



System i

Directory Server

IBM Tivoli Directory Server for i5/OS (LDAP)

バージョン 6 リリース 1





System i

Directory Server

IBM Tivoli Directory Server for i5/OS (LDAP)

バージョン 6 リリース 1

ご注意！

本書および本書で紹介する製品をご使用になる前に、349 ページの『特記事項』に記載されている情報をお読みください。

本書は、IBM i5/OS (製品番号 5761-SS1) バージョン 6、リリース 1 モディフィケーション 0 に適用されます。また、改訂版で断りがない限り、それ以降のすべてのリリースおよびモディフィケーションにも適用されます。このバージョンは、すべての RISC モデルで稼働するとは限りません。また CISC モデルでは稼働しません。

IBM 発行のマニュアルに関する情報のページ

<http://www.ibm.com/jp/manuals/>

こちらから、日本語版および英語版のオンライン・ライブラリーをご利用いただけます。また、マニュアルに関するご意見やご感想を、上記ページよりお送りください。今後の参考にさせていただきます。

(URL は、変更になる場合があります)

お客様の環境によっては、資料中の円記号がバックスラッシュと表示されたり、バックスラッシュが円記号と表示されたりする場合があります。

| | |
|-----|---|
| 原典： | System i Directory Server IBM Tivoli Directory Server for i5/OS (LDAP) Version 6 Release 1 |
| 発行： | 日本アイ・ピー・エム株式会社 |
| 担当： | ナショナル・ランゲージ・サポート |

目次

| | |
|---|------------|
| IBM Tivoli Directory Server for i5/OS (LDAP) | 1 |
| I V6R1 の新機能 | 1 |
| IBM Tivoli Directory Server for i5/OS (LDAP) の PDF ファイル | 3 |
| Directory Server の概念 | 4 |
| ディレクトリー | 4 |
| I 配布ディレクトリー | 8 |
| 識別名 (DN) | 10 |
| 接尾部 (命名コンテキスト) | 14 |
| スキーマ | 16 |
| ディレクトリー構造の推奨される措置 | 38 |
| 公開 | 40 |
| 複製 | 42 |
| レルムおよびユーザー・テンプレート | 52 |
| 検索パラメーター | 53 |
| 各国語サポート (NLS) に関する考慮事項 | 54 |
| 言語タグ | 55 |
| LDAP ディレクトリーの参照 | 56 |
| トランザクション | 57 |
| Directory Server のセキュリティー | 57 |
| オペレーティング・システム・プロジェクト・バックエンド | 94 |
| Directory Server および i5/OS ジャーナリングのサポート | 101 |
| 固有属性 | 102 |
| 操作属性 | 102 |
| サーバー・キャッシュ | 103 |
| 制御および拡張操作 | 105 |
| 保存と復元に関する考慮事項 | 106 |
| Directory Server の概要 | 106 |
| マイグレーションの考慮事項 | 106 |
| Directory Server の計画 | 112 |
| Directory Server の構成 | 114 |
| ディレクトリーへのデータの取り込み | 115 |
| Web 管理 | 116 |
| Directory Server のシナリオ | 119 |
| シナリオ: Directory Server のセットアップ | 119 |
| シナリオ: HTTP サーバー妥当性検査リストから Directory Server へのユーザーのコピー | 128 |
| Directory Server の管理 | 130 |
| 一般管理タスク | 130 |
| 管理グループのタスク | 150 |
| 検索限界グループのタスク | 152 |
| プロキシー許可グループのタスク | 155 |
| 固有属性タスク | 158 |
| パフォーマンス・タスク | 160 |
| 複製タスク | 164 |
| 複製トポロジー・タスク | 187 |
| セキュリティー・プロパティー・タスク | 196 |
| スキーマ・タスク | 207 |
| ディレクトリー項目タスク | 218 |
| ユーザーとグループのタスク | 227 |
| レルムおよびユーザー・テンプレートのタスク | 230 |
| アクセス制御リスト (ACL) のタスク | 239 |
| 参照 | 244 |
| Directory Server のコマンド行ユーティリティー | 244 |
| I LDAP データ交換形式 (LDIF) | 281 |
| Directory Server 構成スキーマ | 288 |
| オブジェクト ID (OID) | 326 |
| IBM Tivoli Directory Server と同等の製品 | 336 |
| Directory Server のデフォルト構成 | 336 |
| Directory Server のトラブルシューティング | 337 |
| Directory Server のジョブ・ログを使ったエラーおよびアクセスのモニター | 338 |
| TRCTCPAPP を使用した問題の検出 | 339 |
| LDAP_OPT_DEBUG オプションを使用したエラーのトレース | 339 |
| GLEnnnn メッセージ ID | 340 |
| LDAP クライアントに関する一般的なエラー | 343 |
| パスワード・ポリシー関連エラー | 346 |
| QGLDCPYVL API のトラブルシューティング | 347 |
| 関連情報 | 347 |
| 付録. 特記事項 | 349 |
| 商標 | 350 |
| 資料に関するご使用条件 | 351 |

IBM Tivoli Directory Server for i5/OS (LDAP)

IBM® Tivoli® Directory Server for i5/OS® (以降、Directory Server と呼びます) は、Lightweight Directory Access Protocol (LDAP) サーバーを提供する i5/OS の 1 つの機能です。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) で稼働し、インターネット・アプリケーションおよび非インターネット・アプリケーション両方のディレクトリー・サービスとしてよく用いられています。

以下のトピックには、Directory Server を理解し、使用する上で役立つ情報があります。

V6R1 の新機能

IBM Tivoli Directory Server for i5/OS (LDAP) のトピック集に関する新規情報または大幅に変更された情報を一読してください。

複製の競合の解決

複数のマスター・サーバーを擁するネットワークで、競合する変更を自動的に検出して解決する機能が IBM Tivoli® Directory に備えられています。これにより、すべてのサーバー上のディレクトリーの整合性が保たれます。複製の競合が検出されると、競合している変更がサーバー・ログにレポートされるとともに、「遺失物取り扱い」ログ・ファイルにも記録されます。これにより、管理者は消失したデータをリカバリーすることができます。

- 複製の概要
- 遺失物取り扱いログの設定の変更
- 遺失物取り扱いログ・ファイルの表示

ldapmodify コマンド

リジェクトされた項目の書き込み先のファイルを指定するため、`-e errorfile` オプションが `ldapmodify` コマンドに追加されています。加えた変更の前に感嘆符を付けたうえで標準出力に出力するように、`-n` オプションが追加されています。

- `ldapmodify` および `ldapadd`
- LDAP データ交換形式 (LDIF)

マルチスレッド複製

複数のスレッドを使って複製を行うことができます。これにより、複製の総体的なスループットが向上します。

- マルチスレッド複製
- 複製契約

パスワードの暗号化

IBM Tivoli Directory Server には、ディレクトリーへの保管の前にユーザー・パスワード・データを暗号化するための構成オプションが配備されています。この暗号化オプションを使用すれば、正規のディレクトリー・ユーザーに加えて管理ディレクトリー・ユーザーからの平文パスワード・データへのアクセスを防止できます。

- | • パスワードの暗号化
- | • パスワード・ポリシー・プロパティの設定

| **IBMAttributeTypes 属性**

| IBM Tivoli Directory Server 6.0 では、属性の最初の 128 文字を使用してテーブル名を作成することができます。

- | • IBMAttributeTypes 属性

| **許可されないスキーマの変更**

| スキーマを変更すれば、列のサイズを大きくすることができます。これにより、Web 管理または ldapmodify ユーティリティーを使用したスキーマの変更を通して、属性の最大長を増大することができます。

- | • 許可されないスキーマの変更

| **配布ディレクトリー**

| IBM Tivoli Directory Server は、配布ディレクトリーとして機能します。プロキシ・サーバーとの結合により、配布ディレクトリーのフィーチャーでは、一連のディレクトリーを 1 つのディレクトリーとみなすことができます。配布ディレクトリーのフィーチャーは、プロキシ・サーバーのフィーチャーと連携して、ディレクトリー・デプロイメントでの数百万件の項目の保管を可能にします。

- | • 配布ディレクトリー

| **ldapmodrdn**

| IBM Tivoli Directory Server は、リーフ・ノード上の newsuperior 属性を持った modifyDN をサポートします。

- | • ldapmodrdn

| **TRCTCPAPP を使用した問題の検出**

| TRCTCPAPP コマンドを使用して、アクティブなサーバー・インスタンスをトレースすることができます。

- | • TRCTCPAPP を使用した問題の検出

| **プロジェクト・ユーザーへの読み取りアクセス**

| ユーザー・プロジェクト・バックエンドを対象としたすべての検索操作を禁止することができます。

- | • LDAP 操作
- | • プロジェクト・ユーザーへの読み取りアクセス

| **複数のサーバー・インスタンス**

| i5/OS® システム上に複数の Directory Server を置くことができます。それぞれのサーバーが、いわゆるインスタンスになります。前のリリースの i5/OS で Directory Server を使用していた場合、それは、QUSRDIR という名前のインスタンスにマイグレーションされます。Directory Server の複数のインスタンスを作成して、アプリケーションがそれらのサービスを受けられるようにすることができます。

- | • インスタンスの管理
- | • Directory Server の構成

マイグレーションに関する考慮事項

- IBM Tivoli Directory Server は、最初の始動時に、さらに新しいバージョンにアップグレードされます。
- V5R4 または V5R3 からの V6R1 へのマイグレーション

パスワード・ポリシー

- 認証障害数が多すぎる場合、管理アカウントをロックすることができます。このフィーチャーは、リモート・クライアント接続に対してのみ用いることができます。そのアカウントは、サーバーの始動時にリセットされます。アカウントを管理ロックできるように新しい属性が定義されています。

- 管理パスワードおよびロックアウトのポリシーの設定
- パスワード・ポリシー・プロパティの設定

- オープン (使用可能)、ロック済み、または期限切れといった、特定のアカウントの状況の取り出しのために、拡張操作であるアカウント状況要求が用意されています。

- ldapexop



その他

- IBM® Tivoli® Directory Server と同等の製品: V6R1 Directory Server は、IBM Tivoli Directory Server バージョン 6.0 と同等です。

- Tivoli Software Information Center

新規または変更箇所の確認方法

- 技術的な変更が加えられた箇所には、その箇所が識別できるように、この情報では以下のイメージが使用されています。

-  イメージは、新規情報または変更された情報が始まる個所を示します。
-  イメージは、新規情報または変更された情報が終わる個所を示します。

- PDF ファイルの場合、新規および変更された情報の左マージンには、リビジョン・バー (I) が付いています。

- このリリースでの新機能または変更点に関する他の情報を調べるには、プログラム資料説明書を参照してください。

IBM Tivoli Directory Server for i5/OS (LDAP) の PDF ファイル

IBM Tivoli Directory Server for i5/OS (LDAP) の PDF ファイルを表示および印刷することができます。

本書の PDF 版を表示またはダウンロードするには、IBM Tivoli Directory Server for i5/OS (LDAP) を選択します。

その他の情報


関連資料および IBM Redbooks 資料の PDF を表示または印刷するには、347 ページの『関連情報』を参照してください。

PDF ファイルの保管

表示または印刷のために PDF ファイルをワークステーションに保存するには、以下のようにします。

1. ご使用のブラウザで該当の PDF リンクを右クリックする。
2. PDF をローカル側で保存するオプションをクリックする。
3. PDF ファイルを保存したいディレクトリーに進む。
4. 「保存」をクリックする。

Adobe Reader のダウンロード

これらの PDF を表示または印刷するには、お客様のシステムに Adobe Reader をインストールする必要があります。Adobe Web サイト (www.adobe.com/products/acrobat/readstep.html)  から無償でコピーをダウンロードできます。

Directory Server の概念

Directory Server の概念に関する情報。

Directory Server は、Internet Engineering Task Force (IETF) LDAP V3 仕様をインプリメントします。Directory Server には、機能およびパフォーマンスの領域において IBM により追加された拡張機能も組み込まれています。このバージョンでは、IBM DB2 Universal Database™ for iSeries™ を補助ストレージとして使用し、LDAP 操作ごとのトランザクションの健全性、ハイパフォーマンス操作、およびオンラインのバックアップと復元の機能を提供します。また、IETF LDAP V3 ベースのクライアントと相互運用します。

ディレクトリー

Directory Server は、i5/OS 統合ファイル・システムの編成に類似した方法で情報を階層構造に保管するタイプのデータベースへのアクセスを許可します。

オブジェクトの名前が既知である場合、その特性を検索できます。特定の個別のオブジェクトの名前が既知でない場合、ディレクトリーを検索して特定の要件を満たすオブジェクトのリストを作成できます。通常、ディレクトリーは、事前定義されたカテゴリーのセットによってだけでなく、特定の基準によって検索されます。

ディレクトリーは、汎用リレーショナル・データベースとは異なる特性を持つ特殊なデータベースです。ディレクトリーの特性の 1 つは、更新 (書き込み) よりもアクセス (読み取りまたは検索) されることがはるかに多いという点です。ディレクトリーは高容量の読み取り要求をサポートできなければならないため、通常それは読み取りアクセス向けに最適化されています。ディレクトリーは、汎用のデータベースほど多くの機能を備えていないので、大規模な分散環境で、より多くのアプリケーションに対して、ディレクトリー・データへの高速アクセスを低コストで提供できるように最適化できます。

ディレクトリーは、中央型または分散型となります。ディレクトリーが中央型の場合、ディレクトリーへのアクセスを提供するディレクトリー・サーバー (またはサーバー・クラスター) は、1 つの場所に 1 台となります。ディレクトリーが分散型の場合、ディレクトリーへのアクセスを提供するサーバーは複数あり、通常地理的に分散しています。

ディレクトリーが分散型のとき、ディレクトリーに保管されている情報は、区画化されるか複製されます。情報が区画化される場合、各ディレクトリー・サーバーは、情報の固有かつオーバーラップしないサブセットを保管します。すなわち、各ディレクトリー項目は、1 台のサーバーのみにより保管されます。ディレク

トリーを区画化するために使用する技法は、LDAP 参照です。LDAP 参照を使用すれば、ユーザーは、Lightweight Directory Access Protocol (LDAP) 要求の参照先として、異なる (または同じ) サーバーに保管されている同じネーム・スペースまたは異なるネーム・スペースのいずれかを指定できます。情報が複製される場合、同じディレクトリー項目が複数のサーバーにより保管されます。分散ディレクトリーでは、一部の情報が区画化され、一部の情報が複製される可能性があります。

LDAP ディレクトリー・サーバー・モデルは、項目 (オブジェクトともいう) を基に構成されています。各項目は、1 つ以上の属性 (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。

6 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、ディレクトリー構造と内容を決定する 1 組の規則です。Web 管理ツールを使用してスキーマを表示することができます。

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。

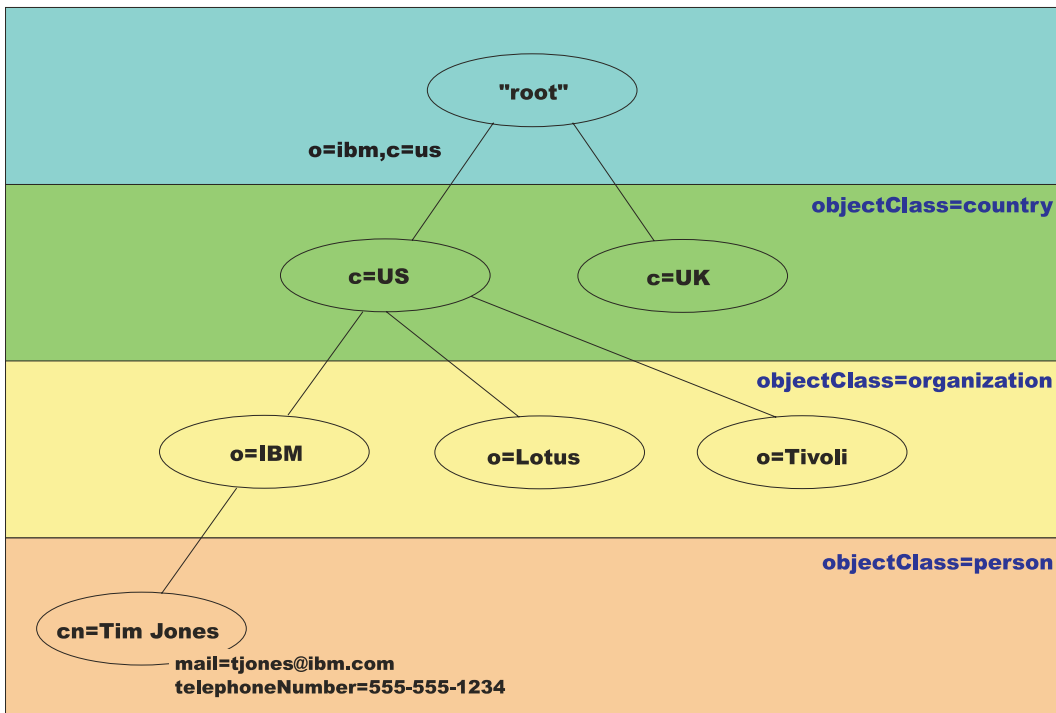
スキーマにより定義された属性に加えて、項目にもサーバーが保守する 1 組の属性があります。操作属性と呼ばれるこれらの属性には、項目が作成された時やアクセス制御情報などが含まれます。

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 (6 ページの図 1 を参照)。階層の最上位には国または地域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。

LDAP は、識別名 (DN) で項目を参照します。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、6 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、6 ページの図 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。

LDAP ディレクトリー構造



RV4Q100-1

図1. LDAP ディレクトリー構造

ディレクトリー構造を作成する際には、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きました。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。

ここで、名前、電話番号、および E メール・アドレスなどの従業員データを含むドメイン・コンポーネント構造を使用するディレクトリーを作成するとします。TCP/IP ドメインを基にした接尾部または命名コンテキストを使用します。このディレクトリーを視覚化すると、以下の図のようなものになります。

```

/
|
+- ibm.com
  |
  +- employees
    |
    +- Tim Jones
      |
      | 555-555-1234
      | tjones@ibm.com
    +- John Smith
      |
      | 555-555-1235
      | jsmith@ibm.com
  
```

Directory Server に入力すると、このデータは実際には以下ようになります。

```

# suffix ibm.com
dn: dc=ibm,dc=com
  objectclass: top
  objectclass: domain
dc: ibm

```

```

# employees directory
dn: cn=employees,dc=ibm,dc=com
  objectclass: top
objectclass: container
cn: employees

# employee Tim Jones
dn: cn=Tim Jones,cn=employees,dc=ibm,dc=com
  objectclass: top
    objectclass: person
objectclass: organizationalPerson
objectclass: inetOrgPerson
objectclass: publisher
objectclass: ePerson
cn: Tim Jones
cn: "Jones, Tim"
sn: Jones
givenname: Tim
telephonenumber: 555-555-1234
mail: tjones@ibm.com

# employee John Smith
dn: cn=John Smith,cn=employees,dc=ibm,dc=com
  objectclass: top
    objectclass: person
objectclass: organizationalPerson
objectclass: inetOrgPerson
objectclass: publisher
objectclass: ePerson
  cn: John Smith
cn: "Smith, John"
sn: Smith
givenname: John
telephonenumber: 555-555-1235
mail: jsmith@ibm.com

```

各項目に `objectclass` と呼ばれる属性値が含まれていることに注意してください。 `objectclass` 値は、項目内で許可される属性 (`telephonenumber`、`givenname` など) を定義します。許可されたオブジェクト・クラスはスキーマで定義されます。スキーマは、データベースで許可された項目のタイプを定義する 1 組の規則です。

ディレクトリー・クライアントおよびサーバー

ディレクトリーは、通常、クライアント/サーバー・モデルの通信を使用してアクセスされます。クライアントおよびサーバー・プロセスは、同じマシン上にある場合と、そうでない場合があります。1 つのサーバーで多くのクライアントにサービスを提供できます。ディレクトリー内の情報に読み書きをするアプリケーションは、直接ディレクトリーにアクセスしません。その代わりに、メッセージを別のプロセスに送信する機能またはアプリケーション・プログラミング・インターフェース (API) を呼び出します。この 2 番目のプロセスが、要求しているアプリケーションの代わりにディレクトリー内の情報にアクセスします。読み取りまたは書き込みの結果は、要求しているアプリケーションにその後戻されます。

API は、サービスにアクセスするために特定のプログラム言語が使用するプログラミング・インターフェースを定義します。クライアントとサーバーの間で交換されたメッセージの形式および内容は、プロトコルでの取り決めに従う必要があります。LDAP は、ディレクトリー・クライアントおよびディレクトリー・サーバーにより使用されるメッセージ・プロトコルを定義します。さらに、C 言語用の関連した LDAP API、および Java Naming and Directory Interface (JNDI) を使用して Java アプリケーションからディレクトリーにアクセスする方法もあります。

ディレクトリーのセキュリティ

ディレクトリーは、セキュリティ・ポリシーをインプリメントするために必要な基本的な機能をサポートしている必要があります。ディレクトリーは、基礎となるセキュリティ機能を直接提供しないかもしれませんが、基本的なセキュリティ・サービスを備えるトラステッド・ネットワーク・セキュリティ・サービスにそれが統合されている可能性があります。最初に、ユーザーの認証のための方式が必要です。認証は、ユーザーが本人であるかを検証するものです。ユーザー名およびパスワードが基本認証方式となっています。ユーザーの認証が完了すると、特定のオブジェクトに対して要求された操作を実行するための権限または許可を持っているかを判別する必要があります。

権限は、たいいていアクセス制御リスト (ACL) を基にしています。ACL は、ディレクトリー内のオブジェクトおよび属性に付加できる権限のリストです。ACL は、各ユーザーまたはユーザーのグループが、どのアクセスのタイプを許可または否認されているかをリストにしています。ACL をより短く、より管理しやすくするために、同じアクセス権限を持つユーザーは、たいいていグループにまとめられます。

関連概念

16 ページの『スキーマ』

スキーマは、ディレクトリーにデータを保管する方法を定める 1 組の規則です。スキーマは、許可されている項目のタイプ、それらの属性構造、および属性の構文を定義します。

102 ページの『操作属性』

Directory Server に対して特殊な意味を持つ、操作属性という幾つかの属性があります。これらは、サーバーによって保守される属性であり、サーバーがある 1 つの項目について管理している情報を反映するか、またはサーバーの動作に影響を及ぼします。

10 ページの『識別名 (DN)』

ディレクトリー内のすべての項目には、識別名 (DN) があります。DN は、ディレクトリー内の項目を一意的に識別する名前です。DN の最初のコンポーネントは、相対識別名 (RDN) と呼ばれています。

Lightweight Directory Access Protocol (LDAP) API

Directory Server API の詳細は、『Lightweight Directory Access Protocol (LDAP) APIs』を参照してください。

57 ページの『Directory Server のセキュリティ』

多彩な機能を使用して、Directory Server をセキュアにする方法を学んでください。

関連情報



The Java Naming and Directory Interface (JNDI) Tutorial Web site

1 配布ディレクトリー

1 配布ディレクトリーとは、複数の Directory Server にまたがってデータが区画に分割されているディレク
1 リー環境をいいます。クライアント・アプリケーションにとって、配布ディレクトリーが 1 つのディレク
1 トリーに見えるようにするため、すべてのサーバーとそこに収められているデータを認識している 1 つ以
1 上のプロキシ・サーバーが用意されます。

1 プロキシ・サーバーは、着信要求を適切なサーバーに配布し、その結果を収集してから、応答を統一して
1 クライアントに返送します。一連のバックエンド・サーバーは、自身が分担する配布ディレクトリーの一部
1 を保持します。基本的に、そのようなバックエンド・サーバーは、標準の LDAP サーバーであり、別のサ
1 ーバーで定義されているユーザーや、別々のサーバーで定義されているグループに所属するユーザーに代わ
1 って要求を発行するための、プロキシ・サーバーに対する追加のサポートが設けられています。

IBM Tivoli Directory Server バージョン 6 およびそれ以降 (分散プラットフォーム) では、プロキシ・サーバー、バックエンド・サーバー、およびそのディレクトリーをセットアップするためのツールを備えた、そのような配布ディレクトリーが提供されます。数百万件の項目に対応するように、このディレクトリーを拡大することができます。

配布ディレクトリーに対する IBM Directory Server for i5/OS のサポート

IBM Directory Server for i5/OS は、IBM Tivoli Directory Server 配布ディレクトリー内のバックエンド・サーバーとして稼働することができます。i5/OS Directory Server は、プロキシ・サーバーとして稼働することはできず、配布ディレクトリーをセットアップするのに必要なツールも組み込まれていません。この場合、プロキシ・サーバーは、別のプラットフォーム上で稼働する一方で、実際のデータは、1 つ以上の i5/OS Directory Server 上または i5/OS と Tivoli プラットフォームを混合した Directory Server 上に常駐することができます。

配布ディレクトリー・トポロジーで使用するために、i5/OS Directory Server の既存のディレクトリー・データを区分するには、そのデータを i5/OS ディレクトリーから LDIF ファイルにエクスポートし、その LDIF ファイルを使用して、Tivoli プラットフォーム上で Tivoli によって用意されている配布ディレクトリー・セットアップ・ツールを実行し、そのデータを、配布ディレクトリー用のバックエンド・サーバーとして一翼を担う i5/OS および Tivoli Directory Server に再ロードする必要があります。この処理は、i5/OS サーバーでも Tivoli プラットフォーム・サーバーでも違いはなく、ユーザーは、Tivoli プラットフォーム上でプロキシ・サーバーを保有しているので、すでに配布ディレクトリー・セットアップ・ツールを保有していることとなります。

配布ディレクトリーのサポートのための制御および拡張操作

ユーザーとそのユーザーが所属するグループを、複数のサーバーに振り分けて分散できるので、IBM Tivoli Directory Server では、配布ディレクトリー内でのグループのメンバーシップとアクセス制御をサポートするための一連の制御と拡張操作が定義されています。また、発信元のクライアントまでさかのぼって「監査証跡」を記録するためのメカニズムも装備されています。

注: 1 つのサーバーとそのレプリカごとに、ディレクトリー項目が保管されます。ただし、配布ディレクトリーでは、ユーザーは 1 つのサーバー上の 1 つ以上のグループに所属し、さらに、別のサーバーで定義されている他のグループにも所属することもあります。同様に、ユーザー自身は、特定の要求を処理するバックエンド・サーバー上で定義されていないことがあります。

監査制御

監査制御は、プロキシ・サーバーから発行されたクライアント要求の固有 ID をバックエンド・サーバーに送信するときにプロキシ・サーバーが使用するメカニズムです。監査制御では、固有 ID に加えて、発信元のクライアント IP も一緒に送信されます。この固有 ID は、バックエンド・サーバー上の監査項目に対して、プロキシ・サーバー上の監査項目を突き合わせるのに使用される ID です。複数のサーバーを通して要求が送られる場合、各サーバーの IP 情報が付け加えられます。それは、元のクライアントまでさかのぼる途中の各サーバーの証跡を提供します。

グループ・メンバーシップの評価の拡張操作

この拡張操作では、許可クライアント (プロキシ・サーバー) がユーザーに関する情報をバックエンド・サーバーに送信し、バックエンド・サーバー上のユーザーがメンバーとして所属するグループのリスト (静的、ネスト、または動的) を要求することができます。

グループ・メンバーシップの制御

この制御では、許可クライアント (プロキシ・サーバー) は、アクセス制御のために使用されるグループ・リストを送信することができます。このグループ・リストを使用して、アクセス制御が評価されます。つまり、評価では、サーバーが通常の判断で使用するグループ・リスト (サーバーに対してローカル側で保管されているグループ情報をベースとします) は使用されません。標準的な用法では、このグループ・リストは、プロキシ・サーバーがグループ・メンバーシップ評価拡張操作を介して各バックエンド・サーバーから収集したグループのリストを指します。

配布ディレクトリーの監査サポート

i5/OS のセキュリティ監査は、配布ディレクトリーをサポートするために拡張されています。

- **監査制御:** 発信元のクライアントにまでさかのぼって要求をたどると役に立ちます。i5/OS は、既存の DI セキュリティ監査ジャーナル項目に「ルーティング」フィールドを追加することによって、「監査制御」を監査します。その内容は検証不能であっても、プロキシ許可の使用を認可されているという理由で、トラステッド・クライアントであるはずのクライアントから発信されたものということになります。
- **グループ・メンバーシップ制御:** グループ制御があるかないかは、2 つの部分で監査されます。つまり、DI セキュリティ監査ジャーナル項目に単一文字「group membership assertion (グループ・メンバーシップ表明)」フィールドが追加されています。また、クライアントから提供されたグループ・リストを必要に応じて監査するように、サーバーを構成することもできます。このオプションを構成すると、サーバーは DI ジャーナル項目の「XD cross reference (XD 相互参照)」フィールドも監査し、一致する「XD cross reference (XD 相互参照)」フィールドとグループ・リスト (ジャーナル項目あたりの最大グループ数は 5 つ) を示した 1 つ以上の XD セキュリティ監査ジャーナル項目を作成します。

i5/OS のセキュリティ監査の詳細は、以下の関連リンク中の『セキュリティ監査』のトピックを参照してください。また、Internet Engineering Task Force Web サイトにアクセスして *rfc4648* を見つけ出し、Directory Server の監査の構成について調べることもできます。

配布ディレクトリーと配布ディレクトリーのセットアップに関する詳細は、Tivoli Software Information Center の Distributed Directories のトピックを参照してください。

関連概念

58 ページの『監査』

監査を使用して、特定の Directory Server トランザクションの詳細をトラックすることができます。

関連情報

セキュリティ監査

監査の詳細については、『セキュリティ監査』のトピックを参照してください。

Object Identifiers (OIDs) for extended operations and controls

識別名 (DN)

ディレクトリー内のすべての項目には、識別名 (DN) があります。DN は、ディレクトリー内の項目を一意的に識別する名前です。DN の最初のコンポーネントは、相対識別名 (RDN) と呼ばれています。

DN は、「属性 = 値」の組で構成され、次の例のようにコンマで区切ります。

```
cn=Ben Gray,ou=editing,o=New York Times,c=US
cn=Lucille White,ou=editing,o=New York Times,c=US
cn=Tom Brown,ou=reporting,o=New York Times,c=US
```


ディレクトリー・スキーマに定義されたすべての属性は、DN を構成するために使用できます。コンポーネント属性値の組の順序は、大切です。DN は、ルートからその項目が置かれているレベルまでのディレクトリー階層のそれぞれのレベルごとに 1 つのコンポーネントを含みます。LDAP DN は、最も具体性の高い属性 (通常はある種の名前) から始まり、徐々に意味の広い属性へと続き、たいていは国の属性で終了します。DN の最初のコンポーネントは、**相対識別名 (RDN)** と呼ばれています。これは、同じ親を持つ他の項目と区別される項目を識別します。上記の例では、RDN 「cn=Ben Gray」は、最初の項目と 2 番目の項目 (RDN は「cn=Lucille White」) を区別します。これらの 2 つの DN の例は、それ以外は同等です。項目に対する RDN を構成する「属性 = 値」の組も項目に存在していなければなりません。(これは、DN の他のコンポーネントにおいては当てはまりません。)

この例に従って、人の項目を作成します。

```
dn: cn=Tim Jones,o=ibm,c=us
objectclass: top
objectclass: person
cn: Tim Jones
sn: Jones
telephonenumber: 555-555-1234
```

DN エスケープ規則

幾つかの文字は、DN において特別の意味を持ちます。たとえば、等号 (=) は属性名と値を区切り、コンマ (,) は「属性 = 値」の組を区切ります。特殊文字は、, (コンマ)、= (等号)、+ (プラス)、< (より小)、> (より大)、# (番号記号)、; (セミコロン)、¥ (円記号)、および " (引用符、ASCII 34) です。

特殊文字は、特別な意味を取り除くために、属性値内でエスケープできます。DN スtringにおける属性値内のこれら特殊文字またはその他の文字をエスケープするには、以下の方式を使用してください。

1. エスケープする文字が特殊文字の 1 つである場合、円記号 (「¥」ASCII 92) をその前に付けます。この例では、組織名においてコンマをエスケープする方法を示します。

```
CN=L. Eagle,o=Sue\, Grabbit and Runn,C=GB
```

これは望ましい方法です。

2. それ以外に、エスケープする文字を円記号および 2 文字の 16 進数字に置き換えるという方法もあります。この 16 進数字は、その文字のコードの単一バイトを形成します。文字のコードは、UTF-8 コード・セットである必要があります。

```
CN=L. Eagle,o=Sue¥2C Grabbit and Runn,C=GB
```

3. 属性値全体を " (引用符) (ASCII 34) で囲みます。これは値の一部ではありません。¥ (円記号) を除き、引用文字の対の間にあるすべての文字はそのまま解釈されます。¥ (円記号) は、円記号 (ASCII 92)、引用符 (ASCII 34)、前述のすべての特殊文字、または方法 2 にある 16 進の対をエスケープするために使用できます。たとえば、cn=xyz"qrs"abc の中の引用符をエスケープするには、cn=xyz¥"qrs¥"abc となり、¥ をエスケープするには、次のようにします。

```
"you need to escape a single backslash this way ¥"
```

別の例として、「¥Zoo」は正しくありません。なぜなら「Z」はこのコンテキストではエスケープできないからです。

疑似 DN

疑似 DN は、アクセス制御定義および評価で使用されます。LDAP ディレクトリーは、幾つかの疑似 DN (たとえば、「group:CN=THIS」および「access-id:CN=ANYBODY」) をサポートしており、これらの疑似 DN は、実行中の操作または操作が実行されているオブジェクトとの関係において、共通の特性を共有する多数の DN を参照するために使用されます。

Directory Server では 3 つの疑似 DN がサポートされます。

- access-id: CN=THIS

ACL の一部として指定すると、この DN は、操作対象の DN に一致する bindDN を参照します。たとえば、オブジェクト「cn=personA, ou=IBM, c=US」上で操作が実行され、bindDn が「cn=personA, ou=IBM, c=US」の場合、認可される許可は、「CN=THIS」に与えられている許可と「cn=personA, ou=IBM, c=US」に与えられている許可の組み合わせとなります。

- group: CN=ANYBODY

ACL の一部として指定すると、この DN は、非認証であったとしてもすべてのユーザーを参照します。ユーザーをこのグループから除去することはできず、このグループをデータベースから除去することはできません。

- group: CN=AUTHENTICATED

この DN は、ディレクトリーにより認証済みのすべての DN を参照します。認証の方式は問われません。

注: 「CN=AUTHENTICATED」は、DN を表すオブジェクトの配置場所にかかわらず、サーバー上のどこかで認証済みの DN を参照します。しかし、これは注意して使用する必要があります。たとえば、ある接尾部の下では、「cn=Secret」は、aclentry が「group:CN=AUTHENTICATED:normal:rsc」である「cn=Confidential Material」と呼ばれるノードとなっているとします。別の接尾部の下では、「cn=Common」は、ノード「cn=Public Material」となっているとします。これら 2 つのツリーが同じサーバー上にある場合、「cn=Public Material」へのバインドは認証済みとみなされ、「cn=Confidential Material」オブジェクト上の通常クラスへの許可を取得します。

疑似 DN の幾つかの例を以下に示します。

例 1 オブジェクト「cn=personA, c=US」に対する以下の ACL について考えます。

```
AclEntry: access-id: CN=THIS:critical:rwsc
AclEntry: group: CN=ANYBODY: normal:rsc
AclEntry: group: CN=AUTHENTICATED: sensitive:rcs
```

| ユーザー・バインディング | 受け取る許可 |
|------------------|--|
| cn=personA, c=US | normal:rsc:sensitive:rcs:critical:rwsc |
| cn=personB, c=US | normal:rsc:sensitive:rsc |
| Anonymous | normal:rsc |

この例では、personA は、「CN=THIS」ID に認可された許可、および「CN=ANYBODY」と「CN=AUTHENTICATED」の両方の疑似 DN グループに与えられた許可を受け取ります。

例 2 オブジェクト「cn=personA, c=US AclEntry: access-id:cn=personA, c=US: object:ad」に対する以下の ACL について考えます。

```
AclEntry: access-id: CN=THIS:critical:rwsc
AclEntry: group: CN=ANYBODY: normal:rsc
AclEntry: group: CN=AUTHENTICATED: sensitive:rcs
```

cn=personA, c=US に対して実行される操作は以下のようになります。

| ユーザー・バインディング | 受け取る許可 |
|------------------|--------------------------|
| cn=personA, c=US | object:ad:critical:rwsc |
| cn=personB, c=US | normal:rsc:sensitive:rsc |

| ユーザー・バインディング | 受け取る許可 |
|--------------|------------|
| Anonymous | normal:rsc |

この例では、personA は、「CN=THIS」ID に認可された許可および DN 自体「cn=personA, c=US」に与えられた許可を受け取ります。バインド DN (「cn=personA, c=US」) にはより固有の aclentry (「access-id:cn=personA, c=US」) があるため、グループ許可は与えられないという点に注意してください。

拡張 DN 処理

DN の複合 RDN は、「+」演算子で接続された複数のコンポーネントで構成されていることがあります。サーバーは、そうした DN を持つ項目の検索のサポートを拡張します。検索操作のベースとして、複合 RDN を任意の順序で指定できます。

```
ldapsearch -b "cn=mike+ou=austin,o=ibm,c=us" "(objectclass=*)"
```

サーバーは、DN 正規化拡張操作をサポートします。DN 正規化拡張操作は、サーバー・スキーマを使用して DN を正規化します。この拡張操作は、DN を使用するアプリケーションにおいては便利です。

識別名の構文

識別名 (DN) の正式な構文は、RFC 2253 に基づいています。バックス正規形式 (BNF) 構文は、以下のよう定義されています。

```
<name> ::= <name-component> ( <spaced-separator> )
          | <name-component> <spaced-separator> <name>

<spaced-separator> ::= <optional-space>
                       <separator>
                       <optional-space>

<separator> ::= ", " | ";"

<optional-space> ::= ( <CR> ) *( " " )

<name-component> ::= <attribute>
                    | <attribute> <optional-space> "+"
                    <optional-space> <name-component>

<attribute> ::= <string>
               | <key> <optional-space> "=" <optional-space> <string>

<key> ::= 1*( <keychar> ) | "OID." <oid> | "oid." <oid>
<keychar> ::= letters, numbers, and space

<oid> ::= <digitstring> | <digitstring> "." <oid>
<digitstring> ::= 1*<digit>
<digit> ::= digits 0-9

<string> ::= *( <stringchar> | <pair> )
           | "'" *( <stringchar> | <special> | <pair> ) "'"
           | "#" <hex>

<special> ::= ", " | "=" | <CR> | "+" | "<" | ">"
           | "#" | ";"

<pair> ::= "\" ( <special> | "\" | "'" )
<stringchar> ::= any character except <special> or "\" or "'"
```

```
<hex> ::= 2*<hexchar>
<hexchar> ::= 0-9, a-f, A-F
```

識別名内で RDN を区切るためにはコンマ (,) が標準的な表記ですが、セミコロン (;) 文字も使用できません。

空白文字 (スペース) は、コンマまたはセミコロンのいずれの側にも置くことができます。空白文字は無視され、セミコロンはコンマに置換されます。

加えて、スペース (「 」 ASCII 32) 文字を「+」または「=」の前または後のいずれかに置くことができます。これらのスペース文字は、構文解析時に無視されます。

以下の例は、名前一般的な形式に合わせて設計されている表記法で書かれた識別名です。最初に 3 つのコンポーネントを含む名前があります。最初のコンポーネントは複合 RDN です。複合 RDN には、複数の「属性 : 値」の組が含まれており、単純な CN 値があいまいである場合に、特定の項目を一意的に識別するために使用できます。

```
OU=Sales+CN=J. Smith,O=Widget Inc.,C=US
```

関連概念

4 ページの『ディレクトリー』

Directory Server は、i5/OS 統合ファイル・システムの編成に類似した方法で情報を階層構造に保管するタイプのデータベースへのアクセスを許可します。

57 ページの『Directory Server のセキュリティー』

多彩な機能を使用して、Directory Server をセキュアにする方法を学んでください。

105 ページの『制御および拡張操作』

制御操作と拡張操作では、プロトコルそのものを変更しなくても、LDAP プロトコルを拡張することができます。

接尾部 (命名コンテキスト)

接尾部 (命名コンテキストともいいます) は、ローカルに保持されるディレクトリー階層の最上部の項目を識別する DN です。

LDAP では相対命名方式が使用されているため、この DN は、そのディレクトリー階層内の他のすべての項目の接尾部ともなります。1 つのディレクトリー・サーバーに複数の接尾部を含めて、ローカルに保持されるディレクトリー階層 (たとえば、o=ibm,c=us) をそれぞれの接尾部で識別することもできます。

接尾部に一致する特定の項目は、ディレクトリーに追加しなければなりません。作成する項目では、対象の命名属性を含む objectclass を使用しなければなりません。Web 管理ツールまたは Qshell ldapadd ユーティリティーを使用して、この接尾部に対応する項目を作成する必要があります。

理論的には、グローバル LDAP ネーム・スペースがあります。グローバル LDAP ネーム・スペースでは、DN は以下のように表示されます。

- cn=John Smith,ou=Rochester,o=IBM
- cn=Jane Doe,o=My Company,c=US
- cn=system administrator,dc=myco,dc=com

接尾部「o=IBM」は、第 1 の DN のみがサーバーが保持するネーム・スペースにあるということをサーバーに示します。接尾部の 1 つに含まれないオブジェクトへの参照を試行すると、該当のオブジェクトがないというエラーが出るか、または別のディレクトリー・サーバーへの参照が行われます。

サーバーには、複数の接尾部を含めることができます。Directory Server には、この製品のインプリメンテーションに特有のデータを保持する事前定義の接尾部がいくつかあります。

- cn=schema には、LDAP がアクセス可能なスキーマの表記が含まれています。
- cn=changelog は、使用可能の場合、サーバー変更ログを保持します。
- cn=localhost には、サーバー操作の幾つかの局面を制御する、複製ではない情報 (たとえば、複製構成オブジェクトなど) が含まれています。
- cn=IBMpolicies には、複製されるサーバー操作に関する情報が入っています。
- cn=pwdpolicy には、サーバー全体のパスワード・ポリシーが含まれています。
- 「os400-sys=system-name.mydomain.com」接尾部は、LDAP に対して i5/OS オブジェクトへのアクセスを可能にします。現行では、アクセスはユーザー・プロファイルおよびグループに限定されています。

Directory Server は、デフォルトの接尾部、dc=system-name,dc=domain-name が事前に構成されて出荷されているため、サーバーを開始するのが容易になっています。その接尾部を使用するための要件はありません。ユーザーが独自の接尾部を追加し、事前に構成された接尾部を削除することができます。

接尾部には、よく使用される 2 つの命名規則があります。一方は、組織の TCP/IP ドメインを基にしたものです。他方は、組織の名前と場所を基にしたものです。

たとえば、TCP/IP ドメインが mycompany.com であるとする、dc=mycompany,dc=com のような接尾部を選択できます。ここで、dc 属性は、ドメイン・コンポーネントを指しています。この場合、ディレクトリーに作成した最上位項目は、以下ようになります (LDAP 項目を表すためのテキスト・ファイル形式である LDIF を使用)。

```
dn: dc=mycompany,dc=com
objectclass: domain
dc: mycompany
```

domain objectclass には、使用できるオプション属性も含まれています。スキーマを表示するか、Web 管理ツールを使用して作成した項目を編集して、使用できる追加属性を確認できます。

ご使用の会社名が My Company であり、それがアメリカ合衆国に置かれている場合、以下のいずれかのような接尾部を選択できます。

```
o=My Company
o=My Company,c=US
ou=Widget Division,o=My Company,c=US
```

ここで、ou は、organizationalUnit objectclass の名前、o は、organization objectclass の組織名、さらに c は、国別オブジェクト・クラスに名前を付けるために使用される標準的な 2 文字の国の略語です。この場合、作成する最上位項目は以下ようになります。

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

使用するアプリケーションによっては、特定の接尾部を定義したり、特定の命名規則を使用することが必要な場合があります。たとえば、デジタル証明書の管理にディレクトリーを使用する場合、ディレクトリーの一部を構成して、そこに保持されている証明書のサブジェクト DN と項目名が一致するようにする必要があります。

ディレクトリーに追加される項目は、`ou=Marketing,o=ibm,c=us` のような DN 値と一致する接尾部を持っている必要があります。ローカル・データベースに対して構成されているいずれの接尾部にも一致しない接尾部が照会に含まれている場合、照会は、デフォルトの参照により識別される LDAP サーバーを参照します。デフォルトの LDAP 参照が指定されていない場合、オブジェクトが存在しないという結果が戻されます。

関連概念

218 ページの『ディレクトリー項目タスク』

以下の情報を参考にして、ディレクトリー項目を管理します。

207 ページの『スキーマ・タスク』

以下の情報を参考にして、スキーマを管理します。

関連タスク

139 ページの『Directory Server 接尾部の追加および除去』

以下の情報を参考にして、Directory Server の接尾部を追加または除去します。

関連資料

244 ページの『`ldapmodify` および `ldapadd`』

LDAP `modify-entry` および LDAP `add-entry` コマンド行ユーティリティー

スキーマ

スキーマは、ディレクトリーにデータを保管する方法を定める 1 組の規則です。スキーマは、許可されている項目のタイプ、それらの属性構造、および属性の構文を定義します。

データは、ディレクトリー項目を使用してディレクトリーに保管されます。項目は、1 つのオブジェクト・クラス (必須) およびその属性で構成されます。必須属性とオプション属性があります。オブジェクト・クラスでは、情報の種類が指定されます。この情報の種類は、項目で記述および定義されている属性のセットで決まります。各属性には 1 つ以上の関連した値があります。

スキーマに関連した情報については、以下を参照してください。

関連概念

4 ページの『ディレクトリー』

Directory Server は、i5/OS 統合ファイル・システムの編成に類似した方法で情報を階層構造に保管するタイプのデータベースへのアクセスを許可します。

218 ページの『ディレクトリー項目タスク』

以下の情報を参考にして、ディレクトリー項目を管理します。

207 ページの『スキーマ・タスク』

以下の情報を参考にして、スキーマを管理します。

Directory Server のスキーマ

Directory Server のスキーマは事前定義されていますが、追加要件がある場合にスキーマを変更できます。

Directory Server には、動的スキーマのサポートが組み込まれています。スキーマは、ディレクトリー情報の一部として公開され、Subschema 項目 (DN=`cn=cn=schema`) で使用可能です。 `ldap_search()` API を使用してスキーマを照会でき、`ldap_modify()` を使用してそれを変更できます。

スキーマには、LDAP バージョン 3 Request For Comments (RFC) または標準仕様に含まれている構成情報よりも多くの構成情報があります。たとえば、ある特定の属性において、どの索引を保守する必要がある

かを指定できます。この追加構成情報は、必要ならばサブスキーマ項目内で保守されます。追加オブジェクト・クラスがサブスキーマ項目 IBMsubschema に対して定義されます。IBMsubschema は、拡張スキーマ情報を保持する「MAY」属性を持っています。

Directory Server は、特別なディレクトリー項目、「cn=schema」を使用してアクセスできる単一のスキーマをサーバー全体に対して定義します。その項目には、そのサーバーに対して定義されたすべてのスキーマが含まれます。スキーマ情報を検索するには、以下の例を使用して、ldap_search を実行します。

```
DN: "cn=schema", search scope: base, filter: objectclass=subschema
or objectclass=*
```

スキーマは、以下の属性タイプの値を規定します。

- objectClasses
- attributeTypes
- IBMAttributeTypes
- 突き合わせ規則
- ldap 構文

これらのスキーマ定義の構文は、LDAP バージョン 3 RFC を基にしています。

スキーマ項目のサンプルを以下に示します。

```
objectclasses=( 1.3.6.1.4.1.1466.101.120.111
                NAME 'extensibleObject'
                SUP top AUXILIARY )
```

```
objectclasses=( 2.5.20.1
                NAME 'subschema'
                AUXILIARY MAY
                ( dITStructureRules
                  $ nameForms
                  $ ditContentRules
                  $ objectClasses
                  $ attributeTypes
                  $ matchingRules
                  $ matchingRuleUse ) )
```

```
objectclasses=( 2.5.6.1
                NAME 'alias'
                SUP top STRUCTURAL
                MUST aliasedObjectName )
```

```
attributeTypes=( 2.5.18.10
                  NAME 'subschemaSubentry'
                  EQUALITY distinguishedNameMatch
                  SYNTAX 1.3.6.1.4.1.1466.115.121.1.12
                  NO-USER-MODIFICATION
                  SINGLE-VALUE USAGE directoryOperation )
```

```
attributeTypes=( 2.5.21.5 NAME 'attributeTypes'
                  EQUALITY objectIdentifierFirstComponentMatch
                  SYNTAX 1.3.6.1.4.1.1466.115.121.1.3
                  USAGE directoryOperation )
```

```
attributeTypes=( 2.5.21.6 NAME 'objectClasses'
                  EQUALITY objectIdentifierFirstComponentMatch
                  SYNTAX 1.3.6.1.4.1.1466.115.121.1.37
                  USAGE directoryOperation
                  SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
                  USAGE directoryOperation )
```

```
ldapSyntaxes=( 1.3.6.1.4.1.1466.115.121.1.5 DESC 'Binary' )
ldapSyntaxes=( 1.3.6.1.4.1.1466.115.121.1.7 DESC 'Boolean' )
ldapSyntaxes=( 1.3.6.1.4.1.1466.115.121.1.12 DESC 'DN' )
```

```

ldapSyntaxes=( 1.3.6.1.4.1.1466.115.121.1.15 DESC 'Directory String' )
ldapSyntaxes=( 1.3.6.1.4.1.1466.115.121.1.24 DESC 'Generalized Time' )
ldapSyntaxes=( 1.3.6.1.4.1.1466.115.121.1.26 DESC 'IA5 String' )
ldapSyntaxes=( 1.3.6.1.4.1.1466.115.121.1.27 DESC 'INTEGER' )
ldapSyntaxes=( 1.3.6.1.4.1.1466.115.121.1.50 DESC 'Telephone Number' )
ldapSyntaxes=( 1.3.6.1.4.1.1466.115.121.1.53 DESC 'UTC Time' )

matchingRules=( 2.5.13.2 NAME 'caseIgnoreMatch'
                 SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 )
matchingRules=( 2.5.13.0 NAME 'objectIdentifierMatch'
                 SYNTAX 1.3.6.1.4.1.1466.115.121.1.38 )
matchingRules=( 2.5.13.30 NAME 'objectIdentifierFirstComponentMatch'
                SYNTAX 1.3.6.1.4.1.1466.115.121.1.38 )
matchingRules=( 2.5.13.4 NAME 'caseIgnoreSubstringsMatch'
                SYNTAX 1.3.6.1.4.1.1466.115.121.1.58 )

```

スキーマ情報は、ldap_modify API を使用して変更できます。DN 「cn=schema」を使用すると、属性タイプまたはオブジェクト・クラスを追加、削除、または置換できます。完全な記述を指定することもできます。LDAP バージョン 3 定義または IBM 属性拡張定義のいずれかまたは両方を使用して、スキーマ項目を追加または置換できます。

関連概念

207 ページの『スキーマ・タスク』

以下の情報を参考にして、スキーマを管理します。

Lightweight Directory Access Protocol (LDAP) API

Directory Server API の詳細は、『Lightweight Directory Access Protocol (LDAP) APIs』を参照してください。

19 ページの『オブジェクト・クラス』

オブジェクト・クラスは、オブジェクトを記述するために使用される属性のセットを指定します。

20 ページの『属性』

各ディレクトリー項目には、そのオブジェクト・クラスを介して関連付けられた属性のセットがあります。

関連資料

23 ページの『IBMAttributeTypes 属性』

IBMAttributeTypes 属性は、属性用に LDAP バージョン 3 規格でカバーされていないスキーマ情報を定義するために使用できます。

24 ページの『突き合わせ規則』

突き合わせ規則は、検索操作時のストリング比較のためのガイドラインを規定します。

26 ページの『属性構文』

属性構文は、属性に許容される値を定義します。

30 ページの『動的スキーマ』

スキーマを動的に変更することができます。

共通スキーマのサポート

IBM Directory は、標準ディレクトリー・スキーマをサポートします。

IBM Directory は、以下に定義されている標準ディレクトリー・スキーマをサポートします。

- Internet Engineering Task Force (IETF) LDAP バージョン 3 RFC (RFC 2252 および 2256 など)
- Desktop Management Task Force (DMTF) にある Common Information Model (CIM)
- Network Application Consortium の Lightweight Internet Person Schema (LIPS)

このバージョンの LDAP には、LDAP バージョン 3 で定義済みのスキーマのデフォルト・スキーマ構成が組み込まれています。ここにはさらに、DEN スキーマ定義も組み込まれています。

IBM はさらに、他の IBM 製品が LDAP ディレクトリーを活用する時に共用する、拡張共通スキーマ定義のセットも備えています。これには、以下のものが含まれます。

- ePerson、グループ、国、組織、組織単位と役割、地域、都道府県などのホワイト・ページ・アプリケーション用のオブジェクト。
- アカウント、サービスおよびアクセス・ポイント、権限、認証、セキュリティー・ポリシーなどのその他のサブシステム用のオブジェクト。

関連情報

 [Internet Engineering Task Force \(IETF\)](#)

 [Desktop Management Task Force \(DMTF\)](#)

 [Network Application Consortium](#)

オブジェクト・クラス

オブジェクト・クラスは、オブジェクトを記述するために使用される属性のセットを指定します。

たとえば、オブジェクト・クラス **tempEmployee** を作成した場合、そこには、**idNumber**、**dateOfHire**、または **assignmentLength** などの一時従業員に関連した属性を含めることができます。組織の必要に適合するカスタム・オブジェクト・クラスを追加することができます。IBM Directory Server スキーマは、以下のような、幾つかの基本的なオブジェクト・クラスのタイプを規定します。

- Groups
- Locations
- Organizations
- People

注: Directory Server に特有のオブジェクト・クラスには、接頭部「ibm-」があります。

オブジェクト・クラスは、タイプ、継承、および属性の特性により定義されています。

オブジェクト・クラス・タイプ

オブジェクト・クラスは、以下の 3 つのタイプの中の 1 つとなります。

構造化:

すべての項目は唯一の構造化オブジェクト・クラスに属する必要があり、構造化オブジェクト・クラスは項目の基本内容を定義します。このオブジェクト・クラスは、現実に即したオブジェクトです。すべての項目は構造化オブジェクト・クラスに属する必要があるため、これは最もよく使用されるタイプのオブジェクト・クラスです。

要約:

このタイプは、他の (構造化) オブジェクト・クラスのスーパークラスまたはテンプレートとして使用されます。これは、構造化オブジェクト・クラスのセットに共通の属性のセットを定義します。これらのオブジェクト・クラスは、要約クラスのサブクラスとして定義された場合、定義済み属性を継承します。従属のオブジェクト・クラスごとに属性を定義する必要はありません。

補助：

このタイプは、特定の構造化オブジェクト・クラスに属する項目に関連付けることができる追加属性を示します。項目は、単一の構造化オブジェクト・クラスにしか属することができませんが、複数の補助オブジェクト・クラスに属することができます。

オブジェクト・クラスの継承

このバージョンの Directory Server は、オブジェクト・クラスおよび属性定義におけるオブジェクトの継承をサポートします。新規オブジェクト・クラスは、複数の親クラス (複数継承) および追加または変更された属性を使用して定義できます。

各項目は、単一の構造化オブジェクト・クラスに割り当てられます。すべてのオブジェクト・クラスは、要約オブジェクト・クラス、**top** から継承します。それらは、他のオブジェクト・クラスから継承することもできます。オブジェクト・クラスの構造により、特定の項目における必須属性および許可された属性のリストが決定されます。オブジェクト・クラスの継承は、オブジェクト・クラス定義の順序に依存しています。オブジェクト・クラスは、その前のオブジェクト・クラスからのみ継承できます。たとえば、**person** 項目用のオブジェクト・クラスの構造は、LDIF ファイルで以下のように定義されているかもしれません。

```
objectClass: top
objectClass: person
objectClass: organizationalPerson
```

この構造において、**person** オブジェクト・クラスは **top** オブジェクト・クラスからのみ継承しますが、**organizationalPerson** は、**person** および **top** オブジェクト・クラスから継承します。そのため、**organizationalPerson** オブジェクト・クラスを項目に割り当てる時、そのオブジェクト・クラスは、必須属性および許可された属性を自動的に上位のオブジェクト・クラス (この場合、**person** オブジェクト・クラス) から継承します。

スキーマの更新操作が処理されコミットされる前に、それとスキーマ・クラス階層との整合性が検査されません。

属性

すべてのオブジェクト・クラスには、幾つかの必須属性およびオプション属性が含まれています。必須属性は、オブジェクト・クラスを使用する項目内に存在している必要がある属性です。オプション属性は、オブジェクト・クラスを使用する項目内に存在している可能性がある属性です。

属性

各ディレクトリー項目には、そのオブジェクト・クラスを介して関連付けられた属性のセットがあります。

オブジェクト・クラスは、項目に含まれる情報のタイプを記述しますが、実際のデータは属性に含まれています。属性は、名前、アドレス、または電話番号などの特定のデータ・エレメントを持つ 1 つ以上の名前と値の対で表されます。Directory Server は、データを、名前と値の対である記述属性 (**commonName** (**cn**) など)、および情報の特定の部分 (**John Doe** など) として表します。

たとえば、**John Doe** の項目には、幾つかの属性 (名前と値の対) が含まれている可能性があります。

```
dn: uid=jdoe, ou=people, ou=mycompany, c=us
objectClass: top
objectClass: person
objectClass: organizationalPerson
cn: John Doe
sn: Doe
givenName: Jack
givenName: John
```

標準属性はすでにスキーマで定義済みですが、組織の必要に適合する属性定義を作成、編集、コピー、または削除することができます。

詳細については、以下を参照してください。

共通サブスキーマ・エレメント:

エレメントは、サブスキーマ属性値の文法を定義するために使用されます。

以下のエレメントは、サブスキーマ属性値の文法を定義するために使用されます。

- alpha = 'a' - 'z', 'A' - 'Z'
- number = '0' - '9'
- anh = alpha / number / '-' / ';' ;
- anhstring = 1 * anh
- keystring = alpha [anhstring]
- numericstring = 1 * number
- oid = descr / numericoid
- descr = keystring
- numericoid = numericstring *("." numericstring)
- woid = whsp oid whsp ; set of oids of either form (numeric OIDs or names)
- oids = woid / ("(" oidlist ")")
- oidlist = woid *("\$" woid) ; object descriptors used as schema element names
- qdescrs = qdescr / (whsp "(" qdescrlist ")" whsp)
- qdescrlist = [qdescr *(qdescr)]
- whsp "" descr "" whsp

objectclass 属性:

objectclasses 属性は、サーバーによりサポートされるオブジェクト・クラスをリストします。

この属性のそれぞれの値は、別個のオブジェクト・クラス定義を表します。 cn=schema 項目の objectclasses 属性をふさわしく変更することにより、オブジェクト・クラス定義を追加、削除、または変更できます。 objectclasses 属性の値には、RFC 2252 で定義された以下の文法があります。

```
ObjectClassDescription = "(" whsp
    numericoid whsp ; Objectclass identifier
    [ "NAME" qdescrs ]
    [ "DESC" qdstring ]
    [ "OBSOLETE" whsp ]
    [ "SUP" oids ] ; Superior objectclasses
    [ ( "ABSTRACT" / "STRUCTURAL" / "AUXILIARY" ) whsp ] ; default is structural
    [ "MUST" oids ] ; AttributeTypes
    [ "MAY" oids ] ; AttributeTypes
    whsp ")"
```

たとえば、person objectclass の定義は以下のようになります。

```
( 2.5.6.6 NAME 'person' DESC 'Defines entries that generically represent people. ' STRUCTURAL
SUP top MUST ( cn $ sn ) MAY ( userPassword $ telephoneNumber $ seeAlso $ description ) )
```

- このクラスの OID は 2.5.6.6 です
- 名前は「person」です

- 構造化オブジェクト・クラスです
- オブジェクト・クラス「top」から継承します
- 次の属性が必要です: cn、sn
- 以下の属性はオプションです: userPassword、telephoneNumber、seeAlso、description

関連概念

207 ページの『スキーマ・タスク』

以下の情報を参考にして、スキーマを管理します。

attributetypes 属性:

attributetypes 属性は、サーバーによりサポートされる属性をリストします。

この属性のそれぞれの値は、別個の属性定義を表します。 cn=schema 項目の attributetypes 属性をふさわしく変更することにより、属性定義を追加、削除、または変更できます。 attributetypes 属性の値には、RFC 2252 で定義された以下の文法があります。

```
AttributeTypeDescription = "(" whsp
    numericoid whsp ; AttributeType identifier
    [ "NAME" qdescrs ] ; name used in AttributeType
    [ "DESC" qdstring ] ; description
    [ "OBSOLETE" whsp ]
    [ "SUP" woid ] ; derived from this other AttributeType
    [ "EQUALITY" woid ; Matching Rule name
    [ "ORDERING" woid ; Matching Rule name
    [ "SUBSTR" woid ] ; Matching Rule name
    [ "SYNTAX" whsp noidlen whsp ]
    [ "SINGLE-VALUE" whsp ] ; default multi-valued
    [ "COLLECTIVE" whsp ] ; default not collective
    [ "NO-USER-MODIFICATION" whsp ] ; default user modifiable
    [ "USAGE" whsp AttributeUsage ] ; default userApplications
    whsp ")"
```

```
AttributeUsage =
    "userApplications" /
    "directoryOperation" /
    "distributedOperation" / ; DSA-shared
    "dSAOperation" ; DSA-specific, value depends on server
```

突き合わせ規則および構文値は、以下により定義された値の 1 つである必要があります。

- 24 ページの『突き合わせ規則』
- 26 ページの『属性構文』

「userApplications」属性のみがスキーマ内で定義または変更できます。

「directoryOperation」、「distributedOperation」、および「dSAOperation」属性は、サーバーにより定義され、サーバー操作に特定の意味を持ちます。

たとえば、「description」属性には、以下の定義があります。

```
( 2.5.4.13 NAME 'description' DESC 'Attribute common to CIM and LDAP schema to provide lengthy
description of a directory object entry.'EQUALITY caseIgnoreMatch SUBSTR
caseIgnoreSubstringsMatch SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 USAGE userApplications )
```

- この OID は 2.5.4.13 です
- この名前は「description」です
- この構文は 1.3.6.1.4.1.1466.115.121.1.15 (Directory String) です

関連概念

207 ページの『スキーマ・タスク』

以下の情報を参考にして、スキーマを管理します。

IBMAttributeTypes 属性:

IBMAttributeTypes 属性は、属性用に LDAP バージョン 3 規格でカバーされていないスキーマ情報を定義するために使用できます。

IBMAttributeTypes の値は、以下の文法に従う必要があります。

```
IBMAttributeTypesDescription = "(" whsp
    numericoid whsp
    [ "DBNAME" qdescrs ] ; at most 2 names (table, column)
    [ "ACCESS-CLASS" whsp IBMAccessClass whsp ]
    [ "LENGTH" wlen whsp ] ; maximum length of attribute
    [ "EQUALITY" [ IBMwlen ] whsp ] ; create index for matching rule
    [ "ORDERING" [ IBMwlen ] whsp ] ; create index for matching rule
    [ "APPROX" [ IBMwlen ] whsp ] ; create index for matching rule
    [ "SUBSTR" [ IBMwlen ] whsp ] ; create index for matching rule
    [ "REVERSE" [ IBMwlen ] whsp ] ; reverse index for substring
whsp ")"
```

```
IBMAccessClass =
    "NORMAL" / ; this is the default
    "SENSITIVE" /
    "CRITICAL" /
    "RESTRICTED" /
    "SYSTEM" /
    "OBJECT" /
```

```
IBMwlen = whsp len
```

Numericoid

attributetypes の値を IBMAttributeTypes の値と関連させるために使用されます。

DBNAME

最大 2 つまでの名前を (実際に 2 つの名前を指定するようなことがあれば) 規定できます。最初の名前は、この属性用に使用されるテーブル名です。2 番目の名前は、テーブル内の属性の完全正規化値用に使用される列名です。1 つの名前のみを規定する場合、それはテーブル名および列名として使用されます。DBNAME を指定しない場合は、属性名 (固有であること) の先頭の 128 文字を基にした名前が使用されます。データベース・テーブル名は、128 文字になるように切り捨てられます。列名は、30 文字になるように切り捨てられます。

ACCESS-CLASS

この属性タイプのアクセス分類。ACCESS-CLASS を省略した場合、デフォルトで normal になります。

LENGTH

この属性の最大長。長さは、バイト数で表されます。Directory Server には、属性の長さを指定するための機能があります。attributetypes 値において、以下のストリング、
(attr-oid ... SYNTAX syntax-oid{len} ...)

を使用して、oid attr-oid を持つ attributetype が最大長を持つことを指示できます。

EQUALITY, ORDERING, APPROX, SUBSTR, REVERSE

これらの属性のいずれかが使用された場合、対応する突き合わせ規則のための索引が作成されます。オプションで長さを指定すると、索引列の幅を指定できます。複数の突き合わせ規則をインプリメントするために、単一の索引が使用されます。ユーザーが指定しないとき、Directory Server

は、500 の長さを割り当てます。サーバーは、そうする理由があるときには、ユーザーが要求した長さより短い長さを使用することもあります。たとえば、索引の長さが属性の最大長を超えると、索引の長さは無視されます。

突き合わせ規則:

突き合わせ規則は、検索操作時の文字列比較のためのガイドラインを規定します。

突き合わせ規則は、次の 3 つのカテゴリに分けられています。

- 等価
- 順序付け
- サブ文字列

ディレクトリー・サーバーは 2 進数を除いて、すべての構文で等価突き合わせをサポートしています。2 進数構文を使用して定義された属性では、サーバーがサポートするのは存在検索のみで、例えば、「(jpegphoto=*)」などです。IA5 String および Directory String の構文では、属性定義を大/小文字を区別するか、または大/小文字を区別しないなど、さらに定義することができます。例えば、cn 属性では、「John Doe」と「john doe」の値を等しいものとする caseIgnoreMatch 突き合わせ規則を使用します。大/小文字を区別しない突き合わせ規則では、値を大文字に変換した後で比較が行われます。大文字アルゴリズムでは、ロケールによって区別されないで、すべてのロケールで正しい訳ではありません。

ディレクトリー・サーバーは、Directory String、IA5 String、および Distinguished Name 構文属性でサブ文字列突き合わせをサポートしています。サブ文字列突き合わせの検索フィルターは「*」文字を使用して、ストリーム中のゼロ以上の文字を突き合わせます。例えば、検索フィルター「(cn=*smith)」は、文字列「smith」で終わる cn 値をすべて突き合わせます。

Integer、Directory String、IA5 String、および Distinguished Name の構文では、順序付け突き合わせがサポートされています。文字列構文では、突き合わせは UTF-8 文字列値の単純なバイト配列に基づいて行われます。大/小文字を区別しない規則で属性が定義された場合は、順序付けは大文字文字列値を使用して実行されます。前にも記述したとおり、大文字アルゴリズムは、すべてのロケールに正しい訳ではありません。

IBM Directory Server では、サブ文字列および順序づけの突き合わせ動作は突き合わせ規則に従って実施されます。すなわち、サブ文字列突き合わせをサポートする構文にはすべて暗黙のサブ文字列突き合わせ規則があり、順序付けをサポートする構文にはすべて暗黙の順序付け規則があります。大/小文字を区別しない突き合わせ規則を使用して定義された属性では、暗黙のサブ文字列および順序づけの突き合わせ規則でも、大/小文字は区別されません。

| 等価突き合わせ規則 | | |
|----------------------------|----------------------------|---------------------|
| 突き合わせ規則 | OID | 構文 |
| caseExactIA5Match | 1.3.6.1.4.1.1466.109.114.1 | Directory String 構文 |
| caseExactMatch | 2.5.13.5 IA5 | String 構文 |
| caseIgnoreIA5Match | 1.3.6.1.4.1.1466.109.114.2 | IA5 String 構文 |
| caseIgnoreMatch | 2.5.13.2 | Directory String 構文 |
| distinguishedNameMatch | 2.5.13.1 | DN - 識別名 |
| generalizedTimeMatch | 2.5.13.27 | Generalized Time 構文 |
| ibm-entryUuidMatch | 1.3.18.0.2.22.2 | Directory String 構文 |
| integerFirstComponentMatch | 2.5.13.29 | Integer 構文 - 整数値 |

| 等価突き合わせ規則 | | |
|-------------------------------------|-----------|---|
| 突き合わせ規則 | OID | 構文 |
| integerMatch | 2.5.13.14 | Integer 構文 - 整数値 |
| objectIdentifierFirstComponentMatch | 2.5.13.30 | 収容する側の OID に対しては String。OID は、数字 (0-9) および小数点 (.) が使用されたストリングです。. |
| objectIdentifierMatch | 2.5.13.0 | 収容する側の OID に対しては String。OID は、数字 (0-9) および小数点 (.) が使用されたストリングです。 |
| octetStringMatch | 2.5.13.17 | Directory String 構文 |
| telephoneNumberMatch | 2.5.13.20 | Telephone Number 構文 |
| uTCTimeMatch | 2.5.13.25 | UTC Time 構文 |

| 順序付け突き合わせ規則 | | |
|--------------------------------|------------------|---------------------|
| 突き合わせ規則 | OID | 構文 |
| caseExactOrderingMatch | 2.5.13.6 | Directory String 構文 |
| caseIgnoreOrderingMatch | 2.5.13.3 | Directory String 構文 |
| distinguishedNameOrderingMatch | 1.3.18.0.2.4.405 | DN - 識別名 |
| generalizedTimeOrderingMatch | 2.5.13.28 | Generalized Time 構文 |

| サブストリング突き合わせ規則 | | |
|--------------------------------|-----------|---------------------|
| 突き合わせ規則 | OID | 構文 |
| caseExactSubstringsMatch | 2.5.13.7 | Directory String 構文 |
| caseIgnoreSubstringsMatch | 2.5.13.4 | Directory String 構文 |
| telephoneNumberSubstringsMatch | 2.5.13.21 | Telephone Number 構文 |

注: UTC-Time は、ASN.1 標準で定義されたタイム・ストリング・フォーマットです。ISO 8601 および X680 を参照してください。UTC-Time 形式で時刻値を保管するためにこの構文を使用してください。

関連資料

37 ページの『一般化時刻および UTC 時刻』

Directory Server は、一般化時刻および協定世界時 (UTC) 構文をサポートします。

索引付け規則:

属性に付加された索引規則は、情報の検索をより高速に行うことを可能にします。

属性のみが指定されている場合、索引は保守されません。Directory Server は、以下の索引付け規則を備えています。

- 等価
- 順序付け
- 近似
- サブストリング

- 反転

属性のための索引付け規則の仕様:

属性のための索引付け規則を指定すると、属性値の特別な索引の作成および保守を制御します。これにより、それらの属性を含むフィルターで検索するための応答時間がかなり向上します。

候補となる 5 つの索引付け規則のタイプが検索フィルターに適用される操作に関連しています。

等価 以下の検索操作に適用されます。

- equalityMatch 「=」

たとえば次のようになります。

```
"cn = John Doe"
```

順序付け

以下の検索操作に適用されます。

- greaterOrEqual '>='
- lessOrEqual '<='

たとえば次のようになります。

```
"sn >= Doe"
```

近似 以下の検索操作に適用されます。

- approxMatch 「~=」

たとえば次のようになります。

```
"sn ~= doe"
```

サブストリング

サブストリング構文を使用する以下の検索操作に適用されます。

- サブストリング 「*」

たとえば次のようになります。

```
"sn = McC*"
"cn = J*Doe"
```

反転 以下の検索操作に適用されます。

- 「*」サブストリング

たとえば次のようになります。

```
"sn = *baugh"
```

検索フィルターで使用する属性には、少なくとも等価索引を指定することをお勧めします。

属性構文:

属性構文は、属性に許容される値を定義します。

サーバーは、属性用の構文定義を使用してデータの妥当性検査を行い、値を突き合わせる方法を決定します。たとえば、「Boolean」属性は、「TRUE」および「FALSE」の値しか持ちません。

属性は単一値または複数値のいずれかとして定義できます。複数値属性には順序がないので、特定の順序で戻される属性の値のセットに依存するアプリケーションを作成するべきではありません。配列された値のセットを必要とする場合には、以下のように、値のリストを単一の属性値に入れることを考慮してください。

preferences: 1st-pref 2nd-pref 3rd-pref

あるいは以下のように配列情報を値に含めることを考慮してください。

```
preferences: 2 yyy
preferences: 1 xxx
preferences: 3 zzz
```

複数値属性は、項目が幾つかの名前で知られている場合に便利です。たとえば、cn (共通名) は複数値です。項目は以下のように定義できます。

```
dn: cn=John Smith,o=My Company,c=US
objectclass: inetorgperson
sn: Smith
cn: John Smith
cn: Jack Smith
cn: Johnny Smith
```

これにより、John Smith および Jack Smith を検索すると、同じ情報が戻ります。

Binary 属性は、任意のバイト・ストリング (たとえば、JPEG 写真など) を含んでおり、項目の検索には使用できません。

Boolean 属性は、ストリング TRUE または FALSE を含んでいます。

DN 属性は、LDAP 識別名を含んでいます。その値は、既存の項目の DN である必要はありませんが、有効な DN 構文を持っている必要があります。

Directory String 属性は、UTF-8 文字を使用するテキスト・ストリングを含んでいます。属性は、(属性に定義された突き合わせ規則を基にした) 検索フィルターで使用される値に関して大/小文字を区別することもできますし、それを無視することもできます。しかし、値は常に最初に入力したとおりに戻されます。

Generalized Time 属性は、GMT 時刻とオプションの GMT 時間帯オフセットを使用する 2000 年問題に対応した日時のストリング表記を含んでいます。

IA5 String 属性は、IA5 文字セット (7 ビット US ASCII) を使用するテキスト・ストリングを含んでいます。属性は、(属性に定義された突き合わせ規則を基にした) 検索フィルターで使用される値に関して大/小文字を区別することもできますし、それを無視することもできます。しかし、値は常に最初に入力したとおりに戻されます。IA5 String では、サブストリング検索にワイルドカード文字を使用することもできます。

Integer 属性は、値のテキスト・ストリング表記を含んでいます。たとえば、0 または 1000 を含みます。Integer 構文属性の値は -2147483648 から 2147483647 の範囲内でなければなりません。

Telephone Number 属性は、電話番号のテキスト表記を含んでいます。Directory Server は、この値に対して特定の構文を規定していません。次の値はすべて有効な値です: (555)555-5555、555.555.5555、および +1 43 555 555 5555。

UTC Time 属性は、日時を表記するために、以前の 2000 年問題未対応のストリング・フォーマットを使用します。

ディレクトリー・スキーマでは、属性の構文はそれぞれの構文に割り当てたオブジェクト ID (OID) を使用して指定されます。ディレクトリー・サーバーとその OID でサポートされる構文は以下の表にリストされています。

| 構文 | OID |
|---|-------------------------------|
| Attribute Type Description 構文 | 1.3.6.1.4.1.1466.115.121.1.3 |
| Binary - オクテット・ストリング | 1.3.6.1.4.1.1466.115.121.1.5 |
| Boolean - TRUE/FALSE | 1.3.6.1.4.1.1466.115.121.1.7 |
| Directory String 構文 | 1.3.6.1.4.1.1466.115.121.1.15 |
| DIT Content Rule Description 構文 | 1.3.6.1.4.1.1466.115.121.1.16 |
| DITStructure Rule Description 構文 | 1.3.6.1.4.1.1466.115.121.1.17 |
| DN - 識別名 | 1.3.6.1.4.1.1466.115.121.1.12 |
| Generalized Time 構文 | 1.3.6.1.4.1.1466.115.121.1.24 |
| IA5 String 構文 | 1.3.6.1.4.1.1466.115.121.1.26 |
| IBM Attribute Type Description | 1.3.18.0.2.8.1 |
| Integer 構文 - 整数値 | 1.3.6.1.4.1.1466.115.121.1.27 |
| LDAP Syntax Description 構文 | 1.3.6.1.4.1.1466.115.121.1.54 |
| Matching Rule Description | 1.3.6.1.4.1.1466.115.121.1.30 |
| Matching Rule Use Description | 1.3.6.1.4.1.1466.115.121.1.31 |
| Name Form Description | 1.3.6.1.4.1.1466.115.121.1.35 |
| Object Class Description 構文 | 1.3.6.1.4.1.1466.115.121.1.37 |
| 収容する側の OID に対しては String。OID は、数字 (0-9) および小数点 (.) が使用されたストリングです。 | 1.3.6.1.4.1.1466.115.121.1.38 |
| Telephone Number 構文 | 1.3.6.1.4.1.1466.115.121.1.50 |
| UTC Time 構文。UTC-Time は、ASN.1 標準で定義されたタイム・ストリング・フォーマットです。ISO 8601 および X680 を参照してください。UTC-Time 形式で時刻値を保管するためにこの構文を使用してください。 | 1.3.6.1.4.1.1466.115.121.1.53 |

関連概念

『オブジェクト ID (OID)』

オブジェクト ID (OID) は 10 進数のストリングで、オブジェクトを一意的に識別します。これらのオブジェクトは、通常、オブジェクト・クラスまたは属性です。

関連資料

37 ページの『一般化時刻および UTC 時刻』

Directory Server は、一般化時刻および協定世界時 (UTC) 構文をサポートします。

オブジェクト ID (OID)

オブジェクト ID (OID) は 10 進数のストリングで、オブジェクトを一意的に識別します。これらのオブジェクトは、通常、オブジェクト・クラスまたは属性です。

OID を持っていない場合には、オブジェクト・クラスまたは属性名に **-oid** を追加して指定することができます。たとえば、属性 **tempID** を作成する場合、OID は **tempID-oid** として指定できます。

専用の OID を正当な権限から取得することは絶対に重要です。正当な OID を取得するために、2 つの基本方針があります。

- オブジェクトを登録局に登録する。この方針は、OID を多数必要としない場合などに便利です。

- 登録局から arc (arc とは、OID ツリーの個々のサブツリーです) を取得し、必要に応じて独自の OID を割り当てる。多数の OID が必要な場合、または OID の割り当てが安定していない場合にこの方針がふさわしいかもしれません。

米国規格協会 (ANSI) は、アメリカ合衆国の組織名のための登録局で、International Standards Organization (ISO) および国際電気通信連合 (ITU) により確立されたグローバル登録処理に従って登録を行います。組織名の登録に関する詳しい情報は、ANSI Web サイト (www.ansi.org) にあります。組織のための ANSI OID arc は、2.16.840.1 です。ANSI は、番号 (NEWNUM) を割り当て、新規 OID arc である 2.16.840.1.NEWNUM を作成します。

ほとんどの国または地域では、各国の標準協会が OID 登録を保守しています。ANSI arc に関しては、通常 arc は、OID 2.16 以降に割り当てられます。特定の国または地域では、OID 権限を検索するために少しの調査が必要になる場合があります。お客様の国または地域の各国標準組織は、ISO メンバーである可能性があります。ISO メンバーの名前および連絡先情報は、ISO Web サイト (www.iso.ch) にあります。

Internet Assigned Numbers Authority (IANA) は、専用企業番号を割り当てます。これは OID で、arc 1.3.6.1.4.1 です。IANA は番号 (NEWNUM) を割り当て、新規 OID arc が 1.3.6.1.4.1.NEWNUM となるようにします。これらの番号は、IANA Web サイト (www.iana.org) から取得できます。

組織が OID の割り当てを受けると、その OID の末尾に追加することにより、ユーザー独自の OID を定義できます。たとえば、組織が仮に OID 1.1.1 を割り当てられたとします。他のどの組織も「1.1.1」で始まる OID は割り当てられません。「.1」を追加して 1.1.1.1 を形式することにより、LDAP の範囲を作成できます。さらにこれを、objectclass 用 (1.1.1.1.1)、属性タイプ用 (1.1.1.1.2) などの範囲に小さく分割したり、OID 1.1.1.1.2.34 を属性「foo」に割り当てることもできます。

関連情報



ANSI Web サイト



ISO Web サイト



IANA Web サイト

サブスキーマ項目

サーバーごとに 1 つのサブスキーマ項目があります。ディレクトリー内のすべての項目は、暗黙の subschemaSubentry 属性タイプを持っています。subschemaSubentry 属性タイプの値は、その項目に対応するサブスキーマ項目の DN です。同じサーバーの下にあるすべての項目は、同じサブスキーマを共用し、それらの subschemaSubentry 属性タイプは同じ値を持っています。サブスキーマ項目は、ハードコーディングされている DN 「cn=schema」を持っています。

サブスキーマ項目は、オブジェクト・クラス「top」、「subschema」、および「IBMsubschema」に属しません。「IBMsubschema」オブジェクト・クラスには MUST 属性はなく、1 つの MAY 属性タイプ (「IBMattributeTypes」) があります。

IBMsubschema オブジェクト・クラス

IBMsubschema オブジェクト・クラスは、特定の Directory Server のすべての属性およびオブジェクト・クラスを保管する固有のオブジェクト・クラスです。

IBMsubschema オブジェクト・クラスは、以下のようにして、サブスキーマ項目内のみで使用されます。

```
( 1.3.18.0.2.6.174
NAME 'ibmSubSchema'
DESC 'IBM specific object class that stores all the attributes and object classes for a given directory
server.'
SUP 'subschema'
STRUCTURAL MAY ( IBMAttributeTypes ) )
```

スキーマ照会

ldap_search() API を使用して、サブスキーマ項目を照会できます。

ldap_search() API を使用して、以下の例に示されているように、サブスキーマ項目を照会できます。

```
DN          : "cn=schema"
search scope : base
filter      : objectclass=subschema or objectclass=*
```

この例では、全スキーマを検索します。選択した属性タイプのすべての値を検索するには、ldap_search で attrs パラメーターを使用します。特定の属性タイプの特定の値だけを検索できません。

関連概念

Lightweight Directory Access Protocol (LDAP) API

Directory Server API の詳細は、『Lightweight Directory Access Protocol (LDAP) APIs』を参照してください。

動的スキーマ

スキーマを動的に変更することができます。

動的スキーマの変更を実行するには、DN を「cn=schema」にして、ldap_modify API を使用してください。一度に 1 つのスキーマ・エンティティ (たとえば、属性タイプ、オブジェクト・クラスなど) のみを追加、削除、または置換することが許可されています。

スキーマ項目を削除するには、スキーマ項目を定義するスキーマ属性 (objectclasses または attributetypes) を指定し、その値として OID を括弧内に指定します。たとえば、OID <attr-oid> を持つ属性を削除するには、以下のようにします。

```
dn: cn=schema
changetype: modify
delete: attributetypes
attributetypes: ( <attr-oid> )
```

完全な記述を指定することもできます。いずれの事例においても、削除するスキーマ・エンティティを検索するために使用される突き合わせ規則は、objectIdentifierFirstComponentMatch です。

スキーマ・エンティティを追加または置換するには、LDAP バージョン 3 定義を規定する必要があり (MUST)、IBM 定義を規定することも可能です (MAY)。すべての事例において、該当するスキーマ・エンティティの定義 (複数も可) のみを規定する必要があります。

たとえば、属性タイプ「cn」(その OID は 2.5.4.3) を削除するには、以下のようにして ldap_modify() を使用します。

```
LDAPMod attr;
LDAPMod *attrs[] = { &attr, NULL };
char *vals [] = { "( 2.5.4.3 )", NULL };
attr.mod_op = LDAP_MOD_DELETE;
attr.mod_type = "attributeTypes";
attr.mod_values = vals;
ldap_modify_s(ldap_session_handle, "cn=schema", attrs);
```

属性「name」から継承し、20 文字の長さを持つ OID 20.20.20 の新規属性タイプ bar を追加するには、以下のようにします。

```
char *vals1[] = { "( 20.20.20 NAME 'bar' SUP name )" NULL };
char *vals2[] = { "( 20.20.20 LENGTH 20 )", NULL };
LDAPMod attr1;
LDAPMod attr2;
LDAPMod *attrs[] = { &attr1, &attr2, NULL };
attr1.mod_op = LDAP_MOD_ADD;
attr1.mod_type = "attributeTypes";
attr1.mod_values = vals1;
attr2.mod_op = LDAP_MOD_ADD;
attr2.mod_type = "IBMattributeTypes";
attr2.mod_values = vals2;
ldap_modify_s(ldap_session_handle, "cn=schema", attrs);
```

上記の LDIF バージョンは、以下のようになります。

```
dn: cn=schema
changetype: modify
add: attributetypes
attributetypes: ( 20.20.20 NAME 'bar' SUP name )
-
add: ibmattributetypes
ibmattributetypes: (20.20.20 LENGTH 20)
```

アクセス制御

動的スキーマの変更は、複製のサプライヤーまたは管理者 DN のみが実行できます。

複製

動的スキーマの変更が実行される時、これは複製されます。

許可されないスキーマの変更

すべてのスキーマ変更が許可されるわけではありません。

変更の制約事項には、以下が含まれます。

- スキーマを変更しても、スキーマは整合状態のままでなければなりません。
- 別の属性タイプのスーパータイプである属性タイプは、削除できません。オブジェクト・クラスの「MAY」または「MUST」属性タイプとなっている属性タイプは、削除できません。
- 別のオブジェクト・クラスのスーパークラスであるオブジェクト・クラスは、削除できません。
- 存在しないエンティティ（たとえば、構文やオブジェクト・クラスなど）を参照する属性タイプまたはオブジェクト・クラスは、追加できません。
- 属性タイプまたはオブジェクト・クラスは、存在しないエンティティ（たとえば、構文やオブジェクト・クラスなど）を参照する結果となるようには変更できません。
- 新規の属性は、それらの IBMattributeType 定義中にある既存のデータベース・テーブルを使用できません。
- 既存のディレクトリー項目で使用された属性は削除できません。
- 属性の長さおよび構文は変更できません。
- 属性と関連したデータベース・テーブルまたは欄は変更できません。
- 既存のオブジェクト・クラスの定義に使用された属性は削除できません。
- 既存のディレクトリー項目で使用されたオブジェクト・クラスは削除できません。

- | スキーマを変更すれば、列のサイズを大きくすることができます。これにより、Web 管理または
- | ldapmodify ユーティリティを使用したスキーマの変更を通して、属性の最大長を増大することができま
- | す。

サーバーの操作に影響を与えるスキーマの変更は許可されません。ディレクトリー・サーバーには、以下のスキーマ定義が必要です。これらは変更できません。

オブジェクト・クラス:

- accessGroup
- accessRole
- alias
- os400-usrprf
- referral
- replicaObject
- top

属性:

- aclEntry
- aclPropagate
- aclSource
- aliasedObjectName、aliasedentryName
- businessCategory
- cn、commonName
- createTimestamp
- creatorsName
- description
- dn、distinguishedName
- entryOwner
- hasSubordinates
- ibm-entryChecksum
- ibm-entryChecksumOp
- ibm-entryUuid
- member
- modifiersName
- modifyTimestamp
- name
- o、organizationName、organization
- objectClass
- os400-acgcde
- os400-astlvl
- os400-atnpgm
- os400-audlvl
- os400-aut

- os400-ccsid
- os400-chridctl
- os400-cntryid
- os400-curlib
- os400-dlvry
- os400-docpwd
- os400-dspsgninf
- os400-eimassoc
- os400-gid
- os400-groupmember
- os400-grpaut
- os400-grpauttyp
- os400-grpprf
- os400-homedir
- os400-IaspStorageInformation
- os400-inlmnu
- os400-inlpgm
- os400-invalidSignonCount
- os400-jobd
- os400-kbdbuf
- os400-langid
- os400-lclpwdmgt
- os400-lmtcpb
- os400-lmtdevssn
- os400-locale
- os400-maxstg
- os400-msgq
- os400-objaud
- os400-outq
- os400-owner
- os400-password
- os400-passwordExpirationDate
- os400-passwordLastChanged
- os400-previousSignon
- os400-profile
- os400-prtdev
- os400-ptylmt
- os400-pwdexp
- os400-pwdexpitv
- os400-setjobatr

- os400-sev
- os400-spcaut
- os400-spcenv
- os400-srtseq
- os400-status
- os400-storageUsed
- os400-storageUsedOnIasp
- os400-supgrprpf
- os400-sys os400-text
- os400-uid
- os400-usrcls
- os400-usropt
- ou、organizationalUnit、organizationalUnitName
- owner
- ownerPropagate
- ownerSource
- ref
- replicaBindDN
- replicaBindMethod
- replicaCredentials、replicaBindCredentials
- replicaHost
- replicaPort
- replicaUpdateTimeInterval
- replicaUseSSL
- seeAlso

構文: All

突き合わせ規則:

All

スキーマ検査

サーバーが初期化される時、スキーマ・ファイルが読み取られ、整合性および正確さが検査されます。

検査が不合格の場合、サーバーは初期化に失敗し、エラー・メッセージが出されます。動的スキーマの変更時、結果として作成されるスキーマも整合性および正確さが検査されます。検査が不合格の場合、エラーが戻され、変更は失敗します。幾つかの検査は文法の一部です (たとえば、属性タイプは最大 1 つのスーパータイプを持つことができ、オブジェクト・クラスは幾つでもスーパークラスを持つことができます)。

以下の項目が属性タイプに対して検査されます。

- 異なる 2 つの属性タイプが同じ名前または OID を持つことはできない。
- 属性タイプの継承階層は循環しない。
- 属性タイプのスーパータイプも、その定義が後で表示されるか別個のファイルに置かれる可能性があるが、定義されなければならない。

- 属性タイプが別の属性タイプのサブタイプである場合、それら両方は同じ USAGE を持つ必要がある。
- すべての属性タイプは、直接定義された、あるいは継承された構文を持つ。
- 操作属性のみが NO-USER-MODIFICATION とマークされる。

以下の項目がオブジェクト・クラスに対して検査されます。

- 異なる 2 つのオブジェクト・クラスが同じ名前または OID を持つことはできない。
- オブジェクト・クラスの継承階層は循環しない。
- オブジェクト・クラスのスーパークラスも、その定義が後で表示されるか別個のファイルに置かれる可能性があるが、定義されなければならない。
- オブジェクト・クラスの「MUST」および「MAY」属性タイプも、その定義が後で表示されるか別個のファイルに置かれる可能性があるが、定義されなければならない。
- すべての構造化オブジェクト・クラスは、top の直接または間接的なサブクラスである。
- 要約オブジェクト・クラスがスーパークラスを持つ場合、そのスーパークラスも要約でなければならない。

スキーマに対する項目の検査

LDAP 操作により項目が追加または変更される時、項目はスキーマに対して検査されます。デフォルトでは、この節にリストされているすべての検査が実行されます。しかしながら、スキーマの検査レベルを変更することにより、幾つかのスキーマ検査を選択的に使用不可にすることができます。これは、System i™ Navigatorを使用して、「Directory Server」プロパティの「データベース/接尾部」ページ上にある、「スキーマ検査」フィールドの値を変更することにより行います。

スキーマに従うために、項目は、以下の条件において検査されます。

オブジェクト・クラスに関するもの:

- 少なくとも 1 つの属性タイプの値「objectClass」を持つ必要がある。
- 任意の数の補助オブジェクト・クラスを持つことができる (なくてもよい)。これは検査ではなく、説明です。これを使用不可にするオプションはありません。
- 任意の数の要約オブジェクト・クラスを持つことができるが、クラス継承の結果としてのみである。これは、項目が持つすべての要約オブジェクト・クラスにおいて、項目は、その要約オブジェクト・クラスから直接または間接的に継承する構造化または補助オブジェクト・クラスも持つということを意味します。
- 少なくとも 1 つの構造化オブジェクト・クラスを持つ必要がある。
- ちょうど 1 つの直接または基本構造オブジェクト・クラスを持つ必要がある。つまり、項目が規定する構造化オブジェクト・クラスはすべて、その構造化オブジェクト・クラスのうちのいずれか 1 つのスーパークラスでなければなりません。ほとんどの導出されたオブジェクト・クラスは、項目の「直接」または「基本構造」オブジェクト・クラス、または単に項目の「構造化」オブジェクト・クラスと呼ばれます。
- その直接の構造化オブジェクト・クラスを変更できない (ldap_modify 上で)。
- 項目で規定された各オブジェクト・クラスにおいて、そのすべての直接または間接スーパークラスのセットが計算される。これらの中のいずれかのスーパークラスが項目で規定されていない場合、それは自動的に追加されます。

- スキーマ検査レベルが「バージョン 3 (厳密な)」に設定されている場合、すべての構造化スーパークラスを規定する必要がある。たとえば、objectclass inetorgperson を持つ項目を作成するには、次の objectclass を指定する必要があります。person、organizationalperson、および inetorgperson。

項目の属性タイプの妥当性は、以下のようにして判別されます。

- 項目の MUST 属性タイプは、そのすべてのオブジェクト・クラス (暗黙の継承されたオブジェクト・クラスを含む) の MUST 属性タイプのセットの和集合として計算される。項目の MUST 属性タイプのセットが、その項目が含む属性タイプのセットのサブセットではない場合、その項目はリジェクトされます。
- 項目の MAY 属性タイプは、そのすべてのオブジェクト・クラス (暗黙の継承されたオブジェクト・クラスを含む) の MAY 属性タイプのセットの和集合として計算される。項目に含まれる属性タイプのセットが、その項目の MUST および MAY 属性タイプのセットの和集合のサブセットではない場合、その項目はリジェクトされます。
- 項目に定義されたいずれかの属性タイプが NO-USER-MODIFICATION とマークされている場合、その項目はリジェクトされる。

項目の属性タイプ値の妥当性は、以下のようにして判別されます。

- 項目に含まれるすべての属性タイプにおいて、属性タイプが単一値であり、項目に複数值がある場合、その項目はリジェクトされる。
- 項目に含まれるすべての属性タイプのすべての属性値において、その構文がその属性の構文のための構文検査ルーチンに従わない場合、その項目はリジェクトされる。
- 項目に含まれるすべての属性タイプのすべての属性値において、その長さがその属性タイプに割り当てられている最大長より大きい場合、その項目はリジェクトされる。

DN の妥当性は以下のようにして検査されます。

- 構文は、BNF に準拠して DistinguishedNames を検査する。準拠しない場合、その項目はリジェクトされる。
- RDN がその項目に対して有効な唯一の属性タイプで構成されていることが検査される。
- RDN で使用されている属性タイプの値がその項目にあることが検査される。

関連概念

288 ページの『Directory Server 構成スキーマ』

この情報では、ディレクトリー情報ツリー (DIT) および ibmslapd.conf ファイルの構成に使用する属性を説明します。

iPlanet 互換性

Directory Server で使用される構文解析プログラムは、スキーマ属性タイプ (objectClasses および attributeTypes) の属性値を、iPlanet の文法を使用して指定することを許可しています。

たとえば、descr および numeric-oid を、(qdescr であるかのように) 単一引用符で囲むことにより指定できます。しかしながら、スキーマ情報は、必ず ldap_search を介して使用可能になります。ファイル内の属性値に対して単一の動的変更 (ldap_modify を使用) が実行されるとすぐに、ファイル全体は、すべての属性値が Directory Server 仕様に従うものに置換されます。ファイル上および ldap_modify 要求で使用される構文解析プログラムは同じであるため、属性値のために iPlanet の文法を使用する ldap_modify も正しく処理されます。

iPlanet サーバーのサブスキーマ項目に対して照会が行われると、結果の項目は、特定の OID に対して複数值を持つことがあります。たとえば、ある属性タイプが 2 つの名前 (「cn」および「commonName」な

ど)を持つ場合、その属性タイプの記述は二度(名前ごとに一度)指定されます。Directory Server は、単一の属性タイプまたはオブジェクト・クラスの記述が同じ記述で複数回現れるスキーマ (NAME および DESCR を除く) を構文解析できます。しかしながら、Directory Server がスキーマを公開する時、Directory Server は、すべての名前がリストされているそうした属性タイプの単一の記述を提供します(短い名前が最初にリストされます)。たとえば、iPlanet が共通名属性を記述する方法を以下に示します。

```
( 2.5.4.3 NAME 'cn'  
  DESC 'Standard Attribute'  
  SYNTAX '1.3.6.1.4.1.1466.115.121.1.15' )
```

```
( 2.5.4.3 NAME 'commonName'  
  DESC 'Standard Attribute, alias for cn'  
  SYNTAX '1.3.6.1.4.1.1466.115.121.1.15' )
```

次は、Directory がそれを記述する方法です。

```
( 2.5.4.3 NAME ( 'cn' 'commonName' ) SUP name )
```

Directory Server は、サブタイプをサポートします。「cn」を name のサブタイプにたくない場合(標準からは逸脱する)、以下のように宣言することができます。

```
( 2.5.4.3 NAME ( 'cn' 'commonName' )  
  DESC 'Standard Attribute'  
  SYNTAX '1.3.6.1.4.1.1466.115.121.1.15' )
```

最初の名前(「cn」)は優先名または短縮名として、「cn」以降の他のすべての名前は代替名として取られます。この時点から、ストリング「2.3.4.3」、「cn」、および「commonName」(大/小文字を区別しない同等のストリングを含む)は、スキーマ内部またはディレクトリーに追加された項目に対して相互に置き換えて使用できます。

一般化時刻および UTC 時刻

Directory Server は、一般化時刻および協定世界時(UTC)構文をサポートします。

日時に関連した情報を指定するために使用される様々な表記があります。たとえば、1999年2月4日は、以下のように記述されます。

```
2/4/99  
4/2/99  
99/2/4  
4.2.1999  
04-FEB-1999
```

この他にも多数の表記があります。

Directory Server は、LDAP サーバーが2つの構文をサポートするようにして、タイム・スタンプ表記を標準化します。

- Generalized Time 構文は次の形式を取ります。

```
YYYYMMDDHHMMSS[.fraction][(+|-HHMM)|Z]
```

年に4桁、月、日、時、分、および秒それぞれに2桁、および秒のオプションの小数部があります。これ以上追加しない場合には、日時はローカル時間帯という前提になります。時刻を協定世界時で測ることを示すために、時刻または地方時の時差に大文字の Z を追加してください。たとえば次のようになります。

```
"19991106210627.3"
```

これは地方時では、1999年11月6日、午後9時6分27.3秒です。

```
"19991106210627.3Z"
```

これは協定世界時です。

```
"19991106210627.3-0500"
```

これは最初の例と同じ地方時で、協定世界時と比較すると 5 時間の差があります。

秒のオプションの小数部を指定する場合は、ピリオドまたはコンマが必要です。地方時の時差では、「+」または「-」を時間と分の値の前に入れる必要があります。

- Universal time 構文は次の形式を取ります。

```
YYMMDDHHMM[SS][(+ | -)HHMM][Z]
```

年、月、日、時、分、およびオプションの秒フィールドそれぞれに 2 桁があります。GeneralizedTime のように、オプションの時刻の時差を指定できます。たとえば、地方時が 1999 年 1 月 2 日の午前で、協定世界時が 1999 年 1 月 2 日の正午 12 時である場合、UTCTime の値は以下のいずれかになります。

```
"9901021200Z"  
または  
"9901020700-0500"
```

地方時が 2001 年 1 月 2 日の午前で、協定世界時が 2001 年 1 月 2 日の正午 12 時である場合、UTCTime の値は以下のいずれかになります。

```
"0101021200Z"  
または  
"0101020700-0500"
```

UTCTime では、年の値に 2 桁のみしか許可されないため、この使用は推奨されていません。

サポートされる突き合わせ規則は、等価の場合には generalizedTimeMatch、不等価の場合には generalizedTimeOrderingMatch です。サブストリング検索は許可されません。たとえば、以下のフィルターは有効です。

```
generalized-timestamp-attribute=199910061030  
utc-timestamp-attribute>=991006  
generalized-timestamp-attribute=*
```

以下のフィルターは無効です。

```
generalized-timestamp-attribute=1999*  
utc-timestamp-attribute>=*1010
```

ディレクトリー構造の推奨される措置

Directory Server はユーザーおよびグループのリポジトリーとして使用されることがあります。この項では、ユーザーおよびグループの管理を最適化する構成をセットアップするための推奨事項を説明します。この構成および関連のセキュリティーのモデルは、ディレクトリーの他の用途に拡張することができます。

ユーザーは通常、単一または少数の場所に保管されます。すべてのユーザーの親項目である単一コンテナ cn=users が存在するか、あるいは別個に管理される別の組のユーザー用に、別のコンテナが存在します。例えば、社員、取引先、および自己登録インターネット・ユーザーはそれぞれ、cn=employees、cn=vendors、および cn=internet のユーザー名が付いたオブジェクトに入れられます。通常、社員は、その所属の組織に入れようと考えますが、社員が別の組織に移動すると、ディレクトリー項目の移動も必要となり、さらに、グループや他のデータ・ソース (ディレクトリーの内部と外部の両方) でも新規 DN を反映させるために更新が必要となるので、困難が生じる可能性があります。ユーザーと組織構造との関係は、「o」(組織名)、「ou」(組織単位名)、および organizationalPerson や inetOrgPerson の標準スキーマの一部である departmentNumber などのディレクトリー属性を使用してユーザー項目内で把握できます。

同様に、グループは通常、「cn=groups」という名前のコンテナなどの、別個のコンテナに入っています。

ユーザーおよびグループをこの方法で編成すると、設定が必要なアクセス制御リスト (ACL) を入れる場所を少なくすることができます。

ディレクトリー・サーバーの使用方法、およびユーザーおよびグループの管理方法によっては、以下のアクセス制御パターンの 1 つを使用することになります。

- 住所録などのアプリケーションでディレクトリーを使用する場合には、特殊なグループに対して、cn=users コンテナとその親オブジェクトの「normal」属性の読み取りおよび検索権限を認可したいことがあります。
- ほとんどの場合、cn=groups コンテナへのアクセスが必要となるのは、特定のアプリケーションおよびグループの管理者に使用される DN のみです。グループ管理者の DN をもつグループを作成して、そのグループを、cn=groups とその従属の所有者にしたい場合があります。グループ情報を読み取るためにアプリケーションで使用される DN をもつ別のグループを作成し、そのグループに対して、cn=groups への読み取りおよび検索権限を許可します。
- ユーザー・オブジェクトがユーザーによって直接更新される場合は、特殊な access-id cn=this に対して、適切な読み取り、書き出し、および検索の権限を許可します。
- アプリケーションを介してユーザーを更新する場合は、それらのアプリケーションは自身の ID で実行し、これらのアプリケーションのみでユーザー・オブジェクトを更新する権限が必要となります。これらの DN を cn=user 管理者などのグループに追加し、そのグループに、cn=users への必要な権限を許可しておくこと、大変便利であることを再度説明しておきます。

このタイプの構成およびアクセス制御を適用すると、初期ディレクトリーは次のようになるはずですが。

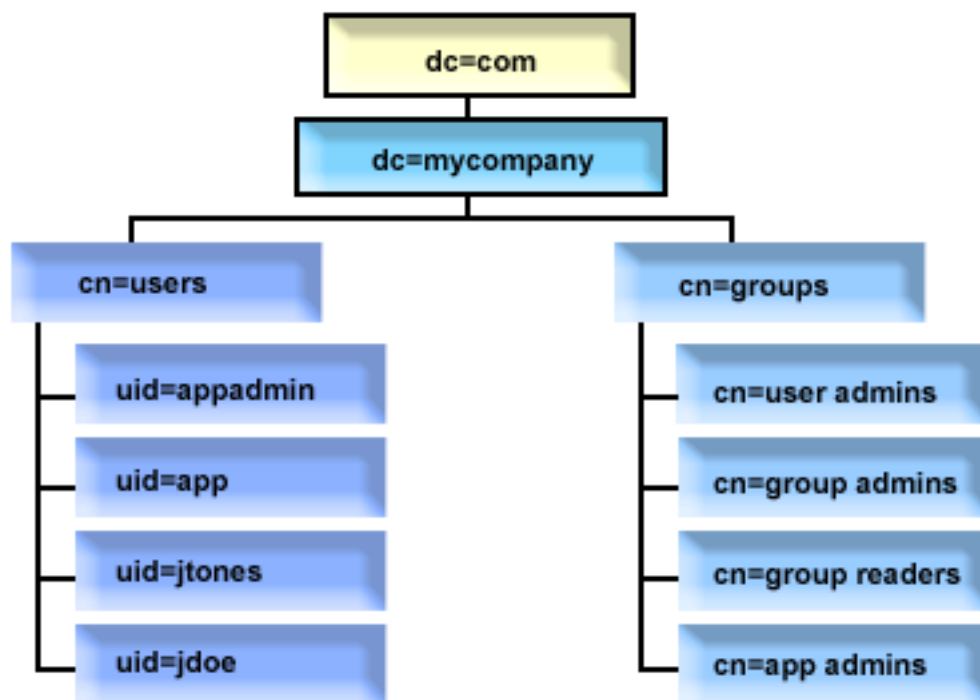


図 2. ディレクトリー構造の例

- `c=mycompany, dc=com` はディレクトリー管理者によって、またはトップレベルのディレクトリーを管理する権限をもつ他のユーザーまたはグループによって所有されています。追加の ACL 項目は、`cn=anybody` または `cn=authenticated` のいずれかの通常属性への読み取りアクセスを許可し、さらに厳密な ACL が必要な場合は、他の一部のグループに対してこれを許可します。
- `cn=users` には、下記の記述よりも多い ACL 項目があって、ユーザーに対して適切なアクセスを許可しています。ACL には、以下のものが含まれます。
 - `cn=anybody` または `cn=authenticated` の通常属性に対する読み取りおよび検索アクセス
 - 管理者の通常属性および機密属性に対する読み取りおよび検索アクセス
 - 個人の項目に対して、その個人に書き込みアクセスを許可するなどの、他の ACL 項目

Lotus Notes:

- 読みやすくするために、完全な DN ではなく、項目の RDN が使用されています。例えば、「`user admins`」グループは、短縮された `uid=app` ではなく、メンバーとして完全な DN の `uid=app,cn=users,dc=mycompany,dc=com` を持っています。
- 特定のユーザーとグループを結合することがあります。例えば、アプリケーション管理者がユーザーを管理する権限をもっていた場合は、アプリケーションはそのアプリケーション管理者の DN によって実行することになります。ただし、これにより、アプリケーションで新規のパスワードを再構成しないでも、アプリケーションの管理者パスワードを変更する機能などが制限されることになります。
- 上記では、ただ 1 つのアプリケーションで使用されるディレクトリーに最適な例を示していますが、ディレクトリー管理者として認証することによって、すべての更新を実行させるようにすると、さらに好都合です。実務としては、前に説明した理由によりお勧めできません。

