

SAP 技术丛书

萨斯喀-亚历山大·拜尔  
(Sascha-Alexander Beyer) 等著  
陈跃东 译



SAP

权限系统

SAP Authorization System

東方出版社

SAP PRESS

SAP 技术丛书

# SAP

## 权限系统

SAP Authorization System

萨斯喀-亚历山大·拜尔  
(Sascha-Alexander Beyer) 等著  
陈跃东 译

東方出版社

SAP

PRESS

著作权合同登记号  
图字：01—2005—5389

责任编辑：任 合  
装帧设计：博克教育  
版式设计：博克教育

### 图书在版编目 (CIP) 数据

SAP 权限系统/ (德) 萨斯喀-亚历山大·拜尔等著; 陈跃东译

—北京: 东方出版社, 2006. 3

ISBN 7-5060-2478-0

I. S... II. ①拜... ②陈... III. 企业管理-应用软件, SAP R/3 IV. F270.7

中国版本图书馆 CIP 数据核字 (2006) 第 021001 号

## SAP 权限系统

### SAP QUANXIAN XITONG

(德) 萨斯喀-亚历山大·拜尔 等 著  
陈跃东 译

---

出版发行 东方出版社

地 址 北京朝阳门内大街 166 号 邮政编码 100706

电 话 (010)65250042 65289539 (人民东方图书销售中心)

网 址 <http://www.peoplepress.net>

经 销 新华书店

印 刷 中煤涿州制图印刷厂印刷

开 本 787 毫米×1092 毫米 1/16 版 次 2006 年 3 月第 1 版

印 张 18 印 次 2006 年 3 月第 1 次印刷

字 数 450 千字 定 价 49.00 元

---

版权所有 侵权必究 印装差错 负责调换

## 主要作者简介:

萨斯喀-亚历山大·拜尔(Sascha-Alexander Beyer)网络安全专家,在应用程序安全方面尤为擅长。

黑尔格·赫尔曼·菲舍尔(Helge Hermann Fischer)在安全咨询领域有着丰富的国际操作经验,并获得了BS7799主任审核员(Lead Auditor)证书。

格雷戈里·古列梅蒂(Gregory Guglielmetti)精通的领域包括:SAP R/3权限概念技术实施、开发审计方法和工具以及大型SAP项目之中的权限概念的质量保证。他在软件开发方面也具有多年的经验。

他们都是IBM业务咨询服务事业部(原普华永道咨询公司,Pwconsulting)的同事,共同研究“业务和信息安全”技术。

## 新书推荐 **100**小时学会 SAP

《100小时学会SAP》学习系统是由SAP中国支持,北京博克教育公司开发的在线学习系统。它主要基于互联网,使学员在网上完成其主要的学习和训练活动,并且自我管理学习计划。《100小时学会SAP》的内容覆盖mySAP ERP的五大核心模块:FI(财务会计)、CO(管理会计)、MM(物料管理)、PP(生产计划)和SD(销售和分销)以及部分BASIS。《100小时学会SAP》是SAP中国的一项创新,它完全基于中文环境,使SAP的用户和爱好者们能在任何时间、任何地点轻松地学习SAP。



# 前    言

由于公司的业务处理主要由信息技术(IT)予以支持,所以 IT 系统越成熟,对人们工作生活的影响就越大。因此,各大公司正不断地修改自己已建立好的流程和组织,进而修改其 IT 系统。当它们将 SAP R/3 作为标准软件予以配置时,对业务处理、组织以及 IT 系统的更改均必须建立相应的模型。这些更改总是在影响着 SAP R/3 的权限概念,若无已定义的结构化流程,则大多数公司将会面临无法发展或不可维护的复杂局面。有些公司拥有数千个 SAP R/3 用户且拥有全球性的组织结构,在这些公司之中,企业基础结构的更改有时可能会让人畏缩,因为有时这一任务可能需要一些耗时的项目,这些项目有时甚至要花费几年的时间,在这段时间之内,项目小组除了正确处理 SAP 技术知识之外,还必须鼓励并论证在业务处理之中的专家以及所涉及组织的意见。

