モバイル コラボレーション

改訂日：2018 年 3 月 1 日

モバイル コラボレーション ソリューションおよびアプリケーションを使用すれば、モバイル ワーカーはどこからでも会社の IP コミュニケーション環境の機能を利用できます。モバイル コラボレーション ソリューションを使用すると、モバイル ユーザは業務上の電話をさまざまなデバイスで扱うことができ、オフィスビル内の移動中やオフィス間の移動中、地理的に会社外のロケーション間の移動中に企業アプリケーションにアクセスできます。モバイル コラボレーション ソリューションでは、モバイル ワーカーは持続的に到達可能性を得ることができ、さまざまな場所での移動中や作業中の生産性を向上させることができます。

モバイル コラボレーション ソリューションは、主に次の 2 つのカテゴリに分けられます。

- 社内型モビリティ

  このタイプのモビリティは、企業の敷地内での移動に限られます。

- 社外型モビリティ

  このタイプのモビリティは、企業インフラストラクチャの外部にまで至るモビリティを指し、一般には何らかの形のインターネット、モバイル ボイス ネットワーク、およびモバイル データ ネットワーク通過が含まれます。

社内型モビリティは、企業のネットワーク境界内に使用が制限されます。この境界は単一の物理的な建物のみを範囲としても、近くの、あるいは離れた複数の物理的な建物を範囲としても、またはホーム オフィスまで広がったネットワーク インフラストラクチャの場合、企業により制御され管理されるホーム オフィスを範囲としてもかまいません。

一方、社外型モビリティには、企業インフラストラクチャによるインターネットまたはモバイル プロバイダー インフラストラクチャへのブリッジングが含まれ、ユーザは公共およびプライベート ネットワークを使用して企業サービスに接続できます。これらの 2 つのタイプのモビリティ間の線引きはあいまいな場合もあり、特にモバイル デバイスが、インターネットまたはモバイル データおよびモバイル音声ネットワークを介したコラボレーション サービスで企業に接続するようなシナリオの場合に顕著です。

社内型モビリティは、フィーチャ セットおよびソリューションに基づき、次の 3 つの主要な領域に分けられます。

- キャンパス/単一サイト モビリティ

  このタイプの企業モビリティでは、ユーザは、一般に単一の IP アドレス空間および PSTN 入出力境界により区切られた単一の物理的な場所内を動き回ります。このタイプのモビリティには、1 つの物理ネットワーク ポートから他のポートへの電話の移動や、無線インフラストラクチャ アクセス ポイント間でのワイヤレス LAN デバイスのローミング、ユーザが一時的に異なる領域への特定の電話機に企業電話番号などのデバイス プロファイルを適用する Cisco エクステンション モビリティ（EM）などの操作や機能が含まれます。

- マルチサイト モビリティ

  このタイプのモビリティでは、ユーザは社内の物理的な場所の間を移動します。この移動には、一般的に IP アドレス空間や PSTN 入出力境界を越えることも含まれます。このタイプのモビリティには、キャンパス モビリティと同じタイプの操作や機能（物理的なハードウェアの移動、WLAN ローミング、Cisco エクステンション モビリティ）が含まれますが、それらは企業内のそれぞれのサイトに複製されます。さらに、デバイス モビリティ機能を利用して、ユーザがサイト間でデバイスを移動させると、電話のコールがローカル サイトのイーグレス ゲートウェイを介してルーティングされ、メディア コーデックが適切にネゴシエートされ、コール アドミッション制御メカニズムでデバイスの場所が認識されるようにできます。

- リモート サイト モビリティ

  このタイプのモビリティでは、ユーザは社外のロケーションに移動しても、仮想的に企業ネットワークをリモート ロケーションまで拡張して、何らかの安全な形式で会社に接続できます。このタイプのモビリティには、VPN ベースのリモート企業接続または VPN なしのリモート企業接続が含まれます。VPN リモート企業接続は、Cisco Virtual Office などのリモート テレワーカー ソリューションや、VPN 対応電話機、クライアント、Office Extend Access Point 機能などのその他のリモート接続方法が含まれます。VPN なしのリモート企業接続は、リバース プロキシ ファイアウォール セッション ベースの接続を有効にし、VPN トンネルを必要とせずにリモート エンドポイントとクライアントが企業に接続できるようにします。VPN なしのリモート接続は、Cisco Expressway モバイル & リモート アクセス機能によりサポートされます。

- クラウドおよびハイブリッド サービス モビリティ

  このモビリティ タイプには、クラウド コラボレーション サービスや、クラウドおよびオンプレミス コラボレーション サービスの統合などがあります。これにはクラウドからのサービスの提供が関係するため、これらのサービスを利用するのに、インターネットに接続可能などのデバイスでも使用できます。ユーザが社内外のいずれにいるかどうか、企業ネットワークまたは別のネットワークに接続しているかどうか、移動中であるかどうかなどに関係なく、ユーザはこれらのクラウド サービスを利用できます。

社外型モビリティは、大まかに次の 2 つの Cisco ソリューション セットに分けられます。

- Cisco Unified Mobility

  Cisco Unified Communications Manager（Unified CM）の一部である Cisco Unified Mobility 機能スイートにより、モバイル ユーザのエンタープライズ番号をユーザのモバイルまたはリモート デバイスに関連付け、エンタープライズ ネットワーク上のユーザの固定の会社のデスクフォンと、モバイル ボイス プロバイダー ネットワーク上のユーザのモバイル デバイスとを接続できます。このタイプの機能は、固定モバイル コンバージェンスと呼ばれることがあります。

- Cisco Mobile クライアント ソリューション

  Cisco Mobile クライアント アプリケーションは、デュアル モード スマート フォンおよび他のモバイル デバイスで実行され、企業のコラボレーション アプリケーションとサービスへのアクセスを提供します。デュアルモード電話には、802.11 ワイヤレス LAN ネットワークと携帯電話音声およびデータ ネットワークの両方に接続できる二重無線アンテナが装備されています。モバイル デバイスに配置された Cisco Mobile クライアントにより、モバイル デバイスは、エンタープライズ ワイヤレス LAN 経由またはパブリックまたはプライベートの Wi-Fi ホット スポットまたはモバイル データ ネットワークを介してインターネット経由で Cisco Unified CM に登録し、次いで IP を介した音声コールとビデオ コールの送受信用のエンタープライズ IP テレフォニー インフラストラクチャを利用できます。デュアル モード電話では、モバイル ユーザが企業の WLAN に関連付けされていない場合、またはこれらのデバイスでエンタープライズ ネットワークに安全に接続されていない場合、電話のコールはモバイル音声プロバイダー ネットワークを使用して行われます。モバイル デバイスの音声サービスとビデオ サービスを有効にするだけでなく、Cisco Mobile クライアントでは、音声とインスタント メッセージング、プレゼンス、エンタープライズ ディレクトリへのアクセスなどの他のコラボレーション サービスへもアクセスできます。

特に断りがない限り、この章で説明するさまざまなアプリケーションと機能は、すべての Cisco Unified Communications 配置モデルに適用されます。

この章ではまず、モビリティ機能と企業インフラストラクチャ内で利用可能なソリューションについて説明します。これには、キャンパス/単一サイトの配置、マルチサイトの配置、さらにはリモート サイトの配置での、機能検証や設計上の考慮事項が含まれます。この一連の包括ソリューションは、企業クラスのコミュニケーションや物理ロケーションに関係しない生産性の改善などを含め、社内のモバイル ワーカーに多くの利点をもたらします。この社内型モビリティに関する説明を踏まえて、モバイル プロバイダーおよびインターネット プロバイダーのインフラストラクチャおよび機能を活用した、社外型モビリティ ソリューションを検証します。これらのソリューションにより、安定した企業モビリティ インフラストラクチャの上に構築できる高度なモバイル機能とコミュニケーション フローを活用するための企業ネットワーク インフラストラクチャとプロバイダー ネットワーク インフラストラクチャのモバイル機能のブリッジングが可能になります。

この章では、企業のコラボレーション モビリティ ソリューションのモビリティ アーキテクチャ、機能性、および設計と配置の示す意味について包括的に検証します。この章の分析と説明は、大まかに次のような構成になっています。

- 社内型モビリティ
  - キャンパス企業モビリティ（21-4 ページ）
  - マルチサイト企業モビリティ（21-12 ページ）
  - リモート企業モビリティ（21-27 ページ）
  - クラウド サービスとハイブリッド サービスのモビリティ（21-36 ページ）
- 社外型モビリティ
  - Cisco Unified Mobility（21-51 ページ）
  - シスコのモバイル クライアントおよびデバイス（21-81 ページ）

この章の変更点

表 21-1 に、この章に新しく追加されたトピック、またはこのマニュアルの以前のリリースから大幅に改訂されたトピックの一覧を示します。

表 21-1　新規情報、またはこのマニュアルの以前のリリースからの変更情報

新規トピックまたは改訂されたトピック	説明箇所	改訂日
Cisco Jabber 対応の Apple プッシュ通知サービス（APNs）	Cisco Jabber for iPhone and iPad 対応の Apple プッシュ通知サービス（APNs）（21-108 ページ）	2018 年 3 月 1 日
Cisco Jabber でのリフレッシュ トークンを使用した OAuth 2.0	Cisco Jabber とリフレッシュ トークンを使用した OAuth でのログイン フロー（21-109 ページ）	2018 年 3 月 1 日

社内型モビリティ

この項では、社内で使用可能なモビリティ機能およびソリューションについて検証します。この検証には、次のタイプの企業モビリティのアーキテクチャ、機能性、および設計と配置の意味に関する説明が含まれます。

- キャンパス企業モビリティ（21-4 ページ）
- マルチサイト企業モビリティ（21-12 ページ）
- リモート企業モビリティ（21-27 ページ）
- クラウド サービスとハイブリッド サービスのモビリティ（21-36 ページ）

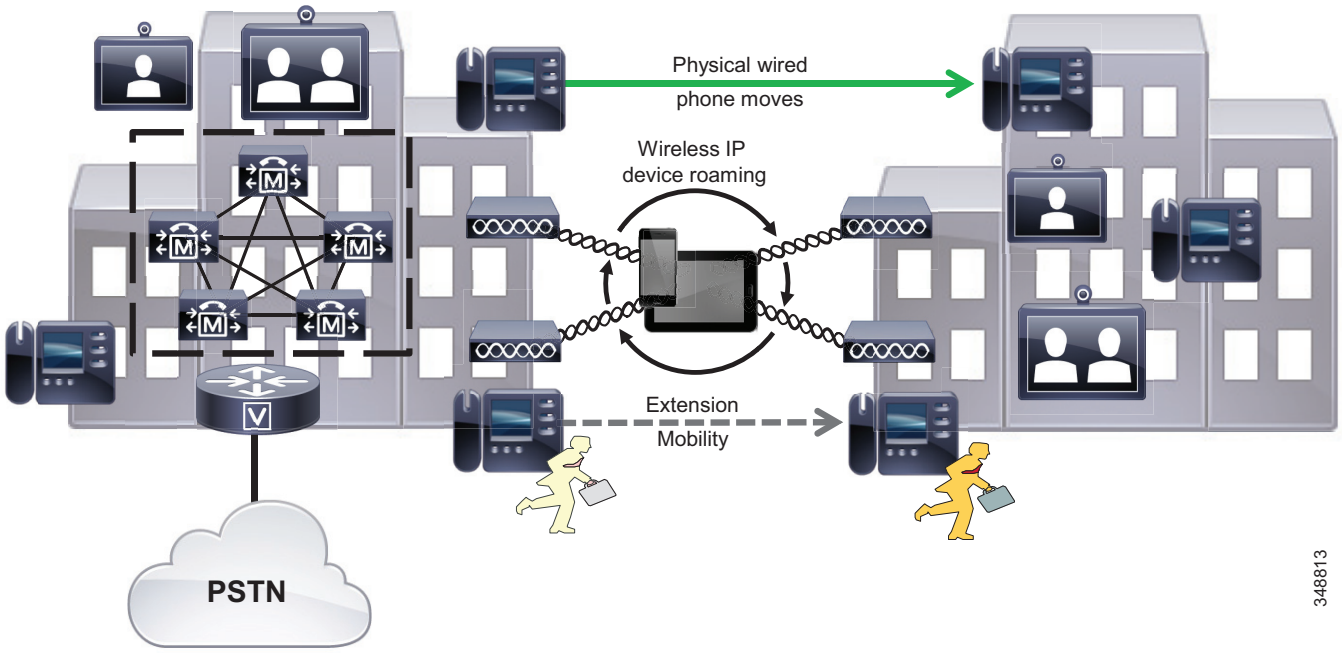
キャンパス企業モビリティ

キャンパスまたは単一サイトの企業モビリティは、一般に単一の IP アドレス空間および PSTN 入出力境界により区切られた単一の物理的な場所内のモビリティを指します。ここでのモビリティには、この物理ロケーション内でのユーザの移動だけではなく、エンドポイント デバイスの移動も含まれます。

キャンパス企業モビリティのアーキテクチャ

図 21-1 に示すように、キャンパス企業モビリティのアーキテクチャは、（図のように）近接する単一の建物または複数の建物を含む単一の物理的な場所に基づいており、ユーザはキャンパス内を自由に移動でき、IP および PSTN 接続を維持できます。一般にキャンパス配置には、単一 IP アドレス空間および PSTN 入出力境界によって区切られた PSTN およびインターネット プロバイダー ネットワークへの、共有一般接続または接続セットが含まれます。この企業キャンパス内のすべてのユーザは、一般ネットワーク インフラストラクチャに接続され、一般ネットワーク インフラストラクチャから到達可能です。

図 21-1　　キャンパス企業モビリティのアーキテクチャ



キャンパス モビリティのタイプ

企業キャンパス内のモビリティには一般的に、デバイス、ユーザ、またはその両方のキャンパス インフラストラクチャ全体の移動が含まれます。シスコ コラボレーション展開内のキャンパス企業モビリティは主に、有線電話機の物理的な移動、ワイヤレス デバイスの移動、電話機や通話ソフトウェアを持たないユーザの移動の 3 つに分けられます。移動のタイプについては後で説明します。

物理的な有線デバイスの移動

図 21-1 に示すように、物理的な有線電話機の移動は、キャンパス インフラストラクチャ内で簡単に行えます。このタイプの電話機の移動は、建物の単一階内、建物の複数階にわたって、またはキャンパス内の建物間で発生することが考えられます。従来の、物理的な電話機のポートが特定のオフィス、パーティション、または建物内のその他の空間に固定されている PBX 配置とは異なり、IP テレフォニーの配置では、電話はネットワーク インフラストラクチャの任意の IP ポートにつないで IP PBX に接続できます。

Cisco 環境では、これは単に Cisco Unified IP Phone または Cisco TelePresence System エンドポイントをネットワークから取り外し、キャンパス内の他の場所に運んで他の有線ネットワーク ポートに接続するだけのことです。新しいネットワーク ロケーションに接続すると、この電話が Unified CM に再登録され、前のロケーションと同じように発信や着信ができます。

物理デバイスのこれと同じ移動は、有線 PC で実行するソフトウェアベースの電話にも適用されます。たとえば、Cisco IP Communicator または Cisco Jabber を実行しているラップトップ コンピュータを、キャンパス内のあるロケーションから別のロケーションへ移動でき、ラップトップを新しいロケーションのネットワーク ポートに接続すると、ソフトウェアベースの電話を Cisco Call Control に再登録して、電話の呼処理を再開できます。

キャンパス内の物理的なデバイス モビリティに対応するには、電話デバイスやソフトウェアベースの電話を実行しているコンピュータを物理的に移動する際は、新しいロケーションで使用されるネットワーク接続の IP 接続、接続速度、Quality of Service、セキュリティ、およびインライン パワーや動的ホスト制御プロトコル（DHCP）などのネットワーク サービスが前の場所のものと同じであるよう注意してください。これらの接続パラメータ、サービス、および機能が同じでないと、機能が低下し、場合によっては、機能が完全に失われます。

ワイヤレス デバイス ローミング

キャンパス エッジで無線ネットワークに接続できるよう無線 LAN ネットワークが配置されている場合、ワイヤレス デバイスは、図 21-1 で示すように、企業キャンパス全体を移動またはローミングできます。

ワイヤレス デバイスの例には、Cisco Unified Wireless IP Phone 7925G および 8821 などのワイヤレス デバイス、無線で接続した Cisco DX80、および Cisco Jabber などの Cisco Mobile クライアントなどが含まれます（シスコのモバイル クライアントおよびデバイス（21-81 ページ）を参照）。

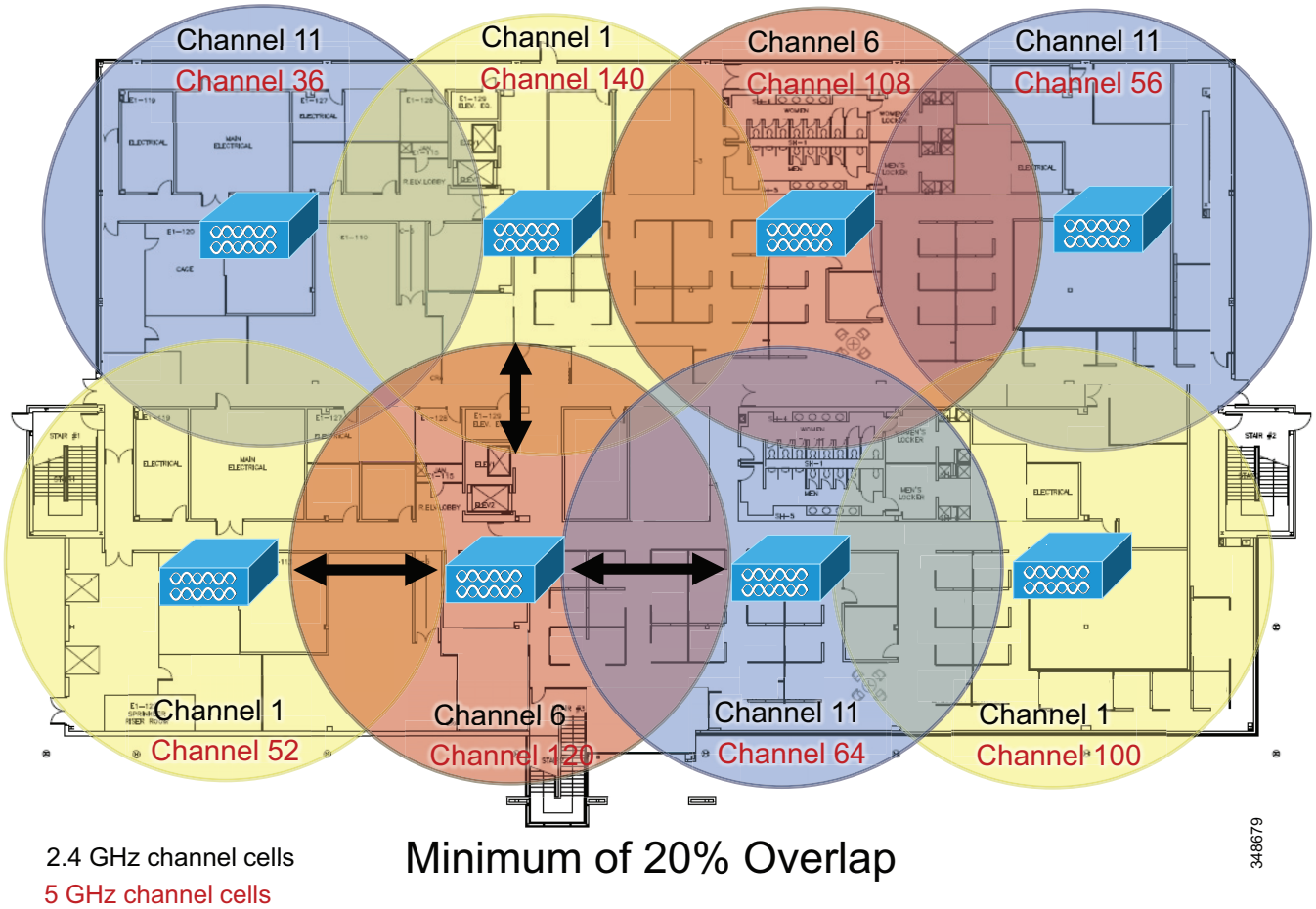
WLAN ネットワークは、1 箇所以上のワイヤレス アクセス ポイント（AP）から構成されます。ワイヤレス AP は、ワイヤレス デバイスに対してワイヤレス ネットワーク接続を提供します。ワイヤレス AP は、ワイヤレス ネットワークと有線ネットワークとの間の境界ポイントとなります。ネットワークのカバー領域および容量を拡張するために、物理的なネットワーク敷設領域に複数の AP が分散して配置されます。

ワイヤレス デバイスおよびワイヤレス クライアントは、基礎となる WLAN インフラストラクチャに依存して重要なシグナリングとリアルタイムの音声とビデオのメディア トラフィックの両方を伝送するため、データ トラフィックとリアルタイム音声トラフィックの両方に最適化された WLAN ネットワークの配置が必要になります。WLAN ネットワークの配置が適切でないと、多くの干渉が発生し、容量が低下するため、音声とビデオの品質が低下するだけでなく、コールがドロップされたり、つながらなかったりする可能性もあります。このように配置された WLAN は、音声コールの発信および受信に使用できなくなります。したがって、ワイヤレス フォンとクライアントを配置する場合は、Voice and Video over WLAN（VVoWLAN）の配置が正常に行われるように、配置前、配置中、配置後に WLAN 無線周波数（RF）事前現地調査を実施して、適切なセル境界、設定、機能設定、容量、および冗長性を判断する必要があります。

AP は、ネットワーク内に自律的に配置して、各 AP が他のすべての AP とは独立して設定、管理、および運用されるようにすることも、WLAN コントローラによってすべての AP が設定、管理、および制御されるように管理モードで配置することもできます。後者のモードでは、WLAN コントローラは、AP の管理、および AP 設定と AP 間ローミングの処理を担当します。いずれの場合も、VVoWLAN を正常に配置するには、次の一般的なガイドラインに従って AP を配置する必要があります。

- 図 21-2 に示すように、隣接していない WLAN AP チャネル セルは、20 % 以上オーバーラップする必要があります。このようにオーバーラップさせることによって、ワイヤレス デバイスがキャンパス ロケーション内で移動した場合に AP 間で正常にローミングして、ボイス ネットワーク接続およびデータ ネットワーク接続を維持できます。2 つの AP 間で正常にローミングしたデバイスは、音声品質や音声パスに目立った変更なしにアクティブな音声コールを維持できます。

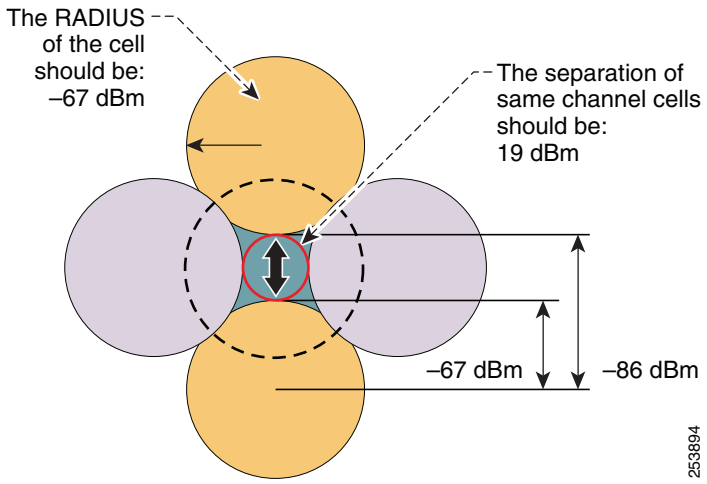
図 21-2　　WLAN チャネル セル オーバーラップ



- 図 21-3 に示すように、WLAN AP チャネル セルは、-67 デシベル/ミリワット（dBm）のセル パワーレベル境界（またはチャネル セル半径）で配置する必要があります。また、同一チャネルのセル境界の分離は、約 19 dBm にする必要があります。

  約 -67 dBm（またはそれ未満）のセル半径にすることで、リアルタイムの音声とビデオのトラフィックで問題となるパケット損失を最小限に抑えることができます。19 dBm の同一チャネル セル分離は、AP またはクライアントにおいて、同じチャネルに関連付けられている他のデバイスとの同一チャネル干渉が発生しないようにするために重要です。同一チャネル干渉が発生すると、音声品質が低下するためです。セル半径についての -67 dBm のガイドラインは、2.4 GHz（802.11b/g/n）と 5 GHz（802.11a/n/ac）の両方の配置に該当します。

図 21-3　　WLAN セル半径および同一チャネル セル分離



(注)　19 dBm の同一チャネル セル分離は、単純化されたものであり、理想的な状態を示しています。ほとんどの配置においては、このような 19 dBm の分離を実現することができません。最も重要な RF 設計基準は、-67 dBm のセル半径と、セル間の 20 % 以上の推奨オーバーラップです。これらの制約を遵守して設計することによって、チャネルの分離が最適化されます。

無線ローミングは無線電話だけではなく、PC で実行するソフトウェアベースの電話にも適用されます。たとえば、ユーザは Cisco IP Communicator または Cisco Jabber を実行しているラップトップ コンピュータを使用して、キャンパス中を無線でローミングできます。

ほとんどのワイヤレス AP、無線電話、およびワイヤレス PC クライアントでは、企業の WLAN に安全にアクセスできるように、さまざまなセキュリティ オプションが用意されていますWLAN インフラストラクチャとワイヤレスデバイスの両方でサポートされており、企業のセキュリティ ポリシーおよびセキュリティ要件に一致するセキュリティの方法を必ず選択してください。

Cisco Unified Wireless Network のインフラストラクチャの詳細については、ワイヤレス LAN インフラストラクチャ (3-66 ページ)を参照してください。WLAN 経由の音声およびビデオなど WLAN 設計上のリアルタイム トラフィックの詳細については、次の Web サイトから入手可能な『*Real-Time Traffic over Wireless LAN Solution Reference Network Design Guide*』を参照してください

https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Mobility/RToWLAN/CCVP_BK_R7805F20_00_rtowlan-srnd.html

エクステンション モビリティ (EM)

図 21-1 に示すように、有線およびワイヤレス電話機の物理的な移動に加え、ユーザ自身も電話機または PC ハードウェアを持たずにキャンパス インフラストラクチャ内を移動できます。これらの場合、ユーザの会社の電話番号および他の設定を含むプロファイルを適用することにより、ユーザは 1 つのデバイスから別のデバイスに、会社の内線番号または会社の番号を移動できます。

EM 機能により、ユーザはセキュリティ クレデンシャル (ユーザ ID および PIN 番号) のセットを使用して、キャンパス内にある IP フォンにログインできます。ログインすると、会社の電話番号やコール特権から、設定したスピード ダイヤルまでを含めたユーザ個人のデバイス プロファイルが、ユーザがデバイスをログアウトするまで、またはログインのタイムアウトまで、一時的にこの電話に適用されます。EM 機能は、Unified CM の一部として使用できます。

この機能は、会社の外でほとんどの時間を費やし、物理的に、オフィスには時々しかいないモバイル企業ユーザに特に役に立ちます。ホット シーティングまたはフリー シーティングと呼ばれることもあるこれらのタイプのモバイル ユーザに、一時的にオフィスのスペースを提供することで、システム管理者は頻度が低く一時的にしか IP フォンハードウェアを使用する必要がない多数のモバイル ユーザに対応できます。

キャンパス内で EM を利用するには、Unified CM 管理者がユーザ デバイス プロファイルおよびユーザ クレデンシャルを設定し、EM 電話サービスへ IP フォンを登録する必要があります。

（注）　EM は Unified CM コール制御によってのみ、EM 対応エンドポイント デバイスだけでサポートされます。

EM の詳細については、エクステンション モビリティ（18-9 ページ）を参照してください。

キャンパス企業モビリティのハイ アベイラビリティ

キャンパス企業モビリティ機能およびソリューションは、モビリティ機能のハイ アベイラビリティを保証するよう、冗長な方式で設定し配置する必要があります。

たとえば、有線の IP 電話およびソフトウェアベースの IP 電話を実行しているコンピュータを効率的にサポートするため、冗長で普及しているネットワーク接続またはポートが使用可能である必要があります。さらに、これらの冗長なネットワーク接続は、適切なセキュリティ、Quality of Service、およびその他のネットワークベースの機能などの、有線デバイスのロケーションを移動しても最適な操作とボイス品質を確保できる適切な特性を備えたまま配置される必要があります。最終的には、正常なキャンパス モビリティの配置は、ネットワーク接続、PSTN 接続、およびその他のアプリケーションやサービスが、ハイ アベイラビリティのある方式で配置されている場合にのみ可能です。

同様に、ワイヤレス デバイスを接続およびローミングするための WLAN ネットワークの配置や調整では、ワイヤレス サービスに対するハイ アベイラビリティを考慮することも重要です。配置するデバイス数に対する弾力性と十分なカバレッジを確保するために、WAN ネットワークは、同一チャネル セルがオーバーラップすることなく、適切で冗長なセルによるカバレッジが保証されるように配置する必要があります。同一チャネル セルがオーバーラップしない十分なセル カバレッジ、および AP 間のローミングを容易に実行可能にするための異なるチャネル セルの十分なオーバーラップを提供することによって、ワイヤレス デバイスおよびクライアントに対するネットワーク接続でハイ アベイラビリティを確保できます。

最後に、EM をキャンパス内のユーザ モビリティに利用する場合、Unified CM クラスタ内の単一ノードの障害が Extension Mobility 機能の動作を妨げないよう、この機能を冗長な方式で配置する必要があります。可用性が高くなるような Cisco Extension Mobility の詳細については、エクステンション モビリティのハイ アベイラビリティ（18-17 ページ）を参照してください。

キャンパス企業モビリティのキャパシティ プランニング

キャンパス企業モビリティを正常に配置するには、これらのモビリティ機能とソリューションを使用するすべてのモバイル ユーザに対応できる十分なキャパシティを用意する必要があります。

有線デバイスおよびコンピュータの物理的な移動に対するキャパシティの考慮は、キャンパス ネットワーク インフラストラクチャ内で使用できるネットワーク ポート数に完全に依存しています。キャンパス内でデバイスを移動するユーザのため、それぞれのロケーションに、モバイル ユーザのデバイスの接続に使用できるある程度の数の使用可能なネットワークポートがある必要があります。ネットワークポートが不足してこの有線デバイスの移動に対応できないと、1 つのロケーションから別のロケーションへ物理的にデバイスを移動できないことになる可能性があります。

企業 WLAN 内にワイヤレス デバイスを配置し、ワイヤレス デバイス ローミングを利用する場合、WLAN インフラストラクチャのデバイスの接続性とコール キャパシティを考慮することも重要です。デバイス数またはアクティブ コール数の面でのキャンパス WLAN インフラストラクチャのオーバーサブスクリプションは、ワイヤレス接続のドロップ、音声とビデオの品質の低下、またはコール セットアップの遅延や失敗の原因となります。Voice and Video over WLAN（VVoWLAN）の配置をオーバーサブスクライブする可能性は、必要なコール キャパシティを処理するために十分な数の AP を配置することで、著しく最小限に抑えられます。AP のコール キャパシティは、単一チャネル セル領域内でサポートできる音声またはビデオの同時双方向ストリームの数に基づきます。VVoWLAN のコール キャパシティの一般的なルールは次のとおりです。

- データ レート 24 Mbps 以上の Bluetooth を無効にした 802.11g/n（2.4 GHz）チャネル セルあたり最大 27 個の同時 Voice over WLAN（VoWLAN）双方向ストリーム。
- データ レート 24 Mbps 以上の 802.11a/n（5 GHz）チャネル セルあたり最大 27 個の同時 VoWLAN 双方向ストリーム。
- 720p のビデオ解像度（高解像度）および最大 1 Mbps のビデオ ビット レート、Bluetooth が無効の 802.11 g/n（2.4 GHz）あたり、または 802.11 a/n（5 GHz）チャネル セルあたり最大 8 の VVoWLAN 同時双方向のストリームを前提としています。

これらの音声およびビデオ コール キャパシティ値は、RF 環境、設定またはサポートされているビデオ解像度とビット レート、ワイヤレス エンドポイントとその固有の機能、および基礎となる WLAN システム機能に大きく依存します。一部の配置では、実際のキャパシティはこれよりも小さくなることもあります。

（注）　同じ AP に関連付けられている 2 台のワイヤレス エンドポイント間の単一のコールは、2 つの同時双方向ストリームであると見なされます。

EM のスケーラビリティは、Unified CM 内のログイン率およびログアウト率にほぼ依存します。十分な EM ログイン/ログアウト キャパシティがモバイル ユーザに提供できるよう、Unified CM クラスタ内で有効なエクステンション モビリティ ユーザ数と、キャンパス内を移動するユーザ数、任意の時間にこの機能を使用しているユーザ数を把握することが重要です。EM キャパシティ プランニングの詳細については、コラボレーション ソリューション サイジング ガイダンス（25-1 ページ）の章を参照してください。

いずれの場合も、キャンパス内の Unified CM クラスタには、有線デバイスかワイヤレス デバイスにかかわらず、移動されたデバイスに対するデバイス登録を処理する十分なデバイス登録キャパシティが必要です。もちろん、キャンパス内を移動しているすべてのデバイスが、すでにキャンパス ネットワーク内に配置されている場合、コール制御プラットフォーム内の十分なキャパシティが、デバイスの移動の前にすでに配置されている必要があります。ただし、新しいデバイスをモビリティを目的として配置に追加する場合は、デバイス登録キャパシティを考慮する必要があり、必要に応じてさらにキャパシティを追加する必要があります。

最後に、Unified CM によって提供される多くの機能により、これらのモビリティ ソリューションの設定および配置はシステム全体のサイジングと関わっています。実際のシステム キャパシティの決定は、エンドポイント デバイスや EM ユーザの数、配置されている CTI アプリケーションの数に対する最繁時呼数（BHCA）レートなどの考慮事項に基づきます。一般的なシステム サイジング、キャパシティ プランニング、および配置上の考慮事項の詳細については、コラボレーション ソリューション サイジング ガイダンス（25-1 ページ）の章を参照してください。

キャンパス企業モビリティの設計上の考慮事項

キャンパス企業モビリティ機能を配置する際は、次の設計上の考慮事項に従ってください。

- キャンパス内の物理的なデバイス モビリティに対応するには、新しいロケーションで使用されるネットワーク接続の IP 接続（VLAN や VLAN 間ルーティングなど）、接続速度、Quality of Service、セキュリティ、およびネットワーク サービス（インライン パワー、動的ホスト制御プロトコル（DHCP）など）が前のネットワーク接続と同じタイプであることを確認してください。これらの接続パラメータ、サービス、および機能が同じでないと、機能が低下するか、場合によっては機能が完全に失われます。
- ワイヤレス IP デバイスやソフトウェアベース クライアントを展開する場合は、Voice and Video over WLAN（VVoWLAN）の展開が正常に行われるように、展開前、展開中、定期的に展開後に WLAN 無線周波数（RF）事前現地調査を実施して、適切なセル境界、設定、機能設定、容量、および冗長性を判断する必要があります。
- AP は、20 % 以上のセル オーバーラップを確保して配置する必要があります。このようにオーバーラップさせることによって、デュアルモード デバイスがロケーション内で移動した場合に AP 間で正常にローミングして、ボイス ネットワーク接続およびデータ ネットワーク接続を維持できます。
- パケット損失を最小限に抑えるために、AP は -67 dBm のセル パワー レベル境界（またはチャネル セル半径）で配置する必要があります。また、同一チャネルのセル境界の分離は、約 19 dBm にする必要があります。19 dBm の同一チャネル セル分離は、AP またはクライアントにおいて、同じチャネルに関連付けられている他のデバイスとの同一チャネル干渉が発生しないようにするために重要です。同一チャネル干渉が発生すると、音声とビデオの品質が低下するためです。
- 単一の Unified CM ノードが失われた場合に機能の実行に悪影響が及ばないように、EM サービスは冗長性の高い方式で配置してください。EM サービスが重要な場合、Unified CM ノード障害を回避し可用性が高い機能を提供するためのサーバ ロード バランシング ソリューションを考えます。EM のハイ アベイラビリティの詳細については、エクステンション モビリティのハイ アベイラビリティ（18-17 ページ）を参照してください。
- キャンパス ネットワークのワイヤレスの音声とビデオコールのキャパシティは十分に用意してください。そのためには、無線ユーザの BHCA レートに基づき、目的のコール キャパシティの処理に適した数のワイヤレス AP を展開します。各 802.11g/n（2.4 GHz）または 802.11a/n/ac（5 GHz）チャネル セルは、24 Mbps 以上のデータ レートで最大 27 の同時音声のみのコールをサポートできます。各 802.11g/n（2.4 GHz）または 802.11a/n/ac（5 GHz）チャネル セルは、最大 1 Mbps ビット レートでビデオ解像度 720p の場合、最大 8 の同時ビデオ コールをサポートできます。2.4 GHz WLAN 配置では、このキャパシティを実現するには Bluetooth を無効にする必要があります。実際のコール キャパシティは、RF 環境、ワイヤレス エンドポイント タイプおよび WLAN インフラストラクチャによって、さらに小さくなることがあります。

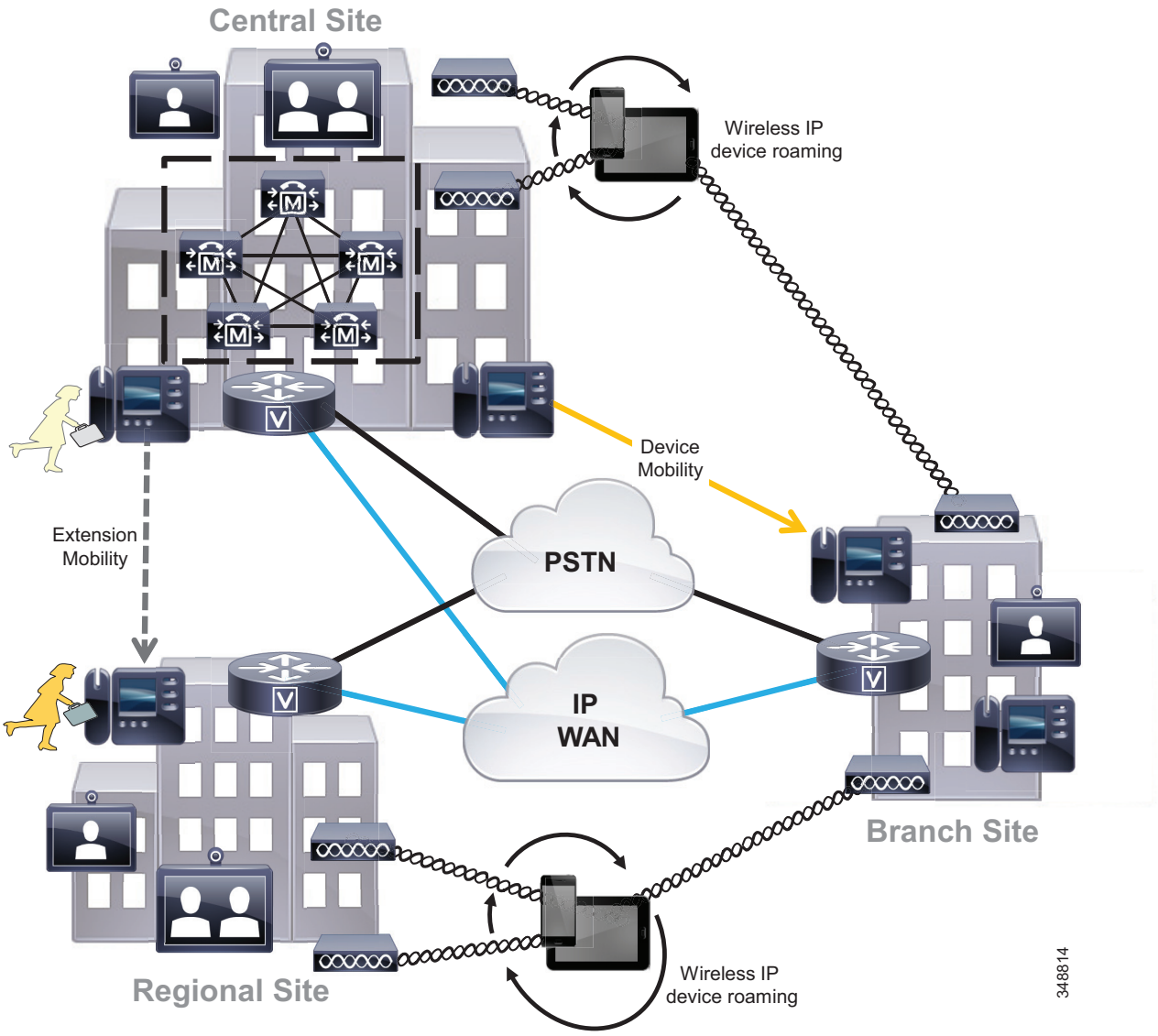
マルチサイト企業モビリティ

マルチサイト企業モビリティとは、複数の物理的な場所があり、それぞれが一意の IP アドレス空間および PSTN 入出力境界を持つ社内でのモビリティを指します。この場合のモビリティには、ユーザやエンドポイント デバイスの各物理ロケーション内の移動だけではなく、サイトおよびロケーション間のユーザやエンドポイント デバイスの移動も含まれます。

マルチサイト企業モビリティのアーキテクチャ

図 21-4 に示すように、マルチサイト企業モビリティのアーキテクチャは、地理的に離れた 2 つ以上のロケーションまたはサイトに基づいています。ユーザとデバイスの数が多い中央またはキャンパス サイトから、ユーザとデバイスの数が少なめの中規模の地域サイト、それよりも小規模な支社サイトまで、サイトの規模は異なってもかまいません。一般にマルチサイト企業配置は、サイトを相互接続する IP WAN リンクや、各ロケーションでのローカル PSTN 入出力で構成されています。さらに多くの場合、サイト間のネットワーク障害中でも機能を維持するため、重要なサービスはそれぞれの物理サイトに複製されています。モビリティの観点からは、ユーザとそのデバイスはサイト内またはサイト間で移動できます。

図 21-4　　マルチサイト企業モビリティのアーキテクチャ



(注)　図 21-4 では、集中呼処理を使用するマルチサイト配置（セントラル サイト内にある単一 Unified CM または VCS クラスタから明らか）を示していますが、マルチサイト企業モビリティの配置と同じ設計および配置の考慮事項が、分散型呼処理環境に適用されます。分散型呼処理環境に配置された場合のモビリティ機能の動作の違いについて、以降で説明します。

マルチサイト企業モビリティのタイプ

マルチサイト企業モビリティ配置には、デバイス、ユーザ、またはその両方の単一サイト内での移動だけではなく、サイト間のユーザおよびデバイスの移動も含まれます。

キャンパス/単一サイト企業配置でサポートされているタイプと同じモビリティ機能とソリューションが、マルチサイト配置の単一サイト内でのユーザやデバイスのサイト内移動に適用されます。これらには、有線電話機の物理的な移動、無線電話ローミング、およびエクステンション モビリティが含まれます。これらのタイプのモビリティソリューションおよび機能の詳細については、キャンパス企業モビリティ (21-4 ページ)を参照してください。

マルチサイト配置でのサイト内モビリティでも、これらのモビリティ機能が同じようにサポートされます。ただし、2 つ以上のサイト間に適用される場合の機能との主な違いとして、これらの機能はデバイス モビリティ機能により拡張されます。デバイス モビリティ機能では、企業ネットワークに接続するときにデバイスが使用する IP アドレスを基にしたダイナミックなロケーション認識メカニズムが提供されます。

物理的な有線デバイスの移動

物理的な有線電話機の移動は、マルチサイト配置の各サイト内でも、サイト間でも簡単に対応できます。キャンパス/単一サイト配置と同様、マルチサイト配置の単一サイトに制限された有線デバイスの移動は、Cisco エンドポイントをネットワークから外し、サイト内の別のロケーションに移動して、別の有線ネットワーク ポートに接続するだけです。新しいネットワークの場所に接続すると、この電話がコール制御プラットフォームに再登録され、前のロケーションと同じように発信や着信ができます。

マルチサイト配置でのサイト間またはロケーション間の有線デバイスの移動も、基本的には同じ形です。ただし、このタイプのモビリティと組み合わせた場合、デバイス モビリティ機能により、デバイスが移動先の新しいロケーションで再登録されると、適切にコール アドミッション制御が動作し、ゲートウェイおよびコーデックが選択されます。この機能の詳細については、デバイス モビリティ (21-15 ページ)を参照してください。

ワイヤレス デバイス ローミング

各サイトで使用できる、無線ネットワークに接続するための無線 LAN ネットワーク インフラストラクチャが使用可能な場合、単一サイトのキャンパス配置と同様、ワイヤレス デバイスは、図 21-4 に示すように、マルチサイト企業配置全体を移動またはローミングできます。しかし、サイト間の有線電話機の移動と同様ワイヤレス デバイスでも、コールの発着信の際に正しいゲートウェイおよびコーデックが確実に使用されるよう、またコール アドミッション制御が帯域幅を適切に管理するよう、デバイス モビリティ機能が配置されなければなりません。この機能の詳細については、デバイス モビリティ (21-15 ページ)を参照してください。

分散型呼処理環境では、有線電話機と同様に、コール ルーティングにより発生する可能性のある問題を回避するため、単一の呼処理プラットフォームまたはクラスタだけにワイヤレス デバイスを登録するように設定する必要があります。

エクステンション モビリティ（EM）

単一サイト内での EM のサポートに加え、図 21-4 に示すように、この機能はサイト間でもサポートされ、ユーザが企業内のサイト間を移動して、各場所で電話機にログオンできます。

また、ユーザが異なる Unified CM クラスタのサイト間や電話間を移動する場合、EM も分散型呼処理の配置でサポートされます。分散型呼処理環境でエクステンション モビリティをサポートするには、Cisco Extension Mobility Cross Cluster（EMCC）機能を設定する必要があります。この機能の詳細については、クラスタ間のエクステンション モビリティ（EMCC）（18-11 ページ）を参照してください。

（注）　EM と EMCC は、Unified CM コール制御によってのみ、EM 対応エンドポイント デバイスだけでサポートされます。

デバイス モビリティ

Cisco Unified CM では、場所、地域、通話サーチ スペース、メディア リソースなど、さまざまな設定を使用して、サイト、つまり物理的な場所が識別されます。特定のサイトにある Cisco Unified IP Phone は、これらの設定により静的に設定されます。Unified CM では、適切なコールの確立、コール ルーティング、メディア リソースの選択などのためにこれらの設定を使用します。一方、Cisco Unified Wireless IP Phone などのデュアルモード電話機やその他のモバイル クライアント デバイスは、各自のホーム サイトからリモート サイトに移動される場合、電話機に静的に設定されているホーム設定を保持しています。この結果 Unified CM では、リモート サイトの電話機にあるこれらのホーム設定を使用します。この状況は、コール ルーティング、コーデックの選択、メディア リソースの選択、およびその他の呼処理機能における問題の原因となる場合があるため望ましくありません。

Cisco Unified CM では、デバイス モビリティという機能を使用します。この機能により、Unified CM では、IP フォンがホーム ロケーションにあるのか、ローミング ロケーションにあるのかを判別できます。Unified CM では、デバイスの IP サブネットを使用して、その IP フォンの正確な場所を判別します。クラスタ内でのデバイス モビリティを使用できるようにすることで、モバイル ユーザは 1 つのサイトから別のサイトにローミングでき、このときサイト固有の設定を取得します。次に、Unified CM では、これらの動的に割り当てられた設定を使用して、コール ルーティング、コーデックの選択、メディア リソースの選択などを行います。

この項では、最初にデバイス モビリティ機能の主要な目的について説明し、続いてデバイス モビリティ機能そのものについて詳細に説明します。ここでは、デバイス モビリティ機能のさまざまなコンポーネントおよび構成要素について取り上げます。この項では、デバイス モビリティ機能が企業ダイヤル プランに与える影響を、さまざまなダイヤル プラン モデルへの影響も含めて詳細に説明します。

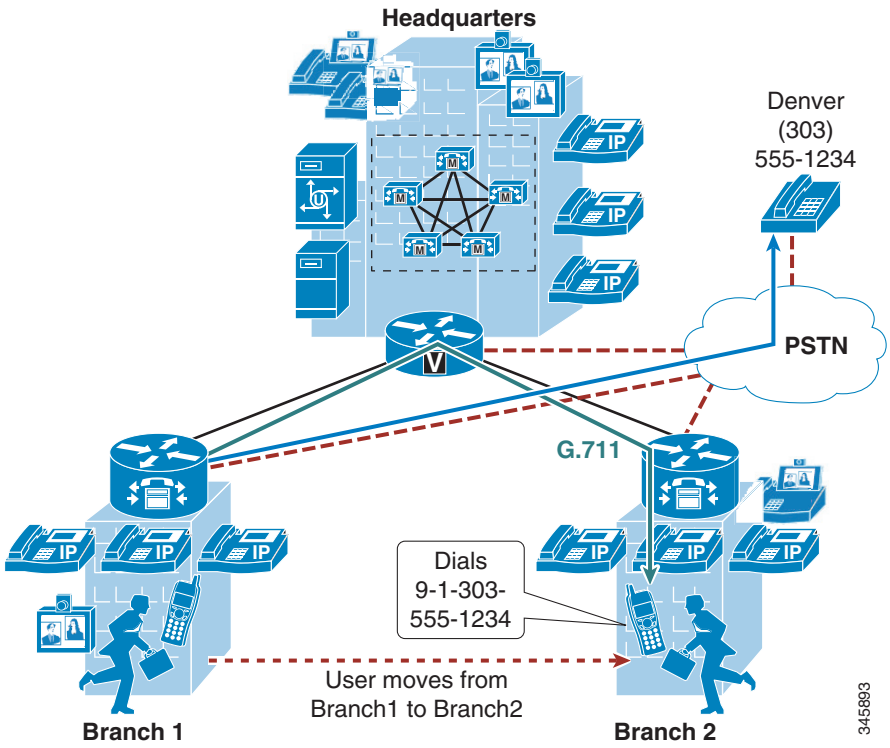
（注）　デバイス モビリティは Unified CM コール制御だけでサポートされます。

デバイス モビリティの必要性

この項では、Unified CM クラスタに多くのモバイル ユーザが含まれている場合のデバイス モビリティの必要性について説明します。

図 21-5 は、本社サイト（HQ）にあり、デバイス モビリティ機能を備えない Unified CM クラスタを含んでいる架空のネットワークを示しています。このクラスタには、支店 1 と支店 2 の 2 つのリモート サイトがあります。サイト内コールでは、いずれも G.711 音声コーデックが使用されます。一方サイト間コール（IP WAN を経由するコール）では、いずれも G.729 音声コーデックが使用されます。各サイトには、外部コールのための PSTN ゲートウェイがあります。

図 21-5　　リモート サイトを 2 つ持つネットワークの例



支社 1 のユーザが支社 2 に移動し、Denver にいる PSTN ユーザに通話すると、次のような動作が発生します。

- Unified CM では、そのユーザが支社 1 から支社 2 に移動したことを認識していません。PSTN への外部コールが WAN を経由して支社 1 のゲートウェイに送られ、そこから PSTN に出ます。これにより、モバイル ユーザの PSTN コールすべてに、引き続きそのユーザのホーム ゲートウェイが使用されます。
- このモバイル ユーザと支社 1 ゲートウェイは、同じ Unified CM リージョンおよびロケーションに存在しています。ロケーション ベースのコール アドミッション制御は、異なるロケーションに存在しているデバイスおよび G.711 音声コーデックを使用するリージョン内コールにだけ適用可能です。したがって、IP WAN を経由する支社 1 ゲートウェイへのコールでは G.711 コーデックが使用され、コール アドミッション制御のための Unified CM によるトラッキングは行われません。この動作の結果、リモート リンクすべてが低速リンクである場合に、IP WAN 帯域幅のオーバー サブスクリプションが発生する場合があります。
- モバイル ユーザが、複数の支社 2 ユーザを Denver にいる PSTN ユーザとの既存のコールに追加することで、会議を作成します。モバイル ユーザは支社 1 ゲートウェイの会議リソースを使用します。したがって、すべての会議ストリームが IP WAN 経由で流れます。

（注） デバイス モビリティは、クラスタ内機能で、複数の Unified CM クラスタには拡張されません。分散型呼処理環境では、配置内の各 Unified CM クラスタでデバイス モビリティを有効にし、設定する必要があります。

(注)　デバイス モビリティが設定されていない環境では、管理者はサイト ロケーション間に WAN 帯域幅を多めにプロビジョニングし、WAN 経由とサイト間のデバイスの物理的な移動で、WAN を多めにサブスクライブしないようにします。各 WAN リンクについて余分にプロビジョニングする帯域幅の量は、ユーザが 2 か所の場所の間でデバイスを移動する際の予測レートによって異なります。

デバイス モビリティ アーキテクチャ

Unified CM デバイス モビリティ機能は、上記の問題を解決するために有用です。この項では、この機能の動作方法を簡単に説明します。この機能の詳細については、次の Web サイトで入手可能な最新バージョンの『*Feature Configuration Guide for Cisco Unified Communications Manager*』で、デバイス モビリティに関する情報を参照してください。

