



# ディレクトリの概要

ディレクトリは、多数の読み取りと検索、および随時の書き込みと更新用に最適化されている特殊なデータベースで構成されます。通常、ディレクトリには、社員の情報や社内ネットワーク上のユーザ特権など、頻繁に変更されないデータが格納されます。

ディレクトリは拡張できるため、ディレクトリに格納する情報のタイプを変更および拡張できます。ディレクトリスキーマという用語は、格納する情報のタイプ、および情報が従う規則を示します。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の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、アプリケーションに、ディレクトリに格納されている情報にアクセスして必要に応じてその情報を変更する標準的な方法を提供します。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が使用できる 1 つのリポジトリに集中させることができるため、追加、移動、および変更が簡単になり、メンテナンスコストを削減できます。

この章では、Cisco CallManager の組み込みディレクトリについて簡単に説明し、Cisco CallManager を社内 LDAP ディレクトリと統合するための主な方針を示します。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が社内 LDAP ディレクトリにアクセスできるようにするための考慮事項についても概説します。

この章の構成は、次のとおりです。

- Cisco CallManager 組み込み LDAP ディレクトリ (P.17-3)
- ディレクトリ アクセスとディレクトリ統合 (P.17-7)
- 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.17-10)
- Cisco CallManager とのディレクトリ統合 (P.17-12)
- 参考情報 (P.17-16)

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 Cisco CallManager エクステンション モビリティ、Cisco IP Manager Assistant、Cisco WebDialer、Bulk Administration Tool、Real-Time Monitoring Tool、および MultiLevel Administration (MLA) 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 URL で利用できる各製品マニュアルを参照してください。

<http://www.cisco.com>

特に、Cisco Unity については、『Cisco Unity 設計ガイド』、ホワイトペーパー「Cisco Unity Data and the Directory」、*「Active Directory Capacity Planning」*、および「Cisco Unity Data Architecture and How Cisco Unity Works」を参照してください。

Cisco Unity の日本語版マニュアルについては、次の URL を参照してください。

[http://www.cisco.com/japanese/warp/public/3/jp/service/manual\\_j/index\\_uc\\_cu.shtml](http://www.cisco.com/japanese/warp/public/3/jp/service/manual_j/index_uc_cu.shtml)

## Cisco CallManager 組み込み LDAP ディレクトリ

Cisco CallManager は、組み込み LDAP ディレクトリとして Data Connection Directory (DC-Directory) を使用します。ユーザに関する認証および許可情報を格納するこのディレクトリは、Cisco CallManager に標準で付属しています（つまり、インストール時に特別な設定は不要です）。認証は、ユーザがシステムにアクセスする権限を与える方式を確立します。一方、許可は、ユーザが使用を許可されている特定の内線番号などのテレフォニー リソースを指定します。

インストール後、Cisco CallManager パブリッシャ サーバには、読み取りおよび書き込みバージョンの LDAP ディレクトリとデータベースが組み込まれており、サブスクリバ サーバには、読み取り専用バージョンが組み込まれています。システムは、LDAP を使用して、Cisco CallManager およびサポートされているすべてのアプリケーションと通信し、TCP ポート 8404 を使用します。セキュリティが使用可能な場合は、LDAPS (LDAP over SSL) が TCP ポート 8405 を使用します（詳細については、P.17-5 の「LDAP と Secured Sockets Layer」を参照してください）。

管理者は、Cisco CallManager Administration の [ユーザの設定] ウィンドウから、組み込み LDAP ディレクトリにアクセスします。管理者は、[ユーザの設定] ウィンドウを使用して、ユーザ ID、パスワード、デバイスの関連付けなどのユーザ情報を追加、更新、および削除します。



(注)

DC Directory は、定期的なパスワードの期限切れや、パスワード長および複雑なルールの適用といったパスワード管理機能をサポートしていません。パスワード管理機能を使用できるようにするには、これらの機能を提供できるエンタープライズ ディレクトリを Cisco CallManager に統合する必要があります。パスワード管理機能とそれらをサポートするエンタープライズ ディレクトリの詳細については、『Cisco Customer Directory Configuration Plugin for Cisco CallManager Release 4.2 (1) インストレーションガイド』を参照してください。

