高可用性とネットワーク設計

高可用性の設計

Cisco Contact Center Enterprise ソリューションは、設計により高可用性の機能を備えています。ソリューション設計には、コアコンポーネントの冗長性を含める必要があります。冗長コンポーネントは自動的にフェールオーバーし、手動操作なしで復元します。設計にも基本以上の高可用性機能を含めることができます。導入を成功させるには、データや音声インターネットワーキング、システム管理および Contact Center Enterprise ソリューション設計および構成に関する経験があるチームが必要です。

高可用性を促す各変更には、コストがかかります。このコストには、より多くのハードウェア、より多くのソフトウェアコンポーネント、およびより多くのネットワーク帯域幅が含まれる場合があります。コストと変更による結果のバランスを取ってください。フェールオーバーシナリオ中に切断を防止することはどれくらい重要でしょうか。システムの一部が復旧するまで、カスタ

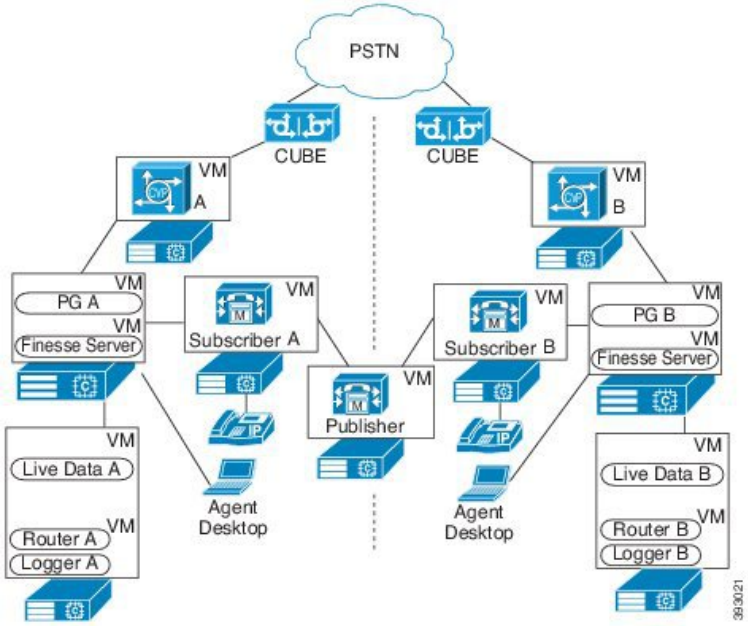
マーに数分待ってもらうことは許容範囲でしょうか。障害中、一部の通話のコンテキストがなくなってしまうことをカスタマーは許してくれるでしょうか。初期設計中により優れたフォールトトレランスに投資し、将来的な拡張性のためにコンタクトセンターを配置するでしょうか。

導入サイクルにおける再設計や今後のメンテナンスの問題を避けるために慎重に計画しましょう。すべての導入サイトの将来的な拡張性を念頭に置いて常に、最悪の障害シナリオを想定して設計します。

Note このガイドでは、Contact Center Enterprise ソリューションそのものの設計に焦点を当ててください。ソリューションは、他のシステムのフレームワークで動作します。このガイドでは、コンタクトセンターをサポートする各システムに関する完全な情報は記載されていません。このガイドは、Cisco Contact Center Enterprise 製品に焦点をおいています。このガイドで別のシステムについて説明する場合は、包括的なビューは提供されません。完全な Cisco Unified Communications 製品一式に関する情報は、http://www.cisco.com/en/US/docs/voice_ip_comm/uc_system/design/guides/UCgoList.html に記載されているシスコソリューション設計書を参照してください。

次の図は、フォールトトレランス Unified CCE 単一サイト展開を示しています。

***Figure 1: Unified CCE* コンポーネントの冗長性**



Note Contact Center Enterprise ソリューションは、実稼働環境で非冗長性（シンプレックス）導入をサポートしません。テスト環境のみで非冗長展開を使用できます。

この設計は、冗長性に対して、コンポーネントがどう重複するかを示しています。すべてのContact Center Enterprise 導入は、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、導入でコア システムの半分が失われることがありますが、ソリューションは引き続き機能します。この状態の場合、導入では、Unified CVP を介してコールを VRU セッションまたは引き続き接続されているエージェントに再ルーティングできます。可能な場合は、コンタクトセンターを導入して、Unified CM Publisher でデバイス、コール処理、またはCTI Manager サービスが実行されていないことを確認します。

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をプライベート ネットワーク パスでインターコネクトします。コンポーネントは、障害検出に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、発行元と複数のサブスクライバが含まれます。エージェントの電話とデスクトップはプライマリ 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。

高可用性と仮想化

仮想化された導入では、高可用性を維持するためにコンポーネントを慎重に配置します。高可用性をサポートするメカニズムは同じです。ただし、1 回の障害から複数のフェールオーバーを最小限に抑えるためのコンポーネントを分散します。ダイレクトアタッチドストレージ（DAS）のみシステムを展開する場合は、次の点を検討してください。

- VM が失敗すると、VM にインストールされているコンポーネントすべてがダウンします。
- 物理サーバが失敗すると、その VMware vSphere Host にインストールされている VM すべてがダウンします。

共有ストレージを備えるシステムへの導入では、VMware 高可用性機能の一部を使用して、復元力を向上できます。サポートされる VMware 機能の詳細については、http://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/uc_system/virtualization/cisco-collaboration-virtualization.html の「シスココラボレーション仮想化」を参照してください。

ハードウェア障害の影響を最小限に抑えるために、次のガイドラインに従います。

- プライマリ VM とバックアップ VM を同じ物理サーバ、シャーシ、またはサイトに配置しないようにします。
- すべてのアクティブコンポーネントを同じ物理サーバ、シャーシ、またはサイト上のフェールオーバーグループに配置しないようにします。
- 同じ物理サーバ、シャーシ、またはサイト上に同じ役割を持つすべての VM を配置しないようにします。

サーバのフェールオーバー

サーバまたはブレードに障害が発生すると、アクティブコールが非アクティブになり、着信通話が中断されます。バックアップコンポーネントがアクティブになると、処理が再開されます。プ

ライマリサーバがリカバリすると、アクティブコールと着信コールの処理はプライマリサーバに返されます。

仮想化の心得

仮想化を計画する際は、次の点に注意してください。

- どのコンポーネントが共存でき、どのコンポーネントが同じ VM で共存させなければならないのかに気を付けます。仮想環境に置けるコンポーネントの配置に関する詳細は、ソリューションの仮想化 Web ページを参照してください。
- Contact Center Enterprise ソリューションは、ゲスト OS（Windows または VOS）の NIC チーミングをサポートしません。
- NIC カードとイーサネットスイッチをオートネゴシエーションに設定します。

VMware 高可用性の考慮事項

高可用性（HA）により、仮想化された Contact Center Enterprise 環境では、ハードウェアおよびオペレーティングシステムの障害に対してフェールオーバー保護が提供されます。VMware の HA 設定をコンタクトセンター アプリケーション VM に使用できるのは、ソリューションで SAN ストレージを使用している場合のみです。

VMware HA が有効なソリューションを展開する場合は、次の点を検討してください。

- シスコは、VMware Distributed Resource Scheduler（DRS）をサポートしていません。
- vCenter で、**[アドミッションコントロールポリシー（Admission Control Policy）] > [フェールオーバーホストの指定（Specify a failover host）]** の順に選択します。ESXi ホストに障害が発生すると、このホスト上のすべての VM が予約済みの HA バックアップ ホストにフェールオーバーします。フェールオーバーホストのアドミッションコントロール ポリシーにより、リソースのフラグメント化が回避されます。Contact Center Enterprise リファレンス設計モデルは、ソリューション内の特定の VM の同じ場所を想定します。この VM の同一ロケーション要件は、Contact Center Enterprise キャパシティ要件に基づいてシステムのパフォーマンスを保証します。
- HA バックアップホストは、プライマリサーバと同じデータセンター内に配置する必要がありますが、コンタクト センター ブレードと同じ物理シャーシに配置はできません。vSphere 管理には 10 GB のネットワーキング接続を使用します。
- vCenter で**[VM監視ステータス（VM monitoring status）] > [（VM監視のみ）]** の順に選択します。
- vCenter で、**ホストの分離応答**として、すべての仮想マシンをシャットダウンする適切なオプションを選択します。
- 一覧されているとおり、**VM の再起動の優先順位**を使用して VM を構成します。

***Table 1: VM* 設定**

VM	VM の再起動の優先順位
Cisco Unified Intelligence Center	低
コンタクトセンター管理ポータルまたはコンタクト センター ドメイン マネージャ	低
Unified CVP レポートサーバ	低
Unified CCE PGs	中
Cisco Finesse	中
Unified CVP サーバ	高
Unified CCE ルータおよび Logger	高
Cisco IdS	中
Cisco Unified CallManager	高
Cisco Live データ	低い
Cisco Customer Collaboration Platform	低い

リファレンス設計に準拠したソリューション用のネットワーク設計

テスト済みリファレンス構成

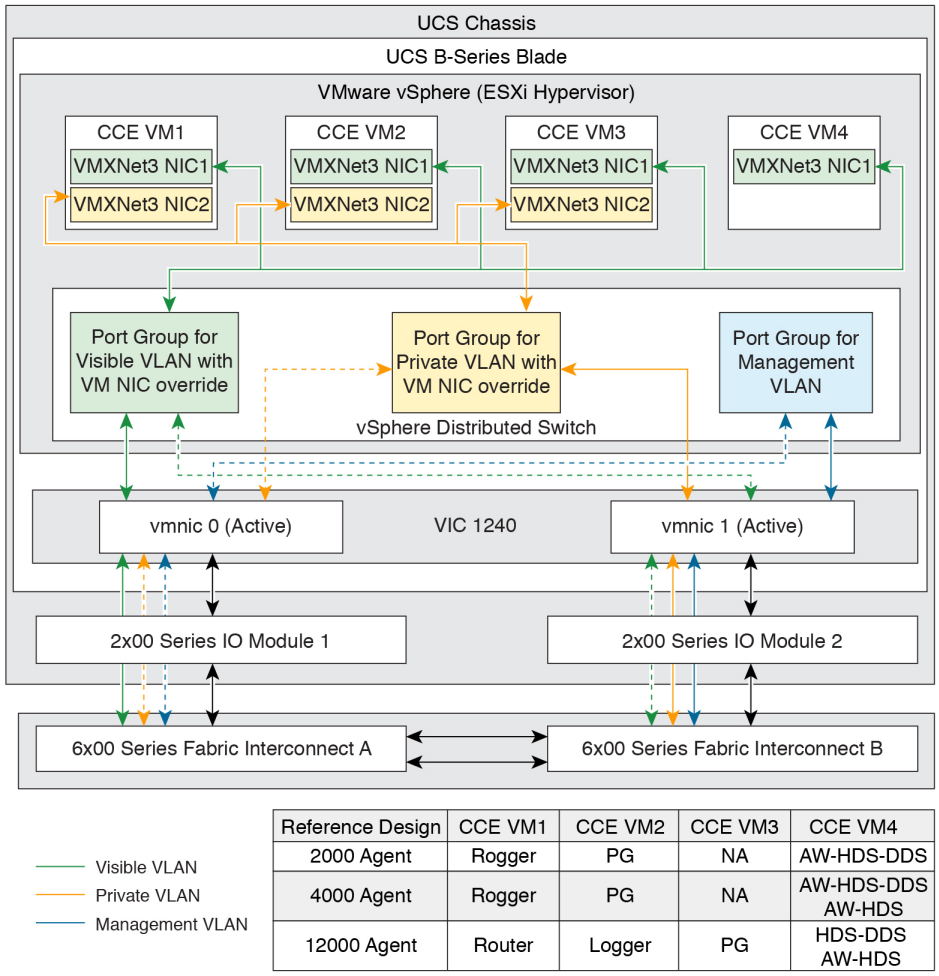
この項では、UCS 導入のネットワーク構成に関するガイダンスを提供します。また、フォールトトレランスと冗長性の情報が含まれます。

Cisco UCS B-Series サーバのネットワーク要件

次の図は、アプリケーションローカル OS NIC からデータセンター ネットワーク スイッチング インフラストラクチャへの仮想から物理への通信パスを示しています。

この設計では、アクティブ/アクティブモードで 2 つの VMNIC を使用する 1 つの仮想スイッチを使用します。この設計では、VMware vSwitch のポートグループ VMNIC オーバーライドメカニズムを使用するファブリック インターコネクトを介して、パブリックネットワークとプライベートネットワークのパスの多様性を調整します。この設計では、ファブリック インターコネクトを介する単一パスの損失による両方のネットワークの障害を回避するため、パブリックネットワークとプラットフォームのパスの多様性が必要です。

図 *2 : Cisco UCS B-Series* サーバのネットワーク要件



Reference Design	CCE VM1	CCE VM2	CCE VM3	CCE VM4
2000 Agent	Rogger	PG	NA	AW-HDS-DDS
4000 Agent	Rogger	PG	NA	AW-HDS-DDS AW-HDS
12000 Agent	Router	Logger	PG	HDS-DDS AW-HDS

UCS B ファブリック インターコネクトを備えたコンタクトセンターは次をサポートします。

- エンドホストモードでのファブリック
- イーサネット インターフェイスは 1/10 GB で、ギガビット イーサネット スイッチに接続されている必要があります。
- UCS Manager の vNIC に有効なファブリック フェールオーバー

（注） アップデート 1 以降、Nexus 1000v および Nexus 1000v を基に下その他シスコ分散仮想スイッチは、ESXi 6.5 との互換性はありません。詳細については、サードパーティ vSwitch の中止に関する VMware の項目を参照してください。

データセンタースイッチの構成

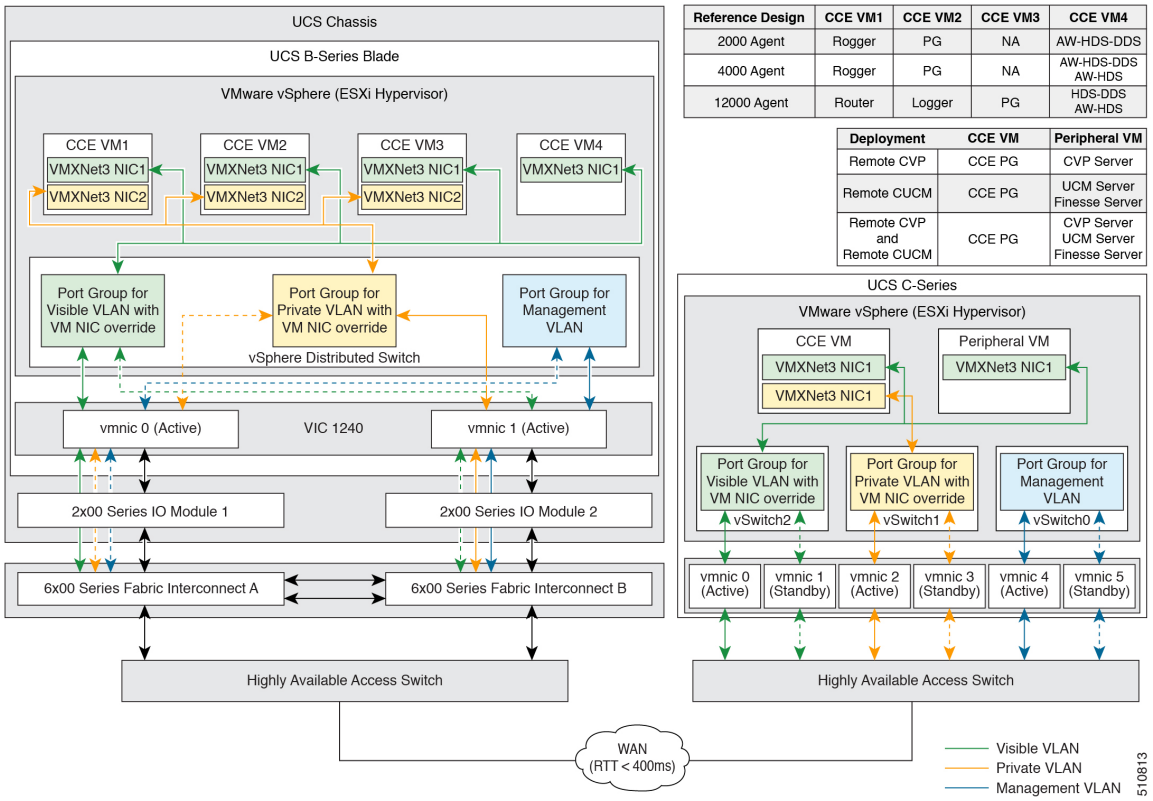
Contact Center Enterprise は、UCS B シリーズ ファブリック インターコネクトからデータベーススイッチまでイーサネットアップリンク構成用の設計をいくつもサポートしています。設計上、仮想スイッチのVLANタグ付けが必要です。データセンタースイッチ機能に応じて、EtherChannel/Link Aggregation Control Protocol（LACP）または Virtual PortEther（vPC）のいずれかを使用できます。

UCSファブリックインターコネクトのパブリックネットワークアップリンクとプライベートネットワーク アップリンクに必要な設計は、Common-L2 設計を使用します。この設計では、両方の VLAN がデータセンタースイッチの 1 つのペアにトランクされます。サービスプロバイダーは、同じリンク上の（VMwareを含む）別の管理およびエンタープライズ ネットワークをトランクすることを選ぶか、これらネットワークを分離するための Disjoint-L2 を使用する場合があります。ここでは Common-L2 モデルのみを使用しますが、どちらの設計もサポートされています。

C シリーズ

次の図は、UCS C-Series サーバのすべてのソリューション向けリファレンス設計と vSphere vSwitch 設計のネットワーク実装を示しています。

図 *3 : Cisco UCS C-Series* サーバのネットワーク要件



この設計では、アクティブ/スタンバイ構成の仮想マシン ネットワーク インターフェイス コントローラ（VMNIC）インターフェイスの VMware NIC Teaming（負荷分散なし）を使用します。このデバイスは、ネットワークへの代替および冗長ハードウェアパスを使用します。

ネットワーク側の実装は、この設計と異なる場合があります。ただし、冗長性が必要であり、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両方に影響を与えるシングル ポイント障害を持つことはできません。

イーサネット インターフェイスは 1/10 GB で、ギガビット イーサネット スイッチに接続されている必要があります。

UCS C シリーズのネットワーキングの詳細については、http://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/uc_system/virtualization/cisco-collaboration-virtualization.html のソリューション向けのシスコ コラボレーション仮想化ページを参照してください。

PSTN ネットワーク設計の考慮事項

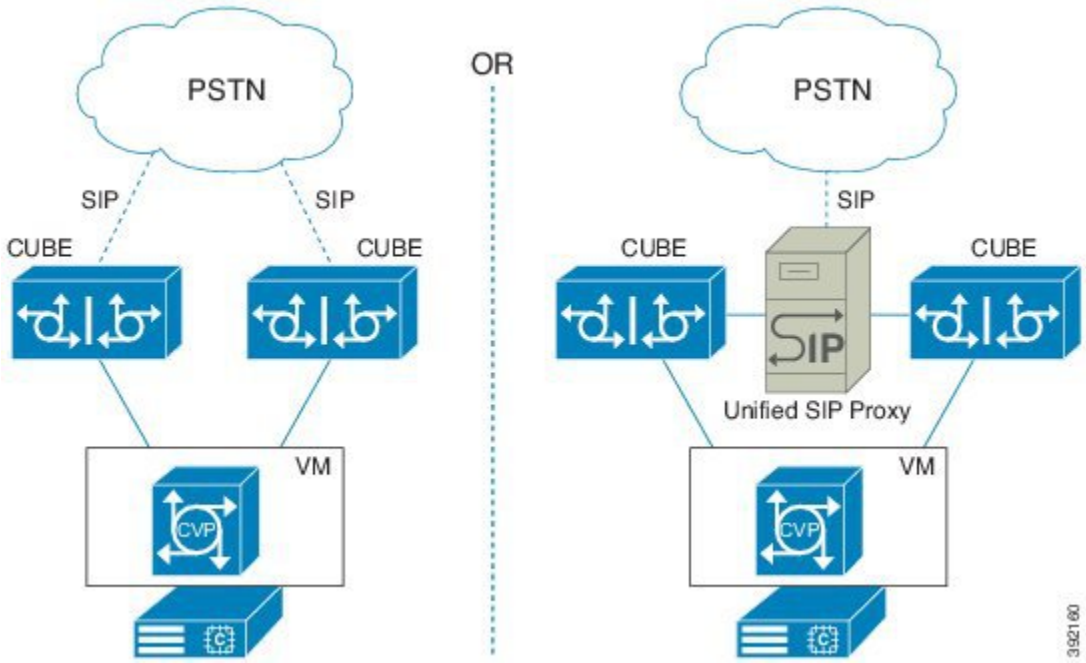
高可用性のコンタクトセンター設計は、データ、マルチメディア、音声トラフィック用のネットワーク インフラストラクチャから開始します。ネットワーク インフラストラクチャの「シングル ポイント障害」は、コンタクトセンターに設計したその他高可用性機能を低く評価します。PSTN から開始し、着信コールに、初期処理とキューイングのために Unified CVP に到達するための複数のパスがあることを確認します。

それぞれ別個の Cisco Unified Border Element（CUBE）に接続する、少なくとも 2 つの SIP トランクを備えた設計が理想です。CUBE トランクまたは SIP トランクに障害が発生した場合、PSTN は残りの SIP トランクを経由してすべてのトラフィックをルーティングできます。すべての SIP トランクを大規模トランクグループとして構成定するか、他の SIP トランクへの再ルーティングまたはオーバーフロー ルーティングを構成することで、PSTN ルートを設定します。Cisco UBE に障害が発生した場合でも SIP トランクが起動している場合、また、冗長 CUBE を各 SIP トランクに接続して、キャパシティを維持できます。

一部のエリアでは、PSTN は、複数の SIP トランクを単一サイトに提供しない場合があります。その場合は、SIP トランクを Cisco Unified SIP Proxy（CUSP）に接続できます。その後、複数の CUBEs を CUSP に接続して、冗長性を提供できます。

