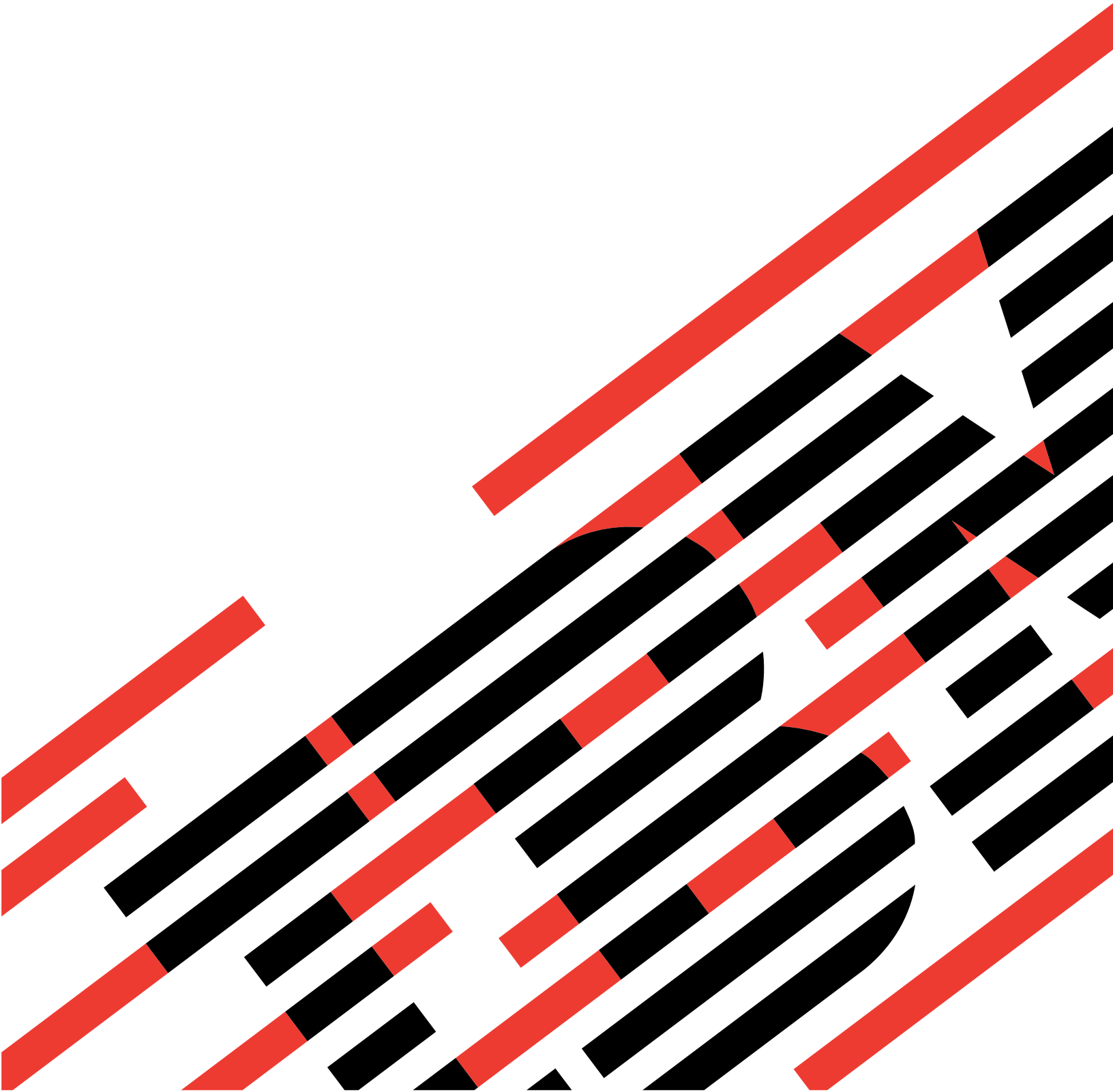
IBM

eserver

iSeries

ネットワーキング
ディレクトリー・サービス (LDAP)



IBM

@server

iSeries

ネットワーキング
ディレクトリー・サービス (LDAP)

目次

第 1 部 ディレクトリー・サービス (LDAP) 1

第 1 章 V5R2 の新機能 3

第 2 章 トピックの印刷 5

第 3 章 ディレクトリー・サービスの概要 7
LDAP に関する基本事項 8
LDAP V3 で LDAP V2 を使用する場合の考慮事項 11
LDAP ディレクトリー・サーバーを計画する 11
ディレクトリー・サービスの旧リリースを V5R2 にマイグレーションする 12
V4R3 または V4R4 のディレクトリー・サービスを V5R2 にマイグレーションする 13
ディレクトリー・サービスをインストールして構成する 15
LDAP ディレクトリー・サーバーを構成する 15
ディレクトリー・サービスのデフォルト構成 17
IBM SecureWay ディレクトリー管理ツール 18

第 4 章 LDAP ディレクトリー・サーバーを管理する 19
LDAP ディレクトリー・サーバーを開始する 19
LDAP ディレクトリー・サーバーを停止する 20
ディレクトリー・サーバーの状況を検査する 20
LDAP ディレクトリー・サーバーのジョブを検査する 21
イベント通知を使用可能にする 21
トランザクション設定値を指定する 21
| ポートまたは IP アドレスを変更する 22
LDAP ディレクトリー・データをシステム間で移動する 22
LDIF ファイルをインポートする 23
LDIF ファイルをエクスポートする 23
ディレクトリー・サーバーの新しいレプリカを設定する 23
情報をディレクトリー・サーバーに発行する 28
ディレクトリー参照用のサーバーを指定する 30
LDAP ディレクトリー・サーバーに接尾部を追加する 31
ディレクトリー・サーバーから接尾部を削除する 31
ディレクトリー・サービス情報の保管と復元 31
ディレクトリー・データの所有権とアクセス権を管理する 32
ディレクトリー・オブジェクトの所有権プロパティーを処理する 32
アクセス制御リスト (ACL) の処理 32
ACL グループを処理する 33
許可ユーザーの管理アクセスを処理する 33
LDAP ディレクトリーに対するアクセスと変更をトラッキングする 34
ディレクトリー・サーバーのオブジェクト監査を使用可能にする 34
LDAP ディレクトリー・サーバーのパフォーマンスを調整する 35

第 5 章 ディレクトリー・サービスの概念と参照情報 37
LDAP アクセス制御リスト (ACL) 37
LDAP データ交換形式 39
各国語サポート (NLS) に関する考慮事項 41
LDAP ディレクトリー・オブジェクトの所有権 41
LDAP ディレクトリーの参照 42

トランザクション 42
レプリカ LDAP ディレクトリー・サーバー 43
ディレクトリー・サービスのセキュリティー 43
LDAP ディレクトリー・サーバーで Secure Sockets Layer (SSL) と Translation Layer Security を使用する 44
LDAP ディレクトリー・サーバーで Kerberos 認証を使用する 44
オペレーティング・システム・プロジェクト・バックエンド 45
OS/400 ユーザー・プロジェクト・ディレクトリー情報ツリー 46
LDAP 操作 47
管理者とレプリカ・バインド DN 51
OS/400 ユーザー・プロジェクト・スキーマ 51
ディレクトリー・サービスと OS/400 ジャーナル・サポート 51

第 6 章 LDAP コマンド行ユーティリティー 53
ldapmodify および ldapadd ユーティリティー 54
例: ldapmodify および ldapadd 55
ldapdelete ユーティリティー 57
例: ldapdelete 58
ldapsearch ユーティリティー 59
例: ldapsearch 61
ldapmodrdn ユーティリティー 64
例: ldapmodrdn 66
LDAP コマンド行ユーティリティーで SSL を使用する上での注意事項™ 66

第 7 章 ディレクトリー・サービスのトラブルシューティング 69
ディレクトリー・サービスに関する基本的なトラブルシューティング手順 69
ディレクトリー・サービスのジョブ・ログによりエラーおよびアクセスをモニターする 70
TRCTCPAPP を使用して問題を検出する 71
LDAP_OPT_DEBUG オプションを使用してエラーをトレースする 71
LDAP クライアントに関する一般的なエラー 72
ldap_search: Timelimit exceeded (時間制限を超えました) 72
[Failing LDAP operation]: Operations error (LDAP 操作失敗: 操作エラー) 72
ldap_bind: No such object (該当のオブジェクトがありません) 72
ldap_bind: Inappropriate authentication (認証に誤りがあります) 73
[Failing LDAP operation]: Insufficient access (LDAP 操作失敗: アクセス権が不十分です) 73
[failing LDAP operation]: Cannot contact LDAP server (LDAP 操作失敗: LDAP サーバーに接続できません) 73
[failing LDAP operation]: Failed to connect to ssl server (LDAP 操作失敗: SSL サーバーに接続できませんでした) 73

第 1 部 ディレクトリー・サービス (LDAP)

ディレクトリー・サービスは、iSeries サーバーで Lightweight Directory Access Protocol (LDAP) サーバーを使用できるようにします。 LDAP は伝送制御プロトコル / インターネット・プロトコル (TCP/IP) で実行されるもので、インターネット・アプリケーションおよびインターネット以外のアプリケーション用のディレクトリー・サービスとしてよく用いられています。

ディレクトリー・サービスを熟知している読者は、このリリースの新機能から読み始めてください。必要な場合は、ディレクトリー・サービス情報の PDF 版を印刷または表示することができます。

以下のトピックでは、ディレクトリー・サービスの概要および iSeries™ サーバーでの LDAP サーバーの管理について説明します。

7 ページの『第 3 章 ディレクトリー・サービスの概要』

19 ページの『第 4 章 LDAP ディレクトリー・サーバーを管理する』

37 ページの『第 5 章 ディレクトリー・サービスの概念と参照情報』

53 ページの『第 6 章 LDAP コマンド行ユーティリティー』

69 ページの『第 7 章 ディレクトリー・サービスのトラブルシューティング』

ディレクトリー・サービスに関する追加情報については、 ディレクトリー・サービス Web ページ  を参照してください。

ディレクトリー・サービスが提供する LDAP サーバーは、 IBM® SecureWay® Directory  です。

第 1 章 V5R2 の新機能

ディレクトリー・サービスには、以下の拡張機能と新機能が追加されています。

- ディレクトリー・サービスは、V5R1 から基本オペレーティング・システムの一部になっています。オプション 32 は、V5R2 から使用不可になりました。
- ディレクトリー・サーバーに保管されたデータの保護を強化するため、新しいセキュリティー拡張が追加されています。
- LDAP ディレクトリー・サーバーは、 Enterprise Identity Mapping (EIM) ドメインのドメイン・コントローラーとして使用できるようになりました。
- iSeries ナビゲーター・アプリケーション・サポートを介してオペレーティング・システムのディレクトリー・サービス管理者 (QIBM_DIRSRV_ADMIN) ファンクション ID へのアクセスが与えられているユーザーに対して、 ディレクトリー・サーバーへの管理アクセスを付与するために管理者が使用できる新しいオプションが用意されています。
- ディレクトリー・サーバーに特定の IP アドレスを使用させるか、またはサーバー上のすべての構成済み IP アドレスを使用するかを選択できます。詳細については、 22 ページの『ポートまたは IP アドレスを変更する』を参照してください。
- V5R2 では、 **ldap_set_option** API に新しいデバッグ・トレース機能が追加されています。 LDAP C API を使用するクライアントの問題の診断を助けるために、 LDAP_OPT_DEBUG オプションを使用することができます。詳細については、 71 ページの『LDAP_OPT_DEBUG オプションを使用してエラーをトレースする』または iSeries Information Center のディレクトリー・サービス API (Directory Services API) を参照してください。

新機能や変更点を見つける方法:

技術的な変更が加えられた個所を見つけやすくするために、この資料では、次のようなイメージが使われています。

- は、新機能や変更点の情報が始まる個所を示します。
- は、新機能や変更点の情報が終わる個所を示します。

第 2 章 トピックの印刷

PDF 版をダウンロードし、表示するには、 OS/400 ディレクトリー・サービス (LDAP) (約 808 KB、82 ページ) を選択します。

その他の情報

以下の PDF も表示したり印刷したりできます。

- *LDAP Implementation Cookbook*
- *Understanding LDAP*
- *Using LDAP for Directory Integration: A Look at IBM SecureWay Directory, Active Directory, and Domino*™
- *Implementation and Practical Use of LDAP on the iSeries Server*

表示用または印刷用の PDF ファイルを Netscape Navigator からワークステーションに保存するには、次のようにします。

1. ブラウザーで PDF を開く (上記のリンクをクリックする)。
2. ブラウザーのメニューから**「ファイル」**をクリックする。
3. **「名前を付けて保存」**をクリックする (IE の場合は、フロッピーディスクのアイコン (名前を付けて保存) をクリックする)。
4. PDF を保存したいディレクトリーに進む。
5. **「保存」**をクリックする。

Adobe Acrobat Reader のダウンロード

上記の PDF を表示または印刷するために Adobe Acrobat Reader が必要な場合は、 Adobe Web サイト (www.adobe.com/products/acrobat/readstep.html) から、そのコピーをダウンロードすることできます。

第 3 章 ディレクトリー・サービスの概要

ディレクトリー・サービスは、iSeries サーバーで Lightweight Directory Access Protocol (LDAP) サーバーを使用できるようにします。 LDAP は伝送制御プロトコル / インターネット・プロトコル (TCP/IP) で実行されるもので、インターネット・アプリケーションおよびインターネット以外のアプリケーション用のディレクトリー・サービスとして一般的になってきています。 OS/400 ベースの LDAP ディレクトリー・サーバーの設定および管理タスクのほとんどは、 iSeries ナビゲーターのグラフィカル・ユーザー・インターフェース (GUI) から実行します。ディレクトリー・サービスを管理するには、 iSeries サーバーに接続している PC に iSeries ナビゲーターをインストールしておく必要があります。ディレクトリー・サービスは、LDAP 対応のアプリケーション (LDAP サーバーから電子メール・アドレスを見つけるメール・アプリケーションなど) で使用することができます。

LDAP サーバーのほかに、ディレクトリー・サービスには次のものが含まれています。

- OS/400 ベースの LDAP クライアント。このクライアントには一組のアプリケーション・プログラム・インターフェース (API) が組み込まれており、 OS/400® プログラムの中でこれを使用して、独自のクライアント・アプリケーションを作成できます。これらの API の詳細については、 iSeries Information Center の『プログラミング』の下にあるディレクトリー・サービスを参照してください。
- IBM SecureWay ディレクトリー・クライアント・ソフトウェア開発キット (SDK) のバージョン 3.2。この SDK には、 Windows® LDAP クライアントのほかに以下のツールが組み込まれています。
  - IBM SecureWay ディレクトリー管理ツール。ディレクトリーの内容を管理するためのグラフィカル・ユーザー・インターフェースを提供します。
  - コマンド行ユーティリティー (ldapsearch、ldapadd など)
  - C LDAP API (ライブラリー・ファイル、ヘッダー・ファイル、サンプル・ソース・コード)
  - IBM JNDI LDAP サービス・プロバイダー (ibmjndi.jar)
  - 上記のすべての項目のオンライン資料。各 HTML ファイルの場所と名前については、 README ファイルを参照してください。

OS/400 の旧バージョンでディレクトリー・サービスを使用している場合には、 12 ページの『ディレクトリー・サービスの旧リリースを V5R2 にマイグレーションする』を参照してください。

LDAP の概要については、 8 ページの『LDAP に関する基本事項』を参照してください。このトピックには OS/400 専用の情報も入っていますので、他のプラットフォームで LDAP サーバーを使用した経験がある方も、このトピックをお読みください。

この基本情報をよく理解したら、 11 ページの『LDAP ディレクトリー・サーバーを計画する』に進んでください。

ディレクトリー・サーバーのインストールと設定については、 15 ページの『ディレクトリー・サービスをインストールして構成する』を参照してください。

資料

Information Center のディレクトリー・サービスでは、 LDAP の概要を示し、特に OS/400 で LDAP ディレクトリー・サーバーを管理する方法について解説しています。この資料には、 SecureWay ディレクトリー・クライアント SDK の十分な資料も用意されています。 LDAP に関するさらに詳しい情報については、以下に示す LDAP の参考文献をご覧ください。

- *LDAP Implementation Cookbook*
- *Understanding LDAP*
- *Using LDAP for Directory Integration: A Look at IBM SecureWay Directory, Active Directory, and Domino*
- *Implementation and Practical Use of LDAP on the iSeries server*
- *LDAP: Programming Directory-enabled Applications with Lightweight Directory Access Protocol* (Tim Howes および Mark Smith 著)。
- *Understanding and Deploying LDAP Directory Services* (Mark C. Smith、Gordon S. Good、および Tim Howes 著)。

iSeries サーバー上のディレクトリー・サービスに関するさらに詳しい情報は、 iSeries サーバーのディレクトリー・サービスのホーム・ページ にあります。

注: この資料で取り扱っている題材には、 University of Michigan が提供する LDAP 関係資料に基づく記事が含まれています。 Copyright © 1992-1996, Regents of the University of Michigan, All Rights Reserved.

LDAP に関する基本事項

Lightweight Directory Access Protocol (LDAP) は、伝送制御プロトコル / インターネット・プロトコル (TCP/IP) 上で実行されるディレクトリー・サービス・プロトコルです。 LDAP バージョン 2 は、 Internet Engineering Task Force (IETF) Request for Comments (RFC) 1777 の *Lightweight Directory Access Protocol* の中で正式に定義されています。 LDAP バージョン 3 は、IETF RFC 2251 の *Lightweight Directory Access Protocol (v3)* の中で正式に定義されています。これらの RFC は、インターネットを使用して次の URL で見ることができます。

http://www.ietf.org

LDAP ディレクトリー・サービスはクライアント / サーバー・モデルに従っています。ディレクトリー・データは、1 つまたは複数の LDAP サーバーに入っています。 LDAP クライアントは LDAP サーバーに接続され、要求を出します。サーバーは、応答または他の LDAP サーバーへのポインター (参照) を戻します。

LDAP の使用:

LDAP は、データベースではなくディレクトリー・サービスの 1 つなので、 LDAP ディレクトリーの中の情報は、通常は記述的な属性ベースの情報です。一般に、LDAP のユーザーが実行するディレクトリー関連の操作は、情報を読み取る方が、情報を変更する場合よりはるかに多く、その更新も、単純な方式の変更 (すべて変更するかまったく変更しないか) であるのが一般的です。よく使われる LDAP ディレクトリーには、オンラインの電話番号ディレクトリーおよび電子メール・ディレクトリーなどがあります。

LDAP ディレクトリーの構造:

LDAP ディレクトリー・サービス・モデルは、 **項目** (**オブジェクト**ともいう) をもとに構成されています。各項目は、1 つまたは複数の**属性** (名前やアドレスなど) と、 1 つの**タイプ**で構成されています。タイプは、一般に、略号ストリング (共通名を意味する cn や、電子メール・アドレスを意味する mail など) から構成されています。

10 ページの図 1 のディレクトリー例に示す Tim Jones の項目には、 *mail* 属性と *telephoneNumber* 属性が含まれています。その他の可能な属性としては、*fax*、*title*、*sn* (姓)、*jpegPhoto* などがあります。

各ディレクトリーには**スキーマ**があります。スキーマは、ディレクトリーの構造と内容を決定する一組の規則です。 IBM SecureWay ディレクトリー管理ツール (DMT) を使用して、 LDAP サーバー用のスキーマ・ファイルを編集する必要があります。ディレクトリー・サービスのインストール後、スキーマ・ファイルはシステムの /QIBM/UserData/OS400/DirSrv にあります。

注: /QIBM/ProdData/OS400/DirSrv には、デフォルト・スキーマ・ファイルのオリジナル・コピーがあります。 UserData ディレクトリー内のファイルを置き換える必要がある場合は、これらのファイルを /QIBM/ProdData/OS400/DirSrv ディレクトリーにコピーできます。

各ディレクトリー項目は、 **objectClass** という特殊属性を持っています。この属性は、項目内で必要とされる属性および使用できる属性を制御します。つまり、objectClass 属性の値により、項目が従わなければならないスキーマ規則を決定します。

各ディレクトリー項目には、LDAP サーバーにより自動的に管理される以下の**運用属性**が設定されています。

- CreatorsName - 項目を作成したときに使用したバインド DN を示します。
- CreateTimestamp - 項目を作成した時刻を示します。
- modifiersName - 項目を最後に修正したときに使用したバインド DN を示します (この属性の初期値は、CreatorsName の値と同じです)。
- modifyTimestamp - 項目を最後に修正した時刻を示します (この属性の初期値は、CreateTimestamp の値と同じです)。

通常、LDAP ディレクトリーの項目は、政治的、地理的、または組織的な境界を反映した階層構造で配置されます (10 ページの図 1 を参照)。階層の最上位には国を表す項目があります。階層の 2 次レベルは、州または国家組織を表す項目で占められます。さらに下位の階層には、個人単位、企業単位、プリンター、文書、その他の事項を表す項目があります。

ディレクトリーを構成する際には、従来の階層にとらわれる必要はありません。たとえば、ドメイン・コンポーネント構造が、一般に用いられるようになっています。この構造を使用すると、項目は TCP/IP のドメイン・ネームのパーツで構成されます。たとえば、o=ibm,c=us よりも dc=ibm,dc=com の方が適しています。

LDAP は、項目を**識別名** (DN) で参照します。識別名は、その項目自体の名前と、ディレクトリー内でそれより上位にあるオブジェクトの名前 (下位から上位順) で構成されています。たとえば、 10 ページの図 1 の左下隅にある項目の完全 DN は、 cn=Tim Jones, o=IBM, c=US です。各項目には、項目に名前を付けるときに使用される属性が少なくとも 1 つあります。この命名属性のことを、項目の**相対識別名 (RDN)** といいます。与えられた RDN の上位の項目のことを、その**親識別名**といいます。上述の例では、cn=Tim Jones という名前が項目に付けられるので、この名前がその項目の RDN となります。 o=IBM, c=US は、cn=Tim Jones の親識別名です。

LDAP サーバーに LDAP ディレクトリーの一部を管理する機能を与えるには、サーバーの設定の中で、最高位の親識別名を指定します。この種の識別名は**接尾部**と呼ばれます。サーバーは、ディレクトリー内のオブジェクトのうち、ディレクトリー階層内で指定の接尾部より下位にあるすべてのオブジェクトにアクセスできます。たとえば、ある LDAP サーバーに、図 1 に示すディレクトリーがある場合に、そのサーバーが Tim Jones に関するクライアントからの照会に応答できるようにするには、サーバーの設定で接尾部 `o=ibm, c=us` を指定しておく必要があります。

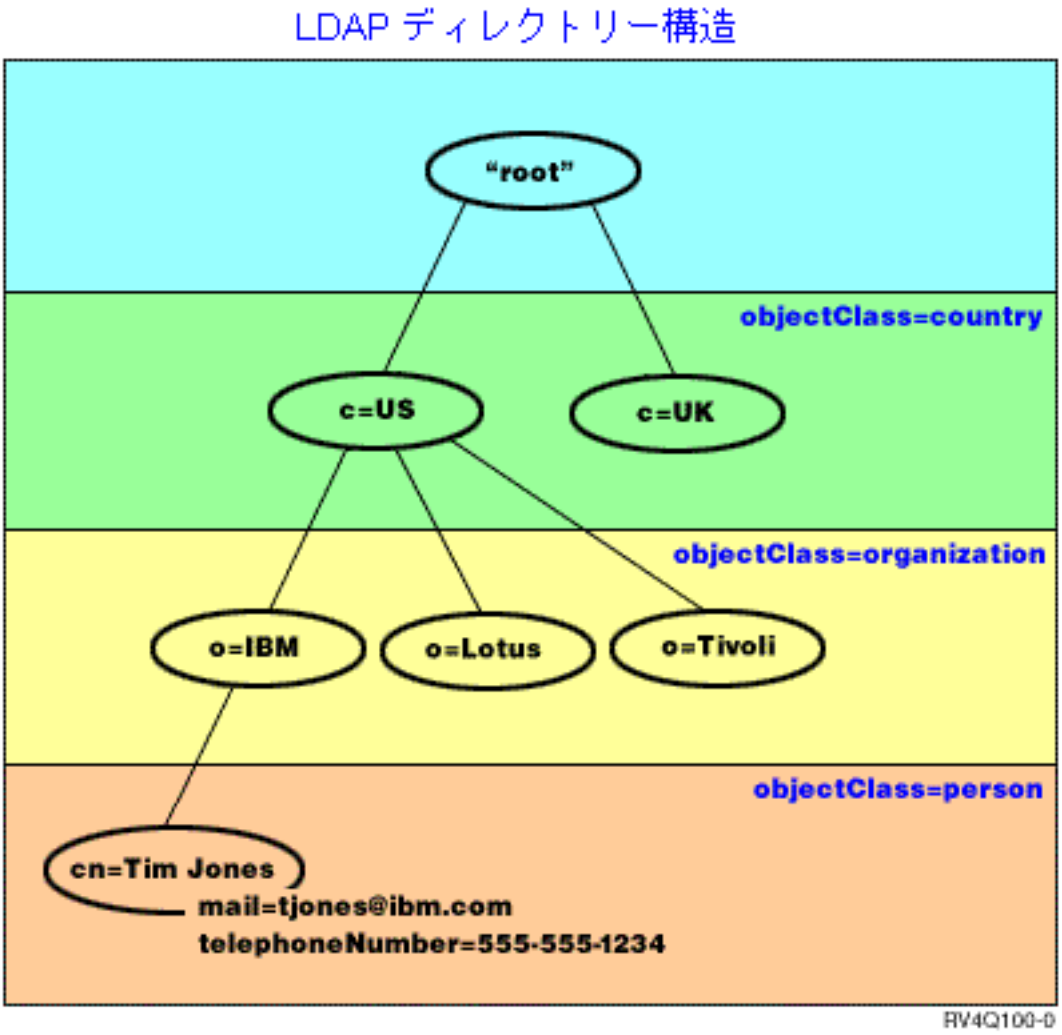


図 1. LDAP ディレクトリーの基本構造

LDAP とディレクトリー・サービスに関する注意事項:

- V4R5 以降の OS/400 LDAP サーバーと OS/400 LDAP クライアントは、両方とも LDAP バージョン 3 をベースにしています。 V3 サーバーで V2 クライアントを使用することができます。ただし、V2 クライアントとしてバインドし、V2 API だけを使用している場合を除いて、 V2 サーバーで V3 クライアントを使用することはできません。詳しくは、LDAP V2/V3 の考慮事項を参照してください。
- Windows LDAP クライアントも LDAP バージョン 3 をベースにしています。
- LDAP は標準なので、すべての LDAP サーバーが多くの共通する基本特性を持っています。しかし、実装形態が違うため、すべてに相互の互換性があるとは限りません。ディレクトリー・サービスが提供す

る LDAP サーバーは、 IBM SecureWay および IBM Directory 製品群の LDAP サーバーとほぼ完全な互換性があります。しかし、他の LDAP サーバーとの互換性はない場合があります。

- ディレクトリー・サービスが提供する LDAP サーバーのデータは、OS/400 データベースにあります。

詳細情報:

LDAP ディレクトリーの使用例については、以下を参照してください。

- レッドブック *Understanding LDAP* のセクション 1.6 の『The Quick Start: A Public LDAP Example』
- レッドブック Understanding LDAP のセクション 3.3 の『Example Scenarios』

LDAP の概念の詳細については、 37 ページの『第 5 章 ディレクトリー・サービスの概念と参照情報』を参照してください。

LDAP V3 で LDAP V2 を使用する場合の考慮事項

V4R5 以降では、OS/400 LDAP サーバーと OS/400 LDAP クライアントは、両方とも LDAP バージョン 3 に基づいています。 V2 サーバーで V3 クライアントを使用することはできません。しかし ldap_set_option() API を使用して、 V3 クライアントのバージョンを V2 に変更することができます。変更終了後、V2 サーバーへのクライアント要求に正常に送信することができます。

V3 サーバーで V2 クライアントを使用することができます。ただし検索要求については、V3 サーバーは UTF-8 形式の全範囲内でデータを返信できますが、 V2 クライアントは IA5 文字セットのデータしか処理できない場合があることにご注意ください。

注: LDAP バージョン 2 は、 Internet Engineering Task Force (IETF) Request for Comments (RFC) 1777 の *Lightweight Directory Access Protocol* の中で正式に定義されています。 LDAP バージョン 3 は、IETF RFC 2251 の *Lightweight Directory Access Protocol (v3)* の中で正式に定義されています。これらの RFC は、インターネットを使用して次の URL で見ることができます。

http://www.ietf.org 

LDAP ディレクトリー・サーバーを計画する

ディレクトリー・サービスをインストールし、LDAP ディレクトリーの設定を始めるにあたり、前もってディレクトリーの計画を立ててください。検討を要する重要事項は次のとおりです。

- **ディレクトリーを編成する**。ディレクトリーの構造の計画を立て、サーバーにどのような接尾部と属性が必要かを判断します。
- **ディレクトリーの大きさを決定する**。その後、どれくらいのストレージが必要かを見積もることができます。ディレクトリーのサイズは次の要素によって異なります。
  - サーバー・スキーマの中の属性の数
  - サーバー上の項目の数
  - サーバーに格納する情報の種類

  たとえば、デフォルトのディレクトリー・サービスのスキーマを使用する記憶域には、約 10MB の記憶域の空きが必要です。デフォルトのスキーマを使用していて、一般的な従業員情報を 1000 項目格納しているディレクトリーには、約 30 MB の記憶域が必要です。この数値は、実際に使用する属性によって異なります。また、写真などの大きいオブジェクトをディレクトリーに格納した場合は、この数値は大幅に増加することがあります。

- **使用するセキュリティー手段を決定する。**ディレクトリー・サービスは、Secure Sockets Layer (SSL) とディジタル認証、および Translation Layer Security (TLS) を使用した通信セキュリティーをサポートしています。 V5R1 からは、Kerberos 認証もサポートされています。
- ディレクトリー・サービスでは、アクセス制御リスト (ACL) を使って、ディレクトリー・オブジェクトへのアクセスを制御することもできます。ディレクトリーを保護するには、OS/400 セキュリティー監査も使用できます。

ディレクトリー・サービスの旧リリースを V5R2 にマイグレーションする

V5R2 の OS/400 では、ディレクトリー・サービスに新しい機能が追加されました。これに伴い、LDAP ディレクトリー・サーバーと iSeries ナビゲーターのグラフィカル・ユーザー・インターフェース (GUI) の仕様が一部変更されています。 GUI の新しい機能を利用できるようにするには、 iSeries サーバーに TCP/IP で接続できる PC に iSeries ナビゲーターをインストールする必要があります。 iSeries ナビゲーターは、iSeries Access for Windows のコンポーネントです。旧バージョンの iSeries ナビゲーターをインストールしてある場合は、 V5R2 にアップグレードするようにしてください。

V5R2 の OS/400 では、V4R5 と V5R1 からのアップグレードがサポートされています。 V5R2 の OS/400 にアップグレードする場合は、 LDAP ディレクトリー・データ・ファイルとディレクトリー・スキーマ・ファイルはいずれも、 V5R2 の形式に準拠するように自動的にマイグレーションされます。ディレクトリー・サービス LDAP サーバーを V4R3 または V4R4 の OS/400 で実行していて、そのサーバーを V5R2 へマイグレーションすることを望む場合は、 追加のマイグレーション・タスクを実行する必要があります。

V5R2 の OS/400 にアップグレードする場合は、マイグレーションに関するいくつかの注意点があります。

- V5R2 にアップグレードする場合は、ディレクトリー・サービスによって、スキーマ・ファイルが自動的に V5R2 にマイグレーションされ、古いスキーマ・ファイルは削除されます。しかし、スキーマ・ファイルを削除または名前変更すると、ディレクトリー・サービスはそれらをマイグレーションすることができません。その場合、エラーが出されるか、または ディレクトリー・サービスはすでにそのファイルがマイグレーションされたと見なします。
- ディレクトリー・サービスは、初めてサーバーを始動するか LDIF ファイルをインポートするとき、ディレクトリー・データを V5R2 形式にマイグレーションします。このマイグレーションが完了するのに必要な十分の時間を計画してください。 V4R4 以前のリリースから V5R2 にアップグレードする場合は、ディレクトリー・データが、 V5R2 では以前のほぼ 2 倍の記憶域を必要とすることにもご注意ください。これは、V4R4 以前のバージョンのディレクトリー・サービスでは、IA5 文字セットだけがサポートされ、 CCSID 37 (単一バイト形式) でデータが保管されていたためです。ディレクトリー・サービスでは、完全 ISO 10646 文字セットがサポートされるようになっています。

  V5R2 にアップグレードした後、新しいデータをインポートする前に、一度サーバーを始動して既存のデータをマイグレーションする必要があります。十分な権限がないのにサーバーを一度始動する前にデータのインポートを試行すると、インポートは失敗する場合があります。
- V4R4 以前のディレクトリー・サービスは、タイム・スタンプの項目を作成するときに、時間帯を考慮に入れませんでした。 V4R5 以降では、ディレクトリーに対するすべての追加および変更で時間帯が使用されています。したがって、V4R4 以前のリリースから V5R2 にアップグレードすると、ディレクトリー・サービスは既存の `createtimestamp` および `modifytimestamp` 属性を、正しい時間帯を反映するように調整します。このことは、ディレクトリーに保管されているタイム・スタンプから、 iSeries で現在定義されている時間帯を引くことにより行われます。現行の時間帯が、項目が最初に作成または変更されたときに活動状態だった時間帯と異なる場合、新しいタイム・スタンプ値は元の時間帯を反映しないので注意してください。

| • マイグレーション後は、TCP/IP の開始時に、 LDAP ディレクトリー・サーバーが自動的に開始するようになります。ディレクトリー・サーバーの自動開始を望まない場合は、 iSeries ナビゲーターを使用して、設定を変更してください。

V4R3 または V4R4 のディレクトリー・サービスを V5R2 にマイグレーションする

V5R2 の OS/400 では、 V4R3 からの直接的なアップグレードがサポートされていません。 V4R3 または V4R4 のディレクトリー・サービス LDAP サーバーを V5R2 にマイグレーションするには、以下のいずれかの手順を実行します。

- V4R3 または V4R4 から中間リリースへ OS/400 をスリップ・インストールする
- データベース・ライブラリーを保存してから、 OS/400 を V4R3 または V4R4 から V5R2 にスクラッチ・インストールする

V4R3 または V4R4 から中間リリースへ OS/400 をスリップ・インストールする

OS/400 の V4R3 および V4R4 から V5R2 へのアップグレードはサポートされていませんが、以下のアップグレードはサポートされています。

- V4R3 および V4R4 から V4R5 へのアップグレード
- V4R4 および V4R5 から V5R1 へのアップグレード
- V4R5 および V5R1 から V5R2 へのアップグレード

ディレクトリー・サービス サーバーをマイグレーションするための 1 つの方法は、まず中間リリース (V4R5 または V5R1) にアップグレードしてから、 V5R2 にアップグレードするという方法です。 OS/400 のインストール手順の詳細については、 ソフトウェアの導入 を参照してください。マイグレーションを実行するための一般的な手順は、次のとおりです。

1. /QIBM/UserData/OS400/DirSrv ディレクトリーのスキーマ・ファイルに加えた変更を記録する。スキーマ・ファイルが自動的にマイグレーションされます。
2. V4R4 または V4R3 の場合は、 OS/400 の V4R5 または V5R1 をスリップ・インストールする。
3. OS/400 の V5R2 にスリップ・インストールする。
4. ディレクトリー・サービス・サーバーをまだ開始していなければ、ここで開始する。
5. ディレクトリー管理ツールを使用し、ステップ 1 で記録したユーザー変更に基づいて、スキーマ・ファイルを編集する。
6. ディレクトリー・サービス・サーバーを再び開始する。

データベース・ライブラリーを保存してから、 OS/400 を V4R3 または V4R4 から V5R2 にスクラッチ・インストールする

ディレクトリー・サービス・サーバーをマイグレーションするもう 1 つの方法は、ディレクトリー・サービスが V4R3 または V4R4 で使用していたデータベース・ライブラリーを保存してから、 V5R2 のスクラッチ・インストールの後で、ライブラリー・ライブラリーを復元するということです。この場合は、中間リリースをインストールする手間が省けます。しかし、サーバーの設定はマイグレーションされないので、サーバーを再構成する必要があります。 OS/400 のインストール手順の詳細については、 ソフトウェアの導入 を参照してください。マイグレーションを実行するための一般的な手順は、次のとおりです。

1. /QIBM/UserData/OS400/DirSrv ディレクトリーのスキーマ・ファイルに加えた変更を記録する。スキーマ・ファイルは、自動的にマイグレーションされないので、変更点を継続したい場合は、手作業で再び変更を加える必要があります。
2. ディレクトリー・サービス・サーバーのプロパティーで、データベース・ライブラリー名などのさまざまな構成設定を記録する。
3. ディレクトリー・サービス・サーバーの構成で指定されているデータベース・ライブラリーを保存する。
4. 発行機能の構成を記録する。
5. システムを V5R2 の OS/400 にスクラッチ・インストールする。
6. EZ-Setup を使用して、ディレクトリー・サービス・サーバーを設定する。
7. ステップ 3 で保存したデータベース・ライブラリーを復元する。
8. ディレクトリー管理ツールを使用し、ステップ 1 で記録したユーザー変更に基づいて、スキーマ・ファイルを変更する。
9. iSeries ナビゲーターを使用して、ディレクトリー・サービスの設定をやり直す。いったん保存して復元したデータベース・ライブラリーを指定する。
10. iSeries ナビゲーターを使用して、発行機能を再構成する。
11. ディレクトリー・サービス・サーバーを再び開始する。

アップグレードの注意点

V4R3 から新しいリリースへアップグレードする場合には、以下の点に留意してください。

- **キー・リング・ファイルからキー・データベースへのマイグレーション**

  V3R2 の Client Access では、 LDAP ディレクトリー・サーバーに Secure Sockets Layer (SSL) を確立するときに、キー・リング・ファイルを使用していました。 iSeries Access for Windows では、キー・データベースという証明書登録リストを使用して SSL を接続します。旧バージョンの LDAP ディレクトリー・サーバーでキー・リング・ファイルを使用していた場合、 SSL を新バージョンでも引き続き使用するためには、キー・リング・ファイルをキー・データベースに変換する必要があります。 LDAP ディレクトリー・サーバーに SSL を初めて接続するときに、 iSeries ナビゲーターはこの変更を行うかどうかを問い合わせてきます。キーを変換するよう指定すると、キー・データベースの情報を指定するよう求められます。情報を入力すると、変換が実行されます。

  V4R3 の LDAP ディレクトリー・サーバーでは、専用の SSL 接続を使用するときにもキー・リング・ファイルを使用していました。 V4R4 以降の LDAP ディレクトリー・サーバーでは、システム証明書登録リストを使用します。 V4R3 のサーバーで SSL を使用するよう設定していた場合、キー・リング・ファイルの内容は証明書登録リストにマイグレーションされます。

- **2 つのストリーム・ファイルが削除されました。**

  V4R3 の ディレクトリー・サービスにより使用されていた以下のストリーム・ファイルが不要になりました。これらのストリーム・ファイルについては、新しいリリースをインストールすると自動的に削除されます。

  ```
  /QIBM/ProdData/OS400/DirSrv/qgldcert.kyr
  /QIBM/ProdData/OS400/DirSrv/qgldcert.sth
  ```

  これらのファイルについては何も行う必要はありません。以上の理由により、これらのファイルがシステムからなくなっていても何の問題もありません。

また、他のリリースから現行のリリースへのアップグレードすることに関連する問題が他にもあるかもしれませんのでご注意ください。

ディレクトリー・サービスをインストールして構成する

ディレクトリー・サービス (LDAP) は、OS/400 をインストールすると自動的にインストールされます。ディレクトリー・サーバーには、 TCP/IP の開始時にディレクトリー・サーバーを自動的に開始するデフォルト構成が組み込まれています。ディレクトリー・サーバーは、OS/400 からディレクトリー・サーバーへのコンピューター情報の発行も開始します。 LDAP ディレクトリー・サーバーの設定をカスタマイズするには、 ディレクトリー・サービス構成ウィザードを実行します。このウィザードを使用するには、特殊権限 *ALLOBJ と *IOSYSCFG が必要になります。

V5R1 からは、ディレクトリー・サービスは基本オペレーティング・システムに統合され、 V5R2 からは、オプション 32 は使用不可になります。

LDAP ディレクトリー・サーバーを構成する

システムが別の LDAP サーバーに情報を発行するような構成になっておらず、なおかつ TCP/IP DNS サーバーに認識されている LDAP サーバーが存在していない場合は、ディレクトリー・サービスが自動的に限定的なデフォルト構成でインストールされるようになりました。ディレクトリー・サービスには、それぞれの必要に合わせて LDAP ディレクトリー・サーバーを設定するためのウィザードが用意されています。このウィザードは、EZ-Setup の一部として実行することもできますし、後ほど iSeries ナビゲーターから実行することもできます。このウィザードは、ディレクトリー・サーバーを最初に構成するときや、ディレクトリー・サーバーを再構成するときに使用します。

注: ウィザードを使ってディレクトリー・サーバーを再構成する場合は、最初から構成し直すことになります。つまり、元の構成は、変更されるのではなく削除されます。ただし、ディレクトリーのデータは削除されず、インストール時に選択したライブラリー (デフォルトでは QUSRDIRDB) に残ります。変更ログも (デフォルトでは QUSRDIRCL ライブラリーに) そのまま残ります。

最初から完全に構成し直したい場合には、ウィザードを開始する前に、それら 2 つのライブラリーを消去してください。

ディレクトリー・サーバーの構成を変更したいが、完全には消去したくない場合、**「ディレクトリー」**を右クリックして、**「プロパティー」**を選択します。この方法では、元の構成は削除されません。

サーバーを設定するには、特殊権限 *ALLOBJ および *IOSYSCFG を持っている必要があります。 OS/400 セキュリティー監査を設定する場合は、 *AUDIT 特殊権限も必要になります。

ディレクトリー・サービスの構成ウィザードを開始するための手順は、次のとおりです。

1. iSeries ナビゲーターで**「ネットワーク」**を展開する。
2. **「サーバー」**を展開する。
3. **「TCP/IP」**をクリックする。
4. **「ディレクトリー」**を右クリックし、**「構成」**を選択する。

注: すでにディレクトリー・サーバーの構成が済んでいる場合は、**「構成」**ではなく**「再構成」**をクリックしてください。

「ディレクトリー・サーバーの構成」ウィザードの指示に従って、 LDAP ディレクトリー・サーバーを構成してください。

注: また、ディレクトリー・データを保管するこのライブラリーは、システム補助記憶域プール (ASP) ではなく、ユーザー ASP に入れておく方が便利なことがあります。ただし、このライブラリーは独立 ASP には保管できません。独立 ASP の中にライブラリーを持つサーバーを構成、再構成、または開始しようとすると、それは失敗します。

| ウィザードが終了すると、LDAP ディレクトリー・サーバーに基本構成が完了します。システムで Lotus® Domino を実行している場合は、ポート 389 (LDAP サーバー用のデフォルト・ポート) が Domino の LDAP 機能によってすでに使用されている可能性があります。以下のいずれかを実行する必要があります。

- Lotus Domino が使用するポートを変更する
- ディレクトリー・サービスが使用するポートを変更する
- 特定の IP アドレスを使用する

この時点でサーバーを開始することができます。ただし、サーバーを開始する前に、次のいくつかまたはすべての操作を実行することを検討してください。

- サーバーにデータをインポートする
- Secure Sockets Layer (SSL) セキュリティーを使用可能にする
- Kerberos 認証を使用可能にする
- 参照を構成する

LDAP ディレクトリー・サーバーで SSL を使用可能にする

| システムにディジタル証明書マネージャーをインストールしてある場合は、 Secure Sockets Layer (SSL) セキュリティーを使用して、 LDAP ディレクトリー・サーバーへのアクセスを保護することができます。ディレクトリー・サーバーで SSL を使用できるようにする作業を行うにあたっては、ディレクトリー・サービスで SSL を使用する方法についての概要を参考にご覧ください。

iSeries ナビゲーターから LDAP ディレクトリー・サーバーを管理するときに SSL 接続を使用する場合、または Windows の LDAP クライアントで SSL を使用する場合には、いずれかのクライアント暗号化製品 (5722CE2 または 5722CE3) を PC にインストールしておく必要があります。

| LDAP サーバーで SSL を使用できるようにするには、ディジタル証明書マネージャー・インターフェースを使用します。ディジタル証明書マネージャーは、 iSeries ナビゲーターの**「インターネット」**フォルダーまたはディレクトリー・サーバーの**「プロパティー」**ダイアログ・ボックスの**「ネットワーク」**ページから立ち上げることができます。

| **「ネットワーク」**ページからディジタル証明書インターフェースを立ち上げるには、以下の手順に従います。

1. iSeries ナビゲーターで**「ネットワーク」**を展開する。
2. **「サーバー」**を展開する。
3. **「TCP/IP」**をクリックする。
4. **「ディレクトリー」**を右クリックし、**「プロパティー」**を選択する。
5. **「ネットワーク」**タブをクリックする。
6. **「ディジタル証明書マネージャー」**をクリックする。

   デフォルトのインターネット・ブラウザーでディジタル証明書マネージャーが立ち上がります。

ディレクトリー・サーバーにディジタル証明書を割り当てるために行う必要がある特定のステップについては、 『LDAP ディレクトリー・サーバーの安全性を高める』を参照してください。

SSL を使用できるようになると、LDAP ディレクトリー・サーバーで使用するポートを変更することにより、安全性の高い接続を確立できるようになります。

LDAP ディレクトリー・サーバーで Kerberos 認証を使用可能にする

システムにネットワーク認証サービスを設定した場合は、 LDAP ディレクトリー・サーバーで Kerberos 認証を使用するための設定ができます。ディレクトリー・サーバーで Kerberos を使用可能にする前に、ディレクトリー・サービスで Kerberos を使用する方法の概要を読んでおくと役に立ちます。

Kerberos 認証を使用可能にするための手順は、次のとおりです。

1. iSeries ナビゲーターで**「ネットワーク」**を展開する。
2. **「サーバー」**を展開する。
3. **「TCP/IP」**をクリックする。
4. **「ディレクトリー」**を右クリックし、**「プロパティー」**を選択する。
5. **「Kerberos」**タブをクリックする。
6. **「Kerberos 認証を使用可能にする (Enable Kerberos authentication)」**をチェックする。
7. それぞれの状況に合わせて、**「Kerberos」**ページの他の設定値を指定する。各フィールドの説明については、そのページのオンライン・ヘルプを参照してください。

ディレクトリー・サービスのデフォルト構成

LDAP ディレクトリー・サーバーは、OS/400 をインストールすると自動的にインストールされます。このときには、デフォルト構成もインストールされます。ディレクトリー・サーバーは、以下の条件がすべて揃った場合に、デフォルト構成を使用します。

- 管理者がディレクトリー・サービス構成ウィザードを実行していないか、プロパティー・ページでディレクトリー設定を変更していない場合。
- ディレクトリー・サービスの発行機能が設定されていない場合。
- LDAP ディレクトリー・サーバーが LDAP DNS 情報を検出できない場合。

LDAP ディレクトリー・サーバーがデフォルト構成を使用すると、以下のような処理が行われます。

- TCP/IP の開始時に、LDAP ディレクトリー・サーバーが自動的に開始します。
- システムがデフォルトの管理者 cn=Administrator を作成します。さらに、内部で使用されるパスワードも生成されます。実際に管理者パスワードを使用しなければならなくなった場合は、ディレクトリー・サービスのプロパティー・ページで新しいパスワードを設定できます。
- システムの IP 名に基づいて、デフォルトの接尾部が作成されます。システム・オブジェクトの接尾部も、このシステム名に基づいて作成されます。たとえば、システム IP 名が mary.acme.com であれば、接尾部は dc=mary,dc=acme,dc=com になります。
- LDAP ディレクトリー・サーバーが、デフォルトのデータ・ライブラリー QUSRDIRDB を使用します。そのライブラリーは、システム ASP 内に作成されます。
- サーバーが、セキュアでない通信のためにポート 389 を使用します。 LDAP 用のディジタル証明書が設定されていない場合は、 Secure Sockets Layer (SSL) が使用可能になり、セキュアな通信用にポート 636 が使用されます。

ディレクトリー・サービスの発行機能については、以下のようなデフォルト設定になります。

- システムは、ローカル LDAP ディレクトリー・サーバーに対して情報を発行します。
- 発行機能は、SSL を使用しません。
- 発行機能は、デフォルト接尾部の下でコンテナーを使用します。
- ディレクトリー・サーバーの認証のために、 OS/400 は、cn=Administrator ID とシステム生成パスワードを使用します。
- システムは、システム情報だけを発行します。

IBM SecureWay ディレクトリー管理ツール

IBM SecureWay ディレクトリー管理ツール (DMT) は、 LDAP ディレクトリーの内容を管理するためのグラフィカル・ユーザー・インターフェースを提供します。 DMT を使って実行できる作業には、以下のものがあります。

- ディレクトリー・スキーマのブラウズ
- オブジェクト・クラスの追加、編集、および削除
- 属性の追加、編集、および削除
- ディレクトリー・ツリーのブラウズおよび検索
- 項目の追加、編集、表示、および削除
- 項目 RDN の編集
- ACL の管理

DMT は、ディレクトリー・サービスに組み込まれている Windows LDAP クライアントの一部です。クライアントは、統合ファイル・システム・ディレクトリーに入っています。

DMT を含む Windows LDAP クライアントを PC にインストールするには、以下のことを行ってください。

1. iSeries ナビゲーターで、**「ファイル・システム」**を展開する。
2. **「ファイル共用」**を展開する。
3. **「Qdirsrv」**をダブルクリックする。
4. **「UserTools」**をダブルクリックする。
5. **「Windows」**をダブルクリックする。
6. **setup.exe** をダブルクリックして、DMT のインストールを開始する。画面の指示に従って、インストールを完了します。

IBM SecureWay ディレクトリー管理ツール (DMT) に関する資料は、 `dparent.htm` ファイルにあります。このファイルは、クライアントのインストール時に、 PC の IBM SecureWay Directory フォルダーにコピーされます。

