信息安全技术 鉴别与授权

基于角色的访问控制模型与管理规范

高志刚
中国科学院软件研究所
zhigang2005@is.iscas.ac.cn
2011-9-22

内容

1. 访问控制简介

- 访问控制策略
- 基于角色访问控制(RBAC)
- RBAC应用中存在的问题

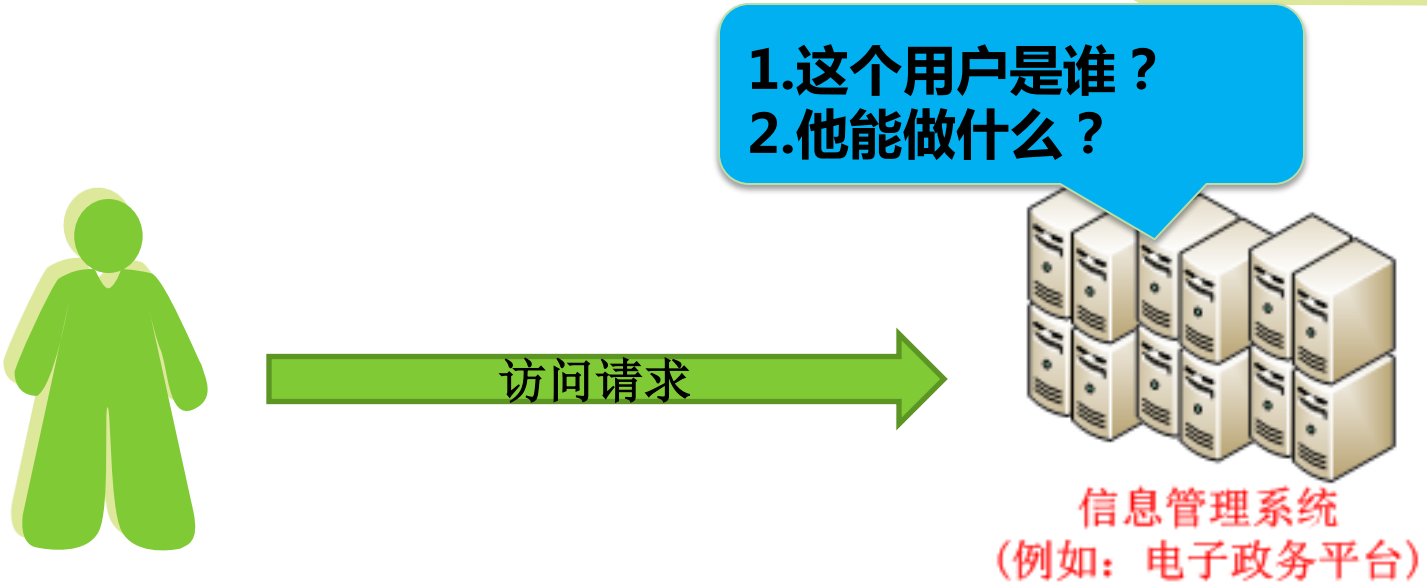
2. 基于角色的访问控制模型与管理规范

- 简介
- 基于角色的访问控制模型
- 基于角色的访问控制系统管理规范

3. RBAC在电子政务中的应用

- 电子政务系统需求分析、建设、验收中的应用
- 电子政务系统运行管理中的应用
- 电子政务系统维护更新中的应用

访问控制简介



身份认证

- 身份认证确定用户与他所声称的身份是否相符，解决用户是谁的问题。
- 口令认证、证书认证等

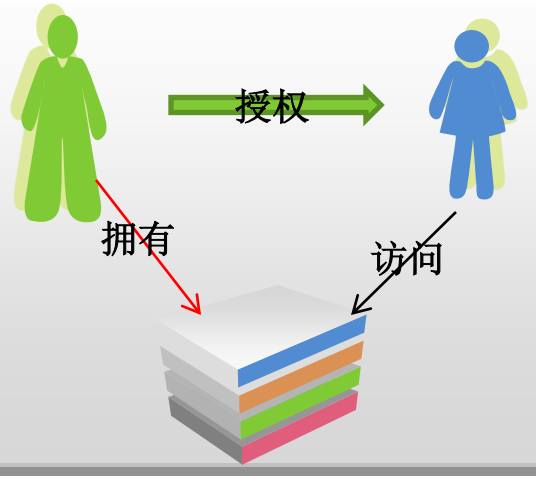
访问控制

- 访问控制是对信息系统资源的访问范围以及方式进行限制的策略
- 保护资源的安全

自主访问控制

自主访问控制

模型



特点和优势

- 授权过程不需要管理员参与，用户之间可以相互授权
- 管理代价较低，非常灵活

