Webex Meetings および Calling 用の Webex Edge Connect のシスコ プリファード アーキテクチャ

設計概要

2022 年 7 月

目次

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：お客様とセールスチーム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。

このマニュアルについて

*Webex Edge Connect シスコ プリファード アーキテクチャ*は次を対象としています。

- コラボレーション ソリューションを設計し販売するセールス チーム

Webex Edge Connect のアーキテクチャと、そのコンポーネントおよび設計上の一般的なベストプラクティスを理解したいと考えているお客様および営業チーム

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、展開、実装の詳細については、Cisco Collaboration Preferred Architectures 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 Edge Connect は QoS サポート対象の専用マネージド IP リンクです。Equinix Cloud Exchange（ECX）でのダイレクトピアリングを通じてオンプレミスから Webex に接続します。会議をインターネットから隔離できるため、輻輳、パケット損失、ジッター、遅延の問題が軽減されます。パブリックインターネットにさらされないため、潜在的な脅威や攻撃に対する防御を強化できます。

テクノロジーの使用例

企業はビジネス プロセスを合理化し、従業員の生産性を向上させ、パートナーや顧客との関係を強化することを求めています。Webex Edge Connect シスコ プリファード アーキテクチャ（PA）は、Webex Cloud サービスに直接接続と専用の高速帯域幅を提供します。さらに、次に挙げるテクノロジーの使用例では、組織が新しい先進的なビジネス プロセスを策定し、以下の領域でさらに多くの価値を生み出す機会を提供します。

- **専用帯域幅：**Webex Meetings サービスへの専用帯域幅スループットと低遅延アクセス
- **会議とコールの品質：**Webex Edge Connect で、会議や通話に支障をきたすことなく、日々のコア業務を行うことができます。一貫性、信頼性、コスト効率に優れた、セキュアなエクスペリエンスがユーザーに保証されるからです。
- **強化されたセキュリティ：**Webex Edge Connect のダイレクトピアリング機能により、接続品質にばらつきがあるインターネットから会議とコールを隔離できます。Edge Connect を利用すれば、パブリックインターネットにおける潜在的な脅威や攻撃から会議を保護できます。

利点

- 専用回路（インターネット経由ではありません）
- ネットワークパスの設定
- 予測可能で安定した遅延とジッター
- 保証帯域幅
- 速度オプション：200M、500M、1G、5G、10G

オーダー可能なサービス

- Webex Meetings
- Webex Events
- Webex アプリ、Webex デバイス、Webex Video Mesh メディア*
- ビデオデバイス対応 Webex Meetings
- Webex Edge Audio
- Webex Calling サービスとコンポーネント**

*Webex アプリ、Webex デバイス（Board、Room、Desk）および Webex ビデオメッシュでは、HTTPS/SSL 経由のシグナリングにインターネットアクセスが必要です。

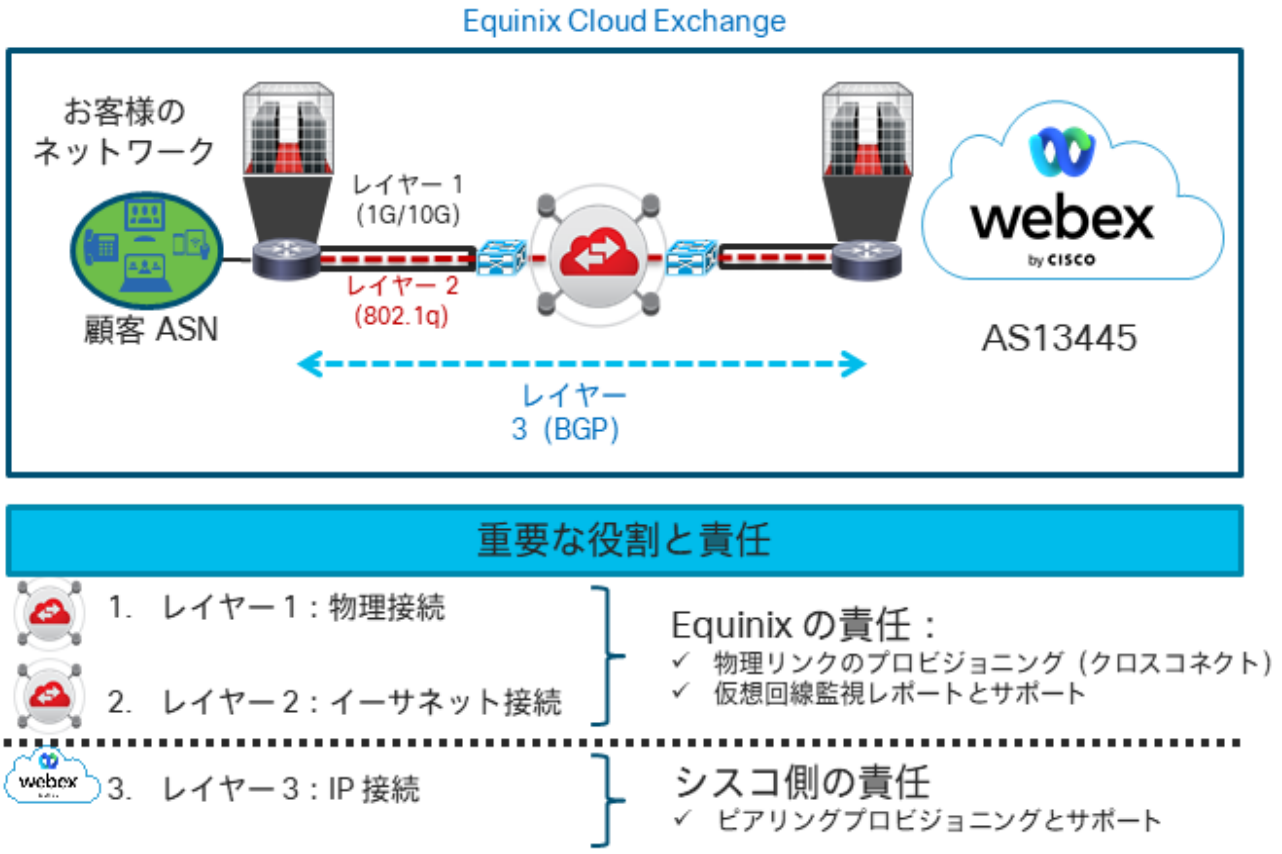
**Webex Calling では、さまざまなサービスに対するインターネットアクセスも必要です。

アーキテクチャ

Webex Edge Connect は、Equinix Cloud Exchange Fabric 使用して、お客様のオンプレミスからクラウドへと接続する専用で、管理された、Quality-of-Service（QoS）をサポートする IP リンクです。この専用のピアリング接続により、インターネットの変動性から会議が隔離され、輻輳、パケット損失、ジッター、遅延が減少します。また、パブリック インターネットに公開されていないことは、潜在的な脅威や攻撃からの保護が向上していることを意味します。このセットアップにより、Webex バックボーンによって強化された Webex Meetings および Calling の品質と速度が向上します。直接接続により、一貫性のあるネットワークパフォーマンスとセキュリティの強化がもたらされ、会議および Calling の品質が向上します。

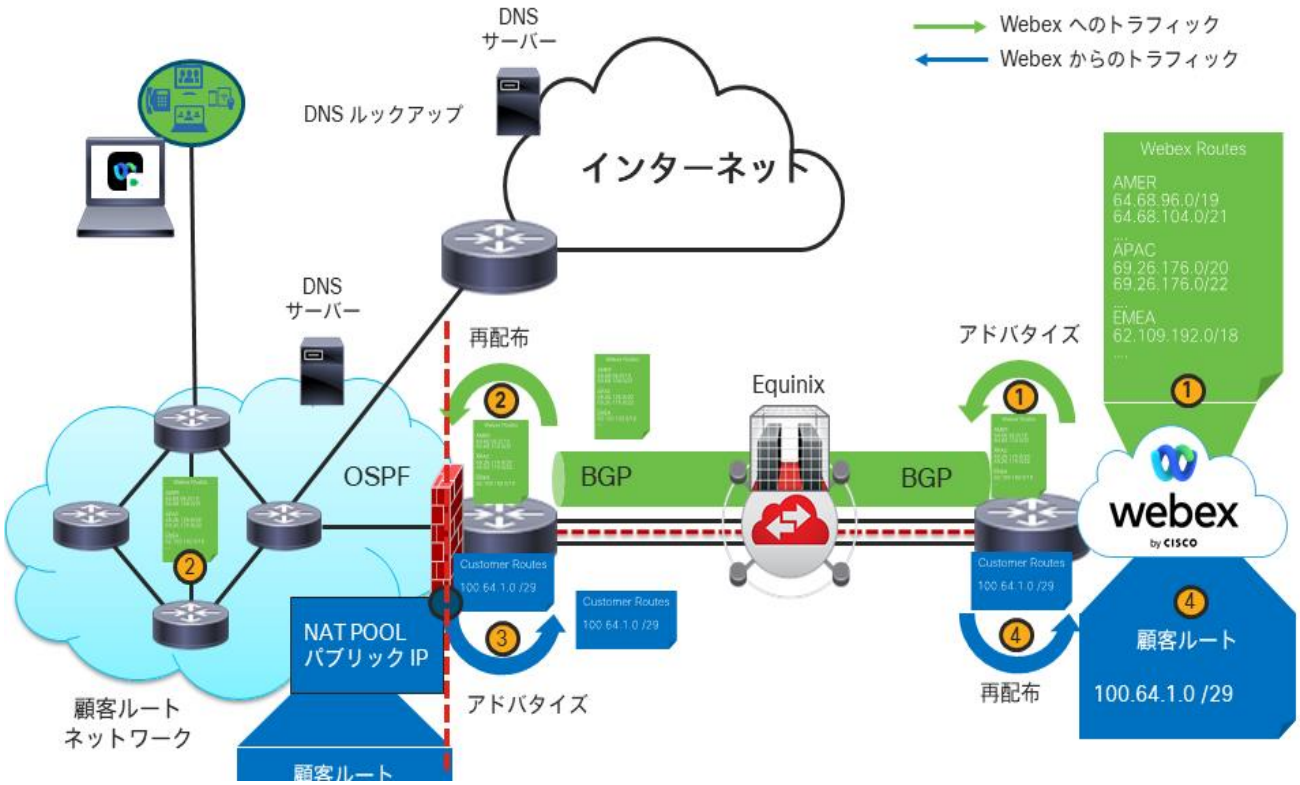
図 1 は、ソリューションの概要を示しています。Equinix Cloud Exchange Fabric（ECX）は、エンドカスタマーを Webex Meetings データセンターと相互接続し、Webex 宛てのトラフィックを BGP（ボーダー ゲートウェイ プロトコル）ピアリングリンク経由で直接ルーティングします。Equinix は、顧客と Webex 間のレイヤー 2 相互接続を管理し、担当します。シスコはレイヤー 3 BGP ピアリングの一方の側を管理し、顧客は自分の側のレイヤー 3 BGP ピアリングを管理します。

図 1　　Webex Edge Connect



Webex からのルートアドバタイズメントを通じて、顧客はピアリングリンクを介して Webex トラフィックをルーティングします。図 2 は、アドバタイズメントルーティングの概要を示しています。番号が付けられた各ステップは、図で数字により強調表示されています。

図 2　　Webex トラフィックルーティング



1) Webex は、ピアリングリンクを介してすべての Webex Meetings および Calling データセンター プレフィックス（サブネット）をアドバタイズします。

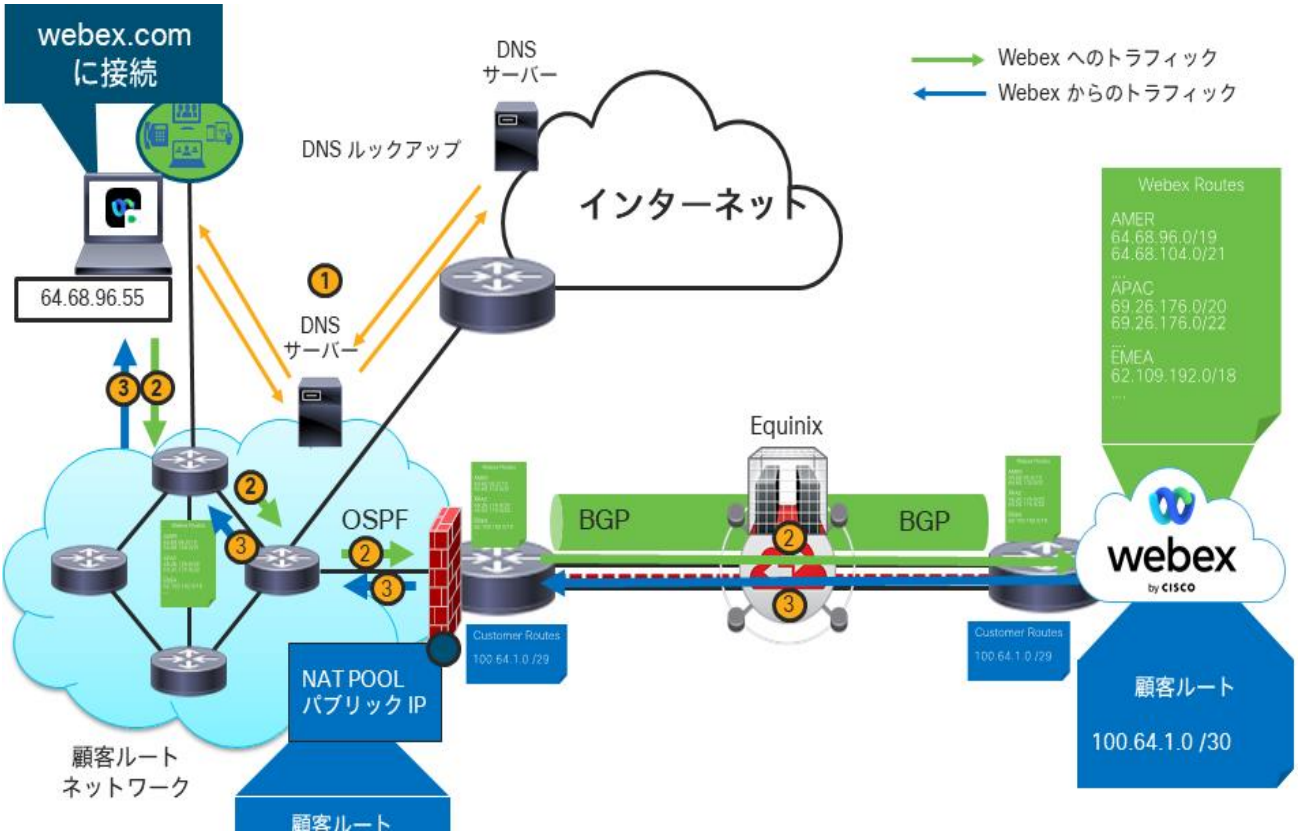
2) 顧客のルータは Webex DC プレフィックス（サブネット）を受信して、それらを内部ルーティングプロトコルで再配布します。ここでは、OSPF がプライベート ルーティング プロトコルの例として使用されています。その後、WebexDC で利用されているサブネットは顧客のルーティングテーブルで使用可能になり、該当するトラフィックはピアリングリンクを流れるようになります。

3) 企業のインターネット接続と同様に、BGP ピアリング接続にはパブリック IP アドレス空間が必要です。そのため、顧客はプライベート IP からパブリック IP に NAT するために使用される IP アドレスのプールを用意する必要があります。これらのアドレスは、顧客のピアリングルータによって Webex BGP ネットワークピアにアドバタイズされます。

4) Webex ルータは顧客によってアドバタイズされた IP アドレススペースを Webex ネットワークに再配布します。これにより、その NAT IP アドレスプールからのリターントラフィックが可能になります。

図 3 は、Webex Meetings デスクトップ アプリケーションによるコールルーティングの簡略化された例と、Edge Connect を介して Webex DC に到達するためのトラフィックパスを示しています。番号が付けられた各ステップは、図で数字により強調表示されています。

図 3　　Edge Connect を介した Webex Meetings デスクトップ アプリケーションのルーティング



1) クライアントは DNS ルックアップを実行して Webex サービスに接続します。この DNS 要求は、例としてインターネットの従来のパスを経由します。Edge Connect を介して DNS をルーティングできる場合があります。詳細については、DNS に関する考慮事項を参照してください。

2) クライアントが接続先のサーバーの IP アドレスを解決したら、図 2 のステップ 1 および 2 で Edge Connect を介してアドバタイズされた Webex サブネットに含まれる該当の IP アドレスを利用しているサーバーに接続します。顧客のネットワークルーティングでは、これらのプレフィックス（サブネット）を使用して、トラフィックを Edge Connect ピアリングに転送できるようになったため、トラフィックはこのパスを介して Webex DC に送信されます。この時点で、顧客の Edge Connect ネットワークのエッジで NAT が実行され、ピアリングリンクを通過する前に IP アドレスがプライベートからパブリックに変換されます。

3) NAT サーバーを元とするこれらのルートは、図 2 のステップ 3 および 4 で顧客のルータによってアドバタイズされたため、リターントラフィックの宛先は Webex DC によって認識されていますしたがって、リターントラフィックには、ピアリングリンクを介して NAT サーバーに戻るルートと、NAT サーバーからクライアントに戻るルートがあります。

注：　このソリューションはレイヤー 3 ルーティングソリューションであるため、さまざまなタイプの Webex トラフィックコンポーネント、エンドポイント、クライアント、または Webex ミーティングサイトに基づいてルーティングすることはできないことに注意することが重要です。すべてのタイプの Webex トラフィックは Edge Connect を通過し、このルーティング動作を変更するためのコンポーネント、クライアント、または Webex ミーティングサイトの指定に対する特定のフィルタ処理はありません。

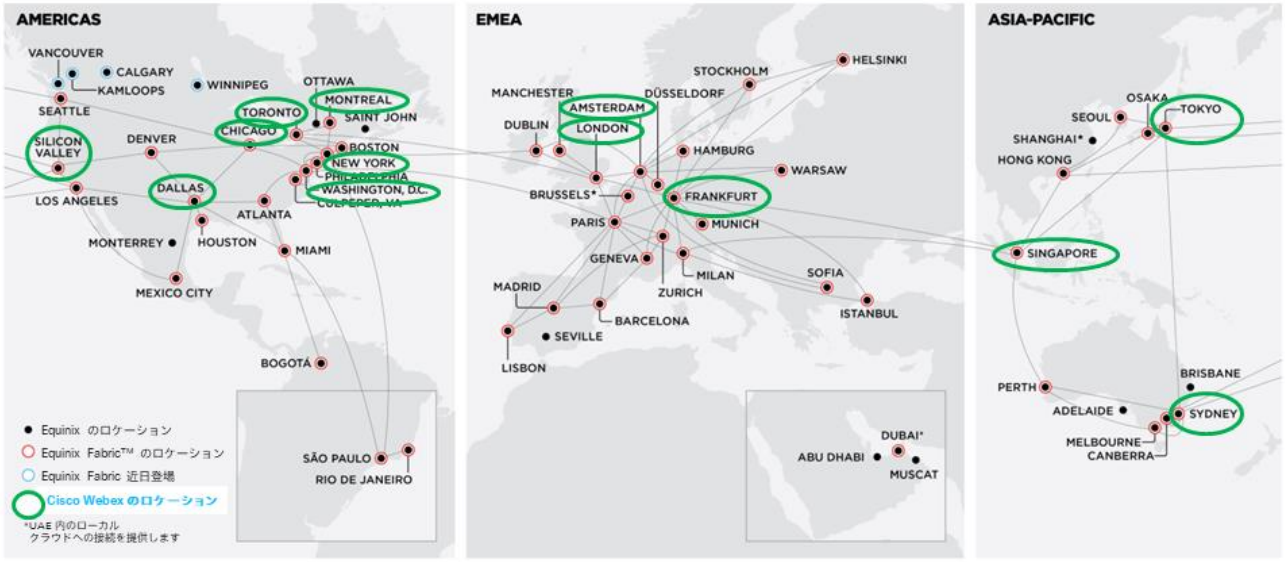
Equinix の施設と Webex DC コロケーション

Webex データセンター（DC）は、複数の Equinix Cloud Exchange ロケーションに配置されています。図 4 は米国と海外のロケーションを示しており、図 5 は、これらの同じロケーションを Equinix Cloud Exchange ロケーションマップに重ねて示しています。

図 4　　Equinix 設備に配置された Webex DC のリスト

北米の拠点	世界の拠点
アッシュバーン（米国バージニア州）	アムステルダム（オランダ）
シカゴ（米国イリノイ州）	ロンドン（英国）
ダラス（米国テキサス州）	フランクフルト（ドイツ）
ニューヨーク（米国ニューヨーク州）	シンガポール（シンガポール）
シリコンバレー（米国カリフォルニア州）	シドニー（オーストラリア）
モントリオール（カナダ）	東京（日本）
トロント（カナダ）	

図 5　　Equinix 設備とオーバーレイされた Webex DC コロケーション



Webex Edge Connect のコンポーネントとロール

このセクションでは、さまざまなソリューション コンポーネントと、ソリューションにおけるコンポーネントのロールについて説明します。このディスカッションでは、Webex Edge Connect コンポーネントを Webex Meetings ソリューション コンポーネントから分離することが重要です。次のセクションでは、Webex Edge Connect ソリューションのコンポーネントとロールについて説明します。

Webex Edge Connect は基本的に、ダイレクト ピアリング ソリューションのルーティングおよびスイッチング コンポーネントで構成されており、通常はインターネット（クラウド）に向かう Webex トラフィックを、ダイレクトピアリングを介して顧客エッジルーティングを介して Webex バックボーンにリダイレクトできます。前のアーキテクチャ図（図 1）で述べたように、Equinix はレイヤー 2 部分を管理し、Webex はレイヤー 3 IP BGP ピアリングを管理します。

Equinix Cloud Exchange（ECX）

Equinix Cloud Exchange（ECX）は、Webex Meetings などのクラウドプロバイダーへのオンデマンドおよび直接アクセスを可能にする相互接続ソリューションです。ECX ソリューションには、いくつかの共通コンポーネントがあります。以下に、これらのコンポーネントとそのロールのいくつかを示します。

Equinix Cloud Exchange（ECX）ポータルは、顧客向けのポータルであり、顧客がポートとクラウド サービス プロバイダーへの接続を注文および構成できるようにします。

回路、ファブリックポートおよび接続

Equinix の ECX ポータルには、クラウドプロバイダーを注文して接続するための特定の名称があります。これらの概念を理解して、設計構成のどこに適合するかを知ることが重要です。

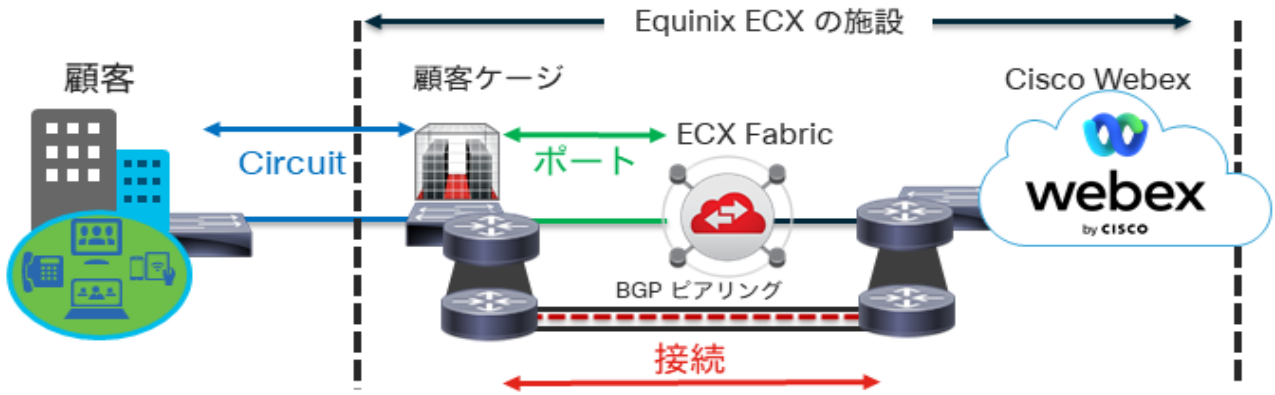
物理回路：お客様の建物と Equinix 設備間のネットワーク回路。この回路は通常、メトロイーサネットですが、他のタイプの物理回路である場合もあります。この回路は、Equinix へのすべてのトラフィックを実行し、複数のクラウドプロバイダーへのトラフィックを実行する場合があります。

Equinix Fabric の「ポート」：ファブリックポート、または単に「ポート」は、ECX ファブリックからケージ内のお客様の機器（ルータまたはスイッチ）に接続されている、ECX で注文された物理ポートです。このファブリックポートは、カスタマーケージ機器を ECX ファブリックに接続します。ポートは、そのポートに割り当てられた帯域幅まで、単一のプロバイダーまたは複数のプロバイダーに使用できます。たとえば、10G ポートは、10 の異なるクラウドプロバイダーへの 10 件の 1G 接続を行う可能性があります。

Equinix の「接続」：これは、顧客が ECX ポータルを使用して、クラウドプロバイダーへの接続リクエストを送信する場所です。この送信には、ピアリングのすべての BGP およびルーティング情報と、Webex Edge Connect に対するシスコの発注書（PO）番号が必要です。Webex Edge ライセンスの詳細については、Webex Edge データシートにアクセスしてください。