为了帮助您通过结构化架构开始学习 SAP R/3 权限概念,我们将在本书之中与您一同分享从无数咨询项目之中总结出来的经验和方法。关于顾客经常咨询的问题,还将为您提供许多技巧和答案,您会觉得这些内容有助于在对流程、组织和版本进行更改之后对现有 SAP R/3 权限概念进行修订。因为正如我们所说明的那样,IT 领域不断发展变化,所以我们将专门用一章的篇幅来论述 SAP 的新发展和 SAP 企业门户。

一个简短的告诫是:尽管我们采用了标准软件,但 SAP R/3 的安装却各不相同。个人定制的设置、版本以及更新级别均可在 SAP R/3 权限系统之中产生不同结果。因此请注意:本书主要以 SAP R/3 4.6 版为基础。

只有那些积极投身到 SAP R/3 权限系统之中的人才可写出这类书籍。

此书是 IBM 德国业务咨询服务事业部 (IBM Business Consulting Services GmbH) 同仁集体智慧的结晶, 他们除了日复一日地与我们的顾客商议活动之外, 还一直在不知疲倦地为我们提供建议。因此, 我们想借此机会感谢那些为此书呕心沥血的每一位同仁, 尤其要感谢: 尤温·普罗布斯特 (Uwe Probst), 米佳娜·凯尔曼-马基 (Mirjana Kelderman-Matkic), 马赛厄斯·赫斯勒 (Matthias Hessler), 克劳斯·杰克 (Klaus Jäck), 亨德里克·哈杰 (Hendrik Hartje), 赫尔格·赫尔曼·费希尔 (Helge Hermann Fischer), 萨斯喀-亚历山大·拜尔 (Sascha-Alexander Beyer) 和格雷戈里·古列梅蒂 (Gregory Guglielmetti)。另外, 我们还要感谢 IBM 市场部的大力支持, 尤其要感谢市场部的安德烈·赫夫曼 (Andrea Hoffmann), 贾塔·雅各比 (Jutta Jacobi) 以及罗莎琳德·托德 (Roselinde Todt) 的鼎力相助。最后, 我们还要感谢德国 Galileo 出版社 (Galileo Press), 他们经常提供一些建设性协助, 对于此书的成功出版, 他们功不可没, 如果没有他们的大力支持, 这本 SAP Press 的书将不可能面世。我们在此特别感谢威伯特·休伯讷 (Wiebke Hübner) 女士、弗洛里安·齐姆尼亚特 (Florian Zimniak) 先生、米歇尔·科特曼 (Michelle Kottemann) 女士、里贾纳·布朗特拉克 (Regina Brautlacht) 女士以及托马斯·韦尔伦 (Tomas Wehren) 先生。

“感恩不仅是伟大品德之一, 而且也是其他所有美德之源。”

——马尔库斯·图利乌斯·西塞罗 (Marcus Tullius Cicero, 公元前 106—43 年), 古罗马演说家和作家

安德烈斯·布林克曼 (Andreas Brinkmann), 总裁  
andreas.brinkmann@de.ibm.com

卡斯滕·希谢尔博士 (Dr. Carsten Schinschel), 副总裁  
carsten.schinschel@de.ibm.com  
IBM 业务咨询服务事业部

2003 年 8 月, 写于柏林和杜塞尔多夫



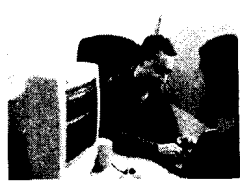
# SAP 目 录

第 1 章 介绍 .....	1
1.1 本书的关注点 .....	1
1.1.1 各章简介 .....	2
1.1.2 目标集团 .....	3
1.1.3 本书重点 .....	5
1.2 SAP R/3 环境 .....	5
1.2.1 SAP R/3 安全 .....	6
1.2.2 IT 基础结构 .....	7
1.2.3 安全方面和基础结构的集成 .....	9
1.2.4 Web 结构的进一步发展(Internet 事务服务器) .....	11
1.2.5 mySAP 工作台/SAP 企业门户 .....	12
1.3 复杂的系统架构 .....	14
1.4 总结 .....	17
第 2 章 SAP R/3 用户和权限 .....	19
2.1 初步评论——SAP R/3 系统中的安全 .....	19
2.1.1 风险 .....	20



