GB

2008年 修订-87

中 国 国 家 标 准 汇 编

2008 年修订-87

中国标准出版社　编

中 国 标 准 出 版 社

北　京

图书在版编目（CIP）数据

中国国家标准汇编：2008年修订.87/中国标准出版社编.—北京：中国标准出版社，2009

ISBN 978-7-5066-5582-8

Ⅰ.中… Ⅱ.中… Ⅲ.国家标准-汇编-中国-2008

Ⅳ.T-652.1

中国版本图书馆CIP数据核字（2009）第203973号

中国标准出版社出版发行

北京复兴门外三里河北街16号

邮政编码：100045

网址 www.spc.net.cn

电话：68523946 68517548

中国标准出版社秦皇岛印刷厂印刷

各地新华书店经销

*

开本 880×1230 1/16 印张 35.5 字数 1 086千字

2009年12月第一版 2009年12月第一次印刷

*

定价 200.00 元

ISBN 978-7-5066-5582-8

9 787506 655828 >

978-7-5066-5582-8

出 版 说 明

1.《中国国家标准汇编》是一部大型综合性国家标准全集。自1983年起，按国家标准顺序号以精装本、平装本两种装帧形式陆续分册汇编出版。它在一定程度上反映了我国建国以来标准化事业发展的基本情况和主要成就，是各级标准化管理机构，工矿企事业单位，农林牧副渔系统，科研、设计、教学等部门必不可少的工具书。

2.《中国国家标准汇编》收入我国每年正式发布的全部国家标准，分为“制定”卷和“修订”卷两种编辑版本。

“制定”卷收入上年度我国发布的、新制定的国家标准，顺延前年度标准编号分成若干分册，封面和书脊上注明“20××年制定”字样及分册号，分册号一直连续。各分册中的标准是按照标准编号顺序连续排列的，如有标准顺序号缺号的，除特殊情况注明外，暂为空号。

“修订”卷收入上年度我国发布的、被修订的国家标准，视篇幅分设若干分册，但与“制定”卷分册号无关联，仅在封面和书脊上注明“20××年修订-1，-2，-3，……”字样。“修订”卷各分册中的标准，仍按标准编号顺序排列（但不连续）；如有遗漏的，均在当年最后一分册中补齐。需提请读者注意的是，个别非顺延前年度标准编号的新制定的国家标准没有收入在“制定”卷中，而是收入在“修订”卷中。

读者配套购买《中国国家标准汇编》“制定”卷和“修订”卷则可收齐上一年度我国制定和修订的全部国家标准。

3. 由于读者需求的变化，自1996年起，《中国国家标准汇编》仅出版精装本。

4. 2008年制修订国家标准共5946项。本分册为“2008年修订-87”，收入新制修订的国家标准4项。

中国标准出版社

2009年10月

目　　录

ICS 35.100.70
L 79

中华人民共和国国家标准

GB/T 16264.2—2008/ISO/IEC 9594-2:2005
代替 GB/T 16264.2—1996

信息技术 开放系统互连 目录 第2部分:模型

Information technology—Open Systems Interconnection—The Directory—Part 2:Models

(ISO/IEC 9594-2:2005 Information technology—Open Systems Interconnection—The Directory:Models,IDT)

