



シスコが推奨する Webex Calling のための アーキテクチャ

設計概要

2022年8月

© 2022 Cisco Systems, Inc. All rights reserved.



目次

このユーザーガイドの更新内容	5
前書き	8
シスコ プリファード アーキテクチャに関するドキュメント	8
使用例	8
このマニュアルについて	8
概要	9
Webex Calling ソリューションの概要	9
サポートされるデバイス	9
ビデオ通話のサポート	10
アーキテクチャの概要	11
Webex Calling データセンター	12
アクセス接続オプション	12
OTT (オーバーザトップ) TLS 接続	12
Webex Edge Connect	12
プライベートネットワーク接続	13
PSTN アクセスとオンプレミスインターコネクト	13
複数の PSTN プロバイダー	14
トランクとルートグループ	15
ローカルゲートウェイの登録	17
専用または共存型のローカルゲートウェイ	18
パートナーがホストするローカルゲートウェイ	19
ローカルゲートウェイコールの設定	20
ダイヤルプラン	21
パターンとパターンマッチング	21
オンプレミスの呼制御システムによるインターコネクト	22
PSTN アクセス用のオンプレミストラंकとクラウド PSTN の組み合わせ	23
複数のオンプレミス呼制御インスタンス	24
コール ルーティングの概要	25
不明な番号の処理	26
トランクで Webex Calling に送信される ID	27
Webex Calling へのトランクコール	27
許可される中継コールと発信者 ID の選択	29
Webex Calling ユーザーからトランク経由で発信するコールの発信者 ID	29
サービスの相互作用	30
ビデオの考慮事項	31
メディアフロー	31
エンドポイントが同じロケーションにある場合と PSTN コールの場合のメディアフロー	31
Webex Calling のお客様間のコールのメディアフロー	32

Webex Calling のリージョン	33
導入のさまざまな側面.....	36
ロケーションの定義.....	36
緊急通報.....	36
ローカルゲートウェイの導入オプション.....	39
ローカルゲートウェイとしての CUBE ハイアベイラビリティ	40
ファイアウォールの要件.....	41
ICE メディアパスの最適化.....	44
候補の収集.....	46
候補の交換.....	47
接続の確認.....	48
メディアパスの最適化.....	50
ローカルゲートウェイ ICE Lite の実装	51
侵入防御システムの要件.....	52
コーデックの選択	53
帯域幅に関する考慮事項.....	54
ディレクトリ統合	56
ダイヤルプラン	57
PSTN 接続先	57
PSTN アクセスコード	57
短縮オンネットダイヤル	57
音声の統合	58
サービスアシュアランス.....	59
CScan.....	59
分析	59
トラブルシューティング	62
Control Hub のトラブルシューティングでサポートされるコールフロー.....	63
Webex Calling 専用インスタンス	64
専用インスタンス UC アプリケーション.....	64
専用インスタンスピアリング (接続)	65
専用インスタンス の PSTN オプション	68
ケーススタディ 1a : 集中型通話処理を行う Unified CM と複数の Webex Calling ロケーション.....	71
コールルーティングに関する考慮事項	74
Webex Calling から Unified CM へのコール.....	74
Unified CM から Webex Calling へのコール.....	77
サービスクラス (CoS)	78
Unified CM ダイヤルプランの統合	80
ローカルゲートウェイの導入	83
Webex Calling ダイヤルプランの設定.....	84

ケース スタディ 1b : 専用インスタンスを使用した Webex Calling	85
専用インスタンス通話フロー	85
お客様の拠点内通話	85
お客様の拠点間通話	86
専用インスタンスからの PSTN 通話	86
専用インスタンス エンドポイントからマルチテナント エンドポイントへの呼び出し	87
コールルーティングに関する考慮事項	88
モバイルおよびリモートアクセスに関する考慮事項	89
専用インスタンスのダイヤルプランに関する考慮事項	89

このユーザーガイドの更新内容

表 1 に、このガイドに追加された更新内容および新規トピックの履歴の一覧を示しています。

表 1 Webex Calling 向けシスコ プリファード アーキテクチャ発行履歴。

日付	更新または新規トピック	更新の詳細と場所
2020 年 7 月	ドキュメントの初公開	初回リリース
2021 年 4 月	ドキュメント全体	「Webex アプリ」のブランド商標変更。フィードバックに基づいた、スペルや文法などを修正するためのテキストや図の軽微な編集。
	オンプレミスベースの PSTN	オンプレミスのローカルゲートウェイを介した PSTN アクセスを指すためにドキュメント全体で 사용되는新しい用語
	Webex Calling リージョン データセンター	カナダの新しい Webex Calling データセンター（「 アーキテクチャの概要 」 > 「 アーキテクチャの概要 」 > 「 Webex Calling のリージョン 」）。
	シスコのコーリングプラン	追加の PSTN アクセスオプションとしての Cisco Calling プランの追加（「 アーキテクチャの概要 」 > 「 PSTN アクセス 」と「 オンプレミスインターコネクト 」）
	トランクとルートグループ	新しいセクション（「 アーキテクチャの概要 」 > 「 PSTN アクセスとオンプレミスインターコネクト 」 > 「 トランクとルートグループ 」）。 ローカルゲートウェイの導入設計ガイダンス（「 ケーススタディ 」 > 「 ローカルゲートウェイの導入 」）
	ダイヤルプラン	新しいセクション（「 アーキテクチャの概要 」 > 「 ダイヤルプラン 」）。 オンプレミスの呼制御を使用したインターコネクトのルーティング動作に関する説明を更新（「 アーキテクチャの概要 」 > 「 ダイヤルプラン 」 > 「 オンプレミスの呼制御システムによるインターコネクト 」）。 新しい導入オプションとしてのオンプレミスのトランクとクラウド PSTN の組み合わせ（「 アーキテクチャの概要 」 > 「 ダイヤルプラン 」 > 「 PSTN アクセス用のオンプレミストラंकとクラウド PSTN の組み合わせ 」）。 Webex Calling ダイヤルプランを使用したオンプレミスの呼制御へのルーティングの確立（「 展開の概要 」 > 「 ダイヤルプラン 」 > 「 短縮オンネットダイヤル 」）。 Webex Calling ダイヤルプランに基づく Webex Calling と Unified CM 間のコールルーティング（「 ケーススタディ 」 > 「 コールルーティングに関する考慮事項 」 > 「 Webex Calling から Unified CM へのコール 」） Webex Calling ダイヤルプラン設定のためのベストプラクティス（「 ケーススタディ 」 > 「 Webex Calling ダイヤルプランの設定 」）

日付	更新または新規トピック	更新の詳細と場所
	ローカルゲートウェイの同時コール	ローカルゲートウェイの同時コールのスケラビリティとネットワーク要件に関する設計ガイダンス (「導入の概要」 > 「ローカルゲートウェイの導入オプション」)。
	分析におけるコール詳細レコード	分析での CDR の可用性 (「導入の概要」 > 「サービスアシュアランス」 > 「分析」)
	Cloud Connected PSTN とオンプレミスペースの PSTN の組み合わせ	Cloud Connected PSTN とオンプレミスペースの PSTN の組み合わせをオプションとして追加 (「ケーススタディ：集中型呼処理と複数の Webex Calling ロケーション」)
	Unified CM から Webex Calling へのコールの着信側の番号の形式	Unified CM から Webex Calling へのコールの着信側番号形式オプションの明確化 (「ケーススタディ」 > 「コールルーティングに関する考慮事項」 > 「Unified CM から Webex Calling へのコール」)
2021 年 10 月	ICE メディアパスの最適化	最適化されたメディアパスに関する言及 (「アーキテクチャの概要」 > 「メディアフロー」 > 「アーキテクチャの概要」 > 「Webex Calling のリージョン」)
	東京と大阪のロケーション	データセンターマップの更新 (「アーキテクチャの概要」 、 「アーキテクチャの概要」 > 「Webex Calling のリージョン」)
	Webex のブランド変更	ドキュメント全体
	Opus コーデックのビットレート	コールごとの帯域幅を 70 kbps から 40 kbps に変更
	コールルーティングフロー	Webex Calling コールルーティングフローに関する説明 (「アーキテクチャの概要」 > 「ダイヤルプラン」 > 「コールルーティングの概要」)
	ロケーションコードのない ESN 発信者 ID	ロケーションプレフィックスが設定されていない場合の ESN 発信者 ID 形式に関する説明 (「アーキテクチャの概要 (Overview)」 > 「ダイヤルプラン」 > 「許可された中継コールと発信者 ID の選択」 、表 5)
	オンプレミスから Webex Calling への + E.164 の発信者 ID に関する説明	スクリーニングサービスが機能するには、発信者 ID が + E.164 形式である必要があります。 (「アーキテクチャの概要」 > 「ダイヤルプラン」 > 「Webex Calling へのトランクコール」)
	トランクが機能するために必要なロケーションのメイン番号	トランクを機能させるには、ロケーションのメイン番号を設定する必要があります (「アーキテクチャの概要」 > 「ダイヤルプラン」 > 「オンプレミス呼制御を使用したインターコネクト」)。
	設定可能なデュアルアイデンティティサポート	設定可能なデュアルアイデンティティサポートによる発信者 ID の処理 (「アーキテクチャの概要」 > 「ダイヤルプラン」 > 「Webex Calling へのトランクコール」 、 「アーキテクチャの概要」 > 「ダイヤルプラン」 > 「許可される中継コールと発信者 ID の選択」 、表 5)
2022 年 8 月	専用インスタンス	ネットワーク接続、PSTN オプション、ディレクトリ統合、ケーススタディ。

日付	更新または新規トピック	更新の詳細と場所
	トランク発信者 ID 形式の要件	トランク上の Webex Calling に送信される発信者 ID 形式 (+E.164、ESN、または内線番号) 要件の明確化 (トランクで Webex Calling に送信される ID)
	トランクから ESN/内線番号への通話	内線番号または ESN への通話を成功させるために前提条件の明確化 (許可される中継コールと発信者 ID の選択)
	緊急通報	緊急通報セクション を更新し、CCP 緊急通報と拡張緊急通報の両方を記載しました。
	詳細な通話履歴、Webex Calling 通話のトラブルシューティング	詳細な通話履歴、トラブルシューティング (展開側面 > サービスアシュアランス > 分析)
	シンガポールのロケーション	データセンターマップの更新 (アーキテクチャの概要 > Webex Calling 地域)
	ビデオの考慮事項	ビデオ通話デバイス、コーデックおよび帯域幅の考慮事項を記載しました。

前書き

シスコ プリファード アーキテクチャは、特定の市場セグメント向けに、一般的なユースケースに基づく推奨導入モデルを提供します。この推奨導入モデルは、シスコ コラボレーション ポートフォリオの全製品のうち、ターゲットとする市場セグメントと定義したユースケースに最も適した製品で構成されています。すぐに使える規範的な導入モデルであり、組織とそのビジネスニーズの変化に対応できる拡張性が備わっています。この規範的なアプローチを採用すれば、システムレベルで複数のコンポーネントを簡単に統合し、個々の組織のビジネスニーズに最も適した導入モデルを選択できます。

シスコ プリファード アーキテクチャに関するドキュメント

- [シスコ プリファード アーキテクチャ \(PA\) 設計概要ガイド](#)：お客様とセールsteamが組織のビジネス要件に基づいて適切なアーキテクチャを選択し、アーキテクチャで使用されている製品について理解するうえで役立ちます。また、設計上の一般的なベストプラクティスを把握できます。このガイドはセールス プロセスをサポートします。
- [Cisco Validated Design \(CVD\) ガイド](#)：シスコ プリファード アーキテクチャを構成するコンポーネントの導入手順を詳しく説明しています。このガイドは PDI (計画、導入、実装) をサポートします。
- [シスコ コラボレーション ソリューション リファレンス ネットワーク デザイン \(SRND\) ガイド](#)：シスコ コラボレーションの設計上のオプションについて詳しく説明しています。設計要件がシスコ プリファード アーキテクチャの対象範囲外である場合は、このガイドを参照してください。

使用例

この Webex Calling 向けシスコ プリファード アーキテクチャ (PA) ドキュメントでは、電話インフラ全体を置き換えることなく組織を成長させていく方法について説明します。また、ユースケースとして、以下のコールルーティングに関する考慮事項についても詳しく取り上げます。

- Webex Calling と専用インスタンス間の通話
- Webex Calling とオンプレミスの Unified CM 間の通話
- サービスクラス (CoS)
- ダイヤルプランの統合

シスコ コラボレーション テクノロジーに関する情報とこのドキュメントで取り扱っていないユースケースについては、[Cisco.com](#) をご覧ください。

このマニュアルについて

「Webex Calling のシスコ優先アーキテクチャ」には、Webex Calling のアーキテクチャに関するガイダンスが記載されています。具体的には、クラウドベースの呼制御システムとして Webex Calling を個別展開する場合と、エンタープライズ向けプリファード アーキテクチャドキュメントに記載されているオンプレミスのコラボレーション ソリューションと組み合わせて Webex Calling を展開する方法について説明します。

本書では特に明記しない限り、「Webex Calling」とは、常に Webex Calling マルチテナントのことを指します。Webex Calling マルチテナントと Unified CM の統合に関する設計ガイダンスは、マルチテナントと専用インスタンス間の統合にも適用されます。

オンプレミスの Unified CM ではなく、専用インスタンスにのみ適用される詳細については、新しいセクションが追加されています。

このガイドの読者は、シスコの音声、ビデオ、コラボレーション製品についての一般的な知識を持ち、これらの製品の導入方法についての基礎を理解している必要があります。

このガイドでは、設計と販売のプロセスをシンプルにするために次の内容について取り上げます。

- エンタープライズ向けに構築され、エンタープライズ市場に適した一連の機能を提供する製品をシスコ コラボレーション ポートフォリオの中から推奨
- コラボレーション アーキテクチャの詳細な説明と、エンタープライズ組織に導入する際の一般的なベストプラクティスを特定

コラボレーション アーキテクチャの設定、導入、実装の詳細については、[コラボレーションのためのデザインゾーン](#)に掲載されている関連 CVD ドキュメントを参照してください。

概要

Webex Calling ソリューションの概要

エンタープライズレベルの組織の意思決定者は、オンプレミスの構内交換機 (PBX) の設置、セキュリティの確保、保守が複雑でコストがかかることを認識しています。追加の機能が開発されると、すでに組織内に展開している PBX システムは古くなり、セキュリティが低下しがちです。

Webex Calling の登場以前にクラウドベースで提供されていた PBX ソリューションは、機能、性能、セキュリティが不十分なため、エンタープライズの PBX や PBX ネットワークを置き換えることはできませんでした。

Webex Calling は、モジュラー型のインテリジェントな統合チーム コラボレーション スイートの一部です。Webex Calling は、かつてオンプレミスの PBX ネットワークでしか実現できなかったエンタープライズクラスの PBX 機能と性能を提供します。ライセンスはサブスクリプションで提供され、Cisco Collaboration Flex Plan を通じて管理されます。このソリューションは Webex、具体的に言うと Webex デバイスと統合されています。また、オプションとして Webex Meetings と Webex Contact Center との統合も可能です。

Webex Calling はクラウドのみのソリューションとして、あるいは、クラウドとオンプレミスの PBX が混在するネットワークが必要な場合はハイブリッドクラウドの一部として導入されます。

Webex Calling データセンターはグローバルに分散していて、各地のデータセンターは地理的に冗長化されています。Webex Calling の販売は、シスコ付加価値リセラー (VAR) チャンネルパートナーが行います。


専用インスタンス：専用インスタンスオプションは、Webex Calling 内の資格であり、単一のお客様専用のプライベートクラウドで、Cisco Unified Communications Manager ベースのアプリケーションスタックを提供します。

エンタープライズクラスの PBX 機能のほか、Webex Calling には次の機能と特長があります。

- Webex Calling グループ機能 (自動アテンダント、ハントグループ、コールキューなどの無制限サブスクリプション)
- 通話中機能、またはユーザーのデスクフォンの制御を使用するソフトクライアント用の Webex アプリ内からの統合通話
- Webex アプリ (メッセージング、画面共有、音声会議、ビデオ会議に対応)
- オプションで Webex Meetings を追加可能 (会議室の録画、会議室のロック、PSTN 経由のリモートダイヤルイン アクセス、最大 1000 人まで参加可能な会議など、高度な会議エクスペリエンスを実現)
- シスコ マルチプラットフォーム フォン (MPP) のすべてのモデルを展開する機能、対応デバイスのリストは <https://help.webex.com/en-US/article/qkwt4j/Supported-Devices-for-Webex-Calling> でご確認ください。
- 公衆電話交換網 (PSTN) へのアクセス

サポートされるデバイス

Webex Calling には、組織やエンドユーザーの要件に基づいた様々なユーザーインターフェイスがあります。Webex Calling は、幅広い Cisco MPP シリーズ IP 電話 (6800、7800、および 8800 シリーズ)、Webex デバイス、およびさまざまなサードパーティデバイスに対応しています。組織で使用するデフォルトの通話アプリケーションは管理者が選択しますが、必要に応じて個人ユーザーが他のアプリケーションを使用できるように設定することも可能です。ソフトウェア オプションには、完全なミーティング機能を備えた、メッセージング、画面、およびファイル共有を備えた Webex アプリが含まれます。詳細については、「<https://help.webex.com/en-us/article/qkwt4j>」を参照してください。優先アーキテクチャの設計詳細については



Webex アプリは、一般的に使用される通話中機能、MPP でのリッチプレゼンス、各ユーザーの単一回線をサポートします。また、ユーザーの Cisco MPP 電話機を操作することもできます。シスコのエンドユーザ向けヘッドセット製品は、MPP デバイスに接続されている場合でも、ユーザのワークステーションや携帯電話に接続されている場合でもサポートされます。これらのシスコソフトウェアオプションに加え、Webex Calling ユーザーは、Microsoft Teams 内から Webex Calling サービスを使用できるように設定できます。この統合については、「<https://help.webex.com/en-us/article/nqmx08cb>」を参照してください。

ビデオ通話のサポート

Webex Calling は、次のエンドポイントとアプリ間のビデオ通話をサポートしています。

- ビデオ対応 MPP 電話機 (8845、8865、8875)
- Webex Devices
- Webex Calling でユーザーが使用できるように設定されている場合は、Webex アプリ (デスクトップとモバイル)

ユーザーは、ビデオ対応電話機で適切に構成されたソフトキーを使用して、SIP アドレスでスピードダイヤルで Webex ミーティングに通話できます。(例：ユーザーのパーソナル会議室) 共有モードの Webex デバイスの場合、それらをクラウドに登録してから、Webex Calling PSTN サービスをワークスペースに追加できます。

アーキテクチャの概要

Webex Calling は、地理的に分散した複数ロケーションにある Webex データセンターでホストされるエンタープライズ向けクラウド通話ソリューションです。

図 1 世界中に分散されたデータセンター



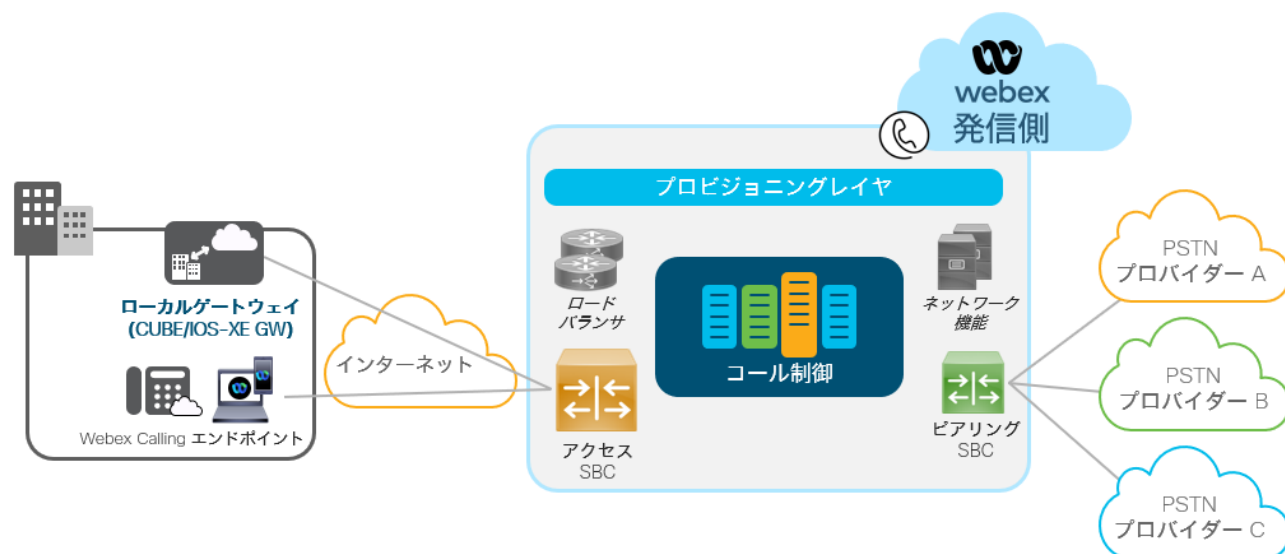
Webex Calling は世界中で利用可能で、米国 (ダラス、シカゴ)、カナダ (バンクーバー、トロント)、ヨーロッパ (フランクフルト、アムステルダム)、英国 (ロンドンの冗長データセンター)、オーストラリア (メルボルン、シドニー)、日本 (東京、大阪) の 6 つのリージョンの冗長データセンターから配信されます。ニューヨークとシンガポールのデータセンターは、メディアの往復時間を最適化するメディアサービスを提供します。シンガポールデータセンターは、オーストラリアまたは日本のリージョンへの往復時間が最適ではない可能性があるアジア諸国の Webex Calling のお客様のメディア往復時間を最適化するために特に使用されます。これらのデータセンターは完全冗長構成になっており、マルチギガビットのバックボーン回線で相互接続されています。

Webex Calling では、シグナリングに SIP、メディアに SRTP を使用しています。IP 電話とローカルゲートウェイの IP アドレスにはダイナミック NAT を使用できます。電話機とローカルゲートウェイが Webex Calling への TLS 接続を開始し、Webex Calling がそれを認証します。Webex Calling は同一のコネクションを使用して IP 電話またはローカルゲートウェイにトラフィックを送り返すため、ファイアウォールを通過できます。

Webex Calling データセンター

各地の Webex Calling データセンターではコールルーティング機能をホストし、Webex Calling へのプロビジョニングインターフェイスへのアクセスを提供しています。

図 2 Webex Calling の機能の要素



データセンターは、アクセス SBC (セッション ボーダー コントローラ) とピアリング SBC もホストします。アクセス SBC は、ローカルゲートウェイ、エンドポイント、ソフトクライアントからのお客様側のすべての SIP 接続を終端し、ピアリング SBC は SIP サービスプロバイダーとの SIP ピアリング接続を終端します。

ロードバランサやその他のネットワーク機能は、拡張性があり、冗長化されたデータセンター アーキテクチャの構築に必要で、Webex Calling データセンターの一部でもあります。

アクセス接続オプション

十分な帯域幅を備えた信頼性の高いネットワーク接続は、Webex Calling を使用するすべての音声およびビデオ対応エンドポイント、クライアント、およびアプリケーションに対してエンドツーエンドで最高のユーザー体験を確保するための基本要件です。

お客様とパートナーには、Webex Calling への接続を最適化できるオーバーザトップ (OTT) インターネット以上のアクセス接続オプションがあり、これらには Webex Edge Connect または Private Network Connect が含まれます。

OTT (オーバーザトップ) TLS 接続

お客様のネットワーク上の Webex Calling エンドポイントは、インターネットを経由して Webex Calling データセンターに接続し、OTT (オーバーザトップ) TLS 接続を確立します。

Webex Edge Connect

Webex Edge Connect は、Webex ミーティングと Webex Calling トラフィックを Equinix Cloud Exchange (ECX) ロケーションとピアリングするソリューションです。このピアリングは、保証された帯域幅と Quality of Service (QoS) を提供することにより、通話とミーティングのユーザーエクスペリエンスを向上させ、ネットワークの待ち時間、パケット損失、およびジッターを最小限に抑えます。設計詳細については、Webex Edge Connect 優先アーキテクチャ

「https://www.cisco.com/c/dam/en/us/td/docs/solutions/PA/EdgeConnect/PA_Edge_Connect_Design.pdf」を参照してください。

プライベートネットワーク接続

プライベートネットワーク接続 (PNC) ソリューションにより、Webex Calling のお客様はプライベートネットワークをクラウドに拡張できます。これは、パートナークラウドまたは直接接続のいずれかを介して実行され、高品質のサービスと音声通話の低遅延を保証します。プライベートネットワーク接続の設計ガイドラインについては、Webex Calling 優先アーキテクチャの「プライベートネットワーク接続」:

<https://www.cisco.com/c/dam/en/us/td/docs/solutions/CVD/Collaboration/cloud/PA-PNC.pdf> を参照してください。

図3 Webex Calling エンドポイントとデータセンター間の OTT (オーバーザトップ) 接続



PSTN アクセスとオンプレミスインターコネクト

Webex Calling は、Cisco Calling Plan、Cloud Connected PSTN、およびオンプレミスベースの PSTN の 3 つの方法で PSTN にアクセスできます。

- Cisco Calling プラン (Cisco PSTN)

Cisco PSTN を使用すると、パートナーはシスコが提供する PSTN オプションを顧客に販売し、包括的なコラボレーションソリューションの購入プロセス全体を簡素化できます。Cisco PSTN を使用すると、番号オーダーとポートのオーダーは、Control Hub 内から開始できます。

- Cloud Connected PSTN (CCP)

シスコは、一部の Cloud Connected PSTN プロバイダーとの共有された SIP 接続を統合しています。Webex Calling では、お客様に任意の Cloud Connected PSTN プロバイダーを選択して直接ご契約いただくから、Webex Control Hub でその Cloud Connected PSTN プロバイダーを選択して PSTN にコールをルーティングします。

- オンプレミスベースの PSTN

Cisco Voice Gateway または Cisco Unified Border Element (CUBE) で実行されているローカルゲートウェイ機能は、既存のエンタープライズ PSTN 接続を利用して、オンプレミスリソースを含む Webex Calling と PSTN 間の通話をルーティングします。通常、ローカルゲートウェイ機能はお客様のオンプレミス環境に導入されますが、パートナーがホストする場合もあります。ローカルゲートウェイは Webex Calling に登録され、PSTN と Webex Calling 間のコールを処理します。オンプレミスベースの PSTN では、複数のトランクを持つトランクまたはルートグループが Webex Control Hub で PSTN の選択肢として選択されている必要があります。各トランクは、ローカルゲートウェイへの接続を表します。

図 4 CCP とローカルゲートウェイ経由の PSTN アクセス

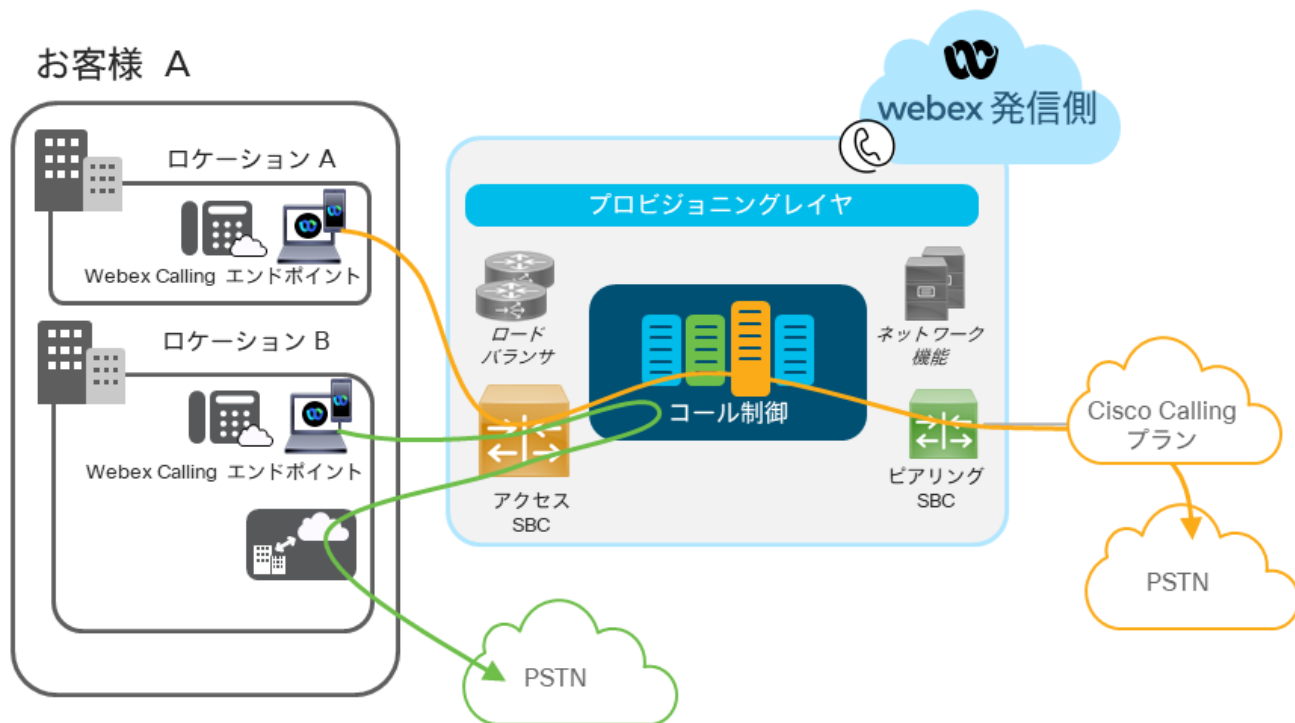


図 4 は、PSTN タイプ（Cisco Calling プラン、Cloud Connected PSTN、またはオンプレミスベースの PSTN）の選択をロケーションごとに設定できることを示しています。ロケーション A のデバイスは PSTN アクセス用の Cisco Calling プランを使用しますが、ロケーション B のデバイスではローカルゲートウェイへのトランクを使用します。クラウド接続された PSTN は図に示されていません。

PSTN アクセスの提供に加え、ローカルゲートウェイは Webex Calling をオンプレミスの呼制御インスタンスに接続することもできます。これを実現するには、ローカルゲートウェイをオンプレミスの呼制御インスタンスに SIP 経由で接続する必要があります。

異なる Webex Calling 顧客間のコールは、法的要件を満たすために、設定された PSTN の選択（Cisco Calling プラン、Cloud Connected PSTN、またはオンプレミスベース PSTN）を介して常に PSTN 経由でルーティングされます。

複数の PSTN プロバイダー

Webex Calling のお客様は、PSTN アクセス用の単一の Cloud Connected PSTN プロバイダーまたは Cisco Calling Plan を使用できるわけではありません。複数の国で展開する場合や料金体系、地理的なプレゼンスを考慮し、それぞれの Webex Calling ロケーションで個別に Cloud Connected PSTN プロバイダーを選択することも可能です。

図 5 複数の PSTN プロバイダー

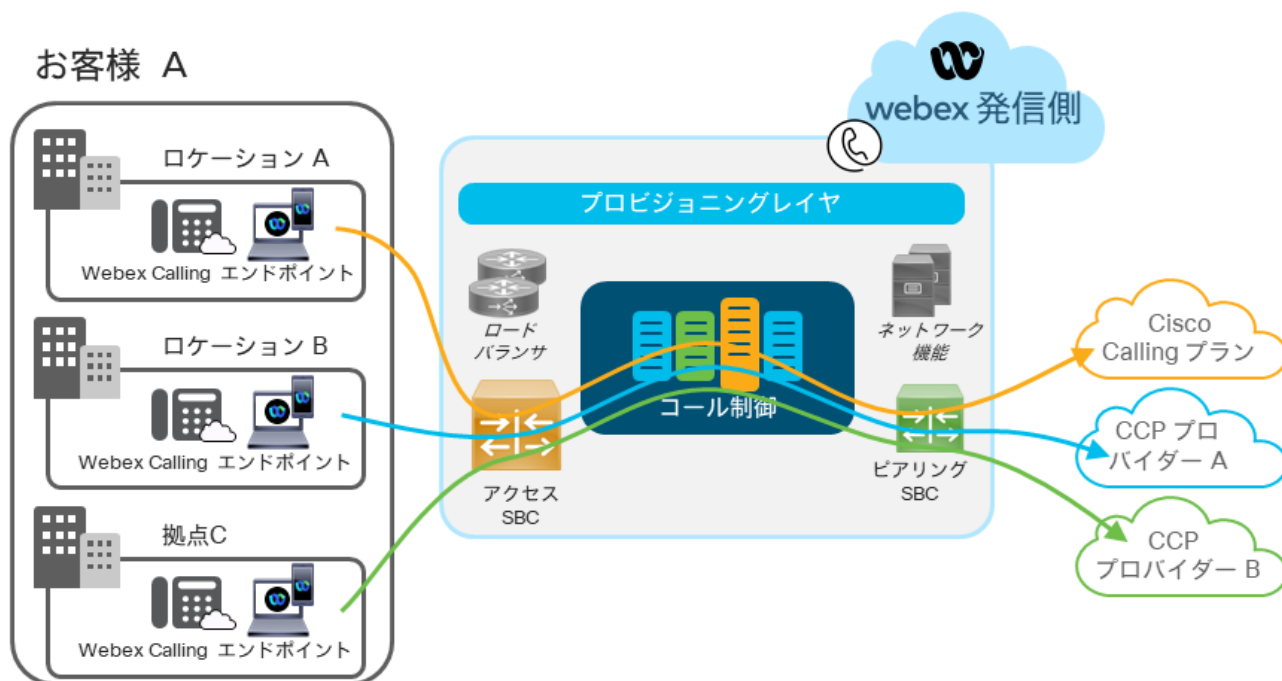


図 5 は、各ロケーションで異なる PSTN を選択して使用する例を示しています。ロケーション A の PSTN サービスは Cisco Calling Plan を使用して提供されますが、ロケーション B と C には 2 つの異なるクラウド接続 PSTN プロバイダーが使用されます。特定のコールに使用される PSTN の選択は、Webex Calling コールの発信元（ロケーション）によって異なります。着信側アドレスといった通話に関連するその他の属性は、PSTN の選択に影響しません。

トランクとルートグループ

トランクは、ローカルゲートウェイを使用して Webex Calling を接続するか、ソリューションに含まれている場合は専用インスタンスに接続します。Control Hub の各トランクは、CUBE（または Cisco Voice Gateway）で設定された 1 つのローカルゲートウェイ インスタンスへのトランクを表します。各 CUBE は、顧客のオンプレミス内またはパートナーデータセンターに配置できます。各トランクはロケーションに割り当てる必要があります。複数のトランクを 1 つのルートグループにグループ化して、冗長性を確保したり、キャパシティを増やしたりすることができます。各トランクは複数のルートグループに属することができます。ルートグループとトランクは、PSTN コールまたはオンプレミスコールの宛先として使用できます。

ルーティングの選択肢としてルートグループを使用することは、ルートグループに 1 つのトランクしか含まれていない場合でも、単一のトランクを使用するよりも優先されます。あらゆる場所でルートグループを使用すると、特定のルートが使用されているすべての場所を更新することなく、ルートグループにトランクを追加するだけで、後でキャパシティまたは冗長性を追加できます。

[ダイヤルプラン (Dial Plan)] セクションには、Webex コールルーティングの選択肢に関する詳細が示されます。

図 6 スケールと冗長性に対応するルートグループ

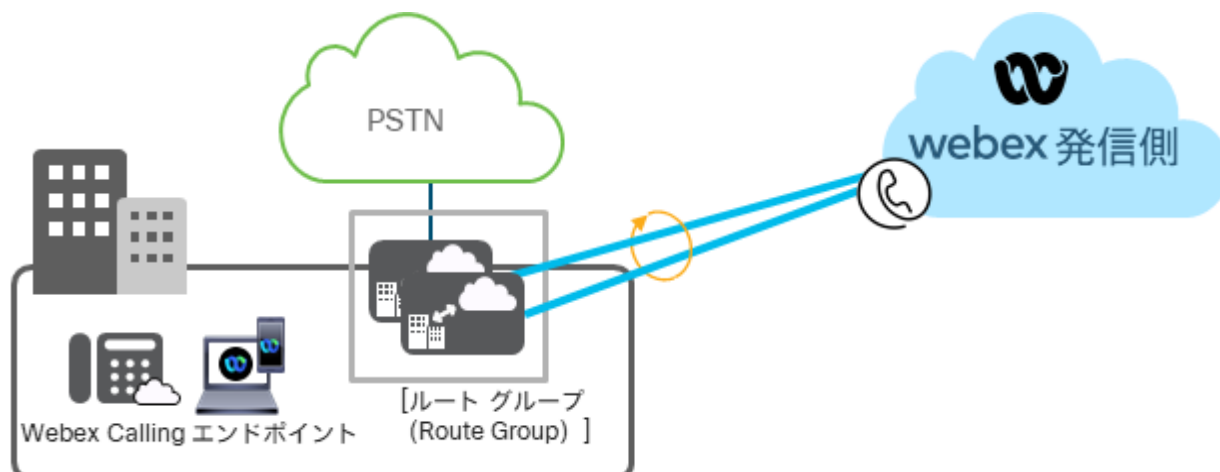


図 6 は、同じロケーションにある 2 つのローカルゲートウェイへのトランクが、そのロケーションのオンプレミスペースの PSTN の選択として設定された 1 つのルートグループに結合される例を示しています。

優先順位は、ルートグループ内の各トランクに割り当てられます。コールがルートグループに送信されると、これらのコールは最も高い優先度（1 = 最高の優先順位）を持つすべてのトランクの中からランダムに分散されます。優先度が最も高いすべてのトランクに対して再ルーティングが行われた場合、コールが正常にルーティングされるか、またはルートグループ内のすべてのトランクが成功せずに試行されるまで、トランクの選択は次に低い優先度のトランクへ続行されます。優先順位が最も高いすべてのトランクに対して再ルーティングが行われた場合、コールが正常にルーティングされるか、またはルートグループ内のすべてのトランクが成功せずに試行されるまで、トランクの選択は次に優先度の低いトランクへ続行されます。

