



## CHAPTER 4

# ハイアベイラビリティのための Unified CVP の設計

---

この章では、ハイアベイラビリティ Unified CVP システムの設計に関するガイドラインおよびベストプラクティスについて説明します。

この章では、次のトピックについて取り上げます。

- 「概要」 (P.4-2)
- 「レイヤ 2 スイッチ」 (P.4-3)
- 「発信元ゲートウェイ」 (P.4-4)
- 「SIP プロキシ」 (P.4-5)
- 「Unified CVP SIP サービス」 (P.4-12)
- 「サーバ グループ」 (P.4-14)
- 「ゲートキーパー」 (P.4-17)
- 「Unified CVP H.323 サービス」 (P.4-20)
- 「Unified CVP IVR サービス」 (P.4-23)
- 「VoiceXML ゲートウェイ」 (P.4-24)
- 「コンテンツ サービス スイッチ (CSS)」 (P.4-30)
- 「メディア サーバ」 (P.4-32)
- 「Unified CVP VXML Server」 (P.4-33)
- 「自動音声認識 (ASR) および音声合成 (TTS) サーバ」 (P.4-34)
- 「Cisco Unified Communications Manager」 (P.4-36)
- 「Intelligent Contact Management (ICM)」 (P.4-37)

## この章の新規情報

表 4-1 に、この章に新しく追加されたトピック、またはこのマニュアルの以前のリリースから大幅に改訂されたトピックの一覧を示します。

表 4-1 新規情報、またはこのマニュアルの以前のリリースからの変更情報

新規トピックまたは改訂されたトピック	説明
「Cisco Unified SIP プロキシ (CUSP) のサポート」 (P.4-7)	CUSP プロキシ サーバの 2 つの展開方法
「サーバ グループ」 (P.4-14)	SIP INVITE の送信を試行する前に、宛先アドレスのステータスを発信元エンドポイントが認識できるようにする、ダイナミック ルーティング機能
「VoiceXML ゲートウェイ」 (P.4-24)	同じコールの異なるレグでの G.729 と G.711 コーデックの混在のサポート、および新しいロード バランシング支援機能

## 概要

ハイアベイラビリティ設計では、トップレベルの障害保護が実現されます。ソリューションは、次のようなビジネス上の必要性によって異なります。

- コール障害に対する耐性
- 予算
- トポロジ上の考慮事項

Unified CVP は、多くのハードウェアおよびソフトウェア コンポーネントを使用する、多くの構成に展開できます。各ソリューションは、コール センターで障害の影響を受けるリソースを最小限に抑えるような設計になっている必要があります。影響を受けるリソースのタイプおよび数は、ビジネス要件の厳しさや、さまざまな Unified CVP コンポーネント（ネットワーク インフラストラクチャを含む）に対して選択する設計特性によって異なります。適切な Unified CVP 設計はほとんどの障害（この章で後ほど定義します）に耐えますが、一部の障害を発信者に分からないようにできないことがあります。

Unified CVP は、ミッションクリティカルなコール センターのために設計された高度なソリューションです。Unified CVP 展開を成功させるには、データと音声のインターネット作業、システム管理、および Unified CVP アプリケーションのコンフィギュレーションに関する経験を持つチームが必要です。

Unified CVP を実装する前に、後で展開作業において高コストなアップグレードやメンテナンスを行わずに済むように、入念な準備および設計計画を使用してください。常に、考えられる最悪の障害シナリオを考慮して設計し、将来のスケラビリティをすべての Unified CVP サイトについて考慮してください。

つまり、事前に計画を立て、このマニュアルおよび次の URL から入手可能な最新バージョンの『Cisco Unified Communications Solution Reference Network Design (SRND) Based on Cisco Unified Communications Manager』に記載されている、すべての設計ガイドラインおよび推奨事項に従ってください。

[http://www.cisco.com/en/US/products/sw/voicesw/ps556/products\\_implementation\\_design\\_guides\\_list.html](http://www.cisco.com/en/US/products/sw/voicesw/ps556/products_implementation_design_guides_list.html)

Unified CVP ソリューションの計画および設計に関する支援については、シスコまたは認定パートナーの Systems Engineer (SE; システム エンジニア) に相談してください。

### Unified CVP コール サーバ コンポーネントに関する注意

このマニュアルの他の章では、Unified CVP コール サーバを単一のコンポーネントとして扱います。これは、これらの章では、Unified CVP コール サーバについてそれ以上の詳細を説明する必要がないためです。ただし、Unified CVP のハイアベイラビリティについて説明する場合、このコンポーネントは実際にはいくつかの部分で構成されていることを理解しておく必要があります。

- H.323 サービス：着信コールと発信コールの H.323 処理、およびゲートキーパーへの登録を行います。H.323 サービスは、以前のバージョンの Unified CVP では、Unified CVP Voice Browser と呼ばれていました。
- SIP サービス：SIP を使用して、着信コールおよび発信コールの処理を行います。
- ICM サービス：ICM へのインターフェイスです。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。ICM サービスは、以前のリリースの Unified CVP ではアプリケーション サーバの一部でしたが、現在は別のコンポーネントになっています。
- IVR サービス：Unified CVP マイクロアプリケーションから VoiceXML ページへ、およびその逆の変換を行います。IVR サービスは、以前のバージョンの Unified CVP では、アプリケーション サーバと呼ばれていました。

## レイヤ 2 スイッチ

図 4-1 に、耐障害性の Unified CVP システムの概要レイアウトを示します。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 Busy Hour Call Attempt (BHCA; 最繁忙時呼数) に応じて異なります。次の各項では、これらのコンポーネントそれぞれに関するフェールオーバー戦略について説明します。

図 4-1 冗長性のある Unified CVP システム

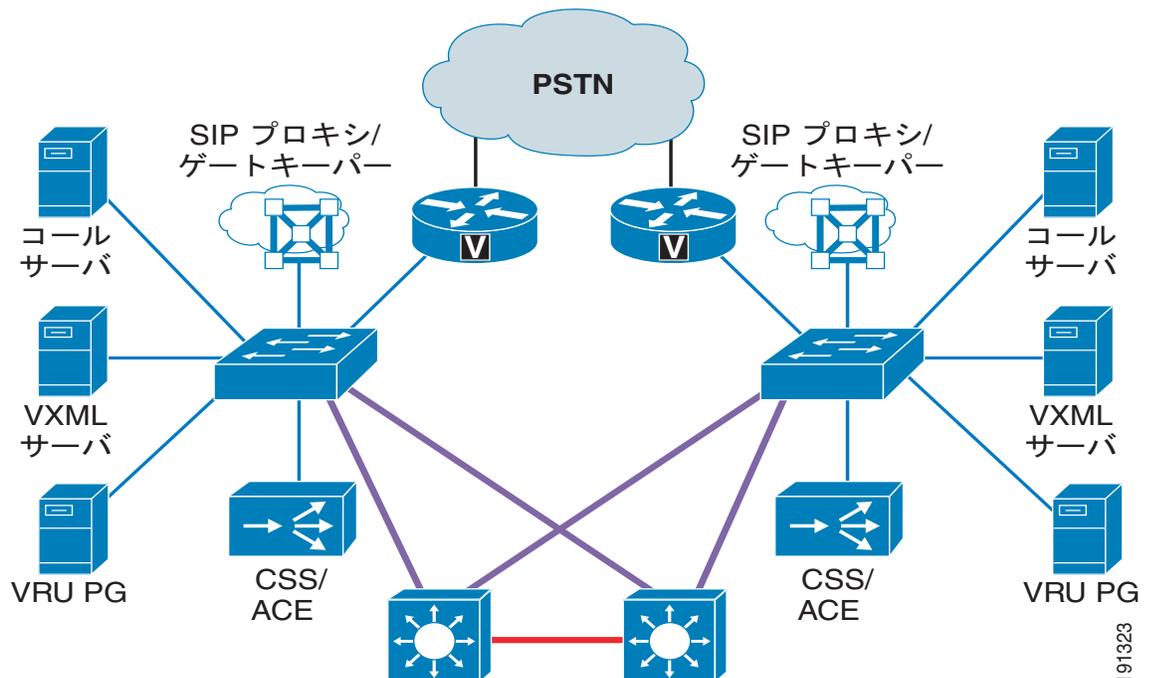


図 4-1 では、2 台のスイッチによって、Unified CVP Server にトップ レベルのネットワーク冗長性がもたらされます。

- 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。もう一方のスイッチに接続されているコンポーネントには、コール処理のために引き続きアクセス可能です。
- Content Services Switch (CSS; コンテンツ サービス スイッチ) を使用している場合、Hot Standby Router Protocol (HSRP; ホットスタンバイ ルータ プロトコル) に似たプロトコルである Virtual Router Redundancy Protocol (VRRP; 仮想ルータ冗長プロトコル) を介して相互に keep-alive メッセージを送信するためには、冗長パートナーが同じ VLAN 上に展開されている必要があります。一方のスイッチに障害が発生しても、他方の CSS は引き続き動作します。
- 図 4-1 では冗長性のために CSS を使用していますが、Application Content Engine (ACE) も使用できます。「Application Content Engine (ACE)」(P.1-16) を参照してください。

データセンター ネットワーク設計の詳細については、次の URL から入手可能なデータセンターに関するマニュアルを参照してください。

<http://www.cisco.com/go/designzone>



(注)

NIC のチーム機能は、Unified CVP ソリューションでは現在サポートされていません。



(注)

NIC カードおよびイーサネット スイッチは、10/100 リンクの 100 MB 全二重に設定するか、ギガビット リンクの自動ネゴシエーションに設定することを推奨します。

## 発信元ゲートウェイ

Unified CVP ソリューションでの発信元ゲートウェイの機能は、PSTN からのコールを受け入れ、コールルーティングおよび IVR 処理のためにこれを Unified CVP に転送することです。

この項では、次のトピックについて取り上げます。

- 「設定」(P.4-4)
- 「コール処理」(P.4-20)

## 設定

発信元ゲートウェイおよび T1/E1 回線に冗長性および信頼性をもたらす方法に関する最新情報については、次の URL から入手可能な最新バージョンの『Cisco Unified Contact Center Enterprise Solution Reference Network Design (SRND)』を参照してください。

[http://www.cisco.com/en/US/products/sw/custcosw/ps1844/products\\_implementation\\_design\\_guides\\_list.html](http://www.cisco.com/en/US/products/sw/custcosw/ps1844/products_implementation_design_guides_list.html)

また、Unified CVP ソリューションでハイアベイラビリティを実現するゲートウェイを設計する場合、次の問題も考慮してください。

- ICM 統合モデルで使用する場合、発信元ゲートウェイは、H.323 または SIP を使用して Unified CVP と通信します。MGCP とは異なり、SIP および H.323 では、冗長性機能はプロトコルに組み込まれていません。代わりに、SIP および H.323 は、ゲートウェイおよびコール処理コンポーネントを使用して、冗長性を実現します。

- ゲートウェイを設定する場合、次の設定例に示すように、H.323 または 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することを推奨します。

H.323 :

```
interface Loopback0
 ip address 10.0.0.10 255.255.255.255
 h323-gateway voip interface
 h323-gateway voip id sj-gk ipaddr 10.0.1.100 1719 <<- GK IP
 h323-gateway voip h323-id sj-gw1
 h323-gateway voip bind srcaddr 10.0.0.10
```

SIP :

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

このコンフィギュレーションでは、物理インターフェイスに依存せずにコールシグナリングが動作します。この方法では、一方のインターフェイスに障害が発生しても、他方のインターフェイスでトラフィックを処理できます。各ゲートウェイインターフェイスを異なる物理スイッチに接続し、一方のスイッチまたはインターフェイスに障害が発生した場合に冗長性を実現する必要があります。ゲートウェイ上の各インターフェイスは、異なるサブネット上の IP アドレスを使用して設定されます。次に、ネットワークの IP ルータは、スタティック ルートまたはルーティング プロトコルを使用して、ループバック アドレスへの冗長ルートを持つように設定されます。ルーティング プロトコルを使用する場合、ゲートウェイと交換するルート数に注意してください。また、ゲートウェイがループバック アドレスだけをアドバタイジングし、ルートを受信しないようにルーティング アップデートを制限するフィルタの使用を考慮してください。

## コール処理

発信元ゲートウェイに障害が発生した場合、次の状態がコール処理に適用されます。

- 進行中のコールはドロップされます。このゲートウェイ上のすべての T1/E1 トランクへの D チャネルを PSTN スイッチが失うため、これらのコールを保持する方法はありません。
- 新しいコールは、代替ゲートウェイで PSTN キャリアによって T1/E1 に転送されます (PSTN スイッチにトランクがあり、ダイヤルプランがこのように設定されている場合)。