公開

Directory Server は、システムが特定の種類の情報を LDAP ディレクトリーに公開する機能を提供します。すなわち、システムは、さまざまなタイプのデータを表す LDAP 項目を作成および更新します。

i5/OS には、以下の情報を LDAP サーバーに公開するための組み込みサポートがあります。

ユーザー

Directory Server に対して情報タイプ「ユーザー」を公開するようにオペレーティング・システムを構成すると、ユーザー情報がシステム配布ディレクトリーから Directory Server 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同期化されます。

ユーザーの公開は、システム配布ディレクトリーから情報への LDAP 検索アクセスを行う場合に便利です (たとえば、Netscape Communicator や Microsoft® Outlook Express のような LDAP が有効な POP3 メール・クライアントに LDAP 住所録アクセスを行う場合)。

公開されたユーザーは、システム配布ディレクトリーから公開されるユーザーもいれば、他の方法でディレクトリーに追加されるユーザーもいるという場合の LDAP 認証をサポートするためにも使用されます。公開されたユーザーは、ユーザー・プロファイルを特定する `uid` 属性を持っており、`userPassword` 属性は持っていません。このような項目に対してバインド要求を受け取った時、サーバーはオペレーティング・システムのセキュリティーを呼び出し、有効なユーザー・プロファイルおよびそのプロファイルの有効なパスワードであるか、UID およびパスワードを妥当性検査します。i5/OS 以外のユーザーを手動でディレクトリーに追加する一方で、LDAP 認証を使用し、

既存のユーザーが自身のオペレーティング・システム・パスワードを使用して認証できるようにするには、この機能の使用を検討する必要があります。

ユーザーを公開するもう 1 つの方法は、既存の HTTP 妥当性検査リストから項目を入手して、ディレクトリー・サーバー中に対応する LDAP 項目を作成する方法です。これは、QGLDPUBVL アプリケーション・プログラム・インターフェース (API) を介して実行されます。この API は、オリジナルの妥当性検査リスト項目とリンクしたパスワードの inetOrgPerson ディレクトリー項目を作成します。この API は、ディレクトリー・サーバーに追加する新規の項目を検査するために一度だけ実行することも、また、定期的に行うようにスケジュールすることもできます。

注: HTTP サーバー (Apache 付き) で使用するために作成された妥当性検査リスト項目のみがこの API でサポートされます。ディレクトリー・サーバーの既存の項目は更新されません。妥当性検査リストから削除されたユーザーは検出されません。

ユーザーをディレクトリーに追加すると、ユーザーは LDAP 認証をサポートするアプリケーションだけでなく、妥当性検査を使用するアプリケーションに対しても認証することができます。

システム情報

Directory Server に対して情報タイプ「システム」を公開するようにオペレーティング・システムを構成すると、以下のタイプの情報が公開されます。

- このマシンおよびオペレーティング・システムのリリースについての基本情報。
- オプションとして、1 つ以上のプリンターを選択して公開可能。その場合は、システム上でそのプリンターに変更があれば、常にシステムが LDAP ディレクトリーを自動的に同期化します。

公開できるプリンター情報には以下が含まれます。

- 存在場所
- 速度 (ページ/分)
- 両面印刷およびカラーのサポート
- タイプおよびモデル
- 説明

この情報は、公開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。この情報は、公開するプリンターを選択する時に最初に公開され、印刷装置書出プログラムが停止または開始される時、またはプリンターのデバイス記述が変更されるときに更新されます。

プリンター共用

プリンター共用を公開するようにオペレーティング・システムを構成すると、選択した iSeries ネットサーバー™・プリンター共用に関する情報は、構成された Active Directory サーバーに公開されます。Active Directory に対して印刷共用情報を公開すると、ユーザーが Windows® 2000 の「プリンタの追加ウィザード」を使って、System i プリンターを Windows 2000 デスクトップに追加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。印刷共用情報は、Microsoft の Active Directory スキーマをサポートしているディレクトリー・サーバーに対して公開する必要があります。

TCP/IP Quality of Service

TCP/IP Quality of Service (QOS) サーバーは、IBM 定義のスキーマを使用して LDAP ディレクトリーに定義された共用 QOS ポリシーを使用するように構成できます。QOS サーバーは、TCP/IP

QOS 公開エージェントを使用してポリシー情報を読み取ります。TCP/IP QOS 公開エージェントは、サーバー、認証情報、およびディレクトリー内のどこにポリシー情報が保管されているかを定義します。

追加の公開エージェントを定義し、ディレクトリー公開 API を活用することにより、このフレームワークを使用して LDAP ディレクトリー内の他の種類の情報を公開または検索するようにアプリケーションを作成できます。

関連概念

Lightweight Directory Access Protocol (LDAP) API

Directory Server API の詳細は、『Lightweight Directory Access Protocol (LDAP) APIs』を参照してください。

関連タスク

145 ページの『Directory Server への情報の公開』

以下の情報を参考にして、Directory Server へ情報を公開します。

複製

複製は、パフォーマンスおよび信頼性を向上させるためにディレクトリー・サーバーで使用される技法です。複製プロセスにより、複数のディレクトリー内のデータが同期化された状態を保ちます。

複製について詳しくは、以下を参照してください。

関連概念

164 ページの『複製タスク』

以下の情報を参考にして、複製を管理します。

109 ページの『複製サーバーのネットワークのマイグレーション』

複製サーバーのネットワークを使用する場合、以下の情報を参考してください。

複製の概要

複製の時、1 つのディレクトリーに行われた変更は、1 つ以上の追加のディレクトリーに伝搬します。それにより、1 つのディレクトリーに変更を行うと、複数の異なるディレクトリーに影響します。

複製には、2 つの主な利点があります。

- 情報の冗長度 - レプリカは、そのサプライヤー・サーバーの内容をバックアップします。
- より高速な検索 - 検索要求を、単一のサーバーにではなく、すべてが同じ内容を持つ幾つかの異なるサーバーに分散して送信できます。これにより、要求の完了の応答時間が向上します。

ディレクトリー内の特定の項目に `ibm-replicationContext objectclass` を追加することにより、それらは複製されたサブツリーのルートとして識別されます。各サブツリーは、独立して複製されます。サブツリーは、リーフ項目またはその他の複製されたサブツリーに到達するまでディレクトリー情報ツリー (DIT) を下っていきます。複製トポロジー情報を含む項目が複製されたサブツリーのルートの下に追加されます。これらの項目は 1 つ以上のレプリカ・グループ記入項目で、その下にレプリカ副項目が作成されます。各サーバーにより提供されるサーバー (複製先のサーバー) を識別し、信任状およびスケジュール情報を定義するレプリカ合意は、各レプリカ副項目に関連付けられます。

IBM Directory は、拡張されたマスター/従属複製モデルをサポートします。複製トポロジーは拡張されて以下を含みます。

- 特定のサーバーのディレクトリー情報ツリー (DIT) のサブツリーの複製
- カスケード複製と呼ばれる複数層トポロジー

- サブツリーによるサーバーの役割 (マスターまたはレプリカ) の割り当て
- 複数のマスター・サーバー。ピアツーピア複製と呼ばれる。
- ネットワーク全体でのゲートウェイ複製

サブツリーによる複製の利点は、レプリカはディレクトリー全体を複製する必要がないという点です。ディレクトリーの一部、つまりサブツリーのレプリカを作成できます。

拡張モデルにより、マスターおよびレプリカ概念は変化します。これらの用語はサーバーにではなく、複製される特定のサブツリーに関してサーバーが持つ役割に適用されるようになりました。サーバーは、幾つかのサブツリーに対してはマスター、他のサブツリーに対してはレプリカとして機能します。マスターという用語は、複製されるサブツリーに対するクライアント更新を受け入れるサーバーに使用されます。レプリカという用語は、複製されるサブツリーのサブライヤーとして指定された他のサーバーからの更新のみを受け入れるサーバーに使用されます。

機能によって定義されるサーバーのタイプは、マスター/ピア、カスケード、ゲートウェイ、およびレプリカがあります。

表 1. サーバーの役割

| ディレクトリー | 説明 |
|---------------|---|
| マスター/ピア | <p>マスター/ピア・サーバーには、マスター・ディレクトリー情報が含まれています。更新情報は、ここからレプリカに伝搬されます。すべての変更は、マスター・サーバー上で行われ、マスターはこれらの変更をレプリカに伝搬させる責任があります。</p> <p>ディレクトリー情報のマスターとして機能する幾つかのサーバーが存在する可能性があり、その場合、各マスターは、他のマスター・サーバーおよびレプリカ・サーバーを更新する責任があります。これはピア複製と呼ばれます。ピア複製により、パフォーマンスと信頼性が向上します。パフォーマンスは、広範囲に分散したネットワークで更新を処理するローカル・サーバーの提供により向上します。信頼性は、1 次マスターに障害が起こった場合ただちに引き継ぐことが可能なバックアップ・マスター・サーバーの提供により向上します。</p> <p>Lotus Notes:</p> <ol style="list-style-type: none"> 1. マスター・サーバーはすべてのクライアント更新を複製しますが、他のマスターから受け取った更新は複製しません。 2. 競合解決が行われなため、複数のサーバーが同じ項目を更新すると、ディレクトリー・データが矛盾する場合があります。 |
| カスケード (転送) | <p>カスケード・サーバーは、送られてきた変更をすべて複製するレプリカ・サーバーです。これは、サーバーに接続されているクライアントによる変更のみを複製するマスター/ピア・サーバーとは対照的です。カスケード・サーバーは、多くのレプリカが広く分散されたネットワークで、マスター・サーバーの複製ワークロードを緩和できます。</p> |
| ゲートウェイ | <p>ゲートウェイ複製はゲートウェイ・サーバーを使用して、複製するネットワーク上で複製情報を効果的に収集して配布します。ゲートウェイ複製の主な利点は、ネットワーク・トラフィックの削減にあります。</p> |
| レプリカ (読み取り専用) | <p>レプリカは、ディレクトリー情報のコピーを持つ追加のサーバーです。レプリカは、マスターのコピーです (またはそれ自身がレプリカであるサブツリーです)。レプリカは、複製されたサブツリーのバックアップとしての役割も果たします。</p> |

複製に失敗した場合は、マスターを再始動しても引き続き失敗します。 Web 管理ツールの「キューの管理」ウィンドウを使用して、失敗する複製を検査できます。

レプリカ・サーバーで更新を要求できますが、実際には、参照をクライアントに戻すことによって更新がマスター・サーバーに転送されます。更新が正常に完了した場合は、マスター・サーバーは更新をレプリカに送信します。マスターが更新情報の複製を完了するまでは、要求元のレプリカ・サーバーにその変更は反映されません。変更は、マスターで行われた順序で複製されます。

レプリカを使用しなくなった場合は、サプライヤーからレプリカ合意を除去する必要があります。レプリカの定義を残しておくこと、サーバーがすべての更新情報をキューに入れるため、ディレクトリー・スペースが無駄に使用されることがあります。また、サプライヤーは欠落しているコンシューマーへの接続を試行し、データの送信を再試行します。

ゲートウェイ複製

ゲートウェイ複製はゲートウェイ・サーバーを使用して、複製するネットワーク上で複製情報を効果的に収集して配布します。ゲートウェイ複製の主な利点は、ネットワーク・トラフィックの削減にあります。ゲートウェイ・サーバーはマスター（書き込み可能）でなければなりません。

以下の図は、ゲートウェイ複製の作業方法を示しています。

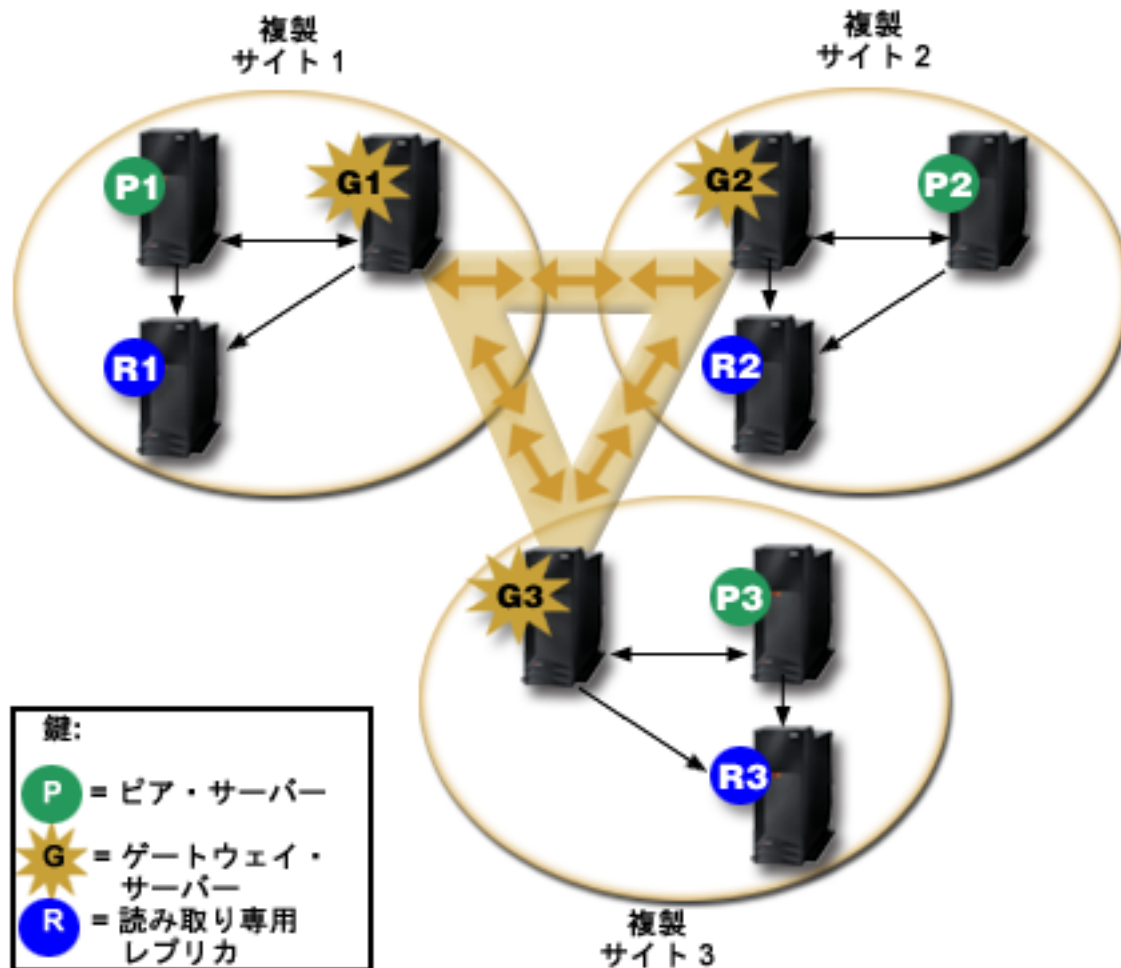


図3. 複製するネットワークとゲートウェイ・サーバー

上記の図の複製するネットワークには、3つの複製サイトがあり、それぞれにゲートウェイ・サーバーが含まれています。ゲートウェイ・サーバーは、複製サイト中のピア/マスター・サーバーから複製更新を収集します。ゲートウェイ・サーバーは複製サイトに常駐して、複製するネットワーク内の他のすべてのゲートウェイ・サーバーに更新を送信します。また、ゲートウェイ・サーバーは、複製ネットワーク中の他のゲートウェイ・サーバーからも複製更新を収集し、ゲートウェイ・サーバーが常駐する複製サイト中のピア/マスターとレプリカにこれらの更新を送信します。

ゲートウェイ・サーバーはサーバー ID およびコンシューマー ID を使用して、複製するネットワーク中の他のゲートウェイ・サーバーに送信する更新を決定し、複製サイト中のローカル・サーバーに送信する更新を決定します。

ゲートウェイ複製をセットアップするには、少なくとも2つのゲートウェイ・サーバーを作成する必要があります。ゲートウェイ・サーバーの作成により複製サイトが確立されます。その後、ゲートウェイと、ゲートウェイの複製サイトに組み込みたいすべてのマスター/ピアおよびレプリカとの間の複製の合意を作成する必要があります。

ゲートウェイ・サーバーはマスター（書き込み可能）でなければなりません。ゲートウェイ・オブジェクト・クラス `ibm-replicaGateway` をマスターでないサブエントリに追加しようとすると、エラー・メッセージが戻されます。

ゲートウェイ・サーバーを作成する方法は2つあります。以下を行うことができます。

- 新規のゲートウェイ・サーバーを作成する
- 既存のピア・サーバーをゲートウェイ・サーバーに変換する

注: それぞれの複製サイトに割り当てるゲートウェイ・サーバーは1つのみであることに注意してください。

1 複製の競合の解決

1 複数のマスター・サーバーを擁するネットワークでは、競合しあう変更を項目に加える可能性があります。
1 そのため、変更の複製後に、それぞれ異なる項目データがサーバーに存在することもあります。競合しあ
1 う変更はあまり起きません。なぜなら、別々のマスター・サーバー上でほぼ同時に変更が加えられる必要が
1 あるからです。競合する変更の例をいくつか以下に示してあります。

- 1 • 2つのサーバー上でそれぞれ異なる属性を持った同じ項目を追加した場合。
- 1 • 2つのサーバー上でそれぞれ異なるパスワードを使用して、項目のパスワードをリセットした場合。
- 1 • 1つのサーバー上で項目の名前を変更する一方で、別のサーバー上で項目を変更した場合。

1 IBM Tivoli Directory Server には、競合する変更を自動的に検出して解決する機能が備えられています。こ
1 れにより、すべてのサーバー上のディレクトリーの整合性が保たれます。複製の競合が検出されると、競合
1 している変更がサーバー・ログにレポートされるとともに、「遺失物取り扱い」ログ・ファイルにも記録さ
1 れます。これにより、管理者は消失したデータをリカバリーすることができます。

1 対等複製での追加および変更の操作における競合解決は、項目および変更のタイム・スタンプをベースとし
1 ます。マスターが複数ある複製環境で、任意のサーバー上で最新のタイム・スタンプを持った更新が、優先
1 される更新です。複製で競合が検出されると、置き換えられる項目は、リカバリーに備えて遺失物取り扱い
1 ログにアーカイブされます。

1 複製済みの削除要求と名前変更要求は、競合解決なしに、受信順に受け入れられます。削除または
1 `modifyDN` (名前変更または移動) 操作がからんだ複製競合が起きた場合、結果的に人的介入を必要とするエ
1 ラーになります。たとえば、1つのサーバーで項目の名前が変更される一方で、別のサーバーでその項目が

変更される場合、複製は、変更操作の前に rename modifyDN 操作に到達することがあります。すると、変更操作に到達した時点で、その操作は失敗します。この場合、管理者は、新しい DN を使用して項目に変更を適用することによって、そのエラーに対処する必要があります。正しい名前を使用して変更をやり直すのに必要なすべての情報は、複製ログとエラー・ログに保存されています。このような複製エラーは、正しく構成された複製トポロジーではめったにありませんが、絶対に起きないと想定するのは安全ではありません。

複数のサーバーが同じ項目を更新すると、ディレクトリー・データに矛盾が起きる場合があります。それは、競合解決は、項目のタイム・スタンプに基づいて行われるからです。最新の変更のタイム・スタンプが優先されます。サーバー上のデータで不整合が生じた場合、以下の関連リンクの ldapdiff のトピックを参照して、サーバーの再同期方法を確認してください。

複製の競合を解決するには、サプライヤー上での項目の更新の前のその項目のタイム・スタンプがサプライヤーから提供される必要があります。V5R4 またはそれ以前のバージョンでは、IBM Tivoli Directory Server for i5/OS には、この種の情報を提供する機能はありません。したがって、サプライヤーが下位レベルのサーバーである場合は、複製の競合の解決は適用されません。V6R1 では、そのような場合、the IBM Tivoli Directory Server for i5/OS コンシューマー・サーバーが複製済みのタイム・スタンプを取り込んで、競合の検査なしにそれを更新して適用します。

注: 旧バージョンの IBM Tivoli Directory Server for i5/OS は、タイム・スタンプによる競合の解決をサポートしません。旧バージョンの IBM Tivoli Directory Server for i5/OS がトポロジーに入っている場合、ネットワーク上のデータの整合性は確保されません。

競合しあった変更が起きないようにするには、ロード・バランサー、仮想 IP アドレスの引き継ぎ、またはその他の手段を用いて、優先サーバーが使用不可になった場合には他のサーバーへの自動フェイルオーバーを配備したうえで、必ず 1 つのサーバーに対してディレクトリーの変更を加えるようにします。

IBM WebSphere® Edge Server などのロード・バランサーには、ディレクトリーへの更新の送信時にアプリケーションで使用される仮想ホスト名が用意されています。ロード・バランサーは、1 つのサーバーにのみ更新を送信するように構成されています。そのサーバーが停止している場合や、ネットワーク障害が原因で利用できない場合、そのサーバーがオンラインに戻って利用不可になるまで、ロード・バランサーは次に利用可能な対等サーバーに更新を送信し続けます。ロード・バランシング・サーバーのインストールと構成の方法の詳細は、ロード・バランサー製品資料を参照してください。

関連タスク

184 ページの『遺失物取り扱いログの設定の変更』

遺失物取り扱いログ (デフォルト名は LostAndFound.log) は、複製の競合として生じたエラーを記録します。ファイルのロケーションと最大サイズや、古いログ・ファイルのアーカイブも含め、遺失物取り扱いログを制御するための設定があります。

172 ページの『ピア複製での単純なトポロジーの作成』

ピア複製とは、複数のサーバーがマスターとなる複製トポロジーです。ピア複製は、更新ベクトルが十分認知されている環境でのみ使用してください。

関連資料

277 ページの『ldapdiff』

LDAP レプリカ同期コマンド行ユーティリティー

複製の用語

複製の解説で使用される特定の用語の定義。

カスケード複製

複数のサーバー層がある複製トポロジー。ピア/マスター・サーバーは、読み取り専用 (転送) サーバーのセットに複製された後、他のサーバーに複製されます。このようなトポロジーにより、マスター・サーバーからの複製作業の負荷が軽減されます。

コンシューマー・サーバー

別の (サプライヤー) サーバーからの複製を介して変更を受け取るサーバー。

信任状 サプライヤーがコンシューマーへのバインドに使用するメソッドおよび必要情報を識別します。単純なバインドの場合は、DN およびパスワードが含まれます。信任状は、レプリカ合意で指定された DN の項目に保管されます。

転送サーバー

マスターまたはピアにより送信されたすべての変更を複製する読み取り専用サーバー。クライアント更新要求は、マスターまたはピア・サーバーを参照します。

ゲートウェイ・サーバー

ローカルの複製サイトに常駐するサーバーで、そのサイトからのすべての複製トラフィックを、複製するネットワーク中の他のゲートウェイ・サーバーに転送します。ゲートウェイ・サーバーは、複製ネットワーク中の他のゲートウェイ・サーバーから複製トラフィックを受け取り、ローカルの複製サイト上のすべてのサーバーに転送します。ゲートウェイ・サーバーはマスター (書き込み可能) でなければなりません。

マスター・サーバー

ある特定のサブツリーにおいて、書き込み可能な (更新可能な) サーバー。

ネストされたサブツリー

ディレクトリーの複製されたサブツリー内のサブツリー。

ピア・サーバー

ある特定のサブツリーに複数のマスターがある場合にマスター・サーバーに対して使用する用語。

レプリカ・グループ

複製コンテキストの下に最初に作成される項目は `objectclass ibm-replicaGroup` を持ち、複製に参加するサーバーの集合を表します。これは、複製トポロジー情報を保護するために ACL を設定する場所として便利です。現在、管理ツールは、各複製コンテキストの下の `ibm-replicagroup=default` という名前の 1 つのレプリカ・グループをサポートしています。

レプリカ副項目

レプリカ・グループ項目の下に `objectclass ibm-replicaSubentry` の項目を 1 つ以上作成できます。この場合、サプライヤーとして複製に参加するサーバーごとに 1 つ作成します。レプリカ副項目は、複製時のサーバーの役割 (マスターか読み取り専用か) を示します。読み取り専用のサーバーはレプリカ合意を持ち、カスケード複製をサポートできます。

複製されたサブツリー

あるサーバーから別のサーバーに複製される DIT の一部。この設計では、サブツリーを複製できるサーバーと、複製できないサーバーがあります。サブツリーは特定のサーバーでは書き込み可能ですが、他のサブツリーは読み取り専用場合があります。

複製するネットワーク

接続された複製サイトが入っているネットワーク。

レプリカ合意

2 つのサーバー間の「接続」または「複製パス」を定義するディレクトリー内に含まれている情

報。一方のサーバーはサプライヤー (変更を送信する側)、他方のサーバーはコンシューマー (変更を受信する側) と呼ばれます。合意には、サプライヤーからコンシューマーへの接続および複製の計画に必要な情報がすべて含まれています。

複製コンテキスト

複製サブツリーのルートを示します。 `ibm-replicationContext` 補助オブジェクト・クラスを項目に追加し、複製領域のルートとしてマークできます。複製トポロジーに関連した情報は、複製コンテキストの下に作成された項目のセットに保持されます。

複製サイト

総合複製のために構成されたゲートウェイ・サーバーおよびすべてのマスター、ピア、レプリカのサーバー。

スケジュール

サプライヤーが累積した変更内容をバッチで送信し、複製を特定の時点で行うようにスケジュールできます。レプリカ合意には、スケジュールを提供する項目の DN があります。

サプライヤー・サーバー

変更を別の (コンシューマー) サーバーに送信するサーバー。

1 マルチスレッド複製

- | マルチスレッド (非同期) 複製を介して、管理者は、マルチスレッド複製を使った複製を行うことができ、
 - | これにより、複製の総体的なスループットが向上します。

 - | 単一スレッド (同期) 複製を使用すれば、クライアントは、複製を他のサーバーに送信するよりも迅速に、
 - | 一貫したやり方で更新を行うことができます。その理由は、標準の複製モデルは単一スレッドを使用して、
 - | すべての変更を受信した順に複製するからです。

 - | また、たとえば、ターゲットの項目がコンシューマー・サーバー上に存在しないために、複製された変更要
 - | 求が失敗した場合など、特定のタイプのエラーが起きたときにも、標準の複製モデルはブロックされます。
 - | この動作は、訂正を必要とする複数のサーバーどうしの間の矛盾に注目を集める一方で、保留中の変更のバ
 - | ックログの巨大化につながる可能性もあります。アプリケーションによっては、このような未複製の変更の
 - | バックログは望ましくないことがあります。

 - | これに対処するため、マルチスレッド複製では、変更の失敗に関する情報をエラー・ログに記録したうえ
 - | で、残りの変更の処理を続ける機能が配備されています。このログには、どの項目に矛盾があるかと、スキ
 - | ップされた変更を判別するのに十分な情報が、エラーの訂正後に変更をやり直すためのツールとともに提供
 - | されます。重大な矛盾が原因で大量の変更がスキップされないようにするため、構成可能なエラーしきい値
 - | が用意されています。この値に達したら、エラーが訂正されて複製エラー・ログがクリアされるまで、複製
 - | はブロックされます。

 - | • サーバーまたはネットワークが信頼性に欠けるために、複製済みの多数の変更がスキップされる場合、
 - | マルチスレッド (非同期) 複製は、管理が困難になる可能性があります。

 - | エラーが起きると、そのエラーは記録されるので、管理者はそれを再現できますが、エラー・ログを丹念に
 - | モニターする必要があります。1 つのサーバーから提供されたすべての契約の複製バックログを表示する
 - | ための検索を以下に示してあります。
- ```
l ldapsearch -h supplier-host -D cn=admin -w ? -s sub
l objectclass=ibm-replicationagreement
l ibm-replicationpendingchangeount ibm-replicationstate
```
- | 複製の状態がアクティブであって、保留中のカウントが増大しつつある場合、更新率が減少するか、または
  - | 複製モードを同期から非同期 (マルチスレッド) に変更しない限り、バックログは減少しません。

複製はまた、更新が最初に適用される場所であるマスター・サーバーのワークロードを増大します。マスター・サーバーは、ディレクトリー・データのコピーの更新に加えて、すべてのレプリカ・サーバーに変更を送信する必要があります。アプリケーションまたはユーザーが即時の複製に頼る必要がない場合、アクティビティのピーク時を避けて慎重に複製をスケジューリングすることで、マスター・サーバーのスループットへの影響を最小化することができます。

マルチスレッド複製では、複製エラーが発生すると、以下が起きます。

- `ibm-slapdReplMaxErrors`: 0 は、複製エラー・ログにはエラーを記録しないで、すべてのエラーをサーバー・ログに記録し、すべてのエラーがクリアされるまで複製を中断することを意味します。
  - 契約に関するエラー数が限度を超えた場合、少なくとも 1 つのエラーがクリアされるか、または契約のエラー数限度を増やすまで、複製は中断されます。
  - 複製契約の状況は次のようになります。
- `ibm-replicationStatus`: エラー・ログがいっぱいです。

## 複製エラー・テーブル

後でリカバリするために、複製エラー・テーブルが失敗した更新を記録します。複製が開始すると、各複製契約ごとにログ記録された障害数がカウントされます。更新が結果として失敗すると、このカウントが増え、新しい項目がテーブルに追加されます。

複製エラー・テーブル内の各項目には、以下が示されます。

- 複製契約 ID。
- 複製変更 ID。
- 更新が試みられた時点のタイム・スタンプ。
- 実施された試行回数 (この値はデフォルトでは 1 であり、各試行ごとに増大します)。
- コンシューマーからの結果コード。
- たとえば、DN、実際のデータ、制御、フラグなどの、更新の一角を成す複製操作から得たすべての情報。

サーバー構成の属性 `ibm-slapdReplMaxErrors` で指定された値が 0 の場合、複製の更新処理は続けられます。属性 `ibm-slapdReplMaxErrors` は、複製構成項目内の属性であり、動的に変更することができます。

属性 `ibm-slapdReplMaxErrors` で指定された値が 0 より大きい場合に、複製契約のエラー件数がその値を超えると、複製では以下のいずれかが行われます。

- **単一スレッド**: 複製は、失敗した更新の複製を試みるためにループに入ります。
- **マルチスレッド**: 複製は中断します。

単一接続を使用するようにサーバーが構成されている場合、複製は、60 秒間待機した後、複製が正常に完了するかまたは管理者が更新をスキップするまで、同じ更新の送信を試み続けます。

複数の接続を使用するようにサーバーが構成されている場合、該当する契約の複製は中断されます。受信側のスレッドは、送信されてきたすべての更新からの状況のポーリングを続けますが、この時点以後は更新は複製されません。複製を再開するには、該当する契約での少なくとも 1 つのエラーをディレクトリー管理者が解消するか、またはサーバー構成の動的変更を使って限度を引き上げる必要があります。

詳細は、以下の関連リンクの『複製キューの管理』トピックを参照してください。また、以下の関連リンクの `ldapexop` トピックの中の `-op controlreplerr` オプションも参照してください。

## 関連タスク

- | 183 ページの『複製キューの管理』
- | 以下の情報を参考にして、このサーバーで使用される複製契約 (キュー) ごとに複製の状況をモニター
- | します。
- | **関連資料**
- | 252 ページの『ldapexop』
- | LDAP 拡張操作コマンド行ユーティリティー

## レプリカ合意

レプリカ合意は、レプリカ副項目の下に作成されたオブジェクト・クラス **ibm-replicationAgreement** のディレクトリーの項目であり、副項目によって表されたサーバーから別のサーバーへの複製を定義します。

これらのオブジェクトは、以前のバージョンの Directory Server で使用していた `replicaObject` 項目に似ています。レプリカ合意は、以下の項目で構成されます。

- 合意の命名属性として使用される、分かりやすい名前。
- LDAP サーバー、ポート番号、および SSL を使用するかどうかを指定する LDAP URL。
- コンシューマー・サーバー ID (既知の場合)。V5R3 より前のディレクトリー・サーバーには、サーバー ID はありません。
- サプライヤーがコンシューマーにバインドするために使用する信任状を含むオブジェクトの DN。
- 複製のためのスケジュール情報を含むオブジェクトへのオプションの DN ポインター。この属性が存在しない場合は、変更がただちに複製されます。

分かりやすい名前は、コンシューマー・サーバー名などの説明的なストリングです。

コンシューマー・サーバー ID は、トポロジーを全探索するために管理 GUI が使用します。コンシューマー・サーバー ID を指定すると、GUI は対応する副項目とその合意を検索できます。データの正確性を確保するために、サプライヤーは、コンシューマーにバインドするときにサーバー ID を root DSE から取得し、合意の値と比較します。サーバー ID が一致しない場合は、警告がログに記録されます。

レプリカ合意は複製できるため、信任状オブジェクトへの DN が使用されます。これにより、ディレクトリーの複製されない領域に信任状を保管できます。(「平文」の信任状の取得元になる) 信任状オブジェクトを複製するという事は、機密漏れが発生する可能性があることを示します。 `cn=localhost` 接尾部は、信任状オブジェクトを作成するための適切なデフォルトの場所です。

オブジェクト・クラスは、サポートされている以下の認証方法ごとに定義されます。

- 単純なバインド
- SASL
- SSL を使用した EXTERNAL メカニズム
- Kerberos 認証

レプリカ副項目を定義せずに `ibm-replicationContext` 補助クラスをサブツリーのルートに追加することによって、複製されるサブツリーの一部を複製しないことを指定できます。

**注:** Web 管理ツールでは、ある合意の下に、複製されるのを待機している変更のセットを指す場合、合意を「キュー」とも呼びます。

- | 単スレッド複製方式を使った複製契約の場合、コンシューマー接続数は常に 1 であり、属性値は無視さ
- | れます。マルチスレッド複製を使った契約の場合、1 から 32 までの接続数を構成することができます。契
- | 約で何も値を指定しないと、コンシューマー接続数は 1 に設定されます。



- 注: cn=ibmpolicies サブツリーの場合、どの複製契約でも、単一スレッド複製方式と 1 つのコンシューマー接続が使用され、属性値は無視されます。

## 複製情報がサーバーに保管される方法

複製情報は、ディレクトリー内のいくつかの場所に保管されます。

- サーバー構成。ここには、複製をするために他のサーバーがこのサーバーに認証する方法に関する情報が含まれます (たとえば、このサーバーがサプライヤーとして機能することを許可する人など)。
- 複製されるサブツリーの先頭にあるディレクトリー。「o=my company」が複製されるサブツリーの先頭である場合、「ibm-replicagroup=default」という名前のオブジェクトがその直下に作成されます (ibm-replicagroup=default,o=my company)。「ibm-replicagroup=default」オブジェクトの下には、サブツリーのレプリカを保持するサーバーおよびサーバー間の合意を記述する追加オブジェクトがあります。
- 「cn=replication,cn=localhost」という名前のオブジェクトは、1 つのサーバーのみにより使用される複製情報を収容するために使用されます。たとえば、サプライヤー・サーバーにより使用される信任状を収容するオブジェクトは、サプライヤー・サーバーのみが必要とします。信任状を「cn=replication,cn=localhost」の下に置くならば、そのサーバーのみがそれにアクセス可能になります。
- 「cn=replication, cn=IBMpolicies」という名前のオブジェクトは、他のサーバーに複製される複製情報を収容するために使用されます。

## 複製情報のセキュリティ考慮事項

特定のオブジェクトのセキュリティ考慮事項を検討してください。

- **ibm-replicagroup=default**: このオブジェクト上のアクセス制御は、ここに保管された複製情報を表示または変更できる人を制御します。デフォルトでは、このオブジェクトはアクセス制御をその親から継承します。このオブジェクト上にアクセス制御を設定して、複製情報へのアクセスを制限することを考える必要があります。たとえば、複製を管理するユーザーを含むグループを定義できます。このグループを「ibm-replicagroup=default」オブジェクトの所有者とし、他のユーザーにそのオブジェクトへのアクセス権を与えないようにすることができます。
- **cn=replication,cn=localhost**: このオブジェクトには、2 つのセキュリティ考慮事項があります。
  - このオブジェクト上のアクセス制御は、ここに保管されたオブジェクトを表示または更新する許可を持つ人を制御します。デフォルトのアクセス制御では、匿名ユーザーはパスワード以外のほとんどの情報を読み取る許可があり、オブジェクトの追加、変更、または削除には管理者権限が必要です。
  - 「cn=localhost」に保管されているオブジェクトは、他のサーバーには決して複製されません。複製信任状は、信任状を使用するサーバー上のこのコンテナに置くことができ、他のサーバーはそれらにアクセスできません。代わりに、信任状を「ibm-replicagroup=default」オブジェクトの下に置くことを選択することもでき、そうすると、複数のサーバーが同じ信任状を共有します。
- **cn=IBMpolicies**: 複製信任状はこのコンテナに入れることができますが、その中のデータはサーバーのすべてのコンシューマーに複製されます。信任状を **cn=replication,cn=localhost** に置くほうが安全性が高くなります。

## 高可用性環境での複製

Directory Server は、多くの場合にシングル・サインオン・ソリューションで使用されますが、その結果、Single Point of Failure となる可能性があります。

複製の 2 つの方法、すなわち、IBM ロード・バランサーまたは IP アドレスの引き継ぎを使用することによって、Directory Server の可用性を高めることができます。このトピックの詳細については、IBM Redbooks 資料「*IBM WebSphere V5.1*」の第 13.2 章『*Performance, Scalability, and High Availability*』に説明されています。

## 関連情報



IBM WebSphere V5.1 Performance, Scalability, and High Availability

## レルムおよびユーザー・テンプレート

Web 管理ツール内に置かれているレルムおよびユーザー・テンプレート・オブジェクトを使用することにより、LDAP の幾つかの基礎的な問題を理解する必要がなくなります。

レルムは、ユーザーおよびグループの集合を示します。それは、ユーザーが置かれている場所、グループが置かれている場所などのフラットなディレクトリー構造内の情報を指定します。レルムは、ユーザーの場所を定義し（たとえば、「cn=users,o=acme,c=us」など）、この項目のすぐ下の従属としてユーザーを作成します（たとえば、John Doe は「cn=John Doe,cn=users,o=acme,c=us」として作成されます）。複数のレルムを定義し、それらに分かりやすい名前を付けることができます（たとえば、Web Users など）。分かりやすい名前は、ユーザーを作成し保守する人により使用されます。

テンプレートは、ユーザーの外観を記述します。それはユーザーを作成するときに使用される `objectclass` (構造化 `objectclass` および含めたい任意の補助クラス) を指定します。さらにテンプレートは、ユーザーを作成または編集するために使用されるパネルのレイアウトを指定します（たとえば、タブの名前、デフォルト値、および各タブに表示される属性）。

新規レルムを追加する時、そのディレクトリーに `ibm-realm` オブジェクトが作成されます。 `ibm-realm` オブジェクトは、ユーザーおよびグループが定義される場所、使用するテンプレートなど、レルムのプロパティを追跡します。 `ibm-realm` オブジェクトは、ユーザーの親である既存のディレクトリー項目を指すことができます。または、それはそれ自体を指すこともでき（デフォルト）、その場合それは新規ユーザー用のコンテナとなります。たとえば、既存の `cn=users,o=acme,c=us` コンテナを持ち、ユーザーおよびグループの場所として `cn=users,o=acme,c=us` を示すディレクトリー（おそらく `cn=realms,cn=admin stuff,o=acme,c=us` と呼ばれるオブジェクト）内の他の場所に `users` という名前のレルムを作成します。これにより、`ibm-realm` オブジェクトが作成されます。

```
dn: cn=users,cn=realms,cn=admin stuff,o=acme,c=us
objectclass: top
objectclass: ibm-realm
objectclass: ibm-staticGroup
ibm-realmUserTemplate: cn=users template,cn=realms,cn=admin stuff,o=acme,c=us
ibm-realmUserContainer: cn=users,o=acme,c=us
ibm-realmGroupContainer: cn=users,o=acme,c=us
ibm-realmAdminGroup: cn=users,cn=realms,cn=admin stuff,o=acme,c=us
ibm-realmUserSearchFilter:
cn: users
```

または、既存の `cn=users,o=acme,c=us` オブジェクトがなかった場合、レルム `users` を `o=acme,c=us` の下に作成し、それがそれ自体を指すようにできます。

ディレクトリー管理者は、ユーザー・テンプレート、レルム、およびレルム管理者グループを管理する責任があります。レルムの作成後、そのレルムの管理者グループのメンバーは、その領域内のユーザーおよびグループを管理する責任があります。

### 関連概念

230 ページの『レルムおよびユーザー・テンプレートのタスク』

以下の情報を参考にして、レルムおよびユーザー・テンプレートを管理します。

### 関連タスク

231 ページの『レルムの作成』

以下の情報を参考にして、レルムを作成します。

## 検索パラメーター

サーバーで使用するリソース量を制限するために、管理者は検索パラメーターを使用して、ユーザーの検索能力を制限することができます。また、特定のユーザーの検索能力を拡張することもできます。

ユーザー検索は以下の方法を使用して制限または拡張することができます。

### 検索の制限

- ページ検索
- ソート検索
- 別名参照解除を使用不可にする

### 検索の拡張

- 検索限界グループ

### ページ検索

ページ結果によって、クライアントは検索要求から戻されたデータの量を管理できます。クライアントはサーバーからすべての結果を一度に受け取る代わりに、項目のサブセット (ページ) を要求できます。以降の検索要求により、結果の次のページを戻します。これは操作が取り消されるか、最後の結果が戻されるまで続けられます。管理者は、管理者のみに使用を許可することによってその使用を制限することができます。

### ソート検索

ソート検索により、クライアントが、基準のリスト (各基準はソート・キーを表す) によりソートされた検索結果を受け取ることが可能になります。これにより、ソートの責任は、クライアント・アプリケーションからサーバーに移ります。管理者は、管理者のみに使用を許可することによってその使用を制限することができます。

### 別名参照解除を使用不可にする

alias または aliasObject のオブジェクト・クラスのディレクトリー項目には属性 aliasedObjectName が含まれていて、これを使用してディレクトリーの他の項目を参照します。検索要求を指定できるのは、別名が参照解除された場合のみです。参照解除とは、別名をオリジナル項目にトレースバックすることです。別名項目がディレクトリーに存在しない場合でも、別名参照解除オプションを「常に実行 (Always)」または「検索して実行 (Search)」に設定して検索する場合に、IBM Directory Server の応答時間は、参照解除オプションを「実行しない (Never)」に設定した検索の時間よりも大幅に長くなることがあります。2 つの設定はサーバーの別名参照解除動作を決定します。すなわち、クライアントの検索要求によって指定される参照解除オプションと、管理者によってサーバーに構成される参照解除オプションです。このように構成された場合、別名オブジェクトがディレクトリー中に存在しない場合にサーバーは別名参照解除を自動的に迂回して、クライアントの検索要求に指定された参照解除オプションをオーバーライドできます。以下の表では、クライアントとサーバー間での別名参照解除のハッシュ方法を説明しています。

表 2. クライアントおよびサーバー設定に基づいた実際の別名参照解除

| サーバー   | クライアント | 実際        |
|--------|--------|-----------|
| never  | 不特定の設定 | never     |
| always | 不特定の設定 | クライアントの設定 |
| 不特定の設定 | always | サーバーの設定   |
| search | find   | never     |
| find   | search | never     |

## 検索限界グループ

管理者は、一般ユーザーより柔軟な検索限界を設定できる検索限界グループを作成することができます。検索限界グループに入っている個別メンバーまたはグループは、一般ユーザーに課せられる制限よりも、緩やかに限定された検索限界が許可されます。

ユーザーが検索を開始すると、まず始めに、検索要求制限が検査されます。ユーザーが検索限界グループのメンバーである場合は、その制限が比較されます。検索限界グループの制限がその検索要求の制限より高い場合には、その検索要求制限が使用されます。検索要求の制限が検索限界グループの制限より高い場合は、その検索限界グループの制限が使用されます。検索限界グループの項目が見つからない場合、サーバー検索限界に対して同じ比較が行われます。サーバー検索限界が設定されていない場合は、デフォルトのサーバー設定に対して比較が行われます。使用される制限は常に、その比較で最も低い設定となります。

ユーザーが複数の検索限界グループに属している場合は、ユーザーには、その検索能力で最も高いレベルまで認可されます。例えば、ユーザーが検索グループ 1 に属していると、2000 項目の検索サイズと、4000 秒の検索時間の検索限界が許可されます。検索グループ 2 に属していると、無制限の項目数の検索サイズと、3000 秒の検索時間の検索限界が許可されます。このユーザーには、無制限の検索サイズ、および 4000 秒の検索時間の検索限界が課せられます。

検索限界グループは localhost または IBMpolicies のいずれかに保管することができます。IBMpolicies にある検索限界グループは複製されますが、localhost にあるグループは複製されません。同じ検索限界グループを localhost と IBMpolicies の両方に保管することができます。検索限界グループがこれらの DN の 1 つに保管されていない場合、サーバーはそのグループの検索限界の部分を見捨て、正常グループとして取り扱います。

ユーザーが検索を開始すると、まず始めに、localhost にある検索限界グループの項目が検査されます。そのユーザーについての項目が見つからない場合、次に IBMpolicies にある検索限界グループの項目が検索されます。localhost で項目が見つかったら、IBMpolicies にある検索限界グループの項目は検査されません。localhost にある検索限界グループの項目は IBMpolicies にある項目よりも優先されます。

### 関連概念

152 ページの『検索限界グループのタスク』

以下の情報を参考にして、検索限界グループを管理します。

### 関連タスク

143 ページの『検索設定の調整』

以下の情報を参考にして、ユーザーの検索機能を制御します。

224 ページの『ディレクトリー項目の検索』

以下の情報を参考にして、ディレクトリー項目を検索します。

## 各国語サポート (NLS) に関する考慮事項

NLS に関する考慮事項には、データ・フォーマット、文字、マッピング方式、およびストリングの大文字小文字などがあります。

以下の NLS 考慮事項に注意してください。

- 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。
- Directory Server 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/小文字を区別しないで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。

### 関連情報

i5/OS グローバリゼーション

NLS に関する考慮事項の詳細は、『i5/OS グローバリゼーション』を参照してください。

## 言語タグ

言語タグ の用語は次のメカニズムを定義します。これによって、Directory Server 中で自然言語コードとディレクトリーに保持された値を関連付けて、特定の自然言語の要件を満たす値をクライアントがディレクトリーで照会できるようになります。

言語タグは属性記述の 1 つのコンポーネントです。言語タグは、接頭部 lang-、英字の基本サブタグ、およびオプションに、ハイフン (-) で結合された後続のサブタグをもつストリングです。後続のサブタグでは、英数字を任意に組み合わせることができますが、基本サブタグは英字のみでなければなりません。サブタグは任意の長さになりますが、唯一、タグの合計長が 240 文字を超えてはいけなく、という制限があります。言語タグには大/小文字の区別がないので、en-us、en-US、および EN-US はみな同じになります。言語タグは DN または RDN のコンポーネント内では使用できません。属性記述で使用できる言語タグは、各記述に 1 つのみです。

注: それぞれの属性単位では、言語タグは固有属性と互いに排他的に使用されます。特にその属性を固有属性として指定した場合は、それと関連付ける言語タグをもつことはできません。

データをディレクトリーに追加する時に言語タグを組み込む場合は、検索操作でこれを使用して、特定言語の属性値を選択して検索できます。検索で要求した属性リスト内の属性記述に言語タグを指定すると、指定されたものと同じ言語タグをもつディレクトリー項目内の属性値のみが戻されることになります。したがって、検索は次のようになります。

```
ldapsearch -b "o=ibm,c=us" (objectclass=organization) description;lang=en
```

サーバーは属性「description;lang=en」の値を戻しますが、属性「description」または「description;lang-fr」の値は戻しません。

属性を指定し、言語タグを指定しないで要求が行われた場合は、その言語タグとは関係なく、すべての属性値が戻されます。

属性タイプと言語タグはセミコロン (;) 文字で区切られます。

注: セミコロン文字は AttributeType の「NAME」の部分で使用することができます。ただし、この文字は AttributeType と言語タグを区切るために使用しているので、AttributeType の「NAME」の部分にこれを使用することはできません。

例えば、クライアントが「description」属性を要求し、突き合わせ項目に以下のものが含まれている場合は、次のようになります。

```
objectclass: top
objectclass: organization
o: Software GmbH
description: software
description;lang=en: software products
description;lang-de: Softwareprodukte
postalAddress: Berlin 8001 Germany
postalAddress;lang-de: Berlin 8001 Deutschland
```

サーバーは次のものを戻します。

```
description: software
description;lang-en: software products
description;lang-de: Softwareprodukte
```

検索で「description;lang-de」属性を要求した場合、サーバーは次のものを戻します。

```
description;lang-de: Softwareprodukte
```

言語タグを使用すると、各種の言語で作動するクライアントをサポートできるディレクトリー内で多国語データを使用することができます。言語タグを使用すると、ドイツ語クライアントは lang-de 属性で入力されたデータのみを見ることになり、フランス語クライアントは lang-fr 属性で入力されたデータのみを見る、というようなアプリケーションを作成できます。

言語タグ機能が使用可能かどうかを判別するには、属性「ibm-enabledCapabilities」を指定して、次のように root DSE 検索を行ってください。

```
ldapsearch -b "" -s base objectclass=* ibm-enabledCapabilities
```

OID "1.3.6.1.4.1.4203.1.5.4" が戻された場合は、その機能は使用可能になっています。

言語タグ・サポートが使用可能でない場合は、言語タグと属性を関連付ける LDAP 操作は拒否されて、エラー・メッセージが出されます。

一部の属性はそれと関連付けられる言語タグをもつことができますが、タグを持っていないものもあります。その属性で言語タグが使用可能かどうかを判別するには、ldapexop コマンドを使用してください。

- 言語タグを使用できる属性の場合: ldapexop -op getattributes -attrType language\_tag -matches true
- 言語タグを使用できない属性の場合: ldapexop -op getattributes -attrType language\_tag -matches false

#### 関連タスク

220 ページの『言語タグの付いた属性を備えた項目の追加』

以下の情報を参考にして、言語タグの付いた属性を備えた項目を作成します。

## 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 Directory Server 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。

Directory Server 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:** Directory Server では、参照オブジェクトには、識別名 (dn)、objectClass (objectClass)、および referral (ref) 属性のみが入っていなければなりません。この制約事項を示す例は、『ldapsearch コマンド』の項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。

#### 関連タスク

138 ページの『ディレクトリー参照用のサーバーの指定』  
以下の情報を参考にして、参照サーバーを指定します。

#### 関連資料

265 ページの『ldapsearch』  
LDAP 検索コマンド行ユーティリティー

## トランザクション

Directory Server 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、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 操作は永続になりません。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くなることになります。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開始するだけで十分です。

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。

#### 関連タスク

137 ページの『トランザクション設定値の指定』  
以下の情報を参考にして、Directory Server トランザクションの設定値を構成します。

## Directory Server のセキュリティ

多彩な機能を使用して、Directory Server をセキュアにする方法を学んでください。

Directory Server のセキュリティについての詳細は以下を参照してください。

#### 関連概念

4 ページの『ディレクトリー』

Directory Server は、i5/OS 統合ファイル・システムの編成に類似した方法で情報を階層構造に保管するタイプのデータベースへのアクセスを許可します。

10 ページの『識別名 (DN)』

ディレクトリー内のすべての項目には、識別名 (DN) があります。DN は、ディレクトリー内の項目を一意的に識別する名前です。DN の最初のコンポーネントは、相対識別名 (RDN) と呼ばれています。

196 ページの『セキュリティ・プロパティー・タスク』

以下の情報を参考にして、セキュリティ・プロパティー・タスクを管理します。

#### 関連タスク

143 ページの『Directory Server のオブジェクト監査の使用可能化』

以下の情報を参考にして、Directory Server のオブジェクト監査を使用可能にします。

## 監査

監査を使用して、特定の Directory Server トランザクションの詳細をトラックすることができます。

Directory Server は、i5/OS セキュリティー監査をサポートしています。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、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、System i Navigator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。

1 監査のグループ名を指定することができます。許可を受けたクライアントは、サーバーがクライアント ID  
1 に関連付けたグループではなく、クライアントによって指定されたグループの権限が、操作の実行で使用さ  
1 れることを要求できます。このような設定により、クライアントが指定したグループのみが使用されている  
1 か、または指定したグループ・リストも組み入れられるかを、そのような要求の監査で示すかどうかを制御  
1 されます。グループ・リストの監査では、各要求ごとのグループ・リストを収めた追加の監査項目が作成さ  
1 れます。

1 グループ名を監査するかどうかを指定するには、次のようにします。

- 1 1. System i Navigatorで「ネットワーク」を展開する。
- 1 2. 「サーバー」を展開する。
- 1 3. 「TCP/IP」をクリックする。
- 1 4. 「IBM Directory Server」を右マウス・ボタン・クリックし、「プロパティー」を選択する。
- 1 5. 「監査」タブで、「Include group names when auditing use of caller-specified groups (呼び出し元指  
1 定のグループの使用の監査時にグループ名を組み入れる)」チェック・ボックスにチェックを付けます。

### 関連概念

8 ページの『配布ディレクトリー』

配布ディレクトリーとは、複数の Directory Server にまたがってデータが区画に分割されているディレ  
クトリー環境をいいます。クライアント・アプリケーションにとって、配布ディレクトリーが 1 つのデ  
ィレクトリーに見えるようにするため、すべてのサーバーとそこに収められているデータを認識してい  
る 1 つ以上のプロキシ・サーバーが用意されます。

### 関連タスク

143 ページの『Directory Server のオブジェクト監査の使用可能化』

以下の情報を参考にして、Directory Server のオブジェクト監査を使用可能にします。

### 関連情報

Security Reference



## セキュリティー監査

監査の詳細については、『セキュリティー監査』のトピックを参照してください。

## Directory Server での Secure Sockets Layer (SSL) と Transport Layer Security (TLS)

Directory Server との通信の安全度をさらに高めるために、Secure Sockets Layer (SSL) セキュリティーおよび Transport Layer Security (TLS) を Directory Server で使用することができます。

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、i5/OS のオプション 34 であるデ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おく必要があります。デジタル認証マネージャー (DCM) は、デジタル証明書および証明書ストアを作成し、管理するためのインターフェースとなるものです。

TLS は SSL の後継として設計され、同じ暗号方式を使用しますが、サポートされる暗号アルゴリズムがさらに増えました。TLS によって、サーバーはデフォルト・ポート 389 を介してクライアントからセキュアと非セキュア通信を受信できます。セキュア通信では、クライアントは StartTLS 拡張操作を使用する必要があります。

クライアントで TLS を使用する場合は、次のようにしてください。

1. TLS または SSLTL を使用するように Directory Server を構成する必要がある。
2. クライアント・コマンド行ユーティリティーに `-Y` オプションを指定する必要がある。

**注:** TLS と SSL には相互運用がありません。SSL ポート上で TLS 開始要求 (`-Y` オプション) を出すと、操作エラーの原因となります。

クライアントは TLS または SSL のいずれかを使用してセキュア・ポート (636) に接続できます。StartTLS は、既存の非セキュア接続 (例えば、ポート 389) を介してセキュア通信を開始できるようにする LDAP 機構です。標準の非セキュア・ポート (389) に使用できるのは StartTLS (またはコマンド行ユーティリティーの `-Y` オプション) のみですが、セキュア接続では StartTLS は使用できません。

### 関連タスク

203 ページの『Directory Server での SSL と Transport Layer Security の使用可能化』

以下の情報を参考にして、Directory Server で SSL と Transport Layer Security を使用可能にします。

203 ページの『Directory Server での SSL と Transport Layer Security の使用可能化』

以下の情報を参考にして、Directory Server で SSL と Transport Layer Security を使用可能にします。

280 ページの『LDAP コマンド行ユーティリティーでの SSL の使用』

以下の情報を参考にして、LDAP コマンド行ユーティリティーでの SSL の使用方法を確認します。

### 関連情報

デジタル証明書マネージャー

Secure Sockets Layer (SSL)

サポートされている SSL および Transport Layer Security (TLS) プロトコル

## Directory Server での Kerberos 認証の使用

Directory Server では、Kerberos 認証を使用することができます。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、ネットワーク認証サービスも設定しておく必要があります。

Directory Server 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、Directory Server の LDAP クライアントも、Windows 2000 の LDAP クライアントも、Directory Server 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 (ldap は小文字であることが必要)、host-name はシステムの完全修飾 TCP/IP 名、および 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。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、Directory Server 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。このオプションを選択した時は、サーバーはディレクトリーからその Kerberos ID を指定した項目を検索します。

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。

### 関連情報

ネットワーク認証サービス

Kerberos の詳細は、『ネットワーク認証サービス』のトピックを参照してください。

ネットワーク認証サービスを構成する

キー・テーブル (keytab) ファイルへの情報の追加に関する情報は、『ネットワーク認証サービスを構成する』のトピックを参照してください。

## パスワードの暗号化

- IBM Tivoli Directory Server では、ユーザー・パスワードへの無許可アクセスを防止することができます。
- 管理者は、片方向の暗号化フォーマットまたは両方向の暗号化フォーマットで、userPassword 属性値が暗号化されるようにサーバーを構成することができます。暗号化されたパスワードには、暗号化アルゴリズム名のタグが付けられるので、別々のフォーマットで暗号化された複数のパスワードがディレクトリー内に共存することができます。暗号化構成を変更しても、既存の暗号化されたパスワードは無変更のまま残り、効果を持続します。

片方向の暗号化フォーマットを使用すると、ユーザー・パスワードは暗号化されてディレクトリーに保管されるので、システム管理者を含め、あらゆるユーザーからのクリア・パスワードへのアクセスが防止されます。両方向の暗号化フォーマットを使用すると、パスワードは暗号化されてデータベースに保管され、許可クライアントへの返送時に暗号化解除されます。両方向の暗号化では、データベースに保管されたパスワードが保護される一方で、サーバーが平文のパスワードにアクセスできることが前提の DIGEST-MD5 などの認証方式の使用がサポートされるとともに、平文パスワードを必要とするアプリケーションもサポートされます。

片方向暗号化パスワードは、パスワードの突き合わせに使用できますが、暗号化解除はできません。ユーザーのログイン時に、ログイン・パスワードは暗号化されて、突き合わせ検証用として保管されているバージョンと比較されます。

特定のフォーマットの新規パスワードを保管するようにサーバーが構成されている場合でも、別の方式で事前に暗号化されたパスワードも受け入れられます。たとえば、AES256 パスワード暗号化を使用するようにサーバーが構成されていても、SHA-1 で暗号化されたパスワードを使用する別のサーバーから、管理者はデータをロードすることはできます。どちらのパスワード・セットを使用しても、単純なパスワード認証を使ってサーバーに対する認証を行うことはできますが、SHA-1 パスワードは、暗号化済みのストリングとして戻され、しかも DIGEST-MD5 認証では使用できません。

片方向暗号化のフォーマットは次のとおりです。

- SHA-1
- MD5
- crypt

サーバーの構成が完了した後、新規パスワード (新規ユーザーの) または変更されたパスワード (既存ユーザーの) はすべて、暗号化されてからディレクトリー・データベースに保管されます。その後 LDAP 検索を実行すると、タグ付きおよび暗号化済みの値が戻されます。

中間層の認証エージェントのように、クリア・パスワードを取り出す必要のあるアプリケーションの場合、ユーザー・パスワードに対する暗号化の両方向の暗号化が実行されるように、ディレクトリー管理者がサーバーを構成する必要があります。この場合、サーバーから戻されるクリア・パスワードは、ディレクトリーの ACL メカニズムによって保護されます。

両方向暗号化のフォーマットは次のとおりです。

- なし
- AES

ディレクトリー内の userPassword 属性の値を暗号化し、元の平文フォーマットで項目の一部として取り出せるようにするために、両方向の暗号化オプション AES が装備されています。これを、128、192、および 256 ビットの鍵の長さを使用するように構成することができます。中間層の認証サーバーなどの一部のアプリケーションでは、平文フォーマットでパスワードを取り出せる必要がありますが、2 次的な永続ストレージへのクリア・パスワードの保管が社内のセキュリティー・ポリシーで禁止されていることがあります。このオプションは、どちらの要件も満足します。

さらに、複製ネットワーク内で AES パスワードの暗号化を使用すれば、すべてのサーバーが同じ AES パスフレーズとソルトで構成されている場合には、パスワード・データは暗号化されたフォームのまま複製されるので、パスワード・データの保護が強化されます。サーバーが AES をサポートしていない場合や、異なる AES 情報で構成されている場合、パスワードは暗号化解除されて平文として複製されます。

注:

- | 1. AES は、V6R1 LDAP より前のサーバーではサポートされません。特に、AES で暗号化されたデータの複製は、V6R1 LDAP より前のサーバーではサポートされません。
- | 2. 他のプラットフォームでは、「なし」の選択項目を選択すると、平文のパスワードがデータベースに保管されます。そのサーバーが、他のプラットフォーム上の IBM Tivoli Directory Server を組み込んだネットワークの一員である場合、AES 暗号化オプションのいずれかを使用することをお勧めします。

| バインド要求に添付されたパスワードが、userPassword 属性の複数の値のうちのいずれかに一致すれば、単純なバインドは正常に完了します。

| Web 管理を使用してサーバーを構成する場合、以下の暗号化オプションのいずれかを選択できます。

| **なし** パスワードは、両方向暗号化されて検証リストに保管されて、項目の一部として元の平文フォーマットで取り出されます。この設定を使用するには、QRETSVRSEC システム値を 1 に設定する必要があります。

| **crypt** パスワードは、ディレクトリーに保管される前に UNIX® crypt 暗号化アルゴリズムによって暗号化されます。crypt の使用時には、パスワードの最初の 8 文字のみが使用されます。8 文字より長いパスワードは切り捨てられます。

| **MD5** パスワードは、ディレクトリーに保管される前に MD5 ハッシュ・アルゴリズムによって暗号化されます。

| **SHA-1** パスワードは、ディレクトリーに保管される前に SHA-1 暗号化アルゴリズムによって暗号化されます。

#### | **AES128**

| パスワードは、ディレクトリーに保管される前に AES128 アルゴリズムで暗号化されて、項目の一部として元のクリア・フォーマットで取り出されます。

#### | **AES192**

| パスワードは、ディレクトリーに保管される前に AES192 アルゴリズムで暗号化されて、項目の一部として元のクリア・フォーマットで取り出されます。

#### | **AES256**

| パスワードは、ディレクトリーに保管される前に AES256 アルゴリズムで暗号化されて、項目の一部として元のクリア・フォーマットで取り出されます。

| **注:** 前のリリースで使用できた imask フォーマットは、今後は暗号化のオプションではなくなります。しかし、imask で暗号化された既存の値はすべて有効です。

| Tivoli Directory Server for i5/OS のデフォルト・オプションは SHA-1 です。これは、これまでのリリースとの互換性があり、AES パスフレーズやソルトを設定する必要はありません。

| userPassword に加え、secretKey 属性の値も、常にディレクトリー内で AES256 で暗号化されます。この暗号化は、userPassword とは違って、secretKey の値に対して強制されます。他のオプションは配備されていません。secretKey 属性は、IBM 定義のスキーマです。アプリケーションは、常に暗号化されている必要がある機密データをディレクトリー内に保管する場合や、ディレクトリー・アクセス制御を使って、データを平文フォーマットで取り出す場合、この属性を使用することができます。

| コマンド行を使用して、たとえば、**crypt** に変更する場合のように、暗号化のタイプを変更する場合は、以下のコマンドを発行します。

```
| ldapmodify -D <adminDN> -w <adminPW> -i <filename>
```

| ただし、<filename> には以下が入っています。

```
| dn: cn=configuration
| changetype: modify
| replace: ibm-slapdPWEncryption
| ibm-slapdPWEncryption: crypt
```

| 更新後の設定が動的に効果を生じるようにするには、次の `Idapexop` コマンドを発行します。

```
| ldapexop -D <adminDN> -w <adminPW> -op readconfig -scope single
| "cn=configuration" ibm-slapdPWEncryption
```

| 注: 構成を変更するには、\*ALLOBJ および \*IOSYSCFG 特殊権限を持った i5/OS ユーザー・プロファイ  
| ル用のプロジェクト・ユーザー DN およびパスワードを使って、認証を受ける必要があります。これ  
| は、他のインターフェースを通してサーバー構成を変更するときに必要な権限と同じ権限です。

#### | 関連タスク

| 197 ページの『パスワード・ポリシー・プロパティの設定』  
| 以下の情報を参考にして、パスワード・ポリシー・プロパティを設定します。

## グループと役割

メンバーのアクセスまたは許可を編成して制御するには、グループおよび役割を使用します。

グループは、リスト、つまり名前の集合です。グループは、アクセスを制御するために **aclentry**、**ibm-filterAclEntry**、および **entryowner** の各属性で使用したり、メーリング・リストなどのアプリケーション固有の用途で使用したりすることができます。グループは、静的、動的、またはネストとして定義できます。

役割とグループは、ディレクトリー内でオブジェクトにより表現されるという点では似ています。役割には、さらに DN のグループも含まれています。

詳細は、以下を参照してください。

#### 関連概念

72 ページの『アクセス制御リスト』

アクセス制御リスト (ACL) を使用すると、LDAP ディレクトリーに保管された情報を保護することができます。管理者は ACL を使用して、ディレクトリーのさまざまな部分へのアクセスや、特定のディレクトリー項目へのアクセスを制限します。

227 ページの『ユーザーとグループのタスク』

以下の情報を参考にして、ユーザーとグループを管理します。

#### 関連タスク

229 ページの『グループの追加』

以下の情報を参考にして、グループを追加します。

234 ページの『グループの作成』

以下の情報を参考にして、グループを作成します。

#### 静的グループ:

静的グループは、メンバーを 1 つずつリストすることで、メンバーを定義します。

静的グループは、構造化 objectclass **groupOfNames**、**groupOfUniqueNames**、**accessGroup**、または **accessRole**、あるいは、補助 objectclass **ibm-staticgroup** を使用して、各メンバーを個別に定義します。**groupOfNames** または **groupOfUniqueNames** 構造化 objectclass を使用する静的グループは、メンバーを少なくとも 1 つ持つ必要があります。**accessGroup** または **accessRole** 構造化 objectclass を使用するグル

ープは空にすることもできます。補助 objectclass **ibm-staticGroup** を使用して静的グループを定義することもできます。この場合、**member** 属性は必要ではないため、空にすることもできます。

一般的なグループ項目を以下に示します。

```
DN: cn=Dev.Staff,ou=Austin,c=US
objectclass: accessGroup
cn: Dev.Staff
member: cn=John Doe,o=IBM,c=US
member: cn=Jane Smith,o=IBM,c=US
member: cn=James Smith,o=IBM,c=US
```

各グループ・オブジェクトには、メンバー DN で構成される複数値の属性が含まれます。

アクセス・グループを削除すると、そのアクセス・グループは、それが適用されているすべての ACL から削除されます。

### 動的グループ:

動的グループは、LDAP 検索を使用してメンバーを定義します。

動的グループは、構造化 objectclass **groupOfURLs** (または補助 objectclass **ibm-dynamicGroup**) と属性 **memberURL** を使用して、簡略 LDAP URL 構文を使った検索を定義します。

```
ldap:///<base DN of search> ?? <scope of search> ? <searchfilter>
```

注: 上記例に示すように、構文にホスト名は指定しないでください。その他のパラメーターは、LDAP の通常の URL 構文と同じように指定します。パラメーターを指定しない場合でも、各パラメーター・フィールドを ? で区切る必要があります。一般に、戻される属性のリストは、基本 DN と検索範囲の間に含まれています。また、このパラメーターは動的メンバーシップの判別時にもサーバーで使用されないため、省略できますが、区切り文字 ? が存在しなければなりません。

ここで、

#### base DN of search

ディレクトリー内の検索の開始点です。接尾部やディレクトリーのルート (**ou=Austin** など) を指定できます。このパラメーターは必須です。

#### scope of search

検索の範囲を指定します。デフォルトの有効範囲は **base** です。

**base** URL に指定された基本 DN についての情報のみを返します。

**one** URL に指定された基本 DN の 1 レベル下の項目について情報を返します。これには、基本項目は含まれません。

**sub** 基本 DN とその下にあるすべてのレベルの項目について情報を返します。

#### searchfilter

検索の有効範囲にある項目に適用するフィルターです。searchfilter (検索フィルター) の構文については、ldapsearch フィルター・オプションを参照してください。デフォルトは objectclass=\* です。

動的メンバーの検索は常にサーバー内部で行われます。そのため、完全な ldap URL を指定する場合とは異なり、ホスト名とポート番号は指定されません。また、プロトコルは常に **ldap** が使用されます (**ldaps** ではありません)。**memberURL** 属性には各種の URL が含まれますが、サーバーは、**ldap:///** で始まる **memberURL** のみを使用して、動的メンバーを判別します。

## 例

スコープが base にデフォルト設定され、フィルターが objectclass=\* にデフォルト設定される単一項目の場合:

```
ldap:///cn=John Doe, cn=Employees, o=Acme, c=US
```

cn=Employees の 1 レベル下にあり、フィルターが objectclass=\* にデフォルト設定されるすべての項目の場合:

```
ldap:///cn=Employees, o=Acme, c=US??one
```

o=Acme の下にあり、objectclass=person が指定されているすべての項目の場合:

```
ldap:///o=Acme, c=US??sub?objectclass=person
```

ユーザー項目の定義に使用するオブジェクト・クラスにもよりますが、これらの項目には、グループ・メンバーシップの判別に適した属性が含まれない場合があります。補助オブジェクト・クラス

**ibm-dynamicMember** を使用すると、ユーザー項目を拡張して **ibm-group** 属性を含めることができます。この属性を使用すると、動的グループのフィルターのターゲットとして機能するユーザー項目に任意の値を追加できます。たとえば次のようになります。

以下の動的グループのメンバーは cn=users,ou=Austin 項目の直下にある項目で、GROUP1 という ibm-group 属性を持っています。

```
dn: cn=GROUP1,ou=Austin
 objectclass: groupOfURLs
 cn: GROUP1
 memberURL: ldap:///cn=users,ou=Austin??one?(ibm-group=GROUP1)
```

次に cn=GROUP1,ou=Austin のメンバーの例を示します。

```
dn: cn=Group 1 member, cn=users, ou=austin
 objectclass: person
 objectclass: ibm-dynamicMember
 sn: member
 userpassword: memberpassword
 ibm-group: GROUP1
```

## ネストされたグループ:

グループをネストすると、階層関係を作成できます。階層関係を使用すると、継承されたグループ・メンバーシップを定義できます。

ネストされたグループは、子グループ項目として定義されます。この子グループ項目は、親グループ項目内に含まれる属性によって参照される DN を持ちます。親グループは、構造化グループ・オブジェクト・クラス (**groupOfNames**、**groupOfUniqueNames**、**accessGroup**、**accessRole**、または **groupOfURLs**) の 1 つを拡張し、**ibm-nestedGroup** 補助オブジェクト・クラスを追加することで作成されます。ネストされたグループを拡張すると、ゼロ個以上の **ibm-memberGroup** 属性を追加できます。その属性の値には、ネストされた子グループの DN を設定できます。たとえば次のようになります。

```
dn: cn=Group 2, cn=Groups, o=IBM, c=US
 objectclass: groupOfNames
 objectclass: ibm-nestedGroup
 objectclass: top
 cn: Group 2
 description: Group composed of static, and nested members.
 member: cn=Person 2.1, cn=Dept 2, cn=Employees, o=IBM, c=US
 member: cn=Person 2.2, cn=Dept 2, cn=Employees, o=IBM, c=US
 ibm-memberGroup: cn=Group 8, cn=Nested Static, cn=Groups, o=IBM, c=US
```

ネストされたグループ階層に循環を導入することは許されていません。ネストされたグループ操作によって循環参照が直接的にまたは継承を介して発生したことが確認された場合、それは制約違反と見なされるため、項目の更新に失敗します。

### ハイブリッド・グループ:

ハイブリッド・グループ・メンバーシップは、静的、動的、およびネストされたメンバー・タイプを組み合わせて記述されます。

たとえば次のようになります。

```
dn: cn=Group 10, cn=Groups, o=IBM, c=US
 objectclass: groupOfURLs
 objectclass: ibm-nestedGroup
 objectclass: ibm-staticGroup
 objectclass: top
 cn: Group 10
 description: Group composed of static, dynamic, and nested members.
 memberURL: ldap:///cn=Austin, cn=Employees, o=IBM, c=US??one?objectClass=person
 ibm-memberGroup: cn=Group 9, cn=Nested Dynamic, cn=Groups, o=IBM, c=US
 member: cn=Person 10.1, cn=Dept 2, cn=Employees, o=IBM, c=US
 member: cn=Person 10.2, cn=Dept 2, cn=Employees, o=IBM, c=US
```

### グループ・メンバーシップの判別:

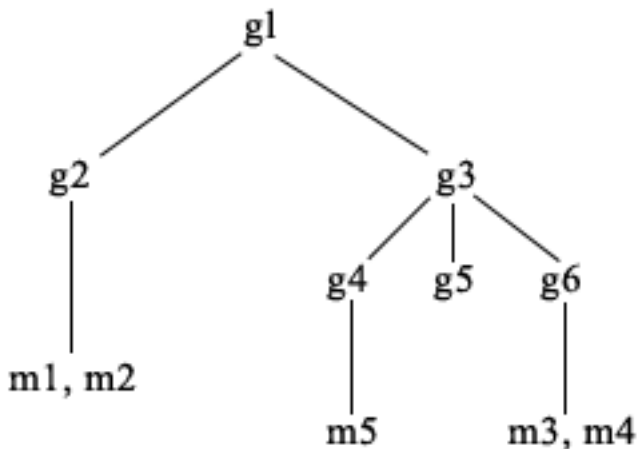
2 つの操作属性が、集合グループ・メンバーシップの照会に使用できます。

**ibm-allMembers** 操作属性は、特定のグループ項目について、グループ・メンバーシップのセットの集合を列挙します (これには、ネストされたグループ階層によって記述された、静的メンバー、動的メンバー、およびネストされたメンバーが含まれます)。**ibm-allGroups** 操作属性は、特定のユーザー項目について、グループのセットの集合を列挙します (これには、そのユーザーがメンバーシップを持つ上位グループが含まれます)。

要求者は、データに対する ACL の設定に応じて、要求したすべてのデータのサブセットしか受け取れないことがあります。**ibm-allMembers** および **ibm-allGroups** 操作属性はいずれのユーザーでも要求できますが、戻されるデータ・セットには、その要求者がアクセス権を持っている LDAP 項目と属性のデータしか含まれません。**ibm-allMembers** 属性または **ibm-allGroups** 属性を要求するユーザーの場合、静的メンバーを参照するには、そのグループおよびネストしたグループの **member** 属性値または **uniquemember** 属性値へのアクセス権を持っている必要があります。また、動的メンバーを参照するには、**memberURL** 属性値に指定されている検索を実行する権限を持っている必要があります。



## 階層の例



この例の場合、**m1** および **m2** は、**g2** のメンバー属性です。**g2** の ACL により、**user1** はメンバー属性を読み取ることができますが、**user2** はメンバー属性へのアクセス権を持っていません。**g2** 項目の項目 LDIF を以下に示します。

```
dn: cn=g2,cn=groups,o=ibm,c=us
objectclass: accessGroup
cn: g2
member: cn=m1,cn=users,o=ibm,c=us
member: cn=m2,cn=users,o=ibm,c=us
aclentry: access-id:cn=user1,cn=users,o=ibm,c=us:normal:rsc
aclentry: access-id:cn=user2,cn=users,o=ibm,c=us:normal:rsc:at.member:deny:rsc
```

**g4** 項目ではデフォルトの `aclentry` が使用されますが、これにより、**user1** と **user2** の両方は、**g4** のメンバー属性を読み取ることができます。**g4** 項目の LDIF を以下に示します。

```
dn: cn=g4, cn=groups,o=ibm,c=us
objectclass: accessGroup
cn: g4
member: cn=m5, cn=users,o=ibm,c=us
```

**g5** 項目は動的グループであり、2 つのメンバーを `memberURL` 属性から取得します。**g5** 項目の LDIF を以下に示します。

```
dn: cn=g5, cn=groups,o=ibm,c=us
objectclass: container
objectclass: ibm-dynamicGroup
cn: g5
memberURL: ldap:///cn=users,o=ibm,c=us??sub?(|(cn=m3)(cn=m4))
```

項目 **m3** および **m4** は、`memberURL` が一致するので、グループ **g5** のメンバーです。**m3** 項目の ACL により、**user1** および **user2** はどちらも、**g5** を検索することができます。**m4** 項目の ACL は、**user2** に対してこの項目の検索を許可していません。**m4** 項目の LDIF を以下に示します。

```
dn: cn=m4, cn=users,o=ibm,c=us
objectclass: person
cn: m4
sn: four
aclentry: access-id:cn=user1,cn=users,o=ibm,c=us:normal:rsc
aclentry: access-id:cn=user2,cn=users,o=ibm,c=us
```

**例 1:** ユーザー 1 が、グループ **g1** のすべてのメンバーを取得するために、検索を実行します。ユーザー 1 はすべてのメンバーに対するアクセス権を持っているので、すべてのメンバーが戻ります。

```
ldapsearch -D cn=user1,cn=users,o=ibm,c=us -w user1pwd -s base -b cn=g1,
cn=groups,o=ibm,c=us objectclass=* ibm-allmembers
```

```
cn=g1,cn=groups,o=ibm,c=us
ibm-allmembers: CN=M1,CN=USERS,O=IBM,C=US
ibm-allmembers: CN=M2,CN=USERS,O=IBM,C=US
ibm-allmembers: CN=M3,CN=USERS,O=IBM,C=US
ibm-allmembers: CN=M4,CN=USERS,O=IBM,C=US
ibm-allmembers: CN=M5,CN=USERS,O=IBM,C=US
```

**例 2:** ユーザー 2 が、グループ **g1** のすべてのメンバーを取得するために、検索を実行します。ユーザー 2 はグループ **g2** メンバー属性に対するアクセス権を持っていないので、メンバー **m1** または **m2** にアクセスできません。ユーザー 2 は **g4** のメンバー属性に対するアクセス権を持っているので、メンバー **m5** にアクセスすることができます。ユーザー 2 は、グループ **g5** の memberURL で項目 **m3** に対する検索を実行し、メンバーをリストすることができますが、**m4** に対する検索を実行することはできません。

```
ldapsearch -D cn=user2,cn=users,o=ibm,c=us -w user2pwd -s base -b cn=g1,
cn=groups,o=ibm,c=us objectclass=* ibm-allmembers
```

```
cn=g1,cn=groups,o=ibm,c=us
ibm-allmembers: CN=M3,CN=USERS,O=IBM,C=US
ibm-allmembers: CN=M5,CN=USERS,O=IBM,C=US
```

**例 3:** ユーザー 2 が、**m3** がグループ **g1** のメンバーであるかどうかを確認するために、検索を実行します。ユーザー 2 はこの検索に対するアクセス権を持っているので、検索では、**m3** がグループ **g1** のメンバーであることが示されます。

```
ldapsearch -D cn=user2,cn=users,o=ibm,c=us -w user2pwd -s base -b cn=m3,
cn=users,o=ibm,c=us objectclass=* ibm-allgroups
```

```
cn=m3,cn=users,o=ibm,c=us
ibm-allgroups: CN=G1,CN=GROUPS,O=IBM,C=US
```

**例 4:** ユーザー 2 が、**m1** がグループ **g1** のメンバーであるかどうかを確認するために、検索を実行します。ユーザー 2 はこのメンバー属性に対するアクセス権を持っていないので、検索では、**m1** がグループ **g1** のメンバーであることが示されません。

```
ldapsearch -D cn=user2,cn=users,o=ibm,c=us -w user2pwd -s base -b
cn=m1,cn=users,o=ibm,c=us objectclass=* ibm-allgroups
```

```
cn=m1,cn=users,o=ibm,c=us
```

ネストされたグループおよび動的グループ用のグループ・オブジェクト・クラス:

ネストされたグループおよび動的グループ用のグループ・オブジェクト・クラスのリスト。

#### **ibm-dynamicGroup**

この補助クラスでは、オプション属性の **memberURL** を使用できます。静的メンバーと動的メンバーの両方を持つハイブリッド・グループを作成するには、これを **groupOfNames** などの構造化クラスとともに使用します。

#### **ibm-dynamicMember**

この補助クラスでは、オプション属性の **ibm-group** を使用できます。これは、動的グループ用のフィルター属性として使用します。

### ibm-nestedGroup

この補助クラスでは、オプション属性の **ibm-memberGroup** を使用できます。親グループ内でサブグループをネストできるようにするには、これを **groupOfNames** などの構造化クラスとともに使用します。

### ibm-staticGroup

この補助クラスでは、オプション属性の **member** を使用できます。静的メンバーと動的メンバーの両方を持つハイブリッド・グループを作成するには、これを **groupOfURLs** などの構造化クラスとともに使用します。

注: **ibm-staticGroup** は、**member** がオプションである唯一のクラスです。 **member** を使用するそれ以外のすべてのクラスでは、最低 1 つのメンバーが必要です。

### グループ属性タイプ:

グループ属性タイプのリスト。

### ibm-allGroups

項目が属しているグループをすべて表示します。項目は、**member**、**uniqueMember**、または **memberURL** 属性によって直接メンバーにすることができます。あるいは、**ibm-memberGroup** 属性によって間接的にメンバーにすることができます。検索フィルターでは、この **Read-only** 操作属性を使用することはできません。 **ibm-allGroups** 属性は、比較要求において、項目が特定のグループのメンバーであるかを判別するために使用できます。たとえば、「cn=john smith,cn=users,o=my company」がグループ「cn=system administrators,o=my company」のメンバーであるかを判別するには、以下のようにします。

```
rc = ldap_compare_s(ld, "cn=john smith,cn=users,o=my company, "ibm-allgroups",
 "cn=system administrators,o=my company");
```

### ibm-allMembers

グループのメンバーをすべて表示します。項目は、**member**、**uniqueMember**、または **memberURL** 属性によって直接メンバーにすることができます。あるいは、**ibm-memberGroup** 属性によって間接的にメンバーにすることができます。検索フィルターでは、この **Read-only** 操作属性を使用することはできません。 **ibm-allMembers** 属性は、比較要求において、DN が特定のグループのメンバーであるかを判別するために使用できます。たとえば、「cn=john smith,cn=users,o=my company」がグループ「cn=system administrators,o=my company」のメンバーであるかを判別するには、以下のようにします。

```
rc = ldap_compare_s(ld, "cn=system administrators,o=my company, "ibm-allmembers",
 "cn=john smith,cn=users,o=my company");
```

### ibm-group

補助クラス **ibm-dynamicMember** で使用される属性です。動的グループ内にある項目のメンバーシップを制御する任意の値を定義するには、この属性を使用します。たとえば、フィルター「ibm-group=Bowling Team」を持つ任意の **memberURL** に項目を含めるには、値「Bowling Team」を追加します。

### ibm-memberGroup

補助クラス **ibm-nestedGroup** で使用される属性です。親グループ項目のサブグループを識別します。このようなサブグループすべてのメンバーは、ACL、または操作属性の **ibm-allMembers** および **ibm-allGroups** を処理する際に、親グループのメンバーと見なされます。サブグループ項目それ自体は、メンバーではありません。ネストされたメンバーシップは再帰的です。

## member

グループの各メンバーの識別名を示します。たとえば、`member: cn=John Smith, dc=ibm, dc=com` となります。

## memberURL

グループの各メンバーと関連した URL を示します。ラベルが付いた任意のタイプの URL を使用できます。たとえば、`memberURL: ldap:///cn=jsmith,dc=ibm,dc=com` となります。

## uniquemember

項目に関連した名前が固有となるようにそれぞれの名前に `uniqueIdentifier` が指定されている場合に、その名前のグループを示します。 `uniqueMember` 属性の値は、DN の後に `uniqueIdentifier` を指定します。たとえば、`uniqueMember: cn=John Smith, dc=ibm, dc=com 17` となります。

## 役割:

役割ベースの許可は、グループ・ベースの許可を概念的に補足するものです。

役割のメンバーであるユーザーは、ジョブを完了するために役割で必要とされる作業を実行する権限があります。グループとは異なり、役割では、暗黙的な許可のセットが提供されます。グループのメンバーになることにより得られる (または失われる) 許可について内在する想定事項はありません。

役割とグループは、ディレクトリー内でオブジェクトにより表現されるという点では似ています。役割には、さらに DN のグループも含まれています。アクセス制御で使用される役割は、`objectclass` 「AccessRole」を持っている必要があります。「Accessrole」 `objectclass` は、「GroupOfNames」 `objectclass` のサブクラスです。

たとえば、「sys admin」などの DN のコレクションがある場合は、最初にそれが「sys admin group」であると考えられるかもしれませんが (グループとユーザーには、最もなじみのある特権属性タイプであるため)。しかし、「sys admin」のメンバーとして受け取ることになっている許可のセットがあるため、DN のコレクションは、「sys admin role」として、より正確に定義することができます。

## 管理アクセス

管理アクセスを使用して、個々の管理用タスクへのアクセスを制御します。

IBM Directory Server では、以下のタイプの管理アクセスが可能です。

- **プロジェクト i5/OS 管理者:** \*ALLOBJ および \*IOSYSCFG 特殊権限によってプロジェクト・ユーザーとして認証されたクライアント (オペレーティング・システム・ユーザー・プロファイルを表す LDAP 項目) は、LDAP インターフェース (cn=configuration サブツリー、または Web 管理ツール「サーバー管理」タスク) を使用してディレクトリー構成を変更する権限と、他のディレクトリー項目 (DB2 接尾部またはスキーマの 1 つに保管された項目) に対して LDAP 管理者として振る舞う権限を持ちます。サーバー構成を変更できるのは、プロジェクト i5/OS 管理者のみです。
- **LDAP 管理者:** Directory Server では、1 つのユーザー ID (DN) を基本 LDAP サーバー管理者にすることができます。また、Directory Server では、プロジェクト・オペレーティング・システム・ユーザー・プロファイルを LDAP 管理者にすることもできます。LDAP サーバー管理者は複製、スキーマ、およびディレクトリー項目の管理など、長いリストの管理用タスクを実行できます。
- **管理ユーザーのグループ:** プロジェクト i5/OS 管理者は、複数のユーザーを管理グループに指名することができます。このグループのメンバーは LDAP サーバー管理者として同じ管理アクセス権限をもつので、多くのタスクを実行することができます。

注: Web 管理の使用時は、管理グループ・メンバーに許可されていないタスクは使用不可となります。

LDAP 管理者または管理グループ・メンバーは、以下のサーバー管理タスクを実行することができます。

- 自身のパスワードの変更。
- 接続の終了。
- パスワード・ポリシーの使用可能化および変更。この場合、プロジェクト i5/OS 管理者のみが変更できるパスワード暗号化については除外されます。
- 固有属性の管理。
- サーバー・スキーマの管理。
- 複製の管理。この場合、プロジェクト i5/OS 管理者のみが実行できる、複製プロパティ・タスク (マスター・サーバー・バインド DN とパスワードおよびデフォルト参照を含む) は除外されます。

#### 関連概念

150 ページの『管理グループのタスク』

以下の情報を参考にして、管理グループを管理します。

100 ページの『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。

#### 関連タスク

140 ページの『プロジェクト・ユーザーへの管理者アクセスの許可』

以下の情報を参考にして、ユーザー・プロファイルに管理者権限を認可します。

## プロキシー許可

プロキシー許可は特殊な形式の認証です。このプロキシー許可メカニズムを使用することによって、クライアント・アプリケーションはディレクトリーに対して自身の識別をバインドできますが、ターゲット・ディレクトリーへのアクセスでは、他のユーザーの代理として操作の実行が許可されます。トラステッド・アプリケーションまたはユーザーの 1 組が、複数のユーザーの代理として Directory Server にアクセスすることができます。

プロキシー許可グループのメンバーは認証された ID とみなすことができますが、管理者または管理グループのメンバーは除外されます。

プロキシー許可グループは localhost または IBMpolicies のいずれかに保管することができます。

IBMpolicies にあるプロキシー許可グループは複製されますが、localhost にあるプロキシー許可グループは複製されません。プロキシー許可グループは localhost と IBMpolicies の両方に保管できます。プロキシー・グループがこれらの DN の 1 つに保管されていない場合、サーバーはそのグループのプロキシー部分を無視して、正常グループとして取り扱います。

この例として、クライアント・アプリケーション client1 は上位のアクセス権で Directory Server にバインドできます。制限されたアクセス権をもつ UserA はクライアント・アプリケーションに要求を送信します。クライアントがプロキシー許可グループのメンバーである場合は、client1 として Directory Server に要求を送信するのではなく、さらに制限されたレベルのアクセス権を使用して UserA として要求を渡すことができます。このことは、client1 として要求を実行するのではなく、アプリケーション・サーバーはその情報のみにアクセスするか、あるいは UserA がアクセスまたは実行できるアクションのみしか実行できないことを意味します。すなわち、UserA の代理として、あるいはそのプロキシーとして要求を実行します。

注: 属性メンバーは DN の形式でその値をもっていなければなりません。そうでない場合、無効 DN 構文メッセージが戻されます。グループの DN は、プロキシー許可グループのメンバーにはなれません。

管理者および管理グループ・メンバーはプロキシー許可グループのメンバーにはなりません。監査ログは、プロキシー許可を使用して実行された各アクションについてバインド DN とプロキシー DN の両方を記録します。

### 関連概念

155 ページの『プロキシー許可グループのタスク』

以下の情報を参考にして、プロキシー許可グループを管理します。

## アクセス制御リスト

アクセス制御リスト (ACL) を使用すると、LDAP ディレクトリーに保管された情報を保護することができます。管理者は ACL を使用して、ディレクトリーのさまざまな部分へのアクセスや、特定のディレクトリー項目へのアクセスを制限します。

ディレクトリー内の各項目および属性の変更は、ACL を使用して制御できます。特定の項目または属性の ACL は、その親項目から継承するか、明示的に定義することができます。

オブジェクトおよび属性のアクセス権を設定する時に、使用するユーザーのグループを作成することにより、アクセス制御計画を設計するのが最善です。ツリーのできるだけ高い位置に所有権およびアクセス権を設定し、制御がツリーの下に継承されるようにします。

entryOwner、ownerSource、ownerPropagate、aclEntry、aclSource、および aclPropagate のような、アクセス制御と関連した操作属性は、論理的に各オブジェクトと関連しているものの、ツリー内でより上の他のオブジェクトに依存する値を持つことができるという点において通常とは異なります。それら操作属性が設定された方法に応じて、それらの属性値はオブジェクトに明示されたり、上位から継承されたりします。

アクセス制御モデルでは、アクセス制御情報 (ACI) と entryOwner 情報という 2 つの属性のセットを定義します。ACI は、指定したサブジェクトが適用されるオブジェクトに対して実行される操作に関連して、そのサブジェクトに設定されるアクセス権限を定義します。aclEntry および aclPropagate 属性が ACI 定義に適用されます。entryOwner 情報は、どのサブジェクトが、関連した項目オブジェクトの ACI を定義できるのかを制御します。entryOwner および ownerPropagate 属性は、entryOwner 定義に適用されます。

2 種類のアクセス制御リスト (フィルター・ベースの ACL と非フィルター・ベースの ACL) から選択することができます。フィルターに掛けられない ACL は、それらを含むディレクトリー項目に明示的に適用されますが、その派生項目にまったく伝搬させないこともできますし、そのすべてに伝搬させることもできます。フィルター・ベースの ACL は、ターゲット・オブジェクトをそれらに適用される有効なアクセスと突き合わせるために、指定されたオブジェクト・フィルターを使用して、フィルター・ベースの比較を行うという点で異なります。

ACL を使用すると、管理者は、ディレクトリーのさまざまな部分や特定のディレクトリー項目に対するアクセスを制限できます。さらに、属性名または属性アクセス・クラスを基にして項目に含まれる属性に対するアクセスも制限できます。LDAP ディレクトリー内の各項目には、関連した ACI のセットがあります。LDAP モデルに従い、ACI および entryOwner 情報は、属性と値の対で表されます。さらに、LDIF 構文を使用すると、これらの値を管理できます。これらの属性を以下に示します。

- aclEntry
- aclPropagate
- ibm-filterAclEntry
- ibm-filterAclInherit
- entryOwner
- ownerPropagate

追加情報については、以下を参照してください。

#### 関連概念

63 ページの『グループと役割』

メンバーのアクセスまたは許可を編成して制御するには、グループおよび役割を使用します。

239 ページの『アクセス制御リスト (ACL) のタスク』

以下の情報を参考にして、アクセス制御リスト (ACL) を管理します。

102 ページの『操作属性』

Directory Server に対して特殊な意味を持つ、操作属性という幾つかの属性があります。これらは、サーバーによって保守される属性であり、サーバーがある 1 つの項目について管理している情報を反映するか、またはサーバーの動作に影響を及ぼします。

222 ページの『アクセス制御リストの編集』

以下の情報を参考にして、アクセス制御リスト (ACL) を管理します。

236 ページの『レルム上の ACL の編集』

以下の情報を参考にして、レルム上の ACL を編集します。

#### 関連タスク

239 ページの『テンプレート上の ACL の編集』

以下の情報を参考にして、テンプレート上の ACL を編集します。

#### フィルター済みのアクセス制御リスト:

フィルター・ベースの ACL (アクセス制御リスト) は、指定されたオブジェクト・フィルターを使用してフィルター・ベースの比較を行い、ターゲット・オブジェクトと、そのターゲット・オブジェクトに適用される有効なアクセスとを突き合わせます。

フィルター・ベースの ACL は、本質的に、関連するサブツリー内の比較で一致したオブジェクトすべてに伝搬します。このため、フィルターに掛けられていない ACL の伝搬を停止するために使用される `aclPropagate` 属性は、新しいフィルター・ベースの ACL には適用されません。

フィルター・ベースの ACL のデフォルト動作では、最下位の収容項目から、祖先項目チェーンを上に向かって、DIT の最上位の収容項目まで累算します。有効なアクセス権は、構成要素になっている祖先の項目により認可または拒否されたアクセス権限の和集合として計算されます。この動作には、例外があります。サブツリーの複製機能との互換性のため、また管理の柔軟性を高めるために、累積を停止する手段として上限属性を使用できます。つまり、その上限属性の含まれている項目で累積を停止できるようになっています。

特にフィルター・ベースの ACL のサポートにおいては、フィルター・ベースの特性を既存の非フィルター・ベースの ACL にマージするのではなく、アクセス制御属性の新しいセットが使用されます。これらの属性を以下に示します。

- `ibm-filterAclEntry`
- `ibm-filterAclInherit`

`ibm-filterAclEntry` 属性は、オブジェクト・フィルター・コンポーネントを追加することにより、`aclEntry` と同じ形式になります。関連する上限属性は、`ibm-filterAclInherit` です。これはデフォルトでは `true` に設定されています。 `false` に設定すると、累算を終了します。

#### 関連概念

78 ページの『伝搬』

項目で `aclEntry` または `entryOwner` が明示的に定義されていないと、これは上位項目から継承されるか、またはツリーを下方方向にたどって伝搬されます。

### アクセス制御属性の構文:

アクセス制御リスト (ACL) 属性を管理するには、LDAP データ交換フォーマット (LDIF) 表記を使用します。新しいフィルター・ベース ACL 属性の構文は、現在の非フィルター・ベース ACL 属性の変更バージョンです。

バックス正規形式 (BNF) を使用したアクセス制御情報 (ACI) 属性および `entryOwner` 属性の構文の定義を以下に示します。

```
<aclEntry> ::= <subject> [":" <rights>]
<aclPropagate> ::= "true" | "false"
<ibm-filterAclEntry> ::= <subject> ":" <object filter> [":" <rights>]
<ibm-filterAclInherit> ::= "true" | "false"
<entryOwner> ::= <subject>
<ownerPropagate> ::= "true" | "false"
<subject> ::= <subjectDnType> ':' <subjectDn> |
 <pseudoDn>
<subjectDnType> ::= "role" | "group" | "access-id"
<subjectDn> ::= <DN>
<DN> ::= distinguished name as described in RFC 2251, section 4.1.3.
<pseudoDn> ::= "group:cn=anybody" | "group:cn=authenticated" |
 "access-id:cn=this"
<object filter> ::= string search filter as defined in RFC 2254, section 4
 (extensible matching is not supported).
<rights> ::= <accessList> [":" <rights>]
<accessList> ::= <objectAccess> | <attributeAccess> |
 <attributeClassAccess>
<objectAccess> ::= "object:" [<action> ":"] <objectPermissions>
<action> ::= "grant" | "deny"
<objectPermissions> ::= <objectPermission> [<objectPermissions>]
<objectPermission> ::= "a" | "d" | ""
<attributeAccess> ::= "at." <attributeName> ":" [<action> ":"]
 <attributePermissions>
<attributeName> ::= attributeType name as described in RFC 2251, section 4.1.4.
 (OID or alpha-numeric string with leading
 alphabet, "-" and ";" allowed)
<attributePermissions> ::= <attributePermission>
 [<attributePermissions>]
<attributePermission> ::= "r" | "w" | "s" | "c" | ""
<attributeClassAccess> ::= <class> ":" [<action> ":"]
```



<attributePermissions>

<class> ::= "normal" | "sensitive" | "critical" | "system" | "restricted"

## サブジェクト

サブジェクト (オブジェクトを操作するためのアクセスを要求しているエンティティ) は、DN (識別名) タイプと DN の組み合わせで構成されます。有効な DN タイプは、アクセス ID (access-id)、グループ (group)、および役割 (role) です。

DN は、特定のアクセス ID、役割、またはグループを識別します。たとえば、サブジェクトは access-id: cn=personA, o=IBM または group: cn=deptXYZ, o=IBM のようになります。

フィールドの区切り文字はコロン (:) です。したがって、DN でコロンが使用されている場合は、二重引用符 ( "" ) で囲む必要があります。DN に二重引用符を使用した文字がすでに入っている場合は、円記号 ( ¥ ) を使用して、該当する文字をエスケープする必要があります。

ディレクトリー・グループはすべて、アクセス制御で使用できます。

**注:** **AccessGroup**、**GroupOfNames**、**GroupofUniqueNames**、または **groupOfURLs** の各構造化 objectclass、または **ibm-dynamicGroup**、**ibm-staticGroup** の補助 objectclass はアクセス制御に使用できます。

アクセス制御モデル内で使用されるもう 1 つの DN タイプは、役割です。役割とグループは、インプリメンテーション上はよく似ていますが、概念的には異なります。ユーザーに役割を割り当てるときは、その役割に関連するジョブの実行に必要な権限が設定済みであるという暗黙の了解があります。グループ・メンバーシップでは、そのグループのメンバーになることで得られる (または否認される) 許可についての前提条件は組み込まれていません。

役割とグループは、ディレクトリー内でオブジェクトにより表現されるという点では似ています。役割には、さらに DN のグループも含まれています。アクセス制御で使用する役割は、**AccessRole** の objectclass を持っている必要があります。

## 疑似 DN

LDAP ディレクトリーには、幾つかの疑似 DN が含まれています。これらの疑似 DN は、実行中の操作または操作が実行されているターゲット・オブジェクトとの関係において、バインド時に共通の特性を共有する多数の DN を参照するために使用されます。

現在、以下の 3 つの疑似 DN がサポートされます。

### **group:cn=anybody**

認証されていないサブジェクトも含めて、すべてのサブジェクトを参照します。すべてのユーザーは、自動的にこのグループに属します。

### **group:cn=authenticated**

ディレクトリーによって認証された DN を参照します。認証の方式は問われません。

### **access-id:cn=this**

操作が実行されるターゲット・オブジェクトの DN と一致するバインド DN を参照します。

## オブジェクト・フィルター

このパラメーターは、フィルターに掛けられた ACL のみに適用されます。RFC 2254 で定義されているストリング検索フィルターは、オブジェクト・フィルター形式として使用されます。ターゲット・オブジェクトは既知であるため、ストリングは実際の検索の実行には使用されません。代わりに、問題となっているターゲット・オブジェクト上のフィルター・ベースの比較が実行され、`ibm-filterAclEntry` 値の特定のセットがそれに適用されるかを判別します。

## 権限

アクセス権限は、オブジェクト全体またはオブジェクトの属性に適用することができます。LDAP のアクセス権限はそれぞれ独立しています。1 つの権限が別の権限を暗黙指定することはありません。権限を一緒に結合すると、必要な権限のリストを提供できます。これは、後で説明する規則のセットに従っています。権限には値を指定しないこともできます。権限に値を指定しない場合、ターゲット・オブジェクト上のサブジェクトにはアクセス権が付与されません。権限は、以下の 3 つの部分から構成されます。

### Action:

定義される値は **grant** または **deny** です。このフィールドがない場合、デフォルトは **grant** に設定されます。

### Permission:

ディレクトリー・オブジェクト上で実行できる基本操作は 6 つです。これらの操作から、ACI 許可の基本セットが処理されます。基本操作には、項目の追加、項目の削除、属性値の読み取り、属性値の書き込み、属性の検索、および属性値の比較があります。

可能な属性の許可には、読み取り (r)、書き込み (w)、検索 (s)、および比較 (c) があります。また、オブジェクトの許可は、項目全体に適用されます。オブジェクトの許可には、子項目の追加 (a) と、この項目の削除 (d) があります。

以下の表は、各 LDAP 操作の実行に必要なとされる許可を要約したものです。

| 操作          | 必要な許可                                                                                                                                                                   |
|-------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ldapadd     | 追加 (親に対する)                                                                                                                                                              |
| ldapdelete  | 削除 (オブジェクトに対する)                                                                                                                                                         |
| ldapmodify  | 書き込み (変更中の属性に対する)                                                                                                                                                       |
| ldapsearch  | <ul style="list-style-type: none"><li>検索、読み取り (RDN 内の属性に対する)</li><li>検索 (検索フィルターで指定された属性に対する)</li><li>検索 (名前とともに戻された属性に対する)</li><li>検索、読み取り (値とともに戻された属性に対する)</li></ul> |
| ldapmodrdn  | 書き込み (RDN 属性に対する)                                                                                                                                                       |
| ldapcompare | 比較 (比較対象の属性に対する)                                                                                                                                                        |

注: 検索操作の場合、サブジェクトは、検索フィルター内のすべての属性への検索アクセス権を持っている必要があります。検索アクセス権を持っていない場合、項目は戻されません。検索から戻される項目について、サブジェクトは、戻される項目の RDN のすべての属性に対して、検索および読み取りアクセス権を持っている必要があります。これらのアクセス権を持っていない場合、項目は戻されません。

**Access Target:**

これらの許可は、オブジェクト全体（子項目の追加、項目の削除）や項目内の個々の属性に適用できます。あるいは、次に説明する属性グループ（属性アクセス・クラス）に適用できます。

同様のアクセス許可を必要としている属性は、クラス内にグループ化されます。属性は、ディレクトリー・スキーマ・ファイル内の属性クラスにマッピングされます。これらのクラスは明確に区別されています。あるクラスにアクセスしても、それによって、別のクラスへのアクセスが暗黙指定されることはありません。許可は、属性アクセス・クラス全体に対して設定されます。ある特定の属性クラスに設定された許可は、個々の属性アクセス許可が指定されない限り、このアクセス・クラス内のすべての属性に適用されます。

IBM では、ユーザー属性へのアクセスの評価に使用する属性クラスとして、**normal**、**sensitive**、および **critical** の 3 つを定義しています。たとえば、属性 **commonName** は **normal** クラスに属し、属性 **userpassword** は **critical** クラスに属します。ユーザー定義属性は、特に指定がない限り、**normal** アクセス・クラスに属します。

他にも **system** および **restricted** の 2 つのアクセス・クラスも定義されています。 **system** クラス属性を以下に示します。

- **creatorsName**
- **modifiersName**
- **createTimestamp**
- **modifyTimestamp**
- **ownerSource**
- **aclSource**

これらは LDAP サーバーにより保守される属性で、ディレクトリー・ユーザーに対しては読み取り専用です。 **OwnerSource** と **aclSource** については、伝搬のトピックに説明されています。

アクセス制御を定義する属性の **restricted** クラスは、以下のとおりです。

- **aclEntry**
- **aclPropagate**
- **entryOwner**
- **ownerPropagate**
- **ibm-filterAclEntry**
- **ibm-filterAclInherit**
- **ibm-effectiveAcl**

すべてのユーザーは、**restricted** 属性への読み取りアクセスがありますが、**entryOwners** のみがこれらの属性を作成、変更、および削除できます。

注: 属性、**ibm-effectiveAcl** は読み取り専用です。

**関連概念**

78 ページの『伝搬』

項目で **aclEntry** または **entryOwner** が明示的に定義されていないと、これは上位項目から継承されるか、またはツリーを下方向にたどって伝搬されます。

**EntryOwner:**

項目の所有者は、**aclEntry** にかかわらず、オブジェクトにすべての操作を行う完全な許可を持っています。

加えて、項目の所有者は、そのオブジェクトの **aclEntry** を管理することが許可されている唯一のユーザーです。 **EntryOwner** は、アクセス制御のサブジェクトで、個人、グループ、または役割として定義できます。

注: デフォルトでは、ディレクトリー管理者はディレクトリー内のすべてのオブジェクトの **entryOwners** の一人で、ディレクトリー管理者の **entryOwnership** は、どのオブジェクトからも除去できません。

#### 伝搬:

項目で **aclEntry** または **entryOwner** が明示的に定義されていないと、これは上位項目から継承されるか、またはツリーを下方向にたどって伝搬されます。

**aclEntry** が配置されている項目は、明示的な **aclEntry** を持っている項目と見なされます。同様に、**entryOwner** が特定の項目に対して設定されている場合、その項目は、明示的な所有者を持っています。この 2 つは、互いに関連しているわけではありません。明示的な所有者を持つ項目が、明示的な **aclEntry** を持つとは限りませんし、明示的な **aclEntry** を持つ項目が、明示的な所有者を持つこともあります。これらの値のいずれかが項目上に明示的に存在していない場合、欠落している値は、ディレクトリー・ツリー内の祖先ノードから継承されます。

明示的な **aclEntry** または **entryOwner** は、それらが設定されている項目にそれぞれ適用されます。また、値は、明示的に設定された値を持たないすべての子孫に適用できます。これらの値は伝搬されるものと見なされ、ディレクトリー・ツリーを通じて伝搬されます。特定の値の伝搬は、別の伝搬中の値が到達するまで続けられます。

注: フィルター・ベースの ACL は、非フィルター・ベースの ACL と同じ方法では伝搬しません。フィルター・ベースの ACL は、関連するサブツリーで比較が一致したオブジェクトに伝搬します。

**AclEntry** および **entryOwner** は、伝搬値を「false」に指定して、特定の項目にのみ適用するように設定することができます。また、伝搬値を「true」に指定して、その項目およびそのサブツリーに適用するように設定することもできます。 **aclEntry** および **entryOwner** はいずれも伝搬できますが、それらの伝搬はリンクされません。

**aclEntry** および **entryOwner** 属性は、複数值が許可されています。ただし、伝搬属性 (**aclPropagate** および **ownerPropagate**) では、同じ項目内のすべての **aclEntry** または **entryOwner** 属性値には、単一値しか保管できません。