2.1.2	目标	20
2.1.3	费用	21
2.1.4	益处	21
2.1.5	环境	21
2.2	SAP R/3 用户	22
2.2.1	用户主记录	22
2.2.2	用户组	27
2.2.3	用户类型	28
2.2.4	密码规则	28
2.2.5	SAP R/3 标准用户	31
2.2.6	与用户主记录相关的 SAP 表格	32
2.3	SAP R/3 权限概念	33
2.3.1	参数文件生成器	34
2.3.2	事务、权限对象以及权限	35
2.3.3	企业结构和组织级别	39
2.3.4	角色	40
2.3.5	权限参数文件	42
2.3.6	技术流程——SAP 参数文件生成器	44
2.3.7	命名惯例	48
2.3.8	与权限和角色相关的 SAP 表	49
2.3.9	划分管理职责	51
2.4	系统缺省设置	52
2.4.1	实例和技术参数文件	54
2.4.2	将 SAP 建议转移到客户表	55
2.5	SAP 应用程序中的权限检查	58
2.6	保护表	63
2.7	保护报表	67
2.7.1	ABAP/4 程序	67
2.7.2	保护程序	67
2.7.3	使用客户开发事务	69





# 目 录

2.8 基础安全 .....	69
2.8.1 初步评论 .....	69
2.8.2 受影响的基础权限 .....	69
2.9 人力资源安全 .....	74
2.9.1 权限对象——权限主开关 .....	75
2.9.2 个人编号检查 .....	77
2.9.3 额外的主数据检查 .....	79
2.9.4 结构权限 .....	79
2.9.5 您可激活的更多权限检查 .....	82
2.9.6 总结 .....	83
2.10 4.6 版的新特征 .....	84
2.11 集中用户管理以及全局用户管理员 .....	86
2.11.1 集中用户管理 .....	86
2.11.2 全局用户管理员 .....	88
2.12 SAP 技术在权限范围内的历史 .....	88
2.12.1 背景 .....	88
2.12.2 面向对象的概念 .....	89
2.12.3 含有 S_TCODE 的面向对象的概念 .....	89
2.12.4 迁移和迁移工具 .....	90
2.13 汇总与总结 .....	91
2.13.1 系统访问保护 .....	91
2.13.2 用户管理 .....	92
2.13.3 权限概念 .....	92
2.13.4 访问保护系统的文档 .....	94
2.13.5 保持期间 .....	94
2.14 权限范围中重要的 SAP 注释 .....	94
第 3 章 内部控制系统中的嵌入 .....	95
3.1 内部控制系统的必要性 .....	96
3.1.1 确定风险环境 .....	98



3.1.2	识别风险源(流程、范围等)	101
3.1.3	风险分析	102
3.2	传输到控制环境	104
3.2.1	控制环境的结构	105
3.2.2	控制环境的要求	106
3.2.3	控制类别	108
3.2.4	控制类型	109
3.3	确定实施	111
3.3.1	SAP R/3 权限概念	111
3.3.2	实施——限制	112
3.3.3	补偿控制	113
3.3.4	权限控制的分类	114
3.3.5	控制归档	114
3.4	监控以及审计内部控制系统	114
3.4.1	内部审计	114
3.4.2	外部审计	115
3.4.3	企业的意识	115
第4章	设计权限概念的程序模型	117
4.1	IBM 的阶段模型	117
4.1.1	简介	117
4.1.2	项目准备以及框架条件	118
4.1.3	定义企业之中的功能(角色)	119
4.1.4	粗略设计——创建任务/功能矩阵	120
4.1.5	详细的设计概念——创建组织/值矩阵	124
4.1.6	实施——创建单角色和参数文件	126
4.1.7	实施——创建复合角色	126
4.1.8	测试、归档和检查	127
4.1.9	配置用户主记录	127
4.1.10	定义支持概念	127



