

IBM® DCE for AIX® and Solaris  
バージョン 3.2



管理ガイド - 入門



IBM® DCE for AIX® and Solaris  
バージョン 3.2



管理ガイド - 入門

**ご注意!**

本書をご使用になる前に、103ページの『付録D. 特記事項』にある一般的な情報を必ずお読みください。

本書は、*IBM DCE for AIX and Solaris* バージョン 3.2 に適用されます。また、改訂版等で特に断りのない限り、これ以降のすべてのリリースにも適用されます。

本書の記述および本書に関連するソフトウェアの一部は、以下の会社または団体に帰属しています。

Copyright © 1995, 1996 Open Software Foundation, Inc.

Copyright © 1990, 1991, 1992, 1993, 1994, 1995, 1996 Digital Equipment Corporation

Copyright © 1990, 1991, 1992, 1993, 1994, 1995, 1996 Hewlett-Packard Company

Copyright © 1989, 1990, 1991, 1992, 1993, 1994, 1995, 1996 Transarc Corporation

Copyright © 1990, 1991 Siemens Nixdorf Informationssysteme AG

Copyright © 1988, 1989, 1995 Massachusetts Institute of Technology

Copyright © 1979, 1980, 1983, 1986, 1988, 1989, 1991, 1992, 1993, 1994 The Regents of the University of California

Copyright © 1995, 1996 Hitachi, Ltd.

プログラムの使用者は、適用されるすべての法律、規則、規制を遵守すること、およびプログラムの配布者に対しても遵守を要求することに同意するものとします。これらの法律、規則、規制は、(i) ライセンス・プログラムまたは文書を輸出または再輸出する場合に適用される技術データの輸出または再輸出に関するもの、(ii) ライセンス・プログラム、文書、技術データについての政府機関の権限を制限するために要求される次のような内容の「権利制限表示」をライセンス・プログラム、文書、技術データに添付することに関するものです。「権利制限表示」の内容は次のとおりです。「米国政府による使用、複写、開示は DFARS 52.227-7013(c)(1)(i)-(ii); FAR 52.227-19; および FAR 52.227-14, Alternate III, または他の連邦政府法規にある同内容の条項で定めるところにより、制限されます。」

本マニュアルに関するご意見やご感想は、次の URL からお送りください。今後の参考にさせていただきます。

<http://www.ibm.com/jp/manuals/main/mail.html>

なお、日本 IBM 発行のマニュアルはインターネット経由でもご購入いただけます。詳しくは

<http://www.ibm.com/jp/manuals/> の「ご注文について」をご覧ください。(URL は、変更になる場合があります)

原典： IBM® Distributed Computing Environment Version 3.2 for AIX® and Solaris Administration Guide-Introduction

発行： 日本アイ・ビー・エム株式会社

担当： ナショナル・ランゲージ・サポート

第1刷 2001.3

この文書では、平成明朝体™W3、平成明朝体™W9、平成角ゴシック体™W3、平成角ゴシック体™W5、および平成角ゴシック体™W7を使用しています。この(書体\*)は、(財)日本規格協会と使用契約を締結し使用しているものです。フォントとして無断複製することは禁止されています。

注\* 平成明朝体™W3、平成明朝体™W9、平成角ゴシック体™W3、平成角ゴシック体™W5、平成角ゴシック体™W7

© Copyright International Business Machines Corporation 1990, 2001. All rights reserved.

Translation: © Copyright IBM Japan 2001

# 目次

図 . . . . .	vii
表 . . . . .	ix
本書について . . . . .	xi
本書の対象読者 . . . . .	xi
適用範囲 . . . . .	xi
本書の目的 . . . . .	xi
本書の使用方法 . . . . .	xi
関連資料 . . . . .	xii
本書で使用される規則 . . . . .	xii
問題の報告 . . . . .	xiii
DCE の資料にあるディレクトリーおよびファイルのパス名 . . . . .	xiii

---

## 第1部 DCE システム管理の紹介 . . . . . 1

<b>第1章 管理者のための DCE 紹介 . . . . .</b>	<b>3</b>
クライアントおよびサーバー . . . . .	3
リモート・プロシージャ・コール . . . . .	4
セル . . . . .	4
ネーム・スペース . . . . .	5
ファイル・スペース . . . . .	5
プリンシパル . . . . .	6
アクセス制御リスト . . . . .	6
キャッシング . . . . .	7
複製 . . . . .	7
環境変数 . . . . .	7
<b>第2章 グローバルおよびセルの考慮事項 . . . . .</b>	<b>9</b>
セル名の設定 . . . . .	11
DNS セル名の設定 . . . . .	11
セル・ネーム・スペース . . . . .	12
セル境界の決定 . . . . .	12
セルの安定保持 . . . . .	12
セル・ネーム・スペース・エントリーのタイプ . . . . .	13
CDS ネーム・スペース複製の考慮事項 . . . . .	16
アクセス制御の計画 . . . . .	16
<b>第3章 クライアントおよびサーバーの考慮事項 . . . . .</b>	<b>19</b>
DCE クライアント・マシンの要件 . . . . .	19
RPC クライアント・プログラム . . . . .	19
セキュリティー・サービス・クライアント・プログラム . . . . .	20
監査サービス・クライアント・プログラム . . . . .	20
CDS クライアント・プログラム . . . . .	20
DTS クライアント・プログラム . . . . .	21
スリム・クライアント・プログラム . . . . .	21
DCE サーバー・マシンの要件 . . . . .	24
DCE サーバー・マシンにインストールするファイル . . . . .	24
DCE RPC サーバー・プログラム . . . . .	24

セキュリティ・サーバー・プロセス	24
監査サーバー・プロセス	25
CDS および GDA サーバー・プロセス	25
DTS サーバー・プログラム	26
イベント管理サービス (EMS) プロセス	27
DCE 管理ユーティリティ	28
DCE 制御プログラム	28
DCE RPC 管理プログラム	28
セキュリティ・サービス管理プログラム	28
CDS 管理プログラム	29
DTS 管理プログラム	29
DCE リモート管理マシンのためのプログラム	29
アプリケーション開発環境マシン	30
<b>第4章 DCE ファイルのインストール場所</b>	<b>31</b>
/opt/dcelocal サブツリー	31
従来の UNIX ディレクトリー (AIX のみ)	32
ファイル・システム	32
ファイルの場所	32
AIX の場合	32
Solaris の場合	33
実行時に作成される構成ファイル	34
作成およびマウントするファイル・システム (AIX のみ)	35
DCE デーモンのコア場所	35
<b>第5章 DCE 保守の概要</b>	<b>37</b>
DCE マシンのネットワーク・アドレスの変更	37
CDS 保守作業	37
CDS のモニター	38
CDS の管理	38
CDS セキュリティおよびアクセスの制御	39
DTS 保守作業	39
分散タイム・サービスの管理	40
システム時刻の変更	40
セキュリティ・サービス保守作業	41
セキュリティ・サービスの管理	41
レジストリーの再構成	43
有効期限が切れた認証ファイルの削除	43

---

## 第2部 追加構成情報 . . . . . 45

<b>第6章 構成応答ファイル</b>	<b>47</b>
DCE 応答ファイルのキーワード	47
セル・セクション・キーワード	48
ホスト・セクション・キーワード	49
マシンを識別するためのキーワード	50
コンポーネント・キーワードの値	50
<b>付録A. 初期 CDS サーバーの移動</b>	<b>55</b>
<b>付録B. 環境変数</b>	<b>57</b>
監査変数	57
構成	59

EMS . . . . .	59
IDL . . . . .	60
NLS/セキュリティー . . . . .	61
RPC . . . . .	62
セキュリティー . . . . .	69
<b>付録C. DCE セル・ネーム・スペース . . . . .</b>	<b>73</b>
CDS スペース . . . . .	73
最上位レベル CDS ディレクトリー . . . . .	74
CDS ホスト・ディレクトリー . . . . .	78
CDS subsys ディレクトリー . . . . .	82
セキュリティー・スペース . . . . .	84
最上位セキュリティー・ディレクトリー . . . . .	86
sec/group ディレクトリー . . . . .	89
sec/group/subsys ディレクトリー . . . . .	92
sec/principal ディレクトリー . . . . .	96
sec/principal/hosts ディレクトリー . . . . .	100
<b>付録D. 特記事項 . . . . .</b>	<b>103</b>
商標 . . . . .	105
索引 . . . . .	107







1.	クライアントとサーバーの対話 . . . . .	4
2.	セル・ネーム・スペースの最上位レベル . . . . .	14
3.	最上位レベル CDS ディレクトリー . . . . .	74
4.	CDS ホスト・ディレクトリー . . . . .	74
5.	最上位セキュリティー・ディレクトリー . . . . .	85
6.	sec/group ディレクトリー . . . . .	85
7.	sec/principal ディレクトリー . . . . .	86



# 一 表

1.	DCE セル・キーワード	49
2.	DCE ホスト・キーワード	50
3.	ホスト識別値	50
4.	コンポーネント・キーワード	51
5.	コンポーネント一般キーワード	51
6.	アカウント・キーワード	52
7.	公開鍵証明キーワード	52
8.	LDAP レジストリー・キーワード	52



---

## 本書について

*IBM DCE for AIX and Solaris* バージョン 3.2: 管理者ガイド では、分散コンピューティング環境 (DCE) の IBM® for AIX® and Solaris バージョンを管理するための概念と手順を説明します。基本的な DCE の用語は、この手引きで紹介されています。DCE 文書すべての用語集は、*IBM DCE for AIX and Solaris* バージョン 3.2: DCE 入門 に記載されています。*IBM DCE for AIX and Solaris* バージョン 3.2: DCE 入門 は DCE テクノロジーを十分に理解していただくためのもので、DCE をサポートしている資料セットを説明しています。

---

## 本書の対象読者

本書は、前に UNIX® 環境を管理していたシステム管理者とネットワーク管理者を対象としています。

---

## 適用範囲

このバージョンは、*DCE for AIX and Solaris* バージョン 3.2 オファリングおよび関連する更新項目に適用されます。(詳細は、ソフトウェア・ライセンスを参照してください。)

---

## 本書の目的

この手引きの目的は、システムおよびネットワーク管理者が DCE の計画、構成、および管理作業を実行できるようにすることです。この手引きを読んだ後、DCE を計画するためにシステム管理者は何をする必要があるかを理解できます。システムに DCE ソース・コードを構築したならば、実行可能ファイルをインストールし、DCE を構成するための手引きとしてこの手引きを使用してください。

---

## 本書の使用法

*IBM DCE for AIX and Solaris* バージョン 3.2: 管理者ガイド は 2 つのブックで構成されています。

- *IBM DCE for AIX and Solaris* バージョン 3.2: 管理ガイド-入門
  - 1ページの『第1部 DCE システム管理の紹介』
  - 45ページの『第2部 追加構成情報』
- *IBM DCE for AIX and Solaris* バージョン 3.2: 管理ガイド--コア・コンポーネント
  - 第 1 部 DCE 制御プログラム
  - 第 2 部 DCE 管理作業
  - 第 3 部 DCE ホストおよびアプリケーションの管理
  - 第 4 部 DCE セル・ディレクトリー・サービス
  - 第 5 部 DCE 分散タイム・サービス
  - 第 6 部 DCE セキュリティー・サービス

---

## 関連資料

分散コンピューティング環境に関する追加情報は、次の資料を参照してください。

- *IBM DCE for AIX* バージョン 3.2: 概説とインストール AIX 版
- *IBM DCE for Solaris* バージョン 3.2: 概説とインストール Solaris 版
- *IBM DCE for AIX and Solaris* バージョン 3.2: DCE 入門
- *IBM DCE for AIX and Solaris* バージョン 3.2: 管理コマンド・リファレンス
- *IBM DCE Version 3.2 for AIX and Solaris: Application Development Reference*
- *IBM DCE Version 3.2 for AIX and Solaris: Application Development Guide—Introduction and Style Guide*
- *IBM DCE Version 3.2 for AIX and Solaris: Application Development Guide—Core Components*
- *IBM DCE Version 3.2 for AIX and Solaris: Application Development Guide—Directory Services*
- *OSF DCE/File-Access Administration Guide and Reference*
- *OSF DCE/File-Access User's Guide*
- *IBM DCE Version 3.2 for AIX and Solaris: Problem Determination Guide*
- *OSF DCE Testing Guide*
- *OSF DCE/File-Access FVT User's Guide*
- *Application Environment Specification/Distributed Computing*
- *IBM DCE for AIX* バージョン 3.2: リリース情報 AIX 版
- *IBM DCE for Solaris* バージョン 3.2: リリース情報 Solaris 版
- *IBM DCE for AIX and Solaris* バージョン 3.2: DCE セキュリティー・レジストリーと LDAP 統合

IBM DCE 3.2 for AIX and Solaris 資料の詳細な説明は、*IBM DCE for AIX and Solaris* バージョン 3.2: DCE 入門 を参照してください。

---

## 本書で使用される規則

本書では、印刷字体に関する次の規則を使用しています。

**太字** 太字の語または文字は、コマンド、オプション、パス名のように、表示されているとおりに使用する必要があるシステム要素を示します。

**イタリック**

イタリックのワードおよび文字は、指定が必須の変数値を表しています。また、イタリック・タイプは新しい DCE 用語を紹介する場合にも使用されます。

**モノスペース**

システムが表示する例および情報はモノスペース体で示されています。

[ ] 大括弧は、形式および構文記述の中の任意選択項目を囲みます。

{ } 中括弧は、形式および構文記述の中から項目を 1 つ選択する必要があるリストを囲みます。

| 垂直バーは選択項目のリストの中の項目を区切ります。

- < > 不等号記号はキーボード上のキーの名前を囲みます。
- ... 水平の省略記号は、その前の項目を 1 回、または複数回繰り返すことができることを示します。

#### *dcelocal*

本書で使用されている OSF 変数 *dcelocal* は、AIX および Solaris 変数 **/opt/dcelocal** と等価です。

#### *dceshare*

本書で使用されている OSF 変数 *dceshare* は、AIX および Solaris 変数 **/opt/dcelocal** と等価です。

本書では、キー入力に対しては次の規則を使用しています。

#### <Ctrl- x> または $\hat{x}$

<Ctrl-x> または  $\hat{x}$  の後ろにキーの名前が続いている場合は、制御文字の順序を表しています。たとえば、<Ctrl-C> は制御キーを押し続けたままで <C> を押すことを意味します。

#### <Return>

<Return> という記法は、Return または Enter という単語または左矢印が付けられた端末あるいはワークステーションのキーを指します。

---

## 問題の報告

ソフトウェアまたは資料に何らかの問題がある場合は、お客様のソフトウェア・ベンダーのお客様窓口の部門にご連絡ください。

---

## DCE の資料にあるディレクトリーおよびファイルのパス名

本書で参照されているディレクトリーおよびファイルのパス名の一覧は、31ページの『第4章 DCE ファイルのインストール場所』 および *OSF DCE Testing Guide* を参照してください。





---

## 第1部 DCE システム管理の紹介



---

## 第1章 管理者のための DCE 紹介

*IBM DCE for AIX and Solaris* バージョン 3.2: *DCE 入門* は、分散コンピューティング環境の IBM AIX および Solaris バージョン (IBM DCE 3.2 for AIX and Solaris) を紹介し、そのサービスの主なコンポーネントを説明します。この章は、システムまたはネットワーク管理者の観点から DCE の概要を説明します。

*IBM DCE for AIX and Solaris* バージョン 3.2: *DCE 入門* で説明しているように、DCE は高度で一貫性のある分散アプリケーション開発および実行環境を構成するサービスのセットです。これらのサービスは、DCE 管理作業をサポートする 1 組のツールを含んでいます。DCE は、単一マシンまたは他の分散システムのアプリケーションでの作業で学習した技法と同じ技法を適用しています。これらの技法により、システム管理者がシステムの内部について知らなくとも DCE を管理できます。初期の要件に適切な構成から開始し、信頼性または柔軟性を損なわずに構成を拡張できます。DCE は、小規模ネットワークだけでなく、多くのユーザーが使用する大規模ネットワークもサポートします。

この章の後続の節で説明する以下の概念は、DCE システム管理の中核をなすものです。

- サービスの要求を行い、それに応答するクライアントとサーバー
- クライアントからサーバーへの通信のためのリモート・プロシージャ・コール (RPC)
- セキュリティー、管理、およびネーミングの境界を共用する、ユーザー、サーバー、およびマシンのグループであるセル
- クライアント・アプリケーションが、ユーザー、マシン、サーバー、サーバーのグループ、およびディレクトリーを含むオブジェクトを識別し、突き止め、管理できるようにする単一のネーム・スペース
- 正しい許可を持つユーザーおよびマシンの中で、データを共用できるようにする単一のファイル・スペース
- プリンシパル。他のエンティティーとセキュリティを保持して通信できるエンティティー (ユーザー、サーバー、およびコンピューターなど)
- アクセス制御リスト (ACL)。オブジェクトに対するアクセスの制御
- センターに保管されている情報を、必要なたびに探索することを避けるため、情報のローカル・コピーを使用する技法であるキャッシング
- 複製。情報のコピーを作成しその一貫性を保つプロセス

---

### クライアントおよびサーバー

DCE はクライアント / サーバー・モデルに基づいています。サーバーは、他のマシンまたはプロセスに特定のサービスを提供するマシンまたはプロセスです。クライアントは、自分自身の作業中に、サーバーの特定のサービスを使用するマシンまたはプロセスです。分散アプリケーションは、サービスの要求を開始するクライアント側と、要求を受け取って実行し、結果をクライアントに戻すサーバー側から構成されます。たとえば、あるクライアントがファイルの印刷を要求し、プリンターが常駐しているサーバーがその要求を実行します。

複数のサーバー・プロセスが、単一マシンに常駐できます。また、1つのマシンがクライアントとサーバーの両方であることも可能です。たとえば、1つのマシンがある DCE コンポーネントにとってはクライアントとなり、別のコンポーネントにとってはサーバーとなることが可能です。

図1 は、ネーム要求を出すクライアントのネーム・サーバーであるマシンを示したものです。同じマシンがファイル・サーバーにとってはクライアントです。

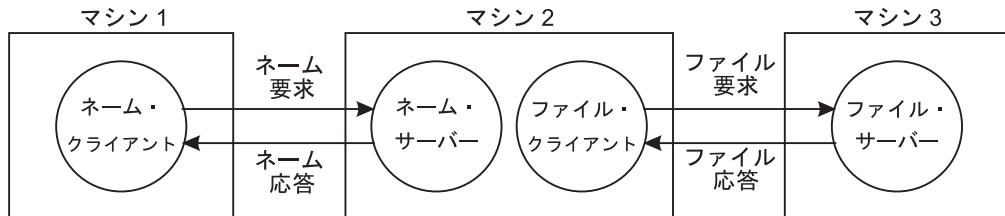


図1. クライアントとサーバーの対話

---

## リモート・プロシージャ・コール

リモート・プロシージャ・コール (RPC) は、ローカル呼び出しプログラムとリモート・プロシージャの間の同期要求と応答です。RPC は、リモート・プロシージャを使用するローカル呼び出しプログラムからの要求で始まり、呼び出しプログラムがプロシージャからすべての結果 (あるいはエラー状態または例外) を受け取ったときに完了します。

---

## セル

セルは、DCE 内の管理の基本単位です。セルは通常、セルの外側のユーザー、マシン、およびリソースよりも、大きなレベルの信頼を互いに持ち、共通の目的を共有する、ユーザー、マシンおよびリソースから構成されます。セルのメンバーは通常、共通の地理的領域に置かれますが、適切に接続すれば、別のビル、別の都市、または別の国に置くことも可能です。セルのサイズは、組織のサイズによって、1つのマシンから数千のマシンまでの広範囲にわたります。組織内のすべてのマシンを1つのセルに組み込むことも、1つの組織内に多くのセルを組み込むことも可能です。

セルは、ユーザーおよびリソースに関するセキュリティ、管理、およびネーミングの境界を指定します。各セルは1つの名前を持ちます。セル名は、DCE コンポーネントをインストールし構成する時に設定します。

同じプロジェクトで作業する組織のメンバーは、おそらく同じセルに属する可能性が大きいといえます。たとえば、複数のセルを持つ大きな組織内で、販売チームが1つのセルに属し、プロジェクト X で作業している技術者が2番目のセルに属し、プロジェクト Y で作業している技術者が3番目のセルに属することがあります。一方、小さな組織では、販売チームと技術者チームが同じセキュリティ要件

を持ち、追加のセルの維持管理に必要な管理上のオーバーヘッドを帳消しにするほど組織のサイズが大きくないので、1つのセルしか持たない場合があります。

DCE サービスは、次の例に示すように、1つのセルのコンテキスト内で管理されます。

- 各 DCE セルは、一般的に、少なくとも1つのセル・ディレクトリー・サービス (CDS) サーバー、3つの分散タイム・サービス (DTS) サーバー、および1つのセキュリティ・サービス・サーバーから構成されます。
- DCE サービスによって管理される DCE オブジェクトのパス名は、オブジェクトが常駐するセルに対して相対的に表すことができます。
- DTS は、ローカル・サーバーとグローバル・サーバーの両方を持っています。ローカル・サーバーは、ローカル・エリア・ネットワーク (LAN) 内で作動します。グローバル・サーバーは、セル内の任意の場所でタイム・サービスを提供します。

---

## ネーム・スペース

ネーム・スペースは DCE オブジェクトの名前の階層のセットです。階層の最上位レベルは、ディレクトリー・サービスが管理します。いくつかの DCE サービス (現在のところ、セキュリティ・サービスと分散ファイル・サービス (DFS™)) は、ネーム・スペースの自分の部分を管理します。ネーム・スペースの各 DCE オブジェクトは、名前およびその特性を記述している関連属性 (いくつかの情報) で構成されています。これらのオブジェクトには、マシンやアプリケーションのようなリソースが含まれます。

ネーム・スペースには、グローバル・ネーム・スペースとセル・ネーム・スペースがあります。セル・ネーム・スペースにはセル内に登録されているオブジェクトが含まれます。セル・ネーム・スペースの論理的なイメージは階層ツリーであり、最上部にセルのルート・ディレクトリーがあり、セル・ルートの下に、名前が入っている1つまたは複数レベルのディレクトリーがあります。セル・ネーム・スペースは、ディレクトリー・サービスのコンポーネントであるセル・ディレクトリー・サービス (CDS) により管理されます。反対に、グローバル・ネーム・スペースは、ローカル DCE セルから見た場合、他のセルの名前のような、ローカル・セルの外側に登録されているオブジェクトを含んでいます。ドメイン・ネーム・システム (DNS) と呼ばれる非 DCE サービスは、グローバル・ネーム・スペースの別の部分を管理します。

管理ツールは、ネーム・スペースを使用して情報を格納し、DCE サービスを突き止めます。DCE サービスは自分自身の位置をネーム・スペースに示します。ネーム・スペースは、DCE サービスを管理可能なグループに編成する方法を提供します。

---

## ファイル・スペース

セル・ネーム・スペースの一部はファイル・スペースであり、これはファイルとディレクトリーから構成されます。これは多くの異なるマシンに物理的に格納でき、適切な許可を持つ限り、すべてのマシン上のユーザーに使用可能です。ファイル・スペースは、関連ファイルの階層グループであるファイル・セットと呼ばれる単位

で管理します。ファイルがネットワーク内に分散し、異なるサーバー上に存在して管理されていても、ユーザーには単一のファイル・スペースであるように見えます。DCE は、ファイル・セットのバックアップ、移動、複製を支援するための管理ツールを提供します。

セル・ファイル・スペース計画のガイドラインは、*IBM DCE for AIX* バージョン 3.2: 概説とインストール *AIX* 版 および *IBM DCE for AIX, Version 3.1: DFS Administration Guide and Reference* を参照してください。

---

## プリンシパル

DCE プリンシパルは、セキュリティー・サービスにより認証されるアイデンティティです。ユーザーがシステムにログインするとき、ユーザーは自分のプリンシパル名を使用します。プリンシパルはプリンシパルのグループに分けられ、またプリンシパルのグループを含む組織にも分けられます。プリンシパルに関連する情報は、従来 UNIX グループとパスワード・ファイルに保持されていた、ユーザー名、グループ ID、グループのメンバー、ユーザーのホーム・ディレクトリーなどです。デフォルトにより、プリンシパルはセルの境界内で知られています。他のセルの認証サービスを承認していることを示す特殊アカウントを作成することで、他のセルのプリンシパルが自分のセルにセキュリティーを保たれて参加できるようにすることができます。これらの特殊アカウントの作成の説明は、*IBM DCE for AIX and Solaris* バージョン 3.2: 管理ガイド--コア・コンポーネント の『トラスト関係の確立』を参照してください。

---

## アクセス制御リスト

アクセス制御リスト (ACL) は許可機構で、これにより、DCE に対するオブジェクトのアクセスを制御する許可を割り当てることができます。次の DCE オブジェクトは、ACL により保護されています。

- セキュリティー・サービスにより管理されるプリンシパル、およびプリンシパルのグループ
- DFS により管理されるファイルおよびファイル・システム・ディレクトリー
- DTS サーバー
- CDS ディレクトリーおよびエントリー
- 管理オペレーション (たとえば、クリアリングハウスの作成) の使用を制限する ACL を持つ、CDS クライアントおよびサーバー

ACL は、以下について定義する複数の ACL エントリー で構成されます。

- オブジェクトを使用できるのは誰か
- オブジェクトに実行できるのはどのオペレーションか

ファイル・スペース内で、ACL は UNIX システムのファイル保護モデルの拡張です。UNIX ファイル・システムの許可はファイルとディレクトリーの保護に限定されますが、DCE ACL は、各データベース・エントリー、セル・ネーム・スペースに登録されているオブジェクト、およびアプリケーションによって管理されているオブジェクトなどの、他のオブジェクトへのアクセスも制御できます。

---

## キャッシング

ネットワーク上で (たとえば、DCE RPC を使用して) 獲得した情報は、ローカル・マシン上のメモリーまたはディスク・キャッシュに格納できます。この技法は、ネットワーク負荷を削減し、頻繁に必要なとされるデータの探索を早めます。たとえば、ネーム・スペースとファイル・スペースについての情報は、DCE クライアント・マシンによりキャッシュされます。

キャッシングはサービスごとに構成できます。DCE の異なるコンポーネントごとに別のキャッシング機構が使用されます。各コンポーネントには、インストール・システムのパフォーマンスを向上させるための構成可能なオプションがあります。

---

## 複製

複製は、複数のマシンにリソースのコピーを持つことにより、リソースの可用性が向上します。たとえば、複製を使用すれば、1 つのマシン上でデータベースを更新し、ネットワーク内の他のマシン上でも自動的に更新を行わせることができます。データを複製し、レプリカを移動し、更新の頻度を制御できます。セキュリティー・サービス、CDS、および DFS はすべて、特殊アプリケーション用にカスタマイズされた複製機能を備えています。

---

## 環境変数

環境変数は DCE が使用する変数で、顧客が自分自身で設定できます。DCE 環境変数の総合的な説明は、57ページの『付録B. 環境変数』を参照してください。





## 第2章 グローバルおよびセルの考慮事項

『第2章 グローバルおよびセルの考慮事項』から 37ページの『第5章 DCE 保守の概要』までの目的は、DCE の計画、インストール、構成、および保守作業を援助することです。DCE 3.2 for AIX のインストールおよび構成についての詳細は *IBM DCE for AIX* バージョン 3.2: 概説とインストール AIX 版 を、DCE 3.2 for Solaris のインストールおよび構成についての詳細は *IBM DCE for Solaris* バージョン 3.2: 概説とインストール Solaris 版 を参照してください。

この章は、DCE セル・ネームの確立方法を説明します。また、この章はセル・ネーム・スペースの編成方法を説明し、セキュリティーの維持およびセル・ネーム・スペースの構成要素の複製に関するガイドラインも示します。この章の最後の部分では、セルに DFS を組み込むための計画を立てる際に考慮しなければならない事柄を説明します。

分散システムを計画する際には多くの質問に答える必要があります。これらの質問に対する答えが、ユーザー環境の基本要件を決定します。DCE の計画時には、次の大局的な考慮事項を心に留めておいてください。

- 環境は数年後にどの程度拡大していると考えられるか。ネットワークの急速な拡張または比較的ゆっくりした拡張のどちらを予想するか。

環境が急速に拡大すると考えるならば、組織のより小さな単位を表すいくつかのセルを設定することを考えてください。ネットワークが拡張するに伴い、これらの小さな単位を管理できます。*IBM DCE for AIX and Solaris* バージョン 3.2: DCE 入門 で説明したように、各セルのメンバーは共通の目的を共用し、セルは管理およびセキュリティーの単位です。ネットワークのゆるやかな拡張を予想するならば、現存する組織に基づいた 1 つまたは複数のセルを設定することもできます。予想される将来の成長に基づいて、DCE セルを保守するために何人の管理担当者が必要になるかを考慮します。

- 環境には、分散する必要のある情報がどのくらいあるか。ネットワークのユーザーはどの程度の情報を共有しているか。

ネットワーク内で共有する必要のある情報が大量にある場合、必要となるディスク・スペースの量と、必要な DFS ファイル・サーバー・マシンの数を検討します。

- どの程度の情報の更新が必要か。ネットワーク内のユーザーは情報を見るのが主であるのか、あるいはユーザーは自分のワークステーションから情報を作成し、変更するのか。