CUBE は、初回処理とキューリングのために Unified CVP にコールを渡します。各 CUBE を、負荷分散用の個別の Unified CVP で登録します。さらにフォールトトレランスを高くするには、バックアップとして別の Unified CVP と一緒に各 CUBE を登録するか、CUBE で SIP サーバグループを構成します。CUBE を Unified CVP に接続できない場合は、TCL スクリプトを使用していくつかのコール処理を実行することもできます。TCL スクリプトでは、コールを別のサイトまたはダイヤル番号に再ルーティングできます。スクリプトは、ローカルに保存されている .wav ファイルを発信者に再生して通話を終了することもできます。

Figure 4: 高可用性の入力点



CUBE、Unified CVP、および音声ネットワークの詳細については、https://www.cisco.com/en/US/docs/voice_ip_comm/uc_system/design/guides/UCgoList.html の「『*Cisco Collaboration System Solution Reference Network Designs*』」を参照してください。

Cisco Unified Survivable Remote Site Telephony（SRST）

Unified CM に対して Cisco Unified Survivable Remote Site Telephony（SRST）オプションを使用する音声ゲートウェイは、同様のフェールオーバープロセスに従います。ゲートウェイが制御サブスクライバから切断されている場合、ゲートウェイは SRST モードにフェールオーバーします。フェールオーバーによってすべての音声コールがドロップされ、ゲートウェイが SRST モードにリセットされます。電話機をローカル呼制御のためにローカル SRST ゲートウェイにリホームします。

SRST モードで実行されている間、Unified CCE は、エージェントがデスクトップから CTI 接続を持っているかのように動作します。ルーティング アプリケーションは、エージェントの準備が完了しておらず、これらエージェントに通話が送信されていないことを検出します。ゲートウェイとサブスクライバが接続を再確立すると、サブスクライバはゲートウェイと電話機を再度制御することで、エージェントが再接続できます。

Active Directory と高可用性

Contact Center Enterprise 設定と Active Directory 間のネットワークリンクに障害が発生した場合、高可用性に影響する次の点を考慮してください。

- リンク障害中、コールトラフィックへの影響はありません。

- ドメイン内の VM はドメイン コントローラ ログイン情報を使用してサインインを制限します。キャッシュされたログイン情報を使用してサインインできます。
- リンクの障害前に Unified CCE サービスを停止する場合、Unified CCE サブコンポーネントを開始する前にリンクを復元する必要があります。
- ローカルの PG 設定にアクセスしたり、Unified CCE Web 設定にサインインすることはできません。
- Unified CCE サービスがアクティブである一方でリンクに障害がある場合、Unified CCE Web 設定、構成ツールそしてスクリプトエディタへのアクセスはできません。
- Unified CCMP によってポータルへのサインインが許可されていても、レポートページへのアクセスはできません。
- 管理者およびスーパーユーザは、Cisco Unified Intelligence Center OAMP ポータルで、Reporting Configuration 以外の任意の属性にアクセスまたはそれを構成できます。
- スーパーバイザは、Cisco Unified Intelligence Center Reporting ポータルにサインインできません。ただし、すでにログインしているスーパーバイザはレポートにアクセスできます。

Contact Center Enterprise ネットワークアーキテクチャ

Cisco Contact Center Enterprise ソリューションは、リアルタイムのデータ転送要件を満たすネットワークインフラストラクチャに依存する分散型、強い、または障害性のネットワーク アプリケーションです。適切に設計されたコンタクトセンターエンタープライズネットワークには、適切な帯域幅、低遅延、および特定の UDP および TCP トラフィックを優先する優先順位付けスキームが必要です。設計要件により、冗長サブコンポーネント間でフォールトトレラントメッセージが確実に同期されます。これらの要件により、時間に依存するステータスデータ（ルーティングメッセージ、エージェントの状態、コール統計、トランク情報など）のシステム全体に配信が確保されます。

ソリューションでは、WAN と LAN のトラフィックは次のカテゴリに分類されます。

音声およびビデオ トラフィック

音声コール（音声キャリアストリーム）は、PSTN ゲートウェイ ポート、Unified CVP ポート、IP Phone などのさまざまなエンドポイント間で実際の音声サンプルを処理する Real-time Transport Protocol（RTP）パケットで構成されています。このトラフィックには、サイレントモニタまたは録音されたエージェントコール用の音声ストリームが含まれます。

呼制御トラフィック

呼制御トラフィックには、コールのエンドポイントに応じて、いくつかのプロトコル（MGCP または TAPI/JTAPI）のデータパケットが含まれます。呼制御には、コールの設定、保守、ティアダウン、またはリダイレクトを行う機能が含まれています。呼制御トラフィックには、音声コールを周辺機器（エージェントやサービスなど）や他のメディアターミネーション リソース（Unified CVP ポートなど）にルートするルーティングおよびサービス制御メッセージが含まれます。制御トラフィックには、周辺機器リソースステータスのリアルタイム更新も含まれます。

データ トラフィック

データトラフィックには、エージェントデスクトップ用の電子メール、Webアクティビティ、SIP シグナリング、および CTI データベース アプリケーション トラフィックが含まれます。優先データには、レポートや構成の更新イベントなど、非リアルタイムシステム状態のデータが含まれます。

この項では、次の間のデータフローについて説明します。

- リモート周辺機器ゲートウェイ（PG）および Unified CCE Central Controller（CC）
- PG または CC 冗長ペアの側面
- デスクトップ アプリケーションと Finesse サーバ

メディア（音声およびビデオ）のプロビジョニングの詳細については、http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html の *Cisco Unified Contact Center Enterprise* アドミニストレーション ガイド を参照してください。

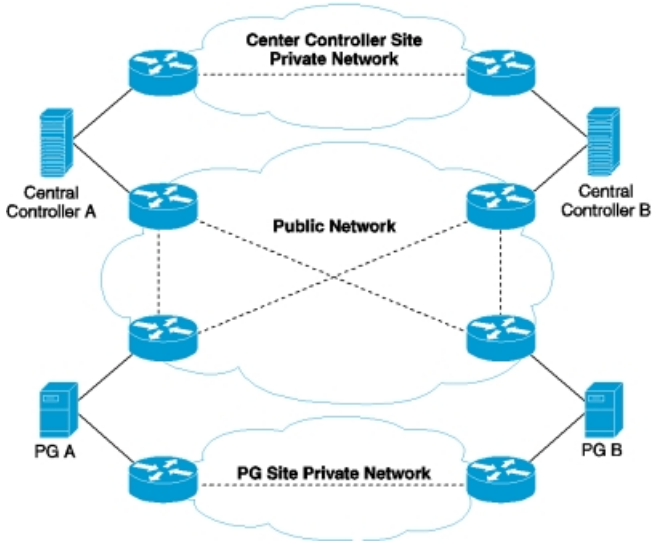
ネットワークリンクの高可用性に関する検討事項

Unified CCE で採用されているフォールト トレラント アーキテクチャには、2 つの独立した通信ネットワークが必要です。これらのネットワークは、個別の物理ネットワークです。プライベートネットワークでは、コンポーネント間の同期の維持と復元に必要なトラフィックを処理します。また、メッセージ配信システム（MDS）を介したクライアント通信も処理します。（別のパスを使用する）パブリックネットワークは、セントラルコントローラと PG 間のトラフィックを処理します。パブリックネットワークは、フォールトトレランス ソフトウェア向けの代替ネットワークとしても機能し、コンポーネントの障害とネットワークの障害を区別します。高可用性を実現するには、パブリックネットワークに冗長接続を含める必要があります。各接続が異なるキャリアを使用するのが理想です。

Note パブリックネットワークは、目に見えるネットワークと呼ばれることもあります。

次の図は、Contact Center Enterprise ソリューション向けのネットワークセグメントを示しています。PG とセントラルコントローラの冗長ペアは、地理的に分かれています。

Figure 5: Unified CCE システムのパブリックおよびプライベート ネットワーク セグメントの例



この場合、パブリックネットワークは、セントラルコントローラ、PG、および Administration & Data サーバ間のトラフィックを処理します。パブリックネットワークは、同期制御トラフィックは処理しません。パブリックネットワーク WAN リンクには、PG、Administration & Data サーバをサポートするための適切な帯域幅が必要です。IP ベースのプライオリティキューイングまたは QoS のどちらかをかならず使用して、コンタクトセンター トラフィックが、遅延およびジッターの両方に対して許容可能な許容度内で処理されているかを確認します。

プライベートネットワークは、セントラルコントローラまたは PG の冗長サイド間でトラフィックを処理します。このトラフィックは、主に同期されたデータと制御メッセージによって構成されています。また、トラフィックは、分離された状態から復旧する際に、冗長サイドの再同期に必要な状態転送も伝達します。WAN を使用して展開する場合、プライベートネットワークは、Contact Center Enterprise ソリューションの全体的な応答で重要となります。ネットワークには、厳しい遅延要件があります。したがって、IP ベースのプライオリティキューイングまたは プライベートネットワーク リンク上の QoS のどちらかを使用する必要があります。

必要なフォールトトレランスを実現するには、プライベート WAN リンクがパブリック WAN リンクから完全に独立している必要があります（別々の IP ルータ、ネットワーク セグメントまたはパスなど）。独立した WAN リンクによって、シングルポイント障害が、パブリックネットワークとプライベートネットワーク間で完全に分離されます。ルート済みネットワークを通過するパブリックネットワーク WAN セグメントを展開すると、ネットワーク全体の PG とセントラルコントローラ間のルートの多様性を維持できます。複数のセッションで共通のパス選択肢と共通の障害ポイントが発生するルートは避けてください。

セントラルコントローラの 1 つのサイドにローカルな PG および Administration & Data サーバは、公共のイーサネットを介してローカルのセントラルコントローラに接続し、公共の WAN リンクを介してリモートのセントラルコントローラに接続します。オプションで、セントラルコントローラ LAN セグメントから分離された PG および Administration & Data サーバにブリッジを展開して、LAN の機能停止に対する保護を強化できます。

パブリック ネットワーク トラフィック フロー

アクティブな PG は、エージェント、コール、キューなどについて状態情報を使用して、セントラル コントローラ コール ルータを連続的に更新します。このトラフィックはリアルタイムトラフィックです。PGは、構成に基づいた間隔で履歴データを送信します。履歴データの優先順位は低いですが、次の間隔が始まる前にセントラルサイトにリーチする必要があります。

PGが開始されると、セントラルサイトはその構成データを提供することで監視するリソースを把握します。この構成をダウンロードすることで、ネットワーク帯域幅の使用量が大幅に増加する可能性があります。

パブリックトラフィックの概要を次に示します。

- **高優先順位トラフィック**：ルーティングおよびデバイス管理プロトコル（DMP）制御トラフィックが含まれます。パブリック高優先順位IPアドレスを使用してTCPで送信されます。
- **ハートビートトラフィック**：パブリック高優先順位の IP アドレスを使用したポート範囲が 39500 ～ 39999 の UDP メッセージ。ハートビートは、PG とセントラルコントローラ間の両方向で、400ミリ秒の間隔で送信されます。
- **中優先順位トラフィック**：PGからセントラルコントローラへのリアルタイムトラフィックおよび構成要求が含まれます。中優先順位トラフィックは、パブリック高優先順位 IP アドレスを使用して TCP で送信されます。
- **低優先順位トラフィック**：履歴データトラフィック、セントラルコントローラからの構成トラフィック、およびコールクローズ通知が含まれます。低優先順位トラフィックは、非パブリック高優先順位 IP アドレスを使用して TCP で送信されます。

プライベート ネットワーク トラフィック フロー

プライベートネットワークは、重要なメッセージ配信サービス（MDS）トラフィックを処理します。

次に、プライベートトラフィックの要約を示します。

- **高優先順位トラフィック** — ルーティング、MDSコントロールトラフィック、およびPIM CTIサーバ、露がなどのMDSクライアントプロセスからの別のトラフィックを含みます。プライベート高優先順位 IP アドレスを使用して TCP で送信されます。
- **ハートビートトラフィック**：プライベート高優先順位のIPアドレスを使用したポート範囲が 39500 ～ 39999 の UDP メッセージ。ハートビートは、デュプレックスサイド間を隔週 100 ミリ秒間隔で送信されます。
- **中優先順位および低優先順位トラフィック** — セントラル コントローラの場合、このトラフィックには、ルーティング クライアントから供給される共有データに加え、Call Router 状態転送（独立したセッション）などの（ルート制御以外の）Call Router メッセージが含まれます。OPC（PG）の場合、このトラフィックには、ルート制御以外の共有周辺機器トラフィックおよびレポーティングトラフィックが含まれます。このクラスのトラフィックは、中優先順位および低優先順位として指定されているTCPセッション内で、それぞれプライベート高優先順位以外の IP アドレスを使用して送信されます。

- **状態転送トラフィック：** Router、OPC、およびその他の同期プロセスの状態同期メッセージ。プライベート高優先順位以外の IP アドレスを使用して TCP で送信されます。

マージされたネットワーク接続

Unified CCE コンポーネントは、パブリックネットワークとプライベートネットワークを使用して通信します。これらのネットワークは、個別の物理ネットワークである必要があります。高可用性を実現するには、パブリックネットワークに冗長接続を含める必要があります。各接続が異なるキャリアを使用するのが理想です。

QoS と帯域幅が正しく設定されている場合、設計でパブリック WAN またはプライベート WAN リンクを他の企業トラフィックとマージできます。非コンタクトセントラフィックをマージするリンクを使用する場合は、パブリックトラフィックとプライベートトラフィックを別のネットワーク上に保持します。ただし、プライベートネットワークトラフィックを低優先順位および高優先順位のデータパスに分割してはいけません。同じリンクが、特定のコンポーネントのすべてのプライベート ネットワーク トラフィックを実行する必要があります。優先順位の低いトラフィックと優先順位の高いトラフィックを異なるリンクに送信すると、コンポーネントのフェールオーバー動作が無効になります。同様に、各周辺機器ゲートウェイからコールルータの低優先順位および高優先順位のアドレスまで、すべての低優先順位および高優先順位のトラフィックが同じパスをとおる必要があります。

パブリックネットワークに障害が発生した場合は、パブリック Unified CM トラフィックをプライベートネットワークに一時的にフェールオーバーできます。追加のトラフィックに対応するために、プライベートネットワークのサイズを設定します。パブリック トラフィックがプライベートネットワークにフェールオーバーした場合は、パブリックネットワークを可能な限り迅速に復元して通常動作に戻します。プライベートネットワークにも障害が発生した場合は、コンタクトセンター内で、1 つの Logger データベースの障害など、不安定性やデータの損失が発生します。

IP ベースの優先順位とサービス品質

Contact Center Enterprise ソリューションでは、すべてのプライベートネットワークで QoS が必要です。パブリックリンクでは、2000 エージェントおよび 4000 エージェントリファレンス設計で QoS を使用できます。12,000 エージェントリファレンス設計のパブリックリンクでは、QoS によってサーバ障害の検出が遅れる可能性があります。

大量の低優先順位のトラフィックが高優先順位のトラフィックの前に来ると、遅延によってフォールトトレランス動作がトリガーされる可能性があります。これらの遅延を回避するには、パブリックネットワークとプライベートネットワーク内の各 WAN リンクに対する優先順位付けスキームが必要です。Contact Center Enterprise ソリューションは、IP ベースの優先順位付けと QoS をサポートします。

低速のネットワークフローでは、単一の大きな（たとえば、1500バイト）パケットが、ネットワーク上で消費する時間は 100 ミリ秒を超える場合があります。この遅延は、1 つ以上のハートビートの明らかな損失の原因となる場合があります。この状況を回避するために、コンタクトセンターは優先順位の低いトラフィックに対して小さい最大伝送ユニット（MTU）を使用します。これにより、より早く優先順位の高いパケットをネットワークに接続できます。（回路の MTU サイズは、PG 設定で構成した回路帯域幅に基づいて計算されます）。

ネットワークに対して間違った優先順位付けをすると、一般的にコールタイムアウトやハートビートの損失の原因となる場合があります。アプリケーションの負荷が増加したり、ネットワーク上に共有トラフィックが配置される時に、問題が増加します。また、遅延条件が極端な場合、送信側でアプリケーション バッファ プールを使い果たすこともあります。

Contact Center Enterprise は、高、中、低の 3 つの優先順位を使用します。QoS を指定しない場合、ネットワークは、送信元および接続先 IP アドレス（別の IP 接続先アドレスに送信される優先順位の高いトラフィック）が特定した 2 つの優先順位のみ認識します。UDP ハートビートに関しては、特定の UDP ポート範囲が特定した 2 つの優先順位のみ認識します。IP ベースの優先順位付けでは、プライオリティキューイングを使用して IP ルータを構成し、優先順位の高い IP アドレスを持つ TCP パケットと他のトラフィックよりも UDP ハートビートを優先します。この優先順位付けスキームを使用する場合、使用可能な帯域幅の合計の 90% が優先順位の高いキューに付与されます。

QoS に対応したネットワークでは、IP アドレスではなく QoS のマーキングに基づいて、パケットに優先順位が付けられた処理（キューイング、スケジューリング、およびポリシー設定）が適用されます。コンタクトセンターは、プライベートおよびパブリック ネットワーク トラフィックに対してレイヤ 3 DSCP のマーキング機能を提供します。トラフィックマーキングは、ネットワークが QoS 認識のため、各ネットワーク インターフェイス コントローラ（NIC）にデュアル IP アドレスを設定する必要がなくなることを意味します。ただし、代わりにネットワークエッジでトラフィックにマークを付けすると、IP アドレスに基づいたアクセス制御リストを使用してパケットを識別するために、デュアル IP 構成が依然として必要です。

Note Microsoft Windows Packet Scheduler が（PG、セントラルコントローラ トラフィックのみに）有効な場合、レイヤ-2 802.1p のマーキングも可能です。ただし、これはサポートされていません。Microsoft Windows Packet Scheduler は、Unified CCE には適していません。802.1p マーキングは広く使用されておらず、DSCP マーキングが使用可能な場合は、必要ありません。

データトラフィックの適切なネットワーク設計に関しては、http://www.cisco.com/c/en/us/solutions/enterprise/design-zone-borderless-networks/index.html のネットワーク インフラストラクチャおよび Quality of Service（QoS）ドキュメントを参照してください。

UDP ハートビートおよび TCP キープアライブ

UDP ハートビート設計は、パブリックネットワークリンクに障害が発生したかどうかを検出します。ハートビート損失の方向に基づいて、接続の両端から検出を行うことができます。接続の両端は、定期的な間隔（ 400 ミリ秒ごと）でハートビートを反対側に送信します。各端は、他の端から類似したハートビートを探します。どちらかの端がハートビート期間の5倍の期間後にハートビートを受信しない場合、その端に問題が発生したとみなされ、アプリケーションはソケット接続を閉じます。この時点で、閉じられた側から通常、TCP Reset メッセージが生成されます。さまざまな要因によって以下のようなハートビート損失の原因となります。

- ネットワーク障害。
- ハートビート障害を送信するプロセス。
- 送信プロセスを実行している VM のシャットダウン。

• UDP パケットの不適切な優先順位付け。

ハートビートには、複数のパラメータが関連付けられています。一般に、これらのパラメータはシステムのデフォルト値のままにします。これらの値の一部は、接続が確立されると指定されます。その他のパラメータは、Windows レジストリで設定できます。最も重要な値は、次の 2 つです。

• ハートビート間の時間の長さ

• 障害を示す既存しないハートビートの数（現在は、5 にハードコード済み）

冗長コンポーネント間のプライベートハートビート間隔のデフォルト値は、100 ミリ秒です。片側は、回路の障害を検出し、もう一方は、500 ミリ秒後に障害を検出します。セントラルサイトと周辺機器ゲートウェイ間のデフォルトのハートビート間隔は、400 ミリ秒です。この場合、回路障害のしきい値に到達するまでに 2 秒かかります。

Contact Center Enterprise QoSの実装では、TCP キープアライブメッセージ を使用して UDP ハートビートを置き換えます。パブリック ネットワーク インターフェイスは、ハートビートまたはキープアライブメカニズムの一貫性を実行します。ただしプライベート ネットワーク インターフェイスは、キープアライブを実行します。QoS がパブリック ネットワーク インターフェイスで使用可能状態になっている場合は TCP キープアライブメッセージが送信され、使用不可状態の場合は UDP ハートビートが保持されます。

TCP スタックで提供される TCP キープアライブは、非アクティブ状態を検出すると、サーバまたはクライアント側を終了する原因となります。TCP キープアライブ機能は、接続が一定の期間アイドル状態が続いた後、接続を通してプローブパケットを送信します。別側からのキープアライブ応答が聞こえない場合、接続がダウンしたとみなされます。Windows サーバでは、接続ごとにキープアライブパラメータを指定できます。Contact Center Enterprise パブリック接続の場合、キープアライブタイムアウトは、（5 * 400）ミリ秒に設定され、2 秒の障害検出時間と UDP ハートビートが一致します。

QoS が有効になっている状態で TCP キープアライブに移行する理由は次のとおりです。

• コンバージド ネットワークでは、ネットワークの輻輳状態を処理するルータアルゴリズムが、TCP と UDP に異なる影響を与える場合があります。その結果、UDP ハートビートトラフィックで発生する遅延と輻輳により、タイムアウトによる接続障害が発生する可能性があります。

• UDP ハートビートを使用すると、ファイアウォール環境での展開が複雑になります。ハートビート通信への動的ポート配分では、幅広いポート番号を開くことができるので、ファイアウォールのセキュリティが低下します。

Note コンタクトセンター トラフィックを処理する WAN では、WAN アクセラレータを使用できません。WAN アクセラレータは、障害検出機能を効果的に無効にする信号を送信できます。

HSRP が有効なネットワーク

ソリューションネットワークがデフォルトゲートウェイの Hot Standby Router Protocol（HSRP）を使用する場合は、次の要件に従います。

- HSRP ホールド時間と関連する処理遅延を、間隔の 5 倍未満（プライベートネットワークでは 100 ミリ秒、パブリックネットワークは 400 ミリ秒）に設定します。このレベルでは、HSRP アクティブルータのスイッチオーバー中にプライベートネットワーク通信が停止しないようにします。