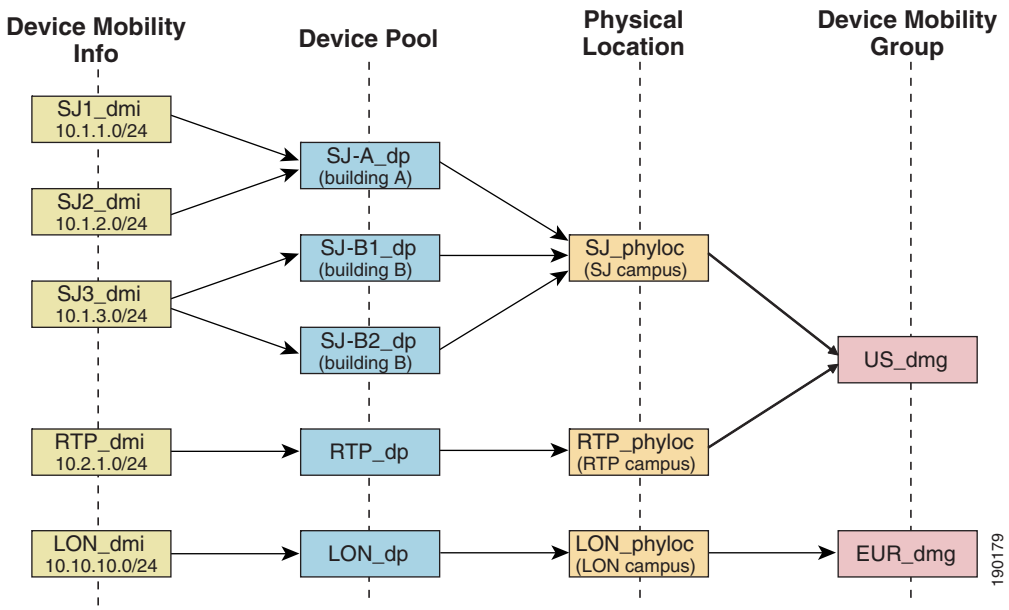
https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html

デバイス モビリティには次のような要素が含まれます。

- デバイス モビリティ情報:IP サブネットを設定し、デバイス プールを IP サブネットに関連付けます。
- デバイス モビリティ グループ:ダイヤリング パターンが類似しているサイトの論理グループを定義します(たとえば、図 21-6 の US_dmg および EUR_dmg)。
- 物理ロケーション:デバイス プールの物理ロケーションを定義します。言い換えると、この要素では、IP 電話およびデバイス プールに関連付けられているその他のデバイスの地理的なロケーションを定義します(たとえば、図 21-6 に示されている San Jose の IP 電話は、すべて物理ロケーション SJ_phyloc を使用して定義されています)。

図 21-6 は、この 3 つの用語すべての関係を示します。

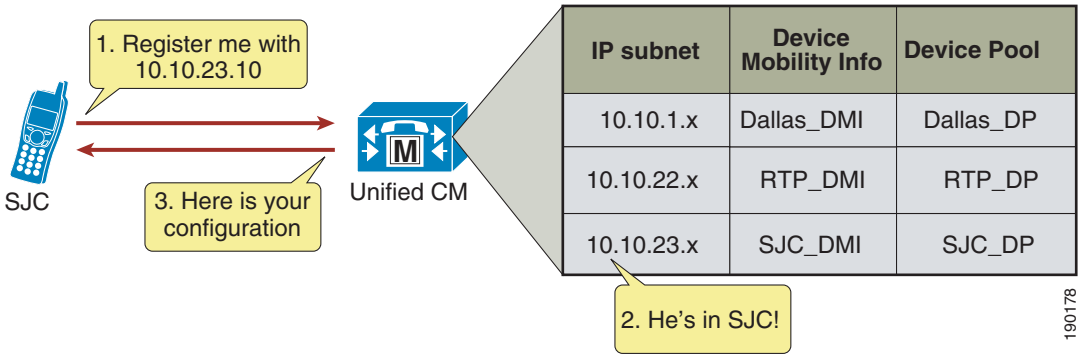
図 21-6　デバイス モビリティ コンポーネントの関係



Unified CM では、デバイスの IP サブネットに基づいてデバイス プールを IP フォンに割り当てます。次の手順は、図 21-7 に図示がありますが、この動作を説明したものです。

1. IP フォンでは、その電話の IP アドレスを Skinny Client Control Protocol（SCCP）または Session Initiation Protocol（SIP）登録メッセージに含めて送信することにより、Unified CM への登録を試行します。
2. Unified CM では、デバイスの IP サブネットを抽出し、デバイス モビリティ情報に設定されているサブネットと照合します。
3. サブネットが一致すると、Unified CM では、デバイス プール設定に基づいて、デバイスに新規設定を提供します。

図 21-7　　電話登録プロセス



Unified CM では、デバイス プール設定にあるパラメータ一式を使用して、デバイス モビリティに対応します。これらのパラメータは、次の 2 つの主要なタイプについてのパラメータです。

- ローミングに依存する設定（21-18 ページ）
- デバイス モビリティ関連の設定（21-19 ページ）

ローミングに依存する設定

これらの設定にあるパラメータは、デバイスがデバイス モビリティ グループの内部または外部をローミングしているときに、デバイス レベルの設定より優先されます。この設定には、次のパラメータが含まれます。

- 日付/時刻グループ
- 地域
- メディア リソース グループ リスト
- 参照先
- ネットワーク ロケール
- SRST リファレンス
- 物理ロケーション
- デバイス モビリティ グループ

ローミングに依存する設定は、主に、適切なコール アドミッション制御および音声コーデックの選択を実施するために有用です。これは、ロケーションおよびリージョンの設定は、デバイスのローミング デバイス プールに基づいて使用されるためです。

さまざまなコール アドミッション制御手法については、帯域幅管理（13-1 ページ）の章を参照してください。

ローミングに依存する設定により、メディア リソース グループ リスト（MRGL）も更新されて、保留音、会議、トランスコーディングなどで適切なリモート メディア リソースが使用されるようになり、これによりネットワークが効率的に使用されます。

ローミングに依存する設定により、Survivable Remote Site Telephony（SRST）ゲートウェイも更新されます。モバイル ユーザは、ローミング中に別の SRST ゲートウェイに登録します。この登録が、ローミング電話機が SRST モードであるときのダイヤリング動作に影響することがあります。

たとえば、ユーザが Unified CM への接続を失う新しいロケーションに電話機を移動した場合、ローミングに依存するデバイス モビリティ設定に基づいて、移動された電話機に対して新しい SRST リファレンスが設定されます。また、移動された電話機はローカルなローミング ロケーション SRST ルータの制御下に入ります。この場合、デバイスの DID が変更されず、ホーム ロケーションに固定されたままになるため、ユーザの電話機は PSTN や他のサイトから到達不能になるだけでなく、SRST 内で実装されている短縮ダイヤルを使用しなければ、ローカルな障害発生サイト内のデバイスから到達することも困難になる可能性があります。

たとえば、ユーザが電話機を San Jose のホーム ロケーション（ディレクトリ番号が 51234 で、関連付けられた DID が 408 555 1234）から New York のリモート ロケーションに移動したとします。また、ユーザが New York ロケーションにローミングして間もなく、New York のサイトと San Jose の間のリンクに障害が発生したとします。このシナリオでは、New York サイトにある電話機はすべて、そのサイト内の SRST ルータにフェールオーバーされます。また、ローミング電話機または移動された電話機は、その SRST リファレンスがデバイス モビリティのローミング依存設定に基づいて更新されたために、New York の SRST ルータに登録されます。このシナリオでは、New York のローカルなデバイスが Unified CM に登録するのと同じように、5 桁の内線番号とともに SRST ルータに登録されます。その結果、ローミング電話機のディレクトリ番号は 51234 のまま変わりません。他のすべてのサイトから、および PSTN からローミング電話機に到達するために、番号 408 555 1234 が、この特定の DID が固定されている San Jose の PSTN ゲートウェイにルーティングされます。New York サイトは San Jose サイトから切断されているため、このようなコールはいずれもユーザのデスクフォンには到達不能です。したがって、コールはユーザのボイスメール ボックスにルーティングされます。同様に、ローカルの障害発生サイト内のコールは、5 桁の短縮ダイヤルを使用して、または SRST ルータ内の **dialplan-pattern** および **extension-length** コマンドで定義されているように設定済みの番号をプレフィックスとして付加して、ダイヤルする必要があります。いずれの場合も、ローカル発信者が、短縮ダイヤルによりローカル ローミング デバイスに到達するために必要なダイヤリング動作を理解している必要があります。ローカル ローミング電話機に到達するために、5 桁をダイヤルするだけでよいこともあれば、ユーザが特別な番号プレフィックスをダイヤルする必要があることもあります。同じロジックが、New York の移動された電話機またはローミング電話機からの発信ダイヤリングにも適用されます。短縮ダイヤルを使用してローカル内線番号に到達するためには、そのダイヤリング動作を変更する必要があるためです。ただし、ローカルなローミング デバイスから PSTN への発信ダイヤリングは、常に同じである必要があります。

デバイス モビリティ関連の設定

これらの設定にあるパラメータは、デバイスがデバイス モビリティ グループの内部をローミングしているときにだけ、デバイス レベルの設定より優先されます。この設定には、次のパラメータが含まれます。

- [デバイス モビリティ コーリング サーチ スペース（Device Mobility Calling Search Space）]
- [AAR コーリングサーチスペース（AAR Calling Search Space）]
- [AAR グループ（AAR Group）]
- [発呼側トランスフォーメーション CSS（Calling Party Transformation CSS）]

コーリング サーチ スペースは、ダイヤルできるパターンまたは到達できるデバイスを指示するため、デバイス モビリティ関連の設定は、ダイヤル プランに影響します。

デバイス モビリティ グループ

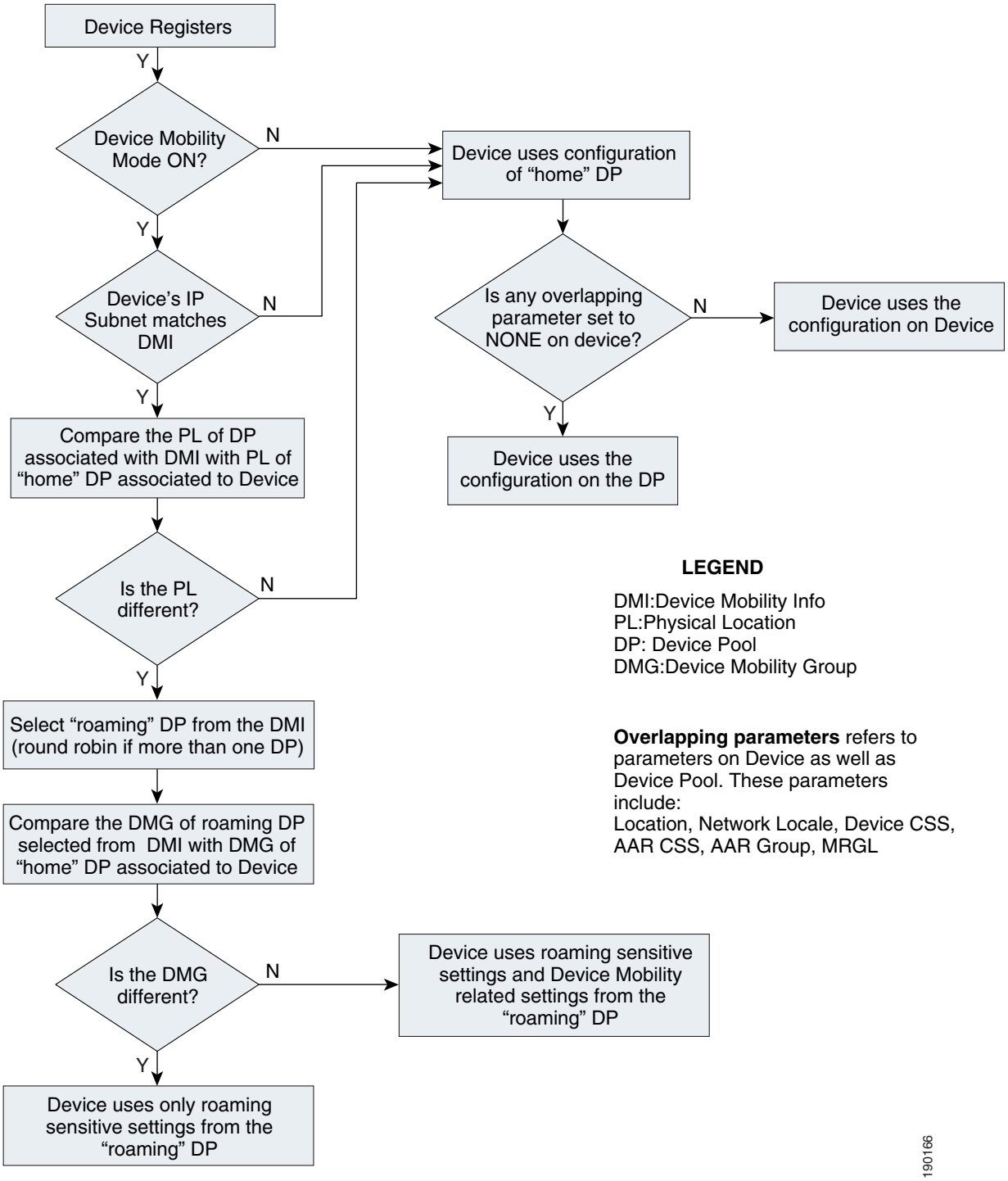
前述したように、デバイス モビリティ グループは、ダイヤリング パターンが類似したサイト（たとえば、同じ PSTN アクセス コードを持つサイトなど）の論理グループを定義します。このガイドラインを使用すると、すべてのサイトがサイト固有のコーリング サーチ スペースに類似したダイヤリング パターンを持ちます。ダイヤリング動作が異なるサイトは、異なるデバイス モビリティ グループに属します。図 21-6 に示すように、San Jose サイトと RTP サイトのデバイス モビリティ情報、デバイス プール、および物理ロケーションは異なります。ただし、必要なダイヤリング パターンと PSTN アクセス コードは 2 つのロケーション間で同じであるため、これらはすべて同じデバイス モビリティ グループ US_dmg に割り当てられています。一方、London サイトは別のデバイス モビリティ グループ EUR_dmg に割り当てられています。これは、必要なダイヤリング パターンと PSTN アクセス コードが US サイトのものとは異なるためです。デバイス モビリティ グループ内をローミングするユーザは、新規コーリング サーチ スペースを受け取った後であっても、ダイヤリング動作をリモート ロケーションで維持できます。デバイス モビリティ グループの外部をローミングするユーザは、自身のホーム コーリング サーチ スペースを使用するため、やはり、ダイヤリング動作をリモート ロケーションで維持できます。

ただし、デバイス モビリティ グループが、異なるダイヤリング パターンを持つ複数のサイトとともに定義されている場合（たとえば、あるサイトではユーザが外線使用時に 9 をダイヤルする必要があるが、別のサイトではユーザが外線使用時に 8 をダイヤルする必要がある場合）、そのデバイス モビリティ グループ内のユーザ ローミングにより、すべてのロケーションで同じダイヤリング動作を維持できいないことがあります。ユーザは、各ロケーションで新規コーリング サーチ スペースを受け取った後で、異なるロケーションにおいて異なる番号をダイヤルする必要がある場合があります。この動作はユーザの混乱を招く可能性があるため、異なるダイヤリング パターンを持つサイトを同じデバイス モビリティ グループに割り当てることは推奨しません。

デバイス モビリティの動作

デバイス モビリティ機能の動作を図 21-8 のフローチャートに示します。

図 21-8　デバイス モビリティ機能の動作



デバイス モビリティ機能には、次のガイドラインが適用されます。

- 図 21-8 にリストされている重複するパラメータがデバイスおよびデバイス プールで同じ設定を持つ場合は、デバイスではこれらのパラメータに NONE を設定できます。次にこれらのパラメータをデバイス プールに設定する必要があります。この方法を実施すると、デバイスにすべてのパラメータを個別に設定する必要がないため、設定の量を大幅に削減できます。
- サイトごとに物理ロケーション 1 つを定義してください。1 つのサイトが複数のデバイス プールを持つことができます。
- PSTN または外部/オフネット アクセスのダイヤリング パターンが類似したサイトを、同じデバイス モビリティ グループを使用して定義してください。
- 企業のポリシーに応じて、未定義のサブネットすべてに対応する、IP サブネット 0.0.0.0 の「catch-all」デバイス モビリティ情報を定義できます。このデバイス モビリティ情報は、ネットワーク リソースのアクセスまたは使用を制限できるデバイス プールを割り当てるために使用できます（たとえば、ローミング中にこのデバイス プールに関連付けられているデバイスからの通話すべてをブロックする通話サーチ スペース NONE を使用してデバイス プールを設定できます）。ただし、これを行う場合、管理者は、911 およびその他の緊急通話であってもブロックされるという事実を承知する必要があります。コーリング サーチ スペースは、911 またはその他の緊急コールだけにアクセスを許すパーティションを含めて設定できます。

ダイヤル プランの設計上の考慮事項

デバイス モビリティ機能は、選択されたローミング デバイス プールの設定、またはエンドポイントが登録されている IP アドレスに基づいて、複数のデバイスおよびデバイス プール設定を使用します。サブネットのデバイス プールの設定により更新される設定の詳細については、次の Web サイトで入手可能な最新バージョンの『*Feature Configuration Guide for Cisco Unified Communications Manager*』で、デバイス モビリティに関する情報を参照してください。

https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html

ダイヤル プランから見ると、主に AAR グループ、AAR CSS、デバイス CSS、ローカル ルート グループ、および発信コールの発呼側変換 CSS 設定が関連しています。

ローミング デバイスのイーグレス ゲートウェイの選択

通常、ローミング デバイスの目的のイーグレス ゲートウェイの選択動作は、訪問したサイトに対してローカルなゲートウェイを使用することです。発信側デバイスに固有のイーグレス ゲートウェイの選択を実装するための推奨される方法は、標準ローカル ルート グループを使用するルート リストを指す PSTN ルート パターンを使用することです。ルート リストの標準ローカル ルート グループを効果的に使用することは、実際のコールをルーティングする際に標準ローカル ルート グループが発信側エンドポイントのデバイス プール内で設定されたローカル ルート グループと置き換えられることを意味します。このスキーマは、サイトが不特定のルート パターンとルート リストが使用できるようになります。サイト固有のイーグレス ゲートウェイ接続は、デバイス プール レベルでローカル ルート グループの設定に完全に依存します。

ローミング デバイスでは（デバイス モビリティ グループ内またはデバイス モビリティ グループ間のローミング）、デバイス モビリティ機能により、ローミング デバイス プールのローカル ルート グループが標準ローカル ルート グループとして常に使用されるようになります。これにより、ローカル ルート グループのイーグレス ゲートウェイの選択で、訪問したサイトに固有のルート グループ（つまり、訪問したサイトに対してローカルなゲートウェイ）が通常使用されることが保証されます。この動作は、たとえば、標準ローカル ルート グループのルート リストを使用するルート パターンによってルーティングされる緊急通話が、訪問したサイトに対してローカルなイーグレス ゲートウェイを常に使用するようになります。

ローカル ルート グループのイーグレス ゲートウェイの選択は、ダイヤル プラン（14-1 ページ）の章で説明されているすべてのダイヤル プラン アプローチで使用できます。

ローミングしたエンドポイントが、特定のコールをホーム サイトのゲートウェイにルーティングする必要がある場合は、標準ローカル グループの代わりに固定されたサイト固有のルート グループを使用するルート リストを指すルート パターンを使用して、このようなコールのルーティングを実装する必要があります。

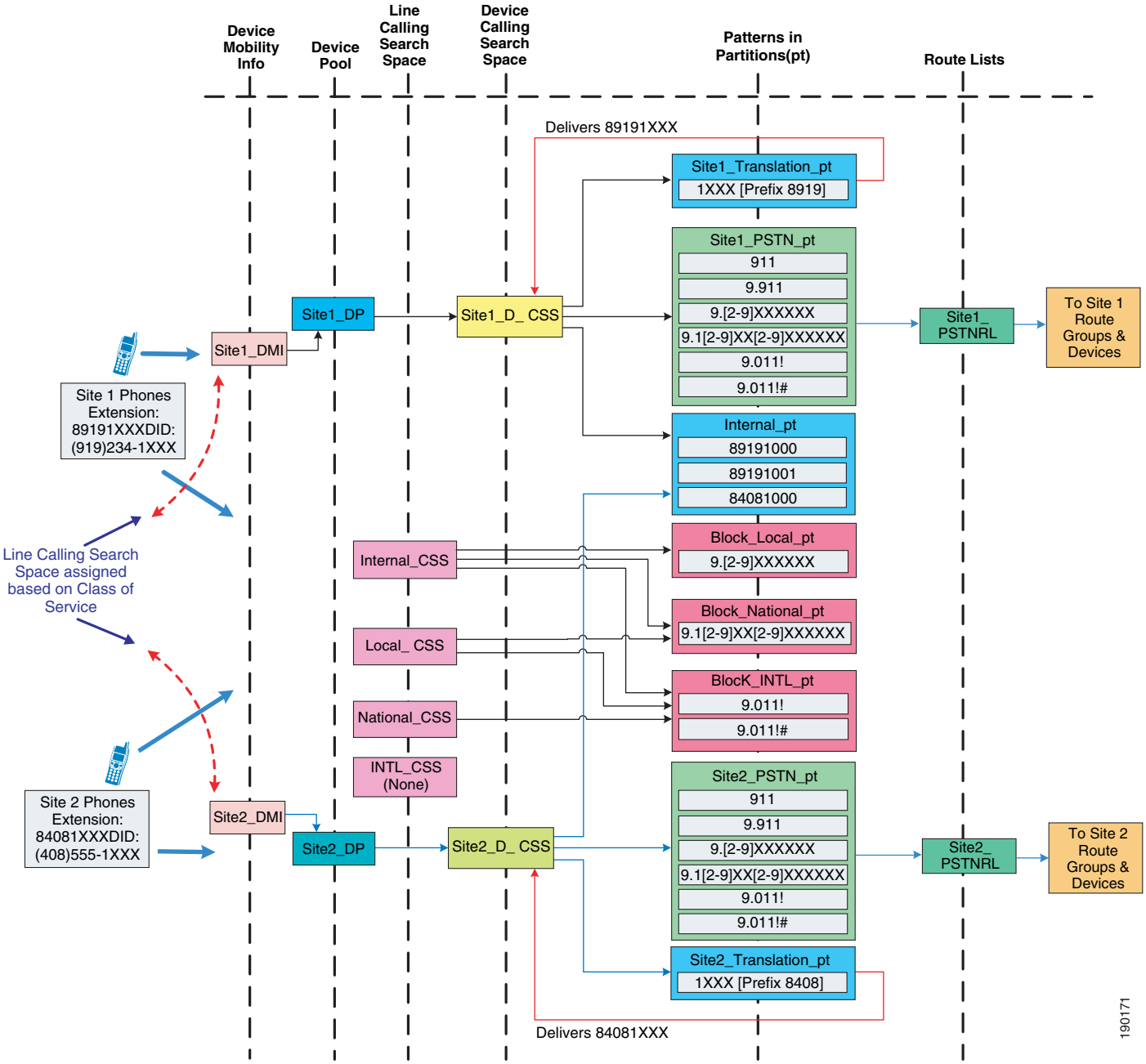
回線/デバイスのダイヤル プラン アプローチでは、これらのルート パターンはエンドポイントで設定されたデバイス CSS によってアドレス指定されます。ローミングし、かつ同一モビリティ グループを使用している場合には、発信側エンドポイントのデバイス CSS は、ローミング デバイス プールで設定されたデバイス モビリティ CSS に置き換えられます。固定されたイーグレス ゲートウェイの選択がいくつかのコールにおいて必要であり、これらのコールのルート パターンがデバイス CSS によってアドレス指定される場合、ローミング デバイスが常にデバイス モビリティ グループをまたがってローミングを行う必要があります。これは、ローミング エンドポイントが、エンドポイントで設定されたデバイス CSS を常に使用することを保証します。

ダイヤル プラン（14-1 ページ）の章で説明されている +E.164 ダイヤル プラン アプローチを使用する場合、すべての PSTN ルート パターンは、ローミング デバイスに対して変更されてないか、更新されていない回線 CSS によってアクセスされます。このダイヤル プランでは、固定ゲートウェイ（たとえば、ローミング デバイスのホーム ロケーション）に特定の PSTN にある宛先を接続しているサイト固有のルート パターンは、デバイス モビリティ動作から影響を受けません。

ローカル ルート グループを持たない回線/デバイス アプローチを使用する、フラット アドレッシングの可変長のオンネット ダイヤリング

図 21-9 は、デバイス モビリティのためのフラット アドレッシングによる可変長オンネット ダイヤリング プランを示します。

図 21-9　デバイス モビリティのためのフラット アドレッシングによる可変長オンネット ダイヤリング プラン



次の設計上の考慮事項が、図 21-9 のダイヤル プラン モデルに適用されます。

- このダイヤル プランで 4 桁のサイト内ダイヤリングを実装するトランスレーション パターンは、デバイス CSS によって参照されます。これは、サイト固有の回線 CSS を持つ要件を回避するために行われます。(ユーザがデバイス モビリティ グループ内でローミングしているとすると)デバイス CSS がローミング デバイス プールのデバイス モビリティ CSS で更新されるため、モバイル ユーザは訪問したサイトのサイト内ダイヤリングを継承します。この動作が望ましくない場合は、各サイトをデバイス モビリティ グループとして定義することを検討してください。ただし、ユーザは、外部 PSTN コールすべてで、モバイル電話では引き続きホーム ゲートウェイが使用され、したがって WAN 帯域幅が消費されることを承知しておく必要があります。これは、標準ローカル ルート グループを使用して回避できます(ローミング デバイスのイーグレス ゲートウェイの選択(21-22 ページ)を参照)。
- PSTN および内部電話機パーティションへのアクセスだけを持つローミング ユーザのために追加のデバイス コーリング サーチ スペースを設定できます。この設定には、サイトごとに 1 つ以上の追加のデバイス プールとコーリング サーチ スペースが必要です。したがって、*N* 個のサイトには、*N* 個のデバイス プールおよび *N* 個のコーリング サーチ スペースが必要です。ただし、この設定では、各サイトをデバイス モビリティ グループとして定義する必要がありません。この設定を適用しているモバイル ユーザは、ローミング時にデバイス CSS からトランスレーション パターンを参照しません。
- リモート SRST ゲートウェイに登録されているモバイル ユーザは、一意な内線番号を持ちます。ただし、モバイル ユーザは、リモート SRST ゲートウェイに登録されているときは、PSTN ユーザがモバイル ユーザと通話できないことを承知しておく必要があります。

従来のアプローチとローカル ルート グループを使用した +E.164 ダイヤル プラン

ダイヤル プラン(14-1 ページ)の章で説明したように、回線/デバイス アプローチにはいくつかの特定の問題があり、回線/デバイス アプローチに基づいて +E-164 ダイヤル プランを作成することは推奨されません。+E.164 ダイヤル プランの推奨されるアプローチは、回線 CSS でサービス クラスの選択とダイヤリングの正規化を組み合わせて、ローカル ルート グループ機能を使用してサイト固有のイーグレス ゲートウェイ選択の要件に対応することです。このアプローチでは、電話機のデバイス CSS はまったく使用されません。デバイス モビリティとこのアプローチを併用する場合、設計のローミングを受けやすい唯一のコンポーネントは、デバイス プールのローカル ルート グループです。ローミング電話機では(デバイス モビリティ グループ内またはデバイス モビリティ グループ間のローミング)、電話のホーム デバイス プールで定義されたローカル ルート グループは、ローミング デバイス プールで定義されたローカル ルート グループによって常に更新されます。これは、すべてのコールが、訪問したサイトに対してローカルなゲートウェイを介して出力されることを保証されます。

マルチサイト企業モビリティのハイ アベイラビリティ

マルチサイト企業モビリティ機能およびソリューションは、モビリティ機能のハイ アベイラビリティを保証するため、冗長性を備えた方法で設定、配置する必要があります。有線電話機の移動、無線ローミング、およびマルチサイト モビリティ配置での EM のハイ アベイラビリティの考慮事項は、キャンパス モビリティ配置での考慮事項と同様です。キャンパス環境と同じく、冗長ネットワーク ポート、無線セル カバレッジ、およびエクステンション モビリティのログインおよびログアウトを処理する Unified CM ノードが、高可用なサービスを確保するために必要です。

また、デバイス モビリティ機能のハイ アベイラビリティを考慮することも重要です。デバイス モビリティ機能はネイティブで Unified CM コール制御内に統合されているため、デバイス モビリティの機能がクラスタ ノードの障害による影響を受けることはありません。パブリッシャ ノードまたは呼処理（サブスクライバ）ノードに障害が発生した場合、デバイス プール、デバイス モビリティ情報、デバイス モビリティ グループ、およびデバイス モビリティに関連する他のすべての設定は保持されます。また、呼処理ノードに障害が発生した場合、影響を受ける電話機は、Unified CM Group の構成要素に基づいて、通常どおりセカンダリ呼処理ノードまたは Survivable Remote Site Telephony（SRST）リファレンス ルータにフェールオーバーします。

（注）　Cisco TelePresence System エンドポイントは Cisco IOS SRST での登録の冗長性をサポートしていません。

マルチサイト企業モビリティのキャパシティ プランニング

デバイス モビリティのスケーラビリティの考慮事項と同様、この機能および各種の構成要素（デバイス プールやデバイス モビリティ グループなど）に関連する特定のキャパシティ制限または強制的なキャパシティ制限はありません。一般的なシステム サイジング、キャパシティ プランニング、および配置上の考慮事項の詳細については、コラボレーション ソリューション サイジング ガイダンス（25-1 ページ）の章を参照してください。

マルチサイト企業モビリティの設計上の考慮事項

企業モビリティの設計上の考慮事項はすべて、マルチサイト企業モビリティ配置にも適用されます（キャンパス企業モビリティの設計上の考慮事項（21-11 ページ）を参照）。さらに、次の設計に関する推奨事項が、特にマルチサイト モビリティ環境に適用されます。

- サイト間の接続や、他のサイトの接続の障害が重要な動作を妨害しないよう、すべての重要なサービス（デバイス登録、PSTN 接続、DNS、DHCP など）をマルチサイト配置内の各サイトで確実に配置してください。加えて、デバイスや必要なコール キャパシティをサポートするため、十分な数の物理ネットワーク ポートおよびワイヤレス LAN AP が各サイトで使用できるようにしてください。
- 異なるダイヤリング パターンを持つ複数のサイト（たとえば、異なる PSTN アクセス コードを持つ複数のサイト）が同じデバイス モビリティ グループ内に設定されている場合、ローミング ユーザが各自のロケーションに基づいて異なる方法で番号をダイヤルする必要があるため、混乱を招く可能性があります。このため、類似のダイヤリング パターンを持つサイト（たとえば、同じ PSTN アクセス コードを持つサイト）を同じデバイス モビリティ グループに割り当てることを推奨します。これにより、ローミング ユーザは、デバイス モビリティ グループ内のすべてのサイトで同じ方法で番号をダイヤルできます。
- 「ローミング」デバイス プールからのデバイス モビリティ設定が適用されるのは、同じデバイス モビリティ グループ内でローミングするときだけです。移動された電話機からの元のコールが「ホーム」またはデバイスで設定されているコーリング サーチ スペースを使用し、結果的にコール ルーティング動作が引き起こされるため、異なるデバイス モビリティ グループ間でのローミングを避けてください。これにより、ローカルな「ローミング」ゲートウェイではなく別のサイトのゲートウェイを経由してコールがルーティングされる可能性があります。その結果、不必要に WAN 帯域幅が消費されることがあります。

- 物理ロケーションは各サイトに 1 つだけ定義してください。そうすることで、ユーザがサイト間でローミングを行う場合にだけ、デバイス モビリティが適用されます。同じサイト内でローミングを行う場合は、デバイス モビリティに影響する要素（たとえば、WAN 帯域幅消費、コーデック選択、コール アドミッション制御など）を考慮する必要はありません。単一のサイト内では通常、低速のリンクは配置されないためです。
- フェールオーバーのシナリオでは、「ローミング」電話機は、「ローミング」デバイス プールのローミング依存設定に従って、SRST リファレンス/ゲートウェイを利用します。したがって、これらの状況においては、「ローミング」電話機の DID は別のロケーションの PSTN ゲートウェイに固定されているために、PSTN からこの電話機に到達することはできません。さらに、「ローミング」電話機からコールを発信する場合は、PSTN アクセス コードなどの要素に対してダイヤリング動作を変更する必要があることがあります。また、電話機で設定されているスピード ダイヤルが使用できなくなることもあります。
- システムで、短縮ダイヤルを使用できることや、短縮ダイヤルに依存するスピード ダイヤルを使用できることが要求されている場合は、固定オンネット ダイヤル プラン モデルを使用することを推奨します。このモデルを使用すると、（直接またはスピード ダイヤルによる）短縮ダイヤルは、モバイル ユーザの電話機がローミングを行う場所にあっても、動作を継続するためです。すべての内線番号またはディレクトリ番号は全サイトにわたって一意であるため、短縮ダイヤルを使用し続けることができます。また、重複する内線番号がないため、短縮ダイヤルを普遍的に使用できます。
- システムが可変長オンネット ダイヤル プラン モデルを使用する場合（回線/デバイスまたは回線 CSS だけの +E.164 ダイヤル プラン アプローチを使用）、コールされたときに単一の一意の内線番号に到達されるように不変的な方法でスピード ダイヤルを設定することを推奨します。完全な +E.164 番号を使用するか、サイトまたはアクセス コードを使用してスピード ダイヤルを設定することにより、ローミング ユーザはすべてのロケーションで同じスピード ダイヤルを使用できます。
- VPN 接続を介して企業ネットワークにアクセスすることがあるユーザに対してデバイス モビリティを有効にした場合は、VPN ロケーションへの「ローミング」により確実に動的デバイス モビリティ設定変更が行われるように、VPN が接続された電話機のデバイス モビリティ情報（DMI）に、VPN コンセントレータにより配信または所有された IP サブネットが含まれている必要があります。DMI は、VPN コンセントレータと同じ場所にあるデバイスに使用されているデバイス プールに関連付ける必要があります。
- Cisco Expressway モバイル & リモート アクセスを介してエンタープライズ ネットワークにアクセスすることがあるユーザに対してデバイス モビリティを有効にした場合は、Expressway ロケーションへの「ローミング」により確実に動的デバイス モビリティ設定変更が行われるように、Expressway に接続しているデバイスのデバイス モビリティ情報（DMI）に、Expressway-C ノードにより使用された IP サブネットが含まれている必要があります。DMI は、Expressway-C ノードと同じ場所に配置されているデバイスに使用されているデバイス プールに関連付ける必要があります。

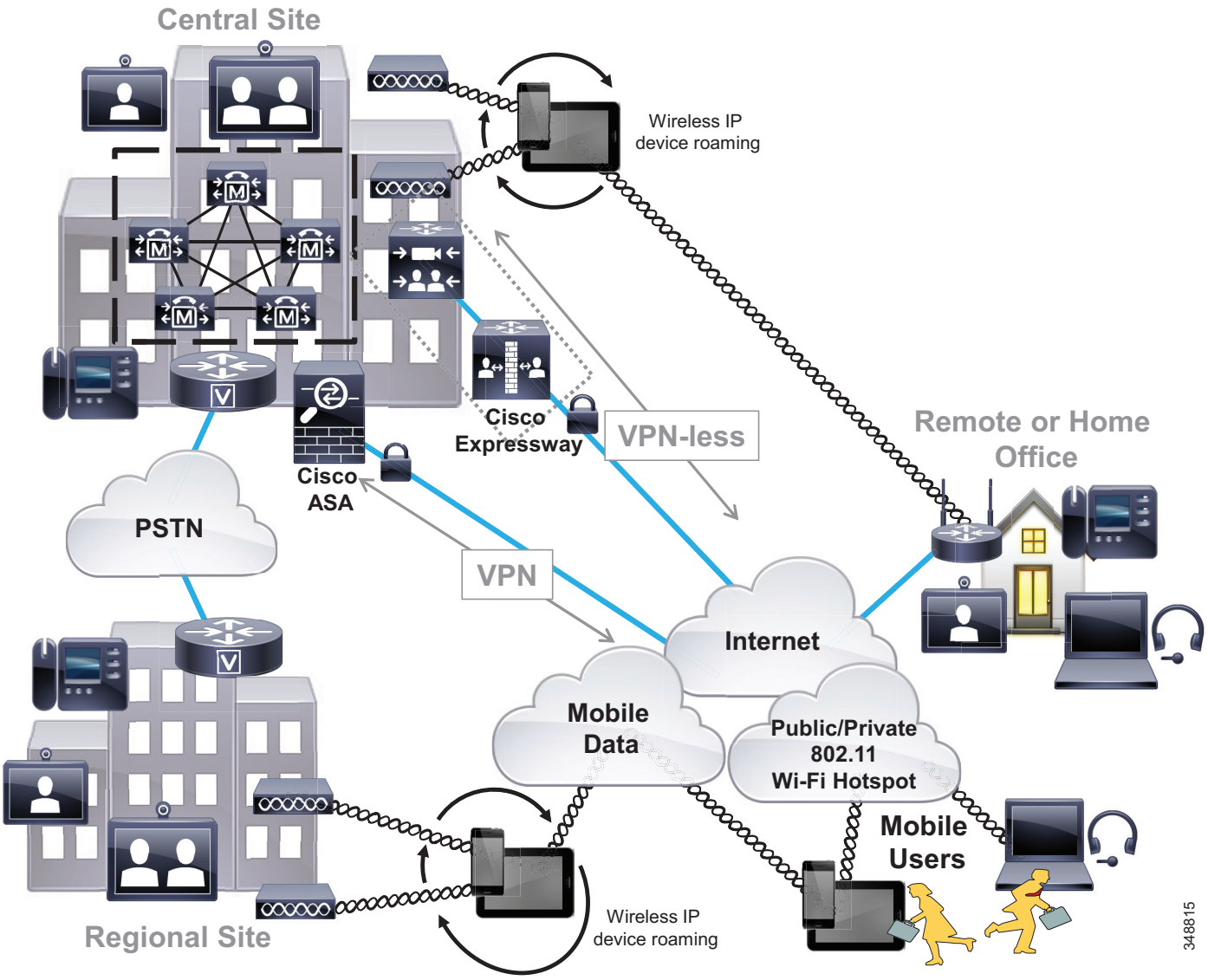
リモート企業モビリティ

リモート企業モビリティは、企業から離れたロケーションにいて、公共のインターネットを介した安全な接続により企業ネットワーク インフラストラクチャに接続しているモバイル ユーザを指します。ここでモビリティは、これらのリモート ロケーションでのエンドポイント デバイスの配置や、企業と各自のロケーション間での頻度に関わらないユーザの移動や、場合によってはユーザが使用するモバイル デバイスを処理します。

リモート企業モビリティのアーキテクチャ

図 21-10 に示すように、リモート企業モビリティのアーキテクチャは、リモート物理ロケーション（一般に、従業員のホーム オフィスや、それ以外の、インターネット経由で会社に安全に接続できるあらゆるリモート ロケーション）に基づいています。これらのリモート サイトは、一般にユーザのコンピュータ、電話機、およびその他の機器またはエンドポイントへ接続できる IP ネットワークで構成されます。場合によっては、この IP ネットワークを企業の制御下に置き、リモート ロケーションとエンタープライズ ネットワーク間に安全なトンネルまたは接続を備えた VPN ルータまたはエッジ セキュリティ プラットフォームを構成できます。また、リモート サイト IP ネットワークはインターネットへの接続を提供し、ユーザのコンピュータまたはエンドポイント デバイスでソフトウェアベースのクライアント機能を使用してエンタープライズ ネットワークへの安全な接続を作成する必要があります。無線接続をリモート ロケーションで使用して、ユーザのコンピュータまたはエンドポイントを無線接続できるようにすることもできます。無線接続をリモート ロケーションで使用する場合、ワイヤレス フォンおよびモバイル デバイスをエンタープライズ ネットワークからホーム オフィスへ移動することもでき、ワイヤレス企業デバイスまたはモバイル電話機をリモート ロケーション内で利用して発信および受信することもできます。

図 21-10　　リモート企業モビリティのアーキテクチャ



リモート企業モビリティのタイプ

リモート企業モビリティ配置は、デバイス モビリティをサポートすることではなく、主にリモート ユーザをサポートすることに重点を置いています。確かにユーザは、エンドポイント デバイスを持っても持たなくても定期的に企業ロケーション間またはロケーションとリモート サイト間を移動できます。ただし、これらの配置の主な目的は、固定したロケーションでも、アクティブに移動している場合でも、企業ユーザのリモート接続をサポートすることです。図 21-10 に示すように、リモート サイト モビリティには、主に 2 つのタイプのセキュア リモート接続があります。

- VPN セキュア リモート接続
- VPN なしのセキュア リモート接続

VPN セキュア リモート接続

VPN セキュア リモート接続は、企業およびリモート ネットワークまたはデバイス間のレイヤ 3 のセキュア トンネルを実現します。安全なリモート企業接続用の VPN 使用して、エンタープライズ ネットワークの境界を実質的に VPN 終端の場所まで拡張します。VPN 終端デバイスまたはネットワークの場所からの VPN 接続は、デバイスやネットワークが物理的に企業の境界内にある場合と同様のネットワークの接続性を提供します。Cisco 適応型セキュリティ アプライアンス（ASA）ヘッドエンド コンセントレータと Cisco AnyConnect クライアントは、安全なコラボレーションとその他の企業ワークフローの両方に VPN 接続を提供します。ルータ ベースの VPN 接続とクライアント ベースの VPN は、2 つの一般的な VPN 展開タイプです。どちらのタイプもリモート サイトへのセキュアな接続をサポートしており、固定された場所に残るものやリモート サイトと企業間で移動可能なものなど、さまざまなエンドポイント デバイスに対応できます。固定された場所のデバイスには、有線ビデオ エンドポイント、IP フォン、デスクトップ コンピュータなどがあります。デュアル モードの携帯電話、ワイヤレス IP フォン、ラップトップ コンピュータ、タブレットは、リモート サイトと企業間で定期的に移動するエンドポイントの例です。

ルータ ベースのリモート VPN 接続

ルータ ベースの VPN トンネルによりセキュアな接続が実現します。図 21-10 に示すように、これらのタイプのシナリオでは、配置したリモート サイト ルータ（たとえば、Cisco Virtual Office ソリューションのルータ）は、エンタープライズ ネットワークへの安全なレイヤ 3 VPN トンネルを設定する必要があります。これにより実質的に、企業ネットワークの境界をリモート サイト ロケーションまで広げます。このタイプの接続のメリットは、より幅広い種類のデバイスとエンドポイントをリモート サイトに配置できることです。これらのデバイスで接続の安全性を確保する必要がなく、特別なソフトウェアや設定の必要がないためです。代わりに、これらのデバイスはリモート サイト ネットワークに接続するだけで、リモート サイト ルータから企業 VPN ヘッドエンドまでの安全な VPN IP パスを利用できます。図 21-10 に示すように、リモート サイト ルータはワイヤレス ネットワーク接続も提供できます。

クライアントベースの安全なリモート接続

ワイヤレスおよび有線 IP フォンと、ソフトウェアベースの PC、スマート フォン、タブレットのテレフォニー クライアントは、図 21-10 に示すように、自宅、モバイル プロバイダー、Wi-Fi ホット スポット ネットワークなどのリモート ネットワークの場所からインターネット経由で接続できます。クライアント ベースの VPN シナリオの VPN 接続は、エンドポイント デバイスで実行しているソフトウェア クライアントによって確立されます。したがって、エンドポイントとソフトウェア クライアントは、企業の VPN ヘッドエンド ターミネーション コンセントレータに安全に VPN 接続する必要があります。これにより実質的に、エンタープライズ ネットワークの境界をリモート デバイスまで広げます。このタイプの接続のメリットは、ルータ ベースの VPN 接続が現実的ではないパブリック ネットワークを含め、より幅広いネットワークの場所に対応できることです。このようなさまざまなネットワーク間の接続によって、クライアント デバイスが移動中であっても安全な接続を実現できます。エンドポイント デバイスのタイプによっては、音声およびビデオ通話などのコラボレーションのワークフローが VPN 接続を利用する唯一の機能である場合があります。PC、スマート フォン、タブレットなどの多目的デバイスの場合、VPN 接続を介した完全な企業ワークフローが可能です。

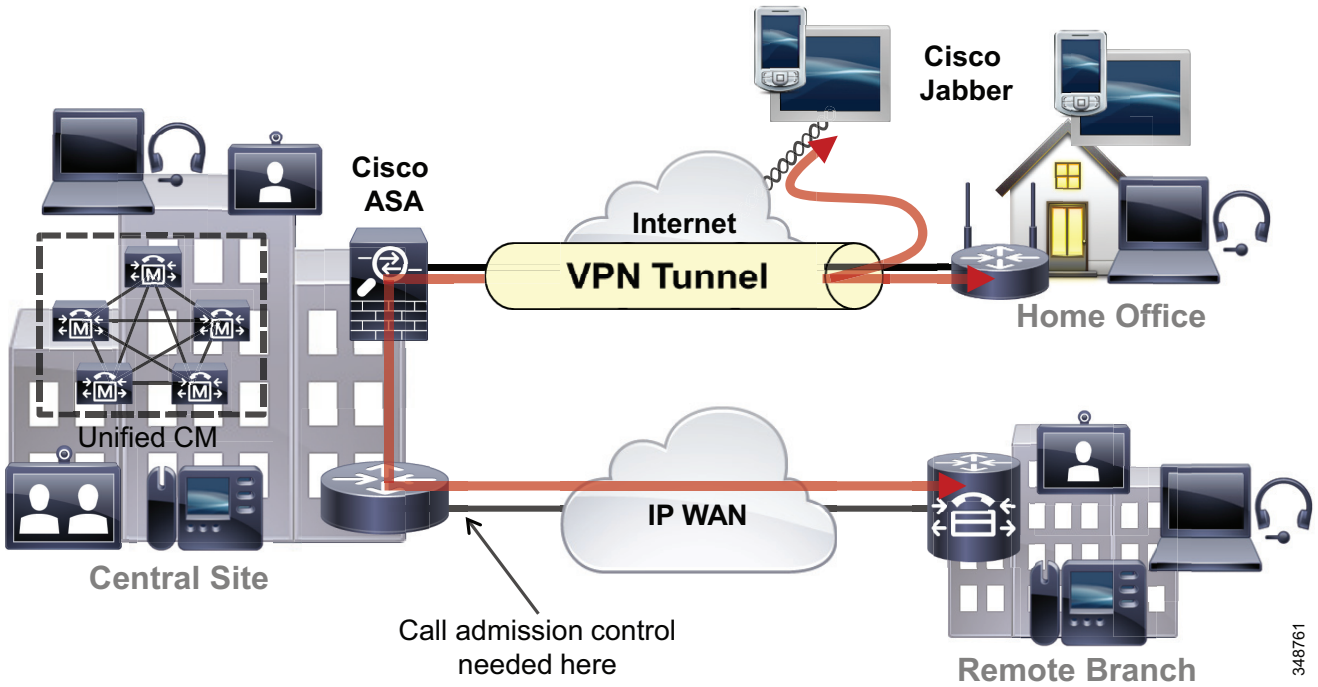
これらのタイプのデバイスの例には、有線またはワイヤレス接続の PC または Cisco AnyConnect などのソフトウェアベースの VPN を使用したワイヤレス接続のモバイル クライアント デバイスや、組み込み VPN クライアントを使用する Cisco Unified IP Phone 7965 などの有線の Cisco Unified IP Phone が含まれます。

デバイス モビリティと VPN のリモート企業接続

クライアントベースまたはルータベースの VPN リモート接続のどちらを配置するかにかかわらず、コール アドミッション制御およびコーデックがエンドポイント デバイスに正しくネゴシエートされ、適切な企業サイトの PSTN ゲートウェイおよびメディア リソースが使用されるようにするため、デバイス モビリティ機能を使用できます。VPN 接続経由で受信したエンドポイント デバイスの IP アドレスに基づいて、Unified CM はデバイスのロケーションを動的に決定します。

図 21-11 は、Cisco Jabber コラボレーション クライアントがリモート サイトのコンピュータまたはモバイル デバイスで実行されている、クライアントベースの安全なリモート接続の例です。このソフトウェアベースのコラボレーション アプリケーションは、クライアントベースの VPN を介して企業に接続され、Unified CM に登録されています。

図 21-11　　リモート サイトの Cisco Jabber 向けのクライアントベースの VPN 接続



次は、クライエントベースまたはルータベースの VPN 接続経由で企業に接続しているリモート サイトにおける、ユーザ デバイスのデバイス モビリティ機能の有効化に関する設計ガイドラインです。

- VPN コンセントレータによって配布または所有されている IP サブネットを指定してデバイス モビリティ情報（DMI）を設定します。
- VPN コンセントレータと同じ場所にあるデバイスに使用されるデバイス プールと同じデバイス プールに DMI を関連付けます。ただし、コール特権、ネットワーク ロケールなどのパラメータを考慮する必要があります。
- リモート サイトのユーザに、クライアントベースまたはルータベースの VPN 接続を行う場合は、地理的に最も近い企業 VPN コンセントレータを指定するよう指導します。

これらのガイドラインにより、確実に、企業 WAN 上でおよびリモート サイトへの接続を介して、コール アドミッション制御が正しく適用されます。

VPN の配置の詳細については、次のサイトの Design Zone for Security の *Security in WAN* で入手可能な各種の VPN 設計ガイドを参照してください。

https://www.cisco.com/c/en/us/solutions/enterprise/design-zone-security/landing_wan_security.html

VPN なしのセキュア リモート接続

VPN なしのセキュア リモート接続により、企業とリモート接続デバイス間のリバース プロキシ TLS のセキュアな接続が可能になります。このタイプの接続では、完全なレイヤ 3 VPN トンネルに必要なオーバーヘッドを最小限に抑えながら、セキュアなファイアウォール トラバーサルが許可されます。VPN なしのリバース プロキシを使用して、セキュアな接続はデバイスまたはクライアント アプリケーションまでエンタープライズ ネットワークの境界を拡張します。Cisco Collaboration Edge アーキテクチャには Cisco Expressway が採用されています。

Cisco Expressway により、トラフィックが企業の物理境界内で生成される場合のように、特定のエンドポイントまたはクライアント アプリケーションのトラフィック フローにセキュアなトラバーサルを提供します。ただし、すべてのトラフィック フローがこの接続タイプでサポートされるわけではありません。ここで説明した Cisco Collaboration Edge Architecture ソリューションは、音声およびビデオ通話、IM およびプレゼンス、ビジュアル ボイスメール、および社内ディレクトリ アクセスなどのコラボレーション ワークフローを保護します。非コラボレーション アプリケーションやサービスへのアクセスを含む完全な企業ワークフローは、次の接続のタイプではサポートされません。

Cisco Collaboration Edge Architecture の詳細については、次のサイトで入手可能なマニュアルを参照してください。

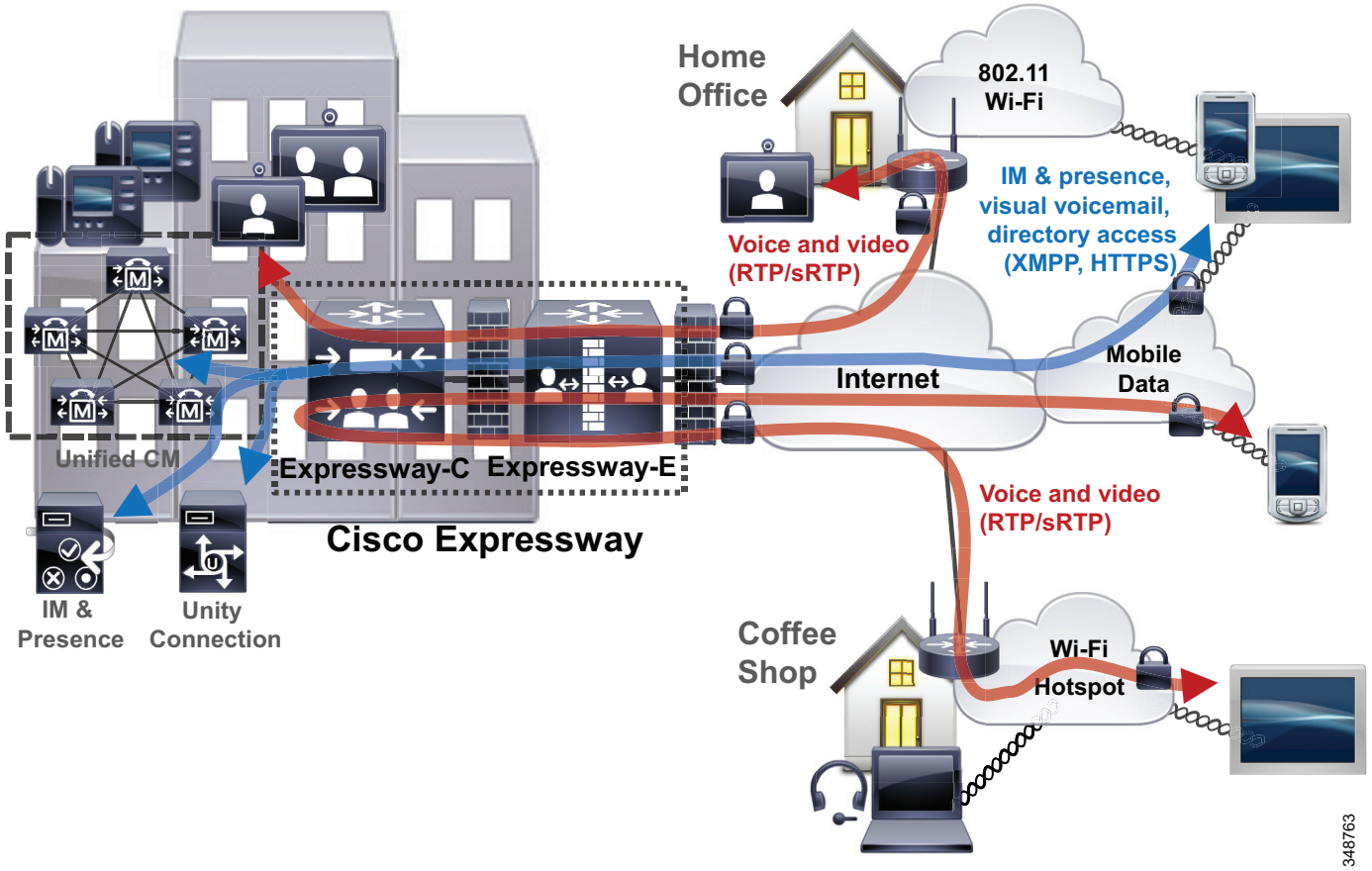
https://www.cisco.com/c/en/us/solutions/collaboration/collaboration-edge-architecture/index.html

