一种真正以业务为中心的访问控制模型

李德辉

众图识人 CEO

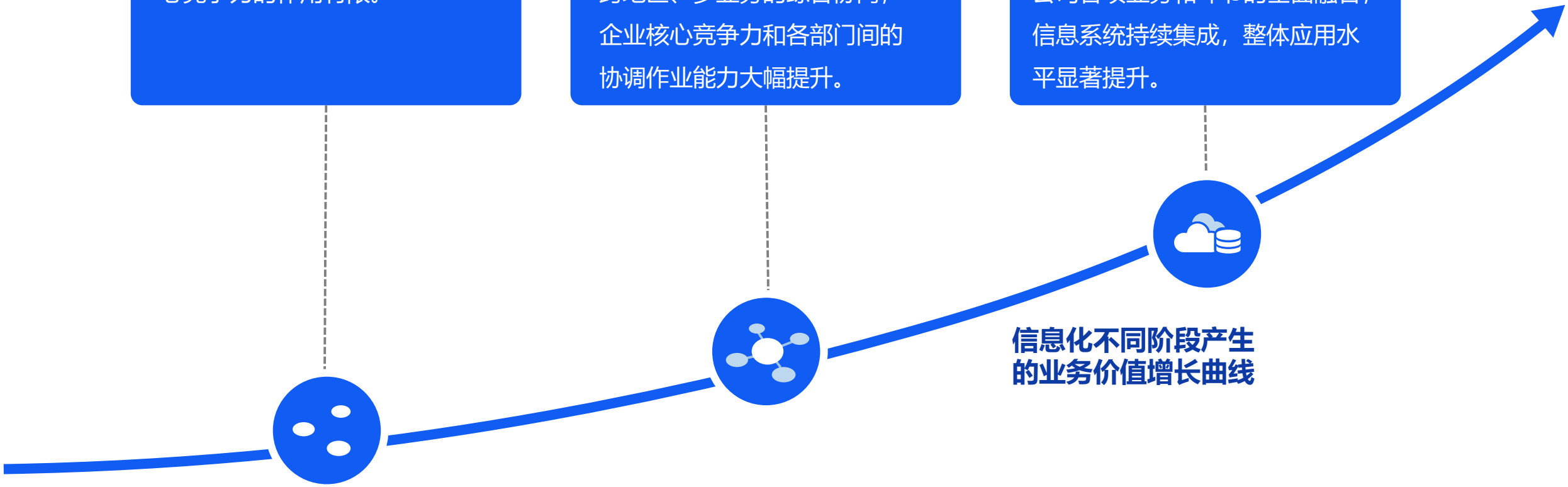
目录

企业信息化不同阶段产生的业务价值

各部门采用信息系统替代独立业务的手工操作，提高企业核心竞争力的作用有限。

通过统一的信息系统平台实现内部业务信息的集成和跨部门、跨地区、多业务的综合协同，企业核心竞争力和各部门间的协调作业能力大幅提升。

信息化开始成为企业发展战略的重要组成部分，实现信息技术与公司各项业务和环节的全面融合，信息系统持续集成，整体应用水平显著提升。



信息化不同阶段产生的业务价值增长曲线

分散建设独立信息系统
单一部门信息化

RBAC 满足需求

统一建设全局信息系统
企业级信息化

RBAC 角色爆炸

持续提升与集成共享信息系统
产业链级信息化

需要新的访问控制模型

分散建设阶段

业务驱动力

各业务部门为了提高工作效率，纷纷采用信息系统替代手工操作，开展基于各自业务的单一信息化建设

信息化特点

- 各部门独立建设
- 信息系统数量多，系统用户少、规模小
- 系统应用效率低，建设、维护成本较高
- 形成众多的信息孤岛，信息共享程度低
- 无法有效支持业务协调和战略决策

