CHAPTER 14

ディレクトリ アクセスとディレクトリ統合

ディレクトリ（電話帳）は、多数の読み取りや検索、および随時の書き込みや更新用に最適化される特殊なデータベースです。ディレクトリには、一般に、社員の情報、企業ネットワークでのユーザ特権など、頻繁に変更されないデータが保存されます。

ディレクトリのもう 1 つの面は、拡張可能であることです。つまり、ディレクトリに保存される情報のタイプを変更し、拡大することが可能です。ディレクトリ スキーマという語は、保存されている情報のタイプ、および情報の規則を指します。多くのディレクトリは、さまざまなアプリケーションによって定義される情報タイプに対応するために、ディレクトリ スキーマを拡張する方法を備えています。この機能により、企業は、ディレクトリをユーザ情報の中央リポジトリとして使用できます。

Lightweight Directory Access Protocol（LDAP）は、ディレクトリに保存されている情報にアクセスし、変更するための標準方式をアプリケーションに提供します。この機能により、企業は、複数のアプリケーションから利用できるすべてのユーザ情報を、単一リポジトリに集中化させることができます。追加、移動、および変更が簡単なので、保守コストも大幅に削減されます。

この章では、Cisco CallManager と社内 LDAP ディレクトリを統合する場合の、設計上の主な原則について説明しています。また、Cisco IP Phone や Cisco IP SoftPhone などの Cisco IP テレフォニー エンドポイントに、社内 LDAP ディレクトリへのアクセスを提供する場合の、設計上の考慮事項についても説明しています。この章の構成は、次のとおりです。

- ディレクトリ アクセスとディレクトリ統合との比較（P.14-2）
- Cisco IP テレフォニー エンドポイントのディレクトリ アクセス（P.14-4）
- Cisco CallManager とのディレクトリ統合（P.14-7）
- ディレクトリ統合のベスト プラクティス（P.14-11）

この章で説明する考慮事項は、Cisco CallManager、および Cisco CallManager にバンドルされているエクステンション モビリティ、IP Management Assistant、Web Dialer、Bulk Administration Tool、Real-Time Monitoring Tool、およびマルチレベル管理という各アプリケーションに適用されます。

その他のシスコ音声アプリケーションについては、次の Web サイトで入手可能なそれぞれの製品資料を参照してください。

http://www.cisco.com

特に、Cisco Unity については、『*Cisco Unity Design Guide*』、および『*Cisco Unity Data and the Directory*』、『*Active Directory Capacity Planning*』、『*Cisco Unity Data Architecture and How Cisco Unity Works*』の各 White Paper を参照してください。

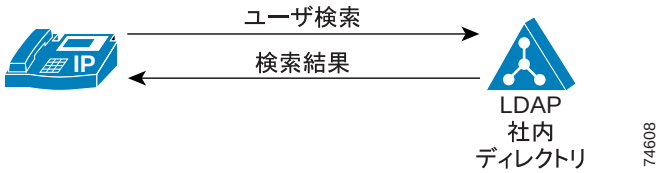
ディレクトリ アクセスとディレクトリ統合との比較

この項では、次の定義が適用されます。

- ディレクトリ アクセスとは、Cisco IP Phone や Cisco IP SoftPhone などの Cisco IP テレフォニー エンドポイントが、社内 LDAP ディレクトリにアクセスする機能のことです。
- ディレクトリ統合とは、Cisco CallManager などのアプリケーションが、独自の組み込みデータベースの替わりに、中央の社内 LDAP ディレクトリに、ユーザ関連情報を保存する機能のことです。

図 14-1 では、この章で定義されるディレクトリ アクセスを示しています。この例では、Cisco IP Phone からアクセスしています。クライアント アプリケーションは、企業の社内ディレクトリなどの LDAP ディレクトリに対してユーザ検索を実行し、一致するエントリを受け取ります。ユーザ検索に対して 1 つのエントリが選択され、エントリは Cisco IP Phone から検索されたユーザにダイヤルするために使用されます。

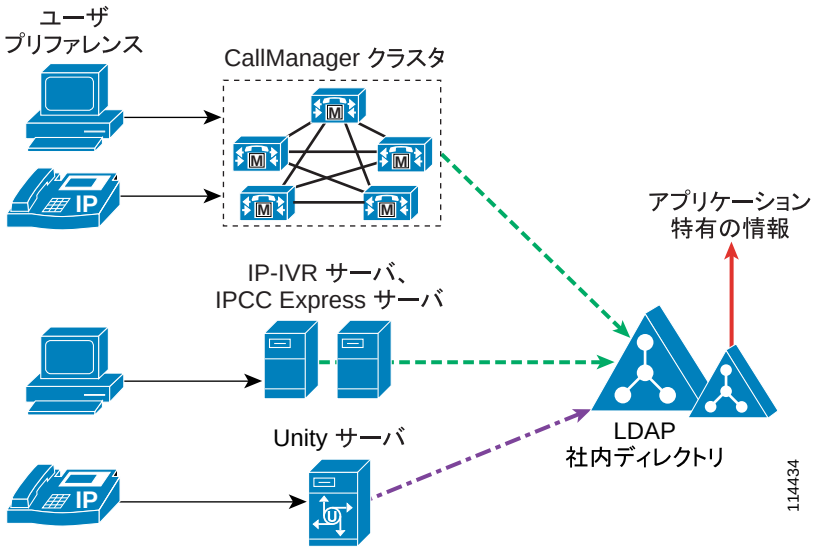
図 14-1　Cisco IP テレフォニー エンドポイントのディレクトリ アクセス



ここで定義しているディレクトリ アクセスには、ディレクトリに対する読み取り操作だけが含まれるため、ディレクトリ スキーマの拡張や他の設定変更は不要であることに注意してください。

一方、複数のアプリケーションと 1 つの社内ディレクトリを統合するディレクトリ統合は、これらのアプリケーションが、独自の個別の組み込みデータベースを使用するのではなく、中央ディレクトリにユーザ関連情報を保存することを意味します。図 14-2 では、この章で定義されるディレクトリ統合の例を示しています。

図 14-2　Cisco IP テレフォニー アプリケーションのディレクトリ統合



ディレクトリ統合には、ディレクトリに対する読み取り操作と書き込み操作が含まれるため、社内 LDAP ディレクトリに対するスキーマの拡張や他の設定変更が必要になることに注意してください。

デフォルトでは、Cisco CallManager は、組み込み LDAP ディレクトリに、ユーザ情報（たとえば、ユーザが制御するデバイス、個人用アドレス帳のエントリなど）を保存します。しかし、通常、電子メール アドレス、オフィスの住所、および役職などの一般的な社員情報を保存するために使用される社内 LDAP ディレクトリに、Cisco CallManager を統合することもできます。この場合、Cisco CallManager は、独自の組み込みディレクトリを使用しなくなり、社内ディレクトリにアプリケーション特有のユーザ情報を保存します。

（注）　Cisco CallManager Release 3.1 では、ディレクトリ統合は、Microsoft Active Directory（AD）2000 および Netscape Directory Server Release 4.*x* でサポートされています。Cisco CallManager Release 3.3(2) で iPlanet/Sun Directory Server 5.1 のサポートが追加され、Cisco CallManager Releases 3.3(3) および 4.0(1)sr2 で Microsoft Active Directory（AD）2003 のサポートが追加されました。

Cisco CallManager などのアプリケーションと社内ディレクトリを統合することには、単にエンドポイントにディレクトリ アクセスを提供すること以外に、次のような意味もあります。

- 社内ディレクトリにアプリケーション固有のユーザ属性を保存するには、ディレクトリ スキーマを拡張する必要があります。この操作は複雑なので、操作の際には、ディレクトリ構造を十分に理解している必要があります。
- アプリケーションはいつでもディレクトリと交信できる必要があり、ディレクトリは適切な応答時間を実現する必要があります。ディレクトリ サービスのアベイラビリティは、アプリケーションの機能に影響を与える場合があります。
- データ保存と、読み取りと書き込み照会によって、ディレクトリに不必要な負荷がかかります。新しいサービスまたはアプリケーションを導入する場合は、サーバのオーバーサブスクリプションを避けるために、慎重な計画とサイジングをお勧めします。

複数のアプリケーションにわたるディレクトリ統合には多くの利点がありますが、ディレクトリ統合が及ぼす影響をすべて理解し、個々の配置ごとにビジネスのニーズを確認することが重要です。