**system** 属性の **aclSource** および **ownerSource** には、**aclEntry** または **entryOwner** を評価する有効なノードの DN がそれぞれ含まれています。そのようなノードが存在しない場合は、値として **default** が割り当てられます。

オブジェクトの有効なアクセス制御定義は、以下のロジックによって得ることができます。

- オブジェクトに明示的なアクセス制御属性のセットがある場合は、それがオブジェクトのアクセス制御定義になります。
- 明示的に定義されたアクセス制御属性がない場合は、伝搬アクセス制御属性のセットを持つ祖先ノードに達するまで、ディレクトリー・ツリーを上方向に全探索します。
- そのような祖先ノードが見つからない場合は、以下に説明されているデフォルト・アクセスがサブジェクトに与えられます。

ディレクトリー管理者は、項目の所有者です。疑似グループ **cn=anybody** (すべてのユーザー) には、**normal** アクセス・クラス内の属性に対する読み取り、検索、および比較アクセス権が付与されます。

## 関連概念

73 ページの『フィルター済みのアクセス制御リスト』

フィルター・ベースの ACL (アクセス制御リスト) は、指定されたオブジェクト・フィルターを使用してフィルター・ベースの比較を行い、ターゲット・オブジェクトと、そのターゲット・オブジェクトに適用される有効なアクセスとを突き合わせます。

### アクセス評価:

特定の操作のためのアクセスが認可されるかまたは否認されるかは、ターゲット・オブジェクト上でその操作を行うための、サブジェクトのバインド DN によって決まります。アクセスが決定されると、処理はただちに停止されます。

アクセスの検査は、まず、有効な **entryOwnership** および **ACI** 定義を検索し、次に、項目の所有権を検査して、最後に、オブジェクトの **ACI** の値を評価することで行われます。

フィルター・ベースの ACL では、最下位の收容項目から、祖先項目チェーンを上に向かって、DIT の最上位の收容項目まで累算します。有効なアクセス権は、構成要素になっている祖先の項目により認可または拒否されたアクセス権限の和集合として計算されます。フィルター・ベースの ACL の有効なアクセスを評価するために、特定規則と結合規則の既存のセットが使用されます。

フィルター・ベースの属性と非フィルター・ベースの属性は、単一の收容ディレクトリー項目内では相互に排他的です。両方のタイプの属性を同じ項目に入れることはできません。制約違反になります。この条件が検出されると、ディレクトリー項目の作成または更新に関連する操作は失敗します。

有効なアクセスを計算する場合、ターゲット・オブジェクト項目の祖先チェーンで検出される最初の ACL タイプにより、計算のモードが設定されます。フィルター・ベース・モードでは、有効なアクセスを計算するときに非フィルター・ベースの ACL は無視されます。同様に、非フィルター・ベース・モードでは、有効なアクセスを計算するときにフィルター・ベースの ACL は無視されます。

有効なアクセスを計算するときに、フィルター・ベースの ACL の累算を制限するには、値を「false」に設定した **ibm-filterAclInherit** 属性を、特定のサブツリーの **ibm-filterAclEntry** の最上位と最下位のオカレンスの間にある項目に配置します。これにより、ターゲット・オブジェクトの祖先チェーンでそれより上にある **ibm-filterAclEntry** 属性のサブセットが無視されます。

フィルター・ベースの ACL モードでは、フィルター・ベースの ACL が適用されない場合、デフォルトの ACL が適用されます (cn=anybody には、normal アクセス・クラス内の属性に対する読み取り、検索、および比較アクセス権が付与されます)。アクセスされる項目が **ibm-filterAclEntry** 値で指定されるどのフィルターにも一致しない時に、この状態が発生します。このデフォルトのアクセス制御を適用したくない場合には、以下のようにして、デフォルトのフィルター ACL を指定できます。

```
ibm-filterAclEntry: group:cn=anybody:(objectclass=*):
```

この例では、アクセス権は付与されません。それを変更して適用したいアクセス権を指定します。

デフォルトでは、ディレクトリー管理者およびマスター・サーバー (複製の場合はピア・サーバー) は、ディレクトリー内のすべてのオブジェクトに対する全アクセス権限を取得します。ただし、system 属性への書き込みアクセス権は除きます。その他の **entryOwners** は、system 属性への書き込みアクセスを除き、その所有権の下オブジェクトへの全アクセス権限を取得します。すべてのユーザーが system および restricted 属性に対する読み取りアクセス権を持っています。これらの事前定義の権限は変更できません。要求を出しているサブジェクトが **entryOwnership** を持っている場合、アクセス権は上記のデフォルト設定によって決定され、アクセス処理は停止されます。

要求を出しているサブジェクトが `entryOwner` でない場合は、オブジェクト項目の ACI の値が検査されません。ACI 内で定義されている、ターゲット・オブジェクトに対するアクセス権は、特定規則と結合規則によって計算されます。

### 特定規則

最も特定の `aclEntry` 定義は、ユーザーへの許可の付与または否認を評価するときに使用される `aclEntry` 定義です。特定性のレベルは、以下のとおりです。

- アクセス ID (`access-id`) は、グループまたは役割よりも特定のです。グループと役割は、同じレベルです。
- 同じ `dnType` レベル内では、個々の属性レベルの許可の方が、属性クラス・レベルの許可よりも特定のです。
- 同じ属性または属性クラス・レベル内では、`deny` の方が `grant` よりも特定のです。

### 結合規則

同じ特定性を持つサブジェクトに与えられた許可は結合されます。同じ特定性のレベル内でアクセスを決定できない場合は、特定性のレベルがより低いアクセス定義が使用されます。定義済みの ACI がすべて適用されてもアクセスが決定されない場合は、アクセスが否認されます。

注: アクセス評価の際に、一致するアクセス ID レベルの `aclEntry` が見つかったら、グループ・レベルの `aclEntry` は、アクセス計算に含まれません。ただし、例外として、一致するアクセス ID レベルの `aclEntries` が `cn=this` の下ですべて定義されている場合は、一致するグループ・レベルの `aclEntries` も、評価の際にすべて結合されます。

つまり、オブジェクト項目内において、バインド DN と一致するアクセス ID サブジェクト DN が、定義済みの ACI 項目に含まれている場合、許可は、最初にその `aclEntry` に基づいて評価されます。同じサブジェクト DN の下で、一致する属性レベルの許可が定義されていると、それらの許可は、属性クラスの下で定義されているすべての許可に取って代わります。同じ属性または属性クラス・レベル定義の下で、競合する許可が存在する場合は、`deny` (否認) された許可が `grant` (付与) された許可をオーバーライドします。

注: ヌル値許可を定義すると、特定性のより低い許可定義は含まれなくなります。

アクセスがまだ決定できず、見つかった `aclEntry` のうち一致するものがすべて「`cn=this`」の下で定義されている場合は、グループ・メンバーシップが評価されます。ユーザーが複数のグループに属している場合、ユーザーは、組み合わせられた許可をそれらのグループから受け取ります。また、ユーザーは自動的に `cn=Anybody` グループに属します。ユーザーが認証済みのバインドを実行した場合は、`cn=Authenticated` グループに属することがあります。これらのグループに対して許可が定義されている場合、ユーザーは、指定された許可を受け取ります。

注: グループおよび役割のメンバーシップは、バインド時に決定されます。これらは、別のバインドが発生するまで、またはアンバインド要求を受け取るまで続きます。ネストされたグループおよび役割 (すなわち、別のグループまたは役割のメンバーとして定義されたグループまたは役割) は、メンバーシップの決定やアクセス評価で解決されません。

たとえば、`attribute1` が `sensitive` 属性クラス内にあり、ユーザー `cn=Person A, o=IBM` が `group1` と `group2` の両方に属しており、以下の `aclEntry` が定義されていると想定します。

1. `aclEntry: access-id: cn=Person A, o=IBM: at.attribute1:grant:rsc:sensitive:deny:rsc`
2. `aclEntry: group: cn=group1,o=IBM:critical:deny:rWSC`
3. `aclEntry: group: cn=group2,o=IBM:critical:grant:r:normal:grant:rsc`

このユーザーのアクセス権は以下のとおりです。

- 「rsc」から attribute1 へのアクセス権を取得します (1. より。属性レベル定義は、属性クラス・レベル定義に取って代わります)。
- ターゲット・オブジェクト内の他の sensitive クラス属性へのアクセス権は取得しません (1. より)。
- その他の権限は与えられません (2. および 3. は、アクセス評価に含まれません)。

別の例として、以下の aclEntry が定義されていると想定します。

1. aclEntry: access-id: cn=this: sensitive
2. aclEntry: group: cn=group1,o=IBM:sensitive:grant:rsc:normal:grant:rsc

このユーザーのアクセス権は以下のとおりです。

- sensitive クラス属性へのアクセス権は持ちません (1. より。access-id の下にヌル値が定義されているため、group1 の sensitive クラス属性への許可を含めることはできません)。
- 「rsc」から normal クラス属性へのアクセス権は持ちます (2. より)。

#### サブツリー複製の考慮事項:

サブツリー複製に組み込まれるフィルター・ベースのアクセスでは、すべての ibm-filterAclEntry 属性が、関連する ibm-replicationContext 項目または項目の下に存在する必要があります。

有効なアクセスは、複製されたサブツリーの上にある祖先項目から累算できないため、ibm-filterAclInherit 属性は、値を **false** に設定して、関連する ibm-replicationContext 項目に常駐する必要があります。

#### ACI と項目所有者の定義の例:

以下の 2 つの例は、コマンド行ユーティリティを使用して設定される管理サブドメインを示しています。

最初に、ドメイン全体に単一ユーザーを entryOwner として割り当てる例を示します。2 番目に、グループを entryOwner として割り当てる例を示します。

```
entryOwner: access-id:cn=Person A,o=IBM
ownerPropagate: true
```

```
entryOwner: group:cn=System Owners, o=IBM
ownerPropagate: true
```

次の例では、アクセス ID 「cn=Person 1, o=IBM」に対して attribute1 を読み取り、検索、および比較する許可を与える方法を示しています。許可は、サブツリー全体のすべてのノード、

「(objectclass=groupOfNames)」比較フィルターと一致するこの ACI を含むノード、またはそのノードの下に適用されます。祖先ノードで一致する ibm-filteraclentry 属性の累算は、ibm-filterAclInherit 属性を「false」に設定することで、この項目で終了しています。

```
ibm-filterAclEntry: access-id:cn=Person 1,o=IBM:(objectclass=groupOfNames):
 at.attribute1:grant:rsc
```

```
ibm-filterAclInherit: false
```

次の例では、グループ「cn=Dept XYZ, o=IBM」に対して attribute1 を読み取り、検索、および比較する許可を与える方法を示しています。この許可は、この ACI を含むノードの下のサブツリー全体に適用されます。

```
aclEntry: group:cn=Dept XYZ,o=IBM:at.attribute1:grant:rsc
aclPropagate: true
```

次の例では、役割「System Admins,o=IBM」に対して、このノードの下にオブジェクトを追加する許可と、attribute2 と critical 属性クラスの読み取り、検索、および比較の許可を与える方法を示しています。この許可は、この ACI を含むノードにしか適用されません。

```
acIEntry: role:cn=System Admins,o=IBM:object:grant:a:at.
 attribute2:grant:rsc:critical:grant:rsc
acIPropagate: false
```

### ACI と項目所有者の値の変更の例:

コマンド行ユーティリティーを使用して、ACI と項目所有者の値を変更するいくつかの例

#### Modify-replace

Modify-replace は、他のすべての属性と同じように機能します。属性値が存在しない場合は、値を作成します。属性値が存在する場合は、値を置換します。

たとえば、項目に対して以下の ACI がある場合、

```
acIEntry: group:cn=Dept ABC,o=IBM:normal:grant:rsc
acIPropagate: true
```

以下の変更を実行すると、

```
dn: cn=some entry
changetype: modify
replace: acIEntry
acIEntry: group:cn=Dept XYZ,o=IBM:normal:grant:rsc
```

新しい ACI は以下ようになります。

```
acIEntry: group:cn=Dept XYZ,o=IBM:normal:grant:rsc
acIPropagate: true
```

この置換により、Dept ABC の ACI 値は失われます。

たとえば、項目に対して以下の ACI がある場合、

```
ibm-filterAcIEntry: group:cn=Dept ABC,o=IBM:(cn=Manager ABC):normal
 :grant:rsc
ibm-filterAcIInherit: true
```

以下の変更を実行すると、

```
dn: cn=some entry
changetype: modify
replace: ibm-filterAcIEntry
ibm-filterAcIEntry: group:cn=Dept XYZ,o=IBM:(cn=Manager XYZ):normal
 :grant:rsc
```

```
dn: cn=some entry
changetype: modify
replace: ibm-filterAcIInherit
ibm-filterAcIInherit: false
```

新しい ACI は以下ようになります。

```
ibm-filterAcIEntry: group:cn=Dept XYZ,o=IBM:(cn=Manager XYZ):normal
 :grant:rsc
ibm-filterAcIInherit: false
```

この置換により、Dept ABC の ACI 値は失われます。

#### Modify-add

ldapmodify-add の実行中に、ACI または entryOwner が存在しない場合は、特定の値を持った ACI



または entryOwner が作成されます。 ACI または entryOwner が存在する場合は、指定された値を所定の ACI または entryOwner に追加します。たとえば、以下の ACI に対して、

```
acIEntry: group:cn=Dept XYZ,o=IBM:normal:grant:rsc
```

以下の変更を加えると、

```
dn: cn=some entry
changetype: modify
add: acIEntry
acIEntry: group:cn=Dept ABC,o=IBM:at.attribute1:grant:rsc
```

以下の複数値の acIEntry が生成されます。

```
acIEntry: group:cn=Dept XYZ,o=IBM:normal:grant:rsc
acIEntry: group:cn=Dept ABC,o=IBM:at.attribute1:grant:rsc
```

たとえば、以下の ACI に対して、

```
Ibm-filterAcIEntry: group:cn=Dept XYZ,o=IBM:(cn=Manager XYZ):normal
 :grant:rsc
```

以下の変更を加えると、

```
dn: cn=some entry
changetype: modify
add: ibm-filterAcIEntry
ibm-filterAcIEntry: group:cn=Dept ABC,o=IBM:(cn=Manager ABC)
 :at.attribute1:grant:rsc
```

以下の複数値の acIEntry が生成されます。

```
Ibm-filterAcIEntry: group:cn=Dept XYZ,o=IBM:(cn=Manager XYZ):normal
 :grant:rsc
ibm-filterAcIEntry: group:cn=Dept ABC,o=IBM:(cn=Manager ABC):at.attribute1
 :grant:rsc
```

同じ属性または属性クラスの下での許可は、基本的なビルディング・ブロックと見なされ、アクションは、修飾子と見なされます。同じ許可値が複数回追加されている場合は、1 つの値のみが保管されます。同じ許可値が異なるアクション値とともに複数回追加されている場合は、最後のアクション値が使用されます。結果の許可フィールドが空 ("") の場合、この許可値はヌルに設定され、アクション値は **grant** に設定されます。

たとえば、以下の ACI に対して、

```
acIEntry: group:cn=Dept XYZ,o=IBM:normal:grant:rsc
```

以下の変更を加えると、

```
dn: cn=some entry
changetype: modify
add: acIEntry
acIEntry: group:cn=Dept XYZ,o=IBM:normal:deny:r:critical:deny::sensitive
 :grant:r
```

以下の acIEntry が生成されます。

```
acIEntry: group:cn=Dept XYZ,o=IBM:normal:grant:sc:normal:deny:r:critical
 :grant::sensitive:grant:r
```

たとえば、以下の ACI に対して、

```
Ibm-filterAcIEntry: group:cn=Dept XYZ,o=IBM:(cn=Manager XYZ):normal
 :grant:rsc
```

以下の変更を加えると、

```
dn: cn=some entry
changetype: modify
add: ibm-filterAclEntry
ibm-filterAclEntry: group:cn=Dept XYZ,o=IBM:(cn=Manager XYZ):normal
 :deny:r:critical:deny::sensitive:grant:r
```

以下の aclEntry が生成されます。

```
ibm-filterAclEntry: group:cn=Dept XYZ,o=IBM:(cn=Manager XYZ):normal
 :grant:sc:normal:deny:r:critical:grant::sensitive
 :grant:r
```

## Modify-delete

特定の ACI 値を削除するには、通常の ldapmodify-delete 構文を使用します。

以下の ACI では、

```
aclEntry: group:cn=Dept XYZ,o=IBM:object:grant:ad
aclEntry: group:cn=Dept XYZ,o=IBM:normal:grant:rWSC
```

```
dn: cn = some entry
changetype: modify
delete: aclEntry
aclEntry: group:cn=Dept XYZ,o=IBM:object:grant:ad
```

サーバー上で存続する以下の ACI が生成されます。

```
aclEntry: group:cn=Dept XYZ,o=IBM:normal:grant:rWSC
```

以下の ACI では、

```
ibm-filterAclEntry: group:cn=Dept XYZ,o=IBM:(cn=Manager XYZ):object
 :grant:ad
ibm-filterAclEntry: group:cn=Dept XYZ,o=IBM:(cn=Manager XYZ):normal
 :grant:rWSC
```

```
dn: cn = some entry
changetype: modify
delete: ibm-filterAclEntry
ibm-filterAclEntry: group:cn=Dept XYZ,o=IBM:(cn=Manager XYZ):object
 :grant:ad
```

サーバー上で存続する以下の ACI が生成されます。

```
ibm-filterAclEntry: group:cn=Dept XYZ,o=IBM:(cn=Manager XYZ):normal
 :grant:rWSC
```

存在しない ACI 値または entryOwner 値を削除しても、ACI または entryOwner は変更されず、属性値が存在しないことを示す戻りコードが戻されます。

## ACI と項目所有者の値の削除の例:

コマンド行ユーティリティーを使用した、ACI と項目所有者の値の削除の例

ldapmodify-delete 操作では、以下のように指定して、entryOwner を削除できます。

```
dn: cn = some entry
changetype: modify
delete: entryOwner
```

この場合、項目は、明示的な entryOwner を持たなくなります。ownerPropagate も自動的に除去されます。この項目は、伝搬規則に従って、ディレクトリー・ツリー内の祖先ノードから、その entryOwner を継承するようになります。

aclEntry を完全に削除する場合も、これと同じ方法が使用できます。

```
dn: cn = some entry
changetype: modify
delete: aclEntry
```

最後の ACI 値または entryOwner 値を項目から削除することと、ACI または entryOwner を削除することとは異なります。項目には、値を持たない ACI または entryOwner を含めることができます。この場合、ACI または entryOwner を照会しても、クライアントには何も戻されません。また、設定は、オーバーライドされるまでは、下層ノードに伝搬されます。いずれのユーザーもアクセスできないようなぶら下がり項目を防止するため、ディレクトリー管理者は、項目にヌルの ACI 値または entryOwner 値がある場合であっても、その項目への全アクセス権限を常に所有します。

### ACI と項目所有者の値の検索の例:

コマンド行ユーティリティーを使用した、ACI と項目所有者の値の検索の例

有効な ACI または entryOwner の値は、必要とする ACL または entryOwner 属性を検索する際に指定するだけで取得できます。

```
ldapsearch -b "cn=object A, o=ibm" -s base "objectclass=*"
 aclentry aclpropagate aclsource entryowner ownerpropagate ownersource
 ibm-filterAclEntry ibm-filterAclInherit ibm-effectiveAcl
```

object A に対するアクセス評価で使用される ACL または entryOwner 情報がすべて戻されます。戻り値は、最初に定義された形と多少異なる場合があることに注意してください。値は、元の形式と同等です。

ibm-filterAclEntry 属性のみを検索すると、収容項目に特定の値のみが戻されます。

読み取り専用の操作属性 ibm-effectiveAcl は、累算された有効なアクセスを表示するために使用されます。ibm-effectiveAcl の検索要求は、非フィルター ACL またはフィルター ACL が DIT 内にどのように分散されているかによって、非フィルター ACL またはフィルター ACL に基づいてターゲット・オブジェクトに適用される有効なアクセスを戻します。

フィルター・ベースの ACL は、複数の祖先ソースから発生することがあるため、aclSource 属性の検索により、関連するソースのリストが作成されます。

## 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。

所有権を割り当てるには、以下のいずれかを行います。

- 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。

Directory Server 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 という名前ですべて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。

## 関連概念

218 ページの『ディレクトリー項目タスク』

以下の情報を参考にして、ディレクトリー項目を管理します。

## パスワード・ポリシー

認証に LDAP サーバーの使用においては、LDAP サーバーがパスワードの有効期限、失敗したログイン試行、およびパスワード規則に関するポリシーをサポートすることが重要です。Directory Server では、この種のポリシー 3 つすべてを構成できます。

パスワード・ポリシーは、userPassword 属性を持つすべてのディレクトリー項目に適用されます。あるポリシーをあるユーザーのセットに定義し、異なるポリシーを別のユーザーのセットに定義することはできません。Directory Server は、クライアントにパスワード・ポリシーに関連した条件 (3 日でパスワードの有効期限が切れる) を知らせるメカニズムや、管理者が、有効期限が切れたパスワードやロックアウトしたアカウントを持つユーザーなどを検索するために使用できる操作属性のセットも提供します。

## Configuration

以下の領域のパスワードに関して、サーバーの動作を構成することができます。

- パスワード・ポリシーを使用可能または使用不可にするためのグローバル「オン/オフ」スイッチ
- 以下を含むパスワード変更の規則
  - ユーザーは自分のパスワードを変更できる。このポリシーは、アクセス制御に追加して適用される点に注意してください。すなわち、アクセス制御により、ユーザーに userPassword 属性を変更する権限と、自分のパスワードを変更することを許可するパスワード・ポリシーを付与する必要があります。このポリシーが使用不可の場合、ユーザーは自分のパスワードを変更できません。userPassword 属性を変更する権限を持つ管理者または他のユーザーのみが項目のパスワードを変更できます。
  - パスワードを再設定後に変更する必要がある。このポリシーが使用可能の場合、そのユーザー以外の誰かがパスワードを変更した時、そのパスワードは再設定としてマークされ、ユーザーは、他のディレクトリー操作を実行する前にそれを変更する必要があります。再設定されたパスワードでのバインド要求は成功します。パスワードを再設定する必要があるという通知を受けるには、アプリケーションはパスワード・ポリシーを取り入れる必要があります。
  - ユーザーは、パスワードを変更する時に旧パスワードを送信する必要がある。このポリシーが使用可能の場合、変更要求によってのみパスワードを変更できます。変更要求には、userPassword 属性 (古い値を持つ) の削除および新規 userPassword 値の追加の両方が含まれます。これにより、確実に自分のパスワードを知っているユーザーのみがそれを変更できるようにします。userPassword 属性を変更する許可を持つ管理者または他のユーザーは、常にパスワードを設定できます。
- 以下を含むパスワード有効期限の規則
  - パスワードは決して有効期限が切れないか、パスワードが最後に変更されてから特定の (構成可能な) 時間の後に有効期限が切れるか。
  - パスワードの有効期限が切れる時にユーザーに警告しないか、パスワードの有効期限が切れることを前もってユーザーに警告するか (どれくらい前に警告するかも構成可能)。パスワードの有効期限が近いという警告を受けるために、アプリケーションはパスワード・ポリシーを取り入れる必要があります。
  - ユーザーのパスワードの有効期限が切れてから特定の猶予ログイン数 (構成可能な数) を許可する。パスワード・ポリシーを取り入れているアプリケーションでは、残りの猶予ログイン数が通知されません。猶予ログインが許可されていない場合、パスワードの有効期限が切れると、ユーザーは自分のパスワードに認証したり、それを変更したりできません。
- 以下を含むパスワード妥当性検査の規則

- 以前に使用された最近の N 個のパスワードおよび拒否されたパスワードの履歴を保存するようにサーバーを設定する特定の (構成可能な) パスワード・履歴・サイズ。
- パスワードがハッシュされた時にサーバーがどのような動作をするかの設定を含むパスワード構文検査。この設定は、以下のいずれかの条件下でサーバーがポリシーを無視するかに影響します。
  - サーバーがハッシュ・パスワードを保管している。
  - クライアントがサーバーにハッシュ・パスワードを提示している (このことは、ソース・サーバーがハッシュ・パスワードを保管している場合に、LDIF ファイルを使用してサーバー間で項目を送る時に発生します)。

いずれの場合においても、サーバーはすべての構文規則を適用できないかもしれません。最小の長さ、最低の英字数、最低の数字数または特殊文字数、反復文字数、直前のパスワードとは異なっていなければならないパスワードの文字数に関する構文規則がサポートされています。

- 以下を含む失敗したログインの規則
  - パスワード変更が許可される最小の時間間隔。これは、ユーザーがあるパスワードのセットを短時間のうちに反復して元のパスワードに戻すことがないようにします。
  - アカウントがロックされる前に許可される失敗したログイン試行の最大数。
  - 特定の (構成可能な) パスワード・ロックアウト期間。この時間の後、直前のロックされたアカウントが使用できます。これは、ユーザーが自分のパスワードを忘れたときに助けとなると同時に、パスワードを破壊しようとするハッカーをロックアウトする助けとなります。
  - サーバーが失敗したログイン試行を追跡する特定の (構成可能な) 時間。失敗したログイン試行の最大数がこの時間内に発生した場合、アカウントがロックされます。この時間が満了すると、サーバーはそのアカウントの直前までの失敗したログイン試行に関する情報を破棄します。

ディレクトリー・サーバーのためのパスワード・ポリシー設定は、オブジェクト「cn=pwdpolicy」に保管されます。例を以下に示します。

```
cn=pwdpolicy objectclass=container objectclass=pwdPolicy
objectclass=ibm-pwdPolicyExt
objectclass=top
cn=pwdPolicy
pwdExpireWarning=0
pwdGraceLoginLimit=0
passwordMaxRepeatedChars=0
pwdSafeModify=false
pwdattribute=userpassword
pwdinhistory=0
pwdchecksyntax=0
passwordminotherchars=0
passwordminalphachars=0
pwdminlength=0
passwordmindiffchars=0
pwdminage=0
pwdmaxage=0
pwdallowuserchange=true
pwdlockoutduration=0
ibm-pwdpolicy=true
pwdlockout=true
pwdmaxfailure=2
pwdfailurecountinterval=0
pwdmustchange=false
```

## パスワード・ポリシー対応アプリケーション

Directory Server のパスワード・ポリシー・サポートには、パスワード・ポリシー対応アプリケーションがパスワード・ポリシー関連の追加条件の通知を受け取るための LDAP コントロールのセットが組み入れられています。

アプリケーションは、以下の警告条件の通知を受け取ることができます。

- パスワードの満了までの残り時間
- パスワードの有効期限が切れた後に残っている猶予ログイン数

アプリケーションは、以下のエラー条件の通知も受け取ることができます。

- パスワードの有効期限が切れた
- アカウントがロックされている
- パスワードが再設定されたので変更する必要がある
- ユーザーは自分のパスワードを変更することが許可されていない
- パスワードを変更する時に旧パスワードを入力する必要がある
- 新規パスワードが構文規則に違反している
- 新規パスワードは短すぎる
- パスワードが変更されてから時間が経っていない
- 新規パスワードは履歴にある

2 つの制御が使用されます。パスワード・ポリシー要求制御を使用して、アプリケーションはパスワード・ポリシー関連条件の通知を受け取りたいことをサーバーに知らせます。この制御は、行いたいすべての操作 (通常は、初期バインド要求およびパスワード変更要求) に対してアプリケーションによって指定する必要があります。パスワード・ポリシー要求制御がある場合、上記のいずれかのエラー状態が存在する場合にパスワード・ポリシー応答制御がサーバーから戻されます。

Directory Server クライアント API には、C アプリケーションがこれらの制御を処理するために使用される API のセットが含まれます。これらの API を以下に示します。

- ldap\_parse\_pwdpolicy\_response
- ldap\_pwdpolicy\_err2string

これらの API を使用しないアプリケーションについては、制御は以下に定義されています。制御を処理するために、使用される LDAP クライアント API により提供される機能を使用する必要があります。たとえば、Java™ Naming and Directory Interface (JNDI) には、幾つかの既知の制御に対する組み込みサポートがあり、JNDI が認識しない制御をサポートするためのフレームワークも提供しています。

## パスワード・ポリシー要求制御

Control name: 1.3.6.1.4.1.42.2.27.8.5.1  
Control criticality: FALSE  
Control value: None

## パスワード・ポリシー応答制御

Control name: 1.3.6.1.4.1.42.2.27.8.5.1 (same as the request control)  
Control criticality: FALSE  
Control value: A BER encoded value defined in ASN.1 as follows:  
    PasswordPolicyResponseValue ::= SEQUENCE {  
        warning [0] CHOICE OPTIONAL {  
            timeBeforeExpiration [0] INTEGER (0 .. MaxInt),  
            graceLoginsRemaining [1] INTEGER (0 .. maxInt) }  
    }

```
error [1] ENUMERATED OPTIONAL {
passwordExpired (0),
accountLocked (1),
changeAfterReset (2),
passwordModNotAllowed (3),
mustSupplyOldPassword (4),
invalidPasswordSyntax (5),
passwordTooShort (6),
passwordTooYoung (7),
passwordInHistory (8) }
```

他の LDAP プロトコル・エレメント同様、BER エンコード方式では、暗黙的なタグ付けが使用されません。

## パスワード・ポリシー運用属性

Directory Server は、userPassword 属性を持つ項目ごとに運用属性のセットを保守します。これらの属性は、許可ユーザーにより検索され、検索フィルター内で使用されるか、検索要求により戻されます。これらの属性を以下に示します。

- pwdChangedTime - パスワードが最後に変更された時刻が含まれる GeneralizedTime 属性。
- pwdAccountLockedTime - アカウントがロックされた時刻が含まれる GeneralizedTime 属性。アカウントがロックされていない場合、この属性は存在しません。
- pwdExpirationWarned - パスワード有効期限警告が最初にクライアントに送信された時刻が含まれる GeneralizedTime 属性。
- pwdFailureTime - 直前の連続ログイン失敗の回数が含まれる複数値の GeneralizedTime 属性。前回のログインが成功であった場合、この属性は存在しません。
- pwdGraceUseTime - 直前の猶予ログイン数が含まれる複数値の GeneralizedTime 属性。
- pwdReset - パスワードが再設定され、ユーザーが変更する必要がある場合 TRUE の値を持つ Boolean 属性。
- ibm-pwdAccountLocked - アカウントが管理上ロックされたことを示す Boolean 属性。

## パスワード・ポリシーの複製

パスワード・ポリシー情報は、サプライヤー・サーバーによりコンシューマーに複製されます。項目 cn=pwdpolicy への変更内容は、スキーマへの変更同様一括変更として複製されます。個々の項目のパスワード・ポリシー状態情報も複製されるため、たとえば、ある項目がサプライヤー・サーバーでロックされる場合、そのアクションはあらゆるコンシューマーに複製されます。読み取り専用レプリカへのパスワード・ポリシー状態変更では、他のサーバーには複製されません。

### 関連概念

196 ページの『パスワード・タスク』

以下の情報を参考にして、パスワード・タスクを管理します。

102 ページの『操作属性』

Directory Server に対して特殊な意味を持つ、操作属性という幾つかの属性があります。これらは、サーバーによって保守される属性であり、サーバーがある 1 つの項目について管理している情報を反映するか、またはサーバーの動作に影響を及ぼします。

## パスワード・ポリシーのヒント

パスワード・ポリシーは、見込みどおりに動作するとは限りません。

パスワード・ポリシーのインプリメンテーションが予測どおりに作動しない領域が次のように 2 つあります。

1. `pwdReset` 属性が項目に設定された場合は、クライアントは項目 DN とリセットされたパスワードを使用して無期限にバインドすることができます。「パスワード・ポリシー要求制御」の存在により、この結果は、応答制御に警告が示された正常バインドとなります。ただし、クライアントが要求制御を指定しない場合、この「パスワード・ポリシーを認識しない」クライアントは、パスワードの変更が必要という表示なしで、正常バインドとみなします。この DN での後続の操作は、「不本意な実行」エラーで失敗します。すなわち、初期バインドの結果のみが「誤り」と見なされます。認証のみのためにバインドが実行された場合にこの問題が生じることがあり、認証のためにディレクトリーを使用する Web アプリケーションの場合などで起こります。
2. パスワードを変更している項目の DN 以外の識別でパスワードを変更するアプリケーションでは、`pwdSafeModify` と `pwdMustChange` のポリシーは予測どおりに作動しないことがあります。このシナリオでは、管理 ID による安全なパスワード変更は、たとえば、`pwdReset` 属性が設定される結果となります。前述したように、パスワードを変更するアプリケーションは、管理者アカウントを使用して `pwdReset` 属性を除去することができます。

## 認証

Directory Server 内のアクセスを制御するには、認証方式を使用します。

Directory Server 内部のアクセス制御は、特定の接続と関連した識別名 (DN) を基にしています。その DN は、Directory Server へのバインド (ログイン) の結果として設定されます。

Directory Server が最初に構成される時、以下の ID を使用してサーバーに認証できます。

- Anonymous
- ディレクトリー管理者 (デフォルトでは `cn=admin`)
- プロジェクト i5/OS ユーザー・プロファイル

ディレクトリーのさまざまな部分を管理する権限が与えられた追加ユーザーを作成し、ディレクトリー管理者 ID を共用する必要がないようにするのは良い方法です。

LDAP の観点では、LDAP に認証するために以下のフレームワークがあります。

- 単純バインド。アプリケーションは DN およびその DN 用の平文パスワードを規定します。
- Simple Authentication and Security Layer (SASL)。これは、CRAM-MD5、DIGEST-MD5、EXTERNAL、GSSAPI、および OS400-PRFTKN を含む幾つかの追加認証方式を提供します。

## 単純なバインド、DIGEST-MD5、および CRAM-MD5

単純バインドを使用するには、クライアントは既存の LDAP の DN およびその項目の `userPassword` 属性と一致するパスワードを入力する必要があります。たとえば、John Smith の項目を以下のようにして作成できます。

```
sample.ldif:
dn: cn=John Smith,cn=users,o=acme,c=us
objectclass: inetorgperson
cn: John Smith
sn: smith
userPassword: mypassword
```

```
ldapadd -D cn=admin -w secret -f sample.ldif
```



これにより、アクセス制御において DN 「cn=John Smith,cn=users,o=acme,c=us」を使用したり、それをアクセス制御で使用されるグループのメンバーにすることができます。

幾つかの事前定義の objectclass により、userPassword に person、organizationalperson、inetorgperson、organization、organizationalunit など (これらに限定されません) を指定できます。

Directory Server のパスワードは大/小文字の区別をします。userPassword 値 secret を持つ項目を作成する場合、パスワード SECRET を指定するバインドは失敗します。

単純バインドを使用するとき、クライアントは平文パスワードをバインド要求の一部としてサーバーに送信します。これにより、パスワードはプロトコル・レベルのスヌープの影響を受けやすくなります。SSL 接続を使用してパスワードを保護できます (SSL 接続を介して送信されるすべての情報は暗号化されます)。あるいは、DIGEST-MD5 または CRAM-MD5 SASL 方式を使用できます。

CRAM-MD5 方式では、サーバーは平文パスワードへのアクセス権が必要となります (パスワード保護は none に設定されます。これは、パスワードが非暗号化形式で保管され、検索時に平文で戻されるということの意味をしています)。また、QRETSVRSEC (サーバー・セキュリティ・データの保存) システム値は 1 (データの保存) に設定されていなければなりません。クライアントは、DN をサーバーに送信します。サーバーは、項目の userPassword 値を検索し、ランダム・ストリングを生成します。ランダム・ストリングはクライアントに送信されます。クライアントおよびサーバーの両方は、パスワードをキーとして使用しランダム・ストリングをハッシュし、クライアントはその結果をサーバーに送信します。2 つのハッシュ・ストリングが一致した場合、バインド要求は成功し、パスワードはサーバーに送信されていません。

DIGEST-MD5 方式は CRAM-MD5 と類似しています。ここでは、サーバーは平文パスワードへのアクセス権が必要です (パスワード保護は none に設定される)。また、QRETSVRSEC システム値は 1 に設定されていなければなりません。サーバーに DN を送信する代わりに、DIGEST-MD5 では、クライアントが username 値をサーバーに送信しなければなりません。通常ユーザー (管理者でない) が DIGEST-MD5 を使用できるようにするには、ディレクトリー中の他の項目が username 属性で同じ値を持たないようにする必要があります。DIGEST-MD5 と異なるその他の点は、構成オプション、すなわち、サーバー・レルム、username 属性、および管理者パスワードにあります。Directory Server によって、ユーザーはプロジェクトまたは公開されたユーザーとしてバインドできます。その場合、サーバーは、システム上のユーザー・プロファイルのパスワードに対して指定されたパスワードを検証します。ユーザー・プロファイルの平文パスワードはサーバーに対して使用できないので、プロジェクトまたは公開されたユーザーでは DIGEST-MD5 は使用できません。

## 公開されたユーザーとしてのバインド

Directory Server は、同じシステム上でパスワードがオペレーティング・システムのユーザー・プロファイルのパスワードとなっている LDAP 項目を持つ手段を備えています。そのためには、項目は次のようであればなりません。

- 値がオペレーティング・システムのユーザー・プロファイルの名前である UID 属性を持っている
- userPassword 属性を持っていない

UID 値を持っていても userPassword は持っていない項目へのバインド要求をサーバーが受け取る時、サーバーはオペレーティング・システムのセキュリティを呼び出し、その UID は有効なユーザー・プロファイル名であり、指定されたパスワードがそのユーザー・プロファイルの正しいパスワードであることの妥当性検査をします。そうした項目は、公開されたユーザーと呼ばれます。ここで言う「公開」とは、システム配布ディレクトリー (SDD) を LDAP に公開するということであり、この時点で項目が作成されます。

## プロジェクト・ユーザーとしてのバインド

オペレーティング・システムのユーザー・プロファイルを表す LDAP 項目は、プロジェクト・ユーザーと呼ばれます。プロジェクト・ユーザーの DN をそのユーザー・プロファイル用の正しいパスワードとともに単純バインドで使用できます。たとえば、システム my-system.acme.com 上のユーザー JSMITH の DN は以下のようになります。

```
os400-profile=JSMITH,cn=accounts,os400-sys=my-system.acme.com
```

## SASL EXTERNAL バインド

SSL または TLS 接続がクライアント認証で使用される場合 (たとえば、クライアントが専用証明書を持つ場合)、SASL EXTERNAL 方式を使用できます。この方式では、サーバーがクライアントの ID を外部ソースから取得するように通知します (この場合、SSL 接続となります)。サーバーは、(SSL 接続の設定の一部としてサーバーに送信された) クライアント証明書の共通部分を取得し、サブジェクト DN を抽出します。その DN は、LDAP サーバーにより接続に割り当てられます。

たとえば、証明書が以下のよう割り当てられているとします。

```
common name: John Smith
organization unit: Engineering
organization: ACME
locality: Minneapolis
state: MN
country: US
```

サブジェクト DN は以下のようになります。

```
cn=John Smith,ou=Engineering,o=acme,l=Minneapolis,st=MN,c=US
```

サブジェクト DN を生成するために、cn、ou、o、l、st、および c エレメントは示されている順序で使用されるという点に注意してください。

## SASL GSSAPI バインド

SASL GSSAPI バインド・メカニズムは、Kerberos チケットを使用してサーバーに認証するために使用されます。これは、クライアントが KINIT または他の形式の Kerberos 認証をしたときに便利です (たとえば、Windows 2000 ドメインのログインなど)。この場合、サーバーはクライアントのチケットを検証した後、Kerberos プリンシパルおよびレルム名を取得します。たとえば、レルム acme.com 内のプリンシパル jsmith は、通常 jsmith@acme.com と表記されます。この ID を DN にマップするには、次の 2 つの方法のいずれかでサーバーを構成することができます。

- 形式 `ibm-kn=jsmith@acme.com` の疑似 DN を生成する。
- `ibm-securityidentities` 補助クラスおよび形式 `KERBEROS:<principal>@<realm>` の `altsecurityidentities` 値を持つ項目を検索する。

jsmith@acme.com 用に使用できる項目は以下のようになります。

```
dn: cn=John Smith,cn=users,o=acme,c=us
objectclass: inetorgperson
objectclass: ibm-securityidentities
cn: John Smith
sn: Smith
altsecurityidentities: kerberos:jsmith@acme.com
```

## OS400-PRFTKN バインド

OS400-PRFTKN SASL バインド・メカニズムは、プロファイル・トークンを使用してサーバーに認証するために使用されます (Generate Profile Token API を参照します)。このメカニズムが使用される時、サーバーはプロファイル・トークンの妥当性検査をし、プロジェクト・ユーザー・プロファイルの DN を接続と関連付けます (たとえば、os400-profile=JSMITH,cn=accounts,os400-system=my-as400.mycompany.com)。アプリケーションがすでにプロファイル・トークンを持っている場合、このメカニズムはユーザー・プロファイル名およびユーザー・パスワードを取得して単純バインドを実行する必要を回避します。このメカニズムを使用するためには、ldap\_sasl\_bind\_s API を使用し、メカニズムにヌル DN、OS400-PRFTKN を指定し、信任状用の 32 バイトのプロファイル・トークンを入れた berval (簡略 BER(Basic Encoding Rules) を使用してエンコードされるバイナリー・データ) を指定します。ローカル・ディレクトリー・サーバーにアクセスするために i5/OS の LDAP API を使用するか、あるいは QSH コマンド・ユーティリティー (ldapsearch など) を使用する時には、パスワードを省略できます。クライアント API はそのジョブの現行ユーザー・プロファイルとしてサーバーに対して認証することになります。たとえば次のようになります。

```
> ldapsearch -m OS400-PRFTKN -b "o=ibm,c=us" "(uid=johndoe)"
```

上記は、ユーザーが下記を使用したかのように、現行のユーザー・プロファイルの権限で検索を実行します。

```
> ldapsearch -D os400-profile=myprofile,cn=accounts,os400-sys=mssystem -w mypassword -b "o=ibm,c=us" "(uid=johndoe)"
```

## 認証サービスとしての LDAP

LDAP は、通常認証サービスを提供するために使用されます。Web サーバーを構成して LDAP に認証できます。複数の Web サーバー (または他のアプリケーション) が LDAP に認証するようにセットアップすることにより、それぞれのアプリケーションまたは Web サービス・インスタンスごとに何度もユーザーを定義するのではなく、それらのアプリケーションに対する単一のユーザー・レジストリーを設定できます。

この処理方法を説明します。簡単に言うと、Web サーバーがユーザーにユーザー名およびパスワードを求めるプロンプトを出します。Web サーバーはこの情報を取得した後、そのユーザー名で LDAP ディレクトリー内で項目の検索をします (たとえば、Web サーバーを、ユーザー名を LDAP 「uid」または「mail」属性にマップするように構成できます)。Web サーバーが 1 つの項目だけを検出した場合、Web サーバーはバインド要求を、その検出された項目の DN およびユーザーが指定したパスワードを使用するサーバーに送信します。バインドに成功した場合、ユーザーは認証されます。プロトコル・レベルのスヌープからパスワード情報を保護するために、SSL 接続が使用されます。

Web サーバーは使用された DN も追跡でき、特定のアプリケーションがその DN を使用できるようにします。これは通常、その項目内、それに関連した別の項目内、または情報を検索するために DN をキーとして使用する別個のデータベース内にカスタマイズ・データを保管することにより行います。

バインド要求の使用の一般的な代替方法は、LDAP 比較操作の使用です。たとえば、ldap\_compare(ldap\_session, dn, "userPassword", enteredPassword) を使用します。これにより、アプリケーションは、認証要求ごとにセッションを開始し終了するのではなく、単一の LDAP セッションを使用します。

### 関連概念

94 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』

システム・プロジェクト・バックエンドには、i5/OS オブジェクトを、LDAP でアクセスできるディ

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 表記のオペレーティング・システム・オブジェクトになります。

227 ページの『ユーザー・タスク』

以下の情報を参考にして、ユーザーを管理します。

Lightweight Directory Access Protocol (LDAP) API

Directory Server API の詳細は、『Lightweight Directory Access Protocol (LDAP) APIs』を参照してください。

### 関連タスク

206 ページの『Directory Server での DIGEST-MD5 認証の構成』

以下の情報を参考にして、Directory Server で DIGEST-MD5 認証を構成します。

205 ページの『Directory Server での Kerberos 認証の使用可能化』

以下の情報を参考にして、Directory Server で Kerberos 認証を使用可能にします。

## サービス妨害

サービス妨害アタックに対する保護を備えるには、サービス妨害構成オプションを使用します。

ディレクトリー・サーバーは以下のようなタイプのサービス妨害攻撃から保護します。

- データ送信が遅い、部分データを送信する、またはデータを送信しないクライアント
- データ結果を読み取らないか、または結果の読み取りが遅いクライアント
- アンバインドしないクライアント
- 長時間実行データベース要求を生成する要求を行うクライアント
- 匿名でバインドするクライアント
- 管理者がサーバーを管理できないようにするサーバー・ロード

ディレクトリー・サーバーでは、サービス妨害攻撃を防止するために、いくつかの方法が管理者に提供されます。長時間実行操作によりサーバーが使用中の場合でも、管理者は常に、緊急スレッドを使用してサーバーにアクセスします。さらに、管理者にはサーバー・アクセスに対する制御権があり、特定のバインド DN または IP アドレスでクライアントを切断できるし、匿名アクセスを許可しないようにサーバーを構成することもできます。サーバーがサービス妨害攻撃を積極的に防止できるようにするために、その他の構成オプションも活動化することができます。

### 関連タスク

133 ページの『サーバー接続の管理』

以下の情報を参考にして、サーバーへの接続、およびその接続で実行される操作を表示します。

134 ページの『接続プロパティの管理』

以下の情報を参考にして、クライアントがサーバーをロックできないようにするためといった目的で、接続プロパティを設定します。

## 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、i5/OS 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 表記のオペレーティング・システム・オブジェクトになります。

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、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、オペレーティング・システム・ユーザー・プロジェクト・バックエンドと呼ばれます。

LDAP 操作は基礎オペレーティング・システム・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。

#### 関連タスク

140 ページの『プロジェクト・ユーザーへの管理者アクセスの許可』

以下の情報を参考にして、ユーザー・プロファイルに管理者権限を認可します。

#### 関連資料

90 ページの『認証』

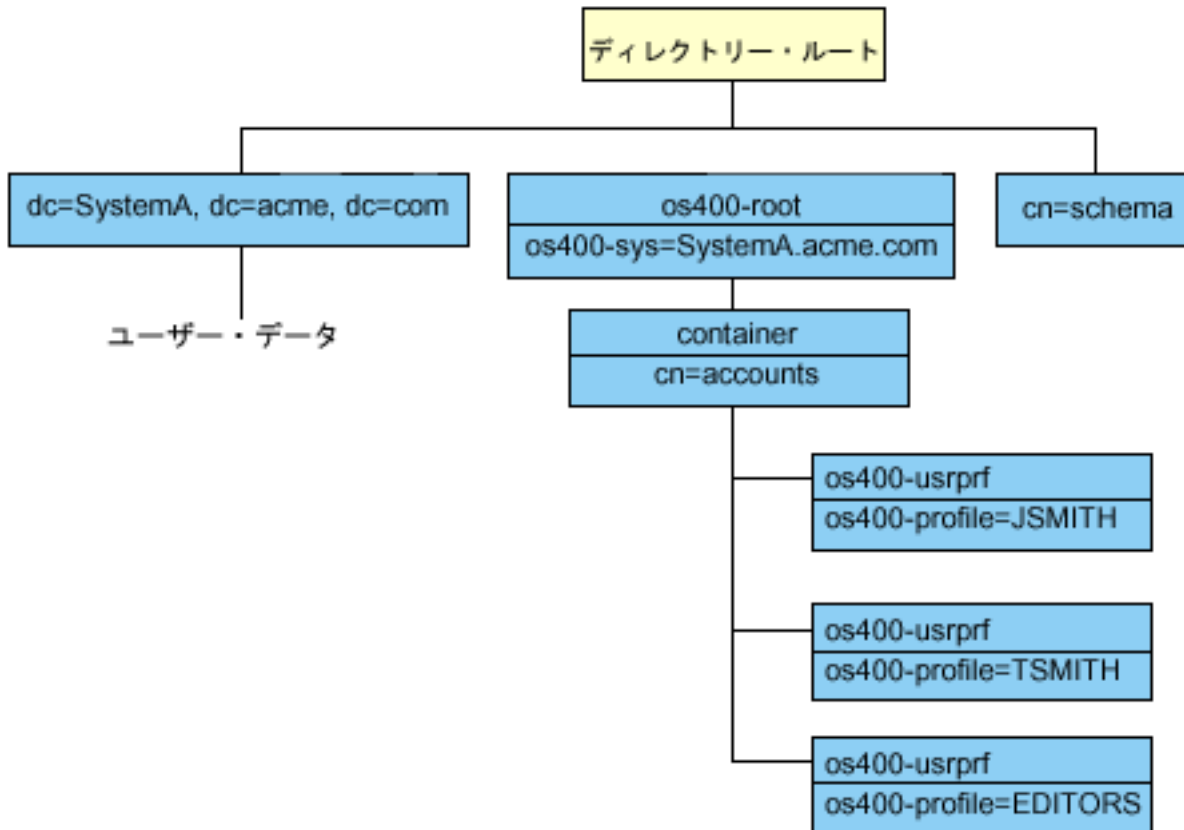
Directory Server 内のアクセスを制御するには、認証方式を使用します。

## ユーザー・プロジェクト・ディレクトリー情報ツリー

ユーザー・プロジェクト・ディレクトリー情報ツリー上で、接尾部およびユーザー・プロファイルがどのように表されるかを説明します。

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、個人のプロファイルとグループ・プロファイル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。objectclass 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項目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 `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・バックエンドに対してどの LDAP 操作を実行できるかの理解。

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。

ディレクトリー・サーバーにプロジェクト・ユーザーとして認証するために、以下の 2 つの追加メカニズムが使用できます。

- GSSAPI SASL バインド。オペレーティング・システムがエンタープライズ識別マッピング (EIM) を使用するように構成されている場合、ディレクトリー・サーバーは EIM を照会して、初期 Kerberos ID から取得したローカル・ユーザー・プロファイルとの関連があるかを判別します。そうした関連があった場合、サーバーはユーザー・プロファイルを接続と関連付け、それをシステム射影バックエンドにアクセスするために使用します。
- OS400-PRFTKN SASL バインド。ディレクトリー・サーバーへの認証にプロファイル・トークンが使用できます。サーバーは、プロファイル・トークン・ユーザー・プロファイルを接続と関連付けます。

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、幾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、`objectclass 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 `objectclass` 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。

- | LDAP 管理者は、ユーザー・プロジェクト・バックエンドを対象としたすべての検索操作を禁止することができます。詳細は、以下の関連リンクの中の『プロジェクト・ユーザーへの読み取りアクセス』のトピックを参照してください。

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 3. 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、および (オプションで) それらのコンテナ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=*<br>objectclass=os400-root<br>objectclass=container<br>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。                               |
| 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)、objectclass、および os400-profile 値のみが戻される。他のフィルターを指定すると、LDAP_UNWILLING_TO_PERFORM が戻されます。 |
| 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)、objectclass、および os400-profile 値のみが戻される。他のフィルターを指定すると、LDAP_UNWILLING_TO_PERFORM が戻されます。 |

表 3. 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・プロファイルとグループ・プロファイルに戻す。                              | 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)、objectclass、および os400-profile 値のみが戻される。他のフィルターを指定すると、LDAP_UNWILLING_TO_PERFORM が戻されます。 |
| 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=*<br>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 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。                            |
| A で始まるすべてのユーザー・プロファイルとグループ・プロファイルに戻す。                        | 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)、objectclass、および os400-profile 値のみが戻される。他のフィルターを指定すると、LDAP_UNWILLING_TO_PERFORM が戻されます。 |
| G で始まるすべてのグループ・プロファイルに戻す。                                    | 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)、objectclass、および os400-profile 値のみが戻される。他のフィルターを指定すると、LDAP_UNWILLING_TO_PERFORM が戻されます。 |
| A で始まるすべてのユーザー・プロファイルに戻す。                                    | 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)、objectclass、および os400-profile 値のみが戻される。他のフィルターを指定すると、LDAP_UNWILLING_TO_PERFORM が戻されます。 |

## 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。

- | LDAP 管理者は、ユーザー・プロジェクト・バックエンドを対象としたすべての比較操作を禁止することができます。詳細は、以下の関連リンクの中の『プロジェクト・ユーザーへの読み取りアクセス』のトピックを参照してください。

## 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 (Delete)

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 OWNBOJPT 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



制御値は以下の形式のストリングです。

- 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

制御値は以下の形式のストリングとして定義されています。

```
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場合、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。

### 関連概念

エンタープライズ識別マッピング (EIM)

『プロジェクト・ユーザーへの読み取りアクセス』

デフォルトでは、LDAP 検索および比較操作を介したユーザー・プロファイル情報への読み取りアクセスが、許可ユーザーに対してシステム射影バックエンドから提供されます。プロジェクト・ユーザーへの読み取りアクセスを有効化または無効化するには、System i Navigator を使用するか、または /QIBM/UserData/OS400/DirSrv/idsslapd-instance/etc/ibmslapd.conf ファイル (デフォルト・サーバー・インスタンス用の /QIBM/UserData/OS400/DirSrv/idsslapd-QUSRDIR/etc/ibmslapd.conf ファイル) 内での構成設定を介します。

## 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。管理者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。

### 関連概念

70 ページの『管理アクセス』

管理アクセスを使用して、個々の管理用タスクへのアクセスを制御します。

## 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になります)。たとえば、os400-usrcls 属性は、CRTUSRPRF コマンドの USRCLS パラメーターに対応します。属性の値は、CRTUSRPRF および CHGUSRPRF コマンドにより受け入れ済みのパラメーター値、またはユーザー・プロファイルを表示するときに表示される値に対応します。Web 管理ツールまたは別のアプリケーションを使用して、os400-usrprf objectclass および関連した os400-xxx 属性の定義を表示します。

## プロジェクト・ユーザーへの読み取りアクセス

- | デフォルトでは、LDAP 検索および比較操作を介したユーザー・プロファイル情報への読み取りアクセス
- | が、許可ユーザーに対してシステム射影バックエンドから提供されます。プロジェクト・ユーザーへの読み
- | 取りアクセスを有効化または無効化するには、System i Navigator を使用するか、または
- | /QIBM/UserData/OS400/DirSrv/idsslapd-instance/etc/ibmslapd.conf ファイル (デフォルト・サーバー・インスタ
- | ンス用の /QIBM/UserData/OS400/DirSrv/idsslapd-QUSRDIR/etc/ibmslapd.conf ファイル) 内での構成設定を介
- | します。
  
- | ユーザー・プロファイル情報への読み取りアクセスを無効にするには、次のようなステップを行います。
- | 1. System i Navigator で「ネットワーク」を展開する。
- | 2. 「サーバー」>「TCP/IP」を展開する。
- | 3. 「IBM Tivoli Directory Server」を右マウス・ボタン・クリックし、「プロパティ」を選択する。

- | 4. 「Database/Suffixes (データベース/接尾部)」タブを選択する。
- | 5. 「Allow read access to user information (ユーザー情報への読み取りアクセスを許可する)」チェック・ボックスのチェック・マークを外す。

| 構成ファイルの cn=Front End, cn=Configuration スタンザ内の以下の行を変更し、ユーザー・プロジェクト・バックエンドに対する検索および比較操作を無効にすることができます。

| ibm-slapdOs400UsrprjRead: TRUE

| 読み取りアクセスを無効にするには、値を TRUE から FALSE に変更します。値が TRUE であるか、または構成ファイル内にこの設定がない場合、プロジェクト・ユーザー情報への読み取りアクセスは有効になります。

#### 関連タスク

144 ページの『プロジェクト・ユーザーへの読み取りアクセスの有効化または無効化』

以下の情報を参考にして、ユーザー・プロジェクト・バックエンドに対する検索および比較操作を禁止します。

#### 関連資料

96 ページの『LDAP 操作』

プロジェクト・バックエンドに対してどの LDAP 操作を実行できるかの理解。

## Directory Server および i5/OS ジャーナリングのサポート

Directory Server は、i5/OS データベース・サポートを使用して、ディレクトリー情報を保管します。

Directory Server は、コミットメント制御を使用してディレクトリー項目をデータベースに保管します。これには、i5/OS ジャーナル・サポートが必要です。

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あるかもしれません。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、コマンド行から以下を実行します。

```
CHGJRN 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古いジャーナル・レシーバーを削除できます。

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

#### 関連情報

ジャーナル変更 (CHGJRN)

## 固有属性

固有属性の機能により、指定された属性はディレクトリー内で常に固有な値をもつようにすることができます。

これらの属性を指定できるのは、`cn=uniqueattribute,cn=localhost` と `cn=uniqueattribute,cn=IBMpolicies` の 2 つのみの項目に対してです。固有属性の検索結果は、そのサーバーのデータベースでのみ固有となります。参照による結果を含む検索結果では固有でないことがあります。

注: 2 進数属性、操作属性、構成属性、および `objectclass` 属性は固有として指定できません。

すべての属性を固有として指定できるわけではありません。属性を固有として指定できるかどうかを判別するには、`ldapexop` コマンドを使用してください。

- 固有にできる属性: `ldapexop -op getattributes -attrType unique -matches true`
- 固有にできない属性: `ldapexop -op getattributes -attrType unique -matches false`

### 関連概念

158 ページの『固有属性タスク』

以下の情報を参考にして、固有属性を管理します。

## 操作属性

Directory Server に対して特殊な意味を持つ、操作属性という幾つかの属性があります。これらは、サーバーによって保守される属性であり、サーバーがある 1 つの項目について管理している情報を反映するか、またはサーバーの動作に影響を及ぼします。

これらの属性には、以下のような特殊な特性があります。

- これらの属性は、検索要求時に (名前で) 具体的に要求しない限り、検索操作では戻りません。
- これらの属性はオブジェクト・クラスの一部ではありません。サーバーは、どの項目にこれらの属性が保管されるかを制御します。

次の操作属性セットは、Directory Server でサポートされる操作属性の一部です。

- `creatorsName`、`createTimestamp`、`modifiersName`、`modifyTimestamp` は、すべての項目上にあります。これらの属性は、バインド DN に加えて、項目が最初に作成された時刻または最後に変更された日時を表示します。これらの属性を検索フィルターで使用し、たとえば、指定した時刻以降に変更されたすべての項目を検索できます。これらの属性はどのユーザーも変更できません。これらの属性はコンシューマー・サーバーに複製されて、LDIF ファイル内でのインポートとエクスポートが行われます。
- `ibm-entryuuid`。サーバーが V5R3 以降である場合に作成されるすべての項目に存在します。この属性は、項目が作成される時にサーバーにより各項目に割り当てられる汎用固有ストリング ID です。これは、さまざまなサーバー上の同一名の項目間で区別をする必要があるアプリケーションでは便利です。属性は DCE UUID アルゴリズムを使用し、タイム・スタンプ、アダプター・アドレス、および他の情報を使用して、すべてのサーバー上のすべての項目にわたり固有の ID を生成します。
- `entryowner`、`ownersource`、`ownerpropagate`、`aclentry`、`aclsource`、`aclpropagate`、`ibm-filteracl`、`ibm-filteraclinherit`、`ibm-effectiveAcl`。
- `hasSubordinates`。すべての項目に存在し、項目が従属項目を持つ場合に値 `TRUE` を持ちます。
- `numSubordinates`。すべての項目に存在し、この項目の子である項目の数を含んでいます。
- `pwdChangedTime`、`pwdAccountLockedTime`、`pwdExpirationWarned`、`pwdFailureTime`、`pwdGraceUseTime`、`pwdReset`、`pwdHistory`。

- subschemasubentry - すべての項目に存在し、ツリーのその部分のためのスキーマの場所を示します。これは、ツリーのその部分で使用するスキーマを検出したい場合、複数のスキーマを持つサーバーの場合に便利です。

操作属性の完全なリストについては、拡張操作 `ldapexop -op getattributes -attrType operational -matches true` を使用してください。

#### 関連概念

4 ページの『ディレクトリー』

Directory Server は、i5/OS 統合ファイル・システムの編成に類似した方法で情報を階層構造に保管するタイプのデータベースへのアクセスを許可します。

72 ページの『アクセス制御リスト』

アクセス制御リスト (ACL) を使用すると、LDAP ディレクトリーに保管された情報を保護することができます。管理者は ACL を使用して、ディレクトリーのさまざまな部分へのアクセスや、特定のディレクトリー項目へのアクセスを制限します。

86 ページの『パスワード・ポリシー』

認証に LDAP サーバーの使用においては、LDAP サーバーがパスワードの有効期限、失敗したログイン試行、およびパスワード規則に関するポリシーをサポートすることが重要です。Directory Server では、この種のポリシー 3 つすべてを構成できます。

## サーバー・キャッシュ

LDAP キャッシュは、将来の利用のために照会、応答、およびユーザー認証などの LDAP 情報の保管に使用されるメモリー内の高速記憶域バッファです。LDAP キャッシュのチューニングはパフォーマンスの向上のために重要です。

LDAP キャッシュにアクセスする LDAP 検索は、情報が DB2<sup>®</sup> でキャッシュされる場合でも、DB2 への接続を必要とするケースより高速です。このために、LDAP キャッシュをチューニングすると、データベースの呼び出しを回避してパフォーマンスの向上が達成できます。反復されるキャッシュ情報を頻繁に検索するアプリケーションでは、LDAP キャッシュは特に有用です。

次の項では、それぞれの LDAP キャッシュについて説明し、ユーザー・システムに最適なキャッシュの判別および設定方法が示されています。

#### 関連概念

160 ページの『パフォーマンス・タスク』

以下の情報を参考にして、パフォーマンスの設定値を調整します。

## 属性キャッシュ

属性キャッシュには、データベース内ではなく、メモリー内でフィルターを解決できる利点があります。また、LDAP add、delete、modify、または modrdn 操作を実行する時に毎回更新されるという利点もあります。

メモリー内に保管したい属性を決定する時には、以下を考慮する必要があります。

- サーバーで使用可能になるメモリー容量
- ディレクトリーのサイズ
- アプリケーションで代表的に使用する検索フィルターのタイプ

注: 属性キャッシュ・マネージャーは次の簡易フィルターを解決できます。すなわち、完全一致フィルターと存在フィルターです。また、結合または非結合の複雑なフィルターも解決できますが、サブフィルターは完全一致、存在、結合または非結合でなければなりません。

すべての属性を属性キャッシュに追加できるわけではありません。その属性がキャッシュに追加できるかどうかを判別するには、`ldapexop` コマンドを使用してください。

- 追加できる属性: `ldapexop -op getattributes -attrType attribute_cache -matches true`
- 追加できない属性: `ldapexop -op getattributes -attrType attribute_cache -matches false`

属性キャッシュは次の 2 つの方法、すなわち、手動または自動で構成することができます。属性キャッシュを手動で構成するには、管理者は `cn=monitor` 検索を実行して、最も効果的な属性キャッシュの作成方法を理解する必要があります。これらの検索では、キャッシュされる属性、各属性キャッシュで使用されるメモリー容量、属性キャッシュで使用されるメモリー容量の合計、属性キャッシュで構成されるメモリー容量、および検索フィルターで最も頻繁に使用される属性リストをリストした最新情報が戻されます。この情報を使用して、管理者は、属性キャッシュで使用するメモリー容量を変更でき、また、新規の `cn=monitor` 検索に基づいて、必要な時はいつでもキャッシュする属性も変更できます。

また、管理者は自動属性キャッシュを構成することができます。自動属性キャッシュが使用可能な時は、Directory Server は管理者によって定義されたメモリー制限内でキャッシュに最適な属性の組み合わせをトラックします。次に、管理者によって構成された時間と時間間隔で属性キャッシュを更新します。

## フィルター・キャッシュ

クライアントがデータの照会を出し、属性キャッシュ・マネージャーがメモリー内でその照会を解決できない時には、その照会はフィルター・キャッシュに進みます。このキャッシュには、キャッシュされた項目 ID が入っています。

フィルター・キャッシュに照会が到着すると、次の 2 つのことが起こります。

- 照会で使用されたフィルター設定と一致する ID はフィルター・キャッシュに配置されます。この場合は、一致した項目 ID のリストが項目キャッシュに送られます。
- 一致した項目 ID はフィルター・キャッシュ内にはキャッシュされません。この場合、必要なデータを検索する際に、DB2 へのアクセスが照会で必要となります。

フィルター・キャッシュをどんなサイズにするかを判別するには、フィルター・キャッシュを別の値に設定してワークロードを実行し、秒当たりの演算数の違いを測定してください。

フィルター・キャッシュ・バイパス制限構成変数では、フィルター・キャッシュに追加できる項目数が制限されます。例えば、迂回制限変数が 1,000 に設定されると、該当する項目が 1,000 件を超える検索フィルターはフィルター・キャッシュに追加されません。これで、異常に大きな検索によって有用なキャッシュ項目が上書きされるのを回避します。ワークロードに最適なフィルター・キャッシュ・バイパス制限を判別するには、そのワークロードを反復実行して、スループットを測定してください。

## 項目キャッシュ

項目キャッシュには、キャッシュされた項目データが入っています。項目 ID は項目キャッシュに送られます。

項目 ID と一致した項目が項目キャッシュ中にあると、その結果がクライアントに戻されます。項目 ID と一致する項目が項目キャッシュに含まれていない場合、一致する項目を検索するために、照会は DB2 に進みます。

項目キャッシュをどんなサイズにするかを判別するには、項目キャッシュを別のサイズに設定してワークロードを実行し、秒当たりの演算数の違いを測定してください。

## ACL キャッシュ

ACL キャッシュには、項目所有者および最近アクセスされた項目の項目アクセス権などのアクセス制御情報が入っています。このキャッシュを使用して、項目を追加、削除、変更、または検索するためのアクセスの評価パフォーマンスを向上させます。

項目が ACL キャッシュ内で見つからない場合、アクセス制御情報をデータベースから検索します。適切な ACL キャッシュ・サイズを判別するには、代表的なワークロードを各種の ACL キャッシュ・サイズで使用し、サーバーのパフォーマンスを測定してください。

## 制御および拡張操作

制御操作と拡張操作では、プロトコルそのものを変更しなくても、LDAP プロトコルを拡張することができます。

### 制御

制御は、サーバーが特定の要求をどのように解釈するかを制御するための追加情報をサーバーに知らせます。たとえば、delete subtree 制御を LDAP 削除要求で指定すると、サーバーは指定した項目だけ削除するのではなく、項目およびそのすべての従属項目を削除します。制御は、以下の 3 つの部分から構成されます。

- 制御タイプ。これは制御を識別する OID です。
- 重大性 (criticality) 標識。これは、サーバーが制御をサポートしていない場合の動作方法を指定します。これは、ブール値です。FALSE は制御が重大でないことを示し、サーバーが制御をサポートしていない場合にはそれを無視します。TRUE は、制御が重大であることを示し、サーバーが制御を行えない場合には要求全体は失敗します (サポートされない重大な拡張機能エラーが出されます)。
- オプションの制御値。これは、制御に特有のその他の情報を含みます。制御値の内容は、ASN.1 表記を使用して指定されます。値そのものは制御データの BER エンコード方式です。

### 拡張操作

拡張操作は、コアとなる LDAP 操作を超えた追加操作を開始するために使用されます。たとえば、拡張操作は、操作のセットを単一ランザクションにグループ化するために定義されています。拡張操作は以下で構成されます。

- 特定の操作を識別する要求名、OID。
- オプションの要求値。これは、要求に特有のその他の情報を含みます。要求値の内容は、ASN.1 表記を使用して指定されます。値そのものは要求データの BER エンコード方式です。

拡張操作には、通常拡張応答があります。応答は以下で構成されます。

- 標準 LDAP 結果のコンポーネント (エラー・コード、一致した DN、およびエラー・メッセージ)
- 応答のタイプを識別する応答名、OID。
- オプションの値。これは、応答に特有のその他の情報を含みます。応答値の内容は、ASN.1 表記を使用して指定されます。値そのものは応答データの BER エンコード方式です。

#### 関連概念

10 ページの『識別名 (DN)』

ディレクトリー内のすべての項目には、識別名 (DN) があります。DN は、ディレクトリー内の項目を一意的に識別する名前です。DN の最初のコンポーネントは、相対識別名 (RDN) と呼ばれています。

#### 関連資料

326 ページの『オブジェクト ID (OID)』

以下の情報では、Directory Server で使用されるオブジェクト ID (OID) について述べています。

## 保存と復元に関する考慮事項

Directory Server は、データと構成情報を複数のロケーションに保管します。

Directory Server は、次のようなロケーションに情報を保管します。

- 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)。

注: System i Navigatorの「IBM Directory Server Properties」パネルの「データベース/接尾部」タブ上に、使用中のデータベース・ライブラリーを表示することができます。

- QDIRSRV2 ライブラリー。公開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。

#### 関連情報

バックアップおよび回復

---

## Directory Server の概要

Directory Server のインストール、マイグレーション、計画、カスタマイズ、および管理の概要について述べます。

Directory Server は、i5/OS をインストールすると自動的にインストールされます。Directory Server には、デフォルトの構成が組み込まれています。Directory Server を開始するときは、以下を参照してください。

## マイグレーションの考慮事項

V5R4 をインストールしようとしており、前のリリースの Directory Server を使用していた場合には、マイグレーションの考慮事項を検討する。

Directory Server は、i5/OS をインストールすると自動的にインストールされます。最初にサーバーが開始される時、既存の構成およびデータすべては自動的にマイグレーションされます。このため、最初にサーバーが開始する前に、長い遅延が発生する可能性があります。



注: 構成およびスキーマ・ファイルのマイグレーションは、インストール時および最初のサーバー開始時に行われます。最初のサーバー始動が完了し、/qibm/userdata/os400/dirsrv 中の構成およびスキーマ・ファイルが前のリリースのバックアップから復元されると、新規リリースのスキーマおよび構成が前のリリースのファイルにオーバーレイされます。また、これは再びマイグレーションされることはありません。マイグレーションの実行後に、前のリリースのスキーマおよび構成を復元すると、サーバーが開始されないで、予測できないエラーの原因になることがあります。サーバー構成およびスキーマのバックアップが必要な場合は、サーバーを正常に開始した後で、このデータを保管する必要があります。

## V5R4 または V5R3 からの V6R1 へのマイグレーション

- | V5R4 または V5R3 で稼働する Directory Server を使用する場合、以下の情報を参考にしてください。
- | i5/OS V6R1 では、Directory Server に新しい機能が追加されました。これらの変更は、LDAP ディレクトリー・サーバーと System i Navigatorのグラフィカル・ユーザー・インターフェース (GUI) の両方に影響します。GUI の新しい機能を利用できるようにするには、TCP/IP を使用して iSeries サーバー に接続できる PC に System i Navigatorをインストールする必要があります。System i Navigatorは、System i Access for Windows のコンポーネントです。旧バージョンの System i Navigatorをインストールしてある場合は、V6R1 にアップグレードするようにしてください。
- | i5/OS V6R1 は、V5R4 および V5R3 からの直接のアップグレードをサポートします。Directory Server は、最初の開始時に V6R1 にアップグレードされます。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、V6R1 のフォーマットに準拠するように自動的にマイグレーションされます。
- | i5/OS V6R1 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幾つかの注意点があります。
  - | • V6R1 にアップグレードして、Directory Server を開始すると、Directory Server によってスキーマ・ファイルが自動的に V6R1 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していた場合、Directory Server 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 Directory Server 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。
  - | • V6R1 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、まず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。Directory Server を初めて開始するかまたは LDIF ファイルをインポートすると、Directory Server によってディレクトリー・データは V6R1 フォーマットにマイグレーションされます。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。
  - | • V6R1 では、i5/OS システム上に複数の Directory Server インスタンスを設ける機能が導入されています。V6R1 へのアップグレードの前に Directory Server を使用していた場合、その Directory Server は 1 つのインスタンスにマイグレーションされます。その一環として、構成ファイルとスキーマ・ファイルが /QIBM/UserData/OS400/DirSrv ディレクトリーから /QIBM/UserData/OS400/DirSrv/idslapd-QUSRDIR ディレクトリーに移動されます。これは、デフォルトの Directory Server インスタンスと呼ばれ、QUSRDIR インスタンスという名前が付けられます。また、QUSRSYS ライブラリー内の 2 つのオブジェクトが新規ライブラリー QUSRDIRCF に移動されます。このマイグレーションが行われるのは、V6R1 へのアップグレード後の Directory Server の最初の開始時点です。
  - | • 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、System i Navigatorを使用して、設定を変更してください。

## V4R4、V4R5、V5R1、または V5R2 から V6R1 へのデータのマイグレーション

V4R4、V4R5、または V5R1 で稼働する Directory Server を使用する場合は、以下の情報を参考にしてください。

i5/OS V5R4 では、V4R4、V4R5 または V5R1 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。

注: V4R4 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。

- V4R4 およびそれ以前のリリースの Directory Server では、タイム・スタンプの項目を作成するときに、時間帯は考慮に入れられませんでした。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 以前のデータをアップグレードすると、Directory Server によって既存の createtimestamp および modifytimestamp 属性は、正しい時間帯を反映するように調整されます。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、システム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。
- V4R4 以前のリリースからのデータをアップグレードする場合は、ディレクトリー・データが、以前のほぼ 2 倍のストレージ・スペース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 Directory Server 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) でデータが保存されていたためです。Directory Server 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きます。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。

これらのリリースを V5R4 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。

### V4R4、V4R5 または V5R1 から暫定リリースへのアップグレード:

- 1 Directory Server をマイグレーションして、まず暫定リリース (V5R2 または V5R3) にアップグレードしてから、V6R1 にアップグレードすることができます。
- 1 V4R4、V4R5、V5R1、および V5R2 から V6R1 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。
  - 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
  - V5R1 および V5R2 から V5R3 へのアップグレード
  - V5R2 および V5R3 から V5R4 へのアップグレード
- 1 • V5R3 および V5R4 から V6R1 へのアップグレード

i5/OS のインストール手順の詳細は、i5/OS とその関連ソフトウェアのインストール、アップグレード、または削除を参照してください。以下のステップに従って、マイグレーションを実行してください。スキーマの変更は自動的にマイグレーションされるはずですが、それぞれをインストールした後、スキーマ変更がまだあることを確認してください。

1. V4R4 では、V5R1 のインストールを行う。次に、V5R3 をインストールします。
- 1 2. V4R5 では、V5R1 または V5R2 のインストールを行う。V5R1 にインストールしている場合は、次に V5R3 にインストールする必要があります。V5R2 にインストールしている場合は、次に V5R3 または V5R4 にインストールする必要があります。

3. V5R1 では、V5R3 のインストールを行う。
4. V5R2 の場合、V5R3 または V5R4 のインストールを行う。
5. V5R3 または V5R4 になったら、V6R1 のインストールを行う。
6. Directory Server をまだ開始していなければ、ここで開始する。

#### データベース・ライブラリーの保存と V6R1 のインストール:

Directory Server が V4R4 または V4R5 で使用するデータベース・ライブラリーを保存し、V6R1 のインストール後にそれを復元することにより、Directory Server をマイグレーションできます。

この方法では、暫定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ため、サーバーを再構成する必要があります。i5/OS のインストール手順の詳細は、i5/OS とその関連ソフトウェアのインストール、アップグレード、または削除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ため、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。LDIF ファイルを `ldapmodify` ユーティリティと組み合わせて使用してスキーマ更新を実行した場合は、新規のリリースでサーバーを実行した後でこれらのファイルを使用できるように、そのファイルを位置指定してください。Directory Management Tool または Web 管理ツール (別の V6R1 システムで実行している) を使用して、個別の属性タイプおよびオブジェクト・クラス定義を表示することができます。その変更が新規の属性タイプと `objectclasses` の追加のみである場合は、ファイル `/qibm/userdata/os400/dirsrv/v3.modifiedschema` のコピーを作成してください。このファイルを使用して、スキーマ更新が含まれている LDIF ファイルを構成することができます。詳しくは、16 ページの『スキーマ』を参照してください。
2. Directory Server のプロパティで、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. Directory Server 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。変更ログを構成した場合には、QUSRDIRCL ライブラリーも保管する必要があります。
4. 公開機能の構成を記録する。公開する構成は、パスワード情報を除いて System i Navigator を使用して表示できます。このナビゲーターでは、システムの「プロパティ」を選択し、「ディレクトリー・サービス」タブをクリックします。
5. i5/OS V6R1 をシステムにインストールする。
6. System i Navigator のウィザードを使用して、Directory Server 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。ステップ 3で QUSRDIRCL ライブラリーを保管した場合、それをここで復元する。
8. System i Navigator を使用して、Directory Server の設定をやり直す。前に構成済みで前のステップで保管、復元されたデータベース・ライブラリーを指定する。
9. System i Navigator を使用して、公開機能を再構成する。
10. Directory Server を再始動する。
11. Web 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。

#### 複製サーバーのネットワークのマイグレーション

複製サーバーのネットワークを使用する場合、以下の情報を参考にしてください。

マスター・サーバーが初めて開始される時、複製を制御するディレクトリー内の情報がマイグレーションされます。cn=localhost の下に objectclass replicaObject を持つ項目は、新規複製モデルにより使用される項目に置換されます。マスター・サーバーは、ディレクトリー内のすべての接尾部を複製するように構成されています。合意項目は、属性 ibm-replicationOnHold を true にして作成されます。これにより、マスターに対して行われる更新は、レプリカの準備ができるまでレプリカ作成用に累積されるようになります。

これらの項目は、複製トポロジーと呼ばれます。新規マスターは、前のバージョンで実行されるレプリカで使うことができます。新機能に関連したデータは、バックレベル・サーバーには複製されません。複製トポロジー項目をマスターからエクスポートし、レプリカ・サーバーのマイグレーションの後にそれらを各レプリカに追加することが必要です。項目をエクスポートするには、Qshell コマンド行ツール 265 ページの『ldapsearch』を使用し、出力をファイルに保管します。検索コマンドは以下のような形式です。

```
ldapsearch -h master-server-host-name -p master-server-port ¥
-D master-server-admin-DN -w master-server-admin-password ¥
-b ibm-replicagroup=default,suffix-entry-DN ¥
-L "(|(objectclass=ibm-replicaSubEntry)(objectclass=ibm-replicationAgreement))" ¥
 > replication.topology.ldif
```

このコマンドにより、現行作業ディレクトリーに replication.topology.ldif という名前の出力 LDIF ファイルが作成されます。そのファイルには、新規項目のみが含まれています。

注: 以下の接尾部は含めないでください。

- cn=changelog
- cn=localhost
- cn=pwdpolicy
- cn=schema
- cn=configuration

ユーザーが作成した接尾部のみを含めてください。

マスター上の接尾部項目ごとにこのコマンドを繰り返します。ただし、「>」を「>>」に置き換えて以降の検索においてデータを出力ファイルに追加します。ファイルの完了後、それをレプリカ・サーバーにコピーします。

正常にマイグレーションが完了した後、ファイルをレプリカ・サーバーに追加します。ディレクトリー・サーバーの前のバージョンを実行するサーバーにはファイルを追加しないでください。ファイルを追加する前にサーバーを開始および停止する必要があります。

サーバーを開始するには、System i Navigatorの「開始」オプションを使用します。

サーバーを停止するには、System i Navigatorの「停止」オプションを使用します。

ファイルをレプリカ・サーバーに追加する時、レプリカ・サーバーが開始されていないことを確認してください。データを追加するには、System i Navigatorの「ファイルのインポート」オプションを使用します。

複製トポロジー項目をロードした後、レプリカ・サーバーを開始し、複製を再開します。以下のいずれかの方法により、複製を再開できます。

- マスター・サーバー上で、Web 管理ツールの「複製管理内のキューの管理 (Manage Queues in Replication Management)」を使用する。
- **ldapexop** コマンド行ユーティリティーを使用する。以下に例を示します。

```
ldapexop -h master-server-host-name -p master-server-port ¥
-D master-server-admin-DN -w master-server-admin-password ¥
-op controlrepl -action resume -ra replica-agreement-DN
```

このコマンドにより、指定した DN を持つ項目内で定義されたサーバーの複製を再開します。

どのレプリカ合意 DN がレプリカ・サーバーに対応するかを判別するために、`replication.topology.ldif` ファイルを調べます。マスター・サーバーは、複製がそのレプリカ用に開始されたというメッセージと、合意内のレプリカ・サーバーの ID がレプリカ・サーバー ID と一致しないという警告をログに記録します。レプリカ合意が正しいサーバー ID を使用するように更新するには、Web 管理ツールの「複製管理 (Replication Management)」またはコマンド行ツール `ldapmodify` を使用します。たとえば次のようになります。

```
ldapmodify -c -h master-server-host-name -p master-server-port ¥
-D master-server-admin-DN -w master-server-admin-password
dn: replica-agreement-DN
changetype: modify
replace: ibm-replicaConsumerID
ibm-replicaConsumerID: replica-server-ID
```

これらのコマンドをコマンド行で直接入力するか、コマンドを LDIF ファイル内に保管し、それらを `-i file` オプションを付けてコマンドに渡します。コマンドを停止するには、「直前の要求の終了 (End Previous Request)」を使用します。

このレプリカのマイグレーションは完了します。

前のバージョンで実行されるレプリカを使用するには、コマンド行ツール `ldapexop` または Web 管理ツールの「複製管理 (Replication Management)」を使用して複製を再開することが必要です。前のバージョンで実行されるレプリカを後でマイグレーションする場合、コマンド行ツール `ldapdiff` を使用してディレクトリー・データを同期化します。これにより、複製されていない項目または属性が確実にレプリカで更新されます。

#### 関連概念

42 ページの『複製』

複製は、パフォーマンスおよび信頼性を向上させるためにディレクトリー・サーバーで使用される技法です。複製プロセスにより、複数のディレクトリー内のデータが同期化された状態を保ちます。

#### 関連タスク

130 ページの『Directory Server の開始』

以下の情報を参考にして、Directory Server を開始します。

## Kerberos サービス名の変更

V5R3 より前の Kerberos を使用する場合は、以下の情報を参考してください。

V5R3 からは、GSSAPI 認証 (Kerberos) 用にディレクトリー・サーバーおよびクライアント API により使用されるサービス名が変更されています。この変更は、V5R3 より前に使用されていたサービス名とは非互換です (V5R2M0 PTF 5722SS1-SI08487 には同じ変更が行われています)。

V5R3 の前に、ディレクトリー・サーバーおよびクライアント API は、認証に GSSAPI メカニズム (Kerberos) が使用されるときに `LDAP/dns-host-name@Kerberos-realm` 形式のサービス名を使用していました。この名前は、プリンシパル名は小文字の「ldap」で始まらなければならないと規定している GSSAPI 認証を定義する規格に準拠していません。結果として、ディレクトリー・サーバーとクライアント API の両方は、他のベンダーの製品と相互運用できない可能性があります。これは、Kerberos 鍵配布センター (KDC) が大/小文字の区別をするプリンシパル名を持っているときには特にそういえます。JNDI 用の

LDAP サービス・プロバイダーで、通常使用されている Java LDAP クライアント API は、正しいサービス名を使用するオペレーティング・システムに含まれているクライアントの例です。

V5R3M0 では、サービス名を規格に準拠するように変更してあります。ところが、これにより、それ自体の互換性問題をもたらしました。

- GSSAPI 認証を使用するように構成されたディレクトリー・サーバーは、このリリースのインストールを開始しません。これは、サーバーは新しいサービス名 (ldap/mysys.ibm.com@IBM.COM) を使用する信任状を探しているのに、サーバーにより使用される keytab ファイルが古いサービス名 (LDAP/mysys.ibm.com@IBM.COM) を使用する信任状を持っているためです。
- V5R3M0 で LDAP API を使用するディレクトリー・サーバーまたは LDAP アプリケーションは、古い OS/400<sup>®</sup> サーバーまたはクライアントに認証できない可能性があります。これを訂正するには、以下のようになります。
  1. KDC が大/小文字の区別をするプリンシパル名を使用している場合、正しいサービス名 (ldap/mysys.ibm.com@IBM.COM) を使用するアカウントを作成する。
  2. Directory Server が使用する keytab ファイルを更新し、新しいサービス名用の信任状を含むようにする。古い信任状を削除することもできます。Qshell keytab ユーティリティを使用して、keytab ファイルを更新できます。デフォルトでは、ディレクトリー・サーバーは /QIBM/UserData/OS/400/NetworkAuthentication/keytab/krb5.keytab ファイルを使用します。System i Navigatorの「V5R3M0 Network Authentication Service (Kerberos) ウィザード (V5R3M0 Network Authentication Service (Kerberos) wizard)」でも、新しいサービス名を使用して keytab 項目を作成できます。
  3. PTF 5722SS1-SI08487 を適用することにより GSSAPI が使用される V5R2M0 OS/400 システムを更新する。

代わりに、ディレクトリー・サーバーとクライアント API が古いサービス名を使用し続けるように選択することもできます。PTF で実行される場合もそうでない場合も、システムの混合ネットワークにおいて Kerberos 認証を使用しているときは、この方法が望ましいと言えます。そのためには、LDAP\_KRB\_SERVICE\_NAME 環境変数を設定します。以下のコマンドを使用して、(サーバー用にサービス名を設定する必要がある) システム全体に対してこれを設定できます。

```
ADDENVVAR ENVVAR(LDAP_KRB_SERVICE_NAME)
```

あるいは、QSH で以下のように設定します (この QSH セッションから実行される LDAP ユーティリティを対象にするため)。

```
export LDAP_KRB_SERVICE_NAME=1
```

## Directory Server の計画

Directory Server の構成と LDAP ディレクトリーの作成を開始する前に、前もってディレクトリーの計画を立ててください。

Directory Server の構成と LDAP ディレクトリーの作成を開始する前に、以下の点を検討してください。

- **ディレクトリーを編成する。**ディレクトリー構造の計画を立て、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。詳細は、『ディレクトリー構造の推奨される措置』のディレクトリー、接尾部、および属性のトピックを参照してください。
- **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 Directory Server のスキーマを使用する空のディレクトリーには、約 10MB のストレージ・スペースが必要です。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 のストレージ・スペースが必要です。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・サーバーは、ユーザーが自分のパスワードを周期的に変更しパスワードが組織の構文パスワード要件を満たせるように、パスワード・ポリシーを適用することを可能にします。

Directory Server は、Secure Sockets Layer (SSL) とデジタル認証、および Transport 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。Kerberos 認証もサポートされています。

Directory Server 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、オペレーティング・システムのセキュリティー監査も使用できます。

さらに、適用するパスワード・ポリシーを決定します。

- **管理者 DN とパスワードを選択する。** デフォルトの管理者 DN は cn=admin です。これは、サーバーが初期構成されるときにディレクトリー項目を作成または変更する権限がある唯一の ID です。デフォルトの管理者 DN を使用するか、異なる DN を選択することができます。管理者 DN のパスワードも作成する必要があります。
- **Directory Server Web 管理ツールの前提条件ソフトウェアをインストールする。** Directory Server Web 管理ツールを使用するためには、以下の前提条件製品がインストール済みである必要があります。
  - IBM HTTP Server for i5/OS (5761-DG1)
  - IBM WebSphere Application Server 6.0 (5733-W60 Base または Express オプション)
- **バックアップおよびリカバリー・ストラテジーの計画。** データおよび構成情報の保存方法の計画をたてます。

### 関連概念

38 ページの『ディレクトリー構造の推奨される措置』

Directory Server はユーザーおよびグループのリポジトリとして使用されることがあります。この項では、ユーザーおよびグループの管理を最適化する構成をセットアップするための推奨事項を説明します。この構成および関連のセキュリティーのモデルは、ディレクトリーの他の用途に拡張することができます。

4 ページの『ディレクトリー』

Directory Server は、i5/OS 統合ファイル・システムの編成に類似した方法で情報を階層構造に保管するタイプのデータベースへのアクセスを許可します。

14 ページの『接尾部 (命名コンテキスト)』

接尾部 (命名コンテキストともいいます) は、ローカルに保持されるディレクトリー階層の最上部の項目を識別する DN です。

20 ページの『属性』

各ディレクトリー項目には、そのオブジェクト・クラスを介して関連付けられた属性のセットがあります。

106 ページの『保存と復元に関する考慮事項』

Directory Server は、データと構成情報を複数のロケーションに保管します。

## 関連情報

### IBM HTTP Server

IBM HTTP Server および IBM WebSphere Application Server についての詳細は、IBM HTTP Server トピックを参照してください。

## Directory Server の構成

Directory Server の設定をカスタマイズするには、「Directory Server Configuration (Directory Server の構成)」ウィザードを実行します。

1. システムが別の LDAP サーバーに情報を公開するような構成になっておらず、しかも 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、Directory Server が限定付きのデフォルト構成で自動的にインストールされます。Directory Server には、それぞれの必要に合わせて Directory Server を構成するためのウィザードが用意されています。後でこのウィザードを System i Navigator から実行することができます。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、また、ディレクトリー・サーバーを再構成するときにもこのウィザードを使用することができます。

**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となります。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」を右マウス・ボタン・クリックして、「プロパティ」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。セキュリティ監査を設定する場合は、\*AUDIT 特殊権限も必要になります。

2. 「Directory Server Configuration (Directory Server 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。
  - a. System i Navigatorで「ネットワーク」を展開する。
  - b. 「サーバー」を展開する。
  - c. 「TCP/IP」をクリックする。
  - d. 「IBM Directory Server」を右マウス・ボタン・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。

3. 「Directory Server の構成ウィザード」の指示に従って、Directory Server 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、それは失敗します。



4. ウィザードが終了すると、Directory Server 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。詳細は、E メールの特ピックの中の同一システム上で Domino LDAP とディレクトリー・サーバーをホストするを参照してください。
  - Directory Server が使用するポートを変更する。詳しくは、138 ページの『ポートまたは IP アドレスの変更』を参照してください。
  - 特定の IP アドレスを使用する。詳しくは、138 ページの『ポートまたは IP アドレスの変更』を参照してください。
5. 構成した接尾部 (複数可) に対応する項目を作成します。詳細については 139 ページの『Directory Server 接尾部の追加および除去』を参照してください。
6. 続ける前に、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。
  - Secure Sockets Layer (SSL) セキュリティーを使用可能にする。203 ページの『Directory Server での SSL と Transport Layer Security の使用可能化』を参照してください。
  - Kerberos 認証を使用可能にする。205 ページの『Directory Server での Kerberos 認証の使用可能化』を参照してください。
  - 参照をセットアップする。138 ページの『ディレクトリー参照用のサーバーの指定』を参照してください。
7. Directory Server を始動する。詳細については 130 ページの『Directory Server の開始』を参照してください。
8. 既存の Directory Server インスタンスは、QUSRDIR インスタンスと呼ばれます。そのスキーマ・ファイルと構成ファイルは、/QIBM/UserData/OS400/DirSrv/idsslapd-QUSRDIR ディレクトリー内にあります。デフォルト・インスタンスの開始を試みれば、サーバー・インスタンスを自動的に作成することができます。他のインスタンスはいずれも、自動的に作成されません。

#### 関連概念

336 ページの『Directory Server のデフォルト構成』

Directory Server は、i5/OS 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。

## ディレクトリーへのデータの取り込み

ディレクトリーにデータを取り込みます。

ディレクトリーにデータを取り込む方法はいくつかあります。

- Directory Server への情報の公開
- LDIF ファイルからのデータのインポート
- HTTP サーバー妥当性検査リストから Directory Server へのユーザーのコピー

#### 関連タスク

145 ページの『Directory Server への情報の公開』

以下の情報を参考にして、Directory Server へ情報を公開します。

147 ページの『LDIF ファイルのインポート』

以下の情報を参考にして、LDAP データ交換形式 (LDIF) ファイルをインポートします。

149 ページの『HTTP サーバー妥当性検査リストから Directory Server へのユーザーのコピー』

以下の情報を参考にして、HTTP サーバー妥当性検査リストから Directory Server へユーザーをコピーします。

## Web 管理

Directory Server を管理するには、Web 管理コンソールをセットアップして使用します。

Web 管理コンソールを使用して、1 つ以上の Directory Servers を管理できます。Web 管理コンソールにより、以下のことが可能になります。

- 管理できる Directory Server のリストを追加または変更する。
- Web 管理ツールを使用して Directory Server を管理する。
- Web 管理コンソールの属性を変更する。

Web 管理コンソールを使用するには、以下のことを行ってください。

1. 初めて Directory Server Web 管理を使用する場合、最初に Web 管理をセットアップする必要があり (117 ページの『Web 管理の初めてのセットアップ』を参照してください)、その後次のステップを続ける。
2. 以下のうちのいずれかを行って Directory Server Web 管理にログインする。
  - System i Navigatorから、サーバーを選択し、「ネットワーク」→「サーバー」→「TCP/IP」をクリックし、「IBM Directory Server」を右クリックし、「サーバー管理 (Server Administration)」をクリックする。
  - 「iSeries Tasks (iSeries タスク)」ページ ([http://your\\_server:2001](http://your_server:2001)) から、「IBM Directory Server」をクリックする。
3. Directory Server を管理するには、以下のようにします。
  - a. 「LDAP ホスト名」フィールドで管理したい Directory Server を選択する。
  - b. 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管理者ログイン DN を入力する。
  - c. 管理者パスワードを入力する。
  - d. 「Login (ログイン)」をクリックする。「IBM Directory Server Web 管理ツール (IBM Directory Server Web Administration Tool)」ページが表示されます。「IBM Directory Server Web 管理ツール (IBM Directory Server Web Administration Tool)」ページについて詳しくは、118 ページの『Web 管理ツール』を参照してください。
4. 管理できる Directory Server のリストを追加または変更したい場合、または Web 管理コンソール属性を変更したい場合には、以下を行ってください。
  - a. 「LDAP ホスト名」フィールドで、「コンソール管理」を選択する。
  - b. コンソール管理者ログインを入力する。
  - c. コンソール管理者パスワードを入力する。
  - d. 「Login (ログイン)」をクリックする。「IBM Directory Server Web 管理ツール (IBM Directory Server Web Administration Tool)」ページが表示されます。「IBM Directory Server Web 管理ツール (IBM Directory Server Web Administration Tool)」ページについて詳しくは、118 ページの『Web 管理ツール』を参照してください。
  - e. 「コンソール管理」をクリックした後、以下のいずれかを選択する。
    - コンソール管理者ログインの名前を変更する「コンソール管理者ログインの変更」。
    - コンソール管理者のパスワードを変更する「コンソール管理者パスワードの変更」。
    - どの Directory Servers を Web 管理コンソールで管理できるかを変更する「コンソール・サーバーの管理」。
    - Web 管理コンソールのプロパティを変更する「コンソール・プロパティの管理」。

## Web 管理の初めてのセットアップ

このトピックでは、初めて Directory Server Web Administration Tool をセットアップする方法を説明します。

1. IBM WebSphere Application Server 6.0 (5733-W60 Base または Express オプション) およびそれに関連した前提条件ソフトウェアがまだインストールされていなければ、それらをインストールする。
2. HTTP ADMIN サーバー・インスタンスのシステム・アプリケーション・サーバー・インスタンスを使用可能にする。詳しくは、IBM HTTP Server トピックを参照してください。

- a. 以下のいずれかにより、HTTP ADMIN サーバー・インスタンスを開始します。
  - System i Navigator で、「ネットワーク」 → 「サーバー」 → 「TCP/IP」をクリックし、「HTTP Administration」を右クリックする。その後「開始」をクリックする。
  - コマンド行で、STRTCPSVR SERVER(\*HTTP) HTTPSVR(\*ADMIN) と入力する。
- b. IBM Web Administration for iSeries にログインする。オペレーティング・システムのユーザー・プロファイルおよびパスワードを使用してiSeries の Tasks ページ ([http://your\\_server:2001](http://your_server:2001)) にログインする。次に、「IBM Web Administration for iSeries」をクリックする。
- c. HTTP Server Administration の「your\_server」ページから、「管理」タブをクリックして、次に「HTTP Server」タブをクリックする。「ADMIN - Apache」が「サーバー」ドロップダウン・リストで選択されていて、さらに、「/QIBM/UserData/HTTPAdmin/conf/admin-cust.conf の組み込み」が「サーバー域」ドロップダウン・リストで選択されていることを確認する。
- d. ページの左ペインにあるオプションから、「一般サーバー構成 (General Server Configuration)」をクリックする。

注: 「一般サーバー構成 (General Server Configuration)」オプションを表示するために、「サーバー・プロパティ」セクションを展開する必要がある場合があります。

- e. 「Admin サーバーを開始するときに、システム・アプリケーション・サーバー・インスタンスを開始する (Start the system application server instance when the 'Admin' server is started)」を「はい」に設定する。
- f. 「OK」をクリックする。
- g. 再始動ボタン (「HTTP Server」タブの下にある 2 番目のボタン) をクリックして、HTTP ADMIN サーバー・インスタンスを再始動します。System i Navigator またはコマンド行を使用して、HTTP ADMIN サーバー・インスタンスを停止および開始することもできます。

以下のいずれかにより、HTTP ADMIN サーバー・インスタンスを停止できます。

- System i Navigator で、「ネットワーク」 → 「サーバー」 → 「TCP/IP」をクリックし、「HTTP Administration」を右クリックする。その後「停止」をクリックする。
- コマンド行で、ENDTCPSVR SERVER(\*HTTP) HTTPSVR(\*ADMIN) と入力する。

以下のいずれかにより、HTTP ADMIN サーバー・インスタンスを開始できます。

- System i Navigator で、「ネットワーク」 → 「サーバー」 → 「TCP/IP」をクリックし、「HTTP Administration」を右クリックする。その後「開始」をクリックする。
- コマンド行で、STRTCPSVR SERVER(\*HTTP) HTTPSVR(\*ADMIN) と入力する。

詳しくは、IBM HTTP Server トピックを参照してください。

3. Directory Server Web 管理ツールにログインします。
  - a. 次のいずれかを行って、ログイン・ページを表示する。

- System i Navigatorから、サーバーを選択し、「ネットワーク」→「サーバー」→「TCP/IP」をクリックし、「IBM Directory Server」を右クリックし、「サーバー管理 (Server Administration)」をクリックする。
  - iSeriesの Tasks ページ ([http://your\\_server:2001](http://your_server:2001)) から、「IBM Directory Server for iSeries」をクリックする。
- b. 「LDAP ホスト名」フィールドで、「コンソール管理」を選択する。
  - c. 「ユーザー名」フィールドに superadmin と入力する。
  - d. 「パスワード」フィールドに secret と入力する。
  - e. 「Login (ログイン)」をクリックする。「IBM Directory Server Web 管理ツール (IBM Directory Server Web Administration Tool)」ページが表示されます。
4. コンソール管理のログインを変更する。
    - a. 左ペインの「コンソール管理」をクリックしてセクションを展開し、次に「コンソール管理者ログインの変更」をクリックする。
    - b. 「コンソール管理者ログインの変更」フィールドに新規コンソール管理ログイン名を入力する。
    - c. 「現在のパスワード」フィールドに現在のパスワード (secret) を入力する。
    - d. 「OK」をクリックする。
  5. コンソール管理のパスワードを変更する。左ペインの「コンソール管理者パスワードの変更」をクリックする。
  6. 管理したい Directory Server を追加する。左ペインの「コンソール・サーバーの管理」をクリックする。
- 注: Directory Server を追加するとき、「管理ポート」は使用されず、無視されます。
7. 必要に応じてコンソール・プロパティを変更する。左ペインの「コンソール・プロパティの管理」をクリックする。
  8. 「ログアウト」をクリックする。「ログアウトの正常終了」画面が表示された時、「ここ (here)」リンクをクリックして、Web 管理ログイン・ページに戻ります。

コンソールを初めて構成した後、いつでもコンソールに戻り、以下のことを行えます。

- コンソール管理者ログインおよびパスワードを変更する。
- どの Directory Servers を Web 管理ツールで管理できるかを変更する。
- コンソール・プロパティを変更する。

## Web 管理ツール

Web 管理ツールに一度ログオンすると、5 つの部分で構成されるアプリケーション・ウィンドウがあります。

### バナー・エリア

バナー・エリアはパネルの上部にあり、アプリケーション名および IBM ロゴが含まれています。

### ナビゲーション領域

ナビゲーション領域はパネルの左側にあります。ここには、以下のような各種のサーバー・コンテンツ・タスクのカテゴリーが展開可能な形式で表示されます。

### ユーザー・プロパティ

このタスクにより、現在のユーザーのパスワードを変更できます。

### スキーマ管理

このタスクでは、オブジェクト・クラス、属性、突き合わせ規則、および構文を扱う作業ができます。

### ディレクトリー管理

このタスクにより、ディレクトリー項目を扱う作業ができます。

### 複製管理

このタスクにより、信任状、トポロジー、スケジュール、およびキューを扱う作業ができます。

### レルムとテンプレート

このタスクにより、ユーザー・テンプレートおよびレルムを扱う作業ができます。

### ユーザーとグループ

このタスクにより、定義済みレルム内のユーザーおよびグループを扱う作業ができます。たとえば、新規 Web ユーザーを作成しようとする場合、「**ユーザーとグループ**」タスクは、単一グループ objectclass、groupOfNames を処理します。グループのサポートは調整できません。

### サーバー管理

このタスクによって、サーバー構成およびセキュリティー設定を変更することができます。

## 作業域

作業域には、ナビゲーション領域で選択されたタスクに関連するタスクが表示されます。たとえば、ナビゲーション領域で「サーバー・セキュリティーの管理 (Managing server security)」を選択した場合、作業域には「サーバー・セキュリティー (Server Security)」ページと、サーバー・セキュリティーのセットアップに関連したタスクを含むタブが表示されます。

## サーバー状況領域

サーバー状況領域は作業域の上部にあります。サーバー状況領域の左端にあるアイコンは、サーバーの現在の状況を示します。アイコンの隣には、管理されるサーバーの名前があります。サーバー状況領域の右端にあるアイコンは、オンライン・ヘルプへのリンクを示します。

## タスク状況域

作業域の下にあるタスク域には、現在のタスクの状況が表示されます。

---

## Directory Server のシナリオ

以下の情報を使用して、Directory Server の標準タスクの例を示すシナリオを検討してみてください。

### シナリオ: Directory Server のセットアップ

Directory Server 上に LDAP ディレクトリーをセットアップする方法の例。

#### 状況

会社のコンピューター・システムの管理者として、電話番号や E メール・アドレスなどの組織の従業員情報を中央 LDAP リポジトリーに配置したい。

#### 目標

このシナリオでは、MyCo 社は Directory Server を構成して、名前、E メール・アドレス、電話番号などの従業員情報を含むディレクトリー・データベースを作成します。

このシナリオの目的は以下のとおりです。

- Lotus Notes または Microsoft Outlook Express メール・クライアントを使用して、従業員が、会社のネットワーク上のどの場所からでも従業員情報を使用できるようにする。
- 管理者がディレクトリー・データベースにある従業員データを変更できるようにすると共に、管理者以外の人が従業員データを変更できないようにする。
- システムが従業員データをディレクトリー・データベースに公開できるようにする。

## 詳細

Directory Server は、mySystem というシステム上で実行されます。

以下の例は、MyCo 社が従業員ごとにディレクトリー・データベースに含める情報を示しています。

```
Name: Jose Alvarez
Department: DEPTA
Telephone number: 999 999 9999
Email address: jalvarez@my_co.com
```

このシナリオのディレクトリー構造を視覚化すると、以下の図のようなものになります。

```
/
|
+- my_co.com
 |
 +- employees
 |
 +- Jose Alvarez
 |
 DEPTA
 999-555-1234
 jalvarez@my_co.com
 +- John Smith
 |
 DEPTA
 999-555-1235
 jsmith@my_co.com
 + Managers group
 Jose Alvarez
 mySystem.my_co.com
 .
 .
 .
```

すべての従業員 (管理者およびそれ以外) は、employees ディレクトリー・ツリーに存在します。管理者は、managers group にも属します。managers group のメンバーは、従業員データの変更権限があります。

システム (mySystem) も従業員データを変更する権限を持っている必要があります。このシナリオでは、システムは employees ディレクトリー・ツリーに置かれており、managers group のメンバーとなっています。

従業員項目をシステム項目とは分離しておきたい場合、別のディレクトリー・ツリー (たとえば: computers) を作成し、そこにシステムを追加することができます。システムは、管理者と同じ権限を持っている必要があります。

## 前提条件と前提事項

Web 管理ツールが正しく構成され、稼働していることが必要です。詳しくは、116 ページの『Web 管理』を参照してください。

## セットアップのステップ

以下のタスクを行います。

### シナリオの詳細: Directory Server のセットアップ

#### ステップ 1: Directory Server を構成する:

注: 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。

1. System i Navigator で、「ネットワーク」 → 「サーバー」 → 「TCP/IP」をクリックする。
2. System i Navigatorの右下にある「サーバー構成タスク (Server Configuration tasks)」ウィンドウ内で、「システムをディレクトリー・サーバーとして構成する (Configure system as Directory server)」をクリックする。
3. 「Directory Server の構成ウィザード (Directory Server Configuration Wizard)」が表示される。
4. 「IBM Directory Server の構成ウィザード - ようこそ (IBM Directory Server Configuration Wizard - Welcome)」ウィンドウ上の「ローカル LDAP ディレクトリー・サーバーの構成 (Configure a local LDAP directory server)」をクリックする。
5. 「IBM Directory Server の構成ウィザード - ようこそ (IBM Directory Server Configuration Wizard - Welcome)」ウィンドウ上の「次へ」をクリックする。
6. 「IBM Directory Server の構成ウィザード - 設定の指定 (IBM Directory Server Configuration Wizard - Specify Settings)」ウィンドウ上で「いいえ」を選択する。これにより、デフォルトの設定値を使用せずに LDAP サーバーを構成できるようになります。
7. 「IBM Directory Server の構成ウィザード - 設定の指定 (IBM Directory Server Configuration Wizard - Specify Settings)」ウィンドウ上で「次へ」を選択する。
8. 「IBM Directory Server の構成ウィザード - 管理者 DN の指定 (IBM Directory Server Configuration Wizard - Specify Administrator DN)」ウィンドウ上で「システム生成 (System-generated)」のチェックマークを外し、以下を入力する。

|          |                  |
|----------|------------------|
| 管理者 DN   | cn=administrator |
| パスワード    | secret           |
| パスワードの確認 | secret           |

注: このシナリオで指定されたすべてのパスワードは、この例だけに使用します。システムまたはネットワーク・セキュリティの暗号漏えいを防ぐために、これらのパスワードをご使用の構成の一部として決して使用しないでください。

