Cisco Single VCS Control - 基本設定

導入ガイド

初版：2009 年 9 月

最終更新日：2015 年 11 月

Cisco VCS X8.7

はじめに

Cisco TelePresence Video Communication Server（VCS）ソフトウェアは、テレプレゼンス会議のセッション管理と制御を簡素化します。柔軟で拡張性に優れた会議アプリケーションを備えているため、従業員の生産性向上や、パートナーおよびお客様とのコミュニケーションの強化が図れます。

VCS は、Cisco TelePresence Management Suite（Cisco TMS）と連携し、優れた拡張性と復元力、安全なコミュニケーション、簡素化された大規模プロビジョニングおよびネットワーク管理を実現します。

VCS は、Cisco Unified Communications Manager（Unified CM）と透過的に連動して機能豊富な TelePresence サービスを提供します。また、サードパーティ製のユニファイド コミュニケーション、IP テレフォニー ネットワーク、VoIP（Voice-over-IP）システムとの相互運用も可能です。

このマニュアルでは、単一の VCS Control プラットフォームを設定し、基本的なビデオ インフラストラクチャ環境で使用する方法について説明（Description）します。導入環境に VCS Expressway が含まれる場合は、このマニュアルではなく、 *『Basic Configuration (Control with Expressway) Deployment Guide』*を使用してください。

詳細なリファレンス情報は、このマニュアルの付録に含まれています。

- 「付録 1：設定の詳細」（23 ページ）に、このマニュアルで使用される VCS 設定の詳細を示します。
- 「付録 2：DNS レコード」（26 ページ）では、この導入例に必要な DNS レコードについて説明（Description）します。

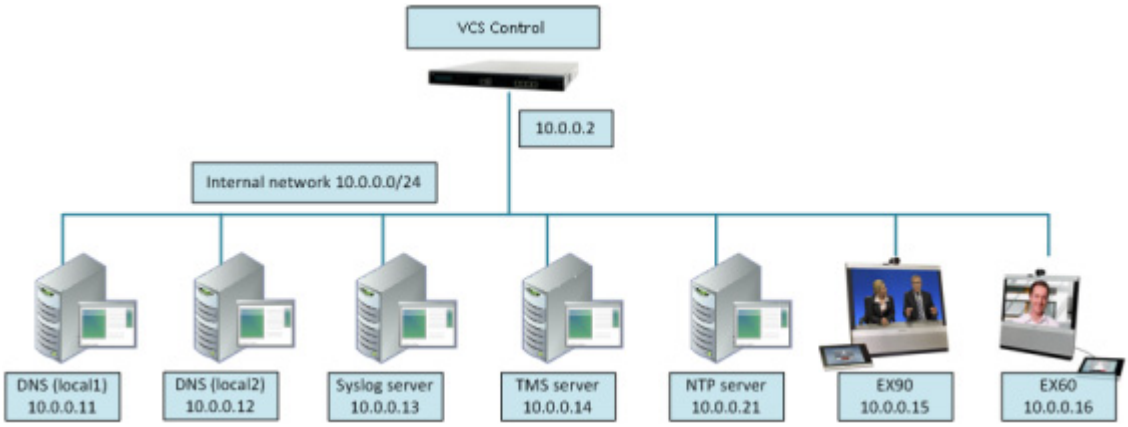
システム設定パラメータの説明（Description）については、 *『VCS Administrator Guide』*、VCS Web アプリケーションのオンライン フィールド ヘルプ およびページ ヘルプ を参照してください。

このマニュアルでは、VCS のクラスタ、あるいはデバイス プロビジョニング、デバイス認証、または FindMe アプリケーションを実行しているシステムの導入方法の詳細については説明（Description）していません。これらの機能の詳細については、次のマニュアルを参照してください。

- *VCS クラスタの作成およびメンテナンス導入ガイド*
- *Cisco TMS Provisioning Extension Deployment Guide*
- *FindMe Express Deployment Guide*
- *Device Authentication on VCS Deployment Guide*

ネットワーク導入例

図 1：このマニュアルで説明（Description）されている導入のネットワーク例



ネットワーク要素

内部ネットワーク要素

内部ネットワーク要素は、組織のローカル エリア ネットワーク上でホスティングされるデバイスです。

内部ネットワーク上の要素は、内部ネットワークのドメイン名を持ちます。この内部ネットワーク ドメイン名を、パブリック DNS が解決することはできません。たとえば、VCS Control には vcsc.internal-domain.net の内部的に解決可能な名前が設定されます（内部 DNS サーバによって IP アドレス 10.0.0.2 に解決されます）。

VCS Control

VCS Control は、SIP レジストラおよびプロキシであり、内部ネットワーク上に存在するデバイスの H.323 ゲートキーパーです。

EX90 および EX60

これらは、VCS Control に登録される内部ネットワーク上でホスティングされるエンドポイントです。

DNS（local 1 および local 2）

VCS Control が使用する DNS サーバで、DNS ルックアップを実行します（内部ネットワーク上のネットワーク名を解決します）。

DHCP サーバ（DHCP Server）

DHCP サーバは、内部ネットワーク上に存在するエンドポイントへのホスト、IP ゲートウェイ、DNS サーバ、および NTP サーバのアドレスを提供します。

Cisco TMS サーバ

管理およびスケジューリング サーバ（UNRESOLVED CROSS-REFERENCE Cisco TMS の設定（任意）（17 ページ）を参照してください）。

Syslog サーバ

Syslog メッセージのロギング サーバ（ステップ 10：ロギングの設定（任意）（19 ページ）を参照してください）。

NTP サーバ

デバイスの同期に使用されるクロック ソースを提供する NTP サーバ。

SIP および H.323 ドメイン

配置例では、ドメイン example.com を使用する URI に対して発信されるコールの SIP（および H.323）シグナリング メッセージをルーティングするように設定されています。

DNS SRV の設定は、「付録 2：DNS レコード（26 ページ）」に記載されています。

前提条件およびプロセスの概要

前提条件

システム設定を開始する前に、次のものにアクセスできることを確認してください。

- 『*VCS Administrator Guide*』および 『*VCS Getting Started Guide*』（参照用）。
- VCS システム。
- イーサネット経由で LAN に接続されている PC で、HTTP（S）を VCS にルーティング可能なもの。
- PC 上で実行されている Web ブラウザ。
- PC およびケーブルのシリアル インターフェイス（初期設定をシリアル インターフェイスを介して実行する場合）

プロセスの概要

設定のプロセスは、次の手順で構成されています。

VCS システムの設定：

- 未解決の相互初期設定（5 ページ）
- ステップ 2：システム名の設定（6 ページ）
- ステップ 3：DNS の設定（7 ページ）

[%=call_control.VCSShort%] システム設定

ステップ 1：初期設定の実行

VCS が工場出荷時の状態の場合、『*VCS Getting Started Guide*』に記載されている初期設定の手順に従って基本ネットワークパラメータを設定します。

- LAN1 IP（IPv4 または IPv6）アドレス
- サブネット マスク（IPv4 を使用している場合）
- デフォルトのゲートウェイ IP アドレス（IPv4 または IPv6）

VCS はスタティック IP アドレスが必要です（DHCP サーバから IP アドレスを取得しません）。

初期設定は、次の 3 つの方法のいずれかで実行できます。

- シリアル ケーブルを使用
- VCS アプライアンスの前面パネル経由
- デフォルト IP アドレス 192.168.0.100 経由

詳細については、『*VCS Getting Started Guide*』の「Initial configuration」の項を参照してください。

この展開ガイドは、Web インターフェイスを使用した設定に基づいています。初期設定（IP アドレスの割り当て）完了後に Web インターフェイスを使用して VCS にアクセスできない場合は、ネットワーク管理者にお問い合わせください。

配置例では、次の設定値が使用されています。

LAN1 IPv4 アドレス（LAN1 IPv4 address）	10.0.0.2
IPv4 ゲートウェイ（IPv4 gateway）	10.0.0.1
LAN1 サブネット マスク（LAN1 subnet mask）	255.255.255.0

ステップ 2：システム名の設定

[システム名（System name）] で VCS の名前を定義します。

[システム名（System name）] は、Web インターフェイスのさまざまな場所、および（他のシステムと同じラック内にある場合でも識別することができるように）アプライアンスの前面パネルに表示されます。システム名は、Cisco TMS でも使用されます。