Cisco Expressway

Cisco Expressway ソリューションのモバイル & リモート アクセス機能は、逆プロキシ ファイアウォール トラバーサル接続を提供します。これにより、リモート ユーザとそのデバイスが企業のコラボレーション アプリケーションおよびサービスにアクセスして利用できます。

図 21-12 に示すように、Cisco Expressway ソリューションには、2 つの主なコンポーネント（Expressway-E ノードと Expressway-C ノード）が含まれています。これら 2 つのコンポーネントは Unified CM と組み合わせて動作し、安全なモバイル & リモート アクセスを実現します。Expressway-E ノードは、モバイル & リモート デバイスにセキュアなエッジ インターフェイスを提供します。通常、このノードはエンタープライズ ネットワークの DMZ 領域内にあります。Expressway-C ノードは、Unified CM へのプロキシ登録を提供し、リモート セキュア エンドポイント登録を可能にします。内部エンタープライズ ネットワークにある Expressway-C ノードは、Expressway-E ノードとのセキュアな TLS アウトバウンド接続を確立します。この接続がセキュアなメディア トラバーサルに使用されます。

図 21-12　Cisco Expressway モバイル & リモート アクセスの安全なリモート コラボレーション



Unified CM に登録されると、リモート デバイスは SIP シグナリングと RTP メディアを使用して IP 経由で音声およびビデオ通話の発信および受信ができるようになります。安全な Cisco Expressway モバイル & リモート接続は、デバイス登録および音声とビデオ通話だけでなく、IM およびプレゼンス、ビジュアル ボイスメール、社内ディレクトリ アクセスなどのコラボレーションのワークフローが追加で可能になります。完全なコラボレーション機能は、VPN トンネルを必要とせずに企業から入手できます。音声およびビデオ メディア、シグナリング、およびその他のコラボレーション トラフィックは Expressway C ノードでエンタープライズ ネットワークを通過します。図 21-12 に示すように、社外の 2 台のリモート デバイス間のコールが社内 Expressway C のノードでヘアピンされます。

セキュアなエンドポイントからすべてのトラフィックが VPN トンネルを通過して企業に戻る VPN セキュア接続とは異なり、Cisco Expressway モバイル & リモート アクセスは、コラボレーション トラフィックのみで企業への安全な接続を実現します。非コラボレーション ワークフローおよびトラフィックはセキュア Cisco Expressway 接続を通過しません。代わりに、他のすべてのトラフィックはローカル ネットワークまたはインターネットに直接送信され、エンタープライズ ネットワークを通過しません。

Cisco Expressway モバイル & リモート アクセス機能は、Cisco ハードウェアのエンドポイントおよび Cisco Jabber ソフトウェア ベースのクライアント エンドポイントの両方をサポートします。サポートされている Cisco ハードウェア エンドポイントには Cisco TelePresence EX、MX、および SX シリーズのビデオ エンドポイント、Cisco DX、7800、および 8800 シリーズのデスクフォンがあります。Cisco Jabber デスクトップおよびモバイル クライアントも、Cisco Expressway モバイル & リモート アクセスをサポートします。特に、Cisco Jabber モバイル クライアントは Cisco Expressway モバイル & リモート アクセス接続を移動中もサポートするため、モバイル ユーザの場所やネットワーク接続のタイプに関係なく、安全なリアルタイム コラボレーションが可能になります。

リモート セキュア接続の実現に VPN を使用する場合と同様、Expressway モバイル & リモート アクセスを使用したデバイス モビリティ設定は、低速リンクのコール量の監視、適切なコーデックのネゴシエーション、およびローカル ゲートウェイ リソースを使用したコールのルーティングのために Unified CM がエンドポイントの場所を追跡できるようにする上で重要です。Expressway モバイル & リモート アクセスを使用している環境でデバイス モビリティを設定するときには、次の作業を必ず行ってください。

- Expressway-C ノードが使用する IP サブネットを使用してデバイス モビリティ情報（DMI）を設定します。
- Expressway-C ノードと同じ場所に配置されているデバイスに使用されているデバイス プールに、DMI を関連付けます。

Cisco Expressway モバイル & リモート アクセス機能では、Expressway-C と Expressway-E クラスタのペアあたり最大 10,000 件の Unified CM へのリモート エンドポイント登録がサポートされています。また Expressway クラスタ ペアでは最大 2,000 の同時ビデオ コールまたは 4,000 の同時音声のみのコールがサポートされています。Expressway ノードあたりのキャパシティを含む Cisco Expressway のキャパシティの詳細については、Cisco Expressway（25-39 ページ）の項を参照してください。

規模拡大または複数の地理的な場所を対象とした設計に対応するため、複数の Expressway クラスタを展開します。複数サイトを導入する場合、場所に関係なくユーザとユーザのデバイスに対してリモート企業接続を提供するため、Expressway クラスタを複数の地域にわたって分散する必要があります。Expressway モバイル & リモート アクセス接続を効果的に分散し、デバイスが最も近い位置の Expressway サービス ノードまたはクラスタに接続できるようにするには、GeoDNS サービスが推奨されます。GeoDNS サービスにより、Expressway DNS サービス レコードに対する DNS クエリの送信元 IP アドレスにより決定される場所、またはデバイスの場所と使用可能な Expressway サービス ノードの間での最も短い平均遅延に基づき、モバイル デバイスは最も近い Expressway サービス ポイントに振り分けられます。

Cisco Expressway 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データ シートおよび製品マニュアルを参照してください。

https://www.cisco.com/c/en/us/products/unified-communications/expressway-series/index.html

リモート企業モビリティのハイ アベイラビリティ

リモート サイト モビリティ環境では、企業 VPN または VPN なしのセキュリティ サービスが、冗長性を備えた方法で企業内に設定され配置されている必要があります。これにより、VPN とリバース プロキシ ファイアウォール トラバーサルによる安全な接続の可用性が高いことが保証されます。企業内または企業エッジの VPN コンセントレータまたは Cisco Expressway ノードで障害が発生した場合、他の VPN または VPN なしのリモート エッジ ノードを備えたクライアントまたはエンドポイントで、新しい安全な接続を設定できます。Unified CM クラスタまたはその他のアプリケーション サーバ ノードの冗長性に基づき、デバイス登録、音声およびビデオ サービス、IM およびプレゼンス、およびその他のコラボレーション サービスの可用性が高くなります。このレベルのコラボレーション サービスの冗長性は、オンプレミスと同様に、エンドポイントとクライアントが VPN 経由で企業に接続される場合にも適用されます。

エンドポイントとクライアントが Cisco Expressway モバイル & リモート アクセスを使用して接続している場合は、コラボレーション アプリケーションとサービスの冗長性が限定されます。Cisco Expressway ソリューションの場合、モバイル & リモート アクセスのハイ アベイラビリティは各ノード タイプのクラスタを配置することによって実現されます。Unified CM ノードのクラスタ、Expressway E のノードのクラスタ、および Expressway C のノードのクラスタの配置では、1 つまたは複数のプライマリ ノードに障害が発生した場合に、バックアップ ノードがモバイル & リモート アクセスおよびデバイス登録を提供できます。

リモート企業モビリティのキャパシティ プランニング

リモート企業モビリティ環境のスケーラビリティの考慮事項で最も重要なのは、企業のヘッドエンド セッション終端装置です。管理者は、すべてのリモート セキュア接続要件に対応する十分な VPN セッションおよび VPN なしの接続キャパシティを配置する必要があります。Cisco Expressway 経由のクライアントまたはルータ ベースの VPN または VPN なしのリモート エッジ セキュア接続の場合も、デバイス登録の負荷およびセキュア接続で利用可能なさまざまなコラボレーションのワークフローを処理できる十分なプラットフォームまたはノードの容量を提供する必要があります。適切なキャパシティを用意しないと、一部のリモート サイトとデバイスが会社に接続できなくなり、基本的なテレフォニー サービスでもアクセスできなくなります。さらに、キャンパスまたはマルチサイト企業モビリティの配置と同様、すべてのリモート ユーザのデバイスを処理できるよう、企業内に十分なデバイス登録キャパシティを用意することが重要です。

Cisco Call Control およびゲートウェイ エッジでのキャパシティ（プラットフォーム固有のエンドポイント設定や登録キャパシティなど）の詳細については、コラボレーション ソリューション サイジング ガイダンス（25-1 ページ）の章を参照してください。

リモート企業モビリティの設計上の考慮事項

モバイル ユーザがリモート サイト接続できるようにする場合、次の設計上の推奨事項を考慮してください。

- デバイス モビリティを使用する場合は、VPN コンセントレータが配布または所有する IP サブネットを含むデバイス モビリティ情報（DMI）、または、Expressway の場合は、Expressway-C ノードで使用されるサブネットを含むデバイス モビリティ情報を、忘れずに設定してください。VPN コンセントレータや Expressway-C ノードと同じ場所に設置されたデバイス用に設定されるデバイス プールに、DMI を割り当てます。
- リモート サイト ユーザに、VPN を接続する場合は最も近い VPN コンセントレータを選択するよう指導します。

- VPN を使用したすべてのリモート サイトの場所およびデバイスへの接続を用意するため、適切な VPN セッション キャパシティが確実に使用できるようにしてください。
- すべてのリモート デバイスへの VPN なしのセキュアな接続を用意するため、適切なリバース プロキシ ファイアウォール通過セッション キャパシティが確実に使用できるようにしてください。十分な Expressway-E と Expressway-C ノードおよびセッション キャパシティが確実に使用できるようにしてください。いずれの場合も、十分な Unified CM 登録キャパシティが必要です。

クラウド サービスとハイブリッド サービスのモビリティ

クラウド サービスとハイブリッド サービスのモビリティとは、Cisco Collaboration Cloud から配信されるコラボレーション アプリケーションとコラボレーション サービスを利用するモバイル ユーザのことです。このようなタイプのモビリティには、クラウド コラボレーション サービスのみを利用する純粋なクラウド展開と、クラウドと企業オンプレミスの両方のコラボレーション アプリケーションやサービスを活用するハイブリッド展開が含まれます。

モバイル デバイスとクライアントは、インターネットを介して Cisco Collaboration Cloud および他のクラウドのコラボレーション アプリケーションとサービスに接続します。クライアントとデバイスは、企業オンプレミスでもリモートのどちらにいてもかまいません。インターネットへのアクセスにより、各デバイスは（移動中でも移動していなくても）エンタープライズ ネットワークや公共ネットワーク、またはプライベート ネットワークを介して接続されるこれらのサービスを利用できます。

企業はクラウドからのコラボレーション サービスを有効にし、状況によっては、さまざまな理由からこれらのサービスを企業のコラボレーション インフラストラクチャに統合します。企業において、ソフトウェア サービスとアプリケーションの配信で、クラウドへの注目度が高まっている主な理由には次のようなものがあります。

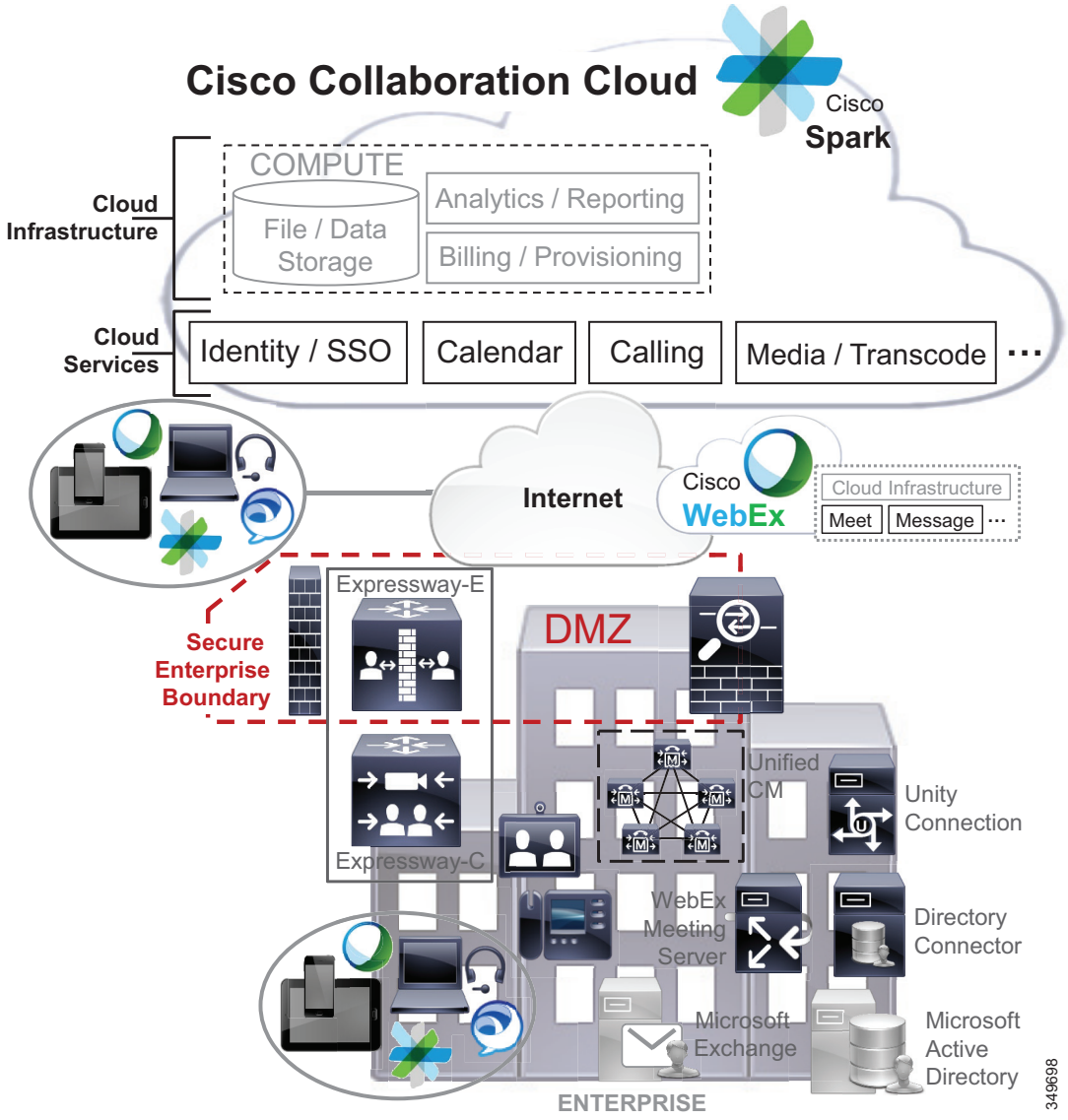
- クラウド サービス更新プログラムは継続的かつ自動的に配信されるため、新しい機能と報告されている問題の解決が迅速に提供される
- コンピューティング リソースが柔軟に運用されるので、オンデマンドのユーザ キャパシティとサービス パフォーマンスが実現
- クラウド アプリケーションおよびサービス機能の一元化されたオンライン管理が可能
- 可用性の高いクラウド アーキテクチャにより、広い地域をカバーすると同時にサービスの復元力を提供
- インフラストラクチャの資本コストと管理は、クラウド ベンダーが負担ベンダーはインフラストラクチャを管理し、そのセキュリティにも責任を持ちます。これには、コンピューティング、ストレージ、電源、ネットワーク、および基本的なサービスとアプリケーションが含まれます。

クラウドおよびハイブリッド サービスのモビリティ アーキテクチャ

図 21-13 に示すように、クラウドおよびハイブリッド サービスのモビリティ アーキテクチャはインターネットに接続された Cisco Collaboration Cloud および Cisco WebEx Collaboration Cloud サービスに基づいています。Collaboration Cloud と WebEx Collaboration Cloud サービスは、セキュアで復元力のあるクラウド コンピューティング インフラストラクチャで実現されます。このアーキテクチャで配信されるクラウド コラボレーション サービスには、Cisco Spark メッセージ、会議、コールと、WebEx ミーティングとメッセージングがあります。これらのサービスは純粋なクラウド導入に加えて、企業のオンプレミス サービスとともに導入することもできます。たとえば、企業は WebEx Meeting Center の会議および WebEx Messenger IM and Presence（クラウドからのサービス）を、Unified CM の音声およびビデオ通話および Unity Connection のボイス メッセージング（オンプレミスで提供されるサービス）と並行して有効にできます。Cisco Spark のメッセージ、会議、通話は、企業アイデンティティ、シングル サインオン（SSO）、予定表、通話などのクラウド ハイブリッド サービスの企業統合で強化できます。

クラウド サービスの企業統合は一般に、サービス関連のトラフィックを企業が送受信するための、クラウドと企業間のセキュアな接続に依存します。このトラフィックは図 21-13 に示すように、セキュアな企業境界 DMZ を通過する必要があります。

図 21-13　クラウドおよびハイブリッド サービスのモビリティ アーキテクチャ



Cisco Jabber、Cisco Spark、Cisco WebEx などのシスコのデスクトップ、Web ブラウザ、モバイル デバイスのコラボレーション アプリケーションやクライアントは、企業外からのインターネットを介したリモート接続または社内接続のどちらでも、シスコ コラボレーション クラウドおよび WebEx Collaboration Cloud からのサービスを利用します。

クラウドベースのサービスを利用できる Cisco クライアントについての詳細は、シスコのモバイル クライアントおよびデバイス（21-81 ページ）を参照してください。

クラウド ハイブリッド サービス統合のタイプ

クラウド ハイブリッド コラボレーション サービスの統合には主に 2 つのタイプがあります。

- Cisco WebEx Collaboration Cloud のハイブリッド統合（21-39 ページ）
- Cisco Spark Hybrid Services（21-39 ページ）

Cisco WebEx Collaboration Cloud のハイブリッド統合

Cisco WebEx Collaboration Cloud の機能はスタンドアロン サービスとして利用可能である一方、ハイブリッド統合により、既存の企業のオンプレミス コラボレーション サービスを強化して、以下も実現できます。

- Cisco WebEx Messenger サービスを使用したインスタント メッセージング（IM）とプレゼンス
- Cisco WebEx Meetings サービスを使用した、デスクトップ共有による音声およびビデオ会議

Cisco WebEx のハイブリッド統合はこの章ではとりあげません。

Cisco WebEx Collaboration Cloud およびハイブリッドの企業のコラボレーションの統合の詳細については、Cisco WebEx Software as a Service（11-28 ページ）のセクションを参照してください。

Cisco WebEx Messenger とハイブリッドの企業の統合の詳細については、Cisco WebEx Messenger（20-68 ページ）のセクションを参照してください。

Cisco Spark Hybrid Services

Cisco Collaboration Cloud で実現される Cisco Spark のハイブリッド コラボレーション サービス統合は次のとおりです。

- Cisco Spark アイデンティティ サービス（21-39 ページ）
- Cisco Spark カレンダー サービス（21-41 ページ）
- Cisco Spark コール サービス（21-44 ページ）

Cisco Spark Hybrid Services に関する一般的な情報については、https://collaborationhelp.cisco.com/article/en-us/DOC-6433 に掲載されている基本情報を参照してください。

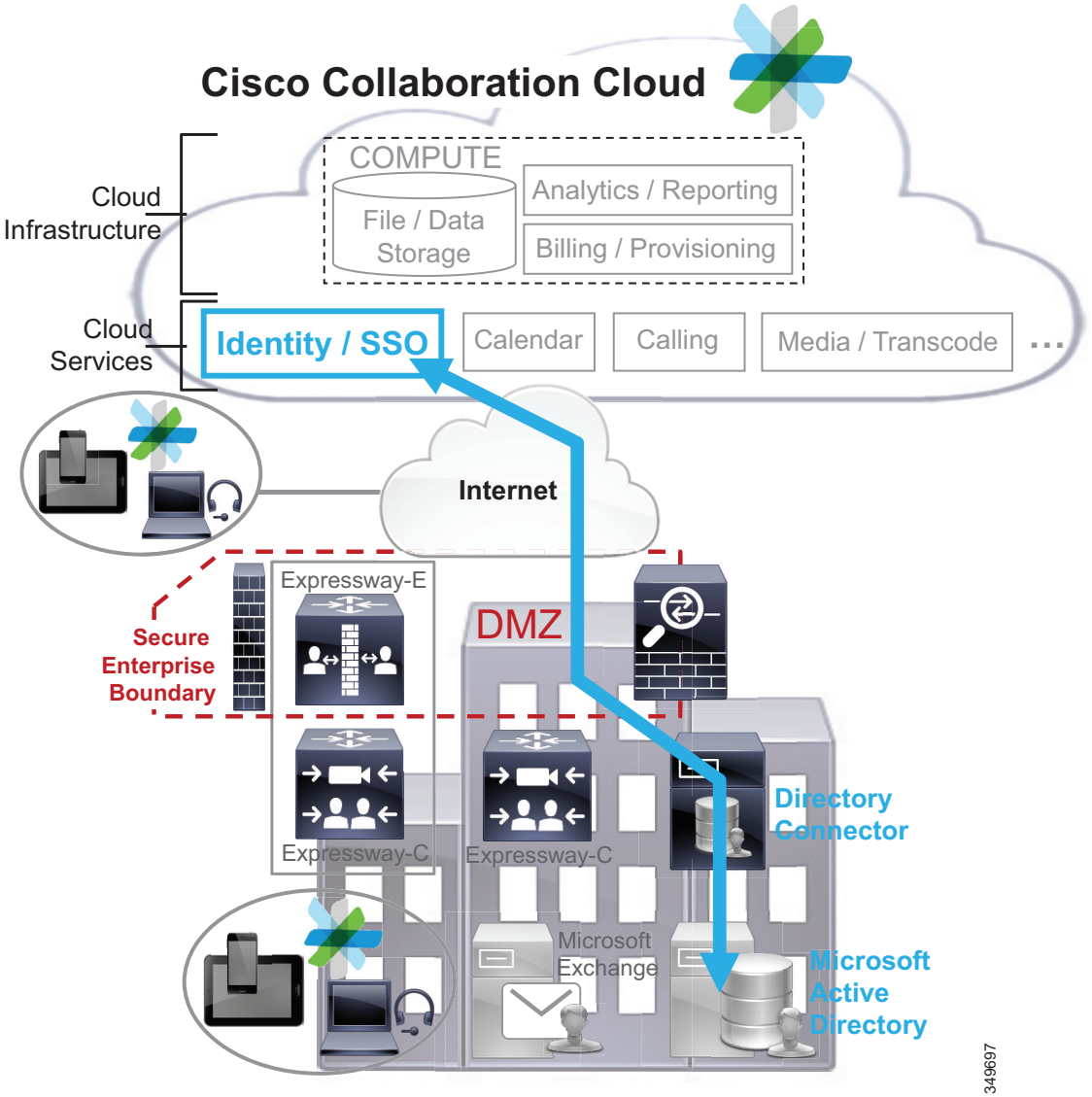
Cisco Spark アイデンティティ サービス

Cisco Spark Hybrid Services は、企業のオンプレミス Microsoft Active Directory を Cisco Collaboration Cloud Common Identity Services（CIS）と統合するためのメカニズムを提供します。エンタープライズ ディレクトリ情報をクラウドの CIS と同期することで、組織はシスコ クラウドための企業ユーザの設定とプロビジョニングを迅速に実現できます。企業が Cisco Spark Hybrid Services のシングル サインオン（SSO）を実装または統合する場合には、クラウドのアイデンティティ サービスに SSO 機能も含まれることに注意してください。

図 21-14 に示すように、オンプレミスの Cisco Directory Connector は、Microsoft Active Directory とエンタープライズ ネットワークを介して通信し、同期します。次に、Directory Connector はディレクトリ データをプッシュし、セキュアな企業境界および企業のファイアウォールを通って、インターネットを介しクラウド アイデンティティ（CIS）および SSO サービスと通信します。クラウドへのこの接続は企業内から開始され、企業のファイアウォールでポートを開く必要はありません。これは、インターネット上の Web サーバへのアウトバウンド接続を開始し、同じ接続で応答を受信する HTTPS Web クライアントに似ています。

クラウドの CIS とオンプレミスの Cisco Directory Connector との間の通信には HTTPS が使用されます。Cisco Directory Connector と Microsoft Active Directory 間の同期には、Microsoft Active Directory API が使用されます。

図 21-14　Cisco Spark Hybrid Services：クラウド アイデンティティ サービスとエンタープライズ ディレクトリの統合



ユーザの同期に使用される CIS と Directory Connector 間の接続は、Directory Connector ソフトウェアのインストール中に自動的にセットアップされます。Directory Connector ソフトウェアは Cisco Spark Control Hub からダウンロードされます。ユーザ情報を同期するために使用される Directory Connector と Microsoft AD 間の接続は、Directory Connector 上の設定で制御されます。Directory Connector 管理ページのグラフィカル ユーザ インターフェイスを使用して、オブジェクト タイプ、LDAP フィールドのマッピング、ベース DN を設定し、どのユーザ アカウントでどのアカウント情報を同期するかを制御します。

Cisco Directory Connector ソフトウェアは Microsoft Windows Server オペレーティング システムが動作するサーバまたは仮想マシンにインストールして実行します。Cisco Directory Connector の導入には次の要件と推奨が適用されます。

- Microsoft Windows サーバまたは仮想マシンは、企業の Microsoft Active Directory ドメインのメンバーである必要があります。
- Directory Connector ソフトウェアはドメインの管理者権限を持つアカウントを使用して Windows サーバまたは仮想マシンにインストールする必要があります。
- Active Directory の電子メール アドレス属性は、Cisco CIS と同期するすべてのユーザ アカウントに設定される必要があります。電子メール アドレスのない Active Directory のユーザ アカウントは、CIS と同期されません。
- Directory Connector は、Active Directory Domain Service（AD DS）および Active Directory Lightweight Directory Service（AD LDS）とは別のサーバまたは仮想マシンにインストールすることを推奨します。

導入の要件、インストール、設定を含め、Cisco Directory Connector の詳細については、以下のリンク先から入手できる最新バージョンの『*Deployment Guide for Cisco Directory Connector*』を参照してください。

https://www.cisco.com/c/en/us/support/unified-communications/spark/products-installation-guides-list.html

企業ユーザがオンプレミス Microsoft Active Directory と Cisco Collaboration Cloud CIS の間で同期された後は、組織の管理者が Cisco Spark Control Hub を使用してユーザ アカウントを簡単に管理できます。管理者はこのハブからユーザ ロールを割り当て、ユーザ機能を管理し、Cisco Spark Hybrid Services などの特定のクラウド サービスに対してユーザに権限を付与したりユーザを有効にしたりします。

Cisco Spark カレンダー サービス

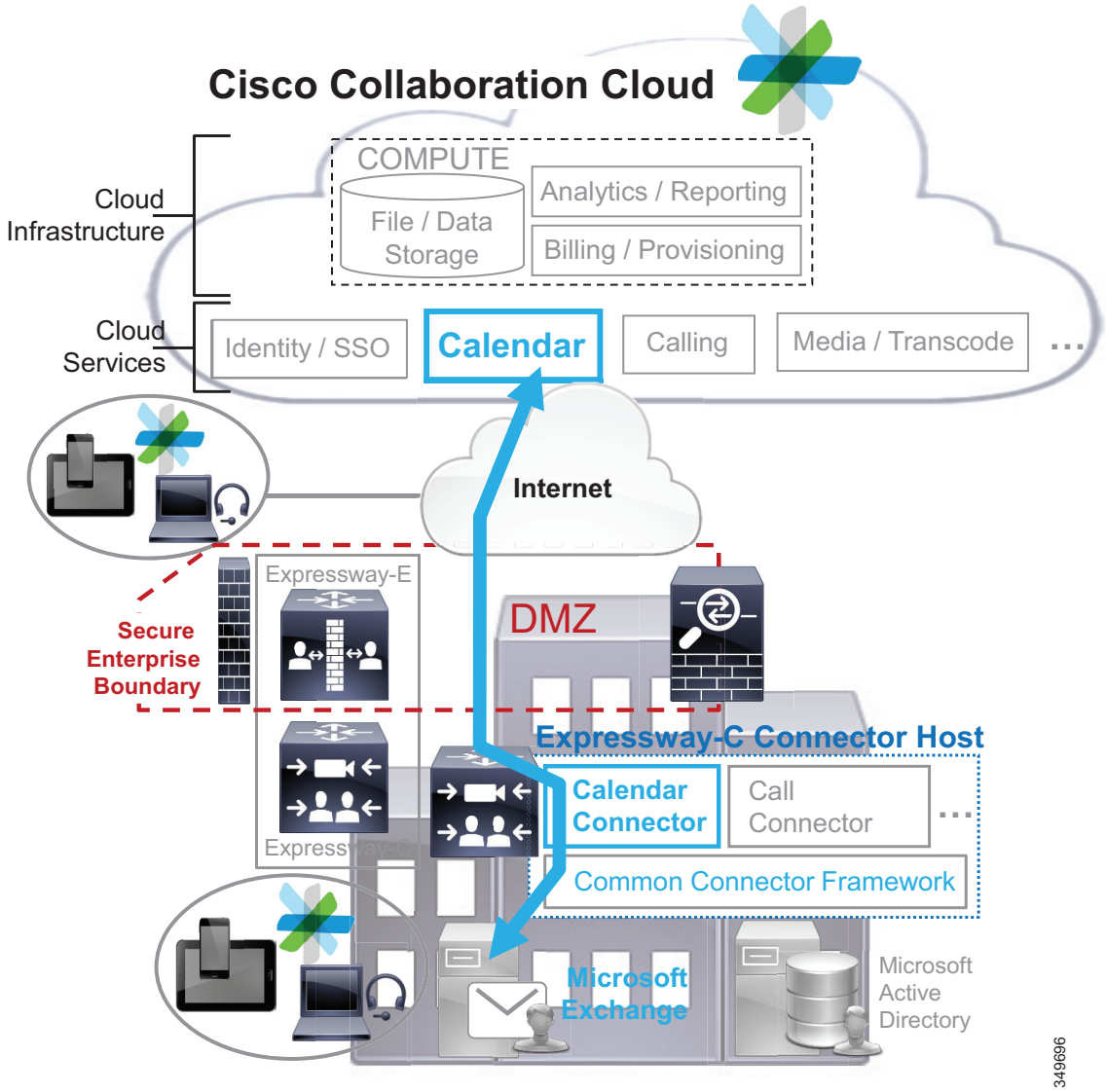
Cisco Spark Hybrid Services は、企業のオンプレミスの Microsoft Exchange の予定表機能を Cisco Collaboration Cloud のカレンダー サービスと統合するためのメカニズムを提供します。企業のカレンダー サービスを Cisco Collaboration Cloud に統合すると、組織は、会議の出席依頼の [ロケーション（location）] フィールドに @spark や @webex を含めるだけで、Outlook の会議の招待に Cisco Spark および Cisco WebEx の豊富なコラボレーション機能を自動的に組み込むことができます。

カレンダー コネクタは、クラウドのカレンダー サービスと企業の Exchange 環境間の統合とコミュニケーションの仲介を担当します。図 21-15 に示すように、基盤となる一般的なコネクタ フレームワークに依存するオンプレミス Cisco Expressway-C コネクタのホスト カレンダー コネクタは、エンタープライズ ネットワークで Microsoft Exchange と通信します。次に、カレンダー コネクタは予定表データをプッシュし、セキュアな企業の境界および企業のファイアウォールを通って、インターネットを介しクラウドのカレンダー サービスと通信します。クラウドへのこの接続は企業内から開始され、企業のファイアウォールでポートを開く必要はありません。これは、インターネット上の Web サーバへのアウトバウンド接続を開始し、同じ接続で応答を受信する HTTPS Web クライアントに似ています。

クラウドのカレンダー サービスとオンプレミスのカレンダー コネクタとの間の通信には HTTPS が使用されます。Expressway-C のカレンダー コネクタ コンポーネントと Microsoft Exchange 環境間の通信には Microsoft Exchange Web サービス（EWS）が使用されます。

カレンダー コネクタは Exchange 環境と通信を行い、通知をモニタしてユーザの予定表からの情報を取得し、Cisco Spark のルーム情報と WebEx ミーティング情報を会議の招待に追加します。

図 21-15　Cisco Spark Hybrid Services：企業予定表の統合



Expressway-C コネクタ ホストと Cisco Collaboration Cloud 間の接続と、クラウドのカレンダー サービスとカレンダー コネクタ間の接続は、Expressway-C のハイブリッド サービス コネクタの設定時に自動的に確立されます。Calendar Connector ソフトウェアは、Expressway-C を正常に登録した後（すでに登録されている場合は、カレンダー コネクタ サービスが Cisco Spark Control Hub から有効にされた時点で）、Cisco Collaboration Cloud から Expressway-C に自動的にダウンロードされ、インストールされます。

Expressway-C のグラフィカル ユーザ インターフェイスでのカレンダー コネクタの設定中に、Microsoft Exchange の接続情報を管理者が提供します（または、企業の Active Directory から取得されることもあります）。さらに管理者は、@webex が招待ロケーション フィールドに指定されたときに WebEx ミーティング ルームの詳細が会議の招待に追加されるよう、組織の WebEx Meeting Center と Collaboration Meeting Room のサイト情報を指定します。

Expressway-C および共通コネクタ フレームワークを利用する Cisco Spark Hybrid Services では Cisco Collaboration Cloud とオンプレミス Expressway-C との間のセキュアな接続が必要です。Expressway-C のカレンダー コネクタを動作させるために、コネクタ管理とカレンダー サービスのために Cisco Collaboration Cloud が提供する CA 署名付き証明書を Expressway-C の証明書信頼リストと照合します。これにより、Expressway-C と Collaboration Cloud 間のセキュアな接続が提供されます。Expressway-C は、Calendar Connector ソフトウェアをダウンロードしてカレンダー コネクタ サービスを開始する前に、クラウドの証明書を確認します。カレンダー コネクタ サービスはクラウドの証明書 CA が信頼リストにない場合、開始されません。クラウドは最初の設定時に、必要なクラウドのパブリック CA 証明書を Expressway-C の信頼リストに自動的に追加します。または、組織がクラウドの証明書を手動で管理することを選択する場合もあります。その場合は、Expressway の管理者がクラウドの CA 証明書を Expressway の信頼リストに追加して、正しい操作を確保します。任意で、Expressway-C のカレンダー コネクタと企業の Exchange サーバ間で CA 証明書を交換し、各サーバの信頼リストに追加すれば、セキュア接続が両者の間の接続にまで拡張されます。

カレンダー コネクタと Microsoft Exchange 間の適切な統合と通信を行うためには、偽装アカウントを使用する必要があります。このアカウントは、個々の予定表の会議情報を照会するために、ユーザに代わってカレンダー コネクタにより使用されます。カレンダー コネクタはユーザの電子メールや連絡先リストにアクセスするためにこのアカウントを使用しません。それで、Cisco Collaboration Cloud はコネクタから Exchange 環境の偽装アカウントの認証情報にアクセスしたりその情報を取得することはできません。さらに、Collaboration Cloud は企業の Exchange 環境に、直接的にもカレンダー コネクタを介してもアクセスできません。

カレンダー コネクタの導入には次の要件と推奨が適用されます。

- ハイブリッド サービスのユーザは Collaboration Cloud Common Identity Service（CIS）に対して認証されるため、Cisco Directory Connector および企業の Active Directory への統合が推奨されます。
- Cisco Spark Hybrid Services には、Cisco Expressway X8.7.1 以降のバージョンが必要です。
- カレンダー サービスの利用が許可されるユーザ数、個々のユーザの Exchange 予定表のサイズ、および @spark と @webex が使用されるレートにより、このサービスを有効にするときに Exchange サーバにかかる追加の負荷の量が決まります。Exchange の偽装アカウントにスロットリング ポリシーを作成して適用すると、企業の Exchange 環境へのカレンダー コネクタおよびカレンダー サービスの影響を低減できます。

導入の要件、インストール、設定を含め、カレンダー コネクタの詳細については、以下のリンク先から入手できる最新バージョンの『*Deployment Guide for Cisco Spark Hybrid Calendar Service*』を参照してください。

https://www.cisco.com/c/en/us/support/unified-communications/spark/products-installation-guides-list.html

カレンダー コネクタが実行され、ユーザが有効になると、有効になったユーザは Cisco Spark のコラボレーションを組み込み、WebEx ミーティング情報を Outlook 予定表の招待に追加できます。そのためには、次の手順を実行します。

- @spark

  @spark が Outlook 予定表の出席依頼の [ロケーション（location）] フィールドに追加されると、カレンダー コネクタとクラウドのカレンダー サービスは、その出席依頼の件名と一致する名前の付いた新しい Cisco Spark コラボレーション ルームを作成します。予定表の出席依頼にあるすべてのユーザは、この Cisco Spark のルームに追加されます。これによりコラボレーションが促進され、会議の主催者と出席者は会議前、会議中、そして会議後でも、やりとりを行ったり、資料を共有することができるようになります。予定表の出席依頼に配布リストが含まれている場合は、配布リストに掲載されたユーザは自動的に Cisco Spark ルームに追加されませんが、会議の招待は受け取ります。

- @webex：これを指定すると、WebEx ミーティング招待情報が Cisco Spark ルームに追加されます。

  @webex（複数の WebEx サイトを持つ組織の場合は @webex:<*サイト*>）を、Outlook 予定表の出席依頼の [ロケーション（location）] フィールドに追加すると、カレンダー コネクタにより、ユーザの WebEx コラボレーション会議室情報が招待に自動的に追加されます。WebEx ミーティング参加リンク（手動または WebEx の生産性向上ツールで追加されます）が、すでに予定表の招待に存在する場合、カレンダー コネクタは WebEx ミーティング情報を追加しません。

@webex を @spark と組み合わせて使用すると、WebEx ミーティング情報は予定表の会議の招待だけではなく、Cisco Spark ルームにも追加されます。

Cisco Spark コール サービス

Cisco Spark Hybrid Services により、Cisco Collaboration Cloud の通話サービスと企業のオンプレミス コール制御との統合が可能になりました。企業のコール サービスをクラウドに統合することにより、組織は既存のオンプレミス電話、コラボレーション クライアント、および Cisco Spark クライアント間でのデスクトップ共有と、音声通話、ビデオ通話を有効にできます。

図 21-16 に示すように、Cisco Spark のハイブリッド コール サービスには次の 3 つのエンタープライズ コンポーネントが必要です。

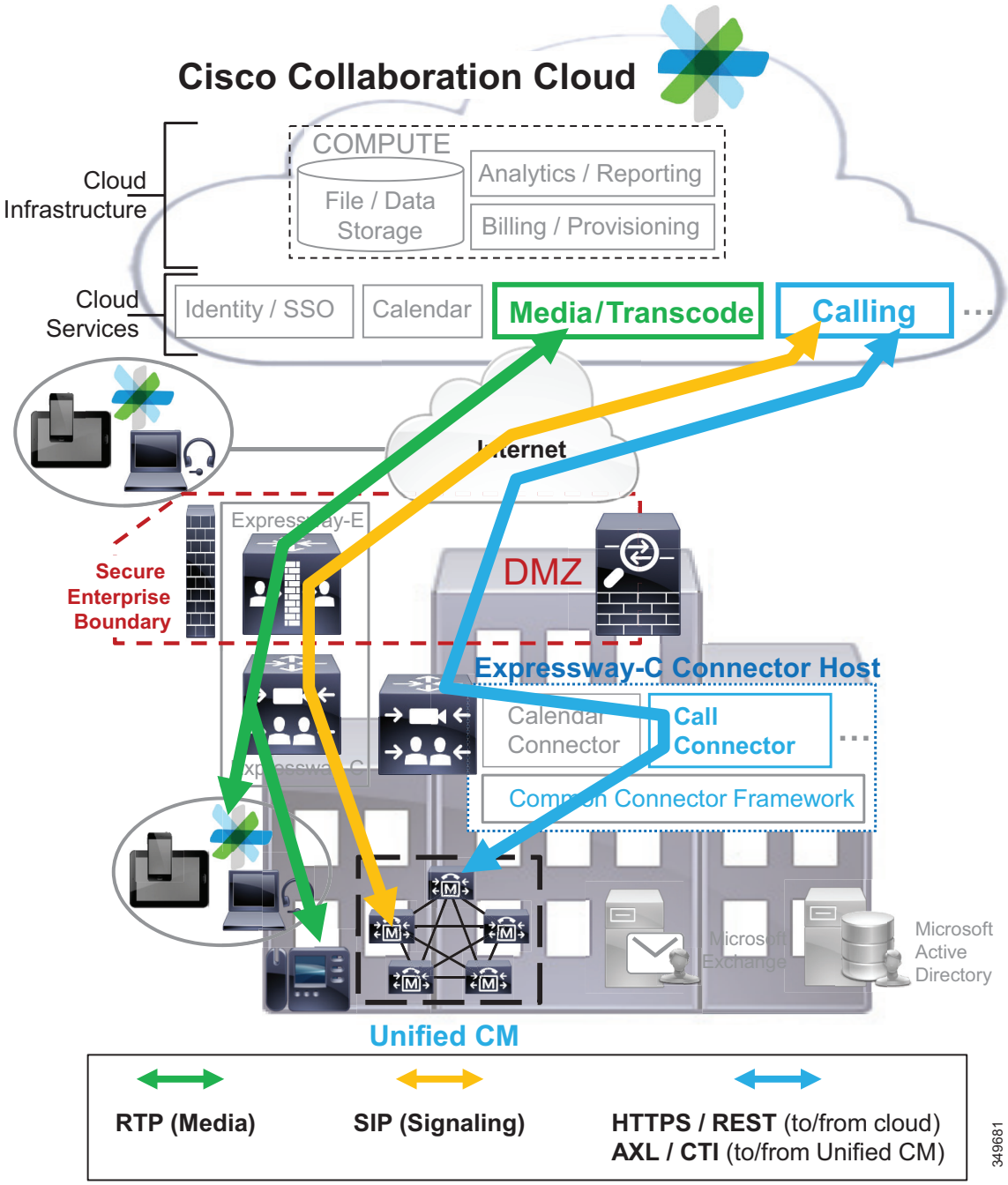
- Cisco Call Connector：このソフトウェアは Cisco Expressway-C コネクタ ホストで動作し、Cisco Collaboration Cloud の通話サービスと企業の Unified CM 展開との間の統合とコミュニケーションを調整します。
- Cisco Unified CM：これは企業のコール制御を担い、企業のエンドポイントとクライアント、および企業が接続しているクラウド クライアントの音声およびビデオ通話サービスと、PSTN 接続を提供します。企業のコール制御は、Cisco Business Edition 6000 または Cisco Hosted Collaboration System（HCS）で行うこともできます。
- Cisco Expressway-E と Expressway-C：このサーバ ペアはコール メディアおよびシグナリングにセキュアなエンタープライズ エッジ ファイアウォール トラバーサルを提供します。Expressway のモバイルおよびリモート アクセスや Business-to-Business（B2B）に使用される既存のサーバ ペアは、十分なコール キャパシティがあれば、利用できます。

Cisco Expressway-C コネクタ ホストにあるコール コネクタは、基本となる共通コネクタ フレームワークを使用して、エンタープライズ ネットワーク経由で Unified CM と通信します。他の企業のクラウド コネクタと同様に、コール コネクタはセキュアな企業の境界および企業のファイアウォールを通って、インターネットを介しクラウドと通信します。クラウドへのこの接続は企業内から開始され、企業のファイアウォールでポートを開く必要はありません。前述したように、これはインターネット上の Web サーバへのアウトバウンド接続を開始する HTTPS Web クライアントに似ています。

コール コネクタは REST ベースの HTTPS を使用して Cisco Collaboration Cloud の通話サービスと通信します。また、Administrative XML Layer（AXL）を使用して Unified CM と通信し、ユーザの企業デバイスの情報を取得するのに加えて、コンピュータ テレフォニー インテグレーション（CTI）を使用して、ユーザの企業回線をモニタします。

カレンダー コネクタと同様、Expressway-C コネクタ ホスト、コール コネクタ、Cisco Collaboration Cloud、およびクラウド通話サービスの間の接続は、Expressway-C でハイブリッド サービス コネクタを設定する際に自動的に確立されます。コール コネクタ ソフトウェアは、Expressway-C コネクタ ホストを正常に登録した後（すでに登録されている場合は、コール コネクタ サービスが Cisco Spark Control Hub と Expressway-C コネクタ ホストの両方から有効にされた時点で）、Cisco Collaboration Cloud から自動的にダウンロードされ、コネクタ ホストにインストールされます。

図 21-16　Cisco Spark Hybrid Services：企業の通話の統合



Cisco Spark Hybrid Services の通話は 2 つの機能を可能にします。

- コール サービス認識

  この機能は、Unified CM に登録済みのエンドポイントで、2 人の Cisco Spark が有効になっているユーザ間の通話に「ワンクリックで共有（one-click-to-share）」機能を提供します。2 人のユーザが企業の回線を使用して 1 対 1 で通話中に、クラウド通話サービスはハイブリッド サービスのコール コネクタから受信した情報に基づいてアクティブ コールを認識し、2 人のユーザ間の Cisco Spark ルームをリストの先頭に移動します（または、その 2 人の間に Cisco Spark ルールが作成されていなかった場合は、1 対 1 のルームを作成します）。そして、両方のユーザの Cisco Spark デスクトップ（または Web）クライアントのルーム内にあるデスクトップ共有ボタンを有効にします。どちらのユーザもこのボタンをクリックして、デスクトップを共有することができます。コール サービス認識を使用すると、Cisco Collaboration Cloud が Cisco Spark のコラボレーション ルームとデスクトップ共有を利用している間、1 対 1 通話のコール メディアとシグナリングは Unified CM と 2 つの企業デバイスでのみ処理されます。デスクトップの共有を可能にするだけでなく、コール サービス認識は統一されたコール履歴リストを Cisco Spark クライアントに提供します。

- コール サービス接続

  この機能により、Cisco Spark ユーザは企業のオンプレミス コール制御（Cisco Unified CM）を使用してコールを発信および受信できるようになります。この機能を設定すると、ユーザのエンタープライズ番号への着信コールは、Unified CM に登録されている電話機とクライアントだけでなく、Cisco Collaboration Cloud にも拡張されてユーザの Cisco Spark クライアントにルーティングされるため、ユーザは一番早く応答できるデバイス（企業の登録されたデスクフォンや、ユーザの携帯電話上で動作する Cisco Spark クライアントなど）を使用して、コールに応答することができます。同様に、Cisco Spark から発信された着信コールは、ユーザの Cisco Spark クライアントだけではなく、Cisco Collaboration Cloud によって企業の Unified CM にまで拡張され、Unified CM に登録されたユーザの各エンドポイントで呼び出し音が鳴ります。

  ユーザが Cisco Spark クライアントの通話タブ内で番号または URI を入力してコールを発信すると、そのコールは企業の Unified CM および必要に応じて企業の PSTN 接続を使用してルーティングされます。コール サービス接続は、コール サービス認識機能が同時に有効になっていないユーザに対しては、有効にすることはできません。

  コール サービス接続機能を有効にするには、各ユーザの Cisco Spark リモート デバイス（Spark RD）が Unified CM 内で設定されていなければなりません。このデバイスは、Cisco Collaboration Cloud のユーザを、リモート接続先として設定された企業 DN および Cisco Spark の通話 SIP URI と関連付けます。このデバイスの関連付けと、設定されたリモート接続先により、コールの発信元に応じてコールが Unified CM とコラボレーション クラウドの両方に分岐されます。Cisco Collaboration Cloud は SIP の連絡先ヘッダーとコール ルーティング ロジックを使用して、クラウドと企業コール制御間のコール分岐ループを防ぎます。

  （注）　Cisco Spark コール サービス接続の以前の導入では CTI リモート デバイスが使用されていましたが、現在の導入に適切な Unified CM デバイス タイプは Cisco Spark リモート デバイス（Spark RD）です。

  コール コネクタは Unified CM に Spark RD を登録します。この登録はコール コネクタが Cisco Collaboration Cloud に接続している限り、アクティブです。

コール サービス接続が有効になっていると、RTP コール メディアおよび SIP コール シグナリングは Expressway-E と Expressway-C サーバ ペアを使用して Cisco Collaboration Cloud との間でルーティングされます（図 21-16 を参照）。コール メディアは企業に接続されたエンドポイント（またはゲートウェイ）と Cisco Collaboration Cloud のメディアおよびトランスコーディング サービス間の Expressway-E および Expressway-C サーバを通過します。クラウド通話サービスと Unified CM 間の SIP シグナリングも、Expressway-E と Expressway-C サーバを通過します。コール サービス接続の RTP メディアと SIP シグナリングは既存のモバイルおよびリモート アクセス、または B2B Expressway-E と Expressway-C サーバを通過できます。または、専用のハイブリッド サービスの Expressway-E および Expressway-C サーバのセットを導入することもあります。

Cisco Spark のカレンダー サービスと全く同じように、Cisco Spark 通話サービスも Expressway-C コネクタ ホストと共通コネクタ フレームワーク間のセキュアな接続に依存します。そしてカレンダー コネクタ同様、コール コネクタを動作させるために、コネクタ管理とコール サービス用に Cisco Collaboration Cloud により提供された CA 署名付き証明書が、Expressway-C コネクタ ホストの証明書信頼リストと照合されます。Expressway-C コネクタ ホストは Call Connector ソフトウェアをダウンロードしてコネクタ サービスを開始する前に、クラウドの証明書を確認します。コール コネクタ サービスはクラウドの証明書 CA が信頼リストにない場合、開始されません。クラウドは最初の設定時に、必要なクラウドのパブリック CA 証明書を Expressway-C コネクタ ホストの信頼リストに自動的に追加します。または、クラウドの証明書を手動で管理することもできます。その場合は、管理者がクラウドの CA 証明書を Expressway-C コネクタ ホストの証明書信頼リストに追加する必要があります。

コール コネクタの導入には次の要件と推奨が適用されます。

- ハイブリッド サービスのユーザは Collaboration Cloud Common Identity Service（CIS）に対して認証されるため、Cisco Directory Connector および企業の Active Directory への統合が必要です。
- Cisco Spark Hybrid Services には、Cisco Expressway X8.7.1 以降のバージョンが必要です。
- コール サービス認識は、コール サービス接続機能の前提条件です。
- 高可用性を実現するためには、Cisco Spark コール サービスに必要な AXL Web サービスと CTIManager サービスが、少なくとも 2 つの Unified CM ノードで有効になっている必要があります。

導入の要件、インストール、設定を含め、コール コネクタの詳細については、以下のリンク先から入手できる最新バージョンの『*Deployment Guide for Cisco Spark Hybrid Call Services*』に記載されているコール サービス対応のセットアップに関する情報を参照してください。

https://www.cisco.com/c/en/us/support/unified-communications/expressway-series/products-installation-and-configuration-guides-list.html

クラウドおよびハイブリッド サービス モビリティのハイ アベイラビリティ

他の企業モビリティの機能とソリューション同様、クラウド サービスのハイ アベイラビリティを提供するためには、クラウドおよびハイブリッド サービスを冗長構成で設定および展開する必要があります。もともと、クラウドのインフラストラクチャとプラットフォームには復元力があります。ほとんどの管理型クラウド インフラストラクチャと同様、Cisco Collaboration Cloud と WebEx Cloud は、高度な RAID ストレージ アレイや電力網、持続的なデータのバックアップ、データ センター分散によるオンデマンド コンピューティング、および移行機能を使用して、可用性の高いクラウド サービスを確保しています。

ハイブリッド サービスを展開する場合、クラウドの復元力に加えて、オンプレミスのインフラストラクチャの冗長性も考慮する必要があります。エンタープライズ ネットワークやセキュアな企業の境界など、オンプレミスのエンタープライズ ネットワーク インフラストラクチャのコンポーネントを、可用性の高い形で配置することが重要です。WebEx Meeting Server、Expressway-C コネクタ ホスト、企業アプリケーション（Microsoft Exchange や Active Directory など）を含むコラボレーション コンポーネントは、冗長構成で配置する必要があります。

従来の Microsoft Exchange および Active Directory のハイ アベイラビリティ導入手法は、これらのアプリケーションが企業運用にとって重要であることを前提とすると、ほぼ間違いなく用意されています。用意されていない場合は、これらのアプリケーションの高可用性を実装することを検討してください。オンプレミスの Microsoft アプリケーションの高可用性は、ハイブリッド サービス統合にも適用されます。

クラウドおよびハイブリッド サービス モビリティのキャパシティ プランニング

クラウドおよびハイブリッド サービスの導入を成功させるには、クラウド サービスを使用するすべてのユーザに対して十分なキャパシティを用意することが必要です。クラウドのキャパシティはオンデマンドであり、クラウド コンピューティングとストレージの柔軟性を考えると事実上無限である一方で、権限付与のコストを検討する必要があります。

ハイブリッド統合に伴い、企業のオンプレミス インフラストラクチャを前提として、拡張性に関する新たな考慮事項が生じます。Microsoft アプリケーション（Exchange と Active Directory）の場合は、容量に関連する Microsoft のガイダンスに従い、既存のオンプレミス使用量を超えるハイブリッド サービスの追加オーバーヘッドに対して適切なキャパシティが提供されるようにします。特に、サーバ リソースのオーバーサブスクリプションを回避するために、Exchange サーバのスロットリング ポリシーを実装することが重要です。

Expressway-C ノード（大規模な OVA または大規模アプライアンス）は最大 5,000 人のクラウド ハイブリッド サービス ユーザをサポートします。

また、Directory Connector の場合、多数のユーザをコラボレーション クラウド CIS と同期しようとしている企業は、他のアプリケーションやサービスを企業に提供するために使用されてるのではない大容量の Windows サーバ（仮想マシンまたはハードウェア）に、Directory Connector を導入する必要があります。

いずれの状況でも、重要なオンプレミス コラボレーション インフラストラクチャのコンポーネント（Exchange、Active Directory、Directory Connector、Expressway-C、および WebEx Meeting Server）をモニタすることが重要です。また、サーバや仮想マシンの故障時や、CPU やメモリ使用量が定期的にクリティカル レベルになる際には、より多くのリソースを追加し、負荷を分散することを検討してください。

