



**Cisco Unified SRST**  
**システム アドミニストレーション ガイド**  
**(すべてのバージョン)**

July 11, 2008

**【注意】シスコ製品をご使用になる前に、安全上の注意**  
( [www.cisco.com/jp/go/safety\\_warning/](http://www.cisco.com/jp/go/safety_warning/) ) をご確認ください。

本書は、米国シスコシステムズ発行ドキュメントの参考和訳です。  
米国サイト掲載ドキュメントとの差異が生じる場合があるため、正式な内容については米国サイトのドキュメントを参照ください。  
また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

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。見当たらない場合には、代理店にご連絡ください。

シスコが採用している TCP ヘッダー圧縮機能は、UNIX オペレーティングシステムの UCB ( University of California, Berkeley ) パブリックドメインバージョンとして、UCB が開発したプログラムを最適化したものです。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、すべてのマニュアルおよび上記各社のソフトウェアは、障害も含めて「現状のまま」として提供されます。シスコおよび上記各社は、商品性や特定の目的への適合性、権利を侵害しないことに関する、または取り扱い、使用、または取り引きによって発生する、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、シスコおよびその代理店は、このマニュアルの使用またはこのマニュアルを使用できないことによって起こる制約、利益の損失、データの損傷など間接的で偶発的に起こる特殊な損害のあらゆる可能性がシスコまたは代理店に知らされていても、それらに対する責任を一切負いかねます。

CCVP, the Cisco logo, and Welcome to the Human Network are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website 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.(0711R)

このドキュメントで使用しているインターネット プロトコル (IP) アドレスは、実在のアドレスではありません。ドキュメント中で示される例、コマンドの画面出力、および図は、いずれも視覚的な説明のみを目的としています。実在する IP アドレスが例示されていた場合、それらは意図して使用したものではありません。

*Cisco Unified SRST システム アドミニストレーション ガイド*  
Copyright © 2008 Cisco Systems, Inc.  
All rights reserved.

Copyright © 2008, シスコシステムズ合同会社 .  
All rights reserved.



## CONTENTS

<b>Cisco Unified Survivable Remote Site Telephony 機能のロードマップ</b>	<b>1</b>
内容	1
マニュアルの構成	2
機能のロードマップ	4
Cisco Unified SRST の新機能について	8
Cisco Unified SRST V4.3/7.0 の新機能	8
Cisco Unified SRST V4.2(1) の新機能	8
Cisco Unified SRST V4.1 の新機能	8
Cisco Unified SRST V4.0 の新機能	8
Cisco Unified IP Phone の追加サポート	8
Cisco IP Communicator のサポート	9
SCCP および ATA サポートを使用した FAX パススルー	9
WAN リンク障害に対する H.323 VoIP コール プリザベーションの機能拡張	10
ビデオ サポート	10
Cisco SRST V3.4 の新機能	10
Cisco SIP SRST 3.4	10
Cisco SRST V3.3 の新機能	10
Secure SRST	11
Cisco Unified IP Phone 7970G および Cisco Unified 7971G-GE のサポート	11
show ephone コマンドの機能拡張	11
Cisco SRST V3.2 の新機能	12
alias コマンドの機能拡張	12
cor コマンドの機能拡張	12
pickup コマンドの機能拡張	12
user-locale コマンドの機能拡張	12
Cisco 3845 でサポートされる Cisco Unified IP Phone の台数の増加	13
MOH ライブ フィードのサポート	13
コール プリザベーションのタイムアウトなし	13
RFC 2833 DTMF リレーのサポート	13
変換プロファイルのサポート	13
Cisco SRST V3.1 の新機能	14

Cisco Unified IP Phone 7920 のサポート	14
Cisco Unified IP Phone 7936 のサポート	14
Cisco SRST V3.0 の新機能	14
IP Phone のディスプレイに対する追加の言語オプション	15
H.450.2 および H.450.3 を使用した打診コール転送および自動転送	15
Cisco Unified IP Phone 用にカスタマイズされたシステム メッセージ	16
二重回線モード	16
E1 R2 シグナリングのサポート	16
欧州の日付形式	17
二重回線モードのハントストップ	17
フラッシュ ファイルからのマルチキャスト用の Music On Hold	17
呼び出しタイムアウトのデフォルト	18
第 2 発信音	18
show ephone コマンドの機能拡張	18
電話機の登録に関するシステム ログ メッセージ	18
3 者間の G.711 Ad Hoc 会議	18
Cisco VG248 Analog Phone Gateway バージョン 1.2(1) 以降のバージョンのサポート	18
Cisco SRST V2.1 の新機能	19
IP Phone のディスプレイに対する追加の言語オプション	19
Cisco SRST の集約	20
Cisco ATA 186 および ATA 188 のサポート	20
Cisco Unified IP Phone 7902G のサポート	20
Cisco Unified IP Phone 7905G のサポート	20
Cisco Unified IP Phone 7912G のサポート	20
Cisco Unified IP Phone 7914 拡張モジュールのサポート	21
dialplan-pattern コマンドの機能拡張	21
Cisco SRST V2.02 の新機能	21
Cisco Unified IP Phone Conference Station 7935 のサポート	21
電話番号の増加	22
PSTN および BRI/PRI を介してインバンド DTMF シグナリングを使用した Cisco Unity ボイスメール統合	22
関連情報	23
<b>Cisco Unified SRST の概要</b>	<b>25</b>
内容	25
Cisco Unified SRST の説明	26
MGCP ゲートウェイと SRST	29

Cisco Unified IP Phone、プラットフォーム、Cisco Unified Communications Manager、信号、言語、およびスイッチのサポート	30
Cisco Unified SRST をサポートする Cisco IOS ソフトウェア リリースの検索	30
Cisco Unified IP Phone のサポート	30
プラットフォームとメモリのサポート	31
Cisco Feature Navigator を使用したプラットフォーム サポートの確認	31
Cisco IOS ソフトウェア イメージのアベイラビリティ	32
Cisco Unified Communications Manager の互換性	32
信号のサポート	32
言語のサポート	32
スイッチのサポート	33
Cisco Unified SRST を設定する場合の前提条件	34
バージョンの前提条件	34
Cisco Unified Communications Manager のインストール	34
Cisco Unified SRST のインストール	34
Cisco SRST V3.0 以降のバージョンのインストール	35
Cisco SRST V2.0 および V2.1 のインストール	35
Cisco SRST V1.0 のインストール	35
Cisco Unified SRST と Cisco Unified Communications Manager の統合	35
Cisco Communications Manager V3.3 以降のバージョンを使用する場合	35
V3.3 以前の Cisco Unified Communications Manager を使用する場合	36
Cisco Unified SRST を設定する場合の制約事項	37
関連情報	39
その他の資料	40
関連資料	40
標準規格	41
MIB	41
RFC	41
テクニカル サポート	42
マニュアルの入手方法、テクニカル サポート、およびセキュリティ ガイドライン	42
シスコのテクニカル サポート	43
Service Request ツールの使用	43
その他の情報の入手方法	44
<b>ネットワークの設定</b>	<b>45</b>
内容	45

ネットワークの設定について	45
ネットワークの設定方法	46
IP ルーティングの有効化	46
MGCP ゲートウェイでの SRST の有効化	46
Cisco IOS Release 12.3(14)T 以前の MGCP ゲートウェイにおける SRST の設定	46
Cisco IOS Release 12.3(14)T 以降の MGCP ゲートウェイにおける SRST の設定	48
制約事項	48
Cisco IOS Release 12.3(14)T を使用する MGCP ゲートウェイで SRST を有効にする設定の例	49
Cisco Unified SRST Phone に対する DHCP の設定	51
単一の DHCP IP アドレス プールを定義する	51
各 Cisco Unified IP Phone に対する個別の DHCP IP アドレス プールを定義する	52
DHCP リレー サーバを定義する	53
キープアライブ インターバルの指定	54
例	55
電話機能をサポートするための Cisco Unified SRST の設定	55
Cisco Unified SRST が有効になっていることの確認	57
トラブルシューティング	58
関連情報	59
<b>Cisco Unified IP Phone の設定</b>	<b>61</b>
内容	61
Cisco Unified IP Phone の設定について	61
Cisco Unified IP Phone の設定方法	62
IP Phone のクロック、日付、および時刻の形式の設定	62
例	63
IP Phone の言語表示の設定	63
例	64
Cisco Unified IP Phone 用にカスタマイズされたシステム メッセージの設定	65
例	66
第 2 発信音の設定	66
例	66
二重回線電話機の設定	66
例	68
各ボタンでの 8 回線（八重回線）の設定	68
前提条件	68

制約事項	69
例	70
Cisco Unified SRST に関する Cisco IP Communicator の設定方法	71
前提条件	71
Cisco IP Communicator の確認	72
Cisco IP Communicator のトラブルシューティング	72
関連情報	72
<b>コール処理の設定</b>	<b>73</b>
内容	73
コール処理の設定について	73
着信コールと発信コールに対するコール処理の設定方法	74
着信コールの設定	74
ビジー信号の受信時または無応答時の自動転送の設定	74
例	75
コールの再ルーティングの設定	76
例	79
コール ピックアップの設定	79
例	80
打診転送の設定	81
電話会議	82
転送番号の収集方法の設定	82
例	83
グローバル プレフィックスの設定	83
例	84
数字変換規則の有効化	85
例	86
変換プロファイルの有効化	86
例	88
変換プロファイルの確認	88
ダイヤル ピアとチャネルのハンティングの設定	89
例	90
ビジー タイムアウトの設定	90
例	91
呼び出しタイムアウトのデフォルトの設定	91
例	92
発信コールの設定	92
ローカルおよびリモートのコール転送の設定	92
例	93

Cisco SRST 3.0 での H.450.2 および H.450.3 を使用した打診コール転送 および自動転送	93
例	96
Cisco SRST 3.0 またはそれ以前のバージョンでのフックフラッシュおよ び H.450.2 標準を使用したアナログ転送の有効化	97
例	101
トランク アクセス コードの設定	101
例	102
桁間タイムアウト値の設定	102
例	103
制限クラスの設定	103
例	105
時刻と曜日または日付に基づいたコール ブロッキング (ツール バー)	107
例	108
WAN リンク障害に対する H.323 VoIP コール プリザベーションの機能拡張	109
関連情報	109
<b>追加のコール機能の設定</b>	<b>111</b>
内容	111
オプション機能の設定方法	112
3 者間 G.711 Ad Hoc 会議の有効化	112
例	113
XML API スキーマの定義	113
関連情報	114
<b>Cisco Unified SRST をマルチキャスト MOH リソースとして使用するための Cisco Unified Communications Manager と Cisco Unified SRST の統合</b>	<b>115</b>
内容	116
Cisco Unified SRST ゲートウェイをマルチキャスト MOH リソースとして使用す るための前提条件	116
Cisco Unified SRST ゲートウェイをマルチキャスト MOH リソースとして使用す るための制限事項	117
Cisco Unified SRST ゲートウェイをマルチキャスト MOH リソースとして使用す るための情報	118
Cisco Unified SRST ゲートウェイと Cisco Unified Communications Manager	118
コーデック、ポート番号、および IP アドレス	119
マルチキャスト MOH 伝送	121
Cisco Unified SRST MOH ライブ フィードのサポート	121
フラッシュ ファイルからの MOH の設定	122



Cisco Unified SRST ゲートウェイをマルチキャスト MOH リソースとして使用する 方法	123
Cisco Unified SRST マルチキャスト MOH 用の Cisco Unified Communications Manager の設定	123
マルチキャストを有効にするための MOH オーディオ ソースの設定	124
Cisco Unified Communications Manager MOH サーバでのマルチキャスト の有効化およびポート番号と IP アドレスの設定	126
MRG と MRGL の作成、MOH マルチキャストの有効化、およびゲート ウェイの設定	129
MOH サーバのリージョンの作成	130
Cisco Unified Communications Manager マルチキャスト MOH の確認	132
マルチキャスト MOH 用の Cisco Unified SRST の設定	133
前提条件	133
Cisco Unified SRST ゲートウェイでのマルチキャスト MOH の有効化	134
基本的な Cisco Unified SRST マルチキャスト MOH ストリーミングの確認	136
PSTN への Cisco Unified SRST MOH の確認	138
IP Phone に対する Cisco Unified SRST マルチキャスト MOH の確認	141
トラブルシューティングに関するヒント	141
Cisco Unified SRST MOH ライブ フィード サポートの設定 (オプション)	142
前提条件	143
制約事項	143
Cisco Unified SRST ゲートウェイ上の音声ポートの設定	143
Cisco Unified SRST ゲートウェイ上の電話番号の設定	144
MOH フィードの確立	145
Cisco Unified SRST MOH ライブ フィードの確認	147
Cisco Unified SRST ゲートウェイの設定例	147
2 つの IP アドレスにルーティングされる MOH : 例	147
MOH ライブ フィード : 例	148
マルチキャスト MOH リソースとしての Cisco Unified SRST に関する機能情報	149
関連情報	150
<b>Secure SRST の設定</b>	<b>151</b>
内容	151
Secure SRST を設定するための前提条件	152
Secure SRST を設定する場合の制約事項	153

Secure SRST の設定について	154
Secure SRST の利点	154
SRST での Cisco IP Phone のクリアテキスト フォールバック	154
SRST ルータおよび TLS プロトコル	155
Cisco Unified SRST ルータおよび PKI	155
Secure SRST の認証および暗号化	156
Secure SRST ルータの Cisco IOS クレデンシャル サーバ	158
Cisco Unified IP Phone への Secure Cisco Unified SRST の確立	158
Secure SRST の設定方法	160
安全に通信を行うための Cisco Unified SRST ルータの準備	160
Cisco IOS 証明書サーバへの CA サーバの設定	160
CA サーバに対する Secure Cisco Unified SRST ルータの自動登録と認証	162
例	164
自動証明書登録の無効化	164
証明書登録の確認	165
Secure Cisco Unified SRST ルータでのクレデンシャル サービスの有効化	167
クレデンシャル設定のトラブルシューティング	168
Secure SRST ルータへの電話機の証明書ファイル ( PEM 形式 ) のインポート	169
Cisco Unified Communications Manager 4.X.X およびそれ以前のバージョン	169
Cisco Unified Communications Manager 5.0 およびそれ以降のバージョン	169
前提条件	169
制約事項	170
例	171
Secure Cisco Unified SRST ルータへの Cisco Unified Communications Manager の設定	176
Cisco Unified Communications Manager への SRST リファレンスの追加	176
Cisco Unified Communications Manager での SRST フォールバックの設定	178
Cisco Unified Communications Manager への CAPF の設定	180
Secure Cisco Unified SRST ルータでの SRST モードの有効化	180
例	181
電話機のステータスおよび登録の確認	182
Secure SRST の設定例	187
Secure SRST : 例	187
コントロール プレーン ポリシング : 例	192

関連情報	192
<b>Cisco Unified SRST へのボイスメールの統合</b>	<b>193</b>
内容	193
Cisco Unified SRST へのボイスメールの統合について	194
Cisco Unified SRST へのボイスメールの統合方法	196
ボイスメールへのダイレクト アクセスの設定	196
例	199
メッセージ ボタンの設定	199
例	200
Cisco Unified Communications Manager ゲートウェイへのリダイレクト	201
ボイスメールへのコール転送の設定	201
DTMF デジタル パターンを使用したコール ルーティング指示	201
前提条件	203
例	205
MWI の設定	205
設定例	207
ローカル ボイスメール システムの設定 (FXO および FXS): 例	207
セントラル ロケーションのボイスメール システムの設定 (FXO および FXS): 例	207
FXO および FXS を介したボイスメール アクセスの設定: 例	208
BRI および PRI を介したボイスメール アクセスの設定: 例	209
関連情報	210
<b>ビデオ パラメータの設定</b>	<b>211</b>
内容	211
ビデオ パラメータを設定するための前提条件	212
ビデオ パラメータの設定に関する制約事項	213
ビデオ パラメータの設定について	214
エンドポイント機能の一致	214
ビデオ コーデック情報の取得	214
オーディオ専用のコールのフォールバック	214
ビデオ エンドポイントでのコール設定	215
2 つのローカル SCCP エンドポイント間でのコール設定	215
SCCP エンドポイントと H.323 エンドポイント間でのコール設定	215
H.323 ネットワークを介した 2 つの SCCP エンドポイント間でのコール設定	215
RTP ビデオ ストリームの流れ	216
Cisco Unified SRST のビデオ パラメータの設定方法	217
低速接続手順の設定	217

Cisco Unified SRST の確認	218
例	219
Cisco Unified SRST のビデオ パラメータの設定	224
例	225
Cisco Unified SRST のビデオのトラブルシューティング	226
関連情報	226
<b>Cisco Unified SRST の監視と保守</b>	<b>227</b>
関連情報	228
<b>E911 サービス</b>	<b>229</b>
内容	229
前提条件	230
制約事項	230
E911 サービスについて	231
概要	231
コール処理	233
バージョン 4.2(1) の新機能	236
携帯電話に関する注意事項	236
E911 サービスの実装の計画	236
既存の Cisco Unified SRST 機能との相互作用	238
ELIN の複数の用途	239
番号の変換	239
コール転送	240
自動転送	240
コール ブロッキング機能	240
コール ウェイティング	240
3 者間会議	240
ダイヤル ピアのロータリー	240
ダイヤル プラン パターン	241
発信者 ID のブロック	241
共有回線	241
E911 サービスの設定	242
緊急応答ロケーションの設定	242
前提条件	242
制約事項	242
緊急応答ゾーン内のロケーションの設定	244
前提条件	244
制約事項	244
E911 サービスの発信ダイヤル ピアの設定	245

緊急コール用のダイヤル ピアの設定	245
緊急応答ゾーン用のダイヤル ピアの設定	246
PSAP からのコールバック用のダイヤル ピアの設定	247
電話機への ERL の割り当て	248
前提条件	249
電話機の IP サブネットへの ERL の割り当て	249
電話機の ephone への ERL の割り当て	250
ダイヤル ピアへの ERL の割り当て	250
カスタマイズ設定値の設定	251
前提条件	252
制約事項	252
2 つの ELIN に対する address コマンドの使用	253
呼詳細レコードの有効化	254
RADIUS アカウンティング サーバからの出力	254
syslog サーバからの出力	254
show call history voice コマンドからの出力	255
E911 設定の確認	255
バージョン 4.2(1) のみ	255
バージョン 4.1 およびバージョン 4.2(1)	256
E911 サービスのトラブルシューティング	257
エラー メッセージ	257
E911 サービスの設定例	258
バージョン 4.2(1) のみ	258
バージョン 4.1 およびバージョン 4.2(1)	259
E911 サービスの機能情報	264
関連情報	264
<b>付録 A : SIP 用の Cisco Unified SRST サポートの準備</b>	<b>265</b>
内容	265
SIP アプリケーション用 DTMF リレーとボイスメール	266
SIP RFC 2833 を使用した DTMF リレー	266
トラブルシューティングに関するヒント	267
SIP Notify (非標準) を使用した DTMF リレー	267
トラブルシューティングに関するヒント	269
関連情報	270

## 索引





# Cisco Unified Survivable Remote Site Telephony 機能のロードマップ

---

Revised: July 11, 2008

この章では、Cisco Unified Survivable Remote Site Telephony ( Cisco Unified SRST ) 機能のリストや機能に関する資料の場所を示します。

プラットフォームのサポートおよび Cisco IOS ソフトウェア イメージのサポートに関する情報を参照するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には <http://www.cisco.com/go/fn> からアクセスできます。Cisco.com のアカウントが必要になります。アカウントを持っていない場合や、ユーザ名またはパスワードを忘れた場合は、ログイン ダイアログボックスで **Cancel** をクリックし、表示された指示に従います。

## 内容

- [マニュアルの構成 \( P.2 \)](#)
- [機能のロードマップ \( P.4 \)](#)
- [Cisco Unified SRST の新機能について \( P.8 \)](#)

## マニュアルの構成

このマニュアルは、表 1 に示す章または付録で構成されています。

表 1 Cisco Unified SRST の設定順序

章または付録	説明
Cisco Unified SRST の概要	SRST の概要について説明します。この章には、次の項があります。 <ul style="list-style-type: none"> <li>• Cisco Unified SRST の説明 ( P.26 )</li> <li>• Cisco Unified IP Phone、プラットフォーム、Cisco Unified Communications Manager、信号、言語、およびスイッチのサポート ( P.30 )</li> <li>• Cisco Unified SRST を設定する場合の前提条件 ( P.34 )</li> <li>• Cisco Unified SRST を設定する場合の制約事項 ( P.37 )</li> <li>• その他の資料 ( P.40 )</li> </ul>
ネットワークの設定	Cisco Unified SRST システムがネットワークと通信するように設定する方法について説明します。この章には、次の作業が含まれています。 <ul style="list-style-type: none"> <li>• IP ルーティングの有効化 ( P.46 )</li> <li>• Cisco Unified SRST Phone に対する DHCP の設定 ( P.51 )</li> <li>• キープアライブインターバルの指定 ( P.54 )</li> <li>• 電話機能をサポートするための Cisco Unified SRST の設定 ( P.55 )</li> <li>• Cisco Unified SRST が有効になっていることの確認 ( P.57 )</li> </ul>
Cisco Unified IP Phone の設定	Cisco Unified SRST Phone の基本的な設定方法について説明します。この章には、次の作業が含まれています。 <ul style="list-style-type: none"> <li>• IP Phone のクロック、日付、および時刻の形式の設定 ( P.62 )</li> <li>• IP Phone の言語表示の設定 ( P.63 )</li> <li>• Cisco Unified IP Phone 用にカスタマイズされたシステム メッセージの設定 ( P.65 )</li> <li>• 第 2 発信音の設定 ( P.66 )</li> <li>• 二重回線電話機の設定 ( P.66 )</li> </ul>
コール処理の設定	着信コールと発信コールの設定方法について説明します。この章には、次の作業が含まれています。 <ul style="list-style-type: none"> <li>• 着信コールの設定 ( P.74 )</li> <li>• 発信コールの設定 ( P.92 )</li> </ul>
追加のコール機能の設定	オプションのシステム パラメータと電話パラメータの設定方法について説明します。この章には、次の作業が含まれています。 <ul style="list-style-type: none"> <li>• 3 者間 G.711 Ad Hoc 会議の有効化 ( P.112 )</li> <li>• XML API スキーマの定義 ( P.113 )</li> </ul>
Cisco Unified SRST をマルチキャスト MOH リソースとして使用するための Cisco Unified Communications Manager と Cisco Unified SRST の統合	マルチキャスト Music-On-Hold ( MOH ) を有効にするように Cisco Unified Communications Manager および Cisco Unified SRST を設定する方法について説明します。この章には、次の作業が含まれています。 <ul style="list-style-type: none"> <li>• Cisco Unified SRST マルチキャスト MOH 用の Cisco Unified Communications Manager の設定 ( P.123 )</li> <li>• マルチキャスト MOH 用の Cisco Unified SRST の設定 ( P.133 )</li> <li>• Cisco Unified SRST MOH ライブフィード サポートの設定 ( オプション )( P.142 )</li> </ul>



表 1 Cisco Unified SRST の設定順序 (続き)

章または付録	説明
Secure SRST の設定	<p>SRST モードにおける Cisco IOS MGCP ゲートウェイ用の Media and Signaling Authentication and Encryption 機能について説明します。この章には、次の作業が含まれています。</p> <ul style="list-style-type: none"> <li>• 安全に通信を行うための Cisco Unified SRST ルータの準備 (P.160)</li> <li>• Secure SRST ルータへの電話機の証明書ファイル (PEM 形式) のインポート (P.169)</li> <li>• Secure Cisco Unified SRST ルータへの Cisco Unified Communications Manager の設定 (P.176)</li> <li>• Secure Cisco Unified SRST ルータでの SRST モードの有効化 (P.180)</li> <li>• 電話機のステータスおよび登録の確認 (P.182)</li> </ul>
Cisco Unified SRST へのボイスメールの統合	<p>ボイスメールの設定方法について説明します。この章には、次の作業が含まれています。</p> <ul style="list-style-type: none"> <li>• ボイスメールへのダイレクトアクセスの設定 (P.196)</li> <li>• メッセージ ボタンの設定 (P.199)</li> <li>• Cisco Unified Communications Manager ゲートウェイへのリダイレクト (P.201)</li> <li>• ボイスメールへのコール転送の設定 (P.201)</li> </ul>
Cisco Unified SRST の監視と保守	<p>Cisco Unified SRST の監視と保守に有用な show コマンドのリストを示します。</p>
E911 サービス	<p>新しい E911 サービス機能について説明します。</p>
付録 A : SIP 用の Cisco Unified SRST サポートの準備	<p>SIP コールをサポートするための特殊な設定について説明します。</p>

## 機能のロードマップ

表 2 に、Cisco Unified SRST 機能の履歴の要約を示します。

表 2 Cisco Unified SRST ソフトウェア バージョン別の機能

Cisco Unified SRST	機能拡張または変更内容
バージョン 7.0/4.3	<ul style="list-style-type: none"> <li>各ボタンでの 8 回線（八重回線）の設定（P.68）</li> <li>打診転送の設定（P.81）</li> </ul>
バージョン 4.2(1)	<p>P.229 の「E911 サービス」に、次の新機能が追加されました。</p> <ul style="list-style-type: none"> <li>ゾーンへの ERL の割り当てによる、発信者に最も近い PSAP へのルーティングの有効化</li> <li>E911 のカスタマイズ（デフォルト ELIN の定義、コールバック時に 911 発信者に到達できない場合の指定番号の設定、Last Caller テーブル内のデータの有効期限の指定、およびすべての緊急コールを通知する syslog メッセージの有効化）</li> <li>E911 ロケーション情報の拡張による名前およびアドレスの追加</li> <li>新しい永続的な呼詳細レコードの追加</li> </ul>
バージョン 4.1	E911 サービス（P.229）
バージョン 4.0	<ul style="list-style-type: none"> <li>Cisco Unified IP Phone の追加サポート（P.8）（Cisco Unified IP Phone 7960G、7911G、7941G-GE、および 7961G-GE）</li> <li>Cisco IP Communicator のサポート（P.9）</li> <li>SCCP および ATA サポートを使用した FAX パススルー（P.9）</li> <li>WAN リンク障害に対する H.323 VoIP コール プリザベーションの機能拡張（P.10）</li> <li>ビデオ サポート（P.10）</li> </ul>
バージョン 3.4	<ul style="list-style-type: none"> <li>Cisco SIP SRST 3.4（P.10）</li> </ul>
バージョン 3.3	<ul style="list-style-type: none"> <li>Secure SRST（P.11）</li> <li>Cisco Unified IP Phone 7970G および Cisco Unified 7971G-GE のサポート（P.11）</li> <li>show ephone コマンドの機能拡張（P.11）</li> </ul>
バージョン 3.2	<ul style="list-style-type: none"> <li>alias コマンドの機能拡張（P.12）</li> <li>pickup コマンドの機能拡張（P.12）</li> <li>user-locale コマンドの機能拡張（P.12）</li> <li>user-locale コマンドの機能拡張（P.12）</li> <li>Cisco 3845 でサポートされる Cisco Unified IP Phone の台数の増加（P.13）</li> <li>MOH ライブフィードのサポート（P.13）</li> <li>コール プリザベーションのタイムアウトなし（P.13）</li> <li>RFC 2833 DTMF リレーのサポート（P.13）</li> <li>変換プロファイルのサポート（P.13）</li> </ul>
バージョン 3.1	<ul style="list-style-type: none"> <li>Cisco Unified IP Phone 7920 のサポート（P.14）</li> <li>Cisco Unified IP Phone 7936 のサポート（P.14）</li> </ul>

表2 Cisco Unified SRST ソフトウェア バージョン別の機能 (続き)

Cisco Unified SRST	機能拡張または変更内容
バージョン 3.0	<ul style="list-style-type: none"> <li>• IP Phone のディスプレイに対する追加の言語オプション (P.15)</li> <li>• H.450.2 および H.450.3 を使用した打診コール転送および自動転送 (P.15)</li> <li>• Cisco Unified IP Phone 用にカスタマイズされたシステム メッセージ (P.16)</li> <li>• 二重回線モード (P.16)</li> <li>• E1 R2 シグナリングのサポート (P.16)</li> <li>• 欧州の日付形式 (P.17)</li> <li>• 二重回線モードのハントストップ (P.17)</li> <li>• フラッシュ ファイルからのマルチキャスト用の Music On Hold (P.17)</li> <li>• 呼び出しタイムアウトのデフォルト (P.18)</li> <li>• 第 2 発信音 (P.18)</li> <li>• show ephone コマンドの機能拡張 (P.18)</li> <li>• 電話機の登録に関するシステム ログ メッセージ (P.18)</li> <li>• 3 者間の G.711 Ad Hoc 会議 (P.18)</li> <li>• Cisco VG248 Analog Phone Gateway バージョン 1.2(1) 以降のバージョンのサポート (P.18)</li> </ul>
バージョン 2.1	<ul style="list-style-type: none"> <li>• Cisco Unified IP Phone 7902G のサポート (P.20)</li> <li>• Cisco Unified IP Phone 7912G のサポート (P.20)</li> </ul> <hr/> <ul style="list-style-type: none"> <li>• IP Phone のディスプレイに対する追加の言語オプション (P.19)</li> <li>• Cisco SRST の集約 (P.20)</li> <li>• Cisco ATA 186 および ATA 188 のサポート (P.20)</li> <li>• Cisco Unified IP Phone 7905G のサポート (P.20)</li> <li>• Cisco Unified IP Phone 7914 拡張モジュールのサポート (P.21)</li> <li>• dialplan-pattern コマンドの機能拡張 (P.21)</li> </ul>
バージョン 2.02	<ul style="list-style-type: none"> <li>• Cisco Unified IP Phone Conference Station 7935 のサポート (P.21)</li> <li>• 電話番号の増加 (P.22)</li> <li>• PSTN および BRI/PRI を介してインバンド DTMF シグナリングを使用した Cisco Unity ボイスメール統合 (P.22)</li> <li>• Cisco Unified SRST が Cisco Catalyst 4500 アクセス ゲートウェイ モジュールおよび Cisco 7200 ルータ (NPE-225、NPE-300、および NPE400) に実装されました。</li> <li>• Cisco MC3810-V3 コンセントレータがサポートされなくなりました。</li> </ul>
バージョン 2.01	<ul style="list-style-type: none"> <li>• Cisco Unified SRST が Cisco 1760 ルータに実装されました。また、Cisco 1750 がサポートされなくなりました。</li> <li>• 接続側の Cisco IP Phone のサポートが追加されました。</li> <li>• Cisco IP Phone の電話番号または仮想音声ポートのサポートが追加されました。</li> </ul>

表 2 Cisco Unified SRST ソフトウェア バージョン別の機能 (続き)

Cisco Unified SRST	機能拡張または変更内容
バージョン 2.0	<p data-bbox="671 306 1479 376">Cisco Unified SRST が Cisco 2600XM および Cisco 2691 ルータに実装されました。</p> <p data-bbox="671 383 1479 495">Cisco Unified SRST が Cisco IOS Release 12.2(8)T に統合され、Cisco 3725 および Cisco 3745 ルータと Cisco MC3810-V3 コンセントレータに実装されました。</p> <ul data-bbox="671 501 1479 1059" style="list-style-type: none"> <li>• Cisco Unified SRST が Cisco 1750 および Cisco 1751 ルータに実装されました。</li> <li>• ハントストップのサポート。</li> <li>• Class Of Restriction (COR; 制限クラス)。</li> <li>• 変換規則のサポート。</li> <li>• Music On Hold (MOH) と保留時のトーン。</li> <li>• 固有の呼び出し音。</li> <li>• Cisco Unified Communications Manager のフォールバック時における PSTN を介したセントラル ボイスメールまたは Auto-Attendant (AA) への自動転送。</li> <li>• Cisco Unified Communications Manager のフォールバック時における電話番号エイリアスのサポート：デフォルトの宛先サポートの拡張。</li> <li>• Cisco Unified Communications Manager のフォールバック時におけるリストベースのコール制限。</li> </ul>

表 2 Cisco Unified SRST ソフトウェア バージョン別の機能 (続き)

Cisco Unified SRST	機能拡張または変更内容
バージョン 1.0	<p data-bbox="675 309 1479 376">Cisco 3660 マルチサービス ルータで 144 台の Cisco IP Phone がサポートされるようになりました。</p> <ul style="list-style-type: none"> <li data-bbox="675 387 1479 488">• Cisco Unified SRST が、Cisco 2600 シリーズおよび Cisco 3600 シリーズ マルチサービス ルータと、Cisco IAD2420 シリーズ統合型 アクセス装置に導入されました。</li> <li data-bbox="675 499 1479 600">• Cisco Unified Communications Manager への WAN リンクに障害が発生した場合に Cisco IP Phone から SRST ルータに接続できるようになりました。</li> <li data-bbox="675 611 1479 678">• Cisco Unified SRST の動作中、サポートされない Cisco Unified IP Phone の機能キーはすべてグレー表示されるようになりました。</li> <li data-bbox="675 689 1479 712">• 内線間ダイヤル。</li> <li data-bbox="675 723 1479 757">• Direct Inward Dialing ( DID; ダイヤルイン方式 )。</li> <li data-bbox="675 768 1479 801">• Direct Outward Dialing ( DOD; ダイヤルアウト方式 )。</li> <li data-bbox="675 813 1479 846">• 発信側 ID ( Caller ID/ANI ) の表示。</li> <li data-bbox="675 857 1479 891">• 最後にかけた番号へのリダイヤル。</li> <li data-bbox="675 902 1479 936">• WAN リンクの障害時におけるローカルでの内線間コールの保持。</li> <li data-bbox="675 947 1479 1014">• WAN リンクの障害時におけるローカルでの内線と PSTN 間のコールの保持。</li> <li data-bbox="675 1025 1479 1093">• 障害が発生した WAN リンクの再確立時における進行中のコールの保持。</li> <li data-bbox="675 1104 1479 1137">• IP ネットワークにおけるコールのブラインド転送。</li> <li data-bbox="675 1149 1479 1182">• Cisco IP Phone ごとの複数回線。</li> <li data-bbox="675 1193 1479 1227">• 電話機全体での複数回線通話。</li> <li data-bbox="675 1238 1479 1272">• コール保留 ( 共有回線 )</li> <li data-bbox="675 1283 1479 1350">• アナログ Foreign Exchange Station ( FXS ) および Foreign Exchange Office ( FXO ) ポート。</li> <li data-bbox="675 1361 1479 1395">• EuroISDN の BRI サポート。</li> <li data-bbox="675 1406 1479 1440">• NET5 スイッチ タイプの PRI サポート。</li> </ul>

