CHAPTER 16

LDAP 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。

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、すべてのユーザ情報を、複数のアプリケーションで利用できる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 Unified CallManager 5.0 に基づく Cisco Unified Communications システムを社内 LDAP ディレクトリと統合する場合の、設計上の主な原則について説明しています。この章の構成は、次のとおりです。

- ディレクトリ統合とは（P.16-2）

  ここでは、一般的な企業の IT 部門における社内 LDAP ディレクトリとの統合に関して、さまざまな要件を分析します。

- 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.16-4）

  ここでは、Cisco Unified Communications エンドポイントのディレクトリ アクセスを有効にする技術的なソリューションについて説明し、そのソリューションに基づく設計上のベスト プラクティスを示します。

- Cisco Unified CallManager 5.0 でのディレクトリ統合（P.16-6）

  ここでは、Cisco Unified CallManager 5.0 でのディレクトリ統合に関して、技術的なソリューションについて説明し、設計上のベスト プラクティスを示します。LDAP 同期機能や LDAP 認証機能などを扱います。

この章で説明する考慮事項は、Cisco Unified CallManager 5.0 とそれにバンドルされているアプリケーション（エクステンション モビリティ、Cisco Unified CallManager Assistant、WebDialer、Bulk Administration Tool、および Real-Time Monitoring Tool）に適用されます。

これより前の Cisco Unified CallManager リリースについては、『*Cisco Unified Communications SRND for Cisco Unified CallManager 4.0 and 4.1*』を参照してください。その他すべて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マニュアルを参照してください。

http://www.cisco.com

特に、Cisco IP Contact Center については、次の Web サイトで入手可能な『*Cisco Cisco Unified Contact Center Enterprise Edition SRND*』および『*Cisco Cisco Unified Contact Center Express SRND*』を参照してください。

http://www.cisco.com/go/srnd

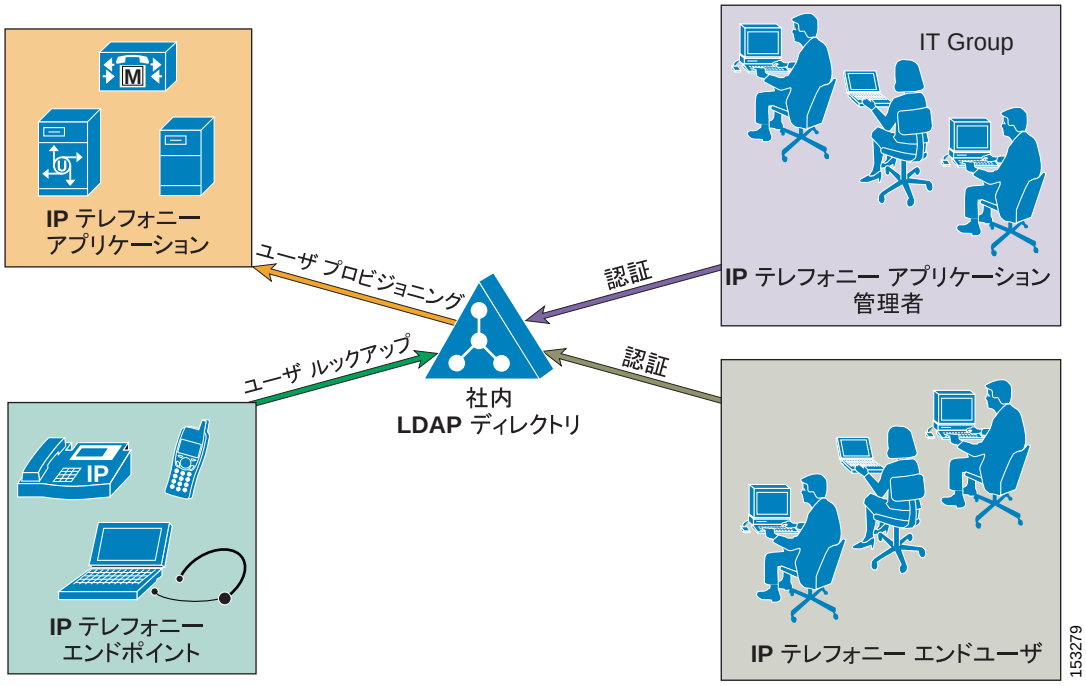
Cisco Unity については、次の Web サイトで入手可能な『*Cisco Unity Design Guide*』、および『*Cisco Unity Data and the Directory*』、『*Active Directory Capacity Planning*』、『*Cisco Unity Data Architecture and How Cisco Unity Works*』の各 White Paper を参照してください。

http://www.cisco.com

ディレクトリ統合とは

音声アプリケーションと社内 LDAP ディレクトリ間の統合は、多くの企業の IT 部門にとって一般的な作業です。ただし、統合の正確な範囲は企業によって異なるため、図 16-1 に示すように、1 つ以上の具体的かつ独立した要件として表すことができます。

図 16-1　ディレクトリ統合のさまざまな要件



たとえば、1 つの一般的な要件は、IP Phone またはその他の音声エンドポイントやビデオ エンドポイントからユーザ ルックアップ（「個人別電話帳」サービスと呼ばれることもあります）を有効にし、ユーザがディレクトリで番号を検索した後に、連絡先に直接ダイヤルできるようにすることです。

もう 1 つの要件は、社内ディレクトリから音声アプリケーションやビデオ アプリケーションのユーザ データベースを、ユーザに自動的に提供することです。この方法により、社内ディレクトリの変更のたびにコア ユーザ情報を手動で追加、削除、または修正する必要がなくなります。

多くの場合、社内ディレクトリ クレデンシャルを使用して、音声アプリケーションやビデオ アプリケーションのエンドユーザと管理者を認証することも必要です。この方法を使用すると、IT 部門がシングル ログオン機能を提供でき、さまざまな社内アプリケーション間で各ユーザが維持する必要があるパスワードの数が減ります。

表 16-1 にまとめているように、使用する Cisco Unified CallManager のバージョンに応じて異なるメカニズムを使用して、これらの要件のそれぞれを Cisco Unified Communications システムで満たすことができます。

表 16-1　ディレクトリの要件とシスコのソリューション

要件	シスコのソリューション	Cisco Unified CallManager 4.*x* の機能	Cisco Unified CallManager 5.0 の機能
エンドポイントのユーザ ルックアップ	ディレクトリ アクセス	Cisco Unified IP Phone Services SDK	Cisco Unified IP Phone Services SDK
ユーザ プロビジョニング	ディレクトリ統合	Cisco Customer Directory Configuration Plugin	LDAP 同期
IP テレフォニー エンドユーザの認証	ディレクトリ統合	Cisco Customer Directory Configuration Plugin	LDAP 認証
IP テレフォニー アプリケーション管理者の認証	ディレクトリ統合	Cisco Customer Directory Configuration Plugin + Cisco Multilevel Administration	LDAP 認証

表 16-1 に示すように、Cisco Unified Communications システムに関係する場合、「ディレクトリ アクセス」という用語は、IP テレフォニー エンドポイントのユーザ ルックアップの要件を満たすメカニズムおよびソリューションを意味します。また、「ディレクトリ統合」という用語は、ユーザ プロビジョニングおよび（エンドユーザと管理者の両方の）認証の要件を満たすメカニズムおよびソリューションを意味します。

この章では、これ以降、Cisco Unified CallManager Release 5.0 に基づく Cisco Unified Communications システムで、これらの要件にどのように対処するかについて説明します。これより前の Cisco Unified CallManager リリースでのディレクトリ統合ソリューションの詳細については、次の Web サイトで入手可能な『*Cisco Unified Communications SRND for Cisco Unified CallManager 4.0 and 4.1*』を参照してください。

http://www.cisco.com/go/srnd

（注）「ディレクトリ統合」という用語については、管理ポリシーおよびセキュリティ ポリシーを集中化するために、Microsoft Active Directory ドメインにアプリケーション サーバを追加する機能といった解釈もあります。Cisco Unified CallManager 5.0 は、カスタマイズした組み込みオペレーティング システムで実行するアプライアンスであり、現在のところ、Microsoft Active Directory ドメインに追加できません。Cisco Unified CallManager のサーバ管理は、Cisco Real-Time Monitoring Tool（RTMT）によって行われます。アプリケーションに合せた強力なセキュリティ ポリシーが組み込みオペレーティング システム内にすでに実装されており、カスタマイズしたバージョンの Cisco Security Agent をどのサーバにもインストールできます。CiscoWorks Management Center for Cisco Security Agents により、セキュリティ ポリシーを集中管理することもできます。

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

この項では、Cisco Unified Communications エンドポイント（Cisco Unified IP Phone など）からユーザ ルックアップを実行するように、LDAP 準拠のディレクトリ 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説明します。Cisco Unified CallManager やその他の IP テレフォニー アプリケーションがユーザ プロビジョニングおよび認証のために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。

ディスプレイ画面を持つ Cisco Unified IP Phone では、ユーザが電話機の Directories ボタンを押すと、ユーザ 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。

デフォルトでは、Cisco Unified IP Phone は、Cisco Unified CallManager の組み込みデータベースに対してユーザ ルックアップを実行するように設定されます。ただし、社内 LDAP ディレクトリでルックアップを実行するように、この設定を変更できます。変更した場合、電話機は HTTP 要求を外部 Web サーバに送信します。このサーバはプロキシとして動作し、要求を社内ディレクトリに対する LDAP 照会に変換します。次に、LDAP 応答は適切な XML オブジェクトにカプセル化され、HTTP 経由で電話機に返送されます。

図 16-2 では、Cisco Unified CallManager が社内ディレクトリに統合されていない配置において、このメカニズムを示しています。このシナリオでは、Cisco Unified CallManager はユーザ ルックアップに関連するメッセージ交換にかかわっていないことに注意してください。

図 16-2　Cisco Unified IP Phone Services SDK を使用する Cisco Unified IP Phone のディレクトリ アクセス