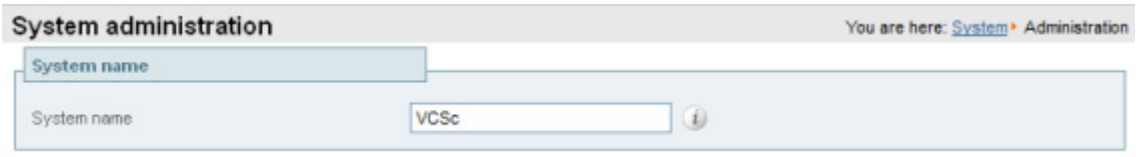
容易かつ一意に識別できる名前を VCS に付けることを推奨します。システム名が 16 文字よりも長い場合、最後の 16 文字が前面パネルに表示されます。

[システム名（System name）] を設定するには、次の手順を実行します。

1. [システム（System）] > [管理（Administration）] に移動します。
2. 次のように [システム名（System name）] を設定します。

システム名（System name）	VCSc と入力します。

3. [保存（Save）] をクリックします。



ステップ 3：DNS の設定

システム ホスト名（System Host Name）

[システム ホスト名（System host name）] で、このシステムを認識する DNS ホスト名を定義します。これは完全修飾ドメイン名ではなく、単にホストのラベル部分であることに注意してください。

<System host name>.<Domain name> = この VCS の FQDN であることに注意してください。

[システム ホスト名（System host name）] を設定するには、次の手順を実行します。

1. [システム（System）] > [DNS] に移動します。
2. 次のように [システム ホスト名（System host name）] を設定します。

システム ホスト名（System host name）	`vcsc` と入力します。

3. [保存（Save）] をクリックします。

ドメイン名（Domain Name）

[ドメイン名（Domain name）] は、DNS サーバを照会する前に非修飾ホスト名に追加される名前です。

[ドメイン名（Domain name）] を設定するには、次の手順を実行します。

1. [システム（System）] > [DNS] に移動します。
2. 次のように [ドメイン名（Domain name）] を設定します。

ドメイン名（Domain Name）	`internal-domain.net` と入力します。

3. [保存（Save）] をクリックします。

DNS サーバ

DNS サーバ アドレスは、ドメイン名の解決時に使用する最大 5 つのドメイン ネーム サーバの IP アドレスです。次のいずれかの場合、アドレス解決のためにクエリーするデフォルトの DNS サーバを少なくとも 1 つ指定する必要があります。

- 外部アドレスの指定時に、IP アドレスではなく FQDN（完全修飾ドメイン名）を使用する（たとえば、LDAP および NTP サーバの場合、ネイバー ゾーンおよびピア）
- URI ダイヤリングまたは ENUM ダイヤリングなどの機能を使用する

VCS は同時に 1 つのサーバのクエリーのみを行います。そのサーバが使用できない場合、VCS はリストから他のサーバを試行します。

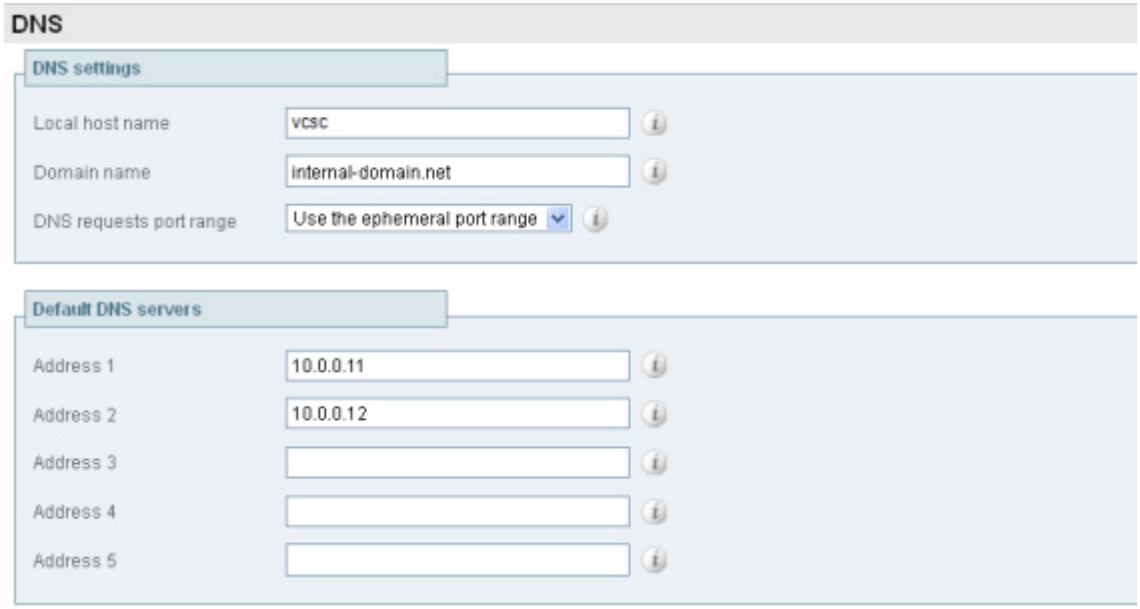
配置例では、2 つの DNS サーバが各 VCS に設定されており、これらは一定レベルの DNS サーバの冗長性を提供しています。VCS Control は、内部ネットワーク上に存在する DNS サーバで設定されます。

[デフォルト DNS サーバ（Default DNS server）] のアドレスを設定するには、次の手順を実行します。

1. [システム（System）] > [DNS] に移動します。
2. 次のように DNS サーバの [アドレス（Address）] フィールドを設定します。

アドレス 1（Address 1）	`10.0.0.11` と入力します。
アドレス 2（Address 2）	`10.0.0.12` と入力します。

3. [保存（Save）] をクリックします。



ステップ 4：デフォルトのサーバ証明書の置換

セキュリティを強化するために、VCS は他のシステム（LDAP サーバやネイバー ゾーンの VCS、または SIP エンドポイントや Web ブラウザのようなクライアント）と TLS 暗号化を使用して通信することもできます。

クライアントとサーバ間の接続でこれを正常に機能させるためには以下が必要です。

- サーバにはそのアイデンティティを検証するためのインストールされた証明書が必要です。この証明書は、認証局（CA）によって署名されている必要があります。

- クライアントはサーバが使用する証明書に署名した CA を信頼する必要があります。

VCS では TLS を使用した接続で、クライアントまたはサーバとして機能できるよう、適切なファイルをインストールすることができます。VCS は、HTTPS 経由のクライアント接続（通常は Web ブラウザから）を認証することもできます。また、LDAP サーバおよび HTTPS クライアント証明書の検証に使用される CA の証明書失効リスト（CRL）をアップロードすることもできます。

VCS はサーバ証明書の署名要求（CSR）を生成できます。そのため、証明書要求を生成し、取得するために外部機能を使用する必要はありません。

セキュアな通信（HTTPS および SIP/TLS）のために、VCS のデフォルトの証明書を、信頼できる CA が生成した証明書に置き換えることを推奨します。

接続では以下に注意してください。

- エンドポイントに対して、VCS は TLS サーバとして機能します。
- LDAP サーバに対しては、VCS はクライアントです。
- 2 つの VCS システム間では、いずれかの VCS がクライアントになり、もう一方の VCS が TLS サーバになることができます。
- HTTPS 経由では、Web ブラウザはクライアントであり、VCS はサーバです。

TLS は設定が難しい場合があります。たとえば、LDAP サーバとともに TLS を使用する際、TLS でのセキュアな接続を行う前に、システムが正しく動作していることを確認することを推奨します。また、TLS を使用するように LDAP サーバが正しく設定されていることを検証するためにサードパーティの LDAP ブラウザを使用することが推奨されます。

注：CA 証明書または CRL が期限切れにならないように注意してください。これらの CA によって署名された証明書が拒否される要因となる可能性があるためです。

信頼できる CA のリストをロードするには、[メンテナンス（Maintenance）] > [セキュリティ証明書（Security certificates）] > [信頼できる CA 証明書（Trusted CA certificate）] に移動します。

CSR を生成するか、VCS のサーバ証明書をアップロードするには（またはその両方を行うには）、[メンテナンス（Maintenance）] > [セキュリティ証明書（Security certificates）] > [サーバ証明書（Server certificate）] に移動します。

詳細については、 *『VCS Certificate Creation and Use Deployment Guide』* を参照してください。

ステップ 5：NTP サーバの設定

[NTP サーバ（NTP server）] アドレス フィールドは、システム時刻の同期に使用される NTP サーバの完全修飾ドメイン名（FQDN）の IP アドレスを設定します。