9. 「IBM Directory Server の構成ウィザード - 管理者 DN の指定 (IBM Directory Server Configuration Wizard - Specify Administrator DN)」ウィンドウ上で「次へ」をクリックする。
10. 「IBM Directory Server の構成ウィザード - 接尾部の指定 (IBM Directory Server Configuration Wizard - Specify Suffixes)」ウィンドウの「接尾部 (Suffix)」フィールドに dc=my\_co,dc=com と入力する。
11. 「IBM Directory Server の構成ウィザード - 接尾部の指定 (IBM Directory Server Configuration Wizard - Specify Suffixes)」ウィンドウで「追加」をクリックする。
12. 「IBM Directory Server の構成ウィザード - 接尾部の指定 (IBM Directory Server Configuration Wizard - Specify Suffixes)」ウィンドウで「次へ」をクリックする。

13. 「IBM Directory Server の構成ウィザード - IP アドレスの選択 (IBM Directory Server Configuration Wizard - Select IP Addresses)」 ウィンドウで「はい、すべての IP アドレスを使用します (Yes, use all IP addresses)」を選択する。
14. 「IBM Directory Server の構成ウィザード - IP アドレスの選択 (IBM Directory Server Configuration Wizard - Select IP Addresses)」 ウィンドウで「次へ」をクリックする。
15. 「IBM Directory Server の構成ウィザード - TCP/IP 設定の指定 (IBM Directory Server Configuration Wizard - Specify TCP/IP Preference)」 ウィンドウで「はい」を選択する。
16. 「IBM Directory Server の構成ウィザード - TCP/IP 設定の指定 (IBM Directory Server Configuration Wizard - Specify TCP/IP Preference)」 ウィンドウで「次へ」をクリックする。
17. 「IBM Directory Server の構成ウィザード - 要約 (IBM Directory Server Configuration Wizard - Summary)」 ウィンドウ上の「完了」をクリックする。
18. 「IBM Directory Server」上を右マウス・ボタン・クリックし、「開始」をクリックする。

#### ステップ 2: Directory server Web 管理ツールを構成する:

1. ブラウザーが `http://mySystem.my_co.com:9080/IDSWebApp/IDSjsp/Login.jsp` を指すようにする。ここで、`mySystem.my_co.com` はご使用のシステムです。
2. ログイン・ページが表示される。「LDAP ホスト名」リストをクリックし、「コンソール管理」を選択します。ユーザー名には `superadmin`、パスワードには `secret` と入力します。「Logon (ログオン)」をクリックする。
3. ご使用のシステム上の LDAP サーバーに接続するように Web 管理ツールを構成する。左方のナビゲーションで、「コンソール管理」→「コンソール・サーバーの管理」を選択します。
4. 「追加」をクリックする。
5. 「サーバーの追加」フィールドに、`mySystem.my_co.com` と入力する。
6. 「OK」をクリックする。「コンソール・サーバーの管理」の下のリストに新規サーバーが表示されます。
7. 左方のナビゲーションで「ログアウト (logout)」をクリックする。
8. Web 管理ツールのログイン・ページで、「LDAP ホスト名」リストをクリックし、今構成したサーバー (`mySystem.my_co.com`) を選択する。
9. 「ユーザー名」フィールドで `cn=administrator` と入力し、「パスワード」フィールドに `secret` と入力する。「Login (ログイン)」をクリックする。IBM Directory Server Web 管理ツールのメインページが表示されるはずですが。

#### シナリオの詳細: ディレクトリー・データベースの作成

データの入力を開始する前に、データを保管する場所を作成する必要があります。

#### ステップ 1: 基本 DN オブジェクトを作成する:

1. Web 管理ツールで、「ディレクトリー管理」→「項目の管理」をクリックする。ディレクトリーの基本レベルのオブジェクトのリストが表示されます。サーバーは新規であるため、構成情報を含む構造オブジェクトのみが表示されます。
2. MyCo 社のデータを含む新規オブジェクトを追加する。まず、ウィンドウの右側の「追加...」をクリックします。次のウィンドウで「オブジェクト・クラス」リスト内をスクロールし、「ドメイン (domain)」を選択してから「次へ」をクリックします。
3. 補助オブジェクト・クラスは追加したくないので、再度「次へ」をクリックする。



4. 「属性の入力 (Enter the attributes)」ウィンドウで、ウィザードですでに作成した接尾部に対応するデータを入力する。「ドメイン (domain)」の「オブジェクト・クラス」ドロップダウン・リストを閉じます。「相対 DN」フィールドに dc=my\_co と入力します。「親 DN」フィールドに dc=com と入力します。「dc」フィールドに my\_co と入力します。
5. ウィンドウの下部の「完了」をクリックする。基本レベルに戻ると、新規基本 DN が表示されるはずですが。

#### ステップ 2: ユーザー・テンプレートを作成する:

MyCo 社の従業員データを追加する際に有用なユーザー・テンプレートを作成します。

1. Web 管理ツールで、「レルムとテンプレート」 → 「ユーザー・テンプレートの追加」をクリックする。
2. 「ユーザー・テンプレート名」フィールドで、Employee と入力する。
3. 「親 DN」フィールドの隣の「ブラウズ...」ボタンをクリックする。前の節で作成した基本 DN、「dc=my\_co,dc=com」をクリックして、ウィンドウの右方にある「選択」をクリックします。
4. 「次へ」をクリックします。
5. 「構造オブジェクト・クラス」ドロップダウン・リストで、「inetOrgPerson」を選択し、「次へ」をクリックする。
6. 「命名属性」ドロップダウン・リストで、「cn」を選択する。
7. 「タブ」リストで「必須属性」を選択し、「編集」をクリックする。
8. 「タブの編集」ウィンドウは、ユーザー・テンプレートにどのフィールドを組み込むかを選択する場所です。「sn」および「cn」が必要です。
9. 「属性」リストで「departmentNumber」を選択し、「追加>>>」をクリックする。
10. 「telephoneNumber」を選択し、「追加 >>>」をクリックする。
11. 「mail」を選択し、「追加 >>>」をクリックする。
12. 「userPassword」を選択し、「追加 >>>」をクリックする。
13. 「OK」の後「完了」をクリックして、ユーザー・テンプレートを作成する。

#### ステップ 3: レルムを作成する:

1. Web 管理ツールで、「レルムとテンプレート」 → 「レルムの追加」をクリックする。
2. 「レルム名」フィールドに employees と入力する。
3. 「親 DN」フィールドの右方にある「ブラウズ...」をクリックする。
4. 作成した親 DN、「dc=my\_co,dc=com」を選択し、ウィンドウの右側にある「選択」をクリックする。
5. 「次へ」をクリックします。
6. 次のウィンドウでは、「ユーザー・テンプレート」ドロップダウン・リストのみを変更する必要があります。作成したユーザー・テンプレート、「cn=employees,dc=my\_co,dc=com」を選択します。
7. 「完了」をクリックする。

#### ステップ 4: 管理者グループを作成する:

1. 管理者グループを作成する。
  - a. Web 管理ツールで、「ユーザーおよびグループ」 → 「グループの追加」をクリックする。
  - b. 「グループ名」フィールドに managers と入力する。
  - c. 「レルム」プルダウン・リストで、必ず「employees」を選択する。
  - d. 「完了」をクリックする。

2. **employees** レルムの管理者グループ管理者を構成する。
  - a. 「レルムとテンプレート」 → 「レルムの管理」をクリックする。
  - b. 作成したレルム、「**cn=employees,dc=my\_co,dc=com**」を選択し、「編集」をクリックする。
  - c. 「管理者グループ」フィールドの右方で、「ブラウズ...」をクリックする。
  - d. 「**dc=my\_co,dc=com**」を選択し、「展開」をクリックする。
  - e. 「**cn=employees**」を選択し、「展開」をクリックする。
  - f. 「**cn=managers**」を選択し、「選択」をクリックする。
  - g. 「レルムの編集」ウィンドウで、「OK」をクリックする。
3. 管理者グループに「**dc=my\_co,dc=com**」接尾部の権限を与える。
  - a. 「ディレクトリー管理」 → 「項目の管理」をクリックする。
  - b. 「**dc=my\_co,dc=com**」を選択し、「ACL の編集...」をクリックする。
  - c. 「ACL の編集」ウィンドウで、「所有者」タブをクリックする。
  - d. 「所有者の伝搬」チェック・ボックスを選択する。管理者グループのメンバー全員は、「**dc=my\_co,dc=com**」データ・ツリーの所有者となります。
  - e. 「タイプ」プルダウン・リストで、「グループ」を選択する。
  - f. 「DN (識別名)」フィールドで、**cn=managers,cn=employees,dc=my\_co,dc=com** と入力する。
  - g. 「追加」をクリックします。
  - h. 「OK」をクリックします。

#### ステップ 5: ユーザーをマネージャーとして追加する:

1. Web 管理ツールで、「ユーザーおよびグループ」 → 「ユーザーの追加」をクリックする。
2. 「レルム」ドロップダウン・メニューで作成したレルム、「**employees**」を選択し、「次へ」をクリックする。
3. 「**cn**」フィールドに Jose Alvirez と入力する。
4. 「**\*sn**」(姓)フィールドに Alvirez と入力する。
5. 「**\*cn**」(完全な名前)フィールドに Jose Alvirez と入力する。cn は項目の DN を作成するために使用されます。\*cn は、オブジェクトの属性です。
6. 「**telephoneNumber**」フィールドに 999 555 1234 と入力する。
7. 「**departmentNumber**」フィールドに DEPTA と入力する。
8. 「**mail**」フィールドに jalvirez@my\_co.com と入力する。
9. 「**userPassword**」フィールドに secret と入力する。
10. 「ユーザー・グループ」タブをクリックする。
11. 「使用可能グループ」リストで、「管理者 (**managers**)」を選択し、「追加 ->」をクリックする。
12. ウィンドウの下部で、「完了」をクリックする。
13. ナビゲーションの左方にある「ログアウト (**Log out**)」をクリックして、Web 管理ツールからログアウトする。

### シナリオの詳細: System i<sup>™</sup> データをディレクトリー・データベースに公開する

システムが自動的にユーザー情報を LDAP ディレクトリーに入力できるように公開を構成する。システム配布ディレクトリーからのユーザー情報は、LDAP ディレクトリーに公開されます。

注: System i Navigatorで作成されたユーザーには、ユーザー・プロファイルおよびシステム配布ディレクトリー・ユーザー項目が与えられます。CL コマンドを使用してユーザーを作成する場合、ユーザー・プロファイル (CRTUSRPRF) およびシステム配布ディレクトリー・ユーザー項目 (WRKDIRE) の両方を作成する必要があります。ユーザーがユーザー・プロファイルとしてのみ存在し、それらをLDAP ディレクトリーに公開したい場合、それらユーザーのためにシステム配布ディレクトリー・ユーザー項目を作成する必要があります。

#### ステップ 1: システムを Directory Server ユーザーにする:

1. Web 管理ツール ([http://mySystem.my\\_co.com:9080/IDSWebApp/IDSjsp/Login.jsp](http://mySystem.my_co.com:9080/IDSWebApp/IDSjsp/Login.jsp)) に管理者としてログインする。
  - a. 「LDAP ホスト名」リストで、「mySystem.my\_co.com」を選択する。
  - b. 「ユーザー名」フィールドに cn=administrator と入力する。
  - c. 「パスワード」フィールドに secret と入力する。
  - d. 「Login (ログイン)」をクリックする。
2. 「ユーザーとグループ」 → 「ユーザーの追加」を選択する。
3. 「レルム」リストで、「employees」を選択する。
4. 「次へ」をクリックします。
5. 「cn」フィールドに mySystem.my\_co.com と入力する。
6. 「\*sn」フィールドに mySystem.my\_co.com と入力する。
7. 「\*cn」フィールドに mySystem.my\_co.com と入力する。
8. 「userPassword」フィールドに secret と入力する。
9. 「ユーザー・グループ」タブをクリックする。
10. グループの「管理者 (managers)」を選択する。
11. 「追加」 → をクリックする。
12. 「完了」をクリックする。

#### ステップ 2: システムがデータを公開するように構成する:

1. System i Navigatorで、左側のナビゲーションの iSeries を右クリックし、「プロパティー」を選択する。
2. 「プロパティー (Properties)」ダイアログ・ボックスで、「Directory Server」タブを選択する。
3. 「ユーザー (Users)」を選択し、「詳細」をクリックする。
4. 「ユーザー情報の公開 (Publish user information)」チェック・ボックスを選択する。
5. 「公開先 (Where to publish)」セクションで、「編集」ボタンをクリックする。ウィンドウが表示されます。
6. mySystem.my\_co.com と入力する。
7. 「親識別名 (Under DN)」フィールドに cn=employees,dc=my\_co,dc=com と入力する。
8. 「サーバー接続 (Server connection)」セクションで、デフォルトのポート番号、「389」が「ポート」フィールドに確実に入力する。「認証方法」ドロップダウン・リストで、「識別名 (Distinguished name)」を選択し、「識別名 (Distinguished name)」フィールドに cn=mySystem,cn=employees,dc=my\_co,dc=com と入力する。
9. 「パスワード」をクリックする。
10. 「パスワード」フィールドに secret と入力する。
11. 「確認パスワード」フィールドに secret と入力する。

12. 「OK」をクリックする。
13. 「検証」ボタンをクリックする。これにより、すべての情報が正しく入力されたことと、システムが LDAP ディレクトリーに接続できることが確認されます。
14. 「OK」をクリックする。
15. 「OK」をクリックする。

## シナリオの詳細: ディレクトリー・データベースへの情報の入力

管理者である Jose Alvarez は、自分の部門にいる個人のデータをここで追加および更新します。Jane Doe に関する幾つかの追加情報を追加する必要があります。Jane Doe は、システム上のユーザーで、彼女の情報は公開されています。Jose Alvarez は、John Smith に関する情報も追加する必要があります。John Smith は、システム上のユーザーではありません。Jose Alvarez は、以下のことを行います。

### ステップ 1: Web 管理ツールにログインする:

Web 管理ツールにログインします。( [http://mySystem.my\\_co.com:9080/IDSWebApp/IDSjsp/Login.](http://mySystem.my_co.com:9080/IDSWebApp/IDSjsp/Login.)) 以下のようになります。

1. 「LDAP ホスト名」リストで、「mySystem.my\_co.com」を選択する。
2. 「ユーザー名」フィールドに cn=Jose Alvarez,cn=myco employees,dc=my\_co,dc=com と入力する。
3. 「パスワード」フィールドに secret と入力する。
4. 「Logon (ログオン)」をクリックする。

### ステップ 2: 従業員データを変更する:

1. 「ユーザーとグループ」 → 「ユーザーの管理」をクリックする。
2. 「レルム」リストで「employees」を選択し、「ユーザーの表示」をクリックする。
3. ユーザー・リストで「Jane Doe」を選択し、「編集」をクリックする。
4. 「departmentNumber」フィールドに DEPTA と入力する。
5. 「OK」をクリックする。
6. 「閉じる」をクリックする。

### ステップ 3: 従業員データを追加する:

1. 「ユーザーとグループ」 → 「ユーザーの追加」をクリックする。
2. 「レルム」プルダウン・メニューで「employees」を選択し、「次へ」をクリックする。
3. 「cn」フィールドに John Smith と入力する。
4. 「\*sn」フィールドに Smith と入力する。
5. 「\*cn」フィールドに John Smith と入力する。
6. 「telephoneNumber」フィールドに 999 555 1235 と入力する。
7. 「departmentNumber」フィールドに DEPTA と入力する。
8. 「mail」フィールドに jsmith@my\_co.com と入力する。
9. ウィンドウの下部の「完了」をクリックする。

## シナリオの詳細: ディレクトリー・データベースのテスト

従業員データをディレクトリー・データベースに入力した後、以下のいずれかを行ってディレクトリー・データベースおよび Directory Server をテストします。

### E メール・アドレス帳を使用してディレクトリー・データベースを検索する:

LDAP ディレクトリー内の情報は、LDAP が使用可能なプログラムで簡単に検索できます。多くの E メール・クライアントは、そのアドレス帳機能の一部として LDAP ディレクトリー・サーバーを検索できます。以下に、Lotus Notes® 6 および Microsoft を構成する手順例を示します。他のほとんどの E メール・クライアントもほとんど同様です。

#### **Lotus Notes:**

1. アドレス帳をオープンする。
2. 「アクション」 → 「新規」 → 「アカウント」をクリックする。
3. 「アカウント名」フィールドに mySystem と入力する。
4. 「Account server name (アカウント・サーバー名)」フィールドに mySystem.my\_co.com と入力する。
5. 「プロトコル」フィールドで「LDAP」を選択する。
6. 「Protocol Configuration (プロトコル構成)」タブをクリックする。
7. 「検索ベース」フィールドに dc=my\_co,dc=com と入力する。
8. 「保管してクローズ (Save and close)」をクリックする。
9. 「作成」 → 「メール」 → 「メモ」をクリックする。
10. 「アドレス...」をクリックする。
11. 「アドレス帳の選択」フィールドで mySystem を選択する。
12. 「開始文字列で検索」フィールドに Alvarez と入力する。
13. 「検索」をクリックする。Jose Alvarez のデータが表示されます。

#### **Microsoft Outlook Express:**

1. 「ツール」 → 「アカウント」をクリックする。
2. 「追加」 → 「ディレクトリ サービス」をクリックする。
3. 「インターネット ディレクトリ (LDAP) サーバー」フィールドにシステムの Web アドレスを入力する (mySystem.my\_co.com)。
4. 「この LDAP サーバーはログオンが必要」チェック・ボックスのチェック・マークを外す。
5. 「次へ」をクリックします。
6. 「次へ」をクリックします。
7. 「完了」をクリックする。
8. mySystem.my\_co.com (今構成したディレクトリー・サービス) を選択して、「プロパティ」をクリックする。
9. 「詳細設定 (Advanced)」をクリックする。
10. 「検索ベース」フィールドに dc=my\_co,dc=com と入力する。
11. 「OK」をクリックする。
12. 「閉じる」をクリックする。
13. Ctrl+E を入力して「人の検索」ウィンドウをオープンする。
14. 「探す場所」リストから mySystem.my\_co.com を選択する。
15. 「名前」フィールドに Alvarez と入力する。
16. 「検索開始」をクリックする。Jose Alvarez のデータが表示されます。

#### **ldapsearch コマンド行コマンドを使用してディレクトリー・データベースを検索する:**

1. 文字ベースのインターフェースで、CL コマンド **QSH** を入力して Qshell セッションをオープンする。

2. 以下を入力して、データベース内のすべての LDAP 項目のリストを検索する。

```
ldapsearch -h mySystem.my_co.com -b dc=my_co,dc=com objectclass=*
```

ここで、

**-h** LDAP サーバーを実行するホスト・マシンの名前です。

**-b** この基本 DN の下を検索します。

**objectclass=\***

ディレクトリー内のすべての項目を戻します。

このコマンドは、以下に類似したものが戻ります。

```
dc=my_co,dc=com
dc=my_co
objectclass=domain
objectclass=top
```

```
cn=MyCo employee,dc=my_co,dc=com
```

```
.
.
.
```

```
cn=Jose Alvarez,cn=MyCo Employees,dc=my_co,dc=com
```

```
sn=Alvarez
departmentNumber=DEPTA
mail=jalvarez@my_co.com
telephoneNumber=999 999 9999
objectclass=top
objectclass=inetOrgPerson
objectclass=organizationalPerson
objectclass=person
cn=Jose Alvarez
```

```
.
.
.
```

各項目の最初の行は、識別名 (DN) と呼ばれています。DN は、各項目の完全なファイル名に類似しています。項目の中には、データを含まず、構造だけのものもあります。行 **objectclass=inetOrgPerson** を持つ項目は、人のために作成した項目に対応します。Jose Alvarez の DN は、**cn=Jose Alvarez,cn=MyCo Employees,dc=my\_co,dc=com** です。

## シナリオ: HTTP サーバー妥当性検査リストから Directory Server へのユーザーのコピー

HTTP サーバー妥当性検査リストから Directory Server へユーザーをコピーする例。

### 状態および概要

現在、妥当性検査リスト MYLIB/HTTPVLDL のインターネット・ユーザーを使用し、HTTP Server (Apache 付き) で稼働するアプリケーションがあるものとします。また、LDAP 認証がある WebSphere Application Server (WAS) と同じインターネット・ユーザーを使用するものとします。なお、妥当性検査リストのユーザー情報および LDAP の重複した保守を回避するために、HTTP サーバー・アプリケーションを構成して LDAP 認証も使用します。

これを行うには、次のステップを実行する必要があります。

1. 既存の妥当性検査リストのユーザーをローカル・ディレクトリー・サーバーにコピーする。
2. WAS サーバーを構成して LDAP 認証を使用する。
3. HTTP サーバーを再構成して、妥当性検査リストの代わりに LDAP 認証を使用する。

## ステップ 1: 既存の妥当性検査リスト・ユーザーをローカル・ディレクトリー・サーバーにコピーする

ディレクトリー・サーバーは接尾部「o=my company」で既に構成されていて、実行中であるものとしません。LDAP ユーザーはディレクトリー・サブツリー「cn=users,o=my company」に保管されます。ディレクトリー・サーバー管理者 DN は「cn=administrator」で、管理者パスワードは「secret」です。

次のようにしてコマンド行から API を呼び出します。

```
CALL PGM(QSYS/QGLDCPYVL) PARM('HTTPVLDL MYLIB ' 'cn=administrator' X'00000000' 'secret'
 X'00000000' 'cn=users,o=my company' X'00000000' '' X'00000000' X'00000000')
```

完了すると、ディレクトリー・サーバーには、妥当性検査リスト項目に基づいて inetorgperson 項目が入れます。例えば、妥当性検査リスト・ユーザーは次のとおりです。

```
User name: jsmith
Description: John Smith
Password: *****
```

結果は、以下のディレクトリー項目となります。

```
dn: uid=jsmith,cn=users,o=my company
objectclass: top
objectclass: person
objectclass: organizationalperson
objectclass: inetorgperson
uid: jsmith
sn: jsmith
cn: jsmith
description: John Smith
userpassword: *****
```

この項目は現在、ディレクトリー・サーバーへの認証のために使用できます。例えば、この QSH ldapsearch を実行すると、サーバーの root DSE 項目が読み取られます。

```
> ldapsearch -D "uid=jsmith,cn=users,o=my company" -w ***** -s base "(objectclass=*)"
```


作成されると、ディレクトリー項目を編集して、さらに情報を入れることができます。例えば、cn と sn の値を変更して、ユーザーのフルネームと姓を反映させるか、あるいは電話番号や E メール・アドレスを追加したいことがあります。

## ステップ 2: WAS サーバーを構成して LDAP 認証を使用する

入力されたユーザー名をその uid 属性値が含まれた inetOrgPerson 項目にマップする検索フィルターを使用して、dn "cn=users,o=my company" にある項目を検索するには、WAS LDAP セキュリティーを構成する必要があります。例えば、ユーザー名 jsmith を使用して WAS に対して認証することは、検索フィルター "(uid=jsmith)" と突き合わせる項目を検索する結果となります。詳細については、iSeries Information Center の Websphere Application Server の『Configure LDAP search filters』を参照してください。

## HTTP サーバーを再構成して、妥当性検査リストの代わりに LDAP 認証を使用する。

注: 下に記述された手順は、LDAP 認証を使用する HTTP サーバーを構成する高レベルの概要を提示して、このシナリオの例題を解りやすく図示するためのものです。詳細情報が必要な場合は、IBM Redbooks™ 資料「Implementation and Practical Use of LDAP on the IBM eServer™ iSeries Server」

(SG24-6193) の  第 6.3.2 章『Setting up LDAP authentication for the powered by Apache server』と、「Set up password protection on HTTP Server (powered by Apache)」を参照してください。

1. HTTP Administration ツールの HTTP サーバーの「構成」タブにある「基本認証」をクリックする。
2. 「ユーザー認証方式」で、「妥当性検査リストのインターネット・ユーザーの使用」を「LDAP サーバーのユーザー項目の使用」に変更して、「OK」をクリックする。
3. 「構成」タブに戻り、「制御アクセス」をクリックする。上記でリンクした Redbooks の説明のとおり、これを構成して「OK」をクリックする。
4. 「構成」タブでは、「LDAP 認証」をクリックする。
  - a. LDAP サーバーのホスト名およびポートを入力する。「ユーザー検索ベース DN」では、`cn=users,o=my company` を入力する。
  - b. 「ユーザー認証のための固有の LDAP DN の作成」では、フィルター (`&objectclass=person(uid=%v1)`) を入力する。
  - c. グループ情報を入力して、「OK」をクリックする。
5. 上記でリンクした Redbooks の説明のとおり、LDAP サーバーへの接続を構成する。

---

## Directory Server の管理

以下の情報を参考にして、Directory Server を管理します。

Directory Server を管理するには、使用しているユーザー・プロファイルが以下の権限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) 特殊権限、および入出力システム構成 (\*IOSYSCFG) 特殊権限
- 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) 特殊権限
- サーバーのジョブ・ログを表示する場合: スプール制御 (\*SPLCTL) 特殊権限

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 (94 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) を持つプロジェクト・ユーザーも管理者になれます。また、ほとんどの管理タスクは、管理グループのユーザーも実行できます (70 ページの『管理アクセス』を参照)。

## 一般管理タスク

以下の情報を参考にして、Directory Server の一般管理を管理します。

### Directory Server の開始

以下の情報を参考にして、Directory Server を開始します。

1. System i Navigator 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. 「**IBM Directory Server**」を右マウス・ボタン・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 Directory Server 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 (132 ページの『Directory Server の状況の検査』を参照)、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。

コマンド `STRTCPSVR *DIRSRV` を入力することにより、文字ベースのインターフェースから Directory Server 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。

コマンド `TRCTCPAPP APP(*DIRSRV) ARGLIST(SAFEMODE)` を入力することにより、文字ベースのインターフェースから構成のみのモードでディレクトリー・サーバーを開始することができます。

構成のみのモードは、`cn=configuration` 接尾部のみをアクティブにしてサーバーを開始し、データベース・バックエンドの正常な初期化に依存しません。

#### 関連タスク

『Directory Server の停止』

以下の情報を参考にして、Directory Server を停止します。

132 ページの『Directory Server の状況の検査』

以下の情報を参考にして、Directory Server の状況を検査します。

## Directory Server の停止

以下の情報を参考にして、Directory Server を停止します。

**注:** Directory Server 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。

1. System i Navigator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. 「**IBM Directory Server**」を右マウス・ボタン・クリックし、「**停止**」を選択する。

システムの数、サーバーの活動量、および使用可能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 (132 ページの『Directory Server の状況の検査』を参照)、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。

コマンド `ENDTCPSVR *DIRSRV`、`ENDTCPSVR *ALL`、または `ENDTCP` を入力することにより、文字ベースのインターフェースから Directory Server 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。

#### 関連タスク

130 ページの『Directory Server の開始』

以下の情報を参考にして、Directory Server を開始します。

## Directory Server の状況の検査

以下の情報を参考にして、Directory Server の状況を検査します。

基本状況情報は System i Navigatorに入っています。詳細情報および完全な状況情報は Web 管理ツールを使用して調べてください。

System i Navigatorは、右フレームの「状況」列に、Directory Server の状況を表示します。

System i Navigatorの Directory Server の状況を検査するには、次のようにしてください。

1. 「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。 System i Navigator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、「IBM Directory Server」を右マウス・ボタン・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、Directory Server の状況を最新表示することができます。

Web 管理ツールでディレクトリー・サーバーの状況を表示するには、次のようにしてください。

1. ナビゲーション領域で「サーバー管理」カテゴリを拡張する。

**注:** Web 管理ツールの「サーバー管理」カテゴリのタスクを使用してサーバー構成設定を変更するには、\*ALLOBJ および IOSYSCFG の特殊権限をもつ i5/OS ユーザー・プロファイルとしてサーバーに認証する必要があります。これは、そのプロファイルのパスワードでプロジェクト・ユーザーとして認証することによって実行できます。Web 管理ツールからプロジェクト・ユーザーとしてバインドするには、os400-profile=MYUSERNAME,cn=accounts,os400-sys=MYSYSTEM.COM の形式の username を入力します。この MYUSERNAME と MYSYSTEM.COM のストリングはそれぞれ、ご使用のユーザー・プロファイル名および構成済みシステム射影接尾部と置き換えられます。

2. 「サーバー状況の表示」をクリックする。
3. 「サーバー状況の表示」パネルでは、各種のタブを選択して状況情報を表示する。

## Directory Server のジョブの検査

以下の情報を参考にして、Directory Server で特定のジョブをモニターします。

System i Navigatorのサーバー・ジョブを検査するには、次のようにしてください。

1. System i Navigator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. 「IBM Directory Server」を右マウス・ボタン・クリックしてから、「サーバーのジョブ (Server Jobs)」を選択する。

## サーバー接続の管理

以下の情報を参考にして、サーバーへの接続、およびその接続で実行される操作を表示します。

管理者は、その接続に基づいて、アクセスを制御する決定をくだし、サービス妨害アタックを防止することができます。これは、Web 管理ツールを使用して実行されます。

**注:** Web 管理ツールの「サーバー管理」カテゴリのタスクを使用してサーバー構成設定を変更するには、\*ALLOBJ および IOSYSCFG の特殊権限をもつ i5/OS ユーザー・プロファイルとしてサーバーに認証する必要があります。これは、そのプロファイルのパスワードでプロジェクト・ユーザーとして認証することによって実行できます。Web 管理ツールからプロジェクト・ユーザーとしてバインドするには、os400-profile=MYUSERNAME,cn=accounts,os400-sys=MYSYSTEM.COM の形式の username を入力します。この MYUSERNAME と MYSYSTEM.COM のストリングはそれぞれ、ご使用のユーザー・プロファイル名および構成済みシステム射影接尾部と置き換えられます。

1. ナビゲーション領域で「サーバー管理」カテゴリを拡張する。
2. 「サーバー接続の管理」をクリックします。

それぞれの接続に関して、以下の情報を示した表が表示されます。

**DN** クライアント接続の DN をサーバーに指定します。

### IP アドレス

サーバーへの接続があるクライアントの IP アドレスを指定します。

### 開始時刻

接続が行われた日付および時刻 (サーバーの時刻) を指定します。

**状況** 接続をアクティブにするか、またはアイドルにするかを指定します。進行中の操作があれば、接続はアクティブとみなされます。

### 開始済み Op 数

接続が確立された後で要求された操作数を指定します。

### 完了した Op 数

各接続で完了した操作数を指定します。

**タイプ** 接続を SSL または TLS のいずれで保護するかを指定します。そうしない場合は、このフィールドはブランクになります。

**注:** この表には、一度に最大 20 の接続が表示されます。

この表は、パネル上部のドロップダウン・メニューを展開して選択することによって、DN または IP アドレスのいずれかで表示するように指定できます。デフォルトの選択は DN です。同様に、この表はを昇順または降順のいずれで表示するかも指定できます。

3. 「再表示」をクリックすると、現行接続情報が更新されます。
4. 管理者または管理グループのメンバーとしてログオンした場合はさらに、パネルで使用可能なサーバー接続を切断するための選択も与えられます。サーバー接続を切断するこの機能によって、サービス妨害攻撃を停止し、サーバー・アクセスを制御することができます。接続の切断は、ドロップダウン・メニューを展開し、DN、IP アドレス、またはこの両方を選択して、「切断」をクリックして実行できます。すべてのサーバー接続 (この要求を行っている接続は除く) を切断するには、「すべての切断」をクリックしてください。確認警告が表示されます。「OK」をクリックして切断アクションを続けるか、あるいは「キャンセル」をクリックしてそのアクションを終了し、「サーバー接続の管理」パネルに戻ります。

サービス妨害アタックの防止の詳細は、『接続プロパティの管理』を参照してください。

### 関連概念

94 ページの『サービス妨害』

サービス妨害アタックに対する保護を備えるには、サービス妨害構成オプションを使用します。

### 関連タスク

『接続プロパティの管理』

以下の情報を参考にして、クライアントがサーバーをロックできないようにするためといった目的で、接続プロパティを設定します。

## 接続プロパティの管理

以下の情報を参考にして、クライアントがサーバーをロックできないようにするためといった目的で、接続プロパティを設定します。

接続プロパティの管理機能によって、クライアントがサーバーをロックできないようにすることができます。また、長時間実行タスクによってバックエンドが使用中になった場合に、管理者が常にサーバーへのアクセスができるようにします。接続プロパティの管理は、Web 管理ツールを使用して実行されます。

注: これらの選択が表示されるのは、この機能をサポートするサーバーに管理者または管理グループのメンバーとしてログインした場合のみです。

接続プロパティを設定するには、次のようにしてください。

1. ナビゲーション領域の「サーバー管理」カテゴリを展開し、「接続プロパティの管理」をクリックする。

注: Web 管理ツールの「サーバー管理」カテゴリのタスクを使用してサーバー構成設定を変更するには、\*ALLOBJ および IOSYSCFG の特殊権限をもつ i5/OS ユーザー・プロファイルとしてサーバーに認証する必要があります。これは、そのプロファイルのパスワードでプロジェクト・ユーザーとして認証することによって実行できます。Web 管理ツールからプロジェクト・ユーザーとしてバインドするには、os400-profile=MYUSERNAME,cn=accounts,os400-sys=MYSYSTEM.COM の形式の username を入力します。この MYUSERNAME と MYSYSTEM.COM のストリングはそれぞれ、ご使用のユーザー・プロファイル名および構成済みシステム射影接尾部と置き換えられます。

2. 「一般」タブを選択する。
3. 匿名接続設定を設定する。匿名バインドが許可されるように、「匿名接続の許可」チェック・ボックスが既に選択されています。これはデフォルトの設定です。このチェック・ボックスをクリックして、「匿名接続の許可」機能を選択解除します。このアクションによって、サーバーはすべての匿名接続をアンバインドします。

注: 匿名バインドが認可されない場合は、一部のアプリケーションでは正常に実行されないことがあります。

4. 「匿名接続のしきい値のクリーンアップ」フィールドでは、匿名接続のアンバインドを開始するためのしきい値数を設定します。0 から 65535 の値を指定できます。

注: 実際の最大数は、処理当りで許可されるファイル数によって制限されます。UNIX システムでは、ulimit -a コマンドを使用して、この制限を判別できます。Windows システムでは、これは固定数です。

デフォルト設定は 0 です。匿名接続のこの数値を超えると、「アイドル・タイムアウト」フィールドにユーザーが設定したアイドル・タイムアウト限界に基づいて接続がクリーンアップされます。

5. 「**認証済み接続のしきい値のクリーンアップ**」フィールドでは、認証済み接続のアンバインドを開始するためのしきい値数を設定します。0 から 65535 の値を指定できます。

注: 実際の最大数は、処理当りで許可されるファイル数によって制限されます。UNIX システムでは、`ulimit -a` コマンドを使用して、この制限を判別できます。Windows システムでは、これは固定数です。

デフォルトは 1100 です。認証済み接続のこの数値を超えると、「**アイドル・タイムアウト**」フィールドにユーザーが設定したアイドル・タイムアウト限界に基づいて接続がクリーンアップされます。

6. 「**すべての接続のしきい値のクリーンアップ**」フィールドでは、すべての接続のアンバインドを開始するためのしきい値数を設定します。0 から 65535 の値を指定できます。

注: 実際の最大数は、処理当りで許可されるファイル数によって制限されます。UNIX システムでは、`ulimit -a` コマンドを使用して、この制限を判別できます。Windows システムでは、これは固定数です。

デフォルトは 1200 です。接続がこの合計数を超えると、「**アイドル・タイムアウト**」フィールドにユーザーが設定したアイドル・タイムアウト限界に基づいて接続がクリーンアップされます。

7. 「**アイドル・タイムアウト限界**」フィールドでは、接続をクリーンアップ処理でクローズする前に、その接続をアイドルにできる秒数を設定します。0 から 65535 の値を指定できます。

注: 実際の最大数は、処理当りで許可されるファイル数によって制限されます。UNIX システムでは、`ulimit -a` コマンドを使用して、この制限を判別できます。Windows システムでは、これは固定数です。

デフォルトは 300 です。クリーンアップ処理を開始すると、処理の対象となっていて、限界を超えた接続はすべてクローズされます。

8. 「**結果のタイムアウト限界**」フィールドでは、書き出しの試行の間で許される秒数を設定します。0 から 65535 の値を指定できます。デフォルトは 120 です。この限界を超えた接続はすべて終了されます。

注: これは、Windows システムにのみ適用されます。30 秒を超えた接続はオペレーティング・システムによって自動的に除去されます。したがって、この「**結果のタイムアウト限界**」設定は、30 秒後にオペレーティング・システムによってオーバーライドされます。

9. 「**Emergency thread (緊急スレッド)**」タブをクリックする。
10. 緊急スレッド設定を設定する。緊急スレッドを活動化できるように、「**緊急スレッドの使用可能化**」チェック・ボックスが既に選択されています。これはデフォルトの設定です。このチェック・ボックスをクリックして、「**緊急スレッドの使用可能化**」機能を選択解除します。このアクションによって、緊急スレッドが活動化されないようにします。
11. 「**保留中の要求のしきい値**」フィールドでは、緊急スレッドを活動化する作業要求の限界数を設定します。0 から 65535 の範囲の値を指定して、緊急スレッドを活動化する前に、待ち行列中に入れることができる作業要求数の限界を設定します。デフォルトは 50 です。指定されたこの限界を超えると、緊急スレッドが活動化されます。
12. 「**時間しきい値**」フィールドでは、最後の作業項目が待ち行列から除去された後に、経過できる分数を指定します。待ち行列に作業項目があって、この時間制限を超えると、緊急スレッドが活動化されます。0 から 240 の値を指定できます。デフォルトは 5 です。
13. ドロップダウン・メニューから、緊急スレッドを活動化するために使用する基準を選択します。以下から選択できます。

- **サイズのみ:** 緊急スレッドが活動化されるのは、待ち行列で保留中の作業項目の指定された容量を超えた場合のみです。
- **時間のみ:** 緊急スレッドが活動化されるのは、除去される作業項目相互間の時間制限が指定された容量を超えた場合のみです。
- **サイズまたは時間:** 緊急スレッドが活動化されるのは、待ち行列サイズまたは時間しきい値が指定された容量を超えた場合のみです。
- **サイズおよび時間:** 緊急スレッドが活動化されるのは、待ち行列サイズおよび時間しきい値が指定された容量を超えた場合のみです。

サイズおよび時間がデフォルト設定です。

14. 「OK」をクリックする。

#### 関連概念

94 ページの『サービス妨害』

サービス妨害アタックに対する保護を備えるには、サービス妨害構成オプションを使用します。

#### 関連タスク

133 ページの『サーバー接続の管理』

以下の情報を参考にして、サーバーへの接続、およびその接続で実行される操作を表示します。

## イベント通知の使用可能化

以下の情報を参考にして、Directory Server のイベント通知を使用可能にします。

イベント通知では、ディレクトリーへの何かの追加といった指定のイベントの発生時に、クライアントが Directory Server から通知を受けられるように、Directory Server に登録しておくことができます。

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. Web 管理ツールのナビゲーション領域で「サーバー・プロパティの管理」の κατηγοリーを展開して、「イベント通知」タブを選択する。
2. 「イベント通知の使用可能化」チェック・ボックスを選択して、イベント通知を使用可能にする。「イベント通知の使用可能化」が使用不可の場合には、サーバーはこのパネル上の他のすべてのオプションを無視します。
3. 「接続当たりの最大登録数」を設定する。「登録」または「無制限」のいずれかのラジオ・ボタンをクリックします。「登録」を選択した場合は、そのフィールドで、各接続で許可される登録の最大数を指定する必要があります。トランザクションの最大数は 2,147,483,647 です。デフォルトの設定は 100 個の登録です。
4. 「最大合計登録数」を設定する。この選択は、サーバーが任意の時点でもつことができる登録数を設定します。「登録」または「無制限」のいずれかのラジオ・ボタンをクリックします。「登録」を選択した場合は、そのフィールドで、各接続で許可される登録の最大数を指定する必要があります。トランザクションの最大数は 2,147,483,647 です。デフォルトの登録数は「無制限」です。
5. 完了したら、「適用」をクリックし、終了しないで変更を保管するか、あるいは「OK」をクリックして変更を適用して終了するか、あるいは「キャンセル」をクリックして変更を行わないで、このパネルを終了する。
6. イベント通知を使用可能にした場合には、その変更を有効にするために、サーバーを再始動する必要があります。設定のみを変更した場合は、サーバーの再始動は必要ありません。

注: イベント通知を使用不可にするには、「イベント通知の使用可能化」チェック・ボックスを選択解除して、サーバーを再始動してください。

- イベント通知の追加情報については、「IBM Tivoli Directory Server Version 6.0 Programming Reference」
- の『Event notification』の節を参照してください。

## 関連情報



IBM Tivoli software Information Center

IBM Tivoli Directory Server の詳細は、IBM Tivoli ソフトウェアの Information Center を参照してください。

## トランザクション設定値の指定

以下の情報を参考にして、Directory Server トランザクションの設定値を構成します。

Directory Server トランザクションでは、LDAP ディレクトリー操作グループを 1 つの単位として扱うことができます。

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。

- Web 管理ツールのナビゲーション領域で「サーバー・プロパティの管理」の κατηγοリーを展開して、「トランザクション」タブを選択する。
- 「トランザクション処理の使用可能化」チェック・ボックスを選択して、トランザクション処理を使用可能にする。「トランザクション処理の使用可能化」が使用不可の場合は、「トランザクション当たりの最大操作数」および「保留の時間制限」などの、このパネルの他のすべてのオプションはサーバーによって無視されます。
- 「トランザクションの最大数」を設定する。「トランザクション」または「無制限」のいずれかのラジオ・ボタンをクリックします。「トランザクション」を選択した場合は、そのフィールドで、トランザクションの最大数を指定する必要があります。トランザクションの最大数は 2,147,483,647 です。デフォルト設定は 20 個のトランザクションです。
- 「トランザクション当たりの最大操作数」を設定する。「操作」または「無制限」のいずれかのラジオ・ボタンをクリックします。「操作」を選択した場合は、そのフィールドで、各トランザクションで許可される操作の最大数を指定する必要があります。操作の最大数は 2,147,483,647 です。この数値が小さければ、パフォーマンスは上がります。デフォルトは 5 個の操作です。
- 「保留中の時間制限」を設定する。この選択では、保留中のトランザクションの最大タイムアウト値(秒数)を指定します。「秒数」または「無制限」のいずれかのラジオ・ボタンをクリックします。「秒数」を選択した場合は、そのフィールドで、各トランザクションで許可される操作の最大秒数を指定する必要があります。最大秒数は 2,147,483,647 です。この時間より長く未完了のままのトランザクションは、キャンセル(ロールバック)されます。デフォルトは 300 秒です。
- 完了したら、「適用」をクリックし、終了しないで変更を保管するか、あるいは「OK」をクリックして変更を適用して終了するか、あるいは「キャンセル」をクリックして変更を行わないで、このパネルを終了する。
- トランザクション・サポートを使用可能にした場合には、その変更を有効にするために、サーバーを再始動する必要がある。設定のみを変更した場合は、サーバーの再始動は必要がありません。

注: トランザクション処理を使用不可にするには、「トランザクション処理の使用可能化」チェック・ボックスを選択解除して、サーバーを再始動してください。

## 関連概念

57 ページの『トランザクション』

Directory Server 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。

## ポートまたは IP アドレスの変更

以下の手順を使って、Directory Server が使用するポートまたは Directory Server が接続を受け入れる IP アドレスを変更します。

Directory Server では、次に示すデフォルト・ポートが使用されます。

- 非セキュア接続の場合は 389
- セキュアな接続の場合は 636 (デジタル認証マネージャーを使用して、Directory Server が、セキュアな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、Directory Server に別のポートを割り当てることができますが、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それぞれ異なる IP アドレスを使用することができます。

Directory Server が使用するポートまたは Directory Server が接続を受け入れる IP アドレスを変更するには、以下のステップを行います。

1. System i Navigator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. 「IBM Directory Server」を右マウス・ボタン・クリックし、「プロパティ」を選択する。
5. 「ネットワーク」タブをクリックする。
6. ポート番号を変更する場合は、使用するポート番号を入力し、「OK」をクリックする。
7. IP アドレスを変更する場合は、「IP アドレス...」ボタンをクリックします。その後、次のステップに進む。
8. 「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。

### 関連情報

同一システム上で Domino LDAP とディレクトリー・サーバーをホストする

## ディレクトリー参照用のサーバーの指定

以下の情報を参考にして、参照サーバーを指定します。

Directory Server 用の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. System i Navigator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. 「IBM Directory Server」を右ボタンでクリックし、「プロパティ」を選択する。
5. 「一般」プロパティ・ページを選択する。
6. 「新規参照 (New referral)」フィールドで、参照サーバーの URL を指定する。
7. 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。

8. 「追加」をクリックする。
9. 「OK」をクリックする。

#### 関連概念

56 ページの『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 Directory Server 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。

## Directory Server 接尾部の追加および除去

以下の情報を参考にして、Directory Server の接尾部を追加または除去します。

接尾部を Directory Server 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. System i Navigator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. 「IBM Directory Server」を右マウス・ボタン・クリックし、「プロパティ」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。

Directory Server から接尾部を除去するには、次のようにしてください。

1. System i Navigator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. 「IBM Directory Server」を右マウス・ボタン・クリックして、「プロパティ」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。

#### 関連概念

14 ページの『接尾部 (命名コンテキスト)』

接尾部 (命名コンテキストともいいます) は、ローカルに保持されるディレクトリー階層の最上部の項目を識別する DN です。

#### Directory Server への接尾部の追加:

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. System i Navigator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. 「IBM Directory Server」を右マウス・ボタン・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。

#### Directory Server からの接尾部の除去:

Directory Server から接尾部を除去するには、次のようにしてください。

1. System i Navigator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. 「IBM Directory Server」を右マウス・ボタン・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。

#### プロジェクト・ユーザーへの管理者アクセスの許可

以下の情報を参考にして、ユーザー・プロファイルに管理者権限を認可します。

Directory Server 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 Directory Server 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・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となります。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となります。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 となります。

「許可ユーザーへの管理アクセスの認可」オプションと Directory Server 管理者機能 ID を選択するには、次のようなステップを行います。

1. System i Navigator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」を右クリックし、「プロパティ」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。
5. System i Navigatorで、システム名を右マウス・ボタン・クリックし、「アプリケーション管理」を選択する。
6. 「ホスト・アプリケーション」タブをクリックする。
7. 「OS/400」を展開する。
8. 「Directory Server 管理者 (Directory Server Administrator)」をクリックしてオプションを強調表示する。
9. 「カスタマイズ」ボタンをクリックする。
10. 「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切ないずれかを展開する。
11. 「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。
12. 「追加」ボタンをクリックする。
13. 「OK」をクリックして変更を保管する。
14. 「アプリケーション管理」ダイアログで「OK」をクリックする。

#### 関連概念

70 ページの『管理アクセス』

管理アクセスを使用して、個々の管理用タスクへのアクセスを制御します。

94 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』

システム・プロジェクト・バックエンドには、i5/OS 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 表記のオペレーティング・システム・オブジェクトとなります。

## 言語タグの使用可能化

以下の情報を参考にして、言語タグを使用可能にします。

言語タグを使用可能にするには、次のようにしてください (デフォルトでは使用不可)。

1. ナビゲーション領域で「サーバー管理」カテゴリーの「サーバー・プロパティの管理」をクリックする。

注: Web 管理ツールの「サーバー管理」カテゴリのタスクを使用してサーバー構成設定を変更するには、\*ALLOBJ および IOSYSCFG の特殊権限をもつ i5/OS ユーザー・プロファイルとしてサーバーに認証する必要があります。これは、そのプロファイルのパスワードでプロジェクト・ユーザーとして認証することによって実行できます。Web 管理ツールからプロジェクト・ユーザーとしてバインドするには、os400-profile=MYUSERNAME,cn=accounts,os400-sys=MYSYSTEM.COM の形式の username を入力します。この MYUSERNAME と MYSYSTEM.COM のストリングはそれぞれ、ご使用のユーザー・プロファイル名および構成済みシステム射影接尾部と置き換えられます。

2. 「一般」タブは事前選択されている。「言語タグ・サポートの使用可能化」チェック・ボックスをクリックして、それを使用可能にします。

注: 言語タグ機能を使用可能にした後、言語タグを項目の属性と関連付けると、サーバーは言語タグのある項目に戻ります。後で言語タグ機能を使用不可にした場合でも、同じものが戻されます。サーバーの動作がアプリケーションの予測どおりでないことがあるので、起こりうる問題を回避するためには、言語タグ機能を使用可能にした後では、それを使用不可にしないでください。

## LDAP ディレクトリーに対するアクセスと変更のトラッキング

以下の情報を参考にして、LDAP ディレクトリーに対するアクセスと変更を追跡します。

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. System i Navigator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. 「IBM Directory Server」を右マウス・ボタン・クリックし、「プロパティ」を選択する。
5. 「変更ログ (Change Log)」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. オプション: 「最大項目数」フィールドで、記録する変更ログの最大の項目数を指定する。「最大存続期間 (Maximum age)」フィールドで、変更ログ項目がどれだけ長く保存されるかを指定します。

注: これらのパラメーターはオプションですが、最大の項目数または最大存続期間のいずれかを指定することを強くお勧めします。いずれも指定しない場合、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=*)
```

## Directory Server のオブジェクト監査の使用可能化

以下の情報を参考にして、Directory Server のオブジェクト監査を使用可能にします。

Directory Server は、i5/OS 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、System i Navigator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。

Directory Server 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. System i Navigator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. 「IBM Directory Server」を右マウス・ボタン・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。
7. 「OK」をクリックする。

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。Directory Server を再始動する必要はありません。

### 関連概念

58 ページの『監査』

監査を使用して、特定の Directory Server トランザクションの詳細をトラックすることができます。

57 ページの『Directory Server のセキュリティー』

多彩な機能を使用して、Directory Server をセキュアにする方法を学んでください。

## 検索設定の調整

以下の情報を参考にして、ユーザーの検索機能を制御します。

Web 管理ツールを使用して、検索パラメーターを設定し、ページ検索やソート検索、サイズや時間制限、および別名参照解除オプションなどのユーザーの検索機能を制御することができます。

ページ結果によって、クライアントは検索要求から戻されたデータの量を管理できます。クライアントはすべての結果を一度に受け取る代わりに、項目のサブセット (ページ) を要求できます。以降の検索要求により、結果の次のページを表示します。これは操作が取り消されるか、最後の結果が戻されるまで続けられません。

ソート検索により、クライアントが、基準のリスト (各基準はソート・キーを表す) によりソートされた検索結果を受け取ることが可能になります。これにより、ソートの責任は、クライアント・アプリケーションからサーバーに移ります。

ディレクトリー・サーバーの検索設定を調整するには、次のようにしてください。

1. ナビゲーション領域の「サーバー管理」カテゴリーを展開し、「サーバー・プロパティーの管理」を選択する。

**注:** Web 管理ツールの「サーバー管理」カテゴリーのタスクを使用してサーバー構成設定を変更するには、\*ALLOBJ および IOSYSCFG の特殊権限をもつ i5/OS ユーザー・プロファイルとしてサーバーに認証する必要があります。これは、そのプロファイルのパスワードでプロジェクト・ユーザー

として認証することによって実行できます。 Web 管理ツールからプロジェクト・ユーザーとしてバインドするには、`os400-profile=MYUSERNAME,cn=accounts,os400-sys=MYSYSTEM.COM` の形式の `username` を入力します。この `MYUSERNAME` と `MYSYSTEM.COM` のストリングはそれぞれ、ご使用のユーザー・プロファイル名および構成済みシステム射影接尾部と置き換えられます。

2. 「**検索設定**」タブを選択する。
3. 「**検索サイズの限界**」を設定する。「**項目数**」または「**無制限**」のいずれかのラジオ・ボタンをクリックします。「**項目数**」を選択した場合は、そのフィールドで、検索で戻す最大項目数を指定する必要があります。デフォルトは 500 です。それ以上の項目数が検索基準と一致しても、それらの項目は戻されません。管理者またはこれ以上の検索サイズの限界が認可される検索限界グループのメンバーには、この限界は適用されません。
4. 「**検索時間制限**」を設定する。「**秒数**」または「**無制限**」のいずれかのラジオ・ボタンをクリックします。「**秒数**」を選択した場合は、そのフィールドに、サーバーが要求処理に費やす最大時間を指定する必要があります。デフォルトは 900 です。管理者またはこれ以上の検索時間制限が認可される検索限界グループのメンバーには、この限界は適用されません。
5. ソート検索機能を管理者に限定するには、「**管理者のみにソート検索を許可**」チェック・ボックスを選択する。
6. ページ検索機能を管理者に限定するには、「**管理者のみにページ検索を許可**」チェック・ボックスを選択する。
7. 「**別名参照解除**」のドロップダウン・メニューを展開して、次の 1 つを選択する。デフォルト設定は「**Always**」です。

**Never** 別名は参照解除されません。

**Find** 検索の開始点を検出する時には別名は参照解除され、その開始項目の下を検索する時には参照解除されません。

**Search** 検索の開始点より下の項目を検索する時には別名は参照解除されますが、開始項目の検出時には参照解除されません。

#### **Always**

別名は常に参照解除されます。すなわち、検索の開始点を検出した時、および開始項目より下の項目を検索する時の両方でこれが実行されます。Always がデフォルトの設定です。

#### **関連タスク**

224 ページの『ディレクトリー項目の検索』

以下の情報を参考にして、ディレクトリー項目を検索します。

#### **関連資料**

53 ページの『検索パラメーター』

サーバーで使用するリソース量を制限するために、管理者は検索パラメーターを使用して、ユーザーの検索能力を制限することができます。また、特定のユーザーの検索能力を拡張することもできます。

## **プロジェクト・ユーザーへの読み取りアクセスの有効化または無効化**

以下の情報を参考にして、ユーザー・プロジェクト・バックエンドに対する検索および比較操作を禁止します。

ユーザー・プロジェクト・バックエンドに対する検索および比較操作を禁止するには、次のようにします。

1. Directory Server を終了します。 `ENDTCPSVR *DIRSRV` と入力します。
2. ファイル `/QIBM/UserData/OS400/DirSrv/ibmslapd.conf` を編集します。たとえば、`EDTF '/QIBM/UserData/OS400/DirSrv/ibmslapd.conf'` と入力します。

3. テキスト `cn=Front End` を探し出します。
4. テキスト `cn=Front End` が置かれている行の直後に、テキスト `ibm-slapdSetEnv: IBMSLDAPDOS400USRPRJREAD=FALSE` が書かれた新しい行を挿入します。以下の例では、2 番目の行が挿入された行です。

```
dn: cn=Front End, cn=Configuration
ibm-slapdSetEnv: IBMSLDAPDOS400USRPRJREAD=FALSE
cn: Front End
```
5. このファイルを保存してエディターを終了します。たとえば、EDTF の使用時には、F2 を押してファイルを保存し、その後で F3 を押してエディターを終了します。
6. Directory Server を再始動します。 `STRTCPSVR *DIRSRV` と入力します。

#### 関連概念

100 ページの『プロジェクト・ユーザーへの読み取りアクセス』

デフォルトでは、LDAP 検索および比較操作を介したユーザー・プロファイル情報への読み取りアクセスが、許可ユーザーに対してシステム射影バックエンドから提供されます。プロジェクト・ユーザーへの読み取りアクセスを有効化または無効化するには、System i Navigator を使用するか、または `/QIBM/UserData/OS400/DirSrv/idsslapd-instance/etc/ibmslapd.conf` ファイル (デフォルト・サーバー・インスタンス用の `/QIBM/UserData/OS400/DirSrv/idsslapd-QUSRDIR/etc/ibmslapd.conf` ファイル) 内での構成設定を介します。

## Directory Server への情報の公開

以下の情報を参考にして、Directory Server へ情報を公開します。

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ディレクトリー・サーバーに対して特定の情報、またユーザー定義の情報も公開する構成ができます。System i Navigatorを使用して i5/OS 上でその情報を変更すると、オペレーティング・システムによってその情報がディレクトリー・サーバーに自動的に公開されます。公開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)、印刷共有情報、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。

データの公開先となる親 DN が存在しない場合は、Directory Server 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公開する他の i5/OS 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公開することもできます。

**注:** i5/OS 情報を i5/OS 上で稼働していない Directory Server に対して公開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。

i5/OS 情報をディレクトリー・サーバーに対して公開できるようにシステムを構成するには、以下の手順に従ってください。

1. System i Navigatorで、ご使用のシステムを右マウス・ボタン・クリックし、「プロパティ」を選択する。
2. 「Directory Server」タブをクリックする。
3. 公開したい情報を選択する。 公開したい情報を選択する。

**ヒント:** 複数の情報が同じ場所に公開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。次に、オペレーション・ナビゲーターは、以降の情報タイプを構成するとき、デフォルト値として 1 つの情報タイプを構成する場合に入力する値を使用します。

4. 「詳細 (Details)」をクリックする。

5. 「システム情報を公開する (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」ボタンをクリックする。表示されたダイアログで、i5/OS の公開先にしたいディレクトリー・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入力する。

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 i5/OS 情報を公開するには、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、60 ページの『Directory Server での Kerberos 認証の使用』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・ボックスによってそのディレクトリーを作成するようにプロンプトが出されます。

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、情報は公開されません。

12. 「OK」をクリックする。

注: i5/OS 情報を別のプラットフォーム上の Directory Server に対して公開することもできます。ユーザー情報とシステム情報は、IBM Directory Server 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・サーバーに対して公開する必要があります。IBM ディレクトリー・スキーマについては、16 ページの『Directory Server のスキーマ』を参照してください。

LDAP サーバー設定用 API と公開用 API により、ユーザー作成の i5/OS プログラムで他の情報を公開することもできます。これらの情報も「Directory Server」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公開エージェントといいます。そして、公開する情報（「Directory Server」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、公開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、使用不可項目としてマークされたエージェント名を 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は、System i Navigatorを使用してディレクトリー・サーバーのプロパティ・ページに移動し、公開エージェントを構成するように指示します。エージェント名の例としては、「Directory Server」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**

情報を公開します。



## 関連概念

40 ページの『公開』

Directory Server は、システムが特定の種類の情報を LDAP ディレクトリーに公開する機能を提供します。すなわち、システムは、さまざまなタイプのデータを表す LDAP 項目を作成および更新します。

Directory Server API

## LDIF ファイルのインポート

以下の情報を参考にして、LDAP データ交換形式 (LDIF) ファイルをインポートします。

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 Directory Server 間で情報を転送することができます。新規の項目をディレクトリーに追加するには、インポート・ツール (およびそれに対応する QgldImportLdif API) を使用します。インポート・ツールを使用して、項目を変更または削除することはできません。また、LDIF ファイルは、変更レコード・スタイル LDIF レコードではなく、ディレクトリー内容スタイルを使用する必要があります。入力 LDIF ファイルに、変更レコード・スタイル LDIF レコードで使用される changetype ディレクティブが入っている場合、changetype 行は、別の属性と解釈されて、項目はディレクトリーに追加されません。

標準の使用法では、エクスポート・ツール (つまり QgldExportLdif API) を使ってディレクトリー全体またはディレクトリーのサブツリーが 1 つのサーバーからエクスポートされてから、別のサーバーにインポートされます。

エクスポート・ツールとインポート・ツールは、ldapsearch および ldapadd コマンド行ユーティリティーの使用と同等ではありません。エクスポート・ツールには、通常は ldapsearch から戻されることはないいくつかの運用属性 (アクセス制御情報や項目作成タイム・スタンプなど) が含まれているのに対して、インポート・ツールは、ldapadd などの、クライアント・アプリケーションでは通常は設定できない属性を設定することができます。ldapadd ユーティリティーを -k オプション (サーバー管理制御) と一緒に使用して、これらのファイルをロードすることができます。

この手順を開始する前に、ストリーム・ファイルとして LDIF ファイルをシステムに転送してください。

LDIF ファイルを Directory Server 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、130 ページの『Directory Server の開始』を参照してください。
2. System i Navigator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. 「IBM Directory Server」を右マウス・ボタン・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。

オプションで、「インポート・データの複製 (Replicate imported data)」を選択することにより、次に開始する時にサーバーが新規にインポートしたデータを複製するようにできます。これは、マスター・サーバー上の既存のディレクトリー・ツリーに新規項目を追加する時に便利です。レプリカ・サーバー (またはピア・サーバー) を初期化するためにデータをインポートしようとする場合、このサーバーをサブライヤーとするサーバー上にはそのデータがすでに存在するため、基本的にデータを複製する必要はありません。

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。

## 関連資料

281 ページの『LDAP データ交換形式 (LDIF)』

LDAP データ交換形式は、LDAP オブジェクトおよび LDAP の更新 (追加、変更、削除、DN の変更) をテキスト・フォームで表すための標準テキスト・フォーマットです。LDIF レコードを収めたファイルを、Directory Server 間でデータを転送するのに使用するか、または **ldapadd** や **ldapmodify** のような LDAP ツールで入力として使用することができます。

244 ページの『ldapmodify および ldapadd』

LDAP modify-entry および LDAP add-entry コマンド行ユーティリティー

## LDIF ファイルのエクスポート

以下の情報を参考にして、LDAP データ交換形式 (LDIF) ファイルをエクスポートします。

別々の LDIF ファイル間で、情報を伝送することができます。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. System i Navigator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. 「IBM Directory Server」を右マウス・ボタン・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: データのエクスポート先となる LDIF ファイルの完全修飾パスを指定しなかった場合は、ファイルは、オペレーティング・システムのユーザー・プロファイルに指定されたホーム・ディレクトリーに作成されます。

5. 「ディレクトリー全体のエクスポート」または「選択したサブツリーのエクスポート」、さらに「操作属性のエクスポート」を実行するかどうかを指定します。エクスポートされる操作属性は creatorsName、createTimestamp、modifiersName、および modifyTimestamp です。

### Lotus Notes:

1. 取り込みのためにデータを V5R3 以前のディレクトリー・サーバーにエクスポートする時には、「操作属性のエクスポート」は選択しないでください。これらの操作属性は V5R3 以前のディレクトリー・サーバーにはインポートできません。
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。-L オプションを使用して、出力をファイルに転送します。
3. 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、System i Navigatorで該当ファイルを右マウス・ボタン・クリックし、「許可」を選択します。

## 関連資料

281 ページの『LDAP データ交換形式 (LDIF)』

LDAP データ交換形式は、LDAP オブジェクトおよび LDAP の更新 (追加、変更、削除、DN の変更) をテキスト・フォームで表すための標準テキスト・フォーマットです。LDIF レコードを収めたファイルを、Directory Server 間でデータを転送するのに使用するか、または **ldapadd** や **ldapmodify** のような LDAP ツールで入力として使用することができます。

265 ページの『ldapsearch』

LDAP 検索コマンド行ユーティリティー

## HTTP サーバー妥当性検査リストから Directory Server へのユーザーのコピー

以下の情報を参考にして、HTTP サーバー妥当性検査リストから Directory Server へユーザーをコピーします。

HTTP サーバーを現在使用中か、あるいは以前に使用したことがある場合は、インターネット・ユーザーとそのパスワードを保管するために妥当性検査リストを作成していることがあります。LDAP 認証をサポートする WebSphere Application Server、Portal Server、およびその他のアプリケーションに移動する時に、既存のインターネット・ユーザーとそのパスワードを継続して使用したいことがあります。これを実行するには、「ディレクトリーへの妥当性検査リストのコピー」API、QGLDCPYVL を使用することができます。

QGLDCPYVL は妥当性検査リストから項目を読み取って、ローカル・ディレクトリー・サーバーと対応の LDAP オブジェクトを作成します。このオブジェクトは userPassword 属性をもった骨組みの inetOrgPerson 項目になり、この中に妥当性検査リスト項目からのパスワード情報のコピーが入れられます。この API を呼び出す方法や時点はユーザーが決定できます。これは、変更されない妥当性検査リストでは 1 度の操作として使用され、あるいは新規の妥当性検査リスト項目を反映するために、ディレクトリー・サーバーを更新するためのスケジュールされたジョブとして使用することもあります。

以下に例を示します。

```
CALL PGM(QSYS/QGLDCPYVL) PARM('HTTPVLDL MYLIB ' 'cn=administrator' X'00000000' 'secret'
X'00000000' 'cn=users,o=my company' X'00000000' '' X'00000000' X'00000000')
```

### 関連概念

Lightweight Directory Access Protocol (LDAP) API

Directory Server API の詳細は、『Lightweight Directory Access Protocol (LDAP) APIs』を参照してください。

### 関連タスク

128 ページの『シナリオ: HTTP サーバー妥当性検査リストから Directory Server へのユーザーのコピー』

HTTP サーバー妥当性検査リストから Directory Server へユーザーをコピーする例。

## インスタンスの管理

- | i5/OS システム上に複数の Directory Server を置くことができます。それぞれのサーバーが、いわゆるインスタンスになります。前のリリースの i5/OS で Directory Server を使用していた場合、それは、QUSRDIR という名前のインスタンスにマイグレーションされます。Directory Server の複数のインスタンスを作成して、アプリケーションがそれらのサービスを受けられるようにすることができます。
- | Directory Server インスタンスのそれぞれの固有性は、どの IP アドレスまたはポート (またはこの両方) をインスタンスが listen するように構成されているかによって定義されます。また、実行される各 Directory Server インスタンスは、それぞれ固有のデータベース、変更ログ、および構成ファイルを持っている必要があります。競合しあったサーバー・インスタンスを作成して構成することは可能ですが、別のアクティブなサーバー・インスタンスと競合するサーバー・インスタンスを開始しようとすると、2 番目のインスタンスは開始せずに、エラー・メッセージが発行されます。
- | Directory Server インスタンスは、コンピューター上で Directory Server を実行するのに必要なすべてのファイルで構成されます。
- | Directory Server インスタンス・ファイルは、次のもので構成されます。
  - | • ibmslapd.conf ファイル (構成ファイル)
  - | • スキーマ・ファイル

- | • ログ・ファイル
- | • 一時状況ファイル

| Directory Server インスタンスのファイルは、`idsslapd-instance_name` という名前のディレクトリーに保管され  
| ます。`instance_name` は、Directory Server インスタンスの名前です。 `idsslapd-instance_name` ディレクト  
| リーは、`/QIBM/UserData/OS400/DirSrv` ディレクトリー内にあります。

| 各 Directory Server インスタンスは、その作成時に新規のアプリケーションをデジタル証明書マネージャー  
| (DCM) に登録します。新規の Directory Server インスタンスには、`QIBM_DIRECTORY_SERVER_`  
| `<instance-name>` という名前が付きます。 SSL を使用する必要がある場合、DCM を使用して、デジタル  
| 証明書を Directory Server インスタンスに関連付ける必要があります。どの Directory Server インスタンス  
| も、その開始時にサーバーとして System i Navigator に登録されます。よって、System i Navigator での追  
| 跡が可能になります。

| Directory Server インスタンスのジョブの場合、そのジョブ名はインスタンス名に設定されます。したがっ  
| て、たとえば QUSRDIR インスタンスには、`xxxxxx/QDIRSRV/QUSRDIR` という完全修飾ジョブ名が付き  
| ます。 `'xxxxxx'` は、ジョブの開始時に決定されるジョブ番号です。これは、現在 Directory Server を使用  
| しているユーザーのものとは異なります。なぜなら、そのジョブ名は `xxxxxx/QDIRSRV/QDIRSRV` である  
| からです。

| インスタンスを管理するには、次のようにします。

- | 1. System i Navigator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. 「IBM Tivoli Directory Server」を右クリックし、「Manage Instances (インスタンスの管理)」を選択  
| する。

| 定期的にインスタンスを保存する場合、`<instance-name>CF` ライブラリーをデータベース・ディレクトリー  
| とともに保存する必要があります。

## 管理グループのタスク

以下の情報を参考にして、管理グループを管理します。

管理グループには、管理者間で単一の ID とパスワードを共用する必要がなく、管理機能を実行できる機  
能があります。管理グループのメンバーは、自分固有の ID とパスワードをもっています。管理グルー  
プ・メンバー DN は相互に一致してはならず、また、IBM Directory Server 管理者 DN と一致してもいけ  
ません。逆に言えば、IBM Directory Server 管理者 DN は、どの管理グループ・メンバーの DN と一致  
するものであってはなりません。

また、この規則は IBM Directory Server 管理者および管理グループ・メンバーの Kerberos または  
Digest-MD5 ID にも適用されます。これらの DN は IBM Directory Server の複製サプライヤーのどの DN  
とも一致するものであってはいけません。また、これは、IBM Directory Server の複製サプライヤーの DN  
が管理グループ・メンバー DN または IBM Directory Server 管理者 DN のいずれとも一致してはいけな  
いことを意味します。

注: IBM Directory Server の複製サプライヤー DN は互いに一致していてもかまいません。

### 関連概念

70 ページの『管理アクセス』

管理アクセスを使用して、個々の管理用タスクへのアクセスを制御します。

## 管理グループの使用可能化

以下の情報を参考にして、管理グループを使用可能にします。

この操作を実行するには、IBM Directory Server 管理者でなければなりません。

1. Web 管理ツールのナビゲーション領域の「サーバー管理」カテゴリを展開し、「管理グループの管理」をクリックする。

**注:** Web 管理ツールの「サーバー管理」カテゴリのタスクを使用してサーバー構成設定を変更するには、\*ALLOBJ および IOSYSCFG の特殊権限をもつ i5/OS ユーザー・プロファイルとしてサーバーに認証する必要があります。これは、そのプロファイルのパスワードでプロジェクト・ユーザーとして認証することによって実行できます。Web 管理ツールからプロジェクト・ユーザーとしてバインドするには、os400-profile=MYUSERNAME,cn=accounts,os400-sys=MYSYSTEM.COM の形式の username を入力します。この MYUSERNAME と MYSYSTEM.COM のストリングはそれぞれ、ご使用のユーザー・プロファイル名および構成済みシステム射影接尾部と置き換えられます。

2. 管理グループを使用可能または使用不可にするには、「管理グループの使用可能化」の横のチェック・ボックスをクリックする。このチェック・ボックスにチェックすると、管理グループが使用可能になります。
3. 「OK」をクリックする。

**注:** 管理グループを使用不可にした場合は、ログインしたメンバーは、そのメンバーの再バインドが必要となるまで、管理操作を続行できます。

## 管理グループ・メンバーの追加、編集、および除去

以下の情報を参考にして、管理グループ・メンバーの追加、編集、および除去を行います。

**前提条件:** この操作を実行するには、IBM Directory Server 管理者でなければなりません。

1. Web 管理ツールのナビゲーション領域の「サーバー管理」カテゴリを展開し、「管理グループの管理」をクリックする。

**注:** Web 管理ツールの「サーバー管理」カテゴリのタスクを使用してサーバー構成設定を変更するには、\*ALLOBJ および IOSYSCFG の特殊権限をもつ i5/OS ユーザー・プロファイルとしてサーバーに認証する必要があります。これは、そのプロファイルのパスワードでプロジェクト・ユーザーとして認証することによって実行できます。Web 管理ツールからプロジェクト・ユーザーとしてバインドするには、os400-profile=MYUSERNAME,cn=accounts,os400-sys=MYSYSTEM.COM の形式の username を入力します。この MYUSERNAME と MYSYSTEM.COM のストリングはそれぞれ、ご使用のユーザー・プロファイル名および構成済みシステム射影接尾部と置き換えられます。

2. 「管理グループの管理」パネルで、「追加」をクリックする。
3. 「管理グループ・メンバーの追加」パネルで、次のようにする。
  - a. メンバーの管理者 DN (これは有効な DN 構文であること) を入力する
  - b. メンバーのパスワードを入力する。
  - c. 確認のために、メンバーのパスワードを再入力する。

- d. オプション: メンバーの Kerberos ID を入力する。この Kerberos ID は `ibm-kn` または `ibm-KerberosName` 形式でなければなりません。この値は大/小文字の区別がないので、例えば、`ibm-kn=root@TEST.ROCHESTER.IBM.COM` は `ibm-kn=ROOT@TEST.ROCHESTER.IBM.COM` と等しくなります。
4. オプション: メンバーの **Digest-MD5 ユーザー名** を入力する。  
**注:** Digest-MD5 ユーザー名は大/小文字の区別があります。
5. 「**OK**」をクリックする。
6. 管理グループに追加したいメンバーごとに、この手順を繰り返す。

メンバー管理者 DN、Digest-MD5 ユーザー名 (指定した場合) および Kerberos ID (指定した場合) は管理グループ・メンバー・リスト・ボックスに表示されます。

管理グループ・メンバーを変更または除去するには、上記と同じ手順に従いますが、「**管理グループの管理**」パネルでは「**編集**」および「**削除**」のボタンを使用してください。

- | 管理者グループ・メンバーのパスワードは、ディレクトリー・サーバー属性変更 (CHGDIRSVRA) コマンドを使用して変更することもできます。バインド DN `cn=adminuser1` を持つ管理グループ・メンバーのパスワードを `newpassword` に変更するには、次のようなコマンドを使用します。
- | `CHGDIRSVRA INSTANCE(QUSRDIR) DN('cn=adminuser1' 'newpassword')`

## 検索限界グループのタスク

以下の情報を参考にして、検索限界グループを管理します。

リソースが過剰に使用され、その結果、サーバー・パフォーマンスの低下を防止するために、指定されたサーバーでの検索要求に対して、検索限界が設けられます。管理者は、サーバーの構成時にこれらの検索限界を、検索のサイズと期間で設定します。

これらの検索限界から免除されるのは、管理者および管理グループのメンバーのみであり、他のすべてのユーザーに対して適用されます。ただし、必要に応じて、管理者は一般ユーザーより柔軟な検索限界を設定できる検索限界グループを作成することができます。この方法では、管理者は、ユーザーのグループに対して特殊な検索特権を付与することができます。

検索限界グループの管理には、Web 管理ツールが使用されます。

### 関連資料

53 ページの『検索パラメーター』

サーバーで使用するリソース量を制限するために、管理者は検索パラメーターを使用して、ユーザーの検索能力を制限することができます。また、特定のユーザーの検索能力を拡張することもできます。

## 検索限界グループの作成

以下の情報を参考にして、検索限界グループを作成します。

検索限界グループを作成するには、Web 管理ツールを使用してそのグループ項目を作成する必要があります。

1. ナビゲーション領域の「**ディレクトリー管理**」カテゴリーを展開し、「**項目の追加**」をクリックする。あるいは、「**項目の管理**」をクリックし、場所 (`cn=IBMpolicies` または `cn=localhost`) を選択してから、「**追加**」をクリックしてください。`cn=IBMpolicies` にある項目は複製されますが、`cn=localhost` の項目は複製されません。

2. グループ・オブジェクト・クラスの 1 つを「構造オブジェクト・クラス」メニューから選択する。
3. 「次へ」をクリックします。
4. 「使用可能」メニューから「**ibm-searchLimits**」補助オブジェクト・クラスを選択して、「追加」をクリックする。追加する必要がある追加の補助オブジェクト・クラスごとに、このプロセスを繰り返してください。また、補助オブジェクト・クラスを選択して「除去」をクリックすると、「選択済み」メニューからその補助オブジェクト・クラスを削除できます。
5. 「次へ」をクリックします。
6. 「**相対 DN**」フィールドに、追加しているグループの相対識別名 (RDN) を入力する。例えば、cn=Search Group1 などです。
7. 「**親 DN**」フィールドに、選択したツリー項目の識別名を入力する。例えば、cn=localhost などです。また、「参照」をクリックして、リストから親 DN を選択することもできます。選択項目を指定し、「**選択**」をクリックして、「親 DN」を指定します。「**親 DN**」のデフォルト値は、ツリーで選択された項目になります。

注: このタスクを「**項目の管理**」パネルから開始した場合、このフィールドには値が入力されていません。「**親の識別名 (Parent DN)**」は、「**追加 (Add)**」をクリックして項目の追加プロセスが開始される前に選択されました。

8. 「**必須属性 (Required attributes)**」タブで、必須属性の値を入力します。
  - **cn** は、前に指定した相対 DN である。
  - 「**ibm-searchSizeLimit**」フィールドでは、検索のサイズを制限するための項目数を指定する。この数値は、0 から 2,147,483,647 までの範囲にすることができます。0 の設定は、「**無制限**」と同じになります。
  - 「**ibm-searchTimeLimit**」フィールドでは、検索の期間を制限するための秒数を指定する。この数値は、0 から 2,147,483,647 までの範囲にすることができます。0 の設定は、「**無制限**」と同じになります。
  - 選択したオブジェクト・クラスによっては、「**メンバー**」または「**uniqueMember**」フィールドが表示される場合があります。これらは、作成しているグループのメンバーです。この項目は DN の形式で、cn=Bob Garcia,ou=austin,o=ibm,c=us などとなります。
9. 特定の属性に複数値を追加したい場合は、「**複数値**」をクリックして、一度に 1 つずつ値を追加します。複数値の追加が終了したら、「**OK**」をクリックする。この値は、属性で表示された拡張可能なメニューに追加されます。
10. サーバーで言語タグが使用可能になっている場合は、「**言語タグ値**」をクリックして、言語タグ記述子の追加または除去を行う。
11. 「**他の属性**」をクリックする。
12. 「**他の属性**」タブで、必要に応じて属性の値を入力する。詳しくは、226 ページの『**バイナリー属性の変更**』を参照してください。
13. 「**完了**」をクリックして項目を作成する。

## 検索限界グループの変更

以下の情報を参考にして、検索限界グループを変更します。

検索限界グループのサイズまたは時間制限の属性を変更することができます。また、グループのメンバーの追加と除去を行うこともできます。Web 管理ツールを使用して、検索限界グループを変更します。

1. ナビゲーション領域で「ディレクトリー管理」のカテゴリーを展開し (まだ開いていない場合)、「項目の管理」をクリックしてください。各種のサブツリーを展開して、作業を行う項目を選択できます。右側のツールバーから「属性の編集 (Edit attributes)」をクリックします。
2. 「必須属性 (Required attributes)」タブで、必須属性の値を入力します。 バイナリー値の追加に関する情報は、226 ページの『バイナリー属性の変更』を参照してください。特定の属性に複数値を追加したい場合は、「複数値」をクリックして、一度に 1 つずつ値を追加します。
3. 「オプション属性 (Optional attributes)」をクリックします。
4. 「オプション属性 (Optional attributes)」タブで、必要に応じてオプション属性の値を入力します。 特定の属性に複数値を追加したい場合は、「複数値」をクリックして、一度に 1 つずつ値を追加します。
5. 「Memberships (メンバーシップ)」をクリックします。
6. 何らかのグループを作成してある場合は、「メンバーシップ (Memberships)」タブで以下の作業を行います。
  - 項目を静的グループ・メンバーシップのメンバーにするには、「使用可能なグループ (Available groups)」からグループを選択して、「追加 (Add)」をクリックします。
  - グループから項目を除去するには、「静的グループ・メンバーシップ (Static group memberships)」からグループを選択し、「除去」をクリックします。
7. 項目がグループ項目の場合は、「メンバー (Members)」タブが使用できます。「メンバー (Members)」タブには、選択されたグループのメンバーが表示されます。グループに対するメンバーの追加と除去を行うことができます。
  - グループにメンバーを追加するには、次のようにします。
    - a. 「メンバー (Members)」タブの「複数値 (Multiple values)」をクリックするか、「メンバー (Members)」タブで「メンバー (Members)」をクリックします。
    - b. 「メンバー (Member)」フィールドに、追加する項目の識別名を入力します。
    - c. 「追加」をクリックします。
    - d. 「OK」をクリックします。
  - グループからメンバーを除去するには、次のようにします。
    - a. 「メンバー (Members)」タブの「複数値 (Multiple values)」をクリックするか、「メンバー (Members)」タブをクリックして「メンバー (Members)」をクリックします。
    - b. 除去する項目を選択します。
    - c. 「除去」をクリックします。
    - d. 「OK」をクリックします。
  - メンバーのリストを更新するには、「更新」をクリックします。
8. 項目を変更するには、「OK」をクリックします。

## 検索限界グループのコピー

以下の情報を参考にして、検索限界グループをコピーします。

同じ検索限界グループを localhost と IBMpolicies の両方に入れたい場合は、検索限界グループのコピーが便利です。また、既存のグループと類似情報を持ち、少しだけ違う新しいグループを作成したい場合にも、これが便利です。

1. ナビゲーション領域で「ディレクトリー管理」のカテゴリーを展開し (まだ開いていない場合)、「項目の管理」をクリックしてください。各種のサブツリーを展開して、作業を行う項目 (John Doe など) を選択できます。右側のツールバーから「コピー (Copy)」をクリックします。



2. 「識別名 (DN)」フィールドで相対識別名 (RDN) の項目を変更します。たとえば、cn=John Doe を cn=Jim Smith に変更します。
3. 「必須属性 (Required attributes)」タブで、cn 項目を新しい相対識別名 (RDN) に変更します。この例の場合は Jim Smith になります。
4. 必要に応じ、他の必須属性に変更を加えます。この例では、sn 属性を Doe から Smith に変更します。
5. 必要な変更処理が終了したら、「OK」をクリックして新規項目を作成します。新規項目 Jim Smith が、項目リストの一番下に追加されます。

## 検索限界グループの除去

以下の情報を参考にして、検索限界グループを除去します。

1. ナビゲーション領域で「ディレクトリー管理」のカテゴリーを展開し (まだ開いていない場合)、「項目の管理」をクリックしてください。各種のサブツリーを展開して、作業を行うサブツリー、接尾部、または項目を選択できます。右側のツールバーから「削除」をクリックします。
2. 削除を確認するプロンプトが出されます。「OK」をクリックします。この項目がディレクトリーから削除され、項目のリストが再び表示されます。

## プロキシ許可グループのタスク

以下の情報を参考にして、プロキシ許可グループを管理します。

プロキシ許可グループのメンバーは Directory Server にアクセスして、複数のユーザーに代わって多くのタスクを実行できますが、各ユーザーに対する再バインドは不要です。プロキシ許可グループのメンバーは認証された ID とみなすことができますが、管理者または管理グループのメンバーは除外されます。

プロキシ許可の管理には、Web 管理ツールが使用されます。

### 関連概念

71 ページの『プロキシ許可』

プロキシ許可は特殊な形式の認証です。このプロキシ許可メカニズムを使用することによって、クライアント・アプリケーションはディレクトリーに対して自身の識別をバインドできますが、ターゲット・ディレクトリーへのアクセスでは、他のユーザーの代理として操作の実行が許可されます。トラステッド・アプリケーションまたはユーザーの 1 組が、複数のユーザーの代理として Directory Server にアクセスすることができます。

## プロキシ許可グループの作成

以下の情報を参考にして、プロキシ許可グループを作成します。

1. ナビゲーション領域の「ディレクトリー管理」カテゴリーを展開し、「項目の追加」をクリックする。あるいは、「項目の管理」をクリックし、場所 (cn=ibmPolicies または cn=localhost) を選択してから、「追加」をクリックしてください。
2. 「構造オブジェクト・クラス」メニューから「groupof Names」オブジェクト・クラスを選択する。
3. 「次へ」をクリックします。
4. 「使用可能」メニューから「ibm-proxyGroup」補助オブジェクト・クラスを選択して、「追加」をクリックする。追加したい追加補助オブジェクト・クラスごとに、このプロセスを繰り返してください。
5. 「次へ」をクリックします。
6. 「相対 DN」フィールドでは、「cn=proxyGroup」を入力する。

7. 「親の識別名 (Parent DN)」フィールドに、選択したツリー項目の識別名 (たとえば、cn=localhost など) を入力します。「参照」をクリックして、リストから「親の識別名」を選択することもできます。選択した項目を指定して「選択」をクリックし、任意の「親の識別名」を指定してください。「親の DN」のデフォルト値は、ツリーで選択された項目になります。

注: このタスクを「項目の管理」パネルから開始した場合は、このフィールドには値が事前に入力されています。「親の識別名 (Parent DN)」は、「追加 (Add)」をクリックして項目の追加プロセスが開始される前に選択されました。

8. 「必須属性 (Required attributes)」タブで、必須属性の値を入力します。
  - **cn** は proxyGroup である。
  - メンバーは DN の形式で、cn=Bob Garcia,ou=austin,o=ibm,c=us などとなる。

バイナリー値の追加について詳しくは、226 ページの『バイナリー属性の変更』を参照してください。

9. 特定の属性に複数値を追加したい場合は、「複数値」をクリックして、一度に 1 つずつ値を追加します。

注: cn 値については、複数の値を作成しないでください。このプロキシー許可グループは、予約済み名の proxyGroup を指定する必要があります。

複数値の追加が終了したら、「OK」をクリックする。この値は、属性で表示された拡張可能なメニューに追加されます。

10. サーバーで言語タグが使用可能になっている場合は、「言語タグ値」をクリックして、言語タグ記述子の追加または除去を行う。
11. 「他の属性」をクリックする。
12. 「他の属性」タブで、必要に応じて属性の値を入力します。バイナリー値の追加について詳しくは、226 ページの『バイナリー属性の変更』を参照してください。
13. 特定の属性に複数値を追加したい場合は、「複数値」をクリックして、一度に 1 つずつ値を追加します。複数値の追加が終了したら、「OK」をクリックする。この値は、属性で表示された拡張可能なメニューに追加されます。
14. サーバーで言語タグが使用可能になっている場合は、「言語タグ値」をクリックして、言語タグ記述子の追加または除去を行う。
15. 「完了」をクリックして項目を作成する。

## プロキシー許可グループの変更

以下の情報を参考にして、プロキシー・グループを変更します。

プロキシー許可グループは、Web 管理ツールを使用し、グループのメンバーを追加または削除するなどして変更できます。

1. ナビゲーション領域で「ディレクトリー管理」のカテゴリーを展開し (まだ開いていない場合)、「項目の管理」をクリックしてください。各種のサブツリーを展開して、作業を行う項目を選択できます。右側のツールバーから「属性の編集 (Edit attributes)」をクリックします。
2. 「必須属性 (Required attributes)」タブで、必須属性の値を入力します。バイナリー値の追加に関する情報は、226 ページの『バイナリー属性の変更』を参照してください。特定の属性に複数値を追加したい場合は、「複数値」をクリックして、一度に 1 つずつ値を追加します。
3. 「オプション属性 (Optional attributes)」をクリックします。

4. 「**オプション属性 (Optional attributes)**」タブで、必要に応じてオプション属性の値を入力します。特定の属性に複数值を追加したい場合は、「**複数值**」をクリックして、一度に 1 つずつ値を追加します。
5. 「**Memberships (メンバーシップ)**」をクリックします。
6. 何らかのグループを作成してある場合は、「**メンバーシップ (Memberships)**」タブで以下の作業を行います。
  - 項目を**静的グループ・メンバーシップ**のメンバーにするには、「**使用可能なグループ (Available groups)**」からグループを選択して、「**追加 (Add)**」をクリックします。
  - グループから項目を除去するには、「**静的グループ・メンバーシップ (Static group memberships)**」からグループを選択し、「**除去**」をクリックします。
7. 項目がグループ項目の場合は、「**メンバー (Members)**」タブが使用できます。「**メンバー (Members)**」タブには、選択されたグループのメンバーが表示されます。グループに対するメンバーの追加と除去を行うことができます。
  - グループにメンバーを追加するには、次のようにします。
    - a. 「**メンバー (Members)**」タブの「**複数值 (Multiple values)**」をクリックするか、「**メンバー (Members)**」タブで「**メンバー (Members)**」をクリックします。
    - b. 「**メンバー (Member)**」フィールドに、追加する項目の識別名を入力します。
    - c. 「**追加**」をクリックします。
    - d. 「**OK**」をクリックします。
  - グループからメンバーを除去するには、次のようにします。
    - a. 「**メンバー (Members)**」タブの「**複数值 (Multiple values)**」をクリックするか、「**メンバー (Members)**」タブをクリックして「**メンバー (Members)**」をクリックします。
    - b. 除去する項目を選択します。
    - c. 「**除去**」をクリックします。
    - d. 「**OK**」をクリックします。
  - メンバーのリストを更新するには、「**更新**」をクリックします。
8. 項目を変更するには、「**OK**」をクリックします。

## プロキシー許可グループのコピー

以下の情報を参考にして、プロキシー許可グループをコピーします。

同じプロキシー許可グループを localhost と IBMpolicies の両方に入れたい場合は、プロキシー許可グループのコピーが便利です。

1. ナビゲーション領域で「**ディレクトリー管理**」のカテゴリーを展開し (まだ開いていない場合)、「**項目の管理**」をクリックしてください。各種のサブツリーを展開して、作業を行う項目 (John Doe など) を選択できます。右側のツールバーから「**コピー (Copy)**」をクリックします。
2. 「**識別名 (DN)**」フィールドで**相対識別名 (RDN)**の項目を変更します。たとえば、cn=John Doe を cn=Jim Smith に変更します。
3. 「**必須属性 (Required attributes)**」タブで、cn 項目を新しい**相対識別名 (RDN)**に変更します。この例の場合は Jim Smith になります。
4. 必要に応じて、他の**必須属性**に変更を加えます。この例では、sn 属性を Doe から Smith に変更します。
5. 必要な変更処理が終了したら、「**OK**」をクリックして新規項目を作成します。新規項目 Jim Smith が、項目リストの一番下に追加されます。

## プロキシー許可グループの除去

以下の情報を参考にして、プロキシー許可グループを除去します。

1. ナビゲーション領域で「ディレクトリー管理」のカテゴリーを展開し (まだ開いていない場合)、「項目の管理」をクリックしてください。各種のサブツリーを展開して、作業を行うサブツリー、接尾部、または項目を選択できます。右側のツールバーから「削除」をクリックします。
2. 削除を確認するプロンプトが出されます。「OK」をクリックします。この項目がディレクトリーから削除され、項目のリストが再び表示されます。

## 固有属性タスク

以下の情報を参考にして、固有属性を管理します。

固有属性の管理は、Web 管理ツールの「サーバー管理」カテゴリーを介して行われます。

注: それぞれの属性単位では、言語タグは固有属性と互いに排他的に使用されます。特にその属性を固有属性として指定した場合は、それと関連付ける言語タグをもつことはできません。

注: Web 管理ツールの「サーバー管理」カテゴリーのタスクを使用してサーバー構成設定を変更するには、\*ALLOBJ および IOSYSCFG の特殊権限をもつ i5/OS ユーザー・プロファイルとしてサーバーに認証する必要があります。これは、そのプロファイルのパスワードでプロジェクト・ユーザーとして認証することによって実行できます。Web 管理ツールからプロジェクト・ユーザーとしてバインドするには、os400-profile=MYUSERNAME,cn=accounts,os400-sys=MYSYSTEM.COM の形式の username を入力します。この MYUSERNAME と MYSYSTEM.COM のストリングはそれぞれ、ご使用のユーザー・プロファイル名および構成済みシステム射影接尾部と置き換えられます。

### 関連概念

102 ページの『固有属性』

固有属性の機能により、指定された属性はディレクトリー内で常に固有な値をもつようにすることができます。

### 関連タスク

159 ページの『固有属性リストの作成』

以下の情報を参考にして、固有属性リストを作成します。

160 ページの『固有属性リストからの項目除去』

以下の情報を参考にして、固有属性リストから項目を削除します。

## 属性を固有属性と指定できるかどうかの判別

以下の情報を参考にして、属性を固有属性と指定できるかどうかを判別します。

すべての属性を固有として指定できるわけではありません。属性を固有属性と指定できない場合の条件を、以下のリストで参照してください。

- 2 進数属性、操作属性、構成属性、および objectclass 属性は固有として指定できません。
- 既存の競合値を持った属性は、固有属性と指定できません。
- それぞれの属性単位では、言語タグは固有属性と互いに排他的に使用されます。特定の属性を固有属性として指定した場合は、それと関連付ける言語タグをもつことはできません。

Web 管理ツール「Manage unique attributes task (固有属性の管理タスク)」には、最初の条件を満たす属性のみが表示されます。管理者としてバインディングを実行した後、ldapexop コマンドを実行すれば、同じ属性リストが表示されます。固有属性の可能性のある属性のリストを表示するには、次のように指定します。

```
ldapexop -op getattributes -attrType unique -matches true
```

固有属性の可能性のない属性のリストを表示するには、次のように指定します。

```
ldapexop -op getattributes -attrType unique -matches false
```

固有属性と指定できるものとしてリストされた属性の中には、競合する値を持っていて、固有属性にできないものもあります。特定の属性を固有属性と指定できるかどうかを判別するには、`ldapexop` コマンドを使用してください。例えば、コマンド

```
ldapexop -op uniqueattr -a uid
```

は、`uid` 属性を固有属性にできるかどうかを示します。またこれは、属性の競合値 (ある場合) もリストします。

`ldapexop` コマンドが、競合値があることを示した場合、`ldapsearch` コマンドを使用して、該当する値を持った項目を見つけることができます。たとえば、以下のコマンドは、`uid=jsmith` を持つすべての項目をリストします。

```
ldapsearch -b "" -s sub "(uid=jsmith)"
```

## 固有属性リストの作成

以下の情報を参考にして、固有属性リストを作成します。

1. ナビゲーション領域で「サーバー管理」カテゴリを拡張する。「固有属性の管理」をクリックします。
2. 固有属性に追加したい属性を「使用可能な属性」メニューから選択する。使用可能な属性としてリストされるのは、固有属性として指定できるもので、例えば、`sn` などです。
3. 「**cn=localhost** への追加」または「**cn=IBMpolicies** への追加」のいずれかをクリックする。これらの 2 つのコンテナの相違点は、`cn=IBMpolicies` 項目は複製されますが、`cn=localhost` 項目は複製されません。属性は、該当するリスト・ボックスに表示されます。両方のコンテナに同じ属性をリストすることができます。

**注:** ある項目を `cn=localhost` と `cn=IBMpolicies` の両方に作成した場合は、これらの 2 つの項目を合併した結果が固有属性リストとなります。例えば、属性 `cn` と `employeeNumber` が `cn=localhost` に固有として指定され、`cn` と `telephoneNumber` が `cn=IBMpolicies` に固有として作成された場合は、サーバーは属性 `cn`、`employeeNumber`、および `telephoneNumber` を固有属性として扱います。

4. 固有属性として追加したい属性ごとに、このプロセスを繰り返す。
5. 「OK」をクリックして変更を保管する。

固有属性項目を追加または変更する時に、リストされた固有属性タイプのいずれかに固有の制約を設定すると、エラーが起こる結果となり、その項目はディレクトリーで追加または作成されません。項目を作成または変更する前に、この問題を解決し、追加または変更するためのコマンドを再発行する必要があります。例えば、固有属性項目をディレクトリーに追加していて、リストされた固有属性タイプの 1 つのテーブルで固有の制約の設定が失敗した場合 (すなわち、データベース中に重複した値をもつ) には、固有属性項目はディレクトリーに追加されません。エラーが検出されます。

アプリケーションが、既存のディレクトリー項目を複製する属性の値でディレクトリーに項目を追加しようとすると、LDAP サーバーからの結果コード 20 のエラー (LDAP: エラー・コード 20 - 属性または値が存在する) が出力されます。

サーバーが開始されると、固有属性のリストが検索されて、各項目に DB2 制約が存在するかどうかを判別されます。この制約が `bulkload` ユーティリティーによって除去されたか、あるいはユーザーが手動で除去

したために、属性の制約が存在しない場合は、それは固有属性リストから除去されて、エラー・ログ `ibmslapd.log` にエラー・メッセージが記録されます。例えば、属性 `cn` が `cn=uniqueattributes,cn=localhost` に固有として指定されて、それに対する DB2 制約がない場合は、次のメッセージが記録されます。

```
Values for the attribute CN are not unique.
The attribute CN was removed from the unique attribute
entry: CN=UNIQUEATTRIBUTES,CN=LOCALHOST
```

#### 関連概念

158 ページの『固有属性タスク』

以下の情報を参考にして、固有属性を管理します。

### 固有属性リストからの項目除去

以下の情報を参考にして、固有属性リストから項目を削除します。

固有属性が `cn=uniqueattribute,cn=localhost` と `cn=uniqueattribute,cn=IBMpolicies` の両方に存在し、これが片方の項目のみから削除された場合は、サーバーはその属性を継続して固有属性として扱います。この属性は、両方の項目から除去された時に非固有となります。

1. ナビゲーション領域の「サーバー管理」カテゴリーを展開し、「固有属性の管理」をクリックする。
2. 該当するリスト・ボックスの属性をクリックして、除去したい属性を固有属性リストから選択する。
3. 「除去」をクリックする。
4. リストから除去したい属性ごとに、このプロセスを繰り返す。
5. 「OK」をクリックして変更を保管する。

注: 最後の固有属性を `cn=localhost` または `cn=IBMpolicies` のリスト・ボックスから除去した場合は、そのリスト・ボックスのコンテナ項目 `cn=uniqueattribute,cn=localhost` または `cn=uniqueattribute,cn=IBMpolicies` は自動的に削除されます。

#### 関連概念

158 ページの『固有属性タスク』

以下の情報を参考にして、固有属性を管理します。

### パフォーマンス・タスク

以下の情報を参考にして、パフォーマンスの設定値を調整します。

次のいずれかを変更することにより、Directory Server のパフォーマンス設定を調整できます。

- ACL キャッシュ・サイズ、項目キャッシュ・サイズ、フィルター・キャッシュに保管する最大検索数、およびフィルター・キャッシュ内にキャッシュする最大規模の検索。
- データベース接続とサーバー・スレッドの数。
- 属性キャッシュ設定値
- サーバーのトランザクション設定値。

#### 関連概念

103 ページの『サーバー・キャッシュ』

LDAP キャッシュは、将来の利用のために照会、応答、およびユーザー認証などの LDAP 情報の保管に使用されるメモリー内の高速記憶域バッファーです。LDAP キャッシュのチューニングはパフォーマンスの向上のために重要です。

## データベース接続およびキャッシュ設定値の設定

以下の情報を参考にして、データベース接続およびキャッシュの設定値を設定します。

データベース接続およびキャッシュ設定値を設定するには、次のようにしてください。

1. Web 管理ツールのナビゲーション領域で「**サーバー・プロパティの管理**」カテゴリを展開して、右ペインの「**パフォーマンス**」タブを選択する。
2. 「**データベース接続数**」を指定する。これは、サーバーで使用される DB2 接続数です。指定する必要がある最小数は 4 です。デフォルト設定は 15 です。LDAP サーバーが高ボリュームのクライアント要求を受け取るか、あるいはクライアントが「接続が拒否された」のエラーを受け取った場合には、DB2 にサーバーで設定した接続数の設定を増やすことで、結果が良くなる場合があります。接続の最大数は、DB2 データベースの設定によって決定されます。指定する接続数についてのサーバー制限がない場合、それぞれの接続でリソースが消費されます。
3. 「**複製でのデータベース接続数**」を指定する。これは、複製のためにサーバーで使用される DB2 接続数です。指定する必要がある最小数は 1 です。デフォルト設定は 4 です。

注: データベース接続に指定する接続合計数 (複製のためのデータベース接続を含む) は、DB2 データベースに設定した接続数を超えることはできません。

4. 「**キャッシュ ACL 情報**」を選択して、次の ACL キャッシュ設定を使用する。
5. 「**ACL キャッシュのエレメントの最大数**」を指定する。デフォルトは 25 000 です。
6. 「**項目キャッシュのエレメントの最大数**」を指定する。デフォルトは 25 000 です。
7. 「**検索フィルター・キャッシュのエレメントの最大数**」を指定する。デフォルトは 25 000 です。検索フィルター・キャッシュは、要求された属性フィルターでの実際の照会と一致した結果の項目 ID で構成されています。更新操作では、フィルター・キャッシュ項目はすべて無効になります。
8. 「**検索フィルター・キャッシュに追加された単一検索からのエレメントの最大数**」を指定する。「**エレメント数**」を選択した場合は、数値の入力が必要です。デフォルトは 100 です。そうでない場合は、「**無制限**」を選択してください。ここで指定した項目数を超えて一致した検索項目は検索フィルター・キャッシュに追加されません。
9. 完了したら、「**OK**」をクリックする。
10. データベース接続数を設定している場合は、その変更を有効にするために、サーバーを再始動する必要があります。キャッシュ設定のみを変更した場合は、サーバーの再始動は必要ありません。

## 属性キャッシュの構成

以下の情報を参考にして、属性キャッシュの設定値を設定します。

属性キャッシュの設定は、Web 管理ツールと System i Navigatorの両方に構成されます。

Web 管理ツールで属性キャッシュ設定を手動で調整するには、次のようにしてください。

1. Web 管理ツールのナビゲーション領域で「**サーバー管理**」カテゴリを展開して、右ペインの「**属性キャッシュ**」タブを選択する。

注: Web 管理ツールの「サーバー管理」カテゴリのタスクを使用してサーバー構成設定を変更するには、\*ALLOBJ および IOSYSCFG の特殊権限をもつ i5/OS ユーザー・プロファイルとしてサーバーに認証する必要があります。これは、そのプロファイルのパスワードでプロジェクト・ユーザーとして認証することによって実行できます。Web 管理ツールからプロジェクト・ユーザーとしてバインドするには、os400-profile=MYUSERNAME,cn=accounts,os400-sys=MYSYSTEM.COM の形式の username を入力します。この MYUSERNAME と MYSYSTEM.COM のストリングはそれぞれ、ご使用のユーザー・プロファイル名および構成済みシステム射影接尾部と置き換えられます。

2. ディレクトリー・キャッシュで使用可能にするメモリー容量 (キロバイト数) を変更する。 デフォルトは 16 384 キロバイト (16 MB) です。
3. 変更ログ・キャッシュで使用可能にするメモリー容量 (キロバイト数) を変更する。 デフォルトは 16 384 キロバイト (16 MB) です。

注: 変更ログが構成されていない場合は、この選択は使用不可になります。変更ログ内で検索が頻繁に行われ、それらの検索のパフォーマンスが重要である場合以外は、変更ログの属性キャッシュを 0 に設定し、属性は構成しないようにしてください。

4. キャッシュしたい属性を「**使用可能な属性**」メニューから選択する。 キャッシュできる属性のみがこのメニューに表示されます。例えば、sn などです。

注: 属性が cn=directory と cn=changelog のコンテナに入れられるまでは、使用可能な属性のリストにそのまま残ります。

5. 「**cn=directory への追加**」または「**cn=changelog への追加**」のいずれかをクリックする。 属性は、該当するリスト・ボックスに表示されます。両方のコンテナに同じ属性をリストすることができます。

注: 変更ログが構成されていない場合は、「**cn=changelog への追加**」は使用不可になります。変更ログ内で検索が頻繁に行われ、それらの検索のパフォーマンスが重要である場合以外は、変更ログの属性キャッシュを 0 に設定し、属性は構成しないようにしてください。

6. 属性キャッシュに追加したい属性ごとに、このプロセスを繰り返す。
7. 完了したら、「**OK**」をクリックする。

System i Navigatorの自動属性キャッシュを使用可能にするには、次のようにしてください。

1. System i Navigator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. 「**IBM Directory Server**」を右マウス・ボタン・クリックし、「**プロパティ**」を選択する。
5. 「**パフォーマンス**」タブをクリックする。
6. 「**データベース**」または「**変更ログ**」のいずれか、あるいはこの両方で「**自動属性キャッシュの使用可能化**」を選択する。変更ログ内で検索が頻繁に行われ、それらの検索のパフォーマンスが重要である場合以外は、変更ログの自動属性キャッシュは使用可能にしないでください。
7. 使用可能にするために選択したキャッシュ・タイプごとに、「**開始時刻**」(サーバーの時刻) および「**間隔**」を指定する。例えば、データベース・キャッシュを使用可能にして、開始時刻を 6.00 a.m. に設定し、間隔を 6 時間に設定した場合は、サーバーが開始された時刻または自動調整が構成された時刻とは関係なく、キャッシュは自動的に 6.00 a.m.、正午、6 p.m.、および深夜 12 時に調整されます。

注: 自動属性キャッシュは、上記の説明のように Web 管理ツールに指定されたキャッシュ用メモリーの最大容量まで属性をキャッシュします。



表 4. 属性キャッシュ設定値の相互作用

| 活動                                       | 実行の内容                                                                                                                                                                                                                                                                                                             |
|------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| サーバー始動                                   | 自動属性キャッシュが現在使用可能で、サーバーが最後に停止された時に自動キャッシュが使用可能であった場合は、サーバーの停止時にキャッシュされたのと同じ属性がサーバーの再始動時に作成される。属性キャッシュで追加のメモリーがまだ使用可能な場合は、手動で構成された属性もキャッシュされる。自動属性キャッシュが現在使用可能で、サーバーが最後に停止された時に使用不可であった場合は、キャッシュのために手動で構成された属性はキャッシュされる。いずれの場合も、サーバーは指定された開始時刻および時間間隔を基に属性キャッシュを自動的に調整する。自動キャッシュが使用可能でない場合は、手動で調整されたキャッシュ設定値が有効となる。 |
| サーバー始動後に自動属性キャッシュが使用可能になる                | サーバー始動で記述したとおりに自動属性キャッシュが行われる。属性キャッシュ用に構成されたメモリー容量内に収まらない手動で構成された属性キャッシュは削除される。                                                                                                                                                                                                                                   |
| サーバー始動後に自動属性キャッシュが使用不可になる                | 手動で構成された属性のみがキャッシュされる。                                                                                                                                                                                                                                                                                            |
| サーバー始動後に自動属性キャッシュが使用可能な間にキャッシュ属性を手動で変更する | 何も起こらない。自動キャッシュが使用不可になった時に、手動構成が有効になる。                                                                                                                                                                                                                                                                            |
| サーバー始動後にキャッシュで使用可能なメモリー容量を変更する。          | 自動キャッシュが使用可能な場合は、サーバーは即時新しいサイズに基づいて再キャッシュする。自動キャッシュが使用不可の場合は、サーバーは手動構成属性を新しいサイズまでキャッシュする。                                                                                                                                                                                                                         |
| サーバー始動後に開始時刻または間隔を変更する                   | 自動キャッシュが使用可能な場合は、新規の設定は開始時刻または指定された間隔で有効となる。自動キャッシュが使用不可の場合は、その設定は保管されて、自動キャッシュが使用可能になった時に有効になる。                                                                                                                                                                                                                  |

## トランザクション設定値の構成

以下の情報を参考にして、トランザクションの設定値を設定します。

トランザクション設定を作成するには、次のようにしてください。

1. Web 管理ツールのナビゲーション領域で「サーバー・プロパティの管理」カテゴリーを展開して、右ペインの「トランザクション」タブを選択する。
2. 「トランザクション処理の使用可能化」チェック・ボックスを選択して、トランザクション処理を使用可能にする。「トランザクション処理の使用可能化」が使用不可の場合には、このパネルの他のすべてのオプションはサーバーによって無視されます。
3. 「トランザクションの最大数」を設定する。「トランザクション」または「無制限」のいずれかのラジオ・ボタンをクリックします。「トランザクション」を選択した場合は、トランザクションの最大数を指定します。トランザクションの最大数は 2 147 483 647 です。デフォルト設定は 20 個のトランザクションです。
4. 「トランザクション当たりの最大操作数」を設定する。「操作」または「無制限」のいずれかのラジオ・ボタンをクリックします。「操作」を選択した場合は、各トランザクションで許可される最大操作数を指定します。操作の最大数は 2 147 483 647 です。この数値が小さければ、パフォーマンスは上がります。デフォルトは 5 個の操作です。
5. 「保留中の時間制限」を設定する。この選択では、保留中のトランザクションの最大タイムアウト値(秒数)を指定します。「秒数」または「無制限」のいずれかのラジオ・ボタンをクリックします。「秒

数」を選択した場合は、各トランザクションで許可される最大秒数を指定します。最大秒数は 2 147 483 647 です。この時間より長く未完了のままのトランザクションは、キャンセル (ロールバック) されます。デフォルトは 300 秒です。

- 完了したら、「OK」をクリックする。
- トランザクション・サポートを使用可能にした場合には、その変更を有効にするために、サーバーを再始動する必要がある。設定のみを変更した場合は、サーバーの再始動は必要ありません。

## 複製タスク

以下の情報を参考にして、複製を管理します。

複製を管理するには、Web 管理ツールの「複製管理」カテゴリを展開します。

### 関連概念

42 ページの『複製』

複製は、パフォーマンスおよび信頼性を向上させるためにディレクトリー・サーバーで使用される技法です。複製プロセスにより、複数のディレクトリー内のデータが同期化された状態を保ちます。

## マスター・レプリカ・トポロジーの作成

以下の情報を参考にして、マスター・レプリカ・トポロジーを作成します。

基本的なマスター・レプリカ・トポロジーを定義するには、以下を行う必要があります。

- マスター・サーバーを作成し、そこに含まれているものを定義する。複製したいサブツリーを選択して、サーバーをマスターとして指定します。165 ページの『マスター・サーバーの作成 (複製されたサブツリー)』を参照してください。
- サプライヤーにより使用される信任状を作成する。167 ページの『複製の信任状の作成』を参照してください。
- レプリカ・サーバーを作成する。169 ページの『レプリカ・サーバーの作成』を参照してください。
- トポロジーをマスターからレプリカにエクスポートする。170 ページの『レプリカへのデータのコピー』を参照してください。
- その変更を複製するために誰が許可されているかを示すレプリカの構成を変更し、参照をマスターに追加する。171 ページの『新規レプリカへのサプライヤー情報の追加』を参照してください。

注:

複製したいサブツリーのルートにある項目がサーバー内にある接尾部ではない場合、サブツリーの追加機能を使用する前に、その ACL が以下のように定義されていることを確認します。

**フィルターに掛けられていない ACL の場合:**