**注意**

統合エンタープライズ ディレクトリ（組み込み DC-Directory とは対照的に）があれば、定期的なパスワードの期限切れなどのパスワード管理機能を設定できる場合があります。システムへの重要なアクセスが中断されるのを防ぐために、CCMAdministrator、CCMSysUser、IPMASysUser の各システム ユーザと、その他に Cisco CallManager アプリケーションが作成および使用するシステム ユーザに対しては、パスワードの有効期限を設定しないでください。これらのユーザには決して期限切れになることのないパスワードを設定する必要があります。

**注意**

DC Directory、Netscape Directory、または Active Directory でカタカナやキリル文字などの 2 バイト文字セットを使用すると、ディレクトリ データベース エラーが発生する可能性があります。このリリースの Cisco CallManager は、どのディレクトリでも 2 バイト文字セットの使用をサポートしていません。

**組み込み LDAP ディレクトリを使用するアプリケーションとサービス**

次の Cisco CallManager アプリケーションおよびサービスは、ユーザ情報や他のタイプの情報用に組み込み LDAP ディレクトリを使用します。

- Bulk Administration Tool (BAT)
- Tool for Auto-Registered Phone Support (TAPS)
- AXL
- Cisco CallManager エクステンション モビリティ
- MultiLevel Administration (MLA)
- Cisco CallManager ユーザ オプション
- Cisco Conference Connection
- CTIManager
- CDR Analysis and Reporting (CAR)
- Cisco IP Manager Assistant (IPMA)
- Cisco Customer Response Solutions (CRS)
- Personal Assistant

- Cisco Emergency Responder (CER)
- Cisco IP Phone サービス
- Personal Address Book (PAB; 個人アドレス帳)
- FastDials
- Cisco WebDialer
- Cisco IP SoftPhone
- Cisco IP Communicator
- Cisco CallManager Attendant Console

LDAP を介したセキュリティについては、[P.17-5](#) の「[LDAP と Secured Sockets Layer](#)」を参照してください。

### LDAP と Secured Sockets Layer

ディレクトリがインストールされるときに (Cisco CallManager のインストール時)、Secured Sockets Layer (SSL) が使用可能な DC-Directory v3.0.02 が自動的にインストールされます。自己署名証明書が自動的に作成されて DC-Directory にインストールされ、LDAP over SSL にポート 8405 を使用するよう設定されます。

LDAP ディレクトリ (LDAPS) は SSL をサポートしています。Cisco CallManager 組み込みディレクトリは、デフォルトで SSL をサポートしています。Microsoft Active Directory など、社内 LDAP ディレクトリを使用する場合は、管理者が SSL を設定できます。LDAPS 機能により、パスワードやユーザ ID などのデータをディレクトリとの間で安全にやりとりできます。

SSL サポートとは、LDAP サーバ (DC-Directory、または Cisco CallManager と統合されている社内ディレクトリのいずれか) にセキュリティ証明書があることを意味します。クライアント (たとえば、Cisco CallManager Administration や BAT) は、証明書ベースのクライアント認証をサポートしません。クライアントが安全な接続を要求すると、サーバが証明書を提示し、クライアントはその証明書自体またはその証明書を発行した certificate authority (CA; 認証局) が信頼されているかどうかを確認します。信頼されている場合、クライアントは安全な接続の確立を開始します。信頼されていない場合、接続は拒否されます。

[表 17-1](#) は、LDAPS をサポートするアプリケーションおよびサービスのリストを示しています。

表 17-1 LDAP をサポートする Cisco CallManager アプリケーション

安全なディレクトリ アプリケーション (LDAPS)	安全でないディレクトリ アプリケーション
Cisco CallManager Administration	Cisco Customer Response Solutions (CRS)
Multilevel Administration	Personal Assistant
Cisco CallManager ユーザ オプション	Cisco Emergency Responder
Cisco CallManager エクステンション モビリティ	Cisco IP Phone サービス
Cisco Conference Connection	個人アドレス帳
CTIManager	FastDials
CDR Analysis and Reporting	Directory Integration API
Cisco IPMA	Cisco WebDialer
Bulk Administration Tool	Cisco IP SoftPhone
	Cisco CallManager Attendant Console
	Cisco IP Communicator