第 4 章 LDAP ディレクトリー・サーバーを管理する

LDAP ディレクトリー・サーバーを管理するには、以下の権限セットを持っている必要があります。

- サーバーを構成したり、サーバー構成を変更したりする場合: すべてのオブジェクト (*ALLOBJ) 特殊特権、および入出力システム構成 (*IOSYSCFG) 特殊特権
- サーバーを開始または停止する場合: ジョブ制御 (*JOBCTL) 権限、および「TCP/IP の終了 (ENDTCP)」、「TCP/IP の開始 (STRTCP)」、「TCP/IP サーバーの開始 (STRTCPSVR)」、「TCP/IP サーバーの終了 (ENDTCPSVR)」の各コマンドに対するオブジェクト権限
- ディレクトリー・サーバーの監査動作を設定する場合: 監査 (*AUDIT) 特殊特権
- サーバーのジョブ・ログを表示する場合: スプール制御 (*SPLCTL) 特殊特権

ディレクトリー・オブジェクト (アクセス制御リスト、オブジェクト所有権、およびレプリカを含む) を管理するには、管理者 DN または適正な LDAP 権限を持つその他の DN を使用して、そのディレクトリーに接続してください。権限統合を使用している場合は、 ディレクトリー・サービスの管理者ファンクション ID への権限を持つプロジェクト・ユーザーも管理者になれます。

ディレクトリー・サーバーの管理には、次の作業が含まれます。

- 『LDAP ディレクトリー・サーバーを開始する』
- 20 ページの『LDAP ディレクトリー・サーバーを停止する』
- 20 ページの『ディレクトリー・サーバーの状況を検査する』
- 21 ページの『LDAP ディレクトリー・サーバーのジョブを検査する』
- 21 ページの『イベント通知を使用可能にする』
- 21 ページの『トランザクション設定値を指定する』
- 22 ページの『ポートまたは IP アドレスを変更する』
- 22 ページの『LDAP ディレクトリー・データをシステム間で移動する』
- 30 ページの『ディレクトリー参照用のサーバーを指定する』
- 31 ページの『LDAP ディレクトリー・サーバーに接尾部を追加する』
- 31 ページの『ディレクトリー・サーバーから接尾部を削除する』
- 31 ページの『ディレクトリー・サービス情報の保管と復元』
- 32 ページの『ディレクトリー・データの所有権とアクセス権を管理する』
- 34 ページの『LDAP ディレクトリーに対するアクセスと変更をトラッキングする』
- 34 ページの『ディレクトリー・サーバーのオブジェクト監査を使用可能にする』
- 35 ページの『LDAP ディレクトリー・サーバーのパフォーマンスを調整する』

LDAP ディレクトリー・サーバーを開始する

LDAP ディレクトリー・サーバーを開始するには、次のようにしてください。

1. iSeries ナビゲーターで**「ネットワーク」**を展開する。
2. **「サーバー」**を展開する。
3. **「TCP/IP」**をクリックする。
4. **「ディレクトリー」**を右クリックし、**「開始」**を選択する。

サーバーの速度および使用可能なメモリーの量によっては、ディレクトリー・サーバーの開始までに数分かかることがあります。ディレクトリー・サーバーを初めて開始するときには、サーバーが新しいファイルを作成しなければならないため、通常より数分多く時間がかかることがあります。 同様に、旧バージョンのディレクトリー・サービスからアップグレードした後、ディレクトリー・サーバーをはじめ

て開始するときには、サーバーがファイルをマイグレーションする必要があるため、通常より数分多く時間がかかることがあります。定期的にサーバーの状況をチェックして、サーバーがすでに開始されているかどうかを確認することができます。

注: コマンド STRTCPSVR *DIRSRV を入力することにより、 5250 セッションからディレクトリー・サーバーを開始することもできます。

さらに、TCP/IP の開始時にディレクトリー・サーバーが開始されるように設定してある場合は、STRTCP コマンドでもサーバーを開始できます。

LDAP ディレクトリー・サーバーを停止する

ディレクトリー・サーバーを停止すると、その停止時にサーバーを使用しているすべてのアプリケーションに影響します。これには、EIM 操作用に現在ディレクトリー・サーバーを使用している、エンタープライズ識別マッピング (EIM) アプリケーションが含まれます。すべてのアプリケーションはディレクトリー・サーバーから切断されますが、サーバーへの再接続を試みることはできます。

LDAP ディレクトリー・サーバーを停止するには、次のようにしてください。

1. iSeries ナビゲーターで**「ネットワーク」**を展開する。
2. **「サーバー」**を展開する。
3. **「TCP/IP」**をクリックする。
4. **「ディレクトリー」**を右クリックし、**「停止」**を選択する。

   システムの速度、サーバーの活動量、および使用可能なメモリーの量によっては、ディレクトリー・サーバーの停止までに数分かかることがあります。定期的にサーバーの状況をチェックして、サーバーがすでに停止しているかどうかを確認することができます。

注: コマンド ENDTCPSVR *DIRSRV、ENDTCPSVR *ALL、または ENDTCP を入力することにより、 5250 セッションからディレクトリー・サーバーを停止することもできます。 ENDTCPSVR *ALL および ENDTCP は、システムで実行されている他の TCP/IP サーバーにも影響を与えます。 ENDTCP では TCP/IP 自体も終了します。

ディレクトリー・サーバーの状況を検査する

iSeries ナビゲーターは、右フレームの**「状況」**列に、ディレクトリー・サーバーの状況を表示します。

ディレクトリー・サーバーの状況を検査するには、次のようにしてください。

1. iSeries ナビゲーターで**「ネットワーク」**を展開する。
2. **「サーバー」**を展開する。
3. **「TCP/IP」**をクリックする。 iSeries ナビゲーターは、ディレクトリー・サーバーも含めてすべての TCP/IP サーバーの状況を、**「状況」**列に表示します。サーバーの状況を更新するには、**「表示」**メニューをクリックし、**「最新表示」**を選択します。
4. ディレクトリー・サーバーの状況に関する詳細情報を表示するには、**「ディレクトリー」**を右クリックし、**「状況」**を選択する。活動状態の接続数のほか、過去および現在の活動レベルなどの情報が表示されます。

   このオプションを使って状況を表示すると、詳細な情報が戻るだけでなく、時間の節約にもなります。他の TCP/IP サーバーの状況を検査するために余分な時間をかけることなく、ディレクトリー・サーバーの状況を最新表示することができます。

LDAP ディレクトリー・サーバーのジョブを検査する

必要に応じて、LDAP ディレクトリー・サーバーの特定のジョブを監視することができます。サーバーのジョブをチェックするには、以下の手順に従います。

1. iSeries ナビゲーターで**「ネットワーク」**を展開する。
2. **「サーバー」**を展開する。
3. **「TCP/IP」**をクリックする。
4. **「ディレクトリー」**を右クリックしてから、**「サーバーのジョブ (Server Jobs)」**を選択する。

イベント通知を使用可能にする

| ディレクトリー・サービスはイベント通知をサポートしています。イベント通知機能では、ディレクトリーに何かが追加されるといった指定のイベントが発生したときに、クライアントが LDAP サーバーから通知を受けられるように登録をすることになります。

| サーバーでイベント通知を使用可能にするための手順は、次のとおりです。

1. iSeries ナビゲーターで**「ネットワーク」**を展開する。
2. **「サーバー」**を展開する。
3. **「TCP/IP」**をクリックする。
4. **「ディレクトリー」**を右クリックし、**「プロパティー」**を選択する。
5. **「イベント (Events)」**をクリックする。
6. **「イベント通知のためにクライアントを登録 (Allow clients to register for event notification)」**を選択する。

1 つの接続についての最大登録数やサーバー全体についての最大登録数も指定できます。

イベント通知の詳細については、 IBM SecureWay Directory Version 3.2: Client SDK Programming Reference  の『Appendix C: Event Notification』を参照してください。

トランザクション設定値を指定する

| ディレクトリー・サービスはトランザクションをサポートしています。トランザクションとは、 1 つの単位として扱われる LDAP ディレクトリー操作の集合を指します。詳細については、 42 ページの『トランザクション』を参照してください。

サーバーのトランザクション設定値を構成するための手順は、次のとおりです。

1. iSeries ナビゲーターで**「ネットワーク」**を展開する。
2. **「サーバー」**を展開する。
3. **「TCP/IP」**をクリックする。
4. **「ディレクトリー」**を右クリックし、**「プロパティー」**を選択する。
5. **「トランザクション (Transactions)」**をクリックする。
6. トランザクション設定値を指定する。

注: トランザクション設定値は、 LDAP サーバーのパフォーマンスに影響を与えるので、いろいろな値を試してみてください。

ポートまたは IP アドレスを変更する

ディレクトリー・サービスにより使用可能にされた LDAP ディレクトリー・サーバーでは、次に示すデフォルト・ポートが使用されます。
- 安全性の低い接続の場合は 389
- 安全性の高い接続の場合は 636 (ディジタル認証マネージャーにより、ディレクトリー・サービスがセキュア・ポートを使用できるアプリケーションとなっている場合)

注: デフォルトでは、ローカル・システムで定義されているすべての IP アドレスがサーバーにバインドされます。

これらのポートをすでに他のアプリケーション用に使用している場合は、ディレクトリー・サービスに別のポートを割り当てるか、またはアプリケーションが特定の IP アドレスへのバインドをサポートしている場合は、 2 つのサーバーに対して異なる IP アドレスを使用することができます。

iSeries ディレクトリー・サービス LDAP サーバーと競合している Domino LDAP サーバーの例について、「Domino LDAP とディレクトリー・サービスを同じ iSeries 上にホストする」を参照してください。

LDAP ディレクトリー・サーバーが使用するポートを変更するには、次のようにしてください。
1. iSeries ナビゲーターで**「ネットワーク」**を展開する。
2. **「サーバー」**を展開する。
3. **「TCP/IP」**をクリックする。
4. **「ディレクトリー」**を右クリックし、**「プロパティー」**を選択する。
5. **「ネットワーク」**タブをクリックする。
6. 使用するポート番号を入力し、**「OK」**をクリックする。

ディレクトリー・サーバーが接続を受信する IP アドレスを変更するには、以下のステップを実行します。
1. iSeries ナビゲーターで**「ネットワーク」**を展開する。
2. **「サーバー」**を展開する。
3. **「TCP/IP」**をクリックする。
4. **「ディレクトリー」**を右クリックし、**「プロパティー」**を選択する。
5. **「ネットワーク」**タブをクリックする。
6. **「IP アドレス」**ボタンをクリックする。
7. **「選択した IP アドレスを使用する (Use selected IP addresses)」**を選択し、接続を受け入れるときに使用する、サーバーの IP アドレスを選択する。

LDAP ディレクトリー・データをシステム間で移動する

ディレクトリー・サービス LDAP サーバーは、他のサーバーから独立して実行することができます。しかし、このサーバーと他のサーバーを協働させる方が便利な場合があります。たとえば次のような場合です。
- 23 ページの『LDIF ファイルをインポートする』
- 23 ページの『LDIF ファイルをエクスポートする』
- 23 ページの『ディレクトリー・サーバーの新しいレプリカを設定する』
- 28 ページの『情報をディレクトリー・サーバーに発行する』

LDIF ファイルをインポートする

LDAP データ交換形式 (LDIF) ファイルを使用することにより、異なる LDAP ディレクトリー・サーバー間で情報を転送することができます。この手順を開始する前に、LDIF ファイルをストリーム・ファイルとして iSeries サーバーに転送してください。

LDIF ファイルを LDAP ディレクトリー・サーバーにインポートするには、次のようにしてください。

1. ディレクトリー・サーバーが開始されている場合は、ディレクトリー・サーバーを停止する。ディレクトリー・サーバーを停止するための情報については、 20 ページの『LDAP ディレクトリー・サーバーを停止する』を参照してください。
2. iSeries ナビゲーターで**「ネットワーク」**を展開する。
3. **「サーバー」**を展開する。
4. **「TCP/IP」**をクリックする。
5. **「ディレクトリー」**を右クリックし、**「ツール」**を選択する。次に**「ファイルのインポート」**を選択する。

注: ldapadd ユーティリティーを使用して、 LDIF ファイルをインポートすることもできます。

LDIF ファイルをエクスポートする

LDAP データ交換形式 (LDIF) ファイルを使用すると、 LDAP ディレクトリー・サーバー間で情報を交換することができます。詳細については、 39 ページの『LDAP データ交換形式』を参照してください。
LDAP ディレクトリーの全体または一部を、LDIF ファイルにエクスポートできます。

ディレクトリー・サーバーから LDIF ファイルをエクスポートするための手順は、次のとおりです。

1. iSeries ナビゲーターで**「ネットワーク」**を展開する。
2. **「サーバー」**を展開する。
3. **「TCP/IP」**をクリックする。
4. **「ディレクトリー」**を右クリックし、**「ツール」**を選択する。次に**「ファイルのエクスポート」**を選択する。

   注: LDIF ファイルのエクスポート先を指定しなかった場合は、 OS/400 ユーザー・プロファイルに指定されたデフォルト・ディレクトリーに保存されます。デフォルト・ディレクトリーを変更していなければ、デフォルト・ディレクトリーはルート・ディレクトリーです。

注:

1. ディレクトリー・データへの無許可アクセスを防ぐために、必ず LDIF ファイルに対する権限を設定してください。そのためには、iSeries ナビゲーターで該当ファイルを右クリックし、**「許可」**を選択します。
2. ldapsearch ユーティリティーを使用して、 LDIF ファイルの一部または全部を作成することもできます (このユーティリティーについては、 58 ページの『ldapsearch ユーティリティー』を参照のこと)。 -L オプションを使用して、出力をファイルに転送します。

ディレクトリー・サーバーの新しいレプリカを設定する

LDAP ディレクトリー・サーバーのレプリカを、他の iSeries サーバーのディレクトリー・サーバーに設定することができます。複製時には、ディレクトリー・サービスは LDAP バージョン 3 の標準プロトコルを使用します。

注:

1. LDAP バージョン 3 と LDAP バージョン 2 サーバーの間では複製を行うことはできません。そのため、複製先のシステムは、複製元のシステムと同じバージョンの LDAP を使用していなければなりま

せん。 OS/400 の V4R3 と V4R4 は、 LDAP バージョン 2 をサポートしており、それ以降のリリースは、LDAP バージョン 3 をサポートしています。

2. ディレクトリー・サービスのディレクトリーは、他のプラットフォームの IBM SecureWay V3.2 以降のサーバーに複製することもできます。そのためには、 OS/400 ディレクトリー・サーバーで 3.2 ACI メカニズムを使用するような設定にしなければなりません。サーバーの複製処理中に問題が発生した場合は、複製処理が停止します。そのような場合のレプリカは、完全ではありません。

ディレクトリー・サーバーの新しいレプリカを設定するには、次のようにしてください。

1. マスター・サーバーとレプリカ・サーバーの両方の設定がまだ済んでいない場合は、ここで設定を行う。

   注: 両方のサーバー間でスキーマと接尾部が一致していることを確認してください。
2. マスター・サーバーを停止する。
3. (オプション) 初期複製用の LDAP データを設定する。マスター・サーバーからレプリカ・サーバーに転送する必要がある初期データがない場合は、このステップは省略してもかまいません。
4. (オプション) LDAP データをマスター・サーバーに移動する。レプリカ・サーバーに次のどちらかの条件が該当する場合は、このステップは省略してください。
   - 新しい LDAP ディレクトリー・サーバーである。
   - 引き続き保持しておく必要のあるデータが含まれていない。
5. 新しいレプリカ・サーバーを設定する。
6. 新しいレプリカを持つようにマスター・サーバーを設定する。
7. マスター・サーバーが更新可能であることを確認する。
   a. iSeries ナビゲーターで、マスター・ディレクトリー・サーバーが実行されるシステムを展開する。
   b. **「ネットワーク」**を展開する。
   c. **「サーバー」**を展開する。
   d. **「TCP/IP」**をクリックする。
   e. **「ディレクトリー」**を右クリックし、**「プロパティー」**を選択する。
   f. **「ディレクトリー更新の許可」**にチェック・マークが付いていない場合は、チェック・マークを付ける。

注: 上記の説明では、マスター・サーバーとレプリカ・サーバーの両方が、同じ PC 上の iSeries ナビゲーターから管理するシステムにあることが前提になっています。これらのシステムを別々の PC から管理している場合は、 2 台の PC 間を移動しながらこの作業をすることができます。マスター・サーバーまたはレプリカ・サーバーのどちらかが OS/400 以外の IBM オペレーティング・システムで実行されている場合は、そのオペレーティング・システム用のドキュメンテーションを参照しながら、サーバーの設定を行ってください。

初期複製用の LDAP データを設定する

マスター LDAP ディレクトリー・サーバーの既存データを新しいレプリカ・サーバーに追加することができます。このことを行うには、まず最初にディレクトリーを LDIF ファイルにエクスポートする必要があります。 LDIF ファイルをエクスポートしている間は、マスター・サーバーが更新されないようにする必要があります。こうするために、次のどちらかの方法をとることができます。

- LDAP ディレクトリー・サーバーを停止する。ディレクトリー内のデータの量によっては、これを行うために時間を延長してサーバーを停止しておくことが必要になる場合があります。
- 更新が許可されないようサーバーのプロパティーを変更する。これにより、サーバーは LDIF ファイルがエクスポートされている間、検索要求に応答し続けることができます。このオプションを採用するには、次のようにしてください。
  1. iSeries ナビゲーターで、マスター・ディレクトリー・サーバーが実行されるシステムを展開する。
  2. **「ネットワーク」**を展開する。

3. **「サーバー」**を展開する。
4. **「TCP/IP」**をクリックする。
5. **「ディレクトリー」**を右クリックし、**「プロパティー」**を選択する。
6. **「ディレクトリー更新の許可」**にチェック・マークが付いている場合は、チェック・マークを外す。これで、複製が完全に設定されるまでディレクトリー更新ができなくなります。
7. **「OK」**をクリックする。
8. LDAP ディレクトリー・サーバーを停止してから、 再始動します。

サーバーを停止するか、ディレクトリーを更新できないようサーバーのプロパティーを変更し終えたら、以下の作業を行います。

1. ディレクトリーを LDIF ファイルにエクスポートする。
2. LDIF ファイルを、レプリカ・サーバーが実行されるシステムに転送する。

LDIF ファイルを、レプリカ・サーバーが実行されるシステムに転送し終わったら、データをレプリカ・サーバーにインポートする必要があります。

1. iSeries ナビゲーターで、レプリカ・ディレクトリー・サーバーが実行されるシステムを展開する。
2. レプリカ・サーバーがまだ停止していない場合は、ここで停止する。状況が**「停止済み」**になるまで、サーバーの状況を最新表示する。
3. **「ネットワーク」**を展開する。
4. **「サーバー」**を展開する。
5. **「TCP/IP」**をクリックする。
6. **「ディレクトリー」**を右クリックし、**「プロパティー」**を選択する。
7. **「ディレクトリー更新の許可」**にチェック・マークが付いていない場合は、チェック・マークを付ける。これでデータのインポートができるようになります。
8. **「OK」**をクリックする。
9. ステップ 2 で転送した LDIF ファイルをインポートする。
10. **「ディレクトリー」**を右クリックし、**「プロパティー」**を選択する。
11. **「ディレクトリー更新の許可」**のチェック・マークを外す。

LDAP データをマスター・サーバーに移動する

レプリカ・サーバー内に LDAP ディレクトリー・サーバーを作成した場合、そのサーバー上のデータは更新できなくなります。レプリカ LDAP ディレクトリー・サーバーとして設定しようとしているサーバーに既存のデータがある場合は、そのデータをマスター・サーバーに移して、引き続き管理できるようにしておく方が便利です。そのためには次のようにしてください。

1. iSeries ナビゲーターで、レプリカ・ディレクトリー・サーバーが実行されるシステムを展開する。
2. **「ネットワーク」**を展開する。
3. **「サーバー」**を展開する。
4. **「TCP/IP」**をクリックする。
5. **「ディレクトリー」**を右クリックし、**「プロパティー」**を選択する。
6. **「ディレクトリー更新の許可」**にチェック・マークが付いている場合は、チェック・マークを外す。これで、複製が完全に設定されるまでディレクトリー更新ができなくなります。
7. **「OK」**をクリックする。
8. LDAP ディレクトリー・サーバーを停止する。
9. ディレクトリーを LDIF ファイルにエクスポートする。
10. LDIF ファイルを、マスター・サーバーの実行先システムに転送する。

LDIF ファイルを、マスター・サーバーが実行されるシステムに転送し終わったら、データをマスター・サーバーにインポートする必要があります。

1. iSeries ナビゲーターで、マスター・ディレクトリー・サーバーが実行されるシステムを展開する。

2. マスター・ディレクトリー・サーバーがまだ停止していない場合は、ここで停止する。状況が**「停止済み」**になるまで、サーバーの状況を最新表示する。
3. **「ネットワーク」**を展開する。
4. **「サーバー」**を展開する。
5. **「TCP/IP」**をクリックする。
6. **「ディレクトリー」**を右クリックし、**「プロパティー」**を選択する。
7. **「ディレクトリー更新の許可」**にチェック・マークが付いていない場合は、チェック・マークを付ける。これでデータのインポートができるようになります。
8. **「OK」**をクリックする。
9. 前述の手順のステップ 10 (25 ページ) で転送した LDIF ファイルをインポートする。
10. **「ディレクトリー」**を右クリックし、**「プロパティー」**を選択する。
11. **「ディレクトリー更新の許可」**のチェック・マークを外す。

新しいレプリカを設定する

新しいレプリカ・サーバーを設定するには、次のようにしてください。

注: この手順を行うには、レプリカ・サーバーの設定が済んでおり、レプリカ・サーバーが停止している必要があります。

1. iSeries ナビゲーターで、レプリカ・ディレクトリー・サーバーが実行されるシステムを展開する。
2. **「ネットワーク」**を展開する。
3. **「サーバー」**を展開する。
4. **「TCP/IP」**をクリックする。
5. サーバーがまだ停止していない場合は、ここでサーバーを停止する。状況が**「停止済み」**になるまで、サーバーの状況を最新表示する。
6. **「ディレクトリー」**を右クリックし、**「プロパティー」**を選択する。
7. **「複製 (Replication)」**タブをクリックする。
8. **「レプリカ・サーバーとして使用 (Use as a replica server)」**を選択する。
9. **「マスター・サーバーが更新用に使用する名前 (Name used by master server for updates)」**フィールドで、更新処理のためにレプリカ・サーバーにログオンするときにマスター・サーバーが使用する名前を選択する。識別名 (DN) または Kerberos ユーザーを選択します。

   DN を選択した場合

   - **「マスター・サーバーが更新用に使用する名前 (Name used by master server for updates)」**フィールドの横にある**「パスワード」**ボタンをクリックする。更新処理のためにレプリカ・サーバーにログオンするときに、マスター・サーバーが使用するパスワードを入力する。

     注: このパスワードと、ステップ 9 で入力した名前は必ず書き留めておいてください。複製用のマスター・サーバーを設定するときに必要になります。

   「Kerberos ユーザーの追加 (Add Kerberos User)」を選択した場合

   - マスター・サーバーの Kerberos 名とデフォルト・レルム (ACME.COM など) を入力するための画面が表示されます。 Kerberos 名については、 `LDAP/` *`hostname`* という形式で指定してください。 *hostname* は、マスター・サーバーの完全修飾ホスト名です。

     注: Kerberos を使用するには、マスター・サーバーとレプリカ・サーバーの両方で Kerberos を使用可能にしておく必要があります。
10. **「マスター・サーバーの URL」**フィールドに、マスター・サーバーの名前を URL 形式で入力する。マスター・サーバーがデフォルト以外のポートを使用する場合は、このポート番号を URL の部分に入力します。

11. **「データベース / 接尾部」**タブをクリックする。複製したい接尾部がリストにない場合は、リストに追加してください。
12. (オプション) 複製時に Secure Sockets Layer (SSL) を使用したい場合は、ディジタル認証マネージャーにより SSL をサーバーで使用できるようにする。ディジタル認証マネージャーは、**「ネットワーク」**タブから開始することができます。ディレクトリー・サーバーで SSL を使用できるようにする方法については、 16 ページの『LDAP ディレクトリー・サーバーで SSL を使用可能にする』を参照してください。
13. **「OK」**をクリックする。

新しいレプリカを持つようにマスター・サーバーを設定する

新しいレプリカを持つようにマスター・サーバーを設定するには、次のようにしてください。

注: この手順を行うには、マスター・サーバーの設定が済んでおり、マスター・サーバーが開始している必要があります。

1. iSeries ナビゲーターで、マスター・ディレクトリー・サーバーが実行されるシステムを展開する。
2. **「ネットワーク」**を展開する。
3. **「サーバー」**を展開する。
4. **「TCP/IP」**をクリックする。
5. **「ディレクトリー」**を右クリックし、**「プロパティー」**を選択する。
6. **「ディレクトリー更新の許可」**にチェック・マークが付いていない場合は、チェック・マークを付ける。
7. **「OK」**をクリックする。
8. LDAP ディレクトリー・サーバーを停止し、再度開始する。状況が**「開始済み」**になるまで、サーバーの状況を最新表示する。
9. 再度、**「ディレクトリー」**を右クリックし、**「プロパティー」**を選択する。
10. **「レプリカの作成」**タブをクリックする。 iSeries ナビゲーターから、接続情報の入力を求められることがあります。その場合は、接続情報を入力し、**「OK」**をクリックしてください。
11. **「追加」**をクリックする。
12. **「サーバー」**フィールドに、レプリカ・サーバーの名前を URL 形式で入力する。
13. 認証方法を選択する。

