



ディレクトリの概要

ディレクトリは、読み取りと検索の回数が多く、書き込みと更新の回数が少ないデータ用に最適化されている専用データベースで構成されています。ディレクトリには通常、従業員情報や社内ネットワーク上のユーザ特権など、更新頻度の少ないデータが格納されています。

ディレクトリは拡張可能なため、格納する情報の種類を変更したり拡張したりできます。ディレクトリスキーマという用語は、格納する情報の種類とそれらの情報が従う規則を指します。多くのディレクトリには、異なるアプリケーションで定義される情報の種類に対応するため、ディレクトリスキーマを拡張する方法が備わっています。この機能により、企業は、ユーザ情報の中央リポジトリとしてディレクトリを使用できます。

Lightweight Directory Access Protocol (LDAP) は、ディレクトリに格納されている情報にアクセスしたり修正したり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が使用できる 1 つのリポジトリにすべてのユーザ情報を集中す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 Unified Communications Manager と Cisco Unity Connection を社内 LDAP ディレクトリと同期するための主な原則について説明します。また、社内 LDAP ディレクトリと同期させないことも可能で、そのように設定した場合の結果についても説明します。また、Cisco Unified IP Phone や Cisco IP SoftPhone などの Cisco Unified Communications 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場合の考慮事項についても説明します。

この章の構成は、次のとおりです。

- 「LDAP ディレクトリの設定チェックリスト」 (P.17-2)
- 「Cisco Unified Communications Manager Business Edition 5000 と社内 LDAP ディレクトリ」 (P.17-3)
- 「ディレクトリ アクセス」 (P.17-5)
- 「DirSync サービス」 (P.17-5)
- 「認証」 (P.17-6)
- 「Cisco Unified Communications Manager データベースの使用と社内 LDAP ディレクトリの使用」 (P.17-7)
- 「Cisco Unified Communications エンドポイントのディレクトリ アクセス」 (P.17-7)
- 「参考情報」 (P.17-8)

LDAP ディレクトリの設定チェックリスト

必要に応じて、ユーザ データをデータベースに同期化することにより、社内ディレクトリから Cisco Unified Communications Manager データベースにユーザを追加できます。Cisco Unified Communications Manager では、次のディレクトリからデータベースへの同期を実行できます。

- Microsoft Active Directory 2000
- Microsoft Active Directory 2003
- Microsoft Active Directory 2008
- Microsoft Active Directory Application Mode 2003
- Microsoft Lightweight Directory Services 2008
- iPlanet Directory Server 5.1
- Sun ONE Directory Server 5.2
- Sun ONE Directory Server 6.x
- OpenLDAP 2.3.39
- OpenLDAP 2.4



(注) Microsoft Active Directory Application Mode のサポートは、ネイティブな Active Directory 接続がサポートされたディレクトリ トポロジに制限されています。マルチフォレスト、マルチツリー シングルフォレスト、グローバル カタログなどのその他のトポロジはサポートされていません。

Cisco Unified Communications Manager は次のタイプの同期化をサポートしています。

- 自動同期化：一定の間隔でデータを同期します。
- 手動同期化：強制的に同期します。
- 同期化停止：現在の同期化を停止します。同期化が実行中の場合、停止してよいかユーザに確認します。

表 17-1 は、LDAP ディレクトリ情報を設定するための一般的な手順とガイドラインを示しています。詳細については、「参考情報」(P.17-8) を参照してください。

表 17-1 ユーザ ディレクトリの設定チェックリスト

設定ステップ		関連した手順と項目
ステップ 1	DirSync サービスをアクティブにして、お客様の社内 LDAP ディレクトリと同期されるようにします。	『Cisco Unified Serviceability Administration Guide』
ステップ 2	[LDAP システムの設定 (LDAP System Configuration)] ウィンドウを使用して、LDAP システムの設定値を設定します。	『Cisco Unified Communications Manager アドミニストレーションガイド』の「LDAP システムの設定」
ステップ 3	LDAP フィルタを使用する場合は、[LDAP フィルタ設定 (LDAP Filter Configuration)] ウィンドウにアクセスして、LDAP フィルタを作成します。	『Cisco Unified Communications Manager アドミニストレーションガイド』の「LDAP カスタム フィルタの設定」
ステップ 4	[LDAP ディレクトリ (LDAP Directory)] ウィンドウを使用して、LDAP ディレクトリの設定値を設定します。	『Cisco Unified Communications Manager アドミニストレーションガイド』の「LDAP ディレクトリの設定」