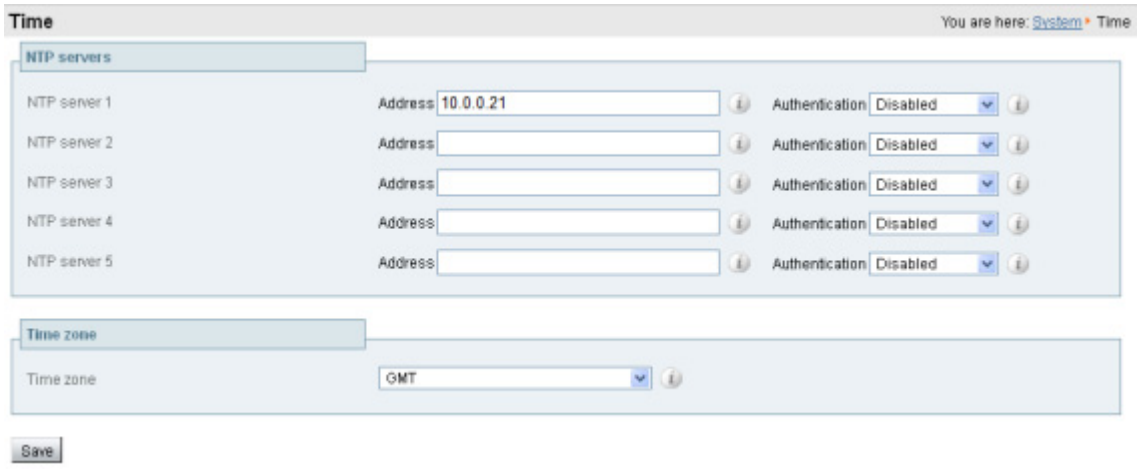
[タイム ゾーン（Time zone）] で、VCS のローカル タイム ゾーンを設定します。

NTP サーバのアドレスおよびタイム ゾーンを設定するには、次の手順を実行します。

1. [システム（System）] > [時間（Time）] に移動します。
2. フィールドを次のように設定します。

NTP サーバ 1（NTP server 1）	`10.0.0.21` と入力します。
タイム ゾーン（Time zone）	この例では *GMT* を選択します。

3. [保存（Save）] をクリックします。



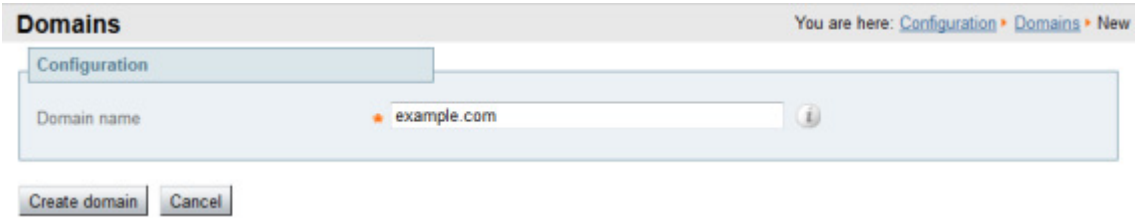
ステップ 6：SIP ドメインの設定

VCS は設定済みの SIP ドメインの SIP レジストラとして動作し、これらのドメインを含むエイリアスで登録を試行する SIP エンドポイントの登録要求を受け入れます。

- 登録の制限（許可（Allow）または拒否（Deny））のルールを設定し、受け入れ可能な登録を制限することができます。ステップ 11：登録制限ポリシーの設定（任意）（20 ページ）を参照してください。
- 認証が有効な場合、適切に認証可能なデバイスのみを登録することができます。

SIP ドメインを設定するには、次の手順を実行します。

1. [設定（Configuration）] > [ドメイン（Domains）] に移動します。
2. [新規（New）] をクリックします。
3. たとえば、`example.com` などのドメイン名を [Name] フィールドに入力します。
4. [ドメインの作成（Create domain）] をクリックします。
5. [ドメイン（Domains）] ページに、設定済みのすべての SIP ドメイン名が表示されます。



ルーティング設定

事前検索トランスフォーメーション

事前検索トランスフォーメーションの設定により、着信検索要求の宛先エイリアス（着信側アドレス）を変更することができます。トランスフォーメーションは、検索が行われる前に、VCS によってローカル ゾーンまたは外部ゾーンに適用されます。

このマニュアルで説明（Description）している事前検索トランスフォーメーションの設定は、H.323 および SIP の両方のデバイスから発信する宛先エイリアスの標準化に使用されます。つまり、H.323 エンドポイントと SIP エンドポイントの両方からのコールに対して同じコール検索が動作します。

たとえば、着信側アドレスが H.323 E.164 エイリアス「01234」の場合、VCS は、コールのセットアップを試行する前に、自動的に設定されたドメイン名（この場合は example.com）を着信側アドレスに追加（つまり、01234@example.com を URI 化）します。

- 事前検索トランスフォーメーションは、すべてのシグナリング メッセージに適用されるため、注意深く使用する必要があります。一致した場合、Unified Communications メッセージ、プロビジョニング、プレゼンス要求だけでなくコール要求のルーティングに影響を与えます。
- トランスフォーメーションは、検索ルールでも行うことができます。検索するために着信側アドレスを変更するには、事前検索トランスフォーメーションまたは検索ルールのどちらの使用が最適かを検討してください。

検索ルール

検索ルールは、特定のコールのシナリオで、VCS がコールを（宛先ゾーンに）ルーティングする方法を定義します。検索ルールが一致すると、検索ルールで定義した条件に応じて宛先エイリアスを変更することができます。

このマニュアルで説明（Description）している検索ルールは、SIP（および H.323）エンドポイントが、E.164 番号または H.323 ID が登録されておりドメイン部分がない H.323 デバイスに確実にダイヤルできるようにするために使用されます。検索ルールは、まず URI のドメイン部分がない受信側の宛先エイリアスを検索し、次に URI 全体を検索します。

このマニュアルのルーティング設定は、有効な SIP URI を持つ（つまり、id@domain などの有効な SIP アドレスを使用している）宛先エイリアスを検索します。

検索ルールをターゲットのローカル ゾーンとともに [任意の IP アドレス（Any IP address）] モードで設定することにより、内部ネットワーク上の未登録のデバイスへのコールを有効にするルーティング（デバイスの IP アドレスへのルーティング）を設定

することができます。ただし、これは推奨しません（このマニュアルでは説明（Description）していません）。ベスト プラクティスは、すべてのデバイスを登録し、宛先エイリアスを使用してルーティングすることです。

ステップ 7：トランスフォーメーションの設定

このマニュアルで説明（Description）している事前検索トランスフォーメーションの設定は、H.323 および SIP の両方のデバイスから発信する宛先エイリアスの標準化に使用されます。

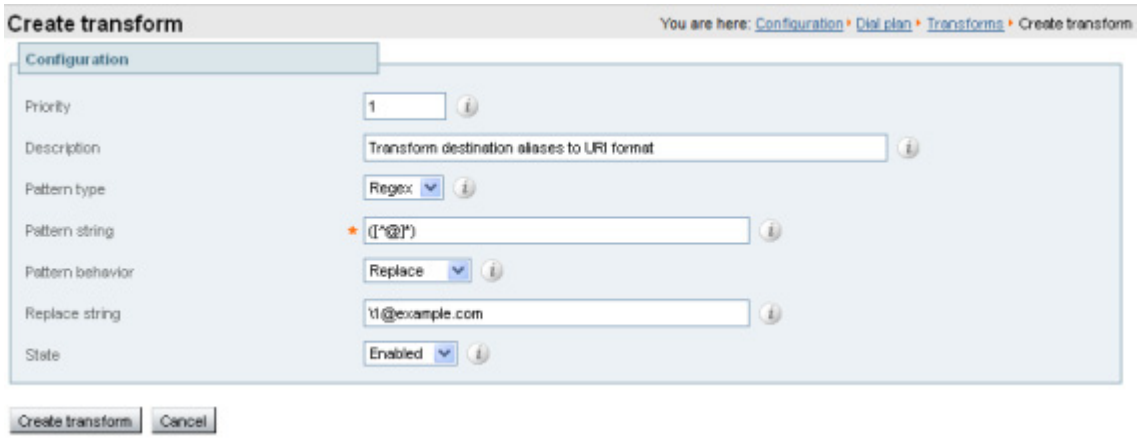
次のトランスフォーメーションは、「@」を含まない宛先エイリアスに対して行われるすべてのコールの試行の宛先エイリアスを変更します。古い宛先エイリアスには、@example.com が追加されています。これは、すべての着信先エイリアスを SIP URI 形式に標準化する効果があります。