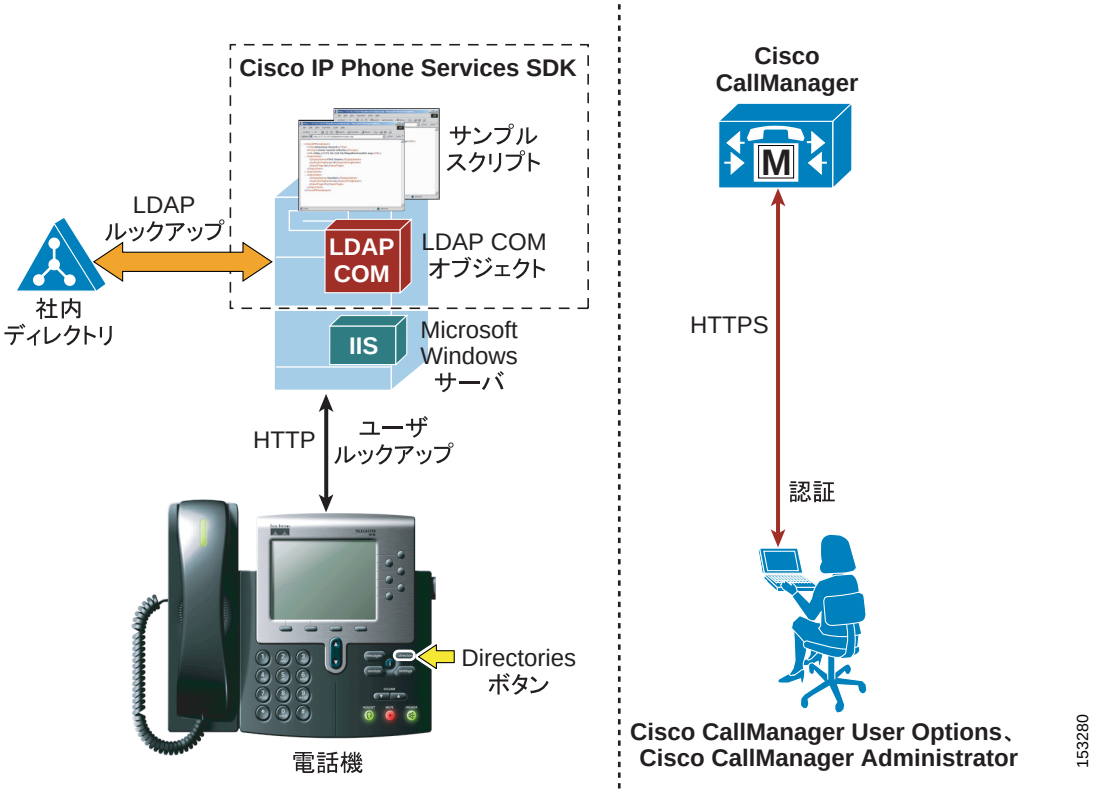


図 16-2 に示す例では、Web サーバのプロキシ機能は、Cisco Unified IP Phone Services Software Development Kit（SDK; ソフトウェア開発キット）バージョン 3.3(4) 以降に組み込まれている Cisco LDAP Search Component Object Model（COM; コンポーネント オブジェクト モデル）サーバによって提供されます。次の Web サイトの Cisco Developer Support Central から最新の Cisco Unified IP Phone Services SDK をダウンロードできます。

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

IP Phone Services SDK は、IIS 4.0 以降を実行する Microsoft Windows Web サーバにはインストールできますが、Cisco Unified CallManager サーバにはインストールできません。SDK には、単純なディレクトリ ルックアップ機能を提供するサンプル スクリプトが入っています。

IP Phone Services SDK を使用する社内ディレクトリ ルックアップ サービスを設定するには、次の手順を実行します。

ステップ 1　社内 LDAP ディレクトリを指すようにサンプル スクリプトのどれかを修正するか、SDK に付属の『*LDAP Search COM Programming Guide*』を使用して独自のスクリプトを作成します。

ステップ 2　Cisco Unified CallManager で、外部 Web サーバ上のスクリプトの URL を指すように URL Directories パラメータ（**System** > **Enterprise Parameters**）を設定します。

ステップ 3　変更を有効にするために電話機をリセットします。

（注）　ユーザのサブセットだけにサービスを提供する場合は、Enterprise Parameters ページではなく、Phone Configuration ページ内で URL Directories パラメータを直接設定します。

まとめると、Cisco Unified IP Phone Services SDK によるディレクトリ アクセスには、次の設計上の考慮事項が適用されます。

- ユーザ ルックアップは、LDAP 準拠の社内ディレクトリに対してサポートされる。
- Microsoft Active Directory に照会する場合、スクリプトがグローバル カタログ サーバを指すようにし、スクリプト設定でポート 3268 を指定することにより、グローバル カタログに対してルックアップを実行できる。この方法では、通常はルックアップが高速化します。
- この機能に関して Cisco Unified CallManager に影響はなく、LDAP ディレクトリ サーバに最小限の影響しか及ばない。
- SDK に付属のサンプル スクリプトでは、最小限のカスタマイズのみが可能である（たとえば、返送されたすべての番号の前に番号ストリングを付けられる）。もっと高度な操作のためには、カスタム スクリプトを開発する必要があり、スクリプトの作成に役立つプログラミング ガイドが SDK に付属しています。
- この機能は、社内ディレクトリに対する Cisco Unified CallManager ユーザのプロビジョニングまたは認証を必要としない。

Cisco Unified CallManager 5.0 でのディレクトリ統合

この項では、社内 LDAP ディレクトリに対するユーザ プロビジョニングと認証を考慮した、Cisco Unified CallManager 5.0 でのディレクトリ統合のメカニズムおよびベスト プラクティスについて説明します。この項では、次のトピックを扱います。

- Cisco Unified CallManager 4.x の方法との比較（P.16-6）

  ディレクトリ統合の方法は、Cisco Unified CallManager Release 4.*x* から 5.0 で大幅に変更されており、この項では、古い方法と比較しながら新しい方法を紹介します。
- Cisco Unified CallManager 5.0 のディレクトリ アーキテクチャ（P.16-8）

  ここでは、Cisco Unified CallManager 5.0 のユーザ関連アーキテクチャの概要を示します。
- LDAP 同期（P.16-11）

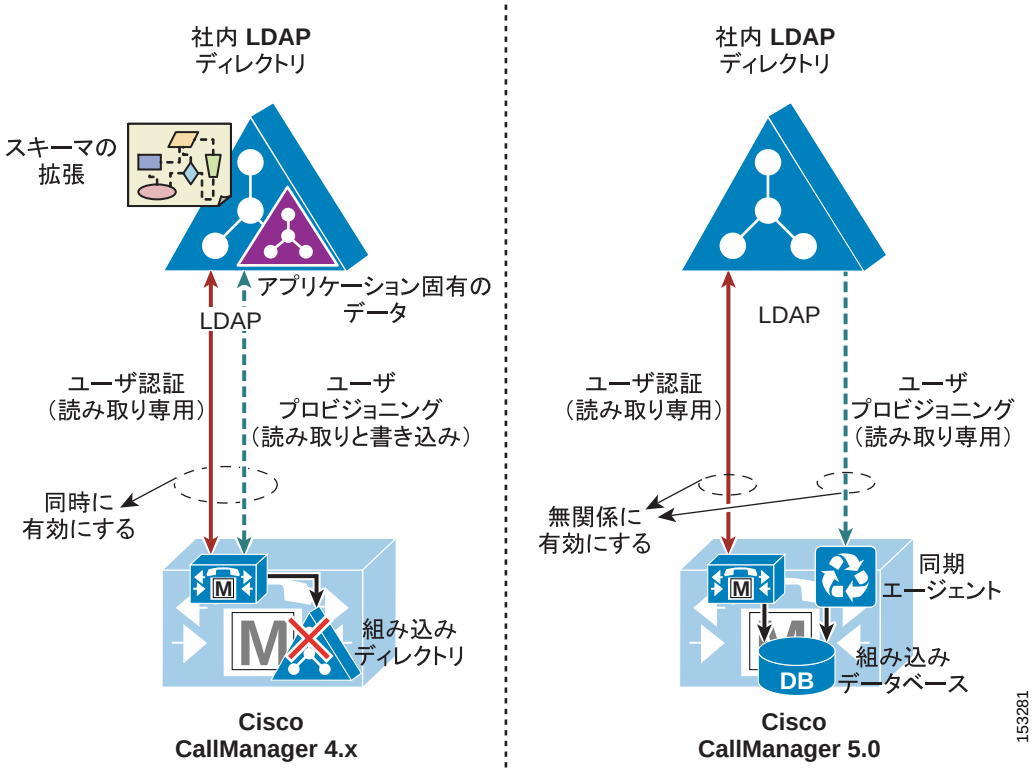
  ここでは、LDAP 同期の機能について説明し、この機能の配置に関する設計上のガイドラインを Microsoft Active Directory に関する追加の考慮事項と共に示します。
- LDAP 認証（P.16-19）

  ここでは、LDAP 認証の機能について説明し、この機能の配置に関する設計上のガイドラインを Microsoft Active Directory に関する追加の考慮事項と共に示します。

Cisco Unified CallManager 4.x の方法との比較

図 16-3 は、*Cisco Unified CallManager 4.x* および 5.0 において、ユーザ プロビジョニングおよび認証のためのディレクトリ統合方法の高レベル機能図を示しています。

図 16-3　Cisco Unified CallManager 4.x および 5.0 におけるディレクトリ統合方法



Cisco Unified CallManager Release 4.*x* では、ユーザ関連情報の保存に組み込み LDAP ディレクトリを使用していました。社内ディレクトリ スキーマを拡張し、組み込みディレクトリをシャットダウンし、ユーザに関連するアプリケーション固有のデータの保存に社内ディレクトリを使用することで、ティレクトリ統合を有効にしていました。社内ディレクトリが実質的にユーザ情報のバックエンド保存リポジトリとして使用されていたため、この方法は、ユーザ プロビジョニングとユーザ認証の両方の要件を満たしています。社内ディレクトリのユーザ データに変更が加えられた場合、Cisco Unified CallManager は同じデータ ストアにアクセスするので、すぐにその変更が認識されていました。

ただし、この方法では、スキーマの拡張と追加データに関して社内ディレクトリに影響があり、Unified Communications システムのリアルタイム機能とディレクトリの可用性の間にも依存関係が発生します。接続が失われるかディレクトリが使用不可になると、Cisco Unified CallManager はすべてのユーザ関連設定にアクセスできなくなり、エクステンション モビリティ、Attendant Console、IP Contact Center Express などのアプリケーションに影響があります。この方法では、ユーザ プロビジョニング機能とユーザ認証機能が同じ統合プロセスに基づいているため、同時に有効にする必要がありました。さらに、社内ディレクトリをアプリケーション固有のデータの保存リポジトリとして使用することで、社内ディレクトリ自体の日常の保守操作が制限を受けることにもなっていました。