Cisco IP テレフォニー エンドポイントのディレクトリ アクセス

Cisco CallManager やその他の IP テレフォニー アプリケーションが社内ディレクトリに統合されているかどうかに関係なく、この項で説明しているガイドラインが適用されます。どちらの場合も、エンドユーザからは同じように見えます。これは、相違点によって影響を受けるのは、アプリケーションがユーザ情報を保存する方法と、ネットワーク上でこの情報の一貫性が保持される方法だけであるためです。

次の各項では、XML 対応電話機（Cisco IP Phone モデル 7940、7960 など）に対して、任意の LDAPv3 準拠ディレクトリ サーバへの社内ディレクトリ アクセスを設定する方法について概説します。

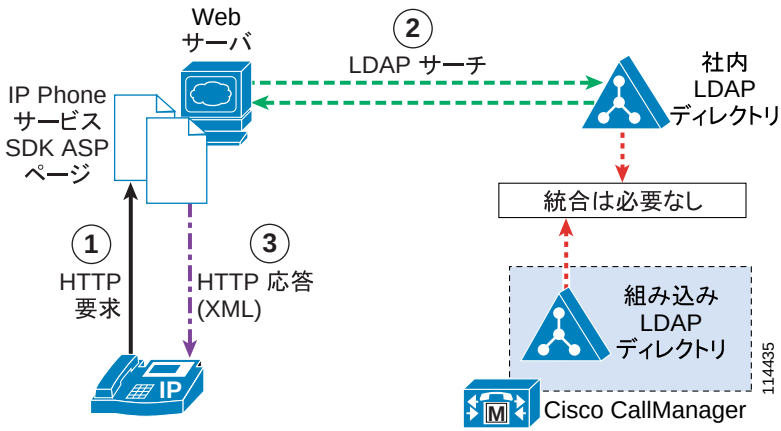
（注）　Cisco IP SoftPhone Release 1.2 以降には、Cisco IP Communicator と同様、LDAP ディレクトリにアクセスして検索するメカニズムが組み込まれています。この機能の設定方法の詳細は、製品資料を参照してください。

Cisco IP Phone のディレクトリ アクセス

XML 対応の Cisco IP Phone（モデル 7940 や 7960 など）は、ユーザが電話機の Directories ボタンを押すと、社内 LDAP ディレクトリを検索できます。IP Phone は、Hyper-Text Transfer Protocol（HTTP; ハイパーテキスト転送プロトコル）を使用して、要求を Web サーバに送信します。Web サーバからの応答には、電話機が解釈して表示できる特定の Extensible Markup Language（XML）オブジェクトが含まれている必要があります。社内ディレクトリを検索する場合、Web サーバは、プロキシとして動作します。電話機から要求を受け取り、その要求を LDAP 要求に変換します。LDAP 要求は、社内ディレクトリ サーバに送信されます。応答は適切な XML オブジェクトにカプセル化された後、解釈され電話機に戻されます。

図 14-3 では、Cisco CallManager が社内ディレクトリに統合されていない配置における、このメカニズムを示しています。このシナリオでは、Cisco CallManager はメッセージ交換に関わっていないことに注意してください。

図 14-3　ディレクトリ統合が行われていない場合の Cisco IP Phone 社内ディレクトリ アクセスのメッセージ交換



Web サーバのプロキシ機能は、Cisco LDAP Search Component Object Model（COM; コンポーネント オブジェクト モデル）サーバが組み込まれている Cisco IP Phone Services Software Development Kit（SDK; ソフトウェア開発キット）バージョン 2.0 以降を使用して設定できます。次の Web サイトの Developer Support Central から最新の Cisco IP Phone Services SDK をダウンロードできます。

http://www.cisco.com/pcgi-bin/dev_support/access_level/product_support

Log in now リンクをクリックしてログインし、**Voice Technology/AVVID** リスト ボックスから **CallManager - IP phone Services SDK** を選択します。

Cisco IP Phone のディレクトリ アクセスを設定するには、次の手順に従います。

ステップ 1　Microsoft Internet Information Server（IIS）を実行している Web サーバに Cisco IP Phone Services SDK をインストールします。このサーバは Cisco CallManager サーバとは異なるサーバである必要がありますが、企業ネットワーク上の既存の Web サーバでもかまいません（インストレーション手順の詳細は、SDK 製品資料を参照）。

ステップ 2　SDK に付属のマニュアルを使用して、LDAP Search COM オブジェクトとインターフェイスするための Active Server Page（ASP）を作成します。SDK にはサンプルの ASP が用意されていますが、高レベルのカスタマイゼーションが必要な場合は、独自の ASP を記述できます。IP Phone Services SDK Release 3.3 を使用している場合は、サンプルの ldapsearch.asp ページを IIS 仮想ディレクトリに置いてから、次のパラメータを設定して、社内 LDAP ディレクトリ サーバを指すようこのファイルを編集します。

- s.server

  このパラメータを LDAP サーバの名前または IP アドレスに設定します（たとえば、ldap.vse.lab）。
- s.port

  このパラメータを、LDAP サーバ上で LDAP 要求に使用するポートに設定します（標準のポートは 389 です）。
- s.base

  このパラメータを、LDAP ルックアップの検索ベースに設定します。この検索ベースには、ルックアップから返されるすべてのユーザが含まれている必要があります（たとえば、cn=Users, dc=vse, dc=lab）。
- s.AuthName

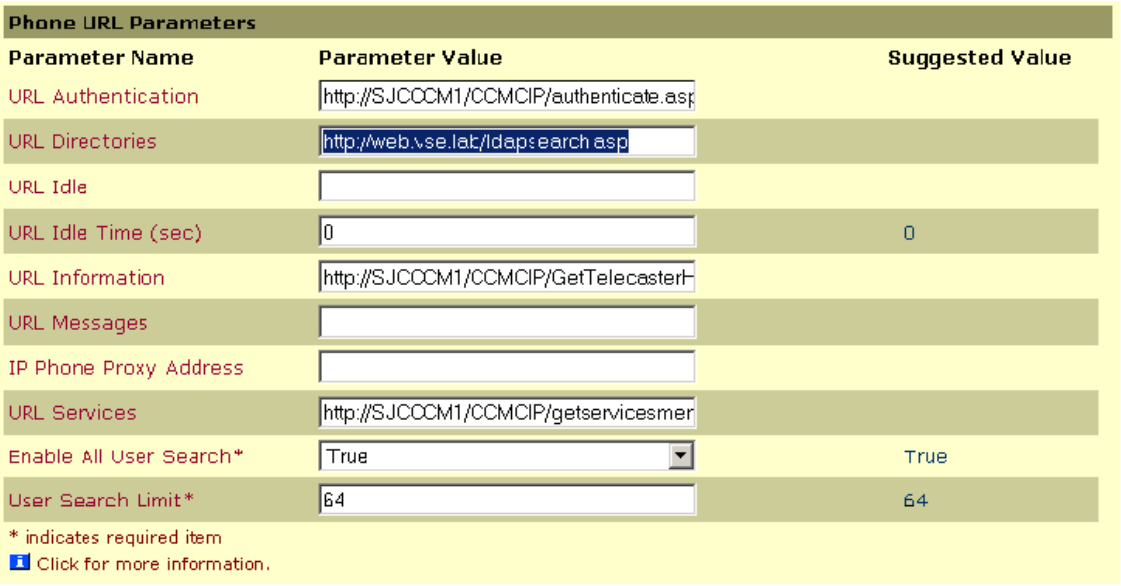
  LDAP サーバがルックアップで認証を要求する場合は、このパラメータを、検索ベースで指定したサブツリーを検索する権限を持つユーザの認定者名に設定します（たとえば、cn=CCMDirMgr, ou=System Accounts, cn=Users, dc=vse, dc=lab）。
- s.AuthPasswd

  LDAP サーバがルックアップで認証を要求する場合は、このパラメータを、検索ベースで指定したサブツリーを検索する権限を持つユーザのパスワードに設定します。

ステップ 3　図 14-4 に示しているように、Cisco CallManager Administration の Enterprise Parameter Configuration ページ（**System** > **Enterprise Parameters**）で、**URL Directories** フィールドを編集します。このフィールドを、前の手順で設定した、Web サーバ上の ldapsearch.asp ファイルへの URL に設定します。

ステップ 4　変更を有効にするために IP Phone をリセットします。

図 14-4　ディレクトリ アクセスを有効にするための Cisco CallManager におけるエンタープライズ パラメータの設定



さらに、Cisco IP Phone のディレクトリ アクセスには、次の特性があります。

- LDAPv3 準拠ディレクトリがすべてサポートされている。
- Cisco CallManager ユーザ プリファレンス（短縮ダイヤル、不在転送、個人用アドレス帳）は、社内 LDAP ディレクトリと統合されない。したがって、ユーザは、Cisco CallManager User Options Web ページにアクセスするために、別のログイン名とパスワードを持ちます。