情報が頻繁に変更され、ネットワークのユーザーがその情報の正確性に依存している場合、どの程度複製を信頼するかを検討する必要があります。頻繁に変更されるデータの場合は、情報のセンターのソースを用いる方がよいです。ユーザーは他のユーザーと共有している情報を見るが、その情報を変更する必要がない場合、複製されたデータの方がより多く用いられます。

- 最も重要なデータは、最も使いやすいデータか。このデータを複製する計画を作成したか。

CDS、セキュリティー・サービス、および DFS は、各データベースのマスター・コピーを維持します。各 CDS ディレクトリーは別々に複製できます。DFS データベースに加えて、個々の DFS ファイル・セットやファイル・セットのグ

ループを複製できます。セキュリティー・サービスはレジストリー・データベース全体を複製します。他のコンポーネントは、セキュリティー・サービスが管理している情報と CDS ネーム・スペースの一部に依存するため、データは常に利用できる必要があります。たとえば、特殊な文字列 *!:* (セル・ルート) は CDS に格納されていて、常に使用可能でなければなりません。

データを複製すると可用性は向上しますが、パフォーマンスおよび必要な管理作業量に影響が出ることに注意してください。

- ネットワークがゲートウェイを持つ場合、サーバーは、これらのサーバーに依存するクライアントと同じゲートウェイの側に位置しているか。

CDS サーバーは定期的にメッセージをブロードキャストし、自分の存在をネットワーク内の CDS クラークに公示します。クラークはこの通知を聞き、サーバーを確認します。サーバーとサーバーに依存するクライアントをゲートウェイの同じ側に置くことは、情報の効率的な更新とクライアント要求への迅速な応答を可能にします。ローカル・エリア・ネットワーク内でのみ有効である公示プロトコルを利用できないサーバーに依存する場合は、追加の管理が必要になります。

地理的に異なる場所にあるユーザーを含むセルを管理する場合、リンクがどの程度の速度になり、どの程度の費用がかかるものかを検討します。リンクをまたがって情報を転送することへの依存度を減らすため、より多くの情報をローカルに保持したいと思われるかもしれません。

- 通信は自分のセルに限定されるか、それとも他のセルと通信する必要があるか。

DCE は、DCE がサポートするグローバル・ディレクトリー・サービスにセルが登録されている標準セル間接続にセルを接続し、そのディレクトリー・サービスに登録されている他のセルと通信します。セルは、DNS ディレクトリー・サービスに登録できます。DNS 名は、セルの別名です。

セルと他のセルとの通信のためにどの方法を使用する場合でも、次の事柄が必要です。

- セルの固有名を確立し、該当するネーム・スペースにその名前を定義する。
- セル内に少なくとも 1 つの GDA を実行させる。
- 通信したい他のセルと、セキュリティー・サービス信頼関係を設定する。

- ご使用の環境中に LDAP があり、LDAP を活用したいと思っているか。

DCE ユーザーを LDAP ディレクトリーに格納する必要がある場合 (たとえば、ユーザーを既存の LDAP ディレクトリーに格納したりそこから読み取ったりするアプリケーションが別にある場合) は、DCE セキュリティー・レジストリーおよび LDAP 統合機能を使用することを考慮できます。

LDAP ベースのセキュリティーを使用して新しく DCE セルを構成するか、または既存のセルを LDAP ベースのセキュリティーにマイグレーションできます。

DCE セキュリティー・レジストリーおよび LDAP 統合機能の詳細な説明は、*IBM DCE for AIX and Solaris* バージョン 3.2: DCE セキュリティー・レジストリーと LDAP 統合 を参照してください。

## セル名の設定

セルの名前を確立してから、その名前を構成します。セキュリティー・サービスのオペレーションには、固有に識別できるセル名が必要です。この名前はセルにおける認証の基礎となるものです。セル名をグローバルで固有にする必要があるかどうかは、他のセルとの通信に関する計画に依存します。

私用セルを作成する場合にそのセルを組織外のセルとの通信に使用しない場合は、グローバルな固有セル名を入手する必要はありません。しかし、他の組織のセルとの通信を計画している場合は、セルにグローバルな固有セル名を入手した後に、セルを構成するようにしてください。

DNS または CDS を介して他のセルとの通信を計画している場合は、そのセルにグローバルな固有名を獲得する必要があります。次のセクションでは、独自のセルの DNS 名を設定する方法を説明します。DNS および CDS でサポートされる有効な文字の説明については、*IBM DCE for AIX and Solaris バージョン 3.2: 管理ガイド--コア・コンポーネント* を参照してください。

## DNS セル名の設定

DCE は DNS を使用することでグローバル・ディレクトリー・オペレーションもサポートします。DNS を使用して他のセルと通信する計画ならば、セルを構成する前に DNS のグローバル名の命名機関から、セルのためのグローバルに固有な名前を入手する必要があります。その後、その名前を DNS ネーム・スペース内に定義します。セルのために入手した名前は、DNS 構文の形です。DNS スタイルのセル名の例は次のとおりです。

```
./.../seattle.abc.com
```

グローバル・ディレクトリー・サービスとして DNS を使用する計画ならば、DCE セル名はサイト名に関して ARPA インターネット・ドメイン・システム規則に従う必要があります。既にインターネットのサイトであるならば、サイトがどう組織化されているかにしたがって、自分のインターネット・ドメイン・ネームに従属する 1 つまたは複数のセルを作成できます。インターネット形式の名前は次の規則に従います。

- 名前には、少なくとも 2 つのレベルが必要です。たとえば、**abc.com** または **sctech.edu** です。最初の 2 レベルの名前は、DNS 名の命名機関であるネットワーク情報センター (NIC) に登録されます。
- 名前は 255 文字よりも長くできません。
- 名前は、2 つの必須のレベルに加えていくつのフィールドを含めてもよく、これらは規則によりピリオドで区切ります。
- 名前は団体の種類を示す接尾部で終わらせる必要があります。この最後のフィールドは、最も重要です。次に、一般的に使用される接尾部をリストします。新しい接尾部が追加されていくので、このリストは包括的なものではありません。
  - **.com** 会社および他の商業組織
  - **.org** 非商業組織
  - **.edu** 教育機関
  - **.gov** 政府機関
  - **.mil** 軍事機関
  - **.net** ネットワーク・サポート組織

- .xx 国際標準化機構 (ISO) に準拠する 2 文字の国コード (ドイツの **.de**、フランスの **.fr** など)

有効な文字、制限、メタ文字、および DNS 名の最大名サイズなどの命名規則の詳細は、*IBM DCE for AIX and Solaris* バージョン 3.2: 管理ガイド--コア・コンポーネント を参照してください。

固有な DNS 名を入手するには、その下にセル名を付けたいサブツリーに責任を持つ管理者に連絡します。

セルを構成した後、DNS 内にそのためのセル・エントリーを作成して、それを DNS グローバル・ネーム・スペース内に定義する必要があります。DNS 内にセル・エントリーを作成するには、管理担当者はリソース・レコードを含むデータ・ファイルを編集する必要があります。

また、通信したい他のすべてのセルと、セル間認証を確立する必要もあります。

---

## セル・ネーム・スペース

DCE セルの計画にとって不可欠な部分は、自分のセル・ネーム・スペースの編成を理解することです。ネットワーク内のセルの編成を計画する際に次のことを考慮してください。

- セキュリティー要件は維持されるか。
- セルの編成は、データ共用の要求が最大の時にネットワーク通信量を受け入れられるか。
- 構成プロセスの間に各 DCE サービス用に作成される管理アカウントをどう管理するか。
- DFS 管理ドメイン (1 つの単位として管理される DFS サーバーのグループ) を何にするか。サーバーをより効率的な管理のためにグループ化できるか。

## セル境界の決定

DCE では、セルの境界はセル・ネーム・スペースの境界と同じです。小さな組織は 1 つのセルで構成できます。大きな組織は多くのセルを持つことができます。セルの境界を決める主要な要素は、セルのプリンシパルにより共有される共通の目的と信頼にあります。セル内のプリンシパルは、同じ特権を共有するグループに属することができます。グループのメンバーは同じレベルの信頼を共有し、あるアクションを実行することを許可されます。

各セルを設定し保守することに関連した 1 セットの管理用作業があるため、組織内のセルの数を最小に保つことが妥当です。しかし、管理のオーバーヘッドよりも、プリンシパルのグループにより共有される信頼レベルの方がより重要な考慮事項です。

## セルの安定保持

必要なセルがいくつかを決め、それらのセルの境界をどこに置くかを決めたら、セルの構造を安定化するための努力をします。サーバーはあるホストから別のホストに簡単に移動することはできません。したがって、再構成を最小限に抑えるため

に、ネーム・スペース構造は慎重に計画してください。マシンを 1 つのセルから別のセルに移動する必要がある場合には、次を実施しなければなりません。

- ホストからサーバー・プロセスを移動する。
- **unconfig.dfs** および **unconfig.dce** コマンドを使用し、古いセルからホストを構成解除する。
- **config.dce** および **config.dfs** コマンドを使用し、新しいセルにホストを再構成する。

## セル・ネーム・スペース・エントリーのタイプ

以下に、セル・ネーム・スペースを構成する様々なエントリー・タイプを説明します。これらのエントリーは、*IBM DCE for AIX* バージョン 3.2: 概説とインストール AIX 版 または *IBM DCE for Solaris* バージョン 3.2: 概説とインストール Solaris 版 で説明されているデフォルト構成パスに従って作成されます。*IBM DCE for AIX and Solaris* バージョン 3.2: 管理ガイド--コア・コンポーネント および *IBM DCE for AIX, Version 3.1: DFS Administration Guide and Reference* では、DCE コンポーネントが使用する名前の詳細を説明しています。セル・ネーム・スペースは、以下の主要な部分に分割できます。

- ネーム・スペースの CDS 部分
- ネーム・スペースのセキュリティー部分
- ネーム・スペースの DFS 部分 (ファイル・スペース)
- ネーム・スペースの **dced** (各ホスト) 部分

DCE サービスのおおのは、セル・ネーム・スペースの中の自分自身のネーム・スペースを保守します。DFS は自分のネーム・スペースを多くのファイル間での整合性を保証するために保守します。セキュリティー・サービスは、DCE セルが安全であることを保証するために自分のネーム・スペースを保守します。これらの 2 つのサービスのクライアントは、バインディング情報を CDS に照会し、これによりセキュリティー・サーバーや DFS サーバーを見つけることができます。バインディング情報が保管されているポイントは、DFS およびセキュリティー・サービスが管理するネーム・スペースのための、CDS ネーム・スペース内のマウント・ポイントとなります。2 つのネーム・スペース間のこの移行点は、ジャンクションと呼ばれます。**./sec** ディレクトリーはセル・ネーム・スペースの CDS 部分からセキュリティー部分へのジャンクションで、**./fs** ディレクトリーはセル・ネーム・スペースの CDS 部分から DFS 部分へのジャンクションです。

ジャンクション **./hosts/hostname/config** は、ネーム・スペースの CDS から **dced** (各ホスト) 部分へのジャンクションです。

14ページの図2 は、セル・ネーム・スペースの最上位レベルを示したものです。場合によっては、セル・ネーム・スペースの名前は固定で (またはウエルノウン)、変更できません。また、リストに示されているものから別の名前を選択することもできます。どの名前がウエルノウンに関する詳細な説明は、*IBM DCE for AIX and Solaris* バージョン 3.2: 管理ガイド--コア・コンポーネント を参照してください。14ページの図2 では、**./** および **cell-profile** がウエルノウン名です。



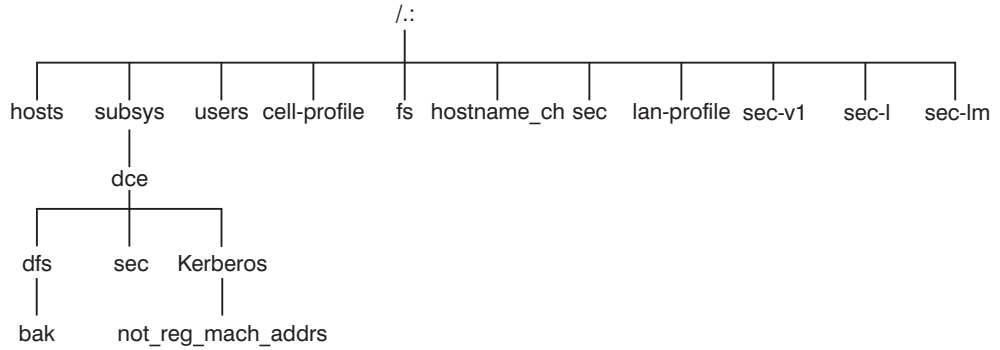


図2. セル・ネーム・スペースの最上位レベル

DCE 制御プログラム (**dcecp**) を使用し、**sec** および **fs** ジャンクションを含め、ネーム・スペースの CDS 部分を表示できます。**ls** などのコマンドを使用してネーム・スペースの DFS 部分の内容を見たり、**dcecp** を使用してセキュリティ部分の内容を見たりすることができます。

### CDS ネーム・スペース・エントリー

CDS ネーム・スペースは、サーバー、ホスト、CDS クリアリングハウス (特定のサーバーに保管されたディレクトリー複製のコレクション)、RPC プロファイル、RPC グループ、およびサブシステムのためのエントリーを含んでいます。エントリーには **directory** という CDS タイプ、つまり**オブジェクト**があり、名前が参照する CDS オブジェクトの種類を示しています。3 番目の CDS タイプである **softlink** は、他のエントリーを指すエントリーです。CDS ディレクトリーは、オブジェクトが保管されるコンテナです。CDS はディレクトリーを使用してオブジェクト・エントリーのグループを編成します。

さらに、CDS ネーム・スペースは他の DCE コンポーネントのために特定のサービス、たとえば、ファイル・セット・ロケーション・データベース (FLDB) に含まれる位置情報などを提供します。FLDB はファイル・セットをそれが存在するファイル・サーバー・マシンにマップするデータベースです。

CDS ネーム・スペースにカタログされたプロファイルは、ディレクトリー・サービスを通して検索パスを指定します。セル・プロファイル (**/\*:/cell-profile**) は、物理位置に関係なく、セルで使用可能なサーバーの場所を格納しています。地理的に分散したセル内では、サーバーは別の市や別の国にさえも設置できます。LAN プロファイルは、地理的な近さが重要である状況で使用できる代替のサーバーを定義します。たとえば、**/\*:/lan-profile** は DTS が使用するデフォルト LAN プロファイルです。このプロファイルは DTS サーバーのローカル・セットのためのエントリーを含んでいます。セルが複数の LAN にまたがっている場合は、**/\*:/lan-profile** の下に別の層を作成し、セルの各部分のプロファイルの位置を指定できます。たとえば、2 つの LAN を含むセルでは、片方の LAN のホストには **lanA-profile** を使用し、別の LAN のホストには **lanB-profile** を使用できます。

### セキュリティ・ネーム・スペース・エントリー

セキュリティ・エントリーのタイプは次のとおりです。

- **principal**: このエントリー・タイプには個別プリンシパルが含まれます。

- **principal** ディレクトリー: このエントリー・タイプには、個別プリンシパルあるいは 1 つまたは複数のプリンシパル・ディレクトリー、あるいはその両方が含まれます。
- **group**: このエントリー・タイプには個別グループが含まれます。
- **group** ディレクトリー: このエントリー・タイプには、個別グループあるいは 1 つまたは複数のグループ・ディレクトリー、あるいはその両方が含まれます。
- **org**: このエントリー・タイプには個別組織が含まれます。
- **org** ディレクトリー: このエントリー・タイプには、個別組織あるいは 1 つまたは複数の組織ディレクトリー、またはその両方が含まれます。
- **policy**: このエントリー・タイプにはセキュリティー・ポリシーが含まれます。

ユーザー (またはアプリケーション) がネーム・スペースのセキュリティー部分にあるエントリーをアクセスしている場合、エントリーの名前のみでセキュリティー・サービスが作業するための十分な情報が提供されます。たとえば、セキュリティー・サーバーはログイン名がネーム・スペースのセキュリティー部分に登録されているプリンシパル名であることが分かります。 `!:/principal_name`、`!..!cell_name/principal_name`、および `principal_name` はすべて、ログインに使用する名前を表す有効な方法です。

注: DCE では最大 1024 バイトのプリンシパル名をサポートしますが、AIX および Solaris では 8 バイトに制限されています。

**dcecp** を使用するときには、操作対象のオブジェクト・タイプを指定した後に、そのオブジェクトを操作します。たとえば、プリンシパル **smith** に関連するアカウント情報を変更するためには、プリンシパルに対するオペレーションの実行を指定した後に、プリンシパル名 **smith** を入力します。 **dcecp** は、以下の 4 つ のオブジェクト・タイプを扱います。

- プリンシパル
- グループ
- 組織
- アカウント

IBM DCE for AIX and Solaris バージョン 3.2: 管理ガイド--コア・コンポーネントでは、プリンシパル、グループ、組織、およびアカウントに関する情報を表示するための **dcecp** 使用方法を説明しています。

セキュリティー・スペースに登録されているオブジェクトの他に、 **dcecp** はネーム・スペース内のすべてのオブジェクトに対しオペレーションを実行します。これらのオブジェクトにオペレーションを実行するためには、以下の例に示されているように、 **dcecp** はオブジェクトの完全修飾パス名を必要とします。

```
!./sec/principal/smith
```

次の指定では不十分です。

```
smith
```

セキュリティー・ネーム・スペースは、ネーム・スペースの以下の部分で構成されています。

- `!./sec/principal`
- `!./sec/group`
- `!./sec/org`

- `./sec/policy`
- `./sec/xattrschemas`

## CDS ネーム・スペース複製の考慮事項

ディレクトリー複製は、CDS ネーム・スペース内の情報をバックアップするための最も信頼できる方法です。CDS データはディレクトリーごとに複製されるので、ディレクトリーを複製すると、その中にあるオブジェクトおよびソフト・リンクのすべてのエントリーは自動的に複製されます。ディレクトリーのレプリカを CDS クリアリングハウスで作成するためには、**dcecp** を使用します。

セル・ネーム・スペースの一部を複製するには、次のガイドラインに従います。

- ルート (`./`) は、クリアリングハウス作成時に自動的に複製されます。
- すべてのネーム・スペースが常に確実に利用できるようにするため、各 CDS ディレクトリーの少なくとも 2 つのコピーを持つべきです。CDS 情報のバックアップに関する詳細な説明は、*IBM DCE for AIX and Solaris* バージョン 3.2: 管理ガイド--コア・コンポーネント を参照してください。

---

## アクセス制御の計画

アクセス制御を計画する際には、セル内のアクセス制御のレベルを、セキュリティが確実に維持される程度までに保つことが重要です。個人の特別なセット、または特別なグループに、セキュリティ・スペースのルート・ディレクトリーにアカウントとグループを作成する許可を与えることができます。DCE 構成時に、**acct-admin** と呼ばれるグループが作成されます。**acct-admin** グループは、セキュリティ・スペースのルート・ディレクトリーにアカウントおよびグループを作成できるただ 1 つのグループです。

セルのセキュリティの適切なレベルを維持しつつ、アクセス制御レベルを設定する時には、DCE サービスを保守する管理担当者の要件を考慮する必要もあります。たとえば、ある人がセル内の DFS の管理に責任がある場合、その人はセキュリティと CDS ネーム・スペースにサーバーの追加が必要になる可能性があります。一方、セキュリティ・サービスの管理責任者はセキュリティ・サーバーを管理しますが、DFS ファイル・スペースを制御しません。

以下は、SMIT または DCE 構成スクリプトを使用して DCE を構成するとき作成されるいくつかのグループです。

- **sec-admin**: このグループは、セキュリティ・サーバー、レジストリー複製、および他のセキュリティ機能を管理します。
- **cds-admin**: このグループは、CDS サーバー、CDS 複製、および他の CDS 機能を管理します。
- **dts-admin**: このグループは、DTS サーバーおよび関連 DTS 機能を管理します。
- **dfs-admin**: このグループは、DFS ファイル・サーバーおよび関連 DFS 機能を管理します。
- **audit-admin**: このグループは、監査デーモンおよび関連監査サービス機能を管理します。

DCE 構成スクリプトにより作成される DCE グループの一覧は、92ページの『`sec/group/subsys` ディレクトリー』を参照してください。



管理グループに加えて、個々のユーザーはレジストリー・データベース内のある情報を制御するための許可が必要です。たとえば、ユーザーは自分のパスワード、ホーム・ディレクトリー、またはログイン・シェ尔を変更できる必要があります。



---

## 第3章 クライアントおよびサーバーの考慮事項

この章は、DCE クライアント・マシン、DCE サーバー・マシンの各種タイプ、DCE リモート管理マシン、および DCE アプリケーション開発環境マシンの構成を説明します。DCE クライアント・マシンはすべての DCE サービスのクライアント・コードを実行できます。DCE サーバー・マシンは、DCE ソフトウェアのある種のセットを実行するよう構成されています。DCE サーバー・ソフトウェア・パッケージは、少なくとも 1 つのデーモンおよびある場合には、DCE コンポーネントのサーバー側を構成する、1 つまたは複数の追加のプログラムで構成されています。DCE サーバー・マシンは、DCE クライアント・ソフトウェアも実行します。DCE リモート管理マシンは、リモート・サーバー管理のために特別に構成されたクライアント・マシンであり、DCE クライアント・ソフトウェアに加えてある種の管理プログラムを含んでいます。DCE アプリケーション開発環境構成は、DCE クライアント・ソフトウェアに加えて、DCE アプリケーション・プログラマーが必要とするファイル (ヘッダー・ファイルなど) を含んでいます。

DCE クライアントおよびサーバーの構成を計画する際には、スペースの必要性について忘れないでください。DCE ソフトウェアの特定の構成を持つマシンは、DCE ソフトウェアとオペレーティング・システム・ソフトウェアの両方のために十分なスペースを必要とします。各種 DCE マシン構成のスペース要件の詳細な説明は、*IBM DCE for AIX* バージョン 3.2: リリース情報 AIX 版 または *IBM DCE for Solaris* バージョン 3.2: リリース情報 Solaris 版 を参照してください。

この章の節の順序は、DCE マシンの構成処理に必要な順序に従っています。

---

### DCE クライアント・マシンの要件

以下に、DCE クライアント・マシンの設定の要件を説明します。また DCE クライアントを構成するためのいくつかの考慮事項についても述べます。すべての DCE マシンは、DCE サーバー・マシンも含めて DCE クライアントであることを覚えておいてください。したがって、適切なサーバー・スペース必要量を DCE クライアント・スペース必要量に追加し、クライアント・マシンのための合計スペース必要量にほぼ達するように、確実に行ってください。

### RPC クライアント・プログラム

DCE クライアントは、次のプログラムを含んでいます。

- **dced** デーモンは、動的バインディングのインターフェースをエクスポートする DCE RPC サーバー・プロセスがあるマシン上で実行されていなければなりません。**dced** デーモンは、(とりわけ他の情報よりも) バインディング情報を登録するために使用されます。

**dced** デーモンは、DCE サービスでそのエンドポイントを **dced** により登録する必要があるため、DCE サービスを構成する前に実行されていなければなりません。1 台のマシンでは、必要な **dced** デーモンは 1 つだけです。実際、これはウェルノウン・ポートを使用するため、一時点には 1 つのマシン上で 1 つしか実行できません。

ネットワーク・インターフェース、ルーティング・サービス、および他のネットワーク・サービスは、DCE RPC が開始する前に使用できる必要があります。

**dced** デーモンは、**start.dce** コマンドにより開始されます。**start.dce** コマンドは、AIX の場合は **/etc/inittab** から、Solaris の場合は **/etc/init.d** から起動することができます。**start.dce** コマンドは、**config.dce** コマンドに **-autostart yes** オプションを指定するか、あるいはこのファイルに **/etc/dce/rc.dce** を追加する (AIX の場合のみ) ことで、ブート時に呼び出すことができます。これにより、マシンがブートされるたびに DCE サービスが起動されるようになります。再ブート時に DCE 3.2 を起動することについては、*IBM DCE for AIX* バージョン 3.2: 概説とインストール AIX 版 または *IBM DCE for Solaris* バージョン 3.2: 概説とインストール Solaris 版 を参照してください。

- DCE 制御プログラム (**dcecp**) は、DCE RPC ソフトウェアを管理および保守します。28ページの『DCE 管理ユーティリティ』は、**dcecp** を説明しています。さらに、**rpccp** はローカル・レジストリーの操作に使用されます。

## セキュリティ・サービス・クライアント・プログラム

各 DCE クライアント・マシンは **dced** デーモンの一部として、セキュリティ妥当性検査サービスを用意しています。このサービスはマシンのプリンシパルの位置を占めます。ほとんどのプリンシパルは対話式ユーザーですが、マシン・プリンシパルはそうではありません。セキュリティ妥当性検査サービスは、マシン上の他のデーモン・プロセスが、マシンのアイデンティティを持って実行しているように見えるよう必要な処理を実行します。

セキュリティ妥当性検査サービスは、マシンのプリンシパルのためのチケット発行チケットを定期的にリフレッシュします。プリンシパルが DCE サービスを使用するためには、DCE クライアント・マシンは有効なチケット発行チケットを持っている必要があります。セキュリティ妥当性検査サービスは、クライアントがセキュリティ・サーバーからチケット発行チケットを要求する時に、セキュリティ・クライアントがセキュリティ・サーバーに実際に連絡しているということをセキュリティ・クライアントに保証するインターフェースもエクスポートします。

## 監査サービス・クライアント・プログラム

監査サービス・クライアント・プログラムはありません。このサービスのクライアントは、監査を使用する DCE サービスのサーバー・プロセスで、たとえば、セキュリティ・サービスの **secd** デーモンです。

## CDS クライアント・プログラム

DCE クライアントは次の CDS プロセスを実行します。

- CDS アドバイザーである **cdsadv** プロセスは、次の操作を実行します。
  - アプリケーションが **cdsd** サーバーを突き止めて通信できるようにします。
  - 必要な CDS クラーク (**cdsclerk**) を開始します。
  - ローカル CDS クラークが共有するキャッシュを作成します。
  - **-p** オプションを使用して、CDS サーバーのプロキシとして実行されます。これは、アドバイザーがサーバー・ブロードキャストを自分自身の LAN に送信できるようにするためです。これは、CDS クライアントがプロキシ・サーバーとして構成されているときに、自動的に実行されます。

- **cdsclerk** は、CDS クライアント・アプリケーションと CDS サーバー間のインターフェースです。クラークは CDS クライアント・アプリケーションを実行するすべてのマシンに存在する必要があります。CDS にアクセスするマシンでは、各 DCE プリンシパルに 1 つの **cdsclerk** プロセスが実行されます。CDS クラークは、クライアント・アプリケーションからサーバーへの要求を扱い、サーバーから返された結果をキャッシュします。サーバー要求の結果はキャッシュされるので、クラークは同じ情報を求めて繰り返しサーバーに行く必要がありません。1 つのマシン上のすべての CDS クラークは 1 つのキャッシュを共有します。1 つのクラークは、同じマシン上で実行される複数のクライアント・アプリケーションをサービスできます。

## DTS クライアント・プログラム

DCE クライアントは次の DTS プロセスを実行します。

- **dttd** デーモンは、クライアントまたはサーバーに設定されます。クライアント・マシンでは、**dttd** はローカル・クロックと同期を取ります。
- DTS ソフトウェアを管理し維持するための DCE 制御プログラム (**dcecp**)。28 ページの『DCE 管理ユーティリティ』は、**dcecp** を説明しています。

## スリム・クライアント・プログラム

通常、クライアント・システムはサーバー・システムに比べメモリーに制限があります。クライアント・システムに DCE ソフトウェアを構成するときは、必要と思われるより多くの DCE デーモンが開始されます。クライアントがセル内の他のシステムに対し DCE サービスを提供していない場合は、これらデーモンにより提供されるすべての機能を必要としない場合があります。DFS クライアントおよび **dceunixd** は、スリム・クライアントと共に実行されます。

スリム・クライアントに関する情報はセル内に保存されていないため、スリム・クライアントを構成するためには **cell-admin** は不要です。スリム・クライアントを構成するには、**config.dce** コマンドを使用します。**start.dce** および **stop.dce** コマンドを使用し、スリム・クライアントをそれぞれ開始および停止します。スリム・クライアントの構成を解除するためには、**unconfig.dce** コマンドを使用します。

スリム・クライアント・オプションを使用すると、クライアント・システムにおける DCE のメモリー消費を抑えることができます。

スリム・クライアントは単一の CDS クラーク・インスタンスとして実行され、他の DCE デーモンは実行されません。単一の CDS クラーク・インスタンスの実行は、クラークに **-n** オプションを指定することで開始されます。これにより、CDS アドバイザーがないクラークが開始されます。これは、スリム・クライアントの構成後に **start.dce** を発行することによって、自動的に実行することができます。

実行可能な他の DCE サービスおよび機能がいくつもある場合は、単一の CDS クラークで十分かどうかという疑問があります。その答えは、大部分の DCE クライアントで必要とする DCE 機能は、次の機能だけです。

- RPC コール (認証ありおよび認証なし)
- DCE ログイン
- CDS 名前探索

RPC コールおよび大部分のログインでは、DCE デーモンは不要です。これらの機能は、単に、RPC 実行時ルーチンとセキュリティー実行時ルーチンを使用するだけです。

CDS 名前探索では、CDS クラークだけが必要です。すべてが備わった DCE では、CDS クラークは CDS アドバイザーにより開始され、CDS アドバイザーが必ず必要となります。しかし、DCE AIX および Solaris バージョン 3.2 では、**cdsclerk** コマンドに **-n** オプションを指定することで 1 つの CDS クラーク・インスタンスが開始され、アドバイザーは不要です。このクラークは、すべてが備わった DCE と異なり、20 分後には終了しません。さらに、クラークをこの方法で開始すると、CDS クライアント・キャッシュの管理について、CDS アドバイザーの役割を引き継ぎます。