## Cisco Unified SRST の新機能について

ここでは、次の内容について説明します。

- [Cisco Unified SRST V4.3/7.0 の新機能 \( P.8 \)](#)
- [Cisco Unified SRST V4.2\(1\) の新機能 \( P.8 \)](#)
- [Cisco Unified SRST V4.1 の新機能 \( P.8 \)](#)
- [Cisco Unified SRST V4.0 の新機能 \( P.8 \)](#)
- [Cisco SRST V3.4 の新機能 \( P.10 \)](#)
- [Cisco SRST V3.3 の新機能 \( P.10 \)](#)
- [Cisco SRST V3.2 の新機能 \( P.12 \)](#)
- [Cisco SRST V3.1 の新機能 \( P.14 \)](#)
- [Cisco SRST V3.0 の新機能 \( P.14 \)](#)
- [Cisco SRST V2.1 の新機能 \( P.19 \)](#)
- [Cisco SRST V2.02 の新機能 \( P.21 \)](#)

### Cisco Unified SRST V4.3/7.0 の新機能

Cisco Unified SRST 7.0/4.3 では、次の新機能がサポートされています。

- [各ボタンでの 8 回線 \( 八重回線 \) の設定 \( P.68 \)](#)
- [打診転送の設定 \( P.81 \)](#)

### Cisco Unified SRST V4.2(1) の新機能

Cisco Unified SRST バージョン 4.2(1) には、次の新機能が導入されています。

- [E911 サービス \( P.229 \)](#) の機能拡張

### Cisco Unified SRST V4.1 の新機能

Cisco Unified SRST バージョン 4.1 には、次の新機能が導入されています。

- [E911 サービス \( P.229 \)](#)

### Cisco Unified SRST V4.0 の新機能

Cisco Unified SRST バージョン 4.0 には、次の新機能が導入されています。

- [Cisco Unified IP Phone の追加サポート \( P.8 \)](#)
- [Cisco IP Communicator のサポート \( P.9 \)](#)
- [SCCP および ATA サポートを使用した FAX パススルー \( P.9 \)](#)
- [WAN リンク障害に対する H.323 VoIP コール プリザベーションの機能拡張 \( P.10 \)](#)
- [ビデオサポート \( P.10 \)](#)

### Cisco Unified IP Phone の追加サポート

Cisco Unified SRST システムでは、次の IP Phone がサポートされるようになりました。

- Cisco Unified IP Phone 7911G
- Cisco Unified IP Phone 7941G および Cisco Unified IP Phone 7941G-GE

- Cisco Unified IP Phone 7960G
- Cisco Unified IP Phone 7961G および Cisco Unified IP Phone 7961G-GE

また、Cisco Unified IP Phone 7914 拡張モジュールを Cisco 7941G-GE および Cisco 7961G-GE に接続できるようになりました。Cisco 7914 拡張モジュールは新機能を備えており、たとえば、電話機に 14 のライン アピランスまたは短縮ダイヤル番号を追加します。IP Phone には拡張モジュールを 2 つまで接続できます。拡張モジュールを 2 つ使用すると、28 のライン アピランスまたは短縮ダイヤル番号が追加され、合計で 34 のライン アピランスまたは短縮ダイヤル番号が使用可能になります。詳細については、『*Cisco IP Phone 7914 Expansion Module Quick Start Guide*』を参照してください。このドキュメントは、次の URL から入手可能です。

[http://www.cisco.com/en/US/docs/voice\\_ip\\_comm/cuipph/7916/english/16enug.pdf](http://www.cisco.com/en/US/docs/voice_ip_comm/cuipph/7916/english/16enug.pdf)

これらの電話機に対して追加の SRST 設定を行う必要はありません。

`show ephone` コマンドは、SRST バージョン 4.0 に追加された新しい Cisco IP Phone の設定およびステータスを表示するように拡張されています。詳細については、『*Cisco Unified SRST and Cisco Unified SIP SRST Command Reference (All Versions)*』に記載されている `show ephone` コマンドを参照してください。このドキュメントは、次の URL から入手可能です。

[http://www.cisco.com/en/US/docs/voice\\_ip\\_comm/cusrst/command/reference/srstcr.html](http://www.cisco.com/en/US/docs/voice_ip_comm/cusrst/command/reference/srstcr.html)

Cisco Unified SRST 4.0 に関連する、互換性のあるファームウェア、プラットフォーム、メモリ、および追加の音声製品を確認するには、次のマニュアルを参照してください。

『*Cisco Unified SRST 4.3 Supported Firmware, Platforms, Memory, and Voice Products*』(このドキュメントは、次の URL から入手可能です)

[http://www.cisco.com/en/US/docs/voice\\_ip\\_comm/cusrst/requirements/guide/srs43spc.html](http://www.cisco.com/en/US/docs/voice_ip_comm/cusrst/requirements/guide/srs43spc.html)

## Cisco IP Communicator のサポート

Cisco IP Communicator は、パーソナル コンピュータでのテレフォニー サポートを拡張するソフトウェアベースのアプリケーションです。この SCCP ベースのアプリケーションを使用すると、コンピュータを IP Phone として機能させることができます。その結果、出先やオフィスなど、ユーザが企業ネットワークにアクセスできる場所であればどこからでも高品質の音声コールを利用できるようになります。Cisco IP Communicator は、カラー画面、キーパッド、機能ボタン、およびソフトウェアを備えたグラフィカルな表示ベースの IP Phone として、ユーザのコンピュータ画面に表示されます。

## SCCP および ATA サポートを使用した FAX パススルー

Cisco VG 224 音声ゲートウェイ、Analog Telephone Adaptor (ATA; アナログ電話アダプタ)、および SCCP を使用した FAX パススルー モードがサポートされました。ATA は SIP ファームウェアに付属しています。そのため、この機能を使用するには SCCP ファームウェアをロードする必要があります。



(注)

Cisco Unified SRST システムに登録されている ATA が FAX コールに参加できるようにするには、FAX パススルー モードで RTP ペイロード タイプとして「標準のペイロード タイプ 0/8」を使用するように、ATA の ConnectMode パラメータを設定する必要があります。Cisco Unified SRST 4.0 以降のバージョンで使用する ATA に対してこのように設定するには、ATA において ConnectMode パラメータのビット 2 を 1 に設定します。詳細については、『*Cisco ATA 186 and Cisco ATA 188 Analog Telephone Adaptor Administrator's Guide for SCCP*』の「Parameters and Defaults」の章を参照してください。このドキュメントは、次の URL から入手可能です。

[http://www.cisco.com/en/US/docs/voice\\_ip\\_comm/cata/186\\_188/2\\_15\\_ms/english/administration/guide/sccp/sccpach5.html](http://www.cisco.com/en/US/docs/voice_ip_comm/cata/186_188/2_15_ms/english/administration/guide/sccp/sccpach5.html)

## WAN リンク障害に対する H.323 VoIP コール プリザベーションの機能拡張

WAN リンク障害に対する H.323 VoIP コール プリザベーションの機能拡張では、Cisco Unified Communications Manager などのエンティティによってシグナリングが処理される H.323 トポロジの接続が保持されるようになりました。このエンティティは、2 つの接続側の間でシグナリングを行う相手方エンドポイントおよびブローカとは異なります。

コール プリザベーションが有用になるのは、ゲートウェイと相手方エンドポイント（通常は Cisco Unified IP Phone）が同じサイトに配置され、コール エージェントがリモート側に配置されているために、接続障害の発生する確率が高くなっている場合です。

詳細については、『[Cisco IOS H.323 Configuration Guide](#), Release 12.4T』の「Configuring H.323 Gateways」の章を参照してください。

## ビデオ サポート

この機能を使用すると、Cisco Unified SRST が Cisco Unified Communications Manager と同等の機能を保持するように、ビデオ パラメータを設定できます。Cisco Unified SRST が有効になっている場合、ビデオ機能に関して Cisco Unified IP Phone を再設定する必要はありません。これは、すべての ephone が、Cisco Unified Communications Manager に対して使用される同一の設定を保持するためです。ただし、call-manager-fallback コンフィギュレーション モードを開始して、Cisco Unified SRST のビデオ パラメータを設定する必要があります。ビデオ用の機能セットは、Cisco Unified SRST オーディオ コールの場合と同じです。

詳細については、[P.211](#) の「[ビデオ パラメータの設定](#)」を参照してください。

## Cisco SRST V3.4 の新機能

Cisco SRST V3.4 には、次の項で説明する新機能が導入されています。

- [Cisco SIP SRST 3.4](#)

### Cisco SIP SRST 3.4

Cisco SIP SRST バージョン 3.4 では、Session Initiation Protocol (SIP) ネットワークの SRST 機能について説明します。Cisco SIP SRST バージョン 3.4 は、基本的なレジストラ サービスと Back-To-Back User Agent (B2BUA; バックツーバック ユーザ エージェント) サービスを提供して、外部の SIP プロキシ サーバへのバックアップを行います。このサービスは、WAN 接続が停止して SIP IP Phone がプライマリ SIP プロキシと通信できなくなった場合に、その SIP 電話機によって使用されます。

Cisco SIP SRST バージョン 3.4 では、ローカルおよび SIP WAN ネットワーク全体で、標準の RFC 3261 機能サポートに基づいて SIP 電話機をサポートすることができます。Cisco SIP SRST バージョン 3.4 を使用すると、Skinny Client Control Protocol (SCCP) 電話機と同じ方法で、SIP 電話機から SIP ネットワークを介してコールを発信できます。SIP SRST バージョン 3.4 の詳細については、『[Cisco SIP SRST Version 3.4 System Administrator Guide](#)』を参照してください。

## Cisco SRST V3.3 の新機能

Cisco SRST V3.3 には、次の項で説明する新機能が導入されています。

- [Secure SRST \(P.11\)](#)
- [Cisco Unified IP Phone 7970G および Cisco Unified 7971G-GE のサポート \(P.11\)](#)
- [show ephone コマンドの機能拡張 \(P.11\)](#)



## Secure SRST

リモートサイトに配置され、ゲートウェイ ルータに接続されている安全な Cisco IP Phone は、WAN を使用して Cisco Unified Communications Manager と安全に通信することができます。ただし、WAN リンクまたは Cisco Unified Communications Manager がダウンした場合、リモート電話機からの通信はすべて保護されていない状態になります。この状況に対処するために、ゲートウェイ ルータは Secure SRST モードで機能できるようになっています。このモードは、WAN リンクまたは Cisco Unified Communications Manager がダウンした場合にアクティブになります。WAN リンクまたは Cisco Unified Communications Manager が回復すると、Cisco Unified Communications Manager は、安全なコール処理機能を再開します。

Secure SRST は、認証、保全性、およびメディア暗号化など、新しい SRST セキュリティ機能を提供します。認証は、ユーザに対して、通話相手の身元が正しいことを保証します。保全性は、特定のデータがエンティティ間で変更されていないことを保証します。暗号化は機密性を意味します。つまり、対象となる受信者以外の人にはデータを読み取れないということです。これらのセキュリティ機能を使用すると、SRST 音声コールのプライバシーが確保され、音声のセキュリティ侵害や ID 盗難から保護されます。詳細については、P.151 の「Secure SRST の設定」を参照してください。

## Cisco Unified IP Phone 7970G および Cisco Unified 7971G-GE のサポート

Cisco Unified IP Phone 7970G および 7971G-GE は、IP ネットワークを介して音声通信を行うフル装備の電話機です。これらの電話機は従来のアナログ電話機と同じように機能するため、電話コールの発信と受信のほか、消音、保留、コール転送、短縮ダイヤル、および自動転送などの機能を利用できます。また、データ ネットワークに接続されるため、拡張 IP テレフォニー機能を利用して、たとえば、ネットワーク情報およびサービスのほか、カスタマイズ可能な機能およびサービスにアクセスすることができます。さらに、ファイル認証、デバイス認証、シグナリング暗号化、およびメディア暗号化などのセキュリティ機能もサポートしています。

Cisco Unified IP Phone 7970G および 7971G-GE は、また、カラー タッチスクリーン、最大 8 つの回線番号または短縮ダイヤル番号のサポート、およびボタンや機能に関する文脈依存オンラインヘルプなど、各種の高度な機能を備えています。SRST に固有の設定を行う必要はありません。

詳細については、[Cisco Unified IP Phone 7900 シリーズ マニュアル](#)を参照してください。



(注) Cisco Unified IP Phone 7970G および 7971G-GE には、Cisco Unified IP Phone 7914 拡張モジュールを接続できます。詳細については、P.21 の「Cisco Unified IP Phone 7914 拡張モジュールのサポート」を参照してください。

## show ephone コマンドの機能拡張

show ephone コマンドは、Cisco Unified IP Phone 7970G および Cisco Unified IP Phone 7971G-GE の設定およびステータスを表示するように拡張されています。詳細については、『[Cisco Unified SRST and Cisco Unified SIP SRST Command Reference \(All Versions\)](#)』に記載されている show ephone コマンドを参照してください。このドキュメントは、次の URL から入手可能です。

[http://www.cisco.com/en/US/docs/voice\\_ip\\_comm/cusrst/command/reference/srster.html](http://www.cisco.com/en/US/docs/voice_ip_comm/cusrst/command/reference/srster.html)

## Cisco SRST V3.2 の新機能

Cisco SRST V3.2 には、次の項で説明する新機能が導入されています。

- [alias コマンドの機能拡張 \(P.12\)](#)
- [cor コマンドの機能拡張 \(P.12\)](#)
- [pickup コマンドの機能拡張 \(P.12\)](#)
- [user-locale コマンドの機能拡張 \(P.12\)](#)
- [Cisco 3845 でサポートされる Cisco Unified IP Phone の台数の増加 \(P.13\)](#)
- [MOH ライブフィードのサポート \(P.13\)](#)
- [コールプリゼーションのタイムアウトなし \(P.13\)](#)
- [RFC 2833 DTMF リレーのサポート \(P.13\)](#)
- [変換プロファイルのサポート \(P.13\)](#)

### alias コマンドの機能拡張

alias コマンドは、次のように拡張されています。

- *cfw* キーワードが追加されました。このキーワードは、無応答時または話中時の自動転送機能を提供します。
- Cisco Unified Communications Manager のフォールバック時に使用不能になる電話番号へのコールを作成するために使用される **alias** コマンドの最大数が 50 に増えました。
- 複数の **alias** コマンドで *alternate-number* 引数を使用できるようになりました。

詳細については、『[Cisco Unified SRST and Cisco Unified SIP SRST Command Reference \(All Versions\)](#)』に記載されている **alias** コマンドを参照してください。このドキュメントは、次の URL から入手可能です。[http://www.cisco.com/en/US/docs/voice\\_ip\\_comm/cusrst/command/reference/srstcr.html](http://www.cisco.com/en/US/docs/voice_ip_comm/cusrst/command/reference/srstcr.html)

### cor コマンドの機能拡張

cor リストの最大数が 20 に増えました。

詳細については、『[Cisco Unified SRST and Cisco Unified SIP SRST Command Reference \(All Versions\)](#)』に記載されている **cor** コマンドを参照してください。このドキュメントは、次の URL から入手可能です。[http://www.cisco.com/en/US/docs/voice\\_ip\\_comm/cusrst/command/reference/srstcr.html](http://www.cisco.com/en/US/docs/voice_ip_comm/cusrst/command/reference/srstcr.html)

### pickup コマンドの機能拡張

**pickup** コマンドは、すべての Cisco Unified IP Phone で PickUp ソフトキーを有効にするために導入されています。このソフトキーを使用すると、SRST の動作中に、特定の外線番号に着信した外部のダイヤルイン (DID) コールを別の外線番号からピックアップできます。

詳細については、『[Cisco Unified SRST and Cisco Unified SIP SRST Command Reference \(All Versions\)](#)』に記載されている **pickup** コマンドを参照してください。このドキュメントは、次の URL から入手可能です。[http://www.cisco.com/en/US/docs/voice\\_ip\\_comm/cusrst/command/reference/srstcr.html](http://www.cisco.com/en/US/docs/voice_ip_comm/cusrst/command/reference/srstcr.html)

### user-locale コマンドの機能拡張

**user-locale** コマンドは、日本語のカタカナ国コードを表示するために導入されています。日本語のカタカナは、Cisco Unified Communications Manager V4.0 以降のバージョンで使用できます。

詳細については、『[Cisco Unified SRST and Cisco Unified SIP SRST Command Reference \(All Versions\)](#)』に記載されている `user-locale` コマンドを参照してください。このドキュメントは、次の URL から入手可能です。[http://www.cisco.com/en/US/docs/voice\\_ip\\_comm/cusrst/command/reference/srstcr.html](http://www.cisco.com/en/US/docs/voice_ip_comm/cusrst/command/reference/srstcr.html)

## Cisco 3845 でサポートされる Cisco Unified IP Phone の台数の増加

Cisco 3845 では、720 台の電話機と最大 960 の ephone-dn または仮想音声ポートがサポートされるようになりました。詳細については、『[Cisco IOS Survivable Remote Site Telephony \(SRST\) 3.2 Specifications for Cisco IOS Software Release 12.3\(11\)T](#)』を参照してください。

## MOH ライブフィードのサポート

Cisco Unified SRST には、機能拡張として新しい `moh-live` コマンドが追加されました。`moh-live` コマンドは、E&M または FXO ポートに接続されたオーディオ デバイスから SRST モードの Cisco IP Phone に対して、ライブ フィード MOH ストリームを提供します。ライブ フィードに FXO ポートを使用する場合、ポートには、バッテリー供給を行う外部のサードパーティ製アダプタを接続する必要があります。ライブ フィードの音楽は、フラッシュ ファイルから読み込まれるのではなく、固定のソースから取得され、MOH 再生バッファに連続的に送られます。ライブ フィード MOH は、Cisco IP Phone に対してマルチキャストを行うこともできます。設定手順については、[P.115 の「Cisco Unified SRST をマルチキャスト MOH リソースとして使用するための Cisco Unified Communications Manager と Cisco Unified SRST の統合」](#)を参照してください。

## コール プリザベーションのタイムアウトなし

停止時にブランチで既存の H.323 コールが保持されるようにするには、`no h225 timeout keepalive` コマンドを入力して、H.225 キープアライブ タイマーを無効にします。この機能は、Cisco IOS Release 12.3(7)T1 以降のバージョンでサポートされています。詳細については、[P.26 の「Cisco Unified SRST の説明」](#)を参照してください。

## RFC 2833 DTMF リレーのサポート

Cisco Skinny Client Control Protocol (SCCP) 電話機 (Cisco SRST システムで使用される電話機など) は、アウトオブバンド DTMF デジタル表示だけをサポートします。SCCP 電話機からリモートの SIP ベース IVR アプリケーションおよびボイスメール アプリケーションにデジタル情報を送信できるようにするには、Cisco SRST 3.2 以降のバージョンで、アウトオブバンド SCCP デジタル表示から DTMF リレー用 SIP 標準 (RFC 2833) への変換を行います。この方法を SIP VoIP ダイアル ピアで選択するには、`dtmf-relay rtp-nte` コマンドを使用します。設定手順については、[P.265 の「付録 A : SIP 用の Cisco Unified SRST サポートの準備」](#)を参照してください。

Cisco Unity Express システムに接続している SIP ネットワーク上のボイスメールを使用するには、非標準の SIP Notify 形式を使用します。Notify 形式を設定するには、`dtmf-relay` コマンドで `sip-notify` キーワードを使用します。`sip-notify` キーワードの使用は、Cisco SRST 3.0 および 3.1 との下位互換性のために必要になる場合があります。

## 変換プロファイルのサポート

Cisco SRST 3.2 以降のバージョンは、変換プロファイルをサポートしています。変換プロファイルを使用すると、変換規則をグループ化して、次の要素と関連付けることができます。

- 着信番号
- 発信番号

- リダイレクトされる着信番号

設定の詳細については、P.86 の「変換プロファイルの有効化」を参照してください。

`translation-profile` コマンドの詳細については、『*Cisco Unified SRST and Cisco Unified SIP SRST Command Reference (All Versions)*』を参照してください。このドキュメントは、次の URL から入手可能です。 [http://www.cisco.com/en/US/docs/voice\\_ip\\_comm/cusrst/command/reference/srstcr.html](http://www.cisco.com/en/US/docs/voice_ip_comm/cusrst/command/reference/srstcr.html)

## Cisco SRST V3.1 の新機能

Cisco SRST V3.1 には、次の項で説明する新機能が導入されています。

- [Cisco Unified IP Phone 7920 のサポート \(P.14\)](#)
- [Cisco Unified IP Phone 7936 のサポート \(P.14\)](#)



(注)

Cisco Unified IP Phone については、[Cisco Unified IP Phone 7900 シリーズ マニュアル](#)を参照してください。

## Cisco Unified IP Phone 7920 のサポート

Cisco Unified Wireless IP Phone 7920 は、使いやすい IEEE 802.11b 準拠の無線 IP Phone で、Cisco Unified Communications Manager および Cisco Aironet 1200、1100、350、340 シリーズの Wi-Fi (IEEE 802.11b) アクセス ポイントと連携して、総合的な音声通信を実現します。この電話機は、Cisco AVVID Wireless Solution の主要部分として、エンドツーエンドの Cisco ネットワークを介して、セキュリティ、モビリティ、QoS (Quality Of Service)、および管理などのシームレスなインテリジェント サービスを提供します。

設定を行う必要はありません。

## Cisco Unified IP Phone 7936 のサポート

Cisco Unified IP Conference Station 7936 は、VoIP テクノロジーを使用した IP ベースでハンドフリーの電話会議用端末です。IP Conference Station は、従来のアナログ会議装置に置き換わるもので、IP ネットワークを介してビジネス会議機能 (コール保留、コール再開、コール転送、コール リリース、リダイヤル、消音、および会議など) を提供します。

設定を行う必要はありません。

## Cisco SRST V3.0 の新機能

Cisco SRST V3.0 には、次の項で説明する新機能が導入されています。

- [IP Phone のディスプレイに対する追加の言語オプション \(P.15\)](#)
- [H.450.2 および H.450.3 を使用した打診コール転送および自動転送 \(P.15\)](#)
- [Cisco Unified IP Phone 用にカスタマイズされたシステム メッセージ \(P.16\)](#)
- [二重回線モード \(P.16\)](#)
- [E1 R2 シグナリングのサポート \(P.16\)](#)
- [欧州の日付形式 \(P.17\)](#)
- [二重回線モードのハントストップ \(P.17\)](#)
- [フラッシュ ファイルからのマルチキャスト用の Music On Hold \(P.17\)](#)
- [呼び出しタイムアウトのデフォルト \(P.18\)](#)

- 第 2 発信音 ( P.18 )
- show ephone コマンドの機能拡張 ( P.18 )
- 電話機の登録に関するシステム ログ メッセージ ( P.18 )
- 3 者間の G.711 Ad Hoc 会議 ( P.18 )
- Cisco VG248 Analog Phone Gateway バージョン 1.2(1) 以降のバージョンのサポート ( P.18 )

## IP Phone のディスプレイに対する追加の言語オプション

Cisco Unified IP Phone 7940G および Cisco Unified IP Phone 7960G のディスプレイには、ドイツ語、デンマーク語、スペイン語、フランス語、イタリア語、日本語、オランダ語、ノルウェー語、ポルトガル語、ロシア語、スウェーデン語、および英語に対応する追加の ISO-3166 コードを設定できます。



(注) この機能が使用可能になるのは、Cisco SRST が Cisco Unified Communications Manager V3.2 の下で動作している場合のみです。

## H.450.2 および H.450.3 を使用した打診コール転送および自動転送

Cisco SRST V1.0、Cisco SRST V2.0、および Cisco SRST V2.1 を使用すると、ブラインド コール転送および自動転送を行うことができます。ブラインド コールでは、コール転送元および自動転送元は、転送先に対して通知または打診を行うことはできません。これら 3 つのバージョンの Cisco SRST は、Cisco SRST 独自のメカニズムを使用して、ブラインド転送を実行します。Cisco SRST V3.0 には、ITU-T H.450.2 ( H.450.2 ) 標準を使用した打診によるコール転送と、ITU-T H.450.3 ( H.450.3 ) 標準を使用した自動転送を H.323 コールに対して実行する機能が追加されています。

Cisco SRST V3.0 では、IP Phone でデフォルト セッション アプリケーションを使用して、H.450.2 および H.450.3 を使用したコール転送および自動転送を開始することがサポートされています。デフォルト セッション アプリケーションによって提供される組み込みの H.450.2 および H.450.3 サポートは、PSTN インターフェイスのタイプに関係なく、IP Phone で開始されるコール転送および自動転送に適用されます。

打診転送を使用できるようにするには、Cisco SRST ルータに二重回線モードを設定する必要があります。P.66 の「二重回線電話機の設定」を参照してください。



(注) VoIP ネットワーク内の音声ゲートウェイ ルータはすべて、H.450 をサポートしている必要があります。H.450 をサポートする場合、Cisco SRST を使用するルータでは、Cisco SRST V3.0 以降のバージョンまたは Cisco IOS Release 12.2(15)ZJ 以降のリリースを実行する必要があります。Cisco SRST を使用しないルータでは、Cisco SRST V2.1 以降のバージョンまたは Cisco IOS Release 12.2(11)YT 以降のリリースを実行する必要があります。

デフォルト セッション アプリケーションの詳細については、『[Default Session Application Enhancements](#)』を参照してください。

設定については、P.93 の「Cisco SRST 3.0 での H.450.2 および H.450.3 を使用した打診コール転送および自動転送」を参照してください。

## Cisco Unified IP Phone 用にカスタマイズされたシステム メッセージ

フォールバック モードの Cisco Unified IP Phone 7905G、Cisco Unified IP Phone 7940G、Cisco Unified IP Phone 7960G、および Cisco Unified IP Phone 7910 ユニットに表示されるディスプレイ メッセージは、カスタマイズできます。新しい `system message` コマンドを使用すると、このディスプレイ メッセージをルータごとに編集できます。カスタム システム メッセージ機能では、英語だけがサポートされています。

詳細については、P.65 の「Cisco Unified IP Phone 用にカスタマイズされたシステム メッセージの設定」を参照してください。

## 二重回線モード

`max-dn` コマンドに追加された新しいキーワードを使用すると、IP Phone を二重回線モードに設定できます。二重回線 IP Phone はそれぞれ、1 つの音声ポートと、2 つの独立したコールを処理する 2 つのチャネルを備えている必要があります。このモードでは、1 つの `ephone-dn` (`ephone` の電話番号) で、コール ウェイティング、コール転送、および会議の各機能を使用できます。Cisco SRST フォールバック時に使用できる DN の数には上限があります。`max-dn` コマンドは、Cisco SRST ルータ上のすべての IP Phone に影響します。

設定については、P.66 の「二重回線電話機の設定」を参照してください。

## E1 R2 シグナリングのサポート

Cisco SRST V3.0 は、E1 R2 シグナリングをサポートしています。R2 シグナリングは、チャンネル化 E1 ネットワークに共通の国際的なシグナリング標準です。ただし、R2 に関する単一のシグナリング標準はありません。R2 は ITU-T Q.400-Q.490 勧告で定義されていますが、まったく異なる方法で R2 を実装している国と地域が数多く存在します。シスコシステムズでは、この問題に対処するため、Cisco IOS ソフトウェアにおいて R2 シグナリングのローカライズされた実装を数多くサポートしています。

シスコシステムズの E1 R2 シグナリングのデフォルトは ITU です。ITU は、デンマーク、フィンランド、ドイツ、ロシア (ITU バリエーション)、香港 (ITU バリエーション)、および南アフリカ (ITU バリエーション) の各国をサポートしています。「ITU バリエーション」という表現は、指定の国に複数の R2 シグナリング タイプが存在することを意味します。ただし、シスコでは ITU バリエーションをサポートしています。

また、シスコシステムズでは、次の国、地域、および企業における E1 R2 シグナリングの特定のローカル バリエーションもサポートしています。

- アルゼンチン
- オーストラリア
- ボリビア
- ブラジル
- ブルガリア
- 中国
- コロンビア
- コスタリカ
- 東欧 (クロアチア、ロシア、およびスロバキア共和国など)
- エクアドル (ITU)
- エクアドル (LME)
- ギリシャ

- グアテマラ
- 香港（中国のバリエーションを使用）
- インドネシア
- イスラエル
- 韓国
- ラオス
- マレーシア
- マルタ
- ニュージーランド
- パラグアイ
- ベルギー
- フィリピン
- サウジアラビア
- シンガポール
- 南アフリカ（Panafel のバリエーション）
- Telmex 社（メキシコ）
- Telnor 社（メキシコ）
- タイ
- ウルグアイ
- ベネズエラ
- ベトナム

## 欧州の日付形式

Cisco IP Phone のディスプレイの日付形式には、次の 2 つの追加形式を設定できます。

- yy-mm-dd ( year-month-day )
- yy-dd-mm ( year-day-month )

設定については、[P.62 の「IP Phone のクロック、日付、および時刻の形式の設定」](#)を参照してください。

## 二重回線モードのハントストップ

**huntstop** コマンドには、新しいキーワードが追加されています。**channel** キーワードを使用すると、プライマリ回線が通話中または無応答の場合に、二重回線設定におけるセカンダリ チャネルのハンティングがスキップされます。

設定については、[P.89 の「ダイヤル ピアとチャネルのハンティングの設定」](#)を参照してください。

## フラッシュ ファイルからのマルチキャスト用の Music On Hold

Cisco SRST は、Music On Hold ( MOH ) をフラッシュ メモリ内のフラッシュ MOH ファイルから連続的にマルチキャスト出力することをサポートするように設定できます。

詳細については、[P.113 の「XML API スキーマの定義」](#)を参照してください。

## 呼び出しタイムアウトのデフォルト

呼び出しタイムアウトのデフォルトは、無応答時の自動転送が有効になっていない内線番号に対して設定できます。タイムアウトが発生すると、着信コールが発信者に接続解除コードを返します。このメカニズムにより、自動転送と接続解除を監視しない Foreign Exchange Office (FXO) などのインターフェイスを介して受信された着信コールが呼び出し中のままになることが防止されます。詳細については、P.91 の「呼び出しタイムアウトのデフォルトの設定」を参照してください。

## 第 2 発信音

第 2 発信音は、Cisco SRST を実行している Cisco Unified IP Phone で使用できます。第 2 発信音が生成されるのは、ユーザが定義済みの PSTN アクセス プレフィックスをダイヤルしたときです。たとえば、外線に接続するために指定番号を押すと、別のダイヤルトーンが聞こえます。

第 2 発信音を作成するには、secondary-dialtone コマンドを使用します。詳細については、P.66 の「第 2 発信音の設定」を参照してください。

## show ephone コマンドの機能拡張

show ephone コマンドは、次の情報を表示するように拡張されています。

- 追加の電話機の設定およびステータス (新しいキーワード: 7905、7914、7935、ATA)
- 1 つ以上の DN で Call-Forwarding All (CFA) 機能が有効になっているすべての電話機のステータス (新しいキーワード: cfa)

詳細については、『Cisco Unified SRST and Cisco Unified SIP SRST Command Reference (All Versions)』に記載されている show ephone コマンドを参照してください。このドキュメントは、次の URL から入手可能です。[http://www.cisco.com/en/US/docs/voice\\_ip\\_comm/cusrst/command/reference/srstcr.html](http://www.cisco.com/en/US/docs/voice_ip_comm/cusrst/command/reference/srstcr.html)

## 電話機の登録に関するシステム ログ メッセージ

電話機が Cisco SRST に対して登録または登録解除された場合は必ず、システム ログに診断メッセージが追加されます。

## 3 者間の G.711 Ad Hoc 会議

Cisco SRST は、G.711 符号化技術を使用した 3 者間の Ad Hoc 会議をサポートしています。会議を使用できるようにするには、IP Phone の 1 つ以上のボタンに 2 つ以上の回線を接続する必要があります。

詳細については、P.112 の「3 者間 G.711 Ad Hoc 会議の有効化」を参照してください。

## Cisco VG248 Analog Phone Gateway バージョン 1.2(1) 以降のバージョンのサポート

Cisco VG248 Analog Phone Gateway は、Cisco AVVID( Architecture for Voice, Video and Integrated Data ) によって実現された混合環境ソリューションです。このソリューションを使用すると、企業は、従来のアナログ デバイスをサポートする一方で、IP テレフォニーを使用して得られる新たな機会を活用することができます。Cisco VG248 は、Cisco Unified Communications Manager をベースにした企業の音声システムにおいてアナログ電話機、FAX マシン、モデム、ボイスメール システム、およびスピーカフォンを使用するための高密度ゲートウェイです。



Cisco Unified Communications Manager のフォールバック中、Cisco SRST は Cisco VG248 を Cisco Unified IP Phone のグループと見なします。Cisco Unified SRST は、Cisco VG248 の 48 個のポートそれぞれを個別の Cisco Unified IP Phone と見なします。Cisco VG248 バージョン 1.2(1) 以降のバージョンのサポートは、Cisco Unified SRST バージョン 2.1 でも利用できます。

詳細については、『[Cisco VG248 Analog Phone Gateway Data Sheet](#)』および『[Cisco VG248 Analog Phone Gateway Version 1.2\(1\) Release Notes](#)』を参照してください。

## Cisco SRST V2.1 の新機能

Cisco SRST V2.1 には、次の項で説明する新機能が導入されています。

- [IP Phone のディスプレイに対する追加の言語オプション \(P.19\)](#)
- [Cisco SRST の集約 \(P.20\)](#)
- [Cisco ATA 186 および ATA 188 のサポート \(P.20\)](#)
- [Cisco Unified IP Phone 7902G のサポート \(P.20\)](#)
- [Cisco Unified IP Phone 7905G のサポート \(P.20\)](#)
- [Cisco Unified IP Phone 7912G のサポート \(P.20\)](#)
- [Cisco Unified IP Phone 7914 拡張モジュールのサポート \(P.21\)](#)
- [dialplan-pattern コマンドの機能拡張 \(P.21\)](#)



(注)

Cisco Unified IP Phone については、[Cisco Unified IP Phone 7900 シリーズ マニュアル](#)を参照してください。

## IP Phone のディスプレイに対する追加の言語オプション

Cisco Unified IP Phone 7940G および Cisco Unified IP Phone 7960G のディスプレイには、次の各国に対応する ISO-3166 コードを設定できます。

- フランス
- ドイツ
- イタリア
- ポルトガル
- スペイン
- 米国



(注)

この機能が使用可能になるのは、Cisco SRST が Cisco Unified Communications Manager V3.2 の下で動作している場合のみです。

設定については、[P.63 の「IP Phone の言語表示の設定」](#)を参照してください。

## Cisco SRST の集約

Cisco Unified Communications Manager 3.3(2) 以降を実行するシステムでは、デフォルト ゲートウェイ上で Cisco SRST を実行する際の制限がなくなりました。複数の SRST ルータを使用して、追加の電話機をサポートすることができます。コール転送と自動転送を正しく機能させるには、ダイヤルピアとダイヤルプランを慎重に計画し、設定する必要があります。