再ルーティングは次の理由によってトリガーされます。

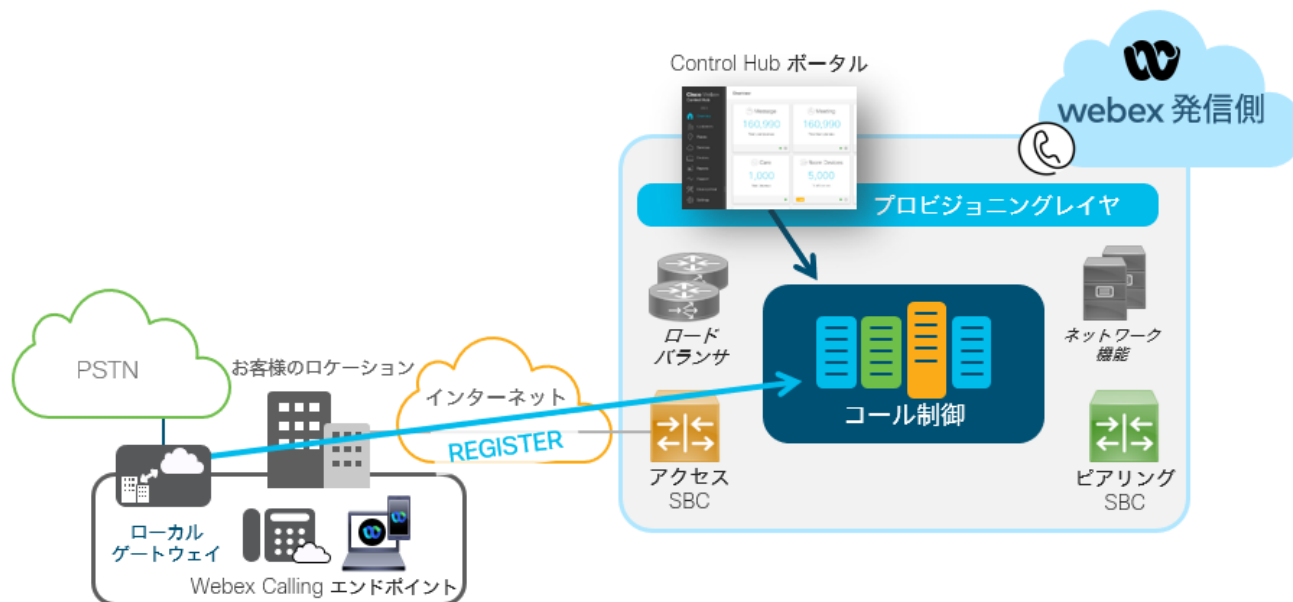
- SIP 応答 401、470、480、および 606（18x 応答を受信する前）
- 403、404、410、413、484、および 486 を除くその他すべての 4xx SIP 応答
- すべての 5xx SIP 応答
- SIP タイムアウト（12 秒）

ロケーションごとに最大 100 のトランクを使用できます。ルートグループには最大 10 のトランクを含めることができ、Webex Calling のお客様には最大 10,000 のルートグループを設定できます。

ローカルゲートウェイの登録

ローカルゲートウェイは、Webex Calling への接続に、認証と登録ベースの SIP トランクを使用します。

図7 ローカルゲートウェイの登録



Webex Control Hub は、トランクのプロビジョニングプロセスの一部として、SIP 認証の接続パラメータとダイジェストクレデンシャルを提供します。

この SIP/TLS (SIPS) 接続は、お客様のネットワーク（エンドポイントとローカルゲートウェイ）から Webex Calling に対してのみ開始されます。企業と Webex Calling 間の SIPS 接続は外部方向のみであるため、企業のファイアウォールで内部方向への接続を設定する必要はありません。

この展開は、「登録ベースのトランク」と呼ばれます。「証明書ベースのトランク」などの他のオプションについては、このドキュメントでは説明していません。

専用または共存型のローカルゲートウェイ

ローカルゲートウェイは、同一筐体に PSTN トランク（TDM または IP）を終端して PSTN に直接接続するか、SIP トランクを介して既存の PSTN ゲートウェイに接続します。

図 8 ローカルゲートウェイの展開オプション

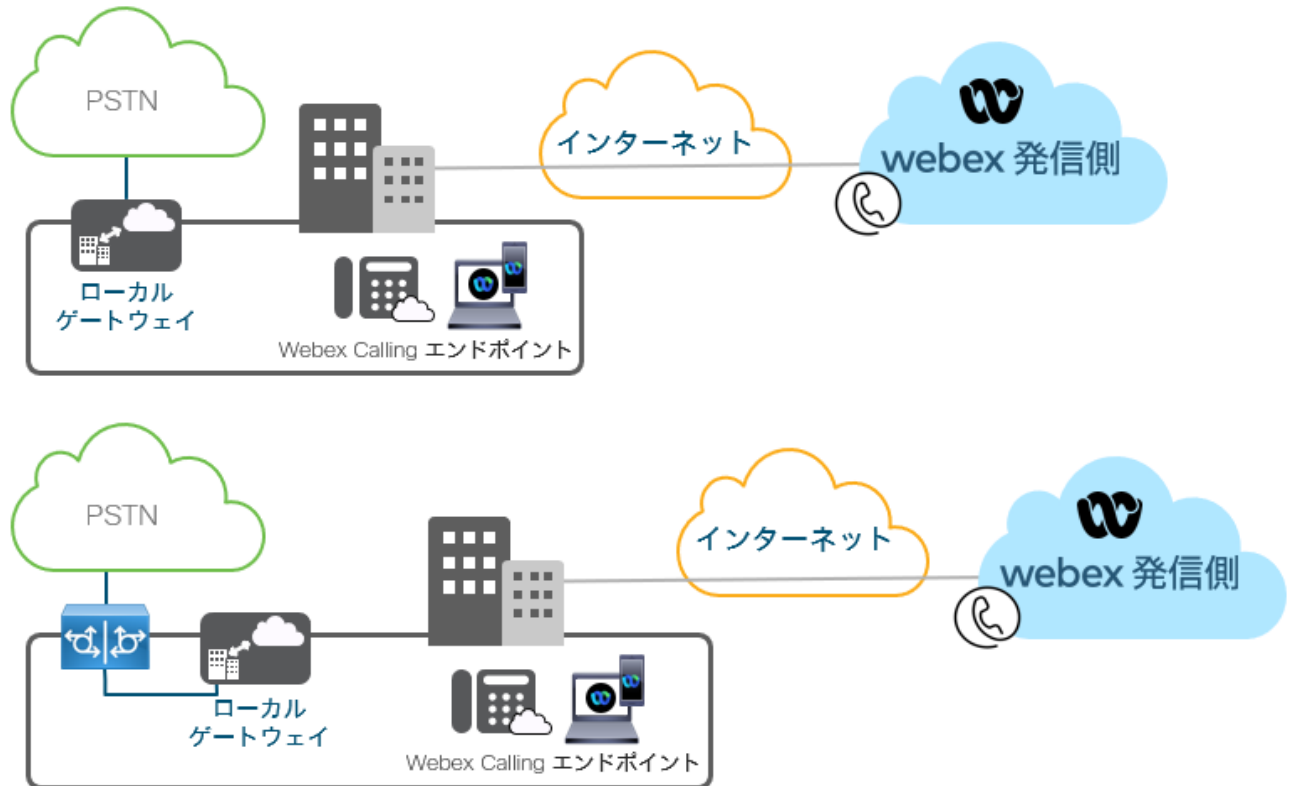


図 8 では両方のオプションを示しています。PSTN アクセスと Webex Calling への接続を組み合わせることで、お客様のネットワークに設置して保守する必要があるハードウェアの数は少なくなります。Webex Calling に移行した後に既存の PSTN ゲートウェイを引き続き使用する場合は、それぞれの機能を別々のデバイスに実装することを推奨します。

パートナーがホストするローカルゲートウェイ

パートナーは、それぞれのお客様のネットワークに個別のローカルゲートウェイを導入する代わりに、パートナーのデータセンターでお客様のローカルゲートウェイをホストすることもできます。

図 9 ホストするローカルゲートウェイ



図 9 は、この例の場合、パートナーのデータセンターに個別のローカルゲートウェイを導入する必要がないことを示しています。個々のお客様のダイヤルピアベースのコールルーティング設定は、1つの CUBE で組み合わせることができます。お客様間のトラフィックの分離は、ダイヤルピアルーティングと音声クラステナントを適切に設定することで実現されます。ローカルゲートウェイ構成ガイド (<https://help.webex.com/ja-jp/jr1i3r/>) に、ダイヤルピアのマッチングの設定方法が記載されています。この設定により、ローカルゲートウェイで、Webex Calling からの受信コールをお客様固有の PSTN トランクにマッピングしたり、発信コールをマッピングをしたりすることができます。複数の仮想ルーティング機能 (VRF) を導入する必要はありません。シグナリングとメディアが両方ともクラウドの Webex Calling のアクセス SBC に固定されているため、パートナーのデータセンターとお客様のネットワーク間の直接 IP 接続は不要です。この導入モデルにより、パートナーは、さまざまなお客様のローカルゲートウェイをより効率的に導入、保守、運用することができます。

この導入モデルでは、パートナーのデータセンターとお客様のネットワーク間のデータ接続は必要ありません。お客様ごとに個別に Webex Calling への登録を行うことで、組み合わせられたローカルゲートウェイ上で異なるお客様のコールを簡単に識別できるため、お客様間の漏話を回避できます。

ローカルゲートウェイとお客様のネットワーク間の IP 接続

音声メディアストリームには、ローカルゲートウェイ、オンプレミスの呼制御システム、関連するエンドポイント間の IP 接続が必要です。

Webex Calling を既存のオンプレミス呼制御システムに接続するローカルゲートウェイ (次のセクションを参照) では、ローカルゲートウェイとオンプレミスの呼制御システム (およびオンプレミスの呼制御システムによって制御されるエンドポイント) 間の音声メディアストリームを有効にするために、ローカルゲートウェイとお客様のネットワーク間の IP 接続が必要です。

パートナーのデータセンターにローカルゲートウェイを導入する場合は、お客様のネットワークをパートナーのデータセンターに拡張する必要があります。ローカルゲートウェイ機能が共有プラットフォームに実装されている場合、ネットワーク分離は、VRF 設定などのネットワーク仮想化メカニズムによって実現されます。こうした複雑なローカルゲートウェイ設定の場合、オーバーヘッドが増え、保守に時間がかかるだけでなく、ネットワークセキュリティの懸念も高まるため、Webex Calling の複数のお客様間で単一のローカルゲートウェイプラットフォームを共有するメリットが失われる可能性があります。オンプレミスの呼制御システムへの接続が必要な場合は、専用のオンプレミス ローカルゲートウェイを展開する方がより効率的な展開オプションになる可能性があります。

ローカルゲートウェイコールの設定

図 10 SIP/TLS 接続の設定フロー

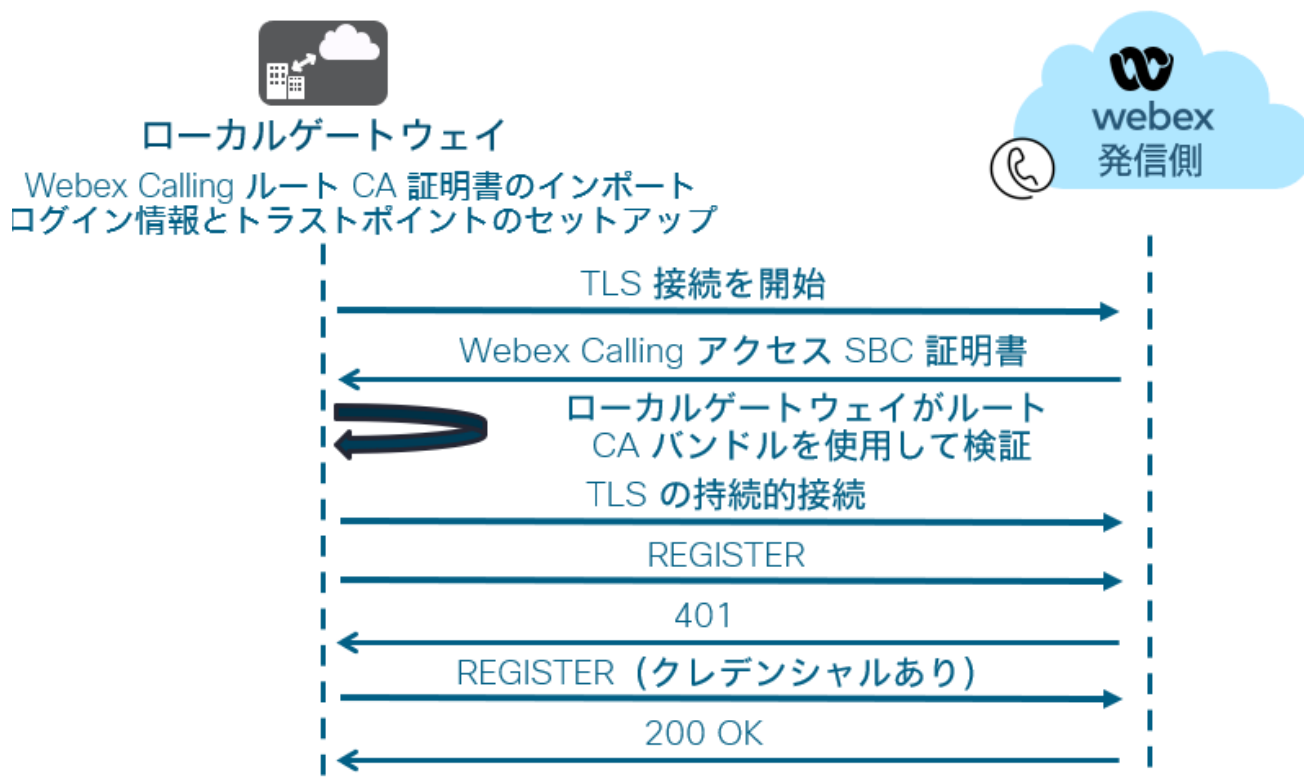


図 10 は、SIPS 接続設定の詳細なフローを示しています。ローカルゲートウェイのプロビジョニングプロセスの一部として、Cisco Trusted Core Root Bundle がインストールされます。バンドルには、一連のパブリック CA トラストアンカーが含まれています。Control Hub から取得したダイジェストクレデンシャルは、ローカルゲートウェイでもプロビジョニングされます。

ローカルゲートウェイは、ドメインネームシステム (DNS) への SRV クエリを開始して、ローカルゲートウェイプロビジョニングプロセス中に Control Hub で取得した SRV ドメインに基づいてアウトバウンドプロキシドメインネームシステム (DNS) A レコード、TCP ポート、優先度および重みを取得します。冗長性のために、複数のレコードが返されます。ローカルゲートウェイは、ドメインネームシステム (DNS) から返された優先度が最も高い (優先度の値が最も小さい番号) ゲートウェイを選択し、続いてドメインネームシステム (DNS) A レコードクエリを送信して、Webex Calling Access SBC の IP アドレスを決定します。TLS 接続の設定中、ローカルゲートウェイは、提示された証明書をルート CA バンドルで検証することにより、Webex Calling のアクセス SBC の真正性を確認します。

Webex 側では、SIP 登録時に提示されたダイジェストログイン情報に基づいてローカルゲートウェイが認証されます。

ローカルゲートウェイの接続と安全な登録は、RFC3261 に準拠しています。持続的な TLS 接続が SIP のトランスポート層として確立されると、ローカルゲートウェイは、SIP 登録をアクセス SBC に送信します。最初の REGISTER メッセージは SIP ダイジェストクレデンシャルなしで送信され、アクセス SBC は登録を拒否します。このとき、認証が必要であることを示す SIP 応答 401 が返されます。401 応答を受信すると、ローカルゲートウェイは別の REGISTER メッセージを送信します。このメッセージには、ローカルゲートウェイの SIP ダイジェストクレデンシャルに基づく必要な認証情報が含まれています。

PSTN プロバイダーは通常、ビデオ通話をサポートしていません。通話設定の失敗を回避するには、<https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/voice/cube/configuration/cube-book/voi-audio-forced.html> で記載されているように、ローカルゲートウェイでビデオ抑制機能を構成することをお勧めします。

ダイヤルプラン

ダイヤルプランでは、ダイヤルプラン内のダイヤルパターンとの一致に基づいて、オンプレミス内ベースの呼制御インスタンスにコールをルーティングする機能、または複数のオンプレミスベースの呼制御インスタンス間でコールをルーティングする機能を追加しています。各ダイヤルプランには最大 10,000 のパターンを設定でき、カスタマーごとに最大 10,000 のダイヤルプランを設定できます。各ダイヤルプランのルーティングの選択肢は、トランクまたはルートグループとなります。宛先がダイヤルプランのパターンに一致するたびに、それぞれのコールが、ダイヤルプランのルーティングの選択肢として選択されたトランクまたはルートグループに送信されます。前述のように、個々のトランクではなくルートグループをルーティングの選択肢として常に使用すると、後でキャパシティや冗長性を簡単に追加できます。

ダイヤルプランは企業に対してグローバルに定義され、ロケーションに関係なくすべてのユーザーに適用されます。ダイヤルプランで定義されるルートを選択は、すべてのユーザーに対して同じです。

パターンとパターンマッチング

数字のパターンは、E.164 番号または企業番号または内線番号のいずれかを表すことができます。E.164 番号のパターンは、先頭に「+」が付き、その後「1」～「9」の一連の数字が続き、最後にオプションのワイルドカード文字が続きます。エンタープライズ番号のパターンは、「1」～「9」の一連の数字と、それに続くオプションのワイルドカード文字で表されます。有効なワイルドカード文字は「!」と「X」のみで、「!」は任意の数字列に一致し、「X」は「0」～「9」の 1 桁の数字に一致します。ワイルドカードの「!」は、E.164 パターンでのみ最後に 1 回だけ利用できます。たとえば、「+ 496100773!」では、「6100773」で始まるドイツのすべての国内番号 (国コード 49) と一致します。84969XXX では、「84969」で始まり、その後任意の 3 桁の数字が続くすべてのダイヤル文字列と一致します。

ダイヤルプランには、数字のパターンに加えて、英数字の SIP URI のルーティングを可能にするドメインパターンを含めることもできます。この主な使用例としては、Webex Calling トランクを使用して相互接続されたオンプレミスベースの呼制御インスタンス間の、URI ルーティングを有効にすることです。ドメインパターンは、SIP URI のホスト部分を照合するために使用されます。ドメインパターンは、完全一致の完全修飾ドメイン、またはドメインサフィックスの一致の場合は「*」を含むドメインです。すべてのドメインパターンには、ドット (.) が少なくとも 1 つ含まれます。

ダイヤルプランパターン (数字および URI) は、企業内で一意です。2 つの異なるダイヤルプランに同じパターンを含めることはできません。これは、確定的なルーティング動作を保証するために適用されています。

URI のホスト部分 (右側) が Webex Calling を参照していない場合に SIP コールを処理すると、Webex Calling ではルート選択のために、プロビジョニングされたドメインパターンに対して URI のホスト部分を照合することのみ、ドメインパターンを考慮します。URI のホスト部分が Webex Calling を参照している場合 (Webex Calling 電話機から発信された、またはトランクから受信された数値コールが、このカテゴリに分類されます) は、数字のユーザーを示す部分 (URI の左側) のある URI に対して、WebEx Calling では最初に、+E.164 パターンに一致するもの、次にエンタープライズパターンに一致するものを検索します。+E.164 パターンとの照合を試みる前には、ダイヤルの正規化は適用されません。数字での一致が見つからない場合、Webex Calling はホスト部分を使用して、ドメインダイヤルパターンの 1 つで一致をチェックします。

複数のダイヤルプランの一致が見つかった場合は、最適な一致ルーティングロジックが適用され、最も明確に限定されたパターンが選択されます。ワイルドカードの「X」を使用する範囲パターンは、最適な一致を決定するために「!」を使用するプレフィックスパターンよりも優先されます。

オンプレミスの呼制御システムによるインターコネクト

ローカルゲートウェイは、Webex Calling に PSTN アクセスを提供するだけでなく、Webex Calling を既存のオンプレミス呼制御サービスに接続することもできます。これにより、お客様は Webex Calling に移行する間、既存のオンプレミス呼制御システムを維持できます。必要に応じて、オンプレミスの呼制御システムをそのまま使い続け、Webex Calling と共存させることも可能です。

図 11 PSTN とオンプレミスの呼制御システムの両方に接続を提供するローカルゲートウェイ

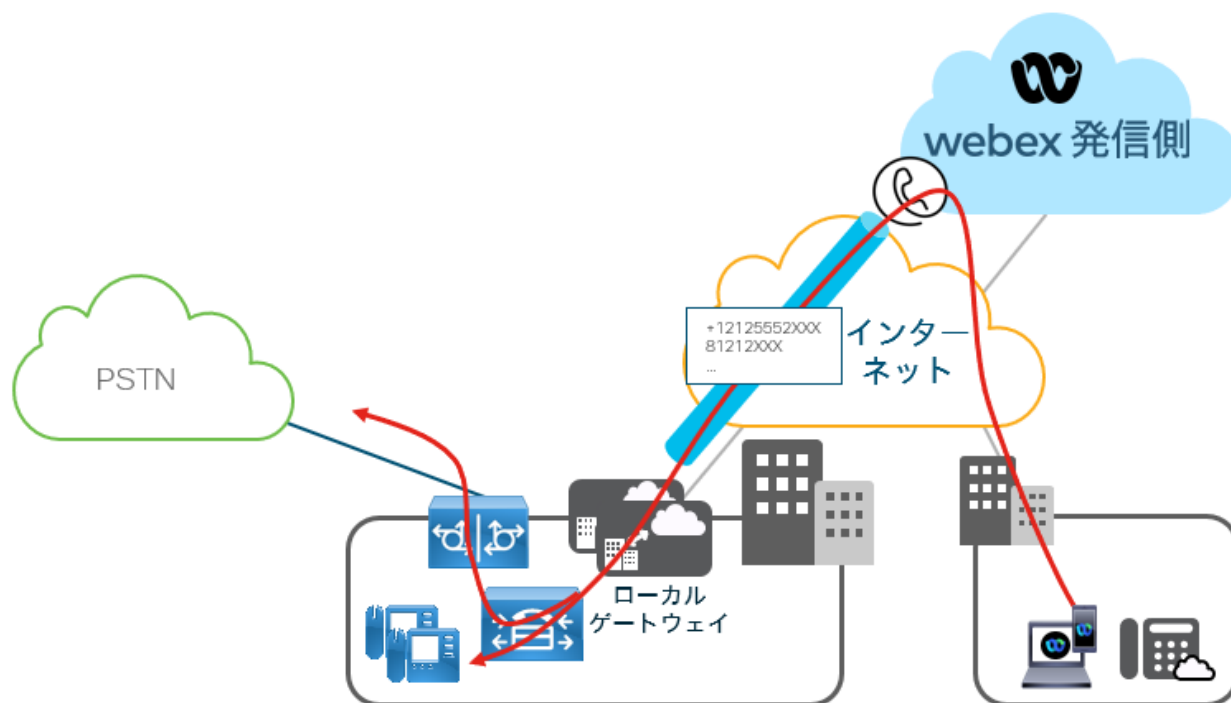
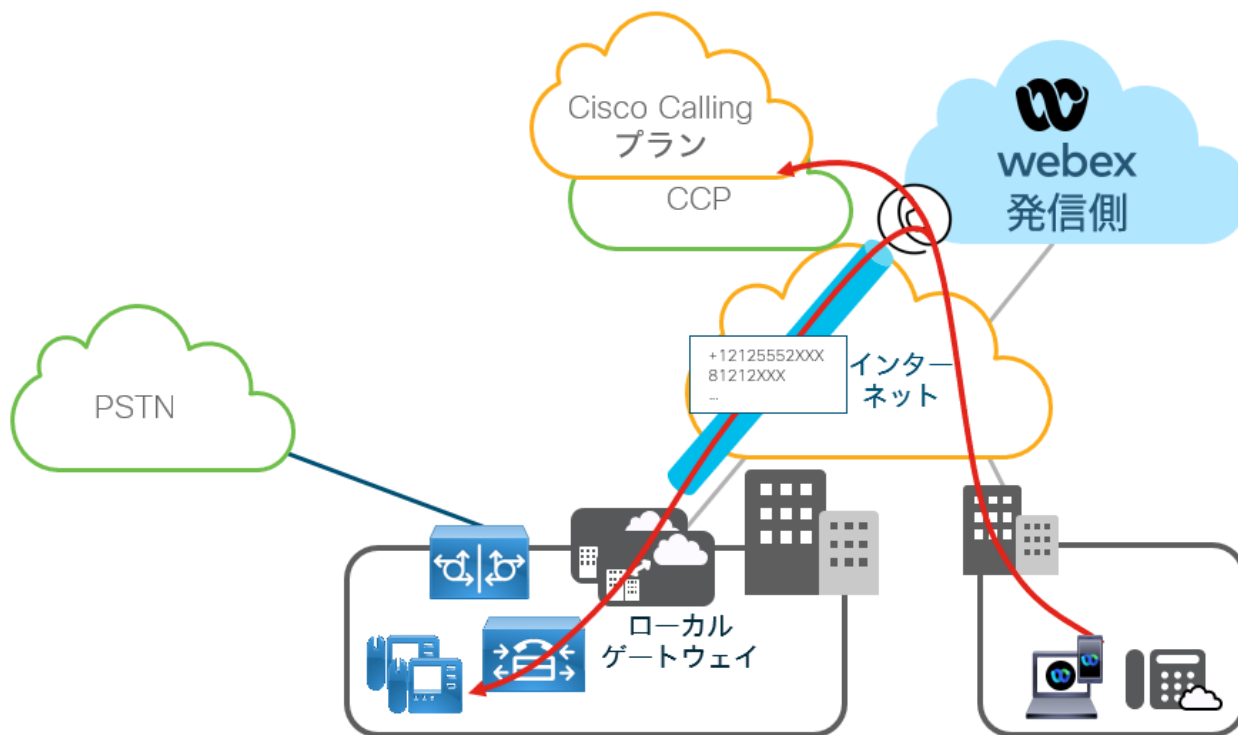


図 11 は、Webex Calling とオンプレミスの呼制御インスタンスが共存している概要を示しています。Webex Calling で設定されたダイヤルプランにより、Unified CM 上にあるエンタープライズの接続先が Webex Calling から呼び出されたときに、オンプレミスの呼制御インスタンスに終端するトランクまたはルートグループにエンタープライズコールとして送信され、他のすべてのコール、ダイヤルプランのパターンは、PSTN コールとしてトランクまたはルートグループに送信されます。この例では、Webex Calling から送信されたコールは、まずオンプレミスの呼制御インスタンスに送られます。このインスタンスでは、オンネットコールとオフネットコールを区別するためにエンタープライズダイヤルプランが使用されます。オフネットコールは、オンプレミスの呼制御インスタンスの通常の PSTN ゲートウェイを介して PSTN に送信され、オンネットコールは、オンプレミスの呼制御インスタンスに登録されているエンドポイントまたはオンプレミスの呼制御インスタンスによって提供されるサービスにルーティングされます。

トランク経由の着信コールと発信コールでは、ロケーションがトランクでのみ使用されていて、そのロケーション内にユーザーが設定されていない場合であっても、トランクのロケーションのメイン番号を設定する必要があります。

PSTN アクセス用のオンプレミストラックとクラウド PSTN の組み合わせ

図 12 PSTN アクセス用のオンプレミストラックとクラウド PSTN の組み合わせ



Webex Calling ロケーションごとに、PSTN (Cisco Calling プラン、Cloud Connected PSTN、またはオンプレミスベース PSTN) を選択して設定する必要があります。各ロケーションに対して選択できる PSTN は 1 つだけです。Webex Calling ダイヤルプランを使用すると、トランクまたはルートグループを介してオンプレミスの Unified CM に接続しながら、ロケーションに選択したクラウドベースの PSTN (Cisco Calling プランまたは Cloud Connected PSTN) を使用できます。この場合、この Webex Calling に構成されたダイヤルプランのパターンに一致するすべての宛先が、企業通話としてトランクまたはルートグループを介してオンプレミスの Unified CM に送信され、PSTN 通話には、設定された PSTN の選択肢が使用されます。

複数のオンプレミス呼制御インスタンス

トランクまたはルートグループと組み合わせたダイヤルプランを使用して、複数のオンプレミス呼制御インスタンスとのインターワーキングを確立することもできます。

図 13 複数のオンプレミス呼制御インスタンスのインターコネクト

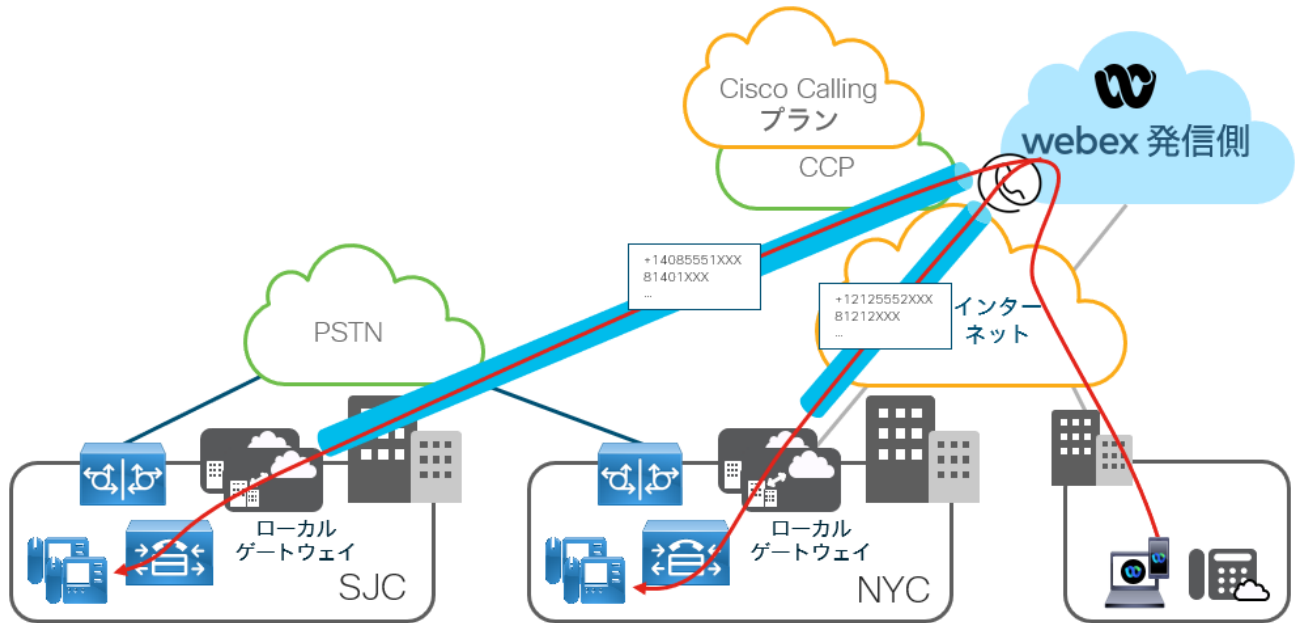
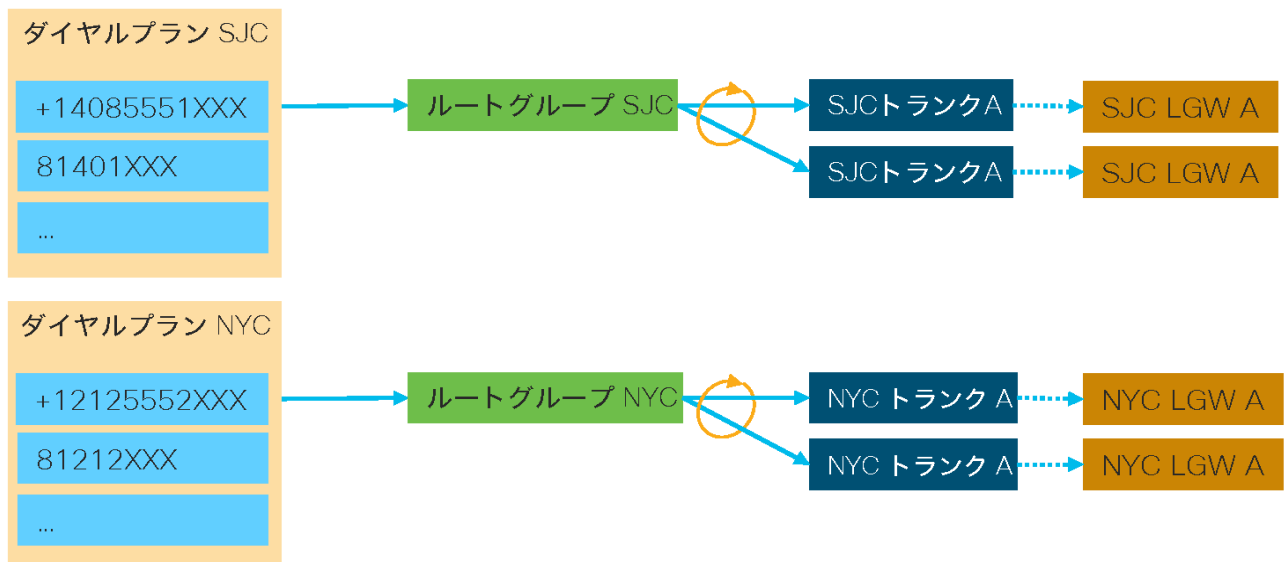


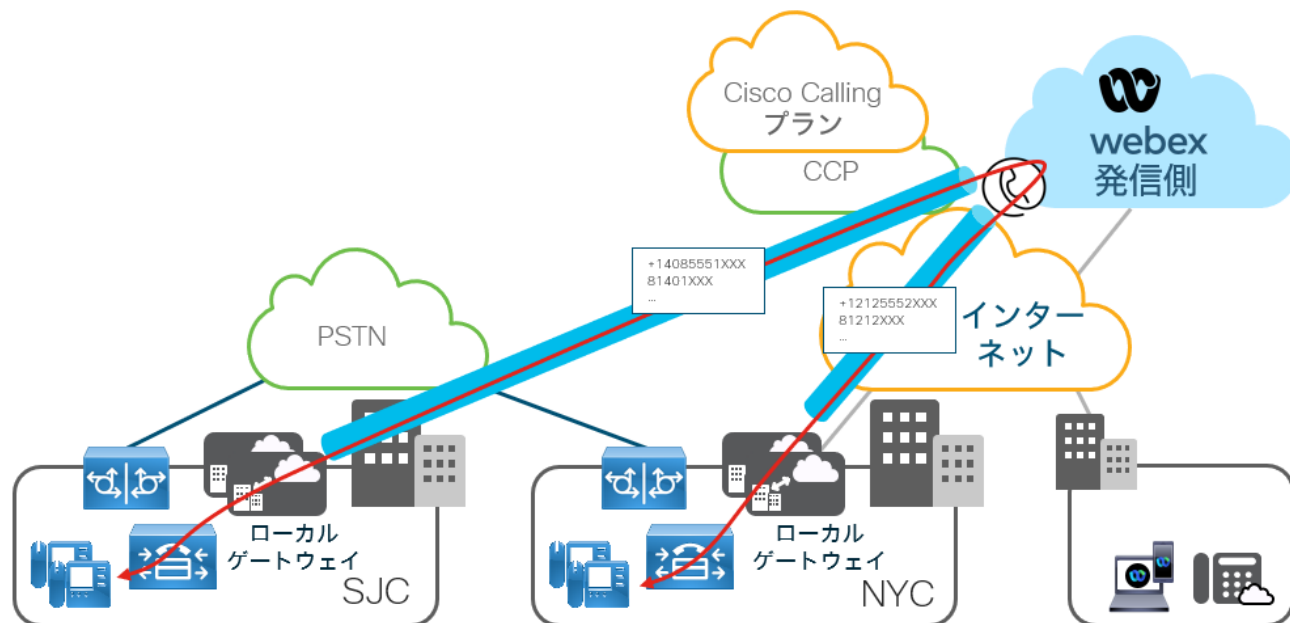
図 13 は、2 つのオンプレミス呼制御インスタンスが Webex Calling に同時に接続されている例を示しています。2 組のローカルゲートウェイによって Webex Calling への接続が確立されています。それぞれのローカルゲートウェイは、Webex Calling のルートグループによって表され、各ルートグループには、個々のローカルゲートウェイに接続するトランクが含まれています。これを次の図に示します。

図 14 2 つのオンプレミス呼制御インスタンスのダイヤルプラン設定



Webex Calling ユーザーから発信された通話の場合、ダイヤルされた宛先はすべてのパターンと照合され、一致が見つかり、そのパターンを含むダイヤルプランでルーティングの選択として設定されたルートグループまたはトランクに、通話がルーティングされます。関連する国内ダイヤルプランに従ったダイヤル文字列の正規化は、一致する前に適用されます。上記の例を使用すると、「81212345」、「+12125552300」、および「9125552300」（外部アクセスコード「9」と想定）は、最後の2つのダイヤル文字列が着信先である NYC オンプレミスロケーションにルーティングされます。ローカルゲートウェイに向かう SIP INVITE は「+12125552300」です。

図 15 オンプレミス呼制御インスタンス間のルーティング



Webex Calling ダイヤルプランによって確立された数字ルーティングスキームは、Webex Calling ユーザーから発信されたコールを特定の呼制御インスタンスに誘導するために使用されるだけでなく、オンプレミスユーザーから発信され、トランクの1つを介したオンプレミス呼制御インスタンスによって Webex Calling に送信されるコールにも適用されます。トランク上の Webex Calling が受信したコールの着信側アドレスが、Webex Calling アドレス（ユーザーまたは任意のサービス）と一致しない場合、Webex Calling ユーザーから発信されたコールと同様に、ダイヤルプランパターンが照合され、どのトランクまたはルートグループにコールを送信するかが決定されます。この場合の Webex Calling は、すべてのオンプレミス呼制御インスタンス間のタンデムとして機能します。

コール ルーティングの概要

Webex Calling ユーザーから発信されたコールの場合、まずダイヤル文字列が発信ユーザーの国内番号計画で定義された緊急番号と比較されます。一致した場合、コールは緊急コールとしてルーティングされます。

次に、ダイヤル文字列が、Webex Calling ユーザーの TN、内線、またはエンタープライズ番号と一致するかどうかチェックされます。この手順では、非常に限定された（単純な）数の正規化のみが適用されます。たとえば、9-1-972-555-0101（PSTN アクセスコードおよび国内プレフィックス付き）としてダイヤルされたコールは、TN + 1-972-555-0101 とはすぐに一致しません。一致した場合、コールはそれぞれのユーザーにルーティングされます。

次に、ダイヤル文字列が仮想オンネット内線番号と照合され、正常に一致する場合は仮想オンネット内線番号のコールロジックが呼び出されます。次に、ダイヤル文字列が数字のダイヤルプランパターンと照合され、一致する場合は、コールがオンプレミスコールとしてダイヤルプランの接続先に送信されます。

最後に、発信側ユーザーの国内ダイヤルプランに基づいてダイヤル文字列が分析されます。ダイヤルプランルックアップの結果として、可能な場合は、ダイヤル文字列は +E.164 に変換されます。ダイヤル文字列が変換されると、フリーダイヤル、国際電話、および国内電話の場合、コールルーティングは、Webex Calling ユーザーに一致するものを探して、上記で再び開始されます。このセカンダリのルックアップにより、コールのダイヤルに使用されるダイヤル手順に関係なく、コールは確実にオンネットでルーティングされます。

セカンダリルックアップが不要で、国内番号計画のルックアップが一致した場合、コールは PSTN に送信されます。不明（国内番号計画と一致しない）ダイヤル文字列の処理については、次のセクションで説明します。

リモートオフィスサービスおよび Office Anywhere サービスは、上記のプロセスに従いません。リモートオフィス/Office Anywhere の接続先は常に外部として扱われるため、接続先をユーザー、仮想オンネット内線番号、またはダイヤルプランと照合することはありません。

不明な番号の処理

不明な番号のルーティング動作は、企業全体での[不明な番号の処理 (Unknown Number Handling)]とロケーションレベルの[オンプレミス内線番号へのコール (Calls to On-Premises Extensions)]の2つの設定によって制御されます。企業レベルの[不明な番号の処理 (Unknown Number Handling)]設定は、[標準の動作 (Standard behavior)]または[レガシー (Legacy)]に設定できます。新規の導入では、[標準の動作 (Standard behavior)]を選択し、Webex Calling ダイヤルプランを設定してオンプレミスへのコールルーティングを確立する必要があります。もう1つのオプションは、主に Webex Calling ダイヤルプランが導入される前に存在していた導入の後方互換性を提供するために提供されています。