図 6 は、これらの ECX コンポーネントが設計全体のどこに存在するかを示しています。

図 6　Equinix Cloud Exchange のコンポーネントとロール：回路、ファブリックポート、および接続

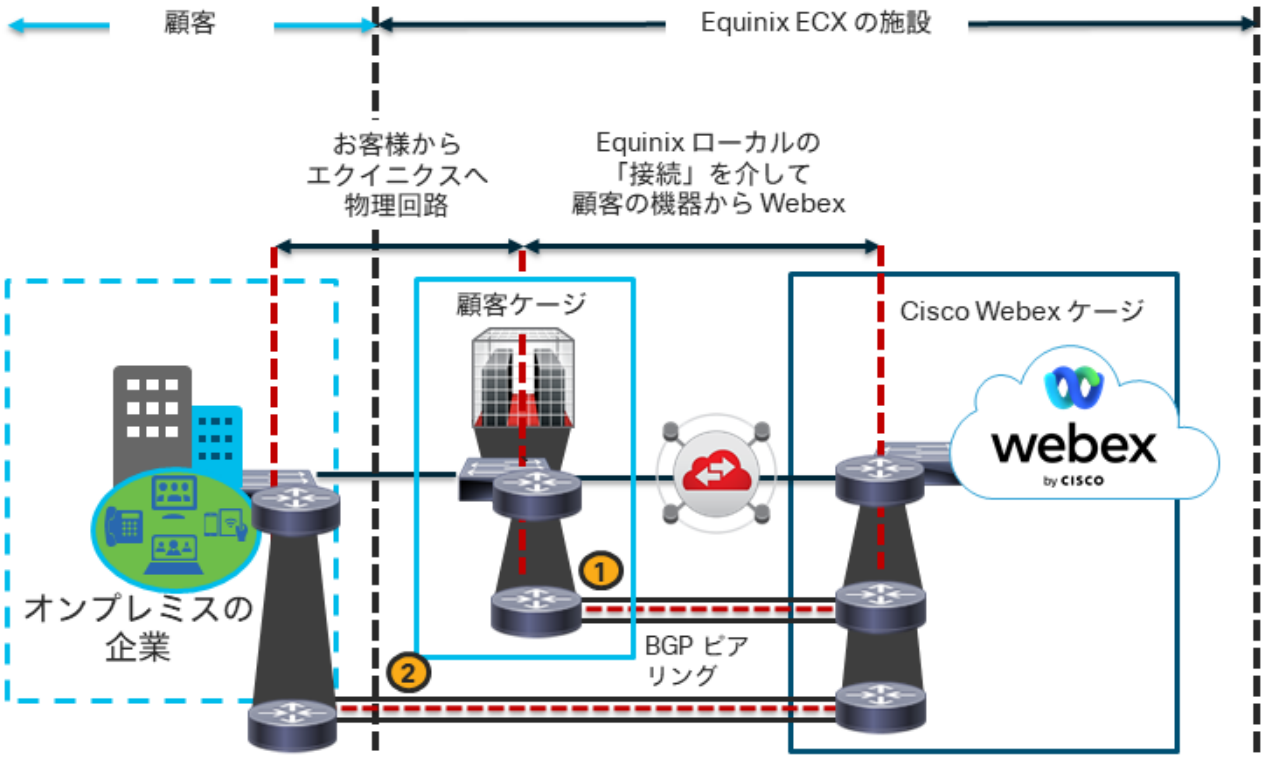


ローカルおよびリモート接続（BGP ピアリングオプション）

Equinix には、ローカル「接続」とリモート「接続」という 2 つの主要な BGP ピアリングオプションがあります。ローカル接続は、上の図 4 および図 5 に Webex ロケーションで示されているように、Webex が同じ場所に配置されている Equinix のケージに顧客の機器がある場所です。リモート接続は、Webex が同じ場所に配置されていない Equinix ロケーションのケージに顧客の機器があるため、Equinix Cloud Exchange からの「リモート接続」が必要な場所です。Equinix の場所は、図 5 に小さな赤い点で示されています（他にもあるため、Equinix Cloud Exchange で最新情報を確認してください）。顧客が Webex が配置されていない ECX ビルに接続している場合、Webex が同じ場所にある ECX ロケーションに接続するために、リモート接続を購入する必要があります。

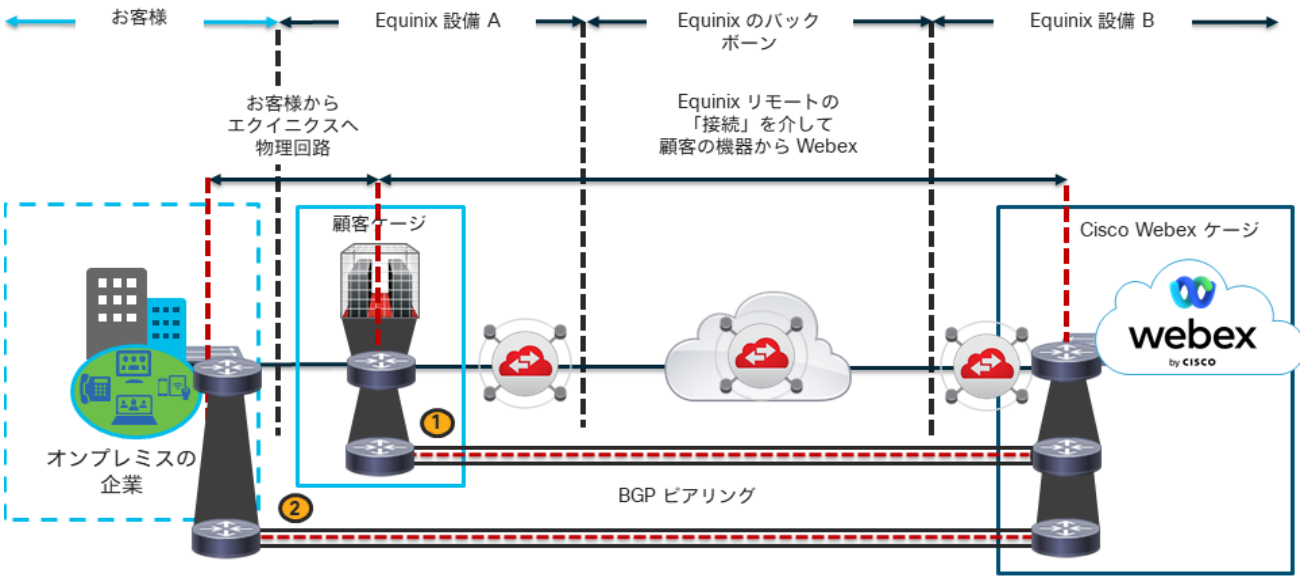
ローカル接続を図 7 に示します。ローカル接続を使用すると、顧客は BGP ピアリング用のルータを Equinix ケージ（図 7 – 1）または企業に配置し、レイヤー 2 経由で Equinix ケージ（図 7 – 2）に接続できます。

図 7　　Edge Connect ローカル接続（顧客ケージ経由）



リモート接続を図 8 に示します。リモート接続により、顧客は BGP ピアリング用のルータを Equinix ケージ（図 8 – 1）または企業に配置し、レイヤー 2 経由で Equinix ケージ（図 8 – 2）に接続できます。

図 8　　Edge Connect リモート接続（顧客ケージ経由）



Webex Edge Connect のコア要件

- BGP とピアリングの原則に精通した IT チーム 。おそらく、このサービスで最も見過ごされているエリアの 1 つです。お客様は、ネットワークアーキテクチャとエンジニアリングに対して責任を負います。非対称ルーティングと最適でないネットワークパスを回避することが重要です。社内にネットワーキングの専門知識がないお客様は、展開を成功させるために、パートナーまたはシスコアドバンスドサービスの利用を検討する必要があります。
- 顧客オフプレミスから Equinix ECX 施設まで確立された回路
- Equinix Cloud Exchange（ECX）アカウントと ECX の Rackspace
- 企業ネットワーク接続用の BGP および Dot1Q タギングをサポートするルータ
- ECX Fabric への接続に利用できる物理ポート [1G/10G 標準]
- さまざまな Webex デバイス シグナリング サービスで利用可能なインターネット接続（詳細については、以下のトラフィックフローを参照）
- **IP アドレス要件**
    - 顧客が所有する IP アドレス：これには、BGP ピアリング接続の両側のアドレスと、プライベートネットワークからパブリックネットワークへの NAT を実行するために使用される、顧客側からアドバタイズするルートが含まれます。
        - BGP ピアリングリンクアドレス空間（パブリック IP）/30 または /31 をサポート
        - アドバタイズされる IP スペース ： パブリックおよびプロバイダーに依存しないアドレス空間が必要です。 Edge Connect は、RFC1918 のようなプライベート IP アドバタイズメントを受け入れません。このアドレス空間は、プライベート IP アドレスから Edge Connect を介してルーティングされるパブリック IP アドレスに変換するために使用されるカスタマーエッジ で利用する NAT プール空間です。
    - 自律システム番号（ASN） ： パブリックまたはプライベートの 2 バイトまたは 4 バイト ASN のサポート
    - Webex がアドバタイズするプレフィックスの最大長は /24 です
    - Webex が受け入れる最大長のプレフィックスは /29 です
    - Webex が受け入れるルートの最大数は 100 です
    - Webex がアドバタイズするルートの数は今後変わる可能性があるため、BGP ピアリング上で Webex から 500 のルートを許可できるように設計することをお勧めします。
    - 双方向フォワーディング検出（BFD）がサポートされ、Webex Edge ルータで 300 ミリ秒 X 3 のデフォルト値で有効になっています

ECX ポータルでの接続の作成（例）

Edge Connect「接続」（ピアリング）リクエスト前の顧客要件

1. 顧客には、Equinix Cloud Exchange（ECX）への回路が必要です
2. また、通常、ECX のケージ内に機器（ルータ/スイッチ）が必要です
3. 接続要求を行うために使用できるポートも必要です。ポートは、ケージから ECX バックボーンまでに作成された物理回路です。上の回路、ファブリックポート、および接続を参照してください
4. Cisco Commerce Workspace からの Edge Connect 購入のシスコ発注書番号（PO 番号）

図 9　　Webex への ECX ポータル接続リクエスト：送信元と接続先のロケーション選択ページ

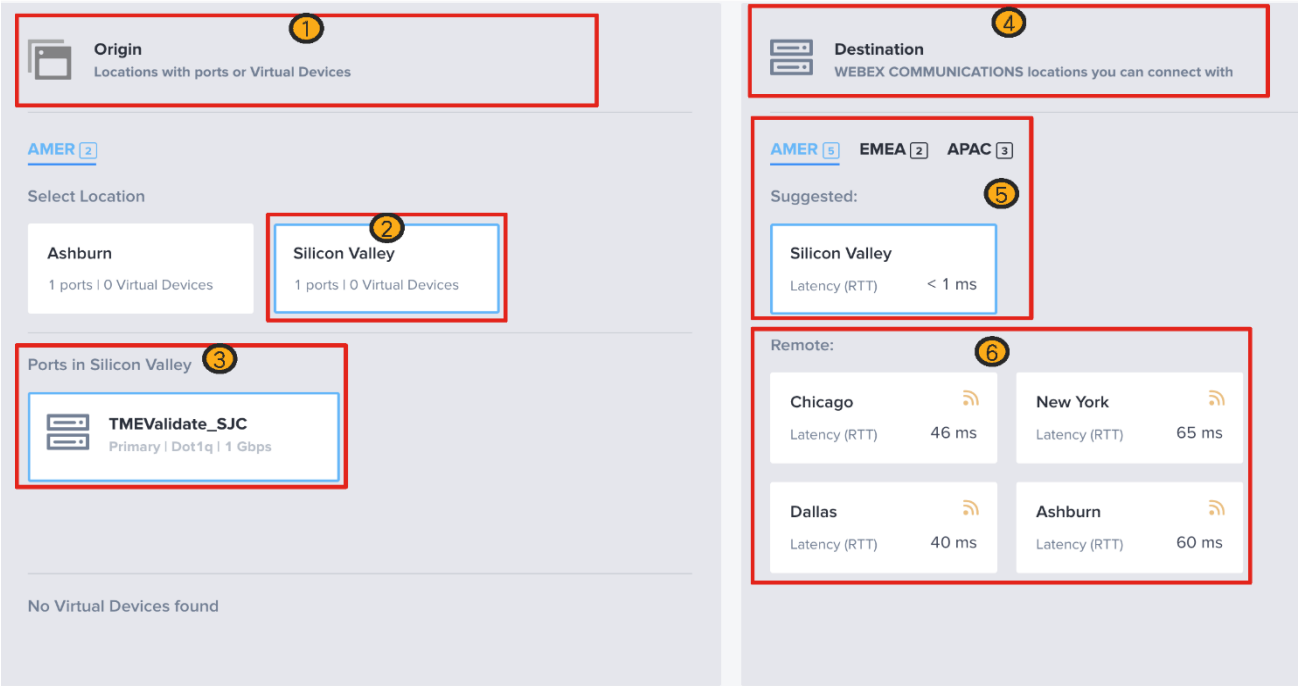


図 9 は、ECX ポータルの Webex 接続リクエストの最初のページを示しています。ここで、送信元ロケーション（顧客）と接続先ロケーション（Webex）が選択されます。次の番号は、図 9 に表示された番号に対応しています。

1. 発信元の場所：顧客の機器が存在し、使用される ECX ポートが置かれる場所。
2. シアターごとに分類された、この正確な送信元の場所。この例では、AMER が選択されたシアターであり、シリコンバレーがケージの場所であり、ポートが構成されたルータが存在します。
3. これは、ECX で構成され、この接続に使用するために選択されるポートです。
4. 接続先の場所: この接続をターミネートするために選択された Webex DC の場所。

注：　接続先側に選択するポートはありません。Webex はこれに応じてポートを関連付けます。同じ顧客の同じサイトへの複数の接続がある場合、シスコはポートとハードウェアの冗長性を確保するために、それらの接続を 2 つの別個のルータ（宅内機器）に設定します。

5. シアターごとに分類されたこの正確な接続先のロケーション。この例では、この接続をローカル接続にする必要があるため、AMER のシリコンバレーが同様に選択されています（図 7 を参照）。
6. これらは、リモート接続を作成する場合に利用される場合がある、 Webex が配置された ECX 設備です（図 8 を参照）。

図 10　　Webex への ECX ポータル接続リクエスト：接続の詳細ページ

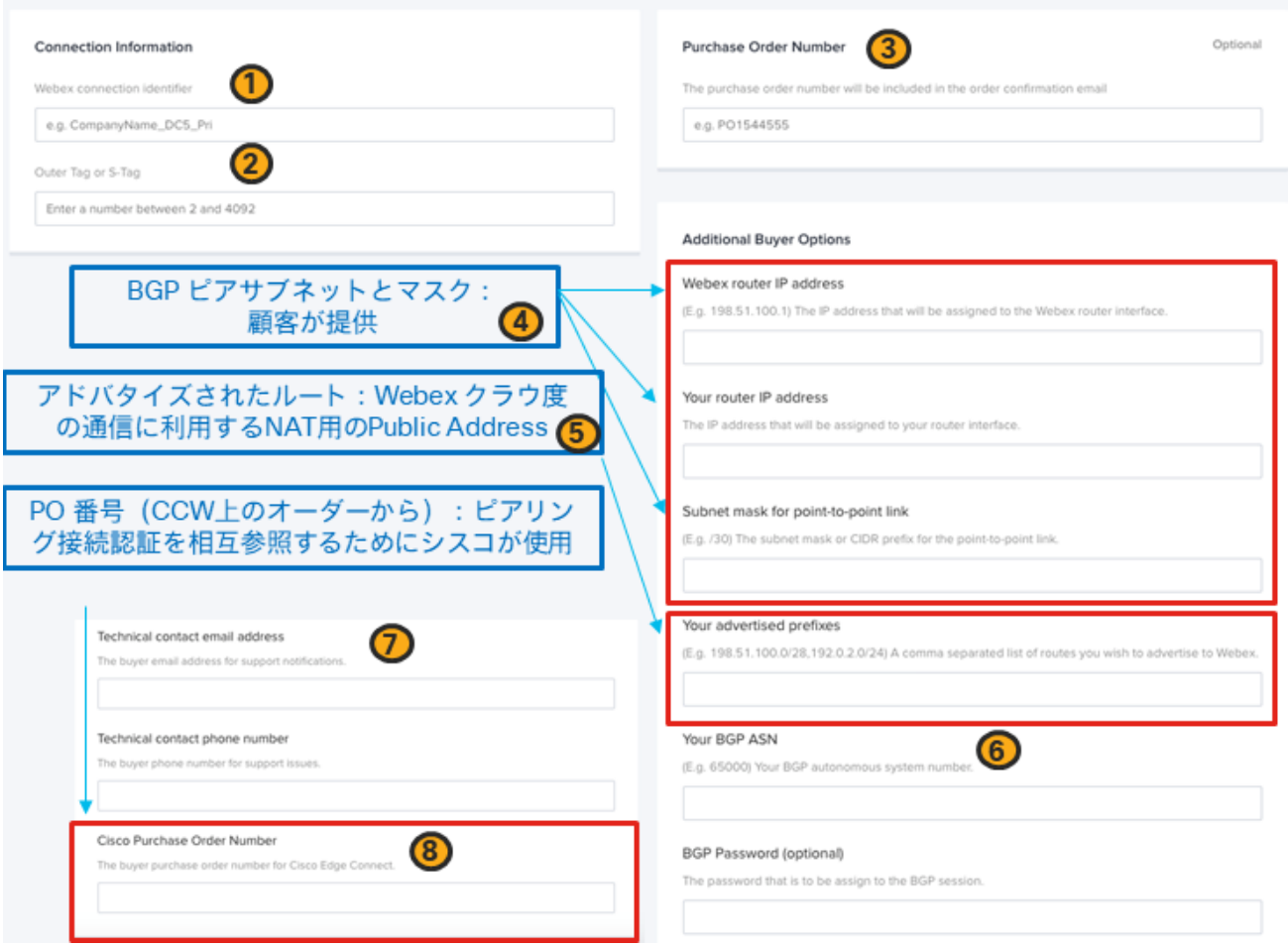


図 10 は、ECX ポータル構成の次のページを示しています。これは、下の「ECX 接続要求リクエスト」セクションで強調表示されている接続の詳細を入力する場所です。次の番号は、図 10 に表示された番号に対応しています。

ECX 接続リクエストの要件

1. Webex 接続識別子：これは、Equinix ECX ポータルで、買い手（顧客）と売り手（Webex）の両方に表示される接続の名前です。この名前は、サービスを提供している顧客及びリンクの目的を示すものであると便利です。たとえば、顧客の名前が Enterprise1 で、この接続が「シリコンバレー」の場所のプライマリ接続である場合、役立つ命名規則は Enterprise1_SV_PRI で、同じ場所のセカンダリ接続は Enterprise1_SV_SEC になります。
2. VLAN ID（顧客と Equinix の間の接続で利用）
    a. シンプルにするために、0x8100 の標準 EtherType で標準 802.1q（Dot1q）フレーミングを使用して、 Equinix Cloud Exchange イーサネットポートをプロビジョニングすることをお勧めします。これらはトランクに関連付けられた通常の値であり、キャリアが通常使用する複雑なメトロイーサネット設定（qinq）は含まれていません。
3. 発注書番号：これは無視してかまいません。使用するのはページの下部にあるものです（ステップ 7）
4. 1 番目のパブリック IP 範囲：BGP ピアリングサブネット（（/30 または /31）：顧客側および Webex 側）

5. 2 番目のパブリック IP 範囲：NAT に使用され、BGP ピアリング経由で Webex にアドバタイズされるサブネット（最大 /29 ~ 最大 100 のサブネット）
6. パブリックまたはプライベート ASN + パスワード（32 ビット対応）
7. 技術担当者（つまり、管理者グループのエイリアス + 電話番号）
8. シスコ発注書（PO）番号（Edge Connect 発注時のもの）

図 11　Webex への ECX ポータル接続リクエスト：接続の詳細ページ：接続速度

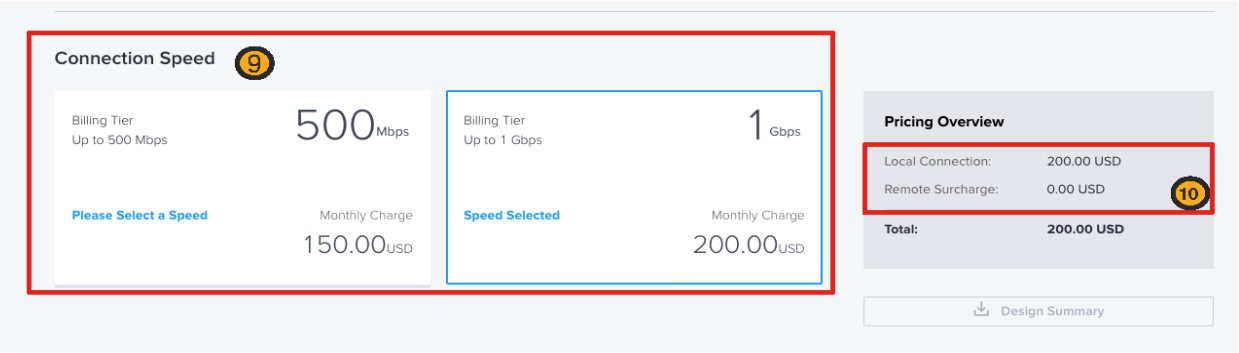


図 11 は、接続速度の選択を示しています。図 11 – 8 は、図 9 – 3 で選択したポートで使用できる速度オプションの例を示しています。図 11 – 9 は接続料金を示していて、これにはローカル接続料金が含まれており、Webex 接続先ロケーションが図 9 で選択されたポートの場所に対してリモートである場合、リモート追加料金が表示されます。次の番号は、図 11 に表示された番号に対応しています。

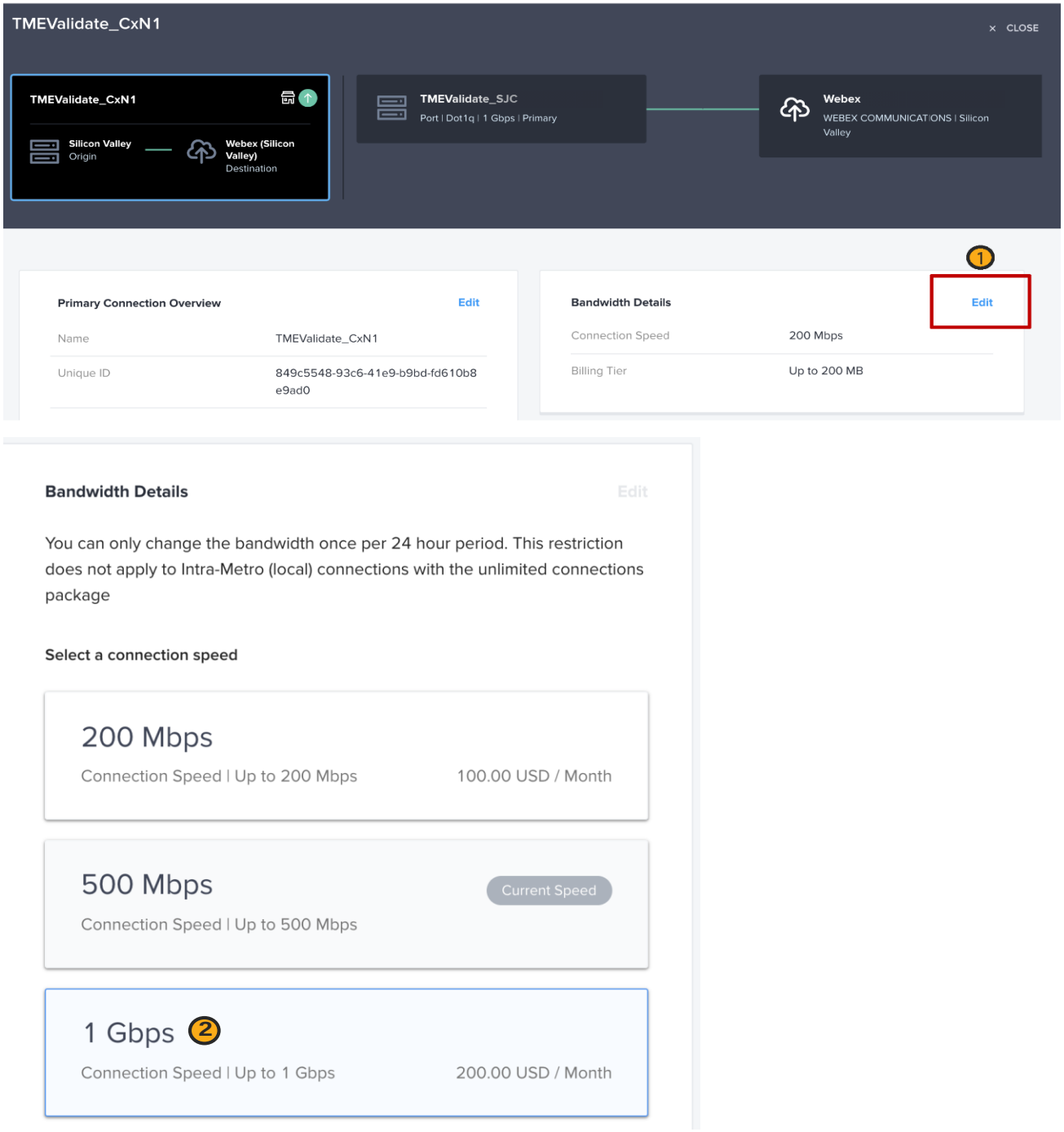
9. プロビジョニングへのリンク速度：200mb、500mb、1gb、5gb、10gb
10. 価格の概要：これには、価格と、リモート接続の追加料金があるかどうか、またはローカル接続のみかどうかが表示されます。