## Cisco ATA 186 および ATA 188 のサポート

Cisco ATA アナログ電話アダプタは、受話器とイーサネット間のアダプタで、このアダプタを使用すると、標準のアナログ電話機を IP ベースのテレフォニー ネットワーク上で動作させることができます。Cisco ATA は、別々の電話番号が割り当てられた 2 つの音声ポートをサポートしています。Cisco ATA 188 には、RJ-45 10/100BASE-T データ ポートも搭載されています。Cisco SRST は、音声コールに対して、Skinny Client Control Protocol (SCCP) を使用した Cisco ATA 186 および Cisco ATA 188 のみをサポートしています。

## Cisco Unified IP Phone 7902G のサポート

Cisco Unified IP Phone 7902G は、エントリレベルの IP Phone であり、ロビー、研究室、製造フロア、および通路など、基本的なコール機能だけが求められるエリアでの音声通信ニーズに対応しています。

この電話機は、リダイヤル、コール転送、会議、およびボイスメール アクセスの各機能にワンタッチでアクセスできる固定の機能キーを備えた単一回線 IP Phone です。他の Cisco IP Phone と同様に、Cisco Unified IP Phone 7902G もインライン パワーをサポートしています。インライン パワーを使用すると、電話機が LAN 経由で電力を受信できるようになります。この機能により、ネットワーク管理者は電力を集中制御できるため、ネットワークのオペラビリティが向上します。

## Cisco Unified IP Phone 7905G のサポート

Cisco Unified IP Phone 7905G は、中核的なビジネス機能を備えた基本的な IP Phone です。この電話機は、単一回線へのアクセスを提供するほか、ピクセルベースの Liquid Crystal Display (LCD; 液晶ディスプレイ) を通してユーザにコール機能の操作方法を案内する 4 つの対話型ソフトキーを備えています。将来のファームウェア リリースでは、ディスプレイのグラフィック機能によって、コール情報を表示したり、機能に直感的にアクセスしたり、言語をローカライズしたりできるようになります。Cisco Unified IP Phone 7905G は、インライン パワーをサポートしています。インライン パワーを使用すると、電話機が LAN 経由で電力を受信できるようになります。

設定を行う必要はありません。

## Cisco Unified IP Phone 7912G のサポート

Cisco Unified IP Phone 7912G は、中核的なビジネス機能を備えており、利用する電話トラフィック量が中程度までのパーティション内作業員に対応しています。4 つの動的なソフトキーを使用して、各種のコール機能にアクセスすることができます。グラフィック ディスプレイでは、コール情報を表示することや、機能にアクセスすることができます。

Cisco Unified IP Phone 7912G は、統合イーサネット スイッチをサポートし、ローカル PC への LAN 接続を提供します。また、この電話機は、インライン パワーをサポートしています。インライン パワーを使用すると、電話機が LAN 経由で電力を受信できるようになります。この機能により、ネットワーク管理者は電力を集中制御できるため、ネットワークのオペラビリティが向上します。インライン パワーとイーサネット スイッチのサポートを組み合わせることで、必要なケーブル配線を減らして、デスクトップへのワイヤ 1 本だけで済ませることができます。

## Cisco Unified IP Phone 7914 拡張モジュールのサポート

Cisco Unified IP Phone 7914 拡張モジュールは、Cisco Unified IP Phone 7960G に接続され、電話機に 14 のライン アピアランスまたは短縮ダイヤル番号を追加します。IP Phone には拡張モジュールを 2 つまで接続できます。拡張モジュールを 2 つ使用すると、28 のライン アピアランスまたは短縮ダイヤル番号が追加され、合計で 34 のライン アピアランスまたは短縮ダイヤル番号が使用可能になります。

## dialplan-pattern コマンドの機能拡張

dialplan-pattern コマンドには、新しいキーワードが追加されています。extension-pattern キーワードは、内線番号の先頭番号が、pattern 変数で定義された E.164 電話番号の先頭番号と異なる場合に、内線番号の先頭番号のパターンを設定します。この拡張により、IP Phone の省略された内線番号のプレフィックス番号を操作できるようになります。『Cisco Unified SRST and Cisco Unified SIP SRST Command Reference (All Versions)』に記載されている dialplan-pattern コマンドを参照してください。このドキュメントは、次の URL から入手可能です。

[http://www.cisco.com/en/US/docs/voice\\_ip\\_comm/cusrst/command/reference/srster.html](http://www.cisco.com/en/US/docs/voice_ip_comm/cusrst/command/reference/srster.html)

## Cisco SRST V2.02 の新機能

Cisco SRST バージョン 2.02 には、次の項で説明する新機能が導入されています。

- [Cisco Unified IP Phone Conference Station 7935 のサポート \(P.21\)](#)
- [電話番号の増加 \(P.22\)](#)
- [PSTN および BRI/PRI を介してインバンド DTMF シグナリングを使用した Cisco Unity ボイスメール統合 \(P.22\)](#)

## Cisco Unified IP Phone Conference Station 7935 のサポート

Cisco IP Conference Station 7935 は、IP ベースの全二重方式でハンドフリーの電話会議用端末で、デスクトップやオフィス、および中小規模の会議室で使用されます。このデバイスは、シンプルな RJ-45 接続によって Cisco Catalyst 10/100 イーサネット スイッチ ポートに接続され、DHCP を介して IP ネットワークにデバイス自体が動的に設定されます。Cisco 7935 をイーサネット スイッチ ポートに接続する作業を除き、管理作業を行う必要はありません。Cisco 7935 は、接続サービスのために Cisco Unified Communications Manager に動的に登録して、適切なエンドポイント電話番号のほか、Cisco Unified Communications Manager に組み込まれているソフトウェア拡張機能や個人用設定をすべて受信します。

Cisco Unified IP Phone 7935 は、ユーザーにコール機能の操作方法を案内する 3 つのソフトキーとメニュー ナビゲーション キーを備えています。また、この電話機はピクセルベースの LCD ディスプレイも備えています。ディスプレイには、日付と時刻、発信側の名前、発信側の番号、ダイヤルされた番号、機能、および回線状況などが表示されます。

設定を行う必要はありません。

## 電話番号の増加

表 3 に示すとおり、ルータの電話番号が増えました。

表 3 Cisco IOS Release 12.2(11)T における電話番号の増加

Cisco ルータ	電話機の最大数	電話番号の最大数の増加	
		以前のリリース	新しいリリース
Cisco 1751	24	96	120
Cisco 1760	24	96	120
Cisco 2600XM	24	96	120
Cisco 2691	72	216	288
Cisco 3640	72	216	288
Cisco 3660	240	720	960
Cisco 3725	144	432	576
Cisco 3745	240	720	960

## PSTN および BRI/PRI を介してインバンド DTMF シグナリングを使用した Cisco Unity ボイスメール統合

Cisco Unity ボイスメールや他のボイスメールを Cisco SRST と統合することができます。ボイスメール統合には、次の 6 つの新しいコマンドが導入されています。

- [pattern direct](#)
- [pattern ext-to-ext busy](#)
- [pattern ext-to-ext no-answer](#)
- [pattern trunk-to-ext busy](#)
- [pattern trunk-to-ext no-answer](#)
- [vm-integration](#)

## 関連情報

コマンドの詳細については、『[Cisco Unified SRST and Cisco Unified SIP SRST Command Reference \(All Versions\)](#)』および P.193 の「[Cisco Unified SRST へのボイスメールの統合](#)」を参照してください。

Cisco Unified SRST の監視および保守については、P.227 の「[Cisco Unified SRST の監視と保守](#)」に進んでください。

追加情報については、P.25 の「[Cisco Unified SRST の概要](#)」の P.40 の「[その他の資料](#)」を参照してください。

P.25 の「[Cisco Unified SRST の概要](#)」に進みます。





# Cisco Unified SRST の概要

Revised: July 11, 2008

この章では、Cisco Unified Survivable Remote Site Telephony ( Cisco Unified SRST ) の概要と動作について説明します。また、Cisco Unified IP Phone、プラットフォーム、Cisco Unified Communications Manager のバージョンサポート、仕様、機能、制約事項、およびその他の資料の参照先についても説明します。



(注)

Cisco Unified IP Phone のサポート、Cisco Unified IP Phone の最大数、DN または仮想音声ポートの最大数、および Cisco Unified SRST のメモリ要件に関する最新情報については、『*Cisco Unified SRST 4.3 Supported Firmware, Platforms, Memory, and Voice Products*』を参照してください。このドキュメントは、次の URL から入手可能です。

[http://www.cisco.com/en/US/docs/voice\\_ip\\_comm/cusrst/requirements/guide/srs43spc.html](http://www.cisco.com/en/US/docs/voice_ip_comm/cusrst/requirements/guide/srs43spc.html)

## 内容

- [Cisco Unified SRST の説明 \( P.26 \)](#)
- [Cisco Unified IP Phone、プラットフォーム、Cisco Unified Communications Manager、信号、言語、およびスイッチのサポート \( P.30 \)](#)
- [Cisco Unified SRST を設定する場合の前提条件 \( P.34 \)](#)
- [Cisco Unified SRST を設定する場合の制約事項 \( P.37 \)](#)
- [関連情報 \( P.39 \)](#)
- [その他の資料 \( P.40 \)](#)
- [マニュアルの入手方法、テクニカル サポート、およびセキュリティ ガイドライン \( P.42 \)](#)

## Cisco Unified SRST の説明

Cisco Unified SRST は、ローカル ネットワーク上の Cisco ルータに接続されている Cisco IP Phone のフォールバック サポートを Cisco Unified Communications Manager に提供します。Cisco Unified SRST を使用すると、Cisco IP Phone がリモートのプライマリ、セカンダリ、またはターティアリ（第三次）Cisco Unified Communications Manager インスタレーションへの接続を失った場合や、WAN 接続がダウンした場合に、ルータが電話機のコール処理をサポートできるようになります。

Cisco Unified Communications Manager は、WAN を介して Cisco マルチサービス ルータに接続されているリモート サイトの Cisco IP Phone をサポートします。Cisco Unified SRST 以前では、ルータと Cisco Unified Communications Manager 間の WAN 接続に障害が発生した場合や、Cisco Unified Communications Manager との接続が何らかの理由で失われた場合、ネットワーク上の Cisco Unified IP Phone は、障害が続く限り使用不能になりました。Cisco Unified SRST はこの問題に対処しており、Cisco Unified IP Phone のコール処理を Cisco Unified SRST ルータから直接サポートすることによって、Cisco IP Phone がサービス（ただし最小限のもの）を継続的に提供できることを保証します。システムは障害を自動的に検出し、Simple Network Auto Provisioning（SNAP; シンプル ネットワーク オート プロビジョニング）テクノロジーを使用して、ルータに登録された Cisco IP Phone のコール処理を行うようにブランチ オフィスのルータを自動設定します。プライマリ Cisco Unified Communications Manager への WAN リンクまたは接続が回復すると、コール処理はプライマリ Cisco Unified Communications Manager に戻ります。

Cisco Unified IP Phone がプライマリ、セカンダリ、およびターティアリ Cisco Unified Communications Manager との接続を失った場合、電話機はコールの発信と受信に必要なコール処理機能を保持するために、ローカル Cisco Unified SRST ルータへの接続を確立する必要があります。Cisco IP Phone は、Settings メニューの Network Configuration 領域で、ローカル Cisco Unified SRST ルータの IP アドレスをデフォルト ルータとして保持します。Settings メニューは、最大 5 つのデフォルト ルータ エントリをサポートしています。ただし、Cisco Unified Communications Manager がサポートするエントリは最大 3 つです。ネットワーク上でセカンダリ Cisco Unified Communications Manager が使用可能になっていない場合、通常の動作中は、ローカル Cisco Unified SRST ルータの IP アドレスが Cisco Unified Communications Manager のスタンバイ接続として保持されます。



(注)

Cisco Unified Communications Manager フォールバック モードの電話サービスを使用できるのは、Cisco Unified SRST ルータでサポートされている Cisco IP Phone に限られます。ネットワーク上の他の Cisco IP Phone は、そのプライマリ、セカンダリ、またはターティアリ Cisco Unified Communications Manager と再接続するまで、アウト オブ サービスの状態になります。

一般に、Cisco Unified Communications Manager への接続に障害が発生したことを電話機が検出するには、キープアライブ期間の 3 倍の時間がかかります。デフォルトのキープアライブ期間は 30 秒です。電話機で Cisco Unified SRST ルータとのアクティブなスタンバイ接続が確立されている場合、フォールバック プロセスには、Cisco Unified Communications Manager との接続が失われた時点から 10 ~ 20 秒がかかります。Cisco Unified SRST ルータへのアクティブなスタンバイ接続が存在するのは、電話機の Unified Communications Manager リストに 1 つの Cisco Unified Communications Manager のロケーションが登録されている場合のみです。登録されていない場合、電話機はセカンダリ Cisco Unified Communications Manager に対してスタンバイ接続をアクティブにします。



(注)

Cisco Unified IP Phone が SRST ルータにフォールバックするのにかかる時間は、電話機のタイプによって異なる場合があります。Cisco 7902、Cisco 7905、および Cisco 7912 などの電話機では、SRST モードにフォールバックするのに約 2 分 30 秒かかる場合があります。



Cisco Unified IP Phone の Cisco Unified Communications Manager リストに複数の Cisco Unified Communications Manager が登録されている場合、電話機は、ローカル Cisco Unified SRST ルータとの接続を試行する前に、セカンダリおよびターティアリ Cisco Unified Communications Manager のリストを処理します。したがって、Cisco IP Phone が Cisco Unified SRST ルータとの接続を最終的に確立するまでの時間は、Cisco Unified Communications Manager への接続が試行されるたびに増加します。Cisco Unified Communications Manager への接続の試行にそれぞれ約 1 分かかると想定すると、当該の Cisco IP Phone は、WAN リンクに障害が発生した時点から 3 分以上にわたってオフラインの状態になる可能性があります。



(注)

WAN 接続の障害時に、Cisco Unified SRST が有効になっている場合、Cisco Unified IP Phone には、電話機が Cisco Unified Communications Manager フォールバック モードで動作していることを通知するメッセージが表示されます。Cisco Unified Communications Manager フォールバック モードで動作している場合、Cisco Unified IP Phone 7960G および Cisco Unified IP Phone 7940G には「CM Fallback Service Operating」というメッセージが表示され、Cisco Unified IP Phone 7910 には「CM Fallback Service」というメッセージが表示されます。Cisco Unified Communications Manager が回復すると、メッセージが消去され、Cisco Unified IP Phone の機能がすべて回復します。

Cisco Unified Communications Manager フォールバック モードになっている場合、Cisco Unified IP Phone は、セントラル オフィスにある Cisco Unified Communications Manager との再接続を定期的に試行します。一般に、Cisco IP Phone がリモートの Cisco Unified Communications Manager への再接続を試行するまでの待機時間は、120 秒です。この時間は、Cisco Unified Communications Manager で変更できます。『[Cisco Unified Communications Manager Administration Guide](#)』の「Device Pool Configuration Settings」の章を参照してください。手動リブートによってただちに Cisco Unified IP Phone を Cisco Unified Communications Manager に再接続することもできます。

Cisco Unified Communications Manager と再接続すると、Cisco Unified IP Phone は、Cisco Unified SRST ルータに対する登録を自動的にキャンセルします。ただし、WAN リンクが不安定な場合、Cisco Unified IP Phone は、Cisco Unified Communications Manager と Cisco Unified SRST の間で接続を切り替えることがあります。アクティブなコールを現在受けている場合、Cisco Unified IP Phone では、セントラル オフィスにあるプライマリ Cisco Unified Communications Manager と再接続することはできません。

図 1 は、Cisco Unified SRST ルータに複数の Cisco IP Phone が接続されているブランチ オフィスを示しています。ルータは WAN リンクと PSTN の両方に接続されています。Cisco Unified IP Phone は、この WAN リンクを介して、セントラル オフィスにあるプライマリ Cisco Unified Communications Manager に接続されています。

図 1 リモートのセントラル Cisco Unified Communications Manager に接続されているブランチ オフィスの Cisco Unified IP Phone

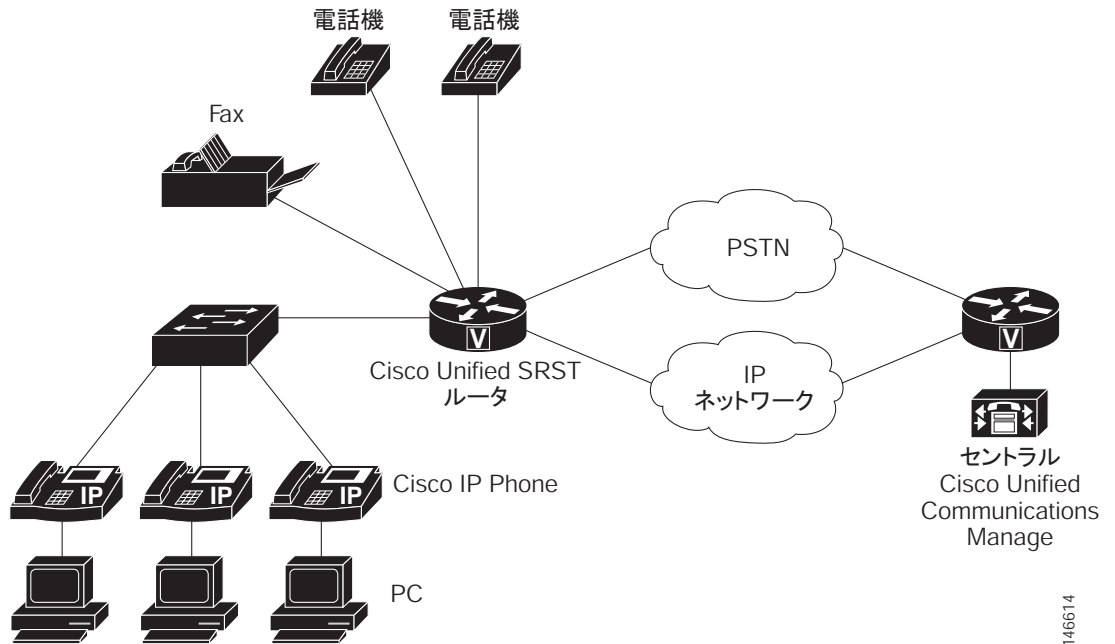
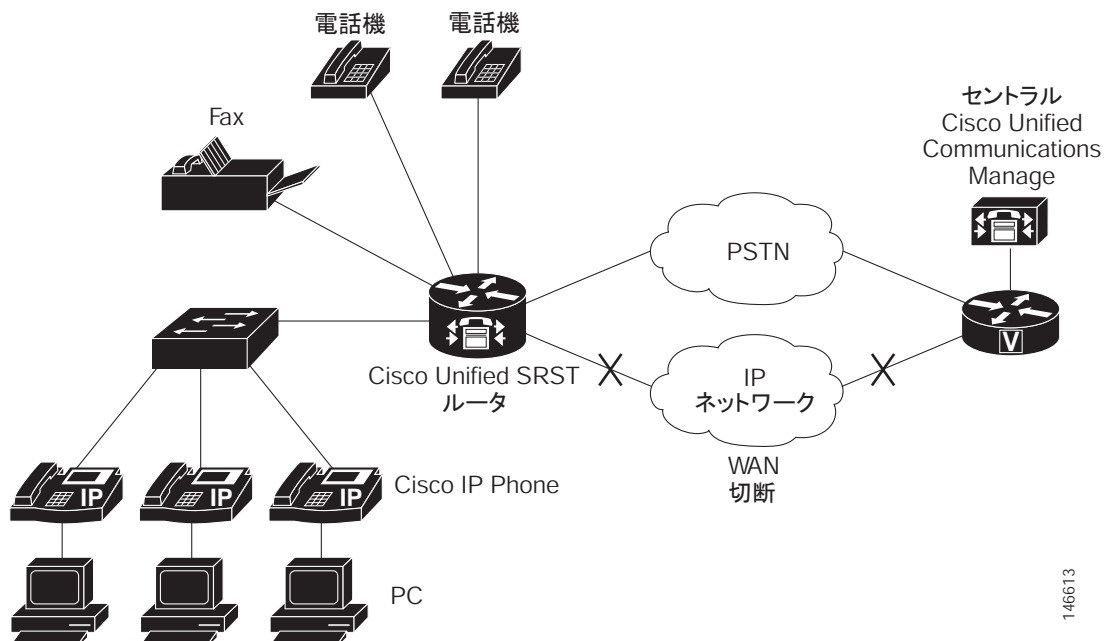


図 2 は、WAN 接続がダウンした同じブランチ オフィスの電話ネットワークを示しています。この状況では、Cisco IP Phone は、Cisco Unified SRST ルータをプライマリ Cisco Unified Communications Manager のフォールバックとして使用します。ブランチ オフィスの Cisco Unified IP Phone は、Cisco Unified SRST ルータを介して PSTN に接続され、オフネット コールを発信および受信できるようになります。

図 2 リモートのセントラル Cisco Unified Communications Manager (SRST モードで動作中) に接続されているブランチ オフィスの Cisco Unified IP Phone



WAN リンクに障害が発生した場合、デフォルトでは、H.323 ゲートウェイにおいて、Cisco Unified IP Phone から PSTN へのアクティブなコールは保持されません。コール プリザベーションは、**no h225 timeout keepalive** コマンドと連携する場合があります。

デフォルト設定では、H.323 ゲートウェイは Cisco Unified Communications Manager に対するキープアライブ信号を保持し、WAN リンク障害などによってキープアライブ信号に障害が発生した場合は、H.323 と PSTN 間のコールを終了します。この動作を無効にして、ローカル Cisco Unified IP Phone からの既存のコールを保持できるようにするには、**no h225 timeout keepalive** コマンドを使用します。キープアライブ メカニズムを無効にした場合に影響を受けるコールは、H.225 キープアライブ信号が消失した場合に切断されるコールだけです。非アクティブな状況が検出された場合のコールの切断については、『[Media Inactive Call Detection](#)』を参照してください。

## MGCP ゲートウェイと SRST

MGCP フォールバックは SRST とは別の機能であり、個別の機能として設定すると、PSTN ゲートウェイで使用できます。MGCP ゲートウェイで SRST をフォールバック モードとして使用するには、SRST および MGCP フォールバックの両方を同じゲートウェイに設定する必要があります。Cisco IOS Release 12.2(11)T 以降では、MGCP と SRST を同じゲートウェイに設定できるようになっています。

MGCP ゲートウェイにおいて SRST モードのときにコールを発信するには、2 つのフォールバック コマンドを MGCP ゲートウェイに設定する必要があります。これら 2 つのコマンドを使用すると、SRST が、音声ポートの制御権と MGCP ゲートウェイでのコール処理の制御権を取得できるようになります。12.3(14)T 以前の Cisco IOS の場合、2 つのコマンドは **ccm-manager fallback-mgcp** コマンドと **call application alternate** コマンドです。12.3(14)T 以降の Cisco IOS リリースの場合は、**ccm-manager fallback-mgcp** コマンドと **service** コマンドを設定する必要があります。これらのコマンドの設定の詳細については、P.46 の「[MGCP ゲートウェイでの SRST の有効化](#)」の項を参照してください。



(注)

上記のコマンドは、両方とも設定されている場合に限り有効となります。たとえば、**ccm-manager fallback-mgcp** コマンドだけを設定した場合、設定は動作しません。

MGCP ゲートウェイのフォールバック方式の詳細については、『[Configuring MGCP Gateway Support for Cisco Unified Communications Manager](#)』または『[MGCP Gateway Fallback Transition to Default H.323 Session Application](#)』を参照してください。

## Cisco Unified IP Phone、プラットフォーム、Cisco Unified Communications Manager、信号、言語、およびスイッチのサポート

次の各項では、Cisco Feature Navigator の説明と、Cisco SRST バージョン 1.0 から Cisco Unified SRST の現行バージョンまでの、Cisco Unified IP Phone、プラットフォーム、および Cisco Unified Communications Manager のサポートに関する履歴を示します。

- Cisco Unified SRST をサポートする Cisco IOS ソフトウェア リリースの検索 ( P.30 )
- Cisco Unified IP Phone のサポート ( P.30 )
- プラットフォームとメモリのサポート ( P.31 )
- Cisco Unified Communications Manager の互換性 ( P.32 )
- 信号のサポート ( P.32 )
- 言語のサポート ( P.32 )
- スwitchのサポート ( P.33 )

### Cisco Unified SRST をサポートする Cisco IOS ソフトウェア リリースの検索

この章の各表には、Cisco Unified SRST に新機能を最初に導入した Cisco IOS ソフトウェア リリースだけが示されています。それ以降の Cisco IOS ソフトウェア リリースでは、Cisco Unified SRST のバージョンを継承している場合があります。特定バージョンの Cisco Unified SRST をサポートする Cisco IOS ソフトウェア リリースのリストを取得するには、Cisco Feature Navigator を使用します。

Cisco Feature Navigator にアクセスするには、<http://www.cisco.com/go/cfn> に移動してください。Cisco.com のアカウントは必要ありません。

### Cisco Unified IP Phone のサポート

Cisco Unified IP Phone のサポートに関する最新情報については、『*Cisco Unified SRST 4.3 Supported Firmware, Platforms, Memory, and Voice Products*』を参照してください。このドキュメントは、次の URL から入手可能です。

[http://www.cisco.com/en/US/docs/voice\\_ip\\_comm/cusrst/requirements/guide/srs43spc.html](http://www.cisco.com/en/US/docs/voice_ip_comm/cusrst/requirements/guide/srs43spc.html)

Cisco Unified SRST 4.0 では、次の IP Phone がサポートされています。

- Cisco Analog Telephone Adaptor ( ATA ) 186 および Cisco ATA 188 バージョン 2.16 以降と、Cisco Unified Communications Manager 3.3 以降のバージョンの組み合わせ  
Cisco Unified SRST は、音声コールに対して、Skinny Client Control Protocol ( SCCP ) を使用した Cisco ATA 186 および Cisco ATA 188 のみをサポートしています。



(注)

Cisco Unified SRST システムに登録されている ATA が FAX コールに参加できるようにするには、FAX パススルー モードで RTP ペイロード タイプとして「標準のペイロード タイプ 0/8」を使用するように、ATA の ConnectMode パラメータを設定する必要があります。Cisco Unified SRST 4.0 以降のバージョンで使用する ATA に対してこのように設定するには、ATA において ConnectMode パラメータのビット 2 を 1 に設定します。詳細については、『*Cisco ATA 186 and Cisco ATA 188 Analog Telephone Adaptor Administrator's Guide for SCCP*』の「Parameters and Defaults」の章を参照してください。このドキュメントは、次の URL から入手可能です。

[http://www.cisco.com/en/US/docs/voice\\_ip\\_comm/cata/186\\_188/2\\_15\\_ms/english/administration/guide/sccp/sccpach5.html](http://www.cisco.com/en/US/docs/voice_ip_comm/cata/186_188/2_15_ms/english/administration/guide/sccp/sccpach5.html)

- Cisco Unified IP Phone 7902G
- Cisco Unified IP Phone 7905G
- Cisco Unified IP Phone 7910
- Cisco Unified IP Phone 7911G
- Cisco Unified IP Phone 7912G
- Cisco Unified IP Phone 7914 拡張モジュール
- Cisco Unified Wireless IP Phone 7920
- Cisco IP Conference Station 7935
- Cisco Unified IP Conference Station 7936
- Cisco Unified IP Phone 7940G
- Cisco Unified IP Phone 7941G および Cisco Unified IP Phone 7941G-GE
- Cisco Unified IP Phone 7960G
- Cisco Unified IP Phone 7961G および Cisco Unified IP Phone 7961G-GE
- Cisco Unified IP Phone 7970G
- Cisco Unified IP Phone 7971G-GE
- Cisco VG224 Analog Phone Gateway (IOS バージョン 12.4(4)XC) と、Cisco IOS Software Release 12.4(4)XC 以降を実行する Cisco Unified SRST 4.0 の組み合わせ。設定については、『[SCCP Controlled Analog \(FXS\) Ports with Supplementary Features in Cisco IOS Gateways](#)』の「Enabling Fallback to Cisco Unified SRST on the Voice Gateway」の項を参照してください。このドキュメントは、次の URL から入手可能です。[http://www.cisco.com/en/US/docs/ios/12\\_4t/12\\_4t2/ht1vg224.html](http://www.cisco.com/en/US/docs/ios/12_4t/12_4t2/ht1vg224.html)
- Cisco VG248 Analog Phone Gateway バージョン 1.2(1) 以降

**(注)**

Cisco Unified Communications Manager のフォールバック中、Cisco Unified SRST は Cisco VG248 を Cisco Unified IP Phone のグループと見なします。Cisco Unified SRST は、Cisco VG248 の 48 個のポートそれぞれを個別の Cisco IP Phone と見なします。Cisco VG248 バージョン 1.2(1) 以降のサポートは、Cisco SRST バージョン 2.1 でも利用できます。詳細については、『[Cisco VG248 Analog Phone Gateway Data Sheet](#)』および『[Cisco VG248 Analog Phone Gateway Version 1.2\(1\) Release Notes](#)』を参照してください。

## プラットフォームとメモリのサポート

Cisco Unified IP Phone の最大数、DN または仮想音声ポートの最大数、および Cisco Unified SRST のメモリ要件に関する最新情報については、『[Cisco Unified SRST 4.3 Supported Firmware, Platforms, Memory, and Voice Products](#)』を参照してください。このドキュメントは、次の URL から入手可能です。

[http://www.cisco.com/en/US/docs/voice\\_ip\\_comm/cusrst/requirements/guide/srs43sps.html](http://www.cisco.com/en/US/docs/voice_ip_comm/cusrst/requirements/guide/srs43sps.html)

## Cisco Feature Navigator を使用したプラットフォーム サポートの確認

Cisco IOS ソフトウェアは、特定のプラットフォームでサポートされている機能セットにパッケージ化されています。この機能のプラットフォーム サポートに関する最新情報を取得するには、Cisco Feature Navigator にアクセスします。Cisco Feature Navigator は、機能のプラットフォーム サポートが新たに追加されると、サポートされるプラットフォームのリストを動的に更新します。

## Cisco IOS ソフトウェア イメージの可用性

特定の Cisco IOS ソフトウェア リリースのプラットフォーム サポートは、そのプラットフォームに対するソフトウェア イメージの可用性によって異なります。プラットフォームによっては、ソフトウェア イメージへの対応が、予告なしに延期、遅延、または変更される場合があります。Cisco IOS ソフトウェア リリースごとのプラットフォーム サポートやソフトウェア イメージの可用性に関する最新情報については、オンラインのリリース ノートまたは Cisco Feature Navigator (サポートされている場合) を参照してください。



(注) Cisco IOS ソフトウェア イメージに関する最新情報については、『*Cisco Unified SRST 4.3 Supported Firmware, Platforms, Memory, and Voice Products*』を参照してください。このドキュメントは、次の URL から入手可能です。  
[http://www.cisco.com/en/US/docs/voice\\_ip\\_comm/cusrst/requirements/guide/srs43spc.html](http://www.cisco.com/en/US/docs/voice_ip_comm/cusrst/requirements/guide/srs43spc.html)

## Cisco Unified Communications Manager の互換性

『*Cisco Unified Communications Manager Compatibility Matrix*』を参照してください。

## 信号のサポート

Cisco Unified SRST は、FXS、FXO、T1、E1、および E1 R2 信号をサポートしています。

## 言語のサポート

Cisco SRST 3.2 以降のバージョンは、次の言語をサポートしています。

- デンマーク語
- オランダ語
- 英語
- フランス語
- ドイツ語
- イタリア語
- 日本語のカタカナ (Cisco Unified Communications Manager 4.0 以降で使用可能)
- ノルウェー語
- ポルトガル語
- ロシア語
- スペイン語
- スウェーデン語



(注) Cisco Unified IP Phone 7911G、Cisco Unified IP Phone 7941G および 7941G-GE、Cisco Unified IP Phone 7961G および 7961G-GE、Cisco Unified IP Phone 7970G、Cisco Unified IP Phone 7971G-GE は、英語だけをサポートしています。

## スイッチのサポート

Cisco SRST 3.2 以降のバージョンは、次のスイッチを含むすべての PRI および BRI スイッチをサポートしています。

- basic-1tr6
- basic-5ess
- basic-dms100
- basic-net3
- basic-ni
- basic-ntt NTT スイッチ タイプ (日本向け)
- basic-ts013
- primary-4ess Lucent 4ESS スイッチ タイプ (米国向け)
- primary-5ess Lucent 5ESS スイッチ タイプ (米国向け)
- primary-dms100 Northern Telecom DMS-100 スイッチ タイプ (米国向け)
- primary-net5 NET5 スイッチ タイプ (英国、欧州、アジア、およびオーストラリア向け)
- primary-ni National ISDN スイッチ タイプ (米国向け)
- primary-ntt NTT スイッチ タイプ (日本向け)
- primary-qsig QSIG スイッチ タイプ
- primary-ts014 TS014 スイッチ タイプ (オーストラリア向け) (廃止)

## Cisco Unified SRST を設定する場合の前提条件

Cisco Unified SRST を設定する前に、次の作業を行う必要があります。

- ソフトウェアをダウンロードするための Cisco.com のアカウントを取得する。  
Cisco.com のアカウントを取得するには、[www.cisco.com](http://www.cisco.com) に移動し、画面上部の **Register** をクリックします。
- Cisco Unified SRST のライセンスを購入する。  
ライセンスを購入するには、<http://www.cisco.com/cgi-bin/tablebuild.pl/ip-key> に移動します。
- 適切な Cisco Unified SRST バージョンを選択する。各 SRST バージョンは、IP Phone、メモリ要件、機能、および Directory Number (DN; 電話番号) の特定のセットをサポートしています。P.31 の「[プラットフォームとメモリのサポート](#)」および P.37 の「[Cisco Unified SRST を設定する場合の制約事項](#)」を参照してください。
- 適切な電話機ロードを選択する。SRST は、Cisco Unified Communications Manager のさまざまなバージョンについてテストされた特定の電話機ロードだけをサポートします。最新の電話機ロードについては、『[Cisco Unified SRST 4.3 Supported Firmware, Platforms, Memory, and Voice Products](#)』を参照してください。このドキュメントは、次の URL から入手可能です。  
[http://www.cisco.com/en/US/docs/voice\\_ip\\_comm/cusrst/requirements/guide/srs43spsc.html](http://www.cisco.com/en/US/docs/voice_ip_comm/cusrst/requirements/guide/srs43spsc.html)
- Cisco Unified Communications Manager がすでにインストールされている場合は、ご使用のバージョンの Cisco Unified Communications Manager が Cisco Unified SRST リリースと互換性があることを確認する。P.32 の「[Cisco Unified Communications Manager の互換性](#)」を参照してください。

### バージョンの前提条件

- 一般的な前提条件については、P.34 の「[Cisco Unified SRST を設定する場合の前提条件](#)」を参照してください。
- E911 サービスの前提条件については、P.230 の「[前提条件](#)」を参照してください。

