L 76

中华人民共和国国家标准

GB/T 16972.1—1997
idt ISO/IEC 10031-1:1991

信息技术　文本与办公系统　分布式办公应用模型　第1部分：一般模型

Information technology—Text and office systems—Distributed-office-applications-model—Part 1:General model

1997-09-02 发布　　1998-04-01 实施

国家技术监督局 发布

前　言

本标准等同采用国际标准ISO/IEC 10031-1:1991《信息技术　文本与办公系统　分布式办公应用模型　第1部分:一般模型》。

通过制定这项国家标准,以便在文本与办公系统中实现分布式办公应用。

GB/T 16972在《信息技术　文本与办公系统　分布式办公应用模型》总标题下,目前包括以下2个部分:

——第1部分:一般模型;

——第2部分:可辨别客体引用和相关规程。

本标准的附录A～附录K都是提示的附录。

本标准由中华人民共和国电子工业部提出。

本标准由电子工业部标准化研究所归口。

本标准起草单位:电子工业部标准化研究所。

本标准主要起草人:高健。

ISO/IEC 前言

ISO(国际标准化组织)和IEC(国际电工委员会)是世界性标准化专门机构。国家成员体(它们都是ISO或IEC的成员国)通过国际组织建立的各个技术委员会参与制定针对特定技术范围的国际标准。ISO和IEC的各技术委员会在共同感兴趣的领域内进行合作。与ISO和IEC有联系的其他官方和非官方国际组织也可参与国际标准的制定工作。

对于信息技术,ISO和IEC建立了一个联合技术委员会,即ISO/IEC JTC1。由联合技术委员会提出的国际标准草案需分发给国家成员体进行表决。发布一项国际标准,至少需要75%的参与表决的国家成员体投票赞成。

国际标准ISO/IEC 10031-1是由ISO/IEC JTC1"信息技术"联合技术委员会制定的。

ISO/IEC 10031在《信息技术　文本与办公系统　分布式办公应用模型》总标题下由下列部分组成:

——第1部分:一般模型

——第2部分:可辨别客体引用和相关规程

本标准中,附录A～附录K仅提供参考信息。

引　　言

开放系统互连标准允许应用的功能组件在网络里进行分布。一些应用进行分布是为减少花费，例如高速局域网(LAN)连接的办公系统，许多昂贵的资源可以共享。另外一些应用分布进行是由于管理或功能的原因，如世界范围的电子邮件系统。这些分布式应用例子的设计不同于传统的“单主机”考虑。通常，技术选项范围的扩大使在大量设计中考虑不同分布的花费和装载不同系统元素的计算成为可能，如在现代办公室的桌面终端设备和用户“在家中”的设备之间的联网。

本系列标准的目的是建立基于远程操作服务元素时分布式办公应用的一般框架。

GB/T 16972 是系列标准之一，它和开放系统互连的标准相关。开放系统互连标准是促进在不同种信息处理系统之间同种的互连。本系列标准在由 GB 9387 定义的开放系统互连协调标准的框架之内。

本系列标准特别着重规定互连兼容性所需的同种外部可见和可验证特征，同时避免对互连的信息处理系统不同种类内部设计和实现作不必要的限制和更改。它通过规定一个通用模型和一组设计原理来实现这个目的，这一模型和这些原理将保证不同的分布式办公应用以密切结合的方式共同发挥各自的作用。

本系列标准定义必要的公共框架，这一框架将使分布式办公应用能继续发展。另外，它也提供适用于分布式办公应用的概念和应用原理，将使之能够：

a) 模块化、简化和扩充相关产品的开发；

b) 实现不同供应商或服务提供者的服务；

c) 相互协作；

d) 优化开发花费。

为了使标准更有效，本系列标准面向于公认的需要。它具有模块扩充的能力，以涵盖在技术和需要上的未来发展。

尽管主要是用于分布式办公应用，本系列标准的内容也可用于其他信息处理环境。

中华人民共和国国家标准

信息技术　文本与办公系统　分布式办公应用模型　第1部分：一般模型

GB/T 16972.1—1997
idt ISO/IEC 10031-1:1991

Information technology—Text and office systems—Distributed-office-applications-model—Part 1:General model

1　范围

本系列标准为分布式办公应用(DOA)协议标准的开发提供框架。它适用于在各个有效物理距离内分布的应用，使它们就像紧密结合在一起的办公系统一样。

本系列标准描述了一种模型。标准化的分布式办公应用应使用它规定的原理。

本系列标准为允许访问不同应用和应用之间交互作用的协议设计提供指南。分布式应用协议位于OSI的应用层，同时符合ISO/IEC 9072定义的远程操作。

本系列标准包含这样一个目的：符合本系列标准一些部分的系统元素能通过不同的供应商和不同的服务提供者提供的设备来实现。

本系列标准并不定义在分布式应用中使用的人机接口。也不定义直接同用户交互的软件和特定应用软件之间的接口。

本系列标准的内容由两部分构成。

本标准描述了分布式办公应用的一般模型，它分成下列两部分：

a) 模型；

b) DOA协议设计指南。

本系列标准的第2部分描述由所有DOA使用的可辨别客体引用和相关规程。

本标准没有一致性要求。本系列标准的其他部分也许规定了那些部分的系统实现规程一致性要求。

2　引用标准

下列标准所包含的条文，通过在本标准中引用而构成为本标准的条文。本标准出版时，所示版本均为有效。所有标准都会被修订，使用本标准的各方应探讨使用下列标准最新版本的可能性。

GB 9387—88　信息处理系统　开放系统互连　基本参考模型(idt ISO 7498:1984)

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：命名和编址(idt ISO 7498—3:1989)

GB/T 15695—1995　信息处理系统　开放系统互连　面向连接的表示服务定义(idt ISO 8822:1988)

GB/T 16262—1996　信息处理系统　开放系统互连　抽象语法记法一(ASN.1)规范(idt ISO/

国家技术监督局1997-09-02批准　　1998-04-01实施

IEC 8824:1990)

GB/T 16264.2—1996 信息处理系统 开放系统互连 目录 第2部分:模型(idt ISO/IEC 9594-2:1990)

GB/T 16264.3—1996 信息处理系统 开放系统互连 目录 第3部分:抽象服务定义(idt ISO/IEC 9594-3:1990)

GB/T 16688—1996 信息处理系统 开放系统互连 联系控制服务元素服务定义(idt ISO 8649:1988)

GB/T 16284.2—1996 信息处理系统 文本通信 面向文本交换系统的信报(MOTIS) 第2部分:总体体系结构(idt ISO/IEC 10021-2:1990)

GB/T 16284.3—1996 信息处理系统 文本通信 面向文本交换系统的信报(MOTIS) 第3部分:抽象服务定义约定(idt ISO/IEC 10021-3:1990)

GB/T 16284.5—1996 信息处理系统 文本通信 面向文本交换系统的信报(MOTIS) 第5部分:信报存储:抽象服务定义(idt ISO/IEC 10021-5:1990)

GB/T 17174.1—1997 信息处理系统 文本通信 可靠传送 第1部分:模型和服务定义(idt ISO/IEC 9066-1:1989)

GB/T 17174.2—1997 信息处理系统 文本通信 可靠传送 第2部分:协议规范(idt ISO/IEC 9066-2:1989)

ISO/IEC 9072-1:1989 信息处理系统 文本通信 远程通信操作 第1部分:模型、记法及服务定义

ISO/IEC 9072-2:1989 信息处理系统 文本通信 远程通信操作 第2部分:协议规范

ISO 9735:1988 用于管理、商业和传输的电子数据交换 应用级语法规则

3 定义

3.1 OSI基本参考模型定义

本标准采用在GB 9387中定义的下列术语:

a) 应用层 Application Layer;

b) 应用实体 application-entity;

c) 应用服务元素 application-service-element;

d) 表示层 Presentation Layer;

e) 表示连接 presentation-connection;

f) 协议 protocol;

g) 服务定义 service definition。

3.2 OSI基本参考模型安全部分定义

本标准采用在GB 9387.2中定义的下列术语:

a) 鉴别 authentication;

b) 授权 authorization;

c) 凭证 credentials;

d) 安全策略 security policy。

3.3 联系控制服务元素(ACSE)定义

本标准采用在GB/T 16688中定义的下列术语:

a) 应用上下文 application context;

b) 联系控制服务元素 Association Control Service Element。

3.4 表示服务定义

本标准采用在GB/T 15695中定义的下列术语：

a）抽象语法 abstract syntax。

3.5 抽象语法记法定义

本标准采用在GB/T 16262中定义的下列术语：

a）抽象语法记法一 ASN.1；

b）外部类型 external type；

c）通用时间 Generalized Time；

d）宏 macro；

e）客体标识符 object identifier；

f）UTC时 UTC Time。

3.6 可靠传送服务元素(RTSE)定义

本标准采用在GB/T 17174中定义的下列术语：

a）可靠传送服务元素 Reliable Transfer Service Element。

3.7 远程操作服务元素(ROSE)定义

本标准采用在ISO/IEC 9072中定义的下列术语：

a）自变量 argument；

b）联编操作 bind-operation；

c）调用 invoke；

d）操作 operation；

e）执行 perform；

f）远程操作 Remote Operations；

g）远程操作服务元素 Remote Operations Service Element；

h）结果 result；

i）断联操作 unbind-operation。

3.8 目录定义

本标准采用在GB/T 16264中定义的下列术语：

a）属性 attribute；

b）属性宏 attribute macro；

c）属性类型 attribute type；

d）属性值 attribute value；

e）筛选器 filter。

3.9 EDIFACT定义

本标准采用在ISO 9735中定义的下列术语：

a）管理、贸易和传输的电子数据交换 EDIFACT。

3.10 面向文本交换系统的信报(MOTIS)定义

本标准采用在GB/T 16284.2中定义的下列术语：

a）正文部分 body part；

b）IP信报 IP-message；

c）信报 message。

3.11 抽象服务定义约定定义

本标准采用在GB/T 16284.3中定义的下列术语：

a）抽象模型 abstract model；

b）抽象操作 abstract operation；

c）抽象服务 abstract service；

d）抽象服务宏 abstract service macro；

e）非对称 asymmetric；

f）端口 port；

g）细化 refinement；

h）对称 symmertric。

3.12 分布式办公应用模型(DOAM)定义

本标准采用下列定义：

3.12.1 受访问者 accessee

一种 x 服务器，它能给客体指派可辨别客体引用(DOR)，该客体是通过来自 x 客户机的请求进行管理的，同时，它能通过由它指派的 DOR 来执行客体指明的操作。

3.12.2 访问者 accessor

一种 x 服务器，它能通过 DOR 和访问带有 DOR 的受访问者来执行指明客体的操作。

3.12.3 控制属性 control-attributes

当与安全主体的特权属性竞争时同安全客体联系的属性，用于授权或拒绝对安全客体的访问。

3.12.4 控制属性包 control-attribute-package

控制属性的集合。

3.12.5 消费操作 consume-operation

由 x 客户机调用给通过 DOR 指定客体的访问者的操作。

3.12.6 数据客体 data-object

表示数据的客体。

3.12.7 数据客体值 data-object-value

依照规则集派生自数据客体的值，或者在没有规则时整个客体的值。

3.12.8 直接值访问 direct-value-access

通过值而不是引用进行的数据客体访问。

3.12.9 直接值传送 direct-value-transfer

数据客体值的直接传送，而不是引用传送。

3.12.10 可辨别客体引用 distinguished-object-reference

在 DOA 环境中，对实客体的唯一引用。

3.12.11 分布式办公应用 distrbuted-office-application

分布在一个或多个开放系统上的信息处理资源集，它把功能性完好的定义集提供给用户(人)，协助一个给定的办公任务。

3.12.12 文件 document

预期人所直接或间接感知的一批结构化信息，借助办公应用，它能被交换、存储、检索和处理。

3.12.13 始发者 initiator

一种 x 客户机，它调用请求 DOR 而不是数据客体值给受访问者的操作，同时，它调用由 DOR 指明客体给访问者的操作。

3.12.14 办公数据客体 office-data-object

一种客体，它能表示办公信息。

3.12.15 办公信息 office-information

在办公环境下使用的数据。

3.12.16 特权属性 privilege-attributes

同安全主体有联系的属性，当与安全客体控制属性竞争时，它被用于授权或拒绝对安全客体的访

问。

3.12.17 特权属性执照 privilege-attribute-certificate

使用特权属性的执照。

3.12.18 生产操作 produce-operation

由x客户机调用给受访问者的操作,受访问者请求DOR而不是数据客体值。

3.12.19 认可属性 qualified-attribute

在使用上有资格的一种属性。

3.12.20 引用客体访问 referenced-object-access

借助引用对客体的访问。

3.12.21 ROA操作 ROA-operation

由访问者调用给受访问者的操作。

3.12.22 安全属性 security-attributes

覆盖特权属性和控制属性两者的一般术语。安全属性的使用是由安全策略定义的。

3.12.23 安全客体 security-object

扮演被动角色的实体,它是根据授权策略批准或拒绝访问。

3.12.24 安全主体 security-subject

扮演主动角色的实体,它是根据授权策略批准或拒绝对安全客体的访问。

3.12.25 用户应用进程 user-application process

一种应用进程,它包含OA用户和一种或多种分布式(办公)应用客户机(如x客户机、y客户机等)。

3.12.26 x-

特定应用名的类属占位符。

3.12.27 x访问 x-access

x应用的功能性定义,在x客户机或x服务器之间可见到。

3.12.28 x访问抽象服务 x-access-abstract-service

在x客户机和x服务器之间的抽象服务。

3.12.29 x访问协议 x-access-protocol

用于x客户机和x服务器之间的协议。

3.12.30 x应用 x-application

某个种类的分布式(办公)应用,如电子邮件应用或归档和检索应用。

3.12.31 x应用系统 x-application-system

x客户机和x服务器系统的集合,它们一起向x用户提供x应用的功能性。

3.12.32 x客户机 x-client

x应用的部分,它是包含x用户应用进程的一部分。

3.12.33 x服务器 x-server

x应用的部分,它是x服务器应用进程的一部分,它提供由x访问抽象服务定义所规定的功能性。

3.12.34 x服务器系统 x-server-system

一个或几个x服务器的集合。

3.12.35 x系统抽象服务 x-system-abstract-service

x服务器之间的抽象服务。

3.12.36 x系统协议 x-system protocol

用于x服务器之间的协议。

3.12.37 x用户 x-user

当使用x应用时，作为假想应用进程的部分。

4 缩略语

ACSE 联系控制服务元素
ASN.1 抽象语法记法一
CAP 控制属性包
DOA 分布式办公应用
DOAM 分布式办公应用模型
DOR 可辨别客体引用
EDIFACT 管理、贸易和传输的电子数据交换
OSI 开放系统互连
PAC 特权属性执照
QoS 服务质量
ROA 引用客体访问
ROSE 远程操作服务元素
RTSE 可靠传送服务元素
UTC 世界时间