表 17-1 ユーザ ディレクトリの設定チェックリスト (続き)

設定ステップ	関連した手順と項目
ステップ 5 [LDAP 認証 (LDAP Authentication)] ウィンドウを使用して、LDAP 認証の設定値を設定します。	「認証」 (P.17-6) 『Cisco Unified Communications Manager アドミニストレーションガイド』の「LDAP 認証の設定」
ステップ 6 LDAP ユーザを Cisco Unified Communications Manager と同期したら、Cisco Unity Connection の管理でユーザを手動で作成する必要があります。ユーザを手動で作成するには、次のいずれかのタスクを実行します。 <ul style="list-style-type: none"> 『User Moves, Adds, and Changes Guide for Cisco Unity Connection』の手順に従って Cisco Unity Connection の管理を設定し、ユーザを Cisco Unity Connection にインポートします。 『Cisco Unified Communications Manager アドミニストレーションガイド』の Cisco Unity Connection ボイスメールボックスの作成の手順に従って、Cisco Unified Communications Manager の管理ページで [ユーザ管理 (User Management)] > [エンドユーザ (End User)] の順に選択し、Cisco Unity Connection メールボックスを作成します。 	『User Moves, Adds, and Changes Guide for Cisco Unity Connection』 『Cisco Unified Communications Manager アドミニストレーションガイド』の Cisco Unity Connection ボイスメールボックスの作成

Cisco Unified Communications Manager Business Edition 5000 と社内 LDAP ディレクトリ

Cisco Unity Connection ディレクトリは Cisco Unified Communications Manager から取得されます。つまり、Cisco Unity Connection の同期ディレクトリ内のコンポーネントは、Cisco Unified Communications Manager から Cisco Unity Connection へ更新されます。

LDAP 同期化を有効にして Cisco Unified サービスアビリティで DirSync サービスをアクティブ化すると、Cisco Unified Communications Manager の DirSync サービスが、Cisco Unified Communications Manager および Cisco Unity Connection の社内ディレクトリのデータを Cisco Unified Communications Manager データベースに合わせて同期します。LDAP 同期化を使用すると、Cisco Unity Connection は LDAP からのユーザ情報を把握しません。Cisco Unity Connection はユーザを Cisco Unified Communications Manager ユーザと見なします。

LDAP ユーザを Cisco Unified Communications Manager と同期したら、Cisco Unity Connection の管理でユーザを手動で作成する必要があります。ユーザを手動で作成するには、次のいずれかのタスクを実行します。

- 『User Moves, Adds, and Changes Guide for Cisco Unity Connection』の手順に従って Cisco Unity Connection の管理を設定し、ユーザを Cisco Unity Connection にインポートします。
- 「Cisco Unity Connection ボイスメールボックスの作成」 (P.88-9) の手順に従って、Cisco Unified Communications Manager の管理ページで [ユーザ管理 (User Management)] > [エンドユーザ (End User)] の順に選択し、Cisco Unity Connection メールボックスを作成します。



ヒント

Cisco Unified Communications Manager の管理ページで LDAP 同期化を有効にすると、Cisco Unity Connection の管理から Web パスワードを変更できません。

LDAP 同期化が有効になっていない場合、Cisco Unity Connection の管理ではエンド ユーザを削除できません。この場合、LDAP ディレクトリでユーザを削除した後に、Cisco DirSync サービスによって Cisco Unified Communications Manager の管理でユーザが削除されます。Cisco DirSync サービスによって Cisco Unified Communications Manager のユーザが削除された場合は、『*User Moves, Adds, and Changes Guide for Cisco Unity Connection*』に従って、Cisco Unity Connection でユーザを手動で削除する必要があります。Cisco Unity Connection の管理でユーザを削除しないと、Cisco Unity Connection によってユーザが孤立したユーザとして分類されます。

Cisco Unified Communications Manager の管理ページの [エンドユーザの設定 (End User Configuration)] ウィンドウ ([ユーザ管理 (User Management)] > [エンドユーザ (End User)]) から、エンドユーザに関するディレクトリ情報にアクセスできます。LDAP 同期化を有効にしない場合は、このウィンドウを使用して、ユーザ ID、パスワード、デバイス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。LDAP 同期化を有効にした場合、[エンドユーザの設定 (End User Configuration)] ウィンドウでは、エンドユーザの追加、削除、および既存のユーザ情報 (ユーザ ID など) の変更を行うことはできません。

