



# Unified Contact Center Enterprise ソリューション設計上の考慮事項

- [コアコンポーネント設計上の考慮事項, on page 1](#)
- [リファレンス設計とトポロジ設計に関する考慮事項, on page 56](#)
- [オプションのシスココンポーネント設計上の考慮事項, on page 60](#)
- [サードパーティ コンポーネント設計上の考慮事項, on page 75](#)

## コアコンポーネント設計上の考慮事項

### 一般的なソリューション要件

#### ソリューションのデータバックアップ

データバックアップツールは、スケジュールされたメンテナンスウィンドウでのみ実行します。ローカル SQL バックアップを使用する場合は、ローカルマシンに十分なキャパシティがあることを確認します。そうでない場合は、ネットワーク上のリモートストレージにバックアップします。

#### NTP および時刻同期

Contact Center Enterprise ソリューションには、ソリューションのすべての部分に同じ時間が必要です。時間のずれは自然に発生しますが、ソリューション コンポーネントの同期を維持するために NTP を設定することは重要です。ライブデータレポートで時間の差異を回避するため、これら VM での NTP 設定は同期されなければなりません。

- ルータ
- Logger
- Administration & Data Server
- Unified Intelligence Center のパブリッシャとサブスクライバ



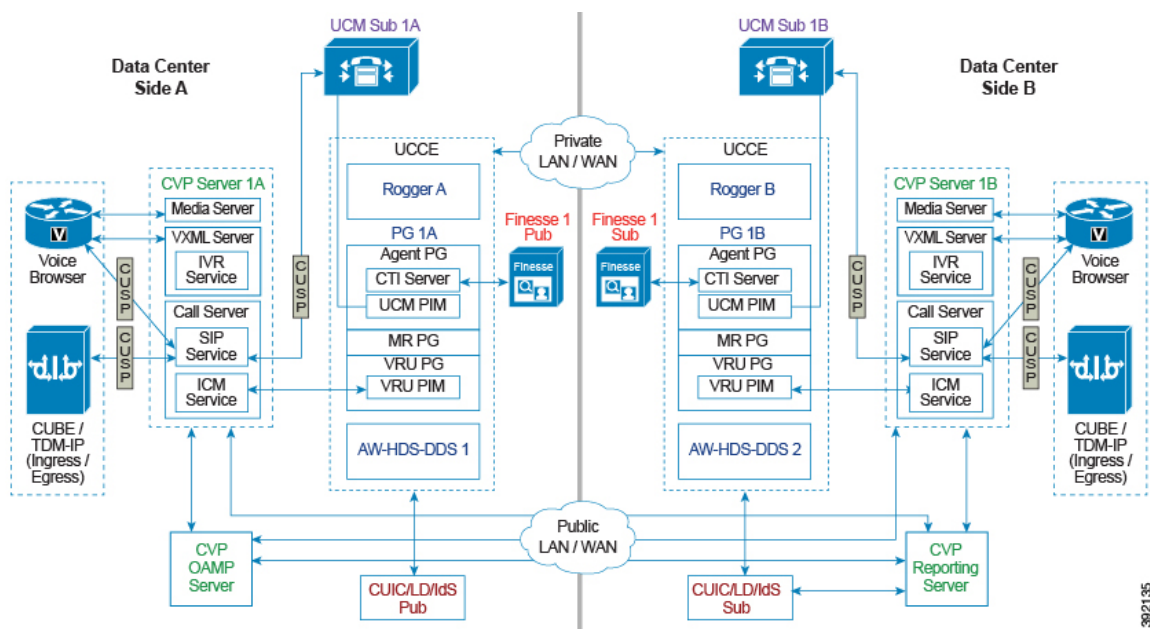
**Note** Finesse Desktop クライアントマシンは、ライブデータレポート内の [期間 (Duration)] フィールドへの正確な更新のため、有効な NTP サーバを使用して、時間を同期する必要があります。

## Contact Center Enterprise リファレンス設計トポロジの詳細

### 詳細な 2000 エージェントリファレンス設計

次の図は、冗長なデータセンター内の両側面間における通常の動作条件での論理的な接続を示しています。

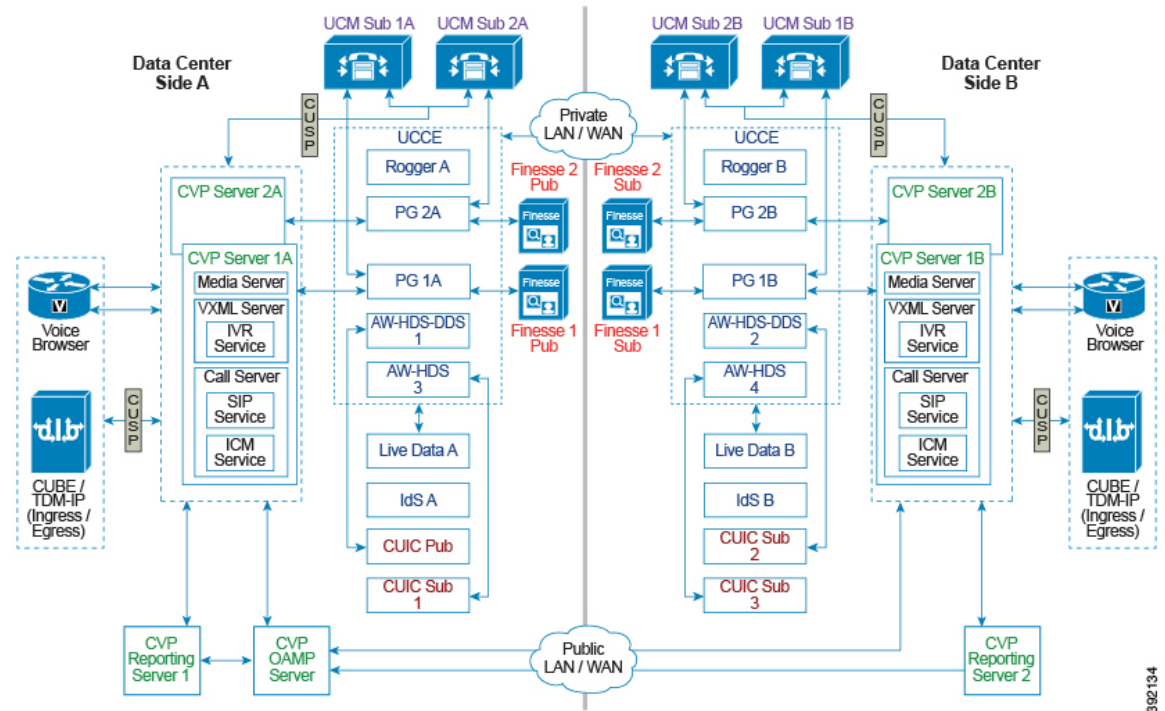
Figure 1: 詳細な 2000 エージェントリファレンス設計



### 詳細な 4000 エージェントリファレンス設計

次の図は、冗長なデータセンター内の両側面間における通常の動作条件での論理的な接続を示しています。

Figure 2: 詳細な 4000 エージェントリファレンス設計

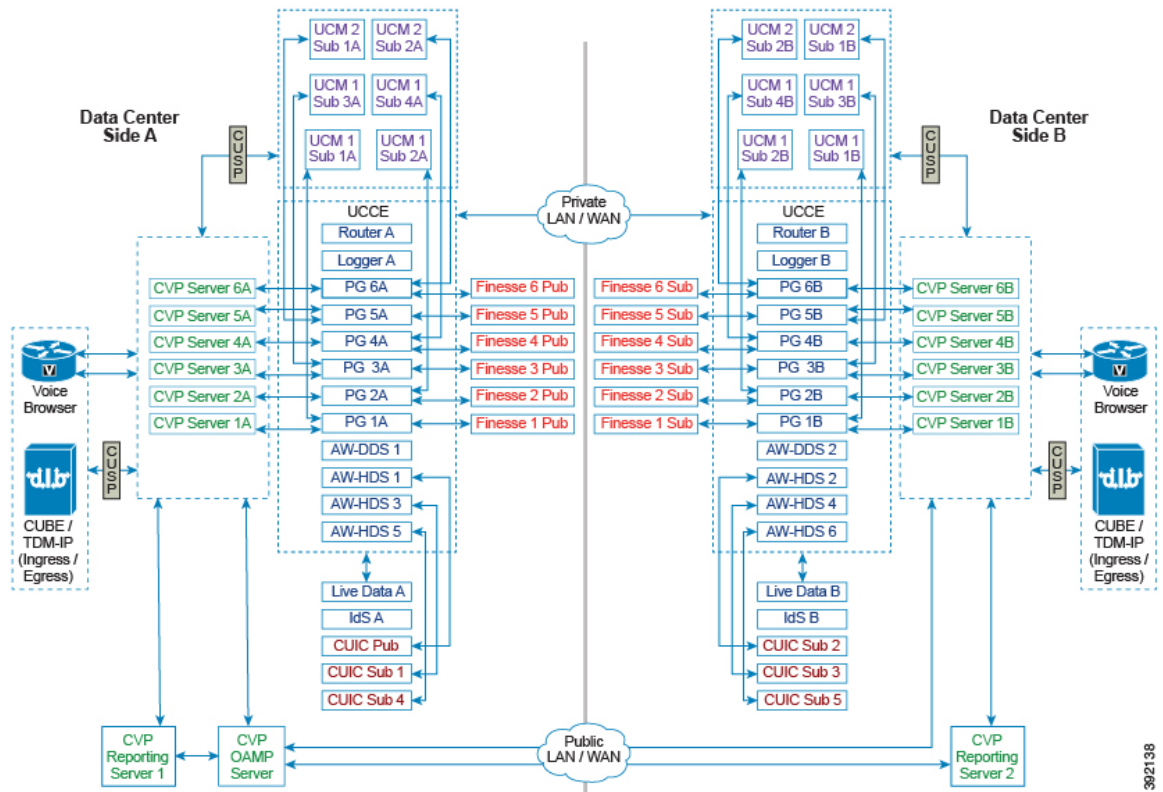


392134

詳細な 12000 エージェントリファレンス設計

次の図は、冗長なデータセンター内の両側面間における通常の動作条件での論理的な接続を示しています。

Figure 3: 詳細な 12000 エージェントリファレンス設計



詳細な 24000 エージェントリファレンス設計

24000 エージェントリファレンス設計では、通常の動作条件での論理的な接続は 12000 エージェントリファレンス設計のパターンに従います。ただし、最小 12 台の CVP、PG、および Finesse サーバがあります。

## 入力/出力/VXML ゲートウェイの設計上の考慮事項

### IOS ゲートウェイの役割

Contact Center Enterprise ソリューションでは、TDM 入力および VXML レンダリングに IOS ゲートウェイが使用されます。通常は、いずれかまたは両方の目的に対して、ソリューションでサポートされている任意の Cisco ゲートウェイを使用できます。次の表は、各機能を使用するコールフローを示しています。

Table 1: コールフロー別の IOS ゲートウェイ機能の使用

コールフロー	TDM 入力	VXML レンダリング
リファレンス設計		

コールフロー	TDM 入力	VXML レンダリング
Unified ICM Micro-Apps を使用する包括的コールフロー	可	一部
Unified CVP VXML Server を使用する包括的コールフロー	可	一部
非リファレンス設計		
スタンドアロンセルフサービス	はい	はい
コールディレクタ	はい	なし
NIC制御ルーティングのみを使用するVRU	はい	はい



**Note** VXML ゲートウェイの代替として Cisco Virtualized Voice Browser を使用できます。

入力およびVXMLの両方が必要な場合は、同じゲートウェイで両方の機能を実行するか、一部のゲートウェイを入力用に指定し、他のゲートウェイをVXML用に指定できます。次のガイドラインに従って、機能を結合するか分割するかを判断してください。

- 到着したブランチでコールがキューに格納されるブランチ オフィス展開では、入力機能とVXML機能を常に結合します。
- 多数の非CVP PSTN 接続でゲートウェイを共有している場合は、各機能ごとに個別のゲートウェイを使用します。
- VXML のみのゲートウェイは、DSP ファームやTDMカードが不要なためコストが低くなります。
- コール量が少ない場合は、通常、冗長性のために機能を結合します。結合されたゲートウェイのいずれかで障害が発生した場合は、容量を低減して、他のゲートウェイで引き続きコールを処理できます。

次に、Cisco サービス統合型ルータ (ISR) またはISR-G2 ゲートウェイのどちらを使用するかを決定します。

ISR ゲートウェイを使用する従来のブランチ オフィスには以下が含まれます。

- TDM コールがPSTNから到着する複数サイトの1つ
- ソリューションの大部分の機器が存在するメインサイトから分離されたサイト
- 各サイトが1つのゲートウェイを使用

**Related Topics**

[Cisco Virtualized Voice Browser の設計上の考慮事項](#), on page 27

**TDM-IP ゲートウェイ設計に関する検討事項**

さまざまな音声ゲートウェイでサポートされる各種デジタル（T1/E1）およびアナログインターフェイスの最新情報については、次のサイトから入手可能な最新の製品マニュアルを参照してください。

- ルーター—<http://www.cisco.com/cisco/web/psa/default.html?mode=prod&level0=268437899>
- **Unified Communications** ゲートウェイ—<http://www.cisco.com/cisco/web/psa/default.html?mode=prod&level0=278875240>

**Cisco Unified Border Element 設計に関する考慮事項**

Cisco Unified Border Element（CUBE）は、SIP を使用した IP 音声ネットワーク間の接続を提供する Session Border Controller（SBC）です。ソリューションでは、物理 CUBE または仮想 CUBE を使用することができます。ソリューションは、すべてのコールが CUBE を介してルーティングされるフロースルー モードでのみ CUBE を使用できます。

**Note**

フロースルー モードとは異なり、フローアラウンドモードでは、DTMF インターワーキング、トランスコーディング、および電話機やメディア機能などのその他の主要機能を使用することはできません。

TDM 音声回線を電話会社の IP 音声トランクに置き換える場合、ソリューションには CUBE が必要となります。CUBE は、IP 音声トランク上で企業をサービスプロバイダーに接続するための機能境界ポイントとして機能します。

**Note**

アウトバウンドコールの場合、物理 CUBE はコール進行状況分析（CPA）をサポートします。仮想 CUBE は、CPA をサポートしていません。

テストでは、以下のシナリオで CUBE を使用できることが示されています。

- シスコによって認定済みの SIP トランクを介したサードパーティ製 SIP デバイスと Unified CVP 間の SIP-to-SIP 接続
- Unified CM と Unified CVP 間の SIP-to-SIP 接続

トポロジや設定など、Unified CVP での CUBE の使用に関する詳細については、[http://cisco.com/en/US/docs/voice\\_ip\\_comm/unified\\_communications/cubecc.html](http://cisco.com/en/US/docs/voice_ip_comm/unified_communications/cubecc.html) の コールセンター ソリューション向け *Cisco Unified Border Element* を参照してください。



**Note** 各 CUBE がサポートする最大セッション数の一覧については、<http://www.cisco.com/c/en/us/support/routers/cloud-services-router-1000v-series/products-installation-and-configuration-guides-list.html> の *Cisco Unified Border Element* コンフィギュレーションガイドを参照してください。



**Note** Cisco IOS の制限により、CUBE では、音声からビデオ、およびビデオから音声への通話中のエスカレーションまたはデスカレーションはサポートされません。



**Note** 現在、CVP は SIP メッセージの Allowed-Methods を確認しません。その結果、アウトバウンドは UPDATE メソッドをサポートしていませんが、UPDATE メッセージをインGRESS からアウトバウンド レッグに渡します。

回避策: UPDATE メッセージをインGRESS レッグの SBC で無効にします。

### CUBE 展開の制限

SIP トランクで CUBE を展開する場合は、以下の制限を遵守してください。

- Unified CVP 展開で、ダイヤルピアのデフォルトモードであるメディアパススルーモードで CUBE を設定します。メディアフローアラウンドモードは、Webex エクスペリエンス管理のみでサポートされています。
- CUBE は、REFER コールフローの開始時に CVP からの Refer-To ヘッダー URI 宛先の受け渡しをサポートしていません。CUBE によって、ダイヤルピアコンフィギュレーションに基づいて宛先アドレスが書き換えられます。そのため、ダイヤルプランは CVP および CUBE で設定する必要があります。
- REFER パススルーを耐障害性で使用することはできません。スクリプトは、他の CUBE の設定に関係なく、REFER メッセージが SIP サービスプロバイダーにリレー送信されないようにします。
- 耐障害性およびルータ再クエリでは REFER 消費を使用できません。存続可能性は、転送が完了していない場合でも、常に REFER を受け入れます。Unified CCE は、転送が成功したと見なし、再クエリーしようとしません。
- サービスプロバイダーの代替宛先ルーティング (ADR) で耐障害性を使用することはできません。スクリプトの処理では、エラーメッセージ (Ring-No-Answer または ビジー) がサービスプロバイダーに到達しないようにします。代わりに、Remote-Party-ID ヘッダの処理が必要となります。
- GTD が着信コール中であるか、または Unified CCE が UII 変数の値を設定する場合、Unified CVP は DTMF 転送でディジットをアウトパルスした直後に BYE を送信します。数字の間に遅延が必要な場合は、ラベルの最後にコンマを使用します。

- 着信コールに GTD が存在しない場合、Unified CCE は UUI 変数の値を設定しません。次に、サービス プロバイダーは、DTMF 転送で数字を受信した後、コールを切断しません。Unified CVP は SIP.ExternalTransferWait タイマーの期限が切れた後、BYE 要求を送信します。
- サービス コールバックを使用したソリューションには、耐障害性が必要です。

**Note**

コール耐障害性は CUBE HA モードでサポートされますが、以下の制限があります。

- CVP に登録されたサービス コールバック (CCB) がある場合、ポスト スイッチ オーバー CCB はサポートされません。
- コール 存続可能性 TCL スクリプトのみ CUBE 高可用性でサポートされます。他の TCL ベースのサービスはサポートされません。
- アクティブ コールのみがチェック ポイントされます。(接続しているコール: 200OK/ACK トランザクション完了)。遷移状態のコールはチェック ポイントされません。

**Related Topics**

[Cisco Unified Border Element](#)

[コンタクトセンター ソリューション向け仮想 CUBE](#)

**Unified Border Element としての Cisco ASR 1000 シリーズ**

Unified CVP は、次の制限がある Cisco IOS XE ソフトウェアをサポートします。

- ASR 1000 シリーズゲートウェイは VXML をサポートしません。そのため、コールの VRU レグを別の VXML ゲートウェイにルートします。コールバックの VRU レグを 発信元の ASR CUBE ゲートウェイにルートするために [発信者に送信 (Send To Originator)] 設定を CVP コールサーバに使用しないでください。スタンドアロン CVP コールを別の VXML ゲートウェイにルートします。
- Unified CVP は、ASR 1000 シリーズゲートウェイ上のグローバル Pass Thru SDP 設定をサポートしません。
- メディアフロースルーではなく、メディア フロー アラウンドの CUBE として ASR を構成する場合、サービス コールバック コールフローは機能しません。
- 通常、セッションボーダーコントローラの背後にプロキシサーバを配置します。プロキシが ASR セッションボーダーコントローラの正面にある場合は、プロキシサーバを使用して、大きなパケット SIP メッセージを受信するときに UDP から TCP アップ変換を実行します。この場合は、プロキシサーバの電源をオフにし、着信コールの接続に UDP トランスポートを使用することを確実にします。
- ASR では、次の Survivability.tcl オプションを使用することはできません。これらのオプションは、従来 POTS ダイアルピア向けです。
  - ani-dnis-split.
  - takeback-method.



- -- \*8.
  - -- hf.
  - icm-tbct.
  - digital-fxo.
- 次の Survivability.tcl オプションは、サポートされていません。
- aa-name — ASR が、CME 自動アテンドサービスをサポートしていないため、このオプションもサポートされていません。
  - standalone — ASR が VXML をサポートしていないため、このオプションもサポートされていません。
  - standalone-isntime — ASR が VXML をサポートしていないため、このオプションもサポートされていません。
- ASR の制限のため、次の機能はサポートされません。
- 再クエリで参照
  - DTMF \*8 ラベルを使用したレガシー転送接続
- ASR 1000 は、TDM トランクを終端しません。したがって、次の TDM ゲートウェイ機能は ASR 1000 に適用されません。
- SIP コールから Unified CCE に関する PSTN ゲートウェイ トランク および DS0 情報
  - SIP OPTIONS メッセージから Unified CCE を介した DS0 トランク リソースのリソースの可用性インジケータ (RAI)



**Note** ソリューションが ASR 1000 シリーズゲートウェイを使用している場合は、品質評価 (A2Q) レビューが必要です。このレビューは、Contact Center Enterprise ソリューション、ASR 1000 にアップグレードする既存のソリューションが対象です。

## Unified Border Element としての Cisco ISR

Unified CVP が ISR をサポートするには次の制限があります。

- CUBE がメディア フロー アラウンド用に構成されているため、サービス コールバック コール フローは ISR では機能しません。代わりに、メディア フロー スルー用に構成します。

## VXML ゲートウェイ設計上の考慮事項



**Note** VXML ゲートウェイの代替として Cisco Virtualized Voice Browser を使用できます。

### DTMF または ASR/TTS を使用する VXML ゲートウェイ

VXML ゲートウェイを使用すると、カスタマーは DTMF トーンまたは ASR/TTS を介して VXML ブラウザと対話できます。ゲートウェイには PSTN インターフェイスが存在しないので、音声トラフィックは、Real-time Transport Protocol (RTP) を使用して VXML ゲートウェイに送信されます。RFC 2833 は、RTP パケット内でインバンドシグナリングを使用し、DTMF トーンを送信します。DTMF または ASR および TTS を使用する VXML を使用すると、展開の規模を拡大し、数百の VXML セッションをサポートできます。

ブランチオフィストポロジでは、別の PSTN ゲートウェイと VXML ゲートウェイを展開して、冗長性の追加レイヤーを提供し、さらにブランチフィスに Survivable Remote Site Telephony (SRST) のサポートを提供します。

### VXML Over HTTP

VXML サーバと音声ブラウザは、VXML over HTTP を使用した要求—応答周期で通信します。Uniform Resource 識別子 (URI) は、VXML ドキュメントをリンクします。ユーザは HTML に似た Web フォームで情報を入力します。フォームには、ユーザが編集してサーバに送り返した入力フィールドが含まれています。

音声ブラウザのリソースは VXML サーバ上にあります。これらのリソースは、VXML ファイル、デジタルオーディオ、音声認識用の命令 (文法)、およびスクリプトです。VXML ブラウザは、音声アプリケーションとの通信プロセスごとに、VXML サーバへの要求として開始します。VXML ファイルには、予測される単語やフレーズを指定する文法が含まれています。リンクには、音声アプリケーションの URL が含まれています。ブラウザは、音声入力と文法の 1 つとの一致が復活するとその URL に接続されます。



**Note** CVP インストーラは、CVP コールサーバ、CVP VXML サーバ、メディアサーバをまとめてインストールします。

VXML サーバのパフォーマンスを決定するには、次の点が重要です。

- Web アプリケーション サーバと音声ゲートウェイ間の QoS およびネットワーク帯域幅
- VXML サーバのパフォーマンス
- 録音済み音声と音声合成 (TTS) の使用

音声ユーザ インターフェイス アプリケーションは、可能であれば録音済みオーディオ ファイルを使用する傾向があります。TTS よりも優れている録音済みオーディオサウンド。ダウンロード時間やブラウザの解釈に影響しない事前録音済みのオーディオファイルの品質を選択します。録音は 8 ビットの  $\mu$ -law 8 kHz フォーマットで行います。

- オーディオファイルのキャッシング

音声ゲートウェイが音声コンテンツをキャッシュするように構成します。キャッシングによって、メディアソースからファイルをダウンロードする際の遅延を回避できます。

- 文法の使用

音声アプリケーションで問題は、正式なユーザビリティテスト、または使用中のアプリケーションの観察によってのみ検知できます。音声認識の精度が低いのは、音声アプリケーションでは一般的です。主な原因としては不十分な文法実装が挙げられます。ユーザが単語の発音を間違えるか、文法の設計者が予想しなかったことを話すと、認識プログラムは入力と文法を照合できません。文法に関するもう1つの一般的な問題は、エントリの識別が難しいことが挙げられます。これらのエントリがあると、間違えて認識された入力そして、VXMLサーバのパフォーマンスの低下の原因となります。認識の精度を向上させるには、そのパフォーマンスを分析し、文法の精度を調整します。

## 分散型ゲートウェイ

以下の項では、各種音声ゲートウェイと分散型展開におけるそれらの影響について説明します。

### Related Topics

[拡張位置のコールアドミッション制御機能](#)

### ブランチでのイングリッシュまたはエグレス音声ゲートウェイ

ソリューションは、ブランチオフィのイングリッシュ音声ゲートウェイを使用して、集中型または非地理的な番号ではなく、ローカルのディレクトリ番号によってアクセスを発信者に提供します。この機能は、複数国にまたがったソリューションにとって重要です。

ソリューションは、ローカライズされた PSTN ブレックアウトのために、またはソリューションに統合された分散化 TDM プラットフォームのために、ブランチでイングリッシュゲートウェイを使用できます。

ソリューションの別のコンポーネントは中央に位置しています。WAN リンクは、各ブランチオフィスからメインサイトにデータ接続を提供します。

### ブランチでのイングリッシュまたは VXML ゲートウェイ

ブランチで実行される他の音声サービスは、イングリッシュゲートウェイまたは VXML ゲートウェイに影響を与える可能性があります。たとえば、ブランチがリモートの Unified CM サイトの場合、Unified CM は ACD エージェント回線と非エージェント回線の両方をサポートできます。この展開では、非エージェント回線からの新しい連絡先およびトラフィックに PSTN ゲートウェイを使用します。ブランチで VXML と音声ゲートウェイが別々のデバイス上で機能する場合は、ダイヤルプランがローカル VXML リソースに VRU レグを送信することを確実にします。これは、Unified CVP コールサーバ `settransferlabel` ラベルが併置されている VXML および音声ゲートウェイ構成のみに適用されるからです。