Webex Calling ユーザーから発信されたコールの場合、まずダイヤル番号が、緊急番号、顧客に定義された Webex Calling 番号、仮想オンネット内線番号、ダイヤルプランパターン、最後に国内番号計画パターンの順に照合されます。これは、前のセクションで詳しく説明した内容です。一致が見つからず、ダイヤル文字列が2～6桁の場合（ダイヤルされた番号は不明な内線番号と見なされます）、コールの発信元ロケーションに対して[オンプレミス内線番号へのコール (Calls to On-Premises Extensions)]が有効になっている場合は、そのロケーションのオンプレミス内線番号へのコール用に設定されたトランクまたはルートグループに「不明な内線番号」のコールとしてルーティングされます。[オンプレミス内線番号へのコール (Calls to On-Premises Extensions)]を無効にすると、企業レベルの[不明な番号の処理 (Unknown Number Handling)]が[レガシー (Legacy)]に設定されている場合にのみ、ロケーションの PSTN として設定されたトランクまたはルートグループに、不明な接続先へのコールが送信されます。不明な番号へのコールがクラウド PSTN (Cisco Calling プランまたは Cloud Connected PSTN) に送信されることはありません。その他のすべての場合は、不明な番号へのコールは拒否されます。[不明な番号の処理 (Unknown Number Handling)]が[レガシー (Legacy)]に設定されている場合にすべての不明な番号をオンプレミスペースの PSTN に送信することは、Webex Calling ダイヤルプランの導入前の Webex Calling のルーティング動作との下位互換性があります。

オンプレミス通話（発信者が Webex Calling ダイヤルプランの接続先と一致する通話）が不明な番号にルーティングされるのは、通話の着信先が内線番号（2～6桁）で、[オンプレミス内線番号への通話 (Calls to On-Premises Extensions)]がも発信元のトランクのロケーションで、有効になっている場合のみです。それ以外の場合では、コールは拒否されます。

表 2 は、不明な番号のルーティング動作をまとめたものです。

表 2 不明な番号のルーティングロジック

			「不明な番号処理」のグローバル設定	
発信元 (From)	宛先	「オンプレミス内線番号へのコール」	「標準」	「レガシー」
Webex Calling	不明な内線番号 (例 : 4099)	有効	ロケーションレベルの [オンプレミスの内線番号へのコール (Calls to On-Premises Extensions)] オプションで設定された、オンプレミス PSTN の選択へのルート	
		無効	拒否	PSTN へのルート (オンプレミススペースの PSTN が選択されている場合)
	その他の不明な番号	任意	拒否	PSTN へのルート (オンプレミススペースの PSTN が選択されている場合)
オンプレミス	不明な内線番号 (例 : 4099)	有効	ロケーションレベルの [オンプレミスの内線番号へのコール (Calls to On-Premises Extensions)] オプションで設定された、オンプレミス PSTN の選択へのルート	
		無効	拒否	
	その他の不明な番号	任意	拒否	
外部	すべての不明な番号	任意	拒否	

トランクで Webex Calling に送信される ID

Webex Calling トランク (いずれかの方向) を介した PSTN 通話の場合、ID (通話、接続) を +E.164 形式で送信する必要があります。他の形式 (内線番号、ESN) は、オンプレミスユーザーとの間の通話にのみに許可されます。

Webex Calling へのトランクコール

Webex Calling への着信では、発信元トランクはローカルゲートウェイによって「From」ヘッダーに挿入された otg タグによって識別されます。次に、通話のスクリーニングされていない発信者 ID を使用して、通話タイプが判別されます。

ローカルゲートウェイからの着信コールがプライバシーを要求すると、ヘッダーが存在する場合は、P-Asserted-Identity (PAI) ヘッダーで伝送されるアサート済み ID が、スクリーニングされていない発信側回線 ID として選択されます。プライバシーが要求されていない場合、またはプライバシーが要求されているが PAI ヘッダーが存在しない場合は、「From」ヘッダーで伝送されるプレゼンテーション ID が、スクリーニングされていない発信側回線 ID として選択されます。

デュアルアイデンティティサポートがトランクで有効になっている場合、受信した「From」ヘッダーと PAI ヘッダーは個別に処理され、両方が以降の処理のために保持されます。デュアル ID サポートをオフにすると、受信した 1 つの ID だけが保持され、PAI ヘッダーが優先して処理されます。

Webex Calling スクリーニングサービスは、一連の選択基準を使用して、スクリーニングの結果に応じて異なるパフォーマンスを実行します。たとえば、選択的な通話転送を使用すると、発信側アドレスがユーザーが指定した発信側アドレス基準に一致する場合に、着信コールを指定された宛先に転送できます。オンプレミス PBX からユーザーへの着信コールの場合、ユーザーのスクリーニングサービスでは、発信者番号が +E.164 形式である必要があります。スクリーニングサービスには、発信側基準としてオンプレミス ESN/不明な内線番号を指定しないでください。

着信コールの場合、スクリーニングされていない発信者 ID は、顧客に設定されたダイヤルプランパターンと照合されます。ユーザー部分は数字のダイヤルプランパターンとの照合に使用され、ホスト部分はドメインパターンの照合に使用されます。一致が見つかった場合、そのコールはオンプレミスコールとして分類されます。

ダイヤルプランの一致が見つからず、グローバルな [不明な番号の処理 (Unknown Number Handling)] 設定が [標準 (Standard)] に設定されている場合、着信トランクの [オンプレミス内線番号へのコール (Calls to On-Premises Extension)] 設定がチェックされます。[オンプレミス内線番号へのコール (Calls to On-Premises Extension)] が有効で、発信者 ID の長さが 2 ~ 6 桁の場合、コールは企業内線番号から発信されたと見なされ、オンプレミスコールとして分類されます。

最後に、グローバルな [不明な番号の処理 (Unknown Number Handling)] 設定が [レガシー (Legacy)] に設定されている場合も、コールはオンプレミスコールとして分類されます。

これらのチェックのいずれも成功しない場合、コールはネットワーク (PSTN) コールとして分類されます。

表 3 に、この動作の概要を示します。

表 3 トランクの着信通話の通話分類。

	「不明な番号処理」のグローバル設定		
	「標準」		「レガシー」
	「オンプレミス内線番号へのコール」		
着信時の発信者 id (番号)	有効	無効	
ダイヤルプランの一致	オンプレミス		オンプレミス
不明な内線番号 (例 : 4200)	オンプレミス	外部	オンプレミス
その他の不明な番号	外部		オンプレミス

コールの分類は、コールがオンネットの送信元から発信されたか、PSTN から発信されたかを考慮するサービスの動作に影響します。さらに、コールの分類によって到達可能な接続先が決まります (詳細については次のセクションを参照)。

許可される中継コールと発信者 ID の選択

Webex Calling ダイヤルプランにより、オンプレミスの呼制御インスタンス間および Webex Calling ユーザーからオンプレミスの呼制御インスタンスへの確定的なルーティングが可能になります。Webex Calling ダイヤルプランは、オンプレミスユーザーにクラウド PSTN を提供することを目的としていません。オンプレミスの呼制御インスタンスからクラウド接続 PSTN または Cisco PSTN への中継コールは許可されません。表 4 に、許可される中継コールと発信者 ID として送信されるものを示します。

表 4 中継呼マトリックスと発信者 ID

		宛先		
		Webex Calling ユーザー	トランク (DP 一致)	クラウド接続 PSTN または Cisco PSTN
発信元 (From)	Webex Calling ユーザー	許可、 ユーザーの内部発信者 ID	次のセクションの 表 5 を参照	許可、 ユーザーの外部発信者 ID
	トランク	許可、 着信の「From」	許可 ¹⁾ 、 着信の「From」	拒否
	クラウド接続 PSTN または Cisco PSTN	許可、 着信の「From」	拒否	拒否

¹⁾トランク間通話は、着信通話がオンプレミス通話として分類された場合のみ許可されます。

トランクからの着信通話は、発信者 ID が内線番号 (2 ~ 6 桁) であるか、発信者 ID がダイヤルプランパターンと一致する場合にのみ、ダイヤルされた内線番号/ESN にルーティングされます。したがって、通話はオンプレミス通話として分類されます。発信者 ID としての内線番号 (2 ~ 6 桁) は、トランクのロケーションでオンプレミスへの不明な内線番号のルーティングが内部通話として有効になっている場合のみ許可されます。上記の要件を満たしていない通話は、ステータスコード 604 で拒否されます。

Webex Calling ユーザーからトランク経由で発信するコールの発信者 ID

ロケーションの PSTN の選択としてオンプレミスペースの PSTN を使用する場合、トランクに送信される PSTN コールでは、プレゼンテーション ID は常にユーザーの発信者 ID 設定によって決定されます。

Webex Calling ユーザーからオンプレミス接続先へのコールの場合、Webex Calling は [オンプレミスとのコールの発信者 ID 形式 (Caller ID Format for Calls from and to On-premises)] パラメータをチェックして、オンプレミスペースのローカルゲートウェイに送信するプレゼンテーション ID を決定します。

[オンプレミスとのコールの発信者 ID 形式 (Caller ID Format for Calls from and to On-premises)] が [ESN (ロケーションルーティングプレフィックス + ユーザーの内線番号 (Location routing prefix + user extension))] に設定されている場合、発信側ユーザーが内線番号と発信者のロケーションを持ち、発信者のロケーションにサイトプレフィックスが設定されている場合にのみ、目的のプレゼンテーション ID 形式を満たすことができます。ユーザーに内線番号がない場合、または発信側ユーザーのロケーションにサイトプレフィックスがない場合は、代わりに、ユーザーの発信者 ID 設定 (直接回線、ロケーション番号、またはユーザーのロケーションから割り当てられた番号) に従って、プレゼンテーション ID の値が決定されます。プレゼンテーション ID は +E.164 として送信されます。

[オンプレミスとのコールの発信者 ID 形式 (Caller ID Format for Calls from and to On-premises)] が [+E.164 電話番号 (+E.164 phone number)] に設定されている場合、Webex Calling はユーザーの発信者 ID 設定を無視し、ユーザーの直接回線をプレゼンテーション ID として使用しようと試みます。ユーザーが電話番号を持っていない場合は、プレゼンテーション ID 値はユーザーの発信者 ID 設定に従って決定されます。

Webex Calling は、個別のプレゼンテーション ID とアサート済み ID をサポートしています。発信側では、プレゼンテーション ID が「From」ヘッダーに含まれ、アサート済み ID が P-Asserted-Identity ヘッダーに含まれます。直接回線を持つユーザーのアサート済み ID は常に直接回線であり、直接回線がないユーザーに対してのみロケーションのメイン番号が使用されます。

次の表に、「From」ヘッダーでプレゼンテーション ID として送信されるもの、およびロケーションプレフィックスが設定されていると想定して PAI ヘッダーでアサート済み ID として送信されるものをまとめています。

表 5 Webex Calling 発信者 ID のプレゼンテーション

ユーザーに電話番号や内線番号が設定されていますか?		オンプレミスとのコールの発信者 ID 形式 (Caller ID Format for Calls from and to On-premises) の設定		
		+E.164 電話番号 (+E.164 phone number)	ESN (ロケーションルーティングプレフィックス + ユーザーの内線番号 (Location routing prefix + user	
電話番号	内線	PAI	発信元 (From)	
はい	はい	電話番号、+E.164	DN、+E.164	ロケーションプレフィックス + 内線番号 ¹
はい	いいえ	電話番号、+E.164	DN、+E.164	ユーザーの発信者 ID 設定に応じる、+E.164
いいえ	はい	ロケーションのメイン番号、+E.164	ユーザーの発信者 ID 設定に応じる、+E.164	ロケーションプレフィックス + 内線番号 ¹
いいえ	いいえ	DN または内線番号が設定されていないコールは許可されません		

¹ロケーションにロケーションプレフィックスが設定されていない場合は、ユーザーの内線番号だけが発信者 ID として使用されます。

注：デュアルアイデンティティサポートがトランクで無効になっている場合、PAI ヘッダーは常に「From」ヘッダーと同じ値に設定されます。

赤色でマークされているケースでは、正しいプレゼンテーション ID を送信できないため、終端側の着信側ユーザー（オンプレミスの Unified CM など）からのコールバックはできません。すべての Webex Calling ユーザーが少なくとも ESN プレゼンテーション ID を使用してプロビジョニングされた内線番号を持っている場合、コールバックが可能になります。+E.164 プレゼンテーション ID では、すべての Webex Calling ユーザーが電話番号を持っている場合のみ、これが可能となります。

ESN プレゼンテーション ID が設定されている場合、Webex Calling からオンプレミスユーザーへのコールが PSTN に転送されると、PSTN コールレグで有効な発信者 ID が使用できなくなります（ESN は有効な PSTN 発信者 ID ではありません）。この場合、発信者 ID は一部の固定値（メイン番号）に対してマスキングされている必要があります。発信者 ID の ESN から +E.164 へのマッピングは、ネクストホップ呼制御インスタンスに、すべての Webex Calling ロケーションの ESN から +E.164 へのすべてのマッピングがある場合に実現できますが、発信元ユーザーが電話番号を持っていない場合に、簡単な +E.164 マッピングでは番号がこの顧客に属さない番号になってしまうリスクがあります。

サービスの相互作用

多くの Webex Calling サービスでは、ダイヤルプランの照合を含むルーティングルックアップを使用します。たとえば、コール転送サービスと自動応答（オペレータへのコール転送）サービスの場合、Webex Calling はダイヤルプランルックアップを実行して、通常ユーザー発信と同じ方法でコールをオンプレミス PBX にルーティングします。管理者は、ユーザーの内線番号と同じ方法で、転送先（forward-to または transfer-to）として ESN 番号をプロビジョニングできます。

ただし、Office Anywhere などの他のサービスでは、ネットワークロケーションへのコールを分岐するときにダイヤルプランルックアップを呼び出しません。このような場合は、この機能は適用されません。

スクリーニングサービスは、一連の選択的な基準を使用して、スクリーニングの結果に応じて異なるパフォーマンスを実行します。スクリーニングサービスでは、発信番号が E.164 形式である必要があります。スクリーニングサービスでは、発信元の照合にオンプレミス ESN や不明な番号を指定しないでください。

ビデオの考慮事項

職場番号または内線番号をダイヤルすることにより、単一の Webex Calling 組織内で、ビデオ対応デバイスまたは Webex アプリ間でビデオ通話が可能です。会議またはビデオアドレス (SIP アドレス)

(username@example.webex.com など) をダイヤルしても、ビデオ通話ができます。デフォルトでは、PSTN は音声のみを伝送し、PSTN 経由でルーティングされる通話は音声通話のみになります。

Webex アプリから誰かにビデオ通話するには、アプリの上部にある [検索、会議、通話 (Search, meet, and call)] バーをクリックしてアプリヘッダーを使用します。システムはコンタクトに割り当てられた電話番号に自動的にダイヤルします。ダイヤルする電話番号がない場合は、割り当てられた E メールアドレスが使用されます。

さらに、ダイヤルパッドはビデオ通話を発信できる Webex アプリ、電話機、および Webex デバイスで使用できます。ダイヤルパッドに相手の番号、名前、E メールアドレス、またはビデオアドレス (ルームデバイス用など) を入力し、ビデオ通話オプションを選択するだけです。

メディアフロー

メディアフローの開始時は、常に Webex Calling アクセス SBC にアンカーされます。電話を含むポイントツーポイントコールの場合、ローカルゲートウェイ、および ICE を使用した Webex アプリケーション メディアパス最適化では、関連するエンティティ間の直接メディアパスを確立しようとします。詳細については、「メディアパスの最適化」のセクションを参照してください。

エンドポイントが同じロケーションにある場合と PSTN コールの場合のメディアフロー

図 16 Webex Calling のメディアフロー (同じロケーションにある場合と PSTN 通話の場合)

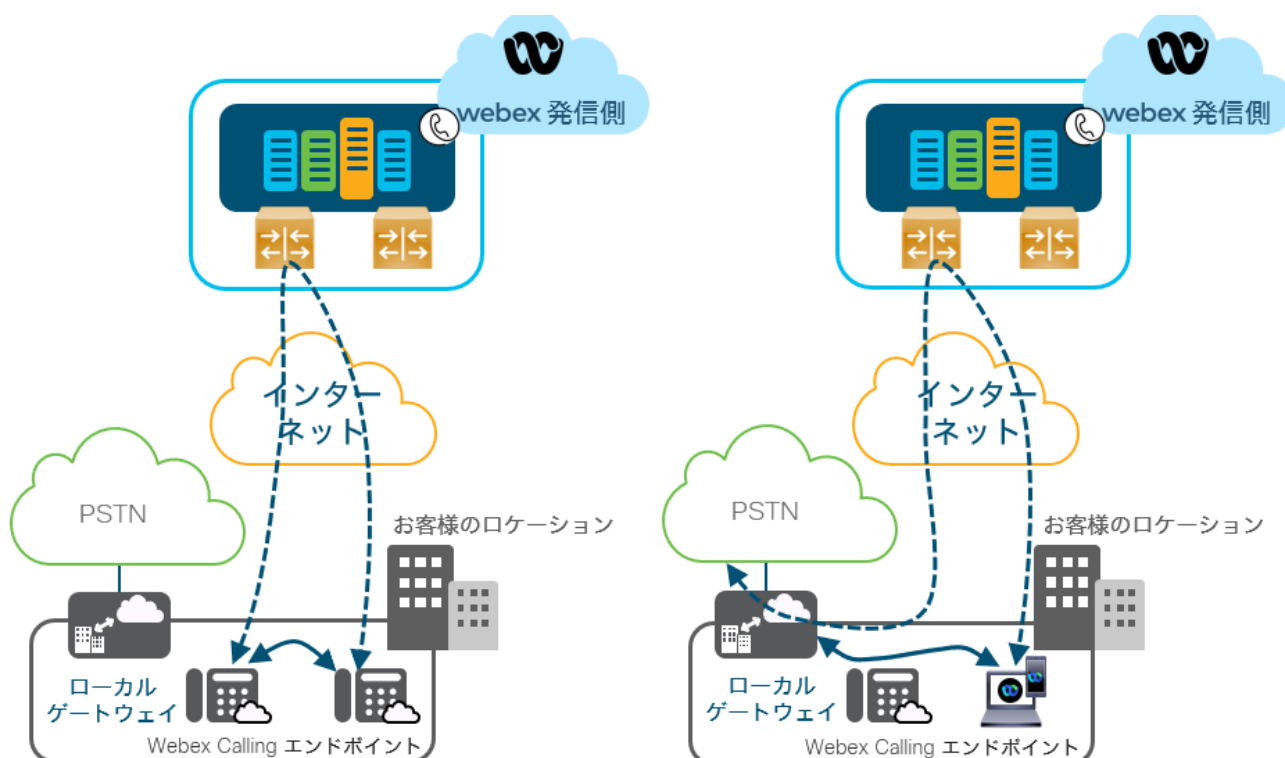


図 16 は、2 つのメディアフローの例を示しています。左側の例は、同じ場所にある 2 つの Webex Calling エンドポイント間のコールを示しています。メディアフローは、ICE ネゴシエーションが成功した場合（実線）は 2 つのエンドポイント間でダイレクトとなり、また ICE ネゴシエーションが失敗した場合は、Webex Calling アクセス SBC にアンカーされます。このため、発信元の電話からお客様のインターネットエッジを介して Webex Calling アクセス SBC にメディアが経由し、接続先のエンドポイント（点線）に戻ります。反対方向のメディアも同じパスをたどります。

右側の例は、PSTN コールのメディアが発信元のエンドポイントからお客様のインターネットエッジを介して Webex Calling アクセス SBC に送信され、そこからお客様のインターネットエッジを介してローカルゲートウェイに再送信されることを示しています。

ICE ネゴシエーションが成功しない場合のみ、2 つの全二重オーディオ/ビデオストリームがお客様のインターネットエッジを通過します。つまり、2 者間のダイレクト UDP メディアはブロックされます。これは、ほとんどの場合、メディアはローカルのままになることを意味します。企業ネットワークのセキュリティ設定によって ICE ネゴシエーションが成功しない場合には、各ロケーションで適切な帯域幅のサイズを確保し、ロケーション内とロケーション間で、また、PSTN コールの混雑時に、この 2 つの全二重オーディオ/ビデオストリームを処理できるようにする必要があります。また、帯域幅の計算では、すべてのコールが最初に Webex Calling アクセス SBC にアンカーされ、コールの確立直後に最適化されたパスにのみ切り替わるという事実も考慮する必要があります。これらのコールは、最適化されたメディアパスへの切り替えにかかる時間を表す平均コール保留時間が短いコールとして、帯域幅計算に織り込むことができます。

Webex Calling のお客様間のコールのメディアフロー

Webex Calling をご利用のお客様間のコールは、法的要件（合法的傍受など）を満たすために PSTN 経由でルーティングする必要があります。

図 17 Webex Calling の 2 名のお客様間の Webex Calling のメディアフローを参照してください。

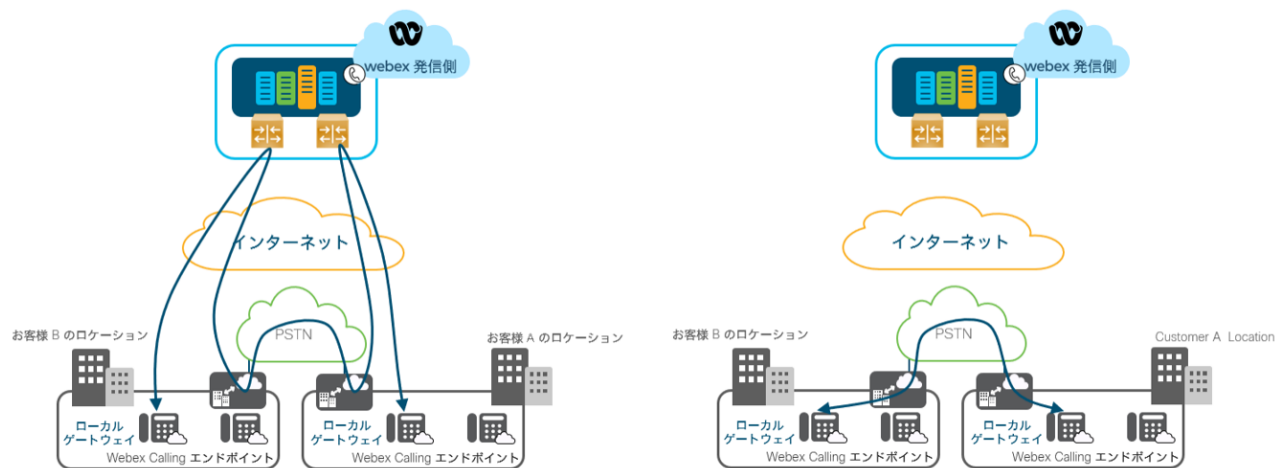


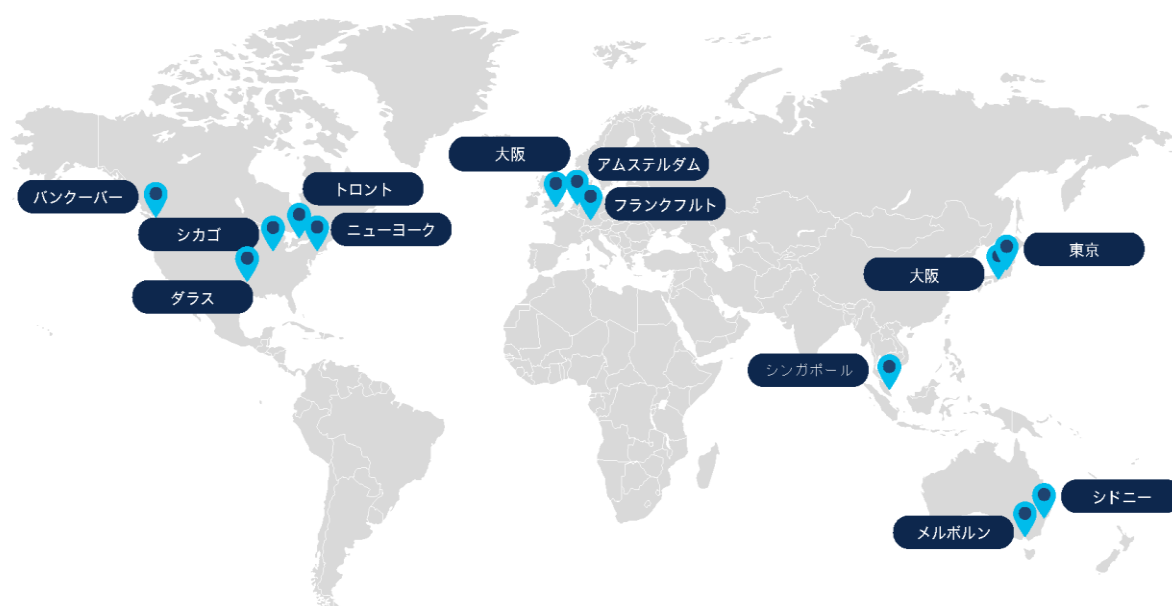
図 17 の左側の図は、メディアパスの最適化なしでメディアフローが Webex Calling アクセスレイヤで 2 回アンカーされ、両方の Webex Calling のお客様のローカルゲートウェイを通過することを示しています。

メディアパスの最適化（右図）では、コールは両方の Webex Calling のお客様のローカルゲートウェイを通過しますが、メディアはローカルゲートウェイと Webex Calling エンドポイント間を直接通過します。

Webex Calling のリージョン

Webex Calling は、米国（ダラス、シカゴ、ニューヨーク）、カナダ（バンクーバー、トロント）、UK（ロンドン、ロンドン）、欧州（アムステルダム、フランクフルト）、APJC 日本（東京、大阪）、および APJC オーストラリア（メルボルン、シドニー）の 6 つのリージョンプラットフォームで運用されています。各 Webex Calling インスタンスは、そのリージョン内に冗長データセンターを提供しています。シンガポールのデータセンターは、APAC 地域の特定の国のユーザーにメディアサービスを提供し、オーストラリアまたは日本の Webex Calling プラットフォームとの過度のメディア往復時間を回避します。

図 18 Webex Calling のグローバルバックボーン

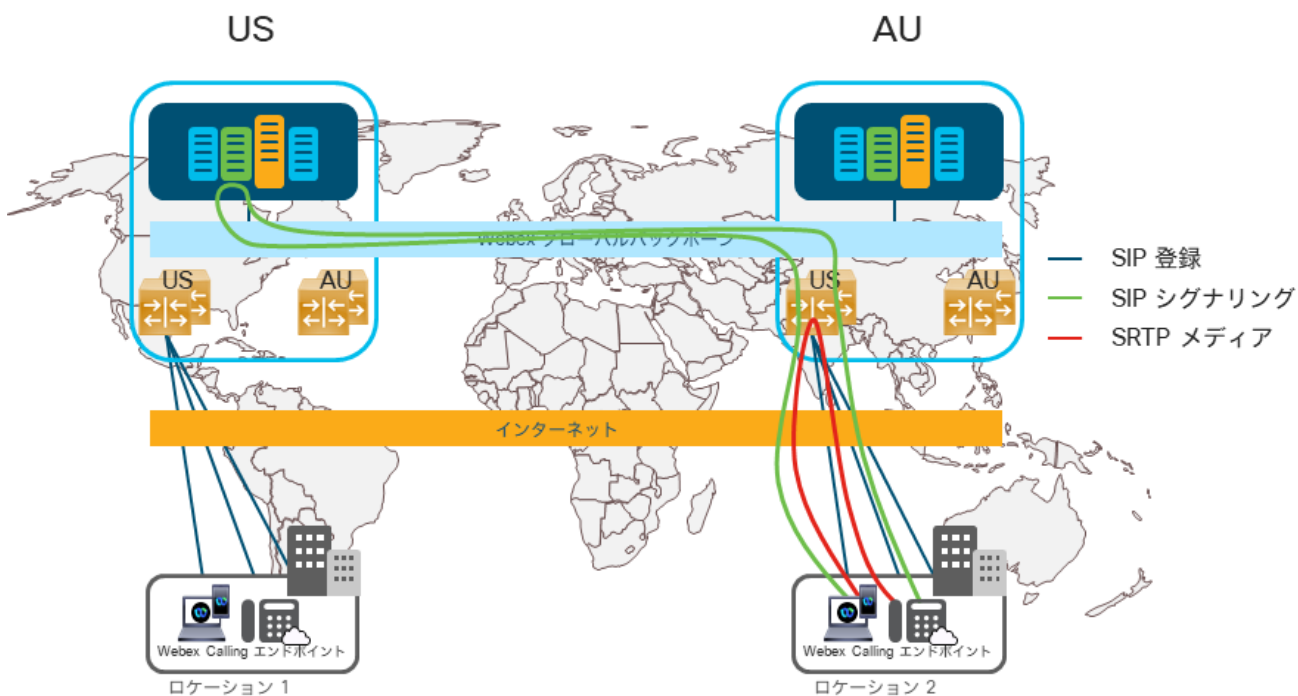


各 Webex Calling のお客様は、6 つの Webex Calling インスタンスのいずれかでプロビジョニングされます。お客様のすべてのプロビジョニング情報がその Webex Calling インスタンスに保存され、そのお客様にプロビジョニングされたすべてのエンドポイントとローカルゲートウェイの SIP シグナリングが、そのお客様がプロビジョニングされている Webex Calling インスタンスに関連付けられます。最初に選択した Webex Calling リージョンは後で変更できないため、Webex Calling リージョンの選択に至る決定プロセスの一部として、すべての関連要因を考慮することが重要です。過度のシグナリング ラウンドトリップ遅延を回避するために、どの Webex Calling インスタンスを使用するかを移行プロセスの早い段階で決定することが重要です。シスコでは、導入における最大数のユーザーに対して最短のシグナリング ラウンドトリップ時間を提供する Webex Calling インスタンスを選択することを推奨します。

Webex Calling リージョンの選択で考慮すべきもう 1 つの要素は、そのリージョン内で利用可能なクラウド接続 PSTN (CCP) プロバイダによって提供される PSTN サービスの国ごとの可用性です。移行期間中は、Webex Calling デバイスの PSTN アクセスをローカルゲートウェイを介して行い、Unified CM 登録デバイスとのインターワーキングを有効にすることもできますが、移行中または移行完了後の任意の時点で、Webex Calling の PSTN アクセスを Cisco Calling プランまたは Cloud Connected PSTN に切り替えることができます。その時点で、Webex Calling のリージョン内で利用可能な Cisco Calling プランまたは CCP プロバイダの国が重要な要素になります。

<https://community.cisco.com/t5/collaboration-voice-and-video/cloud-connected-pstn-provider-partners-for-cisco-webex-calling/ta-p/3916211> で入手可能な、クラウド接続 PSTN プロバイダのリストを参照してください。また、Webex Calling の国ごとの可用性については、『Cisco Webex はどこで入手できますか』の記事：https://help.webex.com/en-us/n6fwepj/Where-is-Cisco-Webex-Available#id_98285 を参照してください。

図 19 リージョンのアクセス SBC



Webex Calling のお客様の地域の選択によって、そのお客様のすべてのコール用の信頼できる呼制御エンティティの場所が決まります。Webex Calling アクセスレイヤにアンカーされているコールの過度なメディア RTT を回避するために、すべての Webex Calling 呼制御エンティティは各リージョンのアクセスリソースを使用できます。

図 19 は、オーストラリアの 2 台の電話機間のコールフローを示しています。わかりやすくするために、図では米国リージョンとオーストラリアリージョンのみを示していますが、この概念はすべてのリージョンに適用されます。お客様が米国リージョンに割り当てられている場合でも、メディアパスは米国の Webex Calling インスタンスが制御するオーストラリアリージョンのアクセス SBC に終端されます。これはフォールバックメディアパスのみです。ICE メディアパスの最適化により、エンドポイント間の直接メディアパスを実現できます。この通話の SIP シグナリングは、米国リージョンでホストされている Webex Calling 呼制御エンティティ（お客様がプロビジョニングされている Webex Calling インスタンス）へ送られます。

図 20 リージョンのアクセス SBC を使用するリージョン間のメディアフロー

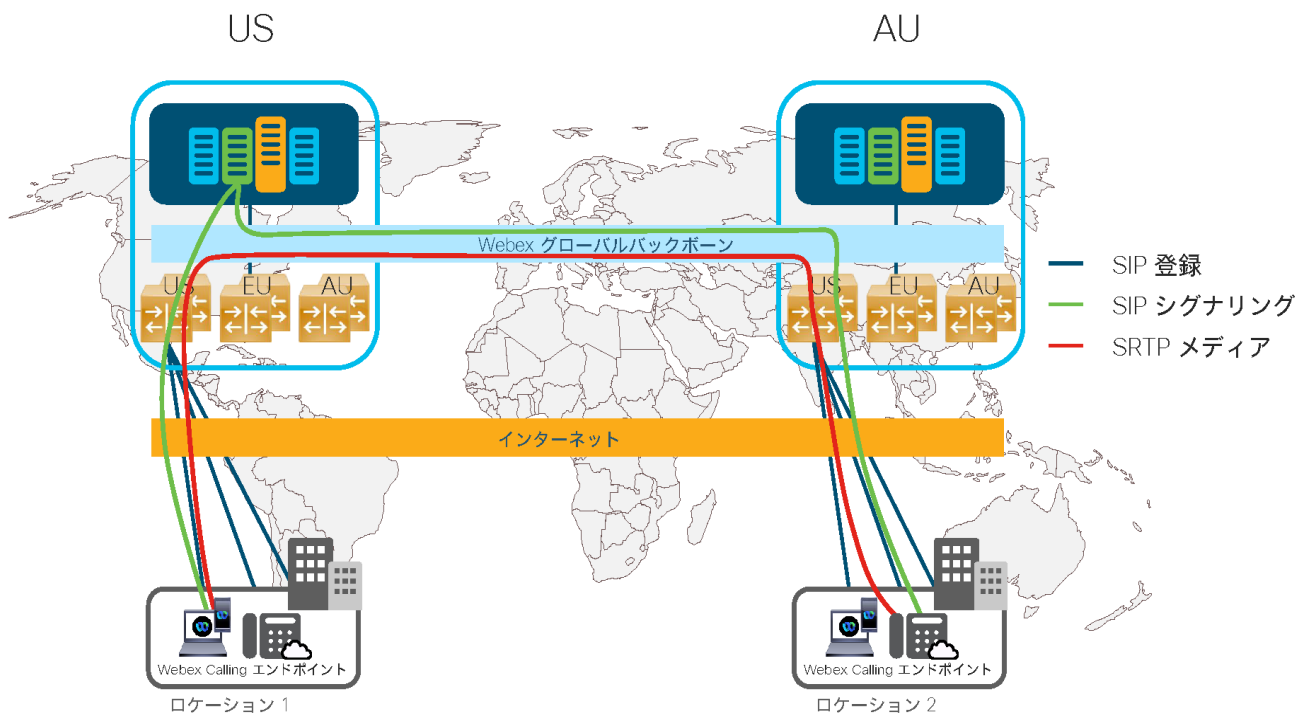


図 20 は、2 つのリージョンのアクセス SBC がリージョン間のコールメディアをアンカーする場合は示しています。アクセス SBC 間のトラフィックは Webex のグローバルバックボーンを経由し、エンドポイントとアクセス SBC 間のメディアフローの一部のみがアクセスネットワークとしてインターネットを経由します。

ローカルゲートウェイを含むメディアフローは上記と同じスキームに従います。つまり、ローカルゲートウェイを含むメディアフローは、ローカルゲートウェイが導入されているリージョンのアクセス SBC でも同様に常時アンカーされます。

導入のさまざまな側面

このセクションでは、ロケーション、ローカルゲートウェイ、ディレクトリ統合の概念など、Webex Calling の導入に関するさまざまな側面について詳しく説明します。

ロケーションの定義

Webex Calling の導入時に組織を「ロケーション」に分割する際は、多くの要素を考慮する必要があります。PSTN の構成とダイヤルプランの考慮事項に加え、緊急サービスの通知方法や内部テレフォニーサービスの提供方法などの要素も重要です。

表 6 ロケーションをまたいで利用できるユーザー機能

機能	他のロケーションのユーザーに許可	他のロケーションのユーザーに未許可
エグゼクティブ アシスタント	X	
ハントグループエージェント	X	
コールキューエージェント	X	
自動応答ユーザールックアップ	X	
回線監視 (ビジーランプ)	X	
シングル ナンバー リーチ	X	
ページング グループ	X	
コールパークグループ		X
ピックアップ グループ		X
番号の移動		X
ユーザーの移動		X
共用ライン アピアランス		X

各ロケーションには PSTN 接続が定義されている必要があります、その接続は他のロケーションと共有できます。PSTN 接続の詳細はこのドキュメントの後半で説明しますが、デフォルトではローカルゲートウェイの最大同時通話数は 250 です。これは、ローカルゲートウェイを使用するロケーションの定義に影響します。Cloud Connected PSTN はこの制限の影響を受けません。後で説明するように、サイト ダイヤル プレフィックスの使用も考慮する必要があります。

Control Hub でロケーションを追加する場合は、住所および連絡先の名前と情報が必要です。Webex Calling VAR では、これらの情報は緊急応答機関 (PSAP) への緊急連絡や組織内で使用する緊急連絡先機能では使用されず、個別に定義されます。

緊急通報

このセクションでは、北米および世界の他の地域の国で必要とされる緊急通報機能について説明します。これらの国では、ローカリゼーションの仕様が非常に細かいため、追加の実装が必要になる場合があります。

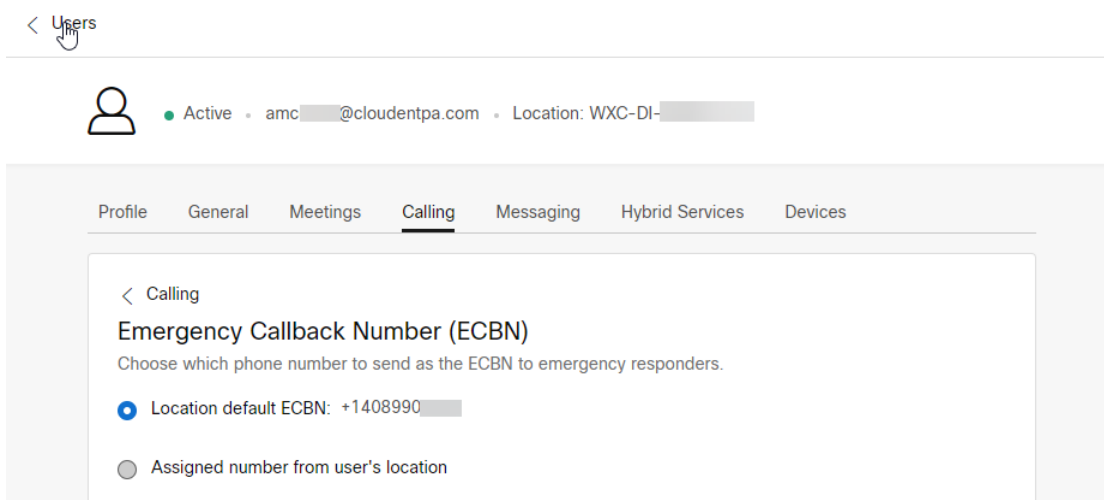
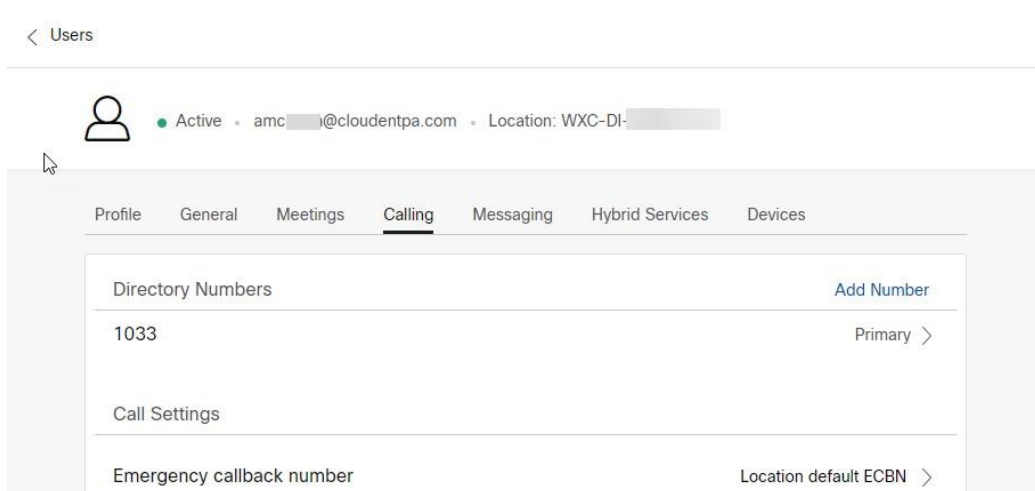
緊急通報を適切なディスパッチセンターにルーティングするという要件は、PSTN サービスを提供するすべての通話サービスの要件です。Webex Calling を使用すると、緊急通報のルーティングはソリューションにネイティブであり、Webex Calling がサポートする国のすべての国内緊急番号のサポートが含まれます。Webex Calling での緊急通報のルーティングは、Control Hub 内で定義されたロケーションと、そのロケーションの PSTN のアクセス方法 (CCP または LGW) に基づいています。Webex Calling の緊急番号は事前定義されており、Webex Calling ユーザーとデバイスが展開されている国に固有です。

Webex Calling で緊急通報を提供するには、2 つの方法があります。基本的な緊急通報ルーティングサービスと強化された緊急通報ルーティングサービスがあります。基本的な緊急通報ルーティングサービスは、管理者が選択した番号を使用して場所を特定し、緊急サービスに連絡するためのルートと呼び出します。基本的な緊急通報の場合、通話パスは通常、お客様の CCP プロバイダーを経由しますが、緊急通報ルーティングに LGW を使用することもできます。Webex Calling には、適切なディスパッチセンターに緊急通報を配信するために全国をカバーするプロバイダーを利用することが必須な規制コンプライアンス要件がある米国およびカナダの展開向けに設計された、強化された緊急通報ルーティングもあります。

すべてのお客様は、少なくとも基本的な緊急通報構成を展開する必要があります。基本的な緊急通報では、Webex Calling で定義された各ロケーションにお客様が所有する E164 番号が少なくとも 1 つ割り当てられている必要があります。基本的な緊急通報の場合、各ロケーションは、緊急時に警察、消防、または救急車が派遣される住所によって定義されます。ほとんどの場合、ロケーションのメイン番号は、緊急事態の物理的な場所を表す最善の選択となります。通常、E164 番号への住所の割り当ては、CCP または LGW プロバイダーと調整されます。以下の画像は、Richardson ロケーションの緊急コールバック番号として使用されるメイン番号の割り当てを示しています。

The screenshot shows the configuration for the Emergency Callback Number (ECBN) for the Richardson location. The location is identified as Richardson, United States, with Location ID: 3d938345-6f54-4b8d-... The 'Emergency Calling' section is expanded, showing the 'Emergency Callback Number' field. Below this, a configuration screen is shown with two radio button options: 'Use location main number: +1585559 (Richardson)' (selected) and 'Use assigned number from this location'.