```
ownsource: <same as the entry DN>
ownerpropagate: TRUE
```

```
acldsource: <same as the entry DN>
aclpropagate: TRUE
```

**フィルターに掛けられた ACL の場合:**

```
ibm-filteraclinherit: FALSE
```

ACL 要件を満たすためには、項目がサーバー内にある接尾部でない場合には、「項目の管理」パネルでその項目の ACL を編集してください。項目を選択し、「ACL の編集」をクリックします。フィルターに掛けられていない ACL を追加したい場合には、該当するタブを選択し、ACL と所有者の両方

にとって ACL を明示的なものにするかどうかを指定するためのチェック・ボックスを選択します。「ACL の伝搬」および「所有者の伝搬」にチェックマークが付けられていることを確認します。フィルターに掛けられた ACL を追加したい場合、そのタブを選択し、ACL および所有者に対して役割 **access-id** を持つ項目 **cn=this** を追加してください。「フィルターに掛けられた ACL の累算」のチェックが外されており、「所有者の伝搬」にチェックマークが付いていることを確認します。詳しくは、239 ページの『アクセス制御リスト (ACL) のタスク』を参照してください。

最初に、このプロセスにより作成された **ibm-replicagroup** オブジェクトは、複製されたサブツリー用のルート項目の ACL を継承します。これらの ACL は、ディレクトリー内の複製情報へのアクセスを制御するには不適切である可能性があります。

## マスター・フォワーダー・レプリカ・トポロジーの作成

以下の情報を参考にして、マスター・フォワーダー・レプリカ・トポロジーを作成します。

基本的なマスター・フォワーダー・レプリカ・トポロジーを定義するには、以下を行う必要があります。

1. マスター・サーバーおよびレプリカ・サーバーを作成する。164 ページの『マスター・レプリカ・トポロジーの作成』を参照してください。
2. オリジナル・レプリカ用のレプリカ・サーバーを作成する。『新規レプリカ・サーバーの作成』を参照してください。
3. データをレプリカにコピーする。170 ページの『レプリカへのデータのコピー』を参照してください。

## マスター・サーバーの作成 (複製されたサブツリー)

以下の情報を参考にして、マスター・サーバーの複製サブツリーを作成します。

注: このタスクを実行するには、サーバーが稼働している必要があります。

このタスクでは、独立して複製されたサブツリーのルートとして項目を指定し、このサーバーをそのサブツリーの単一マスターとして示す **ibm-replicasubentry** を作成します。複製されたサブツリーを作成するには、サーバーに複製させたいサブツリーを指定する必要があります。

ナビゲーション領域の「複製管理」カテゴリーを展開し、「トポロジーの管理」をクリックする。

1. 「サブツリーの追加」をクリックする。
2. 複製するサブツリーのルート項目の DN を入力するか、「ブラウズ」をクリックして項目を展開し、サブツリーのルートにする項目を選択する。
3. マスター・サーバー参照 URL は、LDAP URL の形式で表示される。例を以下に示します。

```
ldap://<myservername>.<mylocation>.<mycompany>.com
```

注: マスター・サーバー参照 URL はオプションです。これは以下の場合のみ使用されます。

- サーバーが読み取り専用サブツリーを含んでいる (またはこれから含む) 場合。
- サーバー上の読み取り専用サブツリーへの更新用に戻される参照 URL を定義するため。

4. 「OK」をクリックする。
5. 新規サーバーは、見出し「複製サブツリー」の下にある「トポロジーの管理」パネル上に表示される。

## 新規レプリカ・サーバーの作成

以下の情報を参考にして、新規のレプリカ・サーバーを作成します。

マスター (server1) およびレプリカ (server2) を持つ複製トポロジーをセットアップ (マスター・サーバーの作成 (複製されたサブツリー)を参照) した場合、server2 の役割を転送サーバーの役割に変更できます。これを行うには、server2 の下に新規レプリカ (server3) を作成する必要があります。

1. Web 管理をマスター (server1) に接続する
2. ナビゲーション領域の「複製管理」カテゴリを展開し、「トポロジーの管理」をクリックする。
3. 複製するサブツリーを選択し、「トポロジーの表示」をクリックする。
4. 「複製トポロジー」選択の隣の矢印をクリックし、サプライヤー・サーバーのリストを展開する。
5. 「server1」選択の隣の矢印をクリックし、サーバーのリストを展開する。
6. 「server2」を選択し、「レプリカの追加」をクリックする。
7. 「レプリカの追加」ウィンドウの「サーバー」タブで、以下のようになります。
  - 作成しているレプリカ (server3) のホスト名およびポート番号を入力する。デフォルト・ポートは、非 SSL の場合は 389、SSL の場合は 636 です。これらは必要フィールドです。
  - SSL 通信を使用可能にするかどうかを選択する。
  - レプリカ名を入力するか、このフィールドをブランクにしてホスト名を使用する。
  - レプリカ ID を入力する。レプリカを作成しているサーバーが実行中の場合は、「レプリカ ID の取得」をクリックすると、このフィールドが自動的に事前に入力されます。追加するサーバーをピアまたは転送サーバーにする場合は、これは必要フィールドです。すべてのサーバーが同じリリースであることが推奨されています。
  - レプリカ・サーバーの説明を入力する。

「追加」タブで、以下のようになります。

- レプリカがマスターとの通信に使用する信任状を指定する。

注: Web 管理ツールでは、以下の 2 つの場所で信任状を定義できます。

- **cn=replication,cn=localhost**: 信任状を使用するサーバーにのみ保持します。
- 複製サブツリー内: サブツリーの残りの部分で信任状が複製されます。

信任状を **cn=replication,cn=localhost** に置くほうが安全性が高くなります。複製サブツリーに置く信任状は、そのサブツリーの **ibm-replicagroup=default** 項目の下に作成されます。

- 「選択」をクリックする。
  - 使用する信任状の場所を選択する。望ましい場所は **cn=replication,cn=localhost** です。
  - 「信任状の表示」をクリックする。
  - 信任状のリストを展開し、使用したい信任状を選択する。
  - 「OK」をクリックする。

合意信任状についての追加情報は、複製の信任状の作成を参照してください。

- ドロップダウン・リストから複製スケジュールを指定するか、「追加」をクリックしてそれを作成する。複製スケジュールの作成を参照してください。
- サプライヤー機能のリストから、コンシューマーに複製したくないすべての機能を選択解除できます。

ネットワークで異なるリリースのサーバーを混用している場合、古いリリースでは使用不可である機能を新しいリリースで使用できます。フィルター ACL やパスワード・ポリシーのような幾つかの機能では、他の変更で複製される操作属性を活用します。ほとんどの場合、これらの機能を使用するときには、すべてのサーバーがこれらの機能をサポートするようにしたいはずですが、もしすべてのサー

バーがその機能をサポートするのでなければ、それを使用したくないでしょう。たとえば、サーバーごとに異なる ACL を使用したくないはずですが、しかしながら、ある機能をサポートするサーバーでそれを使用し、その機能に関連した変更を、その機能をサポートしないサーバーには複製したくない場合もあるかもしれません。そのような場合、機能リストを使用して、複製しない機能を明確にできます。

- 複製方法として、単一スレッドまたはマルチスレッドを選択する。マルチスレッドを指定する場合、複製で使用する接続数 (2 から 32) も指定する必要があります。デフォルトの接続数は 2 です。
- 「OK」をクリックしてレプリカを作成する。

- データを server2 から新規レプリカ server3 にコピーする。 それを行う方法については、レプリカへのデータの複製を参照してください。
- server2 を server3 のサプライヤーとし、server3 を server2 のコンシューマーとするサプライヤー合意を server3 に追加する。 それを行う方法については、新規レプリカへのサプライヤー情報の追加を参照してください。

サーバーの役割は、Web 管理ツールのアイコンで表されます。トポロジはこれで以下のようになります。

- server1 (マスター)
  - server2 (フォワーダー)
  - server3 (レプリカ)

## 複製の信任状の作成

以下の情報を参考にして、複製の信任状を作成します。

Web 管理ツールのナビゲーション領域の「複製管理」カテゴリを展開し、「信任状の管理」をクリックします。

- 信任状の格納に使用する場所をサブツリーのリストから選択します。 Web 管理ツールでは、以下の場所で信任状を定義できます。
  - cn=replication,cn=localhost**: 信任状を現在のサーバーにのみ保持します。

注: ほとんどの複製の事例では、信任状を **cn=replication,cn=localhost** に置くことが好まれます。この方がサブツリーに置かれる複製信任状より高いセキュリティを確保できます。しかしながら、**cn=replication,cn=localhost** に置かれた信任状が選択不可となる特定の状況があります。

サーバー (たとえば、serverA) の下にレプリカを追加しようとしており、異なるサーバー (serverB) に Web 管理ツールを使用して接続している場合、「信任状の選択」フィールドには、オプション「**cn=replication,cn=localhost**」は表示されません。 serverB に接続しているときには、serverA の **cn=localhost** の下にある情報を読み取ったり、その情報を更新したりすることはできないからです。

**cn=replication,cn=localhost** オプションは、レプリカの追加対象サーバーが、Web 管理ツールで接続しているサーバーと同じであるときのみ使用可能です。

- 複製サブツリー内: サブツリーの残りの部分で信任状が複製されます。複製サブツリーに置く信任状は、そのサブツリーの **ibm-replicagroup=default** 項目の下に作成されます。

注: サブツリーが表示されない場合、165 ページの『マスター・サーバーの作成 (複製されたサブツリー)』で複製するサブツリーの作成についての説明を参照してください。

- 「追加」をクリックする。

3. 作成する信任状の名前 (たとえば、**mycreds**) を入力する。cn= は、フィールドに事前に入力されていません。
4. 使用する認証方式のタイプを選択し、「次へ」をクリックする。

- 単純なバインド認証を選択した場合には以下のようにします。
  - a. サーバーがレプリカへのバインドに使用する DN を入力する (たとえば、cn=any)。
  - b. レプリカへのバインド時にサーバーが使用するパスワードを入力する (たとえば、secret)。
  - c. タイプミスがないかを確認するためにパスワードを再入力する。
  - d. 必要に応じて信任状の簡単な説明を入力する。
  - e. 「完了」をクリックする。

注: 信任状のバインド DN およびパスワードは、後で参照できるように記録しておいてください。レプリカ合意を作成する場合は、このパスワードが必要です。

- Kerberos 認証を選択した場合には以下のようにします。
  - a. Kerberos バインド DN を入力する。
  - b. 鍵タブ・ファイル名を入力する。
  - c. 必要に応じて信任状の簡単な説明を入力する。他の情報は不要です。詳しくは、205 ページの『Directory Server での Kerberos 認証の使用可能化』を参照してください。
  - d. 「完了」をクリックする。

「**Kerberos 信任状の追加**」パネルには `ibm-kn=user@realm` という形式のオプションのバインド DN と、オプションの `keytab` ファイル名 (鍵ファイルとして参照される) があります。バインド DN が指定された場合は、サーバーは指定されたプリンシパル名を使用して、コンシューマー・サーバーに対して認証します。そうでない場合には、サーバーの Kerberos サービス名 (`ldap/host-name@realm`) が使用されます。`keytab` ファイルが使用された場合は、サーバーはそれを使用して、指定されたプリンシパル名の信任状を取得します。`keytab` ファイルが使用されない場合は、サーバーはサーバーの Kerberos 構成に指定された `keytab` ファイルを使用します。複数のサプライヤーがある場合には、すべてのサプライヤーにより使用されるプリンシパル名および `keytab` ファイルを指定する必要があります。

信任状を作成したサーバー上で以下のようにします。

- a. 「ディレクトリー管理」を展開し、「項目の管理」をクリックする。
- b. 信任状を保管したサブツリー (たとえば、**cn=localhost**) を選択し、「展開」をクリックする。
- c. 「**cn=replication**」を選択し、「展開」をクリックする。
- d. Kerberos 信任状 (`ibm-replicationCredentialsKerberos`) を選択し、「属性の編集」をクリックする。
- e. 「他の属性」タブをクリックする。
- f. **replicaBindDN** を入力する (たとえば、**ibm-kn=myprincipal@SOME.REALM**)。
- g. **replicaCredentials** を入力する。これは、**myprincipal** 用に使用されるキータブ・ファイル名です。

注: このプリンシパルおよびパスワードは、コマンド行から **kinit** を実行するために使用するものと同じでなければなりません。

レプリカ上で以下のようにします。

- a. ナビゲーション領域で「複製プロパティの管理」をクリックする。

- b. 「**サプライヤー情報**」ドロップダウン・メニューからサプライヤーを選択するか、サプライヤー信任状を構成する複製されたサブツリーの名前を入力します。
  - c. 「**編集**」をクリックする。
  - d. 複製 bindDN を入力する。この例では、**ibm-kn=myprincipal@SOME.REALM** となります。
  - e. 「**複製バインド・パスワード**」に入力し、確認する。これは、**myprincipal** 用に使用される KDC パスワードです。
- サーバーの証明書を使用している場合、「証明書付き SSL」認証を選択すれば、追加情報を指定する必要はありません。サーバーの証明書以外の証明書を使用する場合は、以下を行います。
    - a. 鍵ファイル名を入力する。
    - b. 鍵ファイルのパスワードを入力する。
    - c. 確認のため、鍵ファイル・パスワードを再入力する。
    - d. 鍵ラベルを入力する。
    - e. 必要に応じて簡単な説明を入力する。
    - f. 「**完了**」をクリックする。

詳しくは、203 ページの『Directory Server での SSL と Transport Layer Security の使用可能化』を参照してください。

5. 信任状を作成したサーバー上で、サーバー・セキュリティー情報保存許可 (QRETSVRSEC) システム値を 1 (データ保存) に設定する。複製信任状は、妥当性検査リストに保管されるため、この設定により、サーバーは、レプリカに接続する時に妥当性検査リストから信任状を検索できるようになります。

## レプリカ・サーバーの作成

以下の情報を参考にして、レプリカ・サーバーを作成します。

**注:** このタスクを実行するには、サーバーが稼働している必要があります。

ナビゲーション領域の「複製管理」カテゴリーを展開し、「トポロジーの管理」をクリックする。

1. 複製するサブツリーを選択し、「トポロジーの表示」をクリックする。
2. 「複製トポロジー」選択の隣の矢印をクリックし、サプライヤー・サーバーのリストを展開する。
3. サプライヤー・サーバーを選択し、「レプリカの追加」をクリックする。
4. 「レプリカの追加」ウィンドウの「サーバー」タブで、以下のようになります。
  - a. 作成しているレプリカのホスト名およびポート番号を入力する。デフォルト・ポートは、非 SSL の場合は 389、SSL の場合は 636 です。これらは必要フィールドです。
  - b. SSL 通信を使用可能にするかどうかを選択する。
  - c. レプリカ名を入力するか、このフィールドを空白にしてホスト名を使用する。
  - d. レプリカ ID を入力する。レプリカを作成しているサーバーが実行中の場合は、「レプリカ ID の取得」をクリックすると、このフィールドが自動的に事前に入力されます。追加するサーバーをピアまたは転送サーバーにする場合は、これは必要フィールドです。すべてのサーバーが同じリリースであることが推奨されています。
  - e. レプリカ・サーバーの説明を入力する。
5. 「追加」タブで、以下のようになります。
  - レプリカがマスターとの通信に使用する信任状を指定する。

注: Web 管理ツールでは、以下の場所で信任状を定義できます。

- **cn=replication,cn=localhost**: 信任状を使用するサーバーにのみ保持します。
- 複製サブツリー内: サブツリーの残りの部分で信任状が複製されます。複製サブツリーに置く信任状は、そのサブツリーの **ibm-replicagroup=default** 項目の下に作成されます。

信任状を **cn=replication,cn=localhost** に置くほうが安全性が高くなります。複製サブツリーに置く信任状は、そのサブツリーの **ibm-replicagroup=default** 項目の下に作成されます。

- 「**選択**」をクリックする。
  - 使用する信任状の場所を選択する。望ましい場所は **cn=replication,cn=localhost** です。
  - 「**信任状の表示**」をクリックする。
  - 信任状のリストを展開し、使用したい信任状を選択する。
  - 「**OK**」をクリックする。

合意信任状についての追加情報は、複製の信任状の作成を参照してください。

- ドロップダウン・リストから複製スケジュールを指定するか、「**追加**」をクリックしてそれを作成する。複製スケジュールの作成を参照してください。
- サプライヤー機能のリストから、コンシューマーに複製したくないすべての機能を選択解除できます。

ネットワークで異なるリリースのサーバーを混用している場合、古いリリースでは使用不可である機能を新しいリリースで使用できます。フィルター **ACL** やパスワード・ポリシーのような幾つかの機能では、他の変更で複製される操作属性を活用します。ほとんどの場合、これらの機能を使用するときには、すべてのサーバーがこれらの機能をサポートするにしたいはずですが、もしすべてのサーバーがその機能をサポートするのであれば、それを使用したくないでしょう。たとえば、サーバーごとに異なる **ACL** を使用したくないはずですが、しかしながら、ある機能をサポートするサーバーでそれを使用し、その機能に関連した変更を、その機能をサポートしないサーバーには複製したくない場合もあるかもしれません。そのような場合、機能リストを使用して、複製しない機能を明確にできます。

- 1 | • 複製方法として、単スレッドまたはマルチスレッドを選択する。マルチスレッドを指定する場合、  
1 | 複製で使用する接続数 (2 から 32) も指定する必要があります。デフォルトの接続数は 2 です。
- 「**OK**」をクリックしてレプリカを作成する。

6. 追加アクションが必要であることを通知するメッセージが表示される。「**了解**」をクリックする。

注: 追加レプリカとしてさらにサーバーを追加したり、複雑なトポロジーを作成する場合、マスター・サーバーでのトポロジーの定義を完了するまでは、レプリカへのデータのコピーまたは新規レプリカへのサプライヤー情報の追加には進まないでください。トポロジーを完成させた後に *masterfile.ldif* を作成する場合、それはマスター・サーバーのディレクトリー項目およびトポロジー合意の完全なコピーを含みます。このファイルをサーバーごとにロードすると、各サーバーは以後同じ情報を持つようになります。

## レプリカへのデータのコピー

以下の情報を参考にして、データをレプリカにコピーします。

レプリカを作成した後、トポロジーをマスターからレプリカにエクスポートする必要があります。

1. マスター・サーバー上で、データ用の **LDIF** ファイルを作成する。マスター・サーバー上にあるすべてのデータをコピーするには、以下を行います。



- a. System i Navigatorで「ネットワーク」を展開する。
  - b. 「サーバー」を展開する。
  - c. 「TCP/IP」をクリックする。
  - d. 「IBM Directory Server」を右マウス・ボタン・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。
  - e. 出力 LDIF ファイル名 (たとえば、masterfile.ldif) を指定し、オプションでエクスポートするサブツリー (たとえば、subtreeDN) を指定した後、「OK」をクリックする。
2. レプリカを作成しているマシン上で、以下を行う。
    - a. 複製された接尾部はレプリカ・サーバーの構成で定義されていることを確認する。
    - b. レプリカ・サーバーを停止する。
    - c. LDIF ファイルをレプリカにコピーし、以下を行う。
      - 1) System i Navigator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) 「IBM Directory Server」を右マウス・ボタン・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。
      - 5) 入力 LDIF ファイル名 (たとえば、masterfile.ldif) を指定し、オプションでデータを複製するかを指定した後、「OK」をクリックする。

レプリカ合意、スケジュール、信任状 (複製されたサブツリーに保管されている場合)、および項目データは、レプリカにロードされます。

- d. サーバーを開始する。

## 新規レプリカへのサプライヤー情報の追加

以下の情報を参考にして、新規レプリカにサプライヤー情報を追加します。

その変更を複製するために誰が許可されているかを示すレプリカの構成を変更し、参照をマスターに追加する必要があります。

レプリカを作成しているマシン上で、以下を行います。

1. ナビゲーション領域の「複製管理」を展開し、「複製プロパティの管理」をクリックする。

**注:** 「複製プロパティの管理」パネルの設定を変更するには、\*ALLOBJ および \*IOSYSCFG 特殊権限を持つプロジェクトの OS/400 ユーザーとして、Web 管理ツールにログインする必要があります。

2. 「追加」をクリックする。
3. 「複製されたサブツリー」ドロップダウン・メニューからサプライヤーを選択するか、またはサプライヤー信任状を構成する複製されたサブツリーの名前を入力する。 サプライヤー信任状を編集している場合は、このフィールドは編集できません。
4. 複製 bindDN を入力する。この例では、cn=any となります。

**注:** 状況により、これら 2 つのオプションのいずれかを使用できます。

- 「デフォルトの信任状と参照」を使用して、サーバーに複製されたすべてのサブツリー用の複製バインド DN (およびパスワード) およびデフォルトの参照を設定します。これは、同じサプライヤーからすべてのサブツリーが複製される時に使用されることがあります。

- サブツリーごとにサプライヤー情報を追加することにより、複製されたサブツリーごとに独立して複製バインド DN およびパスワードを設定します。これは、各サブツリーが異なるサプライヤーを持つときに使用されることがあります (すなわち、サブツリーごとに異なるマスター・サーバー)。
5. 信任状のタイプに応じて、信任状パスワードを入力して確認します。(これは将来のために以前に記録済みです。)
- **単純なバインド** - DN およびパスワードを指定します。
  - **Kerberos** - サプライヤーの信任状がプリンシパルおよびパスワードを識別しない場合、すなわち、サーバー自体のサービス・プリンシパルが使用される場合には、バインド DN は、`ibm-kn=ldap/<yourservername@yourrealm>` となります。信任状が `<myprincipal@myrealm>` のようなプリンシパル名を持つ場合、それを DN として使用します。いずれの場合でも、パスワードは必要ありません。
  - **EXTERNAL バインド付き SSL** - 証明書用のサブジェクト DN を指定し、パスワードは指定しません。

167 ページの『複製の信任状の作成』を参照してください。

6. 「OK」をクリックします。
7. 変更を有効にするためにレプリカを再始動する必要があります。

詳しくは、180 ページの『複製プロパティの変更』を参照してください。

レプリカは、延期状態で、複製は行われません。複製トポロジーのセットアップが完了した後、「キューの管理」をクリックし、レプリカを選択した後、「中断/再開」をクリックして複製を開始します。詳しくは、183 ページの『複製キューの管理』を参照してください。レプリカはマスターからの更新を受け取るようになりました。

## ピア複製での単純なトポロジーの作成

ピア複製とは、複数のサーバーがマスターとなる複製トポロジーです。ピア複製は、更新ベクトルが十分に知られている環境でのみ使用してください。

ディレクトリー内の特定のオブジェクトへの更新は、1 つのピア・サーバーのみが実行します。これは、1 つのサーバーがあるオブジェクトを削除した後、別のサーバーがそのオブジェクトを変更するというシナリオを防ぐためです。このシナリオでは、ピア・サーバーが削除コマンドを受け取った後、変更コマンドを受け取るので、競合が生じる可能性があります。複製済みの削除要求と名前変更要求は、競合解決なしに、受信順に受け入れられます。複製の競合解決の詳細は、以下の関連リンクを参照してください。

ナビゲーション領域の「複製管理」カテゴリーを展開し、「トポロジーの管理」をクリックします。

1. 複製するサブツリーを選択し、「トポロジーの表示」をクリックします。
2. 既存のトポロジーを表示するには、既存サーバーの横のボックスをクリックし、サプライヤー・サーバーのリストを展開します。
3. 「Add master (マスターの追加)」をクリックします。

「Add master (マスターの追加)」ウィンドウの「サーバー」タブで、以下のようにします。

- 作成しているサーバーのホスト名およびポート番号を入力します。デフォルト・ポートは、非 SSL の場合は 389、SSL の場合は 636 です。これらは必要フィールドです。
- SSL 通信を使用可能にするかどうかを選択します。
- ゲートウェイ・サーバーとしてサーバーを作成するかどうかを選択します。

- | • サーバー名を入力するか、またはこのフィールドをブランクにしてホスト名を使用します。
- | • サーバー ID を入力します。ピア・マスターの作成場所であるサーバーが実行中の場合は、「**サーバー ID の取得**」をクリックすると、このフィールドの自動事前入力が行われます。サーバー ID が不明の場合、**unknown** と入力します。
- | • サーバーの説明を入力します。
- | • サーバーがマスター・サーバーとの通信で使用する信任状を指定する必要があります。「**選択**」をクリックします。

| **注:** Web 管理ツールでは、以下の場所で信任状を定義できます。

- | - **cn=replication,cn=localhost:** 信任状を使用するサーバーにのみ保持します。信任状を cn=replication,cn=localhost に置くほうが安全性が高くなります。
- | - **cn=replication,cn=IBMpolicies.** これは、レプリカの追加で使用するサーバーが、Web 管理ツールで接続しているのと同じサーバーではない場合でも使用可能です。このロケーションに置かれた信任状が、それらのサーバーに複製されます。

| **注:** ロケーション cn=replication,cn=IBMpolicies を使用できるのは、ルート DSE の `ibm-supportedcapabilities` の下に `IBMpolicies サポート OID 1.3.18.0.2.32.18` がある場合のみです。

- | - 複製サブツリー内: サブツリーの残りの部分で信任状が複製されます。複製サブツリーに置く信任状は、そのサブツリーの **ibm-replicagroup=default** 項目の下に作成されます。
  - | 1. 使用する信任状の場所を選択する。望ましい場所は `cn=replication,cn=localhost` です。
  - | 2. 一連の信任状をすでに作成済みの場合、「信任状の表示」をクリックします。
  - | 3. 信任状のリストを展開し、使用したい信任状を選択します。
  - | 4. 「OK」をクリックします。
  - | 5. 既存の信任状がない場合、「追加」をクリックし、信任状を作成します。

| 「追加」タブで、以下のようにします。

- | 1. ドロップダウン・リストから複製スケジュールを指定するか、または「追加」をクリックしてそれを作成します。複製スケジュールの作成を参照してください。
- | 2. サプライヤー機能のリストから、コンシューマーに複製したくないすべての機能を選択解除できます。

| ネットワークで異なるリリースのサーバーを混用している場合、古いリリースでは使用不可である機能を新しいリリースで使用できます。フィルター ACL やパスワード・ポリシーのような幾つかの機能では、他の変更で複製される操作属性を活用します。たいていの場合、これらのフィーチャーを使用する場合、すべてのサーバーでそのフィーチャーがサポートされるのが望ましいはずですが、もしすべてのサーバーがその機能をサポートするのであれば、それを使用したくないでしょう。たとえば、サーバーごとに異なる ACL を使用したくないはずですが、しかしながら、ある機能をサポートするサーバーでそれを使用し、その機能に関連した変更を、その機能をサポートしないサーバーには複製したくない場合もあるかもしれません。そのような場合、機能リストを使用して、複製しない機能を明確にできます。

- | 3. サプライヤーの信任状の動的更新を有効にするには、「**Add credential information on consumer (コンシューマーに関する信任状情報の追加)**」 チェック・ボックスにチェックを付けます。この選択によって、コンシューマー・サーバーの構成ファイル内のサプライヤー信任状が自動的に更新されます。すると、トポロジー情報をサーバーに複製できるようになります。

- | • コンシューマー・サーバーの管理 DN を入力します。たとえば、`cn=root` と入力します。

注: サーバー構成プロセス中に作成された管理者 DN が cn=root である場合は、完全な管理者 DN を入力します。単に root だけを入力しないでください。

- コンシューマー・サーバーの管理パスワードを入力します。たとえば、secret と入力します。
- 4. 「OK」をクリックします。
- 5. 新規のマスター・サーバーとすべて既存のサーバーの間の、サプライヤーとコンシューマーの契約がリストされます。作成する必要はないと思われる契約はすべて、チェック・マークを外します。これは、ゲートウェイ・サーバーを作成する場合は特に重要です。
- 6. 「続行」をクリックします。
- 7. 追加アクションをとる必要があることを通知するメッセージが表示されることがあります。該当するアクションを実行するか、またはメモをとっておきます。完了したら、「OK」をクリックします。
- 8. 該当する信任状を追加します。

注: 場合によっては、cn=replication,cn=localhost 以外の場所に置かれている信任状を求める「信任状の選択」パネルが表示されます。その状況では、cn=replication,cn=localhost 以外の場所に置かれている信任状オブジェクトを入力する必要があります。既存の信任状のセットからサブツリーで使用される信任状を選択するか、新しい信任状を作成します。

- 9. 「OK」をクリックして、ピア・マスターを作成します。
- 10. 追加アクションをとる必要があることを通知するメッセージが表示されることがあります。該当するアクションを実行するか、またはメモをとっておきます。完了したら、「OK」をクリックします。

#### 関連資料

- 42 ページの『複製の概要』
- 複製の時、1 つのディレクトリーに行われた変更は、1 つ以上の追加のディレクトリーに伝搬します。それにより、1 つのディレクトリーに変更を行うと、複数の異なるディレクトリーに影響します。

## 複雑な複製トポロジーの作成

この概要を参考にしながら、複雑な複製トポロジーをセットアップしてください。

1. すべてのピア・サーバーまたは今後レプリカになるサーバーを開始する。これは、Web 管理ツールがサーバーから情報を収集するために必要です。
2. 「第 1」マスターを開始し、このコンテキスト用のマスターとして構成する。
3. データをまだロードしていない場合、「第 1」マスター上で複製されるサブツリーのデータをロードする。
4. 複製されるサブツリーを選択する。
5. ピア・マスターの候補すべてを「第 1」マスターのレプリカとして追加する。
6. 他のすべてのレプリカを追加する。
7. 他のピア・マスターを移動してプロモートする。
8. レプリカのレプリカ合意をピア・マスターごとに追加する。

注: 信任状が cn=replication,cn=localhost に作成される場合、信任状は、サーバーが再始動した後にサーバーごとに作成する必要があります。信任状オブジェクトが作成されない場合、ピアによる複製は失敗します。

9. 他のマスターのレプリカ合意をピア・マスターごとに追加する。「第 1」マスターはすでにその情報を持っています。
10. 複製されるサブツリーを静止する。これにより、データを他のサーバーにコピーしている間に更新が行われることを防ぎます。

11. 「キュー管理 (Queue management)」を使用してキューごとにすべてスキップする。
12. 複製されるサブツリーのデータを「第 1」マスターからエクスポートする。
13. サブツリーを静止解除する。
14. レプリカ・サーバーを停止し、複製されるサブツリーのデータをそれぞれのレプリカおよびピア・マスター上にインポートする。その後サーバーを再始動する。
15. サプライヤーが信任状を使用する設定になるように各レプリカおよびピア・マスター上の複製プロパティを管理する。

## ピア複製での複雑なトポロジーの作成

以下の情報を参考にして、ピア複製を使って複雑なトポロジーを作成します。

ピア複製とは、複数のサーバーがマスターとなる複製トポロジーです。しかしながら、複数マスター環境とは異なり、ピア・サーバー間での競合解決は行われません。LDAP サーバーは、ピア・サーバーにより提供される更新を受け入れ、それ自体のデータのコピーを更新します。更新を受け取る順序、または複数の更新が競合するかについては考慮されません。

追加マスター (ピア) を追加するには、最初にサーバーを既存のマスターの読み取り専用レプリカとして追加し (169 ページの『レプリカ・サーバーの作成』を参照)、ディレクトリー・データを初期化した後、サーバーをマスターにプロモートします (194 ページの『サーバーの移動またはプロモート』を参照)。

最初に、このプロセスにより作成された **ibm-replicagroup** オブジェクトは、複製されたサブツリー用のルート項目の ACL を継承します。これらの ACL は、ディレクトリー内の複製情報へのアクセスを制御するには不適切である可能性があります。

「サブツリーの追加」操作が成功するには、追加する項目 DN がサーバー内にある接尾部でない場合には、それは正確な ACL でなければなりません。

**フィルターに掛けられていない ACL の場合 :**

- ownersource : <項目 DN>
- ownerpropagate : TRUE
- aclsource : <項目 DN>
- aclpropagate: TRUE

**フィルターに掛けられた ACL の場合 :**

- ownersource : <項目 DN>
- ownerpropagate : TRUE
- ibm-filteraclinherit : FALSE
- ibm-filteraclentry : <任意の値>

Web 管理ツールの「**ACL の編集**」機能を使用して、新規に作成された複製されたサブツリーと関連した複製情報用の ACL を設定します (196 ページの『アクセス制御リストの編集』を参照)。

レプリカは、延期状態で、複製は行われません。複製トポロジーのセットアップが完了した後、「**キューの管理**」をクリックし、レプリカを選択した後、「**中断/再開**」をクリックして複製を開始します。詳しくは、183 ページの『複製キューの管理』を参照してください。レプリカはマスターからの更新を受け取るようになりました。

ピア複製は、ディレクトリー更新のパターンが既知である環境でのみ使用してください。ディレクトリー内の特定のオブジェクトへの更新は、1 つのピア・サーバーのみが実行します。これは、1 つのサーバーがあ

るオブジェクトを削除した後、別のサーバーがそのオブジェクトを変更するというシナリオを防ぐためです。このシナリオでは、ピア・サーバーが削除コマンドを受け取った後変更コマンドを受け取り、競合が生じるという可能性があります。

2 つのピア・マスター・サーバー、2 つの転送サーバー、および 4 つのレプリカで構成されるピア・フォワーダー・レプリカ・トポロジーを定義するには、以下のようにする必要があります。

1. マスター・サーバーおよびレプリカ・サーバーを作成する。164 ページの『マスター・レプリカ・トポロジーの作成』を参照してください。
2. マスター・サーバー用の 2 つの追加レプリカ・サーバーを作成する。169 ページの『レプリカ・サーバーの作成』を参照してください。
3. 新規に作成した各レプリカ・サーバーの下に 2 つのレプリカを作成する。
4. 元のレプリカをマスターにプロモートする。『サーバーのピアへのプロモート』を参照してください。

**注:** マスターにプロモートするサーバーは、従属レプリカを持たないリーフ・レプリカである必要があります。

5. データをマスターから新規マスターおよびレプリカにコピーする。170 ページの『レプリカへのデータのコピー』を参照してください。

#### 関連タスク

194 ページの『サーバーの移動またはプロモート』

以下の情報を参考にして、サーバーを移動またはプロモートします。

### サーバーのピアへのプロモート

以下の情報を参考にして、サーバーをピアにプロモートします。

165 ページの『マスター・フォワーダー・レプリカ・トポロジーの作成』で作成した転送トポロジーを使用して、サーバーをピアにプロモートできます。この例では、レプリカ (server3) をマスター・サーバー (server1) のピアにプロモートします。

1. Web 管理をマスター (server1) に接続する。
2. ナビゲーション領域の「複製管理」カテゴリを展開し、「トポロジーの管理」をクリックする。
3. 複製するサブツリーを選択し、「トポロジーの表示」をクリックする。
4. 「複製トポロジー」選択の隣の矢印をクリックし、サーバーのリストを展開する。
5. 「server1」選択の隣の矢印をクリックし、サーバーのリストを展開する。
6. 「server2」選択の隣の矢印をクリックし、サーバーのリストを展開する。
7. 「server1」をクリックし、「レプリカの追加」をクリックする。server4 を作成する。169 ページの『レプリカ・サーバーの作成』を参照してください。同じ手順で server5 を作成する。サーバーの役割は、Web 管理ツールのアイコンで表されます。トポロジーは以下のようになります。
  - server1 (マスター)
    - server2 (フォワーダー)
    - server3 (レプリカ)
    - server4 (レプリカ)
    - server5 (レプリカ)
8. 「server2」をクリックし、「レプリカの追加」をクリックして server6 を作成する。

9. 「**server4**」をクリックし、「**レプリカの追加**」をクリックして server7 を作成する。同じ手順で server8 を作成する。トポロジーは以下のようになります。

- server1 (マスター)
  - server2 (フォワーダー)
  - server3 (レプリカ)
  - server6 (レプリカ)
  - server4 (フォワーダー)
  - server7 (レプリカ)
  - server8 (レプリカ)
  - server5 (レプリカ)

10. 「**server5**」を選択し、「**移動**」をクリックする。

注: 移動するサーバーは、従属レプリカを持たないリーフ・レプリカである必要があります。

11. 「**複製トポロジー**」を選択し、レプリカをマスターにプロモートする。「**移動**」をクリックする。

12. 「**追加のサプライヤー合意の作成**」パネルが表示される。ピア複製では、各マスターは、トポロジー内の他の各マスターのサプライヤーおよびコンシューマーであり、さらに第 1 レベル・レプリカである server2 および server4 のそれぞれのサプライヤーおよびコンシューマーである必要があります。server5 はすでに server1 のコンシューマーですが、ここで server1、server2、server4 のサプライヤーになる必要があります。サプライヤー合意のボックスの以下の部分にチェックマークが付いていることを確認してください。

表 5.

|   | サプライヤー  | コンシューマー |
|---|---------|---------|
| ✓ | server5 | server1 |
| ✓ | server5 | server2 |
| ✓ | server5 | server4 |

「**続行**」をクリックする。

注: 場合によっては、「**信任状の選択**」パネルが表示され、cn=replication,cn=localhost 以外の場所に置かれている信任状の入力が求められます。その状況では、cn=replication,cn=localhost 以外の場所に置かれている信任状オブジェクトを入力する必要があります。既存の信任状のセットからサブツリーで使用する信任状を選択するか、新しい信任状を作成します。167 ページの『複製の信任状の作成』を参照してください。

13. 「**OK**」をクリックする。トポロジーは以下のようになります。

- server1 (マスター)
  - server2 (フォワーダー)
  - server3 (レプリカ)
  - server6 (レプリカ)
  - server4 (フォワーダー)
  - server7 (レプリカ)
  - server8 (レプリカ)
  - server5 (マスター)
- server5 (マスター)

- server1 (マスター)
- server2 (フォワーダー)
- server4 (フォワーダー)

14. データを server1 からすべてのサーバーにコピーする。 それを行う方法については、 170 ページの『レプリカへのデータのコピー』を参照してください。

## ゲートウェイ・トポロジーのセットアップ

以下の情報を参考にして、ゲートウェイ・トポロジーをセットアップします。

複製トポロジーのセットアップを開始する前に、オリジナルの `ibmslapd.conf` ファイルのバックアップ・コピーを作成してください。複製で何らかの問題が起こった場合は、このバックアップ・コピーを使用して、オリジナル構成を復元することができます。

サーバーのピアへのプロモートにあるプロシージャから、ピア複製の複雑なトポロジーを使用してゲートウェイをセットアップするには、以下のステップを完了する必要があります。

- 既存のピア・サーバー (ピア 1) をゲートウェイ・サーバーに変換して、複製サイト 1 を作成する。
- 複製サイト 2 の新規のゲートウェイ・サーバーおよびピア 1 との合意を作成する。
- 複製サイト 2 のトポロジーを作成する (この例には示されていない)。
- データをマスターからトポロジーのすべてのマシンにコピーする。

1. Web 管理ツールを使用して、マスター (server1) にログインする。
2. ナビゲーション領域の「複製管理」カテゴリを展開し、「トポロジーの管理」をクリックする。
3. 複製するサブツリーを選択し、「トポロジーの表示」をクリックする。
4. 既存のサーバーをゲートウェイ・サーバーに変換するには、「**Manage gateway servers (ゲートウェイ・サーバーの管理)**」を選択する。「server1」またはそのピア「server5」を選択する。この例では、server1 を選択し、「**Make gateway (ゲートウェイにする)**」をクリックします。
5. 「OK」をクリックする。

注: ゲートウェイとして使用したいサーバーがまだマスターになっていない場合には、従属レプリカのないリーフ・レプリカのはずであり、これは、最初にマスターとしてプロモートしてから、ゲートウェイとして指定することができます。

6. 新規のゲートウェイ・サーバーを作成するには、「サーバーの追加」をクリックする。
7. 新規のサーバー「server9」をゲートウェイ・サーバーとして作成する。 それを行う方法については、189 ページの『ピア・マスターまたはゲートウェイ・サーバーの追加』を参照してください。
8. 「追加のサプライヤー合意の作成」パネルが表示される。 このパネルでは、サプライヤー合意のボックスが server1 のみにチェックマークが付いていることを確認してください。その他の合意の選択を解除します。

|   | サプライヤー  | コンシューマー |
|---|---------|---------|
| ✓ | server1 | server9 |
| ✓ | server9 | server1 |
|   | server2 | server9 |
|   | server9 | server2 |
|   | server4 | server9 |
|   | server9 | server4 |
|   | server9 | server5 |



|  | サプライヤー  | コンシューマー |
|--|---------|---------|
|  | server5 | server9 |

9. 「続行」をクリックする。
10. 「OK」をクリックする。
11. 該当する信任状およびコンシューマー情報を追加する。

注: 場合によっては、「信任状の選択」パネルが表示され、cn=replication,cn=localhost 以外の場所に置かれている信任状の入力が求められます。その状況では、cn=replication,cn=localhost 以外の場所に置かれている信任状オブジェクトを入力する必要があります。既存の信任状のセットからサブツリーで使用する信任状を選択するか、新しい信任状を作成します。複製の信任状の作成を参照してください。

12. 「OK」をクリックする。サーバーの役割は、Web 管理ツールのアイコンで表されます。トポロジーは以下ようになります。

- server1 (複製 site1 の master-gateway)
  - server2 (フォワーダー)
  - server3 (レプリカ)
  - server6 (レプリカ)
  - server4 (フォワーダー)
  - server7 (レプリカ)
  - server8 (レプリカ)
  - server5 (マスター)
  - server9 (複製サイト 2 の master-gateway)
- server5 (マスター)
  - server1 (マスター)
  - server2 (フォワーダー)
  - server3 (レプリカ)
  - server6 (レプリカ)
  - server4 (フォワーダー)
  - server7 (レプリカ)
  - server8 (レプリカ)
- server9 (master-gateway)
  - server1 (master-gateway)

13. サーバーを **server9** に追加して、複製サイト 2 のトポロジーを作成する。複製サイト 2 の外部のすべてのサーバーに対する新規サーバーのすべての合意の選択を必ず解除してください。
14. この複製を繰り返して、追加の複製サイトを作成する。それぞれの複製サイトに作成されるゲートウェイ・サーバーは 1 つだけであることを注意してください。ただし、他のゲートウェイ・サーバーとの合意を持った各ゲートウェイ・サーバーが、トポロジー内に存在していなければなりません。
15. トポロジーの作成が完了したなら、server1 からデータをすべての複製サイトの新規のすべてのサーバーにコピーして、サプライヤー情報を新規のすべてのサーバーに追加する。それを行う方法については、レプリカへのデータのコピー および 新規レプリカへのサプライヤー情報の追加を参照してください。

## 関連タスク

187 ページの『レプリカの追加』

以下の情報を参考にして、レプリカを作成します。

189 ページの『ピア・マスターまたはゲートウェイ・サーバーの追加』

このトピックでは、新規のピア・マスターまたはゲートウェイ・サーバーを作成する方法を説明します。

191 ページの『ゲートウェイ・サーバーの管理』

このトピックでは、ゲートウェイ・サーバーの管理について説明します。マスター・サーバーが複製サイトでゲートウェイ・サーバーとしての役割を持つかどうかを指定することができます。

## 複製プロパティの変更

以下の情報を参考にして、複製のプロパティを変更します。

「複製プロパティの管理」パネルの設定を変更するには、\*ALLOBJ および \*IOSYSCFG 特殊権限を持つプロジェクト・ユーザーとして Web 管理ツールにログインする必要があります。

1. ナビゲーション領域の「複製管理」カテゴリを展開し、「複製プロパティの管理」をクリックします。
2. このパネルで、以下を行うことができます。

a. 複製状況照会から戻す保留変更の最大数を変更します。デフォルトは 200 です。

b. コンシューマーへの更新の複製中にサーバーがログ記録をとる複製エラーの最大数を設定します。サーバーが単一スレッド複製を使用している場合、最大数を超えたときは、更新が正常完了するまでか、または、エラーを追加できるように管理者がログをクリアするまで、更新は定期的に再試行されます。サーバーがマルチスレッド複製を使用している場合、最大数を超えたときは、進行中の更新で起きた複製エラーはすべて記録され、複製は、管理者がログをクリアするまで待機します。失敗した更新の再試行または除去を行って、ログをクリアすることができます。各コンシューマーごとに、ログは別々に保守されます。デフォルトは、「none」と同じゼロです。

注：ロギングが使用可能になるのは、ゼロより大きい値を指定した場合です。

c. 複製コンテキスト・キャッシュのバイト単位のサイズを変更します。デフォルトは 100,000 バイトです。

d. 複製の競合の最大項目サイズをバイト数で設定します。バイト単位の項目の合計サイズがこのフィールドの値を超えても、コンシューマーでの複製の競合の解決のために、サプライヤーからこの項目が再度送信されることはありません。デフォルトは、「制限なし」の 0 です。

e. サプライヤー情報を追加、編集、または削除します。

注：サプライヤー DN は、プロジェクト i5/OS ユーザー・プロファイルの DN です。プロジェクト i5/OS ユーザー・プロファイルは、LDAP 管理権限を持つことはできません。ユーザーは、\*ALLOBJ および \*IOSYSCFG 特殊権限を持つユーザーとなることはできず、ディレクトリー・サーバー管理者アプリケーション ID により管理権限を認可されていません。

詳細については、以下を参照してください。

- 181 ページの『サプライヤー情報の追加』
- 181 ページの『サプライヤー情報の編集』
- 182 ページの『サプライヤー情報の除去』

## サプライヤー情報の追加

以下の情報を参考にして、サプライヤー情報を追加します。

1. 「追加」をクリックします。
2. ドロップダウン・メニューからサプライヤーを選択するか、またはサプライヤーとして追加したい複製されたサブツリーの名前を入力します。
3. 信任状の複製バインド DN を入力します。

注: 状況により、これら 2 つのオプションのいずれかを使用できます。

- 「デフォルトの信任状と参照」を使用して、サーバーに複製されたすべてのサブツリー用の複製バインド DN (およびパスワード) およびデフォルトの参照を設定します。これは、同じサプライヤーからすべてのサブツリーが複製される時に使用されることがあります。
  - サブツリーごとにサプライヤー情報を追加することにより、複製されたサブツリーごとに独立して複製バインド DN およびパスワードを設定します。これは、各サブツリーが異なるサプライヤーを持つときに使用されることがあります (すなわち、サブツリーごとに異なるマスター・サーバー)。
4. 信任状のタイプに応じて、信任状パスワードを入力して確認します。(これは将来のために以前に記録済みです。)
    - **単純なバインド** - DN およびパスワードを指定します。
    - **Kerberos** - パスワードなしで「ibm-kn=LDAP-service-name@realm」形式の疑似 DN を指定します。
    - **EXTERNAL** バインド付き **SSL** - 証明書用のサブジェクト DN を指定し、パスワードは指定しません。

167 ページの『複製の信任状の作成』を参照してください。

5. 「OK」をクリックします。

サプライヤーのサブツリーがサプライヤー情報リストに追加されます。

## サプライヤー情報の編集

以下の情報を参考にして、サプライヤー情報を編集します。

1. 編集するサプライヤー・サブツリーを選択する。
2. 「編集」をクリックする。
3. 「デフォルトの信任状と参照」を編集する場合 (これは、cn=configuration の下に cn=Master Server 項目を作成するために使用されます)、 「デフォルト・サプライヤーの LDAP URL」 フィールドに、クライアントでレプリカの更新を受信するサーバーの URL を入力する。これは、有効な LDAP URL (ldap://) である必要があります。それ以外の場合、ステップ 4 にスキップします。
4. 使用する新規信任状の複製バインド DN を入力する。
5. 信任状パスワードを入力して確認する。
6. 「OK」をクリックする。

| 複製サプライヤー DN のパスワードは、ディレクトリー・サーバー属性変更 (CHGDIRSVRA) コマンドを使用しても変更することもできます。複製バインド DN cn=master のパスワードを newpassword に変更するには、次のようなコマンドを使用します。

| CHGDIRSVRA INSTANCE(QUSRDIR) DN('cn=master' 'newpassword')

## 1 サプライヤー情報の除去

以下の情報を参考にして、サプライヤー情報を除去します。

1. 除去するサプライヤー・サブツリーを選択する。
2. 「削除」をクリックする。
3. 削除の確認メッセージが表示された場合は、「OK」をクリックする。

サブツリーが「サプライヤー情報」リストから除去される。

## 複製スケジュールの作成

以下の情報を参考にして、複製のスケジュールを作成します。

複製スケジュールをオプションで定義して、特定の時刻の複製をスケジュールに入れたり、特定の時刻の間には複製しないようスケジュールできます。スケジュールを使用しない場合、変更が行われるときに必ずサーバーにより複製がスケジュールされます。これは、毎日午前 12:00 に開始する即時複製のスケジュールを指定することに相当します。

ナビゲーション領域の「複製管理」カテゴリを展開し、「スケジュールの管理」をクリックします。

「週次スケジュール」タブで、スケジュールを作成するサブツリーを選択し、「スケジュールの表示」をクリックします。スケジュールが存在する場合は、「週次スケジュール」ボックスに表示されます。新規スケジュールを作成または追加するには、以下のようになります。

1. 「追加」をクリックする。
2. スケジュールの名前を入力する。たとえば、**schedule1** と入力します。
3. 曜日ごとに (日曜日から土曜日まで)、毎日のスケジュールは「なし」に指定されている。これは、複製更新イベントはスケジュールされていないことを意味します。最後の複製イベントがもしあれば、そのイベントはまだ有効です。これは新規レプリカで、前の複製イベントはないため、スケジュールは即時複製のデフォルトになっています。
4. 日を選択し、「日次スケジュールの追加」をクリックすると、その日の日次複製スケジュールを作成できる。日次スケジュールを作成する場合、それは各曜日のデフォルトのスケジュールになります。以下を行うことができます。
  - 日次スケジュールを各曜日のデフォルトとして保存したり、特定の日を選択し、スケジュールをなしに変更したりする。複製イベントがスケジュールされていない日であっても、発生した最後の複製イベントは引き続き有効です。
  - 日を選択し、「日次スケジュールの編集」をクリックすることによって、日次スケジュールを変更する。日次スケジュールを変更すると、選択した日だけでなく、そのスケジュールを使用するすべての日に影響が及びます。
  - 日を選択し、「日次スケジュールの追加」をクリックすることによって、別の日次スケジュールを作成する。このスケジュールを作成すると、それは「日次スケジュール」ドロップダウン・メニューに追加されます。スケジュールを使用したい日ごとにこのスケジュールを選択する必要があります。

日次スケジュールのセットアップについて詳しくは、183 ページの『複製の日常スケジュールの作成』を参照してください。

5. 完了したら、「OK」をクリックする。

### 関連タスク

193 ページの『複製のスケジュールの表示』

Web 管理ツールを使用して複製のスケジュールを表示するには、次のステップを行います。

## 複製の日常スケジュールの作成

以下の情報を参考にして、複製の日常スケジュールを作成します。

ナビゲーション領域の「複製管理」カテゴリを展開し、「スケジュールの管理」をクリックします。

「日次スケジュール」タブで、スケジュールを作成するサブツリーを選択し、「スケジュールの表示」をクリックします。スケジュールが存在する場合は、「日次スケジュール」ボックスに表示されます。新規スケジュールを作成または追加するには、以下のようにします。

1. 「追加」をクリックする。
2. スケジュールの名前を入力する。たとえば、**monday1** と入力します。
3. 時間帯設定 (UTC またはローカル) を選択する。
4. ドロップダウン・メニューから以下の複製タイプを選択する。

**即時** 最後の複製イベント以後の保留中の項目の更新をすべて実行してから、次にスケジュールされている更新イベントに達するまで継続的に項目を更新します。

**1 回** 開始時刻より前に保留中の更新をすべて実行します。開始時刻より後の更新は、すべて次にスケジュールされている複製イベントまで待機します。

5. 複製イベントの開始時刻 (サーバーの時刻) を選択する。
6. 「追加」をクリックする。複製イベント・タイプおよび時刻が表示されます。
7. スケジュールを完了するためのイベントを追加または除去する。イベントのリストは日時順に更新されます。
8. 完了したら、「OK」をクリックする。

たとえば次のようになります。

| 複製タイプ | 開始時刻     |
|-------|----------|
| 即時    | 午前 12:00 |
| 1 回   | 午前 10:00 |
| 1 回   | 午後 2:00  |
| 即時    | 午後 4:00  |
| 1 回   | 午後 8:00  |

このスケジュールでは、最初の複製イベントは深夜 12 時に発生し、その時刻より前のすべての保留変更は更新されます。複製更新は、午前 10:00 に発生するまで継続的に行われます。午前 10:00 と午後 2:00 の間の更新は、午後 2:00 に複製されるまで待機します。午後 2:00 と午後 4:00 の間のすべての更新は、午後 4:00 にスケジュールされている複製イベントまで待機します。以後複製更新は次に午後 8:00 にスケジュールされている複製イベントまで続けられます。午後 8:00 より後の更新は、すべて次にスケジュールされている複製イベントまで待機します。

注: 複製イベントのスケジュールが近すぎる場合、次のイベントがスケジュールされている時に前のイベントの更新がまだ進行中である場合は、複製イベントは欠落することがあります。

## 複製キューの管理

以下の情報を参考にして、このサーバーで使用される複製契約 (キュー) ごとに複製の状況をモニターします。

1. ナビゲーション領域の「複製管理」カテゴリを展開し、「キューの管理」をクリックします。

2. キューを管理するレプリカを選択します。
3. レプリカの状態に応じて、「**中断/再開**」をクリックして複製を停止または開始できる。
4. 「**複製の強制**」をクリックすると、次の複製がいつスケジュールされているかに無関係に、すべての保留変更が複製される。
5. レプリカのキューに関する詳細については、「**キューの詳細**」をクリックする。この選択からキューを管理することもできます。
6. 複製エラーの管理パネルを表示するには、「**View Errors (エラーの表示)**」をクリックします。ここで、複製エラー・ログの表示、失敗した変更の再試行、またはログからの項目の除去を行うことができます。
7. 「**再表示**」をクリックすると、キューが更新され、サーバー・メッセージがクリアされる。

「**キューの詳細**」をクリックすると、3 つのタブが表示されます。

- 状況
- 最終試行の詳細
- 変更の保留

「**状況**」タブには、レプリカ名、そのサブツリー、その状況、および複製時間のレコードが表示されます。このパネルで「**再開**」をクリックすると複製を中断または再開できます。「**再表示**」をクリックするとキュー情報が更新されます。

「**最終試行の詳細**」タブには、最後の更新試行に関する情報が表示されます。項目をロードできない場合は、「**ブロッキング項目のスキップ**」をクリックし、次の保留中の項目から複製を続けます。「**再表示**」をクリックするとキュー情報が更新されます。

「**変更の保留**」タブには、レプリカに対するすべての保留変更が表示されます。複製がブロックされている場合、「**すべてスキップ**」をクリックすると、保留変更をすべて削除できます。「**再表示**」をクリックすると、保留変更のリストが更新され、処理済みの新規の更新が反映されます。

注: ブロッキング変更をスキップすることを選択する場合、コンシューマー・サーバーがいつか更新されるようにする必要があります。

#### 関連概念

49 ページの『複製エラー・テーブル』

後でリカバリーするために、複製エラー・テーブルが失敗した更新を記録します。複製が開始すると、各複製契約ごとにログ記録された障害数がカウントされます。更新が結果として失敗すると、このカウントが増え、新しい項目がテーブルに追加されます。

#### 関連資料

277 ページの『Idapdiff』

LDAP レプリカ同期コマンド行ユーティリティー

## 遺失物取り扱いログの設定の変更

遺失物取り扱いログ (デフォルト名は LostAndFound.log) は、複製の競合として生じたエラーを記録します。ファイルのロケーションと最大サイズや、古いログ・ファイルのアーカイブも含め、遺失物取り扱いログを制御するための設定があります。

遺失物取り扱いログの設定を変更するには、次のようにします。

1. IBM Tivoli Directory Server のWeb 管理ツールで、「**Server Administration (サーバー管理)**」を展開表示してから、ナビゲーション域の「**ログ**」を展開表示し、「**Modify log settings (ログ設定の変更)**」をクリックします。
2. 「**Lost and found log (遺失物取り扱いログ)**」をクリックします。
3. エラー・ログのパスおよびファイル名を入力します。ファイルが ldap サーバーに存在し、パスが有効であることを確認します。デフォルトのログ・パスは `<drive>#idsldap-<instance-name>#logs` です。ただし、*drive* は、Directory Server インスタンスの作成時に指定したドライブであり、*instance name* は、Directory Server インスタンスの名前です。受け入れられないファイル名 (たとえば、構文が無効な場合や、ファイルの作成または変更のどちらか一方または両方の権限がサーバーにない場合など) のファイルを指定した場合、LDAP Server is unwilling to perform the operation (LDAP サーバーはこの操作を実行しません) というエラーとともに、この試行は失敗します。
4. 「**Log size threshold (MB) (ログ・サイズしきい値 (MB))**」の下で、最初のラジオ・ボタンを選択し、最大ログ・サイズをメガバイト数で入力します。ログ・サイズに対する制限を設けたくない場合、代わりに「**制限なし**」ラジオ・ボタンを選択します。
5. 「**Maximum log archives (最大ログ・アーカイブ数)**」の下で、以下のうちの 1 つを選択します。
  - 最大数のアーカイブ・ログを指定する場合、編集ウィンドウが隣に付いているラジオ・ボタンを選択します。保存する予定のアーカイブの最大数を入力します。1 つのアーカイブ・ログは、サイズのしきい値に達した、前のログです。
  - ログをアーカイブする予定のない場合は、「**No archives (アーカイブしない)**」を選択します。
  - アーカイブするログの数を制限しない場合、「**制限なし**」を選択します。
6. 「**Log archive path (ログ・アーカイブのパス)**」の下で、以下のいずれかを行います。
  - アーカイブを保管するパスを指定する場合、編集ウィンドウが隣に付いているラジオ・ボタンを選択し、任意のパスを指定します。
  - ログ・ファイルを置いているディレクトリー内にアーカイブを保管する場合、「**Same directory as log file (ログ・ファイルと同じディレクトリー)**」ラジオ・ボタンを選択します。
7. 「**適用**」をクリックして、変更を適用し、ログの処理を続けるか、または「**OK**」をクリックして変更を保存し、「IBM Tivoli Directory Server Web Administration Introduction (IBM Tivoli Directory Server Web 管理の紹介)」パネルに戻ります。変更を保存しないで「IBM Tivoli Directory Server Web Administration Introduction (IBM Tivoli Directory Server Web 管理の紹介)」パネルに戻るには、「**キャンセル**」をクリックします。

#### 関連資料

42 ページの『複製の概要』

複製の時、1 つのディレクトリーに行われた変更は、1 つ以上の追加のディレクトリーに伝搬します。それにより、1 つのディレクトリーに変更を行うと、複数の異なるディレクトリーに影響します。

### 遺失物取り扱いログ・ファイルの表示

複製の遺失物取り扱いログ・ファイルを表示するには、IBM Tivoli Directory Server のWeb 管理ツールを使用するか、または ldapexop ユーティリティのログ・ファイル・オプションを使用するか、あるいは、ファイルを直接表示します。

Web 管理ツールを使用して遺失物取り扱いログ・ファイルを表示するには、Web 管理ナビゲーション域の「**Server Administration (サーバー管理)**」を展開表示してから、展開したリスト中の「**ログ**」を展開表示します。

1. 「**ログの表示**」をクリックします。

2. 「ログの表示」パネルで、「Lost and found log (遺失物取り扱いログ)」を選択し、「表示」ボタンをクリックします。

注: このパネルにアクセスできるユーザーは、ディレクトリー管理者および管理グループ・メンバーのみです。

ldapexop ユーティリティーを使用して遺失物取り扱いログを表示するには、QShell から次のようにします。

```
ldapexop -D -w -op readlog -log LostAndFound -lines all
```

遺失物取り扱いログをクリアするには、次のようにします。

```
ldapexop -D -w -op clearlog -log LostAndFound
```

注: \*ALLOBJ および \*IOSYSCFG 特殊権限を持ったユーザーとしてか、または Directory Server への管理者権限を与えられたユーザーとして i5/OS システムにサインオンする場合、管理者 DN とパスワードを入力する代わりに、-m OS400-PRFTKN オプションを指定した ldapexop ユーティリティーを使用することができます。例:

```
ldapexop -m OS400-PRFTKN -op readlog -log LostAndFound -lines all
```

#### 関連資料

252 ページの『ldapexop』

LDAP 拡張操作コマンド行ユーティリティー

## セキュア接続での複製のセットアップ

以下の情報を参考にして、セキュア接続上で複製をセットアップします。

SSL での複製は、プロセスを通してすべてを確認できるように、いくつかの段階でセットアップする必要があります。

セキュア接続で複製の構成を試みる前に、以下のタスクを (任意の順序で) 完了する必要があります。

- 非セキュア接続で複製を構成する。
- コンシューマー・サーバーを構成して、セキュア・ポート上にセキュア接続を受け入れる。ldapsearch ユーティリティーなどを使用して、クライアントがコンシューマー・サーバーへのセキュア接続を使用できることを確認してください。サプライヤー・サーバーが認証のために信任状 (SSL での SASL 外部バインドなど) を使用するようにしたい場合は、最初にサーバー認証、次に、クライアントとサーバー認証をセットアップしてください。ここでの「サーバー」はコンシューマー・サーバーであり、クライアントはサプライヤー・サーバーです。

注: クライアントおよびサーバー認証を使用するようにサーバーを構成する時には、SSL を使用するすべてのクライアントがクライアント証明書をもっていなければなりません。

- コンシューマーの証明書を発行した認証局を信頼するように、サプライヤー・サーバーを構成する。
  1. Web 管理ツールで、「複製管理」カテゴリの「トポロジーの管理」をクリックする。
  2. セキュアにしたい既存の合意の 1 つを選択する。
  3. 「合意の編集...」を選択し、SSL の使用を選択して、正しいポート番号を使用するようにする。636 が標準セキュア・ポート番号です。
  4. この合意での複製が正しく作動していることを確認する。

セキュア接続を介して DN とパスワードを使用し、認証するための複製のセットアップのみを試みている場合は、これは前のステップで実行されています。クライアント証明書を使用する認証では、その合意でサ



プライヤー・サーバーが別の信任状オブジェクトを使用する必要があり、さらに、サプライヤー・サーバーとしてその証明書を受け入れるようにコンシューマー・サーバーを構成することも必要になります。

## 複製トポロジー・タスク

以下の情報を参考にして、複製されたサブツリーのトポロジーを管理します。

トポロジーは複製されたサブツリーに固有のものです。

### トポロジーの表示

以下の情報を参考にして、サブツリーのトポロジーを表示します。

注: このタスクを実行するには、サーバーが稼働している必要があります。

ナビゲーション領域の「複製管理」カテゴリを展開し、「トポロジーの管理」をクリックする。

表示するサブツリーを選択し、「トポロジーの表示」をクリックする。

トポロジーが「複製トポロジー」リストに表示されます。トポロジーを展開するには、青い三角形をクリックします。このリストから、以下を行うことができます。

- レプリカを追加する。
- 既存のレプリカに関する情報を編集する。
- レプリカの別のサプライヤー・サーバーに変更する、またはレプリカをマスター・サーバーにプロモートする。
- レプリカを削除する。
- 1. 複製のスケジュールを表示する。

### レプリカの追加

以下の情報を参考にして、レプリカを作成します。

注: ここで説明しているステップは、Web 管理タスクを通してレプリカを追加する方法を示しています。これらのステップは、新規サーバーを正しく初期化するのに必要なその他のステップで構成される全体的なプロセスの一部を成します。下記の関連リンクのトピックを参照してください。

注: このタスクを実行するには、サーバーが稼働している必要があります。

ナビゲーション領域の「複製管理」カテゴリを展開し、「トポロジーの管理」をクリックする。

1. 複製するサブツリーを選択し、「トポロジーの表示」をクリックする。
2. 「複製トポロジー」選択の隣の矢印をクリックし、サプライヤー・サーバーのリストを展開する。
3. サプライヤー・サーバーを選択し、「レプリカの追加」をクリックする。
4. 「レプリカの追加」ウィンドウの「サーバー」タブで、以下のようになります。
  - a. 作成しているレプリカのホスト名およびポート番号を入力する。デフォルト・ポートは、非 SSL の場合は 389、SSL の場合は 636 です。これらは必要フィールドです。
  - b. SSL 通信を使用可能にするかどうかを選択する。
  - c. レプリカ名を入力するか、このフィールドを空白にしてホスト名を使用する。

- d. レプリカ ID を入力する。レプリカを作成しているサーバーが実行中の場合は、「**レプリカ ID の取得**」をクリックすると、このフィールドが自動的に事前に入力されます。追加するサーバーをピアまたは転送サーバーにする場合は、これは必要フィールドです。すべてのサーバーが同じリリースであることが推奨されています。
  - e. レプリカ・サーバーの説明を入力する。
5. 「**追加**」タブで、以下のようにします。

- レプリカがマスターとの通信に使用する信任状を指定する。

注: Web 管理ツールでは、以下の場所で信任状を定義できます。

- **cn=replication,cn=localhost**: 信任状を使用するサーバーにのみ保持します。
- 複製サブツリー内: サブツリーの残りの部分で信任状が複製されます。複製サブツリーに置く信任状は、そのサブツリーの **ibm-replicagroup=default** 項目の下に作成されます。

信任状を **cn=replication,cn=localhost** に置くほうが安全性が高くなります。複製サブツリーに置く信任状は、そのサブツリーの **ibm-replicagroup=default** 項目の下に作成されます。

- 「**選択**」をクリックする。
  - 使用する信任状の場所を選択する。望ましい場所は **cn=replication,cn=localhost** です。
  - 「**信任状の表示**」をクリックする。
  - 信任状のリストを展開し、使用したい信任状を選択する。
  - 「**OK**」をクリックする。

合意信任状についての追加情報は、複製の信任状の作成を参照してください。

- ドロップダウン・リストから複製スケジュールを指定するか、「**追加**」をクリックしてそれを作成する。複製スケジュールの作成を参照してください。
- サプライヤー機能のリストから、コンシューマーに複製したくないすべての機能を選択解除できます。

ネットワークで異なるリリースのサーバーを混用している場合、古いリリースでは使用不可である機能を新しいリリースで使用できます。フィルター ACL やパスワード・ポリシーのような幾つかの機能では、他の変更で複製される操作属性を活用します。ほとんどの場合、これらの機能を使用するときには、すべてのサーバーがこれらの機能をサポートするようにしたいはずですが、もしすべてのサーバーがその機能をサポートするのであれば、それを使用したくないでしょう。たとえば、サーバーごとに異なる ACL を使用したくないはずですが、しかしながら、ある機能をサポートするサーバーでそれを使用し、その機能に関連した変更を、その機能をサポートしないサーバーには複製したくない場合もあるかもしれません。そのような場合、機能リストを使用して、複製しない機能を明確にできます。

- 1 • 複製方法として、単一スレッドまたはマルチスレッドを選択する。マルチスレッドを指定する場合、複製で使用する接続数 (2 から 32) も指定する必要があります。デフォルトの接続数は 2 です。
- 1 • 「**OK**」をクリックしてレプリカを作成する。

6. 追加アクションが必要であることを通知するメッセージが表示される。「**了解**」をクリックする。

注: 追加レプリカとしてさらにサーバーを追加したり、複雑なトポロジーを作成する場合、マスター・サーバーでのトポロジーの定義を完了するまでは、レプリカへのデータのコピーまたは新規レプリカへのサプライヤー情報の追加には進まないでください。トポロジーを完成させた後に

*masterfile.ldif* を作成する場合、それはマスター・サーバーのディレクトリー項目およびトポロジー合意の完全なコピーを含みます。このファイルをサーバーごとにロードすると、各サーバーは以後同じ情報を持つようになります。

## 関連タスク

178 ページの『ゲートウェイ・トポロジーのセットアップ』

以下の情報を参考にして、ゲートウェイ・トポロジーをセットアップします。

## ピア・マスターまたはゲートウェイ・サーバーの追加

このトピックでは、新規のピア・マスターまたはゲートウェイ・サーバーを作成する方法を説明します。

**注:** ここで説明しているステップは、Web 管理タスクを通してピア・マスターまたはゲートウェイ・サーバーを追加する方法を示しています。これらのステップは、新規サーバーを正しく初期化するのに必要なその他のステップで構成される全体的なプロセスの一部を成します。下記の関連リンクのトピックを参照してください。

ナビゲーション領域の「複製管理」カテゴリーを展開し、「トポロジーの管理」をクリックします。

- 複製するサブツリーを選択し、「トポロジーの表示」をクリックします。
- 既存のトポロジーを表示するには、「複製トポロジー」の横のボックスをクリックし、サプライヤー・サーバーのリストを展開します。
- 「Add master (マスターの追加)」をクリックします。

「Add master (マスターの追加)」ウィンドウの「サーバー」タブで、以下のようになります。

- 作成しているサーバーのホスト名およびポート番号を入力します。デフォルト・ポートは、非 SSL の場合は 389、SSL の場合は 636 です。これらは必要フィールドです。
- SSL 通信を使用可能にするかどうかを選択します。
- ゲートウェイ・サーバーとしてサーバーを作成するかどうかを選択します。
- サーバー名を入力するか、またはこのフィールドをブランクにしてホスト名を使用します。
- 「server ID (サーバー ID)」に入力します。ピア・マスターの作成場所であるサーバーが実行中の場合は、「サーバー ID の取得」をクリックすると、このフィールドの自動事前入力が行われます。
- サーバーの説明を入力します。
- サーバーが他のマスター・サーバーとの通信で使用する信任状を指定する必要があります。「選択」をクリックします。

**注:** Web 管理ツールでは、以下の場所で信任状を定義できます。

- cn=replication,cn=localhost:** 信任状を使用するサーバーにのみ保持します。信任状を `cn=replication,cn=localhost` に置くほうが安全性が高くなります。
- cn=replication,cn=IBMpolicies.** これは、レプリカの追加で使用するサーバーが、Web 管理ツールで接続しているのと同じサーバーではない場合でも使用可能です。このロケーションに置かれた信任状が、それらのサーバーに複製されます。

**注:** ロケーション `cn=replication,cn=IBMpolicies` を使用できるのは、`root DSE` の `ibm-supportedcapabilities` の下に `IBMpolicies サポート OID 1.3.18.0.2.32.18` がある場合のみです。

- 複製サブツリー内: サブツリーの残りの部分で信任状が複製されます。複製サブツリーに置く信任状は、そのサブツリーの `ibm-replicagroup=default` 項目の下に作成されます。
- 使用する信任状の場所を選択します。望ましい場所は `cn=replication,cn=localhost` です。

2. 一連の信任状をすでに作成済みの場合、「信任状の表示」をクリックします。
3. 信任状のリストを展開し、使用したい信任状を選択します。
4. 「OK」をクリックします。
5. 既存の信任状がない場合、「追加」をクリックし、信任状を作成します。

「追加」タブで、以下のようになります。

1. ドロップダウン・リストから複製スケジュールを指定するか、または「追加」をクリックしてそれを作成します。複製スケジュールの作成を参照してください。
2. サプライヤー機能のリストから、コンシューマーに複製したくないすべての機能を選択解除できます。

ネットワークで異なるリリースのサーバーを混用している場合、古いリリースでは使用不可である機能を新しいリリースで使用できます。フィルター ACL (フィルター済みのアクセス制御リスト) やパスワード・ポリシー (パスワード・ポリシー・プロパティの設定) などの一部の機能では、他の変更にあわせて複製される操作属性を活用します。たいていの場合、これらのフィーチャーを使用する場合、すべてのサーバーでそのフィーチャーがサポートされるのが望ましいはずですが、もしすべてのサーバーがその機能をサポートするのであれば、それを使用したくないでしょう。たとえば、サーバーごとに異なる ACL を使用したくないはずですが、しかしながら、ある機能をサポートするサーバーでそれを使用し、その機能に関連した変更を、その機能をサポートしないサーバーには複製したくない場合もあるかもしれません。そのような場合、機能リストを使用して、複製しない機能を明確にできます。

3. サプライヤーの信任状の動的更新を有効にするには、「**Add credential information on consumer (コンシューマーに関する信任状情報の追加)**」チェック・ボックスにチェックを付けます。その選択によって、作成しようとしているサーバーの構成ファイル内のサプライヤー情報が自動的に更新されます。すると、トポロジー情報をサーバーに複製できるようになります。
  - コンシューマー・サーバーの管理 DN を入力します。たとえば、cn=root と入力します。

注: サーバー構成プロセス中に作成された管理者 DN が cn=root である場合は、完全な管理者 DN を入力します。単に root だけを入力しないでください。

- コンシューマー・サーバーの管理パスワードを入力します。たとえば、secret と入力します。

4. 「OK」をクリックします。
5. 新規のマスター・サーバーとすべて既存のサーバーの間の、サプライヤーとコンシューマーの契約がリストされます。作成する必要はないと思われる契約はすべて、チェック・マークを外します。これは、ゲートウェイ・サーバーを作成する場合は特に重要です。
6. 「続行」をクリックします。
7. 追加アクションをとる必要があることを通知するメッセージが表示されることがあります。該当するアクションを実行するか、またはメモをとっておきます。完了したら、「OK」をクリックします。
8. 該当する信任状を追加します。

注: 場合によっては、cn=replication,cn=localhost 以外の場所に置かれている信任状を求める「信任状の選択」パネルが表示されます。その状況では、cn=replication,cn=localhost 以外の場所に置かれている信任状オブジェクトを入力する必要があります。既存の信任状のセットからサブツリーで使用する信任状を選択するか、新しい信任状を作成します。

9. サプライヤーの信任状の動的更新を有効にするには、「**Add credential information on consumer (コンシューマーに関する信任状情報の追加)**」チェック・ボックスにチェックを付けます。その選択によって、作成しようとしているサーバーの構成ファイル内のサプライヤー情報が自動的に更新されます。すると、トポロジー情報をサーバーに複製できるようになります。
  - コンシューマー・サーバーの管理 DN を入力します。たとえば、cn=root と入力します。

注: サーバー構成プロセス中に作成された管理者 DN が cn=root である場合は、完全な管理者 DN を入力します。単に root だけを入力しないでください。

- コンシューマー・サーバーの管理パスワードを入力します。たとえば、secret と入力します。

10. 「OK」をクリックして、ピア・マスターを作成します。

11. 追加アクションをとる必要があることを通知するメッセージが表示されることがあります。該当するアクションを実行するか、またはメモをとっておきます。完了したら、「OK」をクリックします。

注: Web 管理ツールを使った「Add master (マスターの追加)」の操作中の、コンシューマーに関する信任状の追加のときに、外部信任状オブジェクトを選択した場合、IBM WebSphere Application Server を実行しているマシン上で、以下の設定を構成する必要があります。

- WAS\_HOME\java\jre\lib\ext の下には、次のような jar ファイルがあります。

- ibmjceprovider.jar

- ibmpkcs.jar

- ibmjcefw.jar

- local\_policy.jar

- US\_export\_policy.jar

- ibmjlog.jar

- gsk7cls.jar

- WAS\_HOME\java\jre\lib\security\java.security ファイルには、CMS プロバイダーおよび JCE プロバイダーの登録のための次のような 2 行がなければなりません。

```
security.provider.2=com.ibm.spi.IBMCMSProvider
```

```
security.provider.3=com.ibm.crypto.provider.IBMJCE
```

- IBM WebSphere Application Server を再始動します。

- Gskit がインストール済みであって、gsk7lib がシステム・パス内になければなりません。

- マスター・サーバーがレプリカに接続するときに使用する信任状情報の入った鍵ファイルを Web 管理ツールが読み取って、レプリカに関する信任状を作成するためには、その鍵ファイルは、Windows プラットフォームの場合は C:\temp に、UNIX の場合は /tmp になければなりません。

## 関連タスク

178 ページの『ゲートウェイ・トポロジーのセットアップ』

以下の情報を参考にして、ゲートウェイ・トポロジーをセットアップします。

## ゲートウェイ・サーバーの管理

このトピックでは、ゲートウェイ・サーバーの管理について説明します。マスター・サーバーが複製サイトでゲートウェイ・サーバーとしての役割を持つかどうかを指定することができます。

マスターをゲートウェイ・サーバーにすることを指定するには、ナビゲーション領域の「複製管理」カテゴリを展開し、「トポロジーの管理」をクリックします。

1. 表示するサブツリーを選択し、「トポロジーの表示」をクリックします。

2. 「Manage gateway servers (ゲートウェイ・サーバーの管理)」をクリックします。

3. ゲートウェイ・サーバーにする予定のサーバーを「Master servers (マスター・サーバー)」ボックスで選択します。

4. 「Make gateway (ゲートウェイにする)」をクリックします。そのサーバーは、「Master servers (マスター・サーバー)」ボックスから「Gateway servers (ゲートウェイ・サーバー)」ボックスに移動されます。

5. 「OK」をクリックします。
- ゲートウェイ・サーバーの役割をマスター・サーバーから除去するには、以下のようになります。
1. 「**Manage gateway servers (ゲートウェイ・サーバーの管理)**」をクリックします。
2. マスター・サーバーにする予定のサーバーを「**Gateway servers (ゲートウェイ・サーバー)**」ボックスで選択します。
3. 「**Make master (マスターにする)**」をクリックします。そのサーバーは、「**Gateway servers (ゲートウェイ・サーバー)**」ボックスから「**Master servers (マスター・サーバー)**」ボックスに移動されます。
4. 「OK」をクリックします。

注: どの複製サイトでも、配備できるゲートウェイ・サーバーは 1 つのみであることに注意してください。追加のゲートウェイ・サーバーをトポロジーで作成した場合、そのゲートウェイは Web 管理ツールによってピア・サーバーとして扱われ、トポロジー内のすべてのサーバーに対する契約が作成されます。他のゲートウェイ・サーバーを対象にしていなかったり、またはゲートウェイ自身の複製サイト内になかったりする契約はすべて、必ず選択を解除してください。

詳細は、以下の関連リンクの『ゲートウェイ・トポロジーのセットアップ』のトピックを参照してください。

#### 関連タスク

178 ページの『ゲートウェイ・トポロジーのセットアップ』  
以下の情報を参考にして、ゲートウェイ・トポロジーをセットアップします。

### サーバー情報の表示

「View server (サーバーの表示)」パネルから、サーバー名、ホスト名、ポート、サーバー ID、役割、構成モード、インスタンス名、およびセキュリティーを表示することができます。

Web 管理ツールのナビゲーション領域の「複製管理」カテゴリーを展開し、「トポロジーの管理」をクリックします。

1. 表示するサブツリーを選択し、「トポロジーの表示」をクリックします。
2. 表示するサーバーを選択します。
3. 「**View server (サーバーの表示)**」をクリックして、「View server (サーバーの表示)」パネルを表示します。

「View server (サーバーの表示)」パネルには、次のような情報が表示されます。

#### サーバー名

このフィールドには、ディレクトリー・インスタンスの稼働場所であるサーバーの名前が表示されます。この情報は、hostname:port というフォーマットで表示されます。

#### ホスト名

このフィールドには、Directory Server インスタンスの稼働場所であるマシンのホスト名が表示されます。

**ポート** このフィールドには、サーバーが listen する場所である非セキュア・ポートが表示されます。

#### サーバー ID

このフィールドには、サーバーの最初の始動時にサーバーに割り当てられた固有 ID が表示されます。この ID は、サーバーの役割を判別するために複製トポロジーで使用されます。

**役割** このフィールドには、複製トポロジー内のサーバーの構成済みの役割が表示されます。

## 構成モード

このフィールドでは、サーバーが構成モードで稼働しているかどうかを確認されます。これが TRUE の場合、サーバーは構成モードになっています。 FALSE の場合は、サーバーは構成モードになっていません。

## インスタンス名

このフィールドには、サーバーで稼働する Directory Server インスタンスの名前が表示されます。

## セキュリティー

このフィールドには、サーバーが listen する場所であるセキュアな SSL ポートが表示されます。

サーバー名、ID、および役割とコンシューマーの情報が表示されます。

## 複製のスケジュールの表示

Web 管理ツールを使用して複製のスケジュールを表示するには、次のステップを行います。

Web 管理ツールのナビゲーション領域の「複製管理」カテゴリを展開し、「トポロジーの管理」をクリックします。

1. 表示するサブツリーを選択し、「トポロジーの表示」をクリックする。
2. 表示するマスター・サーバーまたはゲートウェイ・サーバーを選択する。
3. 「スケジュールの表示」をクリックする。

選択したサーバーとそのコンシューマーの間に複製のスケジュールが存在する場合、それが表示されます。そのスケジュールを変更または削除することができます。スケジュールが存在してなくて、作成したい場合、Web 管理ツールのナビゲーション領域の「Manage schedules (スケジュールの管理)」機能を使用する必要があります。スケジュールの管理の詳細は、以下の関連リンクの『複製スケジュールの作成』を参照してください。

### 関連タスク

- 182 ページの『複製スケジュールの作成』
- 以下の情報を参考にして、複製のスケジュールを作成します。

## 合意の編集

以下の情報を参考にして、複製合意を編集します。

レプリカの以下の情報を変更できます。

1. 「サーバー」タブでは、以下のみを変更できます。
  - ホスト名
  - ポート
  - SSL を使用可能にする
  - 説明
2. 「追加」タブで以下を変更できます。
  - 信任状 - 167 ページの『複製の信任状の作成』を参照してください。
  - 複製スケジュール - 182 ページの『複製スケジュールの作成』を参照してください。
  - コンシューマー・レプリカに複製される機能を変更する。サプライヤー機能のリストから、コンシューマーに複製したくないすべての機能を選択解除できます。
3. 完了したら、「OK」をクリックする。

## サーバーの移動またはプロモート

以下の情報を参考にして、サーバーを移動またはプロモートします。

1. サーバーを選択し、「移動」をクリックする。
2. レプリカの移動先のサーバーを選択するか、または「複製トポロジー」を選択してレプリカをマスターにプロモートする。「移動」をクリックする。
3. 場合によっては、「信任状の選択」パネルが表示され、cn=replication,cn=localhost 以外の場所に置かれている信任状の入力が求められます。その状況では、cn=replication,cn=localhost 以外の場所に置かれている信任状オブジェクトを入力する必要があります。既存の信任状のセットからサブツリーで使用する信任状を選択するか、新しい信任状を作成します。167 ページの『複製の信任状の作成』を参照してください。
4. 「追加のサプライヤー合意の作成」が表示される。サーバーの役割にふさわしいサプライヤー合意を選択する。たとえば、レプリカ・サーバーがピア・サーバーとしてプロモートされる場合、他のすべてのサーバーおよびそれらの第 1 レベル・レプリカを含むサプライヤー合意を作成する選択をする必要があります。これらの合意により、プロモートされたサーバーを他のサーバーおよびそのレプリカに対するサプライヤーとして機能させることができます。他のサーバーから新規にプロモートされたサーバーの既存のサプライヤー合意は依然として有効で、再作成する必要はありません。
5. 「OK」をクリックする。

トポロジー・ツリーの変更は、サーバーの移動を反映します。

### 関連タスク

175 ページの『ピア複製での複雑なトポロジーの作成』

以下の情報を参考にして、ピア複製を使って複雑なトポロジーを作成します。

## マスターのデモート

以下の情報を参考にして、サーバーの役割をマスターからレプリカに変更します。

サーバーの役割をマスターからレプリカに変更するには、以下のようになります。

1. デモートするサーバーに Web 管理ツールを接続する。
2. 「トポロジーの管理」をクリックする。
3. サブツリーを選択し、「トポロジーの表示」をクリックする。
4. デモートしたいサーバーのすべての合意を削除する。
5. デモートされるサーバーを選択し、「移動」をクリックする。
6. デモートされるサーバーを下に置くサーバーを選択し、「移動」をクリックする。
7. 新規レプリカの場合と同様、デモートされたサーバーとそのサプライヤー間の新規サプライヤー合意を作成する。詳細は、169 ページの『レプリカ・サーバーの作成』を参照してください。

## サブツリーの複製

以下の情報を参考にして、サブツリーを複製します。

注: このタスクを実行するには、サーバーが稼働している必要があります。

ナビゲーション領域の「複製管理」カテゴリーを展開し、「トポロジーの管理」をクリックする。

1. 「サブツリーの追加」をクリックする。
2. 複製するサブツリーの DN を入力するか、「ブラウズ」をクリックして項目を展開し、サブツリーのルートにする項目を選択する。



3. マスター・サーバー参照 URL を入力する。これは、LDAP URL の形式でなければなりません。例を以下に示します。

```
ldap://<myservername>.<mylocation>.<mycompany>.com
```

4. 「OK」をクリックする。

新規サーバーは、見出し「複製サブツリー」の下にある「トポロジーの管理」パネル上に表示される。

## サブツリーの編集

以下の情報を使用して、このサブツリーおよびそのレプリカから更新を送信する先のマスター・サーバーの URL を変更します。マスター・サーバーのポート番号またはホスト名を変更する場合や、マスターを別のサーバーに変更する場合にはこれを行う必要があります。

1. 編集するサブツリーを選択する。
2. 「サブツリーの編集」をクリックする。
3. マスター・サーバー参照 URL を入力する。これは、LDAP URL の形式でなければなりません。例を以下に示します。

```
ldap://<mynewservername>.<mylocation>.<mycompany>.com
```

このサブツリー上のサーバーが果たしている役割により (マスター、レプリカ、または転送のいずれか)、異なるラベルおよびボタンがパネルに表示されます。

- サブツリーの役割がレプリカである場合、サーバーがレプリカまたはフォワーダーとして機能することを示すラベルが、ボタン「サーバーをマスターにする」と共に表示されます。このボタンをクリックすると、Web 管理ツールが接続しているサーバーがマスターになります。
- サブツリーが補助クラスの追加のみによる複製用に構成されている場合 (デフォルト・グループおよび副項目がない場合)、「このサブツリーは複製されていません」というラベルが「サブツリーの複製」ボタンと共に表示されます。このボタンをクリックすると、Web 管理ツールが接続しているサーバーがマスターになるように、デフォルト・グループおよび副項目が追加されます。
- マスター・サーバー用の副項目がない場合、ラベル「このサブツリーにはマスター・サーバーが定義されていません」が「サーバーをマスターにする」とタイトルが付いたボタンと共に表示されます。このボタンをクリックすると、Web 管理ツールが接続しているサーバーがマスターになるように、欠落した副項目が追加されます。

## サブツリーの除去

以下の情報を参考にして、サブツリーを除去します。

1. 除去するサブツリーを選択する。
2. 「サブツリーの削除」をクリックする。
3. 削除の確認メッセージが表示された場合は、「OK」をクリックする。

サブツリーが「複製されたサブツリー」リストから除去される。

注: この操作は、ibm-replicaGroup=default 項目が空の場合のみ成功します。

## サブツリーの静止

以下の情報を参考にして、サブツリーを静止します。

この機能は、トポロジーの保守時や変更時に有用です。これにより、サーバーに対して行われる更新の数が最小化されます。静止しているサーバーはクライアント要求を受け入れません。サーバー管理制御を使用する管理者からの要求のみが受け入れられます。

この機能はブールです。

1. 「**静止/静止解除**」をクリックし、サブツリーを静止する。
2. アクションの確認メッセージが表示された場合は、「**OK**」をクリックする。
3. 「**静止/静止解除**」をクリックし、サブツリーを静止解除する。
4. アクションの確認メッセージが表示された場合は、「**OK**」をクリックする。

## アクセス制御リストの編集

このトピックでは、アクセス制御リスト (ACL) を編集するのに必要な権限について説明し、ACL を使った作業に関する解説を述べます。

複製情報 (レプリカ副項目、レプリカ合意、スケジュール、そしておそらく信任状も) は特別なオブジェクト、**ibm-replicagroup=default** の下に保管されます。ibm-replicagroup オブジェクトは、複製されたサブツリーのルート項目のすぐ下に置かれます。デフォルトでは、このサブツリーは、複製されたサブツリーのルート項目から ACL を継承します。この ACL は、複製情報へのアクセスを制御するためには適さない可能性があります。

必要な権限:

- 複製の制御 - ibm-replicagroup=default オブジェクトへの書き込みアクセス権限を持っている必要があります (または所有者または管理者である必要があります)。
- 複製のカスケード制御 - ibm-replicagroup=default オブジェクトへの書き込みアクセス権限を持っている必要があります (または所有者または管理者である必要があります)。
- キューの制御 - レプリカ合意への書き込みアクセス権限を持っている必要があります。

Web 管理ツールを使用して ACL プロパティを表示したり、ACL を処理したりするには、239 ページの『アクセス制御リスト (ACL) のタスク』を参照してください。

詳しくは、72 ページの『アクセス制御リスト』を参照してください。

## セキュリティ・プロパティ・タスク

以下の情報を参考にして、セキュリティ・プロパティ・タスクを管理します。

Directory Server には、ユーザー・データのセキュリティを保証するためのメカニズムが多数あります。これには、パスワード管理、SSL や TLS を使用した暗号化、Kerberos 認証、および DIGEST-MD5 認証が含まれます。セキュリティ概念の詳細については、57 ページの『Directory Server のセキュリティ』を参照してください。

### 関連概念

57 ページの『Directory Server のセキュリティ』  
多彩な機能を使用して、Directory Server をセキュアにする方法を学んでください。

## パスワード・タスク

以下の情報を参考にして、パスワード・タスクを管理します。

パスワードを管理するには、Web 管理ツールのナビゲーション領域で「**セキュリティ・プロパティの管理**」カテゴリを展開して、「**パスワード・ポリシー**」タブを選択してください。

### 関連概念

86 ページの『パスワード・ポリシー』  
認証に LDAP サーバーの使用においては、LDAP サーバーがパスワードの有効期限、失敗したログイン

ン試行、およびパスワード規則に関するポリシーをサポートすることが重要です。Directory Server では、この種のポリシー 3 つすべてを構成できます。

### パスワード・ポリシー・プロパティの設定:

以下の情報を参考にして、パスワード・ポリシー・プロパティを設定します。

パスワード・ポリシーを設定するには、次のようにしてください。

- 注: 下記のステップは、ユーザー・パスワード・ポリシーを設定する方法を説明しています。管理グループ・メンバーに適用される管理パスワード・ポリシーの詳細は、以下のリンクの『管理パスワードおよびロックアウトのポリシーの設定』を参照してください。
1. Web 管理ツールのナビゲーション領域で「**セキュリティ・プロパティの管理**」カテゴリを展開して、「**パスワード・ポリシー**」タブを選択する。このパネルには、パスワード・ポリシーを使用している属性の名前が含まれている編集不可の「**パスワード属性**」フィールドが表示されます。
  2. ドロップダウン・リストからパスワード暗号化のタイプを選択する。
- なし** パスワードは、両方向暗号化されて検証リストに保管されて、項目の一部として元の平文フォーマットで取り出されます。この設定を使用するには、QRETSVRSEC システム値を 1 に設定する必要があります。
- crypt** パスワードは、ディレクトリーに保管される前に UNIX crypt エンコード・アルゴリズムによってエンコードされます。
- SHA-1** パスワードは、ディレクトリーに保管される前に SHA-1 エンコード・アルゴリズムによってエンコードされます。
- MD5** パスワードは、ディレクトリーに保管される前に MD5 エンコード・アルゴリズムによってエンコードされます。
- AES128**  
パスワードは、ディレクトリーに保管される前に AES128 アルゴリズムで暗号化されて、項目の一部として元のクリア・フォーマットで取り出されます。
- AES192**  
パスワードは、ディレクトリーに保管される前に AES192 アルゴリズムで暗号化されて、項目の一部として元のクリア・フォーマットで取り出されます。
- AES256**  
パスワードは、ディレクトリーに保管される前に AES256 アルゴリズムで暗号化されて、項目の一部として元のクリア・フォーマットで取り出されます。
- 注: AES は、V6R1 LDAP より前のサーバーではサポートされません。AES で暗号化されたパスワードをエクスポートした後、V6R1 より前のサーバーにインポートすると、そのパスワードは使用不能になります。
- 複数のサーバーを使用している場合に、AES 暗号化を使用するには、すべてのサーバーで同じ AES パスフレーズおよびソルトを使用する必要があります。管理者は、使用可能な構成済みのソルトがサーバー構成で表示されている間、パスフレーズの追跡記録をとる必要があります。管理者は、AES を使用する追加のサーバーをセットアップするときには、正しい AES のパスフレーズとソルトを入力する必要があります。
- 詳細は、以下の関連リンクの『パスワードの暗号化』トピックを参照してください。

3. パスワード・ポリシーを使用可能にするには、「パスワード・ポリシーの使用可能化」チェック・ボックスを選択する。

注: パスワード・ポリシーが使用可能でない場合は、このチェック・ボックスが使用可能になるまで、このパネルや他のパスワード・パネル上の他のどの機能も使用可能にはなりません。デフォルトでは、パスワード・ポリシーは使用不可になります。

4. ユーザーがパスワードを変更できるかどうかを指定するには、「ユーザーがパスワードを変更できる」チェック・ボックスを選択する。
5. ユーザーがリセットされたパスワードでログオンした後、そのパスワードを変更する必要があるかどうかを指定するには、「リセットの後にユーザーがパスワードを変更する必要がある」チェック・ボックスを選択する。
6. 初期ログオンの後、パスワードの変更が可能になる前に、ユーザーが再びパスワードを指定する必要があるかどうかを指定するには、「変更時にユーザーがパスワードを送信する必要がある」チェック・ボックスを選択する。
7. パスワード有効期限を設定する。「パスワードは満了しない」ラジオ・ボタンをクリックして、パスワードが特定の時間間隔で変更する必要がないことを指定します。または、「日数」ラジオ・ボタンをクリックして、パスワードのリセットが必要となる時の時間間隔(日数)を指定します。
8. パスワードが失効する前に、パスワード満了警告をシステムによって出すかどうかを設定する。

「警告しない」ラジオ・ボタンをクリックした場合は、直前のパスワードが失効する前に、ユーザーは警告されません。管理者が新規のパスワードを作成するまで、ユーザーはディレクトリーにアクセスできません。

「満了までの日数」ラジオ・ボタンをクリックして、日数(n)を指定した場合は、ユーザーがログオンすると毎回、パスワード変更の警告プロンプトを受け取り、これは、パスワード失効のn日前から開始されます。ユーザーはパスワード失効まではディレクトリーにアクセスできます。

9. パスワードが満了した後、ユーザーがログインできる回数(ある場合)を指定する。この選択によって、ユーザーは満了パスワードでディレクトリーにアクセスすることができます。
10. 「OK」をクリックする。

注: `ldapmodify` ユーティリティー (244 ページの『`ldapmodify` および `ldapadd`』を参照) を使用してパスワード・ポリシーを設定することもできます。

パスワード・ポリシーについては、86 ページの『パスワード・ポリシー』を参照してください。

### 関連概念

60 ページの『パスワードの暗号化』

IBM Tivoli Directory Server では、ユーザー・パスワードへの無許可アクセスを防止することができます。管理者は、片方向の暗号化フォーマットまたは両方向の暗号化フォーマットで、`userPassword` 属性値が暗号化されるようにサーバーを構成することができます。暗号化されたパスワードには、暗号化アルゴリズム名のタグが付けられるので、別々のフォーマットで暗号化された複数のパスワードがディレクトリー内に共存することができます。暗号化構成を変更しても、既存の暗号化されたパスワードは無変更のまま残り、効果を持続します。

### 関連タスク

199 ページの『管理パスワードおよびロックアウトのポリシーの設定』

管理パスワード・ポリシーを設定するには、コマンド行のみを使用します。Web 管理ツールは、管理パスワード・ポリシーをサポートしません。

## | 管理パスワードおよびロックアウトのポリシーの設定:

| 管理パスワード・ポリシーを設定するには、コマンド行のみを使用します。 Web 管理ツールは、管理パスワード・ポリシーをサポートしません。

| 注: \*ALLOBJ および \*IOSYSCFG 特殊権限を持った i5/OS ユーザーとして認証を受ける必要があります。

| EAL4 セキュア構成を使って管理パスワード・ポリシーをオンにするには、次のようなコマンドを発行します。

```
| ldapmodify -D <adminDN> -w <adminPW> -i <filename>
```

| ただし、<filename> には以下が入っています。

```
| dn: cn=pwdPolicy Admin,cn=Configuration
| changetype: modify
| replace: ibm-slapdConfigPwdPolicyOn
| ibm-slapdConfigPwdPolicyOn: true
```

| 管理パスワード・ポリシーを有効にし、デフォルト設定を変更するには、次のようなコマンドを発行します。

```
| ldapmodify -D <adminDN> -w <adminPW> -i <filename>
```

| ただし、<filename> には以下が入っています。

```
| dn: cn=pwdPolicyAdmin,cn=Configuration
| changetype: modify
| replace: ibm-slapdConfigPwdPolicyOn
| ibm-slapdConfigPwdPolicyOn: TRUE
| -
| replace: pwdlockout
| pwdlockout: TRUE
| #select TRUE to enable, FALSE to disable
| -
| replace:pwdmaxfailure
| pwdmaxfailure: 10
| -
| replace:pwdlockoutduration
| pwdlockoutduration: 300
| -
| replace:pwdfailurecountinterval
| pwdfailurecountinterval: 0
| -
| replace:pwdminlength
| pwdminlength: 8
| -
| replace:passwordminalphachars
| passwordminalphachars: 2
| -
| replace:passwordminotherchars
| passwordminotherchars: 2
| -
| replace:passwordmaxrepeatedchars
| passwordmaxrepeatedchars: 2
| -
| replace:passwordmindiffchars
| passwordmindiffchars: 2
```

| 注: 認証障害数が多すぎる場合、管理アカウントをロックすることができます。このことは、リモート・クライアント接続にのみ当てはまります。そのアカウントは、サーバーの始動時にリセットされます。

| 関連タスク

- 1 197 ページの『パスワード・ポリシー・プロパティの設定』
- 1 以下の情報を参考にして、パスワード・ポリシー・プロパティを設定します。

#### パスワード・ロックアウト・プロパティの設定:

以下の情報を参考にして、パスワード・ロックアウト・プロパティを設定します。

1. Web 管理ツールのナビゲーション領域で「**セキュリティ・プロパティの管理**」カテゴリを展開してから、「**パスワード・ロックアウト**」タブを選択する。

注: パスワード・ポリシーがサーバーで使用可能でない場合は、このパネルの機能も有効にはなりません。

2. 満了する秒数、分数、時間数、または日数を指定する。この後で、パスワードの変更が可能になります。
3. 間違ったログインでパスワードがロックアウトされるかどうかを指定する。
  - 無制限のログイン試行回数を許可したい場合は、「**パスワードはロックアウトされない**」ラジオ・ボタンを選択する。この選択によって、パスワード・ロックアウト機能は使用不可になります。
  - 「**試行回数**」ラジオ・ボタンを選択して、パスワードをロックアウトする前に許可されるログイン試行回数を指定する。この選択によって、パスワード・ロックアウト機能が使用可能になります。
4. ロックアウトの期間を指定する。「**ロックアウトは満了しない**」ラジオ・ボタンを選択して、システム管理者がパスワードをリセットする必要があることを指定するか、あるいは「**秒数**」ラジオ・ボタンを選択して、ロックアウトが満了して、ログイン試行を再開できるようになるまでの秒数を指定します。
5. 間違ったログインの有効期限を指定する。「**間違ったログインのみが正しいパスワードで消去される**」ラジオ・ボタンをクリックして、間違ったログインが正常なログインによってのみ消去されることを指定するか、あるいは「**秒数**」ラジオ・ボタンをクリックして、失敗したログインの試行がメモリーから消去されるまでの秒数を指定します。

注: このオプションが作動するのは、パスワードがロックアウトされない場合のみです。

6. 完了したら、「**適用**」をクリックし、終了しないで変更を保管するか、あるいは「**OK**」をクリックして変更を適用して終了するか、あるいは「**キャンセル**」をクリックして変更を行わないで、このパネルを終了する。

#### パスワード検証プロパティの設定:

以下の情報を参考にして、パスワード検証プロパティを設定します。

1. Web 管理ツールのナビゲーション領域で「**セキュリティ・プロパティの管理**」カテゴリを展開してから、「**パスワード妥当性検査**」タブを選択する。

注: パスワード・ポリシーがサーバーで使用可能でない場合は、このパネルの機能も有効にはなりません。

2. パスワードを再使用できるようにする前に、使用する必要があるパスワード数を設定する。0 から 30 までの数値を入力します。ゼロを入力した場合には、パスワードは制限なしで再使用することができます。
3. ドロップダウン・メニューから、以下の入力フィールドに定義された構文についてパスワードを検査するかどうかを選択する。以下から選択できます。

##### 構文を検査しない

構文検査は行われません。

## 構文を検査する (暗号化されたものは除く)

暗号化されていないパスワードのすべてについて構文検査が行われます。

### 構文を検査する

すべてのパスワードについて構文検査が行われます。

4. パスワードの最小長を設定するための数値を指定する。この値がゼロに設定された場合は、構文検査は行われません。
  - パスワードに必要となる英字の最小数を設定するための値を指定する。
  - パスワードに必要となる数字および特殊文字の最小数を設定するための数値を指定する。

注: 英字、数字、および特殊文字の合計の最小数は、パスワードの最小長として指定された数値と等しいか、それ以下でなければなりません。
5. パスワードで反復できる最大文字数を指定する。このオプションは、パスワード中に特定の文字を含めることができる回数を制限します。この値がゼロに設定された場合は、反復文字数は検査されません。
6. 直前のパスワードとは異なる最小文字数、および「再使用の前のパスワードの最小数」フィールドに指定された直前のパスワード数を指定する。この値がゼロに設定された場合は、異なる文字数は検査されません。
7. 完了したら、「適用」をクリックし、終了しないで変更を保管するか、あるいは「OK」をクリックして変更を適用して終了するか、あるいは「キャンセル」をクリックして変更を行わないで、このパネルを終了する。

### パスワード・ポリシー属性の表示:

以下の情報を参考にして、パスワード・ポリシー属性を表示します。

検索要求で操作属性が戻されるのは、クライアントによって特に要求された場合のみです。検索操作でこれらの属性を使用するには、重要な属性に対するアクセス権か、あるいは使用される特定の属性に対するアクセス権が必要です。

1. 指定された項目のすべてのパスワード・ポリシー属性を表示するには、次のようになります。

```
> ldapsearch -b "uid=user1,cn=users,o=ibm" -s base "(objectclass=*)"
pwdChangedTime pwdAccountLockedTime pwdExpirationWarned
pwdFailureTime pwdGraceUseTime pwdReset
```

2. パスワードが間もなく満了する項目を照会するには、pwdChangedTime 属性を使用してください。例えば、186 日のパスワード満了ポリシーを用いて、2004 年 8 月 26 日に満了するパスワードを検出するとします。そのために、パスワードが少なくとも 186 日 (2004 年 2 月 22 日) 前に変更された項目を照会するには、次のようにします。

```
> ldapsearch -b "cn=users,o=ibm" -s sub
"(!(pwdChangedTime>20040222000000Z))" 1.1
```

ここでは、フィルターは 2004 年 2 月 22 日の深夜 12 時の pwdChangedTime と同じです。

3. ロックされたアカウントを照会するには、次のように、pwdAccountLockedTime 属性を使用してください。

```
> ldapsearch -b "cn=users,o=ibm" -s sub "(pwdAccountLockedTime=*)" 1.1
```

この「1.1」は、項目 DN のみが戻されることを示します。

4. パスワードがリセットされたために、パスワードの変更が必要となるアカウントを照会するには、次のように、pwdReset 属性を使用してください。

```
> ldapsearch -b "cn=users,o=ibm" -s sub "(pwdReset=TRUE)" 1.1
```

## パスワード・ポリシー属性の指定変更:

以下の情報を参考にして、パスワード・ポリシー属性を指定変更します。

以下を最初に行う必要があります。

ディレクトリー管理者は、パスワード・ポリシー操作属性を変更し、サーバー管理制御 (LDAP コマンド行ユーティリティの `-k` オプション) を使用して、特定項目の正規のパスワード・ポリシー動作を指定変更することができます。

1. `userPassword` 属性を設定する時に `pwdChangedTime` 属性を将来の先の日付に設定することによって、特定アカウントのパスワードが満了しないようにすることができます。以下の例は、時刻を 2200 年 1 月 1 日深夜 12 時に設定しています。

```
> ldapmodify -D cn=root -w ? -k
dn: uid=wasadmin,cn=users,o=ibm
changetype: modify
replace: pwdChangedTime
pwdChangedTime: 22000101000000Z
```

2. 次のように、`pwdAccountLockedTime` と `pwdFailureTime` の属性を除去することによって、過大なログイン失敗数のためにロックされたアカウントをアンロックできます。