### Cisco Unified Communications Manager のインストール

Cisco Unified Communications Manager をインストールする場合は、次の要件を考慮してください。

- 『[Cisco Unified Communications Manager \(CallManager\) Install and Upgrade Guides](#)』で、該当するバージョンのインストール手順を参照してください。このドキュメントは、次の URL から入手可能です。  
[http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod\\_installation\\_guides\\_list.html](http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_installation_guides_list.html)
- Cisco Unified SRST を Cisco Unified Communications Manager と統合します。統合は、Cisco Unified Communications Manager から実行します。P.35 の「[Cisco Unified SRST と Cisco Unified Communications Manager の統合](#)」を参照してください。

### Cisco Unified SRST のインストール

インストール手順は、Cisco Unified SRST のバージョンによって異なります。

- [Cisco SRST V3.0 以降のバージョンのインストール \(P.35\)](#)
- [Cisco SRST V2.0 および V2.1 のインストール \(P.35\)](#)
- [Cisco SRST V1.0 のインストール \(P.35\)](#)

Cisco Unified SRST を更新するには、この項に記載されているインストール手順に従います。



## Cisco SRST V3.0 以降のバージョンのインストール

Cisco Unified Communications Manager のバージョンと互換性のある Cisco SRST または Cisco Unified SRST バージョンを含む Cisco IOS ソフトウェア リリース イメージをインストールします。P.32 の「Cisco Unified Communications Manager の互換性」を参照してください。Cisco IOS ソフトウェアは、<http://www.cisco.com/public/sw-center/> の Cisco Software Center からダウンロードできます。

Cisco SRST および Cisco Unified SRST は、Music On Hold (MOH) をフラッシュ メモリ内のフラッシュ MOH ファイルから連続的にマルチキャスト出力することをサポートするように設定できます。詳細については、P.113 の「XML API スキーマの定義」を参照してください。Music On Hold を使用する場合は、<http://www.cisco.com/cgi-bin/tablebuild.pl/ip-iostsp> の Technical Support Software Download サイトに移動し、music-on-hold.au ファイルを Cisco SRST または Cisco Unified SRST ルータ上のフラッシュ メモリにコピーします。

## Cisco SRST V2.0 および V2.1 のインストール

Cisco SRST V2.0 または Cisco SRST V2.1 は、<http://www.cisco.com/public/sw-center/> の Cisco Software Center からダウンロードし、インストールすることができます。

## Cisco SRST V1.0 のインストール

Cisco SRST V1.0 は、Cisco Communications Manager V3.0.5 のみと連携動作します。Cisco Unified Communications Manager および Cisco Unified SRST の最新バージョンにアップグレードすることをお勧めします。

## Cisco Unified SRST と Cisco Unified Communications Manager の統合

Cisco Unified SRST と Cisco Unified Communications Manager との統合には、2 通りの手順があります。使用する Cisco Unified Communications Manager のバージョンに応じて手順を選択します。

## Cisco Communications Manager V3.3 以降のバージョンを使用する場合

Cisco Communications Manager V3.3 以降のバージョンを使用する場合は、SRST リファレンスを作成し、デバイス プールに適用する必要があります。SRST リファレンスとは、Cisco Unified SRST ルータの IP アドレスのことです。

---

### ステップ 1 SRST リファレンスを作成します。

- a. Cisco Unified Communications Manager の任意のページで、**System**、**SRST** の順にクリックします。
- b. Find and List SRST References ページで、**Add a New SRST Reference** をクリックします。
- c. SRST Reference Configuration ページで、SRST Reference Name フィールドに名前を入力し、IP Address フィールドに Cisco SRST ルータの IP アドレスを入力します。
- d. **Insert** をクリックします。

### ステップ 2 SRST リファレンスまたはデフォルト ゲートウェイを 1 つ以上のデバイス プールに適用します。

- a. Cisco Unified Communications Manager の任意のページで、**System**、**Device Pool** の順にクリックします。
- b. Device Pool Configuration ページで、目的のデバイス プール アイコンをクリックします。

- c. Device Pool Configuration ページで、SRST Reference フィールドのメニューから、特定の SRST リファレンスまたは「Use Default Gateway」を選択します。
- 

### V3.3 以前の Cisco Unified Communications Manager を使用する場合

Cisco Unified SRST をデフォルトで有効にするファームウェア バージョンを使用する場合、Cisco Unified Communications Manager で Cisco Unified SRST をサポートするための追加設定を行う必要はありません。使用するファームウェア バージョンによって Cisco Unified SRST がデフォルトで無効になる場合は、各電話機の設定で Cisco Unified SRST を有効にする必要があります。

- 
- ステップ 1** Cisco Unified Communications Manager の Phone Configuration ページに移動します。
- a. Cisco Unified Communications Manager の任意のページで、**Device**、**Phone** の順にクリックします。
  - b. Find and List Phones ページで、**Find** をクリックします。
  - c. 電話機のリストが表示されたら、目的のデバイス名をクリックします。
  - d. Phone Configuration ページが表示されます。
- ステップ 2** Phone Configuration ページで、下部にある Product Specific Configuration セクションに移動し、Cisco Unified SRST フィールドのメニューから **Enabled** を選択し、次に **Update** をクリックします。
- ステップ 3** ステップ 1 とステップ 2 を繰り返し、次の電話機の Phone Configuration ページに移動して、Cisco Unified SRST フィールドのメニューから **Enabled** を選択します。
-

## Cisco Unified SRST を設定する場合の制約事項

表 4 は、Cisco SRST バージョン 1.0 から Cisco Unified SRST の現行バージョンまでの制約事項の履歴を示しています。

表 4 Cisco SRST V1.0 から Cisco Unified SRST の現行バージョンまでの制約事項の履歴

Cisco SRST バージョン	Cisco IOS リリース	制約事項
バージョン 4.1	12.4(15)T	<ul style="list-style-type: none"> <li>• Cisco Unified SRST の E911 サービスは、Cisco Emergency Responder とインターフェイスしません。</li> <li>• 911 を最後にコールした電話機に関する情報は、Cisco Unified SRST のリブート後は保持されません。</li> <li>• リモート IP Phone が Cisco Unified SRST フォールバック モードの場合、Cisco Emergency Responder では、緊急コールの履歴テーブルに加えられた更新内容にアクセスできません。したがって、Cisco Unified IP Phone が Cisco Unified Communications Manager に再登録した後で PSAP がコールバックした場合、Cisco Emergency Responder はそのコールの履歴を保持しません。結果として、そのコールは、最初の 911 発信者にはルーティングされません。代わりに、コールは、Cisco Emergency Responder で対応する ELIN 用に設定されているデフォルトの宛先にルーティングされます。</li> <li>• Cisco Unified Wireless 7920 および 7921 IP Phone の場合、発信者のロケーションを特定できる情報は、システム管理者によって設定された静的な情報に限られます。詳細については、P.236 の「携帯電話に関する注意事項」を参照してください。</li> <li>• 911 発信者の内線番号の変換先となる番号は、Emergency Response Location (ERL; 緊急応答ロケーション) ごとに 2 つの Emergency Location Identification Number (ELIN; 緊急ロケーション識別番号) に限られます。詳細については、P.231 の「概要」を参照してください。</li> <li>• ELIN を複数の目的に使用すると、既存の Cisco Unified SRST 機能との間に予期しない相互作用が引き起こされる可能性があります。このような ELIN の多重使用の例には、ELIN を実際の電話番号 (ephone-dn、voice register dn、または FXS destination-pattern)、コールピックアップ番号、またはエイリアス再ルーティング番号として使用するよう設定することなどがあります。詳細については、P.239 の「ELIN の複数の用途」を参照してください。</li> <li>• E911 サービスが既存の Cisco Unified SRST 機能と対話するための設定は変更可能ですが、変更すると予期しない動作が発生します。E911 サービスと既存の Cisco Unified SRST 機能との相互作用の詳細については、P.238 の「既存の Cisco Unified SRST 機能との相互作用」を参照してください。</li> </ul>

表 4 Cisco SRST V1.0 から Cisco Unified SRST の現行バージョンまでの制約事項の履歴 (続き)

Cisco SRST バージョン	Cisco IOS リリース	制約事項
バージョン 4.0	12.4(4)XC	<ul style="list-style-type: none"> <li>• Cisco SRST バージョン 1.0 のすべての制約事項。</li> <li>• コール転送のサポート対象は、次のものに限られます。 <ul style="list-style-type: none"> <li>- Cisco IOS Release 12.2(11)T を実行し、H.323 非標準の情報要素を使用している Cisco ゲートウェイ間の VoIP H.323、VoFR、および VoATM</li> <li>- FXO および FXS ループスタート (アナログ)</li> <li>- FXO および FXS グラウンドスタート (アナログ)</li> <li>- Ear and Mouth (E&amp;M) (アナログ) および DID (アナログ)</li> <li>- FXO および FXS グラウンドスタート シグナリングによる T1 Channel-Associated Signaling (CAS; 個別線信号方式)</li> <li>- E&amp;M シグナリングによる T1 CAS</li> <li>- PRI および BRI スイッチの全タイプ</li> </ul> </li> <li>• Cisco Unified IP Phone function の次の機能キーは、SRST の動作中はサポートされないため、グレー表示になります。 <ul style="list-style-type: none"> <li>- MeetMe</li> <li>- GPickUp (グループ ピックアップ)</li> <li>- Park</li> <li>- Confrn (会議)</li> </ul> </li> <li>• Cisco IAD2420 シリーズ Integrated Access Device (IAD; 統合型アクセス装置) は Cisco Unified SRST 機能をサポートしていますが、この機能は、企業のブランチ オフィス向けのソリューションとしてはお勧めできません。</li> </ul>
バージョン 3.4	12.4(4)T	
バージョン 3.3	12.3(14)T	
バージョン 3.2	12.3(11)T	
バージョン 3.1	12.3(7)T	
バージョン 3.0	12.2(15)ZJ	
バージョン 2.1	12.2(15)T	
バージョン 2.02	12.2(13)T	
バージョン 2.01	12.2(11)T	
バージョン 2.0	12.2(8)T1	
バージョン 2.0	12.2(8)T	
バージョン 2.0	12.2(2)XT	
バージョン 1.0	12.2(2)XB	
	12.2(2)XG	
	12.1(5)YD	

## 関連情報

このマニュアルの次の各章では、Cisco Unified SRST の設定方法について説明します。表 5 に示すように、各章では作業を実行順序どおりに説明しています。Cisco Unified SRST を設定する最初の作業では、システム内の基本的なソフトウェアとハードウェアを Cisco Unified SRST 用に正しく設定します。手順については、P.34 の「Cisco Unified SRST を設定する場合の前提条件」を参照してください。

表 5 Cisco Unified SRST の設定順序

作業	作業についての参照先
1. Cisco Unified SRST システムがネットワークと通信するための設定	「 <a href="#">ネットワークの設定</a> 」の章
2. Cisco Unified SRST Phone の基本的な設定	「 <a href="#">Cisco Unified IP Phone の設定</a> 」の章
3. 着信コールと発信コールの設定	「 <a href="#">コール処理の設定</a> 」の章
4. オプションのシステム パラメータと電話パラメータの設定	「 <a href="#">追加のコール機能の設定</a> 」の章
5. SRST のオプション セキュリティの設定	「 <a href="#">Secure SRST の設定</a> 」の章
6. ボイスメールの設定	「 <a href="#">Cisco Unified SRST へのボイスメールの統合</a> 」の章
7. E911 サービスの設定	「 <a href="#">E911 サービス</a> 」の章

## その他の資料

次の各項では、Cisco Unified SRST に関連するその他の資料について説明します。

- [関連資料 \(P.40\)](#)
- [標準規格 \(P.41\)](#)
- [MIB \(P.41\)](#)
- [RFC \(P.41\)](#)
- [テクニカル サポート \(P.42\)](#)

## 関連資料

関連項目	マニュアル
Cisco IOS の音声設定	<ul style="list-style-type: none"> <li>• <a href="#">Cisco IOS Voice Configuration Library</a></li> <li>• <a href="#">Cisco IOS Voice Command Reference</a></li> <li>• <a href="#">Cisco IOS Debug Command Reference</a></li> <li>• <a href="#">Cisco IOS Tcl IVR and VoiceXML Application Guide</a></li> </ul>
Cisco IP Phone	<a href="#">Cisco IP Phones and Services</a>
シスコ セキュリティのマニュアル	<ul style="list-style-type: none"> <li>• <a href="#">Media and Signaling Authentication and Encryption Feature for Cisco IOS MGCP Gateways</a></li> <li>• <a href="#">Cisco IOS Certificate Server</a></li> <li>• <a href="#">Manual Certificate Enrollment (TFTP and Cut-and-Paste)</a></li> <li>• <a href="#">Certification Authority Interoperability Commands</a></li> <li>• <a href="#">Certificate Enrollment Enhancements</a></li> </ul>
Cisco SRST コマンド リファレンス	<a href="#">Cisco IOS Survivable Remote Site Telephony Version 3.2 Command Reference</a>
Cisco Unified Communications Manager の Music On Hold	該当する Cisco Unified Communications Manager リリースの『 <a href="#">Cisco Unified CallManager and Cisco Unified IP Phone Administrator's A - Z Feature Guide</a> 』の「Music On Hold」の章。 <a href="#">Cisco Unified Communications Manager</a> のマニュアル ディレクトリで、 <b>Cisco Unified Communications Manager (CallManager) &gt; Maintain and Operate Guides</b> をクリックします。
Cisco Unified Communications Manager のユーザ マニュアル	<ul style="list-style-type: none"> <li>• <a href="#">Cisco Unified Communications Manager</a></li> <li>• <a href="#">Cisco Unified Communications Manager Security Guide</a></li> <li>• <a href="#">Cisco Unified Communications Operating System Administration Guide</a></li> </ul>
Cisco Unified IP Phone	<ul style="list-style-type: none"> <li>• <a href="#">Cisco 7900 Series Unified IP Phones End-User Guides</a></li> <li>• <a href="#">Cisco IP Phone Authentication and Encryption for Cisco Communications Manager</a></li> <li>• <a href="#">Cisco IP Phone 7970 Administration Guide for Cisco Communications Manager リリース 4.x およびそれ以降、「Understanding Security Features for Cisco IP Phones」</a></li> </ul>
Cisco Unified SRST コマンドおよび仕様	<ul style="list-style-type: none"> <li>• <a href="#">Cisco Unified SRST and Cisco Unified SIP SRST Command Reference (All Versions)</a></li> <li>• <a href="#">Cisco Unified SRST 4.3 Supported Firmware, Platforms, Memory, and Voice Products</a></li> </ul>

関連項目	マニュアル
音声コマンドと SRST に関するコマンド リファレンスおよび設定情報	<ul style="list-style-type: none"> <li>• <a href="#">Cisco IOS Voice Command Reference</a></li> <li>• <a href="#">Cisco IOS Debug Command Reference</a></li> <li>• <a href="#">Cisco IOS Survivable Remote Site Telephony Version 3.2 System Administrator Guide</a></li> <li>• <a href="#">Cisco SRST 3.2 Command Reference</a></li> </ul>
音声コマンドとテレフォニー コマンドに関するコマンド リファレンスおよび設定情報	<ul style="list-style-type: none"> <li>• <a href="#">Cisco IOS Voice Command Reference</a></li> <li>• <a href="#">Cisco IOS Debug Command Reference</a></li> </ul>
SRST および MGCP フォールバックの設定	<ul style="list-style-type: none"> <li>• <a href="#">Configuring MGCP Gateway Support for Cisco Unified Communications Manager</a></li> <li>• <a href="#">MGCP Gateway Fallback Transition to Default H.323 Session Application</a></li> <li>• <a href="#">Configuring SRS Telephony and MGCP Fallback</a></li> </ul>
DHCP	<ul style="list-style-type: none"> <li>• <a href="#">Cisco IOS DHCP Server</a></li> </ul>
Media Inactive Call Detection	<ul style="list-style-type: none"> <li>• <a href="#">Media Inactive Call Detection</a></li> </ul>
Cisco Unified SRST の電話機マニュアル	<ul style="list-style-type: none"> <li>• <a href="#">Cisco Unified IP Phones 7900 Series</a></li> <li>• <a href="#">Survivable Remote Site Telephony</a></li> </ul>
標準的な用語集	<ul style="list-style-type: none"> <li>• <a href="#">Cisco IOS Voice Configuration Library Glossary</a></li> </ul>
標準的な前書き	<ul style="list-style-type: none"> <li>• <a href="#">Cisco IOS Voice Configuration Library Preface</a></li> </ul>

## 標準規格

標準	タイトル
ITU X. 509 バージョン 3	<a href="#">Public-Key and Attribute Certificate Frameworks</a>

## MIB

MIB	MIB のリンク
この機能でサポートされる新規の MIB または変更された MIB はありません。また、既存の MIB のサポートは変更されていません。	<p>選択したプラットフォーム、Cisco IOS リリース、および機能セットに関する MIB を探してダウンロードするには、次の URL にある <a href="#">Cisco MIB Locator</a> を使用します。</p> <p><a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></p>

## RFC

RFC	タイトル
RFC 2246	<a href="#">The Transport Layer Security (TLS) Protocol Version 1.0</a>
RFC 3711	<a href="#">The Secure Real-Time Transport Protocol (SRTP)</a>

## テクニカル サポート

説明	リンク
<p>Cisco Technical Support Web サイトでは、オンラインで資料やツールを利用して、トラブルシューティングやシスコ製品およびテクノロジーに関する技術上の問題の解決に役立てることができます。</p> <p>ご使用の製品に関するセキュリティ情報や技術情報を受け取るには、プロダクト アラート ツール ( Field Notices からアクセス )、Cisco Technical Services Newsletter、および Really Simple Syndication ( RSS ) フィードなど、各種のサービスに登録します。</p> <p>Cisco Technical Support Web サイト上のツールにアクセスする際は、いずれも Cisco.com のログイン ID およびパスワードが必要です。</p>	<p><a href="http://www.cisco.com/en/US/support/index.html">http://www.cisco.com/en/US/support/index.html</a></p>

## マニュアルの入手方法、テクニカル サポート、およびセキュリティ ガイドライン

マニュアルの入手方法、Service Request ツールの使用方法、および追加情報の収集方法については、次の URL で、毎月更新される『*What's New in Cisco Product Documentation*』を参照してください。『*What's New in Cisco Product Documentation*』には、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されています。

<http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html>

Really Simple Syndication ( RSS ) フィードとして『*What's New in Cisco Product Documentation*』に登録し、リーダ アプリケーションを使用して、コンテンツがデスクトップに直接配信されるように設定します。RSS フィードは無料サービスです。シスコは現在、RSS バージョン 2.0 をサポートしています。



## シスコのテクニカル サポート

次の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。

<http://www.cisco.com/en/US/support/index.html>

以下を含むさまざまな作業にこの Web サイトが役立ちます。

- テクニカル サポートを受ける
- ソフトウェアをダウンロードする
- セキュリティの脆弱性を報告する、またはシスコ製品のセキュリティ問題に対する支援を受ける
- ツールおよびリソースへアクセスする
  - Product Alert の受信登録
  - Field Notice の受信登録
  - Bug Toolkit を使用した既知の問題の検索
- Networking Professionals ( NetPro ) コミュニティで、技術関連のディスカッションに参加する
- トレーニング リソースへアクセスする
- TAC Case Collection ツールを使用して、ハードウェアや設定、パフォーマンスに関する一般的な問題をインタラクティブに特定および解決する

Japan テクニカル サポート Web サイトでは、Technical Support Web サイト ( <http://www.cisco.com/techsupport> ) の、利用頻度の高いドキュメントを日本語で提供しています。Japan テクニカル サポート Web サイトには、次の URL からアクセスしてください。

<http://www.cisco.com/jp/go/tac>

## Service Request ツールの使用

Service Request ツールには、次の URL からアクセスできます。

<http://www.cisco.com/techsupport/servicerequest>

日本語版の Service Request ツールは次の URL からアクセスできます。

<http://www.cisco.com/jp/go/tac/sr/>

シスコの世界各国の連絡先一覧は、次の URL で参照できます。

<http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml>

## その他の情報の入手方法

シスコの製品、サービス、テクノロジー、ネットワークング ソリューションに関する情報について、さまざまな資料をオンラインで入手できます。

- シスコの E メール ニュースレターなどの配信申し込みについては、Cisco Subscription Center にアクセスしてください。  
<http://www.cisco.com/offer/subscribe>
- 日本語の月刊 Email ニュースレター「Cisco Customer Bridge」については、下記にアクセスください。  
[http://www.cisco.com/web/JP/news/cisco\\_news\\_letter/ccb/](http://www.cisco.com/web/JP/news/cisco_news_letter/ccb/)
- シスコ製品に関する変更やアップデートの情報を受信するには、Product Alert Tool にアクセスし、プロファイルを作成して情報の配信を希望する製品を選択してください。Product Alert Tool には、次の URL からアクセスできます。  
<http://tools.cisco.com/Support/PAT/do/ViewMyProfiles.do?local=en>
- 『Cisco Product Quick Reference Guide』はリファレンス ツールで、パートナーを通じて販売されている多くのシスコ製品に関する製品概要、主な機能、製品番号、および簡単な技術仕様が記載されています。『Cisco Product Quick Reference Guide』を発注するには、次の URL にアクセスしてください。  
<http://www.cisco.com/go/guide>
- ネットワークの運用面の信頼性を向上させることのできる最新の専門的サービス、高度なサービス、リモート サービスに関する情報については、Cisco Services Web サイトを参照してください。Cisco Services Web サイトには、次の URL からアクセスできます。  
<http://www.cisco.com/go/services>
- Cisco Marketplace では、さまざまなシスコの書籍、参考資料、マニュアル、ロゴ入り商品を提供しています。Cisco Marketplace には、次の URL からアクセスできます。  
<http://www.cisco.com/go/marketplace/>
- DVD に収録されたシスコの技術マニュアル (Cisco Product Documentation DVD) は、Product Documentation Store で発注できます。Product Documentation Store には、次の URL からアクセスできます。  
<http://www.cisco.com/go/marketplace/docstore>
- 日本語マニュアルの DVD は、マニュアルセンターから発注できます。マニュアルセンターには下記よりアクセスください。  
[http://www.cisco.com/japanese/warp/public/3/jp/service/manual\\_j/manual\\_center/index.shtml](http://www.cisco.com/japanese/warp/public/3/jp/service/manual_j/manual_center/index.shtml)
- Cisco Press では、ネットワーク、トレーニング、認定関連の出版物を発行しています。Cisco Press には、次の URL からアクセスできます。  
<http://www.ciscopress.com>
- 日本語のシスコプレスの情報は以下にアクセスください。  
<http://www.seshop.com/se/ciscopress/default.asp>
- 『Internet Protocol Journal』は、インターネットおよびイントラネットの設計、開発、運用を担当するエンジニア向けに、シスコが発行する季刊誌です。『Internet Protocol Journal』には、次の URL からアクセスできます。  
<http://www.cisco.com/ipj>
- 『What's New in Cisco Product Documentation』は、シスコ製品の最新マニュアル リリースに関する情報を提供するオンライン資料です。毎月更新されるこの資料は、製品カテゴリ別にまとめられているため、目的の製品マニュアルを見つけることができます。  
<http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html>
- シスコの Web サイトの各国語版へは、次の URL からアクセスしてください。  
[http://www.cisco.com/public/countries\\_languages.shtml](http://www.cisco.com/public/countries_languages.shtml)



# ネットワークの設定

---

Revised: July 11, 2008

この章では、Cisco Unified Survivable Remote Site Telephony (SRST) ルータが DHCP を実行し、Cisco Unified Communications Manager のフォールバック時に IP Phone と通信するように設定する方法について説明します。

## 内容

- [ネットワークの設定について \(P.45\)](#)
- [ネットワークの設定方法 \(P.46\)](#)
- [関連情報 \(P.59\)](#)

## ネットワークの設定について

WAN リンクに障害が発生した場合、Cisco Unified IP Phone は、Cisco Unified Communications Manager からキープアライブ パケットが受信されなくなったことを検出します。次に、Cisco Unified IP Phone はルータに登録します。Cisco Unified SRST ソフトウェアが自動的にアクティブになり、接続されている Cisco Unified IP Phone すべて (設定された最大数まで) のローカル データベースを作成します。IP Phone は、セントラル Cisco Unified Communications Manager がキープアライブ パケットに確認応答しない場合には、バックアップのコール処理ソースとしてルータに対して問い合わせを行うように設定されます。これで、Cisco Unified SRST ルータが、コールの設定、処理、保持、および終了を実行するようになります。

Cisco Unified Communications Manager は、DHCP を使用して、Cisco Unified IP Phone に Cisco Unified Communications Manager の IP アドレスを提供します。リモートのブランチ オフィスでは、DHCP サービスは、通常、SRST ルータ自体または DHCP リレーを実行する Cisco Unified SRST ルータによって提供されます。DHCP を設定することは、ネットワーク通信を設定する 2 つの主要な作業の 1 つです。もう 1 つの作業は、Cisco Unified SRST ルータが特定の IP アドレスを通じて Cisco IP Phone からメッセージを受信するように設定することです。キープアライブ インターバルもこの段階で設定されます。

## ネットワークの設定方法

ここでは、次の作業について説明します。

- IP ルーティングの有効化 (P.46) (必須)
- MGCP ゲートウェイでの SRST の有効化 (必須)
- Cisco Unified SRST Phone に対する DHCP の設定 (P.51) (必須)
- キープアライブ インターバルの指定 (P.54) (オプション)
- 電話機能をサポートするための Cisco Unified SRST の設定 (P.55) (必須)
- Cisco Unified SRST が有効になっていることの確認 (P.57) (オプション)

### IP ルーティングの有効化

IP ルーティングの有効化については、『*Configuring IP Addressing*』を参照してください。

### MGCP ゲートウェイでの SRST の有効化

MGCP ゲートウェイで SRST をフォールバック モードとして使用するには、SRST および MGCP フォールバックの両方を同じゲートウェイに設定する必要があります。下記のように設定すると、SRST が、音声ポートの制御権と MGCP ゲートウェイでのコール処理の制御権を取得できるようになります。Cisco IOS Release 12.3(14)T でコマンドが変更されているため、インストールした Cisco IOS リリースに対応する設定作業を実行してください。



(注)

下記の設定に記載されているコマンドは、両方とも設定されている場合に限り有効となります。たとえば、`ccm-manager fallback-mgcp` コマンドだけを設定した場合、設定は動作しません。



(注)

MGCP によって制御される PRI が SRST モードに移行した場合は、ルータ上で設定を変更したり、設定の変更を NVRAM に保存したりしないでください。SRST モードで設定を変更して保存した場合、通常の MGCP 動作が回復すると、MGCP によって制御される PRI に障害が発生します。

### Cisco IOS Release 12.3(14)T 以前の MGCP ゲートウェイにおける SRST の設定

Cisco IOS Release 12.3(14)T 以前のソフトウェア リリースを使用している場合、MGCP ゲートウェイで SRST を有効にするには、次の作業を実行します。

#### 要約手順

1. `enable`
2. `configure terminal`
3. `ccm-manager fallback-mgcp`
4. `call application alternate [application-name]`  
または  
`service [alternate | default] service-name location`
5. `exit`

詳細手順

	コマンドまたはアクション	目的
ステップ 1	<p><b>enable</b></p> <p>例: Router&gt; enable</p>	<p>特権 EXEC モードを有効にします。</p> <ul style="list-style-type: none"> <li>プロンプトが表示されたら、パスワードを入力します。</li> </ul>
ステップ 2	<p><b>configure terminal</b></p> <p>例: Router# configure terminal</p>	<p>global コンフィギュレーション モードを開始します。</p>
ステップ 3	<p><b>ccm-manager fallback-mgcp</b></p> <p>例: Router(config)# ccm-manager fallback-mgcp</p>	<p>ゲートウェイのフォールバック機能を有効にし、Cisco Unified Communications Manager が使用不能になった場合に、MGCP 音声ゲートウェイが SRST または他の設定済みアプリケーションを通じてコール処理サービスを提供できるようにします。</p>
ステップ 4	<p><b>call application alternate</b> [<i>application-name</i>] or <b>service</b> [<b>alternate</b>   <b>default</b>] <i>service-name</i> <i>location</i></p> <p>例: Router(config)# call application alternate or Router(config)# service default</p>	<p><b>call application alternate</b> コマンドは、MGCP アプリケーションが使用不能になった場合に、デフォルトの音声アプリケーションが処理を引き継ぐように指定します。<i>application-name</i> 引数はオプションで、ダイヤル ピアのアプリケーションに障害が発生した場合に使用する特定の音声アプリケーションの名前を示します。特定のアプリケーション名が入力されていない場合、ゲートウェイは DEFAULT アプリケーションを使用します。</p> <p>または</p> <p><b>service</b> コマンドは、ダイヤル ピアに特定のスタンドアロン アプリケーションをロードし、設定します。キーワードと引数は次のとおりです。</p> <ul style="list-style-type: none"> <li><b>alternate</b> (オプション)。ダイヤル ピアに設定されているサービスに障害が発生した場合に使用する代替サービス。</li> <li><b>default</b> (オプション)。代替サービスに障害が発生した場合に、ダイヤル ピアのデフォルト サービス(「DEFAULT」)が使用されるように指定します。</li> <li><b>service-name</b> : 音声アプリケーションを識別する名前。</li> <li><b>location</b> : TCL スクリプトまたは VoiceXML ドキュメントの URL 形式のディレクトリおよびファイル名。たとえば、フラッシュ メモリ (flash:filename)、TFTP (tftp://../filename)、または HTTP サーバ (http://../filename) は有効なロケーションです。</li> </ul>
ステップ 5	<p><b>exit</b></p> <p>例: Router(config)# exit</p>	<p>global コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。</p>

## Cisco IOS Release 12.3(14)T 以降の MGCP ゲートウェイにおける SRST の設定

Cisco IOS Release 12.3(14)T 以降のバージョンを使用している場合、MGCP ゲートウェイで SRST を有効にするには、次の作業を実行します。

### 制約事項

Cisco IOS Release 12.3(14)T では、**call application alternate** コマンドは **service** コマンドに置き換えられています。**service** コマンドは、Cisco IOS Release 12.3(14)T 以降のすべてのリリースで使用できません。

### 要約手順

1. **enable**
2. **configure terminal**
3. **ccm-manager fallback-mgcp**
4. **application [application-name]**
5. **global**
6. **service [alternate | default] service-name location**
7. **exit**

### 詳細手順

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b>  例: Router> enable	特権 EXEC モードを有効にします。  • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	<b>configure terminal</b>  例: Router# configure terminal	global コンフィギュレーション モードを開始します。
ステップ 3	<b>ccm-manager fallback-mgcp</b>  例: Router(config)# ccm-manager fallback-mgcp	ゲートウェイのフォールバック機能を有効にし、Cisco Unified Communications Manager が使用不能になった場合に、MGCP 音声ゲートウェイが SRST または他の設定済みアプリケーションを通じてコール処理サービスを提供できるようにします。
ステップ 4	<b>application [application-name]</b>  例: Router(config) application app-xfer	<i>application-name</i> 引数はオプションで、ダイヤル ピアのアプリケーションに障害が発生した場合に使用する特定の音声アプリケーションの名前を示します。特定のアプリケーション名が入力されていない場合、ゲートウェイは DEFAULT アプリケーションを使用します。
ステップ 5	<b>global</b>  例: Router(config)# global	global コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 6	<p><b>service</b> <i>[alternate   default] service-name location</i></p> <p><b>例:</b>                      Router(config) service myapp                      https://myserver/myfile.vxml</p>	<p>ダイヤル ピアに特定のスタンドアロン アプリケーションをロードし、設定します。</p> <ul style="list-style-type: none"> <li>• <i>alternate</i> (オプション)。ダイヤル ピアに設定されているサービスに障害が発生した場合に使用する代替サービス。</li> <li>• <i>default</i> (オプション)。代替サービスに障害が発生した場合に、ダイヤル ピアのデフォルト サービス(「DEFAULT」)が使用されるように指定します。</li> <li>• <i>service-name</i> : 音声アプリケーションを識別する名前。</li> <li>• <i>location</i> : TCL スクリプトまたは VoiceXML ドキュメントの URL 形式のディレクトリおよびファイル名。たとえば、フラッシュ メモリ (flash:filename)、TFTP (tftp://../filename)、または HTTP サーバ (http://../filename) は有効なロケーションです。</li> </ul>
ステップ 7	<p><b>exit</b></p> <p><b>例:</b>                      Router(config)# exit</p>	<p>global コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。</p>

### Cisco IOS Release 12.3(14)T を使用する MGCP ゲートウェイで SRST を有効にする設定の例

次に、Cisco IOS Release 12.3(14)T 以降のバージョンを使用している場合の、MGCP ゲートウェイでの SRST の設定例を示します。

```

isdn switch-type primary-net5
!
!
ccm-manager fallback-mgcp
ccm-manager mgcp
ccm-manager config
mta receive maximum-recipients 0
!
controller E1 1/0
pri-group timeslots 1-12,16 service mgcp
!
controller E1 1/1
!
!
!
interface Ethernet0/0
ip address 10.48.80.9 255.255.255.0
half-duplex
!
interface Serial1/0:15
no ip address
no logging event link-status
isdn switch-type primary-net5
isdn incoming-voice voice
isdn bind-13 ccm-manager
no cdp enable
!
!
!
call rsvp-sync
    
```

```
!
call application alternate DEFAULT

!--- For Cisco IOS® Software Release 12.3(14)T or later,
this command was replaced by the service command
in global application configuration mode.
application
global
service alternate Default

!
voice-port 1/0:15
!
mgcp
mgcp dtmf-relay voip codec all mode cisco
mgcp package-capability rtp-package
mgcp sdp simple
!
mgcp profile default
!
!
!
dial-peer cor custom
!
!
!
dial-peer voice 10 pots
application mgcpapp
incoming called-number
destination-pattern 9T
direct-inward-dial
port 1/0:15

!
!
call-manager-fallback
limit-dn 7960 2
ip source-address 10.48.80.9 port 2000
max-ephones 10
max-dn 32
dialplan-pattern 1 704.... extension-length 4
keepalive 20
default-destination 5002
alias 1 5003 to 5002
call-forward busy 5002
call-forward noan 5002 timeout 12
time-format 24
!
!
line con 0
exec-timeout 0 0
line aux
```



## Cisco Unified SRST Phone に対する DHCP の設定

この作業を実行するには、ネットワークに DHCP を設定しておく必要があります。DHCP 設定の詳細については、『*Cisco IOS DHCP Server*』と Cisco Unified Communications Manager のマニュアルを参照してください。