## 併置された VXML サーバと VXML ゲートウェイ

ソリューションでは、すべてのゲートウェイとサーバを中央集中型にするか、各サイトに一連の Unified CVP VXML サーバと VXML ゲートウェイを同じ場所に分散できます。

併置には以下の利点があります。

- WAN の機能停止がセルフサービス アプリケーションに影響を与える可能性はありません。
- VXML は WAN 帯域幅を使用します。

併置には以下の欠点があります。

- 複製されたブランチオフィスには、追加の Unified CVP VXML サーバが必要です。
- 複数の Unified CVP VXML サーバにアプリケーションを展開すると、オーバーヘッドが大きくなります。

## Centralized VXML サーバを使用したブランチにあるゲートウェイ

中央集中型 VXML の利点は次のとおりです。

- 管理とレポート生成が一元化されます。
- ブランチオフィスは、Unified CVP VXML サーバのキャパシティを共有できます。

中央集中型 VXML の欠点は次のとおりです。

- 拠点の存続可能性が制限されます。
- XML over HTTP トラフィックに対してより多くの WAN 帯域幅が必要です。

## Contact Center Enterprise ソリューションのローカルトランク

Contact Center Enterprise ソリューションには、カスタマーオンプレミスのローカルトランクに2つのオプションがあります。

- Cisco Unified Border Element — カスタマーオンプレミスの企業
- カスタマーオンプレミスの TDM ゲートウェイ



### Note

トランスコーディング リソースは、ローカルのカスタマー オンプレミス ゲートウェイから自動的に選ばれるわけではありません。

## CVP 設計上の考慮事項

### CVP コールサーバ設計上の考慮事項

#### ルーティングの Unified CVP アルゴリズム

ダイヤルプランとコールルーティングを設定する場合、Unified CVP 機能を組み合わせて必要なエフェクトを実現できます。たとえば、Location Based CAC、SigDigits、SendToOriginator、LocalSRV および Use Outbound Proxy を使用できます。

CVP はこのプロセスを使用して、Unified CVP からのアウトバウンドコールに対して接続先 SIP URI を作成します。ここでは、Unified CCE からのラベルを含む CONNECT メッセージ (VXML ゲートウェイ、Unified CM など) について説明します。また、呼び出し音サービス、録音サーバ、エラーメッセージ再生サービスにも適用されます。



**Note** このプロセスでは、SIP サブシステムを使用した通話についてのみ説明します。これには、音声のみと基本的なビデオ SIP 通話が含まれます。

CVP は、併置する IOS VXML ゲートウェイとインテリジェント音声ゲートウェイ専用の SendToOriginator アルゴリズムをサポートします。シスコ仮想化音声ブラウザ (VVB) は、アルゴリズムをサポートしません。これは、シスコ VVB を使用する際にゲートウェイを併置できないからです。

Unified CCE ラベルを含むアウトバウンドコール用の接続先 SIP URI ホスト部を作成するプロセスは、次のとおりです。

1. プロセスは、Unified CCE ラベルで開始します。Unified CCE サブシステムはすでに、Location siteID を挿入済み場合があります。SigDigits を使用している場合は、先頭に追加されます。ネットワーク VRU ラベルの場合、Unified CCE サブシステムは、接頭辞および関連 ID にラベルとして渡されます。
2. SendtoOriginator が Unified CCE ラベルと一致する場合、Unified CVP アルゴリズムは、発信者の IP またはホスト名 (インテリジェント音声ゲートウェイ) を使用します。ゲートウェイは、SIP URI を返します。

SendtoOriginator の設定は、Cisco インテリジェント音声ゲートウェイの発信者のみに適用されます (SIP UserAgent ヘッダーが選択されています)。Cisco IOS 以外のゲートウェイには、Cisco IOS VXML ゲートウェイが使用する CVP ブートストラップサービスがありません。

3. [アウトバウンドプロキシを使用 (use outbound proxy)] が設定されている場合、プロキシのホストを使用して SIP URI を返します。
4. ローカルの静的ルートがラベルで検出された場合、SIP URI を返します。



**Note** ローカルの静的ルートが見つからない場合、アルゴリズムは RouteNotFoundException の例外をスローします。

SIP サブシステムを使用したコールについては、次の点を検討してください。

- 複雑なダイヤル番号の文字列を回避するためには、Locations CAC siteID で SigDigits 機能を使用しないでください。
- サーバグループ FQDN（ローカル SRV FQDN）としてアウトバウンドプロキシ FQDN を指定できます。また、サーバグループ FQDN としてローカルの静的ルート接続先を構成できます。
- 着信音 DN（91919191）、録音サーバ（93939393）、およびエラーメッセージサービス（92929292）は、同じプロセスに従います。
- SendtoOriginator は、REFER ラベルで機能します。
- REFER ラベルは、SigDigits 設定で動作します。

## CVP VXML サーバ設計上の考慮事項

VXML アプリケーションが複雑化すると、VXML サーバのパフォーマンスに影響を与えます。許容範囲の VXML サーバのパフォーマンスを維持するために、メモリークとアプリケーションのデッドロックについてアプリケーションの負荷テストを行います。

## CVP メディアサーバ設計に関する検討事項

### 音声プロンプトの展開と管理

次の方法で音声プロンプトを導入できます。

- ローカル ファイル システム

音声プロンプトファイルをローカルシステムに保存します。オーディオによる指示の取得は帯域幅を使用しません。このメソッドでは、音声ブラウザは、プロンプト再生のために音声ファイルを取得する必要が無いので WAN 帯域幅に影響はありません。ただし、プロンプトを変更するには、すべての音声ブラウザで変更します。

- **IOS VXML ゲートウェイ** — プロンプトは、フラッシュメモリで導入されます。

IOS VXML ゲートウェイは、VXML ゲートウェイまたは PSTN ゲートウェイのどちらかであり、同じ場所にあるイングレス音声ゲートウェイと VXML ゲートウェイを持ちます。WAN がダウンした場合のエラーメッセージやメッセージなど、重要なプロンプトだけをここに保存します。

G.711  $\mu$ -law フォーマットで録音した場合、一般的なプロンプトのサイズは 10 ~ 15 KB です。これらのゲートウェイの場合、プロンプトの数とそのサイズを分解して、フラッシュメモリのサイズを調整します。Cisco IOS イメージを保存するためのスペースも残します。

- **Cisco VVB** — ローカルファイルシステムにプロンプトをアップロードします。

Cisco VVB には、組み込みの CVP プロンプトが含まれています。エラー トーン デフォルトプロンプトは、**Cisco VVB 管理者コンソール** で変更できます。

- メディア サーバ

ローカルの各音声ブラウザが適切に設定されている場合、プロンプトのサイズに応じて、多くのプロンプトをキャッシュできます。Cisco VVB は最大 512 MB、Cisco IOS は最大 100 MB キャッシュできます。メディアサーバがメディア ファイルに適切に配信されているかどうかをテストするには、ブラウザのメディアサーバでプロンプトの URL を指定します。お使いの Web ブラウザは、認証なしで .wav ファイルをダウンロードし、再生します。

メディアサーバ導入の設計は、次の要因によって異なります。

- 各ゲートウェイが再生するメディアファイルの数
- ゲートウェイとメディアサーバ間のネットワーク接続
- メディアファイルを変更する頻度

### 多数のメディアファイル設計に関する検討事項

ゲートウェイが顧客に対してさまざまなメディアファイルを再生する場合、ゲートウェイに、すべてのメディアファイルをキャッシュできるスペースがない場合があります。

たとえば、エージェントが多い企業があるとします。各エージェントには、それぞれエージェントグリーンディングファイルがあります。ゲートウェイのフラッシュメモリでは、それらのファイルをキャッシュすることはできません。

### 音声ブラウザを使用してメディアサーバを同じ場所に配置

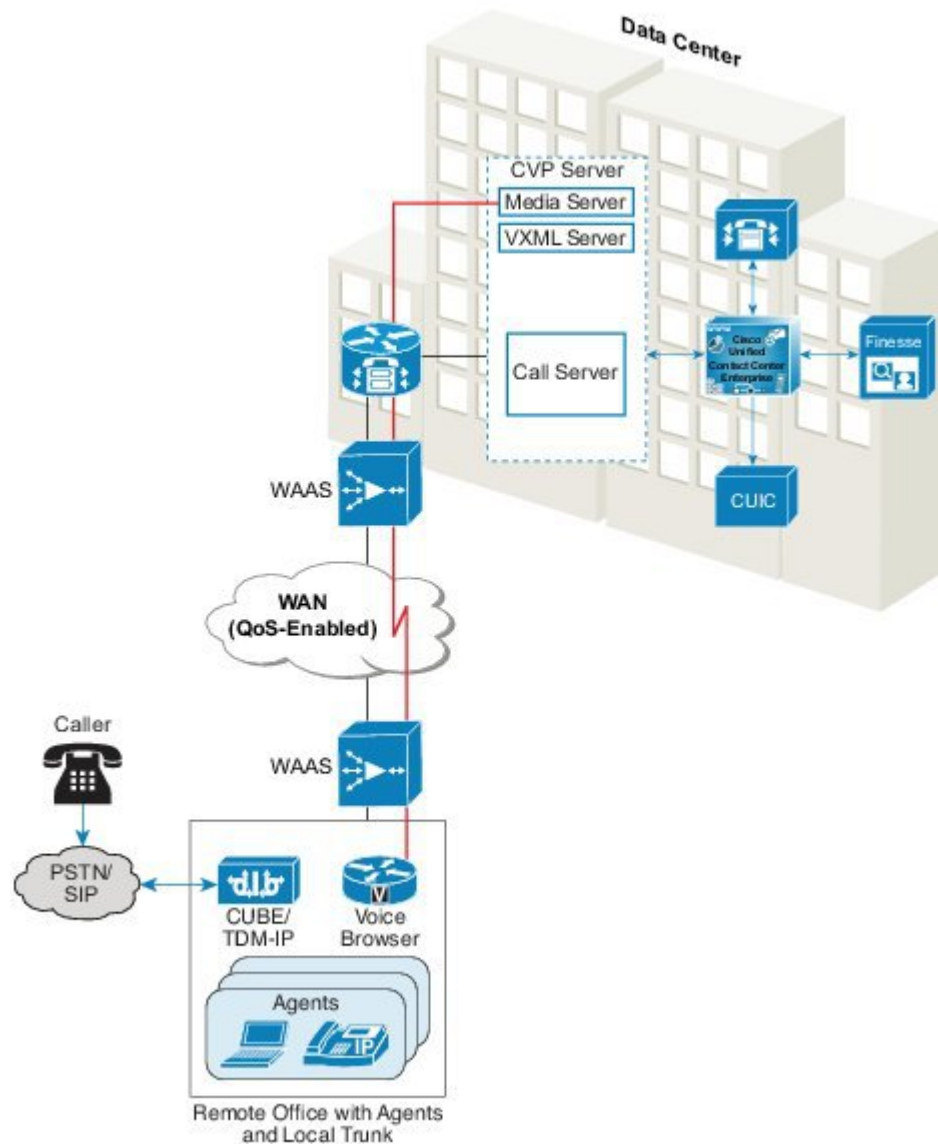
この問題の 1 つの方法は、音声ブラウザを使用してメディアサーバを場所に配置する方法です。メディアサーバと音声ブラウザを十分な帯域幅がある LAN 上で共存させる場合、プロンプトをダウンロードしても大きな遅延は発生しません。

### WAN 上に分散されたメディアサーバと音声ブラウザ

ソリューションでは、WAN 全体の音声ブラウザから分離されたメディアサーバを使用できます。

次の図は、WAN 上での分散型展開を示しています。

Figure 4: WAN 経由の分散型展開



高遅延 WAN 全体のメディアファイルを音声ブラウザにダウンロードすると、大幅な遅延が起こる場合があります。この遅延は、ユーザエクスペリエンスに大きく影響します。この遅延は、WAN 全体で転送されるメディアファイルのサイズと数に大きく影響します。Wide Area Application Services (WAAS) を使用すると、遅延を最適化できます。

#### メディアストリーミングの設計に関する検討事項

LAN 展開と WAN アクセラレータ展開の両方では次の要因を検討します。

- 最大ネットワーク ラウンドトリップ時間 (RTT) の遅延は、200 ミリ秒です。

たとえば、一括管理ファイル転送 (BAFT) を使用した CVP オペレーションコンソールからイングリセスまたは VXML ゲートウェイへのファイル転送など。



- メディアフォークを使用したビデオの追加オーバーヘッドなしの各ゲートウェイでサポートされているストリーミングセッションの最大数。

次の表は、さまざまな展開で使用する優先メディアストリーミング方法を示します。

シナリオ	変更の頻度	LAN 上	WAN 上
少数のファイル	稀	Cached	Cached
少数のファイル	よく利用する	ストリーミング済みまたはキャッシュ済み	WAAS でストリーミング
多数のファイル	稀	ストリーミング済み	WAAS でストリーミング
多数のファイル	よく利用する	ストリーミング済み	WAAS でストリーミング



**Note** Cisco VVB では、メディアストリーミング機能はサポートされていません。

## メディアファイルの展開の設計に関する検討事項

### TCP ソケットの保持はサポートされていません

Unified CVP は TCP ソケットの永続性をサポートしません。

### WAN 高速化サポート

Wide Area Application Services (WAAS) システムは、Wide Area Application Engine (WAEs) と呼ばれるデバイスの一式です。ネットワーク上の TCP トラフィックを最適化するために、WAEs が協働します。Cisco WANAS は、TCP の最適化技術とアプリケーションアクセラレーション機能を使用して、WAN を経由したトラフィックの転送に関する最も一般的な課題を解決します。VXM ゲートウェイ側のネットワークの周辺に展開すると、Cisco WAAS が次の機能を実行します。

- トラフィックを最適化するために TCP ヘッダーを変更します。
- ローカルに配置された大規模な HTTP キャッシュとして機能します。
- 圧縮アルゴリズムを使用してトラフィックをさらに減らします。
- データ冗長性排除 (DRE) 技術によりトラフィックを削減します。

Cisco WAAS は、すべてのデータが強制的に Cisco WAAS にパースルーするインラインモードで展開されます。

### IOS ゲートウェイ上のメディアファイルの展開

#### 非ストリーミングおよびストリーミングモード

## メディアファイルキャッシュタイプ

非ストリーミングモードでは、Media Player がプロンプトの再生を開始する前に、VXML ゲートウェイは、HTTP サーバから音声ファイル全体をダウンロードします。これにより、発信者の遅延が発生します。小規模ファイルの場合、遅延は数ミリ秒です。キャッシングまたはストリーミングモードのいずれかを使用すると、サイズの大きいファイルの遅延を回避できます。

ストリーミングモードでは、Media Player は HTTP サーバから発信者にオーディオをメディアチャックでストリーミングします。Media Player は、最初のチャックを受信するとプロンプトの再生を開始します。ストリーミングモードでは、オーディオによる指示のサイズによって、発信者に遅延が追加されることはありません。ただし、チャックのメディアファイルをフェッチするための前後の対話によりパフォーマンスが低下する場合があります。

メモリ内の音声ファイルをキャッシュすると、HTTP サーバから直接ストリーミングする大きなファイルの利点が少なくなります。

## メディアファイルキャッシュタイプ

メディアファイルを保存するキャッシュは、2 種類あります。

### HTTP Client キャッシュ

非ストリーミングモードでは、HTTP Client キャッシュにメディアファイル全体が保存されます。ストリーミングモードでは、HTTP Client キャッシュに、最初のチャックのメディアファイルが保存されます。HTTP Client キャッシュには、どちらのモードでも 100 MB のプロンプトが保存されます。構成されている HTTP Client のメモリファイルサイズよりも大きいファイルはキャッシュされません。

### VRU メディア プレーヤー キャッシュ

非ストリーミングモードでは、VRU メディア プレーヤー キャッシュは使用しません。ストリーミングの役割では、VRU メディア プレーヤー キャッシュには、ファイルのすべてのサイズが格納されます。非ストリーミングモードでは、VRU メディア プレーヤー キャッシュに 16 MB が保存されます。ストリーミングモードでは、32 MB を保存できます。

## クエリ URL のキャッシング

クエリは、疑問符 (?) の後に 1 つ以上の **name=value** 属性ペアが続く URL です。Unified CVP VXML サーバは、動的 VXML ページの生成時にクエリ URL を使用します。各コールは一意的なもので、クエリ URL から取得したデータは、キャッシュメモリを使い古す場合があります。クエリ URL にアカウント番号や PIN などの情報を含め得る場合があるので、データはセキュリティリスクに該当する場合があります。

Cisco IOS は、デフォルトでクエリ URL キャッシングを無効にします。無効になっていることを確認するには、Cisco IOS で **show run** コマンドを入力し、次の Cisco IOS コマンドが表示されていないことを確認します。

```
Gateway configuration: http client cache query
```

## Cisco VVB でのメディアファイルの展開

Cisco VVB には HTTP クライアントが含まれています。クライアントは、VXML ドキュメント、オーディオファイル、その他のファイルリソースをフェッチし、フラッシュメモリに格納します。

キャッシングプロパティは、VXML リソース、オーディオによる指示、文法ファイル、およびスクリプトファイルに関連付けられます。

デフォルトでは、クエリ URL はキャッシュされません。クエリは、疑問符 (?) の後に 1 つ以上の **name=value** 属性ペアが続く URL です。

## キャッシュ エージング

HTTP Client は、キャッシュされた各エントリの鮮度によってそのキャッシュを管理します。キャッシュされたエントリが新しいのか古いのかは、[経過期間 (Age)] および [FreshTime] によって異なります。[経過期間 (Age)] は、サーバから最後にファイルがダウンロードされてからの経過時間です。[FreshTime] は、ファイルが最後にダウンロードされてから HTTP Client キャッシュにファイルがとどまると想定される時間です。

いくつかの変数は、サーバからの HTTP メッセージヘッダーやキャッシュ更新値などのファイルの [FreshTime] に影響します。

ファイルの [FreshTime] は、次のシーケンスで決定されます。

1. ダウンロード時に、ファイルに Cache Control: max-age ヘッダーがある HTTP メッセージヘッダーがある場合、[FreshTime] は、max-age となります。
2. ステップ 1 を適用しない場合、[FreshTime] は、Expires ヘッダーから Date ヘッダーを引き算した値になります。



### Note

HTTP/1.1 仕様である、*RFC 2616* (ハイパーテキストトランスポートプロトコル) は、Cache Control: max-age ヘッダーまたは Expires ヘッダーのどちらかを使用することを推奨しています。

3. 前述のヘッダーが既存しない場合、FreshTime は、Date ヘッダーの 10% 分の値から、最終更新日ヘッダーを差し引いた値になります。

Cisco IOS VXML ゲートウェイの場合、FreshTime の値を、http client cache refresh コマンドと一緒にファイルに割り当てることができます。ただし、その値が適用されるのは、前のシーケンスで値の設定に失敗した場合のみです。

古いファイルは、必要な場合のみ更新されます。古くキャッシュされたエントリは、次の条件に基づいて新しいファイルのスペースが削除されるまでキャッシュ内に残ります。

- キャッシュされたエントリが古くなった。
- 更新カウントがゼロ (0) である。つまり、キャッシュされたエントリが使用されていない。
- キャッシュには、別のエントリのスペースを創るためのメモリスペースが必要です。

[経過時間 (Age)] が、[FreshTime] を超過し、ファイルを再生する必要がある場合、HTTP Client は、メディアサーバを使用してファイルを更新するか否かを判断します。HTTP Client は、GET リクエストをサーバに送信し、上限付き GET を使用してネットワークトラフィックへの影響を最小限に抑えます。GET 要求では、サーバに送信されるヘッダーに If-Modified-Since が含まれます。このヘッダーがあると、サーバは 304 応答コード (未修正) を返すか、ファイルが最近更新された場合は、ファイル全体を返します。[経過時間 (Age)] が、[FreshTime] を超過し、ファイルを再生する必要がある場合、HTTP Client は、メディアサーバを使用してファイルを更新するか否かを判断します。HTTP Client は、GET リクエストをサーバに送信し、上限付き GET を使用してネッ

ネットワークトラフィックへの影響を最小限に抑えます。GET 要求では、サーバに送信されるヘッダーに If-Modified-Since が含まれます。このヘッダーがあると、サーバは 304 応答コード（未修正）を返すか、ファイルが最近更新された場合は、ファイル全体を返します。

この条件付き GET は非ストリーミングモードにのみ適用されます。ストリーミングモードでは、HTTP Client は常に条件なしの GET を発行します。ストリーミングモードで各 GET が条件なしでリロードされる GET リクエストには、If-Modified-Since ヘッダーは含まれていません。

## CVP コールサーバの設計に関する考慮事項

CVP コールサーバはレポートサービスを提供し、IBM Informix Dynamic サーバ（IDS）データベース管理システムをホスティングします。データベースのスキーマを使用すると、データベースに対してカスタムのレポートを作成できます。レポートサービス自体は、データベースの管理アクティビティおよびメンテナンスアクティビティ（バックアップや消去など）を実行しません。ただし、Unified CVP では、こうしたメンテナンス タスクに Operations Console を介してアクセスできます。

レポートサービス:

- コンタクトセンター内のセルフサービスアクティビティの履歴レポートを提供します。サービスは、コンタクトセンター マネージャーのコールアクティビティをまとめたものです。
- さまざまな VRU アプリケーション運用分析も提供できます。
- VXML サーバの IVR サービスと SIP サービスからレポートデータを受信します。Reporting サービスは、このデータを Informix データベースに変換して書き込みます。

ソリューションは、単一の複数の CVP コールサーバのいずれかを使用できます。単一のコールサーバが、必ずしもシングルポイント障害であるわけではありません。データベース管理システムは、データの安全性とセキュリティを提供します。ソリューションは、ソースコンポーネントに関する情報が永続的にバッファリングされたことが原因の一時的な機能停止に耐えることができます。

ソリューションが複数のコールサーバを使用している場合は、各 CVP コールサーバを 1 つのコールサーバにのみ関連付けできます。また、レポートは、複数の Informix データベース間で作成できません。



**Note** Unified CVP のサブコンポーネントは、マシン時間そのものを同期できません。ロギングとレポートに対して正確なタイムスタンプを保証するために、NTP などのコンポーネント間の時刻同期機能を提供します。

## CVP コールサーバの機能

CVP コールサーバを使用してソリューションを設計する際は、次の点を検討してください。

- Informix データベースのサイズは最大 100 GB です。実稼働環境では、2 GB 以下のデータベースを使用することはできません。

- コールサーバは、Analysis Manager ツールをサポートしています。Analysis Manager は、認証済みのユーザのログイン情報を使用して コールサーバを照会できます。
- コールサーバは、Unified CVP データを 15 分単位で集約します。Cisco Unified Intelligence Center は、15 分間、毎日、および毎週の間隔で、コールデータと優先パス情報を表示するテンプレートを提供しています。
- 管理プロセスのすべてのメタデータは、Ciscoadmin データベースに含まれています。このクエリは、レポートユーザの通常ビューからテーブルを削除します。
- すべてのデータベース バックアップ ファイルは、圧縮され、Reporting Server に保存されます。バックアップファイルは、**cvp\_backup\_data.gz** と呼ばれ、**cvp\_db\_backup** フォルダの %INFORMIXBACKUP% ドライブで保存されます。
- システム CLI を使用して、コールサーバ上のログファイルを一覧するリクエスト (**show log**) を作成できます。この要求には、Informix データベース サーバエンジンのログが含まれています。**show tech-support** コマンドは、これらファイルにも含まれます。
- システム CLI 内でデバッグ レベル 3 (または 0) コマンドを使用すると、デバッグのオンとオフを切り替えられます。オンにすると、このコマンドは、すべての管理手順、消去、統計、およびアグリゲータに関するトレースファイルを生成します。




---

**Note** コマンドをオンにしたら、トレースファイルはデータベースにより大きな不可をかけます。

---

- 管理手順のログデータは、毎晩 **%CVP\_HOME%\logs** フォルダに書き込まれます。
- **StartDateTime**、**EndDateTime** および **EventDateTime** のすべての値は、コールサーバテーブルで UTC で保存されます。
- SIP コールイベントの転送タイプデータおよび転送ラベルは、コールイベントテーブルに保存されます。
- 要約の消去結果が、ログテーブルに記録されます。
- 3 つの新しいスケジュール済みタスクが、コールサーバのスケジューラに追加されました。
  - **CVPSummary** は、要約テーブルを構築します。
  - **CVPCallArchive** は、コールバックデータをアーカイブしてコールバックデータベースのパフォーマンスを維持します。
  - **CVPLogDump** は、毎晩管理ログを抽出します。

## CVP バックアップおよびリストア

Operations Console を使用すると、データベースバックアップの日次スケジュールを設定したり、オンデマンドでデータベースバックアップを実行できます。大きな障害が発生した場合は、前回

のバックアップ時間まで手動でデータベースを復元できます。これにより、データの損失は24時間までになります。

## CVP コールスタジオの設計に関する検討事項

CVP Call Studio でアプリケーションを設計する場合は、アプリケーションを小規模で、ビジネスフローに近い状態でマッピングしてください。大きなアプリケーションでは、保守と作業が難しくなります。サブフローと独立したアプリケーションのバランスを維持します。