ECX ポータルでの接続帯域幅の増加

帯域幅の使用量が限界に近づき始めている場合は、アップグレードの時期です。幸いなことに、これは非常に簡単な修正であり、利用可能な帯域幅のあるポートに接続している限り、サービスが中断されることはありません。したがって、たとえば、10GB ポートが Equinix ECX ファブリックに接続されていて、そのポートで 1GB 接続が確立されている場合、ECX ポータルで接続の帯域幅を追加するリクエストを行うだけで簡単に接続をアップグレードすることができます。一方、1GB ポートが Equinix Fabric に接続されていて、1GB 接続が確立された場合は、別のポートを接続または使用する必要があります。この場合、要求された帯域幅の合計に対して十分な帯域幅を備えた新しいポートを確立する必要があるため、帯域幅のアップグレードはより複雑になります。

新しいポートが必要な場合は、新しいポートをインストールして新しい接続を作成することをお勧めします。新しい接続と BGP ピアリングが起動し、アドバタイズを渡すようになった後は、古い接続を除外して削除できます。

図 12　　ECX ポータルでの接続帯域幅の増加



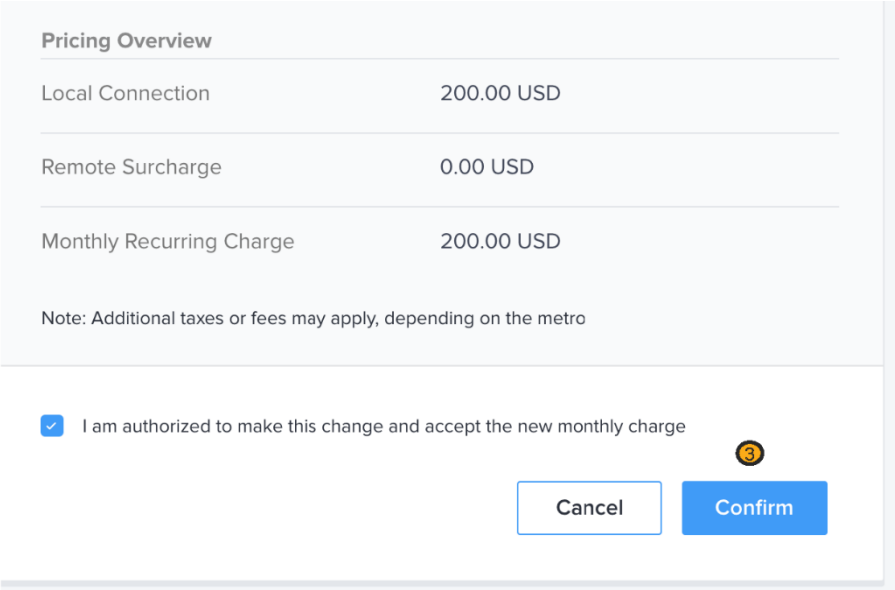


図 12 – 1 は、接続の帯域幅をアップグレードするために編集する必要がある接続と帯域幅の詳細を示しています。図 12 – 2 は、[編集] を選択し、1Gbps 接続速度へのアップグレードを選択した後の帯域幅の詳細を示しています。図 12 – 3 は、価格設定の詳細の概要と注文の確認を示しています。確認が選択されると、Webex はキューにリクエストを受け取ります。Webex には、更新された発注書番号（PO 番号）も必要です。次の情報を csq-peering@cisco.com に E メールで送信して、この送信をフォローアップすることが重要です。

- **会社名：**これは、接続をサブスクライブしている会社の名前です。これは、リセラーやサービスプロバイダーにとって、顧客の会社名が含まれていることを確認するために重要です。
- **接続の名前：**これは、「プライマリ接続の概要」セクションの図 12 – 1 に示されている接続の名前です。
- **発注書番号**：これは、更新された帯域幅要求に対応する PO 番号です。
- **自律システム番号（ASN）**：これは、接続ページの「追加の購入者オプション」で構成された BGP ASN です（接続の詳細ページでの場所については、図 10 を参照してください）。

Webex が ECX 送信リクエストを受信し、接続に関連付けられた PO 番号を検証できると、接続の Webex 側ルータ（販売者側）をリクエストされた速度に更新します。完了すると、ECX ポータルでリクエストを承認し、これにより、ECX ファブリックでの接続の両側で ECX ファブリックの速度変更の自動構成が有効になります。その時点で、この接続をホストする顧客機器のインターフェイス構成の帯域幅を変更することが適切です。

Edge Connect を介した Webex Meeting トラフィックフロー

このセクションでは、Webex Edge Connect を介してトラフィックを送信するさまざまな Webex 製品およびコンポーネントからのトラフィックフローについて説明します。前述のように、次の Webex サービスは Webex Edge Connect 経由でサポートされています。

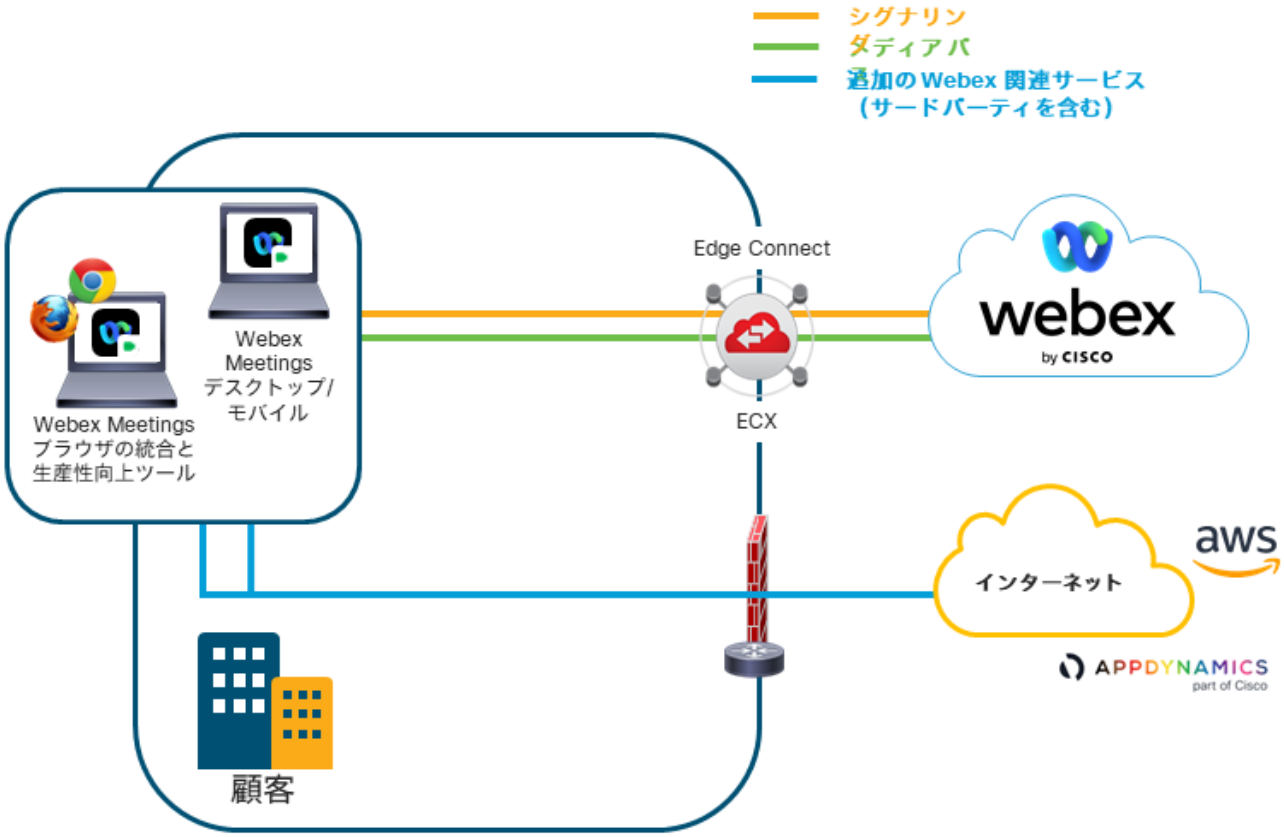
- Webex Meetings
- Webex アプリ メディア（Webex アプリ、Webex デバイス（Board、Room、Desk）およびビデオ メッシュには、シグナリングのためにインターネットアクセスが必要）
- ビデオデバイス対応 Webex Meetings
- Webex Edge Audio

Webex Meetings のトラフィックフロー

Webex ミーティングには、いくつかの異なるエンドポイントとクライアントが参加できます。以下は、Webex ソリューション コンポーネントとそれらに関連付けられたトラフィックフローをまとめたものです。Webex Edge Connect が展開されている場合に、シグナリング及びメディアが Edge Connect パスまたはインターネットパスの関連付けられた出口を通過するフローを示しています。

Webex Meetings デスクトップアプリケーション

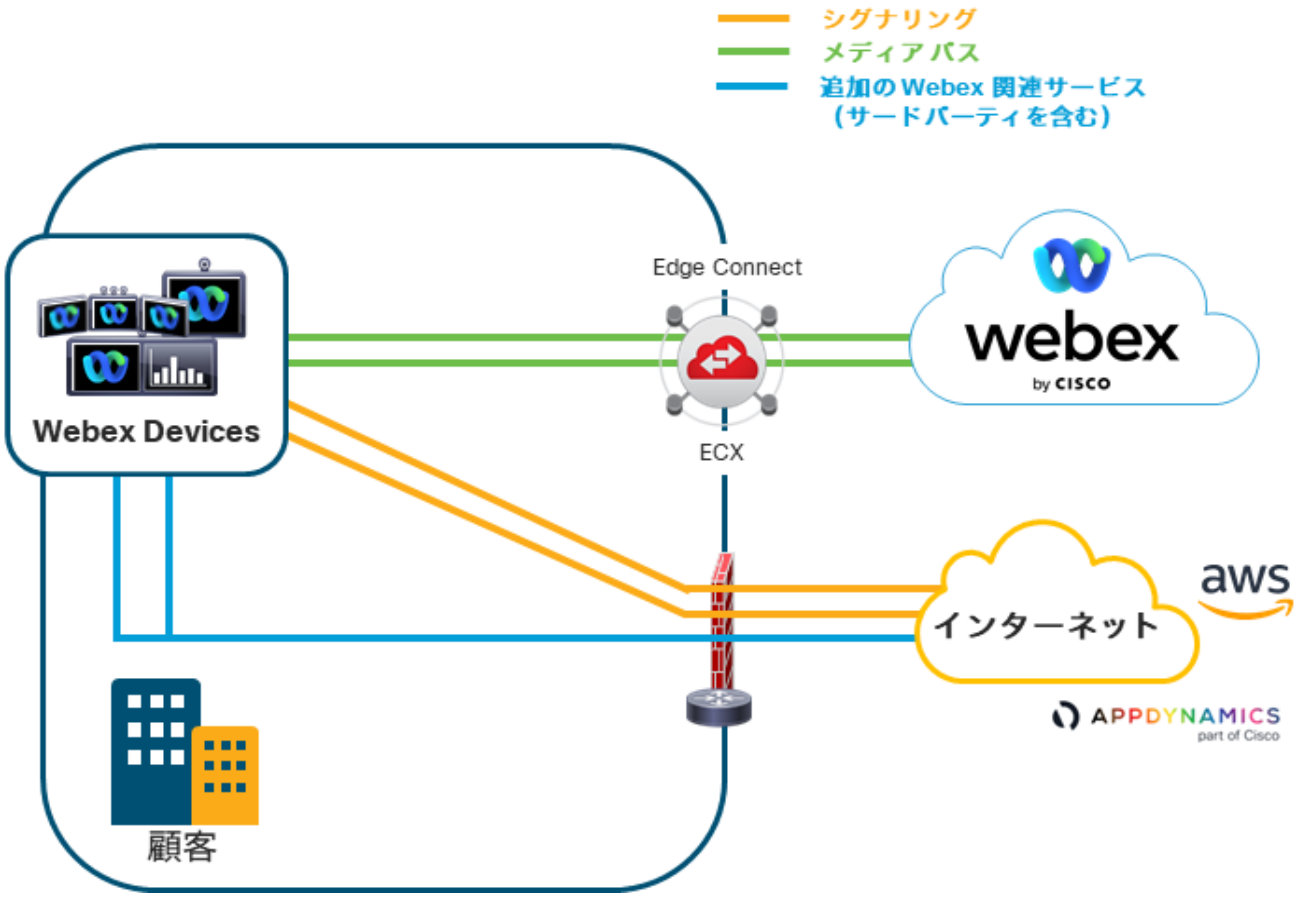
図 13　Webex Meetings デスクトップ アプリケーション、Webex 生産性向上ツール、および Webex Meetings ブラウザインテグレーション



上の図（図 13 ） では、Webex Meetings デスクトップ アプリケーションと Webex Meetings ブラウザおよび生産性向上ツールが、Edge Connect ピアリングを介してシグナリングとメディアを送信します。

Webex Devices

図 14　Webex Devices



上の図（図 14）では、Webex Board と Webex デバイスは、Edge Connect ピアリング経由でメディアのみを送信します。コール制御と分析のためのシグナリングはすべてインターネットを経由します。

Webex アプリ

図 15　　Webex アプリ

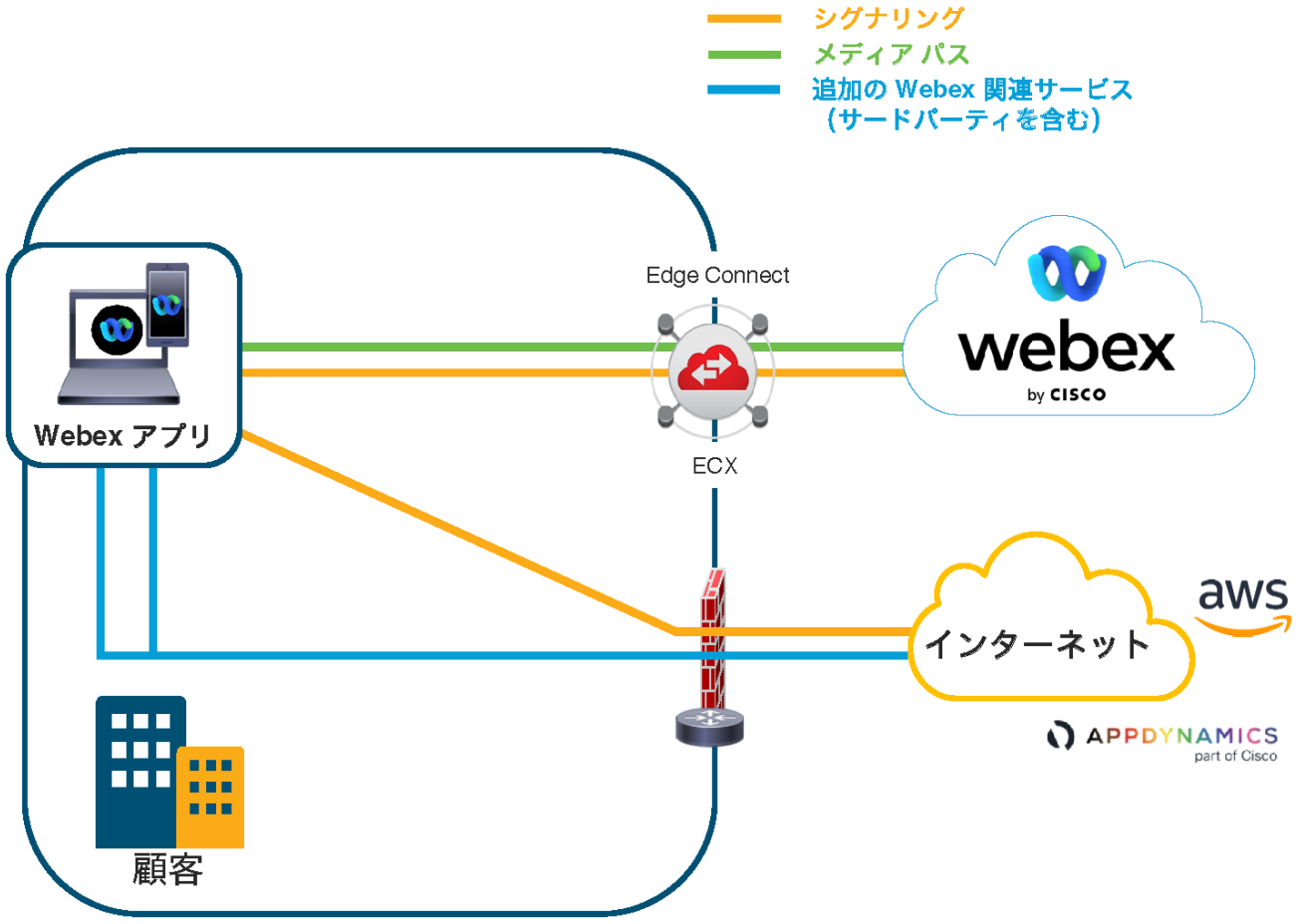
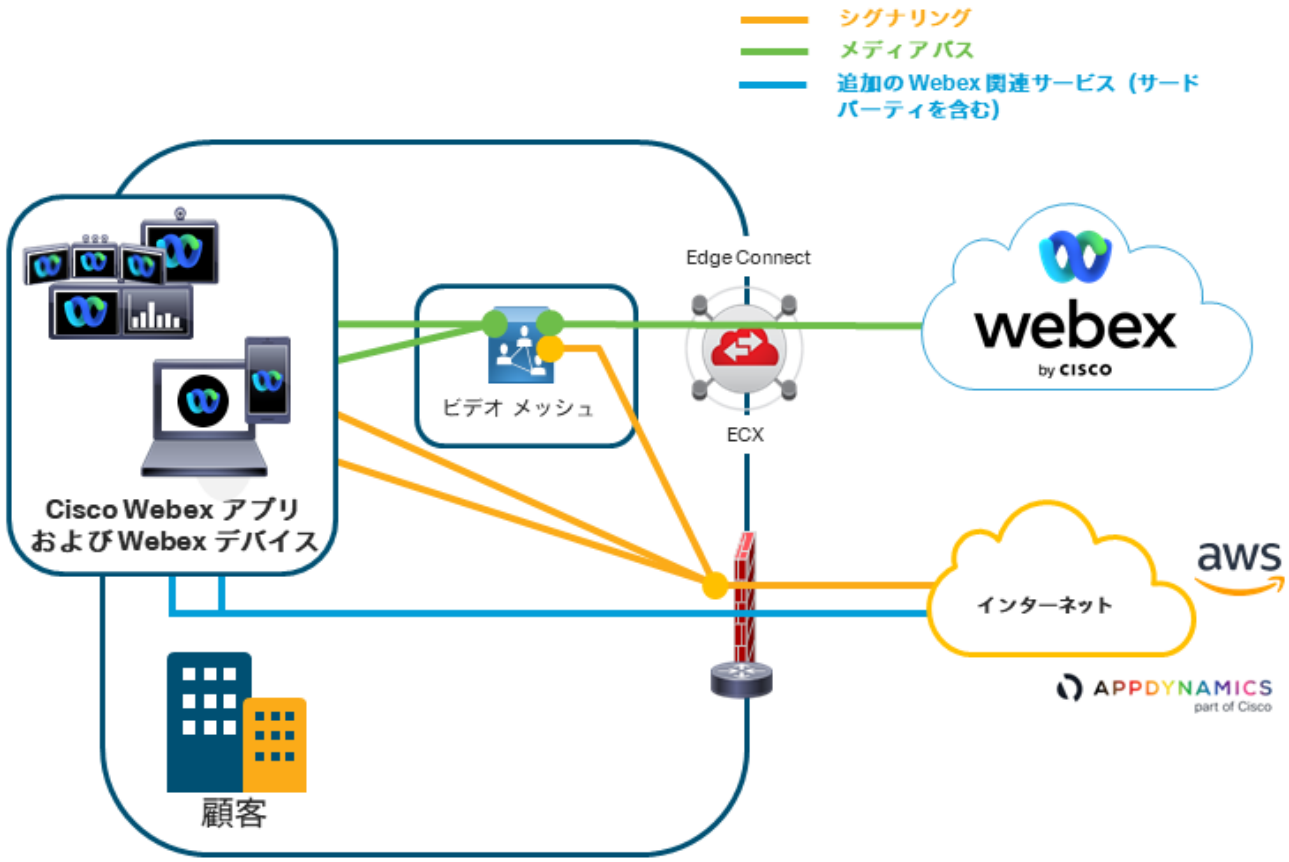


図 15 では、Webex アプリは Edge Connect ピアリング経由でシグナリングとメディアの両方を送信しますが、インターネット経由でコール制御と分析のためのシグナリングも送信します。

ビデオメッシュ利用時の Webex アプリ、Webex Boards、および Webex デバイス

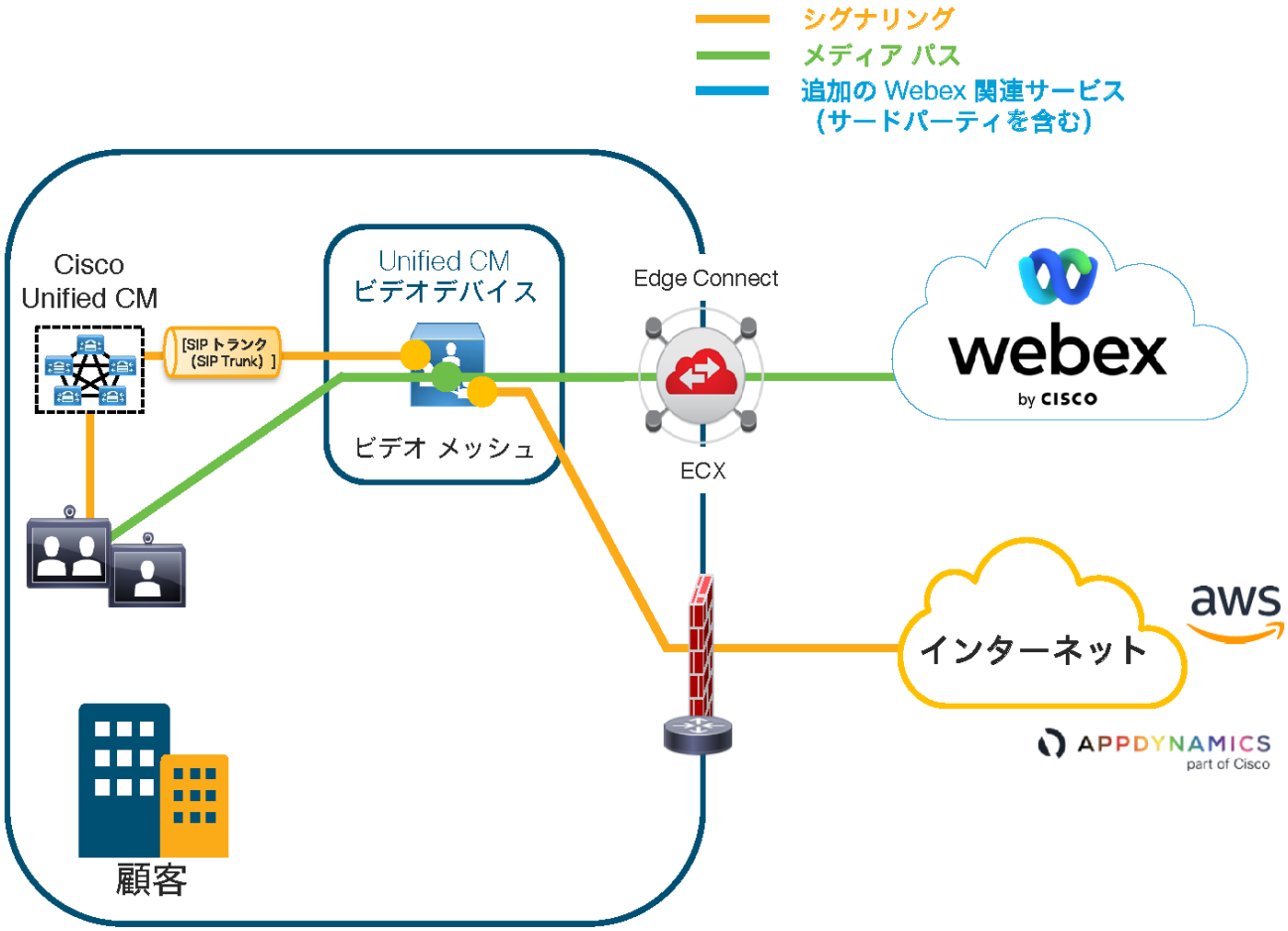
図 16　　ビデオメッシュ利用時の Webex アプリ、Webex Boards、および Webex デバイス