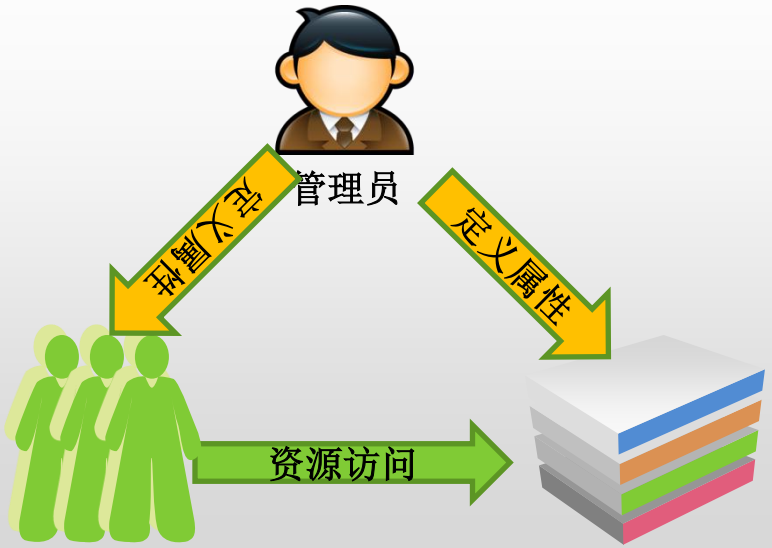
应用及问题

- 应用广泛，例如：Unix，Linux，Windows等
- 安全性较低，在线的权限传递风险较高

强制访问控制

强制访问控制

模型



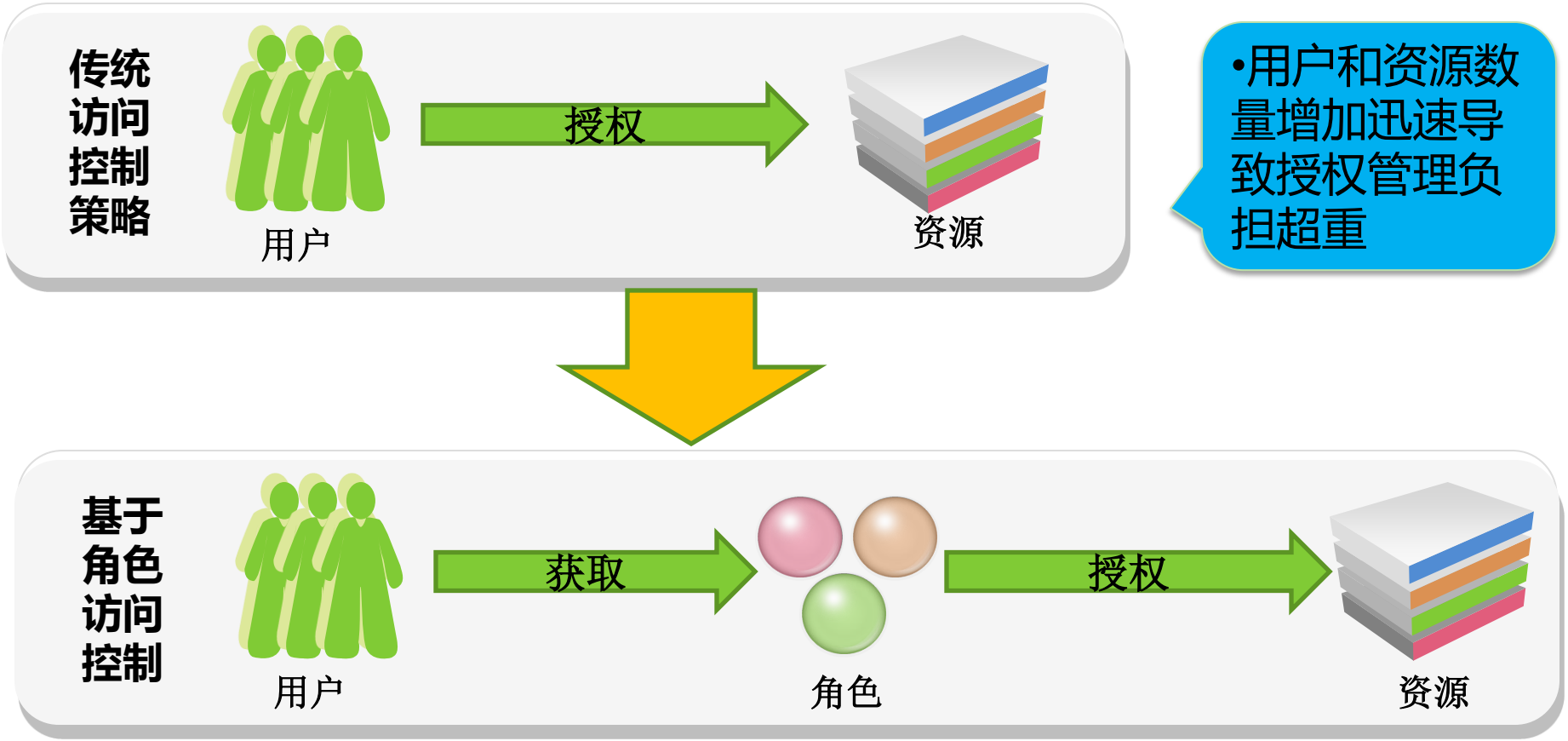
特点和优势

- 系统管理员为用户和资源分配安全属性，用户不能改变自身或任何客体的安全属性
- 按照确定的模式执行访问控制（上读/下写，上写/下读）
- **安全性高**

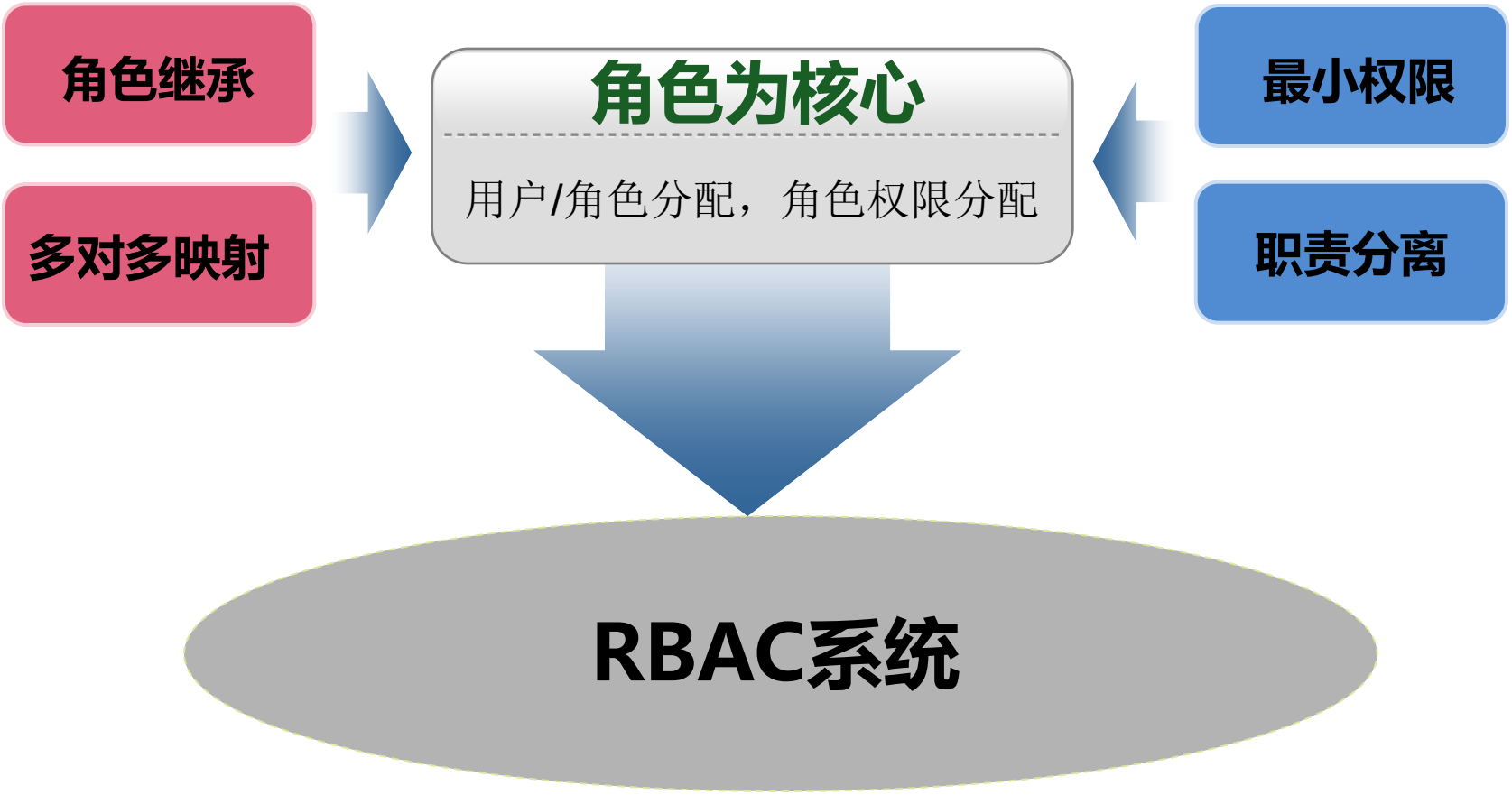
应用及问题

- 应用在高安全级别系统中（如军事系统）
- **管理不便，不够灵活**

基于角色的访问控制（1）


传统访问控制策略
用户
授权
资源
•用户和资源数量增加迅速导致授权管理负担超重
基于角色访问控制
用户
获取
角色
授权
资源

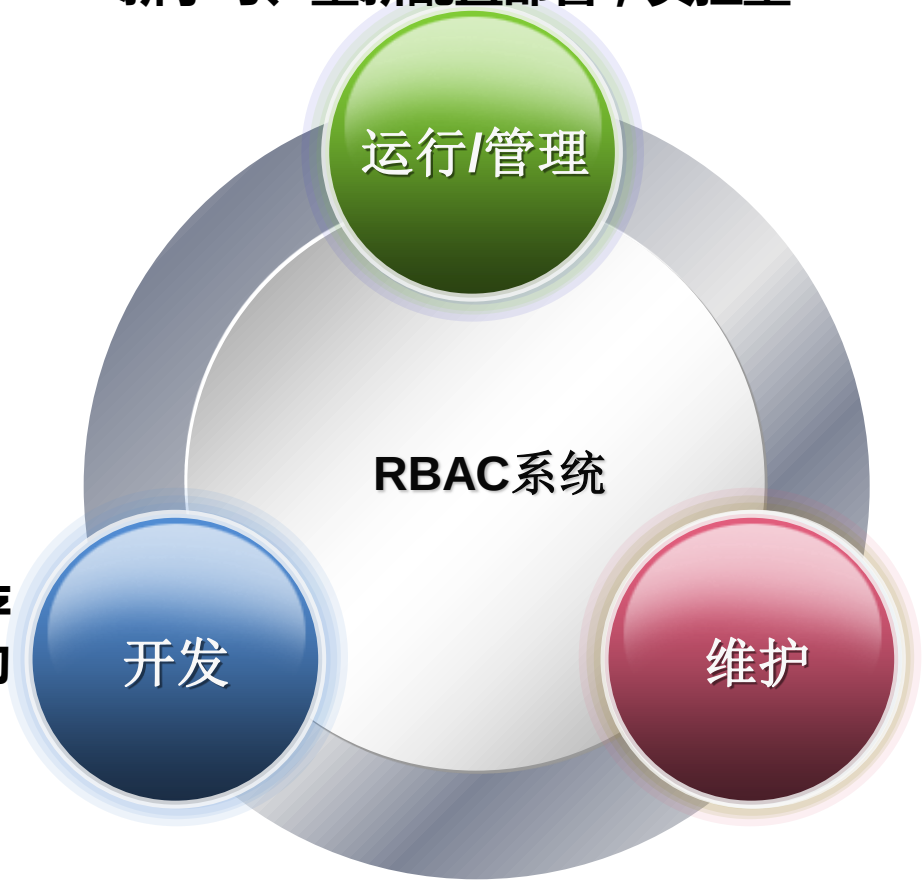
基于角色的访问控制（2）



RBAC应用中面临的问题

•角色抽取和定义缺乏指导，合理性缺乏验证标准，容易导致安全风险

•系统更新或是增加新系统时，要重新学习、重新配置部署，负担重



•对RBAC的特征和含义理解不一致，存在偏差，导致系统功能不合理，不完善

•系统的接口不规范，缺乏互操作性

•不同产品互不兼容，访问控制系统不能重用，增加系统部署和维护成本

内容

1. 访问控制简介

- 访问控制策略
- 基于角色访问控制
- 目前面临的问题

2. 基于角色的访问控制模型与管理规范

- 简介
- 基于角色的访问控制模型
- 基于角色的访问控制系统管理规范

3. 在电子政务中的应用

- 电子政务系统需求分析、建设、验收中的应用
- 电子政务系统使用中的应用
- 电子政务系统管理中的应用

基本信息

名称	信息安全技术 鉴别与授权 基于角色的访问控制模型与管理规范 Information security technology - Authentication and authorization - Role-based access control model and management specification
标准状态	2010-09-02 发布 2011-02-01 实施
起草单位	中国科学院软件研究所 信息安全共性技术国家工程研究中心
归口单位	全国信息安全标准化技术委员会