    識別名 (DN) とパスワードを使用する場合

    a. **「DN とパスワードを使用 (Use DN and password)」**を選択する。

    b. **「接続名 (Connect as)」**フィールドに、レプリカ・サーバーを設定するときにステップ 9 (26 ページ) で指定した名前を入力する。

    c. **「パスワード」**をクリックし、レプリカ・サーバーを設定するときにステップ 9 (26 ページ) で指定したパスワードを入力する。

    Kerberos を使用する場合

    - **「マスター・サーバーの Kerberos アカウントを使用 (Use master server's Kerberos account)」**を選択する。マスター・サーバーは、 Kerberos プリンシパル名を使用して認証を実行します。

      注: Kerberos を使用するには、マスター・サーバーとレプリカ・サーバーの両方で Kerberos を使用可能にしておく必要があります。
14. 複製時に Secure Sockets Layer (SSL) を使用したい場合は、ディジタル認証マネージャーにより SSL をサーバーで使用できるようにする。ディジタル認証マネージャーは、**「ネットワーク」**タブから開始することができます。ディレクトリー・サーバーで SSL を使用できるようにする方法については、16 ページの『LDAP ディレクトリー・サーバーで SSL を使用可能にする』を参照してください。

15. レプリカ・サーバーがデフォルトのポートを使用しない場合は、**「ポート」**フィールドに、使用するポート番号を指定する。
16. マスター・サーバーで項目が変更されるたびにレプリカ・サーバーを更新する必要がない場合は、**「時間」**を選択する。そして、マスター・サーバーがレプリカを更新する頻度を指定してください。
17. **「OK」**をクリックする。
18. **「データベース / 接尾部」**タブをクリックする。複製したい接尾部がリストにない場合は、リストに追加してください。
19. 各レプリカ・サーバーでディレクトリー更新を使用可能にする。
    a. iSeries ナビゲーターで、レプリカ・ディレクトリー・サーバーが実行されるシステムを展開する。
    b. **「ネットワーク」**を展開する。
    c. **「サーバー」**を展開する。
    d. **「TCP/IP」**をクリックする。
    e. **「ディレクトリー」**を右クリックし、**「プロパティー」**を選択する。
    f. **「ディレクトリー更新の許可」**にチェック・マークが付いていない場合は、チェック・マークを付ける。
    g. **「OK」**をクリックする。
20. 各レプリカ・サーバーがまだ開始されていない場合は、ここで開始する。

注: 1 つのサーバーを、マスター・サーバーとレプリカ・サーバーの両方に使用することはできません。

情報をディレクトリー・サーバーに発行する

ご使用のシステムでは、同じシステム上または異なるシステム上の LDAP ディレクトリー・サーバーに対して特定の情報を発行する構成ができます。 iSeries ナビゲーターを使用して OS/400 上でその情報を変更すると、その情報が LDAP ディレクトリー・サーバーに自動的に発行されます。発行できる情報としては、システム情報 (システムとプリンター)、印刷共用情報、ユーザー情報、および TCP/IP のサービスの品質ポリシーがあります。サービスの品質の詳細については、 LDAP 構成と QoS を参照してください。

データの発行先となる親 DN が存在しない場合は、ディレクトリー・サービスがその DN を自動的に作成します。さらに、LDAP ディレクトリーに情報を発行する他の OS/400 アプリケーションをインストールすることもできます。また、ユーザー固有のプログラムに組み込まれたアプリケーション・プログラム・インターフェース (API) を呼び出すことにより、 LDAP ディレクトリーに対して他の情報を発行することもできます。

注:

1. たとえば、LDAP ディレクトリー・サーバーに対して情報タイプ「ユーザー」を発行するように OS/400 を構成すると、ユーザー情報がシステム配布ディレクトリーから LDAP サーバーに自動的にエクスポートされます。その場合には、QGLDSSDD API を使用します。これにより、システム配布ディレクトリーのデータが変更されると、 LDAP ディレクトリーのデータも自動的に変更されます。QGLDSSDD API については、iSeries Information Center の「プログラミング」の下にある OS/400 ディレクトリー・サービスというトピックを参照してください。利用できる情報には、以下のものがあります。
   - 手操作によるこの API の呼び出し方法
   - 特定のユーザーに関する情報が LDAP サーバーにエクスポートされないようにする方法
   - システム配布ディレクトリーのフィールドをエクスポートする方法
2. OS/400 で、LDAP ディレクトリー・サーバーに情報タイプ「システム」を発行するための構成をして、発行用に 1 つまたは複数のプリンターを選択した場合は、システム上のそれらのプリンターに加えられた変更に応じて、 LDAP ディレクトリーが自動的に同期化されます。発行できるプリンター情報としては、プリンターの位置、プリンターの速度 (1 分あたりのページ数)、両面印刷やカラー印刷をサ

ポートしているかどうか、プリンターの型とモデル、プリンターの説明などがあります。この情報は、発行対象のシステムのデバイス記述から読み込まれます。ネットワーク環境のユーザーは、この情報を参考にしてプリンターを選択できます。

3. OS/400 情報を OS/400 上にない LDAP ディレクトリー・サーバーに対して発行することもできます。その場合には、そのサーバーで IBM スキーマを使用するよう設定します。

OS/400 情報を LDAP ディレクトリー・サーバーに対して発行できるようにするには、以下の手順に従います。

1. iSeries ナビゲーターで、ご使用のシステムを右クリックし、**「プロパティー」**を選択する。
2. **「ディレクトリー・サービス」**タブをクリックする。
3. 発行したい情報をクリックする。

   ヒント:

   複数の情報が同じ場所に発行されるようにしたい場合は、それらの情報を一度に選択すると操作の手間を省くことができます。複数の情報を一度に選択した場合には、その中のいずれかの情報を設定するときに入力した値が、以降の情報を設定するときにデフォルトとして使用されます。
4. **「詳細 (Details)」**をクリックする。
5. **「システム情報を発行する (Publish system information)」**チェック・ボックスをクリックする。
6. サーバーで使用したい**認証方法**と、適切な認証情報を指定する。
7. **「(アクティブ) ディレクトリー・サーバー ((Active) Directory server)」**フィールドの横にある**「編集 (Edit)」**ボタンをクリックする。表示されるダイアログで、 OS/400 情報の発行先にしたい LDAP ディレクトリー・サーバーの名前を入力し、**「OK」**をクリックする。
8. **「親識別名 (Under DN)」**フィールドに、情報を追加したいディレクトリー・サーバー上の「親識別名 (DN)」 を入力する。
9. **「サーバー接続 (Server connection)」**フレームの各フィールドで、システムに適した値を設定する。

   注: SSL または Kerberos を使用して、ディレクトリー・サーバーに対して OS/400 情報を発行するには、まずディレクトリー・サーバーで、該当するプロトコルを使用するための設定をしなければなりません。 SSL と Kerberos の詳細については、 44 ページの『LDAP ディレクトリー・サーバーで Kerberos 認証を使用する』を参照してください。
10. ディレクトリー・サーバーがデフォルトのポートを使用していない場合は、**「ポート」**フィールドに正しいポート番号を入力する。
11. **「検証」**をクリックして、親 DN がサーバー上の存在することと、接続情報が正しいことを確認する。指定したディレクトリー・パスが存在しない場合には、ダイアログ・ボックスが表示され、そのディレクトリーを作成するかどうか問い合わせてきます。

    注: 指定した親識別名が存在しないときに、その親識別名を作成しなかった場合、情報は発行されません。
12. **「OK」**をクリックする。

注: OS/400 情報を別のプラットフォーム上の LDAP ディレクトリー・サーバーに対して発行することもできます。ユーザー情報とシステム情報は、ディレクトリー・サービスのスキーマと互換性のあるスキーマを使用しているディレクトリー・サーバーに対して発行する必要があります。 iSeries ディレクトリー・サービスを含む IBM SecureWay ディレクトリー・スキーマ定義は、 ディレクトリー・サービスの Web ページにあります。

印刷共用情報は、 Microsofts の Active Directory スキーマをサポートしているディレクトリー・サーバーに対して発行する必要があります。 Active Directory に対して印刷共用情報を発行すると、

Windows 2000 のデスクトップから Windows 2000 の「プリンタの追加ウィザード」を使って、iSeries プリンターを直接設定できるようになります。そのためには、「プリンタの追加ウィザード」で、プリンターの検索先として Windows 2000 Active Directory を指定してください。

OS/400 情報をディレクトリー・サーバーに対して発行するための API

ディレクトリー・サービスには、ユーザーとシステムの情報を発行するための組み込みサポートがあります。これらの情報は、システムの**「プロパティー」**ダイアログ・ボックスの**「ディレクトリー・サービス」**ページに表示されます。 LDAP サーバー設定用 API と発行用 API により、ユーザー作成の OS/400 プログラムで他の情報を発行することができます。これらの情報も**「ディレクトリー・サービス」**ページに表示されます。ユーザーおよびシステムの場合と同様に、他の情報が示すオブジェクトについても最初は使用不能になっており、 同じ手順によって設定します。 LDAP ディレクトリーにデータを追加するプログラムのことを発行エージェントといいます。そして、発行する情報 (**「ディレクトリー・サービス」**ページに表示される情報) のことをエージェント名といいます。

以下の API により、発行プログラムをユーザー作成プログラムに組み込むことができます。

QgldChgDirSvrA
: アプリケーションは、使用不可になっているエージェント名を CSVR0500 形式で最初に追加します。アプリケーションのユーザーに対する指示で、 iSeries ナビゲーターを使用してディレクトリー・サービスのプロパティー・ページに移動し、発行エージェントを構成するよう指示されます。エージェント名の例としては、**ディレクトリー・サービス・**ページに表示されるシステムおよびユーザーのエージェント名のうち、自動的に使用可能になるシステムおよびユーザーがあります。

QgldLstDirSvrA
: この API の LSVR0500 形式で、システムで現在使用可能なエージェントのリストを表示します。

QgldPubDirObj
: 情報を発行します。

これらの API の詳細については、 iSeries Information Center の「プログラミング」の下にある Lightweight Directory Access Protocol (LDAP) を参照してください。

ディレクトリー参照用のサーバーを指定する

ディレクトリー・サーバーに参照サーバーを割り当てるには、次のようにしてください。

1. iSeries ナビゲーターで**「ネットワーク」**を展開する。
2. **「サーバー」**を展開する。
3. **「TCP/IP」**をクリックする。
4. **「ディレクトリー」**を右ボタンでクリックし、**「プロパティー」**を選択する。
5. **「追加」**をクリックする。
6. プロンプトで、URL 形式で参照サーバーの名前を指定する。以下に示すのは、受け入れ可能な LDAP URL の例です。
   - ldap://test.server.com
   - ldap://test.server.com:400
   - ldap://9.9.99.255

   注: 参照サーバーがデフォルトのポートを使用しない場合は、上述の 2 番目の例でポート 400® を指定したようにして、正しいポート番号を URL 形式で指定します。
7. **「OK」**をクリックする。

LDAP ディレクトリー・サーバーに接尾部を追加する

接尾部を LDAP ディレクトリーに追加すると、サーバーがディレクトリー・ツリーの接尾部の部分を管理できるようになります。

注: 接尾部を追加するときに、サーバーにすでに登録されている接尾部の一部を使用しないでください。たとえば、サーバーに `o=ibm, c=us` という接尾部が登録されている場合には、 `ou=rochester, o=ibm, c=us` という接尾部を追加しないでください。

ディレクトリー・サーバーに接尾部を追加するには、次のようにしてください。
1. iSeries ナビゲーターで**「ネットワーク」**を展開する。
2. **「サーバー」**を展開する。
3. **「TCP/IP」**をクリックする。
4. **「ディレクトリー」**を右クリックし、**「プロパティー」**を選択する。
5. **「データベース / 接尾部」**タブをクリックする。
6. **「新規接尾部」**フィールドに、新しい接尾部の名前を入力する。
7. **「追加」**をクリックする。
8. **「OK」**をクリックする。

注: 接尾部を追加すると、サーバーに対してディレクトリーの 1 つのセクションが指定されますが、実際にオブジェクトが作成されるわけではありません。その新しい接尾部に対応するオブジェクトが実際に存在しない場合は、他のオブジェクトを作成するのと同じ方法で、その種のオブジェクトを作成する必要があります。

ディレクトリー・サーバーから接尾部を削除する

LDAP ディレクトリー・サーバーから接尾部を削除するには、次のようにしてください。
1. iSeries ナビゲーターで**「ネットワーク」**を展開する。
2. **「サーバー」**を展開する。
3. **「TCP/IP」**をクリックする。
4. **「ディレクトリー」**を右クリックし、**「プロパティー」**を選択する。
5. **「データベース / 接尾部」**タブをクリックする。
6. 削除したい接尾部をクリックして選択する。
7. **「除去」**をクリックする。

注: 削除したい接尾部の下にあるディレクトリー・オブジェクトを削除せずに、接尾部を削除するよう選択することができます。これにより、ディレクトリー・サーバーからオブジェクトのデータにはアクセスできなくなります。しかし、接尾部を再び追加すれば、再びデータにアクセスできるようになります。

ディレクトリー・サービス情報の保管と復元

ディレクトリー・サービスの情報の保管場所は、次のとおりです。

- ディレクトリー・サーバーの内容を含むデータベース・ライブラリー (デフォルトは QUSRDIRDB)。
- QDIRSRV2 ライブラリー。発行情報が保管されます。
- QUSRSYS ライブラリー。 QGLD を先頭に、オブジェクトのさまざまな項目が保管されます (QUSRSYS/QGLD* を指定してください)。
- ディレクトリーの変更を記録するようディレクトリー・サーバーを構成すると、その変更が記録される QUSRDIRCL というデータベース・ライブラリーが使用されます。

ディレクトリーの内容が定期的に変更される場合は、データベース・ライブラリーとその中のオブジェクトを定期的に保管する必要があります。構成データは、次のディレクトリーにも保管されます。

```
/QIBM/UserData/OS400/Dirsrv/
```

構成を変更したり、PTF を適用したりする場合には、このディレクトリーにもファイルを保管しなければなりません。

OS/400 データの保管と復元の方法については、 バックアップおよび回復の手引き  を参照してください。

ディレクトリー・データの所有権とアクセス権を管理する

ディレクトリー・データの所有権とアクセス権の管理には、次の作業が含まれます。

- 『ディレクトリー・オブジェクトの所有権プロパティーを処理する』
- 『アクセス制御リスト (ACL) の処理』
- 33 ページの『ACL グループを処理する』

ディレクトリー・オブジェクトの所有権プロパティーを処理する

ディレクトリー・オブジェクトの所有権プロパティーを設定するには、次のようにしてください。

1. iSeries ナビゲーターで**「ネットワーク」**を展開する。
2. **「サーバー」**を展開する。
3. **「TCP/IP」**をクリックする。
4. **「ディレクトリー」**を右クリックし、**「権限」**を選択する。

   ディレクトリー・サーバーに接続していない場合には、**「ディレクトリー・サーバーへの接続」**ダイアログ・ボックスが表示されます。サーバーに接続するときには、サーバー管理者または対象となるオブジェクトの所有者として接続します。
5. ディレクトリー・ツリーの中から対象となるオブジェクトを選択して、**「OK」**をクリックする。

アクセス制御リスト (ACL) の処理

アクセス制御リスト (ACL) の処理には、ディレクトリー・オブジェクトへの明示 ACL および暗黙 ACL の割り当て、 ACL へのユーザーの追加、ACL からのユーザーの削除、およびディレクトリー・オブジェクトのブラウズが含まれます。 V5R1 からの新機能として、ディレクトリー・サービスでは、新しい ACL モデルをサポートするようになりました。したがって、以前から ACL を使っていたユーザーも、 ACL について学び直すようにしてください。

ACL を処理するには次のようにしてください。

1. iSeries ナビゲーターで**「ネットワーク」**を展開する。
2. **「サーバー」**を展開する。
3. **「TCP/IP」**をクリックする。
4. **「ディレクトリー」**を右クリックし、**「権限」**を選択する。

   ディレクトリー・サーバーに接続していない場合には、**「ディレクトリー・サーバーへの接続」**ダイアログ・ボックスが表示されます。サーバーに接続するときには、サーバー管理者または対象となるオブジェクトの所有者として接続します。
5. ディレクトリー・ツリーの中から対象となるオブジェクトを選択して、**「OK」**をクリックする。
6. **「ACL」**タブをクリックする。

ACL グループを処理する

ACL グループを処理するには次のようにしてください。

1. iSeries ナビゲーターで**「ネットワーク」**を選択する。
2. **「サーバー」**を選択する。
3. **「TCP/IP」**をクリックする。
4. **「ディレクトリー」**を右クリックし、**「ACL グループ」**を選択する。

許可ユーザーの管理アクセスを処理する

| V5R2 からは、ディレクトリー・サービス管理者 (QIBM_DIRSRV_ADMIN) ファンクション ID へのアクセスが与えられているユーザー・プロファイルに、管理アクセスを付与することができます。

| たとえば、ユーザー・プロファイル JOHNSMITH にディレクトリー・サーバー管理者ファンクション ID へのアクセスが付与されていて、「ディレクトリー」のプロパティー・ダイアログで「許可ユーザーへの管理者アクセスの認可」オプションが選択されている場合、 JOHNSMITH プロファイルは LDAP 管理者権限を持っていることになります。このプロファイルを使用して、os400-profile=JOHNSMTH,cn=accounts,os400-sys=systemA.acme.com という DN を使用するディレクトリー・サーバーにバインドしているとき、ユーザーは管理者権限を持つことになります。この例では、システム・オブジェクトの接尾部は os400-sys=systemA.acme.com になります。プロジェクト・ユーザーの詳細については、45 ページの『オペレーティング・システム・プロジェクト・バックエンド』を参照してください。

| このオプションを選択するには、以下のステップを実行します。

1. iSeries ナビゲーターで**「ネットワーク」**を展開する。
2. **「サーバー」**を展開する。
3. **「ディレクトリー」**を右マウス・ボタン・クリックし、**「プロパティー」**を選択する。
4. **「管理者情報」**の下の**「一般」**タブで、**「許可ユーザーへの管理アクセスの認可」**オプションを選択する。

| ユーザー・プロファイルに、ディレクトリー・サービス管理者権限ファンクション ID を設定するには、以下のステップを実行します。

1. iSeries ナビゲーターで、システム名を右マウス・ボタンでクリックし、**「アプリケーション管理」**を選択する。
2. **「ホスト・アプリケーション」**タブをクリックする。
3. **「OS/400®」** を展開する。
4. **「ディレクトリー・サービス管理者 (Directory Services Administrator)」**をクリックしてオプションを強調表示する。
5. **「カスタマイズ」**ボタンをクリックする。
6. **「ユーザー」**、**「グループ」**、または**「グループに属さないユーザー」**のうち、それぞれの必要に適したいずれかを展開する。
7. **「アクセス許可」**リストに追加するユーザーまたはグループを選択する。
8. **「追加」**ボタンをクリックする。
9. **「OK」**をクリックして変更を保管する。
10. **「アプリケーション管理」**ダイアログで**「OK」**をクリックする。

LDAP ディレクトリーに対するアクセスと変更をトラッキングする

LDAP ディレクトリーに対するアクセスと変更は記録しておくことができます。 LDAP ディレクトリーの変更ログを使用して、ディレクトリーに加えた変更を記録することができます。変更ログは、特殊な接尾部 cn=changelog の下にあります。これは、QUSRDIRCL ライブラリーに保管されます。

変更ログを使用可能にするには、以下のステップを行います。

1. iSeries ナビゲーターで**「ネットワーク」**を展開する。
2. **「サーバー」**を展開する。
3. **「TCP/IP」**をクリックする。
4. **「ディレクトリー」**を右クリックし、**「プロパティー」**を選択する。
5. **「データベース / 接尾部」**タブをクリックする。
6. **「ディレクトリー変更のログ」**を選択する。
7. (オプショナル) **「最大項目数」**で、記録する変更ログの最大の項目数を指定する。

   注: このパラメーターは任意指定ですが、最大の項目数を指定することを強くお勧めします。最大の項目数を指定しないと、変更ログはすべての項目を記録するため、非常に大きくなる可能性があります。

ディレクトリー・サーバーに適用される変更を表すために、 changeLogEntry オブジェクト・クラスが使われます。変更の設定は、changeNumber によって定義されているように、変更ログのコンテナー内にあるすべての項目の順序セットによって指定されます。変更ログの情報は読み取り専用です。

cn=changelog 接尾部のアクセス制御リストにあるユーザーは、変更ログにある項目を検索することができます。検索を実行するのは、変更ログの接尾部が cn=changelog であるものに対してだけにしてください。変更ログの接尾部に対する追加、変更、または削除は、そうする権限があるとしても行わないでください。それを行うと、予期せぬ結果になる場合があります。

例:

以下の例では、ldapsearch コマンド行ユーティリティーを使用して、サーバーに記録されているすべての変更ログ項目を検索します。

```
ldapsearch -h ldaphost -D cn=admininistrator -w password -b cn=changelog  (changetype=*)
```

ディレクトリー・サーバーのオブジェクト監査を使用可能にする

ディレクトリー・サービスは、OS/400 セキュリティー監査をサポートしています。 QAUDCTL システム値を *OBJAUD に指定した場合は、 iSeries ナビゲーターからオブジェクト監査を使用可能にすることができます。

ディレクトリー・サービスのオブジェクト監査を使用可能にするための手順は、次のとおりです。

1. iSeries ナビゲーターで**「ネットワーク」**を展開する。
2. **「サーバー」**を展開する。
3. **「TCP/IP」**をクリックする。
4. **「ディレクトリー」**を右クリックし、**「プロパティー」**を選択する。
5. **「監査 (Auditing)」**タブをクリックする。
6. サーバーの監査設定を選択する。

監査設定の変更は、**「OK」**をクリックした時点で有効になります。 LDAP ディレクトリー・サーバーを再始動する必要はありません。詳細は、 43 ページの『ディレクトリー・サービスのセキュリティー』を参照してください。

LDAP ディレクトリー・サーバーのパフォーマンスを調整する

次のいずれかを変更することにより、LDAP ディレクトリー・サーバーのパフォーマンスを調整できます。

- 検索のサイズ
- 検索に使用できる最大時間
- サーバーのトランザクション設定値
- データベース接続とサーバー・スレッドの数

ディレクトリー・サーバーのパフォーマンス値を調整するには、次のようにしてください。

1. iSeries ナビゲーターで**「ネットワーク」**を展開する。
2. **「サーバー」**を展開する。
3. **「TCP/IP」**をクリックする。
4. **「ディレクトリー」**を右クリックし、**「プロパティー」**を選択する。
5. **「パフォーマンス」**タブをクリックする。

サーバーが使用するデータベース接続とサーバー・スレッドの数を変更して、ディレクトリー・サーバーのパフォーマンスを調整することもできます。この値を変更するには、次のようにしてください。

1. iSeries ナビゲーターで**「ネットワーク」**を展開する。
2. **「サーバー」**を展開する。
3. **「TCP/IP」**をクリックする。
4. **「ディレクトリー」**を右クリックし、**「プロパティー」**を選択する。
5. **「データベース / 接尾部」**タブをクリックする。

第 5 章 ディレクトリー・サービスの概念と参照情報

ディレクトリー・サービスの LDAP サーバーとその運用方法については、次に示す概念情報と参照情報が役に立ちます。

- 『LDAP アクセス制御リスト (ACL)』
- 39 ページの『LDAP データ交換形式』
- 41 ページの『各国語サポート (NLS) に関する考慮事項』
- 41 ページの『LDAP ディレクトリー・オブジェクトの所有権』
- 42 ページの『LDAP ディレクトリーの参照』
- 42 ページの『トランザクション』
- 43 ページの『レプリカ LDAP ディレクトリー・サーバー』
- 43 ページの『ディレクトリー・サービスのセキュリティー』
- 45 ページの『オペレーティング・システム・プロジェクト・バックエンド』
- 51 ページの『ディレクトリー・サービスと OS/400 ジャーナル・サポート』

LDAP の基本情報および LDAP サーバーの計画については、7 ページの『第 3 章 ディレクトリー・サービスの概要』も参照してください。

LDAP アクセス制御リスト (ACL)

| 多くの場合、LDAP ディレクトリー・サーバーのデータへのアクセスを制限する必要はありません。たとえば、会社のイントラネットの LDAP サーバーに従業員の電話番号リストが入っているとします。このリストの中のデータは、通常、すべての従業員が見ることができるようにする必要があります。

| しかし、社長は、自分の電話番号をすべての社員が参照できるようにはしたくないとします。このような場合に、**アクセス制御リスト (ACL)** を組み込むことができます。この ACL を使って、社長が電話を受ける意志のある従業員だけが社長のサーバー項目へアクセスできるように、制限することができます。

ACL を使うと、ディレクトリー・オブジェクトを追加および削除する権限を誰に付与するかを制御できます。ユーザーにディレクトリー属性を読み取り、書き込み、検索、および比較する権限を与えるかどうかも指定できます。 ACL は継承でも明示的でも構いません。つまり、次のどちらかの方法で ACL を使用することができます。