クラウドおよびハイブリッド サービス モビリティの設計に関する考慮事項

クラウド サービスとハイブリッド サービスを実現し、導入する際には、次の設計要件と推奨事項を考慮してください。

- Cisco Directory Connector ソフトウェアは、企業の Active Directory ドメインのメンバーである Microsoft Windows サーバに、ドメインの管理者権限のあるアカウントを使用してインストールする必要があります。
- Cisco Directory Connector は Active Directory Domain Service（AD DS）または Active Directory Lightweight Directory Services（AD LDS）が有効な Windows サーバにインストールしてはなりません。
- Cisco Spark Hybrid Services の認証には、Cisco Directory Connector と企業の Active Directory を統合することをお勧めします。
- Cisco Spark Hybrid Services には、Cisco Expressway X8.7.1 以降のバージョンが必要です。
- カレンダー サービスが有効なユーザ数、個々のユーザの Exchange 予定表のサイズ、および @spark と @webex が使用されるレートにより、Cisco Spark カレンダー サービスを有効にするときに Exchange サーバにかかる追加の負荷の量が決まります。Exchange の偽装アカウントにスロットリング ポリシーを作成して適用すると、企業の Exchange 環境へのカレンダー コネクタおよびカレンダー サービスの影響を低減できます。
- ユーザに対してコール サービス接続機能を有効にするには、コール サービス認識を有効にする必要があります。
- Cisco Spark コール サービスには Unified CM AXL Web サービスと CTIManager サービスが必要であり、これらのサービスの高可用性を実現するためには、少なくとも 2 つの Unified CM ノードで有効になっている必要があります。

Cisco Collaboration Cloud および Cisco Spark Hybrid Services の詳細については、https://collaborationhelp.cisco.com/article/en-us/nkg4mud に掲載されている Cisco Spark の情報を参照してください。

Cisco Spark Hybrid Services のデプロイに関する詳細は、https://www.cisco.com/go/pa から入手できる最新バージョンの『*Preferred Architecture for Cisco Spark Hybrid Services, CVD*』を参照してください。

社外型モビリティ

Cisco のモバイル コラボレーション ソリューションを使用すると、モバイル ユーザは、デスクフォンだけでなく、1 台以上のリモート電話機でも会社の電話番号へのコールを処理できます。また、モビリティ ユーザは、まるで社内から電話をかけているかのようにリモート電話機から電話をかけることもできます。さらに、モビリティ ユーザは、保留、転送、会議などのエンタープライズ機能だけでなく、携帯電話上でのボイスメール、会議、プレゼンスなどのエンタープライズ アプリケーションも利用できます。これによって、ユーザは外出先でも生産性を持続させることができます。

さらに、モバイル音声ネットワークやモバイル データ ネットワークおよび 802.11 WLAN への接続を提供するデュアルモード電話を使用すると、ユーザは社外で企業アプリケーションを利用できるだけでなく、社内にいるとき、またはエンタープライズ ネットワークにリモート接続されているときにエンタープライズ テレフォニー インフラストラクチャを利用して、モバイル音声ネットワークの分単位の料金を支払わずにコールの発信と受信を行うことができます。

Cisco Unified Mobility ソリューション内に配布される Fixed Mobile Convergence（FMC）モビリティ機能は、Cisco Unified CM によって提供され、Cisco Jabber などの Cisco Mobile クライアントと併用できます。

Cisco Unified Mobility では、次のモビリティ アプリケーション機能が提供されます。

- シングル ナンバー リーチ（SNR）

  シングル ナンバー リーチを使用すれば、1 つの会社の電話番号でユーザの IP デスクフォンと携帯電話の両方を同時に呼び出すことができます。SNR ユーザは、着信コールをデスクフォンでも携帯電話でも受けることができ、通話中のコールを妨げることなく別の電話に転送できます。

- 通話切替機能

  通話切替機能により、モビリティ コールの通話中に、携帯電話の保留、保留解除、転送、会議、およびリダイレクト コール パーク機能を呼び出すことができます。これらの機能は、携帯電話のキーによって呼び出され、保留音やカンファレンス ブリッジといった企業のメディア リソースを活用します。

- シングル企業ボイスメール ボックス

  シングル企業ボイスメール ボックスは、モバイル ボイスメール回避機能を提供し、ユーザの会社の電話番号に着信し、さらに携帯電話に転送されたコールに応答がなかった場合に、携帯電話のボイスメール システムではなく、会社のボイスメール システムにコールを蓄積します。これにより、ボイスメール ボックスが 1 箇所に統合され、ユーザは複数のボイスメール システムでメッセージを確認する必要がなくなります。

- モバイル音声アクセスとエンタープライズ機能アクセスの 2 段階ダイヤリング

  モバイル音声アクセスとエンタープライズ機能アクセスの 2 段階ダイヤリングによって、まるで会社の IP デスクフォンからかけているかのように、携帯電話から発信できます。長距離電話や国際電話、または通常は企業外部から到達不能なシステム上の内部の DID 以外の内線番号へのコールにおいてこれらの機能を使用すると、通話料金を節約できます。また、企業でこれらの 2 ステージ ダイヤリング機能を使用すると、中央で一括管理されたコール詳細レコードによって、ユーザのコール発信を容易に追跡管理できるようになります。さらに、これらの機能によって、発信者 ID を送信する際にユーザの携帯電話番号を隠すことができます。代わりに、発信者 ID として、ユーザの会社の電話番号が送信されます。これによって、ユーザへの返信コールは会社の電話番号にかけられるため、コールを会社で一括管理できます。

Cisco Mobile クライアントおよびデバイスは、音声とデータ接続用のモバイル プロバイダー ネットワークおよび 802.11 のワイヤレス ネットワークの両方に接続できる機能を提供します。これは、ユーザが 1 つのデバイスから両方のエンタープライズ コール制御、場合によってはモバイル ネットワークのコール制御を利用できるようにします。可能であれば、コールを送受信するための企業のテレフォニー インフラストラクチャを利用することによって、また、デュアル モード電話機の場合は企業接続が利用できないときだけにモバイル音声ネットワークに戻ることによって、モバイル クライアントおよびデバイスは、テレフォニーのコストの削減を支援できます。また、デュアルモード電話、およびそこで実行されるクライアントには、ハンドオフ メカニズムが備えられているため、ユーザが社外に移動した場合に、通話中のボイスコールにおいて、WLAN インターフェイスとモバイル音声インターフェイスを簡単に切り替えることができます。

Cisco Mobile クライアントでは、モバイル デバイスを有効にして、802.11 WLAN の IP 経由またはモバイル データ ネットワーク経由で音声またはビデオ コールを発信できるようにすることに加え、Dial via Office 機能を使用した企業の自動化ダイヤリングも有効にしました。Dial via Office コールは、IP ネットワーク経由の SIP シグナリングを使用して設定され、一方メディア パスは、モバイル音声ネットワークおよび PSTN 経由で設定されます。シスコのモバイル クライアントとデバイスは、社内ディレクトリ アクセス、プレゼンスおよびインスタント メッセージング（IM）などの他の Unified Communications サービスも提供します。これらのデバイスとクライアントでは、モバイル ユーザは、コラボレーション アプリケーションへのアクセスを提供することによって社内、社外にかかわらず生産性を維持できると同時に、ユーザは、パブリックまたはプライベートの WiFi モバイル ホット スポットやモバイル データ ネットワーク、社内で WLAN 経由にかかわらず、モバイル デバイスからエンタープライズ コールを送受信できます。

この項では、まず、Unified Mobility の特徴、機能、および設計と配置に関する考慮事項について説明します。Unified Mobility のさまざまなメリットおよびモバイル クライアントとデバイスを統合することによってその機能が利用できるという事実を前提として、Cisco Jabber などのモバイル クライアント アプリケーションを検証します。この項には、次のモビリティ アプリケーションおよび機能のアーキテクチャ、機能性、および設計と配置の意味に関する説明も含まれます。

- Cisco Unified Mobility（21-51 ページ）
- シスコのモバイル クライアントおよびデバイス（21-81 ページ）

Cisco Unified Mobility

Cisco Unified Mobility は、Cisco Unified CM に組み込まれたネイティブなモビリティ機能を意味し、シングル ナンバー リーチ、モバイル音声アクセス、およびエンタープライズ機能アクセスの各機能が含まれます。

Unified Mobility の機能は、Unified CM の設定によって異なります。したがって、この設定だけでなく、論理コンポーネントの特性も理解することが重要です。

図 21-17 に、Unified Mobility に関する設定要件を示します。まず、ユーザに関しては、モビリティ ユーザの会社の電話機は、電話番号、パーティション、通話サーチ スペースなどの該当する回線レベル設定値を使用して設定されます。この他に、会社の電話機のデバイス レベルの設定には、デバイス プール、共通デバイス設定、コーリング サーチ スペース、メディア リソース グループ リスト、ユーザとネットワークの保留音源などのパラメータが含まれます。ユーザの会社の電話機に関するこれらの回線およびデバイス設定のすべてが、着信コールと発信コールのコール ルーティングや保留音（MoH）の動作に影響を与えます。

次に、Unified Mobility 機能が利用できるように、モビリティ ユーザごとのリモート接続先プロファイルを設定する必要があります。リモート接続先プロファイルは、ユーザの会社の電話回線と同じ電話番号、パーティション、および通話サーチ スペースを使用して回線レベルで設定します。これによって、リモート接続先プロファイルと会社の電話機の間で回線が共有されます。リモート接続先プロファイル設定には、デバイス プール、コーリング サーチ スペース、コーリング サーチ スペースの再ルーティング、およびユーザとネットワークの保留音源に関するパラメータが含まれます。リモート接続先プロファイルは、その設定にユーザの回線レベルの会社の電話機の設定が反映されますが、回線レベルの設定とプロファイル レベルの設定を組み合わせることによって、ユーザのリモート接続先電話機に継承されるコール ルーティングおよび MoH 動作が決定される仮想電話機と見なす必要があります。リモート接続先プロファイルと会社の電話機の間で共有されるユーザの会社の電話番号を使用すれば、その番号に電話することによってユーザのリモート接続先に転送できます。

図 21-17　Cisco Unified Mobility の設定アーキテクチャ

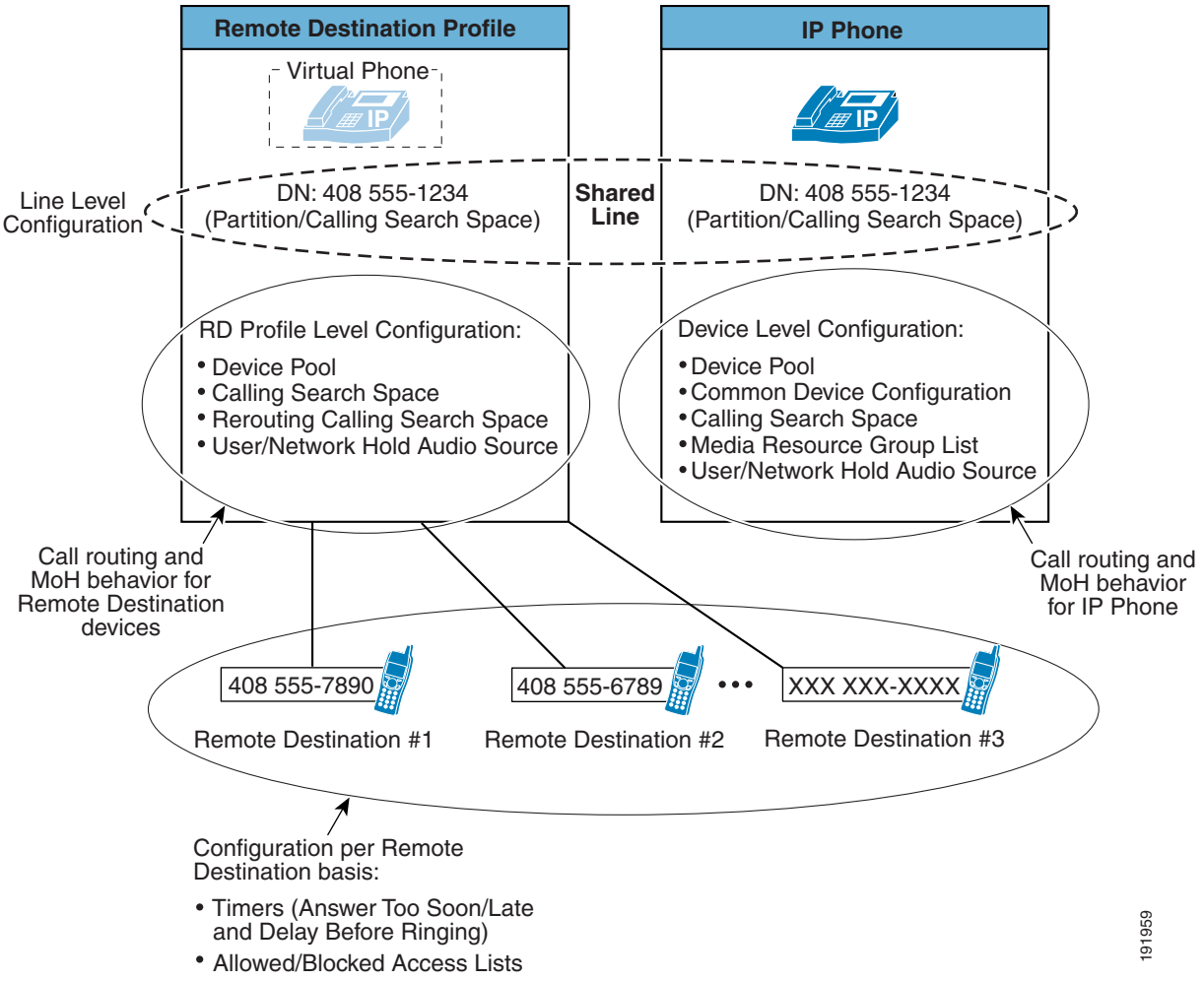


図 21-17 に示すように、モビリティ ユーザは、1 つまたは複数のリモート接続先をリモート接続先プロファイルに関連付けることができます。リモート接続先は、ユーザを呼び出すための単一の PSTN 電話番号を表しています。ユーザは、最大で 10 個のリモート接続先を定義できます。リモート接続先ごとにコール ルーティング タイマーを設定して、コールを特定のリモート電話に転送する時間だけでなく、コールを転送する前に待機する時間とリモート電話でコールを受ける準備ができるまでの時間を調整できます。また、モビリティ ユーザは、リモート接続先ごとに、リモート電話に転送する特定の電話番号からのコールを許可または拒否するフィルタを設定できます。

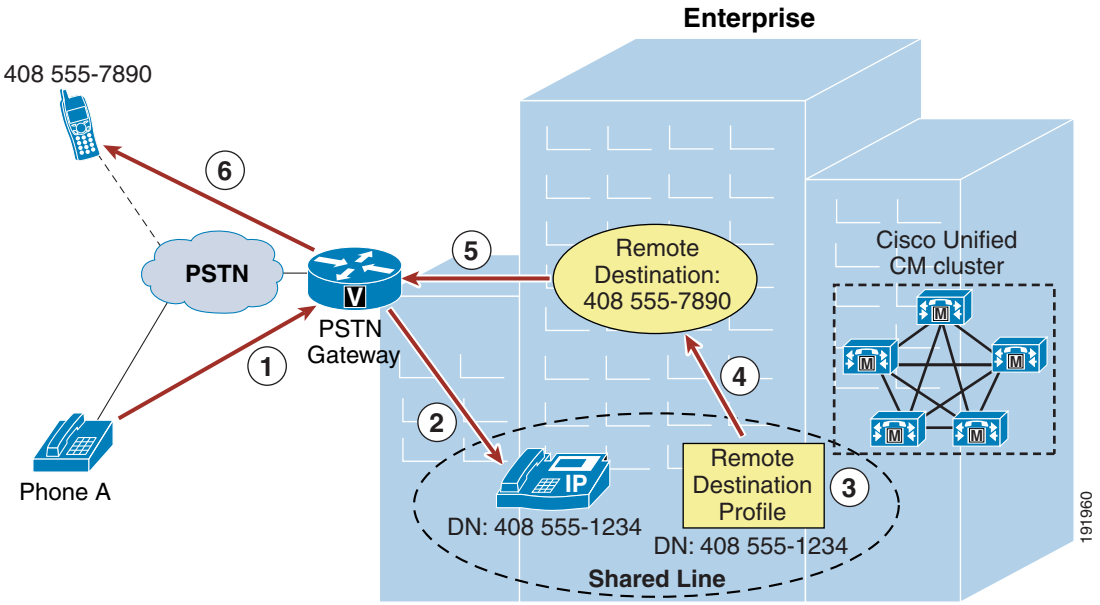
シングル ナンバー リーチ

シングル ナンバー リーチ（SNR）機能を使用すれば、企業ユーザへの着信コールをそのユーザの IP デスク フォンのほかに、最大 10 個の設定可能なリモート接続先に転送できます。一般的に、ユーザのリモート接続先は携帯電話です。コールがデスクトップフォンとリモート接続先電話機の両方に転送されれば、ユーザはどちらかの電話機で応答できます。ユーザは、リモート接続先電話機のいずれかまたは IP デスクトップフォンでコールに応答したときに、そのコールを別の電話機でハンドオフするか、ピックアップするかを選択できます。

シングル ナンバー リーチ機能

図 21-18 に、シングル ナンバー リーチの基本的なコール フローを示します。この例では、PSTN 上の電話機 A から SNR ユーザの会社の電話番号（DN）408-555-1234 に電話をかけます（ステップ 1）。コールが会社の PSTN ゲートウェイから Unified CM を経由して DN 408-555-1234 の IP フォンに転送され（ステップ 2）、この電話が鳴り出します。コールは、同じ DN を共有するユーザのリモート接続先プロファイルにも転送されます（ステップ 3）。次に、コールがユーザのリモート接続先プロファイルに関連付けられたリモート接続先（この場合は 408-555-7890）に発信されます（ステップ 4）。リモート接続先への発信コールが PSTN ゲートウェイを介してルーティングされます（ステップ 5）。最後に、番号が 408 555-7890 のリモート接続先 PSTN 電話機で呼出音が鳴ります（ステップ 6）。どちらの電話機でも応答できます。

図 21-18　　シングル ナンバー リーチ



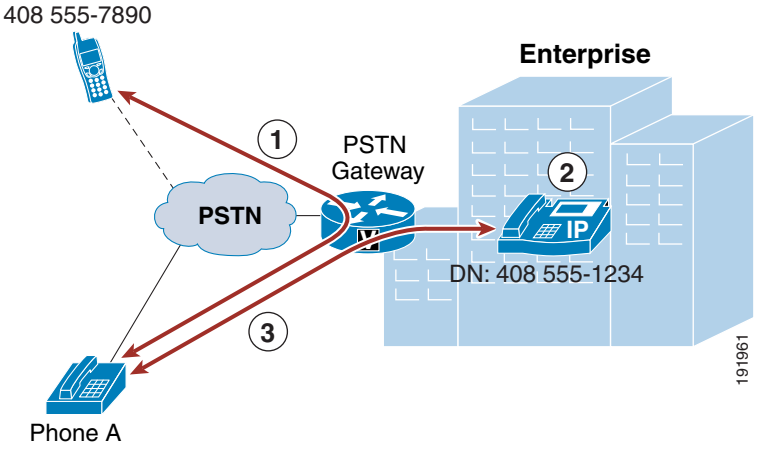
通常、シングル ナンバー リーチ ユーザの設定済みリモート接続先は、モバイル ボイス ネットワークまたはセルラー プロバイダー ネットワーク上の携帯電話です。ただし、PSTN により到達可能な任意の接続先をユーザのリモート接続先として設定できます。さらに、SNR ユーザは 10 件までリモート接続先を設定できるため、着信コールは最大で 10 台の PSTN 電話機とユーザのデスク フォンを呼び出すことができます。デスクトップフォンまたはリモート接続先電話機のいずれかでコールに応答すると、他のリモート接続先またはデスクトップフォン（デスクトップフォンで応答しなかった場合）に転送されたすべてのコール レッグがクリアされます。リモート接続先で着信コールに応答した場合は、2 つのゲートウェイ ポートを使用している会社の PSTN ゲートウェイ内で音声メディア パスがヘアピンされます。SNR 機能を配置する場合はこの利用を考慮する必要があります。

（注）　図 21-18 に示すようにシングル ナンバー リーチを動作させるには、[エンドユーザ（End User）] 設定ページでユーザ レベルの [モビリティの有効化（Enable Mobility）] チェックボックスがオンになっており、少なくとも 1 つのユーザの設定済みリモート接続先で [シングルナンバーリーチを有効にする（Enable Single Number Reach）] チェックボックスがオンになっていることを確認します。

デスク フォンのピックアップ

図 21-19 に示すように、ユーザがリモート接続先デバイスでシングル ナンバー リーチに応答した場合（ステップ 1：この場合は 408 555-7890）は、ユーザはデスク フォンの [再開（Resume）] ソフトキーを押すだけで、いつでもリモート接続先でコールをいったん切ってから、デスク フォンでピックアップできます（ステップ 2：この場合は DN 408 555-1234）。電話機 A を使用している元の発信者とデスクトップフォンとの間でコールが再開されます（ステップ 3）。

図 21-19　デスクトップフォンのピックアップ



デスクトップフォンのピックアップは、設定済みのリモート接続先電話機で会社の固定コールの通話が行われた後、その電話が切られた場合にいつでも実行できます。

（注）　会社の固定コールとは、会社の PSTN ゲートウェイ経由で接続された少なくとも 1 つのコール レッグがあり、リモート接続先から会社の DID に発信された、あるいはシングル ナンバー リーチ、モバイル ボイス アクセス、エンタープライズ機能アクセス、または Intelligent Session Control によって発信されたすべてのコールを指します。

デスクトップフォンでコールをピックアップまたは保留解除するためのオプションは、一定時間しか使用できません。そのため、シングル ナンバー リーチ ユーザは、必ず、着信電話機が切れていることを確認してから、リモート接続先電話機を切るようにしてください。これによって、他の誰かがデスクトップフォンでコールを保留解除できないことが保証されます。デフォルトで、リモート接続先電話機が切られてから 10 秒間はコールをデスクトップフォンでピックアップできます。ただし、この時間は設定可能であり、[End User] 設定ページで Maximum Wait Time for Desk Pickup パラメータを変更することによって、ユーザごとに 0 ～ 30,000 ミリ秒に設定できます。デスクトップフォンのピックアップは、リモート接続先電話機で通話切替保留機能を呼び出した後でも実行できます。ただし、このような場合は、Maximum Wait Time for Desk Pickup パラメータの設定が、ピックアップに使用できる時間に影響しません。通話切替保留されたコールは、リモート電話機とデスクトップフォンのどちらかで手動で保留解除されるまで、保留のままで、デスクトップフォンでピックアップできます。

デスクトップフォンのピックアップを実行するもう 1 つの方法に、通話切替セッション ハンドオフ機能を使用する方法があります。この通話切替機能は、セッション ハンドオフのデフォルトのエンタープライズ機能アクセス コードである *74 を手動で入力することによって呼び出します。これにより、Unified CM への DTMF シーケンスが生成されます。この機能が呼び出されると、Unified CM からユーザの会社のデスクトップフォンに新しいコールが送信されます。ユーザは、セッション ハンドオフを完了させるために、この新しいコールがデスクトップフォンの点滅表示または呼出音によって通知されたらこのコールに応答する必要があります。

デスクトップフォンのピックアップを行う場合にこの方法を使用すると、他の方法（携帯電話でコールを切断する方法や通話切替保留機能を使用する方法など）と比較して、ユーザと遠端の電話機との間の会話がハンドオフ プロセス中にも維持されるという利点があります。*74 シーケンスを入力すると、ハンドオフ コールがユーザのデスクトップフォンに送信されるため、ユーザは会話を継続できます。ユーザがデスクトップフォンでコールに応答すると、コール レッグが切り替えられて、遠端へのコール レッグが、デスクトップフォンに作成された新しいコール レッグに接続されます。これにより、音声パスが切断されずに、またはほぼ瞬間的にカットスルーされます。モバイル デバイスの元のコール レッグは、後でクリアされます。

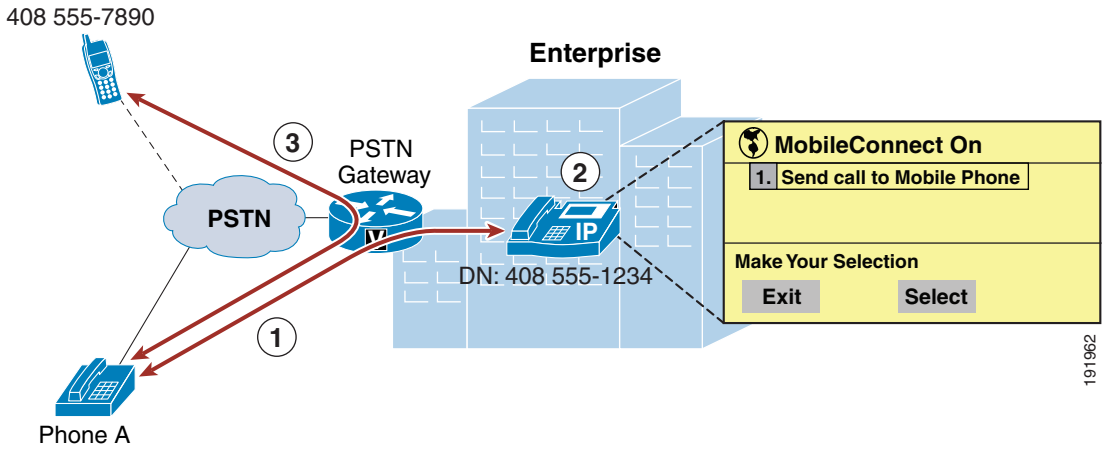
コールを切断してデスク フォンのピックアップを呼び出す方法では、エンド ユーザの [デスクフォンピックアップの最大待機時間（Maximum Wait Time for Desk Pickup）] の設定によってデスク フォンでコールをピックアップできる時間が決定されます。一方、セッション ハンドオフでは、[セッションハンドオフアラートタイマー（Session Handoff Alerting Timer）] サービス パラメータによって、デスク フォンでどの程度の時間呼出音または点滅表示によってコールが通知された後にハンドオフ コールがクリアされるかが決定されます。デフォルトのハンドオフ アラート時間は 10 秒です。また、セッション ハンドオフでは、デスクトップフォンに設定されたどの自動転送設定も関与しません。その結果、ハンドオフ機能では、ボイスメールやその他の自動転送宛先への転送は行われません。Session Handoff Alerting Timer 期間を経過してもコールに応答しないと、コールはクリアされて、ユーザのデスクフォン回線から Remote In Use 状態が削除されます。ただし、このシナリオでは、携帯電話の元のコールは維持されます。

セッション ハンドオフおよびその他の通話切替機能の詳細については、通話切替機能（21-56 ページ）を参照してください。

リモート接続先電話のピックアップ

図 21-20 に、シングル ナンバー リーチのリモート接続先電話のピックアップ機能を示します。電話機 A から SNR ユーザの会社の DN 408 555-1234 にコールを発信し、そのユーザがデスク フォンで応答してコールが通話中になっている場合（ステップ 1）は、ユーザは [モビリティ（Mobility）] ソフトキーを押す必要があります。この電話機で SNR 機能が有効になっており、リモート接続先ピックアップが使用できる場合、ユーザは [選択（Select）] ソフトキーを押します（ステップ 2）。ユーザのリモート接続先電話機に対するコール（この場合は 408 555-7890）が実行され、リモート電話機が鳴り出します。リモート電話機でコールが応答されると、電話機 A と、番号が 408 555-7890 の SNR ユーザのリモート電話機との間でコールが再開されます（ステップ 3）。

図 21-20　　リモート接続先電話のピックアップ



シングル ナンバー リーチ ユーザに対して複数のリモート接続先が設定されている場合は、[選択(Select)] ソフトキーを押したときに各リモート接続先が呼び出され、ユーザは好きな電話機をピックアップできます。

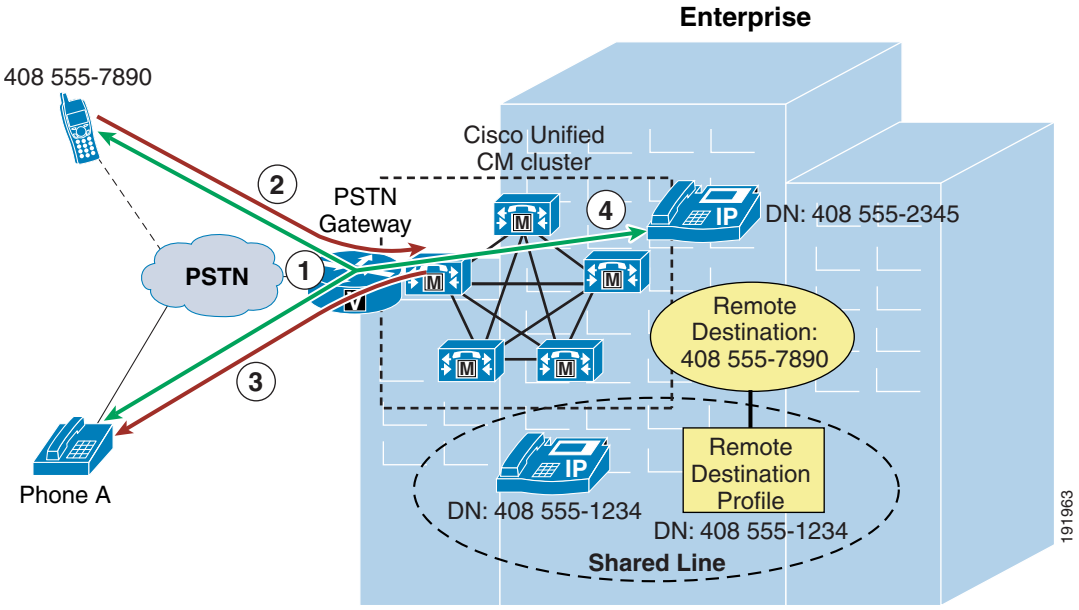
(注)　図 21-20 に示すように、リモート接続先電話機のピックアップを動作させるには、1 つ以上のユーザの設定済みリモート接続先で [Mobile Phone] チェックボックスがオンになっていることを確認してください。加えて、[Mobility] ソフトキーをすべてのモビリティ ユーザの関連するデスクトップフォン ソフトキー テンプレートに追加する必要があります。[Mobile Phone] チェックボックスをオンにして、Mobility ユーザが [Mobility] ソフトキーを使用できるようにしなければ、リモート接続先電話機のピックアップ機能が使用できません。

(注)　Cisco TelePresence System の C、EX、MX、SX、TX の各シリーズのビデオ エンドポイントは、上述のリモート接続先のピックアップをサポートしていません。これらのエンドポイントでは、モビリティ ソフトキーまたは [Send call to Mobile Phone] オプションはユーザから見えないようになっています。したがって、これらのエンドポイントは、リモート接続先のピック アップを使用してモバイル デバイスに進行中のコールを送信できません。

通話切替機能

図 21-21 に示すように、ユーザがリモート接続先デバイスでシングル ナンバー リーチ コールに応答(ステップ 1:この場合は 408 555-7890)したら、会社の PSTN ゲートウェイ経由でリモート接続先電話機から Unified CM に DTMF 番号を送信することによって、保留、保留解除、転送、会議、ダイレクト コール パーク、セッション ハンドオフなどの通話切替機能を呼び出すことができます(ステップ 2)。通話切替機能の保留、転送、会議、またはダイレクト コール パークが呼び出されると、Unified CM から電話の相手に MoH が送信されます(ステップ 3:この場合は電話機 A)。通話中のコールを別の電話機やダイレクト コール パーク番号に転送したり、会社の会議リソースを使用して新しい電話機で会議に参加できます(ステップ 4)。

図 21-21　　モビリティ通話切替機能



Unified CM に転送された一連の DTMF 番号によって、リモート接続先電話機で通話切替機能が呼び出されます。Unified CM で受信されるこれらの番号シーケンスが、設定済みの保留、独占保留、保留解除、転送、会議、およびセッション ハンドオフ用のエンタープライズ機能アクセス コードと照合され、該当する機能が実行されます。

(注)　ダイレクト コール パークの通話切替機能を有効にするには、ダイレクト コール パーク番号とコール パーク取得プレフィックスを使用して Cisco Unified CM を設定する必要があります。

(注)　転送、会議、およびダイレクト コール パークの通話切替機能を実行するために、コールに応答して、ユーザ入力（PIN 番号、通話切替機能アクセス コード、およびターゲット番号を含む）を取得し、必要なコール レッグを作成して転送、会議、またはダイレクト コール パークの処理を完了させる、システム設定のエンタープライズ機能アクセス DID への別のコール レッグがリモート接続先電話機で生成されます。

通話切替セッション ハンドオフ機能では、遠端は保留にならないため、MoH は遠端に転送されません。モバイル ユーザがデスクトップフォンでハンドオフ コールに応答するまでの間、元の音声パスが維持されます。ユーザがコールに応答すると、コール レッグが会社のゲートウェイで切り替えられ、音声パスが引き続き維持されます。

通話切替機能は、手動で機能アクセス コードを入力し、適切なキー シーケンスを入力することによって呼び出されます。表 21-2 に、通話切替機能を呼び出すためのキー シーケンスを示します。

表 21-2　手動通話切替機能のキー シーケンス

通話切替機能	エンタープライズ機能アクセス コード（デフォルト）	手動キー シーケンス
保留	*81	入力：*81
独占保留	*82	入力：*82
復帰	*83	入力：*83
転送	*84	1. 入力：*82（独占保留） 2. エンタープライズ機能アクセス DID への新しいコールの発信 3. 接続時の入力： <*PIN_number*> # *84 # <*Transfer_Target/DN*> # 4. 転送ターゲットでの応答時（打診転送の場合）またはリングバック時（初期在席転送の場合）の入力：*84
ダイレクト コール パーク	該当なし	1. 入力：*82（独占保留） 2. エンタープライズ機能アクセス DID への新しいコールの発信 3. 接続時の入力： <*PIN_number*> # *84 # <*Directed_Call_Park_Number*> # *84 # （注）　パークされたコールを取得するには、モバイル ボイス アクセスまたはエンタープライズ機能アクセス 2 ステージ ダイヤリングを使用してコールをダイレクト コール パーク番号に発信する必要があります。ダイヤルするダイレクト コール パーク番号が入力する際、適切なコール パーク取得プレフィックスを付加する必要があります。
会議	*85	1. 入力：*82（独占保留） 2. エンタープライズ機能アクセス DID への新しいコールの発信 3. 接続時の入力： <*PIN_number*> # *85 # <*Conference_Target/DN*> # 4. 会議ターゲットによる応答時の入力：*85
セッション ハンドオフ	*74	1. 入力：*74 2. デスクトップフォンに呼出音または点滅表示で通知されたら応答

(注)　保留や会議などの通話切替機能のためのメディア リソース割り当ては、リモート接続先プロファイル設定、またはデュアルモード電話機および Unified Mobile Communicator の場合にはデバイス設定で決定されます。リモート接続先プロファイルまたはモバイル クライアント デバイスに設定されたデバイス プールのメディア リソース グループ リスト（MRGL）が、会議通話切替機能のための会議ブリッジの割り当てに使用されます。リモート接続先プロファイルまたはモバイル クライアント デバイスのユーザ保留オーディオ ソースとネットワーク保留 MoH オーディオ ソースの設定、およびデバイス プールのメディア リソース グループ リスト（MRGL）が、保留デバイスに送信する MoH ストリームの決定に使用されます。

シングル企業ボイスメール ボックスによるモバイル ボイスメール回避

Cisco Unified Mobility シングル ナンバー リーチに関する追加の考慮事項は、モバイル ボイスメール回避です。シングル企業ボイスメール ボックス機能では、応答がないすべての企業ビジネス コールは最終的に企業ボイスメール システムに転送されます。これによって、ユーザは、応答がない会社の電話番号へのコール用に用意された複数のメールボックス（会社、携帯電話、自宅など）をチェックする必要がなくなります。この機能は、モバイルまたは非企業のボイス メールを避けるために、2 種類の方式を提供します。

- タイマー制御方式: この方法によってシステムは、自動転送タイマーと組み合わせた 1 組のタイマー（リモート接続先ごとに 1 つ）に依存し、無応答時にコールがボイスメール システムに転送されると企業ボイスメール システムがコールを受信するようになります。
- ユーザ制御方式: この方法によってシステムは、コールが応答されてコールがユーザまたは非企業ボイス メールに受信されたかを判断する場合はリモート接続先からの DTMF トーンの確認に依存します。

システム設定は、タイマー制御方式またはユーザ制御方式が使用されているかどうかを判断します。使用される方式は、Voicemail Selection Policy サービス パラメータによってグローバルに設定でき、また、Single Number Reach Voicemail Policy によって個々のリモート接続先ごとに設定できます。デフォルトでは、システムおよびすべてのリモート宛先はタイマー制御メソッド方式を使用します

タイマー コントロールのモバイル ボイスメールの回避

この方式では、システムは [Remote Destination] 設定ページのタイマーのセットに依存します。これらのタイマーの目的は、コールが無応答呼び出しでボイスメール システムに転送されたときに、そのコールがリモート接続先のボイスメール システムではなく、会社のボイスメール システムに転送されることを保証することです。これらのタイマーは、他のシステム無応答転送タイマーとともに、次のように非企業ボイスメール システムを回避するように設定する必要があります。

- デスクフォンの無応答転送時間をリモート接続先電話機よりも短くします。

  これを実現するために、Unified CM のグローバルな無応答転送タイマー フィールドまたは個々の電話回線の無応答呼び出し期間フィールドを、リモート接続先電話機のモバイル ボイスメール システムに転送されるまでの呼び出し期間より短い値に設定します。加えて、[Remote Destination] 設定ページの [Delay Before Ringing Timer] パラメータを使用して、リモート接続先電話機の呼び出しを遅らせることによって、リモート接続先電話機からそのモバイル ボイスメール ボックスに転送されるまでの時間を延ばすことができます。ただし、[Delay Before Ringing Timer] パラメータを調整する場合は、グローバルな Unified CM 無応答転送タイマー（または回線レベルの無応答呼び出し期間フィールド）が、モビリティ ユーザが余裕を持ってリモート接続先電話機の呼び出しに応答できる値に設定されていることを確認する必要があります。[呼び出し前の遅延タイマー（Delay Before Ringing Timer）] パラメータは、リモート接続先ごとに設定することが可能で、デフォルト値は 4,000 ミリ秒です。

- 着信コールがモバイル ボイスメール システムに転送されるまでリモート接続先デバイスで呼び出しを停止します。

  これを実現するには、各リモート接続先に Answer Too Soon Timer および Answer Too Late Timer を使用します。まず、[Remote Destination] 設定ページの [Answer Too Soon Timer] パラメータに、電源オフまたは圏外の携帯電話へのコールがモバイル ボイスメール システムに転送されるまでにかかる時間より長い値を設定する必要があります。デフォルトでは、このタイマーは 1,500 ミリ秒（つまり 1.5 秒）に設定されます。Answer Too Soon Timer が切れる前にコールが応答された場合、リモート接続先へのコール レッグが切断されます。これにより、モバイル ボイスメール システムにすぐに転送されたコールは接続されませんが、呼び出し後にユーザが応答したコールは接続されます。

  次に、[Remote Destination] 設定ページの [Answer Too Late Timer] パラメータを、リモート接続先電話機が呼び出されてからボイスメール ボックスに転送されるまでの時間より短い値に設定します。デフォルトでは、このタイマーは 19,00 ミリ秒（つまり 19 秒）に設定されます。このタイマーが切れる前にコールに応答がなかった場合、リモート接続先へのコール レッグが切断されます。これにより、コールがモバイル ボイスメール システムに転送されるまでリモート接続先電話機で呼び出しが停止されます。

（注） モビリティ ユーザが、[呼び出し開始タイマー（Answer Too Soon Timer）] が切れてから、手動でリモート接続先に宛先変更した着信コールは、最終的にモバイル ボイスメール ボックスに転送される可能性があります。この発生を回避するには、モビリティ ユーザがユーザ制御方式を設定するか、またはボイス メールに宛先変更する着信コールの呼出音を無視または停止するように指示される必要があります。これによって、無応答コールは必ず、企業ボイスメール ボックスに転送されることが保証されます。

（注） ほとんどの配置シナリオでは、[Delay Before Ringing Timer]、[Answer Too Late Timer]、および [Answer Too Soon Timer] のデフォルト値で十分であり、変更する必要はありません。

ユーザ制御のモバイル ボイスメールの回避

この方式では、システムは、コールが応答されたときのリモート宛先からの DTMF 確認トーンにコールに依存します。DTMF トーンがシステムによって受信された場合、システムはユーザがコールに応答し、DTMF トーンを生成するキーを押したことを認識します。一方、DTMF トーンがシステムで受信されない場合、システムは、コール レッグが非企業ボイス メール システムで応答されてコール レッグが切断されると見なします。

ユーザ制御方式が有効な場合、エンド ユーザの応答時に、DTMF トーンを生成するキー パッド ボタンを押すように求める音声プロンプトが再生されます。デフォルトでは、音声プロンプトは、ユーザがコールに応答してから 1 秒後に再生されます。ユーザが応答直後に DTMF トーンを生成するキー パッドを押すと、音声プロンプトが聞こえない場合があります。音声プロンプトは、リモート接続先のコール レッグでだけ再生されるため、遠端側にはプロンプトが聞こえません。音声プロンプトがユーザに再生されたら、デフォルトでシステムは、DTMF トーンを受信するために 5 秒間待機します。トーンが受信されない場合、システムはコール レッグを切断しますが、通話がユーザによって応答されるまで、または企業ボイス メール システムに転送されるまで、ユーザの設定した他のデバイスを鳴らし続けます。

(注)　ユーザ制御のモバイル ボイス メールの回避方式は、モバイル ボイス ネットワークまたは PSTN のリモート宛先から Unified CM まで DTMF トーンのリレーが成功することに完全に依存しています。DTMF トーンは Unified CM にアウトオブバンドで送信されます。DTMF リレーがネットワークおよびシステムで正しく設定されていない場合、DTMF は受信されず、ユーザ制御方式に依存するリモート宛先へのすべてのコール レッグは切断されます。システム管理者は、ユーザ制御方式を有効にする前に、企業のテレフォニー ネットワークで適切な DTMF の相互運用およびリレーを確認する必要があります。DTMF が PSTN から Unified CM に効果的にリレーできない場合、代わりにタイマー コントロールのモバイル ボイス メールの無効化方式を使用する必要があります。

シングル ナンバー リーチの有効化および無効化

シングル ナンバー リーチ（SNR）機能は、次の方法のいずれかを使用して有効または無効にできます。

- エンド ユーザのための Cisco Unified CM Administration または Cisco Unified CM Self Care Portal

  管理者またはユーザが、[シングルナンバーリーチを有効にする（Enable Single Number Reach）] チェックボックスをオフにしてその機能を無効にするか、[シングルナンバーリーチを有効にする（Enable Single Number Reach）] チェックボックスをオンにしてその機能を有効にします。これをリモート接続先ごとに実行します。

- モバイル ボイス アクセスまたはエンタープライズ機能アクセス

  モビリティ対応ユーザが、モバイル ボイス アクセスまたはエンタープライズ機能アクセスにダイヤルインして、適切なクレデンシャルを入力後に、数字の 2 を入力して有効にするか、数字の 3 を入力して無効にします。モバイル ボイス アクセスでは、単一のリモート接続先またはすべてのリモート接続先の SNR を有効/無効にするように促されます。エンタープライズ機能アクセスでは、呼び出しているリモート接続先の SNR しか有効/無効にできません。

- デスク フォンの [モビリティ（Mobility）] ソフトキーまたはアイコン

  ユーザは、電話がオンフック状態のときに [Mobility] ソフトキーを押して、モバイル コネクトを有効にするか、無効にするかを選択します。一部の電話機のモデルでは、ユーザはモビリティ アイコンにタッチしてから、[オフ（Off）] を選択して、シングル ナンバー リーチを無効にします。または、[この電話だけ呼び出す（Ring only this phone）] を選択することもできます。シングル ナンバー リーチを再度有効にするには、[すべてのデバイスを呼び出す（Ring all devices）] を選択します。この方法では、ユーザのリモート接続先すべてでシングル ナンバー リーチが有効または無効にされます。

(注)　前述の [モビリティ（Mobility）] ソフトキーを押すと表示されるダイアログ ボックスでは、新しい機能名である「シングル ナンバー リーチ」ではなく、古い機能名「モバイル コネクト」が使用されています。機能および有効化と無効化の手順は同じです。

シングル ナンバー リーチ コールの許可または拒否用のアクセス リスト

アクセス リストは、Cisco Unified CM 内で設定して、リモート接続先に関連付けることができます。アクセス リストは、モビリティ対応ユーザのリモート接続先に転送される着信コールを許可または拒否（着信コールの発信者 ID に基づく）するために使用されます。さらに、これらのアクセス リストは時刻に基づいて呼び出されます。

アクセス リストは、拒否または許可するモビリティ対応ユーザごとに設定されます。アクセス リストには、特定の番号または番号マスクで構成された 1 つ以上のメンバーまたはフィルタが含まれており、このフィルタが発信側の着信コールの発信者 ID と比較されます。発信者 ID と照合するための特定の番号文字列または番号マスクが含まれることに加えて、アクセス リストには、発信者 ID が使用できない、または、発信者 ID がプライベートに設定されている着信コール用のフィルタも含めることができます。拒否対象のアクセス リストには、アクセス リストに入力された番号からのコールは拒否されるが、その他の番号からのコールは許可されるように、リストの最後に暗黙の「すべて許可」が含まれています。許可対象のアクセス リストには、アクセス リストに入力された番号からのコールは許可されるが、その他の番号からのコールは拒否されるように、リストの最後に暗黙の「すべて拒否」が含まれています。

設定したアクセス リストを [リモート接続先（Remote Destination）] 設定画面で設定した [呼び出しスケジュール（Ring Schedule）] に関連付けると、設定した [呼び出しスケジュール（Ring Schedule）] と選択したアクセス リストの組み合わせによって、リモート接続先ごとのシングル ナンバー リーチ コールの時刻コール フィルタリングが提供されます。Cisco Unified CM Administration インターフェイスを使用している管理者または Cisco Unified CM Self Care Portal を使用しているエンド ユーザは、アクセス リストと Ring Schedule を設定してリモート接続先に関連付けることができます。

シングル ナンバー リーチのアーキテクチャ

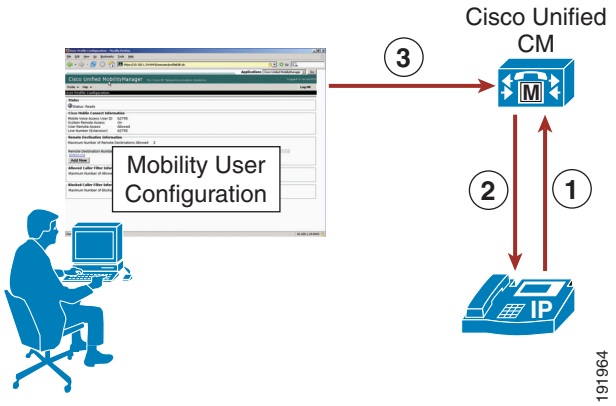
シングル ナンバー リーチ（SNR）機能のアーキテクチャを理解することは、その機能を理解することと同様に重要です。図 21-22 に、SNR に必要なメッセージ フローとアーキテクチャを示します。次の相互作用とイベントのシーケンスが、Unified CM、SNR ユーザ、および SNR ユーザのデスク フォンの間で発生する可能性があります。

1. SNR 機能の有効化または無効化、あるいはリモート接続先電話機の通話中コールのピックアップを希望している SNR 電話機のユーザが、デスク フォンの [モビリティ（Mobility）] ソフトキーを押します（図 21-22 のステップ 1 を参照）。
2. Unified CM から SNR のステータス（オンまたはオフ）が返されます。ユーザは、電話が接続状態であれば携帯電話にコールを転送するオプションを選択することも、電話がオン フック状態であれば SNR のステータスを有効/無効にすることもできます（図 21-22 のステップ 2 を参照）。
3. シングル ナンバー リーチ ユーザは、Unified CM Self Care Portal を使用して、次の URL にある Web ベースの設定ページ経由で独自のモビリティ設定を構成できます。

   https://<*Unified-CM_Server_IP_Address*>/ucmuser/

   ここで、<*Unified-CM_Server_IP_Address*> は、Unified CM パブリッシャ サーバの IP アドレスです（図 21-22 のステップ 3 を参照）。

図 21-22　　シングル ナンバー リーチのアーキテクチャ



シングル ナンバー リーチのハイ アベイラビリティ

シングル ナンバー リーチ機能には、次のコンポーネントが必要です。

- Unified CM サーバ
- PSTN ゲートウェイ

各コンポーネントの冗長性または弾力性を向上させて、さまざまな障害シナリオでシングル ナンバー リーチの機能が失われないようにする必要があります。

Unified CM サーバの冗長性

シングル ナンバー リーチ機能には、Unified CM サーバが不可欠です。Unified CM Group による電話機とゲートウェイの登録が冗長になっていれば、Unified CM サーバが故障しても SNR 機能は影響を受けません。

SNR ユーザが Unified CM Self Care Portal Web インターフェイスを使用してモビリティ設定（リモート接続先とアクセス リスト）を構成できるようにするには、Unified CM パブリッシャ サーバが使用可能である必要があります。パブリッシャがダウンすると、ユーザはモビリティ設定を変更できなくなります。同様に、管理者も Unified CM でモビリティ設定を変更できなくなります。ただし、既存のモビリティ設定と機能は維持されます。最後に、システムで SNR のステータスに対する変更を Unified CM パブリッシャ サーバ上に記録する必要があります。Unified CM パブリッシャが使用できない場合は、SNR を有効化または無効化できなくなります。

PSTN ゲートウェイの冗長性

シングル ナンバー リーチ機能は、新しいコール レッグを PSTN に拡張して SNR ユーザのリモート接続先電話機に到達する機能に依存しているため、PSTN ゲートウェイの冗長性は重要です。PSTN ゲートウェイが故障したり、容量不足の場合は、SNR コールを完了できません。通常は、会社の IP テレフォニー ダイヤル プランを通して、物理的なゲートウェイの冗長性とコールの再ルーティング機能だけでなく、予想されるコール アクティビティを処理する十分な容量が提供されることによって、PSTN アクセスに冗長性が提供されます。Unified CM が、コール ルーティングの弾力性を確保するための十分な容量、複数のゲートウェイ、およびルート グループとルート リストの構造で構成されていれば、この冗長性によって SNR 機能の持続性が保証されます。

モバイル ボイス アクセスとエンタープライズ機能アクセス

モバイル ボイス アクセス（システム リモート アクセスとも呼ばれる）とエンタープライズ機能アクセス 2 段階ダイヤリングは、シングル ナンバー リーチ アプリケーションに組み込まれている機能です。両方の機能を使用すれば、モビリティ対応ユーザは、外出先でも、Unified CM に直接接続されているかのように電話をかけることができます。この機能は、従来のテレフォニー環境では、一般的に、Direct Inward System Access（DISA）と呼ばれています。これらの機能を通して、通話料金を抑えたり、モバイル ユーザごとに通話料を請求するのではなく、直接会社に請求するように配慮することによって、会社にメリットがもたらされます。加えて、これらの機能を使用すれば、ユーザは、発信者 ID を外部に送信するときに、携帯電話やリモート接続先の番号を隠すことができます。代わりに、発信者 ID として、ユーザの会社の電話番号が送信されます。これによって、ユーザへの返信コールは会社の電話番号にかけられるため、コールを会社で一括管理できます。また、モバイル ユーザは、これらの機能を使用して、通常は企業外部から到達不能な内部の内線番号や DID 以外の会社の電話番号にダイヤルできます。

モバイル ボイス アクセスには、H.323 または SIP VoiceXML（VXML）ゲートウェイで応答および処理されるシステム設定の DID 番号を呼び出すことによってアクセスします。VoiceXML ゲートウェイによって、モバイル ボイス アクセス ユーザに対する双方向音声応答（IVR）プロンプトが再生され、ユーザ認証と電話機のキーパッド経由でダイヤルされる番号入力が要求されます。

エンタープライズ機能アクセス機能には、前述した通話切替機能や会議機能だけでなく、2 ステージ ダイヤリング機能が含まれています。2 ステージ ダイヤリングは、IVR プロンプトを除いて、モバイル ボイス アクセスと同様の方法で動作します。システム設定のエンタープライズ機能アクセス DID が Unified CM によって応答されます。ユーザは、電話機のキーパッドまたはスマート フォン ソフトキーを使用して、認証とダイヤルする番号を入力します。これらの入力はプロンプトなしで受信されます。

モバイル ボイス アクセスとエンタープライズ機能アクセス 2 段階ダイヤリングの両方の機能を使用すれば、ユーザは、入力番号に対するコールが接続されたときに、通話切替機能を呼び出したり、シングル ナンバー リーチと同様にデスク フォンでコールをピックアップしたりできます。この動作は、コールが会社のゲートウェイに固定されることによって可能になります。

モバイル ボイス アクセス IVR VoiceXML ゲートウェイ URL

モバイル ボイス アクセス機能を使用するには、Unified CM VoiceXML アプリケーションを H.323 または SIP ゲートウェイ上にインストールする必要があります。このアプリケーションをロードするための URL は次のとおりです。

http://<*Unified-CM-Publisher_IP-Address*>:8080/ccmivr/pages/IVRMainpage.vxml

ここで、<*Unified-CM-Publisher_IP-Address*> は、Unified CM パブリッシャ ノードの IP アドレスです。

モバイル ボイス アクセス機能

図 21-23 に、モバイル ボイス アクセスのコール フローを示します。この例では、モバイル ボイス アクセス ユーザが PSTN 電話機（408 555-7890）からモバイル ボイス アクセス会社の DID DN 408-555-2345 にダイヤルします（ステップ 1）。