上の図（図 16）Webex アプリ（フル機能の Meetings が無効になっている）では、Webex Board と Webex デバイスは、ローカル ビデオ メッシュ ノードが使用可能なときに、メディアを直接ローカル ビデオ メッシュ ノードに送信します。ビデオメッシュノードは、すべてのカスケードメディアを Edge Connect ピアリング経由で送信し、他の Webex アプリ、Webex Board、および Webex デバイスのシグナリングとともに、コール制御と分析のためのすべてのシグナリングをインターネットに直接送信します。

ビデオメッシュ利用時の Unified CM 登録済みビデオデバイス

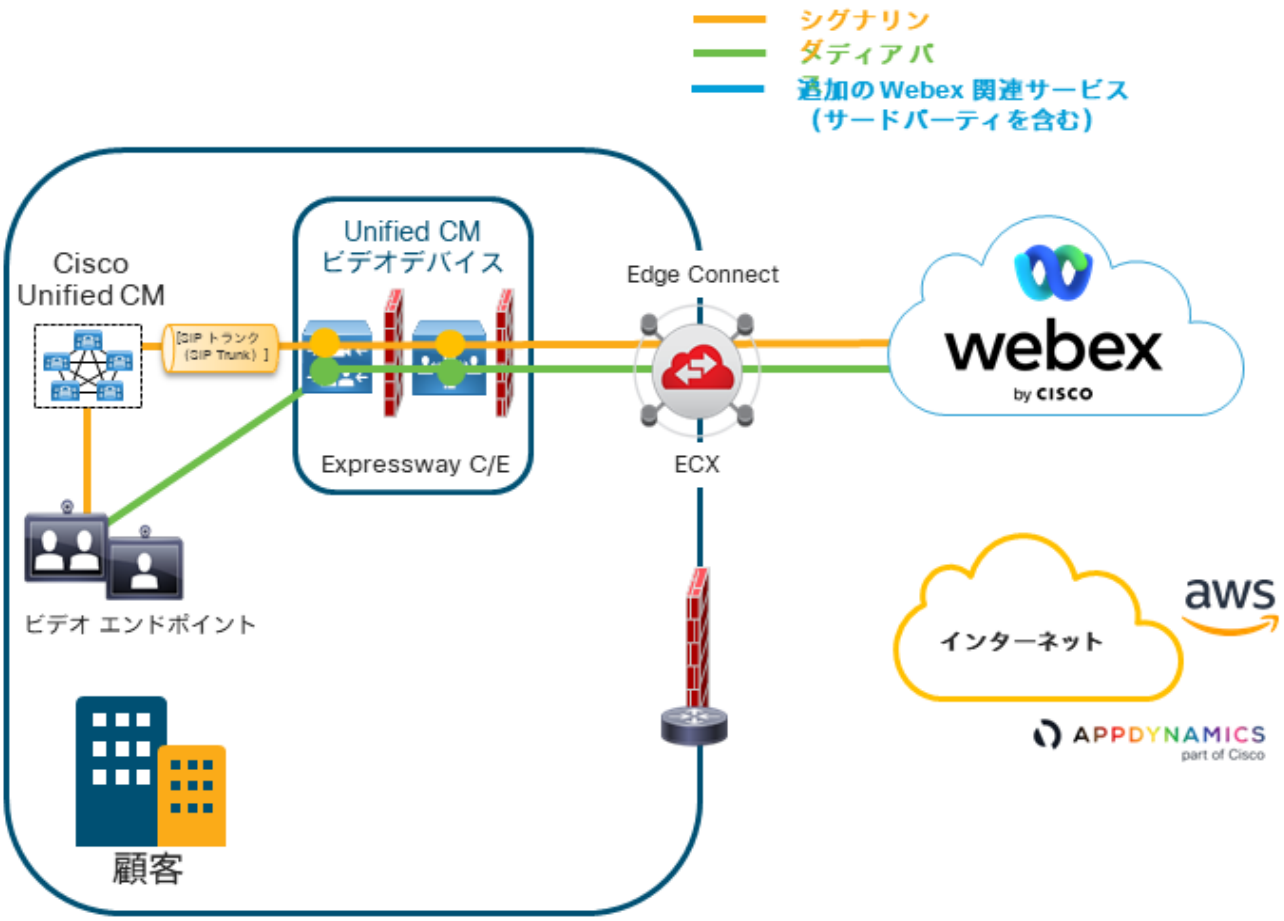
図 17　　Unified CM 登録済みビデオデバイス



上の図（図 17）は、ビデオメッシュ経由で Webex Meetings に接続する Unified CM 登録済みビデオデバイスを示しています。Unified CM は SIP トランクを介してビデオメッシュに信号を送り、ビデオエンドポイントはメディアをビデオメッシュノードに直接送ります。ビデオメッシュノードは、すべてのカスケードメディアを Edge Connect ピアリング経由で送信し、コール制御と分析のためのすべてのシグナリングをインターネットに直接送信します。

Webex Video Meetings と Unified CM の登録済みビデオエンドポイントとの統合

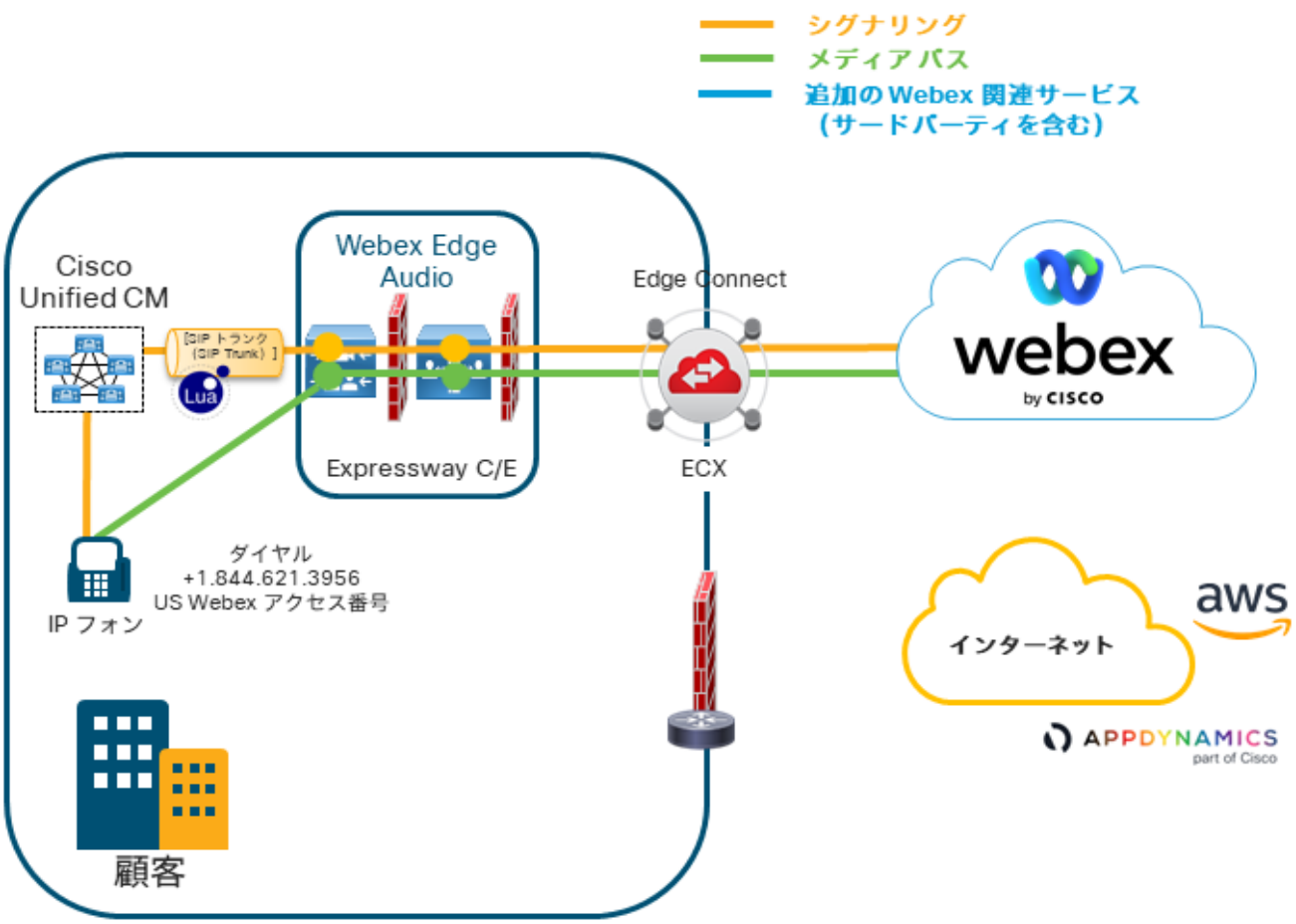
図 18　　Webex ビデオミーティング



上の図（図 18）は、展開された Expressway Edge を介して Webex Meetings に接続する Unified CM 登録済みビデオデバイスを示しています。Expressway 展開時は、すべてのコール制御シグナリングと関連メディアが Edge Connect ピアリングリンクを直接通過します。Unified CM は SIP トランクを介して Expressway-C サーバーに信号を送り、ビデオエンドポイントはメディアを Expressway-C に直接送ります。次に、Expressway-C はすべてのシグナリングとメディアを Expressway-E に直接送信し、Edge Connect を介して Webex DC に送信します。

Unified CM を使用した Webex Edge Audio

図 19　Webex Edge Audio



上の図（図 19）は、Edge Audio ソリューションを介して Webex Meetings に接続する Unified CM の登録済みテレフォニーデバイスを示しています。Edge Audio は、Expressway Edge 展開を使用して Webex Meetings とインターフェイスします。Edge Audio の Expressway 展開では、すべてのコール制御シグナリングと関連するメディアが Edge Connect ピアリングリンクを直接通過します。Edge Audio には着信と発信の両方で複数のタイプのコールフローがありますが、すべてのシグナリングとメディアは Edge Connect ピアリングリンクを介して実行されます。

Webex ハイブリッドサービス

図 20　　ハイブリッドサービス

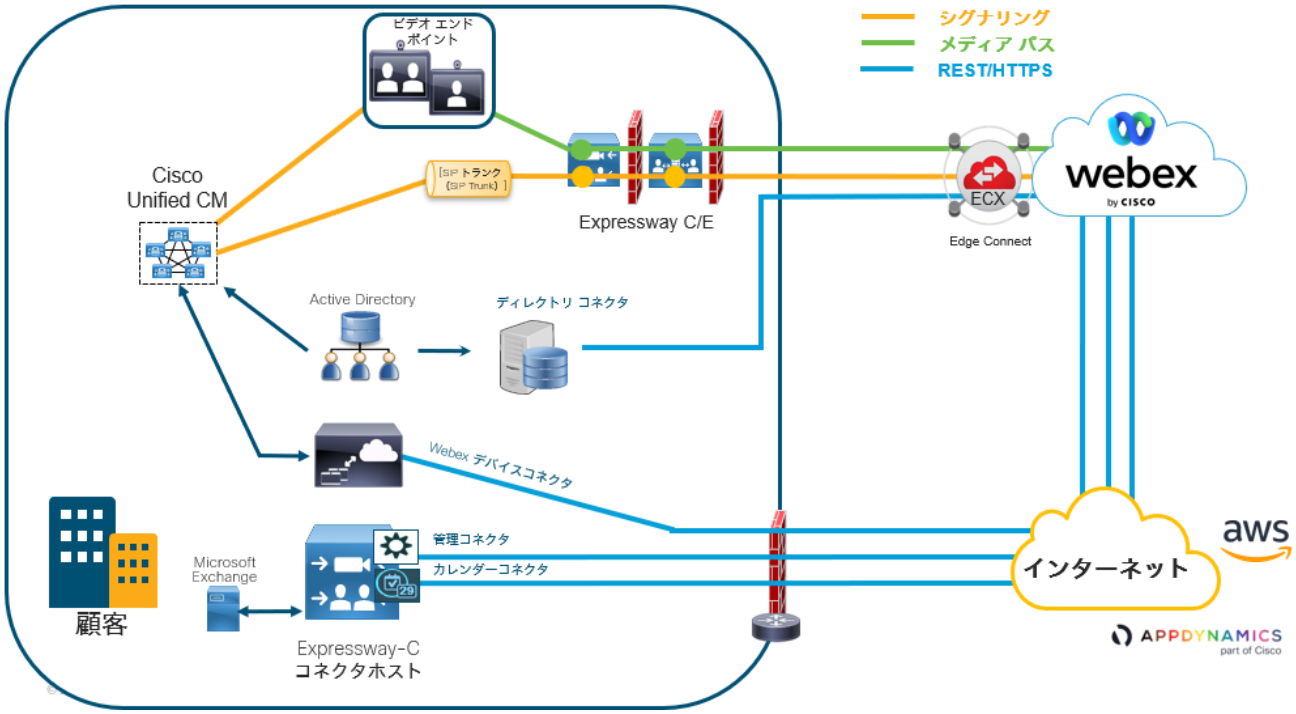


図 20 は、Webex ハイブリッドコネクタ（管理コネクタ、カレンダーコネクタ、ディレクトリコネクタ、およびデバイスコネクタ）がすべてインストールされ、実行されている Webex ハイブリッド サービス ソリューションを示しています。ディレクトリコネクタを除き、これらのコネクタのほとんどはインターネットを使用して Webex Cloud と通信します。ディレクトリコネクタは、Edge Connect パスを使用して Webex Cloud と通信します。ハイブリッドコールフローは、Edge Connect ピアリングリンクを利用して接続された Expressway を介してシグナリングの通信を行います。この Expressway ペアは、Edge Connect を介して Webex クラウドへのシグナリングとメディアを管理し、Webex のコールシグナリングとメディアフローのみを担当します。一方、コネクタはさまざまなロールを持ち、さまざまなデバイス上にあり、対応するサービスノードと個別に通信します。

Webex アプリ、デバイス（Board、Room、Desk）およびビデオメッシュの Webex Edge Connect の設計に関する考慮事項

アマゾンウェブサービス（AWS）は、Webex アプリ、デバイス（Board、Room、Desk）、ビデオメッシュのさまざまなマイクロサービスをホストします。Webex アプリ、デバイス（Board、Room、Desk）およびビデオメッシュの Webex アプリサービスは、シスコが所有する （ID サービス、キー管理サービス、およびメディアサーバー用の Webex データセンターなど）または Amazon AWS プラットフォームの Cisco Virtual Private Cloud（VPC） （Webex App マイクロサービス、メッセージおよびファイルストレージサービスなど）でホストされている、グローバルに分散されたデータセンターでホストされます。すべてのデータは送信中および保管中に暗号化されます。

最近の Webex の拡張中に、 Webex アプリ、デバイス（Board、Room、Desk）、およびビデオメッシュ用のサービスように新しいメディアサービスが Amazon Web Services （AWS） Cisco Virtual Private Cloud （VPC）上に追加されました。

そのため、Webex Edge Connect に関するこの影響を理解することが重要です。Webex Edge Connect は、BGP ピアリング経由で AWS VPC プレフィックスをアドバタイズしません。Edge Connect を介した Webex Meeting トラフィックフローで説明されているように、Webex デバイスとビデオメッシュは、インターネットを使用して、通常の機能の一部として AWS VPC のシグナリング マイクロサービスにアクセスします。メディアサービスは現在 AWS VPC に存在するため、検出プロセスにより、使用する最も近いリソースが決定されます。Edge Connect 上のメディアリソースは、

AWS VPC で利用可能なリソースよりも往復時間（RTT）が短いことが予想されるため、これはほとんどの展開で問題にならない可能性が高いと思われます。つまり、これらのメディアリソースは AWS で利用可能であり、そのパス経由では RTT の方が低い場合、メディアフローはインターネット経由で AWS VPC にルーティングされる可能性があることに注意する必要があります。

このメカニズムがどのように機能するかをよりよく理解するには、Webex アプリ、デバイス（Board、Room、Desk）、およびビデオメッシュの検出プロセスを理解することが重要です。

Webex アプリ、デバイス（Board、Room、Desk）の検出

Webex アプリまたはデバイスが起動すると、Webex コールコントロールに登録されます。次に Webex は、クラウドメディアサービスと、その Webex アプリ/デバイス組織用にプロビジョニングされた ビデオメッシュノード（VMN）クラスタのアドレスリストを返します。次に、Webex アプリ/デバイスはいくつかのテストを実行して、会議中にメディアを送信する先を決定します。

ディスカバリ

Webex アプリとデバイスが実行する最初のテストは、クラウドメディアサービスとビデオ メッシュ ノード クラスタに接続できるかどうかを確認するクラスタ到達可能性テストです。

クライアントまたはデバイスが実行する 2 番目のテストは、エンドポイントとメディアノード（Video Mesh、Webex クラウドおよび Cisco VPC）間のラウンドトリップ遅延時間（RTD）を決定するための STUN テストです。ほとんどの場合、オンプレミスの Webex アプリエンドポイントの場合、Video Mesh クラスタの RTD はクラウドメディアサービスよりも短くなるはずです。Webex クライアントまたはデバイスは、STUN テストの結果を Webex にレポートします。次に、Webex は Webex アプリエンドポイントを割り当て、ラウンドトリップ遅延時間が最も小さいメディアサービスノードにメディアを送信します。クライアントは、クラウドメディアノードよりもネットビデオメッシュノード（VMN）を優先します。ただし、最も近い VMN クラスタが 250 ミリ秒を超え、クラウドノードが 200 ミリ秒以下の場合を除きます。これは、お客様が構成することはできません。

Webex アプリは、以下のいずれかのイベントが発生したときに、バックグラウンドでこれらのテストを実行します。

- Webex アプリとデバイスの起動
- ネットワーク変更イベント
- メディア サービス キャッシュの有効期限

メディアノード検出のキャッシュ有効期限は 2 時間です。展開済みの Video Mesh に 新しいノードが追加されると、Webex アプリエンドポイントがこのイベントを認識するのに最大 2 時間かかる場合があります。Webex アプリエンドポイントを再起動すると、エンドポイントは接続性と STUN テストを再度実行し、新しい Video Mesh ノードを認識します。

設計上の考慮事項

通常、Edge Connect ピアリングの先にある利用可能なメディアリソースに対する遅延が減少するため、 Amazon Web Services（AWS）Cisco Virtual Private Cloud（VPC）IP ブロックを利用しているメディアサービスは使用されない可能性があります。AWS VPC にあるこれらのメディアサービスは、Edge Connect を介したメディアサービスよりも RTT（往復時間）が大きくなります。とは言え、Webex アプリまたは Webex デバイスがネットワーク内のどこに配置されているか、およびダイレクト インターネット アクセス（DIA）ポイントと Edge Connect ポイントの間の遅延に応じて、Edge Connect を介した接続先リソースよりもこれらのリソースを選択する可能性があります。いくつかの理由により、インターネット上でこれらの IP セグメントをブロックすることはお勧めしません。1 つは、インターネットセグメントが通常 Edge Connect のバックアップとして使用されることです。これをブロックすると、インターネットへの接続に失敗し、低遅延で接続できる可能性のあるサービスへのアクセスをブロックします。もう 1 つの理由は、すべての Webex コンポーネントが AWS VPC メディアサービスを使用するための同じ検出メカニズムと到達可能性メカニズムを備えているわけではないため、IP セグメントをブロックすると、会議が失敗する可能性があることです。そのため、Webex コンポーネントの検出および到達可能性メカニズムによって、ネットワーク内の場所に基づいて利用可能な最も低遅延のリソースを決定できるようにすることをお勧めします。

DNS に関する考慮事項

Webex リソースが顧客のメールサービスのドメイン名でルックアップを行うシナリオがあります。たとえば、MX レコードルックアップで、Webex のスケジュールされた会議リクエストを配信するためのメールサーバーを決定します。このような状況では、Webex DC の Webex マイクロサービスがルックアップを実行し、企業組織の外部 DNS サーバーのアドレスを取得します。DNS サーバーが Webex Edge Connect プレフィックスを含むネットワークセグメントによっても提供されている場合、これにより DNS クエリ応答の非対称ルーティングが発生し、ファイアウォールによってブロックされる可能性があります。

図 21　　非対称 DNS クエリ/応答の例

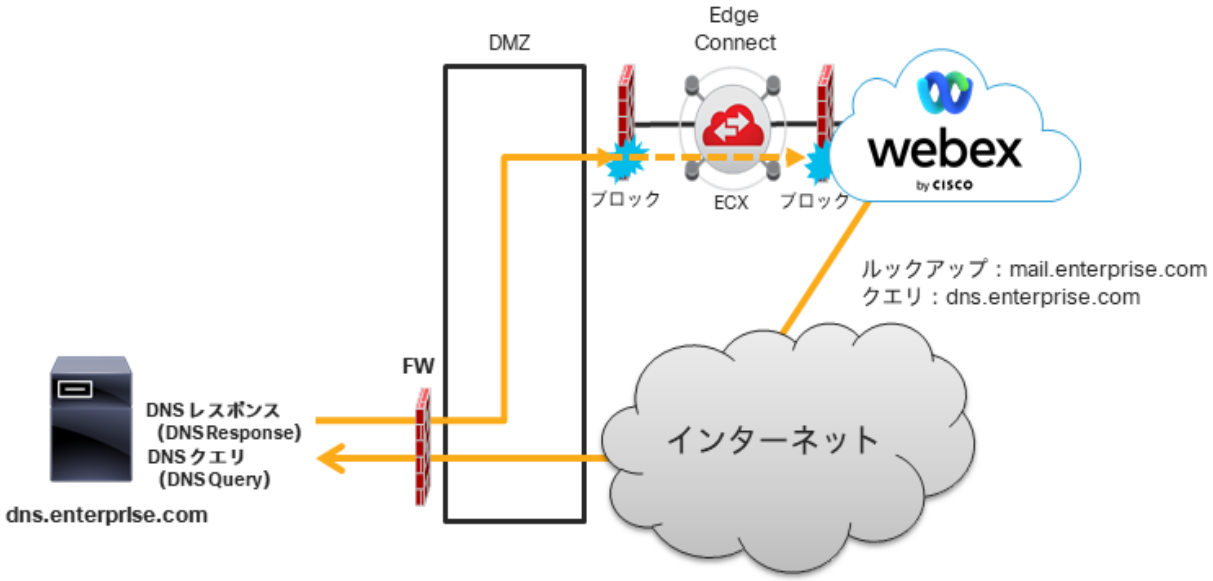


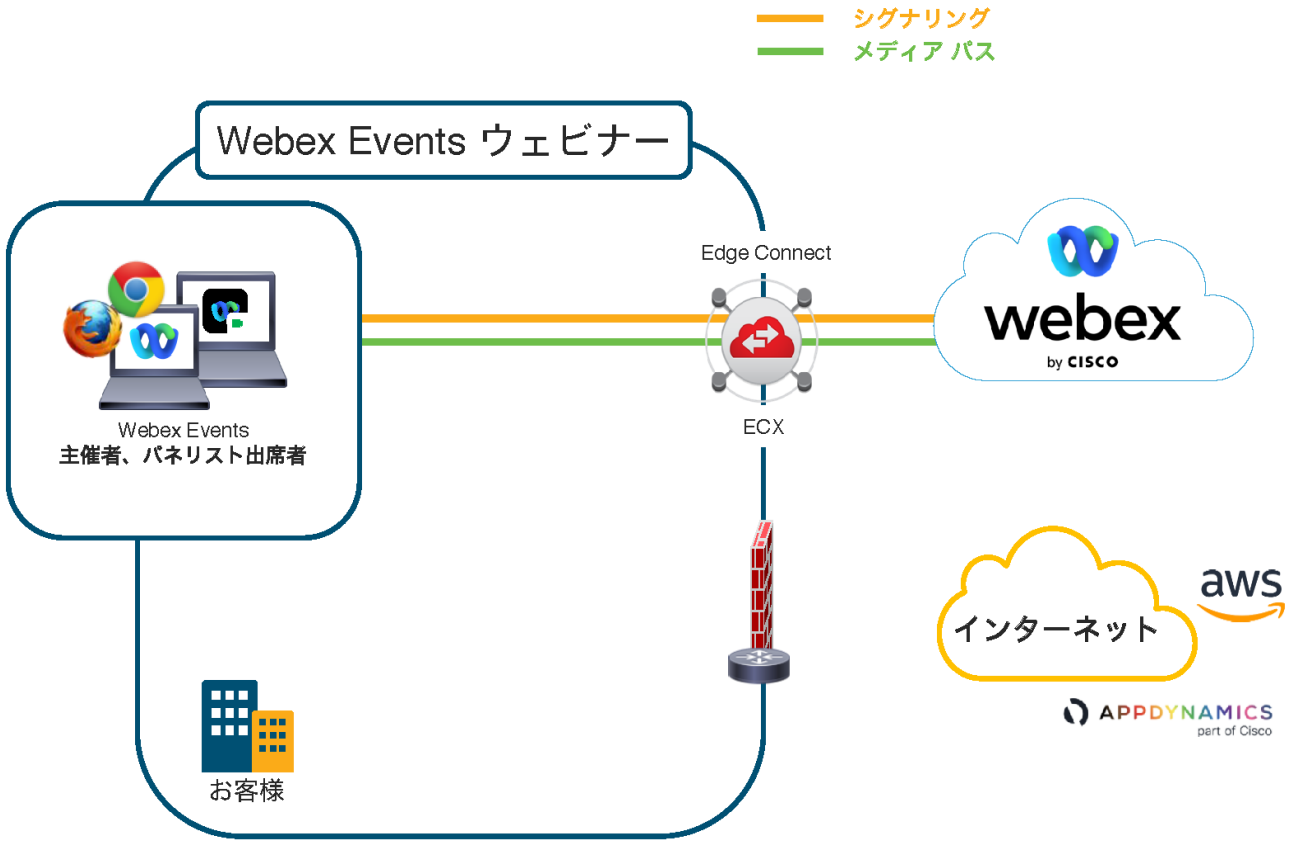
図 21 は、インターネットと Edge Connect が同じネットワークセグメント（DMZ）からサービスが提供される設計を示しています。コンポーネント サーバーの場合、この場合、Webex のメール配信エージェントは mail.enterprise.com の Mx レコードでルックアップを実行し、企業 DNS サーバーに対して DNS クエリを実行します。DNS サーバーは Edge Connect ではなくインターネットからのみアドバタイズされるため、このクエリは、インターネット経由で企業に送信されます。ただし、この場合、インターネットにサービスを提供するネットワークセグメントに応答が返されると、Edge Connect を介してアドバタイズされたルートからのパスと一致するため、DNS クエリの送信元 IP アドレスへのパスがあります。そのため、DNS 応答は Edge Connect を介してルーティングされ、非対称ルーティングのためにファイアウォールによってブロックされます。