Cisco IP Phone は、Cisco Unified SRST システムに接続されると、自動的に DHCP サーバに対して問い合わせを行います。DHCP サーバは応答すると、Cisco IP Phone に IP アドレスを割り当て、DHCP オプション 150 を通じて TFTP サーバの IP アドレスを提供します。次に、電話機は Cisco Unified Communications Manager システム サーバに登録し、DHCP サーバから提供された Cisco Unified Communications Manager TFTP サーバアドレスからコンフィギュレーション ファイルと電話機ファームウェア ファイルの取得を試みます。

ネットワークを設定する場合は、DHCP サーバをサイトのローカル側に設定します。SRST ルータを使用して DHCP サービスを提供することもできます (推奨)。DHCP サーバが WAN を介して配置されている場合、WAN の停止が長引くと、Cisco Unified IP Phone の DHCP リース期間が期限切れになる可能性があります。期限切れになると、電話機の IP アドレスが失われることがあります。その場合は、サービスが停止します。DHCP リースが期限切れになって DHCP サーバを使用できなくなった場合、電話機をリブートしても、電話機は再度アクティブにはなりません。これは、電話機が IP アドレスやその他の情報を取得できないためです。DHCP サーバをリモートサイトのローカル側に配置すると、WAN の障害が長引いた場合でも、電話機が IP アドレス リースを継続的に更新できることが保証されます。

Cisco Unified IP Phone に対する DHCP サービスを設定するには、次のいずれかの作業を選択します。

- [単一の DHCP IP アドレス プールを定義する \(P.51\)](#): この方法は、Cisco Unified SRST ルータが DHCP サーバであり、すべての DHCP クライアントに対して単一の共有アドレス プールを使用できる場合に使用します。
- [各 Cisco Unified IP Phone に対する個別の DHCP IP アドレス プールを定義する \(P.52\)](#): この方法は、Cisco Unified SRST ルータが DHCP サーバであり、IP Phone 以外の電話機の DHCP クライアント用に別のプールが必要な場合に使用します。
- [DHCP リレー サーバを定義する \(P.53\)](#): この方法は、Cisco Unified SRST ルータが DHCP サーバではなく、IP Phone からの DHCP 要求を別のルータの DHCP サーバにリレーする場合に使用します。

### 単一の DHCP IP アドレス プールを定義する

この作業では、IP アドレスの大規模な共有プールを作成します。このプールでは、すべての DHCP クライアントが、オプション 150 の TFTP サーバ IP アドレスを含む同一の情報を受信します。この方法を選択すると、設定する DHCP プールが 1 つだけで済みます。ただし、単一の DHCP IP アドレス プールを定義すると、一部の (IP Phone 以外の電話機の) クライアントが別の TFTP サーバアドレスを使用することが必要になった場合に問題となる可能性があります。

#### 要約手順

1. `ip dhcp pool pool-name`
2. `network ip-address [mask | prefix-length]`
3. `option 150 ip ip-address`
4. `default-router ip-address`
5. `exit`

## ■ ネットワークの設定方法

## 詳細手順

	コマンドまたはアクション	目的
ステップ 1	<code>ip dhcp pool pool-name</code>  例: Router(config)# ip dhcp pool mypool	DHCP サーバ アドレス プールの名前を作成し、DHCP プール コンフィギュレーション モードを開始します。
ステップ 2	<code>network ip-address [mask   prefix-length]</code>  例: Router(config-dhcp)# network 10.0.0.0 255.255.0.0	DHCP アドレス プールの IP アドレスと、オプションのマスクまたはアドレス プレフィックスのビット数 (前にスラッシュを付ける) を指定します。
ステップ 3	<code>option 150 ip ip-address</code>  例: Router(config-dhcp)# option 150 ip 10.0.22.1	Cisco IP Phone がイメージコンフィギュレーション ファイルをダウンロードする際のダウンロード元となる TFTP サーバ アドレスを指定します。このアドレスは、Cisco Unified Communications Manager の IP アドレスにする必要があります。
ステップ 4	<code>default-router ip-address</code>  例: Router(config-dhcp)# default-router 10.0.0.1	Cisco Unified IP Phone が直接接続されるルータを指定します。  <ul style="list-style-type: none"> <li>このルータは、WAN の停止時に SRST サービスを取得するために使用されるデフォルト アドレスとなるため、Cisco Unified SRST ルータにする必要があります。Cisco IP Phone は、Cisco Unified SRST ルータに接続されている限り、必要なネットワークの詳細情報を取得できません。</li> </ul>
ステップ 5	<code>exit</code>  例: Router(config-dhcp)# exit	DHCP プール コンフィギュレーション モードを終了します。

## 各 Cisco Unified IP Phone に対する個別の DHCP IP アドレス プールを定義する

この作業では、DHCP サーバ アドレス プールの名前を作成し、IP アドレスを指定します。この方法では、Cisco Unified IP Phone ごとにエントリを作成する必要があります。

## 要約手順

1. `ip dhcp pool pool-name`
2. `host ip-address subnet-mask`
3. `option 150 ip ip-address`
4. `default-router ip-address`
5. `exit`

詳細手順

	コマンドまたはアクション	目的
ステップ 1	<code>ip dhcp pool pool-name</code>  例: Router(config)# ip dhcp pool pool2	DHCP サーバ アドレス プールの名前を作成し、DHCP プール コンフィギュレーション モードを開始します。
ステップ 2	<code>host ip-address subnet-mask</code>  例: Router(config-dhcp)# host 10.0.0.0 255.255.0.0	電話機で使用する IP アドレスを指定します。
ステップ 3	<code>option 150 ip ip-address</code>  例: Router(config-dhcp)# option 150 ip 10.0.22.1	Cisco IP Phone がイメージコンフィギュレーション ファイルをダウンロードする際のダウンロード元となる TFTP サーバ アドレスを指定します。このアドレスは、Cisco Unified Communications Manager の IP アドレスにする必要があります。
ステップ 4	<code>default-router ip-address</code>  例: Router(config-dhcp)# default-router 10.0.0.1	Cisco Unified IP Phone が直接接続されるルータを指定します。  <ul style="list-style-type: none"> <li>このルータは、WAN の停止時に SRST サービスを取得するために使用されるデフォルトアドレスとなるため、Cisco Unified SRST ルータにする必要があります。Cisco IP Phone は、Cisco Unified SRST ルータに接続されている限り、必要なネットワークの詳細情報を取得できます。</li> </ul>
ステップ 5	<code>exit</code>  例: Router(config-dhcp)# exit	DHCP プール コンフィギュレーション モードを終了します。

DHCP リレー サーバを定義する

この作業では、Cisco Unified IP Phone が接続される LAN インターフェイスに DHCP リレーを設定し、DHCP クライアント（電話機）からの要求を DHCP サーバにリレーするための Cisco IOS DHCP サーバ機能を有効にします。DHCP 設定の詳細については、『[Cisco IOS DHCP Server](#)』を参照してください。

デフォルトでは、Cisco IOS DHCP サーバ機能は、ルータで有効になっています。DHCP サーバが Cisco Unified SRST ルータで有効になっていない場合は、次の手順に従って有効にします。

要約手順

1. `service dhcp`
2. `interface type number`
3. `ip helper-address ip-address`
4. `exit`

## 詳細手順

	コマンドまたはアクション	目的
ステップ 1	<code>service dhcp</code>  例： Router(config)# service dhcp	ルータで Cisco IOS DHCP サーバ機能を有効にします。
ステップ 2	<code>interface type number</code>  例： Router(config)# interface serial 0	指定されたインターフェイスのインターフェイス コンフィギュレーション モードを開始します。詳細については、『 <a href="#">Cisco IOS Interface and Hardware Component Command Reference, Release 12.3T</a> 』を参照してください。
ステップ 3	<code>ip helper-address ip-address</code>  例： Router(config-if)# ip helper-address 10.0.22.1	TFTP サーバおよび Domain Name System (DNS; ドメイン ネーム システム) の要求に対する、認識されないブロードキャストのヘルパー アドレスを指定します。サーバが別々のホスト上にある場合は、サーバごとに <code>ip helper-address</code> コマンドを使用する必要があります。また、複数のサーバに <code>ip helper-address</code> コマンドを使用すると、複数の TFTP サーバターゲットを設定できます。
ステップ 4	<code>exit</code>  例： Router(config-if)# exit	インターフェイス コンフィギュレーション モードを終了します。

## キープアライブ インターバルの指定

キープアライブ インターバルは、ネットワーク デバイスが送信するキープアライブ メッセージの時間間隔です。キープアライブ メッセージとは、ネットワーク デバイスが別のネットワーク デバイスに対し、2 者間の仮想回線が引き続きアクティブであることを通知するために送信するメッセージのことです。



(注) メッセージの時間間隔にデフォルトの 30 秒を使用する場合、この作業を実行する必要はありません。

## 要約手順

1. `call-manager-fallback`
2. `keepalive seconds`
3. `exit`

詳細手順

	コマンドまたはアクション	目的
ステップ 1	<b>call-manager-fallback</b>  例: Router(config)# call-manager-fallback	call-manager-fallback コンフィギュレーション モードを開始します。
ステップ 2	<b>keepalive seconds</b>  例: Router(config-cm-fallback)# keepalive 60	Cisco Unified IP Phone がルータに送信するキープアライブメッセージの時間間隔を秒単位で設定します。  • <i>seconds</i> : 範囲は 10 ~ 65535 です。デフォルトは 30 です。
ステップ 3	<b>exit</b>  例: Router(config-cm-fallback)# exit	call-manager-fallback コンフィギュレーション モードを終了します。

例

次の例では、キープアライブ インターバルを 45 秒に設定します。

```
call-manager-fallback
keepalive 45
```

電話機能をサポートするための Cisco Unified SRST の設定



ヒント


Cisco Unified SRST が有効になっている場合、Cisco Unified Communications Manager フォールバックモードになっているときは Cisco Unified IP Phone を再設定する必要はありません。これは、電話機が Cisco Unified Communications Manager に対して使用していた設定と同じものを保持するためです。

Cisco Unified IP Phone の機能をサポートするようにルータの Cisco Unified SRST を設定するには、global コンフィギュレーション モードを開始して、次のコマンドを使用します。

要約手順

1. **call-manager-fallback**
2. **ip source-address ip-address [port port] [any-match | strict-match]**
3. **max-dn max-directory-numbers [dual-line] [preference preference-order]**
4. **max-ephones max-phones**
5. **limit-dn {7910 | 7935 | 7940 | 7960} max-lines**
6. **exit**

## 詳細手順

	コマンドまたはアクション	目的
ステップ 1	<b>call-manager-fallback</b>  <b>例:</b> Router(config)# call-manager-fallback	call-manager-fallback コンフィギュレーション モードを開始します。
ステップ 2	<b>ip source-address ip-address [port port]</b> <b>[any-match   strict-match]</b>  <b>例:</b> Router(config-cm-fallback)# ip source-address 10.6.21.4 port 2002 strict-match	ルータが指定の IP アドレスを通じて Cisco IP Phone からのメッセージを受信できるようにし、IP アドレスの厳密な検証を行います。デフォルトのポート番号は 2000 です。
ステップ 3	<b>max-dn max-directory-numbers [dual-line]</b> <b>[preference preference-order]</b>  <b>例:</b> Router(config-cm-fallback)# max-dn 15 dual-line preference 1	<p>ルータでサポートできる Directory Number( DN; 電話番号) または仮想音声ポートの最大数を設定し、二重回線モードをアクティブにします。</p> <ul style="list-style-type: none"> <li>• <b>max-directory-numbers</b> : ルータでサポートされる電話番号または仮想音声ポートの最大数。最大数は、プラットフォームによって異なります。デフォルトは 0 です。詳細については、<a href="#">P.31 の「プラットフォームとメモリのサポート」</a>を参照してください。</li> <li>• <b>dual-line</b> ( オプション )。Cisco Unified Communications Manager フォールバック モードの IP Phone が、2 つのチャンネルを持つ仮想音声ポートを使用できるようにします。</li> <li>• <b>preference preference-order</b> ( オプション )。プライマリ番号に関連付けられたすべての電話番号に対する VoIP ダイアル ピアを作成する場合のグローバル プリファレンスを設定します。範囲は 0 ~ 10 です。デフォルトは 0 ( 最高の優先順位 ) です。</li> </ul> <p><b>alias</b> コマンドにも、<b>alias</b> コマンドのプリファレンス値を設定する <b>preference</b> キーワードが用意されています。<b>alias</b> コマンドの <b>preference</b> キーワードを設定すると、<b>max-dn</b> コマンドによるデフォルトのプリファレンスセットを上書きできます。<b>max-dn</b> コマンドと <b>alias</b> コマンドの併用に関する詳細については、<a href="#">P.76 の「コールの再ルーティングの設定」</a>を参照してください。</p> <p> <b>(注)</b> 電話番号または仮想音声ポートの最大数の設定後にその制限を引き下げるには、ルータをリブートする必要があります。</p>

	コマンドまたはアクション	目的
ステップ 4	<p><code>max-ephones max-phones</code></p> <p>例: Router(config-cm-fallback)# max-ephones 24</p>	<p>ルータがサポートできる Cisco IP Phone の最大数を設定します。デフォルトは 0 です。最大数は、プラットフォームによって異なります。詳細については、P.31 の「プラットフォームとメモリのサポート」を参照してください。</p> <p> (注) Cisco IP Phone の最大数の設定後にその制限を引き下げるには、ルータをリブートする必要があります。</p>
ステップ 5	<p><code>limit-dn {7910   7935   7940   7960}</code> <code>max-lines</code></p> <p>例: Router(config-cm-fallback)# limit-dn 7910 2</p>	<p>Cisco Unified Communications Manager のフォールバック時における Cisco IP Phone の電話番号の回線数を制限します。</p> <p> (注) このコマンドは、いずれかの電話機が実際に Cisco Unified SRST ルータに登録する前の、Cisco Unified SRST ルータの最初の設定時に設定する必要があります。ただし、回線数は後で変更できます。</p> <p>回線の最大数の設定値は 1 ~ 6 のいずれかです。回線の最大数は、デフォルトで 6 に設定されています。アクティブな電話機の最後の回線番号がこの制限を超えた場合は、電話機のリセットに関する警告情報が表示されます。</p>
ステップ 6	<p><code>exit</code></p> <p>例: Router(config-cm-fallback)# exit</p>	<p>call-manager-fallback コンフィギュレーション モードを終了します。</p>

## Cisco Unified SRST が有効になっていることの確認

Cisco Unified SRST 機能が有効になっていることを確認するには、次の手順を実行します。

- ステップ 1 `show running-config` コマンドを入力して、設定を確認します。
- ステップ 2 `show call-manager-fallback all` コマンドを入力して、Cisco Unified SRST 機能が有効になっていることを確認します。
- ステップ 3 ネットワーク内の Cisco IP Phone の Settings 画面を使用して、電話機のデフォルトルータの IP アドレスが Cisco Unified SRST ルータの IP アドレスと一致していることを確認します。
- ステップ 4 いずれかの Cisco IP Phone の TCP ポート 2000 Skinny Client Control Protocol (SCCP) 接続を一時的にブロックして、Cisco IP Phone に強制的に Cisco Unified Communications Manager への接続を切断させ、Cisco Unified SRST ルータに登録させるには、次の手順を実行します。
  - a. 適切な IP access-list コマンドを使用して、Cisco Unified IP Phone を Cisco Unified Communications Manager から一時的に切断します。

WAN 接続の障害時に、Cisco Unified SRST が有効になっている場合、Cisco Unified IP Phone には、電話機が Cisco Unified Communications Manager フォールバック モードで動作していることを通知するメッセージが表示されます。Cisco Unified Communications Manager フォールバック モードで動作している場合、Cisco IP Phone 7960 および Cisco IP Phone 7940 には「CM Fallback Service Operating」というメッセージが表示され、Cisco IP Phone 7910 には「CM Fallback Service」というメッセージが表示されます。Cisco Unified Communications Manager が回復すると、メッセージが消去され、Cisco IP Phone の機能がすべて回復します。

- b. 適切な `access-list` コマンドの `no` 形式を入力して、電話機の通常のサービスを回復させます。
- c. `debug ephone register` コマンドを使用して、Cisco Unified SRST ルータでの Cisco IP Phone の登録プロセスを監視します。
- d. `show ephone` コマンドを使用して、Cisco Unified SRST ルータに登録された Cisco IP Phone を表示します。

## トラブルシューティング

Cisco Unified SRST の設定のトラブルシューティングを行うには、次のコマンドを使用します。

- Cisco IP Phone に関するキープアライブ デバッグを設定するには、`debug ephone keepalive` コマンドを使用します。
- Cisco IP Phone に関する登録デバッグを設定するには、`debug ephone register` コマンドを使用します。
- Cisco IP Phone に関する状態デバッグを設定するには、`debug ephone state` コマンドを使用します。
- Cisco IP Phone に関する詳細デバッグを設定するには、`debug ephone detail` コマンドを使用します。
- Cisco IP Phone に関するエラー デバッグを設定するには、`debug ephone error` コマンドを使用します。
- Cisco IP Phone に関するコール統計情報デバッグを設定するには、`debug ephone statistics` コマンドを使用します。
- 音声パケット レベルのデバッグを設定し、1024 個の音声パケットごとに 1 つの音声パケットの内容を表示するには、`debug ephone pak` コマンドを使用します。
- すべての SCCP メッセージについて未加工で低レベルのプロトコル デバッグを表示するには、`debug ephone raw` コマンドを使用します。

その他のデバッグについては、Cisco IOS ソフトウェア リリースに適合する『[Cisco IOS Debug Command Reference](#)』を参照してください。このドキュメントを入手するには、[Cisco IOS Software Support Resources](#) に移動し、適切なリリース バージョンをクリックしてから、**Command References** をクリックします。



## 関連情報

次のステップでは、電話機を設定し、ダイヤル トーンを取得します。手順については、「[Cisco Unified IP Phone の設定](#)」の章を参照してください。

追加情報については、「[Cisco Unified SRST の概要](#)」の章の P.40 の「[その他の資料](#)」を参照してください。





# Cisco Unified IP Phone の設定

Revised: July 11, 2008

この章では、発信者に表示されるディスプレイおよび機能の設定方法や、Cisco Unified Communications Manager のフォールバック時における Cisco Unified IP Phone の使用方法について説明します。

## 内容

- [Cisco Unified IP Phone の設定について \(P.61\)](#)
- [Cisco Unified IP Phone の設定方法 \(P.62\)](#)
- [Cisco Unified SRST に関する Cisco IP Communicator の設定方法 \(P.71\)](#)
- [関連情報 \(P.72\)](#)

## Cisco Unified IP Phone の設定について

Cisco Unified SRST に関する Cisco Unified IP Phone の設定には制限があります。これは、IP Phone が、Cisco Unified Communications Manager のフォールバック時も Cisco Unified Communications Manager の設定のほとんどすべてを保持するためです。Cisco Unified Communications Manager のフォールバック時に Cisco Unified IP Phone に表示される日付形式、時刻形式、言語、およびシステム メッセージを設定できます。これら 4 つの設定にはデフォルトが用意されています。使用可能な言語オプションは、使用する IP Phone と Cisco Unified Communications Manager のバージョンによって異なります。また、第 2 発信音も設定できます。第 2 発信音は、電話機ユーザが定義済みの PSTN アクセス プレフィックスをダイヤルしたときに生成し、追加の番号がダイヤルされたときに終了することができます。Cisco Unified Communications Manager のフォールバック時に二重回線電話機を動作させる場合は、二重回線電話機を設定する必要があります。

## Cisco Unified IP Phone の設定方法

ここでは、次の作業について説明します。

- IP Phone のクロック、日付、および時刻の形式の設定 (P.62) (オプション)
- IP Phone の言語表示の設定 (P.63) (オプション)
- Cisco Unified IP Phone 用にカスタマイズされたシステム メッセージの設定 (P.65) (オプション)
- 第 2 発信音の設定 (P.66) (オプション)
- 二重回線電話機の設定 (P.66) (特定の条件下で必須)
- 各ボタンでの 8 回線 (八重回線) の設定 (P.68) (オプション)

### IP Phone のクロック、日付、および時刻の形式の設定

Cisco Unified IP Phone 7970G および Cisco Unified IP Phone 7971G-GE の各 IP Phone は、Cisco Unified Communications Manager から適切なタイムゾーンを取得します。また、SRST 登録時に SRST ルータから Coordinated Universal Time (UTC; 世界標準時) 時刻も受信します。SRST モードになっている場合、電話機は、タイムゾーンと UTC 時刻を取得し、タイムゾーンのオフセットを適用して正しい時刻を表示します。

Cisco IP Phone 7960 やその他の類似した SCCP 電話機 (Cisco IP Phone 7940 など) は、SRST 登録時に SRST ルータのローカル時刻から、表示クロックの情報を取得します。Cisco Unified SRST ルータが、Network Time Protocol (NTP; ネットワーク タイム プロトコル) を使用して Cisco Unified SRST ルータの時刻を NTP タイムサーバと自動的に同期させるように設定されている場合、ルータには UTC 時刻だけが送信されます。これは、NTP サーバが世界のあらゆる場所 (タイムゾーン) に物理的に配置される可能性があるためです。正しいローカル時刻を表示することは重要であるため、**clock timezone** コマンドを使用して、Cisco Unified SRST ルータの時刻を調節またはオフセット処理します。

Cisco Unified Communications Manager フォールバック モードのときにすべての Cisco Unified IP Phone のディスプレイに表示される日付と時刻の形式を設定するには、**date-format** コマンドと **time-format** コマンドを下記の設定に従って使用します。

#### 要約手順

1. **clock timezone** *zone hours-offset [minutes-offset]*
2. **call-manager-fallback**
3. **date-format** {*mm-dd-yy | dd-mm-yy | yy-dd-mm | yy-mm-dd*}
4. **time-format** {*12 | 24*}
5. **exit**

## 詳細手順

	コマンドまたはアクション	目的
ステップ 1	<b>clock timezone zone hours-offset</b> [minutes-offset]  <b>例:</b> Router(config)# clock timezone PST -8	表示用のタイムゾーンを設定します。 <ul style="list-style-type: none"> <li>• <i>zone</i> : 標準時が有効になっているときに表示するタイムゾーンの名前。zone 引数の長さは 7 文字に制限されています。</li> <li>• <i>hours-offset</i> : 世界標準時 (UTC) との時間差 (時間数)</li> <li>• <i>minutes-offset</i> (オプション)。UTC との時間差 (分数)</li> </ul>
ステップ 2	<b>call-manager-fallback</b>  <b>例:</b> Router(config)# call-manager-fallback	call-manager-fallback コンフィギュレーションモードを開始します。
ステップ 3	<b>date-format {mm-dd-yy   dd-mm-yy   yy-dd-mm   yy-mm-dd}</b>  <b>例:</b> Router(config-cm-fallback)# date-format yy-dd-mm	IP Phone の表示用の日付形式を設定します。選択肢は、mm-dd-yy、dd-mm-yy、yy-dd-mm、および yy-mm-dd です。表示の意味は次のとおりです。 <ul style="list-style-type: none"> <li>• dd : 日</li> <li>• mm : 月</li> <li>• yy : 年</li> </ul> デフォルトでは、mm-dd-yy に設定されています。
ステップ 4	<b>time-format {12   24}</b>  <b>例:</b> Router(config-cm-fallback)# time-format 24	ルータに登録された Cisco Unified IP Phone すべての時刻の表示形式を設定します。デフォルトでは、12 時間制に設定されています。
ステップ 5	<b>exit</b>  <b>例:</b> Router(config-cm-fallback)# exit	call-manager-fallback コンフィギュレーションモードを終了します。

## 例

次の例では、タイムゾーンを、UTC から 8 時間遅れの Pacific Standard Time (PST; 太平洋標準時) に設定し、時刻の表示形式を 24 時間制に設定します。

```
Router(config)# clock timezone PST -8
Router(config)# call-manager-fallback
Router(config-cm-fallback)# time-format 24
```

## IP Phone の言語表示の設定

Cisco Unified Communications Manager のフォールバック時、Cisco Unified IP Phone の言語表示は、デフォルトで US (米国) の ISO-3166 国コードに設定されます。Cisco Unified IP Phone 7940 および Cisco Unified IP Phone 7960 では、**user-locale** コマンドを使用して、さまざまな言語 (文字セットとスペリング規則) に設定することができます。



**(注)** この設定オプションは、Cisco Unified Communications Manager V3.2 以降の下で動作している Cisco SRST V2.1 以降のバージョンで使用できます。Cisco Unified SRST V2.1 および Cisco Unified Communications Manager V3.2 よりも前のソフトウェアを含むシステムでは、デフォルトの国である米国 (US) だけを使用できます。

## 要約手順

1. `call-manager-fallback`
2. `user-locale country-code`
3. `exit`

## 詳細手順

	コマンドまたはアクション	目的
ステップ 1	<code>call-manager-fallback</code>  例: Router(config)# <code>call-manager-fallback</code>	call-manager-fallback コンフィギュレーション モードを開始します。
ステップ 2	<code>user-locale country-code</code>  例: Router(config-cm-fallback)# <code>user-locale ES</code>	Cisco IP Phone 7940 および Cisco IP Phone 7960 に表示する国別の言語を選択します。  次の ISO-3166 コードは、Cisco Communications Manager V3.2 以降のバージョンの下で動作している Cisco SRST および Cisco Unified SRST システムで使用できます。 <ul style="list-style-type: none"> <li>• DE：ドイツ語</li> <li>• DK：デンマーク語</li> <li>• ES：スペイン語</li> <li>• FR：フランス語</li> <li>• IT：イタリア語</li> <li>• JP：日本語のカタカナ（Cisco Unified Communications Manager V4.0 以降のバージョンで使用可能）</li> <li>• NL：オランダ語</li> <li>• NO：ノルウェー語</li> <li>• PT：ポルトガル語</li> <li>• RU：ロシア語</li> <li>• SE：スウェーデン語</li> <li>• US：米国英語（デフォルト）</li> </ul>
ステップ 3	<code>exit</code>  例: Router(config-cm-fallback)# <code>exit</code>	call-manager-fallback コンフィギュレーション モードを終了します。

## 例

次の例は、ポルトガルのユーザ ロケールの設定を示しています。

```
call-manager-fallback
user-locale PT
```

## Cisco Unified IP Phone 用にカスタマイズされたシステム メッセージの設定

`system message` コマンドは、Cisco Unified Communications Manager のフォールバック時に Cisco Unified IP Phone 7910、Cisco Unified IP Phone 7940G、および Cisco Unified IP Phone 7960G のすべてのユニットに表示されるシステム メッセージをカスタマイズするときに使用されます。

コマンドには、`primary` と `secondary` のどちらかのキーワードを含める必要があります。`primary` キーワードは、フォールバック時に静的なテキスト メッセージをサポートできる IP Phone (Cisco IP Phone 7940 および Cisco IP Phone 7960 ユニットなど) に対して使用します。フォールバック モードのプライマリ IP Phone に対するデフォルトの表示メッセージは「CM Fallback Service Operating」です。

`secondary` キーワードは、静的なテキスト メッセージをサポートしない、表示領域の限られた Cisco Unified IP Phone (Cisco IP Phone 7910 など) に対して使用します。セカンダリ IP Phone では、フォールバック時にメッセージが点滅します。フォールバック モードのセカンダリ IP Phone に対するデフォルトの表示メッセージは「CM Fallback Service」です。

表示メッセージに対する変更は、設定後または各コールの終了後ただちに反映されます。



(注) 通常のインサービスの静的なテキスト メッセージは、Cisco Unified Communications Manager によって制御されます。

### 要約手順

1. `call-manager-fallback`
2. `system message {primary primary-string | secondary secondary-string}`
3. `exit`

### 詳細手順

	コマンドまたはアクション	目的
ステップ 1	<code>call-manager-fallback</code>  例: Router(config)# call-manager-fallback	call-manager-fallback コンフィギュレーション モードを開始します。
ステップ 2	<code>system message {primary primary-string   secondary secondary-string}</code>  例: Router(config-cm-fallback)# system message primary Custom Message	フォールバック モードの IP Phone に対するシステム表示メッセージのテキストを宣言します。  <ul style="list-style-type: none"> <li>• <code>primary primary-string</code>: フォールバック時に静的なテキスト メッセージをサポートできる Cisco Unified IP Phone (Cisco Unified IP Phone 7940 および Cisco Unified IP Phone 7960 ユニットなど) に対して使用します。約 27 ~ 30 文字の文字列が使用可能です。</li> <li>• <code>secondary secondary-string</code>: 静的なテキスト メッセージをサポートしない Cisco Unified IP Phone (Cisco Unified IP Phone 7910 など) に対して使用します。約 20 文字の文字列が使用可能です。</li> </ul>
ステップ 3	<code>exit</code>  例: Router(config-cm-fallback)# exit	call-manager-fallback コンフィギュレーション モードを終了します。

## 例

次の例では、ルータ上のすべての Cisco Unified IP Phone に対するシステム表示メッセージとして「SRST V3.0」を設定します。

```
call-manager-fallback
system message primary SRST V3.0
system message secondary SRST V3.0
exit
```

## 第 2 発信音の設定

第 2 発信音は、電話機ユーザが定義済みの PSTN アクセス プレフィックスをダイヤルしたときに生成し、追加の番号がダイヤルされたときに終了することができます。たとえば、外線に接続するために番号 9 をダイヤルすると、第 2 発信音が聞こえます。

## 要約手順

1. `call-manager-fallback`
2. `secondary-dialtone digit-string`
3. `exit`

## 詳細手順

	コマンドまたはアクション	目的
ステップ 1	<code>call-manager-fallback</code>  例: Router(config)# call-manager-fallback	call-manager-fallback コンフィギュレーションモードを開始します。
ステップ 2	<code>secondary-dialtone digit-string</code>  例: Router(config-cm-fallback)# secondary-dialtone 9	数字列がダイヤルされたときに第 2 発信音をアクティブにします。
ステップ 3	<code>exit</code>  例: Router(config-cm-fallback)# exit	call-manager-fallback コンフィギュレーションモードを終了します。

## 例

次の例では、番号 8 によって第 2 発信音をトリガーするように設定します。

```
call-manager-fallback
secondary-dialtone 8
```

## 二重回線電話機の設定

Cisco Unified Communications Manager のフォールバック時に二重回線電話機を動作させる場合は、二重回線電話機を設定する必要があります。また、打診転送も設定する必要があります (P.93 の「Cisco SRST 3.0 での H.450.2 および H.450.3 を使用した打診コール転送および自動転送」を参照)。

Cisco Unified Communications Manager のフォールバック時に二重回線 IP Phone をサポートするには、`max-dn` コマンドを使用します。二重回線 IP Phone は、1 つの音声ポートと、2 つの独立したコールを処理する 2 つのチャンネルを備えています。この機能では、1 つの電話回線ボタンで、コールウェイトリング、コール転送、および会議の各機能を使用できます。



二重回線モードでは、各 IP Phone とそれに関連付けられた回線ボタンでコールを 2 つまでサポートできます。同一回線上の 2 つのコールのどちらかを選択するには、電話機のディスプレイの下部にある青色の Navigation ボタンを使用します。二重回線チャンネルのどちらかが特定の電話機で使用されている場合、ephone-dn を共有する他の電話機ではセカンダリ チャンネルを使用できません。セカンダリ チャンネルは、プライマリ二重回線チャンネル用に予約されます。

セカンダリ チャンネルに対するハンティングは無効にすることをお勧めします。詳細については、P.89 の「ダイヤル ピアとチャンネルのハンティングの設定」を参照してください。

## 要約手順

1. `call-manager-fallback`
2. `max-dn max-directory-numbers [dual-line] [preference preference-order]`
3. `exit`

## 詳細手順

	コマンドまたはアクション	目的
ステップ 1	<b>call-manager-fallback</b>  <b>例:</b> Router(config)# call-manager-fallback	call-manager-fallback コンフィギュレーション モードを開始します。
ステップ 2	<b>max-dn max-directory-numbers [dual-line] [preference preference-order]</b>  <b>例:</b> Router(config-cm-fallback)# max-dn 15 dual-line preference 1	ルータでサポートできる Directory Number( DN; 電話番号) または仮想音声ポートの最大数を設定し、二重回線モードをアクティブにします。 <ul style="list-style-type: none"> <li>• <b>max-directory-numbers</b> : ルータでサポートされる電話番号または仮想音声ポートの最大数。最大数は、プラットフォームによって異なります。デフォルトは 0 です。詳細については、P.31 の「プラットフォームとメモリのサポート」を参照してください。</li> <li>• <b>dual-line</b> ( オプション )。Cisco Unified Communications Manager フォールバック モードの IP Phone が、2 つのチャンネルを持つ仮想音声ポートを使用できるようにします。</li> <li>• <b>preference preference-order</b> ( オプション )。プライマリ番号に関連付けられたすべての電話番号に対する VoIP ダイヤル ピアを作成する場合のグローバルプリファレンスを設定します。範囲は 0 ~ 10 です。デフォルトは 0 ( 最高の優先順位 ) です。   <b>alias</b> コマンドにも、<b>alias</b> コマンドのプリファレンス値を設定する <b>preference</b> キーワードが用意されています。<b>alias</b> コマンドの <b>preference</b> キーワードを設定すると、<b>max-dn</b> コマンドによるデフォルトのプリファレンスセットを上書きできます。<b>max-dn</b> コマンドと <b>alias</b> コマンドの併用に関する詳細については、P.76 の「コールの再ルーティングの設定」を参照してください。</li> </ul>
ステップ 3	<b>exit</b>  <b>例:</b> Router(config-cm-fallback)# exit	call-manager-fallback コンフィギュレーション モードを終了します。

## 例

次の例では、ルータでサポートできる DN または仮想音声ポートの最大数を 10 に設定し、Cisco Unified Communications Manager フォールバック モードのすべての IP Phone に対して二重回線モードをアクティブにします。

```
call-manager-fallback
max-dn 10 dual-line
exit
```

## 各ボタンでの 8 回線（八重回線）の設定

八重回線機能では、1 つのボタンで最大 8 つのアクティブ コール（着信と発信の両方）がサポートされます。八重回線電話番号に 8 つのコールが着信した場合、それぞれの呼び出し音は同時に鳴ります。いずれかの着信コールに 응답すると、呼び出し音が停止し、残りの 7 つの着信コールに対応するコール ウェイティング トーンが聞こえます。

八重回線電話番号への着信コールに 응답すると、 응답した電話機は接続状態になります。電話番号を共有する他の電話機は remoteMultiline 状態になります。ここで新しいコールが着信した場合、現在のコールに接続されている電話機にはコール ウェイティング トーンが送信され、remoteMultiline 状態になっている他の電話機には呼び出し音が送信されます。電話番号を共有する電話機はすべて、未応答の着信コールをピックアップできます。

複数の電話機で共有されている八重回線電話番号において複数の着信コールの呼び出し音が鳴っている場合、コールに 응답した電話機では呼び出し音が停止し、残りの未応答のコールに対応するコール ウェイティング トーンが聞こえます。電話番号を共有する他の ephone には、呼び出し中のコールに対応する複数のインスタンスが表示されます。八重回線電話番号の接続済みコールが保留になった場合、この電話番号を共有する電話機はすべて、保留中のコールをピックアップできるようになります。特定の電話機がコール転送または会議作成を処理している場合、八重回線電話番号を共有する他の電話機がその処理中のコールを取得することはできません。