## Unified CVP の併置

SIP 呼制御に必要なサーバの数を計算するには、次の式を使用します。

$$(Self\ Service + Queue\ and\ Collect + Talking) / 3000, \text{ rounded up}$$

ここで、

セルフサービスは、SIP 呼制御を要求し、VXML サーバ上でアプリケーションを実行するコールの数です。

キューと収集は、SIP 呼制御を必要とするコールの数であり、コールサーバ上でのみ Microapps を使用してアプリケーションを実行します。

通話中は、エージェントのコール数です。

次の例は、VXML セッションおよび HTTP セッションだけに適用されます。

$$((3000) + (500) + 3700) / 3000 = 3 \text{ servers}$$

VXML 要件を処理するフロースルーコールにセッション ボーダー コントローラ (SBC) として CUBE を使用する場合は、例で示すサイジング情報を使用します。

フロースルーコールのみ (VXMLなし) を処理するためにセッション ボーダー コントローラ (SBC) として CUBE を使用する場合、音声アクティビティ検出 (VAD) を考慮し、[http://www.cisco.com/c/en/us/products/collateral/unified-communications/unified-border-element/order\\_guide\\_c07\\_462222.html](http://www.cisco.com/c/en/us/products/collateral/unified-communications/unified-border-element/order_guide_c07_462222.html) の『Cisco Unified Border Element Ordering Guide』に記載されているサイジング情報を参照してください。

## Contact Center Enterprise 設計上の考慮事項

Contact Center Enterprise ソフトウェアは、企業全体へのマルチチャネル コンタクトのディストリビューションを実現します。このソフトウェアは、インバウンドおよびアウトバウンドの電話、Web コラボレーション要求、Eメールメッセージ、チャット要求をサポートできます。また、地理的に離れているコンタクトセンターもサポートできます。Contact Center Enterprise ソフトウェアはオープンな標準ベースのソリューションであり、ルーティング、キューイング、モニタリング、耐障害性などの機能を備えています。



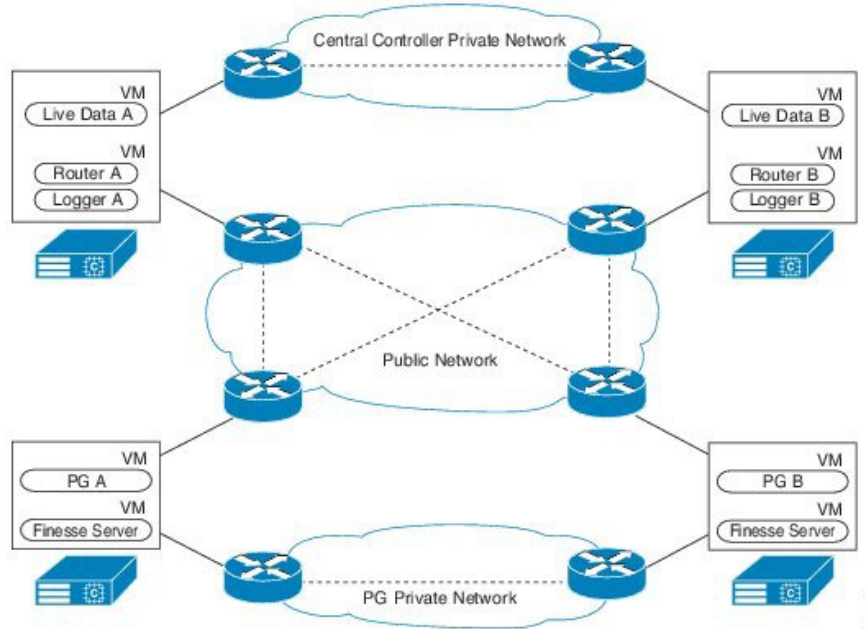
### Note

Unified CCE は、Contact Center Enterprise ソリューションのいずれかと、すべてのソリューションのコア コンポーネントのいずれかの両方を示す名前です。

## ルータの設計上の考慮事項

冗長 Unified CCE サーバを地理的に分散したり、同じ物理サイトで配置できます。実稼働の展開では、ルータと Logger は、パブリックネットワークとは分離されたプライベートネットワーク経由で接続する必要があります。

Figure 5: セントラルコントローラの高可用性の設計



**Note** セントラルコントローラと PG には同じプライベート ネットワーク パスを使用できます。

## Logger の設計上の考慮事項

Logger データベースの設計は、通常 2 週間分のデータが保持されています。この期間は、データが AW-HDS-DDS に複製されるのに十分な時間を与えます。

この Logger は、ルータとして同じプライベートネットワーク パスを使用します。

## 周辺機器ゲートウェイ設計上の考慮事項

### エージェント周辺機器ゲートウェイ設計上の考慮事項

エージェント PG は、CTI Manager を介して Unified CM クラスタと通信します。エージェント PG は、クラスタ内の任意の場所でエージェントの電話機と CTI ルートポイントを制御できます。エージェント PG は、クラスタ内の Unified CM サブスクリバ上で CTI Manager に登録します。CTI Manager は、クラスタに対して PG からのすべての JTAPI リクエストを受け入れます。PG が別のサブスクリバの電話機またはルートポイントをリクエストすると、CTI Manager はそのリクエストを別のサブスクリバに転送します。

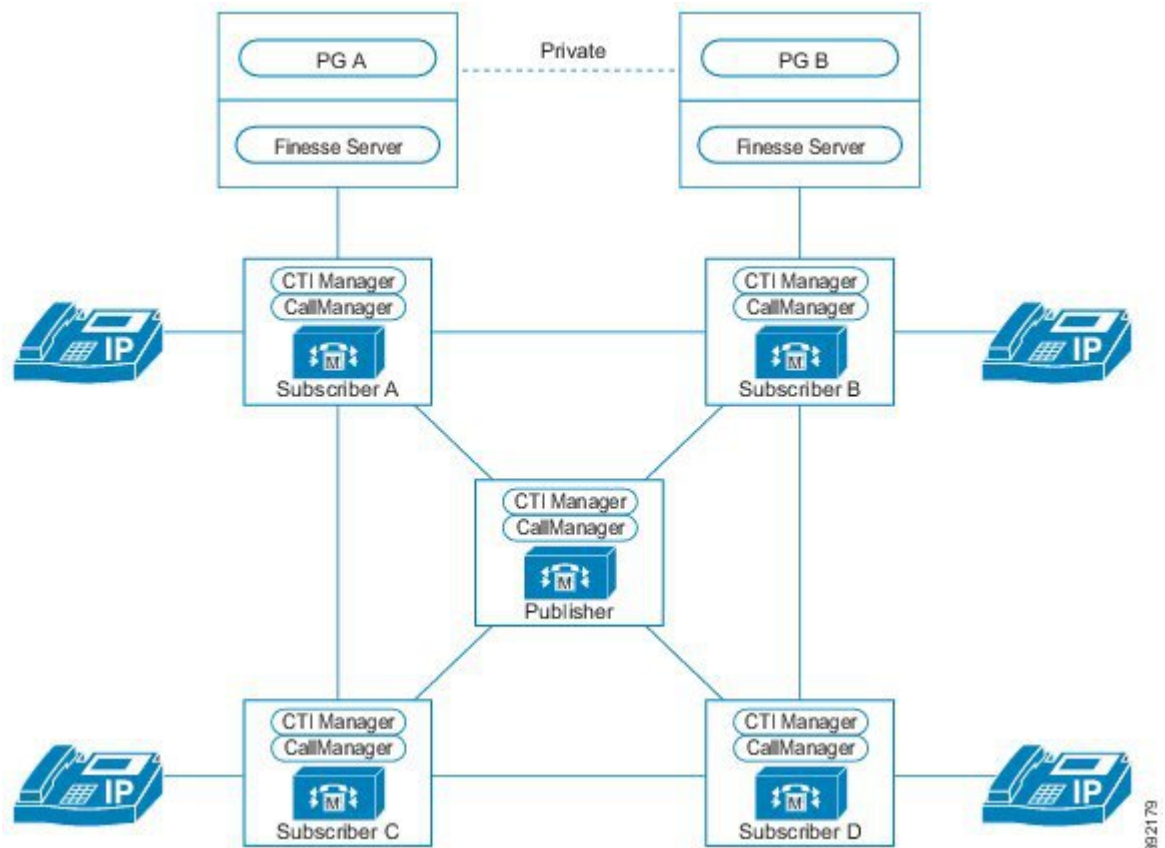


**Note** エージェント PG は、Unified CM PIM を含む PG です。これは、Unified CM PG と呼ばれる場合があります。非リファレンス設計でのみ、エージェント PG は汎用 PG である場合があります。

フォールトトレランス設計は、冗長構成でのエージェント PG 展開します。これは、PG のみが単一 CTI Manager を介してクラスタに接続するからです。その CTI Manager に障害が発生すると、PG は、クラスタと通信できなくなります。冗長 PG は、クラスタの異なるサブスライバ上の異なる CTI Manager を介して二次的な経路を提供します。

高可用性クラスタの最小設計は、1つのパブリッシャと2つのサブスライバです。プライマリサブスライバに障害が発生した場合、デバイスはクラスタのパブリッシャではなく、セカンダリサブスライバにリホームされます。

Figure 6: Unified CM クラスタの高可用性の設計



冗長 PG は、パブリックネットワークとは分離されたプライベートネットワークを介して同期を維持します。2台の PG サーバが地理的に分散されている場合は、プライベートネットワーク用に別個の WAN 接続を使用します。ネットワーク内のシングルポイント障害を回避するために、パブリックネットワークに対して同じ回路またはネットワークギアを使用しないでください。

エージェント PG 内では、JTAPI ゲートウェイおよび Unified CM PIM が、クラスタへの接続を管理します。JTAPI ゲートウェイは、Jabber ソケット接続プロトコルおよび PIM および CTI Manager



間のメッセージを処理します。PIM は、Unified CCE、JTAPI ゲートウェイおよびクラスタ間のインターフェイスを管理します。クラスタからのルートリクエストを監視および処理する特定のオブジェクトをリクエストします。PG は、ノード管理プロセスとして JTAPI ゲートウェイと PIM を自動的に開始します。PG が監視および処理をして、障害が発生した場合は、自動的に再起動します。

両方の冗長エージェント PG からの JTAPI サービスは、初期化後に CTI Manager にサインインします。エージェント PG-A がプライマリ CTI Manager にサインインし、エージェント PG B がセカンダリ CTI Manager にサインインします。ペアになっている 1 つの PG のみが、電話機と CTI ルートポイントを積極的に登録し、監視します。冗長 PG は、ホットスタンバイモードのみで実行されます。冗長 PG はセカンダリ CTI Manager にサインインし、インターフェイスを初期化して、フェールオーバーで使用できるようにします。この取り決めにより、フェールオーバーの時間が大幅に短縮されます。

システムが起動すると、最初に Router サーバに接続された PG とリクエスト構成情報が、アクティブな PG になります。ルータは、接続が最適な PG がアクティブになることを確認します。「サイド A」と「サイド B」の名目上の指定することで、どの PG がアクティブになるかへの影響はありません。プライベートリンクの障害による PG のフェールオーバー中、重みづけメカニズムは、どの PG をアクティブにするかを選択し、コンタクトセンターへの影響を最小に抑えます。

PIM が運用可能になる前に、コールが CTI ルートポイントに到着した場合、リカバリ回数を設定しない限りそのコールは失敗し続けます。ルートポイントの [未登録時のコール転送 (Call Forward on Unregistered)] または [障害時のコール転送 (Call Forward on Failure)] 設定にリカバリ回数を指定します。たとえば、[自動応答 (Auto Attendant)] の Cisco Unity 音声メールシステムに対してリカバリ回数を設定できます。

**Note**

別のパーティションの別の CTI ルートポイントでの CTI ルートポイントの DN は使用できません。DN がすべてのパーティション上のすべての CTI ルートポイントで一意であることを確認します。

### アクティブ PG シャットダウン

実稼働環境でアクティブな周辺機器ゲートウェイがシャットダウンしないようにします。これにより、反対側に接続してアクティブになる間、1 分以上のサービスの中断が発生します。中断の長さは、構成のサイズと周辺機器の種類によって異なります。たとえば、VRU 周辺機器は、通常より短い時間しかかかりません。VRU の別のサイドでは、再アクティブ化まで 30 秒以下を要する場合があります。

### 音声応答設備の周辺機器ゲートウェイ設計上の考慮事項

標準規格の 3 つの PG モデルでは、VRU PG にはサイド A とサイド B にある CVP サーバに 1:1 ペアリングをする 2 台の PIM が含まれています。

### メディアリソース周辺機器ゲートウェイ設計上の考慮事項

標準規格 3 台の PG モデルでは、MR PG に次の機能をサポートする PIM が含まれます。

- アウトバウンド オプション
- ビジネス チャットおよび E メール
- Customer Collaboration Platform— この PIM は、タスクルーティングとエージェントリクエストを処理します。
- サードパーティ製品との統合

## Administration & Data サーバ設計上の考慮事項

### リファレンス設計ごとの Administration & Data サーバ制限

各 Logger に対してたくさんの Administration & Data サーバを展開できます。

**Table 2: Logger ごとの Administration & Data サーバ展開制限**

各 Logger 側のコンポーネント	2000 エージェント	4000 エージェント	12,000 エージェント
AW-HDS-DDS	各サイドに 1 つ、コアコンポーネントと同じサーバにインストールされます。	サイドごとに 2 つ	NA
HDS-DDS	該当なし	該当なし	サイドごとに 1 つ
AW-HDS	オプションで、コアコンポーネントとは別のサーバにインストールされた、各サイドごとに 1 つの AW-HDS または AW-HDS-DDS のいずれか	NA	各サイドごとに 3 つ
リアルタイムディストリビュータのみ <sup>1</sup>	サイドごとに 2 つ	サイドごとに 2 つ	各サイドごとに 5 つ

<sup>1</sup> この AW は構成専用です。リファレンス設計レイアウトに表示されているサーバからインストールします。



**Note** 各リアルタイムディストリビュータは 64 人のユーザをサポートできます。

## Live Data サーバ設計上の考慮事項

### ライブデータ構成によるクライアントのレポート

2000 エージェントリファレンス設計にはライブデータの併置構成を使用します。スタンドアロン Live Data サーバを使用するソリューションの場合、Unified CCE Logger 展開に対して通常、小規

模の Live Data 展開構成を使用します。通常は、個別のルータおよび Logger を使用して大規模の Live Data 展開構成を使用します。



**Note** 標準規格の Cisco Finess エージェントデスクトップには、ライブデータガジェットが含まれます。

## Cisco Virtualized Voice Browser の設計上の考慮事項

ソリューションに必要な仮想化音声ブラウザは、ソリューションが VXML ゲートウェイで必要とする VRU ポートに応じて異なります。ソリューションに必要な SIP セッションの数に応じた Cisco VVB をインストールしてください。以下の表に、Cisco VVB による機能サポートを示します。

プラットフォームまたは機能	Cisco Virtualized Voice Browser に関する考慮事項
音声コーデック	G711
コールフロー	スタンドアロンコールフロー、およびコール存続可能性を備えた包括的コールフローがサポートされます。
ASR/TTS	サポート対象
サービス コールバック	サポート対象
HTTP	サポート対象
HTTPS	サポート対象
ローカル プロンプト	サポート対象
ローカル ホスト名の解決	サポート対象
MRCP v1 および v2	サポート対象
VXML 2.0 および 2.1	サポート対象
RTSP ストリーミング	未サポート
ビデオ	未サポート

## Unified Communications Manager の設計上の考慮事項



### Note

リファレンス設計のレイアウトでは 7500 ユーザの Unified CM OVA を使用しており、サブスクライバの冗長ペアごとに 2000 の Contact Center Enterprise エージェントがサポートされます。別の Unified CM OVA を使用する場合は、リファレンス設計のレイアウト内のサーバからクラスタを移動させるか、仕様ベースのハードウェアポリシーに従ってください。仕様ベースのポリシーの詳細については、[http://www.cisco.com/c/dam/en/us/td/docs/voice\\_ip\\_comm/uc\\_system/virtualization/cisco-collaboration-virtualization.html](http://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/uc_system/virtualization/cisco-collaboration-virtualization.html) でソリューションに応じた *Cisco Collaboration Virtualization* のページを参照してください。

Cisco Unified Communications Manager (Unified CM) は、Unified CVP から渡されたコールを Unified CCE で選択されたエージェントに接続します。Unified CVP は、SIP を使用する Unified CCE エージェント電話またはデスクトップに発信者を転送します。Unified CVP コールサーバは、Unified CCE からエージェントラベルを受信し、そのコールを SIP プロキシを使用してルーティングします。コールはクラスタ内の適切な Unified CM サブスクライバに送信され、発信者がエージェントに接続されます。コールサーバがコールシグナリングの代わりになり、転送完了後、コールシグナリングパスに留まります。ただし、RTP ストリームは、発信元ゲートウェイから電話に直接流れます。

すべての Contact Center Enterprise ソリューションは、冗長 Unified CM、Unified CCE、Unified CVP のコンポーネントを使用します。冗長性のために、ソリューションでコアシステムの半分が失われることがあります。ソリューションは引き続き機能します。そのような場合、ソリューションは、まだ動作可能なコンポーネント上の VRU セッションまたはエージェントに、Unified CVP を介してコールを再ルーティングすることによりコールを処理します。可能な場合は、Unified CM パブリッシャでデバイス、コール処理、CTI Manager サービスが実行されないように、Unified CCE を展開してください。

自動フェールオーバーとリカバリを有効にするには、冗長コンポーネントペアをプライベートネットワークパスを介して相互接続します。コンポーネントは、障害検出に TCP ハートビートメッセージを使用します。Unified CM は、フェールオーバーとリカバリにクラスタ設計を使用します。各クラスタには Unified CM パブリッシャと複数の UM サブスクライバが含まれています。エージェントの電話とコンピュータはプライマリターゲットに登録されますが、プライマリで障害が発生した場合は、バックアップターゲットに自動的に再登録されます。

Contact Center Enterprise ソリューションの Unified CM クラスタを設定するには、以下の手順を実行します。

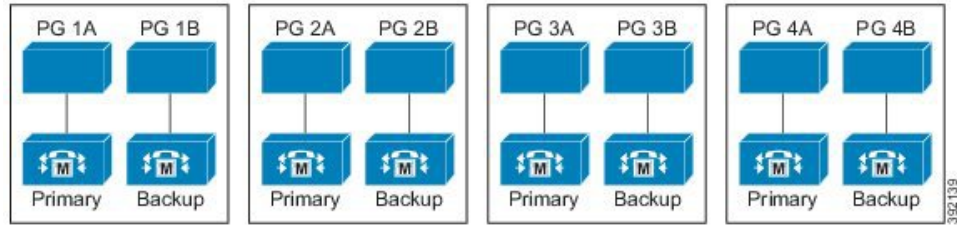
- Unified CM で SIP トランクを設定します。
- エージェントラベルを設定するときは、どのデバイスがルーティングクライアントかを考慮します。ラベルが Unified CM に直接返される場合は、Unified CM がルーティングクライアントになります。ラベルが Unified CVP に送信される場合は、Unified CVP スイッチレグコールサーバのそれぞれにラベルを関連付けます。

## エージェント PG への Unified CM 接続

次の方法で、Agent PG を展開すると Unified Communications Manager クラスタに接続できます。

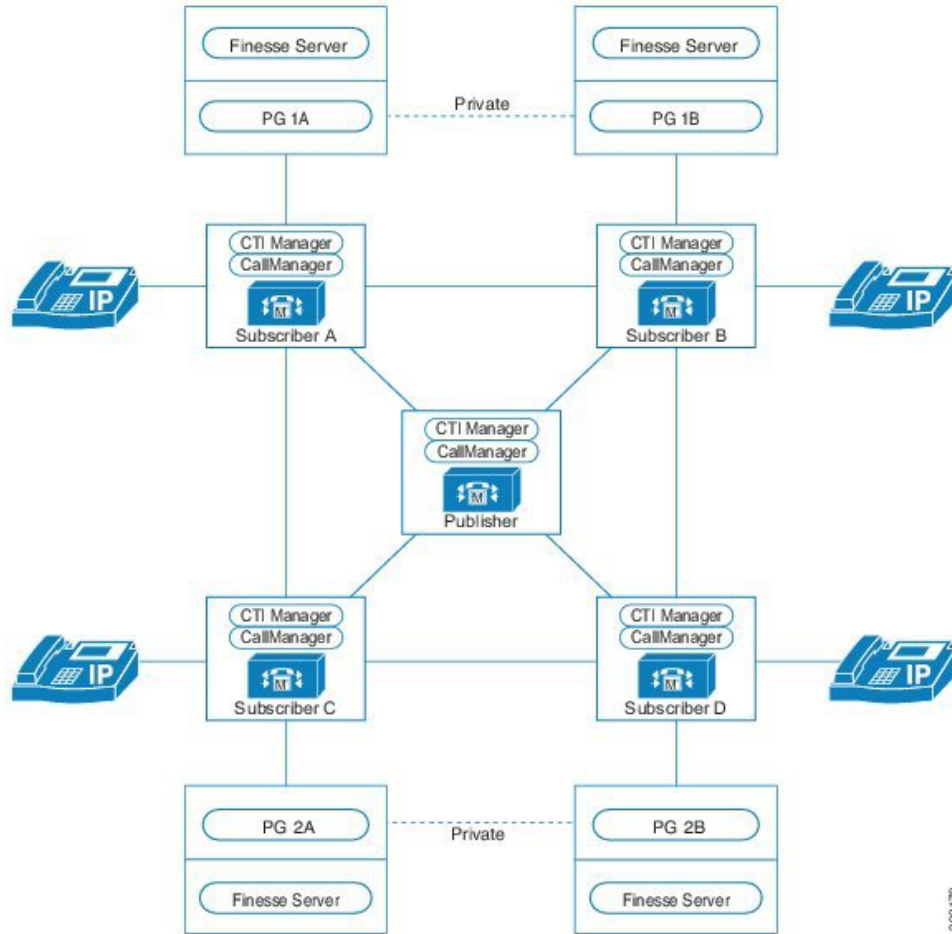
- サブスライバの各ペアにエージェント PG を導入します。各サブスライバは、CTI Manager サービスを実行します。各エージェント PG は、対応するサブスライバペア上で実行されている CTI Manager に接続します。次の図は、4 つのプライマリサブスライバが必要で、4 つのバックアップサブスライバが導入され、1:1 の冗長性を提供する例を示しています。

Figure 7: クラスタ内のサブスライバの各ペアのエージェント PG の導入



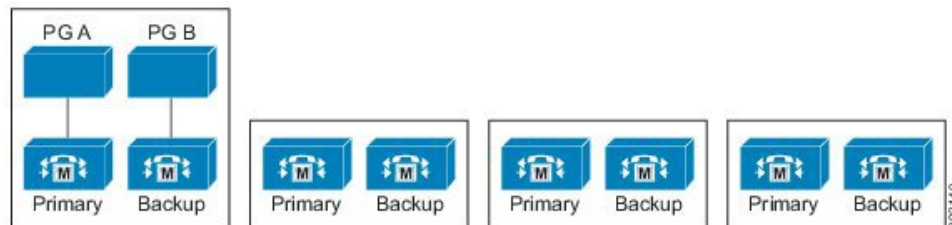
次の図は、2つのエージェント PG ペアを含むソリューションのコンポーネントと4つのサブスライバを持つクラスタ間の接続を示しています。

Figure 8: Unified CM クラスタ用の 2つのエージェント PG ペア



- クラスタ全体に対して1つのエージェント PG を導入します。このタイプの導入では、CTI Manager を実行している1ペアのサブスクリバが必要です。CTI Manager サービスを実行しているサブスクリバを含む、すべてのサブスクリバ間でエージェントの電話機の登録を分散します。次の図は、4つのプライマリサブスクリバが必要で、4つのバックアップサブスクリバを導入して1:1の冗長性を提供する例を示しています。

Figure 9: クラスタ全体に対する単一エージェント PG の導入

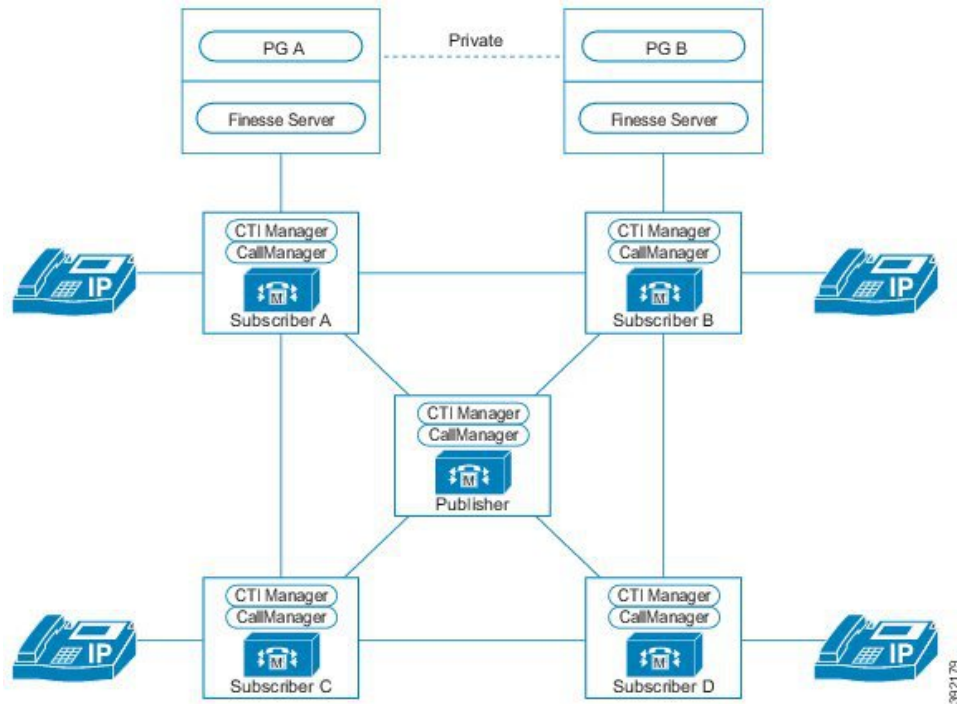




**Note** クラスタがバックオフィス電話機とエージェント電話機の両方をサポートしている場合は、このオプションを使用します。

次の図は、2つのエージェント PG ペアを含むソリューションのコンポーネントと4つのサブスライバを持つクラスタ間の接続を示しています。

**Figure 10: Unified CM クラスタ全体に対する単一エージェント PG ペア**



このモデルでは、PGのサーバ数が減ります。もう1つの利点は、クラスタ全体に対して単一のPIMが使用できることです。そのため、多くのサブスライバにまたがり、チームを作成できます。これにより、たとえば、スーパーバイザは、クラスタ内のサブスライバに登録されたエージェント電話機をモニタできます。ただし、この導入では、クラスタ上のリソース使用率が若干高くなる可能性があります。Cisco Unified Communications Manager Capacity ツールを使うと、ソリューションの Unified CM サーバのサイズを変更できます。