ほとんどの場合、その場所の派遣先住所は建物の住所が使用されます。ただし、特定のユーザーまたはデバイスに追加の場所の詳細が必要な場合、管理者は上記と同じプロセスを使用して、それらのデバイスを特定の住所または住所のより正確な場所 (フロアや部屋など) に割り当てることができます。Control Hub のユーザー管理の [通話 (Calling)] タブでは、ユーザーとそのデバイスが特定の派遣先住所を取得するために特定の番号を使用できます。次の図は、特定の番号をデバイスに割り当てる方法を示しています。管理者は、デバイスが使用する番号に正しい派遣先住所が割り当てられていることを確認する責任があります。住所の割り当ては、通常、CCP または LGW PSTN サービスプロバイダーを通じて行われます。



強化された緊急通報ソリューションを提供する必要がある米国ベースのテレフォニー展開の場合、Webex Calling は、緊急通報のルーティングに Webex Calling に統合された RedSky の Horizon Mobility を使用します。コールルーティングに RedSky を使用する場合は、管理者は シスコを介してアカウントを登録し、[通話 (Calling)] -> [サービス設定 (Service Settings)] で適切な情報を構成して、この機能を有効にする必要があります。RedSky サービスがシステムレベルで有効になったら、管理者は各ロケーションレベルで RedSky サービスを有効にします。Webex Calling ロケーションで強化された緊急通報を有効にすると、そのロケーションに割り当てられているすべてのデバイスのサービスが有効化されます。強化された緊急通報対応デバイスは、Cisco MPP 電話機と Cisco の Webex アプリです。

ロケーションで強化された緊急通報を有効にする設定は 2 つあります。[RedSky がネットワーク接続情報とテスト通話を受信できるようにする (Allow RedSky to receive network connectivity information and test calls)] を使用して、デバイスとインフラストラクチャ マッピングの RedSky 構成が正しいことを確認する必要があります。この設定により、テスト通話で 933 に発信して、発信者の位置を読み取るために RedSky の IVR システムを使用して位置を確認することもできます。本書では、位置追跡の RedSky 構成については説明しませんが、管理者は、RedSky にルーティングする緊急通報を有効化する前に、常に位置検出をテストする必要があります。テストが完了し、正確であることが確認されると、管理者は [緊急通報を RedSky にルート (Route Emergency Calls to RedSky)] を切り替えて、通話を RedSky にルートします。このトグルは、そのロケーションのすべての緊急通報を RedSky に転送し、そのロケーションの応答センターに配信します。

強化された緊急通報設定は、オンプレミスとオフプレミスの両方の Webex アプリクライアントにも適用されます。オンプレミスの場合、Webex アプリは MPP 電話機が追跡されるのと同じ方法で追跡できます。オフプレミスの場合、ユーザーは Webex アプリ内で自分の場所を動的に直接設定できます。緊急通報の詳細については、<https://help.webex.com/en-us/article/av6003/Enhanced-Emergency-Calling-for-Webex-Calling> の「Webex Calling 向け強化された緊急通報」に関する Webex ヘルプセンター記事を参照してください。

テレフォニーサービス

ほとんどのコール機能は、定義されたロケーション全体のユーザーが使用できます。これらには、自動応答、ハントグループ、コールキュー、ページンググループ、および定義されたさまざまなロケーションのユーザーとグループメンバーのエグゼクティブアシスタントが含まれます。コールパークグループや共有ラインアピアランスなどの一部の機能では、ユーザーは同一の定義されたロケーション内にいる必要があります。

PSTN の DID 番号もロケーション別に追加され、番号の検証（カリフォルニア州サンノゼで市外局番「302」を使用できるかの検証など）は行われません。これにより、地理的な境界を越えるロケーションでも、ユーザの割り当てを論理的に使用できるようにすることができます（緊急コール用の正しい番号の割り当て条件内にて）。

ネットワーク接続

既存のプロバイダーのデータ接続（MPLS、SD-WAN など）を考慮し、通常はお客様の導入環境内の各ロケーションで直接インターネットアクセスを計画します。クラウドベースのサービスが利用されるため、十分な帯域幅を備えた信頼性の高いインターネット接続が基本要件です。

信頼性の高いネットワーク接続が利用できることを条件として、Webex Calling は世界各地のすべてのお客様のロケーションからアクセスできるため、エンドポイントの存続性を確保する必要がなくなります。

ローカルゲートウェイの導入オプション

Control Hub の各トランクは、単一のローカルゲートウェイ インスタンスへの接続を表します。複数のトランクを 1 つのルートグループにグループ化することで、キャパシティや冗長性の確保を向上させることができます。オンプレミスベースの PSTN 宛てに、あるロケーションから発信されたすべてのコールは、コールルーティング設定に基づいてトランクまたはこのトランクを含むルートグループに送信されます。Webex Calling のお客様は、複数のロケーションに同じローカルゲートウェイ インスタンスを利用できます。

現在、Webex Calling では、1 つのローカルゲートウェイ インスタンスからの同時セッション数が 250 を超えることはできません。これは、デフォルトで、ローカルゲートウェイからのコールのセッション数、つまり Unified CM と Webex Calling エンドポイント間のオンプレミスベース PSTN のコールまたはサイト間のコールのセッション数のデフォルトの制限となります。トランクとルートグループを使用して複数のローカルゲートウェイを組み合わせて、キャパシティを増やすことができます。ただし、単一のローカルゲートウェイの展開で 250 を超える同時コールが必要な場合は、シスコアカウントチームに連絡して、他の展開オプションを検討してください。

ローカルゲートウェイと Webex Calling アクセス SBC 間のネットワーク状態が悪いと、シグナリング接続のパフォーマンスが制限され、同時コールの制限がさらに低くなる可能性があります。ローカルゲートウェイと Webex Calling データセンター間の一方方向の遅延は 100 ミリ秒以下、ジッターは 10 ミリ秒以下、パケット損失は 0.5% 未満である必要があります。

この容量制限を超えるコールは「403 Forbidden」で拒否されます。「show call active voice」コマンドをローカルゲートウェイの任意のインスタンスで実行することで、アクティブコールの合計数を確認することができます。

```
LocalGateway# show call active total-calls
Total Number of Active Calls : 153
```

上記のコマンドの出力で、ローカルゲートウェイでコールが 250 を超えるかどうか（この例では 153）が表示され、トラブルシューティングの結果、Webex Calling アクセス SBC によって「403 Forbidden」の SIP 応答で一部のコールが拒否されることが判明した場合は、Cisco Technical Assistance Center (TAC) にお問い合わせください。

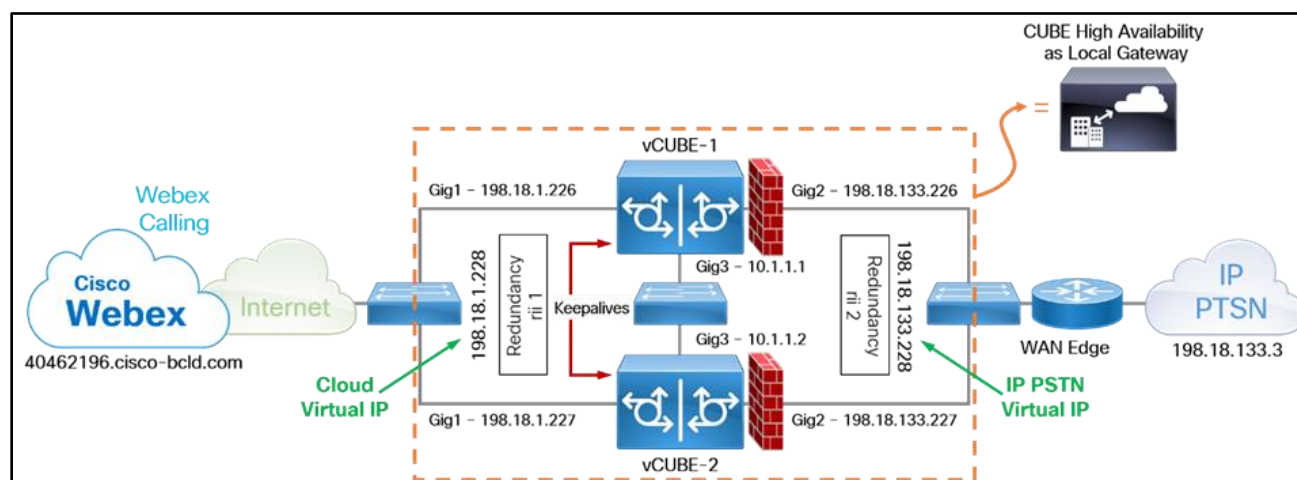
ローカルゲートウェイとしての CUBE ハイアベイラビリティ

すべての IP ベースの環境で、CUBE ハイアベイラビリティ (HA) をローカルゲートウェイ (LGW) として導入し、通話を保持するオプションがあります。CUBE ハイアベイラビリティのレイヤ 2 ボックスツーボックス冗長性は、冗長グループ (RG) インフラストラクチャ プロトコルを使用してルータのアクティブ/スタンバイペアを形成します。アクティブ/スタンバイペアは、それぞれのインターフェイスで同じ仮想 IP アドレス (VIP) を共有し、常にステータスメッセージを交換します。CUBE のセッション情報は、ルータのアクティブとスタンバイのペア間でチェックポイントが作成されるため、アクティブルータが停止した場合は、スタンバイルータが CUBE のコール処理のすべてをすぐに引き継ぐことができます。これにより、シグナリングとメディアの処理状況が保持された状態で引き継がれます。

注：チェックポイントが作成されるのは、メディアパケットにより利用される接続中の通話のみです。（発信中や呼び出し中の状態など）接続前の通話のチェックポイントは作成されません。

次の図 21 は、ローカルゲートウェイとして設定されている一般的な CUBE ハイアベイラビリティを示しています。

図 21 ローカルゲートウェイとして使用する CUBE ハイアベイラビリティ



ローカルゲートウェイが CUBE のハイアベイラビリティを使用して、通話のステートフル フェールオーバーを実現するためには次の要件が必要です。

- ローカルゲートウェイ導入オプションとして、CUBE HA がサポートされているプラットフォームは、ISR 4000 および CSR1000 シリーズです。
- CUBE HA では、TDM またはアナログインターフェイスを冗長構成にできません。
- Gig1 と Gig2 はトラフィック (SIP/RTP) 向けのインターフェイス、Gig3 は冗長グループ (RG) 制御/データ向けのインターフェイスです。
- 2 つ以上の CUBE HA ペアを同じレイヤ 2 ドメインに配置することはできません（グループ ID 1 のペアとグループ ID 2 のペアの 2 つまで）。グループ ID が同じ 2 つの HA ペアを設定する場合、RG 制御/データインターフェイスは別のレイヤ 2 ドメイン (VLAN、個別のスイッチ) に属している必要があります。
- ポートチャネルは、RG 制御/データおよびトラフィック向けインターフェイスの両方でサポートされます。
- シグナリング/メディアはすべて、仮想 IP アドレスが送信元/宛先になります。
- プラットフォームが CUBE HA 構成でリロードされる場合は、必ずスタンバイとして起動します。

- すべてのインターフェイス下位番号 (Gig1、Gig2、Gig3) は、同じプラットフォーム上にある必要があります。
- 冗長インターフェイス識別子 (RII) は、同じレイヤ 2 上のペア/インターフェイスの組み合わせに対して一意である必要があります。
- 両方の CUBE の設定は、物理構成を含めて同一であり、同じ種類のプラットフォームと IOS-XE バージョンで実行する必要があります。
- ループバック インターフェイスは常に UP 状態のため、バインドとして使用することはできません。
- 複数のトラフィック (SIP/RTP) 向けインターフェイス (Gig1、Gig2) を使用する場合は、インターフェイストラッキングを設定する必要があります。
- RG 制御/データリンク (Gig3) のクロスケーブル直結接続は、CUBE HA ではサポートされません。
- CUBE HA を機能させるには、同じようなインターフェイスのすべてでプラットフォームを同一にし、1 台の物理スイッチを介して接続する必要があります (CUBE-1 と CUBE-2 の GE0/0/0 を同じスイッチで終端させるなど)。
- WAN を 直接 CUBE で、または片側のデータ HA で終端させることはできません。
- アクティブ/スタンバイの両方が同じデータセンター内にある必要があります。
- 冗長性を確保するために個別の L3 インターフェイス (RG 制御/データ、Gig3) を使用する必要があります (トラフィック用のインターフェイスを HA のキーブアライブやチェックポイント作成に使用することはできません)。
- フェールオーバー時には、**シグナリング/メディアは保持され、以前アクティブだった CUBE はリロードされる**ようになっています。

ローカルゲートウェイとしての CUBE HA の詳細については、<https://help.webex.com/ja-jp/ndiofhf/Implement-CUBE-High-Availability-as-Local-Gateway> をご覧ください。

ファイアウォールの要件

企業ファイアウォールという観点では、プロビジョニングと登録の両方がアウトバウンド TLS 接続を使用して設定されるため、ファイアウォールでインバウンド接続を許可する必要はありません。

図 22 TCP 接続のファイアウォールトラバースルメカニズム

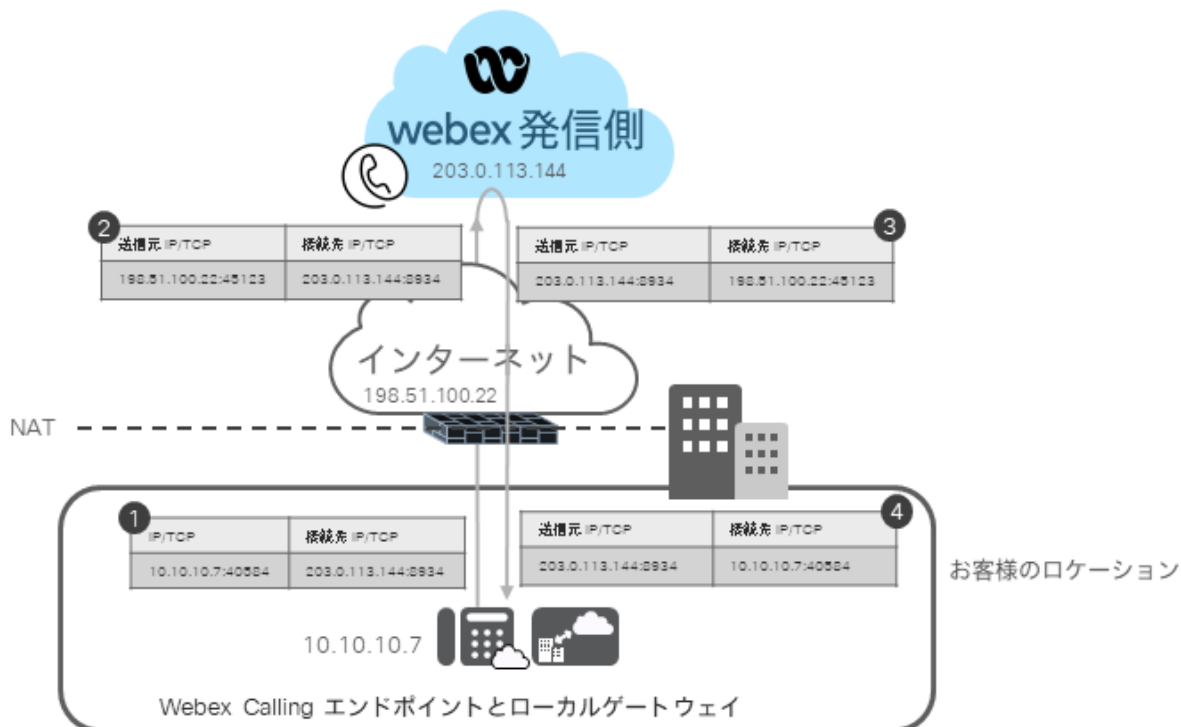


図 22 は、IP フォンが TCP/TLS での SIP 接続を確立するプロセスを示しています。ファイアウォールは、電話機のプライベート IP アドレスをパブリック IP アドレスに変換し、送信元ポートを変更します（ステップ 1 とステップ 2 を参照）。Webex から送信されるリターントラフィックには、同じ外部トランスポートアドレスが使用されます。ファイアウォールはリターントラフィックを許可し、パブリック IP アドレスとポートを、電話機が使用する内部プライベート IP アドレスとポートに変換します（ステップ 3 とステップ 4）。

TLS 接続が確立されると、電話機は Webex Calling との間で SIP シグナリングメッセージを送受信できるようになります。Webex Calling から電話機への SIP シグナリングトラフィックは、電話の登録時に確立された同じ SIP/TLS 接続が再利用されます。ローカルゲートウェイは Webex Calling への SIP トランクの登録を使用するため、企業ファイアウォールの内側から SIP/TLS トランスポート接続を作成するのと同じメカニズムがローカルゲートウェイにも適用されます。SIP/TLS 接続では、企業ファイアウォールで外向き（出力）TCP ポート 8934 を開く必要があります。

NAT が適用される環境では、SIP シグナリングメッセージ内のローカルゲートウェイと IP フォンによってアドバタイズされるトランスポートアドレスは、常に内部（プライベート）IP アドレスです。これらのプライベートアドレスは、Webex Calling アクセスなどの外部エンティティからは到達できません。ただし、受信した SIP シグナリングメッセージのレイヤ 3 トランスポートアドレスを SIP メッセージに含まれるアドレスと照合することで、Webex Calling アクセスレイヤは NAT を検出できます。アドレスが異なる場合は、Webex Calling アクセスとエンドポイントまたはローカルゲートウェイ間に NAT が存在しています。NAT が検出されると、SBC は常に既存の TCP 接続を再利用し、Via ヘッダーに含まれる IP アドレスへの応答や、Contact ヘッダーに含まれるアドレスを使用した新しい SIP リクエストを送信しません。

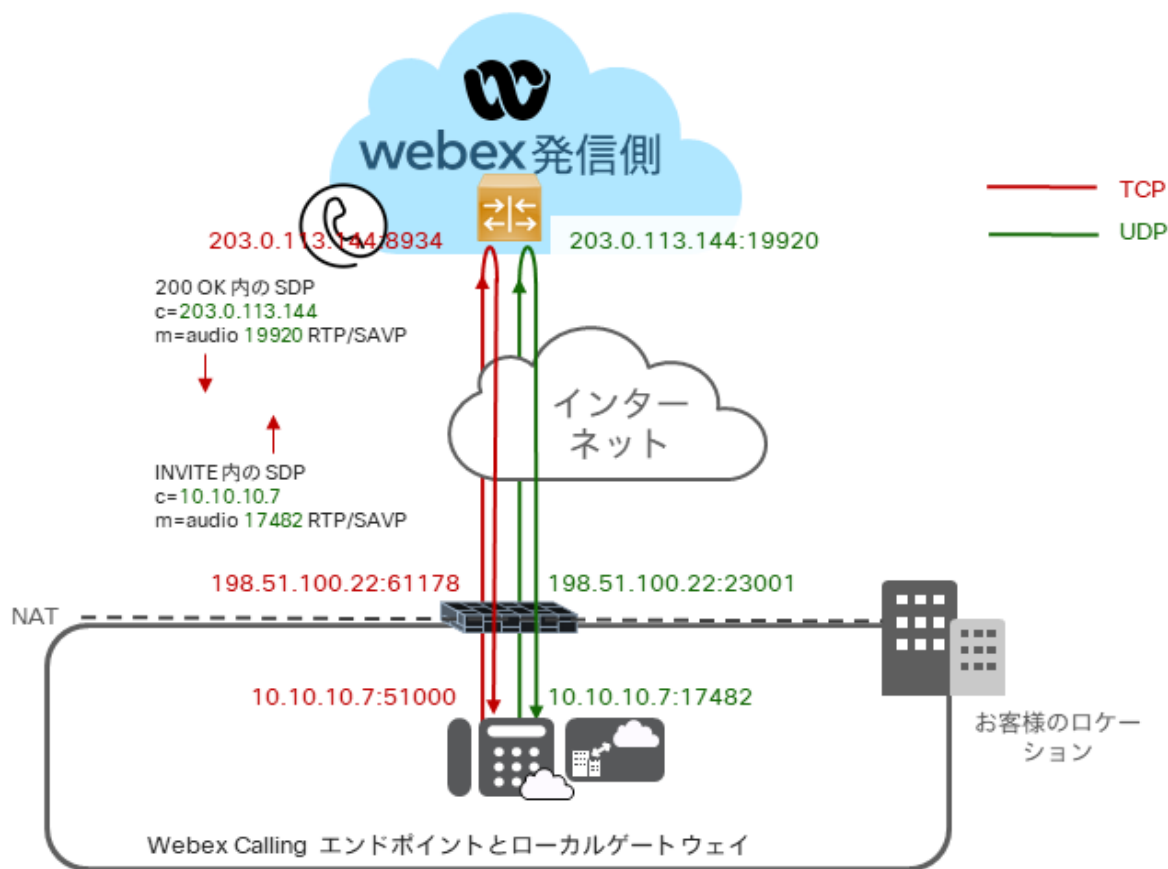
メディアの送受信に使用される IP アドレスは、SIP シグナリング内の SDP メディアネゴシエーションの一部として、エンドポイントとローカルゲートウェイによってアドバタイズされます。ただし、ほとんどの場合、これらはプライベートアドレスであり、Webex Calling アクセスレイヤはこれらのアドレスを使用してメディアの送信を行うことはできません。これらのプライベート トランスポート アドレスが NAT によって変換されるパブリック IP アドレスとポートを判別する方法はありません。リターンメディアに使用するパブリック トランスポート アドレスを決定するために、Webex アクセスレイヤは、SDP 交換の手法としてアクセスレイヤ用にネゴシエートされたリスニングポートで最初のメディアパケットの受信を待機し、受信したメディアパケットの送信元トランスポートアドレスを電話機またはローカルゲートウェイに送り返すメディアトラフィックの宛先として使用します。

Webex Calling アクセスレイヤは、同じロジックを使用して、ローカルゲートウェイまたは IP フォンで NAT の変換（コール保留後の再開など）が発生したかどうかを検出し、それに応じて、既存のフローに属しているため外部から企業のファイアウォールを通過することができる、リターントラフィックの IP アドレスとポート情報を更新することもできます。

SDP に依存するのではなく、受信したメディアパケットからリターンメディアアドレスとポートを推定するメカニズムは「メディアラッチング」と呼ばれます。メディアラッチングでは、企業ファイアウォール内のエンドポイント（ローカルゲートウェイと IP フォン）がメディアパケットを必ず Webex Calling アクセスに送信してから、その逆方向にメディアパケットを返す必要があります。企業ネットワーク内から送信されたメディアパケットは、NAT バインディングを作成し、ファイアウォールを介して接続を開きます。

図 23 は、オンプレミスの Webex Calling エンドポイントまたはローカルゲートウェイと Webex 間のシグナリングとメディアのファイアウォールトラバーサルの例を示しています。

図 23 Webex Calling のファイアウォールトラバーサル メカニズム



この図は、Webex Calling のシグナリングとメディアに対するファイアウォールトラバーサルの例を示しています。

1. エンドポイントまたはローカルゲートウェイは、プライベート IP 10.10.10.7 とポート 51000 を使用して TLS 接続を開始します。宛先アドレスは、Webex Calling アクセスの IP 203.0.113.144 とポート 8934 です。
2. SIP は、この TLS 接続をトランスポートとして使用します。エンドポイントまたはローカルゲートウェイは、音声メディアの送受信に使用する IP 10.10.10.7 とポート 17482 を含む INVITE を SBC に送信します。
3. SBC は同じ TLS 接続で応答 (200 OK) します。このメッセージ (200 OK) 内の SDP 情報には、Webex アクセス音声メディア用の IP アドレス 203.0.113.144 とポート 19920 が含まれています。

4. エンドポイントまたはローカルゲートウェイは、200 OK で受信した SDP から取得した IP アドレスとポート宛にメディアの送信を開始します。これらのメディアパケットの送信元ポートは、最初の INVITE で送信された SDP でアダプタイズされた UDP ポート（この場合は 17482）です。この時点では、アクセス SBC が最初の INVITE の SDP から取得した IP アドレスとポートの両方がファイアウォールでまだ認識できない値に変換されるため、Webex Calling アクセスはリターンパケットを送信できません。最初のメディアパケットが、Webex Calling アクセス（このコールに対してアクセス SBC によってアダプタイズされたポート）に到達すると、SBC は、受信したメディアトラフィックの送信元 IP アドレスとポート（この例では、198.51.100.22 と 23001）からパブリック トランスポートアドレスを取得します。Webex Calling アクセスの接続状態は、このトランスポートアドレスに応じて更新され、Webex Calling から電話機またはローカルゲートウェイに戻されるメディアは、このトランスポートアドレスを使用してストリーミングされます。

ローカルゲートウェイを使用する一部のシナリオでは、両方のコールレグがファイアウォールから見て内向き通信になる場合があります。たとえば、Webex Calling に接続されている IP フォンがローカルゲートウェイ経由で PSTN 番号に発信し、着信側の PSTN デバイスがそのコールを同じネットワークに属する別の IP フォンに転送する場合などです。この 2 つのコールレグはファイアウォールから見て内向きになります。ファイアウォールの内側からは RTP メディアパケットが送信されていないため、ファイアウォールはコールレグをブロックします（送信されていればファイアウォールで接続が開かれます）。このデッドロックを解決するには、ローカルゲートウェイで STUN を設定する必要があります。STUN が設定されている場合、ローカルゲートウェイは、SDP を介してネゴシエートされたメディアの IP アドレスとポートに STUN パケットを送信します。実際のメディアパケットは送信されませんが、UDP STUN パケットはファイアウォールから見て UDP の外向きパケットとなるため接続が確立され、内向きのメディアが同じ接続で流れるようになります。STUN の設定に失敗すると、一部のシナリオで双方向メディアがブロックされることがあります。

要約すると、Webex Calling ではファイアウォールで内向きのポートを開く必要はなく、特定の IP アドレスとポートへの、UDP と TCP の外向きトラフィックのみを許可する必要があります。必要な宛先（ポート、IP アドレス、DNS ドメインの完全なリスト）は『Webex Calling のポート参照情報』（https://help.webex.com/en-us/b2exve/Port-Reference-for-Cisco-Webex-Calling-Value-Added-Resellers#id_112963）に記載されています。

ICE メディアパスの最適化

Webex Calling アクセスにアンカーされているメディアフローから、Webex Calling アクセスがメディアパスに関与しない直接のピアツーピアメディアに切り替えるために、ファイアウォール トラバーサルがクライアントによって実行されることが必要です。これは、Interactive Connectivity Establishment (ICE) プロトコルフレームワークを使用して実現されます。

本ドキュメントで使用される ICE の特殊な用語を紹介します。最もよく使用される用語を次に説明します。

トランスポートアドレス：IP アドレス、トランスポートプロトコル、およびトランスポートポートの組み合わせ

ホストアドレス：エンドポイントのローカルインターフェイスに関連付けられたトランスポートアドレス

サーバー再帰アドレス：STUN サーバーを通じて取得されたトランスポートアドレス。ファイアウォール NAT により変換されたエンドポイントのトランスポートアドレスに対応しています。

ピア再帰アドレス：接続確認によって取得した、ファイアウォール NAT によって変換されたトランスポートアドレス

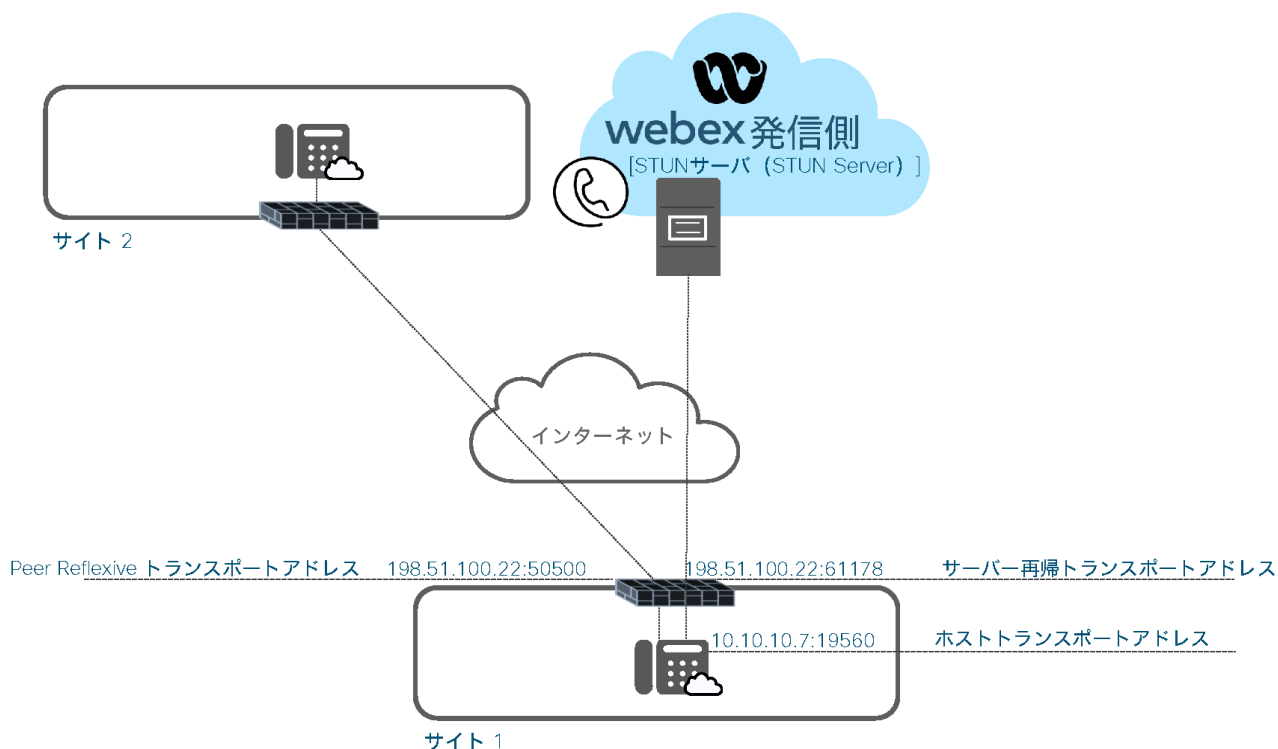
候補：エンドポイントにメディアを送信する候補（ホスト、サーバー再帰、ピア再帰）。接続確認によって、ICE ネゴシエーションが成功した場合、これらのいずれかが選択されます。

5 タプル：2 つのシステム間の接続を識別します。トランスポートプロトコル、送信元および宛先 IP、送信元および宛先トランスポートポートによって識別されます。

選択されたペア：接続確認により選択された発信側と着信側エンドポイントのトランスポートアドレス

図 24 は、さまざまな候補タイプを示しています。

図 24 ホスト、サーバー再帰、ピア再帰の候補



ファイアウォールの外部のシステムと通信するエンドポイントの場合、ホスト トランスポート アドレス（エンドポイントのローカル IP アドレスとポート）は、ファイアウォール NAT によって外部トランスポートアドレスに変換されます。エンドポイントがファイアウォールの外部にあるエンドポイントと双方向 UDP 通信を確立するためには、その外部トランスポートアドレスを把握することが重要です。STUN サーバーを使用することで、これが可能となります。図 24 は、内部トランスポートアドレス 10.10.10.7:19560 を使用するエンドポイントが 2 つの異なるホストに対してパケットを送信する場合、ファイアウォールの NAT によって異なる外部トランスポートアドレスが作成されることを示しています。（STUN サーバーに送信されるパケットのサーバー再帰アドレスと、サイト 2 のエンドポイントに送信されるパケットのピア再帰アドレス）NAT が異なる外部システムとの通信に異なる外部トランスポートアドレスを割り当てる場合、これはアドレス依存と呼ばれます。外部トランスポートアドレスが宛先 IP アドレスだけでなく宛先ポートにも依存する場合、これはアドレスとポート依存と呼ばれます。宛先 IP またはポートに関係なく、同じ内部トランスポートアドレスからのすべてのパケットに同じ外部トランスポートアドレスが使用される場合、これはエンドポイント非依存 NAT と呼ばれます。

エンドポイント非依存 NAT を使用すると、エンドポイントは、この送信元 IP とポートを使用して外部エンドポイントとの接続を開始する前に、外部 STUN サーバーを使用して、特定の送信元 IP とポートのパブリック トランスポート アドレス（サーバー再帰トランスポートアドレス）を決定できます。アドレス依存（またはアドレスおよびポート依存）NAT が存在する場合、外部トランスポートアドレス（ピア再帰トランスポートアドレス）は事前に決定できず、代わりにリモートエンドポイントから取得する必要があります。双方向メディアに、サーバーまたはピアの再帰トランスポートアドレスを使用して学習する手順については、以降の項で説明します。

ICE で許可されるさまざまなオプションの中で、Webex Calling は次のプロトコルと機能をサポートしています。

- ICE 情報を伝送するために使用される SIP SDP アンサー/オファーモデル
- STUN プロトコル
- [STUN サーバー (STUN Server)]
- UDP ベースのメディア
- Webex Calling アクセスにアンカーされた標準メディアパスへの自動フォールバック

ICE によるコールセットアップは、次の 4 つのフェーズに分けることができます。

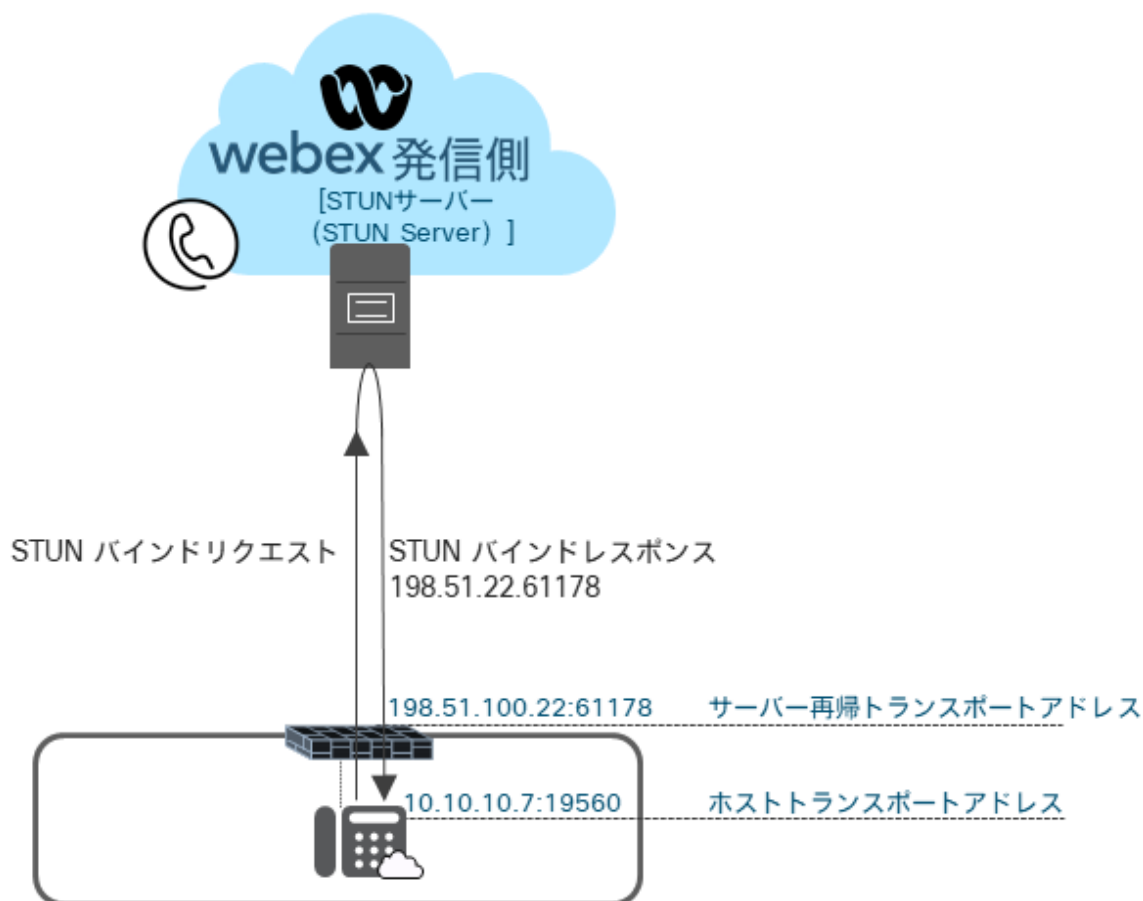
1. 候補の収集：エンドポイントは、コールを発信または応答する前に、STUN サーバーと通信してサーバーの再帰アドレスを取得します。
2. 候補の交換：エンドポイントは、SIP シグナリングを介して、ホストとサーバーの再帰候補を相手側と交換します。
3. 接続性チェック：ホスト、サーバー再帰、および最終的に検出されたピア再帰候補が、メディアの送受信に使用される選択されたペアを指定するために各当事者によってチェックされます。
4. メディアパスの最適化：選択したペアは SIP シグナリングを介してアダプタイズされ、メディアは選択したペアを使用してフローを開始します。