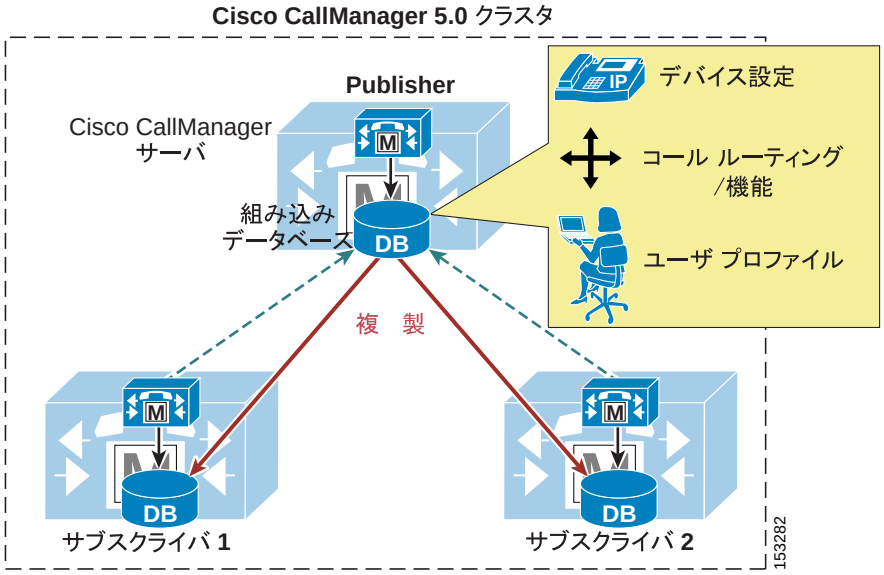
これとは逆に、Cisco Unified CallManager Release 5.0 で採用されたディレクトリ統合方法は、2 つの独立したコンポーネントに基づいてユーザ プロビジョニングとユーザ認証の要件を別々に満たします。ユーザ プロビジョニングは、社内ディレクトリから Cisco Unified CallManager の組み込みデータベースへのユーザ データの一方向同期により実行します。同期では標準 LDAPv3 を使用します。変更を Cisco Unified Communications システムに確実に反映するために、同期を手動で起動することも、定期的に実行するようにスケジューリングすることもできます。このソリューションでは、社内ディレクトリへの書き込みの必要がなくなり、スキーマの拡張も必要ありません。

ユーザ認証は、ユーザ プロビジョニングとは無関係に有効になり、社内ディレクトリ クレデンシャルに対してエンドユーザ パスワードの認証を実現します。この方法では、社内ディレクトリが使用不能または到達不能の場合でも、Cisco Unified Communications システムはすべてのリアルタイム機能を維持します。

Cisco Unified CallManager 5.0 のディレクトリ アーキテクチャ

図 16-4 は、Cisco Unified CallManager 5.0 クラスタの基本アーキテクチャを示しています。組み込みデータベースには、デバイス関連データ、コール ルーティング、その他の機能やユーザ プロファイルなど、すべての設定情報が保存されます。データベースは Cisco Unified CallManager クラスタ内のすべてのサーバ上に存在し、パブリッシャ サーバからすべてのサブスクライバ サーバに自動的に複製されます。

図 16-4　Cisco Unified CallManager 5.0 のアーキテクチャ



デフォルトでは、Cisco Unified CallManager Administration インターフェイスを介してすべてのユーザを手動でデータベースにプロビジョニングします。Cisco Unified CallManager 5.0 では、データベースのユーザを次の 2 つのカテゴリに分類することで、重要な新しい概念を導入しています。

- エンド ユーザ：現実の人および対話形式のログインに関連付けられているすべてのユーザ。このカテゴリには、すべての IP テレフォニー ユーザのほか、User Groups and Roles 設定（以前のバージョンの Cisco Unified CallManager にある Cisco Multilevel Administration 機能に相当）を使用する場合の Cisco Unified CallManager 管理者も含まれます。
- アプリケーション ユーザ：Cisco Unified Communications の他の機能またはアプリケーション（Cisco Attendant Console、Cisco IP Contact Center Express、Cisco Unified CallManager Assistant など）に関連付けられているすべてのユーザ。これらのアプリケーションは Cisco Unified CallManager に対して認証する必要がありますが、この内部「ユーザ」は対話形式のログインを行わず、単にアプリケーション間の内部通信のみを処理します。

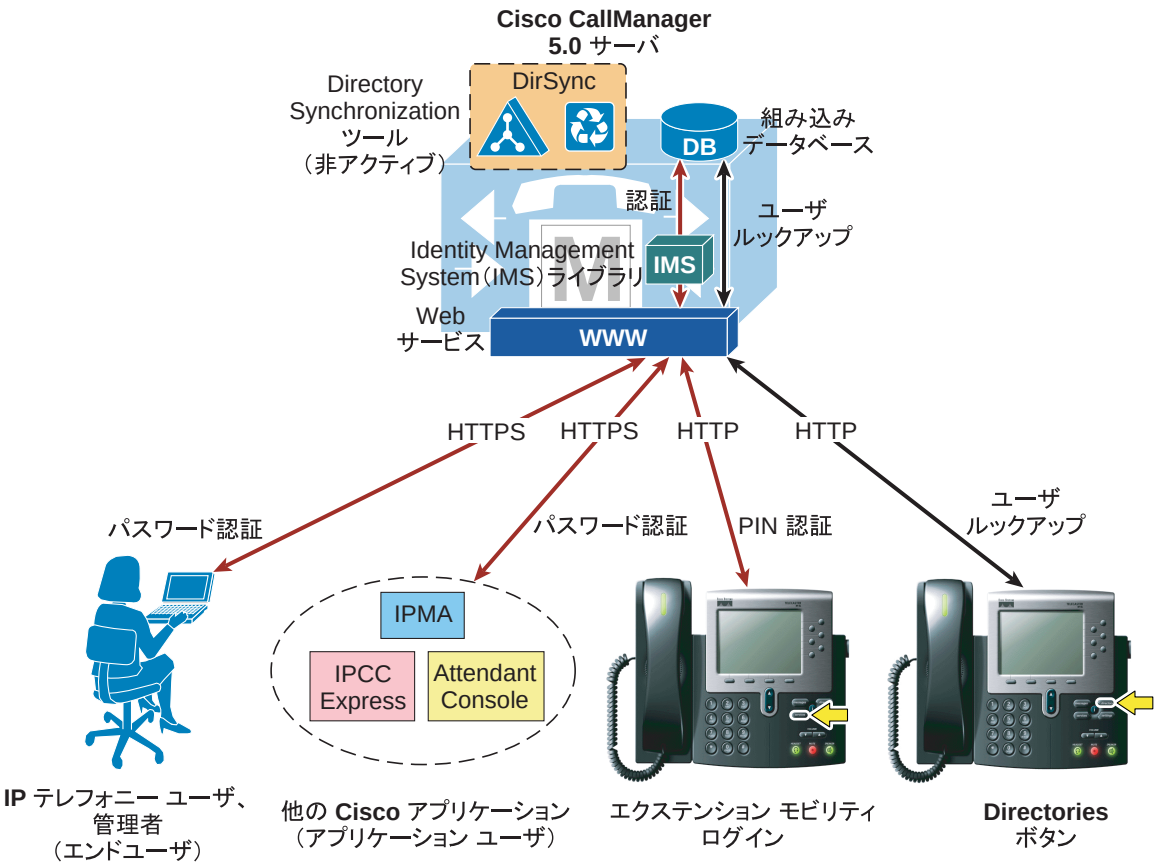
表 16-2 では、Cisco Unified CallManager データベースにデフォルトで作成されるアプリケーション ユーザのリストを、それらのユーザが使用される機能またはアプリケーションと共に示しています。Cisco Unified Communications の他のアプリケーションを統合する場合に、追加のアプリケーション ユーザを手動で作成できます（たとえば、Cisco Attendant Console の **ac** アプリケーション ユーザ、Cisco IP Contact Center Express の **jtapi** アプリケーション ユーザなど）。

表 16-2　Cisco Unified CallManager 5.0 のデフォルトのアプリケーション ユーザ

アプリケーション ユーザ	使用される機能またはアプリケーション
CCMAdministrator	Cisco Unified CallManager Administration（デフォルトは「スーパー ユーザ」）
CCMQRTSecureSysUser	Cisco Quality Reporting Tool
CCMQRTSysUser	
CCMSysUser	Cisco エクステンション モビリティ
IPMASecureSysUser	Cisco Unified CallManager Assistant
IPMASysUser	
WDSecureSysUser	Cisco WebDialer
WDSysUser	

これらの考慮事項に基づいて、図 16-5 は、ルックアップ、プロビジョニング、認証などのユーザ関連操作に対する Cisco Unified CallManager 5.0 でのデフォルト動作を示しています。

図 16-5　Cisco Unified CallManager 5.0 のユーザ関連操作に対するデフォルト動作



エンド ユーザは、HTTPS 経由で Cisco Unified CallManager User Options ページにアクセスし、ユーザ名およびパスワードで認証します。User Groups and Roles によって管理者として設定されている場合、エンド ユーザは同じクレデンシャルで Cisco Unified CallManager Administration ページにもアクセスします。

同様に、シスコの他の機能とアプリケーションは、それぞれのアプリケーション ユーザに関連付けられたユーザ名およびパスワードで、HTTPS 経由で Cisco Unified CallManager に対して認証します。

HTTPS メッセージによって伝送される認証確認は、Cisco Unified CallManager の Web サービスにより、Identity Management System（IMS）という内部ライブラリにリレーされます。デフォルト設定では、IMS ライブラリは、組み込みデータベースに対してエンド ユーザとアプリケーション ユーザの両方を認証します。このように、IP Communications システムにおける「現実の」ユーザと内部アプリケーション アカウントの両方が、Cisco Unified CallManager に設定されたクレデンシャルを使用して認証されます。

エンド ユーザは、IP Phone からエクステンション モビリティ サービスにログインするときに、ユーザ名と数値パスワード（PIN）で認証することもできます。この場合、認証確認は HTTP 経由で Cisco Unified CallManager に伝送されますが、やはり Web サービスにより IMS ライブラリにリレーされ、IMS ライブラリは組み込みデータベースに対してクレデンシャルを認証します。

さらに、Directories ボタンを介して IP テレフォニー エンドポイントによって実行されるユーザ ルックアップでは、HTTP 経由で Cisco Unified CallManager の Web サービスと通信し、組み込みデータベースのデータにアクセスします。

エンド ユーザとアプリケーション ユーザの区別の重要性は、社内ディレクトリとの統合が必要な場合に明らかになります。前の項で説明したように、この統合は次の 2 つの独立したプロセスによって実現されます。

- LDAP 同期

  このプロセスでは、Cisco Unified CallManager の Cisco Directory Synchronization（DirSync）という内部ツールを使用して、社内 LDAP ディレクトリから多数のユーザ属性を（手動または定期的に）同期します。この機能を有効にすると、ユーザは社内ディレクトリから自動的にプロビジョニングされます。この機能はエンド ユーザだけに適用され、アプリケーション ユーザは独立したままで、引き続き Cisco Unified CallManager Administration インターフェイスを介してプロビジョニングされます。要約すると、エンド ユーザは社内ディレクトリで定義され、Cisco Unified CallManager データベースに同期されますが、アプリケーション ユーザは Cisco Unified CallManager データベースに保存されるだけで、社内ディレクトリで定義する必要はありません。