八重回線に新しいコールが着信した場合、システムは `huntstop chan tag` コマンド（`tag` は 1 ~ 8 の番号）を使用して、次に使用可能なアイドル回線を検索します。アイドルチャンネルは、番号の最も小さいものから順に選択されます。受信されたコールが指定の最大数に達すると、システムは使用可能なチャンネルのハンティングを停止します。このコマンドを使用すると、八重回線電話番号への着信コールの数を制限し、発信コールや各種機能（コール転送や電話会議など）のためにチャンネルを予約することができます。

新機能を使用すると、次の操作を実行できます。

- 二重回線モードのみの設定
- 八重回線モードのみの設定
- 二重回線モードと八重回線モードの設定

## 前提条件

- Cisco Unified SRST 7.0/4.3
- Cisco Unified Communications Manager 6.0
- Cisco IOS リリース 12.4(15)XZ

## 制約事項

- 八重回線電話番号は、Cisco Unified IP Phone 7902、7920、7931 のほか、Cisco ATA または Cisco VG224 に接続されたアナログ電話機ではサポートされていません。
- 電話番号の最大数は、すべての回線の合計数以上になっている必要があります。
- SIP エンドポイントは、H.323 トランクではサポートされません。SIP エンドポイントがサポートされるのは、SIP トランクのみです。

## 要約手順

1. `enable`
2. `configure terminal`
3. `call-manager-fallback`
4. `max-dn max-no-of-directories [dual-line / octo-line] [<num> octo-line]`
5. `huntstop channel 1-8`
6. `end`

## 詳細手順

	コマンドまたはアクション	目的
ステップ 1	<code>enable</code>  例: Router> enable	特権 EXEC モードを有効にします。  • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	<code>configure terminal</code>  例: Router# configure terminal	global コンフィギュレーション モードを開始します。
ステップ 3	<code>call-manager-fallback</code>  例: Router(config)# call-manager-fallback	call-manager-fallback コンフィギュレーション モードを開始します。
ステップ 4	<code>max-dn max-no-of-directories [dual-line   octo-line] [&lt;num&gt; octo-line]</code>  例: Router(config-cm-fallback)# max-dn 15 dual-line 6 octo-line	ルータでサポートできる Directory Number (DN; 電話番号) または仮想音声ポートの最大数を設定し、二重回線モード、八重回線モード、またはその両方のモードをアクティブにします。  • max-directory-numbers : ルータでサポートされる電話番号または仮想音声ポートの最大数。最大数は、プラットフォームによって異なります。デフォルトは 0 です。  • dual-line : (オプション) Cisco Unified Communications Manager フォールバック モードの IP Phone が、2 つのチャネルを持つ仮想音声ポートを使用できるようにします。  • octo-line : (オプション) Cisco Unified Communications Manager フォールバック モードの IP Phone が、8 つのチャネルを持つ仮想音声ポートを使用できるようにします。  • num (オプション): 八重モードの電話番号の数を設定します。範囲は 0 ~ 8 です。デフォルトは 8 です。

	コマンドまたはアクション	目的
ステップ 5	<b>huntstop channel 1-8</b>  <b>例:</b> Router(config-cm-fallback)# huntstop channel 4	八重回線でチャンネル ハントストップを有効にします。これにより、最後の使用可能なチャンネルが通話中または無応答の場合に、コールが電話番号の次のチャンネルをハントしなくなります。 <ul style="list-style-type: none"> <li>• <i>number</i> : 着信コールを受信できるチャンネルの数。残りのチャンネルは、発信コールや各種機能（コール転送、コール ウェイティング、会議など）のために予約されます。範囲は 1 ~ 8 です。デフォルトは 8 です。</li> <li>• このコマンドは、八重回線電話番号だけでサポートされます。</li> </ul>
ステップ 6	<b>end</b>  <b>例:</b> Router(config)# end	特権 EXEC モードに戻ります。

## 例

次の例では、八重回線モードを有効にし、八重回線電話番号の数を 8 に、電話番号の最大数を 23 に、および着信コールを受信できるチャンネルの最大数を 6 に設定します。

```
!
call-manager-fallback
max-dn 23 octo-line 8
huntstop channel 6
!
```

## Cisco Unified SRST に関する Cisco IP Communicator の設定方法

Cisco IP Communicator は、パーソナル コンピュータでのテレフォニー サポートを拡張するソフトウェアベースのアプリケーションです。Cisco IP Communicator は、カラー画面、キーパッド、機能ボタン、およびソフトキーを備えたグラフィカルな表示ベースの IP Phone として、ユーザのコンピュータ画面に表示されます。

動作については、Cisco IP Communicator のオンライン ヘルプとユーザ マニュアルを参照してください。

### 前提条件

この作業を開始する前に、次のものを準備しておく必要があります。

- Cisco Unified SRST TFTP サーバの IP アドレス
- PC 用のマイクロフォン付きヘッドセット（オプションで、PC の内部スピーカおよびマイクロフォンも使用可能）

### 要約手順

1. 最新バージョンの Cisco IP Communicator ソフトウェアをダウンロードし、PC にインストールします。
2. (オプション) ヘッドセットを PC に接続します。
3. Cisco IP Communicator ソフトウェア アプリケーションを起動します。
4. Cisco Unified SRST TFTP サーバの IP アドレスを定義します。
5. Cisco IP Communicator アプリケーションが Cisco Unified SRST システムに接続して登録するまで待ちます。
6. Cisco Unified SRST ルータから Cisco IP Communicator のボタンおよび番号の最終設定を実行します。

### 詳細手順

- 
- ステップ 1** 最新バージョンの Cisco IP Communicator ソフトウェアをダウンロードし、PC にインストールします。
- ステップ 2** (オプション) ヘッドセットを PC に接続します。
- ステップ 3** Cisco IP Communicator ソフトウェア アプリケーションを起動します。
- ステップ 4** Cisco Unified SRST TFTP サーバの IP アドレスを定義します。
- a. Network > User Preferences ウィンドウを開きます。
  - b. Cisco Unified SRST TFTP サーバの IP アドレスを入力します。
- ステップ 5** Cisco IP Communicator アプリケーションが Cisco Unified SRST システムに接続して登録するまで待ちます。
-

## Cisco IP Communicator の確認

- 
- ステップ 1** `show running-config` コマンドを使用して、この電話機に関連付けられた `ephone-dn` および `ephone` の情報を表示します。
- ステップ 2** Cisco IP Communicator が Cisco Unified CME に登録された場合は、設定内に内線電話番号とソフトキーが表示されます。これらの設定が正しいことを確認します。
- ステップ 3** 電話機からローカル コールを発信し、他のユーザにこちらに電話するように依頼します。双方向音声パスが確立されたことを確認します。
- 

## Cisco IP Communicator のトラブルシューティング

`debug ephone detail` コマンドを使用して、コールに関する問題を診断します。詳細については、『[Cisco IOS Debug Command Reference](#)』を参照してください。

## 関連情報

次のステップでは、コール処理を設定します。手順については、[P.73 の「コール処理の設定」](#)を参照してください。

追加情報については、『[Cisco Unified SRST の概要](#)』の章の [P.40 の「その他の資料」](#)を参照してください。



# コール処理の設定

---

Revised: July 11, 2008

この章では、着信コールと発信コールに関する Cisco Unified Survivable Remote Site Telephony( SRST ) の設定方法について説明します。

## 内容

- [コール処理の設定について \( P.73 \)](#)
- [着信コールと発信コールに対するコール処理の設定方法 \( P.74 \)](#)
- [WAN リンク障害に対する H.323 VoIP コール プリザベーションの機能拡張 \( P.109 \)](#)
- [関連情報 \( P.109 \)](#)

## コール処理の設定について

Cisco Unified SRST が提供するコール処理機能は、Cisco Unified Communications Manager よりも種類が少なくなっています。この機能に関する多くの設定では、Cisco Unified Communications Manager または Cisco Unified IP Phone の既存の設定を有効にする必要があります。

## 着信コールと発信コールに対するコール処理の設定方法

コール処理の設定では、次の作業を行う必要があります。

- [着信コールの設定 \(P.74\)](#)
- [発信コールの設定 \(P.92\)](#)

### 着信コールの設定

着信コールの設定では、次の作業を行うことができます。

- コールの自動転送と再ルーティング
  - [ビジー信号の受信時または無応答時の自動転送の設定 \(P.74\)](#)(オプション)
  - [コールの再ルーティングの設定 \(P.76\)](#)(オプション)
  - [コール ピックアップの設定 \(P.79\)](#)(オプション)
  - [転送番号の収集方法の設定 \(P.82\)](#)
- 電話番号の変換
  - [グローバル プレフィックスの設定 \(P.83\)](#)(オプション)
  - [数字変換規則の有効化 \(P.85\)](#)(オプション)
  - [変換プロファイルの有効化 \(P.86\)](#)(オプション)
  - [変換プロファイルの確認 \(P.88\)](#)(オプション)
- ハンティングと呼び出しタイムアウトの動作
  - [ダイヤル ピアとチャネルのハンティングの設定 \(P.89\)](#)(オプション)
  - [ビジー タイムアウトの設定 \(P.90\)](#)(オプション)
  - [呼び出しタイムアウトのデフォルトの設定 \(P.91\)](#)(オプション)

### ビジー信号の受信時または無応答時の自動転送の設定

Cisco Unified Communications Manager のフォールバック中、コールの着信時にビジー信号が受信された場合や応答がない場合に、そのコールを 1 つ以上の E.164 番号に自動転送するように設定できます。

#### 要約手順

1. `call-manager-fallback`
2. `call-forward busy directory-number`
3. `call-forward noan directory-number timeout seconds`
4. `exit`



詳細手順

	コマンドまたはアクション	目的
ステップ 1	<code>call-manager-fallback</code>  例: Router(config)# call-manager-fallback	call-manager-fallback コンフィギュレーション モードを開始します。
ステップ 2	<code>call-forward busy directory-number</code>  例: Router(config-cm-fallback)# call-forward busy 50..	Cisco IP Phone が通話中の場合に別の番号に自動転送するように設定します。  <ul style="list-style-type: none"> <li><code>directory-number</code> : 完全修飾 E.164 番号を表す特定の電話番号。この番号には、内線電話番号の右揃えの数字に対応する「.」ワイルドカード文字を含めることができます。</li> </ul>
ステップ 3	<code>call-forward noan directory-number timeout seconds</code>  例: Router(config-cm-fallback)# call-forward noan 5005 timeout 10	Cisco IP Phone からの応答が受信されない場合に別の番号に自動転送するように設定します。  <ul style="list-style-type: none"> <li><code>directory-number</code> : 完全修飾 E.164 番号またはローカル内線番号を表す特定の電話番号。この番号には、内線電話番号の右揃えの数字に対応する「.」ワイルドカード文字を含めることができます。</li> <li><code>timeout seconds</code> : コールを別の電話機に自動転送するまでの待機時間を秒単位で設定します。<code>seconds</code> の範囲は 3 ~ 60000 です。</li> </ul>
ステップ 4	<code>exit</code>  例: Router(config-cm-fallback)# exit	call-manager-fallback コンフィギュレーション モードを終了します。

例

次の例では、コールの着信時に IP Phone の内線番号からビジー信号が受信された場合や応答がない場合に、コールを内線番号 5005 に自動転送します。コールが着信してから 15 秒間呼び出し音を鳴らし、その後で内線番号 5005 に自動転送します。

```
call-manager-fallback
call-forward busy 5005
call-forward noan 5005 timeout seconds 15
```

次の例では、内線番号が通話中または無応答の場合に、自動転送のために内線番号を変換します。`call-forward busy` コマンドには 50.. という引数を指定しています。これにより、着信内線番号の下 2 桁の前に、数字の 50 が付加されます。最終的な内線番号は、最初の内線番号が通話中または無応答の場合に着信コールを自動転送する宛先番号となります。たとえば、通話中の内線番号 6002 にコールが着信した場合、そのコールは内線番号 5002 に自動転送されます。また、通話中の内線番号 3442 にコールが着信した場合、そのコールは内線番号 5042 に自動転送されます。コールが着信してから 15 秒間呼び出し音が鳴り、その後で自動転送されます。

```
call-manager-fallback
call-forward busy 50..
call-forward noan 50.. timeout seconds 15
```

## コールの再ルーティングの設定



(注)

`alias` コマンドは、`default-destination` コマンドに置き換わるものです。`default-destination` コマンドの代わりに使用することをお勧めします。

`alias` コマンドは、フォールバック時に使用不能になる電話番号にコールを再ルーティングするためのメカニズムを提供します。Cisco Unified Communications Manager のフォールバック時に使用不能になる電話番号へのコールに対して、最大 50 セットの再ルーティング エイリアス規則を作成できます。エイリアス規則のセットを作成するには、`alias` コマンドを使用します。エイリアスは、設定された `alternate-number` エイリアスと一致する電話番号の電話機が登録すると、アクティブになります。この状態になると、着信コールは代替番号に再ルーティングされます。`alternate-number` 引数は、複数の `alias` コマンドで使用できます。その場合は、複数の異なる番号を同一のターゲット番号に再ルーティングできます。

設定された `alternate-number` は、Cisco Unified SRST ルータに登録されている IP Phone に属する特定の E.164 電話番号または内線番号になっている必要があります。`alternate-number` と一致する番号を持つ IP Phone が登録すると、追加の POTS ダイアル ピアが作成されます。宛先パターンは、最初に設定された `number-pattern` に設定されます。また、POTS ダイアル ピアの音声ポートは、`alternate-number` に関連付けられた音声ポートと一致するように設定されます。

最初の `number-pattern` の範囲内にある特定の電話番号を持つ他の IP Phone が登録した場合、コールは `alternate-number` ではなく、IP Phone にルーティングされます（通常のダイアル ピアの最長一致規則、プリファレンス規則、およびハントストップ規則に従います）。

## 自動転送先

`cfw` キーワードを使用すると、通話中または無応答のコールに対する自動転送先を設定できます。無応答時の自動転送とは、ユーザ設定可能な期間にわたって電話機で呼び出し音が鳴り、コールへの応答がない場合に、コールが設定済みの宛先に自動転送されることを指します。話中時の自動転送と無応答時の自動転送を特定のストリングに設定し、グローバルに設定された自動転送設定を上書きすることができます。



(注)

グローバルな設定は、`call-manager-fallback` の下で選択された設定であり、SRST サービスに登録するすべての電話機に適用されます。

また、特定の番号に固有の自動転送パスを作成することもできます。`cfw` キーワードを使用すると、SRST の動作中に、本来であれば到達不能となる番号から使用可能な電話機に対して、コールを再ルーティングできます。自動転送規則に基づいて基本的なハント グループを作成すると、最初の SRST 電話機が通話中の場合に、コールを 2 つ目の SRST 電話機に自動転送できるようになります。

また、`cfw` キーワードを使用して、電話番号のエイリアスをその番号自体に割り当てることもできます。次に、番号のエイリアスをその番号自体に割り当てる例を示します。内線番号 1001 の電話機が登録すると、電話機にコールをルーティングするダイアル ピアが 1001 に対して自動的に作成されます。この最初のダイアル ピアに対する `call-manager-fallback` ダイアル ピア プリファレンス (`max-dn` コマンドで設定される) が 2 に設定されている場合、ダイアル ピアはそのプリファレンス設定として 2 を使用します。

次に、`alias` コマンドを使用して、電話番号のエイリアスをその番号自体に割り当てます。

```
alias 1 1001 to 1001 preference 1 cfw 2001 timeout 20
```

この例では、1001 に対して、1001 にコールをルーティングする 2 つ目のダイヤル ピアを作成しました。ただし、プリファレンスは 1 で、自動転送先は 2001 になっています。この場合、**alias** コマンドで作成されたダイヤル ピアのプリファレンスは、ダイヤル ピアが最初に作成したプリファレンスよりも値が小さくなっているため、すべてのコールは最初に、**alias** コマンドで作成されたダイヤル ピアに送られます。したがって、コールは、グローバルに設定された自動転送の代わりに、**alias** コマンドで設定された自動転送に従うようになります。

### 個別のエイリアスでのハントストップ

エイリアスの **huntstop** キーワードが意味を持つのは、**call-manager-fallback** の下でグローバルな **no huntstop** コマンドも設定している場合のみです。また、複数の **alias** コマンドに同一の *number-pattern* を指定し、エイリアス間で話中時のハンティングを有効にする場合は、グローバルな **no huntstop** の設定が必要になることがあります。つまり、*number-pattern* のどちらかのエイリアスが試行され、その電話機が通話中であった場合は、*number-pattern* の 2 つ目のエイリアスが試行されます。

エイリアスの **huntstop** キーワードを使用すると、**no huntstop** コマンドでハントストップをグローバルにオフにした場合に、個別のエイリアスに対してハントストップ動作をオンに戻すことができます。個別のエイリアスに対して **huntstop** キーワードを設定すると、そのエイリアスでハンティングが停止し、そのエイリアスがハントシーケンスの最後のメンバになります。

### 要約手順

1. **call-manager-fallback**
2. **alias tag number-pattern to alternate-number** [*preference preference-value*] [*cfw number timeout timeout-value*] [**huntstop**]
3. **max-dn max-directory-numbers** [*dual-line*] [*preference preference-order*]
4. **end**
5. **show dial-peer voice summary**

詳細手順

	コマンドまたはアクション	目的
ステップ 1	<p><b>call-manager-fallback</b></p> <p>例： Router(config)# call-manager-fallback</p>	<p>call-manager-fallback コンフィギュレーション モードを開始します。</p>
ステップ 2	<p><b>alias tag number-pattern to alternate-number [preference preference-value] [cfw number timeout timeout-value] [huntstop]</b></p> <p>例： Router(config-cm-fallback)# alias 1 60.. to 5001 preference 1 cfw 2000 timeout 10</p>	<p>Cisco Unified Communications Manager のフォールバック時に使用不能になる電話機のセットにコールを再ルーティングするための一連の規則を作成します。</p> <ul style="list-style-type: none"> <li>• <i>tag</i> : エイリアス規則の範囲の識別子。範囲は 1 ~ 50 です。</li> <li>• <i>number-pattern</i> : 着信電話番号と照合するパターン。このパターンにはワイルドカードを含めることができます。</li> <li>• <i>to</i> : tag 番号のパターンを代替番号に接続します。</li> <li>• <i>alternate-number</i> : 番号パターンと一致する着信コールをルーティングする代替電話番号。代替番号は、Cisco Unified SRST ルータに登録されているアクティブな IP Phone に属する特定の内線番号にする必要があります。代替電話番号は、複数の <i>alias</i> コマンドで使用できます。</li> <li>• <i>preference preference-value</i> ( オプション )。エイリアスにダイヤル ピア プリファレンス値を割り当てます。関連付けられたダイヤル ピアのプリファレンス値の範囲は 0 ~ 10 です。<i>max-dn</i> コマンドとともに使用します。</li> <li>• <i>cfw number</i> ( オプション )。 <i>cfw</i> キーワードを使用すると、ユーザは、話中時の自動転送と無応答時の自動転送を特定のストリングに設定し、グローバルに設定された自動転送設定を上書きすることができます。</li> <li>• <i>timeout timeout-value</i> ( オプション )。自動転送に関する無応答時の呼び出しタイムアウト期間を秒単位で設定します。範囲は 3 ~ 60000 です。</li> <li>• <i>huntstop</i> ( オプション )。代替番号の試行後にコールハンティングを停止します。</li> </ul>
ステップ 3	<p><b>max-dn max-directory-numbers [dual-line] [preference preference-order]</b></p> <p>例： Router(config-cm-fallback)# max-dn 10 preference 2</p>	<p>ルータでサポートできる電話番号または仮想音声ポートの最大数を設定し、プライマリ番号に関連付けられたすべての電話番号の VoIP ダイヤル ピアを作成する場合のグローバルプリファレンスを設定します。</p> <ul style="list-style-type: none"> <li>• <i>max-dn</i> コマンドを使用すると、<i>alias</i> コマンドで作成されたデフォルトのダイヤル ピアのプリファレンスが設定されます。</li> <li>• コールの再ルーティングを設定する場合は、<i>max-dn preference</i> を、<i>alias</i> コマンドで設定されたプリファレンスよりも大きなプリファレンス値に設定します。</li> </ul>

	コマンドまたはアクション	目的
ステップ 4	<b>end</b>  <b>例:</b> Router(config-cm-fallback)# end	特権 EXEC モードに戻ります。
ステップ 5	<b>show dial-peer voice summary</b>  <b>例:</b> Router# show dial-peer voice summary	音声ダイヤル ピアの情報を表示します。  • ダイヤル ピアに問題がある場合は、このコマンドを使用し、 <b>alias</b> コマンドで作成されたダイヤル ピアを表示します。

例

次の例では、**alias** コマンドの **preference** キーワードを、**max-dn** コマンドで作成されたプリファレンス値よりも小さな値に設定します。小さな値に設定すると、**cfw** キーワードを有効にできます。内線番号 1000 への着信コールは、プリファレンス値が小さいため、エイリアスをハントします。また、無応答または通話中の 1000 へのコールは 2000 に自動転送されます。その他の SRST モードの内線番号に対する着信コールはすべて、10 秒後に 3000 に自動転送されます。

```
call-manager-fallback
alias 1 1000 to 1000 preference 1 cfw 2000 timeout 10
max-dn 10 preference 2
call-forward busy 3000
call-forward noan 3000 timeout 10
```

コール ピックアップの設定

**pickup** コマンドを設定すると、すべての SRST 電話機で PickUp ソフトキーが有効になります。その状態で PickUp キーを押すと、設定された *telephone-number* と一致する DID 着信番号を持つ呼び出し中の IP Phone へのコールに応答することができます。このコマンドでは、Group PickUp (GPickUp) ソフトキーは有効になりません。

ユーザが PickUp ソフトキーを押すと、SRST はすべての SRST 電話機を検索し、設定された *telephone-number* と一致する着信番号を持つ呼び出し中のコールを見つけます。一致するものが見つかったら、そのコールは、コール ピックアップを要求した電話機の内線番号に自動転送されます。

SRST の **pickup** コマンドは、Cisco Unified Communications Manager と互換性のある方法で動作するように設計されています。



**(注)** Cisco 7905 および Cisco 7912 IP Phone の場合、Cisco Unified Communications Manager Release 4.0(1) のデフォルトの電話機ロードでは、フォールバック時に PickUp ソフトキーは有効になりません。Cisco 7905 および Cisco 7912 IP Phone で PickUp ソフトキーを有効にするには、デフォルトの電話機ロードを Cisco Unified Communications Manager バージョン 4.0(1) Sr2 にアップグレードしてください。別の方法として、電話機ロードをそれぞれ [cmterm-7905g-sccp.3-3-8.exe](#) または [cmterm-7912g-sccp.3-3-8.exe](#) にアップグレードしてもかまいません。

要約手順

1. **call-manager-fallback**
2. **no huntstop**
3. **alias tag number-pattern to alternate-number**
4. **pickup telephone-number**
5. **end**

■ 着信コールと発信コールに対するコール処理の設定方法

詳細手順

	コマンドまたはアクション	目的
ステップ 1	<code>call-manager-fallback</code>  例: Router(config)# call-manager-fallback	call-manager-fallback コンフィギュレーション モードを開始します。
ステップ 2	<code>no huntstop</code>  例: Router(config-cm-fallback)# no huntstop	ハントストップを無効にします。
ステップ 3	<code>alias tag number-pattern to alternate-number</code>  例: Router(config-cm-fallback)# alias 1 8005550100 to 5001	Cisco Unified Communications Manager のフォールバック時に使用不能になる電話機のセットにコールを再ルーティングするための一連の規則を作成します。  <ul style="list-style-type: none"> <li>• <i>tag</i> : エイリアス規則の範囲の識別子。範囲は 1 ~ 50 です。</li> <li>• <i>number-pattern</i> : 着信電話番号と照合するパターン。このパターンにはワイルドカードを含めることができます。</li> <li>• <i>to</i>:tag 番号のパターンを代替番号に接続します。</li> <li>• <i>alternate-number</i> : 番号パターンと一致する着信コールをルーティングする代替電話番号。代替番号は、Cisco Unified SRST ルータに登録されているアクティブな IP Phone に属する特定の内線番号にする必要があります。代替電話番号は、複数の <i>alias</i> コマンドで使用できます。</li> </ul>
ステップ 4	<code>pickup telephone-number</code>  例: Router(config-cm-fallback)# pickup 8005550100	すべての Cisco Unified IP Phone で PickUp ソフトキーを有効にします。このソフトキーを使用すると、SRST の動作中に、特定の内線番号に着信した外部のダイヤルイン (DID) コールを別の内線番号からピックアップできます。 <i>telephone-number</i> 引数は、着信番号と照合する電話番号です。
ステップ 5	<code>end</code>  例: Router(config-cm-fallback)# end	特権 EXEC モードに戻ります。

例

`pickup` コマンドは `alias` コマンドとともに使用するのが最適です。次に示す `show running-config` コマンドの部分的な出力は、ハントグループのパイロット番号にコールルーティングを適用するように設定された `pickup` コマンドと `alias` コマンドを示しています。

```
call-manager-fallback
no huntstop
alias 1 8005550100 to 5001
alias 2 8005550100 to 5002
alias 3 8005550100 to 5003
alias 4 8005550100 to 5004
pickup 8005550100
```

800 555-0100 への DID 着信コールが受信された場合、`alias` コマンドは、そのコールを 4 つの内線番号 (5001 ~ 5004) のいずれかにランダムにルーティングします。`pickup` コマンドが設定されているため、内線番号 5002 で DID コールの呼び出し音が鳴った場合、他の内線番号 (5001、5003、5004) のいずれかで PickUp ソフトキーを押すと、そのコールに応答できます。

`pickup` コマンドが動作すると、着信した DID 着信番号に基づいて一致する番号が検索されます。この例では、内線番号 5004 から内線番号 5001 へのコール (内線コール) では `pickup` コマンドはアクティブになりません。これは、着信番号 (5001) が設定済みのピックアップ番号 (800 555-0100) と一致しないためです。このように、`pickup` コマンドは、複数のコールによって呼び出し音が同時に鳴っている場合に、内線コールと外線コールを区別します。

## 打診転送の設定

Cisco Unified SRST 4.3 以前の打診転送機能では、ダイヤル トーンが再生され、ダイヤルされた番号が収集されます。この番号収集は、その番号が打診転送、ブラインド転送、または PSTN 転送ブロッキング用のパターンと一致するまで続けられます。営業時間外ブロッキング基準は、打診転送の番号収集およびパターン マッチングの終了後に適用されます。

新機能では、転送番号収集プロセスが変更され、Cisco Unified Communications Manager との整合がとられています。この機能がサポートされるのは、`call-manager-fallback` コンフィギュレーションモードで `transfer-system full-consult` コマンド (デフォルト) が指定され、アイドル回線またはチャネルの確保、番号収集、およびダイヤルが可能になっている場合のみです。

打診転送には、2 つの回線が必要です。転送する側が八重回線電話番号である場合、Cisco Unified SRST は、その電話番号で次に使用可能なアイドル チャネルを選択します。その電話番号で最大数のチャネルが使用中の場合は、転送する側の電話機で別のアイドル回線が選択されます。電話機で `auto-line` コマンドが設定されている場合、指定された自動回線がアイドル状態であれば、その回線が他の非自動回線よりも優先されます。転送する側の電話機に使用可能なアイドル回線がない場合は、打診転送ではなく、ブラインド転送が開始されます。

打診転送の処理中、転送する側の電話機において転送される側との回線がロックされるため、同じ電話番号を共有する他の電話機によってその回線が取得されることが防止されます。ユーザが打診転送のために Transfer ソフトキーを押した場合、この確保された打診転送コール レッグで番号のダイヤルおよび収集が終了するまで、Transfer ソフトキーは表示されなくなります。打診転送のパターン マッチング、ブラインド転送、PSTN 転送ブロッキング、または時間外ブロッキング基準の方法は従来と同じですが、マッチング後の操作は異なります。ブラインド転送の基準が満たされた場合、Cisco Unified SRST は、打診転送コール レッグを終了し、コールを転送するように Cisco IOS ソフトウェアに通知し、元のコール バブルを終了します。PARK FAC コードの処理は、新しいコールの場合と同様に行われ、Cisco IOS ソフトウェアによる 10 秒間タイマーの適用が必要となります。



(注)

新しい機能拡張では、デフォルトで、新しいコール レッグから転送番号が収集されます。必要に応じて、元のコール レッグから転送番号を収集するようにシステムを設定することもできます。[P.82 の「転送番号の収集方法の設定」](#)を参照してください。

転送ブロッキングまたは桁間タイマーの期限切れによって転送が失敗した場合のエラー処理は残されています。このエラー処理では、プロンプト行にエラー メッセージが表示され、「`debug ephone error`」が有効になっている場合にはエラー メッセージがログに記録され、小刻みなビジー トーンまたは通常のビジー トーンが再生された後、打診転送コール レッグが終了します。

これらの機能拡張をサポートするための新しい設定は必要ありません。コール転送機能を設定する場合は、『[Cisco IOS Survivable Remote Site Telephony Version 3.2 System Administrator Guide](#)』を参照してください。

## 電話会議

この電話会議の機能拡張に関する設定作業は必要ありません。

### 単一回線電話番号

電話会議の開始側が単一回線電話番号で、電話機に複数の電話番号が設定されている場合、システムは、別の電話番号のアイドルチャンネルを選択して会議を作成します。電話機に複数の電話番号（二重回線または単一回線電話番号）が設定されており、各番号でコールが保留になっている場合、システムはユーザに対し、電話会議用の回線を選択するように要求します。

### 二重回線電話番号

電話会議の開始側が二重回線電話番号である場合、システムは、二重回線電話番号の別のアイドルチャンネルを選択します。選択したチャンネルでコールが保留になっている場合は、会議操作により自動的に、保留中のチャンネルが選択され、会議が作成されます。

### 八重回線電話番号

電話会議の開始側が八重回線電話番号である場合、システムは、開始側の電話番号のアイドルチャンネルを選択します。その後、ユーザが新しいコールを確立して会議を作成する必要があります。同じ電話番号にアイドルチャンネルがない場合、同じ電話機で他のアイドル電話番号またはチャンネルが選択されることはありません。同じ電話番号の他のチャンネル、または他の電話番号で既存のコールが保留になっている場合、ユーザは、そのコールを選択して会議に参加させることはできません。同じ電話番号にアイドルチャンネルがない場合、会議は中止され、No Line Available メッセージが表示されます。

## 転送番号の収集方法の設定

デフォルトでは、転送番号は新しいコール レッグから収集されます。転送番号の収集方法を変更するには、次の手順を実行します。

### Cisco Unified SRST 4.3 の前提条件

- Cisco Unified SRST 4.3
- Cisco Unified Communications Manager 6.0
- Cisco IOS リリース 12.4(15)XZ

### Cisco Unified SRST 4.3 の制約事項

- Cisco 3200 シリーズ Mobile Access Router では、SRST はサポートされていません。

## 要約手順

1. `enable`
2. `configure terminal`
3. `call-manager-fallback`
4. `transfer-digit-collect {new-call | orig-call}`
5. `end`



詳細手順

	コマンドまたはアクション	目的
ステップ 1	<code>enable</code>  例: Router> enable	特権 EXEC モードを有効にします。  • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	<code>configure terminal</code>  例: Router# configure terminal	global コンフィギュレーション モードを開始します。
ステップ 3	<code>call-manager-fallback</code>  例: Router(config)# call-manager-fallback	call-manager-fallback コンフィギュレーション モードを開始します。
ステップ 4	<code>transfer-digit-collect {new-call   orig-call}</code>  例: Router(config-cm-fallback)# transfer-digit-collect orig-call	打診コール転送に使用する番号収集方法を選択します。  • <i>new-call</i> : 番号は新しいコール レッグから収集されます。これはデフォルト値です。 • <i>orig-call</i> : 番号は元のコール レッグから収集されます。これは、Cisco Unified SRST 4.3 以前のバージョンでのデフォルト動作です。
ステップ 5	<code>end</code>  例: Router(config)# end	特権 EXEC モードに戻ります。

例

次の例は、orig-call という従来の値に設定された transfer-digit-collect 方法を示しています。

```
!
call-manager-fallback
  transfer-digit collect orig-call
!
```

グローバル プレフィックスの設定

**dialplan-pattern** コマンドは、省略された内線番号を完全修飾 E.164 番号に拡張するためのグローバル プレフィックスを指定するダイヤル プラン パターンを作成します。

**extension-pattern** キーワードを使用すると、省略された内線番号のプレフィックス番号を追加操作できます。このキーワードとその引数を使用すると、内線番号パターンの先頭番号が除去され、対応するダイヤル プラン パターンの先頭番号に置き換えられます。このコマンドを使用すると、たとえば 0101 という 4 桁の内線番号になる 408-555-0101 のようなダイヤルイン (DID) 番号を回避できます。


グローバル プレフィックスを設定するには、**dialplan-pattern** コマンドを使用します。最大 5 つのダイヤル プラン パターンを作成できます。**no-reg** キーワードは、柔軟性のあるダイヤリングを可能にし、ダイヤル ピアの E.164 番号がゲートキーパーに登録することを防止します。ゲートキーパーに番号を登録しないようにするオプションを使用すると、その番号を他のテレフォニー サービスで使用できるようになります。

■ 着信コールと発信コールに対するコール処理の設定方法

要約手順

1. `call-manager-fallback`
2. `dialplan-pattern tag pattern extension-length length [extension-pattern extension-pattern] [no-reg]`
3. `exit`