トランスフォーメーションを設定するには、次の手順を実行します。

1. [設定（Configuration）] > [ダイヤル プラン（Dial plan）] > [トランスフォーメーション（Transforms）] に移動します。
2. [新規（New）] をクリックします。
3. 次のようにトランスフォーメーション フィールドを設定します。

プライオリティ（Priority）	`1` を入力します。
説明（Description）	`Transform destination aliases to URI format` と入力します。
パターン タイプ（Pattern type）	*Regex*
パターン文字列（Pattern string）	`([^@]*)` と入力します。
パターン動作（Pattern behavior）	*置換（Replace）*
文字列の置換（Replace string）	`\1@example.com` と入力します。
状態 （State）	*有効（Enabled）*

4. [トランスフォーメーションの作成（Create transform）] をクリックします。



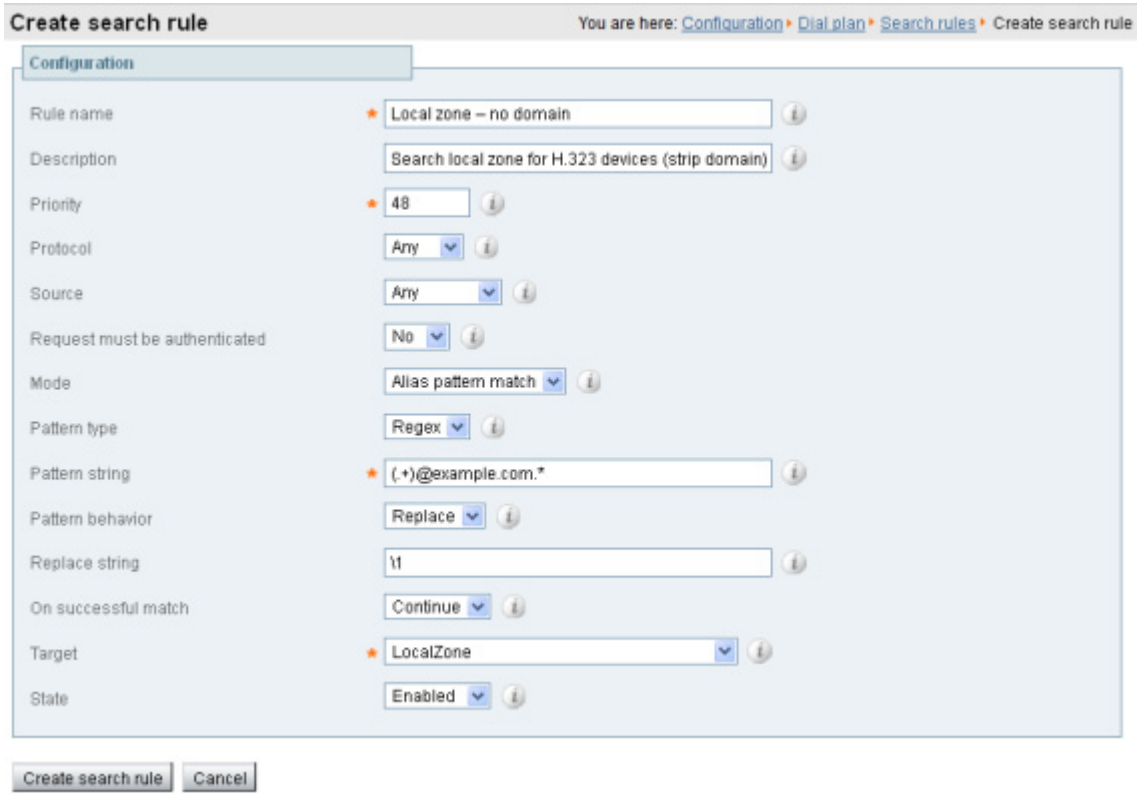
ステップ 8：ローカル ゾーン検索ルールの設定

コールをローカル ゾーン（ローカルに登録されたエンドポイント エイリアス）にルーティングする検索ルールを設定するには、次の手順を実行します。

1. [設定（Configuration）] > [ダイヤル プラン（Dial plan）] > [検索ルール（Search rules）] に移動します。
2. デフォルトの検索ルール（**LocalZoneMatch**）の横にあるチェックボックスをオンにします。
3. [削除（Delete）] をクリックします
   （デフォルトの検索ルールが削除され、より具体的な設定に置換されます）。
4. [OK] をクリックします。
5. [新規（New）] をクリックします。
6. 次のように検索ルールのフィールドを設定します。

ルール名 （Rule name）	`Local zone - no domain` と入力します。
説明（Description）	`Search local zone for H.323 devices (strip domain)` と入力します。
プライオリティ（Priority）	`48` を入力します。
プロトコル（Protocol）	*任意（Any）*
ソース（Source）	*任意（Any）*
リクエストは認証される必要がある（Request must be authenticated）	*なし（No）*
モード（Mode）	*エイリアスのパターン マッチ（Alias pattern match）*
パターン タイプ（Pattern type）	*Regex*
パターン文字列（Pattern string）	`(.+)@example.com.*` と入力します。
パターン動作（Pattern behavior）	*置換（Replace）*
文字列の置換（Replace string）	`\1` を入力します。
正常に一致する場合（On successful match）	*続行（Continue）*
ターゲット（Target）	*LocalZone*
状態 （State）	*有効（Enabled）*

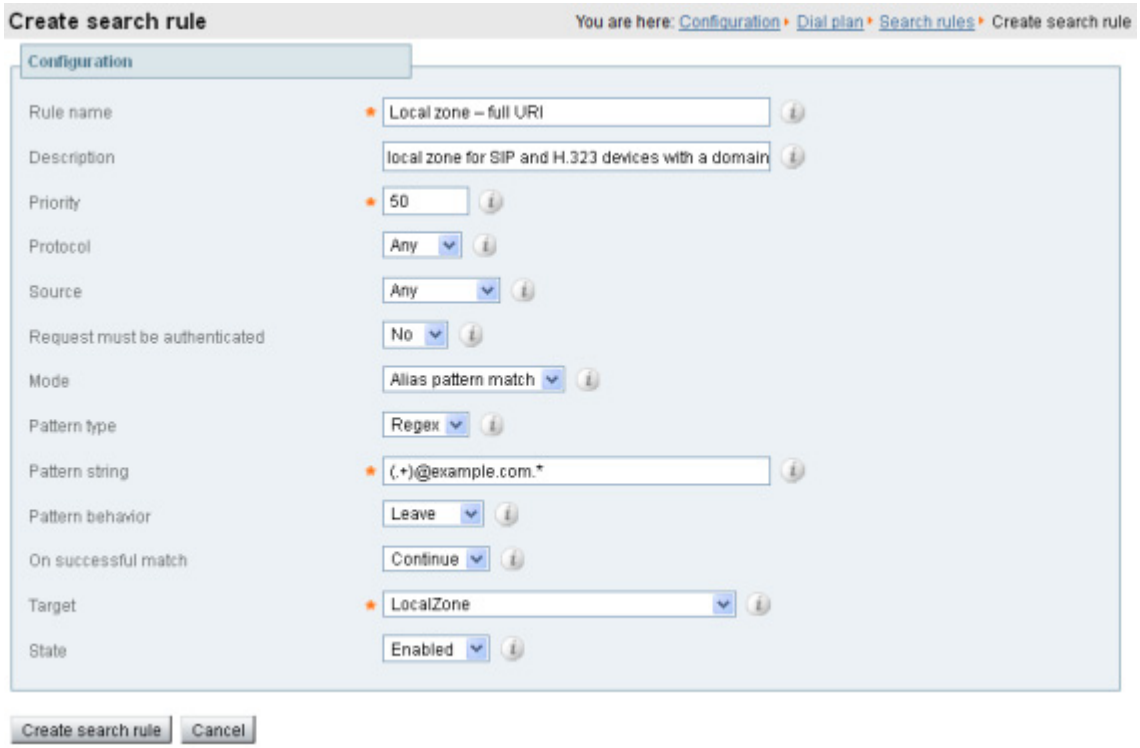
7. [検索ルールの作成（Create search rule）] をクリックします。



8. [新規（New）] をクリックします。
9. 次のように検索ルールのフィールドを設定します。

ルール名 （Rule name）	`Local zone - full URI` と入力します。
説明（Description）	`Search local zone for SIP and H.323 devices with a domain` と入力します。
プライオリティ（Priority）	`50` を入力します。
プロトコル（Protocol）	*任意（Any）*
ソース（Source）	*任意（Any）*
リクエストは認証される必要がある（Request must be authenticated）	*なし（No）*
モード（Mode）	*エイリアスのパターン マッチ（Alias pattern match）*
パターン タイプ（Pattern type）	*Regex*
パターン文字列（Pattern string）	`(.+)@example.com.*` と入力します。
パターン動作（Pattern behavior）	*変更なし（Leave）*
正常に一致する場合（On successful match）	*続行（Continue）*
ターゲット（Target）	*LocalZone*
状態 （State）	*有効（Enabled）*