2008-08-06 发布　　2009-01-01 实施

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会　发布

前　言

GB/T 16264《信息技术　开放系统互连　目录》包括以下10个部分：

——第1部分：概念、模型和服务的概述；

——第2部分：模型；

——第3部分：抽象服务定义；

——第4部分：分布式操作规程；

——第5部分：协议规范；

——第6部分：选定的属性类型；

——第7部分：选定的客体类；

——第8部分：公钥和属性证书框架；

——第9部分：复制(待发布)；

——第10部分：公用目录管理机构的系统管理用法(待发布)。

本部分是GB/T 16264的第2部分。

本部分等同采用ISO/IEC 9594-2:2005《信息技术　开放系统互连　目录　模型》，仅有编辑性修改。

本部分代替GB/T 16264.2—1996。

本部分与GB/T 16264.2—1996的差异在于增加了下列各项内容：

——目录管理模型；

——目录管理和操作信息模型；

——目录模式；

——目录服务管理；

——DSA模型；

——DSA信息模型；

——DSA操作框架；

——扩充了GB/T 16264.2—1996中各章条内容。

本部分的附录A～附录H是规范性附录，附录I～附录T是资料性附录。

本部分由中华人民共和国信息产业部提出。

本部分由全国信息技术标准化技术委员会归口。

本部分起草单位：中国电子技术标准化研究所。

本部分主要起草人：徐冬梅、冯惠、张翠、胡顺。

本部分于1996年首次发布，本次为第一次修订。

引　言

GB/T 16264 的本部分连同本标准其他部分是为方便信息处理系统之间的互连以提供目录服务而制定的。所有这些系统的集合，连同它们所拥有的目录信息可被视为一个整体，被称为“目录”。目录所拥有的信息，总称为目录信息库(DIB)，典型地被用于方便客体之间的通信、与客体的通信或有关客体的通信等，这些客体如应用实体、个人、终端和分布列表等。

目录在开放系统互连中扮演了重要角色，其目标是，在它们自身的互连标准之外做最少的技术约定的情况下，允许下述各种信息处理系统之间的互连：

——来自不同生产厂商；

——具有不同的管理；

——具有不同的复杂程度，以及

——有不同的年代。

本部分为目录提供一组不同的模型，作为其他部分参考的框架。这些模型包括总体(功能)模型、管理机构模型、提供关于目录信息的目录用户和管理用户视图的通用目录信息模型、通用目录系统代理(DSA)和 DSA 信息模型以及操作框架和安全模型。

例如，通用目录信息模型描述了客体的相关信息如何分组，形成该客体的目录条目以及那些信息如何为客体提供名(称)。

通用 DSA 和 DSA 信息模型以及操作框架为目录的分布提供了支持。

本部分提供了通用目录信息模型的专门化以支持对目录模式的管理。

本部分提供了一些基础框架，在此框架基础上，其他标准化组织和业界论坛可以定义工业配置集。在这些框架中定义为可选的许多特性，可通过配置集的说明，在某种环境下作为必选特性来使用。目前 ISO/IEC 9594 的第 5 版是原有国际标准第 4 版的修订和增强，但不是替代。在系统实现时仍可以声明为符合第 4 版。然而，在某些方面，将不再支持第 4 版(即不再消除一些报告上来的错误)。建议在系统实现时尽快符合第 5 版。

第 5 版详细定义了目录协议的第 1 版和第 2 版。

第 1 版和第 2 版仅定义了协议第 1 版。本版本(第 5 版)中定义的许多服务和协议被设计为可运行在第 1 版下。然而，一些增强的服务和协议，如署名错误，只有包含在操作中的所有的目录条目都协商支持协议第 2 版时才可运行。无论协商的是哪一版，第 5 版中所定义的服务之间的差异和协议之间的差异，除了那些特别分配给第 2 版的外，都可以使用 GB/T 16264.5—2008 中定义的扩展规则调节。

本部分使用术语“第 1 版系统”来指遵循国际标准第 1 版的所有系统，即 ISO/IEC 9594:1990 版本；本部分使用术语“第 2 版系统”来指遵循国际标准第 2 版本的所有系统，即 ISO/IEC 9594:1995 版本；本部分使用术语“第 3 版系统”来指遵循国际标准第 3 版的所有系统，即 ISO/IEC 9594:1998 版本；本部分使用术语“第 4 版系统”来指遵循国际标准第 4 版的所有系统，即 ISO/IEC 9594:2001 版本的第 1 部分到第 10 部分；本部分使用术语“第 5 版系统”来指遵循国际标准第 5 版的所有系统，即 ISO/IEC 9594:2005 版本。

GB/T 16264—1996 是参照 ISO/IEC 9594:1990 而制定的。我国没有制定与国际标准第 2 版、第 3 版、第 4 版对应的国家标准。本部分提到的版本号是指国际标准的版本号。