アドバイザーがないと、**cdsclerk** は **dcecp** または **cdscp** では管理できません。以下のコマンドは失敗します。

```
cdscp show clerk
cdscp disable clerk
cdscp show cached clearinghouse
cdscp define cached server
cdscp show cached server
cdscp clear cached server
dcecp -c cdscache create
dcecp -c cdscache delete
dcecp -c cdscache show -server
dcecp -c cdscache show -clearinghouse
```

**dced** を構成するサービスのうち、**dced** が DCE クライアント・システムで実行されていないために使用不能になる機能は、次のとおりです。

- **dced** エンドポイント・マッパー・サービス: リモート・プロシーチャー・コール (RPC) を介してアクセスできるサービスを提供しているシステムでは、実行する必要があります。このようなサーバーは、RPC サーバーと呼ばれます。システムが RPC サービスに対し RPC を出すとき、システムは RPC 実行時ルーチンを使用して特定のマシン・アドレスに要求を送信し、希望する RPC サービスを名前により要求します。サービスが用意されているマシンに RPC が到達すると、エンドポイント・マッパー・サービスは該当するサービスを実行する特定のプログラムのエンドポイント (つまりポート番号) へ RPC サービス名をマップします。エンドポイントが分かったら、クライアントは特定の RPC サービスにバインドされ、RPC はそのサービスに直接出すことができますようになります。

すべての DCE クライアント・システムでは RPC を出しますが、大部分の場合はエンドポイント・マッパー・サービスを必要としません。これは、システムが通常は RPC サーバーではないからです。したがって、クライアント・システムでは **dced** を実行しないという RPC 関連の制限は、そのシステムが RPC サーバーにはなれないという制限になります。

- **セキュリティー妥当性検査サービス**: 以下に示す機能を実行します。クライアント・システムでこれらの機能を必要としない場合は、**dced** セキュリティー妥当性検査サービスは不要になります。このサービスが実行されていないシステムでも、**dce\_login** および認証 RPC を出すことができる点に注意してください。
  - **セキュリティー・サーバー証明機能**: クライアントがログイン時に有効な DCE セキュリティー・サーバーと通信できるようにします。これは、他の DCE コ



ンポーネントが **dced** に RPC を出すことでその機能を使用するという意味で、実際にはサーバー・タイプの機能です。

- **dcelogin** 時のサード・パーティー事前認証: DCE 3.2 for AIX and Solaris では、**dce\_login** 機能はサード・パーティー事前認証をユーザーが必要としていることを想定しています。このためには、**dced** セキュリティー妥当性検査サービスが必要です。(このサード・パーティー事前認証が試みられた後、サード・パーティー事前認証を要求するようにユーザー・アカウントが構成されていることの確認が行われます。)しかし、セキュリティ妥当性検査サービスが **dce\_login** 時に活動状態でない場合、**dce\_login** はサード・パーティー事前認証を回避し、タイム・スタンプ事前認証を実行します。ユーザーがサーバーで完全なサード・パーティー事前認証を必要とするように構成されていない限り、エラーは出されません。
- **マシン・コンテキストの最新化**: DCE を実行するすべてのマシンにはプリンシパル名があり、マシンはその名前でログインし、DCE デーモンはその名前で実行されます。このマシン・ログインは、他の DCE コンポーネントにアクセスするための特権チケット認可チケット (PTGT) を獲得するために、DCE サーバー・デーモンにより要求されます。**dced** セキュリティー妥当性検査サービスの 1 つの役割は、このマシン PTGT の有効期限が切れないようにすることです。このプロセスは、マシン・コンテキストの最新化と呼ばれます。マシン・コンテキスト最新化機能が必要なのは、DCE サーバーだけです (サーバーが RPC を受け取る時)。
- **パスワードおよびグループのオーバーライド**: セキュリティー妥当性検査サービスの 1 つの役割は、**/opt/dcelocal/etc/** の **passwd** および **group** ファイルからの DCE ユーザーおよびグループ情報に関するオーバーライドを処理することです。管理者がローカル・マシンにこれらのファイルを作成している場合は、エラーにはなりません。これらのファイルは、スリム・クライアントにより無視されます。
- **セキュリティ統合機能**: スリム・クライアントで実行できます。証明サービスが使用できないため、ユーザー・ログイン時に、ユーザーの ID が正しいセキュリティ・サーバーから出されたことを証明できない点に注意してください。また、スリム・クライアントのセキュリティ統合機能では **passwd** および **group** オーバーライドを使用できない点にも注意してください。マシン・コンテキストが使用できないため、スリム・クライアントのセキュリティ統合機能ではレジストリーに対する未認証アクセスを必要とします。
- **システム管理サービス**:  
DCE が提供しているシステム管理機能を以下に示します。**dced** がいないと、クライアント・システムをこれらの機能によりリモート管理することはできません。
  - **ホスト・データ管理**: このサービスは、ホスト・データのローカル・ファイル (ホスト名、セル名、およびセル別名が含まれている) およびポスト・プロセッサ・ファイルを維持します。ポスト・プロセッサ・ファイルには、他のホスト・データ項目と突き合わされるプログラム名が含まれています。**dced** は、対応するホスト・データ項目が変更されるとプログラムを実行します。
  - **サーバー制御**: このサービスは、各サーバーの始動構成および実行状態を記述しているデータを維持します。また、特定のサーバーを開始または停止した

り、サーバーの特定のサービスを使用可能にしたり使用禁止にすることもできます。このサービスは、RPC サーバーを実行しないクライアントでは不要です。

- **キー・テーブル管理:** このサービスにより、サーバーのキー・テーブルのリモート保守が可能になります。このサービスは、RPC サーバーを実行しないクライアントでは不要です。

---

## DCE サーバー・マシンの要件

以下のサブセクションでは、DCE サーバー・マシンのセットアップに関する考慮事項を説明します。

## DCE サーバー・マシンにインストールするファイル

以下のサブセクションでは、各種 DCE サーバー・マシンのそれぞれにインストールしなければならないファイルの一覧を示します。すべての DCE サーバーは DCE クライアントでもあるため、19ページの『DCE クライアント・マシンの要件』で説明しているファイルはサーバー・マシンにもインストールする必要があります。したがって、サーバー・マシンのスペース要件のおおまかな合計を算出するためには、クライアントのおおまかなスペース要件を DCE サーバー・マシンのスペース要件に加算してください。

## DCE RPC サーバー・プログラム

DCE クライアント上で実行されるプログラムの他に DCE RPC サーバー・プログラムはありません。

## セキュリティ・サーバー・プロセス

すべてのセルは、1つのマスター・セキュリティ・サービス・マシンを持っており、スレーブ・セキュリティ・サービス・マシンを持つこともできます。次のプロセスは、セキュリティ・サービスのマスターまたはスレーブ・サーバー・マシンで実行します。

- セキュリティ・サーバー (つまり **secd** プロセス) は、認証サービス、特権サービス、およびレジストリー・サービスを実行します。
- **sec\_create\_db** プログラムは、セキュリティ・データベースを初期設定します。このコマンドには、そのマシン上にマスター、スレーブ、または LDAP スレーブ・セキュリティ・サーバーを作成したいことを示すオプションを与えます。
- セキュリティ・ソフトウェアを登録、管理、および維持するための DCE 制御プログラム (**dcecp**)。28ページの『DCE 管理ユーティリティ』は、**dcecp** を説明しています。
- 識別マッピング・サーバー (IDMS) (つまり **idmsd** プロセス) は、ユーザーの公開鍵証明を DCE プリンシパル名にマッピングする PRC サーバーです。公開鍵証明ログインを使用する DCE セルに 1つ以上の IDMS が必要です。
- パスワード・ストレングス・サーバー (つまり **pwd\_strengthd** プロセス) は、カスタマイズされたパスワード検査とパスワード生成を実行して、セル中のパスワード・ストレングス・ポリシーを拡張します。



セキュリティー・サーバーを計画する時には、次の考慮事項に留意してください。

- マスター・セキュリティー・サーバーを実行するノードは、非常に高い可用性を提供し、物理的に安全なものである必要があります。マスター・セキュリティー・サーバー・マシンを鍵のかかる部屋に置き、誰がマシンをアクセスしたかを記録するログを保持することを検討してください。
- ネットワークからノードを取り外したり、一定期間ノードをシャットダウンする前に、マスター・セキュリティー・サーバーを確実に移動してください。変更はマスター・セキュリティー・サーバーに対して行われ、セルを通してスレーブに伝搬されます。マスター・セキュリティー・サーバーが利用できないと、変更は行われません。
- セルはマスター・セキュリティー・サーバーを 1 つしか持てません。独立したマスター・セキュリティー・サーバーを持つ複数の既存のセルから 1 つのセルを作成する計画の場合は、最初にそのレジストリーをマージする必要があります。
- マスター・セキュリティー・サーバーが含まれているホストがダウンしても、スレーブ・サーバーが含まれているホストであればレジストリー情報を提供できます。したがって、ネットワークにいくつかのスレーブを組み込むことを考慮してください。セル内のマシンの数や、セキュリティー・サーバーを実行するマシンの信頼性、セルの利用できるリソースといった要素を使用して、スレーブ・セキュリティー・サーバーをいくつ持つ必要があるかを決めてください。
- LDAP を使用してセキュリティー・データを格納するつむりの場合は、関連する計画上の考慮事項について、*IBM DCE for AIX and Solaris* バージョン 3.2: *DCE セキュリティー・レジストリーと LDAP 統合* を参照してください。

セキュリティー・サービスの計画に関する詳細な説明は、*IBM DCE for AIX and Solaris* バージョン 3.2: *管理ガイド--コア・コンポーネント* を参照してください。

## 監査サーバー・プロセス

監査サーバーは、DCE 監査機能をアクセスする他の DCE サービスを提供します。監査サーバーは、**auditd** デーモンを実行します。DCE セル内で監査が利用できるためには、各マシンはデーモンを実行する必要があります。

## CDS および GDA サーバー・プロセス

CDS サーバーはセル内にオブジェクト名を保管および保守し、データの作成、修正、および探索の要求を扱います。セルが他のセルと通信するためには、そのセル内に GDA サーバー (**gdad** デーモン) が必要です。

次のプロセスは、CDS サーバー・マシンで実行します。

- CDS デーモン (**cdsd**) は CDS サーバー・プロセスです。
- DCE クライアント・マシンの **cdsadv** は、どのサーバーが使用可能かを見つけるためのサーバー通知を受け取ります。CDS サーバー・マシン上では、これはサーバーの通知の送付も行います。
- Name Service Gateway (**nsid** ともいう) は、固有の Microsoft® RPC アプリケーションから DCE ネーム・サービスへのアクセス権を備えています。

- CDS ソフトウェアの管理および保守のための DCE 制御プログラム (**dcecp**)。さらに、**cdscp** プログラムは CDS クラークおよびサーバーに関する情報の制御および表示に使用されます。28ページの『DCE 管理ユーティリティ』は、**dcecp** を説明しています。

CDS を準備する際には、セル内にクリアリングハウス (CDS データベース) を保管、保守するサーバー・ノードを選択する必要があります。信頼性、最適なパフォーマンス、およびデータ可用性を確保するため、次のガイドラインに留意してください。

- 信頼できるノードを選択します。CDS サーバーはできるだけダウン時間を避け、ダウン時間が発生した場合には迅速に再始動する必要があります。クライアント・アプリケーションと他の DCE サーバーは、最新の情報を CDS サーバーに依存するため、CDS サーバーはネットワーク上で最初に利用できるシステムの 1 つである必要があります。CDS サーバーは、DCE が構成される時に CDS ネーム・スペースを初期化します。
- 信頼性の高いネットワーク接続を使用します。これは、CDS がスカルクを実行する時に、ディレクトリーのレプリカを保守しているすべてのサーバーに行けるよう保証するのを助けます。スカルクは、すべてのレプリカの整合性を検査する定期的な更新です。
- CDS サーバーがいくつ必要かを定める時には、セルのサイズおよび、セルが地理的にどのように分散しているかを考慮します。サーバーの 1 つが利用できなくなった場合にデータへのアクセスを確かなものにするため、各 CDS ディレクトリーの少なくとも 2 つのコピー (1 つのマスターと 1 つのレプリカ) を持つべきです。
- セル内の各 CDS サーバーは、少なくとも 1 つのクリアリングハウスを保守する必要があります。すべてのクリアリングハウスは、そこに複製されている他のディレクトリーに加えて、ルートのコピーを含む必要があります。
- ディレクトリーの内容が参照される場所に基づいて複製の決定を行います。内容が読み出される場所にはレプリカを置き、内容が書き込まれる場所にはマスターを置きます。初期 CDS サーバーの移動の説明は、55ページの『付録A. 初期 CDS サーバーの移動』を参照してください。

DNS を使用する DCE 構成では、グローバル・ディレクトリー・サービスにアクセスするためには CDS は少なくとも 1 つの GDA に連絡できなければなりません。CDS は **gdad** デーモンを介して GDA と連絡します。このデーモンはセル名に関する探索要求を DNS へ送信し、要求を開始したセルの CDS クラークに結果を戻します。

GDA は、CDS サーバーと同じマシン上でもよく、または別のマシンに独立して存在することもできます。GDA の可用性を保証するためには、セル内で複数の **gdad** デーモンを実行できます。

## DTS サーバー・プログラム

DCE クライアント構成には、任意選択のタイム・プロバイダーを除き、DTS サーバー・マシンに必要なすべてのファイルがすでに含まれています。必要なファイルは次のものです。

- DCE クライアント・マシンにインストールすることのできる **dttd** デーモンは、DTS サーバー・マシンにインストールされたときにサーバーとして実行されるように構成されます。**dttd** はクライアント・マシン上で実行する場合と同様にローカル・クロックの同期処理を実行しますが、それ以外に、サーバー・プロセスとして DTS サーバーとの同期も取ります。
- **dts\_device\_name\_provider** は、DTS サーバー・プロセスとタイム・プロバイダー・プロセス間の通信を指定します。*device\_name* には、使用する装置を指定します。これには、無線、クロック、モデム、または DTS の UTC 時間の他のソースを使用できます。タイム・プロバイダーは任意選択です。タイム・プロバイダーを使用する場合は、これをサーバー・プロセスに接続する必要があります。
- DTS ソフトウェアの管理および保守のための DCE 制御プログラム (**dcecp**)。28ページの『DCE 管理ユーティリティ』は、**dcecp** を説明しています。
- セル内に構成されているタイム・サーバーが 2 つ以下の場合、以下のいずれかのコマンドを使用します。

```
dtscp set servers required n
(n はセル内のタイム・サーバーの数)
dcecp dts modify -miniservers n
(n はセル内のタイム・サーバーの数)
```

これにより、サーバーが同期処理を試みるたびに警告メッセージがログに記録されることはなくなります。

DTS 導入を計画する際には、次のガイドラインを考慮してください。

- 各セルは少なくとも 3 つの DTS サーバーを持つ必要があります。時刻を照会された時に、いずれか 1 つに障害があるかどうかを検出するには、少なくとも 3 つの DTS サーバーが必要です。冗長性を持たせるため、4 つ以上の DTS サーバーを持つことが望まれます。追加のサーバーは、時刻同期化の正確度を増します。しかし、時刻を照会されるサーバーの数を増やすと、ネットワークの活動も増加します。管理担当者は、正確度のレベルとネットワーク活動の量とのバランスをとる必要があります。
- タイム・プロバイダーは DTS 内では任意選択です。しかし、時間標準と厳密に同期を取らなければならないセルの場合、少なくとも 1 つのタイム・プロバイダーが必要です。
- サーバーは、異なるネットワーク接続をより多く持つサイトに置く必要があります。

ネットワーク構成に関する決定の多くが DTS 計画に影響を与えます。*IBM DCE for AIX and Solaris* バージョン 3.2: 管理ガイド--コア・コンポーネント では、ローカル・エリア・ネットワーク (LAN)、拡張 LAN、および広域ネットワーク (WAN) の構成計画も含め、DTS 計画プロセス全体の詳細を説明しています。*IBM DCE for AIX and Solaris* バージョン 3.2: 管理ガイド--コア・コンポーネント では、使用するネットワークのためのタイム・ソースを選択するときに必要な基準を説明しています。

## イベント管理サービス (EMS) プロセス

EMS は DCE セル中のイベント・サービスを管理します。EMS 中では、イベントとは、イベント提供側から EMS に、および EMS から 1 つまたは複数のイベント消費側に伝送されるデータのことです。EMS は **emsd** デーモンにより実行されま

す。消費側がイベントを受け取ったり提供側がイベントを送信したりできるようにするには、このデーモンを DCE 中のホスト・システム上で実行しなければなりません。

---

## DCE 管理ユーティリティー

以下のサブセクションでは、DCE ソフトウェアを管理および保守するために DCE で用意しているユーティリティー・プログラムを説明します。最後のサブセクションでは、DCE サーバーのリモート管理を実行するために特別に構成されているマシンに用意するユーティリティーを説明します。

## DCE 制御プログラム

DCE のための総合管理ツールである **dcecp** には、DCE サービスを管理するための機能が備わっています。このプログラムを使用して DFS を管理することはできません。

**dcecp** ユーティリティーは、DFS を除いたすべての DCE サーバー・ソフトウェア・パッケージに含まれています。

## DCE RPC 管理プログラム

RPC 固有の管理ツールである、**rpccp** プログラムは、DCE ネーム・スペースに保管されているエントリーの DCE RPC 属性および、ローカルとリモートの **dced** デーモンにより管理されているエンドポイントを表示、更新、追加、および削除できるようにします。

## セキュリティー・サービス管理プログラム

セキュリティー・サービスは、次の管理ユーティリティーを提供します。

- **dcecp acl** コマンドは、特定オブジェクトの ACL エントリーを表示、追加、修正、および削除します。 *IBM DCE for AIX and Solaris* バージョン 3.2: 管理コマンド・リファレンス には、**dcecp acl** コマンドの使用に関する詳細な説明が含まれています。
- **dcecp account**、**group**、**organization**、**principal**、**registry**、**user**、および **xattraschema** コマンドを使用し、レジストリー・データベースまたはローカル・レジストリーを編集できます。レジストリー・データベースのほとんど大部分の編集は、これらのコマンドを使用して実行します。 *IBM DCE for AIX and Solaris* バージョン 3.2: 管理コマンド・リファレンス では、これらのコマンドの使用法を説明しています。
- **passwd\_import** コマンドを使用し、DCE セキュリティーを実現していないマシンからのグループおよびパスワード・ファイルを基に、レジストリー・エントリーを作成できます。
- **passwd\_export** コマンドを使用し、UNIX **/etc/passwd** および **/etc/group** ファイルを更新できます。現行ユーザー情報は、レジストリーから入手します。
- **passwd\_override** および **group\_override** ファイルを使用し、レジストリー内の情報に対するオーバーライドを確立できます。
- **rmxcred** コマンドは、認証ディレクトリーから有効期限切れのチケットを消去します。

- **dcecp registry** コマンドは、レジストリーのサーバー・レプリカの管理、マスター・サーバー・サイトの変更、セキュリティ・サーバーの LDAP へのマイグレーション、およびスレーブ・サーバーの再初期設定に役立ちます。このコマンドは、セキュリティ・サーバーおよびそのデータベースの管理にも使用できます。セキュリティ・サーバーの停止およびデータベースに関する新しいマスター・キーの生成などの作業を実行できます。

## CDS 管理プログラム

CDS は、次の管理ユーティリティを提供します。

- CDS 制御プログラム (**cdscp**) は、CDS サーバーおよびクラークの管理およびネーム・スペースとその内容の管理に使用されるコマンド・インターフェースです。**cdscp** コマンド・インターフェースは以前の DCE バージョンで使用されていたもので、**dcecp** ユーティリティへ簡単にマイグレーションできるように用意されています。CDS 制御プログラムの詳細な説明は、*IBM DCE for AIX and Solaris* バージョン 3.2: 管理ガイド--コア・コンポーネント を参照してください。
- DCE ユーザーは **cdsli** を使用することで、セルのネーム・スペースを再帰的にリストできます。
- **cdsdel** は、セルのネーム・スペースを再帰的に削除します。
- CDS アドバイザー (**cdsadv**) は、アプリケーションが **cdsd** にアクセスして通信できるようにし、必要な CDS クラークを開始し、ローカル CDS クラークが共用するキャッシュを作成します。
- CDS クラーク (**cdsclerk**) は、CDS クライアント・アプリケーションと CDS サーバーとのインターフェースです。
- DCE 制御プログラム (**dcecp**) は、CDS エントリーのブラウズ、更新、および削除、およびネーム・スペースの管理に使用できます。このプログラムは **cdscp** を置き換えます。
- **mkreg.dce** コマンドは、ドメイン・ネーム・サーバー (AIX では **named** デーモン、Solaris では **in.named** デーモン) が保守するデータベースに DCE セルの情報を入力します。
- **rmreg.dce** コマンドは、**mkreg.dce** コマンドにより追加されたドメイン・ネーム・サーバー (AIX では **named** デーモン、Solaris では **in.named** デーモン) が保守するデータベースから情報を削除します。

## DTS 管理プログラム

DTS 制御プログラム (**dtscp**) は、DTS を管理できるようにするものであり、これには、**dttd** デーモンをクライアントまたはサーバーのどちらかとして構成することが含まれます。**dtscp** プログラムは、DCE クライアント・ソフトウェアに含まれています。

## DCE リモート管理マシンのためのプログラム

システム・ユーザーは、セル管理者としてログインしたときは、セル内の任意のマシンから管理作業を実行できます。管理作業を実行するためには、ユーザーは認証されていなければならない、作業を実行するために必要なツールが揃っていることを



確認する必要があります。インストールする必要がある管理ユーティリティーは、DCE クライアント・ソフトウェアの他に、次のようなものがあります。

- CDS クラークとサーバーに対するある種のオペレーションを制御するための **cdscp** プログラム。
- レジストリーのローカル・コピーを保守するための **rgy\_edit** プログラム。
- **passwd\_override**、**sec\_admin**、**sec\_create\_db**、および **sec\_salvage\_db** プログラムは、セキュリティー・サービス管理を実行するためにインストールする必要があります。
- CDS クラークとサーバーに対するある種のオペレーションを制御するための **cdscp** プログラム。
- レジストリーのローカル・コピーを保守するための **rgy\_edit** プログラム。

**dcecp** および DCE クライアント・ソフトウェア以外のソフトウェアは、DCE RPC、DTS、セキュリティー、または CDS の管理には不要です。

---

## アプリケーション開発環境マシン

DCE マシンは、DCE アプリケーションの開発用に構成することもできます。開発作業には、いくつかのインクルード (**.h**) およびインターフェース仕様 (**.idl**) ファイル、および **idl** プログラムを基本 DCE クライアント構成に追加する必要があります。

---

## 第4章 DCE ファイルのインストール場所

DCE が使用するファイルは、次の場所にグループ化されます。

- **/opt/dcelocal** サブディレクトリー
- 従来の UNIX サブディレクトリー

信頼性向上のためおよびセキュリティーが維持されていることを確認するために、一部の情報はマシン上にローカルに保存する必要があります。たとえば、DCE を構成するとき、セル名を含むファイルは構成されているマシン上になければなりません。このファイルは **dcelocal** サブツリーに格納されています。

**/opt/dcelocal** サブツリーは、DCE コンポーネントのインストール時に作成されます。

ファイルは、パフォーマンス上の理由で **/usr/lib**、**/usr/bin**、または **/bin** などのディレクトリーにインストールされることがあります。また、従来の UNIX サブディレクトリーから **/opt/dcelocal** に対しシンボリック・リンクを張ることもあります。

この章には以下のトピックが含まれています。

- 『**/opt/dcelocal** サブツリー』
- 32ページの『ファイル・システム』
- 32ページの『従来の UNIX ディレクトリー (AIX のみ)』
- 32ページの『ファイルの場所』
- 35ページの『DCE デーモンのコア場所』

---

### **/opt/dcelocal** サブツリー

サーバーを初めてブートしてセルを構成するためには、必須サーバー (CDS およびセキュリティー) のための適切なファイルがそのサーバー・マシン上で使用できなければなりません (**/opt/dcelocal** サブツリー内)。デフォルト DCE インストール・プロシージャでインストールされていたプログラムとデータ・ファイルの最小セットのコピーを、スタンドアロン・オペレーションおよび緊急保守のためのサーバー・マシンにローカルに保存することを強くお勧めします。

**/opt/dcelocal** サブツリーの内容は DCE セル内のマシンごとに変え、特殊の構成を受付処理することができるようになっています。さらに、すべてのマシンには特定のファイルに対するローカル・アクセス権が必要です。それは、マシンがセルから切り離されたり区分された場合に各マシンをスタンドアロン・システムとして実行できるようにするためです。サーバー・マシンに対しローカルでなければならない DCE サーバー上の該当するファイルは、**/opt/dcelocal** の下に格納させる必要があります。クライアント関連データ・ファイルは、**/opt/dcelocal/etc** (静的構成データ) および **/opt/dcelocal/var/adm** の下に格納されます。すべてのサーバー用データ・ファイルは、**/opt/dcelocal/var/dce-component-name** ディレクトリーに存在します。

**DCELOCAL** のデフォルト・パスは **/opt/dcelocal** に設定されます。これは固定のパス名です。すべてのマシンには構成するために必要なファイルに対するローカ

ル・アクセス権が必要です (セル内の DFS アクセスを活動化するまで)。

**/opt/dcelocal/dce\_cf.db** ファイルは、構成するホスト名およびセル名が含まれた DCE 構成ファイルです。マシンは、各種の DCE コンポーネントを開始するため、およびローカル構成情報とログ情報のため、マシンのローカル・ディスクに保持されているこの DCE ファイルの小さなセットをアクセスする必要があります。

DCE 構成はローカル・ファイル・システムをマウントした後に行われるため、これらのどのファイルもルート区画で利用可能である必要はありません。

**/opt/dcelocal** サブツリーには、DCE インストールおよび構成時に内容が入り、初期設定されます。

---

## 従来の UNIX ディレクトリー (AIX のみ)

DCE が使用するいくつかのファイルおよびディレクトリーは、従来の UNIX ディレクトリー内でアクセス可能です。これらの DCE ファイルとディレクトリーは、従来の場所でアクセスできるようにする必要があります。これは、**/usr/bin** ディレクトリーの **idl** や **/etc/zoneinfo** ディレクトリーの **localtime** などの使用頻度の高いユーティリティーやデータにユーザーが容易にアクセスできるようにするためです。ヘッダー・ファイルは **/usr/include** またはそのサブディレクトリー **/usr/include/dce** でアクセスでき、**libdce.a** などのライブラリーは **/usr/lib** に保存されています。

---

## ファイル・システム

すべての DCE ファイルは **/opt** の下に保持されます。ファイル・システムがいっぱいになると、DCE および **/opt** に依存する他のサブシステムは正しく操作できなくなります。

DCE 製品のインストールに必要なスペースに加えて (セクション xxx - (圧縮サイズ・テーブル) を参照)、次のスペースを予約しておいてください。

- 初期構成の 30 メガバイト
- CDS サーバー (このマシン上に構成される場合) の 30 メガバイト
- セキュリティー・サーバー (このマシン上に構成される場合) の 10 メガバイト

---

## ファイルの場所

### AIX の場合

DCE 3.2 for AIX のインストール・プロセスでは、ファイルを次の場所に格納しています。

**/usr/lpp/dce**

この一覧の他の個所に含まれていないすべての DCE ファイル

**/usr/lpp/dce/tcl/dcedcf**

DCE/DFS 構成スクリプト

**/usr/lpp/dcedoc**

すべての DCE for AIX 資料ファイルおよびその関連ツール



### **/etc/dce**

以下のファイル

- **rc.dce**
- **dce.clean**
- **rpc.clean**

### **/etc/dce/rspfiles**

構成応答ファイル

### **/etc/zoneinfo**

DTS の時間帯規則

### **/tmp/dce**

構成処理の一時場所

### **/usr/lib/nls/msg/en\_US**

英語のメッセージ・カタログ

### **/usr/include**

インクルード・ファイル (通常は **/usr/include/dce** の下)

### **/usr/lib**

**libdce.a**、**libcfgdce.a**、**libdcelibc\_r.a**、**libdcephreads.a**、および  
**libidlcxx.a**

### **/usr/lib/security**

AIX/DCE 統合セキュリティー・オペレーションのための **DCE** ロード・モジュール。公開鍵証明ログイン・オペレーションのための **DCEPKC** ロード・モジュール

**/opt/dcelocal** は **/usr/lpp/dce** へのシンボリック・リンクとして設定されます。  
**/opt/dcelocal/var** は **/var/dce** へのシンボリック・リンクとして設定されます。  
**/opt/dcelocal/etc** は **/etc/dce** へのシンボリック・リンクとして設定されます。  
**/opt/dcelocal/tmp** は **/tmp/dce** へのシンボリック・リンクとして設定されます。  
各 DCE コマンドのリンクは、**/usr/bin** の下に置かれます。

さらに、SMIT オブジェクトはオブジェクト・データ管理プログラム (ODM) データベースへロードされます。

## **Solaris の場合**

DCE 3.2 for Solaris のインストール・プロセスでは、ファイルを次の場所に格納しています。

### **/opt/dce**

DCE バイナリー (必ずしもすべての DCE ファイルが **/opt/dce** からアクセス可能なわけではなく、また **/opt/dcelocal** を使用するわけではない)