5 模型

注：本章所使用概念的辅导背景信息，见附录D。

5.1 DOA 抽象模型

5.1.1 访问抽象模型

分布式办公应用的开发应和图1中显示的客户机-服务器抽象模型相一致，它使用GB/T 16284.3中定义的抽象服务定义约定。

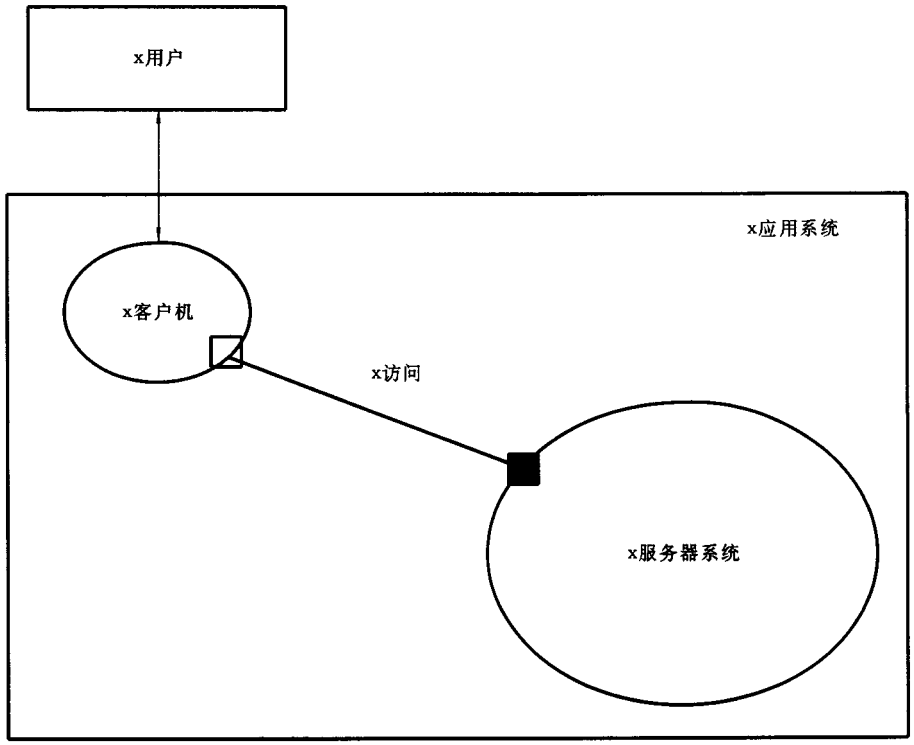


图1 访问分布式办公应用抽象模型

在图1中,x用户是x应用的使用者,它由x应用系统提供。x用户和x客户机相互作用,使用x应用提供的服务。x客户机通过x访问来访问x服务器。x服务器系统可以是分开的并且分布到不只一个x服务器。x服务器系统的内部结构细节在5.1.2中定义。

在x客户机和x服务器之间可以定义一个或多个端口。对于每个端口,端口类型应是非对称的。

注1:访问对称端口提供的服务超出本标准的范围。

在x客户机和x服务器系统之间交换的信息应是办公信息。办公信息是在办公环境中使用的数据,如:

a) 文件;

b) 信报;

c) EDIFACT 数据;

d) 文件属性;

e) 时间;

f) 和信报有关的信息;

g) 归档文件的信息;

h) 打印文件(包括字型)的信息;

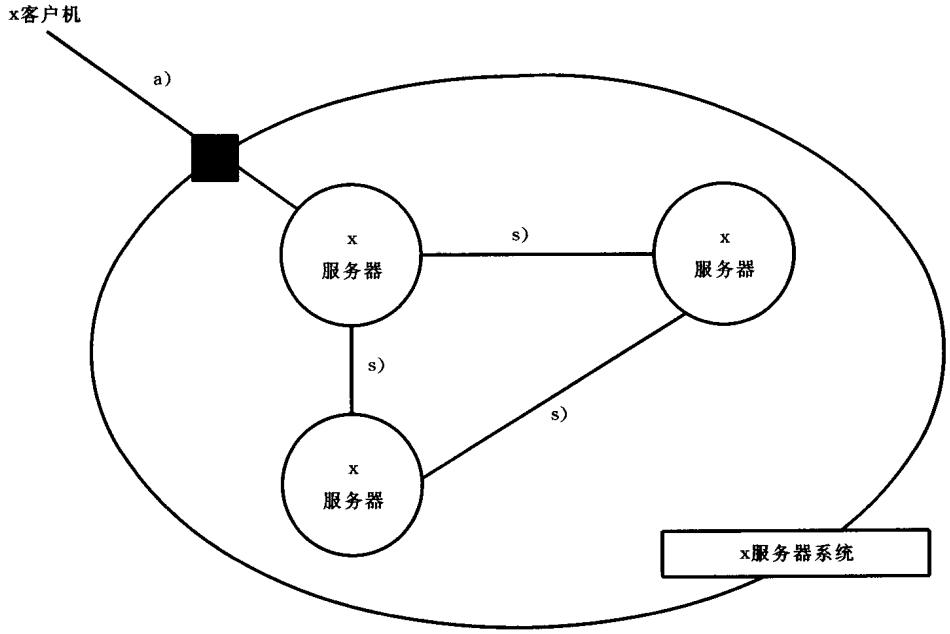
i) 服务器的管理信息。

这种信息被看作办公数据客体的集合,它能被个别或成组的访问并操纵。

注2:不属于办公信息的其他信息的交换已在并将在其他标准中定义。

5.1.2 服务器系统的抽象模型

图1中x服务器系统可以细化,通过服务器之间定义一个抽象服务将x服务器系统分布化,见GB/T 16284.3的建议。图2显示了x服务器系统的细化。



a) x访问抽象服务

s) x系统抽象服务

图2 x服务器系统的细化

在图2中,x客户机通过x访问的抽象服务a访问x服务器系统。在x服务器系统中,x服务器响应此访问。x服务器可以通过x系统抽象服务s与其他x服务器交互作用,实现x客户机请求的服务。

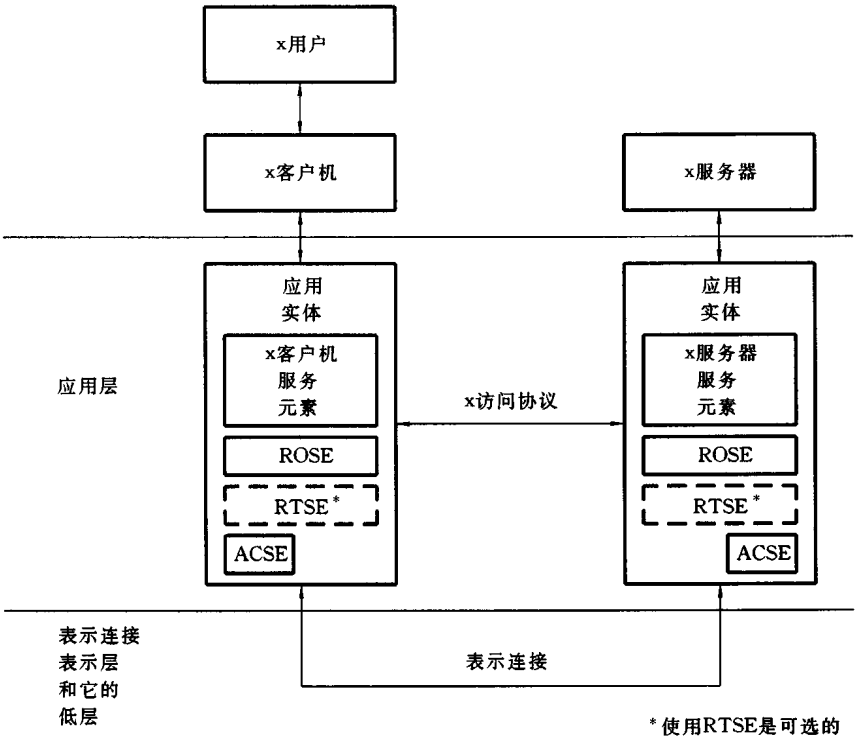
一种x服务器系统可以包含不同类型的x服务器。

在x服务器之间可以定义一个或多个端口。任何类型的端口都可被使用。

5.2 DOA 抽象模型的实现

5.2.1 访问抽象模型的实现

为了实现访问抽象模型，由 ISO/IEC 9072 定义的 ROSE 及它的 OSI 映射应被使用。在图 3 中显示了层次模型。关于如何标识x客户机和x服务器的进一步信息，见 6.4.4。



注

1 本图是一个例子，并且不限制映象。

2 一个x客户机和x服务器可以有几种应用实体，反之亦然。

3 应用实体可以服务于不同服务器类型。

图 3 访问 DOA 抽象模型实现的层次模型

5.2.2 服务器系统的抽象模型的实现

在实现服务器系统抽象模型上没有限制。例子见附录 D。

5.3 引用客体访问

5.3.1 数据访问的种类

数据客体值的访问从概念上包括三个部分：

a) 始发者，请求访问；

b) 受访问者，数据客体值存储和生产；

c) 访问者，数据客体值消费或修正。

在分布式办公应用中，将存在作为数据客体的受访问者或访问者的应用，例如文卷、文件或正文部分。

当始发者同受访问者或访问者任一个互定位时，数据访问作为访问请求部分发生。这称为直接值访问。

假如始发者与访问者和受访问者两者经过物理上或一段时期分开，使用直接值访问可以包括两种数据传送(“读”和“写”操作)。作为选择，为使网络的能力更加有效，始发者可以要求受访问者返回一个引用而不是它的实际值给数据客体。这个引用能由始发者交给访问者，它能通过单个传送访问数据客体

值直接和受访问者接触。

使用高级程序设计语言作为类推，当使用直接访问时，能考虑自变量或结果“按值”进行传送，当使用引用数据访问时“按名”进行传送。

5.3.2 引用客体访问的功能模型

5.3.2.1 功能模型

当始发者、受访问者和访问者被从空间上或暂时地分离时，引用客体访问(ROA)功能模型是能应用的。图4阐明了此功能模型。例如，始发者、受访问者和访问者可以在三个不同系统中运行，或者始发者系统在以后作为受访问者或访问者。

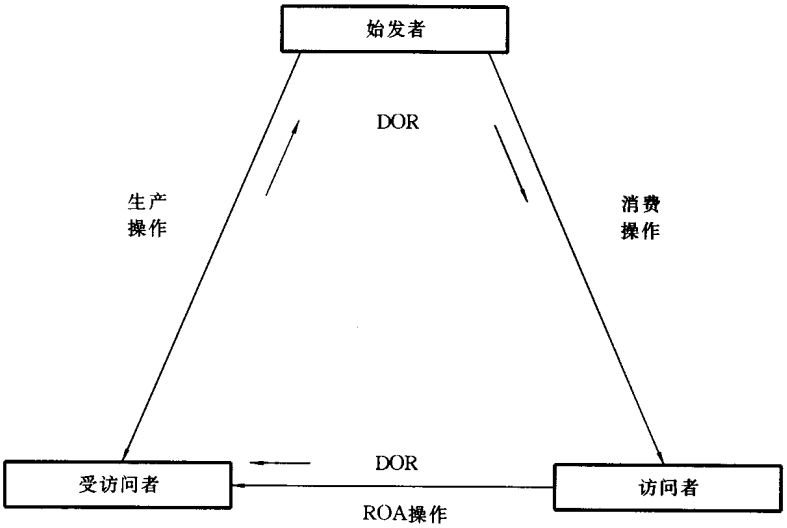


图4 引用客体访问模型

在ROA中，对数据客体值的引用(称作可辨别客体引用或DOR)在生产操作结果中被返回给始发者，并且在消费操作自变量中传递给访问者。然后访问者调用ROA操作。在写操作情况中，一个新值或修正数据值的指令能和访问请求一起被传递。在读操作情况中，引用数据客体的实际值在访问操作结果中被返回。

当执行ROA操作时，根据应用特殊规则，被访问值和受访问者已知的数据相关，应用特殊规则是生产操作期间和DOR有联系的。例如，可以定义DOR去引用特殊MOTIS IP信报第一个正文部分。

ROA操作不必被迫访问固定的或永久的数据客体。

在图4中，DOR是由受访问者在响应由始发者调用生产操作时生成。DOR是由始发者提交给访问者的，它作为消费操作的参数。然后访问者使用DOR和受访问者相互作用。

5.3.2.2 生产操作

在一些数据操作中，始发者使用应用特定协议从受访问者中选择数据客体值(完整的数据客体或数据客体某个子集或导出的部分)。此类操作称为“生产操作”。

在直接值传送中，受访问者返回数据客体值给始发者，始发者扮演访问者的角色。在间接情况中，从另一方面说，始发者请求引用数据客体而不是数据客体值，并且受访问者返回DOR给始发者。DOR识别它们联系的唯一数据值。

在DOR由生产协议元素支持中，要求调用中的参数要规定是返回直接数据值还是返回DOR。相应地结果应包括数据值或DOR。

5.3.2.3 消费操作

始发者也能使用应用特定协议促使数据客体值被访问者访问。这类操作称为“消费操作”。在直接值传送中，始发者扮作受访问者，同时提供协议中的数据客体值。在间接情况中，始发者提供一个DOR(先前从受访问者中获得)给访问者。访问者使用此DOR实现对受访问者的访问操作去读或写引用数

据客体值。

在DOR由消费协议元素支持的地方,提供的数据可以是数据客体值也可以是DOR。这个结果在两种情况中有相同的语义,但是如果使用DOR,访问者需在消费操作结果返回前等待ROA操作结果。

5.3.2.4 ROA操作

分布式办公应用模型定义特定协议类,这种协议总是使用DOR和受访问者应用客体相互作用,它还提供操作的一般集。这个类称为"引用客体访问协议(ROA协议)"。

5.3.2.5 支持DOR的含意

DOR要求在受访问者和访问者中建立附加功能:

a) 响应生产操作时,受访问者需能够提供DOR,而不是数据客体值;

b) 消费操作中访问者需能够接收DOR,而不是数据客体值;

c) 访问者需能够调用访问操作;

d) 受访问者需能够实现访问操作。

在应用特定协议中,标准可以选择是否:

a) 在供应或返回给数据客体引用的地方,允许在任何协议元素中使用DOR;

b) 在允许DOR的地方,放置附加限制;

c) 定义特定协议元素以处理ROA生产和ROA消费操作。

这些任选项的头一项被强烈地推荐,应尽可能被使用。

如果在特殊目的访问中受访问者或访问者都不支持DOR,则始发者没有选择,只能执行两个连续直接值的传送。既然这样,由始发者从受访问者那里调用生产操作,返回数据客体值给始发者,同时在消费操作自变量中始发者传送数据客体值给访问者。(这个描述适用于读操作。在写操作情况中,数据将流向反方向。)

5.3.2.6 服务质量

一些数据客体值将随着时间改变,或者客体可被删除。单个协议可以选择DOR是否:

a) 在DOR被生成时,引用数据客体值;

b) 引用数据客体当前值;

c) 如果客体被更新,变为未定义。

为协助在引用控制中动态地改变客体,DOR可以包括服务的质量(QoS)指示。QoS为DOR和相联的数据值两者的有效性描述预期或要求范围。X访问协议需要支持更新QoS的协议元素。

5.3.2.7 DOR构造

DOR构造细则和相关的规程由本系列标准第2部分定义。

6 协议设计指南

6.1 引言

本章显示应被所有分布式办公应用标准遵循的协议设计指南。

6.2 办公信息

分布式办公应用的主要目的是交换、存储、检索和处理办公信息。

为了维护现存的多样性或者为了维护未来办公信息的概念和类型,抽象语法和办公数据客体的语义对于分布式办公应用协议来说可以是透明的。既然这样,在DOA协议的抽象语法中办公数据客体应作为ASN.1外部类型在"直接引用"变体中出现(即,没有编码规则的表示层协商)。外部类型的"直接引用"OBJECT IDENTIFIER"值引用抽象语法和客体的编码两者。这个值应在标识客体类型的属性中使用。

6.3 客体模型和远程操作

6.3.1 远程操作的使用

在 ISO/IEC 9072 中定义的远程操作为联编操作、断联操作和操作(在客体模型中称为类型操作)提供记法和协议规范。操作的标准集和命名指南在后面的条中描述。

分布式办公应用的所有访问协议应符合 ISO/IEC 9072 中规定的远程操作。更详细地说,访问协议应使用标准的记法和概念,同时应允许 ISO/IEC9072 第 11 章中定义的任何映射。附录 J 给出了考虑 6.4的应用规则,对访问协议的上下文中这些概念的介绍。

对于系统协议,只要可能,都鼓励使用远程操作。

6.3.2 对 x 服务定义的抽象服务技术的使用

抽象服务技术是基于大量的 ASN.1 宏,它被用于描述服务的功能和参数。服务的描述技术同正式定义的远程操作方法密切相关。该技术保证服务定义和协议规范之间完全一致。由于对服务所作的定义形成进入正式协议的可能,也保留工作和文件资料的备份。它也很易于在一个 DOA 和另一个 DOA 中形成入口定义,不必须重定义或重新文件化。MHS 和目录的标准正使用这一技术。所有未来 DOA 也应使用服务文件资料的相同技术。