Cisco CallManager とのディレクトリ統合

CallManager は、組み込み Microsoft SQL データベースを使用して、システムとデバイスの設定データ（たとえば、ダイヤル プラン情報、電話機とゲートウェイの設定、メディア リソースの使用率）を保存します。また、組み込み LDAP ディレクトリを使用して、ユーザとアプリケーションのプロファイル（たとえば、ユーザが制御するデバイス、Computer Telephony Integration（CTI; コンピュータ / テレフォニー インテグレーション）ユーザ パラメータ、個人用アドレス帳のエントリ）を保存します。

SQL データベースと LDAP ディレクトリはどちらも、クラスタ内の各 Cisco CallManager サーバで実行され、サーバ間で複製アグリーメントが自動的にセットアップされます。パブリッシャ サーバには、SQL データベースと LDAP ディレクトリの両方のマスター コピーが入っています。パブリッシャ サーバは、すべてのサブスクライバ サーバへの複写を処理します。サブスクライバ サーバには、両方のリポジトリの読み取り専用コピーが入っています。

（注）　この章の例と推奨事項は、いくつかの新機能と機能拡張が導入された Cisco CallManager Releases 4.0 および 4.1 に基づいています。旧バージョンの Cisco CallManager を実行している場合は、一部の動作が異なっていたり、一部の機能が使用できなかったりする場合があります。

アプリケーション固有の情報を LDAP ディレクトリに保存するために、Cisco CallManager は、組み込みディレクトリの使用時と、社内ディレクトリとの統合時の両方で有効な方法を採用します。

通常は、ディレクトリ ベンダーが異なると、異なる User オブジェクト モデルが使用され、各モデルが複数の標準外の追加属性を持っています。このため、Cisco CallManager は、User オブジェクトの標準 LDAPv3 コア属性だけを使用します。User オブジェクトは、次の属性が入っている補助クラス ciscoocUser で拡張されます。

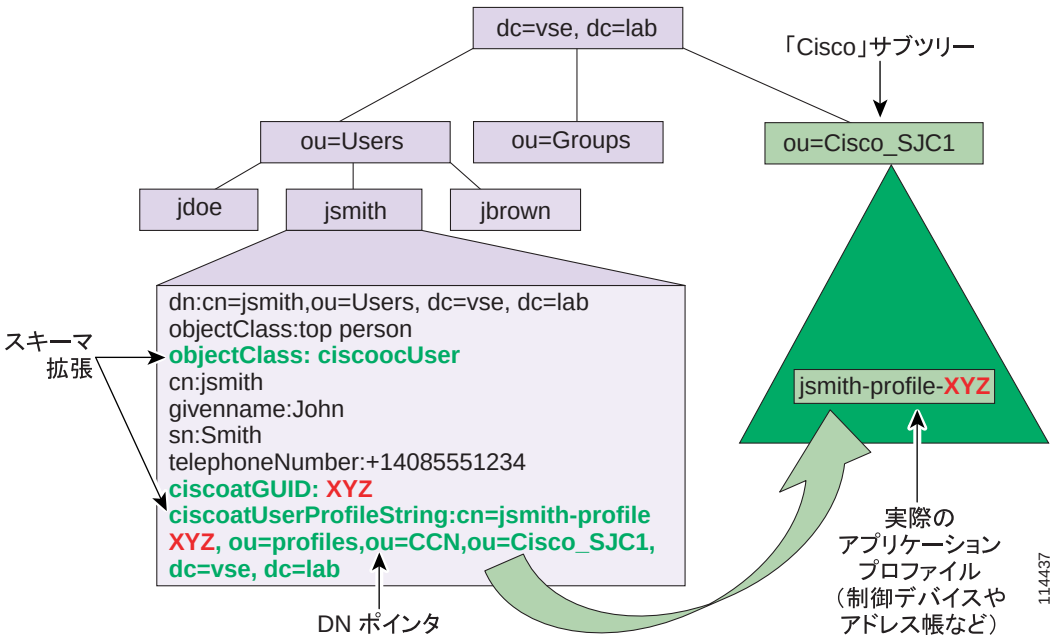
- ciscoatGUID

  この属性は、ディレクトリ内のユーザを固有に識別します。
- ciscoatUserProfile

  この属性は、以前のバージョンの Cisco CallManager および他のアプリケーションによって使用されます。この属性は下位互換性のために残っています。
- ciscoatUserProfileString

  この属性は、ユーザのアプリケーション固有のプロファイルが入っている、ディレクトリ内の別のオブジェクトを指す認定者名ポインタです。この方法により、コア User オブジェクトに対する影響が最小限に抑えられ、アプリケーション特有のすべての情報を、通常 Cisco サブツリー、CISCOBASE、または Cisco Directory Information Tree（DIT; ディレクトリ インフォメーション ツリー）と呼ばれる、ディレクトリ内の別個の Organizational Unit（OU; 組織ユニット）に保存できます。図 14-5 では、このプロセスを示しています。

図 14-5　アプリケーション特有のユーザ情報をディレクトリに保存するための Cisco CallManager の方法



ciscoatUserProfileString 属性が指すオブジェクトは、ciscoocUserProfile と呼ばれる構造型オブジェクト クラスに属しています。このオブジェクトの主な目的は、ユーザのロケール、ユーザの Cisco IP Manager Assistant（IPMA）アシスタント、ディレクトリと統合されているすべてのシスコ アプリケーションのさまざまな固有プロファイル オブジェクトへのポインタなど、ユーザに固有のいくつかの詳細を保存することです。Cisco CallManager が使用するアプリケーション プロファイルは ciscoCCNocAppProfile と呼ばれる補助クラスに属し、Cisco CallManager はここにユーザのエクステンション モビリティ PIN、ユーザが制御するデバイスのリスト、ユーザが CTI アプリケーションの使用を許可されているかどうかなどの情報を保存します。Cisco CallManager は「Cisco」サブツリーの下にこれらのプロファイル オブジェクトの両方を作成します。

（注）　ユーザに関連付けられるデバイスのリストは、多値属性としてディレクトリに保存されます。組み込み Cisco CallManager ディレクトリを使用している場合は、ユーザに関連付けることのできるデバイスの最大数は 2,000（クラスタ内のすべてのサブスクライバがデュアル CPU サーバである場合は 2,500）です。ただし、Microsoft Active Directory では、多値属性の値の数が 850 に制限されます。したがって、CallManager を Microsoft Active Directory と統合する場合、ユーザに関連付けることのできるデバイスの最大数は 850 になります。

Cisco Customer Directory Configuration Plugin

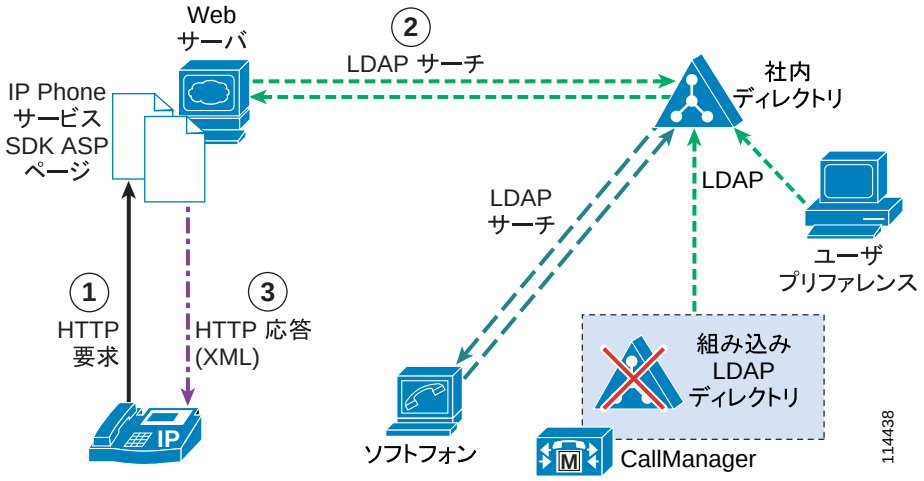
Cisco CallManager を外部 LDAP ディレクトリと統合するには、Cisco CallManager にバンドルされている Cisco Customer Directory Configuration Plugin を実行します（**Applications** > **Install Plugins**）。このプラグインを利用する主な目的は、次の 3 点です。

- 社内ディレクトリ スキーマを拡張して、アプリケーション固有のオブジェクトと属性に対応すること。
- 「Cisco」サブツリーに、Cisco CallManager が必要とする設定オブジェクトを取り込むこと。
- 社内ディレクトリを使用するように Cisco CallManager を設定し、その組み込みディレクトリを使用不可にすること。