候補の収集

別のピアとの通信を開始する前に、ICE クライアント (Webex アプリまたは Webex Calling 電話機) は、クライアントが他のピアとの通信に使用を試みるプライベート トランスポート アドレスから UDP STUN バインディングリクエスト パケットをポート 5004 で STUN サーバーに送信することにより、STUN サーバーを使用してサーバーの再帰アドレスを決定します。STUN サーバーは、そのリクエストに対して STUN サーバーから見た外部 IP アドレスとポートである、サーバー再帰アドレスを含む STUN バインディングレスポンスで応答します。エンドポイントは、使用するトランスポートアドレスごとにこの STUN バインディング交換を使用します。少なくとも 2 つのサーバー再帰トランスポートアドレスを決定する必要があります。1 つは SRTP 用、もう 1 つは Real Time Control Protocol (RTCP) 用です。

図 25 にこのプロセスを示しています。

図 25 STUN サーバーを介した候補の収集



このプロセスの最期に、エンドポイントにはメディアの送受信に使用できる候補のリストがあります。たとえば、音声通話が SRTP と RTCP UDP ポートを使用する場合、SIP オファーには次の 4 つの候補が含まれます。

- メディアのホスト トランスポートアドレス (SRTP)
- RTCP のホスト トランスポートアドレス
- SRTP のサーバー再帰アドレス
- RTCP のサーバー再帰アドレス

候補の交換

収集された候補は、SIP INVITE メッセージの最初の SDP オファーで送信されます。

メッセージは Webex Calling に送信され、着信側デバイスに中継されます。図 26 の左側にこのプロセスを示しています。

図 26 SIP シグナリングを介した候補の交換

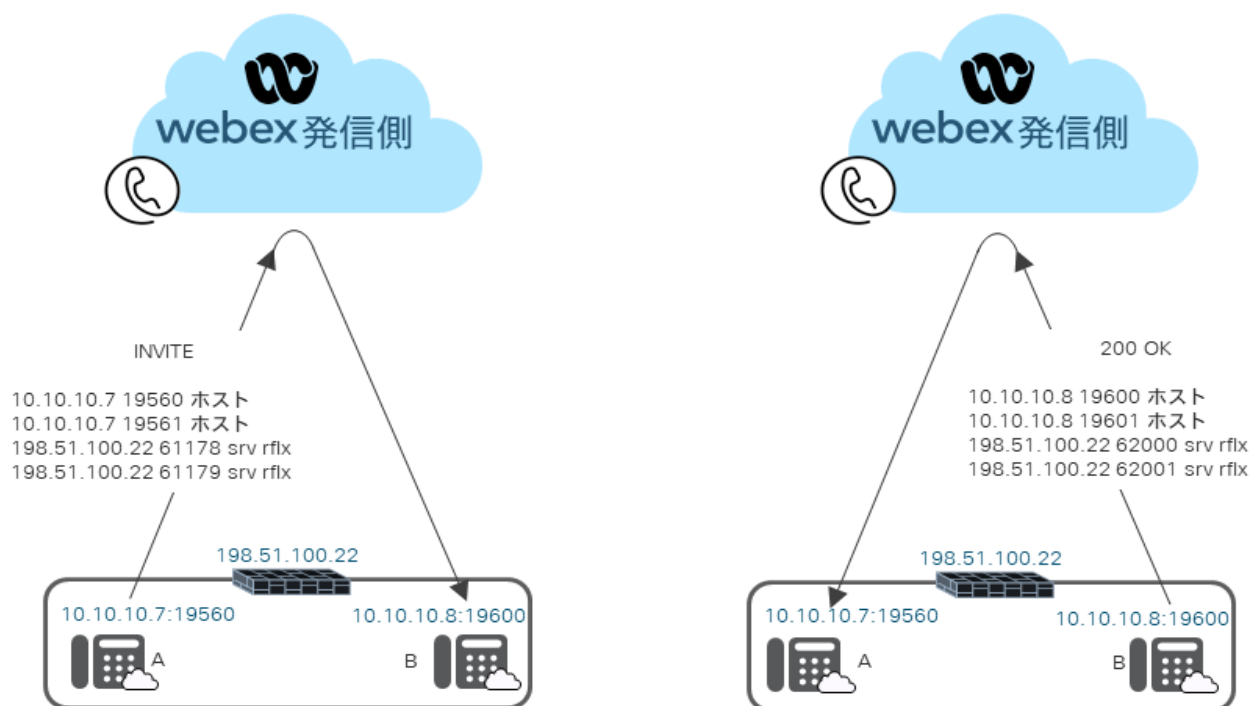


図 25 に示すように、INVITE への応答として、着信側デバイスは候補を SIP 応答の SDP 応答で返します。発信側デバイスと着信側デバイスの候補を取得するプロセスは同じです。

この時点で、両方のエンドポイントに両側からの候補があり、接続確認を開始することができます。

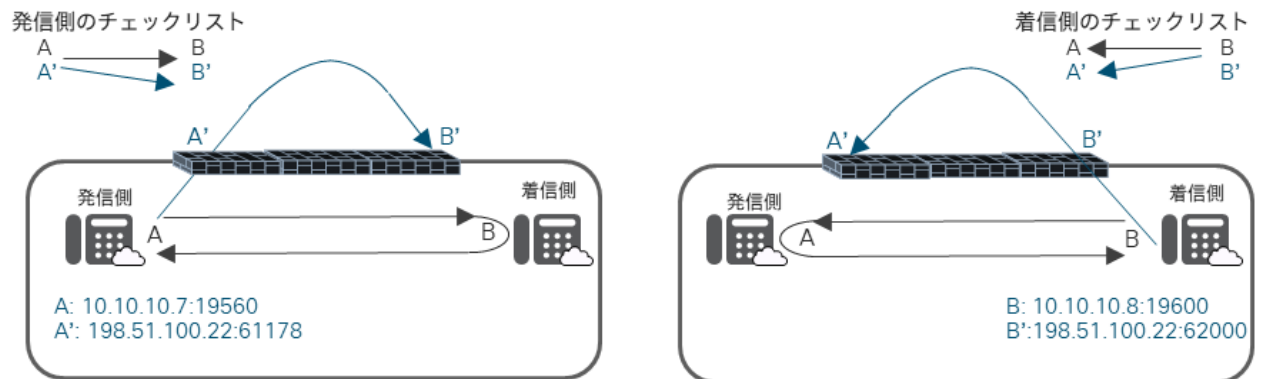
この例では、各デバイスは相手側に対応する次のアドレスを受信します。	発信側エンドポイントが受信した着信側アドレス	着信側エンドポイントが受信した発信側アドレス
SRTP のホスト トランスポートアドレス	10.10.10.8:19600	10.10.10.7:19560
RTCP のホスト トランスポートアドレス	10.10.10.8:19601	10.10.10.7:19561
SRTP のサーバー再帰アドレス	198.51.100.22:62000	198.51.100.22:61178
RTCP のサーバー再帰アドレス	198.51.100.22:62001	198.51.100.22:61179

接続の確認

次に、エンドポイントごとに候補が並べ替えられます。STUN バインドリクエストとレスポンスを使用した接続確認は、メディアの送信に使用されるものと同じトランスポートアドレスを使用して実行されます。接続の確認は双方向で、すべてのエンドポイントで接続確認が送受信されます。候補ペアは、接続確認が双方向で成功した場合に有効と見なされます。

次の例では、A と B はホスト トランスポートアドレスで、A' と B' はそれぞれ発信側と着信側のサーバー再帰アドレスです。図 27 に示すように、A と B は同じ LAN 内にあるため、A と B 間の接続確認は成功します。A と B' 間の接続確認、および B' から A への接続確認は、ファイアウォールの動作によって機能する場合と機能しない場合があります。ファイアウォールがローカルネットワーク内からパブリック IP アドレスを介した内部サービスへのアクセスを許可する場合にのみ、A' と B' を含む接続確認が成功します。このファイアウォールの動作は、NAT ヘアピン、NAT リフレクション、または NAT ループバックと呼ばれます。

図 27 同じネットワーク内の 2 つのエンドポイント間の接続確認

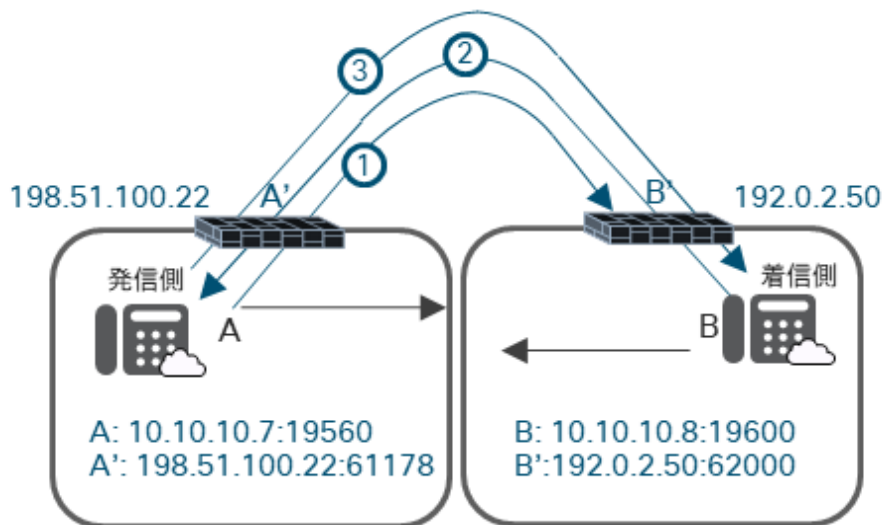


ファイアウォールが NAT リフレクション用に設定されていない場合、動作するペアは A と B のみで、本ドキュメントではこれを [A、B] と表記しています。この表記は、A から B および B から A への接続確認が成功したことを意味します。

NAT リフレクションが有効な場合、動作ペアは [A、B] と [A'、B'] です。この例の [A、B'] と [A'、B] は、[A'、B'] に一致する点に注意してください。これは、A が NAT によって A' に一意に変換され、B が B' に変換されるためです。これは、エンドポイントに依存しない NAT にも当てはまります。アドレス依存型 NAT が存在する場合、STUN サーバーから取得されたサーバー再帰候補は、使用できません。これは、STUN サーバー以外のピアとの通信には、ファイアウォールによって異なるピア再帰トランスポートアドレスが選択され、STUN サーバー以外のトランスポートアドレスから外部のサーバー再帰アドレスに到達したパケットは、ファイアウォールによってネットワークへの侵入が許可されないためです。外部トランスポートアドレスの ICE 接続確認は、1 つのエンドポイントが有効なサーバー再帰アドレスを取得できるように、少なくとも一方でエンドポイント非依存 NAT が使用されている場合にのみ成功します。アドレス依存型 NAT を使用すると、アドレス依存型 NAT の背後にあるエンドポイントは、他のエンドポイントから受信した STUN Binding 応答からピア再帰アドレスを取得します。

次の例では、2 つのエンドポイントが分離されたネットワークにあります。この場合、A と B の間の接続確認は失敗します。図 28 に示すように、どちらのエンドポイントもサーバー再帰アドレスへの接続を試みます。

図 28 分離されたネットワーク内の 2 つのエンドポイント間の接続確認



この例では、サーバー再帰アドレスへの最初の STUN 接続確認メッセージは、A から B' に送信されます (ステップ 1)。これは、着信側ファイアウォールの観点から新しい着信接続であるため、このパケットはブロックされます。ただし、発信側デバイスが B' に STUN メッセージを送信すると、ファイアウォールにピンホールが開き、リターントラフィックを受信できるようになります。このため、B と A' 間の STUN 接続確認メッセージは成功します (ステップ 2)。これは、A から B' に使用されたものと同じ 5 タプルを使用し、その結果、ファイアウォールによってリターントラフィックとして認識されるためです。

B から A に送信された STUN メッセージが、着信側ファイアウォールにピンホールを作成したため、A から B' への新しい接続確認が成功します。

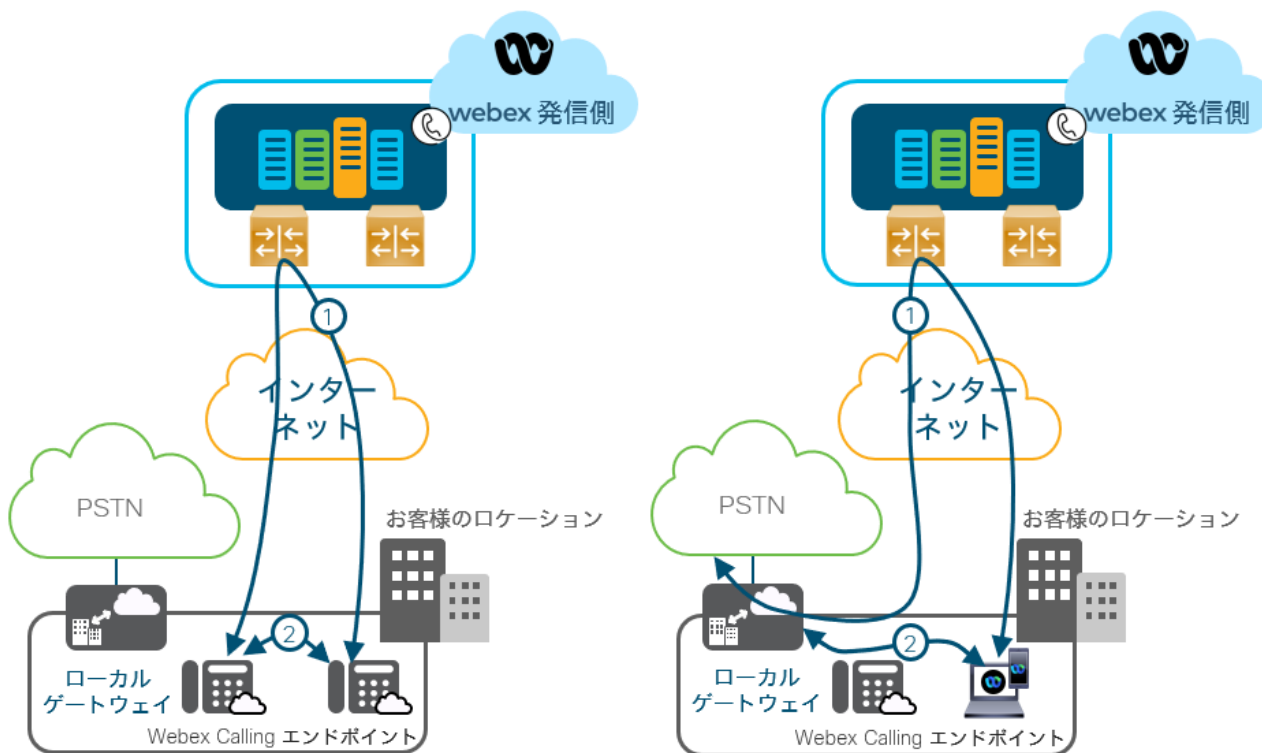
これが、接続確認が複数回実行される理由です。最初のパケットがファイアウォールによって廃棄された場合は、ファイアウォールのアウトバウンドのピンホールが各方法で開かれるため、後続のパケットが許可される可能性があります。

接続確認の結果として、両方のエンドポイントには 1 つ以上の検証済み候補のリストができます。メディアパス最適化の最適な候補を選択するために、識別された候補が候補タイプに基づいて優先順位付けされ (ホスト、ピア再帰、サーバー再帰の順)、最適なペアがネゴシエートされます。

メディアパスの最適化

コールのセットアップが SIP 200 OK メッセージで成功した直後に、メディアがフローを開始します。これは、接続確認が開始される前に発生するため、メディアは標準のパスである Webex Calling を経由します。図 29 は、ステップ 1 のこの初期のメディアパスを示しています。これは、電話から電話へ、および電話からローカルへのゲートウェイのシナリオです。

図 29 ICE ネゴシエーションが成功した後のメディアパスの変更



STUN 接続確認が成功したことが証明された後、新しいシグナリングフェーズを介してメディアを再ネゴシエートする必要があります。ICE 制御エージェントは、多くの場合に発信側エンドポイントに対応し、SIP メッセージの SDP 本文に選択された候補が含まれている re-INVITE を送信します。Webex Calling が新しい INVITE を受信すると、SDP が ICE

ネゴシエーションが成功したと判断し、SDP に独自のトランスポートアドレスを追加せずに、エンドポイントから受信した候補を使用して SDP を中継します。同様に、他のエンドポイントは、SDP メディア再ネゴシエーションの一部として選択された候補を返します。その結果、両方のエンドポイントは、ネゴシエートされたホスト、サーバー再帰またはピア再帰のトランスポートアドレスを使用するように切り替わり、エンドポイント間のメディアは Webex Calling アクセスにアンカーされなくなります。メディアの再ネゴシエーションをステップ 2 に示しています。

ICE ネゴシエーションが成功しない場合、ステップ 1 で示したように、メディアはステップ 2 に移ることなく Webex Calling ネットワークによって中継されます。

ローカルゲートウェイ ICE Lite の実装

ローカルゲートウェイは、ICE 仕様のオプションとして定義されている「Lite」の実装をサポートしています。

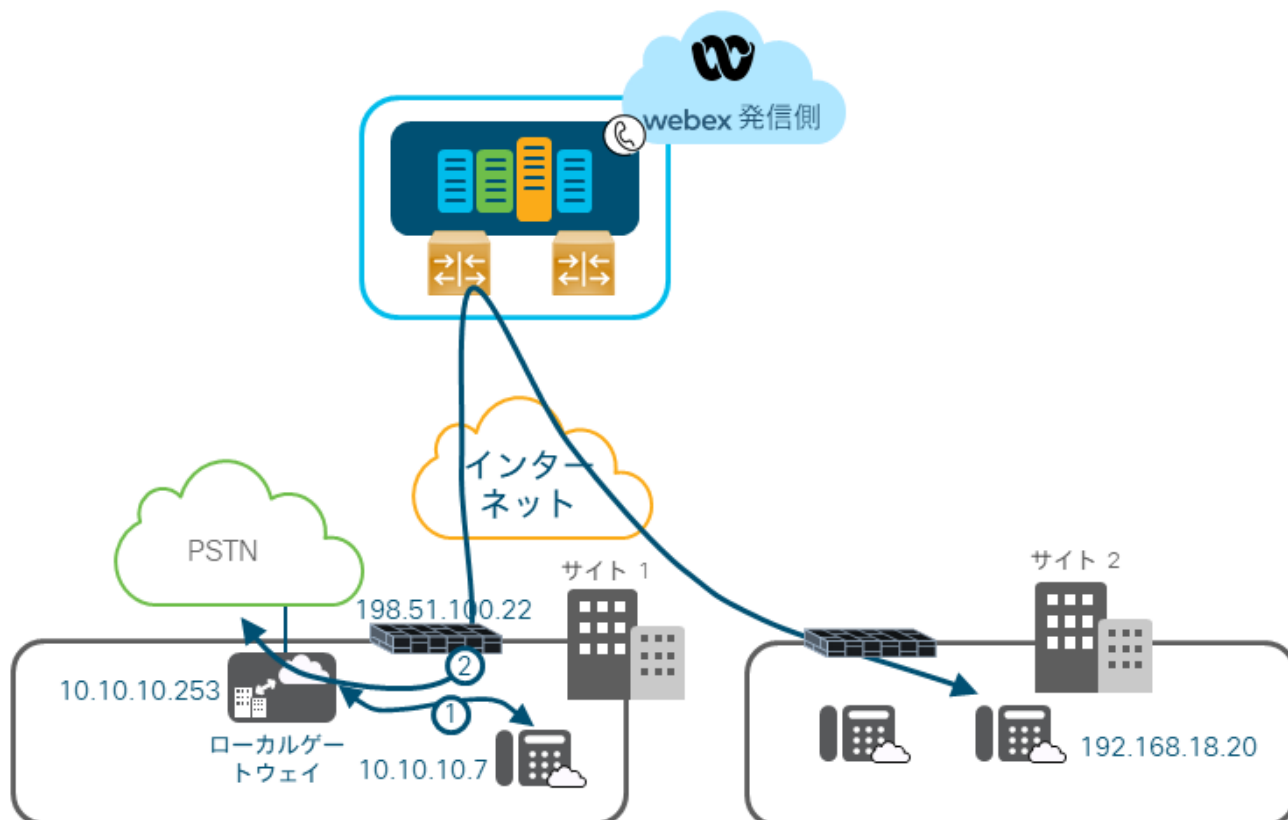
ICE Lite をサポートするデバイスには、次のような ICE の完全なデバイスとの主な違いがあります。

- STUN 手順による候補の収集を行いません。したがって、ホスト候補のみがリモートパーティにアダプタサイズされます。
- 接続確認は開始しませんが、接続確認に回答はします。
- ICE Lite を実装するシステムに複数のインターフェイスがある場合、SDP でアダプタサイズできるのは 1 つのインターフェイスだけです。

ローカルゲートウェイでの ICE-Lite の実装による影響は次のとおりです。

- 簡易実装のローカルゲートウェイはサーバー再帰候補を収集しないため、NAT で分離された分離ネットワークからローカルゲートウェイにアクセスすることはできません。これを図 30 に示しています。

図 30 ローカルゲートウェイを使用したメディアパスの最適化



次の図は、メディアがローカルゲートウェイに直接送信される、サイト 1 の IP 10.10.10.7 のエンドポイントを示しています。この場合、ローカルゲートウェイのローカルトランスポートアドレスは、エンドポイントとローカルゲートウェイ間のパスで NAT によって変換されないため、メディアの最適化が可能です。サイト 2 のエンドポイントの場合のように、ローカルゲートウェイが NAT 変換アドレスを介してのみ表示される場合、メディアは Webex Calling ネットワークを介して流れます。

ローカルゲートウェイは、ファイアウォールで着信ポートを開く必要がないように設計されています。このため、ローカルゲートウェイは内部ネットワークに展開することができます。DMZ にデュアルインターフェイスで展開され、ICE Lite が Webex Calling への発信ダイヤルピアで設定されている場合、ローカルゲートウェイには外部インターフェイスのホスト候補が含まれます。セキュリティ管理者が、内部エンドポイントがローカルゲートウェイの外部インターフェイスにアクセスすることを許可しない場合、PSTN メディアは Webex Calling を介してローカルゲートウェイに送信されます。

CUBE での ICE メディアパスの最適化は、IP-to-IP コールレグに対してのみ機能します。IP-to-PSTN (Webex Calling と CUBE 上の PSTN インターフェイス間) コールレグは、ICE メディアパスの最適化によるメリットを受けません。

侵入防御システムの要件

シグナリングとメディアの両方が暗号化されるため、シスコは、両方を許可し、ローカルゲートウェイと IP 電話に透過的に流すことを推奨します。

IPS 検査は、トラフィックがローカルゲートウェイに到達した後、Unified CM またはエンドポイントにそのまま送信される前に実行できます。IPS は、ローカルゲートウェイと UCM の間に配置する必要があります。検査を実行するには、ローカルゲートウェイと Cisco Unified CM またはエンドポイント間のトラフィックを非暗号化で送信する必要があります。この場合、ローカルゲートウェイは Webex Calling からのトラフィックを復号した後で、SIP シグナリングを Unified CM に、RTP メディアを宛先エンドポイントまたはゲートウェイに送信します。

正当なトラフィックを悪意のあるトラフィックとして識別するなど、IPS によってシステム全体の正常な動作が妨げられる場合、ローカルゲートウェイと Unified CM またはエンドポイント間のトラフィックの IPS 検査を無効にする必要があります。

コーデックの選択

Webex Calling では、プラットフォーム上のほとんどのクライアントでサポートされている Opus コーデックを使用して通話の音質を最適化しています。Opus は、Webex アプリと MPP 電話機でサポートされています。また、ローカルゲートウェイでは、オーディオ コーデック トランスコーディングの機能を持たない、つまり G.711 などの他のコーデックへの Opus の変換は実行できないエンドツーエンドのコーデックとしても、サポートされています。ただし、アナログ電話アダプタ (ATA) 、DECT 電話機では現在サポートされていません。また、ほとんどの PSTN プロバイダーではサポートされていないため、PSTN と UCM 間のコールに推奨されるコーデックは G.711 です。

一貫した通話品質のエクスペリエンスとコーデックネゴシエーションを確保するためには、ローカルゲートウェイで G.711 コーデックのみを設定し、Webex Calling を使用したすべての UCM と PSTN 間のコールで G.711 がコーデックとして選択されるように設定することを推奨します。G.729 のみをサポートしている IP PSTN プロバイダーがローカルゲートウェイを使用して Webex Calling 導入環境で PSTN との相互接続を提供する場合は、ローカルゲートウェイの音声クラスコーデック設定で G.729 と G.711 を追加することをお勧めします。

Webex アプリと Cisco phone 8800 シリーズは、H.264 コーデックを使用してビデオ品質を最適化します。H.264 コーデックは、最適化されたビデオ通話品質のために Webex アプリと Cisco phone 8800 シリーズでサポートされています。

以下に示すとおり、その他すべてのコールフローでは Opus コーデックがサポートされます。

- Webex アプリ (デスクトップ) ↔ Webex アプリ (デスクトップ)
- マルチプラットフォーム フォン ↔ マルチプラットフォーム フォン
- マルチプラットフォーム フォン ↔ Webex アプリ (デスクトップ)
- マルチプラットフォーム フォン ↔ 自動応答
- マルチプラットフォーム フォン ↔ ボイスメール
- Webex アプリ (デスクトップ) ↔ 自動応答
- Webex アプリ (デスクトップ) ↔ ボイスメール

帯域幅に関する考慮事項

Webex Calling のインターネットアクセスに必要な帯域幅を決定するには、同時コールレグ数と各コールレグに使用されるコーデックを考慮する必要があります。

表 7 に、Webex Calling の導入環境で使用可能なコールタイプ、各コールタイプに必要なコーデック、最大帯域幅を記載しています。各コールタイプに必要な音声通話の帯域幅は、次の一般的な式を使用して計算できます。

$$\text{予想される同時コール数} \times \text{各コーデックの 1 コールあたりの帯域幅} = \text{総帯域幅}$$

表 7 Webex Calling の通話タイプごとの帯域幅の計算

コールタイプ	コーデック - 帯域幅	総帯域幅
Webex アプリ/MPP 電話機 → Webex アプリ	Opus - 40 kbps	同時コール数 × 40 kbps
Webex アプリ/MPP 電話機 → MPP 電話機	Opus - 40 kbps	同時コール数 × 40 kbps
Webex アプリ/MPP 電話機 → ローカルゲートウェイ経由の PSTN	G.711 - 80 kbps	同時コール数 × 80 kbps
Webex アプリ/MPP 電話機 → Cloud Connected PSTN 経由の PSTN	G.711 - 80 kbps	同時コール数 × 80 kbps
Webex アプリ/MPP 電話機 → ローカルゲートウェイ経由の企業電話システム	G.722 - 80 kbps	同時コール数 × 80 kbps
Webex アプリ/MPP 電話機 → Webex Calling ボイスメール	Opus - 40 kbps	同時コール数 × 40 kbps

同時に必要となるコールタイプごとのネットワークスループットを合計することで、特定のサイトの予想される帯域幅要件の合計を決定できます。

すべてのコールレグは、シグナリング部分の Webex Calling アクセス SBC に常に固定されていますが、ICE が成功した場合、メディアは直接接続される可能性があります。Webex Calling の特定のロケーションに必要なインターネット帯域幅を決定するには、ロケーション間のコールだけでなく、ロケーション内のコールとそのロケーションのローカルゲートウェイとの間のコールも考慮する必要があります。たとえば 2 つの MPP 間のサイト内コールでは、ロケーションのインターネットアクセスで 2 × 40 kbps の双方向の接続が必要になります。

同時に必要となるコールタイプごとのネットワークスループットを合計することで、特定のサイトの予想される帯域幅要件の合計を決定できます。

表 8 に、すべてのデバイスが同じロケーションにある場合の合計帯域幅の計算例を示します。

表 8 Webex Calling の帯域幅の計算例

コールタイプ	同時コール数	総帯域幅
Webex アプリ/MPP 電話機 → Webex アプリ	15	$2 \times 15 \times 40 \text{ kbps} = 1,200 \text{ kbps}$
Webex アプリ/MPP 電話機 → MPP 電話機	15	$2 \times 15 \times 40 \text{ kbps} = 1,200 \text{ kbps}$
Webex アプリ/MPP 電話機 → ローカルゲートウェイ経由の PSTN	50	$2 \times 50 \times 80 \text{ kbps} = 8,000 \text{ kbps}$
Webex アプリ/MPP 電話機 → Cloud Connected PSTN 経由の PSTN	0	$0 \times 80 \text{ kbps}$
Webex アプリ/MPP 電話機 → ローカルゲートウェイ経由の企業電話システム	15	$2 \times 15 \times 80 \text{ kbps} = 2,400 \text{ kbps}$
Webex アプリ/MPP 電話機 → Webex Calling ボイスメール	5	$15 \times 40 \text{ kbps} = 200 \text{ kbps}$
合計コール数/総帯域幅	100 コール	12,000 kbps/12 Mbps

ビデオ通話帯域幅の場合、Webex アプリと 8800 MPP 電話機は、1 通話あたりの最大帯域幅 1,500 kbps で最大解像度 720p の H.264 ビデオをサポートします。ただし、通話中に消費される帯域幅の量は、ビデオ通信に固有の可変ビットレートに基づいて変動します。

表 9 Webex Calling の通話タイプごとの帯域幅の計算

ビデオ通話の種類	コーデック - 帯域幅	総帯域幅
Webex アプリ/MPP 電話機 → Webex アプリ/MPP 電話機	H.264 - 1,500 kbps	同時コール数 × 1,500 kbps

表 10 同じロケーション内での Webex Calling ビデオ帯域幅の計算

ビデオ通話の種類	同時ビデオ通話数	総帯域幅
Webex アプリ/MPP 電話機 → Webex アプリ/MPP 電話機	10	$2 * 10 * 1,500 \text{ kbps} =$ 30,000 kbps
合計コール数/総帯域幅	10 回の通話	30,000 kbps / 30 Mbps

注：上記の帯域幅の計算は、コーデックの正味ビットレートに基づいています。インターネットアクセスのシグナリング帯域幅と L3 帯域幅を決める場合は、オーバーヘッドを考慮する必要があります。

ICE および ICE Lite が有効になっている場合、帯域幅は LAN/WAN ネットワークでのみ消費される場合があります。ただし、ICE 通話の初期設定では、パスの最適化が行われる直前にメディアストリームが数秒間 Webex に送信されることに注意してください。したがって、Webex への合計帯域幅を決定するには、同時通話の数が依然として重要です。ただし、同時通話数は、ICE 以外の場合よりもはるかに短い期間で計算されるため、数が減少します。たとえば、会社がピーク時に ICE を使用しないインターネットに対して合計 4 Mbps の 100 の同時通話があると判断した場合、ICE を使用すると、通話の最適化が数秒後に行われるため、この数が減少し、インターネット帯域幅が解放されます。

ディレクトリ統合

Webex Calling ディレクトリは、Control Hub の [ユーザー (User)] メニューの一部として表示されます。ユーザーを Control Hub にインポートするには、いくつかの方法があります。

- Directory Connector を介してオンプレミスの Active Directory からユーザーを同期する
- Okta や Azure AD などのクラウドベースのディレクトリからユーザーを同期する
- Control Hub または CSV ファイル経由でユーザーを手動で追加する
- People API 経由でユーザーを追加する（このオプションでは、カスタマイズされたプロビジョニングシステムの一部として API を使用する必要があります）

Cisco Directory Connector は、ディレクトリを Webex クラウドと同期します。これにより、管理者は Active Directory 内のユーザーアカウントとデータを維持できます。オンプレミス側の変更は自動的にクラウドに複製されます。

Azure AD や Okta などのクラウドベースのディレクトリには、Directory Connector は必要ありません。ユーザー同期は、Control Hub とクラウドベースのディレクトリの両方で構成されています。

Control Hub インターフェイスから CSV ファイルをインポートすることで、手動でユーザーのプロビジョニングを行うこともできます。

Cisco Directory Connector に関連するドキュメントは、

https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cloudCollaboration/spark/hybridServices/directoryconnector/cmqt_b_directory-connector-guide-admins.html にあります。

ユーザーは、<https://settings.webex.com> ページのエンドユーザーポータルから連絡先を追加し、ユーザーディレクトリを検索できます。

ダイヤルプラン

Webex Calling でユーザが有効になると、そのユーザは特定のロケーションに割り当てられ、そのロケーション内でユーザの内線番号が設定されます。オプションで、事前に定義された使用可能な電話番号のプールから電話番号 (DID) をユーザに割り当てることもできます。電話番号のプールは、Webex Control Hub で定義されます。すべての電話番号は、その到達可能性を確立するために、PSTN プロバイダを介して割り当てられ、お客様の正しい PSTN トランクにルーティングされるか、クラウド PSTN プロバイダ (Cisco または Cloud Connected PSTN プロバイダ) を介して割り当てられる必要があります。

PSTN 接続先

Webex Calling ユーザーは、PSTN 接続先にダイヤルする際、ロケーションが割り当てられている国の一般的な PSTN ダイヤル手順を使用できます。たとえば米国のロケーションから米国内の PSTN 接続先にコールを発信する場合は、10 桁 (「1」の後に 10 桁) または 7 桁をダイヤルします。7 桁の番号をダイヤルすると、ダイヤルされた番号の前にロケーションのメイン番号の NPA が Webex Calling によって自動的に付加されます。同様に、海外の宛先の場合は「011」の後に完全な E.164 番号をダイヤルします。また、Webex Calling ユーザーは +E.164 ダイヤル (「+」の後に E.164 番号をダイヤル) を使用できます。

PSTN アクセスコード

オプションで、ロケーションごとに PSTN 発信ダイヤル番号を定義することができます。これは「PSTN アクセスコード」と呼ばれます。通常、PSTN アクセスコードは他のオンネットダイヤル手順との重複を避けるために企業環境で使用されます。米国では一般的に、PSTN アクセスコードとして「9」が使用されます。

たとえば、米国のロケーションの PSTN アクセスコードとして「9」が定義されている場合、米国内の宛先には「9」の後に 10 桁、「91」の後に 10 桁、または 7 桁 (同じ NPA 内の番号) をダイヤルします。国際電話の場合は「9011」の後に完全な E.164 番号をダイヤルします。

短縮オンネットダイヤル

短縮オンネットダイヤルの場合は、Webex Calling のお客様ごとにルーティングプレフィックス長、内部ルーティングプレフィックス、内線番号の長さを設定する必要があります。

- ルーティングプレフィックス長：各ロケーションに設定するすべてのルーティングプレフィックスの長さを定義します。
- 内部ルーティングプレフィックス (ステアリング桁)：すべてのロケーションのルーティングプレフィックスに共通する最初の数字です。
- 内線番号の長さ：各ロケーションで使用する内線番号の長さを定義します。

この 3 つを設定することにより、次の形式で、サイト間のオンネットダイヤル手順が定義されます。
<internal routing prefix>-<site code>- 内線番号。

たとえば、内部ルーティングプレフィックスを「8」、ルーティングプレフィックス長を 4、内線の長さを 4 に設定した場合、すべてのオンネット宛先に「8-XXX-XXXX」の形式でダイヤルできます。この場合、先頭の「8」とそれに続く 3 桁の数字がロケーションのプレフィックスです。最後の 4 桁はロケーション内で定義された内線番号です。

設定するルーティングプレフィックス長には、内部ルーティングプレフィックスが含まれることに注意してください。つまり、3 桁のサイトコードを使用するには、ルーティングプレフィックス長を 4 に設定する必要があります。

ルーティングプレフィックスを「8」、ルーティングプレフィックス長を 4 と設定した場合、ロケーションのルーティングプレフィックスの定義には必ず先頭の「8」が含まれます。

ロケーションのルーティングプレフィックスを設定する際は、[ダイヤル時の遅延を減らすために、グローバルコール設定のステアリング桁 8 と一致するルーティングプレフィックスを入力して保存してください。 (Enter and save a routing prefix that aligns with global Call Settings steering digit 8 to reduce delays in dialing.)] という警告が表示され、管理者にこの要件が通知されます。

表 11 拠点間短縮オンネットダイヤルの設定例 (ステアリング桁は 8、ルーティングプレフィックス長と内線の長さは両方とも 4)

サイト	サイトコード	ロケーションプレフィックス	内線番号の範囲	短縮オンネットダイヤル
SJC	140	8140	4000 ~ 4999	81404XXX
NYC	121	8121	4000 ~ 4999	81214XXX
RTP	191	8191	1000 ~ 1999	81911XXX

表 11 は、サイトコード、内部ルーティングプレフィックス「8」、ルーティングプレフィックス長 4 桁、内線番号の長さ 4 桁が設定された 3 つのサイトの例を示しています。また、各サイトの宛先への、サイト間短縮オンネットダイヤルも記載されています。

SJC と NYC で使用する内線番号の範囲は同じですが、この 2 つのサイトの宛先へのサイト間短縮オンネットダイヤル手順は一意です。サイトコードはすべて 3 桁で、ステアリング桁「8」と合わせて 4 桁のロケーションプレフィックスになります。

上記のとおり、サイト間短縮オンネットダイヤル用に固定桁数を定義することで、Webex Calling が Webex Calling デバイスにダイヤルプランを送ることができるようになります。オフックされると、電話機はこのサイト間短縮オンネットダイヤル手順を認識し、すぐに番号の収集を停止して、番号分析とコールルーティングを行うためにダイヤルされた番号を Webex Calling に送信します。