抽象服务宏在 GB/T 16284.3 中定义。

6.4 应用规则

为了简化大量应用中共享资源的管理,建立了下面一些规则。

6.4.1 并发性和资源共享

6.4.1.1 并发性

在集中系统中存在建立的技术,它控制并发访问和保持数据的完整性。对于分布式系统,分布式数据的通用事例没有经济的通用解决方案。

应用应避免通用情况。在较强要求出现和为特殊应用得出的解决方案之前,指南一般用于弱一致管理,即:

a) 允许非一致的数据;

b) 对每一数据项都有一主要拷贝,更新它是一指定服务器的职责;

c) 有一传播队列改变该数据项的拷贝和改变相关数据项;

d) 将不同服务器数据项之间的关系减为最小;

e) 提供管理控制,调整一项改变进行传播所要花的时间;

f) 设计应用,以容忍过期的数据或对它有弹性。

根据本指南,并发性控制能被限制在单一 x 服务器中,或者至少在一个 x 系统中。对协议的影响被限制于资源共享影响上。

6.4.1.2 资源共享

服务器中的共享资源由服务器管理(它依次依赖于节点的低层操作系统)。

对协议的影响被限制对某一时间在不能响应互操作服务器的影响的管理上。可通过拒绝接受交互作用,指示延迟响应或推迟的响应表明。扮作 x 用户的实体施加超时规律。

如果要求,x 系统可以在它的 x 服务器之间提供资源共享管理。这将要求在 x 系统协议中进行表达,但是除上面描述的以外将不影响 x 访问协议。

6.4.2 网络透明性

为了使用户与环境网络配置的细节隔离开,服务器和客户机应按名而不是按表示地址提交。目录可用于提供这个转换 。

6.4.3 时间的公共定义

在分布式办公应用环境中的所有协议应使用 GB/T 16262 定义的数据类型“Generalized Time”表达时间。

TIME::=GeneralizedTime

注:GB/T 16264 和 GB/T 16284 现在使用“UTCTime”代替“GeneralizedTime”。在这些标准中 GeneralizedTime 的

使用预期将保持向下兼容。

6.4.4 标识符公共定义

在DOA标准中定义的所有客体应至少有一个全局唯一名。名的公共理解和标识符的公共定义在GB/T 9387.3、GB/T 16262和GB/T 16264中定义。在附录E中介绍它们。

遵循这一模型应用所使用名的ASN.1编码在GB/T 16264中定义。

6.4.5 属性和筛选器的使用

在分布式办公应用上下文中,许多客体(如在信息库中表示的)由属性定性。属性由属性类型组成,它识别属性和符合属性值给出的信息类。

属性概念、支持属性定义的记法和属性的抽象记法在GB/T 16264.2中定义。子集在GB/T 16284.5中定义。分布式办公应用的标准,如果合适,应使用这些属性,同时参考GB/T 16264.2。

如果由信息库中项目表示的客体由属性定性,则信息检索(如项目选择)可以请求筛选器。筛选器应用一项测试,看它是满意还是不满意(如通过特殊项目)。筛选器用关于某些属性(如项目)值或存在的断言表达。

筛选器的语义和抽象语法在GB/T 16264.3中定义,同时子集在GB/T 16284.5中定义。分布式办公应用标准如果合适应使用这些筛选器,同时也参考GB/T 16264.3。

为一个应用定义的属性类型可被另一个应用重新使用,只要定义和语义是相同的即可。在GB/T 16262中定义的OBJECT IDENTIFIER可作为工具来使用以达此目的。

属性宏在GB/T 16264.2中定义。

"认可属性"技术被认为可在分布式办公应用上使用。例如它使客户机能标记一特定属性是不是强制的,其意义就是相应的服务器必须懂得属性的语义和知道如何响应,或者标记是否服务器能忽略所属属性或用缺省值来代替。

注:此技术用法的例子见ISO/IEC 10175—1《信息技术 文本与办公系统 文件打印应用 第1部分:抽象服务定义和规程》。

6.4.6 引用客体访问

在访问协议中的数据客体值和DOR可以典型地作为ASN.1的外部类型出现。

6.4.7 应用服务元素和应用上下文

实现几个访问协议所要求的功能的应用服务元素可以被结合在单一应用上下文里。要求每一个这些应用服务元素有独特的抽象语法。(也见图3。)

6.5 安全规则

6.5.1 引言

建立下列规则是为了简化访问控制和鉴别安全方面的执行和管理。

这个规则使一个比较广的范围安全策略被使用,不用改变分布式办公应用协议,它包含要求个人使用分布式办公应用的特殊职能的安全策略。

注:安全概念的详细辅导介绍见附录F。

6.5.2 安全主体

安全主体通常是操作实现中起特殊责任的个体。在一些安全策略里,职能可以赋予公众中的一组人,或者一个用户。分布式办公应用可以控制依照安全主体标识的访问,或者控制依照安全主体要求能力的访问(存在确认这样的要求技术)。特权属性执照是一个数据结构,它安全地负载安全主体的属性;在结构中出现的值依赖于安全主体和有效的安全策略。

分布式办公应用应使用特权属性执照(PAC)表示安全主体的鉴别性和特权性。在安全策略有效地要求特殊责任的地方,PAC应包括必要的标识。

PAC通过BIND来传递,同时它应适用所有在联系中的随后的操作直到UNBIND和ABORT终止它为止。每个特殊操作应允许客户机传递给另一个PAC;这应为特殊操作补充BIND的PAC。

在操作导致对操作或者 UNBIND 或 ABORT 的随后处理的地方，操作的有效 PAC 也应用于随后的处理。

6.5.3 安全客体

安全客体是正被保护的客体，以便安全主体的访问被有效安全策略调整。安全策略可以要求检查是按照安全主体标识要求的基本特权，也可以是按照安全主体要求的基本特权，或者两种途径的某种结合。控制属性包(CAP)是一个数据结构，它安全地运载访问控制信息；表示的值取决于有效的安全策略和个别客体。

分布式办公应用应使用控制属性包(CAP)运送办公数据客体的访问控制信息。当创建客体、修正客体或传送客体它的访问控制信息时，这就可能。

6.5.4 访问控制

前面的安全规则是从协议中运送的安全元素的设计中分离出分布式办公应用协议的设计。这有利于在不同安全环境中相同协议的使用。

分布式办公应用的操作定义和数据结构模型应允许一个广泛范围的安全策略与它的协议一起使用。

任何安全策略假定，例如从安全客体到另一个安全客体的访问控制属性的隐式拷贝，应被“服从有效安全策略的限制”认可。

6.5.5 安全差错

几乎所有操作都可根据安全的理由被完全拒绝。

安全拒绝可以作为差错来报告，它优先于其他差错(除防碍安全主体、安全客体和操作确定的协议错误之外)。安全差错响应不应以这样的方式表达，也不伴随或者随其他差错响应，它隐含或运送不应给安全主体的信息。

如果访问被拒绝，导致对单一安全客体进行访问的操作在该客体上应没有影响。

访问几种安全客体的操作可以遇到在这些客体上的安全拒绝。这样操作的结果和响应将被定义。

6.6 操作标准集

本条显示抽象操作的标准集。

它最初的目的是协调抽象操作集，同时协调它们对不同分布式办公应用的名。这个协调将减少标准化特定分布式办公应用所需的时间和精力，同时将使 DOA 标准的实现者容易熟悉和使用特定应用的操作。

特殊分布式办公应用的开发者应使用这个标准集的操作去适当地定义在它们的特殊分布式办公应用中的操作集。

下列是 DOA 抽象操作的标准集：

a) 列表；
b) 读；
c) 修正；
d) 拷贝；
e) 移动；
f) 搜寻；
g) 创建；
h) 删除；
i) 保留；
j) 通告；
k) 放弃。

这些操作细则的例子在附录 K 中显示。

附 录 A
（提示的附录）
提示附录的引用标准、定义和缩略语

A1 引言

本附录给出本标准提示附录中特有的引用标准、定义和缩略语。在本标准正文中出现的引用标准、定义和缩略语不包括在这里。

A2 引用标准

下列标准所包含的条文，通过在本标准中引用而构成为本标准附录的条文。本标准出版时，所示版本均为有效。所有标准都会被修订，使用本标准的各方应探讨使用下列标准最新版本的可能性。

GB/T 9387.4—1996 信息处理系统 开放系统互连 基本参考模型 第4部分：管理框架(idt ISO 7498—4：1989)

GB/T 14814—93 信息处理 文本与办公系统 标准通用置标语言(SGML)(idt ISO/IEC 8879：1986)

GB/T 15936—1996 信息处理系统 文本与办公系统 办公文件体系结构(ODA)和交换格式(idt ISO 8613：1989)

GB 16505—1996 信息处理系统 开放系统互连 文本传送、访问和管理(FTAM)(idt ISO 8571：1988)

GB 17176—1997 信息技术 开放系统互连 应用层结构(ALS)(idt ISO/IEC 9545：1989)

A3 定义

A3.1 OSI基本参考模型定义

本标准的附录采用GB 9387中定义的下列术语：

a）应用进程 application-process。

A3.2 OSI基本参考模型安全部分定义

本标准的附录采用GB 9387.2中定义的下列术语：

a）访问控制 access control；

b）访问控制列表 access control list；

c）审计 audit；

d）审计跟踪 audit trail；

e）鉴别信息 authentication information；

f）能力 capability；

g）机密性 confidentiality；

h）数据完整性 data integrity；

i）数据来源鉴别 data origin authentication；

j）数字鉴名 digital signature；

k）加密 encryption；

l）密钥 key；

m）密钥管理 key management；

n）否认 repudiation。

A3.3 面向文本信报交换系统(MOTIS)的定义

本标准的附录采用 GB/T 16284.2 中定义的下列术语：

a) 信报传送 **message transfer**；

b) 信报传送系统 **message transfer system**；

c) 信报存储 **message store**；

d) **P2**；

e) 用户代理 **user agent**。

A3.4 分布式办公应用模型(DOAM)定义

本标准的附录采用下列定义。

A3.4.1 访问控制策略 **access-control-policy**

一个规则集，属于安全策略的部分，用此规则集对人用户或他们的代表进行鉴别。并用此规则集进行这些用户对服务和安全客体的访问。

A3.4.2 访问上下文 **access-context**

用诸如位置、日期时间、低层联系的安全级别等这些变量表示的上下文，在其中形成对安全客体的访问。

A3.4.3 密码密钥 **cryptographic key**

见密钥。

A3.4.4 数据客体格式规范 **data-obiect-format-specification**

在 ASN.1 意义上，独立于 x 访问协议定义的数据类型。

A3.4.5 节点 **node**

数据处理设备，它提供作为网络部分的信息处理资源。节点可以支持用户应用进程、服务器应用进程或两种类型进程的组合。

A3.4.6 OA 用户 **OA-user**

应用进程的一部分，它直接同人用户交互作用，同时它在代表人用户使用一个或多个办公应用。

A3.4.7 安全管理者 **security-administrator**

负责实现安全域的安全策略的权力机构(一个人或一批人)。

A3.4.8 安全域 **security-domain**

安全客体和安全主体的有界组，由单一安全管理者执行的单一安全策略适用于它。

A3.4.9 安全设施 **security-facility**

规程、进程、机械装置或组合体，它们模型化一个有关安全的功能。

A3.4.10 服务器应用进程 **server-application-process**

应用进程，它可实现由 x 服务定义所定义的部分或全部功能。

A3.4.11 用户 **user**

人用户或 x 用户。

A3.4.12 用户应用进程 **user-application-process**

应用进程，包括 OA 用户和分布式(办公)应用的一个或多个客户机(如 x 客户机、y 客户机等)。

A3.4.13 **x-、y-、z-、… x-,y-,z-,…**

特殊应用名的类属占位符。

A3.4.14 **x** 应用接口 **x-application-interface**

x 应用的接口，在 x 用户和 x 客户机之间为可见的。

A3.4.15 **x** 服务定义 **x-service-definition**

x 应用功能性定义，在 x 客户机和 x 系统之间为可见的。

A4 缩略语

ASE	应用服务元素
CCR	委托、并发和恢复
DSSSL	文件风格语义和规范语言
FTAM	文卷传送、访问和管理
MS	信报存储
MOTIS	面向文本的信报交换系统
OA	办公应用
ODA	办公(开放)文件体系结构
ODP	开放分布式处理
RDA	远程数据库访问
SGML	标准通用置标语言
SPDL	标准页面描述语言
TP	事务处理
VTP	虚拟终端协议

附 录 B
(提示的附录)
和其他标准的关系

B1 上下文

本标准涉及集成方面,而且还有支持专业的、技术的和管理的用户的分布式办公系统。本标准不涉及实时处理也不涉及事务处理,它一般支持第一线操作的职员,如售货点、预售职员、现金管理者等。

本标准涉及使用通过 OSI 对多厂商设备的使用问题,同时它涉及各组织之间的交互工作。它有安全条款;当 OSI 安全标准变的更清楚和更稳定时,就将增加稳定的详细指南。

B2 其他标准使用

通过正常方式 OSI 高层协议的 ROSE 进行本模型下的协议开发。假定目录在整个分布式办公系统中都能利用。

B3 和其他标准的配合

面向信报的本文交换系统(MOTIS)和目录给分布式办公应用公共的许多方面设定了惯例。由于历史原因,MOTIS 有的方面并不和本标准完全一致。

可处理信息、可打印信息、可发邮件信息的文件是办公信息的主要形式。当在此模型下被开发的协议不依赖于文件特殊编码的使用时,将在现有的正在制订的办公(开放)文件体系结构(ODA)文件标准、标准通用置标语言(SGML)、标准页面描述语言(SPDL)和文件风格语义和规范语言(DSSSL)之间有着最佳配合。

远程数据库访问(RDA)可以作为办公功能,与 DOAM 的某种协调将是有益的。

B4 和其他标准共存

B4.1 虚拟终端协议(VTP)

由于VTP被定位在应用和人用户之间，它超出本标准的范围。

B4.2 文卷传送协议

文卷传送访问和管理(FTAM)不直接被按照文件和类似于关系式的数据访问进行操作的大多数办公系统用户所感知。本标准规定不与FTAM一起实现的指南。然而，希望使用类似于FTAM的文卷存储模型和功能度的用户应用也将能同办公应用一样使用FTAM。

B4.3 事务处理(TP)和委托、并发和恢复(CCR)

目前没有要求在分布式TP环境中使用办公应用。目前没有CCR训练要求。本标准当前并不要求办公应用协议在风格上被设计为适合即将出版的标准。

B4.4 开放分布式处理(ODP)

本标准当前并不ODP工作项目。但是期望在适当时候进行协调。

附 录 C
(提示的附录)
要 求

C1 引言

分布式办公应用由集成分布式办公系统使用。分布式办公系统由网络链接的用户节点和服务器节点组成。用户节点通过网络访问服务器节点，它使用访问协议。集成化办公系统维护各个办公应用的紧密合作。

在单一主机作为单一单元的环境中，数据处理应用被分流在系统的不同智能部件中。分流导致需要对应用的不同部分之间内部关系加以标准化。

在分布式办公系统中，所有资源的同时可利用性不能被保证，并且支持性的或生产性的应用都不应假设特殊分布进程(如信报转送)的所有各方是同时在通信，由进程语义请求的除外。这引导出存储和转发通信(如信报传输)的概念，那里始发者潜在的接受者媒介者的信报传送代理在同一时间中都不是联机的。