## SIP プロキシ

SIP プロキシ サーバは、Unified CVP ソリューションにおいて、ゲートキーパーに似た役割を果たします。SIP プロキシ サーバは、SIP エンドポイントの代わりにダイヤルプランの解決法を提供し、ダイヤルプラン情報を各 SIP デバイスにスタティックに設定するのではなく、集中的に設定します。SIP プロキシ サーバは、Unified CVP ソリューションでは必要ありませんが、集中的に設定およびメンテナンスできるという利点のため、ほとんどのソリューションで使用されます。複数の SIP プロキシ サーバをネットワークに展開し、ロードバランシング、冗長性、および地域の SIP コールルーティング サービスを実現できます。Unified CVP ソリューションでは、SIP コールルーティングの選択肢は次のとおりです。

- SIP プロキシ サーバ
  - 利点：
    - 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。

SIP プロキシは、ダイヤル プランの解決法またはクラスタ間コール ルーティングのために、すでに存在しているかまたはその他のアプリケーションに使用されている場合があります。

– 欠点：

追加のサーバまたはハードウェアあるいはこれら両方が SIP プロキシに必要（展開済みでない場合）。

- DNS サーバ上でサーバ グループ（DNS SRV レコード）を使用するスタティック ルート

– 利点：

加重ロード バランシングおよび冗長性。

– 欠点：

DNS サーバの場所によっては、既存の DNS サーバを使用できない場合があります。

DNS サーバ管理権限を共有または委任する機能が、一部の組織では使用できない場合があります。

ダイヤル プラン コンフィギュレーションを各デバイス（Cisco Unified Communications Manager、Unified CVP、およびゲートウェイ）に対して個別に設定する必要があります。

DNS SRV ルックアップが Unified CVP によってすべてのコールそれぞれに対して実行されず、DNS サーバの応答が遅い、DNS サーバを使用できない、DNS サーバが WAN の外側にある場合などでは、パフォーマンスに影響します。

- ローカル DNS SRV レコードを使用するスタティック ルート

– 利点：

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ため、ポイント障害、遅延、および DNS サーバのパフォーマンスの問題が発生しません。

– 欠点：

ダイヤル プランを各デバイス（Cisco Unified Communications Manager、Unified CVP、およびゲートウェイ）に対して個別に設定する必要があります。



(注)

DNS サーバによる SRV の使用またはサーバ グループの使用によるスタティック ルートの選択により、プライマリの宛先が停止中またはネットワークに接続されていないときに、Unified CVP コール サーバ上での UDP 転送によるフェールオーバーまたはロード バランシング中に予期しない長時間の遅延が引き起こされる可能性があります。UDP で、ホスト名にサーバ グループ（srv.xml）内で異なるプライオリティを持つ複数の要素がある場合、CVP は、要素ごとに 2 回、各試行間を 500 ミリ秒で試行します。最初の要素が応答しない場合、次の要素を 1 秒後に試行しようとします。この遅延は、ロードバランシングに応じて、また T1 タイマーに関する RFC 3261 の第 17.1.1.1 項に準拠して、障害が発生している間、すべてのコールに発生します。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。これは、TCP にも適用されます。

- IP アドレスを使用したスタティック ルート
    - 利点：
      - 宛先にコールを配信する際に他のデバイス（DNS またはプロキシ）に依存しません。
    - 欠点：
      - Unified CVP からの SIP コールに対して冗長性を持たせることができません。
      - ダイヤル プランを各デバイス個別に設定する必要があります。
- このオプションは、冗長性がない（単一のサーバ）環境または実験での展開の環境でのみ意味があります。

Unified CVP ソリューションの各デバイスは、上記の方法を使用して、コールの送信先を決定できます。SIP ネットワークへの Unified CVP コール サーバ インターフェイスは、Unified CVP SIP サービスを使用します。このサービスについては、「Unified CVP SIP サービス」(P.4-12) の項で説明します。



(注)

DNS を Cisco Unified Presence プロキシ サーバで使用すると長時間の遅延が発生するため、Cisco Unified Presence Server (CUP Server) 上では DNS サーバをディセーブルにすることを推奨します。詳細については、CUP Server のリリース ノートを参照してください。

## Cisco Unified SIP プロキシ (CUSP) のサポート

Unified CVP Release 8.0(1) は、Cisco Unified SIP Proxy Server (CUSP Server; Cisco Unified SIP プロキシ サーバ) バージョン 1.1.4 で検証されています。つまり、Unified CVP は、CUP プロキシ サーバと CUSP プロキシ サーバの両方をサポートするようになりました。

次に、2 つの実装の相違点を示します。

- CUSP は専用 SIP プロキシ サーバであり、CUP プロキシは、プロキシ エンジンを備えたプレゼンス サーバです。
- これらは異なるハードウェア上で実行されます。CUSP Server はゲートウェイで実行され、CUP Server は MCS マシンで実行されます。
- また、CUP にはさまざまなデフォルト設定があります。たとえば、CUP プロキシでは、MS OCS フェデレーションに必要となるためレコード ルートはデフォルトでオンです。CUSP プロキシでは、レコード ルートはデフォルトでオフです。
- 詳細については、ソリューション サイジング ツール (<http://tools.cisco.com/cucst/faces/login.jsp>) を参照してください。

### CUSP の展開方法

CVP ソリューションの CUSP プロキシでは、2 つの展開オプションがサポートされています。これらの方法は、次の 2 つのトピックに記載されています。

#### 展開オプション A - 冗長 SIP プロキシ サーバ

この方法は、次のとおりです。

- 冗長性のために、地理的に離れた 2 つのゲートウェイから構成されます。それぞれに 1 つのプロキシ モジュールがあります。プロキシの冗長性のために SRV プライオリティが使用されます。HSRP はありません。

- ISR は、プロキシブレード機能専用です。これは、CUSP に関するプラットフォームの認証制約のため、VXML ゲートウェイまたは TDM ゲートウェイと同じ場所には展開されません。
- TDM ゲートウェイは、SRV またはダイヤル ピア設定で設定され、プライマリ CUSP プロキシまたはセカンダリ CUSP プロキシを使用します。
- CUSP は、サーバグループを使用して設定され、プライマリおよびバックアップの Unified CVP、Unified CM および VXML ゲートウェイを検索します。
- 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。
- Cisco 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。

#### オプション A の例

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、セカンダリプライオリティブレードにフェールオーバーする必要がある場合だけ WAN を超えます。

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)
```

#### 展開オプション B - 冗長 SIP プロキシサーバ (二重容量)

この方法は、次のとおりです。

- 冗長性のために、2つのゲートウェイから構成されます。各シャーシに2つのプロキシモジュールがあります。4つのプロキシサーバすべてがアクティブモードで、コールはこれらの中でバランシングされます。
- SRV を使用して、プライオリティによりプロキシ間でロードバランシングを行います。
- ISR は、プロキシブレード機能専用です。これは、CUSP に関するプラットフォームの認証制約のため、VXML ゲートウェイまたは TDM ゲートウェイと同じ場所には展開されません。
- TDM ゲートウェイは、SRV またはダイヤル ピア設定で設定され、プライマリ CUSP プロキシまたはセカンダリ CUSP プロキシを使用します。
- CUSP は、サーバグループを使用して設定され、プライマリおよびバックアップの Unified CVP、Unified CM および VXML ゲートウェイを検索します。
- 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。
- Cisco 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。

#### オプション B の例

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、セカンダリプライオリティブレードにフェールオーバーする必要がある場合だけ WAN を超えます。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)
```

## CUSP 展開のパフォーマンス マトリックス

CUSP 公開データシート「Performance Measured in the Number of New Call Attempts per Second」の表 2 に、CUSP Server のパフォーマンス データを示します。

CUSP ベースライン テストは、プロキシ上で隔離して行われ、キャパシティの数値（毎秒 **450 TCP**、**500 UDP** トランザクション）が最高クラスのベンチマークとして使用され、許容される最も負荷がかかる条件で実行されました。

プロキシサーバの観点では、CVP コールは、平均すると次の 4 つの異なる SIP コールになります。

- 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 キューイングとの協議が発生すると、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。

## CUSP 設計上の考慮事項

プロキシサーバにおいて、レコード ルート設定を常にオフにしてシングル ポイント障害を回避し、耐障害性ルーティングを可能にし、プロキシサーバのパフォーマンスを向上します。プロキシサーバでレコード ルート設定を使用すると、CUSP ベースライン マトリックスに示すようにパフォーマンスへの影響が 2 倍になります。また、プロキシが停止した場合、これがコールに対してシングル ポイント障害になるため、ハイアベイラビリティ モデルではなくなります。

CUSP では、レコード ルートはデフォルトでオフです。



(注)

### SIP ハートビートを使用したアップストリーム要素ルーティング

CUSP プロキシでは、INVITE または OPTIONS への応答はすべて適切な応答であるため、CUSP は、応答を受信すれば要素ダウンのマークを付けません。応答が、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設定されている場合、CUSP は、グループ内の次の要素にフェールオーバーします。そうでない場合、CUSP は、応答を最終応答としてダウンストリームに送信します。

CUP プロキシ バージョン 7.0(5) では、CUSP への実装方法はさまざまですが、OPTIONS ping および INVITE 要求を使用するアップストリーム ルート宛先ステータスをサポートしています。CUP がルートの ping を開始するのは、コール試行または OPTIONS ping が 5XX 応答で失敗した後だけです。宛先には、INVITE または OPTIONS メッセージへの 5XX 応答を使用してアウトオブサービスのマークが付けられます。

## 設定

次の各項では、SIP プロキシ サーバと、SIP を使用する Cisco IOS ゲートウェイのコンフィギュレーションについて説明します。ここでは、コンフィギュレーション オプションの完全なリストを示しているわけではなく、特定のコンフィギュレーション概念にだけ焦点を当てています。

### SIP プロキシ サーバ コンフィギュレーション

SIP プロキシ サーバは、適切なデバイス（Unified CVP コール サーバ、VoiceXML ゲートウェイ、Cisco Unified Communications Manager クラスタなど）を指すスタティック ルートを使用して設定する必要があります。SIP プロキシ サーバ コンフィギュレーションでは、ルートのプライオリティを指定できます。1 つの宛先へのルートが複数ある場合、同じプライオリティを持つ宛先間でロード バランシングするように SIP プロキシを設定するか、または異なるプライオリティを使用して優先順位を付けてコールを送信するように SIP プロキシを設定できます。

Cisco Unified Presence Server SIP プロキシは、発信コールに DNS SRV を使用できません。ロード バランシングまたはフェールオーバーを行うために、複数のスタティック ルートを使用して設定する必要があります（Cisco Unified Presence Server は、DNS SRV 機能をサポートしていませんが、Unified CVP 展開ではテストされていません）。スタティック ルートは、IP アドレスまたは通常の DNS A ホスト レコードを指すことができます。

プロキシ サーバの障害の影響を軽減するには、RecordRoute ヘッダーに SIP プロキシ サーバからデータ入力されないようにすることを推奨します（これは、Cisco Unified Presence Server プロキシでは、デフォルトでオンになっています）。こうすることにより、着信コールが SIP プロキシを通過するようになりますが、コールが Unified CVP コール サーバ（コール サーバ）に到達すると、シグナリングが発信元デバイスとコール サーバの間で直接交換され、SIP プロキシの障害は、進行中のコールには影響しなくなります。

### Cisco IOS ゲートウェイ コンフィギュレーション

Cisco IOS ゲートウェイでは、ダイヤルピアを使用して、電話番号を照合し、宛先を SIP プロキシ サーバ、DNS SRV、または IP アドレスにできます。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 プロキシ サーバに送信する Cisco IOS ゲートウェイ コンフィギュレーションを示します。

```

sip-ua
  sip-server ipv4:10.4.1.100:5060

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

```

ダイヤルピアでの **sip-server** コマンドは、Cisco IOS ゲートウェイに対して、**sip-ua** で設定されたグローバル定義の **sip-server** を使用するよう指示します。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 プロキシ サーバを直接指すように複数のダイヤルピアを設定できます。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せん。

```
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 プロキシサーバに送信されます。複数の Unified CVP コールサーバがある場合、SIP プロキシサーバは、ロードバランシングおよび冗長性のために複数のルートを使用して設定されます。Cisco IOS ゲートウェイでは、SIP プロキシサーバを使用せずに、ロードバランシング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ロードバランシングするように、複数のダイヤルピアを使用した Cisco IOS ゲートウェイ コンフィギュレーションを示します。