### **/opt/dcelocal**

いくつかのサブディレクトリーは **/opt/dce** へのリンクです。他のサブディレクトリーにはローカル・マシンに固有のファイル (たとえばデータベース・ファイルやログ) が含まれています。すべての DCE ファイルは **/opt/dcelocal** からアクセス可能です。

次の場所から **/opt/dce** および **/opt/dcelocal** にあるファイルへのシンボリック・リンクが作成されます。

#### **/usr/bin/**

**/opt/dcelocal** にあるファイルへの DCE 実行可能ファイルのリンクが作成されます。

#### **/usr/lib**

**/opt/dcelocal** にあるファイルへの DCE ライブラリーのリンクが作成されます。

#### **/usr/lib/dce**

**/opt/dcelocal** にあるファイルへのいくつかの DCE ライブラリーのリンクが作成されます。

#### **/usr/lib/locale/{LANG}/LC\_MESSAGES**

**/opt/dcelocal** にあるファイルへの DCE メッセージ・カタログのリンクが作成されます。

`/usr/lib/locale/en_US/LC_MESSAGES`

`/usr/lib/locale/es/LC_MESSAGES`

`/usr/lib/locale/it/LC_MESSAGES`

`/usr/lib/locale/ja/LC_MESSAGES`

`/usr/lib/locale/ja_JP/LC_MESSAGES`

`/usr/lib/locale/ko/LC_MESSAGES`

`/usr/lib/locale/pt_BR/LC_MESSAGES`

`/usr/lib/locale/zh/LC_MESSAGES`

`/usr/lib/locale/zh.GBK/LC_MESSAGES`

#### **/usr/lib/libpkc.so**

DCEPKC のリンクが作成されます。

#### **/usr/ccs/lib**

**/opt/dcelocal** にあるファイルへのいくつかの DCE ライブラリーのリンクが作成されます。

#### **/etc**

- **rc.dce**
- **rpc.clean**
- **dcesetup**

## 実行時に作成される構成ファイル

以下のファイルは実行時に作成されるファイルです。

- **cfg.dat** には、DCE/DFS コンポーネントの現行構成状態のデータが含まれています。
- **cfgdce.dat** には、非表示構成データが含まれています。
- **cfgdce.log** 構成ログ
- **cfgdce.log** の **cfgdce.bck** バックアップ - **cfgdce.log** ファイルが 100000 バイトを超えると作成されます。
- **protseqs.rpc** は使用されているプロトコルをリストします。
- **dce\_cf.db** にはローカル・マシンのセル名と DCE ホスト名が含まれています。

- **cfgarg.dat** には DCE デーモンを再起動するために使用されるオプションが含まれています。

## 作成およびマウントするファイル・システム (AIX のみ)

DCE を効果的に使用するために、次のような新しい AIX JFS ファイル・システムを作成できます。

### **/var/dce**

すべての DCE コンポーネントは、**/var/dce** ディレクトリーに情報を格納します。**/var** ファイル・システムがいっぱいになると、DCE および **/var** に依存する他のサブシステム (メールおよびスプーラー・サブシステムなど) は正しく操作できなくなります。

DCE インストール前に **/var/dce** にマウントされていた新しいファイル・システムを作成する必要があります。初期 DCE 構成の場合、**/var/dce** に約 30 MB 確保します。

### **/var/dce/directory**

このディレクトリー・ツリー内に CDS サーバーはクリアリングハウス・ファイルを格納します。これらのファイルには、ネーム・スペースのこのサーバーの部分とローカル・データが含まれます。

このマシンを CDS サーバーとして構成する場合、DCE インストール前に **/var/dce/directory** にマウントされていた新しいファイル・システムを作成することをお勧めします。

サーバーのために約 30 MB 確保する必要があります。

CDS サーバーのために別個のファイル・システムを作成しない場合は、**/var/dce** に 30 MB 余分に追加してください。

### **/var/dce/security**

セキュリティー・サーバーは、レジストリー、認証、およびローカル・データをここに格納します。このマシンがセキュリティー・サーバーとして使用される場合は、サーバーが使用できるように **/var/dce** に 10 MB 余分に追加してください。

**/var/dce** に格納されるファイルは、個別マシンに特別なファイルです。**/var/dce** (および関連する個別ファイル・システム) 内のスペースの使用状況を監視し、いっぱいになっていないことを確認します。**/var/dce** 内の有効期限切れの認証ファイルをクリーンアップするためには、**/usr/lpp/dce/bin/rmxcred** コマンドを使用します。DCE 監査機能も、**/var/dce** 内のスペースを使用します。**rmxcred** および DCE 監査に関する詳細な説明は、*IBM DCE for AIX and Solaris* バージョン 3.2: 管理コマンド・リファレンス を参照してください。

---

## DCE デーモンのコア場所

以下のリストは、DCE デーモンの場所およびそれらがコアをダンプする場所を示したものです。

- **secd** - **/opt/dcelocal/var/security/adm/secd**
- **dced** - **/opt/dcelocal/var/dced**
- **cdsd** - **/opt/dcelocal/var/directory/cds/adm/cdsd**

- **gdad** - /opt/dcelocal/var/directory/cds/adm/gdad
- **csdadv** - /opt/dcelocal/var/adm/directory/cds/cdsadv
- **cdsclerk** - /opt/dcelocal/var/adm/directory/cds/cdsclerk
- **dtsd** - /opt/dcelocal/var/time/adm/dtsd
- **pwd\_strengthd** - /opt/dcelocal/var/security/adm/pwd\_strength
- **idmsd** - /opt/dcelocal/var/security/adm/idmsd
- **emsd** - /opt/dcelocal/var/sysmgmt/adm/emsd
- **dceagtd** - /opt/dcelocal/var/sysmgmt/adm/dceagtd
- **audit** - /opt/dcelocal/var/audit/adm
- **nsid** - /opt/dcelocal/var/directory/cds/adm/nsid
- **session\_manager** - /tmp/sessmgr
- **session\_manager\_control** - /tmp/session\_control

以下は Solaris 固有です。

- **nss\_dce\_server** - /opt/dcelocal/var/security/adm/nss

以下は AIX 固有です。

- **dceunixd** - /opt/dcelocal/var/security/adm/dceunixd

---

## 第5章 DCE 保守の概要

DCE システムの計画、インストール、および構成に必要な作業を実施した後、システムの保守に必要な作業を実施できます。計画、インストールおよび構成の初期作業は頻繁には実行されず、あるものは一度だけです。しかし、保守作業はシステムの存続時間にわたって定期的に実行されます。

分散システムの保守には次の領域が含まれます。

- パフォーマンスの調整
- 構成の制御
- セキュリティーおよびアクセスの制御

この章は、主要な DCE 管理作業のいくつかを要約します。この章の最初のセクションでは、DCE の開始方法を説明します。残りのセクションでは、個別 DCE コンポーネントに適用される作業を説明します。DCE コンポーネント作業は、*IBM DCE for AIX and Solaris* バージョン 3.2: 管理ガイド--コア・コンポーネント、および *IBM DCE for AIX, Version 3.1: DFS Administration Guide and Reference* で詳細に説明しています。

---

### DCE マシンのネットワーク・アドレスの変更

時折、DCE を実行するマシンがそのネットワーク・アドレスを変更する必要があることがあります。DCE は、更新しなければならないいくつかのファイルにネットワーク・アドレスを格納します。IP アドレスの変更方法については、*IBM DCE for AIX and Solaris* バージョン 3.2: 管理ガイド--コア・コンポーネント を参照してください。

---

### CDS 保守作業

CDS コンポーネントは、クラーク、サーバー、およびクリアリングハウスを含めて、多くの部分が自己統制されています。ルーチン・モニターを除き、CDS はシステム管理のための介入をほとんど必要としません。介入が必要な場合、CDS はシステム管理ツールを提供し、CDS ネーム・スペースおよび CDS サーバーのモニターと管理を援助します。

*IBM DCE for AIX and Solaris* バージョン 3.2: 管理ガイド--コア・コンポーネント で説明している DCE 制御プログラム (**dcecp**) コマンドを使用し、CDS ネーム・スペースのコンポーネントを作成し管理できます。

大きな組織の場合、CDS サーバーに責任を持つシステム管理者を 1 人、ネーム・スペースに責任を持つシステム管理者を 1 人持つことで効率を改善できます。別の管理者にアクセス制御権を認可することで、ネーム・スペースのサブツリーに対する責任を別の管理者に代行させることができます。

CDS 保守作業の詳細な説明は、*IBM DCE for AIX and Solaris* バージョン 3.2: 管理ガイド--コア・コンポーネント を参照してください。

## CDS のモニター

CDS モニター作業は、次の 2 つのカテゴリに分けられます。

- ネーム・スペースのモニター
  - クリアリングハウスのサイズと使用度をモニターし、新しい CDS サーバーおよびクリアリングハウスの必要性を判別する。これらの新しいサーバーおよびクリアリングハウスの構成を計画し、監視する。
  - ネーム・スペースのマップを保守しモニターする。
- CDS サーバーのモニター
  - イベント・ログを使用可能にし、CDS イベントをモニターし、システム特有の問題が起こった場合にはこれを解決する。必要な場合、他の CDS サーバーまたはクラークに影響を与える可能性のある問題について、ネーム・スペース管理者に通知する。
  - サーバーで発信されたスカルクの成功をモニターする。スカルクは、オペレーションの反復によってすべてのレプリカを更新する方法です。
  - サーバーのクリアリングハウスのサイズと使用をモニターし、必要な場合、いくつかのレプリカを再配置したり、新しいクリアリングハウスを作成する必要性についてネーム・スペース管理者に相談する。
  - CDS サーバー・オペレーションに影響する、または影響されるシステム・パラメーターをモニターし、調整する。

注: CDS サーバーのメモリー使用度をモニターする場合、メモリーはある条件のもとでは割り振りされたままになっているということを理解することが重要です。オブジェクトに関連付けられたメモリーは、スカルクが正常に終了するまで割り振りされたままになっています。ディレクトリーに関連付けられたメモリーは、サーバーが使用不能にされるか再始動されるまで割り振られたままになっています。

これらの作業の詳細な説明は、*IBM DCE for AIX and Solaris* バージョン 3.2: 管理ガイド--コア・コンポーネント を参照してください。

## CDS の管理

CDS 管理作業は、次の 2 つのカテゴリに分けられます。

- ネーム・スペースの管理
  - 新しいディレクトリーの作成を監視し、標準にしたがって名前を割り当てる、または名前の割り当てに確立されたガイドラインが使用されるようにする。(ディレクトリー階層のあるレベル以下は、ディレクトリーの作成と保守の責任を代行者に任せることができます。作成された新しいディレクトリーについては追跡を続け、適切に複製されているかを確認する必要があります。)
  - デフォルトのアクセス制御ポリシーを決定する。
  - ディレクトリーとエントリーに対して確立されたアクセス制御ポリシーを管理し、それが使用されるようにする。
  - いつ、どこでディレクトリーの新しいレプリカが必要かを判別する。
  - 場所が変更されたオブジェクト、または名前変更の必要があるオブジェクトのためのソフト・リンクを作成する。オブジェクトは、ディスク、アプリケーション、あるいはノードといった、CDS 名を与えられているリソースです。名

前と属性によりオブジェクト・エントリーは構成されます。ソフト・リンクは、オブジェクト・エントリーに代替名を提供するポインターです。

新しい名前を公表し使用を勧めることで、最終的にソフト・リンクを削除できるようにする。

- 複数 CDS サーバーに関係する問題の解決を実施、または指示する。
- CDS サーバーの管理
  - ディレクトリーとオブジェクトへのアクセス制御を管理し、サーバーのクリアリングハウス内のディレクトリーのサイズと使用度をモニターする。必要な場合、おそらくネーム・スペース管理者と一緒に、新しいディレクトリーを作成する。
  - ディレクトリー内に新しいオブジェクトを作成する、またはその作成を監視する。(ディレクトリー階層のあるレベル以下は、ディレクトリーとその中のオブジェクトの保守の責任を代行者に任せるともできます。)
  - **cds-admin** セキュリティー・グループに新しい管理者を追加します。

*IBM DCE for AIX and Solaris* バージョン 3.2: 管理ガイド--コア・コンポーネントは、これらの作業の実行方法を詳細に説明しています。

## CDS セキュリティーおよびアクセスの制御

DCE 制御プログラム (**dcecp**) と CDS ACL 管理プログラムは共同作業を実行することで、CDS における許可を管理します。CDS ネーム・スペースにおいて ACL エントリーの修正、追加、削除、または表示を実行するためには、**dcecp acl** コマンドを使用します。**dcecp** が CDS オブジェクトに対するオペレーションを実行するための要求を出すと、CDS ACL 管理プログラムは ACL エントリーに基づいて許可を検査し、要求を認可または拒否します。CDS ACL 管理プログラムは、**cdsd** および **cdsadv** プロセスの必須構成要素です。

*IBM DCE for AIX and Solaris* バージョン 3.2: 管理ガイド--コア・コンポーネントは、新しいネーム・スペースにおけるアクセス制御の設定のガイドラインなど、CDS セキュリティーおよびアクセス制御の処理に関する詳細な説明を行っています。

---

## DTS 保守作業

CDS と同様、DTS はサービスの構成が完了した後では多くの部分が自己統制されています。しかし、介入が必要な場合もあります。**dcecp** を使用し、以下の DTS 構成および管理作業を実行します。

- システム・クロック問題を識別する。
- システム・クロックを調整する。
- 各種の WAN 条件用に DTS 属性を変更する。
- ネットワーク環境が変更された場合に、システム構成を変更する。

DTS 保守作業の詳細な説明は、*IBM DCE for AIX and Solaris* バージョン 3.2: 管理ガイド--コア・コンポーネント を参照してください。



## 分散タイム・サービスの管理

**dcecp** を使用し、DTS を作成したり使用可能にしたりできます。一度これを実施すると、パフォーマンスの改善や、ネットワークの再構成、およびローカル時間の変更といった定常的な管理作業を実施できます。

いくつかのコマンドと特性により、ネットワークのパフォーマンスを変更し改善できます。 **dts modify** コマンドは、これらの特性のいくつかの値を変更します。 **dts show** コマンドは、任意の時点の特性の値を表示します。以下に示すのは、DTS コマンドを使用して実施できるいくつかの作業と、設定できる DTS の特性です。

- DTS がシステム・クロックを同期化する前に、システムに時刻値を提供する必要があるサーバーの数を表示、または変更する。
- 不正確さを受容可能なレベルにもどすためにシステムを強制的に同期化させるための、不正確さの限界値を表示または変更する。
- クロック同期化を起こさせたい時間間隔を表示、または変更する。
- 障害のあるシステム・クロックへの対応を表示、または変更する。
- サーバーを照会する頻度を示す設定を表示、または変更する。

これらの作業および以下の作業の詳細な説明は、*IBM DCE for AIX and Solaris* バージョン 3.2: 管理ガイド--コア・コンポーネント を参照してください。

- DTS を作成し、使用可能にする。
- ネットワークの他の部分との通信を可能にするため、サーバーに運搬の役割を割り当てる。
- 初期構成の後、ネットワークに追加するサーバーのためのエポック番号を突き合わせる。エポック番号 は、サーバーが他のサーバーに送る、時刻値に付加する ID です。サーバーは他のサーバーからの時刻値を、エポック番号を共有する相手の場合のみ使用します。
- DTS サーバーを CDS にアダプタイズし、それにより DTS サーバーをネーム・スペース内のオブジェクトとして登録する。

## システム時刻の変更

システム時刻を変更する必要がある場合があります。ネットワークでタイム・プロバイダーを使用せず、ネットワーク・システムが何らかの時間の間実行される場合、電話、無線、サテライト、または他の外部参照源などから、国際標準時刻、協定世界時 (UTC) と一致するように時刻を更新できます。 **clock set** コマンドは、時刻を徐々に修正することでこの作業を実行します。

-abruptly オプションを指定して使用される **clock set** コマンドおよび **dts synchronize** コマンドは、システム・クロックの調整およびシステムの同期化を実行するための追加的な方法を提供しています。しかし、例のコードも外部タイム・プロバイダーも IBM ではサポートしていません。



---

## セキュリティ・サービス保守作業

以下のサブセクションでは、セキュリティ・サービス管理時に実行する保守作業を要約しています。セキュリティの保守作業に関する詳細な説明は、*IBM DCE for AIX and Solaris* バージョン 3.2: 管理ガイド--コア・コンポーネント を参照してください。

## セキュリティ・サービスの管理

セキュリティ・サービス管理作業には次のものがあります。

- **dcecp** を使用するアカウントの作成と保守

**dcecp** は、人、ユーザー・グループ、およびアカウントなどのレジストリー情報の作成および保守のためのコマンドを用意しています。

DCE アカウントを管理する場合、次のことに留意してください。

- レジストリーを使用しない他のシステムとファイルを共有する場合は、レジストリーと外部パスワードおよびグループ・ファイル間で名前、UNIX ID、およびアカウント情報の互換性があることを確認してください。

**passwd\_import** を使用して、存在する競合を識別し解決します。*IBM DCE for AIX and Solaris* バージョン 3.2: 管理ガイド--コア・コンポーネント では、**passwd\_import** の動作を説明しています。

- 標準 UNIX 形式の **/etc/passwd** および **/etc/group** ファイルを保守する場合は、**passwd\_export** を実行し、ローカル・マシン上のパスワード、グループ、および編成ファイルをレジストリーと整合性を持たせるようにする必要があります。**passwd\_export** コマンドの詳細な説明は、*IBM DCE for AIX and Solaris* バージョン 3.2: 管理ガイド--コア・コンポーネント を参照してください。
- セル内のオブジェクトをアクセスする他のセルのプリンシパルに対しては、セルのレジストリー内に外部セルのための特別なアカウントを設定する必要があります。このアカウントは、外部の認証サービスがそのユーザーを正しく認証していることを信頼する、ということを示します。外部セルのアカウントを作成するためには、**dcecp registry connect** コマンドを使用します。

- ACL の使用

セル・ネーム・スペース内の特定のオブジェクトの ACL エントリーを表示、追加、修正、および削除するためには、**dcecp acl** コマンドを使用します (**dcecp acl** コマンドの使用の詳細な説明は、*IBM DCE for AIX and Solaris* バージョン 3.2: 管理ガイド--コア・コンポーネント を参照してください)。

- レジストリー・ポリシーの設定および保守

レジストリー・ポリシーには、あるパスワードとアカウント情報が含まれます。ポリシーには、特定のマシンに結び付けられた例外であるオーバーライドも含まれます。レジストリー・ポリシーを設定および保守するためには、**dcecp registry** コマンドを使用します。これらのコマンドの詳細は、*IBM DCE for AIX and Solaris* バージョン 3.2: 管理ガイド--コア・コンポーネント に記載されています。

チケット有効期限、パスワードの存続期間、パスワード形式、およびパスワード有効期限日などは設定できるレジストリー・ポリシーの例です。たとえば、パスワード形式に対して、組織ポリシーおよびレジストリー・ポリシーの両方が存在する場合、より制限的なポリシーが適用されます。

レジストリーに含まれる情報にオーバーライドを設定できます。オーバーライド情報は、ローカル・マシン上の **passwd\_override** および **group\_override** ファイルに格納されています。**passwd\_override** ファイルには、ホーム・ディレクトリー、ログイン・シェル、パスワードをオーバーライドするためのエントリー、および GECOS 情報 (オフィスおよび電話番号など、ユーザーにより使用される一般的な情報ですがシステムでは不要なもの) が含まれています。

**passwd\_override** ファイルの編集方法の詳細は、*IBM DCE for AIX and Solaris* バージョン 3.2: 管理ガイド--コア・コンポーネント を参照してください。

注: パスワード満了またはパスワード存続時間に関するセル・ポリシーが **forever** 以外に設定されていると、**dce\_rgy** なども含めすべてのプリンシパルに適用されます。この制限を超えると、**secd** は認証処理を実行できません。したがって、セキュリティー・サーバーは操作不能になります。したがって、これらの制限項目を **forever** に設定し、他の制限項目は組織またはアカウントを基準に設定することをお勧めします。

- レジストリーのバックアップ

*IBM DCE for AIX and Solaris* バージョン 3.2: 管理ガイド--コア・コンポーネント は、マスター・レジストリー・サイトのために従わなければならないバックアップ手順を説明しています。データベースを復元する場合、これは自動的にスレーブまで伝搬されます。

*IBM DCE for AIX and Solaris* バージョン 3.2: DCE セキュリティー・レジストリーと LDAP 統合 には、LDAP セキュリティー・サーバー上でのレジストリーのバックアップに関する情報が含まれています。

- LDAP セキュリティー・サーバーの管理

LDAP セキュリティー・サーバーを使用するセルの管理やトラブルシューティングに関する用は、*IBM DCE for AIX and Solaris* バージョン 3.2: DCE セキュリティー・レジストリーと LDAP 統合 を参照してください。

- 監査サービス・データの設定および保守

監査サービス・データには、イベント番号、イベント・クラス番号、イベント・クラス・ファイル、監査フィルター、および監査証跡が含まれます。監査サービス・データを管理するためには、**dcecp aud**、**audevents**、**audfilter**、および **audtrail** コマンドを使用します。*IBM DCE for AIX and Solaris* バージョン 3.2: 管理コマンド・リファレンス は、監査関連 **dcecp** オブジェクトおよびコマンドを説明しています。監査サービス管理に関する詳細な説明は、*IBM DCE for AIX and Solaris* バージョン 3.2: 管理ガイド--コア・コンポーネント を参照してください。

- トラブルシューティング

日常の管理手順では解決できない問題に遭遇した、またはハードウェア障害によりレジストリー操作が停止した場合、使用できるいくつかのトラブルシューティング手順があります。*IBM DCE for AIX and Solaris* バージョン 3.2: 管理ガイド--コア・コンポーネント は、以下の作業を説明しています。

- レジストリー・レプリカの再作成
- マスター・レジストリーの回復
- レプリカの強制的削除
- その所有者が削除されたため、孤児となったレジストリー・オブジェクトの受付

## レジストリーの再構成

セキュリティー・サービスの管理に含まれる 2 つの主要な再構成作業があります。以下の作業は、*IBM DCE for AIX and Solaris* バージョン 3.2: 管理ガイド--コア・コンポーネント で説明しています。

- マスター・レジストリー・サーバーを実行するマシンを、自分のネットワークから除去する、または一定期間、そのマシンをシャットダウンする計画である場合に、マスター・レジストリーのサイトを変更する。
- スレーブ・レジストリー・サーバーを実行させているマシンをネットワークから除去する、またはそのマシンを一定期間シャットダウンする計画である場合に、ネットワークからサーバー・ホストを除去する。

---

## 有効期限が切れた認証ファイルの削除

`/var` ファイル・システムは有効期限が切れた認証ファイルを削除しない場合など、定期的にいっぱいになる可能性があります。 `root` の場合は、`rmxcred` ツールを使用して、認証ディレクトリー (`dcelocal/var/security/creds`) から有効期限が切れたチケットを削除できます。このツールは、`cron` ジョブがこのツールを毎日実行するようにセットアップするなどして、定期的に行うことができます。



---

## 第2部 追加構成情報



---

## 第6章 構成応答ファイル

応答ファイルには、通常はコマンド行に指定する情報が含まれています。応答ファイルを使用すると、コマンド行に情報を入力する必要がなくなるため、構成プロセスを自動化できます。応答ファイルは、**config.dce** および **unconfig.dce** コマンドで使用できます。これらのコマンドの詳細な説明は、*IBM DCE for AIX and Solaris* バージョン 3.2: 管理コマンド・リファレンス を参照してください。

プロセスの一部だけを自動化したい場合は、一部だけまたはいくつかのオプションの情報が含まれた部分応答ファイルを作成できます。次に、コマンド行に残りのオプションを指定できます。コマンド行で指定されたオプションは、応答ファイルで提供される値をオーバーライドします。

DCE 応答ファイルは、複数の管理構成の実行時に非常に役立つことがあります。グローバル・セクションでは、すべてのマシンの共通情報を定義することができます。個々のホスト・セクションでは、どのマシンで構成ステップを実行させるのかを指定することができます。このような応答ファイルを使えば、**config.dce** または **unconfig.dce** コマンドは、一度しか起動しなくてよくなります。

応答ファイル内の各行には、キーワードと関連値が含まれています。この値は、コマンド行に入力した場合と同様に構成プログラムにより使用されます。次の例を考えてください。

```
dce_hostname=georgia
```

この例では、キーワードは **dce\_hostname** で、関連値は **georgia** です。構成プログラムは、**-dce\_hostname** コマンド行オプションの値として **georgia** を使用します。

DCE for AIX パッケージには 1 つのサンプル応答ファイル (**DCE Client Services**) が含まれています。このファイルを使用して自分自身の応答ファイルを作成します。次の操作を実行します。

1. `/opt/dcelocal/etc/rspfiles/dce_smpl.rsp` を `XXXXXXXXX.RSP` としてコピーします。ここで、`XXXXXXXXX` は新しい応答ファイルに選択する名前です。
2. 自分のインストール・システムに合わせ、キーワード値を変更することでファイルを編集します。

注: キーワードを削除したり値を変更することはできますが、キーワード名を変更することはできません。

---

### DCE 応答ファイルのキーワード

DCE 構成応答ファイルには、セル情報とホスト (マシン) 情報の 2 種類の情報が含まれています。(通常、セル情報はある応答ファイルに格納され、ホスト情報は別の応答ファイルに格納されます。次に、これらのファイルのいずれかを他のファイルに組み込むことで、これらのファイルはリンクされます。これによりセル内のマシンは、それぞれ、同じセル応答ファイルと個別ホスト・ファイルを使用できるようになります。)

応答ファイル内のすべての情報は任意選択です。DCE 構成プログラムが応答ファイルに含まれていない情報を必要とする場合、その情報が見つからない旨の情報を構成インターフェースが通知します。

応答ファイルは、ASCII テキスト編集プログラムを使用して作成できます。編集ファイルを使用して応答ファイルを作成する場合は、以下のフォーマット規則を参照してください。

- 各行は、コメントか応答行のいずれかです。空白行はコメント行として扱われます。
- コメント行の最初の空白以外の文字はアスタリスク (\*) または番号記号 (#) でなければなりません。コメントを応答行に組み込むことはできません。
- キーワードは大文字小文字の区別はなく、行の任意の個所から開始できます。しかし、値が 1 つしかないキーワードの場合は、全体を 1 行で指定する必要があります。
- 応答行には、次の形式のいずれかの情報が含まれていなければなりません。

#### 値ストリング

応答行には、キーワード、等号 (=)、および値が含まれます。たとえば次のとおりです。

```
config_type=local
```

値ストリングは 1 行でなければならず、括弧を含めることはできません。

#### 値リスト

応答行には、キーワード、等号 (=)、および括弧で囲まれたいくつかの値をコンマで区切ったものが含まれます。値リスト内の各値は、1 つの値でも値ストリングでも構いません。たとえば次のとおりです。

```
host_id=(  
  tcpip_name=chariot.roma.italia.com  
)
```

値リストに別の値リストを含むこともでき、また空でも構いません。行に終了括弧 ")" だけを指定すると、値リストの最後を指定したことになります。

- 応答ファイルのセクション内のキーワードの順序は任意で構いません。
- 応答ファイルを別の応答ファイルに組み込むためには、**include** キーワードを使用します。たとえば次のように指定します。

```
⋮  
include /mydir/svrresp2.rsp  
⋮
```

## セル・セクション・キーワード

応答ファイルのセル・セクションには、セル全体に適用されるキーワードおよび情報が含まれます。このため、セル情報だけのための応答ファイルを作成できます。このファイルをいくつかのホスト応答ファイルに組み込むことができます。

以下のキーワードは、セルに関連する情報を指定します。これらのキーワードは、セル・セクションでだけ使用します。



表 1. DCE セル・キーワード

キーワード	値のタイプ	値の制限	コマンド行オプション
<b>cell_name</b>	PCS (スペースおよび @、:、および - 文字を除く)	最大長: 220	<b>-cell_name</b>
<b>cell_administrator</b>	PCS (スペースおよび @、:、および - 文字を除く)	最大長: 255	<b>-cell_admin</b>
<b>cell_admin_unix_id</b>	数字	範囲: 0~2、147、483、647	<b>-cell_admin_unix_id</b>
<b>max_unix_id</b>	数字	範囲: 0~2、147、483、647	<b>-max_unix_id</b>
<b>min_group_unix_id</b>	数字	範囲: 0~2、147、483、647	<b>-min_group_id</b>
<b>min_organization_unix_id</b>	数字	範囲: 0~2、147、483、647	<b>-min_org_id</b>
<b>min_principal_unix_id</b>	数字	範囲: 0~2、147、483、647	<b>-min_princ_id</b>
<b>master_security_server</b>	値リスト	51ページの表4	<b>-sec_master</b>
<b>cds_server</b>	値リスト	51ページの表4	<b>-cds_server</b>
<b>host</b>	値リスト	50ページの表2	(該当せず)

## ホスト・セクション・キーワード

ホスト情報は、応答ファイルのホスト・セクションに含まれています。ホスト・セクションは **host=(** キーワードで始まり、右括弧 **)** で終わります。応答ファイルのホスト・セクションは、ホスト・キーワードだけで構成されます。ホスト・セクション内のセル・キーワードは無視されます。