- LDAP 認証

  このプロセスでは、IMS ライブラリにより、社内 LDAP ディレクトリに対してユーザ クレデンシャルを認証できます。この機能を有効にすると、エンド ユーザ パスワードは社内ディレクトリに対して認証されますが、アプリケーション ユーザ パスワードは引き続きローカルで Cisco Unified CallManager データベースに対して認証されます。Cisco エクステンション モビリティの PIN も引き続きローカルで認証されます。

Cisco Unified CallManager データベースに対して内部でアプリケーション ユーザを維持および認証すると、社内 LDAP ディレクトリの可用性とは無関係に、これらのアカウントを使用して Cisco Unified CallManager と通信するすべてのアプリケーションと機能に対して復元性が提供されます。

Cisco エクステンション モビリティの PIN も Cisco Unified CallManager データベース内で維持されます。これらの PIN はリアルタイム アプリケーションの必須部分であり、リアルタイム アプリケーションは社内ディレクトリの応答性に依存しないようにする必要があるためです。

次の 2 つの項では、LDAP 同期と LDAP 認証についてさらに詳しく説明し、両方の機能に関して設計上のベスト プラクティスを示します。

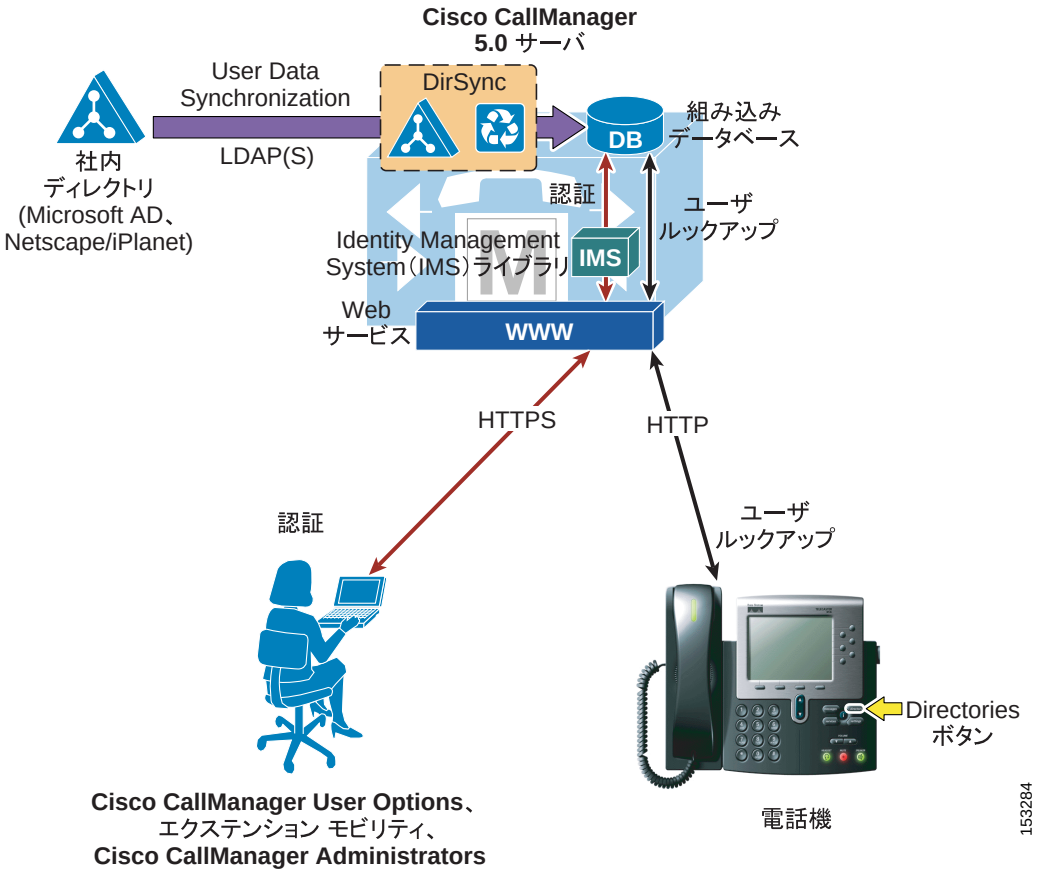
（注）　P.16-4 の「IP テレフォニー エンドポイントのディレクトリ アクセス」の項で説明したように、外部 Web サーバで Cisco Unified IP Phone Services SDK を設定することにより、エンドポイントからのユーザ ルックアップを社内ディレクトリに対して実行することもできます。

LDAP 同期

Cisco Unified CallManager を社内 LDAP ディレクトリに同期すると、LDAP ディレクトリに保存されたユーザ データを再利用でき、社内 LDAP ディレクトリをその情報の中央リポジトリとして使用できます。Cisco Unified CallManager は、ユーザ データを保存するための統合データベースを備え、またユーザ データをそのデータベースで作成して維持するための Web インターフェイスを、Cisco Unified CallManager Administration 内に備えています。同期を有効にすると、ローカル データベースは引き続き使用されますが、ユーザ アカウントを作成する Cisco Unified CallManager ファシリティが無効になります。その後、ユーザ アカウントの管理は、LDAP ディレクトリのインターフェイスを介して実施されます（図 16-6 を参照）。

ユーザ アカウント情報は、LDAP ディレクトリから Cisco Unified CallManager パブリッシャ サーバにあるデータベースにインポートされます。LDAP ディレクトリからインポートされた情報は、Cisco Unified CallManager から変更できません。Cisco Unified CallManager 実装に固有の追加のユーザ情報は、Cisco Unified CallManager によって管理され、そのローカル データベース内だけに保存されます。たとえば、デバイスとユーザのアソシエーション、短縮ダイヤル、ユーザ PIN は Cisco Unified CallManager が管理するデータであり、社内 LDAP ディレクトリには存在しません。次に、ユーザ データは組み込みデータベース同期によって、Cisco Unified CallManager パブリッシャ サーバからサブスクライバに伝達されます。

図 16-6　ユーザ データ同期の有効化



同期のために、次のディレクトリが Cisco Unified CallManager でサポートされています。

- Microsoft Active Directory（AD）2000 および 2003

- Netscape Directory Server 4.x、iPlanet Directory Server 5.1、Sun ONE Directory Server 5.2

LDAP 同期をアクティブにすると、上記の LDAP 製品グループのうち、一度にいずれか 1 つのみをクラスタ用に選択できます。また、ディレクトリ ユーザの 1 つの属性が Cisco Unified CallManager User ID フィールドにマッピングするために選択されます。Cisco Unified CallManager はデータへのアクセスに標準 LDAPv3 を使用します。

Cisco Unified CallManager がインポートするデータはすべて、標準属性のデータです。表 16-3 は使用される属性のリストを示しており、これらの属性は 2 つの LDAP 実装グループ間で異なります。Cisco Unified CallManager User ID にマッピングされるディレクトリ属性のデータは、そのクラスタのすべてのエントリ内で固有のものになっている必要があります。**sn** 属性にはデータを格納する必要があります。そうしないと、そのレコードは社内ディレクトリからインポートされません。エンドユーザ アカウントのインポート中に使用するプライマリ属性が Cisco Unified CallManager データベースのいずれかのアプリケーション ユーザと一致する場合、そのユーザはスキップされます。

一部の Cisco Unified CallManager データベース フィールドではディレクトリ属性を選択できますが、同期アグリーメントごとに単一のマッピングだけを選択できます。

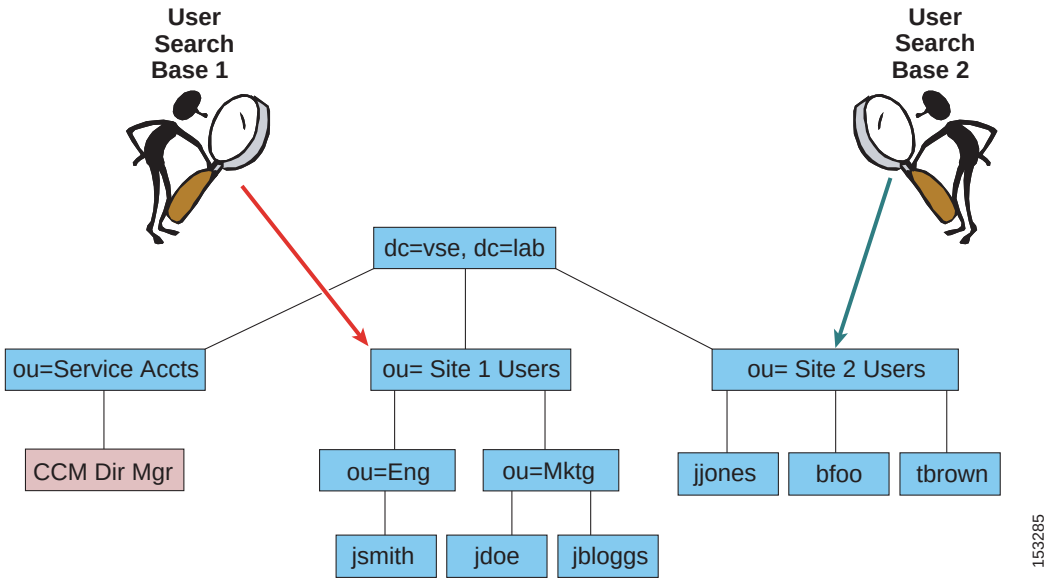
表 16-3　Cisco Unified CallManager でインポートされるデータ属性

Cisco Unified CallManager のユーザ フィールド	Microsoft Active Directory（AD）の属性	Netscape、iPlanet、または Sun ONE の属性
User ID	*次のいずれか* sAMAccountName mail employeeNumber telephoneNumber UserPrincipalName	*次のいずれか* uid mail employeeNumber telephonePhone
First Name	givenName	givenname
Middle Name	*次のいずれか* middleName initials	initials
Last Name	sn	sn
Manager ID	manager	manager
Department	department	departmentnumber
Phone Number	*次のいずれか* telephoneNumber ipPhone	telephonenumber
Mail ID	*次のいずれか* mail sAMAccountName	*次のいずれか* mail uid

同期は、Serviceability Web ページで有効にする Cisco DirSync というプロセスによって実行されます。このプロセスを有効にすると、1 つ以上の同期アグリーメントをシステムで設定できます。アグリーメントでは、LDAP ツリー内で Cisco Unified CallManager がユーザ アカウントの検索を開始する場所となる検索ベースを指定します。Cisco Unified CallManager は、特定の同期アグリーメントについて検索ベースで指定したドメインの領域に存在するユーザのみをインポートできます。