```
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）に対して使用する必要があるホストを定義できます。また、これらのホスト間でのロードバランシングの特性を定義できます。次の例では、上記のように設定された3つのダイヤルピアで実現される冗長性が DNS SRV レコードを使用して単一のダイヤルピアに置き換えられます。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、スタティック ホスト レコードと同様に DNS SRV レコードをスタティックに定義できます。この機能を使用すると、DNS SRV ロードバランシングおよび冗長性を実現しながらダイヤルピア コンフィギュレーションを簡素化できます。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 サービスのスタティック SRV レコードのコンフィギュレーションを示します。cvp.cisco.com の SIP SRV レコードは、3台のサーバ間でロードバランシングするように設定されます。

```
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
```

## コール処理

次の障害シナリオの場合、コールは示されているように処理されます。

- プライマリ SIP プロキシ サーバの障害  
アクティブ コールは保持されます。後続のコール転送は正常に行われます。ただしこれは、バックアップの SIP プロキシを使用でき、RecordRoute ヘッダーが SIP プロキシによってデータ入力されていない場合です。RecordRoute ヘッダーにデータが入力されている場合、ゲートウェイへのシグナリングは実行できず、後続の転送は失敗します。
- すべての SIP プロキシ サーバに障害が発生または到達不能  
ゲートウェイで存続可能性が設定されている場合、ゲートウェイに到着する新しいコールは、デフォルトのルートにルーティングされます。

## Unified CVP SIP サービス

Unified CVP SIP サービスは、Unified CVP コール サーバ（コール サーバ）上のサービスで、すべての着信および発信の SIP メッセージングおよび SIP ルーティングを処理します。コール サーバは、発信ダイヤル プランの解決法に SIP プロキシ サーバを使用するように設定できます。または、IP アドレスまたは DNS SRV に基づいてスタティック ルートを使用するように設定できます。コール サーバは、スタティック ルートに関するコンフィギュレーション情報を共有しません。したがって、スタティック ルートを変更する必要がある場合、各コール サーバの SIP サービスで変更を行う必要があります。コンフィギュレーション オーバーヘッドを最小限にするために、1 つの SIP プロキシ サーバを使用することを推奨します。

## 設定

単一の SIP プロキシ サーバだけがコール サーバからの発信コール ルーティングに必要な場合、SIP サービスを設定するときに SIP プロキシ コンフィギュレーションを選択します。Unified CVP Operations Console Server（Operations Console）で、次のように設定します。

- SIP プロキシ サーバを追加し、このサーバの IP アドレスを指定します。

[Call Server SIP Service] 設定で、次のように設定します。

- [Enable Outbound Proxy] = [True]
- [Use DNS SRV type query] = [False]
- [Outbound Proxy Host] = 上記で設定した SIP プロキシ サーバ

コール サーバからの発信冗長性のために複数の SIP プロキシ サーバを使用する場合、DNS 名を使用して SIP プロキシを設定し、SIP プロキシ サーバに到達するために DNS SRV レコードを設定します。DNS SRV レコードは、外部 DNS サーバ上に存在できます。または、このレコードは、各 CVP Server 上のローカル DNS SRV レコードで設定できます。OAMP Console で、次のように設定します。

- SIP プロキシ サーバを追加し、このサーバの DNS 名を指定します。

[SIP Service] 設定で、次のように設定します。

- [Enable Outbound Proxy] = [True]
- [Use DNS SRV type query] = [True]
- SIP プロキシ サーバのリストを使用して、DNS SRV レコードを設定します。

各サーバ上でローカル DNS SRV レコードを設定するには、[SIP Service] 設定で、[Resolve SRV records locally] のチェックをオンにします。

冗長プロキシ サーバにサーバ グループを使用するには、次の手順を実行します。

1. [resolve SRV records locally] を選択し、発信プロキシ ドメイン名にサーバ グループの名前を入力します。
2. [System] > [Server Groups] で、プライオリティ 1 と 2 の 2 台のプロキシ サーバを含む新しいサーバ グループを作成します。
3. サーバ グループ コンフィギュレーションをコール サーバに展開します。

## 進行中のコールのハイアベイラビリティの設定

進行中のコールがあるコール サーバに障害が発生した場合、特定のゲートウェイ コンフィギュレーション手順を実行済みの場合は、すべてのコールを保持できます。コール サーバの障害では、次のいずれかが生じる可能性があります。

- サーバのクラッシュ。
- プロセスのクラッシュ。
- プロセスのハング。
- ネットワークの停止。

この項で説明するコンフィギュレーションにより、これらの状況すべてに対して保護されます。ただし、次の 2 つの状況からは保護できません。

- 進行中のコールを含むプロセスが停止された場合。この状況は、システム管理者が、プロセスを停止する前にまずコール サーバをアウトオブサービスにしてから進行中のコールを終了することを忘れた場合に発生します。
- 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絶対数に対するスロットルはありますが、コール レートに対するスロットルはありません。一般的に、推奨の Calls Per Second (cps; 1 秒当たりのコール) を長時間超えると、いずれかのコンポーネントが正しくサイジングされていない場合、またはコール ロードが各コール処理コンポーネントの加重およびサイジングに応じて分散されていない場合、CVP ソリューションの特定のコンポーネントで不安定で予測できないコール動作が引き起こされる可能性があります (コール サーバのコール レートの詳細については、第 14 章「サイジング」を参照してください)。

コール存続可能性を実現するには、次の URL から入手可能な最新バージョンの『*Configuration and Administration Guide for Cisco Unified Customer Voice Portal (CVP)*』の説明に従って、発信元ゲートウェイを設定します。

[http://www.cisco.com/en/US/products/sw/custcosw/ps1006/products\\_installation\\_and\\_configuration\\_guides\\_list.html](http://www.cisco.com/en/US/products/sw/custcosw/ps1006/products_installation_and_configuration_guides_list.html)

survivability.tcl スクリプト自体には、一部の指示および有用な情報も含まれています。

ほとんどのダウンストリーム障害（コールサーバの障害を含む）の場合、コールは、発信元ゲートウェイによってデフォルトのルートにルーティングされます。存続可能性は、Unified CVP スタンドアロンおよび NIC ルーティング モデルには当てはまりません。これらのモデルには、関連する Unified CVP H.323 または SIP サービスがないためです。

Unified CVP が認識せずにクリアされたコールを検出するメカニズムもあります。

- 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 サービスは、発信元ゲートウェイなどのエンドポイントが自身でセッション更新を実行できるように、Session Expires ヘッダーをコールに追加できます。SIP コールでの Session Expires の使用法の詳細については、RFC 4028 (『*Session Timers in the Session Initiation Protocol*』) を参照してください。

## コール処理

次のシナリオの場合、コールは示されているように処理されます。

- コールが進行中

発信者が転送（IP 電話、VoiceXML ゲートウェイ、他の外部へのゲートウェイへの転送など）された後に、Unified CVP SIP サービスに障害が発生した場合、Unified CVP SIP サービスからの後続の転送動作（ある場合）が必要になるまで、コールは通常どおりに継続します。発信者が電話を切らずに追加の動作を待っている場合、9～18 秒の無音の後、発信者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。

コールが転送されていない場合、発信者は 9～18 秒の無音の後、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（存続可能性は、NIC ルーティング モデルでは適用されません）。

- 新しいコール

新しいコールは、SIP プロキシによって、代替 Unified CVP コールサーバに転送されます。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（存続可能性は、NIC ルーティング モデルでは適用されません）。

## サーバグループ

サーバグループは、SIP INVITE の送信を試行する前に宛先アドレスのステータスを発信元エンドポイントが認識できるようにする、ダイナミック ルーティング機能です。宛先がネットワークを介して到達不能、またはアプリケーション層でアウトオブサービスの場合、発信元 SIP ユーザ エージェントは、ハートビートメカニズムを介してステータスを事前に認識できます。

H.323 エンドポイント登録メカニズムはすでにありましたが、サーバグループ機能によってハートビートメカニズムが SIP のエンドポイントに追加されます。

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。



(注)

- サーバグループは、自動的には作成されません。サーバグループは、8.0(1) へのアップグレードによって自動的に作成されるわけではありません。この機能を利用するには、展開用にサーバグループを明示的に設定し、アップグレード後にこの機能をオンにする必要があります。
- **すでにローカル SRV を使用しているユーザの場合のアップグレード。**すでに `srv.xml` ファイルをローカル SRV で設定している Release 7.0(2) ユーザは、コンフィギュレーションを Unified CVP Operations Console Server データベースにインポートするために、下記の `import` コマンドを実行する必要があります。この作業は、以前のコンフィギュレーションの上書きを回避するために、新しいサーバグループを保存し、展開する前に行ってください。

Unified CVP SIP サブシステムは、Release 7.0(1) で使用可能なローカル SRV コンフィギュレーション XML に基づいて作成されています。

サーバグループは、1 つ以上の宛先アドレス（エンドポイント）で構成され、サーバグループドメイン名で識別されます。このドメイン名は、SRV クラスタドメイン名、または FQDN とも呼ばれます。SRV メカニズムが使用されますが、レコードの DNS サーバ解決は実行されません。サーバグループは、Release 7.0(1) のローカル SRV 実装 (`srv.xml`) と同じままですが、サーバグループ機能には、その機能に加えてハートビートメカニズムがオプションとして追加されます。



(注)

- Unified CVP のサーバグループおよび CUSP プロキシサーバのサーバグループは、同じように機能します。
- ハートビートが送信されるようにできるのは、サーバグループで定義されたエンドポイントだけです。

Release 7.0(1) では `srv.xml` コンフィギュレーションファイルは、DNS SRV クエリのオーバーヘッドを回避するよう SRV レコードをローカルに設定するのに使用されます。ただし、コンフィギュレーションの方法は手動で、Unified CVP Operations Console Server (Operations Console) からプッシュできませんでした。また、フィールドの最小値および最大値の検証はありませんでした。

Release 8.0(1) では、サーバグループの概念を使用して、このコンフィギュレーションが Operations Console SIP サブシステムに追加されます。サーバグループの条件は、ローカル SRV コンフィギュレーションの参照のみを行います。[*Server Groups with Heartbeating*] をオンにすると、Unified CVP でエンドポイントのステータスを事前にモニタできるダイナミックルーティング機能を取得できます。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、CUSP プロキシサーバは、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。

## サーバグループのハートビート設定

サーバグループのハートビートのデフォルト設定では、2 回の ping の間の ping up/down 間隔が設定されます。これは、同じエンドポイントへの ping の間の設定ではありません。サーバグループは、特定の間隔で動作してすべての要素を ping することはありません。これは、この方法が、CPU 使用率に対してシーソー効果をもたらすためです。また、システムが多くのエンドポイントを ping する必要がある場合、より多くのリソースを使用します。たとえば、すべてのグループ間で合計 3 つの要素がある場合、30 秒間隔で各要素を事前に ping するには、ping 間隔を 10 秒に設定する必要があります。

現在停止している要素が変化し、ping 間隔もこれに応じて変化することがあるため、事後対応モードでは未確定性が増します。



(注)

- サーバグループのハートビート動作設定。要素が稼働中のときに ping をオフにするには、[Up Endpoint Heartbeat Interval] をゼロに設定します（事後対応型 ping）。要素が停止しているときに ping をオフにするには、[Down Endpoint Heartbeat Interval] をゼロに設定します（事前対応型 ping）。要素が稼働中または停止中のいずれかのときに ping するには、ハートビート間隔をゼロより大きくします（適応型 ping）。
- ハートビート応答処理。CVP がコールをルーティングする先のエンドポイントは、OPTIONS に対して応答（200 OK または他の応答）で応答する必要があります。ハートビートに対して応答がある場合は、もう一方の側が動作して到達可能であることを示します。通常 200 OK が返されますが、Cisco Unified Presence Server (CUP Server) や Cisco Unified SIP Proxy Server (CUSP Server) のようなプロキシサーバは、OPTIONS メッセージで max-forwards ヘッダーがゼロに設定されているため、483 Too Many Hops 応答を返す場合があります。エンドポイントで OPTIONS または ping が許可されず、405 Method Not Allowed を返す場合もあります（これも問題ありません）。

デフォルトでは、サーバグループのハートビートは、UDP ソケット接続を使用して実行されます。[Operations Console Server Groups] ウィンドウで、トランスポートタイプを [TCP] に変更できます。要素が到達不能または過負荷のステータスの場合は、必ずその要素は、完全停止のマークを付けられず（つまり、UDP トランスポートと TCP トランスポートの両方に対して）。要素が再び稼働中になると、UDP と TCP の両方でルーティング可能になります。



(注)

TLS トランスポートはサポートされていません。

複製サーバグループ要素は、ハートビートがその要素に対して確立済みのため、ハートビートから除外されます。



(注)