サイト間短縮オンネットダイヤル用の固定桁数を設定することは、桁間タイムアウトの待ち時間の回避と、全体的なユーザエクスペリエンスの向上に役立ちます。

Unified CM からオンプレミスの Unified CM へのコールと正しいコールタイプの分類を有効にするには、少なくとも 1 つのダイヤルプランを Webex Calling で設定し、Unified CM に登録されているすべてのエンタープライズおよび +E.164 の番号範囲について、そのダイヤルプランでそれぞれの +E.164 および ESN パターンを設定する必要があります。これにより、Unified CM への Unified CM 接続先の正しいルーティングが保証されるだけでなく、トランクから Webex Calling が受信したコールについて、発信者 ID の一致に基づいて、そのコールがオンプレミスまたは PSTN コールとして正しく分類されるようになります。

音声の統合

Webex Calling の統合された音声により、Webex Meetings と Webex Calling の両方のサブスクリプションを持っている組織は、Webex Meetings 音声への最適化されたコールルーティングパスを利用できます。コールインまたはコールバックオプションを使用して Webex ミーティングに参加する場合、通話は Webex 内に留まり、PSTN 経由でルーティングされる通話数を減らすことで組織のコストを節約できます。設計の詳細については、Webex Edge Audio の「優先アーキテクチャ」: <https://www.cisco.com/c/dam/en/us/td/docs/solutions/PA/WbxEdge/PAEdgeAudio.pdf> を参照してください。

サービスアシュアランス

サービスアシュアランスとは、お客様、パートナー、シスコが Webex Calling の導入を適切に実施して管理するためのツール群のことを指します。

CScan は、初期導入時のトラブルシューティングや、Webex Calling コールの健全性のモニタリングに使用できます。

CScan

Cscan は、Webex Calling 用に設計されたネットワークの接続状況を確認するためのツールです。お客様とパートナーは、Cscan を使用してインターネット経由のネットワーク接続をテストできます。

接続をテストするには、cscan.webex.com に移動し、ユーザの（ユーザに最も近い）ロケーション（Webex Calling のデータセンターの 1 つ）を選択します。ユーザーは、インターネット接続をテストする基本的なテストを実行できます（遅延、ダウンロードとアップロードの速度、Webex Calling に必要なポートに関する情報が提供されます）。高度な診断オプションでは、QoS パラメータに関する追加の詳細情報（ジッター、パケット損失、遅延など）が提供されます。

Cscan の使用の詳細については、Webex のヘルプページ (<https://help.webex.com/ja-ip/v27bei/Use-CScan-to-Test-Webex-Calling-Network-Quality>) を参照してください。

分析

Webex Control Hub での分析

管理者は、Webex Control Hub の [分析 (Analytics)] ページを使用して、最大 13 ヶ月分の Webex Calling データの履歴を表示できます。組織に Pro Pack がある場合、管理者は Webex アプリに基づく通話の 13 ヶ月分のデータにもアクセスできます。組織に Pro Pack がない場合、管理者は Webex アプリに基づく通話の 3 ヶ月分のデータにアクセスできます。

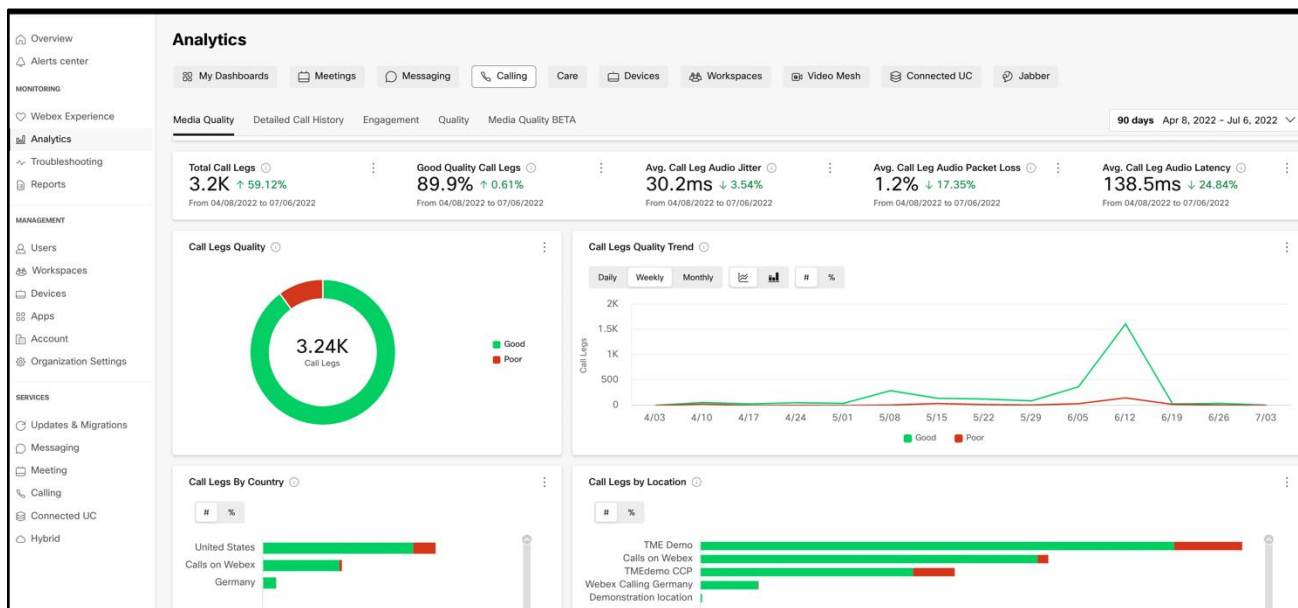
シスコは、Webex Calling デスクフォン、Webex App アプリ（デスクトップおよびモバイル）、および Webex Calling アプリ（デスクトップおよびモバイル）に関連する通話の履歴データを保持します。

メディア品質分析

Control Hub の [メディア品質 (Media Quality)] ダッシュボードを使用すると、組織全体で Webex 通話と Webex 通話の品質を簡単に管理できます。高レベルの重要業績評価指標 (KPI) により、管理者は全体的な通話品質をすばやく確認できます。チャートには、ロケーション、IP アドレス、メディアタイプ、接続タイプ、コーデック、エンドポイントタイプ、および IP 電話モデル別のデータの詳細なビューが表示されます。

データもほぼリアルタイムで更新されるようになりました。管理者は、通話が終了してから 15 分以内に通話品質データを確認できます。

図 31 Webex Calling メディア品質分析

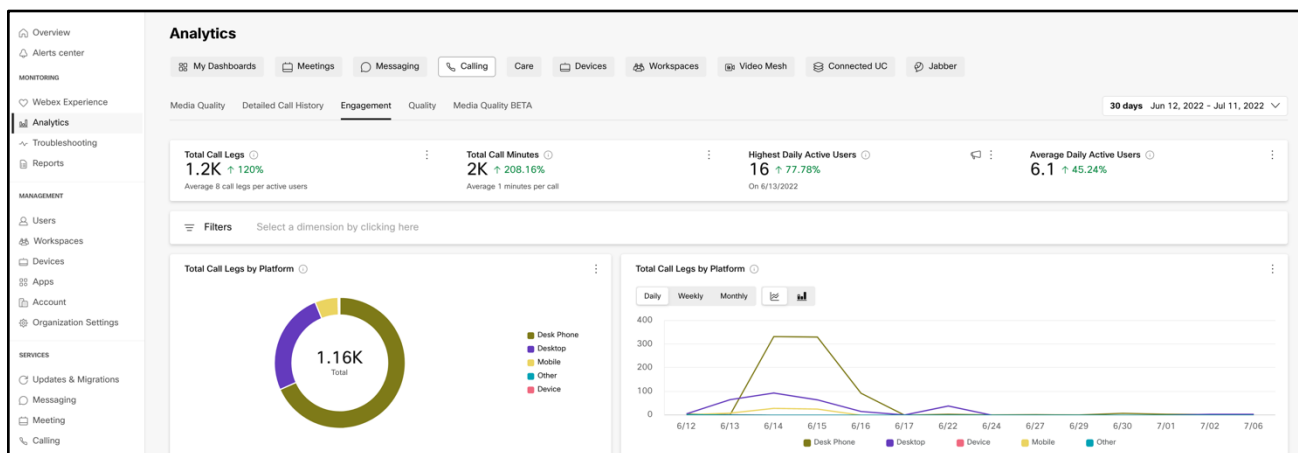


管理者は、Webex Calling 通話の品質メトリックと対応業務分析の詳細も取得できます。コールの使用状況とエンゲージメントについての履歴データを、メディアの品質に関する記録を含めて表示することが可能です。Webex Calling 分析は、Control Hub の [分析とコール (Analytics and Calling)] で利用できます。

エンゲージメント分析

エンゲージメント分析では、コール件数とコール時間 (分) に関する情報がグラフで表示され、組織内で行われたすべてのエンドポイント間のコールの詳細が示されます。

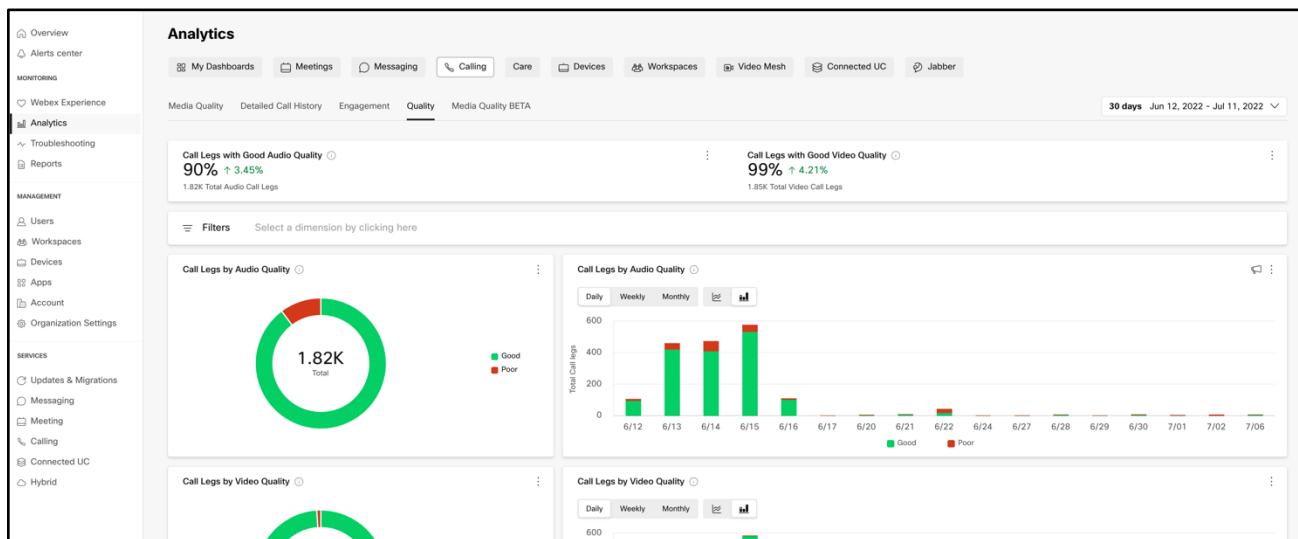
図 32 Webex Calling の対応業務分析



品質分析

[品質分析 (Quality Analytics)] タブでは、管理者が各コールの記録を表示し、スライダを使用して品質統計情報に基づいてコールをフィルタリングできます。

図 33 Webex Calling の品質分析



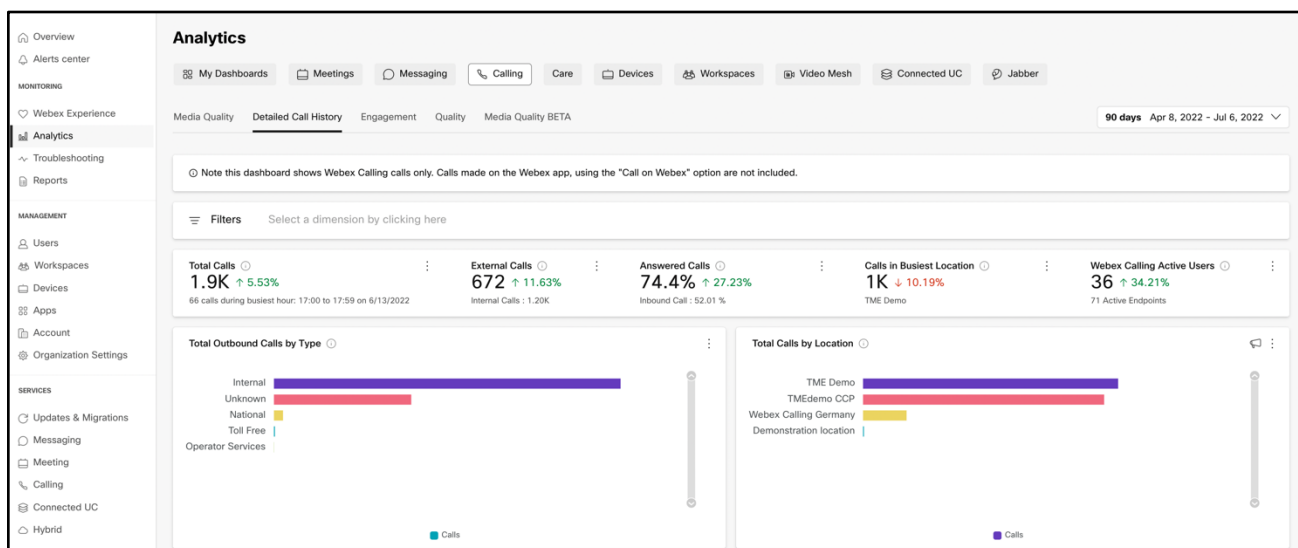
すべての統計情報がデバイス/エンドポイントから直接収集されるため、QoS パラメータ（パケット損失、ジッター、遅延）にはエンドユーザから見たコールエクスペリエンスが反映されます。

詳細な通話履歴

管理者は、Webex Control Hub の [分析 (Analytics)] タブで [詳細なコール履歴 (Detailed call history)] を選択することで通話詳細レコードを取得できます。

現在の日付から最大 12 か月のコール詳細レコード (CDR) を使用して、ユーザーのコール動作パターンを特定できます。

図 34 Webex Calling の詳細な通話履歴



トラブルシューティング

Control Hub からの Webex Calling のトラブルシューティングビューにより、管理者は、Webex 通話のメディア品質問題をトラブルシュートできます。管理者は、通話関連情報を検索したり、メディア統計を表示したり、問題が発生した場所を特定したり、問題を解決したりできます。

管理者は、次の条件を使用して検索し、少なくとも 1 つの Webex Calling 登録済みエンドポイントでメディアセッションが利用された通話のリストを取得できます。

- 電子メール ID
- 電話番号（文字列完全一致）
- MAC アドレス
- 通話 ID

図 35 Webex Calling のトラブルシューティング

Quality	Service	Start Time	Meeting / Caller	Name	Host / Caller	Participants	Duration	Site / Location	Conference / Call ID
Poor		2022-07-02 05:40:05 PM	+14085558513	Rodrigo Ayala Lobato + Roth Bridges	Rodrigo Ayala Lobato	2	00:48	TME Demo	SSE224005035020722-1883643452...
Poor		2022-07-02 05:38:32 PM	+14085558513	Rodrigo Ayala Lobato + Roth Bridges	Rodrigo Ayala Lobato	2	01:28	TME Demo	SSE223832139020722-225097212...
Poor		2022-07-01 01:31:12 PM	+14085558513	Rodrigo Ayala Lobato + 2597951018...	Rodrigo Ayala Lobato	2	00:21	TME Demo	SSE183112660010722-384109194...
Good		2022-07-01 10:43:10 AM	+14085558513	Rodrigo Ayala Lobato + roayatal@cisc...	Rodrigo Ayala Lobato	2	00:03	TME Demo	SSE154310736010722-209806021...
Good		2022-07-01 10:11:44 AM	+14085558513	Rodrigo Ayala Lobato + roayatal@cisc...	Rodrigo Ayala Lobato	2	00:13	TME Demo	SSE151144163010722-561200367...
Good		2022-06-30 05:42:51 PM	+14085558513	Rodrigo Ayala Lobato + roayatal@cisc...	Rodrigo Ayala Lobato	2	00:16	TME Demo	SSE224251456300622-1532979062...
Poor		2022-06-30 05:37:17 PM	+14085558513	Rodrigo Ayala Lobato + roayatal@cisc...	Rodrigo Ayala Lobato	2	00:19	TME Demo	SSE223717729300622-1310167214...

メディア品質のトラブルシューティングにより、管理者は次のことができます。

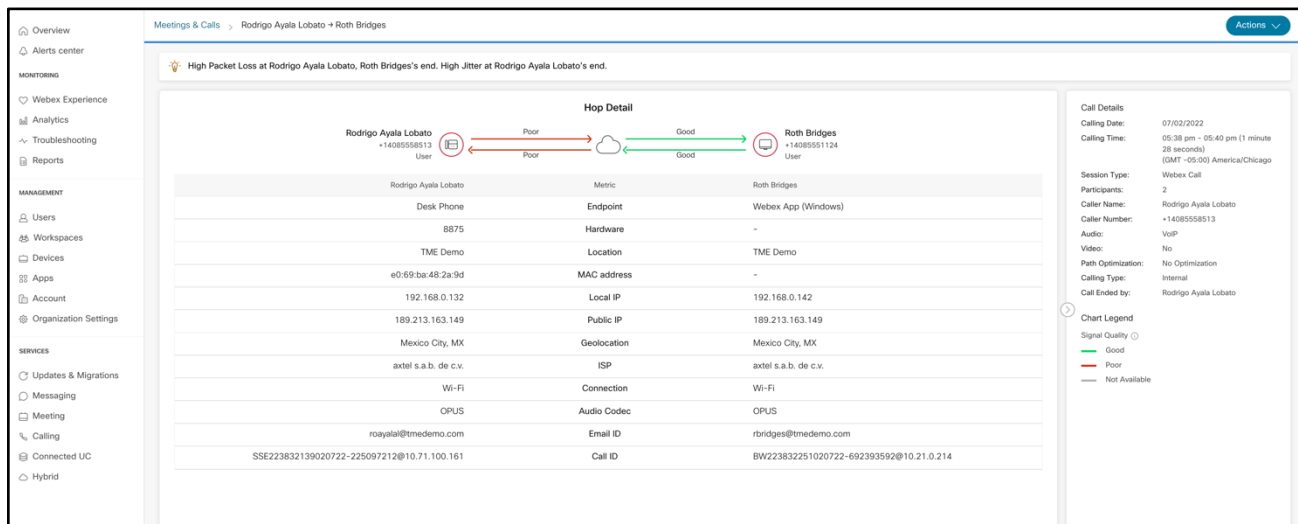
- 通話参加者のエンドツーエンドのエクスペリエンスの表示。
- 通話のホップ詳細の表示
- メディアが Webex Calling クラウドを通過するか、ユーザー間の直接接続かを表示（Interactive Connectivity Establishment (ICE) を使用）。
- 過去 21 日間の通話を表示。
- ユーザーのエクスペリエンスに影響を与えた通話品質のメトリックを分析。たとえば、管理者は、Wi-Fi ネットワークに接続されているクライアントで高いジッターが観測される場合がありますが、パケット損失と遅延は許容できる場合があります。
- 問題が発信者にあるのか着信者にあるのかを検出。

Control Hub のトラブルシューティングでサポートされるコールフロー

メディア品質レポートは、発信者、着信者エンドポイントおよびメディアリレーポイントから収集されます。これにより、メディアエクスペリエンスのセグメンテーションを絞り込んで、問題が次の場所で発生したかどうかを特定できます。

- 発信者または着信者
- Webex Calling クラウドとの間のメディア パス

図 36 Webex Calling トラブルシューティング ホップの詳細



トラブルシューティングの使用の詳細については、Webex ヘルプ ページ : <https://help.webex.com/en-us/article/fr11efb/Troubleshoot-Webex-Calling-Media-Quality-in-Control-Hub> を参照してください。

Webex Calling 専用インスタンス

専用インスタンスは、シスコのコラボレーションテクノロジーである Webex Calling および Cisco Unified Communications Manager (Cisco UCM) ベースのアーキテクチャによって強化された、シスコの Cloud Calling ポートフォリオの一部です。このサービスは、Cisco IP 電話、モバイルデバイス、デスクトップクライアントの機能と利点を備え、音声、ビデオ、メッセージ、ボイスメール、会議およびモバイルソリューションを提供します。専用インスタンスは Webex Calling と統合されているため、お客様は UC Manager のエクスペリエンスを維持しながら Webex プラットフォームのエクスペリエンスを活用できます。カスタマイズされたクラウドベースの企業レベルの機能が必要なお客様は、専用インスタンスを展開し、豊富な Webex Calling 機能をインストールベースに提供できます。

専用インスタンスは、シスコにより Webex データセンターの北米、欧州、アジア太平洋、オーストラリア地域でホストおよび運用されています。シスコ Webex データセンターはグローバルに分散していて、各地のデータセンターは地理的に冗長化されています。

専用インスタンス UC アプリケーション

専用インスタンスには、次のアプリケーションが含まれています。

- Cisco Unified Communications Manager
- Cisco Unified Communications Manager IM & プレゼンス サービス
- Cisco Unity Connection
- Cisco Expressway
- Cisco Emergency Responder (AMER のみ)

専用インスタンスは、すべての UC アプリケーションに対して 1 つのクラスターで展開され、必要に応じて拡張することにより、Webex Calling サブスクリプションで購入した追加のユーザーに対応できます。追加のキャパシティが必要な場合、お客様は追加のクラスターを柔軟にリクエストできます。これは、サービスリクエスト (SR) を開くことにより可能です。

専用インスタンス アプリケーションはクラウドベースのソリューションですが、構成ガイドラインとベスト プラクティスは、オンプレミスシナリオに展開されたものと同様です。UC アプリケーションのベスト プラクティスについては、<https://www.cisco.com/c/en/us/td/docs/solutions/CVD/Collaboration/enterprise/14/collbcvd/control.html> の「コラボレーション企業 CVD」を参照してください。

シスコは、マルチテナントと専用インスタンスの間に SIP トランクを作成します。パートナー/お客様は、既存のダイヤルプランを取り込み、内部ダイヤル用プラットフォームに接続できます。

シスコは、Webex Calling マルチテナントおよび専用インスタンスの展開でトランクを事前に構成します。パートナーとお客様は、最小限の構成で既存のダイヤルプランをプラグインできます。

マルチテナントおよび専用インスタンス アプリケーションは、クラウドにデプロイされたゲートウェイを介して通信します。次の構成は、マルチテナントと専用インスタンスの両方の展開で (Cisco によって) 行われます。

マルチテナント：

- 相互接続のためのロケーション
- リージョン DC のゲートウェイへの 2 つの冗長構成済み SIP トランクとマルチテナントへの登録
- 2 つのトランクを含むように事前構成されたルートグループ

専用インスタンス :

- 各地域のデータセンターでゲートウェイをプロビジョニング
- 事前に Unified CM に構成された SIP ゲートウェイへの トランク
- ゲートウェイへの 2 つの トランクを含む RG (ルートグループ)
- それぞれの RG への RL (ルートリスト)

注 : パートナー/お客様は、マルチテナントまたは専用インスタンスの展開で事前構成された トランクを削除しないでください。これは、内部通話の動作に影響するためです。専用インスタンスの基本構成の詳細については、<https://help.webex.com/en-us/article/2vpf1/Dedicated-Instance-for-Webex-Calling---Base-Configuration> を参照してください。

専用インスタンスピアリング (接続)

ピアリングは、専用インスタンスネットワークと、専用インスタンス コラボレーション サービスとの通信を可能にするパートナーまたはお客様のネットワーク間の相互接続です。お客様は、パートナーと一緒にオンボーディングするか、直接接続オプションを使用してシスコに直接オンボーディングします。これは、地理的エリアごとに一度実行される必須のプロセスです。

ピアリングは以下を確立します。

- パートナー管理および運用ネットワーク
- パートナーの顧客アグリゲーション フレームワーク
- それぞれのプライベート専用インスタンスへのお客様によるアクセス
- パートナーの補足サービスフレームワーク
- お客様へのクラウドベースのソフトウェアサービスとマネージドサービス

ピアリングリンクが確立されると、パートナーは、1 つ以上のお客様、管理ネットワーク、およびオーバーザトップ (OTT) クライアントまたは MRA クライアントのインターネットアクセスのトラフィックを論理的に分割できます。

ピアリング後、パートナーは専用インスタンスで次のサービスにアクセスできます。

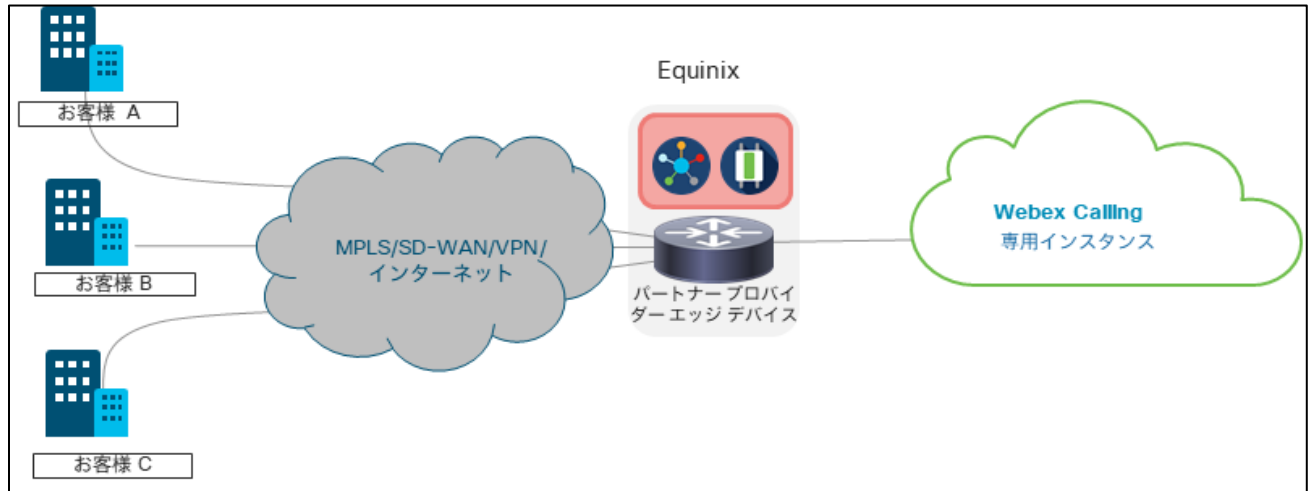
- 専用インスタンスのアプリケーション管理インターフェース
- 運用ツール - アシュアランスポータル、RTMT
- プロビジョニングツール (オプション)
- レポート
- API アクセス

パートナー接続ピアリング

パートナー接続ピアリングモデルでは、パートナーはお客様の WAN を集約して、サービスを提供する各地域の専用インスタンスに接続します。

パートナー接続モデルでは、1 GB または 10 GB のシングルモードファイバを使用して、各物理的な場所に Equinix プレゼンスと直接接続する必要があります。パートナーの機器は、個別の VRF の dot1q タギングを使用したレイヤー 3 サブインターフェイスをサポートする必要があります。パートナーは、ロケーションごとに 1 つまたは 2 つのデバイス (レイヤー 3 WAN ルーターなど) を展開できます。パートナーは、提供されたすべての接続 (顧客、管理、インターネット、PSTN) を集約します。パートナーは、顧客のネットワーク アクセス オプション (MPLS、SD-WAN、VPN、またはインターネット) も定義します。

図 37 専用インスタンスパートナー接続



Webex Edge Connect

Webex Edge Connect ピアリングは、パブリックインターネットをバイパスし、Equinix 経由でネットワークを Cisco Webex データセンターの場所に接続するプライベート ポイントツーポイント リンクです。お客様は、専用のマネージド型冗長 IP リンクをお客様の WAN から専用インスタンスに接続します（通話ワークロードのみ）。お客様は、Equinix クラウドエクスチェンジ経由で Webex バックボーンに WAN を接続します。Webex Edge Connect は、Webex クラウドサービスに直接接続と専用の高速帯域幅を提供します。

ピアリングは、200 MB から 10 GB の帯域幅オプションを備えた Equinix Cloud Exchange (ECX) ファブリックローケーションを介して行われます。

Equinix は、ピアリングポイントから専用インスタンス データ センターへのネットワークフローを処理します。Equinix は、物理接続と各仮想接続に対して課金します。

Webex Edge Connect に関する詳細は、

https://www.cisco.com/c/dam/en/us/td/docs/solutions/PA/EdgeConnect/PA_Edge_Connect_Design.pdf にある「Webex Edge Connect 優先アーキテクチャ」を参照してください。

図 38 カスタマー接続ピアリング : Webex Edge Connect

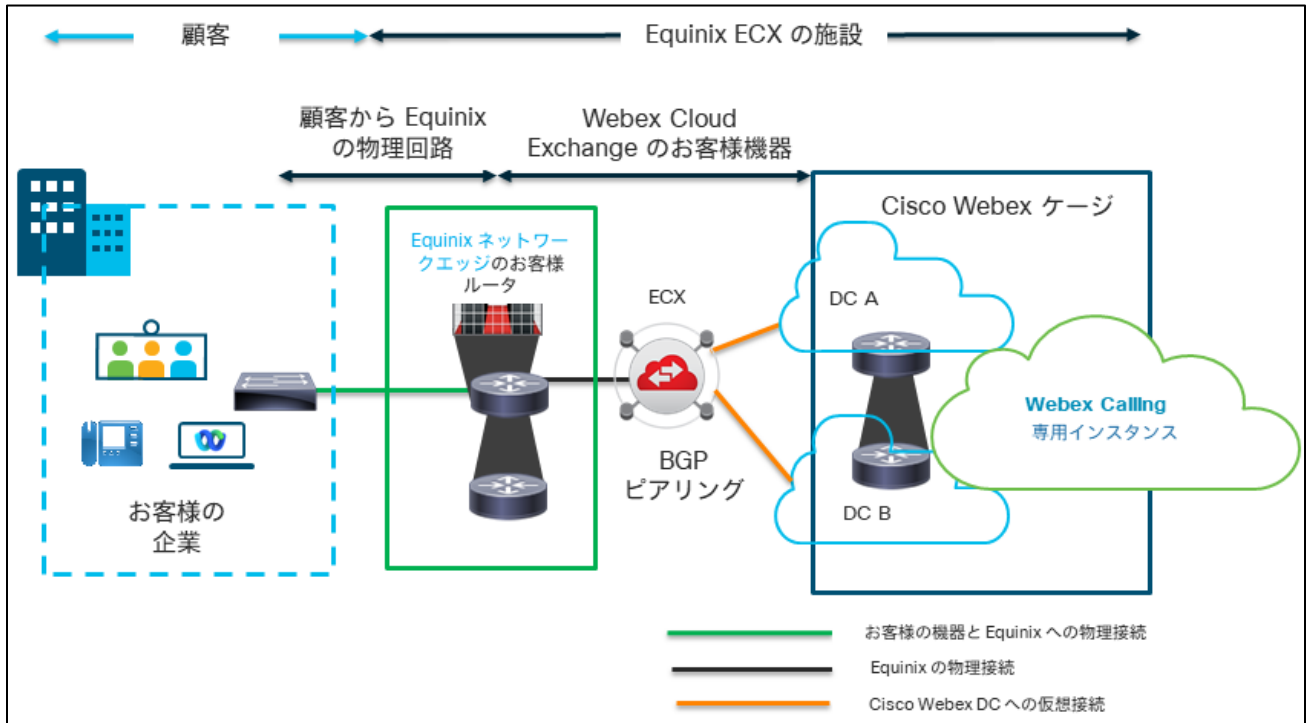


図 38 に示すように、お客様は Equinix と ECX ファブリックを介して Cisco Webex バックボーンに接続します。お客様は、ネットワークから Equinix への物理的な接続を保持し、次に、地域ごとに 2 つの仮想回線をシスコデータセンターに接続します。

仮想接続 (VPN)

仮想接続は、専用インスタンスへのクラウド接続用の追加アドオンオプションです。仮想接続により、お客様はポイントツーポイントの IP VPN トンネルを使用して、インターネット経由でプライベートネットワークを安全に拡張できます。この接続オプションを使用すると、既存の Customer Premise Equipment (CPE) とインターネット接続を使用してプライベートネットワーク接続を素早く確立できます。

仮想接続には、トンネルあたり 250 Mbps の帯域幅制限があり、小規模な展開に推奨されます。2 つのポイントツーポイント VPN トンネルが使用されるため、クラウドへのすべてのトラフィックはお客様のヘッドエンド CPE を通過する必要があるため、多くのリモート拠点がある場所には適さない場合があります。ただし、ユーザーがリモートにいるほとんどの場合、モバイルおよびリモートアクセスを展開できるため、仮想接続回線の帯域幅の影響が軽減されます。

図 39 Customer Connected ピアリング：仮想接続

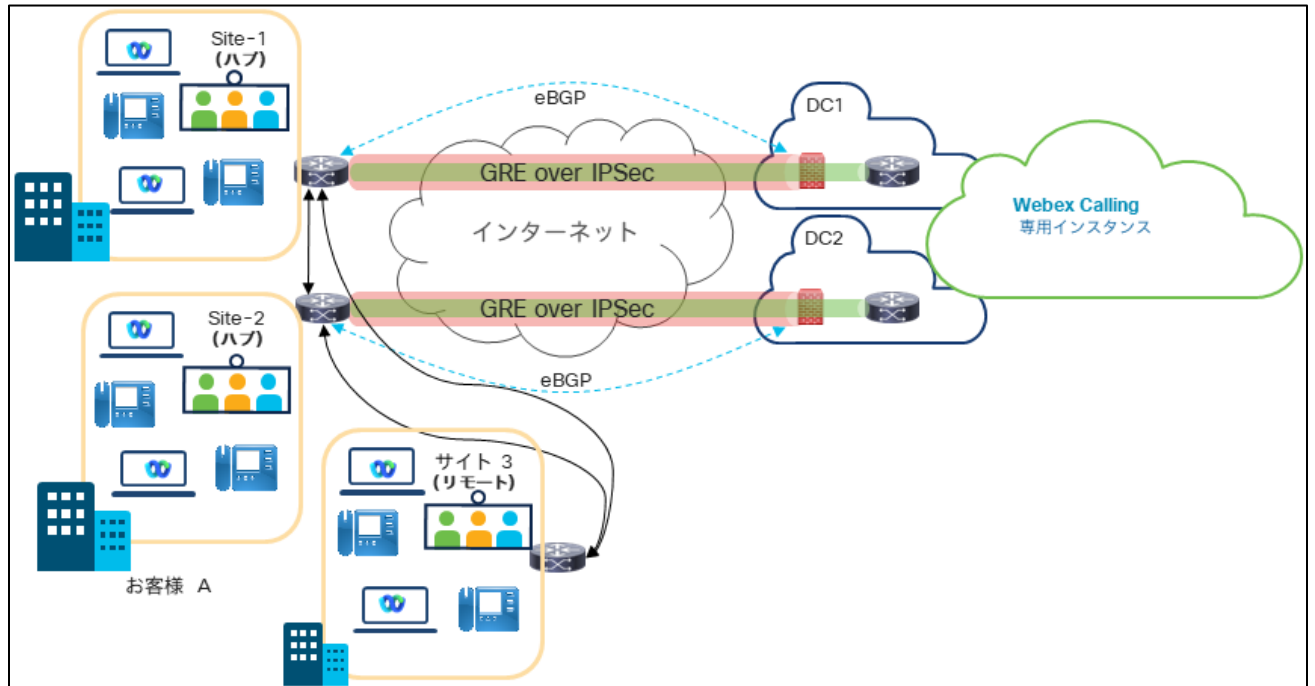


図 39 に示すように、冗長性を高めるために 2 つのハブ拠点推奨されますが、2 つのトンネルを持つ 1 つのハブ拠点もサポートされている展開モデルです。

専用インスタンス（オンプレミス-オンプレミス）に登録されたエンドポイント間の通話の場合、メディアはお客様の LAN/WAN 内を流れます。

メディアは、次のシナリオでオンプレミスエンドポイントの専用インスタンスのトンネルを通過します。

- CCP PSTN（Webex Calling での CCP PSTN の活用）
- WxC から専用インスタンスエンドポイントへの発信、およびその逆
- Webex ミーティングのオンネット SIP トランクを利用した統合音声

さらに、WxC と専用インスタンス間の通話は常に Webex データセンターを経由します。

仮想接続についての詳細は、https://help.webex.com/en-us/article/v8ihcv/Dedicated-Instance-Virtual-Connect#Cisco_Concept.dita_a94968f5-46a9-4b47-9250-ce51169b33e3 にある「専用インスタンス—仮想接続のドキュメント」を参照してください。

専用インスタンスの PSTN オプション

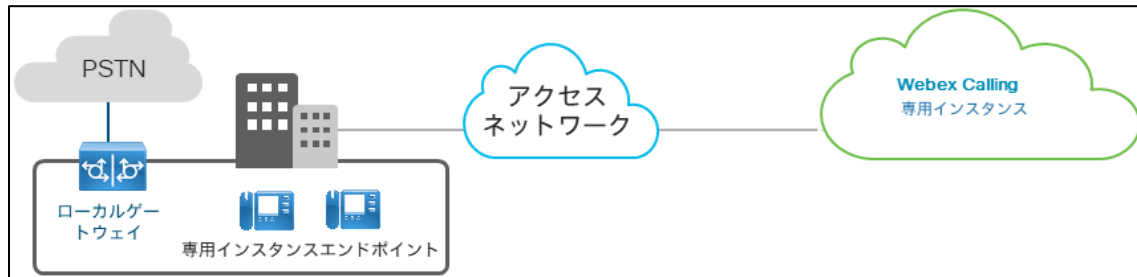
- 専用インスタンスのお客様は、次のいずれかのオプションを使用して PSTN にアクセスできます。
- お客様のオンプレミスにあるローカルゲートウェイ（ローカルブレイクアウト）
- パートナーがホストするローカルゲートウェイ（バンドルされた PSTN）
- CCPP（Cloud Connected PSTN プロバイダー）

ローカルゲートウェイ（ローカルブレイクアウト）

ローカルゲートウェイ機能は、お客様またはパートナーのオンプレミスに展開されます。ローカルゲートウェイは専用インスタンスにトランクとして登録し、PSTN と専用インスタンス間のすべての通話をルーティングします。

ローカルゲートウェイは、同じルータ上の PSTN トランク（TDM または IP）を終端して PSTN に直接接続するか、SIP トランクを介して既存の PSTN ゲートウェイに接続します。シスコの Voice ゲートウェイまたは Cisco Unified Border Element（CUBE）エンタープライズで実行されるローカルゲートウェイ機能を使用して通話を PSTN にルーティングできます。

図 お客様専用ローカルゲートウェイの展開



PSTN アクセスと専用インスタンスへの接続を組み合わせることで、お客様のネットワークに設置して保守する必要があるハードウェア (CUBE) の数は少なくなります。拠点を専用インスタンスに移行した後に既存の PSTN ゲートウェイを使用する場合は、両方の機能を別々のデバイスに実装することを推奨します。

パートナーがホストするローカルゲートウェイ (バンドルされた PSTN)