附录 A 是规范性附录，总结了本标准中 ASN.1 客体标识符的用法。

附录 B 是规范性附录，提供了 ASN.1 模块。

附录 C 是规范性附录，提供了子模式管理模式的 ASN.1 定义。

附录 D 是规范性附录，提供了服务管理的 ASN.1 模块定义。

附录 E 是规范性附录，提供了基本访问控制的 ASN.1 模块定义。

附录 F 是规范性附录，提供了一个 ASN.1 模块定义，该模块中包含了所有与 DSA 操作属性类型相关的定义。

附录 G 是规范性附录，提供了一个 ASN.1 模块定义，该模块中包含了与操作绑定管理操作相关的所有定义。

附录 H 是规范性附录，提供了一个 ASN.1 模块定义，该模块中包含了与增强的安全相关的所有定义。

附录 I 是资料性附录，对与树型结构相关的数学术语进行了概述。

附录 J 是资料性附录，描述了在设计名(称)时可以考虑的一些准则。

附录 K 是资料性附录，对模式的不同方面提供了一些示例。

附录 L 是资料性附录，提供了与基本访问控制许可相关的语义方面的概述。

附录 M 是资料性附录，提供了基本访问控制用法的一个扩展示例。

附录 N 是资料性附录，描述了一些 DSA 特定条目的组合。

附录 O 是资料性附录，提供了对知识建模的框架。

附录 P 是资料性附录，描述了一个名(称)是可替代辨别名还是主辨别名，它是否可以包括可替代值以及它是否可以包括上下文信息等的判断准则。

附录 Q 是资料性附录，描述了子过滤器的概念。

附录 R 是资料性附录，描述了如何对家族成员进行命名的建议和示例。

附录 S 是资料性附录，介绍了命名概念和相关的考虑。

附录 T 是资料性附录，以字母表顺序列出了本部分中定义的术语。

信息技术　开放系统互连　目录
第2部分:模型

第一篇:综述

1　范围

GB/T 16264的本部分中定义的模型为GB/T 16264的其他部分提供了一个概念框架和术语框架,这些部分规定了目录的各种特性。

功能模型和管理机构模型定义了目录进行功能分布和管理分布的方法。通用DSA和DSA信息模型以及操作框架也是为支持目录分布而提供的。

通用目录信息模型分别从目录用户和主管部门用户的角度描述了DIB的逻辑结构。事实上,但在这些模型中,目录是分布的而不是集中的,是不可见的。

本部分提供了通用目录信息模型的专门化以支持对目录模式的管理。

GB/T 16264—2008的其他部分使用了本部分中定义的概念,对通用信息和DSA模型进行专门化定义以提供特定的信息、特定的DSA和操作模型,用以支持特定的目录能力(如复制):

a) 目录提供的服务(在GB/T 16264.3—2008中定义)是根据信息框架的概念而描述的:这就允许所提供的服务在某种程度上独立于DIB的物理分布;

b) 规定了目录的分布式操作(在GB/T 16264.4—2008中定义),以此可以提供上述服务,并因此可以维护该逻辑信息结构,即使该DIB实际上是高度分布的;

c) 规定了目录的组成部分所提供的用以提高目录整体性能的复制能力(在ISO/IEC 9594-9中定义)。

安全模型为规范访问控制机制建立了一个框架。它为在DIT的特定部分内有效标识访问控制方案提供了一种机制,并且定义了三种灵活的、特定的访问控制方案,这些模式广泛适用于各种不同的应用以及使用风格。通过使用如密码和数字签名等机制,安全模型还为保护目录操作的保密性和完整性提供了一个框架,它使用了ISO/IEC 9594-8中定义的鉴别框架以及GB/T 18237.1—2000中定义的通用高层安全工具。

DSA模型为目录组件操作规范建立了一个框架,包括:

a) 目录功能模型描述了目录是如何表示为一个或多个组件(每个组件为一个DSA);

b) 目录分布模型描述了一些原则,按照这些原则,DIB条目和条目拷贝可以在DSA间分布;

c) DSA信息模型描述了目录用户以及DSA内存储的操作信息的结构;

d) DSA操作框架描述了为获得特定目标(例如影像),构造DSA之间特定合作形式定义的方法。

2　规范性引用文件

下列文件中的条款通过GB/T 16264的本部分的引用而成为本部分的条款。凡是注日期的引用文件,其随后所有的修改单(不包括勘误的内容)或修订版均不适用于本部分,然而,鼓励根据本部分达成协议的各方研究是否可使用这些文件的最新版本。凡是不注日期的引用文件,其最新版本适用于本部分。