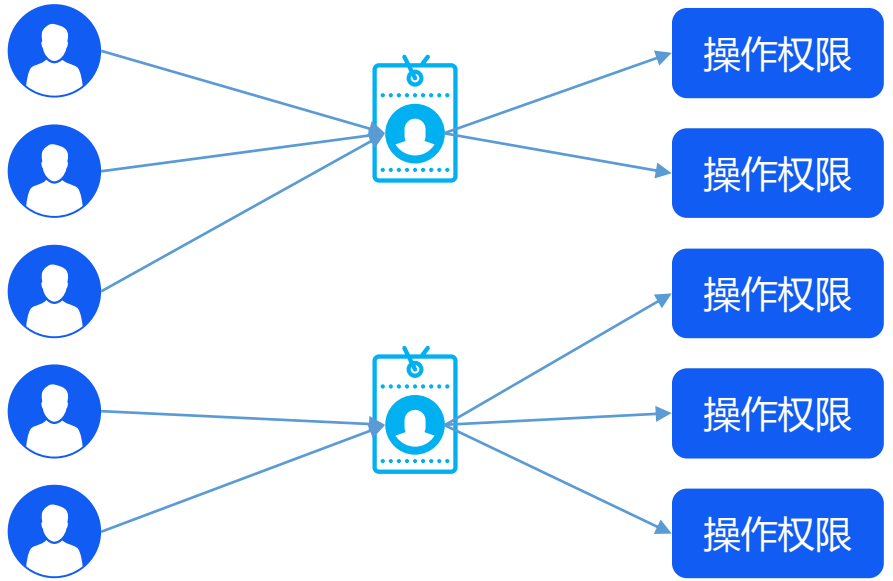
业务价值

- 企业各业务部门处理各自相对简单的研发设计、生产及经营业务，提高了工作效率
- 对提高企业核心竞争力的作用有限

访问控制

- 访问用户少，业务范围小
- 访问控制到操作级别，不进行数据级控制
- 访问环境简单：设备固定，网络环境简单
- 适合RBAC模型

RBAC 权限管理模型



统一建设阶段

业务驱动力

通过统一的信息系统平台实现内部业务信息的集成和跨部门、跨地区、多业务的综合应用，企业核心竞争力和各部门间的协调作业能力大幅提升

信息化特点

- 信息系统数量大幅减少
- 各系统用户多、规模大、应用范围广
- 系统应用效率高，整体运行维护成本下降
- 信息孤岛数量大幅度减少，信息共享成都大幅提高
- 信息安全和在被体系基本完备

业务价值

- 实现业务、资金、信息在一个平台上管理
- 实现业务信息的跨部门、跨地区、多业务综合应用
- 企业的核心竞争力和各部门间的协调作业能力大幅提升
- 基本实现业务系统和支持战略决策