ホスト・セクションには次の 2 つのタイプがあります。

### グローバル

応答ファイルは、グローバル・ホスト・セクションを 1 つだけ含むことができます。これは、後続の特定ホスト・セクションのための構成値を初期設定するために使用される情報のためのセクションです。応答ファイルのグローバル・セクションには、**dce\_hostname** または **host\_id** キーワードは含まれません。グローバル・ホスト・セクションが応答ファイルに含まれている場合は、検出される最初のホスト・セクションでなければなりません。DCE 構成プログラムが最初のホスト・セクションの後ろにグローバル・ホスト・セクションを検出すると、警告がログ・ファイルに出され、そのグローバル・セクションは無視されます。

**特定** **dce\_hostname** または **host\_id** キーワードが含まれます。特定ホスト・セクションには、特定ホストの構成値が含まれます。特定ホスト・セクションは、キーワードを指定してそれらを別の値に設定することで、グローバル値をオーバーライドします。応答ファイルには、複数の特定ホスト・セクションを組み込むことができます。

以下の表は、ホスト情報キーワードを説明しています。

表2. DCE ホスト・キーワード

キーワード	値のタイプ	値の制限	コマンド行オプション
<b>config_type</b>	オプション	選択項目: <b>full</b> 、 <b>admin</b> 、 <b>local</b>	<b>-config_type</b>
<b>cds_replica</b>	値リスト	表3	<b>-cds_replica_list</b>
<b>dce_hostname</b>	テキスト	最大長: 255	<b>-dce_hostname</b>
<b>lan_profile</b>	テキスト	最大長: 255	<b>-lan_profile</b>
<b>wrap_audit_trail</b>	オプション	選択項目: <b>yes</b> 、 <b>no</b>	<b>-wrap_audit_trail</b>
<b>host_id</b>	値リスト	表3	(該当せず)
<b>protocols<sup>1</sup></b>	オプション	選択項目: <b>tcip_connection_oriented</b> 、 <b>tcip_connectionless</b> 、 <b>all</b> 、 <b>none</b>	<b>-protocol</b>
<b>autostart</b>	オプション	選択項目: <b>yes</b> 、 <b>no</b>	<b>-autostart</b>
<b>clean_autostart</b>	オプション	選択項目: <b>yes</b> 、 <b>no</b>	<b>-clean_autostart</b>
<b>sync_clock</b>	オプション	選択項目: <b>yes</b> 、 <b>no</b>	<b>-sync_clocks</b>
<b>sync_server</b>	値リスト	表3	<b>-time_server</b>
<b>components</b>	値リスト	51ページの表4	(該当せず)
<b>public_key</b>	値リスト	52ページの表7	(該当せず)
<b>ldap_registry</b>	値リスト	52ページの表7	<b>-ldap_registry</b>
注: 1. このキーワードにはコンマで区切られた値を指定します。コンマとトークン間にはスペースは指定できません。たとえば次のように指定します。 protocols=tcip_connection_oriented,tcip_connectionless			

## マシンを識別するためのキーワード

いくつかのセルおよびホスト・キーワードには、ホストと通信するマシン（通常はサーバー）のネットワーク ID が含まれた値リストを指定する必要があります。マシンのネットワーク ID は、値を指定した 1 つまたは複数の以下のキーワードを使用して指定できます。

表3. ホスト識別値

キーワード	値のタイプ	値の制限	コマンド行オプション
<b>tcip_name</b>	IP ホスト名	ドット付き形式、最大長: 255; 例: uniqienm.domain.ibm.com	<b>-host_id</b>
<b>tcip_addr</b>	IP アドレス	ピリオドで区切られた数字、最大長: 15; 例: 123.45.67.89	<b>-host_id</b>

## コンポーネント・キーワードの値

コンポーネント・キーワードは、ホストに構成するコンポーネントを識別します。コンポーネント値リストには、51ページの表4 に示されているいくつかのコンポーネントを組み込むことができます。

以下の表は、コンポーネントを指定するために使用できるキーワードおよび各コンポーネントに必要な値の一覧です。

表4. コンポーネント・キーワード

キーワード	説明	値のタイプ	値	コマンド行オプション
<b>client</b>	すべてのクライアント・コンポーネント	値リスト	表5	<b>all_cl</b>
<b>nsid</b>	ネーム・サービス・インターフェース・デモン	値リスト	表5	<b>nsid</b>
<b>pam</b> (Solaris のみ)	移植可能な認証モジュール	値リスト	表5	<b>pam</b>
<b>nsswitch</b> (Solaris のみ)	ネーム・サービス・スイッチ	値リスト	表5	<b>nsswitch</b>
<b>slim_client</b>	スリム・クライアント・コンポーネント	値リスト	表5	<b>slim_cl</b>
<b>sec_cl</b>	セキュリティー・クライアント	値リスト	表5	<b>sec_cl</b>
<b>sec_svr</b>	マスター・セキュリティー・サーバー	値リスト	表5	<b>sec_srv</b>
<b>sec_rep</b>	セキュリティー・レプリカ・サーバー	値リスト	表5	<b>sec_rep</b>
<b>cds_cl</b>	CDS クライアント	値リスト	表5	<b>cds_cl</b>
<b>cds_svr</b>	初期 CDS サーバー	値リスト	表5	<b>cds_srv</b>
<b>cds_second</b>	追加 CDS サーバー	値リスト	表5	<b>cds_second</b>
<b>gda_svr</b>	グローバル・ディレクトリー・エージェント	値リスト	表5	<b>gda</b>
<b>dts_client</b>	DTS クライアント	値リスト	表5	<b>dts_cl</b>
<b>dts_local</b>	DTS ローカル・サーバー	値リスト	表5	<b>dts_local</b>
<b>dts_global</b>	DTS グローバル・サーバー	値リスト	表5	<b>dts_global</b>
<b>rpc</b>	RPC	値リスト	表5	<b>rpc</b>
<b>sec_audit</b>	監査	値リスト	表5	<b>audit</b>
<b>pw_strength_svr</b>	パスワード同期サーバー (複数も可)	値リスト	表5	<b>pw_strength_srv</b>
<b>ems</b>	イベント管理サービス	値リスト	表5	<b>ems_srv</b>
<b>snmp</b>	DCE SNMP サブエージェント	値リスト	表5	<b>snmp_srv</b>
<b>idms</b>	アイデンティティー・マッピング・サーバー	値リスト	表5	<b>idms</b>
<b>dceunixd</b> (AIX のみ)	統合ログイン	値リスト	表5	<b>dce_unixd</b>

表5. コンポーネント一般キーワード

キーワード	値のタイプ	値の制限	コンポーネント	コマンド行オプション
<b>config_state</b>	オプション	選択項目: <b>configured</b> 、 <b>not_configured</b>	すべてのコンポーネント	(該当せず)

表 5. コンポーネント一般キーワード (続き)

キーワード	値のタイプ	値の制限	コンポーネント	コマンド行オプション
<b>unconfig_depend</b>	オプション	選択項目: <b>yes</b> 、 <b>no</b>	すべてのコンポーネント	<b>-dependents</b>
<b>force_unconfig</b>	オプション	選択項目: <b>yes</b> 、 <b>no</b>	すべてのコンポーネント	<b>-force</b>
<b>name</b>	テキスト	最大長 255	secrep、secsvr	<b>-sec_server_name</b>
<b>proxy</b>	オプション	選択項目: <b>yes</b> 、 <b>no</b>	cds_cl	<b>-proxy</b>
<b>clearinghouse</b>	テキスト	最大長 255	cds_second	<b>-clr_house</b>
<b>ldap_server<sup>1</sup></b>	テキスト	最大長 255	gda_svr	<b>-ldap_server</b>
<b>role</b>	オプション	選択項目: <b>noncourier</b> 、 <b>courier</b> 、 <b>backupcourier</b>	dts_local、dts_global	<b>-courier_role</b>
<b>server_command</b>	テキスト	最大長 255	pw_strength_svr	<b>-pwdstr_cmd</b>
<b>command_args</b>	テキスト	最大長 255	pw_strength_svr	<b>-pwdstr_arg</b>
<b>account</b>	値リスト	表6	pw_strength_svr	(該当せず)
<b>no_pesite_update</b>	オプション	選択項目: <b>yes</b> 、 <b>no</b>	rpc	<b>-no_pesite_update</b>
<b>pesite_update_time</b>	数字	範囲: 10~1440	rpc	<b>-pesite_update_time</b>
<b>num_dce_unixd</b>	数字	範囲: 1~5	dceunixd	<b>-num_dce_unixd</b>
<b>cache_lifetime</b>	数字	範囲: 2~120	dceunixd	<b>-cache_lifetime</b>

注: 1. **gdd\_svr** コンポーネントの値リスト中と **ldap\_registry** 値リスト中の両方の **ldap\_server** キーワードの値が指定されている場合は、**ldap\_registry** 値リスト中に指定されている値がオーバーライドします。

表 6. アカウント・キーワード

キーワード	値のタイプ	値の制限	コマンド行オプション
<b>name</b>	テキスト	最大長: 255	<b>-pwdstr_principal</b>
<b>protect_level</b>	オプション	選択項目: <b>pktprivacy</b> 、 <b>pktinteg</b> 、 <b>cdmf</b>	<b>-pwdstr_protect_level</b>

表 7. 公開鍵証明キーワード

キーワード	値のタイプ	値の制限	コマンド行オプション
<b>certificate_based_login</b>	オプション	選択項目: <b>yes</b> 、 <b>no</b>	<b>-certificate_based_login</b>
<b>kdc_ini_file</b>	テキスト	最大長: 511	<b>-kdc_ini_file</b>
<b>kdc_profile</b>	テキスト	最大長: 255	<b>-kdc_profile</b>
<b>kdc_passphrase</b>	テキスト	最大長: 511	<b>-kdc_passphrase</b>

表 8. LDAP レジストリー・キーワード

キーワード	値のタイプ	値の制限	コマンド行オプション
<b>ldap_server<sup>1</sup></b>	テキスト	最大長: 255	<b>-ldap_server</b>
<b>ldap_dn</b>	テキスト	最大長: 255	<b>-ldap_dn</b>
<b>ldap_dn_pw</b>	テキスト	最大長: 511	<b>-ldap_dn_pw</b>
<b>ldap_ssl</b>	オプション	選択項目: <b>yes</b> 、 <b>no</b>	<b>-ldap_ssl</b>

表 8. LDAP レジストリー・キーワード (続き)

キーワード	値のタイプ	値の制限	コマンド行オプション
<b>ldap_keyring</b>	テキスト	最大長: 511	<b>-ldap_keyring</b>
<b>ldap_keyring_pw</b>	テキスト	最大長: 511	<b>-ldap_keyring_pw</b>
<b>ldap_auth</b>	オプション	選択項目: <b>none</b> 、 <b>ssl</b> 、 <b>gssapi</b> 、 <b>cram-md5</b>	<b>-ldap_auth</b>
<b>ldap_master_key_in_ldap</b>	オプション	選択項目: <b>yes</b> 、 <b>no</b>	<b>-ldap_master_key_in_ldap</b>
<b>ldap_dce_master_key</b>	テキスト	最大長: 511	<b>-ldap_dce_master_key</b>

注: 1. **ldap\_registry** コンポーネントの値リスト中と **gda\_svr** 値リスト中の両方の **ldap\_server** キーワードの値が指定されている場合は、**ldap\_registry** 値リスト中に指定されている値がオーバーライドします。



## 付録A. 初期 CDS サーバーの移動

注: この手順は、2 番目の CDS サーバーがすでに定義されている場合だけ有効です。1 つまたは複数の CDS サーバーが活動状態でマスター・レプリカが異なったクリアリングハウスに分散している場合は、この手順は有効ではありません。レプリカ・セットを定義するとき、既存のすべてのレプリカを指定する必要があります。

1. 初期 CDS サーバーにしたい追加 CDS サーバーをマシン上に作成します。この新しい CDS サーバーを BoxB とします。オリジナルのマスター CDS サーバーのあるマシンを BoxA とします。

```
# config.dce cds_second  
または (AIX のみ)  
# smit mkcdssrv
```

2. 両方のマシン上で cell\_admin として DCE にログインします。
3. cdsli コマンドを使用し、CDS 内のディレクトリーを検査します。すべてのディレクトリーを BoxA から BoxB にコピーします。

```
# cdsli -dR
```

4. 追加 CDS サーバーが BoxB 上で空であることを確認します。

```
# cdscp  
cdscp> set cdscp preferred clearinghouse ./:<BoxB>_ch  
cdscp> show dir ./:/*  
cdscp> quit
```

5. 新規の追加 CDS サーバーの (BoxB) クリアリングハウスにすべての CDS ディレクトリーの複製を作成し、それらをマスター・レプリカにします。

```
# for dir in $(cdsli -R); do  
> echo "Creating replica for $dir"  
> cdscp create replica $dir clear ./:<BoxB>_ch  
> done  
  
# for dir in $(cdsli -R); do  
> echo "Swapping master CDS attribute for $dir"  
> cdscp set dir $dir to new epoch master ./:<BoxB>_ch readonly ./:<BoxA>_ch  
> done  
  
cdscp set dir ./: to new epoch master ./:<BoxB>_ch readonly ./:<BoxA>_ch
```

6. スワップが実行されたことを確認します。/: ディレクトリーが BoxB のクリアリングハウスに存在することなど、すべてについてマスター・レプリカを調べます。

```
# cdscp  
cdscp> show dir ./:  
cdscp> show dir ./:/*
```

7. DCE を停止して再始動し、両方のマシン上で CDS キャッシュを削除します。

```
# stop.dce  
# cd /var/dce/adm/directory/cds  
# rm cds_cache.*  
# start.dce
```

または

```
# stop.dce  
# clean_up.dce  
# start.dce
```

8. BoxA から追加 CDS サーバーを削除したい場合は、

```
# unconfig.dce cds_second
```

9. DCE を開始して再始動し、セル内のすべてのシステムで CDS クライアント・キャッシュ再生処理を実行します。

```
# stop.dce  
# cd /var/dce/adm/directory/cds  
# rm cds_cache.*#  
start.dce
```

または

```
# stop.dce  
# clean_up.dce  
# start.dce
```



---

## 付録B. 環境変数

環境変数は DCE が使用する変数で、ユーザーが自分自身で設定できます。これらの変数は、監査、CDS/XDS、構成、IDL、NLS/セキュリティ、RPC、およびセキュリティ変数に関する以下の節で説明しています。

---

### 監査変数

DCE 監査環境変数の設定を、以下のトピックで説明します。

#### DCEAUDITON

**目的** アプリケーションについて監査をオンにします。

**形式**

DCEAUDITON = <any\_value>

**説明**

アプリケーション開始時にこの変数を宣言しておくこと、監査がオンになります。

開始時にこの変数を指定するかどうかにより、どのアプリケーションが監査を使用するかを選択できます。

**例**

DCEAUDITON=1

#### DCEAUDITOFF

**目的** アプリケーションの監査をオフにします。

**形式**

DCEAUDITOFF = <any\_value>

**説明**

アプリケーション開始時にこの変数を宣言すると、監査はオフになります。これは、**DCEAUDITON** より優先されます。両方を宣言すると、監査はオフになります。監査は、デフォルトではオフです。

開始時にこの変数を指定するかどうかにより、どのアプリケーションが監査を使用するかを選択できます。

**例**

DCEAUDITOFF=1

#### DCEAUDITFILTERON

**目的** アプリケーションに関するイベント・フィルターをオンにします。

**形式**

DCEAUDITFILTERON = <any\_value>

## 説明

アプリケーション開始時にこの変数を宣言すると、監査フィルターがオンになります。デフォルトではオフです。

開始時にこの変数を指定するかどうかにより、どのアプリケーションがイベント・フィルターを使用するかを選択できます。

**注:** バインディングをエンドポイント・マップへエクスポートしないプログラムでフィルターをオンにすると (たとえば、RPC ベース・アプリケーション・サーバーでない)、監査ではそのプログラムにより生成されるイベントを処理できなくなります。

## 例

```
DCEAUDITFILTERON
```

### DCEAUDITTRAILSIZ

**目的** 監査証跡の最大サイズを設定します。

#### 形式

```
DCEAUDITTRAILSIZ = <size_in_bytes>
```

#### 説明

アプリケーション開始時にこの変数を宣言すると、その値は書き込み先の監査証跡の最大サイズを指定します。

## 例

```
DCEAUDITTRAILSIZ=1000000
```

### DCEAUDITWRAP

**目的** アプリケーションがラップするためのストレージ・ストラテジーを設定します。

#### 形式

```
DCEAUDITWRAP = <any_value>
```

#### 説明

アプリケーション開始時にこの変数を宣言すると、アプリケーションの書き出し先になる監査証跡はラップ・ストレージ・ストラテジー (**aud\_c\_trl\_ss\_wrap**) を使用します。ラップがオンのとき、監査はサイズ限界値に達するまで監査レコードを書き出します。その後、証跡の先頭までラップし、そこから監査レコードの書き出しを継続します。保管ストレージ・ストラテジー (**aud\_c\_trl\_ss\_store**) がデフォルト値です。これは、アプリケーションが監査レコードを送信する先の監査証跡にだけ適用されます。

## 例

```
DCEAUDITWRAP=1
```

### SECDAUDITWRAP

**目的** セキュリティー・サーバーがラップするためのストレージ・ストラテジーを設定します。

#### 形式

SECDAUDITWRAP = <any\_value>

#### 説明

セキュリティー・サーバー開始時にこの変数を宣言すると、ラップ・ストレージ・ストラテジー (**aud\_c\_trl\_ss\_wrap**) を使用します。ラップがオンのとき、監査はサイズ限界値に達するまで監査レコードを書き出します。その後、証跡の先頭までラップし、そこから監査レコードの書き出しを続けます。保管ストレージ・ストラテジー (**aud\_c\_trl\_ss\_save**) がデフォルト値です。

#### 例

SECDAUDITWRAP = 1

---

## 構成

### DCELOCAL

目的 **/opt/dcelocal** パスを設定します。

### DCE\_CFG\_LOG\_MAX

目的 DCE 構成ログのサイズを変更します。デフォルト値は 100,000 バイトです。

### DCE\_CONFIG\_LOGPATH

目的 DCE 構成ログを再配置します。

---

## EMS

DCE イベント管理サービス (EMS) 変数の設定を、以下のトピックで説明します。

### EMS\_QUEUE\_SIZE

目的 EMS デーモン (emsd) のイベント・キューを設定します。

#### 形式

```
export EMS_QUEUE_SIZE=n (n > 0)
```

説明 **EMS\_QUEUE\_SIZE** 環境変数を使用して、EMS イベント・キューのサイズを設定できます。キューがいっぱいになったことを示すエラーを EMS が受け取り始めたら、キューのサイズを大きくしてデーモンを再始動する必要があります。

デフォルトのキュー・サイズは 512 です。キュー・サイズはゼロより大きい任意の整数値に設定できますが、キューが小さすぎたり大きすぎたりしないようにする必要があります。キューがいっぱいであることを示すエラーを受け取らなくなるまで、256 ずつ値を大きくしてみてください。

DCE を再始動しないと変更内容は有効になりません。

#### 例

```
export EMS_QUEUE_SIZE=768
```

## EMS\_EVENTLOG\_DIR

**目的** EMS イベント・ログを入れるディレクトリーを設定します。

**形式**

```
export EMS_EVENTLOG_DIR=<path to log directory>
```

**説明** EMS イベント・ログを使用して、EMS が失敗した場合のイベントが格納されます。EMS はすべてのイベントをイベント・ログに書き込み、イベントを受け取ることになっているすべての消費側にイベントが伝送された後にイベント・レコードを削除します。イベント・ログは、**emsd** を実行しているマシン上のファイルに保持されます。

変更内容を有効にするには、DCE を再始動しなければなりません。

**emslog** オブジェクトは EMS イベント・ログを表します。たとえば、**dcecp -c emslog show** を使用して、コマンド行からイベント・ログを表示できます。

**例**

```
export EMS_EVENTLOG_DIR=/tmp
```

---

## IDL

DCE IDL 環境変数の設定を、以下のトピックで説明します。

### IDL\_GEN\_AUX\_FILES

**目的** コンパイルのためのダミー補助ファイルを生成します。

**形式**

```
export IDL_GEN_AUX_FILES=<any value>
```

**説明** 古いリリースで IDL コンパイラーが生成する補助ファイル (**\_caux.c** および **\_saux.c**) は生成されなくなりました。スタブおよびヘッダー・ファイルだけが必要です。古いアプリケーションの Makefile にはこれらのファイルに対する参照が含まれていることがあります。したがって、以前の DCE リリースからマイグレーションするユーザーは、アプリケーション Makefile からこれらの補助ファイルに対する参照を削除しなければならないことがあります。また、Makefile エラーを回避するために、環境変数 **IDL\_GEN\_AUX\_FILES** を (任意の値に) 設定してダミー補助ファイルを生成することもできます。

**例**

```
export IDL_GEN_AUX_FILES=1
```

### IDL\_GEN\_INTF\_DATA

**目的** ストレージ情報リストを生成スタブ・ファイルのタイプ・ベクトル定義に追加します。

**形式**

```
export IDL_GEN_INTF_DATA=any value
```

## 説明

この環境変数が NULL でないと、IDL コンパイラーはクライアント・スタブおよびサーバー・スタブ・ファイル内のタイプ・ベクトル定義にストレージ情報リストを追加します。

## 例

```
export IDL_GEN_INTF_DATA=1
```

---

## NLS/セキュリティー

DCE NLS/セキュリティー 環境変数の設定を、以下のトピックで説明します。

### DCE\_USE\_NONPORTABLE\_NAMES

**目的** PGO 名の OSF 命名規則を拡張し、DCE ポータブル文字セット外の文字を使用できるようにします。

### 形式

```
DCE_USE_NONPORTABLE_NAMES=1
```

### 説明

標準 (OSF) DCE に従い、プリンシパル名などのセキュリティー・ネーム・スペースのエントリーは、DCE ポータブル文字セットに含まれる文字でだけ構成できます (DCE 紹介の DCE のアーキテクチャーの概要を参照)。DCE for AIX バージョン 3.2 ではオーバーライド機能を用意していて、非ポータブル文字を使用できるようにしています。この機能は、コード・セットが同種である環境でだけ、およびすべての DCE インストール・システムがこの拡張機能をサポートしている環境でだけ使用してください。非ポータブル文字を使用するセキュリティー・ネーム・スペース・エントリーの正しい動作が保証されるのは、企業全体のコード・セットが名前を作成するプロセスのコード・セットと等しい場合だけです。非ポータブル・セキュリティー名を使用可能にするためには、DCE セキュリティーが実行されるすべてのクライアントおよびサーバー・プロセスにおいて、DCE を開始する前にこの環境変数を設定する必要があります。

## 例

```
DCE_USE_NONPORTABLE_NAMES=1
```

### DCE\_USE\_WCHAR\_NAMES

**目的** CDS 名を処理するときに、特定のユーザー制約アジア環境においてパフォーマンスを向上させます。

### 形式

```
DCE_USE_WCHAR_NAMES=0
```

### 説明

標準 (OSF) DCE に従い、ディレクトリー名などの CDS ネーム・スペースの一部のエントリーは、DCE ポータブル文字セット外からの文字で構成できます。DCE では CDS 名のコード・セット変換を実行しないため、非ポータブル文字はコード・セットに関して同種である環境でだけ使用してください。アジア・ロケールを使用する場合で名前をポータブル文字セットに限定する場合は、この環

境変数を 0 に設定することでパフォーマンスは向上します。デフォルトでは、1 に設定されています。

例

```
DCE_USE_WCHAR_NAMES=0
```

---

## RPC

DCE RPC 環境変数の設定を、以下のトピックで説明します。

### DCERPCCHARTRANS

**目的** 置き換え ASCII/EBCDIC 変換テーブルが含まれたファイルを指します。

**形式**

```
export DCERPCCHARTRANS=file name
```

**説明** 環境変数 **DCERPCCHARTRANS** に指定されたファイルには、ASCII から EBCDIC および EBCDIC から ASCII のテーブルに関する置き換え変換テーブルが含まれています。このファイルは、RPC 実行時ルーチンに含まれるデフォルト・テーブルを置き換えます。

例

```
export DCERPCCHARTRANS=tmp.tab
```

### RPC\_CN\_AUTH\_SUBTYPE

**目的** RPC がパケットのエンコードを行うときに使用するチェックサム・アルゴリズムを決定します。

**形式**

```
export RPC_CN_AUTH_SUBTYPE=number  
/* where number is 0 for DES and 1 for MD5 */
```

**説明** この環境変数は、RPC がパケットをエンコードするときに使用するチェックサム・アルゴリズムを決定します。指定できる値は、8 バイト DES チェックサムの場合は 0 で、16 バイト MD5 チェックサムの場合は 1 です。この変数を設定しないと、デフォルト・アルゴリズムは MD5 になります。

例

```
export RPC_CN_AUTH_SUBTYPE=0
```

### RPC\_DEFAULT\_ENTRY

**目的** ディレクトリー・サービス探索に関する開始点を指定します。

**形式**

```
export RPC_DEFAULT_ENTRY=entry name in the namespace
```

**説明** インポートおよび探索ルーチンが互換性のあるサーバーに関するインディケーション情報を探索するための開始点として使用するネーム・サービス・データベース内のデフォルト・エントリーを指定します。通常、開始エントリーはプロファイルです。

デフォルト・エンタリー名を使用するアプリケーションは、この環境変数を定義する必要があります。RPC 実行時ルーチンでは、デフォルト値を用意していません。特に、**auto\_handle** IDL 属性を使用するときは、この環境変数は必須です。

たとえば、クライアント・アプリケーションがネーム・サービス・データベースを探索してサーバー・バインディング・ハンドルを見つけなければならないものと仮定します。アプリケーションは、**rpc\_ns\_binding\_import\_begin** ルーチンを探索の一部として使用できます。この場合、アプリケーションは、探索を開始するネーム・サービス・データベース内のエンタリーの名前をルーチンの *entry\_name* パラメーターに指定する必要があります。

**RPC\_DEFAULT\_ENTRY** 環境変数が指定しているエンタリーから探索を開始する場合は、アプリケーションはルーチン

**rpc\_ns\_binding\_import\_begin** 内のパラメーター *entry\_name* に値 NULL を指定する必要があります。

例

```
export RPC_DEFAULT_ENTRY=././Servers
```

#### **RPC\_DEFAULT\_ENTRY\_SYNTAX**

**目的** ディレクトリー・サービス・エンタリーの構文を指定します。

**形式**

```
export RPC_DEFAULT_ENTRY_SYNTAX=value
```

**説明** **RPC\_DEFAULT\_ENTRY** 環境変数に指定する名前の構文を指定します。さらに、名前構文パラメーターにデフォルト値を指定できる RPC NSI ルーチンの構文も提供します。有効な値は、デフォルト構文の場合は 0 で、DCE 構文の場合は 3 です。

**RPC\_DEFAULT\_ENTRY\_SYNTAX** 環境変数を定義しないと、RPC 実行時デフォルト値は DCE 名前構文になります。

例

```
export RPC_DEFAULT_ENTRY=3
```

#### **RPC\_DISABLE\_EP\_RESOLVE\_V4**

**目的** OS/390® ロード・バランシングのサポートを使用不能にします。

**形式**

```
export RPC_DISABLE_EP_RESOLVE_V4=any value
```

**説明** この環境変数を指定すると、RPC 実行時ルーチンは **rpc\_ep\_resolve\_binding** インターフェースのバージョン 3 をバージョンの 4 の代わりに使用します。バージョン 4 はエンドポイントと IP アドレスの両方を戻し、OS/390 がロード・バランシングの目的で異なった IP アドレスを戻すことができるようにしています。バージョン 3 ではエンドポイントだけを戻します。

例

```
export RPC_DISABLE_EP_RESOLVE_V4=YES
```

#### **RPC\_DISABLE\_SINGLE\_THREAD**

**目的** 単一スレッド動作を使用不能にします。

**形式**

```
export RPC_DISABLE_SINGLE_THREAD=any value
```

**説明** この環境変数は、コネクションレス RPC アプリケーションのクライアント側で単一スレッド動作を使用不能にします。通常は、この環境変数を使用する理由はないはずです。

**例**

```
export RPC_DISABLE_SINGLE_THREAD=YES
```

## RPC\_EXTRA\_INTERFACE

**目的** RPC ランタイムが使用する余分の IP インターフェースを追加します。

**形式**

```
export RPC_EXTRA_INTERFACE=ip address
```

**説明** この環境変数を使用して、余分の IP インターフェースを、RPC ランタイムが使用する IP インターフェースのリストに追加します。これは、RPC ランタイムがこのインターフェースの存在をまだ検出していないときに使用されます。

**例**

```
export RPC_EXTRA_INTERFACE=111.111.111.111
```

## RPC\_ITIMER\_SIGNAL

**目的** RPC が単一スレッドのときに使用される itimer 信号のタイプを指定します。

**形式**

```
export RPC_TIMER_SIGNAL=SIGVTALRM or SIGALRM
```

**説明** この環境変数は、RPC が単一スレッドのときに使用されるインターバル・タイマーのタイプを設定するために使用されます。指定できる値は **SIGVTALRM** および **SIGALRM** です。デフォルト値は **SIGVTALRM** です。 **SIGVTALRM** はタイプ **ITIMER\_REAL** のタイマーと **SIGVTALRM** 信号を指定します。 **SIGALRM** はタイプ **ITIMER\_REAL** のタイマーと **SIGALRM** 信号を指定します。