GB/T 9387.1—1998　信息技术　开放系统互连　基本参考模型　第1部分:基本模型(idt ISO/IEC 7498-1:1994)

GB/T 9387.2—1995 信息处理系统 开放系统互连 基本参考模型 第2部分:安全体系结构(idt ISO 7498-2:1989)

GB/T 9387.3—1995 信息处理系统 开放系统互连 基本参考模型 第3部分:命名与编址(idt ISO 7498-3:1989)

GB/T 16262.1—2006 信息技术 抽象语法记法一(ASN.1) 第1部分:基本记法规范(ISO/IEC 8824-1:2002,IDT)

GB/T 16262.2—2006 信息技术 抽象语法记法一(ASN.1) 第2部分:信息客体规范(ISO/IEC 8824-2:2002,IDT)

GB/T 16262.3—2006 信息技术 抽象语法记法一(ASN.1) 第3部分:约束规范(ISO/IEC 8824-3:2002,IDT)

GB/T 16262.4—2006 信息技术 抽象语法记法一(ASN.1) 第4部分:ASN.1规范的参数化(ISO/IEC 8824-4:2002,IDT)

GB/T 16264.1—2008 信息技术 开放系统互连 目录 第1部分:概念、模型和服务的概述(ISO/IEC 9594-1:2005,IDT)

GB/T 16264.3—2008 信息技术 开放系统互连 目录 第3部分:抽象服务定义(ISO/IEC 9594-3:2005,IDT)

GB/T 16264.4—2008 信息技术 开放系统互连 目录 第4部分:分布式操作规程(ISO/IEC 9594-4:2005,IDT)

GB/T 16264.5—2008 信息技术 开放系统互连 目录 第5部分:协议规范(ISO/IEC 9594-5:2005,IDT)

GB/T 16264.6—2008 信息技术 开放系统互连 目录 第6部分:选定的属性类型(ISO/IEC 9594-6:2005,IDT)

GB/T 16264.7—2008 信息技术 开放系统互连 目录 第7部分:选定的客体类(ISO/IEC 9594-7:2005,IDT)

GB/T 17965—2000 信息技术 开放系统互连 高层安全模型(idt ISO/IEC 10745:1995)

GB/T 18237.1—2000 信息技术 开放系统互连 通用高层安全 第1部分:概述、模型和记法(idt ISO/IEC 11586-1:1996)

GB/T 18794.2—2002 信息技术 开放系统互连 开放系统安全框架 第2部分:鉴别框架(idt ISO/IEC 10181-2:1996)

GB/T 18794.3—2003 信息技术 开放系统互连 开放系统安全框架 第3部分:访问控制框架(ISO/IEC 10181-3:1996,IDT)