  プライベートまたはパブリックネットワークの停止通知を超えるコンバージェンス遅延があると、HSRP フェールオーバー時間が検出しきい値を超えて、フェールオーバーが発生する可能性があります。HSRP 構成にプライマリおよびセカンダリの指定があり、プライマリパスルータに障害が発生した場合、HSRP は、可能な場合に限り、プライマリパスを復元します。この復元は、2 回目の停止検出につながる場合があります。

  プライベートネットワークの場合は 500 ミリ秒近く、パブリックネットワークの場合は 2 秒に近い HSRP コンバージェンス遅延のあるプライマリおよびセカンダリ指定を使用しないでください。ただし、検出されたしきい値（透過的な HSRP フェールオーバーが発生する結果となります）を下回るコンバージェンス遅延では、優先パス構成は必須ではありません。次のアプローチが理想的です。パスの値とコストが同じ場合は、ルータを対照的に有効化し続けます。ただし、使用可能な帯域幅とコストが 1 つのパスを好む場合は（パスの移行が透過的である）、プライマリパスとルータの指定を推奨します。

- フォールトトレラント設計では、プライベートネットワークは物理的にパブリックネットワークから分離している必要があります。したがって、一方のタイプのネットワークトラフィックを他のネットワーク リンクに対してフェールオーバーするように HSRP を構成しないでください。

- コンタクトセンターの帯域幅の要件は、常に HSRP で保証する必要があります。それ以外の場合、システムの動作は不安定となります。たとえば、ロード共有用に HSRP を構成する場合は、最悪の場合の障害が発生した場合に、存続するリンクに十分な帯域幅が残すようにしなければなりません。

ネットワーク障害時の Unified CCE フェールオーバー

ネットワークの障害は、影響を受けるネットワーク全体にトラフィックを送信するコンポーネントに同時に影響します。Unified CCE のサブコンポーネントは、プライベートネットワークとパブリックネットワークの両方のリンクを使用して通信します。

プライベートネットワーク上のトラフィックは、次の機能を実行します。

- コンポーネント起動時の状態転送
- ルータの冗長ペアの同期
- 冗長 Logger データベースの同期
- PG の冗長ペアの同期

パブリックネットワークは、音声データ、コールコンテキストデータ、レポートデータなどのサブコンポーネント間の残りのトラフィックを処理します。パブリックネットワークには、Unified CCE サブコンポーネント間のすべてのパブリック ネットワーク リンクが含まれています。

Note 仮想化されたコンタクトセンターでは、仮想 NIC などの仮想環境での障害からネットワーク障害が発生するか、物理的なリソースの障害によってネットワーク障害が発生します。

プライベートネットワークの障害対応

プライベートネットワークの障害時、コンタクトセンターはすぐに 各サイドまたは両側が分離対応の運用に移行する状態になります。分けられた運用は、ルータがプライベートネットワークの回復を検出するまで継続されます。ルータとPGの冗長ペアは再同期し、通常運用を再開します。

ルータ A がペア対応側、ルータ B がペア無効側とします。プライベートネットワークに障害が発生すると、ルータ A は次のように動作します。

- ルータ A に多数のデバイスがある場合、デバイスは分離対応運用に移行し、トラフィックの処理を続けます。
- ルータAにデバイスが多数存在しない場合、デバイスは分非離対応運用に移行し、トラフィックの処理を停止します。

プライベートネットワークに障害が発生すると、ルータ B は次のように動作します。

- ルータBにデバイスが多数存在しない場合、デバイスは分非離対応運用に移行し、トラフィックは処理されません。
- ルータ B にデバイスが多数存在する場合は、テスト状態になります。ルータ B は、パブリックネットワークを介してルータAに接続するために、PGが有効になっていると指示します。次に、ルータ B は次のように応答します。
  - PG がルータ A に接続して状態を確認できる場合、ルータ B は分離対応状態に移行し、トラフィックの処理を開始します。このケースでは、ルータ A とルータ B の両方が分離対応状態で実行される可能性があります。
  - PG がルータ A に接続して、ルータ A が非分離無効状態である場合、ルータ B は分離対応状態に移行し、トラフィックの処理を開始します。
  - PG がルータ A に接続して、ルータ A が分離無効状態である場合、ルータ B は非分離対応状態に移行し、トラフィックの処理を停止します。

ルータのフェールオーバー処理中は、存続するルータが分離状態になるまで、ルータのルート要求がキューに入ります。ルータの障害が、VRUまたはエージェントにすでの到達している進行中のコールには影響しません。

ルータがアイドル状態になっている場合、対応するLoggerがシャットダウンされます。各Loggerは、割り当てられているルータのみと通信します。プライベートネットワーク接続が復元され、分離状態のルータのLoggerは、そのデータを使用して、別のLoggerを再同期します。プライベー

トネットワーク接続が、Config_Message_Logテーブルの14日の保持期間前にバックアップされた場合、システムは自動でLogger構成データベースを再同期します。また、プライベートネットワーク接続が14日の保持期間以上ダウンしたままの場合、https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-maintenance-guides-list.html の「アドミニストレーション ガイド」で説明のあるUnified ICMDBAアプリケーションを使用してLogger上で構成データを再同期する必要があります。

PGの各冗長ペアでは、有効なPGと無効なPGがあります。システムの開始時点で、最初に接続されたPGが有効なPGになります。ただし、プライベートネットワークでの障害発生後、冗長ペアの中で最大の重みを持つPGが有効なPGになります。もう1つのPGが無効なPGになります。

パブリックネットワークの障害対応

一般的に、高可用性ネットワークには、パブリックネットワーク用の冗長なチャネルが含まれます。一方のチャネルに障害が発生すると、もう一方のチャネルにシームレスに引き継がれます。2つのサブコンポーネント間のすべてのチャネルに障害が発生した場合、コンタクトセンターはパブリックネットワークの障害を検知します。

Note 冗長的なパブリックネットワーク無しのコンタクトセンターでは、1つのチャネルで障害が発生した場合に、コンタクトセンターで障害を検出します。

コンタクトセンターによるパブリックネットワーク障害への対応は、サイト数、機能数、サイトのリンク方法によって異なります。次の項では、より一般的または重要なシナリオについて説明します。

Unified Communication Managers 間の障害

最も大きな問題を引き起こすシナリオには、Unified CMのサブスクライバがパブリックリンクを失うことが挙げられます。機能しているプライベートネットワークでは、ルータとエージェントPGが同期し続けるため、ルータは依然としてすべてのエージェントデバイスを検出できます。このような状況で、ルータは、パブリックネットワーク障害のもう一方の側にあるサブスクライバに登録されているエージェントデバイスにコールを割り当てる場合があります。ただし、ローカルCVPは、パブリックネットワーク障害のもう一方の側にあるエージェントデバイスに接続情報を渡すわけではありません。コールは失敗しますが、ルーティングクライアントは、リモートサブスクライバのエージェントデバイスにルートされたコールとしてマークします。

WAN を介したクラスタリングの障害

間の障害サイト

WANトポロジを使用したクラスタリングでは、低遅延で十分な帯域幅を備え、高可用性で高い信頼性のあるWANが必要です。パブリックネットワークは、コンタクトセンターのフォールトトレランスには重要です。高可用性のWANは完全に冗長化されており、通常は別々のキャリア間でシングルポイント障害はありません。WANに部分的な障害が発生した場合、冗長リンクでは、サイトのリストに追加しますQoSパラメータ内のフル ロードを処理する機能が必要です。冗長WANの代替として、Metro Area Networks（MAN）、高密度波長分割多重（DWDM）またはイー

サネットWANを採用できます。高可用性かつ高い復元力を備えたWANの設計に関しては、Cisco Design Zone の https://www.cisco.com/c/en/us/solutions/enterprise/design-zone-branch-wan/index.html に記載されている「ブランチ *WAN* の *Design Zone*」を参照してください。

Note WiMAX、Munincipal Wi-Fi または VSAT などのワイヤレス WAN は、Contact Center Enterprise ソリューションには使用できません。

サイトのリストに追加します 間のパブリックネットワークに障害が起こった場合、システムは、次の方法で応答します。

1. Unified CM のサブスクライバが障害を検出。サブスクライバは、引き続きローカルで機能し、ローカルのコール処理や呼制御に影響しません。ただし、パブリックネットワーク上で設定されたコールには障害が起こります。
2. ルータおよび PG が、障害を検出。PG は自動的に、データ通信ストリームをローカルルータに再調整します。その後、ローカルルータは、プライベートネットワークの別サイドのルータにデータを渡し、コール処理を続けます。データパスが変更されても PG やルータのフェールオーバーの原因にはなりません。

パブリックネットワークの障害がエージェントに与える影響は、電話機とデスクトップの登録場所によって異なります。

- 最も一般的なケースは、エージェントデスクトップとエージェントの電話機の両方が同じサイド（たとえばサイド A）の PG と サブスクライバに登録されている場合です。サイトのリストに追加します 間のパブリックネットワークに障害が発生した場合、エージェントは、引き続き通常通りコールを処理できます。
- 場合によっては、エージェントデスクトップ（この例ではサイド A）とエージェント電話機（この例ではサイド B）が異なるサイドに登録されることがあります。このような場合、CTI Manager は、パブリックネットワーク上の電話イベントを、別サイドの PG にダイレクトします。サイトのリストに追加します 間のネットワークに障害が発生した場合、電話機はクラスタのサイド A にはリホームされません。電話機はサイド B で操作可能状態のままですが、サイド A の PG はこの電話機を検出できません。Unified CCE サブコンポーネントがエージェントの電話機にコールを送信できなくなったため、Unified CCE は自動的にエージェントをサインアウトします。
- 通常、冗長 Desktop サーバペアは、エージェントデスクトップ接続の負荷分散を行います。そのため、デスクトップの半分は、パブリックネットワークを介してアクティブな CTI サーバを備えた PG に接続する Desktop サーバに登録されます。パブリックネットワークに障害が発生すると、Desktop サーバからリモート CTI サーバへの接続は切断されます。Desktop サーバは、アクティブなエージェントデスクトップを切断して、リモート側にある冗長 Desktop サーバに強制的にリホームします。エージェントデスクトップは自動的に冗長 Desktop サーバを使用します。エージェントデスクトップは、冗長 Desktop サーバへの接続が確立されるまで無効の状態のままとなります。

エージェントサイトの障害

WAN を介したクラスタリングの Contact Center Enterprise トポロジは、エージェントが複数のサイトにリモートで配置されていることを前提としています。各エージェントサイトでは冗長性を確保するためにパブリックネットワーク経由で、両方のサイトのリストに追加しますにアクセスする必要があります。完全なネットワーク障害が発生した場合、これらの接続は SRST の基本的な機能も提供します。そのため、エージェントサイトは緊急コールである 911 に電話をかけることができます。

エージェントサイトでサイトのリストに追加しますに接続するパブリックネットワークの接続が切断された場合、システムは次の方法で応答します。

1. 切断されたサイトで Unified CM サブスクライバにホーム接続されている IP 電話は、他のサイトのサブスクライバに自動的にリホームされます。リホーミング動作を使用するには、冗長グループを構成します。
2. その切断されたサイトの Desktop サーバに接続されているエージェントデスクトップは、他のサイトの冗長サーバに自動的に再調整されます。（エージェントデスクトップは、再調整プロセス中に無効になります。）

エージェントサイトでサイトのリストに追加しますの両方に接続するパブリックネットワークの接続が切断された場合、システムは次の方法で応答します。

1. ローカルの音声ゲートウェイ（VG）は、クラスタへの通信パスの障害を検出します。その後、VG は SRST モードに切り替わり、ローカルダイヤル トーン機能を提供します。
2. Unified CVP を使用すると、VG が Unified CVP サーバへの切断を検出します。その後、VG はローカルの存続可能性 TCL スクリプトを実行して、IME 除外グループを再ルートします。
3. ローカルの PSTN 接続上で、アクティブなコールが切断されたエージェントサイトに入電した場合、そのコールはアクティブなままです。ただし、PG はコールへのアクセスを失い、TCD レコードを作成します。
4. Finesse サーバは、エージェントデスクトップへの接続が失われたことを検出し、エージェントをシステムから自動的にサインアウトします。IP 電話機が SRST モードになっている間は、Contact Center Enterprise エージェントとして機能できません。

両方のネットワークの障害への応答

パブリックネットワークとプライベートネットワークの一部に別々に障害が発生した場合、エージェントとコールへの影響が限定される場合があります。ただし、両方のネットワークに同時に障害が発生した場合、システムの機能は制限されます。この障害は、壊滅的です。このような障害は、組み込みバックアップと復元力を備えた慎重な WAN 設計によって回避できます。

サイト内の両方のネットワークで同時に障害は発生すると、サイトはシャットダウンされます。

2 つのサイト間のパブリックネットワークとプライベートネットワークで同時に障害が発生した場合、システムは次の方法で応答します。

1. 両方のルータが過半数のデバイスをチェックします。各ルータは、ルータに過半数のデバイスがある場合は分離有効モードになり、ルータに過半数のデバイスがない場合は分離無効モードになります。
2. PG は、必要に応じて自動的にデータ通信をローカルルータに再調整します。アクティブルータに接続できない PG は非アクティブになります。
3. Unified CM のサブスクライバは、障害を検出し、ローカルのコール処理と呼制御に影響を与えずに、ローカルで機能し続けます。
4. パブリック WAN リンクを介するアクティブな音声パスメディアを送信する進行中のコールは、リンクで障害が発生します。コールで障害が発生すると、PG は、そのコールに対して TCD レコードを作成します。
5. WAN トポロジを介したクラスタリングでは、各側の Unified CM サブスクライバはローカルコンポーネントのみにアクセスし動作します。
6. コール ルーティング スクリプトは、周辺機器オンライン ステータス チェックを使用してオフラインのデバイス周辺をルートします。
7. ローカル Unified CM サブスクライバに登録されている電話機とデスクトップを備えたエージェントには影響はありません。電話機とデスクトップの再ホーム中、他のすべてのエージェントは、一部またはすべての機能を失います。正確なシステム設定に応じて、このようなエージェントは、自信がサインアウトされていることを認識できる場合があります。
8. Unified CCE は、無効になったサイドに新規コールをルートしません。ただし、CTI ルートポイントの障害時に標準規格の Unified CM リダイレクトを使用するか、入力音声ゲートウェイの Unified CVP 存続可能性 TCL スクリプトを使用すると、これらのコールをリダイレクトまたは処理できます。

イングレス、エグレスおよび VXML ゲートウェイの高可用性に関する考慮事項

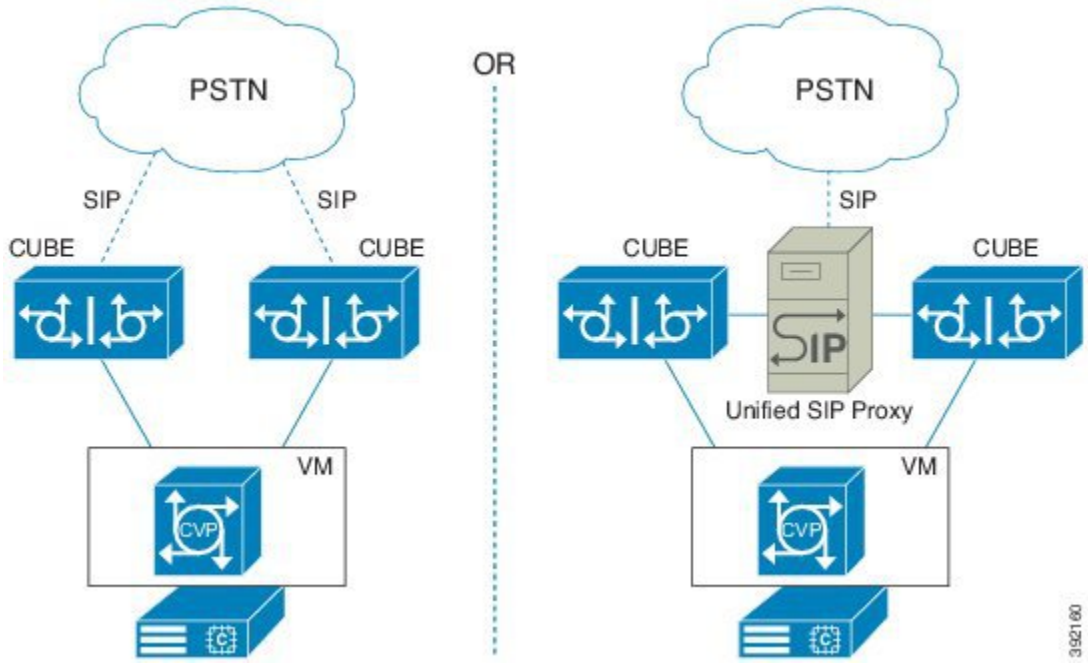
高可用性のコンタクトセンター設計は、データ、マルチメディア、音声トラフィック用のネットワーク インフラストラクチャから開始します。ネットワーク インフラストラクチャの「シングル ポイント障害」は、コンタクトセンターに設計したその他高可用性機能を低く評価します。PSTN から開始し、着信コールに、初期処理とキューイングのために Unified CVP に到達するための複数のパスがあることを確認します。

それぞれ別個の Cisco Unified Border Element（CUBE）に接続する、少なくとも 2 つの SIP トランクを備えた設計が理想です。CUBE トランクまたは SIP トランクに障害が発生した場合、PSTN は残りの SIP トランクを経由してすべてのトラフィックをルーティングできます。すべての SIP トランクを大規模トランクグループとして構成定するか、他の SIP トランクへの再ルーティングまたはオーバーフロー ルーティングを構成することで、PSTN ルートを設定します。Cisco UBE に障害が発生した場合でも SIP トランクが起動している場合、また、冗長 CUBE を各 SIP トランクに接続して、キャパシティを維持できます。

一部のエリアでは、PSTNは、複数のSIPトランクを単一サイトに提供しない場合があります。その場合は、SIP トランクを Cisco Unified SIP Proxy（CUSP）に接続できます。その後、複数の CUBEs を CUSP に接続して、冗長性を提供できます。

CUBE は、初回処理とキューリングのために Unified CVP にコールを渡します。各 CUBE を、負荷分散用の個別の Unified CVP で登録します。フォールトトレランスをさらに高めるには、バックアップとして各 CUBE を異なる Unified CVP に登録します。CUBE を Unified CVP に接続できない場合は、TCL スクリプトを使用していくつかのコール処理を実行することもできます。TCL スクリプトでは、コールを別のサイトまたはダイヤル番号に再ルーティングできます。スクリプトは、ローカルに保存されている .wav ファイルを発信者に再生して通話を終了することもできます。

Figure 6: 高可用性の入力点



CUBE、Unified CVP および一般的な音声ネットワークに関しては、http://www.cisco.com/en/US/docs/voice_ip_comm/uc_system/design/guides/UCgoList.html の『*Cisco Collaboration System Solution Reference Network Designs*』を参照してください。

Cisco Unified Survivable Remote Site Telephony（SRST）

Unified CM に対して Cisco Unified Survivable Remote Site Telephony（SRST）オプションを使用する音声ゲートウェイは、同様のフェールオーバープロセスに従います。ゲートウェイが制御サブスクライバから切断されている場合、ゲートウェイは SRST モードにフェールオーバーします。フェールオーバーによってすべての音声コールがドロップされ、ゲートウェイが SRST モードにリセットされます。電話機をローカル呼制御のためにローカル SRST ゲートウェイにリホームします。

SRST モードで実行されている間、Unified CCE は、エージェントがデスクトップから CTI 接続を持っているかのように動作します。ルーティング アプリケーションは、エージェントの準備が完

了しておらず、これらエージェントに通話が送信されていないことを検出します。ゲートウェイとサブスクライバが接続を再確立すると、サブスクライバはゲートウェイと電話機を再度制御することで、エージェントが再接続できます。

イングレスおよびエグレスゲートウェイの高可用性

イングレスゲートウェイは、PSTN からの通話を受け入れ、その通話を VRU 処理およびコールルーティングのために Unified CVP にリダイレクトします。同じゲートウェイは、特定のコールフロー内のエグレスゲートウェイとして機能できます。

Note イングレスゲートウェイは、発信ゲートウェイと呼ばれる場合があります。

Contact Center Enterprise リファレンス設計では、イングレスゲートウェイは、SIP を使用して、Unified CVP と通信します。SIP プロトコルには冗長性機能が組み込まれていません。SIP は、冗長性をゲートウェイとコール処理コンポーネントに依存します。次のテクニックを使用すると、コールシグナリングを物理インターフェイスから独立させることができます。一方のインターフェイスに障害が発生した場合、もう一方のインターフェイスがトラフィックを処理します。

ダイヤルピアバインド

ダイヤルピアレベルバインドでは、各ダイヤルピアに対して異なるバインドを設定します。すべてのサブネットから到達可能な 1 つのインターフェイスを保持する必要はありません。ダイヤルピアは、さまざまなネットワークからのトラフィックを分離するのに役立ちます（たとえば、サービスプロバイダーの SIP トランクおよび SIP トランクから Unified CM または CVP へ）。次の例は、ダイヤルピアレベルのバインドを示しています。

```
Using voice-class sip bind
 dial-peer voice 1 voip
 voice-class sip bind control source-interface GigabitEthernet0/0
```

グローバルバインド

他のゲートウェイでは、グローバルバインドを使用できます。各ゲートウェイインターフェイスを別の物理スイッチに接続して冗長性を提供します。各ゲートウェイインターフェイスは、異なるサブネット上に IP アドレスを持っています。IP ルータは、静的ルートまたはルーティング プロトコルのいずれかによって、ループバックアドレスへの冗長ルートを使用します。

ルーティングプロトコルを使用すると、ゲートウェイと交換されるルートの数を確認できます。その場合は、フィルタを使用してルーティングの更新を制限します。ゲートウェイにループバックアドレスのみをアドバタイズさせ、受信ルートをアドバタイズしないようにします。次の例に示すように、SIP シグナリングを仮想ループバック インターフェイスにバインドします。

```
voice service voip
 sip
  bind control source-interface Loopback0
  bind media source-interface Loopback0
```