パートナーは、それぞれのお客様のネットワークに個別のローカルゲートウェイを展開する代わりに、パートナーのデータセンターでお客様のローカルゲートウェイをホストすることもできます。

図 39 パートナーがホストするローカルゲートウェイ オプション

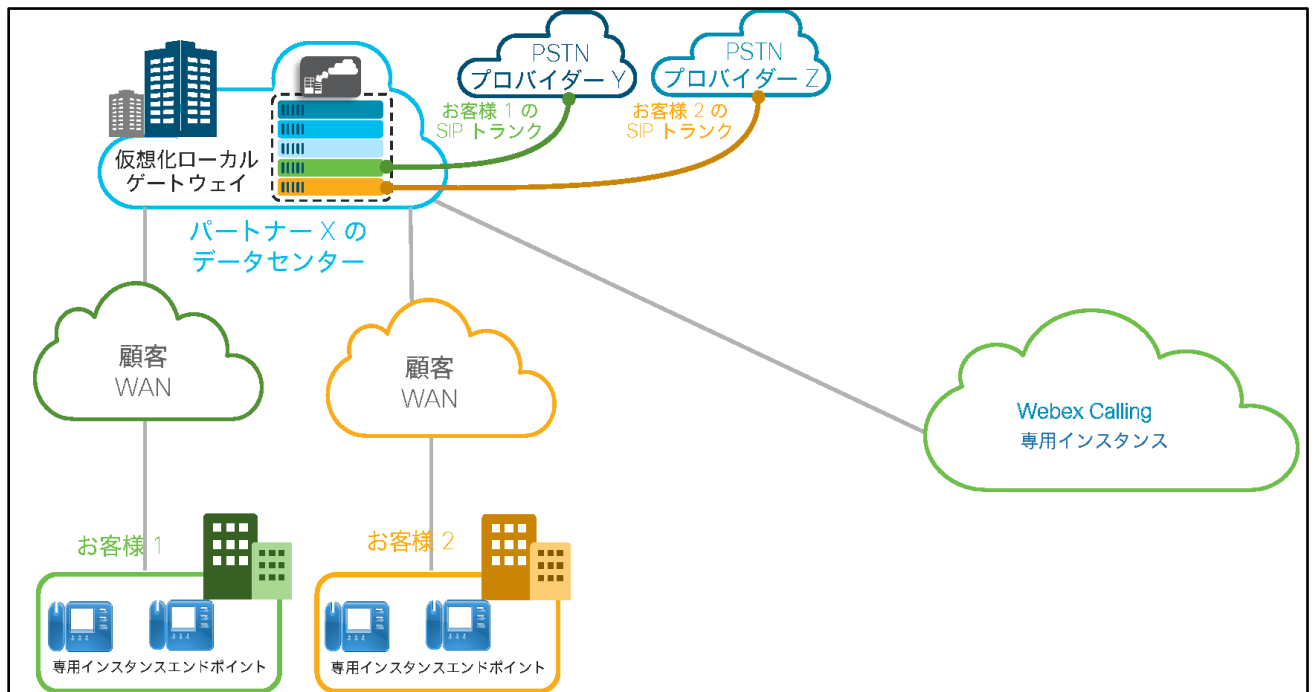


図 39 は、この例の場合、パートナーがデータセンターにローカルゲートウェイを展開していることを示しています。個々のお客様のダイヤルピアコールルーティング設定は、1 つの CUBE で組み合わせることができます。お客様間のトラフィックの分離は、ダイヤルピアルーティングを適切に設定することで実現されます。この設定により、パートナーはローカルゲートウェイを経由して、専用インスタンスから受信した通話をお客様指定の PSTN トランクにマッピングしたり、その逆にマッピングしたりできます。この展開モデルにより、パートナーは、様々な顧客に対してより効率的にローカルゲートウェイを展開、維持、運用できます。

CCPP (Cloud Connected PSTN プロバイダー)

Cloud Connected PSTN (CCP) は、専用インスタンスのグローバルクラウド PSTN 通話オプションを有効化します。専用インスタンスは、この機能のために Webex Calling との既存の CCP パートナーピアリングを活用します。専用インスタンスの CCP を有効にするには、管理者は Webex Control Hub でルートリストを構成する必要があります。

図 40 クラウド接続 PSTN



図 40 に示すように、お客様は企業のさまざまな CCP プロバイダーからの PSTN サービスを使用できます。

CCPP の詳細については、<https://help.webex.com/en-us/article/nw3ygtq/Cloud-Connected-PSTN> の「クラウド接続 PSTN ドキュメント」を参照してください。

ケーススタディ 1a : 集中型通話処理を行う Unified CM と複数の Webex Calling ロケー ション

既存の Unified CM 導入環境に Webex Calling を追加することで、使用可能な WAN 帯域幅が不十分であるか、その他のロジスティクス面での課題が原因で集中型コール処理ができない場合のソリューションを提供します。

この導入事例では、Webex Calling のロケーションがマルチサイトの Unified CM 導入と組み合わされているシナリオを検証します。このタイプの導入は、比較的小規模なサイトを Unified CM から Webex Calling ロケーションに移行するようなシナリオで役立ちます。

ローカルゲートウェイは、Webex Calling とオンプレミスの Unified CM 間の接続を確立するために必要なコンポーネントです。Webex Calling ダイアルプランルーティングロジックを使用して、これを Cisco PSTN または Cloud Connected PSTN で補完し、Webex Calling ユーザーに PSTN サービスを提供することができます。クラウド PSTN が存在しない場合、ローカルゲートウェイはオンプレミスコールと PSTN コールの両方に使用されます。

ローカルゲートウェイはスタンドアロンで導入できますが、この導入事例では Cisco Unified CM 導入環境との統合に焦点を当てています。

図 41 スタンドアロンのローカルゲートウェイ展開

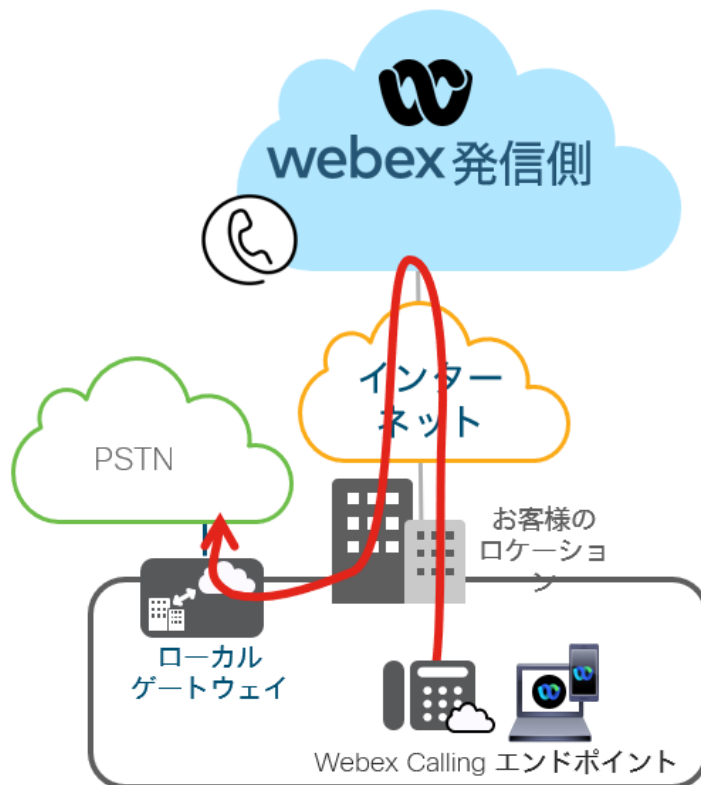
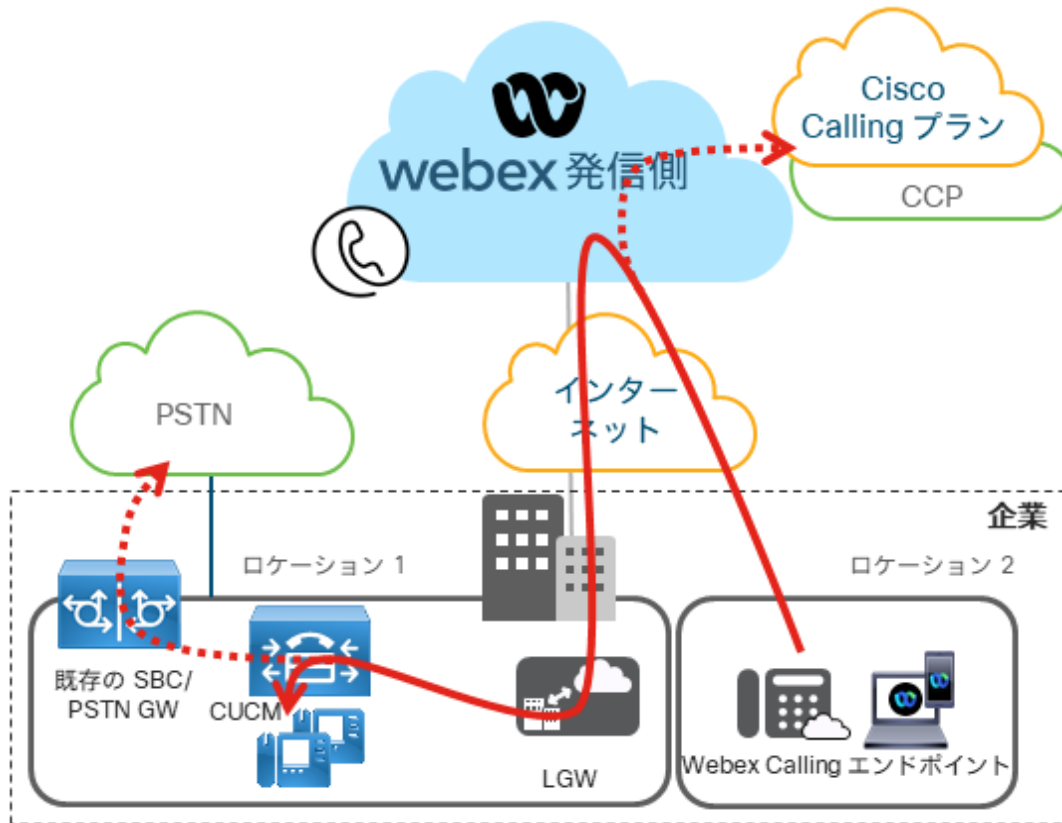


図 41 は、ローカルゲートウェイを使用した単一ロケーションでの Webex Calling の導入を示しています。この場合、Webex Calling エンドポイントから発信される PSTN コールは、PSTN へのアクセスを提供するローカルゲートウェイに送信されます。

オンプレミスの呼制御システムとして展開された Unified CM に登録されている電話から Webex Calling ロケーションに直接ダイヤルする必要がある場合には、ローカルゲートウェイの統合が必要です。

図 ローカルゲートウェイと専用 PSTN ゲートウェイの統合



図は、Webex Calling エンドポイントから発信された通話が、Webex Calling ダイヤル プラン ルーティング ロジックに基づいてローカルゲートウェイに送信されることを示しています。ローカルゲートウェイはこのコールを Unified CM に送信します。Unified CM にプロビジョニングされている企業のダイヤルプランによって、コールを Unified CM に登録されたエンドポイントに拡張する必要があるか、または既存の PSTN ゲートウェイ インフラストラクチャを介した PSTN に拡張する必要があるかどうか決定されます。PSTN へのルーティングは、Webex 発信ロケーションがオンプレミスペースの PSTN に設定されている場合のみのオプションです。代わりにクラウド PSTN が使用される場合、Webex Calling ユーザーからの PSTN コールは、発信側ユーザーのロケーションに設定されたクラウド PSTN に送信されます。

図 42 ローカルゲートウェイと PSTN ゲートウェイの共存

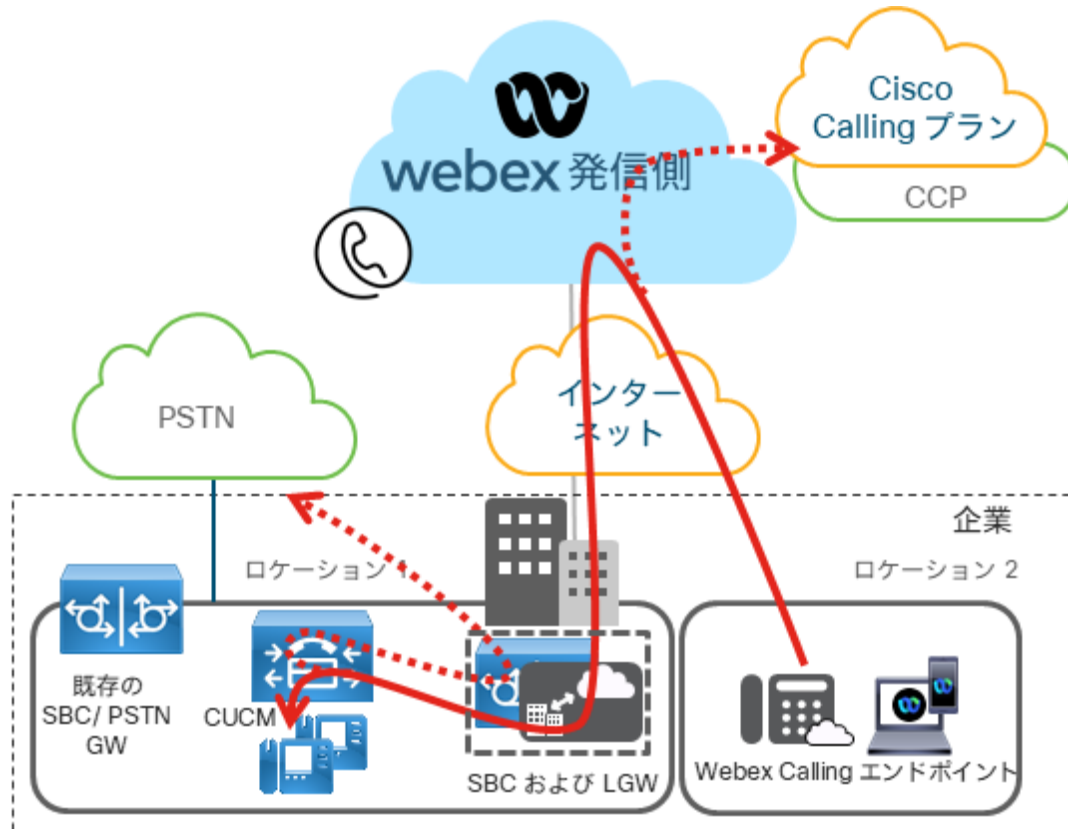


図 42 は、この導入モード（ローカルゲートウェイと PSTN アクセス機能が同じデバイス上に存在）のバリエーションを示しています。このシナリオの違いは、ローカルゲートウェイと PSTN ゲートウェイを組み合わせたデバイスの設定です。Webex Calling の観点からも Unified CM の設定からも、前のシナリオとの大きな違いはありません。このシナリオでは、Unified CM は PSTN アクセスとローカルゲートウェイ機能をホストする CUBE から 2 種類のコールを受信します。つまり、PSTN からのコールと Webex Calling からのコールです。これらのコールタイプに異なるサービスクラスを適用するには、CUBE と Unified CM の間に 2 つ（コールタイプごとに 1 つ）の SIP トランクを設定する必要があります。これを実現するには、SIP トランクのセキュリティプロファイルで Unified CM の各 SIP トランクに異なる SIP リスニングポートを設定する必要があります。

クラウド PSTN に Webex Calling のロケーションが設定されている場合は、ローカルゲートウェイから受信した PSTN コールと Webex Calling コールの区別も必要です。PSTN コールをローカルゲートウェイ経由で Webex Calling から Unified CM に転送して PSTN に戻す必要はありませんが、その場合でも Unified CM では区別されたサービスクラスを適用する必要があります。Webex Calling から発信されるコールは、マルチクラス展開のリモート オンネット ロケーション（接続された Unified CM SME 経由など）にアクセスする必要がありますが、PSTN からのコールでは通常、このアクセスを必要としません。

同じデバイスで両方の機能を組み合わせることで、コスト効率の高い導入が可能になります。

コールルーティングに関する考慮事項

Webex Calling から Unified CM へのコール

アーキテクチャの概要で前述したように、Webex Calling ユーザーからのコールは、Webex Calling ダイアルプランに基づいてオンプレミストラックにルーティングされます。オンプレミススペースの PSTN を使用する場合、PSTN コールもオンプレミストラックに送信されます。2 つのコールタイプの識別は、Unified CM でプロビジョニングされている企業ダイアルプランに基づいて Unified CM が行います。

図 46 Webex Calling から Unified CM へのダイヤル

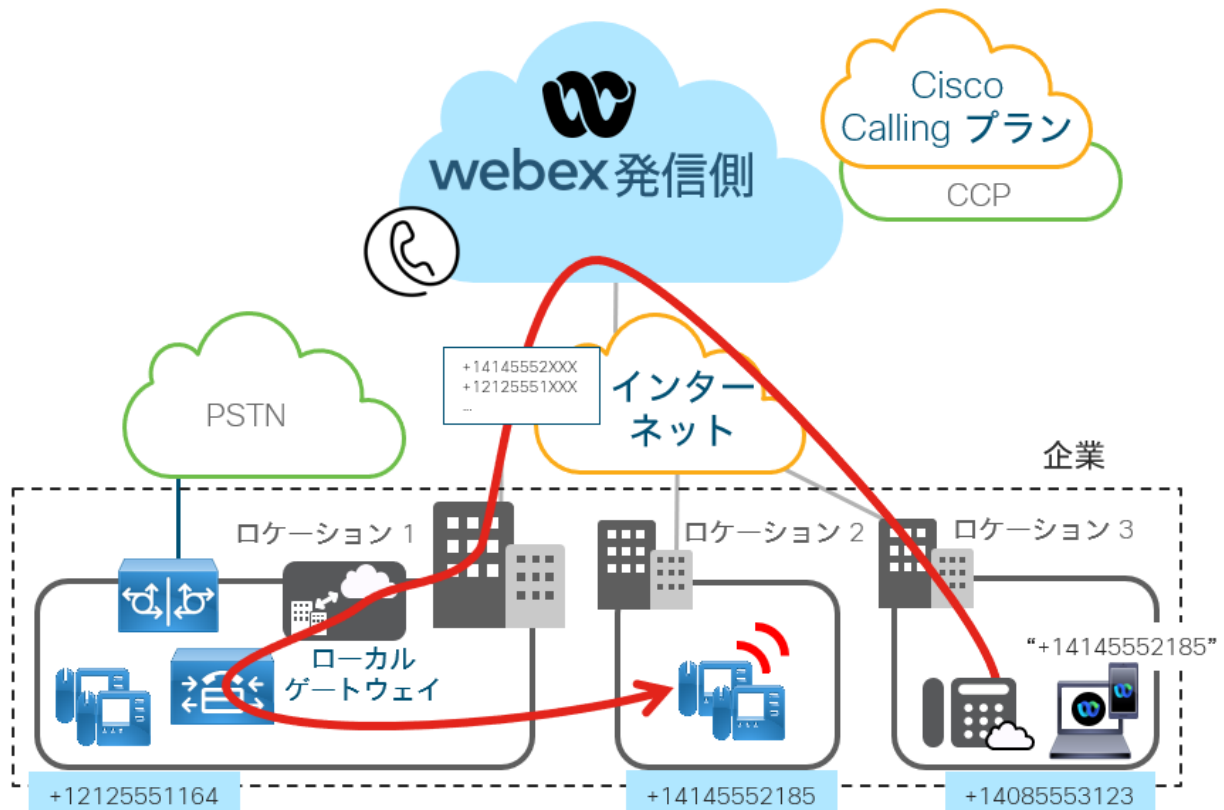


図 46 は、集中型通話処理を使用したマルチサイト Unified CM の展開例を示しています。Webex Calling ユーザーが +E.164 番号をダイヤルした場合、ダイヤルされた番号が Webex Calling 上でお客様がプロビジョニングした番号と一致していないが、その番号が Webex 内でダイアルプランに構成されている +E.164 パターンと一致しています。したがって、このコールは、そのダイアルプランのルーティング選択肢として選択されたトラックまたはルートグループに送信されます。ローカルゲートウェイはこのコールを Unified CM に送信します。ローカルゲートウェイでのコールルーティングでは、着信側のアドレスは考慮されません。ルーティングはトラック属性のみに基づいているため、Unified CM から受信したコールは Webex Calling に転送され、Webex Calling から受信したコールは Unified CM に転送されます。Webex Calling から Unified CM へのローカルゲートウェイ経由のコールログに表示される着信側の番号は、発信側が最初にダイヤルした接続先であり、+E.164 形式です。Unified CM は設定されているダイアルプランを参照し、コールされた宛先がディレクトリ番号としてプロビジョニングされているローカル登録のエンドポイントにそのコールをルーティングします。

Webex Calling から Unified CM への企業短縮オンネットサイト間ダイヤリングも有効にするには、それぞれの企業パターンを Webex Calling ダイアルプランに追加する必要があります。

図 43 Webex Calling からの企業のオンネット短縮ダイヤル

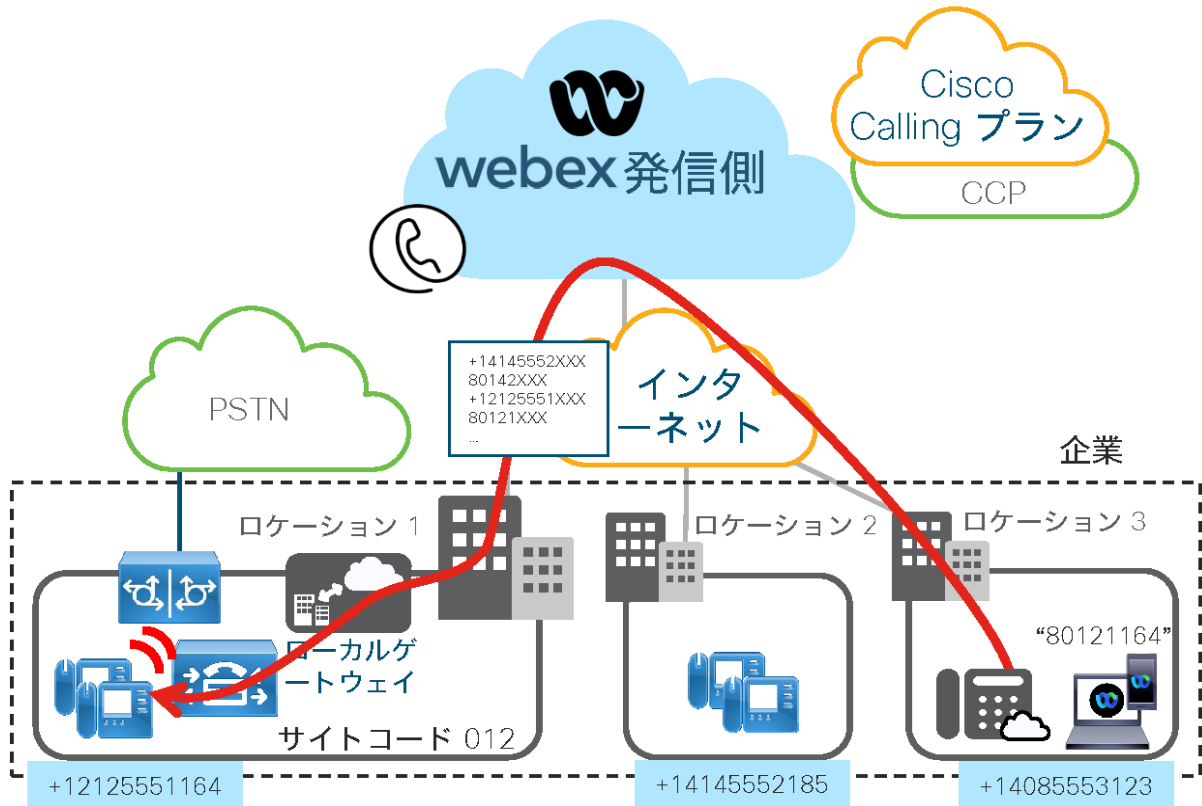


図 43 は、企業の番号計画（ステアリング桁「8」、4 桁のルーティングプレフィックス、4 桁の内線番号）を使用している企業の例です。

この企業の番号計画は、Webex Calling に登録しているデバイスでダイヤルする場合に使用できます。ダイヤルされた番号は、Webex Calling で解析され、ダイヤルプランで定義されたエンタープライズパターンと一致し、Webex Calling ダイアルプランのルーティングの選択肢として定義されたトランクまたはルートグループにコールが送信されます。このコールはローカルゲートウェイによって Unified CM に送信されます。

上記のように企業の番号計画を使用してサイト間短縮オンネットダイヤルを Unified CM で実装している場合、ダイヤルされた番号「80121164」が Unified CM に登録されているエンドポイントの DID にマッピングされ、コールが接続されます。Webex Calling から Unified CM への企業の短縮ダイヤルを可能にするには、適切な設定（内線番号の長さ、プレフィックス長、ステアリング桁）を設定し、Webex Calling から受信したコールをルーティングする際にこのダイヤル手順をサポートするように Unified CM を設定する必要があります。

図 44 Webex Calling から PSTN 接続先へのコール

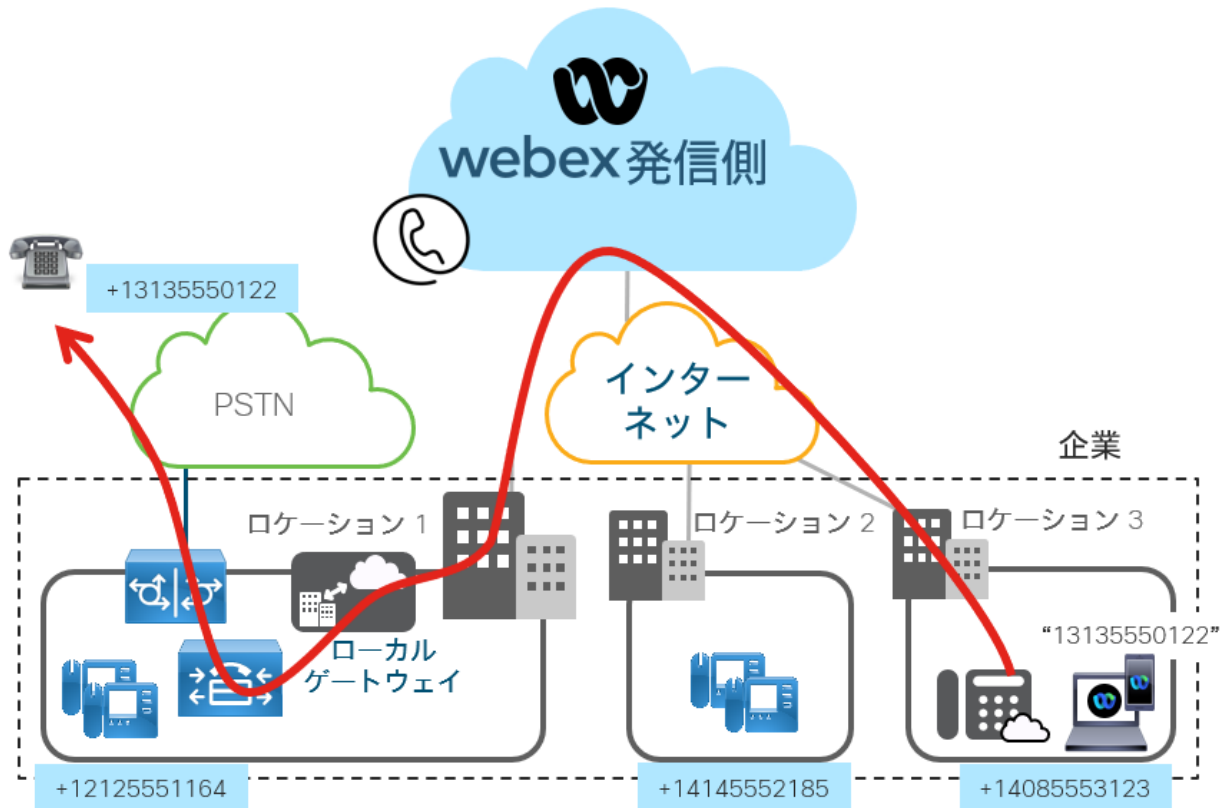


図 44 は、ロケーションの PSTN としてオンプレミスペースの PSTN が設定されたロケーションの Webex Calling デバイスからダイヤルされた、PSTN の接続先を示しています。コールは Webex Calling から見てオフネットと見なされ、ローカルゲートウェイに送信されてから、Unified CM に送信されます。Unified CM は、Webex Calling から受信した +E.164 アドレスと一致するオンネットを見つけられないため、Unified CM が制御する既存の PSTN ゲートウェイを介してコールを PSTN に送信します。

Unified CM から Webex Calling へのコール

Unified CM から Webex Calling へのコールルーティングを有効にするには、Unified CM で一連のルートを提供する必要がある場合があります。これにより、Webex Calling の +E.164 アドレスと企業番号計画のアドレスのセットが定義されます。

図 45 Unified CM から Webex Calling へのコール

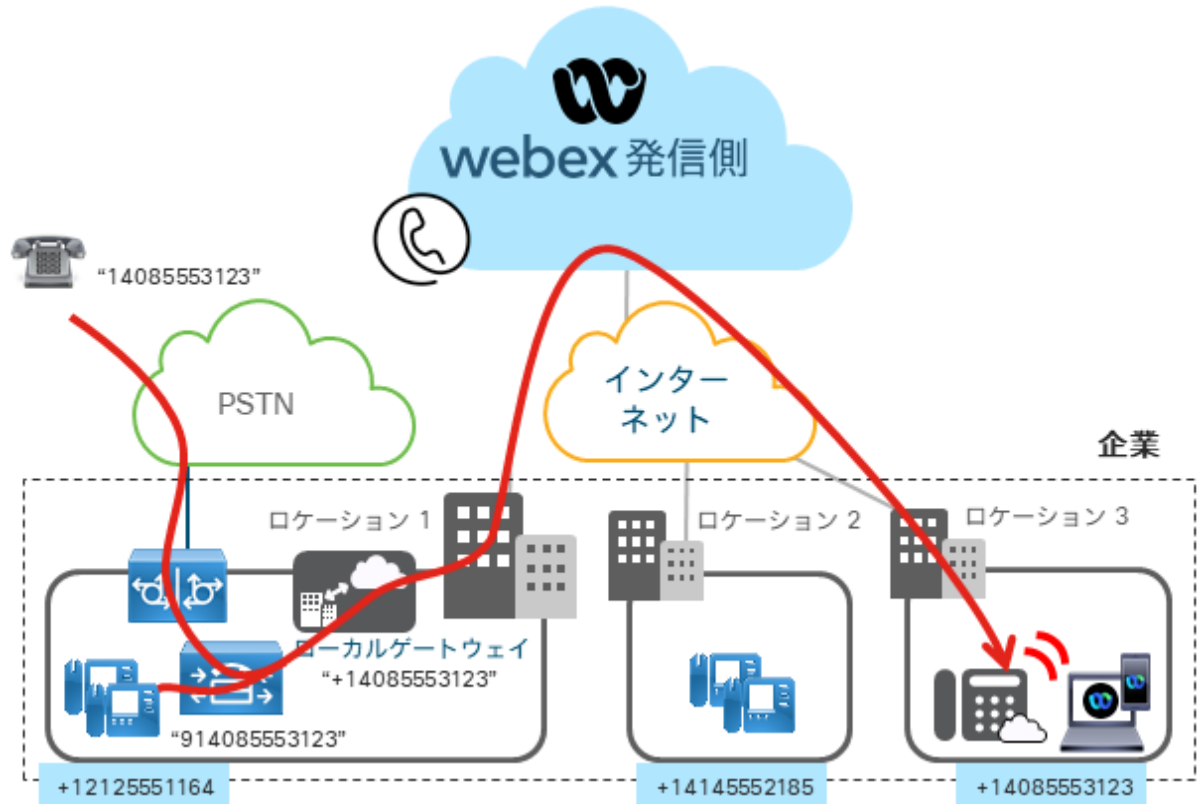


図 45 は、これらのルートが設定されていれば、ここに示す両方のコールシナリオが可能であることを示しています。発信側の PSTN から Webex Calling デバイスに割り当てられている DID をコールすると、コールは企業の PSTN ゲートウェイ経由で企業に送信され、その後 Unified CM に送信されます。そのコールで呼び出されたアドレスは Unified CM でプロビジョニングされている Webex Calling のルートのいずれかと一致し、コールがローカルゲートウェイに送信されます。このとき、宛先アドレスは +E.164 形式でローカルゲートウェイに送信される必要があります。Webex Calling のルーティングロジックは、DID の割り当てに基づいて、目的の Webex Calling デバイスにコールをルーティングします。PSTN からのコールは、Webex ロケーションがオンプレミスペースの PSTN を使用している場合、またはクラウドベースの PSTN への移行中に番号がまだ新しいプロバイダに移動されていない場合にのみ、Unified CM によって Webex Calling に転送される必要があります。

Unified CM に登録されているエンドポイントから Webex Calling 宛てに発信されるコールは、Unified CM でプロビジョニングされているダイヤルプランに従って処理されます。通常、このダイヤルプランでは、ユーザは企業の一般的なダイヤル手順を使用して発信できます。

Webex Calling へのコールの着信アドレスは、+E.164 形式、エンタープライズ形式、または内線番号形式にすることができます。着信側アドレスが内線番号 (2 ~ 6 桁) の場合、Webex Calling では、着信したトランクの場所をルーティングコンテキストとして使用し、Webex Calling の内線番号がグローバルに一意でない場合に曖昧さを解消できるようにします。

Unified CM から Webex Calling への着信側アドレスとして企業番号または内線番号を使用できるようにすることで、Unified CM から Webex Calling ユーザーへのコールが可能となりました。

図 46 Unified CM から Webex Calling へのコール

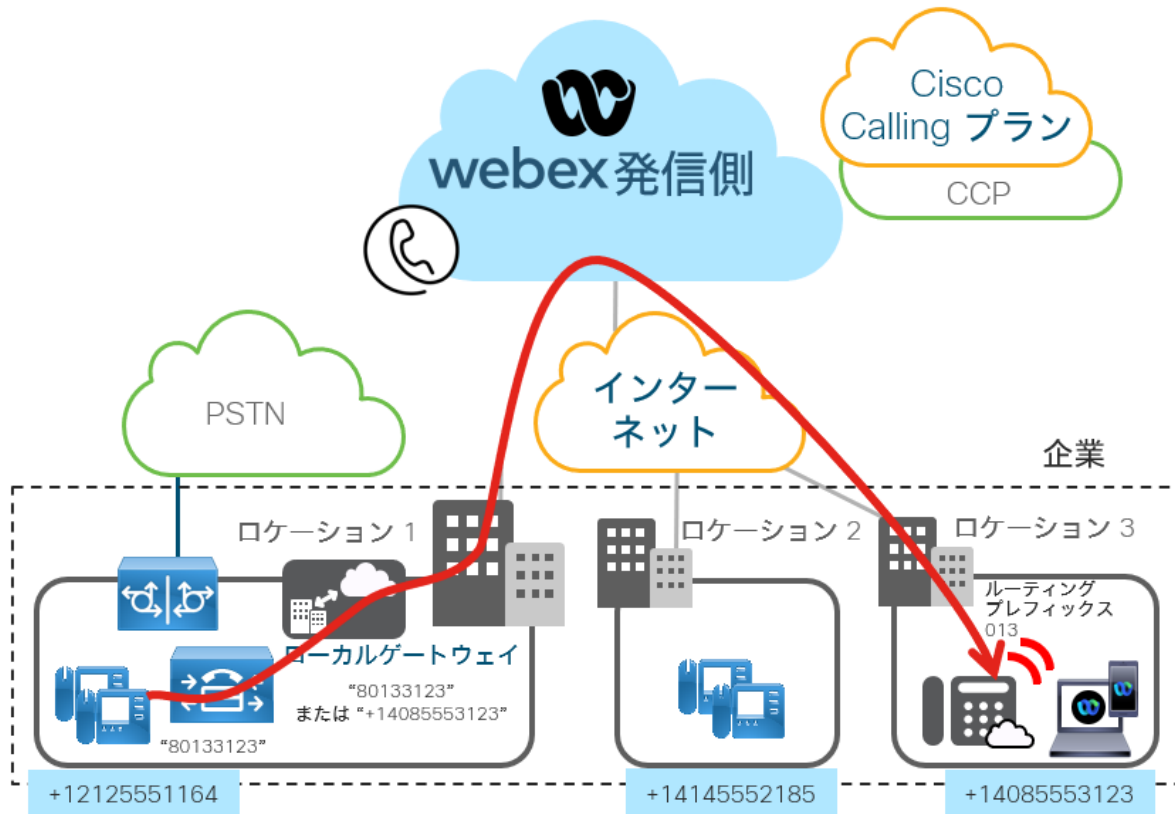


図 46 は、Unified CM で適切なダイヤル正規化を使用することで、Unified CM に登録されているデバイスから Webex Calling ロケーションへのサイト間短縮オンネットダイヤルを有効にする方法を示しています。着信側アドレスは、+E.164 に正規化するか、変換せずに送信できます。着信側アドレスを +E.164 に正規化するには、Unified CM はすべての Webex Calling ロケーションの ESN から +E.164 へのマッピングを認識する必要があります。着信側アドレスを変更せずに送信する場合、Unified CM の企業の番号計画は、Webex Calling で設定されたエンタープライズ番号計画と互換性がある必要があります。Unified CM から Webex Calling へのコールに対して +E.164 への企業のダイヤリングを正規化しない場合、電話番号のない Webex Calling ユーザー（内線番号のみのユーザー）へのコールが有効になります。

サービスクラス (CoS)

厳格な CoS 制限には、コールループの回避や不正通話の防止など、さまざまなメリットがあります。Webex Calling のローカルゲートウェイと Unified CM の CoS を統合する場合は、以下のそれぞれについて CoS を検討します。

- Unified CM に登録しているデバイス
- PSTN からコールを受信する Unified CM
- Webex Calling からコールを受信する Unified CM

Unified CM に登録しているデバイスの CoS

Webex Calling の宛先は、既存の CoS に新しいクラスの宛先として追加されます。Webex Calling の宛先への発信許可は、（サイト間を含む）オンプレミスの宛先への発信許可と同等です。