## 単一回線および複数回線機能のサポート

### 単一回線および複数回線のサポート

Unified CCE は、単一回線と複数のエージェント回線の Unified CM ベースのモニタリングをサポートします。複数回線がサポートする機能は次のとおりです。

- 全回線のコールのモニタリングとレポート。

- コール開始以外では、ACD 以外の内線上のすべての呼制御は、複数回線に対応したデスクトップでサポートされています。初期コール設定後、デスクフォンから開始されたコールを制御できます。
- 最大 2 つのコールアピランスが必要です。
- 1 台の電話機あたり最大 4 回線、1 ACD 回線、および最大 3 つの非 ACD 回線をサポートします。
- ACD および非 ACD 回線の共有電話をサポートします。相違点については、以下の表を参照してください。
- ACD 以外の回線を共有している複数のデバイスを構成できますが、エージェントにログインできるのは 1 つのデバイスのみです。Unified CCE は、共有電話をサポートしているため、自宅やオフィス両方で音声設備を備えているエージェントが音声メール回線を共有できるようにします。



**Note** 共有 ACD 以外の回線は、PG Explorer で非 ACD 回線影響の構成をサポートしません。

- マルチライン エージェント モードが有効な場合、Unified CCE にサードパーティの CTI アプリケーションとの下位互換性がない場合があります。サードパーティベンダーとのマルチラインサポートを検証します。

#### 単一回線の対複数回線の動作

操作	単一回線の動作	複数回線の動作
通話が 2 番目の回線にあるときに、ルーティングされた通話を受けるとはできますか。	あり	はい。展開に影響がないことを確認するために非 ACD 回線影響が設定されている場合。
Unified CM ベースのサイレントモニタを使用したスーパーバイザモニタ	はい	はい <b>Note</b> ACD 以外の回線では、Unified CM ベースのサイレントモニタリングはサポートされていません。
コールパーク	監視されていない 2 つ目の回線でサポート	すべての回線がモニタ対象のため、サポートされていません。



操作	単一回線の動作	複数回線の動作
通話待機/ビジートリガー > 1	サポートあり	サポートは終了しました。69xx シリーズの電話機では <b>1</b> にハードコードされています（複数回線を有効にする前に構成する必要があります）。
2番目の回線コールに関するレポート	Unified CM での CDR の使用	監視されていないデバイスを使用したエージェントの非 ACD 回線、または別のエージェントの非 ACD 回線との間の通話に対する終了通話詳細レコードは、非 ACD 周辺機器通話タイプで報告されます。ACD 以外の回線上のすべてのコールに対するレポートは、そのエージェントの [エージェント間隔 (Agent Interval)] テーブルでキャプチャされます。
電話機で構成済みの回線数	制限に関する説明はなし（1回線の監視のみ）	4回線を超える構成は行わないでください。構成すると、エージェントが任意の回線にサインインできなくなります。これにより、構成アラートが生成されます。
ACD 共有回線	共有電話は、最大2台のデバイスに対し ACD 回線でサポートされています。デバイス制御は、オフフックにするか、通話を発信または受信することで、デバイスそのものを介して選択されます。	共有電話は、最大2台のデバイスに対し ACD 回線でサポートされています。デバイス制御は、オフフックにするか、通話を発信または受信することで、デバイスそのものを介して選択されます。

操作	単一回線の動作	複数回線の動作
<p>ACD 以外の共有回線</p> <p>ACD 以外の回線を共有している複数のデバイスを構成できますが、エージェントにログインできるのは1つのデバイスのみです。Unified CCE は、共有電話をサポートしているので、自宅やオフィス両方で音声設備を備えているエージェントが音声メール回線を共有できるようにします。</p> <p><b>Note</b> 共有 ACD 以外の回線は、PG Explorer で非 ACD 回線影響の構成をサポートしません。</p>	<p>監視されていない回線でのサポート、構成制限無し</p>	<p>非 ACD 回線のサポートは、共通の2番目の回線を持つデバイスに1人のエージェントがログインする場合に限られています。</p> <p>エージェントは両方の電話機に同時にサインインできません。</p> <p>別のエージェントは、同じ共通回線を持つ別のデバイスにサインインできません。</p>

## Unified CM トランクでの MTP の使用

ソリューションで Unified CM SIP トランク を使用する場合は、Cisco Unity Voice Mail や Mobile Agent などの特定のコールフローに、MTP リソースが必要な場合があります。

これは、DTMF のインバンド対アウトオブバンド機能など、エンドポイントの交渉済みメディア機能が一致しない場合の必要です。この場合、Unified CM は、DTMF メディア機能の不一致により、MTP を動的に配置します。

サードパーティ製のデバイスで相互運用する場合、ソリューションに MTP が必要になる場合があります。

## モバイル & リモート アクセス

シスコ コラボレーション エッジアーキテクチャには、エンタープライズ ネットワークにはないデバイスによるアクセスを可能にする Unified Communications Mobile and Remote Access (MRA) が含まれています。MRA は Expressway を使用して、安全なファイアウォール トラバースを提供し、Unified CM 登録をサポートします。Unified CM は、サポートされているデバイスに呼制御、プロビジョニング、メッセージング、およびプレゼンスサービスを提供できます。

コラボレーションエッジの詳細については、<http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-system/tsd-products-support-series-home.html> 次のドキュメントを参照してください。Expressway の展開と構成の詳細については、<http://www.cisco.com/c/en/us/support/unified-communications/expressway-series/tsd-products-support-series-home.html> のドキュメントを参照してください。MRA のデバイスサポートの詳細については、ソリューションの互換性マトリックスを参照してください。

ソリューションで MRA を使用する場合は、次の点を検討してください。

- Cisco Finesse クライアントとサーバ間の接続は、MRA 接続ではなく、VPN を使用していません。
- 一部の電話機は、MRA でのエクステンションモビリティをサポートしていません。
- Contact Center Enterprise ビデオ展開は、MRA に対応していません。
- 電話機の BiB に依存する Agent Greeting、Unified CM ベースのサイレントモニタリングなどのコンタクトセンターの特定機能は MRA を介してはサポートされていません。
- VPN のスプリットトンネリングが構成されている場合は、同じクライアントマシン上で、MRA を備えた Jabber と Finesse デスクトップを使用できます。Cisco AnyConnect モビリティクライアントスプリットトンネリングの構成に関しては、<https://www.cisco.com/c/en/us/support/security/anyconnect-secure-mobility-client/products-installation-and-configuration-guides-list.html> を参照してください。
- VPN スプリットトンネリングを利用できない場合は、2 つのクライアントに分割した後に実行できます。
  - 1 台のクライアントマシンで MRA を備えた Jabber と 2 台目のクライアントマシンで VPN 接続経由の Finesse デスクトップを実行するリモートエージェント。
  - MRA 経由で接続されているラップトップで Jabber ソフトフォンを実行し、Xenapp シンクライアントとして Finesse デスクトップを実行するリモートエージェント。

## Cisco Finesse の設計上の考慮事項

Cisco Finesse は、Contact Center Enterprise ソリューションで使用するスーパーバイザおよびエージェントのデスクトップです。Cisco Finesse サーバは VM 上にインストールします。クライアントは Cisco Finesse サーバを指し示す Web ブラウザを使用します。Cisco Finesse ソフトウェアはクライアントにインストールされません。これにより、インストールとアップグレードが簡素化され、その所要時間も短縮されます。

Cisco Finesse クライアント（管理コンソール、エージェントデスクトップ、スーパーバイザデスクトップ）でサポートされるブラウザとオペレーティングシステムについては、*Contact Center Enterprise* 互換性マトリクスを参照してください。

Cisco Finesse デスクトップアプリケーションは、クライアントコンポーネントとサーバコンポーネントから構成されています。クライアントは、OpenSocial 1.0 仕様に準拠するガジェットとして分散される標準の Web プログラミング要素（HTML、JavaScript）を使用します。シスコやサードパーティのガジェットを使用するように、レイアウト管理機能を使ってエージェントデスクトップを設定できます。

Cisco Finesse は Enterprise Mashup と呼ばれるアプリケーションクラスの一部です。Enterprise Mashup は、クライアント側のアプリケーションを結合する Web 中心のメソッドです。Cisco Finesse ガジェットベースのアーキテクチャによって、クライアント側のマッシュアップが可能になり、よ

り簡単に統合できるようになります。ガジェットのアップグレードは個別に処理されるので、バージョンの互換性の依存関係はわずかです。

Cisco Finesse 管理コンソールを使って、エージェントとスーパーバイザのデスクトップをカスタマイズすることができます。管理者は、デスクトップに表示するタブの名前を定義して、各タブに表示するガジェットを設定できます。

次の表は、Cisco Finesse の機能の要約です。

**Table 3:** デスクトップの機能

デスクトップ機能	Cisco Finesse
デスクトップチャット	可
チームメッセージ	可
ブラウザベースのデスクトップ	可
カスタム開発	可 (HTML や JavaScript などの標準の Web コンポーネントを使用)
デスクトップのセキュリティ	可 <b>Note</b> Cisco Finesse は、各 PG ペアの最大 2000 エージェントに対して HTTPS をサポートします。
ワークフローの自動化	可
モバイル (リモート) エージェント	可
通話モニタリング	可
モニタモードのアプリケーション	NA
アウトバウンドコール	可
Microsoft ターミナルサービスのサポート	NA
Citrix Presentation Server のサポート	NA
エージェントのモビリティ	可
エージェントのグリーンディング	可

## Cisco Finesse REST API

Cisco Finesse は、クライアントアプリケーション向けの REST API を提供して、サポートされているサーバ機能にアクセスします。REST API は、HTTPS 経由で XML ペイロードをトランスポートします。

Cisco Finesse は、サードパーティの統合を支援する JavaScript ライブラリおよびサンプルガジェットコードも提供しています。REST API、JavaScript ライブラリ、およびサンプルガジェットの開発マニュアルは、<https://developer.cisco.com/site/finesse/> のシスコ開発者ネットワークで確認できます。

## Cisco Finesse エージェントデスクトップ

エージェントデスクトップには次の追加設定なしの機能が備わります。

- 基本呼制御（通話への応答、保留、取得、終話、発信）
- 高度な呼制御（コンサルテーション、コンサルト後の転送、コンサルト後の会議）
- シングルステップ転送（エージェントは、最初にコンサルテーションコールを開始せずにコールを転送できます）
- キュー統計ガジェット（エージェントが割り当てられているキューに関する情報を表示）
- エージェントのコール履歴と状態履歴の表示
- 準備中およびサインアウトの理由コード
- 連絡先リスト
- ワークフロー
- モバイルエージェントのサポート
- Progressive、Predictive、Preview Outbound、Direct Preview Outbound
- デスクトップチャット
- チームメッセージ

## Cisco Finesse スーパーバイザデスクトップ

Cisco Finesse スーパーバイザ機能により、エージェントデスクトップが拡張し、より多くのスーパーバイザ専用ガジェットが追加されます。たとえば、次のような機能があります。

- エージェントのステータスを表示するシステムアドミニストレーションガイドガジェット
- スーパーバイザのキューのキュー（スキルグループ）統計を表示するキュー統計ガジェット
- スーパーバイザコール履歴と状態履歴の表示
- スーパーバイザチーム内のエージェントのコール履歴と状態履歴を表示
- システムアドミニストレーションガイドガジェット（TPG）からのエージェントコール情報

- Unified CM のサイレント モニタリング
- 割り込み
- 代行受信
- エージェントの状態変更（スーパーバイザはエージェントをサインアウトでき、強制的に[準備中 (Not Ready)] ステータスまたは[準備完了 (Ready)] ステータスに変更できます）

## Cisco Finesse IP 電話エージェント

Cisco Finesse IP Phone Agent (IPPA) を使用すると、エージェントは、ブラウザを介してではなく、Cisco IP 電話から Cisco Finesse 機能にアクセスできます。Cisco Finesse IPPA は、ブラウザで使用可能な Cisco Finesse 機能のサブセットのみを提供します。これにより、エージェントとスーパーバイザは、PC にアクセスせずに Cisco Finesse コールを受信および管理できます。



**Note** スーパーバイザは、IP Phone 上でのみエージェントタスクを実行できます。Cisco Finesse IPPA は、モニタ、割り込み、代行受信などのスーパーバイザタスクをサポートしていません。

Cisco Finesse IPPA は次の機能をサポートしています。

- ログインおよびログアウト
- コール変数の表示
- 保留ステータス
- ラップアップの理由
- オプションの要約
- 準備中の理由
- 理由コードを使用したステータス変更
- ワンボタンサインイン

## Cisco Finesse 管理コンソール

Cisco Finesse には、管理者が次を構成できる管理アプリケーションが含まれています。

- CTI サーバおよび Administration & Data サーバデータベースへの接続
- VOS 複製用のクラスタ設定
- 準備中およびサインアウトの理由コード
- ラップアップの理由
- 連絡先リスト

- ワークフローとワークフローアクション
- コール変数および ECC 変数レイアウト
- デスクトップのレイアウト
- Desktop Chat サーバの設定
- チームリソース
- Cisco Finesse IP 電話エージェント (IPPA)

理由コード、ラップアップの理由、連絡先リスト、ワークフロー、およびデスクトップレイアウトは、グローバルか（すべてのエージェントに適用）、特定のチームにすることができます。

## Cisco Finesse 展開に関する検討事項

### Cisco Finesse とマルチライン機能

Unified CCE がマルチライン用に構成されている場合、Cisco Finesse は、エージェント電話機での複数回線の構成をサポートします。エージェント電話機で複数の二次回線を構成できます。ただし、Cisco Finesse サーバは、二次回線での操作の応答で CTI サーバが送信するイベントをブロックします。Cisco Finesse サーバは、これらのイベントを Cisco Finesse クライアントに発行しません。二次回線上のコールに関する情報は、Cisco Finesse デスクトップには表示されません。

エージェントが 8900 シリーズまたは 9900 シリーズの電話機を使用している場合は、Unified CM 周辺機器でマルチラインを有効にします。この構成オプションは、周辺機器全体に適用されるオプションです。8900 シリーズまたは 9900 シリーズの電話機を使用する 1 つのエージェントに対してマルチラインを有効にする場合は、すべてのエージェントに対しても有効にします。

マルチラインをサポートするには、すべての電話機を次の設定で構成します。

- [Maximum number of calls] を 2 に設定します。
- 1.へのセットの使用中のきっかけ。

### Cisco Finesse と Citrix

Contact Center Enterprise ソリューションは、Citrix 環境内での Cisco Finesse デスクトップの実行をサポートします。Cisco Finesse は、Citrix XenApp および XenDesktop をサポートします。



#### Note

AW、構成専用管理サーバ、および管理クライアントは、特定の VM 上で単一のリモートインスタンスとしてのみ動作できます。

サポートされるバージョンの詳細については、<https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-device-support-tables-list.html> の「互換性マトリックス」を参照してください。

## NAT およびファイアウォールを使用した Cisco Finesse

一部のソリューションには、ネットワークアドレス変換（NAT）をインターコネクトする 2 つ以上の切り離されたネットワークがあります。

Cisco Finesse は、NAT に対するサポートが限定されています。Cisco Finesse は、Cisco Finesse サーバとクライアント間の基本的な NAT（1 対 1 の IP アドレスマッピング）をサポートします。

次の注意事項は、Cisco Finesse と NAT に適用されます。

- Cisco Finesse サーバとクライアントの間では、PAT/NPAT（ポートを使用する 1 対多アドレスマッピング）を使用できません。
- Cisco Finesse サーバおよび接続されている任意のサーバ間では、NAT は使用できません。
- Cisco Finesse IP Phone Agent（IPPA）は NAT をサポートしません。



**Note** NAT とファイアウォールに関しては、ソリューションセキュリティの章を参照してください。

## IP Phone および IP Communicator のサポート

Cisco Finesse は、Cisco IP ハードウェア電話機および Cisco IP Communicator ソフトウェア電話機の使用をサポートしています。

サポートされる電話機モデルおよび IP Communicator のバージョンの詳細については、<https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-device-support-tables-list.html> のソリューション向け「互換性マトリックス」を参照してください。

### IP Phone およびサイレントモニタリング

サイレントモニタリングは、IP ハードウェア電話機と Cisco IP Communicator の両方をサポートします。

### IP Phone およびモバイルエージェント

モバイルエージェント機能では、特定のタイプの電話機は不要です。この機能ではアナログ電話でも使用できます。

### IP Phones および Citrix または MTS

Cisco Finesse は、Citrix または MTS の使用時に、IP ハードウェア電話機および Cisco IP Communicator の両方をサポートします。

このような環境では、エージェントデスクトップ PC に Cisco IP Communicator をインストールします。Citrix または MTS サーバに Cisco IP Communicator を展開することはできません。



## Cisco Finesse と Cisco Jabber

Cisco Finesse は Contact Center Enterprise の音声エンドポイントとして Windows 版 Cisco Jabber をサポートしています。Cisco Finesse は次の Jabber 機能をサポートしています。

- 音声とビデオ
- サイレントモニタリングの組み込みブリッジ (BIB)
- IM and Presence



**Note** エージェントは、Jabberを使用して通話を転送、または電話会議することはできません。エージェントは、転送や会議に Cisco Finesse デスクトップを使用する必要があります。

Cisco Finesse で Jabber を使用するには、デフォルトの Jabber 構成を次のように変更します。

- コールの最大数を 6 から 2 に変更します。
- ビジートリガーを 2 から 1 に変更します。

Jabber サポートの詳細については、<https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-device-support-tables-list.html> のソリューションに対する「互換性マトリックス」を参照してください。

## デスクトップチャット

デスクトップチャットは XMPP ブラウザベースのチャットであり、これは Cisco Instant Messaging and Presence (IM & P) サービスによって提供されます。デスクトップチャットを使用すると、エージェント、スーパーバイザは、組織内の各分野の専門家 (SME) とチャットを行うことができます。

詳細については、<https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-implementation-design-guides-list.html> を参照してください。

インスタントメッセージングおよびプレゼンス (IM&P) は、Unified CM プラットフォーム内でプレゼンスおよびチャット機能を提供します。デスクトップチャットインターフェイスは、Finesse エージェントデスクトップにホストされ、個別に IM&P サービスにログインする必要があります。

**Note**

Release 12.5(1)からのHCS展開では、デスクトップチャットユーザ検索に、デフォルトではLDAPのすべてのユーザが表示されます。この検索を調整して、エージェントまたはスーパーバイザが検索を開始した対応するカスタマーのユーザを、Cisco Unified Communications Manager IM and Presence Service で定義されている組織ユニット (OU) に基づいて表示できます。これは Cisco Unified Communications Manager IM and Presence Service、リリース 12.5(1)SU2 ES ビルドバージョン 12.5.1.12900-26 以降でサポートされています。詳細については、Cisco TAC にお問い合わせください。

デスクトップチャットでは、Cisco Mobile Remote Agent /VPN ベースの IM&P サーバへのアクセスはサポートされていません。デスクトップチャットでは、チャットサーバに接続する IM&P サーバへのダイレクトアクセスが必要となります。

詳細については、<https://www.cisco.com/c/en/us/support/customer-collaboration/finesse/products-maintenance-guides-list.html> にある『Cisco Finesse アドミニストレーションガイド』の「Desktop Chat サーバの設定」の項を参照してください。

## シスコインスタントメッセージングおよびプレゼンス (IM&amp;P)

IM&P は Jabber プラットフォームを組み込み、XMPP プロトコルをサポートし、複数のデバイスを介してユーザのプレゼンスを追跡できます。IM&P は、チャット機能が有効になっているユーザそして、Unified CM (LDAP 統合が有効である場合は、LDAP から) からユーザリストをプルします。チャット機能が有効になっている Unified CM ユーザのみ IM&P にログインできます。

Cisco IM&P は、高可用性を実現するためにクラスタ化された展開の複数の形式をサポートします。Finesse は、特定のエージェント PG で構成されます。このエージェント PG は、特定の IM&P クラスタに関連付けられた Unified CM に接続されます。Finesse を IM&P クラスタに接続するよう構成します。

**アイデンティティ、プレゼンス、Jabber**

ユーザは、IM&P で識別され、これは、`username@FQDN.com` 形式の固有のアイデンティティです。

Unified CCE では、アイデンティティが Unified CCE で設定されたユーザ名または `peripheralID` と同じではありません。

ユーザは、ユーザ ID、プレゼンスステータス (使用可能、使用不可、またはビジー)、およびユーザのプレゼンス機能の観点から説明されます。

ユーザのプレゼンスステータスは、エージェントステータスとは関係なく、ユーザのポストログインによって個別に管理される必要があります。

Cisco IM&P サービスは、複数のデバイスでユーザのプレゼンスステータスを組み合わせ、連絡先リストに連絡先を追加したサブスクライバに公開します。

IM&P は、エージェントがログインしているすべてのデバイスの状態マトリックスから導出される、ユーザの構成されたプレゼンスをサポートします。Cisco IM&P は、ユーザに対する XMPP クライアントからのプレゼンスの送信元を、CUCM からオンホック、およびオフホックステータス

を、Microsoft Exchange から会議中ステータスを取得し、ユーザの全体的な構成されたプレゼンスを生成します。デスクトップチャットでは、構成されているユーザのプレゼンスが表示されます。構成されたプレゼンスの到達方法に関しては、<https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-user-guide-list.html> の『Cisco IM&P ユーザガイド』を参照してください。

展開ガイドに関係なく、デスクトップチャットは、Finesse デスクトップにログイン後、ユーザの IM&P アイデンティティを使用して明示的なログインをする必要があります。

SSO はデスクトップチャットではサポートされていないため、SSO モードでは明示的なログインが必要です。

デスクトップチャットのプレゼンスは、設定されているデバイス間で通信できるユーザの存在を示しています。

デスクトップチャットの可用性は、ユーザの統合された IM&P プレゼンスにも反映します。

デスクトップチャットにログインすると、デフォルトで、ユーザのステータスは利用可能に設定されます。

デスクトップチャットにログインするエージェントは、Jabber または IM&P に接続されている XMPP プラットフォームでは利用可能として見られ、該当ユーザと連絡を取り合うことができます。



**Note** ファイル転送は、デスクトップチャットを使用したユーザ間の通信でのみサポートされています。サポートされているファイルタイプおよび添付ファイルの最大サイズに関する詳細は、『Cisco Unified Contact Center Express Administration and Operations Guide』の「デスクトッププロパティ CLI」項を参照してください。

### デスクトップチャットの可用性の例

デスクトップチャットユーザは、デスクトップチャットと Jabber に同時にログインできます。着信チャットは、デスクトップチャットを含む、ログインしているすべてのクライアントにリレーされます。ただし、デスクトップチャットではマルチデバイスメッセージングがサポートされていません。そのため、Jabber などの他の XMPP クライアントから送信されたメッセージはデスクトップチャット内に表示されません。代替クライアントが着信チャットへの応答に使用されると、ユーザがデスクトップチャットを使用して応答を開始するまで、後続メッセージはデスクトップチャットに表示されません。

ネットワーク設計に関する詳細は、<https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-implementation-design-guides-list.html> の『ソリューションリファレンスネットワーク設計ガイド』を参照してください。

Finesse サーバからのチャットサーバ URI を取得すると、Finesse ブラウザによって HTTP を介して Cisco IM&P に個別に接続することができるようになります。HTTPS 導入で自己署名証明書を使用する場合は、別個の証明書を受け入れる必要があります。

チャットの相互作用は、XMPP プロトコルを介して、長期ポーリングを使用した HTTP 接続、または、Cisco IM&P で確立された BOSH で発生します。

Cisco IM&P サーバ構成の取得以外では、チャット関連の機能に対する Finesse サーバおよびブラウザ間の通信はありません。

チャットログの持続は、デスクトップセッション中にブラウザで利用できます。

ユーザ検索機能には、Unified CM LDAP 統合が必要です。それがない場合、リモートの連絡先はユーザが手動で追加する必要があります。

ユーザが、既存の Jabber ユーザの場合、デスクトップチャットおよびセッションで維持される Jabber 間で同じ連絡先が共有されます。

Cisco IM&P で推奨されている制限やガイドライン以外で、デスクトップチャットでの進行中のチャットや連絡先の数には制限はありません。進行中のチャットや連絡先の数に対する制限、およびチャット向けの Cisco IM&P サーバの構成方法に関しては、『[IM&P ソリューションリファレンス ネットワーク ガイド](#)』を参照してください。



#### Note

デスクトップチャットでは、信頼する Cisco IM and Presence の証明書が必要です。証明書の受け入れ方法の詳細については、<https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-express/products-user-guide-list.html> の『*Cisco Unified Contact Center Express* 向け *Cisco Finesse* エージェントおよびスーパーバイザユーザガイド』の「一般的なタスク」章にある「セキュリティ証明書の承認」項を参照してください。

### Cisco IM&P 展開に関する考慮事項

Finesse は、Cisco Finesse Administration インターフェイスを介してプライマリおよびセカンダリ IM&P チャットサーバを構成します。