ISO/IEC 9594-8:2005 信息技术 开放系统互连 目录:公钥和属性证书框架

ISO/IEC 9594-9:2005 信息技术 开放系统互连 目录:复制

ISO/IEC 9594-10:2005 信息技术 开放系统互连 目录:公用目录管理机构的系统管理用法

ISO/IEC 9834-1:2005 信息技术 开放系统互连 OSI登记机构的操作规程:一般规程和ASN.1客体标识符树的顶级弧

ISO/IEC 10021-2 信息技术 消息处理系统(MHS):总体结构

ISO/IEC 10021-4:2003 信息技术 消息处理系统(MHS):消息传送系统 抽象服务定义和规程

CCITT 建议 X.800:1991 CCITT应用的开放系统互连安全体系结构

IETF RFC 3377:2002 轻量级目录访问协议(v3):技术规范

3 术语和定义

下列术语和定义适用于GB/T 16264的本部分。

3.1 通信定义

本部分使用 GB/T 16264.5 中定义的术语：

a) 应用实体 *application entity*；

b) 应用层 *application Layer*；

c) 应用进程 *application process*。

3.2 基本目录定义

本部分使用 GB/T 16264.1 中定义的术语：

a) 目录 *directory*；

b) 目录访问协议 *Directory Access Protocol*；

c) 目录信息库 *Directory Information Base*；

d) 目录操作绑定管理协议 *Directory Operational Binding Management Protocol*；

e) 目录系统协议 *Directory System Protocol*；

f) (目录)用户 *(Directory) user*。

3.3 分布式操作定义

本部分使用 GB/T 16264.4 中定义的术语：

a) 访问点 *access point*；

b) 分等级操作绑定 *hierarchical operational binding*；

c) 名(称)解析 *name resolution*；

d) 非特定分等级操作绑定 *non-specific hierarchical operational binding*；

e) 相关的分等级操作绑定 *relevant hierarchical operational binding*。

3.4 复制定义

下列术语在 ISO/IEC 9594-9 中定义：

a) 高速缓冲拷贝 *cache-copy*；

b) 使用者引用 *consumer reference*；

c) 条目拷贝 *entry-copy*；

d) 主 DSA *master DSA*；

e) 主影像 *primary shadowing*；

f) 复制区 *replicated area*；

g) 复制 *replication*；

h) 次影像 *secondary shadowing*；

i) 影像使用者 *shadow consumer*；

j) 影像提供者 *shadow supplier*；

k) 影像的 DSA 特定条目 *Shadowed DSA-Specific Entry*；

l) 影像 *shadowing*；

m) 提供者引用 *supplier reference*。

本部分定义的术语在每一章开头的适当位置。为便于参考，在本部分的附录 T 中提供了这些术语的索引。

4 缩略语

GB/T 16264 的本部分使用如下缩写词：

ACDF	访问控制决策功能	(Access Control Decision Function)
ACI	访问控制信息	(Access Control Information)
ACIA	访问控制内部区	(Access Control Inner Area)

ACSA	访问控制特定区	(Access Control Specific Area)
ADDMD	公共目录管理域	(Administration Directory Management Domain)
ASN.1	抽象语法记法一	(Abstract Syntax Notation One)
AVA	属性值断言	(Attribute Value Assertion)
BER	(ASN.1)基本编码规则	((ASN.1) Basic Encoding Rules)
DACD	目录访问控制域	(Directory Access Control Domain)
DAP	目录访问协议	(Directory Access Protoco)
DIB	目录信息库	(Directory Information Base)
DISP	目录信息影像协议	(Directory Information Shadowing Protocol)
DIT	目录信息树	(Directory Information Tree)
DMD	目录管理域	(Directory Management Domain)
DMO	域管理组织	(Domain Management Organization)
DOP	目录操作绑定管理协议	(Directory Operational Binding Management Protocol)
DSA	目录系统代理	(Directory System Agent)
DSE	DSA 特定条目	(DSA-Specific Entry)
DSP	目录系统协议	(Directory System Protocol)
DUA	目录用户代理	(Directory User Agent)
HOB	分等级操作绑定	(Hierarchical Operational Binding)
LDAP	轻量级目录访问协议	(Lightweight Directory Access Protocol)
NHOB	非特定分等级操作绑定	(Non-specific Hierarchical Operational Binding)
NSSR	非特定下级引用	(Non-Specific Subordinate Reference)
PRDMD	专用目录管理域	(Private Directory Management Domain)
RDN	相关可辨别名	(Relative Distinguished Name)
RHOB	相关的分等级操作绑定	(适当情况下,指 HOB 或 NHOB)
	(Relevant Hierarchical Operational Binding (a HOB or NHOB,as appropriate))	
SDSE	影像 DSE	(Shadowed DSE)

5 约定

术语“目录规范(或本目录规范)”指的是 GB/T 16264.2—2008。术语“系列目录规范”指的是 GB/T 16264 的所有部分。

本目录规范使用术语“第 1 版系统”来指遵循系列目录规范第 1 版的所有系统,即 1988 年版本的 CCITT X.500 系列建议书和 GB/T 16264—1996 版本。本目录规范使用术语“第 2 版系统”来指遵循系列目录规范第 2 版本的所有系统,即 1993 版本的 ITU-T X.500 系列建议书和 ISO/IEC 9594:1995 版本。本目录规范使用术语“第 3 版系统”来指遵循系列目录规范第 3 版的所有系统,即 1997 版本的 ITU-T X.500 系列建议书和 ISO/IEC 9594:1998 版本。本目录规范使用术语“第 4 版系统”来指遵循系列目录规范第 4 版的所有系统,即 ISO/IEC 9594:2001 年版本的第 1 到第 10 部分。