简介

出发点

- 解决对基于角色的访问控制特征、效用和含义理解的不规范性和不确定性
- 解决不同产品间的互操作问题

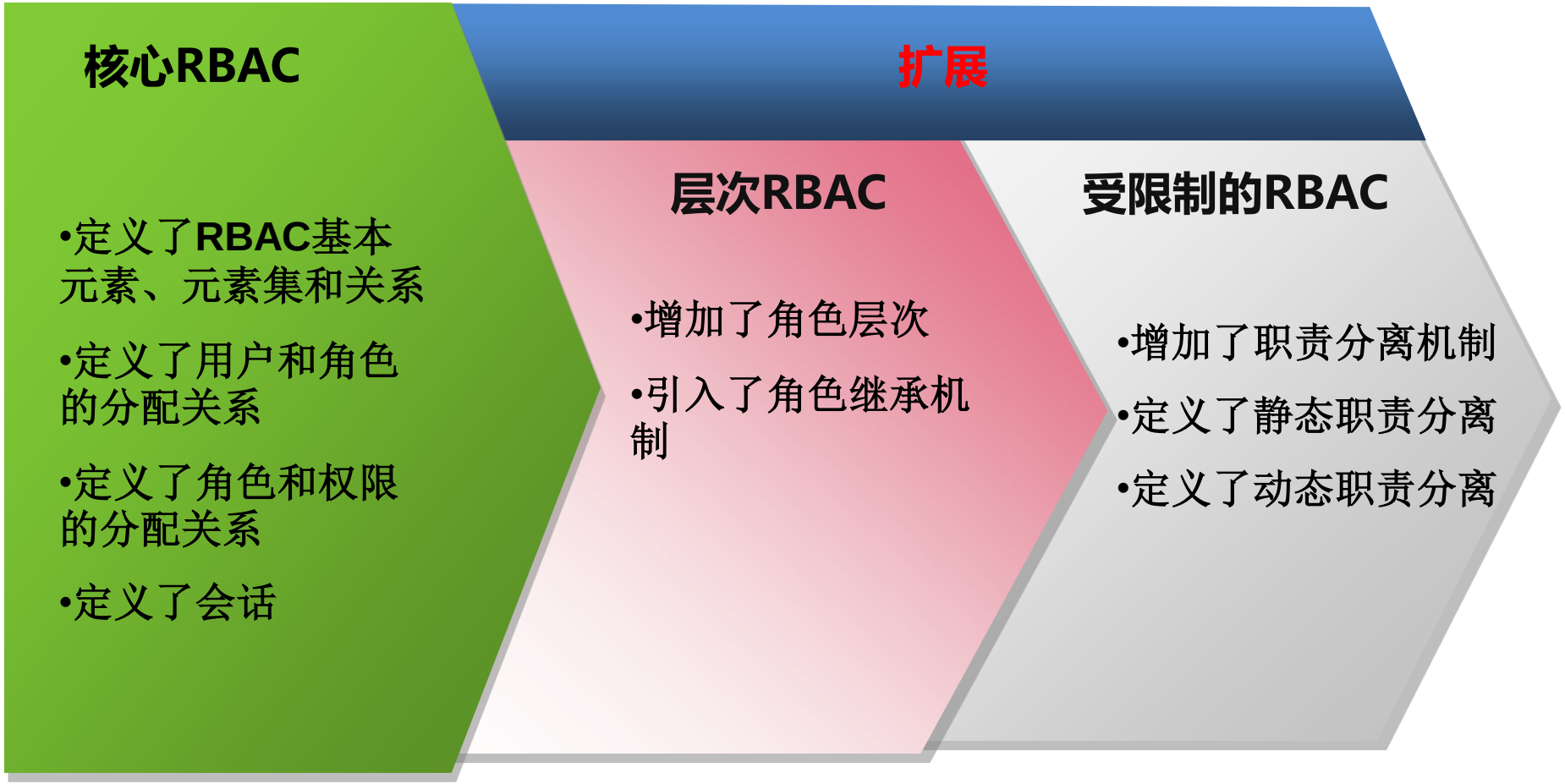
解决方法

- 定义一个可组合的、分层次的基于角色访问控制模型
- 定义基于角色访问控制系统管理接口和功能定义

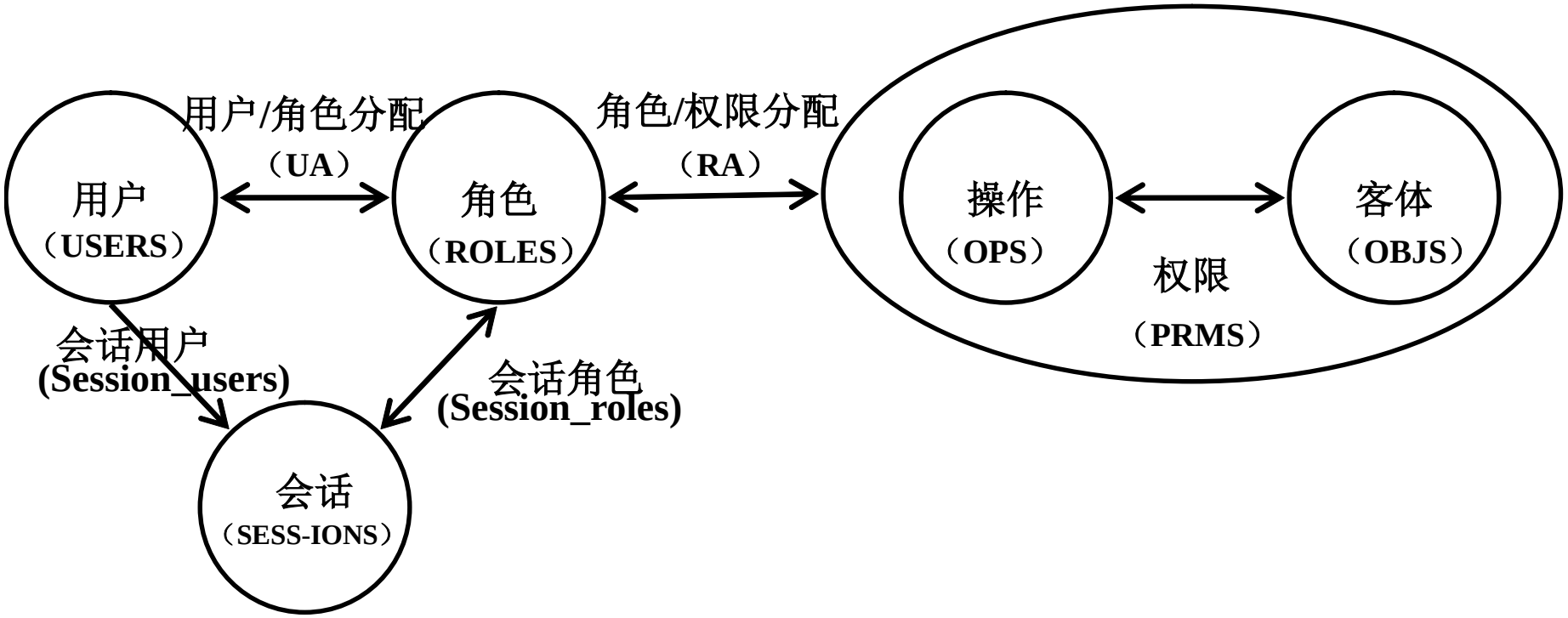
目标

- 为基于角色访问控制系统一致性和互操作问题提供解决方案
- 促进基于角色访问控制系统的研究和应用

RBAC参考模型


核心RBAC
•定义了RBAC基本元素、元素集和关系
•定义了用户和角色的分配关系
•定义了角色和权限的分配关系
•定义了会话
扩展
层次RBAC
•增加了角色层次
•引入了角色继承机制
受限制的RBAC
•增加了职责分离机制
•定义了静态职责分离
•定义了动态职责分离