10. [検索ルールの作成（Create search rule）] をクリックします。



エンドポイントの登録

ネットワーク設定の図には、2 つのエンドポイントが示されています。

エンドポイント（Endpoint）	IP アドレス	ネットワーク
EX90	10.0.0.15	内部ネットワーク
EX60	10.0.0.16	内部ネットワーク

次のシステム設定、エンドポイント登録は、次のエンドポイント設定の詳細を使用して実施する必要があります。

EX90（SIP プロトコルを使用）	
SIP URI	user.one.ex90@example.com
SIP Proxy1	vcsc.internal-domain.net
EX60（H.323 および SIP プロトコルを使用）	
H.323 ID	user.two.mxp@example.com
H.323 E.164	7654321
ゲートキーパーの IP アドレス	vcsc.internal-domain.net
SIP URI	user.two.mxp@example.com
SIP Proxy1	vcsc.internal-domain.net

システム チェック

登録ステータス（Registration Status）

登録することが想定されているすべてのエンドポイントが実際に該当する VCS に登録されており、想定されているエイリアスを登録していることを確認します。正常に登録されたすべてのエンドポイントは、[ステータス（Status ）] > [登録（Registrations）] > [デバイスごと（By device）] にリストされます。

想定されているエンドポイントが登録されていない場合は、次の手順を実行します。

- 外部ネットワーク/インターネットにある場合は VCS Expressway に登録され、内部ネットワークにある場合は VCS Control に登録されるように設定されているかについて、エンドポイントの登録設定を確認します。
- SIP ドメインを確認します（ステップ 6：SIP ドメインの設定（10 ページ））。
- VCS に適用されている登録制限の設定を確認します（ステップ 11：登録制限ポリシーの設定（任意）（20 ページ）を参照してください）。

コール シグナリング（Call Signaling）

コールが完了しない場合、エンドポイントが正常に VCS に登録されたかどうかにかかわらず、次の手順を実行します。

- VCS Control 検索ルールの設定を確認します。
- 検索の試行および失敗について検索履歴ページを確認します（[ステータス（Status）] > [検索履歴（Search history）]）。
- コール接続の失敗理由についてイベント ログを確認します（[ステータス（Status）] > [ログ（Logs）] > [イベント ログ（Event Log）]）。

日常的なメンテナンス

システム バックアップの作成

VCS システム データのバックアップを作成するには、次の手順を実行します。

1. [メンテナンス（Maintenance）] > [バックアップと復元（Backup and restore）] に移動します。
2. 任意で、バックアップ ファイルを暗号化する [暗号化パスワード（Encryption password）] を入力します。

   パスワードが指定されている場合、ファイルを復元するには同じパスワードが必要です。
3. [システム バックアップ ファイルの作成（Create system backup file）] をクリックします。

4. バックアップ ファイルが作成されると、ポップアップ ウィンドウが表示され、ファイルを保存するよう指示されます（実際の表現は、ブラウザによって異なります）。デフォルト名は、**<ソフトウェアのバージョン>_<ハードウェアのシリアル番号>_<日付>_<時刻>_backup.tar.gz** の形式です。

   （ファイル拡張子は、暗号化パスワードを指定した場合、通常は **.tar.gz.enc** です。ただし、暗号化されたバックアップ ファイルの作成に Internet Explorer を使用する場合、ファイル名の拡張子はデフォルトで **.tar.gz.gz** になります。ファイル名の拡張子がこのように異なっても運用上の影響はありません。対応しているブラウザを使用して暗号化されたバックアップ ファイルを作成し、復元できます。）

   システム バックアップ ファイルの準備が完了するまで数分かかる場合があります。ファイルが準備されている間は、このページから移動しないでください。

5. 指定された場所にファイルを保存します。

システム バックアップ ファイルには、ログ ファイルは含まれません。

任意の設定作業

ステップ 9：Cisco TMS の設定（任意）

次の設定により、VCS システムを Cisco TelePresence Management Server（Cisco TMS）に統合することができます。

VCS を完全に Cisco TMS サーバと統合するには、Cisco TMS 上でさらに設定作業が必要です。*『Cisco TMS Administrator Guide』* を参照してください。

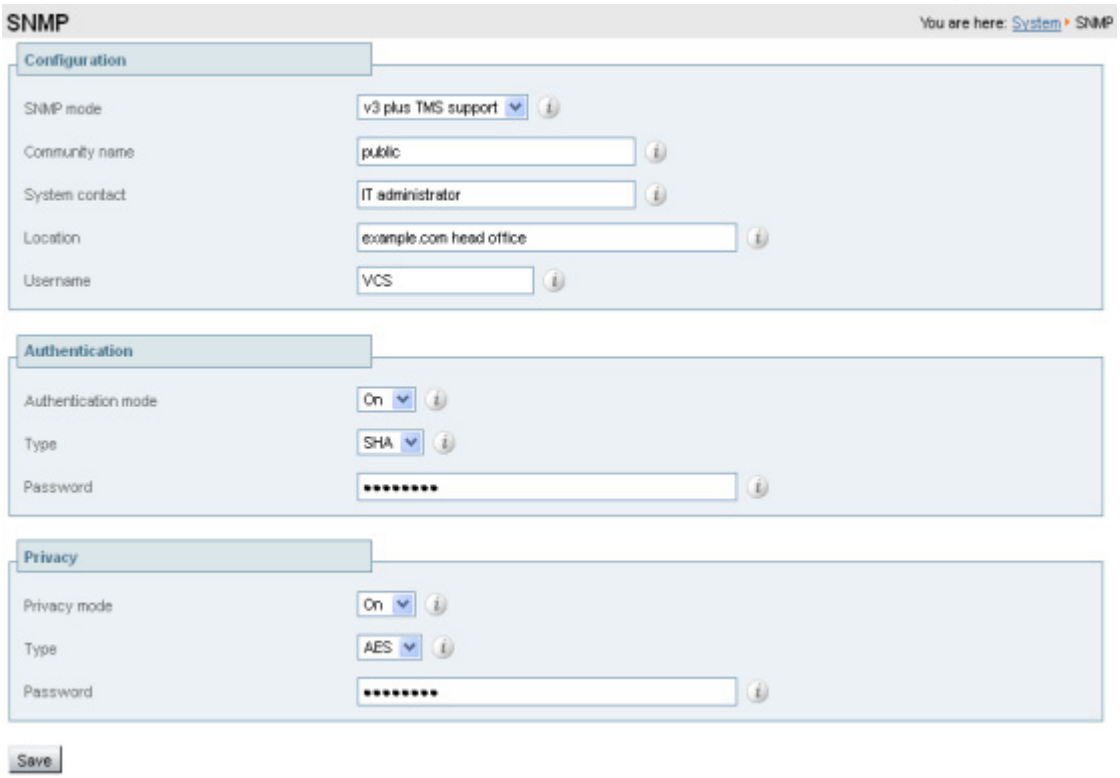
- SNMP を有効にすると VCS と Cisco TMS の統合プロセスを高速化しますが、必須ではありません。

SNMP を有効化し、設定するには、次の手順を実行します。

1. [システム（System）] > [SNMP] に移動します。
2. 次のように SNMP フィールドを設定します。

SNMP モード（SNMP mode）	*v3 と TMS のサポート（v3 plus TMS support）*
コミュニティ名（Community name）	`public` であることを確認します。
システム管理者（System contact）	`IT administrator` と入力します。
参照先（Location）	`example.com head office` と入力します。
ユーザ名（Username）	`VCS` と入力します。
認証モード（Authentication Mode）	*オン（On）*
タイプ（Type）	*SHA*
パスワード（Password）	`ex4mpl3.c0m` と入力します。
プライバシー モード（Privacy Mode）	*オン（On）*
タイプ（Type）	*AES*
パスワード（Password）	`ex4mpl3.c0m` と入力します。