C2 功能要求

从分布式办公系统中由用户要求的服务以及框架涉及的服务包括：

a) 个人之间的信报传送，为同其他用户通信；

b) 成组通信，为同用户组通信；

c) 转换，允许不同语法或字符编码文件的互换；

d) 文件的归档和检索，允许文件的多关键字检索和有序归档；

e) 文件输入和输出到分布式办公系统的不同物理设备，如扫描仪、打印机等；

f) 目录，知道在哪里和如何访问远程通信元素、应用或用户；

g) 鉴别，避免未授权访问不同应用；

h) 局部访问时基，为了诸如整个网络的时间邮戳信报和文卷的目的；

i) 直接访问远程服务器(如可视图文)和用户(如经由智能用户电报)；

j) 与远程系统间接通信(存储和转寄)，传送非实时信息或访问其他网络，如信报传送系统；

k) 不同应用或远程服务器之间的数据传送。

上面列出的应用将在未来增长(如数据库访问)。大多数附加应用可能是生产性的应用，因为它们的主要目的是给办公工作者提供特殊设施。

这些应用的典型用法需高度的集成化。如，文件可以从信报存储服务器中取出、存储在归档文件和

检索服务器中，并在打印服务器上打印。

在分布式办公应用之上的一些操作(通常如成组通信、文件归档和检索、打印)需要使用其他扮演支持应用角色的应用(如目录、鉴别)。

不论如何，应用和他们的用户不应被执行支持应用的方式所影响。特别是，对用户来说实际分布应尽可能是透明的。

支持应用对人用户不必是可见的，但是它能使整个系统能够安全、可靠和平滑地操作。

C3 设计要求

协议设计应保证：

a) 稳定性：

推荐的设计原理应使得分布式办公应用协议设计者能规定高度稳定的分布应用交互作用，同时广泛使用公共支持应用。

b) 模块化设计：

1) 减小一个仍然是可扩充的生产应用表的不同办公应用间的内部依赖性；

2) 能够完成所要求高度集成；

c) 协议的公共风格设计：

1) 支持应用和设施的同种用法；

2) 远程操作服务元素的同种用法；

d) 安全性：对用户规定不同的级别；

e) 简明性：这是来自分布式办公应用人用户观点的关键点。这意味着用户应不卷入到应用管理其请求的方法中。

本标准规定在不同应用中的交互作用原理。

附 录 D
(提示的附录)
基 本 概 念

D1 引言

根据人用户的观点，分布式办公应用被归类为构成集成办公系统的大量应用。

分布式办公系统由通过整个网络连接的节点构成。当这个系统为了人用户利益存在时，任何应用进程部分可以使用办公应用。

用户节点是同人用户直接交互的设备。它提供直接交互功能。

服务器节点是一个设备，它管理由很多用户共享的资源。

分布式办公系统和人用户的交互作用可以引出大量的活动，它在大量的节点上实现。如何由进程、任务等表示在一个节点上，这些独立活动不在本标准中涉及。在一个节点上的一个活动和另一个节点上的一个活动之间的交互作用在OSI模型中通过一对应用进程调用之间的交互作用来表示，每个节点上有一个应用进程调用。应用进程调用执行OSI应用进程的功能性。

为了更清楚起见，本章依照应用进程描述交互作用。本章中描述的每个功能实体同应用进程相关；执行功能的每个独立活动同独立应用进程调用有关。

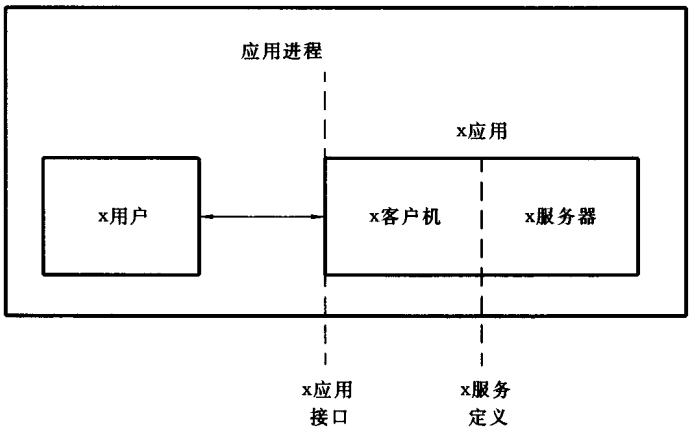
D2 客户机服务器模型

本章采用一种辅导方式是解释单个x应用即某类应用的分布。

D2.1 非分布式单一应用

在非分布式单一x应用中，x用户和x应用是互定位的。当x用户和人用户交互作用，或当x用户代表人用户与x应用交互作用时，在这一特定情况下，x用户称为OA用户，同时应用进程称为用户应用进程(见D3.1)。x用户通过x应用接口和x应用交互作用，此接口通常是专有的，并且未被标准化(见图D1)。

如果x应用是分布的候选者，x服务定义需要作为潜在的未来分布专有线。



图D1 非分布式办公应用

D2.2 分布式单一应用

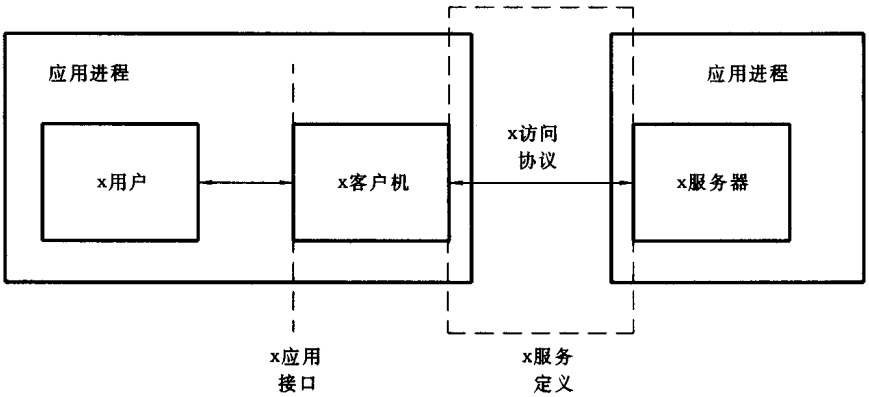
x应用分布对于x用户应是透明的，从而使x应用接口不会改变。x客户机和x用户互定位。x用户和x客户机一起在一个应用进程中。

x服务器一般对用户是远程的。x服务器是应用进程的一部分，它称为服务器应用进程。

x客户机和x服务器依靠x访问协议在网络上进行通信。在x客户机和x服务器之间可以有几个独立交互作用。

图D2中描述了新情况，它显示图D1的x服务定义扩展成“虚线”框封住的x访问协议。

在分布情况下，x服务定义和x访问协议需被标准化。



图D2 分布式办公应用

D2.3 客户机服务器OSI通信

x访问协议是x客户机获得访问它的远程x服务器的标准方法。下列模型显示OSI原理如何被使用来规定x访问协议。

按照OSI参考模型，协议在对等实体间使用。在图D2中，OSI通信仅出现于虚线框中。因此，对等实体OSI通信是在虚线框中，而不在它之外。

依照OSI参考模型，x客户机和x服务器被认为是应用进程的部分，同时有应用实体同它们联系。应用实体是OSI参考模型应用层的一部分，同时包括应用服务元素集。按照服务定义，应用服务元素提

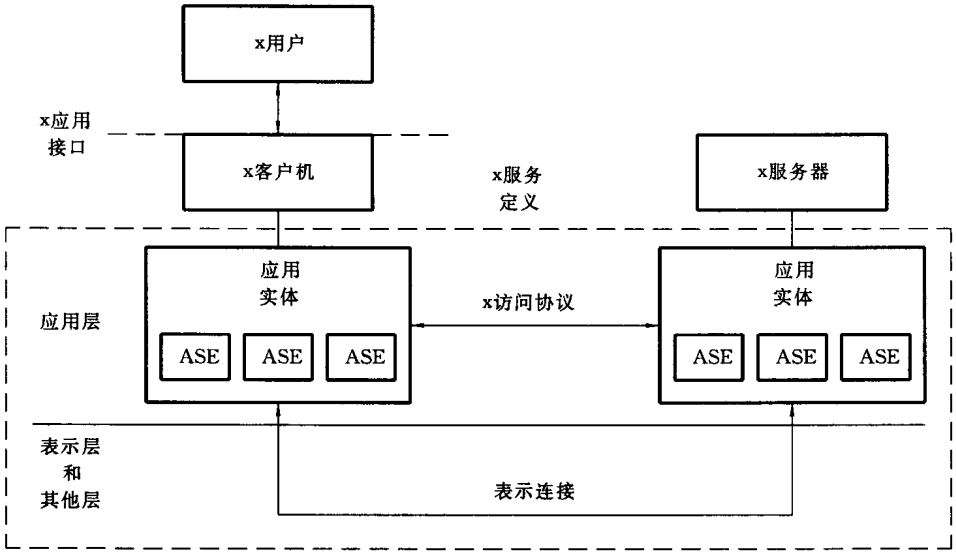
供通信功能给x客户机和x服务器，同时实现x访问协议。如此做，应用服务元素可以使用在同一应用实体中由其他应用服务元素提供的服务，同时通过OSI参考模型表示层来提供。

在图D3中，虚线框得到扩充以给出x客户机和x服务器之间OSI通信的更详细模型。

详细的说，交互作用发生在应用实体调用之间。在同一对应用进程调用之间交互作用的离散集在应用实体调用的离散对之间实现。

不论如何，对于多数实际目的，不必提及上述详细结构。相反，用x访问协议的x客户机/x服务器通信的模型对于讨论的分布式办公应用来说通过就足够了。

关于x客户机/x服务器通信的附加细则在第D4章中规定。



图D3 OSI通信的分布式办公应用

D2.4 分布式办公应用客体模型

分布式办公应用的应用进程的交互工作要求共享概念模式描述共享的领域。

典型的讨论领域是由它们之间的客体和关系组成，同时可以提供客体分类。

客户机/服务器模型被认为是开发概念模式的面向应用的工具。客体模型有宽阔的视角并且更抽象。分布式办公应用的部件(如电子邮箱、归档组合箱等)作为客体都被编址。

在客体模型中开发的工具用于概念模式的规范。概念模式是服务定义的基础。

需注意在分布式办公应用上下文中使用另一种客体类型。这些是数据客体(如ASN.1数据类型、信报内容、个人间信报正文部分、私人文件格式)。这些数据客体抽象语法的定义独立于x访问协议和x系统协议。

D3 功能模型

D3.1 在集成系统中的多个应用

集成办公系统由办公应用集构成(如信报传送、文件的归档和检索、打印)。办公应用的集成由OA用户实现。OA用户和人用户交互，并代表人用户和办公应用集交互作用。在OA用户和x服务器之间的交互作用通过x客户机实现。在客户机之间的交互作用通过OA用户实现。这在图D4中描述。

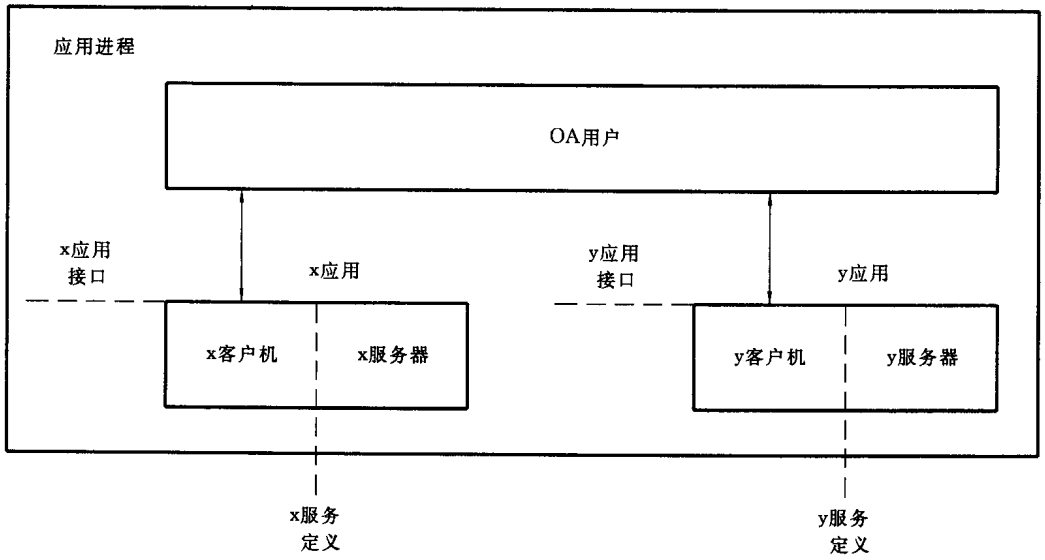


图 D4　多非分布式办公应用

D3.2　多个分布式办公应用

OA 用户和客户机是在称为用户应用进程的一个应用进程中(见图 D5)。几个用户应用进程可以共存于一个用户节点上,但它们在本标准中保持独立。

对于某些应用(如目录、信报存储),访问一个服务器每个 OA 用户的表示称为用户代理。用户代理包括客户机和 OA 用户。

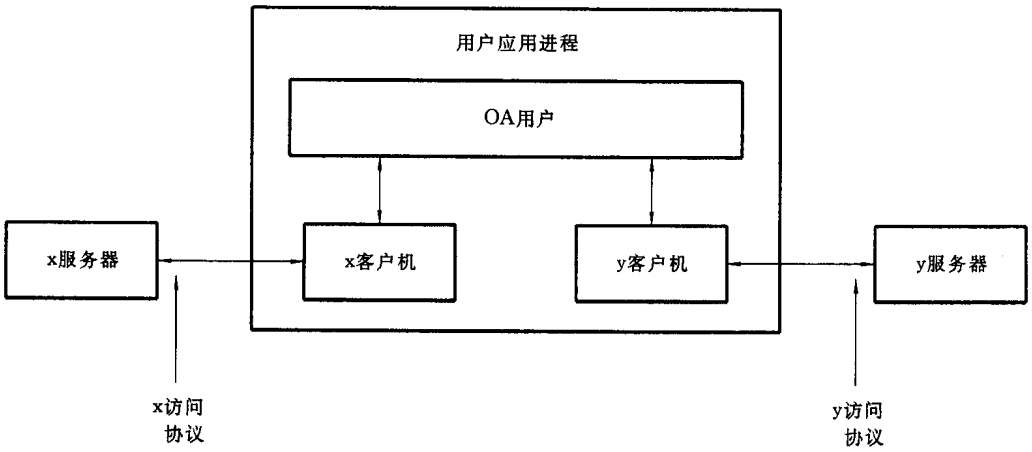


图 D5　多分布式办公应用

D3.3　服务器的组织

可能有第二个分布步骤,将一个 x 应用的服务器部分功能分布到几个节点上的几个 x 服务器上。x 服务器集称为 x 系统。每个 x 服务器功能是相等的,它支持同一 x 访问协议。每个 x 服务器都在一个节点中。

x 系统可由下列各项组成:

a) 单个 x 服务器;

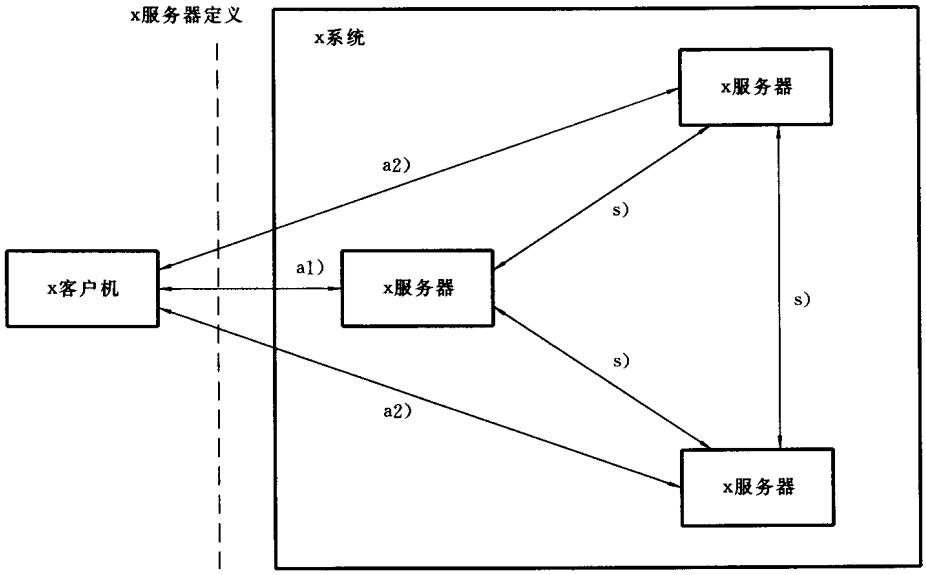
b) 几个非交互作用 x 服务器;

c) 几个交互作用 x 服务器。

x 客户机和 x 服务器之间的交互作用由 x 访问协议进行控制(见图 D6)。这些协议属于特殊 x 应用标准,不在本标准的细则里涉及。

通过网络连接的几个 x 服务器可以交互作用以构成整个 x 系统。在该情况下,它们依靠 x 系统协议相互操作。这些协议属于特殊 x 应用标准,并且不在此处细则中涉及。

在x客户机和特殊x服务器之间能利用的x访问协议子集取决于x服务定义和x服务器的分区。例如对于维持分布式信息库的x服务器，如果x系统协议不存在，或者如果x服务器不能或不愿意以对x客户机透明的方法来实现它，x访问协议可以包括指示机制(它意味着接触的x服务器返回一个提示给x客户机，说明为了找到一项特殊信息要与其他x服务器中哪一个进行接触)。



a1) x访问协议
a2) x访问协议(可选的)
s) x系统协议(必要时)