このタイプの設計の推奨事項は、Webex サービスとの通信で使用される DNS サーバーまたは公開ネットワークコンポーネントが Edge Connect を介してアドバタイズされるようにすることです。これにより、障害シナリオ時に Edge Connect およびインターネットを介した対称ルーティングが可能になります。

Edge Connect を介した Webex Events トラフィックフロー

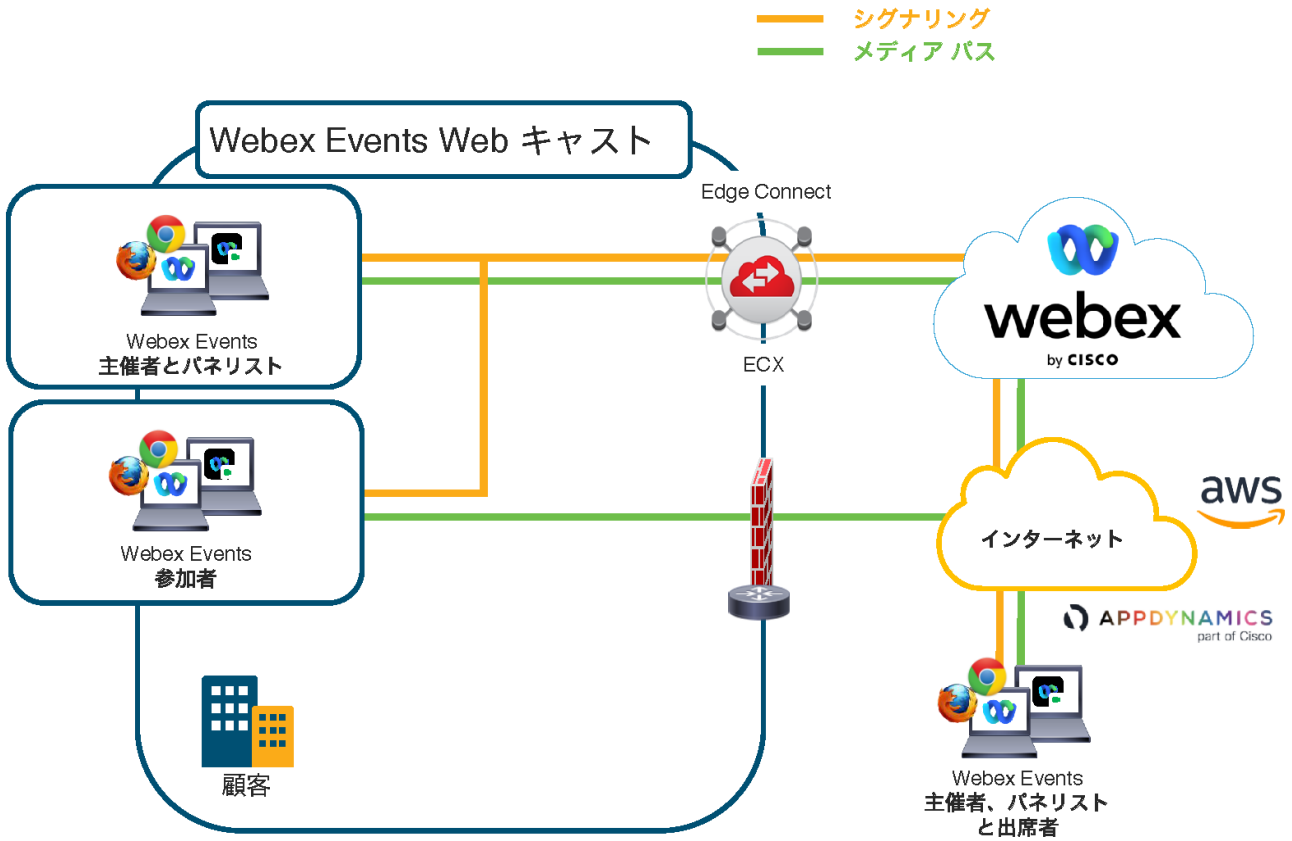
Webex Events サービスにより、主催者は仮想イベントやウェビナーを開催できます。主催者は、Webex Events でウェビナーモードと Web キャストモードのいずれかを選択できます。

図 22　　Webex Events ウェビナー



Webex Events ウェビナー機能では、主催者、共同主催者、パネリスト、出席者が Edge Connect を介してメディアとシグナリングを送信します。図 22 にこの機能を示します。

図 23　　Webex Events ウェブキャスト



Webex Events の Web キャスト機能では、主催者、共同主催者、およびパネリストは Edge Connect を介してメディアとシグナリングを送信しますが、出席者は Edge Connect を介してシグナリングを送信しメディアはインターネット経由で送信します。図 23 にこの機能を示します。

Edge Connect を介した Webex Calling トラフィックフロー

Webex Calling は 2 つのカテゴリにグループ化できるいくつかの異なるエンドポイントとクライアントを利用します。ローカルゲートウェイ、 Calling エンドポイントおよびクライアントです。以下は、Webex ソリューション コンポーネントとそれらに関連付けられたトラフィックフローをまとめたものです。Webex Edge Connect が展開されている場合に、シグナリング及びメディアが Edge Connect パスまたはインターネットパスの関連付けられた出口を通過するフローを示しています。

Webex Edge Connect では、次の Webex Calling サービスがサポートされています。

1. ローカルゲートウェイ：
    a. Cisco Unified Border Element（CUBE）
2. Calling エンドポイントおよびクライアント：
    a. マルチプラットフォームフォン（MPP）
    b. ビデオ対応電話機（8845、8865）
    c. 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の両方）
    d. Webex Calling アプリケーション（デスクトップとモバイルの両方）

図 24　Webex Calling エンドポイントとローカル ゲートウェイ シグナリングとメディアフロー

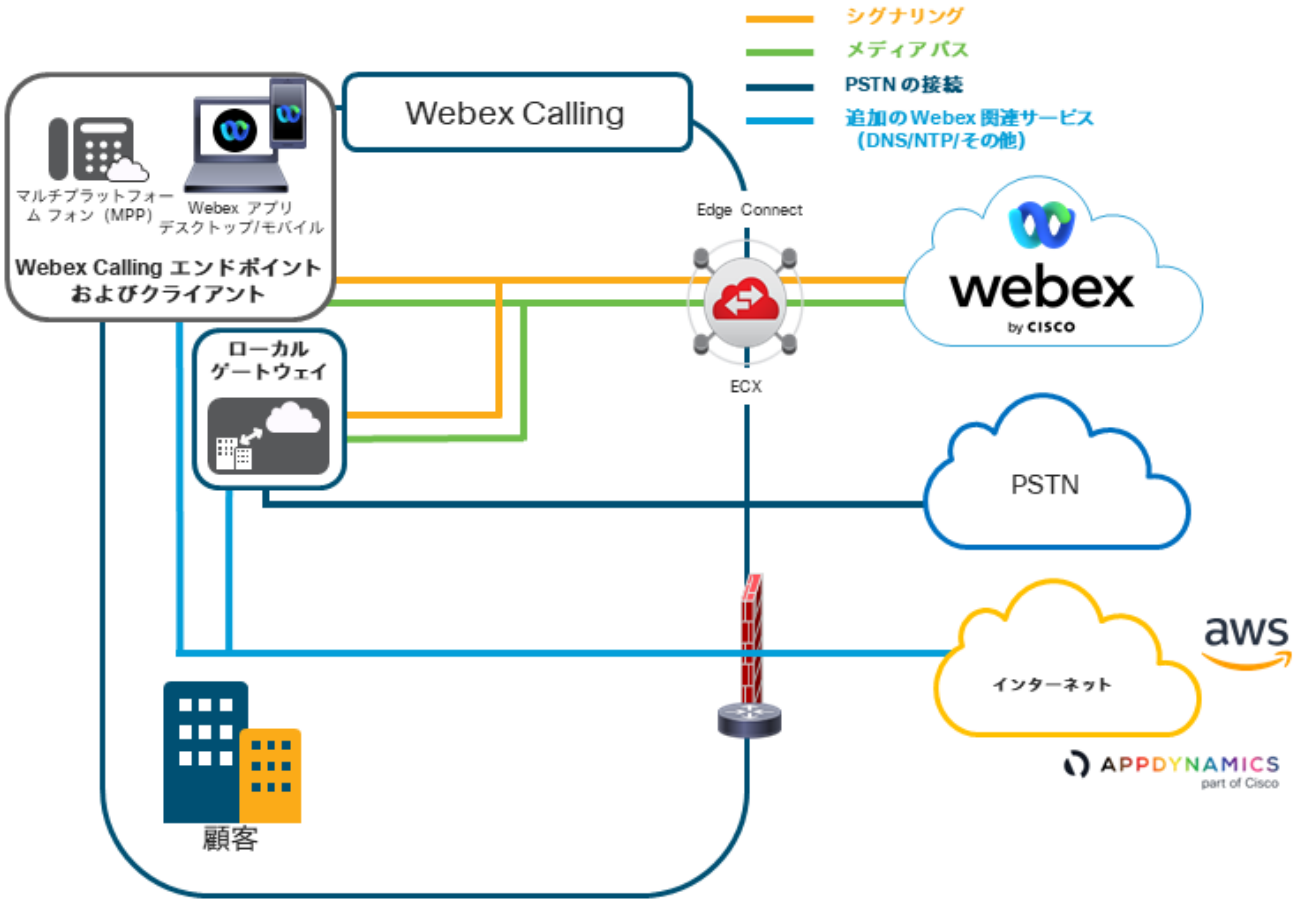


図 24 は、マルチプラットフォームフォン（MPP）や Webex アプリなどの Webex Calling エンドポイントとクライアント、および Edge Connect リンクを介してコール制御シグナリングとメディアを送信するローカルゲートウェイを示しています。この場合の Webex アプリは、Webex Calling のシグナリングとメディアのみを参照しています。Webex Meetings の Webex シグナリングとメディアについては、Webex Meetings トラフィックフローで説明します。ローカルゲートウェイには、Unified CM クラスタへの接続、または SIP 経由の PSTN または PSTN プロバイダーへの接続など、企業内に他の接続がある場合があります。最後に、Webex Calling エンドポイント、クライアント、およびローカルゲートウェイから作成されたいくつかの接続があり、Webex サービス、DNS または NTP など、他の Webex サービスまたはインフラストラクチャ サービスにインターネット接続が必要になる場合があります。

高可用性と冗長性

高可用性と冗長性は、いくつかの方法で実現できます。このセクションでは、ローカル冗長性、サイト冗長性（リモート冗長性）、およびフェイルオーバーとしてのインターネットについて説明します。トラフィック エンジニアリングは企業によって管理およびサポートされていることに注意してください。次の例は、Edge Connect 展開時の BGP ルーティングの機能を理解するためにの可能性のある展開モデルのサンプルです。

ローカル冗長性

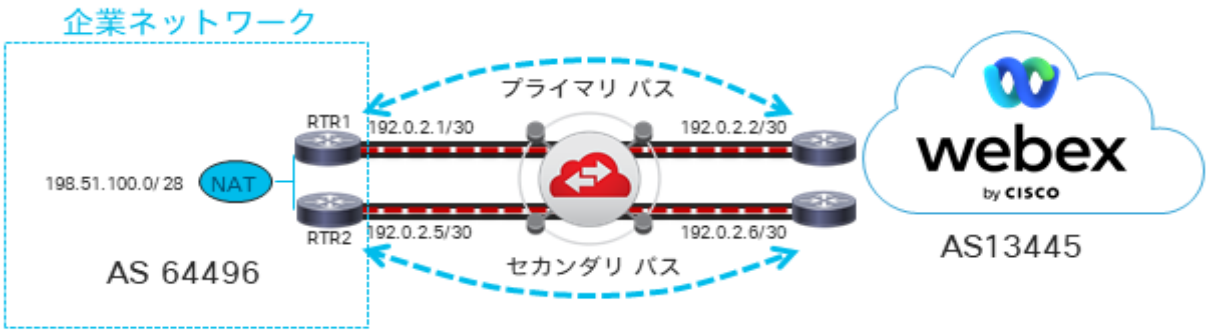
ローカル冗長性は、Edge Connect ピアリングのローカル冗長性（同じサイト）で構成されます。これは、アクティブ / パッシブまたはアクティブ / アクティブピアリング回路など、いくつかの方法で実現できます。それぞれの利点については、各サブセクションで説明します。

注： Webex Edge Connect は、複数のレイヤー 2 ポートを介した単一ピアリングリンクをサポートしていません。そのため、このオファーでは、単一の BGP ピアリングでレイヤー 2 冗長性モデルを展開することはできません。各ピアリング（接続）にはそれぞれポートが必要です。

BGP パス冗長性

BGP パスの冗長性では、アクティブ / アクティブまたはアクティブ / パッシブルーティング構成の同じ場所に 2 つの個別の BGP ピアリングがあります。推奨事項は、アクティブリンクとパッシブリンクの帯域幅量が等しいアクティブ / パッシブルーティング構成を設定することです。各リンクは、ピーク時間にサービスをサポートするようにプロビジョニングする必要があります。詳細については、帯域幅のプロビジョニング（帯域幅のプロビジョニング）のセクションを参照してください。

図 25 BGP パス冗長性



BGP パス冗長を設定するには複数の方法があります。BGP トラフィック エンジニアリングを構成および管理するのは最終的には顧客次第ですが、Webex は、最高レベルの制御とルーティングの実現ために、BGP コミュニティ属性とローカルプリファレンスのタグ付けをサポートしています。Webex では、顧客がトラフィック エンジニアリングに影響を与えるために使用できるいくつかの BGP コミュニティ属性を提供します。

注： AS-PATH プリペンドは、自律システム番号（ASN）を繰り返して AS-PATH 属性の長さを人為的に増やすことにより、ルートの優先順位を下げるために使用される手法です。他のすべての基準が等しいと仮定すると、BGP でのルート選択では、短い AS パス長が優先されます。これは、BGP ルーティングとパス選択に影響を与えるために使用される別のトラフィック エンジニアリング ツールです。AS-PATH プリペンドは、顧客がパブリック ASN を利用してピアリングした Edge Connect でのみサポートされています。プライベート ASN の場合は、ASN は Webex ネットワークに入るときに除去されるため、AS-PATH プリペンドをサポートできません。

BGP コミュニティ

次の BGP コミュニティは、Webex インバウンドルートポリシーによって受け付けられ、Edge Connect リンクの優先度に影響を与えるために顧客によって使用される場合があります。

リンク優先コミュニティ

- なし：デフォルト（最も望ましくないパスおよび/またはホットポテト）
- 13445:200：ローカルプリファレンス 200
- 13445:300：ローカルプリファレンス 300
- 13445:400：ローカルプリファレンス 400
- 13445:500：ローカルプリファレンス 500
- 13445:600：ローカルプリファレンス 600

- 13445:700：ローカルプリファレンス 700
- 13445:800：ローカルプリファレンス 800
- 13445:900：ローカルプリファレンス 900（最も望ましいパス）

ルート伝達スコーピングコミュニティ

Webex とグローバルピアリング契約を結んでいる顧客は、Webex クラウド内のルートアドバタイズメントをローカル ジオグラフィック シアターに制限したい場合があります。次のコミュニティは、Webex ネットワーク全体での顧客ルートの伝達を制限するために使用できます。

- なし：デフォルトの許可グローバル到達可能性
- 13445:677：ローカルシアターの到達可能性を許可

Webex ルートオリジンコミュニティ

Webex は、BGP コミュニティタグを適用して、Webex プレフィックスの発信元を示します。これは、ロケーションタグに基づいてルートのフィルタ処理を実行する場合に役立ちます。次の BGP コミュニティは、地理的シアターによってグループ化された Webex プレフィックスの発信元を示しています。地理的シアターに基づいてのみフィルタ処理することを推奨します。

Webex Meetings コミュニティ（シアター別）

- 13445:10000：AMER
- 13445:10010：EMEA
- 13445:10020：APAC

Webex Calling コミュニティ（シアター別）

- 13445:20000：AMER
- 13445:20010：EMEA
- 13445:20020：ANZ
- 13445:20060：APAC

Webex ルートオリジンコミュニティの例

以下に、プレフィックスのシアターグループまたは Webex ソリューション（つまり、Webex Meetings または Webex Calling）でフィルタ処理する BGP コミュニティストリングを使用した基本的なルータ設定の 2 つの例です。

図 26 は、Webex Calling プレフィックスのみがルーティングテーブルに受け入れられるため、Webex Meetings プレフィックスがフィルタ処理で除去される設計を示しています。

図 26　　コミュニティストリングによる Webex Calling プレフィックスのフィルタ処理

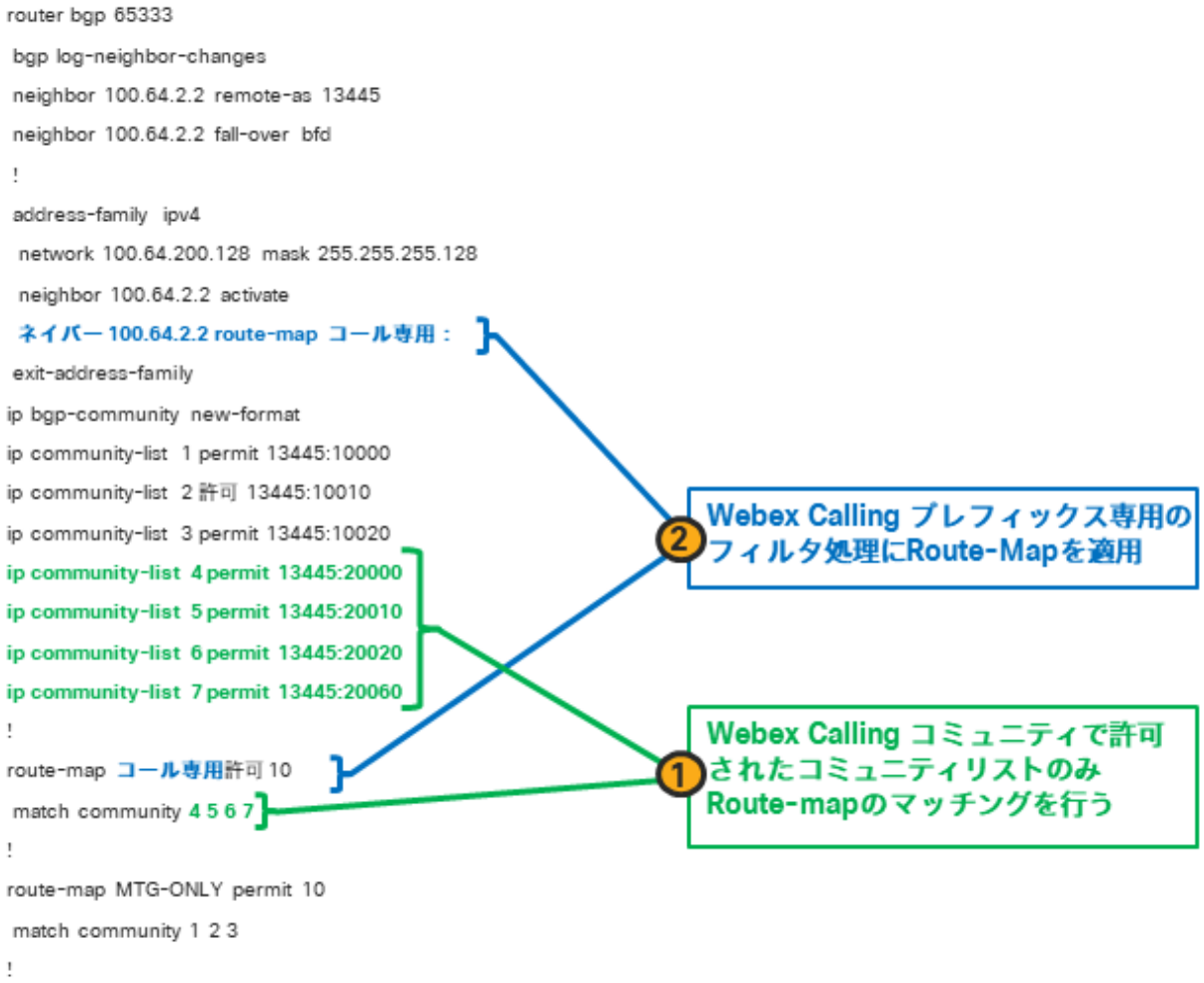


図 26 では、ソリューションとシアターごとに 1 つずつ、7 つのコミュニティストリングが作成されています。コミュニティリスト 1 ~ 3 は Webex Meetings の 3 つのシアターをカバーし、コミュニティリスト 4 ~ 7 は Webex Calling の 4 つのシアターをカバーします。この構成では、CALL-ONLY という名前のルートマップが作成され、Webex Calling のすべてのシアターであるコミュニティリスト 4 ~ 7 を許可します（図 26：ステップ 1）。次に、この route-map がネイバーに適用されるため、BGP ルーティングテーブルへのコミュニティ 4 ~ 7 のみが許可されます（図 26：手順 2）。

図 27 は、Webex Meetings プレフィックスのみがルーティングテーブルに受け入れられるため、Webex Calling プレフィックスがフィルタ処理で除去される設計を示しています。

図 27　　コミュニティストリングによる Webex Meetings プレフィックスのフィルタ処理

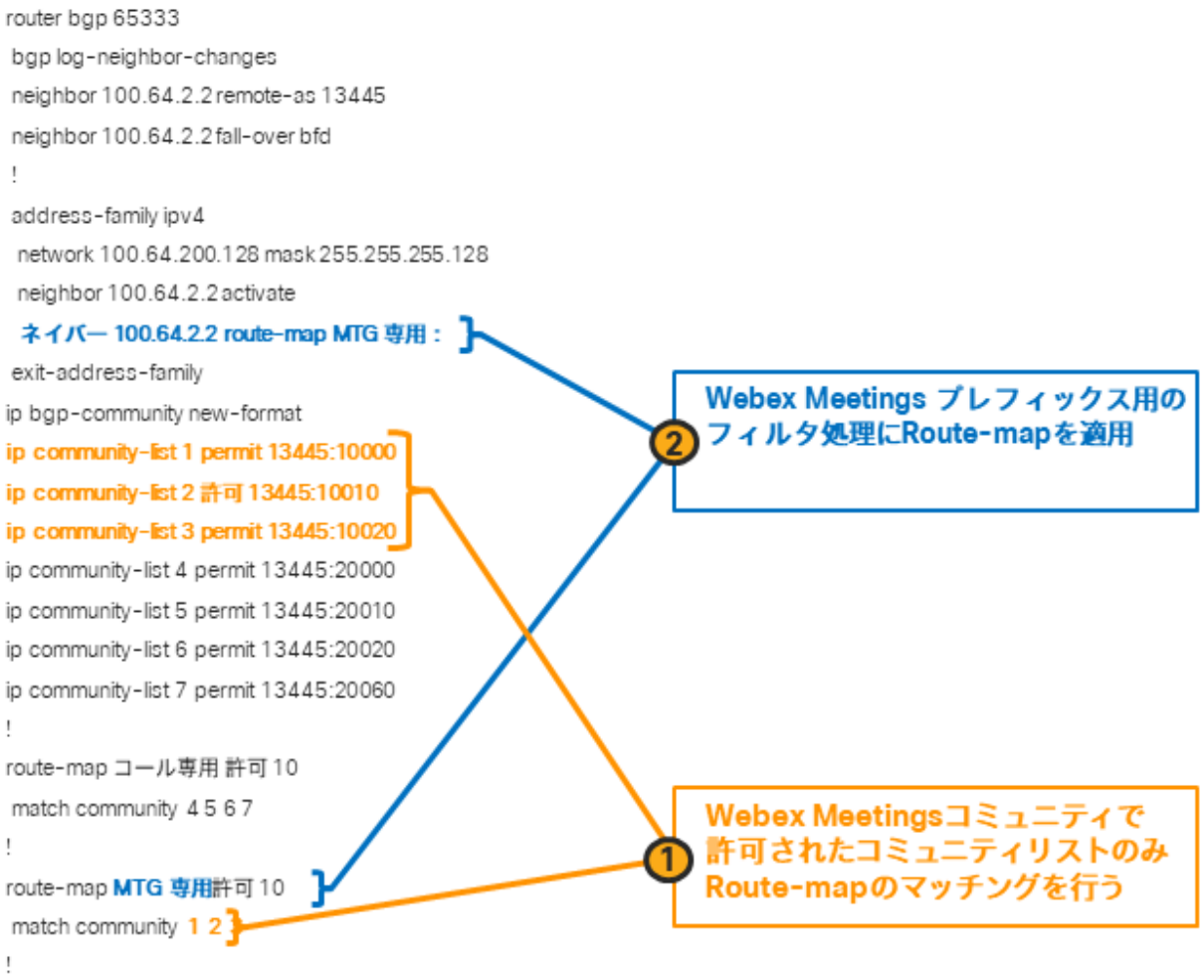


図 27 では、ソリューションとシアターごとに 1 つずつ、同じ 7 つのコミュニティ ストリングがあります。コミュニティリスト 1 ~ 3 は Webex Meetings の 3 つのシアターをカバーし、コミュニティリスト 4 ~ 7 は Webex Calling の 4 つのシアターをカバーします。この構成では、MTG-ONLY という名前のルートマップが作成され、Webex Meetings のすべてのシアターであるコミュニティリスト 1 ~ 3 を許可します（図 27：ステップ 1）。次に、この route-map がネイバーに適用されるため、BGP ルーティングテーブルへのコミュニティ 4 ~ 7 のみが許可されます（図 27 ：ステップ 2）。