核心RBAC


用户/角色分配
（UA）
角色/权限分配
（RA）
用户
（USERS）
角色
（ROLES）
操作
（OPS）
客体
（OBJS）
权限
（PRMS）
会话用户
(Session_users)
会话角色
(Session_roles)
会话
（SESS-IONS）

RBAC参考模型

核心RBAC

- 定义了RBAC基本元素、元素集和关系
- 定义了用户和角色的分配关系
- 定义了角色和权限的分配关系
- 定义了会话

扩展

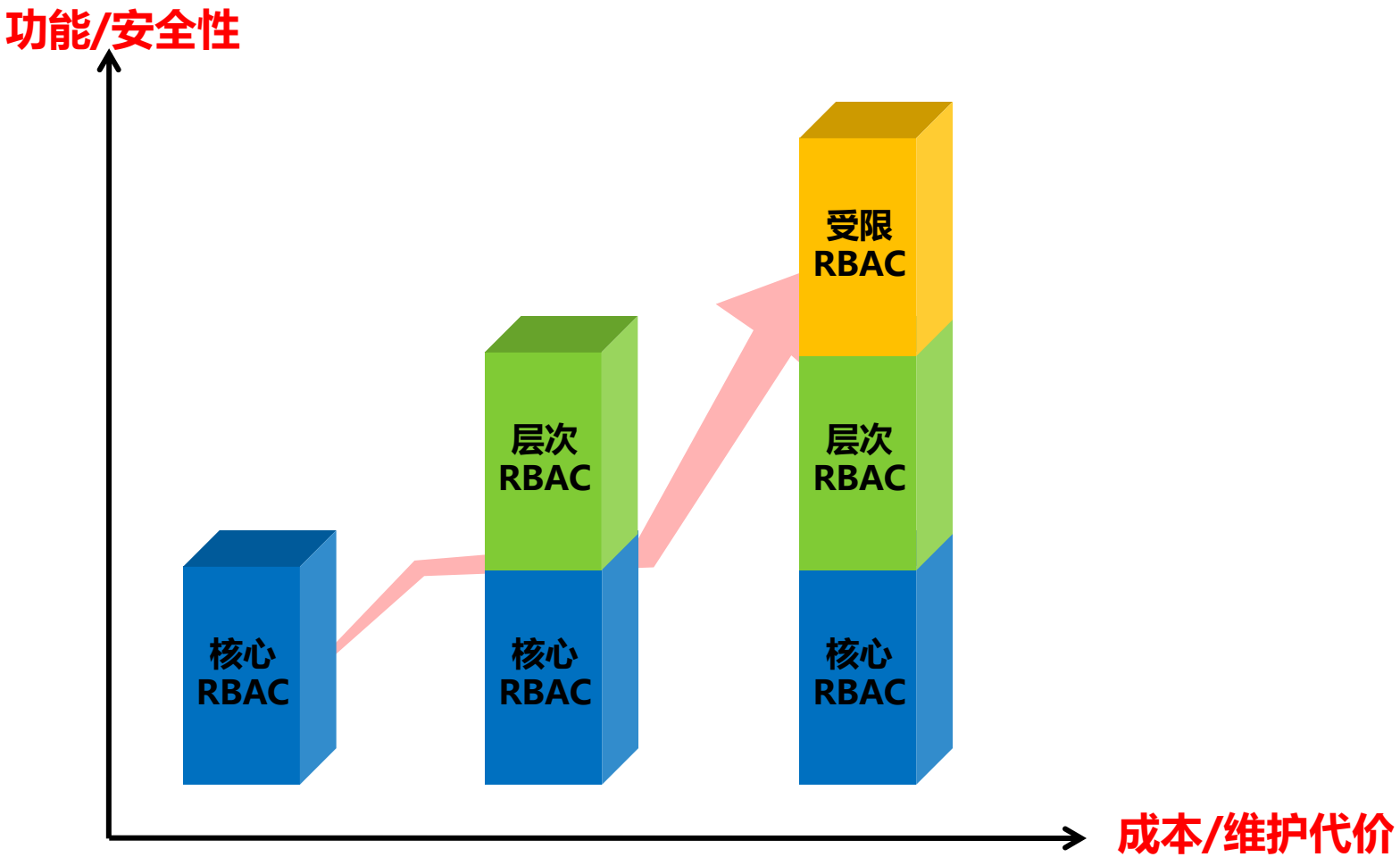
层次RBAC

- 增加了角色层次