访问控制挑战

- 访问用户多，必须区分业务范围
- 需要根据业务上下文进行访问控制
- 继续采用RBAC模型导致角色爆炸

RBAC 在加入业务上下文后产生角色爆炸

某股份制银行：不同网点柜员，可选择的金融产品和操作的金额不一样，银行在全国有上万个网点，产生上千种角色

某大型制造业：不同地区公司的相同岗位的人能够访问的数据不同，能够进行的操作不同，ERP中的数十万角色

持续提升阶段

业务驱动力

信息化开始成为企业发展战略的重要组成部分，实现信息技术与公司各项业务和环节的全面融合，信息系统持续集成，整体应用水平显著提升

信息化特点

- 系统功能持续完善，系统集成度持续提升，更加满足业务需求
- 系统的应用更深入，更广泛，对业务的支持作用持续提升
- 信息化与业务战略发展和转型实现一体化

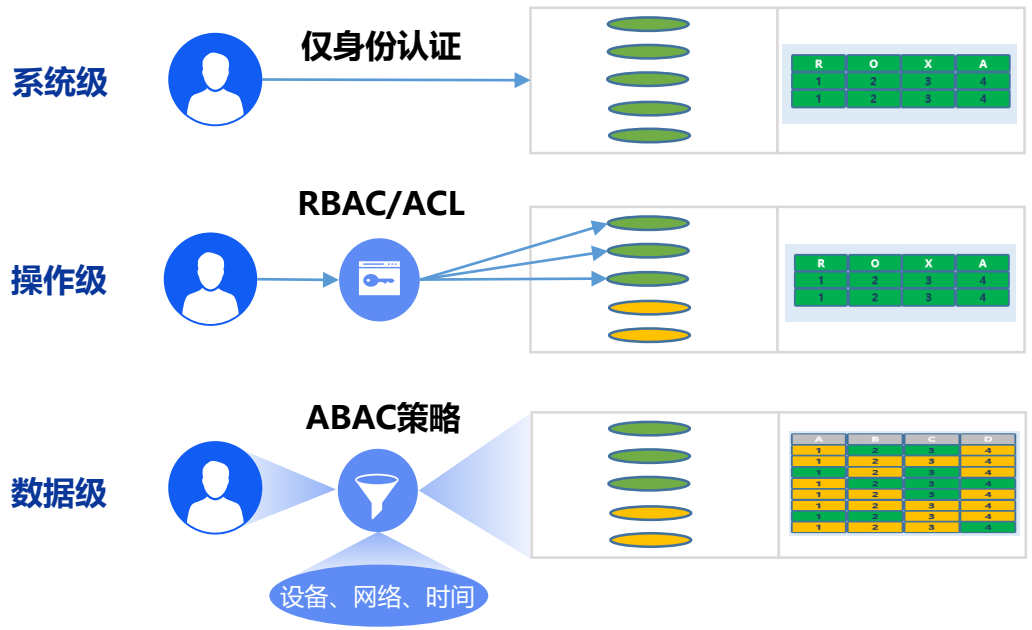
业务价值

- 信息化全面融入研发、设计、生产、经营、管理、决策活动，基于知识进行快速战略决策
- 多行业、多地区、多业务全面集成与协同，有效改造和提升企业价值链

访问控制挑战

- 信息系统相互集成需要访问控制：
  - 系统级的访问控制
  - 操作级的访问控制
  - **数据级的访问控制**
  - **结合访问环境上下文进行访问控制**