Cisco CallManager が社内 LDAP ディレクトリを使用する必要がある場合、管理者は、カスタマー ディレクトリ プラグインを使用して、この機能を設定する必要があります。Cisco Customer Directory プラグインでは、Cisco CallManager を次のいずれかのエンタープライズディレクトリと統合できます。

- Microsoft Active Directory (AD)、Microsoft Windows 2000 で使用可能
- Microsoft Active Directory (AD 2003)、Microsoft Windows 2003 で使用可能
- Netscape Directory Server (バージョン 4.x)、iPlanet Directory Server (バージョン 5.1)、および Sun ONE Directory Server (バージョン 5.2)

この機能については、P.17-7 の「ディレクトリ アクセスとディレクトリ統合」および P.17-12 の「Cisco CallManager とのディレクトリ統合」を参照してください。

統合およびインストールの手順については、『Cisco Customer Directory Configuration Plugin for Cisco CallManager インストレーションガイド』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

この章全体にわたって、次の定義および区別が適用されます。

- 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を使用せずに、中央の社内 LDAP ディレクトリにユーザ関連の情報を格納する機能です。

図 17-1 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

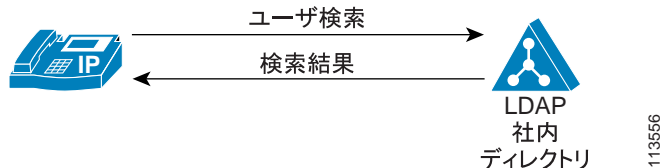
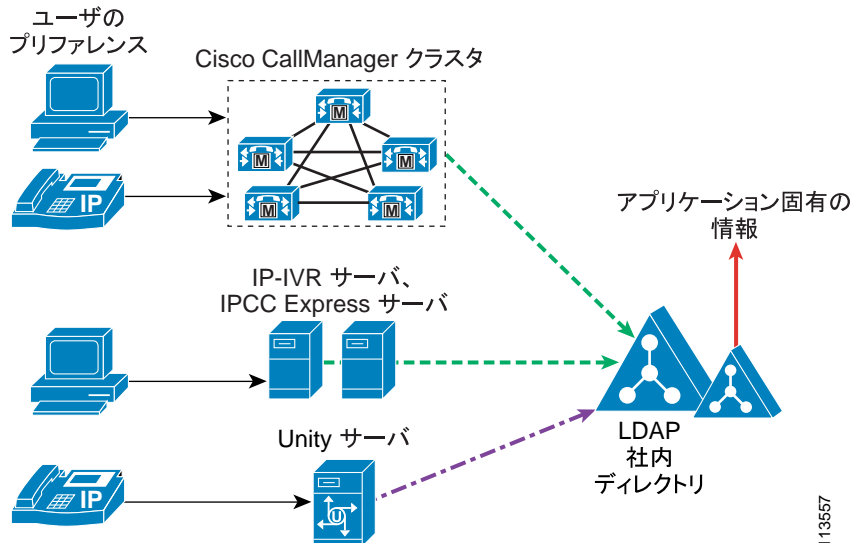


図 17-1 は、この章で定義するディレクトリ アクセスを示しています。この例では、Cisco IP Phone がアクセスしています。クライアント アプリケーションが、LDAP ディレクトリ（企業の社内ディレクトリなど）に対してユーザ検索を実行し、複数的一致するエントリを受け取ります。その後、1つのエントリを選択し、そのエントリを使用して、Cisco IP Phone から対応するユーザにダイヤルできます。

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を1つの社内ディレクトリと統合するディレクトリ統合は、それらのアプリケーションが、独自の組み込みデータベースを使用するのではなく、中央のディレクトリにユーザ関連の情報を実際に格納することを意味します。図 17-2 は、この章で定義しているディレクトリ統合の例を示しています。