サーバグループ機能の一般的なコンフィギュレーションについては、『*Configuration and Administration Guide for Cisco Unified Customer Voice Portal*』を参照してください。マニュアルは、[http://www.cisco.com/en/US/products/sw/custcosw/ps1006/products\\_installation\\_and\\_configuration\\_guides\\_list.html](http://www.cisco.com/en/US/products/sw/custcosw/ps1006/products_installation_and_configuration_guides_list.html) から入手可能です。

## スタティック ルートの認証

スタティック ルートのホスト名および IP アドレスは、DNS ルックアップ解決を使用して、起動時およびコンフィギュレーション展開時に検証されます。ホスト名が A レコードまたは SRV レコードに解決されない場合、ルートがディセーブルになり、Unified CVP エラー ログに通知が書き込まれます。この状態では、このルートへのコールのルーティングは不可能になります。ホストがローカル SRV サーバグループ コンフィギュレーション内に SRV 名として含まれる場合、ホストはローカル SRV 名に解決されるためこのチェックは実行されません。IP アドレスは、常にこの検証をパスします。

## 設計上の考慮事項

サーバグループを実装する場合、次の設計上の考慮事項を確認してください。

- ローカル SRV コンフィギュレーションを使用している場合、このコンフィギュレーションは、DNS SRV コンフィギュレーションと連携しません。ただし、要素は IP アドレスではなく A レコードホスト名として宣言され、DNS サーバルックアップまたは OS などのホスト ファイルを使用して解決される場合があります。

- CUP プロキシを使用している場合、一般的に SRV クラスタ名 (*proxy-servers.cisco.com* など) は、プロキシ コンフィギュレーションのサービス パラメータ セクションで定義する必要があります。それ以外の場合、*404 not found* 拒否になります。CUSP プロキシの場合、CLI でも同様のコンフィギュレーションを行うことができます。

## 診断

CVP ログ ファイルには、エンドポイント ステータス イベントを示すトレースがあります。  
[http://www.cisco.com/en/US/products/sw/custcosw/ps1006/products\\_installation\\_and\\_configuration\\_guides\\_list.html](http://www.cisco.com/en/US/products/sw/custcosw/ps1006/products_installation_and_configuration_guides_list.html) から入手可能な「*Configuration and Administration Guide for Cisco Unified Customer Voice Portal*」の Unified CVP System CLI の指示を参照してください。

## ゲートキーパー

H.323 ゲートキーパーが使用されるのは、モデル #4 (NIC 制御ルーティングのみを使用する VRU) を除くいずれかの ICM 統合展開モデルで H.323 が使用される場合です。モデル #4 では、呼制御に Unified CVP はまったく使用されません。また、SIP が呼制御プロトコルとして使用される場合、ゲートキーパーは必要ありません。発信元ゲートウェイは、スタティック IP アドレスを含む VoIP ダイアルピアを使用して、すべての H.323 コール ルーティングを実行します。一方、Unified CVP H.323 サービスは、必ずゲートキーパーの Remote Access Service (RAS; リモート アクセス サービス) ルックアップを実行して、コールをルーティングします。



(注)

[VAdmin SetTransferLabel] オプションを使用しているとき、ある特定の状況では、H.323 サービスは、ゲートキーパーから返された IP アドレスを無視し、IVR コール レッグをコールの発信元ゲートウェイにルーティングします。この機能により、IVR の処理またはキューイングの間に WAN 帯域幅が使用されないようになります。この状況でもゲートキーパーは必要です。これは、コールの発信元ゲートウェイへの転送に失敗した場合に H.323 サービスがゲートキーパー ルックアップ機能を実行して、考えられる代替エンドポイントを取得するためです。

Unified CVP は、ゲートキーパーのハイアベイラビリティ メカニズムの次のタイプのいずれかを使用できます。

- 「HSRP を使用するゲートキーパー冗長性」(P.4-17)
- 「代替ゲートキーパーを使用したゲートキーパー冗長性」(P.4-18)

HSRP および代替ゲートキーパーだけが Unified CVP でサポートされます。代替ゲートキーパーのサポートは、Unified CVP 3.1 SR1 で導入されました。

### HSRP を使用するゲートキーパー冗長性

HSRP は、シスコ所有のルータ冗長性プロトコルで、2 つ以上のゲートキーパーが同じ IP アドレスをアクティブ/スタンバイとして共有できます。HSRP を使用すると、2 台のゲートキーパーが連携し、LAN 上の単一の仮想 IP アドレスのようになります。

これらのゲートキーパーは、同じ IP アドレスおよび MAC アドレスを共有します。したがって、ゲートキーパーのいずれかに障害が発生しても、LAN 上のホストは、パケットを同じ IP アドレスおよび MAC アドレスに転送し続けることができます。一方のデバイスから他方のデバイスにルーティング機能を移すプロセスは、ユーザには分からないように実行されます。H.323 エンドポイント (Unified CVP H.323 サービス、Cisco Unified Communications Manager、ゲートウェイなど) は、HSRP ゲートキーパーのペアを表す仮想 IP アドレスに登録されます。

一方のゲートキーパーに障害が発生しても、他方のゲートキーパーがプライマリ制御を引き継ぎます。ただし HSRP には、HSRP フェールオーバー ペアの両方のゲートキーパーが同じ IP サブネットまたは VLAN に存在している必要があるため、通常これらは地理的に分離できないという欠点があります。また、冗長性のために HSRP を使用するゲートキーパーは、状態の情報を共有しません。したがって、フェールオーバーが発生した場合は、スクラッチから、すべてのデバイスをゲートキーパーに再登録する必要があります。

Unified CVP 3.1 SR1 以降、HSRP は推奨されていません。ゲートキーパー冗長性を実現するためには、代わりに、ゲートキーパー クラスターリングおよび Unified CVP での代替ゲートキーパー コンフィギュレーションが推奨されます。

## 代替ゲートキーパーを使用したゲートキーパー冗長性

Unified CVP H.323 サービスは、代替ゲートキーパー（必要な数だけ、制限なし）のリストを使用して設定できます。開始された H.323 サービスは、リストの最初のゲートキーパーに登録しようとします。登録に成功しない場合、登録に成功するまで、リストの残りのゲートキーパーに順次登録しようとします。

H.323 サービスは、次のいずれかのイベントが発生するまで、そのゲートキーパーに登録されたままになります。

- あるタイプの障害がゲートキーパーに発生した場合、H.323 サービスは、次のいずれかの方法でゲートキーパーの障害を認識します。
  - ゲートキーパーへの定期的な RAS Registration Request (RRQ; RAS 登録要求) がタイムアウトまたは拒否される。
  - 転送に対する Admission Request (ARQ; アドミッション要求) がタイムアウトになる。
  - ゲートキーパーが H.323 サービスに登録解除を事前に通知する（管理者がゲートキーパー コンフィギュレーションを停止する場合など）。
- ユーザが VAdmin から別の setGK を実行した場合、これにより、H.323 サービスはリストに最初のゲートキーパー（このゲートキーパーが使用可能な場合）に登録します。そのゲートキーパーが使用不可の場合は、再び登録を順次試行します。

Unified CVP の代替ゲートキーパーを使用するためには、ゲートキーパー クラスターリングは必要ありません。2 台のゲートキーパーを同じコンフィギュレーションにできます。また、代替ゲートキーパーを使用して Unified CVP を設定し、冗長性を実現できます。

Unified CVP H.323 サービスは、ゲートキーパー クラスターリング メッセージをサポートしていませんが、ゲートキーパーを GUP クラスターの一部にできない理由はありません。この方法で、元々クラスターリングをサポートする他の H.323 エンドポイント（Cisco Unified Communications Manager や Cisco IOS ゲートウェイなど）は、ゲートキーパー クラスターリングの利点を利用できます。Unified CVP は、クラスターリング メッセージ（クラスター内のゲートキーパーのいずれかが過負荷になった場合や Unified CVP がゲートキーパーに登録した場合など）を単に無視します。

Unified CVP は、ゲートキーパーに登録するときに、ゲートキーパー クラスターの他のメンバーを自動的に学習しないため、Unified CVP でゲートキーパー クラスターのメンバーをスタティックに定義する必要があります。Unified CVP は、クラスター内で 1 つ以上のゲートキーパーをリスト内の代替ゲートキーパーとして使用し、この項で説明済みのルールに従って障害を検出します。

## 設定

この項では、次のトピックについて取り上げます。

- 「HSRP のコンフィギュレーション」(P.4-19)

- 「代替ゲートキーパー」(P.4-19)

## HSRP のコンフィギュレーション

プライマリ ゲートキーパーで、次のコマンドを入力します。

```
interface ethernet 0
 ip address 10.0.1.98 255.255.255.0
 ! Unique IP address for this GK
 standby 1 ip 10.0.1.100
 ! Member of standby group 1, sharing virtual address 10.0.1.100
 standby 1 preempt
 ! Claim active role when it has higher priority.
 standby 1 priority 110
 ! Priority is 110.
```

バックアップ ゲートキーパーで、次のコマンドを入力します。

```
interface ethernet 0
 ip address 10.0.1.99 255.255.255.0
 standby 1 ip 10.0.1.100
 standby 1 preempt
 standby 1 priority 100
```

両方のゲートキーパーで、同じゲートキーパー コンフィギュレーションを入力します。例：

```
gatekeeper
 ! Enter gatekeeper configuration mode.
 zone local gk-sj cisco.com 10.0.1.100
 ! Define local zone using HSRP virtual address as gatekeeper RAS address.
```

詳細については、次の URL から入手可能な最新バージョンの『*Configuration and Administration Guide for Cisco Unified Customer Voice Portal (CVP)*』を参照してください。

[http://www.cisco.com/en/US/products/sw/custcosw/ps1006/products\\_installation\\_and\\_configuration\\_guides\\_list.html](http://www.cisco.com/en/US/products/sw/custcosw/ps1006/products_installation_and_configuration_guides_list.html)

## 代替ゲートキーパー

次の例に示すように、Unified CVP VAdmin を使用して、代替ゲートキーパーを設定します。

```
set GK "10.0.1.100, 10.0.2.100, 10.0.3.100"
```

この例では、H.323 サービスが登録できる 3 台のゲートキーパーを設定します。いずれの場合にも、H.323 サービスは、このゲートキーパーで設定される最初のローカルゾーンに登録されます。このサービスは、デフォルトの RAS ポート 1719 も使用します。

```
setGK "10.0.1.100:zone1:1718, 10.0.2.100"
```

この例では、H.323 サービスは、まずローカルゾーン zone1 を使用して、ポート 1718 のゲートキーパー 10.0.1.100 に登録しようとしています。このゲートキーパーに障害がある場合、H.323 サービスは、このゲートキーパーで定義された最初のローカルゾーンを使用して、ポート 1719 の 10.0.2.100 に順次登録しようとしています。

## コール処理

この項に記載されているコール処理は、HSRP と代替ゲートキーパーの両方に適用されます。

ゲートキーパーの障害は、次のいずれかの場合に発生します。

- プライマリ ゲートキーパーに障害が発生する。
  - 進行中のコールの一部は、エンドポイントがバックアップ ゲートキーパーへの再登録を行っている間は転送されない場合があります。転送に失敗した後、ICM にエラーが返されます。ICM スクリプトがエラーを返すようにコーティングされていて (END ノードがこれを実行します)、同時にゲートウェイで存続可能性が設定されている場合、コールはデフォルトのルートにルーティングされます。
  - 着信ゲートウェイおよび Unified CVP に到着する新しいコールは、正しく処理されます。ただし、コールの一部は、エンドポイントがバックアップ ゲートキーパーに再登録している間に存続可能性を呼び出す可能性があります。
- すべてのゲートキーパーに障害が発生する。
  - Unified CVP H.323 サービスは、アウトオブサービスになります。
  - 進行中のコールは転送されません。転送に失敗した後、ICM にエラーが返されます。ICM スクリプトがエラーを返すようにコーティングされていて (END ノードがこれを実行します)、同時にゲートウェイで存続可能性が設定されている場合、コールはデフォルトのルートにルーティングされます。
  - ゲートウェイで存続可能性が設定されている場合、ゲートウェイに到着する新しいコールは、デフォルトのルートにルーティングされます。
- プライマリ ゲートキーパーが降格するが障害は発生しない。
  - この動作は、通常、メモリ リークによるメモリ低下またはデバッグ レベル超過による CPU の過負荷の 2 つの条件により発生します。
  - この状況では、バックアップ ゲートキーパーに正常にフェールオーバーされない場合があるため、コール処理動作が予測不能になります。ゲートウェイで存続可能性が設定されている場合、コールはデフォルトのルートにルーティングされます。