デスクトップチャットは、構成済みサーバの接続し、ユーザに対して構成された適切な IM&P ノードを自動的に検出し、IM&P 内の適切なノードに接続します。この解決は、ユーザがブラウザのキャッシュをクリアするまで、チャットが初めてロードされ、その後同じノードを使用するときのみ実行されます。



#### Note

デスクトップチャットは、Jabber とは異なり DNS\_SRV\* レコードを使用しません。また、ネットワーク構成に基づいて自動的に構成されません。チャットサーバの検出には、管理ページからの明示的なチャット URI 構成が必要です。

Cisco IM&P 展開の詳細については、[https://www.cisco.com/c/en/us/td/docs/voice\\_ip\\_comm/cucm/srnd/collab12/collab12/presence.html](https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/srnd/collab12/collab12/presence.html) の『Unified CM ソリューションリファレンス ネットワーク設計ガイド』を参照してください。

次の詳細に関しては、『[Cisco Unified Communications Manager 上の IM および Presence サービスの構成および管理ガイド](#)』を参照してください。

- IM&P サービスのインストールおよび構成方法。
- IM&P を構成し、エンドユーザに対してチャットサービスを有効にする方法。
- クラスタと高可用性展開の構成方法。
- IM&P フェデレーションの構成方法。

## Desktop Chat サーバの設定

デスクトップチャットは XMPP ブラウザベースのチャットであり、これは Cisco Instant Messaging and Presence (IM & P) サービスによって提供されます。Unified CM プラットフォーム内にプレゼンスおよびチャット機能を提供します。詳細については、<https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html> の「*IM and Presence Service* の構成と管理」を参照してください。

デスクトップチャットは、エージェントデスクトップをホストしているブラウザからポート 5280 経由で Cisco IM&P サーバに接続します。クライアントがこの機能を使用する場合は、IM&P サーバの可視性およびポートへのアクセス性を確保する必要があります。デスクトップチャットガジェットは、BOSH HTTP を介して IM&P サーバと通信するためにデスクトップが使用する IM&P ホスト BOSH URL を構成します。

IM & P はクラスタ化された設計であり、ユーザはクラスター内の複数のノードに分散されます。デスクトップチャットはまず、ユーザが構成した IM&P ノードを検出し、この情報をキャッシュし、ブラウザのキャッシュがクリアされるまで、後続のログインの実際のサーバと通信します。最初の検出負荷を分散するには、展開に 1 つ以上の Finesse クラスタがある場合、ラウンドロビンでノードを構成することをお勧めします。たとえば、IM&P ノードが 5 つある場合は、ノード 1 と 2 で Finesse クラスタ A を構成し、ノード 3 と 4 で Finesse クラスタ B を構成します。

IM&P URL を構成する一方で、ノードを利用できるよう考慮する必要があります。セカンダリノードは、最初のノードが到達不可能なシナリオで利用できます。セカンダリノードは、プライマリノードが到達不可能な場合にのみ、検出のために接続されます。

構成する URL については、『システム、サービスパラメータ』の「Cisco Unified Presence」を参照してください。必要な IM&P サーバを選択し、Cisco XCP Web 接続マネージャーを選択します。[HTTP バインドパス (*HTTP Binding Path*)] フィードバックに、URL バインドパスが一覧されます。Finesse で構成する完全な URL は `https://<hostname>:5280/URL-binding-path` です。

Desktop Chat サーバの設定を使用して、Finesse デスクトップのチャットを構成します。次の表に、Desktop Chat サーバ設定ガジェットのフィールドを示します。

フィールド	説明
プライマリチャットサーバ	デスクトップチャットの IM&P プライマリサーバの URL を入力します。

フィールド	説明
セカンダリチャットサーバ	デスクトップチャットの IM&P セカンダリサーバの URL を入力します。

#### デスクトップチャットサーバガジェットでのアクション

- **[保存 (save) ]:** 構成変更を保存します
- **元に戻す:** 直前に保存されたサーバ設定を取得します



#### Important

デスクトップチャットが問題なく動作する場合は、次のサービスが IM&P 上で実行されている事を確認してください。

- Cisco Presence Engine
- Cisco XCP Text Conference Manager
- Cisco XCP Web Connection Manager
- Cisco XCP Connection Manager
- Cisco XCP Directory Service
- Cisco XCP Authentication Service
- Cisco XCP File Transfer Manager



#### Note

ブラウザによって自動的に信頼されない証明書で Cisco IM and Presence が構成されている場合、Finesse デスクトップへのサインイン中にセキュリティ証明書を受け入れるプロンプトがユーザに表示されます。証明書を受け入れるプロンプトが必ず表示されるのを避けるために、ユーザは、証明書をブラウザの信頼ストアに追加するか、CA で署名された証明書を使用して IM and Presence を構成するか、サポートされているブラウザのグループポリシーを通じて自己署名証明書をプッシュする必要があります。



#### Note

デスクトップチャットは、IM&P の無制限バージョンではサポートされません。

#### デスクトップチャット検索



#### Note

Cisco Finesse でこの機能を有効にするには、Finesse 12.0(1) ES4 COP 以降をインストールします。

デフォルトでは、デスクトップチャットユーザ検索にはLDAPのすべてのユーザが表示されます。この検索を調整して、エージェントまたはスーパーバイザが検索を開始した対応するカスタマーのユーザを、Cisco Unified Communications Manager IM and Presence Service で定義されている組織ユニット（OU）に基づいて表示できます。これは Cisco Unified Communications Manager IM and Presence Service、リリース 12.5(1)SU2 ES ビルドバージョン 12.5.1.12900-26 以降でサポートされています。詳細については、Cisco TAC にお問い合わせください。

Cisco Unified Communications Manager IM and Presence Service では、管理者が [クライアントユーザ（Client User）] フィールドを [検索可能なLDAP属性（Searchable LDAP Attributes）] テーブルの [適切なLDAPユーザ（Appropriate LDAP User）] フィールドにマップする必要があります。

検索可能な LDAP 属性（[クライアント（Client）] フィールドと [LDAP] フィールド間の属性マッピング）

設定は、選択したLDAPサーバのタイプによって異なり、LDAPサーバの各論理的なエンティティと完全に一致する必要があります（たとえば、姓、名、氏名など）。XMPP ユーザ検索を行うには、次のようにして各クライアントユーザを [LDAP] フィールド属性にマッピングします。

- Active Directory は、[クライアントユーザ（Client User）] フィールドと [LDAPユーザ（LDAP user）] フィールドのデフォルト値を提供します。使用している構成に合わせて、必要に応じて各フィールドを編集できます。
- 汎用ディレクトリサーバは、デフォルト値を提供しません。XMPP ユーザ検索を行うには、各 [クライアントユーザ（Client User）] フィールドにマッピングする LDAP 属性を指定する必要があります。

Table 4: クライアントから LDAP へのフィールド属性マッピングのサンプル

クライアントユーザフィールド	LDAPユーザフィールド
OU	ou
ラストネーム（姓）	sn
fullname	cn
uid	sAMAccountName

サードパーティのXMPPクライアントのLDAP検索設定の詳細については、<https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html> の『IM and Presence Service の構成及び管理』に記載されている「LDAPディレクトリ統合」章を参照し、検索可能なLDAP属性に関しては、『IM and Presence Service オンラインヘルプ』を参照してください。

CLI コマンドを使用して、Cisco Finesse でのデスクトップチャット OU 検索を構成します。CLI コマンドの詳細については、<https://www.cisco.com/c/en/us/support/customer-collaboration/finesse/products-maintenance-guides-list.html> の「Cisco Finesse アドミニストレーションガイド」に記載されている『デスクトップのプロパティ』項を参照してください。

# Cisco Unified Intelligence Center の設計上の考慮事項

## Unified Intelligence Center の展開

Unified Intelligence Center の展開は、次の要素で構成されています。

- クラスタ内の 1 つ以上の Unified Intelligence Center レポート（メンバー）ノード
- リアルタイムおよび履歴データソース
- ライブデータソース
- その他オプションのデータソース

**Note**

Unified Intelligence Center とデータソースサーバが同じ NTP サーバと同期中であることを確認してください。

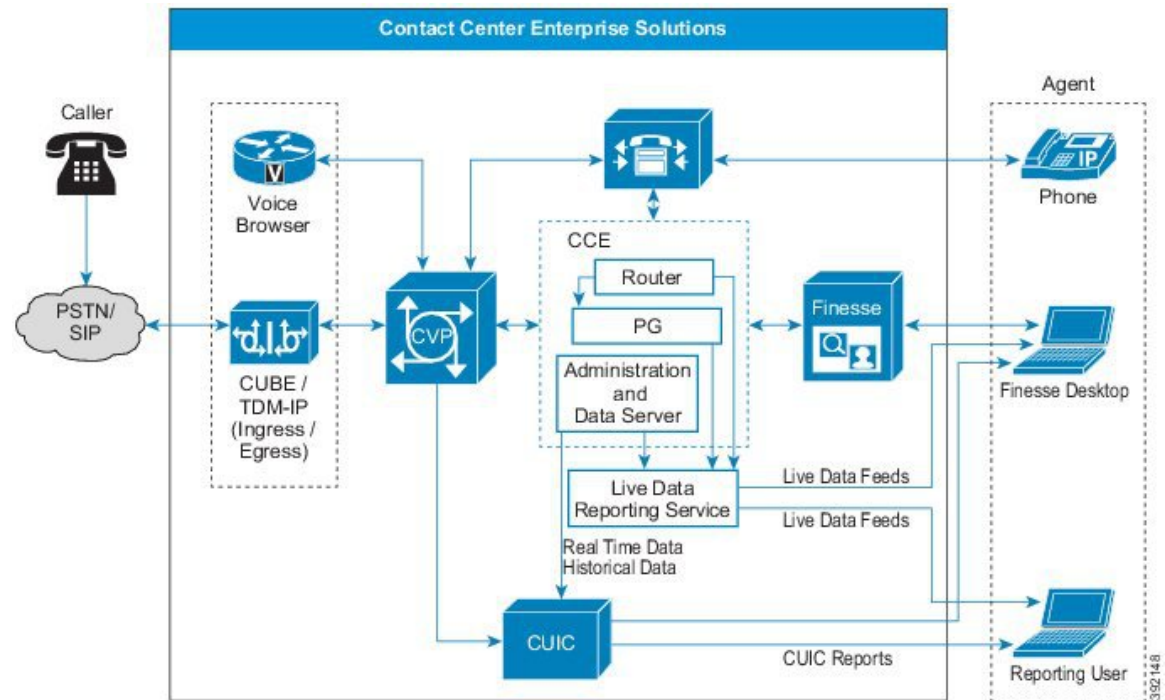
Unified Intelligence Center ノードは、Contact Center Enterprise ソリューションのスタンドアロン VM に展開されます。Unified Intelligence Center は、履歴レポート、リアルタイムレポート、ライブデータレポートをサポートしています。

履歴レポートまたはリアルタイムレポートのデータフローは、次のように実行されます。

1. Web クライアントは、Unified Intelligence Center の履歴レポートまたはリアルタイムレポートに対して HTTPS 要求を行います。
2. Unified Intelligence Center レポートノード上の Web サーバが要求を受信します。
3. レポートノードは、データソースサーバからレポートデータをプルします。
4. レポートノードは、Web サーバを介してレポートを Web クライアントに送信します。



Figure 11: Unified Intelligence Center の展開



クライアントは、Live Data サービスの Live Data イベントストリームから ライブデータレポートを更新します。ライブデータ制御とデータフローの詳細については、<http://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-and-configuration-guides-list.html> の *Cisco Unified ICM/Contact Center Enterprise* サービスアビリティ ベスト プラクティス ガイドを参照してください。

## Unified Intelligence Center Reporting ノード

レポートノードは Unified Intelligence Center の中核であり、レポート用のすべての機能が備わっています。レポートノードは、以下の構成で展開できます。

- コントローラノード上のスタンドアロン レポート ノード
- クラスタ内に最大 7 つのレポートメンバーノードを含むコントローラノード

レポートノードには、次のアプリケーションが含まれます。

- ファイアウォール
- Unified Intelligence Center アプリケーションを実行する Web サーバ
- Web リクエストを HTML に変換する JAVA サービスおよび JSP ページ
- クラスタ内での複製をサポートする Unified Intelligence Center Database (Informix)
- 管理 (OAMP) アプリケーション (発行元ノード上)

### Unified Intelligence Center Database (Informix)

各レポートノードには、Unified Intelligence Center アプリケーションデータベースが含まれます。Unified Intelligence Center データベースは、Unified Intelligence Center レポート Web アプリケーションの主要データストアです。クラスタ内の各ノードのユーザ、レポート、およびユーザアクセス権関連の構成情報が保持されています。

Unified Intelligence Center クラスタでは、各データベースサーバは他のすべてのデータベースサーバに接続します。データは、任意のサーバから他のすべてのサーバにすぐに複製されます。

日次自動削除は、午前 0 時に実行され、データベースのメンテナンスアクティビティを処理します。必要に応じて、削除スケジュールを変更できます。削除とバックアップは、ローカルの Unified Intelligence Center データベースの唯一のローカル データベースメンテナンス タスクです。

## Unified Intelligence Center データソース

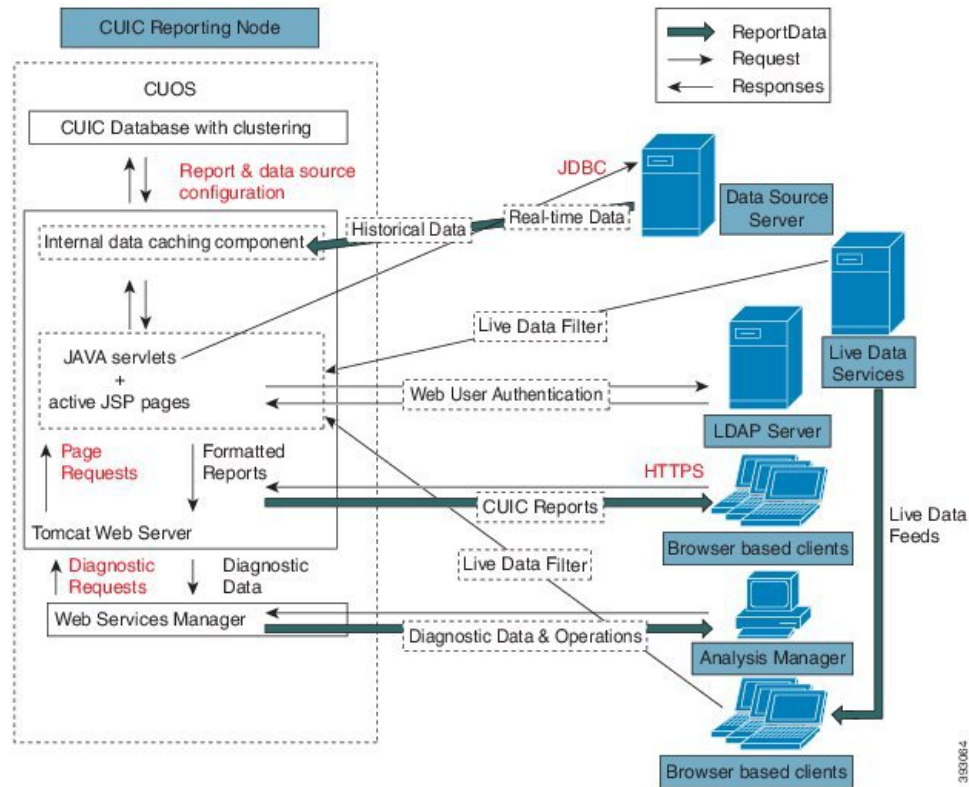
Unified Intelligence Center は、次のデータソースをサポートしています。

- リアルタイムレポートおよび履歴レポート用の Microsoft SQL ベースまたは Informix データソース。SQL ベースのデータソースは、有効な JDBC 対応データベースであり、レポートデータを格納するスキーマです。
- ライブデータレポートに対するストリーミングデータソース

これらデータソースサーバは、以下のレポートをサポートします。

- Cisco Finesse ガジェットに表示されるレポートを含む、Contact Center Enterprise レポート。
- インポート可能な Unified CVP レポート
- Customer Collaboration Platform レポート
- ビジネス チャットおよび E メール reports

Figure 12: Unified Intelligence Center アーキテクチャ



39306-4

### Unified Intelligence Center のライブデータ

Unified CCE は、WebSockets を介してエージェント、スキルグループ、およびコールタイプステータスでリアルタイムの更新を公開します。Unified Intelligence Center レポートは、これらのメッセージをライブデータサービスから直接消費し、リアルタイムで更新を表示します。

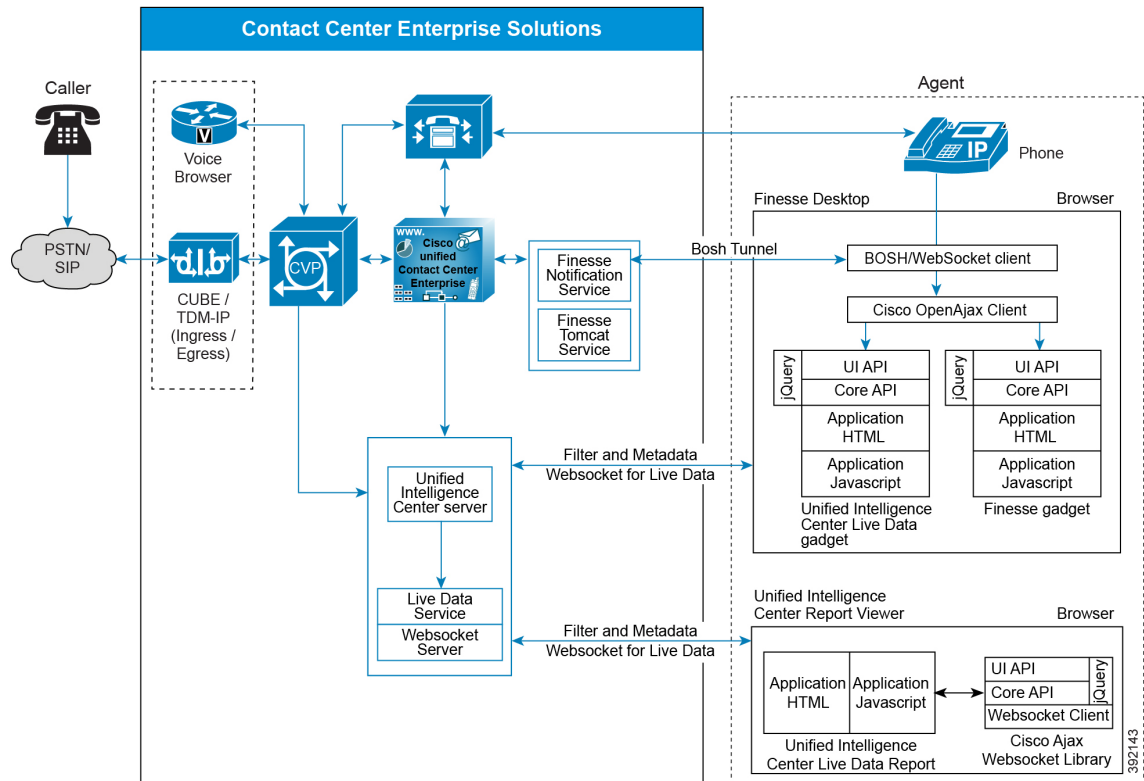
Unified CCE では、ライブデータサービスは独自の VM 上に存在します。

ライブデータレポートは、Unified Intelligence Center レポートビューアで実行できます。Cisco Finesse デスクトップでは、ガジェットにライブデータレポートを表示できます。Cisco Finesse デスクトップの親コンテナからライブデータサービスの1つまでWebSocketトンネルを使用します。ガジェットは、ロード中にトンネルを作成します。

WebSocket 接続に障害が発生すると、ライブデータレポートは、現在接続されている Live Data ノードに自動的にフェールオーバーします。

次の図は、Contact Center Enterprise 展開におけるライブデータレポートのアーキテクチャを示しています。

Figure 13: Contact Center Enterprise のライブデータレポート



## データソースとしての Administration & Data サーバ

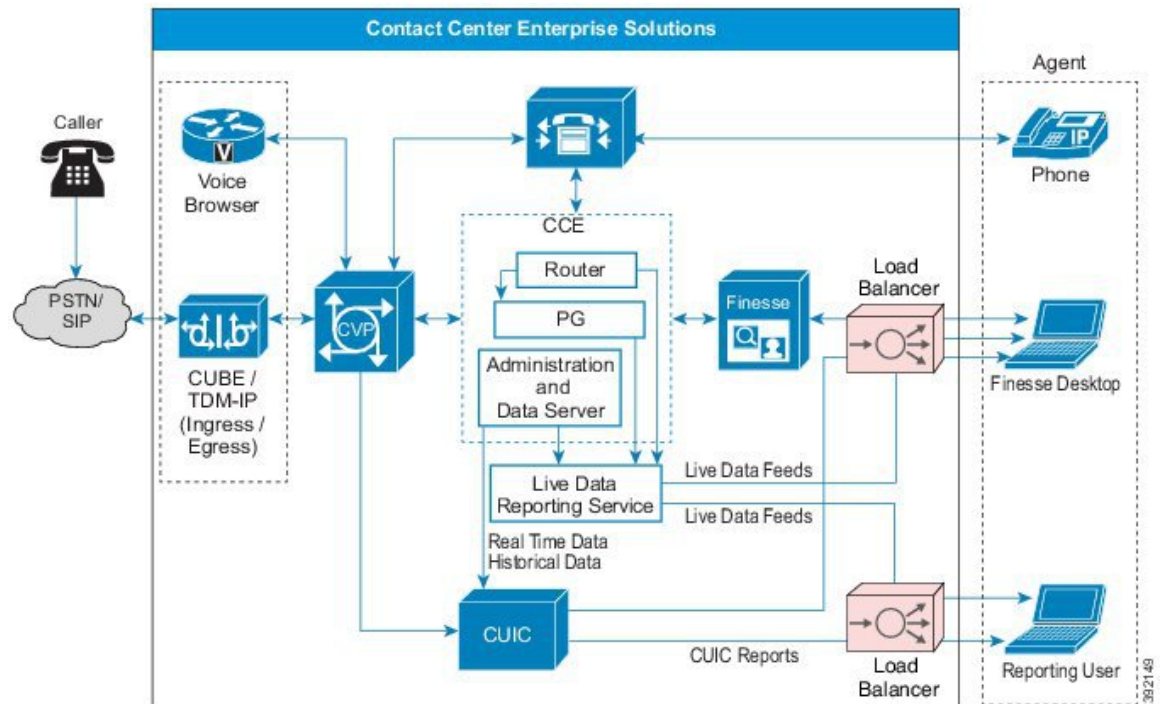
Unified Intelligence Center の株価レポートでは、データソースとして Administration & Data サーバを使用します。Contact Center Enterprise 展開では、複数の Administration & Data サーバを使用できます。Unified Intelligence Center は、データベースとそのビューをデータソースクエリのテーブルとして使用します。

Unified Intelligence Center をインストールすると、レポート（メンバー）ノードに2つのデータソースが追加されます。

- 履歴データソースは、履歴レポートとユーザ統合にデータを提供します。
- リアルタイムデータソースは、リアルタイムレポートにデータを提供します。

展開では、両方のデータソースに同じ AW-HDS を使用できます。また、データソースごとに異なるサーバを構成することもできます。Unified Intelligence Center では、標準規格の履歴レポートのデータソースとして AW-HDS が必要です。ただし、標準規格のリアルタイムレポートにはデータソースとして AW を使用できます。Unified Intelligence Center では、TCD レコードに関するカスタムレポートのデータソースとして AW-HDS-DDS または HDS-DDS が必要です。

Figure 14: 履歴レポートとリアルタイムレポート用の Unified CCE を使用した Unified Intelligence Center の展開



## データソースとしての Unified CVP

Unified CVP からレポートをインポートする展開の場合、Unified Intelligence Center は、データソースとして CVP コールサーバを使用します。

CVP コールサーバはレポートングサービスを提供し、IBM Informix Dynamic サーバ (IDS) データベース管理システムをホスティングします。データベースのスキーマを使用すると、データベースに対してカスタムのレポートを作成できます。ソリューションには、複数の CVP コールサーバを含めることができます。

Unified Intelligence Center は、CVP コールサーバにのみ接続します。CVP コールサーバは、他の Unified CVP サブコンポーネントと Unified Intelligence Center 間を仲介します。

## WAN 展開での Unified Intelligence Center

Unified Intelligence Center クラスタは、WAN 上で分散できます。クラスタ内の各ノードには、他のすべてのノードへの接続が必要です。クラスタ内では、LAN または WAN を使用して、一方のノード上に作成された構成定オブジェクトは、他のノードに自動的に複製されます。複製では、WAN 全体の帯域幅が使用されます。ただし、構成オブジェクトを作成する頻度は低いため、レポートを実行するよりも WAN 帯域幅に影響を与える頻度が低くなります。

オブジェクトは、ローカルノード上で即座に利用可能なユーザになります。オブジェクトが他のノードに複製されるまで数秒かかる場合があります。複製用の WAN 帯域幅は、クラスタの構成によって異なります。

## サイト組織

Unified Intelligence Center クラスタは、最大で8つのノードを保持できます。完全な冗長クラスタリングを保持するには、ノードの数は最大4つです。資格がある場合、各Unified Intelligence Center は、標準規格のレポートプロファイルで、最大200人のレポートユーザをサポートします。クラスタ内では、最大8つのノードを持つこともできますが、レポートユーザの最大数に関するリファレンス設計上の考慮事項制限を超えることはできません。