- 引入了角色继承机制

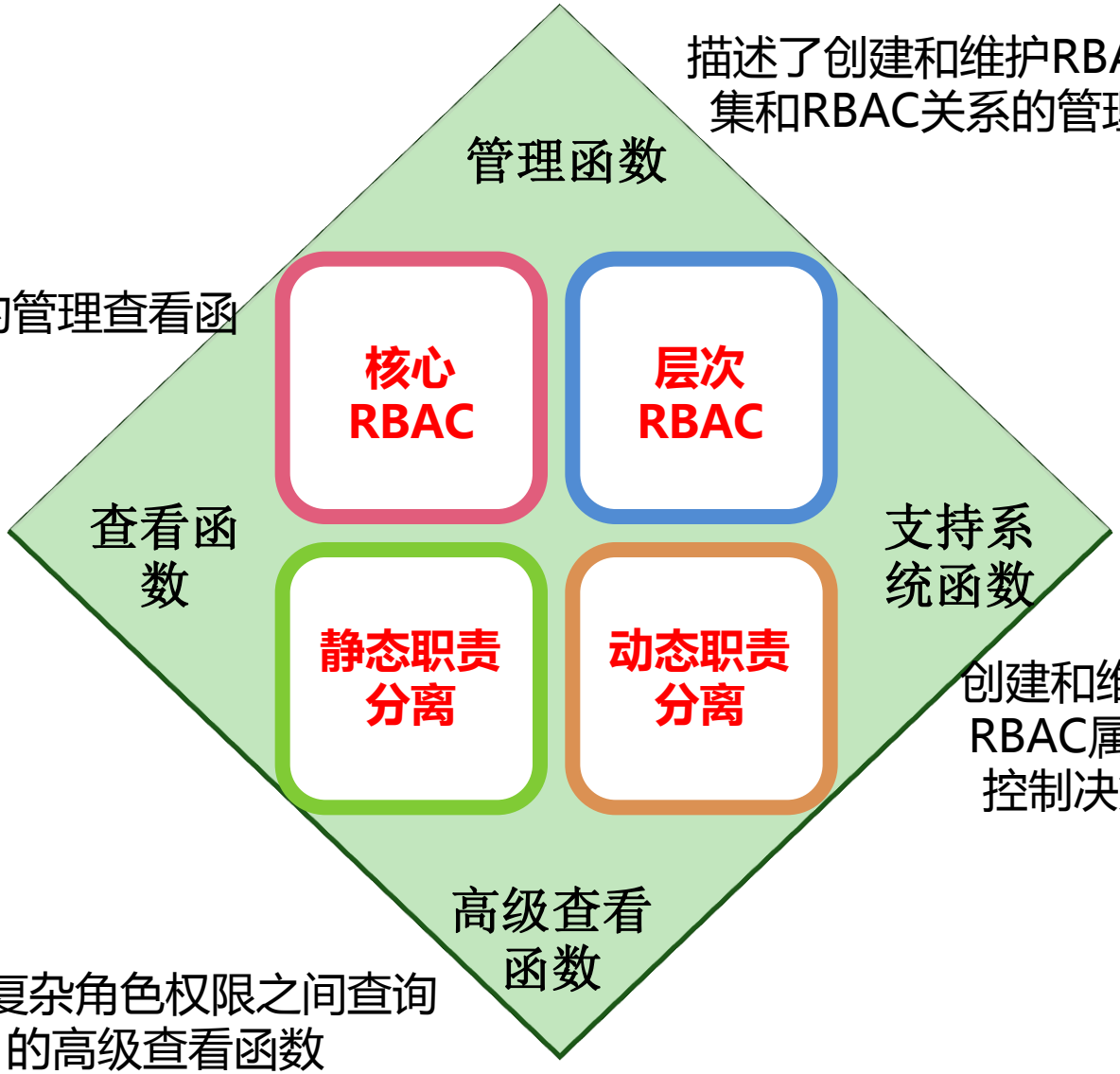
受限制的RBAC

- 增加了职责分离机制
- 定义了静态职责分离
- 定义了动态职责分离

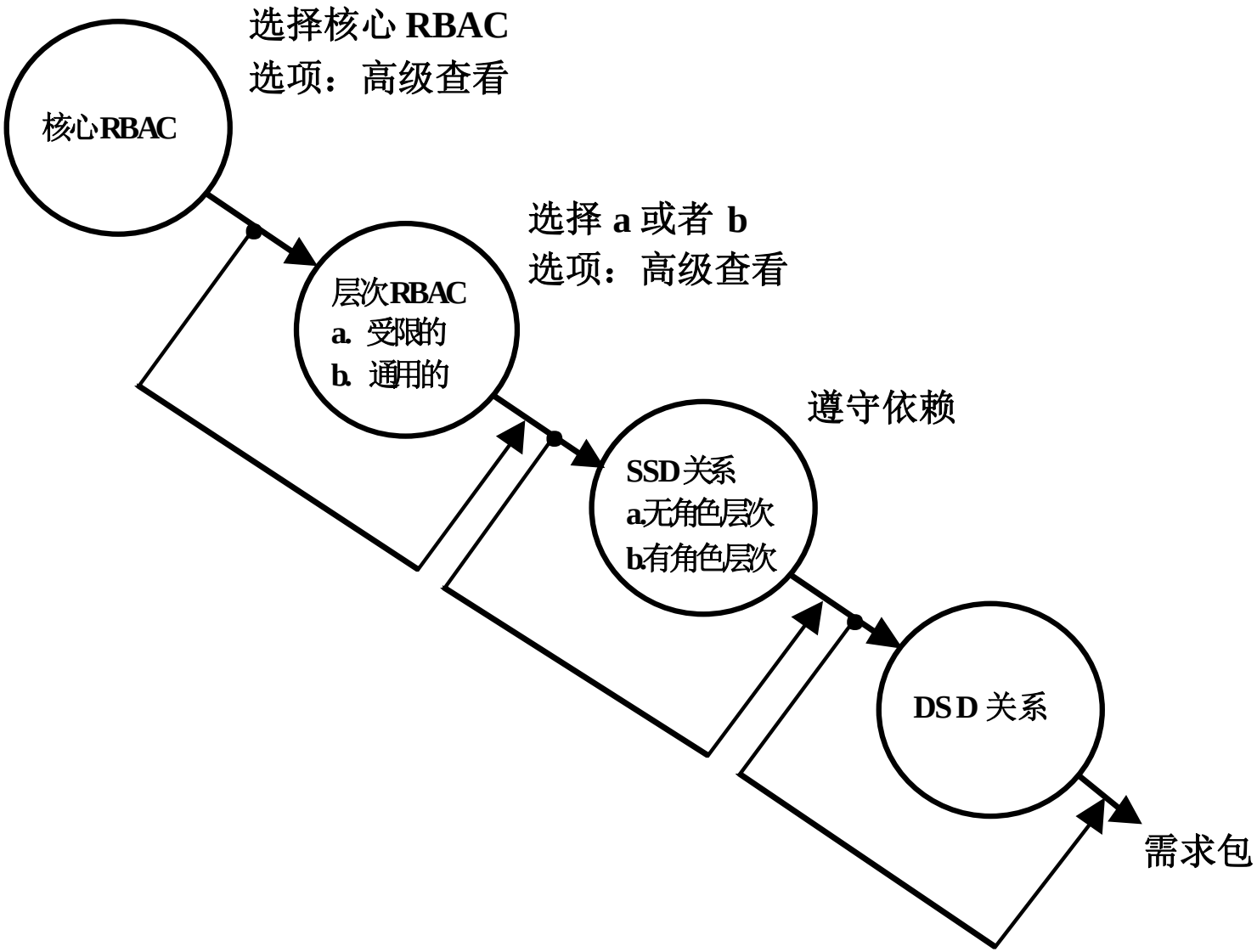
RBAC组件的组合



RBAC系统和管理规范



示例——创建功能组件


选择核心 RBAC
选项：高级查看
核心RBAC
选择 a 或者 b
选项：高级查看
层次RBAC
a. 受限的
b. 通用的
遵守依赖
SSD 关系
a.无角色层次
b.有角色层次
DSD 关系
需求包