- 特定のオブジェクト用の ACL を明示的に設定する。
- オブジェクトが LDAP ディレクトリー階層の上位のオブジェクトから ACL を継承することを指定する。

| 上記の例では、おそらく社長は従業員が自分の電話番号を参照できるようにはしたくありませんでした。しかし、社長は、管理職が社長の番号を参照できるようにしたかったのです。このような場合、**ACL グループ**を使うと、管理職に権限を付与するのが簡単になります。 ACL グループを使うと、個人単位で権限を付与するのではなく、ユーザー・グループ単位でアクセス権を認可することができます。これは、同じグループに属するユーザーが複数のオブジェクト・グループにアクセスする必要がある場合に特に便利です。たとえば、社長の電話番号へのアクセス権を持っている管理職グループが、後で給与項目へもアクセスする必要が生じた場合、その ACL グループを再利用することができます。

ACL モデル

すべてのバージョンのディレクトリー・サービスは、アクセス・クラス・レベルの許可モデルをサポートしています。このモデルは、個々の LDAP 属性タイプに、Normal (通常)、Sensitive (機密)、 Critical (クリテ

ィカル) の種別があります。これらの種別は、属性スキーマ・ファイルで制御します。ユーザーをオブジェクトの ACL に追加するとき、そのユーザーが読み取り、書き込み、検索、および比較を実行できる種別がどれであるかを指定します。ほとんどのスキーマでは、電話番号は Normal (通常) 属性として分類されます。したがって、上の例で社長の電話番号へのアクセス権を管理職に与えるには、社長のディレクトリー・オブジェクトの Normal (通常) 属性への読み取りアクセス権を管理職に与えます。 Sensitive (機密) および Critical (クリティカル) の情報には、これまで同様、管理職でもアクセスできません。すべてのバージョンのディレクトリー・サービスは、アクセス・クラス・レベルの許可設定をサポートしています。

ディレクトリー・サービスは、属性レベルの許可モデルもサポートしています。このモデルでは、アクセス・レベルにかかわりなく、属性ごとに、読み取り、書き込み、検索、比較の各権限を指定できます。上記の例をここでも使えば、属性レベルの許可モデルの場合は、全体的な ″Normal″ 属性を持っていない管理職に対しても、 `telephoneNumber` 属性への読み取りアクセスを与えることができるというわけです。

属性レベルの許可モデルは、 SecureWay ディレクトリー・サービス バージョン 3.2 以上のサーバーでのみ有効です。デフォルトでは、これはオフになっています。 ACL を処理するときに、この許可モデルを使用可能にするかどうかを選択できます。いったん使用可能にすると、サーバーを構成し直して、ディレクトリー・データベースを復元しない限り、この許可モデルを使用不可にすることはできません。この許可モデルを使用可能にする場合は、 LDAP V2 クライアント (V5R1 より前の iSeries ナビゲーターを含む) からは管理できないことや、 ACL 項目を破壊する可能性があることを念頭に置いてください。

特別な ACL 値

最初は、ディレクトリー・サービスのディレクトリー・サーバーの中のすべてのオブジェクトに、すべてのディレクトリー・ユーザーが登録されている特殊な ACL グループ `CN=Anybody` が設定されています。デフォルトでは、このグループに対して、すべてのオブジェクトの Normal (通常) クラスの属性に関する読み取り、検索、比較のアクセス権が与えられます。

一部のオブジェクトに、非匿名の通信でディレクトリー・サーバーにバインドするすべてのユーザーに対する同じアクセス許可を与えることができます。こうするには、特殊なアクセス制御リスト (ACL) グループ `cn=Authenticated` を使用します。

特定のオブジェクトに対するアクセス許可を指定するときには、 `cn=this` という特殊な DN を使用することができます。これを使用すると、ACL を継承する子項目が、その所有するオブジェクトに対する操作を実行するよう自動的に許可することができます。

補足事項

iSeries ナビゲーターを通じて ACL を管理する場合、ディレクトリー・サービスが ACL を実装する方法の詳細を知っている必要はありません。しかし、 LDIF ファイルの使用時に ACL 関連の属性を指定する必要がある場合、または ACL を LDAP コマンド行ユーティリティーと共に使用したい場合には、 ACL で使われる属性をよく理解しておく必要があります。 ACL の属性については、 IBM SecureWay ディレクトリー管理ツールの資料 にあるアクセス制御リストの参考資料 を参照してください。

ACL および ACL グループの設定方法と変更方法の詳細については、次のトピックにリンクしてください。

32 ページの『アクセス制御リスト (ACL) の処理』
33 ページの『ACL グループを処理する』

LDAP データ交換形式

LDAP データ交換形式 (LDIF) は、 LDAP ディレクトリー・サーバー間でディレクトリー情報を転送するための簡単な方法を提供します。 LDIF ファイルには、LDAP ディレクトリー項目が単純なテキスト形式で収められています。 ディレクトリー・サーバーが使用する LDIF ファイルの形式は、ディレクトリー・サービスの V4R5 からわずかに変更されました。 LDIF ファイルは、ディレクトリー項目か、ディレクトリー項目への一まとまりの変更のいずれかを記述する一連の行で構成されています。 このファイルで、両方を記述することはできません。

LDIF 項目の一般形式は次のとおりです。

```
version: 1
dn: distinguished name
attrtype1: attrvalue1
...
```

ここで、

- *version* は、LDIF ファイル形式のバージョンを示します。バージョン番号は 1 にする必要があります。バージョン番号を指定しないと、LDIF ファイルは旧式の LDIF ファイル形式であると見なされます。LDIF ファイルがバージョン 1 である場合、その内容は UTF-8 でエンコードする必要があります。
- *distinguished name* はディレクトリー項目の識別名です。
- *attrtype1* は LDAP 属性タイプ (cn、ou など) です。
- *attrvalue1* は属性の値です。

各項目はそれぞれ複数の属性を持つことができます。各属性にそれぞれ単独の行が使用されます。 1 つの属性が 1 行より長い場合は、次の行に継続し、継続行の先頭にはスペースまたはタブ文字を置きます。

同じ LDIF ファイル内に複数の項目がある場合は、項目間がブランク行で区切られます。ポンド記号 (#) で始まる行はすべて注釈行で、 LDIF ファイルの構文を解析する際には無視される必要があります。

以下の要件を満たす識別名または属性値は、ベース 64 でエンコードする必要があります。
- 復帰または改行が含まれている。
- コロン (:)、スペース、またはより小 (<) で始まっている。
- スペースで終了している。

ベース 64 でエンコードした属性は、属性名とその値の間にコロンを 2 つ使用して指定されます。

外部参照は、file:// URL 形式です。属性タイプと外部参照値の間には、コロンとより小記号 (:<) を置く必要があります。

ここで、LDIF ファイルの例をいくつか示します。

例 1: 項目が 2 つの単純な LDAP ファイル

```
version: 1
   dn: cn=Barbara Jensen, ou=Rochester, o=Big Company, c=US
   objectclass: top
   objectclass: person
   objectclass: organizationalPerson
   cn: Barbara Jensen
   cn: Barbara J Jensen
   cn: Babs Jensen
   sn: Jensen
   uid: bjensen
   telephonenumber: +1 408 555 1212
   description: A big sailing fan.
```

```
   dn: cn=Bjorn Jensen, ou=Rochester, o=Big Company, c=US
   objectclass: top
   objectclass: person
   objectclass: organizationalPerson
   cn: Bjorn Jensen
   sn: Jensen
   telephonenumber: +1 408 555 1212
   description:Babs is a big sailing fan, and travels extensively in
   search of perfect sailing conditions.
   title:Product Manager, Rod and Reel Division
```

例 2: ベース 64 でエンコードされた値を含むファイル

```
version: 1
   dn: cn=Gern Jensen, ou=Rochester, o=Big Company, c=US
   objectclass: top
   objectclass: person
   objectclass: organizationalPerson
   cn: Gern Jensen
   cn: Gern O Jensen
   sn: Jensen
   uid: gernj
   telephonenumber: +1 408 555 1212
   description:: V2hhdCBhIGNhcmVmdWwgcmVhZGVyIHlvdSBhcmUhICBUaGlzIHZhbHVlIGlzIGJ
    hc2UtNjQtZW5jb2RlZCBiZWNhdXNlIGl0IGhhcyBhIGNvbnRyb2wgY2hhcmFjdGVyIGluIGl0ICh
    hIENSKS4NICBCeSB0aGUgd2F5LCB5b3Ugc2hvdWxkIHJlYWxseSBnZXQgb3V0IG1vcmUu
```

例 3: 一連の変更レコードおよび注記を含むファイル

注: 変更レコードを使った LDIF ファイルは、直接サーバーにインポートすることはできません。しかし、それらは LDAP シェル・ユーティリティーによってサポートされます。

```
version: 1
   # Add a new entry
   dn: cn=Fiona Jensen, ou=Rochester, o=Big Company, c=US
   changetype: add
   objectclass: top
   objectclass: person
   objectclass: organizationalPerson
   cn: Fiona Jensen
   sn: Jensen
   uid: fiona
   telephonenumber: +1 408 555 1212
   jpegphoto:< file:///usr/local/directory/photos/fiona.jpg

   # Delete an existing entry
   dn: cn=Robert Jensen, ou=Rochester, o=Big Company, c=US
   changetype: delete

   # Modify an entrys relative distinguished name
   dn: cn=Paul Jensen, ou=Rochester, o=Big Company, c=US
   changetype: modrdn
   newrdn: cn=Paula Jensen
   deleteoldrdn: 1
```

LDIF ファイル内の項目の順序は重要です。 LDIF ファイルに指定されている項目を正常に LDAP ディレクトリーに追加するには、まず、その項目の親項目がディレクトリーのネーム・スペースの中に存在していなければなりません。上記の例の場合、第 1 の項目が存在していなければ、第 2 と第 3 の項目は追加できません。

同様に、接尾部が設定されているサーバーに LDIF ファイルをインポートする場合は、 LDIF ファイルにその接尾部を表す項目が存在していることが必要です。たとえば、「ou=Rochester, o=Big Company, c=US」という接尾部がサーバーに設定されている場合には、上述の LDIF ファイルをインポートすること

ができます。しかし、「o=Big Company, c=US」という接尾部がサーバーに設定されている場合には、まずその接尾部を表す項目を LDIF ファイルに指定する必要があります。以下に入力例を示します。

```
dn: o=Big Company, c=US
objectclass: organization
o: Big Company
```

個々の LDIF ファイルの形式と内容は、そのエクスポート元となるサーバーのスキーマによって決まります。 LDIF ファイルは、そのファイルのエクスポート元となったサーバーと同じスキーマを使用する任意の LDAP サーバーにインポートできます。異なるベンダーの LDAP サーバーは、それぞれ異なるスキーマを使用しています (オブジェクト・クラスおよび属性が異なります)。したがって、このようなサーバーで作成した LDIF ファイルを、別のサーバーにインポートできないことがあります。

LDIF ファイル仕様に関する Request for Comments (RFC) は、以下の URL に用意されています。

http://www.ietf.org/rfc/rfc2849.txt 

関連プロシージャー:

23 ページの『LDIF ファイルをインポートする』
23 ページの『LDIF ファイルをエクスポートする』

各国語サポート (NLS) に関する考慮事項

V4R5 以降の OS/400 LDAP サーバーと OS/400 LDAP クライアントは、両方とも LDAP バージョン 3 をベースにしています。以下の NLS の考慮事項にご注意ください。

- データは LDAP サーバーとクライアントの間で UTF-8 形式で転送されます。すべての ISO 10646 文字を使用できます。
- ディレクトリー・サービス LDAP サーバーは、 UTF-16 マッピング方式を使用して、データベースにデータを保管します。
- サーバーとクライアントは、大文字小文字を区別せずにストリングを比較します。英大文字のアルゴリズムが、すべての言語 (ロケール) で正しいわけではありません。

UCS-2 の詳細については、 iSeries Information Center の「計画」の下のグローバリゼーションを参照してください。

LDAP ディレクトリー・オブジェクトの所有権

LDAP ディレクトリーの各オブジェクトには、1 人以上の所有者が設定されています。オブジェクト所有者には、オブジェクトを削除する権限があります。オブジェクトの所有権プロパティーおよびアクセス制御リスト (ACL) 属性を変更できるユーザーは、所有者とサーバー管理者だけです。オブジェクトの所有権は、継承される場合と明示的に付与される場合があります。つまり、所有権を割り当てるには次のどちらかの方法を使用できます。

- 特定オブジェクトの所有権を明示的に設定する。
- LDAP ディレクトリー階層内の上位にあるオブジェクトから、オブジェクトが所有者を継承するように指定する。

ディレクトリー・サービスでは、1 つのオブジェクトに複数の所有者を指定することができます。また、オブジェクトをそれ自体の所有者として指定することもできます。その場合には、オブジェクト所有者のリストに cn=this という特殊な DN を指定します。たとえば、オブジェクト cn=A の所有者が cn=this である場合、 cn=A という名前でサーバーに接続しているユーザーはすべて、 cn=A オブジェクトに所有者としてアクセスすることができます。

関連プロシージャー:

32 ページの『ディレクトリー・オブジェクトの所有権プロパティーを処理する』

LDAP ディレクトリーの参照

参照を使用することにより、複数の LDAP ディレクトリー・サーバーがチームとして機能できるようになります。クライアントが要求した DN が、あるディレクトリーにない場合は、サーバーは自動的にその要求を他の LDAP サーバーに送信 (参照) します。

ディレクトリー・サービスでは、2 種類の参照を使用することができます。 デフォルトの参照サーバーを指定することができます。ディレクトリー内に DN がないときは、LDAP サーバーはこのサーバーにクライアントを参照します。また、LDAP クライアントを使用して、 objectClass が referral である項目をディレクトリー・サーバーに追加することもできます。 これにより、クライアントが要求する特定の DN に基づく参照を指定できます。

注: ディレクトリー・サービスでは、参照オブジェクトに、識別名 (dn)、オブジェクト・クラス (objectClass)、および参照 (ref) 属性だけは必ず指定する必要があります。この制約事項を示す例については、 58 ページの『ldapsearch ユーティリティー』を参照してください。

参照サーバーとレプリカ・サーバーとは密接に関連付けられています。レプリカ・サーバーにあるデータをクライアントの側から変更することはできないので、レプリカは、ディレクトリー・データの変更を求める要求をすべてマスター・サーバーに参照します。

トランザクション

システムの LDAP ディレクトリー・サーバーを構成して、クライアントがトランザクションを使用できるようにすることができます。トランザクションとは、 1 つの単位として扱われる LDAP ディレクトリー操作の集合を指します。トランザクションを設定しておくと、トランザクション内のすべての操作が正常に完了し、トランザクションがコミットされるまで、トランザクション内の個々の LDAP 操作は確定しません。いずれかの操作が失敗したり、トランザクションが取り消されたりすると、残りの操作は元に戻されてしまいます。この機能を使えば、 LDAP 操作をうまく編成することができます。たとえば、いくつかのディレクトリー項目を削除するトランザクションをクライアントに設定するとしましょう。トランザクションの処理中にクライアントとサーバーの接続が失われると、項目の削除は一切行われないことになります。したがって、どの項目が正常に削除されているのかを調べなくても、トランザクションを再びやり直すだけで事は足りるのです。

トランザクションに組み込める LDAP 操作は、次のとおりです。

- 追加
- 変更
- RDN の変更
- 削除

注: トランザクションには、ディレクトリー・スキーマ (cn=schema 接尾部) の変更を組み込まないでください。実際に組み込むことは可能ですが、トランザクションが失敗したときにバックアウトができません。したがって、ディレクトリー・サーバーに予測不能な問題が発生する可能性があります。

トランザクションの詳細については、 IBM SecureWay Directory Client SDK Programming Reference  にある付録『Limited Transaction Support』  を参照してください。

レプリカ LDAP ディレクトリー・サーバー

レプリカ LDAP ディレクトリー・サーバーに格納される情報は、メイン・サーバー、つまりマスター LDAP ディレクトリー・サーバーにある情報と同じです。 LDAP ディレクトリーのレプリカを 1 つまたは複数設けることには、大きな利点が 2 つあります。

- レプリカを使用すると検索が速くなります。すべてのクライアントの検索要求を 1 つのマスター・サーバーに集中させる代わりに、マスター・サーバーとレプリカ・サーバーに要求を分散させることができます。
- レプリカはマスター・サーバーのバックアップとしての役割を果たします。マスター・サーバーが使用不可になっても、レプリカが検索要求に応じるため、ディレクトリー・データへアクセスできます。

レプリカ・サーバーは読み取り専用です。許可ユーザーがレプリカ・サーバーにある項目を変更しようとすると、レプリカ・サーバーは、その要求をマスター・ディレクトリー・サーバーに参照します。

関連プロシージャー:

23 ページの『ディレクトリー・サーバーの新しいレプリカを設定する』

ディレクトリー・サービスのセキュリティー

セキュリティー監査

V5R1 から、ディレクトリー・サービスでは、 OS/400 セキュリティー監査をサポートするようになりました。監査ができる項目は、次のとおりです。

- ディレクトリー・サーバーへのバインドとディレクトリー・サーバーからのアンバインド。
- LDAP ディレクトリー・オブジェクトの許可の変更。
- LDAP ディレクトリー・オブジェクトの所有権の変更。
- LDAP ディレクトリー・オブジェクトの作成、削除、検索、変更。
- 管理者パスワードの変更と識別名 (DN) の更新。
- ユーザー・パスワードの変更。
- ファイルのインポートとエクスポート。

ディレクトリー項目の監査を有効にするには、 OS/400 の監査設定を変更しなければならない場合もあります。 QAUDCTL システム値を *OBJAUD に指定した場合は、 iSeries ナビゲーターからオブジェクト監査を使用可能にすることができます。監査の詳細については、 iSeries Information Center の*機密保護解説書* またはセキュリティー監査を参照してください。

接続認証とセキュリティー

ディレクトリー・サービスでは、 LDAP クライアントと LDAP ディレクトリー・サーバーの間の通信セキュリティーを高めるために、次のメカニズムが用意されています。

- Secure Sockets Layer (SSL) 接続
- Kerberos 認証
- CRAM-MD5 パスワード暗号化

LDAP ディレクトリー・サーバーで Secure Sockets Layer (SSL) と Translation Layer Security を使用する

LDAP ディレクトリー・サーバーとの通信の安全度をさらに高めるために、ディレクトリー・サービスでは Secure Sockets Layer (SSL) セキュリティーを使用することができます。

ディレクトリー・サービスで SSL を使用するには、システムにいずれかの暗号アクセス・プロバイダー製品 (5722-ACx) をインストールしておく必要があります。 iSeries ナビゲーターから SSL を使用したい場合は、いずれかのクライアント暗号化製品 (5722-CEx) を PC にインストールしておく必要もあります。このソフトウェアが必要なのは、次のような場合です。

- SSL 接続を使用して、ワークステーションからディレクトリー・サービスを設定および管理する。これには、iSeries ナビゲーターから実行するタスクが含まれます。
- Windows クライアント API (アプリケーション・プログラム・インターフェース) により作成するアプリケーションで、 SSL 接続を使用する。

SSL が標準のインターネット・セキュリティーです。 SSL を使用して、LDAP クライアントのほか、レプリカ LDAP サーバーとも通信できます。サーバー認証に加えてクライアント認証を使用して、SSL 接続の安全性をさらに高めることができます。クライアント認証では、接続が確立される前に、サーバーに対するクライアントの識別を確認するディジタル証明書を LDAP クライアントが与える必要があります。

SSL を使用するには、 OS/400 のオプション 34 であるディジタル認証マネージャー (DCM) をシステムにインストールしてあることが必要です。 ディジタル認証マネージャー (DCM) は、ディジタル証明書および証明書登録リストを作成し、管理するためのインターフェースとなるものです。 ディジタル証明書と DCM の使用について詳しくは、 ディジタル認証マネージャー (DCM) に関する資料を参照してください。 iSeries で SSL を使用するための情報については、 SSL でアプリケーションをセキュアにするを参照してください。 iSeries サーバーでの TLS について詳しくは、 サポートされている SSL および Transport Layer Security (TLS) プロトコルを参照してください。

LDAP ディレクトリー・サーバーで Kerberos 認証を使用する

ディレクトリー・サービスでは、LDAP ディレクトリー・サーバーで Kerberos 認証を使用するための設定ができるようになりました。 Kerberos とは、秘密鍵の暗号を使用して、クライアント / サーバー型のアプリケーションに強力な認証機能を提供するネットワーク認証プロトコルです。

Kerberos 認証を使用可能にするには、システムにいずれかの暗号サービス・プロバイダー製品 (5722AC2 または 5722AC3) をインストールしておく必要があります。ネットワーク認証サービスも設定しておかなければなりません。

ディレクトリー・サービスの Kerberos サポートでは、 GSSAPI SASL メカニズムがサポートされています。そのため、 SecureWay の LDAP クライアントも、 Windows 2000 の LDAP クライアントも、 LDAP ディレクトリー・サーバーで Kerberos 認証を使用できます。

サーバーが使用する **Kerberos プリンシパル名**の形式は、次のとおりです。

```
service-name/host-name@realm
```

`service-name` は LDAP、 `host-name` はシステムの完全修飾 TCP/IP 名、 `realm` はシステムの Kerberos 設定で指定されているデフォルト・レルムです。

たとえば、 `my-as400` という名前のシステムが、 `acme.com` という TCP/IP ドメインにあり、デフォルトの Kerberos レルムとして `ACME.COM` が指定されている場合は、 LDAP サーバーの Kerberos プリンシパル名は、 `LDAP/my-as400.acme.com@ACME.COM` となります。デフォルトの Kerberos レルムは、 Kerberos 構成フ

ファイル (デフォルトでは /QIBM/UserData/OS400/NetworkAuthentication/krb5.conf) の default_realm ディレクティブ (default_realm = ACME.COM) で指定されています。規則として、Kerberos レルム名は英大文字、ホスト名は英小文字で指定することになっています。 LDAP/ は、英大文字で入力しなければなりません。デフォルト・レルムが設定されていない場合は、ディレクトリー・サーバーで Kerberos 認証を使用するための設定はできません。

Kerberos 認証を使用する場合は、 LDAP ディレクトリー・サーバーが、ディレクトリー・データへのアクセスを決定するための接続に対して、識別名 (DN) を関連付けます。サーバーが DN を関連付けるには、次のような方法があります。

- サーバーが Kerberos ID に基づいて DN を作成する方法。この方法の場合は、 principal@realm という形式の Kerberos ID から、 ibm-kn=principal@realm という形式の DN が生成されます。 ibm-kn= は ibm-kerberosName= と同じです。
- サーバーがディレクトリーの中で、 Kerberos プリンシパルと Kerberos レルムの項目を含んでいる識別名 (DN) を検索する方法。この方法の場合は、次のような流れで、その Kerberos ID を指定した項目が検索されます。
  - サーバーは、ディレクトリーの中で、 krbRealmName-V2 属性が Kerberos レルムと一致する krbRealm-V2 オブジェクトを検索します。そのような項目が見つかった場合は、 princSubtree 属性で指定されている DN の中で、 krbPrincipalName 属性がプリンシパル名およびレルム名と一致する項目を検索します。 krbAliasedObjectName で構成されている DN に、以前に検出した項目の DN が含まれている場合は、 krbAliasedObjectName で構成されている DN が使用されます。そうでなければ、その項目の DN が使用されます。この方法が使用されるのは、基本的に、 Kerberos KDC が Kerberos プリンシパル情報を LDAP ディレクトリーに保管している場合です。
  - そのような検索が失敗した場合は、 ibm-securityIdentities 補助クラスを使用し、なおかつ altSecurityIdentities 属性の値が KERBEROS:principal@realm になっているディレクトリー項目を検索します。この方法で Kerberos ID とディレクトリー項目が関連付けられるのは、 KDC がそのディレクトリーにプリンシパルを保管していない場合です。

LDAP サービス・プリンシパルのキーが入っているキー・テーブル (keytab) ファイルが必要です。 iSeries サーバーでの Kerberos の詳細については、 Information Center の「セキュリティー」の下にあるネットワーク認証サービスを参照してください。 ネットワーク認証サービスの構成には、キー・テーブル・ファイルにデータを追加するための情報が記載されています。

オペレーティング・システム・プロジェクト・バックエンド

システム・プロジェクト・バックエンドには、 OS/400 オブジェクトを、 LDAP でアクセスできるディレクトリー・ツリー内の項目としてマップする機能があります。プロジェクト・オブジェクトは、 LDAP サーバー・データベース内に保管されている実際の項目ではなく、 LDAP 表記の OS/400 オブジェクトになります。 V5R2 では、ディレクトリー・ツリー内の項目としてマップまたはプロジェクトされるオブジェクトは、 OS/400 ユーザー・プロファイルだけです。ユーザー・プロファイル・オブジェクトのマッピングは、 OS/400 ユーザー・プロジェクト・バックエンドと呼ばれます。

LDAP 操作は基礎 OS/400 オブジェクトにマップされており、 LDAP 操作はこれらのオブジェクトにアクセスするためにオペレーティング・システムの機能を実行します。ユーザー・プロファイルで実行されるすべての LDAP 操作は、そのクライアント接続に関連したユーザー・プロファイルの権限の下で実行されます。