注：　顧客は、すべての Webex ルートを受け入れるか、コミュニティストリングを使用して、ソリューション（Webex Calling または Webex Meetings）および/またはシアター（AMER、EMEA など）によってルートをフィルタ処理し、プレフィックスリストまたはルートポリシーのハードコーディングを避けることをお勧めします。トラフィックが分岐、または非対称ルーティングの問題につながる可能性があるため、CIDR ブロックに基づくフィルタ処理は推奨されません。コミュニティストリングに基づくフィルタ処理により、設計と構成が簡素化されます。

アクティブ / パッシブローカル冗長性

アクティブ / パッシブローカル冗長性では、それぞれ別個のピアリングがある 2 つの接続がインストールされ、同じ NAT プールをアドバタイズし、同じ Webex ルートプレフィックスを受信します。この例では、各 BGP ピアリングが個別のルータ上にあり、ルータの冗長性をさらに高めています。この例では、BGP コミュニティとローカルプリファレンスを使用して、1 つのピアリングリンクがアクティブであることを確認し、2 つ目のピアリングリンクは、最初のパスに障害が発生した場合にのみトラフィックに使用されます。この例は、図 28 に示されているアクティブ / パッシブのパス選択を確実にするために、BGP コミュニティのローカルプリファレンスを使用して同じ場所にある Webex への 2 つの Edge Connect 回路がある企業ネットワークを示しています。

図 28　　アクティブ / パッシブローカル冗長性：BGP コミュニティのローカルプリファレンス

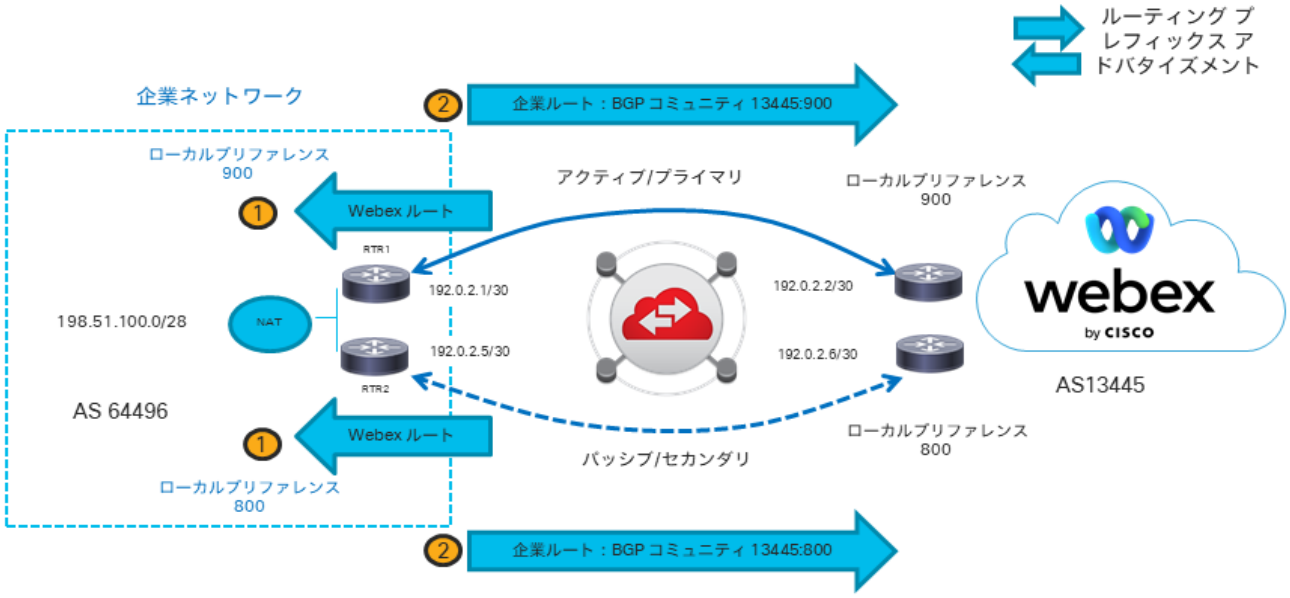


図 28 では、RTR1 はアクティブなプライマリリンクであり、RTR2 はパッシブなセカンダリリンクです。この場合、BGP ローカルプリファレンスを使用して、RTR1 経由を最も望ましいパスだと示します。これは両方向で必要です。ローカルプリファレンスは、ピアの Webex ルータから RTR1 および RTR2 で受信したインバウンドルートに設定され、アウトバウンドルーティング動作（企業から Webex へのトラフィックのルーティング動作）に影響を与えます。その後、BGP リンク プライオリティ コミュニティを使用して、顧客ネットワークに戻る企業ルートのローカル設定を Webex に示すことができます。

注：　Edge Connect ライセンスを購入すると、冗長オプションを利用できます。この冗長性オプションにより、Edge Connect ライセンスを購入するときに、セカンダリ接続のコストを節約できます。したがって、たとえば 1GB 接続購入時に冗長オプションを選択すると、アクティブ / パッシブローカル冗長モデルで 2 つの 1GB 接続が可能になります。この冗長性ライセンスオプションは、アクティブ / パッシブローカル冗長性でのみ使用でき、アクティブ / アクティブローカル冗長性モデルやアクティブ / アクティブな地理的に分散した Edge Connect 回路またはアクティブ / パッシブな地理的に分散した Edge Connect 回路などのサイト冗長性モデルでは使用できません。

企業から Webex ネットワークへのパスの選択：

RTR1 は、Webex BGP ピアリングから受信したルート（プレフィックス）にインバウンドポリシーを適用して、900 のローカルプリファレンスを設定し、RTR2 は 800 のローカルプリファレンスを Webex プレフィックスに適用します。これを図 28 - 1 に示します。その結果、企業ネットワークから Webex クラウドプレフィックスに到達するための最適なパスは、最高のローカルプリファレンスが割り当てられているため、RTR1 です。

Webex から企業ネットワークパスの選択：

RTR1 は、BGP コミュニティ 13445:900 を設定するアウトバウンドポリシーを適用し、RTR2 は、コミュニティ 13445:800 を Webex にアドバタイズされた企業プレフィックス 198.51.100.0/28 に適用します。これを図 28 - 2 に示します。その結果、Webex クラウドは、最も望ましいリンク プライオリティ コミュニティ（900）をアドバタイズしているため、RTR1 パスを選択します。

RTR1 と RTR2 の次の構成は、ローカルプリファレンスを設定するために BGP コミュニティを使用した上記のネットワークパス選択の構成例です。青で強調表示されたルートマップは、コミュニティおよびローカルプリファレンスの設定に使用される構成を示しています。

RTR1 BGP 構成の例

```
router bgp 64496
 neighbor 192.0.2.2 remote-as 13445
!
 address-family ipv4
  neighbor 192.0.2.2 activate
  neighbor 192.0.2.2 send-community both
  neighbor 192.0.2.2 route-map PRIMARY-OUTout
  neighbor 192.0.2.2 route-map PRIMARY-IN in
exit-address-family
!
ip prefix-list ADVERTISE-TO-WEBEX seq 5 permit 198.51.100.0/28
!
route-map PRIMARY-OUT permit 10
 match ip address prefix-list ADVERTISE-TO-WEBEX
 set community 13445:900
!
route-map PRIMARY-IN permit 10
 set local-preference 900
```

RTR2 BGP 構成の例

```
router bgp 64496
neighbor 192.0.2.6 remote-as 13445
 !
 address-family ipv4
  neighbor 192.0.2.6 activate
  neighbor 192.0.2.6 send-community both
  ネイバー 192.0.2.6 ルートマップ SECONDARY-OUT アウト
  ネイバー 192.0.2.6 ルートマップ SECONDARY-IN イン
exit-address-family
!
ip prefix-list ADVERTISE-TO-WEBEX seq 5 permit 198.51.100.0/28
!
route-map SECONDARY-OUT permit 10
 match ip address prefix-list ADVERTISE-TO-WEBEX
 set community 13445:800
!
route-map SECONDARY-IN permit 10
 set local-preference 800
```

アクティブ/アクティブローカル冗長性

アクティブ / アクティブローカル冗長性では、別個のルータ上の別個のピアリングを備えた 2 つのリンクが、同じ NAT プールをアドバタイズし、同じ Webex ルートプレフィックスを受信します。この例では、ルータプラットフォーム自体の冗長性をさらに高めるために、各 BGP ピアリングが個別のルータ上にあります。BGP 構成では、両方のピアリングリンクがトラフィックに対してアクティブであることを確認するために特別なことは必要ありません。この例は、図 29 に示されているアクティブ / アクティブリンクとて同じ場所にある Webex への別個のルータに 2 つの Edge Connect 回路を備えた企業ネットワークを示しています。

図 29　　アクティブ / アクティブローカル冗長性

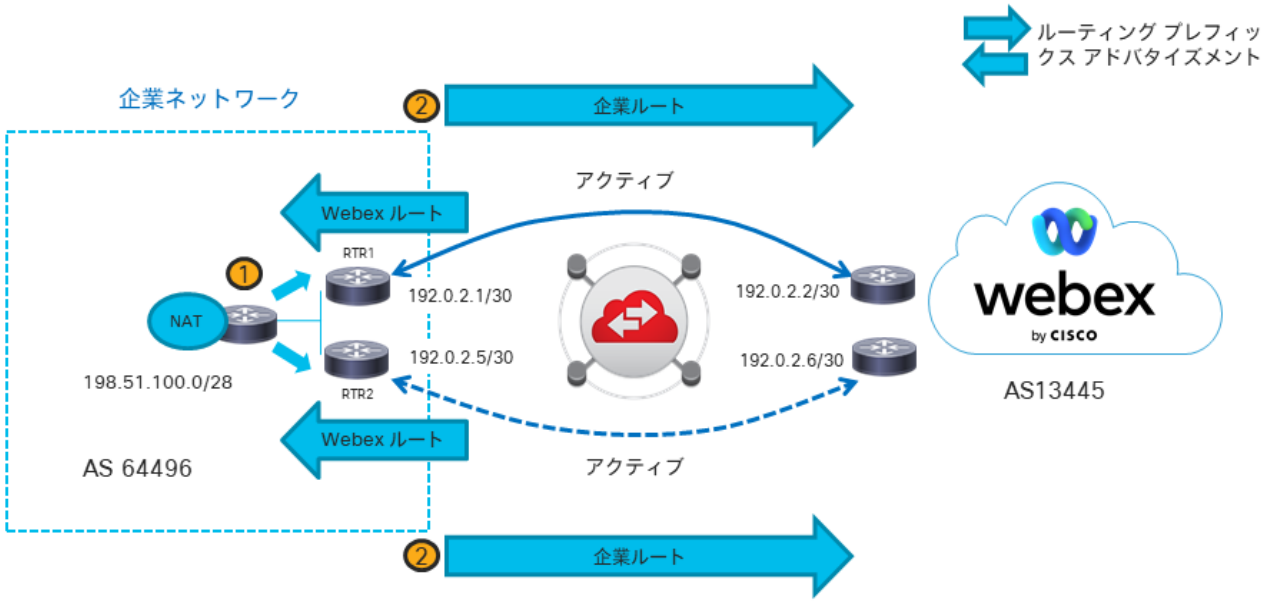


図 29 では、RTR1 と RTR2 は両方とも、いずれかの方向から受信するトラフィックのルーティングでアクティブです。この場合、この例の BGP 構成で特別なことは要求されません。トラフィックを受信するルータは、パスを介して受信するすべてのトラフィックを転送します。ただし、企業ルータは、RTR1 および RTR2 の前で負荷分散する必要があります。内部ルーティングプロトコル側の別のルータは、RTR1 と RTR2 へのトラフィックを負荷分散するために必要であり、ローカル ルーティング プロトコルにアドバタイズされる Webex サブネットの RTR1 と RTR2 の等コストネクストホップパスを確保する必要があります。これを図 29 - 1 に示します。図 29 - 2 では、プライベート IP からパブリック IP への NAT に使用される企業ルート 198.51.100.0/28 のアドバタイズは、特定のリンクの優先順位なしで Webex Cloud にアドバタイズされます。

注：　Webex Cloud への両方のピアリングリンクに単一のルータが使用されている場合、BGP マルチパスは、2 つの個別のピアリングリンクを負荷分散するために必要な構成です。技術的には実現可能ですが、ルータが 2 つのリンクの単一障害点になり、単一の場所における複数のピアリングリンクの価値を低下させるため、これは推奨されません。

サイトの冗長性（リモート冗長性：地理的に分散）

サイト冗長性とは、各 Edge Connect 回路が地理的に離れたサイトにあるプライマリパスとセカンダリパスを指します。これは、各 Edge Connect サイトが相互に離れた場所にありながら、リンクまたはサイトに障害が発生した場合に備えて相互にバックアップする場合です。次の 2 つの例は、アクティブ / アクティブおよびアクティブ / パッシブサイトの冗長性を示しています。

アクティブ / アクティブ地理的に分散した Edge Connect 回路

このセットアップでは、East と West の 2 つのサイトが Edge Connect 回路をホストしています。West ネットワーク ドメイン ユーザーの場合、West Edge Connect 回路はプライマリで、East Edge Connect 回路はセカンダリです。East ネットワーク ドメイン ユーザーの場合、East はプライマリで、West はセカンダリです。これを図 30 と図 31 に示します。前述のように、2 つの回路が地理的に離れているため、2 つの個別の NAT プールが必要です。NAT プールは個別で一意であるため、クラウドから企業に戻るクライアントトラフィックは、常に特定の一意の NAT プールに、そしてサイトにルーティングされます。図 30 は、West ユーザーが West 接続を介してプライマリ（図 30 - 1）としてルーティングされ、East 接続がセカンダリ（図 30 - 2）としてルーティングされていることを示しています。図 31 は、East ネットワーク ドメイン ユーザーがプライマリ（図 31 - 1）として East 接続を介してルーティングされ、セカンダリ（31 - 2）として West 接続を介してルーティングされていることを示しています。

このルーティングシナリオは、両方の回路がサイトのユーザーのトラフィックをアクティブにルーティングしているため、アクティブ / アクティブと名付けられており、障害が発生した場合、両方の回路がもう片方のサイトのバックアップとして使用できます。サイジングの観点から、各回路は、障害が発生した場合に両方のサイトの帯域幅要件を処理できる必要もあります。そのため、各回路は適宜プロビジョニングする必要があります。サイトが企業 WAN によって分離されている場合、トラフィックが WAN を介してサイト間でルーティングされるときは、それに応じて WAN のサイズも設定する必要があります。

図 30　　サイト間の冗長性アクティブ / アクティブ回路：West のプライマリ / セカンダリパス

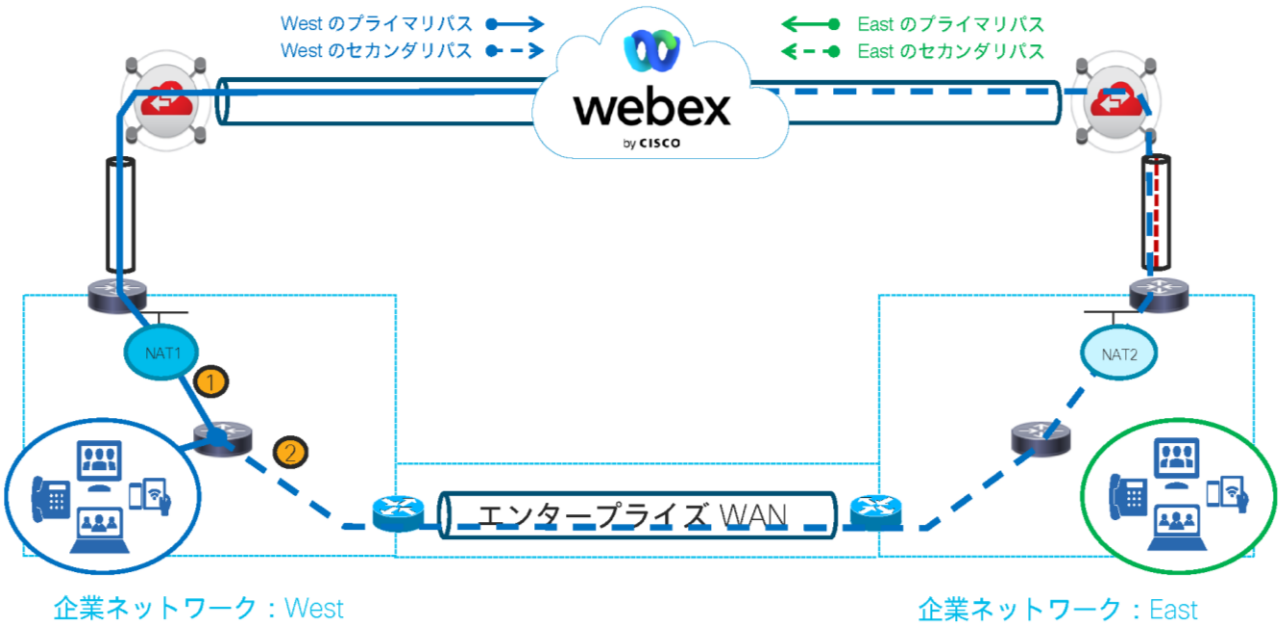
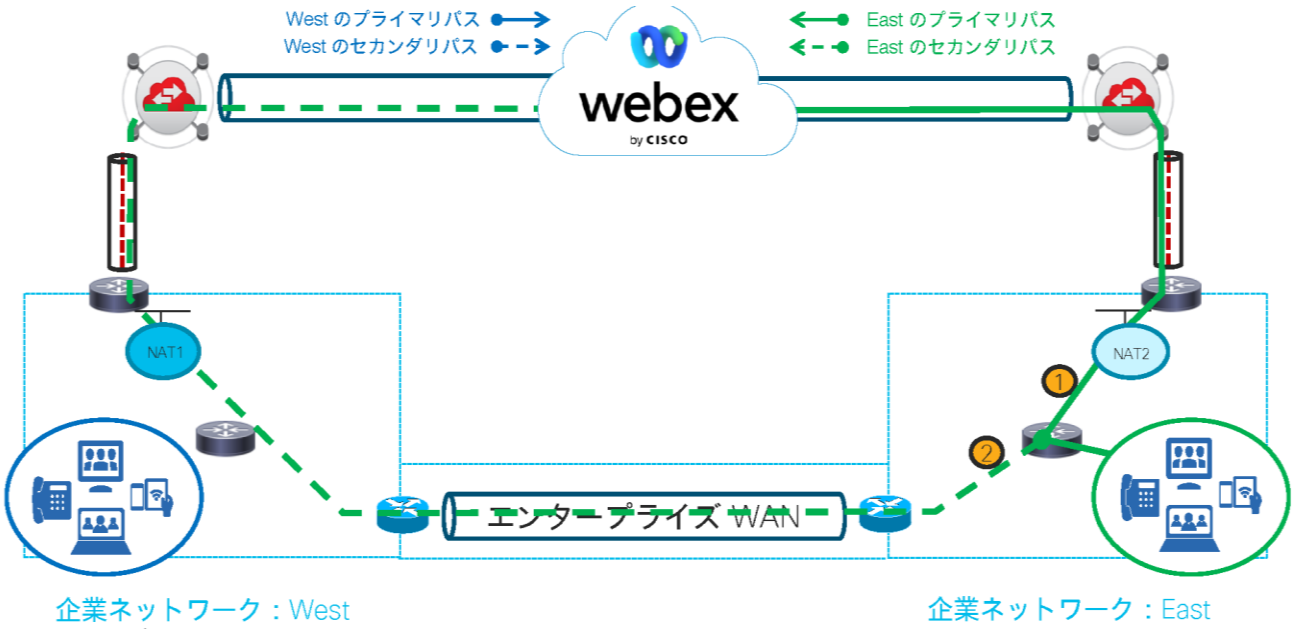


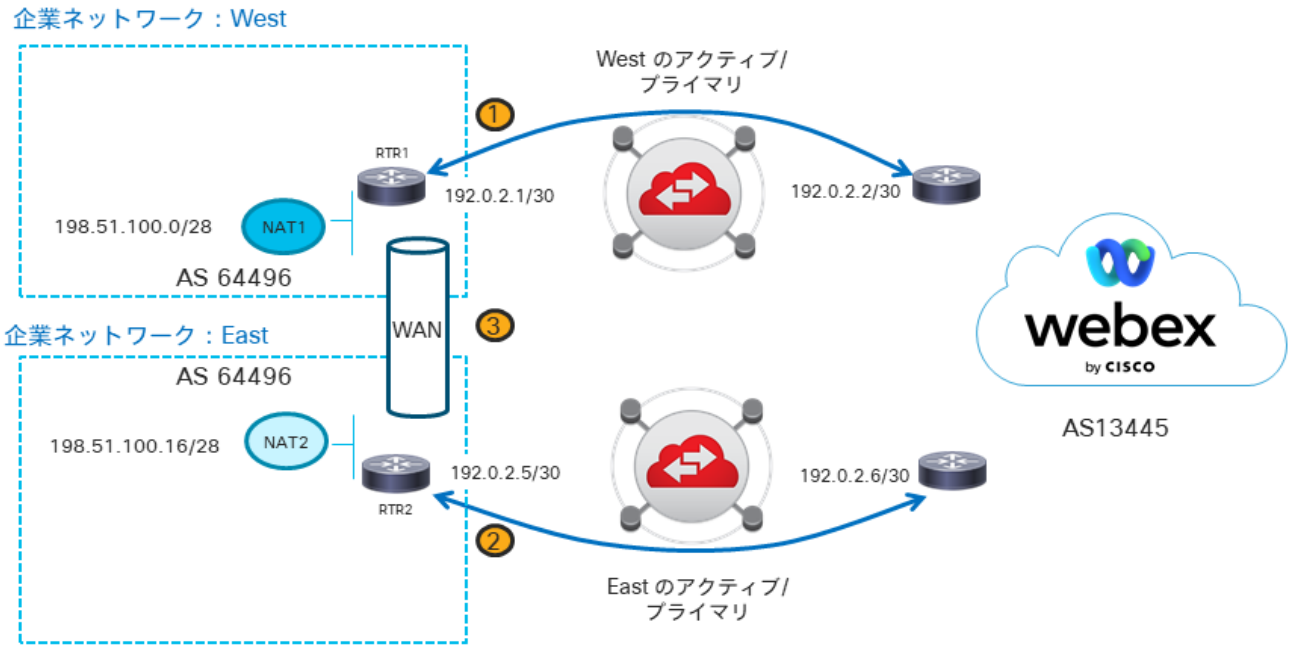
図 31　サイト間の冗長性アクティブ / アクティブ回路：East のプライマリ / セカンダリパス



地理的に離れている各サイトには一意の NAT プールが必要であるため、その NAT プールを介したリターントラフィックは常に Webex Cloud からそのサイトに返され、非対称にルーティングされたトラフィックに関する懸念がなくなります。

図 32 は、ローカルプリファレンスを使用してトラフィックのアクティブ / アクティブルーティングを保証する 2 つのサイトを示しています。この場合、West 接続（図 32 - 1）はプライマリで、East 接続（図 32 - 2）はセカンダリです。内部 WAN を介したロケーション間のトラフィックのエンジニアリング（図 32 - 3）は、このルーティングされた動作を確実にするために重要である点に注意することが重要です。

図 32　地理的に離れたサイトアクティブ / アクティブ回路



この構成は図 32 で説明されています。

RTR1 を West のプライマリアクティブリンクとして、RTR2 を East のプライマリアクティブリンクとして使用します。

Webex から企業ネットワークパスの選択：

RTR1 と RTR2 は、一意のプレフィックスをアドバタイズしています。そのため、Webex ネットワークからのリターントラフィックは、常にそれらの送信元 ネットワークプレフィックスからのリターンパスに従います。