フェールオーバー中のコール存続可能性

ゲートウェイに障害が発生した場合、コール廃棄には次の条件が適用されます。

- **進行中のコール** — PSTN スイッチは、このゲートウェイのすべての T1/E1 トランクへの D-チャネルを失います。アクティブ コールは保存されません。
- **着信通話** — PSTN キャリアは、代替ゲートウェイの T1/E1 に通話を転送します。PSTN スイッチのトランクを保持する必要があり、ダイヤルプランは正しく構成されている必要があります。

VXML ゲートウェイの高可用性

VXML ゲートウェイは、Unified CVP VXML サーバまたは外部 VXML ソースから VXML ドキュメントを解析およびレンダリングします。VXML ドキュメントのレンダリングには、次を含めます。

- 事前録音されたオーディオファイルの取得と再生
- ユーザ入力の収集と処理
- 音声認識および動的音声合成変換のために ASR/TTS サーバに接続

VXML ゲートウェイと Unified CVP コールサーバ間のパスではロードバランサは使用できません。

Unified CVP コールサーバからイングレスゲートウェイを区別するトポロジでは、コールサーバサイトで VXML ゲートウェイを同一場所に配置します。この配置により、メディアストリームが WAN 全体の帯域幅を使用するのを防ぎます。

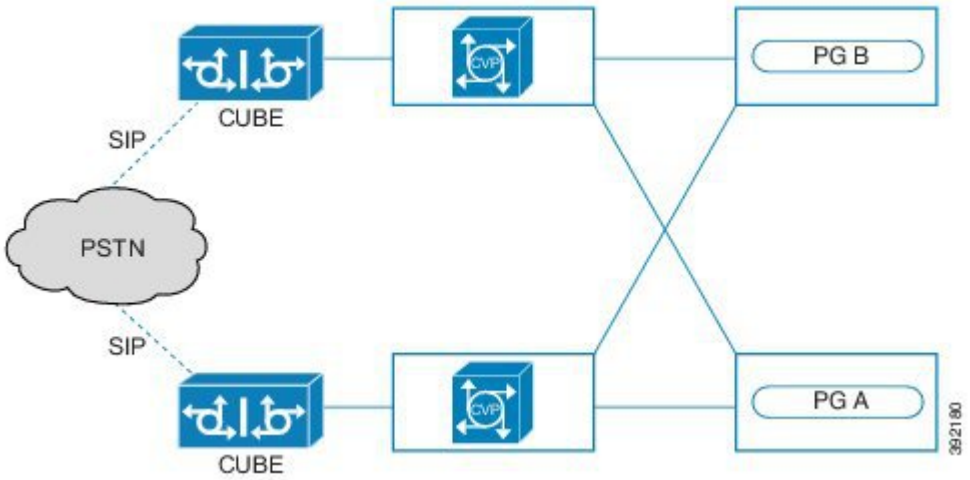
VXML ゲートウェイが失敗すると、コールは次のように影響を受けます。

- **進行中のコール：** イングレスゲートウェイの存続可能性機能は、デフォルトで進行中のコールを代替のロケーションにルートします。
- **着信コール：** 着信コールは、代替 VXML ゲートウェイを検索します。

CVP 高可用性の考慮事項

Contact Center Enterprise リファレンス設計 は、コールの扱いとキューに対して Unified CVP を使用します。CVP は、JTAPI 呼制御向けの Unified CM ではなく、呼制御向けの SIP を使用します。

Figure 7: Unified CVP 高可用性の展開



Unified CVP は、次のシステムコンポーネントを使用できます。

- Cisco Unified Border Element（CUBE）は、SIP トランキングへの移行をサポートします。CUBE は、PSTN とコンタクトセンター間でインターワーキング、責任分界、セキュリティサービスを提供します。
- Cisco Voice Gateway（VG）は、DM PSTN トランクを終了して、IP ネットワーク上の IP ベースのコールに変換します。Unified CVP は、SIP をサポートする特定の Cisco IOS 音声ゲートウェイを使用して、より柔軟な呼制御を実現します。Unified CVP によって制御される VG は、Cisco IOS の組み込み Voice Extensible Markup Language（VoiceXML）ブラウザを使用して、発信者やコールキューを処理します。CVP は、Cisco IOS VG の Media Resource Control Protocol（MRCP）インターフェイスを利用して、自動音声認識（ASR）と音声合成（TTS）機能を追加することもできます。
- コールがイングレスゲートウェイと別のエンドポイントゲートウェイまたは Unified CCE エージェント間で切り替わった際、CVP サーバは、呼制御シグナリングを提供します。CVP サーバは、Unified CCE VRU 周辺機器ゲートウェイ（PG）にもインターフェイスを提供します。CVP サーバは、特定の Unified CCE VRU コマンドを VXML コードに変換して、VG 上でレンダリングします。ソリューションの一部として CVP サーバは、SIP を使用してゲートウェイと通信できます。高可用性の議論については、次のサブコンポーネントとして CVP サーバを表示できます。
  - **SIP サービス**：すべての着信 SIP メッセージングと SIP ルーティングを担当します。

Note コールサーバを構成し、アウトバウンド ダイヤル プランの解決に対する SIP プロキシサーバを使用します。SIP プロキシサーバは、構成オーバーヘッドを最小限に抑えます。

IP アドレスまたは DNS SRV に基づいて静的ルートを使用するためにも構成します。コールサーバは、静的ルートの構成情報を共有しません。静的ルートを変更する場合は、各コールサーバの SIP サービスで変更する必要があります。

- **ICM サービス**：ICM へのインターフェイスを担当します。ICM サービスは、GED-125 を使用して VRU PG と通信し、ICM で IVR 制御が可能になります。

- CVP メディアサーバは、VXML 処理の一部として、事前に定義された音声ファイルを音声ブラウザに提供する Web サーバとして機能します。Cisco コンテンツサービススイッチ（CSS）製品を使用して メディアサーバをクラスタ化できます。クラスタリングすることで、すべての音声ブラウザからアクセスできるように 1 つのURLの背後に複数の メディアサーバをプールできます。
- CVP サーバは、Unified CVP VXML ランライム環境をホストします。VXML サービス作成環境では、CVP Call Studio アプリケーションで Eclipse Toolkit ブラウザを使用します。ランタイム環境は、動的 VXML アプリケーションを実行し、外部システムおよびデータベースアクセスに対する Java サービスおよび Web サービス呼び出しを処理します。
- CVP で使用される Cisco Unified SIP Proxy（CUSP）サーバは、音声ブラウザを選択して、特定のダイヤル番号に関連付けます。ネットワークに入電すると、VG は Unified SIP プロキシにクエリして、ダイヤルされた番号に基づいてコールを送信する場所を特定します。

Important Contact Center Enterprise ソリューションは、Unified CM のクラスタ間 Enhanced Location Call Admission Control（ELCAC）機能をサポートしません。

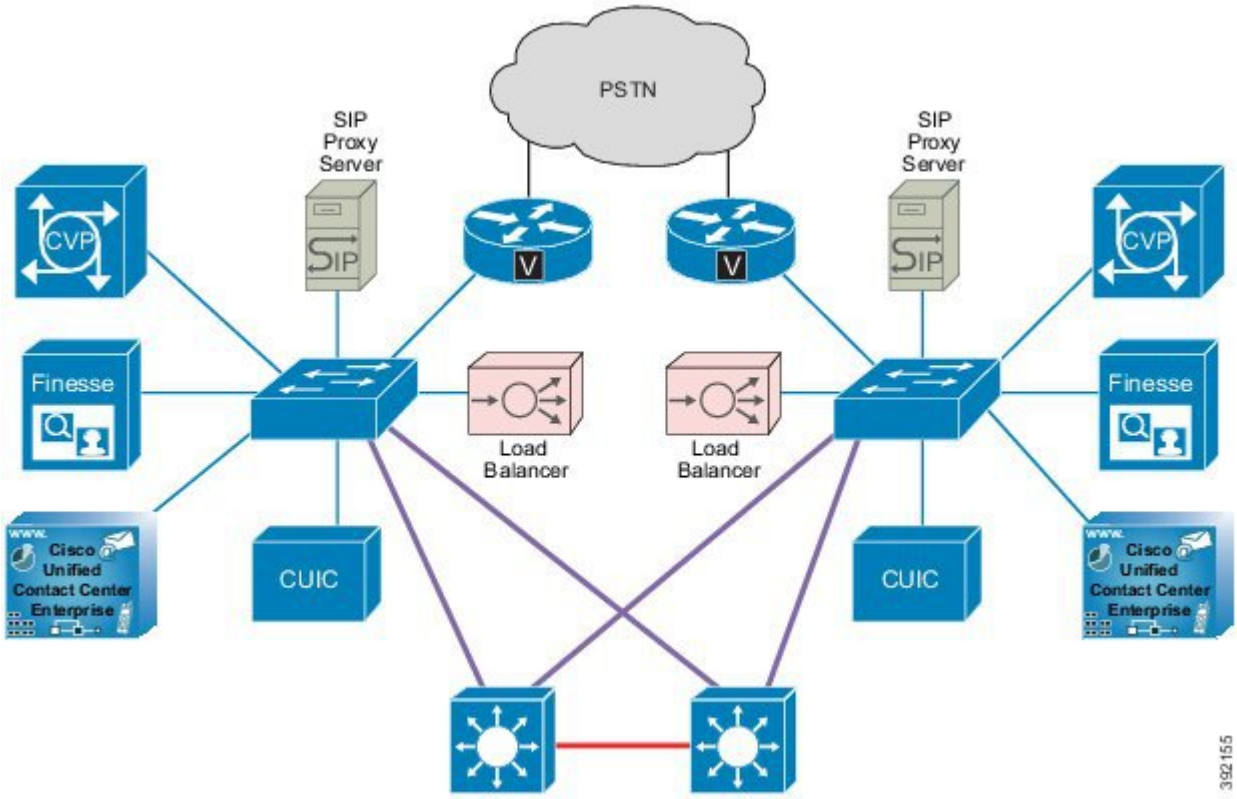
次の方法により、CVP の高可用性が向上します。

- CVP サーバ全体で自動コール バランスを提供するには、Unified CCE PG の制御下に冗長の CVP サーバを追加します。
- ゲートウェイが CVP サーバに接続できない条件を処理するには、存続可能性 TCL スクリプトをゲートウェイに追加します。たとえば、別の CVP が制御するゲートウェイ上の別の CVP サーバにコールをリダイレクトできます。
- 複数の CVP メディアサーバ間で音声ファイル要求と複数のサーバにわたる VXML URL アクセスを負荷分散するには、Cisco Content サーバを追加します。

この図は、フォールトトレラント Unified CVP システムのハイレベルなレイアウトを示しています。Unified CVP サイトの各コンポーネントは、冗長性を実現するために複製されています。これ

らのコンポーネントそれぞれの数は、特定の展開に対して予想される最繁時呼数（BHCA）に応じて異なります。

Figure 8: 冗長性のある ***Unified CVP*** システム



図にある 2 つのスイッチは、Unified CVP サーバのネットワーク冗長性を提供します。一方のスイッチに障害が発生しても、アクセスできなくなるのは、コンポーネントの 1 つのサブセットだけです。残りのスイッチに接続されているコンポーネントは、引き続きコール処理でアクセスできます。

バランスを取る高可用性の要因

CVP に次のコンポーネントとサブコンポーネントを追加することで、Contact Center Enterprise ソリューションの高可用性を実現できます。

- **複数ゲートウェイ、Unified CVP サーバ、Unified CVP VXML サーバ、および VRU PG** — インバウンドとアウトバウンドコールの処理および VRU サービスが個々のコンポーネント障害時に継続できます。
- **Unified CVP メディアサーバ** — プライマリメディアサーバが到達不可の場合、VVoice ブラウザが、リクエストをバックアップメディアサーバに送信します。適切なフェールオーバーを発生させるため、すべてのメディアサーバで、ウィスパーアナウンスメントとエージェントグリーティング音声ファイルが重複しているかを確認します。

- **複数のコール処理ロケーション**—コール処理ロケーションが暗くなっている場合に、コール処理を引き続きできるようにします。
- **冗長 WAN リンク** — 各 WAN リンクに障害があった場合、Unified CVP コール処理をできるようにします。

フェールオーバー中のコール存続可能性

次の項では、コール存続可能性に対する Contact Center Enterprise コンポーネントと CVP サブコンポーネントの障害の影響度を説明します。

音声ブラウザ

音声ブラウザは、1 つまたは複数のソースから取得した VXML ドキュメントを解析してレンダリングします。VXML ゲートウェイで障害が発生すると、次の処理が行われます。

- **進行中のコール：**イングレスゲートウェイの存続可能性機能は、デフォルトで進行中のコールを代替のロケーションにルートします。
- **着信コール：**着信コールは、代替 VXML ゲートウェイを検索します。

Unified CVP IVR サービス — CVP IVR サービスは、Unified CVP Micro アプリケーションを実装する VXML ページを作成します。マイクロアプリケーションは、Unified CCE から受信した RunExternalScript 指示に基づいています。IVR サービスで障害が発生すると、次の処理が行われます。

- **進行中のコール** — 発信ゲートウェイの存続可能性によって、進行中のコールはデフォルトで、代替ロケーションにルートされます。
- **着信コール** — 着信コールは、アクティブな IVR サービスにダイレクトされます。

Unified CM

CVP コールサーバは、Unified CM の障害を認識すると、次を実行します。

- **進行中のコール**—サーバは、アクティブコールを保持する必要があると想定し、発信ゲートウェイへのシグナリングチャネルを維持します。発信ゲートウェイは、Unified CM の障害を認識しません。アクティブコールでそれ以上のアクティビティ（保留、転送、会議など）を行うことはできません。終話後、電話機は別の Unified CM サーバにルーティングされます。
- **着信コール** — 着信コールは、クラスタ内の代替 Unified CM サーバにダイレクトされます。

CVP コール サーバ

CVP コールサーバには、フェールオーバー中にコールの存続可能性を処理する次のサービスが含まれます。

- **Unified CVP SIP サービス** — CVP SIP サービスは、すべての着信および発信 SIP メッセージおよびSIPルーティングを処理します。SIPサービスで障害が発生すると、次の処理が行われます。
  - **進行中のコール** — 発信者の転送後に、CVP SIP サービスに障害が発生すると（IP 電話または音声ブラウザへの転送を含む）、コールは引き続き通常通り動作します。ただし、CVP SIP サービスは、そのコールを再度転送できません。発信者が転送される前に障害が発生した場合、デフォルトの存続可能ルーティングは、コールを別の場所に転送します。
  - **着信コール** — Unified SIP Proxy は、着信コールを代替 Unified CVP コールサーバにダイレクトします。使用可能なコール サーバがない場合、コールは、存続可能性によって代替場所のデフォルトのルートにルーティングされます

CVP メディアサーバ

オーディオファイルは、VXML ゲートウェイにあるフラッシュメモリか、HTTP または TFTP File サーバにローカルで保存されます。ローカルに保存されたオーディオファイルは高可用性です。ただし、HTTP または TFTP File サーバには、音声ファイルの集中管理という利点があります。

メディアサーバに障害が発生すると、次の処理が行われます。

- **進行中のコール**—進行中のコールは自動的に復元します。高可用性構成手法により、発信者に対して障害が透過的になります。メディアリクエストに失敗した場合は、スクリプト手法を使いエラーを回避します。
- **着信コール** — 着信コールは、バックアップのメディアサーバに透過的にダイレクトされ、サービスは影響されません。

Note メディアサーバは、VXML ゲートウェイから WAN を介して見つけることができます。WAN 接続に障害が発生している場合、ゲートウェイは、リクエスト済みのプロンプトの期限が切れるまで、引き続きゲートウェイキャッシュからのプロンプトを使用します。その後、ゲートウェイは、メディアの再取得を試行し、存続可能が有効でない場合、コールは失敗します。存続可能性が有効になっている場合、コールはデフォルトのルートにルーティングされます。

CVP VXML サーバ

Unified CVP VXML サーバは、音声ブラウザと VXML ページを交換することにより、高度な VRU アプリケーションを実行します。CVP VXML サーバに障害が発生すると、次の処理が行われます。

- **進行中のコール** — 進行中のコールは、スクリプト技術を使用して、Unified CCE が統合された展開で復元できます。たとえば、最初に Unified CVP VXML サーバ A に接続するようにスクリプトを構成します。Unified CVP VXML Server ICM スクリプトノードの X パスでアプリケーションに障害が発生した場合、Unified CVP VXML サーバ B が試されます。

- **着信コール** — 着信コールは、透過的に代替 CVP VXML サーバにダイレクトされます。

CVP レポートサーバ

CVP コールサーバの障害は、コールの存続可能性に影響を与えません。

コールサーバは、バックアップおよび消去などの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。単一の CVP 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。データの安全とセキュリティは、データベース管理システムによって提供されます。ソースコンポーネント上の情報の永続的なバッファリングにより、一時的な停止が許容されます。

より多くのコール存続可能性ポイント

ソリューションでコールの存続可能性を計画する場合は、次の点を検討してください。

- 障害時にコールリカバリができないシナリオがあります。
  - 進行中のコールを含むプロセスが停止された場合。たとえば、システム管理者が、コールサーバをシャットダウンし忘れたとします。この場合、CVP サーバは、ライセンスをリリースするためにすべてのアクティブコールを終了します。
  - コール サーバが推奨コール レートを超えた場合。コールサーバで許可されるコールの数には制限があります。ただし、通話料金に強制的な制限はありません。一般に、推奨される毎秒の通話（CPS）を長時間超える場合、一貫性がなく、予測不能な通話の動作が発生します。ソリューションのサイズを正しく設定し、各コール処理コンポーネント全体でコールの負荷を適切に分散します。
- 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* に説明のあるコール存続可能性の発信ゲートウェイを構成します。`survivability.tcl` スクリプトには指示と有用な情報も含まれています。
- Unified CVP の知識がなくてもクリアされた通話を検出できます。
  - Unified CVP は、設定時間（デフォルトでは 120 分）を超える長さの着信コールを 2 分ごとにチェックします。
  - これらのコールについて、Unified CVP は UPDATE メッセージを送信します。メッセージが拒否または送信不能を受信すると、コールがクリアされ、ライセンスがリリースされます。
- CVP SIP サービスが、コールにセッションの期限切れヘッダーを追加することで、エンドポイントは、独自にセッションを更新できます。RFC 4028（セッションボーダーコントローラのセッションタイマー）には、SIP コールでのセッション切れの使用方法に関する詳細が含まれています。
- フェールオーバー中に、Unified CVP 制御下のコールは、イングレス音声ゲートウェイ存続可能性 TCL スクリプトから処理を行います。このような場合、Unified CCE セントラルコント

ローラのルーティング ダイアログが停止します。存続可能性スクリプトが通話を別のアクティブ Unified CCE コンポーネントにリダイレクトした場合、通話はレポートや追跡目的で、元の通話とは関係がない状態で、「新規通話」としてシステムに表示されます。

CVP を使用する SIP Proxy サーバ

SIP Proxy サーバは、SIP エンドポイントのダイヤルプラン解決を提供します。ダイヤルプラン情報は、各 SIP デバイスで静的に構成する代わりに、中央で設定できます。ソリューションに SIP Proxy サーバは不要です。中央集中型の構成とメンテナンスの利点を検討してください。複数の SIP Proxy サーバを展開することで、負荷分散、冗長性、地域の SIP コール ルーティング サービスを実現できます。ソリューションには、SIP コールルーティングに関して次の選択肢があります。

SIP Proxy サーバ

SIP Proxy サーバには、次の利点があります。

- 加重ロード バランシングおよび冗長性。
- 集中型ダイヤル プラン コンフィギュレーション。
- すでに SIP プロキシを使用している場合、または他のアプリケーションでダイヤルプランの解決やクラスタ間コールルーティングに使用されている場合は、既存の資産を活用できます。

ただし、SIP Proxy サーバには別のサーバが必要な場合があります。

DNS サーバ上でサーバグループ（DNS SRV レコード）を使用する静的ルート

この種の静的ルーティングにより、重み付けされた負荷分散と冗長性を実現できます。

ただし、この方法では次の欠点があります。

- 既存のサーバを使用する機能は、DNS サーバの場所によって異なります。
- 組織によっては、DNS サーバの管理権限を共有または代理する機能が制限されています。
- ダイヤルプランは、各デバイスで個別に構成する必要があります（Unified CM、Unified CVP、およびゲートウェイ）。
- Unified CVP は、すべてのコールに対して DNS SRV ルックアップを実行します。DNS サーバの応答が遅い、利用できない、または WAN をまたがった場合、パフォーマンスに問題が発生します。

ローカル DNS SRV レコードを使用した静的ルート

次の利点は、次のタイプの静的ルーティングで実現できます。

- 加重ロード バランシングおよび冗長性。

- 外部 DNS サーバに依存しない遅延、DNS サーバパフォーマンス、および障害のポイントに関する懸念を排除します。

しかし、ダイヤルプランは、各デバイスで個別に構成する必要があります（Unified CM、Unified CVP、およびゲートウェイ）。

Note DNS サーバを使用する SRV を使用する静的ルート、またはサーバグループを使用すると、フェールオーバーと負荷分散中に予想外の遅延が長く発生する可能性があります。これは、プライマリ接続先がシャットダウンされている、またはネットワークがオフの場合に、Unified CVP コールサーバ上の TCP または UDP トランスポートで発生します。UDP では、ホスト名にサーバグループ（srv.xml）の優先順位の異なる要素がある場合、Unified CVP は要素ごとに 2 回試行し、遅延は 500 ミリ秒となります。遅延は、負荷分散に応じて、障害発生中に各コールに発生し、T1 タイマーに関する RFC 3261 の 17.1.1.1 項に準拠します。サーバ グループのハートビートがオンになっている場合、要素のステータスに応じて、遅延は 1 回だけ発生するか、まったく発生しない可能性があります。

Cisco Unified SIP プロキシサポート

Cisco Unified SIP Proxy（CUSP）は SIP Proxy サーバの実装です。CUSP は、ゲートウェイまたは仮想マシン上で実行される専用の SIP Proxy サーバです。