通常、このプラグインを Cisco CallManager 上でローカルに実行すると、スキーマの更新が行われます。ただし、Cisco CallManager Release 4.0 以降では、LDAP Data Interchange Format（LDIF）ファイルを別個に作成する新しいオプションが用意されています。このため、LDIF ファイルを使用して、社内ディレクトリのスキーマ マスター サーバ上で直接スキーマの更新を行うことができます。このオプションを使用すると、さまざまなグループのユーザがその作業の関連部分を実行でき、Cisco CallManager がスキーマ マスター サーバに対してローカルでない場合に、ネットワークを介して更新する必要性が低くなります。

プラグインの実行後、Cisco CallManager は、社内ディレクトリを効果的に使用して、ユーザ プリファレンスを保存します。前の項で説明しているように、Cisco IP テレフォニー エンドポイントもこの社内ディレクトリにアクセスできる場合は、図 14-6 に示すようなシナリオになります。

図 14-6　Cisco CallManager が社内ディレクトリと統合されている場合の Cisco IP Phone 社内ディレクトリ アクセスのメッセージ交換



セキュリティの考慮事項

Cisco CallManager Release 4.1 以降では、Cisco CallManager と組み込みディレクトリの間の通信が、デフォルトで、LDAPS とも呼ばれる LDAP over Secure Socket Layer（SSL）を使用するように設定されています。

社内ディレクトリと統合する場合も、LDAP over SSL を有効にすることができます。これにより、すべての機密 LDAP データが保護接続を介して伝送されることが保証されます。LDAP over SSL オプションは、Cisco Customer Directory Plugin の一部として設定できます。このオプションでは、社内ディレクトリと共有され、同じ認証局によって発行された証明書が必要となります。

Cisco CallManager で LDAP over SSL が有効である場合は、次に示す Cisco IP Communications アプリケーションもこのセキュア チャネルを介してディレクトリと通信します。

- Cisco CallManager Administration 内のユーザ ページ
- Cisco Multi-Level Administration（MLA; マルチレベル管理）
- Cisco IP Phone Options ページ
- エクステンション モビリティ アプリケーション：Cisco CallManager サーバ上で実行されているエクステンション モビリティ アプリケーションと、社内ディレクトリの間の通信に SSL が使用されます。ただし、IP Phone とエクステンション モビリティ アプリケーションの間の通信には SSL が使用されず、HTTP が使用されます。

- Cisco CTI Manager
- Serviceability および Cisco Real-Time Monitoring Tool（RTMT）
- Cisco CDR Analysis and Reporting（CAR）
- Cisco IP Manager Assistant（IPMA）サービス
- Cisco Bulk Administration Tool（BAT）

ドメインへの Cisco CallManager サーバの追加

Microsoft Windows ドメインへの Cisco CallManager サーバの追加は、Cisco CallManager と外部ディレクトリの統合とは大きく異なります。これらの操作は相互排他的ではありませんが、異なる意味を持つ完全に独立した操作です。

- Cisco CallManager サーバを Microsoft Windows Active Directory（AD）ドメインに追加すると、ドメイン ポリシーが Windows 2000 Server オペレーティング システムに適用されることがあります。また、このような追加は Cisco CallManager サーバ自体の管理だけに影響を及ぼします。
- Cisco CallManager を外部ディレクトリ（Microsoft Active Directory や Netscape Directory Server など）と統合すると、Cisco CallManager がすべてのユーザ情報およびプリファレンスをそのディレクトリに保存します。ただし、このような統合は、Cisco CallManager サーバ自体の管理に影響を及ぼしません。

Cisco CallManager サーバをワークグループ サーバとして保持することをお勧めします。ただし、サーバをドメインに追加する場合は、サーバの正常な動作を妨げる可能性のあるドメイン ポリシーをサーバに適用することは避けてください。

サーバをドメインに追加する場合のその他の推奨事項については、次の Web サイトで入手可能な最新の Cisco CallManager 製品資料を参照してください。

http://www.cisco.com

ディレクトリ統合のベスト プラクティス

ディレクトリ統合プロセスには、ネットワーク内の複数のコンポーネントおよびサービスが関連します。したがって、ディレクトリ統合プロセスは、慎重に計画して実装する必要があります。この項では、次のトピックを扱います。

- ディレクトリ統合の計画（P.14-11）
- 統合のためのディレクトリの準備（P.14-12）
- Cisco CallManager とディレクトリの統合（P.14-17）
- ディレクトリ統合の管理（P.14-20）

（注） 既知の Cisco CallManager 統合の大部分は、Microsoft Active Directory（AD）との間で行われているため、ここでは AD に対するベスト プラクティスを中心に説明します。ただし、この項で述べる推奨事項やベスト プラクティスのほとんどは、Cisco CallManager によってサポートされているもう 1 つのディレクトリ製品 Sun/iPlanet Netscape Directory Server にも適用されます。

ディレクトリ統合の計画

ディレクトリは、企業全体のリソースであり、多数のアプリケーションおよびエンド ユーザによって使用される可能性があるため、統合を慎重に計画して、他のすべてのアプリケーションへの影響を最小限に抑えることが重要です。

ヒント 統合を開始する前に、社内のディレクトリ チームが計画、設計、および実装の各段階に携わっていることを確認してください。

この章で前述したように、Cisco CallManager および他のアプリケーションを外部ディレクトリと統合する場合は、ディレクトリ スキーマを拡張する必要があります。スキーマの拡張は、細心の注意を要する操作です。たとえば、Microsoft Windows 2000 Active Directory の場合、スキーマの変更を取り消すことはできません。ディレクトリの損傷を避けるために、次の予防措置を講じる必要があります。

- 計画したスキーマ変更を社内のディレクトリ チームと共に再検討する。この作業は、社内の変更制御手順の一部である必要があります。
- 実験用設備で実稼働ディレクトリのレプリカを作成し、そのレプリカに対して統合をテストする。
- 統合前に実稼働ディレクトリ（データとスキーマの両方）をバックアップし、復元が必要となったときにデータとスキーマを正常に復元するための有効なバックアウト計画を用意しておく。
- 他のアプリケーションおよびエンド ユーザへの影響を最小限に抑えるため、オフピーク時にスキーマの拡張を計画して実行する。

上記の予防措置リストを見て不安になったとしても、実際は、スキーマの拡張によって、バックアウトを必要とするような問題が発生することはほとんどありません。ただし、操作がいかに安全であると認識されていても、予期せぬ問題から回復できるようにするための予防措置を怠ってリスクを高めることのないよう注意してください。

もう 1 つの重要な考慮事項は、音声アプリケーションはディレクトリと統合するとすぐに、そのディレクトリに依存して正常な動作を行うため、ディレクトリ サーバに到達できないと音声システムに悪影響が及ぶ可能性があるということです。

たとえば、ディレクトリが突然使用できなくなると、エンド ユーザが Cisco CallManager User Options Web ページにログインして自分のプリファレンスを設定できなくなったり、エクステンション モビリティ ユーザ、Attendant Console オペレータ、および IPCC Express エージェントがログインもログアウトもできなくなったり、名前によるダイヤル機能が使用できなくなったりします。

このような問題を避けるため、すべてのシスコ音声アプリケーションに高いアベイラビリティを提供できるようにディレクトリ インフラストラクチャを設計する必要があります。次のいずれかの方法で、このような高いアベイラビリティを実現できます。

- ディレクトリ複製メカニズムを活用して、ディレクトリ サーバをシスコ音声アプリケーションと同じロケーションに置く。
- Cisco IOS ソフトウェアの Server Load Balancing（SLB）などのサーバ ロードバランシング メカニズムを使用して、特定のキャンパスまたはデータ センタ内でサーバの冗長性を実現し、できる限りローカル サーバへのアクセスが行われるようにする。
- ディレクトリ プラグインを設定する場合は、特定のドメイン コントローラ ホスト名ではなく、Domain Name System（DNS; ドメイン ネーム システム）ドメイン名を使用する。

冗長サーバがある場合は、DNS によって最初に返される名前のサーバが、後の応答で返される名前のサーバほど、Cisco CallManager に対してローカルでないことがあります。また、DNS サーバでラウンドロビン機能が有効である場合、DNS サーバは応答で意図的に複数のアドレスを 1 つずつ順番に返します。クライアント側の DNS キャッシュ タイムアウトなどのメカニズム、およびその間に同じドメインに対して照会する他のクライアントによっては、Cisco CallManager が 2 つの連続した操作を 2 つの異なる Domain Controller（DC; ドメイン コントローラ）に対して行うことがあります。前述のローカル性の問題の他に、DNS 冗長性を使用すると、最初の操作とその後の照会の間にディレクトリが複製されなかった場合、最初の操作で作成したオブジェクトを、その後の照会で別の DC に対して検索しても見つけることができないという問題もあります。したがって、DNS を使用して実装を冗長にすることを決定する前に、これらの問題が配置に影響を及ぼさないことを確認してください。