企業から Webex ネットワークへのパスの選択：

図 26 では、RTR1 と RTR2 は、それぞれのサイト（図 26 - 1）と（図 26 - 2）で同じコストになります。同じルートのプライマリローカルパス（プレフィックス）がダウンしたときに、WAN 上の BGP ピアリングから学習したサブネット（図 26 -3）を再配布するのは、内部ルーティングプロトコル次第です。

RTR1 と RTR2 の次の設定は、上記のネットワークパス選択の設定例です。青で強調表示されているルートマップは、NAT プールをアドバタイズするために使用される構成を示しています。

RTR1 BGP 構成の例

```
router bgp 64496
 neighbor 192.0.2.2 remote-as 13445
!
 address-family ipv4
  neighbor 192.0.2.2 activate
  neighbor 192.0.2.2 send-community both
  neighbor 192.0.2.2 route-map PRIMARY-OUTout
exit-address-family
!
ip prefix-list ADVERTISE-NAT1-TO-WEBEX seq 5 permit 198.51.100.0/28
!
route-map PRIMARY-OUT permit 10
 match ip address prefix-list ADVERTISE-NAT1-TO-WEBEX
```

RTR2 BGP 構成の例

```
router bgp 64496
neighbor 192.0.2.6 remote-as 13445
 !
 address-family ipv4
  neighbor 192.0.2.6 activate
  neighbor 192.0.2.6 send-community both
  ネイバー 192.0.2.6 ルートマップ SECONDARY-OUT アウト
exit-address-family
!
ip prefix-list ADVERTISE-NAT2-TO-WEBEX seq 5 permit 198.51.100.16/28
!
route-map SECONDARY-OUT permit 10
 match ip address prefix-list ADVERTISE-NAT2-TO-WEBEX
```

アクティブ / パッシブ地理的に分散した Edge Connect 回路

このセットアップでは、一方のサイト（West）は両方のサイト（West と East）のプライマリである Edge Connect 回路をホストし、もう一方のサイト（East）は両方のサイト（West と East）のセカンダリの回路をホストします。これを図 33 と図 34 に示します。この場合、「企業ネットワーク：West」は Edge Connect へのプライマリパスをホストし、そのリンクに障害が発生した場合は、「企業ネットワーク：East」パスを使用する必要があります。2 つの別個の NAT プールが必要な地理的分離のため、このケースは同じサイトの 2 つの回路とは異なります。これら 2 つの個別の NAT プールがあるため、企業からのリターントラフィックは、各サイトに固有の NAT プールがあることにより、常に特定のサイトにルーティングされます。図 33 は、West ユーザーが West 接続を介してプライマリ（図 33 - 1）としてルーティングされ、East 接続がセカンダリ（図 33 - 2）としてルーティングされていることを示しています。図 34 は、East ユーザーに、West 接続を介してプライマリ（図 34 - 1）としてルーティングされ、East 接続がセカンダリ（図 34 - 2）としてルーティングされていることを示しています。

West 回路が両方のサイトのユーザーのトラフィックをアクティブにルーティングしているため、このルーティングシナリオはアクティブ / パッシブと呼ばれます。サイジングの観点から、各回路は、障害シナリオの場合に両方のサイトの帯域幅要件を処理できる必要もあります。そのため、各回路は適宜プロビジョニングする必要があります。

図 33　サイト間の冗長性アクティブ / パッシブ回路: West のプライマリ / セカンダリパス

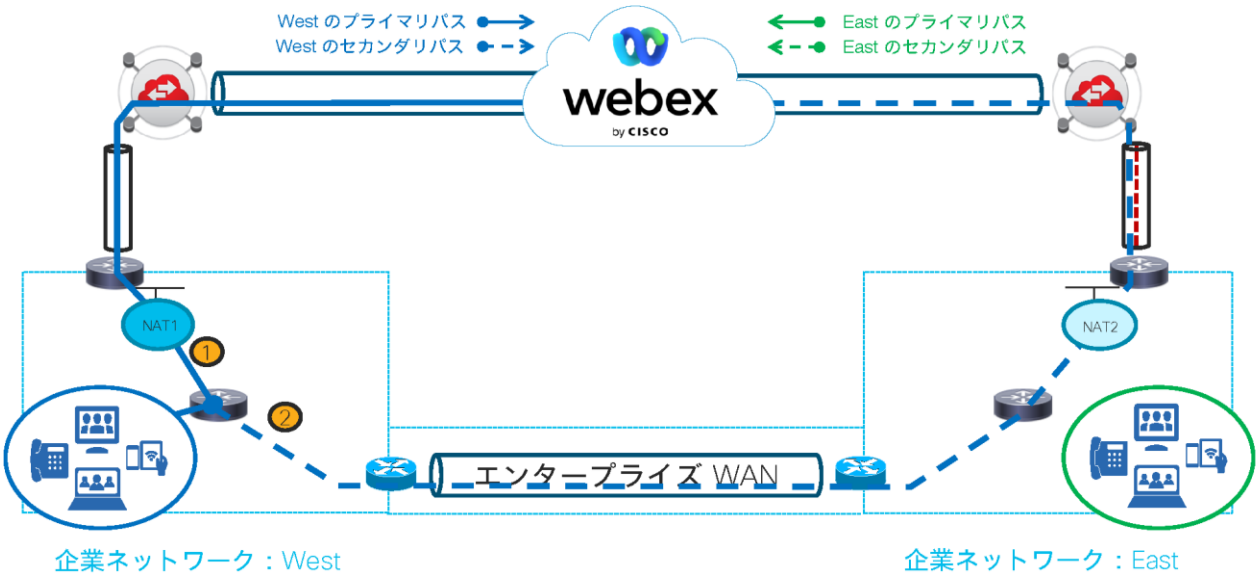
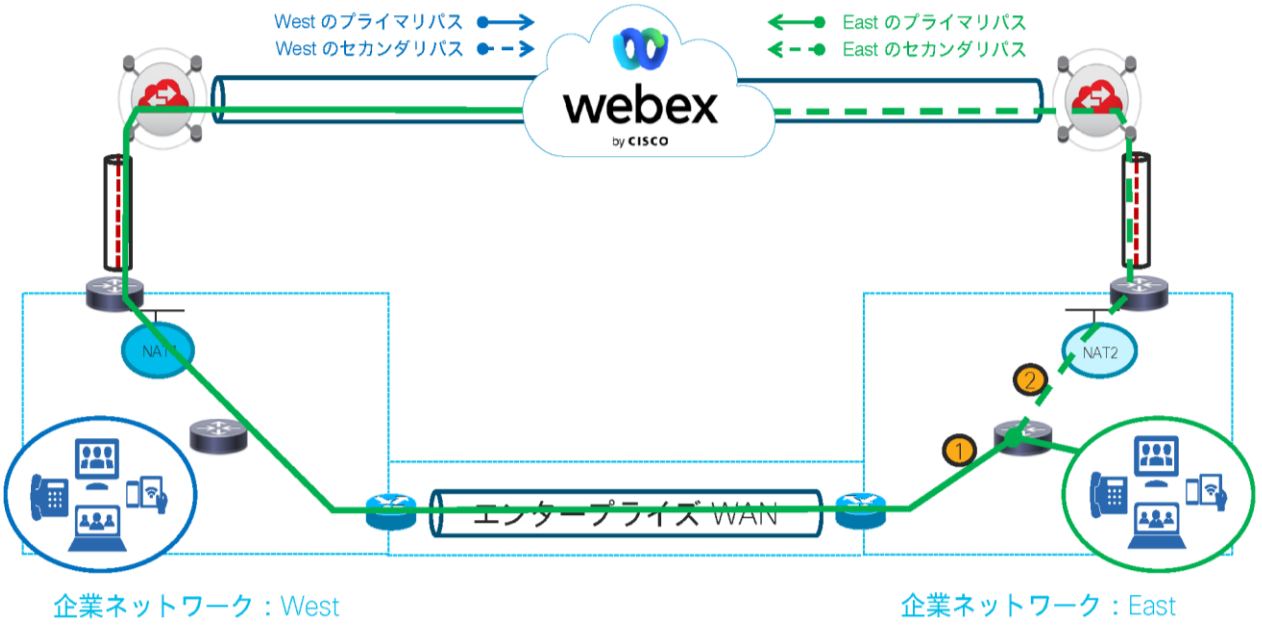


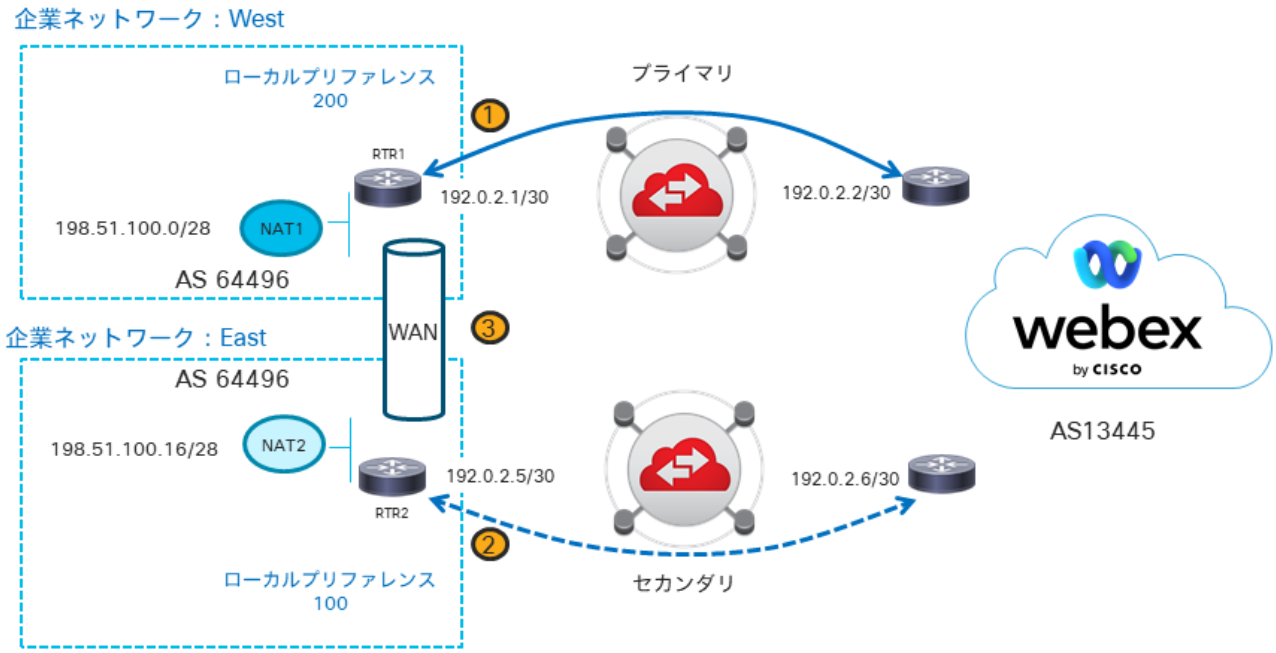
図 34　　サイト間の冗長性アクティブ / パッシブ回路: East のプライマリ / セカンダリパス



地理的に離れている各サイトには一意の NAT プールが必要であるため、その NAT プールを介したリターントラフィックは常に Webex Cloud からそのサイトに返され、非対称にルーティングされたトラフィックに関する懸念がなくなります。

図 35 は、ローカルプリファレンスを使用してトラフィックのアクティブ / スタンバイルーティングを保証する 2 つのサイトを示しています。この場合、West（図 35 - 1）がプライマリで、East（図 35 - 2）がセカンダリです。内部 WAN を介したロケーション間のトラフィックのエンジニアリング（図 35 - 3）は、このルーティング された動作を確実にするために重要である点に注意することが重要です。各ネットワークセグメント（East と West）には、すべての Webex プレフィックスに対して低コストのルートが必要です。

図 35　　地理的に離れたサイトにある Webex への 2 つの Edge Connect 回路を備えた企業ネットワーク



この構成は図 35 図 35 で説明されています。

RTR1 はプライマリリンクで、RTR2 はセカンダリリンクです。RTR1 は 200 のローカルプリファレンスを使用しているのに対し、RTR2 は 100 のローカルプリファレンスを使用しています。

Webex から企業ネットワークパスの選択：

図 35 では、RTR1 と RTR2 が一意のプレフィックスをアドバタイズしています。Webex ネットワークは、NAT を実行しているルータに応答します。

企業から Webex ネットワークへのパスの選択：

RTR1 は 200 のローカルプリファレンス（図 35 - 1）を適用して Webex ネットワークへの最も望ましいパスにしますが、RTR2 は 100 のローカルプリファレンスを適用し （図 35 - 2）、West と比較して望ましくありません。BGP でのこのローカルプリファレンスの優先順位を反映するコストで、West と East でのネットワークの観点から、Webex サブネットプレフィックスに関しては East パスよりも West パスが優先されるように、WAN を介した BGP ピアリングから学習したサブネットを再配布するのは内部ルーティングプロトコル次第です（図 35 - 3）。

RTR1 と RTR2 の次の構成は、BGP ローカルプリファレンスを使用した上記のネットワークパス選択の構成例です。青で強調表示されたルートマップは、ローカルプリファレンスの設定に使用される構成を示しています。

RTR1 BGP 構成の例

```
router bgp 64496
 neighbor 192.0.2.2 remote-as 13445
!
 address-family ipv4
  neighbor 192.0.2.2 activate
  neighbor 192.0.2.2 send-community both
  neighbor 192.0.2.2 route-map PRIMARY-OUTout
  neighbor 192.0.2.2 route-map PRIMARY-IN in
exit-address-family
!
ip prefix-list ADVERTISE-NAT1-TO-WEBEX seq 5 permit 198.51.100.0/28
!
route-map PRIMARY-OUT permit 10
 match ip address prefix-list ADVERTISE-NAT1-TO-WEBEX
!
route-map PRIMARY-IN permit 10
 set local-preference 200
```

RTR2 BGP 構成の例

```
router bgp 64496
neighbor 192.0.2.6 remote-as 13445
 !
 address-family ipv4
  neighbor 192.0.2.6 activate
  neighbor 192.0.2.6 send-community both
  ネイバー 192.0.2.6 ルートマップ SECONDARY-OUT アウト
  ネイバー 192.0.2.6 ルートマップ SECONDARY-IN イン
exit-address-family
!
ip prefix-list ADVERTISE-NAT2-TO-WEBEX seq 5 permit 198.51.100.16/28
!
route-map SECONDARY-OUT permit 10
 match ip address prefix-list ADVERTISE-NAT2-TO-WEBEX
!
route-map SECONDARY-IN permit 10
 set local-preference 100
```

フェイルオーバーとしてのインターネット

Webex Cloud へのゲートウェイとしてインターネットを使用してすでに展開されている Webex の顧客は、Edge Connect の実装を設計するときに、インターネットをフェイルオーバーパスとして使用できます。このタイプのフェイルオーバーには、予想されるトラフィックの負荷を処理するのに十分な帯域幅を備えたインターネット接続が必要です。何らかの理由で Edge Connect パスが失敗した場合、ローカル ルーティング プロトコルに再配布されたルートは、これらのプレフィックスの Edge Connect へのルートを削除し、トラフィックはデフォルトゲートウェイを使用するため、トラフィックをルーティングするインターネットは、Edge Connect の展開前の Webex トラフィックのルーティングと一貫しています。図 36 は、フェイルオーバーとしてのインターネットを示しています。

図 36　　フェイルオーバーとしてのインターネット

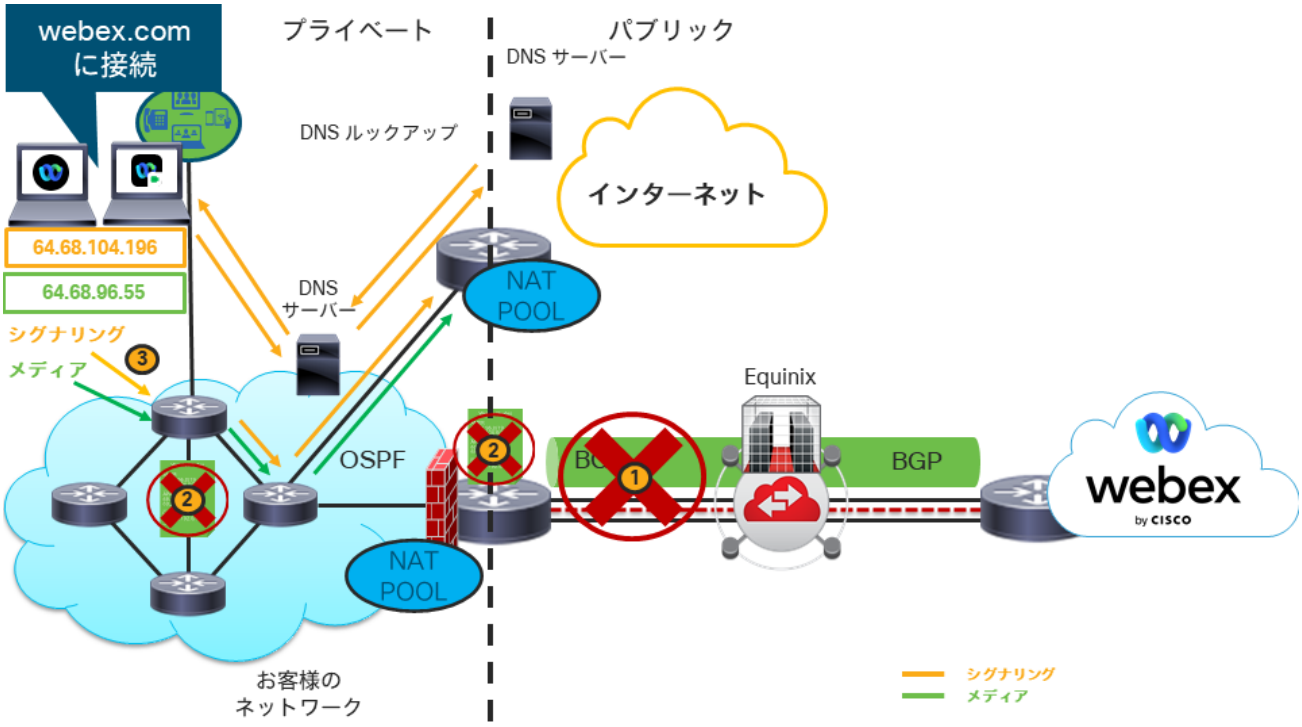


図 36 - 1 では、Edge Connect リンクがダウンしています。リンク障害の結果、ルーティングプロトコルが収束し、Webex からのルートプレフィックスがローカル ルーティング プロトコルから削除されます（図 36 - 2）。この結果、トラフィックは新しいパスにリダイレクトされます。ほとんどの場合、インターネットパスと Edge Connect パスは別々にルーティングされる場所になるため、同じ NAT プールからルーティングされません。NAT プールの変更により、Edge Connect を介してすでに確立された接続は、インターネットを介して再確立する必要があります。これは、いくつかの要因により、成功する場合と失敗する場合があります。接続が自動的に再確立される保証はなく、ユーザーは強制的にミーティングに再接続する場合があります。

帯域幅のプロビジョニングとキャパシティ プランニング

最繁時のアクティブな参加者全員に十分な帯域幅を確保し、さらに成長の余地を確保することは大変な作業です。このタスクを簡素化するために、現在の使用量の値（月間の会議時間（分））に基づいて、アクティブな会議参加者数（この例ではアクティブなコールと同義）を計算することを推奨します。アクティブなコール（参加者）の数を数えて、100% のオーディオ使用率とビデオ使用率の妥当な割合を求めます。時間の経過に伴う成長の割合を追加し、リンクのサイズを適切に設定する必要があります。

アクティブな参加者（アクティブコール）の特定

同時通話またはアクティブコールの価値を判断するために使用する有効な方法は、Webex Control Hub Analytics で記録された毎月の参加者分数を**ポート効率値**で割ることです。この場合のポートは、アクティブコールと同等です。この用語は、カンファレンスリリースエンジニアリングで使用されます。ポート効率の値は、月間参加者分数に基づいてアクティブなコール数を判断するのに役立つ値です。これにより、使用中の参加者分数に基づいて、最繁時に必要なアクティブな接続の見込みを把握できます。つまり、参加者分数が多ければ、それだけポートが増え、必要なアクティブ接続が増えるということです。合理的なポート効率（割り当てられたリソースに基づく使用率）を持つ既存のお客様からのデータに基づいて、**ポート効率値**は、ポートあたり 500 ~ 8500 分と推定されます。これは、システムの規模が大きくなる（アクティブなコールが増える）につれて、システムの効率が向上し、その結果としてポート効率の値が大きくなることから、月間参加者分数の範囲に依存します。計算で使用されるポート効率の値については、以下の図 38 を参照してください。

サイジングのサマリー

1. 「月間参加者分数」を特定します。
2. 「ポート効率値」を得るために、毎月の時間範囲のどこに該当するかを特定します。
3. 「月間参加者分数」を「ポート効率値」で割り、アクティブコールを計算します（「月間参加者分数」/「ポート効率値」=「アクティブコール」）。
4. アクティブなコールの数を求めたら、帯域幅使用率の計算を開始できます。

最初のステップは、Control Hub の分析で 1 か月あたりの参加者分数の最大時間を確認することです（図 37 図 37_ - 1 ~ 5）。Webex Control Hub の分析では、12 か月間（図 37 - 2）の「参加者別使用時間（分）」（図 37 - 1）を表示することで、特定の月（図 37 - 3）における参加者分数の最大時間を簡単に判断することができます。たとえば、Edge Connect 回路に基づいて「米国」に対してサイジングする場合、このピアリングで想定されるトラフィックに適している場合にのみ、「米国」を「場所別の使用状況」（図 37 - 4）に含めます。

図 37　Webex Control Hub の分析による月次参加者会議時間の例

次のステップでは、アクティブなコールを計算するために、「月間参加者分数」の値を取得し（図 37 - 3）、その値を月間分が発生する範囲に相当する「ポート効率値」で除算します。図 38 に推奨値を示します。

図 38　　ポート効率の計算値に対する月単位の時間範囲

月間分数	ポート効率値
0 ～ 50,000	月間分数/500
50,000 ～ 500,000	月間分数(月あたりの時間)/1000
500,000 ～1000,000	月間分数(月あたりの時間)/2000
1000,000 ～ 2000,000	月間分数(月あたりの時間)/3000
2,000,000 ～ 8,000,000	月間分数(月あたりの時間)/4000
8,000,000 ～15,000,000	月間分数(月あたりの時間)/5700
15,000,000 ～ 30,000,000	月間分数(月あたりの時間)/6500
30,000,000 ～40,000,000	月間分数(月あたりの時間)/7000
40,000,000 ～ 100,000,000	月間分数(月あたりの時間)/7500
> 100,000,000	月間分数(月あたりの時間)/8500

たとえば、ある月の最大参加者分数（分）が 2,550 万である場合（図 38 - 3）、月間分数（月あたりの時間）/6,500 の計算に分類されます。25,500,000 / 6500 = 3923 のアクティブな接続となります。また、これを 3950 のアクティブな接続に切り上げて、簡素化とオーバープロビジョニングを行うこともできます。

使用帯域幅（Bandwidth Utilization）

次に、単一のユーザー / デバイスがアクティブな Webex Meetings コールで平均的に消費する帯域幅の概算を示す平均帯域幅値を計算する必要があります。エンドポイントにはさまざまなタイプがあり、最大解像度と帯域幅のさまざまな機能があるため、これらを異なるグループに分割すると便利です。

すべての Webex デバイスとアプリケーションは、レートアダプテーションを使用してネットワークの状態と使用可能な帯域幅に応じてビットレートを動的に調整しますが、通常どのくらいの帯域幅がコールで使用されているかを知り、ユーザーエクスペリエンスを損なうことなく、最繁時のトラフィックに対応するために Edge Connect をプロビジョニングできるようにすることは重要です。

図 39 は、さまざまなタイプの Webex コンポーネントのオーディオとビデオの帯域幅の推奨事項を示しています。送信および受信の帯域幅の値を決定するための変数は多数あります。これらの帯域幅の値は計算しやすいように簡略化されています。この値は、成長率と余分なオーバーヘッドの両方を追加しています。回路の使用率を低くして容量近くまで稼働しないようにするためです。Webex アプリと Webex デバイスには、メインビデオと共有コンテンツビデオの両方があることにも注意してください。コンテンツを共有するデバイスとビデオのみを送信するデバイスに基づくビデオ帯域幅の送受信には違いがありますが、これらの違いはわずかであり、大規模なキャパシティプランニングを行う場合には関係ありません。一般に、帯域幅の計算に使用されるユーザーの数が多いほど、ビデオ帯域幅使用率の変動に関して平均が平坦になります。