CUSP 展開オプション

以下の項では、Contact Center Enterprise ソリューションで CUSP を展開するためのオプションについて説明します。

冗長 SIP Proxy サーバ

このオプションでは、2 つのゲートウェイを使用し、それぞれに 1 つのプロキシ VM を設定します。ゲートウェイは冗長性のため地理的に分離されています。プロキシの冗長性には SRV 優先順位が使用され、HSRP は使用しません。

このオプションを選択する場合は、次の点に注意してください。

- 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。
- CUSP はサーバグループと一緒に設定され、プライマリおよびバックアップの Unified CVP、Unified CM、および音声ブラウザを検索します。
- 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。

この例では、ISR1 が東海岸にあり、ISR2 が西海岸にあります。TDM ゲートウェイは、最も近い ISR を使用し、セカンダリ 優先順位ブレードに失敗した場合にのみ WAN を交差します。

SRV レコードは、次のようになります。

```
east-coast.proxy.atmycompany.com
blade 10.10.10.10 priority 1 weight 10 (this blade is in ISR1 on east coast)
blade 10.10.10.20 priority 2 weight 10 (this blade is in ISR2 on west coast)

west-coast.proxy.atmycompany.com
blade 10.10.10.20 priority 1 weight 10 (this blade is in ISR2 on west coast)
blade 10.10.10.10 priority 2 weight 10 (this blade is in ISR1 on east coast)
```

二重キャパシティの冗長 SIP Proxy サーバ

このオプションでは、2 つのゲートウェイを使用し、それぞれに 2 つのプロキシ VM を用意します。4 つのプロキシサーバすべてがアクティブモードで、コールはプロキシサーバ間でバランスが保たれます。ゲートウェイは冗長性のため地理的に分離されています。これらは、SRV 優先順位を使用して、優先順位を持つプロキシ全体の負荷分散を行います。

このオプションを選択する場合は、次の点に注意してください。

- CUSP のプラットフォーム検証制限により、ISR はプロキシブレード機能専用です。ISR は、音声ブラウザとして、また TDM ゲートウェイとして併置されません。
- 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。
- CUSP はサーバグループと一緒に設定され、プライマリおよびバックアップの Unified CVP、Unified CM、および音声ブラウザを検索します。
- 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。

この例では、ISR1 が東海岸にあり、ISR2 が西海岸にあります。TDM ゲートウェイは、最も近い ISR を使用し、セカンダリ 優先順位ブレードに失敗した場合にのみ WAN を交差します。

SRV レコードは、次のようになります。

```
east-coast.proxy.atmycompany.com
blade 10.10.10.10 priority 1 weight 10 (this blade is in ISR1 on east coast)
blade 10.10.10.20 priority 1 weight 10 (this blade is in ISR1 on east coast)
blade 10.10.10.30 priority 2 weight 10 (this blade is in ISR2 on west coast)
blade 10.10.10.40 priority 2 weight 10 (this blade is in ISR2 on west coast)

west-coast.proxy.atmycompany.com
blade 10.10.10.30 priority 1 weight 10 (this blade is in ISR2 on west coast)
blade 10.10.10.40 priority 1 weight 10 (this blade is in ISR2 on west coast)
blade 10.10.10.10 priority 2 weight 10 (this blade is in ISR1 on east coast)
blade 10.10.10.20 priority 2 weight 10 (this blade is in ISR1 on east coast)
```

高可用性に向けた CUSP 設計

次の点は、CUSP の高可用性に影響します。

- **プロキシ サーバ レコード ルートを使用しない**— このオプションは、プロキシサーバのパフォーマンスに影響し、「シングルポイント障害」を発生させます。このオプションはオンにしないでください。

  RecordRoute ヘッダーが入力されていない場合、着信コールが Unified CVP コールサーバに到達すると、シグナリングが CUSP をバイパスします。ルーティングのその時点から、シグナリングは発信元デバイスから CVP コールサーバに直接実行されます。

- **SIP ハートビートがあるアップストリーム要素ルーティング** — CUSPは、INVITE または OPTIONS への応答を良い応答として扱います。したがって、CUSP は、応答を受信したときに要素をダウンとしてマークしません。サーバグループのフェールオーバー応答コードリストで応答が構成されている場合、CUSPはグループ内の次の要素にフェールオーバーします。それ以外の場合、CUSP は、最終応答として応答をダウンストリームに送信します。

サーバグループと CVP 高可用性

サーバグループは、ダイナミックルーティング機能です。送信元のエンドポイントは、サーバグループを介して、SIP INVITE を送信する前に接続先アドレスのステータスを確認できます。ハートビートメソッドは、送信元 SIP ユーザに関する宛て先のステータスを伝えます。この機能を使用すると、障害のあるエンドポイントが原因の遅延をなくすことによって、呼制御のフェールオーバーを高速化できます。

サーバグループは、1 つ以上の接続先アドレス（エンドポイント）で構成されています。サーバグループには、SRV クラスタドメインとして知られるドメイン名または FQDN があります。サーバグループは、ローカル SRV 実装（`srv.xml`）のように機能しますが、サーバグループは、オプションとして SRV に追加のハートビートメソッドを追加します。この機能が対象としているのは、Unified CVP からの発信コールだけです。Unified CVP への着信コールを対象に含めるために、SIP Proxy サーバは、類似のハートビートを Unified CVP に送信できます。Unified CVP は、ステータス応答で応答できます。

Note

- Unified CVP および SIP Proxy サーバのサーバグループは、同じように機能します。
- サーバグループは、その中で定義されたエンドポイントに対して、ハートビートだけを送信します。
- 録音ルートが OFF に設定されている場合、mid-dialog SIP メッセージは、サーバグループで定義された要素をバイパスします。これらメッセージには、REFERs または REINVITES が含まれます。これらのメッセージは、ダイアログで他のエンドポイントに直接配信されます。

Unified CCE の高可用性に関する検討事項

Unified CCE のサブコンポーネントは、手動による操作を行わずにほとんどの障害シナリオから復旧できます。冗長アーキテクチャにより、ソリューションは単一のサブコンポーネント障害シナ

リオでのコールの処理を継続できます。複数のサブコンポーネントが同時に障害を起こすことはまれですが、ビジネス運用が中断されます。

冗長性とフォールトトレランス

ペア化された冗長方法でルータと Logger を展開します。冗長化された導入の 2 つのサイドは、サイド A とサイド B と呼ばれます。たとえば、ルータ A とルータ Bが、2 つの異なる VM で実行しているルータの冗長インスタンスです。通常動作では、両サイドが実行されています。一方のサイドがダウンしている場合は、構成がスタンドアロンモードで実行されています。これらのモードは、デュプレックスモードおよびシンプレックスモードと呼ばれる場合があります。

Note ルータと Logger のスタンドアロン（シンプレックス）展開は、実稼働環境ではサポートされていません。これらのコンポーネントは、冗長ペアで展開しなければなりません。

この 2 つのサイドは冗長性を備え、負荷分散用ではありません。いずれのサイドも、ソリューションの完全な負荷を実行できます。サイド A と B はどちらも同じメッセージ一式を実行し、同じ結果を生成します。論理的には、ルータは 1 つのみです。同期された実行とは、両サイドがすべてのコールを処理するという意味です。障害が発生すると、存続しているルータが通話の途中で引き継ぎ、ユーザの介入なしに続行します。

周辺機器ゲートウェイ（PG）コンポーネントは、ホットスタンバイモードで実行されます。1 つの PG だけがアクティブで、Unified CM または適切な周辺機器を制御します。アクティブな方で障害が発生すると、存続している方は、自動で引継ぎ処理を行います。障害中、存続している方は、冗長側が復元されるまでスタンドアロンモードで実行されます。その後、PG は自動的に冗長運用に戻ります。

Administration & Data サーバは、構成とリアルタイムデータを処理し、フォールトトレランスのためにペアで展開されます。拡張性の目的で複数のペアを展開できます。履歴データ向けの Administration & Data サーバは、冗長性および拡張性向けの N+1 アーキテクチャに従います。各 Administration & Data サーバには、推奨およびプライマリデータソースとして、Logger（サイド A または B）があります。

ルータの高可用性に関する考慮事項

多数のデバイスとフェールオーバー

デバイスの大半は、ルータが無効な状態にするかどうかを決定します。ルータは、冗長ルータとの接続を失ったデバイスの大半を確認します。各ルータは、ルータ自体のデバイスの過半数を決定します。なし、1 つ、または両方のルータが同時にデバイスの過半数を持つことができます。

デバイスの過半数を持つには、ルータが次のいずれかの条件を満たす必要があります。

- ルータはサイド A ルータであり、有効な PG 全体の少なくとも半分と通信できる。
- ルータはサイド B ルータであり、有効な PG 全体の半分以上と通信できる。

ルータ フェールオーバーのシナリオ

エージェント PG リンクに障害が発生した CTI Manager

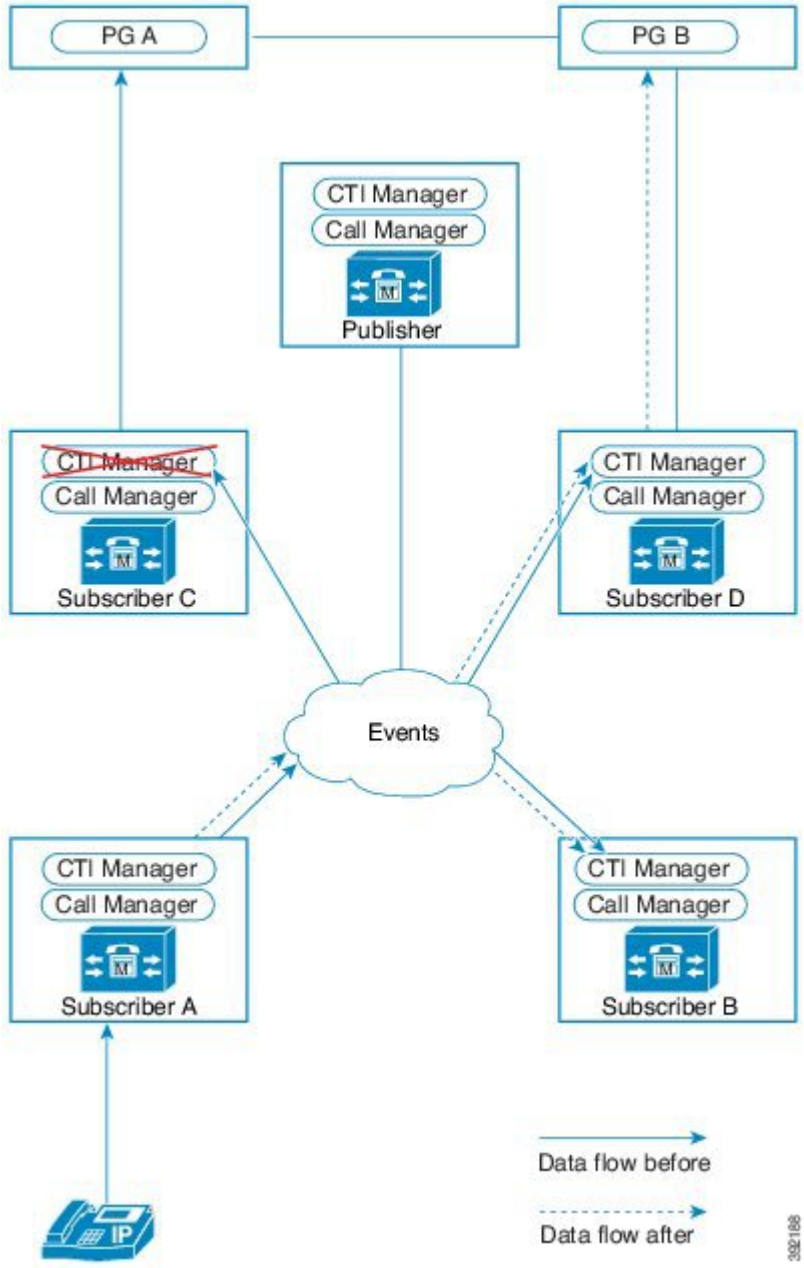
各 エージェント PG は1つの CTI Manager 接続のみをサポートします。各サブスクライバには CTI Manager がありますが、通常は 2 つのサブスクライバのみが エージェント PG に接続します。4 サブスクライバ クラスタ 内のすべてのサブスクライバがエージェント PG に直接接続できるようにするには、エージェント PG の別のペアを追加する必要があります。

以下の図は、エージェント PGへの接続がある CTI Manager の障害を示しています。サブスクライバ C および D のみが、エージェント PG に接続するように構成されています。

以下の条件がシナリオに適用されます。

- 冗長性のために、サブスクライバ A に登録されているすべての電話とゲートウェイは、サブスクライバ B をバックアップ サーバとして使用します。
- サブスクライバ C および D の CTI Manager は、エージェント PGに JTAPI サービスを提供します。

Figure 9: エージェント *PG* 接続を使用する *CTI Manager* に障害が発生します



障害復旧は次のように発生します。

1. サブスクライバ C の CTI Manager に障害が発生すると、エージェント PG サイド A は障害を検出し、PG サイド B にフェールオーバーします。
2. エージェント PG サイド B は、サブスクライバ D の CTI Manager を使用してすべてのダイヤル番号と電話機を登録し、コール処理を続行します。

3. 進行中のコールはアクティブな状態が続きますが、エージェントがサインインするまで、エージェントは転送などの電話サービスを使用できません。
4. サブスクライバ C の CTI Manager が復旧すると、エージェント PG サイド B はアクティブであり続け、サブスクライバ D の CTI Manager を使用します。このモデルではエージェント PG は、フェールバックしません。

CTI Manager からエージェント PG へのリンクが正常なサブスクライバ

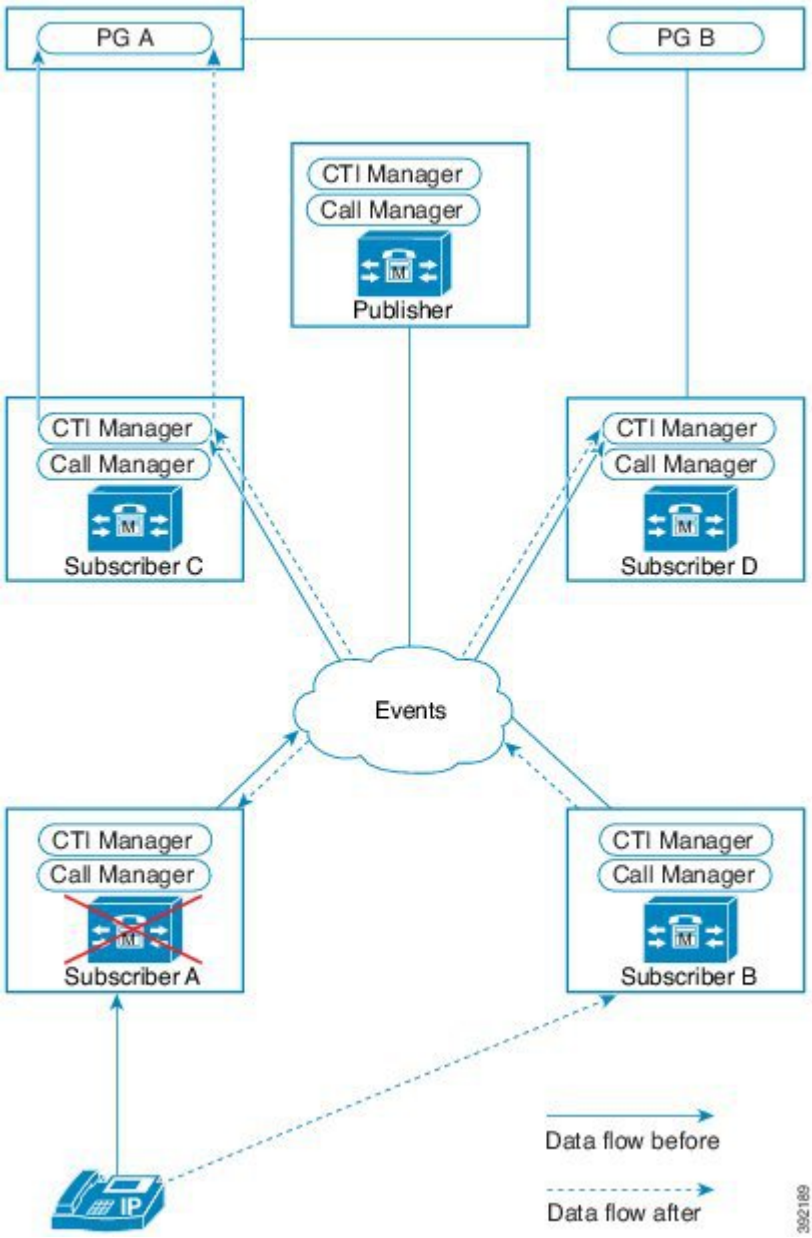
各 エージェント PG は1つの CTI Manager 接続のみをサポートします。各サブスクライバには CTI Manager がありますが、通常は 2 つのサブスクライバのみが エージェント PG に接続します。4 サブスクライバ クラスタ 内のすべてのサブスクライバがエージェント PG に直接接続できるようにするには、エージェント PG の別のペアを追加する必要があります。

次の図は、エージェント PG に直接接続できないサブスクライバ A の障害を示しています。

以下の条件がシナリオに適用されます。

- 冗長性のために、サブスクライバ A に登録されているすべての電話とゲートウェイは、サブスクライバ B をバックアップ サーバとして使用します。
- サブスクライバ C と D はエージェント PG に接続し、CTI Manager のローカルインスタンスは、PG に JTAPI サービスを提供します。

Figure 10: エージェント *PG* へのリンクのない *Unified Communications Manager* の障害



障害復旧は次のように発生します。

1. サブスクライバ A に障害が発生した場合、登録された電話機とゲートウェイがバックアップサブスクライバ B に対して再設定されます。
2. エージェント PG サイド A はアクティブな状態が維持され、サブスクライバ C の CTI Manager に接続されます。JTAPI と CTI Manager 間の接続に障害が発生していないため、PG はフェールオーバーしません。ただし、PG は電話機とデバイスの登録が自動的にサブスクライバ A からサブスクライバ B に切り替わるのを検出します。

3. コール処理は、サブスクライバ A に登録されていないデバイスで続行されます。
4. エージェントの電話機が登録されていない場合、エージェント PG はエージェントデスクトップを無効にします。この応答は、エージェントがサブスクライバ接続なしでシステムを使用するのを防ぎます。エージェント PG は、コールをエージェントにルートしないように、この移行中にエージェントをサインアウトします。
5. 電話機がバックアップサブスクライバを再登録した後、コール処理が再開されます。
6. 進行中のコールは、サブスクライバ A に登録された電話機で継続されますが、エージェントが再度サインインするまで、転送のような電話サービスを使用することはできません。
7. 進行中のコールが終了すると、その電話機はバックアップサブスクライバに再登録されます。エージェント PG は、コールをエージェントにルートしないように、この移行中にエージェントをサインアウトします。
8. サブスクライバ A が復元すると、電話機とゲートウェイは、復元したサブスクライバ A にリホームされます。サブスクライバにリホームを設定すると、電話とデバイスグループを時間の経過とともに正常に戻すことができます。そうでない場合は、電話機を再配布してコールセンターへの影響を最小限に抑えるために、メンテナンス期間中に手動による介入を要求できます。このリホームプロセス中、CTI Manager は、サブスクライバ B から元のサブスクライバ A に切り替える登録のエージェント PG を通知します。
9. コール処理は、電話機とデバイスが元のサブスクライバに戻った後も通常通り継続されます。

何度か失敗したシナリオ

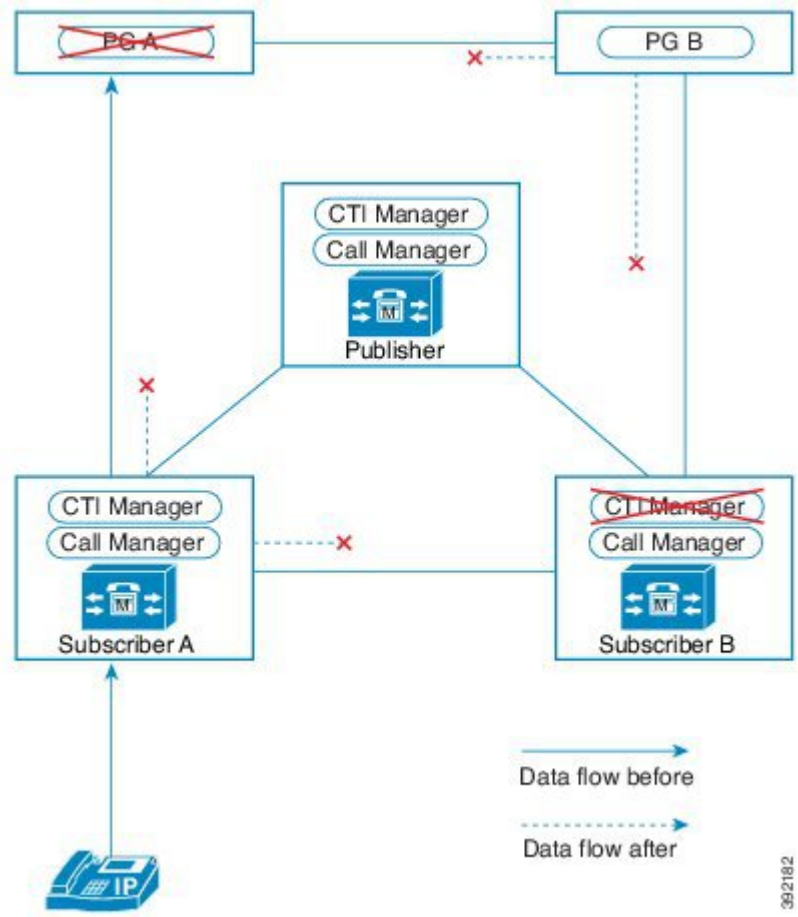
複数のコンポーネントに障害が発生した場合、Unified CCE は、単一コンポーネントの障害時ほどシームレスに失敗しません。次の項では、Unified CCE がマルチコンポーネント障害に対してどのように応答するのかについて説明します。