データベースを使用するアプリケーションとサービス

次の Cisco Unified Communications Manager Business Edition 5000 アプリケーションとサービスは、ユーザ情報やその他の種類の情報にデータベースを使用します。

- Cisco Unity Connection
- 一括管理ツール (BAT)
- Cisco Unified Communications Manager Auto-Register Phone Tool
- AXL
- Cisco エクステンション モビリティ
- Cisco Unified CM のユーザ オプション
- Cisco Conference Connection
- CTIManager
- Cisco Unified Communications Manager CDR Analysis and Reporting
- Cisco Unified Communications Manager Assistant
- Cisco Customer Response Solutions (CRS)
- Cisco Emergency Responder (CER)
- Cisco Unified IP Phone サービス
- 個人アドレス帳 (PAB)
- FastDials
- Cisco WebDialer
- Cisco IP Communicator

ディレクトリ アクセス

次の定義は、この章全体に適用されます。

- ディレクトリ アクセスとは、Cisco Unified IP Phone や Cisco IP SoftPhone などの Cisco Unified Communications 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ある。

図 17-1 Cisco Unified Communications エンドポイントのディレクトリ アクセス

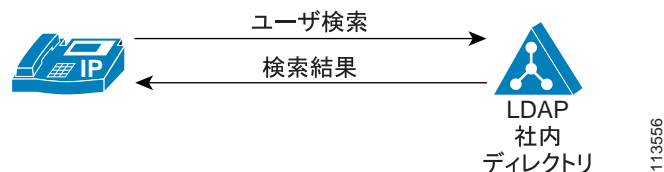


図 17-1 は、この章で定義されているディレクトリ アクセスを示しています。この例では、Cisco Unified IP Phone がアクセスしています。クライアントアプリケーションは、LDAP ディレクトリ（企業の社内ディレクトリなど）に対してユーザ検索を実行し、一致するいくつかのエントリを受信します。Cisco Unified IP Phone ユーザはこの中から 1 つのエントリを選択し、そのエントリを使用して対応する人物に Cisco Unified IP Phone からダイヤルできます。



(注)

ここで定義されているディレクトリ アクセスには、ディレクトリ上の読み取り操作だけが含まれ、ディレクトリスキーマの拡張やその他の設定変更は必要ありません。

DirSync サービス

Cisco Unity Connection ディレクトリは Cisco Unified Communications Manager から取得されます。つまり、Cisco Unity Connection の同期ディレクトリ内のコンポーネントは、Cisco Unified Communications Manager から Cisco Unity Connection へ更新されます。LDAP 同期化を有効にして Cisco Unified サービスアビリティで DirSync サービスをアクティブ化すると、Cisco Unified Communications Manager の DirSync サービスが、Cisco Unified Communications Manager および Cisco Unity Connection の社内ディレクトリのデータを Cisco Unified Communications Manager データベースに合わせて同期します。

Cisco Unified サービスアビリティで DirSync サービスをアクティブにした後は、Cisco Unified Communications Manager の管理ページの次のウィンドウで、LDAP 関連の情報を設定してください。

- [LDAP システムの設定 (LDAP System Configuration)] ([システム (System)] > [LDAP システム (LDAP System)])
- [LDAP ディレクトリの検索と一覧表示 (Find and List LDAP Directories)] ([システム (System)] > [LDAP] > [LDAP ディレクトリ (LDAP Directory)])

DirSync を使用すると、社内ディレクトリのデータを Cisco Unified Communications Manager に同期できます。同期がサポートされているディレクトリの詳細については、「[LDAP ディレクトリの設定 チェックリスト](#)」(P.17-2) を参照してください。



(注) 社内ディレクトリ内にユーザを設定するときは、ユーザの姓を必ず設定してください。Cisco Unified Communications Manager の管理ページで LDAP 同期化を設定すると、社内ディレクトリ内に姓がないユーザは Cisco Unified Communications Manager データベースと同期されなくなります。Cisco Unified Communications Manager の管理ページにはエラーが表示されませんが、同期されなかったユーザはログ ファイルで示されます。



(注) Microsoft Active Directory で起動された DirSync は、データの完全な（すべての）同期化を行います。

DirSync には、次の Cisco Unified CM ユーザ オプションがあります。

- 自動同期化：一定の間隔でデータを同期します。
- 手動同期化：強制的に同期します。
- 同期化停止：現在の同期化を停止します。同期化が実行中の場合、停止してよいかユーザに確認します。