## Unified CVP H.323 サービス

Unified CVP において、冗長性およびスケーラビリティの目的で複数の Unified CVP コール サーバ (コール サーバ) が使用されている場合、ロード バランシングおよびフェールオーバー サービスのためにゲートキーパーを使用することを推奨します。H.323 サービスは、H.323 メッセージを処理し、ゲートキーパーに登録する、コール サーバのコンポーネントです。

コール サーバの特定の IP アドレスを持つダイヤルピアを使用して、入力 PSTN ゲートウェイで H.323 コールを H.323 サービスに送信することは可能ですが、これを行うと、障害発生時に発信者への対応に遅延が生じます。このシナリオでは、ダイヤルピアは、Unified CVP Server 間でロード バランシングされるように、入力ゲートウェイでスタティックに設定されるか、または、通常の条件下ではプライマリ サーバが常に使用されるように優先順位付けして、入力ゲートウェイでスタティックに設定されます。何らかの理由で H.323 サービスに到達できなくなった場合、ダイヤルピアは、障害のあるサーバにコールを送信しようとし、タイムアウトになるのを待ってから、設定済みの次のダイヤルピアに進みます。このプロセスは、新しいコールごとに発生します。

代わりにゲートキーパーが使用されると、ゲートウェイ ダイアルピアは、単にゲートキーパーを指し、ゲートキーパーがアクティブなコール サーバを判別し、これらの中でロード バランシングを行います。ゲートキーパーの登録プロセスで、使用可能なサーバを認識でき、ダイアルピアと同じタイムアウトは発生しません。したがって、冗長性およびロード バランシングのためには、スタティック Cisco IOS ダイアルピアの代わりにゲートキーパーを使用することを推奨します。

## 設定

ハイアベイラビリティのための Unified CVP H.323 コンフィギュレーションは、主に入力ゲートウェイで行われますが、H.323 サービスを設定して、ゲートキーパーに登録する必要もあります。

### 新しいコールのためのハイアベイラビリティの設定

ゲートキーパーは、コール サーバがインサービスかアウトオブサービスかを認識します。したがって、ゲートキーパーにより着信コールがコール サーバにルーティングされるようにすることが重要です。デフォルトでは、Unified CVP H.323 サービスは、Technology Prefix (tech-prefix; テクノロジー プレフィクス) の **2#** を付けてゲートキーパーに登録します。Unified CVP H.323 サービスは、tech-prefix を付けて登録する必要があります。tech-prefix がないと、H.323 サービスを設定できません。

テクノロジー プレフィクスは、ゲートキーパーが登録エンドポイントを機能ごとに分類する方法です。通常、ゲートキーパーで着信コールに対して追加のコンフィギュレーションを行う必要はありません。H.323 サービスは、2# を付けてゲートキーパーに登録し、発信元ゲートウェイは、Dialed Number Identification Service (DNIS; 着信番号識別サービス) の番号の先頭に 2# を付加します。ゲートキーパーは、ゲートウェイの要求を使用可能なコール サーバと照合する方法を自動的に認識します。ゲートキーパーで、コマンド **show gatekeeper gw-type-prefix** を使用すると、ゲートキーパーがコールのルーティングに使用するルート プランが表示されます。

発信元ゲートウェイで、次のようにコール サーバのダイアルピアを定義します。

```
dial-peer voice 11111 voip
  session target ras
  tech-prefix 2#
```

コマンド **session target ras** を使用すると、ゲートウェイは、コールを該当のゲートキーパーに送信します。コマンド **tech-prefix 2#** を使用すると、ゲートウェイは、コールをゲートキーパーに送信するときに、DNIS 番号の先頭に 2# を付加します。

### 進行中のコールのハイアベイラビリティの設定

進行中のコールがあるコール サーバに障害が発生した場合、特定のゲートウェイ コンフィギュレーション手順を実行済みの場合は、すべてのコールを保持できます。コール サーバは、次のいずれかの場合に障害が発生する可能性があります。

- サーバのクラッシュ。
- プロセスのクラッシュ。
- プロセスのハング。
- ネットワークの停止。

この項で説明するコンフィギュレーションにより、これらの状況すべてに対して保護されます。ただし、次の 2 つの状況からは保護できません。

- 進行中のコールを含むプロセスが停止された場合。この状況は、システム管理者が、プロセスを停止する前にまずコール サーバをアウトオブサービスにしてから進行中のコールを終了することを忘れた場合に発生します。

- 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絶対数に対するスロットルはありますが、コール レートに対するスロットルはありません。通常、5 Calls Per Second (cps; 1 秒当たりのコール) を長時間超えると、コールサーバの動作が不安定で予測できなくなります。この状況は、Unified CVP システムを正しくサイジングすることによって防止できます。

コール存続可能性を実現するには、次の URL から入手可能な最新バージョンの『*Configuration and Administration Guide for Cisco Unified Customer Voice Portal (CVP)*』の説明に従って、発信元ゲートウェイを設定します。

[http://www.cisco.com/en/US/products/sw/custcosw/ps1006/products\\_installation\\_and\\_configuration\\_guides\\_list.html](http://www.cisco.com/en/US/products/sw/custcosw/ps1006/products_installation_and_configuration_guides_list.html)

survivability.tcl スクリプト自体には、一部の指示および有用な情報も含まれています。

ほとんどのダウンストリーム障害（コールサーバの障害を含む）の場合、コールは、発信元ゲートウェイによってデフォルトのルートにルーティングされます。存続可能性は、Unified CVP スタンドアロンおよび NIC ルーティング モデルには適用されません。その理由は、これらのモデルには、関連する Unified CVP コールサーバがないためです。

## 追加の Cisco IOS ゲートウェイ コンフィギュレーション

次の例のコマンドを使用すると、ゲートウェイ上で H.225 シグナリングの TCP タイムアウトがディセーブルになります。

```
voice service voip
  h323
  no h225 timeout keepalive
```

この操作では、ゲートウェイがコールサーバまたは Cisco Unified Communications Manager との接続を失いますが、引き続きアクティブ コールを保持します。このコマンドを使用しないと、このコマンドを使用している場合に障害の影響を受けない、引き続きアクティブなコール（つまり、RTP ストリームがエンドポイント間で引き続きストリーミングしている）は、TCP セッションがタイムアウトになると、接続解除されます。

次のコマンドは、RTP メディア タイムアウトを指定します。

```
ip rtcp report interval 2000

gateway
  timer receive-rtcp 4
```

RTCP メッセージが指定の間隔で受信されなかったことをゲートウェイが検出すると、コールは接続解除されます。

## コール処理

Unified CVP H.323 サービスに障害が発生すると、次の状態が適用されます。

- コールが進行中
 

発信者が転送（IP 電話、VoiceXML ゲートウェイ、他の外部へのゲートウェイへの転送）された後に、Unified CVP H.323 サービスに障害が発生した場合、Unified CVP H.323 サービスからの後続の転送動作（ある場合）が必要になるまで、コールは通常どおりに継続します。発信者が電話を切らずに追加の動作を待っている場合、9 ~ 18 秒の無音の後、発信者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。

コールが転送されていない場合、発信者は 9 ~ 18 秒の無音の後、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（存続可能性は、NIC ルーティング モデルでは適用されません）。

- 新しいコール

新しいコールは、ゲートキーパーによって、代替 Unified CVP コール サーバに転送されます。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（存続可能性は、Unified CVP スタンドアロンおよび NIC ルーティング モデルでは適用されません）。

## Unified CVP IVR サービス

Unified CVP 3.1 以前のリリースでは、IVR サービス（以前はアプリケーション サーバと呼ばれていた）は、H.323 サービス（以前は、Voice Browser と呼ばれていました）および VoiceXML ゲートウェイに依存せずに処理されました。ハイアベイラビリティは、アプリケーション サーバの IP アドレスのリストまたは Content Services Switch (CSS; コンテンツ サービス スイッチ) を使用するか、あるいはこれら両方を使用して、Unified CVP Voice Browser および VoiceXML ゲートウェイを設定することにより、実現されていました。Unified CVP 4.0 以降のリリースでは、IVR サービスは、SIP サービスまたは H.323 サービスと厳密に結合されています。IVR サービスがアウトオブサービスになると、H.323 または SIP サービスもアウトオブサービスになり、Unified CVP コール サーバでコールを受け付けなくなります。

## 設定

使用する IVR サービスを H.323 または SIP サービスに通知するために、追加のコンフィギュレーションを行う必要はありません。デフォルトでは、H.323 および SIP サービスは、同じサーバ上にある IVR サービスを使用します。また、コール サーバの IVR サービスの IP アドレスを使用して VoiceXML ゲートウェイを設定する必要もなくなります。SIP を使用する場合、SIP サービスは、コールが VoiceXML ゲートウェイに送信されるときに、コール サーバの IVR サービスの URL を SIP INVITE メッセージのヘッダーに挿入します。VoiceXML ゲートウェイは、使用するコール サーバを決定するときに SIP INVITE からこの情報を抽出し、使用します。H.323 を使用する場合、VoiceXML ゲートウェイは、コール サーバからの着信コールのソース IP アドレスを検査します。次に、この IP アドレスは、コール サーバの IVR サービスのアドレスとして使用されます。

次の例は、コールを受信したときに呼び出される VoiceXML ブートストラップ サービスを示しています。

```
service bootstrap flash:bootstrap.tcl
  paramspace english index 0
  paramspace english language en
  paramspace english location flash
  paramspace english prefix en
```

Unified CVP 3.1 以前のリリースと異なり、Unified CVP 4.0 以降のリリースでは、コール サーバの IP アドレスを設定する必要はありません。bootstrap.tcl は、ソース コール サーバの IP アドレスを学習し、これをこのコール サーバとして使用します。コール サーバからコールを受信するという事は、サーバが起動して、動作中であることを示しているため、CSS またはバックアップ コール サーバ コンフィギュレーションは必要ありません。

ゲートウェイのフラッシュ メモリには、handoff.tcl、survivability.tcl、recovery.vxml、いくつかの .wav ファイルなど、ハイアベイラビリティと関係のあるファイルがあります。Trivial File Transfer Protocol (TFTP; 簡易ファイル転送プロトコル) を使用して、適切なファイルをフラッシュにロードし

ます。各ファイルのコンフィギュレーション情報は、ファイル内にあります。詳細については、次の URL から入手可能な最新バージョンの『*Configuration and Administration Guide for Cisco Unified Customer Voice Portal (CVP)*』を参照してください。

[http://www.cisco.com/en/US/products/sw/custcosw/ps1006/products\\_installation\\_and\\_configuration\\_guides\\_list.html](http://www.cisco.com/en/US/products/sw/custcosw/ps1006/products_installation_and_configuration_guides_list.html)

## コール処理

Unified CVP IVR サービスに障害が発生すると、次の状態がコール処理に適用されます。

- 進行中のコールは、発信元ゲートウェイの存続可能性によって代替の場所のデフォルトのルートにルーティングされます。(存続可能性は、NIC ルーティング モデルでは適用されません)。
- 新しいコールは、インサービスの Unified CVP IVR サービスに転送されます。

## VoiceXML ゲートウェイ

VoiceXML ゲートウェイは、次の 1 つまたはいくつかのソースから取得した VoiceXML ドキュメントを解析し、レンダリングします。Unified CVP コール サーバ (この IVR サービスから)、Unified CVP VXML Server、または他の外部 VoiceXML ソースの一部。VoiceXML ドキュメントのレンダリングは、事前に録音されたオーディオ ファイルの取得および再生、ユーザ入力の収集および処理、または音声認識およびダイナミックな音声合成変換のための ASR/TTS サーバへの接続、あるいはこれらすべてから構成されます。

CVP 展開での混在コーデックの使用に関する説明については、「[G.729 および G.711 コーデックの混在サポート](#)」(P.7-9) を参照してください。各コーデックの利点および欠点の説明については、「[音声トラフィック](#)」(P.9-2) を参照してください。

## 設定

VoiceXML ゲートウェイのハイアベイラビリティ コンフィギュレーションは、H.323 のゲートキーパー、SIP の SIP プロキシ、または Unified CVP コール サーバ (コール サーバ)、あるいはこれらすべてによって制御されます。VoiceXML ゲートウェイが分散型か集中型かによっても、ハイアベイラビリティの達成度は影響されます。

