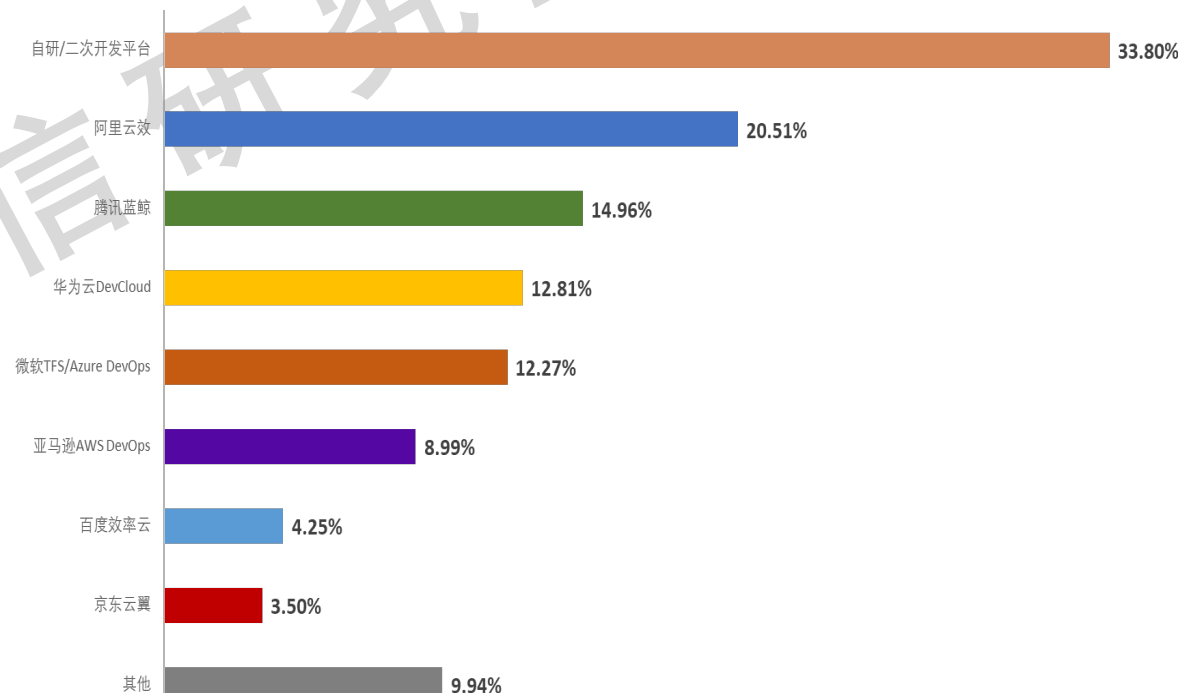
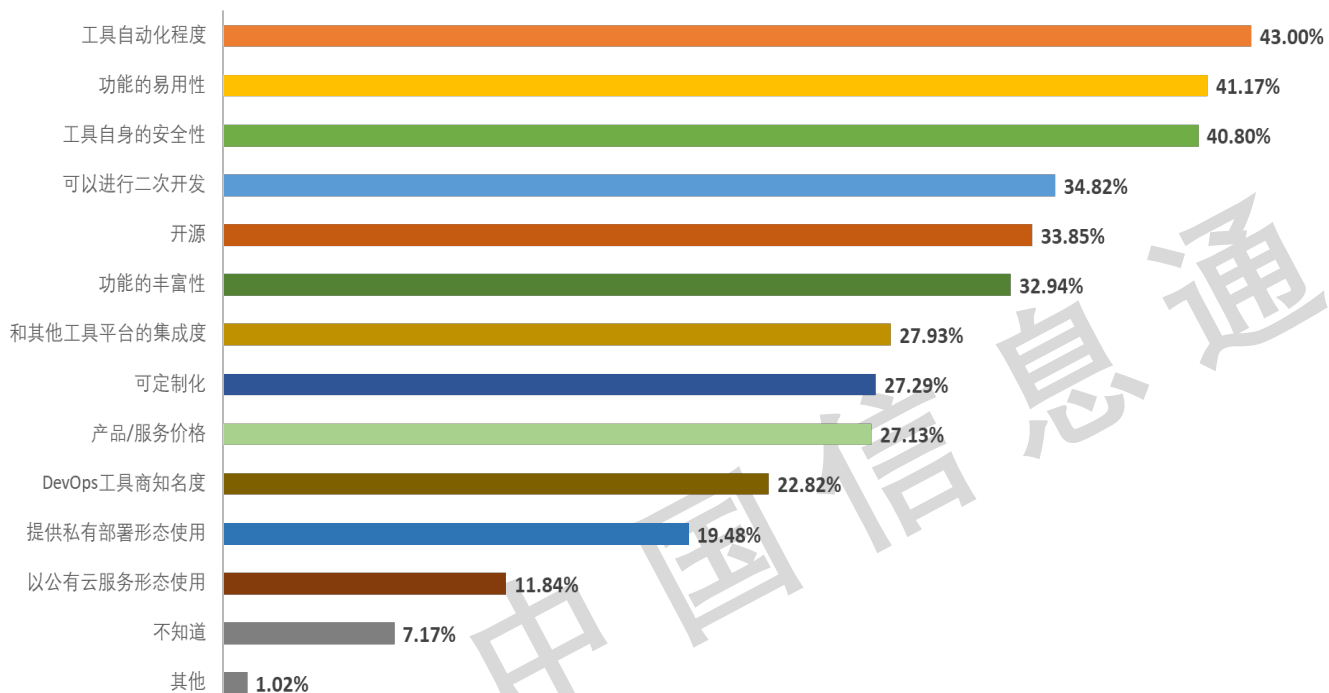