3. [保存（Save）] をクリックします。



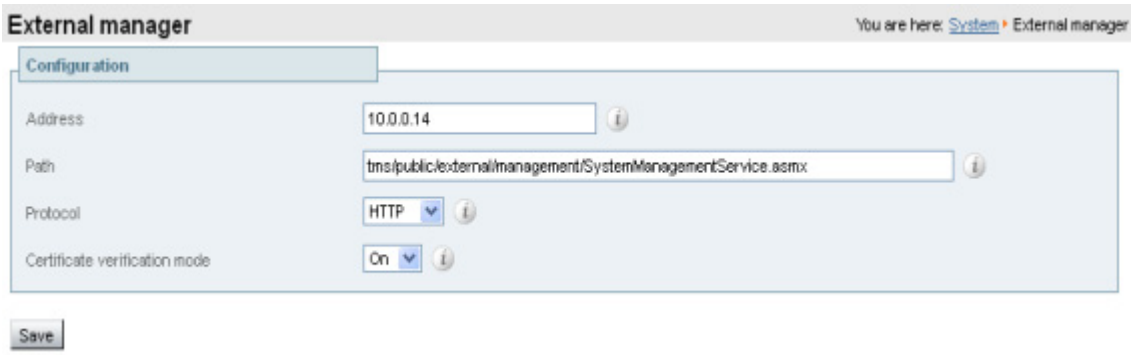
必要な外部のマネージャ（Cisco TMS）のパラメータを設定するには、次の手順を実行します。

1. [システム（System）] > [外部マネージャ（External manager）] に移動します。
2. フィールドを次のように設定します。

アドレス（Address）	`10.0.0.14` と入力します。
パス（Path）	`tms/public/external/management/SystemManagementService.asmx` と入力します。
プロトコル（Protocol）	[HTTP] または [HTTPS] を選択します。
証明書検証モード（Certificate verification mode）	[オン（On）] または [オフ（Off）] を選択します（下の注を参照してください）。

値が [オン（On）] でプロトコルが [HTTPS] に設定されている場合にのみ、証明書が検証されることに注意してください。オンに切り替える場合は、Cisco TMS および VCS に適切な証明書がある必要があります。

3. [保存（Save）] をクリックします。



ステップ 10：ロギング設定（任意）

次の設定により、イベント ログを外部のロギング サーバに送信することができます（SYSLOG プロトコルを使用）。

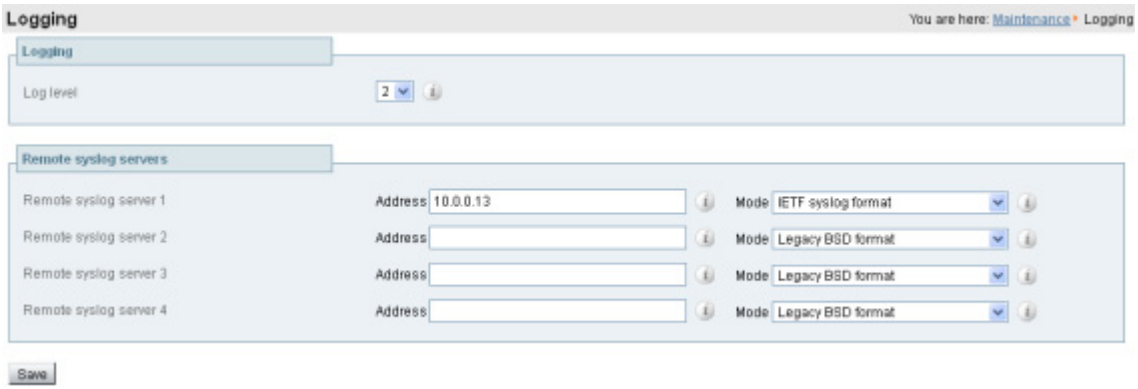
- [ログ レベル（Log level）] は、イベントのロギングの粒度を制御します。1 は最も詳細度が低く、4 が最も高くなります。
- 最小のログ レベルである 2 を推奨します。このレベルでは、システムおよび基本の両方のシグナリング メッセージのロギングが提供されるためです。

ロギング サーバを設定するには、次の手順を実行します。

1. [メンテナンス（Maintenance）] > [ロギング（Logging）] に移動します。
2. フィールドを次のように設定します。

ログ レベル（Log level）	*2*
リモート Syslog サーバ 1：アドレス（Remote syslog server 1: Address）	`10.0.0.13` と入力します。
リモート Syslog サーバ 1：モード（Remote syslog server 1: Mode）	*IETF syslog 形式（IETF syslog format）*

3. [保存（Save）] をクリックします。



ステップ 11：登録制限ポリシーの設定（任意）

エンドポイントが登録可能なエイリアスは、許可（ホワイト）リストまたは拒否（ブラック）リストのいずれかを使用して制限することができます。

次の設定は、「@example.com」を含むアイデンティティで登録するエンドポイントへの登録を制限します。

許可リストの登録の制限を設定するには、次の手順を実行します。

1. [設定（Configuration）] > [登録（Registration ）] > [許可リスト（Allow List）] に移動します。
2. [新規（New）] をクリックします。
3. 次のようにフィールドを設定して、許可パターンを作成します。

説明（Description）	`Only allow registrations containing "@example.com"` と入力します。
パターン タイプ（Pattern type）	*Regex*
パターン文字列（Pattern string）	`.*@example.com` と入力します。

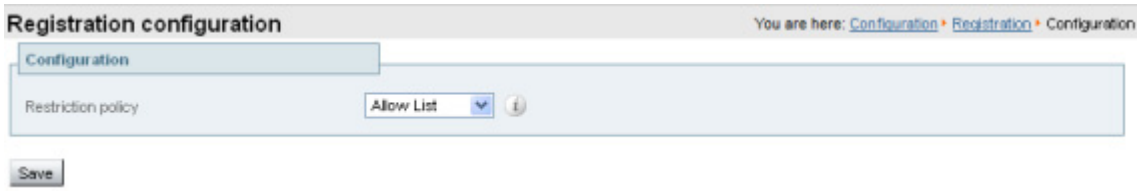
4. [許可リストのパターンの追加（Add Allow List pattern）] をクリックします。

登録の制限をアクティブにするには、次の手順を実行します。

1. [設定（Configuration）] > [登録（Registration）] > [設定（Configuration）] に移動します。
2. 次のように [制限ポリシー（Restriction policy）] を設定します。

制限ポリシー（Restriction policy）	*許可リスト（Allow List）*

3. [保存（Save）] をクリックします。



ステップ 12：デバイス認証ポリシーの設定（任意）

認証ポリシーは、VCS によってゾーン レベルおよびサブゾーン レベルで適用されます。これにより、VCS がゾーンまたはサブゾーンからの着信メッセージ（プロビジョニング、登録、プレゼンス、電話帳、およびコール）にどのように対処するか、およびこれらのメッセージが拒否されるか、認証済みとして処理されるか、または VCS 内で未認証として処理されるかを制御します。

各ゾーンおよびサブゾーンでは、それぞれの [認証ポリシー（Authentication policy）] を [クレデンシャルを確認する（Check credentials）]、[クレデンシャルを確認しない（Do not check credentials）]、または [認証済みとして扱う（Treat as authenticated）] に設定できます。

- 登録の認証は、デフォルト サブゾーン（または関連する代替サブゾーン）設定で制御されます。
- 最初のプロビジョニング登録要求の認証は、デフォルト ゾーン設定で制御されます。
- コール、プレゼンス、および電話帳要求の認証は、エンドポイントが登録されている場合はデフォルト サブゾーン（または関連する代替サブゾーン）で、エンドポイントが登録されていない場合はデフォルト ゾーンで制御されます。

デフォルトでは、ゾーンおよびサブゾーンは [クレデンシャルを確認しない（Do not check credentials）] に設定されます。

ステップ 13：ISDN ゲートウェイへのアクセスの制限（任意）

任意の ISDN ゲートウェイ リソースへの不正アクセスを制限する（不正通話防止とも呼ばれます）には、VCS のユーザが適切な処置を実施することを推奨します。この任意の手順では、実現可能ないくつかの方法を示します。

これらの例では、ISDN ゲートウェイがプレフィックス 9 を持つ（および/または 9 で開始するコールをルーティングするように指定されたネイバー ゾーンを持つ）VCS Control に登録されています。

この例では、ゲートウェイからのコールがゲートウェイ外へのコール バックをルーティングできないように、VCS Control を設定する方法を示しています。これは、いくつかの特別に構築された CPL を VCS Control にロードし、その [コール ポリシー モード（Call policy mode）] で *ローカル CPL* を使用するように設定することによって行います。