内容

1. 访问控制简介

- 访问控制策略
- 基于角色访问控制
- 目前面临的问题

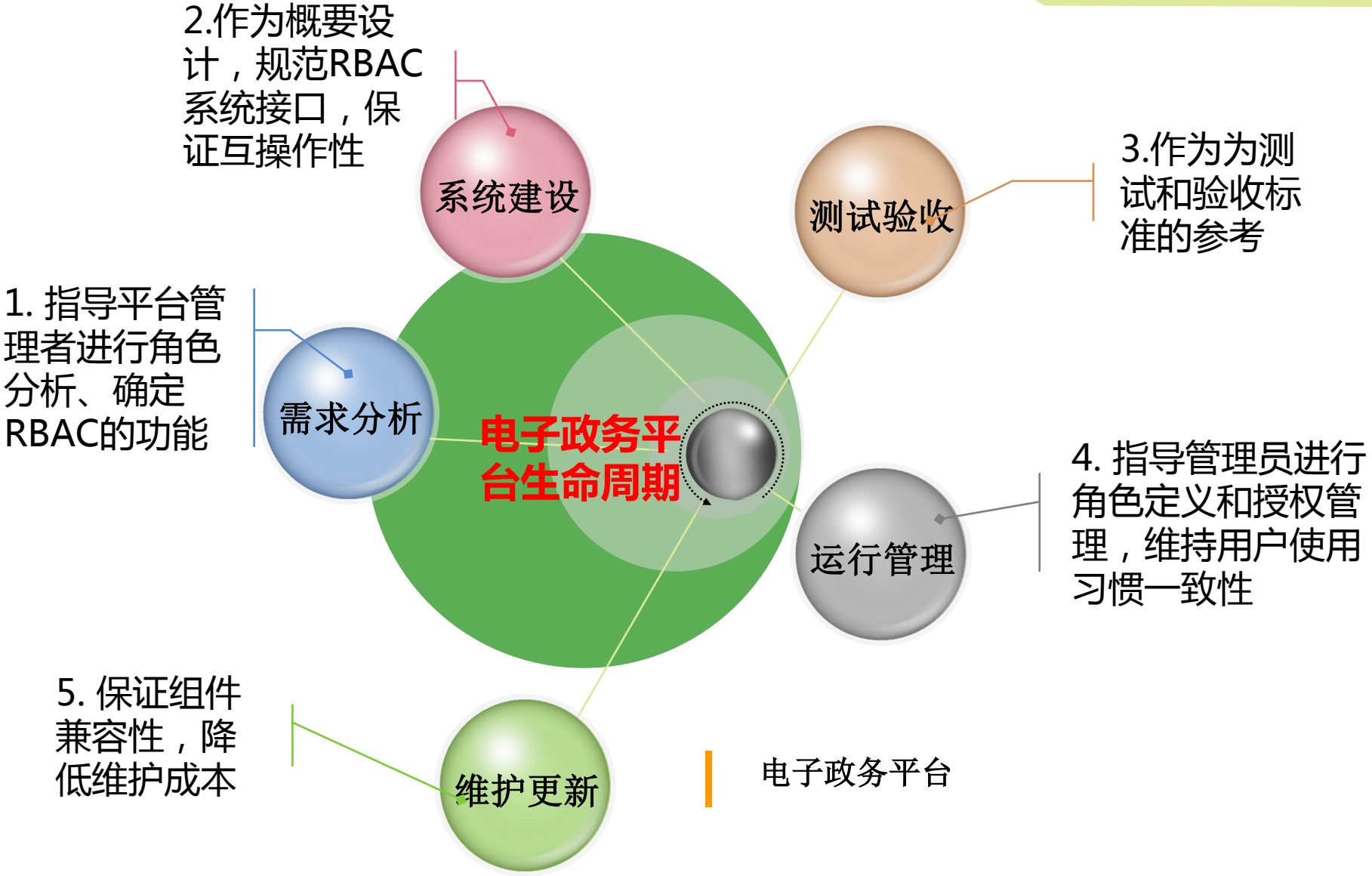
2. 基于角色的访问控制模型与管理规范

- 简介
- 基于角色的访问控制模型
- 基于角色的访问控制系统和管理规范

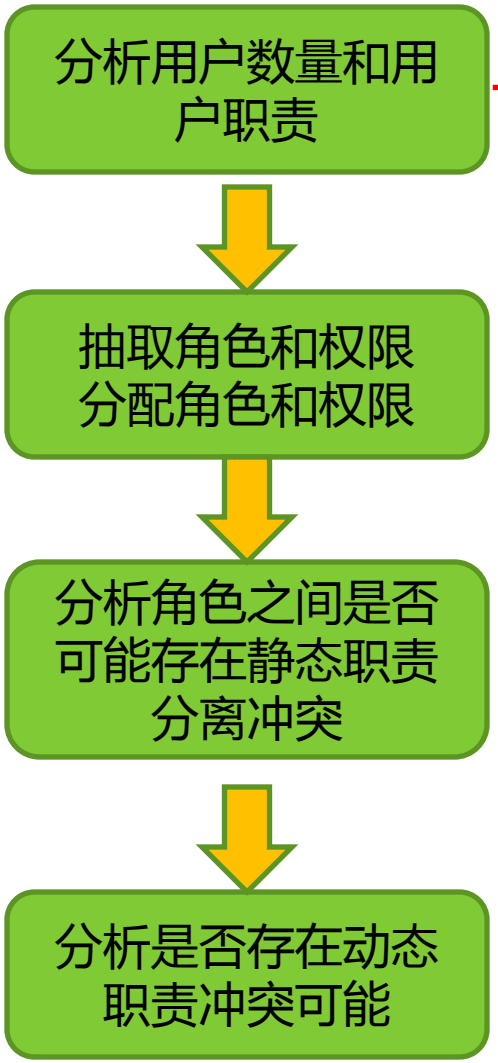
3. 在电子政务中的应用

- 电子政务系统需求分析、建设、验收中的应用
- 电子政务系统使用中的应用
- 电子政务系统管理中的应用

RBAC规范在电子政务平台中的应用点



应用实例——需求分析



层次RBAC？
如果用户数量大，且用户的职责之间存在一部分共性，则需要层次RBAC

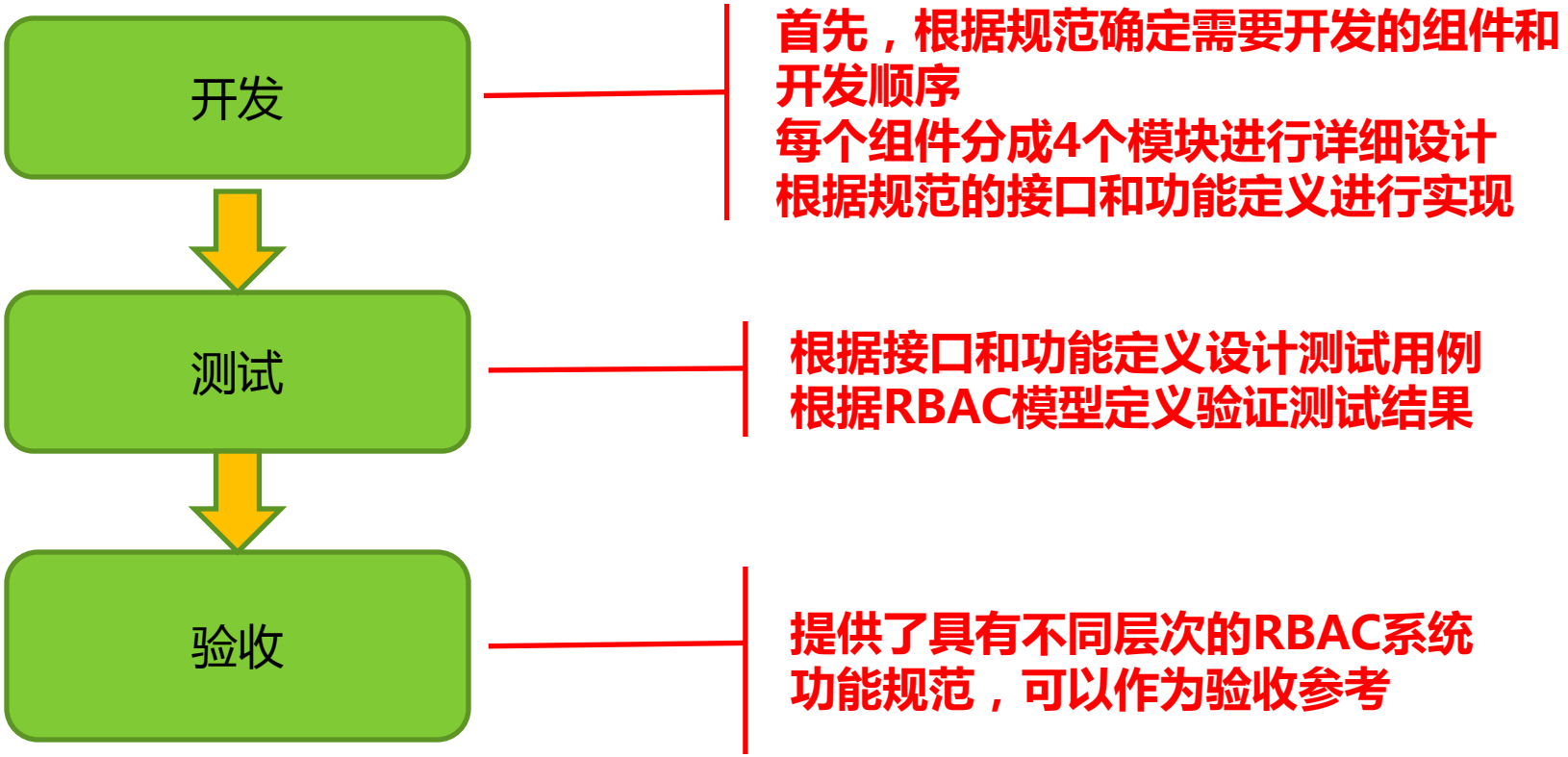
实现最小权限？
权限分配存在冲突？

静态职责分离机制？
如果存在静态职责冲突的风险，则需要实现静态职责分离机制。

动态职责分离机制？