数据来源：中国信息通信研究院

安全工具使用现状

工具的自动化程度、易用性和安全性是企业选择DevOps工具的重要因素。

采用自研/对开源工具进行二次开发的DevOps平台类工具成为企业的首选。



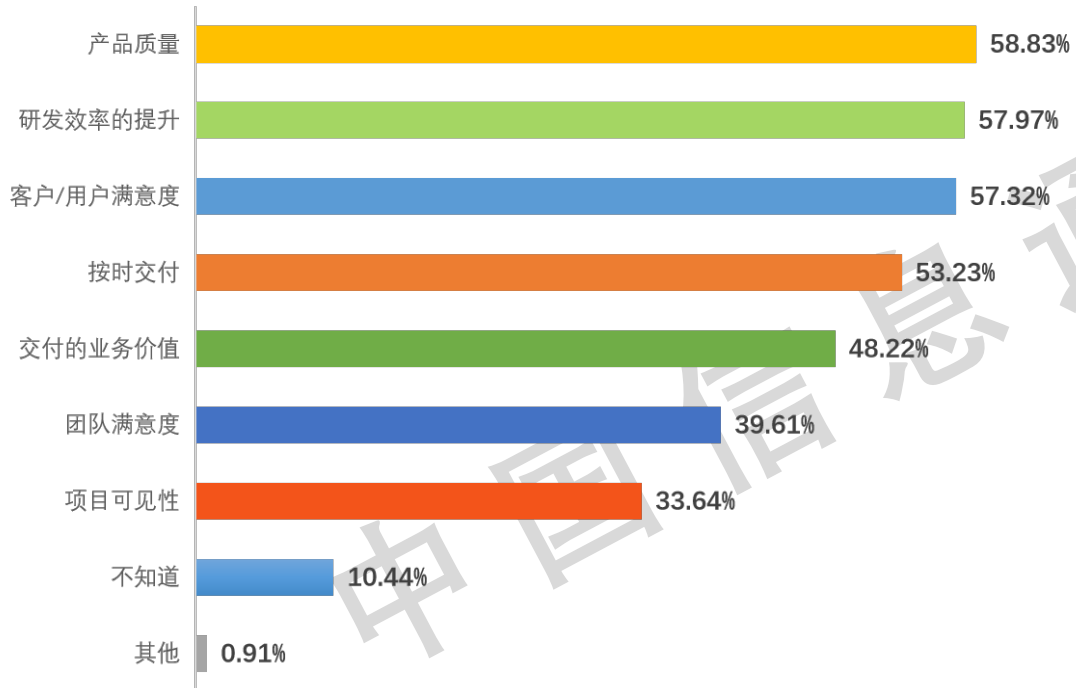
数据来源：中国信息通信研究院

数据来源：中国信息通信研究院

DevOps工具选择因素

DevOps平台类工具选择分布

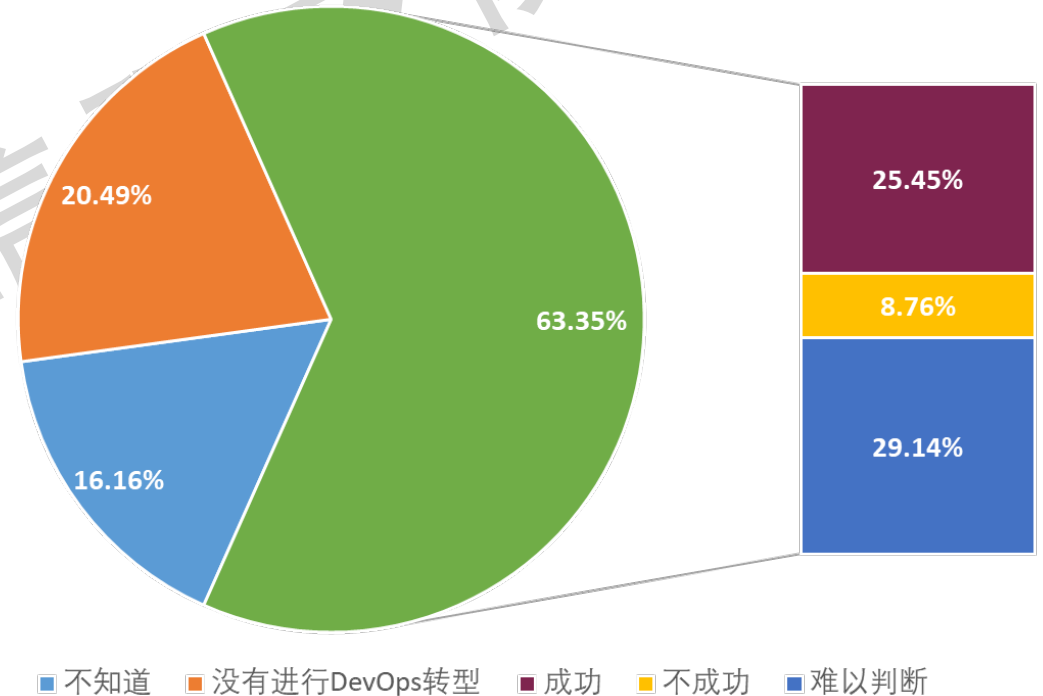
产品质量、研发效率的提升、客户满意度和按时交付是企业判断DevOps成功与否的主要标准。