このコールは、VoiceXML ゲートウェイとしても機能する会社の PSTN H.323 または SIP ゲートウェイに到達します（ステップ 2）。

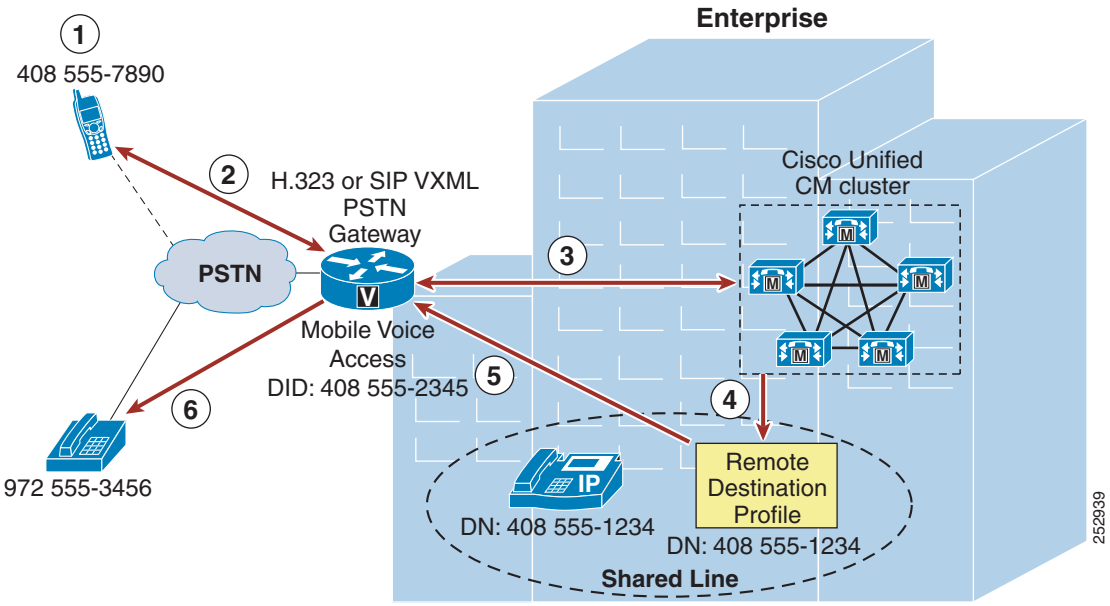
(注)　ネイティブ VoiceXML のサポートは Cisco IOS XE では利用できないため、Cisco 4000 シリーズ Integrated Services Router（ISR）をモバイル ボイス アクセスの VoiceXML ゲートウェイとして導入することはできません。代わりにネイティブ VXML をサポートする Cisco IOS ゲートウェイを使用する必要があります。

ユーザは、IVR 経由で、数字のユーザ ID（後ろに # 記号が続く）、PIN 番号（後ろに # 記号が続く）、および 1 の入力と、相手の電話番号が続くモバイル ボイス アクセス コールの発信を要求されます。この場合は、ユーザが相手の番号として 9 1 972 555 3456（後ろに # 記号が続く）を入力します。

(注)　モバイル ボイス アクセス ユーザがかけている PSTN 電話機が、そのユーザのシングル ナンバー リーチ リモート接続先として設定されており、Unified CM で着信コールの発信者 ID とこのリモート接続先を照合可能な場合は、数字のユーザ ID を入力する必要がありません。代わりに、PIN 番号の入力だけが要求されます。

その一方で、IVR プロンプトが Unified CM からゲートウェイに転送され、ゲートウェイでユーザに対してプロンプトが再生され、ゲートウェイでユーザの数字の ID と PIN 番号を含む入力が収集されます。この情報は、認証と 9 1 972 555 3456 へのコールを発信するために Unified CM に転送されます（ステップ 3）。ユーザの認証とダイヤルする番号の受信後に、Unified CM でユーザのリモート接続先プロファイル経由のコールが発信されます（ステップ 4）。972 555-3456 への発信コールが、PSTN ゲートウェイ経由で経路設定されます（ステップ 5）。最後に、番号が 972 555-3456 の PSTN 接続先電話機で呼出音が鳴ります（ステップ 6）。

図 21-23　モバイル ボイス アクセス



(注)　モバイル ボイス アクセスを図 21-23 のように動作させるには、システム全体の Enable Mobile Voice Access サービス パラメータが True に設定され、[End User] 設定ページでユーザごとに [Enable Mobile Voice Access] チェックボックスがオンになっていることを確認してください。

(注)　モバイル ボイス アクセス機能を使用するには、Unified CM Serviceability の設定ページで [Cisco Unified Mobile Voice Access Service] を手動でアクティブにする必要があります。このサービスは、パブリッシャ ノードでのみアクティブにできます。

(注)　ネイティブ VoiceXML をサポートしない Cisco 4000 シリーズ ISR を PSTN ゲートウェイとして使用する場合、モバイル ボイス アクセスに必要な VoiceVXML 機能を H.323 Cisco IOS ゲートウェイで提供するようにしてください。次のセクションで説明するように、H.323 Cisco IOS ゲートウェイでは、ヘアピニングという導入方法を使用してネイティブ VoiceXML をサポートします。

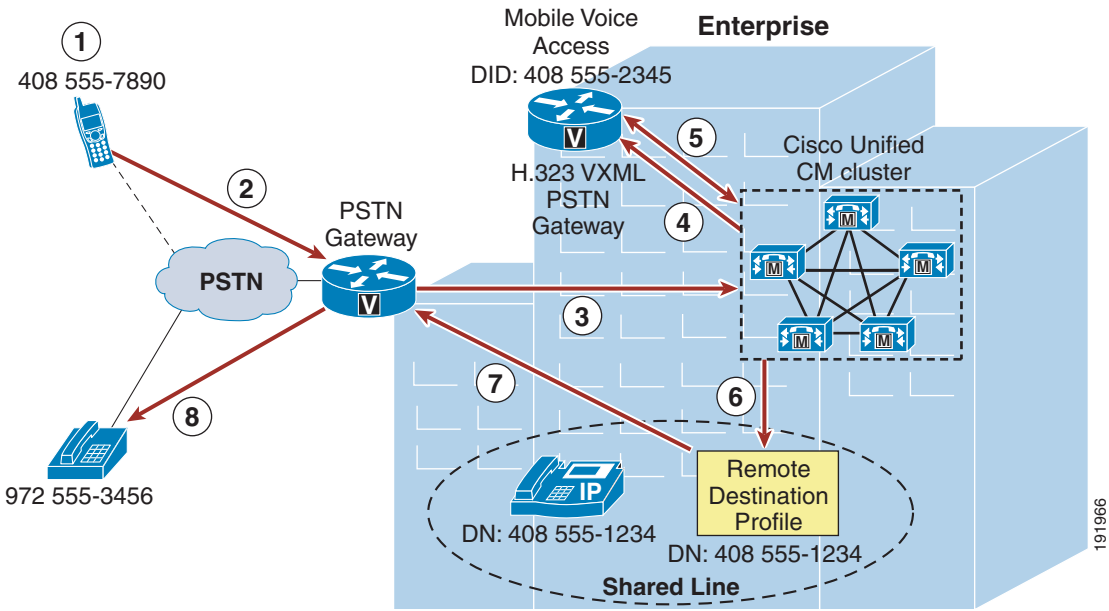
ヘアピニングを使用したモバイル ボイス アクセス

会社の PSTN ゲートウェイで H.323 または SIP が使用されていない配置では、H.323 を実行している別のゲートウェイ上のヘアピニングを使用することによってモバイル ボイス アクセス機能を提供することもできます。ヘアピニングを使用したモバイル ボイス アクセスの場合は、VoiceXML 機能を別の H.323 ゲートウェイに持たせる必要があります。図 21-24 に、ヘアピニングを使用したモバイル ボイス アクセスのコール フローを示します。この例では、前の例と同じく、モバイル ボイス アクセス ユーザが PSTN 電話機（408 555-7890）からモバイル ボイス アクセス会社の DID DN 408-555-2345 にダイヤルします（ステップ 1）。コールが、会社の PSTN ゲートウェイに入ってきて（ステップ 2）、呼処理のために Unified CM に転送されます（ステップ 3）。Unified CM が着信コールを H.323 VoiceXML ゲートウェイにルーティングします（ステップ 4）。IVR がユーザに、自分の数字のユーザ ID と PIN、およびモバイル ボイス アクセス コールを作成するための 1 を入力し、続けて接続先の電話番号を入力するように求めます。この場合も、ユーザが相手の番号として 9 1 972 555 3456（後ろに # 記号が続く）を入力します。

(注)　ヘアピニングを使用したモバイル ボイス アクセスでは、システムを呼び出しているユーザが発信者 ID によって自動的に特定されません。代わりに、PIN を入力する前に、手動でリモート接続先の番号を入力する必要があります。ユーザが自動的に特定されない理由は、ヘアピニングを使用する配置では、公衆網ゲートウェイにおいて最初にコールを Unified CM にルーティングして、ヘアピンされるモバイル ボイス アクセス ゲートウェイに到達する必要があるためです。コールが最初に Unified CM にルーティングされるため、発信番号が携帯の番号から会社の電話番号に変換されてから、コールがモバイル ボイス アクセス ゲートウェイによって処理されます。このため、モバイル ボイス アクセス ゲートウェイでは、発信番号と設定されているリモート接続先の照合を行うことができず、ユーザはリモート接続先番号の入力を求められます。これは、ヘアピニングを使用する配置に特有の現象です。通常のモバイル ボイス アクセスのフローにおいては、モバイル ボイス アクセス機能はローカル ゲートウェイで利用できるため、PSTN ゲートウェイで最初にコールを Unified CM にルーティングしてからモバイル ボイス アクセスにアクセスする必要がありません。

その間に、H.323 VoiceXML ゲートウェイは、ユーザ入力を収集して Unified CM に転送し、転送された IVR プロンプトを PSTN ゲートウェイおよびモバイル ボイス アクセス ユーザに対して再生します。これを受けて Unified CM がユーザ入力を受信し、ユーザを認証し、ユーザ入力に基づいて適切な IVR プロンプトを H.323 VoiceXML ゲートウェイに転送します（ステップ 5）。ダイヤルする番号の受信後に、Unified CM でユーザのリモート接続先プロファイルを使用したコールが発信されます（ステップ 6）。972 555-3456 への発信コールが、PSTN ゲートウェイ経由で経路設定されます（ステップ 7）。最後に、番号が 972 555-3456 の PSTN 接続先電話機で呼出音が鳴ります（ステップ 8）。

図 21-24　　ヘアピニングを使用したモバイル ボイス アクセス



(注)　モバイル ボイス アクセスをヘアピニング モードで配置する場合は、PSTN ゲートウェイでのモバイル ボイス アクセス DID と Cisco Unified CM 内のモバイル ボイス アクセス電話番号（**Media Resources - Mobile Voice Access**）を別々の番号として設定することを推奨します。そうすれば、Unified CM 内のトランスレーション パターンを使用して、モバイル ボイス アクセス DID の着信番号を設定済みのモバイル ボイス アクセス電話番号に変換できます。Unified CM 内で設定されたモバイル ボイス アクセス電話番号は管理者にしか表示されないため、DID と電話番号間の変換をエンド ユーザが意識する必要はなく、エンド ユーザのダイヤリング動作に変更は生じません。この方法は、マルチクラスタ環境でのモビリティ コール ルーティング問題を回避するために推奨されています。この推奨事項は、非ヘアピニング モードのモバイル ボイス アクセスには当てはまりません。

(注)　ヘアピニング モードのモバイル ボイス アクセスは、H.323 VXML ゲートウェイだけでサポートされています。

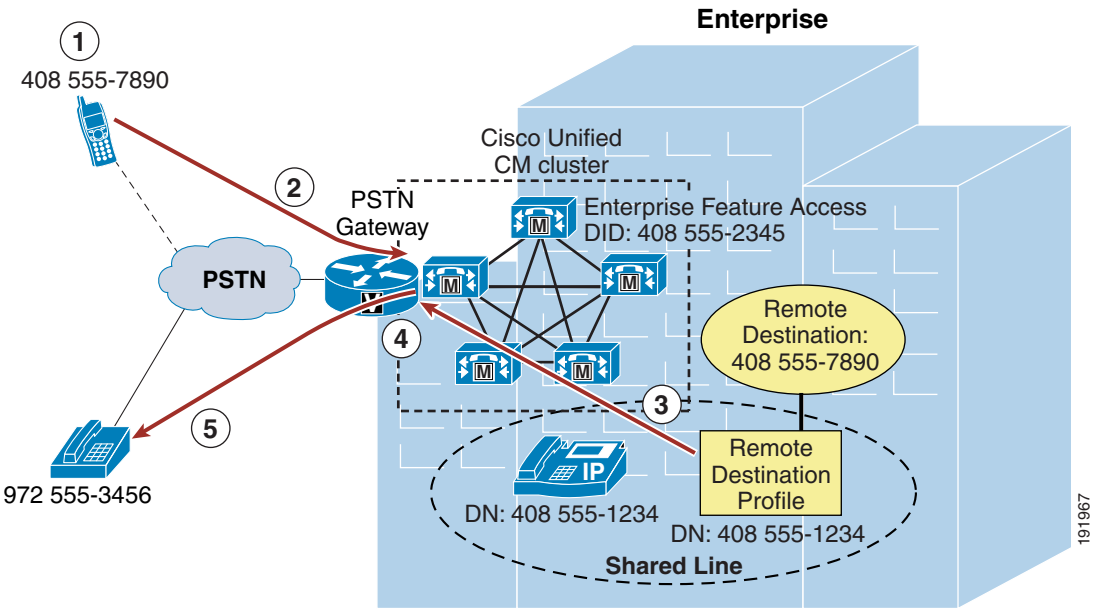
2 段階ダイヤリングを伴うエンタープライズ機能アクセス

図 21-25 に、エンタープライズ機能アクセス 2 ステージ ダイヤリングを示します。この例では、モビリティ ユーザがリモート接続先電話機（408 555-7890）からエンタープライズ機能アクセス DID 408 555-2345 にダイヤルします（ステップ 1）。コールが接続されると、Unified CM で認証されるユーザの PIN（後ろに # 記号が続く）で始まる DTMF 番号を PSTN ゲートウェイ経由で Unified CM に送信するためにリモート接続先電話機が使用されます。次に、2 ステージ ダイヤリング対象コールが試みられることを示す 1（後ろに # 記号が続く）と相手の電話番号が送信されます。この場合は、ユーザが接続先番号として 9 1 972 555 3456 と入力します（ステップ 2）。

(注)　モバイル ボイス アクセスとは違って、エンタープライズ機能アクセスでは、エンド ユーザ アカウントに対して発信者 ID と PIN を照合するためにリモート接続先として設定された電話機から、すべての 2 ステージ ダイヤリング対象コールを発信する必要があります。エンタープライズ機能アクセスにおいては、モビリティ ユーザが自身を識別するためのリモート接続先番号または ID をシステムに入力するための仕組みは用意されていません。同一性は、着信コールの発信者 ID と入力された PIN の組み合わせを通してのみ確立できます。

次に、発信コールがユーザのリモート接続先プロファイル経由で開始され（ステップ 3）、PSTN 番号 972 555-3456 へのコールが会社の PSTN ゲートウェイ経由で経路設定されます（ステップ 4）。最後に、PSTN 電話機が呼び出されます（ステップ 5: この場合は 972 555-3456）。モバイル ボイス アクセスと同様に、各エンタープライズ機能アクセス 2 ステージ ダイヤリング対象コールの音声メディア パスは、2 つのゲートウェイ ポートを使用している PSTN ゲートウェイ内でヘアピンされます。

図 21-25　エンタープライズ機能アクセス 2 ステージ ダイヤリング機能



(注)　エンタープライズ機能アクセス 2 ステージ ダイヤリングを図 21-25 のように動作させるには、システム全体の Enable Enterprise Feature Access サービス パラメータが True に設定されていることを確認してください。

デスク フォンとリモート接続先電話機のピックアップ

モバイル ボイス アクセス機能とエンタープライズ機能アクセス機能はシングル ナンバー リーチと緊密に統合されているため、モバイル ボイス アクセスまたはエンタープライズ機能アクセス 2 段階ダイヤリング対象コールが確立されていれば、ユーザはシングル ナンバー リーチ機能を利用して、最初に着信した電話機をオン フックしてデスク フォンの [再開（Resume）] ソフトキーを押すだけで、または、通話切替保留機能を使用して、通話中のコールをデスク フォンでピックアップできます。さらに、その後で、ユーザの設定済みリモート接続先電話機で Mobility ソフトキーを押して Send Call to Mobile Phone を選択することによって、そのコールをピックアップできます。

シングル ナンバー リーチの有効化および無効化

モバイル ボイス アクセスとエンタープライズ機能アクセスのユーザはまるで社内にいるかのように PSTN から電話がかけられるだけでなく、H.323 または SIP VoiceXML ゲートウェイ上のモバイル ボイス アクセスで提供される機能とエンタープライズ機能アクセスで提供される機能によって、ユーザは電話機のキーパッドを使用して、リモート接続先ごとのシングル ナンバー リーチ機能をリモートで有効または無効にすることもできます。1 を入力して電話をかけるのではなく、ユーザは、2 を入力してシングル ナンバー リーチ機能を有効にし、3 を入力してシングル ナンバー リーチ機能を無効にします。

モバイル ボイス アクセスを使用するにあたって、複数のリモート接続先を設定する場合は、シングル ナンバー リーチ機能を有効または無効にするリモート接続先の電話番号を入力するように要求されます。エンタープライズ機能アクセスでは、呼び出しているリモート接続先電話機のシングル ナンバー リーチしか有効/無効にできません。

（注）　[モバイルボイスアクセスの有効化（Enable Mobile Voice Access）] サービス パラメータが [False（False）] に設定されており、2 段階ダイヤリング対象コールを行うことができない場合でも、モバイル ボイス アクセスでは、リモートからシングル ナンバー リーチを有効または無効にする機能が提供されます。システムにモバイル ボイス アクセス電話番号が設定され、ユーザのアカウントでモバイル ボイス アクセスが有効にされ、Cisco Unified Mobile Voice Access サービスがパブリッシャ上で実行されている限り、認証済み発信側のユーザはシングル ナンバー リーチを有効または無効にできます。

モバイル ボイス アクセスとエンタープライズ機能アクセスの番号拒否

管理者は、モバイル ボイス アクセスとエンタープライズ機能アクセスの 2 ステージ ダイヤリングのユーザが、それらの機能の使用中は特定の番号にダイヤルできないようにできます。オフネット コールに対してこれらの機能を使用している場合に特定の番号へのコールを制限または拒否するには、[System Remote Access Blocked Numbers] サービス パラメータ フィールドでそのような番号のカンマ区切りのリストを設定できます。このパラメータに拒否する番号を設定したら、モバイル ボイス アクセスまたはエンタープライズ機能アクセスが使用されている場合は、ユーザのリモート接続先電話機からそれらの番号にダイヤルできなくなります。管理者が拒否したい番号には、911 などの緊急電話番号を含めることができます。拒否する番号を設定する場合は、会社のユーザが該当するプレフィックスまたは振り分け用の数字を付けてダイヤルするようにそれらの番号が設定されていることを確認してください。たとえば、緊急電話番号を拒否対象とし、システム ユーザが緊急電話番号をダイヤルするときは 9911 を使用しなければならない場合は、[System Remote Access Blocked Numbers] フィールドに設定する番号を 9911 にする必要があります。

モバイル ボイス アクセスのアクセス番号

Unified CM システムでは、1 つのモバイル ボイス アクセス電話番号だけを設定することもできますが、これらの内部で設定された番号にアクセス可能な外部番号を複数使用できます。たとえば、米国の New York に配置されたシステム、San Jose のリモート サイト、および London の海外サイトがある場合を考えます。システムのモバイル ボイス アクセス電話番号が 555-1234 に設定されている場合でも、各ロケーションのゲートウェイを設定して、ローカル DID 番号またはフリーダイヤル DID 番号をこのモバイル ボイス アクセス電話番号にマッピングできます。たとえば、New York のゲートウェイの DID である +1 212 555 1234 と +1 800 555 1234 の両方をモバイル ボイス アクセス番号にマッピングし、さらに San Jose のゲートウェイの DID +1 408 666 5678 および London のゲートウェイの DID +44 208 777 0987 もシステムのモバイル ボイス アクセス番号にマッピングできます。

システム管理者は、複数のローカル DID 番号またはフリーダイヤル DID 番号を用意することによって、モバイル ボイス アクセスの 2 段階ダイヤリング対象コールが常にローカルまたはフリーダイヤルのコールとしてシステムに発信されるようにでき、さらにテレフォニー関連コストを削減できます。

リモート接続先の設定と発信者 ID の照合

モバイル ボイス アクセス機能およびエンタープライズ機能アクセス 2 段階ダイヤリング機能に加えて、DTMF ベースの通話切替機能の転送と会議のユーザを認証するときに、発信元のリモート接続先電話機の発信者 ID がシステム内で設定されたすべてのリモート接続先に対して照合されます。この発信者 ID の照合は、リモート接続先番号の設定方法、システムで PSTN 振り分け用数字を含めるために番号プレフィックスが必要かどうか、[Matching Caller ID with Remote Destination] パラメータが [Partial Match] と [Complete Match] のどちらに設定されているかなどの複数の要因に左右されます。いずれの場合も、要件は、1 つまたは複数のリモート接続先番号に基づいて各モビリティ ユーザを識別できることです。したがって、リモート宛先番号がシステム内で一意に設定されるだけでなく、着信コールの発信者 ID の一致（完全照合を使用するか、一部照合を使用するか）が 1 つのリモート宛先に常に一意に対応しなければならないことも重要です。単一または一意の一致が見つからない場合、発信者 ID 照合は失敗します。

この照合の特性を制御するために、次の 2 つのアプローチを検討してください。

完全発信者 ID 照合の使用

このアプローチでは、発信者 ID が PSTN から供給されているかのようにリモート接続先を設定します。たとえば、リモート接続先電話機の発信者 ID を PSTN からシステムに 4085557890 として供給する場合は、[Remote Destination] 設定ページでこの番号を設定する必要があります。

このリモート接続先にシングル ナンバー リーチ コールを適切にルーティングするには、+E.164 ダイヤル方式または番号プレフィックス メカニズムを使用して必要な PSTN アクセス コードおよび他の必要な数字にプレフィックスを付けるようにダイヤル プランを設定する必要があります。たとえば、グローバル +E.164 ダイヤル プランを使用しないで、企業からのコールをダイヤルするときに 9 個のまたは他の PSTN 振り分け用数字または国番号が PSTN に到達するために必要であることが想定される場合、設定済みのリモート接続先番号の先頭に適切な PSTN 振り分け用数字と国番号を追加するように番号プレフィックスを設定する必要があります。番号プレフィックスは、Unified CM システム内でトランスレーション パターン、ルート パターン、またはルート リスト コンストラクトを使用して実施する必要があります。この完全照合アプローチおよび番号プレフィックス方式を使用する場合、Matching Caller ID with Complete Match パラメータをデフォルト設定の [Complete Match] のままにする必要があります。

アプリケーション ダイヤル ルールは、これらのシナリオで番号プレフィックスを提供するためにも使用されることがあります。ただし、アプリケーション ダイヤル ルールが着信ディジット ストリングの長さに基づくため分割できないことも注目すべきことであり、それは、システム全体でグローバルに適用されることを意味します。これは特に、複数のダイヤル ドメイン（たとえば、異なる国）が単一の Unified CM クラスタでサポートされる必要があるシナリオにおけるアプリケーション ダイヤル ルールの使用を厳しく制限します。

(注)　アプリケーション ダイヤル ルールはシングル ナンバー リーチ、モバイル ボイス アクセス、およびエンタープライズ機能アクセスのコールに適用されるだけでなく、Cisco WebDialer、Cisco Unified CM Assistant、および Cisco Jabber アプリケーションから発信されたコールにも適用されます。したがって、すべてのアプリケーションを通してダイヤリング動作が期待どおりに機能するように、これらの規則を慎重に設定する必要があります。

推奨されるダイヤル プラン アプローチは、発信者 ID を PSTN からの入力の +E.164 に常にグローバル化し、リモート接続先を +E.164 として常に設定することです。これによって、すべての設定済みリモート接続先と比較すると、PSTN からの発信者 ID（正規化後）が一意の一致を常に提供することが保証されます。+E.164 ダイヤリングをサポートするダイヤル プランと組み合わせると、これは複数の国際番号計画をサポートしている場合でも、番号プレフィックスを不要にし、リモート接続先のユーザおよび番号の一意の ID を確認します。推奨されるダイヤル プラン アプローチがトランクの要件やユーザの希望に従って入力の発信者 ID をグローバル化し、出力でローカライズするため、PSTN から供給される発信者 ID を使用することはこのアプローチと互換性がありません。

部分発信者 ID 照合の使用

このアプローチでは、リモート接続先が、システムから PSTN にダイヤルされたかのように設定されます。たとえば、リモート接続先の番号が 14085557890 で、システムから PSTN にアクセスするために 9 を入力する必要がある場合は、[Remote Destination] 設定ページでこの番号を 914085557890 に設定する必要があります。このアプローチでは、システムにおける番号プレフィックス メカニズムの設定を必要としませんが、[Matching Caller ID with Remote Destination] サービス パラメータを [Partial Match] に設定し、[Number of Digits for Caller ID Partial Match] をリモート接続先発信者 ID に対して照合すべき連続桁数を表す適切な数字に設定する必要があります。たとえば、リモート接続先の発信者 ID が 14085557890 で、リモート接続先が 914085557890 に設定されている場合は、[Number of Digits for Caller ID Partial Match] を 10 または 11 に設定するのが理想的です。この例では、このパラメータをさらに少ない桁数に設定できます。ただし、システム内のすべての設定済みリモート接続先を一意的に識別できるように十分な連続桁数が照合されることを保証するように注意してください。部分発信者 ID 照合を使用したときに完全な一致が見つからない場合、または複数の設定済みリモート接続先が一致した場合は、システムで一致するリモート接続先番号が存在しないものとして処理されます。したがって、モバイル ボイス アクセスの場合は、PIN を入力する前にリモート接続先番号/ID を手動で入力する必要があります。エンタープライズ機能アクセスには、ユーザがリモート接続先番号を入力するメカニズムがありません。そのため、この機能を使用する場合は、一致が一意的にしか発生しないことを確認してください。

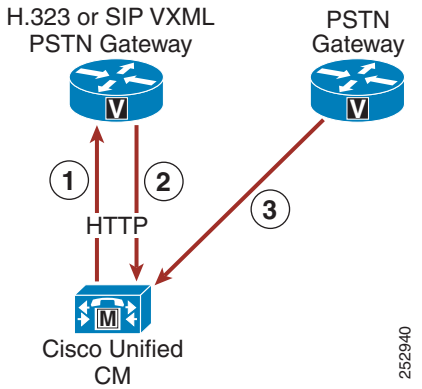
(注)　PSTN サービス プロバイダーが可変長の発信者 ID を送信する場合は、着信コールごとの一意的な発信者 ID の一致が保証できない可能性があるため、部分発信者 ID 照合の使用は推奨できません。これらのシナリオでは、完全発信者 ID 照合または +E.164 ダイヤル プランは望ましい方法です。

モバイル ボイス アクセスとエンタープライズ機能アクセスのアーキテクチャ

モバイル ボイス アクセスとエンタープライズ機能アクセスのアーキテクチャを理解することは、それらの機能性を理解することと同じくらい重要です。図 21-26 は、モバイル ボイス アクセスとエンタープライズ機能アクセスに必要なメッセージ フローとアーキテクチャを示しています。Unified CM、PSTN ゲートウェイ、および H.323 または SIP VXML ゲートウェイの間には、次の一連の対話とイベントが発生します。

1. Unified CM から HTTP 経由で IVR プロンプトとインストラクションが H.323 または SIP VXML ゲートウェイに転送されます（図 21-26 のステップ 1 を参照）。これによって、VXML ゲートウェイで着信モバイル ボイス アクセス発信者に対してこれらのプロンプトを再生できます。
2. H.323 または SIP VXML ゲートウェイでは、HTTP を使用してモバイル ボイス アクセス ユーザの入力が Unified CM に戻されます（図 21-26 のステップ 2 を参照）。
3. PSTN ゲートウェイでは、リモート接続先電話機からのエンタープライズ機能アクセス 2 ステージ ダイヤリングおよび通話切替機能に関するユーザまたはスマート フォンのキー シーケンスに応答して DTMF 番号が転送されます（図 21-26 のステップ 3 を参照）。

図 21-26　モバイル ボイス アクセスとエンタープライズ機能アクセスのアーキテクチャ



（注）　図 21-26 では PSTN ゲートウェイとは別のボックスとして H.323 または SIP VoiceXML ゲートウェイが描かれていますが、これはアーキテクチャ上の要件ではありません。PSTN ゲートウェイで H.323 または SIP 以外のプロトコルを実行する必要がなければ、VoiceXML 機能と PSTN ゲートウェイ機能を同じボックスで処理できます。H.323 または SIP ゲートウェイは、モバイル ボイス アクセス VoiceXML 機能に不可欠です。

（注）　Cisco IOS XE ではネイティブ VoiceXML のサポートを提供していないため、Cisco 4000 シリーズ ISR をモバイル ボイス アクセスの VoiceXML ゲートウェイとして使用することはできません。Cisco 4000 シリーズ ISR を PSTN ゲートウェイとして使用する場合は、VoiceXML 機能のほとんどを、ネイティブ VoiceXML をサポートする Cisco IOS ゲートウェイで提供する必要があります。

モバイル ボイス アクセスおよびエンタープライズ機能アクセスのハイ アベイラビリティ

モバイル ボイス アクセス機能とエンタープライズ機能アクセス機能には、シングル ナンバー リーチ機能と同じコンポーネントと冗長性メカニズムが必要です（シングル ナンバー リーチのハイ アベイラビリティ（21-63 ページ）を参照）。Unified CM Group は、PSTN ゲートウェイ登録の冗長性に欠かせません。同様に、PSTN の物理ゲートウェイとゲートウェイ接続の冗長性を提供する必要があります。PSTN と会社間の冗長なアクセスは、ゲートウェイが故障した場合に、リモート接続先電話機からモバイル ボイス アクセス機能とエンタープライズ機能アクセス機能にアクセスするために必要です。ただし、必要に応じて、H.323 または SIP VoiceXML ゲートウェイに対して物理的な冗長性を提供できますが、Unified CM 上には、Cisco Unified Mobile Voice Access サービス用の冗長性メカニズムがありません。このサービスは、パブリッシャ ノードでしか有効にして実行することができません。そのため、パブリッシャ ノードが無効な場合は、モバイル ボイス アクセス機能が使用できません。エンタープライズ機能アクセスと 2 ステージ ダイヤリング機能には、このようなパブリッシャとの依存関係がないため、モビリティ ユーザに同等の機能性（IVR プロンプトが再生されない）を提供できます。

Cisco Unified Mobility の配置の設計

Cisco Unified Mobility ソリューションでは、Cisco Unified CM を介してモビリティ機能が提供されます。機能には、シングル ナンバー リーチ、モバイル ボイス アクセス、およびエンタープライズ機能アクセスが含まれます。この機能を配置する場合は、ダイヤル プランの意味、ガイドラインと制約事項、および性能と容量に関する考慮事項を理解しておくことが重要です。

Cisco Unified Mobility のダイヤル プランに関する考慮事項

Unified Mobility を適切に設定してプロビジョニングするには、リモート接続先プロファイル設定のコール ルーティング動作とダイヤル プランの意味を理解しておくことが重要です。

リモート接続先プロファイルの設定

Unified Mobility を設定する場合は、[Remote Destination Profile] 設定ページにある次の 2 つの設定を考慮する必要があります。

- [コーリングサーチスペース（Calling Search Space）]

  この設定と電話番号または回線レベルのコーリング サーチ スペース（CSS）を組み合わせて、モビリティ ダイヤル対象コール用にアクセス可能なパーティションが決定されます。この設定は、モバイル ボイス アクセスとエンタープライズ機能アクセス 2 ステージ ダイヤリングを含む、リモート接続先電話機からのモビリティ ユーザによるコールだけでなく、通話切替の転送機能と会議機能の組み合わせによるコールにも影響します。この CSS と回線レベルの CSS の組み合わせの中に、ユーザのリモート接続先電話機から発信されたビジネス コールのためにアクセスする必要のあるすべてのパーティションが含まれていることを確認してください。ローカル ルート グループを持つ回線だけの従来のアプローチを使用する +E.164 ダイヤル プランでは、この CSS は必要なく、**<None>** に設定できます。

- [再ルーティング用コーリング サーチ スペース（Rerouting Calling Search Space）]

  この設定によって、ユーザのリモート接続先電話機にコールが送信されたときにアクセスするパーティションが決定されます。これは、すべてのシングル ナンバー リーチ コールに適用されます。ユーザの会社の電話番号へのコールもシングル ナンバー リーチ経由でユーザのリモート接続先に送信される場合は、この CSS によってシステムからリモート接続先電話機に到達する方法が決定されます。したがって、CSS を通して、PSTN またはモバイル ボイス ネットワークに到達するために、適切なルート パターンとゲートウェイを含むパーティションにアクセスできる必要があります。

リモート接続先プロファイル ルーティング CSS を設定する場合は、この CSS 内のルート パターンが、ユーザのデスクトップフォンへの着信コールを経路設定するゲートウェイと同じコール アドミッション制御ロケーションにあるゲートウェイを指すようにすることを推奨します。これによって、コールをリモート接続先に経路設定するときに、2 地点間の帯域幅不足によるコール アドミッション制御拒否が発生しなくなります。さらに、WAN 帯域幅が不十分な場合は、初期シングル ナンバー リーチ コールの経路設定後のコール アドミッション制御チェックで拒否されないため、同じコール アドミッション制御ロケーション内のゲートウェイに着信コール レッグと発信コール レッグを経路設定することによって、このコール中の以降のデスク フォンまたはリモート接続先のピックアップ動作で WAN 帯域幅のオーバーサブスクリプションが発生する可能性のあるコール アドミッション制御の必要がなくなることが保証されます。

標準ローカル ルート グループを使用するルート リストを指すルート パターンを使用する場合は、発信者のデバイス プールで設定されたローカル ルート グループが使用されます。この場合リモート接続先へのコール レッグの出力ゲートウェイは、元の発信側デバイスに対してローカルです。PSTN からのコールの場合、これは、元の発信者（この場合、着信ゲートウェイ）と同じコール アドミッション制御ロケーションで出力ゲートウェイを使用する上記の要件を満たすのに役立ちます。

2 段階ダイヤリング対象コールを送信したときのコール アドミッション制御拒否が最小化されるようにすることも同様に重要です。2 段階ダイヤリング対象コールのコール アドミッション制御拒否は、発信コール レッグをルーティングするために使用される出力ゲートウェイが着信コール レッグの入力ゲートウェイによって選択されるようにローカル ルート グループ コンストラクトを使用することによって最小化、または回避できます。この方法で、使用される入力ゲートウェイおよび出力ゲートウェイは、同じコール アドミッション制御ロケーションにあるようになります。また、リモート接続先プロファイルのデバイス レベルの CCS 内のルート パターンは、モバイル ボイス アクセス システムまたはエンタープライズ機能アクセス システムのアクセス番号への着信コール レッグを処理した入力ゲートウェイと同じコール アドミッション制御ロケーションにある出力ゲートウェイを指す必要があります。ただし、デスクトップフォンがモバイル ボイス アクセスまたはエンタープライズ機能アクセス システムのアクセス番号が転送されるゲートウェイとは異なるコール アドミッション制御ロケーション内に存在する場合は、以降のデスクトップフォンのピックアップによって、WAN 帯域幅のオーバーサブスクリプションが発生する可能性があることに注意してください。

自動発信者 ID 照合とエンタープライズ コール アンカリング

理解しておく必要のある Unified Mobility ダイヤル プランのもう一つの側面は、設定済みのリモート接続先電話機からの着信コールに対する自動発信者 ID 識別に関するシステム動作です。着信コールがシステムに入ると、そのコールに対して提供された発信者 ID が設定済みのすべてのリモート接続先電話機と比較されます。一致するものが見つかった場合は、そのコールが自動的にその会社のものと固定されるため、ユーザは通話切替機能を呼び出したり、通話中のコールをデスクトップフォンでピックアップできます。この動作は、着信コールがモバイル ボイス アクセスまたはエンタープライズ機能アクセスを使用したモビリティ コールとして開始されていない場合でも、モビリティ ユーザのリモート接続先電話機からの着信コールすべてに対して行われます。

(注)　設定済みのリモート接続先番号に対する自動着信コール発信者 ID 照合は、Matching Caller ID with Remote Destination サービス パラメータが Partial Match と Complete Match のどちらに設定されているかの影響を受けます。この設定に関する詳細については、リモート接続先の設定と発信者 ID の照合（21-70 ページ）を参照してください。

自動エンタープライズ コール アンカリングに加えて、設定済みのリモート接続先電話機から会社に電話がかかった場合の着信コール ルーティングと発信コール ルーティングも考慮する必要があります。設定済みのリモート接続先からのコールに対する着信コール ルーティングは、Inbound Calling Search Space for Remote Destination サービス パラメータの設定によって次の 2 つの方法のどちらかで発生します。デフォルトで、このサービス パラメータは、**Trunk or Gateway Inbound Calling Search Space** に設定されます。このサービス パラメータがデフォルト値に設定されている場合、設定済みのリモート接続先からの着信コールは、コールが着信する PSTN ゲートウェイまたはトランクの着信通話サーチ スペース（CSS）を使用してルーティングされます。一方、[リモート接続先の着信通話サーチ（Inbound Calling Search Space for Remote Destination）] パラメータが [リモート接続先プロファイル+回線通話サーチスペース（Remote Destination Profile + Line Calling Search Space）] に設定されている場合は、リモート接続先からの着信コールが、PSTN ゲートウェイまたはトランクの着信 CSS をバイパスして、代わりに、関連するリモート接続先プロファイル CSS（と回線レベル CSS の組み合わせ）を使用してルーティングされます。

リモート接続先電話機からの着信コールの特性を考えると、このような着信コールへのアクセスを社内の電話機に到達させるために必要なすべてのパーティションに提供するためには、コーリング サーチ スペースが適切に設定されていることを確認する必要があります。これによって、リモート接続先電話機からの適切なコール ルーティングが保証されます。

(注)　設定済みのリモート接続先電話機からではない着信コールでは、必ず、トランクまたはゲートウェイ着信 CSS が使用されるため、Inbound Calling Search Space for Remote Destination サービス パラメータの影響を受けません。

モバイル ボイス アクセスまたはエンタープライズ機能アクセス コールの発信コール ルーティングでは、必ず、リモート接続先プロファイル回線 CSS とデバイス レベル CSS を連結したものが使用されるため、オフネットまたは PSTN アクセスに必要なすべてのルート パーティションへのアクセスを提供するためには、これらのコーリング サーチ スペースが適切に設定されていることを確認する必要があります。これによって、リモート接続先電話機からの適切な発信コール ルーティングが保証されます。

Intelligent Session Control およびすべてのシェアド ライン呼び出し

Intelligent Session Control 機能を使用すると、設定されたリモート接続先番号への社内からの直接コールを、自動的にコール アンカリングできます。通常、モビリティ コール アンカリングは、ユーザの会社の電話番号にかけられたコール、またはユーザの会社の電話番号からかけられたコールでだけ行われます。エンタープライズ 2 段階ダイヤリングによって外部から発信されたコールは、内部コールとしてルーティングされるため、システムはアンカリングを行います。Intelligent Session Control 機能を有効にすると、社内から設定済みリモート接続先への直接コールもアンカリングが行われます。

この機能は、Reroute Remote Destination Calls to Enterprise Number サービス パラメータを True に設定することによって有効にします。デフォルトで、このサービス パラメータは False に設定されており、この機能は無効になっています。この機能を有効にすると、ダイヤルされたリモート接続先へのコールが PSTN 経由でルーティングされるだけでなく、コールが自動的に会社のゲートウェイ内部で固定されます。このタイプのコールを固定することによって、着信側モバイル ユーザが通話切替機能およびデスクトップフォンのピックアップまたはセッション ハンドオフを呼び出すことができるようになります。

たとえば、Intelligent Session Control 機能が有効にされており、モビリティ対応ユーザのリモート接続先番号が携帯の番号に対応する 408 555 1234 として設定されているとします。別のユーザがデスクトップフォンからそのモビリティ対応ユーザのリモート接続先番号（408 555 1234）にダイヤルすると、そのコールは PSTN 経由でリモート接続先にルーティングされ、同時に会社のゲートウェイでアンカリングされます。コールがセットアップされて固定されると、着信側モビリティ対応ユーザは、保留、転送、会議などの通話切替機能を呼び出したり、デスクトップフォンのピックアップまたはセッション ハンドオフを実行したりできるようになります。

この同じ例で、Intelligent Session Control 機能が無効であるとすると、システム ユーザがこのモビリティ対応ユーザのリモート接続先に社内のデスク フォンから直接ダイヤルした場合、そのコールは PSTN 経由で着信側リモート接続先にルーティングされますが、アンカリングはされません。その結果、モバイル ユーザは、保留や転送などの通話切替機能を呼び出したり、デスクトップフォンのピックアップまたはセッション ハンドオフを実行したりできません。

この機能を有効にする場合は、ダイヤル プランの設定およびコール ルーティングへの影響を理解することが重要となります。この機能を呼び出すには、内部ユーザが PSTN のリモート接続先番号に到達するためにダイヤルする番号（必要なすべての PSTN 振り分け用数字を含む）は、システムに設定されているリモート接続先（またはモビリティ ID）番号と一致する必要があります。たとえば、リモート接続先番号がシステムに 408 555 1234 と設定されており、通常、発信する番号に加えて PSTN 振り分け用数字 91 を内部ユーザがダイヤルする必要がある場合は、再ルーティングおよびそれによるエンタープライズ コール アンカリングは実行されません。これは、ユーザが PSTN のリモート接続先に到達するために 91 408 555 1234 をダイヤルした一方、リモート接続先は 408 555 1234 と設定されており、これらの番号が一致しないためです。

この機能が適切に機能するには、設定されたリモート接続先と、PSTN のこのリモート接続先に到達するためにダイヤルする必要がある番号とが一致する必要があります。これらの番号が一致するようにするには、Matching Caller ID with Remote Destination サービス パラメータを **Partial Match** に設定します。このパラメータを Partial Match に設定し、Number of Digits for Caller ID Partial Match サービス パラメータを使用して部分一致対象桁数を指定することによって、ダイヤルされた番号に PSTN 振り分け用数字が含まれていても、設定されたリモート接続先番号とダイヤルされた番号が一致します。

前の例を使用し、システムが 10 桁の部分一致を使用するように設定されているとすると、ダイヤルされた番号 9 1 408 555 1234 は、設定されたリモート接続先 408 555 1234 に一致します。これは、部分一致では、Number of Digits for Caller ID Partial Match に指定された桁数（この場合は 10 桁）が照合されるためです。2 つの番号は、右から左に向かって照合されます。ダイヤルされた番号 9 1 408 555 1234 の最後の 10 桁は 408 555 1234 であり、この 10 桁が、10 桁の設定されたリモート接続先（408 555 1234）に一致します。この例では、発信コールは社内で固定され、着信側モバイル ユーザは通話切替機能を呼び出したり、デスクトップフォンのピックアップまたはセッション ハンドオフを実行したりできます。

この機能を使用する場合、一見すると、必要なすべての PSTN 振り分け用数字を含むリモート接続先番号またはモビリティ ID 番号を設定する方が簡単に見えます。しかし、必要な PSTN 振り分け用数字を含む番号を設定し、発信者 ID の部分一致を設定していない場合、設定されたリモート接続先またはモビリティ ID からの着信コールに対して発信者 ID の自動照合およびエンタープライズ アンカリングを実行できません。前の例では、リモート接続先番号が 9 1 408 555 1234 と設定されており、発信者 ID の完全一致が使用されている場合、リモート接続先からの着信コールの発信者 ID は 408 555 1234 となり、これらの番号が一致せず、リモート接続先からの着信コールが想定どおりに固定されません。

このように発信コールでダイヤルされる Intelligent Session Control 機能を使用する場合には、番号と、着信コールの設定されたリモート接続先番号が異なる可能性があるため、PSTN に到達するために 1 つ以上の振り分け用数字が必要なすべての配置において、発信者 ID の（完全一致ではなく）部分一致を有効にすることを推奨します。これにより、PSTN 振り分け用数字を使用してリモート接続先番号に直接発信されたコールが一致し、アンカーされるようになります。一方で、PSTN に到達するために振り分け用数字が必要なく、ユーザが完全な E.164 番号をダイヤルして PSTN にコールをルーティングできる場合には、発信者 ID と照合されるリモート接続先の番号が、PSTN のリモート接続先またはモビリティ ID に到達するために内部ユーザがダイヤルする番号と同じであるため、発信者 ID の完全一致設定を使用することを推奨します。

Intelligent Session Control 機能を有効にする場合は、再ルーティング機能の実行時の、会社の回線およびリモート接続先回線の動作を理解することも重要です。コールの再ルーティングでは、Do Not Disturb（DND）、Access Lists と Time of Day コール フィルタリング、および Delay Before Ringing Timer の各リモート接続先回線設定は無視されます。再ルーティングされるすべてのコールは、フィルタリングされずにすぐにルーティングされます。会社のデスクトップフォン回線設定も、デフォルトで無視されるか、またはバイパスされます。ただし、Ignore Call Forward All on Enterprise DN サービス パラメータを False に設定することによって、再ルーティング機能の実行時に会社のデスクトップフォン回線の Call Forward All 設定を有効にできます。このパラメータが False に設定されている場合、会社のデスクトップフォン回線に Call Forward All の接続先が設定されていると、再ルーティングの実行時にコールはリモート接続先にルーティングされません。代わりに、コールは Call Forward All の接続先にルーティングされます。デフォルトで、このサービス パラメータは True に設定されており、会社のデスクトップフォン回線の Call Forward All 設定は無視されます。

Intelligent Session Control 機能は、すべてのシェアド ライン呼び出し機能を使用することによって、さらに強化できます。この機能は、すべてのシェアド ライン呼び出しサービス パラメータを True に設定することによって有効になります。デフォルトで、このサービス パラメータは True に設定されており、この機能は有効になっています。ただし、すべてのシェアド ライン呼び出し機能は Intelligent Session Control 機能に依存しており、この機能も、すべてのシェアド ライン呼び出し機能を使用するときに順番に有効にする必要があります。すべてのシェアド ライン呼び出し機能、Intelligent Session Control 機能の両方を有効にすると、システムが内部で発信されたコールをダイヤル対象リモート接続先に PSTN でルーティングさせるだけでなく、ユーザの他のシェアド ライン デバイスもすべて、コールを受信します。これには、ユーザの会社のデスクフォンおよび他の設定済みリモート接続先が含まれます。呼び出されたユーザは、デバイス上で着信コールに応答でき、コールは会社にアンカーされます。

（注）　すべてのシェアド ライン呼び出しが有効であるときに、モバイル クライアント デバイスは、デバイスが Unified CM に登録されている場合にはデバイスの携帯電話音声インターフェイスでコールを受信しません。

発信者 ID 変換

設定済みのリモート接続先番号によってクラスタに発信されたコールは、自動的に、発信者 ID または発番号が、発信元のリモート接続先電話機の番号から関連する会社のデスクトップフォンの番号に変更されます。たとえば、408 555-7890 という番号のリモート接続先電話機が設定され、555-1234 という番号の会社のデスクトップフォンに関連付けられている場合は、クラスタ内の任意の電話番号に向けられたユーザのリモート接続先電話機からのコールがすべて、自動的に、発信者 ID が 408 555-7890 のリモート接続先電話番号から 555-1234 の会社の電話番号に変更されます。これによって、アクティブ コールの発信者 ID 表示とコール履歴ログの発信者 ID に、ユーザの携帯電話の番号ではなく、会社の卓上電話の番号が反映され、すべての返信コールがユーザの会社の電話番号に対して発信され、このようなコールが会社に固定されることが保証されます。

同様に、リモート接続先電話機から外部の PSTN 接続先へのコールと、モバイル ボイス アクセスやエンタープライズ機能アクセス 2 段階ダイヤリング経由で会社にアンカーされたコール、つまり、シングル ナンバー リーチの結果として PSTN に分岐されたコールも、発信者 ID が発信元のリモート接続先電話機の番号から関連する会社の電話番号に変更されます。

最後に、発番号を会社の電話番号ではなく、会社の DID 番号として外部の PSTN 電話機に供給する場合は、発信側のトランスフォーメーション パターンを使用できます。発信側のトランスフォーメーション パターンを使用して発信者 ID を会社の電話番号から会社の DID に変換することによって、外部の接続先からの返信コールは、完全な会社の DID 番号でダイヤルされていることから、その会社に固定されます。このような変換とダイヤル プランの意味については、Cisco Unified Mobility 固有の考慮事項（14-92 ページ）を参照してください。

モバイル ボイスと Unified Mobility の間の相互作用のインテリジェント プロキシミティ

Cisco DX シリーズ エンドポイントと Cisco IP Phone 8851 および 8861 でのモバイル ボイス機能のインテリジェント プロキシミティには、Unified Mobility 機能セット（シングル ナンバー リーチ（SNR）、リモート接続先およびデスク フォンのピックアップ、エンタープライズ 2 段階ダイヤリング、およびモバイル ボイスメールの回避を含む）との互換性があります。DX シリーズ エンドポイントと IP Phones 8851 および 8861 でのモバイル ボイスと Bluetooth ペアリングのインテリジェント プロキシミティの詳細については、インテリジェント プロキシミティ（8-15 ページ）を参照してください。

Unified Mobility に関するガイドラインと制約事項

（注）　Cisco Unified Mobility ソリューションは、シスコ機器でのみ検証されています。このソリューションは他のサードパーティ製 PSTN ゲートウェイおよびセッション ボーダー コントローラ（SBC）でも機能しますが、Cisco Mobility のそれぞれの機能が期待通りに機能する保証はありません。サードパーティ製 PSTN ゲートウェイまたは SBC でこのソリューションを使用している場合、シスコ テクニカル サポートが発生した問題を解決できない可能性があります。

次のガイドラインと制約事項は、Unified CM テレフォニー環境内のシングル ナンバー リーチの配置と動作に関連して適用されます。

- シングル ナンバー リーチは、PRI TDM PSTN 接続だけでサポートされます。T1 接続または E1-CAS、FXO、FXS、および BRI PSTN 接続はサポートされません。この PRI 要件は、完全な機能サポートを保証するためには、Cisco Unified CM で PSTN からの迅速な応答と切断の指示を受信する必要があることに基づいています。応答指示は、シングル ナンバー リーチ コールが特定のリモート接続先で応答されたときに、Cisco Unified CM でデスク フォンとその他のリモート接続先の呼び出しを停止するために必要です。加えて、応答指示は、シングル企業ボイスメール ボックス機能をサポートするために必要です。最後に、切断指示はデスクトップフォンピックアップのために必要です。PRI PSTN 接続では、必ず、応答指示または切断指示が提供されます。
- シングル ナンバー リーチは、SIP トランク VoIP PSTN 接続でもサポートされます。Unified CM SIP トランクとサービス プロバイダー トランクの間の責任分界点として、Cisco IOS Unified Border Element の使用が推奨されます。VoIP ベースの PSTN 接続では、VoIP ベースの PSTN 接続によって提供されるエンドツーエンドのシグナリング パスによって、Unified CM に迅速な応答と切断の指示を提供できます。
- シングル ナンバー リーチでは、ユーザあたり最大 2 つの同時コールをサポートできます。それ以上の着信コールは、自動的に、ユーザのボイスメールに転送されます。

- シングル ナンバー リーチは、Multilevel Precedence and Preemption（MLPP）と連動しません。コールが MLPP によって割り込まれた場合は、そのコールに対するシングル ナンバー リーチ機能が無効になります。
- シングル ナンバー リーチ サービスでは、ビデオ コールに応答できません。デスクトップ フォンで受信されたビデオ コールは携帯電話でピックアップできません。
- リモート接続先は、別のクラスタまたはシステム上の時分割多重（TDM）装置またはオフシステム IP 電話にする必要があります。IP 電話は、リモート接続先と同じ Unified CM クラスタ内に設定できません。
- モバイル ボイス アクセスの VoiceXML 機能は、Cisco IOS XE ソフトウェアではサポートされていません。Cisco IOS XE はネイティブ VoiceXML をサポートしていないため、Cisco 4000 シリーズ ISR をモバイル ボイス アクセスの VoiceXML ゲートウェイとして使用することはできません。代わりに、VoiceXML 機能を提供するために別個の H.323 Cisco IOS ゲートウェイを導入し、ヘアピニング対応のモバイル ボイス アクセスを設定してください。

ガイドラインと制約事項の詳細については、次の Web サイトで入手可能な『*Feature Configuration Guide for Cisco Unified Communications Manager*』の最新版で Cisco Unified Mobility に関する情報を参照してください。

https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html

Cisco Unified Mobility のキャパシティ プランニング

Cisco Unified Mobility は、Unified CM クラスタあたり最大 40,000 のリモート接続先またはモビリティ ID をサポートします。モビリティ対応ユーザの最大数は、ユーザあたり 1 つのリモート接続先またはモビリティ ID を想定すると、40,000 人のユーザになります。ユーザあたりのリモート接続先数またはモビリティ ID 数が増加するほど、サポートされるモビリティ対応ユーザ数が減少します。

（注）　モビリティ対応ユーザは、リモート接続先プロファイルを持ち、1 つ以上のリモート接続先またはモバイル クライアント デバイスおよびモビリティ ID が設定されているユーザとして定義されます。

（注）　モビリティ ID は、システム内でリモート接続先と同様に設定され、リモート接続先と同じ容量になります。ただし、リモート接続先と違って、モビリティ ID は、リモート接続先プロファイルではなく、直接電話機に関連付けられます。モビリティ ID は、Cisco Jabber を実行するデュアル モード モバイル クライアント デバイスだけに適用されます。