オペレーティング・システム・プロジェクト・バックエンドの詳細については、以下を参照してください。

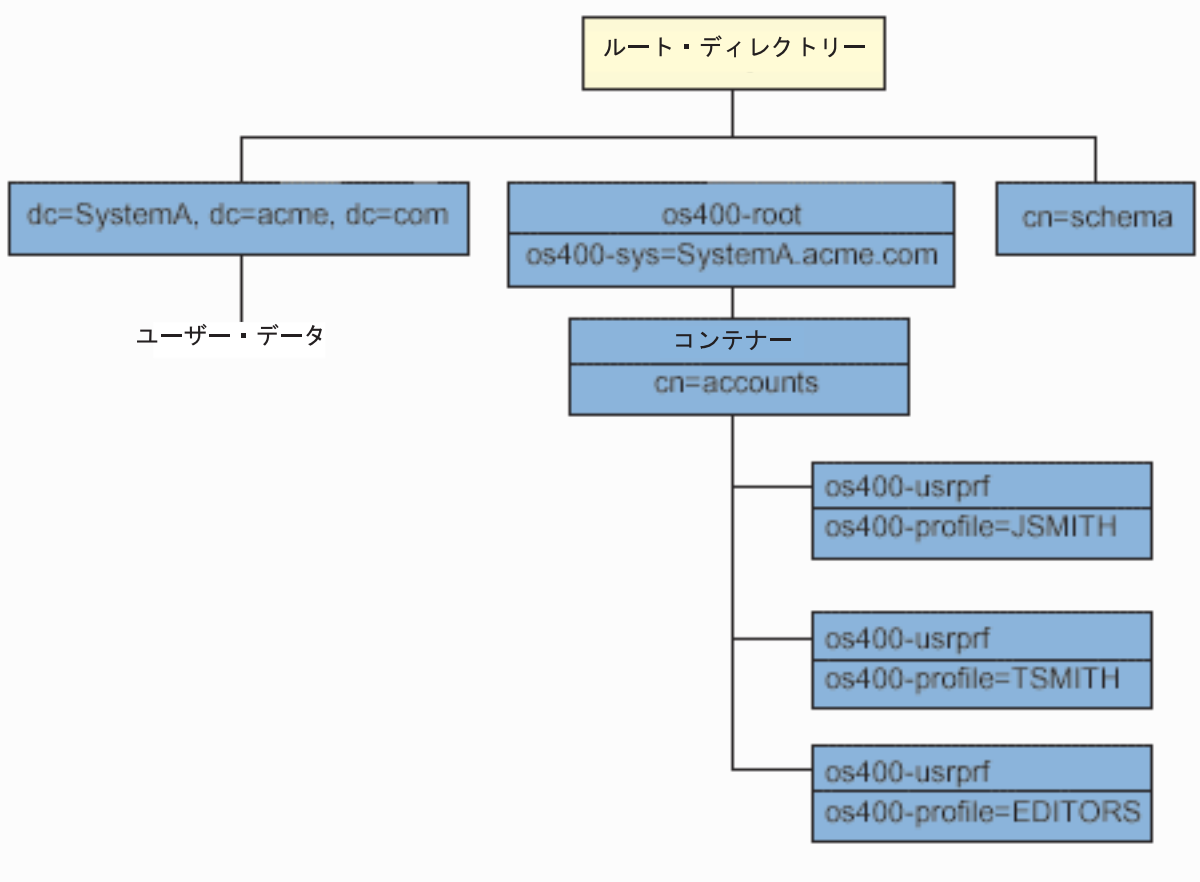
- 46 ページの『OS/400 ユーザー・プロジェクト・ディレクトリー情報ツリー』

- 47 ページの『LDAP 操作』
- 51 ページの『管理者とレプリカ・バインド DN』
- 51 ページの『OS/400 ユーザー・プロジェクト・スキーマ』

OS/400 ユーザー・プロジェクト・ディレクトリー情報ツリー

以下の図は、ユーザー・プロジェクト・バックエンドの、サンプルのディレクトリー情報ツリー (DIT) を表しています。この図には、個人のプロパティーとグループのプロパティーの両方が表されています。この図中の JSMITH と TSMITH はユーザー・プロファイルで、これは内部的には GID=*NONE (または 0) というグループ ID (GID) で示されます。 EDITORS はグループ・プロファイルで、これは内部的にはゼロ以外の GID で示されます。

接尾部 dc=SystemA,dc=acme,dc=com は、参照用に図に含めてあります。この接尾部は、他の LDAP 項目を管理している現行データベース・バックエンドを表します。接尾部 cn=schema は、使用されている現行のサーバー全体のスキーマです。



ツリーのルートは接尾部であり、これはデフォルトで `os400-sys=`*`SystemA.acme.com`* (*`SystemA.acme.com`* はシステムの名前) になります。オブジェクト・クラスは `os400-root` です。 DIT を変更したり削除したりすることはできませんが、システム・オブジェクトの接尾部は再構成できます。ただし、接尾部が変更されればエントリーの変更が必要になる ACL やシステム上の他の場所で、現行の接尾部が使用されていないことを確認する必要があります。

上記の図では、ルートの下にコンテナー cn=accounts が表示されています。このオブジェクトは変更できません。コンテナーは、将来オペレーティング・システムによってプロジェクトされる可能性がある他の種類の情報やオブジェクトを見越してこのレベルに据えられています。 cn=accounts コンテナーの下には、

objectclass=os400-usrprf としてプロジェクトされるユーザー・プロファイルがあります。このユーザー・プロファイルは、プロジェクト・ユーザー・プロファイルと呼ばれ、os400-profile=JSMITH,cn=accounts,os400-sys=SystemA.acme.com の形式で LDAP に認識されます。

LDAP 操作

プロジェクト・ユーザー・プロファイルを使用して実行できる LDAP 操作は、以下のとおりです。

バインド

LDAP クライアントは、プロジェクト・ユーザー・プロファイルを使用して、 LDAP サーバーにバインド (認証) できます。これは、バインド DN のプロジェクト・ユーザー・プロファイル識別名 (DN) と、認証用の正しい OS/400 ユーザー・プロファイル・パスワードを指定することによって行います。バインド要求で使用される DN の例は、 os400-profile=jsmith,cn=accounts,os400-sys=systemA.acme.com です。

システム・プロジェクト・バックエンドの情報にアクセスするには、クライアントはプロジェクト・ユーザーとしてバインドされる必要があります。サーバーは、すべての操作を、そのユーザー・プロファイルの権限を使用して実行します。プロジェクト・ユーザー・プロファイル DN も、他の LDAP 項目の DN と同じように LDAP ACL で使用できます。バインド要求でプロジェクト・ユーザー・プロファイルが指定されているときに許可されるバインド方式は、単純バインド方式だけです。

検索

システム・プロジェクト・バックエンドは、いくつかの基本的な検索フィルターをサポートしています。検索フィルターには、オブジェクト・クラス os400-profile と、os400-gid 属性を指定することができます。os400-profile 属性はワイルドカードをサポートしています。 os400-gid attribute 属性に指定できるのは、(os400-gid=0) (個々のユーザーのプロファイル) か、 !(os400-gid=0) (グループ・プロファイル) に限られます。パスワードとこれに類似した属性を除いて、ユーザー・プロファイルのすべての属性を検索できます。

特定のフィルターでは、 DN オブジェクト・クラスと os400-profile 値のみが戻されます。ただし、その後の検索は、より詳細な情報が戻されるように設定することができます。

以下の表では、検索操作におけるシステム・プロジェクト・バックエンドの動作について説明しています。

表 1. 検索操作におけるシステム・プロジェクト・バックエンドの動作

検索要求	検索ベース	検索範囲	検索フィルター	コメント
os400-sys=SystemA と、(オプションで) その下のコンテナー、および (オプションで) それらのコンテナーの中のオブジェクトについての情報を戻す。	os400-sys=SystemA.acme.com	base、sub、または one	objectclass=* objectclass=os400-root objectclass=container objectclass=os400-usrprf	指定された範囲とフィルターに基づく適切な属性とその値を戻す。システム・オブジェクトの接尾部とその下のコンテナーに対してハードコーディングされている属性とその値が戻される。

表 1. 検索操作におけるシステム・プロジェクト・バックエンドの動作 (続き)

検索要求	検索ベース	検索範囲	検索フィルター	コメント
すべてのユーザー・プロファイルを戻す。	cn=accounts, os400-sys=SystemA.acme.com	one または sub	os400-gid=0	プロジェクト・ユーザー・プロファイルの識別名 (DN)、オブジェクト・クラス、および os400-profile 値のみが戻される。他のフィルターが指定されていると、LDAP_UNWILLING_TO_PERFORM が戻される。
すべてのグループ・プロファイルを戻す。	cn=accounts, os400-sys=SystemA.acme.com	one または sub	(!(os400-gid=0))	プロジェクト・ユーザー・プロファイルの識別名 (DN)、オブジェクト・クラス、および os400-profile 値のみが戻される。他のフィルターが指定されていると、LDAP_UNWILLING_TO_PERFORM が戻される。
すべてのユーザー・プロファイルとグループ・プロファイルを戻す。	cn=accounts, os400-sys=SystemA.acme.com	one または sub	os400-profile=*	プロジェクト・ユーザー・プロファイルの識別名 (DN)、オブジェクト・クラス、および os400-profile 値のみが戻される。他のフィルターが指定されていると、LDAP_UNWILLING_TO_PERFORM が戻される。
特定のユーザー・プロファイルまたはグループ・プロファイル (ユーザー・プロファイル JSMITH など) の情報を戻す。	cn=accounts, os400-sys=SystemA.acme.com	one または sub	os400-profile=JSMITH	他の属性を指定して戻すことができる。
特定のユーザー・プロファイルまたはグループ・プロファイル (ユーザー・プロファイル JSMITH など) の情報を戻す。	os400-profile=JSMITH, cn=accounts, os400-sys=SystemA.acme.com	bas、sub、または one	objectclass=os400-usrprf objectclass=* os400-profile=JSMITH	他の属性を指定して戻すことができる。 1 つのレベルの範囲を指定できるが、 DIT の中のユーザー・プロファイル JSMITH の下には何もないので、検索結果として値は戻されない。

表 1. 検索操作におけるシステム・プロジェクト・バックエンドの動作 (続き)

検索要求	検索ベース	検索範囲	検索フィルター	コメント
A で始まるすべてのユーザー・プロファイルとグループ・プロファイルを戻す。	cn=accounts, os400-sys=SystemA.acme.com	one または sub	os400-profile=A*	プロジェクト・ユーザー・プロファイルの識別名 (DN)、オブジェクト・クラス、および os400-profile 値のみが戻される。他のフィルターが指定されていると、LDAP_UNWILLING_TO_PERFORM が戻される。
G で始まるすべてのグループ・プロファイルを戻す。	cn=accounts, os400-sys=SystemA.acme.com	one または sub	(&(!(os400-gid=0)) (os400-profile=G*))	プロジェクト・ユーザー・プロファイルの識別名 (DN)、オブジェクト・クラス、および os400-profile 値のみが戻される。他のフィルターが指定されていると、LDAP_UNWILLING_TO_PERFORM が戻される。
A で始まるすべてのユーザー・プロファイルを戻す。	cn=accounts, os400-sys=SystemA.acme.com	one または sub	(&(os400-gid=0) (os400-profile=A*))	プロジェクト・ユーザー・プロファイルの識別名 (DN)、オブジェクト・クラス、および os400-profile 値のみが戻される。他のフィルターが指定されていると、LDAP_UNWILLING_TO_PERFORM が戻される。

比較

LDAP 比較操作は、プロジェクト・ユーザー・プロファイルの属性値を比較する場合に使用することができます。 os400-aut 属性と os400-docpwd 属性は比較できません。

追加と変更

ユーザー・プロファイルは、LDAP 追加操作を使用して作成でき、さらに LDAP 変更操作を使用して変更できます。

削除

ユーザー・プロファイルは、LDAP 削除操作を使用して削除できます。 DLTUSRPRF OWNOBJOPT パラメーターと PGPOPT パラメーターの動作を指定するための、 2 つの LDAP サーバー制御が新しく提供さ

れています。これらの制御は LDAP 削除操作で指定できます。これらのパラメーターの動作の詳細については、ユーザー・プロファイルの削除 (DLTUSRPRF) コマンドを参照してください。

LDAP のクライアント削除操作で指定できる制御とそのオブジェクト ID (OID) は以下のとおりです。

- os400-dltusrprf-ownobjopt 1.3.18.0.2.10.8

  制御値

  - controlValue ::= ownObjOpt [newOwner]
  - ownObjOpt ::= *NODLT / *DLT / *CHGOWN

  ownObjOpt 制御値は、ユーザー・プロファイルがオブジェクトを所有している場合に取られる処置を示します。値 *NODLT は、ユーザー・プロファイルがオブジェクトを所有している場合は、そのユーザー・プロファイルを削除しないことを示します。 *DLT 値は、所有されているオブジェクトを削除することを示し、 *CHGOWN 値は、所有権を他のプロファイルに移すことを示します。

  newOwner 値は、所有権を移すプロファイルを示します。 ownObjOpt が *CHGOWN に設定されている場合、この値は必須です。

  制御値の例

  - *NODLT: プロファイルがオブジェクトを所有している場合は、そのプロファイルを削除できないことを示します。
  - *CHGOWN SMITH: オブジェクトの所有権を SMITH ユーザー・プロファイルに移すことを示します。

- オブジェクト ID (OID) は、LDAP_OS400_OWNOBJOPT_CONTROL_OID として ldap.h で定義されています。

  - os400-dltusrprf-pgpopt 1.3.18.0.2.10.9

    制御値は以下のように定義されています。

    controlValue ::=pgpOpt [newPgp [newPgpAut]]
    pgpOpt ::= *NOCHG / *CHGPGP
    newPgp ::= *NONE / user-profile-name
    newPgpAut ::= *OLDPGP / *PRIVATE / *ALL / *CHANGE / *USE / *EXCLUDE

    pgpOpt 値は、削除するプロファイルが任意のオブジェクトの 1 次グループである場合に取られる処置を示します。 *CHGPGP が指定されている場合は、newPgp も指定されていなければなりません。 newPgp 値は、1 次グループ・プロファイル名または *NONE を指定します。新しい 1 次グループ・プロファイルが指定されている場合は、 newPgpAut 値も指定することができます。 newPgpAut 値は、新しい 1 次グループに与えられている、オブジェクトに対する権限を示します。

  制御値の例

  - *NOCHG: プロファイルが任意のオブジェクトの 1 次グループである場合は、そのプロファイルを削除できないことを示します。
  - *CHGPGP *NONE: オブジェクトの 1 次グループを除去することを示します。
  - *CHGPGP SMITH *USE: 1 次グループを SMITH ユーザー・プロファイルに変更し、この 1 次グループに *USE 権限を付与することを示します。

  削除でこれらの制御がいずれも指定されないと、 QSYS/DLTUSRPRF コマンドに対して現在有効なデフォルトが代わりに使用されます。

ModRDN

| プロジェクト・ユーザー・プロファイルは、オペレーティング・システムでサポートされていないため、リ
| ネームできません。

| API のインポートとエクスポート

| QgldImportLdif API と QgldExportLdif API は、システム・プロジェクト・バックエンド内のデータのイン
| ポートやエクスポートはサポートしていません。

| 管理者とレプリカ・バインド DN

| プロジェクト・ユーザー・プロファイルは、構成済みの管理者またはレプリカ・バインド DN として指定
| することができます。ユーザー・プロファイルのパスワードが使用されます。プロジェクト・ユーザー・プ
| ロファイルは、ディレクトリー・サーバー管理者ファンクション ID (QIBM_DIRSRV_ADMIN) に対する権
| 限を有していれば、 LDAP 管理者になることも可能です。管理アクセスは複数のユーザー・プロファイル
| に付与することができます。

| 詳細については、 33 ページの『許可ユーザーの管理アクセスを処理する』を参照してください。

| OS/400 ユーザー・プロジェクト・スキーマ

| プロジェクト・バックエンドのオブジェクト・クラスと属性は、サーバー全体のスキーマの中にあります。
| LDAP 属性の名前は os400-*nnn* の形式になります (ここで *nnn* は、一般にユーザー・プロファイル・コマ
| ンドの属性のキーワード (CRTUSRPRF や CHGUSRPRF など) になります)。詳細については、 46 ページ
| の『OS/400 ユーザー・プロジェクト・ディレクトリー情報ツリー』を参照してください。

ディレクトリー・サービスと OS/400 ジャーナル・サポート

ディレクトリー・サービスの OS/400 データベース・サポートは、ディレクトリー情報を格納するための機能です。 OS/400 ジャーナル・サポートとは、ディレクトリー・サービスがコミットメント制御によりディレクトリー項目をデータベースに格納するときに必要な機能です。

サーバーまたは LDIF インポート・ツールを初めて開始すると、以下のものが作成されます。

- ジャーナル
- ジャーナル・レシーバー
- 最初に必要とされるデータベース・テーブル

ジャーナル QSQJRN は、すでに設定されているデータベース・ライブラリーに作成されます。ジャーナル・レシーバー QSQJRN0001 は、すでに設定されているデータベース・ライブラリーに最初に作成されます。

運用環境、ディレクトリーのサイズと構造、または保管 / 復元方針によっては、オブジェクトの管理方法や使用するサイズ限界値などをデフォルトから変更する必要が生じるかもしれません。ジャーナル・コマンド・パラメーターは、必要に応じて変更可能です。 LDAP ジャーナル処理は、デフォルトでは古いレシーバーを削除するように設定されます。変更ログが構成されていて、古いレシーバーを保持したい場合は、OS/400 コマンド行から以下のコマンドを実行します。

```
JRN(QUSRDIRCL/QSQJRN) DLTRCV(*NO)
```

変更ログを設定した場合は、以下のコマンドで変更ログのジャーナル・レシーバーを削除できます。

```
CHGJRN JRN(QUSRDIRCL/QSQJRN)  DLTRCV(*YES)
```

ジャーナル・コマンドの情報については、 iSeries Information Center の「プログラミング」の下にある OS/400 コマンドを参照してください。

第 6 章 LDAP コマンド行ユーティリティー

ディレクトリー・サービスには、 OS/400 の Qshell コマンド環境から LDAP ディレクトリー・サーバーに対してアクションを実行するための 5 つのユーティリティーが用意されています。これらのユーティリティーでは LDAP API が使用されます。各ユーティリティーは、qsh のコマンド行から実行することも、プログラムから呼び出すこともできます。これらのユーティリティーはプログラミングの例としても役に立ちます。ディレクトリー・サービスに含まれる Windows LDAP クライアントをインストールすると、シェル・ユーティリティーのソース・コードに大変よく似たコードもインストールされます。

ユーティリティーは次のとおりです。
- 『ldapmodify および ldapadd ユーティリティー』。LDAP ディレクトリーの項目を追加および変更します。
- 56 ページの『ldapdelete ユーティリティー』。LDAP ディレクトリーから項目を削除します。
- 58 ページの『ldapsearch ユーティリティー』。LDAP ディレクトリー内の項目を検索します。
- 64 ページの『ldapmodrdn ユーティリティー』。LDAP ディレクトリーの項目の相対識別名 (RDN) を変更します。

コマンド行ユーティリティーと共に SSL を使用する方法については、 66 ページの『LDAP コマンド行ユーティリティーで SSL を使用する上での注意事項™』を参照してください。

ldapmodify および ldapadd ユーティリティー

ldapmodify ユーティリティーを使うと、システムの QSH コマンド・シェルから LDAP ディレクトリー・サーバーに対して項目の変更または項目の追加を行うことができます。これは ldap_modify、ldap_add、および ldap_delete アプリケーション・プログラミング・インターフェース (API) を使用します。 ldapadd ユーティリティーの機能は、 -a フラグが自動的にオンになるという点を除けば、ldapmodify ユーティリティーとほとんど同じです。

形式:

ldapmodify [-a] [-V] [-b] [-c] [-r] [-M] [-n] [-v] [-F] [-R] [-C *charset***] [-d** *debuglevel***] [-D** *binddn***] [-w** *passwd* **] [-m** *mechanism***] [-O***hopcount***] [-h** *ldaphost***] [-p** *ldapport***] [-f** *file***] [-Z] [-K** *keyfile***] [-P** *keyfilepw***] [-N** *certificatename***]**

ldapadd [-V] [-b] [-c] [-r] [-M] [-n] [-v] [-F] [-R] [-C *charset***] [-d** *debuglevel***] [-D** *binddn* **] [-w** *passwd***] [-m** *mechanism***] [-O***hopcount***] [-h** *ldaphost***] [-p** *ldapport***] [-f** *file***] [-Z] [-K** *keyfile***] [-P** *keyfilepw***] [-N** *certificatename***]**

注: *file* から項目情報を提供するための **-f** オプションを指定しなかった場合、ユーティリティーは、標準入力から項目が読み取られるまで待ちます。この待ち状態を中断するには、SysReq キーを押してから、 2．前の要求の終了を選択してください。

診断:

エラーがない場合は、戻り状況は 0 です。エラーがあった場合は、ゼロ以外の戻り状況が発生し、標準エラーに診断メッセージが書き込まれます。

これらのユーティリティーの使用方法を見るには、 ここをクリックしてください。

パラメーター:

-V	ユーティリティーが LDAP サーバーにバインドするために使用する LDAP のバージョンを指定します。デフォルトの設定では、LDAP V3 接続を使用します。明示的に LDAP V3 を選択する場合は -V 3 と指定し、 LDAP V2 アプリケーションとして実行する場合は -V 2 と指定します。
-a	このパラメーターは ldapmodify のみで使用します。これは、デフォルトでユーティリティーは項目を変更するのではなく追加することを示します。このパラメーターを使用した場合、ldapadd を使用した場合と同じです。
-b	˽/ で始まるすべての値はバイナリー値で、実際の値は、値の代わりにパスで指定されているファイルに入っていると見なされます。
-c	連続オペレーション・モード。エラーは報告されますが、ldapmodify または ldapadd は変更処理または追加処理を続行します。デフォルトの設定では、エラーの報告後に終了します。
-r	デフォルトの設定では、既存の値が置換されます。
-M	参照オブジェクトを普通の項目として管理します。
-n	実行される処理が表示されますが、実際の項目変更は行いません。 -v と併用してデバッグに使用すると便利です。
-v	冗長モードを使用して、多くの診断結果を標準出力に書き込みます。
-F	replica: で始まる入力行の内容に関係なく、すべての変更を強制適用します (デフォルトの設定では、 replica: 行を使用中の LDAP サーバー・ホストおよびポートと比較することにより、複製ログ・レコードを実際に適用するかどうかが決定されます)。
-R	参照を自動的に行わないことを指定します。
-C *charset*	ユーティリティーへの入力として提供されたストリングを、ローカル文字セット (*charset*) で表されるようにし、 UTF-8 に変換されるよう指定します。入力ストリングのコード・ページがジョブのコード・ページ値と異なる場合には、 **-C** 文字セット・オプションを使用します。 サポートされている *charset* 値について調べるには、ldap_set_iconv_local_charset() API に関する資料を参照してください。
-d *debuglevel*	デバッグ・レベルを *debuglevel* にセットします。
-D *binddn*	*binddn* を使用して LDAP ディレクトリーにバインドします。 *binddn* は、ストリング表記の DN です。
-w *passwd*	*passwd* を認証用のパスワードとして使用します。
-m *mechanism*	*mechanism* を使用して、クライアントがサーバーへのバインドに使用する SASL メカニズムを指定します。クライアントは、 ldap_sasl_bind_s() API を使用します。使用可能なメカニズムとしては、 CRAM-MD5 (パスワードの暗号化)、 EXTERNAL (SSL での使用)、 GSSAPI (Kerberos) があります。 **-V 2** を設定した場合、このコマンドは、 **-m** パラメーターを無視します。 **-m** を指定しないと、単純認証が使用されます。
-O*hopcount*	参照を追跡する際にクライアント・ライブラリーが取るホップの最大数を設定するよう *hopcount* を指定します。デフォルトのホップ・カウントは 10 です。
-h *ldaphost*	LDAP サーバーを実行する代替ホストを指定します。
-p *ldapport*	LDAP サーバーが listen する代替伝送制御プロトコル (TCP) ポートを指定します。デフォルトの LDAP ポートは 389 です。この値の指定がなく、**-Z** が指定されている場合は、デフォルトの LDAP SSL ポート 636 が使用されます。
-f *file*	標準入力からではなく、LDIF ファイルから項目の変更情報を読み取ります。 LDIF ファイルを指定しない場合には、標準入力を使用して、LDIF 形式で更新レコードを指定する必要があります。