数据来源：中国信息通信研究院

判断DevOps成功实践的标准

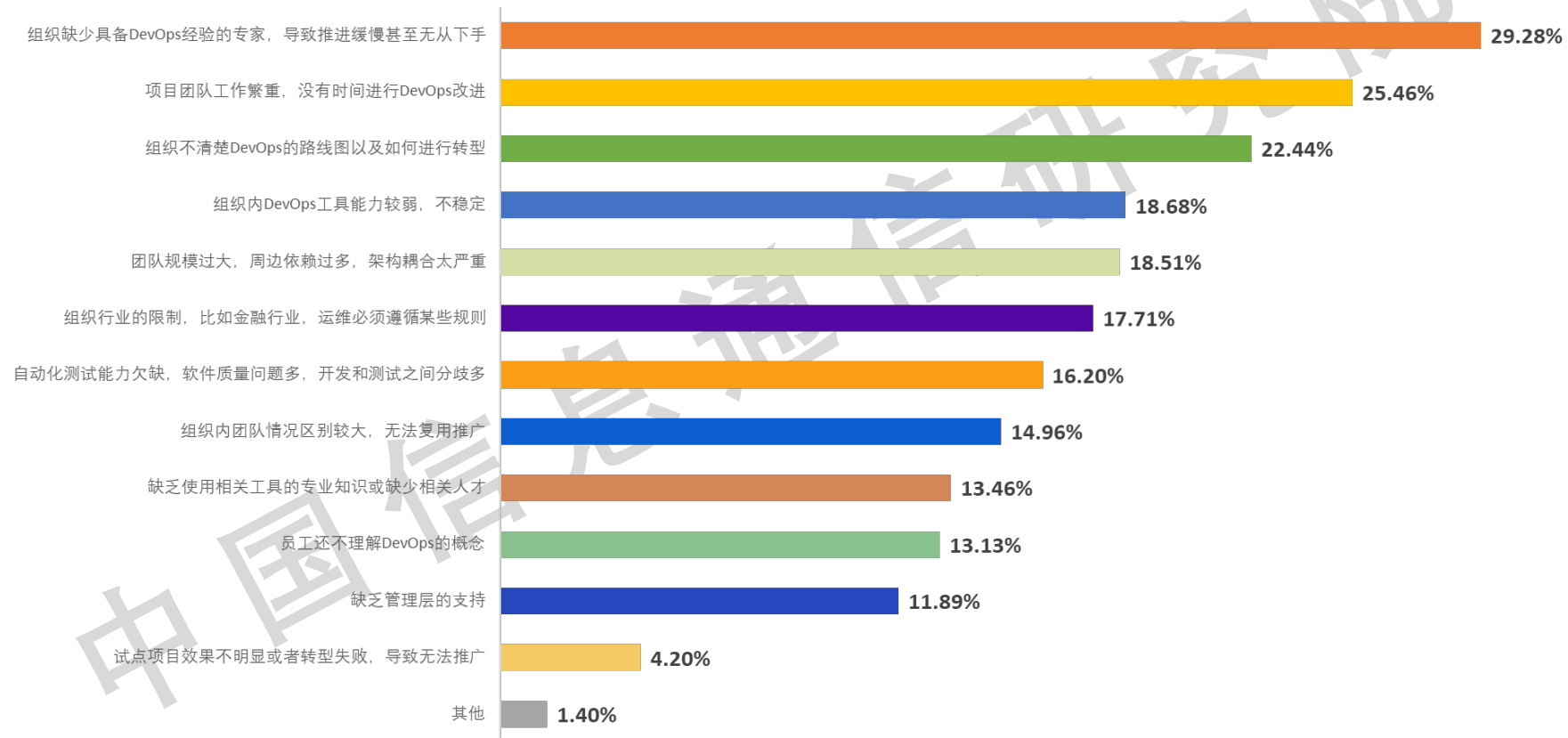
超六成企业已实践DevOps，但难以确认转型成功与否。