Cisco Unified Mobility の拡張性と性能は、モビリティ ユーザ数、ユーザごとのリモート接続先数またはモビリティ ID 数、およびそれらのユーザの最繁時呼数（BHCA）レートに依存します。ユーザあたりの複数のリモート接続先またはユーザあたりの高い BHCA によって、Cisco Unified Mobility の容量が減少することがあります。Unified CM サーバ ノードのキャパシティ、およびハードウェア固有のノードあたりとクラスタあたりのキャパシティを含む Cisco Unified Mobility のサイジングの詳細については、コラボレーション ソリューション サイジング ガイダンス（25-1 ページ）の章を参照してください。

Cisco Unified Mobility の設計上の考慮事項

Unified Mobility を配置する場合は、次の設計上の推奨事項に従ってください。

- PSTN ゲートウェイ プロトコルで、アウトオブバンド DTMF リレーが使用できる、または、インバンド DTMF をアウトオブバンド DTMF に変換するためのメディア ターミネーション ポイント（MTP）が割り当てられていることを確認します。PSTN 接続用の Cisco IOS ゲートウェイを使用している場合は、アウトオブバンド DTMF リレーがサポートされます。ただし、サードパーティ製ゲートウェイでは、一般的なアウトオブバンド DTMF 方式がサポートされない可能性があるため、結果として、MTP が必要になる場合があります。エンタープライズ機能アクセス 2 ステージ ダイヤリング機能と通話切替機能を使用するには、Cisco Unified CM で DTMF 番号をアウトオブバンドで受信する必要があります。

  （注）　インバンド DTMF をアウトオブバンド DTMF に変換するために MTP 上でリレーする場合は、十分な MTP 容量が提供されることを確認してください。エンタープライズ機能アクセス 2 ステージ ダイヤリングまたは通話切替機能の高い使用頻度が予想される場合は、ハードウェア ベースの MTP または Cisco IOS ソフトウェア ベースの MTP を推奨します。

- Unified Mobility を配置する前に、PSTN プロバイダーと連携して次のことを保証する必要があります。
  - 会社へのすべての着信コールに関する発信者 ID が、サービス プロバイダーから供給される。これは、エンタープライズ機能アクセス 2 ステージ ダイヤリングまたは通話切替転送、会議、およびダイレクト コール パーク機能が必要な場合の要件です。
  - 発信コールの発信者 ID は、サービス プロバイダーに制限されない。これは、モビリティ対応ユーザが、一般的な会社のシステム番号やその他の意味のない発信者 ID ではなく、リモート接続先にいる元の発信者の発信者 ID を受信することが期待される場合の要件です。

    （注）　プロバイダーによっては、トランク上の発信コールの発信者 ID が、そのトランクで処理される DID に制限される場合があります。そのため、発信者 ID が制限されない別の PRI トランクをプロバイダーから入手する必要があります。無制限の PRI トランクを要求すると、プロバイダーによっては、このトランク経由で緊急電話番号にコールを送信または発信しないことが記された署名付きの同意書を要求される場合があります。

    （注）　プロバイダーによっては、[Redirected Dialed Number Identification Service (RDNIS)] フィールドまたは SIP の Diversion ヘッダーにトランクで処理される DID が含まれている限り、そのトランクには発信コールの発信者 ID を無制限で許可します。ゲートウェイまたはトランクの設定ページで [Redirecting Number IE Delivery] > [Outbound] チェックボックスをオンにすることによって、リモート接続先に分岐されたコールの RDNIS または SIP の Diversion ヘッダーにユーザの企業番号を取り入れることができます。RDNIS または SIP の Diversion ヘッダーに対応し、発信コールの発信者 ID を無制限で許可しているかどうかは、サービス プロバイダーに問い合わせてください。

- 一般に、モビリティ コール フローには複数の PSTN コール レッグが含まれるため、Unified Mobility にとって PSTN ゲートウェイ リソースの計画と配置が極めて重要です。モビリティ対応ユーザ数が多い場合は、PSTN ゲートウェイ リソースを増やす必要があります。PSTN 利用を制限または削減するために、次の方法が推奨されています。
  - モビリティ対応ユーザあたりのリモート接続先数を 1 つに制限します。これによって、着信コールをユーザのリモート接続先に転送するために必要な DS0 数が削減されます。コールがユーザの会社の電話番号に送られると、そのコールがリモート接続先のいずれかで応答されなくても、設定済みのリモート接続先ごとに 1 つずつの DS0 が消費されます。コールがリモート接続先で応答されなくても、リモート接続先あたり 1 つの DS0 が 10 秒間も使用される可能性があります。
  - アクセス リストを使用して、着信コールの発信者 ID に基づいて、特定のリモート接続先へのコールの拡張を拒否または制限します。時刻に基づいてアクセス リストを呼び出すことができるため、エンド ユーザまたは管理者がアクセス リストを頻繁に更新する必要がありません。
  - 会社の番号に電話がかかってきたときに DS0 が使用されないよう、不要になったシングル ナンバー リーチを無効にするようエンド ユーザに伝えてください。シングル ナンバー リーチが無効になっている場合は、着信コールでデスク フォンの呼出音が鳴りますが、誰も電話に出なければ、そのコールが会社のボイスメールに転送されます。
- ロケーション間の WAN 帯域幅の不足によってコール アドミッション制御が拒否される可能性と、デスク フォンのピックアップまたはリモート接続先のピックアップによって WAN 帯域幅のオーバーサブスクリプションが発生する可能性があるため、リモート接続先プロファイル CSS と CSS の再ルーティングを設定して、CSS 内のルート パターンが、着信コール レッグが到達するゲートウェイと同じコール アドミッション制御ロケーション内に配置されたゲートウェイを指すようにすることを推奨します。詳細については、リモート接続先プロファイルの設定（21-73 ページ）を参照してください。
- 公衆網にアクセスするために公衆網振り分け用数字をダイヤルする必要がある配置において Intelligent Session Control 機能を有効にする場合は、[リモート接続先との発信者 ID の一致（Matching Caller ID with Remote Destination）] サービス パラメータを [部分一致（Partial Match）] に設定し、適切な桁数（[発信者 ID の部分一致の桁数（Number of Digits for Caller ID Partial Match）] サービス パラメータ）を設定して、設定されたリモート接続先またはモビリティ ID の部分一致が実行されるようにすることを推奨します。これにより、Intelligent Session Control 機能、およびモビリティの発信者 ID の自動照合機能とアンカリング機能が適切に機能するようになります。

シスコのモバイル クライアントおよびデバイス

モバイル ユーザ、携帯電話、携帯通信事業者サービスが普及するにつれて、単一のデバイスを使用して社内および社外の両方で音声、ビデオ、およびデータ サービスを使用できることがますます魅力的なソリューションとなっています。デュアル モード スマート フォン、およびそのスマート フォンで実行されるクライアントなどのモバイル デバイスは、企業に対して、カスタマイズされた音声、ビデオ、およびデータ サービスを社内にいながらユーザに提供する機能、および一般的な音声およびデータ サービスの代替の接続方法としてモバイル通信事業者ネットワークを利用する機能を利用可能にします。社内で音声、ビデオ、およびデータ サービスを利用可能にし、モバイル クライアント サービスに対してネットワーク接続を提供することによって、企業はこれらのサービスをローカルまたはリモートでより安価な接続コストで提供できます。たとえば、企業ネットワーク上で発信される Voice over IP（VoIP）コールは、通常、モバイル ボイス ネットワーク上で発信される同じコールよりもコストが少なく済みます。

Voice and Video over IP（VVoIP）機能に加えて、これらのモバイル クライアントとデバイスによって、モバイル ユーザは他のバック エンドのコラボレーション アプリケーションとサービスにアクセスできます。シスコのモバイル クライアントとサービスを通じて利用可能なサービスおよびアプリケーションには、会社のディレクトリ、会社のボイス メール、および XMPP ベースの IM（インスタント メッセージング）とプレゼンスが含まれます。さらに、ユーザがシングル ナンバー リーチ、モバイル ボイス アクセスまたはエンタープライズ機能アクセスを介したエンタープライズ 2 段階ダイヤリング、および 1 つの企業ボイスメール ボックスなどのモバイル デバイスで追加機能を利用できるように、これらのクライアントおよびデバイスは Cisco Unified Mobility とともに配置できます。

この項では、モバイル クライアントのアーキテクチャについて説明します。また、企業の WLAN ネットワークとモバイル ボイス ネットワークとの間でアクティブなボイスコールを移動する場合のリモート セキュア接続およびハンドオフに関する考慮事項を含む、シスコのモバイル クライアントとデバイスによって提供される共通の機能について説明します。一般的なモバイル クライアント ソリューション アーキテクチャおよび機能について説明した後、ここでは、次の特定のモバイル クライアントとデバイスのさまざまな機能および統合に関する考慮事項について説明します。

- Cisco Jabber：Android および iPhone や iPad などの Apple iOS モバイル デバイスに使用できるモバイル クライアントです。企業の WLAN ネットワークの IP 経由、またはモバイル データ ネットワーク経由で音声またはビデオ コールを発信する機能、ならびに社内ディレクトリと企業ボイスメール サービス、および XMPP ベースの企業向け IM およびプレゼンスにアクセスする機能を提供します。
- Cisco Spark：Android および iPhone や iPad などの Apple iOS デバイスに使用できるモバイル クライアントです。IP 経由の音声コールやビデオ コール、セキュアなパーシステント メッセージング、およびファイル共有を可能にする、1 対 1 および 1 対多のクラウド ベースのコラボレーション ルームを提供します。
- Cisco WebEx Meetings：Android、BlackBerry、Windows Mobile、および iPhone や iPad などの Apple iOS デバイスに使用できるモバイル クライアントです。ユーザが移動中に Cisco WebEx 会議に出席、参加する機能を提供します。
- Cisco AnyConnect Mobile：Android および Apple iOS デバイスで使用可能なモバイル クライアントであり、ユーザが企業外にいる場合でも、オンプレミス コラボレーション アプリケーションおよびサービスへのアクセスに対して、企業が安全にリモート VPN から接続できるようにします。

また、シスコのモバイル クライアントとデバイスのハイ アベイラビリティおよびキャパシティ プランニングの考慮事項についても説明します。

シスコのモバイル クライアントおよびデバイスのアーキテクチャ

シスコのモバイル クライアントは、IP ベースのネットワーク接続機能（IEEE 802.11 無線ローカル エリア ネットワークまたはモバイル プロバイダーのデータ ネットワーク）およびデュアル モード電話機だけを備えたタブレットおよびハンドヘルド デバイスなどのさまざまなモバイル デバイスで配置されます。デバイスが従来のセルラーまたはモバイル ネットワーク テクノロジーによってモバイル ボイス ネットワークとデータ キャリア ネットワークの両方に接続でき、また、802.11 を使用してワイヤレス ローカルエリア ネットワーク（WLAN）に接続できる 2 つの物理インターフェイスが含まれます。シスコのモバイル クライアントとデバイスは、802.11 WLAN 経由でのオンプレミス データおよびリアルタイム トラフィック（音声およびビデオ）接続を可能にします。また、これらのクライアントおよびデバイスは、パブリックまたはプライベートの WLAN 経由、またはモバイル データ ネットワーク経由で企業へのリモート データおよびリアルタイム トラフィック（音声およびビデオ）接続を提供します。プロバイダーの携帯電話音声の無線を備えたデバイスでは、音声接続がモバイル ボイス ネットワークおよび PSTN 経由で有効にされることもあります。

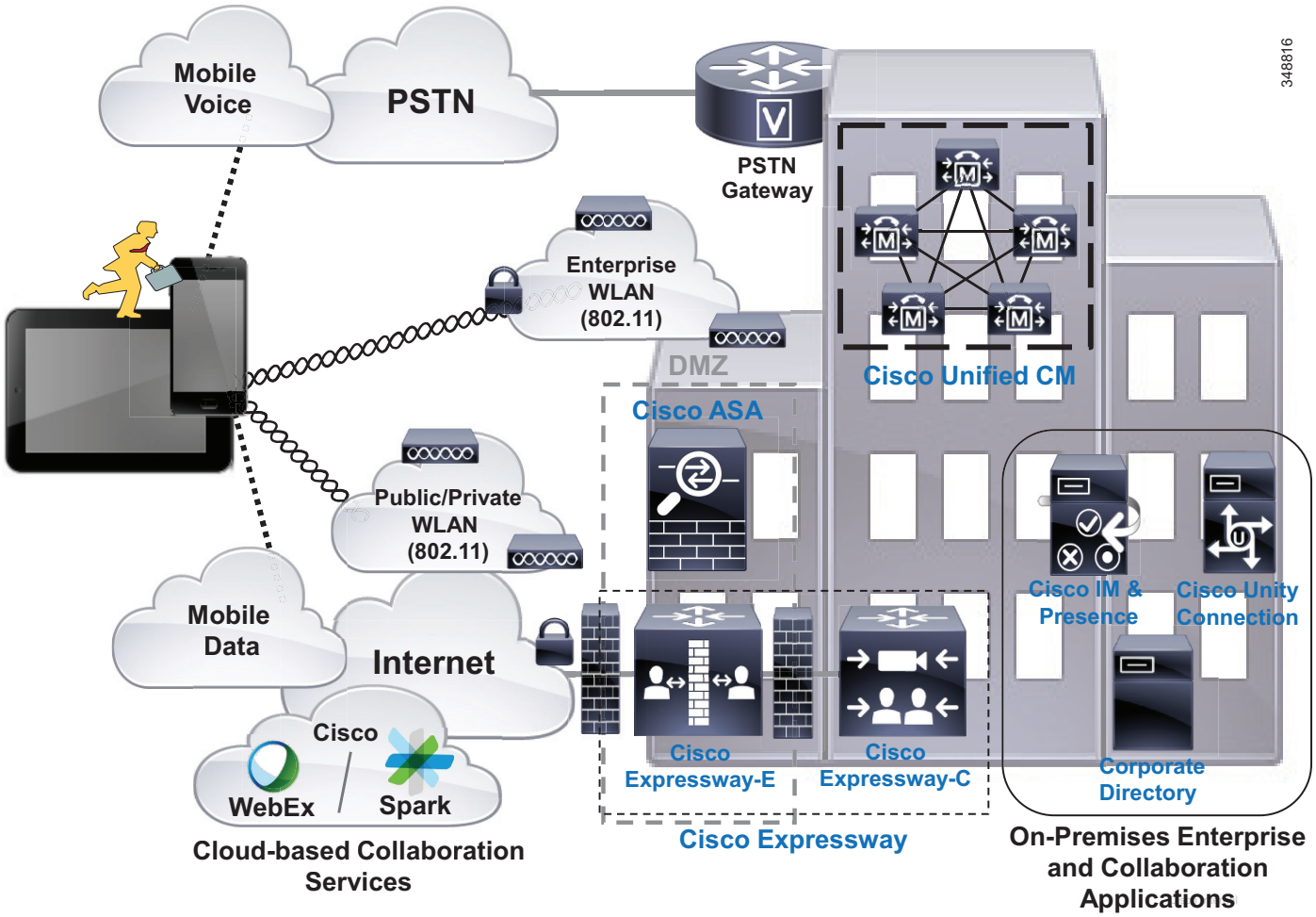
(注)　この項で*デュアルモード電話機*という用語を使用する場合、802.11 に準拠した無線機、および音声とデータの通信事業者ネットワークへの接続用の携帯電話無線機を備えたデバイスを指します。Digital Enhanced Cordless Telecommunications（DECT）やその他の規格に準拠した無線機、または複数の携帯電話無線機を備えたデュアルモード デバイスは、この項のデュアルモード電話機には含まれません。

図 21-27 は、Cisco Collaboration 展開にモバイル クライアント デバイスを接続して有効にするための、基本的なシスコのモバイル クライアントおよびデバイスのソリューション アーキテクチャを示します。音声サービスとビデオ サービスの場合は、モバイル クライアント デバイスが企業の WLAN に関連付けられるか、インターネットに（パブリックまたはプライベートから WLAN ホット スポットまたはモバイル データ ネットワークから）接続され、シスコのモバイル クライアントは、Session Initiation Protocol（SIP）を使用して会社の電話機として Cisco Unified CM に登録されます。登録されると、クライアント デバイスは、基礎となる企業の Cisco IP テレフォニー ネットワークを利用して、コールを発信および受信します。モバイル デバイスが企業ネットワークに接続されており、かつクライアントが Unified CM に登録されている場合、そのデバイスはユーザが持つ会社の電話番号を使用して発着することができます。ユーザの会社の電話番号に着信コールがあると、モバイル クライアント デバイスの呼出音が鳴ります。ユーザが Cisco IP デスク フォンを持っている場合は、モバイル クライアントを登録すると、ユーザの会社の番号でシェア ド回線インスタンスが使用可能になり、コールが着信すると、ユーザのデスク フォンとモバイル デバイスの両方の呼出音が鳴ります。モバイル クライアント デバイスが登録されておらず、かつ条件を満たしていない場合（携帯電話網へ接続している、ユーザに対して Cisco Unified Mobility が有効になっている、ユーザの携帯電話番号に対してシングル ナンバー リーチが有効になっている）、そのモバイル クライアント デバイスは会社の番号への着信コールを受け取りません。このようなシナリオではモバイル ボイス ネットワークおよび PSTN は音声のみのコールの発信および受信に使用されます。

シングル ナンバー リーチなどの Unified Mobility 機能は、携帯電話音声の無線を持たないタブレットや他のモバイル クライアント デバイスと互換性がありません。その理由は、これらの非デュアル モードのデバイスはネイティブ PSTN の到達可能番号を持たないためです。非デュアル モードのデバイスは、企業に接続してエンタープライズ呼制御システムに登録される場合だけ、エンタープライズ コールを発信および受信できます。

図 21-27 に示すように、シスコのモバイル クライアントとデバイスは、企業に接続されると、社内ディレクトリ、Cisco Unity Connection 企業ボイス メール システム、およびメッセージングやプレゼンスなどの追加エンタープライズ コラボレーション サービスにアクセスするための Cisco IM and Presence サービスなどの他のバック エンド アプリケーション サーバと直接通信することもできます。シスコのモバイル クライアントとデバイスは、IM and Presence と Web Conferencing サービスを提供する Cisco WebEx などのクラウドベースのコラボレーション サービスとも統合します。

図 21-27　シスコのモバイル クライアントおよびデバイスのアーキテクチャ



(注)　コールの音声とビデオの品質は、Wi-Fi またはモバイル データ ネットワーク接続によって異なります。Cisco Technical Assistance Center（TAC）は、3G/4G モバイル データ ネットワークまたは非社内 Wi-Fi ネットワーク経由で接続または音声およびビデオ品質の問題を解決できません。

モバイル ボイス ネットワークとモバイル データ ネットワーク、および WLAN ネットワークの両方に同時に接続するために、デュアルモードのモバイル クライアント デバイスでは、デュアル転送モード（DTM）がサポートされている必要があります。デバイスで DTM がサポートされていると、デバイスの携帯電話無線機と WLAN インターフェイスの両方からデバイスに到達可能になり、両方のインターフェイスでコールを発信および受信できます。モバイル ボイス ネットワークおよびモバイル データ ネットワークでデュアル接続デバイスがサポートされていない場合には、適切なモバイル クライアント操作が実行できない場合があります。

ワイヤレス LAN ネットワーク インフラストラクチャを介した音声およびビデオ

さまざまなモバイル クライアント デバイス機能、およびこれらの機能がエンタープライズ テレフォニー インフラストラクチャに与える影響について考慮する前に、適切に調整され、QoS に対応し、ハイ アベイラビリティを備えた WLAN ネットワークを計画して配置することが重要です。デュアルモード電話機および他のモバイル デバイスは、重要なシグナリング トラフィック、コールのセットアップやさまざまなアプリケーションへのアクセスのためのその他のトラフィック、およびリアルタイムの音声とビデオのメディア トラフィックにおいて、基礎となる WLAN インフラストラクチャを利用するため、データ トラフィックおよびリアルタイムのメディア トラフィックの両方に最適化された WLAN ネットワークの配置が必要になります。WLAN ネットワークの配置が適切でないと、多くの干渉が発生し、容量が低下するため、音声とビデオの品質が低下するだけでなく、コールがドロップされたり、つながらなかったりする可能性もあります。このように展開された WLAN は、コールの発信および受信に使用できなくなります。したがって、デュアル モード フォンと他のモバイル デバイスを配置する場合は、Voice and Video over WLAN の配置が正常に行われるように、配置前、配置中、配置後に WLAN 無線周波数（RF）サイト サーベイを実施して、適切なセル境界、設定、機能設定、容量、および冗長性を判断する必要があります。実稼働環境への配置の前に、WLAN の配置に対してモバイル デバイスのデバイス タイプまたはクライアントごとにテストを実施して、統合および動作が適切に行われるようにする必要があります。Quality of Service を含む WLAN サービス（Cisco Unified Wireless Network など）経由の最適なリアルタイム トラフィックが提供されるように配置および設定された WLAN を使用することによって、モバイル クライアント デバイスを正常に展開できます。

シスコでは、可能な場合は、音声およびビデオ トラフィックを生成できるモバイル クライアントとデバイスを接続するための 5 GHz 帯域 WLAN を利用することを推奨します（802.11a/n/ac）。5 GHz WLAN は、音声コールとビデオ コールに対し、スループットを改善して干渉を低減します。

Voice and Video over WLAN の配置およびワイヤレス デバイス ローミングの詳細については、ワイヤレス デバイス ローミング（21-6 ページ）を参照してください。

（注）　デュアルモード電話と他のモバイル クライアント デバイスは、インターネットを経由して会社に接続して呼制御やその他の Unified Communications サービスを利用できますが、シスコでは、このように接続した場合の音声とビデオの品質を保証できず、接続または音声とビデオの品質上の問題を解決できません。このような接続には、パブリックまたはプライベートの WLAN アクセス ポイント（AP）やホット スポット経由、あるいはモバイル データ ネットワーク経由の企業へのリモート接続があります。シスコでは、デュアル モード電話機およびその他のモバイル クライアント デバイスを接続するためのエンタープライズ クラスの音声およびビデオが最適化された WLAN ネットワークを推奨します。ほとんどのパブリックまたはプライベートの WLAN AP およびホット スポットは、データ アプリケーションおよびデバイスに合せて調整されています。この場合、AP 無線が最大電力に合わせて調整され、ダイナミック パワー コントロールにより、ネットワーク接続時にデバイスで最大電力が有効になり、クライアントの容量が大きくなります。このような調整方法は、パケットのドロップや損失時に再送信ができるデータ アプリケーションにとっては理想的ですが、パケットのドロップが大量に発生する可能性があるため、リアルタイム トラフィック アプリケーションでは音声とビデオの品質が非常に悪くなる可能性があります。同様に、モバイル プロバイダーのデータ ネットワークは、輻輳や接続のドロップの影響を受けやすいため、コール品質が低下したり、コールがドロップされる可能性があります。

クラウドまたはオフプレミスのコラボレーション インフラストラクチャ

シスコが提供する Cisco WebEx および Cisco Spark クラウド サービスは、企業構内にハードウェアを配置せずに利用することができます。すべてのサービス（音声、ビデオ、メッセージング、ファイルおよびコンテンツ共有、ミーティングおよびコラボレーション ルーム情報）は、インターネットまたはクラウドで安全にホストされます。これは、クライアントからのすべてのコンテンツ、音声とビデオのトラフィックがインターネットを通過し、Cisco Collaboration Cloud 内で混合され管理されていることを意味します。

Cisco Collaboration Cloud インフラストラクチャは、モバイル クライアントとデバイスに WebEx および Cisco Spark の以下の機能を提供します。

- WebEx ミーティング。コンテンツ共有機能を備えた Web 対応の音声およびビデオ会議を提供します。
- WebEx Messenger。XMPP IM and Presence、ポイントツーポイントの音声およびビデオ通話を提供します。
- Cisco Spark。ビデオ通話、メッセージング、ファイル共有機能を備えた 1 対 1 および 1 対多のコラボレーション ルームを提供します。

モバイル クライアントとデバイスの Quality of Service

シスコのモバイル クライアントのアプリケーションおよびデバイスは、シスコのコラボレーション QoS マーキング推奨事項に従って、一般にレイヤ 3 QoS パケット値をマークします。表 21-3 に、これらのマーキングを要約します。

表 21-3　シスコのモバイル クライアントのレイヤ 3 QoS マーキング

トラフィックのタイプ	レイヤ 3 マーキング	
	DSCP[1]	PHB[2]
音声メディア（音声のみ）	DSCP 46	PHB EF
ビデオ メディア（音声およびビデオ）	DSCP 34	PHB AF41
コール シグナリング	DSCP 24	PHB CS3

1. DiffServ コード ポイント
2. Per-hop behavior

シスコのモバイル クライアントのレイヤ 2 802.11 WLAN パケット マーキング（ユーザ プライオリティ、または UP）には、さまざまなモバイル プラットフォームおよびファームウェアの制約による課題があります。シスコのモバイル クライアントがさまざまなモバイル デバイスで実行されるため、レイヤ 2 ワイヤレス QoS が矛盾する場合があります。したがって、レイヤ 2 ワイヤレス QoS のマーキングを、WLAN のトラフィックを適切に処理するためには使用できません。

適切なモバイル クライアントのアプリケーション レイヤ 3 またはレイヤ 2 パケット マーキングにかかわらず、モバイル デバイスは、データおよびリアルタイム トラフィックの両方を含むさまざまなタイプのトラフィックの生成において、デスクトップ PC と同じさまざまな課題を示します。これを考えると、一般にモバイル デバイスはコラボレーション エンドポイントの信頼できないカテゴリに分類されます。モバイル クライアント デバイスが信頼されているエンドポイントとして見なされない配置では、ネットワークのプライオリティ キューイングと専用帯域幅が適切なトラフィックに適用されるようにするために、トラフィック タイプとポート番号に基づいてパケット マーキングまたは再マーキングすることが必要です。モバイル デバイスのトラフィックを再マーキングするだけでなく、ネットワーク ベースのポリシングとレート制限を使用してモバイル クライアント デバイスが大量のネットワーク帯域幅を消費しないようにすることを推奨します。

また、シスコのモバイル クライアントのレイヤ 3 マーキングが適切で、モバイル クライアント デバイスが信頼されているとすると、シスコのモバイル クライアントのトラフィックは、プライオリティの音声キューイングおよび専用ビデオ メディアとコール シグナリング帯域幅キューを使用して企業ネットワークを通過すると、適切にキューに入ります。

シスコのモバイル クライアントおよびデバイスの性能と機能

シスコのモバイル クライアントおよびデバイスは、さまざまな性能と機能が用意されます。機能や動作はデバイスによって異なりますが、この項に説明する共通の動作はすべての非クラウドベースのシスコ モバイル クライアントに適用されます。

エンタープライズ コール ルーティング

シスコのモバイル クライアントとデバイスが企業のテレフォニー インフラストラクチャおよび呼制御サービスを使用してコールを発信および受信できるため、モバイル クライアント デバイスに関係するコール ルーティングの性質と動作を理解することが重要です。

着信コール ルーティング

モバイル クライアントとデバイスが会社の電話番号を持つエンタープライズ デバイスとして Unified CM に登録すると、モバイル デバイスは、システムへの着信コールがユーザの会社の電話番号宛てである場合に呼出音が鳴ります。これは、PSTN または他の Unified CM クラスタや企業 IP テレフォニー システムから発信された着信コール、および同じ Unified CM 内の他のユーザから発信された着信コールにおける動作です。モバイル クライアント デバイスのユーザは、会社の電話番号に関連付けられている他のデバイスまたはクライアントを持っている場合には、これらのデバイスもシェアド ラインとして呼び出されます。コールがいずれかのデバイスまたはクライアントで応答されると、他のすべてのデバイスおよびクライアントの呼出音は停止します。

ユーザに対して Cisco Unified Mobility が有効になっており、ユーザのデュアルモード携帯電話の番号でシングル ナンバー リーチが有効になっているシナリオにおいては、着信コールはユーザの携帯電話の番号に対応するモビリティ ID に転送される場合があります。ただし、これは、モバイル デバイスが企業の WLAN ネットワークに接続されているか、セキュアな接続で企業ネットワークに接続され、Unified CM に登録されているかによって異なります。デバイスが企業ネットワークに直接接続されているか、セキュア リモート接続を介して接続されている場合には、携帯の番号でシングル ナンバー リーチが有効になっていても、ユーザの会社の電話番号への着信コールは、シングル ナンバー リーチによってモバイル デバイスのモビリティ ID に転送されません。Unified CM に登録されている場合にデュアルモード モバイル デバイスのモビリティ ID に会社の電話番号への着信コールが転送されない理由は、デバイスが企業ネットワークに接続され、利用可能であるということがシステムによって認識されるためです。したがって、企業の PSTN リソースの利用を少なくするために、Unified CM では、PSTN を経由してデュアルモード携帯電話のモバイル ボイス ネットワーク インターフェイスにコールを転送する処理は行われません。代わりに、会社の電話番号に対応する WLAN またはモバイル データ ネットワーク インターフェイスだけがコールを受信します。

（注） Dial Via Office が有効になっている場合（Dial Via Office（21-93 ページ）を参照してください）で、クライアントが登録されていても、Unified CM は着信コールを VoIP 経由で会社の電話番号に転送せず、シングル ナンバー リーチを使用してユーザの携帯電話番号に転送します。

モバイル デバイスが企業ネットワークに直接またはセキュア リモート接続を介して接続されていないか、Unified CM に登録されていない状況では、ユーザに対して Unified Mobility が有効になっており、そのモビリティ ID に対してシングル ナンバー リーチが有効である場合、会社の番号への着信コールが、設定済みのモビリティ ID ごとのデュアル モード携帯電話番号に転送されます。Unified Mobility でのモバイル クライアントおよびデバイスの統合の詳細については、Cisco Jabber と Cisco Unified Mobility との間の相互作用（21-116 ページ）を参照してください。

上記と同じ動作とロジックが、すべてのシェアド ライン呼び出し機能に当てはまります。この機能が有効である場合、デュアル モード モバイル クライアント デバイスが Unified CM に*登録されていない*場合に限り、コールはモビリティ ID または携帯電話番号に転送されます。すべてのシェアド ライン呼び出し機能の詳細については、Intelligent Session Control およびすべてのシェアド ライン呼び出し（21-75 ページ）を参照してください。

いずれの場合も、デュアル モード デバイスのモバイル ネットワーク電話番号に直接発信された着信コールは、プロバイダー ネットワークまたはデバイス設定がモバイル ネットワークによってデバイスに転送されないように設定されていないかぎり、常にモバイル ネットワークのデュアル モード デバイスのモバイル ボイス インターフェイスに直接ルーティングされます。このようなコールは、ユーザの会社の電話番号に対して発信されたコールではないため、適切な動作です。これらのコールは個人的なコールであると見なされるため、会社経由でルーティングされません。

（注） タブレット デバイスなどの携帯電話音声の無線のないモバイル クライアント デバイスは、デュアルモード デバイスではなく、モバイル ボイス ネットワーク インターフェイスでは到達できません。これらのデバイスは、Voice over IP によって会社の電話番号でのみ到達できます。

発信コール ルーティング

デュアルモード モバイル デバイスからの発信コールで使用されるインターフェイスは、ロケーション、およびその特定の時刻におけるデバイスの接続状況に応じて異なります。デュアルモード デバイスが企業に接続されず、Unified CM に登録されていない場合、コールは、通常どおりセルラー音声無線インターフェイスによってモバイル ボイス ネットワークにルーティングされます。ただし、企業に接続され、Unified CM に登録されている場合、モバイル デバイスはすべてのコールをエンタープライズ テレフォニー インフラストラクチャ経由で発信する必要があります。企業接続が使用できない場合、またはモバイル クライアントが登録されていない場合は、会社の番号からコールを発信することはできず、代わりにモバイル クライアント デバイスの携帯の番号を使用してモバイル ボイス ネットワーク経由でコールを発信する必要があります。または、Cisco Unified Mobility に装備されている 2 段階ダイヤリング機能を利用することもできます（モバイル ボイス アクセスとエンタープライズ機能アクセス（21-64 ページ）を参照）。

ダイヤル プラン

企業のダイヤル プランによって、モバイル クライアント デバイスが企業に接続され、Unified CM に登録されている場合のダイヤリング動作が決定されます。たとえば、企業のダイヤル プランの設定で、内部の内線番号に到達するために短縮ダイヤルの使用が許可されている場合、Unified CM に登録されているモバイル デバイスではこの短縮ダイヤルを利用できます。デュアルモードの携帯電話ユーザが発信コールにおいて社内で企業のダイヤリング手順、短縮ダイヤル、およびサイト ベースの番号または PSTN 振り分け用数字を使用してダイヤルできることは確かに便利ですが、携帯電話ユーザは、通常、携帯電話において、モバイル ボイス ネットワークで発信コールに対して要求される完全な E.164 ダイヤル ストリングを使用して発信コールの番号をダイヤルするため、これは若干不自然なダイヤリング方式となります。

企業におけるエンド ユーザ ダイヤリング エクスペリエンスは、最終的には企業のポリシーおよび企業のテレフォニー配置の管理者によって決定されます。ただし、デュアルモード モバイル デバイスでは、デバイスが企業ネットワークに接続されて Unified CM に登録されているかどうかにかかわらず、デュアルモード クライアント デバイスのダイヤリング手順が維持されるように、必要なダイヤル ストリングを正規化することを推奨します。モバイル ボイス ネットワークにおけるダイヤリングは、通常完全な +E.164（先頭に「+」が付きます）を使用して行われ、携帯電話の連絡先は通常完全な +E.164 番号で保存されるため、デュアルモード モバイル デバイスにおいては、企業のダイヤル プランは先頭に「+」を付けた完全な +E.164 番号を使用できるように設定することを推奨します。Unified CM 内で、デュアルモード電話のこのような発信ダイヤリングを処理するようにダイヤル プランが設定されている場合、ユーザは連絡先を +E.164 形式で 1 セットだけ電話機に保存するだけで済みます。これらの連絡先からダイヤルする場合や、完全な +E.164 番号を使用して手動でダイヤルする場合、デバイスが企業ネットワークに直接接続されているか、セキュア リモート接続を介して接続され Unified CM に登録されているか、またはモバイル ボイス ネットワークにだけ接続されているかにかかわらず、コールは常に適切な接続先にルーティングされます。このように企業のダイヤル プランを設定すると、ユーザのモバイル デバイスのダイヤリング手順が維持され、デバイスが企業に接続され Unified CM に登録されているかどうかを気にする必要がなくなるため、最善のエンド ユーザ ダイヤリング エクスペリエンスが提供されます。

デュアルモード電話から正規化されたダイヤリングを行うには、企業に接続されているか、またはモバイル ボイス ネットワークだけに接続されているかにかかわらず、次の点を考慮して Unified CM 内のダイヤル プランを設定します。

- 企業のダイヤル プランで、デュアルモード電話機からの、通常モバイル ボイス ネットワークで使用されるダイヤル ストリングを処理できるようにします。たとえば、ダイヤル プランでは、携帯電話からモバイル ボイス ネットワークを経由して特定の電話機に到達するためにダイヤルされる +1 408 555 1234 や 408 555 1234 などのストリングを処理できるように設定する必要があります。後者の 10 桁のダイヤル方式（たとえば、408 555 1234）をサポートすると、サイト内の短縮ダイヤルなどの他のダイヤリング手順と潜在的にオーバーラップする可能性があります。この場合、管理者は、どのオーバーラップしているダイヤリング手順（10 桁のダイヤルまたはサイト内の短縮ダイヤル）が企業ネットワークに登録されているデュアル モード電話機で使用できるようにする必要があるかを決定する必要があります。デュアル モード電話機でサポートされているダイヤリング手順のセットは、標準のエンドポイントでサポートされるダイヤリング手順のセットと異なることがよくあります。
- 会社の他の電話番号へのコールにおいては、短縮ダイヤルが設定されているシステムでは、ダイヤル ストリングを変更して、必要に応じて会社の内線番号に再ルーティングできる必要があります。たとえば、企業のダイヤル プランが 5 桁の内部ダイヤルに基づいているとすると、会社の内線番号へのコール ルーティングが処理されるようにシステムを設定して、デュアルモード デバイスが Unified CM に登録されているときにコールが発信された場合、+1 408 555 1234 や 408 555 1234 に発信されたコールが変更されて、51234 に再ルーティングされるようにする必要があります。
- 会社のデュアルモード デバイスへのすべての着信コールの発信番号または発信者 ID プレフィックスの先頭に適切な数字を付加して、不在コール、発信コール、および着信コールのコール履歴リストが完全な +E.164 形式となるようにします。これにより、デュアルモード デバイスのユーザは、ダイヤル ストリングを編集することなくコール履歴リストからダイヤルできます。ユーザは、企業に接続されているかどうかにかかわらず、コール履歴リストから番号を選択してリダイヤルできます。たとえば、社内の 51234 からデュアルモード ユーザの会社の電話番号にコールが発信され、そのコールに応答がない場合、発信番号を操作して、デュアルモード デバイスの履歴リストに 408 555 1234 または +1 408 555 1234 という形式のエントリが残るように Unified CM を設定する必要があります。この番号は、デュアル モード デバイスが、これ以上の処理の必要とすることなく、企業または単にモバイル ボイス ネットワークに接続されているかどうかダイヤルできます。

デュアルモード デバイスの正規化されたダイヤリングの例外の 1 つに、会社の内線番号または電話に内部からだけ到達可能なシナリオがあります(つまり、対応する外部から到達可能な DID 番号がない場合)。このような場合は、短縮形式を使用して、外部から到達できない番号をダイヤルできます(手動でダイヤルするか、または連絡先からダイヤルします)。これらの番号は外部では利用できず、社内からだけダイヤルできるため、連絡先リストにこれらの番号を保存する場合には、社内だけで使用できるという何らかのマークが必要となります。さらに、これらの内部専用番号からの着信コールの発信番号をコール履歴リストに保存する場合は、番号が変更されないようにする必要があります。これらの番号には、社内からだけ発信できるためです。すべてのコール履歴リストにおいて、これらの内線番号からのコールは番号を変更しないで保存する必要があります。このように変更しないで保存された番号、つまり短縮ダイヤル ストリングは、デバイスが企業に接続され Unified CM に登録されているときにだけ正常にダイヤルできます。

タブレットなどの携帯電話音声の無線がないモバイル クライアント デバイスは、企業接続および企業の音声とビデオ テレフォニーまたはクラウドベースのコラボレーション サービスだけに依存します。

緊急サービスおよびダイヤリングの考慮事項

モバイル クライアント デバイスから 911、999、112 などの緊急サービス番号に対してコールを発信する場合、事態は少々複雑になります。モバイル クライアント デバイスは社内または社外に位置する可能性があるため、緊急時におけるデバイスおよびユーザの位置の通知について考慮する必要があります。セルラー音声無線を備えたデュアルモード モバイル デバイスはプロバイダー ネットワークの位置サービスを利用しています。デバイスが接続され、通常は企業ワイヤレス ネットワークよりもはるかに正確に位置を特定できる場合は、これらの位置サービスは常に利用可能できます。そのため、デュアルモード デバイス ユーザは緊急コールを発信し、デバイスおよびユーザの位置を特定する場合には、モバイル ボイス ネットワークを利用することを推奨します。シスコのデュアルモード クライアント デバイスが緊急サービスおよび位置サービスにモバイル プロバイダーのボイス ネットワークのみを利用するよう、これらのクライアントは、モバイル クライアント デバイス設定ページの [緊急電話番号(Emergency Numbers)] フィールドに設定された番号に対するすべてのコールを強制的にモバイル ボイス ネットワーク経由でルーティングします。さらに、デュアルモード電話機のユーザに対して、すべての緊急コールを企業ネットワークではなくモバイル ボイス ネットワーク経由で発信するように指示します。

WLAN またはモバイル データ ネットワークを介した緊急コールを発信することは推奨されませんが、携帯電話音声の無線がないモバイル デバイスは、これらのデータ インターフェイスだけを経由して発信できます。携帯電話音声の無線がないモバイル デバイスは、緊急コール発信用に利用すべきではありません。

会社の発信者 ID

モバイル クライアント デバイスが企業に接続され、Unified CM に(モバイル データ ネットワークまたは WLAN 経由で)登録された場合、WLAN またはモバイル データ ネットワーク経由の企業回線で行われたすべてのコールは、発信者 ID としてユーザの会社の電話番号でルーティングされます。これにより、遠端でコール履歴リストから発信される返信コールはユーザの会社の電話番号に対して発信されることになり、常に会社経由でルーティングされます。デュアルモード モバイル デバイス ユーザに対して Cisco Unified Mobility が有効になっており、携帯電話の番号でシングル ナンバー リーチがオンになっている場合、デュアルモード デバイスが企業に接続されていないときには、会社の電話番号への返信コールも PSTN 経由でデュアルモード デバイスに転送されます。

通話切替機能

モバイル クライアント デバイスが企業に接続され、企業エンドポイントとして Unified CM に登録されている場合、Unified CM でサポートされている SIP コール シグナリング方式を使用して、保留、保留解除、転送、会議などの呼処理付加サービスを呼び出すことができます。Unified CM に登録された IP Phone やクライアントと同様に、これらのデバイスでは、保留音（MoH）、カンファレンス ブリッジ、メディア ターミネーション ポイント、トランスコーダなどの企業のメディア リソースを利用できます。

外部コール ルーティング

デュアル モード モバイル クライアント デバイスが企業に接続されている場合、または Unified CM に登録されていない場合は、モバイル ボイス ネットワーク経由だけでコールを発信および受信できます。このため、デュアルモード モバイル デバイスが登録されていない場合に発信または受信されるすべてのコールにおいて、Unified CM は関与しません。企業に接続されていないデュアルモード電話からコールが発信された場合、ネットワークに送信される発信者 ID は携帯の番号です。このため、応答されなかったコールへの返信コールは、会社経由でルーティングされるのではなく、デュアルモード デバイスの携帯の番号に直接発信されることになります。

デュアルモード モバイル クライアント デバイスが Cisco Unified Mobility と統合されている場合は、デュアルモード デバイスが社外にあり Unified CM に登録されていない場合でも、エンタープライズ 2 段階ダイヤリング サービスを利用して会社経由でコールを発信できます。Unified Mobility の 2 段階ダイヤリングは、モバイル ボイス アクセスまたはエンタープライズ機能アクセスを使用して実行され、ユーザはエンタープライズ システム アクセスの DID 番号をダイヤルし、クレデンシャルを入力してから発信番号をダイヤルする必要があります。Unified Mobility の 2 ステージ ダイヤリング機能の詳細については、モバイル ボイス アクセスとエンタープライズ機能アクセス（21-64 ページ）を参照してください。

同様に、デュアルモード電話機が Unified Mobility と統合されている場合、ユーザは、会社の電話番号への着信コールをシングル ナンバー リーチ経由で携帯の番号で受信したり、DTMF キー シーケンスを使用して保留、保留解除、転送、会議などの通話切替機能を呼び出したり、デスク フォンのピックアップを実行してアクティブなコールを携帯電話から会社のデスク フォンに移動したりできます。

リモート セキュア企業接続

モバイル クライアント デバイスは、Unified CM に対してクライアントを登録し、その他のコラボレーション アプリケーションやサービスにアクセスするために企業に安全な接続があるとすれば、企業に接続されていない場合でも IP コールや他のコラボレーション サービス経由でエンタープライズ音声およびビデオ用の IP テレフォニーのインフラストラクチャを利用できます。これらのデバイスに対するリモート セキュア接続は、インターネット経由のクライアント接続を保護するために Cisco AnyConnect モバイル クライアント VPN ソリューションまたは VPN なしの Cisco Expressway モバイルおよびリモート アクセス機能の使用が必要です。

リモート接続されたモバイル クライアント デバイスの音声およびビデオの品質とユーザ エクスペリエンスは、インターネット ベースのネットワーク接続の特性によって異なります。このようなクライアント接続タイプでは、シスコは音声とビデオの品質も正常接続も保証しません。このような接続を業務上重要な通信に使用する場合は、注意が必要です。信頼できない、または低帯域幅のインターネット接続を備えたデュアルモード デバイスの場合、デュアルモード デバイスのユーザは、接続が使用可能である場合、リモート企業テレフォニー インフラストラクチャに依存するのでなく、モバイル ボイス ネットワーク経由でコールを発信することが推奨されます。

追加のサービスおよび機能

呼処理サービスや呼制御サービスに加えて、シスコのモバイル クライアントとデバイスは、この項で説明する追加の機能およびサービスを提供できます。

デュアルモード コール ハンドオフ

デュアル モード デバイス配置の、1 つの非常に重要な側面は、ユーザが社内と社外の間を移動する、またはデバイスが企業ネットワークとの間で接続、切断するときに、ネットワーク接続が携帯電話音声の無線から WLAN 無線に切り替わり、また、その逆のことが起こるコール プリザベーションです。デュアルモード電話のユーザは多くの場合移動するため、デュアルモード ユーザが社内と社外の間を移動するときにアクティブなコールが維持されることが重要です。このため、デュアルモード クライアント デバイスおよび基礎となる企業のテレフォニー ネットワークでは、何らかの形式のコール ハンドオフが可能である必要があります。

デュアルモード クライアント、および基礎となる IP テレフォニー インフラストラクチャの両方でサポートされる必要がある 2 種類のコール ハンドオフがあります。

- ハンドアウト

  コール ハンドアウトとは、アクティブ コールをデュアルモード電話の WLAN またはモバイル データ ネットワーク インターフェイスからデュアルモード電話のセルラー音声インターフェイスに移動することを指します。このためには、コールが、会社の PSTN ゲートウェイ経由で、企業の IP ネットワークからモバイル ボイス ネットワークにハンドアウトされることが必要です。

- ハンドイン

  コール ハンドインとは、アクティブ コールをデュアルモード電話のセルラー音声インターフェイスからデュアルモード電話の WLAN またはモバイル データ ネットワーク インターフェイスに移動することを指します。このためには、コールが、会社の PSTN ゲートウェイ経由で、モバイル ボイス ネットワークから企業の IP ネットワークにハンドインされることが必要です。

デュアルモード電話機のハンドオフ動作は、デュアルモード クライアントの特性およびその特定の機能に依存しています。デュアル モード クライアントのハンドオフは、ユーザによって手動で呼び出したり、またはネットワーク条件に基づいて自動的に呼び出したりできます。手動ハンドオフのシナリオにおいては、デュアルモード ユーザは、各自のロケーションおよび必要性に基づいてハンドオフ動作を行い、完了する必要があります。自動ハンドオフにより、モバイル クライアントは WLAN 信号をモニタし、クライアントの WLAN 信号の強弱に基づいてハンドオフの決定を行います。弱い WLAN 信号の場合はハンドアウトが行われ、強い WLAN 信号の場合はハンドインが行われます。自動ハンドオフは、WLAN 信号の強度をモニタする機能を提供するモバイル デバイスに依存します。

ハンドオフ動作は、電話のコールにおいてエンタープライズ IP テレフォニー インフラストラクチャを最大限に活用するために重要となります。また、これらの動作は、音声の継続性と良好なユーザ エクスペリエンスを提供し、ユーザが元のコールをいったん切ってから再度コールを発信し直す必要がないようにするためにも必要です。

XMPP ベースの IM およびプレゼンス

一部のモバイル クライアントは、オンプレミスまたはオフプレミスのアプリケーション サーバまたはサービスとの統合によって、Extensible Messaging and Presence Protocol（XMPP）に基づいて企業インスタント メッセージング（IM）およびプレゼンス サービスを提供できます。いずれの場合も、これらのモバイル クライアントの IM およびプレゼンス機能は、次を有効化します。

- ユーザを連絡先リストまたはバディ リストに追加する。
- ユーザのプレゼンスおよび応答可能性のステータスを設定および伝達する。
- バディまたは連絡先のプレゼンス ステータスを受信する。
- インスタント メッセージング（IM）またはテキスト メッセージを作成し、送信する。
- IM またはテキスト メッセージを受信する。

IM and Presence はモバイル クライアントの必須機能ではありませんが、これによって、ユーザは自分のプレゼンス ステータスを連絡先に表示したり、連絡先のプレゼンス ステータスを表示したりできるため、生産性が向上します。また、ユーザは、モバイル ショート メッセージ サービス（SMS）メッセージのコストをかけずに、企業ベースの IM メッセージを送信できます。

社内ディレクトリ アクセス

モバイル クライアントとデバイスは、連絡先を検索するために企業ディレクトリにアクセスできます。次のいずれかを使用して、企業ディレクトリへのアクセスを有効にします。

- クライアントと互換性のある LDAP ディレクトリの間の通信用の Lightweight Directory Access Protocol（LDAP）
- クライアントと User Data Services（UDS）API 間の REST ベース（HTTPS）通信。この通信では、Unified CM クラスタのエンドユーザ データベース内に格納されるユーザの連絡先情報への認証済みアクセスを有効にする一連の操作が提供されます。

  連絡先の検索には、UDS-to-LDAP プロキシを使用することもできます。有効にしても、連絡先の検索は UDS によって処理されますが、モバイル クライアントに結果をリレーする UDS を使用して、社内 LDAP ディレクトリにプロキシされます。これにより、モバイル クライアントでは Unified CM 内でサポートされるユーザの数を上回る社内ディレクトリを検索することができます。

社内ディレクトリ アクセスはモバイル デバイスおよびクライアントに必須の機能ではありませんが、モバイル デバイスから社内ディレクトリ情報にアクセスできると、モバイル ユーザのユーザ エクスペリエンスが向上します。

企業ボイスメール サービス

多くのモバイル クライアントとデバイスも、企業ボイス メール サービスにアクセスできます。シスコのモバイル クライアントでは、ユーザの企業ボイスメール ボックスに未読のボイスメールが存在し、モバイル デバイスが企業ネットワークに接続されている場合に、企業のメッセージ待機インジケータを受信できます。さらに、モバイル クライアントを使用して、企業ボイスメール メッセージを取得することもできます。通常、企業ボイスメール メッセージは、ユーザがボイスメール システム番号にダイヤルし、必要なクレデンシャルを入力してから各自のボイスメール ボックスに移動して取得します。ただし、Cisco Jabber モバイル クライアントは、ボイスメール ボックス内のすべてのメッセージのリストをダウンロードおよび表示し、モバイル デバイスにダウンロードして再生する個別のメッセージを選択することによって、ボイスメール ボックスからボイスメール メッセージを取得する機能を備えています。この機能は、ビジュアル ボイスメールと呼ばれることもあります。モバイル クライアントおよび企業ボイスメール システムの両方において、ネットワーク経由でのメッセージ待機インジケータ（MWI）、ボイスメール メッセージ情報、およびメッセージのダウンロードの提供と受信が可能である必要があります。Cisco Unity Connection は、REST（HTTPS）を使用したビジュアル ボイスメールをサポートし、MWI、ボイス メール リスト、およびメッセージのダウンロードを提供します。

Dial Via Office

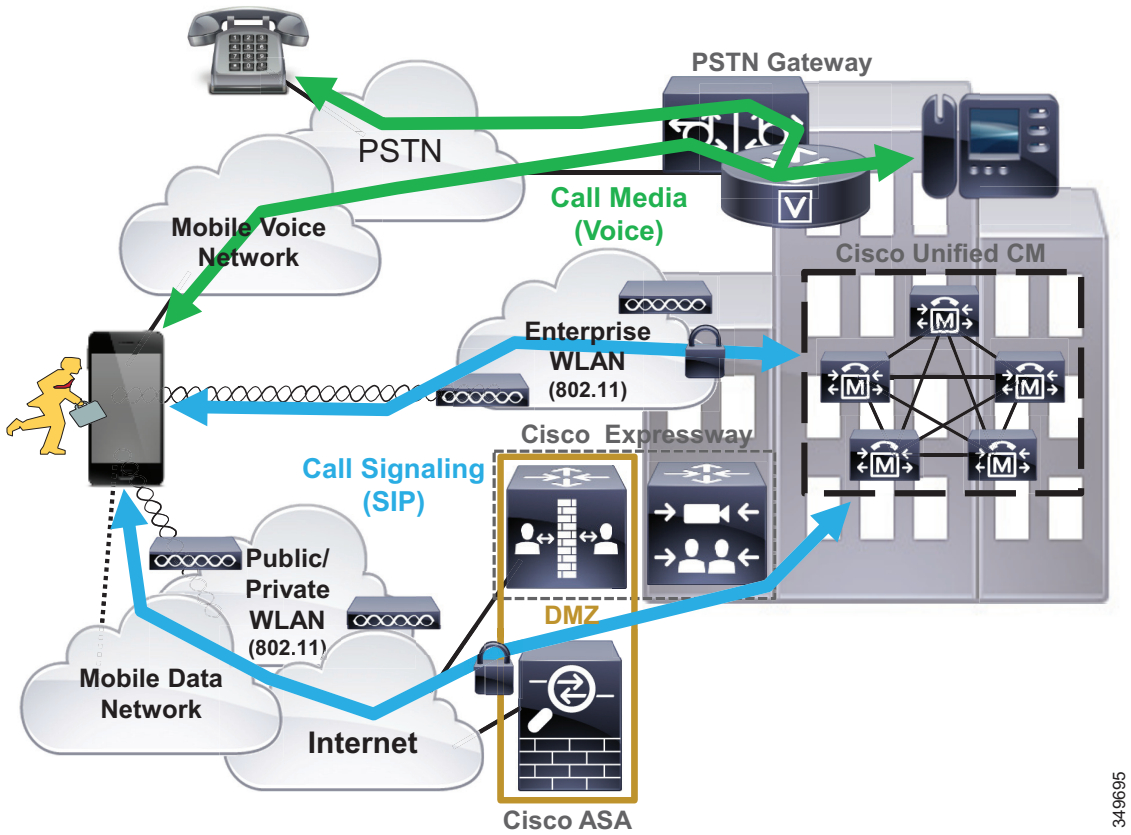
Dial Via Office（DVO）機能によって企業のダイヤリング機能が自動化され、デュアル モードのモバイル デバイスが企業テレフォニー インフラストラクチャ経由でコールを開始できるようになりました。DVO 通話を導入すると、企業に次の利点がもたらされます。