不同粒度的访问控制

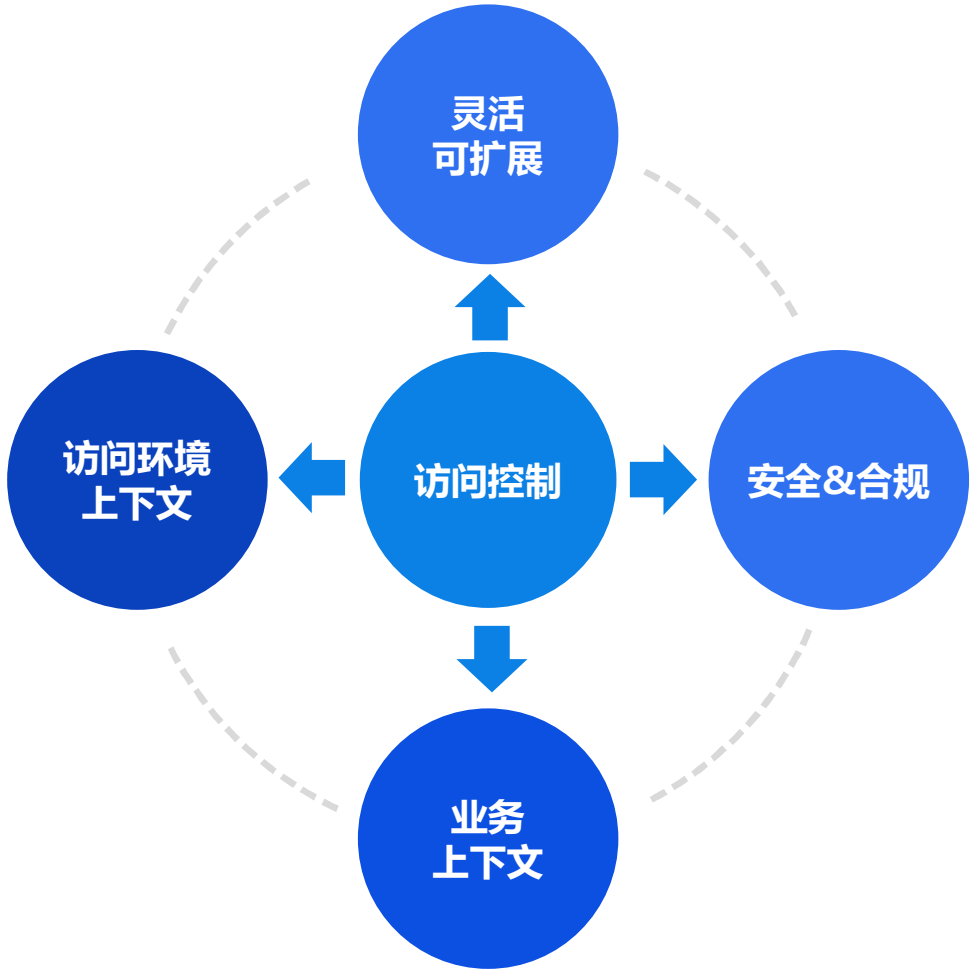


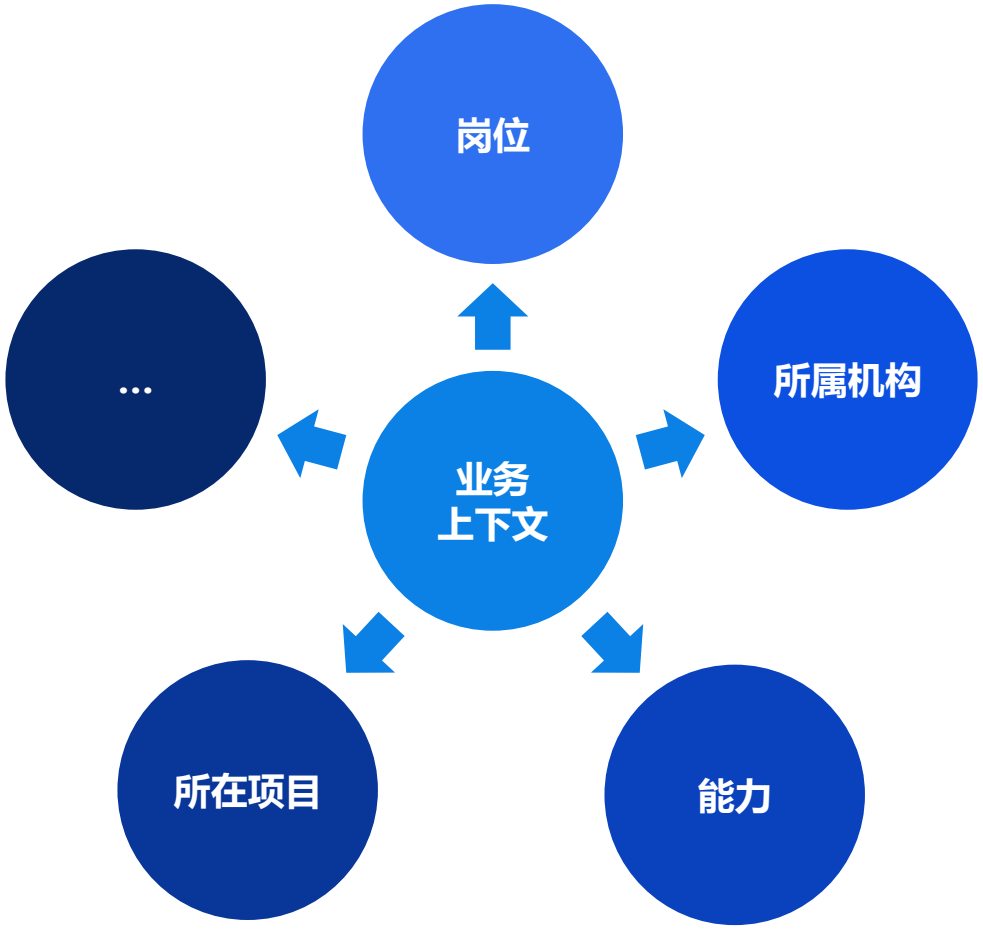
信息化发展及新技术应用对访问控制的挑战

用户	访问环境	信息系统	数据	IT 基础设施
内部员工	受管理的PC 内网有线访问	各部门分散建设	分散存储在信息系统中 仅部门内访问	传统数据中心
供应商、合作伙伴 外包员工、客户	PC、平板、移动电话、 企业网络、移动互联网	统一建设，分级管理	建立数据分布，满足用户在任何地方以任何方式访问已授权的信息	混合云、公有云