数据来源：中国信息通信研究院

DevOps转型是否成功

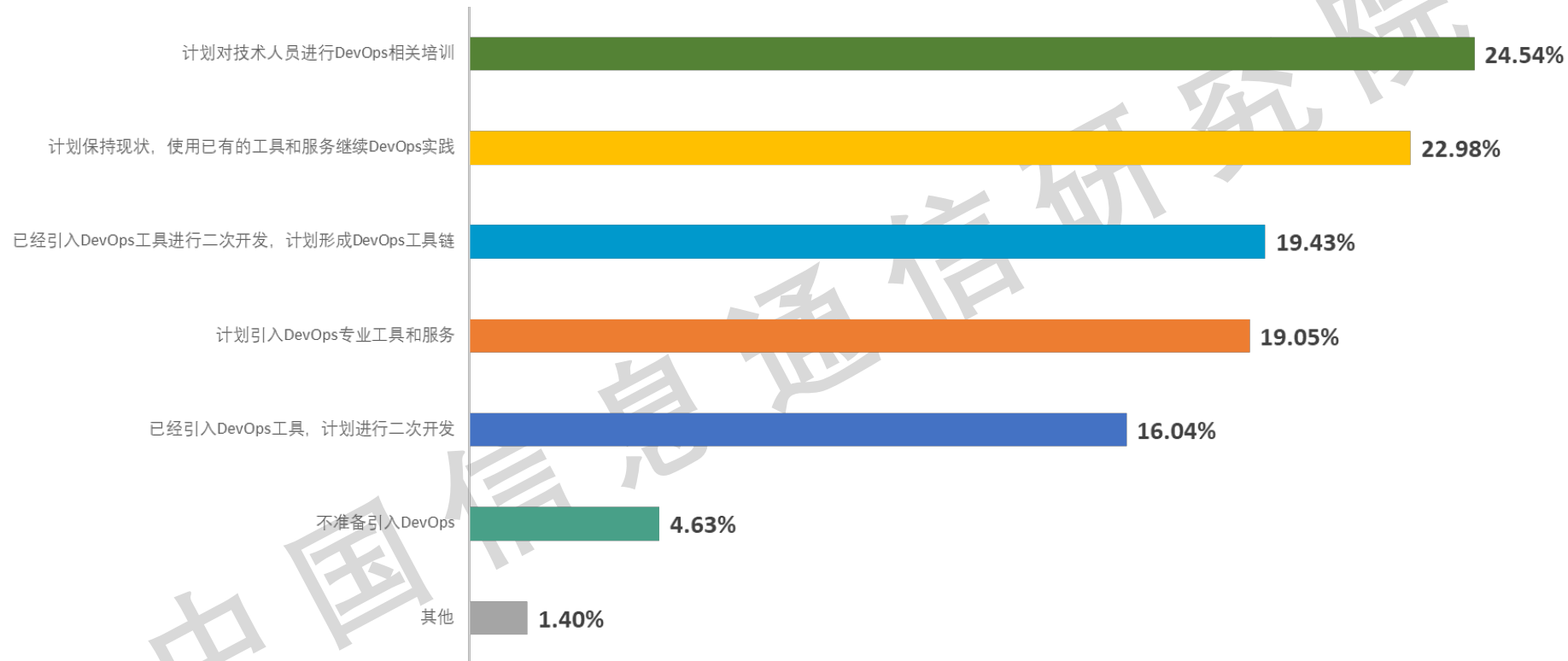
缺乏相关领域专家、转型路径不清晰等多方面问题成为组织级DevOps转型的最大阻碍。