# 目 录

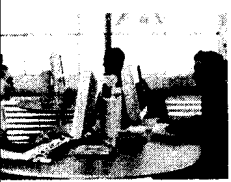
4.1.11	上线准备——知识传递与培训 .....	127
4.1.12	展开支持和上线支持 .....	128
4.1.13	监控和检查 .....	128
4.2	涉及各方 .....	128
4.2.1	概述 .....	128
4.2.2	指导委员会 .....	130
4.2.3	项目管理 .....	130
4.2.4	审计员 .....	131
4.2.5	模块专家和流程专家 .....	131
4.2.6	来自用户部门的联系人 .....	131
4.2.7	用户和权限管理 .....	132
4.3	详细介绍一些重要方面 .....	132
4.3.1	11条基本规则 .....	132
4.3.2	框架条件 .....	134
4.3.3	SAP 权限概念的详细程度 .....	136
4.3.4	权限角色归档 .....	137
4.3.5	模板方案 .....	140
4.3.6	命名惯例 .....	143
4.4	工作范围的定义 .....	149
4.4.1	定义使用的 SAP 功能范围 .....	149
4.4.2	定义企业中角色的程序 .....	149
第 5 章	实施权限概念的过程模型 .....	157
5.1	概述 .....	157
5.2	实施 .....	158
5.2.1	参数文件生成器——概述 .....	158
5.2.2	初始化参数文件生成器 .....	162
5.2.3	SAP 提供的角色 .....	165
5.2.4	用户菜单 .....	165
5.2.5	生成权限 .....	167



5.2.6	复制角色和继承功能 .....	170
5.2.7	复合角色 .....	172
5.3	测试已实施角色 .....	173
5.3.1	要求 .....	173
5.3.2	单元测试 .....	174
5.3.3	角色集成测试 .....	174
5.3.4	用户接受测试 .....	175
5.3.5	最后检查 .....	175
5.3.6	角色测试的技术实施 .....	175
5.3.7	手工维护权限数据 .....	178
5.4	配置用户主记录 .....	181
5.5	上线 .....	182
5.6	日常操作 .....	183
5.6.1	生产系统中的权限概念 .....	183
5.6.2	用户管理和角色管理 .....	184
5.6.3	更改请求程序 .....	186
5.7	紧急事件概念 .....	189
5.7.1	背景 .....	189
5.7.2	多级的紧急事件概念 .....	189
5.7.3	请求和登录的流程和处理 .....	190
5.8	技术细节 .....	190
5.8.1	“权限”信息系统 .....	191
5.8.2	减少权限检查的范围 .....	191
5.8.3	SAP_ALL 和 SAP_NEW .....	192
第 6 章	SAP R/3 权限概念的审计 .....	195
6.1	用户信息系统 .....	196
6.1.1	结构 .....	196
6.1.2	总结 .....	199
6.2	审计信息系统 .....	199

# 目 录

6.2.1	历史 .....	199
6.2.2	审计途径 .....	199
6.2.3	结构 .....	200
6.2.4	系统审计 .....	203
6.2.5	审计信息系统子树“用户管理” .....	206
6.2.6	审计信息系统的权限 .....	208
6.2.7	审计信息系统角色概念 .....	209
6.2.8	审计权限概念的权限 .....	211
6.2.9	数据收集和评估技巧 .....	212
6.2.10	总结 .....	214
6.2.11	关于审计信息系统的更多信息 .....	215
6.3	直接表存取 .....	215
6.4	补充审计范围 .....	215
6.5	其他审计工具 .....	216
6.5.1	SAP 审计——CheckAud(检查审计) .....	217
6.5.2	ACE .....	218
6.5.3	APM .....	219
6.5.4	更多工具 .....	220
6.5.5	总结 .....	221
第 7 章	SAP 企业门户 .....	223
7.1	一般方面 .....	223
7.2	门户组件 .....	225
7.2.1	Web 服务器 .....	226
7.2.2	应用服务器 .....	226
7.2.3	运行和开发环境 .....	226
7.2.4	目录服务 .....	226
7.2.5	数据库 .....	227
7.2.6	搜索引擎 .....	227
7.3	门户和 SAP R/3 之间的交互 .....	227