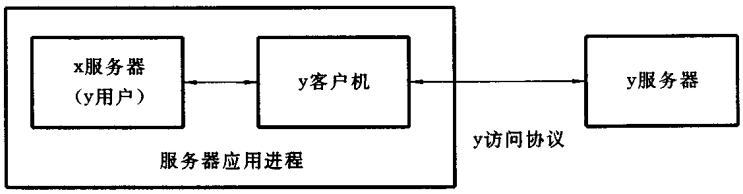
图D6 x系统

注意，虽然应用进程和应用实体等的同样OSI概念被应用，x客户机不是为x系统协议引入的。固有的客户机/服务器模型非对称性在一些系统协议设计中也没有什么用处。

D3.4 服务器之间的协作

D3.4.1 一个服务器作为另一个服务器的用户

有时一个系统(x系统)将使用另一个系统(y系统)。它是通过将需要使用y系统的x服务器描述为扮演y应用的一个y用户的角色来模型化。在这种情况下，y客户机存在于包含x服务器的应用进程中。



图D7 作为另一个服务器用户的服务器

当两个服务器是同一类型时，即当一个x服务器正使用另一个x服务器时，也能使用此模型。

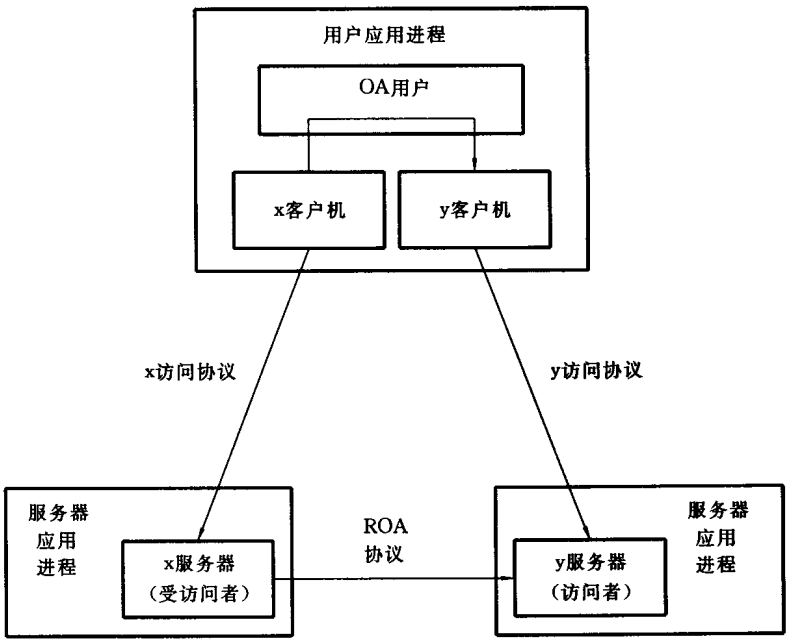
D3.4.2 引用客体访问

对于一些数据客体类型(见D2.4)x服务器扮演源而y服务器扮演数据值的接收端(如信报存储服务器可以是源，打印服务器也可以是象人与人之间信报正文部分一样是打印文件接收端)。一般来说，服务器可以同时扮演源点和数据接收端(如文件归档和检索服务器、信报存储服务器)。

如果x客户机和y客户机在应用进程内互定位，并且客体值必须从x服务器传送给y服务器，那么

从x服务器经过x访问协议将此客体值传送给y服务器，随后从y客户机经由y访问协议传送给y服务器(见图D8)，这样可能效率很差。在这种情况下，仅传送访问协议中客体值的引用效率更高些引用的客体值本身直接从源x服务器传送给接收端y服务器传送。

当客体值同x访问协议在x客户机和x服务器之间传送时，用户应用进程使用可辨别客体引用(DOR)管理数据传送也许是有益的。



图D8 引用客体访问

D4 客户机-服务器通信模型

根据在D2.3和图D3中介绍的模型，本章规定一些关于在x客户机和x服务器之间通信的附加细则。

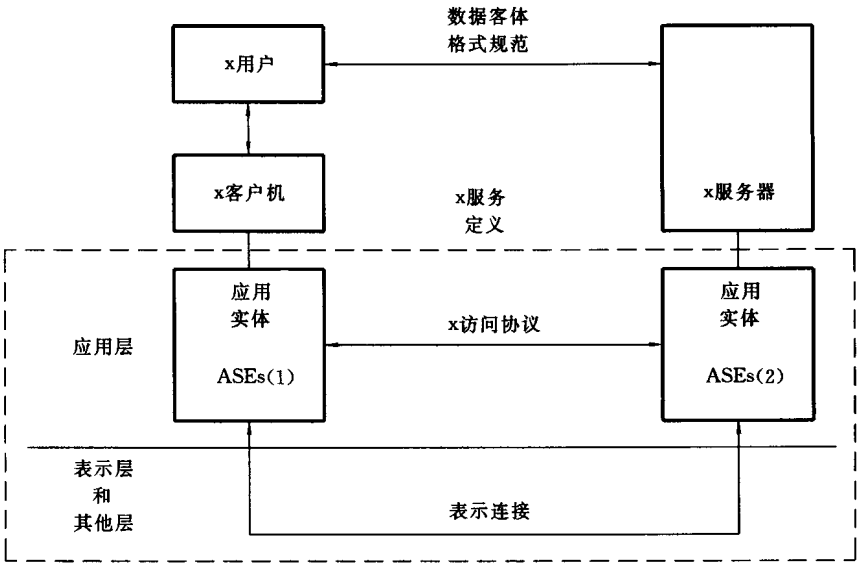
图D9～图D12给出不同配置的例子，这些配置要求应用服务元素的不同集。在每个应用服务元素集中，要求联合控制服务元素(ACSE)。此外，在每个集中要求远程操作服务元素(ROSE)。可靠传送服务元素(RTSE)是可选的。在给定的集中要求哪种附加应用服务元素取决于：

a) 分布式办公应用有关的本质；

b) 是否该集同客户机或服务器有联系；

c) 是否该集实现访问协议或系统协议。

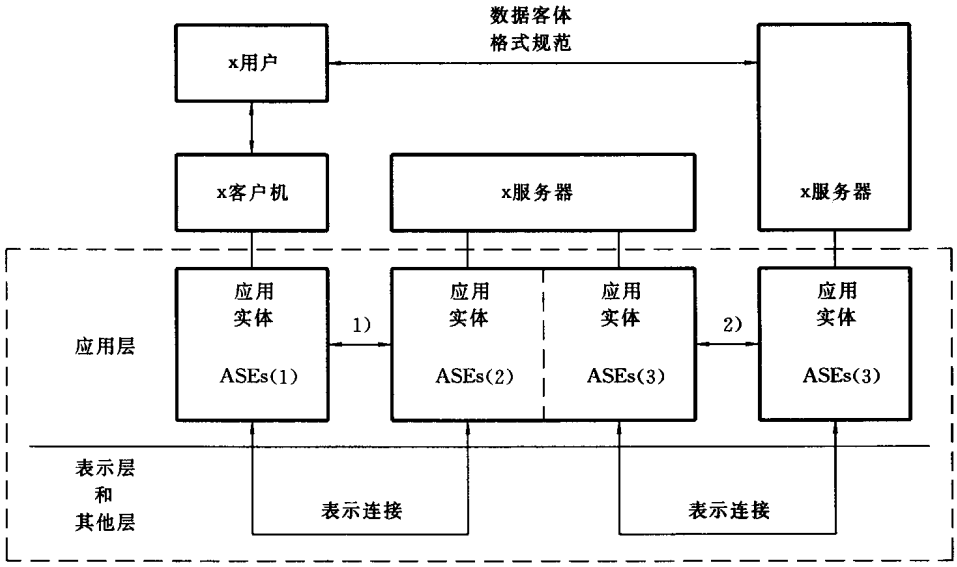
数据客体格式规范表示在x用户和x服务器之间，或OA用户之间的协作基础。



ASEs(1)：此应用服务元素集实现由使用 x 访问协议和 x 服务器通信的 x 客户机要求的功能。

ASEs(2)：此应用服务元素集实现由使用 x 访问协议和 x 客户机通信的 x 服务器要求的功能。

图 D9　在 x 客户机和 x 服务器之间的 OSI 通信



ASEs(1)：此应用服务元素集实现由使用 x 访问协议和 x 服务器通信的 x 客户机要求的功能。

ASEs(2)：此应用服务元素集实现由使用 x 访问协议和 x 客户机通信的 x 服务器要求的功能。

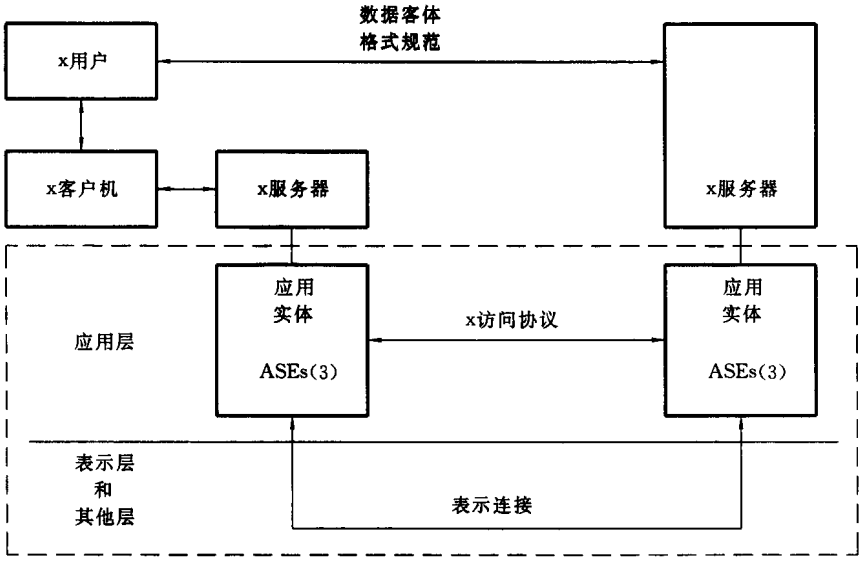
ASEs(3)：此应用服务元素集实现由使用 x 访问协议和另一个 x 服务器通信的 x 服务器要求的功能。

1) x 访问协议。

2) x 系统协议。

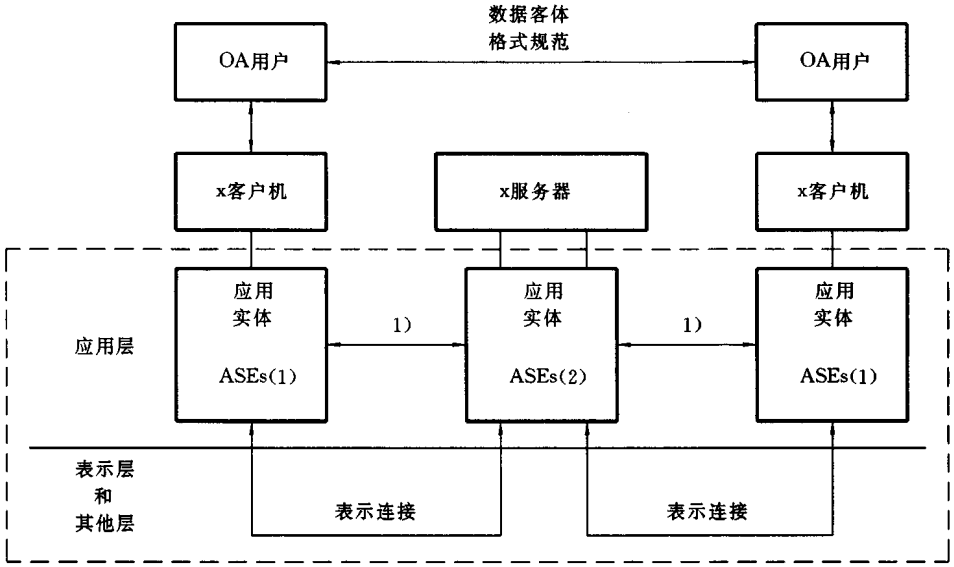
注：分别包含 ASEs(2)和 ASEs(3)的应用实体可以结合进单一应用实体中，它支持两个应用上下文。

图 D10　在 x 客户机、x 服务器之间和在两个 x 服务器之间的 OSI 通信



ASEs(3)此应用服务元素集实现由使用 x 系统协议和另一个 x 服务器通信的 x 服务器要求的功能。

图 D11　在 x 客户机和互定位 x 服务器和另一个 x 服务器之间的 OSI 通信



ASEs(1)此应用服务元素集实现由使用 x 访问协议和 x 服务器通信的 x 客户机要求的功能。

ASEs(2)此应用服务元素集实现由使用 x 访问协议和 x 客户机通信的 x 服务器要求的功能。

1) x 访问协议。

注：在图 D12 中，在两个 OA 用户(如在文件归档和检索或信报传送中)之间，x 服务器用作存储和转发系统。既然这样，数据客体格式规范表示在两个 OA 用户之间合作的基础。在单个应用上下文中可以定义多于一个访问协议。

图 D12　在两个 x 客户机和 x 服务器和在两个用户之间的 OSI 通信

D5　功能分类

D5.1　生产的和支持的应用和设施

在支持的应用和生产的应用之间，以及在应用的支持角色和生产角色之间形成了差别。

注意到应用分类或“生产的”或“支持的”有几分不精确，尽管如此它还是有用的。如，基本信报传送应用作为对其他应用的支持应用而潜在地使用，如分布目录在目录服务器之间更新。同样的，虽然目录应用一般被视作支持的应用，当它作为响应人用户查询信息使用时也能被认为是生产的应用。差别在于

应用是否直接提供人用户感兴趣的设施，而不是应用的内部特性。

各个支持角色的应用为了给用户提供稳定的、“高级”环境而进行合作。恰如程序设计环境由许多程序组成(很多是通用实用程序)，对生产的分布式应用的网络操作环境包括几个支持的应用。这些支持应用是使用与生产应用相同的模型概念建立的，它构成生产应用能接受的一般操作支持，并向 OSI 分布式办公应用的用户提供对其环境的“高级”看法，例如允许它们各种设施和资源的定位和物理的编址中进行去耦。

换言之，这些支持的应用构成生产应用和这些应用的用户的高级支持环境。

可被人用户见到的生产应用，被认为是有用的，同时由他特别使用。对于一般办公室工作人员，生产应用包括远程打印、文件归档和检索、邮件、某些目录使用等。

D5.2 操作支持

由生产应用假设的一般操作支持包括，如：

a) 时基；

b) 鉴别和属性设施；

c) 某些目录功能(如命名地址映射)。

这里列表的不是排它的，附录 H 给出这些角色更详细的内容。

D5.3 管理

某些管理功能特别重要，例如，记录分布式办公应用环境操作行为的那些功能。

其他管理功能被看作不同的应用，同时它被人视为生产应用。对管理信息的分析和表示更是如此。

管理是未来标准化的课题。

D5.4 应用指南

某些支持应用(如鉴别)对其他的访问协议有较大的冲击。这有两个方面，一个是依照协议负载信息，一个是依照操作被实现的序列。框架将依次规定如，鉴别、请求和得到对服务器访问所要求允许的序列。鉴别方面是未来标准化的课题。

