CHAPTER 6

LDAP ディレクトリと Cisco Unity Connection の連動

Lightweight Directory Access Protocol（LDAP; ライトウェイト ディレクトリ アクセス プロトコル）は、社内ディレクトリに保存されたユーザ情報にアクセスするための標準方式を Cisco Unity Connection などのアプリケーションに提供します。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。

Cisco Unity Connection7.x は、LDAP ディレクトリの同期化および認証をサポートする最初の Connection リリースです。

Connection と LDAP ディレクトリの連動により、次のような利点があります。

- **ユーザ作成**：LDAP ディレクトリからデータをインポートして Connection ユーザを作成できます。
- **データの同期化**：Connection データベース内のユーザ データと LDAP ディレクトリ内のデータを自動的に同期化するように Connection を設定できます。
- **シングル サインオン**：ユーザが複数のアプリケーションでパスワードを管理しなくてもいいように、オプションで、Connection Web アプリケーションのユーザ名とパスワードを LDAP ディレクトリに対して認証するように Connection を設定できます （電話パスワードは引き続き、Connection データベース内で管理されます）。

Connection は LDAP ディレクトリ内のデータへのアクセスに、標準の LDAPv3 を使用します。Connection によって同期化がサポートされる LDAP ディレクトの一覧については、『*System Requirements for Cisco Unity Connection Release 7.x*』の「Requirements for an LDAP Directory Integration」の項を参照してください。

この章では、Cisco Unity Connection 7.x と社内 LDAP ディレクトリの連動における主要な設計上の問題について説明します。次の各項を参照してください。

LDAP の同期化

LDAP の同期化では、Cisco Directory Synchronization（DirSync）という内部ツールを使用して、Cisco Unity Connection ユーザ データ（氏名、エイリアス、電話番号など）の小さいサブセットと、社内 LDAP ディレクトリ内の対応するデータを同期化します。Connection データベース内のユーザ データを社内 LDAP ディレクトリ内のユーザ データと同期化するには、次のタスクを実行します。

1. LDAP 同期化を設定し、Connection 内のデータと LDAP ディレクトリ内のデータの関係を定義します。「LDAP 同期化の設定」（P.6-2）を参照してください。

2. LDAP ディレクトリからデータをインポートしたり、既存の Connection ユーザのデータを LDAP ディレクトリ内のデータに関連付けたりして、新しい Connection ユーザを作成します。「Cisco Unity Connection ユーザの作成」（P.6-5）を参照してください。

   さらに細かく制御するために、Connection ユーザを作成する前に LDAP フィルタを作成できます。「LDAP ユーザのフィルタリング」（P.6-6）を参照してください。

LDAP 同期化の設定

LDAP ディレクトリの同期化を設定する場合は、Cisco Unity Connection サーバまたはクラスタごとに、最大 5 つの LDAP ディレクトリ構成を作成できます。各 LDAP ディレクトリ構成では、1 つのドメインまたは 1 つの Organizational Unit（OU; 組織ユニット）だけをサポートできます。5 つのドメインまたは OU からユーザをインポートする場合は、LDAP ディレクトリ構成を 5 つ作成する必要があります。

Connection デジタル ネットワークも、ネットワークに参加するそれぞれの Connection サーバまたはクラスタに対して最大 5 つの LDAP ディレクトリ構成をサポートします。たとえば、サーバが 5 つあるデジタル ネットワークの場合、最大 25 のドメインからユーザをインポートできます。

各 LDAP ディレクトリで、次の項目を指定します。

- **構成がアクセスするユーザ検索ベース。**ユーザ検索ベースは、Connection がユーザ アカウントの検索を開始する LDAP ディレクトリ ツリー内の位置です。Connection は、検索ベースで指定されたツリーまたはサブツリー（ドメインまたは OU）内のユーザをすべてインポートします。Connection サーバまたはクラスタは、たとえば同じ Active Directory フォレストなど、同じディレクトリ ルートを持つサブツリーからだけ、LDAP データをインポートできます。

  Microsoft Active Directory 以外の LDAP ディレクトリを使用していて、ディレクトリのルートをユーザ検索ベースとして指定した Connection LDAP ディレクトリ構成を作成した場合、Connection はディレクトリ内のすべてのユーザのデータをインポートします。ディレクトリのルートに、Connection がアクセスすべきでないサブツリー（たとえば、サービス アカウントのサブツリー）が含まれている場合は、次のいずれかを行う必要があります。