詳細手順

	コマンドまたはアクション	目的
ステップ 1	<p><code>call-manager-fallback</code></p> <p>例: Router(config)# <code>call-manager-fallback</code></p>	<p><code>call-manager-fallback</code> コンフィギュレーション モードを開始します。</p>
ステップ 2	<p><code>dialplan-pattern tag pattern extension-length length [extension-pattern extension-pattern] [no-reg]</code></p> <p>例: Router(config-cm-fallback)# <code>dialplan-pattern 1 4085550100 extension-length 3 extension-pattern 4..</code></p> <p> (注) この例では、4xx という内線番号すべてを 40855501xx という PSTN 番号にマップします。したがって、内線番号 412 は 4085550112 に対応します。</p>	<p>省略された内線番号を完全修飾 E.164 番号に拡張するために使用できるグローバル プレフィックスを作成します。</p> <ul style="list-style-type: none"> <li>• <code>tag</code>: 10 桁の電話番号の前に使用されるダイヤルプラン スtringのタグ。タグ番号の範囲は 1 ~ 5 です。</li> <li>• <code>pattern</code>: ダイヤルプラン パターン。たとえば、エリアコード、プレフィックス、および内線番号の最初の 1 桁または 2 桁に、内線番号の残りの桁に対応するワイルドカード記号またはドット(.)を付加したものになります。</li> <li>• <code>extension-length</code>: 内線番号の桁数を設定します。</li> <li>• <code>length</code>: 内線番号の桁数。範囲は 1 ~ 32 です。</li> <li>• <code>extension-pattern</code>: (オプション) 内線番号の先頭番号が、<code>pattern</code> 引数で定義された E.164 電話番号の先頭番号と異なる場合に、内線番号の先頭番号のパターンを設定します。</li> <li>• <code>extension-pattern</code>: (オプション) 内線番号の先頭番号のパターン。1 桁以上の数字およびワイルドカード記号またはドット(.)で構成されます。たとえば、5.. の場合は内線番号 500 ~ 599 が含まれ、5... の場合は 5000 ~ 5999 が含まれます。</li> <li>• <code>no-reg</code>: (オプション) ダイヤルピアの E.164 番号がゲートキーパーに登録することを防止します。</li> </ul>
ステップ 3	<p><code>exit</code></p> <p>例: Router(config-cm-fallback)# <code>exit</code></p>	<p><code>call-manager-fallback</code> コンフィギュレーション モードを終了します。</p>

例

次の例は、4085550 で始まる電話プレフィックスを持つ内線番号 101 ~ 199 に対するダイヤルプランパターン 1 を作成する方法を示しています。次の例が設定されている場合、ルータは、4085550144 がダイヤルプランパターン 1 と一致することを認識します。次に、`extension-length` キーワードを使用して、番号 144 の下 3 桁を抽出し、着信コールの発信者 ID として表示します。

```
call-manager-fallback
dialplan-pattern 1 40855501.. extension-length 3 no-reg
```

次の例では、3桁の内線番号の先頭プレフィックス番号を0から4へ変換します。その結果、内線番号の範囲は400～499になります。

```
call-manager-fallback
dialplan-pattern 1 40855500.. extension-length 3 extension-pattern 4..
```

次の例では、**dialplan-pattern** コマンドは、4085559で始まる電話プレフィックスを持つ内線番号801～899に対応するダイヤルプランパターン2を作成します。内線番号パターンの各番号がnumberコマンドで宣言されると、2つのPOTSダイヤルピアが作成されます。例では、それらのダイヤルピアは、801（オフィスの内線番号）および4085559001（外線番号）です。

```
call-manager-fallback
dialplan-pattern 2 40855590.. extension-length 3 extension-pattern 8..
```

## 数字変換規則の有効化

Cisco Unified Communications Manager のフォールバック時は、数字変換規則を有効にすることができます。変換規則は、番号操作メカニズムであり、ダイヤルされた番号に電話エリアコードとプレフィックスコードを自動的に追加するといった操作を実行します。



(注)

数字変換規則には、多くの用途やバリエーションがあります。詳細については、『[Cisco IOS Voice Configuration Library](#)』を参照してください。

Cisco SRST 3.2以降またはCisco Unified SRST 4.0以降を実行している場合は、下記の**translate**コマンドではなく、[P.86の「変換プロファイルの有効化」](#)に記載されている設定を使用してください。変換プロファイルはCisco SRST 3.2で導入されたもので、追加の機能を提供します。

変換規則を使用すると、次の操作が可能になります。

- 音声コールの Answer Number Indication (ANI) (発信番号) または Dialed Number Identification Service (DNIS; 着信番号識別サービス) (着信番号) 番号を操作する。
- コールが着信ダイヤルピアと照合される前、またはコールが発信ダイヤルピアによって自動転送される前に、電話番号を別の番号に変換する。

システムに設定されている変換規則を表示するには、**show translation-rule** コマンドを使用します。

## 要約手順

1. **call-manager-fallback**
2. **translate {called | calling} translation-rule-tag**
3. **exit**

■ 着信コールと発信コールに対するコール処理の設定方法

詳細手順

	コマンドまたはアクション	目的
ステップ 1	<code>call-manager-fallback</code>  例: Router(config)# <code>call-manager-fallback</code>	<code>call-manager-fallback</code> コンフィギュレーションモードを開始します。
ステップ 2	<code>translate {called   calling}</code> <code>translation-rule-tag</code>  例: Router(config-cm-fallback)# <code>translate called 20</code>	Cisco Unified Communications Manager のフォールバックがアクティブのときに Cisco Unified IP Phone ユーザがダイヤルまたは受信する電話番号を変更するための変換規則を適用します。  <ul style="list-style-type: none"> <li>• <code>called</code> : 変換規則を発信コールの番号に適用します。</li> <li>• <code>calling</code> : 変換規則を着信コールの番号に適用します。</li> <li>• <code>translation-rule-tag</code> : 変換規則の参照番号 (1 ~ 2147483647)</li> </ul>
ステップ 3	<code>exit</code>  例: Router(config-cm-fallback)# <code>exit</code>	<code>call-manager-fallback</code> コンフィギュレーションモードを終了します。

例

次の例では、内線番号 1111 に着信するコールに変換規則 10 を適用します。Cisco Unified Communications Manager のフォールバック時、1111 への着信コールはすべて 2222 に送られます。

```
translation-rule 10
  rule 1 1111 2222 abbreviated
  exit
call-manager-fallback
  translate calling 10
```

次の例は、数字変換規則 20 の設定を示しています。この設定では、変換規則の優先順位は 1 (範囲は 1 ~ 15) で、完全な番号の省略表現 (1234) が番号 2345 に置き換えられます。

```
translation-rule 20
  rule 1 1234 2345 abbreviated
  exit
```

変換プロファイルの有効化

Cisco SRST 3.2 以降と Cisco Unified SRST 4.0 以降では、変換プロファイルがサポートされています。変換プロファイルでは、変換規則をグループ化し、変換規則を次の要素に適用する方法を指示することができるため、使用をお勧めします。

- 着信番号
- 発信番号
- リダイレクトされる着信番号

下記の設定では、`voice translation-rule` コマンドと `rule` コマンドを使用して、番号の操作方法を設定および定義します。`voice translation-profile` モードの `translate` コマンドは、操作する番号のタイプ (着信、発信、またはリダイレクトされる番号など) を定義します。変換プロファイルを定義したら、ダイヤル ピアや音声ポートなど、さまざまな場所に変換プロファイルを適用できます。SRST に対するプロファイルは、`call-manager fallback` モードで適用します。

Cisco IP Phone は、SRST モードのときに、1 つの着信変換プロファイルと 1 つの発信変換プロファイルをサポートします。



(注) Cisco SRST 3.2 以降と Cisco Unified SRST 4.0 以降では、P.85 の「数字変換規則の有効化」に記載されている変換規則の設定ではなく、下記の `voice translation-rule` コマンドと `translation-profile` コマンドが使用されます。音声変換規則は、変換規則とは別の機能です。詳細については、『Cisco IOS Voice Command Reference』に記載されている `voice translation-rule` コマンドを参照してください。また、変換規則とプロファイルに関するその他の一般事項については、『VoIP Gateway Trunk and Carrier Based Routing Enhancements』を参照してください。

### 要約手順

1. `voice translation-rule number`
2. `rule precedence/match-pattern/ /replace-pattern/`
3. `exit`
4. `voice translation-profile name`
5. `translate {called | calling | redirect-called} voice-translation-rule-tag`
6. `exit`
7. `call-manager-fallback`
8. `translation-profile {incoming | outgoing} name`
9. `exit`

### 詳細手順

	コマンドまたはアクション	目的
ステップ 1	<code>voice translation-rule number</code>  例: Router(config)# voice translation-rule 1	音声コールの変換規則を定義し、voice translation-rule コンフィギュレーション モードを開始します。 <ul style="list-style-type: none"> <li>• <code>number</code> : 変換規則を識別する番号。範囲は 1 ~ 2147483647 です。</li> </ul>
ステップ 2	<code>rule precedence/match-pattern/ /replace-pattern/</code>  例: Router(cfg-translation-rule)# rule 1/^9/ //	変換規則を定義します。 <ul style="list-style-type: none"> <li>• <code>precedence</code> : 変換規則の優先順位。範囲は 1 ~ 15 です。</li> <li>• <code>match-pattern</code> : 着信コール情報の照合に使用される Stream Editor (SED) 式。スラッシュ (/) は、パターンのデリミタです。</li> <li>• <code>replace-pattern</code> : コール情報の照合パターンを置換するとき使用される SED 式。スラッシュ (/) は、パターンのデリミタです。</li> </ul>
ステップ 3	<code>exit</code>  例: Router(cfg-translation-rule)# exit	voice translation-rule コンフィギュレーション モードを終了します。
ステップ 4	<code>voice translation-profile name</code>  例: Router(config)# voice translation-profile name1	音声コールの変換プロファイルを定義します。 <ul style="list-style-type: none"> <li>• <code>name</code> : 変換プロファイルの名前。音声変換プロファイルの名前の最大長は、英数字で 31 文字です。</li> </ul>

■ 着信コールと発信コールに対するコール処理の設定方法

	コマンドまたはアクション	目的
ステップ 5	<pre>translate {called   calling   redirect-called} translation-rule-number</pre> <p>例: Router(cfg-translation-profile)# translate called 1</p>	<p>音声変換規則を音声変換プロファイルに関連付けます。</p> <ul style="list-style-type: none"> <li>• <i>called</i> : 変換規則を着信番号に関連付けます。</li> <li>• <i>calling</i> : 変換規則を発信番号に関連付けます。</li> <li>• <i>redirect-called</i> : 変換規則をリダイレクトされる着信番号に関連付けます。</li> <li>• <i>translation-rule-number</i> : 変換規則の参照番号 (1 ~ 2147483647)。</li> </ul>
ステップ 6	<pre>exit</pre> <p>例: Router(cfg-translation-profile)# exit</p>	<p>translation-profile コンフィギュレーション モードを終了します。</p>
ステップ 7	<pre>call-manager-fallback</pre> <p>例: Router(config)# call-manager-fallback</p>	<p>call-manager-fallback コンフィギュレーション モードを開始します。</p>
ステップ 8	<pre>translation-profile {incoming   outgoing} name</pre> <p>例: Router(config-cm-fallback)# translation-profile outgoing name1</p>	<p>Cisco IP Phone の着信または発信コール レッグに変換プロファイルを割り当てます。</p> <ul style="list-style-type: none"> <li>• <i>incoming</i> : 変換プロファイルを着信コールに適用します。</li> <li>• <i>outgoing</i> : 変換プロファイルを発信コールに適用します。</li> <li>• <i>name</i> : 変換プロファイルの名前。</li> </ul>
ステップ 9	<pre>exit</pre> <p>例: Router(config-cm-fallback)# exit</p>	<p>call-manager-fallback コンフィギュレーション モードを終了します。</p>

例

次の例は、2つの音声変換規則を使用して name1 という変換プロファイルを作成する設定を示しています。rule1 は関連付けられた発信番号で構成され、rule2 はリダイレクトされる着信番号で構成されます。SRST モードの Cisco Unified IP Phone には name1 が設定されます。

```
voice translation-profile name1
  translate calling 1
  translate called redirect-called 2

call-manager-fallback
  translation-profile incoming name1
```

変換プロファイルの確認

変換プロファイルを確認するには、次の手順を実行します。

要約手順

1. show voice translation-rule number
2. test voice translation-rule number input-test-string [type match-type [plan match-type]]

## 詳細手順

### ステップ 1 `show voice translation-rule number`

このコマンドを使用して、変換プロファイル用に定義した変換規則を確認します。

```
Router# show voice translation-rule 6

Translation-rule tag: 6
  Rule 1:
  Match pattern: 65088801..
  Replace pattern: 6508880101
  Match type: none   Replace type: none
  Match plan: none   Replace plan: none
```

### ステップ 2 `test voice translation-rule number input-test-string [type match-type [plan match-type]]`

このコマンドを使用して、変換プロファイルをテストします。詳細については、『[Cisco IOS Voice Command Reference](#)』に記載されている `test voice translation-rule` コマンドを参照してください。

```
Router(config)# voice translation-rule 5
Router(cfg-translation-rule)# rule 1 /201/ /102/
Router(cfg-translation-rule)# end
Router# test voice translation-rule 5 2015550101
Matched with rule 5
Original number:2015550101   Translated number:1025550101
Original number type: none   Translated number type: none
Original number plan: none   Translated number plan: none
```

## ダイヤル ピアとチャンネルのハンティングの設定

ダイヤル ピア ハンティングは、使用可能な電話回線に対するダイヤル ピアのグループの検索機能であり、デフォルトでは、Cisco Unified Communications Manager のフォールバック時には無効になります。ダイヤル ピア ハンティングを有効にするには、`no huntstop` コマンドを使用します。ダイヤル ピア ハンティングの詳細については、『[Cisco IOS Voice Configuration Library](#)』を参照してください。

二重回線電話機を設定した場合（P.66 の「[二重回線電話機の設定](#)」を参照）、最初のチャンネルが通話中または無応答のときに、着信コールが 2 つ目のチャンネルをハントしないようにするには、`huntstop` コマンドで `channel` キーワードを使用します。

また、チャンネル ハントストップを使用することで、コールが最初の回線チャンネルで 30 秒間呼び出し音を鳴らし、応答がない場合は 2 つ目のチャンネルで再度 30 秒間呼び出し音を鳴らし、さらに別の回線に転送されるという状況に陥ることが防止されます。

## 要約手順

1. `call-manager-fallback`
2. `huntstop [channel]`
3. `exit`

■ 着信コールと発信コールに対するコール処理の設定方法

詳細手順

	コマンドまたはアクション	目的
ステップ 1	<code>call-manager-fallback</code>  例: <code>Router(config)# call-manager-fallback</code>	call-manager-fallback コンフィギュレーション モードを開始します。
ステップ 2	<code>huntstop [channel]</code>  例: <code>Router(config-cm-fallback)# huntstop channel</code>	Communications Manager フォールバック時に作成される Cisco Unified IP Phone ダイアル ピアに関連付けられたダイアル ピア用のハントストップ アトリビュートを設定します。  • 二重回線設定の場合、 <i>channel</i> キーワードを使用すると、最初のチャンネルが通話中または無応答のときに、着信コールが 2 つ目のチャンネルをハントしないようになります。
ステップ 3	<code>exit</code>  例: <code>Router(config-cm-fallback)# exit</code>	call-manager-fallback コンフィギュレーション モードを終了します。

例

次の例では、Cisco Unified Communications Manager のフォールバック時のダイアル ピア ハンティングと、二重回線電話機の設定におけるセカンダリ チャンネルのハンティングを無効にします。

```
call-manager-fallback
no huntstop channel
```

ビジー タイムアウトの設定


この作業では、通話中の宛先に対するコール転送のタイムアウト値を設定します。ビジー タイムアウト値とは、コールの転送時にビジー信号が受信されてから、コールが接続解除されるまでの許容時間です。

要約手順

1. `call-manager-fallback`
2. `timeouts busy seconds`
3. `exit`



詳細手順

	コマンドまたはアクション	目的
ステップ 1	<code>call-manager-fallback</code>  例: Router(config)# <code>call-manager-fallback</code>	call-manager-fallback コンフィギュレーション モードを開始します。
ステップ 2	<code>timeouts busy seconds</code>  例: Router(config-cm-fallback)# <code>timeouts busy 20</code>	コールが通話中の宛先に転送されてから切断されるまでの時間を設定します。  • <code>seconds</code> : 秒数。範囲は 0 ~ 30 です。デフォルトは 10 です。   (注) このコマンドは、通話中の宛先に転送されたコールのビジー タイムアウトだけを設定するもので、通話中の宛先に直接ダイヤルするコールのタイムアウトには影響しません。
ステップ 3	<code>exit</code>  例: Router(config-cm-fallback)# <code>exit</code>	call-manager-fallback コンフィギュレーション モードを終了します。

例

次の例では、通話中の宛先に転送されたコールのタイムアウトを 20 秒に設定します。

```
call-manager-fallback
timeouts busy 20
```

呼び出しタイムアウトのデフォルトの設定

呼び出しタイムアウトのデフォルトとは、電話機で呼び出し音が鳴ってから、応答がないために発信者に切断コードを返すまでの時間です。このタイムアウトにより、自動転送と接続解除を監視しない Foreign Exchange Office (FXO) などのインターフェイスを介して受信されたコールが呼び出し中のままになることが防止されます。このタイムアウトは、無応答時の自動転送が有効になっていない内線番号にのみ使用されます。

要約手順

1. `call-manager-fallback`
2. `timeouts ringing seconds`
3. `exit`

■ 着信コールと発信コールに対するコール処理の設定方法

詳細手順

	コマンドまたはアクション	目的
ステップ 1	<code>call-manager-fallback</code>  例: Router(config)# <code>call-manager-fallback</code>	<code>call-manager-fallback</code> コンフィギュレーションモードを開始します。
ステップ 2	<code>timeouts ringing seconds</code>  例: Router(config-cm-fallback)# <code>timeouts ringing 30</code>	呼び出しタイムのデフォルトを秒単位で設定します。範囲は 5 ~ 60000 です。デフォルト値はありません。
ステップ 3	<code>exit</code>  例: Router(config-cm-fallback)# <code>exit</code>	<code>call-manager-fallback</code> コンフィギュレーションモードを終了します。

例

次の例では、呼び出しタイムアウトのデフォルトを 30 秒に設定します。

```
call-manager-fallback
timeouts ringing 30
```

発信コールの設定

発信コールの設定では、次の作業を行うことができます。

- コール転送の設定
  - ローカルおよびリモートのコール転送の設定 (P.92)(オプション)
  - Cisco SRST 3.0 での H.450.2 および H.450.3 を使用した打診コール転送および自動転送 (P.93)(オプション)
  - Cisco SRST 3.0 またはそれ以前のバージョンでのフックフラッシュおよび H.450.2 標準を使用したアナログ転送の有効化 (P.97)(オプション)
- トランク アクセス コードの設定 (P.101)(特定の条件下で必須)
- 桁間タイムアウト値の設定 (P.102)(オプション)
- 制限クラスの設定 (P.103)(オプション)
- 時刻と曜日または日付に基づいたコール ブロッキング (ツールバー)(P.107)(オプション)

ローカルおよびリモートのコール転送の設定

Cisco Unified SRST では、Cisco Unified IP Phone がローカル IP ネットワークの外部からの電話コールを別の Cisco Unified IP Phone に転送できるように設定する必要があります。デフォルトでは、Cisco Unified IP Phone の電話番号または仮想音声ポートはすべて転送先として使用可能です。最大 32 個の転送パターンを入力できます。

コール転送を設定するには、`transfer-pattern` コマンドを使用します。

要約手順

1. `call-manager-fallback`
2. `transfer-pattern transfer-pattern`
3. `exit`

詳細手順

	コマンドまたはアクション	目的
ステップ 1	<code>call-manager-fallback</code>  例: Router(config)# call-manager-fallback	call-manager-fallback コンフィギュレーション モードを開始します。
ステップ 2	<code>transfer-pattern transfer-pattern</code>  例: Router(config-cm-fallback)# transfer-pattern 52540..	指定された転送パターンを使用して、IP Phone 以外の電話機の番号からのコールを同じ IP ネットワーク上の別の Cisco Unified IP Phone に転送できるようにします。  • <i>transfer-pattern</i> : 許可するコール転送の数字列。ワイルドカードが使用可能です。
ステップ 3	<code>exit</code>  例: Router(config-cm-fallback)# exit	call-manager-fallback コンフィギュレーション モードを終了します。

例

次の例では、`transfer-pattern` コマンドは、5550100 ~ 5550199 の範囲の番号を使用して、IP Phone 以外の電話機の番号からのコールを同じ IP ネットワーク上の任意の Cisco Unified IP Phone に転送できるようにします。

```
call-manager-fallback
transfer-pattern 55501..
```

Cisco SRST 3.0 での H.450.2 および H.450.3 を使用した打診コール転送および自動転送

H.450.2 を使用した打診コール転送には、ITU-T H.450.2 および ITU-T H.450.3 標準を使用して、コール レッグでコール転送と自動転送を開始するためのサポートが追加されています。H.450.2 および H.450.3 を使用したコール転送と自動転送は、ブラインドまたは打診のどちらかです。ブラインドコール転送またはブラインド自動転送とは、呼び出し音が鳴る前に転送元電話機が発信者を転送先回線に接続する方式のことです。打診転送とは、転送元が、呼び出し中の電話機（リングバックが聞こえる）に発信者を接続する、または第三者と会話してから発信者を第三者に接続する方式のことです。



(注) Cisco SRST 3.1 以降のバージョンと Cisco Unified SRST 4.0 以降のバージョンでは、H.450.2 を使用したコール転送と自動転送は、デフォルト セッション アプリケーションで自動的にサポートされます。

前提条件

- 打診によるコール転送を使用できるのは、IP Phone で 2 つ目の回線またはコール インスタンスがサポートされている場合のみです。max-dn コマンドの *dual-line* キーワードを参照してください。
- VoIP ネットワーク内の音声ゲートウェイ ルータはすべて、H.450 標準をサポートしている必要があります。
- VoIP ネットワーク内の音声ゲートウェイ ルータはすべて、次のソフトウェアを実行している必要があります。
  - Cisco IOS Release 12.3(2)T 以降のリリース
  - Cisco SRST 3.0

**制約事項**


ルータ間での H.450.12 補足サービス機能の交換は実装されていません。

**要約手順**

1. `call-manager-fallback`
2. `call-forward pattern pattern` (コール転送のみ)
3. `transfer-system {blind | full-blind | full-consult | local-consult}` (コール転送のみ)
4. `transfer-pattern transfer-pattern` (コール転送のみ)
5. `exit`
6. `voice service voip`
7. `h323`
8. `h450 h450-2 timeout {T1 | T2 | T3 | T4} milliseconds`
9. `end`

**詳細手順**

	コマンドまたはアクション	目的
ステップ 1	<p><code>call-manager-fallback</code></p> <p>例: Router(config)# <code>call-manager-fallback</code></p>	<p><code>call-manager-fallback</code> コンフィギュレーション モードを開始します。</p>
ステップ 2	<p><code>call-forward pattern pattern</code></p> <p>例: Router(config-cm-fallback)# <code>call-forward pattern 4...</code></p>	<p>自動転送に対して H.450.3 標準を指定します。</p> <ul style="list-style-type: none"> <li>• <code>pattern</code> : H.450.3 標準を使用した自動転送において照合する番号。着信コールの発信元番号がパターンと一致する場合、H.450.3 標準を使用して自動転送することができます。T というパターンは、H.450.3 標準を使用してすべての発信元を自動転送します。</li> </ul>

	コマンドまたはアクション	目的
ステップ 3	<p><b>transfer-system</b> {<i>blind</i>   <i>full-blind</i>   <i>full-consult</i>   <i>local-consult</i>}</p> <p><b>例:</b> Router(config-cm-fallback)# transfer-system full-consult</p>	<p>転送先が Cisco ATA、Cisco VG224、または SCCP 制御の FXS ポート上にある場合はサポートされません。</p> <p>Cisco Unified SRST ルータで管理されるすべての回線のコール転送方式を定義します。</p> <ul style="list-style-type: none"> <li><b>blind</b> : シスコ独自の方式を使用し、単一電話回線で、打診を行わずにコールを転送します。</li> </ul> <p> <b>(注)</b> <i>blind</i> キーワードはお勧めできません。代わりに、<i>full-blind</i> または <i>full-consult</i> キーワードを使用してください。</p> <ul style="list-style-type: none"> <li><b>full-blind</b> : H.450.2 標準方式を使用し、打診を行わずにコールを転送します。</li> <li><b>full-consult</b> : 使用可能な 2 つ目の電話回線を使用し、打診を行ってコールを転送します。2 つ目の回線が使用できない場合は、<b>full-blind</b> に戻ります。</li> <li><b>local-consult</b> : 使用可能な 2 つ目の電話回線を使用し、ローカルで打診を行ってコールを転送します。打診先または転送先がローカル以外の場合は、<b>blind</b> に戻ります。</li> </ul>
ステップ 4	<p><b>transfer-pattern</b> <i>transfer-pattern</i></p> <p><b>例:</b> Router(config-cm-fallback)# transfer-pattern 52540..</p>	<p>Cisco Unified IP Phone による電話コールを指定の電話番号パターンに転送できるようにします。</p> <ul style="list-style-type: none"> <li><i>transfer-pattern</i> : 許可するコール転送の数字列。ワイルドカードが使用可能です。</li> </ul>
ステップ 5	<p><b>exit</b></p> <p><b>例:</b> Router(config-cm-fallback)# exit</p>	<p>call-manager-fallback コンフィギュレーション モードを終了します。</p> <p> <b>ワンポイント・アドバイス</b> 既存の call-manager-fallback コンフィギュレーション モードの前に、Cisco Unified SRST Phone のネットワーク全体について設定する必要がある他のパラメータをすべて設定してください。</p>
ステップ 6	<p><b>voice service voip</b></p> <p><b>例:</b> Router(config)# voice service voip</p>	<p>(オプション) voice service コンフィギュレーション モードを開始します。</p>
ステップ 7	<p><b>h323</b></p> <p><b>例:</b> Router(conf-voi-serv)# h323</p>	<p>(オプション) H.323 voice service コンフィギュレーション モードを開始します。</p>

■ 着信コールと発信コールに対するコール処理の設定方法

	コマンドまたはアクション	目的
ステップ 8	<pre>h450 h450-2 timeout {T1   T2   T3   T4} milliseconds</pre> <p><b>例:</b> Router(conf-serv-h323)# h450 h450-2 timeout T1 750</p>	<p>(オプション) 補足サービス タイマーのタイムアウトをミリ秒単位で設定します。このコマンドは、主に、このタイマーのデフォルト設定がネットワークの遅延パラメータに適合しない場合に使用されます。このタイマーの詳細については、ITU-T H.450.2 の仕様を参照してください。</p> <ul style="list-style-type: none"> <li>• T1: 応答を識別するまで待機するときのタイムアウト値。デフォルトは 2000 です。</li> <li>• T2: コールが設定されるまで待機するときのタイムアウト値。デフォルトは 5000 です。</li> <li>• T3: 応答を開始するまで待機するときのタイムアウト値。デフォルトは 5000 です。</li> <li>• T4: 応答が設定されるまで待機するときのタイムアウト値。デフォルトは 5000 です。</li> <li>• <i>milliseconds</i>: ミリ秒数。範囲は 500 ~ 60000 です。</li> </ul>
ステップ 9	<pre>end</pre> <p><b>例:</b> Router(conf-serv-h323)# end</p>	<p>(オプション) 特権 EXEC モードに戻ります。</p>

例

次の例では、Cisco Unified SRST ルータで管理するすべての IP Phone に対して、H.450.2 標準を使用した打診による転送を指定します。

```
dial-peer voice 100 pots
destination-pattern 9.T
port 1/0/0

dial-peer voice 4000 voip
destination-pattern 4...
session-target ipv4:10.1.1.1

call-manager-fallback
transfer-pattern 4...
transfer-system full-consult
```

次の例では、H.450.3 標準を使用した自動転送を有効にします。

```
dial-peer voice 100 pots
destination-pattern 9.T
port 1/0/0
!
dial-peer voice 4000 voip
destination-pattern 4
session-target ipv4:10.1.1.1
!
call-manager-fallback
call-forward pattern 4
```

## Cisco SRST 3.0 またはそれ以前のバージョンでのフックフラッシュおよび H.450.2 標準を使用したアナログ転送の有効化

フックフラッシュおよび H.450.2 標準を使用したアナログ コール転送を利用すると、アナログ電話機で、転送を開始するためのフックフラッシュを使用し、打診を行ってコールを転送することができます。フックフラッシュとは、コール中に電話機などのデバイスによって一般に生成される短いオンフック状態を指します。この状態は、その電話機が PBX からのダイヤルトーンの再呼び出しを実行しようとしていることを示します。フックフラッシュは、コール転送を実行するためによく使用されます。たとえば、発信者がアナログ電話機の受話器台のフックを瞬時に 1 回押して放すと、フックフラッシュが発生します。

この機能を使用するには、Tool Command Language (TCL) スクリプトをインストールする必要があります。<http://www.cisco.com/cgi-bin/tablebuild.pl/ip-istosp> にある Cisco Software Center から app-h450-transfer.tcl スクリプトをダウンロードし、Cisco Unified SRST ルータからアクセス可能な TFTP サーバ、または Cisco Unified SRST ルータ上のフラッシュ メモリにコピーする必要があります。このスクリプトをすべてのダイヤル ピアにグローバルに適用するには、global コンフィギュレーション モードで `call application global` コマンドを使用します。TCL スクリプトには、`call application voice` コマンドで AV (Attribute-Value) のペアを使用して値を渡すことが可能なパラメータが含まれています。この機能に適用されるパラメータは次のとおりです。

- **delay-time** : 遅延タイマーを使用し、アナログ電話機からのコール転送時における打診コールの設定時間を短縮または遅延します。すべての数字が収集されると、遅延タイマーが開始します。受信側に対するコール設定は、遅延タイマーが期限切れになるまで開始しません。転送元がオンフックになってから遅延タイマーが期限切れになった場合、転送は打診転送ではなく、ブラインド転送であると見なされます。転送元がオンフックになる前に遅延タイマーが期限切れになった場合、転送先電話機で呼び出し音が鳴っているとき、または転送先が応答したときは、転送は打診転送であると見なされます。

TCL スクリプトだけでなく、ReadMe ファイルにも、スクリプトや設定可能な AV のペアの説明が記載されています。新しいバージョンのスクリプトをダウンロードしたら、必ず ReadMe ファイルをお読みください。このファイルには、設定パラメータやユーザ インターフェイスの説明など、スクリプト固有の情報が記載されている場合があります。



(注)

Cisco SRST 3.1 以降のバージョンと Cisco Unified SRST 4.0 以降のバージョンでは、H.450.2 を使用したコール転送は、デフォルト セッション アプリケーションで自動的にサポートされます。

### 前提条件

- Cisco Software Center から app-h450-transfer.tcl という H.450 TCL スクリプトをダウンロードする必要があります。使用可能なスクリプトのバージョンは次のとおりです。
  - app-h450-transfer.2.0.0.2.tcl (Cisco IOS Release 12.2(11)YT1 以降のリリースに対応)
  - app-h450-transfer.2.0.0.1.tcl (Cisco IOS Release 12.2(11)YT に対応)
- VoIP ネットワーク内の音声ゲートウェイ ルータはすべて、H.450 をサポートし、次のソフトウェアを実行している必要があります。
  - Cisco IOS Release 12.2(11)YT 以降のリリース
  - Cisco SRST V3.0 またはそれ以前のバージョン
  - TCL IVR 2.0
  - H.450 TCL スクリプト (app-h450-transfer.tcl)



(注)

app-h450-transfer.2.0.0.1.tcl スクリプトは、Cisco IOS Release 12.2(11)YT1 以降をインストールした場合でも引き続き使用できます。一方、app-h450-transfer.2.0.0.2.tcl スクリプトは、Cisco IOS Release 12.2(11)YT1 以前のリリースの Cisco IOS ソフトウェアでは使用できません。

### 制約事項

- アナログ FXS 電話機でフックフラッシュを使用して打診転送を行う場合、最初の転送動作が完了して、転送される側が転送先に接続される前に、打診コール自体を再転送することはできません（つまり、この転送を再帰的または連鎖式の転送にすることはできません）。最初の転送動作が完了し、通話者が転送される側と転送先だけになった場合、転送先はコールを再転送できます。
- 打診によるコール転送は、Cisco ATA-186、Cisco ATA-188、および Cisco IP Conference Station 7935 ではサポートされていません。これらのデバイスから試行される転送は、ブラインド転送として実行されます。

### 要約手順

1. **call application voice** *application-name location*
2. **call application voice** *application-name language number language*
3. **call application voice** *application-name set-location language category location*
4. **call application voice** *application-name delay-time seconds*
5. **dial-peer voice** *number pots*
6. **application** *application-name*
7. **exit**
8. **dial-peer voice** *number voip*
9. **application** *application-name*
10. **exit**



詳細手順

	コマンドまたはアクション	目的
<p><b>ステップ 1</b></p>	<pre>call application voice application-name location</pre> <p><b>例:</b> Router(config)# call application voice transfer_app flash:app-h450-transfer.tcl</p>	<p>TCL スクリプトをロードし、そのアプリケーション名を指定します。</p> <ul style="list-style-type: none"> <li>• <i>application-name</i> : IVR アプリケーションのユーザ指定の名前。この名前は、スクリプトのファイル名と一致させる必要はありません。</li> <li>• <i>location</i> : スクリプトの URL 形式のディレクトリおよびファイル名。たとえば、フラッシュメモリ (flash:filename)、TFTP (tftp://../filename)、または HTTP サーバ (http://../filename) は有効なロケーションです。</li> </ul>
<p><b>ステップ 2</b></p>	<pre>call application voice application-name language number language</pre> <p><b>例:</b> Router(config)# call application voice transfer_app language 1 en</p>	<p>(オプション)アプリケーションで使用されるダイナミック プロンプトの言語を設定します。</p> <ul style="list-style-type: none"> <li>• <i>application-name</i> : ステップ 1 で割り当てた IVR アプリケーションの名前。</li> <li>• <i>number</i> : IVR アプリケーションのオーディオファイルで使用される言語を識別する番号。</li> <li>• <i>language</i> : プロンプトの言語を指定する 2 文字のコード。有効なエントリは、en (英語: デフォルト)、sp (スペイン語)、ch (中国語)、または aa (すべて) です。</li> </ul>
<p><b>ステップ 3</b></p>	<pre>call application voice application-name set-location language category location</pre> <p><b>例:</b> Router(config)# call application voice transfer_app set-location en 0 flash:/prompts</p>	<p>アプリケーションでダイナミック プロンプトに使用されるオーディオ ファイルのロケーションおよびカテゴリを定義します。</p> <ul style="list-style-type: none"> <li>• <i>application-name</i> : TCL IVR アプリケーションの名前。</li> <li>• <i>language</i> : プロンプトの言語を指定する 2 文字のコード。有効なエントリは、en (英語: デフォルト)、sp (スペイン語)、ch (中国語)、または aa (すべて) です。</li> <li>• <i>category</i> : このロケーションからのオーディオファイルのカテゴリ グループ (0 ~ 4)。0 という値は、すべてのカテゴリを意味します。</li> <li>• <i>location</i> : アプリケーションで使用される言語オーディオ ファイルを含むディレクトリの URL (ファイル名は含みません)、フラッシュメモリ (flash) やサーバ (TFTP、HTTP、または RTSP) 上のディレクトリはすべて有効です。</li> </ul> <p>プロンプトは、アナログ FXS 電話機からのコール転送で必要になります。IP Phone からのコール転送にはプロンプトは必要ありません。</p>