CTI Manager とエージェント *PG* の障害

CTI Manager は、ローカルサブスクライバと 1 つのエージェント PG にのみ接続します。クラスタ内の他の CTI Manager と直接通信することはできません。CTI Manager は、他のコンポーネントのデータによって同期されます。

各サイドのエージェント PG ともう一方の側の CTI Manager が両方に障害が発生した場合、Unified CCE はクラスタと通信できません。このシナリオでは、システムがこのクラスタ上のエージェントに接続できなくなります。エージェント PG またはバックアップ CTI Manager がオンラインに戻るまで、クラスタは切断された状態のままです。

Figure 11: エージェント *PG* がバックアップの *CTI Manager* に接続できない



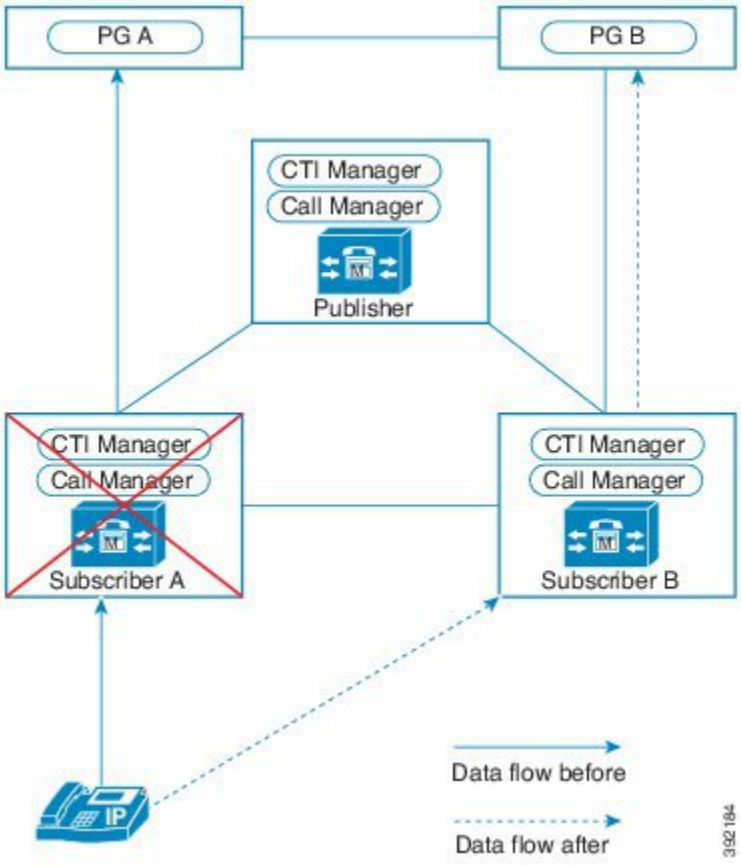
Unified CM サブスクライバと *CTI Manager*の両方の障害

シナリオは、Unified CM サブスクライバ A サーバの完全な障害からのリカバリを示しています。

以下の条件がシナリオに適用されます。

- サブスクライバ A にはプライマリ CTI Manager があります。
- 冗長性のために、サブスクライバ A に登録されているすべての電話とゲートウェイは、サブスクライバ B をバックアップ サーバとして使用します。

Figure 12: Unified Communications Manager と CTI Manager の障害



障害復旧は次のように発生します。

1. サブスクライバ A に障害が発生すると、すべての非アクティブな登録済み電話機およびゲートウェイがサブスクライバ B に再登録されます。
2. 進行中のコールはアクティブなままですが、エージェントは転送などの電話サービスを使用できません。
3. エージェント PG サイド A が障害を検出し、エージェント PG サイド B へのフェールオーバーを引き起こします。
4. エージェント PG サイド B がアクティブになり、すべてのダイヤル番号と電話機を登録します。コール処理が続行されます。
5. 進行中のコールが終了すると、そのエージェントの電話機とデスクトップがバックアップサブスクライバに再登録されます。エージェントデスクトップの正確な状態は、構成とデスクトップによって異なります。
6. サブスクライバ A が復元すると、すべてのアイドル状態の電話機とゲートウェイが再登録されます。アクティブデバイスは、プライマリサブスクライバに再登録する前にアイドルになるまで待機します。

7. エージェント PG サイド B は、サブスクライバ B の CTI Manager を使用してアクティブな状態のままです。
8. 障害からの復旧語、エージェント PG は、冗長ペアのサイド A にフェールバックしません。すべての CTI メッセージングは、サブスクライバ A と通信するサブスクライバ B の CTI Manager を使用して電話機の状態とコール情報を取得するために処理されます。

Logger の高可用性に関する考慮事項

Logger の障害

Unified CCE Logger および Database サーバは、構成（エージェント ID、スキルグループ、通話の種類）およびスクリプト（コールフロースクリプト）のためにシステムデータベースを維持します。サーバは、通話処理から最近の履歴データも保持します。Logger はローカルルータからデータを受信します。ルータは同期されているので、Logger データも同期されています。

Logger の障害により、コール処理にすぐ影響を与えることはありません。冗長 Logger は、ローカルのルータからの一連の通話データを受信します。システムが Logger の障害を復元した場合は、Logger は自動で、バックアップ Logger からいつオフラインになったのかのすべてのトランザクションを要求します。Logger は、データベースで記録されたエントリの順番をトラックするリカバリキーを維持します。冗長 Logger は、これらキーを使用して欠落しているデータを特定します。

Logger が、Config_Message_Log テーブルの 14 日の保持期間を超えてオフラインになったままの場合、システムは、自動で Logger 構成データベースを再同期しません。システム管理者は、https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-maintenance-guides-list.html の『アドミニストレーション ガイド』に説明されている Unified ICMDBA アプリケーションを使用して Logger を手動で再同期できます。手動のプロセスにより、構成データをプライベートネットワーク全体に転送する便利な時間を選択できます。

Logger の複製プロセスは、そのデータを Logger データベースからから Administration および Data サーバ の HDS データベースに送信します。また、複製プロセスでは、Logger が同期された後、Logger データベースが記録する新しい行が自動的に複製されます。

単一のキャンペーンマネージャを使用した Cisco アウトバウンドオプションを使用する展開では、キャンペーンマネージャは、プライマリ Logger だけにロードされます。そのプラットフォームが停止され、Logger がダウンしている場合、任意の発信通話が停止します。

レポーティングの考慮事項

Unified CCE レポート機能は、リアルタイム、5 分間、およびレポート間隔（15 分または 30 分間）のデータを使用して、レポートデータベースを構築します。各 5 分間のレポート間隔の最後に、各 PG はローカルデータを収集し、ルータに送信します。ルータはデータを処理し、データを履歴データストレージ用のローカル Logger に送信します。この Logger は、履歴データを HDS/DDS データベースに複製します。

PG は、5 分間のデータおよびレポート間隔データのバッファリング（メモリおよびディスク上）を提供します。PG は、このバッファされたデータを使用して、ネットワーク応答の低下と、ネッ

トワークサービス復元後のデータの自動再送信を処理します。冗長ペアの両方の PG に障害が発生した場合は、セントラルコントローラに送信されない 5 分間のデータとレポート間隔のデータを失う可能性があります。

エージェントがサインアウトすると、すべてのレポート統計が停止します。エージェントが次にサインインすると、エージェントのリアルタイム統計は 0 から開始します。エージェントデスクトップと、障害が発生した時にエージェントが行っている処理に応じて、一部のフェールオーバーは、エージェントがコンタクトセンターからサインアウトされる原因となります。詳細については、http://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-user-guide-list.html の「*Cisco Unified ICM/Contact Center Enterprise* レポートの概念」を参照してください。

周辺機器ゲートウェイ高可用性に関する検討事項

PG ウェイト

プライベートリンクに障害が発生した場合のフェールオーバー中に、重み付け値によって、有効な PG になる PG が決定します。各側のアクティブコンポーネントの数とタイプによって、PG の加重値が決定されます。各コンポーネントに割り当てられた重み付けは、そのコンポーネントの復元時間と、コンポーネントがダウンした場合のコンタクトセンターの中断を反映します。エージェント PIM は、VRU PIM および CTI サーバよりも重みがあります。コンポーネントの重み付けは構成できません。

フェールオーバー中の記録管理

フェールオーバー中に記録されるコールデータは、どのコンポーネントに障害が発生するかによって異なります。障害の状況に応じて、同じコールデータが失われます。ルータは、障害が原因で、アクティブコールへのアクセスを失う場合があります。アクティブコールは依然としてアクティブ状態ですが、ルータは、コールがドロップしたかのように応答します。通常、エージェント PG は、終話コール詳細（TCD）レコードを Unified CCE データベースに作成します。

エージェントにすでに接続されているコールは、フェールオーバー中に続行できます。エージェント PG は、これらのコールが終了すると、そのコールに対して別の TCD レコードを作成します。

エージェント PG 障害

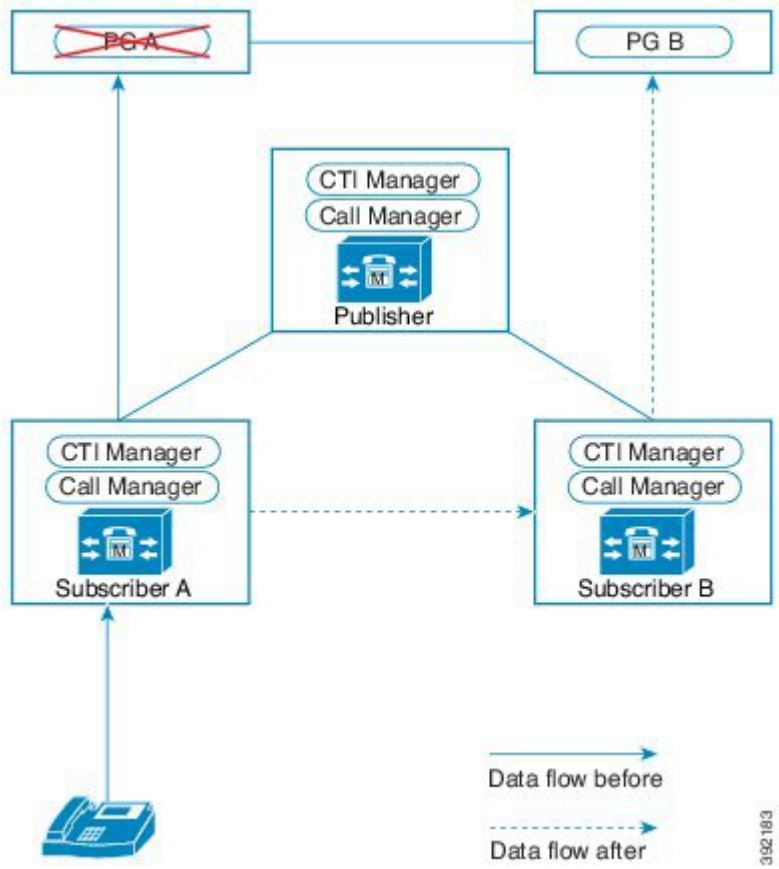
このシナリオは、PG サイド A の障害の復元を示しています。

以下の条件がシナリオに適用されます。

- Unified CM サブスクライバ A にはプライマリ CTI Manager があります。
- 冗長性のために、サブスクライバ A に登録されているすべての電話とゲートウェイは、サブスクライバ B をバックアップ サーバとして使用します。

次の図は、PG サイド A での障害と PG サイド B へのフェールオーバーを示しています。すべての CTI Manager サービスと Unified Communications Manager サービスは、引き続き通常通り実行されます。

Figure 13: エージェント *PG* のサイド *A* の障害



障害復旧は次のように発生します。

1. PG サイド B が PG サイド A の障害を検出します。
2. PG サイド B は、すべてのダイヤル番号と電話機を登録します。コール処理は PG サイド B を通じて続行されます。
3. 電話機とゲートウェイは登録され、サブスクライバ A で運用可能な状態が続き、フェールオーバーしません。
4. 進行中のコールはエージェントの電話機でアクティブな状態のままですが、エージェントがサインインし直すまで、エージェントは転送のような電話サービスを使用できません。
5. PG サイド B へのフェールオーバー中は、構成に応じて占有されていないエージェントの状態とデスクトップが変化する場合があります。3 者通話のオプションが影響を受ける可能性があります。場合によっては、エージェントはフェールオーバーの完了後にサインインまたは手動で状態を変更する必要があります。

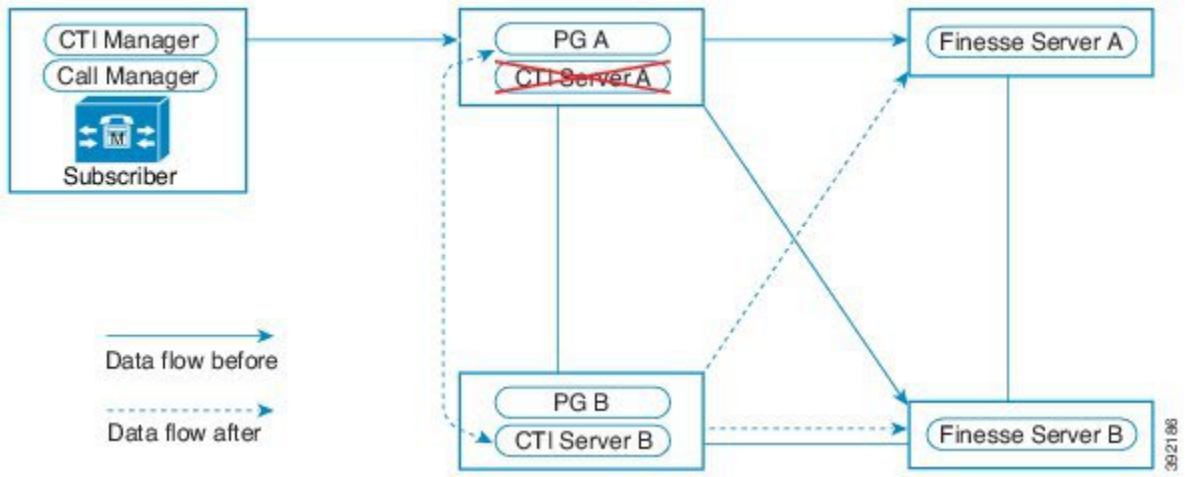
6. 障害からの復旧後、PG サイド B は、アクティブ状態のまま、サブスクライバ B の CTI Manager を使用します。PG がサイド A にフェイルバックしない場合、コールは、PG サイド B で引き続き処理されます。

CTI サーバ障害

CTI サーバは、特定の CTI メッセージ（通話の呼び出し中やオフフックイベントなど）について、エージェント PG トラフィックをモニタします。CTI サーバは、これらのメッセージを Cisco Finesse サーバなどの CTI クライアントで利用できるようにします。CTI サーバは、CTI クライアントからのサードパーティ呼制御メッセージ（コールの送信や応答コールなど）も処理します。CTI サーバは、処理のためにエージェント PG を介して Unified CM にこれらのメッセージを送信します。

冗長ペアで CTI OS サーバを展開します。冗長ペアの各半分は、冗長エージェント PG ペアの半分を持つ VM の同身です。アクティブな CTI サーバの障害発生時には、冗長 CTI サーバがアクティブになり、コールイベントの処理を開始します。

***Figure 14: CTI* サーバ障害**



Finesse サーバは、CTI サーバのクライアントです。Desktop サーバは、CTI サーバではなく、フェールオーバー中にエージェントの状態を維持します。CTI サーバに障害が発生すると、Finesse はエージェントデスクトップを一部無効にします。場合によっては、フェールオーバーが完了した後にエージェントは再サインインする必要があります。

Note アクティブな CTI サーバにクライアントが接続されていない場合、事前設定された期間後、メカニズムが強制的にフェールオーバーを実行します。このフェールオーバーは、CTI クライアントがアクティブな CTI サーバに接続するのを妨げる偽の誤った理由を分離します。

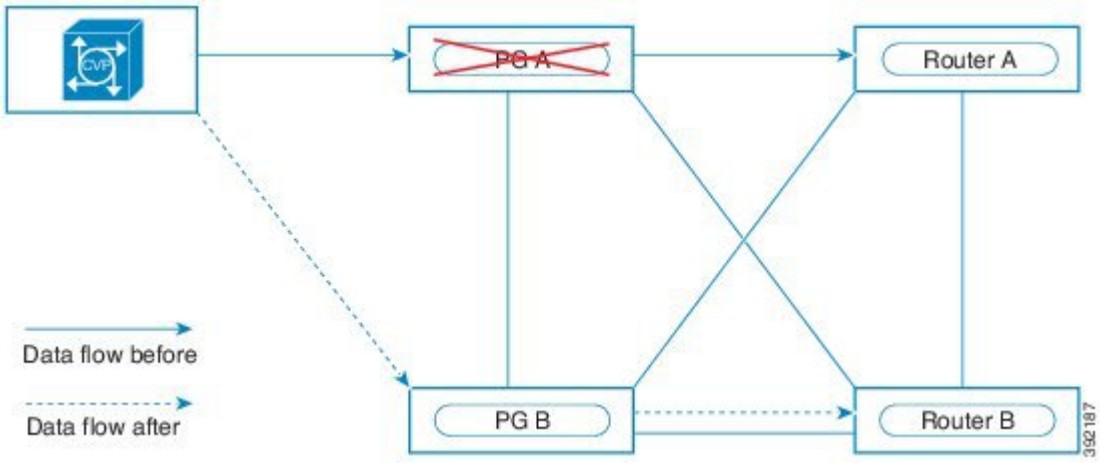
VRU PG 障害

音声応答装置（VRU）PG に障害が発生した場合、進行中のコールや Unified CVP にキューに入ったコールはドロップされません。音声ゲートウェイの存続可能性 TCL スクリプトは、使用可能な

場合、コールをセカンダリ Unified CVP または SIP ダイヤルプラン内の番号にリダイレクトします。

フェールオーバー後、冗長 VRU PG は、Unified CVP に接続され、新しい通話の処理を開始します。障害が発生した VRU PG サイドが復旧すると、現在実行中の VRU PG がアクティブ VRU PG として稼働し続けます。冗長 VRU PG を使用すると、Unified CVP がアクティブキューポイントとして機能したり、コール処理を提供したりできます。

***Figure 15: VRU PG* 障害**



Administration & Data サーバの高可用性に関する検討事項

Administration and Data サーバ障害

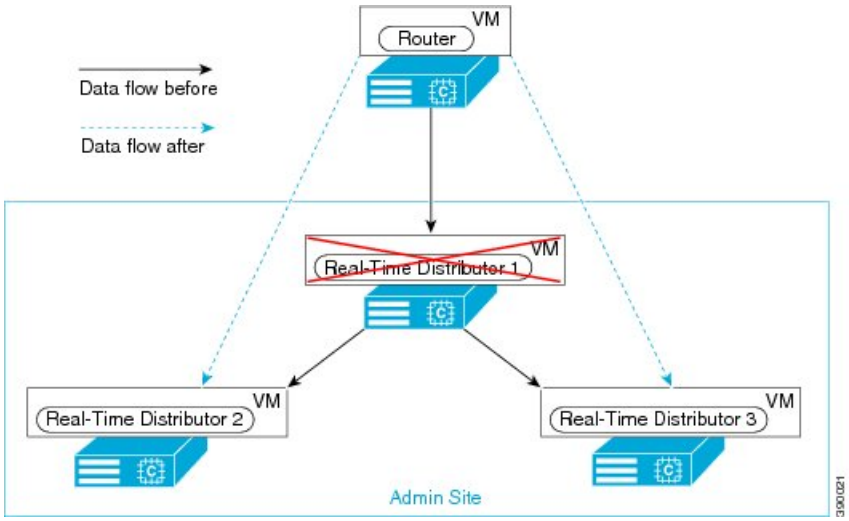
Administration および Data サーバは、構成およびスクリプト変更を行うシステムにユーザインターフェイスを提供します。サーバは、Web ベースのレポートツールとインターネット スクリプトエディタをホストすることもできます。他の Unified CCE コンポーネントとは異なり、Administration および Data サーバは冗長ペアで動作しません。このサーバの機能に冗長性を提供する場合は、設計にさらに Administration および Data サーバを含めます。ただし、自動フェールオーバーの動作はありません。

Administration および Data サーバは、リアルタイム ディストリビュータを介したルータからの Unified CCE 全体からリアルタイムでデータのフィードを受けます。同じサイトに Administration および Data サーバがいくつかある場合、1 つの管理者サイトにリアルタイム ディストリビュータを構成できます。管理者サイトには、プライマリ ディストリビュータと 1 つ以上のセカンダリ ディストリビュータがあります。プライマリ ディストリビュータはルータに登録し、ルータからのネットワーク全体でリアルタイムにフィードを受信します。セカンダリ ディストリビュータは、リアルタイムフィードのソースとしてプライマリディストリビュータを使用します。この調整により、ルータがサポートするリアルタムフィードの数を軽減し、帯域幅をご存します。

プライマリ リアルタイムデスクトップに障害が発生した場合、次の図で示すとおり、セカンダリ リアルタイム ディストリビュータは、リアルタイムフィードのルータに登録します。プライマリ

またはセカンダリ Administration および Data サーバに登録できない管理クライアントは、ディストリビュータがリストアされるまで、タスクを実行できません。

Figure 16: プライマリ リアルタイム ディストリビュータの障害



電解によっては、Administration および Data サーバは、 Unified CCMP のインターフェイスもホストします。このような展開では、Administration および Data サーバがダウンした場合、どちらのツールを使用して行われた構成編網もインターフェイスに渡されません。