  - 複数の Connection LDAP ディレクトリ構成を作成し、Connection がアクセスすべきでないユーザを除外した検索ベースを指定する。
  - LDAP 検索フィルタを作成する。詳細については、『*System Administration Guide for Cisco Unity Connection Release 7.x*』の「Integrating Cisco Unity Connection with an LDAP Directory」の章の「Filtering LDAP Users」の項を参照してください。

  Active Directory 以外のディレクトリの場合は、複数の構成を作成することになっても、同期化に必要な時間を短縮するためにできるだけ少ない数のユーザを含むユーザ検索ベースを指定することをお勧めします。

  Active Directory を使用していてドメインに子ドメインが存在する場合、それぞれの子ドメインにアクセスするための個別の構成を作成する必要があります。Connection は同期化中には Active Directory の照会には従いません。これは、複数のツリーが存在する Active Directory フォレストについても同様です。各ツリーにアクセスするには、1 つ以上の構成を作成する必要があります。この構成では、UserPrincipalName（UPN）属性を Connection の [エイリアス] フィールドにマッピングする必要があります。UPN は、フォレスト全体で一意であることが Active Directory によって保証されます。複数のツリーが存在する AD で UPN 属性を使用する場合のその他の考慮事項については、「認証と Microsoft Active Directory に関するその他の考慮事項」（P.6-8）を参照してください。

それぞれが 1 つの LDAP ディレクトリに統合されている複数の Connection サーバにネットワーク接続するためにデジタル ネットワークを使用している場合は、別の Connection サーバ上にあるユーザ検索ベースにオーバーラップする、Connection サーバ上のユーザ検索ベースを指定しないでください。指定してしまうと、複数の Connection サーバ上に同一の Connection ユーザ用のユーザ アカウントとメールボックスを持つことになります。

（注）　1 つまたは複数の Connection サーバに LDAP フィルタを作成すると、ユーザの重複を避けることができます。詳細については、『*System Administration Guide for Cisco Unity Connection Release 7.x*』の「Integrating Cisco Unity Connection with an LDAP Directory」の章の「Filtering LDAP Users」の項を参照してください。

- **Connection が、ユーザ検索ベースで指定されたサブツリーへのアクセスに使用する LDAP ディレクトリ内の管理者アカウント。**Connection はこのアカウントを使用して、ディレクトリへのバインドを実行し、認証します。検索ベース内のすべてのユーザ オブジェクトを「読み取る」だけの最小権限を設定し、パスワードを無期限にした Connection 専用のアカウントを使用することをお勧めします（管理者アカウントのパスワードを変更すると、Connection を新しいパスワードで再構成する必要があります）。

  複数の構成を作成する場合は、構成ごとに 1 つの管理者アカウントを作成し、そのアカウントには、対応するサブツリー内だけのすべてのユーザ オブジェクトの「読み取り」権限を付与することをお勧めします。構成を作成する場合、管理者アカウントには完全識別名を入力します。そのため、このアカウントは LDAP ディレクトリ ツリー内の任意の場所に属することができます。

- **Connection が Connection データベースと LDAP ディレクトリを自動的に再同期化する頻度（実行する場合）。**再同期化について、次回実行する日時、1 回だけ実行するかスケジュールに従って実行するか、またスケジュールに従う場合は、時間、日、週、または月単位で実行する頻度（6 時間以上）を指定できます。複数の規定で同じ LDAP サーバを同時に問い合せることがないように、同期化スケジュールをずらすことをお勧めします。スケジュールの同期化は、営業時間外に実行されます。
- **Connection が LDAP データへのアクセスに使用する LDAP サーバのポート。**
- **オプションで、LDAP サーバと Connection サーバの間で転送されるデータの暗号化に SSL を使用するかどうか。**
- **1 つ以上の LDAP サーバ。**いくつかの LDAP ディレクトリでは、同期化を試行する際に Connection が使用する LDAP ディレクトリ サーバは、3 つまで指定できます。Connection は、指定された順序でサーバへの接続を試行します。どのディレクトリ サーバも応答しない場合、同期化は失敗します。Connection は、次回にスケジュールされた同期化の時間に再実行します。ホスト名ではなく IP アドレスを使用することで、Domain Name System（DNS; ドメイン ネーム システム）の可用性への依存を解消できます。