**例**

```
export RPC_TIMER_SIGNAL=SIGVTALRM
```

## RPC\_MAX\_UDP\_PACKET\_SIZE

**目的** 最大 UDP パケット・サイズを設定します。

**形式**

```
export RPC_MAX_UDP_PACKET_SIZE=number
```

**説明** RPC 実行時ルーチンは、**ncadg\_ip\_udp** プロトコルが使用されると、大きな RPC コールを 4352 バイトの UDP パケットにデフォルトで分割します。それより大きなパケットをサポートしなければならない場合は、**RPC\_MAX\_UDP\_PACKET\_SIZE** 環境変数を希望する最大サイズに設定できます。この環境変数はそれより小さな



値に設定し、UDP パケットの IP フラグメントが発生しないようにすることもできます。これが必要になるのは、パケットがリソースの極端に少ないネットワークを通過したり構成が間違っていて断片が除去されるファイアウォールを通過する場合です。

#### 例

```
export RPC_MAX_UDP_PACKET_SIZE=16384
```

### RPC\_NETADDRS\_ORDER

**目的** PRC 実行時ルーチンが使用する IP インターフェースの順序を定義します。

#### 形式

```
export RPC_NETADDRS_ORDER=ipaddress:ipaddress
```

**説明** この環境変数は、構成されている TCPIP ネットワーク・インターフェースの使用順序を指定します。つまり、ローカル TCPIP インターフェースが RPC 実行時ルーチンにより使用される順序を制御します。デフォルトでは、構成されているすべての TCPIP インターフェースを、戻される順序で使用します。CDS データベースおよびエンドポイント・マップへのサーバーの登録を、インターフェースを順序付けることで、制御できます。この環境変数に組み込まれていないインターフェースは、使用可能なインターフェースのリストの末尾に追加されます。これは、複数のネットワーク・アダプターがあり、一部のネットワーク・インターフェースを使用して DCE トラフィックをターゲットにしたり外したりしなければならないマシンで便利です。たとえば、あるインターフェースでのトラフィックが過密な場合に、そのインターフェースの順序を末尾にすると、DCE は他の使用率の低いインターフェースを使用します。インターフェースを除外してはいないので、他のすべてインターフェースに問題がある場合は、依然として DCE はこの最も優先順位の低いインターフェースを使用できます。

上記のマシンに次のインターフェースがあるものとします。

インターフェース	アドレス
eno	125.46.78.91
en1	125.46.125.91
tr0	9.25.47.91

以下の例では **RPC\_NETADDRS\_ORDER** 環境変数を使用し、以下のアドレスによりトークンリング・ネットワークと両方のイーサネット・ネットワークを順序付けます。

```
RPC_NETADDRS_ORDER=9.25.47.91:125.46.78.91:125.46.125.91
```

## 例

```
export RPC_NETADDRS_ORDER=125.46.125.91:9.25.47.91:125.46.78.91
```

## RPC\_NETIFS\_ORDER

**目的** PRC 実行時ルーチンが使用する IP インターフェースの順序を定義します。

### 形式

```
export RPC_NETIFS_ORDER=if_0:if_1
```

**説明** この環境変数は、構成されている TCPIP ネットワーク・インターフェースの使用順序を指定します。つまり、ローカル TCPIP インターフェースが RPC 実行時ルーチンにより使用される順序を制御します。デフォルトでは、構成されているすべての TCPIP インターフェースを、必須の順序で使用します。CDS データベースおよびエンドポイント・マップへのサーバーの登録を、インターフェースを順序付けることで、制御できます。この環境変数に組み込まれていないインターフェースは、使用可能なインターフェースのリストの末尾に追加されます。これは、複数のネットワーク・アダプターがあり、一部のネットワーク・インターフェースを使用して DCE トラフィックをターゲットにしたり外したりしなければならないマシンで便利です。たとえば、あるインターフェースでのトラフィックが過密な場合に、そのインターフェースの順序を末尾にすると、DCE は他の使用率の低いインターフェースを使用します。インターフェースを除外してはいないので、他のすべてインターフェースに問題がある場合は、依然として DCE はこの最も優先順位の低いインターフェースを使用できます。

## 例

```
export RPC_NETIFS_ORDER=tr0:en0:en1
```

## RPC\_RESTRICTED\_PORTS

**目的** RPC が使用する TCPIP ポート番号を特定の範囲に制限します。

### 形式

```
export RPC_RESTRICTED_PORTS=1stprotseq[port#-port#]:2ndprotseq[port#-port#]
```

**説明** この環境変数は、RPC が使用する TCPIP ポート番号を特定の範囲に制限します。問題は、DFS などの RPC アプリケーションが、ルーターのフィルターをセキュリティー手段として使用するサイト間で動作しなくなる点です。これらのフィルターは、入力ネットワーク・パケットを特定のポートの特定のアドレスに制限します。RPC はサービスのポート番号を動的に決定するため、この環境では動作しません。この環境変数を使用すると、RPC は指定された範囲のポート番号だけを使用します。そのため、フィルターは最大これらの範囲でだけオープンできます。

RPC を Solaris 上で実行している場合に、

**RPC\_RESTRICTED\_PORTS** と

**RPC\_RESTRICTED\_SERVER\_PORTS** の両方ともあると、

**RPC\_RESTRICTED\_PORTS** は無視されます。

RPC を AIX 上で実行している場合に、  
**RPC\_RESTRICTED\_PORTS** と  
**RPC\_RESTRICTED\_SERVER\_PORTS** の両方ともあると、  
**RPC\_RESTRICTED\_SERVER\_PORTS** は無視されます。

例

```
export RPC_RESTRICTED_PORTS=ncadg_ip_udp[5000-5500]:ncacn_ip_tcp[6000-6500]
export RPC_RESTRICTED_PORTS=ncacn_ip_tcp[5000-5500,5800-6000]
```

## RPC\_RESTRICTED\_SERVER\_PORTS

**目的** DCE が使用する TCPIP ポート番号を特定の範囲に制限します。

**形式**

```
export RPC_RESTRICTED_SERVER_PORTS=1stprotseq[port#-port#]:
2ndprotseq[port#-port#]
```

**説明** この環境変数は、DCE が使用する TCPIP ポート番号を特定の範囲に制限します。これは、DCE サーバー (cdsd、cdsav、secd、および gdad など) で使用できるポートを制限することにより、ファイアウォールをサポートするのに役立ちます。これらのフィルターは、入力ネットワーク・パケットを特定のポートの特定のアドレスに制限します。

RPC を Solaris 上で実行している場合に、  
**RPC\_RESTRICTED\_PORTS** と  
**RPC\_RESTRICTED\_SERVER\_PORTS** があると、  
**RPC\_RESTRICTED\_PORTS** は無視されます。

RPC を AIX 上で実行している場合に、  
**RPC\_RESTRICTED\_PORTS** と  
**RPC\_RESTRICTED\_SERVER\_PORTS** の両方ともあると、  
**RPC\_RESTRICTED\_SERVER\_PORTS** は無視されます。

例

```
export RPC_RESTRICTED_SERVER_PORTS=ncadg_ip_udp[5000-5004]
```

## RPC\_SUPPORTED\_PROTSEQS

**目的** RPC 実行時ルーチンが使用するプロトコル・シーケンスを制限します。

**形式**

```
export RPC_SUPPORTED_PROTSEQS=protseq:protseq
```

**説明** この環境変数は、サポートされるプロトコル・シーケンスのセットを指定されたシーケンスに制限するように RPC 実行時ルーチンに通知する場合に使用します。構文では、希望するプロトコル・シーケンス・ストリングをコロン (セミコロンではない) で区切ってリスト形式で指定します。デフォルト値は、**ncacn\_ip\_tcp** および **ncadg\_ip\_udp** などのように、すべてのプロトコル・シーケンスを使用します。この環境変数を使用する場合には注意が必要です。指定されないプロトコル・シーケンスについてはサポートしなくなるため、サポートしていないプロトコル・シーケンスを介してクライアントがサーバーへの接続を試みると通信障害が発生する可能性があります。

## 例

```
export RPC_SUPPORTED_PROTSEQS=ncadg_ip_udp
```

### RPC\_UNSUPPORTED\_NETADDRS

**目的** 指定された IP インターフェースを RPC 実行時ルーチンが使用しないようにします。

#### 形式

```
export RPC_UNSUPPORTED_NETADDRS=ipaddress:ipaddress
```

**説明** この環境変数は、DCE に使用させたくない TCP/IP ネットワーク・インターフェースが構成されている場合に使用されます。つまり、どのローカル TCPIP インターフェースが RPC 実行時ルーチンにより使用されるかを制御します。デフォルトでは、構成されているすべての TCPIP インターフェースを使用します。その結果、CDS データベースおよびエンドポイント・マップへのサーバーの登録を、TCP/IP アドレスを介して 1 つまたは複数のネットワークをマスクで除去することで、制御できます。

これは、複数のネットワーク・アダプターがあり、一部のネットワークから DCE トラフィックを除外しなければならないマシンで便利です。たとえば、通常の日常のトラフィックのための 1 つの FDDI ネットワーク接続があり、また、X ステーション・トラフィックだけに使用される 2 つのイーサネット・ネットワークにも接続しているサーバー・マシンを考えてみます。DCE サーバーをこのマシン上で開始すると、サーバーは 3 つのアドレスすべてを CDS ネーム・スペースおよび dced エンドポイント・マップに登録します。つまり、このサーバーと通信を希望する FDDI ネットワーク上のすべてのマシンには、イーサネット・ネットワークに対する有効なルーティング・インターフェースが必要です。これは、サーバーへのアドレスについて CDS に照会すると、CDS は FDDI リングにだけ接続されているマシンへのイーサネット・アドレスのいずれかを戻すからです。

上記のマシンに次のインターフェースがあるものとします。

インターフェース	アドレス
en0	125.46.78.91
en1	125.46.125.91
fi0	9.25.47.91

以下の例では **RPC\_UNSUPPORTED\_NETADDRS** 環境変数を使用し、アドレス

```
RPC_UNSUPPORTED_NETADDRS=125.46.78.91:125.46.125.91
```

により両方のイーサネット・ネットワークを除去します。

## 例

```
export RPC_UNSUPPORTED_NETADDRS=129.46.78.9
```

### RPC\_UNSUPPORTED\_NETIFS

**目的** 指定された IP インターフェースを RPC 実行時ルーチンが使用しないようにします。

#### 形式

```
export RPC_UNSUPPORTED_NETIFS=if_0:if_1
```

**説明** この環境変数は、DCE に使用させたくない TCP/IP ネットワーク・インターフェースが構成されている場合に使用されます。つまり、どのローカル TCPIP インターフェースが RPC 実行時ルーチンにより使用されるかを制御します。デフォルトでは、構成されているすべての TCPIP インターフェースを使用します。その結果、CDS データベースおよびエンドポイント・マップへのサーバーの登録を、TCP/IP インターフェースを介して 1 つまたは複数のネットワークをマスクで除去することで、制御できます。

**例**

```
export RPC_UNSUPPORTED_NETIFS=en0:en1
```

---

## セキュリティ

DCE セキュリティー環境変数の設定を、以下のトピックで説明します。

### KRB5CCNAME

**目的** デフォルト認証キャッシュ・ファイルを指定します。

**形式**

```
KRB5CCNAME=FILE:/var/dce/security/creds/dcecred_[XXXXXXXX]
```

**説明** この環境変数は、`dce_login` コマンドを使用するときまたは AIX/DCE セキュリティー統合機能を使用するとき DCE へログインすると設定されます。KRB5CCNAME は、ログイン時に獲得された DCE 認証がキャッシュされているファイルを指します。ファイル名の XXXXXXXX の部分は、ログインするたびにランダムに生成されます。

ログインし KRB5CCNAME が設定されると、実行する他のプログラムはこれらのキャッシュされた DCE 認証を使用できます (それらが有効な限り)。この場合、認証を獲得するために DCE に対し再認証処理を実行する必要はありません。KRB5CCNAME がデフォルト認証キャッシュを参照していると言われているのは、このためです。

KRB5CCNAME の値を明示的に変更することで、デフォルト DCE 認証を変更できます (以前に DCE にログインしていて別の認証ファイルを獲得している場合)。しかし、KRB5CCNAME の値を変更しても、DFS に関する DCE 認証は変更されません。変更されるのは、DCE へ再びログインするときだけです。

DCE 認証に関する詳細な説明は、*IBM DCE for AIX and Solaris* バージョン 3.2: 管理コマンド・リファレンスの `dcecred_*` ファイルの項を参照してください。

**例**

```
KRB5CCNAME=FILE:/var/dce/security/creds/dcecred_34210983
```

### BIND\_PE\_SITE | TRY\_PE\_SITE

**目的** セキュリティー・レプリカの名前を DCE クライアントが探索する方法を制御します。

**形式**

```
BIND_PE_SITE=[0] | [1]  
TRY_PE_SITE=[0] | [1]
```

**説明** DCE クライアントがセキュリティー・レプリカと通信を希望すると、通常は cds ネーム・スペース内のレプリカ名を探索します。しかし、クライアントがレプリカに頻繁に連絡を取る場合は、これらの cds 探索の実行オーバーヘッドが大きくなる可能性があります。

パフォーマンスを向上させるために、**BIND\_PE\_SITE** および **TRY\_PE\_SITE** 環境変数では、`/opt/dcelocal/etc/security/pe_site` ファイルに含まれているセキュリティー・レプリカ名をクライアントが探索できるようにしています。`pe_site` ファイルには、セルに含まれるセキュリティー・レプリカの名前と場所が含まれています。通常、`pe_site` ファイルを使用してセキュリティー・レプリカを探索した方が、`cds` で探索するより短時間で済みます。

**BIND\_PE\_SITE** も **TRY\_PE\_SITE** も設定しないかあるいは 0 に設定すると、クライアントは cds ネーム・スペース内を従来の方法で調べることでセキュリティー・レプリカを突き止めます。

**TRY\_PE\_SITE** が 1 に設定されていると、クライアントは `pe_site` ファイルを使用してセキュリティー・レプリカを突き止めようとします。どのレプリカとも連絡できない場合は、クライアントは次に、`cds` ネーム・スペース内を調べることでレプリカを突き止めようとします。

**BIND\_PE\_SITE** が 1 に設定されていると、クライアントは `pe_site` ファイルだけを使用してセキュリティー・レプリカを突き止めようとします。これが失敗すると、クライアントは `cds` ネーム・スペースを調べません。その代わりに、セキュリティー・レプリカに対する連絡の試みは失敗します。

**TRY\_PE\_SITE** も **BIND\_PE\_SITE** も 1 に設定されていると、**TRY\_PE\_SITE** 動作が優先されます。

`pe_site` ファイルには、セルに含まれるセキュリティー・レプリカの名前と場所が含まれています。このファイルは、DCE クライアントがセルへ最初に構成された時点で作成されます。セキュリティー・レプリカが使用可能になったり使用不能になったりすると、`pe_site` ファイル内のセキュリティー・レプリカに関する情報は `cds` ネーム・スペース内の最新情報と異なる可能性があります。このため、**BIND\_PE\_SITE** または **TRY\_PE\_SITE** は、セキュリティー・レプリカに頻繁に連絡しなければならないプログラムを実行するときだけ設定してください (たとえば、DCE ログインまたはレジストリー・オペレーションを頻繁に行う場合)。

`pe_site` ファイルは、`dced` デーモン (一定の間隔でファイル更新を行う) により、セキュリティー・レプリカの現在情報で更新されます。また、`chpesite` コマンドの実行によっても更新できます。

**例**

```
BIND_PE_SITE=1  
TRY_PE_SITE=0
```





---

## 付録C. DCE セル・ネーム・スペース

この付録では、CDS および DCE セキュリティー・サービスが DCE セル・ネーム・スペース内で使用する名前を説明します。これらのネーム・スペース・エントリは初期 DCE 構成中に作成されます。

以下の表では、CDS クラス・フィールドは **CDS\_Clearinghouse** エントリおよび RPC NSI により内部的に使用されます。ウェルノウン・フィールドは、名前の最後のコンポーネントがアーキテクチャー上で必須名かどうかを示しています。デフォルト ACLS フィールドは、DCE 構成スクリプトを実行することで作成される ACL を示しています。

*hostname*、*lclhostname*、*cellname*、および *creator* エントリは、次のように定義されています。

- *hostname*

これはセル相対ホスト名です。たとえば、**machine1.abc.com** という名前のホストの *hostname* は **machine1** です。サブドメインを持つセルの場合、ディレクトリー構造が可能であることに注意してください。たとえば、ホスト **apollo.mercury.acs.cmu.edu** には、*hostname* **acs/mercury/apollo** を割り当てることができます。

- *lclhostname*

これは単一コンポーネント・ホスト名です。この名前は、常に最小の有効なホスト名のコンポーネントです。以前に示した例の *lclhostname* は **machine1** および **apollo** です。

- *cellname*

これはセルのグローバル名で、特殊文字ストリング **I..J** はありません。たとえば、**seattle.abc.com** または **C=US/O=ABC/OU=Seattle** です。

- *creator*

これはセルを作成したプリンシパルの名前です。

---

## CDS スペース

74ページの図3 から 85ページの図5 は、DCE セル・ネーム・スペースの CDS ネーム・スペースを示したものです。それに続くサブセクションに、各エントリーの説明があります。

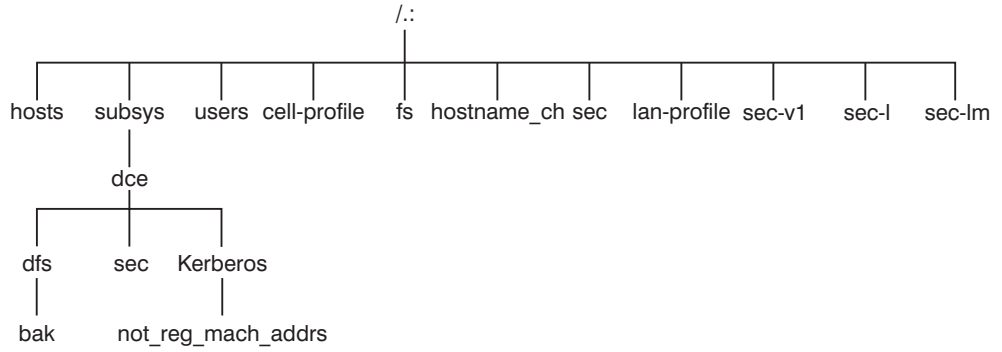


図3. 最上位レベル CDS ディレクトリー

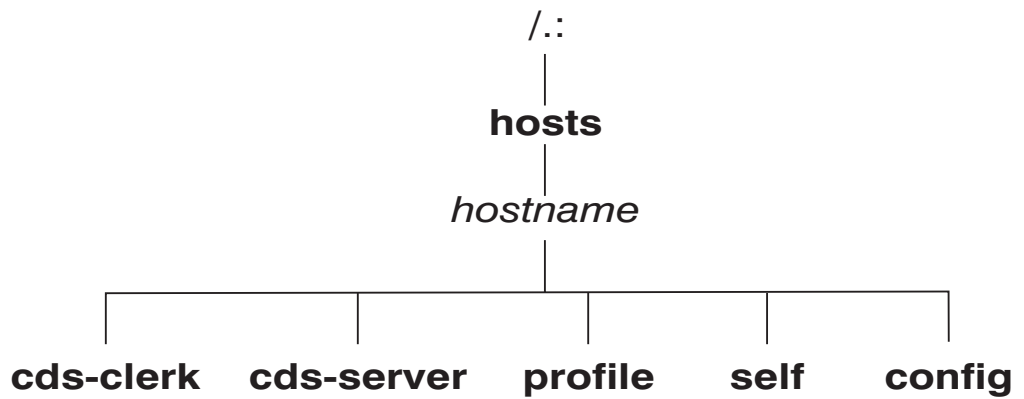


図4. CDS ホスト・ディレクトリー

## 最上位レベル CDS ディレクトリー

以下の表は、最上位 CDS ディレクトリーである /: のネーム・スペース・エントリーを説明しています。

名前	/:/cell-profile
CDS タイプ	オブジェクト
CDS クラス	<b>RPC_Profile</b>
ウェルノウン	はい

名前	<b>./:cell-profile</b>
説明	これは、セルのマスター・デフォルト・プロファイルです。最終的には、すべての他のプロファイルは、このプロファイルにリンクする必要があります。このプロファイルは、セル作成時に作成され、次のエントリーを含む必要があります。 <i>LAN-Services-UUID</i> <i>./:cellname/lan-profile</i> すべてのプロファイル・エントリーと同様、グローバル名しか使用できないことに注意してください。このプロファイルは、特権サーバー、レジストリー・サーバー、および認証サーバーのためのインターフェースを含む必要があります。複数 LAN セルでは、これは DTS グローバル・セット・エントリーが入力されるプロファイルです。
デフォルト ACL オブジェクト ACL	<pre>{unauthenticated r- - t- } {user creator rwdtc} {group subsys/dce/cds-admin rwdtc} {group subsys/dce/cds-server rwdtc} {group subsys/dce/dts-admin rw- t- } {group subsys/dce/dts-servers rw- t- } {group subsys/dce/sec-servers : rw_t-} {any_other r- - t- }</pre>

名前	<b>./:fs</b>
CDS タイプ CDS クラス ウェルノウン 説明	オブジェクト <b>RPC_Group</b> いいえ これは、セル・ネーム・スペース内の DFS ファイル・スペースへのジャンクションです。文字ストリング <i>!</i> は <i>./:fs</i> への CDS ソフト・リンクです。FLDB を備えるすべてのファイル・セット・データベース・マシンの RPC バインディングは、このグループにリストされています。このグループは、次の形式の RPC エントリーで構成されています。 <i>./:cellname/hosts/hostname/self</i> このオブジェクトには、単一のオブジェクト UUID が付加されています。
デフォルト ACL オブジェクト ACL	<pre>{unauthenticated r- - t- } {user creator rwdtc} {group subsys/dce/cds-admin rwdtc} {group subsys/dce/cds-server rwdtc} {group subsys/dce/dfs-fs-servers rwdtc} {group subsys/dce/dfs-admin rwdtc} {any_other r- - t- }</pre>

名前	<b>./:hosts</b>
CDS タイプ ウェルノウン	ディレクトリー いいえ

名前	<b>./:/hosts</b>
説明	ホスト・ディレクトリーはここにカタログされます。
デフォルト ACL オブジェクト ACL	<pre>{unauthenticated r- - t- - - } {user creator rwdtcia} {user hosts/hostname/cds-server rwdtcia} {user hosts/hostname/self rwdtcia} {group subsys/dce/cds-admin rwdtcia} {group subsys/dce/cds-server rwdtcia} {any_other r- - t- - - }</pre>
初期オブジェクト ACL	<pre>{unauthenticated r- - t- - - } {group subsys/dce/cds-admin rwdtc- - } {group subsys/dce/cds-server rwdtc- - } {any_other r- - t- - - }</pre>
初期コンテナ ACL	<pre>{unauthenticated r- - t- - - } {group subsys/dce/cds-admin rwdtcia} {group subsys/dce/cds-server rwdtcia} {any_other r- - t- - - }</pre>

名前	<b>./:/lan-profile</b>
CDS タイプ CDS クラス ウェルノウン 説明	オブジェクト <b>RPC_Profile</b> いいえ これは DTS が使用し、他のサービスも使用する可能性のある、デフォルトの LAN プロファイルです。単一 LAN セルでは、これは DTS ローカル・セット・エントリー用のエントリーを含めるプロファイルです。
デフォルト ACL オブジェクト ACL	<pre>{unauthenticated r- - t- } {user creator rwdtc} {group subsys/dce/cds-admin rwdtc} {group subsys/dce/cds-server rwdtc} {group subsys/dce/dts-admin rwdtc} {group subsys/dce/dts-servers rwdtc} {any_other r- - t- }</pre>

名前	<b>./:/lclhostname_ch</b>
CDS タイプ CDS クラス ウェルノウン 説明	オブジェクト <b>CDS_Clearinghouse</b> いいえ すべてのクリアリングハウスは、セル・ルートにカタログされます。この名前は、構成する最初の CDS サーバーの場合のみ固定です。構成する任意の追加 CDS サーバーには、別の名前を選択できません。
デフォルト ACL	

名前	<code>/./lclhostname_ch</code>
オブジェクト ACL	<pre>{unauthenticated r- - t- } {group subsys/dce/cds-admin rwdtc} {group subsys/dce/cds-server rwdtc} {any_other r- - t- }</pre>

名前	<code>/./sec</code>
CDS タイプ CDS クラス ウェルノウン 説明	<p>オブジェクト <b>RPC_Group</b> いいえ これは、このセルのすべてのセキュリティー・サーバーの RPC グループです。エントリー <code>/./lcellname/subsys/dce/sec/master</code> および (たとえば) <code>/./lcellname/subsys/dce/sec/rep_1</code> が含まれます。これは、セキュリティー・ネーム・スペースへのジャンクションです。</p>
デフォルト ACL オブジェクト ACL	<pre>{unauthenticated r- - t- } {user creator rwdtc} {user dce-rgy rwdtc} {user hosts/rep_1_hostname/self rwdtc} {group subsys/dce/cds-admin rwdtc} {group subsys/dce/cds-server rwdtc} {group subsys/dce/sec-admin rwdtc} {group subsys/dce/sec-servers:rwdtc} {any_other r- - t- }</pre>

名前	<code>/./subsys</code>
CDS タイプ ウェルノウン 説明	<p>ディレクトリー いいえ このディレクトリーは、このセルの中の別のサブシステムのためのディレクトリーを含んでいます。 <b>dce</b> サブディレクトリーが含まれています。 DCE ヘサブシステムを追加する会社では商標をディレクトリー名として使用することで、 <b>subsys</b> の下に固有なディレクトリーを作成する規則に準拠してください (<code>/./subsys/trademark</code>)。これらのディレクトリーは、サービスについての、場所に依存しない情報を格納するために使用されます。セル全体のサーバー・エントリー、グループ、およびプロファイルは、 <b>subsys</b> の下のディレクトリーに格納してください。</p>
デフォルト ACL オブジェクト ACL	<pre>{unauthenticated r- - t- - - } {user creator rwdtcia} {user hosts/hostname rwdtcia} {group subsys/dce/cds-admin rwdtcia} {group subsys/dce/cds-server rwdtcia} {any_other r- - t- - - }</pre>

名前	<i>./:/subsys</i>
初期オブジェクト ACL	{unauthenticated r- - t- - - } {group subsys/dce/cds-admin rwdtc- - } {group subsys/dce/cds-server rwdtc- - } {any_other r- - t- - - }
初期コンテナ ACL	{unauthenticated r- - t- - - } {group subsys/dce/cds-admin rwdtcia} {group subsys/dce/cds-server rwdtcia} {any_other r- - t- - - }

## CDS ホスト・ディレクトリー

以下の表は、CDS **hosts** ディレクトリーである *./:/hosts* のネーム・スペース・エントリーを説明しています。

名前	<i>./:/hosts/hostname</i>
CDS タイプ ウェルノウン 説明	ディレクトリー いいえ 各ホストは、このホストに関連する RPC サーバー・エントリー、グループ、およびプロファイルを保管するディレクトリーを持っています。これは単に CDS ディレクトリーです。ディレクトリー・オブジェクト自身にはバインディングはありません。エントリーはディレクトリーの下にあります。
デフォルト ACL オブジェクト ACL	{unauthenticated r- - t- - - } {user creator rwdtcia} {user hosts/hostname/cds-server rwdtcia} {user hosts/hostname/self rwdtcia} {group subsys/dce/cds-admin rwdtcia} {group subsys/dce/cds-server rwdtcia} {any_other r- - t- - - }
初期オブジェクト ACL	{unauthenticated r- - t- - - } {group subsys/dce/cds-admin rwdtc- - } {group subsys/dce/cds-server rwdtc- - } {any_other r- - t- - - }
初期コンテナ ACL	{unauthenticated r- - t- - - } {group subsys/dce/cds-admin rwdtcia} {group subsys/dce/cds-server rwdtcia} {any_other r- - t- - - }

名前	<i>./:/hosts/hostname/cds-clerk</i>
CDS タイプ CDS クラス ウェルノウン 説明	オブジェクト <b>RPC_Entry</b> いいえ このエントリーは、CDS クラークのためのバインディングを含んでいます。
デフォルト ACL	

名前	<code>./:/hosts/hostname/cds-clerk</code>
オブジェクト ACL	<pre>{unauthenticated r- - t- } {user creator rwdtc} {user hosts/hostname/self rw- t- } {group subsys/dce/cds-admin rwdtc} {group subsys/dce/cds-server rwdtc} {any_other r- - t- }</pre>

名前	<code>./:/hosts/hostname/cds-server</code>
CDS タイプ CDS クラス ウェルノウン 説明	<p>オブジェクト <b>RPC_Entry</b> いいえ このエントリーは、CDS サーバーのためのバインディングを含んでいます。</p>
デフォルト ACL オブジェクト ACL	<pre>{unauthenticated r- - t- } {user creator rwdtc} {user hosts/hostname/self rw- t- } {group subsys/dce/cds-admin rwdtc} {group subsys/dce/cds-server rwdtc} {any_other r- - t- }</pre>

名前	<code>./:/hosts/hostname/config</code>
CDS タイプ CDS クラス ウェルノウン 説明	<p>オブジェクト <b>RPC_Entry</b> はい これは特定ホストの <b>dced</b> のサーバー・エントリーです。その <b>dced</b> の命名ツリーの最上位でもあります。プログラムは、<code>dce_cf_dced_entry_from_host( )</code> コールを使用することでこの名前を入手します。</p>
デフォルト ACL オブジェクト ACL	<pre>{unauthenticated r- - t- - - } {user hosts/hostname/self rwdtc- - } {group subsys/dce/cds-admin rwdtc- - } {group subsys/dce/cds-server rwdtc- - } {any_other r- - t- - - }</pre>