本目录规范使用术语“第 5 版系统”来指遵循系列目录规范第 5 版的所有系统,即 GB/T 16264—2008 版本的第 1 到第 7 部分以及 ISO/IEC 9594:2005 年版本的第 8 到第 10 部分。

本目录规范使用粗体字体来表示 ASN.1 符号。若在常规文本中要表示 ASN.1 的类型和值时,为了区别于常规文本,使用了粗体字表示。为了表示过程的语义而引用过程名时,为了区别于常规文本,使用了粗体字表示。访问控制许可使用斜体字表示。

第二篇:目录模型概述

6 目录模型

6.1 定义

本部分使用下列术语和定义:

6.1.1

公共管理机构 administrative authority

域管理组织的一个代理机构,负责目录管理的不同方面。

6.1.2

公共目录管理域 administration directory management domain;ADDMD

由管理部门管理的目录管理区(DMD)。

注:术语"管理"指公共远程通信管理部门或提供公共远程通信服务的组织。

6.1.3

目录管理和操作信息 directory administrative and operational information

出于目录管理和操作的目的而使用的信息。

6.1.4

DIT 域 DIT domain

由 DSA 所拥有的构成一个 DMD 的全球 DIT 的一部分。

6.1.5

目录管理域 directory management domain;DMD

由一个单独的组织所管理的一个或多个 DSA 以及零个或多个 DUA 的集合。

6.1.6

域管理组织 domain management organization

管理一个 DMD(以及相应的 DIT 域)的组织。

6.1.7

目录用户信息 directory user information

关于用户及其应用的感兴趣的信息。

6.1.8

目录系统代理 directory system agent;DSA

一个 OSI 应用进程,是目录的一个组成部分。

6.1.9

(目录)用户 (directory) user

目录的端用户,即访问目录的实体或人员。

6.1.10

目录用户代理 directory user agent;DUA

OSI 的一个应用进程,它在访问目录过程中代表某一个用户。

注:DUA 可能还会提供一个本地范围的便利工具以帮助用户构成请求并解释响应。

6.1.11

客户机 LDAP client LDAP

一个应用进程,表示通过轻量级目录访问协议(LDAP)来访问目录的用户。

6.1.12

LDAP 请求者 LDAP requestor

一个 DSA,能够通过轻量级目录访问协议(LDAP)来发起请求,并且能够理解和处理 LDAP 的

响应。

6.1.13

LDAP 响应者　LDAP responder

一个 DSA，能够理解并响应轻量级目录访问协议(LDAP)的请求。

6.1.14

LDAP 服务器　LDAP server

一个组成目录的应用进程，它拥有 DIB 的一部分，并且能够通过轻量级目录访问协议(LDAP)对请求进行响应。

6.1.15

专用目录管理域　private directory management domain；PRDMD

由公共主管部门之外的组织所管理的一个目录管理域(DMD)。

6.2　目录及其用户

目录是一个信息仓库，这个仓库被称为目录信息库(DIB)。为用户提供的目录服务实际上是关于对这些信息的各种方式的访问。

目录提供的服务在 GB/T 16264.3—2008 中定义。

一个目录用户(如一个人或一个应用进程)通过访问目录而获得目录服务。更准确地说，是一个目录用户代理(DUA)或一个轻量级目录访问协议(LDAP)的客户机代表每个用户去真正地访问目录，并与目录交互以获取其服务。目录提供一个或多个访问可进行的访问点。上述概念如图 1 所示。

DUA 表现为一个应用进程。在任何一个通信实例中，每个 DUA 都确切地代表一个目录用户。

目录表现为一个或多个应用进程的集合，这些应用进程被称为目录系统代理(DSA)和/或轻量级目录访问协议(LDAP)服务器，每个 DSA 或 LDAP 服务器都提供零个、一个或多个访问点。关于 DSA 的更详细描述，见 21.2。