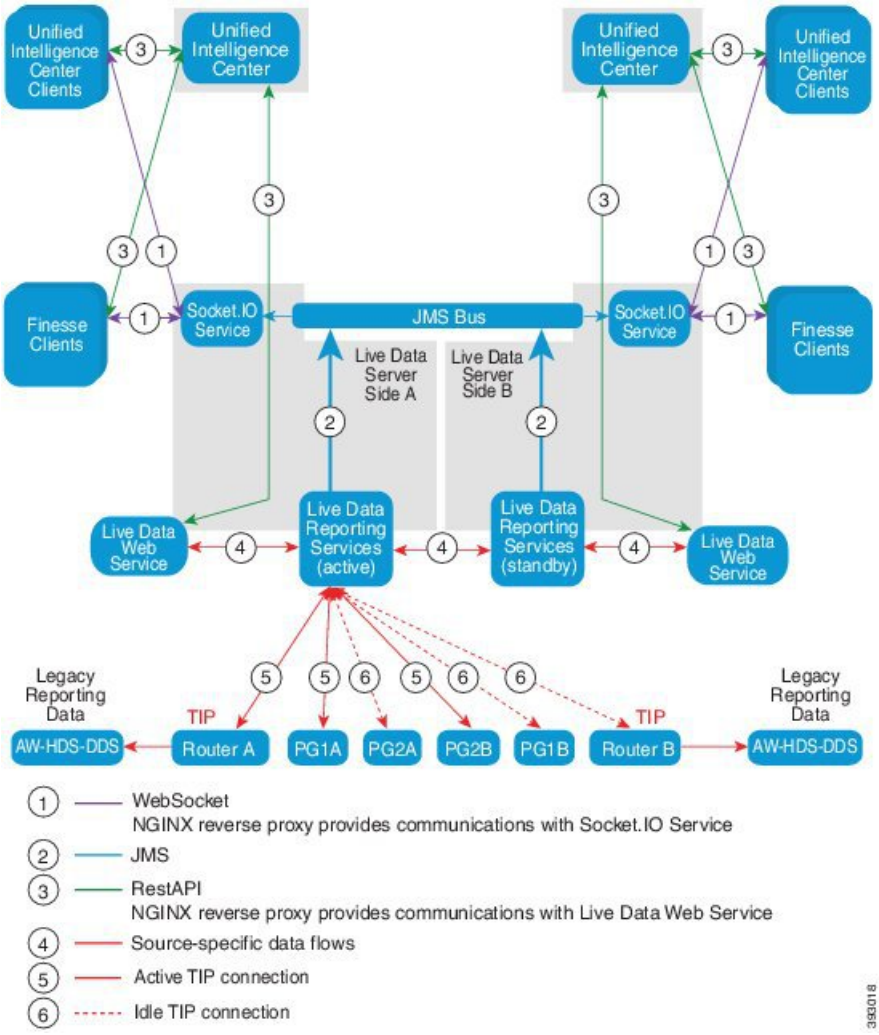
ライブデータの高可用性に関する検討事項

ライブデータは、1 つが サイド Aに、もう 1 つがサイド B に導入された 2 つのライブデータシステムとして導入された高可用性システムです。設計上、ライブデータの導入は、シングルポイント障害に耐えることができます。フェールオーバーには次の 3 つの層があります。

- サーバ
- ヒント
- Socket.IO ストリーム

Note Live Data サーバのフェールオーバーは、Live Data クラスタフェールオーバーとも呼ばれます。このドキュメントでは、Live Data サーバ フェールオーバーという用語を使用します。

Figure 17: ライブデータレポートトポロジ



Live Data サーバのフェールオーバー

Live Data サーバは、コールドアクティブまたはスタンバイ モードで動作します。いつでもアクティブにできるのは、1 つの Live Data サーバのみです。もう 1 つの Live Data サーバはスタンバイ状態です。スタンバイの Live Data サーバは、アクティブなサーバのステータスを絶えずモニタしています。アクティブなサーバに障害が発生すると、スタンバイのサーバが引き継ぎ、アクティブになります。障害のあるサーバは、サービスを提供する準備ができたらスタンバイサーバになります。

重み付けアルゴリズムにより、次の 2 つのシナリオでアクティブな Live Data サーバを決定します。

シナリオ 1：両方の Live Data サーバが同時に起動すると、サーバは、ルータと同じデバイスの過半数の計算を使用します。

シナリオ 2：アクティブな Live Data サーバは、一部の PG に対する接続を失う場合があります。スタンバイサーバはその切断を検出します。2 分間アクティブサーバよりも 130% PG多い場合、アクティブステータスを想定するように要求します。スタンバイサーバがアクティブサーバになり、以前アクティブだったサーバがスタンバイサーバになります。

TIP フェールオーバー

Live Data は、TIP トランスポートプロトコルを使用してルータおよび PG サーバと通信します。アクティブな Live Data サーバは、ルータと PG の両サイドに TIP 接続を確立します。スタンバイの Live Data サーバは、TIP 接続を確立しません。サイド A かサイド B のどちらか一方でのみ TIP 接続がアクティブになります。アクティブな TIP 接続に障害が発生した場合、アクティブな Live Data サーバがアイドル状態の TIP 接続を復元します。

Socket.IO フェールオーバー

Socket.IO クライアントは、Live Data サーバのどちらかのサイドに接続して、ライブデータレポートイベントストリーム（Socket.IO ストリーム）を受信します。Unified Intelligence Center クライアントは、Socket.IO クライアントの例です。スタンバイ中の Live Data サーバも、アクティブサーバのプロキシごとの Socket.IO ストリームを生成します。Socket.IO クライアントハートビートの損失は、Socket.IO の切断の原因となります。その後、Socket.IO クライアントは、別の Live Data サーバにフェールオーバーします。

仮想化音声ブラウザの高可用性に関する検討事項

シスコ仮想化音声ブラウザ（VVB）は、アクティブの冗長性に対する組み込み式高可用性のない単一ノードです。可用性のレベルを向上し、シングルポイント障害を排除するために、追加の VVB を導入します。CVP SIP サーバグループに追加の VV を含めると、パッシブ冗長性を構築できます。さらに VVB を展開することで、1 つの VVB のスケジュールされていないダウンタイムとスケジュールいるダウンタイムを管理できます。

VVB に障害が発生した場合、障害が発生した VVB 切断時のすべてのアクティブコールとすべてのコールデータが失われます。CVP が SIP サーバグループ内の VVB の障害を検出すると、CVP は残りのアクティブ VVB に着信コールをルートします。CVP ハートビートメカニズムによって、障害が発生した VVB のリカバリをが検出されると、CVP はリカバリ済みの VVB にコールバックをルートします。

Unified CM の高可用性に関する検討事項

データネットワークを設計した後、Cisco Unified Communications インフラストラクチャを設計します。ダイヤルしたり、通話を受信するためには、任意のテレフォニー アプリケーションを展開する前に Unified CM クラスタおよび CTI Manager を設置する必要があります。

各 Unified CM サーバ上でソリューションを実行するためのいくつかの重要なサービス

- Unified CM
- CTI Manager

- CallManager サービス
- TFTP

これらすべてのサービスのアーキテクチャの詳細については、http://www.cisco.com/en/US/docs/voice_ip_comm/uc_system/design/guides/UCgoList.html の 『*Cisco Collaboration System Solution Reference Network Designs*』 を参照してください。

クラスタの高可用性の設計では、Unified CM、CTI Manager、CallManager サービスがどのように相互対話をするか理解する必要があります。Unified CM は、CTI Manager サービスを使用して CTI リソースを処理します。CTI Manager は、特定の Unified CM サーバへのアプリケーションの物理的なバインドを制限するアプリケーションブローカーとして機能します。CallManager サービスは、すべての Cisco Unified Communications デバイスを登録および監視します。

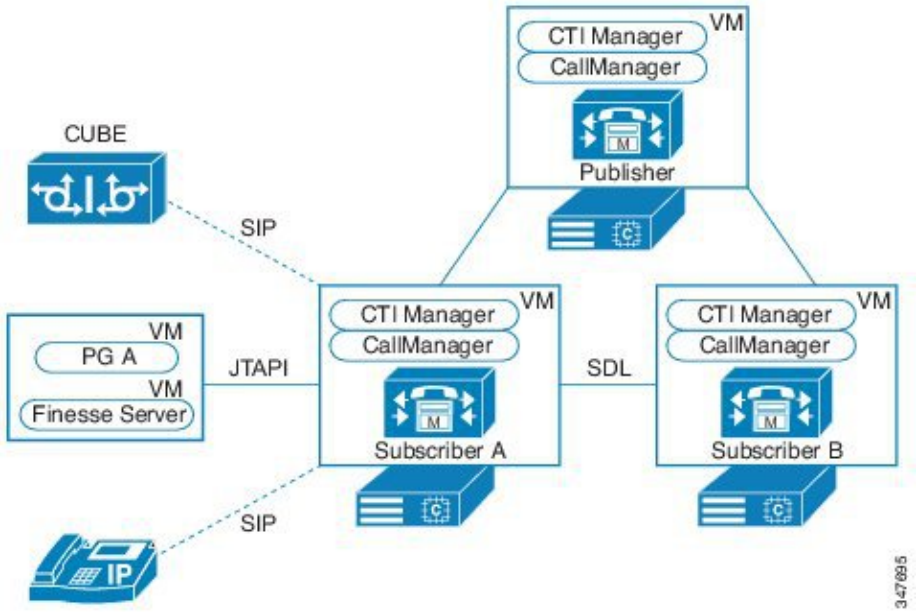
CTI Manager は、CTI アプリケーションであるエージェント PG からメッセージを受け入れ、クラスタ内の適切なリソースに送信します。CTI Manager は、Cisco JTAPI を使用する JTAPI メッセージルータのように動作し、エージェント PG に通信します。Unified CM の JTAPI クライアントライブラリは、CallManager サービスに直接接続する代わりに CTI Manager に接続します。

CallManager サービスは、システム内のすべての Cisco Unified Communications リソースとデバイスのスイッチとして機能します。各 Unified CM サーバ上の CallManager は、パブリックネットワークを介して単一ディストリビューションレイヤ（SDL）とリンクしています。このリンクにより、クラスタの同期が維持されます。各 CTI Manager は、サーバ上の Unified CM および CallManager サービスに接続します。CTI Manager は、クラスタ内の他の CTI Manager に直接接続できません。

エージェント PG は、通常、「JTAPI ユーザ」または「PG ユーザ」と呼ばれる、Unified CM で CTI 対応のユーザアカウントを使用します。エージェント PG は CTI Manager にサインインして、そのユーザのデバイスに接続します。適切なデバイスがローカルの CallManager にある場合、CTI Manager は、そのデバイスの要求を処理します。デバイスがローカルのサブスクライバにない場合、CallManager サービスは、他の CallManager サービスへのプライベートリンクを通じて、リクエストを適切なサブスクライバに転送します。

次の図は、クラスタ内の接続を示します。

Figure 18: Unified Communications Manager クラスタ内の接続



高可用性の場合は、クラスタ内のすべてのサブスクライバにデバイス登録を分散します。登録を単一のサブスクライバに集中させると、トラフィックは、そのサブスクライバに大きな負荷を与えます。エージェント PG が登録済みデバイスの監視に使用するメモリオブジェクトは、サブスクライバのデバイスの重み付けにも追加されます。

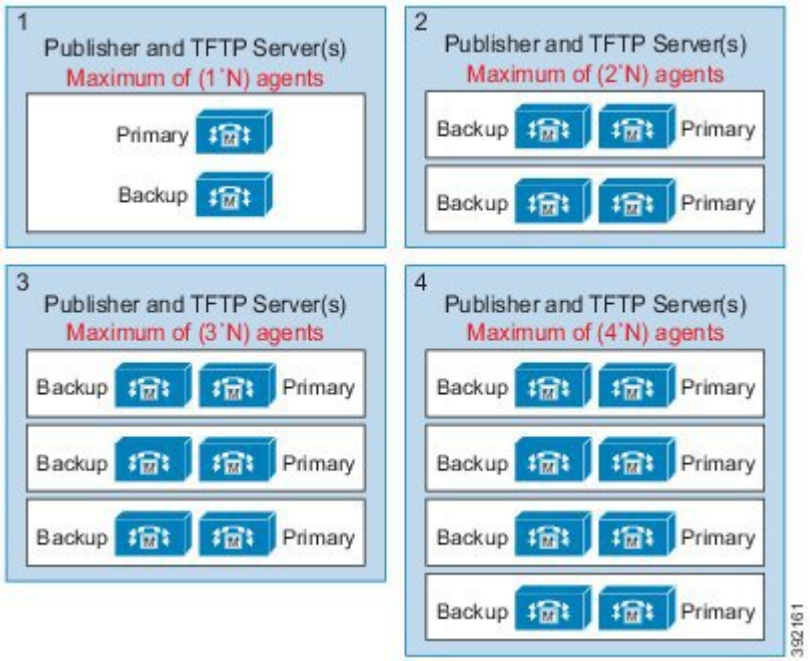
サブスクライバに接続されている PG に障害が発生した場合、冗長 PG は、すべての要求を引き継いで、別のサブスクライバに送信します。次に、ローカルの CallManager サービスは、クラスタ全体でこれらのリクエストに対する CTI Manager メッセージングを元のサブスクライバにルートする必要があります。このフェールオーバー条件化でメッセージを追加すると、クラスタに大きな負荷がかかります。

Unified CM の冗長性

Unified CM の展開環境の中には、2:1 の冗長性スキームを使用する場合があります。プライマリサブスクライバの各ペアは、1 つのバックアップサブスクライバを共有します。しかし、コンタクトセンターでのより高い電話機の使用率、そしてアップグレード処理の簡易化により、Contact Center Enterprise ソリューションは、サブスクライバに対して 1:1 冗長性スキームを使用します。各プライマリサブスクライバには、それぞれ独自のバックアップサブスクライバが必要です。

次の図は、異なるサイズのクラスタを示しています。Unified CVP を使用する Contact Center Enterprise ソリューションの場合、*N* は、この図の 2000/ペアのサブスクライバと同じになります。

Figure 19: 冗長構成のオプション



Unified CM 負荷分散

Unified CM サブスクライバ用の 1:1 冗長性スキームでは、プライマリサブスクライバとバックアップサブスクライバのペアでデバイスのバランスを調整できます。通常、プライマリサブスクライバが利用できない限り、バックアップサブスクライバにはデバイスが登録されません。

Unified CM の冗長性グループとデバイスプールの設定により、負荷分散を有効にできます。プライマリサブスクライバからセカンダリサブスクライバにデバイスの負荷の半分まで移動できます。この方法により、サーバが使用できなくなることによる影響を半分に減らすことができます。停止の影響を最小限に抑えるために、すべてのデバイスと通話ボリュームをアクティブなサブスクライバ全体に均等に分散します。

Cisco Finesse 高可用性の考慮事項

Cisco Finesse サーバは、Contact Center Enterprise ソリューションの冗長ペアで展開します。両方の Cisco Finesse サーバが常にアクティブになります。Cisco Finesse サーバが動作しない場合、そのサーバ上のエージェントは [準備中（NOT READY）] または [準備の保留（pending NOT READY）] のステータスになります。別のサーバのサインインページにリダイレクトされます。このような状況は、次の状況が発生した場合に発生します。

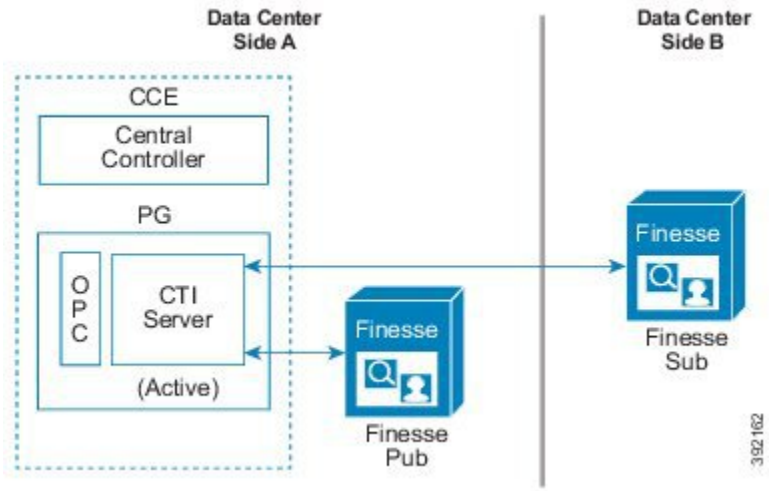
- Cisco Finesse Tomcat サービスの停止。
- シスコ通知サービスの停止。

• Cisco Finesse から両方の CTI サーバへの接続が切断された。

クライアントが切断されると、2 つの内の利用可能な Cisco Finesse サーバの 1 つに再接続を試行します。再接続に 2 分以上かかる場合、Cisco Finesse はエージェントをサインアウトします。クライアントが再接続されると、エージェントはサインインする必要があります。

1 つのエージェント PG は、2 台のサーバ、発行元、サブスクライバで構成される Cisco Finesse クラスタの 1 つのインスタンスをサポートします。複数の Finesse クラスタは、同じエージェント PG/CTI サーバには通信できません。各 Cisco Finesse サーバは、CTI サーバがサポートする最大 2,000 ユーザをサポートできます。このキャパシティにより、他のサーバに障害が発生した場合、一方の Cisco Finesse サーバが全負荷を処理できます。2 台の Cisco Finesse サーバ間のユーザの総数は 2,000 名を超えることはできません。次の図に示すように、各 Cisco Finesse サーバには 1 つの CTI 接続が必要です。

Figure 20: 複数の ***Cisco Finesse*** サーバ



Cisco Finesse を展開する場合は、http://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/uc_system/virtualization/cisco-collaboration-virtualization.html の「シスコ コラボレーション仮想化」で説明されている併置ポリシーに従います。

Cisco Finesse IP Phone エージェントの障害時動作

デスクトップとは異なり、Cisco Finesse IP Phone Agent（Cisco Finesse IPPA）は、代替の Cisco Finesse サーバに自動的にフェールオーバーしません。適切なフェールオーバー動作が発生する場合は、Unified CM で最低 2 つの Cisco Finesse IP Phone サービスを構成します。各サービスは、異なる Cisco Finesse サーバを使用する必要があります。

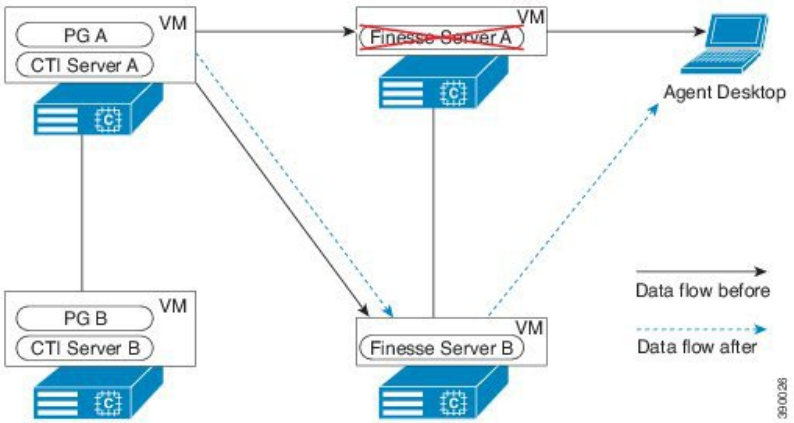
Cisco Finesse サーバに障害が発生すると、Cisco Finesse IPPA は 5 秒ごとに再接続を試行します。3 回試行が失敗すると、Cisco Finesse IPPA はエージェントに対してサーバが使用できない旨のメッセージを表示します。サービス停止までの合計時間は約 15 秒です。

障害のシナリオでは、エージェントはサインアウトしてから、代替の Cisco Finesse サーバにサインインする必要があります。すると、エージェントは通常動作を再開できます。

Cisco Finesse サーバ障害

専用の仮想マシンでは、Cisco Finesse サーバを冗長ペアで展開します。Cisco Finesse サーバはどちらも、アクティブモードで実行されます。

***Figure 21: Cisco Finesse* サーバ障害**



Cisco Finesse サーバに障害が発生すると、次のように障害回復が発生します。

1. サーバにサインインしているエージェントデスクトップは、切断を検出し、冗長サーバにフェールオーバーします。
2. エージェントは、フェールオーバー後、新しいサーバに自動的にログインします。

Note Cisco Finesse サーバに障害が発生した場合、デスクトップ チャット ステータスは、保持され、すべてのアクティブセッションが失われます。

3. Cisco Finesse REST API を使用するサードパーティ製アプリケーションは、アプリケーションロジック内でフェールオーバーを実行して、冗長サーバに移動する必要があります。
4. Cisco Finesse サーバは自動的に再起動しません。障害が発生したサーバを再起動すると、新しいエージェント デスクトップ セッションがそのサーバにサインインできます。冗長サーバにサインインしているエージェントデスクトップは、そのサーバに残ります。

Note 別のサイドの Cisco Finesse Tomcat に障害が発生した場合は、Cisco Finesse サーバがフェールオーバーします。

他のコンポーネントに障害が発生した場合の Cisco Finesse の動作

次の項では、他の Unified CCE コンポーネントに障害が発生した場合の Cisco Finesse の動作について説明します。

エージェント PG または CTI サーバの障害

Cisco Finesse サーバは、CTI サーバが併置され、接続されているアクティブエージェント PG に接続します。アクティブなエージェント PG または、CTI サーバに障害が発生した場合、Cisco Finesse は冗長の CTI サーバへの接続を試行します。冗長サーバが利用できない場合、Finesseは、接続するまでどちらかのサーバへの接続を試行します。その後、Finesse は、すべてのエージェント、スキルグループ、およびコールデータをクリアします。Cisco Finesse は、エージェントとコールの状態を含む冗長 CTI サーバから現在のすべての構成を受信するまでは使用できません。切断された場合、エージェントはデスクトップに赤いバナーを表示し、再接続されたら緑のバナーを表示します。

ベンチマークパラメータ

Cisco Finesse、Release 12.5 (1) CTI フェールオーバーとデスクトップ フェールオーバーのパフォーマンスを最適化します。

- CTI フェールオーバー — エージェント PG 12.5(1) を展開する際の CTI サーバまたはエージェント PG フェールオーバーの最長時間は、35 秒から 75 秒です。
- デスクトップ フェールオーバー — エージェント PG 12.5(1) を展開する際におけるデフォルト デスクトップ レイアウトのデスクトップ フェールオーバーの最長時間は、50 秒から 110 秒です。