（注）　同期化のために Connection がアクセスする LDAP ディレクトリ サーバが利用できなくなるときに備えて追加の LDAP ディレクトリ サーバをバックアップとして指定することは、すべての LDAP ディレクトリでサポートされているわけではありません。使用している LDAP ディレクトリが複数のディレクトリ サーバの指定をサポートするかどうかの詳細については、『*System Requirements for Cisco Unity Connection Release 7.x*』の「Requirements for an LDAP Directory Integration」の項を参照してください。

- **LDAP ディレクトリ属性の Connection フィールドへのマッピングについては、表 6-1 に記載されています。**Connection の [エイリアス] フィールドへのマッピングは、すべての構成で同一にする必要があります。LDAP 属性を Connection の [エイリアス] フィールドにマッピングする場合は、次の手順を実行します。
  - LDAP ディレクトリから Connection にインポートするすべてのユーザが、その属性で一意の値を持つことを確認します。
  - Connection データベース内にすでにユーザが存在する場合は、ディレクトリからインポートするユーザの属性の値と、既存の Connection ユーザの [エイリアス] フィールドの値が一致しないことを確認します。

  ディレクトリから Connection にインポートするすべてのユーザについて、LDAP の sn 属性に値が存在する必要があります。sn 属性の値が空白の LDAP ユーザは、Connection データベースにインポートされません。

  LDAP ディレクトリ内のデータの完全性を保護するために、インポートする値は Connection ツールを使用して変更できません。Connection 固有のユーザ データ（グリーティング、通知デバイス、カンバセーション プリファレンスなど）は Connection で管理され、Connection のローカル データベースだけに保存されます。

  パスワードまたは PIN は、LDAP ディレクトリから Connection データベースにコピーされません。Connection ユーザを LDAP ディレクトリに対して認証する場合は、「LDAP 認証」（P.6-6）を参照してください。

表 6-1　Cisco Unity Connection ユーザ フィールドへの LDAP ディレクトリ属性のマッピング

LDAP ディレクトリ属性	Cisco Unity Connection ユーザ フィールド
次のいずれかの属性： • samAccountName • mail • employeeNumber • telephoneNumber • userPrincipleName	エイリアス
givenName	名
次のいずれかの属性： • middleName • initials	イニシャル
SN	姓
manager	マネージャ
department	部署名
次のいずれかの属性： • telephoneNumber • ipPhone	社内電話番号
次のいずれかの属性： • mail • samAccountName	社内電子メール アドレス
title	役職

表 6-1　Cisco Unity Connection ユーザ フィールドへの LDAP ディレクトリ属性のマッピング （続き）

LDAP ディレクトリ属性	Cisco Unity Connection ユーザ フィールド
homePhone	自宅（インポートされるが、現在は使用されない。Connection Administration では表示されない）
mobile	携帯電話（インポートされるが、現在は使用されない。Connection Administration では表示されない）
pager	ポケットベル（インポートされるが、現在は使用されない。Connection Administration では表示されない）

クラスタリング（アクティブ/アクティブ高可用性）構成の場合、LDAP ディレクトリからインポートされたデータも含めて、すべてのユーザ データは Connection パブリッシャ サーバからサブスクライバ サーバに自動的にレプリケートされます。この構成では、Cisco DirSync サービスはパブリッシャ サーバだけで実行されます。

Cisco Unity Connection ユーザの作成

LDAP ディレクトリと連動する Cisco Unity Connection システムでは、LDAP ディレクトリからデータをインポートするか、既存の Connection ユーザを変換して LDAP ディレクトリと同期化するか、またはその両方を実行して、Connection ユーザを作成できます。次のことに注意してください。

- LDAP データをインポートして Connection ユーザを作成する場合、Connection は表 6-1 で指定された値を LDAP ディレクトリから取得し、指定した Connection ユーザ テンプレートから残りの情報を入力します。
- 既存のユーザを変換する場合、表 6-1 に示すフィールドの既存の値は、LDAP ディレクトリ内の値で置き換えられます。
- LDAP ディレクトリからインポートするすべてのユーザについて、Connection [エイリアス] フィールドにマッピングする LDAP 属性の値は、Connection オブジェクト（スタンドアロン ユーザ、LDAP ディレクトリからインポート済みのユーザ、AXL を使用して Cisco Unified Communications Manager からインポートされたユーザ、連絡先、同報リストなど）のすべての Connection [エイリアス] フィールド内の値と一致してはいけません。
- Connection を LDAP ディレクトリと同期化したら、引き続き、LDAP ディレクトリと連動していない Connection ユーザを追加できます。AXL サーバを使用して Cisco Unified Communications Manager からユーザをインポートして、Connection ユーザの追加を継続することもできます。
- Connection を LDAP ディレクトリと同期化した後は、新しい LDAP ディレクトリ ユーザが自動的に Connection にインポートされることはないため、手動でインポートする必要があります。
- LDAP からユーザをインポートすると、そのユーザは Cisco Unity Connection Administration のユーザ ページで、「LDAP ディレクトリからインポートされたアクティブ ユーザ」として識別されます。
- その後、社内ディレクトリ内のユーザ データが変更されると、LDAP ディレクトリから入力された Connection フィールドは、次回にスケジュールされた再同期化の際に LDAP の新しい値で更新されます。