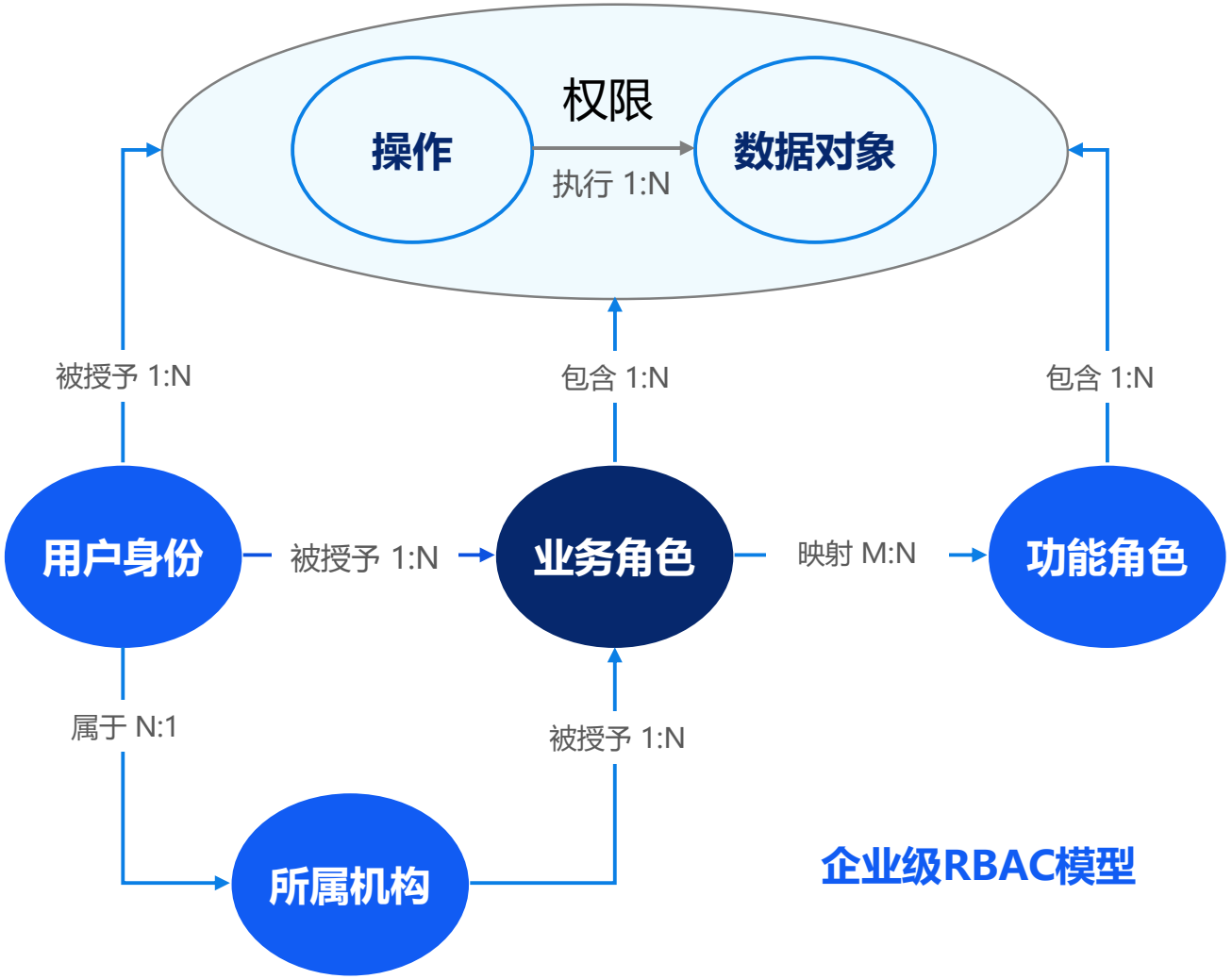
目录

从业务视角分析访问控制





传统访问控制模型 RBAC