(注) ディレクトリの同期が有効になっている場合、Cisco Unified Communications Manager の管理ページでは、お客様の社内ディレクトリから同期されているユーザ情報を更新することはできません。

DirSync サービス パラメータ

DirSync サービスのサービス パラメータを設定できます。Cisco Unified Communications Manager の管理ページで、[システム]>[サービスパラメータ]を選択します。表示されるウィンドウで、[サーバ (Server)] ドロップダウン リスト ボックスからサーバを選択します。[サービス (Service)] ドロップダウン リスト ボックスで Cisco DirSync サービスを選択します。[サービスパラメータ設定 (Service Parameter Configuration)] ウィンドウで、DirSync サービス パラメータを設定できます。



(注) DirSync サービスをアクティブにする方法の詳細については、『Cisco Unified Serviceability Administration Guide』を参照してください。

認証

認証プロセスでは、ユーザにシステムへのアクセス権を付与する前に、ユーザ ID とパスワード/PIN を検証することにより、ユーザの身元を確認します。この検証は、Cisco Unified Communications Manager データベースまたは LDAP 社内ディレクトリとの照合によって行われます。

LDAP 同期化を有効にする場合、設定できるのは LDAP 認証だけです。

同期化と LDAP 認証が両方とも有効になっている場合、システムは常にアプリケーション ユーザとエンドユーザの PIN を Cisco Unified Communications Manager データベースに照合して認証します。エンドユーザのパスワードは社内ディレクトリとの照合によって認証されるため、エンドユーザは社内ディレクトリ パスワードを使用する必要があります。

同期化だけが有効になっている (LDAP 認証は有効になっていない) 場合、エンドユーザは Cisco Unified Communications Manager データベースとの照合によって認証されます。この場合、管理者は、Cisco Unified Communications Manager の管理ページの [エンドユーザの設定 (End User Configuration)] ウィンドウでパスワードを設定できます。

Cisco Unified Communications Manager データベースの使用と社内 LDAP ディレクトリの使用

ディレクトリ情報を使用するには、次の 2 つの Cisco Unified CM ユーザ オプションがあります。

- ユーザに Cisco Unified Communications Manager データベースを使用する場合、[エンドユーザの設定 (End User Configuration)] ウィンドウでユーザを作成し、データベース (パスワード、名前、デバイスの関連付けなど) に追加します。認証は、Cisco Unified Communications Manager の管理ページで設定されている情報との照合によって行われます。この方式を使用している場合は、エンドユーザと管理者はパスワードを変更できます。この方式では、LDAP 同期化は行われません。

Cisco Unity Connection ディレクトリは Cisco Unified Communications Manager から取得されます。つまり、Cisco Unity Connection の同期ディレクトリ内のコンポーネントは、Cisco Unified Communications Manager から Cisco Unity Connection へ更新されます。

- 社内 LDAP ディレクトリを使用するには、次の手順を実行する必要があります。
 - ユーザが LDAP 社内ディレクトリ パスワードを使用するために、LDAP 認証を設定する必要があります ([システム] > [LDAP] > [LDAP 認証 (LDAP Authentication)])。
 - まず LDAP 同期化を設定しないと、LDAP 認証を設定できません。そのように設定すると、Cisco Unified Communications Manager の管理ページで以後のエンドユーザの設定が阻止されます。
 - LDAP ユーザを Cisco Unified Communications Manager と同期化したら、Cisco Unity Connection のユーザを手動で作成する必要があります。この作業の実行方法については、「[Cisco Unified Communications Manager Business Edition 5000 と社内 LDAP ディレクトリ \(P.17-3\)](#)」を参照してください。



ヒント 認証の設定は Cisco Unified CM ユーザ オプションであることに注意してください。認証が有効になっていない場合、管理者とエンドユーザは、社内ディレクトリのパスワードと、Cisco Unified Communications Manager パスワードの 2 つのパスワードを持ちます。

Cisco Unified Communications 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 Unified Communications Manager やその他の Cisco Unified Communications アプリケーションが社内ディレクトリと同期しているかどうかに関係なく適用されます。同期しているかどうかの違いは、アプリケーションがユーザ情報を格納する方法と、その情報がネットワーク全体で一貫性を保持される方法に影響するだけなので、どちらの場合もエンドユーザには同じに見えます。

次の項では、XML 対応の電話機 (Cisco Unified IP Phone 7940 や 7960 など) による 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説明します。