図 17-2 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



113557

ディレクトリ統合には、ディレクトリに対する読み取りおよび書き込み操作が含まれるため、社内 LDAP ディレクトリに対してスキーマの拡張や他の設定変更が必要となります。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（ユーザが制御するものや、個人アドレス帳エントリなど）を格納します。ただし、一般的な社員情報（電子メール アドレス、オフィスの住所、役職名など）の格納に通常使用される社内 LDAP ディレクトリと Cisco CallManager を統合することもできます。その場合、Cisco CallManager は、独自の組み込みディレクトリを使用しなくなり、アプリケーション固有のユーザ情報を社内ディレクトリに格納します。



(注) Cisco CallManager リリース 3.1 は、Microsoft Active Directory (AD) 2000 および Netscape Directory Server (バージョン 4.x) のディレクトリ統合をサポートしています。Cisco CallManager リリース 3.3(2) およびそれ以降のリリースでは、iPlanet Directory Server (バージョン 5.1) および Sun ONE Directory Server (バージョン 5.2) のサポートが追加されています。



Cisco CallManager などのアプリケーションを社内ディレクトリと統合することには、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、次のような意味合いも含まれます。

- アプリケーション固有のユーザ属性を社内ディレクトリに格納するには、ディレクトリ スキーマを拡張する必要がある。この複雑な操作を行うには、ディレクトリ構造を熟知している必要があります。
- アプリケーションがディレクトリといつでも通信でき、ディレクトリが十分な応答時間を確保できる必要がある。ディレクトリ サービスの可用性は、アプリケーションの機能に影響を及ぼすことがあります。
- データの保管と、読み取りおよび書き込みクエリーによって、ディレクトリに追加の負荷がかかる。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、サーバの過剰使用を避けるために、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、各展開のビジネス ニーズを確認する必要があります。

# 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

この項で示すガイドラインは、Cisco CallManager や他の IP テレフォニー アプリケーションが社内ディレクトリと統合されているかどうかに関係なく適用されます。統合されているかどうかの違い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格納する方法と、ネットワーク上でその情報の一貫性が保持される方法だけであるため、どちらの場合もエンド ユーザからは同じに見えます。

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 対応ディレクトリ 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)

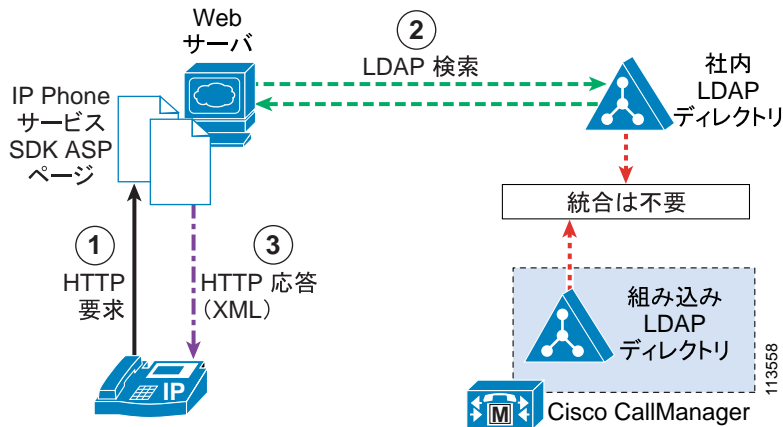
Cisco IP SoftPhone リリース 1.2 以降には、Cisco IP Communicator と同様、LDAP ディレクトリにアクセスして検索するメカニズムが組み込まれています。この機能を設定する方法の詳細については、製品マニュアルを参照してください。

## 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、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、HyperText Transfer Protocol (HTTP; ハイパーテキスト転送プロトコル) を使用して、Web サーバに要求を送信します。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、電話機から要求を受け取ってその要求を LDAP 要求に変換することにより、プロキシとして機能します。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 17-3 は、Cisco CallManager が社内ディレクトリと統合されていない展開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ません。

図 17-3 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 サーバによって提供されるプロキシ機能を設定するには、Cisco LDAP Search Component Object Model (COM) サーバが組み込まれている Cisco IP Phone Services Software Development Kit (SDK) バージョン 2.0 以降を使用します。