プライマリ（コントローラ）ノードはプライマリサイトにあります。プライマリノードは、次のサービスをホストします。

- 管理アプリケーション
- スケジューラ

## WAN 障害

各 Unified Intelligence Center ノードは、複製データをバッファし、クラスタ内の他のノードに送信します。切断中、別のノードへの接続が復元されるまでノードは、データをキューに入れます。各ノードは、接続障害が発生した場合でも、個別に動作し続けます。キューは最大1600MBを保持します。バッファ消費の前に接続が復元された場合、ノードはキューに入っているデータの量と接続帯域幅に比例した速度で同期します。

ノードがバッファ消費に近い場合、アラームが送信されます。バッファが使い果たされる前に接続が復元されなかった場合、複製がリセットされます。復元をリセットすることで、ノードは、引き続きレポートを実行し、個別に動作します。複製をリセットするセカンダリノードでは、プライマリノードとの再接続後、プライマリノードとの完全同期（プライマリデータベースのバックアップとセカンダリノードでの復元）が必要です。複製がリセットされると、セカンダリノード上に作成または変更されたすべてのオブジェクトがプライマリデータベースの状態にロールバックされます。

プライマリノードに障害が発生した場合は、再インストールして保存済みバックアップに戻します。データ損失を回避するために、プライマリノードを定期的にバックアップします。

データ複製の詳細については、『Cisco Unified Intelligence Center 向け管理コンソールユーザガイド』を参照してください。

## Unified Intelligence Center Administration

Unified Intelligence Center Administration サーバは、運用、管理、メンテナンス、プロビジョニング（OAMP）機能を提供します。Administration サーバは、Unified Intelligence Center クラスタでデバイスを構成およびプロビジョニングするためのプライマリインターフェイスです。クラスタ内のプライマリ（コントローラ）ノードで管理機能を展開しアクセスします。

Cisco Unified Intelligence Center は、アプリケーションクラスタリングに Hazelcast を使用します。Hazelcast は、Unified Intelligence Center アプリケーション層にセカンドレベルのキャッシュを提供します。Hazelcast がキャッシュしたエンティティ（例：レポート、レポート定義など）を、Unified Intelligence Center ノードで更新する際は、クラスタ内の別のすべての Unified Intelligence Center ノードで、エンティティを無効にし、再ロードする必要があります。Hazelcast クラスタは、該当

する無効なエンティティなどの識別子を含むクラスタ全体の通知を発行することで、自動的に該当するクラスタをケアします。

Unified Intelligence Center では、Hazelcast クラスタの検出または情報に対するデフォルトメカニズムは、UDP マルチキャストです。Unified Intelligence Center は、マルチキャストグループの IP アドレス 224.2.2.3 およびポート 54327 を使用します。これら設定は、Unified Intelligence Center では変更できません。

次のシナリオでは、UDP マルチキャストベースの検出メカニズムはカスタマーには機能しません。

- ネットワークでマルチキャストが無効化されている場合。
- Unified Intelligence Center クラスタ内のノードが異なるサブネット内にある場合。

このようなシナリオでは、検出メカニズムを TCP/IP に変更できます。デフォルトの UDP マルチキャストベースの検出メカニズムではなく、TCP/IP を使用して CUIC アプリケーションクラスタを形成できます。

管理機能および Hazelcast を使用したクラスタ構成の詳細に関しては、<http://www.cisco.com/c/en/us/support/customer-collaboration/unified-intelligence-center/products-maintenance-guides-list.html> の *Cisco Unified Intelligence Center* 管理コンソール ユーザ ガイド を参照してください。



**Note** 管理アプリケーションは、ネットワーク オプション、証明書、アップグレード、SNMP およびアラート設定などのシステムレベルの機能には使用しないでください。

## 履歴レポートおよびリアルタイムレポートのスロットリング

Unified Intelligence Center のスロットリングメカニズムにより、サーバが極端な負荷の下でメモリ切れ状況で凍結したり、その状況に直面するのを防ぎます。



**Note** サイジングの目的でスロットリングメカニズムを使用しないでください。スロットリングメカニズムは、メモリ切れ状況を回避するのみ使用します。スロットリングは、高品質のサービスを保証するものではありません。導入が過剰に使用されている場合、スロットリングメカニズムがアクティブ化される前に、サービスレベルが大幅に低下する可能性があります。

ソリューションに適したレポートリソースを判断するには、常にサイジングツールを使用します。

レポートデータの処理は、Unified Intelligence Center で最もメモリを消費します。スロットリングメカニズムは、レポートアクティビティによるメモリ消費を制御します。

Unified Intelligence Center は、レポート行を通じてレポートアクティビティを測定します。レポートアクティビティのこの測定により、柔軟性が得られます。いくつかの大規模レポートまたはたくさんの小規模レポートを実行できます。スロットリングメカニズムも調整なしで効果を発揮します。

Unified Intelligence Center は、レポート行を通じてレポートアクティビティを測定します。レポートアクティビティのこの測定により、柔軟性が得られます。いくつかの大規模レポートまたはたくさんのお小規模レポートを実行できます。スロットリングメカニズムも調整なしで効果を発揮します。

ストックレポートを使用したテストでは、2KB がレポート行のサイズに対する保守的な推定値であるという結果が示されています。その推定値に基づいて、Unified Intelligence Center サーバは、サーバがメモリを使い切る前に、最大 250,000 レポート行をメモリにロードできます。

この制限を適用するために、各 Unified Intelligence Center は、現在メモリにロードされているレポート行の数を保持します。すべてのレポート操作は、その数を確認して、メモリにさらにレポート行がロードできるかを判断します。制限に達すると、レポート操作は失敗し、次のようにエラーが表示されます。

- **データソースからデータをフェッチする際の侵害**—レポート実行のキャンセルまたは失敗としてレポートをマークします。Unified Intelligence Center では、部分的な結果を取得しません。システムは、要求に関するすべてのデータを読み取るか、レポートに失敗のマークを付けるか、すべてのデータを保存しません。
- **ブラウザの HTTPS 応答準備中の侵害**—Unified Intelligence Center はディスプレイリクエストを拒否します。サーバのリソースが低く、レポートをレンダリングできない旨が記載されたエラーメッセージが表示されます。

## リファレンス設計とトポロジ設計に関する考慮事項

### Unified CM SME の展開

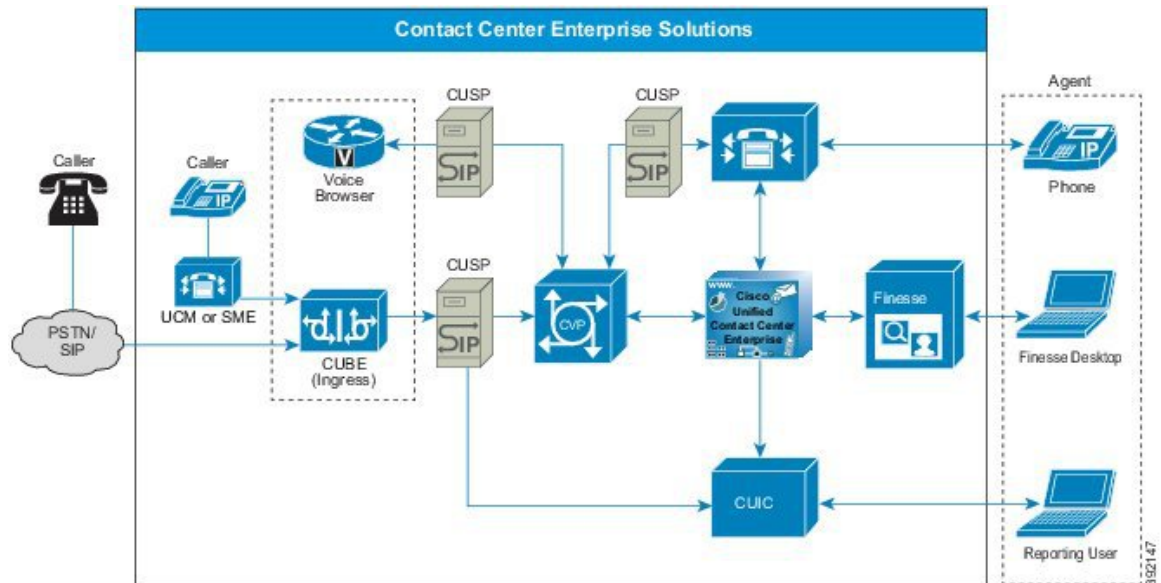
Cisco Unified Communications Manager Session Management Edition (Unified CM SME) は、ダイヤルピア設定機能またはアグリゲータとして Unified CVP と統合し、Contact Center Enterprise ソリューション内の複数の Unified CM クラスタに接続します。

Unified CM SME をバック ツーバック ユーザ エージェントとして構成します。複数の Unified CM クラスタのアグリゲータとして、ダイヤルプランに基づいてコールを適切なクラスタにルートします。

次の図は、Unified CM SME の導入を示しています。



Figure 15: Unified CM SME の展開



Unified CM SME は高可用性をサポートしていないので、シングルポイント障害です。Unified CM SME でのネットワーク接続またはコンポーネントの障害の影響を最小限に抑えるために、これらの設計ポイントを検討してください。

- Unified CVP の出力側で Unified CM SME を冗長クラスタ モードで展開します（少なくとも 1+1 のパブリッシャ サブスクリバ）。
- ゲートウェイと CUBE でセッション更新およびセッションタイマーを構成します。この構成では、ゲートウェイからのコールセッションがクリアされ、Unified CM SME に障害が発生した場合に Unified CVP コールサーバポートがリリースされます。
- Unified CM SME に障害が発生した場合、顧客がコールをドロップした後、すべてのコールサーバポートがクリアされます。



**Note** Unified CM SME に障害が発生した場合、コール補足サービスはすでに確立されているコールでは機能しません。

Unified CM SME へのネットワーク接続に瞬間的な障害が発生すると、次の制限が適用されます。

- 瞬間的な接続障害が発生しエージェントが終話した場合、Unified CM SME はコールをクリアしません。このため、キャッシュされた古いエン트리とポートが Unified CVP アプリケーションで切断します。この場合、発信者はコールを破棄して、古いキャッシュされたエントリをクリアする必要があります。
- コールはエージェントデスクトップからクリアされません。また、エージェントは着信コールを受信できません。エージェントは通話状態のまま、デスクトップからコール

をクリアすることはできません。このような場合は、電話機から手動でコールをクリアします。

- コールのクリアが遅れると、コールレポートデータには、通話時間と理由コードに関する不適切な詳細が反映される場合があります。

Unified CM SME の構成については、<http://www.cisco.com/c/en/us/support/customer-collaboration/unified-customer-voice-portal/products-installation-and-configuration-guides-list.html> のサイトにある『Cisco Unified カスタマー音声ポータル用構成ガイド』を参照してください。

## グローバル展開に関する検討事項

- メインサイトおよびリモートサイト間の最長ラウンドトリップタイム (RTT) は、400 ミリ秒に制限されています。
- サイド A コンポーネントとサイド B サイト間の最長 RTT は、80 ミリ秒に制限されています。



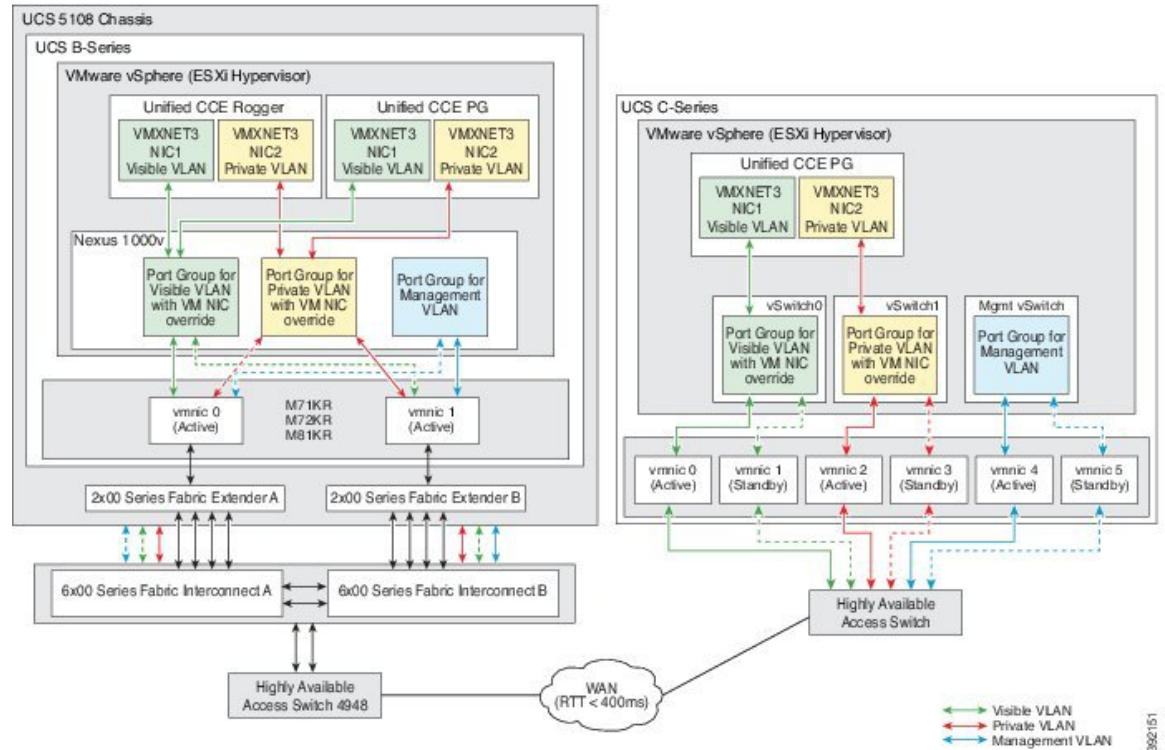
**Note** ポストコール調査を使用する場合、セントラルサイトとリモートサイト間で、最大 12 台の Unified CM PIM を組み合わせることができます。

- CVP メディアサーバのホスト名を使用して、ローカル CVP サーバをポイントする IOS ゲートウェイを構成します。

## グローバル展開のための UCS ネットワーク設計

この図は、パブリックネットワークとプライベートネットワーク通信の要件を満たすようにグローバル展開ス地裁のデフォルト設計を示しています。メインサイトは USB B シリーズブレードを、リモートサイトは UCS C シリーズサーバを使用します。

Figure 16: グローバル展開用の UCS ネットワークリファレンスの設計



## 分散型展開でのコール存続可能性

分散型の導入では、ブランチの他の音声サービスの設計ガイドラインが必要です。たとえば、ACD エージェントと非エージェント電話の両方をサポートするリモート Unified CM サイトであるブランチがあるとします。この導入では、PSTN ゲートウェイが処理するのは、Unified CVP のイングレスコールではありません。また、通常非 ACD 電話に対してイングレスコールとイーグレスコールも処理されます。

WAN のブランチの信頼性は、通常 LAN リンクよりも信頼性が低いため、中央集中型の Unified CVP モデルでは問題になる可能性があります。Unified CVP コールと非 CVP コールのどちらの場合も、コール存続可能性機能を考慮する必要があります。Unified CM エンドポイントの電話の場合、存続可能性は Survivable Remote Site Telephony (SRST) という Cisco IOS 機能を使用して実現されます。

Unified CVP コールの場合、TCL スクリプト (survivability.tcl) からのサービスと SRST 関数の組み合わせがコール存続可能性を処理します。存続可能性 TCL スクリプトは、リモートゲートウェイからのすべての入力コールの SIP 接続をモニタします。シグナリング障害が発生した場合、TCL スクリプトはコールを制御し、設定可能な宛先にリダイレクトします。TCL スクリプトの接続先の選択肢は、Cisco IOS ゲートウェイ構成でパラメータとして構成されます。

**Note**

着信番号が「E164」フォーマットの場合、存続可能性スクリプトは Unified CVP に着信番号を転送する前に着信番号から「+」記号を削除します。Unified CVP または ICM は、DNIS の先頭にあり「+」サインインをサポートしません。

この転送の代替接続先には、別の IP 接続先（リモートサイトの SRST コールエージェントを含む）、コールの再起動、新しい接続先でのコールの再起動、\*8 TNT、またはフックフラッシュが含まれます。リモートサイトの SRST コールエージェントに転送する場合、最も一般的なターゲットは SRST エイリアスまたは基本 ACD ハントグループです。

音声メールおよび録音サーバは、Real-Time Control Protocol (RTCP) パケットを、発信者（TDM 音声ゲートウェイ）に逆方向に送信しません。これにより、存続可能性スクリプトのメディア非アクティブタイマーが誤ってトリガーされる可能性があります。survivability.tcl スクリプトは慎重にダイヤルピアに適用することが重要です。音声メールまたは録音要素にコールが送信された場合、コールはドロップする場合があります。1つの方法は、音声メールまたは録音コールに別個のダイヤルピアを使用し、これらのダイヤルピアには Unified CVP 存続可能性スクリプトを関連付けません。もう1つは、音声メールまたは録音ダイヤルピアに関連付けられている存続可能性スクリプトでメディア非アクティブを無効にする方法です。

これら転送方法の構成と適用に関しては、<http://www.cisco.com/c/en/us/support/customer-collaboration/unified-customer-voice-portal/products-installation-and-configuration-guides-list.html> の *Configuration Guide for Cisco Unified Customer Voice Portal* を参照してください。

**Note**

シグナリング障害で代替ルーティングを活用するには、Unified CVP をポイントしているすべてのゲートウェイで存続可能性サービスを使用します。このサービスの使用を妨げる特定の実装を利用しない限り、必ずこのサービスを使用してください。

存続可能性サービスが Unified CVP からの REFER メッセージを処理し、Unified CVP 包括コールフローで SIP REFER を使用する場合、ルータ再クエリはサポートされません。Cisco IOS が存続可能性サービスなしで REFER を処理する場合、または Unified CM が REFER を処理する場合、他のコールフローは REFER を使用したルータの再クエリをサポートできます。サードパーティ製の SIP トランクの場合、REFER を使用したルータ再クエリのサポートは、SIP REFER 自体の実装とサポートによって異なります。

## オプションのシスココンポーネント設計上の考慮事項

### Customer Collaboration Platform 設計の考慮事項

大規模なシングルサーバとして Customer Collaboration Platform を展開します。Customer Collaboration Platform は、高可用性の目的で冗長トポロジをサポートしません。

「イントラネット」および「インターネット」のトポロジの企業ファイアウォールの内外にサーバを展開できます。

- イントラネットトポロジは、ネットワークファイアウォールのセキュリティを強化して、外部パーティによりシステムがアクセスされるリスクを軽減します。Customer Collaboration Platform が、内部フォーミュラサイトなどの内部フォーミュラにアクセスする際に、このトポロジを使用します。

イントラネットトポロジを使用するとプロキシ構成が複雑になりますが、ディレクトリの統合はシンプルになります。

- インターネットトポロジは、ネットワークファイアウォール外に Customer Collaboration Platform を配置します。これは、Customer Collaboration Platform アプライアンスのビルトインされたセキュリティキャパシティに依存しています。

このトポロジのセキュリティを許容するかどうかは、システムの使用方法および会社のポリシーによって決めます。

インターネットトポロジでは、ディレクトリの統合が複雑になる可能性があります。

Customer Collaboration Platform を展開すると、ユーザの一部は、ファイアウォールまたはプロキシを介してサーバにアクセスできます。

### Customer Collaboration Platform 管理 UI アクセス

デフォルトでは、Customer Collaboration Platform 管理ユーザインターフェースへのアクセスは制限されています。管理者は、クライアントの IP アドレスをホワイトリストに登録してアクセスを提供し、ホワイトリストからクライアントの IP を削除してアクセスを取り消すことができます。

クライアントの IP アドレスをホワイトリストに登録するには、<https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-feature-guides-list.html> の Cisco Unified Contact Center Enterprise 機能ガイドのタスクルーティングセクションにあるホワイトリストコマンドを参照してください。

### Customer Collaboration Platform MR PG 暗号化

Unified CCE 管理システムインベントリで Customer Collaboration Platform を外部マシンとして構成する場合、MR PG サーバを構成し、Customer Collaboration Platform UI でマルチチャネルルーティングの CCE 構成ドロワーを開きます。

メディアルーティングインターフェイスのセキュアなトランスポートモードを有効にするには、セキュリティ保護 (TLS) チェックボックスを使用します。

- オンにすると、MR 通信が TLSv1.2 チャンネルを介して保護されます。
- MR通信はプレーンな TCP チャンネル経由となります。

## タスクルーティングに関する考慮事項

### タスクルーティング

タスクルーティングは、異なるメディアチャンネルからコンタクトセンターのエージェントに要求をルーティングするシステムの機能です。

音声通話、Eメール、チャットなどの組み合わせを処理するようにエージェントを設定できます。たとえば、エージェントが音声、Eメール、およびチャットを処理する場合、3種類のメディアルーティングドメイン（MRD）でスキルグループまたはプレジジョンキューのメンバーとしてエージェントを設定することができます。メディアを問わず、ビジネスルールに基づいてこれらのエージェントに要求を送信するようにルーティングスクリプトを設計できます。複数のMRDにサインインしたエージェントは、タスク単位でメディアを切り替えることができます。

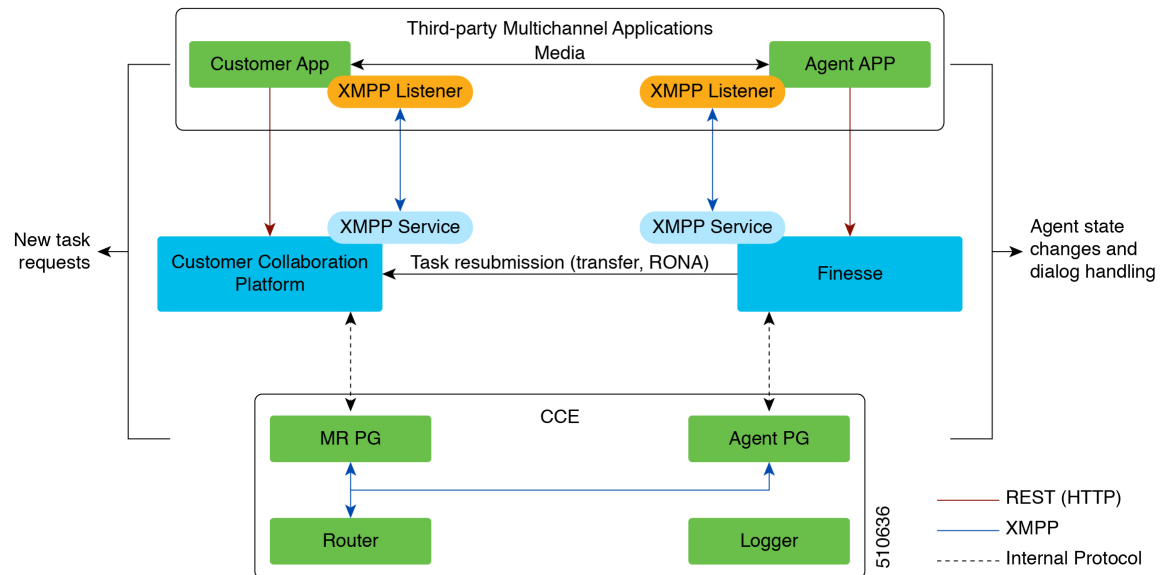
ビジネスチャットおよびEメール追加設定なしで、ユニバーサルキューを提供します。サードパーティマルチチャンネルアプリケーションは、タスクルーティングAPIを使用してCCEと統合することによって、ユニバーサルキューを使用することができます。

タスクルーティングAPIは、CCEでのサードパーティのマルチチャンネルタスクを要求、キューイング、ルーティング、および処理する標準的な方法を提供します。

コンタクトセンターのカスタマーまたはパートナーは、タスクルーティングを使うため、Customer Collaboration Platform および Finesse API を使用してアプリケーションを開発できます。Customer Collaboration Platform Task API は、アプリケーションを有効にして、CCE に非音声タスクリクエストを送信します。Finesse API は、エージェントがさまざまなタイプのメディアにサインインし、タスクを処理できるようにします。エージェントは各メディアにサインインし、独立してそれぞれの状態を管理できます。

Cisco のパートナーは、Cisco DevNet で入手できるサンプルコードを上記アプリケーションの構築ガイドとして利用することができます (<https://developer.cisco.com/site/task-routing/>)。

Figure 17: サードパーティのマルチチャネルアプリケーションソリューションコンポーネント用のユニバーサルキュー



### Customer Collaboration Platform と タスク ルーティング

サードパーティのマルチチャネルアプリケーションは、Customer Collaboration Platform Task API を使用して、音声以外のタスクを CCE に送信します。

この API は、Customer Collaboration Platform タスクフィード、キャンペーン、および通知と連携し、コンタクトセンターにタスクの要求を渡してルーティングさせます。

Task API は、タスクの要求でのコール変数および ECC 変数の使用をサポートします。これらの変数は、チャットルームの URL や E メール処理といったメディアの属性など、顧客固有の情報を要求で送信するために使用されます。



#### Note

CCE ソリューションでは、Finesse および Customer Collaboration Platform で使用される拡張コールコンテキスト変数およびコール変数について、Latin 1 文字セットのみがサポートされています。アレイはサポートされていません。

### CCE および タスク ルーティング

Cisco Unified CCE は、タスクルーティングの一部として以下の機能を提供します。

- タスクの要求を処理します。
- タスクの要求の待機時間を予測します。
- エージェントが選択されている場合に Customer Collaboration Platform を通知します。

- スキルグループまたはプレジジョンキューベースのルーティングを使用して、エージェントにタスクの要求をルーティングします。
- メディア全体のコンタクトセンターアクティビティについて報告します。