フェールオーバーの時間は、WAN 帯域幅、サインインしているユーザの数、遅延、CPU の数および Finesse デスクトップに設定されているガジェットの数によって異なります。

最適なフェールオーバー パフォーマンスを確保するための展開方法とガイドラインの詳細については、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「デスクトップ フェールオーバー最適化のガイドライン」および「フェールオーバー計画」の項を参照してください。

カスタムガジェットによるフェールオーバー パフォーマンスの改善方法の詳細については、https://developer.cisco.com/docs/finesse/#!rest-api-dev-guide にある『Cisco Finesse Web サービスデベロッパーガイド』の「ガジェット開発のベストプラクティス」の項を参照してください。

帯域幅の計測の詳細については、https://www.cisco.com/c/en/us/support/customer-collaboration/finesse/products-technical-reference-list.html にある『Unified Contact Center Enterprise Finesse 帯域幅計算ツール』を参照してください。

Administration & Data サーバの障害

Cisco Finesse は、Administration & Data サーバを使用してエージェントを認証します。Cisco Finesse 管理者は、Cisco Finesse 管理ユーザインターフェイスで、Administration & Data サーバの設定（また必要に応じて、Administration & Data サーバのバックアップ）を構成します。プライマリ Administration & Data サーバの障害とバックアップの Administration & Data サーバが設定されていない場合、Cisco Finesse エージェントはデスクトップにサインインできません。フェールオーバーが発生するとログインしているエージェントは、デスクトップ上で操作を実行できなくなります。

バックアップの Administration & Data サーバが構成された場合、Cisco Finesse は、バックアップサーバへの接続を試行します。Cisco Finesse をバックアップの Administration & Data サーバに接続後、エージェントはサインインでき、デスクトップで操作を実行できます。

Cisco IM&P サーバの障害

Cisco Finesse は、デスクトップチャット機能用のインスタントメッセージングおよびプレゼンス（IM&P）サーバを使用します。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。

フェールオーバーは、デスクトップチャットをサポートしており、IM&P ノード障害は、構成されたユーザとしてノードペアピアへ自動的に接続します。

Note Cisco Finesse サーバに障害が発生した場合、デスクトップ チャット ステータスは、保持され、すべてのアクティブセッションが失われます。

Unified Intelligence Center の高可用性に関する検討事項

Cisco Unified Intelligence Center は、高可用性のために、発行元と最大 7 のサブスクライバを含むクラスタモデルを使用します。構成がクラスタ内で複製されます。プロセスは自動で、失敗したノードをバイパスしてアクティブノード間で広がります。

Unified CM ベースのサイレントモニタリングの高可用性に関する検討事項

既存のコールでは、高可用性はありません。着信コールの場合、コール処理とサイレントモニタリングがバックアップの Unified CM サブスクライバに移動します。

Customer Collaboration Platform ハイアベイラビリティの考慮事項

Cisco Customer Collaboration Platform は、高可用性をサポートしていません。冗長の Customer Collaboration Platform サーバを展開しないでください。 Customer Collaboration Platform は Contact Center Enterprise ソリューションの別のコンポーネントと直接統合はしません。

Customer Collaboration Platform は、小規模または大規模な単一サーバ、オールインワン展開を使用します。負荷分散、分割サイトの展開は使用できません。

Unified SIP プロキシの高可用性に関する検討事項

RecordRoute が無効な場合、Unified SIP Proxy は、アクティブコールのフェールオーバーを処理できます。フェールオーバー中のアクティブコールでは、バックアップ SIP Proxy サーバが新しいトランザクションを処理します。

ビジネス チャットおよびEメールハイ アベイラビリティの考慮事項

ビジネス チャットおよびE メール（ECE）は高可用性を提供します。同じ場所に配置されたECE導入および1500エージェントクラスタは、次の技術を使用して地理的冗長性をサポートします。

- ロードバランサを使用すると、複数の Web サーバに着信要件を分散できます。サーバがダウンした場合、ロードバランサは、障害を検出し、別のアプリケーションサーバにリクエストをリダイレクトします。この機能は、最大 5 台の Web サーバで、各 Web サーバ上で 300 人のエージェントをサポートします。最大キャパシティには冗長性は提供されません。
- ネットワーク ラウンド トリップ時間内に、ECE のすべてのサブコンポーネントを保持します。詳細については、https://www.cisco.com/c/en/us/support/customer-collaboration/cisco-enterprise-chat-email/products-implementation-design-guides-list.html の「企業チャットおよび電子メール設計ガイド」を参照してください。
- Unified CCE コンポーネントに障害が発生した場合に ECE フェールオーバーをサポートするには、高可用性要件にしたばってエージェントと MR PG が実装されていることを確認します。この技法により、単一のサブコンポーネント障害が、すべてのセッションの処理をブロックしないようにします。
- Microsoft SQL サーバの可用性グループのクラスタリング構成を使用してデータベースをインストールします。詳細については、https://www.cisco.com/c/en/us/support/customer-collaboration/cisco-enterprise-chat-email/products-installation-guides-list.html の『企業チャットと電子メールインストレーションおよび構成ガイド』を参照してください。

ロードバランシングの考慮事項ビジネス チャットおよびE メール

ECE デプロイメントの Web サービスコンポーネントの負荷を分散すると、多くのエージェントにサービスを提供できます。ロードバランサの裏に Web（または Web およびアプリケーション）サーバを仮想 IP アドレスで設定できます。エージェントが、仮想 IP アドレスで ECE にアクセスする場合、ロードバランサは、アドレスの裏にあるサーバのいずれかにリクエストを送信します。その後、ロードバランサは、エージェントに応答を返します。このように、セキュリティの観点から、ロードバランサはリバースプロキシサーバとしても機能します。

ロードバランサは、Cookie ベースの永続性を持つスティッキセッションをサポートする必要があります。メンテナンスタスク後は、すべての Web サーバおよびアプリケーションサーバで負荷を

共有できることを確認します。すべてのサーバを使用せずにエージェントのアクセスを許可すると、スティッキ接続機能により、最初の Web サーバとアプリケーションサーバで過負荷が発生する可能性があります。

他のパラメータを使用すると、次の目的を満たす負荷分散アルゴリズムを定義できます。

- 均等な負荷分散
- プライマリ Web サーバとアプリケーションサーバの分離
- 低電力の Web サーバおよびアプリケーションサーバに送信するリクエスト数を減らします。

ロードバランサは、Web サーバとアプリケーションサーバの正常性をクラスタで監視します。障害発生時に、ロードバランサは、使用可能なサーバプールからそのサーバを削除します。

ECE 他のコンポーネントに障害が発生した場合の動作

一般に、他のソリューション コンポーネントに障害が発生した場合、アクティブセッションには影響しません。すべてのアクティブセッションが機能したままとなります。

この項では、別のソリューション コンポーネントに障害が起こった場合の、着信セッションに対する ECE 動作に関して説明します。

エージェント PG フェールオーバー

ECE サーバが接続されているエージェント PG がに障害が発生した場合、着信セッションへの影響は次のようになります。

- **Web コールバックセッション** — フェールオーバー期間中、カスタマーは、障害のある PG のエージェントに対して Web コールバックセッションをスケジュールすることはできません。他にエージェント PG が存在する場合、ECE は、それらの PG 上のエージェントに Web コールバックセッションを割り当てる必要があります。使用可能なエージェントが無い場合、Web コールバックセッションでリソースが利用可能になるまでキューに入れることができます。冗長 PG へのフェールオーバーが完了すると、すべての着信セッションが、その PG で利用可能なエージェントを使用できます。
- **遅延コールバックセッション** — コールバック処理が冗長 PG に切り替わります。指定された遅延が経過すると、コールバックが実行されます。
- **チャットセッション** — 冗長 PG へのフェールオーバーが完了すると、着信チャットセッションがエージェントに到達します。
- **電子メール** — 冗長 PG へのフェールオーバーが完了すると、受信電子メール処理が再開されます。

MR PG フェールオーバー

ECE サーバが接続されている MR PG がに障害が発生した場合、着信セッションへの影響は次のようになります。

- **キューに入っているセッション** — すでにキューに入っているセッションはキューに残ります。冗長 PG へのフェールオーバーが完了すると、ECE は、以前にキューに入ったセッションを PG に再発行します。
- **Web コールバックセッション** — 冗長 PG へのフェールオーバーが完了すると、新しいセッションがカスタマーとエージェント間で確立されます。
- **遅延コールバックセッション** — コールバック処理が冗長 PG に切り替わります。指定された遅延が経過すると、コールバックが実行されます。
- **チャットセッション** — 冗長 PG へのフェールオーバーが完了すると、着信チャットセッションがエージェントに到達します。
- **電子メール** — 冗長 PG へのフェールオーバーが完了すると、受信電子メール処理が再開されます。

CTI Manager のフェールオーバー

ECE サーバが接続されている CTI Manager に障害が発生した場合 、着信セッションへの影響は次のようになります。

- **Web コールバックセッション**— 新規セッションは置き換えることができず、カスタマーは、「システムは、エージェントをリクエストに割り当てることができません」というメッセージを受信します。
- **遅延コールバックセッション** — コールバック処理が冗長 CTI Manager に切り替わります。指定された遅延が経過すると、コールバックが実行されます。
- **チャットセッション** — 冗長 CTI Manager へのフェールオーバーが完了すると、着信チャットセッションがエージェントに到達します。
- **電子メール** — 冗長 CTI Manager へのフェールオーバーが完了すると、受信電子メール処理が再開されます。

ルータのフェールオーバー

アクティブなルータに障害が発生すると、冗長ルータがすべての着信セッションをシームレスに処理します。

ASR TTS 高可用性に関する考慮事項

Unified CCE ソリューションは、冗長 ASR/TTS サーバをサポートします。基本設定では、VXML ゲートウェイは最初に、すべての着信要求をプライマリ ASR/TTS サーバに渡します。プライマリサーバに到達できない場合、ゲートウェイはバックアップサーバに要求を渡します。バックアップサーバに到達した要求は、その要求機関までサーバにとどまります。

ロードバランサを追加して、着信要求を ASR/TTS サーバ全体に分散させることができます。

Cisco VVB は、冗長性に対してアクティブおよびバックアップの ASR/TTS サーバを使用しません。VVB には、ラウンドロビン方式でサーバのリストから選択するロードバランシング機能が組み込まれています。

選択した音声サーバが MRCP セッション設定要求を拒否した場合、VVB はもう一度、別のサーバで MRCP セッション設定を試みます。

アウトバウンドオプションの高可用性に関する検討事項

Cisco アウトバウンドオプションには、次のサブコンポーネントが含まれています。

サブコンポーネント	所在地	冗長性	説明
Campaign Manager	Logger A および B	冗長	コールに関連付けられているダイヤリングリストとルールを管理します。
アウトバウンド オプションのインポート	Logger A および B	冗長	キャンペーンレコードをインポートします。
アウトバウンド オプション データベース	Logger A および B	冗長	コール中のキャンペーンレコードを保留します。
SIP ダイヤラ	エージェント PG A または B MR PG A または B	冗長	キャンペーンに応じて、キャンペーン マネージャが割り当てるダイヤリングタスクを実行します。SIP ダイヤラは、割り当てられたエージェントに接続するコールを転送します。

Cisco アウトバウンドオプションの高可用性を向上させるには、冗長 CUSP ペアを使用して複数の音声ゲートウェイに接続します。冗長ゲートウェイは、ゲートウェイに障害が発生した場合に、ダイヤラが発信に利用できる十分なトランクを確保できるようにします。発信コールがプライマリアプリケーションの場合、これらのゲートウェイを発信コールにのみルーティングできます。

アウトバウンドオプションの高可用性は、Logger サイド A のアウトバウンドオプションと Logger サイド B のアウトバウンドオプション間の双方向複製をサポートします。双方向複製は、Logger 間のパブリックネットワークで実行されます。

ソリューションは、ウォームスタンバイモードで複数のダイヤラと、ダイヤラを制御するキャンペーン マネージャの冗長ペアをサポートします。SIP ダイヤラの冗長ペアは、PG フォールトトレランスモデルと同様のウォームスタンバイモードで動作します。

SIP ダイアラ 設計の留意事項

SIP ダイヤラはウォームスタンバイモードで実行されます。キャンペーン マネージャは、登録されている SIP ダイヤラプールから SIP ダイヤラ を準備完了ステータスで有効化します。アクティブ化されたSIPダイヤラが、準備完了から準備中にステータスを変更した場合、または接続を失った場合、キャンペーン マネージャは、スタンバイの SIP ダイヤラを有効化します。タイムアウト期間経過後、キャンペーン マネージャは、すべての未解決レコードを保留ステータスに戻します。

CTI サーバ、エージェント PG または SIP サーバが切断した場合、アクティブ SIP ダイヤラに障害が発生します。SIPサーバは、音声ゲートウェイまたはCUSPを使用できます。冗長ペアの各ダイヤラを異なる SIP サーバに接続します。

法規制に準拠している場合、SIP Dialerはフェールオーバー中に進行中のコールを自動的に再試行しません。代わりに、ダイヤラは、アクティブなすべての顧客レコードと保留中の顧客レコードを、キャンペーンマネージャに送信します。キャンペーンマネージャが利用できない場合、ダイヤラは内部で閉じます。

CUSP サーバは、各ゲートウェイをサーバグループ構成の一環として、各ゲートウェイを構成することで複数ゲートウェイの展開で重み付けされた負荷分散と冗長性を提供します。ゲートウェイが過負荷状態またはPSTNネットワークへのWANリンクを失った場合、CUSPはアウトバウンドコールを次に利用可能なゲートウェイに再送できます。

キャンペーンマネージャとSIPダイヤラには、すでにウォームスタンバイ機能が含まれています。このため、アウトバウンドオプション専用の CUSP サーバには Hot Swappable Router Protocol（HSRP）機能は使用しないでください。

障害時のアウトバウンド オプション レコード処理

ダイヤラは、カスタマーのレコードの中間ステータスで、キャンペーン マネージャを更新します。これにより、ダイヤラが失敗した場合に、キャンペーン マネージャは次のアクションを追跡できます。

ダイヤラが SIP Invite を送信してカスタマーにコールすると、キャンペーン マネージャにカスタマーレコードの状態更新メッセージが送信されます。その後、キャンペーンマネージャは、[ダイヤリングリスト（DL）（DialingList (DL)] テーブルで、レコードの CallStatus を [ダイヤル済み（Dialed）] 状態に更新します。

また、キャンペーン マネージャは、次のイベントでカスタマーレコードの状態を更新します。

- **通話に成功**: キャンペーン マネージャは、カスタマーレコードを [終了（Closed）] 状態に更新します。
- **ダイヤラとキャンペーン マネージャ間の接続に失敗：**すべての [ダイヤル済み（Dialed）] 状態のレコードは、[ダイヤル済み（Dialed）]状態のままになります。アクティブ状態レコードが [不明（Unknown）] 状態に変わります。
- **ダイヤラと CTI サーバ間の接続に失敗：**キャンペーン マネージャは、カスタマーレコードを [終了（Closed）] 状態に更新します。次に、キャンペーン マネージャは、ダイヤラ切断状態を送信すると、すべてのアクティブ状態のレコードは、[不明（Unknown）]状態となります。

[ダイヤル済み（Dialed）] 状態のレコードは、[ダイヤル済み（Dialed）] 状態のままになります。

- **ダイヤラと SIP ゲートウェイ（GW）間の接続に失敗：**エージェントデスクトップからコールがリリースされると、キャンペーン マネージャは、[終了（Close）] 状態のカスタマー レコード メッセージを受信します。この状況の場合、エージェントデスクトップからコールがリリースされると、すべての [ダイヤル済み（Dialed）] 状態レコードが [終了（Closed）] 状態に変化します。アクティブ状態レコードが [不明（Unknown）] 状態に変わります。
- **ダイヤラと MR PIM 間の接続に失敗：**キャンペーン マネージャは、接続状態のダイヤラ ステータス メッセージのみを受信します。[終了（Closed）] のカスタマー レコード メッセージを受信したら、レコードが [終了（Closed）] 状態に更新されます。
- **キャンペーン マネージャが失敗した場合：**すべての [ダイヤル済み（Dialed）] 状態のレコードが、[終了（Closed）] 状態に変わります。アクティブ状態レコードが [不明（Unknown）] 状態に変わります。

キャンペーン マネージャ高可用性に関する考慮事項

キャンペーン マネージャは、冗長ペアであるサイド A およびサイド B としてウォーム スタンバイモードで実行します。デフォルトでは、サイド A のキャンペーン マネージャ（キャンペーン マネージャ A）は、アクティブなキャンペーン マネージャとして設定されます。キャンペーン マネージャ B はスタンバイのキャンペーン マネージャとして設定されます。Logger の各冗長ペアには、独自のキャンペーン マネージャおよびアウトバウンド オプション インポートがあります。

アウトバウンド オプション高可用性を有効にする際は、プロセスは、連絡テーブル、ダイヤリング リスト、通話禁止テーブルおよび、個人的コールバック（PCB）に対する双方向データベースの複製を開始します。

システムのスタートアップ時に、アウトバウンドオプションインポートおよびダイヤラは、キャンペーン マネージャへの接続を開始します。スタンバイ キャンペーン マネージャは、スタンバイサイドからのアウトバウンドオプションインポート接続を受け入れ、アウトバウンドオプションインポートをスタンバイ状態に設定します。ただし、スタンバイ キャンペーン マネージャは、常駐側からのダイヤラ接続を含むダイヤラ接続を拒否します。アクティブなキャンペーン マネージャは、スタンバイ側からのダイヤラを含む、アウトバウンドオプションインポートおよびダイヤラ接続を受け入れます。

Logger 側のアウトバウンド オプション（ブレンドエージェント）インポート プロセスは、同じ Logger 側のキャンペーン マネージャのみと通信します。したがって、各サイドにあるキャンペーン マネージャとブレンド エージェント インポートのプロセスのステータスは、お互い同期しています。

ダイヤラまたはブレンド エージェント インポート プロセスのいずれかが、EMTClientTimeoutToFailover 間隔内でキャンペーン マネージャに接続できない場合、キャンペーン マネージャは切り替わります。

次の障害が発生した場合、キャンペーン マネージャはフェールオーバーします。

- アウトバウンド オプション インポートへの接続に失敗した場合。

- すべてのダイヤラへの接続に失敗した場合。

Note キャンペーンマネージャが1つのダイヤラに接続されている場合は、アクティブなキャンペーン マネージャはフェールオーバーしません。

- すべてのダイヤラが、アクティブなキャンペーン マネージャに [準備中（Not Ready）] のステータスをレポートする場合。
- ルータへの接続が失敗する場合。

障害が発生したキャンペーン マネージャがオンラインに戻ると、スタンバイ状態に設定されます。アクティブなキャンペーン マネージャはアクティブな状態を継続します。

冗長ペア内の1つの キャンペーン マネージャに障害が発生した場合、別側が、複製フォルダ内のファイルシリーズの複製トランザクションを保管します。Loggerでディスク容量を調整する際は、これを考慮してください。

Note アウトバウンド オプションの高可用性が有効になっていない場合、ルータは、展開入タイプを必要に応じて認識し、フェールオーバー メッセージを破棄します。

キャンペーン マネージャ障害発生時のダイヤラの動作

ダイヤラは、アクティブなキャンペーン マネージャに接続します。ダイヤラは、アクティブなキャンペーンマネージャに接続されるまで、サイドAとサイドBの間でキャンペーン マネージャに接続試行します。アクティブなキャンペーン マネージャがダウンすると、構成可能な間隔（デフォルト値は、60秒）の後、スタンバイ中のキャンペーンマネージャがアクティブになります。

ダイヤラのフェールオーバーの動作は次のとおりです。

- **システム起動時：**サイドAキャンペーン マネージャがアクティブになります。ダイヤラは最初に サイド A のキャンペーン マネージャに接続リクエストを送信します。このキャンペーン マネージャに接続できない場合、設定可能な間隔後、ダイヤラは、サイドBのキャンペーンマネージャにリクエストを送信します。アクティブなキャンペーンマネージャの接続が受領され、確立されます。
- **ダイヤラかアクティブなキャンペーン マネージャへの切断を検出した場合：**ダイヤラは、スタンバイ中のキャンペーンマネージャに接続リクエストを送信します。そのキャンペーンマネージャのフェールオーバーが完了すると、スタンバイ中のキャンペーン マネージャはアクティブなキャンペーン マネージャとなり、ダイヤラに接続します。

  キャンペーン マネージャのフェールオーバーが発生していない場合は、スタンバイ中のキャンペーン マネージャは接続リクエストを拒否します。その後、ダイヤラは、どちらかのキャンペーンマネージャがアクティブになり、接続リクエストを承認するまで、キャンペーンマネージャ間で接続リクエストを交互に送信します。

Microsoft Windows イベントビューア、SYSLOG および SNMP は、ダイヤラの切断および接続試行をキャプチャします。

シングルサインオンの高可用性に関する考慮事項

クラスタとして、Cisco Identity Service（Cisco IdS）を導入します。クラスタには、発行者とサブスクライバが含まれます。クラスタノードは、クラスタ全体で自動的に構成データと承認コードを複製します。ノードが再接続されると、クラスタは最新の構成および承認コードデータを決定し、クラスタ全体の構成を再現します。

コンタクトセンター アプリケーションは、任意のノードに到達できる場合、エージェントまたはスーパーバイザを認証または承認します。コンタクトセンター アプリケーションは、ローカルの Cisco IdS ノードをデフォルトで照会します。そのノードが利用できない場合、アプリケーションは、構成済みのリモートノードを照会します。ローカルノードがクラスタに再接続されると、アプリケーションはローカルノードのクエリに戻ります。

ネットワークでパケット損失が 5% を超えると、他のノードが発行した承認コードを使用してノードがアクセストークンを取得しない可能性があります。この場合、ユーザは再度サインインする必要があります。パケット損失が大き過ぎたか、接続が失われた場合、Cisco IdS は、単独ノードとして機能します。クラスタは、ネットワーク接続が向上すると自動的にリフォームします。