- 直接ダイヤルされた携帯電話コールと比較して、国際電話（おそらくは）長距離電話のコストを削減します。モバイル データ通過の場合は、モバイル データのコストも考慮する必要があることに注意してください。
- 社内番号に電話をかけることができます。DVO コールは会社の内線番号を使用して発信されるため、DID 以外または内部専用の会社の内線番号にも到達できます。

- 携帯電話番号のマスキング。DVO コールでは、システムは携帯電話番号ではなくユーザの社内番号を発信者 ID として送信します。
- 一元化された会社のコール詳細レコード（CDR）とコール ログ。DVO コールは企業テレフォニー インフラストラクチャから発信されるため、コールが PSTN およびモバイル ボイス ネットワークを通過する場合も、管理者はこれらのコールを完全に認識しています。
- 社内コール アンカリング。DVO コールは社内でアンカーされるため、ユーザは Cisco Unified Mobility DTMF ベースの通話切替機能、およびデスクトップフォンのピック アップを利用することができます。

Cisco Jabber クライアントを実行するデュアル モードのモバイル デバイスは、会社の内線番号を使用して電話をかける Unified CM テレフォニー インフラストラクチャと会社の PSTN ゲートウェイを使用して DVO コールを発信することができます。ただし、音声メディアが IP ネットワークを通過する Voice over IP（VoIP）とは異なり、この機能は、図 21-28 に示すように、クライアントと IP 接続（WLAN またはモバイル データ）経由の Unified CM 間の SIP シグナリングと、モバイル デバイス、モバイル ボイス ネットワーク、PSTN 間の音声メディアによって実現されます。

図 21-28　Cisco Dial Via Office のアーキテクチャ



（注）　DVO コールの場合、ユーザの携帯電話からのすべての音声またはメディアは、モバイル ボイス ネットワーク、PSTN、および会社の PSTN ゲートウェイを経由して常に移動します。メディアが会社へのデータ接続を通過することはありません。モバイル データ ネットワーク接続は、コール シグナリング トラフィックとその他のアプリケーションの相互作用以外には使用されません。

Cisco Jabber クライアント向け Dial via Office の詳細については、デュアルモード デバイス向けの Cisco Jabber Dial Via Office（21-104 ページ）を参照してください。

モバイル クライアント ユーザ用の設定の簡素化

シスコのモバイル クライアントは、モバイル クライアント デバイスで初回エンドユーザ クライアントの設定を単純化するための簡素化された設定方式を提供します。この設定方式は、社内 DNS サーバ内の RFC 2782 標準 Domain Name Service（DNS SRV レコード）に依存し、自動的にネットワークのコラボレーション サービスを検出します。DNS SRV レコードは、呼制御や IM およびプレゼンス サービス用の適切なアプリケーション サーバにモバイル クライアントを転送します。この設定とプロビジョニング方式は、ユーザが XMPP IM およびプレゼンス サーバや音声とビデオ呼制御サーバまたは TFTP サーバ ホスト名または IP アドレスを手動で設定する必要性を緩和します。代わりにユーザは単にユーザ ID とドメイン名を入力し、クライアント アプリケーションは自動的に利用可能なコラボレーション サービスを検出し、適切なクレデンシャルをユーザに要求するアプリケーションを使用してこれらのバック エンド サーバに接続します。サービスが検出されない場合、またはサービスの検出操作が失敗した場合、モバイル クライアント アプリケーションは、コラボレーション アプリケーション サーバのホスト名または IP アドレスおよびクレデンシャルを要求する手動の設定モードに戻ります。プライオリティおよび重み付けが表示された複数の DNS SRV レコードは、これらのサービスを提供する複数のサーバにバック エンドのコラボレーション アプリケーション サービスとモバイル クライアント分散のハイ アベイラビリティを確保します。

（注）　モバイル クライアント ユーザの簡素化された設定は、バック エンド アプリケーション サーバのクライアントとサービス設定とプロビジョニング関連する管理タスクを簡素化しません。社内 DNS サーバに DNS SRV レコードを作成することに加え、ユーザ アカウント、モバイル クライアント デバイス、およびサービス設定を追加するすべての管理作業が必要になります。

Cisco Bring Your Own Device（BYOD）インフラストラクチャ

Cisco Jabber などのシスコのモバイル クライアント アプリケーションは、Android や Apple iOS のスマートフォンやタブレットなどのモバイル デバイスのユーザへの、音声、ビデオ、およびインスタント メッセージングを含むコアの Unified Communications およびコラボレーション機能を提供します。シスコのモバイル クライアント デバイスが企業ワイヤレス LAN に接続されている場合、クライアントは Cisco Bring Your Own Device（BYOD）インフラストラクチャ内に配置できます。

シスコのモバイル クライアントとデバイスは、企業ワイヤレス LAN 接続、または VPN 経由のリモート セキュア接続または VPN なしの接続に依存しているため、Cisco Unified アクセス ネットワーク内に配置し、BYOD インフラストラクチャで配信される ID、セキュリティ、およびポリシー機能を利用することができます。

Cisco BYOD インフラストラクチャは、さまざまなデバイスの所有権とアクセス要件に対応するために、種々のアクセス使用例またはシナリオが用意されています。次のハイ レベルなアクセス使用例モデルを考慮する必要があります。

- 基本的なアクセス：この使用例は、ゲストのデバイスの基本的なインターネット アクセスだけを有効にします。この使用例では、企業リソースへのアクセスを提供せずに、従業員所有の個人用デバイスのネットワーク接続を可能にする機能を提供します。
- 制限付きアクセス：この使用例は、社内ネットワーク リソースへのフル アクセスを有効にしますが、企業所有デバイスだけに適用されます。
- 拡張アクセス：この使用例は、社内ポリシーに基づいて、企業所有デバイスと従業員所有の個人用デバイスの両方が社内ネットワーク リソースに対して高精度なアクセスを実現します。

シスコのコラボレーション モバイル クライアントは、企業のデバイスまたは個人のデバイスのいずれで動作しているかにかかわらず、通常は多数のバック エンドのオンプレミスの企業アプリケーション コンポーネントへのフル機能でのアクセスが必要です。このため、制限付きアクセスまたは拡張アクセスの使用例のシナリオは一般に、Cisco Jabber for Android or iPhone などのアプリケーションに適用されます。この 2 つのアクセス モデルの主な違いは、制限付きアクセスでは、企業所有デバイスに社内ネットワーク リソースへのフル アクセスが与えられている点です。拡張アクセスの場合は、従業員所有のデバイスにもフル アクセスが与えられるだけでなく、社内ネットワーク リソースへのアクセスが高精度で行われるため、このアクセス状態で実行されるデバイスとアプリ ケーションは、企業のセキュリティ ポリシーに基づいて特定のリソースだけにアクセスすることができます。

クラウドベースのコラボレーション サービスの場合は、シスコのモバイル クライアントおよびデバイスは、企業ネットワーク接続は不要で、インターネットを介してクラウドに直接接続します。これらの使用例がインターネット アクセスだけを必要とするため、これらのシナリオでは、ユーザおよびモバイル デバイスは、基本的なアクセス モデルを使用して配置できます。

Cisco BYOD インフラストラクチャの詳細と BYOD アクセスの使用例については、以下のリンク先に掲載されている BYOD 情報を参照してください。

https://www.cisco.com/c/en/us/solutions/byod-smart-solution/overview.html

Cisco BYOD インフラストラクチャ内にシスコのモバイル クライアントおよびデバイスを配置する場合は、次のハイレベルな設計と配置のガイドラインを考慮してください。

- ネットワーク管理者は、企業のテレフォニー インフラストラクチャの最大使用を保証するために、音声およびビデオ対応クライアントがバックグラウンドで企業ネットワークに（初期のプロビジョニングの後）、ユーザの介入なしで接続することを許可することを検討する必要があります。具体的には、証明書ベースの ID および認証を使用すると、ネットワーク接続および認証の遅延を最小化することによって優れたユーザ エクスペリエンスを容易にします。
- シスコのモバイル クライアントとデバイスがセキュア VPN または VPN なしの接続を介して企業ネットワークにリモート接続できるシナリオの場合：
  - ネットワーク管理者は、企業テレフォニー インフラストラクチャを最大限に活用するために、企業のセキュリティ ポリシーをユーザの介入のないシームレス セキュア接続の必要性に対して評価する必要があります。証明書ベースの認証を利用し、デバイスのピン ロック ポリシーを適用すると、エンド ユーザがデバイスを所有し、ネットワークにアクセスするためのピン ロックを知っている必要があるため、ユーザの介入および二要素認証のような機能なしでシームレスに接続することができます。二要素認証が必要な場合、デバイスを企業にリモート接続するには、ユーザの介入が必要となります。
  - インフラストラクチャのファイアウォール設定によって、必要なすべてのクライアント アプリケーションのネットワーク トラフィックが企業ネットワークにアクセスできることが重要です。適切なアクセス ソリューションを提供すること、または企業のファイアウォールで適切なポートやプロトコルへのアクセスを開くことに失敗すると、シスコのモバイル クライアントやデバイスを音声およびビデオ テレフォニー サービス用のオンプレミスの Cisco Call Control に登録できなくなったり、企業ディレクトリ アクセスや企業ビジュアル ボイスメールなどの他のクライアント機能を失ったりする可能性があります。

- Cisco Jabber などの企業のコラボレーション アプリケーションが従業員所有のモバイル デバイスにインストールされている場合は、特定の状況下においてデバイスをワイプするか、工場出荷時の設定にリセットすることが企業のセキュリティ ポリシーで定められている場合、デバイスの所有者にそのポリシーについて知らせ、デバイスから個人データを定期的にバックアップすることを奨励する必要があります。
- シスコのコラボレーション モバイル クライアントおよびデバイスを導入する場合、クライアント アプリケーションの音声とビデオ コールの品質、およびすべての機能の適切な動作を保証するために、エンドツーエンドの基盤となるネットワーク インフラストラクチャが、音声メディアと専用ビデオのプライオリティ キューイングやシグナリング帯域幅など必要な QoS クラスのサービスをサポートすることが重要です。

シスコのモバイル クライアントおよびデバイスの設計上の考慮事項

ここでは、次のシスコ モバイル クライアントおよびデバイスの設計上の考慮事項について説明します。

- Cisco Jabber for Android および Apple iOS（21-97 ページ）
- Cisco Spark（21-117 ページ）
- Cisco WebEx Meetings（21-118 ページ）
- Cisco AnyConnect モバイル クライアント（21-118 ページ）

Cisco Jabber for Android および Apple iOS

ここでは、Cisco Jabber の特性および配置上の考慮事項について説明します。

Cisco Jabber モバイル クライアントは、Android および iPad や iPhone などの Apple iOS に使用できます。適切なストアやマーケット（Apple の App Store や Google Play）からクライアント アプリケーションをダウンロードし、Apple iOS または Android デバイスにインストールすると、企業ネットワークに接続して SIP 対応の会社の電話機として Unified CM に登録できます。

Cisco Jabber モバイル クライアントに登録および呼制御サービスを提供するには、Unified CM 内でデバイスが **Cisco Dual Mode for Android** または **iPhone**、あるいは **Cisco Jabber for Tablet** デバイス タイプとして設定される必要があります。次に、企業の WLAN にアクセスして企業の WLAN インフラストラクチャおよびセキュリティ ポリシーに基づいて接続するよう、モバイル デバイスを設定する必要があります。または、モバイル データ ネットワークや非企業 WLAN 経由でモバイル デバイスを企業ネットワークに接続できます。企業ネットワークにアクセスするようにモバイル デバイスを設定すると、Cisco Jabber クライアントが起動したときに、デバイスが Unified CM に登録されます。Unified Mobility と統合し、ハンドオフ機能を利用するには、Android または iPhone スマートフォンの携帯番号を、Unified CM 内で Cisco Dual-Mode for Android または iPhone デバイスに関連付けられたモビリティ ID として設定する必要があります。

Cisco Jabber クライアントは、次のデバイスでサポートされます。

- Android

  Android フォンおよびタブレットのさまざまなモデル。（特定のデバイスおよびファームウェアのサポート情報については、次に参照されているリリース ノートを参照してください。）これらのデバイスで実行するファームウェア バージョンの最小要件は 4.1(2) となっていますが、最新バージョンの Android ファームウェアが必要になる場合もあります。ほとんどの Android デバイスの WLAN インターフェイスで、802.11a、802.11b、802.11g、802.11n および 802.11ac ネットワーク接続がサポートされています。

- Apple iOS

  iPhone、iPad などのさまざまな Apple iOS デバイス。(特定のデバイスおよびファームウェアのサポート情報については、次に参照されているリリース ノートを参照してください。)これらのデバイスでは、iOS バージョン 10.3 以降が実行されている必要があります。ほとんどの Apple iOS デバイスの WLAN インターフェイスでは、802.11a、802.11b、802.11g、および 802.11n ネットワーク接続がサポートされています。新しい一部の Apple デバイスでは、802.11ac がサポートされています。

最新の特定のデバイスおよびファームウェア バージョンの詳細については、次の製品リリース ノートを参照してください。

- Android

  https://www.cisco.com/c/en/us/support/unified-communications/jabber-android/products-release-notes-list.html

- iPhone および iPad

  https://www.cisco.com/c/en/us/support/customer-collaboration/jabber-iphone-ipad/products-release-notes-list.html

Cisco Jabber for Android、iPad、および iPhone クライアントは、音声および Voice-over-IP フォン サービスだけでなく、XMPP ベースの企業インスタント メッセージング(IM)およびプレセンスを提供し、さらに企業のコンタクト ソースにアクセスするよう設定された場合は企業の連絡先およびディレクトリ サービス、Cisco Unity Connection に統合された場合は企業ボイスメール メッセージ待機インジケータ(MWI)およびビジュアル ボイスメールも提供します。

スマートフォン(Android および iPhone)上の Cisco Jabber クライアントでは、Cisco Jabber デュアルモード ハンドオフ(21-101 ページ)の項に説明されているように、手動によるハンドアウトだけを実行できます。

Cisco Jabber Android および Apple iOS クライアント、追加の機能、およびサポートされているハードウェアとソフトウェアのバージョンの詳細については、次の Cisco Jabber マニュアルを参照してください。

- Android

  https://www.cisco.com/c/en/us/support/unified-communications/jabber-android/tsd-products-support-series-home.html

- iPhone および iPad

  https://www.cisco.com/c/en/us/support/customer-collaboration/jabber-iphone-ipad/tsd-products-support-series-home.html

Cisco Jabber サービス ディスカバリ

前述のように、Jabber などのシスコ モバイル クライアントは、DNS ルックアップや DNS SRV DNS サービス レコード解決に基づいて、使用可能なコラボレーション サービスを検出できます。サービス ディスカバリが適切に設定されている場合、ユーザがユーザ名とドメインだけを入力すると、使用可能なコラボレーション サービスをクライアントが自動的に検出して接続します。

図 21-29 に示されているように、クライアントの初期設定時、またはネットワーク接続の変更時に、Jabber は次の SRV レコードに関して DNS に照会することにより、コラボレーション サービスを検出します。

- _cisco_uds._tcp.<*domain*>

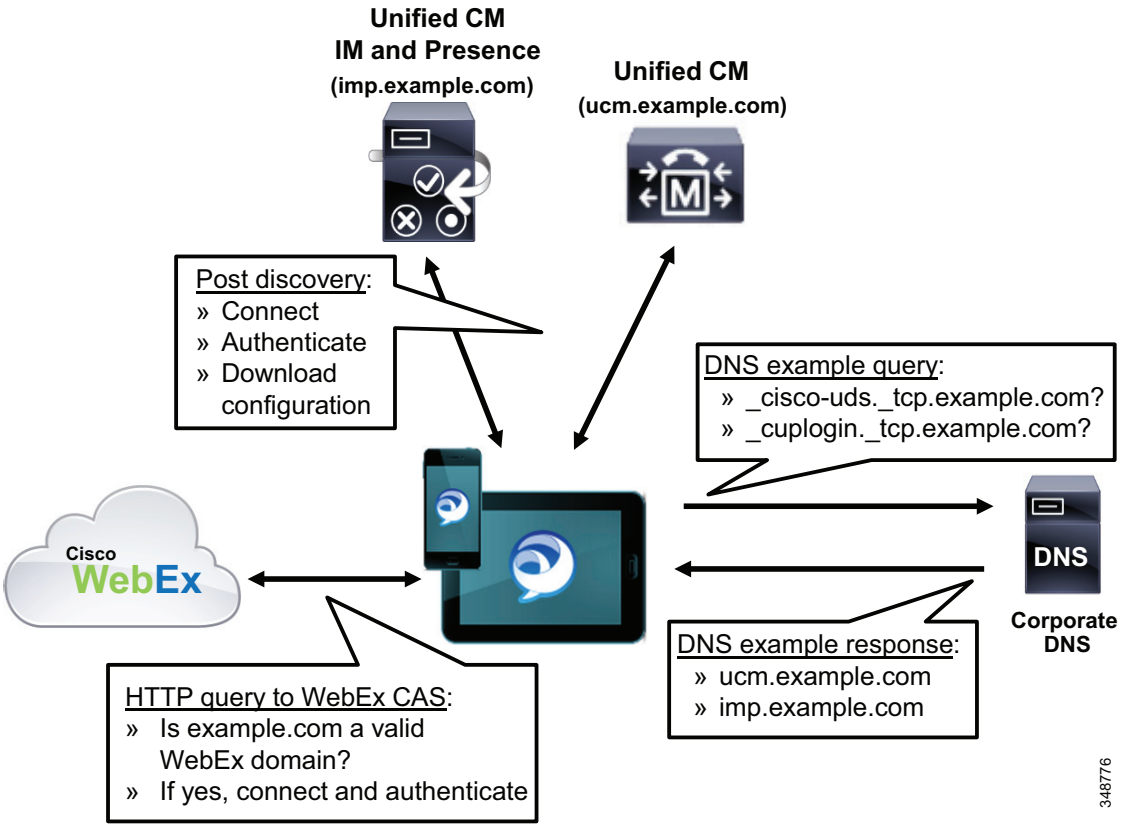
  Voice and Video over IP（VVoIP）通話を有効にする電話専用モード、または音声とビデオ通話および IM とプレゼンスを有効にするフル UC モードで Jabber が配置されると、このタイプの SRV レコードが企業 DNS サーバに追加されます。このレコードのクエリが DNS によって解決されると、Cisco Jabber は Unified CM に接続し、オーセンティケータを決定し、利用可能なサービスを特定します。

- _cuplogin._tcp.<*domain*>

  XMPP ベースの IM とプレゼンスを有効にする IM 専用モードで Jabber が配置されると、このタイプの SRV レコードが企業 DNS サーバに追加されます。このレコードのクエリが DNS によって解決されると、Cisco Jabber は Unified CM IM and Presence に接続し、認証します。

Cisco WebEx Messenger を使用したハイブリッド展開の場合、初期設定時およびネットワーク接続の変更時に、ドメインが有効な WebEx ドメインであるかどうかを判別するために、クライアントは Cisco WebEx Messenger サービスに関して Central Authentication Service（CAS）URL に向けて HTTP クエリも発行します。有効な WebEx ドメインが入力された HTTP クエリに対する肯定の確認をクライアントが受け取ると、クライアントは WebEx Messenger サービスに接続して認証し、Cisco WebEx Org Admin で設定された使用可能な UC サービスとクライアント設定に関する情報を取得します。

図 21-29　　Cisco Jabber サービス ディスカバリ



UDS サービスは Unified CM クラスタのすべてのノードで動作しますが、Unified CM UDS サービスの DNS SRV レコードを設定するとき、管理者は Unified CM サブスクライバ ノードにのみ解決するようレコードを設定する必要があります。これにより、UDS サービスとのクライアント対話でパブリッシャ ノードが回避され、代わりにクラスタ内の呼処理ノードに負荷が分散されます。

サービス ディスカバリが設定されていない展開、または DNS を信頼できない展開では、Jabber クライアントは手動設定に戻ります。その場合、ユーザはオーセンティケータとサービス ノードの IP アドレスを入力する必要があります。手動で設定された IP アドレスは、後続の接続で使用するために Jabber クライアントによってキャッシュされます。

サービス ディスカバリまたは手動設定が完了すると、Jabber は認証を行い、サービス プロファイルや jabber-config.xml ファイル（入手可能な場合）をダウンロードする必要があります。このファイルは、ボイスメールやディレクトリなどの追加のバックエンド アプリケーション サービスにクライアントを誘導し、適切な設定を有効にします。

Cisco Jabber 社内ディレクトリ アクセス

Cisco Jabber モバイル クライアントは、企業の連絡先情報にアクセスするためにさまざまな方法に依存します。ローカル デバイスの連絡先や、以前に Jabber バディ リストに追加された連絡先に加えて、Jabber モバイル クライアントは次の方法を使用して、社内ディレクトリ サービスにアクセスできます。

- Cisco ディレクトリ統合（CDI）

  CDI 方式の社内ディレクトリ アクセスは、Jabber クライアントとサポート対象の LDAP 対応ディレクトリ（Microsoft Active Directory、OpenLDAP など）の間の LDAP 通信に依存します。オンプレミス Jabber クライアントでは、CDI がディレクトリ統合のデフォルト方式となっています。

- Unified CM ユーザ データ サービス（UDS）

  社内ディレクトリ アクセスの UDS 方式は、Unified CM の各ノードで実行される Unified CM UDS サービスと Jabber クライアントとの間の HTTP 通信に依存します。

- Unified CM UDS-to-LDAP プロキシ

  社内ディレクトリ アクセスのこの方式は、ローカル ユーザ ディレクトリを使用する代わりに、社内 LDAP ディレクトリに対してディレクトリ検索を解決またはプロキシする Unified CM UDS サービスに依存します。UDS-to-LDAP プロキシにより、Jabber ユーザはローカル Unified CM クラスタ エンドユーザ データベースに制限されることなく、社内ディレクトリ全体に対して検索を実行できます。

Jabber クライアントのディレクトリ統合方法を設定するため、また Jabber クライアントのいくつかのディレクトリ関連設定を行うために、jabber-config.xml ファイルが使用されます。

オンプレミス クライアントには、CDI 方式のディレクトリ アクセスを使用することをお勧めします。

Expressway モバイルとリモート接続を使用してリモートで Jabber クライアントを接続する場合は、UDS 方式のディレクトリ アクセス（ローカル Unified CM データベースまたは UDS-to-LDAP プロキシ）のみがサポートされます。社内ディレクトリのサイズがローカル Unified CM ディレクトリのサイズを超過する場合（ユーザ数が 160,000 を超える場合）、モバイル クライアント ユーザがディレクトリ全体を検索できるよう、UDS-to-LDAP プロキシを有効にすることを検討してください。

Cisco Jabber デュアルモード ハンドオフ

Cisco Jabber などの Cisco デュアルモード クライアントを適切に配置するには、クライアント内部のハンドオフ動作の特性について理解することが重要です。Cisco Jabber デュアルモード クライアントによって使用されるハンドオフ方式は、Cisco Dual-Mode for iPhone または Cisco Dual-Mode for Android デバイスの設定ページの [モバイル ネットワークへ転送（Transfer to Mobile Network）] 設定に基づきます。

[Transfer to Mobile Network] の設定に応じて、ハンドオフには次の 2 つの方式があります。

- ハンドオフのモバイル ソフトキー方式（21-101 ページ）

  この方式では、[Transfer to Mobile Network] の設定を [Use Mobility Softkey (user receives call)] に設定する必要があります。このタイプのハンドオフでは、Unified CM システムは、PSTN を介してユーザのモバイル番号へのコールを発信します。

- ハンドオフ番号方式のハンドオフ（21-102 ページ）

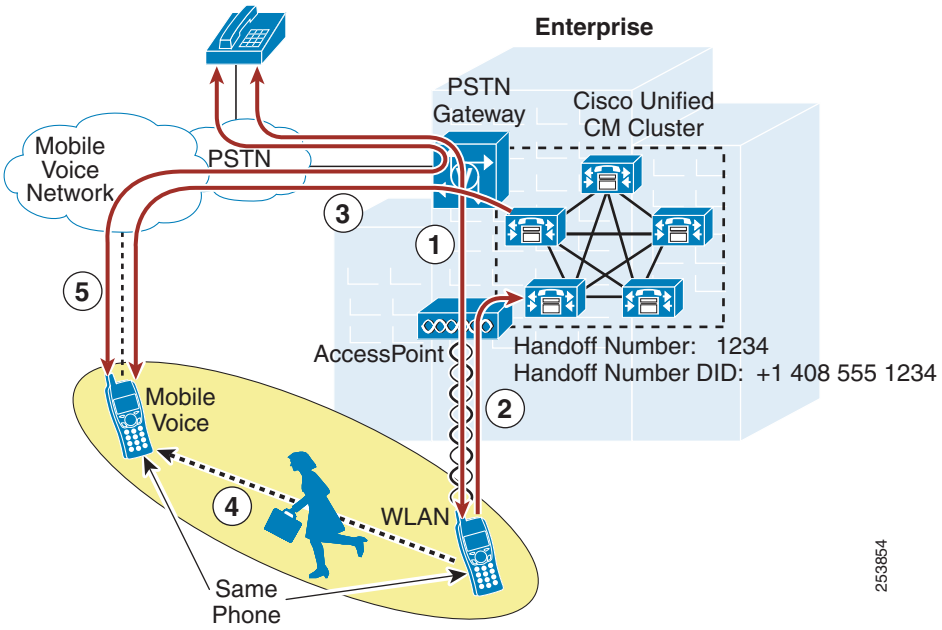
  この方式では、[モバイル ネットワークへ転送（Transfer to Mobile Network）] の設定を [HandoffDN 機能の使用（ユーザが発信）（Use HandoffDN Feature (user places call)）] に設定する必要があります。このタイプのハンドオフでは、モバイル クライアントが、モバイル ボイス ネットワークを介して、Unified CM システム内で設定されているハンドオフ番号に対してコールを発信します。

（注）　ハンドオフ機能は、デュアルモード スマートフォンにのみ適用されます。この機能は、Samsung Galaxy Note Pro など、セルラー音声無線を使用しないデバイスではサポートされません。

ハンドオフのモバイル ソフトキー方式

図 21-30 に示す動作は、社内の iPhone または Android デュアルモード デバイスにおけるアクティブなコールが、手動で WLAN インターフェイスから会社の PSTN ゲートウェイ経由でモバイル ボイス ネットワーク（デバイスの携帯電話インターフェイス）に移動される様子を示しています。図に示すように、企業の WLAN に関連付けられ、Unified CM に登録されたモバイル クライアント デバイスと、PSTN ネットワーク上の電話機との間に既存のコールがあります（ステップ 1）。これは手動のプロセスであるため、ユーザが Cisco Jabber クライアント内のコール中メニューから [モバイル ネットワークの使用（Use Mobile Network）] ボタンを選択して、コールをハンドアウトする意図があることを Unified CM に通知する必要があります（ステップ 2）。次に、Unified CM から、このモバイル デバイスに対応する設定済みのモビリティ ID 番号に対して、会社の PSTN ゲートウェイを経由してコールが発信されます（ステップ 3）。このモビリティ ID へのコールは、モバイル ボイス ネットワーク（iPhone または Android デバイスの携帯電話インターフェイス）に対して発信されます。これで、ユーザは、社外に移動して、WLAN ネットワークのカバー領域から離れることができます（ステップ 4）。一方、Unified CM からの着信コールがモバイル ボイス ネットワーク インターフェイスで受信され、ユーザは手動でこのコールに応答し、ハンドアウトを完了する必要があります。携帯電話インターフェイスで着信コールが応答されると、WLAN を通過していた RTP ストリームが PSTN ゲートウェイにリダイレクトされ、モバイル クライアント デバイスと元の PSTN 電話機との間のコールは会社のゲートウェイでアンカーされて、中断されずに継続します（ステップ 5）。

図 21-30　Cisco Jabber デュアルモード ハンドアウト（WLAN からモバイル ボイス ネットワークへ）：モバイル ソフトキー方式

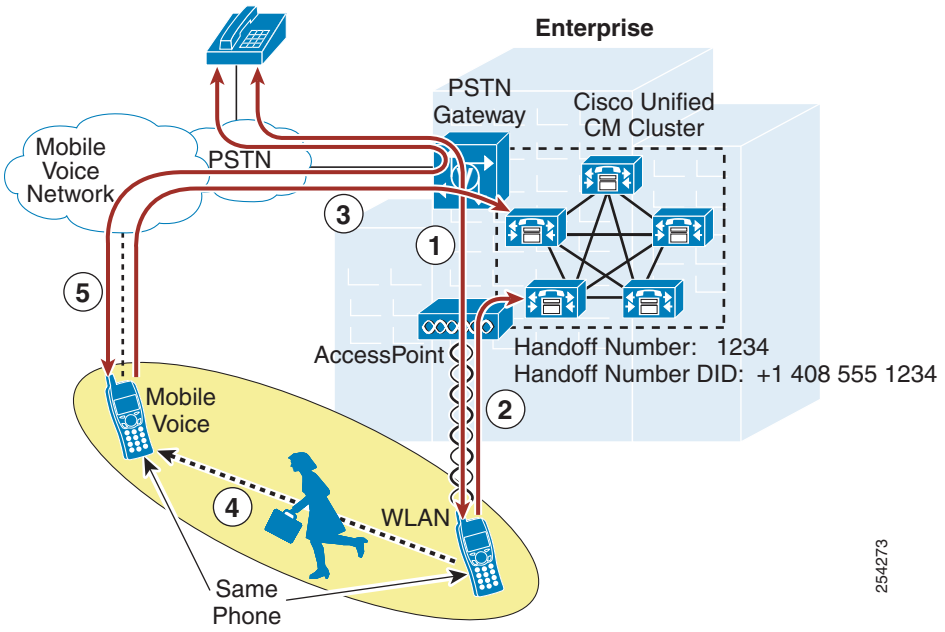


ハンドオフ番号方式のハンドオフ

図 21-31 に、社内の iPhone デュアルモード電話機におけるアクティブなコールが、手動で WLAN インターフェイスから会社の PSTN ゲートウェイ経由でモバイル ボイス ネットワークまたは携帯電話インターフェイスに移動される図 21-30 と同じハンドオフ動作を示します。ただし、このケースでは、ハンドオフ番号方式のハンドアウトが使用されます。

図 21-31 に示すように、企業の WLAN に関連付けられ、Unified CM に登録されたデュアルモード デバイスと、PSTN ネットワーク上の電話機との間に既存のコールがあります（ステップ 1）。これは手動のプロセスであるため、ユーザが Cisco Jabber デュアルモード クライアント内のコール中メニューから [モバイル ネットワークの使用（Use Mobile Network）] ボタンを選択して、コールをハンドアウトすることを Unified CM に通知する必要があります（ステップ 2）。次に、Cisco Jabber クライアントが、Unified CM システム内で設定されているハンドオフ番号に向けて、モバイル ボイス ネットワークを介して携帯電話インターフェイスからコールを自動発信します（ステップ 3）。これで、ユーザは、社外に移動して、WLAN ネットワークのカバー領域から離れることができます（ステップ 4）。その間に、Cisco Jabber クライアントからの着信コールが Unified CM によって受信されます。着信したコールの発信番号がユーザに設定されているモビリティ ID と一致したと仮定すると、WLAN を通過した RTP ストリームが PSTN ゲートウェイにリダイレクトされ、Cisco Jabber モバイル クライアントと元の PSTN 電話との間のコールは、会社のゲートウェイでアンカーされて、中断されることなく継続します（ステップ 5）。

図 21-31　Cisco Jabber デュアルモード ハンドアウト：ハンドオフ番号方式



（注） ハンドオフ番号方式のハンドアウトでは、Unified CM が、着信したコールの発信番号として、ハンドオフを試みている Cisco Dual Mode デバイスの下で設定されているモビリティ ID 番号と一致する番号を PSTN ネットワークから受け取る必要があります。発信者 ID がデュアルモード デバイスから送信されない場合、PSTN プロバイダーが着信したコールの発信者 ID を会社に送信しなかったり、着信したコールの発信者 ID が設定されているモビリティ ID と一致しなかった場合は、ハンドアウト動作は失敗します。

（注） Cisco Jabber デュアルモード クライアントはハンドインをサポートしません。デュアルモード モバイル ボイス ネットワーク（セルラー インターフェイス）と会社の電話（または会社のゲートウェイでコールがアンカーされた PSTN 電話機）との間で通話中のコールがアクティブである場合、コールをデュアルモード デバイスの WLAN インターフェイスに移動するには、コールをいったん切断し、デュアルモード クライアントが企業ネットワークに接続されて Unified CM に登録されてからリダイヤルするのが唯一の方法です。

Cisco Jabber モバイル クライアントの WLAN 設計上の考慮事項

Cisco Jabber モバイル クライアントを配置する際には、次の WLAN ガイドラインを考慮してください。

- 可能な場合は、デバイスの WLAN インターフェイス上で同じ IP アドレスを使用できるように、Cisco Jabber モバイル クライアントが必ず WLAN のレイヤ 2 でだけローミングするようにしてください。デバイスの IP アドレス変更のために、サブネットの境界を越えるレイヤ 3 ローミングのシナリオでは、コールがドロップされます。
- 同じ SSID が AP 全体で使用される WLAN ネットワークに Cisco Jabber モバイル クライアントを配置します。SSID が異なると、AP 間のローミングがはるかに低速になります。

- WLAN 上のすべての AP が、その SSID をブロードキャストするようにしてください。SSID が AP によってブロードキャストされないと、他の Wi-Fi ネットワークに参加するようユーザがデバイスから要求される場合や、デバイスが自動的に他の Wi-Fi ネットワークに参加する場合があります。この場合、コールは中断されます。
- 可能な場合は、5 GHz 帯域 WLAN（802.11a/n/ac）に Cisco Jabber モバイル クライアントを配置します。5 GHz WLAN は、音声コールとビデオ コールに関してスループットを改善し、干渉を低減します。

デュアルモード デバイス向けの Cisco Jabber Dial Via Office

Unified CM の管理者は、Cisco Dual Mode for iPhone または Android デバイス設定ページの [製品固有の設定レイアウト（Product Specific Configuration Layout）] セクションを使用して各デュアルモード デバイスに対する Dial Via Office（DVO）コールを有効または無効にできます。DVO が有効な場合、ユーザは Cisco Jabber アプリケーション内の [コール オプション（Calling Option）] 設定を使用して DVO をオンにできます。DVO のコール オプションは、Jabber クライアントによって使用される発信コール方式だけでなく、着信コール方式も定めることに注目してください。表 21-4 は、ネットワーク接続の種類に基づくさまざまなコール オプションと、対応する発信コール方式と着信コール方式を示しています。

表 21-4　Cisco Jabber Dial Via Office コール オプションを使用した着信コール方式と発信コール方式

デバイス IP 接続	Cisco Jabber DVO コール オプション					
	自動選択		モバイル ボイス ネットワーク		Voice over IP	
	発信コール	着信コール	発信コール	着信コール	発信コール	着信コール
802.11 WLAN（社内/企業）	Voice over IP	Voice over IP	Dial via Office	シングル ナンバー リーチ（Single Number Reach）	Voice over IP	Voice over IP
802.11 WLAN（非社内/企業）						
モバイル データ	Dial via Office	シングル ナンバー リーチ（Single Number Reach）				
IP なし	発信コール：ネイティブ携帯電話 着信コール：シングル ナンバー リーチ					

DVO が最初に有効になったときのデフォルトのコール オプションは [自動選択（Autoselect）] です。これにより、デバイスが 802.11 WAN 経由で接続している場合は Cisco Jabber の着信コールと発信コールの両方で Voice over IP（VoIP）が発生します。デバイスがモバイル データ ネットワークに接続している場合は、発信コールに DVO が使用され、着信コールにシングル ナンバー リーチが使用されます。

いずれの場合も、Unified CM 内のモバイル クライアント デバイス設定で [緊急番号（Emergency Numbers）] フィールドに設定された緊急番号に発信されるコールは、選択されているコール オプションに関係なく、携帯電話ネットワーク経由で直接ダイヤルされます。

（注）　Dial via Office コール機能は、デュアルモードのスマートフォンにのみ適用されます。この機能は Apple iPad などのタブレットではサポートされません。これらのデバイスにセルラー音声無線がないためです。

シングル ナンバー リーチの場合と同様に、Dial Via Office が Cisco Jabber クライアントで有効になっている場合は、Cisco Unified Mobility のモバイル ボイス メール回避またはシングル企業ボイスメール ボックス機能が実行されます。Dial Via Office の場合、このボイス メール回避機能により、DVO コールのセットアップ中にネットワーク パス障害やその他の通信エラーが発生した場合、呼び出されたユーザが発信側ユーザのボイス メール ボックスに転送されないことが保証されます。通常は、ボイスメール回避によるユーザ制御方式が、全体的に最も優れたユーザ エクスペリエンスを実現します。これは、DVO コール レッグが誤ってボイスメール システムによって応答された場合、DTMF トーンが Unified CM によって受信されないとコール レッグが切断され、DVO コールが消去されるためです。Cisco Jabber ユーザでモバイル ボイス メール回避方式によるユーザ制御が有効になっている場合、クライアント デバイスでモビリティ コールを受信したときに、モバイル デバイスのキー パッドにあるボタンを押す必要があることをユーザに通知する必要があります。ボタンを押さないと、コール セットアップで障害が発生します。

(注)　モバイル ボイス メール回避によるユーザ制御方式は、PTSN 接続と PTSN ゲートウェイおよびアウトオブバンド経由でモバイル デバイスから Unified CM まで DTMF トーンが正常に伝達されることに完全に依存しているため、PSTN から Unified CM に着信 DTMF を伝達できない場合、モバイル デバイスから発信した（Dial Via Office Reverse）、またはモバイル デバイスが受信（シングル ナンバー リーチ）した社内コールがすべて切断されます。DTMF が PSTN から Unified CM に効果的にリレーできない場合、代わりにタイマー コントロールのモバイル ボイス メールの無効化方式を使用する必要があります。

シングル企業ボイス メール ボックスのボイス メールの回避機能に関する詳細情報については、シングル企業ボイスメール ボックスによるモバイル ボイスメール回避（21-59 ページ）を参照してください。

Dial Via Office コール オプションの使用例

Dial Via Office を配置するときには、次の Cisco Jabber クライアントのコール オプションのユーザ プロファイルを考慮してください。

- 自動選択

  [自動選択（Autoselect）] の一般的なユーザ プロファイルは、オフィス内とオフィス外の両方で移動するユーザです。このユーザ プロファイルの [自動選択（Autoselect）] は、802.11 WLAN 接続が使用可能な場合、VoIP を利用することでコストをできるだけ抑え、WLAN 接続が使用できない場合は、モバイル ボイスおよびデータ ネットワーク（DVO およびシングル ナンバー リーチ）に戻ります。

- モバイル音声ネットワーク

  [モバイル音声ネットワーク（Mobile Voice Network）] コール オプションの一般的なユーザ プロファイルは、WLAN カバレッジがほとんどなく、IP 接続で高品質かつ信頼性の高い通話を実現するためにモバイル データ接続では満足なスループットと信頼性が得られない高度なモバイル ユーザです。

- Voice over IP

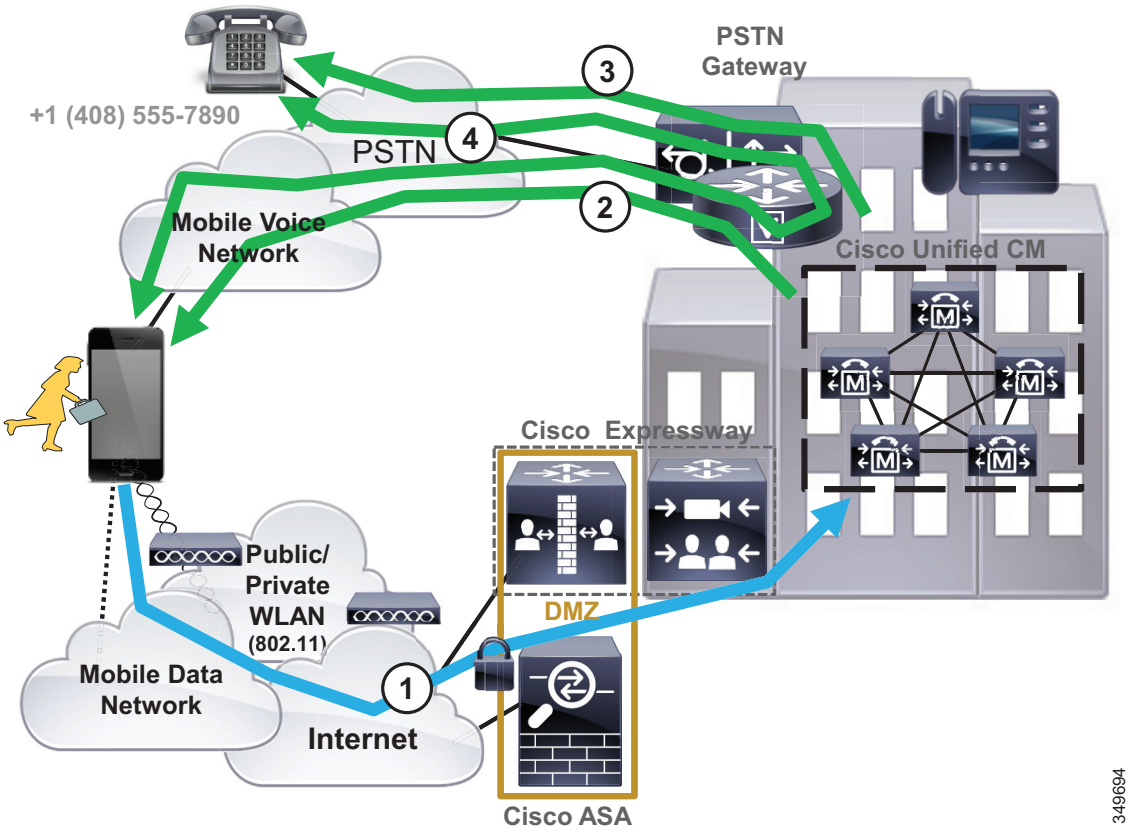
  [Voice over IP] コール オプションの一般的なユーザ プロファイルは、オフィス（自宅または会社）内で移動する、社内コールで社外への発信を通常必要としないユーザです。また、このユーザ プロファイルを使用する場合、企業負担および従業員負担のモバイル ボイス/データ サービスの点で、モバイル ボイスとデータのコストが重要な考慮事項になります。

Dial Via Office Reverse

Cisco Jabber クライアントは Dial Via Office Reverse（DVO-R）をサポートします。DVO のこの方式では、Unified CM システムからユーザ設定されたモビリティ ID または携帯電話番号への着信コールによってコール セットアップが実施されます。

図 21-32 は、DVO-R のコール フローを示しています。この例では、Cisco Jabber ユーザが PSTN 電話機（+1 408 555-7890 ）に電話をかけようとしています。ユーザは番号をダイヤルするか、Cisco Jabber クライアント内の連絡先リストから番号を選択し、企業および Unified CM に IP 接続経由で SIP コール セットアップ要求を生成します（ステップ 1）。コール セットアップ要求に基づいて、Unified CM は社内 PSTN ゲートウェイを使用して、ユーザの設定したモビリティ ID（携帯電話番号）にリバース コールを発信します（ステップ 2）。Unified CM からの着信コールがモバイル デバイスで応答されると、ユーザが呼び出した番号または選択した番号にコールが転送されます（ステップ 3：この場合は +1 408-555-7890）。一度コールが遠端で応答されると、メディア パスが接続され、会社の PSTN ゲートウェイ（ステップ 4）経由で固定されます。コールが会社のゲートウェイに固定されたため、ユーザはこのコール中の任意の時点で Unified Mobility のデスクトップフォン ピックアップ機能を使用したり、Unified Mobility DTMF ベースの通話切替機能を呼び出したりすることができます。

図 21-32　Cisco Jabber Dial Via Office Reverse



(注)　図 21-32 に示すコール フローでは、Cisco Jabber が Unified CM に登録されていると想定し、DVO がユーザに対して有効で、クライアントのコール オプション設定が [モバイル音声ネットワーク(Mobile Voice Network)] または [自動選択(Autoselect)] であると想定しています。クライアント設定が [自動選択(Autoselect)] の場合、Cisco Jabber を実行しているデュアル モード デバイスはモバイル データ ネットワーク経由で IP 接続される必要があります。802.11 WLAN 経由で接続されている場合、クライアントは DVO ではなく Voice over IP を使用します。

デフォルトで、DVO-R コールバックのコール レッグが(図 21-32 に示すように)ユーザのモバイル デバイスに転送されますが、ユーザが Cisco Jabber クライアント内の [DVO コールバック番号(DVO Callback Number)] フィールドで代替コールバック番号を指定することがあります。デフォルトで [DVO コールバック番号(DVO Callback Number)] フィールドには、ユーザ設定のモビリティ ID が入ります。ユーザがこのフィールドに異なる番号を設定すると、DVO-R コールバックのコール レッグがその番号に転送されます。たとえば、ユーザはコールバックを携帯電話で受信するよりも、自宅の電話に転送するよう希望することがあります。

(注)　代替コールバック番号を使用して DVO-R を呼び出す場合、Unified CM からのコールバックのコール レッグがユーザ指定の代替番号へ転送されると、そのコールは会社に固定されません。このような場合、ユーザはデスクトップフォンのピック アップを実行したり、代替コールバック番号を使用した DVO-R コールでの DTMF ベースの通話切替機能を呼び出したりすることができません。また、DVO-R 代替番号へのコールに対してボイス メール回避が適用されません。

(注)　DVO-R コールでは En-bloc ダイヤル方式が利用されるため、[オーバーラップ送信を許可(Allow Overlap Sending)] が有効にされるパターンでも、重複送信は適用されません。

モバイル プロファイルおよび Dial Via Office Reverse

モバイル クライアント デバイス向けモビリティ ID に Cisco Unified CM モビリティ プロファイルが割り当てられることがあります。必須ではありませんが、モビリティ プロファイルは、モビリティ ID または代替コールバック番号に DVO-R コールバックのコール レッグのセットアップ時にシステムによって送信される発信者 ID を指定します。モビリティ プロファイル設定ページの [Dial-via-Office Reverse Callback Configuration] セクションの [Callback Caller ID] フィールドに設定された番号は、発信者 ID として送信される番号ですモビリティ ID にモビリティ プロファイルが割り当てられていない場合、または [コールバック発信者 ID(Callback Caller ID)] フィールドが空白のままである場合、システムは、設定されたデフォルトのエンタープライズ機能アクセス番号を送信します。

(注)　モビリティ プロファイルの [モバイル クライアント コール オプション(Mobile Client Calling Option)] フィールドは DVO 操作に影響しません。この設定に関係なく、DVO コールが有効である場合は Cisco Jabber クライアントが DVO-R コールを発信します。Dial via Office Forward (DVO-F) コール オプションは、現在使用できません。

Cisco Jabber ポイントツーポイント コール

Cisco Jabber モバイル クライアントは、Unified CM の登録を必要としないポイントツーポイントの Voice and Video over IP(VVoIP)通話を提供できます。代わりに、Jabber クライアントは REST/HTTPS コール シグナリング用の Cisco WebEx Messenger クラウド サービスを活用します。ポイントツーポイント コール メディアでは、音声通話に G.722 コーデック、ビデオ通話に H.264 コーデックで RTP プロトコルを利用します。REST ポイントツーポイント コールでは、Jabber モバイル クライアントごとに 1 つのコールだけがサポートされ、保留、保留解除、転送、会議などの通話中の補足機能はサポートされません。

Cisco Jabber for iPhone and iPad 対応の Apple プッシュ通知サービス（APNs）

これまでの Cisco Jabber for iPhone and iPad クライアントでは、デバイス上でバックグラウンドで実行されている間、定期的なダイレクト IP ソケット キープアライブ メッセージを使用して、クライアントがバックグラウンドに移るときに、Voice and Video over IP（VVoIP）サービスや IM およびプレゼンス サービス用の接続を維持していました。このような定期的なメッセージにより、ユーザへの通知とクライアントでの着信コールおよびメッセージの受信が確実になります。Cisco Jabber for iPhone and iPad 11.9 以降、および Cisco Unified CM and IM and Presence Service リリース 11.5 SU3 以降（ならびに最新バージョンの WebEx Messenger）では、Apple iOS デバイス上でクライアントがバックグラウンドで実行中も、クライアントは Apple プッシュ通知サービス（APNs）を介して着信コールおよびメッセージを受信できるようになっています。

図 21-33 に、APNs のアーキテクチャを示します。緑色の矢印で示されているように、Unified CM や Unified CM IM and Presence Service（または WebEx Messenger）でクライアントへの通知が必要になると、Unified CM と Unified CM IM and Presence Service（または WebEx Messenger サービス）は、エンタープライズ ネットワークからインターネット上の Cisco Collaboration Cloud にアウトバウンド HTTPS 通知を送信します（ステップ 1）。Cisco Collaboration Cloud はインターネット上の Apple プッシュ通知サービス（APNs）へのセキュアな接続を確立して、Jabber クライアントへの通知を APNs に転送します（ステップ 2）。APNs は受信した通知を Jabber iOS クライアント デバイスに転送します（ステップ 3）。転送先のデバイスは、キャリア ネットワーク上の Apple デバイスの初期プロビジョニングであらかじめ APNs に登録されます。APNs によるこの通知により、ユーザに対するアラートがトリガーされます。この通知アーキテクチャは、Jabber for Apple iOS クライアントがオンプレミスで接続されているか、あるいは VPN または Expressway モバイルおよびリモート アクセスを介して接続されているかに関係なく適用されます。

図 21-33　Cisco Jabber for Apple iOS と APNs アーキテクチャの概要

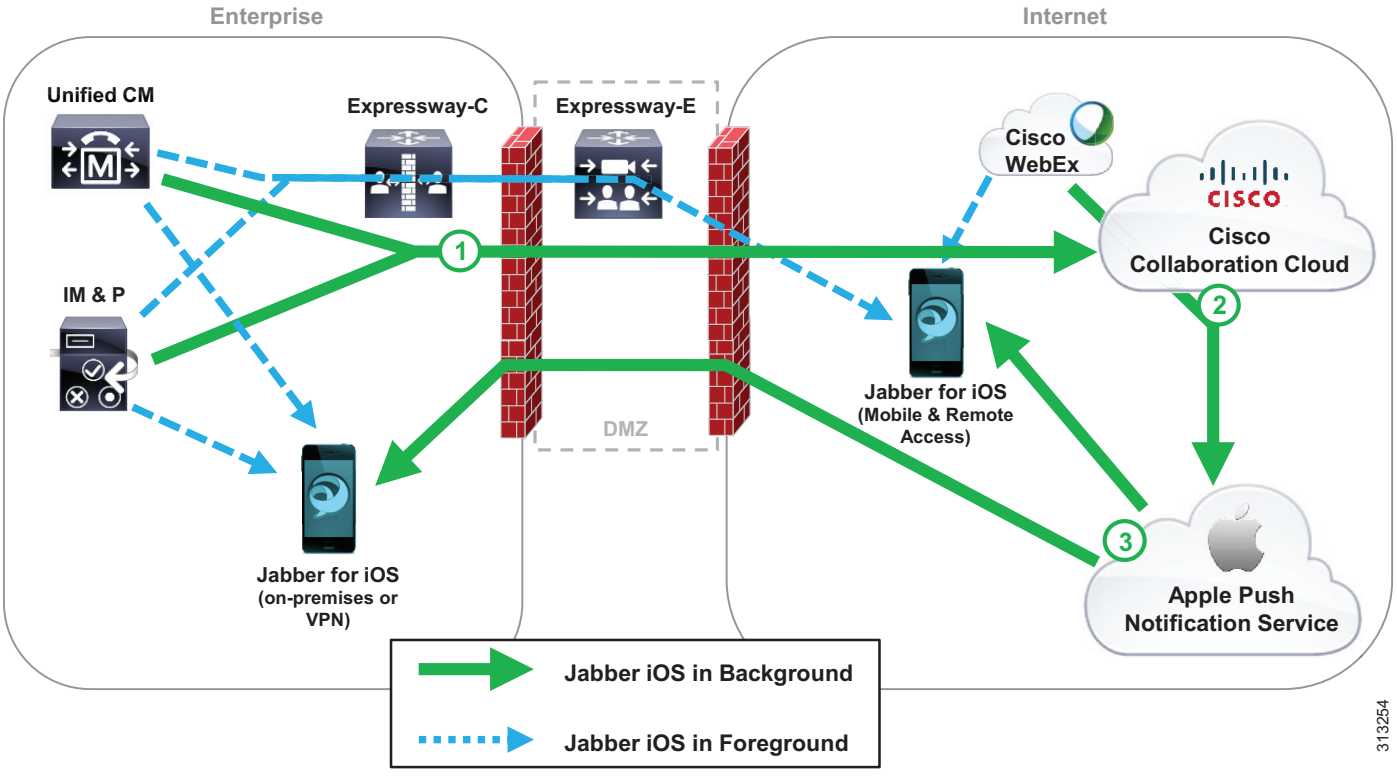


図 21-33 の青色の矢印で示されているように、Jabber for Apple iOS クライアントがフォアグラウンドで実行されているときは、Unified CM や Unified CM IM and Presence Service は SIP および XMPP を使用してクライアントに直接通知を送信します。

オンプレミスの Unified CM および Unified CM IM and Presence 導入環境では、管理者がクラウド オンボーディング プロセスによって、Cisco Jabber for iPhone and iPad クライアントの APNs を Unified CM 上で有効にします。APNs が有効にされると、バックグラウンドで実行中の Cisco Jabber for iPhone and iPad クライアントは、APNs を介してコールやメッセージの通知を受信するようになります。