また、正しい LDAP 照会には DNS が必要であることにも注意してください。Cisco CallManager は、LDAP 照会で返されるどの DC のホスト名も解決できる必要があります。

（注）　Microsoft Windows 2000 DNS には最初にローカル リソースを返す機能（LocalNetPriority）が備わっていますが、この機能は要求側クライアントのクラスフル IP アドレスの調査に基づいています。したがって、この機能はサブネット化されたネットワークではあまり役に立ちません。この機能については、Microsoft Knowledge Base 記事 177883 で説明されています（http://support.microsoft.com/ を参照してください）。Windows 2000 DNS を使用しない場合は、選択した実装のどの機能でこれらの問題を軽減できるかを調べる必要があります。これらの推奨事項は、Cisco CallManager が DNS を使用するように設定され、その DNS が Active Directory によって使用される DNS インフラストラクチャと同じであるという前提に基づいています。

統合のためのディレクトリの準備

Microsoft Windows 2000 Active Directory では、スキーマ変更を許可するようにドメイン コントローラを設定する必要があります。この要件は、スキーマ マスター（変更が行われるロケーション）として機能するドメイン コントローラだけに適用され、次の Web サイトで入手可能な Microsoft Knowledge Base 記事 285172 で詳しく説明されています。

http://support.microsoft.com

Cisco CallManager を Microsoft Windows 2000 Active Directory と統合し、Microsoft Exchange 2000 が同じフォレスト内に共存する必要がある場合は、追加の準備手順が必要になります。Cisco CallManager は、RFC 2798 で定義されている iNetOrgPerson クラスによって指定された

labeledURI 属性を使用します。Microsoft は、現在、Exchange 2000 に対して別の方法でこの属性を定義しています。これにより、Cisco CallManager スキーマとの間で名前の衝突が発生します。この問題については、Microsoft Knowledge Base 記事 314649（http://support.microsoft.com から入手可能）で説明されています。次の Web サイトから iNetOrgPerson キットを入手できます。

http://msdn.microsoft.com/library/en-us/dnactdir/html/inetopkit.asp

注意　スキーマを拡張する前に、必ずディレクトリをバックアップしてください。復元メカニズムが必要となる前に、使用する予定の復元メカニズムを必ずテストしてください。

Cisco CallManager のディレクトリ スキーマを拡張するには、クラスタのパブリッシャ サーバから Cisco Customer Directory Configuration Plugin を実行し、次のベスト プラクティスに従います。

- プラグインを実行する場合は、セットアップ タイプとして必ず **Custom** を使用する。Express セットアップ タイプは、Cisco CallManager や他のシスコ音声アプリケーション専用のスタンドアロン ドメインとの統合だけに適しています。既存のドメインと統合する場合は、Express セットアップを使用しないでください。
- プラグイン設定画面では、**Install Schema on the Schema Master** オプションだけを選択する。
- スキーマ マスター サーバが Cisco CallManager に対してローカルであるか、またはスキーマ マスター サーバと Cisco CallManager の間に高速接続が存在することを確認する。どちらも実現できない場合は、プラグインで LDIF ファイルの作成だけを行い、そのファイルを使用してスキーマ マスター上で直接スキーマを更新することを検討します。
- この段階で、プラグインに、Active Directory の Schema Admins グループのメンバーであるユーザのクレデンシャル（認定者名とパスワード）を入力する。このクレデンシャルは、通常の Cisco CallManager 動作ではなく、スキーマの拡張だけに使用されます。

（注）　大規模な AD フォレストまたは複雑なトポロジがある場合は、スキーマの変更がフォレスト内のすべてのドメインおよびすべてのドメイン コントローラに伝搬されるまで、しばらく時間がかかることがあります。この伝搬のために十分な時間をとってから準備プロセスを続行するか、または必要に応じて強制的に複製を行ってください。

スキーマが拡張されるとすぐに、Cisco CallManager クラスタおよび他のシスコ音声アプリケーションによって使用される「Cisco」OU（サブツリー）を作成する場所を決めることができます。統合される Cisco CallManager クラスタごとに 1 つの組織ユニット（OU）が必要です。

単一ドメインの AD または Netscape Directory Server を使用する配置では、位置は重要ではありません。ツリー内のどこにでも、OU を効果的に配置できます。

マルチドメイン AD フォレストでは、多くの場合、ルート ドメインはユーザもリソースも含まず、プレースホルダ ドメインとして使用されるため、通常、「Cisco」サブツリーは子ドメイン内に存在します。このタイプのマルチドメイン トポロジでは、地理的な境界に基づいてドメインを作成できます。したがって、各ロケーションが各ドメインのローカル ドメイン コントローラを持つ可能性が低くなります。ネットワークを介した複製トラフィックを減らすため、ドメイン コントローラは、通常、必要な場所だけに配置されます。この点を念頭に置いて、所定のクラスタの Cisco OU を、そのクラスタによってサービスを提供されるユーザの大部分を含むドメイン内に置くことをお勧めします。

図 14-7 では、マルチドメイン単一ツリー AD フォレストを示しています。このフォレストでは、2 つの CallManager クラスタの「Cisco」OU が、2 つの個別の子ドメイン emea.vse.lab と amer.vse.lab の中に作成されています。

図 14-7　マルチドメイン単一ツリー AD フォレスト

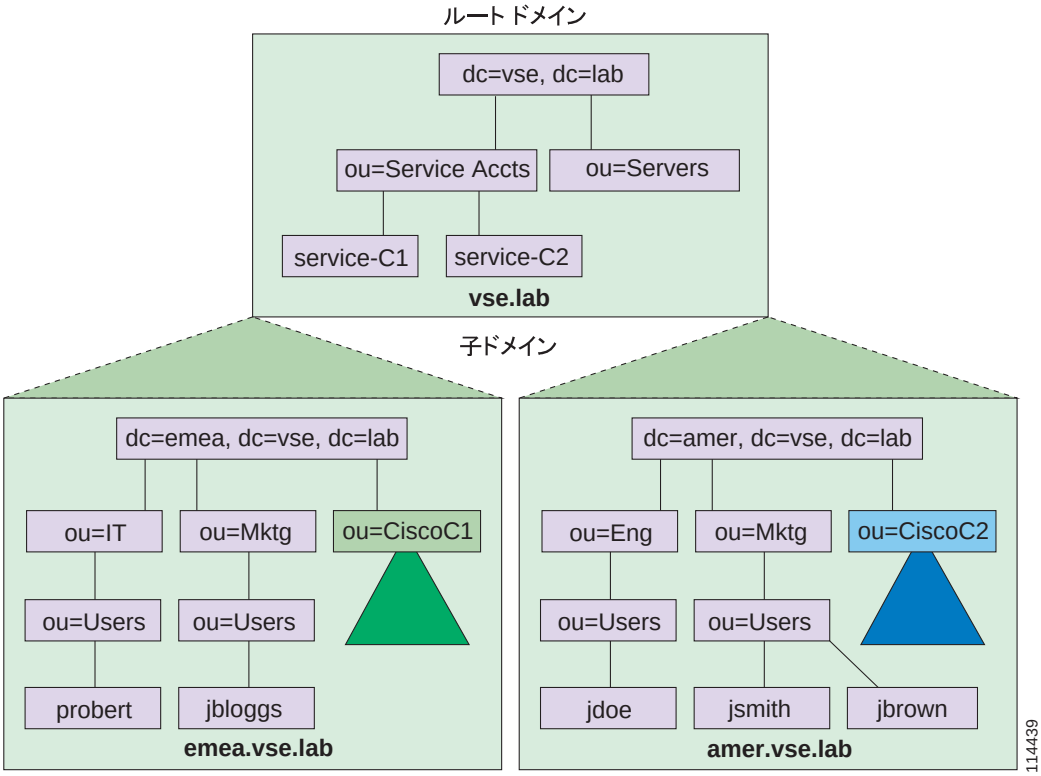
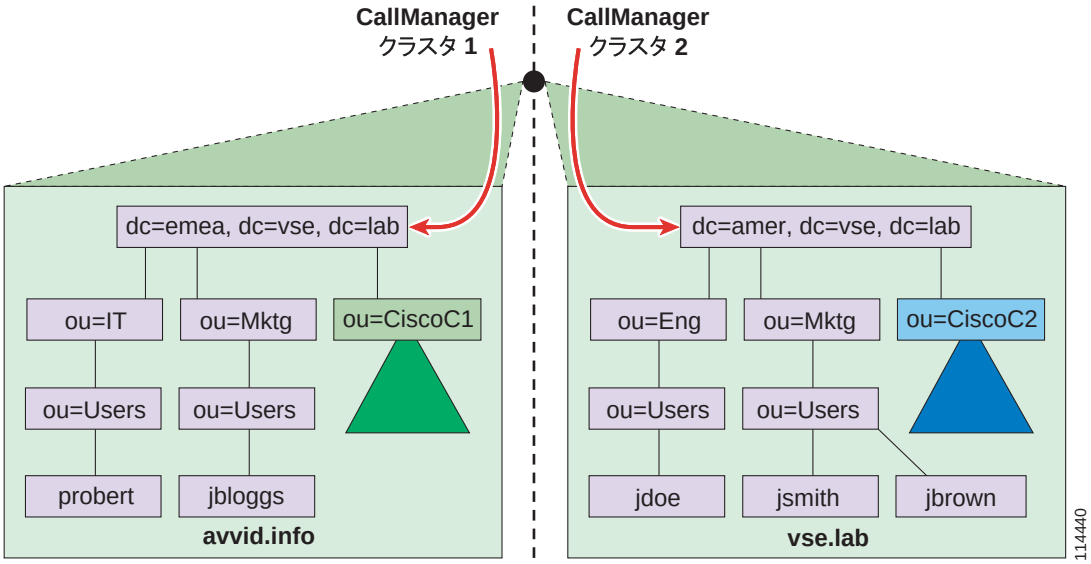