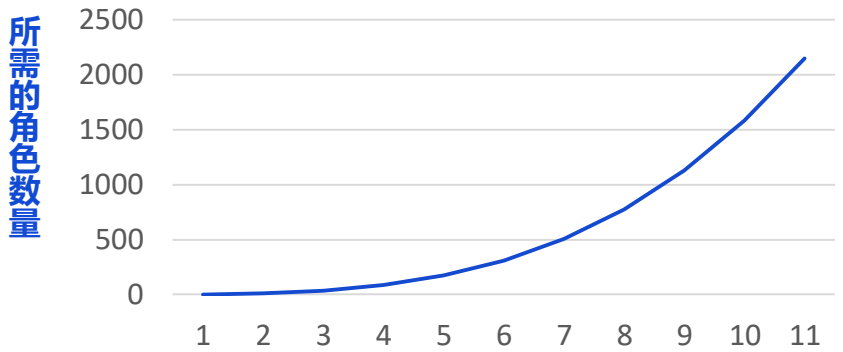


企业级RBAC模型

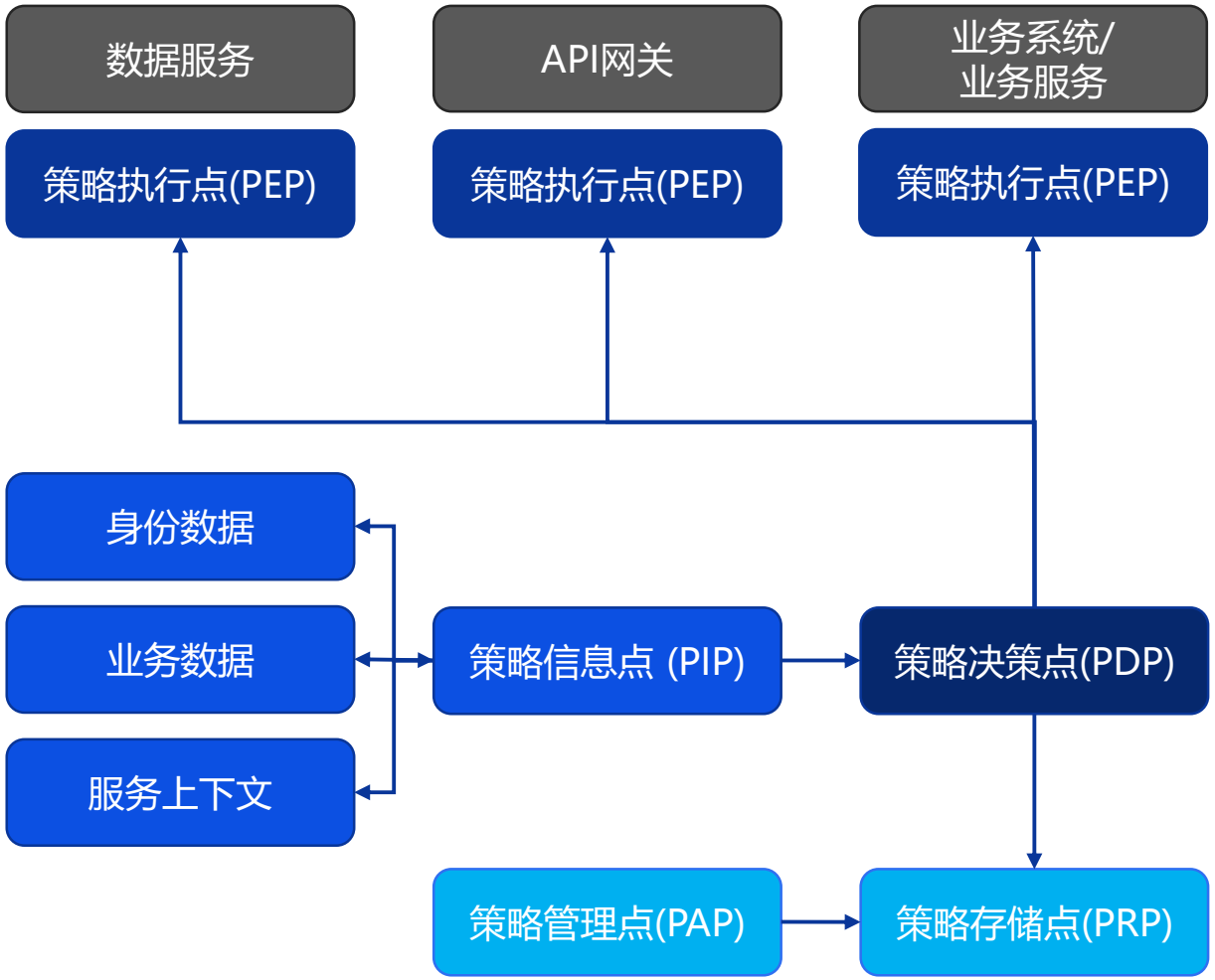
RBAC:

- 基于角色的访问控制，角色定义了一个用户拥有的权限
- **静态授权**，角色需要绑定到用户后才生效
- 适用于信息化**第一阶段**的访问控制场景
- 一旦访问控制因素变多，将产生**角色爆炸**

角色数量随访问控制因素呈几何增长：



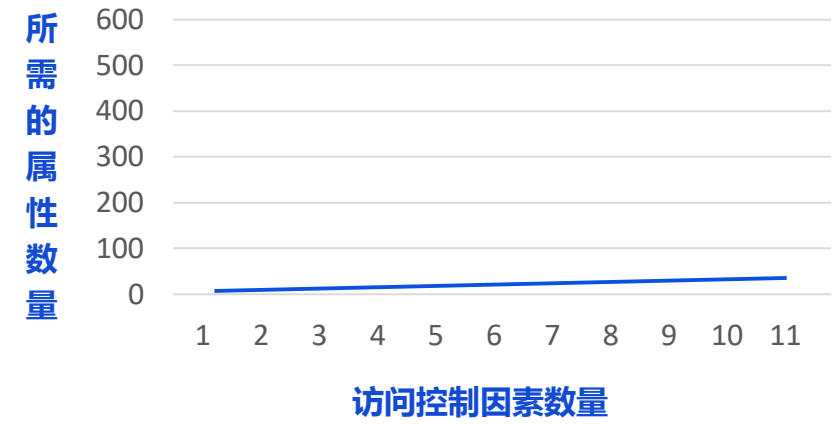
ABAC 访问控制模型



ABAC:

- 基于属性的访问控制模型
- 通过基于属性的访问控制策略灵活定义访问者（身份属性）在什么条件下（访问环境上下文属性）可以访问什么对象（对象属性）
- 运行时**动态授权**，属性或策略改变后权限立即变更生效
- 一旦访问控制因素变多，**只增加一个属性**

属性随访问控制因素呈线性增长:



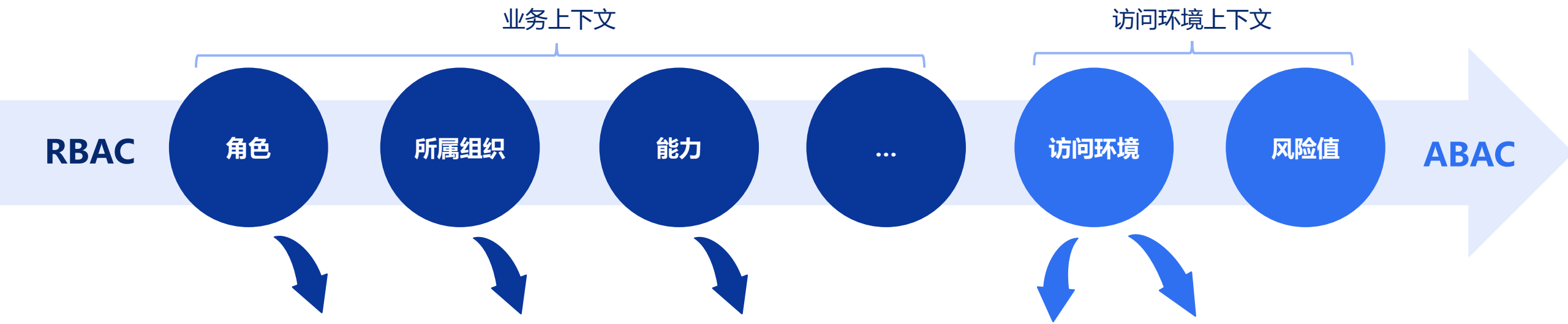
ABAC VS. RBAC

	RBAC	ABAC	业务价值
逻辑表达能力	仅支持一种：角色包含一组权限	可表达逻辑复杂的访问控制策略	几百条访问控制策略替代上百万的用户角色，为业务全面协同带来的复杂访问控制提供**扩展能力**
以业务为中心	否，根据业务规则难以定义角色	是，策略语言直接描述业务规则	
业务上下文	少量，否则会导致角色爆炸	只需要增加一个属性	
环境上下文	不支持	支持	**随时随地**都能安全处理业务
访问控制粒度	操作级	数据级	安全开展部门间、合作伙伴间的**数据共享**业务
访问控制生效	静态，预先定义	动态，运行时生效	**大量减少授权工作**
标准化程度	仅数据结构模型	策略标准、参考架构	保障**互操作性**，实现**中心化授权**

从RBAC进化到ABAC

用ABAC实现RBAC，只需要：

- 定义一个属性：角色
- 定义一条策略：如果用户角色包含了对应权限，用户可以访问



分公司的**身份管理员**可以为**所属公司**的用户授权**办公类**应用帐号，只能在**办公时间**通过**自己的电脑**进行操作

目录

ABAC 已经在美国信息化环境下得到了验证


NIST Special Publication 800-162

Guide to Attribute Based Access Control (ABAC) Definition and Considerations

COMPUTER SECURITY

NIST

标准：
NIST ABAC Guide 2014

大数据：
IC-ITE 使用ABAC对共享情报进行访问控制

企业应用：
SAP 使用ABAC进行动态授权管理 2016

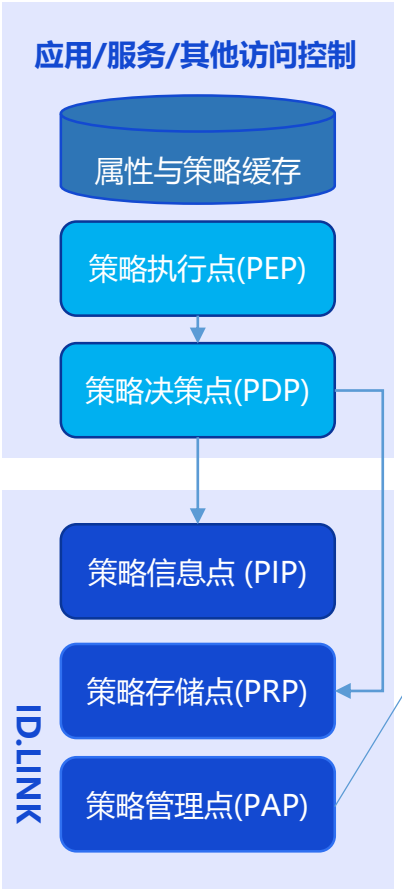
云：
使用ABAC在AWS进行可扩展的权限管理 2018

通过 ID.LINK 获得动态授权的能力

- IAM自身的访问控制
- 为第三方系统提供根据环境上下文的动态访问控制

- 通过ID.LINK集中管理属性及策略
- 与第三方系统集成，提供根据业务上下文的动态访问控制

- 通过ID.LINK集中管理属性及策略
- 为第三方应用提供属性及策略数据



ID.LINK 策略编辑UI

THANKS

2019北京网络安全大会

2019 BEIJING CYBER SECURITY CONFERENCE