-Z	安全性の高い SSL 接続を使用して LDAP サーバーと通信します。 **-Z** オプションは、このツールの SSL 対応バージョンでのみサポートされます。
-K *keyfile*	SSL キー・データベース・ファイルの名前を指定します。キー・データベース・ファイルが現行ディレクトリーにない場合は、完全修飾キー・データベース・ファイル名を指定してください。ユーティリティーがキー・データベースを探し出すことができない場合には、デフォルトのトラステッド認証局ルートのハードコーディングされたセットが使われます。キー・データベース・ファイルには、一般に、クライアントが信頼している認証局 (CA) の 1 つまたは複数の証明書が含まれています。これらのタイプの X.509 証明書は、トラステッド・ルートとも呼ばれています。このパラメーターを使用すると、**-Z** スイッチを使用できるようになります。
-P *keyfilepw*	キー・データベースのパスワードを指定します。このパスワードは、キー・データベース・ファイル内の暗号化された情報 (秘密鍵を含む) にアクセスするために必要です。パスワードの stash ファイルがキー・データベース・ファイルに関連付けられている場合、パスワードはその stash ファイルから取得されるので、このパラメーターは必要ありません。 **-Z** と **-K** をどちらも指定していない場合は、このパラメーターは無視されます。
-N *certificatename*	キー・データベース・ファイル内のクライアント証明書に関連したラベルを指定します。 LDAP サーバーが Server Authentication (サーバー認証) だけを実行するように設定されている場合は、クライアント証明書は不要です。 LDAP サーバーが Client and Server Authentication (クライアントおよびサーバーの認証) を実行するように設定されている場合は、クライアント証明書が必要です。デフォルトの証明書 / 秘密鍵のペアがデフォルトとして指定されている場合は、 *certificatename* は不要です。同様に、指定したキー・データベース・ファイル内に証明書 / 秘密鍵のペアが 1 つある場合も、 *certificatename* は不要です。 **-Z** と **-K** をどちらも指定していない場合は、このパラメーターは無視されます。

代替入力形式:

ldapmodify ユーティリティーは、ユーティリティーの旧バージョンとの互換性を維持するための代替入力形式をサポートしています。この形式は、ブランク行で区切られた 1 つまたは複数の項目から構成されます。各項目の形式は次のとおりです。

```
識別名 (DN)
attr=value
[attr=value ...]
```

attr は属性の名前で、*value* は値です。デフォルトの設定では、値は加算されます。 **-r** コマンド行フラグを指定すると、デフォルトの設定では既存の値が新しい値で置換されます。特定の属性を複数指定することもできます (たとえば、1 つの属性に複数の値を追加してもかまいません)。行末に円記号 (¥) を使用すると、値を次行へ継続し、改行を値自体の中に保存することができます。値を削除するには、*attr* 値の前にダッシュ (-) を付けます。値全体を削除するには、等号 (=) および値を削除します。 **-r** フラグが指定されている場合、値を追加するには、*attr* の前に正符号 (+) を付ける必要があります。

例: ldapmodify および ldapadd

例 1:

/tmp/entrymods というファイルがあり、このファイルの内容が次のとおりであるとします。

```
dn: cn=Modify Me, o=University of Higher Learning, c=US
changetype: modify
replace: mail
mail: modme@student.of.life.edu
```

```
-
add: title
title: Grand Poobah
-
add: jpegPhoto
jpegPhoto:< file:///tmp/modme.jpeg
-
delete: description
-
```

コマンド `ldapmodify -b -r -f /tmp/entrymods` を実行すると、次の処理が行われます。

- Modify Me 項目のメール属性の内容を、値 `modme@student.of.life.edu` で置換する。
- タイトル `Grand Poobah` を追加する。
- ファイル **/tmp/modme.jpeg** の内容を jpegPhoto として追加する。
- `description` 属性を完全に削除する。

古い ldapmodify 入力形式を使って、上と同じ変更を実行することもできます。

```
cn=Modify Me, o=University of Higher Learning, c=US
mail=modme@student.of.life.edu
+title=Grand Poobah
+jpegPhoto=/tmp/modme.jpeg
-description
```

古い形式を使うためのコマンドは、次のとおりです。

```
ldapmodify -b -r -f /tmp/entrymods
```

例 2:

/tmp/newentry というファイルがあり、このファイルの内容が次のとおりであるとします。

```
dn: cn=John Doe, o=University of Higher Learning, c=US
objectClass: person
cn: John Doe
cn: Johnny
sn: Doe
title: Manager
mail: johndoe@student.of.life.edu
uid: jdoe
```

コマンド `ldapadd -f /tmp/entrymods` を実行すると、ファイル /tmp/newentry からの値を使って、John Doe のための新規項目が追加されます。

例 3:

/tmp/newentry というファイルがあり、このファイルの内容が次のとおりであるとします。

```
dn: cn=John Doe, o=University of Higher Learning, c=US
changetype: delete
```

コマンド `ldapmodify -f /tmp/entrymods` を実行すると、John Doe の項目が削除されます。

ldapdelete ユーティリティー

ldapdelete ユーティリティーを使用すると、 LDAP ディレクトリー・サーバーから 1 つまたは複数の項目を削除することができます。このユーティリティーは、 OS/400 の QSH コマンド・シェルから実行します。このユーティリティーでは、 ldap_delete アプリケーション・プログラム・インターフェース (API) が使用されます。

形式:

ldapdelete [-V] [-M] [-n] [-v] [-c] [-R] [-C charset] [-d *debuglevel*] **[-f** *file*] **[-D** *binddn*] **[-w** *passwd*] **[-m** *mechanism*] **[-O** *hopcount*] **[-h** *ldaphost*] **[-p** *ldapport*] **[-Z] [-K** *keyfile*] **[-P** *keyfilepw*] **[-N** *certificatename*] **[***dn*]...

注: *dn* 引き数を指定しなかった場合は、ldapdelete コマンドは、標準入力から DN のリストを読み取るために待ち状態になります。この待ち状態を中断するには、SysReq キーを押してから、 2．前の要求の終了を選択してください。

診断:

エラーがない場合は、戻り状況は 0 です。エラーがあった場合は、ゼロ以外の戻り状況が発生し、標準エラーに診断メッセージが書き込まれます。

ldapdelete ユーティリティーの使用例を見るには、 ここをクリックしてください。

パラメーター:

-V	ユーティリティーが LDAP サーバーにバインドするために使用する LDAP のバージョンを指定します。デフォルトの設定では、LDAP V3 接続を使用します。明示的に LDAP V3 を選択する場合は -V 3 と指定し、 LDAP V2 アプリケーションとして実行する場合は -V 2 と指定します。
-M	参照オブジェクトを普通の項目として管理します。
-n	何が行われるかを示すだけで、実際に項目の削除は行いません。 **-v** と併用してデバッグに使用すると便利です。
-v	冗長モードを使用して、多くの診断結果を標準出力に書き込みます。
-c	連続オペレーション・モード。エラーが報告されますが、ldapdelete は削除を続けます。デフォルトの設定では、エラーの報告後に終了します。
-R	参照を自動的に行わないことを指定します。
-C *charset*	ldapdelete ユーティリティーへの入力として提供された識別名 (DN) が、ローカル文字セット (*charset*) で表されるように設定します。 **-C** *charset* を使用して、省略路の設定を上書きします。この場合、ストリングは UTF-8 で提供される必要があります。入力ストリングのコード・ページがジョブのコード・ページ値と異なる場合には、 **-C** 文字セット・オプションを使用します。サポートされている *charset* 値について調べるには、 ldap_set_iconv_local_charset() API に関する資料を参照してください。
-d *debuglevel*	デバッグ・レベルを *debuglevel* にセットします。
-f *file*	*file* から一連の行を読み取り、各行について 1 回ずつ LDAP 削除を行います。ファイル内の各行には識別名 (DN) が 1 つずつ含まれていることが必要です。
-D *binddn*	*binddn* を使用して LDAP ディレクトリーにバインドします。 *binddn* は、ストリング表記の DN です。
-w *passwd*	*passwd* を認証用のパスワードとして使用します。
-m *mechanism*	*mechanism* を使用して、 SASL メカニズムがサーバーへのバインドを使用するよう指定します。 ldap_sasl_bind_s() API が使用されます。使用可能なメカニズムとしては、CRAM-MD5 (パスワードの暗号化)、 EXTERNAL (SSL での使用)、 GSSAPI (Kerberos) があります。 -V 2 をセットすると、-m パラメーターは無視されます。 **-m** を指定しないと、単純認証が使用されます。
-O *hopcount*	参照を追跡する際にクライアント・ライブラリーが取るホップの最大数を設定するよう *hopcount* を指定します。デフォルトのホップ・カウントは 10 です。

-h *ldaphost*	LDAP サーバーを実行する代替ホストを指定します。
-p *ldapport*	LDAP サーバーが listen する代替伝送制御プロトコル (TCP) ポートを指定します。デフォルトの LDAP ポートは 389 です。この値の指定がなく、**-Z** が指定されている場合は、デフォルトの LDAP SSL ポート 636 が使用されます。
-Z	安全性の高い SSL 接続を使用して LDAP サーバーと通信します。 **-Z** オプションは、このツールの SSL 対応バージョンでのみサポートされます。
-K *keyfile*	SSL キー・データベース・ファイルの名前を指定します。キー・データベース・ファイルが現行ディレクトリーにない場合は、完全修飾キー・データベース・ファイル名を指定してください。ユーティリティーがキー・データベースを探し出すことができない場合には、デフォルトのトラステッド認証局ルートのハードコーディングされたセットが使われます。キー・データベース・ファイルには、一般に、クライアントが信頼している認証局 (CA) の 1 つまたは複数の証明書が含まれています。これらのタイプの X.509 証明書は、トラステッド・ルートとも呼ばれています。このパラメーターを使用すると、**-Z** スイッチを使用できるようになります。
-P *keyfilepw*	キー・データベースのパスワードを指定します。このパスワードは、キー・データベース・ファイル内の暗号化された情報 (秘密鍵を含む) にアクセスするために必要です。パスワードの stash ファイルがキー・データベース・ファイルに関連付けられている場合、パスワードはその stash ファイルから取得されるので、このパラメーターは必要ありません。 **-Z** と **-K** をどちらも指定していない場合は、このパラメーターは無視されます。
-N *certificatename*	キー・データベース・ファイル内のクライアント証明書に関連したラベルを指定します。 LDAP サーバーが Server Authentication (サーバー認証) だけを実行するように設定されている場合は、クライアント証明書は不要です。 LDAP サーバーが Client and Server Authentication (クライアントおよびサーバーの認証) を実行するように設定されている場合は、クライアント証明書が必要です。デフォルトの証明書 / 秘密鍵のペアがデフォルトとして指定されている場合は、 *certificatename* は不要です。同様に、指定したキー・データベース・ファイル内に証明書 / 秘密鍵のペアが 1 つある場合も、 *certificatename* は不要です。 **-Z** と **-K** をどちらも指定していない場合は、このパラメーターは無視されます。
dn	1 つまたは複数の *dn* 引き数を指定します。各 *dn* はストリング表記の DN です。

例: ldapdelete

次のコマンドでは、組織項目 University of Life のすぐ下にある Delete Me という commonName を持つ項目の削除を行います。

```
ldapdelete cn=Delete Me, o=University of Life, c=US
```

実行するには、*binddn* および *passwd* の指定が必要になることがあります (**-D** および **-w** オプションを参照)。

ldapsearch ユーティリティー

ldapsearch ユーティリティーを使用すると、OS/400 の QSH コマンド・シェルから、 LDAP ディレクトリー・サーバー上の項目を検索することができます。このユーティリティーでは、 ldap_search アプリケーション・プログラミング・インターフェース (API) が使用されます。

この検索では、LDAP フィルター用のストリング表現に適合するフィルターを使用します。 LDAP 検索フィルターの詳細については、 iSeries Information Center の「プログラミング」の下にあるOS/400 ディレクトリー・サービスで、 ldap_search API の情報を参照してください。

1 つまたは複数の項目が見つかると、ldapsearch ユーティリティーは、 *attrs* に指定されている属性を検索し、項目と値を標準出力に出力します。属性を指定しなかった場合は、ユーティリティーはすべての属性を戻します。

形式:

ldapsearch [-V] [-n] [-v] [-t] [-A] [-B] [-L] [-M] [-R] [-C *charset***] [-d** *debuglevel***] [-F** *sep***] [-f** *file***] [-D** *binddn***] [-w** *bindpasswd***] [-m** *mechanism***] [-O** *hopcount***] [-h** *ldaphost***] [-p** *ldapport***] [-Z] [-K** *keyfile***] [-P** *keyfilepw***] [-N** *certificatename***] [-b** *searchbase***] [-s** *scope* **] [-a** *deref***] [-l** *time limit***] [-z** *size limit***]** *filter* **[***attrs...***]**

診断:

エラーがない場合は、戻り状況は 0 です。エラーがあった場合は、ゼロ以外の戻り状況が発生し、標準エラーに診断メッセージが書き込まれます。

出力形式:

1 つまたは複数の項目が見つかると、ldapsearch は各項目を次の形式で標準出力に書き込みます。

```
識別名 (DN)
attributename=value
attributename=value
attributename=value
...
```

複数の項目は、それぞれ 1 つのブランク行で区切られます。 **-F** オプションを使って区切り文字を指定した場合は、等号 (=) の代わりにその文字が出力に表示されます。 **-t** オプションを指定した場合は、実際の値が一時ファイルの名前で置き換えられます。 **-A** オプションを指定した場合は、 `attributename` の部分だけが書き込まれます。

ldapsearch ユーティリティーの使用例を見るには、 ここをクリックしてください。

パラメーター:

-V	ユーティリティーが LDAP サーバーにバインドするために使用する LDAP のバージョンを指定します。デフォルトの設定では、LDAP V3 接続を使用します。明示的に LDAP V3 を選択する場合は -V 3 と指定し、 LDAP V2 アプリケーションとして実行する場合は -V 2 と指定します。
-n	何が行われるかを示すだけで、実際の検索は行いません。 **-v** と併用してデバッグに使用すると便利です。
-v	冗長モードを使用して、多くの診断結果を標準出力に書き込みます。
-t	検索した値を一組の一時ファイルに書き込みます。これは、jpegPhoto や audio などのバイナリー値を扱うときに便利です。
-A	属性だけ (値ではなく) を検索します。これは、項目内に属性があるかどうかを知りたいだけで、特定の値には関心がない場合に便利です。
-B	バイナリー値の表示を抑止しません。これは、ISO-8859.1 などの代替文字セットで表される値を扱うときに便利です。このオプションは、**-L** を指定すると暗黙的に指定されます。
-L	検索結果を LDIF 形式で表示します。このオプションを指定すると **-B** オプションもオンになり、 **-F** オプションは無視されます。
-M	参照オブジェクトを普通の項目として管理します。

-R	参照を自動的に行わないことを指定します。
-C *charset*	ldapsearch ユーティリティーへの入力として提供されるストリングが、ローカル文字セット (*charset*) で表されるように指定します。ストリングの入力には、フィルター、バインド DN、およびベース DN が含まれています。同様に、ldapsearch は、データを表示する際、 LDAP サーバーから受け取ったデータを指定の文字に変換します。 入力ストリングのコード・ページがジョブのコード・ページ値と異なる場合には、 **-C** 文字セット・オプションを使用します。 サポートされている *charset* 値について調べるには、ldap_set_iconv_local_charset() API に関する資料を参照してください。また、-C オプションと -L オプションを両方とも指定する場合、入力は指定した文字セットによるものと見なされますが、 ldapsearch からの出力は常に UTF-8 表示で示されるか、印刷不能文字が検出される場合には、そのデータのベース 64 エンコード表示で示されます。これは、標準の LDIF ファイルにストリング・データの UTF-8 (または、ベース 64 エンコードの UTF-8) 表示が含まれている場合だけに当てはまります。
-d *debuglevel*	デバッグ・レベルを *debuglevel* にセットします。
-F *sep*	属性名と属性値の間のフィールド区切り記号として、*sep* を使用します。 **-L** フラグを指定しなかった場合、デフォルトの区切り記号は `= です。この場合、このオプションは無視されます。
-f *file*	ファイル内の各行に対する LDAP 検索を実行しながら、ファイルから一連の行を読み取ります。ファイル内の各行には識別名 (DN) が 1 つずつ含まれていることが必要です。
-D *binddn*	*binddn* を使用して LDAP ディレクトリーにバインドします。 *binddn* は、ストリング表記の DN です。
-w *passwd*	*passwd* を認証用のパスワードとして使用します。
-m *mechanism*	*mechanism* を使用して、 SASL メカニズムがサーバーへのバインドを使用するよう指定します。 ldap_sasl_bind_s() API が使用されます。使用可能なメカニズムとしては、CRAM-MD5 (パスワードの暗号化)、 EXTERNAL (SSL での使用)、 GSSAPI (Kerberos) があります。 **-V** 2 をセットすると、**-m** パラメーターは無視されます。 **-m** を指定しないと、単純認証が使用されます。
-O *hopcount*	参照を追跡する際にクライアント・ライブラリーが取るホップの最大数を設定するよう *hopcount* を指定します。デフォルトのホップ・カウントは 10 です。
-h *ldaphost*	LDAP サーバーを実行する代替ホストを指定します。
-p *ldapport*	LDAP サーバーが listen する代替伝送制御プロトコル (TCP) ポートを指定します。デフォルトの LDAP ポートは 389 です。この値の指定がなく、**-Z** が指定されている場合は、デフォルトの LDAP Secure Sockets Layer (SSL) ポート 636 が使用されます。
-Z	安全性の高い SSL 接続を使用して LDAP サーバーと通信します。 **-Z** オプションは、このツールの SSL 対応のバージョンでのみサポートされます。
-K *keyfile*	SSL キー・データベース・ファイルの名前を指定します。キー・データベース・ファイルが現行ディレクトリーにない場合は、完全修飾キー・データベース・ファイル名を指定してください。ユーティリティーがキー・データベースを探し出すことができない場合には、デフォルトのトラステッド認証局ルートのハードコーディングされたセットが使われます。キー・データベース・ファイルには、一般に、クライアントが信頼している認証局 (CA) の 1 つまたは複数の証明書が含まれています。これらのタイプの X.509 証明書は、トラステッド・ルートとも呼ばれています。このパラメーターを使用すると、**-Z** スイッチを使用できるようになります。

-P *keyfilepw*	キー・データベースのパスワードを指定します。このパスワードは、キー・データベース・ファイル内の暗号化された情報 (秘密鍵を含む) にアクセスするために必要です。パスワードの stash ファイルがキー・データベース・ファイルに関連付けられている場合、パスワードはその stash ファイルから取得されるので、このパラメーターは必要ありません。 **-Z** と **-K** をどちらも指定していない場合は、このパラメーターは無視されます。
-N *certificatename*	キー・データベース・ファイル内のクライアント証明書に関連したラベルを指定します。 LDAP サーバーが Server Authentication (サーバー認証) だけを実行するように設定されている場合は、クライアント証明書は不要です。 LDAP サーバーが Client and Server Authentication (クライアントおよびサーバーの認証) を実行するように設定されている場合は、クライアント証明書が必要です。デフォルトの証明書 / 秘密鍵のペアがデフォルトとして指定されている場合は、 *certificatename* は不要です。同様に、指定したキー・データベース・ファイル内に証明書 / 秘密鍵のペアが 1 つある場合も、 *certificatename* は不要です。 **-Z** と **-K** をどちらも指定していない場合は、このパラメーターは無視されます。
-b *searchbase*	デフォルトの代わりに、*searchbase* を検索の開始点として使用します。 **-b** を指定しないと、ユーティリティーは、 LDAP_BASEDN 環境変数で *searchbase* の定義を調べます。
-s *scope*	検索の範囲を指定します。 *scope* は、base、one、 sub のいずれかです。これは、それぞれ、基本オブジェクト検索、1 レベル検索、サブツリー検索を意味します。デフォルトは sub です。
-a *deref*	別名の参照解除をどのように行うかを指定します。 *deref* は、 never、 always、 search、find のいずれかです。これは、それぞれ、どのようなときも別名を参照解除しない、常に参照解除する、検索時に参照解除する、検索対象の基本オブジェクトを見つけるときのみ参照解除する、を意味します。デフォルトでは、別名は参照解除されません。
-l *timelimit*	最大 *timelimit* 秒が経過するまで、検索が完了するのを待ちます。
-z *sizelimit*	検索結果の項目数を最大 *sizelimit* に制限します。これにより、検索操作で戻される項目数の上限を設定できます。
filter	検索に使用するフィルターの名前を指定します。
attrs...	検索で 1 つまたは複数の項目が見つかった場合に、ユーティリティーが取り出す属性を指定します。 *attrs* に値を指定しなかった場合は、ユーティリティーはすべての属性を戻します。

例: ldapsearch

例 1:

コマンド ldapsearch cn=john doe cn telephoneNumber は、 john doe という commonName を持つ項目を見つけるために、サブツリー検索を実行します (デフォルトの検索ベースを使用)。この検索により、commonName の値と telephoneNumber の値が取り出され、標準出力に出力されます。検索により 2 つの項目が見つかった場合は、出力は次のようになります。

```
cn=John E Doe, ou=College of Literature, Science, and the Arts,
ou=Students, ou=People, o=University of Higher Learning, c=US
cn=John Doe
cn=John Edward Doe
cn=John E Doe 1
cn=John E Doe
telephoneNumber=+1 313 555-5432

cn=John B Doe, ou=Information Technology Division,
```

```
ou=Faculty and Staff,
ou=People, o=University of Higher Learning, c=US
cn=John Doe
cn=John B Doe 1
cn=John B Doe
telephoneNumber=+1 313 555-1111
```

例 2:

コマンド `ldapsearch -t uid=jed jpegPhoto audio` は、 jed というユーザー ID を持つ項目を見つけるために、デフォルトの検索ベースを使用してサブツリー検索を実行します。この検索により、jpegPhoto と audio の値が取り出されて、一時ファイルに書き込まれます。検索により、要求された各属性について 1 つずつ値を持つ項目が 1 つ見つかった場合、出力は次のようになります。

```
cn=John E Doe,
ou=Information Technology Division,
ou=Faculty and Staff,
ou=People, o=University of Higher Learning, c=US
audio=/tmp/ldapsearch-audio-a19924
jpegPhoto=/tmp/ldapsearch-jpegPhoto-a19924
```

例 3:

コマンド `ldapsearch -L -s one -b c=US o=university* o description` は、 c=US レベルでの 1 レベルの検索を実行します。この検索により、`university` で始まる organizationName を持つすべての組織が検出されます。検索の結果は LDIF 形式で表示されます。検索により、organizationName 属性の値と description 属性の値が取り出されて、標準出力に送られます。出力は次のようになります。

```
dn: o=University of Alaska Fairbanks, c=US
o: University of Alaska Fairbanks
description: Preparing Alaska for a brave new tomorrow
description: leaf node only

dn: o=University of Colorado at Boulder, c=US
o: University of Colorado at Boulder
description: No personnel information
description: Institution of education and research

dn: o=University of Colorado at Denver, c=US
o: University of Colorado at Denver
o: UCD
o: CU/Denver
o: CU-Denver
description: Institute for Higher Learning and Research

dn: o=University of Florida, c=US
o: University of Florida
o: UFl
description: Shaper of young minds
...
```

例 4:

42 ページの『LDAP ディレクトリーの参照』で述べたように、ディレクトリー・サービス LDAP ディレクトリーには参照オブジェクトが含まれていることがあります。これは次のものだけを含むオブジェクトです。

- 識別名 (`dn`)
- objectClass (`objectClass`)
- 参照 (`ref`) 属性

次の例は、参照オブジェクトが含まれている場合の検索を示しています。

System_A には参照項目が含まれています。

```
dn: cn=Barb Jensen, ou=Rochester, o=Big Company, c=US
ref: ldap://System_B:389/cn=Barb Jensen,
  ou=Rochester, o=Big Company, c=US
objectclass: referral
```

この項目に関連したすべての属性は、System_B にあります。

System_B には項目が 1 つ含まれています。

```
dn: cn=Barb Jensen, ou=Rochester, o=Big Company, c=US
cn: Barb Jensen
objectclass: organizationalPerson
sn: Jensen
telephonenumber: (800) 555 1212
```

クライアントが System_A に対して要求を出し、manageDsaIT 制御を送信しないと、サーバーは参照を戻します。たとえば、System_A の LDAP サーバーは、ldapsearch で -M を使用することにより、次の URL でクライアントに応答します。

```
ldap://System_B:389/cn=Barb Jensen,
 ou=Rochester, o=Big Company, c=US
```

クライアントはこの情報を使用して、System_B に対する要求を発行します。 System_A の項目に、dn、objectclass、および ref 以外の属性も含まれている場合は、サーバーはそれらの属性を無視します。

クライアントは、サーバーから参照応答を受け取ると、今度は URL が参照されたサーバーに対して、再度要求を発行します。 1 つのレベルの有効範囲での検索が完了している場合、参照要求では基本有効範囲が使用されます。この検索の結果は、検索の有効範囲 (**-b**) に指定する値によって異なります。

-s sub を次のように指定したとします。

```
ldapsearch -h System_A -b ou=Rochester, o=Big Company, c=US
     -s sub sn=Jensen
```

検索の結果、System_A と System_B の両方の ou=Rochester, o=Big Company, c=US の中またはその下位にあって、 sn=Jensen であるすべての項目のすべての属性が戻されます。クライアントは System_A から参照を受けて System_B を検索し、 cn=Barb Jense,ou=Rochester,o=Big Company,c=US を戻します。

-s one を次のように指定したとします。

```
ldapsearch -h System_A -b ou=Rochester, o=Big Company, c=US
     -s one sn=Jensen
```

検索の結果、どちらのシステムについても項目は戻されません。代わりに、サーバーは参照 URL をクライアントに戻します。

```
ldap://System_B:389/cn=Barb Jensen,
  ou=Rochester, o=Big Company, c=US??base
```