注 1：一些开放系统可能会为实际用户(如应用进程或人员等)获取信息提供一个集中式的 DUA 功能。这个对目录来说是透明的。

注 2：DUA 功能和一个 DSA 可以处于同一个开放系统中，并且可以在实现时选择是否让一个或多个 DUA 在 OSI 环境中作为可视的应用实体。

注 3：一个 DUA 可以有本地特性和结构，这些不在本目录规范的定义范围之内。例如，一个表示目录人类用户的 DUA 可能会提供一个本地范围的便利工具来帮助它的用户构成请求并解释响应。

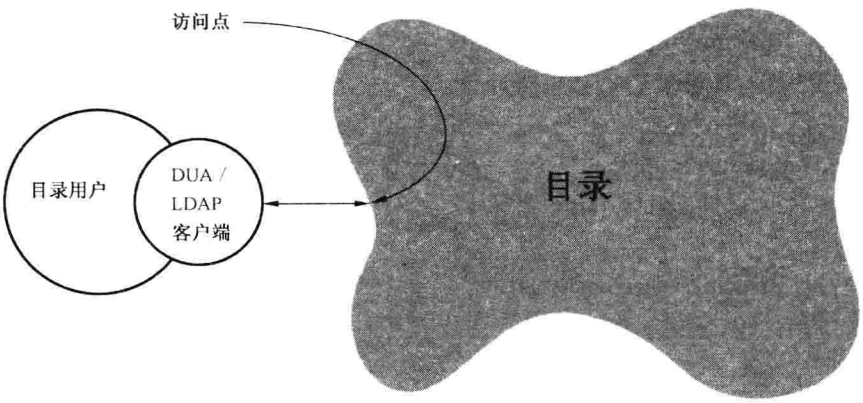

图 1　目录的访问

6.3　目录和 DSA 信息模型

6.3.1　通用模型

目录信息可能分成如下的类：

——用户信息：由用户置于目录内或者代表用户；随后被用户所管理或者代表用户。第 3 部分提供

了该信息的一个模型；或者

——管理和操作信息：由目录拥有，以适应各种不同的管理和操作需求。第5部分提供了该信息的一个模型。另外在第5部分还提供了一个关于用户信息模型、管理和操作信息模型之间关系的规范。

这些模型从不同方面表达了DIB视图，被认为是通用目录信息模型。

目录信息模型描述了目录作为一个整体如何来表示信息。作为一起操作的DSA集合的目录成分从该模型中得出。另一方面，DSA信息模型与DSA以及DSA应拥有的信息尤其相关，以使组成目录的DSA集合能够共同实现目录信息模型。DSA信息模型在本部分第22章到23章提供。

DSA信息模型是一个通用的模型，描述了DSA所拥有的信息以及这些信息与DIB和DIT之间的关系。

DSA信息模型所表示的一些信息可以通过目录抽象服务来访问，但不是全部信息。因此，如果对本系列目录规范中描述的全部信息都通过目录抽象服务来进行管理是不可能的。可以预见到的是，对DSA信息的管理最初应当是一个本地事物，但到最后应该会部署一些通用的系统管理服务来提供对DSA信息模型中描述的所有信息的访问。

6.3.2 特定的信息模型

对于作为整体的目录和它的组件，在通用模型制定以后，特定的信息模型需要对目录及其组件操作的特别方面进行标准化。

通用的目录信息模型为下述特定的信息模型建立了一个框架：

——访问控制信息模型；

——子模式信息模型；

——集合属性信息模型。

相应的，通用的DSA信息模型为下述特定的信息模型建立了一个框架：

——DSA分布知识的模型；

——DSA复制知识的模型。

6.4 目录管理机构模型

目录管理域(DMD)是由单个单独的组织所管理的一个或多个DSA以及零个或多个DUA的集合。

由(DSA组成的)目录管理域(DMD)所拥有的全球DIT的那部分被称为*DIT域*。在DMD和DIT域之间是一对一的对应关系。当提及对目录功能组件的管理时，使用术语“DMD”。当提及对目录信息的管理时，使用术语“DIT域”。与该术语相关的两个要点是：