コール サーバが VoiceXML ゲートウェイに接続できない場合、ICM スクリプトにエラーが返されず、ICM スクリプトでは、VoiceXML ゲートウェイ接続エラーを取得するために、Send to VRU ノードを最初の Run External スクリプト ノードから分離します。END スクリプト ノードが、Send to VRU ノードの X-path から分離されて使用される場合、コールは、発信元ゲートウェイの存続可能性によって、デフォルトのルートにルーティングされます (存続可能性は、VRU のみのモデルでは適用されません)。Queue to Skill グループ ノードも使用できますが、この方法が効果的なのは、エージェントがある場合だけです。それ以外の場合は、ICM は発信者をキューに入れようとして、失敗します (コール サーバが再び VoiceXML ゲートウェイに接続できなくなるため)。次に、END ノードも Queue to Skill Group ノードの X-path から分離して使用され、コールをデフォルトのルートにルーティングできます。



(注) VXML Server には、ロード バランシングを支援する次の 2 つの機能があります。

- ロード バランサの関与の制限
- ロード バランサ用の拡張 HTTP プローブ

[http://www.cisco.com/en/US/products/sw/custcosw/ps1006/products\\_user\\_guide\\_list.html](http://www.cisco.com/en/US/products/sw/custcosw/ps1006/products_user_guide_list.html) から入手可能な『*User Guide for Unified CVP VXML Server and Cisco Unified Call Studio*』のコンフィギュレーション オプション `ip_redirect` および `license_depletion_probe_error` を参照してください。

## 集中型 VoiceXML ゲートウェイ

このコンフィギュレーションでは、VoiceXML ゲートウェイは、Unified CVP コール サーバと同じデータセンターにあります。

### H.323 VoiceXML ゲートウェイ

ゲートキーパーで、データセンターのすべての VoiceXML ゲートウェイの H.323 ID を含むゾーンプレフィクス リストを設定します。たとえば、データセンターに H.323 ID が VoiceXMLgw1、VoiceXMLgw2、および VoiceXMLgw3 である 3 つの VoiceXML ゲートウェイがあり、ネットワーク VRU の ICM ラベルが 5551000 であるとしします。この例では、ゲートキーパーは、実質的にはラウンドロビン スキームでのコールを 3 つの VoiceXML ゲートウェイ間で分散させます (3 つのゲートウェイがすべてインサービスの場合)。

```
zone prefix gkzone-name 5551000* gw-priority 10 VoiceXMLgw1 VoiceXMLgw2 VoiceXMLgw3
```

### SIP VoiceXML ゲートウェイ

Cisco Unified Presence Server を使用している場合、SIP プロキシ サーバで、各ゲートウェイのネットワーク VRU ラベルのスタティック ルートを設定します。VRU ラベルが 5551000 の場合、スタティック ルート パターンは、`correlation-id` が付加され、VoiceXML ゲートウェイにルーティングされるように、`5551000*` になります。

Unified CVP コール サーバで SIP スタティック ルートを使用している場合、コール サーバの SIP サービス コンフィギュレーションで、各ネットワーク VRU ラベルおよびゲートウェイにスタティック ルートを設定します。VRU ラベルが 5551000 の場合、スタティック ルート パターンは、`5551000>` になります。> は、1 つ以上の数字を表すワイルドカードで、DNIS 番号に付加される `correlation-id` を VoiceXML ゲートウェイに正しく渡すために必要です。



(注)

他のワイルドカード文字も使用できます。全ワイルドカードの形式および優先情報については、Operations Console オンライン ヘルプのトピック「**Valid Formats for Dialed Numbers**」を参照してください。

SIP プロキシと Unified CVP スタティック ルートの両方の場合、ルートのネクストホップ アドレスは、ゲートウェイの IP アドレスまたは DNS SRV レコードにできます。IP アドレスを使用している場合、複数のスタティック ルートを作成する必要があります (各 VoiceXML ゲートウェイに 1 つ)。DNS SRV の場合、必要なルートは、ネットワーク VRU ラベルごとに 1 つだけです。SRV レコードが、ロード バランシングおよび冗長性を提供します。

## 分散型 VoiceXML ゲートウェイ（共存入力ゲートウェイおよび VoiceXML）

このコンフィギュレーションでは、PSTN からの着信コールを処理するゲートウェイは、低帯域幅の接続（WAN など）によって Unified CVP Server から分離され、使用される VoiceXML ゲートウェイは、入力ゲートウェイと同じです。このコンフィギュレーションの目的は、WAN 上の帯域幅の使用を回避するために、メディア ストリームをエッジで保持することです。

### H.323 VoiceXML ゲートウェイ

VBAAdmin で SetTransferLabel を使用し（ゲートキーパー ゾーン プレフィクスは使用しない）VoiceXML ゲートウェイの選択を制御します。SetTransferLabel コマンドは、ネットワーク VRU ラベルごとに指定されます。Unified CVP コール サーバが SetTransferLabel で設定されたラベルと一致するラベルを ICM から受信すると、コール サーバは、ゲートキーパー ルックアップを実行しますが、ゲートキーパーから返される宛先ゲートウェイを無視し、コールの発信元のゲートウェイにコールを戻します。H.323 サービスは、H.323 シグナリングのソース IP アドレスを検索して、発信元ゲートウェイを判別します。

### SIP VoiceXML ゲートウェイ

SIP では、SetTransferLabel コマンドと同等のものが、SIP サービスの Send to Originator コンフィギュレーションです。ネットワーク VRU ラベルが 5551000 の場合、Send to Originator パターンは、5551000> になります。> は、1 つ以上の数字を表すワイルドカード パターンです。SIP サービスは、SIP INVITE メッセージの Remote-Party-ID ヘッダーを検索して、発信元ゲートウェイを判別します。



(注)

他のワイルドカード文字も使用できます。全ワイルドカードの形式および優先情報については、Operations Console オンライン ヘルプのトピック「**Valid Formats for Dialed Numbers**」を参照してください。

## 分散型 VoiceXML ゲートウェイ（分離入力ゲートウェイおよび VoiceXML）

このコンフィギュレーションでは、PSTN からの着信コールを処理するゲートウェイは、低帯域幅の接続（WAN など）によって Unified CVP Server から分離され、使用される VoiceXML ゲートウェイは、入力ゲートウェイとは異なりますが、入力ゲートウェイと同じサイトにあります。このコンフィギュレーションの目的は、入力ゲートウェイと VoiceXML ゲートウェイを分離することが適切な場合に、メディア ストリームを同じサイトに保持し、WAN 上の帯域幅の使用を回避し、VoiceXML ゲートウェイのサイズを最適化することです。この場合、コールの IVR レッグを入力ゲートウェイに戻さないため、setTransferLabel および Send to Originator は使用できません。また、各リモートサイトの ICM で別のネットワーク VRU、ネットワーク VRU ラベル、およびお客様を設定する必要があるため、ゲートキーパーまたは SIP プロキシを使用してコール ルーティングを制御することもできません。代わりに、SetSigDigits 機能を使用します。

この方法では、コール サーバが、着信 DNIS 番号から先頭の最上位の数字を除去します。除去した値は保存され、このコールを後続するときに先頭に付加されます。

### H.323 VoiceXML ゲートウェイ

H.323 を使用する場合、最上位の数字の先頭に # 記号が付加され、ゲートキーパーがこれをテクノロジー プレフィクスとして処理します。リモートサイトの VoiceXML ゲートウェイは、DNIS 番号から除去された先頭の最上位の数字と同じテクノロジー プレフィクスを使用して、ゲートキーパーに登録する必要があります。ゲートキーパーは、コールの IVR レッグを正しい VoiceXML ゲートウェイにルーティングします。Cisco Unified Communications Manager (Unified CM) を使用している場合、Unified CVP は、すべての転送（Unified CM への転送を含む）に sigdigits 値を無差別に付加すること

を忘れないでください。したがって、このシナリオで Unified CM を使用している場合、次の例に示すように、VoiceXML ゲートウェイのテクノロジー プレフィクスそれぞれにゲートキーパー制御のトランクを定義し、ゾーン プレフィクス コンフィギュレーションを Unified CM エージェントのゲートキーパーに追加する必要があります。

### 入カゲートウェイのコンフィギュレーション

```
dial-peer voice 1000 voip
  tech-prefix 2# (gets the call to CVP)
  translate-outgoing called 99
```

着信 DNIS 番号の先頭に値 3 を付加する変換ルールを適用します。

```
translation-rule 99
  Rule 1 8002324444 38002324444
```

DNIS 番号が 8002324444 の場合、Unified CVP にルーティングされる最終 DNIS ストリングは、2#38002324444 です。

### VB Admin のコンフィギュレーション

```
setTechPrefix 2#
setSigDigits 1
```

2# のテクノロジー プレフィクスを除去した後、DNIS 番号から 1 つの数字を除去します。

### VoiceXML ゲートウェイのコンフィギュレーション

テクノロジー プレフィクス 3# を使用してゲートキーパーに登録します。

```
h323-gateway voip tech-prefix 3#
```

### Cisco Unified CM コンフィギュレーション (使用する場合)

VXML ゲートキーパーが使用するテクノロジー プレフィクスそれぞれに対応する、別個のゲートキーパー制御のトランクを作成します。

### ゲートキーパー コンフィギュレーション

ゾーン プレフィクスを定義して、コールを Unified CM エージェントに適切にルーティングします (Cisco Unified CM を使用している場合のみ)。

### コール ルーティングのまとめ

1. コールは、Unified CVP に DNIS ストリング 2#38002324444 で到着します。
2. Unified CVP は、まずテクノロジー プレフィクス (2#) を除去し、38002324444 になります。
3. 次に Unified CVP は、DNIS ストリングの先頭から 1 つの数字 (3) を除去し、8002324444 になります。
4. 8002324444 がコール ルーティング用に ICM に渡されます。
5. 転送時、ICM はラベル 5551000102 を返すとします。Unified CVP は、3# を先頭に付加し、3#5551000102 になります。この値がアドレス解決のためにゲートキーパーに渡されます。
6. ゲートキーパーは、テクノロジー プレフィクス 3# を付けて登録した VoiceXML ゲートウェイに対してこのラベルを解決します。
7. VoiceXML ゲートウェイは、3# を除去し、宛先アドレスは 5551000102 になります。

## SIP VoiceXML ゲートウェイ

SIP を使用する場合、DNIS 番号の先頭に最上位の数字が付加され、この付加された数字に基づいてルーティングするように SIP プロキシを設定できます。VoiceXML ゲートウェイの SIP プロキシにあるスタティック ルートは、先頭に数字を付加する必要があります。この付加された数字は、元々入力ゲートウェイによって入力されたため、SIP プロキシは、これを使用して、着信ゲートウェイに基づいて使用する VoiceXML ゲートウェイを判別できます。この方法で、特定のサイトに到着するコールは、VoiceXML の処理のために常にこのサイトに戻すことができ、音声 RTP ストリームを転送するために WAN 帯域幅は使用されません。Unified CVP は、すべての転送 (Unified CM への転送を含む) に sigdigits 値を無差別に付加することを忘れないでください。したがって、このシナリオで Unified CM を使用している場合、次の例に示すように、コールが到着したときに、先頭に付加された数字を除去し、Unified CM が電話の実際の DNIS 番号を使用して、このコールをルーティングする必要があります。

### 入力ゲートウェイのコンフィギュレーション

着信 DNIS の先頭に値 3333 を付加する変換ルールを適用します。

```
translation-rule 99
  rule 1 8002324444 33338002324444

dial-peer voice 1000 voip
  translate-outgoing called 99
```

DNIS 番号が 8002324444 の場合、Unified CVP にルーティングされる最終 DNIS ストリングは、33338002324444 です。

### Unified CVP SIP サービスのコンフィギュレーション

SIP サービスを設定するには、Operations Console で、[Call Server] > [SIP] タブを選択します。多くの設定が [Advanced Configuration] ウィンドウにあります。

### VoiceXML ゲートウェイのコンフィギュレーション

DNIS ストリング (先頭に付加された数字を含む) に一致するように VXML ゲートウェイを設定します。

```
dial-peer voice 3000 voip
  incoming-called number 33335551000T
  service bootstrap
  ...
```

sigdigits パラメータを使用して、Unified CVP の bootstrap.tcl アプリケーションを設定し、着信 DNIS ストリングから数字をいくつ除去するかを指示します。

```
application
  service bootstrap flash:bootstrap.tcl
  param sigdigits 4
  ...
```

### Cisco Unified CM コンフィギュレーション (使用する場合)

[SIP Trunk configuration] ページの Significant Digits コンフィギュレーションまたは変換パターンを使用して、先頭に付加された数字を除去するように Unified CM を設定します。

### SIP プロキシ コンフィギュレーション

先頭に付加された数字を使用して、適切な VoiceXML ゲートウェイに送信されるように SIP プロキシのスタティック ルートを定義します。Unified CM クラスタのエージェントへの転送にも先頭に数字が付加されるため、エージェント電話のスタティック ルートにも付加された数字が含まれている必要があります。