名前	<code>./:/hosts/hostname/profile</code>
CDS タイプ CDS クラス ウェルノウン 説明	<p>オブジェクト <b>RPC_Entry</b> いいえ これはホスト <code>hostname</code> のデフォルト・プロファイルです。この中には、<code>./:/cell-profile</code> を指す (間接的な場合もある) デフォルト値が含まれています。プログラムは <code>dce_cf_profile_entry_from_host( )</code> コールを使用することでこの名前を入手します。</p>
デフォルト ACL	

名前	<code>./:/hosts/hostname/profile</code>
オブジェクト ACL	<pre>{unauthenticated r- - t- } {user creator rwdtc} {user hosts/hostname/self rw- t- } {group subsys/dce/cds-admin rwdtc} {group subsys/dce/cds-server rwdtc} {any_other r- - t- }</pre>

名前	<code>./:/hosts/hostname/self</code>
CDS タイプ CDS クラス ウェルノウン 説明	<p>オブジェクト <b>RPC_Entry</b> はい このエントリーには、ホスト <i>hostname</i> 上の <b>dced</b> デーモンへのバインディングが含まれています。 <code>dce_cf_binding_entry_from_host( )</code> コールは、ホスト名が渡されたときはこのエントリーの名前またはホスト名が指定されなかったときは現行ホストのいずれかを戻すことができます。</p>
デフォルト ACL オブジェクト ACL	<pre>{unauthenticated r- - t- } {user creator rwdtc} {user hosts/hostname/self rwrtdtc} {group subsys/dce/cds-admin rwdtc} {group subsys/dce/cds-server rwdtc} {any_other r- - t- }</pre>

## ホスト・デーモン・ディレクトリー

以下の表は、ホスト・デーモン・ディレクトリーである `./:/hosts/hostname/config` の **dced** ネーム・スペース・エントリーを説明しています。これらはすべて、構成処理の一部として **dced** により作成されます。

名前	<code>./:/hosts/hostname/config</code>
<b>dced</b> タイプ ウェルノウン 説明	<p><b>dced</b> オブジェクト はい <b>dced</b> サーバー自身</p>
デフォルト ACL オブジェクト ACL	<pre>{user hosts/hostname/self crws}</pre>

名前	<code>./:/hosts/hostname/config/hostdata</code>
<b>dced</b> タイプ ウェルノウン 説明	<p><b>dced</b> コンテナ はい 特定ホストの <b>hostdata</b> オブジェクトのコンテナ</p>
デフォルト ACL オブジェクト ACL 初期オブジェクト ACL	<pre>{user hosts/hostname/self cril} {user hosts/hostname/self cdprw}</pre>



名前	<code>./:/hosts/hostname/config/keytab</code>
<b>dced</b> タイプ ウェルノウン 説明 デフォルト ACL オブジェクト ACL 初期オブジェクト ACL	<b>dced</b> コンテナー はい 特定ホストの <b>keytab</b> オブジェクトのコンテナー  {user hosts/hostname/self criI} {user hosts/hostname/self acdepr}

名前	<code>./:/hosts/hostname/config/secval</code>
<b>dced</b> タイプ ウェルノウン 説明 デフォルト ACL オブジェクト ACL	<b>dced</b> オブジェクト はい <b>secval</b> サービスの名前  {user hosts/hostname/self csux}

名前	<code>./:/hosts/hostname/config/srvrconf</code>
<b>dced</b> タイプ ウェルノウン 説明 デフォルト ACL オブジェクト ACL 初期オブジェクト ACL	<b>dced</b> コンテナー はい <b>dced</b> に登録された構成済みサーバーのコンテナー  {user hosts/hostname/self criI} {user hosts/hostname/self cdfrx}

名前	<code>./:/hosts/hostname/config/srvexec</code>
<b>dced</b> タイプ ウェルノウン 説明 デフォルト ACL オブジェクト ACL 初期オブジェクト ACL	<b>dced</b> コンテナー はい <b>dced</b> に登録された実行サーバーのコンテナー  {user hosts/hostname/self criI} {user hosts/hostname/self crws}

名前	<code>./:/hosts/hostname/config/xattrschema</code>
<b>dced</b> タイプ ウェルノウン 説明 デフォルト ACL オブジェクト ACL 初期オブジェクト ACL	<b>dced</b> コンテナー はい 拡張属性スキーマ定義のコンテナー  {user hosts/hostname/self criI} {user hosts/hostname/self crwd}

## CDS subsys ディレクトリー

以下の表は、CDS **subsys** ディレクトリーである **./subsys** のネーム・スペース・エントリーを説明しています。

名前	<b>./subsys/dce</b>
CDS タイプ ウェルノウン 説明	ディレクトリー いいえ このディレクトリーは DCE 特有の名前を含んでいません。
デフォルト ACL オブジェクト ACL	<pre>{unauthenticated r- - t- - - } {user creator rwdtcia} {user hosts/hostname/cds-server rwdtcia} {group subsys/dce/cds-admin rwdtcia} {group subsys/dce/cds-server rwdtcia} {any_other r- - t- - - }</pre>
初期オブジェクト ACL	<pre>{unauthenticated r- - t- - - } {group subsys/dce/cds-admin rwdtc- - } {group subsys/dce/cds-server rwdtc- - } {any_other r- - t- - - }</pre>
初期コンテナ ACL	<pre>{unauthenticated r- - t- - - } {group subsys/dce/cds-admin rwdtcia} {group subsys/dce/cds-server rwdtcia} {any_other r- - t- - - }</pre>

名前	<b>./subsys/dce/dfs</b>
CDS タイプ ウェルノウン 説明	ディレクトリー いいえ このディレクトリーには DFS 固有名すべてが含まれています。
デフォルト ACL オブジェクト ACL	<pre>{unauthenticated r- - t- - - } {user creator rwdtcia} {user hosts/hostname/cds-server rwdtcia} {group subsys/dce/cds-admin rwdtcia} {group subsys/dce/cds-server rwdtcia} {group subsys/dce/dfs-admin rwdtcia} {any_other r- - t- - - }</pre>
初期オブジェクト ACL	<pre>{unauthenticated r- - t- - - } {group subsys/dce/cds-admin rwdtc- - } {group subsys/dce/cds-server rwdtc- - } {group subsys/dce/dfs-admin rwdtc- - } {any_other r- - t- - - }</pre>
初期コンテナ ACL	<pre>{unauthenticated r- - t- - - } {group subsys/dce/cds-admin rwdtcia} {group subsys/dce/cds-server rwdtcia} {group subsys/dce/dfs-admin rwdtcia} {any_other r- - t- - - }</pre>

名前	<b>./subsys/dce/dfs/bak</b>
CDS タイプ	オブジェクト
CDS クラス	<b>RPC_Entry</b>

名前	<b><i>././subsys/dce/dfs/bak</i></b>
ウェルノウン 説明	いいえ バックアップ・データベースを保管している、すべてのバックアップ・データベース・マシンの RPC バインディングは、このエントリー内にリストされています。このエントリーは、メンバーが <b><i>././Jcellname/hosts/hostname/self</i></b> 形式の RPC エントリーであるという点で、 <b><i>././fs</i></b> グループと同じです。さらに、このグループは単一オブジェクト UUID を付加されている必要があります。
デフォルト ACL オブジェクト ACL	<pre>{unauthenticated r- - t- } {user creator rwdtc} {user hosts/hostname/cds-server rwdtc} {group subsys/dce/cds-admin rwdtc} {group subsys/dce/cds-server rwdtc} {any_other r- - t- }</pre>

名前	<b><i>././subsys/dce/sec</i></b>
CDS タイプ ウェルノウン 説明	ディレクトリー いいえ このディレクトリーには、セキュリティー固有名が含まれています。
デフォルト ACL オブジェクト ACL	<pre>{unauthenticated r- - t- - - } {user creator rwdtcia} {user hosts/hostname/cds-server rwdtcia} {user dce-rgy rwdtci- } {user hosts/rep_1_hostname/self rwdtia} {group subsys/dce/cds-admin rwdtcia} {group subsys/dce/cds-server rwdtcia} {group subsys/dce/sec-admin rwdtcia} {group subsys/dce/sec-servers:rwdtcia} {any_other r- - t- - - }</pre>
初期オブジェクト ACL	<pre>{unauthenticated r- - t- - - } {user dce-rgy rwdt- - - } {user hosts/rep_1_hostname/self rwdtc} {group subsys/dce/cds-admin rwdtc- - } {group subsys/dce/cds-server rwdtc- - } {group subsys/dce/sec-admin rwdtc- - } {group subsys/dce/sec-servers:rwdtcia} {any_other r- - t- - - }</pre>
初期コンテナ ACL	<pre>{unauthenticated r- - t- - - } {unauthenticated r- - t- - - } {user hosts/rep_1_hostname/self rwdtcia} {group subsys/dce/cds-admin rwdtcia} {group subsys/dce/cds-server rwdtcia} {group subsys/dce/sec-admin rwdtcia} {group subsys/dce/sec-servers:rwdtcia} {any_other r- - t- - - }</pre>

名前	<b><i>././subsys/dce/sec/sec_svr_name</i></b>
CDS タイプ	オブジェクト

名前	<i>./:/subsys/dce/sec/sec_svr_name</i>
CDS クラス ウェルノウン 説明  デフォルト ACL オブジェクト ACL	<b>RPC_Entry</b> いいえ これは、このセルのマスター・セキュリティー・サーバーのサーバー・エンタリーです。レジストリー・サーバー、特権サーバー、および認証サーバーのためのバインディングは、レジストリー・サーバーにより、このエンタリーにエクスポートされます。  <pre>{unauthenticated r- - t- } {user dce-rgy rwdt- } {user creator rwdtc} {group subsys/dce/cds-admin rwdtc} {group subsys/dce/cds-server rwdtc} {group:subsys/dce/sec-servers:rwdt-} {group subsys/dce/sec-admin rwdtc} {any_other r- - t- }</pre>

名前	<i>./:/subsys/dce/sec/sec_svr_name</i>
CDS タイプ CDS クラス ウェルノウン 説明  デフォルト ACL オブジェクト ACL	オブジェクト <b>RPC_Entry</b> いいえ これは、このセルのスレーブ・セキュリティー・サーバーのためのサーバー・エンタリーです。レジストリー・サーバー、特権サーバー、および認証サーバーのためのバインディングは、レジストリー・サーバーにより、このエンタリーにエクスポートされます。  <pre>{unauthenticated r- - t- } {user dce-rgy rwdt-} {user creator rwdtc} {user hosts/rep_1_hostname/self rwdtc} {group subsys/dce/cds-admin rwdtc} {group subsys/dce/cds-server rwdtc} {group:subsys/dce/sec-servers:rwdt-} {group subsys/dce/sec-admin rwdtc} {any_other r- - t- }</pre>

## セキュリティー・スペース

85ページの図5 から 86ページの図7 は、DCE セル・ネーム・スペース内のセキュリティー・ネーム・スペースを示したものです。それに続くサブセクションに、各エンタリーの説明があります。セキュリティー・ネーム・スペースを構成するサブディレクトリーは、**principal**、**group**、**org**、**policy**、**replist**、および **xattrschema** です。

これらの任意のネーム・スペース・エンタリー上の ACL を操作するには、セキュリティー・ジャンクションの名前を含める必要があります。たとえば、DCE 制御プログラムの (**dcecp**) **acl** コマンドを使用するとき、グループ名 **acct-admin** はデータベース・オブジェクト名である **./:/sec/group/acct-admin** として参照されます。

しかし、**dcecp principal**、**group**、または **organization** コマンドを使用するとき、名前の一部として組み込まれている **./:/sec** および **principal**、**group**、または **organization** を使用しないプリンシパル、グループ、または組織名にオペレーションを実行します。たとえば、グループ **acct-admin** の属性を表示するためには、このパス名がないグループ名 **acct-admin** を指定している **group show** コマンドを出します。

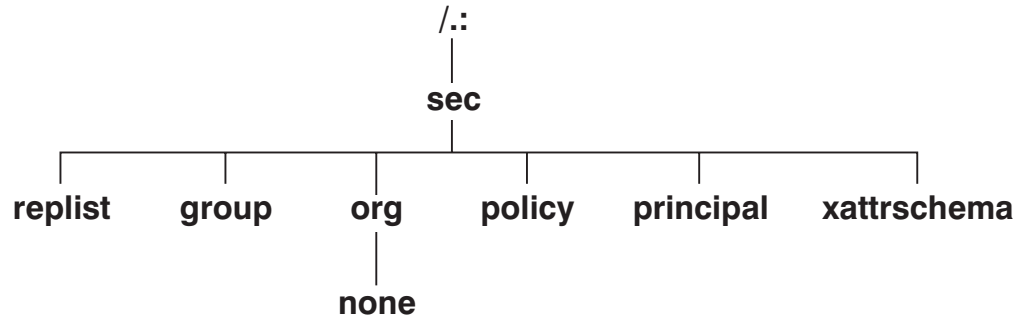


図5. 最上位セキュリティー・ディレクトリー

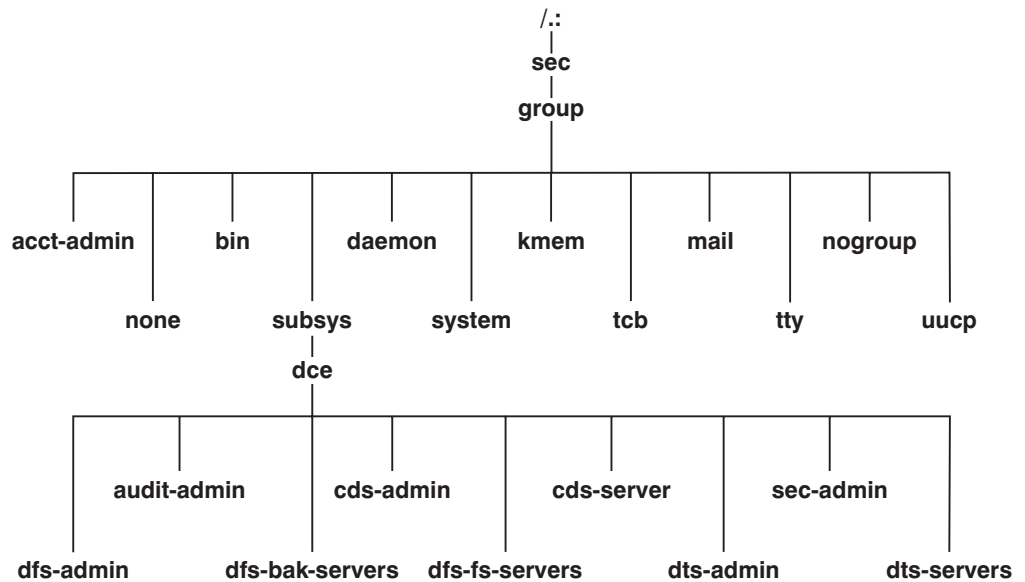


図6. *sec/group* ディレクトリー

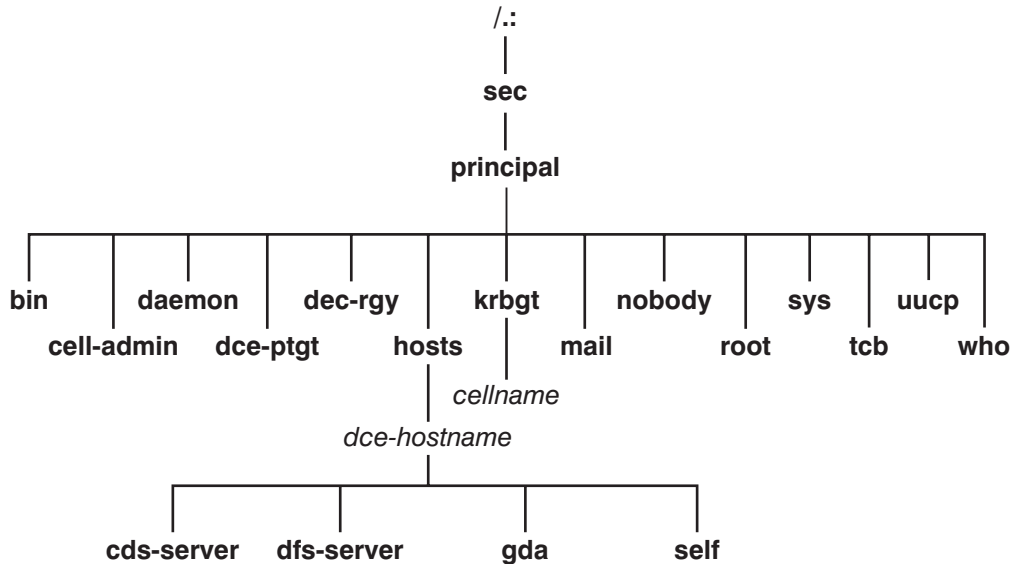


図7. *sec/principal* ディレクトリー

以下のサブセクションでは、初期セキュリティー・ネーム・スペースのエントリーを説明します。含まれているのは、割り当てられる、お勧めする UNIX ユーザー ID (UNIX UID) またはグループ ID (UNIX GID) です。ベンダーは、可能ならばこれらの値を使用する必要があります。パスワードおよびグループ変更ファイルは、必要な場合、パスワードおよびグループを正しいローカル値で置き換えることができます。一部のエントリーには 100 から始まり、次の使用可能な ID が割り当てられます。したがって、これらはセルごとに異なる可能性があります。これらは、“Generated” として示されています。

## 最上位セキュリティー・ディレクトリー

以下の表は、最上位セキュリティー・ディレクトリーである */:/sec* のネーム・スペース・エントリーを説明しています。

名前	<i>/:/sec/group</i>
ウェルノウン	はい。この名前は体系的には定義されず、実際の導入側により定義されます。
説明	これは、すべてのグループを保持するセキュリティー・ディレクトリーです。
デフォルト ACL オブジェクト ACL	<pre>{unauthenticated r- - - - - } {user creator rcidDn} {group acct-admin rcidDn} {other_obj r- - - - - } {any_other r- - - - - }</pre>
初期オブジェクト ACL	<pre>{unauthenticated r- t- - - - - } {user creator rctDnfmM} {group_obj r- t- - - - - } {group acct-admin rctDnfmM} {other_obj r- t- - - - - } {any_other r- t- - - - - }</pre>

名前	<b>./sec/group</b>
初期コンテナ ACL	<pre>{unauthenticated r- - - - } {user creator rcidDn} {group acct-admin rcidDn} {other_obj r- - - - } {any_other r- - - - }</pre>

名前	<b>./sec/org</b>
ウェルノウン	はい。この名前は体系的には定義されず、実際の導入側により定義されます。
説明	これは、すべての組織を保持するセキュリティー・ディレクトリーです。
デフォルト ACL オブジェクト ACL	<pre>{unauthenticated r- - - - } {user creator rcidDn} {group acct-admin rcidDn} {other_obj r- - - - } {any_other r- - - - }</pre>
初期オブジェクト ACL	<pre>{unauthenticated r- t- - - - } {user creator rctDnfmM} {group acct-admin rctDnfmM} {other_obj r- t- - - - } {any_other r- t- - - - }</pre>
初期コンテナ ACL	<pre>{unauthenticated r- - - - } {user creator rcidDn} {group acct-admin rcidDn} {other_obj r- - - - } {any_other r- - - - }</pre>

名前	<b>./sec/org/none</b>
ウェルノウン	はい
説明	これは、デフォルトの組織です。
デフォルト ACL オブジェクト ACL	<pre>{unauthenticated r- t- - - - } {user creator rctDnfmM} {group acct-admin rctDnfmM} {other_obj r- t- - - - } {any_other r- t- - - - }</pre>

名前	<b>./sec/policy</b>
ウェルノウン	はい。この名前は体系的には定義されず、実際の導入側により定義されます。
説明	このエントリーは、セル全体にわたるセキュリティー・ポリシーを設定する能力を提供します。
デフォルト ACL オブジェクト ACL	<pre>{unauthenticated r- - - - } {user creator rcmas} {group acct-admin rcma-} {other_obj r- - - - } {any_other r- - - - }</pre>

名前	<b>././sec/policy</b>

名前	<b>././sec/principal</b>
ウェルノウン	はい。この名前は体系的には定義されませんが、DCE 1.1 では変更できません。
説明	これは、すべてのプリンシパルを保持するセキュリティー・ディレクトリーです。
デフォルト ACL オブジェクト ACL	<pre>{unauthenticated r- - - - - } {user creator rcidDn} {group acct-admin rcidDn} {other_obj r- - - - - } {any_other_obj r- - - - - }</pre>
初期オブジェクト ACL	<pre>{unauthenticated r- - - - - - - } {user_obj r- - - f- - ug} {user creator rcDnfmaug} {group acct-admin rcDnfmaug} {other_obj r- - - - - - - g} {any_other r- - - - - - - }</pre>
初期コンテナ ACL	<pre>{unauthenticated r- - - - - } {user creator rcidDn} {group acct-admin rcidDn} {other_obj r- - - - - } {any_other r- - - - - }</pre>

名前	<b>././sec/replist</b>
ウェルノウン	はい。この名前は体系的には定義されませんが、DCE 1.1 では変更できません。
説明	このエントリーは、異なるセキュリティー・レプリカについての情報を保持します。
デフォルト ACL オブジェクト ACL	<pre>{user creator cidmA- } {user hosts/hostname/self - i- m- I} {group:subsys/dce/sec-servers: -i-m-I} {group acct-admin cidmA- }</pre>

名前	<b>././sec/xattrschema</b>
ウェルノウン	はい。この名前は体系的には定義されませんが、DCE 1.1 では変更できません。
説明	これは、拡張レジストリー属性スキーマ・エントリーのためのコンテナです。このディレクトリー内のエントリーは、他のレジストリー・オブジェクト (たとえば、プリンシパル) に付加されている場合がある ERA の形式を定義します。
デフォルト ACL オブジェクト ACL	<pre>{unauthenticated r- - - - } {user creator rcidm} {other_obj r- - - - } {any_other r- - - - }</pre>



名前	<code>./sec/xattrschema</code>

## sec/group ディレクトリー

以下の表は、セキュリティー **sec/group** ディレクトリーである `./sec/group` のネーム・スペース・エントリーを説明しています。

名前	<code>./sec/group/acct-admin</code>
ウェルノウン 説明	いいえ これは、アカウントを作成できるプリンシパルの唯一のグループです。
デフォルト ACL オブジェクト ACL	<pre>{unauthenticated r- t- - - - - } {user creator rctDnfmM} {group_obj r- t- - - - - } {other_obj r- t- - - - - } {any_other r- t- - - - - }</pre>
UNIX GID	Generated

名前	<code>./sec/group/bin</code>
ウェルノウン 説明	いいえ これは、システム・バイナリーのためのグループです。
デフォルト ACL オブジェクト ACL	<pre>{unauthenticated r- t- - - - - } {user creator rctDnfmM} {group_obj r- t- - - - - } {group acct-admin rctDnfmM} {other_obj r- t- - - - - } {any_other r- t- - - - - }</pre>
UNIX GID	3

名前	<code>./sec/group/daemon</code>
ウェルノウン 説明	いいえ これは、デーモンのためのグループです。
デフォルト ACL オブジェクト ACL	<pre>{unauthenticated r- t- - - - - } {user creator rctDnfmM} {group_obj r- t- - - - - } {group acct-admin rctDnfmM} {other_obj r- t- - - - - } {any_other r- t- - - - - }</pre>
UNIX GID	1

名前	<code>./sec/group/kmem</code>
ウェルノウン	いいえ

名前	<b>./sec/group/kmem</b>
説明	これは、カーネル・メモリーに読み取りアクセスを持つグループです。
デフォルト ACL オブジェクト ACL	<pre>{unauthenticated r- t- - - - - } {user creator rctDnfmM} {group_obj r- t- - - - - } {group acct-admin rctDnfmM} {other_obj r- t- - - - - } {any_other r- t- - - - - }</pre>
UNIX GID	4

名前	<b>./sec/group/mail</b>
ウェルノウン 説明	いいえ これは、メール・サブシステムのためのグループです。
デフォルト ACL オブジェクト ACL	<pre>{unauthenticated r- t- - - - - } {user creator rctDnfmM} {group_obj r- t- - - - - } {group acct-admin rctDnfmM} {other_obj r- t- - - - - } {any_other r- t- - - - - }</pre>
UNIX GID	6

名前	<b>./sec/group/nogroup</b>
ウェルノウン 説明	はい これは、NFS アクセスのデフォルト・グループです。ユーザー ID <b>nobody</b> と共に使用されます。
デフォルト ACL オブジェクト ACL	<pre>{unauthenticated r- t- - - - - } {user creator rctDnfmM} {group_obj r- t- - - - - } {other_obj r- t- - - - - } {any_other r- t- - - - - }</pre>
UNIX GID	-2

名前	<b>./sec/group/none</b>
ウェルノウン 説明	はい このメンバーはグループには属しません。デフォルト・グループです。
デフォルト ACL オブジェクト ACL	<pre>{unauthenticated r- t- - - - - } {user creator rctDnfmM} {group_obj r- t- - - - - } {group acct-admin rctDnfmM} {other_obj r- t- - - - - } {any_other r- t- - - - - }</pre>
UNIX GID	12

名前	<b>./sec/group/none</b>

名前	<b>./sec/group/subsys</b>
ウェルノウン 説明	はい このディレクトリーには <b>dce</b> が含まれます (CDS ネーム・スペース内の <b>./subsys</b> を参照)。
デフォルト ACL オブジェクト ACL	<pre>{unauthenticated r- - - - - } {user creator rcidDn} {group acct-admin rcidDn} {other_obj r- - - - - } {any_other r- - - - - }</pre>
初期オブジェクト ACL	<pre>{unauthenticated r- t- - - - - } {user creator rctDnfmM} {group_obj r- t- - - - - } {group acct-admin rctDnfmM} {other_obj r- t- - - - - } {any_other r- t- - - - - }</pre>
初期コンテナ ACL	<pre>{unauthenticated r- - - - - } {user creator rcidDn} {group acct-admin rcidDn} {other_obj r- - - - - } {any_other r- - - - - }</pre>

名前	<b>./sec/group/system</b>
ウェルノウン 説明	いいえ これは、システム・アカウントのためのグループです。
デフォルト ACL オブジェクト ACL	<pre>{unauthenticated r- t- - - - - } {user creator rctDnfmM} {group_obj r- t- - - - - } {group acct-admin rctDnfmM} {other_obj r- t- - - - - } {any_other r- t- - - - - }</pre>
UNIX GID	0

名前	<b>./sec/group/tcb</b>
ウェルノウン 説明	いいえ これは、OSF/1 C2/B1 保護システム上のセキュリティー・ポリシー・デーモンにより使用されるグループです。
デフォルト ACL オブジェクト ACL	<pre>{unauthenticated r-t-----} {user creator rctDnfmM} {group_obj r-t-----} {group acct-admin rctDnfmM} {other_obj r-t-----} {any_other r-t-----}</pre>
UNIX GID	18

名前	<b>./sec/group/tcb</b>

名前	<b>./sec/group/tty</b>
ウェルノウン 説明	いいえ これは、端末に書き込みアクセスを持つグループです。
デフォルト ACL オブジェクト ACL	<pre>{unauthenticated r- t- - - - - } {user creator rctDnfmM} {group_obj r- t- - - - - } {group acct-admin rctDnfmM} {other_obj r- t- - - - - } {any_other r- t- - - - - }</pre>
UNIX GID	7

名前	<b>./sec/group/uucp</b>
ウェルノウン 説明	いいえ これは、UUCP サブシステムのためのグループです。
デフォルト ACL オブジェクト ACL	<pre>{unauthenticated r- t- - - - - } {user creator rctDnfmM} {group_obj r- t- - - - - } {group acct-admin rctDnfmM} {other_obj r- t- - - - - } {any_other r- t- - - - - }</pre>
UNIX GID	2

## sec/group/subsys ディレクトリー

以下の表は、セキュリティー **sec/group/subsys** ディレクトリーである **./sec/group/subsys** のネーム・スペース・エントリーを説明しています。

名前	<b>./sec/group/subsys/dce</b>
ウェルノウン 説明	はい ディレクトリーは、DCE により使用されるグループを含んでいます。
デフォルト ACL オブジェクト ACL	<pre>{unauthenticated r- - - - - } {user creator rcidDn} {group acct-admin rcidDn} {other_obj r- - - - - } {any_other r- - - - - }</pre>
初期オブジェクト ACL	<pre>{unauthenticated r- t- - - - - } {user creator rctDnfmM} {group_obj r- t- - - - - } {group acct-admin rctDnfmM} {other_obj r- t- - - - - } {any_other r- t- - - - - }</pre>

名前	<b>././sec/group/subsys/dce</b>
初期コンテナ ACL	<pre>{unauthenticated r- - - - - } {user creator rcidDn} {group acct-admin rcidDn} {other_obj r- - - - - } {any_other r- - - - - }</pre>

名前	<b>././sec/group/subsys/dce/cds-admin</b>
ウェルノウン 説明	<p>いいえ これは、管理オブジェクトのためのデフォルト ACL 上にある管理グループです。クリアリングハウスは、その ACL 上にすべての権限を備えて、このグループを持っています。セルの最初のユーザーは、作成直後に、このグループに追加する必要があります。</p>
デフォルト ACL オブジェクト ACL	<pre>{unauthenticated r- t- - - - - } {user creator rctDnfmM} {group_obj r- t- - - - - } {group acct-admin rctDnfmM} {other_obj r- t- - - - - } {any_other r- t- - - - - }</pre>
UNIX GID	Generated