LDAP ユーザのフィルタリング

さまざまな理由により、Cisco Unity Connection にインポートする LDAP ユーザをより細かく制御したい場合があります。次の例を参考にしてください。

- LDAP ディレクトリが、ユーザ検索ベースの指定では十分に制御できないフラット構造になっている。
- LDAP ユーザ アカウントのサブセットだけを Connection ユーザにする必要がある。
- LDAP ディレクトリ構造が、Connection へのユーザのインポート方法に適さない。次の例を参考にしてください。
  - 組織ユニットが組織階層に従って設定されており、ユーザは地理情報によって Connection にマッピングされる場合、この 2 つの間にオーバーラップはほとんどありません。
  - ディレクトリ内のすべてのユーザが 1 つのツリーまたはドメイン内にあるのに、複数の Connection サーバをインストールしたい場合、ユーザが複数の Connection サーバ上でメールボックスを持つような事態を避けるための処置を行う必要があります。

このような場合は、「set cuc ldapfilter」CLI コマンドを使用して、ユーザ検索ベースをより細かく制御することがあります。次のことに注意してください。

- 「set cuc ldapfilter」CLI コマンドは、Cisco Unified CMBE では使用できません。
- Connection サーバまたは Connection クラスタ ペアごとに、フィルタは 1 つだけ作成できます。したがって、LDAP フィルタでは Connection ユーザと同期化するすべてのユーザを指定する必要があります。
- Connection で LDAP 同期化を設定する場合は、ユーザ検索ベースを選択することで、LDAP ユーザをさらにフィルタリングできます。
- フィルタは、RFC 2254『The String Representation of LDAP Search Filters（LDAP サーチ フィルタのストリング リプレゼンテーション）』で規定された LDAP フィルタ構文に従う必要があります。
- このフィルタ構文は検証されず、エラー メッセージも返されません。LDAP フィルタ構文を検証してから、コマンドで使用することをお勧めします。
- このコマンドを再実行して、前回のフィルタではアクセス可能だったユーザの一部を除外するフィルタを指定する場合、現在アクセスできない LDAP ユーザに関連付けられている Connection ユーザは、次にスケジュールされた 2 回の同期化または 24 時間以内のいずれか長い方の期間、スタンドアロン Connection ユーザに変換されます。このユーザは引き続き電話ユーザ インターフェイスを使用して Connection にログオンできます。発信者はその時点でもこのユーザにメッセージを残すことができ、そのメッセージは削除されません。ただし、Connection がユーザをスタンドアロン ユーザに変換している間は、そのユーザは Connection Web アプリケーションにログオンできなくなります。また、スタンドアロン ユーザになった後は、ユーザの Web アプリケーション パスワードは Connection アカウントが作成されたときに割り当てられたパスワードになります。

LDAP 認証

企業によっては、アプリケーションのシングル サインオン クレデンシャルが必要な場合があります。LDAP ディレクトリ内のユーザの資格情報に対して Connection Web アプリケーションへのログオンを認証するには、「LDAP の同期化」（P.6-1）に説明されているように、Connection ユーザ データと LDAP ディレクトリ内のユーザ データを同期化する必要があります。

Connection Web アプリケーション（管理者の Cisco Unity Connection Administration、エンド ユーザの Cisco Personal Communications Assistant）のパスワード、および Connection ボイス メッセージへのアクセスに使用される IMAP 電子メール アプリケーションのパスワードだけは、社内ディレクトリ

に対して認証されます。LDAP ディレクトリの管理アプリケーションを使用して、これらのパスワードを管理します。認証が有効な場合、パスワード フィールドは Cisco Unity Connection Administration に表示されなくなります。