#### コール ルーティングのまとめ

1. コールは、Unified CVP に DNIS 番号 33338002324444 で到着します。
2. 次に Unified CVP は、DNIS スtring の先頭から 4 つの数字 (3333) を除去し、8002324444 になります。
3. 8002324444 がコール ルーティング用に ICM に渡されます。
4. 転送時、ICM はラベル 5551000102 を返すとします。Unified CVP は、3333 を先頭に付加し、33335551000102 になります。
5. SIP サービスは、SIP プロキシまたはローカル スタティック ルートを使用してこのアドレスを解決し、このコールを VoiceXML ゲートウェイに送信します。
6. VoiceXML ゲートウェイの bootstrap.tcl は、3333 を除去し、宛先アドレスは 5551000102 になります。

## H.323 代替エンドポイント

集中型展開または分散型展開のすべての場合において、VoiceXML ゲートウェイが着信要求を拒絶した場合 (エラーや過負荷が原因) に備えて、VoiceXML ゲートウェイそれぞれに対して代替エンドポイントを設定します。

```
endpoint alt-ep h323id VoiceXMLgw1 ip-address-VoiceXMLgw2
endpoint alt-ep h323id VoiceXMLgw2 ip-address-VoiceXMLgw3
endpoint alt-ep h323id VoiceXMLgw3 ip-address-VoiceXMLgw1
```

## コール処理

VoiceXML ゲートウェイに障害が発生した場合、次の状態がコール処理に適用されます。

- 進行中のコールは、入力ゲートウェイの存続可能性によって代替の場所のデフォルトのルートにルーティングされます (存続可能性は、NIC ルーティング モデルでは適用されません)。
- 新しいコールは、代替 VoiceXML ゲートウェイを見つけます。

## 音声ゲートウェイでのハイアベイラビリティのためのハードウェア設定

個々のハードウェア コンポーネントには、次のハイアベイラビリティ オプションがあります。

- 冗長電源および手元のスペア
- ハイアベイラビリティのための別個のコンポーネント
- 相互作用の問題が少ない専用コンポーネント

**例 1 :** 別個の PSTN ゲートウェイおよび VoiceXML ゲートウェイ

PSTN ゲートウェイおよび別個の VoiceXML ゲートウェイによって、PSTN と VoiceXML が結合されたゲートウェイよりも高いアベイラビリティが実現されます。

**例 2 :** ハイアベイラビリティのためのコンポーネントの複製

- 8-T1 PSTN ゲートウェイが 2 つあると、16-T1 PSTN ゲートウェイ 1 つよりも高いアベイラビリティが実現されます。
- 96 ポート Unified CVP VXML Server が 2 つあると、192 ポート Unified CVP VXML Server 1 つよりも高いアベイラビリティが実現されます。
- 大規模な設計では、ハイアベイラビリティのために N+1 のスペアを使用できます。

**例 3 :** ハイアベイラビリティのための地理的な冗長性

地理的な冗長性およびハイアベイラビリティは、サイド A とサイド B で同じハードウェアを購入することにより実現できます。

## コンテンツ サービス スイッチ (CSS)

VoiceXML ゲートウェイは、CSS への要求を作成する Unified CVP システムにある、唯一のボックスです。VoiceXML ゲートウェイでメディア (ASR/TTS または VoiceXML) への要求を作成する必要がある場合、このコンフィギュレーションを確認して、要求を作成する場所を決定します。CSS を使用している場合、VoiceXML ゲートウェイで設定された IP アドレスは、CSS で設定されたサービスを指す仮想 IP アドレスです。VoiceXML ゲートウェイ クライアントが CSS から要求できるサービスのタイプは 3 つあります。

- メディア サーバ
- ASR/TTS
- Unified CVP VXML Server

これらの要求を実行するプライマリ CSS に障害が発生した場合、クライアント VoiceXML ゲートウェイは、メディアおよび VoiceXML をサーバから引き続き取得する必要があります。



**(注)** CSS を使用して、ハートビートを介して使用可能な VXML Server を検索し、ロード バランシングを実行することを推奨します。VoiceXML ゲートウェイと VXML Server の間の後続の要求および応答は、CSS をバイパスする必要があります。



**(注)** VXML Server には、ロード バランシングを支援する次の 2 つの機能があります。

- ロード バランサの関与の制限
- ロード バランサ用の拡張 HTTP プロープ

[http://www.cisco.com/en/US/products/sw/custcosw/ps1006/products\\_user\\_guide\\_list.html](http://www.cisco.com/en/US/products/sw/custcosw/ps1006/products_user_guide_list.html) から入手可能な『*User Guide for Unified CVP VXML Server and Cisco Unified Call Studio*』のコンフィギュレーション オプション `ip_redirect` および `license_depletion_probe_error` を参照してください。

## 設定

次の URL から入手可能な最新バージョンの『*Configuration and Administration Guide for Cisco Unified Customer Voice Portal (CVP)*』の説明に従って、Virtual IP (VIP; 仮想 IP) 冗長性の方法を使用して CSS のハイアベイラビリティを設定できます。

[http://www.cisco.com/en/US/products/sw/custcosw/ps1006/products\\_installation\\_and\\_configuration\\_guides\\_list.html](http://www.cisco.com/en/US/products/sw/custcosw/ps1006/products_installation_and_configuration_guides_list.html)

次の URL から入手可能な最新バージョンの『CSS Redundancy Configuration Guide』も参照してください。

[http://www.cisco.com/en/US/products/hw/contnetw/ps792/products\\_installation\\_and\\_configuration\\_guides\\_list.html](http://www.cisco.com/en/US/products/hw/contnetw/ps792/products_installation_and_configuration_guides_list.html)

本質的に、CSS のマスターとバックアップのペアは、HSRP ゲートキーパーのペアとほぼ同じように機能します。このペアは、同じ VLAN にあり、HSRP と非常によく似たプロトコルである Virtual Router Redundancy Protocol (VRRP; 仮想ルータ冗長プロトコル) を使用して、ハートビートを交換します。プライマリ CSS に障害が発生した場合、バックアップ CSS は、3 秒以内に障害を認識し、設定された仮想 IP アドレスへのクライアント要求の処理を開始します。マスター CSS とバックアップ CSS のコンフィギュレーションは、常に同期が取られている必要があります。

## コール処理

マスター CSS に障害が発生した場合、次の状態がコール処理に適用されます。

- 進行中のコールには、VoiceXML ゲートウェイ クライアントが要求したサービスのタイプに応じて、さまざまな動作が発生します。
  - メディア サーバ要求には、影響ありません。  
VoiceXML ゲートウェイの、音声ファイルの CSS を使用した相互作用は非常に短いです。ゲートウェイからメディア サーバ要求を受信するとき、CSS は、VoiceXML ゲートウェイに HTTP リダイレクト IP アドレスを与えるだけです。この時点で、ゲートウェイは、メディア サーバから音声ファイルを直接フェッチし、CSS とのさらなる相互作用をバイパスします。また、VoiceXML ゲートウェイは、以前に取得したメディア ファイルをキャッシュするため、CSS へのメディア ファイル要求の頻度は非常に低いです。
  - Unified CVP IVR サービス要求には、影響ありません。  
Unified CVP IVR サービスへの最初の VoiceXML ドキュメント要求だけが CSS を使用します。CSS は、要求を実行するために、まず Unified CVP IVR サービスを選択します。最初のドキュメントは、VoiceXML ゲートウェイに戻るときに CSS を通過します。ただし、後続の VoiceXML 要求は、VoiceXML ゲートウェイ クライアントから Unified CVP IVR サービスに直接行われます。最初の VoiceXML ドキュメントが戻される、非常に短い時間に CSS に障害が発生した場合、VoiceXML ゲートウェイは、単に要求を再実行します。バックアップ (現在のプライマリ) CSS が前回と同じ Unified CVP IVR サービスを選択した場合、重複コールインスタンスのためにエラーになります。この場合、発信者は、発信元ゲートウェイの存続可能性によってデフォルトのルートにルーティングされます。
  - ASR/TTS 要求は、通常障害が発生しますが、回復できる場合があります。  
VoiceXML ゲートウェイが CSS に対して ASR/TTS 要求を初めて行うとき、TCP 接続が VoiceXML ゲートウェイから Media Resource Control Protocol (MRCP) サーバに開かれます。この TCP 接続は、CSS に到達し、発信者が接続解除するか、エージェントに転送されるまで維持されます。プライマリ CSS に障害が発生すると、TCP 接続は切断されます。VoiceXML ゲートウェイによってエラー コードが返されます。これに回避するためのスクリプトを書き込めます。最悪のシナリオは、発信者が発信元のゲートウェイの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ることです。
  - Unified CVP VXML Server 要求は、障害が発生する場合があります。  
VoiceXML ゲートウェイは、VoiceXML セッションの間、特定の Unified CVP VXML Server に対して「スティッキー」になります。このゲートウェイは、CSS クッキーを使用して、このスティッキー性を実現します。

アクティブとバックアップの VIP 冗長および仮想インターフェイス冗長環境で CSS ピアに対して Adaptive Session Redundancy (ASR) を設定すると、ほとんどの既存のコールのステータスフェールオーバーが実現します。ASR は、マスター CSS に障害が発生した場合、バックアップ CSS が、マスターの役割を引き継ぐときに中断せずに、ほとんどのアクティブ コールを継続するために必要なフローステート情報を持つことを保証します。

既存のコールを継続できない、まれな場合には、VoiceXML ゲートウェイによってエラーコードが返されます。これに回避するためのスクリプトを書き込みます。最悪のシナリオは、発信者が発信元のゲートウェイの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ることです。

CSS の Adaptive Session Redundancy (ASR) 機能を使用すると、ポート ライセンスが VXML Server で一時的に不必要に使用できなくなることはありません。VXML Server はステータスフェールで、ASR 機能は、CSS フェールオーバー中に VXML Server ライセンス ポート使用率を最小化します。

新しいコールは、ユーザには意識されずにバックアップ CSS の VIP に転送され、サービスには影響ありません。

## メディアサーバ

音声ファイルは、VoiceXML ゲートウェイまたは HTTP/TFTP ファイルサーバ上のフラッシュ メモリにローカルに保存できます。定義上、音声ファイルをローカルに保存する方法は可用性が非常に高くなります。ただし、HTTP/TFTP ファイルサーバには、音声ファイルの集中管理という利点があります。

## Unified CVP マイクロアプリケーション使用時のコンフィギュレーション

VoiceXML ゲートウェイは、HTTP 要求を HTTP メディアサーバに送信し、音声ファイルを取得します。このゲートウェイは、CSS を使用しない場合、次の VoiceXML ゲートウェイ コンフィギュレーションパラメータを使用して、サーバを検索します。

```
ip host mediaserver <ip-address-of-primary-media-server>
ip host mediaserver-backup <ip-address-of-secondary-media-server>
```

バックアップサーバは、プライマリサーバにアクセスできない場合だけ呼び出されます。これは、ロードバランシングメカニズムではありません。新しい各コールは、プライマリサーバに接続しようとし、フェールオーバーが発生すると、バックアップサーバがコールの間使用されます。次の新しいコールは、プライマリサーバに接続しようとし、

*mediaserver* は固定された名前ではなく、ICM スクリプトで *media\_server* ECC 変数に割り当てられた名前と一致する必要があります。

VoiceXML ゲートウェイも、CSS を使用するとき、次の VoiceXML ゲートウェイ コンフィギュレーションパラメータを使用して、サーバを検索します。

```
ip host mediaserver <ip-address-of-CSS-VIP-for-media-server>
ip host mediaserver-backup <ip-address-of-CSS-VIP-for-media-server>
```

CSS は、最初の要求に関して、ほとんどの場合メディアサーバを検索するため、バックアップサーバが呼び出されることはほとんどありません。ただし、複数のデータセンターそれぞれに CSS がある場合の展開に CSS を使用する場合、バックアップサーバを設定すると便利です。

## Unified CVP マイクロアプリケーション使用時のコール処理

メディア サーバに障害が発生した場合、次の状態がコール処理に適用されます。

- 進行中のコールは、自動的に回復されます。上記で説明したハイアベイラビリティ コンフィギュレーション技術により、障害が発信者には分からないようにする必要があります。メディア要求に障害が発生した場合、スクリプティング技術を使用してエラーを回避します（要求の再試行、エージェントまたはラベルへの転送、TTS の使用など）。
- 新しいコールは、ユーザには意識されずにバックアップ メディア サーバに転送され、サービスには影響ありません。
- メディア サーバが VoiceXML ゲートウェイから WAN を超えて展開されていて、WAN 接続に障害が発生した場合、ゲートウェイは、要求されたプロンプトが期限切れになるまで、ゲートウェイ キャッシュからのプロンプトの使用を続けます。要求されたプロンプトが期限切れになると、ゲートウェイは、メディアの再フェッチを試行し、存続可能性がイネーブルになっていない場合、コールは失敗します。存続可能性がイネーブルになっている場合、コールはデフォルトのルートにルーティングされます。