如登录和计帐这类其他功能对应用设计和规范有影响。安全登录方面和计帐方面是未来标准化的课题。

分布式办公应用系统的管理者将选择某些这方面的策略；如生产应用将必须能适应这些策略的改变。

本标准的第 6 章给出指南的初始集，它们在目前可使用，直到某些方面(如安全方面)的研究达到更深的程度。

D6 应用之间的交互作用类型

本章描述和划归它们交互作用的不同类型，如在第 D5 章中介绍的与支持应用和生产应用的分类关系。

交互作用的这些类型在本附录的后面条中使用。

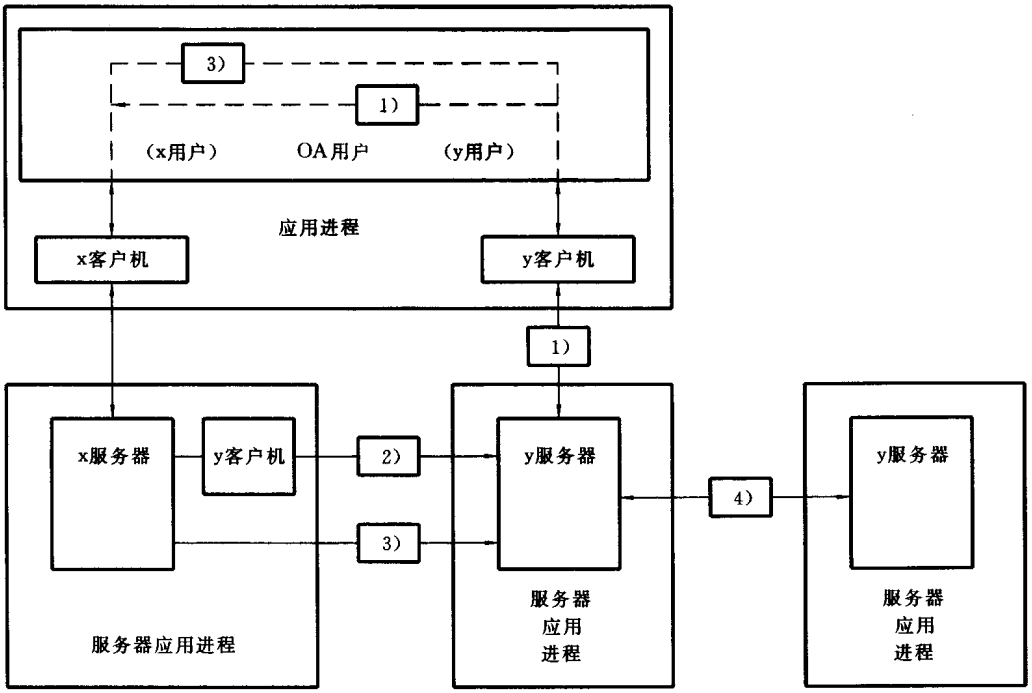
在 x 用户和生产 x 应用之间交互作用在本附录的前面章条中描述，这里不重复。

交互作用，举例来说，x 用户和支持应用可以在 OA 用户和生产应用之间交互作用相关于在图 D13 给出为 OA 用户和(支持的)y 应用之间类型 1 交互作用。在类型 1 交互作用中获得的信息被在同(生产的)x 应用交互作用中的 OA 用户使用。交互作用分别地使用 x 和 y 访问协议。

在两个服务器之间的交互作用(可以是生产的或支持的任一个)在图 D13 中作为类型 2 交互作用显示。x 服务器使用互定位 y 客户机访问使用 y 访问协议的 y 服务器。

最终协调的存在交互作用集，它扮作引用客体访问。这里使用 x 和 y 访问协议的用户或实体扮作 x 用户和 y 用户，指导 x 服务器和 y 服务器实现信息传送。在图 D13 中它显示为类型 3 交互作用。类型 3 交互作用因此包含两个调整动作。第一个，内部到用户的动作，调整引用客体和 x 服务器在 y 服务器的

建立,第二个,要求的访问本身。



1) 类型1交互作用,在OA用户或扮演x用户角色的服务器与y服务器之间的交互作用,这些交互作用在信息中的结果是从与x应用交互作用中正使用的y服务器处得到的。

2) 类型2交互作用,在使用y客户机和y访问协议的x服务器与y服务器之间的交互作用。

3) 类型3交互作用,在两个服务器之间的交互作用,这两个服务器的动作依靠OA用户发出的指令或扮演x用户及y用户(使用x访问协议和y访问协议)角色的实体发出的指令。从x服务器把信息传送给y服务器使用ROA协议。

4) 类型4交互作用,在同一类型的两个服务器之间的交互作用,它们使用为该目的定义的系统协议。图D13显示类型4交互作用中使用y系统协议的两个y服务器。

图D13 交互作用类型

D7 应用交互作用实例

图D14显示在OA用户和实现生产的和支持的功能应用之间的交互作用实例。

一旦OA用户开始信报存储器的联编操作,在信报存储器中归档收到信报的简单动作要求下列操作:

a) 信报存储服务器访问鉴别和安全属性服务器(类型2交互作用)。

b) OA用户访问信报存储服务器来标识以后作为客体提交信报。

c) OA用户访问目录得到文件归档地址以便检索服务器能够归档信报(类型1交互作用)。

d) OA用户访问文件归档和检索服务器去选择一个结构,在此结构下,该信报必须被归档并用作为先前交互作用2)的结果提供的引用来标识它。

e) 文件归档和检索服务器从信报存储服务器通过ROA协议(类型3交互作用)得到信报。

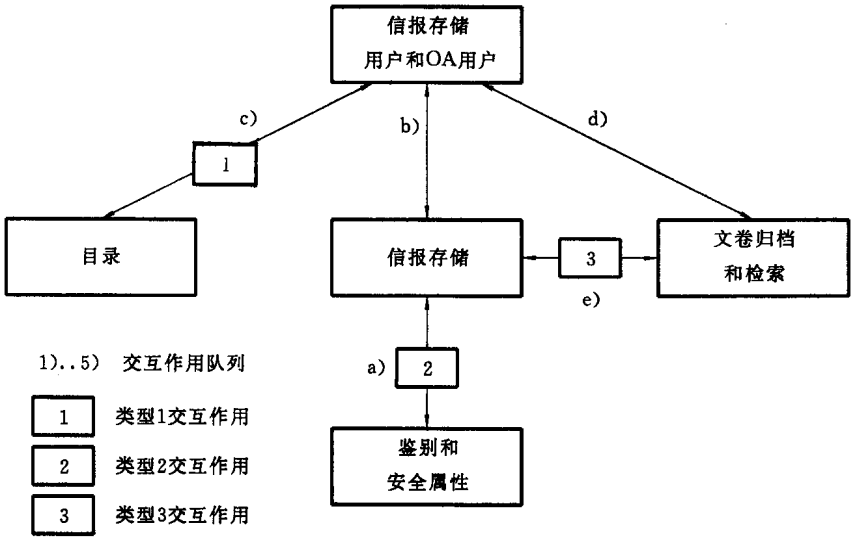


图 D14　在信报存储器的 OA 用户和其他应用之间的交互作用

附　录　E
（提示的附录）
标 识 考 虑

E1　一般要求

分布式办公应用环境由实体的地理性和逻辑传播表示其特性，这些实体如应用、节点、客体、客户机和服务器。这些实体必须全部紧密的联在一起工作以便分布式办公应用有效地完成它的任务。

在开发紧密的互连中的重要工具是使用称为“命名”的概念。“名字”是语言学的概念，它从所有实体集中标识一个特殊实体。一个实体，如服务器，将有它自己的名字使它区别于其他服务器。这个可辨别名可在目录应用中查到。

一些有可辨别名的系统在下面实体列出：

——人用户；

——人用户组；

——节点（用户节点和服务器节点）；

——服务器；

——数据客体（如文件存储器）。

附加标识独立实体，命名概念协助提供分布式办公应用需要的其他功能能力。例如，用户节点和服务器节点需要能够找到下列名：

——包括特殊归档组合箱的归档和检索服务器；

——服务器，它包括特殊用户的信报存储器；

——服务器，它拥有数据的主拷贝（如：其中之一是允许更新目录部分）；

——在组织中打印服务器，它能提供精美的字型和打印机的宽行滚筒。

由于目录提供具有下列功能的能力，用户能完成这些动作：

——给属性命名联编（Name-to-attributes binding）：这个能力联编一个名字给用名字调用的实体（客体）相关的一块信息。给地址命名的联编是属性命名联编的特例。大量可以驻留在分布式办公应用系统中的实体，使这一能力成为基本能力。此功能类似于“白页”目录。

——给名字集的属性联编（Attribute-to-set-of-names binding）：这个能力列出给出属性的实体（客体）名。其例之一是能被使用的“黄页”目录，例如，在一个有“精美”字体和宽行滚筒的组织中找到所有远

程打印服务器的名字。

——替换的名字:同一实体(客体)的不同名字,也就是别名,在允许用户更灵活的访问分布式办公应用环境的大量实体方面是有用的。为了提供同一客体的不同拼写,可以方便的介绍别名(如 MUNICH/MUNCHEN)。类似的,在一个企业内部环境中,服务器可以通过与内部使用名不同的名来为外部引用,以隐藏任何组织细节。

E2 名字类型

E2.1 概述

分布式办公应用标准要求下列命名和编址信息:

a) 应用联系的控制所要求的名字和地址;

b) 人用户和 x 用户标识符所要求的名字;

c) 数据客体所要求的名字。

E2.2 应用联合控制的名字和地址

GB 9387.3 为命名和编址确定某些原则。应用联系控制要求的名字和地址在 GB/T 16688(ACSE)中定义。

E2.3 用户命名

在 MOTIS 上下文中,用户由 O/R 名字标识。O/R 名字可选择包括一个可辨别名字。

在其他分布式办公应用上下文中的用户由可辨别名字标识。

O/R 名字在 GB/T 16284.2 中定义,可辨别名字在 GB/T 16264.2 中定义。

E2.4 客体命名

如果客体信息存储在目录中(如文件存储),这些客体由可辨别名字标识(见 GB/T 16264.2)。

在客体集合中可能有标识客体的规定,如在文件存储中标识文件。

要求唯一标识(见附录第 E3 章)的其他客体由 ASN.1 客体标识符标识。

E3 标识符登记

对大量客体类型将必须作为各别的标准部分或由某些登记机构给出标准的标识符。一些例子在下面给出。标识符是 GB/T 16262 中定义的 OBJECT IDENTIFIER。

E3.1 应用上下文

联合控制服务元素(GB/T 16688)要求应用上下文的标识。

E3.2 信报内容类型

在 MOTIS 中定义的信报内容类型识别由 P1 协议支持的不同类型的内容。内容类型是数据客体格式规范的例子(图 D9)。细节见 GB/T 16284.2。

E3.3 信报正文部分类型

信报正文部分类型标识不同格式/编码的类型,它能作为用户信报(见 GB/T 16284)部分被找到。这些信报正文部分类型也是数据客体格式规范。

一些信报正文部分类型在 GB/T 16284.7 中定义。其他可以在其他标准中或由登记机构定义。

E3.4 DOR 客体类型

DOR 客体类型需被标识(见本系列标准第 2 部分)。

E3.5 属性类型

通过使用“属性”概念(见 6.4.5),属性类型将被各个分布式办公应用标准定义。如果属性类型标识符在一个应用中已被分配给信息的特殊类型,这种类型能(和应)被需要同样属性类型的其他应用所使用。

附 录 F
（提示的附录）
安 全 概 念

F1 引言

本附录是辅导性的。

F1.1 “安全”定义

对本标准来说“安全”是指办公系统的一些特征，这些特征给出对偶发事件、故障和误使用的抵御，不论它们是有意或无意。因此，安全指的是规程的、逻辑的和物理的措施之综合，这些措施目的是控制和管理这些措施的工具，一道预防、检测和纠正某类偶发事件、故障和误使用。

按照这个定义，安全不仅仅涉及有意的误用，如有意威胁系统，它也涉及偶发事件，象信报的错误路由选择和指出错误路由选择的原因，从而使得能标识责任方。

通过这种方法，除了解决对本身的威胁外，安全还提高了业务的完整性。

F1.2 安全范围

许多不同安全需隐含独立于办公应用提供的安全功能的公共集。这些公共、安全功能将在用户和生产的应用之间在生产的应用和支持应用之间的交互中成为可见的，在应用和低层系统的安装、维护和管理中也可见。这些功能，它们的交互动作和它们的管理构成在本标准的安全范围。

F1.3 安全策略

为更加有效，安全措施需要是有条理的。因此，一个组织将在安全策略中定义它的安全措施和操纵和管理这些措施的方法。安全管理人员履行执行安全策略和维护它的有效性的责任。

下面是安全策略所涉及安全措施的例子。哪种措施可作为给出安全策略部分来实现，这取决于组织的环境。

a）系统包含和/或系统处理的信息的完整性；

b）(选择的)信息的可信度由系统包含和/或由系统处理；

c）服务和功能的完整性由系统提供；

d）服务和功能的可信度由系统提供；

e）某个操作获得第三方的担保的方法。换言之，第三方的进程和信息完整性的验证是必需的；

f）按照定义的规则鉴别特殊用户或用户组的方法；

g）对在系统上或通过系统都是可利用的服务器、功能和信息的访问的控制；

h）在系统中和系统之间的信息流量的控制。

在一般情况下组织将要求同其他组织交互作用。组织将选择他自己的策略；每一种安全策略可以说是适用于一个给定安全域，它是在单一安全管理者控制之下。业务隐含要求在安全域之间的交互作用。这也需要由安全策略来解决。

在某些情况中，两个安全域可以直接交互作用，在其他情况中它们可以通过第三方交互作用。并且，在安全域之间的信任度也可以变化。

F2 分布式办公应用的安全要求

F2.1 一般安全要求

本条介绍在分布式办公应用环境中出现的一般安全要求。这些要求反映出两个隐含要求——例如没有某种形式的访问控制系统就不可能是安全的——以及从用户角度看到的特定安全功能要求——例如，数据源的鉴别。

F2.1.1 访问保护

F2.1.1.1 概述

访问控制提供限制对某个已知用户进行访问和控制这些用户对特定操作的特定资源进行访问的方法。因此,访问控制有两个主要成分:用户鉴别和已鉴别的用户的访问授权。访问控制按照适用于安全域的访问控制策略来实施。

F2.1.1.2 鉴别

得到访问分布式办公应用系统权限的用户在被许可访问服从于安全控制策略的任一特殊应用之前,将首先被鉴别。用户也可以要求访问的服务器是可信的。用户这个可以从同x服务器属于同一个安全域的节点访问x服务器或从属于另一安全域的节点来访问x服务器。在任一情况中,交换鉴别信息的公认规程必须被使用。

鉴别是有时间限制的;在通信中重复鉴别可以被确定的安全策略所要求。

F2.1.1.3 访问授权

分布式办公应用环境中的节点可以要求使用访问授权来保护安全客体的可信度和完整性以及服务器节点的完整性。授权方法可以使用多种多样机制,例如访问控制列表、能力和其他安全属性、单一或结合使用。

在包含的安全域的主要安全策略下,用户将被授权访问x服务器和在x服务器根据它们的特权属性访问x服务器中的安全客体。

一旦用户访问不属于它们的安全域的服务器或安全客体,服务安全域要求的授权信息将被以安全方式传递。

F2.1.2 数据信息的保护

安全策略可以要求与分布式办公系统互换或存储在分布式办公系统上的数据免受外部的冲击。在上下文中"外部"是用来指明不是通过正常系统访问路由(例如电线轻触,媒体失窃)。

数据保护涉及可信度(保密)和完整性(防止改变)。

在分布式办公应用环境中,下列关于数据保护的要求适用:

a) 在存储器中数据的保护(甚至在可移动媒体上);

b) 交换中的保护,例如在系统之间交换的访问控制信息、信报、电子文件和文卷。

保护指阻止敏感信息的泄露及阻止可信信息同不可信信息混在一起。

除非必须依赖物理保护,可信度可以要求使用加密,完整性可以要求使用数字签名。

加密技术要求密码钥匙的使用。系统支持的加密在安全域内和在安全域之间使用必须提供钥匙管理的安全方法。

F2.1.3 资源使用的保护

安全策略可以要求资源使用的保护。这种保护有两种方式:对使用保密(用法的可信度)和防止拒绝服务。

F2.1.4 资源使用可记帐性

安全策略可要求确保资源使用可记帐性的方法。可记帐性包括操作审计跟踪有选择的登记(尝试和已完成),以及数据源和接受的非否认。

非否认是向第三方证明实体的标识,该实体发出或接收例如一个给定的信报。它与数据完整性密切相关,并且它经常同数据完整性相结合。

F2.2 安全管理要求

F2.2.1 一般考虑

支持安全分布式办公应用的系统应向操作的组织提供一些工具,去管理这些系统的安全设施。这些工具的例子是安全软件安装和对安全设施操作进行审计的审计设施。

分布式办公应用的用户信任系统部件完整性,以执行预期功能而非其他的功能。

F2.2.2 安全管理方面

对于为分布式办公应用环境定义的安全功能的各个类型，误用或安全缺口的四个方面应被指出，它们一起定义这些功能的管理要求。这四个方面是：保护、检测、恢复和操纵。根据要求的安全级别，一些方面或所有这些方面在现实的实现都可见。