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

- システムは、LDAPv3 対応のすべてのディレクトリをサポートしている。
- Cisco CallManager ユーザプリファレンス（短縮ダイヤル、Call Forward All、個人アドレス帳）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 ユーザ オプション ウィンドウ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

Cisco CallManager は、組み込み Microsoft SQL データベースを使用して、ダイヤルプラン情報、電話機やゲートウェイの設定、メディア リソースの使用率など、システムおよびデバイスの設定データを格納します。また、組み込み LDAP ディレクトリを使用して、ユーザが制御しているデバイス、Computer Telephony Integration (CTI; コンピュータ テレフォニー統合) ユーザパラメータ、個人アドレス帳エントリなど、ユーザおよびアプリケーションのプロファイルを格納します。

SQL データベースも LDAP ディレクトリもクラスタ内の各 Cisco CallManager サーバ上で実行され、サーバ間で複製許諾契約が自動的に設定されます。パブリッシュ 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 コピーが保管されています。パブリッシュ サーバは、すべてのサブスクリイバ サーバへの複製を処理します。サブスクリイバ サーバには、両方のリポジトリの読み取り専用コピーが保管されています。

アプリケーション固有の情報を LDAP ディレクトリに格納するために、Cisco CallManager は、組み込みディレクトリを使用する場合と社内ディレクトリと統合する場合の両方で有効な方法を使用します。

通常は、ディレクトリのベンダーが異なると、異なるユーザ オブジェクト モデルが使用され、各モデルが複数の非標準追加属性を持っています。このため、Cisco CallManager は、ユーザ オブジェクトの標準 LDAPv3 コア属性だけを使用します。ユーザ オブジェクトは、次の属性を含む補助クラス `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一意に識別します。

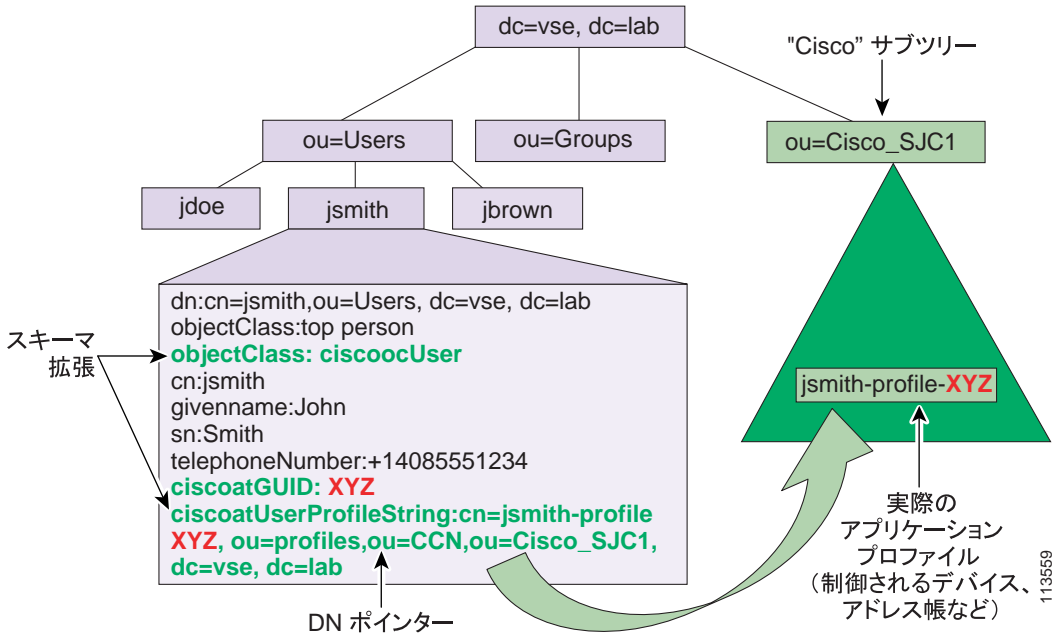
- `ciscoatUserProfile`

以前のバージョンの Cisco CallManager や他のアプリケーションは、この属性を使用します。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、アプリケーション固有のユーザ プロファイルを含む、ディレクトリ内の別のオブジェクトへの識別名ポインタを示します。この方法により、コア ユーザ オブジェクトへの影響を最小限に抑えながら、アプリケーション固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) と呼ばれる、ディレクトリ内の別の organizational unit (OU; 組織ユニット) に格納できます。図 17-4 は、このプロセスを示しています。