図 14-7 では、各クラスタが、集中型コール処理モデルで、地理的に対応する場所にサービスを提供します。したがって、AD に保存されているユーザ データもローカルであることが保証されます。この設計により、ローカルでない DC から情報を取り出す必要がなくなり、検索で関連情報を見つけるために必要な LDAP 照会の数が減ります。

Cisco CallManager クラスタが、異なるドメインのユーザにサービスを提供するようにすることはお勧めしません。なぜなら、ドメイン コントローラがローカルでないドメインが含まれている場合、ユーザ データ取得中の応答時間が最適ではなくなる可能性があるためです。ただし、マルチドメイン AD を作成する理由（つまり、地理、帯域幅、または組織構造）は、通常、複数のクラスタを必要とする理由と同じであるため、このシナリオは一般的ではありません。

現在、クラスタは AD フォレスト内の複数のツリーにまたがることはできません。なぜなら、ツリーは、LDAP 照会の要件である連続したネームスペースを持たないためです。クラスタは 1 つのドメインまたは単一のツリー内に存在でき、（前述のように）マルチツリー フォレスト内に存在することもできます。ただし、図 14-8 に示しているように、特定のクラスタのすべてのユーザが同じネームスペースに含まれている必要があります。

図 14-8　Cisco CallManager クラスタは単一ツリー（連続したネームスペース）に含まれる必要がある



User Search Base は、ディレクトリと統合する場合に Cisco CallManager によって使用されるもう 1 つの重要な要素です。User Search Base は、クラスタ内のデバイスと関連付けることができるユーザを検索するために Cisco CallManager によって使用されるサブツリーのルートを示します（このパラメータを設定する方法については、P.14-17 の「Cisco CallManager とディレクトリの統合」の項を参照してください）。

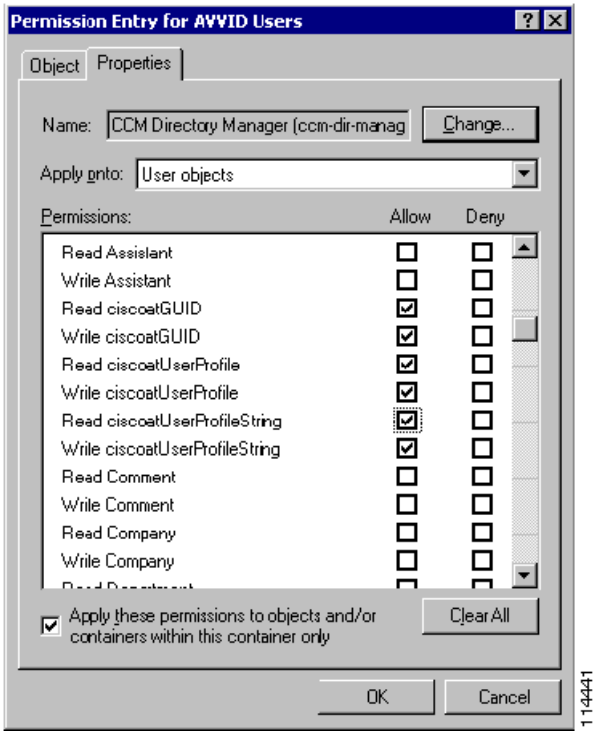
Cisco CallManager や他のシスコ音声アプリケーションがディレクトリに対するアクセスおよび管理に使用できる、特別なユーザ アカウントを作成する必要があります。Cisco CallManager クラスタごとに 1 つのアカウントが必要です。なぜなら、これにより、必要な場合にだけ各アカウントに特定の権限を付与し、企業の他の部門に影響を与えることなく、クラスタごとの簡単な管理を行うことができるためです。この章の例では、このアカウントの名前を CCM Directory Manager としていますが、このユーザ アカウントに異なる名前を付けてもかまいません。

各 CCM Directory Manager アカウントには、ディレクトリ内で少なくとも次の権限を付与する必要があります。

- それぞれの「Cisco」OU サブツリーに対する **Read/Write/Create all child objects/Delete all child objects** 特権。これらの権利は、オブジェクトとプロパティの両方で **This object and all child objects** に適用されるように設定する必要があります。AD では、Active Directory Users and Computers（ADUC）内のセキュリティの詳細オプションを使用して、この特権を設定できます。デフォルトでは、そのオブジェクトだけに適用するように設定されているため、権利を変更する必要があります。
- User Search Base およびその下に含まれているすべての OU に対する **Read** 特権。ツリーの下部で継承がブロックされていない限り、User Search Base レベルだけでこの特権を設定できます。
- User Search Base の下に含まれているすべての User オブジェクトの ciscoatGUID、ciscoatUserProfile、および ciscoatUserProfileString 属性に対する **Read/Write** 特権。AD では、ADUC 内のセキュリティの詳細オプションを使用して、この特権を設定できます。

ヒント　AD では、User Search Base 内のすべての User オブジェクトの ciscoatGUID、ciscoatUserProfile、および ciscoatUserProfileString 属性に対する権限を設定するには、User Search Base のルートで組織単位（OU）の Advanced security ウィンドウから CCM Directory Manager ユーザを選択します（この章では、このユーザの名前を CCM Directory Manager としていますが、ユーザ名は異なっていてもかまいません）。その後、**View/Edit** をクリックし、図 14-9 に示しているような、新しいウィンドウの **Properties** タブに移動します。**Apply onto** ドロップダウン メニューから **User objects** を選択し、下にスクロールして ciscoatGUID、ciscoatUserProfile、および ciscoatProfileString 属性まで移動します。これらすべてに対して **Write** 権限を許可します。

図 14-9　Active Directory でのユーザ アカウントに対する権限の設定



ヒント　CCM Directory Manager アカウントを作成する場合は、**Password never expires** オプションを設定してください。パスワードを変更する場合は、Cisco CallManager から CCMPwdChanger ユーティリティを実行します。この方法により、AD でパスワードが更新され、Cisco CallManager でレジストリが更新されて、ディレクトリ初期化ファイルが更新されます。

Cisco CallManager とディレクトリの統合

前項の説明に従ってディレクトリを準備した後、Cisco Customer Directory Configuration Plugin を再び実行して統合を行うことができます。この時点で考慮する必要のある 2 つの主な概念は、User Search Base と User Creation Base です。

（注）　User Creation Base は、Cisco CallManager Release 4.0 で導入されました。以前のバージョンの Cisco CallManager では、ユーザの作成にも User Search Base が使用されます。

前項で述べたように、User Search Base パラメータは、Cisco CallManager によってすべてのユーザ検索に使用されるサブツリーのルートを示します。

User Creation Base パラメータは、次のようなシステム アカウントを作成する場所を Cisco CallManager に指示します。これらのアカウントは、いくつかのアプリケーションおよびそのアプリケーションにバンドルされている機能で必要となります。

- CCM Administrator：Cisco CallManager Multilevel Administration Access（MLA）によって使用されます。
- CCM SysUser：コールバックおよびエクステンション モビリティによって使用されます。
- IPMA SysUser：Cisco IP Manager Assistant によって使用されます。