保护基于管理安全功能或应用的规则。这样规则的例子如每三个月改变一次口令。

检测基于系统安全操作的审计。

与操作相关的安全审计将涉及系统安全功能的有效性和使用的反馈一起提供给安全管理员。

审计有三个部分：

a）审计跟踪生成和采集；

b）审计跟踪分析；

c）审计跟踪存档。

属于操纵方面。

在分布式办公应用环境中，应用可以分布于多安全域。在这样的地方，公认的审计技术需有利于域内的合作。

安全缺口(真实的或猜想)的恢复可以要求改变在分布式系统的不同节点处可利用的安全规程和信息。因此，协议和规程必须支持恢复措施的实现。

操纵有两个同系统生命相关的方面：

a）汇集来自系统的信息；

b）创建系统信息。

第一个方面涉及由已登录在受保护数据库的信息形成的报告。必须提供特别的筛选器以便安全管理员能调整报告只得到他需要的信息类型。第二个方面处理安全主体和安全客体的创建和删除，也处理关键字、权力和口令的定义(至少是初始口令)。

F3 安全系统模型

F3.1 概述

在安全分布式系统中，必须进行大量活动以提供安全性。

安全系统模型把这些活动分为元素，每个在整个安全体系条款中扮演单一、清晰的角色。这些抽象元素意图成为推理工具而不是作为安全功能的真实执行。这些元素作为安全设施引用。

在标识安全设施和它们之间的通信后就能显示它们可以如何结合在一起形成支持安全应用，或者它们如何变成用户应用进程和服务器应用进程的可信部件，和在适合于它们彼此的交互以及和分布式办公应用环境元素的交互动作的地方实现规定的标准协议的可信部件。

依照 OSI 模型，这里涉及的观察级别在应用层以上。描述的支持安全应用使用充分安全的服务进行通信，来满足它们的需要。在某种可接受的程度，这些需要采用以下担保的形式，它们之间的通信和它们与不信任的对等者的通信是可信度和不能修改的，同时每种通信是与已知的和已标识对等实体进行。

在 OSI 低层中，提供这些保证的模型可以是未来标准的主题。

有两个根本不同的级别，分布式系统的安全要求需在这两种级别上加以解决：

a）应用独立的级别，控制访问作为用户应用进程、服务器应用进程、工作站、通信资源等的分布式系统安全客体；

b）应用特定级别，控制访问在应用中的特定安全客体(如文件)。

观察的两个级别有非常不同的要求，反映在不同的安全策略子集中，它们适合于所涉的不同种类的受保护安全客体和负责对它们进行支持的不同部件。在一种级别中看作保护安全客体的一些事情可能在另一处成为一个访问的安全主体。

F3.2 安全设施

在此描述阶段,读者不应有设施分布程度的假设;从作为单一安全服务器到作为每个分布式支持或生产应用的一个方面它也会变化。也不建议这些设施需在分布式系统的每个节点上全都可利用。它们应被视为一个建造块列表,从该表中能作出适合于分布式系统所要求的安全策略及安全级别的选择。然而,通过标识完整的列表,模型导致清晰的遗漏和被分开而任一产生的安全弱点不是偶然的。附录F的F3.3和附录H的第2章给出某些安全设施结合在三种支持的安全应用中。本附录的这一部分标识了下列安全设施:

F3.2.1 用户保证设施

在分布式系统中(独立于可能正在使用的任一服务)知道一个安全主体对受保护安全客体的当前访问。涉及的安全主体一般是人用户,但是在对服务器访问其他服务器进行控制的策略下,安全主体可能是x服务器。它的职责包括:

a) 传递鉴别凭证;

b) 服务选择的初始化;

c) 超时不活动用户。

F3.2.2 鉴别设施

接受和检查安全主体凭证、向其他安全设施通知它的结论。安全主体将是经由他的用户保证者的人用户,作为安全主体的非安全应用(即,使用y服务器的x服务器),或是联机出现并使它自己可用的非安全应用。

F3.2.3 安全属性设施

提供适当与主体相关的访问机构属性和访问控制属性,用来授权或拒绝安全主体对安全客体请求的访问。

F3.2.4 授权设施

使用访问上下文、(安全主体)机构属性和(安全客体)控制属性,以授权或拒绝安全主体对安全客体的请求访问。

F3.2.5 联系管理设施

这个设施保证:

a) 安全低层通信,包括保证通信实体的标识。

b) 机构,通过机构设施,代表控制用户授权两个实体通信。

上层体系结构功能如何与联系管理设施关联或如何用于支持联合管理设施可以是未来标准的主题。

F3.2.6 安全状态设施

维护在分布式系统中鉴别的安全主体和安全客体的当前动态状态,它们的联系和机构属性由那些联系运载。

F3.2.7 安全审计设施

接收来自其他安全设施的事件信息,以便记录及立即或以后进行分析。

F3.2.8 安全恢复设施

按照安全管理员定义的规则集,对来自安全审计设施的事件信息采取动作。

F3.2.9 域内设施

控制和映射一个安全领域对安全主体的标识、安全客体的标识、鉴别和授权数据的解释到另一个安全领域的解释。帮助联系管理构成在不同安全领域中实体间的联系。

F3.2.10 密码支持设施

提供密码其他安全设施和应用使用的密码功能,以使数据在存储器中安全并以下列特殊方法转发口:

a) 数据的可密度;

b）通信的可密度；

c）通信的完整性；

d）数据源鉴别；

e）源的非否认；

f）接受的非否认。

F3.3 支持安全应用

为本标准的目的，以下三个安全应用被标识：

a）鉴别和安全属性应用。它结合鉴别设施和安全属性设施；

b）域内应用。这是域内设施；

c）安全审计应用。这是安全审计设施。

另外，其他支持的安全应用可以被定义，实现在附录 F3.2 中给出的安全设施的其他结合。注意出现的安全设施，例如，联合管理，不管作为独立实体或作为用户应用进程部分和服务器应用进程的部分，将需要分布式办公应用的附加协议元素。

F3.4 代理人

在某些情况中 x 服务器可由 y 服务器而不直接由用户访问。这有两种情况：

a）初始化 x 服务器代表它自己动作；或

b）x 服务器代表另一个安全主体动作(例如人用户)。

第一个情况可使用，例如，限制访问安全客体，它已拥有一个服务器(称作文卷服务器)，要通过另一个(称作数据库服务器)来访问。它完全适于数据库服务器的动作，着眼于文件服务器作为安全主体和它自己的标识及访问授权。

在另一方面，它可以适于初始化 x 服务器，代表用户(通过代理人)动作和假设它的一些或全部安全属性。代理人能包含用户对单一特别访问请求的信任或者它能包含更大的权力。代理人可以包括访问请求细节或者它可以包括这些细节的引用。这可以是未来标准化的主题。

用这种方法，访问能依照所用路由来控制。

F4 分布式办公应用的访问权

有一些 DOA 规定安全特性。例子是访问权。分布式办公应用的访问权将按本条的基本描述来设计。表 F1 显示在抽象操作的标准集和访问权选项的一个可能集之间的关系举例。

表 F1 访问权和允许的操作

	OWN	RMD	RM	RO
列表	x	x	x	x
读	x	x	x	x
修正	x	x	x	
拷贝	x	x	x	x
移动	x	x		
搜寻	x	x	x	x
创建	x			
删除	x	x		
保留	x	x	x	
通告				

表 F1(完)

	OWN	RMD	RM	RO
放弃	x	x	x	x

x 意味着在相应访问权下所允许的相应操作。

注：表 F1 显示下列访问权的四个级别：

a) 所有者 (OWN)；

b) 读—修正—删除(RMD)；

c) 读—修正 (RM)；

d) 只读 (RO)。

附 录 G
(提示的附录)
管 理

分布式办公应用要求过程的、逻辑的和物理的步骤，它提供给分布式办公应用的管理者计划、组织、监督、控制和计帐以使用分布式办公应用的能力。这些步骤可以操作在单一分布式办公应用或操作在跨越大量开放系统的多分布式办公应用中。这些步骤作为“管理”被引用。

管理是由大量设施提供，每个支持所需步骤的每一个方面。这些设施包括：

a) 故障管理；

b) 计帐管理；

c) 配置和命名管理；

d) 性能管理；

e) 安全管理。

一般 OSI 管理在 GB 9387.4 中进一步讨论。

附 录 H
(提示的附录)
应用的分类和关系

H1 引言

本附录检查办公应用的一般需要，在不同时间任一应用可以有支持的或生产性质的角色。在前面情况中，应用支持(提供服务给)另一个应用。其他应用通常是生产性质的角色，一般提供给人用户一个可见的服务。本附录描述协作在应用执行支持角色的应用和负担生产服务角色的应用之间完成。

注：在本附录中，术语支持的和生产的将用于描述任何应用在与描述活动有关的时间所扮的角色。本附录不假定应用是固有支持的或生产的。

H2 支持的应用操作和设施

H2.1 时基设施

随着国际组织当前不断增加，一个全球意义上提供可靠的和明确的时间基是必要的。大量节点同全球网络联接，它们自己也同另一些网络互连，这在未来中将变得很重要。

任何分布式系统的各种部件必须能获得当前时间。这个时间能被另一个应用使用，例如，时间邮戳

文卷、时间邮戳信报、使鉴别能够完成。

同步不须精确，但时间应保持在合理的范围中(例如有规律的 10min 的一些事情)。在整个分布式系统中，精度由管理员设置。

如果要求(例如时间邮戳)，许多精密定时由节点中局部时间设施使用。时间局部派生的值可能需要被指明时间值的源的位置信息所认可。

各种主机获得和维护正确时间的方法超出本标准范围。

这个设施提供阳历中包括日、月和年的通用国际时间(具有任选的秒)，它能规定精确到一秒或一分。

H2.2 支持的安全应用

H2.2.1 引言

本条描述支持的安全应用，它们一起提供支持：

——独立于应用级别安全去控制访问分布式系统安全客体，如客户机、服务器、工作站、通信资源；

——应用规定级别安全去控制访问在一个应用中的特殊安全客体(如文件)。

下列支持的安全应用在以后条中标识和描述：

——鉴别和安全属性应用(H2.2.2)；

——域内的应用(H2.2.3)；

——安全审计应用(H2.2.4)。

这些安全应用不负责：

——建立在安全应用客户机和安全应用服务器之间的安全通信(这能通过加密的主关键字安装作为系统建立部分来完成)；

——作为分布式系统真正的和授权的成员的节点鉴别。

这些事情是安全管理在安装、配置和再配置期间的责任；管理机制可以是未来标准的主题。

应注意到这些安全应用是独立于它们支持和服务的办公应用。

H2.2.2 鉴别和安全属性应用

这个应用规定鉴别和处理人用户和应用级安全客体如 x 服务器的安全属性。

一般说来，鉴别依赖于人用户、x 用户或 x 服务器，由该人用户、x 用户或 x 服务器证明拥有(保密的)某块信息证明它的身份。这采取三个基本形式：

a) 人用户、x 用户或 x 服务器产生信息块的拷贝，信息块是由人用户、x 用户或 x 服务器保持秘密，系统借助某个映象表(传统口令途径)的将它和人用户、x 用户或 x 服务器联系起来。信息有效性检查通过另一 y 服务器的使用完成(例如检查 ISO 目录中简单凭证操作)；

b) 人用户、x 用户或 x 服务器使用没有明确地传送给它的一些信息块，如系统(哪个知道它的)能证明它的满意于发送者拥有信息。再根据内部映射，发送者的标识被证明(密码技术基于常规的关键字模式)。

c) 人用户、x 用户或 x 服务器使用没有明确地传送的一些信息块，使系统(也知道它)能满意的证明发送者拥有此信息。根据内部映射或显式传送的信息，确证发送者身份(密码技术基于公共关键字模式)。

可以使用交换鉴别的不同协议，例如，挑战/响应协议阻挠鉴别序列的重放。

为了提供灵活的途径，x 用户和人用户同特别安全属性值相联系。这个应用规定主体相关机构属性和同时客体相关控制属性的处理和存储，它们用于授权或否认要求访问应用级别的安全客体，例如 x 服务器。在安全属性值这两个集上的测试由鉴别设施完成；这些测试可以是复杂的和把外部因素计算在内。

鉴别结果和安全属性值不是无限有效的。在一些安全策略下，例如，人用户不时将要求重新鉴别自己和重新建立安全属性。

在许多安全策略下，鉴别和安全属性应用的用户被登记在安全审计应用中。

H2.2.3 领域内应用

人用户和/或一个分布式系统的部件可以在不同的安全领域中。这影响它们之间安全方面的交互作用。例如，在一个安全领域中人用户可自由访问的安全客体只对一些在安全领域之外很少的人用户是可以访问的。

保护某个“秘密”安全客体不能被任何来自其他安全领域的用户访问是非常重要的。无论怎样，允许某个来自其他安全领域的用户访问另一个“非秘密的”安全客体是需要的。即使如此，如果在远程安全领域的安全破坏了，应保护局部安全领域中“秘密的”安全客体。

在安全领域之间哪个安全客体是不可访问的可以有不同的选择，它取决于安全领域之间的关系。这个选项也不是纯粹分级的。因为在两个安全领域之间的工作关系，特殊的安全客体集对于安全领域中一些用户是可访问的，同时对另一些安全领域中的所有用户是不可访问的，另一方面从此安全领域不可访问的其他安全客体对其他安全领域的一些用户可访问。换言之，一个安全领域可以“信任”另一个以访问安全客体限制集。这个集取决于安全领域中安全主体和安全客体之间的关系。

假定信任在安全领域之间对安全客体集访问，基于安全主体身份和属性，安全客体的安全领域中最终级别的控制是必要的。安全客体的安全领域将必须托付安全主体的身份以安全主体的安全领域，同时也可以使用由安全主体的安全领域支持的安全主体属性。

在安全领域之间的关系将是双方的(及反映低层的商业安排)。因此，对任何两个交互作用的安全领域，有一个逻辑不同的领域内的应用。

下面是领域内的应用映射一个安全领域对以下内容的解释到另一个安全领域的解释中：

a) 安全主体标识(人用户和用户的)；

b) 安全客体标识；

c) 安全属性。

领域内应用与鉴别和安全属性应用交互作用来完成此。在任何安全策略下，领域内应用和安全审计应用一起登录活动。

H2.2.4 安全审计应用

审计跟踪是对安全的任何有效监督的基本要求。

安全策略规定事件或出现，事件或出现可以被生产的应用和支持的应用记录。它们通过使用安全审计应用记录事件或出现。

为了以后的分析，有适当安全属性的人用户安全地拥有安全审计跟踪。(一些事件或出现可以导致立即对分布式系统的指定的人用户或指定的部件做出报告和警告。)

H2.3 目录应用

目录应用扮演一个关键角色，向用户提供对分布式办公应用环境的稳定“高级”观察，尽管在低层固有地可改变网络和物理设施。

在适用的地方，分布式办公应用将使用在GB/T 16264中规定的目录应用，如下列功能：

a) 目录应用的最基本功能是给表示地址名的分辨。用户根据命名在网络上引用一个实体，同时通过目录服务器，应用将此还原为表示地址，表示地址通常支持和“物理位置”相近的关系。实体能用便于记住的命名引用，这对于系统用户来说是一个友善的接口。

b) 目录应用也提供管理实体组(列表)的方法(如增加和删除成员，递归的扩展和成员验证)。这有许多应用，如信报处理；

c) 另外，目录应用提供有限的但只是通常有用的设施，由引用一些实体属性对实体定位(如，在特定领域中寻找某个x应用的x服务器的实体集；或者联编到第一个x服务器可利用的实例)。

H2.4 引用客体访问

几种办公应用将作为客体的源或汇集，如文卷、文件或P2正文部分。

大量数据客体值的传送在概念上包括三方面：要求和组织这个传送的用户，生产数据客体值的源和消费数据客体值的汇集。

在两方传送中，用户可以是源也可以是汇集，和第二方分别是汇集或源。在某些情况中，用户可以是中间汇集和往后的同一数据客体值的中间源，即数据客体值从源传送给用户，往后从用户传送给汇集。在此情况中，如果用户组织从源到汇集的一个(直接)数据传送，它更有效。