(注)　最新バージョンの Apple iOS（iOS 10 と iOS 11 を含む）では引き続き、バックグラウンドで実行中の Cisco Jabber for iPhone and iPad クライアントが接続を維持するためのキープアライブ メッセージをサポートしています。したがって、Unified CM 上で APNs を有効化することは、まだ要件ではありません。ただし、Apple ではダイレクト IP ソケット方式の通知のサポートを終了していることから、Apple iOS デバイス上でバックグラウンドで実行中の Jabber for Apple iOS クライアントに通知を送信するには、APNs が間もなく要件となるはずです。現行のダイレクト IP ソケット方式が今後の Apple iOS リリースで除去された時点で、Cisco Jabber for iPhone and iPad クライアントがバックグラウンドで実行されている間、ユーザに着信コールやメッセージを通知する手段は APNs のみとなります。

WebEx Messenger を使用するクラウドまたはハイブリッド導入環境では、APNs は WebEx クラウド内でデフォルトによって有効にされています。したがって、バックグラウンドで実行中の Cisco Jabber for iPhone and iPad 11.9 以降のクライアントは APNs を介して IM 通知を受信します。

WebEx Messenger での Jabber 間コールは APNs でサポートされていません。WebEx Messenger で Jabber 間コール機能を使用する予定の場合は、jabber-config.xml ファイルの **< Policies >** **< Push_Notification_Enabled >** パラメータを使用して手動で APNs を無効にする必要があります。jabber-config.xml のパラメータについて詳しくは、以下のリンク先から入手できる最新バージョンの『*Parameters Reference Guide for Cisco Jabber*』を参照してください。

https://www.cisco.com/c/en/us/support/customer-collaboration/jabber-iphone-ipad/products-installation-guides-list.html

WebEx Messenger でエンドツーエンドの暗号化（AES）ポリシーを [強制（enforced）] または [オプション（optional）] に設定すると、APNs が自動的に無効にされて、バックグラウンドで実行中のクライアントは通常の方法で IM 通知を受信することになります。

(注)　バックグラウンドで実行中の Jabber に対する APNs の使用は、Cisco Jabber for iPhone and iPad クライアントにのみ適用されます。Windows、Mac、および Android Jabber クライアントには適用されないため、これらのクライアントはバックグラウンドで実行されている間、引き続き通常の方法で IM 通知を受信します。

Cisco Jabber とリフレッシュ トークンを使用した OAuth でのログイン フロー

Cisco Jabber 11.9 以降、OAuth 2.0 承認フレームワークを使用して、クライアント承認と認証を容易に行えるようになっています。これにより、ログインが迅速化されるとともに、起動時やネットワーク遷移時の再認証も迅速化されます。Cisco Unified CM 12.0 および Unified CM 11.5(1) SU3 の前までは、導入環境内でシングル サインオン（SSO）が有効にされている場合、Cisco Jabber は OAuth のみを使用していました。OAuth 実装は、認証を行い承認トークンをクライアントに発行する承認サーバとしての役割を果たす Unified CM パブリッシャに依存します。このトークンとリフレッシュ トークンにより、クライアントがコラボレーション サービスに要求を行い承認を取得することが可能になります。また、リフレッシュ トークンを使用して、期限切れの承認トークンを素早く更新できます。OAuth 2.0 フレームワークの詳細については、承認フレームワーク（16-46 ページ）の項を参照してください。

OAuth を Jabber クライアントの承認と認証に使用するには、Cisco Unified CM、Unified CM IM and Presence、Unity Connection で、**OAuth with Refresh Login Flow** サービス パラメータを有効にする必要があります。同様に、Jabber クライアントが Expressway モバイルおよびリモート アクセスで OAuth を使用するには、**Authorize by OAuth token with refresh** 設定を Expressway-C で有効にする必要があります。

Cisco Jabber での OAuth 展開の詳細については、次の URL で入手可能な最新バージョンのホワイト ペーパー『*Deploying OAuth with Cisco Collaboration Solution Release 12.0*』を参照してください。

https://www.cisco.com/c/en/us/support/unified-communications/jabber-windows/products-installation-guides-list.html

Cisco Jabber および Expressway モバイルとリモート アクセス

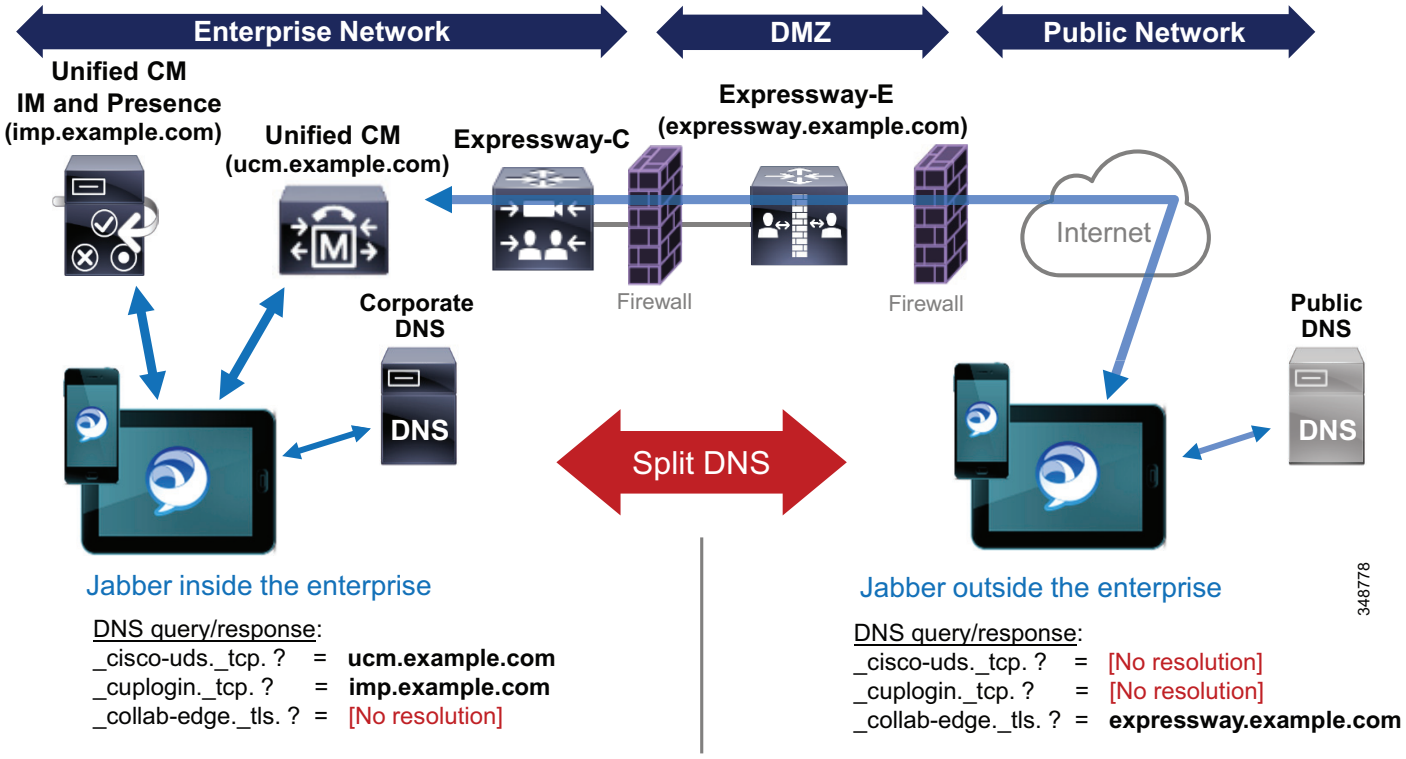
Cisco Expressway ソリューションのモバイルおよびリモート アクセス機能は、Cisco Jabber 用のセキュアなファイアウォール トラバーサルを提供します。これにより、リモート Jabber ユーザが企業の外にいるときに、モバイル デバイスから企業のコラボレーション アプリケーションやサービスにアクセスできます。

Expressway モバイルおよびリモート アクセス接続を通過するすべてのコラボレーション トラフィック（コール メディアやシグナリングを含む）は暗号化されます。暗号化された接続は、企業内の Expressway C ノードと Jabber エンドポイントの間で行われます。Expressway C と企業内のエンドポイントおよびアプリケーションの間のトラフィックは、デフォルトでは暗号化されません。Unified CM Cisco 証明書信頼リスト（CTL）プロバイダーおよび認証局プロキシ関数（CAPF）サービスに基づくセキュリティ設定によって促進されるデバイス認証、SRTP メディア、および TLS SIP シグナリング暗号化の混合モードとして Unified CM クラスタが設定されている場合にのみ、企業内のメディアとシグナリング トラフィックが暗号化されます。

DNS クエリ解決およびスプリット DNS 解決設計に基づいて、Jabber は企業との相対的なロケーション（内部または外部）を判別します。この場合、Unified CM のサービス レコード（_cisco-uds._tcp）および Unified CM IM and Presence のサービス レコード（_cuplogin._tcp）が社内 DNS でのみ設定され、Expressway のサービス レコード（_collab-edge._tls）がパブリック DNS でのみ設定されます。この分けられた設計により、企業内の場合は社内 DNS 解決で Jabber がコラボレーション サービスに直接誘導され、パブリック DNS 解決では Expressway 経由で接続するように Jabber に指示します。モバイル デバイスのネットワーク接続が変更されるたびに DNS クエリが Jabber によって送信されます。

図 21-34 に示すように、Jabber は _cisco-uds._tcp、_cuplog._tcp、および _collab-edge._tls の 3 つの SRV サービス レコードに関して DNS に照会します。企業内に位置している場合、Jabber クライアントは Unified CM または Unified CM IM and Presence を指し示す解決を社内 DNS から受け取ります。この場合、Jabber は解決されたコラボレーション アプリケーション サービス ノードに直接接続します。企業の外に位置している場合、Jabber はパブリック DNS から Unified CM または Unified CM IM and Presence の解決を受け取らず、代わりに Expressway を介して企業に接続するようクライアントに指示する Expressway 解決を受け取ります。

図 21-34　Cisco Jabber：企業内外のスプリット DNS 解決



（注）　Cisco AnyConnect VPN がリモート エンタープライズ接続に使用される場合、Jabber は VPN トンネル経由で社内 DNS から DNS クエリ解決を受け取り、コラボレーション サービス ノードに直接接続します。

Cisco Jabber モバイル クライアント用の Expressway モバイルおよびリモート アクセスを配置するときには、以下のサポートされない機能について考慮してください。

- デュアルモード ハンドオフ

  Jabber デバイスの WLAN インターフェイスからセルラー音声インターフェイスへのアクティブ コールの移動は、Expressway 接続ではサポートされません。

- エンドポイント認証およびメディアとシグナリングの暗号化のための CAPF 登録

  安全なメディアおよびシグナリングが企業ネットワークで必要とされる場合、Jabber デバイスはオンプレミスで、Expressway 経由の接続の前に、CAPF 登録を完了する必要があります。

- ユーザ単位またはデバイス単位のアクセス制限

  Expressway モバイルおよびリモート アクセスを介して接続しないよう特定のユーザやデバイスを制限するメカニズムはありません。コラボレーション インフラストラクチャ（Unified CM および Unified CM IM and Presence）で Expressway モバイルおよびリモート アクセスが展開されて Jabber 用にユーザがすでにプロビジョニングされている場合、ユーザは Expressway を介して接続できます。

- セッションの永続性

  Expressway モバイルおよびリモート アクセス経由のすべてのコールおよび他のコラボレーション アプリケーション接続は、ネットワーク パスが変更されるか失われると、必ず消去されます。

- LDAP ディレクトリ アクセス

  Expressway モバイルおよびリモート アクセス接続では LDAP トラフィックが無効です。このため、ディレクトリ アクセス方式として CDI が設定されていても、Expressway 経由で接続する際にすべての Jabber クライアントは社内ディレクトリ アクセスに UDS 方式だけを使用できます。

上記のいずれかの機能を配置する必要がある場合、安全な企業リモート アクセス用に Expressway の代わりに AnyConnect VPN を使用することを考慮してください。

Cisco AnyConnect VPNス プリット トンネルを使用した Cisco Jabber と Expressway モバイルおよびリモート アクセス

Jabber ユーザが VPN または Expressway のいずれかを介して接続できるようにするために、VPN および Expressway を並行して展開する必要が生じることがあります。このような状況では、2 つの方式を使用できます。Jabber ユーザはコラボレーション ワークロード用に Expressway モバイルおよびリモート アクセス機能を使用できます。また、企業への接続でコラボレーション外部のワークロードが必要な場合は、すべてのデバイス トラフィック用に VPN を使用できます。これらのシナリオでは、Cisco AnyConnect VPN クライアントによって企業への接続が確立されると、VPN オンデマンド トリガーまたはユーザによる手動起動のためにアクティブな接続がドロップされます。ユーザが使用を再開するには、VPN を介してプロビジョニングされたコラボレーション サービスに Jabber クライアントが再接続するのを待つ必要があります。これは、ユーザ エクスペリエンスを低下させます。

別の方法として、スプリット トンネリングを使って AnyConnect VPN と Expressway を同時に使用することもできます。この場合、コラボレーション フローは Expressway モバイルおよびリモート アクセス接続を必ず経由し、他すべてのトラフィックは VPN トンネルを経由します。この代替的な方法では、VPN トンネルが確立されると Jabber クライアントは Expressway から切断して VPN で再接続するのを回避できるため、通常はユーザ エクスペリエンスが向上します。

図 21-35 に示すように、この展開方法によって実現するスプリット トンネリングは、2 つの基本原則に依存しています。

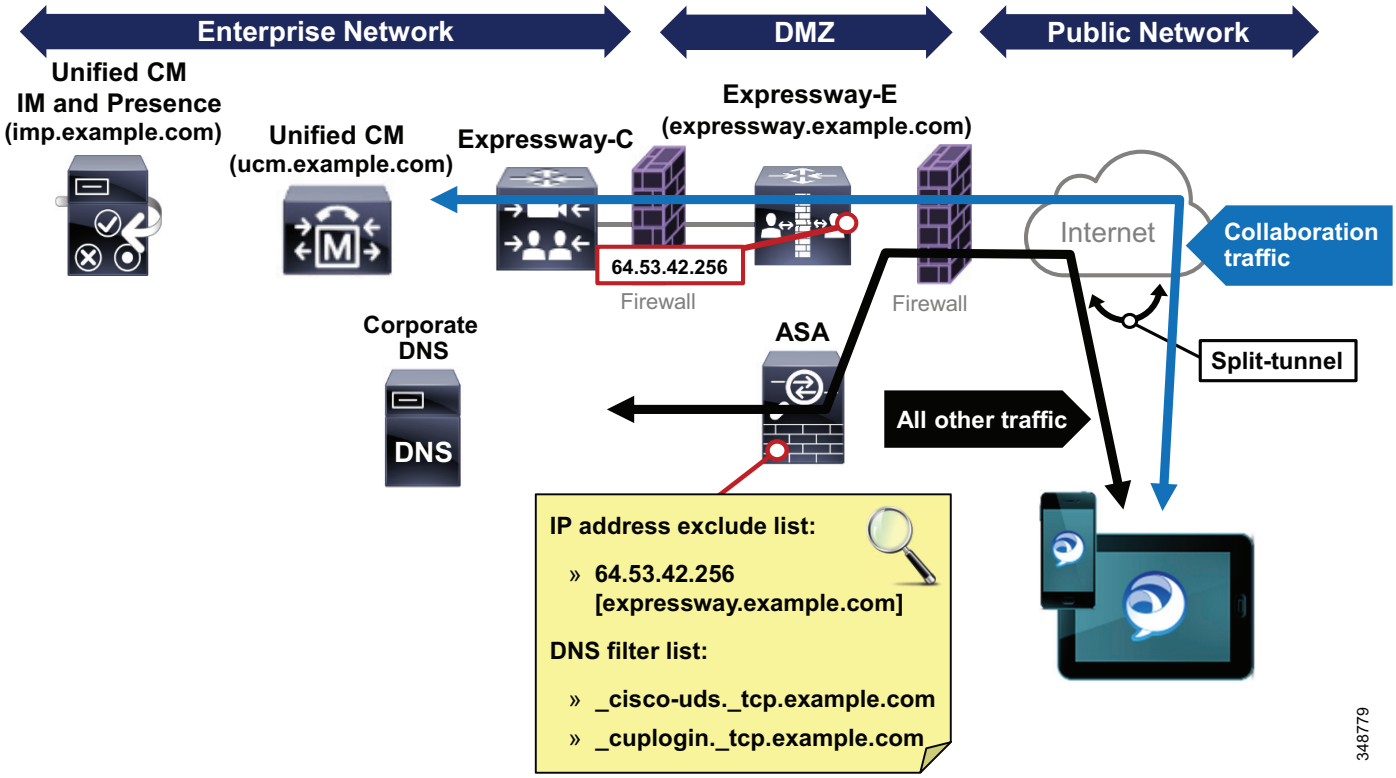
- Cisco 適応型セキュリティ アプライアンス（ASA）VPN ヘッドエンドでの DNS フィルタリング

  _cisco-uds._tcp.<*domain*> および _cuplogin._tcp.<*domain*> に関する Jabber クライアントからの DNS クエリをフィルタリングするために ASA でのトラフィック フィルタリングが使用されます。これらの DNS クエリがフィルタリングされるため、Jabber クライアントはコラボレーション サービスに直接接続するための Unified CM および IM and Presence サービス レコード要求を解決できません。したがって _collab-edge._tcp.<*domain*> に関する DNS 解決のみが得られ、結果として Expressway 接続とトラバーサルが常に使用されます。

- VPN トンネルでの Expressway アクセスの除外

  パブリックにインターフェイスに面している Expressway-E に Jabber クライアントが接続するのを防ぐために、ASA での IP アドレス フィルタリングが使用されます。Expressway-E ノードのパブリック インターフェイス IP アドレスをフィルタリングするとき、スプリット トンネル VPN 接続が作成され、結果として VPN トンネルから Jabber トラフィックが除外されます。こうして、このトラフィックが Expressway を通過し、その他すべてのトラフィックは VPN トンネルを通過します。

図 21-35　Cisco Jabber：Expressway モバイルおよびリモート アクセスと Cisco AnyConnect VPN



Expressway モバイルおよびリモート アクセスを使用する AnyConnect VPN スプリット トンネリングの場合、パブリック DNS で設定された同じ Expressway DNS SRV レコード（_collab-edge._tls）が社内 DNS に追加されます。これにより、VPN トンネル経由でパブリック DNS へのアクセスを提供したり DNS クエリを転送したりする必要がなくなります。

同じ _collab-edge._tls SRV レコードを社内 DNS で設定することは、Jabber と Expressway モバイルおよびリモート アクセスの配置で期待される基本的なスプリット DNS 設計にそぐわないように思われるかもしれませんが、実際には Jabber での SRV 解決設定順序によって適切な動作が保証されます。Jabber での SRV 解決設定順序によると、最初は Unified CM（_cisco-uds._tcp）、次に IM and Presence（_cuplogin._tcp）、そして最後に Expressway（_collab-edge._tls）です。したがって、_collab-edge._tls クエリが社内 DNS で解決できる場合でも、社内 DNS が _cisco-uds._tcp または _cuplogin._tcp サービスのクエリを最初に解決するため、クライアントはコラボレーション サービスに直接接続します。

AnyConnect VPN を使用する Jabber と Expressway モバイルおよびリモート アクセスの詳細については、次の URL で入手できる『*Cisco Unified Access (UA) and Bring Your Own Device (BYOD) CVD*』の Cisco Expressway シリーズとモバイルおよびリモート アクセスのコラボレーションに関する情報を参照してください。

https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Borderless_Networks/Unified_Access/BYOD_Design_Guide.html

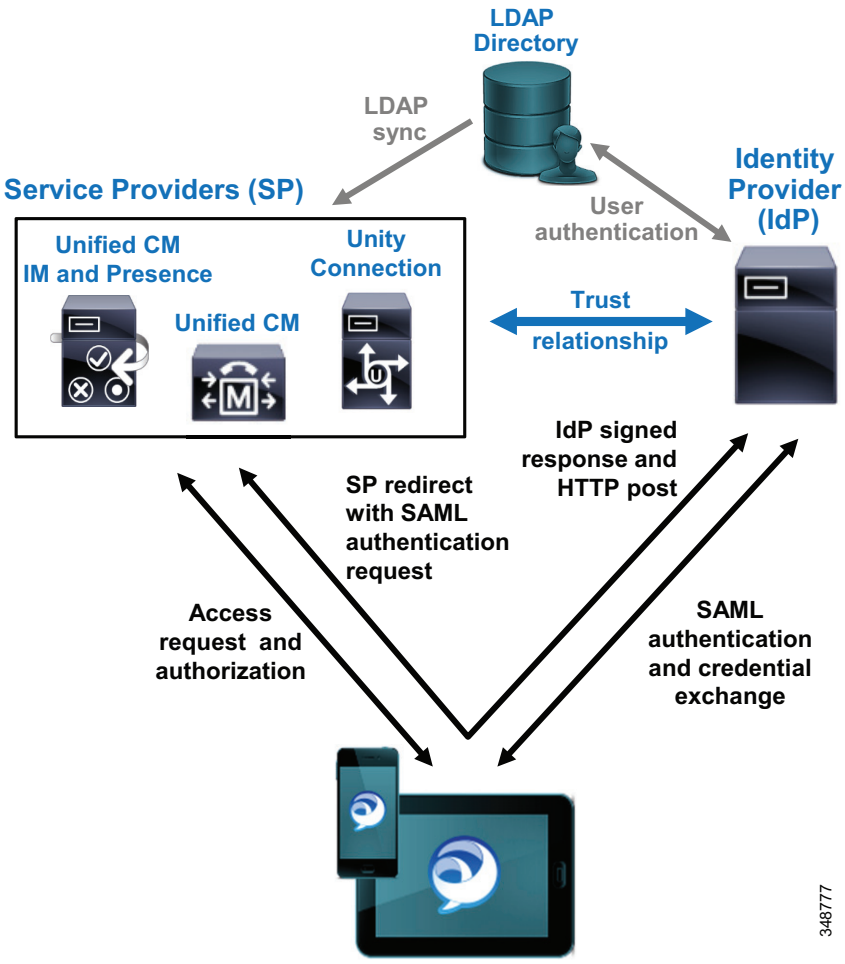
Cisco Jabber と SAML シングル サインオン

Cisco Jabber モバイル クライアントは、Security Assertion Markup Language（SAML）バージョン 2 を使用してシングル サインオン（SSO）を活用できます。Jabber とシスコ コラボレーション インフラストラクチャ（Unified CM、Unified CM IM and Presence など）、および Unity Connection は、ユーザ接続を識別して認証するために Web ベースの SSO SAML v2 を使用します。これにより、Jabber ユーザ クレデンシャルの単一セットを使ってすべてのコラボレーション サービスにアクセスできます。

図 21-36 に示すように、Cisco Jabber SSO は、Unified CM などのコラボレーション アプリケーション（サービス プロバイダーとも呼ばれます）と ID プロバイダー（IdP）の間の事前に確立された信頼関係に依存します。Unified CM および Unity Connection サービス プロバイダーは、ユーザを特定するために、社内 LDAP ディレクトリとの LDAP 同期および統合を使用します。同様に、IdP はユーザを認証するために LDAP 社内ディレクトリを使用します。Cisco Jabber およびコラボレーション サービスでサポートされる IdP には、Ping Federate、Microsoft Active Directory フェデレーション サービス（ADFS）、および Open Access Manager（OpenAM）が含まれます。

図 21-36 には、基本的な Jabber SSO のフローが示されています。SSO フローは、コラボレーション サービス プロバイダーへのアクセス（たとえば、呼制御サービス用の Unified CM へのアクセス）を要求する Jabber クライアントで始まります。サービス プロバイダーは、コラボレーション サービス プロバイダーに直接ログインしてアクセスする代わりに、SAML 認証要求を使って Jabber クライアントを IdP にリダイレクトします。IdP は Jabber ユーザに認証クレデンシャルを要求し、社内 LDAP ディレクトリに対してユーザを認証します。ユーザが正常に認証された場合、IdP は署名付きアサーションを返します。Jabber は HTTP POST を使用してこれをコラボレーション サービス プロバイダーに転送します。次にコラボレーション サービス プロバイダーは、署名付きアサーションを検証し、Jabber クライアントに許可を与えます。たとえば、Jabber は Unified CM に正常に登録されます。

図 21-36　SAML SSO を使用する Cisco Jabber



署名付きアサーションを Jabber クライアントに転送することに加えて、IdP は認証済み Jabber クライアントのセキュリティ コンテキストを保存します。クライアントが他のコラボレーション サービス プロバイダーへのアクセスを要求した場合、IdP は改めてクレデンシャルを交換する必要がなく、後続の署名付きアサーションを提供できます。こうして SSO により、Jabber ユーザまたはクライアントは、クレデンシャルを一度だけ入力して、複数のコラボレーション サービスにアクセスすることができます。

ユーザ認証時にコラボレーション サービス プロバイダーが IdP とは直接通信しない点に注意してください。

SSO の詳細については、アイデンティティ管理アーキテクチャの概要（16-35 ページ）および最新バージョンの『*SAML SSO Deployment Guide for Cisco Unified Communications Applications*』を参照してください（次の URL から入手できます）。

https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html

SSO でユーザを識別し、オンプレミス コラボレーション アプリケーション/サービスに対して認証することに加えて、Expressway モバイルおよびリモート アクセス接続でのユーザ認証のために SAML SSO を有効にすることもできます。これらのシナリオでは、インバウンド リモート アクセス接続用の認証を仲介させるために、HTTPS リバース プロキシを企業の DMZ に配置します。HTTPS リバース プロキシは社内 IdP と通信し、リモート クライアントと社内 IdP の間の SAML 要求/認証交換を仲介します。DMZ の HTTPS リバース プロキシとして任意の汎用 HTTPS リバース プロキシを使用できますが、SSO SAML 要求の仲介やプロキシのために IdP プロキシの役割を果たす IdP インスタンスを DMZ にインストールするオプションが、一部の IdP ベンダーで提供されています。

Cisco Jabber と Cisco Unified Mobility との間の相互作用

Cisco Jabber モバイル クライアントを Cisco Unified Mobility に統合することで、Cisco シングル ナンバー リーチ、通話切替 DTMF 機能、2 段階ダイヤリング、シングル企業ボイスメール ボックスのモバイル ボイスメール回避を利用できます。

Unified Mobility と統合するには、iPhone または Android デュアルモード携帯電話番号を、Cisco Dual Mode for iPhone または Cisco Dual Mode for Android デバイスに関連付けられたモビリティ ID として Unified CM 内で設定する必要があります。システム内で携帯の番号をモビリティ ID として設定した後は、iPhone または Android デュアルモード デバイスが企業に接続されず Unified CM に登録されていない場合に、シングル ナンバー リーチを利用して、ユーザの会社の電話番号への着信コールをモバイル ボイス ネットワーク経由で iPhone または Android デュアルモード デバイスに転送できます。デュアル モード デバイスが会社に接続され、Unified CM に登録されている場合、着信 Voice-over-IP コールが有効になるようにクライアント コール オプションが設定されると（デバイスが WLAN に接続しているときの [Voice over IP] または [自動選択（Autoselect）]）、会社の電話番号に対する着信 IP コールはデバイスのモバイル ボイス ネットワーク インターフェイスに転送されません。iPhone または Android デュアルモード デバイスが企業に接続されている場合は、デバイスの WLAN またはモバイル データ インターフェイスだけが着信コールを受信します。これにより、会社の PSTN ゲートウェイ リソースの必要以上の消費を回避できます。

携帯電話音声ネットワークを介して社内コールを処理する場合、iPhone または Android デュアルモード デバイスは、DTMF を使用して通話切替機能を呼び出したり、会社の任意の固定コールに対するデスクトップフォンのピック アップを実行したりできます。また、デュアルモード デバイスでは、コールを発信する場合にモバイル ボイス アクセスとエンタープライズ機能アクセスの 2 ステージ ダイヤリング機能を利用して、これらのコールを会社経由でルーティングし、会社の PSTN ゲートウェイにアンカリングできます。

iPhone または Android デュアルモード デバイスにモビリティ ID を設定することに加えて、リモート接続先として追加の携帯電話番号またはオフシステム電話番号を設定して、それらの番号を Unified CM 内で Cisco Dual Mode for iPhone または Cisco Dual Mode for Android デバイスに関連付けることができます。モビリティ ID および追加のリモート接続先をデュアルモード デバイスに関連付けるときに、リモート接続先プロファイルを設定する必要はありません。

（たとえば Android スマートフォンで Cisco Jabber for Android を実行し、Apple iPad で Cisco Jabber for iPhone and iPad を実行しているユーザなど）モバイル ユーザが複数のモバイル デバイスにまたがる複数のシスコ モバイル クライアントをプロビジョニングする場合、モビリティ ID をタブレット デバイス（Cisco Jabber for Tablet）ではなく、デュアルモード デバイス（Cisco Dual Mode for Android など）に関連付けます。デュアルモード デバイスは、デュアルモード ハンドオフや Dial Via Office などのモビリティ ID 固有の機能を利用するため、モビリティ ID をこのデバイスに関連付ける必要があります。モビリティ ID と同じデバイスに他のリモート接続先をすべて関連付けます。同じユーザに対して異なるモバイル クライアント デバイスの異なるリモート宛先を関連付けると、設定がより複雑になり、問題の修復が難しくなります。

Cisco Unified Mobility のフィーチャ セット、および設計と配置の考慮事項の詳細については、Cisco Unified Mobility（21-51 ページ）を参照してください。

Cisco Jabber とモバイル音声用 Cisco Intelligent Proximity の間の相互作用

モバイル音声用のインテリジェント プロキシミティ機能は、携帯電話またはデュアルモード デバイスのモバイル回線でハンズフリー音声を可能にするために設計されています。このため通常は、Jabber クライアント デバイスの携帯電話回線の通話でのみ、インテリジェント プロキシミティ可能な IP エンドポイントでハンズフリー音声再生を行えます。Cisco Jabber での Voice and Video over IP コールの場合、モバイル音声のインテリジェント プロキシミティは起動されません。これに関する唯一の例外は、Cisco IP Phone 8851 および 8861 エンドポイントです。これらの IP フォンは音声専用であるため、モバイル音声のインテリジェント プロキシミティを使用すると、Jabber IP ベース コールの音声が 8851 フォンまたは 8861 フォンを経由してストリーミングされ、このコールのビデオ部分は Jabber クライアント デバイスに残ります。モバイル音声のインテリジェント プロキシミティが可能なその他のハードウェア エンドポイントの場合、Jabber IP ベースのコールの音声は IP エンドポイントで再生されません。

Cisco Spark

Cisco Spark モバイル クライアントは、Android および iPad や iPhone などの Apple iOS で使用できます。適切なアプリケーション ストア（Apple の App Store や Google Play）からクライアント アプリケーションをダウンロードし、Apple iOS または Android デバイスにインストールした後、ユーザは自分の電子メール アドレスを入力し、結果として送られてくるプロビジョニング電子メールでアカウントをアクティブにする必要があります。ユーザがアカウントをアクティブにすると、クライアントは Cisco Collaboration Cloud に接続します。ユーザは、暗号化されたインスタント メッセージ（IM）を使って 1 人以上の他のユーザと通信するための安全なコラボレーション ルームを作成できます。ユーザは、自分のアカウントのパスワードを設定するために、Web ブラウザを使用して少なくとも一度 Cisco Spark（https://web.ciscospark.com/）にアクセスする必要があります。あるいは、ユーザは https://download.ciscospark.com/ からダウンロードして入手できるデスクトップ用の Cisco Spark クライアントを使用することもできます。これを行わないと、ユーザがモバイル クライアントで接続するたびに、電子メールを介してアカウントを有効にする必要が生じます。

Cisco Spark for Android、iPad、および iPhone クライアントは、セキュアで持続的な IM コラボレーション ルームを提供するだけでなく、暗号化された Voice and Video over IP やファイル共有機能も提供します。

Cisco Spark クライアントが正常に動作するには、モバイル デバイスがワイヤレス ネットワーク（企業またはパブリック/プライベート 802.11 WLAN、あるいはモバイル プロバイダー データ ネットワーク）に接続することで、インターネットにアクセスできる必要があります。

（注）　Cisco Jabber と同じく、Apple iOS デバイス上で稼働する, Cisco Spark モバイル クライアント（iPhone と iPad）も、バックグラウンドでの実行中に Apple プッシュ通知サービス（APNs）を使用します（Cisco Jabber for iPhone and iPad 対応の Apple プッシュ通知サービス（APNs）（21-108 ページ）を参照）。

Cisco Spark モバイル クライアント、追加の機能、およびサポートされているハードウェアとソフトウェアのバージョンの詳細については、次の Cisco Spark のドキュメントを参照してください。

https://support.ciscospark.com/

Cisco WebEx Meetings

Cisco WebEx Meetings モバイル クライアントは、特定の Android、Apple iOS、BlackBerry、および Windows Phone モバイル デバイスで稼働します。このクライアントを使用すると、モバイル エンドポイントはデスクトップ ブラウザ ベースの Cisco WebEx Meetings と同様の機能を持つ Cisco WebEx Meetings に参加できます。このクライアントによって、Cisco WebEx 音声およびビデオ会議へのアクティブな参加（参加者リストや共有コンテンツを表示する機能を含む）が可能になります。

Cisco WebEx モバイル クライアントに関する詳細情報については、次の URL にある製品情報を参照してください。

https://www.cisco.com/c/en/us/products/conferencing/webex-meetings/index.html

シスコのクラウド コラボレーション サービス：Cisco Spark および Cisco WebEx 用の SAML SSO

前述のオンプレミス エンタープライズおよびコラボレーション エッジと同様に、Cisco Spark や Cisco WebEx などのクラウド コラボレーション サービスに安全にログインにするためにエンタープライズ SSO を使用することもできます。このタイプの配置では、企業 IdP と、企業 DMZ に配置された HTTPS リバース プロキシを併用することで、企業クレデンシャルを活用してユーザを識別し、Cisco Spark や Cisco WebEx へのアクセスを認証します。

Cisco AnyConnect モバイル クライアント

Cisco AnyConnect モバイル クライアントは、Cisco Jabber モバイル デバイス クライアント用の安全なリモート接続機能を提供し、モバイル データ ネットワークと非企業 WLAN 経由の接続を有効にします。Cisco AnyConnect モバイル クライアントは、Apple の App Store または Google Play（以前の Android Market）からダウンロードできます。このクライアント アプリケーションは、Cisco Adaptive Security Appliance（ASA）ヘッドエンドで利用可能な Cisco AnyConnect VPN ソリューションを使用して、Apple iOS および Android モバイル デバイスに SSL VPN 接続を提供します。

モバイル データ ネットワークあるいはパブリック/プライベート Wi-Fi ホット スポットを介した接続に VPN ネットワーク接続を利用する場合は、企業のセキュリティ要件およびポリシーに沿った広帯域かつセキュアな VPN インフラストラクチャを配置することが重要です。この接続を利用するユーザおよびデバイスの数に基づき、広帯域幅、信頼性の高い接続、および適切なセッションまたは接続キャパシティをこの VPN インフラストラクチャで提供できるよう、慎重に計画することが必要です。

Cisco AnyConnect を使用したセキュアなリモート VPN 接続の詳細については、次の Web サイトで入手可能な Cisco AnyConnect Secure Mobile Client マニュアルを参照してください。

https://www.cisco.com/c/en/us/support/security/anyconnect-secure-mobility-client/tsd-products-support-series-home.html

シスコのモバイル クライアントおよびデバイスのハイ アベイラビリティ

モバイル デバイス、特にデュアルモード電話機はその特性上、ネットワーク接続に関して高い可用性を備えています（WLAN ネットワークが利用できない場合には、モバイル ボイスおよびデータ ネットワークを音声およびデータ サービスに使用できます）。しかし企業の WLAN および IP テレフォニー インフラストラクチャのハイ アベイラビリティについては、まだ考慮すべき点があります。

まず、企業の WLAN は、冗長な WLAN アクセスが可能になるように配置する必要があります。たとえば、AP およびその他の WLAN インフラストラクチャ コンポーネントは、ワイヤレス AP の 1 つに障害が発生しても、モバイル デバイスのネットワーク接続には影響がないように配置する必要があります。同様に、モバイル デバイスが常にネットワークに安全に接続できるように、WLAN の管理およびセキュリティ インフラストラクチャも高い冗長性を備えた配置にする必要があります。コントローラベースのワイヤレス LAN インフラストラクチャが推奨されます。その理由は、企業内 AP の集中型設定および管理が可能であり、ネットワーク アクティビティや AP の障害に基づいて WLAN を動的に調整できるためです。

次に、Cisco ASA ヘッドエンド VPN ターミネータや Cisco Expressway E および Expressway C ノードを含むリモート セキュア接続ソリューションのコンポーネントは、高い冗長性を備えた配置にする必要があります。こうすると Cisco ASA や Cisco Expressway ノードの損失がモバイル クライアントの安全なモバイルやリモート アクセスの接続に影響したり、妨げになったりしません。

次に、Unified CM の呼処理サービスおよび登録サービスのハイ アベイラビリティについて考慮する必要があります。Unified CM の呼処理サービスを利用する企業内の他のデバイスの場合と同様に、モバイル クライアント デバイスを Unified CM に登録する必要があります。Unified CM クラスタのアーキテクチャにはプライマリとバックアップの呼処理サービスおよびデバイス登録サービスが用意されており、冗長な特性を持っているため、1 つの Unified CM サーバ ノードで障害が発生しても、モバイル デバイスの登録やコール ルーティングは引き続き利用可能です。

PSTN アクセスについても同様の事項を考慮する必要があります。IP テレフォニー配置と同様、複数の PSTN ゲートウェイおよびコール ルーティング パスを配置して、PSTN への可用性の高いアクセスを確保する必要があります。このことは、モバイル クライアント デバイスの配置に固有の考慮事項ではありませんが、それでも重要な考慮事項です。

Cisco Collaboration Cloud の場合、クラウド データセンターにおける冗長性の高いコンポーネントおよびリソース設計（コンピューティングとネットワーク アクセスの両方のプラットフォームを含む）のために、WebEx および Cisco Spark サービスは高い可用性を備えています。この耐障害性に優れたインフラストラクチャ設計は、Cisco Collaboration Cloud サービスに依存するシスコ モバイル クライアントに信頼性の高いアクセスを提供します。

シスコのモバイル クライアントおよびデバイスのキャパシティ プランニング

シスコのモバイル クライアントおよびデバイス（デュアルモード電話機を含む）におけるキャパシティ プランニングに関する考慮事項は、登録、呼処理、PSTN アクセス サービスのために IP テレフォニー インフラストラクチャやアプリケーションを利用している他の IP テレフォニー エンドポイントまたはデバイスの場合と同じです。

Unified CM を使用してシスコのモバイル クライアントとデバイスを配置するときには、Unified CM での登録負荷および Unified Mobility の制限事項を考慮することが重要です。1 つの Unified CM サーバは、最大 40,000 台のデバイスの設定と登録を処理できます。モバイル クライアントとデバイスを配置するときには、クラスタあたりサポートされる最大デバイス数を考慮する必要があり、場合によっては追加的な負荷を処理するために呼処理クラスタをさらに配置する必要が生じることもあります。

また、前に説明したように、1 つの Unified CM クラスタ内のリモート接続先およびモビリティ ID の最大数は 40,000 です。ほとんどのデュアルモード モバイル クライアント デバイスは、シングル ナンバー リーチ、シングル企業ボイスメール ボックス、モバイル ボイスメール、モバイル ボイスメール回避、デスクトップフォンのピックアップ、2 段階ダイヤリングなどの機能を利用するために Unified Mobility と統合されることが多いため、これらの各デュアルモード モバイル デバイスの携帯電話番号を Unified CM クラスタ内のモビリティ ID として設定する必要があります。これは、Unified Mobility との統合を容易にするため、またハンドオフ番号方式のハンドアウトを容易にするために必要です。したがって、これらのデュアルモード デバイスを Unified Mobility と統合するときには、Unified CM クラスタにおけるリモート接続先およびモビリティ ID の全体的な容量を考慮して、十分な容量を確保することが重要です。追加のユーザまたはデバイスがシステム内の Unified Mobility にすでに統合されている場合は、これらのユーザまたはデバイスによって、デュアルモード デバイスで利用可能なリモート接続先およびモビリティ ID の空き容量が制限される可能性があります。

シスコのモバイル クライアントの拡張性に関するもう 1 つの考慮事項は、Expressway C と Expressway E での Cisco Expressway モバイル/リモート アクセス コールおよびプロキシ登録キャパシティです。Expressway C および Expressway E クラスタは、最大 10,000 件のプロキシ登録と最大 2,000 のビデオまたは 4,000 の音声コールをサポートします。シスコのモバイル クライアントに使用できるキャパシティを決定する際、その他の Expressway 接続デバイス（たとえば Cisco TelePresence MX/SX シリーズのデバイスのような Jabber デスクトップ クライアントや固定エンドポイント、および 7800 や 8800 シリーズのデバイスのようなシスコ デスク フォン）を計算に含めるのを忘れないでください。同様に、Expressway モバイルおよびリモート アクセスを介して企業に接続するシスコのモバイル クライアント デバイスに関して、Unified CM クラスタ ノードの登録負荷を考慮する必要もあります。Cisco Expressway モバイルおよびリモート アクセスのサイジングについては、Cisco Expressway（25-39 ページ）を参照してください。

モバイル クライアント デバイスを展開するときには、Unified CM システムおよび PSTN ゲートウェイの全体的な呼処理能力を考慮する必要もあります。モバイル デバイスの実際の設定および登録を処理する以外に、こうしたシステムでは、これらのモバイル デバイスとユーザによって増加する BHCA の影響に対処するための十分な能力も必要です。同様に、モバイル デバイスを処理するのに十分な PSTN ゲートウェイ能力を確保することも重要です。通常、デュアルモード モバイル デバイスを持つユーザは頻繁に移動することが多いため、Unified Mobility に統合されているデュアルモード デバイスではこれが特に当てはまります。通常、頻繁に移動するユーザは、モバイル ユーザの会社の電話番号への着信コールによって PSTN への 1 つ以上のコールが発信されるシングル ナンバー リーチなどのモビリティ機能や、会社の PSTN ゲートウェイを利用してユーザが会社経由でコールを発信する 2 ステージ（段階）ダイヤリングなどを使用することで、会社の PSTN ゲートウェイの負荷を高める傾向にあります。

最後に、シスコのモバイル クライアントとデバイスを配置する場合、企業モビリティ配置と同様に、802.11 WLAN コール キャパシティを考慮する必要があります。前述のとおり、802.11 チャネル セルあたり、最大 27 件の VoWLAN コールまたは最大 8 件の VVoWLAN コールが可能です。ここでは、デバイスが 2.4 GHz 帯域に配置される場合の Bluetooth なし、VoWLAN コール用に 24 Mbps 以上のデータ レート、および VVoWLAN コール用に最大 1 Mbps ビット レートで 720p のビデオ解像度を想定しています。実際のコール キャパシティは、RF 環境、ワイヤレス エンドポイント タイプおよび WLAN インフラストラクチャに応じてさらに小さくなることがあります。802.11 WLAN コール キャパシティの詳細については、キャンパス企業モビリティのキャパシティ プランニング（21-9 ページ）を参照してください。

上記のすべての考慮事項が、モバイル クライアントやデバイスに固有であるわけではありません。これらの考慮事項は、デバイスやユーザが Unified CM に追加されてシステム全体の負荷が高まるすべての状況に当てはまります。

一般的なシステム サイジング、キャパシティ プランニング、および配置上の考慮事項の詳細については、コラボレーション ソリューション サイジング ガイダンス（25-1 ページ）の章を参照してください。

シスコのモバイル クライアントおよびデバイスの設計上の考慮事項

シスコのモバイル クライアントとデバイスを配置する際は、次の設計上の推奨事項に従ってください。

- モバイル ボイス ネットワークとモバイル データ ネットワーク、および WLAN ネットワークの両方に同時に接続するために、デュアルモード モバイル デバイスでは、デュアル転送モード（DTM）がサポートされている必要があります。これにより、デバイスのセルラー無線と WLAN インターフェイスの両方からデバイスに到達可能になり、両方のインターフェイスでコールを発信および受信できます。モバイル ボイス ネットワークおよびモバイル データ ネットワークでデュアル接続デバイスがサポートされていない場合には、適切なデュアルモード クライアント操作が実行できない場合があります。
- WLAN AP は、20 % 以上のセル オーバーラップを確保して配置される必要があります。このようにオーバーラップさせることによって、モバイル デバイスがロケーション内で移動した場合に AP 間で正常にローミングして、ボイス ネットワーク接続およびデータ ネットワーク接続を維持できます。
- パケット損失を最小限に抑えるために、WLAN AP は -67 dBm のセル パワー レベル境界（またはチャネル セル半径）で配置される必要があります。また、同一チャネルのセル境界の分離は、約 19 dBm にする必要があります。AP またはクライアントにおいて、同じチャネルに関連付けられている他のデバイスとの同一チャネル干渉を発生させないようにするには、19 dBm の同一チャネル セル分離が重要です。このような干渉が発生すると、音声とビデオの品質が低下する場合があります。
- 可能であれば、音声およびビデオ トラフィックを生成できるモバイル クライアントおよびデバイス接続用の 5 GHz WLAN 帯域（802.11a/n/ac）を利用してください。5 GHz WLAN は、音声コールとビデオ コールに関してスループットを改善し、干渉を低減します。
- クライアント アプリケーションの音声とビデオ コールの品質、およびすべての機能の適切な動作を保証するために、音声メディアと専用ビデオおよびシグナリング帯域幅に対するプライオリティ キューイングを含む必要なエンドツーエンド QoS サービス クラスをサポートするように、企業の有線および無線 LAN を配置して設定する必要があります。ほとんどのクライアントがシスコの QoS の推奨事項に基づいてレイヤ 3 でトラフィックを適切にマークしますが、適切なレイヤ 2 WLAN UP マーキングはクライアント デバイスとベンダー実装に依存します。このため、レイヤ 2 マーキングはプラットフォーム間で一貫しておらず、信頼度は低くなります。
- モバイル デバイスがデスクトップ コンピュータと同様に、多種多様なデータおよびリアルタイム トラフィックを生成する可能性があるため、これらのデバイスは通常、信頼できないと見なされます。したがって、ポート番号やプロトコルに基づいてこれらのクライアント デバイスからのすべてのトラフィックを再マーキングするよう、ネットワークを設定する必要があります。同様に、ネットワークへの入口のレート制限およびポリシングが推奨されます。
- シスコでは、モバイル デバイスやクライアントに接続するために、エンタープライズ クラスの音声/ビデオ最適化された WLAN ネットワークだけを使用することを推奨します。ほとんどのモバイル クライアント デバイスは、パブリック/プライベート WLAN アクセス ポイントやホット スポットに接続し、インターネット経由で会社に接続して呼制御やその他のコラボレーション サービスを利用できますが、このようなタイプの接続の場合、音声とビデオの品質は保証されません。
- シスコのコラボレーション モバイル クライアントおよびデバイスを Bring Your Own Device（BYOD）インフラストラクチャに配置する場合、管理者は、ユーザの介入を必要とせず、IP テレフォニー インフラストラクチャを最大限に活用できるネットワーク接続方式を考慮する必要があります。さらに、リモート接続シナリオでは、シスコ モバイル クライアントとデバイスがコラボレーション サービスにアクセスできるように、すべての関連するポートを企業ファイアウォールでオープンにする必要があります。

- BYOD インフラストラクチャにおいて、紛失または盗難されたモバイル デバイスをリモートで消去、あるいは工場出荷時の状態にリセットすることが企業のポリシーにより定められている場合、個人のモバイル デバイスを使用している従業員はポリシーを認識し、定期的に個人データをバック アップする必要があります。
- デュアルモード デバイスが社内にあり、Unified CM に登録されている場合、Unified Mobility シングル ナンバー リーチ機能は、デュアルモード デバイスの設定済みモビリティ ID に着信コールを転送しません。これは、企業の PSTN リソースの利用を削減するための仕様です。デュアルモード デバイスは Unified CM に登録されるため、システムでは、デバイスが社内で到達可能であるかどうかを把握できます。社内で到達可能である場合は、コールを PSTN に転送してデュアルモード デバイスのセルラー音声無線を呼び出す必要性がありません。シングル ナンバー リーチでは、デュアルモード デバイスが登録されていない場合にのみ、ユーザの会社の電話番号への着信コールが公衆網のモビリティ ID 番号に転送されます。
- モバイル デバイスを配置するときには、モバイル デバイスが企業に接続されているかどうかにかかわらずユーザがダイヤリング手順を維持できるように、必要なダイヤル ストリングを正規化することを推奨します。モバイル ネットワークにおけるダイヤリングは通常、完全な E.164（先頭に「+」が付く場合と付かない場合がある）を使って行われ、携帯電話の連絡先は通常、完全な E.164 番号で保存されるため、完全な E.164 番号と、先頭に「+」を付けた完全な E.164 番号をモバイル クライアント デバイス用に使用できるよう企業のダイヤル プランを設定することを推奨します。このように企業のダイヤル プランを設定すると、ユーザはデバイスが Unified CM に登録されているかどうかを気にする必要がなくなるため、最善のエンド ユーザ ダイヤリング エクスペリエンスを提供できます。
- デュアルモード電話機のユーザが緊急コールを発信してデバイスやユーザの位置を特定するときには、モバイル ボイス ネットワークのみを使用させることを推奨します。その理由は、モバイル プロバイダー ネットワークが通常、WLAN ネットワークよりもはるかに信頼性の高い位置情報を提供するためです。デュアルモード電話機から緊急コールや位置サービスを利用するときにモバイル ボイス ネットワークだけが使用されるようにするには、Unified CM 内のデュアルモード デバイスの [緊急番号（Emergency Numbers）] フィールドを、911、999、112 などの緊急番号に設定し、これらのコールが強制的にモバイル ボイス ネットワーク経由で送信されるようにします。デュアルモード電話機のユーザに対して、すべての緊急コールを企業ネットワークではなくモバイル ボイス ネットワーク経由で発信するように指示します。企業の WLAN またはモバイル データ ネットワークを介して緊急コールを発信することは推奨されませんが、セルラー音声無線がないモバイル デバイスは、これらのデータ インターフェイスを介してのみ発信できます。セルラー音声無線がないモバイル デバイスを、緊急コールの発信用に使用すべきではありません。
- モバイル デバイス上に Cisco Jabber を配置するときには、次の配置ガイドラインを満たすよう WLAN ネットワークを設定してください。
  - WLAN のレイヤ 3 で Cisco Jabber モバイル クライアント デバイスのローミングを最小限に抑えます。デバイスの IP アドレスが変わるレイヤ 3 のローミングでは、ローミング時間が長くなり、音声パケットがドロップされ、コールがドロップされる場合もあります。
  - 最も高速な AP 間ローミングを確保するために、WLAN 内の Cisco Jabber モバイル クライアント デバイスで使用されるすべての AP に対して同一の SSID を設定します。
  - コール中に WLAN インフラストラクチャ内の他の AP に参加するように求められるとコールが中断されるおそれがあるので、これを防ぐために、会社のすべての WLAN AP が自身の SSID をブロードキャストするように設定します。

- モビリティ対応ユーザの BHCA レートに基づき、適切なコール キャパシティを処理できる適切な数のワイヤレス AP を配置することにより、シスコのモバイル クライアントおよびデバイス用に企業ワイヤレス ネットワークで十分なワイヤレス音声およびビデオ コール キャパシティを提供します。各 802.11g/n（2.4 GHz）または 802.11a/n/ac（5 GHz）チャネル セルは、24 Mbps 以上のデータ レートで最大 27 件の音声専用コールを同時にサポートできます。各 802.11g/n（2.4 GHz）または 802.11a/n/ac（5 GHz）チャネル セルは、最大 1 Mbps ビット レートでビデオ解像度 720p の場合、最大 8 件のビデオ コールを同時にサポートできます。2.4 GHz WLAN 配置では、このキャパシティを実現するには Bluetooth を無効にする必要があります。実際のコール キャパシティは、RF 環境、ワイヤレス エンドポイント タイプおよび WLAN インフラストラクチャに応じてさらに小さくなることがあります。
- Dial via Office Reverse（DVO-R）を配置するとき、ユーザ制御によるボイス メール回避方式を使用すると、受信側ユーザが発信側ユーザのボイス メールボックスに転送されなくなります。このボイス メール回避方式では、DVO-R コールを接続するために、発信側ユーザがモバイル デバイス キー パッドで番号を押す必要があります。モバイル デバイスのキーを押さない場合、DVO コールが消去されます。
- 代替コールバック番号を使用する DVO-R コールは会社に固定されていないため、デスクトップフォン ピック アップと DTMF ベースの通話切替機能をこれらのコールに使用することはできません。また、代替コールバック番号へのコールにはボイス メール回避が適用されません。
- WLAN からのセルラー デュアルモード ハンドオフ、LDAP ディレクトリ アクセス、ユーザ単位またはデバイス単位のアクセス制限、ネットワーク パス変更時のセッション永続性といった機能は、Expressway モバイルおよびリモート アクセス接続ではサポートされません。これらの機能のいずれかが必要な場合、Jabber モバイル クライアント用の Cisco AnyConnect VPN ソリューションの導入を検討してください。
- さまざまなモバイル デバイスのさまざまなシスコ モバイル クライアントがモバイル ユーザに提供される場合、モビリティ ID および追加的なリモート接続先が常に Cisco Jabber デュアル モード デバイス タイプに関連付けられる必要があります。
- モバイル デバイスを介して Cisco Spark アカウントを最初にダウンロード、インストールし、アクティブ化した後、ユーザは自分のアカウントのパスワードを作成するために Web ブラウザまたはデスクトップ クライアントを使って Cisco Spark にアクセスする必要があります。これが完了すると、ユーザは任意のクライアント（モバイル、デスクトップ、または Web ブラウザ）を使用して Cisco Spark にアクセスできるようになります。パスワードを設定しないと、サインアウトした後に毎回、ユーザは電子メールでアカウントを再アクティブ化しなければなりません。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。