## Cisco Unified Call Studio スクリプティング使用時のコンフィギュレーション

Cisco Unified Call Studio でスクリプティングしている場合は、ICM スクリプティングとは異なり、メディア ファイルの「バックアップ」の概念はありません。スクリプトを書き込んでいるユーザができる最良の方法は、アプリケーションで、[Properties] -> [AudioSettings] -> [Default Audio Path URI] を単一のメディア サーバまたはメディア サーバのファームの CSS VIP アドレスにすることです。

## Unified CVP VXML Server

VoiceXML ゲートウェイは、Unified CVP VXML Server に対する HTTP 要求を作成し、VoiceXML ドキュメントを取得します。

### 設定

Unified CVP VXML Server のハイアベイラビリティ コンフィギュレーションおよび動作は、次の各項で説明するように、スタンドアロン展開と ICM と統合展開で異なります。

### スタンドアロン セルフサービス展開

プライマリとバックアップの Unified CVP VXML Server の設定方法については、[http://www.cisco.com/en/US/products/sw/custcosw/ps1006/products\\_installation\\_and\\_configuration\\_guides\\_list.html](http://www.cisco.com/en/US/products/sw/custcosw/ps1006/products_installation_and_configuration_guides_list.html) から入手可能な最新バージョンの『Cisco Unified CVP Configuration and Administration Guide』を参照してください。

特に、Unified CVP VXML Server のハイアベイラビリティ特性を制御するのは、CVPPrimaryVXMLServer ゲートウェイ パラメータおよび CVPBackupVXMLServer ゲートウェイ パラメータです。Unified CVP VXML Server のロード バランシング機能およびさらの強固なフェールオーバー機能が必要な場合、CSS または ACE デバイスを使用できます（設定の詳細については、最新バージョンの『Cisco Unified CVP Configuration and Administration Guide』を参照してください）。

ロード バランシングは、CSS または ACE デバイス使用しなくても、複数のゲートウェイでプライマリおよびバックアップの Unified CVP VXML Server コンフィギュレーションを変えることにより実現できます。

## ICM を使用した展開

Unified CVP VXML Server を ICM とともに使用する場合、ICM スクリプトは、VoiceXML アプリケーションを呼び出すために、VoiceXML ゲートウェイに URL を渡します。Unified CVP VXML Server A への接続を初めて試行するように ICM スクリプトを設定できます。アプリケーションが Unified CVP VXML Server の ICM スクリプト ノードの X-path で障害が発生すると、Unified CVP VXML Server B への接続が試行されます。URL の IP アドレスは、CSS の Unified CVP VXML Server VIP を表すこともできます。

## コール処理

Unified CVP VXML Server に障害が発生すると、次の状態がコール処理に適用されます。

- スタンドアロン展開の進行中のコールは、接続解除されます。ICM 統合展開の進行中のコールは、上記のスクリプトで示したようにスクリプティング技術を使用して回復し、エラーを回避できません (要求の再試行、エージェントまたはラベルへの転送、END スクリプト ノードを使用して強制的にエラーにし、発信元ゲートウェイの存続可能性を呼び出すなど)。
- 新しいコールは、ユーザには意識されずに代替 Unified CVP VXML Server に転送されます。



(注) CSS または ACE デバイスがない場合、発信者は、コールの最初で遅延が発生し、プライマリ Unified CVP VXML Server への接続を試行しながら、システムがタイムアウトになるのを待つ必要がある場合があります。

## 自動音声認識 (ASR) および音声合成 (TTS) サーバ

VoiceXML ゲートウェイは、VoiceXML ドキュメントで定義されている音声認識および音声合成の指示を実行するために、MRCP 要求を ASR/TTS サーバに送信します。

## 設定

ASR/TTS ハイアベイラビリティのコンフィギュレーションおよび動作は、次の各項で説明するように、スタンドアロン展開と ICM 統合展開で異なります。

### スタンドアロンセルフサービス展開

スタンドアロン展開で、ASR/TTS に対してフェールオーバー機能を提供するには、CSS または ACE デバイスが必要です。ASR/TTS に対して CSS または ACE デバイスを設定する方法およびスタンドアロン展開で ASR/TTS サーバを設定する方法については、次の URL から入手可能な最新バージョンの『*Configuration and Administration Guide for Cisco Unified Customer Voice Portal (CVP)*』を参照してください。

[http://www.cisco.com/en/US/products/sw/custcosw/ps1006/products\\_installation\\_and\\_configuration\\_guides\\_list.html](http://www.cisco.com/en/US/products/sw/custcosw/ps1006/products_installation_and_configuration_guides_list.html)

## ICM を使用した展開

VoiceXML ゲートウェイは、CSS または ACE デバイスを使用している場合と使用していない場合の両方で、ゲートウェイ コンフィギュレーション パラメータを使用して、ASR/TTS サーバを検索します。バックアップ サーバは、プライマリ サーバにアクセスできない場合だけ呼び出されます。これは、ロード バランシング メカニズムではありません。新しい各コールは、プライマリ サーバに接続しようとし、フェールオーバーが発生すると、バックアップ サーバがコールの間使用されます。次の新しいコールは、プライマリ サーバに接続しようとし、

ホスト名 (**asr-en-us** など) は固定され、変更できません。変更できるのは、ロケールだけです。次の例では、プライマリとバックアップの英語の ASR/TTS サーバのセットおよびスペイン語のサーバのセットがあります。次の URL から入手可能な最新バージョンの『*Configuration and Administration Guide for Cisco Unified Customer Voice Portal (CVP)*』の指示に従って、CSS (使用する場合) を設定します。

[http://www.cisco.com/en/US/products/sw/custcosw/ps1006/products\\_installation\\_and\\_configuration\\_guides\\_list.html](http://www.cisco.com/en/US/products/sw/custcosw/ps1006/products_installation_and_configuration_guides_list.html)

CSS を使用している場合、次の例で説明する IP アドレスは、CSS 上での ASR/TTS サービスの仮想 IP アドレスです。

```
ip host asr-en-us <ip-address-of-primary-English-ASR-server>
ip host asr-en-us-backup <ip-address-of-secondary-English-ASR-server>
ip host tts-en-us <ip-address-of-primary-English-TTS-server>
ip host tts-en-us-backup <ip-address-of-secondary-English-TTS-server>
ip host asr-es-es <ip-address-of-primary-Spanish-ASR-server>
ip host asr-es-es-backup <ip-address-of-secondary-Spanish-ASR-server>
ip host tts-es-es <ip-address-of-primary-Spanish-TTS-server>
ip host tts-es-es-backup <ip-address-of-secondary-Spanish-TTS-server>
```

CVP 展開での混在コーデックの使用に関する説明については、「[G.729 および G.711 コーデックの混在サポート](#)」(P.7-9) を参照してください。各コーデックの利点および欠点の説明については、「[音声トラフィック](#)」(P.9-2) を参照してください。



(注)

ASR スピーチ ライセンスは、発信者がエージェントに転送されるまでリリースされません。

## コール処理

ASR/TTS MRCP サーバに障害が発生すると、次の状態がコール処理に適用されます。

- スタンドアロン展開の進行中のコールは、接続解除されます。ICM 統合展開の進行中のコールは、スクリプティング技術を使用して回復し、エラーを回避できます (要求の再試行、エージェントまたはラベルへの転送、残りのコールの事前に記録されたプロンプトおよび DTMF のみの入力への切り替え、END スクリプト ノードを使用して強制的にエラーにし、発信元ゲートウェイの存続可能性を呼び出すなど)。
- CSS を使用している場合、スタンドアロン展開または ICM 統合展開の新しいコールは、ユーザには意識されずに代替 ASR/TTS サーバに転送されます。「-backup」というゲートウェイ ホスト名を使用していた場合、ICM 統合展開の新しいコールは、ユーザには意識されずに代替 ASR/TTS サーバに転送されます。

# Cisco Unified Communications Manager

Unified CVP は、H.323 または SIP を使用して、発信者を Cisco Unified Contact Center Enterprise (Unified CCE) エージェント電話またはデスクトップに転送します。Unified CVP コール サーバ (以降、コール サーバとといいます) は、ICM からエージェント ラベルを受信し、ゲートキーパーまたは SIP プロキシを使用してコールをルーティングします。コールは、クラスタ内の適切な Cisco Unified Communications Manager (Unified CM) に送信され、発信者をエージェントに接続します。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。このことは、ハイアベイラビリティの説明において非常に重要です。

Unified CVP バージョン 8.0(1) は、Analysis Manager もサポートします。「[Analysis Manager](#)」(P.13-8) を参照してください。

## 設定

Unified CM でのハイアベイラビリティの実現に関する最新情報については、[http://www.cisco.com/en/US/products/sw/custcosw/ps1844/products\\_implementation\\_design\\_guides\\_list.html](http://www.cisco.com/en/US/products/sw/custcosw/ps1844/products_implementation_design_guides_list.html) から入手可能な最新バージョンの『*Cisco Unified Contact Center Enterprise Solution Reference Network Design (SRND)*』を参照してください。

## コール処理

コールをホストしているまたは電話をホストしているサーバで Unified CM プロセスに障害が発生した場合、次の状態がコール処理に適用されます。

- 進行中のコールは保持されます。 Skinny Client Control Protocol (SCCP) 電話には、Unified CM を失ったことを検出したときでも、コールを保持する機能があります。発信者とエージェントの会話は、発信者またはエージェントのいずれかが電話を切るまで継続されます。Unified CVP コール サーバは、Unified CM に障害が発生したことを認識し、コールを保持する必要があると推測し、発信元ゲートウェイへのシグナリング チャネルを維持します。こうすることにより、発信元ゲートウェイは、Unified CM に障害が発生したことを認識しません。コールで追加操作 (保留、転送、会議など) は、できないことに注意してください。いったん電話が切られると、この電話は別の Unified CM サーバに接続されるようになります。エージェントが電話を切ると、Real-Time Control Protocol (RTCP) パケットが発信元ゲートウェイへの送信を停止します。この結果、ゲートウェイは、エージェントが電話を切った 9 ~ 18 秒後に接続解除されます。ゲートウェイで存続可能性が設定されていて、発信者が追加の操作を待っている場合 (エージェントは、発信者が別の宛先にブラインド転送されていると考える場合があります)、発信者は別の場所のデフォルトのルートにルーティングされます。
- 新しいコールは、クラスタ内の代替 Unified CM サーバに転送されます。

# Intelligent Contact Management (ICM)

Cisco Intelligent Contact Management (ICM) ソフトウェアは、地理的に分散したコンタクトセンター間でマルチチャネル コンタクト（電話による着信および発信コール、Web 共同要求、電子メール メッセージ、およびチャット要求）を企業全体に分散させます。ICM ソフトウェアは、ルーティング、キューイング、モニタリング、耐障害性等の機能を持つオープン標準ベースのソリューションです。

## 設定

ハイアベイラビリティを実現するための ICM の設定に関する最新情報については、次の URL から入手可能な最新バージョンの『Cisco Unified Contact Center Enterprise Solution Reference Network Design (SRND)』を参照してください。

[http://www.cisco.com/en/US/products/sw/custcosw/ps1844/products\\_implementation\\_design\\_guides\\_list.html](http://www.cisco.com/en/US/products/sw/custcosw/ps1844/products_implementation_design_guides_list.html)

## コール処理

Cisco ICM には多くのコンポーネントがあり、コール処理は障害が発生したコンポーネントによって異なります。いくつかの例外はありますが、次の状態がコール処理に適用されます。

- Voice Response Unit (VRU; 音声応答装置) Peripheral Gateway (PG; ペリフェラル ゲートウェイ) または VRU PG 上のコンポーネントに障害が発生した場合、進行中のコールは、発信元ゲートウェイの存続可能性によってデフォルトのルートにルーティングされます。
- Logger に障害が発生した場合、進行中のコールには影響ありません。
- プライマリ ルータに障害が発生した場合、進行中のコールには影響ありません。サイド A とサイド B のルータ両方に障害が発生した場合、進行中のコールは、発信元ゲートウェイの存続可能性によってデフォルトのルートにルーティングされます。
- 新しいコールは、バックアップの ICM コンポーネントに転送されます。