Cisco CallManager はシステム アカウント ユーザを認証する前に検索できる必要があるため、User Creation Base は User Search Base 内に含まれている必要があります。

User Search Base を設定するには、クラスタによってサービスを提供されるユーザが置かれている場所を参照し、そのようなユーザをすべて含む第 1 レベルに User Search Base を設定します。User Search Base を低いレベルに設定するほど、応答時間やパフォーマンスが向上します。なぜなら、検索で多くの照会を行ったり、低速 WAN リンク通過してリモート ドメイン コントローラに到達したりする必要がなくなるためです。また、クラスタが必要としないユーザ データを検索で解析する必要もありません。

単一ドメイン AD フォレスト（またはスタンドアロン Netscape Directory）では、User Search Base を、Cisco CallManager クラスタのすべてのユーザを含む最下位レベルの組織ユニット（OU）（たとえば、ou=AVVID Users, dc=vse, dc=lab）に設定します。この OU は、ドメインのルート（たとえば、dc=vse, dc=lab、または o=avvid.lab）になる場合もあります。それは、ユーザがその OU の直下の複数の OU に散在している場合です。

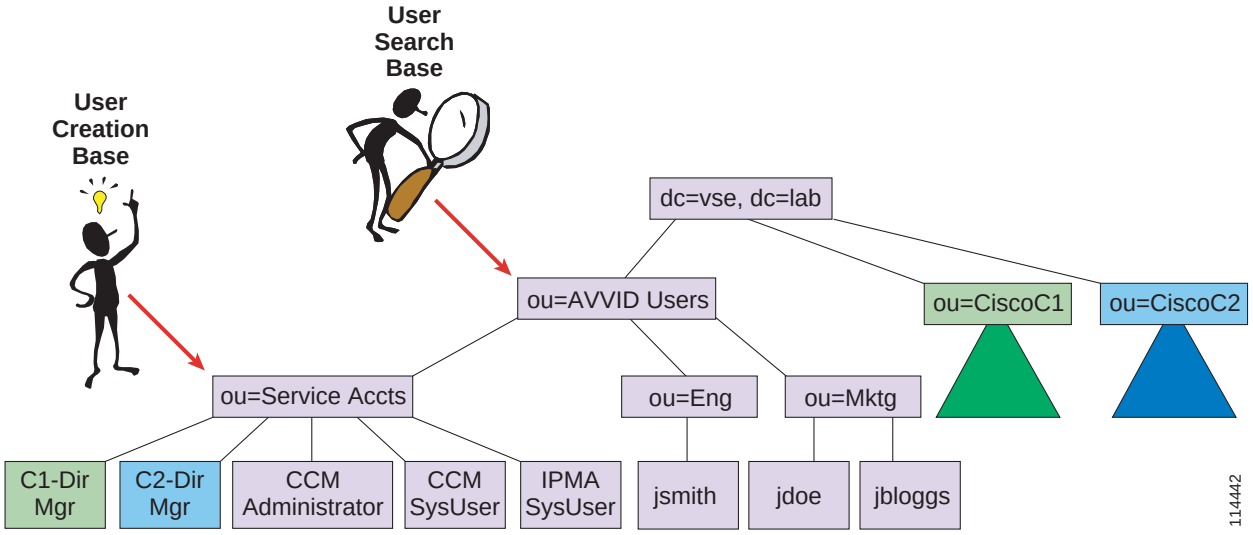
マルチドメイン AD フォレストでは、特定の Cisco CallManager クラスタのユーザを単一のドメイン内に保持するようにし、前述のガイドラインに従います。ユーザが複数のドメインに散在しているため、単一のドメイン内に保持できない場合は、Cisco CallManager クラスタによってサービスを提供されるユーザのドメインをすべて含むツリー内の最下位ポイントに User Search Base を設定します。サービスを提供される複数の子ドメインが最上位レベル ドメインの直下にある構造では、User Search Base を AD フォレスト全体のルートに設定する必要があります。ただし、どのような場合でも、サービスを提供される各ドメインのドメイン コントローラを Cisco CallManager と同じ場所に置くか、またはネットワークの回復力と高速性を十分高くして、ローカル検索に比べてリモート検索でパフォーマンスが大きく低下しないようにする必要があります。

（注）　User Creation Base は User Search Base 内に存在する必要がありますが、User Creation Base 内に作成されるシステム アカウントに既存の Active Directory ユーザ ポリシーが適用されないように注意してください。システム アカウントにユーザ ポリシーが適用されないようにする簡単な方法は、アカウントをサブ OU 内に入れ、その OU に Group Policy Object（GPO）が継承されないようにすることです。

複数の Cisco CallManager クラスタを同じ AD フォレストと統合できます。ただし、お客様の AD 構成と、Cisco CallManager と共に配置されてディレクトリを使用できるシスコ音声アプリケーションの組み合せが多数である可能性があるため、マルチクラスタ統合を進める前に、シスコのエンジニアリング チームに特別なサポートを要請する必要があります。お近くのシスコの代理店に連絡して、サポートを要請してください。Cisco CallManager 以外のシスコ音声アプリケーション（CDR Analysis and Reporting ツール、Multilevel Administration Access、IP Contact Center、IPCC Express など）を配置する場合は、追加の制限が適用されることがあります。このような他製品の詳細については、それぞれのオンライン マニュアルおよびリリース ノートを参照してください。

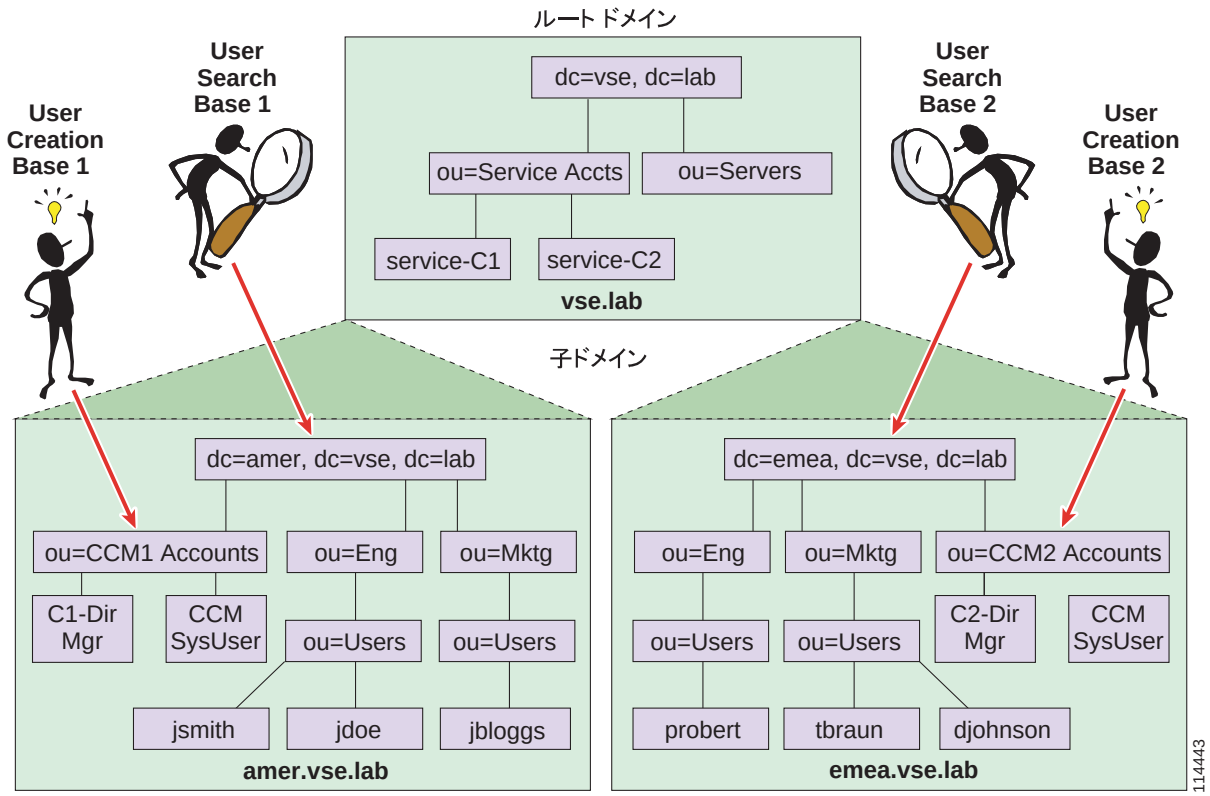
複数の Cisco CallManager クラスタを同じ AD ドメイン（またはスタンドアロン Netscape Directory）と統合する場合は、図 14-10 で示しているように、同じ User Creation Base を指定することによって、クラスタ間でシステム アカウントを共有できます。