### Finesse および タスク ルーティング

Finesse は、Media API および Dialog API 経由で タスク ルーティング 機能を提供します。

Media API の場合、サードパーティのマルチチャネルアプリケーションを使用するエージェントは、以下の処理が可能です。

- 別の MRD にログインします。
- 別の MRD で状態を変更します。

Dialog API を使用すると、サードパーティのマルチチャネルアプリケーションを使用するエージェントは、別の MRD からのタスクを処理することができます。

### タスクルーティングの使用例

タスクルーティング API を使用して、CCE でサードパーティ製マルチチャネルタスクを要求、キュー、ルーティング、および処理します。

次の使用例がサポートされています。

- 1 つの Media Routing Domain (MRD) の複数の同時タスクを MRD 内で処理するエージェント。
- 割り込み可能 MRD これら MRD のタスクを処理するエージェントは、別の MRD のタスクによって中断される場合があります。たとえば、電子メール MRD を中断可能にセットすると、電子メールのタスクを処理しているエージェントは、音声通話やチャットなどの別の MRD からのタスクによって中断される場合があります。
- 指定されたスクリプトセレクタへのブラインド転送。直接転送はサポートされていません。
- 割り当てられたタスクを使用してエージェントがサインアウトします。これらのタスクは、Finesse Media API のエージェントの dialogLogoutAction 設定に応じて、閉じたり転送されます。
- RONA. エージェントが、MRD のタイムアウト開始しきい値以内にオファーされたタスクを受け入れない場合、Finesse はルーティング用にタスクをサイド提出し、そのエージェントをルーティング可能にします。

### タスクルーティング タスク フロー

このタスクフローでは、エージェントが電子メールとチャットタスクを処理するように構成されている一般的なマルチチャネルシナリオについて説明します。

電子メールメディアルーティングドメイン (MRD) は割り込み可能であり、エージェントは、その MRD で割り込みを許可するよう構成されます。電子メール MRD は、割り込み可能なので、別の MRD からのタスクが電子メールタスクを処理するエージェントに割り込むことができます。



エージェントが割り込みを受け入れるように構成されているため、別のMRDからのタスクがエージェントに割り当てられると、電子メールMRDでのエージェントの状態、電子メールタスク、Finesse ダイアログは、[割り込み中 (INTERRUPTED)] に変わります。割り込み中、エージェントは、電子メールタスクの作業を行うことはできません。

チャットMRDは中断できません。

MRDの中断および中断の許可、却下に関しては、<https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-feature-guides-list.html> の *Cisco Unified Contact Center Enterprise* 機能ガイドを参照してください。

パートナーは、Finesse および Customer Collaboration Platform API に統合された電子メールおよびチャットアプリケーションを開発しました。

1. カスタマーが会社の電子メールを送信します。電子メールアプリケーションは、新規電子メールタスクリクエストをCCEに送信します。タスクリクエストには、スクリプトセレクト、電子メールへの処理を含むカスタマー固有の情報が入った Call および ECC 変数が含まれます。
2. CCEが、スクリプトセレクトを通話タイプにマッピングすると、どのルーティングスクリプトが実行されるか決まります。ルーティングスクリプトは、電子メールタスクを電子メールMRDの適切なスキルグループまたはポスト コール調査にキューします。
3. 電子メールアプリケーションは、ステータスと推定待機時間 (EWT) をポーリングします。
4. エージェントが、電子メールMRDにサインインすると、ステータスが [準備完了 (Ready)] に変わります。
5. CCEは、電子メールをエージェントに割り当てます。タスクを作成するために使用する Call および ECC 変数は、ダイアログ メディア プロパティに含まれます。アプリケーションはこれらの変数を使用して、エージェントが電子メールに返信できるようにします。エージェントは Finesse の電子メールダイアログで作業を開始します。
6. 別のカスタマーがチャットリクエストを会社に送信します。チャットアプリケーションは、CCEに新しいチャットタスクリクエストを送信します。コール変数とECC変数には、チャットルームのURLが含まれます。
7. CCEが、チャットリクエストで送信されたスクリプトセレクトをコールタイプにマッピングすると、どのルーティングスクリプトを実行するかが決まります。ルーティングスクリプトは、チャットタスクをチャットMRDの適切なスキルグループまたはポスト コール調査にキューします。
8. チャットアプリケーションは、ステータスと推定待機時間 (EWT) をポーリングします。
9. 電子メールタスクの作業中に、同じエージェントがチャットMRDにサインインするとステータスが [準備完了 (Ready)] に変わります。
10. CCEは、チャットタスクをエージェントに割り当てます。アプリケーションは、Call および ECC 変数を使用して、エージェントをカスタマーとのチャットルームに追加します。エージェントは Finesse のチャットメールダイアログで作業を開始します。

11. 電子メール MRD のエージェントのステータスは [割り込み中 (Interrupted)] に変わり、電子メールダイアログのステータスが [割り込み中 (Interrupted)] に変わります。アプリケーションは、電子メールダイアログのアクションを無効にします。
12. エージェントは、チャットタスクを別のスクリプトセクタに転送します。Finesse はチャットダイアログを閉じ、タスクを Customer Collaboration Platform に再送信します。アプリケーションはチャットルームを閉じます。
13. エージェントは他の非割り込みダイアログを処理せず、電子メールダイアログはアクティブになります。
14. エージェントは、電子メールダイアログの作業を続行します。エージェントは、ダイアログを一時停止して、短い休憩を取り、ダイアログを再開します。
15. 電子メールの返信が完了すると、エージェントはそのダイアログのまとめ作業を実行します。エージェントはダイアログを閉じます。Finesse は、電子メールタスクのために Customer Collaboration Platform にハンドイベントを送信します。アプリケーションは、カスタマーに対して電子メールの返信を送信します。

## タスクルーティング設計への影響

### 企業リファレンス設計タスク ルーティング サポート

すべてのソリューションは、タスクルーティングをサポートしますが、コンタクトセンター用の HCS の小規模コンタクトセンター ソリューションは例外です。

### タスクルーティングの導入要件

#### タスク ルーティング サードパーティ製マルチチャネル アプリケーションの導入要件

- Finesse および Customer Collaboration Platform が必要です。タスクルーティングに対してシステムを構成する前に Finesse および Customer Collaboration Platform をインストールし、構成してください。

<https://www.cisco.com/c/en/us/support/customer-collaboration/finesse/tsd-products-support-series-home.html> にある Finesse のマニュアルを参照してください。

<https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-express/tsd-products-support-series-home.html> の Customer Collaboration Platform ドキュメントを参照してください。

[ホワイトリスティング機能 (Whitelisting Feature)] 項で記載されている Customer Collaboration Platform サーバのホワイトリスティング手順を完了してください。

- 展開環境にインストールできる Customer Collaboration Platform マシンは 1 つのみです。
- Customer Collaboration Platform は、Media Routing Peripheral Gateway (MR PG) の一方の側と地理的に同じ場所である必要があります。
- CCE、Finesse およびサードパーティ製マルチチャネル Customer Collaboration Platform タスクルーティングアプリケーションがネットワーク上でアクセスできる場所に Customer Collaboration Platform をインストールします。

DMZ に Customer Collaboration Platform をインストールする場合は、CCE と Finesse のポートを開いて接続します。Customer Collaboration Platform に接続する CCE のデフォルトポートは 38001 です。Finesse は Customer Collaboration Platform over HTTPS、ポート 443 経由で接続されます。

Customer Collaboration Platform を使いローカルにサードパーティ製マルチチャネルアプリケーションをインストールするか、アプリケーションを接続するために、Customer Collaboration Platform サーバでポートを開きます。

#### タスクルーティングのサイジングとキャパシティの制限

サードパーティ製マルチチャネルアプリケーションのタスクルーティングのサイジングとキャパシティ制限は次のとおりです。

- システムごとのマルチメディアエージェントの最大数: 2,000 エージェント
- 1 時間あたりの最大タスク数: 15,000 タスク
- 同時タスクの最大数: 20,000 タスク
- すべてのエージェントの MDS にわたるエージェントごとの最大タスク: 5 タスク
- 単一 MRD に置けるエージェントごとの最大タスク数: 5 タスク
- タスク送信率: 毎秒 5 タスク

Customer Collaboration Platform は、CCE に対するタスク送信率を毎秒 5 タスクに調整します。Customer Collaboration Platform は、送信の目的でキューに最大 10,000 タスクを保持します。キューが 1 万タスクを超えると、Customer Collaboration Platform は、廃棄コード NOTIFICATION\_RATE\_LIMITED で、追加タスクを破棄します。キューが再度対応可能になると、追加のタスクがキューに追加されます。

#### タスクルーティングの帯域幅、遅延、QoS に関する考慮事項

Customer Collaboration Platform に関して、HTTP を確実にサポートするためにネットワークに十分な帯域幅が必要です。タスクルーティング REST API 要求はメタデータのみを伝送します。メディアは伝送しません。カスタマーアプリケーションが、タスクステータス通知を受け取るために XMPP を介して Customer Collaboration Platform に接続されている場合、ネットワークは、Customer Collaboration Platform XMPP サーバとの永続的な TCP 接続を確実にサポートする必要があります。XMPP を介した Customer Collaboration Platform への接続は、ネットワーク帯域幅に大きな影響を及ぼしません。

Finesse デスクトップのタスクルーティングタスクに必要な帯域幅を計算するには、*Finesse Bandwidth Calculator* (<https://www.cisco.com/c/en/us/support/customer-collaboration/finesse/products-technical-reference-list.html>) を使用します。

CCE では、タスクルーティングタスクの帯域幅、遅延、QoS に関する考慮事項は、音声コールに対する考慮事項と同様です。タスクルーティングタスクは、音声コールと同じ帯域幅を使用します。

## Related Topics

[Unified CCE の帯域幅、遅延、および QoS](#)

# Unified SIP プロキシ設計上の考慮事項

ソリューションに Cisco Unified SIP Proxy (CUSP) を追加する際は、次の点を検討してください。

- CUSP は、UCS B、C、および E シリーズのサーバに配置できる VM です。
- 標準規格の CUSP トポロジは、地理的に分離された 2 つの冗長ゲートウェイで構成されています。ゲートウェイには、それぞれ 1 つのプロキシモジュールがあります。プロキシの冗長性には SRV 優先順位が使用されます。HSRP は使用しません。
- CUSP は、VXML または TDM ゲートウェイとコアサイドに接続できます。
- SRV またはダイヤルピア設定を使用して TDM ゲートウェイを構成すると、プライマリおよびセカンダリ CUSP プロキシが使用できます。
- プライマリとバックアップの Unified CVP、Unified CM、および VCM ゲートウェイを検索するには、サーバグループを使用して CUSP を設定します。
- Unified CVP は、サーバグループを使用して設定され、プライマリ CUSP プロキシおよびセカンダリ CUSP プロキシを使用します。
- Unified CM は、複数の SIP トランクを持つルートグループを使用して設定され、プライマリ CUSP プロキシおよびセカンダリ CUSP プロキシを使用します。

## CUSP 展開のパフォーマンス マトリクス

プロキシ上での分離での CUSP の基準値テストでは、毎秒最大キャパシティで 450 TCP トランザクションになります。これを最高ベンチマークとして使用し、最も重視する条件の許容値として使用します。プロキシサーバの観点からすると、CVP コールによって、平均で 4 つの個別の SIP コールが生成されます。

- 発信者の着信レグ
- VXML 発信レグ
- 着信音の発信レグ
- エージェントの発信レグ

CVP キューイングとのコンサルトが発生すると、セッションでさらに 4 つの SIP トランザクションが発生し、実質的にコール数が 2 倍になります。

レコードルートは、CUSP でデフォルトでオフになります。



**Note** プロキシサーバでは、レコードルート設定は常にオフにしておきます。これにより、シングルポイント障害が回避され、フォールトトレラントルーティングが許可され、プロキシサーバのパフォーマンスが向上します。プロキシサーバの設定を使用すると、パフォーマンスへの影響が倍増します。また、高可用性モデルが壊れます。プロキシがダウンした場合、プロキシは、コールに対してシングルポイント障害となります。

## CUSP によるコール廃棄

ここでは、SIP を使用した Cisco IOS ゲートウェイ構成について説明します。以下の例では、特定の構成概念を強調表示しています。

### Cisco IOS ゲートウェイの構成

Cisco IOS ゲートウェイでは、ダイヤルピアを使用して、ディレクトリ番号を照会します。接続先は SIP Proxy サーバ、DNS、SRV または IP アドレスに指定できます。次の例に、SIP プロキシの IP アドレスを使用して、コールを SIP Proxy サーバに送信する Cisco IOS ゲートウェイ構成を示します。

```
sip-ua
  sip-server ipv4:10.4.1.100:5060

dial-peer voice 1000 voip
  session target sip-server
...
```

ダイヤルピアの **sip-server** コマンドは、Cisco IOS ゲートウェイに **sip-ua** 設定で構成した全体的に定義された SIP サーバを使うように指示します。冗長性のために複数の SIP プロキシを設定するためには、次の例に示すように、IP アドレスを DNS SRV レコードに変更できます。DNS SRV レコードでは、単一の DNS 名を複数のコールサーバにマップできます。

```
sip-ua
  sip-server dns:cvp.cisco.com

dial-peer voice 1000 voip
  session target sip-server
...
```

代わりに、次の例に示すように、複数の SIP Proxy サーバを直接指すように複数のダイヤルピアを構成できます。このコンフィギュレーションでは、DNS を使用する代わりに IP アドレスを指定できます。

```
dial-peer voice 1000 voip
  session target ipv4:10.4.1.100
  preference 1
...
dial-peer voice 1000 voip
  session target ipv4:10.4.1.101
  preference 1
...
```

前の例では、ダイヤルプランの解決およびコールルーティングのためにコールが SIP Proxy サーバに送信されます。Unified CVP コールサーバが複数ある場合、SIP Proxy サーバは、負荷分散および冗長性のために複数のルートを使用して構成されます。Cisco IOS ゲートウェイでは、SIP Proxy

サーバを使用せずに、負荷分散および冗長性を実現できます。次の例では、3つの Unified CVP コールサーバ間でコールを負荷分散するように、複数のダイヤルピアを使用した Cisco IOS ゲートウェイ構成を示します。

```
dial-peer voice 1001 voip
  session target ipv4:10.4.33.131
  preference 1
...
dial-peer voice 1002 voip
  session target ipv4:10.4.33.132
  preference 1
...
dial-peer voice 1003 voip
  session target ipv4:10.4.33.133
  preference 1
...
```

DNS SRV レコードによって、管理者は、DNS ラウンドロビン冗長性およびロードバランシングを使用した場合よりも詳細に冗長性およびロードバランシングを設定できます。DNS SRV レコードを使用すると、特定のサービス（この場合のサービスは SIP）に対して使用しなければならないホストを定義できます。また、これらのホスト間での負荷分散の特性を定義できます。次の例では、上記のように構成された3つのダイヤルピアによって提供される冗長性が、DNS SRV レコードを使用して、単一ダイヤルピアに置き換えられるケースを示しています。DNS ルックアップを行うためには、DNS サーバが必要であることに注意してください。

```
ip name-server 10.4.33.200
dial-peer voice 1000 voip
  session target dns:cvp.cisco.com
```

Cisco IOS ゲートウェイでは、静的ホストレコードと同様に、DNS SRV レコードを静的に定義できます。この機能を使用すると、DNS SRV 負荷分散および冗長性を実現しながら、ダイヤルピア構成を簡素化できます。この方法には、SRV レコードの変更が必要な場合、集中型 DNS サーバではなく各ゲートウェイで設定を変更する必要があるという欠点があります。次の例は、cvp.cisco.com で処理された SIP サービスの静的 SRV レコードの構成を示します。cvp.cisco.com の SIP SRV レコードは、3 台のサーバ間で負荷分散を行うよう構成されます。

```
ip host cvp4cc2.cisco.com 10.4.33.132
ip host cvp4cc3.cisco.com 10.4.33.133
ip host cvp4cc1.cisco.com 10.4.33.131
```

(SIP/TCP の SRV レコード)

```
ip host _sip._tcp.cvp.cisco.com srv 1 50 5060 cvp4cc3.cisco.com
ip host _sip._tcp.cvp.cisco.com srv 1 50 5060 cvp4cc2.cisco.com
ip host _sip._tcp.cvp.cisco.com srv 1 50 5060 cvp4cc1.cisco.com
```

(SIP/UDP の SRV レコード)

```
ip host _sip._udp.cvp.cisco.com srv 1 50 5060 cvp4cc3.cisco.com
ip host _sip._udp.cvp.cisco.com srv 1 50 5060 cvp4cc2.cisco.com
ip host _sip._udp.cvp.cisco.com srv 1 50 5060 cvp4cc1.cisco.com
```

## SIP プロキシのダイヤルプラン構成

SIP プロキシがある場合は、Unified CM ルーティングクライアントと CVP ルーティングクライアントに異なる VRU ラベルを使用します。Unified CM ルーティングクライアントは、VRU ラベルを使用して、CVP コールサーバにコールを送信して、最初に呼制御を受け渡します。CVP ルーティングクライアントは、VRU ラベルを使用して、処理のために VXML ゲートウェイにコール

を送信します。コールが CVP になると、CVP は CVP ルーティングクライアントの VRU ラベルに転送します。その後、VXML ゲートウェイにコールを送信し、キュー処理を行います。

SIP プロキシでダイヤルプランを次のように構成します。

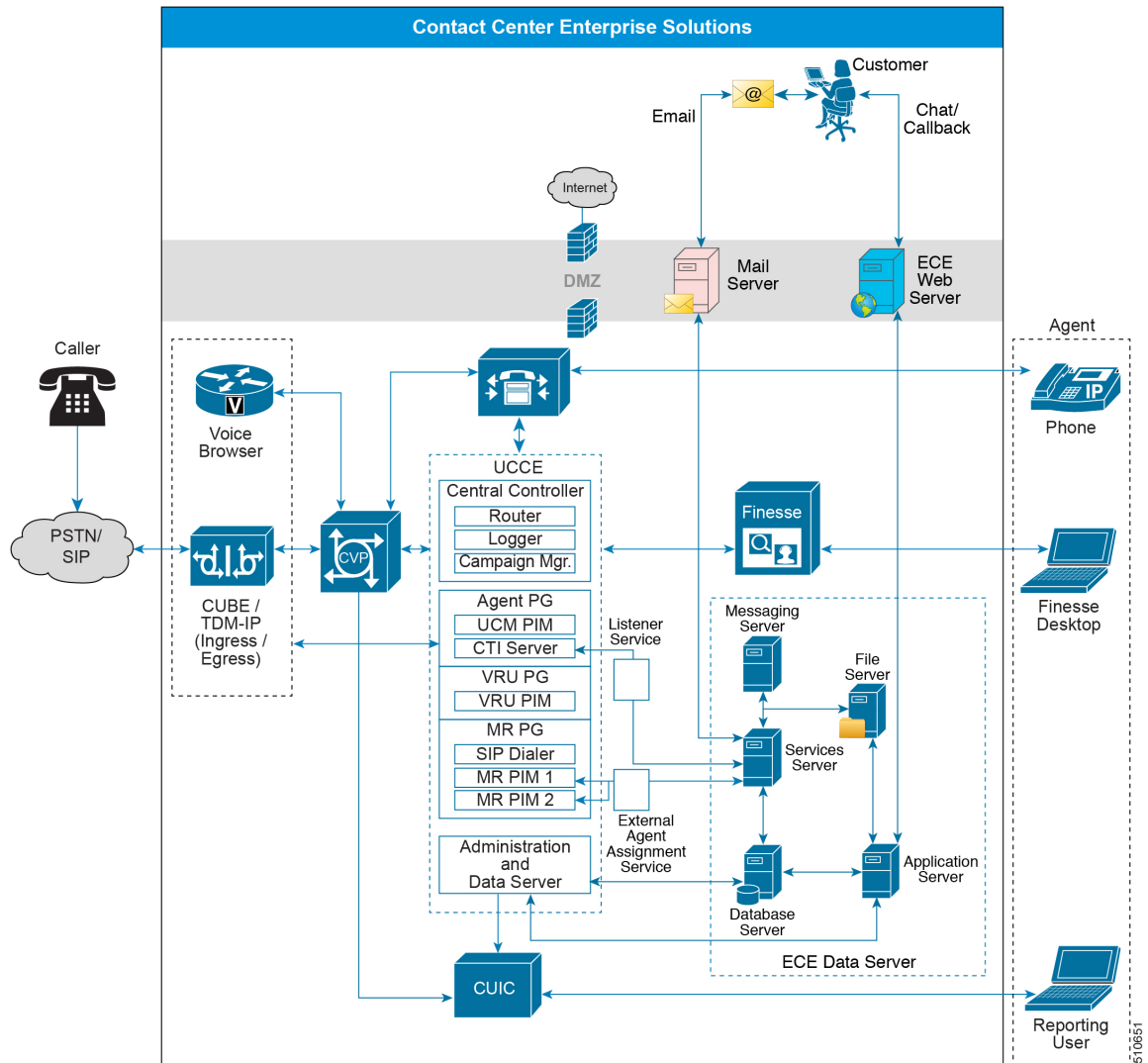
```
[Unified CM routing client VRU label + correlation-id]: pointing to CVP servers  
[CVP routing client VRU label + correlation-id]: pointing to VXML Gateways
```

## Enterprise Chat and Email の設計上の考慮事項

ビジネス チャットおよび E メールによって、エージェントと管理者は共通の Web サーバとページを通じて、Web と Eメールのインタラクションを管理できます。この機能は Contact Center Enterprise ソリューションと統合され、さまざまなメディアチャネルからエージェントへのコンタクトのユニバーサルキューイングを提供します。

アーキテクチャおよび設計の詳細については、『Enterprise チャットおよび Eメール設計ガイド』（<http://www.cisco.com/c/en/us/support/customer-collaboration/cisco-enterprise-chat-email/products-implementation-design-guides-list.html>）を参照してください。

Figure 18: Enterprise Chat and Email の設計上の考慮事項



## ビジネス チャットおよび E メール 展開オプション

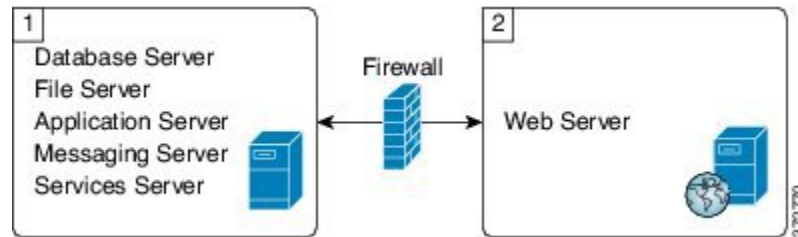
モジュラーおよびコンポーネントベースのアーキテクチャが原因で、ビジネス チャットおよび E メール（ECE）同時ユーザ負荷に対する増幅した需要に対応します。さまざまなサイズの導入に適した柔軟性を提供するために、ECE ソリューションは、ソリューション内のさまざまなサーバに分散できるさまざまなコンポーネントをサポートしています。

### 併置展開

同じ場所に配置された展開では、Web サーバを 1 つのサーバにインストールし、他のすべてのコンポーネントを別のサーバにインストールします。必要に応じて、ファイアウォールの外部に Web サーバをインストールできます。



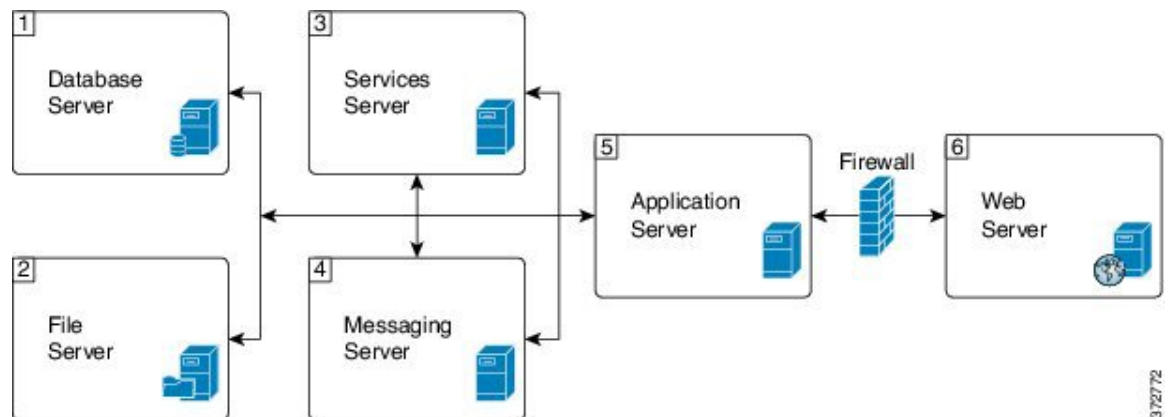
Figure 19: 併置展開



### 分散型サーバの展開

分散型サーバの展開では、各コンポーネントをファイアウォールの外部にWebサーバを持つ別のサーバにインストールします。他のサーバを再起動しなくても、この構成では、アプリケーション、メッセージ、サービスそしてWebサーバは個別に再起動できます。

Figure 20: 分散型サーバの展開



## サイレントモニタリングの設計上の考慮事項

チームを管理しているスーパーバイザの場合は、Unified CM ベースのサイレントモニタリングの非干渉メカニズムを利用して、エージェントの音声コールをモニタできます。

従来の SPAN ベースのサイレントモニタリングは、非リファレンス設計に対してのみサポートされます。

### Unified CM ベースのサイレントモニタリング設計上の考慮事項

#### Unified CM ベースのサイレントモニタリングコールフロー

Cisco Finesse は、Unified CM のサイレントモニタリングを介してサイレントモニタリング機能を提供します。Cisco Finesse は、Unified CM サイレントモニタリング機能時に、以下のように動作します。