——一个DIT域由一个或多个不相交的DIT子树组成(见11.5)。一个DIT域不得包含全球DIT的根；

——当管理的两个方面(目录功能组件管理和目录信息管理)放在一起考虑时，术语“DMD”作为一般术语使用。

管理某个DMD(以及关联的DIT域)的组织被称为一个*域管理组织(DMO)*。

注1：域管理组织可能是一个管理部门(即一个公共远程通信管理部门，或者其他提供公共远程通信服务的组织)，在这种情况下，被管理的DMD被称做公共目录管理域(ADDMD)；否则，它就是一个专用目录管理域(PRDMD)。应当认识到的是，关于ITU-T成员对专用目录系统的支持，这种指配属于国家法规的框架之内。因此，提供目录服务的主管部门可以提供所描述的技术可能性，也可不提供。专用目录管理域的内部操作和配置不在本目录规范的定义范围之内。

图2举例说明了DMO、DMD和DIT域之间的关系。

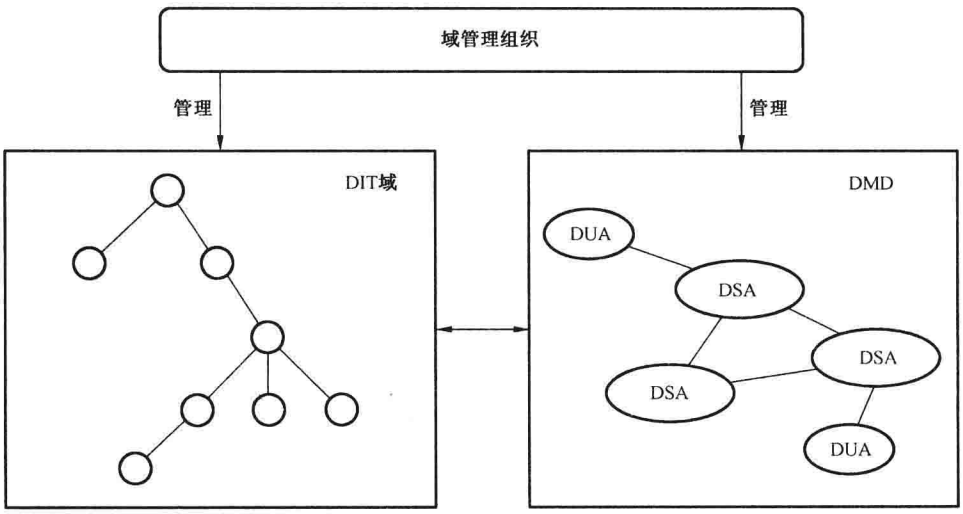

图 2　目录管理

由 DMO 对 DUA 进行管理意味着 DMO 对该 DUA 负有服务的责任，例如：维护，或在某些情况下被 DMO 拥有。DMO 可以选择或不选择使用本系列目录规范来管理 DMD 域内 DUA 和 DSA 之间的任何交互。

与目录管理的不同特性相关的域管理组织(DMO)的代理机构被称为*管理机构*。“管理权力”指的是由域管理组织授予某个管理机构的用以执行策略的权力。

注 2：目录管理机构模型在第四篇规定。

为便于引用，如在搜索规则中，可给 DMD 分配一个客体标识符(DMD-id)。

第三篇：目录用户信息模型

7　目录信息库

7.1　定义

本部分使用下列术语和定义：

7.1.1

别名条目　alias entry

一个包含用于为客体或者别名条目提供可替换名信息的“别名”类的项。

7.1.2

祖(条目)　ancestor

组成一个复合条目的家族成员所形成的层次结构中的根条目。

7.1.3

复合条目　compound entry

表示一个客体，该客体由家族成员组成，且这些家族成员分层次地组织起来形成一个或多个条目的家族。

7.1.4

派生条目　derived entry

在搜索结果中的条目信息，其包含的属性值是通过从一个或多个目录条目中获取的原始数据进行结合而得到的。