電話ユーザ インターフェイスまたはボイス ユーザ インターフェイスによる Connection ボイス メッセージへのアクセスでは、引き続き Connection データベースに対して数値パスワード（PIN）で認証されます。これらのパスワードは、Connection Administration で管理するか、またはユーザが Cisco PCA で管理します。

LDAP 認証がサポートされる LDAP ディレクトリは、同期化をサポートされる LDAP ディレクトリと同じです。『*System Requirements for Cisco Unity Connection* Release 7.x』の「Requirements for an LDAP Directory Integration」の項を参照してください。

詳細については、次の各項を参照してください。

- 「LDAP 認証の設定」（P.6-7）
- 「LDAP 認証の仕組み」（P.6-7）
- 「認証と Microsoft Active Directory に関するその他の考慮事項」（P.6-8）

LDAP 認証の設定

LDAP 認証の設定は、同期化の設定よりもずっと簡単です。次の項目を指定するだけです。

- **ユーザ検索ベース。**複数の LDAP 構成を作成した場合、認証の設定時に LDAP 構成で指定したユーザ検索ベースをすべて含むユーザ検索ベースを指定する必要があります。
- **Cisco Unity Connection が検索ベースへのアクセスに使用する LDAP ディレクトリ内の管理者アカウント。**検索ベース内のすべてのユーザ オブジェクトを「読み取る」だけの最小権限を設定し、パスワードを無期限にした Connection 専用のアカウントを使用することをお勧めします（管理者アカウントのパスワードが変更されると、Connection を新しいパスワードで再構成する必要があります）。管理者アカウントには完全識別名を入力します。そのため、このアカウントは LDAP ディレクトリ ツリー内の任意の場所に属することができます。
- **1 つ以上の LDAP サーバ。**Connection が認証に使用する LDAP ディレクトリ サーバは、3 つまで指定できます。Connection は、指定された順序でサーバへの接続を試行します。どのディレクトリ サーバも応答しない場合、認証は失敗します。ホスト名ではなく IP アドレスを使用することで、Domain Name System（DNS; ドメイン ネーム システム）の可用性への依存を解消できます。

LDAP 認証の仕組み

Cisco Unity Connection で LDAP 同期化および認証が設定されると、社内 LDAP ディレクトリに対するユーザのエイリアスおよびパスワードの認証は、次のように機能します。

1. ユーザは HTTPS 経由で Cisco Personal Communications Assistant（PCA）に接続し、エイリアス（たとえば、jsmith）とパスワードを使用して認証を試みます。
2. Connection は、エイリアス jsmith の LDAP クエリを発行します。クエリの範囲として、Connection は Cisco Unity Connection Administration で LDAP 同期化を設定する際に指定した LDAP 検索ベースを使用します。SSL オプションを選択した場合は、LDAP サーバに送信される情報が暗号化されます。
3. 社内ディレクトリ サーバは、ユーザ jsmith の完全 Distinguished Name（DN; 識別名）で応答します（たとえば、「cn=jsmith, ou=Users, dc=vse, dc=lab」）。
4. Connection はこの完全 DN と、ユーザが指定した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、Connection はユーザが Cisco PCA に進むことを許可します。

Connection LDAP ディレクトリ構成で指定されたすべての LDAP サーバが使用できない場合、Connection Web アプリケーションの認証は失敗し、ユーザのアプリケーションへのアクセスは許可されません。ただし、電話およびボイス ユーザ インターフェイスの認証はその時点でも機能します。これらの PIN は、Connection データベースに対して認証されるためです。

Connection ユーザの LDAP ユーザ アカウントが無効または削除された場合、または LDAP ディレクトリ構成が Connection システムから削除された場合、次のことが発生します。

1. 最初に、Connection ユーザが Connection Web アプリケーションにログオンしようとすると、Connection は依然として LDAP ディレクトリに対して認証を試みるため、LDAP 認証が失敗します。

   複数の LDAP ユーザ検索ベースにアクセスする複数の LDAP ディレクトリ構成が存在し、構成が 1 つだけ削除された場合は、それに関連付けられたユーザ検索ベース内のユーザだけが影響を受けます。他のユーザ検索ベース内のユーザは、引き続き Connection Web アプリケーションにログオンできます。

2. 最初にスケジュールされた同期化で、ユーザは Connection 内で「LDAP 非アクティブ」としてマークされています。

   Connection Web アプリケーションにログオンしようとすると、失敗します。

3. ユーザが「LDAP 非アクティブ」としてマークされた後、24 時間以上経過してから実行される次回のスケジュールされた同期化では、アカウントが LDAP アカウントに関連付けられていたすべての Connection ユーザは、Connection スタンドアロン ユーザに変換されます。