図 16-7 は、2 つの同期アグリーメントを示しています。一方の同期アグリーメントでは、User Search Base 1 を指定し、ユーザ jsmith、jdoe、jbloggs をインポートします。もう一方の同期アグリーメントでは、User Search Base 2 を指定し、ユーザ jjones、bfoo、tbrown をインポートします。CCMDirMgr アカウントは、ユーザ検索ベースで指定した場所の下位に存在しないので、インポートされません。ユーザを LDAP ディレクトリの構造に編成すると、その構造を使用して、どのユーザ グループをインポートするかを制御できます。この例では、単一の同期アグリーメントを使用してドメインのルートを指定することもできましたが、その検索ベースでは Service Accts もインポートしていたと考えられます。検索ベースではドメイン ルートを指定する必要はなく、ツリーのどの場所でも指定できます。

図 16-7　ユーザ検索ベース



データを Cisco Unified CallManager データベースにインポートするために、LDAP Manager Distinguished Name として設定で指定されたアカウントを使用して、システムが LDAP ディレクトリへのバインドを実行し、データベースの読み取りがこのアカウントで実行されます。Cisco Unified CallManager のログインのために、LDAP ディレクトリでアカウントが使用可能である必要があります。ユーザ検索ベースで指定したサブツリー内のすべてのユーザ オブジェクトの読み取り可能な権限を持つ、固有のアカウントを作成することをお勧めします。同期アグリーメントでは、そのアカウントがドメイン内のどこにでも存在できるように、アカウントの完全認定者名を指定します。図 16-7 の例では、CCMDirMgr が同期に使用するアカウントです。

アカウントのインポートは、LDAP Manager Distinguished Name アカウントの権限を使用して制御できます。この例では、ou=Eng への読み取りアクセスはできるが ou=Mktg への読み取りアクセスはできないようにこのアカウントを制限した場合、Eng の下位にあるアカウントのみがインポートされます。

同期アグリーメントには、複数のディレクトリ サーバを指定して冗長性を実現する機能があります。同期の試行時に使用するディレクトリ サーバを 3 つまで、順序付きのリストにして設定に指定できます。これらのサーバでの試行が、リストの最後まで順に行われます。どのディレクトリ サーバも応答しない場合、同期には失敗しますが、設定済みの同期スケジュールに従って再試行されます。

同期のメカニズム

同期アグリーメントでは、同期を開始する時刻を指定し、再同期の期間を時間、日、週、月のいずれかの単位（最小値は 6 時間）で指定します。同期アグリーメントは、特定の時刻に 1 回だけ実行するように設定することもできます。

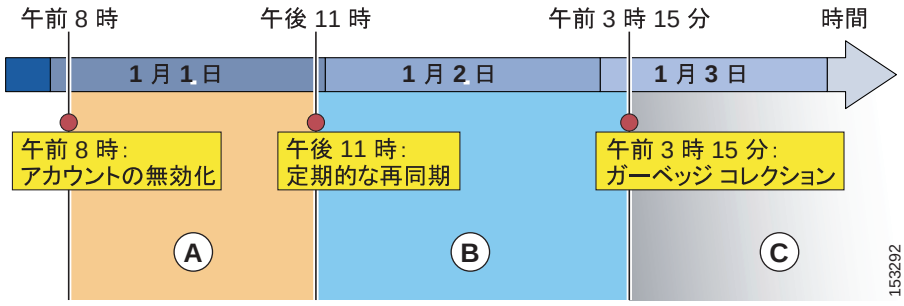
Cisco Unified CallManager パブリッシャ サーバで同期を初めて有効にすると、社内ディレクトリに存在するユーザ アカウントが Cisco Unified CallManager データベースにインポートされます。そして、その後のプロセスに従って、既存の Cisco Unified CallManager エンドユーザ アカウントがアクティブになってデータが更新されるか、新しいエンドユーザ アカウントが作成されます。

1. エンドユーザ アカウントがすでに Cisco Unified CallManager データベースに存在するときに同期アグリーメントを設定した場合、Cisco Unified CallManager ですべての既存のアカウントは非アクティブとマークされます。同期アグリーメントの設定で、Cisco Unified CallManager UserID への LDAP データベース属性のマッピングを指定します。同期中に LDAP データベースのアカウントが既存の Cisco Unified CallManager アカウントと一致すると、その Cisco Unified CallManager アカウントは再びアクティブとマークされます。
2. 同期の完了後、アクティブに設定されなかったアカウントは、ガーベッジ コレクション プロセスの実行時に Cisco Unified CallManager から永続的に削除されます。ガーベッジ コレクションは、午前 3 時 15 分の定時に自動的に実行されるプロセスで、設定はできません。Cisco Unified CallManager は同期が設定されている間はアカウントを管理できないので、LDAP ディレクトリ アカウントと一致しない Cisco Unified CallManager アカウントの削除が必要です。
3. 後で社内ディレクトリに変更を加えると、スケジューリングされた次回の同期期間に、完全な再同期として Microsoft Active Directory から同期が行われます。これに対して、Netscape、iPlanet、Sun ONE の各製品は、ディレクトリに変更が加えられると差分同期を実行します。次の項では、2 つのシナリオのそれぞれの例を示します。

Active Directory でのアカウント同期

図 16-8 は、LDAP 同期と LDAP 認証の両方を有効にした Cisco Unified CallManager 配置について、イベントのスケジュールの例を示しています。再同期は、毎日午後 11 時に設定されています。

図 16-8　Active Directory での変更の伝達



最初の同期の後、アカウントの作成、削除、または無効化は、図 16-8 に示すスケジュールに従って、次の手順で説明するように Cisco Unified CallManager に伝達されます。

1. 1 月 1 日の午前 8 時に、AD でアカウントを無効にするか削除します。これ以降、期間 A 中は、Cisco Unified CallManager が認証を AD にリダイレクトするため、このユーザのパスワード認証（たとえば、Cisco Unified CallManager User Options ページ）は失敗します。ただし、PIN は Cisco Unified CallManager データベースに保存されているため、PIN 認証（たとえば、エクステンション モビリティ ログイン）は今までどおり成功します。

2. 定期的な再同期は、1 月　1 日の午後　11 時にスケジューリングされています。このプロセス中、Cisco Unified CallManager はすべてのアカウントを検証します。AD で無効にするか削除したアカウントは、この時点で、Cisco Unified CallManager データベースでは非アクティブとしてタグ付けされます。1 月　1 日の午後　11 時より後に、アカウントが非アクティブとマークされると、Cisco Unified CallManager による PIN 認証とパスワード認証は両方とも失敗します。
3. アカウントのガーベッジ コレクションは、毎日午前　3 時 15 分の定時に実行されます。このプロセスでは、24 時間以上にわたって非アクティブとマークされていたレコードについて、ユーザ情報を Cisco Unified CallManager データベースから永続的に削除します。この例では、1 月　2 日の午前　3 時 15 分に実行するガーベッジ コレクションでは、アカウントが非アクティブになってまだ 24 時間が経過していないので、アカウントを削除しません。したがって、アカウントは 1 月　3 日の午前　3 時 15 分に削除されます。この時点で、ユーザ データは Cisco Unified CallManager から永続的に削除されます。

期間 A の開始時にアカウントを AD で作成していた場合、そのアカウントは期間　B の開始時に実行される定期的な再同期で Cisco Unified CallManager にインポートされ、Cisco Unified CallManager ですぐにアクティブになります。

（注）　上記の動作は　Cisco Unified CallManager Release 5.0(3)　以降に適用されます。Release 5.0(1)　および 5.0(2) では、非アクティブとマークされたユーザの PIN 認証は失敗しないので、図 16-8 で削除されたユーザでも、期間　B 中にエクステンション モビリティ サービスにログインできます。これらのリリースでは、ディレクトリ認証を有効にしない場合、ユーザが非アクティブとマークされているとき（つまり、期間　B 中）にパスワード認証も成功します。

Netscape、iPlanet、または Sun ONE でのアカウント同期

Netscape、iPlanet、Sun ONE の各製品は差分同期アグリーメントをサポートし、Active Directory とは異なる同期スケジュールを使用します。図 16-9 では、LDAP 同期と LDAP 認証の両方を有効にした Cisco Unified CallManager 配置について、この同期スケジュールの例を示しています。

図 16-9　Netscape、iPlanet、Sun ONE での変更の伝達

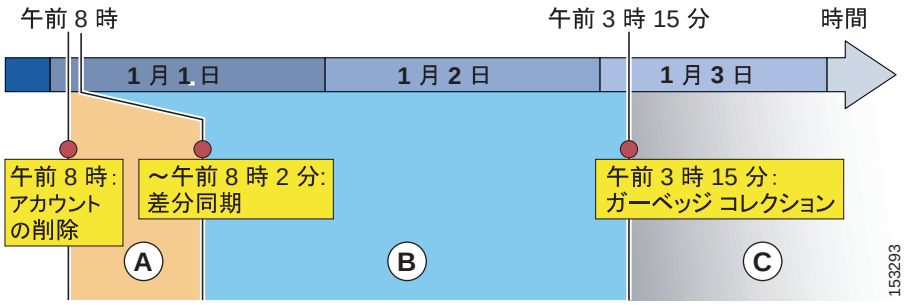


図 16-9 の例は、次の手順から構成されます。

1. 1 月　1 日の午前　8 時にアカウントが社内ディレクトリから削除され、これにより、差分更新データが LDAP サーバから Cisco Unified CallManager に送信されます。Cisco Unified CallManager は、データに対応するコピーを非アクティブに設定します。LDAP 認証が設定されているので、LDAP サーバがレコードを削除するとすぐに、ユーザはパスワードによるログインができなくなります。また、Cisco Unified CallManager レコードが非アクティブとマークされると、PIN をログインに使用できません。
2. 期間 B 中は、ユーザのレコードは非アクティブですが、まだ Cisco Unified CallManager に存在します。

3. 1 月 2 日の午前 3 時 15 分にガーベッジ コレクションが実行されるときは、レコードが非アクティブになってまだ 24 時間が経過していません。データは 1 月 3 日の期間 C の開始時まで Cisco Unified CallManager データベースに残り、ガーベッジ コレクション プロセスがこの日の午前 3 時 15 分に再び実行され、レコードが 24 時間以上にわたって非アクティブであったことを確認します。その結果、レコードはデータベースから永続的に削除されます。

ディレクトリで新規に作成したアカウントは、差分更新データによって同様に Cisco Unified CallManager に同期し、差分更新データが受信されるとすぐに使用できます。

（注）　上記の動作は Cisco Unified CallManager Release 5.0(3) 以降に適用されます。Release 5.0(1) および 5.0(2) では、Sun ONE Directory Server から削除されたユーザ アカウントは、非アクティブの段階を経ることなく、差分同期が実行されるとすぐに Cisco Unified CallManager データベースから削除されます。