```
> ldapmodify -D cn=root -w ? -k
dn: uid=user1,cn=users,o=ibm
changetype: modify
delete: pwdAccountLockedTime
-
delete: pwdFailureTime
```

3. 次のように、`pwdChangedTime` を変更し、`pwdExpirationWarned` と `pwdGraceUseTime` の属性を消去して、満了したアカウントをアンロックすることができます。

```
> ldapmodify -D cn=root -w ? -k
dn: uid=user1,cn=users,o=ibm
changetype: modify
replace: pwdChangedTime
pwdChangedTime: 20040826000000Z
-
delete: pwdExpirationWarned
-
delete: pwdGraceUseTime
```

4. 次のように、`pwdReset` 属性を設定して、「パスワードを変更する必要がある」状況を消去または設定することができます。

```
> ldapmodify -D cn=root -w ? -k
dn: uid=user1,cn=users,o=ibm
changetype: modify
delete: pwdReset
```

```
> ldapmodify -D cn=root -w ? -k
dn: uid=user2,cn=users,o=ibm
changetype: modify
replace: pwdReset
pwdReset: TRUE
```

5. アカウントは、`ibm-pwdAccountLocked` 操作属性を `TRUE` に設定することによって、管理のためにロックすることができます。

書き込みアクセス権が必要となる属性のユーザー設定は `ibm-pwdAccountLocked` 属性で、これは `CRITICAL` アクセス・クラス中に定義されます。



```
> ldapmodify -D uid=useradmin,cn=users,o=ibm -w ?
dn: uid=user1,cn=users,o=ibm
changetype: modify
replace: ibm-pwdAccountLocked
ibm-pwdAccountLocked: TRUE
```

- この属性を FALSE に設定することによって、アカウントをアンロックできます。この方法でアカウントをアンロックした場合は、パスワードの失敗が多いためか、あるいはパスワード満了のためかにかかわらず、ロックされているアカウントの状況には影響しません。

書き込みアクセス権が必要となる属性のユーザー設定は `ibm-pwdAccountLocked` 属性で、これは CRITICAL アクセス・クラス中に定義されます。

```
> ldapmodify -D uid=useradmin,cn=users,o=ibm -w ?
dn: uid=user1,cn=users,o=ibm
changetype: modify
replace: ibm-pwdAccountLocked
ibm-pwdAccountLocked: FALSE
```

## Directory Server での SSL と Transport Layer Security の使用可能化

以下の情報を参考にして、Directory Server で SSL と Transport Layer Security を使用可能にします。

システムにデ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) セキュリティを使用して、Directory Server 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 を使用可能にする前に、『Directory Server での Secure Sockets Layer (SSL) と Transport Layer Security (TLS)』のトピックを読んでおくに役立ちます。

LDAP サーバーで SSL を使用できるようにするには、以下を行います。

### 1. Directory Server と証明書を関連付ける

- System i Navigator から SSL 接続を介して Directory Server を管理する予定の場合は、*System i Access for Windows User's Guide* (System i Navigatorのインストール時にオプションで PC にインストールされます) を参照してください。ディレクトリー・サーバーへの SSL 接続と非 SSL 接続を両方許可する計画の場合は、このステップはスキップしても構いません。
- IBM デジタル証明書マネージャーを開始します。詳細は、「デジタル証明書マネージャー」のトピックの「デジタル証明書マネージャーの開始」を参照してください。
- 証明書を取得または作成する必要がある場合や、それ以外にも証明書システムのセットアップや変更を行う必要がある場合は、それを行ってください。証明書システムのセットアップについては、「デジタル証明書マネージャー」を参照してください。Directory Server に関連するアプリケーションには、サーバー・アプリケーションが 2 つ、クライアント・アプリケーションが 1 つあります。以下のとおりです。

#### Directory Server アプリケーション

Directory Server アプリケーションはサーバーそのものです。

#### Directory Server 公開アプリケーション

Directory Server 公開アプリケーションは、公開の際に使用される証明書を識別します。

#### Directory Server クライアント・アプリケーション

Directory Server クライアント・アプリケーションは、LDAP クライアント ILE API を使用するアプリケーションのデフォルト証明書を識別します。

- 「証明書ストアの選択 (Select a Certificate Store)」ボタンをクリックします。
- 「\*SYSTEM」を選択する。「続行」をクリックする。
- \*SYSTEM 証明書ストアのパスワードを入力します。「続行」をクリックする。

- g. 左側のナビゲーション・メニューが再ロードされたら、「アプリケーションの管理 (Manage Applications)」を展開します。
- h. 「証明書割り当ての更新 (Update certificate assignment)」をクリックします。
- i. 次の画面で、アプリケーションの種類として「サーバー」を選択します。「続行」をクリックする。
- j. 「Directory Server サーバー (Directory Server server)」を選択します。
- k. 「証明書割り当ての更新 (Update Certificate Assignment)」をクリックして、System i Access for Windows クライアントに対する ID の確立に使用する Directory Server に証明書を割り当てます。

注: 選択した証明書の発行元 CA の CA 証明書が System i Access for Windows クライアントのキー・データベースにない場合は、SSL を使用するためにデータベースに CA 証明書を追加する必要があります。この手順は、証明書の割り当てを開始する前に終了させておいてください。

- l. サーバーに割り当てる証明書をリストから選択します。
  - m. 「新規証明書の割り当て (Assign New Certificate)」をクリックします。
  - n. 確認メッセージが出され、DCM が「証明書割り当ての更新 (Update Certificate Assignment)」ページを再ロードします。Directory Server の証明書のセットアップが終了したなら、「完了 (Done)」をクリックします。
2. オプション: Directory Server 公開と証明書を関連付ける。SSL 接続を使用した、システムから Directory Server への公開も可能にする場合は、Directory Server 公開に証明書も関連付けることができます。これにより、独自のアプリケーション ID や代替のキー・データベースを指定していない LDAP ILE API 使用アプリケーションのデフォルト証明書やトラステッド CA が識別されるようになります。
- a. IBM デジタル証明書マネージャーを開始します。
  - b. 「証明書ストアの選択 (Select a Certificate Store)」ボタンをクリックします。
  - c. 「\*SYSTEM」を選択する。「続行」をクリックする。
  - d. \*SYSTEM 証明書ストアのパスワードを入力します。「続行」をクリックする。
  - e. 左側のナビゲーション・メニューが再ロードされたら、「アプリケーションの管理 (Manage Applications)」を展開します。
  - f. 「証明書割り当ての更新 (Update certificate assignment)」をクリックします。
  - g. 次の画面で、アプリケーションの種類として「クライアント」を選択します。「続行」をクリックする。
  - h. 「Directory Server 公開 (Directory Server publishing)」を選択します。
  - i. 「証明書割り当ての更新 (Update Certificate Assignment)」をクリックして、ID を確立する Directory Server 公開に証明書を割り当てます。
  - j. サーバーに割り当てる証明書をリストから選択します。
  - k. 「新規証明書の割り当て (Assign new certificate)」をクリックします。
  - l. 確認メッセージが出され、DCM が「証明書割り当ての更新 (Update Certificate Assignment)」ページを再ロードします。

注: これらのステップは、すでに情報が非 SSL 接続を使用して Directory Server に公開されていることを前提としています。公開に関する完全な情報は、145 ページの『Directory Server への情報の公開』を参照してください。

3. オプション: **Directory Server クライアントと証明書に関連付ける。** Directory Server への SSL 接続を使用するアプリケーションが他にも存在する場合は、Directory Server クライアントにも証明書に関連付ける必要があります。
  - a. IBM デジタル証明書マネージャーを開始します。
  - b. 「**証明書ストアの選択 (Select a Certificate Store)**」 ボタンをクリックします。
  - c. 「**\*SYSTEM**」を選択する。「**続行**」をクリックする。
  - d. \*SYSTEM 証明書ストアのパスワードを入力します。「**続行**」をクリックする。
  - e. 左側のナビゲーション・メニューが再ロードされたら、「**アプリケーションの管理 (Manage Applications)**」を展開します。
  - f. 「**証明書割り当ての更新 (Update certificate assignment)**」をクリックします。
  - g. 次の画面で、アプリケーションの種類として「**クライアント**」を選択します。「**続行**」をクリックする。
  - h. 「**Directory Server クライアント (Directory Server client)**」を選択します。
  - i. 「**証明書割り当ての更新 (Update Certificate Assignment)**」をクリックして、ID を確立する Directory Server クライアントに証明書を割り当てます。
  - j. サーバーに割り当てる証明書をリストから選択します。
  - k. 「**新規証明書の割り当て (Assign New Certificate)**」をクリックします。
  - l. 確認メッセージが出され、DCM が「**証明書割り当ての更新 (Update Certificate Assignment)**」ページを再ロードします。

SSL を使用できるようになると、Directory Server が使用するポートを変更することにより、保護された接続を確立できるようになります。

SSL または TLS を使用するには、System i Navigatorでそれを使用可能にする必要があります。

1. System i Navigator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**」を右クリックし、「**プロパティー**」を選択する。
4. 「**ネットワーク**」タブでは、「**セキュア**」の横のチェック・ボックスにチェックする。

また、セキュアにしたいポート番号を指定することもできます。「**セキュア**」チェック・ボックスをクリックすることは、アプリケーションがセキュア・ポートで SSL または TLS 接続を開始できることを表します。また、これは、非セキュア・ポートで TLS 接続を可能にするためにアプリケーションが StartTLS 操作を実行できることも表します。代わりに、クライアント・コマンド行ユーティリティーから -Y オプションを使用して TLS を起動することができます。コマンド行を使用する場合は、ibm-slapdSecurity 属性は TLS または SSLTLS と等しくなければなりません。

#### 関連概念

59 ページの『Directory Server での Secure Sockets Layer (SSL) と Transport Layer Security (TLS)』 Directory Server との通信の安全度をさらに高めるために、Secure Sockets Layer (SSL) セキュリティーおよび Transport Layer Security (TLS) を Directory Server で使用することができます。

## Directory Server での Kerberos 認証の使用可能化

以下の情報を参考にして、Directory Server で Kerberos 認証を使用可能にします。

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、Directory Server で Kerberos 認証を使用するための設定ができます。Kerberos 認証は、ユーザーと管理者に対して適用されます。ディレクトリー・サーバーで Kerberos を使用可能にする前に、Directory Server で Kerberos を使用する方法の概要を読んでおくのと役に立ちます。

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. System i Navigator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. 「IBM Directory Server」を右マウス・ボタン・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、各ページのオンライン・ヘルプを参照してください。

#### 関連資料

90 ページの『認証』

Directory Server 内のアクセスを制御するには、認証方式を使用します。

## Directory Server での DIGEST-MD5 認証の構成

以下の情報を参考にして、Directory Server で DIGEST-MD5 認証を構成します。

DIGEST-MD5 は SASL 認証メカニズムです。クライアントが DIGEST-MD5 を使用すると、パスワードは平文では送信されず、プロトコルによってリプレイ・アタックが防止されます。DIGEST-MD5 を構成するには、Web 管理ツールが使用されます。

1. 「サーバー管理」で、ナビゲーション領域の「セキュリティー・プロパティーの管理」カテゴリを展開して、「DIGEST-MD5」タブを選択する。

**注:** Web 管理ツールの「サーバー管理」カテゴリのタスクを使用してサーバー構成設定を変更するには、\*ALLOBJ および IOSYSCFG の特殊権限をもつ i5/OS ユーザー・プロファイルとしてサーバーに認証する必要があります。これは、そのプロファイルのパスワードでプロジェクト・ユーザーとして認証することによって実行できます。Web 管理ツールからプロジェクト・ユーザーとしてバインドするには、os400-profile=MYUSERNAME,cn=accounts,os400-sys=MYSYSTEM.COM の形式の username を入力します。この MYUSERNAME と MYSYSTEM.COM のストリングはそれぞれ、ご使用のユーザー・プロファイル名および構成済みシステム射影接尾部と置き換えられます。

2. 「サーバー・レルム」で、事前選択された「デフォルト」設定 (サーバーの完全修飾ホスト名) を使用するか、あるいは「レルム」をクリックして、サーバーを構成したいレルムの名前を入力する。このレルム名をクライアントで使用して、使用するユーザー名およびパスワードが判別されます。複製を使用する時には、同じレルムで構成されたすべてのサーバーを持つことがあります。
3. **Username** 属性では、事前選択された「デフォルト」設定 (uid) を使用するか、あるいは「属性」をクリックして、DIGEST-MD5 SASL バインド時のユーザー項目を一意的に識別するためにサーバーで使用する属性の名前を入力する。
4. ディレクトリー管理者としてログインした場合は、「管理者 username」で、その管理者 username を入力する。管理グループのメンバーはこのフィールドを編集できません。DIGEST-MD5 SASL バインドに指定された username がこのストリングと一致した場合は、そのユーザーは管理者です。

**注:** 管理者 username は大/小文字が区別されます。

- 完了したら、「OK」をクリックする。

#### 関連資料

90 ページの『認証』

Directory Server 内のアクセスを制御するには、認証方式を使用します。

## スキーマ・タスク

以下の情報を参考にして、スキーマを管理します。

スキーマの管理は、Web 管理ツールを使用したり、ldapmodify のような LDAP アプリケーションと LDIF ファイルの組み合わせを使用して行うことができます。新規の objectclass や属性を定義するのが初めての場合は、Web 管理ツールが一番使いやすいかもかもしれません。新規スキーマを別のサーバーにコピーする（恐らく、製品もしくは展開しているツールの一部として）必要がある場合は、ldapmodify ユーティリティーが比較的使いやすいでしょう。詳細は、218 ページの『他のサーバーへのスキーマのコピー』を参照してください。

#### 関連概念

14 ページの『接尾部 (命名コンテキスト)』

接尾部 (命名コンテキストともいいます) は、ローカルに保持されるディレクトリー階層の最上部の項目を識別する DN です。

16 ページの『スキーマ』

スキーマは、ディレクトリーにデータを保管する方法を定める 1 組の規則です。スキーマは、許可されている項目のタイプ、それらの属性構造、および属性の構文を定義します。

## オブジェクト・クラスの表示

以下の情報を参考にして、オブジェクト・クラスを表示します。

Web 管理ツールまたはコマンド行を使用して、スキーマ内のオブジェクト・クラスを表示することができます。

- ナビゲーション領域の「スキーマ管理 (Schema management)」を展開し、「オブジェクト・クラスの管理 (Manage object classes)」をクリックしてください。スキーマ内のオブジェクト・クラスとその特性を表示できる読み取り専用パネルが表示されます。オブジェクト・クラスはアルファベット順に表示されます。「前へ (Previous)」と「次へ (Next)」をクリックすると、それぞれ 1 ページずつ前後のページに移動できます。これらのボタンの隣にあるフィールドは、現在のページを識別します。また、このフィールドのドロップダウン・メニューを使用して、特定のページにスキップすることもできます。確認したいオブジェクト・クラスを見つけやすくするため、ページの先頭にリストされるオブジェクト・クラスには、併せてページ番号が表示されます。たとえば、**person** というオブジェクト・クラスを探している場合は、ドロップダウン・メニューを展開して、「14/16 ページ nsLiServer (Page 14 of 16 nsLiServer)」および「15/16 ページ printerLPR (Page 15 of 16 printerLPR)」という項目までスクロールします。「person」は、アルファベット順で nsLiServer と printerLPR の間になりますから、14 ページを選択して「Go」をクリックします。

オブジェクト・クラスをタイプ別にソートして表示することも可能です。「タイプ (Type)」を選択し、「ソート (Sort)」をクリックします。オブジェクト・クラスは、タイプ (「要約 (Abstract)」、「補助 (Auxiliary)」、または「構造化 (Structural)」) ごとにアルファベット順にソートされます。同様に、「降順 (Descending)」を選択して「ソート (Sort)」をクリックすれば、リストの順番を逆にすることもできます。

- オブジェクト・クラスを特定すると、そのオブジェクト・クラスのタイプ、継承、必須属性、およびオプション属性を表示できます。各特性の完全なリストを表示させるには、継承、必須属性、およびオ

プシヨナル属性のドロップダウン・メニューを展開してください。右手のツールバーからは、実行したいオブジェクト・クラス操作を選択できます。たとえば、次のような操作が行えます。

- 追加 (Add)
- 編集 (Edit)
- コピー (Copy)
- 削除 (Delete)

3. 作業が終了したなら、「閉じる」をクリックして、IBM Directory Server の「ようこそ」パネルに戻ります。

コマンド行を使用して、スキーマに格納されているオブジェクト・クラスを表示するには、次のように入力します。

```
ldapsearch -b cn=schema -s base objectclass=* objectclasses
```

## オブジェクト・クラスの追加

以下の情報を参考にして、オブジェクト・クラスを追加します。

ナビゲーション領域の「スキーマ管理 (Schema management)」を展開し (まだ開いていない場合)、「オブジェクト・クラスの管理 (Manage object classes)」をクリックしてください。新規オブジェクト・クラスを作成するには、次のようにします。

1. 「追加」をクリックします。

注: このパネルへは、ナビゲーション領域の「スキーマ管理 (Schema management)」を展開し、「オブジェクト・クラスの追加 (Add an object class)」をクリックすることによってもアクセスできます。

2. 「一般プロパティ (General properties)」タブでは、以下の作業を行います。

- 「オブジェクト・クラス名 (Object class name)」を入力します。このフィールドは必要フィールドであり、そのオブジェクト・クラスの機能を記述します。たとえば、臨時従業員 (temporary employees) のトラッキングに使用されるオブジェクト・クラスには、**tempEmployee** という名前が付きます。
- オブジェクト・クラスの「説明 (Description)」を入力します。たとえば、「臨時従業員用に使用するオブジェクト・クラス」などとします。
- オブジェクト・クラスの「オブジェクト ID (OID)」を入力します。これは必要フィールドです。28 ページの『オブジェクト ID (OID)』を参照してください。OID がいない場合は、「オブジェクト・クラス名 (Object class name)」の値に **-oid** を付けたものを使用できます。たとえば、オブジェクト・クラス名が **tempEmployee** であるなら、OID は **tempEmployee-oid** になります。このフィールドの値は、変更することができます。
- ドロップダウン・リストから**上級オブジェクト・クラス**を 1 つ選択してください。このオプションは、そのオブジェクト・クラスを継承する他の属性があるかどうかを判別します。一般に、**上級オブジェクト・クラス**は**最上位**を表すことが多いものの、これにはさらに上位の別のオブジェクト・クラスが存在する場合があります。たとえば、**tempEmployee** というオブジェクト・クラスであれば、さらに **ePerson** という**上級オブジェクト・クラス**が存在することも考えられます。
- **オブジェクト・クラス・タイプ**を選択してください。オブジェクト・クラス・タイプに関する補足的な情報は、19 ページの『オブジェクト・クラス』を参照してください。
- オブジェクト・クラスの必要およびオプション属性を指定したり、継承属性を確認する場合は「属性 (Attributes)」タブを、新規オブジェクト・クラスを追加する場合は「OK」を、変更を行わずに「オブジェクト・クラスの管理 (Manage object classes)」に戻る場合は「キャンセル」をクリックします。

3. 「属性 (Attributes)」タブでは、以下の作業を行います。

- 「使用可能な属性 (Available attributes)」のアルファベット順のリストから属性を選択し、その属性をオブジェクト・クラスの必須属性にする場合は「必須属性に追加 (Add to required)」を、オプション属性にする場合は「オプション属性に追加 (Add to optional)」をクリックします。属性は、該当する選択済み属性のリストに表示されます。
- 選択するすべての属性に対してこのプロセスを繰り返してください。
- 属性は、別のリストに移動させたり、選択リストから削除することもできます。属性を選択してから、該当する「移動 (Move to)」ボタンか「削除」ボタンをクリックしてください。
- 必須継承属性やオプション継承属性のリストを表示できます。継承属性のリストは、「一般 (General)」タブで選択されている上級オブジェクト・クラスに基づいて表示されます。これらの継承属性を変更することはできません。ただし、「一般 (General)」タブで上級オブジェクト・クラスが変更されると、表示される継承属性のセットも変わります。

4. 新規オブジェクト・クラスを追加する場合は「OK」を、変更を行わずに「オブジェクト・クラス管理 (Manage object classes)」に戻る場合は「キャンセル」をクリックします。

注: 何も属性を追加しないまま「一般 (General)」タブで「OK」をクリックしてしまった場合は、この新しいオブジェクト・クラスを編集することによって、属性を追加できます。

コマンド行を使用してオブジェクト・クラスを追加する場合は、以下のコマンドを発行します。

```
ldapmodify -D <adminDN> -w <adminPW> -i <filename>
```

ただし、<filename> には以下が入っています。

```
dn: cn=Schema
changetype: modify
add: objectclasses
objectclasses: (<myobjectclass-oid> NAME '<myObjectClass>' DESC '<An object class
I defined for my LDAP application>' SUP '<objectclassinheritance>'
<objectclasstype> MAY (<attribute1> $ <attribute2>))
```

## オブジェクト・クラスの編集

以下の情報を参考にして、オブジェクト・クラスを編集します。

すべてのスキーマ変更が許可されるわけではありません。変更に関する制約事項については、31 ページの『許可されないスキーマの変更』を参照してください。

ナビゲーション領域の「スキーマ管理 (Schema management)」を展開し (まだ開いていない場合)、「オブジェクト・クラス管理 (Manage object classes)」をクリックしてください。オブジェクト・クラスを編集するには、次のようにします。

1. 編集するオブジェクト・クラスの隣にあるラジオ・ボタンをクリックします。
2. 「編集」をクリックします。
3. タブを選択します。

- 以下の作業には、「一般 (General)」タブを使用します。
  - 「説明 (Description)」を変更します。
  - 上級オブジェクト・クラスを変更します。ドロップダウン・リストから上級オブジェクト・クラスを 1 つ選択してください。このオプションは、そのオブジェクト・クラスを継承する他の属性があるかどうかを判別します。一般に、上級オブジェクト・クラスは最上位を表すことが多いもの

の、これにはさらに上位の別のオブジェクト・クラスが存在する場合があります。たとえば、**tempEmployee** というオブジェクト・クラスであれば、さらに **ePerson** という上級オブジェクト・クラスが存在することも考えられます。

- 「**オブジェクト・クラス・タイプ (Object class type)**」を変更します。オブジェクト・クラス・タイプを選択してください。オブジェクト・クラス・タイプに関する補足的な情報は、19 ページの『オブジェクト・クラス』を参照してください。
- オブジェクト・クラスの必要およびオプション属性を変更したり、継承属性を確認する場合は「属性 (Attributes)」タブを、変更を適用する場合は「**OK**」を、変更を行わずに「**オブジェクト・クラスの管理 (Manage object classes)**」に戻る場合は「**キャンセル**」をクリックします。
- 以下の作業には、「**属性 (Attributes)**」タブを使用します。

「**使用可能な属性 (Available attributes)**」のアルファベット順のリストから属性を選択し、その属性をオブジェクト・クラスの必須属性にする場合は「**必須属性に追加 (Add to required)**」を、オプション属性にする場合は「**オプション属性に追加 (Add to optional)**」をクリックします。属性は、該当する選択済み属性のリストに表示されます。

選択するすべての属性に対してこのプロセスを繰り返してください。

属性は、別のリストに移動させたり、選択リストから削除することもできます。属性を選択してから、該当する「**移動 (Move to)**」ボタンか「**削除**」ボタンをクリックしてください。

必須継承属性やオプション継承属性のリストを表示できます。継承属性のリストは、「**一般 (General)**」タブで選択されている**上級オブジェクト・クラス**に基づいて表示されます。これらの継承属性を変更することはできません。ただし、「**一般 (General)**」タブで**上級オブジェクト・クラス**が変更されると、表示される継承属性のセットも変わります。

4. 変更を適用する場合は「**OK**」を、変更を行わずに「**オブジェクト・クラスの管理 (Manage object classes)**」に戻る場合は「**キャンセル**」をクリックします。

コマンド行を使用してスキーマに格納されているオブジェクト・クラスを表示するには、次のコマンドを発行します。

```
ldapsearch -b cn=schema -s base objectclass=* objectclasses
```

コマンド行を使用してオブジェクト・クラスを編集する場合は、以下のコマンドを発行します。

```
ldapmodify -D <adminDN> -w <adminPW> -i <filename>
```

ただし、<filename> には以下が入っています。

```
dn: cn=schema
changetype: modify
replace: objectclasses
objectclasses: (<myobjectClass-oid> NAME '<myObjectClass>' DESC '<An object class
I defined for my LDAP application>' SUP '<newsuperiorclassobject>'
<newobjectclasstype> MAY (attribute1 $ <attribute2>
$ <newattribute3>))
```

## オブジェクト・クラスのコピー

以下の情報を参考にして、オブジェクト・クラスをコピーします。

ナビゲーション領域の「**スキーマ管理 (Schema management)**」を展開し (まだ開いていない場合)、「**オブジェクト・クラスの管理 (Manage object classes)**」をクリックしてください。オブジェクト・クラスをコピーするには、次のようにします。

1. コピーするオブジェクト・クラスの隣にあるラジオ・ボタンをクリックします。



2. 「コピー」をクリックする。

3. タブを選択します。

- 以下の作業には、「一般 (General)」タブを使用します。
  - 「オブジェクト・クラス名 (Object class name)」を変更します。デフォルトの名前は、コピー元のオブジェクト・クラス名に COPY が付加されます。たとえば、tempPerson なら tempPersonCOPY となります。
  - 「説明 (Description)」を変更します。
  - 「オブジェクト ID (OID)」を変更します。デフォルトの OID は、コピー元オブジェクト・クラスの OID に COPY が付加されます。たとえば、tempPerson-oid なら tempPerson-oidCOPY となります。
  - 上級オブジェクト・クラスを変更します。ドロップダウン・リストから上級オブジェクト・クラスを 1 つ選択してください。このオプションは、そのオブジェクト・クラスを継承する他の属性があるかどうかを判別します。一般に、上級オブジェクト・クラスは最上位を表すことが多いものの、これにはさらに上位の別のオブジェクト・クラスが存在する場合があります。たとえば、tempEmployeeCOPY というオブジェクト・クラスであれば、さらに ePerson という上級オブジェクト・クラスが存在することも考えられます。
  - 「オブジェクト・クラス・タイプ (Object class type)」を変更します。オブジェクト・クラス・タイプを選択してください。オブジェクト・クラス・タイプに関する補足的な情報は、19 ページの『オブジェクト・クラス』を参照してください。
  - オブジェクト・クラスの必要およびオプション属性を変更したり、継承属性を確認する場合は「属性 (Attributes)」タブを、変更を適用する場合は「OK」を、変更を行わずに「オブジェクト・クラスの管理 (Manage object classes)」に戻る場合は「キャンセル」をクリックします。
- 以下の作業には、「属性 (Attributes)」タブを使用します。

「使用可能な属性 (Available attributes)」のアルファベット順のリストから属性を選択し、その属性をオブジェクト・クラスの必須属性にする場合は「必須属性に追加 (Add to required)」を、オプション属性にする場合は「オプション属性に追加 (Add to optional)」をクリックします。属性は、該当する選択済み属性のリストに表示されます。

選択するすべての属性に対してこのプロセスを繰り返してください。

属性は、別のリストに移動させたり、選択リストから削除することもできます。属性を選択してから、該当する「移動 (Move to)」ボタンか「削除」ボタンをクリックしてください。

必須継承属性やオプション継承属性のリストを表示できます。継承属性のリストは、「一般 (General)」タブで選択されている上級オブジェクト・クラスに基づいて表示されます。これらの継承属性を変更することはできません。ただし、「一般 (General)」タブで上級オブジェクト・クラスが変更されると、表示される継承属性のセットも変わります。

4. 変更を適用する場合は「OK」を、変更を行わずに「オブジェクト・クラスの管理 (Manage object classes)」に戻る場合は「キャンセル」をクリックします。

コマンド行を使用して、スキーマに格納されているオブジェクト・クラスを表示するには、次のコマンドを発行します。

```
ldapsearch -b cn=schema -s base objectclass=* objectclasses
```

コピーするオブジェクト・クラスを選択してください。エディターを使用して、変更が必要な情報に変更を加え、変更したものを <filename> に保存します。次のコマンドを発行します。

```
ldapmodify -D <adminDN> -w <adminPW> -i <filename>
```

ただし、<filename> には以下が入っています。

```
dn: cn=schema
changetype: modify
add: objectclasses
objectclasses: (<mynewobjectClass-oid> NAME 'mynewObjectClass'
DESC 'A new object class
I copied for my LDAP application'
SUP 'superiorclassobject'<objectclasstype> MAY (attribute1)
$ <attribute2> $ <attribute3>)
```

## オブジェクト・クラスの削除

以下の情報を参考にして、オブジェクト・クラスを削除します。

すべてのスキーマ変更が許可されるわけではありません。変更に関する制約事項については、31 ページの『許可されないスキーマの変更』を参照してください。

ナビゲーション領域の「スキーマ管理 (Schema management)」を展開し (まだ開いていない場合)、「オブジェクト・クラスの管理 (Manage object classes)」をクリックしてください。オブジェクト・クラスを削除するには、次のようにします。

1. 削除するオブジェクト・クラスの隣にあるラジオ・ボタンをクリックします。
2. 「削除」をクリックする。
3. オブジェクト・クラスの削除を確認するプロンプトが表示されます。 オブジェクト・クラスを削除する場合は「OK」を、変更を行わずに「オブジェクト・クラスの管理 (Manage object classes)」に戻る場合は「キャンセル」をクリックします。

スキーマに含まれているオブジェクト・クラスを表示するには、次のコマンドを発行します。

```
ldapsearch -b cn=schema -s base objectclass=* objectclasses
```

削除するオブジェクト・クラスを選択し、以下のコマンドを発行してください。

```
ldapmodify -D <adminDN> -w <adminPW> -i <filename>
```

ただし、<filename> には以下が入っています。

```
dn: cn=schema
changetype: modify
delete: objectclasses
objectclasses: (<myobjectClass-oid>)
```

## 属性の表示

以下の情報を参考にして、属性を表示します。

Web 管理ツール (推奨されている方法) やコマンド行を使用して、スキーマ内の属性を表示することができます。

1. ナビゲーション領域の「スキーマ管理 (Schema management)」を展開し、「属性の管理 (Manage attributes)」をクリックしてください。

スキーマ内の属性とその特性を表示できる読み取り専用パネルが表示されます。属性はアルファベット順に表示されます。「前へ (Previous)」と「次へ (Next)」をクリックすると、それぞれ 1 ページずつ前後のページに移動できます。これらのボタンの隣にあるフィールドは、現在のページを識別します。また、このフィールドのドロップダウン・メニューを使用して、特定のページにスキップすることもできます。確認したいオブジェクト・クラスを見つけやすくするため、ページの先頭にリストされるオブジ

エクト・クラスには、併せてページ番号が表示されます。たとえば、**authenticationUserID** という属性を探している場合は、ドロップダウン・メニューを展開して、「**3/62 ページ applSystemHint (Page 3 of 62 applSystemHint)**」および「**4/62 ページ authorityRevocatonList (Page 4 of 62 authorityRevocatonList)**」という項目までスクロールします。「authenticationUserID」は、アルファベット順で applSystemHint と authorityRevocatonList の間になりますから、3 ページを選択して「**Go**」をクリックします。

属性を構文別にソートして表示することも可能です。「**構文 (Syntax)**」を選択し、「**ソート (Sort)**」をクリックします。属性は、各構文の中でアルファベット順にソートされます。構文のリスト、または構文のタイプについては、26 ページの『属性構文』を参照してください。同様に、「**降順 (Descending)**」を選択して「**ソート (Sort)**」をクリックすれば、リストの順番を逆にすることもできます。

属性を特定すると、その属性の構文、その属性が複数值かどうか、およびその属性が含まれているオブジェクト・クラスを表示できます。その属性が含まれているオブジェクト・クラスのリストを見るには、オブジェクト・クラスのドロップダウン・メニューを展開してください。

2. 作業が終了したなら、「**閉じる**」をクリックして、IBM Directory Server の「**ようこそ**」パネルに戻ります。

スキーマに格納されている属性を表示するには、次のコマンドを発行します。

```
ldapsearch -b cn=schema -s base objectclass=* attributeTypes IBMAttributeTypes
```

## 属性の追加

以下の情報を参考にして、属性を追加します。

新規属性の作成には、次のいずれかの方法を使用してください。推奨されているのは、Web 管理ツールを使用する方法です。

ナビゲーション領域の「**スキーマ管理 (Schema management)**」を展開し (まだ開いていない場合)、「**属性の管理 (Manage attributes)**」をクリックしてください。新規属性を作成するには、次のようにします。

1. 「**追加**」をクリックします。

**注:** このパネルへは、ナビゲーション領域の「**スキーマ管理 (Schema management)**」を展開し、「**属性の追加 (Add an attribute)**」をクリックすることによってもアクセスできます。

2. 「**属性名 (Attribute name)**」を入力します (たとえば、**tempId** など)。これは必要フィールドであり、先頭は必ず英字になっていなければなりません。
3. 属性の「**説明 (Description)**」を入力します。たとえば、「**臨時従業員用に割り当てられた ID 番号**」などとして。
4. 属性の「**オブジェクト ID (OID)**」を入力します。これは必要フィールドです。28 ページの『オブジェクト ID (OID)』を参照してください。OID がない場合は、属性名に **-oid** を付けたものを使用できます。たとえば、属性名が **tempID** であるなら、デフォルトの OID は **tempID-oid** になります。このフィールドの値は、変更することができます。
5. ドロップダウン・リストから**上級属性**を 1 つ選択します。上級属性は、他の属性によってプロパティを継承される属性を判別します。
6. ドロップダウン・リストから「**構文 (Syntax)**」を選択します。構文に関する補足的な情報は、26 ページの『属性構文』を参照してください。
7. この属性の最大長を指定する「**属性の長さ (Attribute length)**」を入力します。長さは、バイト数で表されます。

8. 属性に複数を指定できるようにするには、「複数を許可する (Allow multiple values)」チェック・ボックスを選択します。
9. 等価、順序付け、およびサブストリングの突き合わせ規則の各ドロップダウン・メニューから、突き合わせ規則を選択します。 突き合わせ規則の完全なリストは、24 ページの『突き合わせ規則』を参照してください。
10. 属性に追加の拡張を指定する場合は「IBM 拡張」タブを、新規属性を追加する場合は「OK」を、変更を行わずに「属性の管理 (Manage attributes)」に戻る場合は「キャンセル」をクリックします。
11. 「IBM 拡張」タブでは、以下の作業を行います。
  - 「DB2 テーブル名 (DB2 table name)」を変更します。このフィールドが空白のままになっている場合は、サーバーが DB2 テーブル名を生成します。なお、DB2 テーブル名を入力する場合は、DB2 列名も入力する必要があります。
  - 「DB2 列名 (DB2 column name)」を変更します。このフィールドが空白のままになっている場合は、サーバーが DB2 列名を生成します。なお、DB2 列名を入力する場合は、DB2 テーブル名も入力する必要があります。
  - 「セキュリティ・クラス (Security class)」を設定します。ドロップダウン・リストから「normal (通常)」、「sensitive (重要)」、「critical (重大)」のいずれかを選択します。
  - 「索引規則 (Indexing rules)」を設定します。1 つ以上の索引規則を選択してください。索引規則に関する補足的な情報は、25 ページの『索引付け規則』を参照してください。

注: 検索フィルターで使用する属性には、少なくとも等価索引を指定することをお勧めします。

12. 新規属性を追加する場合は「OK」を、変更を行わずに「属性の管理 (Manage attributes)」に戻る場合は「キャンセル」をクリックします。

注: 何も拡張を追加しないまま「一般」タブで「OK」をクリックしてしまった場合は、この新しい属性を編集することによって、拡張を追加できます。

コマンド行を使用して属性を追加する場合は、以下のコマンドを発行します。次の例では、「ディレクトリー・ストリング (Directory String)」構文 (26 ページの『属性構文』参照) と、「大/小文字を区別しない等価 (Case Ignore Equality)」突き合わせ (24 ページの『突き合わせ規則』参照) が指定された、「myAttribute」という属性の属性タイプ定義を追加します。定義の中の IBM 固有の部分には、属性データが "myAttrTable" というテーブルの "myAttrColumn" という列に保管されることが示されます。これらの名前が指定されなかった場合は、列名とテーブル名のいずれも、デフォルトで "myAttribute" になります。属性は "normal" アクセス・クラスに割り当てられており、値の最大長は 200 バイトに設定されています。

```
ldapmodify -D <adminDn> -w <adminpw> -i myschema.ldif
```

ここで、**myschema.ldif** ファイルには以下が含まれています。

```
dn: cn=schema
changetype: modify
add: attributetypes
attributetypes: (myAttribute-oid NAME ('myAttribute')
DESC 'An attribute I defined for my LDAP application'
EQUALITY 2.5.13.2 SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
USAGE userApplications)
-
add: ibmattributetypes
ibmattributetypes: (myAttribute-oid DBNAME ('myAttrTable' 'myAttrColumn')
ACCESS-CLASS normal LENGTH 200)
```

## 属性の編集

以下の情報を参考にして、属性を編集します。

すべてのスキーマ変更が許可されるわけではありません。変更に関する制約事項については、31 ページの『許可されないスキーマの変更』を参照してください。

この属性を使用する項目が追加されていない状態では、定義のすべての部分に変更が可能です。属性の編集には、次のいずれかの方法を使用してください。推奨されているのは、Web 管理ツールを使用する方法です。

ナビゲーション領域の「スキーマ管理 (Schema management)」を展開し (まだ開いていない場合)、「属性の管理 (Manage attributes)」をクリックしてください。属性を編集するには、次のようになります。

1. 編集する属性の隣にあるラジオ・ボタンをクリックします。
2. 「編集」をクリックする。
3. タブを選択します。
  - 以下の作業には、「一般 (General)」タブを使用します。
    - いずれかのタブを選択します。
      - 次の作業には、「一般 (General)」タブを使用します。
        - 「説明 (Description)」の変更
        - 「構文 (Syntax)」の変更
        - 「属性の長さ (Attribute length)」の変更
        - 複数値の設定の変更
        - 突き合わせ規則の選択
        - 上級属性の変更
      - 属性の拡張を編集する場合は「IBM 拡張」タブを、変更を適用する場合は「OK」を、変更を行わずに「属性の管理 (Manage attributes)」に戻る場合は「キャンセル」をクリックします。
      - 次の作業には、「IBM 拡張」タブを使用します (IBM Directory Server を使用している場合)。
        - 「Security class (セキュリティー・クラス)」の変更
        - 「索引付け規則」の変更
      - 変更を適用する場合は「OK」を、変更を行わずに「属性の管理 (Manage attributes)」に戻る場合は「キャンセル」をクリックします。
4. 変更を適用する場合は「OK」を、変更を行わずに「属性の管理 (Manage attributes)」に戻る場合は「キャンセル」をクリックします。

コマンド行を使用して属性を編集する場合は、以下のコマンドを発行します。次の例では、属性に索引付けを追加し、検索がよりスムーズに行えるようにします。定義の変更には `ldapmodify` コマンドと LDIF ファイルを使用します。

```
ldapmodify -D <adminDn> -w <adminpw> -i myschemachange.ldif
```

ここで、**myschemachange.ldif** ファイルには以下が含まれています。

```
dn: cn=schema
changetype: modify
replace: attributetypes
attributetypes: (myAttribute-oid NAME ('myAttribute') DESC 'An attribute
 I defined for my LDAP application' EQUALITY 2.5.13.2
 SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 USAGE userApplications)
-
replace: ibmattributetypes
ibmattributetypes: (myAttribute-oid DBNAME ('myAttrTable' 'myAttrColumn')
 ACCESS-CLASS normal LENGTH 200 EQUALITY SUBSTR)
```

注: 変更されるのは **ibmattributetypes** セクションだけであったとしても、置換操作には必ず両方の部分 (**attributetypes** と **ibmattributetypes**) を含めてください。変更される点は、等価突き合わせとサブストリング突き合わせの索引を要求するために、定義の最後に "EQUALITY SUBSTR" が追加される点だけです。

## 属性のコピー

以下の情報を参考にして、属性をコピーします。

属性のコピーには、次のいずれかの方法を使用してください。推奨されているのは、Web 管理ツールを使用する方法です。

ナビゲーション領域の「スキーマ管理 (Schema management)」を展開し (まだ開いていない場合)、「属性の管理 (Manage attributes)」をクリックしてください。属性をコピーするには、次のようにします。

1. コピーする属性の隣にあるラジオ・ボタンをクリックします。
2. 「コピー」をクリックする。
3. 「属性名 (Attribute name)」を変更します。デフォルトの名前は、コピー元の属性名に COPY が付加されます。たとえば、**tempID** なら **tempIDCOPY** となります。
4. 属性の「説明 (Description)」を変更します。たとえば、「臨時従業員用に割り当てられた ID 番号」などとしします。
5. 「オブジェクト ID (OID)」を変更します。デフォルトの OID は、コピー元属性の OID に COPYOID が付加されます。たとえば、**tempID-oid** なら **tempID-oidCOPYOID** となります。
6. ドロップダウン・リストから上級属性を 1 つ選択します。上級属性は、他の属性によってプロパティを継承される属性を判別します。
7. ドロップダウン・リストから「構文 (Syntax)」を選択します。構文に関する補足的な情報は、26 ページの『属性構文』を参照してください。
8. この属性の最大長を指定する「属性の長さ (Attribute length)」を入力します。長さは、バイト数で表されます。
9. 属性に複数を指定できるようにするには、「複数を許可する (Allow multiple values)」チェック・ボックスを選択します。
10. 等価、順序付け、およびサブストリングの突き合わせ規則の各ドロップダウン・メニューから、突き合わせ規則を選択します。突き合わせ規則の完全なリストは、24 ページの『突き合わせ規則』を参照してください。
11. 属性の追加拡張を変更する場合は「IBM 拡張」タブを、変更を適用する場合は「OK」を、変更を行わずに「属性の管理 (Manage attributes)」に戻る場合は「キャンセル」をクリックします。
12. 「IBM 拡張」タブでは、以下の作業を行います。
  - 「DB2 テーブル名 (DB2 table name)」を変更します。このフィールドがブランクのままになっている場合は、サーバーが DB2 テーブル名を生成します。なお、DB2 テーブル名を入力する場合は、DB2 列名も入力する必要があります。
  - 「DB2 列名 (DB2 column name)」を変更します。このフィールドがブランクのままになっている場合は、サーバーが DB2 列名を生成します。なお、DB2 列名を入力する場合は、DB2 テーブル名も入力する必要があります。
  - 「セキュリティ・クラス (Security class)」を変更します。ドロップダウン・リストから「normal (通常)」、「sensitive (重要)」、「critical (重大)」のいずれかを選択します。
  - 「索引規則 (Indexing rules)」を変更します。1 つ以上の索引規則を選択してください。索引規則に関する補足的な情報は、25 ページの『索引付け規則』を参照してください。

注: 検索フィルターで使用する属性には、少なくとも等価索引を指定することをお勧めします。

13. 変更を適用する場合は「OK」を、変更を行わずに「属性の管理 (Manage attributes)」に戻る場合は「キャンセル」をクリックします。

注: 何も拡張を追加しないまま「一般 (General)」タブで「OK」をクリックしてしまった場合は、この新しい属性を編集することによって、拡張を追加できます。

スキーマに格納されている属性を表示するには、次のコマンドを発行します。

```
ldapsearch -b cn=schema -s base objectclass=* attributeTypes IBMAttributeTypes
```

コピーする属性を選択してください。エディターを使用して、変更が必要な情報に変更を加え、変更したものを <filename> に保存します。次いで、次のコマンドを発行します。

```
ldapmodify -D <adminDN> -w <adminPW> -i <filename>
```

ただし、<filename> には以下が入っています。

```
dn: cn=schema
changetype: modify
add: attributetypes
attributetypes: (<mynewAttribute-oid> NAME '<mynewAttribute>' DESC '<A new
 attribute I copied for my LDAP application>' EQUALITY 2.5.13.2
 SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 USAGE userApplications)
-
add: ibmattributetypes
ibmattributetypes: (myAttribute-oid DBNAME ('myAttrTable' 'myAttrColumn')
 ACCESS-CLASS normal LENGTH 200)
```

## 属性の削除

以下の情報を参考にして、ディレクトリー・ツリーの属性を削除します。

すべてのスキーマ変更が許可されるわけではありません。変更に関する制約事項については、31 ページの『許可されないスキーマの変更』を参照してください。

属性の削除には、次のいずれかの方法を使用してください。推奨されているのは、Web 管理ツールを使用する方法です。

ナビゲーション領域の「スキーマ管理 (Schema management)」を展開し (まだ開いていない場合)、「属性の管理 (Manage attributes)」をクリックしてください。属性を削除するには、次のようにします。

1. 削除する属性の隣にあるラジオ・ボタンをクリックします。
2. 「削除」をクリックする。
3. 属性の削除を確認するプロンプトが表示されます。属性を削除する場合は「OK」を、変更を行わずに「属性の管理 (Manage attributes)」に戻る場合は「キャンセル」をクリックします。

コマンド行を使用して属性を削除する場合は、以下のコマンドを発行します。

```
ldapmodify -D <adminDN> -w <adminPW> -i myschemadelete.ldif
```

ここで、myschemadelete.ldif ファイルには以下が含まれています。

```
dn: cn=schema
changetype: modify
delete: attributetypes
attributetypes: (<myAttribute-oid>)
```

## 他のサーバーへのスキーマのコピー

以下の情報を参考にして、他のサーバーにスキーマをコピーします。

他のサーバーへスキーマをコピーするには、次のようにします。

1. `ldapsearch` ユーティリティを使用して、スキーマをファイルにコピーします。

```
ldapsearch -b cn=schema -L "(objectclass=*)" > schema.ldif
```

2. スキーマ・ファイルには、すべての `objectclass` と属性が組み込まれます。そこで、LDIF ファイルを編集して必要なスキーマ・エレメントだけを含めるか、`grep` などのツールを使用して `ldapsearch` の出力をフィルターにかけます。なお、`objectclass` の前に、`objectclass` が参照する属性を必ず含めてください。たとえば、次のようなファイルができるかもしれません（ここで、継続する各行の末尾にシングル・スペースが入っており、後に続く行の先頭にも 1 つ以上のスペースが入っていることに注目してください）。

```
attributetypes: (myattr1-oid NAME 'myattr1' DESC 'Some piece of
information.' SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 EQUALITY 2.5.13.2
USAGE userApplications)
IBMAttributetypes: (myattr1-oid DBNAME('myattr1' 'myattr1')
ACCESS-CLASS normal LENGTH 500)
attributetypes: (myattr2-oid NAME 'myattr2' DESC 'Some piece of
information.' SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 EQUALITY 2.5.13.2
USAGE userApplications)
IBMAttributetypes: (myattr2-oid DBNAME('myattr2' 'myattr2')
ACCESS-CLASS normal LENGTH 500)
objectclasses: (myobject-oid NAME 'myobject' DESC 'Represents
something.' SUP 'top' STRUCTURAL MUST (cn) MAY (myattr1 $ myattr2))
```

3. `objectclass` や `attributetype` 行の値を項目 `cn=schema` に追加する LDIF ディレクティブを構成するため、各 `objectclass` や `attributetype` 行の前に行を挿入します。各オブジェクト・クラスや属性の追加は、それぞれ別々の変更として追加される必要があります。

```
dn: cn=schema
changetype: modify
add: attributetypes ibmattributetypes
attributetypes: (myattr1-oid NAME 'myattr1' DESC 'Some piece of
information.' SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 EQUALITY 2.5.13.2
USAGE userApplications)
IBMAttributetypes: (myattr1-oid DBNAME('myattr1' 'myattr1')
ACCESS-CLASS normal LENGTH 500)
```

```
dn: cn=schema
changetype: modify
add: attributetypes ibmattributetypes
attributetypes: (myattr2-oid NAME 'myattr2' DESC 'Some piece of
information.' SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 EQUALITY 2.5.13.2
USAGE userApplications)
IBMAttributetypes: (myattr2-oid DBNAME('myattr2' 'myattr2')
ACCESS-CLASS normal LENGTH 500)
```

```
dn: cn=schema
changetype: modify
add: objectclasses
objectclasses: (myobject-oid NAME 'myobject' DESC 'Represents
something.' SUP 'top' STRUCTURAL MUST (cn) MAY (myattr1 $ myattr2))
```

4. `ldapmodify` ユーティリティを使用して、別のサーバーにスキーマをロードします。

```
ldapmodify -D cn=administrator -w <password> -f schema.ldif
```

## ディレクトリー項目タスク

以下の情報を参考にして、ディレクトリー項目を管理します。



ディレクトリー項目の管理を行うには、Web 管理ツールのナビゲーション領域で「ディレクトリー管理」の 카테고리を展開します。

### 関連概念

14 ページの『接尾部 (命名コンテキスト)』

接尾部 (命名コンテキストともいいます) は、ローカルに保持されるディレクトリー階層の最上部の項目を識別する DN です。

16 ページの『スキーマ』

スキーマは、ディレクトリーにデータを保管する方法を定める 1 組の規則です。スキーマは、許可されている項目のタイプ、それらの属性構造、および属性の構文を定義します。

85 ページの『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。

## ディレクトリー・ツリーのブラウズ

以下の情報を参考にして、ディレクトリー・ツリーをブラウズします。

以下を最初に行う必要があります。

それに合わせて、ステージを設定しておく必要があります。

1. ナビゲーション領域で「ディレクトリー管理」の 카테고리を展開してください (まだ開いていない場合)。
2. 「項目の管理」をクリックする。

各種のサブツリーを展開して、作業を行う項目を選択できます。実行したい操作は、右側のツールバーから選択できます。

## 項目の追加

以下の情報を参考にして、ディレクトリー・ツリーに項目を追加します。

1. ナビゲーション領域で「ディレクトリー管理」の 카테고리を展開してください (まだ開いていない場合)。
2. 「項目の追加 (Add an entry)」をクリックします。
3. ドロップダウン・リストから**構造化オブジェクト・クラス**を 1 つ選択します。
4. 「次へ」をクリックします。
5. 「使用可能なオブジェクト・クラス (Available object classes)」ボックスから、使用したい任意の**補助オブジェクト・クラス**を選択し、「追加 (Add)」をクリックしてください。追加する補助オブジェクト・クラスごとにこのプロセスを繰り返してください。また、「選択済みオブジェクト・クラス (Selected object classes)」ボックスから補助オブジェクト・クラスを選択して「除去」をクリックすると、選択済みのボックスから補助オブジェクト・クラスを削除できます。
6. 「次へ」をクリックします。
7. 「**相対識別名 (Relative DN)**」フィールドに、追加する項目の相対識別名 (RDN) を追加します (たとえば、cn=John Doe など)。
8. 「**親の識別名 (Parent DN)**」フィールドに、選択したツリー項目の識別名 (たとえば、ou=Austin、o=IBM など) を入力します。また、「参照」をクリックして、リストから親 DN を選択することもできます。また、選択した項目を展開して、サブツリーにあるさらに下位の項目を表示する

ことも可能です。選択した項目を指定して「**選択 (Select)**」をクリックし、希望する親の識別名を指定してください。「**親 DN**」のデフォルト値は、ツリーで選択された項目になります。

**注:** このタスクを「**項目の管理**」パネルから開始した場合、このフィールドには値が事前に入力されています。

9. 「**必須属性 (Required attributes)**」タブで、必須属性の値を入力します。特定の属性に複数值を追加したい場合は、「**複数值**」をクリックして、一度に 1 つずつ値を追加します。
10. 「**オプション属性 (Optional attributes)**」をクリックします。
11. 「**オプション属性 (Optional attributes)**」タブで、必要に応じてオプション属性の値を入力します。バイナリー値の追加に関する情報は、226 ページの『**バイナリー属性の変更**』を参照してください。特定の属性に複数值を追加したい場合は、「**複数值**」をクリックして、一度に 1 つずつ値を追加します。
12. 「**OK**」をクリックして項目を作成します。
13. 「**アクセス制御リスト (ACL)**」ボタンをクリックして、この項目のアクセス制御リストに変更を加えます。アクセス制御リストに関する詳細は、72 ページの『**アクセス制御リスト**』を参照してください。
14. 少なくとも必要フィールドへの入力を完了させた上で、新規項目を追加する場合は「**追加 (Add)**」を、ディレクトリーへの変更を行わずに「**ブラウズ・ツリー (Browse tree)**」に戻る場合は「**キャンセル**」をクリックします。

## 言語タグの付いた属性を備えた項目の追加

以下の情報を参考にして、言語タグの付いた属性を備えた項目を作成します。

言語タグのある属性を含む項目を作成するには、次のようにしてください。

1. 言語タグを使用可能にする。141 ページの『**言語タグの使用可能化**』を参照してください。
2. ナビゲーション領域の「**ディレクトリー管理**」カテゴリーを展開し、「**項目の管理**」をクリックする。
3. 「**属性の編集**」ボタンをクリックする。
4. 言語タグを作成したい属性を選択する。
5. 「**言語タグ値**」ボタンをクリックして、「**言語タグ値**」パネルにアクセスする。
6. 「**言語タグ**」フィールドで、作成したいタグの名前を入力する。タグは接尾部 lang- で開始します。
7. 「**値**」フィールドにタグの値を入力する。
8. 「**追加**」をクリックする。言語タグとその値がメニュー・リストに表示されます。
9. ステップ 4、5、および 6 を繰り返して、追加の言語タグを作成するか、あるいは属性の既存の言語タグを変更する。必要な言語タグを作成したら、「**OK**」をクリックします。
10. 「**言語タグ付き表示**」メニューを展開して、言語タグを選択する。「**表示の変更**」をクリックすると、その言語タグに入力した属性値が表示されます。この表示で追加または編集した値は、選択した言語タグのみに適用されます。
11. 終了したら、「**OK**」をクリックする。

### 関連資料

55 ページの『**言語タグ**』

言語タグの用語は次のメカニズムを定義します。これによって、Directory Server 中で自然言語コードとディレクトリーに保持された値を関連付けて、特定の自然言語の要件を満たす値をクライアントがディレクトリーで照会できるようになります。

## 項目の削除

以下の情報を参考にして、ディレクトリー・ツリーから項目を削除します。

1. ナビゲーション領域で「**ディレクトリー管理**」のカテゴリーを展開し (まだ開いていない場合)、「**項目の管理**」をクリックしてください。各種のサブツリーを展開して、作業を行うサブツリー、接尾部、または項目を選択できます。右側のツールバーから「**削除**」をクリックします。
2. 削除を確認するプロンプトが出されます。「**OK**」をクリックします。この項目がディレクトリーから削除され、項目のリストが再び表示されます。

## 項目の編集

以下の情報を参考にして、ディレクトリー・ツリーの項目を編集します。

1. ナビゲーション領域で「**ディレクトリー管理**」のカテゴリーを展開し (まだ開いていない場合)、「**項目の管理**」をクリックしてください。各種のサブツリーを展開して、作業を行う項目を選択できます。右側のツールバーから「**属性の編集 (Edit attributes)**」をクリックします。
2. 「**必須属性 (Required attributes)**」タブで、必須属性の値を入力します。バイナリー値の追加に関する情報は、226 ページの『**バイナリー属性の変更**』を参照してください。特定の属性に複数を追加したい場合は、「**複数值**」をクリックして、一度に 1 つずつ値を追加します。
3. 「**オプション属性 (Optional attributes)**」をクリックします。
4. 「**オプション属性 (Optional attributes)**」タブで、必要に応じてオプション属性の値を入力します。特定の属性に複数を追加したい場合は、「**複数值**」をクリックして、一度に 1 つずつ値を追加します。
5. 「**Memberships (メンバーシップ)**」をクリックします。
6. 何らかのグループを作成してある場合は、「**メンバーシップ (Memberships)**」タブで以下の作業を行います。
  - 項目を静的グループ・メンバーシップのメンバーにするには、「**使用可能なグループ (Available groups)**」からグループを選択して、「**追加 (Add)**」をクリックします。
  - グループから項目を除去するには、「**静的グループ・メンバーシップ (Static group memberships)**」からグループを選択し、「**除去**」をクリックします。
7. 項目がグループ項目の場合は、「**メンバー (Members)**」タブが使用できます。「**メンバー (Members)**」タブには、選択されたグループのメンバーが表示されます。グループに対するメンバーの追加と除去を行うことができます。
  - グループにメンバーを追加するには、次のようにします。
    - a. 「**メンバー (Members)**」タブの「**複数值 (Multiple values)**」をクリックするか、「**メンバー (Members)**」タブで「**メンバー (Members)**」をクリックします。
    - b. 「**メンバー (Member)**」フィールドに、追加する項目の識別名を入力します。
    - c. 「**追加**」をクリックします。
    - d. 「**OK**」をクリックします。
  - グループからメンバーを除去するには、次のようにします。
    - a. 「**メンバー (Members)**」タブの「**複数值 (Multiple values)**」をクリックするか、「**メンバー (Members)**」タブをクリックして「**メンバー (Members)**」をクリックします。
    - b. 除去する項目を選択します。
    - c. 「**除去**」をクリックします。
    - d. 「**OK**」をクリックします。
  - メンバーのリストを更新するには、「**更新**」をクリックします。

8. 項目を変更するには、「OK」をクリックします。

## 項目のコピー

以下の情報を参考にして、ディレクトリー・ツリーの項目をコピーします。

この機能は、類似した項目を作成する場合に便利です。コピーは、オリジナルの属性をすべて継承します。新しい項目に名前を付けるには、いくつかの変更を加える必要があります。

1. ナビゲーション領域で「**ディレクトリー管理**」のカテゴリーを展開し (まだ開いていない場合)、「**項目の管理**」をクリックしてください。各種のサブツリーを展開して、作業を行う項目 (John Doe など) を選択できます。右側のツールバーから「**コピー (Copy)**」をクリックします。
2. 「識別名 (DN)」フィールドで相対識別名 (RDN) の項目を変更します。たとえば、cn=John Doe を cn=Jim Smith に変更します。
3. 「必須属性 (Required attributes)」タブで、cn 項目を新しい相対識別名 (RDN) に変更します。この例の場合は Jim Smith になります。
4. 必要に応じ、他の必須属性に変更を加えます。この例では、sn 属性を Doe から Smith に変更します。
5. 必要な変更処理が終了したら、「OK」をクリックして新規項目を作成します。新規項目 Jim Smith が、項目リストの一番下に追加されます。

注: この手順でコピーされるのは、項目の属性だけです。オリジナルの項目のグループ・メンバーシップは、新しい項目にコピーされません。メンバーシップを追加するには、「属性の編集 (Edit attributes)」機能を使用してください。

## アクセス制御リストの編集

以下の情報を参考にして、アクセス制御リスト (ACL) を管理します。

Web 管理ツール・ユーティリティを使用して ACL のプロパティーを表示し、ACL に対する作業を行う場合は、239 ページの『アクセス制御リスト (ACL) のタスク』を参照してください。

### 関連概念

72 ページの『アクセス制御リスト』

アクセス制御リスト (ACL) を使用すると、LDAP ディレクトリーに保管された情報を保護することができます。管理者は ACL を使用して、ディレクトリーのさまざまな部分へのアクセスや、特定のディレクトリー項目へのアクセスを制限します。

## 補助オブジェクト・クラスの追加

以下の情報を参考にして、補助オブジェクト・クラスを追加します。

ディレクトリー・ツリー内の既存の項目に補助オブジェクト・クラスを追加するには、ツールバーの「**補助クラスの追加 (Add auxiliary class)**」ボタンを使用します。補助オブジェクト・クラスは、追加先の項目に追加の属性を与えます。

ナビゲーション領域で「**ディレクトリー管理**」のカテゴリーを展開し (まだ開いていない場合)、「**項目の管理**」をクリックしてください。各種のサブツリーを展開して、作業を行う項目 (John Doe など) を選択できます。右側のツールバーから、「**補助クラスの追加 (Add auxiliary class)**」をクリックします。

1. 「使用可能なオブジェクト・クラス (Available object classes)」ボックスから、使用したい任意の**補助オブジェクト・クラス**を選択し、「**追加 (Add)**」をクリックしてください。追加する補助オブジェクト・クラスごとにこのプロセスを繰り返してください。また、「**選択済みオブジェクト・クラス (Selected object classes)**」ボックスから補助オブジェクト・クラスを選択して「**除去**」をクリックすると、選択済みのボックスから補助オブジェクト・クラスを削除できます。

2. 「**必須属性 (Required attributes)**」タブで、必須属性の値を入力します。特定の属性に複数を追加したい場合は、「**複数值**」をクリックして、一度に 1 つずつ値を追加します。
3. 「**オプション属性 (Optional attributes)**」をクリックします。
4. 「**オプション属性 (Optional attributes)**」タブで、必要に応じてオプション属性の値を入力します。特定の属性に複数を追加したい場合は、「**複数值**」をクリックして、一度に 1 つずつ値を追加します。
5. 「**Memberships (メンバーシップ)**」をクリックします。
6. 何らかのグループを作成してある場合は、「**メンバーシップ (Memberships)**」タブで以下の作業を行います。
  - 項目を**静的グループ・メンバーシップ**のメンバーにするには、「**使用可能なグループ (Available groups)**」からグループを選択して、「**追加 (Add)**」をクリックします。
  - グループから項目を除去するには、「**静的グループ・メンバーシップ (Static group memberships)**」からグループを選択し、「**除去**」をクリックします。
7. 項目を変更するには、「**OK**」をクリックします。

## 補助クラスの削除

以下の情報を参考にして、補助クラスを削除します。

補助クラスの削除は、補助クラスの追加プロシージャの中でも行うことができますが、単一の補助クラスを項目から削除しようとしているのであれば、補助クラスの削除機能を使用した方が簡単です。ただし、項目から複数の補助クラスを削除するときには、補助クラスの追加プロシージャを使用した方が便利な場合があります。

1. ナビゲーション領域で「**ディレクトリー管理**」のカテゴリーを展開し (まだ開いていない場合)、「**項目の管理**」をクリックしてください。各種のサブツリーを展開して、作業を行う項目 (John Doe など) を選択できます。右側のツールバーから「**補助クラスの削除 (Delete auxiliary class)**」をクリックします。
2. 補助クラスのリストから削除する補助クラスを選択し、「**OK**」をクリックします。
3. 削除を確認するプロンプトが表示されるので、「**OK**」をクリックしてください。
4. 補助クラスは項目から削除され、表示は項目のリストに戻ります。

これらのステップを、削除する補助クラスごとに繰り返してください。

## グループ・メンバーシップの変更

以下の情報を参考にして、グループ・メンバーシップを変更します。

ナビゲーション領域で「**ディレクトリー管理**」のカテゴリーを展開してください (まだ開いていない場合)。

1. 「**項目の管理**」をクリックする。
2. ディレクトリー・ツリーからユーザーを選択し、ツールバーの「**属性の編集 (Edit attributes)**」アイコンをクリックします。
3. 「**メンバーシップ (Memberships)**」タブをクリックします。
4. ユーザーのメンバーシップを変更します。「**メンバーシップの変更 (Change memberships)**」パネルに、ユーザーを追加できる「**使用可能なグループ (Available groups)**」と、「**静的グループ・メンバーシップ (Static Group Memberships)**」の項目が表示されます。

- 項目を選択したグループのメンバーにするには、「使用可能なグループ (Available groups)」からグループを選択して、「追加 (Add)」をクリックします。
  - グループから項目を除去するには、「静的グループ・メンバーシップ (Static Group Memberships)」からグループを選択し、「除去」をクリックします。
5. 変更を保管する場合は「OK」を、変更を保管せずに直前のパネルに戻る場合は「キャンセル」をクリックします。

## ディレクトリー項目の検索

以下の情報を参考にして、ディレクトリー項目を検索します。

ディレクトリー・ツリーの検索には、3 つのオプションがあります。

- 事前定義された検索基準のセットを使用する単純検索
- ユーザー定義の検索基準のセットを使用する拡張検索
- 手動検索

検索オプションは、ナビゲーション領域の「ディレクトリー管理」のカテゴリーを展開し、「項目の検索 (Find entries)」をクリックすると使用できます。「検索フィルター (Search filters)」または「オプション (Options)」タブを選択してください。

注: なお、パスワードなどのバイナリー項目は検索できません。

単純検索では、以下のデフォルトの検索基準を使用します。

- 基本識別名は「すべての接尾部 (All suffixes)」
- 検索範囲は「サブツリー (Subtree)」
- 検索サイズは「無制限 (Unlimited)」
- 時間制限は「無制限 (Unlimited)」
- 別名の参照解除は「実行しない (never)」
- 追跡参照は選択解除 (オフ)

拡張検索では、検索の制約事項を指定したり、検索フィルターを使用可能にすることができます。デフォルトの検索基準を使用する場合は、単純検索を使用してください。

1. 単純検索を実行するには、次のようにします。
  - a. 「検索フィルター (Search filter)」タブで、「単純検索 (Simple search)」をクリックします。
  - b. ドロップダウン・リストからオブジェクト・クラスを選択します。
  - c. 選択した項目タイプの特定の属性を選択します。属性を指定した検索を選択する場合は、ドロップダウン・リストから属性を選択し、「検索する属性値 (Is equal to)」ボックスに属性値を入力します。属性が指定されない場合は、選択された項目タイプのディレクトリー項目がすべて戻されます。
2. 拡張検索を実行するには、次のようにします。
  - a. 「検索フィルター (Search filter)」タブで、「拡張検索 (Advanced search)」をクリックします。
  - b. ドロップダウン・リストから属性を選択します。
  - c. 以下の中から比較演算子を選択します。
  - d. 比較に使用する値を入力します。
  - e. 複雑な照会には検索演算子のボタンを使用します。
    - **AND** は、すでに検索フィルターを 1 つ以上追加しており、さらに追加の検索基準を指定する場合にクリックします。 **AND** コマンドは、両方の検索基準のセットと一致する項目を戻します。

- **OR** は、すでに検索フィルターを 1 つ以上追加しており、さらに追加の検索基準を指定する場合にクリックします。 **OR** コマンドは、いずれかの検索基準のセットと一致する項目を戻します。
- 拡張検索に検索フィルター基準を追加する場合は「**追加 (Add)**」をクリックします。
- 拡張検索から検索フィルター基準を除去する場合は「**削除**」をクリックします。
- すべての検索フィルターをクリアする場合は「**リセット (Reset)**」をクリックします。

### 3. 手動検索を実行するには、検索フィルターを作成します。

たとえば、姓を検索するときは、フィールドに `sn=*` と入力します。なお、複数の属性を検索する場合は、検索フィルター構文を使用する必要があります。たとえば、特定の部署に属するメンバーの姓を検索するときは、次のように入力します。

```
(&(sn=*)(dept=<departmentname>))
```

「**オプション (Options)**」タブでは、以下のことを行えます。

- 「**基本識別名の検索 (Search base DN)**」 - ドロップダウン・リストから接尾部を選択し、その接尾部でのみ検索を行います。

注: このタスクを「**項目の管理**」パネルから開始した場合、このフィールドには値が入力されています。

「**親の識別名 (Parent DN)**」は、「**追加 (Add)**」をクリックして項目の追加プロセスを開始する前に選択されています。

ツリー全体を検索する場合は、「**すべての接尾部 (All suffixes)**」を選択することもできます。

注: 「**すべての接尾部**」を選択したサブツリー検索では、スキーマ情報、変更ログ情報は戻されず、またシステム・プロジェクト・バックエンドからも何も戻されません。

#### • 検索範囲

- 選択されたオブジェクトの中でのみ検索を実行する場合は、「**オブジェクト (Object)**」を選択します。
- 選択されたオブジェクトの直接の子でのみ検索を実行する場合は、「**1 レベル (Single level)**」を選択します。
- 選択された項目の子孫すべてに対して検索を実行する場合は、「**サブツリー (Subtree)**」を選択します。
- 「**検索サイズ制限 (Search size limit)**」 - 検索する項目の最大数を入力するか、「**無制限 (Unlimited)**」を選択してください。
- 「**検索時間制限 (Search time limit)**」 - 検索にかける最大秒数を入力するか、「**無制限 (Unlimited)**」を選択してください。
- ドロップダウン・リストから「**別名の参照解除 (Alias dereferencing)**」のタイプを選択します。
  - 「**実行しない (Never)**」 - 選択された項目が別名である場合、その項目を検索のために参照解除しません (つまり、別名への参照は無視されます)。
  - 「**実行して検索 (Finding)**」 - 選択された項目が別名である場合、別名は参照解除され、その別名の位置から検索が実行されます。
  - 「**検索して実行 (Searching)**」 - 選択された項目は参照解除されませんが、検索によって検出された項目はすべて参照解除されます。
  - 「**常に実行 (Always)**」 - 検索中に検出されるすべての別名が参照解除されます。
- 検索で参照が戻されたときに別のサーバーへの追跡参照を行う場合は、「**追跡参照 (Chase referrals)**」チェック・ボックスを選択してください。参照によって別のサーバーへの検索が指示される場合、サー

バーへの接続には現行の信任状が使用されます。そのため、Anonymous でログインしている場合には、認証済み識別名を使用したサーバー・ログインが必要になる場合があります。

### 関連タスク

143 ページの『検索設定の調整』

以下の情報を参考にして、ユーザーの検索機能を制御します。

### 関連資料

53 ページの『検索パラメーター』

サーバーで使用するリソース量を制限するために、管理者は検索パラメーターを使用して、ユーザーの検索能力を制限することができます。また、特定のユーザーの検索能力を拡張することもできます。

## バイナリー属性の変更

以下の情報を参考にして、バイナリー・データのインポート、エクスポート、または削除を行います。

属性にバイナリー・データが必要な場合は、属性のフィールドの隣に「**バイナリー・データ (Binary data)**」ボタンが表示されます。属性にデータが含まれない場合は、フィールドはブランクになります。バイナリー属性は表示することができないため、属性にバイナリー・データが含まれている場合は、フィールドに「**バイナリー・データ - 1 (Binary Data - 1)**」と表示されます。属性に複数值が含まれている場合は、フィールドがドロップダウン・リストとして表示されます。

バイナリー属性の処理を行うには、「**バイナリー・データ (Binary data)**」ボタンをクリックします。

バイナリー・データのインポート、エクスポート、または削除を実行できます。

1. 属性にバイナリー・データを追加するには、次のようにします。
  - a. 「**バイナリー・データ (Binary data)**」ボタンをクリックします。
  - b. 「**インポート**」をクリックする。
  - c. 希望するファイルのパス名を入力することもできますし、「**ブラウズ**」をクリックしてバイナリー・ファイルを探し、選択することもできます。
  - d. 「**ファイルのサブミット (Submit file)**」をクリックします。「**ファイルがアップロードされました (File uploaded)**」というメッセージが表示されます。
  - e. 「**閉じる**」をクリックする。これで、「**バイナリー・データ項目 (Binary data entries)**」の下に「**バイナリー・データ - 1 (Binary Data - 1)**」が表示されるようになります。
  - f. 追加したいバイナリー・ファイルの数だけ、このインポート・プロセスを繰り返してください。後続の項目は、「**バイナリー・データ - 2 (Binary Data - 2)**」、「**バイナリー・データ - 3 (Binary Data - 3)**」という要領でリストされます。
  - g. バイナリー・データの追加が終了したら、「**OK**」をクリックしてください。
2. バイナリー・データをエクスポートするには、次のようにします。
  - a. 「**バイナリー・データ (Binary data)**」ボタンをクリックします。
  - b. 「**エクスポート**」をクリックする。
  - c. リンク「**ダウンロードするバイナリー・データ (Binary data to download)**」をクリックします。
  - d. ウィザードの指示に従って、バイナリー・ファイルを表示するか、バイナリー・ファイルを新しい位置に保管してください。
  - e. 「**閉じる**」をクリックする。
  - f. エクスポートするバイナリー・ファイルの数だけ、このエクスポート・プロセスを繰り返してください。
  - g. データのエクスポートが終了したら、「**OK**」をクリックしてください。



3. バイナリー・データを削除するには、次のようにします。
  - a. 「バイナリー・データ (Binary data)」 ボタンをクリックします。
  - b. 削除するバイナリー・データ・ファイルにチェックを付けます。ファイルは複数選択できます。
  - c. 「削除」をクリックする。
  - d. 削除を確認するプロンプトが表示されたなら、「OK」をクリックしてください。削除のターゲットとしてマークされているバイナリー・データがリストから除去されます。
  - e. データの削除が終了したら、「OK」をクリックしてください。

注: バイナリー属性で検索できるのは、存在のみです。

## ユーザーとグループのタスク

以下の情報を参考にして、ユーザーとグループを管理します。

ユーザーとグループの管理を行うには、Web 管理ツールのナビゲーション領域で「ユーザーとグループ (Users and groups)」のカテゴリーを展開します。

### 関連概念

63 ページの『グループと役割』

メンバーのアクセスまたは許可を編成して制御するには、グループおよび役割を使用します。

## ユーザー・タスク

以下の情報を参考にして、ユーザーを管理します。

レルムとテンプレートをセットアップしたら、今度はこれにユーザーを移植できます。

### 関連資料

90 ページの『認証』

Directory Server 内のアクセスを制御するには、認証方式を使用します。

### ユーザーの追加:

以下の情報を参考にして、ユーザーを追加します。

Web 管理ツールのナビゲーション領域で「ユーザーとグループ」のカテゴリーを展開します。

1. 「ユーザーの追加 (Add user)」をクリックするか、「ユーザーの管理 (Managing users)」をクリックしてから「追加 (Add)」をクリックします。
2. ドロップダウン・メニューから、ユーザーを追加するレルムを選択する。
3. 「次へ」をクリックします。そのレルムに関連付けられているテンプレートが表示されます。必要フィールド (アスタリスク (\*) で示されている) に情報を入力し、タブの他の任意のフィールドに値を入れます。レルム内にすでにグループが作成されている場合は、1 つ以上のグループにユーザーを追加することもできます。
4. 完了したら、「完了」をクリックする。

### レルム内でのユーザーの検索:

以下の情報を参考にして、レルム内でユーザーを検索します。

Web 管理ツールのナビゲーション領域で「ユーザーとグループ」のカテゴリーを展開します。

1. 「**ユーザーの検索 (Find user)**」をクリックするか、「**ユーザーの管理 (Manage users)**」をクリックしてから「**検索 (Find)**」をクリックします。
2. 「**レルムの選択 (Select realm)**」フィールドから、検索を実行するレルムを選択します。
3. 「**命名属性 (Naming attribute)**」フィールドに検索ストリングを入力します。ワイルドカードがサポートされています。たとえば、**\*smith** と入力した場合は、末尾が **smith** の命名属性を持つすべての項目が戻されます。
4. 選択したユーザーに対して以下の操作を実行できます。
  - **編集** - 『ユーザー情報の編集』を参照してください。
  - **コピー** - 『ユーザーのコピー』を参照してください。
  - **削除** - 『ユーザーの除去』を参照してください。
5. 完了したら、「**OK**」をクリックしてください。

#### ユーザー情報の編集:

以下の情報を参考にして、ユーザーの情報を編集します。

Web 管理ツールのナビゲーション領域で「**ユーザーとグループ**」のカテゴリーを展開します。

1. 「**ユーザーの管理 (Manage users)**」をクリックします。
2. ドロップダウン・メニューからレルムを選択します。ユーザーがまだ「**ユーザー (Users)**」ボックスに表示されていない場合は、「**ユーザーの表示 (View users)**」をクリックします。
3. 編集するユーザーを選択し、「**編集 (Edit)**」をクリックします。
4. タブ上の情報に変更を加え、グループ・メンバーシップを変更します。
5. 完了したら、「**OK**」をクリックしてください。

#### ユーザーのコピー:

以下の情報を参考にして、ユーザーをコピーします。

ほとんど同じ情報を持つユーザーを幾つか作成する必要がある場合は、1 つ目のユーザーをコピーし、情報を変更することによって、2 つ目以降のユーザーを作成できます。

Web 管理ツールのナビゲーション領域で「**ユーザーとグループ**」のカテゴリーを展開します。

1. 「**ユーザーの管理 (Manage users)**」をクリックします。
2. ドロップダウン・メニューからレルムを選択します。ユーザーがまだ「**ユーザー (Users)**」ボックスに表示されていない場合は、「**ユーザーの表示 (View users)**」をクリックします。
3. コピーするユーザーを選択し、「**コピー (Copy)**」をクリックします。
4. 新しいユーザーの情報を適宜変更します。たとえば、sn や cn など、固有のユーザーを識別する必須の情報などを変更できます。いずれのユーザーにも共通している情報は、変更する必要はありません。
5. 完了したら、「**OK**」をクリックしてください。

#### ユーザーの除去:

以下の情報を参考にして、ユーザーを除去します。

Web 管理ツールのナビゲーション領域で「**ユーザーとグループ**」のカテゴリーを展開します。

1. 「**ユーザーの管理 (Manage users)**」をクリックします。

2. ドロップダウン・メニューからレルムを選択します。ユーザーがまだ「**ユーザー (Users)**」ボックスに表示されていない場合は、「**ユーザーの表示 (View users)**」をクリックします。
3. 除去するユーザーを選択し、「**除去**」をクリックします。
4. 削除を確認するプロンプトが表示されたら、「**OK**」をクリックします。
5. ユーザーは、ユーザーのリストから除去されます。

## グループ・タスク

以下の情報を参考にして、グループを管理します。

レルムとテンプレートをセットアップしたら、今度はグループを作成できます。

### グループの追加:

以下の情報を参考にして、グループを追加します。

Web 管理ツールのナビゲーション領域で「**ユーザーとグループ**」のカテゴリーを展開します。

1. 「**グループの追加 (Add group)**」をクリックするか、「**グループの管理 (Manage groups)**」をクリックしてから「**追加 (Add)**」をクリックします。
2. 作成するグループの名前を入力する。
3. ドロップダウン・メニューから、グループを追加するレルムを選択します。
4. 「**完了**」をクリックしてグループを作成する。レルム内にすでにユーザーが存在する場合は、「**次へ (Next)**」をクリックすると、グループに追加するユーザーを選択できます。次に、「**完了**」をクリックする。

### 関連概念

63 ページの『**グループと役割**』

メンバーのアクセスまたは許可を編成して制御するには、グループおよび役割を使用します。

### レルム内でのグループの検索:

以下の情報を参考にして、レルム内でグループを検索します。

Web 管理ツールのナビゲーション領域で「**ユーザーとグループ**」のカテゴリーを展開します。

1. 「**グループの検索 (Find group)**」をクリックするか、「**グループの管理 (Manage groups)**」をクリックしてから「**検索 (Find)**」をクリックします。
2. 「**レルムの選択 (Select realm)**」フィールドから、検索を実行するレルムを選択します。
3. 「**命名属性 (Naming attribute)**」フィールドに検索ストリングを入力します。ワイルドカードがサポートされています。たとえば、**\*club** と入力した場合は、**club** の命名属性を持つすべての項目 (たとえば、**book club**、**chess club**、**garden club** など) が戻されます。
4. 選択したグループに対して以下の操作を実行できます。
  - **編集** - 『**グループ情報の編集**』を参照してください。
  - **コピー** - 230 ページの『**グループのコピー**』を参照してください。
  - **削除** - 230 ページの『**グループの除去**』を参照してください。
5. 完了したら、「**閉じる**」をクリックしてください。

### グループ情報の編集:

以下の情報を参考にして、グループの情報を編集します。

Web 管理ツールのナビゲーション領域で「**ユーザーとグループ**」のカテゴリーを展開します。

1. 「**グループの管理 (Manage groups)**」をクリックします。
2. ドロップダウン・メニューからレルムを選択します。グループがまだ「**グループ (Groups)**」ボックスに表示されていない場合は、「**グループの表示 (View groups)**」をクリックします。
3. 編集するグループを選択し、「**編集 (Edit)**」をクリックします。
4. 「**フィルター (Filter)**」をクリックして、「**使用可能なユーザー (Available users)**」の数を制限できます。たとえば、「姓 (Last name)」フィールドに \*smith と入力すると、使用可能なユーザーを Ann Smith、Bob Smith、Joe Goldsmith などの smith で終わるユーザーに制限できます。
5. グループに対するユーザーの追加または除去を実行できます。
6. 完了したら、「**OK**」をクリックしてください。

#### グループのコピー:

以下の情報を参考にして、グループをコピーします。

ほとんど同じメンバーを持つグループを幾つか作成する必要がある場合は、1 つ目のグループをコピーし、情報を変更することによって、2 つ目以降のグループを作成できます。

Web 管理ツールのナビゲーション領域で「**ユーザーとグループ**」のカテゴリーを展開します。

1. 「**グループの管理 (Manage groups)**」をクリックします。
2. ドロップダウン・メニューからレルムを選択します。グループがまだ「**グループ (Groups)**」ボックスに表示されていない場合は、「**グループの表示 (View groups)**」をクリックします。
3. コピーするグループを選択し、「**コピー (Copy)**」をクリックします。
4. 「**グループ名 (Group name)**」フィールドのグループ名を変更します。新しいグループのメンバーは、オリジナルのグループと同じメンバーになっています。
5. グループ・メンバーを変更できます。
6. 完了したら、「**OK**」をクリックしてください。新しいグループが作成されます。メンバーはオリジナルのグループと同じで、コピー・プロシージャの中で行われた任意の追加または除去の変更が加えられています。

#### グループの除去:

以下の情報を参考にして、グループを除去します。

Web 管理ツールのナビゲーション領域で「**ユーザーとグループ**」のカテゴリーを展開します。

1. 「**グループの管理 (Manage groups)**」をクリックします。
2. ドロップダウン・メニューからレルムを選択します。グループがまだ「**グループ (Groups)**」ボックスに表示されていない場合は、「**グループの表示 (View groups)**」をクリックします。
3. 除去するグループを選択し、「**除去**」をクリックします。
4. 削除を確認するプロンプトが表示されたら、「**OK**」をクリックします。
5. グループは、グループのリストから除去されます。

## レルムおよびユーザー・テンプレートのタスク

以下の情報を参考にして、レルムおよびユーザー・テンプレートを管理します。

レルムとユーザー・テンプレートの管理を行うには、Web 管理ツールのナビゲーション領域で「レルムおよびテンプレート (Realms and templates)」をクリックします。レルムやユーザー・テンプレートは、外部からディレクトリーへのデータの入力を容易にするために使用します。

#### 関連概念

52 ページの『レルムおよびユーザー・テンプレート』

Web 管理ツール内に置かれているレルムおよびユーザー・テンプレート・オブジェクトを使用することにより、LDAP の幾つかの基礎的な問題を理解する必要がなくなります。

## レルムの作成

以下の情報を参考にして、レルムを作成します。

レルムを作成するには、次のようにします。

1. Web 管理ツールのナビゲーション領域で、「レルムとテンプレート」 カテゴリーを展開します。
2. 「レルムの追加」をクリックする。
  - レルムの名前を入力します。(たとえば、**realm1** など。)
  - レルムの位置を識別する親 DN を入力します。この項目は、接尾部の形式 (たとえば、**o=ibm,c=us**) で表されます。この項目は接尾部にすることもできますし、ディレクトリー内の別の項目として置くこともできます。「参照」をクリックして、望むサブツリーの位置を選択できます。
3. 「次へ」をクリックして先へ進むか、「完了」をクリックする。
4. 「次へ」をクリックすると、情報を確認できます。この時点ではまだ、実際のレルムの作成は行われていません。ですから、「ユーザー・テンプレート (User template)」と「ユーザー検索フィルター (User search filter)」は無視してかまいません。
5. 「完了」をクリックしてレルムを作成する。

#### 関連概念

52 ページの『レルムおよびユーザー・テンプレート』

Web 管理ツール内に置かれているレルムおよびユーザー・テンプレート・オブジェクトを使用することにより、LDAP の幾つかの基礎的な問題を理解する必要がなくなります。

## レルム管理者の作成

以下の情報を参考にして、レルム管理者を作成します。

レルム管理者を作成するには以下を行って、まず、レルムの管理グループを作成する必要があります。

1. レルムの管理グループを作成します。
  - a. Web 管理ツールのナビゲーション領域で、「ディレクトリー管理」 カテゴリーを展開する。
  - b. 「項目の管理」をクリックする。
  - c. ツリーを展開し、今作成したレルム、**cn=realm1,o=ibm,c=us** を選択する。
  - d. 「ACL の編集」をクリックする。
  - e. 「所有者」タブをクリックする。
  - f. 「所有者の伝搬」がチェックされていることを確認する。
  - g. レルムの DN、**cn=realm1,o=ibm,c=us** を入力する。
  - h. 「タイプ」をグループに変更する。
  - i. 「追加」をクリックする。
2. 管理者の項目を作成します。管理者のユーザー項目がない場合には作成する必要があります。
  - a. Web 管理ツールのナビゲーション領域で、「ディレクトリー管理」 カテゴリーを展開する。

- b. 「**項目の管理**」をクリックする。
- c. 管理者の項目を置く位置までツリーを展開する。

注: 管理者の項目をレルムの外部に置くと、管理者にそれ自身を誤って削除する機能を与えてしまうことを避けることができます。この例では、位置は **o=ibm,c=us** です。

- d. 「**追加**」をクリックする。
  - e. 「**構造化オブジェクト・クラス**」、たとえば **inetOrgPerson** を選択する。
  - f. 「**次へ**」をクリックします。
  - g. 追加する補助オブジェクト・クラスを選択する。
  - h. 「**次へ**」をクリックします。
  - i. 項目に、必須属性を入力する。 例:
    - **RDN** cn=JohnDoe
    - **DN** o=ibm,c=us
    - **cn** John Doe
    - **sn** Doe
  - j. 「**他の属性 (Other attributes)**」タブで、パスワードが割り当てられていることを確認する。
  - k. 完了したら、「**完了**」をクリックする。
3. 管理者を管理グループに追加します。
    - a. Web 管理ツールのナビゲーション領域で、「**ディレクトリー管理**」 カテゴリーを展開する。
    - b. 「**項目の管理**」をクリックする。
    - c. ツリーを展開し、今作成したレルム、**cn=realm1,o=ibm,c=us** を選択する。
    - d. 「**属性の編集**」をクリックする。
    - e. 「**メンバー**」タブをクリックする。
    - f. 「**メンバー**」をクリックする。
    - g. 「**メンバー**」フィールドで管理者の DN、この例では **cn=John Doe,o=ibm,c=us** を入力する。
    - h. 「**追加**」をクリックする。 DN が「**メンバー**」リストに表示されます。
    - i. 「**OK**」をクリックする。
    - j. 「**更新**」をクリックする。 DN が「**現行メンバー (Current members)**」リストに表示されます。
    - k. 「**OK**」をクリックする。
  4. レルム内での項目を管理できる管理者が作成されました。

## テンプレートの作成

以下の情報を参考にして、テンプレートを作成します。

レルムを作成した後の次のステップはユーザー・テンプレートの作成です。テンプレートは、入力する情報を編成するのに役立ちます。Web 管理ツールのナビゲーション領域で、「**レルムとテンプレート**」 カテゴリーを展開します。

1. 「**ユーザー・テンプレートの追加**」をクリックする。
  - テンプレートの名前、たとえば **template1** を入力します。
  - テンプレートを置く位置を入力します。複製目的のため、このテンプレートを使用するレルムのサブツリーにテンプレートを配置します。たとえば、前の操作で作成したレルム **cn=realm1,o=ibm,c=us**。「**参照**」をクリックして、テンプレートの位置として別のサブツリーを選択することもできます。

2. 「次へ」をクリックします。「完了」 をクリックして空のテンプレートを作成できます。後にテンプレートに情報を追加できます。 238 ページの『テンプレートの編集』を参照してください。
3. 「次へ」をクリックした場合、たとえば **inetOrgPerson** など、構造化オブジェクト・クラスをテンプレート用に選択する。 任意の補助オブジェクト・クラスを追加することもできます。
4. 「次へ」をクリックします。
5. 「必須 (Required)」タブがテンプレートに作成されています。 このタブに含まれる情報を変更できます。
  - a. タブ・メニューで「必須 (Required)」を選択し、「編集」をクリックする。「タブの編集」パネルが表示されます。「必須 (Required)」タブの名前と、オブジェクト・クラス (**inetOrgPerson**) に必要な選択済みの以下の属性が表示されます。
    - \*sn - surname
    - \*cn - common name

注: \* は必要な情報を示します。
  - b. このタブに追加情報を追加する場合、「属性」メニューから属性を選択する。たとえば、**departmentNumber** を選択し「追加」をクリックする。**employeeNumber** を選択して「追加」をクリックする。**title** を選択して「追加」をクリックする。これで、「選択された属性」メニューは、以下のようになります。
    - title
    - employeeNumber
    - departmentNumber
    - \*sn
    - \*cn
  - c. テンプレートでのこれらのフィールドの表示を変更するには、選択済み属性を強調表示し、「上に移動」または「下に移動」をクリックします。これで属性の位置が 1 つ変更されます。属性を望む順序に配置するまでこの手順を繰り返します。例:
    - \*sn
    - \*cn
    - title
    - employeeNumber
    - departmentNumber
  - d. また、それぞれの選択済み属性を変更することもできます。
    - 1) 「選択済み属性 (Selected attributes)」ボックスにある属性を強調表示し、「編集」をクリックします。
    - 2) テンプレートに使用されるフィールドの表示名を変更できます。たとえば、 **departmentNumber** を **Department number** として表示するには、それを「表示名」フィールドに入力します。
    - 3) また、デフォルト値を提供して、テンプレートの属性フィールドを事前充てんすることもできます。たとえば、入力するユーザーのほとんどが部門 789 のメンバーである場合、789 をデフォルト値として入力できます。テンプレートのフィールドは 789 で事前充てんされます。値は、実際のユーザー情報を追加するときに変更できます。
    - 4) 「OK」をクリックする。
  - e. 「OK」をクリックする。
6. 追加情報のために別のタブ・カテゴリーを作成するには、「追加」をクリックする。

- 新規のタブの名前を入力する。たとえば、住所情報など。
  - このタブに、「属性」メニューから属性を選択する。たとえば、**homePostalAddress** を選択し「追加」をクリックする。**postOfficeBox** を選択して「追加」をクリックする。**telephoneNumber** を選択して「追加」をクリックする。**homePhone** を選択して「追加」をクリックする。**facsimileTelephoneNumber** を選択して「追加」をクリックする。「選択された属性」メニューは、以下ようになります。
    - homePostalAddress
    - postOfficeBox
    - telephoneNumber
    - homePhone
    - facsimileTelephoneNumber
  - テンプレートでのこれらのフィールドの表示を変更するには、選択済み属性を強調表示し、「上に移動」または「下に移動」をクリックします。これで属性の位置が 1 つ変更されます。属性を望む順序に配置するまでこの手順を繰り返します。例:
    - homePostalAddress
    - postOfficeBox
    - telephoneNumber
    - facsimileTelephoneNumber
    - homePhone
  - 「OK」をクリックする。
7. 他の作成するタブに対してもこのプロセスを繰り返す。完了したら、「完了」をクリックしてテンプレートを作成する。

## レルムへのテンプレートの追加

以下の情報を参考にして、レルムにテンプレートを追加します。

レルムおよびテンプレートを作成した後、テンプレートをレルムに追加する必要があります。Web 管理ツールのナビゲーション領域で、「レルムとテンプレート」 カテゴリーを展開します。

1. 「レルムの管理」をクリックする。
2. テンプレートを追加するレルムを選択する。この例では、**cn=realm1,o=ibm,c=us**。それから「編集」をクリックする。
3. 「ユーザー・テンプレート」までスクロールダウンし、ドロップダウン・メニューを展開する。
4. テンプレートを選択する。この例では、**cn=template1,cn=realm1,o=ibm,c=us**。
5. 「OK」をクリックする。
6. 「閉じる」をクリックする。

## グループの作成

以下の情報を参考にして、グループを作成します。

Web 管理ツールのナビゲーション領域で「ユーザーとグループ」のカテゴリーを展開します。

1. 「グループの追加」をクリックする。
2. 作成するグループの名前を入力する。例: **group1**。
3. ドロップダウン・メニューから、ユーザーを追加するレルムを選択する。この場合は、**realm1**。



4. 「完了」をクリックしてグループを作成する。ユーザーがすでにそのレルムにある場合、「次へ」をクリックして `group1` に追加するユーザーを選択できる。次に、「完了」をクリックする。

#### 関連概念

63 ページの『グループと役割』

メンバーのアクセスまたは許可を編成して制御するには、グループおよび役割を使用します。

### レルムへのユーザーの追加

以下の情報を参考にして、レルムにユーザーを追加します。

Web 管理ツールのナビゲーション領域で「ユーザーとグループ」のカテゴリーを展開します。

1. 「ユーザーの追加」をクリックする。
2. ドロップダウン・メニューから、ユーザーを追加するレルムを選択する。この場合は、**realm1**。
3. 「次へ」をクリックします。今作成したテンプレート、`template1` が表示されます。必要フィールド (アスタリスク (\*) で示されている) に情報を入力し、タブの他の任意のフィールドに値を入れます。レルム内にすでにグループが作成されている場合は、1 つ以上のグループにユーザーを追加することもできます。
4. 完了したら、「完了」をクリックする。

### レルムのタスク

以下の情報を参考にして、レルムを管理します。

最初のレルムをセットアップしデータを取り込んだ後、さらにレルムを追加したり、既存のレルムを変更したりすることができます。

ナビゲーション領域で、「レルムとテンプレート」カテゴリーを展開し、「レルムの管理」をクリックします。既存のレルムのリストが表示されます。このパネルから、レルムの追加、レルムの編集、レルムの除去、またレルムのアクセス制御リスト (ACL) の編集を行うことができます。

#### レルムの追加:

以下の情報を参考にして、レルムを追加します。

Web 管理ツールのナビゲーション領域で、「レルムとテンプレート」カテゴリーを展開します。

1. 「レルムの追加」をクリックします。
  - レルムの名前を入力します。例: **realm2**。
  - すでに存在するレルム、たとえば **realm1** などがある場合、1 つのレルムを選択してその設定を、作成するレルムにコピーすることができます。
  - レルムの位置を識別する親 DN を入力します。この項目は、接尾部の形式 (たとえば、**o=ibm,c=us**) で表されます。「参照」をクリックして、望むサブツリーの位置を選択できます。
2. 「次へ」をクリックして先へ進むか、「完了」をクリックする。
3. 「次へ」をクリックすると、情報を確認できます。
4. ドロップダウン・メニューから「ユーザー・テンプレート」を選択する。すでに存在するレルムから設定をコピーした場合、そのテンプレートはこのフィールドにすでに事前充てんされています。
5. 「ユーザー検索フィルター」を入力する。
6. 「完了」をクリックしてレルムを作成する。

#### レルムの編集:

以下の情報を参考にして、レルムを編集します。

Web 管理ツールのナビゲーション領域で、「レルムとテンプレート」 カテゴリーを展開します。

- 「レルムの管理」をクリックする。
- レルムのリストから編集するレルムを選択する。
- 「編集」をクリックする。
  - 「参照」 ボタンを使用して以下を変更できます。
    - 管理者グループ
    - グループ・コンテナ
    - ユーザー・コンテナ
  - ドロップダウン・メニューから別のテンプレートを選択できます。
  - 「編集」 をクリックして、「ユーザー検索フィルター」を編集します。
- 終了したら、「OK」 をクリックする。

#### レルムの除去:

以下の情報を参考にして、レルムを除去します。

Web 管理ツールのナビゲーション領域で、「レルムとテンプレート」 カテゴリーを展開します。

1. 「レルムの管理」 をクリックする。
2. 除去するレルムを選択する。
3. 「削除」 をクリックする。
4. 削除を確認するプロンプトが表示されたら、「OK」 をクリックする。
5. そのレルムはレルムのリストから除去される。

#### レルム上の ACL の編集:

以下の情報を参考にして、レルム上の ACL を編集します。

Web 管理ツール・ユーティリティーを使用して ACL のプロパティーを表示し、ACL に対する作業を行う場合は、239 ページの『アクセス制御リスト (ACL) のタスク』を参照してください。

##### 関連概念

72 ページの『アクセス制御リスト』

アクセス制御リスト (ACL) を使用すると、LDAP ディレクトリーに保管された情報を保護することができます。管理者は ACL を使用して、ディレクトリーのさまざまな部分へのアクセスや、特定のディレクトリー項目へのアクセスを制限します。

#### テンプレート・タスク

以下の情報を参考にして、テンプレートを管理します。

最初のテンプレートを作成した後、さらにテンプレートを追加したり、現存のテンプレートを変更したりすることができます。

ナビゲーション領域で、「レルムとテンプレート」 カテゴリーを展開し、「ユーザー・テンプレートの管理」 をクリックします。既存のテンプレートのリストが表示されます。このパネルから、テンプレートの追加、テンプレートの編集、テンプレートの除去、またテンプレートのアクセス制御リスト (ACL) の編集を行うことができます。

## ユーザー・テンプレートの追加:

以下の情報を参考にして、ユーザー・テンプレートを追加します。

Web 管理ツールのナビゲーション領域で、「レلمとテンプレート」 カテゴリーを展開します。

1. 「ユーザー・テンプレートの追加」または「ユーザー・テンプレートの管理」をクリックして、「追加」をクリックする。
  - 新規のテンプレートの名前を入力します。例: **template2**。
  - すでに存在するテンプレート、たとえば **template1** などがある場合、1 つのテンプレートを選択してその設定を、作成するテンプレートにコピーすることができます。
  - テンプレートの位置を示す親 DN を入力します。この項目は DN の形式です。例: **cn=realm1,o=ibm,c=us**。「参照」をクリックして、望むサブツリーの位置を選択できます。
2. 「次へ」をクリックします。「完了」をクリックして空のテンプレートを作成できます。後にテンプレートに情報を追加できます。 238 ページの『テンプレートの編集』を参照してください。
3. 「次へ」をクリックした場合、たとえば **inetOrgPerson** など、構造化オブジェクト・クラスをテンプレート用を選択する。任意の補助オブジェクト・クラスを追加することもできます。
4. 「次へ」をクリックします。
5. 「必須 (Required)」タブがテンプレートに作成されています。このタブに含まれる情報を変更できます。
  - a. タブ・メニューで「必須 (Required)」を選択し、「編集」をクリックする。「タブの編集」パネルが表示されます。「必須 (Required)」タブの名前と、オブジェクト・クラス (**inetOrgPerson**) に必要な選択済みの以下の属性が表示されます。
    - \*sn - surname
    - \*cn - common name

注: \* は必要な情報を示します。
  - b. このタブに追加情報を追加する場合、「属性」メニューから属性を選択する。たとえば、**departmentNumber** を選択し「追加」をクリックする。**employeeNumber** を選択して「追加」をクリックする。**title** を選択して「追加」をクリックする。これで、「選択された属性」メニューは、以下のようになります。
    - title
    - employeeNumber
    - departmentNumber
    - \*sn
    - \*cn
  - c. テンプレートでのこれらのフィールドの表示を変更するには、選択済み属性を強調表示し、「上に移動」または「下に移動」をクリックします。これで属性の位置が 1 つ変更されます。属性を望む順序に配置するまでこの手順を繰り返します。例:
    - \*sn
    - \*cn
    - title
    - employeeNumber
    - departmentNumber
  - d. また、それぞれの選択済み属性を変更することもできます。

- 1) 「**選択済み属性 (Selected attributes)**」ボックスにある属性を強調表示し、「**編集**」をクリックします。
  - 2) テンプレートに使用されるフィールドの表示名を変更できます。たとえば、**departmentNumber** を **Department number** として表示するには、それを「**表示名**」フィールドに入力します。
  - 3) また、デフォルト値を提供して、テンプレートの属性フィールドを事前充てんすることもできます。たとえば、入力するユーザーのほとんどが部門 789 のメンバーである場合、789 をデフォルト値として入力できます。テンプレートのフィールドは 789 で事前充てんされます。値は、実際のユーザー情報を追加するときに変更できます。
  - 4) 「**OK**」をクリックする。
- e. 「**OK**」をクリックする。
6. 追加情報のために別のタブ・カテゴリを作成するには、「**追加**」をクリックする。
- 新規のタブの名前を入力する。たとえば、住所情報など。
  - このタブに、「**属性**」メニューから属性を選択する。たとえば、**homePostalAddress** を選択し「**追加**」をクリックする。**postOfficeBox** を選択して「**追加**」をクリックする。**telephoneNumber** を選択して「**追加**」をクリックする。**homePhone** を選択して「**追加**」をクリックする。**facsimileTelephoneNumber** を選択して「**追加**」をクリックする。「**選択された属性**」メニューは、以下ようになります。
    - homePostalAddress
    - postOfficeBox
    - telephoneNumber
    - homePhone
    - facsimileTelephoneNumber
  - テンプレートでのこれらのフィールドの表示を変更するには、選択済み属性を強調表示し、「**上に移動**」または「**下に移動**」をクリックします。これで属性の位置が 1 つ変更されます。属性を望む順序に配置するまでこの手順を繰り返します。例:
    - homePostalAddress
    - postOfficeBox
    - telephoneNumber
    - facsimileTelephoneNumber
    - homePhone
  - 「**OK**」をクリックする。
7. 他の作成するタブに対してもこのプロセスを繰り返す。完了したら、「**完了**」をクリックしてテンプレートを作成する。

### テンプレートの編集:

以下の情報を参考にして、テンプレートを編集します。

Web 管理ツールのナビゲーション領域で、「**レلمとテンプレート**」カテゴリを展開します。

- 「**ユーザー・テンプレートの管理**」をクリックする。
- レلمのリストから編集するレلمを選択する。
- 「**編集**」をクリックする。
- すでに存在するテンプレート、たとえば **template1** などがある場合、1 つのテンプレートを選択してその設定を、編集するテンプレートにコピーすることができます。

- 「次へ」をクリックします。
  - ドロップダウン・メニューを使用してテンプレートの構造化オブジェクト・クラスを変更できます。
  - 補助オブジェクト・クラスを追加または変更することもできます。
- 「次へ」をクリックします。
- テンプレートに含まれるタブおよび属性を変更することができます。タブの変更方法については、ステップ5 (237 ページ)を参照してください。
- 完了したら、「完了」をクリックする。

#### テンプレートの除去:

以下の情報を参考にして、テンプレートを除去します。

Web 管理ツールのナビゲーション領域で、「レームとテンプレート」 カテゴリーを展開します。

1. 「ユーザー・テンプレートの管理」をクリックする。
2. 除去するテンプレートを選択する。
3. 「削除」をクリックする。
4. 削除を確認するプロンプトが表示されたら、「OK」をクリックする。
5. そのテンプレートはテンプレートのリストから除去される。

#### テンプレート上の ACL の編集:

以下の情報を参考にして、テンプレート上の ACL を編集します。

Web 管理ツールのナビゲーション領域で、「レームとテンプレート」 カテゴリーを展開します。

1. 「ユーザー・テンプレートの管理」をクリックする。
2. ACL を編集するテンプレートを選択する。
3. 「ACL の編集」をクリックする。

Web 管理ツール・ユーティリティを使用して ACL のプロパティを表示し、ACL に対する作業を行う場合は、『アクセス制御リスト (ACL) のタスク』を参照してください。

#### 関連概念

72 ページの『アクセス制御リスト』

アクセス制御リスト (ACL) を使用すると、LDAP ディレクトリーに保管された情報を保護することができます。管理者は ACL を使用して、ディレクトリーのさまざまな部分へのアクセスや、特定のディレクトリー項目へのアクセスを制限します。

## アクセス制御リスト (ACL) のタスク

以下の情報を参考にして、アクセス制御リスト (ACL) を管理します。

#### 関連概念

72 ページの『アクセス制御リスト』

アクセス制御リスト (ACL) を使用すると、LDAP ディレクトリーに保管された情報を保護することができます。管理者は ACL を使用して、ディレクトリーのさまざまな部分へのアクセスや、特定のディレクトリー項目へのアクセスを制限します。

## 特定の有効な ACL のアクセス権限の表示

以下の情報を参考にして、特定の有効なアクセス制御リスト (ACL) のアクセス権限を表示します。

有効な ACL は、選択された項目の明示的な ACL と継承による ACL です。

1. ディレクトリー入力を選択する。例: cn=John Doe,ou=Advertising,o=ibm,c=US。
2. 「**ACL の編集**」をクリックする。「ACL の編集 (Edit ACL)」パネルが表示され、「**有効な ACL**」タブが事前選択されます。「**有効な ACL**」タブには、ACL に関する読み取り専用の情報が示されません。
3. 特定の有効な ACL を選択し、「**表示**」をクリックする。「**アクセス権の表示**」パネルが開きます。
4. 「**OK**」をクリックして「有効な ACL」タブに戻ります。
5. 「**キャンセル**」をクリックして「ACL の編集」パネルに戻ります。

## 有効な所有者の表示

以下の情報を参考にして、有効な所有者を表示します。

有効な所有者は、選択された項目の明示的で継承された所有者です。

1. ディレクトリー入力を選択する。例: cn=John Doe,ou=Advertising,o=ibm,c=US。
2. 「**ACL の編集**」をクリックする。
3. 「**Effective owners (有効な所有者)**」タブをクリックする。「**Effective owners (有効な所有者)**」タブには、ACL に関する読み取り専用の情報が示されます。
4. 「**キャンセル**」をクリックして「ACL の編集」パネルに戻ります。

## 未フィルターの ACL の追加、編集、および除去

以下の情報を参考にして、未フィルターのアクセス制御リスト (ACL) を管理します。

項目に、新規のフィルターに掛けられていない ACL を追加したり、または既存のフィルターに掛けられていない ACL を編集したりすることができます。

フィルターに掛けられていない ACL は伝搬することができます。つまり、1 つの項目に対して定義されているアクセス・コントロール情報を、そのすべての従属の項目に対して適用できます。ACL ソースは、選択された項目の現行の ACL のソースです。項目に ACL がない場合、その項目は親オブジェクトの ACL 設定に基づいて親オブジェクトから ACL を継承します。

「**フィルターに掛けられていない ACL (Non-filtered ACLs)**」タブに以下の情報を入力します。

- **ACL の伝搬** - 「**伝搬 (Propagate)**」チェック・ボックスを選択して、明示的に定義された ACL のない子孫がこの項目から継承することができるようにします。このチェック・ボックスが選択された場合、子孫はこの項目から ACL を継承し、ACL が子項目に明示的に定義されている場合、親から継承された ACL は追加された ACL に置き換えられます。チェック・ボックスが選択されていない場合、明示的に定義された ACL のない子孫項目は、このオプションが使用可能であるこの項目の親から ACL を継承します。
- **DN (識別名)** - 選択された項目に対する操作の実行アクセスを要求しているエンティティの **(DN) 識別名**を入力します (cn=Marketing Group など)。
- **タイプ** - DN の **タイプ**を入力します。DN がユーザーの場合、たとえば access-id を選択します。

「**追加**」ボタンをクリックして DN (識別名) フィールドの DN を ACL リストに追加するか、または「**編集**」ボタンをクリックして既存の DN の ACL を変更します。

「アクセス権の追加」パネルおよび「アクセス権の編集」パネルでは、新規または既存のアクセス制御リスト (ACL) にアクセス権を設定することができます。「タイプ」フィールドは、デフォルトで「ACL の編集」パネルで選択したタイプになります。ACL を追加する場合、他のすべてのフィールドはデフォルトで空白になります。ACL を編集する場合、フィールドには先回 ACL が編集された時に設定された値が含まれています。

以下を行うことができます。

- ACL タイプを変更する
- 追加および削除の権限を設定する
- セキュリティー・クラスの許可を設定する

アクセス権を設定するには以下のようにします。

1. ACL の項目の**タイプ**を選択します。DN がユーザーの場合、たとえば `access-id` を選択します。
2. 「**権利**」セクションに対象の追加および削除権限が表示されます。
  - 「**子の追加**」は、ディレクトリー項目を選択された項目の下に追加する権限を付与または拒否します。
  - 「**項目の削除**」は対象に、選択された項目を削除する権限を付与または拒否します。
3. 「**セキュリティ・クラス (Security class)**」セクションでは、属性クラスに対する許可が定義されています。属性は、セキュリティ・クラスのグループに分けられています。
  - **Normal (通常)** - 通常属性クラスは最小限度のセキュリティを必要とします。例としては、属性 `commonName` があります。
  - **Sensitive (重要)** - 重要属性クラスは適度のセキュリティを必要とします。例としては、`homePhone` があります。
  - **Critical (重大)** - 重大属性クラスは最大のセキュリティを必要とします。例としては、属性 `userpassword` があります。
  - **システム** - システム属性はサーバーによって保守される読み取り専用属性です。
  - **制限付き** - 制限付き属性はアクセス制御を定義するために使用されます。

それぞれのセキュリティ・クラスには、許可が関連しています。

- **読み取り** - 対象は、属性を読み取ることができます。
- **書き込み** - 対象は、属性を変更することができます。
- **検索** - 対象は、属性を検索することができます。
- **比較** - 対象は、属性を比較することができます。

加えて、属性が属するセキュリティ・クラスの代わりに属性に基づいて許可を指定することもできます。属性セクションは「**重大セキュリティ・クラス (Critical security class)**」の下にリストされています。

- 「**属性の定義 (Define an attribute)**」ドロップダウン・リストから属性を選択する。
- 「**Define (定義)**」をクリックする。属性が許可のテーブルと共に表示されます。
- 属性に関連した 4 つのセキュリティ・クラスの許可をそれぞれ認可するか拒否するかを指定する。
- この手順を複数の属性に対して繰り返すことができます。
- 属性を削除するには、単にその属性を選択して「**削除**」をクリックする。
- 完了したら、「**OK**」をクリックする。

2 つの方法のどちらかで ACL を除去することができます。

- 削除する ACL の横にあるラジオ・ボタンを選択する。「除去」をクリックする。
- 「すべて除去」をクリックし、リストからすべての DN を削除する。

## フィルター済みの ACL の追加、編集、および除去

以下の情報を参考にして、フィルター済みのアクセス制御リスト (ACL) のアクセス権限を表示します。

項目に、新規のフィルターに掛けられた ACL を追加したり、または既存のフィルターに掛けられた ACL を編集したりすることができます。

フィルター・ベースの ACL は、指定されたオブジェクト・フィルターを使用してフィルター・ベースの比較を行い、ターゲット・オブジェクトと、そのターゲット・オブジェクトに適用される有効なアクセスを突き合わせます。

フィルター・ベースの ACL のデフォルト動作では、最下位の収容項目から、祖先項目チェーンを上に向かって、DIT の最上位の収容項目まで累算します。有効なアクセス権は、構成要素になっている祖先の項目により認可または拒否されたアクセス権限の和集合として計算されます。この動作には、例外があります。サブツリーの複製機能との互換性のため、また管理の柔軟性を高めるために、累積を停止する手段として上限属性を使用できます。つまり、その上限属性の含まれている項目で累積を停止できるようになっています。

「フィルターに掛けられた ACL」タブに以下の情報を入力します。

- フィルターに掛けられた ACL の累積 -
  - 「指定なし」ラジオ・ボタンを選択し、`ibm-filterACLInherit` 属性を選択された項目から除去する。
  - 「真」ラジオ・ボタンを選択し、選択された項目の ACL が、その項目から、上位項目チェーンを上に向かって DIT のフィルター ACL の最高レベルの収容項目へと累積するようにします。
  - 「偽」ラジオ・ボタンを選択し、選択された項目でのフィルター ACL の累積を停止します。
- DN (識別名) - 選択された項目に対する操作の実行アクセスを要求しているエンティティの (DN) 識別名を入力します (`cn=Marketing Group` など)。
- タイプ - DN のタイプを入力します。DN がユーザーの場合、たとえば `access-id` を選択します。

「追加」ボタンをクリックして DN (識別名) フィールドの DN を ACL リストに追加するか、または「編集」ボタンをクリックして既存の DN の ACL を変更します。

「アクセス権の追加」パネルおよび「アクセス権の編集」パネルでは、新規または既存のアクセス制御リスト (ACL) にアクセス権限を設定することができます。「タイプ」フィールドは、デフォルトで「ACL の編集」パネルで選択したタイプになります。ACL を追加する場合、他のすべてのフィールドはデフォルトでブランクになります。ACL を編集する場合、フィールドには前回 ACL が編集された時に設定された値が含まれています。

以下を行うことができます。

- ACL タイプを変更する
- 追加および削除の権限を設定する
- フィルターに掛けられた ACL にオブジェクト・フィルターを設定する
- セキュリティー・クラスの許可を設定する

アクセス権限を設定するには以下のようにします。

1. ACL の項目のタイプを選択します。DN がユーザーの場合、たとえば `access-id` を選択します。



2. 「**権利**」セクションに対象の追加および削除権限が表示されます。
  - 「**子の追加**」は、ディレクトリー項目を選択された項目の下に追加する権限を付与または拒否します。
  - 「**項目の削除**」は対象に、選択された項目を削除する権限を付与または拒否します。
3. フィルター・ベースの比較にオブジェクト・フィルターを設定します。「**オブジェクト・フィルター**」フィールドに、選択された ACL に対して望ましいオブジェクト・フィルターを入力します。検索フィルター・ストリングを合成する支援のために、「**フィルターの編集**」ボタンをクリックします。現行のフィルターに掛けられた ACL は、関連したサブツリー中の、このフィールド中のフィルターに一致する子孫オブジェクトに伝搬します。
4. 「**セキュリティー・クラス (Security class)**」セクションでは、属性クラスに対する許可が定義されています。属性は、セキュリティー・クラスのグループに分けられています。
  - **Normal (通常)** - 通常属性クラスは最小限度のセキュリティーを必要とします。例としては、属性 `commonName` があります。
  - **Sensitive (重要)** - 重要属性クラスは適度のセキュリティーを必要とします。例としては、`homePhone` があります。
  - **Critical (重大)** - 重大属性クラスは最大のセキュリティーを必要とします。例としては、属性 `userpassword` があります。
  - **システム** - システム属性はサーバーによって保守される読み取り専用属性です。
  - **制限付き** - 制限付き属性はアクセス制御を定義するために使用されます。

それぞれのセキュリティー・クラスには、許可が関連しています。

- **読み取り** - 対象は、属性を読み取ることができます。
- **書き込み** - 対象は、属性を変更することができます。
- **検索** - 対象は、属性を検索することができます。
- **比較** - 対象は、属性を比較することができます。

加えて、属性が属するセキュリティー・クラスの代わりに属性に基づいて許可を指定することもできます。属性セクションは「**重大セキュリティー・クラス (Critical security class)**」の下にリストされています。

- 「**属性の定義 (Define an attribute)**」ドロップダウン・リストから属性を選択する。
- 「**Define (定義)**」をクリックする。属性が許可のテーブルと共に表示されます。
- 属性に関連した 4 つのセキュリティー・クラスの許可をそれぞれ認可するか拒否するかを指定する。
- この手順を複数の属性に対して繰り返すことができます。
- 属性を削除するには、単にその属性を選択して「**削除**」をクリックする。
- 完了したら、「**OK**」をクリックする。

2 つの方法のどちらかで ACL を除去することができます。

- 削除する ACL の横にあるラジオ・ボタンを選択する。「**除去**」をクリックする。
- 「**すべて除去**」をクリックし、リストからすべての DN を削除する。

## 所有者の追加または除去

以下の情報を参考にして、所有者を追加または除去します。

項目の所有者には、オブジェクトに対してどのような操作を行ってもよい完全な許可があります。項目の所有者は、明示的であることもあるいは伝搬される（継承される）こともできます。

「所有者」タブに以下の情報を入力します。

1. 「所有者の伝搬」チェック・ボックスを選択して、明示的に定義された所有者のない子孫がこの項目から継承することができるようにします。チェック・ボックスが選択されていない場合、明示的に定義された所有者のない子孫項目は、このオプションが使用可能であるこの項目の親から所有者を継承します。
2. DN (識別名) - 選択された項目に対する操作の実行アクセスを要求しているエンティティの **(DN) 識別名** を入力します (cn=Marketing Group など)。他のオブジェクトに所有権を伝搬するオブジェクトに cn=this を使用すると、それぞれのオブジェクトがそれ自体に所有されているディレクトリー・サブツリーの作成が容易になります。
3. タイプ - DN の **タイプ** を入力します。DN がユーザーの場合、たとえば access-id を選択します。

所有者を追加するには、「追加」ボタンをクリックして、**DN (識別名) フィールド**の DN をリストに追加します。

2 つの方法のどちらかで所有者を除去することができます。

- 削除する所有者の横にあるラジオ・ボタンを選択する。「除去」をクリックする。
- 「すべて除去」をクリックし、リストからすべての所有者 DN を削除する。

---

## 参照

コマンド行ユーティリティーや LDIF 情報などの、Directory Server に関連した参照資料。

追加の参照情報は、以下を参照してください。

## Directory Server のコマンド行ユーティリティー

この項では、Qshell コマンド環境から実行できる Directory Server ユーティリティーについて説明します。

ストリングの中には、Qshell コマンド環境で正しくプロセスされるには引用符で囲まれる必要のあるものがあることに注意してください。これには一般に、DN、検索フィルター、および ldapsearch によって戻される属性のリストであるストリングが関係しています。以下のリストの例を参照してください。

- スペースを含むストリング: "cn=John Smith,cn=users"
- ワイルドカード文字を含むストリング: "\*"
- 括弧を含むストリング: "(objectclass=person)"

Qshell コマンド環境について詳しくは、『Qshell』トピックを参照してください。

詳しくは、以下のコマンドを参照してください。

## ldapmodify および ldapadd

LDAP modify-entry および LDAP add-entry コマンド行ユーティリティー

### 概要