使用类似“高级程序设计语言”，汇集和源服务的远程操作在两方传送的情况下使用“按值的自变量或结果”技术，同时在通过引用数据传送情况下使用“按引用的自变量或结果”技术。

引用客体访问不代替在服务器之间所有其它类型的相互作用。特别地，当相同x应用的x服务器需要有一些不同于简单数据传送的相互作用时，对给定应用可定义特别x系统协议。

当不同应用服务器需要有一些不同于在附录D3.3.2、第D6章和第D7章中描述的简单数据传送的相互作用时它们使用访问协议。

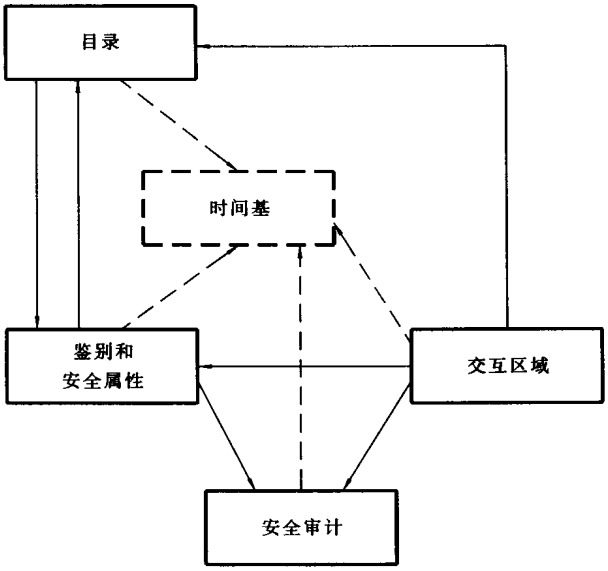
H2.5 在支持的应用之间的相互作用

在支持的应用之间有许多相互作用。本条描述最重要的一个。

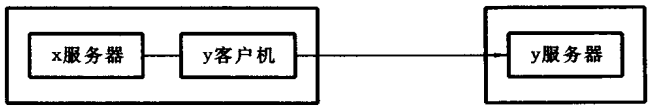
每个支持的应用使用时基。这些相互作用通过在图H1的图形和箭头描述。得到时间的方法超出本标准的范围。当时间是局部可用的，通过局部方法来访问它；唯一要求是与时基同步的一个交互作用，这在H2.1中解释。

目录应用使用鉴别和安全属性应用以便目录鉴别它的用户。这是类型2相互作用。

如果鉴别和安全属性应用被分布在许多服务器之间，则它的任何服务器作为用户与目录应用互相作用，去查找这个应用的另一服务器的表示地址(类型2相互作用)。



注：给出的框线和箭头代表下列客户机/服务器的关系。



图H1 支持应用之间的交互作用

H3 生产的应用支持

H3.1 引言

本章以辅导形式描述生产应用如何使用支持的应用。例子包括信报传送、信报存储、文件归档和检索，及文件打印应用。

在此描述的支持的相互作用对这些生产应用的人用户来说一般是不可见的，即对人用户不要求必须明确规定这些交互作用。

交互作用类型在下列条中提及，它在附录D的第D6章中描述。

H3.2 信报传送应用支持

H3.2.1 信报传送应用描述

信报传送应用使它的用户能够发送和接收不同长度和内容的信报。信报传送应用对分布式办公应用系统的所有用户都是直接可访问的，允许在被较近或较远的物理距离所分开的用户之间互换信报。从发送者到接收者的信报传送以存储和转发的方法运行。

信报传送应用在GB/T 16284.3中定义。

信报传送应用可以提供特定设施，如支持分布表，在一个名字下把许多接收者组成组。

H3.2.2 信报传送应用操作

信报传送应用要求从时间基、鉴别、安全属性应用和目录应用中得到支持。

下列交互作用可以包括在信报传送应用的典型使用中：

a) 信报传送应用用户访问时基；

b) 信报传送应用用户访问目录应用以获得信报传送服务器(交互作用类型1)的表示地址；

c) 信报传送应用用户访问鉴别和安全属性应用以获得访问信报传送服务器的安全属性(交互作用类型1)；

d) 信报传送应用用户提交信报给信报传送服务器；

e) 信报传送服务器访问鉴别和安全属性应用，鉴别信报传送应用用户(交互作用类型2)；

f) 信报传送服务器访问时基以生成每个信报的时间邮戳；

g) 信报传送服务器访问目录应用，扩展任何在分布表上的“接收者”(交互作用类型2)；

h) 信报传送服务器访问目录应用，获得每个接收者的信报存储器服务器的表示地址(交互作用类型2)。

H3.3 信报存储(MS)的支持

H3.3.1 信报存储访问的描述

信报存储应用是紧紧结合着信报传送应用的。信报传送应用事实上是把信报投送到“邮箱”，邮箱同用户联系，同时信报存储应用允许用户获得邮件。信报存储应用在GB/T 16284.5中定义。

H3.3.2 信报存储应用的操作

信报存储应用要求从时间基、鉴别、安全属性应用和目录应用中得到支持。

下列交互作用可以包括在信报存储应用的典型使用中：

a) 如在GB/T 16284.2中信报用户代理(UA)访问时间基；

b) 用户代理访问目录应用，获得信报存储的表示地址(交互作用类型1)；

c) 用户代理访问鉴别和安全属性应用，获得访问信报存储的安全属性(交互作用类型2)；

d) 用户代理请求来自信报存储的邮件信报；

e) 信报存储可以访问鉴别和安全属性应用，鉴别用户代理(交互作用类型2)；

f) 信报存储使用鉴别设施检查是否许可访问；

g) 信报存储返回信报给用户。

H3.4 文件归档和检索应用支持

H3.4.1 文件归档和检索应用描述

文件归档和检索应用提供大容量文件存储归档和检索的能力给分布式系统中的多用户。

文件归档和检索应用也提供对占有文件的访问控制。

H3.4.2 文件归档和检索应用的操作

在安全领域中文件归档和检索应用要求从时间基和鉴别和安全属性和目录应用中得到支持。

下列交互作用可以包括在文件归档和检索应用(此例中为检索)的使用中,它们是:

a) 文件归档和检索应用用户访问时基;

b) 文件归档和检索应用用户访问目录应用,获得它要求的文件归档和检索服务器的表示地址(交互作用类型 2);

c) 文件归档和检索应用用户访问鉴别和安全属性应用,获得为访问文件归档和检索应用服务器的安全属性(交互作用类型 1);

d) 文件归档和检索应用用户从文件归档和检索应用中要求文件;

e) 文件归档和检索服务器可以访问鉴别和安全属性应用,鉴别文件归档和检索应用用户(交互作用类型 2);

f) 文件归档和检索应用给文件归档和检索应用用户返回文件。

H3.5 文件打印应用支持

H3.5.1 文件打印应用描述

文件打印应用为分布式系统中的多用户提供共享贵的、高级设施映象设备的能力。

H3.5.2 文件打印应用的操作

在安全领域中文件打印应用要求从时间基和鉴别和安全属性和目录应用中得到支持。

下列交互作用可包含在文件打印应用的使用中(在此例中,打印文件):

a) 文件打印应用用户访问时基;

b) 文件打印应用用户访问目录应用,获得它要求的打印服务器的表示地址(交互作用类型 1);

c) 文件打印应用用户访问鉴别和安全属性应用,获得使用打印服务器的安全属性(交互作用类型 1);

d) 打印服务器访问鉴别和安全属性应用,鉴别文件打印应用用户(交互作用类型 2);

e) 文件打印应用用户发送文件给打印服务器;

f) 打印服务器为文件打印排队;

g) 文件打印应用通告文件打印应用用户完成了请求。

附 录 J
(提示的附录)
客 体 模 型

J1 引言

客户机和服务器两者都被认为包含客体。

客体所有外部可视行为在客体类型规范中描述。由相同客体类型规范描述的客体说成是客体类型的事例。客体类型规范是类型操作的集,每一个是独特的和逻辑上完成的。每种类型操作在抽象级别上规定,它定义发生了什么,而不是怎样发生的。

类型操作的效果取决于客体状态;从前面实现的类型操作的子集得到状态。客体状态的改变和对类型操作的效果在客体类型规范中描述。

x 服务器由一个或多个各种客体类型的集合所模型化。这些客体称为 x 服务器客体。x 服务器的外

部可视行为由客体集合中的x服务器客体的客体类型规范描述。类似地,x客户机外部可视行为由客体类型规范来描述。这些客体称为x客户机客体。所有在客户机和服务器之间的交互作用由x服务定义描述,x服务定义全部从服务器和客户机的客体类型规范中派生出来。

在客户机调用和服务器调用之间的通信工作由联编操作建立。联编操作将交互作用系列限制为:

a) 一个应用上下文,它规定在x服务定义中可用的类型操作的子集和x服务定义中说明的排序规则;

b) x服务器客体实例和可选x客户机客体实例的特殊集。

在交互作用系列中,在由联编操作建立的限制中,对感兴趣的客体实例集,可以有进一步的限制、放松和改变。这些总在由联编操作建立的限制。

联编操作和断联操作在x服务器的客体类型规范中描述,它们是x服务定义的部分。

根据较近的检查,x客户机客体或x服务器客体可以包含几个下级客体。这些下级客体可以有相关的类型操作。交互作用的子系列可以限定这些下级客体的特定集。这些客体的类型操作和这些客体的标识按客体类型规范的类型操作的参数表示。

J2 x服务器和客体事例之间的关系

x系统的服务器客体往后将作为x客体引用。依照x客体的本质,一个或多个x服务器可以参与代表一个x客户机对一个x客户机事例完成类型操作。

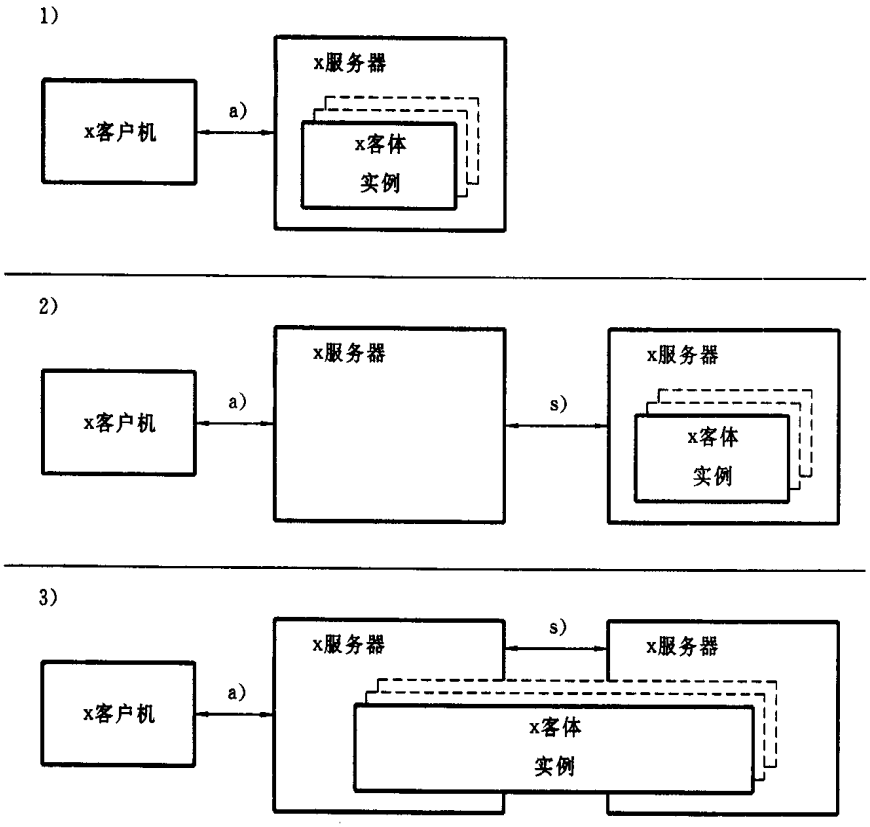
图J1阐明了关于x服务器的x客体事例的三种不同情况:

a) x客体类型的一个或多个事例由同x客户机通信的x服务器完全拥有(例如信报存储器事例由信报存储服务器拥有);

b) x客体类型的一个或多个事例由不是同x客户机通信的x服务器所拥有(例如在目录服务器的信息库中目录信息的部分)。在x服务器之间对x客体事例的访问通过x系统协议或x客户机和x访问协议之一来实现;

c) x客体类型的一个或多个事例由几个x服务器拥有(例如在整个或部分分布式数据库中)。访问客体由共享x服务器来协调,或使用x系统协议,或使用x客户机和x访问协议。

从x客户机的观点看,这三种情况没有不同。使用x访问协议,x客户机简单地规定涉及与x客户机通信的x服务器的类型操作。每个分布式办公应用不必都支持上面三种情况。



a) x 访问协议

s) x 系统协议或 x 客户机和 x 访问协议

图 J1　服务器和客体事例

附　录　K
（提示的附录）
操作的标准集

K1　引言

本附录给出在本标准 6.6 中介绍的 DOA 抽象操作的标准集的详细例子。

下列是抽象操作的集：

a）列表；

b）读；

c）修正；

d）拷贝；

e）移动；

f）搜寻；

g）创建；

h）删除；

i）保留；

j）通告；

k）放弃。

K2 每个操作的描述

注

1 “客体的标识符”是标识一个客体的客体名或DOR。

在消费操作或访问操作情况中，使用DOR。

2 所有操作可以包括操作特定的安全控制信息。

K2.1 列表

列表操作用于得到在指定客体中成分的列表。

列表操作的自变量可以包括下列成分：

a) 客体标识符；

b) 选择符；

c) 请求的属性；

d) 请求指示(请求的客体的值或DOR)。

列表操作结果可包括下列成分：

a) 列表的值或列表的DOR。

K2.2 读

读操作用于得到值或DOR，和指定客体的属性。

读操作的自变量可以包括下列成分：

a) 客体标识符；

b) 选择符；

c) 请求的属性；

d) 请求指示(请求的客体的值或DOR)。

读操作的结果可包括下列成分：

a) 读出的客体值或要被读的客体的DOR。

K2.3 修正

修正操作用于改变指定客体的值和/或属性。

修正操作的自变量可以包括下列成分：

a) 客体的标识符；

b) 改变(移去、替换或增加)。

修正操作的结果不需包括任何成分。

K2.4 拷贝

拷贝操作用于拷贝客体。

拷贝操作的自变量可以包括下列成分：

a) 客体的标识符；

b) 选择符；

c) 请求的属性；

d) 目的客体的标识符；

拷贝操作的结果不需包括任何成分。

K2.5 移动

移动操作用于移动客体。

移动操作的自变量可以包括下列成分：

a) 客体的标识符；

b) 选择符；

c) 请求的属性；

d）目的客体的标识符。

移动操作的结果不需包括任何成分。

K2.6 搜寻

搜寻操作用于标识客体，这些客体匹配于特定条件并在指定目的客体中放置结果。

搜寻操作的自变量可以包括下列成分：

a）客体的标识符；

b）选择符；

c）请求的属性；

d）目的客体的标识符；

e）请求指示（请求的客体的值或DOR）。

搜寻操作的结果可以包括下列成分：

a）目的客体的标识符。

K2.7 创建

创建操作用于创建一个客体。它可以允许客体值和属性的任选赋值。

创建操作的自变量可以包括下列成分：

a）客体的标识符；

b）提供的属性；

c）客体和/或属性的值；

d）请求指示（请求的客体的值或DOR）。

创建操作的结果可以包括下列成分：

a）客体的标识符。

K2.8 删除

删除操作用于删除客体。

删除操作可以包括下列成分：

a）客体的标识符；

b）选择符。

删除操作结果不需包括任何成分。

K2.9 保留

保留操作用于“锁定”客体，防止其他用户检索或删除锁定的客体。

保留操作的自变量可以包括下列成分：

a）客体标识符；

b）请求的行动（保留或不保留）。

保留操作结果不需包括任何成分。

K2.10 通告

通告操作用于给出关于特定客体状态改变的信息。

通告操作的自变量可以包括下列成分：

a）客体的标识符。

通告操作的结果不需包括任何成分。

K2.11 放弃

放弃操作用于放弃一个最初请求任务（如搜寻）的执行。

放弃操作的自变量标识任务。

放弃操作的结果不需包括任何成分。