セキュリティの考慮事項

アカウントのインポート中は、LDAP ディレクトリから Cisco Unified CallManager データベースに、パスワードも PIN もコピーされません。Cisco Unified CallManager で LDAP 認証を有効にしない場合、エンド ユーザのパスワードと PIN は、Cisco Unified CallManager Administration を使用して管理します。デフォルトでは、アカウントの作成時にパスワードは **ciscocisco** に設定され、PIN は **12345** に設定されます。これらの設定は、ユーザがユーザ Web ページを使用するか、管理者が管理者 Web ページを使用して変更できます。パスワードと PIN は、暗号化形式で Cisco Unified CallManager データベースに保存されます。ディレクトリ パスワードを使用してエンド ユーザを認証する場合は、P.16-19 の「LDAP 認証」の項を参照してください。

Cisco Unified CallManager および LDAP サーバで Secure LDAP（SLDAP）を有効にすることにより、Cisco Unified CallManager パブリッシャ サーバとディレクトリ サーバ間の接続を保護できます。Secure LDAP を使用すると、Secure Socket Layer（SSL）接続で LDAP 送信ができます。Cisco Unified CallManager Platform Administration 内で SSL 証明書をアップロードすることにより、Secure LDAP を有効にできます。詳細な手順については、http://www.cisco.com で入手可能な Cisco Unified CallManager の製品マニュアルを参照してください。

LDAP 同期のベスト プラクティス

Cisco Unified CallManager 5.0 で LDAP 同期を配置する場合は、設計と実装に関する次のベスト プラクティスに従ってください。

- 社内ディレクトリ内で特定のアカウントを使用し、Cisco Unified CallManager 同期アグリーメントがそのディレクトリに対して接続および認証できるようにする。目的の検索ベース内にあるすべてのユーザ オブジェクトを「読み取る」ように最小権限を設定し、期限切れにならないようにパスワードを設定した状態で、Cisco Unified CallManager 専用のアカウントを使用することをお勧めします（このアカウントのパスワードをディレクトリで変更した場合、変更を考慮して Cisco Unified CallManager を再設定する必要があります）。
- 所定のクラスタにあるすべての同期アグリーメントは、同じ LDAP サーバ ファミリ（Microsoft AD または Netscape、iPlanet、Sun ONE）と統合する必要がある。
- 複数のアグリーメントが同時に同じ LDAP サーバに照会することがないように、同期アグリーメントの定期性に時間差を設ける。待機期間中の同期時刻を選択します。
- ユーザ データのセキュリティが重要な場合、Cisco Unified CallManager Administration の LDAP Directory 設定ページで **Use SSL** フィールドのチェックボックスをオンにして、Secure LDAP（SLDAP）を有効にする。
- Cisco Unified CallManager UserID フィールドへのマッピングのために選択した LDAP ディレクトリ属性が、そのクラスタのすべての同期アグリーメント内で固有であることを確認する。

- UserID として選択した属性は、Cisco Unified CallManager で定義したアプリケーション ユーザのいずれかの属性と同じであってはならない。
- 同期前の Cisco Unified CallManager データベースにある既存のアカウントは、LDAP ディレクトリからインポートされたアカウントの属性に一致する場合にのみ維持される。Cisco Unified CallManager UserID に一致する属性は、同期アグリーメントによって確認されます。
- 冗長性が得られるように、2 台以上の LDAP サーバを設定する。ホスト名の代わりに IP アドレスを使用すると、Domain Name System（DNS; ドメイン ネーム システム）の可用性に依存しなくなります。
- エンドユーザ アカウントは LDAP ディレクトリの管理ツールによって管理し、これらのアカウントのシスコ固有データは Cisco Unified CallManager Administration Web ページによって管理する。

Microsoft Active Directory に関する追加の考慮事項

ドメインの同期アグリーメントでは、ドメイン外のユーザや子ドメイン内のユーザは同期されません。同期プロセス中は Cisco Unified CallManager が AD 照会に従わないためです。図 16-10 の例では、すべてのユーザをインポートするために 3 つの同期アグリーメントが必要です。Search Base 1 ではツリーのルートを指定しますが、子ドメインのいずれかに存在するユーザはインポートしません。範囲は VSE.LAB に限定されており、残りの 2 つのドメインに対し、そのユーザをインポートするように別々のアグリーメントが設定されています。

図 16-10　複数の Active Directory ドメインでの同期

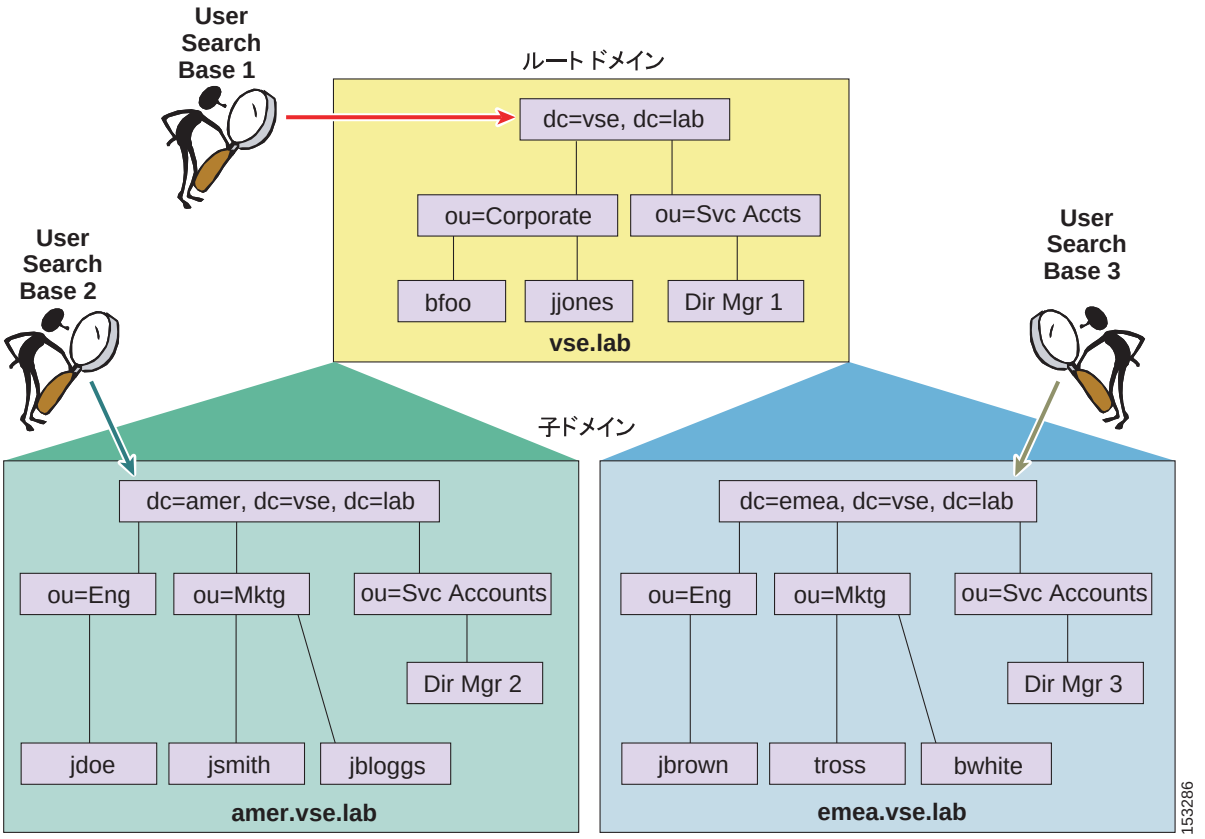
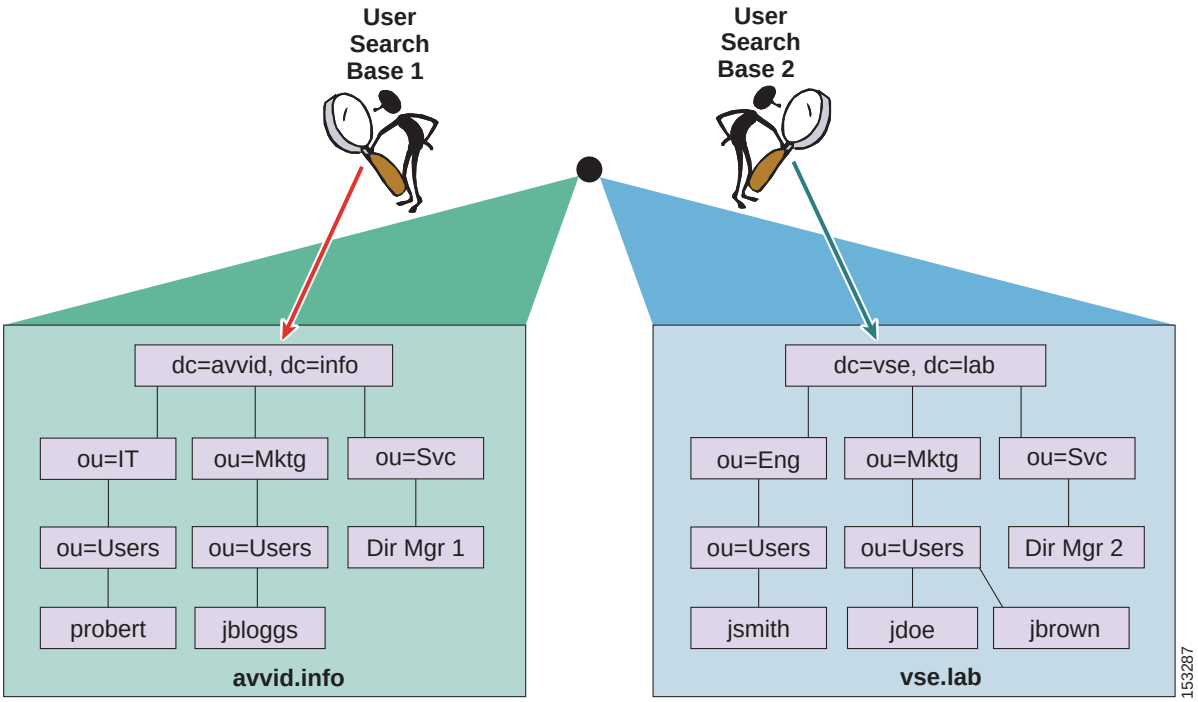


図 16-10 では、ドメインとサブドメインのそれぞれに少なくとも 1 つの Domain Controller（DC; ドメイン コントローラ）が関連付けられ、3 つの同期アグリーメントはそれぞれ適切なドメイン コントローラを指定します。DC にある情報は、その DC が存在するドメイン内のユーザの情報だけなので、すべてのユーザをインポートするために 3 つの同期アグリーメントが必要です。