CPL ファイルの作成

VCS にアップロードする CPL ファイルは、テキスト エディタで作成できます。

次に、CPL の 2 組の例を示します。例について説明（Description）しておきます。

- 「GatewayZone」は、ISDN ゲートウェイへのネイバー ゾーンです

- 「GatewaySubZone」は ISDN ゲートウェイへのサブゾーンです（ゲートウェイがプレフィックス 9 を VCS に登録している場合に必要）
- ISDN ゲートウェイへのコールおよび FindMe を押すことにより、そのゲートウェイを使用するデバイスが呼び出されません。たとえば、携帯電話に転送されたコールは許可されません

この CPL の例には、発呼側が認証されているかどうかの確認は含まれていません。

```
<?xml version="1.0" encoding="UTF-8" ?>
<cpl xmlns="urn:ietf:params:xml:ns:cpl"
xmlns:taa="http://www.tandberg.net/cpl-extensions"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="urn:ietf:params:xml:ns:cpl cpl.xsd">
<taa:routed>
  <taa:rule-switch>
    <!--Check that gateway is not hairpinning call - Neighbor zone -->
    <taa:rule originating-zone="GatewayZone" destination="9.*">
      <!-- Calls coming from the gateway may not send calls back out of this gateway -->
      <!-- Reject call with a status code of 403 (Forbidden) -->
      <reject status="403" reason="ISDN hairpin call denied"/>
    </taa:rule> <!-- Check that gateway is not hairpinning call - Subzone for registered gateway -->
<taa:rule originating-zone="GatewaySubZone" destination="9.*"> <!-- Calls coming from the gateway may not
send calls back out of this gateway --> <!-- Reject call with a status code of 403 (Forbidden) --> <reject
status="403" reason="ISDN hairpin call denied"/> </taa:rule>     <taa:rule origin=".*" destination=".*">
      <!-- All other calls allowed -->
      <proxy/>
    </taa:rule>
  </taa:rule-switch>
</taa:routed>
</cpl>
```

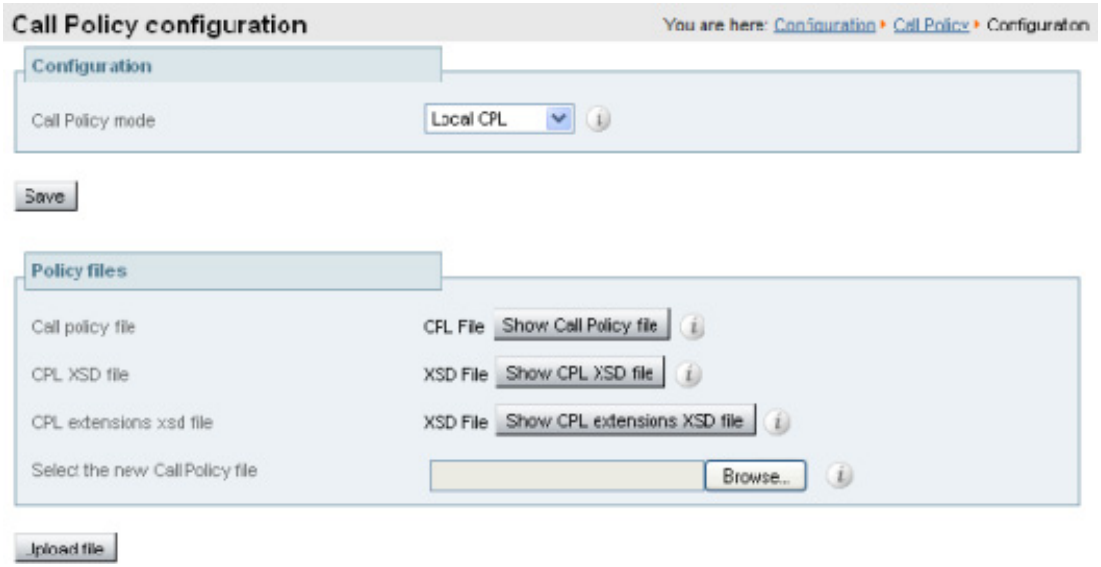
この CPL の例では、発呼側が認証されているかどうかも確認します。

```
<?xml version="1.0" encoding="UTF-8" ?>
<cpl xmlns="urn:ietf:params:xml:ns:cpl"
xmlns:taa="http://www.tandberg.net/cpl-extensions"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="urn:ietf:params:xml:ns:cpl cpl.xsd">
<taa:routed>
  <taa:rule-switch>
    <!-- Check that calling party is authenticated -->
    <taa:rule authenticated-origin="" destination="9.*">
      <!-- Reject call with a status code of 403 (Forbidden) -->
      <reject status="403" reason="ISDN call denied as unauthenticated caller"/>
    </taa:rule>
    <!-- Check that gateway is not hairpinning call - Neighbor zone -->
    <taa:rule originating-zone="GatewayZone" destination="9.*">
      <!-- Calls coming from the gateway may not hairpin and send calls back out -->
      <!-- Reject call with a status code of 403 (Forbidden) -->
      <reject status="403" reason="ISDN hairpin call denied"/>
    </taa:rule> <!-- Check that gateway is not hairpinning call - Subzone for registered gateway -->
<taa:rule originating-zone="GatewaySubZone" destination="9.*"> <!-- Calls coming from the gateway may not
hairpin and send calls back out --> <!-- Reject call with a status code of 403 (Forbidden) --> <reject
status="403" reason="ISDN hairpin call denied"/> </taa:rule>     <taa:rule origin=".*" destination=".*">
      <!-- All other calls allowed -->
      <proxy/>
    </taa:rule>
  </taa:rule-switch>
</taa:routed>
</cpl>
```

VCS Control への CPL のロード

CPL を使用するように VCS Control を設定するには、次の手順を実行します。

1. [設定（Configuration）] > [コール ポリシー（Call Policy）] > [設定（Configuration）] に移動します。
2. [参照...（Browse...）] をクリックし、ファイル システムから（上記で作成した）CPL ファイルを選択します。
3. [ファイルのアップロード（Upload file）] をクリックします。
   - 「File upload successful」メッセージが表示されます。
   - 「XML invalid」メッセージが表示された場合は、CPL ファイルの問題を修正して、再度アップロードする必要があります。
4. *ローカル CPL* の [コール ポリシー モード（Call policy mode）] を選択します。
5. [保存（Save）] をクリックします。



付録 1：設定の詳細

この付録では、VCS Control に必要な設定について説明（Description）します。

VCS Control システムの設定

設定項目	値	VCS のページ
システム設定		
システム名（System name）	VCSc	[システム（System）] > [管理（Administration）]
LAN1 IPv4 アドレス（LAN1 IPv4 address）	10.0.0.2	[システム（System）] > [ネットワーク インターフェイス（Network interfaces）] > [IP]

設定項目	値	VCS のページ
IPv4 ゲートウェイ（IPv4 gateway）	10.0.0.1	[システム（System）] > [ネットワーク インターフェイス（Network interfaces）] > [IP]
LAN1 サブネット マスク（LAN1 subnet mask）	255.255.255.0	[システム（System）] > [ネットワーク インターフェイス（Network interfaces）] > [IP]
DNS サーバ アドレス 1（DNS server address 1）	10.0.0.11	[システム（System）] > [DNS]
DNS サーバ アドレス 2（DNS server address 2）	10.0.0.12	[システム（System）] > [DNS]
DNS ドメイン名（DNS domain name）	internal-domain.net	[システム（System）] > [DNS]
DNS システム ホスト名（DNS System host name）	vcsc	[システム（System）] > [DNS]
NTP サーバ 1（NTP server 1）	10.0.0.21	[システム（System）] > [時間（Time）]
タイム ゾーン（Time zone）	GMT	[システム（System）] > [時間（Time）]
プロトコル設定		
SIP ドメイン名（SIP DOMAIN NAME）	example.com	[設定（Configuration）] > [ドメイン（Domains）]

VCS Control のトランスフォーメーション ルールおよび検索ルール

設定項目	値	VCS のページ
トランスフォーメーション		
パターン文字列（Pattern string）	([^@]*)	[設定（Configuration）] > [ダイヤル プラン（Dial plan）] > [トランスフォーメーション（Transforms）]
パターン タイプ（Pattern type）	Regex	[設定（Configuration）] > [ダイヤル プラン（Dial plan）] > [トランスフォーメーション（Transforms）]
パターン動作（Pattern behavior）	置換（Replace）	[設定（Configuration）] > [ダイヤル プラン（Dial plan）] > [トランスフォーメーション（Transforms）]
文字列の置換（Replace string）	\1@example.com	[設定（Configuration）] > [ダイヤル プラン（Dial plan）] > [トランスフォーメーション（Transforms）]
ローカル検索ルール 1		
ルール名 （Rule name）	Local zone - no domain	[設定（configuration）] > [ダイヤル プラン（Dial plan）] > [検索ルール（Search rules）]
プライオリティ（Priority）	48	[設定（configuration）] > [ダイヤル プラン（Dial plan）] > [検索ルール（Search rules）]
ソース（Source）	任意（Any）	[設定（configuration）] > [ダイヤル プラン（Dial plan）] > [検索ルール（Search rules）]
モード（Mode）	エイリアスのパターン マッチ（Alias pattern match）	[設定（configuration）] > [ダイヤル プラン（Dial plan）] > [検索ルール（Search rules）]