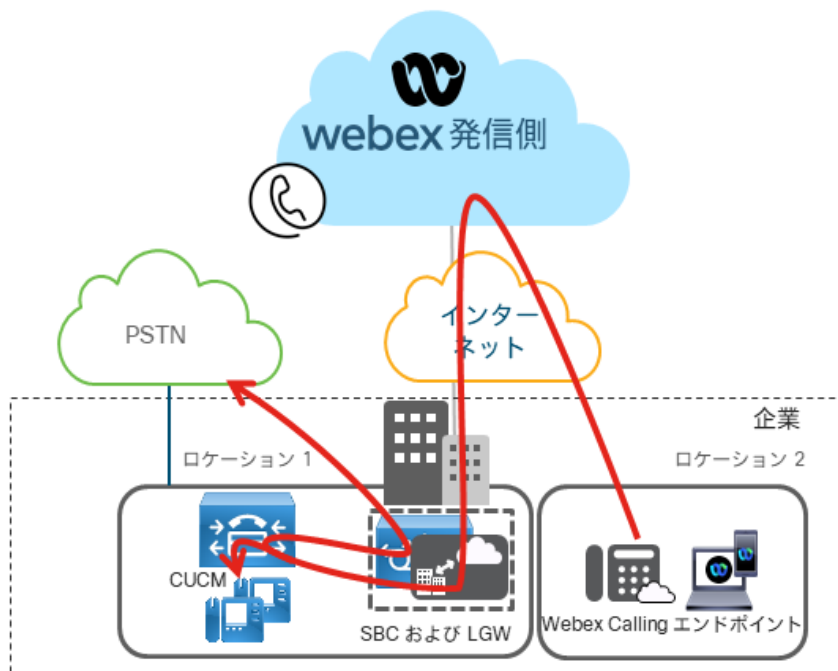
企業のダイヤルプランですでに「サイト間（短縮）オンネット」権限を実装している場合、Unified CM ですでにパーティションが設定され、同じパーティションですべての既知のオンネット Webex Calling 向けの接続先を設定するために使用されます。「サイト間（短縮）オンネット」権限がまだ存在しない場合は、新しいパーティション（「onNetRemote」など）を設定する必要があります。Webex Calling の宛先はこのパーティションに追加されます。パーティションは適切なコーリングサーチスペースに追加する必要があります。

PSTN または Webex Calling からのコールの CoS

PSTN からのコールでは、Webex Calling ロケーションでオンプレミスペースの PSTN が使用されている場合、またはクラウド PSTN への移行中のみ、すべての Webex Calling の接続先にアクセスする必要があります。このため、Webex Calling のすべての宛先を保持する前述のパーティションを、PSTN トランクでの着信コールに使用するコーリングサーチスペースに追加する必要があります。Webex Calling の宛先へのアクセスは、既存のアクセスに追加されます。

PSTN からのコールには、Unified CM の DID と Webex Calling の DID へのアクセスが必要です。Webex Calling からのコールには、Unified CM の DID と PSTN 接続先へのアクセスが必要です。後者の場合、Webex Calling ロケーションがオンプレミスペースの PSTN を使用する場合にのみ必要です。

図 47 PSTN からの通話用と Webex Calling からの通話用の異なる CoS



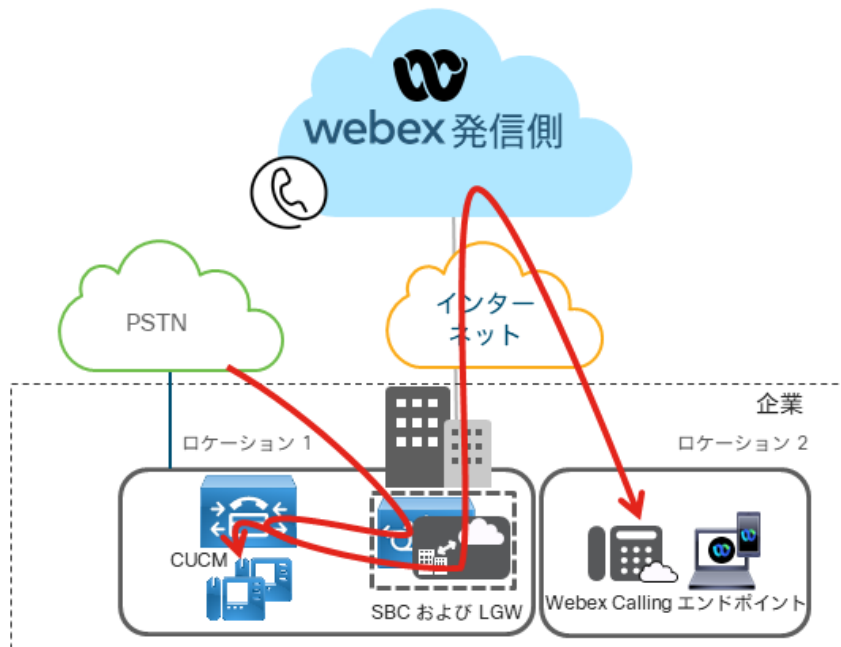


図 47 は、PSTN からのコール用と Webex Calling からのコール用の 2 つのサービスクラスを示しています。PSTN ゲートウェイ機能がローカルゲートウェイと共有されている場合、統合された PSTN のゲートウェイとローカルゲートウェイから Unified CM へ 2 つのトランク (1 つは PSTN 発信のコール用、もう 1 つは Webex Calling 発信のコール用) が必要です。これは、トラフィックタイプごとに異なるコーリングサーチスペースを適用するための要件に基づいています。Unified CM で 2 つの着信トランクを使用した場合のみ、各トランクの着信コールに必要なコーリングサーチスペースを設定することで、簡単にこの要件を実現できます。Unified CM の 2 つの SIP トランクに異なる SIP リスニングポートを使用することで、ローカルゲートウェイと Unified CM 間の複数のトランクを設定できます。SIP リスニングポートは、SIP トランクのセキュリティプロファイルで設定されます。

Unified CM のダイヤルプランは、コールのタイプ (PSTN または Webex Calling) に応じて両方のトランクを使用するように設定されます。ローカルゲートウェイでは、コールが受信されるトランクは、INVITE の最上位の VIA ヘッダーのポート番号を照合することで識別されます。これは、ローカルゲートウェイに着信ダイヤルピア上の `incoming uri via <some voice class>および voice class uri <some voice class>` 上の `pattern :<UCM listening port>` を組み合わせることで実現します。

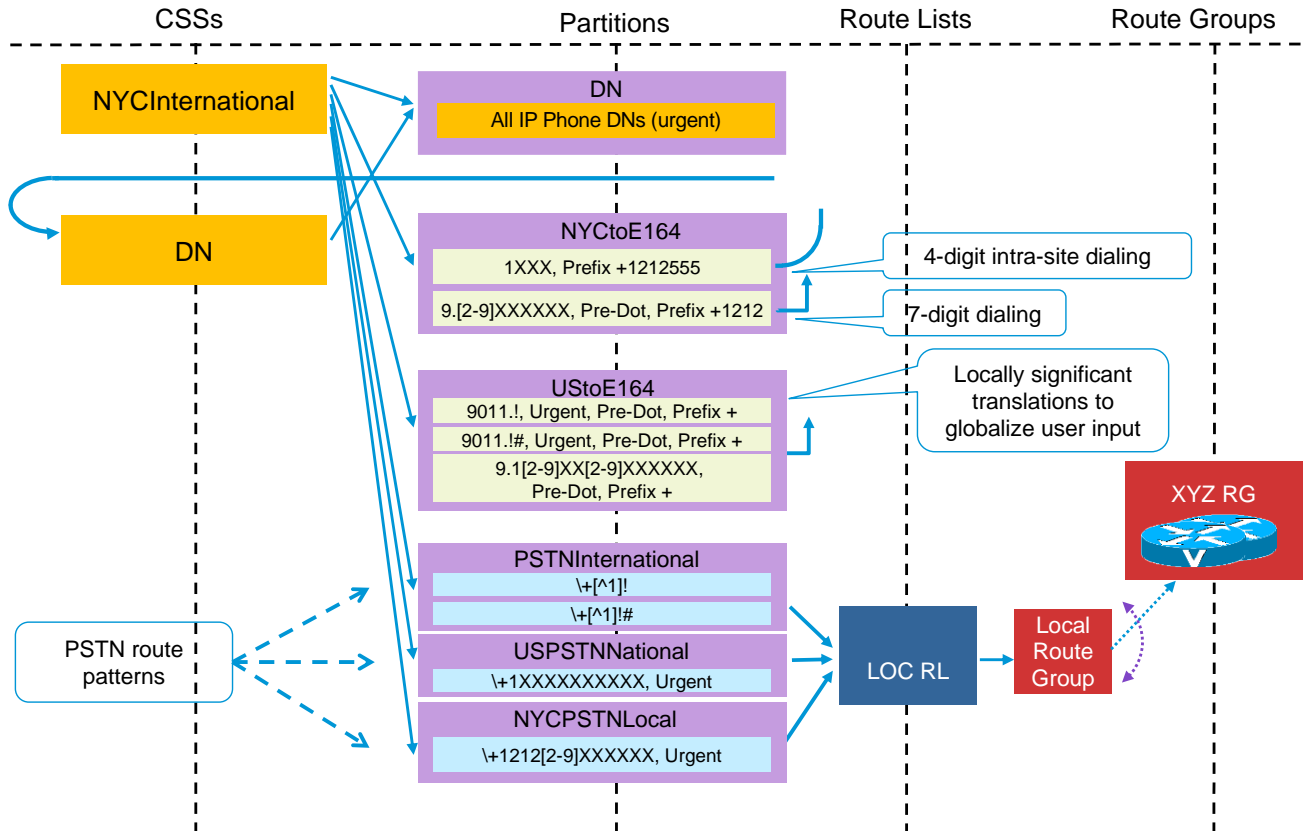
Unified CM ダイヤルプランの統合

このガイドは『Preferred Architecture for Cisco Collaboration On-Premises Deployments, CVD』 (https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/uc_system/design/guides/PAdocs.html) の最新バージョンに記載されているベストプラクティスに基づいた既存環境を前提としています。

推奨されるダイヤルプランの設計は、<https://www.cisco.com/go/ucsrnd> に掲載されている Cisco Collaboration System の最新バージョンの SRND の「Dial Plan」の章で説明されている設計アプローチに従います。

次の情報は、Cisco Unified CM でのサービスクラスの設定を示しています。

図 48 ダイアルプランの推奨事項



前の図は、推奨されるダイアルプラン設計の概要を示しています。このダイアルプラン設計の主な特徴は次のとおりです。

- Unified CM で設定されているすべてのディレクトリ番号は +E.164 形式です。
- すべてのディレクトリ番号は同じパーティション (DN) にあり、緊急とマークされています。
- コアルーティングは +E.164 に基づいています。
- +E.164 ではないダイヤル手順。たとえば、共通のダイヤル手順を使用するサイト内短縮ダイヤルと PSTN ダイヤルは、ダイヤル正規化変換パターンを使用して +E.164 に正規化 (グローバル化) されます。
- ダイヤル正規化変換パターンでは、変換パターンのコーリングサーチスペースが継承され使用されます。つまり、[発信側コーリングサーチスペースを使用 (Use Originator's Calling Search Space)] オプションがオンです。
- サービスクラスは、サイトとサービスクラスに固有のコーリングサーチスペースを使用して実装されます。
- PSTN アクセス機能 (国際 PSTN の宛先へのアクセスなど) は、それぞれ +E.164 ルートパターンを設定したパーティションを、サービスクラスを定義するコーリングサーチスペースに追加することによって実装されます。

図 49 ダイアルプランへの Webex Calling 接続先の追加

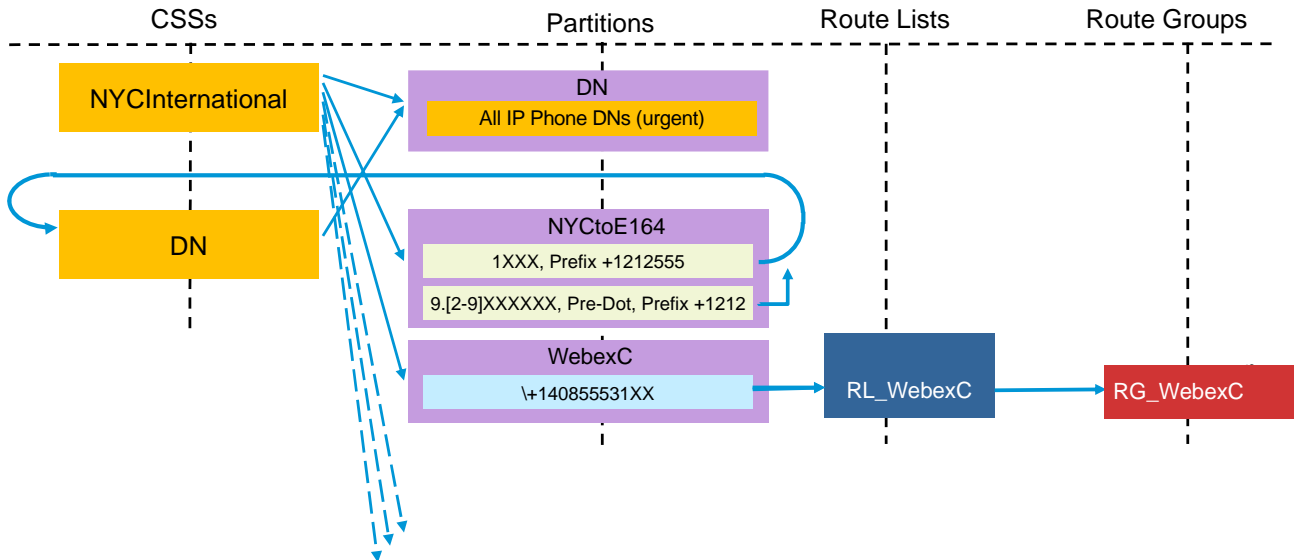


図 49 は、このダイヤルプランに Webex Calling の宛先へのアクセスを追加する方法を示しています。Webex Calling のすべての宛先を表すパーティション「WebexC」を作成する必要があります。Webex Calling の各 DID 範囲の +E.164 ルートパターンがこのパーティションに追加されます。このルートパターンは、メンバーを 1 つだけを含むルートリスト (Webex Calling へのコール用のローカルゲートウェイに対する SIP トランクを含むルートグループ) を参照します。複数のローカルゲートウェイが存在する場合、Unified CM ルートグループをロードバランシングと冗長性を使用することができます。ダイヤルされたすべての宛先は、Unified CM に登録されているエンドポイントから発信されるコールを処理するダイヤル正規化変換パターンか、PSTN から発信されるコールを処理する着信側の変換を使用して +E.164 に正規化されるため、この単一セットの +E.164 ルートパターンで問題なく (使用されるダイヤル手順には関係なく) Webex Calling の宛先に到達します。

たとえば、ユーザが「914085553165」をダイヤルすると、パーティション「UStoE164」のダイヤル正規化変換パターンがこのダイヤル文字列を「+14085553165」に正規化します。これは、パーティション「WebexC」の Webex Calling が宛先のルートパターンと一致するため、Unified CM は最終的にローカルゲートウェイにコールを送信します。

図 50 拠点間短縮ダイヤルの追加

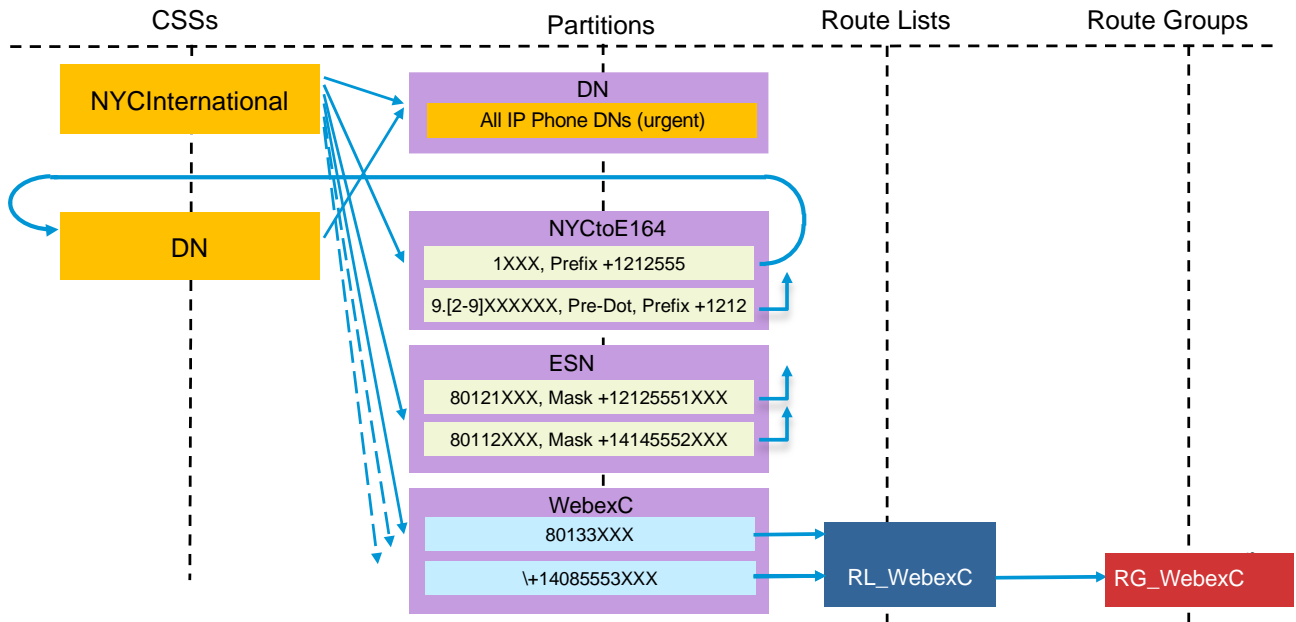


図 50 **Error! Reference source not found.**は、拠点間短縮ダイヤルを参照ダイヤルプランに追加する場合の推奨方法を示しています。企業番号計画に従ってすべての拠点のダイヤル正規化変換パターンを専用パーティション（Enterprise Significant Number (ESN)）に追加することをお勧めします。これらの変換パターンは、企業の番号計画のダイヤルフォーマットを +E.164 に正規化します。

Webex Calling の宛先として企業の短縮ダイヤルを追加するには、Webex Calling ロケーション宛の各ルートパターンを「WebexC」パーティション（「80133XXX」など）に追加します。着信番号は変換されず、Webex Calling にそのまま送信されます。これにより、Unified CM から内線番号のみを設定した Webex Calling ユーザへの企業の短縮ダイヤルを使用できます。

ローカルゲートウェイの導入

Webex Calling と Unified CM 間の接続には、少なくとも 1 つのローカルゲートウェイをプロビジョニングする必要があります。拡張性と冗長性に対応するために、複数のローカルゲートウェイを設定できます。ローカルゲートウェイが割り当てられているロケーションは、Unified CM から Webex Calling への内線ダイヤルコールに対してダイヤリングコンテキストを確立する必要がある場合にのみ関連します。同じロケーションのユーザーの一部が Unified CM に存在し、別のユーザーが Webex Calling に存在する状況で、部分的な移行が発生しない場合は、Unified CM から Webex Calling への内線ダイヤリングは有効な使用例ではないため、この場合は、ローカルゲートウェイのロケーションの関連付けは重要ではありません。展開するローカルゲートウェイの数とローカルゲートウェイの展開先の決定は、主に規模と信頼性の要件によって決定されます。

最も単純なケースでは、すべてのローカルゲートウェイが単一のルートグループに追加されます。

Webex Calling ダイアルプランの設定

グローバルな [不明な番号の処理 (Unknown Numbers Handling)] パラメータが [標準の動作 (Standard behavior)] に設定されているため、Unified CM へのルーティングとコール分類は、企業のダイアルプランのダイアルプランパターンに基づきます。すべてのローカルゲートウェイを持つ単一のルートグループが、そのダイアルプランのルーティングとして使用されます。

Webex Calling から発信されたコールを Unified CM にてコールバックが可能になるように、グローバルな [オンプレミスとのコールの発信者 ID 形式 (Caller ID Format for Calls from and to On-premises)] 設定を [ESN] に設定する必要があります。

Unified CM の各エンタープライズおよび +E.164 番号範囲について、それぞれのパターンがダイアルプランに追加されます。

各 Webex Calling ロケーションに、エンドツーエンドの企業のダイアルプランに従って、内部ダイヤリング ルーティングプレフィックスを設定します。各ロケーションに固有のサイトプレフィックスを選択することが重要です。Webex Calling と Unified CM に同じサイトプレフィックスを同時に存在させることはできません。[不明な内線番号の内部コールとしてのルーティングを有効にする (Enable routing unknown extension to the Premises as internal calls)] オプションは無効になっています。

ケース スタディ 1b : 専用インスタンスを使用した Webex Calling

このケーススタディでは、Webex Calling ロケーションが Webex Calling 専用インスタンスと組み合わさったシナリオを検証します。このタイプの展開では、Cisco Unified Communications Manager ベースのアプリケーションスタックが提供され、Webex でホストされ、単一のお客様専用の Webex Calling サービスの一部が提供されます。

専用インスタンス通話フロー

専用インスタンスは、エンドポイント間で直接送信されるクラウドとメディアを介したシグナリング標準的なアプローチに従います。エンドポイント間のメディアは、拠点内および異なる拠点間の両方のお客様のネットワークを使用します。

このセクションの通話フローの説明には、お客様の拠点内通話、お客様の拠点間通話、専用インスタンスからの PSTN 通話、およびマルチテナントおよび専用インスタンス プラットフォームに登録されているエンドポイント間の通話が含まれます。外部デバイスへの通話は、お客様の WAN 経由で PSTN 接続を介して流れます。お客様がモバイルおよびリモートアクセス (MRA) を構成している場合、通話はお客様の WAN を経由します。

お客様の拠点内通話

お客様の拠点内線番号通話シグナリングは、専用インスタンスクラウドを介して送信されます。メディアは、お客様の拠点内のオンプレミスにとどまります。

図 51 専用インスタンスのお客様拠点内ダイヤル

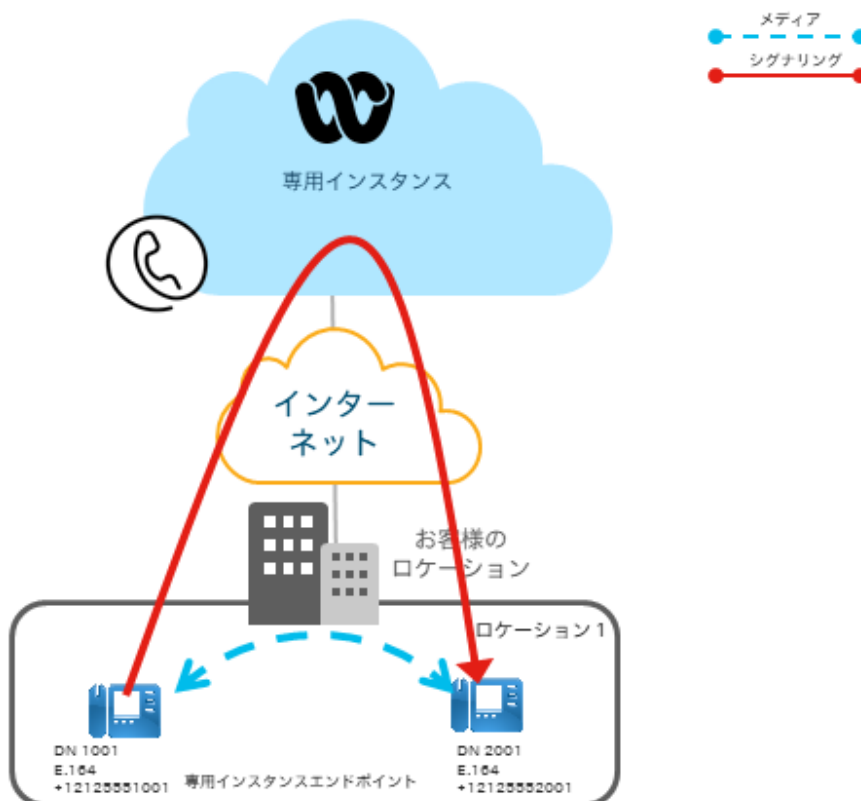


図 51 は、単一ロケーションによる Webex Calling 専用インスタンスの展開を示しています。電話機は専用インスタンスに登録されています。1001 が 2001 にダイヤルすると、通話シグナリングは専用インスタンスクラウドを通過します。2001 が通話に応答すると、メディアは電話機間でローカルに接続されます。

お客様の拠点間通話

お客様の拠点間通話は、専用インスタンスクラウドを経由し、メディアは、お客様の WAN を経由します。

図 52 専用インスタンスのお客様拠点間ダイヤル

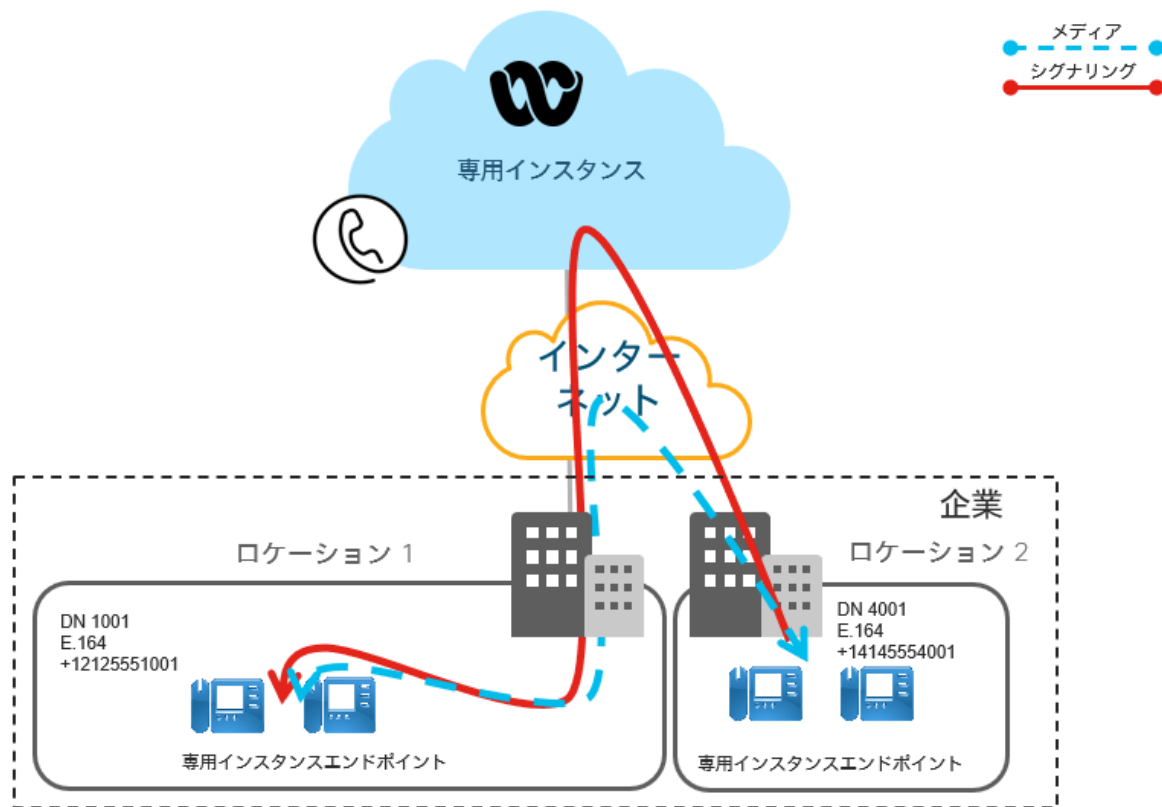


図 52 は、複数ロケーションによる Webex Calling 専用インスタンスの展開を示しています。両ロケーションの電話機が専用インスタンスに登録されます。ロケーション 2 にある電話機 4001 が、ロケーション 1 の内線番号 1001 をダイヤルすると、専用インスタンスクラウドに通話を送信します。専用インスタンスでプロビジョニングされた企業ダイヤルプランは、通話を 1001 に送信します。1001 が通話に応答すると、メディアはお客様の WAN を介して流れます。

専用インスタンスからの PSTN 通話

ローカルゲートウェイは、お客様またはパートナーのオンプレミスにデプロイされます。ローカルゲートウェイは、SIP トランクを介して専用インスタンスの Unified CM に接続され、PSTN 通話を専用インスタンスに接続します。

図 53 専用インスタンスの PSTN 通話

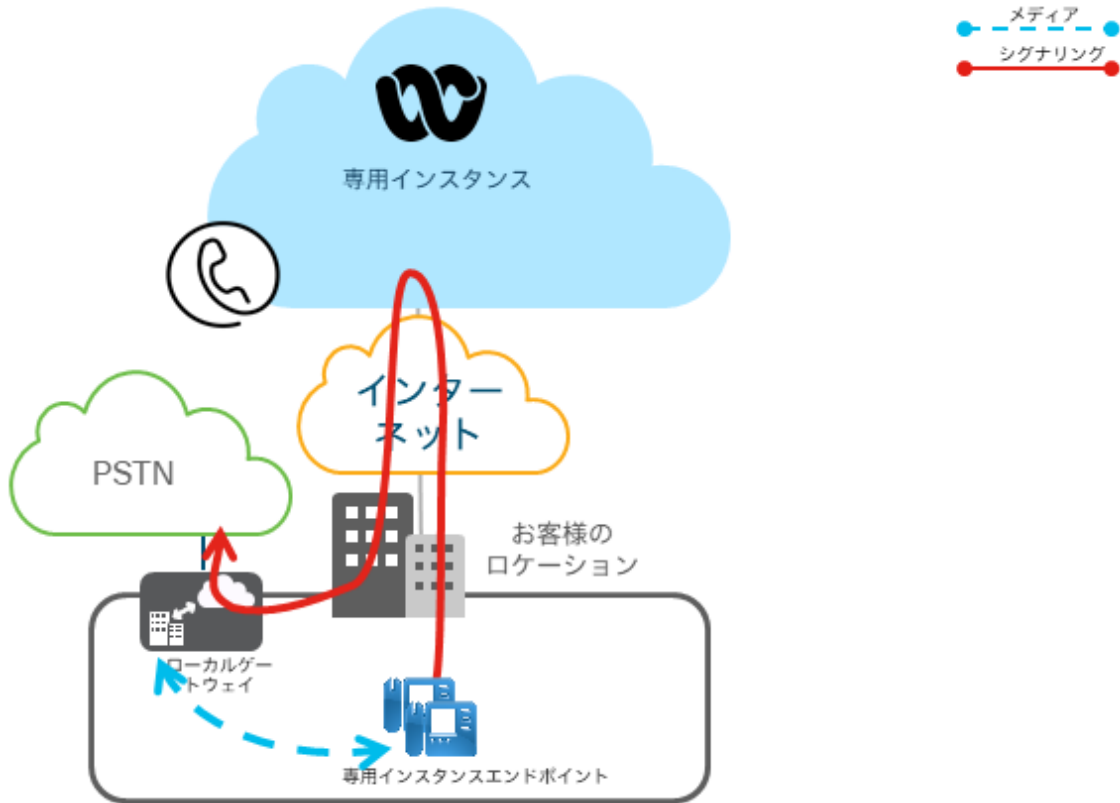


図 53 は、ローカルゲートウェイを使用した単一ロケーションでの Webex Calling の展開を示しています。Webex Calling 専用インスタンスエンドポイントから発信された通話は、Webex Calling 専用インスタンス ダイヤル プラン ルーティング ロジックに基づき、ローカルゲートウェイに送信されます。次に、ローカルゲートウェイは通話を PSTN に送信します。Webex Calling 専用インスタンスでプロビジョニングされた企業ダイヤルプランは、通話を Webex Calling で登録されたエンドポイントに転送するか、ローカルゲートウェイを介して PSTN に転送するかを判断します。

専用インスタンス エンドポイントからマルチテナント エンドポイントへの呼び出し

専用インスタンスの登録済みエンドポイントとマルチテナントの登録済みエンドポイント間の通話の場合、シグナリングとメディアは Webex Calling クラウドを経由します。

図 54 マルチテナント エンドポイントから専用インスタンスへの呼び出し

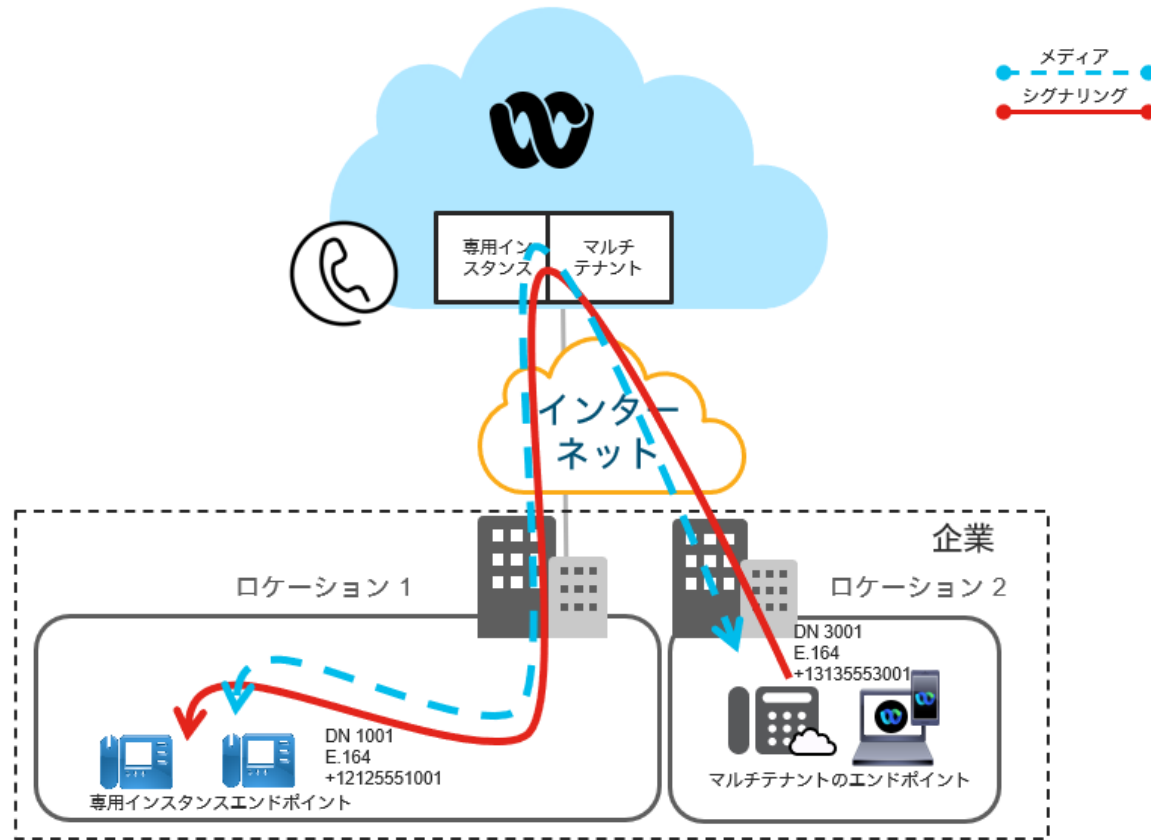


図 54 は、専用インスタンスの登録済みエンドポイントを呼び出すマルチテナント エンドポイントの例を示しています。Webex Calling ユーザーは、1001 番をダイヤルし、ダイヤルした番号が、マルチテナントでお客様用にプロビジョニングされた番号と一致していないが、その番号がダイヤルプランで構成されたダイヤルプランパターンと一致しています。したがって、このコールは、そのダイヤルプランのルーティング選択肢として選択されたトランクまたはルートグループに送信されます。事前構成されたローカルゲートウェイは、専用インスタンスに通話を送信します。事前構成されたローカルゲートウェイのコールルーティングでは、着信側の住所は考慮されません。ルーティングはトランク属性のみに基づいているため、専用インスタンスから受信した通話はすべて、マルチテナントに転送され、マルチテナントから受信した通話はすべて、専用インスタンスに転送されます。専用インスタンスは構成されているダイヤルプランを参照し、コールされた宛先がディレクトリ番号としてプロビジョニングされているローカル登録のエンドポイントにその通話をルーティングします。

コールルーティングに関する考慮事項

Webex Calling 専用インスタンスとマルチテナントのコールルーティングの考慮事項は、ケース スタディ 1a で取り上げた複数の Webex Calling ロケーションを使用する Unified CM の同じ概念と構成に従います。Webex Calling マルチテナント電話機が専用インスタンスの電話機に発信する場合、ダイヤルプランを使用して、事前構成されたトランクに通話を送信し、専用インスタンスの電話機に到達します。パートナーとお客様は、最小限の構成で既存のダイヤルプランをプラグインできます。パートナー/お客様は、専用インスタンスとマルチテナント展開の両方で事前構成されたトランクを削除しないでください。削除すると、内部ダイヤルに影響し、接続を再確立するためにサービスリクエストが必要になります。基本設定の詳細については、<https://help.webex.com/en-us/article/2vpf1/Dedicated-Instance-for-Webex-Calling---Base-Configuration> を参照してください。

モバイルおよびリモートアクセスに関する考慮事項

Expressway を介したモバイルおよびリモートアクセスは、必要に応じてリモートユーザーに展開できます。これには、WAN トラフィックへの影響を軽減するという利点があります。ICE はモバイルおよびリモートアクセスを介してサポートされているため、多くの場合、MRA を介して 2 人のユーザーが直接メディアを使用できます。一部のモバイルおよびリモートアクセスユーザーがハードウェア エンドポイントと Webex アプリの両方を持っている場合、Webex アプリが専用インスタンス Unified CM への VPN レス接続を使用すると、Webex アプリから MRA 電話機を CTI で制御することがサポートされるシナリオ (ボーダレス CTI) になります。ユーザーだけでなく、小規模オフィスもこの機能を有効活用でき、他の接続オプションの代わりに MRA を使用できます。

専用インスタンスのダイヤルプランに関する考慮事項

ダイヤルプランは、Webex Calling 専用インスタンスの主要要素で、通話に対応するすべてのエージェントにとって不可欠です。概説すると、ダイヤルプランは、コールをどのようにルーティングするかを通話に対応するエージェントに指示する役割を果たします。具体的には、ダイヤルプランは、次の主要な機能を実行します。

- エンドポイントアドレス：通話に対応するエージェントに登録された接続先の場合、アドレスは、到達可能性を提供するために割り当てられます。これらの内部の接続先には、すべてのエンドポイント (IP 電話、ビデオエンドポイント、ソフトクライアント、アナログエンドポイント) とアプリケーション (ボイスメールシステム、自動参加、会議システム) が含まれます。
- パスの選択：発信元デバイスとダイヤルされた接続先に応じて、ダイヤルされた接続先へのパスが選択されます。セカンダリパスがある場合、プライマリパスに障害が発生した場合、このパスも検討されます。
- 通話権限：特定の接続先へのアクセスを許可または拒否することによって、異なるデバイスグループにそれぞれ異なるサービスクラスを割り当てることができます。たとえば、ロビーにある電話からはシステム内部および市内の PSTN 接続先にしか到達できないようにし、その一方で、幹部社員の電話からは無制限に PSTN アクセスできるようにします。
- ダイヤル番号の操作：ダイヤルしたデバイスからダイヤルされた宛先へのパスで、ダイヤルプランによりダイヤルされた番号を操作することができます。たとえば、ドイツの PSTN の接続先に到達するために、米国のユーザーは 9011496901234 をダイヤルしますが、一方でフランスのユーザーは 000496901234 をダイヤルすると同じ接続先に到達できる場合があります。このダイヤルされる接続先は、米国のゲートウェイの PSTN トランクには 011496901234 として表示され、フランスのゲートウェイの PSTN トランクには、00496901234 として表示されます。
- 通話 ID に関する情報の表示：セッション確立中で、通話中、発信側と着信側の両方のデバイス他のデバイスに関する情報が表示されます。通話状態および方向に応じて、発信元、転送元、アラート側、接続先の情報が含まれます。ダイヤルプランは、表示される情報の形式と内容に影響するマッピングを定義できます。

専用インスタンスでダイヤルプランを実装する方法については、「[シスコ エンタープライズプリファードアーキテクチャ](#)」を参照してください。



Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1005R)