```
l ldapmodify [-a] [-b] [-c] [-C charset] [-d debuglevel][--D binddn] [-e errorfile]
[-g] [-f file][--F][-g][-G realm] [-h ldaphost] [-i file] [-k] [--K keyfile]
[-m mechanism] [--M][-n][--N certificatename] [-O maxhops] [--p ldapport]
```

[-P keyfilepw] [-r] [-R][-U username] [-v] [-V] [-w passwd | ?] [-y proxydn]  
[-Y] [-Z]

| ldapadd [-a] [-b] [-c] [-C charset] [-d debuglevel] [-D binddn] [-e errorfile]  
[-g] [-f file] [-F] [-g] [-G realm] [-h ldaphost] [-i file] [-k] [-K keyfile]  
[-m mechanism] [-M] [-n] [-N certificatename] [-O maxhops] [-p ldapport]  
[-P keyfilepw] [-r] [-R][-U username] [-v] [-V] [-w passwd | ?] [-y proxydn]  
[-Y] [-Z]

## 説明

| **ldapmodify** は、`ldap_modify`、`ldap_add`、`ldap_delete`、および `ldap_rename` アプリケーション・プログラミング・インターフェース (API) へのコマンド行インターフェースです。 **ldapadd** は `ldapmodify` のリネームされたバージョンとしてインプリメントされています。 `ldapadd` として呼び出されると、**-a** (新規の項目追加) フラグが自動的に立てられます。

**ldapmodify** は LDAP サーバーへの接続を開き、サーバーにバインドします。 **ldapmodify** を使用して入力を変更または追加することができます。入力情報は、標準入力またはファイルから、**-i** オプションの使用を通して読み取られます。

**ldapmodify** または **ldapadd** の構文ヘルプを表示するには、以下を入力します。

`ldapmodify -?`

または

`ldapadd -?`

## オプション

**-a** 項目の新規追加。 **ldapmodify** のデフォルトのアクションは、現存の項目の変更です。 **ldapadd** として呼び出されると、このフラグが常に立てられます。

**-b** `/` で始まるすべての値はバイナリー値であり、また実際の値は、値の代わりにパスが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** 連続操作モード。エラーは報告されますが、 **ldapmodify** は変更処理を続行します。そうでなければ、デフォルトのアクションでは、エラーの報告後に終了します。

**-C charset**

**ldapmodify** および **ldapadd** ユーティリティへの入力として提供された文字列を、charset で指定されるローカル文字セットで表されるようにし、 UTF-8 に変換されるよう指定します。入力文字列のコード・ページがジョブのコード・ページ値と異なる場合には、 **-C charset** 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 を参照してください。

**-d debuglevel**

LDAP 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、文字列表記の DN です。 **-m DIGEST-MD5** で使用する場合は、権限 ID を指定するために使用します。これは DN とすることもできるし、あるいは「u:」または「dn:」で始まる `authzId` 文字列とすることもできます。

| **-e errorfile**

| リジェクトされた項目の書き込み先のファイルを指定します。このオプションには、**-c** 連続稼働オ

プシオンが必要です。項目の処理が失敗した場合、その項目はリジェクト・ファイルに書き込まれ、リジェクトされた項目のカウントが増やされます。 `ldapmodify` または `ldapadd` コマンドへの入力がファイルからのものである場合、そのファイルが処理されるたびに、リジェクト・ファイルに書き込まれた項目の合計数が示されます。

**-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。  
**-i** または **-f** オプションを使用して、入力ファイルを指定することができます。動作は同じです。

**-F replica:** で開始する入力行の内容と関係なく、アプリケーションにすべての変更を強制します (デフォルトによって、**replica:** 行が使用中の LDAP サーバー・ホストおよびポートと比較されて、複製ログ・レコードを実際に適用する必要があるかどうかを判別されます)。

**-g** 属性値の末尾スペースを除去しません。

**-G** レルムを指定します。このパラメーターはオプションです。**-m DIGEST-MD5** と一緒に使用すると、その値はバインド中にサーバーに渡されます。

#### **-h ldaphost**

LDAP サーバーを実行する代替ホストを指定します。

**-i 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。  
**-i** または **-f** オプションを使用して、入力ファイルを指定することができます。動作は同じです。

**-k** サーバー管理制御の使用を指定します。

#### **-K keyfile**

**kdb** のデフォルト拡張子のある 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。キー・データベース・ファイル名が指定されていない場合、このユーティリティーはまず関連したファイル名の `SSL_KEYRING` 環境変数の存在を探します。  
`SSL_KEYRING` 環境変数が定義されていない場合、あればシステム鍵リング・ファイルが使用されます。

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。i5/OS 上のディレクトリー・サーバーでは、**-Z** を使用して **-K** または **-N** を使用しない場合、ディレクトリー・サービス・クライアント・アプリケーション ID に関連した証明が使用されます。

**-l** 変更を複製しません。「Do Not Replicate (複製しない)」制御は、ある特定の変更を複製しないことを要求するときに使用します。これは、複製トポロジーで使用するための制御です。つまり、他のサーバーに変更が加えられる原因とならないように、複製トポロジーを同期させるための変更をターゲット・サーバーが複製しないようにします。また、管理クライアントがこの制御を使用することもできます。

#### **-m mechanism**

**mechanism** を使用して、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。`ldap_sasl_bind_s()` API が使用されます。**-V 2** をセットすると、**-m** パラメーターは無視されます。**-m** を指定しない場合、単純認証が使用されます。以下が有効なメカニズムです。

- CRAM-MD5 - サーバーに送信されるパスワードを保護する。
- EXTERNAL - SSL 認証を使用する。**-Z** が必要。
- GSSAPI - ユーザーの Kerberos 信任状を使用する。

- DIGEST-MD5 - クライアントは `username` 値をサーバーに送信する必要があります。-U が必要。権限 ID を指定するには、-D パラメーター (通常、バインド DN) が使用されます。これは DN とすることもできるし、あるいは「u:」または「dn:」で始まる `authzId` スtring とすることもできます。
- OS400\_PRFTKN - システム・プロジェクト・バックエンド中のユーザーの DN を使用して、ローカル LDAP サーバーに対して現行 i5/OS ユーザーとして認証します。-D (バインド DN) および -w (パスワード) パラメーターは指定しないでください。

**-M** 参照オブジェクトを普通の項目として管理します。

**-n** ノーオペレーション・オプションを指定します。それにより、ディレクトリーに対するアクションを実際に行う前に、発行しようとしているコマンドの結果をプレビューすることができます。加えた変更は、その前に感嘆符を付けられて、標準出力に出力されます。ディレクトリーの変更を実行する関数の呼び出しの前に、入力ファイルの処理で見つかった構文エラーはすべて、標準エラーとして表示されます。このオプションにデバッグ操作の -v オプションを指定すると、エラーの検出時に特に便利です。

**-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 サーバーがサーバー認証だけを実行するように構成されている場合は、クライアント証明書は不要です。LDAP サーバーがクライアントおよびサーバーの認証を実行するように構成されている場合は、クライアント証明書が必要です。証明書/秘密鍵のペアがキー・データベース・ファイルの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。i5/OS 上のディレクトリー・サーバーでは、-Z を使用して -K または -N を使用しない場合、ディレクトリー・サービス・クライアント・アプリケーション ID に関連した証明が使用されます。

**-O** *maxhops*

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 *maxhops* を指定します。デフォルトのホップ・カウントは 10 です。

**-p** *ldapport*

LDAP サーバーが listen する代替 TCP ポートを指定します。デフォルトの LDAP ポートは 389 です。**-p** 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。

**-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、1 つ以上の秘密鍵を含む場合のあるキー・データベース・ファイル内の暗号化された情報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、パスワードはそのパスワード `stash` ファイルから取得されるので、**-P** 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。

**-r** デフォルトの設定では、既存の値が置換されます。

**-R** 参照を自動的に行わないことを指定します。

**-U** ユーザー名を指定します。**-m** DIGEST-MD5 には必要ですが、その他のメカニズムでは無視されます。

**-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。

**-V** *version*

LDAP サーバーにバインドするときに、`ldapmodify` によって使用されるよう、LDAP バージョン

を指定します。デフォルトの設定では、LDAP V3 接続が確立されます。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。

**-w passwd | ?**

**passwd** を認証用のパスワードとして使用します。 ? を使用してパスワード・プロンプトを生成します。

**-y proxydn**

プロキシ権限オプションのプロキシ ID を設定します。

**-Y** セキュア LDAP 接続 (TLS) を使用します。

**-Z** セキュア SSL 接続を使用して LDAP サーバーと通信します。 i5/OS 上のディレクトリー・サーバーでは、**-Z** を使用して **-K** または **-N** を使用しない場合、ディレクトリー・サービス・クライアント・アプリケーション ID に関連した証明が使用されます。

## 入力フォーマット

ファイルの内容 (あるいは、**-i** フラグがコマンド行で与えられていない場合には標準入力) は LDIF 形式に準拠する必要があります。

## 例

/tmp/entrymods というファイルがあり、このファイルの内容は次のとおりです。

```
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: /tmp/modme.jpeg
-
delete: description
-
```

次のコマンド:

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

は、**Modify Me** 入力のメール属性の内容を値 **modme@student.of.life.edu** で置き換え、**Grand Poobah** のタイトルとファイル **/tmp/modme.jpeg** の内容を **jpegPhoto** として追加し、完全に記述属性を除去します。これらの同じ変更は、以下の古い **ldapmodify** 入力形式:

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

および、次のコマンドを使用して行うことができます。

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

/tmp/newentry というファイルがあり、このファイルの内容は次のとおりです。

```
dn: cn=John Doe, o=University of Higher Learning, c=US
objectClass: person
cn: John Doe
cn: Johnny
sn: Doe
title: the world's most famous mythical person
mail: johndoe@student.of.life.edu
uid: jdoe
```

次のコマンド:

```
ldapadd -i /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。

## Lotus Notes

ファイルから **-i** オプションの使用によって、項目情報が提供されていない場合、**ldapmodify** コマンドは、標準入力から項目が読み取られるまで待ちます。

## 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。

### 関連概念

14 ページの『接尾部 (命名コンテキスト)』

接尾部 (命名コンテキストともいいます) は、ローカルに保持されるディレクトリー階層の最上部の項目を識別する DN です。

Lightweight Directory Access Protocol (LDAP) API

Directory Server API の詳細は、『Lightweight Directory Access Protocol (LDAP) APIs』を参照してください。

288 ページの『Directory Server 構成スキーマ』

この情報では、ディレクトリー情報ツリー (DIT) および `ibmslapd.conf` ファイルの構成に使用する属性を説明します。

### 関連資料

281 ページの『LDAP データ交換形式 (LDIF)』

LDAP データ交換形式は、LDAP オブジェクトおよび LDAP の更新 (追加、変更、削除、DN の変更) をテキスト・フォームで表すための標準テキスト・フォーマットです。LDIF レコードを収めたファイルを、Directory Server 間でデータを転送するのに使用するか、または **ldapadd** や **ldapmodify** のような LDAP ツールで入力として使用することができます。

## ldapdelete

LDAP 項目削除コマンド行ユーティリティー

### 概要

```
ldapdelete [-c] [-C charset] [-d debuglevel][--D binddn] [-f file]
[-G realm] [-h ldaphost] [-i file] [-k] [-K keyfile] [-m mechanism]
[-M] [-n] [-N certificatename] [-O maxops] [-p ldapport]
[-P keyfilepw] [-R] [-s][-U username} [-v] [-V version]
[-w passwd | ?] [-y proxydn][-Y] [-Z] [dn].....
```

## 説明

**ldapdelete** は、`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) へのコマンド行インターフェースです。

**ldapdelete** は LDAP サーバーへの接続を開き、1 つ以上の項目にバインドしてそれらを削除します。1 つ以上の識別名 (DN) 引数が供給されている場合、それらの DN のある項目は削除されます。各 DN はストリング表記の DN です。DN 引数が供給されていない場合、DN のリストは標準入力から、あるいは **-i** フラグが使用されている場合にはファイルから読み取られます。

**ldapdelete** の構文ヘルプを表示するには、以下を入力します。

```
ldapdelete -?
```

## オプション

- c** 連続操作モード。エラーは報告されますが、**ldapdelete** は削除処理を続行します。そうでなければ、デフォルトのアクションでは、エラーの報告後に終了します。
- C charset**  
**ldapdelete** ユーティリティへの入力として提供された DN が、`charset` で指定されたローカル文字セットで表されるように設定します。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 charset** 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 を参照してください。
- d debuglevel**  
LDAP 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。**-m DIGEST-MD5** で使用する場合は、権限 ID を指定するために使用します。これは DN とすることもできるし、あるいは「u:」または「dn:」で始まる `authzId` ストリングとすることもできます。
- f file** ファイル内の各行に対する LDAP 削除を実行しながら、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。
- G realm**  
レルムを指定します。このパラメーターはオプションです。**-m DIGEST-MD5** と一緒に使用すると、その値はバインド中にサーバーに渡されます。
- h ldaphost**  
LDAP サーバーを実行する代替ホストを指定します。
- i file** ファイル内の各行に対する LDAP 削除を実行しながら、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が 1 つずつ含まれていることが必要です。
- k** サーバー管理制御の使用を指定します。
- 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。i5/OS 上の Directory Server では、**-Z** を使用して **-K** または **-N** を使用しない場合、ディレクトリー・サービス・クライアント・アプリケーション ID に関連した証明が使用されます。

**-m** *mechanism*

*mechanism* を使用して、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。ldap\_sasl\_bind\_s() API が使用されます。**-V 2** をセットすると、**-m** パラメーターは無視されます。**-m** を指定しない場合、単純認証が使用されます。以下が有効なメカニズムです。

- CRAM-MD5 - サーバーに送信されるパスワードを保護する。
- EXTERNAL - SSL 認証を使用する。**-Z** が必要。
- GSSAPI - ユーザーの Kerberos 信任状を使用する。
- DIGEST-MD5 - クライアントは username 値をサーバーに送信する必要があります。**-U** が必要。権限 ID を指定するには、**-D** パラメーター (通常、バインド DN) が使用されます。これは DN とすることもできるし、あるいは「u:」または「dn:」で始まる authzId スtring とすることもできます。
- OS400\_PRFTKN - システム・プロジェクト・バックエンド中のユーザーの DN を使用して、ローカル LDAP サーバーに対して現行 i5/OS ユーザーとして認証します。**-D** (バインド DN) および **-w** (パスワード) パラメーターは指定しないでください。

**-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。

**-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 サーバーがサーバー認証だけを実行するように構成されている場合は、クライアント証明書は不要です。LDAP サーバーがクライアントおよびサーバーの認証を実行するように構成されている場合は、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。i5/OS 上のディレクトリー・サーバーでは、**-Z** を使用して **-K** または **-N** を使用しない場合、ディレクトリー・サービス・クライアント・アプリケーション ID に関連した証明が使用されます。

**-O** *maxhops*

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 *maxhops* を指定します。デフォルトのホップ・カウントは 10 です。

**-p** *ldapport*

LDAP サーバーが listen する代替 TCP ポートを指定します。デフォルトの LDAP ポートは 389 です。**-p** 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。

**-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、1 つ以上の秘密鍵を含む場合のあるキー・データベース・ファイル内の暗号化された情報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、パスワードはそのパスワード stash ファイルから取得されるので、**-P** 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。

**-R** 参照を自動的に行わないことを指定します。

- s** このオプションを使用して選択された項目にルートのあるサブツリーを削除します。
- U *username***  
ユーザー名を指定します。**-m DIGEST-MD5** には必要ですが、その他のメカニズムでは無視されま  
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。
- V *version***  
LDAP サーバーにバインドするときに、**ldapdelete** によって使用されるよう、LDAP バージョンを  
指定します。デフォルトの設定では、LDAP V3 接続が確立されます。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。
- w *passwd* | ?**  
**passwd** を認証用のパスワードとして使用します。? を使用してパスワード・プロンプトを生成し  
ます。
- y *proxydn***  
プロキシ権限操作のプロキシ ID を設定します。
- Y** セキュア LDAP 接続 (TLS) を使用します。
- Z** セキュア SSL 接続を使用して LDAP サーバーと通信します。i5/OS 上のディレクトリー・サー  
バーでは、**-Z** を使用して **-K** または **-N** を使用しない場合、ディレクトリー・サービス・クライ  
アント・アプリケーション ID に関連した証明が使用されます。
- dn** 1 つまたは複数の DN 引数を指定します。各 DN はストリング表記の DN です。

## 例

次のコマンドを使用します。

```
ldapdelete -D cn=administrator -w secret "cn=Delete Me, o=University of Life, c=US"
```

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。

## Lotus Notes

DN 引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。

## 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。

### 関連概念

Directory Server API

## ldapexop

LDAP 拡張操作コマンド行ユーティリティー

## 概要

```
ldapexop [-C charset] [-d debuglevel] [-D binddn] [-e] [-G realm]
[-h ldaphost] [-help] [-K keyfile] [-m mechanism] [-N certificatename]
[-p ldapport] [-P keyfilepw] [-?] [-U] [-v] [-w passwd | ?] [-Y] [-Z]
-op {cascrepl | controlqueue | controlrepl | getAttributes |
getusertype | quiesce | readconfig | uniqueattr}
```

## 説明

**ldapexop** ユーティリティーは、ディレクトリー・サーバーにバインドして単一の拡張操作を拡張操作値を構成するデータと共に発行する機能を提供するコマンド行インターフェースです。

**ldapexop** ユーティリティーは、すべての LDAP クライアント・ユーティリティーによって使用される、標準ホスト、ポート、SSL、および認証オプションをサポートします。さらに、オプションのセットが定義され、実行される操作およびそれぞれの拡張操作ごとの引数が指定されます。

**ldapexop** の構文ヘルプを表示するには、以下を入力します。

```
ldapexop -?
```

または

```
ldapexop -help
```

## オプション

**ldapexop** コマンドのオプションは、2 つのカテゴリに分けられています。

1. ディレクトリー・サーバーへの接続方法を指定する一般のオプション。これらのオプションは、オペレーションの特定のオプションの前に指定する必要があります。
2. 実行する拡張操作を示す拡張操作オプション。

### 一般オプション

これらのオプションは、サーバーへの接続方法を指定するもので、**-op** オプションの前に指定する必要があります。

#### **-C** *charset*

**ldapexop** ユーティリティーへの入力として提供された DN が、*charset* で指定されたローカル文字セットで表されるように設定します。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** *charset* 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 を参照してください。

#### **-d** *debuglevel*

LDAP 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。**-m** DIGEST-MD5 で使用する場合は、権限 ID を指定するために使用します。これは DN とすることもできるし、あるいは「u:」または「dn:」で始まる *authzId* ストリングとすることもできます。

**-e** LDAP ライブラリーのバージョン情報を表示し、それから終了します。

**-G** レルムを指定します。このパラメーターはオプションです。**-m** DIGEST-MD5 と一緒に使用すると、その値はバインド中にサーバーに渡されます。

#### **-h** *ldaphost*

LDAP サーバーを実行する代替ホストを指定します。

**-help** コマンド構文および使用法の情報を表示します。

**-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、システム・キー・データベースが使用されます。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。i5/OS 上のディレクトリー・サーバーでは、**-Z** を使用して **-K** または **-N** を使用しない場合、ディレクトリー・サービス・クライアント・アプリケーション ID に関連した証明が使用されます。

**-m** *mechanism*

*mechanism* を使用して、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。

ldap\_sasl\_bind\_s() API が使用されます。**-V 2** をセットすると、**-m** パラメーターは無視されません。**-m** を指定しない場合、単純認証が使用されます。以下が有効なメカニズムです。

- CRAM-MD5 - サーバーに送信されるパスワードを保護する。
- EXTERNAL - SSL 認証を使用する。**-Z** が必要。
- GSSAPI - ユーザーの Kerberos 信任状を使用する。
- DIGEST-MD5 - クライアントは username 値をサーバーに送信する必要があります。**-U** が必要。権限 ID を指定するには、**-D** パラメーター (通常、バインド DN) が使用されます。これは DN とすることもできるし、あるいは「u:」または「dn:」で始まる authzId スtring とすることもできます。
- OS400\_PRFTKN - システム・プロジェクト・バックエンド中のユーザーの DN を使用して、ローカル LDAP サーバーに対して現行 i5/OS ユーザーとして認証します。**-D** (バインド DN) および **-w** (パスワード) パラメーターは指定しないでください。

**-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 サーバーがサーバー認証だけを実行するように構成されている場合は、クライアント証明書は不要です。LDAP サーバーがクライアントおよびサーバーの認証を実行するように構成されている場合は、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。i5/OS 上のディレクトリー・サーバーでは、**-Z** を使用して **-K** または **-N** を使用しない場合、ディレクトリー・サービス・クライアント・アプリケーション ID に関連した証明が使用されます。

**-p** *ldapport*

LDAP サーバーが listen する代替 TCP ポートを指定します。デフォルトの LDAP ポートは 389 です。**-p** 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。

**-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、1 つ以上の秘密鍵を含む場合のあるキー・データベース・ファイル内の暗号化された情報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

はそのパスワード `stash` ファイルから取得されるので、**-P** 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。

- ?** コマンド構文および使用法の情報を表示します。
- U** ユーザー名を指定します。**-m DIGEST-MD5** には必要ですが、その他のメカニズムでは無視されません。
- 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。
- w passwd | ?**  
*passwd* を認証用のパスワードとして使用します。 `?` を使用してパスワード・プロンプトを生成します。
- Y** セキュア LDAP 接続 (TLS) を使用します。
- Z** セキュア SSL 接続を使用して LDAP サーバーと通信します。 i5/OS 上のディレクトリー・サーバーでは、**-Z** を使用して **-K** または **-N** を使用しない場合、ディレクトリー・サービス・クライアント・アプリケーション ID に関連した証明が使用されます。

## 拡張操作オプション

**-op extended-op** オプションは、実行する拡張操作を示します。拡張操作は、以下のいずれかの値です。

- **acctstatus**: アカウント状況拡張操作。指定されたアカウントの状況を表示します。  
`ldapexop -op acctstatus -d <DN>`  
`-d DN`  
取り出されるアカウント状況を持った項目の DN を識別します。  
アカウント状況は、オープン、ロック済み、または期限切れになります。
- **cascrepl**: カスケード制御複製拡張操作。要求されたアクションが指定されたサーバーに適用され、またおよび該当するサブツリーのすべてのレプリカへも受け渡されます。これらに転送レプリカがあれば、それらのレプリカにも拡張操作がパスされます。操作はレプリケーション・トポロジーの全体にわたってカスケードします。

### **-action quiesce | unquiesce | replnow | wait**

これは実行されるアクションを指定する必須属性です。

#### **quiesce**

複製を除き、その後の更新は許可されません。

#### **unquiesce**

通常の操作を再開し、クライアント更新は受け入れられます。

#### **replnow**

スケジュールにかかわらず、キューに入れられたすべての変更をすべてのレプリカ・サーバーへ、可能な限り早く複製します。

#### **wait**

すべての変更がすべてのレプリカに複製されるまで待ちます。

### **-rc contextDn**

これはサブツリーのルートを指定する必須属性です。

### **-timeout secs**

これはオプション属性で、これがある場合にはタイムアウト期間を秒で指定します。ない場合、または 0 の場合には、操作は無限に待機します。

例:

```
ldapexop -op cascrepl -action -quiesce -rc "o=acme,c=us" -timeout 60
```

| • **clearlog | getlogsize | readlog -log ...**

| この 3 つの操作は、次のような新規のログ・ファイルをサポートします。

| LostAndFound

| この操作は、i5/OS Directory Server (V6R1 およびそれ以降) で使用できますが、次のように一部のログ・ファイルのみがサポートされます。

| LostAndFound – 複製の競合のログ・ファイル。

- **controlqueue:** 制御待ち行複製拡張操作。この操作により、複製障害のため実行されずにキューに入れられた複製変更のリストから、保留の変更を削除または除去することができます。この操作は、レプリカ・データを手動で修正する際に便利です。そのときに、この操作を使用してキューに入れられた障害をスキップします。

**-skip all | change-id**

これは必須属性です。

- **-skip all** はこの契約ではすべての保留変更をスキップすることを示します。
- **change-id** は、単一の変更がスキップされることを示します。サーバーがこの変更を現時点で複製していない場合、この要求は失敗します。

**-ra agreementDn**

これは、複製合意の DN を指定する必須属性です。

例:

```
ldapexop -op controlqueue -skip all -ra "cn=server3,
ibm-replicaSubentry=master1-id,ibm-replicaGroup=default,
o=acme,c=us"
```

```
ldapexop -op controlqueue -skip 2185 -ra "cn=server3,
ibm-replicaSubentry=master1-id,ibm-replicaGroup=default,
o=acme,c=us"
```

- **controlrepl:** 制御複製拡張操作

**-action suspend | resume | replnow**

これは実行されるアクションを指定する必須属性です。

**-rc contextDn | -ra agreementDn**

**-rc contextDn** は複製コンテキストの DN です。アクションはこのコンテキストのすべての契約に対して実行されます。**-ra agreementDn** は複製契約の DN です。アクションは指定された複製合意に対して実行されます。

例:

```
ldapexop -op controlrepl -action suspend -ra "cn=server3,
ibm-replicaSubentry=master1-id,ibm-replicaGroup=default,
o=acme,c=us"
```

| • **controlreplerr**

| controlreplerr 拡張操作では、i5/OS V6R1 (または IBM Tivoli Directory Server v6.0) またはそれ以降のサーバー上で、複製エラー・テーブルを管理することができます。オプションは次のとおりです。

| ldapexop -op controlreplerr -show <failure\_ID> -ra <agreementDN>

| これを使用して、複製エラー・テーブル内の項目を表示することができます。

| **<failure\_ID>**

| 障害の ID です。すべての項目を表示するには、0 を指定します。

| **<agreementDN>**

| 項目が関係付けられている複製合意。

| `ldapexop -op controlreplerr -delete <failure_ID> -ra <agreementDN>`

| これを使用して、複製エラー・テーブルから項目を削除することができます。

| **<failure\_ID>**

| 障害の ID です。すべての項目を表示するには、0 を指定します。

| **<agreementDN>**

| 項目が関係付けられている複製合意。

| `ldapexop -op controlreplerr -retry <failure_ID> -ra <agreementDN>`

| これを使用して、複製エラー・テーブル内の項目を再試行することができます。

| **<failure\_ID>**

| 障害の ID です。すべての項目を表示するには、0 を指定します。

| **<agreementDN>**

| 項目が関係付けられている複製合意。

#### | • **evaluateGroups**

| 次のように、新規の `evaluateGroups` 操作が `ldapexop` ユーティリティーでサポートされています。

| `ldapexop -op evaluateGroups -d userDN -a <list of attribute and value pairs each separated by a space>`

| これは、指定した `userDN` の所属先のグループのリストを表示します。

| "-a" オプションが使用されているのは、項目の属性値を指定するためと、その項目に一致する動的グループを取り出すためです。"-a" オプションを指定しないと、静的グループのみに関する要求がサーバーに送信されます。この拡張操作は、サーバー上に存在しない `userDN` (たとえば、リモート・グループ・メンバーを表す `userDN`) に関するグループ・メンバーシップ情報を取り出すために使用します。その `userDN` を擁するサーバーのグループ・メンバーシップをリストするには、`ibm-allGroups` 運用属性を使用する必要があります。

| **例:**

| 項目の `departmentnumber` および `objectclass` 属性値に基づいて、項目 `uid=sample,cn=users,o=ibm` のグループ・メンバーシップを評価するには、次のようにします。

| `ldapexop -op evaluateGroups -d uid=sample,cn=users,o=ibm -a objectclass=person departmentnumber=abc`

| **注:** 通常、この拡張操作では、対象となる項目のすべての属性値が提供されることになります。

#### | • **getattributes -attrType<type> -matches bool<value>**

| **-attrType {operational | language\_tag | attribute\_cache | unique | configuration}**

| これは要求している属性のタイプを指定する必須属性です。

**-matches bool {true | false}**

戻された属性のリストが **-attrType<** オプションで指定された属性タイプと一致しているかどうかを指定します。

**例:**

```
ldapexop -op getattributes -attrType unique -matches bool true
```

固有属性として指定されたすべての属性のリストを戻します。

```
ldapexop -op getattributes -attrType unique -matches bool false
```

固有属性として指定されなかったすべての属性のリストを戻します。

• **getusertype: request user type extended operation**

この拡張操作は、バインドされた DN に基づいてユーザー・タイプを戻します。

**例:**

```
ldapexop - D <AdminDN> -w <Adminpw> -op getusertype
```

は以下を戻します。

```
User : root_administrator
Role(s) : server_config_administrator directory_administrator
```

```
| User : global_admin_group_member
| Role(s) : directory_administrator
```

• **quiesce: quiesce** または **unquiesce** サブツリー複製拡張操作

**-rc contextDn**

これは、静止または静止解除される複製コンテキスト (サブツリー) の DN を指定する必須属性です。

**-end** これはオプション属性で、これがある場合にはサブツリーの静止解除を指定します。指定されていない場合、デフォルトでサブツリーは静止されます。

**例:**

```
ldapexop -op quiesce -rc "o=acme,c=us"
```

```
ldapexop -op quiesce -end -rc "o=ibm,c=us"
```

• **readconfig: 構成ファイル再読み取り拡張操作**

**-scope entire | single<entry DN><attribute>**

これは必須属性です。

- **entire** は構成ファイル全体を再読み取りすることを示します。
- **single** は、指定された単一記入項目および属性を読み取ることを意味します。

**例:**

```
ldapexop -op readconfig -scope entire
```

```
ldapexop -op readconfig -scope single "cn=configuration" ibm-slapdAdminPW
```

**注:** 以下の入力で、

- <sup>1</sup> は readconfig の後に即時有効になります
- <sup>2</sup> でマークされたものは新規の操作で有効になります



- <sup>3</sup> でマークされたものはパスワードが変更されるとすぐに有効になります (readconfig は必要ありません)
- <sup>4</sup> でマークされたものは、i5/OS 上のコマンド行ユーティリティーにサポートされますが、i5/OS のディレクトリー・サーバーではサポートされません

```
cn=Configuration
ibm-slapdadmin2
ibm-slapdadminpw2, 3
ibm-slapderrorlog1, 4
ibm-slapdpwncryption1
ibm-slapdsizelimit1
ibm-slapdsysloglevel1, 4
ibm-slapdtimeout1
```

```
cn=Front End, cn=Configuration
ibm-slapdaclcache1
ibm-slapdaclcachesize1
ibm-slapdentrycachesize1
ibm-slapdfiltercachebypasslimit1
ibm-slapdfiltercachesize1
ibm-slapdidletimeout1
```

```
cn=Event Notification, cn=Configuration
ibm-slapdmaxeventsperconnection2
ibm-slapdmaxeventstotal2
```

```
cn=Transaction, cn=Configuration
ibm-slapdmaxnumoftransactions2
ibm-slapdmaxoppertransaction2
ibm-slapdmaxtimelimitoftransactions2
```

```
cn=ConfigDB, cn=Config Backends, cn=IBM SecureWay, cn=Schemas, cn=Configuration
ibm-slapdreadonly2
```

```
cn=Directory, cn=RDBM Backends, cn=IBM SecureWay, cn=Schemas, cn=Configuration
ibm-slapdbulkloadererrors1, 4
ibm-slapdclierrors1, 4
ibm-slapdpagedresallownonadmin2
ibm-slapdpagedreslimit2
ibm-slapdpagesizelimit2
ibm-slapdreadonly2
ibm-slapdsortkeylimit2
ibm-slapdsortsrchallownonadmin2
ibm-slapdsuffix2
```

| • **repltopology -rc [options]:**

| repltopology 拡張操作を使用するのは、サプライヤー・サーバー上のトポロジーに対して、コンシューマー・サーバー上の複製トポロジー情報を突き合わせる場合です。

| ldapexop -op repltopology -rc [-timeout secs] [-ra agreementDn]

| ここで

| **-rc contextDn**

| これはサブツリーのルートを指定する必須属性です。

| **-timeout secs**

| これはオプション属性で、これがある場合にはタイムアウト期間を秒で指定します。ない場合、または 0 の場合には、操作は無限に待機します。

## **-ra agreementDn**

**-ra agreementDn** は複製契約の DN です。アクションは指定された複製合意に対して実行されます。**-ra** オプションを指定しないと、コンテキストのもとで定義されているすべての複製契約に対してアクションが実行されます。

### 例:

```
ldapexop -op repltopology -rc "o=acme,c=us" -ra "cn=server3,
 ibm-replicaSubentry=master1-id,ibm-replicaGroup=default,
 o=acme,c=us"-timeout 60
```

サプライヤー・サーバーは、構成済みの複製信任状を使用して、コンシューマー・サーバーにバインドします。サプライヤー DN には、コンシューマー (レプリカ) サーバーの構成サプライヤーに接尾部を追加する権限が付帯しています。これは、複製トポロジー拡張操作の一環としてサプライヤー・サーバーで使用されて、欠落している接尾部がコンシューマー・サーバーに追加されます。contextDN 項目がまだ存在していない接尾部の場合、サプライヤー DN には、新規の複製済みサブツリーを作成する権限も与えられます。contextDN 項目がすでに存在する場合、それは、複製済みサブツリーのルートとしてすでに定義済みである必要があります。つまり、ibm-replicationcontext オブジェクト・クラスを持っていないければなりません。

- **unbind {-dn<specificDN> | -ip<sourceIP> | -dn<specificDN> -ip<sourceIP> | all}:**

は DN、IP、DN/IP に基づいて接続を切断するか、あるいはすべての接続を切断します。何の操作もないすべての接続および作業待ち行列上に操作のある接続をすべて即時終了します。現在、その接続で作業が行われている場合は、その 1 つの作業が完了すると、接続は即時終了されます。

#### **-dn<specificDN>**

DN のみによる接続を終了するための要求を出します。この要求は、指定された DN を基にバインドされたすべての接続を除去する結果となります。

#### **-ip<sourceIP>**

IP のみによる接続を終了するための要求を出します。この要求は、指定された IP ソースからのすべての接続を除去する結果となります。

#### **-dn<specificDN> -ip<sourceIP>**

DN/IP の対によって決定された接続を終了するための要求を出します。この要求は、指定された DN を基にバインドされ、指定された IP ソースからのすべての接続を除去する結果となります。

#### **-all**

すべての接続を終了するための要求を出します。この要求は、この要求を発信した場所からの接続を除いて、すべての接続を除去する結果となります。この属性は **-D** または **-IP** の属性と一緒に使用できません。

### 例:

```
ldapexop -op unbind -dn cn=john
ldapexop -op unbind -ip 9.182.173.43
ldapexop -op unbind -dn cn=john -ip 9.182.173.43
ldapexop -op unbind -all
```

- **uniqueattr -a <attributeType>:** 特定の属性の非固有のすべての値を識別します。

#### **-a <attribute>**

矛盾する値をすべてリストする属性を指定します。

注: 2 進数属性、操作属性、構成属性、および objectclass 属性の複製値は表示されません。固有属性では、これらの属性はサポートされる拡張操作ではありません。

## 例:

```
ldapexop -op uniqueattr -a "uid"
```

この拡張操作では、次の行が「cn=Directory,cn=RDBM Backends,cn=IBM Directory,cn=schema,cn=Configuration」項目の下の構成ファイルに追加されます。

```
ibm-slapdPlugin: extendedop /QSYS.LIB/QGLDRDBM.SRVPGM initUniqueAttr
```

## 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。

### 関連概念

#### Directory Server API

##### 49 ページの『複製エラー・テーブル』

後でリカバリするために、複製エラー・テーブルが失敗した更新を記録します。複製が開始すると、各複製契約ごとにログ記録された障害数がカウントされます。更新が結果として失敗すると、このカウントが増え、新しい項目がテーブルに追加されます。

### 関連タスク

##### 185 ページの『遺失物取り扱いログ・ファイルの表示』

複製の遺失物取り扱いログ・ファイルを表示するには、IBM Tivoli Directory Server の Web 管理ツールを使用するか、または ldapexop ユーティリティのログ・ファイル・オプションを使用するか、あるいは、ファイルを直接表示します。

## ldapmodrdn

LDAP modify-entry RDN™ コマンド行ユーティリティ

### 概要

```
ldapmodrdn [-c] [-C charset] [-d debuglevel][-D binddn]
[-f file][-G realm] [-h ldaphost] [-i file] [-k] [-K keyfile]
[-m mechanism] [-M] [-n] [-N certificatename] [-O hopcount]
[-p ldapport] [-P keyfilepw] [-r] [-R] [-U username] [-v] [-V version]
[-w passwd | ?] [-y proxydn] [-Y] [-Z] [dn newrdn | [-i file]]
```

### 説明

ldapmodrdn は、ldap\_rename アプリケーション・プログラミング・インターフェース (API) へのコマンド行インターフェースです。

ldapmodrdn は LDAP サーバーへの接続を開き、項目にバインドし、その移動またはその名前変更を行います。項目の情報は、標準入力から読み取られるか、-f オプションの使用によってファイルから読み取られるか、コマンド行の DN と RDN の対から読み取られます。項目を移動する -s オプションを使用すると、その -s オプションは、コマンドの実行対象のすべての項目に適用されます。

ldapmodrdn の構文ヘルプを表示するには、以下を入力します。

```
ldapmodrdn -?
```

### オプション

-c 連続操作モード。エラーは報告されますが、ldapmodrdn は変更処理を続行します。そうでなければ、デフォルトのアクションでは、エラーの報告後に終了します。

**-C charset**

**ldapmodrdn** ユーティリティーへの入力として提供された文字列が、**charset** で指定されたローカル文字セットで表されるように設定します。入力文字列のコード・ページがジョブのコード・ページ値と異なる場合には、**-C charset** オプションを使用します。サポートされる **charset** 値を調べるには `ldap_set_iconv_local_charset()` API を参照してください。**charset** のサポートされる値は、バージョン 1 LDIF ファイルでオプションとして定義されている **charset** タグのためにサポートされている値と同じであることを注意してください。

**-d debuglevel**

LDAP 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** は文字列表記の DN です。**-m DIGEST-MD5** で使用する場合は、権限 ID を指定するために使用します。これは DN とすることもできるし、あるいは「u:」または「dn:」で始まる **authzId** 文字列とすることもできます。

**-f file** 標準入力またはコマンド行 (**dn** および新規の **rdn** の指定による) 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。また、標準入力をファイル (< file) から提供することもできます。

**-G realm**

レルムを指定します。このパラメーターはオプションです。**-m DIGEST-MD5** と一緒に使用すると、その値はバインド中にサーバーに渡されます。

**-h ldaphost**

LDAP サーバーを実行する代替ホストを指定します。

**-i file** 標準入力またはコマンド行 (**rdn** および **newrdn** を指定) からではなく、ファイルから項目の変更情報を読み取ります。標準入力はファイル ("< file") から提供されます。

**-k** サーバー管理制御の使用を指定します。

**-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。i5/OS 上のディレクトリー・サーバーでは、**-Z** を使用して **-K** または **-N** を使用しない場合、ディレクトリー・サービス・クライアント・アプリケーション ID に関連した証明が使用されます。

**-m mechanism**

**mechanism** を使用して、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。`ldap_sasl_bind_s()` API が使用されます。**-V 2** をセットすると、**-m** パラメーターは無視されます。**-m** を指定しない場合、単純認証が使用されます。以下が有効なメカニズムです。

- CRAM-MD5 - サーバーに送信されるパスワードを保護する。
- EXTERNAL - SSL 認証を使用する。**-Z** が必要。
- GSSAPI - ユーザーの Kerberos 信任状を使用する。

- DIGEST-MD5 - クライアントは `username` 値をサーバーに送信する必要があります。-U が必要。権限 ID を指定するには、-D パラメーター (通常、バインド DN) が使用されます。これは DN とすることもできるし、あるいは「u:」または「dn:」で始まる `authzId` ストリングとすることもできます。
- OS400\_PRFTKN - システム・プロジェクト・バックエンド中のユーザーの DN を使用して、ローカル LDAP サーバーに対して現行 i5/OS ユーザーとして認証します。-D (バインド DN) および -w (パスワード) パラメーターは指定しないでください。

**-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。

**-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 サーバーがサーバー認証だけを実行するように構成されている場合は、クライアント証明書は不要です。LDAP サーバーがクライアントおよびサーバーの認証を実行するように構成されている場合は、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。i5/OS 上のディレクトリー・サーバーでは、-Z を使用して -K または -N を使用しない場合、ディレクトリー・サービス・クライアント・アプリケーション ID に関連した証明が使用されます。

**-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。

**-p** *ldapport*

LDAP サーバーが `listen` する代替 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。

**-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 (1 つ以上の秘密鍵を含む場合がある) 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、パスワードはそのパスワード `stash` ファイルから取得されるので、-P 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。

**-r** 項目から、古い RDN 値を除去します。デフォルトのアクションでは古い値が保持されます。

**-R** 参照を自動的に行わないことを指定します。

| **-s** *newSuperior*

| 名前変更後の項目の再配置先の新しい上位項目の DN を指定します。newSuperior 引数は、ゼロの長さのストリング (-s "") でかまいません。

| 注: 新規の superior オプションは、V6R1 (ITDS v6.0) より前のリリースのサーバーへの接続時にはサポートされません。現在、このオプションは、リーフ項目に対してのみ指定できます。

**-U** *username*

ユーザー名を指定します。-m DIGEST-MD5 には必要ですが、その他のメカニズムでは無視されます。

**-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。

**-V version**

LDAP サーバーにバインドするときに、**ldapmodrdn** によって使用されるよう、LDAP バージョンを指定します。デフォルトの設定では、LDAP V3 接続が確立されます。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。**ldapmodrdn** などのアプリケーションでは、`ldap_open` の代わりに `ldap_init` が使用され、LDAP V3 が優先プロトコルとして選択されます。

**-w passwd | ?**

**passwd** を認証用のパスワードとして使用します。 **?** を使用してパスワード・プロンプトを生成します。

**-y proxydn**

プロキシ権限操作のプロキシ ID を設定します。

**-Y** セキュア LDAP 接続 (TLS) を使用します。

**-Z** セキュア SSL 接続を使用して LDAP サーバーと通信します。 i5/OS 上のディレクトリー・サーバーでは、**-Z** を使用して **-K** または **-N** を使用しない場合、ディレクトリー・サービス・クライアント・アプリケーション ID に関連した証明が使用されます。

**dn newrdn**

詳しくは、以下の『dn newrdn の入力形式』のセクションを参照してください。

## dn newrdn の入力フォーマット

コマンド行引数 **dn** および **newrdn** を指定した場合は、DN で指定された項目の RDN である **dn** が、**newrdn** で置き換えられます。これらの引数を指定しない場合は、ファイルの内容 (または、**-i** フラグを指定していない場合は標準入力) 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)

1 行以上のブランク行でそれぞれの DN と RDN ペアを分離する場合があります。

## 例

/tmp/entrymods というファイルがあり、このファイルの内容は次のとおりです。

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

次のコマンド:

```
ldapmodrdn -r -i /tmp/entrymods
```

は、Modify Me 項目の RDN を、Modify Me から The New Me に変更し、古い cn、Modify Me は除去されます。

## Lotus Notes

**-i** オプションを使用してファイルから (またはコマンド行ペア **dn** および **rdn** から) 入力情報が供給されていない場合は、**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。

## 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。

### 関連概念

Directory Server API

10 ページの『識別名 (DN)』

ディレクトリー内のすべての項目には、識別名 (DN) があります。DN は、ディレクトリー内の項目を一意的に識別する名前です。DN の最初のコンポーネントは、相対識別名 (RDN) と呼ばれています。

## ldapsearch

LDAP 検索コマンド行ユーティリティ

### 概要

```
ldapsearch [-a deref] [-A] [-b searchbase] [-B] [-C charset] [-d debuglevel]
[-D binddn] [-e] [-f file] [-F sep] [-G realm] [-h ldaphost] [-i file] [-K keyfile]
[-l timelimit] [-L] [-m mechanism] [-M] [-n] [-N certificatename]
[-o attr_type] [-O maxhops] [-p ldapport] [-P keyfilepw] [-q pagesize]
[-R] [-s scope] [-t] [-T seconds] [-U username] [-v] [-V version]
[-w passwd | ?] [-z sizelimit] [-y proxydn] [-Y] [-Z]
filter [-9 p] [-9 s] [attrs...]
```

### 説明

**ldapsearch** 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) へのコマンド行インターフェースです。

**ldapsearch** は LDAP サーバーへの接続を開き、バインドし、フィルターを使用して検索を行います。フィルターは、LDAP フィルターのストリング表記に準拠している必要があります (詳しくは、Directory Server APIs の `ldap_search` を参照してください)。

**ldapsearch** により 1 つまたは複数の項目が見つかり、`attrs` で指定された属性がリトリブされ、項目および値は標準出力に書き込まれます。`attrs` がリストされていない場合、すべての属性が戻されます。

**ldapsearch** の構文ヘルプを表示するには、`ldapsearch -?` を入力します。

### オプション

#### **-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。

**-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 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** を指定しない場合、ユーティリティは、`LDAP_BASEDN` 環境変数で `searchbase` の定義を調べます。どちらも設定されていない場合、デフォルト・ベースは "" に設定されます。

**-B** 非 ASCII 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** オプションを指定すると暗黙的に指定されます。

#### **-C charset**

`ldapsearch` ユーティリティーへの入力として提供される文字列が、ローカル文字セット (charset によって指定) で表されるように指定します。文字列の入力には、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セットに変換します。入力文字列のコード・ページがジョブのコード・ページ値と異なる場合には、**-C charset** 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 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 表示で保持されるか、印刷不能文字が検出される場合には、そのデータの base-64 エンコード表示で示されます。これは、標準の LDIF ファイルには文字列・データの UTF-8 (または、base-64 エンコードの UTF-8) 表示のみが含まれているためです。charset のサポートされる値は、バージョン 1 LDIF ファイルでオプションとして定義されている charset タグのためにサポートされている値と同じであることを注意してください。

#### **-d debuglevel**

LDAP 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` は文字列表記の DN です (LDAP 識別名を参照)。`-m DIGEST-MD5` で使用する場合は、権限 ID を指定するために使用します。これは DN とすることもできるし、あるいは「u:」または「dn:」で始まる `authzId` 文字列とすることもできます。

**-e** LDAP ライブラリーのバージョン情報を表示し、終了します。

**-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。

#### **-G realm**

レルムを指定します。このパラメーターはオプションです。`-m DIGEST-MD5` と一緒に使用すると、その値はバインド中にサーバーに渡されます。

#### **-h ldaphost**

LDAP サーバーを実行する代替ホストを指定します。

**-i 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。この場合、コマンド行で与えられるフィルターがパターンとして扱われ、そこで最初に現れる % がファイルからの行で置き換えられます。ファイルが単一の "-" 文字である場合、行は標準入力から読み取られます。

#### **-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。i5/OS 上のディレクトリー・サーバーでは、**-Z** を使用して **-K** または **-N** を使用しない場合、ディレクトリー・サービス・クライアント・アプリケーション ID に関連した証明が使用されます。

#### **-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。

- 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 mechanism**

**mechanism** を使用して、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。

ldap\_sasl\_bind\_s() API が使用されます。**-V 2** をセットすると、**-m** パラメーターは無視されます。**-m** を指定しない場合、単純認証が使用されます。以下が有効なメカニズムです。

- CRAM-MD5 - サーバーに送信されるパスワードを保護する。
- EXTERNAL - SSL 認証を使用する。**-Z** が必要。
- GSSAPI - ユーザーの Kerberos 信任状を使用する。
- DIGEST-MD5 - クライアントは username 値をサーバーに送信する必要があります。**-U** が必要。権限 ID を指定するには、**-D** パラメーター (通常、バインド DN) が使用されます。これは DN とすることもできるし、あるいは「u:」または「dn:」で始まる authzId スtring とすることもできます。
- OS400\_PRFTKN - システム・プロジェクト・バックエンド中のユーザーの DN を使用して、ローカル LDAP サーバーに対して現行 i5/OS ユーザーとして認証します。**-D** (バインド DN) および **-w** (パスワード) パラメーターは指定しないでください。

- 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。

#### **-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。

注: LDAP サーバーがサーバー認証だけを実行するように構成されている場合は、クライアント証明書は不要です。LDAP サーバーがクライアントおよびサーバーの認証を実行するように構成されている場合は、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。

i5/OS 上のディレクトリー・サーバーでは、**-Z** を使用して **-K** または **-N** を使用しない場合、ディレクトリー・サービス・クライアント・アプリケーション ID に関連した証明が使用されます。

#### **-o attr\_type**

検索結果のソート基準として使用する属性を指定するには、**-o** (order) パラメーターを使用します。複数の **-o** パラメーターを使用してさらにソート順序を定義できます。以下の例では、検索結果はまず姓 (sn) で、それから名前でソートされ、名前 (givenname) は接頭部の負符号 (-) で指定されているように逆 (降順) の順序でソートされます。

```
-o sn -o -givenname
```

したがって、ソート・パラメーターの構文は以下ようになります。

```
[-]<attribute name>[:<matching rule OID>]
```

ここで

- attribute name はそれでソートする属性の名前です。
- matching rule OID はソートに使用するマッチング規則のオプション OID です。マッチング規則の OID 属性は、ディレクトリー・サーバーではサポートされていませんが、他の LDAP サーバーはこの属性をサポートする場合があります。
- 負符号 (-) は、結果が逆順にソートされることを示します。
- 重大性は、常に重大です。

ldapsearch 操作はデフォルトでは、戻された結果をソートしません。

#### **-O maxhops**

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 maxhops を指定します。デフォルトのホップ・カウントは 10 です。

#### **-p ldapport**

LDAP サーバーが listen する代替 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。

#### **-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 (1 つ以上の秘密鍵を含む場合がある) 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、パスワードはそのパスワード stash ファイルから取得されるので、**-P** 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。

#### **-q pagesize**

検索結果のページングを指定するには、2 つのパラメーター: -q (照会ページ・サイズ)、および -T (検索の間の時間 (秒)) を使用できます。以下の例では、検索結果はその検索に対するすべての結果が戻されるまで、15 秒ごとに一度に 1 ページ (25 項目) を戻します。ldapsearch クライアントはそれぞれの結果のページングの要求ごとに、検索操作の期間を通してすべての接続の継続を扱います。

これらのパラメーターはクライアントに限定リソースがあるとき、またクライアントが低帯域幅の接続で CAN されているときに便利です。一般に、これにより、検索要求からデータが戻される速度をコントロールすることができます。すべての結果を一度に受信する代わりに、(ページごとに) 幾つかの項目で受信することができます。さらに、それぞれのページ要求間の遅延の継続時間を制御してクライアントに結果をプロセスする時間を与えることができます。

```
-q 25 -T 15
```

-v (冗長) パラメーターを指定した場合、たとえば、**30 total entries have been returned. (合計 30 の項目が戻されました。)** のように、ldapsearch は、サーバーから戻されるそれぞれの項目のページごとに、それまで幾つの項目が戻されたかをリストします。

複数の -q パラメーターが使用可能になるので、単一の検索操作中を通して、異なるページ・サイズを指定することができます。以下の例では、最初のページは 15 項目、2 番目のページは 20 項目、そして 3 番目のパラメーターがページングされた結果/検索操作を終了します。

```
-q 15 -q 20 -q 0
```

以下の例では、最初のページは 15 項目、残りのすべてのページは 20 項目で、最後の指定 **-q** 値で検索操作が完了するまで続きます。

```
-q 15 -q 20
```

ldapsearch 操作は、デフォルトでは、単一の要求ですべての項目を戻します。デフォルトの ldapsearch 操作では、ページングは行われません。

**-R** 参照を自動的に行わないことを指定します。

**-s scope**

検索の範囲を指定します。scope は、base、one、または 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。

**-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 などの非 ASCII 値を扱うときに便利です。

**-T seconds**

検索の間隔 (秒)。**-T** オプションは **-q** オプションが指定されている場合にのみサポートされます。

**-U username**

ユーザー名を指定します。**-m DIGEST-MD5** には必要ですが、その他のメカニズムでは無視されません。

**-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。

**-V** LDAP サーバーにバインドするときに、ldapmodify によって使用されるよう、LDAP バージョンを指定します。デフォルトの設定では、LDAP V3 接続が確立されます。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。ldapmodify などのアプリケーションでは、ldap\_open の代わりに ldap\_init が使用され、LDAP V3 が優先プロトコルとして選択されます。

**-w passwd | ?**

**passwd** を認証用のパスワードとして使用します。? を使用してパスワード・プロンプトを生成します。

**-y proxydn**

プロキシ権限操作のプロキシ ID を設定します。

**-Y** セキュア LDAP 接続 (TLS) を使用します。

**-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。

**-Z** セキュア SSL 接続を使用して LDAP サーバーと通信します。i5/OS 上のディレクトリー・サーバーでは、**-Z** を使用して **-K** または **-N** を使用しない場合、ディレクトリー・サービス・クライアント・アプリケーション ID に関連した証明が使用されます。

**フィルター**

検索に適用するフィルターのストリング表記を指定します。簡易フィルターは、attributetype=attributevalue として指定できます。より複雑なフィルターは、以下のバックス正規形式 (BNF) に従って接頭表記法を使用して指定できます。

```
<filter> ::= '(' <filtercomp> ')'
<filtercomp> ::= <and> | <or> | <not> | <simple>
<and> ::= '&' <filterlist>
<or> ::= '|' <filterlist>
<not> ::= '!' <filter>
<filterlist> ::= <filter> | <filter> <filterlist>
<simple> ::= <attributetype> <filtertype>
<attributevalue>
<filtertype> ::= '=' | '^=' | '<=' | '>='
```

'=' 構成は、近似マッチングの指定のために使用されています。 <attributetype> および <attributevalue> の表記については、RFC 2252, LDAP V3 Attribute Syntax Definitions に説明されています。さらに、filtertype が '=' の場合、<attributevalue> は、属性存在テストを行うときは単一の \* でかまいませんが、サブストリング・マッチングを行うときには、テキストとアスタリスク (\*) がその中に散在していてもかまいません。

たとえば、フィルター "mail=" はメール属性のある項目を検出します。フィルター "mail=\*@student.of.life.edu" では、指定されたストリングで終わるメール属性のある項目を検出します。フィルターに括弧を書き込むには、エスケープ文字として、円記号 (¥) 文字を入れてください。

注: Bob とアスタリスク ( \* ) の間にスペースがある "cn=Bob \*" などのフィルターでは、IBM Directory 中の "Bob Carter" はマッチングしますが、"Bobby Carter" はマッチングしません。"Bob" とワイルドカード文字 ( \* ) の間のスペースは、フィルターを使用した検索の結果に影響します。

許容されるフィルターに関する完全な説明は、"RFC 2254, A String Representation of LDAP Search Filters" を参照してください。

## 出力フォーマット

1 つ以上の項目が検出された場合、各項目は次の形式で標準出力に書き込まれます。

識別名 (DN)

attributename=value

attributename=value

attributename=value

複数の項目は、それぞれ 1 つの空白行で区切られます。分離文字の指定に **-F** オプションが使用されている場合、空白行が '=' 文字の代わりに使用されます。**-t** オプションを指定した場合は、実際の値の代わりに一時ファイルの名前が使用されます。**-A** オプションが与えられている場合には、"attributename" の部分のみが書き込まれます。

## 例

次のコマンドを使用します。

```
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)。commonName および telephoneNumber の値が検索され、標準出力にプリントされます。2 つの項目が検出された場合、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
```

次のコマンド:

```
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。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。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
```

次のコマンド:

```
ldapsearch -L -s one -b "c=US" "o=university*" o description
```

は、university で始まる organizationName を持つすべての組織を検出する 1 レベル検索を行います。検索結果は LDIF 形式 (『LDAP データ交換形式』を参照してください。) で表示されます。organizationName と記述属性値が検索され、標準出力にプリントされ、以下のような出力になります。

```
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: UF1
description: Shaper of young minds
```

次のコマンド:

```
ldapsearch -b "c=US" -o ibm-slapdDN "objectclass=person" ibm-slapdDN
```

は、c=US レベルですべての人々を検出するサブツリー・レベルの検索を行います。この特別な属性 (ibm-slapdDN) は、ソートする検索のために使用すると、検索結果を識別名 (DN) のストリング表記でソートします。出力は次のようになります。

```
cn=Al Edwards,ou=Widget Division,ou=Austin,o=IBM,c=US
cn=Al Garcia,ou=Home Entertainment,ou=Austin,o=IBM,c=US
cn=Amy Nguyen,ou=In Flight Systems,ou=Austin,o=IBM,c=US
cn=Arthur Edwards,ou=Widget Division,ou=Austin,o=IBM,c=US
cn=Becky Garcia,ou=In Flight Systems,ou=Austin,o=IBM,c=US
cn=Ben Catu,ou=In Flight Systems,ou=Austin,o=IBM,c=US
cn=Ben Garcia Jr,ou=Home Entertainment,ou=Austin,o=IBM,c=US
cn=Bill Keller Jr.,ou=In Flight Systems,ou=Austin,o=IBM,c=US
cn=Bob Campbell,ou=In Flight Systems,ou=Austin,o=IBM,c=US
```

次のコマンド:

```
ldapsearch -h hostname -o sn -b "o=ibm,c=us" "title=engineer"
```

は、IBM 従業員ディレクトリーにある役職が "engineer" であるすべての項目を、結果を姓でソートして戻します。

次のコマンド:

```
ldapsearch -h hostname -o -sn -o cn -b "o=ibm,c=us" "title=engineer"
```

は、IBM 従業員ディレクトリーにある役職が "engineer" であるすべての項目を、結果を姓で (降順) し、それから通称で (昇順) ソートして戻します。

次のコマンド:

```
ldapsearch -h hostname -q 5 -T 3 -b o=ibm,c=us "title=engineer"
```

は、IBM 従業員ディレクトリーにある役職が "engineer" であるすべての項目を、ページングごとに 5 項目、ページ間 3 秒の遅延で戻します。

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。 Directory Server LDAP ディレクトリは、次のものだけを格納している限り、参照オブジェクトを格納することができます。

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

'System\_A' には以下の参照項目が置かれていると想定します。

```
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' への要求を発行した場合、 System\_A 上の LDAP サーバーは、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 (**-R** フラグを指定して追跡参照をしないという指示をしない場合)。

クライアントは、サーバーから参照応答を受け取ると、今度は戻された URL の参照先であるサーバーに対して、再度要求を発行します。新規の要求には、元の要求と同じ有効範囲があります。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 base** 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 base '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。

**-s sub** を次のように指定したとします。

```
ldapsearch -s sub "cn=John"
```

サーバーはすべての接尾部を検索して、「cn=John」があるすべての項目を戻します。これは、ヌル・ベースのサブツリー検索と呼ばれます。検索ベースとして、異なる接尾部ごとに複数の検索を実行するのではなく、ディレクトリ全体が 1 つの検索操作で検索されます。このタイプの検索操作では、ディレクトリ全体 (すべての接尾部) が検索されるために、時間が長くなり、システム・リソースの消費も多くなります。

注: ヌル・ベースのサブツリー検索では、スキーマ情報、変更ログ情報は戻されず、またシステム・プロジェクト・バックエンドからも何も戻されません。

-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。

-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
```

クライアントは次の要求を実行依頼します。

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

これも結果を出しませんが、それは項目

```
dn: cn=Barb Jensen, ou=Rochester, o=Big Company, c=US
```

resides at

```
ou=Rochester, o=Big Company, c=US
```

-s one による検索では、以下のすぐ下のレベルでの項目が検出されます。

```
ou=Rochester, o=Big Company, c=US
```

## 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。

### 関連概念

#### Directory Server API

56 ページの『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 Directory Server 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。

### 関連資料

281 ページの『LDAP データ交換形式 (LDIF)』

LDAP データ交換形式は、LDAP オブジェクトおよび LDAP の更新 (追加、変更、削除、DN の変更) をテキスト・フォームで表すための標準テキスト・フォーマットです。LDIF レコードを収めたファイルを、Directory Server 間でデータを転送するのに使用するか、または **ldapadd** や **ldapmodify** のような LDAP ツールで入力として使用することができます。

### 関連情報

 [RFC 2252, LDAP V3 Attribute Syntax Definitions](#)

 [RFC 2254, A String Representation of LDAP Search Filters](#)



## ldapchangepwd

LDAP パスワード変更コマンド行ユーティリティー

### 概要

```
ldapchangepwd -D binddn -w passwd | ? -n newpassword | ?
[-C charset] [-d debuglevel] [-G realm] [-h ldaphost]
[-K keyfile] [-m mechanism] [-M] [-N certificatename]
[-O maxhops] [-p ldapport] [-P keyfilepw] [-R]
[-U username] [-v] [-V version] [-y proxydn] [-Y] [-Z] [-?]
```

### 説明

パスワード変更要求を LDAP サーバーに送信します。ディレクトリー項目に対するパスワードの変更を許可します。

### オプション

#### -C *charset*

ldapdelete ユーティリティーへの入力として提供された DN が、*charset* で指定されたローカル文字セットで表されるように設定します。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 *charset* 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 を参照してください。

#### -d *debuglevel*

LDAP 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。-m DIGEST-MD5 で使用する場合は、権限 ID を指定するために使用します。これは DN とすることもできるし、あるいは「u:」または「dn:」で始まる *authzId* ストリングとすることもできます。

#### -G *realm*

レルムを指定します。このパラメーターはオプションです。-m DIGEST-MD5 と一緒に使用すると、その値はバインド中にサーバーに渡されます。

#### -h *ldaphost*

LDAP サーバーを実行する代替ホストを指定します。

#### -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。i5/OS 上のディレクトリー・サーバーでは、-Z を使用して -K または -N を使用しない場合、ディレクトリー・サービス・クライアント・アプリケーション ID に関連した証明が使用されます。

#### -m *mechanism*

*mechanism* を使用して、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。

`ldap_sasl_bind_s()` API が使用されます。-V 2 をセットすると、-m パラメーターは無視されます。-m を指定しない場合、単純認証が使用されます。以下が有効なメカニズムです。

- CRAM-MD5 - サーバーに送信されるパスワードを保護する。
- EXTERNAL - SSL 認証を使用する。-Z が必要。
- GSSAPI - ユーザーの Kerberos 信任状を使用する。
- DIGEST-MD5 - クライアントは `username` 値をサーバーに送信する必要があります。-U が必要。権限 ID を指定するには、-D パラメーター (通常、バインド DN) が使用されます。これは DN とすることもできるし、あるいは「u:」または「dn:」で始まる `authzId` ストリングとすることもできます。

**-M** 参照オブジェクトを普通の項目として管理します。

**-n newpassword | ?**

新規パスワードを指定します。? を使用してパスワード・プロンプトを生成します。

**-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 サーバーがサーバー認証だけを実行するように構成されている場合は、クライアント証明書は不要です。LDAP サーバーがクライアントおよびサーバーの認証を実行するように構成されている場合は、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。i5/OS 上のディレクトリー・サーバーでは、-Z を使用して -K または -N を使用しない場合、ディレクトリー・サービス・クライアント・アプリケーション ID に関連した証明が使用されます。

**-O maxhops**

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 **maxhops** を指定します。デフォルトのホップ・カウントは 10 です。

**-p ldapport**

LDAP サーバーが `listen` する代替 TCP ポートを指定します。デフォルトの LDAP ポートは 389 です。**-p** 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。

**-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、1 つ以上の秘密鍵を含む場合のあるキー・データベース・ファイル内の暗号化された情報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、パスワードはそのパスワード `stash` ファイルから取得されるので、**-P** 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。

**-R** 参照を自動的に行わないことを指定します。

**-U username**

ユーザー名を指定します。**-m DIGEST-MD5** には必要ですが、その他のメカニズムでは無視されます。

**-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。

**-V version**

LDAP サーバーにバインドするときに、**ldapdchangepwd** によって使用されるよう、LDAP バージョンを指定します。デフォルトの設定では、LDAP V3 接続が確立されます。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。**ldapdchangepwd** などのアプリケーションでは、`ldap_open` の代わりに `ldap_init` が使用され、LDAP V3 が優先プロトコルとして選択されます。

**-w passwd | ?**

**passwd** を認証用のパスワードとして使用します。 ? を使用してパスワード・プロンプトを生成します。

**-y proxydn**

プロキシ権限操作のプロキシ ID を設定します。

**-Y** セキュア LDAP 接続 (TLS) を使用します。

**-Z** セキュア SSL 接続を使用して LDAP サーバーと通信します。 i5/OS 上のディレクトリー・サーバーでは、**-Z** を使用して **-K** または **-N** を使用しない場合、ディレクトリー・サービス・クライアント・アプリケーション ID に関連した証明が使用されます。

**-?** ldapchangepwd の構文ヘルプを表示します。

## 例

次のコマンドを使用します。

```
ldapchangepwd -D cn=John Doe -w a1b2c3d4 -n wxyz9876
```

は、commonName が "John Doe" である項目のパスワードを、a1b2c3d4 から wxyz9876 に変更します。

## 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。

### 関連概念

Lightweight Directory Access Protocol (LDAP) API

Directory Server API の詳細は、『Lightweight Directory Access Protocol (LDAP) APIs』を参照してください。

## ldapdiff

LDAP レプリカ同期コマンド行ユーティリティー

**注:** このコマンドは、複製される項目 (およびそれらの項目の属性) の数によっては、長い時間をかけて実行されます。

## 概要

(複製環境にある 2 つのサーバー間で、データ入力項目を比較し、同期化します。)

```
ldapdiff -b baseDN -sh host -ch host [-a] [-C countnumber]
[-cD dn] [-cK keyStore] [-cw password] [-cN keyLabel]
[-cp port] [-cP keyStorePwd] [-cZ] [-F] [-L filename] [-sD dn] [-sK keyStore]
[-sw password] [-sN keyLabel] [-sp port] [-sP keyStorePwd]
[-sZ] [-v]
```

または

(2 つのサーバー間でスキーマを比較します。)

```
ldapdiff -S -sh host -ch host [-a] [-C countnumber] [-cD dn]
[-cK keyStore] [-cw password] [-cN keyLabel] [-cp port]
[-cP keyStorePwd] [-cZ] [-L filename] [-sD dn]
[-sK keyStore] [-sw password] [-sN keyLabel] [-sp port]
[-sP keyStorePwd] [-sZ] [-v]
```

## 説明

このツールは、レプリカ・サーバーをそのマスターと同期にします。**ldapdiff** の構文ヘルプを表示するには、以下を入力します。

```
ldapdiff -?
```

## オプション

以下のオプションは、**ldapdiff** コマンドに適用されます。サプライヤー・サーバーまたはコンシューマー・サーバーのどちらかに特別に適用される 2 つのサブグループがあります。

- a 読み取り専用のレプリカに書き込むため、サーバー管理制御の使用を指定します。
- b *baseDN*  
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** を指定しない場合、ユーティリティは、`LDAP_BASEDN` 環境変数で *searchbase* の定義を調べます。
- C *countnumber*  
修正する項目の数を数えます。指定された数よりも多いミスマッチが検出された場合、ツールは終了します。
- F これは修正オプションです。指定されると、コンシューマー・レプリカの内容はサプライヤー・サーバーの内容と一致するように変更されます。これは、**-S** も指定されている場合には使用できません。
- L **-F** オプションが指定されていない場合、このオプションを使用して出力のために LDIF ファイルを生成してください。LDIF ファイルを使用して、コンシューマーを更新し、差異を除去することができます。
- S 両方のサーバー上のスキーマの比較を指定します。
- 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。

## 複製サプライヤーのオプション

以下のオプションは、コンシューマー・サーバーに適用され、オプション名のイニシャル「s」で示されています。

- sD *dn dn* を使用して LDAP ディレクトリーにバインドします。 *dn* は、ストリング表記の DN です。
- sh *host*  
ホスト名を指定します。
- sK *keyStore*  
**kdb** のデフォルト拡張子のある SSL キー・データベース・ファイルの名前を指定します。このパラメーターの指定がない場合、または値が空ストリング (`-sK""`) である場合、システム鍵ストアが使用されます。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。
- sN *keyLabel*  
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。鍵ストアの指定なしにラベルが指定されている場合、そのラベルはデジタル証明書マネージャー (DCM) 中のアプリケーション ID です。デフォルト・ラベル (アプリケーション ID) は `QIBM_GLD_DIRSRV_CLIENT` です。LDAP サーバーがサーバー認証だけを実行するように構成されている場合は、クライアント証明書は不要です。LDAP サーバーがクライアントおよびサーバーの認証を実行するように構成されている場合は、クライアント証明書が必要です。デフォルトの

証明書/秘密鍵のペアが指定されている場合は、**keyLabel** 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、**keyLabel** は不要です。**-sZ** と **-sK** 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。

**-sp** *ldapport*

LDAP サーバーが listen する代替 TCP ポートを指定します。デフォルトの LDAP ポートは 389 です。**-sp** の指定がなく、**-sZ** 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。

**-sP** *keyStorePwd*

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、1 つ以上の秘密鍵を含む場合のあるキー・データベース・ファイル内の暗号化された情報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、パスワードはそのパスワード stash ファイルから取得されるので、**-sP** パラメーターは必要ありません。**-sZ** と **-sK** 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。使用の鍵ストアに stash ファイルがある場合、パスワードは使用されません。

**-st** *trustStoreType*

**trust** 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 サーバーがサーバー認証だけを実行するように構成されている場合は、クライアント証明書は不要です。LDAP サーバーがクライアントおよびサーバーの認証を実行するように構成されている場合は、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、**trustStoreType** 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、**trustStoreType** は不要です。**-sZ** と **-sT** 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。

**-sZ** セキュア SSL 接続を使用して LDAP サーバーと通信します。

## 複製コンシューマーのオプション

以下のオプションは、コンシューマー・サーバーに適用され、オプション名のイニシャル「c」で示されています。**-cK**、**-cN**、または **-cP** の値の指定なしに **-cZ** が指定されている場合、便宜上、これらのオプションは、サプライヤー SSL オプションに指定されているものと同じ値を使用します。サプライヤー・オプションをオーバーライドしてデフォルト設定を使用するには、**-cK ""** **-cN ""** **-cP ""** を指定します。

**-cD** *dn dn* を使用して LDAP ディレクトリーにバインドします。**dn** は、ストリング表記の DN です。

**-ch** *host*

ホスト名を指定します。

**-cK** *keyStore*

**kdb** のデフォルト拡張子のある SSL キー・データベース・ファイルの名前を指定します。値が空ストリング (**-sK""**) である場合、システム鍵ストアが使用されます。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。

**-cN** *keyLabel*

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 サーバーがサーバー認証だけを実行するように構成されている場合は、クライアント証明書は不要です。鍵ストアの指定なしにラベルが指定されている場合、そのラベルはデジタル証明書マネージャー (DCM) 中のアプリケーション ID です。デフォルト・ラベル (アプリケーション ID) は **QIBM\_GLD\_DIRSrv\_CLIENT** です。LDAP サーバーがクライアントおよびサーバーの認証を実行するように構成されている場合は、クライアント証明書が必要です。デフォルトの証明書/秘密鍵のペアが指定されている場合は、**keyLabel** は不要です。同様に、指定したキー・データベース・フ

イル内に証明書/秘密鍵のペアが 1 つある場合も、*keyLabel* は不要です。-cZ と -cK 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。

#### -cp ldapport

LDAP サーバーが listen する代替 TCP ポートを指定します。デフォルトの LDAP ポートは 389 です。-cp の指定がなく、-cZ 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。

#### -cP keyStorePwd

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、1 つ以上の秘密鍵を含む場合のあるキー・データベース・ファイル内の暗号化された情報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、パスワードはそのパスワード stash ファイルから取得されるので、-cP パラメーターは必要ありません。-cZ と -cK 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。

#### -cw password ! ?

*password* を認証用のパスワードとして使用します。? を使用してパスワード・プロンプトを生成します。

-cZ セキュア SSL 接続を使用して LDAP サーバーと通信します。

## 例

```
ldapdiff -b <baseDN> -sh <supplierhostname> -ch <consumerhostname> [options]
```

または

```
ldapdiff -S -sh <supplierhostname> -ch <consumerhostname> [options]
```

## 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。

### 関連タスク

183 ページの『複製キューの管理』

以下の情報を参考にして、このサーバーで使用される複製契約 (キュー) ごとに複製の状況をモニターします。

### 関連資料

42 ページの『複製の概要』

複製の時、1 つのディレクトリーに行われた変更は、1 つ以上の追加のディレクトリーに伝搬します。それにより、1 つのディレクトリーに変更を行うと、複数の異なるディレクトリーに影響します。

## LDAP コマンド行ユーティリティーでの SSL の使用

以下の情報を参考にして、LDAP コマンド行ユーティリティーでの SSL の使用方法を確認します。

59 ページの『Directory Server での Secure Sockets Layer (SSL) と Transport Layer Security (TLS)』に、Directory Server LDAP サーバーでの SSL の使用が取り上げられています。この情報には、デ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、証明書ストアに 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 信任状が含まれます。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. デジタル認証マネージャー (DCM) を使用して、取得した CA 証明書を証明書ストアにインポートする。
3. DCM を使用して、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、証明書ストアにインポートして、「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。

- システム証明書ストアに 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 信任状が含まれます。
- 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。

#### 関連概念

59 ページの『Directory Server での Secure Sockets Layer (SSL) と Transport Layer Security (TLS)』  
Directory Server との通信の安全度をさらに高めるために、Secure Sockets Layer (SSL) セキュリティーおよび Transport Layer Security (TLS) を Directory Server で使用することができます。

## LDAP データ交換形式 (LDIF)

LDAP データ交換形式は、LDAP オブジェクトおよび LDAP の更新 (追加、変更、削除、DN の変更) をテキスト・フォームで表すための標準テキスト・フォーマットです。LDIF レコードを収めたファイル  
を、Directory Server 間でデータを転送するのに使用するか、または **ldapadd** や **ldapmodify** のような LDAP ツールで入力として使用することができます。

LDIF コンテンツ・レコードは、LDAP ディレクトリーの内容を表すのに使用されますが、これは、オブジェクトを識別する 1 行と、その後続く、オブジェクトの属性値ペアを記した行で構成されます。このタイプのファイルは、**ldapadd** Qshell ユーティリティーで使用されるほか、System i Navigator 内のディレクトリーのインポート/エクスポート・ツールや、CPYFRMLDIF (LDIF2DB) および CPYTOLDIF (DB2LDIF) CL コマンドでも使用されます。

注: DB2LDIF コマンドは、1 つのスタンドアロン・ジョブで実行することをお勧めします。

LDIF 変更レコードは、ディレクトリーの更新を表すのに使用します。このレコードは、ディレクトリー・オブジェクトを識別する 1 行と、その後続く、オブジェクトに加えられた変更を説明する行で構成されます。そのような変更には、オブジェクトの追加、削除、名前変更、または移動や、既存オブジェクトの変更などがあります。

この 2 つのレコードには、2 種類の入力スタイルがあります。1 つは、RFC 2849 で定義されている標準 LDIF スタイルである、LDAP データ交換形式 (LDIF) - 技術仕様であり、もう 1 つは、それより古い非

| 標準の変更スタイルです。標準 LDIF スタイルの使用をお勧めします。古いスタイルについては、このス  
| タイルを生成または使用する古いツールでの使用に備えて、本書で取り上げています。

## | 入力スタイル

| **ldapmodify** および **ldapadd** Qshell ユーティリティーは、2 種類のフォームの入力を受け入れます。入力  
| タイプは、**ldapmodify** または **ldapadd** に記入した最初の入力行のフォーマットで判別されます。

| **ldapmodify** または **ldapadd** コマンドへの最初の入力行には、追加または変更するディレクトリーの識別名  
| を書き入れる必要があります。この入力行のフォームは次のようなものでなければなりません。

| dn: distinguished\_name

| または

| distinguished\_name

| ただし dn: は、リテラル・ストリングであり、distinguished\_name は、変更 (または追加) するディレク  
| トリー項目の識別名です。dn: が検出されると、入力スタイルは RFC 2849 LDIF スタイルに設定されま  
| す。これが検出されない場合、入力スタイルは変更スタイルに設定されます。

| 注:

- | 1. **ldapadd** コマンドは、**ldapmodify -a** コマンドの呼び出しと同等です。
- | 2. **ldapmodify** および **ldapadd** ユーティリティーは、base64 エンコードの識別名をサポートしま  
| せん。

### | 関連資料

| 244 ページの『ldapmodify および ldapadd』

| LDAP modify-entry および LDAP add-entry コマンド行ユーティリティー

| 265 ページの『ldapsearch』

| LDAP 検索コマンド行ユーティリティー

## | RFC 2849 LDIF の入力

| RFC 2849 で定義されている標準 LDIF スタイル: LDAP データ交換形式 (LDIF) をお勧めします。LDIF  
| ファイルは、オプションの version および charset ディレクティブで開始することができます。このバ  
|ージョンは 1、文字セットは ISO-8859-1 です。

| charset ディレクティブは、CCSID を使ったファイルへのタグ付けをサポートしない他のプラットフォー  
| ム上でファイル・システムを使用するとき便利です。i5/OS での標準の動作は、UTF-8 (CCSID 1208)  
| での LDIF ファイルのオープンであり、ここではファイル・システムが、このファイルの CCSID から  
| UTF-8 へのデータの変換を行うことができ、しかも通常は charset ディレクティブは必要ありません。

| オプションのバージョンおよび文字セットの行の後には、以下の説明どおり、一連の変更レコードが続きま  
| す。

| RFC 2849 LDIF 入力を使用すると、属性のタイプと値は単一のコロンの (:) または二重の (::) で区切られま  
| す。さらに、属性値に加えた個々の変更は、changetype: 入力行で区切られます。RFC 2849 LDIF での  
| 一般の入力行フォームは、次のとおりです。

| change\_record  
| <blank line>  
| change\_record



```
| <blank line>
| .
| .
| .
```

| RFC 2849 LDIF スタイルの入力ファイルは、単一のブランク行で区切られた 1 つ以上の `change_record` 行  
| セットで構成されます。各 `change_record` は、次のようなフォームになります。

```
| dn: <distinguished name>
| [changetype: {modify|add|modrdn|moddn|delete}]
| change_clause
| change_clause
| .
| .
| .
```

| このように、変更しようとしているディレクトリー項目の識別名を示す行と、ディレクトリー項目に対して  
| 実行する変更のタイプを示すオプションの行、および 1 つ以上の `change_clause` 行セットによって  
| `change_record` は構成されます。 `changetype:` 行を省略すると、`changetype` を `add` とみなす  
| `ldapmodify -a` または `ldapadd` のコマンド呼び出しでない限り、変更タイプは `modify` であるとみなされま  
| す。

| 変更タイプが `modify` であると、各 `change_clause` は、次のようなフォームの一連の行として定義されま  
| す。

```
| add: {attrtype}
| {attrtype}{sep}{value}
| .
| .
| .
| -
```

| または

```
| replace: {attrtype}
| {attrtype}{sep}{value}
| .
| .
| .
| -
```

| または

```
| delete: {attrtype}
| [{attrtype}{sep}{value}]
| .
| .
| .
| -
```

| または

```
| {attrtype}{sep}{value}
| .
| .
| .
```

| `replace` を指定すると、属性の既存の値はすべて、指定した一連の属性に置き換えられます。 `add` を指定  
| すると、既存の一連の属性値への追加が行われます。属性と値のペアのレコードを指定しないで `delete` を  
| 指定すると、指定した属性のすべての値が除去されます。1 つ以上の属性と値のペアのレコードを後に付  
| けて `delete` を指定すると、その属性と値のペアのレコードに指定した値のみが除去されます。

| add: *attrtype*、replace:*attrtype*、または delete: *attrtype* の行 (変更標識) のいずれかを指定した場合、ハ  
| イフン (-) が使われている行は、その *attrtype* の変更の終了区切り文字であるとみなされます。変更標識  
| とハイフン行にはさまれた入力行上には、属性と値のペアが入るとみなされます。changetype 行を省略す  
| ると、changetype は、ldapadd の場合は add とみなされ、ldapmodify の場合は replace とみなされま  
| す。

| 使用する区切り文字 *sep* に応じて、テキスト・ストリング、base-64 エンコード、またはファイル URL と  
| して属性値を指定することができます。

#### | **attrtype: value**

| 単一のコロンの (:) は、値がストリング *value* であることを指定します。

#### | **attrtype:: base64string**

| 二重コロンの (: :) は、*base64string* がバイナリー値の base 64 エンコード・ストリングであるか、  
| またはマルチバイト文字から成る UTF-8 ストリングであることを指定します。

#### | **attrtype:< fileURL**

| コロンと左不等号括弧 (:<) は、fileURL で識別されたファイルからの値の読み取りを指定します。  
| jpegPhoto 属性の値がファイル /tmp/photo.jpg にあることを指定する、ファイル URL 行の例は次  
| のとおりです。

| jpegphoto:< file:///tmp/photo.jpg

| 区切り文字と属性値にはさまれた空白文字はすべて無視されます。複数の行にまたがって属性値を続けるに  
| は、入力の次の行の先頭文字としてシングル・スペース文字を使用します。二重コロンを区切り文字として  
| 使用すると、入力は base64 フォーマットであるとみなされます。このフォーマットは、3 つのバイナリ  
| ー・バイトごとの 4 つのテキスト文字を表すエンコード方式です。

| 複数の属性値は、複数の (*attrtype*){*sep*}{*value*} の指定を使って指定します。

| 変更タイプが add であると、各 *change\_clause* は、次のようなフォームの一連の行として定義されます。

| {*attrtype*}{*sep*}{*value*}

| modify の変更タイプと同様に、区切り文字 *sep* と値は、単一コロンの (:)、二重コロンの (: :)、またはコロ  
| ンと左不等号括弧 (:<) のいずれでもかまいません。区切り文字と属性値にはさまれた空白文字はすべて無視  
| されます。複数の行にまたがって属性値を続けるには、入力の次の行の先頭文字としてシングル・スペース  
| 文字を使用します。二重コロンを区切り文字として使用すると、入力は base64 フォーマットであるとみな  
| されます。

| 変更タイプが modrdn または moddn であると、各 *change\_clause* は、次のようなフォームの一連の行とし  
| て定義されます。

| newrdn: value  
| deleteoldrdn:{0|1}  
| [newsuperior: newSuperiorDn]

| これらは、modify RDN (rename) または modifyDN (move) LDAP 操作で指定できるパラメーターです。  
| newrdn 設定の値は、modify RDN 操作の実行時に使用される新規の RDN になります。deleteoldrdn 設  
| 定の値としては、古い RDN 内に属性を保存する場合は 0を指定し、古い RDN 内の属性値を除去するに  
| は 1 を指定します。newsuperior 設定の値は、項目の移動時の新しい上位項目 (親) の DN になりま  
| す。

| 変更タイプが delete の場合、*change\_clause* は指定されません。

#### | **LDIF スタイルの例:**

| このトピックでは、RFC 2849 LDIF スタイルを使用する **ldapmodify** コマンドの有効な入力の例を示しま  
| す。

### | 新規項目の追加

| 以下の例は、名前 cn=Tim Doe、ou=Your Department、o=Your Company、c=US を使用して、新しい項目をデ  
| イレクトリーに追加します。ただし、**ldapadd** または **ldapmodify -a** を呼び出すと想定しています。

```
| dn:cn=Tim Doe, ou=Your Department, o=Your Company, c=US
| changetype:add
| cn: Tim Doe
| sn: Doe
| objectclass: organizationalperson
| objectclass: person
| objectclass: top
```

| 以下の例は、名前 cn=Tim Doe、ou=Your Department、o=Your Company、c=US を使用して、新しい項目をデ  
| イレクトリーに追加します。ただし、**ldapadd** または **ldapmodify -a** を呼び出すと想定しています。

| jpegphoto 属性は、ファイル /tmp/timdoe.jpg からロードされることに注意してください。

```
| dn:cn=Tim Doe, ou=Your Department, o=Your Company, c=US
| changetype:add
| cn: Tim Doe
| sn: Doe
| jpegphoto:< file:///tmp/timdoe.jpg
| objectclass: inetorgperson
| objectclass: organizationalperson
| objectclass: person
| objectclass: top
```

### | 属性タイプの追加

| 以下の例は、2 つの新しい属性タイプを既存の項目に追加します。 registeredaddress 属性には、以下の  
| 2 つの値が割り当てられることに注意してください。

```
| dn:cn=Tim Doe, ou=Your Department, o=Your Company, c=US
| changetype: modify
| add: telephonenumber
| telephonenumber: 888 555 1234
| -
| add: registeredaddress
| registeredaddress: td@yourcompany.com
| registeredaddress: ttd@yourcompany.com
```

### | 項目名の変更

| 以下の例は、既存の項目の名前を cn=Tim Tom Doe、ou=Your Department、o=Your Company、c=US に変更し  
| ます。古い RDN である cn=Tim Doe は、cn 属性の追加の属性値として保持されます。新しい RDN であ  
| る cn=Tim Tom Doe は、LDAP サーバーによって項目内の cn 属性の値に自動的に追加されます。

```
| dn: cn=Tim Doe, ou=Your Department, o=Your Company, c=US
| changetype:modrdn
| newrdn: cn=Tim Tom Doe
| deleteoldrdn: 0
```

| 以下の例は、cn=Tim Doe を ou=New Department に移動します。RDN (cn=Tim Doe) は変更されません。

```
| dn: cn=Tim Doe, ou=Your Department, o=Your Company, c=US
| changetype:moddn
| newrdn: cn=Tim Doe
| deleteoldrdn: 0
| newsuperior: ou=New Department, o=Your Company, c=US
```

## | 属性値の置換

| 以下の例は、telephonenumber および registeredaddress 属性の属性値を、指定された属性値に置き換えます。

```
| dn: cn=Tim Tom Doe, ou=Your Department, o=Your Company, c=US
| changetype: modify
| replace: telephonenumber
| telephonenumber: 888 555 4321
| -
| replace: registeredaddress
| registeredaddress: tim@yourcompany.com
| registeredaddress: timtd@yourcompany.com
```

## | 属性の削除と追加

| 以下の例は、telephonenumber 属性を削除し、1 つの registeredaddress 属性値を削除し、description 属性を追加します。

```
| dn:cn=Tim Tom Doe, ou=Your Department, o=Your Company, c=US
| changetype: modify
| add: description
| description: This is a very long attribute
| value that is continued on a second line.
| Note the spacing at the beginning of the
| continued lines in order to signify that
| the line is continued.
| -
| delete: telephonenumber
| -
| delete: registeredaddress
| registeredaddress: tim@yourcompany.com
```

## | 項目の削除

| 以下の例は、名前 cn=Tim Tom Doe, ou=Your Department, o=Your Company, c=US の付いたディレクトリー項目を削除します。

```
| dn:cn=Tim Tom Doe, ou=Your Department, o=Your Company, c=US
| changetype:delete
```

## | 変更スタイル LDIF 入力

| **ldapmodify** または **ldapadd** コマンドへの古い非標準の変更入力スタイルは、RFC 2849 LDIF スタイルほど柔軟ではありません。ただし場合によっては、LDIF スタイルを使用するより簡単です。

| 変更スタイル入力を使用する場合、属性タイプと値を等号 (=) で区切ります。変更スタイルでの一般的な入力行フォームは、次のとおりです。

```
| change_record
| <blank_line>
| change_record
| <blank_line>
| .
| .
| .
```

| 変更スタイルの入力ファイルは、単一のブランク行で区切られた 1 つ以上の *change\_record* 行セットで構成されます。各 *change\_record* は、次のようなフォームになります。

```
| distinguished_name
| [+|-]{attrtype} = {value_line1[¥
| value_line2[¥
```

```
| ...value_lineN]]}
| .
| .
| .
```

| このように、変更しようとしているディレクトリー項目の識別名を示す行に加えて、1 つ以上の属性変更行  
| によって *change\_record* が構成されます。各属性変更行は、オプションの追加または削除標識 (+ または  
| -)、属性タイプ、および属性値で構成されます。正符号 (+) を指定した場合、変更タイプは **add** に設定さ  
| れます。ハイフン (-) を指定した場合、変更タイプは **delete** に設定されます。削除変更の場合、属性全体  
| を除去するには、等号 (=) と *value* を省略する必要があります。追加または削除標識を指定しなかった場  
| 合は、変更タイプを **replace** に設定する **-r** オプションを指定しない限り、変更タイプは **add** に設定され  
| ます。先頭または末尾に付けた空白文字はすべて、属性値から除去されます。末尾に空白文字をつける必要  
| のある属性値の場合、RFC 2849 LDIF スタイルの入力を使用する必要があります。行を続けるには、行の  
| 最後の文字として円記号 (¥) を使用します。行を続けると、円記号が除去されて、次の行は、円記号の直  
| 前にあった文字の直後に付け加えられます。入力行の末尾の改行文字は、属性値の一部として保持されませ  
| ん。

| 複数の属性値を指定するには、複数の *attrtype=value* を指定します。

| ファイル・オプションのサポート・バイナリ値 (-b) を指定した場合、その値はファイル名であること  
| が、*'/'*で始まる *value* によって示されます。たとえば、以下の行は、**jpegphoto** 属性をファイル  
| /tmp/photo.jpg から読み取るよう指示します。

```
| jpegphoto=/tmp/photo.jpg
```

#### | 変更スタイルの例:

| このトピックでは、変更スタイルを使用する **ldapmodify** コマンドの有効な入力の例を示します。

#### | 新規項目の追加

| 以下の例は、名前 **cn=Tim Doe**, **ou=Your Department**, **o=Your Company**, **c=US** を使って、新しい項目をディ  
| レクトリーに追加します。

```
| cn=Tim Doe, ou=Your Department, o=Your Company, c=US
| cn=Tim Doe
| sn=Doe
| objectclass=organizationalperson
| objectclass=person
| objectclass=top
```

#### | 新規属性タイプの追加

| 以下の例は、2 つの新しい属性タイプを既存の項目に追加します。 **registeredaddress** 属性には、以下の  
| 2 つの値が割り当てられることに注意してください。

```
| cn=Tim Doe, ou=Your Department, o=Your Company, c=US
| +telephonenumber=888 555 1234
| +registeredaddress=td@yourcompany.com
| +registeredaddress=ttd@yourcompany.com
```

#### | 属性値の置換

| コマンドの呼び出しは、次のとおりであったと想定します。

```
| ldapmodify -r ...
```

| 以下の例は、telephonenumber および registeredaddress 属性の属性値を、指定された属性値に置き換えます。 **-r** コマンド行オプションを指定しないと、属性値は、既存の一連の属性値に追加されます。

```
| cn=Tim Doe, ou=Your Department, o=Your Company, c=US
| telephonenumber=888 555 4321
| registeredaddress: tim@yourcompany.com
| registeredaddress: timtd@yourcompany.com
```

## | 属性タイプの削除

| 以下の例は、1 つの registeredaddress 属性値を既存の項目から削除します。

```
| cn=Tim Doe, ou=Your Department, o=Your Company, c=US
| -registeredaddress=tim@yourcompany.com
```

## | 属性の追加

| 以下の例は、description 属性を追加します。 description 属性値は、次のように、複数の行にまたがります。

```
| cn=Tim Doe, ou=Your Department, o=Your Company, c=US
| +description=This is a very long attribute ¥
| value that is continued on a second line. ¥
| Note the backslash at the end of the line to ¥
| be continued in order to signify that ¥
| the line is continued.
```

## | Directory Server 構成スキーマ

この情報では、ディレクトリー情報ツリー (DIT) および `ibmslapd.conf` ファイルの構成に使用する属性を説明します。

前のリリースでは、ディレクトリー構成設定は、構成ファイル内に専用形式で保管されていました。現在は、ディレクトリー設定は LDIF 形式で構成ファイルに保管されています。

構成ファイルには、`ibmslapd.conf` という名前が付いています。構成ファイルが使用するスキーマも現在使用可能です。属性タイプは `v3.config.at` ファイルにあり、オブジェクト・クラスは `v3.config.oc` ファイルにあります。属性は、`ldapmodify` コマンドを使用して変更できます。

### 関連概念

34 ページの『スキーマ検査』

サーバーが初期化される時、スキーマ・ファイルが読み取られ、整合性および正確さが検査されます。

### 関連資料

244 ページの『`ldapmodify` および `ldapadd`』

LDAP `modify-entry` および LDAP `add-entry` コマンド行ユーティリティー

## ディレクトリー情報ツリー

この情報は、Directory Server のディレクトリー情報ツリー (DIT) について説明します。

cn=Configuration

- cn=Admin
- cn=Event Notification
- cn=Front End
- cn=Kerberos
- cn=Master Server

- cn=Referral
- cn=Schema
  - cn=IBM Directory
    - cn=Config Backends
      - cn=ConfigDB
    - cn=RDBM Backends
      - cn=Directory
      - cn=ChangeLog
    - cn=LDCF Backends
      - cn=SchemaDB
- cn=SSL
  - cn=CRL
- cn=Transaction

## cn=Configuration

**DN** cn=Configuration

**説明** これは構成 DIT の最上位項目です。この中にはサーバーにとって重要な全体的なデータが含まれますが、実際には雑多な項目も含まれています。この項目のそれぞれの属性は、`ibmslapd.conf` の最初のセクション (グローバル・スタンザ) から来ています。

**数値** 1 (必要)

**オブジェクト・クラス**

ibm-slapdTop

**必須属性**

- cn
- ibm-slapdAdminDN
- ibm-slapdAdminPW
- ibm-slapdErrorLog
- ibm-slapdPort
- ibm-slapdPwEncryption
- ibm-slapdSizeLimit
- ibm-slapdSysLogLevel
- ibm-slapdTimeLimit
- objectClass

**オプション属性**

- ibm-slapdACLAccess
- ibm-slapdACIMechanism
- ibm-slapdConcurrentRW (使用すべきでない)
- ibm-slapdMaxPendingChangesDisplayed
- ibm-slapdServerId
- ibm-slapdSupportedWebAdmVersion

- ibm-slapdVersion

### **cn=Admin**

**DN** cn=Admin, cn=Configuration

**説明** IBM Admin Daemon のグローバル構成設定

**数値** 1 (必要)

**オブジェクト・クラス**

ibm-slapdAdmin

**必須属性**

- cn
- ibm-slapdErrorLog
- ibm-slapdPort

**オプション属性**

- ibm-slapdSecurePort

### **cn=Event Notification**

**DN** cn=Event Notification, cn=Configuration

**説明** ディレクトリー・サーバーのグローバル・イベント通知設定

**数値** 0 または 1 (オプション、イベント通知を使用可能にする場合にのみ必要)

**オブジェクト・クラス**

ibm-slapdEventNotification

**必須属性**

- cn
- ibm-slapdEnableEventNotification
- objectClass

**オプション属性**

- ibm-slapdMaxEventsPerConnection
- ibm-slapdMaxEventsTotal

### **cn=Front End**

**DN** cn=Front End, cn=Configuration

**説明** サーバーが始動時に適用するグローバル環境設定

**数値** 0 または 1 (オプション)

**オブジェクト・クラス**

ibm-slapdFrontEnd

**必須属性**

- cn
- objectClass

**オプション属性**

- ibm-slapdACLCache



- ibm-slapdACLCacheSize
- ibm-slapdDB2CP
- ibm-slapdEntryCacheSize
- ibm-slapdFilterCacheBypassLimit
- ibm-slapdFilterCacheSize
- ibm-slapdPlugin
- ibm-slapdSetenv
- ibm-slapdIdleTimeOut

### **cn=Kerberos**

**DN** cn=Kerberos, cn=Configuration

**説明** ディレクトリー・サーバーのグローバル Kerberos 認証設定

**数値** 0 または 1 (オプション)

**オブジェクト・クラス**

ibm-slapdKerberos

**必須属性**

- cn
- ibm-slapdKrbEnable
- ibm-slapdKrbRealm
- ibm-slapdKrbKeyTab
- ibm-slapdKrbIdentityMap
- ibm-slapdKrbAdminDN
- objectClass

**オプション属性**

- なし

### **cn=Master Server**

**DN** cn=Master Server, cn=Configuration

**説明** レプリカを構成するとき、この項目はマスター・サーバーのバインド信任状および参照 URL を保持します。

**数値** 0 または 1 (オプション)

**オブジェクト・クラス**

ibm-slapdReplication

**必須属性**

- cn
- ibm-slapdMasterPW (Kerberos 認証を使用していない場合に必須。)

**オプション属性**

- ibm-slapdMasterDN
- ibm-slapdMasterPW (Kerberos 認証を使用している場合はオプション。)
- ibm-slapdMasterReferral