図 39　Webex コンポーネントの帯域幅要件（レイヤー 3 オーバーヘッドを含む）

Webex コンポーネント	[オーディオ帯域幅（Audio Bandwidth）]	ビデオ帯域幅平均（最大）	高 FPS コンテンツ共有	グリッド 5 X 5
Webex Meetings デスクトップアプリ/ブラウザ	100 kbps	2mbps（3mbps）	1mb ~ 2.5mbps	5mbps
Webex アプリ	170 kbps	2mbps（4mbps）	1mb ~ 2.5mbps	なし
ビデオメッシュ展開時 （Webex アプリ、Unified CM インテグレーション）	600 kbps	12mbps（20Mbps）	該当なし	該当なし
DX シリーズ、SX10、MX シリーズ、SX20、SX80、Webex アプリ Room Kit、Webex Board *	100 kbps	2mbps（4mbps）	該当なし	該当なし
Expressway Edge 展開（Webex Edge Audio/Webex ビデオミーティング/Webex Hybrid）	80 kbps	2mbps（顧客設定**）	該当なし	該当なし

* デュアルスクリーンシステムの場合、ビデオ帯域幅の使用率が 2 倍になります。

** Expressway ビデオフローの最大ビットは、Unified CM に登録されたエンドポイントで設定されます

この例では、3950 のアクティブな接続に対応します。これらの 3950 の接続がすべて Webex Meetings アプリであり、65% のビデオの有効化が期待される場合、帯域幅について次の計算を実行できます。65% のビデオ有効化は、Control Hub からも計算できます（図 37 - 5 を参照）**アクティビティ別の使用量：ビデオ**。この例では、ミーティング参加者の 65.2% がビデオを有効にしたことがわかります。したがって、帯域幅の計算では、ビデオの割合として 65% を使用できます。

Webex Meetings アプリユーザーの帯域幅計算（例）：

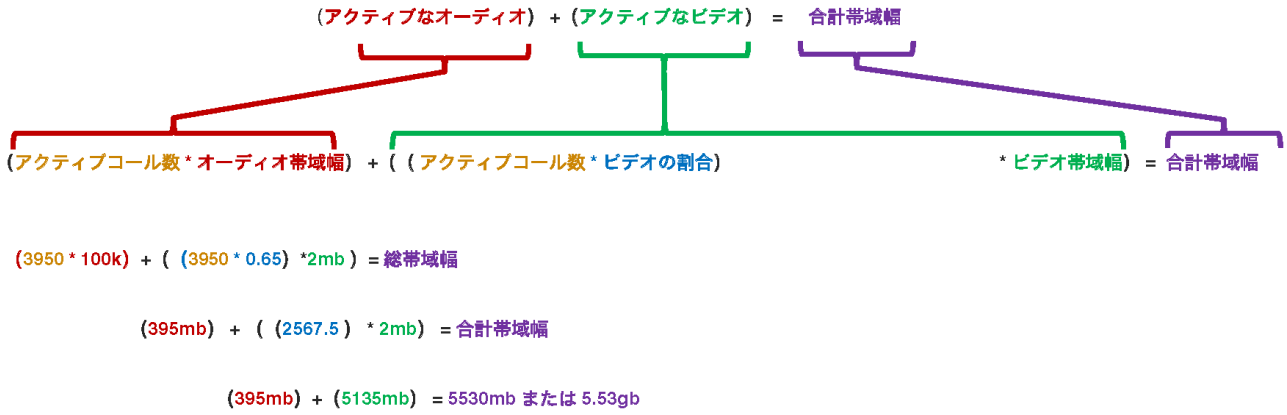
アクティブな通話 = **3950**

アクティブなオーディオ =（**アクティブなコール数** * オーディオ帯域幅）=（**3950** * 100k）= **395mb**

アクティブなビデオ =（（**アクティブなコール数** * **ビデオのパーセンテージ**）* ビデオ帯域幅） =（（**3950** * **0.65**） * 2mb） = **5135mb**

Webex アプリの合計帯域幅 =（**アクティブなオーディオ**）+（**アクティブなビデオ**）=（**395mb**） + （**5135mb**） = **5530mb または 5.53gb**

図 40　　帯域幅の計算



したがって、この分析に基づいて、米国の Edge Connect 回路には約 5.6gb が必要であると想定できます。この計算に関するいくつかのメモ。Webex Control Hub では、データはミーティングに接続されているすべての参加者に対するものです。ダイレクト インターネット アクセス（DIA） または企業ネットワーク経由で Webex Meetings に参加するゲストや参加者は区別されません。この情報を見分けるのに役立つデータを収集する方法がありますが、それはこのドキュメントの範囲外です。したがって、確認できる場合は、オンネットとオフネットの使用状況の違いを考慮することができます。そうでない場合は、計算された値を使用して、過剰なプロビジョニングと低使用率を確認することを推奨します。

最後のステップは、伸びしろを追加することです。成長の数値は、たとえば、会社全体の Webex の使用の予想される成長などの既知の要因に基づいている可能性があります。これは、ロールアウトプロセスまたは独自のシステムを使用して Webex に移行する会社のさまざまな部分が原因である可能性があり、理由はさまざまであっても、重要なのは、これが既知の変数であり、パーセンテージとして追加できるということです。したがって、たとえば、現在の計算は会社の 80% に基づいており、会社の残りの部分が間もなく Webex を展開すると予想されます。その後、係数の期待が同じであれば、つまり、計算で使用されたのと同じプラットフォーム（Webex デスクトップアプリ）の 20% が増加するなら、20% を計算に追加できます。

もう 1 つの例は、Room システムの展開です。たとえば、300 の Room システムが Webex デバイス（Board、Room、および Desk） で展開される場合、この使用量は接続されたエンドポイントの総数として追加できます。したがって、ピーク時間にこれらの Room システムの 100% が使用されることが予想されるとすると、その場合、100kbps のオーディオと 2mbps のビデオからなる 300 の Room システムを計算し、それを上で計算した数字に追加できます。

Room システムの帯域幅の計算（オーディオおよびビデオ）：

Room システム = **300**

Room システムオーディオ =（**アクティブな Room システム** * オーディオ帯域幅）=（**300** * 100k）= **30mb**

Room システムビデオ =（（**アクティブな Room システム** * ビデオのパーセンテージ）* ビデオ帯域幅）=（（**300** * 2mb）= **600mb**

Room システムの合計帯域幅 =（**アクティブオーディオ**）+（**アクティブビデオ**）=（**30mb**）+（**600mb**）= **630mb**

合計帯域幅の計算（合計 Room システム帯域幅 + 合計 Webex アプリ帯域幅）：

合計帯域幅 = Webex アプリの合計帯域幅 + Room システムの合計帯域幅 = 5530mb + 630mb = 6160mb または 6.16gb

上記の計算を考慮すると、この企業は 10gb 接続で安全に使用できます。また、7gb 接続（5gb + 2gb）を使用することもできますが、Equinix のコストとシスコの 7gb と 10gb のコストの価格設定を確認した後、10gb を使用した方が価格設定に優れていることがわかる可能性があります。10gb は、ビデオ使用量の未知数に対応できるだけでなく、未知の将来的な成長に備えることができます。

Webex シグナリングとメディアの QoS

メディアの QoS は、ネットワークでの質の高いエクスペリエンスを確保するために不可欠です。Edge Connect は、主にオーバープロビジョニングされ、低使用率のサービスである必要があります。Edge Connect の価値は、専用帯域幅と低遅延です。また、Edge Connect はメディアのためにインターネットをバイパスし、インターネットリンクに関連する遅延と過度のパケット損失を取り除きます。そのため、Edge Connect はオーバープロビジョニングする必要があります。しかしエッジテクノロジーであることに変わりはなく、企業ネットワークに出入りする QoS マーキングを確保することが重要です。これにより、不測の事態による輻輳や、不測の事態で発生しうる異常な高利用時に保護することができます。また、企業全体で他の WAN または輻輳ポイントに到達した場合（リモートサイトから Edge Connect が展開されているセントラルサイトにトラフィックを配信するリモートサイト WAN など）のダウンストリーム パケット マーキングも確保します。

QoS のベストプラクティスと推奨事項の概要については、「Webex ハイブリッドサービス（CVD）の推奨アーキテクチャ」の帯域幅管理の章を参照してください。ハイブリッドサービス CVD は、すべての Webex コラボレーション コンポーネントをカバーするわけではありませんが、それらの大部分をカバーし、Webex Meetings トラフィックのマーキングとキューイングの戦略に関する洞察が得られます。

Webex クラウドは、オーディオの場合は EF、ビデオの場合は AF41 にネイティブにトラフィックをマークします。これは、メディアの推奨事項をマーキングするコラボレーション アプリケーションのシスコの QoS と一致しています。ほとんどの場合、サービスプロバイダーがインターネット エクスチェンジを介してすべての QoS を BE（dscp 0）に再マーキングするため、この QoS マーキングは失われます。ただし、Edge Connect を使用すると、DSCP マーキングはそのままになり、Webex Cloud から企業への入力のときに、会社の QoS マーキングポスチャで適切に信頼または注釈を付けることができます。

図 41　Webex アプリエンドポイント、アプリケーション、およびビデオメッシュノードから来るトラフィックで使用される DSCP 値

トラフィックのタイプ	DSCP	注意
Audio	EF; 46	音声専用通話のオーディオ ストリーム、ビデオ コールのオーディオ ストリーム、および関連した RTCP パケットを含む
ビデオ	AF41; 34	ビデオストリーム（メインビデオ、プレゼンテーション、またはコンテンツ）、および関連する RTCP パケットを含む
その他のトラフィック	ベストエフォート、0	メッセージング、ファイル転送、設定、通話、およびミーティングの設定を含む

入力マーキング、出力キューイング

前述のように、Edge Connect は、企業ネットワークが Webex クラウド サービス ネットワークに移行するエッジに展開されます。ネットワークの他のエッジエリアと同様に、これはマーキングとキューイングが発生する場所です。マーキングはルータインターフェイスの入口で発生し、キューイングはルータインターフェイスの出口で発生します。図 42 は、マーキングとキューイングが発生する可能性のある Edge Connect ネットワークの領域を示しています。

図 42　　Webex トラフィックのマーキングおよびキューイング

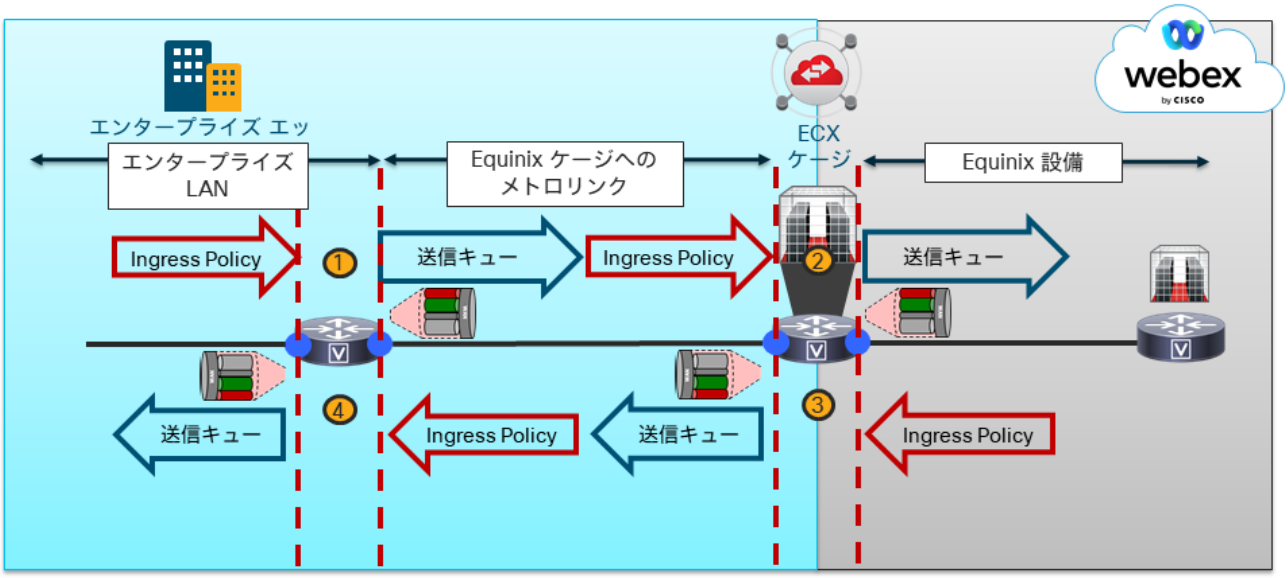


図 42 は、QoS マーキングポリシーを配置できるネットワーク領域と、アウトバウンド キューイング ポリシーを配置できるエリアを示しています。上が企業からクラウドへのトラフィック（ルータの場所 1 と 2）で、下がクラウドから企業へのトラフィック（ルータの場所 3 と 4）です。これは、トラフィックがルータに入るとき、QoS マーキングが行われる場所です。ネットワーク内の他の場所でトラフィックがどのようにマークされているかにかかわらず、ネットワークのエッジに QoS マーキングポリシーを設定して、企業内でトラフィックをマークできなかったすべての場所が、アウトバウンド インターフェイスと後続のキューに向かう前に確実にキャプチャされるようにすることが重要です。

ロケーション 1 では、インバウンドポリシーは、企業から来るすべての Webex 宛てのトラフィックをキャプチャし、適切にマークできます。次に、アウトバウンド インターフェイスのロケーション 1 でキューイングポリシーを設定して、トラフィックのバーストや予期しない使用率の高いイベントが発生した場合に、トラフィックがキューイングを必要とするとき、回路に送信される前にここで管理されるようにすることができます 。キューイングポリシーが作成されていない場合、アウトバウンド インターフェイスの送信リングが輻輳すると、トラフィックはデフォルトの FIFO（先入れ先出し）キューに送信され、優先順位に関係なく必要に応じて過剰なトラフィックがドロップされます。これにより、ビデオからオーディオがドロップされ、オーディオ品質の問題が発生する可能性があります。一般に、ビデオは損失に対する耐性がはるかに高く、帯域幅の変化への適応に優れています。オーディオは損失に対する許容度がはるかに低いため、ビデオよりも損失の影響を受けます。そのため、少なくともオーディオ用のプライオリティキュー（PQ）とビデオ用のクラスベースの重み付け均等化キュー（CBWFQ）を使用して、オーディオがビデオよりも常に優先され、ドロップが発生した場合は、最初にビデオがドロップされて、発生した損失に基づいてレートを調整でき、高品質のオーディオ接続が確保されるようにすることをお勧めします。

図 42 のロケーション 2 は、ケージ内のルータ上にあり、QoS マーキングおよびキューイングのもう 1 つの潜在的なロケーションです。マーキングがロケーション 1 で行われた場合、マーキングは必要ありませんが、PQ/CBWFQ と FIFO キューを介して輻輳が確実に規制されるように、引き続きキューイングを実施する必要があります。

クラウドから企業に向かうロケーション 3 のリバーストラフィックの場合。これは、クラウドからのトラフィックを企業 QoS ポリシーの値にマークする場所です。Webex Cloud は、オーディオ用に EF をマークし、ビデオ用に AF41 をマークして、他のすべてのトラフィックは BE にマークします。そのため、EF と AF41 が単純に信頼される場合でも、これは、CS3 および他のトラフィックへのシグナリングを適宜リマークするのに適した場所です。ロケーション 1 および 2 に適用したのと同じキューイングポリシーをロケーション 3 および 4 のアウトバウンド インターフェイスにも適用する必要があります。

注： ネットワークは全二重と見なされ、異なる有線を介して送受信され、対称的なコールフローでもトラフィックパターンがまったく異なる場合があります。このような輻輳は、インバウンドで発生する可能性があり、アウトバウンドでは見られません。したがって、これらのインターフェイスでキューイングポリシーを確保して、トラフィックが正しく優先順位付けされ、輻輳の発生時に効率的にドロップされるようにすることが重要です。

帯域割り当て

キューに帯域幅を割り当てるには、オーディオとビデオの以前のキャパシティプランニングの計算を使用して、PQ と CBWFQ のパーセンテージの概算を決定できます。以下は、前に行ったグロス計算のタイプに基づいて可能なことのほんの一例です。帯域幅の計算と割り当ては、さまざまなプロセスとさまざまな精度で推定できます。この例では、モデルはオーディオが PQ に配置され、決してドロップされません。そのため、下の例に示すように、PQ のオーバープロビジョニングを確実にすることが重要です。しかし、どのようなものでも現実的に 33% を超えると、PQ が FIFO キューに変わり始め、他のキューを枯渇させる可能性があります。そのため、通常、33% を超える PQ を帯域幅全体に割り当てることは推奨されません。下の例ではその状態に近づきませんが、シナリオによっては可能性があります。オーディオが帯域幅全体の 33% を超える場合は、オーディオをビデオとは別の CBWFQ に入れ、オーディオとビデオの両方を別の CBWFQ で管理することをお勧めします。

例での接続サイズ設定の計算では、Room システムからの音声が 30mb、Webex Meetings アプリからの音声が 395mb で、合計 425mb でした。ビデオの場合、ビデオにはそれぞれ 600mb + 5135mb があり、合計は 5735mb でした。6.16gb の合計帯域幅のこの例では、オーディオは帯域幅の合計量の約 7% を使用し、ビデオは約 93% を使用します。これは、PQ および CBWFQ に許可される帯域幅の割合を概算するのに役立ちます。PQ のサイズを決定するために、輻輳の場合に PQ で使用されていない分が CBWFQ に割り当てられることがわかっているため、パーセンテージ以上をオーディオに追加できます。そのため、10gb 接続があり、その 15% を PQ に許可すると、PQ のオーディオに 1.5gb が割り当てられます（計算から必要な量の 3 倍）。ビデオには最低 5735 または約 6gb が必要です。したがって、ビデオ CBWFQ に 70% を割り当てて、7gb を可能にします。これにより、帯域幅の約 15% がシグナリング、データのルーティング、および超過帯域幅に使用されます。このように構成することで、オーディオが欠落したり遅延したりすることはなく、ビデオが共有をより多くを使用する場合、それに応じて CBWFQ からテールドロップが発生します。繰り返しますが、ここでの計算は成長に備えて行われており、未知の使用のために十分な帯域幅を確保するためにオーバープロビジョニングされていますが、より多くのオーディオが必要な場合、ビデオに影響を与えることなくオーディオの割合を最大 3 倍に増やすことができるように保護されています. その間、ビデオは PQ からの未使用の帯域幅を使用して、極端な使用状況でのエクスペリエンスの品質を確保できます。

QoS および Webex メディアのスケジューリングとキューイングの詳細については、「Webex ハイブリッドサービス（CVD）の推奨アーキテクチャ」の帯域幅管理の章を参照してください。

注： 「Webex ハイブリッドサービス（CVD）の推奨アーキテクチャ」の帯域幅管理の章にはすべての Webex Meetings のトラフィックは含まれていないことに注意してください。たとえば、Webex Meetings アプリケーションのトラフィックはこの例にありません。しかし、帯域幅管理の章で説明されている概念は、すべての Webex Meetings クライアント、エンドポイント、およびエッジ機器に適用できます。ほとんどの場合、オーディオ、ビデオ、シグナリングプロトコル、使用されるポート、または NBAR などの他の適用可能な分類メカニズムなど、トラフィックを効果的にマークして分類するために必要な情報を収集するだけの問題です。

Equinix ECX 物理ポートの考慮事項

ECX 接続は、物理インターフェイスの帯域幅キャパシティ以下の指定された帯域幅の物理ポート上の仮想回路です。たとえば、プロビジョニングされたポートが 1gb ポートで、接続が 500mb に設定されている場合、物理ルータインターフェイスのサブインターフェイスが構成され、500mb の帯域幅に設定されます。

仮想接続は、帯域幅レートで Equinix によってポリシングされます。このように、ルータの物理インターフェイス上のトラフィックシェーパーは、サブインターフェイスの仮想回路機能を超える 1 秒未満のバーストからトラフィックを保護します。トラフィックシェーパーは、トラフィックの短期間のバーストのために Equinix リンクに配置されているポリサー

によってトラフィックがドロップされないようにします。したがって、接続が 500mb に設定されている場合、500mb の一致するシェーパーを実装して、Equinix による帯域幅プロビジョニングを超える 1 秒未満のトラフィックバーストを回避できます。トラフィックシェーピングと CBWFQ の利点を得るために、CBWFQ にトラフィックシェーパーを配置することを推奨します。これに関する詳細は、「QoS：パケットフロー制御のコンフィギュレーションガイド」を参照してください。

QoS ポリシーの例

図 43 は、200mbps へのトラフィックシェーピングと、Webex 関連トラフィックでの一致のための NBAR での QoS ポリシー（PQ/CBWFQ）を使用した階層型出力ポリシーの IOS 構成を示しています。

注： これは単なる例であり、すべてのタイプの Webex トラフィックを一致させるには、プロトコルと送信元/接続先 UDP/TCP ポートを使用して、他の Webex 宛てのトラフィック（つまり、SIP またはビデオメッシュ）を識別する ACL とのより完全な一致ポリシーが必要です。

図 43 NBAR を使用した階層型 QoS およびトラフィック シェーピング ポリシー

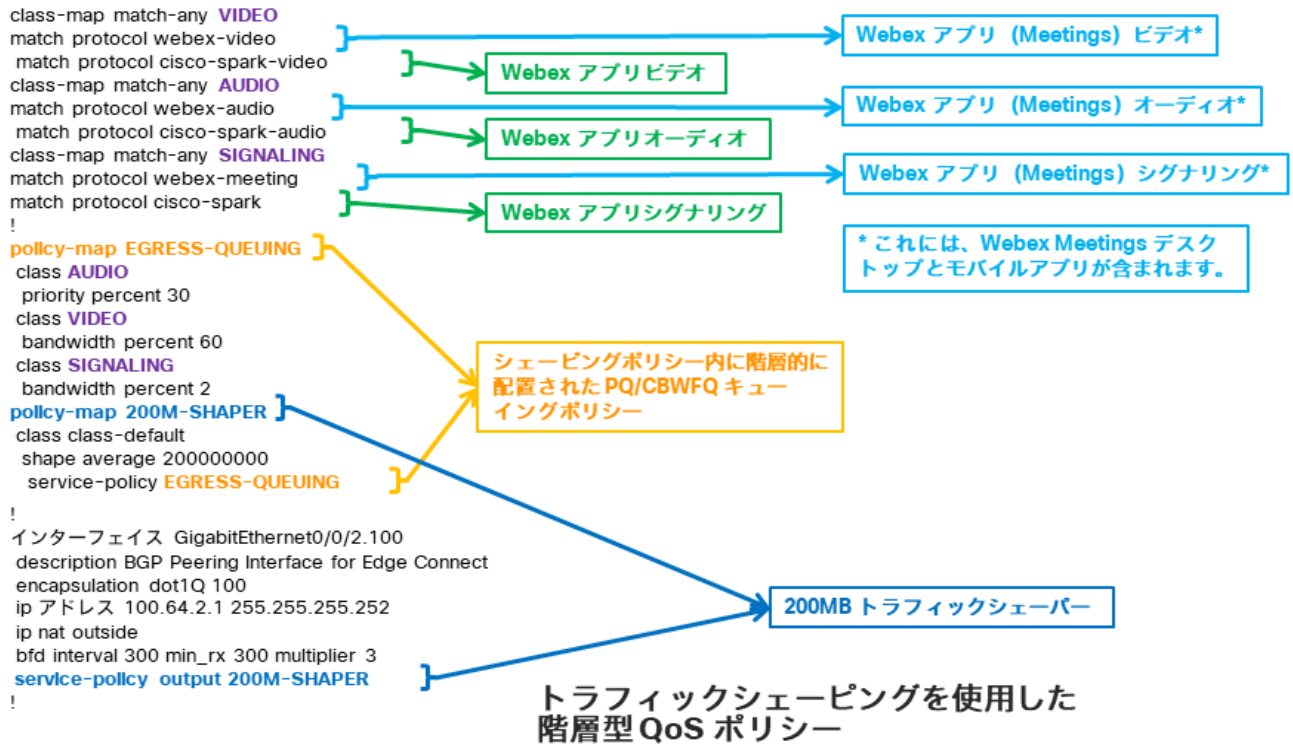


図 43 には、EGRESS-QUEUING と 200M-SHAPER の 2 つのポリシーマップがあります。まず、200M-SHAPER ポリシーは、トラフィックが 200mbps にシェーピングされることを保証するトラフィック シェーピング ポリシーです。これにより、トラフィックの 1 秒未満のバーストが平滑化され、バーストに関連するドロップが発生しないようになります。次に、EGRESS-QUEUING ポリシーマップは 200M-SHAPER ポリシーにネストされており、Webex オーディオ用の PQ（プライオリティキュー）と Webex ビデオおよびシグナリングトラフィック用の CBWFQ（クラスベースの重み付け均等化キュー）を持つ出力キューイングポリシーです。このポリシーは、リンク帯域幅の 92% を使用し、PQ の音声に 30%、ビデオに 60%、Webex シグナリングトラフィックには 2% のみを確保します。8% は使用されず、通常、BGP、BFD、またはその他のシグナリングプロトコルなどの他のトラフィックがキューに確実にアクセスできるようにするために、デフォルトキューまたは別の CBWFQ を必要とします。EGRESS-QUEUING に関連付けられたクラスマップは、Webex アプリおよび Webex デバイス関連のトラフィックの NBAR プロトコルで一致するように設定されています。これには、フル機能のミーティングが有効なトラフィックを備えた Webex アプリも含まれます。フル機能のミーティングを備えた Webex アプリのトラフィックは、Webex Meetings デスクトップアプリのトラフィックと同じであるため、このトラフィックサブセットの照合には同じ NBAR プロトコルが使用されます。

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.**