   各 Connection ユーザの、Connection Web アプリケーションのパスワード、および Connection ボイス メッセージにアクセスするための IMAP 電子メールのパスワードは、ユーザ アカウントの作成時に Connection データベースに保存されたパスワードになります（これは通常、ユーザの作成に使用されたユーザ テンプレート内のパスワードです）。Connection ユーザはこのパスワードを知らないため、管理者はパスワードをリセットする必要があります。

   電話ユーザ インターフェイスおよびボイス ユーザ インターフェイスの数値パスワード（PIN）は、変更されないままです。

LDAP ユーザ アカウントが無効化または削除されたユーザ、または Connection から削除された LDAP ディレクトリ構成を使用して同期化されていた Connection ユーザについては、次の点に注意してください。

- Connection が LDAP 同期化ユーザからスタンドアロン ユーザに変換している間は、ユーザは引き続き電話で Connection にログオンできます。
- このユーザのメッセージは削除されません。
- 発信者はその時点でもこの Connection ユーザにメッセージを残すことができます。

認証と Microsoft Active Directory に関するその他の考慮事項

Active Directory を使用した LDAP 認証を有効にする場合は、応答時間を短縮するため、Active Directory グローバル カタログ サーバに問い合せるように Cisco Unity Connection を設定することをお勧めします。グローバル カタログ サーバへのクエリを有効にするには、Connection Administration でグローバル カタログ サーバの IP アドレスまたはホスト名を指定します。LDAP ポートには、LDAP サーバと Connection サーバ間で送信するデータの暗号化に SSL を使用しない場合は 3268、SSL を使用する場合は 3269 を指定します。

グローバル カタログ サーバを認証に使用すると、複数のドメインに属する Active Directory からユーザが同期化される場合、Connection が照会に従うことなく即座にユーザを認証できるため、さらに効率化されます。このような場合は、Connection をグローバル カタログ サーバにアクセスするように設定し、LDAP ユーザ検索ベースをルート ドメインの最上位に設定します。

1 つの LDAP ユーザ検索ベースに複数の名前空間を含めることはできません。そのため、Active Directory フォレストに複数のツリーが存在する場合は、Connection はユーザの認証に別のメカニズムを使用する必要があります。この構成では、LDAP の userPrincipalName（UPN）属性を Connection の [エイリアス] フィールドにマッピングする必要があります。UPN 属性の値は、電子メール アドレス（username@companyname.com）に似ており、フォレスト内で一意にする必要があります。

（注）　Active Directory フォレスト内に複数のツリーが存在する場合は、各ユーザの UPN サフィックス（電子メール アドレスの @ マークの後ろの部分）は、ユーザが属するツリーのルート ドメインに対応している必要があります。UPN サフィックスがツリーの名前空間と一致しない場合、Connection ユーザは Active Directory フォレスト全体に対して認証できません。ただし、別の LDAP 属性を Connection の [エイリアス] フィールドにマッピングして、LDAP 連動をフォレスト内の単一のツリーに限定できます。

たとえば、Active Directory フォレストに avvid.info と vse.lab の 2 つのツリーが存在するとします。また、各ツリーには samAccountName が jdoe であるユーザが含まれているとします。Connection は、avvid.info ツリー内の jdoe に対して、次のようにログオンの試行を認証します。

1. ユーザ jdoe が HTTPS 経由で Cisco Personal Communications Assistant（PCA）に接続し、UPN（jdoe@avvid.info）とパスワードを入力します。
2. Connection はこの UPN を使用して、Active Directory グローバル カタログ サーバに対して LDAP クエリを実行します。LDAP 検索ベースが UPN サフィックスから判断されます。この場合、エイリアスが jdoe で、LDAP 検索ベースが「dc=avvid, dc=info」です。
3. Active Directory は、このエイリアスに対応する DN を LDAP クエリで指定されたツリー内から検索します（この例では、「cn=jdoe, ou=Users, dc=avvid, dc=info」）。
4. Active Directory がこのユーザの完全 DN を使用して、LDAP を通じて Connection に応答します。
5. Connection はこの DN と、ユーザが最初に入力したパスワードを使用して、LDAP バインドを試行します。
6. LDAP バインドが成功した場合、Connection はユーザが Cisco PCA に進むことを許可します。