図 14-10　単一 AD ドメイン内の User Search Base と User Creation Base の設定



複数の Cisco CallManager クラスタをフォレスト内の異なる AD ドメインと統合する場合は、図 14-11 で示しているように、User Creation Base を関連ドメイン内の OU に設定して、クラスタごとに異なる User Creation Base を定義することをお勧めします。

図 14-11　マルチクラスタ マルチドメイン フォレスト内の User Search Base と User Creation Base の設定



ヒント

システム アカウントおよびサービス アカウントが Cisco CallManager Administration に表示されないようにするには、ユーザの Description フィールドに **CiscoPrivateUser** という文字列を追加します。CCM Administrator、CCM SysUser、および IPMA SysUser の各アカウントの場合は、このフィールドがデフォルトで設定されていますが、CCM Directory Manager アカウントにも問題なくこの Description を追加できます。Description フィールドを更新するには、Microsoft ADSIEdit（Windows 2000 Support Tools の一部として使用できる Active Directory Service Interfaces）または他の LDAP ツールを使用してください。

User Search Base および User Creation Base をどのように設定するか決めた後、クラスタ内の Cisco CallManager パブリッシャ サーバ上で Cisco Customer Directory Configuration Plugin を再び実行できます。この手順を実行する場合は、次のベスト プラクティスに従ってください。

- **Custom** プラグイン セットアップ タイプを選択し、**Configure Active Directory** オプションと **Enable CallManager Integration with Active Directory** オプションだけを選択する。
- Cisco CallManager と同じ LAN に置かれているドメイン コントローラのホスト名を指定する。または、DNS を使用しており、このドメインのすべてのドメイン コントローラが Cisco CallManager と同じ LAN に置かれている場合は、ドメイン名を使用します。ディレクトリ統合で高いアベイラビリティを実現する方法の詳細については、P.14-11 の「ディレクトリ統合の計画」を参照してください。

パブリッシャ サーバ上でこれらの手順を完了した後、3 つのシステム アカウントのパスワードを設定します。これを行うには、Cisco CallManager にバンドルされている CCMPwdChanger ツールを使用するか（**Start** > **Run** を選択し、**cmd** と入力して DOS ウィンドウを開き、**CCMPwdChanger** と入力して **Enter** キーを押します）、または社内ディレクトリのインターフェイス（たとえば、Active Directory の場合は ADUC）を使用します。パスワードが期限切れになったり、最初のログインで変

更するよう設定されたりしないように、これらのユーザのパスワード ポリシーを設定することをお勧めします。このパスワード ポリシーを使用することで、これらのアカウントに GPO が適用されないようにすることもできます。

有効期限ポリシーを適用すると、パスワードが期限切れになったときに Cisco CallManager が動作を停止しますが、期限切れのパスワードが問題であることを知らせる警告は表示されません。たとえば、3　か月ごとにパスワードの変更を必要とするポリシーがある場合は、3　か月ごとに CCMPwdChanger ツールを実行する必要があります。

前述の手順をすべて完了した後、Cisco CallManager クラスタ内のサブスクライバ サーバごとに Cisco Customer Directory Configuration Plugin を実行できます。

（注）　統合を行う場合、Cisco CallManager 組み込みディレクトリと社内ディレクトリの間のデータ移行は行われません。組み込みディレクトリに設定したユーザとプロファイルを移行する場合のために、シスコはこのタスクに役立ついくつかの移行スクリプトを開発しました。これらのスクリプトを入手するには、シスコのアカウント チームまたは販売代理店に問い合せてください。これらのスクリプトは、現状のまま、サポートなしで提供されることに注意してください。

ディレクトリ統合の管理

Cisco CallManager を外部ディレクトリと統合した後、ユーザとパスワードの管理手順およびポリシーを適宜設定する必要があります。

次の管理操作には、社内ディレクトリのインターフェイス（またはサポートされている API）を使用します。

- ユーザの追加
- ユーザの削除
- コア ユーザ属性（表示名、部門、アドレス、パスワードなど）の設定および変更

また、次の管理操作には、Cisco CallManager Administration を使用します。

- CallManager 固有のユーザ属性（PIN やユーザ ロケールなど）の設定
- ユーザとデバイス（IP Phone や CTI ポートなど）の関連付け

デフォルトでは、Cisco CallManager Administration を使用してユーザを追加することも削除することもできません。また、名前や電話番号など、コア ユーザ属性を変更することもできません。Cisco CallManager Administration でユーザを追加および削除できるようにするには、次の Web サイトで入手可能な『*Installing the Cisco Customer Directory Configuration Plugin for Cisco CallManager Release 4.0(1)*』の説明に従って、Cisco CallManager サーバ上の UMDirectoryConfiguration.ini ファイルを修正します。

http://www.cisco.com

この機能は便宜的に提供しているもので、既存のユーザ管理ツールやディレクトリ管理ツールに取って代わるものではありません。この機能は限定的であることに注意してください。通常は、他の使用可能なツールでユーザを追加または削除することをお勧めします。

Active Directory ではパスワードをクリアテキスト LDAP で設定できないため、Cisco CallManager が Microsoft Active Directory と統合されている場合でも、Cisco CallManager Administration でユーザ パスワードを設定することも変更することもできません。ディレクトリ パスワードを安全な方法で変更するには、Cisco CallManager にバンドルされている CCMPwdChanger ツール、またはディレクトリ ベンダーによって提供される管理インターフェイスを使用できます。

Cisco CallManager 上の UMDirectoryConfiguration.ini ファイルを修正した後でも、AD 内のユーザを作成および削除するための十分な権限を CCM Directory Manager アカウントに与える必要があります。

複数の Cisco CallManager クラスタを同じディレクトリと統合する場合は、同じユーザを異なるクラスタ内のデバイスに関連付けることはできないことに注意してください。各ユーザは、どの時点でも、単一の特定の Cisco CallManager クラスタと関連付ける必要があります（もちろん、あるクラスタから別のクラスタにユーザを移動できます。これを行うには、単に、最初のクラスタでユーザとデバイスの関連付けを解除し、2 番目のクラスタでユーザをデバイスに関連付けます）。

ユーザがパスワードを変更したりプリファレンスを設定したりする場合は、次の方法で行うようユーザに指示してください。

- パスワードを変更する場合は、ディレクトリ　アプリケーションのインターフェイスを使用する。Microsoft Active Directory の場合、パスワードの変更は、ユーザの Windows ワークステーションから、または管理ツールを使用する管理者によって行われます。
- PIN または Cisco CallManager プリファレンス（短縮ダイヤルや不在転送番号など）を変更する場合は、Cisco CallManager User Options Web ページを使用する。

（注）　ユーザは AD との統合後でも Cisco CallManager User Options Web ページを使用してパスワードを変更できますが、各ユーザが Windows のパスワードを同時に変更していることに気付かない可能性があるため、この操作はお勧めしません。また、クライアント ワークステーションと Cisco CallManager サーバの間の通信では HTTP が使用されるため、パスワードがクリア テキストでネットワークを通過します。Active Server Page（ASP）から関連コードを削除するだけで、Cisco CallManager User Options Web ページから **Change your Password** オプションを削除できます。

追加、削除、および変更という点では、Cisco CallManager がディレクトリと統合されている場合、次の操作がサポートされないことに注意してください。

- ユーザ名（AD の場合、sAMAccountName）の変更
- ある OU から別の OU へのユーザの移動
- 「Cisco」OU の移動または名前変更

ただし、これらの制限に対処するために、ユーザの CallManager 固有属性（該当するユーザの「Cisco」OU 内のプロファイルや、ciscoatGUID 属性、ciscoatUserProfile 属性、および ciscoatUserProfileString 属性内のデータなど）を手動で削除できます。その後、ディレクトリ管理ツールを使用してユーザ名の変更またはユーザの移動を行ってから、ユーザを Cisco CallManager 加入者として再び追加できます。これは煩雑な手順ですが、この手順によってディレクトリ アプリケーション内でユーザのファイル所有権およびセキュリティ方針が維持されます。

Cisco CallManager のアップグレード

Cisco CallManager のメジャー リリースごとにスキーマが変更される可能性があるため、アップグレード後には必ず Cisco Customer Directory Integration Plugin を実行する必要があります。

複数の Cisco CallManager クラスタを同じディレクトリと統合した場合は、スキーマを 1 回だけ拡張する必要があります。クラスタが、異なる Cisco CallManager リリースを実行している場合は、最新のリリースを実行しているクラスタ内からスキーマを拡張する必要があります。