図 16-11 に示すように、複数のツリーを含む AD フォレストで同期を有効にした場合も、上記と同じ理由で複数の同期アグリーメントが必要です。さらに、UserPrincipalName（UPN）属性がフォレスト全体で固有であることが Active Directory によって保証され、この属性は Cisco Unified CallManager UserID にマッピングする属性として選択する必要があります。マルチツリーの AD シナリオで UPN 属性を使用する場合の追加の考慮事項については、P.16-22 の「Microsoft Active Directory に関する追加の考慮事項」の項を参照してください。

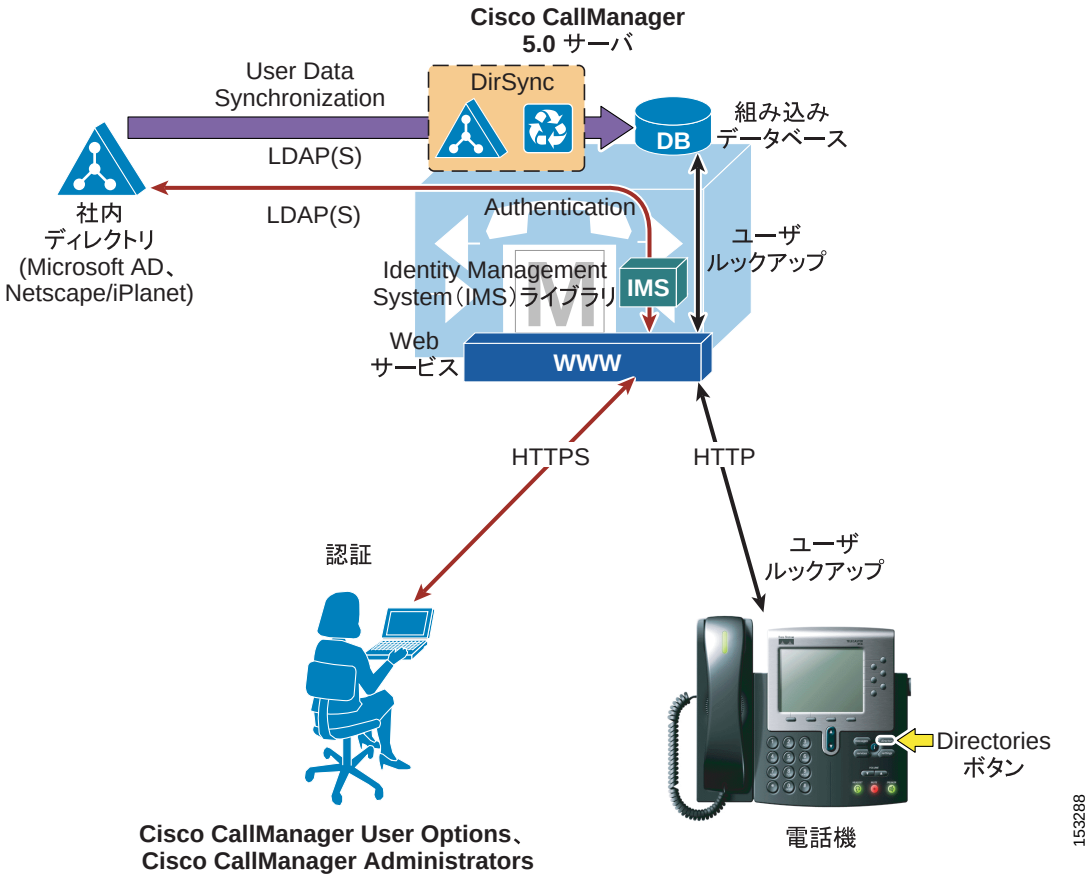
図 16-11　複数の AD ツリー（不連続なネームスペース）での同期



LDAP 認証

LDAP 認証機能を使用すると、組み込みデータベースを使用する代わりに、社内 LDAP ディレクトリに対して Cisco Unified CallManager でエンド ユーザ パスワードを認証できます。図 16-12 に示すように、Cisco Unified CallManager 内の IMS モジュールと社内ディレクトリ サーバ間で確立した LDAPv3 接続によって、この認証が実現されます。

図 16-12　LDAP 認証の有効化



LDAP 同期機能の場合と同様に、次の社内ディレクトリ製品がサポートされます。

- Microsoft Active Directory（AD）2000 および 2003
- Netscape Directory Server 4.x、iPlanet Directory Server 5.1、Sun ONE Directory Server 5.2

認証機能では、冗長性を得るためにサーバを 3 つまで設定でき、必要に応じて Secure LDAP（SLDAP）を有効にした場合、ディレクトリ サーバへの保護接続もサポートされます。認証機能は、LDAP 同期機能とは無関係に有効にできます。ただし、認証を単独で有効にする場合は、Cisco Unified CallManager のユーザ ID が社内ディレクトリで定義されているユーザ ID と一致することを確認する必要があります。

認証を有効にした場合の Cisco Unified CallManager の動作説明を、次に示します。

- エンド ユーザ パスワードは、社内ディレクトリに対して認証される。
- アプリケーション ユーザ パスワードは、Cisco Unified CallManager データベースに対して認証される。
- エンド ユーザ PIN は、Cisco Unified CallManager データベースに対して認証される。

この動作は、リアルタイム IP Communications システムの操作を社内ディレクトリの可用性に依存しないようにしながら、シングル ログオン機能をエンド ユーザに提供するという原則に従ったものです。図 16-13 に図示します。

図 16-13　エンド ユーザ パスワード、アプリケーション ユーザ パスワード、エンド ユーザ PIN の認証

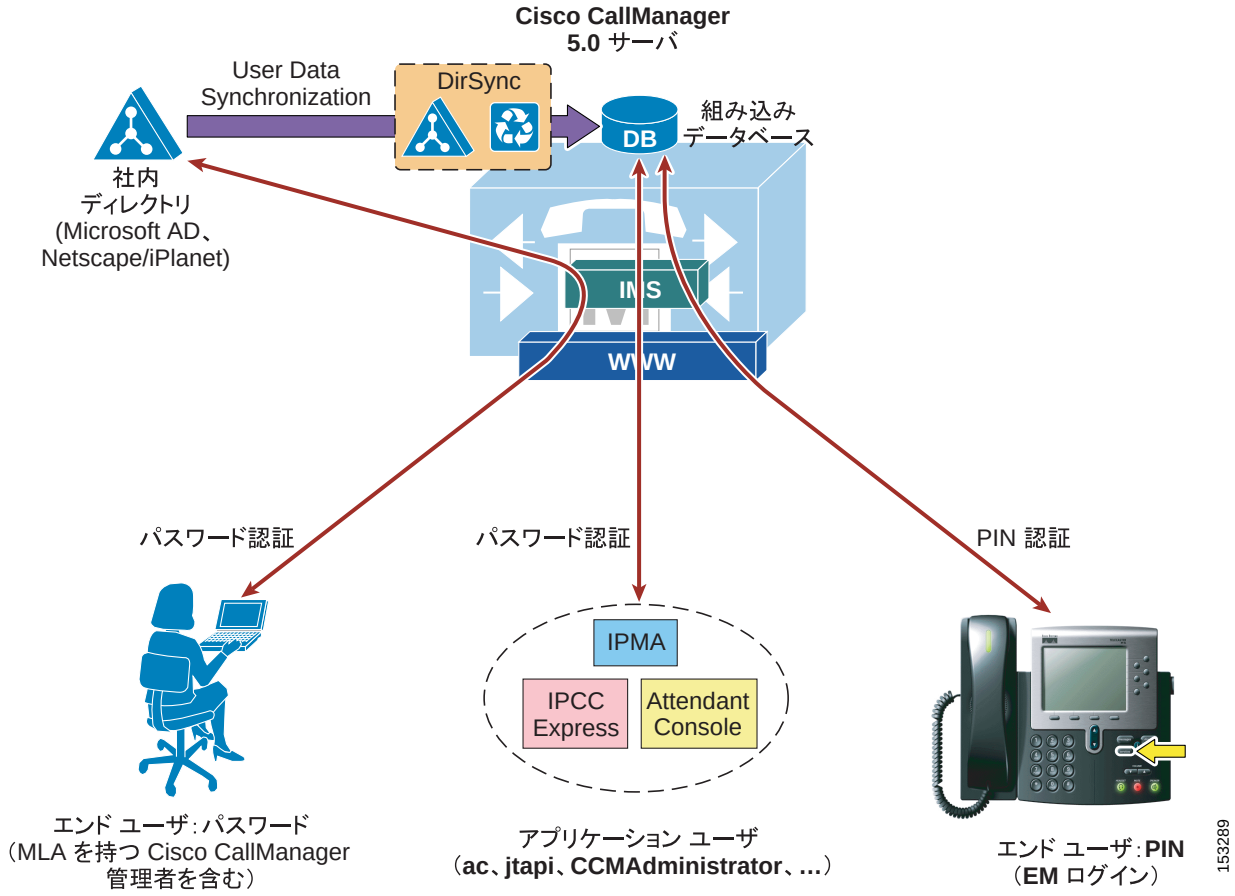
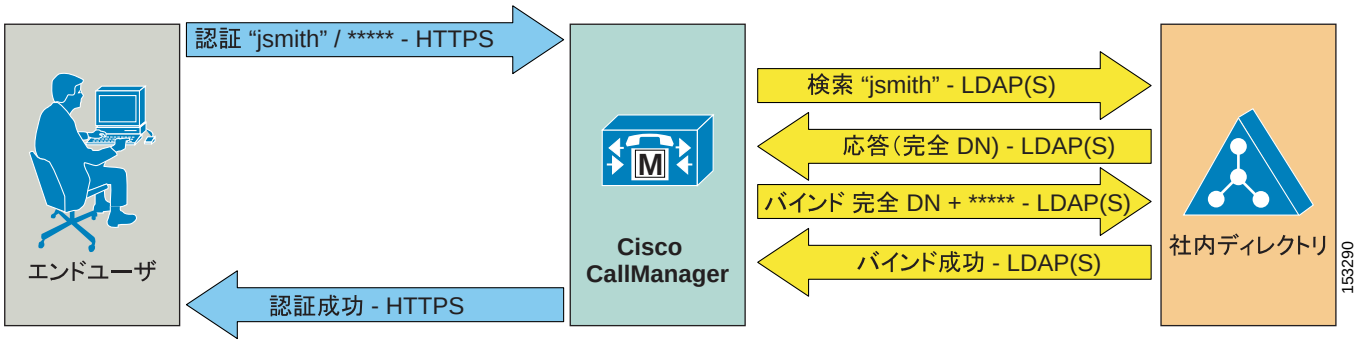