数据来源：中国信息通信研究院

阻碍DevOps转型的因素

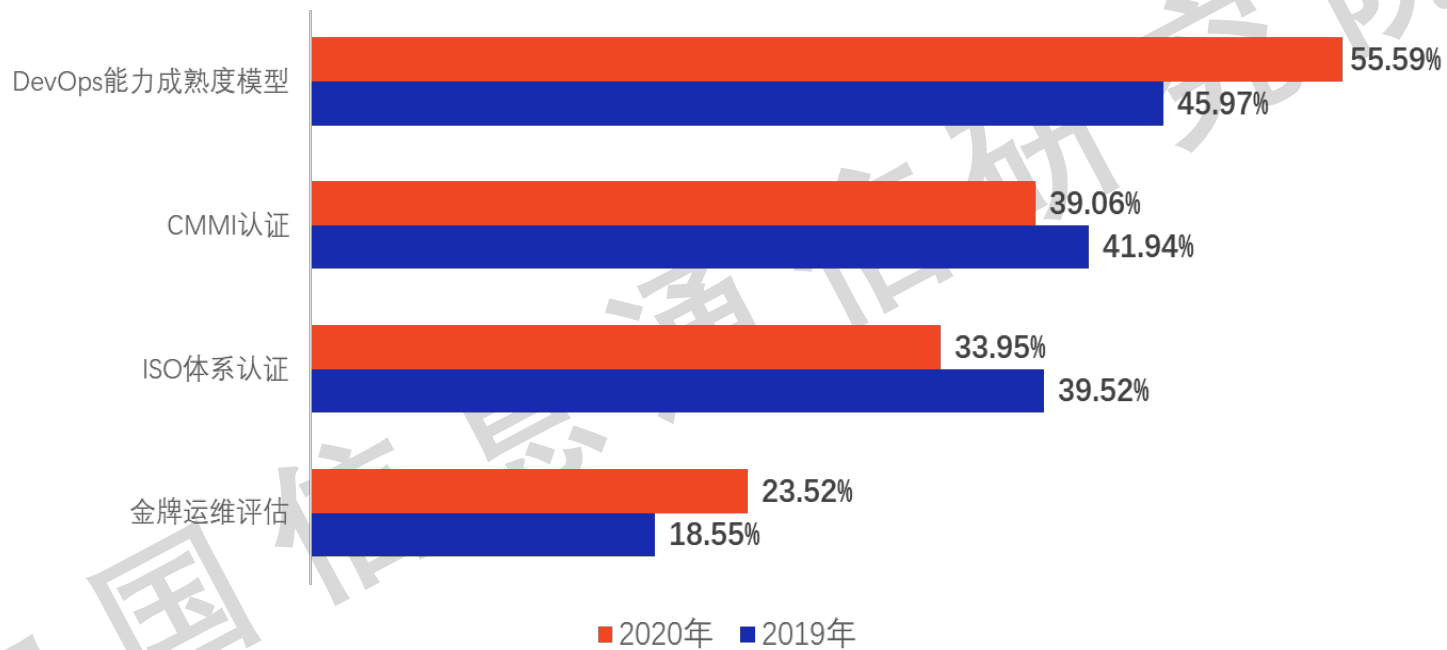
企业关注DevOps相关人才培养。



数据来源: 中国信息通信研究院

企业未来对DevOps投入计划分布

DevOps能力成熟度评估受关注程度上涨。



数据来源：中国信息通信研究院

感兴趣的评估或认证

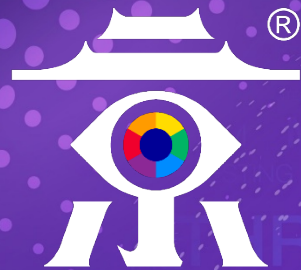


联系人：刘凯铃

电话：15650786171（同微信）

邮箱:liukailing@caict.ac.cn

中国信息通信研究院



2020 北京网络安全大会

2020 BEIJING CYBER SECURITY CONFERENCE

THANKS

全球网络安全 倾听北京声音