如果存在动态职责冲突的风险，则需要实现静态职责分离机制。

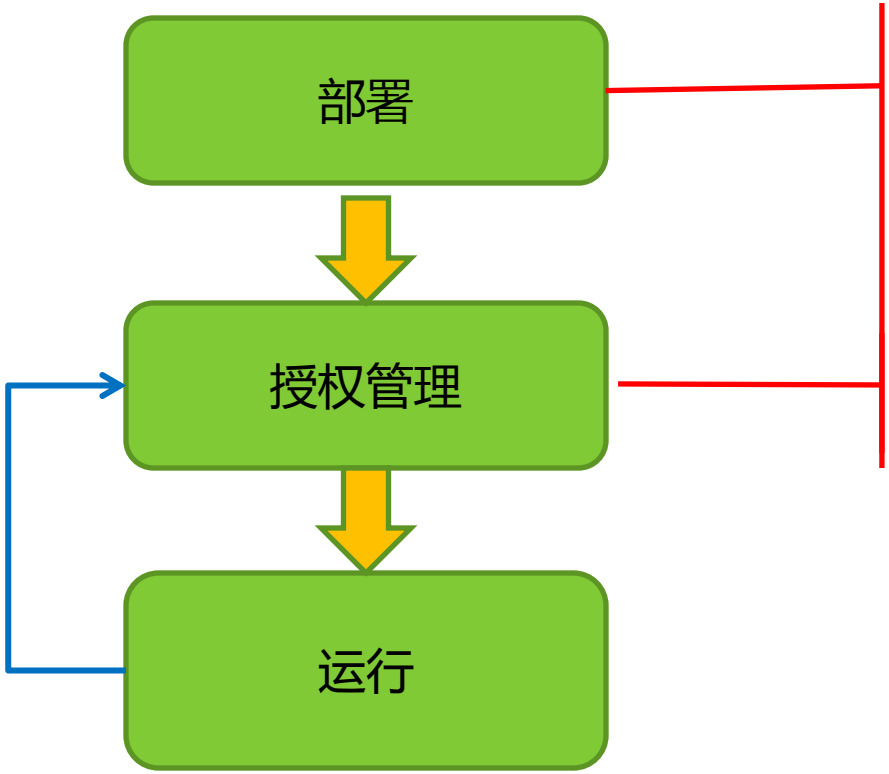
应用实例——系统建设

为开发人员提供RBAC系统功能、模块和接口的严格定义，保证不同RBAC系统的互操作性



应用实例——运行管理

帮助管理员抽取角色和权限、分配角色权限、分析权限分配潜在的风险



通过规范定义的管理功能接口学习管理方法，可以在不同的产品保持使用习惯

使用RBAC模型定义验证角色权限抽取是否合理，是否存在冲突

应用实例——维护更新

保证RBAC组件接口一致性和互操作性，降低投入和管理负担

现有RBAC系统功能升级

减少重复支出 只需要购买所需层次的RBAC功能实现，即可增加新功能，避免重复投入

降低管理 现有的配置和管理模式不用改变，减少管理负担

增加新信息系统

无缝结合

不同企业的产品通过一致的接口使用RBAC系统，不需要重复购买，同时也不需要重新配置授权信息

请批评指正

谢谢