7.3.1	拖放/关联 .....	229
7.4	访问控制和管理 .....	230
7.4.1	识别和鉴别 .....	231
7.4.2	用户管理 .....	233
7.4.3	角色 .....	235
7.4.4	个性化 .....	236
7.4.5	同步 .....	236
7.4.6	单点登录 .....	237
7.5	其他安全控制 .....	241
7.5.1	要求 .....	241
7.5.2	风险 .....	241
7.5.3	物理安全 .....	243
7.5.4	组织安全 .....	244
7.5.5	安装更新 .....	244
7.5.6	防病毒软件 .....	244
7.5.7	互联网的安全周长 .....	245
7.5.8	入侵检测系统 .....	245
7.5.9	加密和完整校验 .....	245
7.5.10	安全操作系统配置 .....	246
7.5.11	总结 .....	246
第8章	未来发展和方法 .....	249
8.1	引言 .....	249
8.1.1	访问企业目录(轻量级目录访问协议) .....	250
8.1.2	集中用户管理 .....	252
8.1.3	权限和角色管理(SAP Web 应用服务器) .....	252
8.1.4	用户鉴别 .....	254
8.2	相关事宜 .....	255
8.2.1	其他事务 .....	256
8.3	现状 .....	257



# 目 录

附录 A 权限对象 .....	259
附录 B SAP 注释 .....	265
附录 C 关于作者 .....	271



# SAP 介绍

# 1

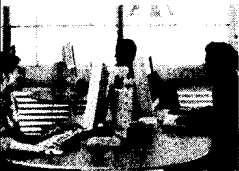
信息是企业最有价值的资产之一，这一观点已被普遍接受。如今，各大企业对建立全面有效的安全机制的呼声越来越高，对系统管理和监控日常操作的呼声也是一浪高过一浪。尽管 SAP R/3 权限系统是企业安全策略之中一个必不可少的关键因素，但它也仅仅是其中的一个组件而已。

## 1.1 本书的关注点

由于业务处理和流程(既包括企业内部的，又包括企业与企业之间的业务处理和流程)日趋复杂，所以建立一个安全程序尤为重要，这一安全程序可对企业数据进行处理，预防误用。对于系统访问而言，特别是对于企业资源规划系统(ERP 系统，例如 SAP R/3)而言，数据保护的一个前提便是具有适当的系统访问结构。

在本书之中，我们将为您解决与 SAP R/3 权限概念实施有关的问题。并总结了已实施项目的实践经验，向您展示如何设计 SAP R/3 权限概念，该权限概念可帮助您达到数据安全这一企业目标。还要特别向您讲述





SAP R/3 权限概念的开发如何支持该系统的有效实施。

然而，请您注意：此书不应被视为是一本完整的权限概念方面的书籍。相反，我们希望此书能成为您考虑权限概念方面的一个目录。权限概念的发展和实施是为每家企业定制的解决方案，它以指定方法和数个基本规则为特征的。在 SAP R/3 权限概念的计划制定和实施期间，您应予以考虑的驱动因素包括：

- ▶ 降低商务风险；
- ▶ 在 SAP R/3 之中对信息安全的企业及法定要求；
- ▶ 保持数据的完整性，使之避免受到任意或恶意的操纵或损坏，或使之避免无意识的误用；
- ▶ 确保企业内部信息的保密性；
- ▶ 配备 SAP R/3 实施所需的专家，但目前企业内部所需的 SAP R/3 专家仍未配备；
- ▶ 管理任务的成本功效，尤其是在权限组织之中管理任务的成本功效；
- ▶ 确保对这些概念的管理会促进易用性；
- ▶ 对于已计划好的扩展（例如购置或重组）而言，权限概念的可扩展性。

此清单仅列出少量需要考虑的必要因素；您将在以下各章中看到关于潜在影响及其他事项的更多详细描述。

### 1.1.1 各章简介

以下对本书各章的简介旨在帮助您快速容易地寻找您所需要的关键信息。

**第 1 章** 概括性地讲述了影响 R/3 权限概念实施的因素以及可能产生的后果。另外，本章还讨论了 SAP R/3 系统的特殊安全和关于 IT 基础结构的基础。

**第 2 章** 主要面向 SAP R/3 的新用户，向其介绍技术基础、结构、SAP R/3 权限管理的细节并对以上各项内容予以汇总。本章除了对 R/3 用户、权限对象、单角色以及复合角色予以定义之外，还简单地介绍了如何使用 SAP R/3 参数文件生成器。