設定項目	値	VCS のページ
パターン タイプ（Pattern type）	Regex	[設定（configuration）] > [ダイヤル プラン（Dial plan）] > [検索ルール（Search rules）]
パターン文字列（Pattern string）	(.+)@example.com.*	[設定（configuration）] > [ダイヤル プラン（Dial plan）] > [検索ルール（Search rules）]
パターン動作（Pattern behavior）	置換（Replace）	[設定（configuration）] > [ダイヤル プラン（Dial plan）] > [検索ルール（Search rules）]
文字列の置換（Replace string）	\1	[設定（configuration）] > [ダイヤル プラン（Dial plan）] > [検索ルール（Search rules）]
正常に一致する場合（On successful match）	続行（Continue）	[設定（configuration）] > [ダイヤル プラン（Dial plan）] > [検索ルール（Search rules）]
ターゲット（Target）	LocalZone	[設定（configuration）] > [ダイヤル プラン（Dial plan）] > [検索ルール（Search rules）]
ローカル検索ルール 2		
ルール名 （Rule name）	Local zone - full URI	[設定（configuration）] > [ダイヤル プラン（Dial plan）] > [検索ルール（Search rules）]
プライオリティ（Priority）	50	[設定（configuration）] > [ダイヤル プラン（Dial plan）] > [検索ルール（Search rules）]
ソース（Source）	任意（Any）	[設定（configuration）] > [ダイヤル プラン（Dial plan）] > [検索ルール（Search rules）]
モード（Mode）	エイリアスのパターン マッチ（Alias pattern match）	[設定（configuration）] > [ダイヤル プラン（Dial plan）] > [検索ルール（Search rules）]
パターン タイプ（Pattern type）	Regex	[設定（configuration）] > [ダイヤル プラン（Dial plan）] > [検索ルール（Search rules）]
パターン文字列（Pattern string）	(.+)@example.com.*	[設定（configuration）] > [ダイヤル プラン（Dial plan）] > [検索ルール（Search rules）]
パターン動作（Pattern behavior）	変更なし（Leave）	[設定（configuration）] > [ダイヤル プラン（Dial plan）] > [検索ルール（Search rules）]
正常に一致する場合（On successful match）	続行（Continue）	[設定（configuration）] > [ダイヤル プラン（Dial plan）] > [検索ルール（Search rules）]
ターゲット（Target）	LocalZone	[設定（configuration）] > [ダイヤル プラン（Dial plan）] > [検索ルール（Search rules）]

付録 2：DNS レコード

内部メッセージを VCS Control に対してルーティングするには、内部からルーティング可能なドメインである internal-domain.net をホスティングするローカル DNS で、次のレコードを設定する必要があります。

ローカル DNS A レコード

ホスト	ホスト IP アドレス（Host IP address）
vcsc.internal-domain.net	10.0.0.2

ローカル DNS SRV レコード

名前（Name）	サービス（Service）	プロトコル（Protocol）	プライオリティ（Priority）	重み付け（Weight）	ポート（Port）	ターゲット ホスト（Target host）
internal-domain.net.	h323cs	tcp	10	10	1720	vcsc.internal-domain.net.
internal-domain.net.	h323ls	udp	10	10	1719	vcsc.internal-domain.net.
internal-domain.net.	h323rs	udp	10	10	1719	vcsc.internal-domain.net.
internal-domain.net.	sip	tcp	10	10	[5060]	vcsc.internal-domain.net.
internal-domain.net.	sip	udp *	10	10	[5060]	vcsc.internal-domain.net.
internal-domain.net.	sips	tcp	10	10	5061	vcsc.internal-domain.net.

* SIP UDP は VCS ではデフォルトで無効になっています。

たとえば、DNS レコードは次のとおりです。

```
_h323cs._tcp.internal-domain.net.86400 IN SRV 10 10 1720 vcsc.internal-domain.net.
_h323ls._udp.internal-domain.net.86400 IN SRV 10 10 1719 vcsc.internal-domain.net. _h323rs._udp.internal-domain.net.86400 IN SRV 10 10 1719 vcsc.internal-domain.net. _sip._tcp.internal-domain.net.86400 IN SRV 10 10 5060 vcsc.internal-domain.net.
_sip._udp.internal-domain.net.86400 IN SRV 10 10 5060 vcsc.internal-domain.net.
_sips._tcp.internal-domain.net.86400 IN SRV 10 10 5061 vcsc.internal-domain.net.
vcsc.internal-domain.net.86400 IN A 10.0.0.2
```

マニュアルの入手方法およびテクニカル サポート

資料の入手方法、Cisco Bug Search Tool（BST）の使用方法、サービス要求の送信および追加情報の収集方法については、『What's New in Cisco Product Documentation（Cisco 製品資料の更新情報）』（http://www.cisco.com/c/en/us/td/docs/general/whatsnew/whatsnew.html）を参照してください。

『What's New in Cisco Product Documentation』は、シスコの新規および改訂版の技術マニュアルの一覧も示し、RSS フィードとして購読できます。また、リーダー アプリケーションを使用してコンテンツをデスクトップに配信することもできます。RSS フィードは無料のサービスです。

マニュアルの変更履歴

日付（Date）	説明（Description）
2015 年 11 月	新しいテンプレートを適用。X8.7 用に再発行。
2015 年 7 月	X8.6 に関する内容を更新。
2015 年 4 月	X8.5 のメニュー パスを変更。X8.5.2 で再公開。
2014 年 12 月	X8.5 用に再発行。
2014 年 6 月	X8.2 用に再発行。
2013 年 12 月	X8.1 に関する内容を更新。
2012 年 8 月	ドキュメント構造を変更および X7.2 に関する内容を更新。
2010 年 10 月	新しいドキュメント テンプレートを適用。
2009 年 9 月	初版。

シスコの法的情報

このマニュアルに記載されている仕様および製品に関する情報は、予告なしに変更されることがあります。このマニュアルに記載されている表現、情報、および推奨事項は、すべて正確であると考えていますが、明示的であれ黙示的であれ、一切の保証の責任を負わないものとします。このマニュアルに記載されている製品の使用は、すべてユーザ側の責任になります。

対象製品のソフトウェア ライセンスおよび限定保証は、製品に添付された『Information Packet』に記載されています。添付されていない場合には、代理店にご連絡ください。

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system.All rights reserved.Copyright © 1981, Regents of the University of California.

ここに記載されている他のいかなる保証にもよらず、各社のすべてのマニュアルおよびソフトウェアは、障害も含めて「現状のまま」として提供されます。シスコおよびこれら各社は、商品性の保証、特定目的への準拠の保証、および権利を侵害しないことに関する保証、あるいは取引過程、使用、取引慣行によって発生する保証をはじめとする、明示されたまたは黙示された一切の保証の責任を負わないものとします。

いかなる場合においても、シスコおよびその供給者は、このマニュアルの使用または使用できないことによって発生する利益の損失やデータの損傷をはじめとする、間接的、派生的、偶発的、あるいは特殊な損害について、あらゆる可能性がシスコまたはその供給者に知らされていても、それらに対する責任を一切負わないものとします。

このマニュアルで使用している IP アドレスおよび電話番号は、実際のアドレスおよび電話番号を示すものではありません。マニュアル内の例、コマンド出力、ネットワーク トポロジ図、およびその他の図は、説明（Description）のみを目的として使用されています。説明（Description）の中に実際のアドレスおよび電話番号が使用されていたとしても、それは意図的なものではなく、偶然の一致によるものです。

ハード コピーおよびソフト コピーの複製は公式版とみなされません。最新版はオンライン版を参照してください。

シスコは世界各国 200 箇所にオフィスを開設しています。各オフィスの住所、電話番号、FAX 番号は当社の Web サイト（www.cisco.com/go/offices [英語]）をご覧ください。

シスコの商標または登録商標

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. シスコの商標の一覧は www.cisco.com/web/JP/trademark_statement.html に掲載されています。Third-party trademarks mentioned are the property of their respective owners.The use of the word partner does not imply a partnership relationship between Cisco and any other company.(1110R)