- サイレントモニタリングを開始するため、スーパーバイザアプリケーションは、Cisco Finesse サーバに REST 要求を送信します。

2. サイレント モニタリング セッションを開始するため、Cisco Finesse サーバは、AgentSuperviseCall() メッセージを Unified CCE に送信します。
3. Unified CCE は、Unified CM に CallStartMonitor() メッセージを送信します。
4. Unified CM はスーパーバイザの電話機に対し、エージェント電話機の組み込みブリッジ (BIB) にコールするよう指示します。
5. スーパーバイザの電話機は、エージェント電話機で BIB をコールします。
6. エージェントの電話機は、エージェントの音声ストリームと顧客の音声ストリームの組み合わせを転送します。
7. Unified CM は、サイレント モニタリング コールのコールイベントを Unified CCE に送信します。
8. Unified CCE は、Cisco Finesse サーバに更新イベントを送信します。
9. Cisco Finesse サーバは、Cisco Finesse スーパーバイザアプリケーションに XMPP アップデートを送信します。

Cisco Finesse では、モバイルエージェントのサイレントモニタリングはサポートされません。スーパーバイザは、モバイルエージェントをサイレントモニタリングできず、モバイルスーパーバイザは、サイレントモニタリングを実行できません。

スーパーバイザは、Cisco Finesse IP Phone からサイレントモニタリングを実行できません。スーパーバイザは、Cisco Finesse デスクトップからのサイレントモニタリングのみ実行できます。

### Unified CM ベースのサイレントモニタリングの影響

Unified CM は、スーパーバイザ (監視) デバイスとエージェント (監視対象) デバイスの間のコールを使用してサイレントモニタリングを行います。エージェントの電話機はエージェントの会話をミックスしてスーパーバイザの電話機に送信し、スーパーバイザに再生します。

Unified CCE は、Unified CM で利用可能なサイレント モニタリング機能をサポートしています。Unified CM のサイレント モニタリングでは、同じエージェント電話に対して1つのサイレントモニタリングセッションおよび1つの録音セッションのみがサポートされます。



#### Note

Unified CM サイレント モニタリングは、モバイル エージェントはサポートしていません。

以下の条件に該当する場合、Unified CM サイレントモニタリングは、任意の Unified CCE エージェントデスクトップを監視できます。

- 監視対象のエージェントは、互換性のある Cisco Unified IP Phone または Cisco IP Communicator を使用します。ソリューションの詳細に関しては、「互換性マトリクス」を参照してください。
- コンタクトセンターでは、互換性のあるバージョンの Cisco Unified CM が使用されています。使用するソリューションの詳細については、互換性マトリクスを参照してください。

スーパーバイザは、Cisco IP Communicator を含む任意の Cisco IP 電話を使用してエージェントをサイレントモニタできます。

Unified CM サイレント モニタリングは、Unified CM で提供されるその他のコール制御機能 (会議や転送など)と同様に動作します。サイレントモニタリングのセッションが開始されると、デスクトップは Unified CCE を介してメッセージを送信し、サイレントモニタが実行されている電話機に送信します。

Unified CCE および Unified CM を介したメッセージングは、Unified CCE のパフォーマンスに影響を及ぼします。

## サードパーティ コンポーネント設計上の考慮事項

サードパーティ製コンポーネントが CTI サーバを介して Unified CCE に接続する場合は、次の設計上の考慮事項に注意してください。

### All-Event クライアントの制限

CTI サーバは、All-Event クライアントを使用します。

#### 最大 2 台の vCPU 小規模エージェント PG OVA

各エージェント PG では、CTI サーバ上に最大 7 つの All-Event クライアントを作成できます。Cisco Finesse は、次の 2 つのクライアントを使用します。

#### vCPU 大規模エージェント PG OVA を最大 4 個まで

vCPU を 4 つ使用する大規模 OVA から作成された VM は、より多くの All-Event クライアントとモニタモード接続をサポートできます。各エージェント PG では、CTI サーバ上に最大 20 つの All-Event クライアントを作成できます。Cisco Finesse は、次の 2 つのクライアントを使用します。

#### All-Event クライアント

Cisco Finesse デスクトップ ソリューションは、2 つの利用可能な All-Event クライアントを使用します。他に考えられるクライアントの消費者の一部を次に示します。

- Outbound Dialer
- リアルタイム遵守 (2)
- 一部のサードパーティ製録音ベンダー (2)
- ビジネス チャットおよび E メール (2)
- B+S CRM コネクタ

## DNSサーバ導入に関する考慮事項

ソリューション用の DNS サーバを設定する際は、以下を考慮してください。

- DNS サーバを逆引き参照用に設定する。
- NAT ネットワーク境界を超えて DNS サーバを設定しない。
- 検索を実行するサーバとの接続に低遅延の冗長 DNS サーバを配置する。

## ロードバランサの設計上の考慮事項

### Cisco Finesse サインイン向けロードバランサ

エージェントが Cisco Finesse デスクトップにサインインすると、Cisco Finesse デスクトップクライアントは両方の Cisco Finesse サーバの IP アドレスをキャッシュします。Cisco Finesse サーバがサービス停止中の場合、Cisco Finesse クライアントは、自動的にエージェントをリダイレクトし、別の Cisco Finesse サーバにサインインさせます。このクライアント側のロジックを考えると、フェールオーバーの目的でロードバランサを使用することはできません。

ただし、次の2つのシナリオでは、Cisco Finesse でロードバランサを使用できます。

**Note**

これらのシナリオは、Cisco Finesse デスクトップにのみ適用されます。これらのシナリオは、Cisco Finesse IP Phone エージェントには適用されません。

### Cisco Finesse サインインページにアクセスする方法

エージェントが停止しているまたは到達不可能な Cisco Finesse サーバに移動すると、エージェントはサインインページにアクセスできません。エージェントがエラーを受け取ると、他の Cisco Finesse サーバに手動でサインインする必要があります。この手動による手順を回避するために、URL リダイレクトモードのロードバランサを使用してエージェントをアクティブな Cisco Finesse サーバに送信できます。Cisco Finesse SystemInfo REST API には、Cisco Finesse サーバのステータスが表示されます。この API の詳細については、『Cisco Finesse Web サービス開発者ガイド』を参照してください。

Cisco Finesse サーバのステータスを決定するためにロードバランサを設定する場合は、次のコールフローを使用します。

1. エージェントは、ロードバランサにブラウザを向けます。
2. ロードバランサは、エージェントブラウザを適切な Cisco Finesse サーバにリダイレクトします。
3. エージェントは、直接 Cisco Finesse サーバにサインインします。この段階で、ロードバランサは、コールフローの一部ではなくなります。

### Cisco Finesse API の直接使用

Cisco Finesse REST API を直接使用している場合、コールフローは、Cisco Finesse クライアント側のフェールオーバーロジックを使用できません。高可用性を管理するためのロードバランサの使用を選択できます。ロードバランサはカスタムアプリケーションの一部で、すべてのカスタムアプリケーション同様、シスコではサポートされません。カスタマーまたはシスコパートナーがロードバランサに必要なサポートを提供します。

Cisco Finesse クライアントと Cisco Finesse サーバとの間には次の 2 つの接続があります。

- 要求と応答用の REST チャンネル
- サーバからクライアントに通知を送信する XMPP チャンネル

該当のクライアントに対する両方のチャンネルは、同じ Cisco Finesse サーバに接続する必要があります。ロードバランサを一方の Cisco Finesse サーバの REST 接続、およびもう一方の Cisco Finesse サーバの XMPP チャンネル接続に接続することはできません。このような設定は予期しない結果を招くだけでなく、サポートされてもいません。

## Cisco Unified Intelligence Center 向けロードバランサ

Unified Intelligence Center には、ロードバランサを使用してアクセスできます。次の条件が適用されます。

- ロードバランサでのセッションスティッキ性は、Unified Intelligence Center へのアクセスに必須です。
- ライブデータレポートは、ロードバランサを介してアクセスできません。
- CUIC ノードとブラウザクライアントが WAN で分割されている場合、ロードバランサはサポートされません。

## CVP 向けロードバランサ

Unified CVP ソリューションコンポーネントがあるロードバランサを使うと、HTTP、HTTPS、および MRCP トラフィックのロードバランサと高可用性を実現できます。ロードバランサは、VXML ゲートウェイと VXML サーバ間の VXML ページのレンダリングを分散できます。また、ロードバランサは、メディアサーバの VRU スクリプト実行用のメディアファイルのフェッチを展開することもできます。



**Note** ソリューションが、MRCPv2 の場合、負荷分散に CUSP を使用します。

CVP は現在、次の要件を満たすサードパーティ製のロードバランサをサポートしています。

- SSL オフローディングと SSL パススルーの両方のサポート
- ロードバランサ高可用性のサポート
- 必須セッションのスティッキ性は保持しない

- 永続性のため cookie を挿入
- 流通アルゴリズムはラウンドロビン

## Unified CCE 管理ツール向けロードバランサ

これらのシナリオでは、Unified CCE Administration ツールでロードバランサを使用できます。

### Unified CCE 管理サインインページに移動

管理者またはスーパーバイザが、ダウンしているか到達不可能なサーバの Unified CCE Administration ツールに移動すると、サインインページにアクセスできません。管理者またはスーパーバイザには、エラーが表示され、別のサーバの Unified CCE Administration に手動でサインインしなければなりません。この手動による手順を回避するために、URL リダイレクトモードのロードバランサを使用して、セッションをアクティブサーバにダイレクトします。

使用シナリオ

1. ユーザはブラウザをロードバランサに向けます。
2. ロードバランサは、ブラウザセッションを適切な Unified CCE Administration サーバにリダイレクトします。
3. ユーザは、Unified CCE Administration サーバに直接サインインします。

### Unified CCE 管理 API の直接使用

Unified CCE Administration REST API を直接使用する場合は、ロードバランサを使用して高可用性を管理できます。ロードバランサはカスタムアプリケーションの一部で、すべてのカスタムアプリケーション同様、シスコではサポートされません。カスタマーまたはシスコパートナーがロードバランサに必要なサポートを提供します。

## とロードバランサビジネス チャットおよび E メール

でロードバランサのリダイレクトモードを使用しないでください。ビジネス チャットおよび E メール

## 録音設計に関する検討事項

### ネットワークベースの録音設計に関する検討事項

ネットワークベースの録音（NBR）機能は、Real-time Transport Protocol（RTP）ストリームに対するソフトウェアベースのフォーキングをサポートします。メディアフォーキングを使用すると、1回の通話でオーディオとビデオのミッドコール複数ストリーム（またはブランチ）を作成できます。その後、データのストリームを別の通知先に送信できます。CUBE を使用してネットワークベースの録音を有効にするには、録音に関する構成ガイドを参照してください。特定のコマンドを構成するか、コールエージェントを使用できます。CUBE はレコーディングクライアント

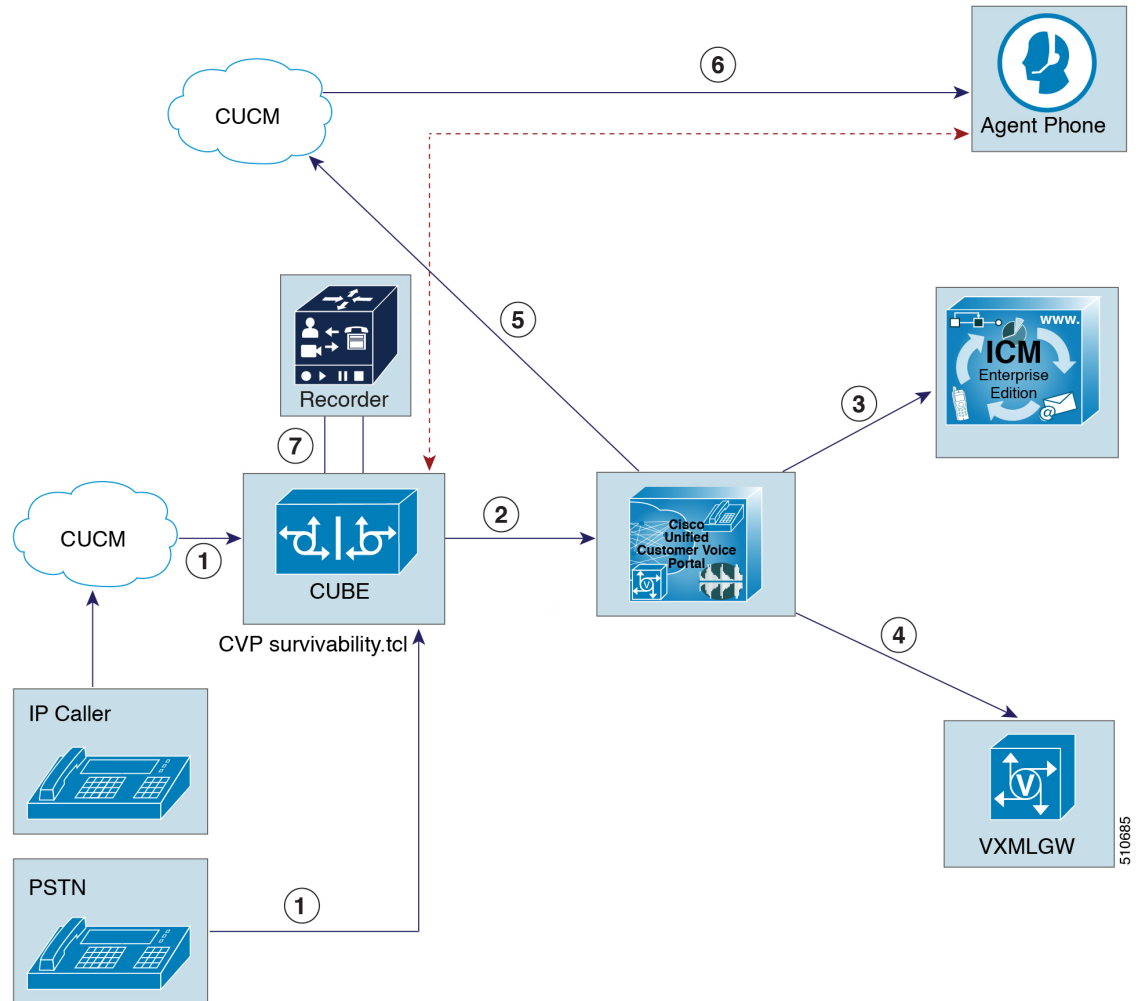


**Note** ネットワークベースの録音は、コール存続可能性機能と連携して機能します。

次の図は、ネットワークベースの録音のコールフローを示しています。

**Figure 21:** ネットワークベースの録音コールフロー

**Figure 22:** ネットワークベースの録音コールフロー



ネットワークベースの録音に関する一般的なコールフローは次のとおりです。

1. 着信コールが CUBE に到達します。
2. イングレスゲートウェイはそのコールを Unified CVP に送信します。
3. Unified CVP は、着信コールリクエストを Unified CCE に送信し、VRU ラベルを取得します。
4. Unified CVP から VXML ゲートウェイにコールが送信されます。発信者に VRU が再生されません。ただし、コールは記録されません。

5. エージェントが利用可能になると、Unified CVP は発信者とエージェントを接続します。
6. この会話に対してネットワークベースの録音が始まります。

## ネットワークベースの録音の制限

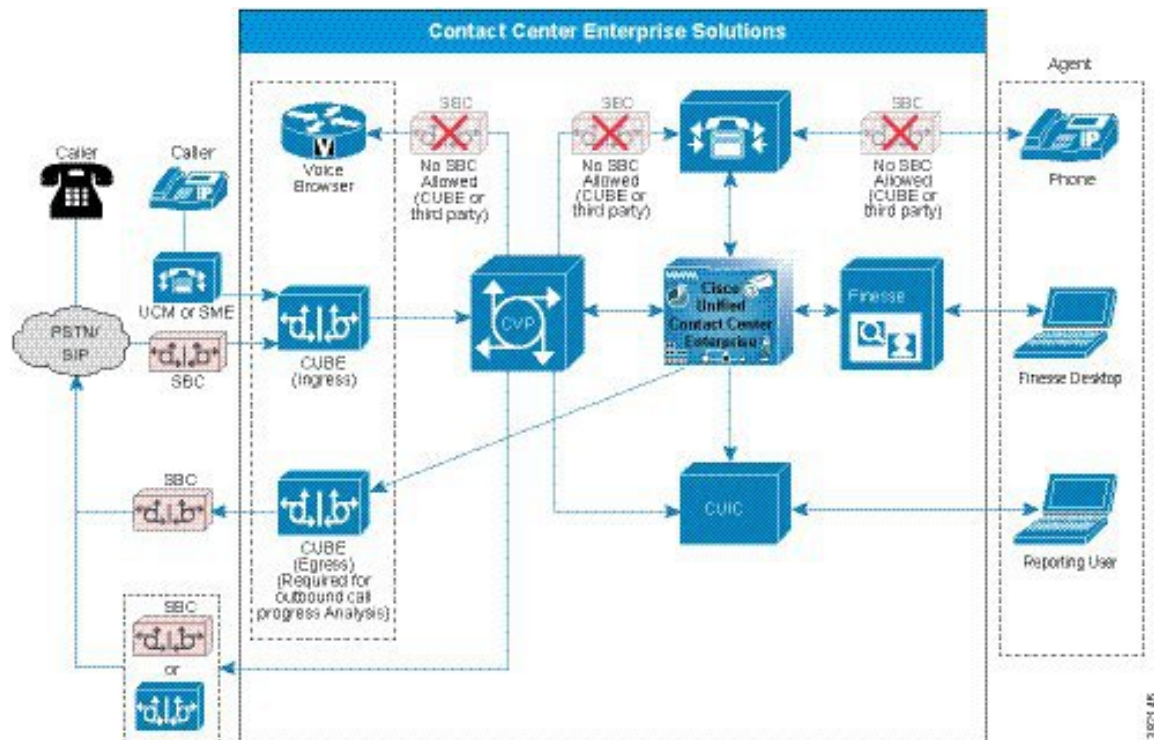
- エージェント間の通話転送では、ネットワークベースの録音は機能しませんが、電話ベースの録音は機能します。ネットワークベースの録音を使用する場合は、Unified CVP と Unified CM 間で ISR ゲートウェイを使用できます。
- NBR 機能は IOS イメージトレインでのみサポートされます。サポートされている IOS イメージトレインの詳細については、ご使用のソリューション向けの「互換性マトリックス」を参照してください。

## セッションボーダーコントローラ

サードパーティ製のセッションボーダーコントローラ（SBC）を、PSTN とコンタクトセンター間の入力境界または出力境界要素として使用できます。ほとんどのソリューションは、すべての Contact Center Enterprise 機能をサポートするためサードパーティ製 SBC および Unified CVP 間の CUBE を要求します。導入環境では、他のほとんどの通信レグにある SBC を使用することはできません。

次の図は、SBC を使用できる場所と使用できない場所を示しています。

Figure 23: SBC の実装







**Note** CUBE には SBC 機能と Contact Center Enterprise 向けの機能の両方が含まれます。CUBE を、SBC 機能のみを提供するサードパーティ製 SBC に置き換えることができます。ソリューションには、Contact Center Enterprise 機能の CUBE が必要です。

サードパーティ製 SBC のテストは積極的にテストしていません。

展開に SBC を追加検討する場合、次の一般設計ガイドラインと制限事項を考慮してください。

#### サポートポリシー

相互運用性の問題がある場合、シスコは、コールフローから SBC を一時的に削除するよう要求する場合があります。SBC なしで問題が見つからない場合は、Cisco TAC がケースをその SBC のメーカーに引き渡します。

## CUBE なしのサードパーティ SBC の使用

SIP PSTN サービスプロバイダーを含むサードパーティの SIP デバイスに接続する場合は、CUBE を使用します。Unified CVP と SIP デバイスの間に CUBE を配置しない場合は、双方が完全な統合テストと互換性を持ち合っている必要があります。

CUBE なしで PSTN SIP トランキングサービスに接続する場合は、コンタクトセンターとサービスプロバイダー間の接続を保護する方法を慎重に検討してください。NAT を実行してアドレスを非表示化する方法も検討してください。それ以外の場合、サービスプロバイダーネットワークは、コンタクトセンターネットワークにフルアクセスできます。シスコが提供するサービスプロバイダーのインターコネクト インターフェイスとして、CUBE アドレスでは、これらの両方の懸念事項を処理します。

特定の CVP 機能を使用しないソリューションについては、サードパーティの SBC を CVP に直接接続できます。このような解決策には、相互運用性を確認するための慎重なテストが必要です。



#### Important

サードパーティの SBC を Unified CVP に直接接続する設計では、シスコからの特別な例外をもって展開する必要があります。

#### Supported Features

特定のテストを実施しない場合、どの機能のサポートも保証されません。過去のテストでは、一般に次の機能がサポートされています。

- G.711ulaw、G.711alaw、および G.729 (Annex B なし) コーデック
- DNIS および ANI プレゼンテーション
- SBC の内部インターフェイスの SIP/TCP、外部インターフェイスの SIP/UDP
- CVP ベースのキュー
- DTMF を使用する CVP アプリケーション

- re-INVITE を使用した CVP ベースのイントラサイト転送
- Unified CM ベースのイントラサイト転送および会議
- SBC ベースの通話中コーデックのネゴシエーション基本的なコールフローは一般に機能しますが、複雑なコールフローは機能するのが難しい場合があります。
- Cisco Unified Communications Manager (Unified CM) 通話中コーデックのネゴシエーション (必要な場合は、トランスコーデック挿入を使用)。基本的なコールフローは一般に機能しますが、複雑なコールフローは機能するのが難しい場合があります。
- SBC の SIP INFO メッセージを CVP から RFC2833 トーンに変換 (DTMF ベースの転送の場合)




---

**Note** CVP と SBC 間のタイミングの問題により、SBC が転送を完了する前に CVP がコールを切断する場合があります。

---

- REFER での SBC による REFER 転送




---

**Note** CVP は、転送が完了すると SBC からサブスクリプションを終了する BYE または最終的な NOTIFY を必要とします。SBC がこれらの 1 つも送信しない場合、コールはサブスクリプション期間中に停止し、CVP ライセンスはリリースされません。

---

- 消費モードの SBC を使用した SIP 302 リダイレクト応答
- 応答なしでの CVP ベースのリダイレクト
- コール保留

### サポートされない機能

特定のテストを実施しない場合、どの機能のサポートも保証されません。過去のテストでは、一般に、これらの機能がサポートされていないことが示されています。

- SIP コールプログレス分析によるアウトバウンドオプション
- サービス コールバック
- コールの存続可能性と関連機能 (survivability.tcl スクリプト、ローカルブランチ SRST および TOD ルーティング、フックフラッシュ、TBCT)
- VRU PG 障害の処理および存続可能性によるダウンストリーム障害処理
- エッジでのキュー (CVP `SendToOriginator` 機能を使用)
- ビデオコールフロー
- SIP over TLS および SRTP

- ロケーションベースの CAC
- REFER と置換
- シスココンポーネント間のメッセージに対して（CUSPではなく）SIPプロキシとして構成された SBC
- ネットワーク トランク グループの使用率とレポート
- トランクグループの使用率
- SIP リソースの可用性インジケータ（RAI）動的コールルーティング
- SIP ダイアルピアベースの録音

一般に、さまざまな Unified CCE 機能と CVP 機能が、サードパーティの SBC に存在しない特定の CUBE 機能に依存しているため、機能は、サポートされません。

### その他の注意点

サードパーティの SBC を導入環境に追加する場合は、次の注意事項を検討してください。

- ほとんどのサードパーティの SBC は、Unified CCE がエンドツーエンドのコール トラッキングに使用する Cisco-Guid ヘッダーを生成しません。
- SBC と CVP の間で SIP over TCP を使用する場合、SBC が高可用性機能を介して切り替わる場合、一部のコールがドロップする場合があります。使用される CVP サーバごとに、スイッチオーバーが発生した後に1つのコールがドロップする場合があります。特定の CVP サーバで進行中の他のすべてのコールは、処理状態を把握するシグナリングとメディアを使用してアクティブな状態をとります。ドロップされたコールは、スイッチオーバー後に SBC に SIP メッセージを送信する最初のコールです。SIP over UDP ではこの動作は表示されません。
- サードパーティの SBC を使用するソリューションでは、ネットワークが SBC とサブネット間にコンタクトセンターソリューションコンポーネントがあるファイアウォールを備える場合があります。ファイアウォールの構成では、SBC と CVP 間の SIP 関連の通信を許可します。

TCP を通じた SIP トラフィックの場合、CVP は SBC 用の SIP ポートとの発信接続を作成しません。CVP では、SBC と CVP の間にコールがない場合でも、アイドル状態の TCP 接続は 4 時間確立された状態のままです。

ファイアウォールの構成では、CVP で検出されなくても、このようなアイドル状態の接続が解放される可能性があります。次に CVP が着信コールを受信すると、CVP が発信 TCP 接続上の SIP リクエストを SBC に送信できないため、一部のコールが失敗します。CVP が SBC への新しい接続を確立するまで、コールは失敗する可能性があります。

- シナリオによっては、CVP が通話中および無応答時の通知を SBC に送信する必要があります。このような場合は、Remote-Party-ID ヘッダーを使用してヘッダーを操作して、表示名の最後に「--CVP」を含める必要があります。

- すべての SIP サービスプロバイダーが、REFER、302 リダイレクトメッセージ、DTMF ベースの取り消しと転送、またはデータ転送（UUI、GTD、NSS 等）の拡張機能をサポートするわけではありません。
- Unified CM は、CVP へのシグナリングパス上のセッション更新に UPDATE メソッドを使用できます。この使用例はテストされていないため、CVP がサードパーティの SBC に直接接続されている場合はサポートされません。
- CVP は、IPv6 SDP と IPv4 SDP の両方をサポートします。SBC がセッションの説明で IPv4 と IPv6 の両方を使用する場合は、代替ネットワーク アドレス フォーマット（ANAT）を使用します。

### Cisco Virtualized Voice Browser

シスコでは、サードパーティ製 SBC を使用して Cisco VVB をテストしていません。

## 音声認識と音声合成

自動音声認識（ASR）または音声合成（TTS）サーバは、無音圧縮を使用できないため、G.711 コーデックを使用する必要があります。