- objectClass

### cn=Referral

**DN** cn=Referral, cn=Configuration

**説明** この項目には、ibmslapd.conf の最初のセクション (グローバル・スタンザ) からのすべての参照項目が含まれます。参照がない場合 (デフォルトではなし)、この項目はオプションです。

**数値** 0 または 1 (オプション)

**オブジェクト・クラス**

ibm-slapdReferral

**必須属性**

- cn
- ibm-slapdReferral
- objectClass

**オプション属性**

- なし

### cn=Schemas

**DN** cn=Schemas, cn=Configuration

**説明** この項目は、スキーマのコンテナとしての役割があります。スキーマはオブジェクト・クラス ibm-slapdSchema により識別できるため、この項目は実際には必要ありません。これは、DIT を読みやすくするために組み込まれています。

現在許可されているスキーマ項目は、cn=IBM Directory の 1 つだけです。

**数値** 1 (必要)

**オブジェクト・クラス**

Container

**必須属性**

- cn
- objectClass

**オプション属性**

- なし

### cn=IBM Directory

**DN** cn=IBM Directory, cn=Schemas, cn=Configuration

**説明** この項目には、ibmslapd.conf の最初のセクション (グローバル・スタンザ) からのすべてのスキーマ構成データが含まれます。これは、スキーマを使用するすべてのバックエンドのコンテナとしての役割もあります。現在のところ、多重スキーマはサポートされていませんが、サポートされる場合には、スキーマごとに 1 つの ibm-slapdSchema 項目があることとなります。多重スキーマは非互換とされていることに注意してください。したがって、バックエンドは、1 つのスキーマしか関連付けることができません。

**数値** 1 (必要)

## オブジェクト・クラス

ibm-slapdSchema

### 必須属性

- cn
- ibm-slapdSchemaCheck
- ibm-slapdIncludeSchema
- objectClass

### オプション属性

- ibm-slapdSchemaAdditions

## cn=Config Backends

DN cn=Config Backends, cn=IBM Directory, cn=Schemas, cn=Configuration

説明 この項目は、Config バックエンドのコンテナーとしての役割があります。

数値 1 (必要)

## オブジェクト・クラス

Container

### 必須属性

- cn
- objectClass

### オプション属性

なし

## cn=ConfigDB

DN cn=ConfigDB, cn=Config Backends, cn=IBM Directory, cn=Schemas, cn=Configuration

説明 IBM Directory Server 構成の構成バックエンド

数値 0 - n (オプション)

## オブジェクト・クラス

ibm-slapdConfigBackend

### 必須属性

- ibm-slapdSuffix
- ibm-slapdPlugin

### オプション属性

- ibm-slapdReadOnly

## cn=RDBM Backends

DN cn=RDBM Backends, cn=IBM Directory, cn=Schemas, cn=Configuration

説明 この項目は、RDBM バックエンドのコンテナーとしての役割があります。すべての副項目を DB2 バックエンドとして識別することにより、ibmslapd.conf からデータベース rdbm 行を効果的に置き換えます。RDBM バックエンドはオブジェクト・クラス ibm-slapdRdbmBackend により識別できるため、この項目は実際には必要ありません。これは、DIT を読みやすくするために組み込まれています。

数値 0 または 1 (オプション)

#### オブジェクト・クラス

Container

#### 必須属性

- cn
- objectClass

#### オプション属性

- なし

### cn=Directory

**DN** cn=Directory, cn=RDBM Backends, cn=IBM Directory, cn=Schemas, cn=Configuration

**説明** この項目は、デフォルト RDBM データベース・バックエンドのすべてのデータベース構成設定が含まれます。

任意の名前を持つ複数のバックエンドを作成することはできますが、サーバー管理では、"cn=Directory" がメイン・ディレクトリー・バックエンドで、"cn=ChangeLog" はオプション変更ログ・バックエンドであると想定されます。"cn=Directory" で表示される接尾部のみが、サーバー管理を通して構成可能 (変更ログを使用可能化して透過的に設定する変更ログの接尾部は例外) です。

数値 0 - n (オプション)

#### オブジェクト・クラス

ibm-slapdRdbmBackend

#### 必須属性

- cn
- ibm-slapdDbInstance
- ibm-slapdDbName
- ibm-slapdDbUserID
- objectClass

#### オプション属性

- ibm-slapdBulkloadErrors
- ibm-slapdChangeLogMaxEntries
- ibm-slapdCLIErrors
- ibm-slapdDBAlias
- ibm-slapdDB2CP
- ibm-slapdDbConnections
- ibm-slapdDbLocation
- ibm-slapdPagedResAllowNonAdmin
- ibm-slapdPagedResLmt
- ibm-slapdPageSizeLmt
- ibm-slapdPlugin
- ibm-slapdReadOnly

- ibm-slapdReplDbConns
- ibm-slapdSortKeyLimit
- ibm-slapdSortSrchAllowNonAdmin
- ibm-slapdSuffix
- ibm-slapdUseProcessIdPw

注: **ibm-slapdUseProcessIdPw** を使用している場合には、スキーマを変更して、**ibm-slapdDbUserPW** オプションを作成することをご検討ください。

## cn=Change Log

**DN** cn=Change Log, cn=RDBM Backends, cn=IBM Directory, cn=Schemas, cn=Configuration

**説明** この項目は、変更ログ・バックエンドのすべてのデータベース構成設定が含まれます。

**数値** 0 - n (オプション)

### オブジェクト・クラス

ibm-slapdRdbmBackend

### 必須属性

- cn
- ibm-slapdDbInstance
- ibm-slapdDbName
- ibm-slapdDbUserID
- objectClass

### オプション属性

- ibm-slapdBulkloadErrors
- ibm-slapdChangeLogMaxEntries
- ibm-slapdCLIErrors
- ibm-slapdDBAlias
- ibm-slapdDB2CP
- ibm-slapdDbConnections
- ibm-slapdDbLocation
- ibm-slapdPagedResAllowNonAdmin
- ibm-slapdPagedResLmt
- ibm-slapdPageSizeLmt
- ibm-slapdPlugin
- ibm-slapdReadOnly
- ibm-slapdReplDbConns
- ibm-slapdSortKeyLimit
- ibm-slapdSortSrchAllowNonAdmin
- ibm-slapdSuffix
- ibm-slapdUseProcessIdPw

注: **ibm-slapdUseProcessIdPw** を使用している場合には、スキーマを変更して、**ibm-slapdDbUserPW** オプションを作成することをご確認ください。

## cn=LDCF Backends

**DN** cn=LDCF Backends, cn=IBM Directory, cn=Schemas, cn=Configuration

**説明** この項目は、LDCF バックエンドのコンテナとしての役割があります。すべての副項目を LDCF バックエンドとして識別することにより、これは `ibmslapd.conf` からデータベース `ldcf` 行を効果的に置き換えます。LDCF バックエンドは、オブジェクト・クラス `ibm-slapdLdcfBackend` により識別できるため、この項目は実際には必要ありません。これは、DIT を読みやすくするために組み込まれています。

**数値** 1 (必要)

**オブジェクト・クラス**  
Container

**必須属性**

- cn
- objectClass

**オプション属性**

- `ibm-slapdPlugin`

## cn=SchemaDB

**DN** cn=SchemaDB, cn=LDCF Backends, cn=IBM Directory, cn=Schemas, cn=Configuration

**説明** この項目は、`ibmslapd.conf` の `ldcf` データベース・セクションのすべてのデータベース構成データが含まれます。

**数値** 1 (必要)

**オブジェクト・クラス**  
`ibm-slapdLdcfBackend`

**必須属性**

- cn
- objectClass

**オプション属性**

- `ibm-slapdPlugin`
- `ibm-slapdSuffix`

## cn=SSL

**DN** cn=SSL, cn=Configuration

**説明** ディレクトリー・サーバーのグローバル SSL 接続設定。

**数値** 0 または 1 (オプション)

**オブジェクト・クラス**  
`ibm-slapdSSL`

**必須属性**

- cn

- ibm-slapdSecurity
- ibm-slapdSecurePort
- ibm-slapdSslAuth
- objectClass

#### オプション属性

- ibm-slapdSslCertificate
- ibm-slapdSslCipherSpec

注: **ibm-slapdSslCipherSpecs** は、使用すべきではありません。代わりに、**ibm-slapdSslCipherSpec** を使用してください。 **ibm-slapdSslCipherSpecs** を使用する場合には、サーバーは、サポートされている属性に変換します。

- ibm-slapdSslKeyDatabase
- ibm-slapdSslKeyDatabasePW

#### cn=CRL

**DN** cn=CRL, cn=SSL, cn=Configuration

**説明** この項目は、ibmslapd.conf の最初のセクション (グローバル・スタンザ) からの証明書取り消しリストを含みます。これは、cn=SSL 項目の "ibm-slapdSslAuth = serverclientauth" およびクライアント証明書が CRL 検証のために発行されている場合にのみ必要です。

**数値** 0 または 1 (オプション)

#### オブジェクト・クラス

ibm-slapdCRL

#### 必須属性

- cn
- ibm-slapdLdapCrlHost
- ibm-slapdLdapCrlPort
- objectClass

#### オプション属性

- ibm-slapdLdapCrlUser
- ibm-slapdLdapCrlPassword

#### cn=Transaction

**DN** cn = Transaction, cn = Configuration

**説明** グローバル・トランザクション・サポート設定値を指定します。次のプラグインの使用でトランザクション・サポートが供給されています。

```
extendedop /QSYS.LIB/QGLDTRANEX.SRVPGM tranExtOpInit 1.3.18.0.2.12.5
1.3.18.0.2.12.6
```

サーバー (slapd) は、**ibm-slapdTransactionEnable = TRUE** である場合、開始の時点でこのプラグインを自動的にロードします。プラグインは、**ibmslapd.conf** に明示的に追加する必要はありません。

**数値** 0 または 1 (オプション、トランザクションを使用する場合にのみ必要)

## オブジェクト・クラス

ibm-slapdTransaction

### 必須属性

- cn
- ibm-slapdMaxNumOfTransactions
- ibm-slapdMaxOpPerTransaction
- ibm-slapdMaxTimeLimitOfTransactions
- ibm-slapdTransactionEnable
- objectClass

### オプション属性

- なし

## 属性

この情報では、ibmslapd.conf ファイルの構成に使用する Directory Server の属性について説明します。

- cn
- ibm-slapdACIMechanism
- ibm-slapdACLAccess
- ibm-slapdACLCache
- ibm-slapdACLCacheSize
- ibm-slapdAdminDN
- ibm-slapdAdminGroupEnabled
- ibm-slapdAdminPW
- ibm-slapdAllowAnon
- ibm-slapdAllReapingThreshold
- ibm-slapdAnonReapingThreshold
- ibm-slapdBoundReapingThreshold
- ibm-slapdBulkloadErrors
- ibm-slapdCachedAttribute
- ibm-slapdCachedAttributeAutoAdjust
- ibm-slapdCachedAttributeAutoAdjustTime
- ibm-slapdCachedAttributeAutoAdjustTimeInterval
- ibm-slapdCachedAttributeSize
- ibm-slapdChangeLogMaxEntries
- ibm-slapdCLIErrors
- ibm-slapdConcurrentRW
- ibm-slapdDB2CP
- ibm-slapdDBAlias
- ibm-slapdDbConnections
- ibm-slapdDbInstance
- ibm-slapdDbLocation



- ibm-slapdDbName
- ibm-slapdDbUserID
- ibm-slapdDbUserPW
- ibm-slapdDerefAliases
- ibm-slapdDigestAdminUser
- ibm-slapdDigestAttr
- ibm-slapdDigestRealm
- ibm-slapdEnableEventNotification
- ibm-slapdEntryCacheSize
- ibm-slapdErrorLog
- ibm-slapdESizeThreshold
- ibm-slapdEThreadActivate
- ibm-slapdEThreadEnable
- ibm-slapdETimeThreshold
- ibm-slapdFilterCacheBypassLimit
- ibm-slapdFilterCacheSize
- ibm-slapdIdleTimeOut
- ibm-slapdIncludeSchema
- ibm-slapdKrbAdminDN
- ibm-slapdKrbEnable
- ibm-slapdKrbIdentityMap
- ibm-slapdKrbKeyTab
- ibm-slapdKrbRealm
- ibm-slapdLanguageTagsEnabled
- ibm-slapdLdapCrlHost
- ibm-slapdLdapCrlPassword
- ibm-slapdLdapCrlPort
- ibm-slapdLdapCrlUser
- ibm-slapdMasterDN
- ibm-slapdMasterPW
- ibm-slapdMasterReferral
- ibm-slapdMaxEventsPerConnection
- ibm-slapdMaxEventsTotal
- ibm-slapdMaxNumOfTransactions
- ibm-slapdMaxOpPerTransaction
- ibm-slapdMaxPendingChangesDisplayed
- ibm-slapdMaxTimeLimitOfTransactions
- ibm-slapdPagedResAllowNonAdmin
- ibm-slapdPagedResLmt
- ibm-slapdPageSizeLmt

- ibm-slapdPlugin
- ibm-slapdPort
- ibm-slapdPwEncryption
- ibm-slapdReadOnly
- ibm-slapdReferral
- ibm-slapdReplDbConns
- ibm-slapdReplicaSubtree
- ibm-slapdSchemaAdditions
- ibm-slapdSchemaCheck
- ibm-slapdSecurePort
- ibm-slapdSecurity
- ibm-slapdServerId
- ibm-slapdSetenv
- ibm-slapdSizeLimit
- ibm-slapdSortKeyLimit
- ibm-slapdSortSrchAllowNonAdmin
- ibm-slapdSslAuth
- ibm-slapdSslCertificate
- ibm-slapdSslCipherSpec
- ibm-slapdSslKeyDatabase
- ibm-slapdSslKeyDatabasePW
- ibm-slapdSslKeyRingFile
- ibm-slapdSuffix
- ibm-slapdSupportedWebAdmVersion
- ibm-slapdSysLogLevel
- ibm-slapdTimeLimit
- ibm-slapdTransactionEnable
- ibm-slapdUseProcessIdPw
- ibm-slapdVersion
- ibm-slapdWriteTimeout
- objectClass

## **cn**

**説明** これは、X.500 共通名属性であり、オブジェクトの名前が含まれます。

**構文** ディレクトリー・ストリング

**最大長** 256

**値** 複数値

### **ibm-slapdACIMechanism**

**説明** サーバーがどの ACL モデルを使用するかを決定します。(v3.2 の時点では i5/OS および OS/400 でのみサポートされており、他のプラットフォームでは無視されます。)

- 1.3.18.0.2.26.1 = IBM SecureWay v3.1 ACL model
- 1.3.18.0.2.26.2 = IBM SecureWay v3.2 ACL model

#### **デフォルト値**

1.3.18.0.2.26.2 = IBM SecureWay v3.2 ACL model

**構文** ディレクトリー・ストリング

**最大長** 256

**値** 複数値

### **ibm-slapdACLAccess**

**説明** ACL へのアクセスを使用可能にするかどうかを制御します。TRUE に設定すると、ACL へのアクセスが可能になります。FALSE に設定すると、ACL へのアクセスは使用不可になります。

#### **デフォルト値**

TRUE

**構文** ブール

**最大長** 5

**値** 単一値

### **ibm-slapdACLCache**

**説明** サーバーが ACL 情報をキャッシュするかどうかを制御します。

- TRUE に設定すると、サーバーは ACL 情報をキャッシュします。
- FALSE に設定すると、サーバーは ACL 情報をキャッシュしません。

#### **デフォルト値**

TRUE

**構文** ブール

**最大長** 5

**値** 単一値

### **ibm-slapdACLCacheSize**

**説明** ACL キャッシュに保持する項目の最大数。

#### **デフォルト値**

25000

**構文** 整数

**最大長** 11

**値** 単一値

### **ibm-slapdAdminDN**

**説明** ディレクトリー・サーバーの管理者バインド DN。

### デフォルト値

cn=root

構文 DN

最大長 制限なし

値 単一値

### ibm-slapdAdminGroupEnabled

説明 管理グループが現在使用可能になっているかどうかを指定します。TRUE に設定された場合は、サーバーは管理グループのユーザーのログインを許可します。

### デフォルト値

FALSE

構文 ブール

最大長 128

値 単一値

### ibm-slapdAdminPW

説明 ディレクトリー・サーバーの管理者バインド・パスワード。

### デフォルト値

secret

構文 バイナリー

最大長 128

値 単一値

### ibm-slapdAllowAnon

説明 匿名バインドが許可されるかどうかを指定します。

### デフォルト値

True

構文 ブール

最大長 128

値 単一値

### ibm-slapdAllReapingThreshold

説明 接続管理を活動化する前に、サーバーで保守する接続数を指定します。

### デフォルト値

1200

構文 大/小文字を区別するディレクトリー・ストリングの突き合わせ

最大長 1024

値 単一値

### ibm-slapdAnonReapingThreshold

説明 匿名接続の接続管理を活動化する前に、サーバーで保守する接続数を指定します。

デフォルト値

0

構文 大/小文字を区別するディレクトリー・ストリングの突き合わせ

最大長 1024

値 単一値

### **ibm-slapdBoundReapingThreshold**

説明 匿名およびバインド済み接続の接続管理を活動化する前に、サーバーで保守する接続数を指定します。

デフォルト値

1100

構文 大/小文字を区別するディレクトリー・ストリングの突き合わせ

最大長 1024

値 単一値

### **ibm-slapdBulkloadErrors**

説明 bulkload エラー・メッセージが書き込まれる ibmslapd ホスト・マシンのファイル・パスまたはデバイス。

デフォルト値

/var/bulkload.log

構文 大/小文字を区別するディレクトリー・ストリングの突き合わせ

最大長 1024

値 単一値

### **ibm-slapdCachedAttribute**

説明 属性キャッシュにキャッシュされる属性の名前が入っていて、値ごとに 1 つの属性名をもちます。

デフォルト値

なし

構文 ディレクトリー・ストリング

最大長 256

値 複数値

### **ibm-slapdCachedAttributeAutoAdjust**

説明 ibm-slapdCachedAttributeAutoAdjustTime および ibm-slapdCachedAttributeAutoAdjustTimeInterval に定義された構成済み時間間隔でサーバーが属性キャッシュを自動的に調整するかどうかを制御します。

デフォルト値

FALSE

構文 ブール

最大長 5

値 単一値

### **ibm-slapdCachedAttributeAutoAdjustTime**

説明 `ibm-slapdCachedAttributeAutoAdjust` が TRUE に設定された場合、サーバーが属性キャッシュの自動調整を開始する時刻を制御します。

Minimum = T000000

Maximum = T235959

デフォルト値

T000000

構文 24 時間時計

最大長 7

値 単一値

### **ibm-slapdCachedAttributeAutoAdjustTimeInterval**

説明 `ibm-slapdCachedAttributeAutoAdjust` が TRUE に設定された場合、属性キャッシュの自動調整時間間隔を制御します。

Minimum = 1

Maximum = 24

デフォルト値

2

構文 整数

最大長 2

値 単一値

### **ibm-slapdCachedAttributeSize**

説明 属性キャッシュで使用できるメモリー容量 (バイト数)。値が 0 の場合は、属性キャッシュを使用しないことを示します。

デフォルト値

0

構文 整数

最大長 11

値 単一値

### **ibm-slapdChangeLogMaxEntries**

説明 この属性は、RDBM データベースで許容される変更ログ項目の最大数を指定するため、変更ログ・プラグインによって使用されます。それぞれの変更ログに、それ独自の `changeLogMaxEntries` 属性があります。

最小 = 0 (無制限)

Maximum = 2,147,483,647 (32-bit, signed integer)

デフォルト値

0

構文 整数

最大長 11

値 単一値

### **ibm-slapdCLIErrors**

説明 CLI エラー・メッセージが書き込まれる `ibmslapd` ホスト・マシンのファイル・パスまたはデバイス。

デフォルト値

`/var/db2cli.log`

構文 大/小文字を区別するディレクトリー・ストリングの突き合わせ

最大長 1024

値 単一値

### **ibm-slapdConcurrentRW**

説明 これを `TRUE` に設定すると、更新と同時に検索を実行できます。これにより、「ダーティー読み取り」、つまり、結果がデータベースのコミット状態と必ずしも整合しない読み取りを実行できます。

重要: この属性は使用すべきではありません。

デフォルト値

`FALSE`

構文 ブール

最大長 5

値 単一値

### **ibm-slapdDB2CP**

説明 ディレクトリー・データベースのコード・ページを指定します。1208 は、UTF-8 データベースのコード・ページです。

構文 大/小文字を区別するディレクトリー・ストリングの突き合わせ

最大長 11

値 単一値

### **ibm-slapdDBAlias**

説明 DB2 データベース別名

構文 大/小文字を区別するディレクトリー・ストリングの突き合わせ

最大長 8

値 単一値

### **ibm-slapdDbConnections**

説明 DB2 サーバーが DB2 バックエンドに対して専用にする接続の数を指定します。値は、5 & 50 (5 と 50 を含む) でなければなりません。

注: `ODBCCONS` 環境変数は、ディレクティブの値をオーバーライドします。

`ibm-slapdDbConnections` (または `ODBCCONS`) が、5 より小さい、あるいは 50 より大きい場合には、サーバーはそれぞれ 5 または 50 を使用します。複製のために、接続が 1 つ追加して作成さ

れます (複製が定義されていない場合も同様に作成されます)。変更ログのために、2 つの接続が追加されて作成されます (変更ログが使用可能になっている場合)。

#### デフォルト値

15

構文 整数

最大長 50

値 単一値

#### **ibm-slapdDbInstance**

説明 このバックエンドの DB2 データベース・インスタンスを指定します。

#### デフォルト値

ldapdb2

構文 大/小文字を区別するディレクトリー・ストリングの突き合わせ

最大長 8

値 単一値

注: すべての `ibm-slapdRdbmBackend` オブジェクトは、同一の `ibm-slapdDbInstance`、`ibm-slapdDbUserID`、`ibm-slapdDbUserPW`、および DB2 文字セットを使用しなければなりません。

#### **ibm-slapdDbLocation**

説明 バックエンド・データベースが配置されているファイル・システム・パス

構文 大/小文字を区別するディレクトリー・ストリングの突き合わせ

最大長 1024

値 単一値

#### **ibm-slapdDbName**

説明 このバックエンドの DB2 データベース名を指定します。

#### デフォルト値

ldapdb2

構文 大/小文字を区別するディレクトリー・ストリングの突き合わせ

最大長 8

値 単一値

#### **ibm-slapdDbUserID**

説明 このバックエンドについて DB2 データベースにバインドするユーザー名を指定します。

#### デフォルト値

ldapdb2

構文 大/小文字を区別するディレクトリー・ストリングの突き合わせ

最大長 8

値 単一値



注: すべての `ibm-slapdRdbmBackend` オブジェクトは、同一の `ibm-slapdDbInstance`、`ibm-slapdDbUserID`、`ibm-slapdDbUserPW`、および `DB2` 文字セットを使用しなければなりません。

### **ibm-slapdDerefAliases**

説明 検索要求の最大別名参照解除レベルで、クライアント要求に指定されている場合がある `derefAliases` とは無関係です。使用可能な値は **never**、**find**、**search**、および **always** です。

デフォルト値

`always`

構文 ディレクトリー・ストリング

最大長 6

値 単一値

### **ibm-slapdDbUserPW**

説明 このバックエンドについて `DB2` データベースにバインドするユーザー・パスワードを指定します。パスワードは、非暗号化テキストにすることも、`imask` 暗号化を使用することもできます。

デフォルト値

`ldapdb2`

構文 バイナリー

最大長 128

値 単一値

注: すべての `ibm-slapdRdbmBackend` オブジェクトは、同一の `ibm-slapdDbInstance`、`ibm-slapdDbUserID`、`ibm-slapdDbUserPW`、および `DB2` 文字セットを使用しなければなりません。

### **ibm-slapdDigestAdminUser**

説明 LDAP 管理者または管理グループ・メンバーの `Digest MD5` ユーザー名を指定します。`MD5 Digest` 認証を使用して管理者を認識するために使用されます。

デフォルト値

なし

構文 ディレクトリー・ストリング

最大長 512

値 単一値

### **ibm-slapdDigestAttr**

説明 デフォルトの `DIGEST-MD5 username` 属性をオーバーライドします。`DIGEST-MD5 SASL` バインド `username` ルックアップで使用するための属性の名前。この値が指定されない場合、サーバーは `uid` を使用します。

デフォルト値

指定されない場合、サーバーは `uid` を使用します。

構文 ディレクトリー・ストリング

最大長 64

値 単一値

## ibm-slapdDigestRealm

**説明** デフォルトの DIGEST-MD5 レalmをオーバーライドします。使用する `username` およびパスワードをユーザーに通知できるストリング (異なるサーバーに対して異なる `username` とパスワードを使用する場合)。概念としては、ユーザー・アカウントを含めるアカウントの集合名。このストリングは、少なくとも認証を行うホストの名前を含む必要があり、さらに、アクセス権をもつユーザーの集合を示す場合があります。この 1 例は、`registered_users@gotham.news.example.com` です。この属性が指定されない場合、サーバーはそのサーバーの完全修飾 `hostname` を使用します。

### デフォルト値

サーバーの完全修飾 `hostname`

**構文** ディレクトリー・ストリング

**最大長** 1024

**値** 単一値

## ibm-slapdEnableEventNotification

**説明** イベント通知を使用可能にするかどうかを指定します。TRUE または FALSE のいずれかに設定しなければなりません。

FALSE に設定されると、サーバーは、イベント通知を登録するクライアント要求すべてを拒否し、拡張結果 `LDAP_UNWILLING_TO_PERFORM` を返します。

### デフォルト値

TRUE

**構文** ブール

**最大長** 5

**値** 単一値

## ibm-slapdEntryCacheSize

**説明** 項目・キャッシュに保持する項目の最大数。

### デフォルト値

25000

**構文** 整数

**最大長** 11

**値** 単一値

## ibm-slapdErrorLog

**説明** エラー・メッセージが書き込まれるディレクトリー・サーバー・マシンのファイル・パス、またはデバイスを指定します。

### デフォルト値

`/var/ibmslapd.log`

**構文** 大/小文字を区別するディレクトリー・ストリングの突き合わせ

**最大長** 1024

**値** 単一値

### **ibm-slapdESizeThreshold**

**説明** 緊急スレッドを活動化する前の、作業待ち行列上の作業項目数を指定します。

**デフォルト値**

50

**構文** 整数

**最大長** 1024

**値** 単一値

### **ibm-slapdEThreadActivate**

**説明** 緊急スレッドが活動化されることになる条件を指定します。以下の値のいずれかに設定する必要があります。

**S** サイズのみ

**T** 時間のみ

**SOT** サイズまたは時間

**SAT** サイズと時間

**デフォルト値**

SAT

**構文** スtring

**最大長** 1024

**値** 単一値

### **ibm-slapdEThreadEnable**

**説明** 緊急スレッドがアクティブであるかどうかを指定します。

**デフォルト値**

True

**構文** ブール

**最大長** 1024

**値** 単一値

### **ibm-slapdETimeThreshold**

**説明** 緊急スレッドを活動化する前に、作業待ち行列から項目を除去する間隔の時間 (分数) を指定します。

**デフォルト値**

5

**構文** 整数

**最大長** 1024

**値** 単一値

### **ibm-slapdFilterCacheBypassLimit**

**説明** この項目の数を超えて一致する検索フィルターは、検索フィルター・キャッシュには追加されませ

ん。フィルターに一致した項目 ID のリストはこのキャッシュに組み込まれるため、この設定は、メモリーの使用を制限するのに役立ちます。値が 0 の場合には、制限がないことを示します。

**デフォルト値**

100

構文 整数

最大長 11

値 単一値

**ibm-slapdFilterCacheSize**

説明 検索フィルター・キャッシュに保持する項目の最大数を指定します。

**デフォルト値**

25000

構文 整数

最大長 11

値 単一値

**ibm-slapdIdleTimeOut**

説明 接続時になにもアクティビティーがない場合に LDAP 接続をオープンしたままにする最大時間。LDAP 接続のアイドル時間は、接続時の最後のアクティビティーと現在時刻との間の時間 (秒) です。この属性の値よりも長いアイドル時間のため接続が失効すると、LDAP サーバーは LDAP 接続をクリーンアップおよび終了し、他の着信要求で使用できるようにします。

**デフォルト値**

300

構文 整数

長さ 11

カウント

単一

使用法 ディレクトリー操作

ユーザー変更

はい

アクセス・クラス

Critical (重大)

必要 なし

**ibm-slapdIncludeSchema**

説明 スキーマ定義を含むディレクトリー・サーバー・マシンのファイル・パスを指定します。

**デフォルト値**

- /etc/V3.system.at
- /etc/V3.system.oc
- /etc/V3.config.at
- /etc/V3.config.oc

- /etc/V3.ibm.at
- /etc/V3.ibm.oc
- /etc/V3.user.at
- /etc/V3.user.oc
- /etc/V3.ldapsyntaxes
- /etc/V3.matchingrules

**構文** 大/小文字を区別するディレクトリー・ストリングの突き合わせ

**最大長** 1024

**値** 複数值

### **ibm-slapdKrbAdminDN**

**説明** LDAP 管理者の Kerberos ID を指定します (たとえば、ibm-kn=admin1@realm1)。これは、サーバー管理インターフェースにログする際に、Kerberos 認証を使用して管理者を認証するのに使用されます。これは、adminDN および adminPW の代わりに指定することも、adminDN および adminPW に加えて指定することもできます。

**デフォルト値**

事前設定されているデフォルトはありません。

**構文** 大/小文字を区別するディレクトリー・ストリングの突き合わせ

**最大長** 128

**値** 単一値

### **ibm-slapdKrbEnable**

**説明** サーバーが Kerberos をサポートするかどうかを指定します。 TRUE または FALSE のいずれかでなければなりません。

**デフォルト値**

TRUE

**構文** ブール

**最大長** 5

**値** 単一値

### **ibm-slapdKrbIdentityMap**

**説明** Kerberos 識別マッピングを使用するかどうかを指定します。 TRUE または FALSE のいずれかに設定しなければなりません。 TRUE に設定される場合には、クライアントが Kerberos ID で認証される際に、サーバーは一致する Kerberos 認証のあるすべてのローカル・ユーザーを検索し、この接続のバインド信任状にこれらのユーザー DN を追加します。こうすると、LDAP ユーザー DN の ACL が引き続き Kerberos で使用可能になります。

**デフォルト値**

FALSE

**構文** ブール

**最大長** 5

**値** 単一値

## ibm-slapdKrbKeyTab

**説明** LDAP サーバー Kerberos キータブ・ファイルを指定します。このファイルには、Kerberos アカウ  
ントに関連付けられる、LDAP サーバー秘密鍵が含まれます。このファイルは、(サーバー SSL キ  
ー・データベース・ファイルと同様に) 保護されなければなりません。

### デフォルト値

事前設定されているデフォルトはありません。

**構文** 大/小文字を区別するディレクトリー・ストリングの突き合わせ

**最大長** 1024

**値** 単一値

## ibm-slapdKrbRealm

**説明** LDAP サーバーの Kerberos レルムを指定します。これは、root DSE で ldapservicename 属性を公  
開するのに使用されます。1 つの LDAP サーバーを複数の KDC (およびレルム) のアカウント情  
報のリポジトリとして使用できますが、その LDAP は、kerberized サーバーとして、単一レルム  
のメンバーにしかありません。

### デフォルト値

事前設定されているデフォルトはありません。

**構文** 大/小文字を区別しないディレクトリー・ストリングの突き合わせ

**最大長** 256

**値** 単一値

## ibm-slapdLanguageTagsEnabled

**説明** 言語タグをサーバーが許可するかどうかを指定します。この属性の ibmslapd.conf ファイルから読  
み取られる値は FALSE ですが、TRUE に設定することができます。

### デフォルト値

FALSE

**構文** ブール

**最大長** 5

**値** 単一値

## ibm-slapdLdapCrlHost

**説明** クライアント x.509v3 証明書を妥当性検査するために、証明書取り消しリスト (CRL) を含む  
LDAP サーバーのホスト名を指定します。このパラメーターは、CRL 妥当性検査で  
ibm-slapdSslAuth=serverclientauth およびクライアント証明書が発行される際に必要になります。

### デフォルト値

事前設定されているデフォルトはありません。

**構文** 大/小文字を区別しないディレクトリー・ストリングの突き合わせ

**最大長** 256

**値** 単一値

## ibm-slapdLdapCrlPassword

**説明** クライアント x.509v3 証明書を妥当性検査するために、証明書取り消しリスト (CRL) を含む

LDAP サーバーにバインドするのにサーバー・サイドの SSL が使用するパスワードを指定します。このパラメーターは、CRL 妥当性検査で `ibm-slapdSslAuth=serverclientauth` およびクライアント証明書が発行される際に必要になります。

注: CRL を保持する LDAP サーバーが、CRL の対して非認証アクセス (つまり、匿名アクセス) を許可する場合には、`ibm-slapdLdapCrlPassword` は必要ではありません。

#### デフォルト値

事前設定されているデフォルトはありません。

構文 バイナリー

最大長 128

値 単一値

### **ibm-slapdLdapCrlPort**

説明 クライアント x.509v3 証明書を妥当性検査するために、証明書取り消しリスト (CRL) を含む LDAP サーバーに接続するのに使用するポートを指定します。このパラメーターは、CRL 妥当性検査で `ibm-slapdSslAuth=serverclientauth` およびクライアント証明書が発行される際に必要になります。(IP ポートは符号なしの、16 ビット整数で、範囲は 1 - 65535 です。)

#### デフォルト値

事前設定されているデフォルトはありません。

構文 整数

最大長 11

値 単一値

### **ibm-slapdLdapCrlUser**

説明 クライアント x.509v3 証明書を妥当性検査するために、証明書取り消しリスト (CRL) を含む LDAP サーバーにバインドするのにサーバー・サイドの SSL が使用する `bindDN` を指定します。このパラメーターは、CRL 妥当性検査で `ibm-slapdSslAuth=serverclientauth` およびクライアント証明書が発行される際に必要になります。

注: CRL を保持する LDAP サーバーが、CRL の対して非認証アクセス (つまり、匿名アクセス) を許可する場合には、`ibm-slapdLdapCrlUser` は必要ではありません。

#### デフォルト値

事前設定されているデフォルトはありません。

構文 DN

最大長 1000

値 単一値

### **ibm-slapdMasterDN**

説明 マスター・サーバーのバインド DN を指定します。この値は、マスター・サーバーに定義される `replicaObject` の `replicaBindDN` に一致しなければなりません。レプリカを認証するのに Kerberos が使用される場合には、`ibm-slapdMasterDN` は、Kerberos ID の DN 表記を指定しなければなりません (たとえば、`ibm-kn=freddy@realm1`)。Kerberos が使用される場合には、`MasterServerPW` は無視されます。

#### デフォルト値

事前設定されているデフォルトはありません。

構文 DN

最大長 1000

値 単一値

#### ibm-slapdMasterPW

**説明** マスター・レプリカ・サーバーのバインド・パスワードを指定します。この値は、マスター・サーバーに定義される replicaObject の replicaBindDN に一致しなければなりません。レプリカを認証するのに Kerberos が使用される場合には、ibm-slapdMasterDN は、Kerberos ID の DN 表記を指定しなければなりません (たとえば、ibm-kn=freddy@realm1)。Kerberos が使用される場合には、MasterServerPW は無視されます。

#### デフォルト値

事前設定されているデフォルトはありません。

構文 バイナリー

最大長 128

値 単一値

#### ibm-slapdMasterReferral

**説明** マスター・レプリカ・サーバーの URL を指定します。例:

```
ldap://master.us.ibm.com
```

SSL のみに設定されるセキュリティーの場合:

```
ldaps://master.us.ibm.com:636
```

none にセキュリティーが設定されており、標準外ポートを使用している場合:

```
ldap://master.us.ibm.com:1389
```

#### デフォルト値

none

構文 大/小文字を区別しないディレクトリー・ストリングの突き合わせ

最大長 256

値 単一値

#### ibm-slapdMaxEventsPerConnection

**説明** 接続ごとに登録できるイベント通知の最大数を指定します。

最小 = 0 (無制限)

Maximum = 2,147,483,647

#### デフォルト値

100

構文 整数

最大長 11

値 単一値



### **ibm-slapdMaxEventsTotal**

**説明** すべての接続で登録できるイベント通知の最大総数を指定します。

最小 = 0 (無制限)  
Maximum = 2,147,483,647

**デフォルト値**

0

**構文** 整数

**最大長** 11

**値** 単一値

### **ibm-slapdMaxNumOfTransactions**

**説明** サーバーごとのトランザクションの最大数を指定します。

最小 = 0 (無制限)  
Maximum = 2,147,483,647

**デフォルト値**

20

**構文** 整数

**最大長** 11

**値** 単一値

### **ibm-slapdMaxOpPerTransaction**

**説明** トランザクションごとの操作の最大数を指定します。

最小 = 0 (無制限)  
Maximum = 2,147,483,647

**デフォルト値**

5

**構文** 整数

**最大長** 11

**値** 単一値

### **ibm-slapdMaxPendingChangesDisplayed**

**説明** 表示する保留の変更の最大数。

**デフォルト値**

200

**構文** 整数

**最大長** 11

**値** 単一値

### **ibm-slapdMaxTimeLimitOfTransactions**

**説明** 保留トランザクションの最大タイムアウト値を指定します。

最小 = 0 (無制限)  
Maximum = 2,147,483,647

デフォルト値  
300  
構文 整数  
最大長 11  
値 単一値

### ibm-slapdPagedResAllowNonAdmin

説明 非管理者が検索要求でページ結果要求をバインドできるようにサーバーが許可するかどうかを指定します。 `ibmslapd.conf` ファイルから読み取られる値が `FALSE` である場合には、サーバーは、管理者権限のあるユーザーにより実行依頼されるクライアント要求のみ処理します。クライアントが検索操作でページ結果を要求する場合で、クライアントに管理者権限がない場合、およびこの属性について `ibmslapd.conf` ファイルから読み取られる値が `FALSE` の場合には、サーバーは、戻りコード `insufficientAccessRights; no searching or paging will be performed` をクライアントに戻します。

デフォルト値  
FALSE  
構文 ブール  
長さ 5  
カウント  
単一  
使用法 ディレクトリー操作  
ユーザー変更  
はい  
アクセス・クラス  
Critical (重大)  
オブジェクト・クラス  
`ibm-slapdRdbmBackend`  
必要 なし

### ibm-slapdPagedResLmt

説明 同時にアクティブ状態にできる未処理のページ検索結果要求の最大数。範囲 = 0.... クライアントがページ結果操作を要求する際に、最大数の未処理ページ結果が現時点でアクティブ状態の場合、サーバーは、クライアントに戻りコード `busy; no searching or paging will be performed` を戻します。

デフォルト値  
3  
構文 整数  
長さ 11  
カウント  
単一  
使用法 ディレクトリー操作

## ユーザー変更

はい

## アクセス・クラス

Critical (重大)

必要 なし

## オブジェクト・クラス

ibm-slapdRdbmBackend

## ibm-slapdPageSizeLmt

**説明** クライアント検索要求で指定されるページ・サイズにかかわらず、ページ結果制御が指定される際に個々のページの検索から戻される項目の最大数。範囲 = 0... クライアントがページ・サイズを渡した場合には、クライアント値の小さい方の値および `ibmslapd.conf` から読み取られる値が使用されます。

## デフォルト値

50

構文 整数

長さ 11

## カウント

単一

**使用法** ディレクトリー操作

## ユーザー変更

はい

## アクセス・クラス

Critical (重大)

必要 なし

## オブジェクト・クラス

ibm-slapdRdbmBackend

## ibm-slapdPlugin

**説明** プラグインは、サーバーの機能を拡張する、動的ロード・ライブラリーです。 `ibm-slapdPlugin` 属性は、プラグイン・ライブラリーをロードおよび初期化する方法を指定します。構文:

```
keyword filename init_function [args...]
```

構文は、ライブラリー命名規則のために、それぞれのプラットフォームに応じてわずかに異なります。

ほとんどのプラグインはオプションですが、RDBM バックエンド・プラグインはすべての RDBM バックエンドで必要です。

## デフォルト値

```
database /bin/libback-rdbm.dll rdbm_backend_init
```

構文 大/小文字を区別するディレクトリー・ストリングの突き合わせ

最大長 2000

値 複数値

## ibm-slapdPort

**説明** 非 SSL 接続で使用される TCP/IP ポートを指定します。これは、ibm-slapdSecurePort と同じ値に指定することはできません。(IP ポートは符号なしの、16 ビット整数で、範囲は 1 - 65535 です。)

**デフォルト値**

389

**構文** 整数

**最大長** 5

**値** 単一値

## ibm-slapdPWEncryption

**説明** ユーザー・パスワードがディレクトリーに保管される前の、エンコード・メカニズムを指定します。none、imask、crypt、または sha のいずれかに指定しなければなりません (SHA-1 エンコードを取得するには、キーワード **sha** を指定しなければなりません)。SASL cram-md5 バインドを正常に実行するには、値を none に指定しなければなりません。

**デフォルト値**

none

**構文** 大/小文字を区別しないディレクトリー・ストリングの突き合わせ

**最大長** 5

**値** 単一値

## ibm-slapdReadOnly

**説明** この属性は、通常、ディレクトリー・バックエンドにのみ適用されます。これは、バックエンドに書き込みができるかどうかを指定します。TRUE または FALSE のいずれかに指定しなければなりません。指定がない場合は、デフォルトとして FALSE になります。TRUE に設定されると、サーバーは、読み取り専用データベースでデータを変更するクライアント要求に対する応答として LDAP\_UNWILLING\_TO\_PERFORM (0x35) を戻します。

**デフォルト値**

FALSE

**構文** ブール

**最大長** 5

**値** 単一値

## ibm-slapdReferral

**説明** ローカル接尾部が要求に一致しない場合に戻される参照 LDAP URL を指定します。これは、上位参照に使用されます (つまり、接尾部は、サーバーの命名コンテキストには含まれません)。

**デフォルト値**

事前設定されているデフォルトはありません。

**構文** 大/小文字を区別するディレクトリー・ストリングの突き合わせ

**最大長** 32700

**値** 複数值

## ibm-slapdReplDbConns

**説明** 複製により使用されるデータベース接続の最大数。

**デフォルト値**

4

**構文** 整数

**最大長** 11

**値** 単一値

## ibm-slapdReplicaSubtree

**説明** 複製されたサブツリーの DN を識別します。

**構文** DN

**最大長** 1000

**値** 単一値

## ibm-slapdSchemaAdditions

**説明** `ibm-slapdSchemaAdditions` 属性は、どのファイルが新しいスキーマ項目を保持しているかを明示的に識別するために使用されます。これは、デフォルト値 `/etc/V3.modifiedschema` に設定されます。この属性が定義されていない場合には、サーバーは、前のリリースと同様に最後の `ibm-slapdIncludeSchema` ファイルを使用します。

バージョン 3.2 以前では、`slapd.conf` にある最後の `includeSchema` 項目は、サーバーがクライアントから追加要求を受け取った場合に、新規のスキーマ項目が追加されたファイルでした。通常、最終 `includeSchema` は `V3.modifiedschema` ファイルであり、これは、この目的のためだけにインストールされている空ファイルです。

注: これは、新規項目しか保管しないため、名前変更をすると、まぎらわしくなります。既存のスキーマ項目への変更は、オリジナル・ファイルでなされます。

**デフォルト値**

`/etc/V3.modifiedschema`

**構文** 大/小文字を区別するディレクトリー・ストリングの突き合わせ

**最大長** 1024

**値** 単一値

## ibm-slapdSchemaCheck

**説明** 追加/変更/削除操作での、スキーマ検査メカニズムを指定します。これは、V2、V3、または `V3_lenient` に指定されなければなりません。

- V2 - v2 および v2.1 検査を保持。移行目的では、これをお勧めします。
- V3 - v3 検査を実行。
- `V3_lenient` - 親オブジェクト・クラスすべてを必要としません。項目を追加する際には、直接のオブジェクト・クラスだけが必要になります。

**デフォルト値**

`V3_lenient`

**構文** 大/小文字を区別しないディレクトリー・ストリングの突き合わせ

最大長 10

値 単一値

### **ibm-slapdSecurePort**

**説明** SSL 接続に使用される TCP/IP ポートを指定します。これは、ibm-slapdPort と同じ値に指定することはできません。(IP ポートは符号なしの、16 ビット整数で、範囲は 1 - 65535 です。)

**デフォルト値**

636

**構文** 整数

最大長 5

値 単一値

### **ibm-slapdSecurity**

**説明** SSL 接続および TLS 接続を使用可能にします。none、SSL、または SSLOnly、TLS、または SSLTLS のいずれかでなければなりません。

- none - サーバーは、非セキュア・ポートでのみ listen する。
- SSL - サーバーは、SSL および非 SSL ポートの両方で listen する。セキュア・ポートは、セキュア接続を使用する唯一の方法です。
- SSLOnly - サーバーは SSL ポートでのみ listen する。
- TLS - サーバーは、非セキュア・ポートでのみ listen する。StartTLS 拡張操作は、セキュア接続を使用する唯一の方法です。
- SSLTLS - サーバーは、デフォルトとセキュア・ポートの両方で listen する。StartTLS 拡張操作を使用して、デフォルト・ポート上のセキュア接続を取得することができます。また、クライアントはセキュア・ポートを直接使用することもできます。セキュア・ポート上で StartTLS を送信すると、メッセージ LDAP\_OPERATIONS\_ERROR が戻されます。

**デフォルト値**

none

**構文** 大/小文字を区別しないディレクトリー・ストリングの突き合わせ

最大長 7

値 単一値

### **ibm-slapdServerId**

**説明** 複製で使用するサーバーを識別します。

**構文** 大/小文字を区別する IA5 ストリング

最大長 240

値 単一値

### **ibm-slapdSetenv**

**説明** サーバーは、始動時に、ibm-slapdSetenv のすべての値について **putenv()** を実行し、サーバー実行時環境を変更します。シェル変数 (%PATH% や \$LANG など) は、拡張されません。

**デフォルト値**

事前設定されているデフォルトはありません。

構文 大/小文字を区別するディレクトリー・ストリングの突き合わせ

最大長 2000

値 複数值

### ibm-slapdSizeLimit

説明 クライアント要求で指定されたサイズ制限にかかわらず、検索から戻される項目の最大数を指定します (範囲 = 0...)。クライアントが制限を渡した場合には、クライアント値の小さい方の値および **ibmslapd.conf** から読み取られる値が使用されます。クライアントが制限を渡しておらず、admin DN としてバインドした場合には、この制限は無制限になります。クライアントが制限を渡しておらず、admin DN としてバインドしていない場合には、この制限は **ibmslapd.conf** ファイルから読み取られる値になります。 0 = 無制限。

デフォルト値

500

構文 整数

最大長 12

値 単一値

### ibm-slapdSortKeyLimit

説明 単一の検索要求で指定できるソート条件 (キー) の最大数。範囲 = 0... クライアントが、検索要求で許容されている制限より多いソート・キーを渡した場合で、ソート検索制御重大性が FALSE の場合には、サーバーは、**ibmslapd.conf** ファイルから読み取られる値を優先し、この制限に達した後に検出されるソート・キーはすべて無視します。クライアントが、検索要求で許容されている制限より多いソート・キーを渡した場合で、ソート検索制御重大性が TRUE の場合には、サーバーは、戻りコード **adminLimitExceeded** - no searching or sorting will be performed をクライアントに戻します。

デフォルト値

3

構文 cis

長さ 11

カウント

単一

使用法 ディレクトリー操作

ユーザー変更

はい

アクセス・クラス

Critical (重大)

オブジェクト・クラス

ibm-slapdRdbmBackend

必要 なし

### ibm-slapdSortSrchAllowNonAdmin

説明 検索要求のソートに関する非管理者バインドをサーバーが許可するかどうかを指定します。

ibmslapd.conf ファイルから読み取られる値が FALSE である場合には、サーバーは、管理者権限のあるユーザーにより実行依頼されるクライアント要求のみ処理します。クライアントが検索操作でソートを要求する場合で、クライアントに管理者権限がない場合、およびこの属性について ibmslapd.conf ファイルから読み取られる値が FALSE の場合には、サーバーは、戻りコード insufficientAccessRights; no searching or sorting will be performed をクライアントに戻します。

#### デフォルト値

FALSE

構文 ブール

長さ 5

カウント

単一

使用法 ディレクトリー操作

ユーザー変更

はい

アクセス・クラス

Critical (重大)

オブジェクト・クラス

ibm-slapdRdbmBackend

必要 なし

### ibm-slapdSslAuth

説明 SSL 接続の認証タイプを、serverauth または serverclientauth のいずれかで指定します。

- serverauth - クライアントでのサーバー認証をサポートします。これはデフォルトです。
- serverclientauth - サーバーおよびクライアント認証の両方をサポートします。

デフォルト値

serverauth

構文 大/小文字を区別しないディレクトリー・ストリングの突き合わせ

最大長 16

値 単一値

### ibm-slapdSslCertificate

説明 キー・データベース・ファイルで、サーバー個人証明書を識別するラベルを指定します。このラベルは、**gsk4ikm** アプリケーションでサーバー秘密鍵および証明書が作成される際に指定されます。ibm-slapdSslCertificate が指定されない場合には、LDAP サーバーは、キー・データベース・ファイルで定義されているデフォルト秘密鍵を SSL 接続に使用します。

デフォルト値

事前設定されているデフォルトはありません。

構文 大/小文字を区別するディレクトリー・ストリングの突き合わせ

最大長 128

値 単一値



## ibm-slapdSslCipherSpec

サーバーにアクセスするクライアントの SSL 暗号化の方式を指定します。以下のいずれかに設定する必要があります。

表 6. SSL 暗号化の方式

| 属性            | 暗号化レベル                                       |
|---------------|----------------------------------------------|
| TripleDES-168 | 168 ビット・キーおよび SHA-1 MAC を使用した Triple-DES 暗号化 |
| DES-56        | 56 ビット・キーおよび SHA-1 MAC を使用した DES 暗号化         |
| RC4-128-SHA   | 128 ビット・キーおよび SHA-1 MAC を使用した RC4 暗号化        |
| RC4-128-MD5   | 128 ビット・キーおよび MD5 MAC を使用した RC4 暗号化          |
| RC2-40-MD5    | 40 ビット・キーおよび MD5 MAC を使用した RC4 暗号化           |
| RC4-40-MD5    | 40 ビット・キーおよび MD5 MAC を使用した RC4 暗号化           |
| AES           | AES 暗号化                                      |

構文 IA5 ストリング

最大長 30

## ibm-slapdSslKeyDatabase

説明 LDAP サーバー SSL キー・データベース・ファイルへのファイル・パスを指定します。このキー・データベース・ファイルは、LDAP クライアントからの SSL 接続を処理し、レプリカ LDAP サーバーへのセキュア SSL 接続を作成するのに使用されます。

デフォルト値

/etc/key.kdb

構文 大/小文字を区別するディレクトリー・ストリングの突き合わせ

最大長 1024

値 単一値

## ibm-slapdSslKeyDatabasePW

説明 ibm-slapdSslKeyDatabase パラメーターで指定されている、LDAP サーバー SSL キー・データベース・ファイルに関連するパスワードを指定します。LDAP サーバー・キー・データベース・ファイルに関連パスワード stash ファイルがある場合には、ibm-slapdSslKeyDatabasePW パラメーターは省略することも、none に設定することもできます。

注: このパスワードの stash ファイルは、キー・データベース・ファイルと同じディレクトリーに入っていないければならず、キー・データベース・ファイルと同じファイル名で、拡張子 .kdb の代わりに .sth を付けなければなりません。

デフォルト値

none

構文 バイナリー

最大長 128

値 単一値

### **ibm-slapdSslKeyRingFile**

**説明** LDAP サーバーの SSL キー・データベース・ファイルへのパス。このキー・データベース・ファイルは、LDAP クライアントからの SSL 接続を処理し、レプリカ LDAP サーバーへのセキュア SSL 接続を作成するのに使用されます。

**デフォルト値**

key.kdb

**構文** 大/小文字を区別するディレクトリー・ストリングの突き合わせ

最大長 1024

値 単一値

### **ibm-slapdSuffix**

**説明** このバックエンドに保管される命名コンテキストを指定します。

注: これは、オブジェクト・クラスと同じ名前になります。

**デフォルト値**

事前設定されているデフォルトはありません。

**構文** DN

最大長 1000

値 複数値

### **ibm-slapdSupportedWebAdmVersion**

**説明** この属性は、このサーバーの cn=configuration をサポートする Web 管理ツールの最も古いバージョンを定義します。

**デフォルト値**

**構文** ディレクトリー・ストリング

最大長

値 単一値

### **ibm-slapdSysLogLevel**

**説明** slapd.errors ファイルにデバッグおよび演算統計をログ記録するレベルを指定します。l、m、または h に指定しなければなりません。

- h - 高 (ほとんどの情報を提供)
- m - 中 (デフォルト)
- l - 低 (最低限の情報を提供)

**デフォルト値**

m

**構文** 大/小文字を区別しないディレクトリー・ストリングの突き合わせ

最大長 1

値 単一値

### **ibm-slapdTimeLimit**

**説明** クライアント要求で指定された時間制限にかかわらず、検索要求にかける最大時間を秒数で指定します。クライアントが制限を渡した場合には、クライアント値の小さい方の値および **ibmslapd.conf** から読み取られる値が使用されます。クライアントが制限を渡しておらず、admin DN としてバインドした場合には、この制限は無制限になります。クライアントが制限を渡しておらず、admin DN としてバインドしていない場合には、この制限は **ibmslapd.conf** ファイルから読み取られる値になります。 0 = 無制限。

**デフォルト値**

900

**構文** 整数

**最大長**

値 単一値

### **ibm-slapdTransactionEnable**

**説明** トランザクション・プラグインがロードされたものの **ibm-slapdTransactionEnable** が FALSE に設定されている場合には、サーバーはすべての StartTransaction 要求を拒否し、応答 LDAP\_UNWILLING\_TO\_PERFORM を返します。

**デフォルト値**

TRUE

**構文** ブール

**最大長** 5

値 単一値

### **ibm-slapdUseProcessIdPw**

**説明** TRUE に設定すると、サーバーは **ibm-slapdDbUserID** および **ibm-slapdDbUserPW** 属性を無視し、独自のプロセス信任状を使用して DB2 を認証します。

**デフォルト値**

FALSE

**構文** ブール

**最大長** 5

値 単一値

### **ibm-slapdVersion**

**説明** IBM Slapd バージョン番号

**デフォルト値**

**構文** 大/小文字を区別するディレクトリー・ストリングの突き合わせ

**最大長**

値 単一値

## ibm-slapedWriteTimeout

**説明** ブロックされた書き込みのタイムアウト値 (秒数) を指定します。時間制限に達すると、接続は除去されます。

**デフォルト値**

120

**構文** 整数

**最大長** 1024

**値** 単一値

## objectClass

**説明** objectClass 属性の値は、項目で表されるオブジェクトの種類を説明します。

**構文** ディレクトリー・ストリング

**最大長** 128

**値** 複数値

## オブジェクト ID (OID)

以下の情報では、Directory Server で使用されるオブジェクト ID (OID) について述べています。

- 以下の表に示された OID が Directory Server で使用されます。これらの OID は root DSE 中にあります。この root DSE 項目には、サーバー自身に関する情報が入っています。下記の制御および拡張操作に関連した要求データおよび応答データのエンコードも含め、拡張操作および制御用のオブジェクト ID (OID) の詳細は、Tivoli Software Information Center を参照してください。

## 制御

表 7. サポートされる Directory Server 制御

| 名前                        | OID                      | 最も古いか、または i5/OS または OS/400 リリース | 最も古い IBM Tivoli Directory Server バージョン | 説明                                                                                |
|---------------------------|--------------------------|---------------------------------|----------------------------------------|-----------------------------------------------------------------------------------|
| DSA IT の管理                | 2.16.840.1.1137.30.3.4.2 | V4R5                            | V3.2                                   | 参照項目を正規の項目として処理します。                                                               |
| 57 ページの『トランザクション』         | 1.3.18.0.2.10.5          | V4R5                            | V3.2                                   | 操作にトランザクションの一部としてマークを付けます。                                                        |
| os400-dltusrprf-ownobjopt | 1.3.18.0.2.10.8          | V5R2                            |                                        | オブジェクト所有者用のユーザー・プロファイル削除オプション。詳しくは、94 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。 |

表 7. サポートされる Directory Server 制御 (続き)

| 名前                     | OID                                                            | 最も古いか、または i5/OS または OS/400 リリース | 最も古い IBM Tivoli Directory Server バージョン | 説明                                                                                                   |
|------------------------|----------------------------------------------------------------|---------------------------------|----------------------------------------|------------------------------------------------------------------------------------------------------|
| os400-dltusrprf-pgpopt | 1.3.18.0.2.10.9                                                | V5R2                            |                                        | 1 次グループ用のユーザー・プロファイル削除オプション。詳しくは、94 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。                      |
| ソート検索                  | 1.2.840.113556.1.4.473 (要求)<br>および 1.2.840.113556.1.4.474 (応答) | V5R2 (PTF 付)                    | V4.1                                   | 項目をクライアントに戻す前に検索結果をソートします。53 ページの『検索パラメーター』を参照してください。                                                |
| ページ検索                  | 1.2.840.113556.1.4.319                                         | V5R2 (PTF 付)                    | V4.1                                   | 検索結果をクライアントにすべて一度に戻す代わりにページ内に戻します。53 ページの『検索パラメーター』を参照してください。                                        |
| ツリーの削除制御               | 1.2.840.113556.1.4.805                                         | V5R3                            | V5.1                                   | この制御は、削除要求に付加され、指定した項目およびすべての派生項目を削除することを示します。ユーザーは、ディレクトリー管理者である必要があります。削除する項目は複製コンテキストになることはできません。 |
| 86 ページの『パスワード・ポリシー』    | 1.3.6.1.4.1.42.2.27.8.5.1                                      | V5R3                            | V5.1                                   | 余分のパスワード・ポリシー・エラー情報をクライアントに戻します。                                                                     |
| サーバー管理                 | 1.3.18.0.2.10.15                                               | V5R3                            | V5.1                                   | 通常拒否される修理操作を管理者が実行することを許可します (たとえば、読み取り専用レプリカの更新、静止サーバーの更新、または特定の操作属性の設定)。                           |

表7. サポートされる Directory Server 制御 (続き)

| 名前              | OID                      | 最も古いか、または i5/OS または OS/400 リリース | 最も古い IBM Tivoli Directory Server バージョン | 説明                                                                               |
|-----------------|--------------------------|---------------------------------|----------------------------------------|----------------------------------------------------------------------------------|
| 71 ページの『プロキシ許可』 | 2.16.840.1.113730.3.4.18 | V5R4                            | V5.2                                   | クライアント・アプリケーションはディレクトリーに対して自身の ID でバインドできますが、他のユーザーの代理としても操作の実行が許可されます。          |
| 複製サプライヤー・バインド制御 | 1.3.18.0.2.10.18         | V5R3                            | V5.2                                   | サプライヤーがゲートウェイ・サーバーである場合は、この制御はサプライヤーによって追加されます。                                  |
| 最新表示入力制御        | 1.3.18.0.2.10.24         | V6R1                            | V6.0                                   | この制御は、複製競合解決をサポートするためにサーバーによって内部で使用されます。                                         |
| 複製競合解決なし        | 1.3.19.0.2.10.27         | V6R1                            | V6.0                                   | この制御は、複製競合解決をサポートするためにサーバーによって内部で使用されます。                                         |
| 複製しない制御         | 1.3.19.0.2.10.23         | V6R1                            | V6.0                                   | この制御を管理者が指定することによって、関連操作を他のサーバーに複製しないことを要求することができます。この制御には、制御値はありません。            |
| 監査制御            | 1.3.18.0.2.10.22         | V6R1                            | V6.0                                   | この制御は、複数のサーバーを経由してルーティングされる要求の発信元のクライアントを識別するために、プロキシ・サーバーなどの許可クライアントによって使用されます。 |

表7. サポートされる Directory Server 制御 (続き)

| 名前             | OID              | 最も古いか、または i5/OS または OS/400 リリース | 最も古い IBM Tivoli Directory Server バージョン | 説明                                                                                                                                                       |
|----------------|------------------|---------------------------------|----------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------|
| グループ許可制御       | 1.3.18.0.2.10.21 | V6R1                            | V6.0                                   | この制御は、ローカル・サーバーのメンバーシップではなく、クライアントの許可 ID のグループ・メンバーシップを表明するために使用されます。これは、プロキシの許可制御と一緒に使用されます。                                                            |
| 変更グループのみの制御    | 1.3.18.0.2.10.25 | V6R1                            | V6.0                                   | この制御を使用する操作 (delete または modrdn/dn) は、dn の削除も名前変更も行わない特殊タイプの操作として、バックエンド・サーバーによって認識されます。つまり、dn が置かれているグループは、そのメンバーシップ内のターゲット dn への参照の削除または名前変更のために変更されます。 |
| グループ参照整合性の省略制御 | 1.3.18.0.2.10.26 | V6R1                            | V6.0                                   | 削除要求または modrdn 要求上のグループ参照整合性処理を省略します。ACI およびグループ・メンバーシップは、変更を反映するように更新されることはありません。                                                                       |
| AES バインド制御     | 1.3.18.0.2.10.28 | V6R1                            | V6.0                                   | この制御では、IBM Tivoli Directory Server は、AES を使ってすでに暗号化されたパスワードで、コンシューマー・サーバーに更新を送信することができます。                                                                |

## 拡張操作

表 8. 拡張操作の OID

| 名前          | OID                    | 最も古い i5/OS<br>または OS/400 リ<br>リース | 最も古い<br>IBM Tivoli<br>Directory<br>Server パー<br>ジョン | 説明                                           |
|-------------|------------------------|-----------------------------------|-----------------------------------------------------|----------------------------------------------|
| イベントの登録     | 1.3.18.0.2.12.1        | V4R5                              | V3.2                                                | Tivoli Directory Server イベント・サポートのイベントの登録を要求 |
| イベントの抹消     | 1.3.18.0.2.12.3        | V4R5                              | V3.2                                                | イベント登録要求の使用のために登録されたイベントの抹消                  |
| トランザクションの開始 | 1.3.18.0.2.12.5        | V4R5                              | V3.2                                                | トランザクション・コンテキストの開始                           |
| トランザクションの終了 | 1.3.18.0.2.12.6        | V4R5                              | V3.2                                                | トランザクション・コンテキスト (commit/rollback) の終了        |
| DN 正規化要求    | 1.3.18.0.2.12.30       | V5R3                              | V5.1                                                | DN または一連の DN の正規化の要求                         |
| StartTLS    | 1.3.6.1.4.1.1466.20037 | V5R4                              | V5.2                                                | Transport Layer Security の開始要求               |

クライアントにより開始されることを意図していない追加拡張操作は定義されています。これらの操作は ldapexop ユーティリティーまたは Web 管理ツールにより実行される操作を介して使用されます。これらの操作、およびそれらを開始するために必要な権限は、以下にリストされています。

表 9. 追加の拡張操作

| 名前    | OID              | 最も古い i5/OS<br>リリース | 最も古い<br>IBM Tivoli<br>Directory<br>Server パー<br>ジョン | 説明                                                                                                                                                                                  |
|-------|------------------|--------------------|-----------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 複製の制御 | 1.3.18.0.2.12.16 | V5R3               | V5.1                                                | この操作は、その発行先のサーバー上での要求アクションを実行し、複製トポロジ内でのそのサーバーの下のすべてのコンシューマーに呼び出しをカスケードします。クライアントはディレクトリー管理者であるか、関連した複製コンテキスト用の <code>ibm-replicagroup =default</code> オブジェクトへの書き込み権限を持っている必要があります。 |



表 9. 追加の拡張操作 (続き)

| 名前         | OID              | 最も古い i5/OS リリース | 最も古い IBM Tivoli Directory Server バージョン | 説明                                                                                                                                                                                                                      |
|------------|------------------|-----------------|----------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 複製キューの制御   | 1.3.18.0.2.12.17 | V5R3            | V5.1                                   | この操作では、指定した合意に対して <code>already replicated</code> としてアイテムにマークを付けます。この操作は、クライアントにレプリカ合意に対する書き込み権限があるときのみ許可されます。                                                                                                          |
| 静止または静止解除  | 1.3.18.0.2.12.19 | V5R3            | V5.1                                   | この操作は、サブツリーがクライアント更新を受け入れない状態 (またはこの状態を終了する状態) にします。ただし、サーバー管理制御が存在するディレクトリー管理者として認証済みのクライアントからの更新は例外です。クライアントはディレクトリー管理者として認証済みであるか、関連した複製コンテキスト用の <code>ibm-replicagroup =default</code> オブジェクトへの書き込み権限を持っている必要があります。 |
| 制御複製のカスケード | 1.3.18.0.2.12.15 | V5R3            | V5.1                                   | この操作は、その発行先のサーバー上での要求アクションを実行し、複製トポロジー内でそのサーバーの下のすべてのコンシューマーに呼び出しをカスケードします。クライアントはディレクトリー管理者であるか、関連した複製コンテキスト用の <code>ibm-replicagroup =default</code> オブジェクトへの書き込み権限を持っている必要があります。                                     |
| 構成の更新      | 1.3.18.0.2.12.28 | V5R3            | V5.1                                   | この操作は、サーバーに、その構成から指定した設定を再読み取りさせるために使用されます。この操作は、クライアントがディレクトリー管理者であるあるときのみ許可されます。                                                                                                                                      |
| 接続要求の強制終了  | 1.3.18.0.2.12.35 | V5R4            | V5.2                                   | サーバー上の接続を強制終了する要求呼び出し元は、ディレクトリー管理者である必要があります。                                                                                                                                                                           |
| 固有属性要求     | 1.3.18.0.2.12.44 | V5R4            | V5.2                                   | 指定された属性名のすべての非固有値のリストをサーバーによって戻す要求 252 ページの『 <code>ldapexop</code> 』の <code>-op uniqueattr</code> を参照してください。呼び出し元は、ディレクトリー管理者である必要があります。                                                                                |

表 9. 追加の拡張操作 (続き)

| 名前           | OID              | 最も古い i5/OS リリース | 最も古い IBM Tivoli Directory Server バージョン | 説明                                                                                                                                                                       |
|--------------|------------------|-----------------|----------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 属性タイプ要求      | 1.3.18.0.2.12.46 | V5R4            | V5.2                                   | 特別な特性をもつ属性の名前のリストをサーバーによって戻す要求 252 ページの『Idapexop』の <code>-op getattributes</code> を参照してください。                                                                             |
| ユーザー・タイプ要求   | 1.3.18.0.2.12.37 | V5R3            | V5.2                                   | バインドされたユーザーのユーザー・タイプを取得するように要求します。                                                                                                                                       |
| 複製エラー・ログ拡張操作 | 1.3.18.0.2.12.56 | V6R1            | V6.0                                   | IBM 複製エラー制御拡張要求は、複製エラー・ログの表示、ログからの項目の再試行、またはログ項目の削除のために使用されます。呼び出し元は、ディレクトリー管理者であるか、または関連した複製コンテキスト用の <code>ibm-replicagroup=default</code> オブジェクトへの書き込み権限を持っている必要があります。 |
| グループ評価拡張操作   | 1.3.18.0.2.12.50 | V6R1            | V6.0                                   | ある特定のユーザーの所属先のすべてのグループを要求します。呼び出し元は、ディレクトリー管理者である必要があります。                                                                                                                |
| 複製トポロジー拡張操作  | 1.3.18.0.2.12.54 | V6R1            | V6.0                                   | 特定の複製コンテキストのもとの複製トポロジー関連の項目の複製をトリガーします。呼び出し元は、ディレクトリー管理者であるか、または関連した複製コンテキスト用の <code>ibm-replicagroup=default</code> オブジェクトへの書き込み権限を持っている必要があります。                        |
| アカウント状況拡張操作  | 1.3.18.0.2.12.58 | V6R1            | V6.0                                   | この拡張操作は、 <code>userPassword</code> 属性を入れた項目の DN をサーバーに送信します。するとサーバーから、オープン、ロック済み、または期限切れの、照会したユーザー・アカウントのいずれかの状況が返送されます。呼び出し元は、ディレクトリー管理者である必要があります。                     |

表 9. 追加の拡張操作 (続き)

| 名前          | OID              | 最も古い i5/OS リリース | 最も古い IBM Tivoli Directory Server バージョン | 説明                                                                                                                                                             |
|-------------|------------------|-----------------|----------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ファイルの取得拡張操作 | 1.3.18.0.2.12.73 | V6R1            | V6.0                                   | サーバー上の指定されたファイルの内容を戻します。呼び出し元は、ディレクトリー管理者である必要があります。LostAndFound ログと Tivoli Directory Server 監査ログをサポートします。監査ログは、Directory Server の i5/OS セキュリティー監査機能とは関係ありません。 |
| 行の取得拡張操作    | 1.3.18.0.2.12.22 | V6R1            | V6.0                                   | ログ・ファイルからの行の取得を要求します。呼び出し元は、ディレクトリー管理者である必要があります。LostAndFound ログと Tivoli Directory Server 監査ログをサポートします。監査ログは、Directory Server の i5/OS セキュリティー監査機能とは関係ありません。    |
| 行数の取得拡張操作   | 1.3.18.0.2.12.24 | V6R1            | V6.0                                   | ログ・ファイルの行数を要求します。呼び出し元は、ディレクトリー管理者である必要があります。LostAndFound ログと Tivoli Directory Server 監査ログをサポートします。監査ログは、Directory Server の i5/OS セキュリティー監査機能とは関係ありません。        |

## サポートされている使用可能な機能

以下の表には、サポートされて使用可能な機能の OID を示します。これらの OID を使用して、特定のサーバーでこれらの機能がサポートされているかどうかを調べることができます。

表 10. サポートされている使用可能な機能の OID

| 名前        | OID             | 説明                                                                 |
|-----------|-----------------|--------------------------------------------------------------------|
| 拡張複製モデル   | 1.3.18.0.2.32.1 | サブツリーとカスケード複製を含めて、IBM Directory Server v5.1 に導入された複製モデルを識別します。     |
| 項目チェックサム  | 1.3.18.0.2.32.2 | このサーバーが ibm-entrychecksum と ibm-entrychecksumop の機能をサポートすることを示します。 |
| 項目 UUID   | 1.3.18.0.2.32.3 | このサーバーが ibm-entryuuid 操作属性をサポートすることを識別します。                         |
| フィルター ACL | 1.3.18.0.2.32.4 | このサーバーが IBM Filter ACL モデルをサポートすることを識別します。                         |

表 10. サポートされている使用可能な機能の OID (続き)

| 名前                                                             | OID              | 説明                                                                                                                                                                                                                                                                                                 |
|----------------------------------------------------------------|------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| パスワード・ポリシー                                                     | 1.3.18.0.2.32.5  | このサーバーがパスワード・ポリシーをサポートすることを識別します。                                                                                                                                                                                                                                                                  |
| DN によるソート                                                      | 1.3.18.0.2.32.6  | DN によってソートするために、このサーバーが <code>ibm-slappedDn</code> 属性の使用をサポートすることを識別します。                                                                                                                                                                                                                           |
| 管理グループの代行                                                      | 1.3.18.0.2.32.8  | サーバーは、構成バックエンドに指定された管理者グループへのサーバー管理の代行をサポートします。                                                                                                                                                                                                                                                    |
| サービス妨害の予防                                                      | 1.3.18.0.2.32.9  | サーバーはサービス妨害の予防機能をサポートします。読み取り/書き込みタイムアウトおよび緊急スレッドを含みます。                                                                                                                                                                                                                                            |
| 項目とサブツリーの動的更新                                                  | 1.3.18.0.2.32.15 | サーバーは項目およびサブツリーでの動的構成更新をサポートします。                                                                                                                                                                                                                                                                   |
| 別名参照解除オプション                                                    | 1.3.18.0.2.32.10 | サーバーはデフォルトによって別名を参照解除しないためのオプションをサポートします。                                                                                                                                                                                                                                                          |
| グループ特定検索限界                                                     | 1.3.18.0.2.32.17 | グループ特定検索限界は、ある人々のグループに対する拡張検索限界をサポートします。                                                                                                                                                                                                                                                           |
| 動的トレース                                                         | 1.3.18.0.2.32.14 | サーバーは LDAP 拡張操作によるサーバーのアクティブ・トレースをサポートします。                                                                                                                                                                                                                                                         |
| TLS 機能                                                         | 1.3.18.0.2.32.28 | サーバーが実際に TLS を実行できることを指定します。                                                                                                                                                                                                                                                                       |
| 管理デーモン監査                                                       | 1.3.18.0.2.32.11 | サーバーは管理デーモンの監査をサポートします。                                                                                                                                                                                                                                                                            |
| Kerberos 機能                                                    | 1.3.18.0.2.32.30 | サーバーが実際に Kerberos を実行できることを指定します。                                                                                                                                                                                                                                                                  |
| 非ブロッキング複製                                                      | 1.3.18.0.2.32.29 | コンシューマーがエラーを戻した場合、サブライヤーは更新を再送信しない場合があります。                                                                                                                                                                                                                                                         |
| <code>ibm-allMembers</code> と <code>ibm-allGroups</code> の操作属性 | 1.3.18.0.2.32.31 | バックエンドは、 <code>ibm-allMembers</code> と <code>ibm-allGroups</code> の操作属性を介して静的、動的、およびネストされたグループの検索をサポートします。静的、動的、およびネストされたグループ (または、このいずれか) のメンバーは、 <code>ibm-allMembers</code> 操作属性で検索を実行して取得できます。メンバー DN が属している静的、動的、およびネストされたグループ (または、このいずれか) は、 <code>ibm-allGroups</code> 操作属性で検索を実行して取得できます。 |
| グローバル固有属性                                                      | 1.3.18.0.2.32.16 | 固有属性値をグローバルに強制するためのサーバー機能。                                                                                                                                                                                                                                                                         |
| モニター操作カウント                                                     | 1.3.18.0.2.32.24 | サーバーは、開始および完了した操作タイプのモニター操作カウントを提供します。                                                                                                                                                                                                                                                             |
| モニター・ログ・カウント                                                   | 1.3.18.0.2.32.20 | サーバーは、サーバー、CLI、および監査ログ・ファイルに追加されたメッセージのモニター・ログ・カウントを提供します。                                                                                                                                                                                                                                         |
| モニター接続タイプ・カウント                                                 | 1.3.18.0.2.32.22 | サーバーは、SSL および TLS 接続のモニター接続タイプ・カウントを提供します。                                                                                                                                                                                                                                                         |
| アクティブ・ワーカー情報のモニター                                              | 1.3.18.0.2.32.21 | サーバーは、アクティブ・ワーカー ( <code>cn=workers,cn=monitor</code> ) のモニター情報を提供します。                                                                                                                                                                                                                             |

表 10. サポートされている使用可能な機能の OID (続き)

| 名前                   | OID                    | 説明                                                                                        |
|----------------------|------------------------|-------------------------------------------------------------------------------------------|
| モニター接続情報             | 1.3.18.0.2.32.23       | サーバーは、接続 ID (cn=connections, cn=monitor) ではなく、IP アドレスによる接続のモニター情報を提供します。                  |
| モニター・トレース情報          | 1.3.18.0.2.32.25       | サーバーは、現在使用しているトレース・オプションのモニター情報を提供します。                                                    |
| 属性キャッシュ検索フィルター解決     | 1.3.18.0.2.32.13       | サーバーは、検索フィルター解決の属性キャッシュをサポートします。                                                          |
| プロキシ許可               | 1.3.18.0.2.32.27       | サーバーは、ユーザー・グループのプロキシ許可をサポートします。                                                           |
| 言語タグ・オプション・サポート      | 1.3.6.1.4.1.4203.1.5.4 | サーバーが RFC 2596 に定義された言語タグをサポートすることを示します。                                                  |
| 最大経過日数 ChangeLog 項目  | 1.3.18.0.2.32.19       | サーバーが経過日数を基に changelog 項目を保存できることを示します。                                                   |
| IBMpolicies 複製サブツリー  | 1.3.18.0.2.32.18       | サーバーは cn=IBMpolicies サブツリーの複製をサポートします。                                                    |
| NULL ベース・サブツリー検索     | 1.3.18.0.2.32.26       | サーバーでは、サーバーに定義された DIT 全体を検索する、ヌル・ベース・サブツリー検索が許可されます。                                      |
| オートノミック属性キャッシュ       | 1.3.18.0.2.32.50       | オートノミック属性キャッシュをサポートします。                                                                   |
| ibm-entrychecksumop  | 1.3.18.0.2.32.56       | 6.0 IDS ibm-entrychecksumop 機能                                                            |
| フィルター済み参照サーバー機能      | 1.3.18.0.2.32.36       | 拡張フィルター済み参照のサポートを示すのに使用されます。これは、参照内のフィルター済みの値は、検索要求上の元のフィルターと結合されることを意味します。               |
| グローバル管理グループ・サーバー機能   | 1.3.18.0.2.32.38       | グローバル管理グループのサポートを示すのに使用されます。                                                              |
| 比較の監査機能              | 1.3.18.0.2.32.40       | 比較操作の監査のサポートを示すのに使用されます。                                                                  |
| AES パスワード暗号化         | 1.3.18.0.2.32.39       | AES パスワード暗号化のサポートを示します。                                                                   |
| 最大項目サイズ              | 1.3.18.0.2.32.51       | 複製競合を解決するのに使用されます。サプライヤーは、この数値に基づいて、複製競合の解決のためにターゲット・サーバーに項目を再度追加する必要があるかどうかを判断することができます。 |
| LostAndFound ログ・ファイル | 1.3.18.0.2.32.52       | 複製競合解決の結果として置き換えられた項目をアーカイブするファイル。                                                        |
| ログ管理                 | 1.3.18.0.2.32.41       | ログ・ファイル・アクセス拡張操作と Tivoli Directory Server 監査ログのサポートを示します。                                 |
| マルチスレッド複製            | 1.3.18.0.2.32.42       |                                                                                           |
| 複製のサプライヤーのサーバー構成。    | 1.3.18.0.2.32.43       |                                                                                           |
| IBMPolicies 複製サブツリー  | 1.3.18.0.2.32.18       | cn=ibmpolicies サブツリーを使用して、cn=ibmpolicies および cn=schema の複製の構成をサポートします。                    |

## ACL メカニズムの OID

以下の表に、ACL メカニズムの OID を示します。

表 11. ACL メカニズムの OID

| 名前                         | OID             | 説明                                                                    |
|----------------------------|-----------------|-----------------------------------------------------------------------|
| IBM SecureWay V3.2 ACL モデル | 1.3.18.0.2.26.2 | LDAP サーバーが IBM SecureWay V3.2 ACL モデルをサポートしていることを示します。                |
| IBM フィルター・ベースの ACL メカニズム   | 1.3.18.0.2.26.3 | LDAP サーバーが IBM Directory Server v5.1 のフィルター・ベース ACL をサポートしていることを示します。 |
| システム制限 ACL サポート            | 1.3.18.0.2.26.4 | サーバーが ACL 項目でシステムおよび制限付きアクセス・クラスをサポートしていることを示します。                     |

### 関連概念

105 ページの『制御および拡張操作』

制御操作と拡張操作では、プロトコルそのものを変更しなくても、LDAP プロトコルを拡張することができます。

## IBM Tivoli Directory Server と同等の製品

Directory Server には、他のプラットフォームで利用できる IBM Tivoli Directory Server 製品と互換性があります。以下の表は、個々のバージョンの i5/OS Directory Server に対応する、それぞれと同等の IBM Tivoli Directory Server 製品をリストしています。個々の製品ごとに、Directory Server の前提条件を i5/OS Directory Server が満たすかどうかを判別するときに、この表が役に立ちます。

表 12. IBM Tivoli Directory Server と同等の製品

| i5/OS Directory Server             | IBM Tivoli Directory Server                 |
|------------------------------------|---------------------------------------------|
| バージョン 6 リリース 1                     | IBM Tivoli Directory Server バージョン 6.0       |
| バージョン 5 リリース 4                     | IBM Tivoli Directory Server バージョン 5.2       |
| バージョン 5 リリース 3                     | IBM Directory Server バージョン 5.1              |
| バージョン 5 リリース 2 (PTF SI08487 を適用済み) | IBM Directory Server バージョン 4.1              |
| バージョン 5 リリース 2 (GA)                | IBM SecureWay® Directory Server バージョン 3.2.2 |

## Directory Server のデフォルト構成

Directory Server は、i5/OS 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、「Directory Server Configuration (Directory Server の構成)」ウィザードを実行していないか、またはプロパティー・ページでディレクトリー設定を変更していない場合。
- Directory Server の公開が構成されていない場合。
- Directory Server が LDAP DNS 情報を検出できない場合。

Directory Server 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、Directory Server 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、Directory Server のプロパティ・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、システムの 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。
- Directory Server 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、非セキュア通信のためにポート 389 を使用します。LDAP 用のデジタル証明書が設定されている場合は、Secure Sockets Layer (SSL) が使用可能になり、セキュアな通信にポート 636 が使用されます。

#### 関連タスク

114 ページの『Directory Server の構成』

Directory Server の設定をカスタマイズするには、「Directory Server Configuration (Directory Server の構成)」ウィザードを実行します。

---

## Directory Server のトラブルシューティング

問題を解決するために役立つ情報。サービス・データの収集および特定の問題の解決のための提案が含まれています。

Directory Server 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。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。

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。

Directory Server の一般的な問題の詳細については、Directory Server のホーム・ページ ([www.iseries.ibm.com/ldap](http://www.iseries.ibm.com/ldap)) を参照してください。

Directory Server は、QSQRVVR ジョブであるいくつかの 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、このサーバーがどの SQL サーバー・ジョブを開始したかが分かれば、追加のエラーをどの QSQRVVR ジョブ・ログで探せばよいか分かるようになります。

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。

```

 システム: MYSYSTEM
Job . . . : QDIRSRV User . . . : QDIRSRV Number . . . : 174440

>> CALL PGM(QSYS/QGLDSVR)
 Job 057448/QUSER/QSQRVVR used for SQL server mode processing.
 Job 057340/QUSER/QSQRVVR used for SQL server mode processing.
 Job 057448/QUSER/QSQRVVR 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 Server started successfully.

メッセージは、サーバーに対して開始された QSQSRVR ジョブに関するものです。サーバー上のメッセージの数は、構成およびサーバー開始に必要な QSQSRVR ジョブの数により、異なる場合があります。

System i Navigator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・ページで、サーバーの始動後のディレクトリー操作に Directory Server が使用する SQL サーバーの合計数を指定します。追加の SQL サーバーは、複製のために開始されます。

#### 関連情報



Directory Server ホーム・ページ

## Directory Server のジョブ・ログを使ったエラーおよびアクセスのモニタ

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。

ディレクトリー・サーバー用のジョブ・ログを表示することにより、エラーを警告し、サーバー・アクセスを監視することができます。ジョブ・ログには以下が含まれます。

- サーバー・オペレーションおよび SQL サーバー・ジョブや複製の障害などのサーバー内の問題に関するメッセージ。
- 間違ったパスワードなどの、クライアントによる操作を反映するセキュリティ関連のメッセージ。
- 必須属性の欠落などのクライアントのエラーについての詳細のメッセージ。

クライアントの問題をデバッグしている場合以外は、クライアント・エラーをログに記録することは望まな  
いかもしれません。クライアント・エラーのロギングは、System i Navigatorの Directory Server の「一  
般」プロパティ・タブで制御できます。

### サーバーの開始後の QDIRSRV ジョブ・ログの表示

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. System i Navigator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. 「IBM Directory Server」を右マウス・ボタン・クリックしてから、「サーバーのジョブ (Server Jobs)」を選択する。
5. 「ファイル (File)」メニューで、「ジョブ・ログ (Job Log)」を選択する。

### サーバーの停止後の QDIRSRV ジョブ・ログの表示

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. System i Navigator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. System i Navigator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: System i Navigator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、Directory Server は他のシステム・リソースを使用します。このようなり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、Directory Server 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 を使用した問題の検出

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。

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ために、Directory Server で、TCP/IP アプリケーションのトレース (TRCTCPAPP) コマンドを使用することができます。
- | TRCTCPAPP コマンドを使用して、アクティブなサーバー・インスタンスをトレースすることができます。たとえば次のようになります。
- | TRCTCPAPP APP(\*DIRSRV) INSTANCE(QUSRDIR)
- | また、STRTCPSVR コマンドを使用し、'-h dft' インスタンス始動値を追加して、トレースを開始することもできます。すると、トレースがサーバー・インスタンス内で開始し、サーバー・インスタンスを開始します。たとえば次のようになります。
- | STRTCPSVR SERVER(\*DIRSRV) INSTANCE(QUSRDIR '-h dft')
- | トレースを終了するには、次のコマンドを使用します。
- | TRCTCPAPP APP(\*DIRSRV) SET(\*OFF)

### 関連概念

通信トレース

### 関連情報

TCP/IP アプリケーションのトレース (TRCTCPAPP)

## LDAP\_OPT\_DEBUG オプションを使用したエラーのトレース

LDAP C API を使用しているクライアントの問題をトレースします。

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(1d, 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 を使用する場合は `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で、コマンド行に次のように入力します。

```
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、コマンド行に次のように入力します。

```
DSPPFM QAP0ZDMP QP0Znnnnn
```

QAP0ZDMP はゼロを含み、nnnnn はジョブ番号です。

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. コマンド行に以下を入力する。

```
SAVOBJ OBJ(QAP0ZDMP) LIB(QTEMP) DEV(*SAVF) SAVF(xxx)
```

ここで QAP0ZDMP はゼロを含み、xxx は、SAVF ファイルに指定した名前です。

### 関連概念

Lightweight Directory Access Protocol (LDAP) API

Directory Server API の詳細は、『Lightweight Directory Access Protocol (LDAP) APIs』を参照してください。

### 関連情報

環境変数追加 (ADDENVVAR)

ユーザー・トレース・ダンプ (DMPUSRTRC)

物理ファイル・メンバー表示 (DSPPFM)

保存ファイル作成 (CRTSAVF)

オブジェクト保存 (SAVOBJ)

## GLEnnnn メッセージ ID

GLE メッセージ ID とその説明をリストした情報を以下に示します。

メッセージ ID は GLEnnnn の形式をとり、ここの nnnn は 10 進数エラー番号です。例えば、戻りコード 50 (0x32) の説明は次のコマンドを入力して表示することができます。

```
| DSPMSGD RANGE(GLE0050) MSGF(QGLDMSG)
```

これは、LDAP\_INSUFFICIENT\_ACCESS の説明を示しています。

以下の表には、GLE メッセージ ID とその説明がリストされています。

| メッセージ ID | 説明                                                        |
|----------|-----------------------------------------------------------|
| GLE0000  | 要求は正常に実行された (LDAP_SUCCESS)                                |
| GLE0001  | 操作エラー (LDAP_OPERATIONS_ERROR)                             |
| GLE0002  | プロトコル・エラー (LDAP_PROTOCOL_ERROR)                           |
| GLE0003  | 時間制限を超えた (LDAP_TIMELIMIT_EXCEEDED)                        |
| GLE0004  | サイズ限界を超えた (LDAP_SIZELIMIT_EXCEEDED)                       |
| GLE0005  | 比較されたタイプと値が項目中に存在しない<br>(LDAP_COMPARE_FALSE)              |
| GLE0006  | 比較されたタイプと値が項目中に存在する<br>(LDAP_COMPARE_TRUE)                |
| GLE0007  | 認証方式がサポートされていない<br>(LDAP_AUTH_METHOD_NOT_SUPPORTED)       |
| GLE0008  | 強力な認証が必要である<br>(LDAP_STRONG_AUTH_REQUIRED)                |
| GLE0009  | 部分的な結果および参照を受け取った<br>(LDAP_PARTIAL_RESULTS)               |
| GLE0010  | 参照が戻された (LDAP_REFERRAL)                                   |
| GLE0011  | 管理限界を超えた (LDAP_ADMIN_LIMIT_EXCEEDED)                      |
| GLE0012  | 重要な拡張がサポートされていない<br>(LDAP_UNAVAILABLE_CRITICAL_EXTENSION) |
| GLE0013  | 機密性が必要である<br>(LDAP_CONFIDENTIALITY_REQUIRED)              |
| GLE0014  | SASL バインドが進行中<br>(LDAP_SASL_BIND_IN_PROGRESS)             |
| GLE0016  | そのような属性がない (LDAP_NO_SUCH_ATTRIBUTE)                       |
| GLE0017  | 未定義の属性タイプ (LDAP_UNDEFINED_TYPE)                           |
| GLE0018  | 不適切な突き合わせ<br>(LDAP_INAPPROPRIATE_MATCHING)                |
| GLE0019  | 制約違反 (LDAP_CONSTRAINT_VIOLATION)                          |
| GLE0020  | タイプまたは値が存在する<br>(LDAP_TYPE_OR_VALUE_EXISTS)               |
| GLE0021  | 構文が無効 (LDAP_INVALID_SYNTAX)                               |
| GLE0032  | そのようなオブジェクトがない<br>(LDAP_NO_SUCH_OBJECT)                   |
| GLE0033  | 別名の問題 (LDAP_ALIAS_PROBLEM)                                |
| GLE0034  | DN 構文が無効 (LDAP_INVALID_DN_SYNTAX)                         |
| GLE0035  | オブジェクトがリーフである (LDAP_IS_LEAF)                              |
| GLE0036  | 別名参照解除の問題 (LDAP_ALIAS_DEREF_PROBLEM)                      |
| GLE0048  | 不適切な認証 (LDAP_INAPPROPRIATE_AUTH)                          |
| GLE0049  | 認証が無効 (LDAP_INVALID_CREDENTIALS)                          |
| GLE0050  | 不十分なアクセス (LDAP_INSUFFICIENT_ACCESS)                       |
| GLE0051  | ディレクトリー・サーバーは使用中 (LDAP_BUSY)                              |

| メッセージ ID | 説明                                                          |
|----------|-------------------------------------------------------------|
| GLE0052  | ディレクトリー・サービス・エージェントが使用可能でない (LDAP_UNAVAILABLE)              |
| GLE0053  | ディレクトリー・サーバーが要求された操作を実行しようとしなない (LDAP_UNWILLING_TO_PERFORM) |
| GLE0054  | ループを検出した (LDAP_LOOP_DETECT)                                 |
| LE0064   | 命名違反 (LDAP_NAMING_VIOLATION)                                |
| LE0065   | オブジェクト・クラス違反 (LDAP_OBJECT_CLASS_VIOLATION)                  |
| GLE0066  | 操作は非リーフでは許可されない (LDAP_NOT_ALLOWED_ON_NONLEAF)               |
| GLE0067  | 操作は相対識別名では許可されない (LDAP_NOT_ALLOWED_ON_RDN)                  |
| GLE0068  | 既に存在している (LDAP_ALREADY_EXISTS)                              |
| GLE0069  | オブジェクト・クラスを変更できない (LDAP_NO_OBJECT_CLASS_MODS)               |
| GLE0070  | 結果が大きすぎる (LDAP_RESULTS_TOO_LARGE)                           |
| GLE0071  | 複数のサーバーに影響する (LDAP_AFFECTS_MULTIPLE_DSAS)                   |
| GLE0080  | 不明なエラー (LDAP_OTHER)                                         |
| GLE0081  | LDAP サーバーに連絡できない (LDAP_SERVER_DOWN)                         |
| GLE0082  | ローカル・エラー (LDAP_LOCAL_ERROR)                                 |
| GLE0083  | エンコード・エラー (LDAP_ENCODING_ERROR)                             |
| GLE0084  | デコード・エラー (LDAP_DECODING_ERROR)                              |
| GLE0085  | 要求がタイムアウトした (LDAP_TIMEOUT)                                  |
| GLE0086  | 不明な認証方式 (LDAP_AUTH_UNKNOWN)                                 |
| GLE0087  | 不良の検索フィルター (LDAP_FILTER_ERROR)                              |
| GLE0088  | ユーザーが操作をキャンセルした (LDAP_USER_CANCELLED)                       |
| GLE0089  | LDAP ルーチンへのパラメーターが不良 (LDAP_PARAM_ERROR)                     |
| GLE0090  | メモリー不足 (LDAP_NO_MEMORY)                                     |
| GLE0091  | 接続エラー (LDAP_CONNECT_ERROR)                                  |
| GLE0092  | 機能がサポートされていない (LDAP_NOT_SUPPORTED)                          |
| GLE0093  | 制御が検出されない (LDAP_CONTROL_NOT_FOUND)                          |
| GLE0094  | 結果が戻されない (LDAP_NO_RESULTS_RETURNED)                         |
| GLE0095  | 戻す結果が多すぎる (LDAP_MORE_RESULTS_TO_RETURN)                     |
| GLE0096  | LDAP URL でない (LDAP_URL_ERR_NOTLDAP)                         |
| GLE0097  | URL に DN がない (LDAP_URL_ERR_NODN)                            |
| GLE0098  | URL 有効範囲値が無効 (LDAP_URL_ERR_BADSCOPE)                        |
| GLE0099  | メモリー割り振りエラー (LDAP_URL_ERR_MEM)                              |
| GLE0100  | クライアント・ループ (LDAP_CLIENT_LOOP)                               |

| メッセージ ID | 説明                                                          |
|----------|-------------------------------------------------------------|
| GLE0101  | 参照限界を超えた<br>(LDAP_REFERRAL_LIMIT_EXCEEDED)                  |
| GLE0112  | SSL 環境は既に初期化された<br>(LDAP_SSL_ALREADY_INITIALIZED)           |
| GLE0113  | 初期化の呼び出しが失敗した<br>(LDAP_SSL_INITIALIZE_FAILED)               |
| GLE0114  | SSL 環境が初期化されていない<br>(LDAP_SSL_CLIENT_INIT_NOT_CALLED)       |
| GLE0115  | 無許可 SSL パラメーター値が指定された<br>(LDAP_SSL_PARAM_ERROR)             |
| GLE0116  | セキュア接続のネゴシエーションに失敗した<br>(LDAP_SSL_HANDSHAKE_FAILED)         |
| GLE0118  | SSL ライブラリーを検出できない<br>(LDAP_SSL_NOT_AVAILABLE)               |
| GLE0128  | 明示的所有者が検出されない<br>(LDAP_NO_EXPLICIT_OWNER)                   |
| GLE0129  | 必要なリソースでのロックを取得できない<br>(LDAP_NO_LOCK)                       |
| GLE0133  | LDAP サーバーが DNS で検出されない<br>(LDAP_DNS_NO_SERVERS)             |
| GLE0134  | DNS の結果が切り捨てられた<br>(LDAP_DNS_TRUNCATED)                     |
| GLE0135  | DNS データを解析できなかった<br>(LDAP_DNS_INVALID_DATA)                 |
| GLE0136  | システム・ドメインまたは nameserver を解決できない<br>(LDAP_DNS_RESOLVE_ERROR) |
| GLE0137  | DNS 構成ファイル・エラー<br>(LDAP_DNS_CONF_FILE_ERROR)                |
| GLE0160  | 出力バッファのオーバーフロー (LDAP_XLATE_E2BIG)                           |
| GLE0161  | 入力バッファが切り捨てられた<br>(LDAP_XLATE_EINVAL)                       |
| GLE0162  | 使用できない入力文字 (LDAP_XLATE_EILSEQ)                              |
| GLE0163  | 文字はコード・セット・ポイントにマップされない<br>(LDAP_XLATE_NO_ENTRY)            |

## 関連情報

メッセージ記述表示 (DSPMSGD)

## LDAP クライアントに関する一般的なエラー

以下の情報は、一般的な LDAP クライアント・エラーを説明しています。

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、「プログラミング」のトピック集の中の『Directory Server API』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 i5/OS 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解決方法は異なるものと思われます。

#### 関連概念

Lightweight Directory Access Protocol (LDAP) API

Directory Server API の詳細は、『Lightweight Directory Access Protocol (LDAP) APIs』を参照してください。

### ldap\_search: Timelimit exceeded (時間制限を超えました)

このエラーが起きるのは、ldapsearch コマンドの実行が緩慢な場合です。

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。

- ディレクトリー・サーバーの検索時間制限を大きくする。
- 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。

#### 関連タスク

143 ページの『検索設定の調整』

以下の情報を参考にして、ユーザーの検索機能を制御します。

### [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幾つかあります。

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、QDIRSRV ジョブ・ログ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。

#### 関連概念

337 ページの『Directory Server のトラブルシューティング』

問題を解決するために役立つ情報。サービス・データの収集および特定の問題の解決のための提案が含まれています。

#### 関連タスク

338 ページの『Directory Server のジョブ・ログを使ったエラーおよびアクセスのモニター』

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。

### 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一般的な原因は、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場合があります。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、QDIRSRV ジョブ・ログを調べてください。

#### 関連タスク

338 ページの『Directory Server のジョブ・ログを使ったエラーおよびアクセスのモニター』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。

### **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 が正しくない場合、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 i5/OS 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 i5/OS 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、QDIRSRV ジョブ・ログを調べてください。

#### **関連タスク**

338 ページの『Directory Server のジョブ・ログを使ったエラーおよびアクセスのモニター』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。

### **[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、QDIRSRV ジョブ・ログを調べてください。

#### **関連タスク**

338 ページの『Directory Server のジョブ・ログを使ったエラーおよびアクセスのモニター』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。

### **[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)**

このエラーの最も一般的な原因には、サーバーが準備完了になる前の要求や、無効なポート番号があります。

このエラーの最も一般的な原因は次のとおりです。

- 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、QDIRSRV ジョブ・ログを調べてください。ディレクトリー・サーバーが正常に開始されている場合は、Directory Server started successfully (ディレクトリー・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。

#### **関連タスク**

338 ページの『Directory Server のジョブ・ログを使ったエラーおよびアクセスのモニター』  
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。

## **[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。

i5/OS 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、「プログラミング」トピックの『Directory Server APIs』を参照してください。

### **関連概念**

Lightweight Directory Access Protocol (LDAP) API

Directory Server API の詳細は、『Lightweight Directory Access Protocol (LDAP) APIs』を参照してください。

## **パスワード・ポリシー関連エラー**

パスワード・ポリシーを使用可能にすると、予期しないエラーが起こる原因となる場合があります。

特定のパスワード・ポリシーが使用可能になっていると、明示的にできない障害の原因となる場合があります。以下のことを検討して、パスワード・ポリシー関連エラーのトラブルシューティングに役立ててください。

**適切なパスワードによるバインドが「無効な信任状」で失敗:** パスワードが満了したか、あるいはアカウントがロックされた可能性があります。項目の `pwdchangedtime` と `pwdaccountlockedtime` の属性を調べてください。

**正常なバインド後に「実行しようとしなさい」で要求が失敗:** パスワードがリセットされた可能性があります、その場合、バインドは正常に行われますが、サーバーで許可される唯一の操作は、ユーザーの場合、そのパスワードを変更することです。パスワードを変更するまで、その他の要求は「実行しようとしなさい」で失敗します。

**リセットされたパスワードによる認証は予期しない動作となる:** パスワードがリセットされると、上で記述したとおり、バインド要求は正常に行われます。これは、リセットされたパスワードを使用してユーザーが無期限に認証できることを意味します。

### **関連資料**

89 ページの『パスワード・ポリシーのヒント』

パスワード・ポリシーは、見込みどおりに動作するとは限りません。



## QGLDCPYVL API のトラブルシューティング

「User Trace」機能を使用することによって、エラーを解明したり、保守が必要かどうかを判別したりできる場合があります。

この API は「User Trace」機能を使用して、その操作を記録します。エラーが起こるか、あるいはその疑いがある場合は、トレースによって明白なエラーの説明が示されるか、あるいはサービスが必要かどうかの説明できる場合があります。トレースは、以下のようにして入手できます。

```
STRTRC SSNID(COPYVLDL) JOBTRCTYPE(*TRCTYPE) TRCTYPE((*DIRSRV *INFO))
CALL QGLDCPYVL PARM(...)
ENDTRC SSNID(COPYVLDL) DTALIB(QTEMP) PRTRC(*YES)
```

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. コマンド・プロンプトに以下を入力する。

```
SAVOBJ OBJ(QAP0ZDMP) LIB(QTEMP) DEV(*SAVF) SAVF(xxx)
```

ここで QAP0ZDMP はゼロを含み、xxx は、SAVF ファイルに指定した名前です。

### 関連概念

Lightweight Directory Access Protocol (LDAP) API

Directory Server API の詳細は、『Lightweight Directory Access Protocol (LDAP) APIs』を参照してください。

### 関連情報

トレース開始 (STRTRC)

保存ファイル作成 (CRTSAVF)




オブジェクト保存 (SAVOBJ)

---



## 関連情報

以下は、Directory Server トピックと関連した IBM Redbooks 資料 (PDF 形式)、Web サイト、および Information Center のトピックです。以下は、PDF で表示したり印刷したりできます。

### IBM Redbooks の資料 ([www.redbooks.ibm.com](http://www.redbooks.ibm.com))

- Understanding LDAP, SG24-4986 
- Using LDAP for Directory Integration: A Look at IBM SecureWay Directory, Active Directory, and Domino®, SG24-6163 
- Implementation and Practical Use of LDAP on the iSeries Server, SG24-6193 

### Web サイト

- IBM Directory Server for iSeries Web サイト  ([www.ibm.com/servers/eserver/iseriess/ldap](http://www.ibm.com/servers/eserver/iseriess/ldap))
- The Java Naming and Directory Interface (JNDI) Tutorial Web site  ([java.sun.com/products/jndi/tutorial/](http://java.sun.com/products/jndi/tutorial/))

## その他の情報

「プログラミング」カテゴリの 『Lightweight Directory Access Protocol (LDAP) APIs』

---

## 付録. 特記事項

本書は米国 IBM が提供する製品およびサービスについて作成したものです。

本書に記載の製品、サービス、または機能が日本においては提供されていない場合があります。日本で利用可能な製品、サービス、および機能については、日本 IBM の営業担当員にお尋ねください。本書で IBM 製品、プログラム、またはサービスに言及していても、その IBM 製品、プログラム、またはサービスのみが使用可能であることを意味するものではありません。これらに代えて、IBM の知的所有権を侵害することのない、機能的に同等の製品、プログラム、またはサービスを使用することができます。ただし、IBM 以外の製品とプログラムの操作またはサービスの評価および検証は、お客様の責任で行っていただきます。

IBM は、本書に記載されている内容に関して特許権 (特許出願中のものを含む) を保有している場合があります。本書の提供は、お客様にこれらの特許権について実施権を許諾することを意味するものではありません。実施権についてのお問い合わせは、書面にて下記宛先にお送りください。

〒106-8711  
東京都港区六本木 3-2-12  
日本アイ・ビー・エム株式会社  
法務・知的財産  
知的財産権ライセンス渉外

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

この情報には、技術的に不適切な記述や誤植を含む場合があります。本書は定期的に見直され、必要な変更は本書の次版に組み込まれます。IBM は予告なしに、随時、この文書に記載されている製品またはプログラムに対して、改良または変更を行うことがあります。

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

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

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

IBM Corporation  
Software Interoperability Coordinator, Department YBWA  
3605 Highway 52 N  
Rochester, MN 55901  
U.S.A.

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

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

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

IBM 以外の製品に関する情報は、その製品の供給者、出版物、もしくはその他の公に利用可能なソースから入手したものです。IBM は、それらの製品のテストは行っておりません。したがって、他社製品に関する実行性、互換性、またはその他の要求については確認できません。IBM 以外の製品の性能に関する質問は、それらの製品の供給者をお願いします。

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

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

本書はプランニング目的としてのみ記述されています。記述内容は製品が使用可能になる前に変更になる場合があります。

本書には、日常の業務処理で用いられるデータや報告書の例が含まれています。より具体性を与えるために、それらの例には、個人、企業、ブランド、あるいは製品などの名前が含まれている場合があります。これらの名称はすべて架空のものであり、名称や住所が類似する企業が実在しているとしても、それは偶然にすぎません。

著作権使用許諾:

本書には、様々なオペレーティング・プラットフォームでのプログラミング手法を例示するサンプル・アプリケーション・プログラムがソース言語で掲載されています。お客様は、サンプル・プログラムが書かれているオペレーティング・プラットフォームのアプリケーション・プログラミング・インターフェースに準拠したアプリケーション・プログラムの開発、使用、販売、配布を目的として、いかなる形式においても、IBM に対価を支払うことなくこれを複製し、改変し、配布することができます。このサンプル・プログラムは、あらゆる条件下における完全なテストを経ていません。従って IBM は、これらのサンプル・プログラムについて信頼性、利便性もしくは機能性があることをほめかしたり、保証することはできません。

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

---

## 商標

以下は、IBM Corporation の商標です。

Application System/400

AS/400

DB2

Lotus Domino  
e(ロゴ)server  
eServer  
i5/OS  
IBM  
iSeries  
JavaLotus  
Lotus Notes  
Operating System/400  
OS/400  
Redbooks  
RDN  
SecureWay  
System i  
Tivoli  
UNIX  
WebSphere  
XT  
400

Adobe、Adobe ロゴ、PostScript、PostScript ロゴは、Adobe Systems Incorporated の米国およびその他の国における商標または登録商標です。

Microsoft、Windows、Windows NT および Windows ロゴは、Microsoft Corporation の米国およびその他の国における商標です。

Java およびすべての Java 関連の商標およびロゴは Sun Microsystems, Inc.の米国およびその他の国における商標です。

UNIX は The Open Group の米国およびその他の国における登録商標です。

他の会社名、製品名およびサービス名等はそれぞれ各社の商標です。

---

## 資料に関するご使用条件

これらの資料は、以下の条件に同意していただける場合に限りご使用いただけます。

**個人使用:** これらの資料は、すべての著作権表示その他の所有権表示をしていただくことを条件に、非商業的な個人による使用目的に限り複製することができます。ただし、IBM の明示的な承諾をえずに、これらの資料またはその一部について、二次的著作物を作成したり、配布 (頒布、送信を含む) または表示 (上映を含む) することはできません。

**商業的使用:** これらの資料は、すべての著作権表示その他の所有権表示をしていただくことを条件に、お客様の企業内に限り、複製、配布、および表示することができます。ただし、IBM の明示的な承諾をえずにこれらの資料の二次的著作物を作成したり、お客様の企業外で資料またはその一部を複製、配布、または表示することはできません。

ここで明示的に許可されているもの以外に、資料や資料内に含まれる情報、データ、ソフトウェア、またはその他の知的所有権に対するいかなる許可、ライセンス、または権利を明示的にも黙示的にも付与するものではありません。

資料の使用が IBM の利益を損なうと判断された場合や、上記の条件が適切に守られていないと判断された場合、IBM はいつでも自らの判断により、ここで与えた許可を撤回できるものとさせていただきます。

お客様がこの情報をダウンロード、輸出、または再輸出する際には、米国のすべての輸出入関連法規を含む、すべての関連法規を遵守するものとします。

IBM は、これらの資料の内容についていかなる保証もしません。これらの資料は、特定物として現存するままの状態を提供され、商品性の保証、特定目的適合性の保証および法律上の瑕疵担保責任を含むすべての明示もしくは黙示の保証責任なしで提供されます。





Printed in Japan