名前	<b>././sec/group/subsys/dce/cds-server</b>
ウェルノウン 説明	<p>はい これは、ローカル・セルのためのすべての CDS サーバーのグループです。新しいサーバーがセルに追加されるたびに、それをこのグループに追加する必要があります。CDS サーバー認証は、このグループ内にサーバーのメンバーシップを検査することから成り立ちます。</p>
デフォルト ACL オブジェクト ACL	<pre>{unauthenticated r- t- - - - - } {user creator rctDnfmM} {group_obj r- t- - - - - } {group acct-admin rctDnfmM} {group subsys/dce/cds-admin rctDnfmM} {group subsys/dce/cds-server rctDnfmM} {other_obj r- t- - - - - } {any_other r- t- - - - - }</pre>
UNIX GID	Generated

名前	<b>././sec/group/subsys/dce/dfs-admin</b>
ウェルノウン 説明	<p>いいえ これは、DFS 管理者のグループです。このグループのメンバーは、セル内の DFS 構成を変更するためのすべての許可を持っています。</p>
デフォルト ACL	

名前	<b>./sec/group/subsys/dce/dfs-admin</b>
オブジェクト ACL	<pre>{unauthenticated r- t- - - - - } {user creator rctDnfmM} {group_obj r- t- - - - - } {group acct-admin rctDnfmM} {other_obj r- t- - - - - } {any_other r- t- - - - - }</pre>
UNIX GID	Generated

名前	<b>./sec/group/subsys/dce/dfs-bak-servers</b>
ウェルノウン 説明	<p>はい</p> <p>これは、すべての DFS バックアップ・データベース・サーバーが属しているセキュリティ・グループです。CDS グループ <b>./subsys/dce/fs</b> のサーバー・エントリーは、このセキュリティ・グループに属するかどうかを判別することで、バックアップ・データベース・サーバーとして動作するための許可について検査されます。</p>
デフォルト ACL オブジェクト ACL	<pre>{unauthenticated r- t- - - - - } {user creator rctDnfmM} {group_obj r- t- - - - - } {group acct-admin rctDnfmM} {group:subyss/dce/dfs-admin:rctDfmM} {other_obj r- t- - - - - } {any_other r- t- - - - - }</pre>
UNIX GID	Generated

名前	<b>./sec/group/subsys/dce/dfs-fs-servers</b>
ウェルノウン 説明	<p>はい</p> <p>すべてのファイル・セット・データベース・マシンの DFS サーバー・プリンシパルの省略形が、このグループにリストされています。グループに格納されているマシンの DFS サーバー・プリンシパルの省略形は、<b>hosts/hostname/dfs-server</b> の形式です。CDS グループ <b>./fs</b> から取り出されたサーバー・エントリーは、このグループに属しているかどうかを判別することで、ファイル・セット場所サーバーとして動作するための許可について検査されます。</p>
デフォルト ACL オブジェクト ACL	<pre>{unauthenticated r- t- - - - - } {user creator rctDnfmM} {group_obj r- t- - - - - } {group acct-admin rctDnfmM} {group subsys/dce/dfs-admin rctDnfmM} {other_obj r- t- - - - - } {any_other r- t- - - - - }</pre>
UNIX GID	Generated

名前	<b>./:/sec/group/subsys/dce/dts-admin</b>
ウェルノウン 説明	いいえ これは、DTS 管理者のグループです。このグループのメンバーは、サーバー等々を追加することにより、DTS を管理するためのすべての許可を持っています。
デフォルト ACL オブジェクト ACL	<pre>{unauthenticated r- t- - - - - } {user creator rctDnfmM} {group_obj r- t- - - - - } {group acct-admin rctDnfmM} {other_obj r- t- - - - - } {any_other r- t- - - - - }</pre>
UNIX GID	Generated

名前	<b>./:/sec/group/subsys/dce/dts-servers</b>
ウェルノウン 説明	はい これは、DTS サーバーのグループです。
デフォルト ACL オブジェクト ACL	<pre>{unauthenticated r- t- - - - - } {user creator rctDnfmM} {group_obj r- t- - - - - } {group acct-admin rctDnfmM} {group subsys/dce/dts-admin rctDnfmM} {other_obj r- t- - - - - } {any_other r- t- - - - - }</pre>
UNIX GID	Generated

名前	<b>./:/sec/group/subsys/dce/sec-admin</b>
ウェルノウン 説明	いいえ これは、セキュリティ管理者のグループです。このグループのメンバーは、セキュリティ・データベースを管理するためのすべての許可を持っています。
デフォルト ACL オブジェクト ACL	<pre>{unauthenticated r- t- - - - - } {user creator rctDnfmM} {group_obj r- t- - - - - } {group acct-admin rctDnfmM} {other_obj r- t- - - - - } {any_other r- t- - - - - }</pre>
UNIX GID	Generated

名前	<b>./:/sec/group/subsys/dce/audit-admin</b>
ウェルノウン 説明	いいえ これは、監査デーモン管理者のグループです。このグループのメンバーには、監査デーモン ( <b>auditd</b> ) を管理するための許可がすべて与えられています。
デフォルト ACL	

名前	<code>././sec/group/subsys/dce/audit-admin</code>
オブジェクト ACL	<pre>{unauthenticated r- t- - - - - } {user creator rctDnfmM} {group_obj r- t- - - - - } {group acct-admin rctDnfmM} {other_obj r- t- - - - - } {any_other r- t- - - - - }</pre>
UNIX GID	Generated

## sec/principal ディレクトリー

以下の表は、セキュリティー **sec/principal** ディレクトリーである `././sec/principal` のネーム・スペース・エントリーを説明しています。

名前	<code>././sec/principal/bin</code>
ウェルノウン 説明	いいえ これは、システム・バイナリーの所有者です。
デフォルト ACL オブジェクト ACL	<pre>{unauthenticated r- - - - - - - - } {user_obj r- - - f- - ug} {user creator rcDnfmAug} {group acct-admin rcDnfmAug} {other_obj r- - - - - - - g} {any_other r- - - - - - - - }</pre>
UNIX UID	3

名前	<code>././sec/principal/cell_admin</code>
ウェルノウン 説明	いいえ これは、初期セル構成を行うプリンシパルです。
デフォルト ACL オブジェクト ACL	<pre>{unauthenticated r- - - - - - - - } {user_obj rcDnfmAug} {user creator rcDnfmAug} {group acct-admin rcDnfmAug} {other_obj r- - - - - - - g} {any_other r- - - - - - - }</pre>
UNIX UID	Generated

名前	<code>././sec/principal/daemon</code>
ウェルノウン 説明	いいえ これは、各種デーモンのユーザーです。
デフォルト ACL オブジェクト ACL	<pre>{unauthenticated r- - - - - - - - } {user_obj r- - - f- - ug} {user creator rcDnfmAug} {group acct-admin rcDnfmAug} {other_obj r- - - - - - - g} {any_other r- - - - - - - }</pre>
UNIX UID	1



名前	<code>./sec/principal/dce-ptgt</code>
ウェルノウン 説明	はい これは、特権サーバーの体系的に定義されたプリンシ パル名です。
デフォルト ACL オブジェクト ACL	<code>{unauthenticated r- - - - - }</code> <code>{user_obj r- - - f- - ug}</code> <code>{user_creator rcDnfmaug}</code> <code>{group acct-admin rcDnfmaug}</code> <code>{other_obj r- - - - - g}</code> <code>{any_other r- - - - - }</code>
UNIX UID	20

名前	<code>./sec/principal/dce-rgy</code>
ウェルノウン 説明	はい これは、レジストリー・サーバーの体系的に定義され たプリンシパル名です。
デフォルト ACL オブジェクト ACL	<code>{unauthenticated r- - - - - }</code> <code>{user_obj r- - - f- - ug}</code> <code>{user_creator rcDnfmaug}</code> <code>{group acct-admin rcDnfmaug}</code> <code>{other_obj r- - - - - g}</code> <code>{any_other r- - - - - }</code>
UNIX UID	21

名前	<code>./sec/principal/hosts</code>
ウェルノウン 説明	いいえ このディレクトリーは、すべての DCE ホスト・プリ ンシパルを含んでいます。
デフォルト ACL オブジェクト ACL	<code>{unauthenticated r- - - - }</code> <code>{user_creator rcidDn}</code> <code>{group acct-admin rcidDn}</code> <code>{other_obj r- - - - }</code> <code>{any_other r- - - - }</code>
初期オブジェクト ACL	<code>{unauthenticated r- - - - - }</code> <code>{user_obj r- - - f- - ug}</code> <code>{user_creator rcDnfmaug}</code> <code>{group acct-admin rcDnfmaug}</code> <code>{other_obj r- - - - - g}</code> <code>{any_other r- - - - - }</code>
初期コンテナ ACL	<code>{unauthenticated r- - - - }</code> <code>{user_creator rcidDn}</code> <code>{group acct-admin rcidDn}</code> <code>{other_obj r- - - - }</code> <code>{any_other r- - - - }</code>

名前	<code>./sec/principal/krbtgt</code> ( <code>./...</code> としても認識される)
ウェルノウン 説明	はい これは、外部セル名がカタログされているセキュリティー・ネーム・スペースの、体系的に指定された名前です。このセルが通信するすべてのセルが、ここに現れます。
デフォルト ACL オブジェクト ACL	<pre>{unauthenticated r- - - - - } {user creator rcidDn} {group acct-admin rcidDn} {other_obj r- - - - - } {any_other r- - - - - }</pre>
初期オブジェクト ACL	<pre>{unauthenticated r- - - - - - - - } {user_obj r- - - f- - ug} {user creator rcDnfmaug} {group acct-admin rcDnfmaug} {other_obj r- - - - - - g} {any_other r- - - - - - - }</pre>
初期コンテナ ACL	<pre>{unauthenticated r- - - - - } {user creator rcidDn} {group acct-admin rcidDn} {other_obj r- - - - - } {any_other r- - - - - }</pre>

名前	<code>./sec/principal/krbtgt/cellname</code> ( <code>./:</code> としても認識される)
ウェルノウン 説明	いいえ これは <code>./:cellname</code> という名前のセルの認証サーバーのプリンシパルです。ローカル・セルでは、これは <code>./:</code> のプリンシパルです。
デフォルト ACL オブジェクト ACL	<pre>{unauthenticated r- - - - - - g} {user_obj r- - - f- - ug} {user creator rcDnfmaug} {group acct-admin rcDnfmaug} {other_obj r- - - - - - g} {any_other r- - - - - - - }</pre>

名前	<code>./sec/principal/mail</code>
ウェルノウン 説明	いいえ これは、メール・サブシステムのユーザーです。
デフォルト ACL オブジェクト ACL	<pre>{unauthenticated r- - - - - - - } {user_obj r- - - f- - ug} {user creator rcDnfmaug} {group acct-admin rcDnfmaug} {other_obj r- - - - - - g} {any_other r- - - - - - - }</pre>
UNIX UID	6

名前	<b>./sec/principal/nobody</b>
ウェルノウン 説明	いいえ これは、NFS アクセスのためのデフォルト・ユーザーです。
デフォルト ACL オブジェクト ACL	<pre>{unauthenticated r- - - - - } {user_obj r- - - f- - ug} {user_creator rcDnfmaug} {group acct-admin rcDnfmaug} {other_obj r- - - - - g} {any_other r- - - - - }</pre>
UNIX UID	2

名前	<b>./sec/principal/root</b>
ウェルノウン 説明	いいえ これは、ローカル・オペレーティング・システム・スーパーユーザーです。
デフォルト ACL オブジェクト ACL	<pre>{unauthenticated r- - - - - } {user_obj r- - - f- - ug} {user_creator rcDnfmaug} {group acct-admin rcDnfmaug} {other_obj r- - - - - g} {any_other r- - - - - }</pre>
UNIX UID	0

名前	<b>./sec/principal/sys</b>
ウェルノウン 説明	いいえ これは、装置を読むことを許可されたユーザーですが、スーパーユーザーではありません。
デフォルト ACL オブジェクト ACL	<pre>{unauthenticated r- - - - - } {user_obj r- - - f- - ug} {user_creator rcDnfmaug} {group acct-admin rcDnfmaug} {other_obj r- - - - - g} {any_other r- - - - - }</pre>
UNIX UID	2

名前	<b>./sec/principal/tcb</b>
ウェルノウン 説明	いいえ これは、OSF/1 C2/B1 保護システム上のセキュリティ・ポリシー・デーモンのユーザーです。
デフォルト ACL オブジェクト ACL	<pre>{unauthenticated r- - - - - } {user_obj r- - - f- - ug} {user_creator rcDnfmaug} {group acct-admin rcDnfmaug} {other_obj r- - - - - g} {any_other r- - - - - }</pre>

名前	<code>././sec/principal/tcb</code>
UNIX UID	9

名前	<code>././sec/principal/uucp</code>
ウェルノウン 説明 デフォルト ACL オブジェクト ACL	いいえ これは、UUCP サブシステムのユーザーです。  <pre>{unauthenticated r- - - - - } {user_obj r- - - f- - ug} {user_creator rcDnfmaug} {group acct-admin rcDnfmaug} {other_obj r- - - - - g} {any_other r- - - - - }</pre>
UNIX UID	4

名前	<code>././sec/principal/who</code>
ウェルノウン 説明 デフォルト ACL オブジェクト ACL	いいえ これは、リモート <b>who</b> アクセスのユーザーです。  <pre>{unauthenticated r- - - - - } {user_obj r- - - f- - ug} {user_creator rcDnfmaug} {group acct-admin rcDnfmaug} {other_obj r- - - - - g} {any_other r- - - - - }</pre>
UNIX UID	5

## sec/principal/hosts ディレクトリー

以下の表は、セキュリティー `sec/principal/hosts` ディレクトリーである `././sec/principal/hosts` のネーム・スペース・エントリーを説明しています。

名前	<code>././sec/principal/hosts/hostname</code>
ウェルノウン 説明 デフォルト ACL オブジェクト ACL	いいえ このディレクトリーには、ホスト <code>hostname</code> のセキュリティー・プリンシパルが含まれています。  <pre>{unauthenticated r- - - - - } {user_creator rcidDn} {group acct-admin rcidDn} {other_obj r- - - - - } {any_other r- - - - - }</pre>
初期オブジェクト ACL	<pre>{unauthenticated r- - - - - g} {user_obj r- - - f- - ug} {user_creator rcDnfmaug} {group acct-admin rcDnfmaug} {other_obj r- - - - - g} {any_other r- - - - - }</pre>

名前 初期コンテナ ACL	<b><i>./sec/principal/hosts/hostname</i></b>  {unauthenticated r- - - - - } {user creator rcidDn} {group acct-admin rcidDn} {other_obj r- - - - - } {any_other r- - - - - }
------------------	---

名前	<b><i>./sec/principal/hosts/hostname/cds-server</i></b>
ウェルノウン 説明	いいえ ノード <i>hostname</i> 上の CDS サーバーは、このプリンシパルとして実行されます。このプリンシパルは、 <b><i>./sec/group/subsys/dce/cds-server</i></b> セキュリティー・グループのメンバーでなければなりません。
デフォルト ACL オブジェクト ACL	{unauthenticated r- - - - - } {user_obj r- - - f- - ug} {user creator rcDnfmaug} {group acct-admin rcDnfma- g} {group subsys/dce/cds-admin rcDnfma- g} {other_obj r- - - - - g} {any_other r- - - - - }
UNIX UID	Generated

名前	<b><i>./sec/principal/hosts/hostname/dfs-server</i></b>
ウェルノウン 説明	いいえ これは、ノード <i>hostname</i> 上の DFS サーバーのプリンシパル名です。
デフォルト ACL オブジェクト ACL	{unauthenticated r- - - - - g} {user_obj r- - - f- - ug} {user creator rcDnfmaug} {group acct_admin rcDnfma- g} {other_obj r- - - - - g} {any_other r- - - - - }
UNIX UID	Generated

名前	<b><i>./sec/principal/hosts/hostname/gda</i></b>
ウェルノウン 説明	いいえ ノード <i>hostname</i> 上の GDA はこのプリンシパルとして実行されます。このプリンシパルは、 <b><i>./sec/group/subsys/dce/cds-servers</i></b> セキュリティー・グループのメンバーでなければなりません。
デフォルト ACL オブジェクト ACL	{unauthenticated r- - - - - g} {user_obj r- - - f- - ug} {user creator rcDnfmaug} {group acct-admin rcDnfmaug} {group subsys/dce/cds-admin rcDnfmaug} {other_obj r- - - - - g} {any_other r- - - - - }

名前	<code>././sec/principal/hosts/<i>hostname</i>/gda</code>
UNIX UID	Generated

名前	<code>././sec/principal/hosts/<i>hostname</i>/self</code>
ウェルノウン 説明	はい このエントリーはホスト <i>hostname</i> のプリンシパルです。 <b>dced</b> デーモンのセキュリティー妥当性検査サービスでは、このプリンシパルを使用します。これは、ローカル・ルート・プロセスが継承できる ID でもあります。
デフォルト ACL オブジェクト ACL	<pre>{unauthenticated r- - - - - } {user_obj r- - - f- - ug} {user_creator rcDnfma- g} {group acct-admin rcDnfma- g} {other_obj r- - - - - g} {any_other r- - - - - }</pre>
UNIX UID	Generated

## 付録D. 特記事項

本書において、日本では発表されていない IBM 製品（機械およびプログラム）、プログラミングまたはサービスについて言及または説明する場合があります。しかし、このことは、弊社がこのような IBM 製品、プログラミングまたはサービスを、日本で発表する意図があることを必ずしも示すものではありません。本書で IBM ライセンス・プログラムまたは他の IBM 製品に言及している部分があっても、このことは当該プログラムまたは製品のみが使用可能であることを意味するものではありません。IBM 製品、プログラム、またはサービスに代えて、IBM の有効な知的所有権またはその他の法的に保護された権利を侵害することのない、機能的に同等の製品、プログラム、またはサービスを使用することができます。ただし、IBM によって明示的に指定されたものを除き、他社の製品と組み合わせた場合の操作の評価と検証はお客様の責任で行っていただきます。

IBM は、本書で解説されている主題について特許権（特許出願を含む）、商標権、または著作権を所有している場合があります。本書の提供は、これらの特許権、商標権、および著作権について、本書で明示されている場合を除き、実施権、使用権等を許諾することを意味するものではありません。実施権、使用権等の許諾については、下記の宛先に、書面にてご照会ください。

〒106-0032 東京都港区六本木3丁目2-31

AP 事業所

IBM World Trade Asia Corporation

Intellectual Property Law & Licensing

以下の保証は、国または地域の法律に沿わない場合は、適用されません。IBM およびその直接または間接の子会社は、本書を特定物として現存するままの状態を提供し、商品性の保証、特定目的適合性の保証および法律上の瑕疵担保責任を含むすべての明示もしくは黙示の保証責任を負わないものとします。国または地域によっては、法律の強行規定により、保証責任の制限が禁じられる場合、強行規定の制限を受けるものとします。

本書に対して、周期的に変更が行われ、これらの変更は、文書の次版に組み込まれます。IBM は、随時、この文書に記載されている製品またはプログラムに対して、改良または変更を行うことがあります。

本書において IBM 以外の Web サイトに言及している場合がありますが、便宜のため記載しただけであり、決してそれらの Web サイトを推奨するものではありません。それらの Web サイトにある資料は、この IBM 製品の資料の一部ではありません。それらの Web サイトは、お客様の責任でご使用ください。

IBM は、お客様が提供するいかなる情報も、お客様に対してなんら義務も負うことのない、自ら適切と信ずる方法で、使用もしくは配布することができるものとします。

本プログラムのライセンス保持者で、(i) 独自に作成したプログラムとその他のプログラム（本プログラムを含む）の間での情報交換、および (ii) 交換された情報の相互利用を可能にすることを目的として、本プログラムに関する情報を必要とする方は、下記に連絡してください。

IBM Corporation  
Department LZKS  
11400 Burnet Road  
Austin, TX 78758  
U.S.A.

本プログラムに関する上記の情報は、適切な使用条件の下で使用することができませんが、有償の場合もあります。

本書で説明されているライセンス・プログラムまたはその他のライセンス資料は、IBM所定のプログラム契約の契約条項、IBM プログラムのご使用条件、またはそれと同等の条項に基づいて、IBMより提供されます。

この文書に含まれるいかなるパフォーマンス・データも、管理環境下で決定されたものです。そのため、他の操作環境で得られた結果は、異なる可能性があります。一部の測定が、開発レベルのシステムで行われた可能性があります。その測定値が、一般に利用可能なシステムのものと同じである保証はありません。さらに、一部の測定値が、推定値である可能性があります。実際の結果は、異なる可能性があります。お客様は、お客様の特定の環境に適したデータを確かめる必要があります。

IBM 以外の製品に関する情報は、その製品の供給者、出版物、もしくはその他の公に利用可能なソースから入手してください。IBM は、それらの製品のテストは行っておりません。また、IBM 以外の製品に関するパフォーマンスの正確性、互換性、またはその他の要求は確認できません。IBM 以外の製品の性能に関する質問は、それらの製品の供給者をお願いします。

IBM の将来の方向または意向に関する記述については、予告なしに変更または撤回される場合があります、単に目標を示しているものです。

表示されている IBM の価格は IBM が小売り価格として提示しているもので、現行価格であり、通知なしに変更されるものです。卸価格は、異なる場合があります。

著作権ライセンス:

本書の情報には、ソース言語によるサンプル・アプリケーション・プログラムが含まれていますが、これらは各種オペレーティング・プラットフォーム上のプログラミング技法を例示したものです。これらのサンプル・プログラムは、IBM に料金を支払うことなく、サンプル・プログラムが作成されたオペレーティング・プラットフォームのアプリケーション・プログラミング・インターフェースに準拠したアプリケーション・プログラムを開発、使用、販売または配布する目的で、コピー、変更、および配布することができます。

これらの例は、すべての条件下で十分にテストされているわけではありません。したがって、IBM はこれらのプログラムの信頼性、保守容易性、または機能の保証または暗示を行っていません。これらのサンプル・プログラムは、IBM に料金を支払うことなく、IBM のアプリケーション・プログラミング・インターフェースに準拠したアプリケーション・プログラムを開発、使用、販売または配布する目的で、コピー、変更、および配布することができます。



これらのサンプル・プログラムまたはその派生物の全体または一部のコピーには、次のような著作権表示を組み込む必要があります。

© (ユーザーの会社名) (年). Portions of this code are derived from IBM Corp. Sample Programs. © Copyright IBM Corp. 1990, 2001. All rights reserved.

この情報をソフトコピーでご覧になっている場合は、写真やカラーの図表は現れない場合があります。

---

## 商標

次のものは、IBM Corporation の米国およびその他の国における商標です。

- AIX
- DFS
- IBM
- OS/390

Microsoft は Microsoft Corporation の米国およびその他の国における商標です。

UNIX は、The Open Group がライセンスしている米国およびその他の国における登録商標です。

他の会社名、製品名およびサービス名等はそれぞれ各社の商標または登録商標です。



# 索引

日本語, 数字, 英字, 特殊文字の順に配列されています。なお, 濁音と半濁音は清音と同等に扱われています。

## [ア行]

- アカウント
  - 管理 41
  - UNIX 41
- アクセス制御
  - ネーム・スペースにおける 39
- アクセス制御リスト (ACL)
  - 説明 6
- アプリケーション開発マシン 30

## [カ行]

- 監査サーバー
  - 計画ガイドライン 25
- 監査サービス
  - クライアント要件 20
- 環境変数
  - 監査変数
    - DCEAUDITFILTERON 57
    - DCEAUDITOFF 57
    - DCEAUDITON 57
    - DCEAUDITTRAILSIZE 58
    - DCEAUDITWRAP 58
    - SECAUDITWRAP 58
- 構成
  - dcelocal 59
- セキュリティ
  - BIND\_PE\_SITE | TRY\_PE\_SITE 69
  - KRB5CCNAME 69
- IDL 60
  - IDL\_GEN\_AUX\_FILES 60
  - IDL\_GEN\_INTF\_DATA 60
- NLS/セキュリティ
  - DCE\_USE\_NONPORTABLE\_NAMES 61
  - DCE\_USE\_WCHAR\_NAMES 61
- RPC
  - DCERPCCHARTRANS 62
  - RPC\_CN\_AUTH\_SUBTYPE 62
  - RPC\_DEFAULT\_ENTRY 62
  - RPC\_DEFAULT\_ENTRY\_SYNTAX 63
  - RPC\_DISABLE\_EP\_RESOLVE\_V4 63
  - RPC\_DISABLE\_SINGLE\_THREAD 63
  - RPC\_EXTRA\_INTERFACE 64
  - RPC\_ITIMER\_SIGNAL 64

環境変数 (続き)

- RPC (続き)
  - RPC\_MAX\_UDP\_PACKET\_SIZE 64
  - RPC\_NETADDRS\_ORDER 65
  - RPC\_NETIFS\_ORDER 66
  - RPC\_RESTRICTED\_PORTS 66
  - RPC\_RESTRICTED\_SERVER\_PORTS 67
  - RPC\_SUPPORTED\_PROTSEQS 67
  - RPC\_UNSUPPORTED\_NETADDRS 68
  - RPC\_UNSUPPORTED\_NETIFS 68

管理、DCE の  
説明 3  
ユーティリティ 28

管理ツール

- ブラウザー 37

管理プログラム 28  
レジストリー 29

- cdsadv 29
- cdsclerk 29
- cdscp 29
- cdsdel 29
- cdsli 29
- dcecp 28, 29
- group\_override 28
- passwd\_export 28
- passwd\_import 28
- passwd\_override 28
- rmxcred 28
- rpccp 28

キャッシング

- 説明 7
- クライアント / サーバー・モデル 3

クリアリングハウス 37

グローバル・ディレクトリー・エージェント (GDA)  
サーバー要件 26

ゲートウェイ

- セル構成における 10

構成、DCE の

- クライアント・マシン 19
- 計画 9
- サーバー・マシン 24

## [サ行]

サーバー・マシン

- 構成 24

作業

- 保守 37, 39, 41

作成、ファイル・システム 35

- 実行時ファイル 34
- ジャンクション 13
- スカルク 38
- セキュリティー・サーバー
  - 要件 24
- セキュリティー・サービス
  - アクセス制御計画 16
  - 管理ユーティリティー 28
  - クライアント要件 20
  - 保守作業 41
- セル 3
  - 間の通信 10
  - アクセス制御 16
  - 計画ガイドライン 9
  - 説明 4
  - ホストの削除 12
- セル間接続 10
- セル・ディレクトリー・サービス (CDS)
  - 管理ユーティリティー 29
  - クライアント要件 20
  - ルート・ディレクトリー構造および内容 73
  - hosts ディレクトリーの内容 78
  - subsys ディレクトリーの内容 82
- セル・ネーム・スペース
  - セキュリティー 39
  - 内容の表示 37
  - モニター 38

## [タ行]

- 追加ファイル・システム、作成する 35
- ドメイン・ネーム・システム (DNS)
  - セル名 11
  - セル名の登録 12
  - セル命名規則 11

## [ナ行]

- ネーム・スペース
  - 構成ガイドライン 12
  - 構造および内容 73
  - 説明 5

## [ハ行]

- バックアップ
  - レジストリー 42
- ファイル
  - インストール後に作成 35
  - 実行時に作成される 34
- ファイルの場所
  - UNIX サブディレクトリー 32

- ファイルの場所 (続き)
  - /opt/dcelocal 31
- ファイル・スペース
  - 説明 5
- 複製
  - 説明 7
  - セル構成 9, 16
- ブラウザー 37
- プリンシパル
  - 説明 6
- 分散タイム・サービス (DTS)
  - クライアント要件 21
  - サーバー要件 26
- 保守作業
  - セキュリティー・サービス 41
  - CDS 37
  - DTS 39
- ホスト 3
- ポリシー
  - オーバーライド 41
  - 設定および保守 41

## [マ行]

- マシン
  - セルから削除 12

## [ラ行]

- リモート・プロシージャ・コール (RPC)
  - クライアント要件 19
  - 説明 4
- レジストリー 29
  - 再構成の処理 43
  - バックアップ 42
  - dcecp の使用 41
- レジストリー・データベース
  - 構造および内容 14, 84
  - 最上位ディレクトリー 86
  - sec/group ディレクトリー 89
  - sec/group/subsys ディレクトリー 92
  - sec/principal ディレクトリー 96

## A

- ACL 41

## C

- CDS
  - 制御プログラム 37
  - ブラウザー 37

CDS (続き)  
 保守作業 37  
 モニター 38  
CDS サーバー  
 計画ガイドライン 25  
cdsadv 29  
cdsclerk 29  
cdscp 29  
cdsdel 29  
cdsli 29

## D

DCE リモート・プロシージャ・コール (RPC)  
 サーバー要件 24  
dcecp 28, 29  
dcelocal 31  
DTS  
 保守作業 39  
dtscp 39

## G

group\_override 28  
group\_override file (group\_override ファイル) 42

## P

passwd\_export 28, 41  
passwd\_import 28, 41  
passwd\_override 28  
passwd\_override file (passwd\_override ファイル) 42

## R

rmxcred 28

## U

UNIX ディレクトリー 32

## [特殊文字]

/opt/dcelocal サブツリー 31  
/var/dce 35







Printed in Japan