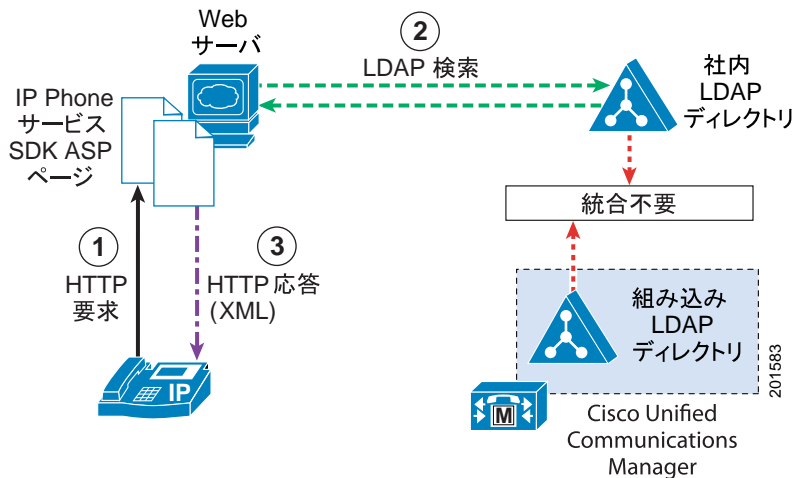
(注) Cisco IP SoftPhone リリース 1.2 以降には、Cisco IP Communicator と同様、LDAP ディレクトリへのアクセスと検索を行うメカニズムが組み込まれています。この機能の設定方法の詳細については、製品マニュアルを参照してください。

Cisco Unified IP Phone のディレクトリ アクセス

XML 対応の Cisco Unified IP Phone (モデル 7940 や 7960 など) では、電話機のディレクトリ ボタンを押すと、社内 LDAP ディレクトリの検索ができます。この 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 サーバはプロキシとして動作し、電話機から要求を受信してその要求を LDAP 要求に変換し、それから社内ディレクトリ サーバに送信します。応答は、適切な XML オブジェクトにカプセル化された後、解釈されて電話機に戻されます。

図 17-2 は、Cisco Unified Communications Manager が社内ディレクトリと同期化されていない環境における、このメカニズムを示しています。このシナリオでは、Cisco Unified Communications Manager はメッセージ交換にかかわっていません。

図 17-2 ディレクトリの同期化が行われない Cisco Unified IP Phone 社内ディレクトリ アクセスのメッセージ交換



Web サーバから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 Unified IP Phone Services Software Development Kit (SDK) バージョン 2.0 以降を使用します。

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

- システムはすべての LDAPv3 対応ディレクトリをサポートしている。
- Cisco Unified Communications Manager ユーザ プリファレンス (スピードダイヤル、すべてのコールの転送、個人アドレス帳) は、社内 LDAP ディレクトリとは同期化されない。したがって、ユーザは Cisco Unified CM のユーザ オプション ウィンドウにアクセスするための別のログイン名とパスワードを持ちます。

参考情報

関連項目

- 「LDAP ディレクトリの設定チェックリスト」 (P.17-2)
- 「Cisco Unified Communications Manager Business Edition 5000 と社内 LDAP ディレクトリ」 (P.17-3)

- 「ディレクトリ アクセス」 (P.17-5)
- 「DirSync サービス」 (P.17-5)
- 「認証」 (P.17-6)
- 「Cisco Unified Communications Manager データベースの使用と社内 LDAP ディレクトリの使用」 (P.17-7)
- 「Cisco Unified Communications エンドポイントのディレクトリ アクセス」 (P.17-7)
- 『Cisco Unified Communications Manager アドミニストレーションガイド』の「LDAP システムの設定」
- 『Cisco Unified Communications Manager アドミニストレーションガイド』の「LDAP ディレクトリの設定」
- 『Cisco Unified Communications Manager アドミニストレーションガイド』の「LDAP 認証の設定」
- 『Cisco Unified Serviceability Administration Guide』
- 「参考情報」 (P.5-20)
- 「アプリケーション ユーザとエンド ユーザ」 (P.18-1)
- 「クレデンシャル ポリシー」 (P.19-1)
- 『Cisco Unified Communications Manager アドミニストレーションガイド』の「アプリケーション ユーザの設定」
- 『Cisco Unified Communications Manager アドミニストレーションガイド』の「エンド ユーザの設定」

参考資料

- 『Installing Cisco Unified Communications Manager Release 8.5(1)』
- 『Cisco Unified Communications Solution Reference Network Design (SRND)』
- 『User Moves, Adds, and Changes Guide for Cisco Unity Connection』