クライアントは次の要求を実行依頼します。

```
 ldapsearch -h System_B -b cn=Barb Jensen, ou=Rochester, o=Big Company, c=US
     -s base sn=Jensen
```

この結果、cn=Barb Jensen,ou=Rochester,o=Big Company,c=US が戻されます。

ldapmodrdn ユーティリティー

ldapmodrdn ユーティリティーを使用すると、 LDAP ディレクトリー・サーバー上の相対識別名 (RDN) の項目を変更できます。このユーティリティーは、 OS/400 の QSH コマンド・シェルから使用します。このユーティリティーでは、 ldap_modrdn アプリケーション・プログラム・インターフェース (API) が使用されます。

形式:

ldapmodrdn [-V] [-r] [-M] [-n] [-v] [-c] [-R] [-C *charset*] **[-d** *debuglevel*] **[-D** *binddn*] **[-w** *passwd*] **[-m** *mechanism*] **[-O** *hopcount*] **[-h** *ldaphost*] **[-p** *ldapport*] **[-Z] [-K** *keyfile*] **[-P** *keyfilepw*] **[-N** *certificatename*] **[-f** *file* **] [***dn rdn***]**

注:

1. コマンド行引き数 *dn* および *rdn* を指定した場合は、 DN で指定された項目の RDN である *dn* が、 *rdn* で置き換えられます。これらの引き数を指定しない場合は、ファイルの内容 (または、 **-f** フラグを指定していない場合は標準入力の内容) は、 1 つまたは複数の項目で構成されます。

   識別名 (DN)

   相対識別名 (RDN)

   各 DN/RDN のペアは 1 つまたは複数のブランク行で区切られます。
2. **-f** オプションを使用して *file* から (またはコマンド行ペア *dn* および *rdn* から) 入力情報を与えなかった場合は、 ldapmodrdn コマンドは標準入力から項目を読み取るまで待機します。この待ち状態を中断するには、SysReq キーを押してから、 **2．前の要求の終了**を選択してください。

診断:

エラーがない場合は、戻り状況は 0 です。エラーがあった場合は、ゼロ以外の戻り状況が発生し、標準エラーに診断メッセージが書き込まれます。

ldapmodrdn ユーティリティーの使用例を表示するには、 ここをクリックしてください。

パラメーター:

-V	ユーティリティーが LDAP サーバーにバインドするために使用する LDAP のバージョンを指定します。デフォルトの設定では、LDAP V3 接続を使用します。明示的に LDAP V3 を選択する場合は -V 3 と指定し、 LDAP V2 アプリケーションとして実行する場合は -V 2 と指定します。
-r	項目から古い相対識別名 (RDN) の値を削除します。デフォルトの設定では古い値が保持されます。
-M	参照オブジェクトを普通の項目として管理します。
-n	何が行われるかを示すだけで、実際には項目の変更は行いません。 **-v** と併用してデバッグに使用すると便利です。
-v	冗長モードを使用して、多くの診断結果を標準出力に書き込みます。
-c	連続オペレーション・モード。エラーが報告されますが、ldapmodrdn は変更を続けます。デフォルトの設定では、エラーの報告後に終了します。
-R	参照を自動的に行わないことを指定します。

-C *charset*	ユーティリティーへの入力として提供されたストリングを、ローカル文字セット (*charset*) で表されるようにし、 UTF-8 に変換されるよう指定します。入力ストリングのコード・ページがジョブのコード・ページ値と異なる場合には、 **-C** 文字セット・オプションを使用します。 サポートされている *charset* 値について調べるには、ldap_set_iconv_local_charset() API に関する資料を参照してください。
-d *debuglevel*	デバッグ・レベルを *debuglevel* にセットします。
-D *binddn*	*binddn* を使用して LDAP ディレクトリーにバインドします。 *binddn* は、ストリング表記の DN です。
-w *passwd*	*passwd* を認証用のパスワードとして使用します。
-m *mechanism*	*mechanism* を使用して、 SASL メカニズムがサーバーへのバインドを使用するよう指定します。 ldap_sasl_bind_s() API が使用されます。使用可能なメカニズムとしては、CRAM-MD5 (パスワードの暗号化)、 EXTERNAL (SSL での使用)、 GSSAPI (Kerberos) があります。 -V 2 をセットすると、-m パラメーターは無視されます。 **-m** を指定しないと、単純認証が使用されます。
-O *hopcount*	参照を追跡する際にクライアント・ライブラリーが取るホップの最大数を設定するよう *hopcount* を指定します。デフォルトのホップ・カウントは 10 です。
-h *ldaphost*	LDAP サーバーを実行する代替ホストを指定します。
-p *ldapport*	LDAP サーバーが listen する代替伝送制御プロトコル (TCP) ポートを指定します。デフォルトの LDAP ポートは 389 です。この値の指定がなく、**-Z** が指定されている場合は、デフォルトの LDAP SSL ポート 636 が使用されます。
-Z	安全性の高い SSL 接続を使用して LDAP サーバーと通信します。 **-Z** オプションは、このツールの SSL 対応のバージョンでのみサポートされます。
-K *keyfile*	SSL キー・データベース・ファイルの名前を指定します。キー・データベース・ファイルが現行ディレクトリーにない場合は、完全修飾キー・データベース・ファイル名を指定してください。ユーティリティーがキー・データベースを探し出すことができない場合には、デフォルトのトラステッド認証局ルートのハードコーディングされたセットが使われます。キー・データベース・ファイルには、一般に、クライアントが信頼している認証局 (CA) の 1 つまたは複数の証明書が含まれています。これらのタイプの X.509 証明書は、トラステッド・ルートとも呼ばれています。このパラメーターを使用すると、**-Z** スイッチを使用できるようになります。
-P *keyfilepw*	キー・データベースのパスワードを指定します。このパスワードは、キー・データベース・ファイル内の暗号化された情報 (秘密鍵を含む) にアクセスするために必要です。パスワードの stash ファイルがキー・データベース・ファイルに関連付けられている場合、パスワードはその stash ファイルから取得されるので、このパラメーターは必要ありません。 **-Z** と **-K** をどちらも指定していない場合は、このパラメーターは無視されます。
-N *certificatename*	キー・データベース・ファイル内のクライアント証明書に関連したラベルを指定します。 LDAP サーバーが Server Authentication (サーバー認証) だけを実行するように設定されている場合は、クライアント証明書は不要です。 LDAP サーバーが Client and Server Authentication (クライアントおよびサーバーの認証) を実行するように設定されている場合は、クライアント証明書が必要です。デフォルトの証明書 / 秘密鍵のペアがデフォルトとして指定されている場合は、 *certificatename* は不要です。同様に、指定したキー・データベース・ファイル内に証明書 / 秘密鍵のペアが 1 つある場合も、*certificatename* は不要です。 **-Z** と **-K** をどちらも指定していない場合は、このパラメーターは無視されます。
-f *file*	標準入力またはコマンド行 (*dn* および新しい *rdn* を指定) からではなく、 LDIF ファイルから項目の変更情報を読み取ります。標準入力をファイル (< file) から取り込むこともできます。

dn rdn	名前変更する項目の識別名と、その項目の新しい相対識別名を指定します。

例: ldapmodrdn

すでにテキスト・ファイル **/tmp/entrymods** が作成されており、その内容が次のとおりであるとします。

```
cn=Modify Me, o=University of Life, c=US
cn=The New Me
```

次のコマンドを使用したとします。

```
ldapmodrdn -r -f /tmp/entrymods
```

このコマンドは、Modify Me 項目の RDN を、 Modify Me から The New Me に変更します。古い cn である Modify Me は削除されます。

LDAP コマンド行ユーティリティーで SSL を使用する上での注意事項™

コマンド行ユーティリティーの Secure Sockets Layer (SSL) 機能を使用するには、いずれかの暗号アクセス・プロバイダー製品 (5722-ACx) をインストールしておく必要があります。

44 ページの『LDAP ディレクトリー・サーバーで Secure Sockets Layer (SSL) と Translation Layer Security を使用する』には、ディレクトリー・サービス LDAP サーバーでの SSL の使用についての説明があります。この情報には、ディジタル認証マネージャーによるトラステッド認証局の管理および作成に関する説明も含まれます。

クライアントがアクセスする一部の LDAP サーバーは、サーバー認証しか使用しません。そのような場合には、証明書登録リストに 1 つまたは複数のトラステッド・ルート証明書を定義しておけば、サーバー認証において、クライアントは、ターゲットの LDAP サーバーがトラステッド認証局 (CA) の 1 つから証明書の発行を受けていることを確認できます。また、サーバーとの SSL 接続を介して流れるすべての LDAP トランザクションは暗号化されます。これには、ディレクトリー・サーバーにバインドするために使用するアプリケーション・プログラム・インターフェース (API) で提供される LDAP 認証が含まれます。たとえば、LDAP サーバーが保証付き Verisign 証明書を使用している場合は、次のことを行ってください。

1. Verisign から CA 証明書を取得する。
2. ディジタル認証マネージャー (DCM) により、取得した CA 証明書を証明書登録リストにインポートする。
3. DCM により、取得した CA 証明書に「承認済み」であることを示すマークを付ける。

LDAP サーバーが非公開のサーバー証明書を使用している場合は、サーバーの管理者からサーバーの証明書要求ファイルのコピーを取得することができます。証明書要求ファイルを取得したら、証明書登録リストにインポートして、「承認済み」であることを示すマークを付けてください。

シェル・ユーティリティーを使用して、クライアント認証とサーバー認証の両方を使用する LDAP サーバーにアクセスする場合は、次のことをする必要があります。

- 証明書登録リストに 1 つまたは複数のトラステッド・ルート証明書を定義する。これにより、クライアントは、ターゲットの LDAP サーバーがトラステッド CA の 1 つから証明書の発行を受けていることを確認できます。また、サーバーとの SSL 接続を介して流れるすべての LDAP トランザクションは暗号化されます。これには、ディレクトリー・サーバーにバインドするために使用するアプリケーション・プログラム・インターフェース (API) で提供される LDAP 認証が含まれます。

- キーの対を作成し、CA からのクライアント証明書を要求する。 CA から承認済み証明書を受け取ったら、その証明書をクライアントのキー・リング・ファイルに登録してください。

第 7 章 ディレクトリー・サービスのトラブルシューティング

ディレクトリー・サービスの LDAP のような信頼性の高いサーバーでも、ときには問題が起きることがあります。 LDAP ディレクトリー・サーバーに問題が起きたときは、その原因と解決方法を突き止めるのに次の情報が役立ちます。

- 『ディレクトリー・サービスに関する基本的なトラブルシューティング手順』
- 72 ページの『LDAP クライアントに関する一般的なエラー』

ディレクトリー・サービスの一般的な問題の詳細については、以下の URL にあるディレクトリー・サービスのホーム・ページ  を参照してください。

```
http://www.iseries.ibm.com/ldap
```

ディレクトリー・サービスに関する基本的なトラブルシューティング手順

LDAP エラーの戻りコードは、ldap.h ファイルの中にあります。このファイルは、システムの QSYSINC/H.LDAP に入っています。

LDAP ディレクトリー・サーバーにエラーが起き、それについて詳細を知りたいときは、 QDIRSRV ジョブ・ログを表示してください。エラーが繰り返し発生する場合は、 TCP/IP アプリケーションのトレース (TRCTCPAPP APP(*DIRSRV)) コマンドを使用して、エラーのトレースを実行することができます。詳細については、 71 ページの『TRCTCPAPP を使用して問題を検出する』を参照してください。

ディレクトリー・サービスは、いくつかの SQL (構造化照会言語) サーバーを使用します。 SQL エラーが発生すると、通常次のメッセージが QDIRSRV ジョブ・ログに記録されます。

```
SQL error -1 occurred
```

このような場合、QDIRSRV ジョブ・ログには、 SQL サーバー・ジョブ・ログに対する参照が含まれています。しかし、場合によっては、問題の原因が SQL サーバーであっても、 QDIRSRV にこのメッセージと参照が含まれていないこともあります。その場合は、どの SQL サーバーを開始するか、および ディレクトリー・サービスがそれらのサーバーを何のために使用するかが分かっていると便利です。

LDAP ディレクトリー・サーバーは、正常に始動すると次のようなメッセージを生成します。

注: 開始される SQL サーバー・ジョブのメッセージとジョブ数は、以下に示す場合によって変わってきます。

- はじめてサーバーを始動している場合。
- マイグレーションする必要がある場合。
- サーバーが変更ログを使用している場合。
- サーバーが多数のデータベース接続を許可する設定になっている場合。

```
                                                    System:   WARMERS
 Job . . :   QDIRSRV       User . . :   QDIRSRV       Number . . . :   174440

  >> CALL PGM(QSYS/QGLDSVR)
     Job 057448/QUSER/QSQSRVR used for SQL server mode processing.
     Job 057340/QUSER/QSQSRVR used for SQL server mode processing.
     Job 057448/QUSER/QSQSRVR used for SQL server mode processing.
     Job 057166/QUSER/QSQSRVR used for SQL server mode processing.
     Job 057279/QUSER/QSQSRVR used for SQL server mode processing.
  Job 057288/QUSER/QSQSRVR used for SQL server mode processing.
     Directory Services server started successfully.
```

ディレクトリー・サービスは、LDAP サーバーの始動時に、第 1 の SQL サーバーである 057448/QUSER/QSQSRVR を使用します。ディレクトリー・サービスは、はじめてサーバーを始動している場合、マイグレーションする必要がある場合、またはサーバーが変更ログを使用している場合、 LDAP サーバーの始動時に、必要に応じてさらに LDAP サーバーを始動することがあります。始動後に、これらの SQL サーバーは除去されます。

この例では、マイグレーションまたはサーバーの始動で追加の SQL サーバーは使用されておらず、変更ログは構成されていません。ディレクトリー・サービスは、次の SQL サーバー (057340/QUSER/QSQSRVR) を複製に使用します。

add、modify、modrdn、および delete 操作には、この例の最後の接続 (057288/QUSER/QSQSRVR) が使用されます。他の接続は、search、bind、および compare に使用されます。

iSeries ナビゲーターにあるディレクトリー・サーバーの **「データベース / 接尾部」** プロパティー・ページで、サーバーの始動後のディレクトリー操作にディレクトリー・サービスが使用する SQL サーバーの合計数を指定します。なお、常に 1 つの SQL サーバーが複製用に構成されている必要があります。

ディレクトリー・サービスのジョブ・ログによりエラーおよびアクセスをモニターする

LDAP サーバー用のジョブ・ログを表示することにより、エラーの有無を確認し、サーバー・アクセスを監視することができます。

サーバーがすでに開始されているときに、QDIRSRV ジョブ・ログを見るには、次のようにしてください。
1. iSeries ナビゲーターで**「ネットワーク」**を展開する。
2. **「サーバー」**を展開する。
3. **「TCP/IP」**をクリックする。
4. **「ディレクトリー」**を右クリックし、**「Server Jobs (サーバーのジョブ)」**を選択する。
5. **「File (ファイル)」**メニューで、**「Job Log (ジョブ・ログ)」**を選択する。

サーバーが停止しているときに QDIRSRV ジョブ・ログを見るには、次のようにしてください。
1. iSeries ナビゲーターで**「基本操作」**を展開する。
2. **「プリンター出力」**をクリックする。
3. iSeries ナビゲーターの右パネルの**「ユーザー」**列に QDIRSRV が表示される。ジョブ・ログを表示するには、同じ行の QDIRSRV の左にある**「Qpjoblog」**をダブルクリックする。

   注: iSeries ナビゲーターは、スプール・ファイルだけを表示するように設定されている場合があります。リストに QDIRSRV が表示されていない場合は、**「プリンター出力」**をクリックし、**「オプション」**メニューから**「組み込み」**を選択します。**「ユーザー」**フィールドに **「すべて (ALL)」**を指定し、**「OK」**をクリックします。

注: 実行するタスクによっては、ディレクトリー・サービスは他のシステム・リソースを使用します。このようなリソースにエラーが起きた場合は、ジョブ・ログから、関連の情報がどこにあるかを知ることができます。場合によっては、ディレクトリー・サービスは関連情報がどこにあるかを判別できないこともあります。その場合は、SQL (構造化照会言語) サーバーのジョブ・ログを見て、問題が SQL サーバーに関連するものでないかどうかを確認してください。

TRCTCPAPP を使用して問題を検出する

サーバーには、通信回線上のデータを収集する、ローカル・エリア・ネットワーク (LAN) や広域ネットワーク (WAN) インターフェースなどの通信トレースがあります。標準的なユーザーには、トレース・データの内容をすべては理解できないかもしれません。ただし、2 点間のデータ交換が実際に行われたかどうかはトレース項目を使用して判別できます。

クライアントまたはアプリケーションにおける問題を見つけるには、LDAP ディレクトリー・サーバーで、 TCP/IP アプリケーションのトレース (TRCTCPAPP) コマンドに *DIRSRV オプションを指定して使用することができます。

LDAP での TRCTCPAPP コマンドの使用に関する詳細と、必須権限に関する制約事項については、TRCTCPAPP (TCP/IP アプリケーションのトレース) コマンドの説明を参照してください。

通信トレースの使用に関する一般情報については、 通信トレースを参照してください。

LDAP_OPT_DEBUG オプションを使用してエラーをトレースする

| V5R2 からは、**ldap_set_option()** API の LDAP_OPT_DEBUG オプションを使用して、 LDAP C API を
| 使用しているクライアントの問題をトレースできます。デバッグ・オプションには、これらのアプリケーション
| の問題のトラブルシューティングに役立てられる、複数のデバッグ・レベルの設定があります。

| 以下は、クライアントのトレースのデバッグ・オプションを使用可能にする例です。

```
| int debugvalue= LDAP_DEBUG_TRACE | LDAP_DEBUG_PACKETS;
| ldap_set_option(  ld, LDAP_OPT_DEBUG, &debugvalue);
```

| デバッグ・レベルを設定する別の方法は、クライアント・アプリケーションが実行しているジョブの
| LDAP_DEBUG 環境変数の数値を、 **ldap_set_option()** API を使用する場合の debugvalue と同じ数値に構成
| する方法です。

| LDAP_DEBUG 環境変数を使用してクライアント・トレースを使用可能にする例は、以下のとおりです。

```
| ADDENVVAR ENVVAR(LDAP_DEBUG) VALUE(0x0003)
```

| 問題の発生元のクライアントを実行した後は、 iSeries プロンプトで以下を入力します。

```
| DMPUSRTRC ClientJobNumber
```

| ここで ClientJobNumber はクライアント・ジョブの数です。

| この情報を対話式に表示するには、 iSeries プロンプトで以下を入力します。

```
| DSPPFM QAPOZDMP QPOZnnnnnn
```

| nnnnnn はジョブの数です。

| この情報をサービスに送信するために保管するには、以下のステップを実行します。
| 1. SAVF の作成 (CRTSAVF) コマンドを使用して SAVF ファイルを作成する。
| 2. iSeries コマンド・プロンプトで以下を入力する。

```
|    SAVOBJ OBJ(QAPOZDMP LIB(QTEMP) DEV(*SAVF) SAVF(xxx)
```

| ここで *xxx* は、SAVF ファイルに指定した名前です。

LDAP クライアントに関する一般的なエラー

LDAP クライアントに関する一般的なエラーの原因が分かっていると、サーバーに関する問題を解決するのに役立ちます。 LDAP クライアントのエラー状態に関する完全なリストについては、 iSeries Information Center の「プログラミング」の下にある OS/400 ディレクトリー・サービスというトピックを参照してください。

クライアント・エラー・メッセージの形式は次のとおりです。

```
[Failing LDAP operation]:[LDAP client API error conditions]
```

注: 以降に示すエラーの説明は、クライアントが OS/400 上の LDAP サーバーと通信していることを前提としています。異なるプラットフォーム上のサーバーと通信しているクライアントでも同様のエラーが発生することがありますが、その場合におけるエラーの原因と対処方法は異なるものと思われます。

一般的なメッセージには次のものがあります。

- 『ldap_search: Timelimit exceeded (時間制限を超えました)』
- 『[Failing LDAP operation]: Operations error (LDAP 操作失敗: 操作エラー)』
- 『ldap_bind: No such object (該当のオブジェクトがありません)』
- 73 ページの『ldap_bind: Inappropriate authentication (認証に誤りがあります)』
- 73 ページの『[Failing LDAP operation]: Insufficient access (LDAP 操作失敗: アクセス権が不十分です)』
- 73 ページの『[failing LDAP operation]: Cannot contact LDAP server (LDAP 操作失敗: LDAP サーバーに接続できません)』
- 73 ページの『[failing LDAP operation]: Failed to connect to ssl server (LDAP 操作失敗: SSL サーバーに接続できませんでした)』

ldap_search: Timelimit exceeded (時間制限を超えました)

このエラーは、ldapsearche の実行速度が遅いときに起こります。このエラーを訂正するには、次のどちらか、または両方の処置を行います。

- LDAP ディレクトリー・サーバーの検索時間最大値を大きくする。詳細については、 35 ページの『LDAP ディレクトリー・サーバーのパフォーマンスを調整する』を参照してください。
- システム上の活動量を少なくする。実行中の LDAP クライアント・ジョブの数を減らすという方法もあります。

[Failing LDAP operation]: Operations error (LDAP 操作失敗: 操作エラー)

このエラーが生成される原因はいくつかあります。特定の状況においてこのエラーが発生する原因については、 69 ページの『ディレクトリー・サービスに関する基本的なトラブルシューティング手順』に記載されている QDIRSRV および構造化照会言語 (SQL) サーバーのジョブ・ログを参照してください。

ldap_bind: No such object (該当のオブジェクトがありません)

このエラーが起こる主な原因は、操作を実行する際に犯す入力ミスです。別の主な原因としては、 LDAP クライアントが実際には存在しない DN にバインドしようとすることがあります。これは、ユーザーが誤って管理者 DN と考えるものを指定するときによく生じます。たとえば、実際の管理者 DN がたとえば cn=Administrator であるにもかかわらず、ユーザーは `QSECOFR` または `Administrator` を指定する場合があります。

エラーの詳細については、 69 ページの『ディレクトリー・サービスに関する基本的なトラブルシューティング手順』の説明に従って、QDIRSRV ジョブ・ログを調べてください。

ldap_bind: Inappropriate authentication (認証に誤りがあります)

パスワードまたはバインド DN が正しくないと、サーバーは無効な信任状を戻します。クライアントが以下のいずれかとしてバインドを試みると、サーバーは不適切な認証を戻します。

- userpassword 属性を持たない項目
- UID 属性を持ち、userpassword 属性を持たない OS/400 ユーザーを表す項目。これによって、指定されたパスワードと OS/400 ユーザー・パスワードの比較が行われますが、これらは一致しません。
- プロジェクト・ユーザーと、単純以外のバインド方式が要求されていることを表す項目。

このエラーは、通常、クライアントが無効なパスワードを使ってバインドしようとした場合に発生します。エラーの詳細については、 69 ページの『ディレクトリー・サービスに関する基本的なトラブルシューティング手順』の説明に従って、QDIRSRV ジョブ・ログを調べてください。

[Failing LDAP operation]: Insufficient access (LDAP 操作失敗: アクセス権が不十分です)

このエラーは、通常、バインドの実行元 DN に、クライアントが要求している操作 (追加または削除など) を実行するための権限がない場合に発生します。エラーの詳細については、 69 ページの『ディレクトリー・サービスに関する基本的なトラブルシューティング手順』の説明に従って、QDIRSRV ジョブ・ログを調べてください。

[failing LDAP operation]: Cannot contact LDAP server (LDAP 操作失敗: LDAP サーバーに接続できません)

このエラーは、通常、次のことが原因で発生します。

- 指定のシステムの LDAP サーバーが開始されて選択待ちの状態になる前に、 LDAP クライアントが要求を出した。
- ユーザーが無効なポート番号を指定した。たとえば、サーバーがポート 386 で listen しているときに、クライアントが要求時にポート 387 を使用しようとした場合に発生します。

エラーの詳細については、 69 ページの『ディレクトリー・サービスに関する基本的なトラブルシューティング手順』の説明に従って、QDIRSRV ジョブ・ログを調べてください。ディレクトリー・サービス・サーバーが正常に開始されている場合は、 Directory Services server started successfully (ディレクトリー・サービス・サーバーが正常に開始されました) というメッセージが QDIRSRV ジョブ・ログに記録されます。

[failing LDAP operation]: Failed to connect to ssl server (LDAP 操作失敗: SSL サーバーに接続できませんでした)

このエラーは、安全性の高いソケット接続を確立することができないため、 LDAP サーバーがクライアントからの接続要求を拒否したときに起こります。原因としては、次のいずれかが考えられます。

- クライアントがサーバーに接続しようとしたところ、認証管理サポートによって接続が拒否された。ディジタル認証マネージャーを使用して、証明書が正しく設定されているかどうかを確認してから、サーバーを再始動して、再び接続を試みてください。
- ユーザーが *SYSTEM 証明書ストア (デフォルトでは /QIBM/userdata/ICSS/Cert/Server/default.kdb) に対する読み取りアクセスを持っていない可能性がある。

OS/400 C アプリケーションの場合は、 SSL エラー情報がさらに存在します。詳細については、 ディレクトリー・サービスの各 API の資料を参照してください。

Printed in Japan

日本アイ・ビー・エム株式会社
〒106-8711　東京都港区六本木3-2-12