図 17-4 アプリケーション固有のユーザ情報をディレクトリに格納するための 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 クラスに属します。このオブジェクトには、ユーザ 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が格納されています。Cisco CallManager が使用するアプリケーション プロファイルは、`CCNocAppProfile` 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格納します。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)

この章では、Cisco CallManager リリース 4.2 に基づいて例や推奨事項を示しています。以前のバージョンの 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ことがあります。

## Cisco Customer Directory Configuration プラグイン

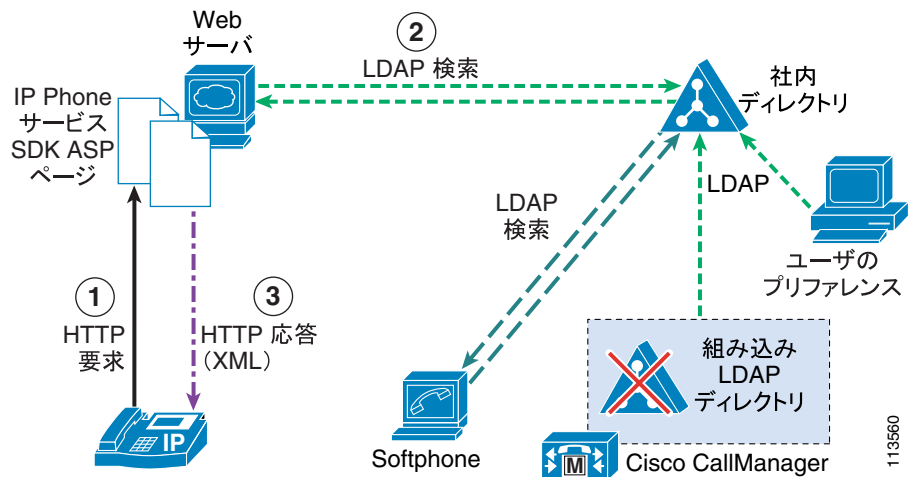
Cisco CallManager を外部 LDAP ディレクトリと統合するには、Cisco CallManager にバンドルされている Cisco Customer Directory Configuration プラグインを実行します (**Applications > Install Plugins**)。このプラグインは、次の目的を果たします。

- 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および属性に対応できるようにする。
- 「Cisco」サブツリーに、Cisco CallManager が必要とする設定オブジェクトを実装する。
- 社内ディレクトリを使用するように Cisco CallManager を設定し、組み込みディレクトリを使用不可にする。
- 管理者が LDAP over SSL を設定できるようにする。LDAP over SSL が設定されている場合、ディレクトリとの間でデータがやりとりされるたびに、SSL ポート番号と、サーバ証明書へのパスが要求されます。

通常、Cisco CallManager 上でローカルにプラグインを実行すると、スキーマの更新が行われます。ただし、Cisco CallManager リリース 4.0 からは、LDAP Data Interchange Format (LDIF) ファイルを別個に作成する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施でき、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減ります。

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 プリファレンスを格納します。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ように設定されている場合は、[図 17-5](#) に示すようなシナリオになります。

図 17-5 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



113560

## 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と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る。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格納する。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、サーバの通常の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。

## 参考情報

### 関連項目

- [Cisco CallManager グループ \(P.5-2\)](#)
- [システム設定チェックリスト \(P.5-20\)](#)

### 参考資料

- *Cisco Customer Directory Configuration Plugin for Cisco CallManager Release 4.2 (1) インストレーションガイド*
- *Cisco CallManager Release 4.2(1) インストレーションガイド*
- *Cisco IP テレフォニー ソリューション リファレンス ネットワーク デザイン ガイド*