図 16-14 は、エンド ユーザを社内 LDAP ディレクトリに対して認証するために Cisco Unified CallManager で採用された、次のプロセスを示しています。

1. まず、ユーザは、HTTPS 経由で Cisco Unified CallManager User Options ページに接続し、ユーザ名とパスワードで認証を試行します。この例では、ユーザ名は jsmith です。
2. 次に、Cisco Unified CallManager はユーザ名 jsmith に関する LDAP 照会を発行し、LDAP Authentication 設定ページの LDAP Search Base で指定された値を、この照会の範囲として使用します。SLDAP を有効にした場合、この照会は SSL 接続を通じて行われます。
3. 社内ディレクトリ サーバは、LDAP 経由で、ユーザ jsmith の完全 Distinguished Name（DN; 認定者名）で応答します（たとえば、「cn=jsmith, ou=Users, dc=vse, dc=lab」）。
4. 次に、Cisco Unified CallManager は、この完全 DN とユーザが提供するパスワードを使用して、LDAP バインドを試行します。
5. LDAP バインドが成功した場合、Cisco Unified CallManager は、要求された設定ページにユーザが進むことを許可します。

図 16-14　認証プロセス



Cisco Unified CallManager 5.0 で LDAP 認証を配置する場合は、設計と実装に関する次のベスト プラクティスに従ってください。

- 社内ディレクトリ内でアカウントを作成し、Cisco Unified CallManager がそのディレクトリに対して接続および認証できるようにする。目的の検索ベース内にあるすべてのユーザ オブジェクトを「読み取る」ように最小権限を設定し、期限切れにならないようにパスワードを設定した状態で、Cisco Unified CallManager 専用のアカウントを使用することをお勧めします（このアカウントのパスワードをディレクトリで変更した場合、変更を考慮して Cisco Unified CallManager を再設定する必要があります）。LDAP 同期も有効にした場合は、同じアカウントを両方の機能に使用できます。
- LDAP Manager Distinguished Name および LDAP Password で前述のアカウントのクレデンシャルを指定し、LDAP User Search Base ですべてのユーザが存在するディレクトリ サブツリーを指定することにより、Cisco Unified CallManager で LDAP 認証を有効にする。
- 冗長性が得られるように、2 台以上の LDAP サーバを設定する。ホスト名の代わりに IP アドレスを使用すると、Domain Name System（DNS; ドメイン ネーム システム）の可用性に依存しなくなります。
- この方法では、シングル ログオン機能をすべてのエンド ユーザに提供する。エンド ユーザは、Cisco Unified CallManager User Options ページにログインすると、社内ディレクトリ クレデンシャルを使用できるようになります。
- 社内ディレクトリ インターフェイスでエンド ユーザ パスワードを管理する（認証を有効にすると、Cisco Unified CallManager Administration ページにパスワード フィールドが表示されなくなります）。
- Cisco Unified CallManager Administration または Cisco Unified CallManager User Options ページでエンド ユーザ PIN を管理する。
- Cisco Unified CallManager Administration でアプリケーション ユーザ パスワードを管理する（これらの仮想ユーザは Cisco Unified Communications の他の機能およびアプリケーションとの通信専用であり、実在の人物に関連付けられていません）。
- 対応するエンド ユーザを Cisco Unified CallManager Administration ページから Unified CM Super Users ユーザ グループに追加することにより、Cisco Unified CallManager 管理者のシングル ログオンを有効にする。カスタマイズしたユーザ グループおよびロールを作成することにより、複数レベルの管理者権利を定義できます。

Microsoft Active Directory に関する追加の考慮事項

Microsoft Active Directory で LDAP 認証を有効にする場合、応答時間の短縮のために Microsoft Active Directory グローバル カタログ サーバに照会するように Cisco Unified CallManager を設定することをお勧めします。

グローバル カタログに対する照会を有効にするには、グローバル カタログ ロールが有効になっているドメイン コントローラの IP アドレスまたはホスト名を指すように LDAP Authentication ページの LDAP Server Information を設定し、LDAP ポートを 3268 として設定するだけです。

Microsoft AD から同期するユーザが複数のドメインに属していると、認証へのグローバル カタログの使用がさらに効率的になります。Cisco Unified CallManager は、照会に従う必要がなく、すぐにユーザを認証できるためです。このような場合は、Cisco Unified CallManager がグローバル カタログ サーバを指すようにし、LDAP User Search Base をルート ドメインの最上位に設定します。

複数のツリーを含む Microsoft AD フォレストの場合には、追加の考慮事項が適用されます。単一の LDAP 検索ベースでは複数のネームスペースを扱えないので、Cisco Unified CallManager は別のメカニズムを使用して、これらの不連続なネームスペース間でユーザを認証する必要があります。

P.16-11 の「LDAP 同期」の項で説明したように、複数のツリーがある AD フォレストで同期をサポートするために、UserPrincipalName（UPN）属性を Cisco Unified CallManager 内でユーザ ID として使用する必要があります。ユーザ ID が UPN の場合、Cisco Unified CallManager Administration の LDAP Authentication 設定ページで LDAP Search Base フィールドへの入力はできませんが、その代わりに「LDAP user search base is formed using userid information.」という注意が表示されます。

実際には、図 16-15 に示すように、ユーザごとに UPN サフィックスからユーザ検索ベースが導き出されます。この例では、Microsoft Active Directory フォレストは avvid.info と vse.lab という 2 つのツリーで構成されます。同じユーザ名が両方のツリーに表示される場合があるため、同期プロセス中および認証プロセス中は UPN を使用してデータベースのユーザを固有に識別するように、Cisco Unified CallManager が設定されています。

図 16-15　複数のツリーがある Microsoft AD フォレストでの認証

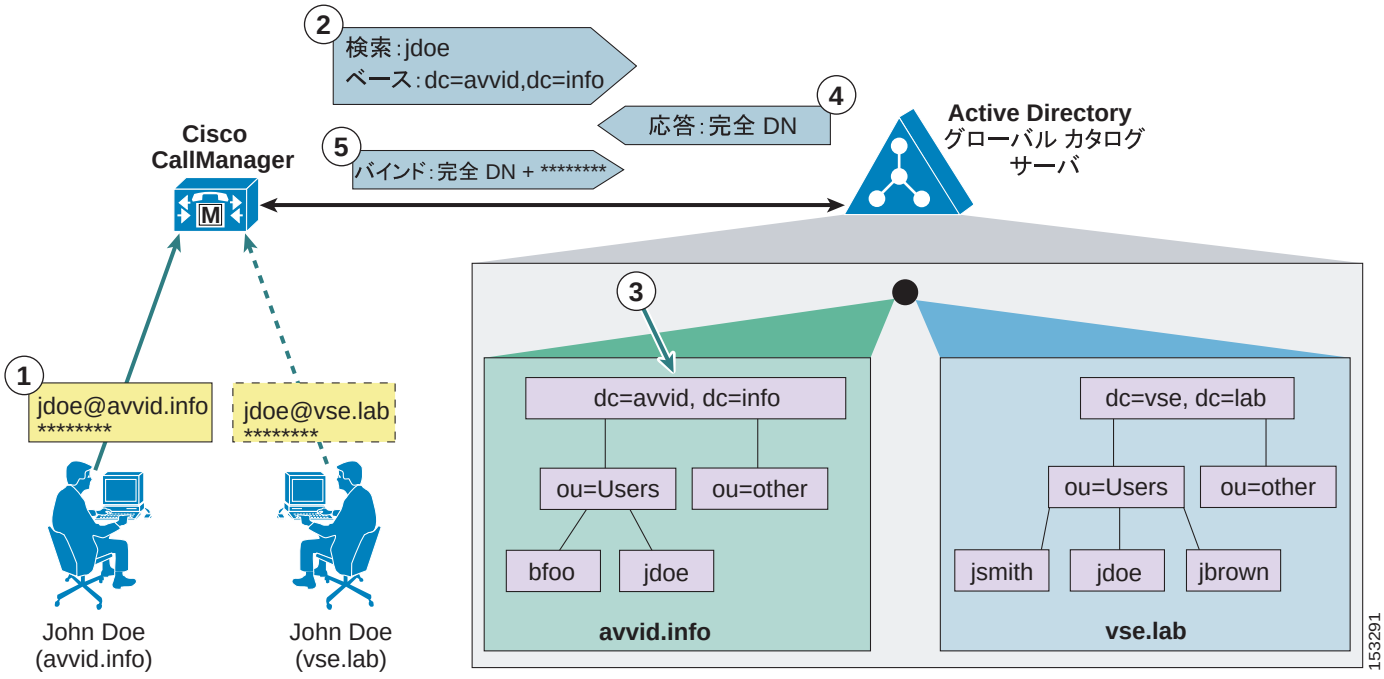


図 16-15 に示すように、John Doe という名前のユーザが avvid.info ツリーと vse.lab ツリーの両方に存在します。次の手順は、UPN が jdoe@avvid.info となる第 1 のユーザに対する認証プロセスを示しています。

1. ユーザは、ユーザ名（UPN に対応するもの）とパスワードを使用し、HTTPS 経由で Cisco Unified CallManager に対して認証します。
2. Cisco Unified CallManager は、Microsoft Active Directory グローバル カタログ サーバに対して LDAP 照会を実行し、UPN で指定したユーザ名（@ 記号より前の部分）を使用して、UPN サフィックス（@ 記号より後の部分）から LDAP 検索ベースを得ます。この場合、ユーザ名は jdoe で、LDAP 検索ベースは「dc=avvid, dc=info」です。
3. Microsoft Active Directory は、LDAP 照会で指定したツリーのユーザ名に対応する正しい認定者名を識別します。この場合は、「cn=jdoe, ou=Users, dc=avvid, dc=info」です。
4. Microsoft Active Directory は LDAP 経由で、このユーザの完全認定者名を使用して Cisco Unified CallManager に応答します。
5. Cisco Unified CallManager は、提供された認定者名とユーザが最初に入力したパスワードで LDAP バインドを試行し、その後は図 16-14 に示す標準的な場合と同様に、認証プロセスが続行されます。

（注）　複数のツリーを含む Microsoft AD フォレストでの LDAP 認証のサポートは、上記の方法だけで行われます。したがってサポートは、ユーザの UPN サフィックスが、そのユーザが存在するツリーのルート ドメインに対応する配置だけに限定されます。UPN サフィックスがツリーの実際のネームスペースから分離されている場合は、Microsoft Active Directory フォレスト全体で Cisco Unified CallManager ユーザを認証できなくなります（ただし、その場合でも、別の属性をユーザ ID として使用し、統合をフォレスト内の単一のツリーに限定することはできます）。