■ 着信コールと発信コールに対するコール処理の設定方法

	コマンドまたはアクション	目的
ステップ 4	<p><b>call application voice</b> <i>application-name</i> <i>delay-time seconds</i></p> <p><b>例:</b> Router(config)# call application voice transfer_app delay-time 1</p>	<p>(オプション) H.450 アプリケーションを使用してコール転送を行うアナログ電話機に対して、打診コールの設定の遅延時間を設定します。このコマンドは、AV のペアを使用して TCL スクリプトに値を渡します。</p> <ul style="list-style-type: none"> <li><i>seconds</i> : コール設定を遅延する秒数。範囲は 1 ~ 10 です。デフォルトは 2 です。</li> </ul> <p>遅延が 2 秒を超えると、多くのユーザがそのことに気づきます。</p> <p>AV のペアや H.450 コール転送および自動転送用の TCL スクリプトの詳細については、スクリプトに付属している ReadMe ファイルを参照してください。</p>
ステップ 5	<p><b>dial-peer voice</b> <i>number pots</i></p> <p><b>例:</b> Router(config)# dial-peer voice 25 pots</p>	<p>POTS ダイアル ピアを設定するために dial-peer コンフィギュレーション モードを開始します。</p>
ステップ 6	<p><b>application</b> <i>application-name</i></p> <p><b>例:</b> Router(config-dial-peer)# application transfer_app</p>	<p>ステップ 1 で指定したアプリケーションをダイアルピアにロードします。</p>
ステップ 7	<p><b>exit</b></p> <p><b>例:</b> Router(config-dial-peer)# exit</p>	<p>dial-peer コンフィギュレーション モードを終了します。</p> <p></p> <p><b>ワンポイント・アドバイス</b> 既存の dial-peer コンフィギュレーション モードの前に、このダイアル ピアについて設定する必要がある他のダイアルピアパラメータをすべて設定してください。</p>
ステップ 8	<p><b>dial-peer voice</b> <i>number voip</i></p> <p><b>例:</b> Router(config)# dial-peer voice 29 voip</p>	<p>VoIP ダイアル ピアを設定するために dial-peer コンフィギュレーション モードを開始します。</p>
ステップ 9	<p><b>application</b> <i>application-name</i></p> <p><b>例:</b> Router(config-dial-peer)# application transfer_app</p>	<p>ステップ 1 で指定したアプリケーションをダイアルピアにロードします。</p>
ステップ 10	<p><b>exit</b></p> <p><b>例:</b> Router(config-dial-peer)# exit</p>	<p>dial-peer コンフィギュレーション モードを終了します。</p> <p></p> <p><b>ワンポイント・アドバイス</b> 既存の dial-peer コンフィギュレーション モードの前に、このダイアル ピアについて設定する必要がある他のダイアルピアパラメータをすべて設定してください。</p>

## 例

次の例では、フックフラッシュを使用したアナログ転送用の H.450 TCL スクリプトを有効にし、遅延時間を 1 秒に設定します。

```
call application voice transfer_app flash:app-h450-transfer.tcl
call application voice transfer_app language 1 en
call application voice transfer_app set-location en 0 flash:/prompts
call application voice transfer_app delay-time 1
!
dial-peer voice 25 pots
 destination-pattern 9.T
 port 1/0/0
 application transfer_app
!
dial-peer voice 29 voip
 destination-pattern 4...
 session-target ipv4:10.1.10.1
 application transfer_app
```

## トランク アクセス コードの設定



(注)

トランク アクセス コードの設定が必要になるのは、通常のネットワーク ダイアル プラン設定により、フォールバック時に使用可能なトランク アクセスを提供する永続的な POTS 音声ダイアル ピアを設定することが禁止されている場合のみです。ローカル PSTN ポートに、ダイアル ピアによって提供される適切なアクセス コードがすでに設定されている場合(たとえば、FXO PSTN 回線を選択するときは 9 をダイヤルする) この設定は必要ありません。

トランク アクセス コードを使用すると、IP Phone が Cisco Unified Communications Manager のフォールバック時に PSTN にアクセスできるようになります。これを可能にするために、Cisco Unified Communications Manager のフォールバック時にのみアクティブになる POTS 音声ダイアル ピアが作成されます。この一時的なダイアル ピアは、音声ポート (BRI、E&M、FXO、および PRI) に適合させることができ、このダイアル ピアを使用すると、Cisco Unified IP Phone が Cisco Unified Communications Manager フォールバック モードのときにトランク回線にアクセスできるようになります。Cisco Unified SRST がアクティブの場合、同一タイプの PSTN インターフェイスはすべて同等のものとして処理され、PSTN コールの発信時には任意のポートが選択されることがあります。

トランク アクセス コードを作成するには、`access-code` コマンドを使用します。

## 要約手順

1. `call-manager-fallback`
2. `access-code` `{ {fxo | e&m} dial-string | {bri | pri} dial-string [direct-inward-dial] }`
3. `exit`

詳細手順

	コマンドまたはアクション	目的
ステップ 1	<b>call-manager-fallback</b>  <b>例:</b> Router(config)# call-manager-fallback	call-manager-fallback コンフィギュレーション モードを開始します。
ステップ 2	<b>access-code</b> {{ <i>fxo</i>   <i>e&amp;m</i> } <i>dial-string</i>   { <i>bri</i>   <i>pri</i> } <i>dial-string</i> [ <i>direct-inward-dial</i> ]}  <b>例:</b> Router(config-cm-fallback)# access-code e&m 8	トランク アクセス コードを回線のタイプごとに設定します。その結果、Cisco Unified SRST が有効になっている場合、Cisco Unified Communications Manager フォールバック モードのときに、Cisco Unified IP Phone がトランク回線にのみアクセスできるようになります。 <ul style="list-style-type: none"> <li>• <i>fxo</i> : Foreign Exchange Office( FXO )インターフェイスを有効にします。</li> <li>• <i>e&amp;m</i> : アナログ Ear and Mouth ( E&amp;M ) インターフェイスを有効にします。</li> <li>• <i>dial-string</i> : ダイヤル ピアを作成して、指定された回線タイプごとにダイヤル アクセス コードを設定する文字列。 <i>dial-string</i> 引数は、指定された回線タイプごとに一時的なダイヤル ピアを設定するために使用されます。</li> <li>• <i>bri</i> : BRI インターフェイスを有効にします。</li> <li>• <i>pri</i> : PRI インターフェイスを有効にします。</li> <li>• <i>direct-inward-dial</i> :( オプション )POTS ダイヤルピアにおいてダイヤルイン ( DID ) を有効にします。</li> </ul>
ステップ 3	<b>exit</b>  <b>例:</b> Router(config-cm-fallback)# exit	call-manager-fallback コンフィギュレーション モードを終了します。

例

次の例では、BRI 用にアクセス コード番号 8 を作成し、POTS ダイヤル ピアにおいて DID を有効にします。

```
call-manager-fallback
access-code bri 8 direct-inward-dial
```

桁間タイムアウト値の設定

桁間タイムアウト値の設定では、Cisco Unified SRST ルータに接続されたすべての Cisco Unified IP Phone が最初の数字または後続の数字のダイヤル後に待機する時間を秒単位で指定する必要があります。 **timeouts interdigit** タイマーは、発信者が数字を入力すると有効になり、発信者が後続の数字を入力するたびに再起動されます。この動作は、宛先アドレスが識別されるまで続きます。宛先アドレスが識別される前に設定済みのタイムアウト値を超えると、トーンが聞こえてコールが終了します。



(注) この値の設定が重要になるのは、可変長のダイヤル ピア宛先パターン (ダイヤル プラン) を使用する 場合です。ダイヤル プランの設定の詳細については、『Cisco IOS Voice, Video, and Fax Configuration Guide, Release 12.2』を参照してください。

要約手順

1. `call-manager-fallback`
2. `timeouts interdigit seconds`
3. `exit`

詳細手順

	コマンドまたはアクション	目的
ステップ 1	<code>call-manager-fallback</code>  例: Router(config)# <code>call-manager-fallback</code>	call-manager-fallback コンフィギュレーション モードを開始します。
ステップ 2	<code>timeouts interdigit seconds</code>  例: Router(config-cm-fallback)# <code>timeouts interdigit 5</code>	(オプション) ルータに接続されたすべての Cisco IP Phone の桁間タイムアウト値を設定します。  • <code>seconds</code> : すべての Cisco Unified IP Phone の桁間タイムアウト期間 (秒数)。有効なエントリは、2 ~ 120 の整数です。
ステップ 3	<code>exit</code>  例: Router(config-cm-fallback)# <code>exit</code>	call-manager-fallback コンフィギュレーション モードを終了します。

例

次の例では、すべての Cisco Unified IP Phone の桁間タイムアウト値を 5 秒に設定します。この例では、5 秒が経過しても完全にダイヤルされていない番号はタイムアウトします。たとえば、必須の 10 桁 (4085550100) ではなく 9 桁 (408555010) をダイヤルした場合、5 秒のタイムアウト期間が経過すると、発信者にはビジー トーンが聞こえます。

```
call-manager-fallback
timeouts interdigit 5
```

制限クラスの設定

制限クラス (COR) 機能を使用すると、ダイヤル ピアでプロビジョニングされた着信および発信の制限クラスに基づいて、特定のコールを拒否できます。この機能により、柔軟なネットワーク設計が可能になります。また、ユーザは、コール (たとえば、900 番へのコール) をブロックすることや、異なる発信者からのコールに対してそれぞれ異なる制限を適用することができます。cor コマンドは、Cisco Unified Communications Manager のフォールバック時に作成される電話番号に関連付けられたダイヤル ピア用のダイヤル ピア COR パラメータを設定します。

■ 着信コールと発信コールに対するコール処理の設定方法

着信コールおよび発信コールごとに最大 20 の COR リストを設定できます。どの COR リストの番号または番号範囲にも一致しない電話番号には、デフォルト COR が割り当てられます。割り当てられた COR は、Communications Manager フォールバックの登録時に自動的に各電話番号に対して作成されたダイヤル ピアから呼び出されます。

COR が (着信コール用の) 着信ダイヤル ピアに適用されている場合、その COR が (発信コール用の) 発信ダイヤル ピアに適用されている COR の上位セットまたは同一セットであるときは、コールは正常に処理されます。コールが着信と発信のどちらであるかは、音声ポートで判別されます。電話機を Cisco Unified SRST ルータ上の FXS ポートに接続し、その電話機からコールを発信する場合、コールはルータおよび音声ポートへの着信コールと見なされます。FXS 電話機にコールを発信する場合、コールは発信コールと見なされます。

デフォルトでは、着信コール レッグには最高の COR 優先順位が割り当てられ、発信コール レッグには最低の優先順位が割り当てられます。ダイヤル ピアに着信コールの COR が設定されていない場合は、そのダイヤル ピアに接続された電話機からコールを発信できます。結果として、コールは、そのダイヤル ピアの COR 設定に関係なく、任意のダイヤル ピアから発信されます。表 6 は、COR リストの設定方法に基づいたコール機能を説明しています。

表 6 COR リストの組み合わせと結果

着信ダイヤル ピアの COR リスト	発信ダイヤル ピアの COR リスト	結果
COR なし	COR なし	コールは正常に処理されます。
COR なし	発信コールに COR リストを適用	コールは正常に処理されます。デフォルトでは、COR が適用されていない場合、着信ダイヤル ピアには最高の COR 優先順位が割り当てられます。ダイヤル ピアに着信コール レッグの COR を適用しない場合、そのダイヤル ピアは、発信ダイヤル ピアの COR 設定に関係なく、他の任意のダイヤル ピアからコールを発信できます。
着信コールに COR リストを適用	COR なし	コールは正常に処理されます。デフォルトでは、発信ダイヤル ピアには最低の優先順位が割り当てられます。着信または発信ダイヤル ピアに着信コールの COR が設定されているため、この COR は、発信または終端ダイヤル ピアに対する発信コールの COR 設定の上位セットとなります。
着信コールに COR リストを適用 (発信ダイヤル ピアで発信コールに適用されている COR リストの上位セット)	発信コールに COR リストを適用 (着信ダイヤル ピアで着信コールに適用されている COR リストのサブセット)	コールは正常に処理されます。着信ダイヤル ピアにおける着信コール用の COR リストは、発信ダイヤル ピアにおける発信コール用の COR リストの上位セットです。
着信コールに COR リストを適用 (発信ダイヤル ピアで発信コールに適用されている COR リストのサブセット)	発信コールに COR リストを適用 (着信ダイヤル ピアで着信コールに適用されている COR リストの上位セット)	コールは正常に処理されません。着信ダイヤル ピアにおける着信コール用の COR リストが、発信ダイヤル ピアにおける発信コール用の COR リストの上位セットになっていません。

要約手順

1. call-manager-fallback
2. cor {incoming | outgoing} cor-list-name {cor-list-number starting-number - ending-number | default}
3. exit

詳細手順

	コマンドまたはアクション	目的
ステップ 1	<b>call-manager-fallback</b>  <b>例:</b> Router(config)# call-manager-fallback	call-manager-fallback コンフィギュレーション モードを開始します。
ステップ 2	<b>cor {incoming   outgoing} cor-list-name</b> [cor-list-number starting-number - ending-number   default]	電話番号に関連付けられたダイヤル ピアに COR を設定します。 <ul style="list-style-type: none"> <li>• <b>incoming</b> : 着信ダイヤル ピアで使用される COR リスト。</li> <li>• <b>outgoing</b> : 発信ダイヤル ピアで使用される COR リスト。</li> <li>• <b>cor-list-name</b> : COR リストの名前。</li> <li>• <b>cor-list-number</b> : COR リストの識別子。作成可能な COR リストの最大数は 20 です。このリストは、着信または発信ダイヤル ピアで構成されます。最初の 6 つの COR リストは、電話番号の範囲に適用されます。COR が設定されていない電話番号は、デフォルト COR リストに割り当てられます。</li> <li>• <b>starting-number - ending-number</b> : 電話番号の範囲 (たとえば、2000 - 2025)。</li> <li>• <b>default</b> : 既存のデフォルト COR リストを使用するようにルータに指示します。</li> </ul>
ステップ 3	<b>exit</b>  <b>例:</b> Router(config-cm-fallback)# exit	call-manager-fallback コンフィギュレーション モードを終了します。

例

次の例は、フォールバック時に作成される Cisco Unified IP Phone ダイヤル ピアおよび電話番号に対して、発信コール用のダイヤル ピア COR パラメータを設定する方法を示しています。

```
call-manager-fallback
cor outgoing LockforPhoneC 1 5010 - 5020
```

次の例は、デフォルト COR リスト内の Cisco IP Phone ダイヤル ピアおよび電話番号に対して、着信コール用のダイヤル ピア COR パラメータを設定する方法を示しています。

```
call-manager-fallback
cor incoming LockforPhoneC default
```

次の例は、COR のサブセットおよび上位セットの作成方法を示しています。最初に、カスタム ダイヤル ピア COR を作成し、その下で名前を宣言します。

```
dial-peer cor custom
name 911
name 1800
name 1900
name local_call
```

次の設定例では、COR リストを作成し、ダイヤル ピアに適用します。

```
dial-peer cor list call911
  member 911

dial-peer cor list call1800
  member 1800

dial-peer cor list call1900
  member 1900

dial-peer cor list calllocal
  member local_call

dial-peer cor list engineering
  member 911
  member local_call

dial-peer cor list manager
  member 911
  member 1800
  member 1900
  member local_call

dial-peer cor list hr
  member 911
  member 1800
  member local_call
```

次の例では、宛先番号 734....、1800.....、1900.....、316....、および 911 に対する 5 つのダイヤル ピアを設定します。COR リストは、各ダイヤル ピアに適用します。

```
dial-peer voice 1 voip
  destination pattern 734....
  session target ipv4:10.1.1.1
  cor outgoing calllocal

dial-peer voice 2 voip
  destination pattern 1800.....
  session target ipv4:10.1.1.1
  cor outgoing call1800

dial-peer voice 3 pots
  destination pattern 1900.....
  port 1/0/0
  cor outgoing call1900

dial-peer voice 5 pots
  destination pattern 316....
  port 1/1/0
  ! No COR is applied.

dial-peer voice 4 pots
  destination pattern 911
  port 1/0/1
  cor outgoing call911
```

最後に、COR リストを個別の電話番号に適用します。

```
call-manager-fallback
  max-conferences 8
  cor incoming engineering 1 1001 - 1001
  cor incoming hr 2 1002 - 1002
  cor incoming manager 3 1003 - 1008
```



この設定例は、次の設定にも使用可能です。

- 内線番号 1001 から 734... 番、911、および 316... にコールする
- 内線番号 1002 から 734...、1800 番、911、および 316... にコールする
- 内線番号 1003 ~ 1008 から Cisco Unified SRST ルータの考えられるすべての番号にコールする
- すべての内線番号から 316... にコールする

### 時刻と曜日または日付に基づいたコール ブロッキング (トールバー)

電話機の不正使用を防ぐためのコール ブロッキングでは、指定された時刻と曜日または日付に、指定された番号パターンが照合されます。最大 32 の番号パターンを指定できます。コール ブロッキングは IP Phone のみでサポートされ、アナログ FXS 電話機ではサポートされません。

コール ブロッキング用に定義された期間に、コール ブロッキング用に指定されたパターンと一致する番号にユーザがコールを発信しようとするすると、約 10 秒間、小刻みなビジー信号が再生されず。その後、コールが終了し、回線はオンフック状態に戻ります。

SRST (call-manager-fallback 設定) モードでは、営業時間外のコール ブロッキングを電話機ベースまたは PIN ベースで除外することはできません。

#### 要約手順

1. `call-manager-fallback`
2. `after-hours block pattern tag pattern [7-24]`
3. `after-hours day day start-time stop-time`
4. `after-hours date month date start-time stop-time`
5. `exit`

#### 詳細手順

	コマンドまたはアクション	目的
ステップ 1	<code>call-manager-fallback</code>  例: Router(config)# call-manager-fallback	call-manager-fallback コンフィギュレーション モードを開始します。
ステップ 2	<code>after-hours block pattern tag pattern [7-24]</code>  例: Router(config-cm-fallback)# after-hours block pattern 1 91900	ブロックする発信番号のパターンを定義します。個別にコマンドを使用することにより、最大 32 のパターンを定義できます。  <ul style="list-style-type: none"> <li>• 7-24 キーワードを指定すると、番号パターンは週 7 日、1 日 24 時間、常にブロックされます。</li> <li>• 7-24 キーワードを指定しない場合、番号パターンは <code>after-hours day</code> コマンドと <code>after-hours date</code> コマンドを使用して定義した曜日と日付に基づいてブロックされます。</li> </ul>

■ 着信コールと発信コールに対するコール処理の設定方法

	コマンドまたはアクション	目的
ステップ 3	<p><code>after-hours day day start-time stop-time</code></p> <p>例: Router(config-cm-fallback)# after-hours day mon 19:00 7:00</p>	<p><code>after-hours block pattern</code> コマンドを使用して定義した発信ダイヤル パターンへのコールをブロックする期間を曜日で定義します。</p> <ul style="list-style-type: none"> <li>• <code>day</code>: 曜日の省略形。使用できる曜日の省略形は、<code>sun</code>、<code>mon</code>、<code>tue</code>、<code>wed</code>、<code>thu</code>、<code>fri</code>、および <code>sat</code> です。</li> <li>• <code>start-time stop-time</code>: コール ブロッキングの開始時刻と終了時刻。24 時間制の HH:MM 形式で指定します。終了時刻に開始時刻よりも小さい値を指定すると、終了時刻は開始日の翌日の同時刻になります。たとえば、「<code>mon 19:00 07:00</code>」は、「月曜日の午後 7 時から火曜日の午前 7 時まで」を意味します。</li> </ul>
ステップ 4	<p><code>after-hours date month date start-time stop-time</code></p> <p>例: Router(config-cm-fallback)# after-hours date jan 1 0:00 0:00</p>	<p><code>after-hours block pattern</code> コマンドを使用して定義した発信ダイヤル パターンへのコールをブロックする期間を月日で定義します。</p> <ul style="list-style-type: none"> <li>• <code>month</code>: 月の省略形。使用できる月の省略形は、<code>jan</code>、<code>feb</code>、<code>mar</code>、<code>apr</code>、<code>may</code>、<code>jun</code>、<code>jul</code>、<code>aug</code>、<code>sep</code>、<code>oct</code>、<code>nov</code>、および <code>dec</code> です。</li> <li>• <code>date</code>: 日付。範囲は 1 ~ 31 です。</li> <li>• <code>start-time stop-time</code>: コール ブロッキングの開始時刻と終了時刻。24 時間制の HH:MM 形式で指定します。終了時刻には、開始時刻よりも大きな値を指定する必要があります。24:00 という値は無効です。終了時刻として 00:00 を入力した場合、この時刻は 23:59 に変更されます。開始時刻と終了時刻の両方に 00:00 を入力した場合は、指定した日付の 24 時間全体にわたってコールがブロックされます。</li> </ul>
ステップ 5	<p><code>exit</code></p> <p>例: Router(config-cm-fallback)# exit</p>	<p><code>call-manager-fallback</code> コンフィギュレーション モードを終了します。</p>

例

次の例では、発信コールをブロックする番号パターンを定義します。パターン 1 と 2 は、「1」と「011」で始まる外線番号へのコールをブロックするパターンで、月曜日から金曜日の午前 7 時以前と午後 7 時以降、土曜日の午前 7 時以前と午後 1 時以降、および日曜日の終日にわたってブロックされます。パターン 3 は、900 番へのコールを週 7 日、1 日 24 時間ブロックします。

```
call-manager-fallback
after-hours block pattern 1 91
after-hours block pattern 2 9011
after-hours block pattern 3 91900 7-24
after-hours block day mon 19:00 07:00
after-hours block day tue 19:00 07:00
after-hours block day wed 19:00 07:00
after-hours block day thu 19:00 07:00
after-hours block day fri 19:00 07:00
after-hours block day sat 13:00 12:00
after-hours block day sun 12:00 07:00
```

## WAN リンク障害に対する H.323 VoIP コール プリザベーションの機能拡張

WAN リンク障害に対する H.323 VoIP コール プリザベーションの機能拡張では、Cisco Unified Communications Manager などのエンティティによってシグナリングが処理される H.323 トポロジの接続が保持されるようになりました。このエンティティは、2 つの接続側の間でシグナリングを行う相手方エンドポイントおよびブローカとは異なります。

コール プリザベーションが有用になるのは、ゲートウェイと相手方エンドポイント（通常は Cisco Unified IP Phone）が同じサイトに配置され、コール エージェントがリモート側に配置されているために、接続障害の発生する確率が高くなっている場合です。

設定については、『Cisco IOS H.323 Configuration Guide, Release 12.4T』の「Configuring H.323 Gateways」の章を参照してください。このドキュメントは、次の URL から入手可能です。

[http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgr/vvfax\\_c/calle\\_c/h323\\_c/323conf/4gwconf.htm](http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgr/vvfax_c/calle_c/h323_c/323conf/4gwconf.htm)

## 関連情報

次のステップでは、Cisco Unified SRST で使用できる追加の機能を設定する必要があるかどうかを確認します。説明と設定手順については、「追加のコール機能の設定」の章を参照してください。セキュリティを設定する必要がある場合は、「Secure SRST の設定」の章を参照してください。ボイスメールを設定する必要がある場合は、「Cisco Unified SRST へのボイスメールの統合」の章を参照してください。これらの機能がいずれも必要ない場合は、「Cisco Unified SRST の監視と保守」の章に進んでください。

追加情報については、「Cisco Unified SRST の概要」の章の P.40 の「その他の資料」を参照してください。





## 追加のコール機能の設定

---

Revised: July 11, 2008

この章では、次に示すオプションの追加のコール機能について説明します。

- 3 者間 G.711 Ad Hoc 会議 : Cisco Unified Survivable Remote Site Telephony ( SRST ) による同時 3 者間会議のサポート。
- eXtensible Markup Language ( XML ) アプリケーション プログラム インターフェイス ( API ) : このインターフェイスは、Cisco Unified SRST から管理ソフトウェアにデータを供給します。
- Cisco Unified Survivable Remote Site Telephony ( SRST ) の Music On Hold ( MOH ) の統合 : MOH は、Cisco Unified SRST ルータのフラッシュ ファイルから、G.711、オンネット VoIP、および PSTN コールに対して使用できます。MOH の詳細については、[P.115 の「Cisco Unified SRST をマルチキャスト MOH リソースとして使用するための Cisco Unified Communications Manager と Cisco Unified SRST の統合」](#)を参照してください。

### 内容

- [オプション機能の設定方法 \( P.112 \)](#)
- [関連情報 \( P.114 \)](#)

## オプション機能の設定方法

次の項では、オプション機能の設定方法について説明します。

- [3 者間 G.711 Ad Hoc 会議の有効化 \(P.112\)](#)
- [XML API スキーマの定義 \(P.113\)](#)

### 3 者間 G.711 Ad Hoc 会議の有効化

3 者間 G.711 Ad Hoc 会議の有効化には、Cisco Unified SRST ルータがサポートしている同時 3 者間会議の最大数を設定する作業が含まれます。会議を使用できるようにするには、IP Phone の 1 つ以上のボタンに 2 つ以上の回線を接続する必要があります。P.66 の「[第 2 発信音の設定](#)」を参照してください。

#### 要約手順

1. `call-manager-fallback`
2. `max-conferences max-conference-numbers`
3. `exit`

#### 詳細手順

	コマンドまたはアクション	目的
ステップ 1	<code>call-manager-fallback</code>  例: Router(config)# <code>call-manager-fallback</code>	<code>call-manager-fallback</code> コンフィギュレーションモードを開始します。
ステップ 2	<code>max-conferences max-conference-numbers</code>  例: Router(config-cm-fallback)# <code>max-conferences 16</code>	ルータでサポートされている同時 3 者間会議の最大数を設定します。最大数は、プラットフォームによって異なります。 <ul style="list-style-type: none"> <li>• Cisco 1751 ルータ : 8</li> <li>• Cisco 1760 ルータ : 8</li> <li>• Cisco 2600 シリーズ ルータ : 8</li> <li>• Cisco 2600-XM シリーズ ルータ : 8</li> <li>• Cisco 2801 ルータ : 8</li> <li>• Cisco 2811、Cisco 2821、および Cisco 2851 ルータ : 16</li> <li>• Cisco 3640 および Cisco 3640A ルータ : 8</li> <li>• Cisco 3660 ルータ : 16</li> <li>• Cisco 3725 ルータ : 16</li> <li>• Cisco 3745 ルータ : 16</li> <li>• Cisco 3800 シリーズ ルータ : 24</li> </ul>
ステップ 3	<code>exit</code>  例: Router(config-cm-fallback)# <code>exit</code>	<code>call-manager-fallback</code> コンフィギュレーションモードを終了します。

## 例

次の例では、ルータに最大 8 つの同時 3 者間会議を設定します。

```
call-manager-fallback
max-conferences 8
```

## XML API スキーマの定義

この項の Cisco IOS コマンドを使用すると、XML API に関連したパラメータを指定できます。詳細については、『[XML Provisioning Guide for Cisco CME/SRST](#)』を参照してください。

## 要約手順

1. `call-manager-fallback`
2. `xmlschema schema-url`
3. `exit`

## 詳細手順

	コマンドまたはアクション	目的
ステップ 1	<code>call-manager-fallback</code>  <b>例:</b> Router(config)# <code>call-manager-fallback</code>	call-manager-fallback コンフィギュレーション モードを開始します。
ステップ 2	<code>xmlschema schema-url</code>  <b>例:</b> Router(config-cm-fallback)# <code>xmlschema</code> <code>http://server2.example.com/</code> <code>schema/schema1.xsd</code>	この Cisco Unified SRST システムで使用する XML API スキーマの URL を指定します。 <ul style="list-style-type: none"> <li>• <code>schema-url</code> : RFC 2396 で定義されたローカルまたはリモート URL</li> </ul>
ステップ 3	<code>exit</code>  <b>例:</b> Router(config-cm-fallback)# <code>exit</code>	call-manager-fallback コンフィギュレーション モードを終了します。

設定手順については、P.142 の「[Cisco Unified SRST MOH ライブ フィード サポートの設定 \(オプション\)](#)」を参照してください。

## 関連情報

MOH については、P.115 の「Cisco Unified SRST をマルチキャスト MOH リソースとして使用するための Cisco Unified Communications Manager と Cisco Unified SRST の統合」を参照してください。

Cisco Unified SRST の監視および保守については、P.227 の「Cisco Unified SRST の監視と保守」を参照してください。

追加情報については、P.25 の「Cisco Unified SRST の概要」の P.40 の「その他の資料」を参照してください。





# Cisco Unified SRST をマルチキャスト MOH リソースとして使用するための Cisco Unified Communications Manager と Cisco Unified SRST の統合

---

Revised: July 11, 2008

この章では、フォールバック時および通常の Cisco Unified Communications Manager 動作時に Cisco Unified Communications Manager が Cisco Unified SRST ゲートウェイをマルチキャスト Music On Hold (MOH) リソースとして使用できるように、Cisco Unified Communications Manager と Cisco Unified Survivable Remote Site Telephony (Cisco Unified SRST) を設定する方法について説明します。ローカルゲートウェイが MOH を提供する分散 MOH 設計では、WAN を介して MOH を流す必要がなくなるため、帯域幅を節約できます。

## この章の機能情報について

お使いの Cisco Unified CME バージョンによっては、この章に記載されている機能の一部または全部がサポートされていない場合があります。各機能をサポートしているバージョンのリストについては、[P.149 の「マルチキャスト MOH リソースとしての Cisco Unified SRST に関する機能情報」](#)を参照してください。

## 内容

- [Cisco Unified SRST ゲートウェイをマルチキャスト MOH リソースとして使用するための前提条件 \(P.116\)](#)
- [Cisco Unified SRST ゲートウェイをマルチキャスト MOH リソースとして使用するための制限事項 \(P.117\)](#)
- [Cisco Unified SRST ゲートウェイをマルチキャスト MOH リソースとして使用するための情報 \(P.118\)](#)
- [Cisco Unified SRST ゲートウェイをマルチキャスト MOH リソースとして使用する方法 \(P.123\)](#)
- [Cisco Unified SRST ゲートウェイの設定例 \(P.147\)](#)
- [関連情報 \(P.150\)](#)

## Cisco Unified SRST ゲートウェイをマルチキャスト MOH リソースとして使用するための前提条件

- H.323 および MGCP のマルチキャスト MOH は、Cisco Unified Communications Manager 3.1.1 以降のバージョンでサポートされています。
- Cisco Unified Communications Manager が次のように設定されている必要があります。
  - マルチキャスト MOH が有効である。
  - どのデバイスがマルチキャスト MOH を受信し、どのデバイスがユニキャスト MOH を受信するかを制御する、Media Resource Group (MRG; メディア リソース グループ) および Media Resource Group List (MRGL; メディア リソース グループ リスト) が設定されている。
  - Cisco Unified SRST マルチキャスト MOH リソースが呼び出されるときには必ず G.711 が使用されるように、Cisco Unified Communications Manager リージョンが割り当てられている。
- Cisco Unified SRST ゲートウェイが Cisco IOS Release 12.2(15)ZJ2 以降のリリース上の Cisco Unified SRST 3.0 で動作する必要があります。
- Cisco Unified Communications Manager および Cisco Unified SRST が H.323 または MGCP で動作する必要があります。
- Cisco Unified SRST を実行しないブランチでは、Cisco Unified Communications Manager のマルチキャスト MOH パケットが WAN を通過する必要があります。そのためには、ネットワークでマルチキャスト ルーティングが有効になっている必要があります。マルチキャスト ルーティングの詳細については、『[Cisco IOS IP Configuration Guide, Release 12.4T](#)』の「IP Multicast」の項を参照してください。
- 12.3(14)T より前の Cisco IOS の場合は、`ccm-manager fallback-mgcp` コマンドと `call application alternate` コマンドを使用して、Cisco Unified SRST を MGCP ゲートウェイのフォールバックモードとして設定します。12.3(14)T 以降の Cisco IOS リリースの場合は、`ccm-manager fallback-mgcp` コマンドと `service` コマンドを設定する必要があります。これら 2 つのコマンドを設定すると、Cisco Unified SRST が、音声ポートの制御権と MGCP ゲートウェイでのコール処理の制御権を取得できるようになります。Cisco Unified SRST をフォールバックモードとして設定する方法の詳細については、『[Cisco Unified Communications Manager Administration Guide, Release 5.1\(3\) Survivable Remote Site Telephony Configuration](#)』を参照してください。

## Cisco Unified SRST ゲートウェイをマルチキャスト MOH リソースとして使用するための制限事項

- Cisco Unified SRST マルチキャスト MOH は、ユニキャスト MOH をサポートしません。
- ネットワーク全体で 1 つの Cisco Unified Communications Manager オーディオソースだけを使用できます。ただし、各 Cisco Unified SRST ゲートウェイのフラッシュメモリ上のオーディオファイルは異なってもかまいません。
- Cisco Unified SRST マルチキャスト MOH は、G.711 だけをサポートします。
- Cisco Unified Communications Manager 3.3.2 のどのバージョンでも、H.323 のマルチキャスト MOH サポートは使用できません。詳細については、Cisco [Bug Toolkit](#) を使用して CSCdz00697 を参照してください。
- Cisco 1700 シリーズ ゲートウェイの Cisco IOS Release 12.2(15)ZJ イメージでは、Cisco Unified SRST マルチキャスト MOH に H.323 モードのサポートが含まれていません。

## Cisco Unified SRST ゲートウェイをマルチキャスト MOH リソースとして使用するための情報

Cisco Unified SRST ゲートウェイを MOH リソースとして設定するには、次の概念を理解する必要があります。

- [Cisco Unified SRST ゲートウェイと Cisco Unified Communications Manager \( P.118 \)](#)
- [コーデック、ポート番号、および IP アドレス \( P.119 \)](#)
- [マルチキャスト MOH 伝送 \( P.121 \)](#)
- [Cisco Unified SRST MOH ライブフィードのサポート \( P.121 \)](#)

### Cisco Unified SRST ゲートウェイと Cisco Unified Communications Manager

Cisco Unified SRST ゲートウェイは、フォールバック時および通常の Cisco Unified Communications Manager 動作時にフラッシュメモリから Real-Time Transport Protocol ( RTP ) パケットをマルチキャストするように設定できます。そのためには、Cisco Unified Communications Manager をマルチキャスト MOH 用に設定して、オーディオパケットが WAN を通過しないようにする必要があります。その代わりに、オーディオパケットは、Cisco Unified SRST ゲートウェイのフラッシュメモリから、Cisco Unified Communications Manager マルチキャスト MOH に設定されているマルチキャスト MOH IP アドレスおよびポート番号にブロードキャストされます。リモートサイトの IP Phone は、セントラル Cisco Unified Communications Manager からではなく、ローカルのブランチゲートウェイからマルチキャストされた RTP パケットをピックアップできます。

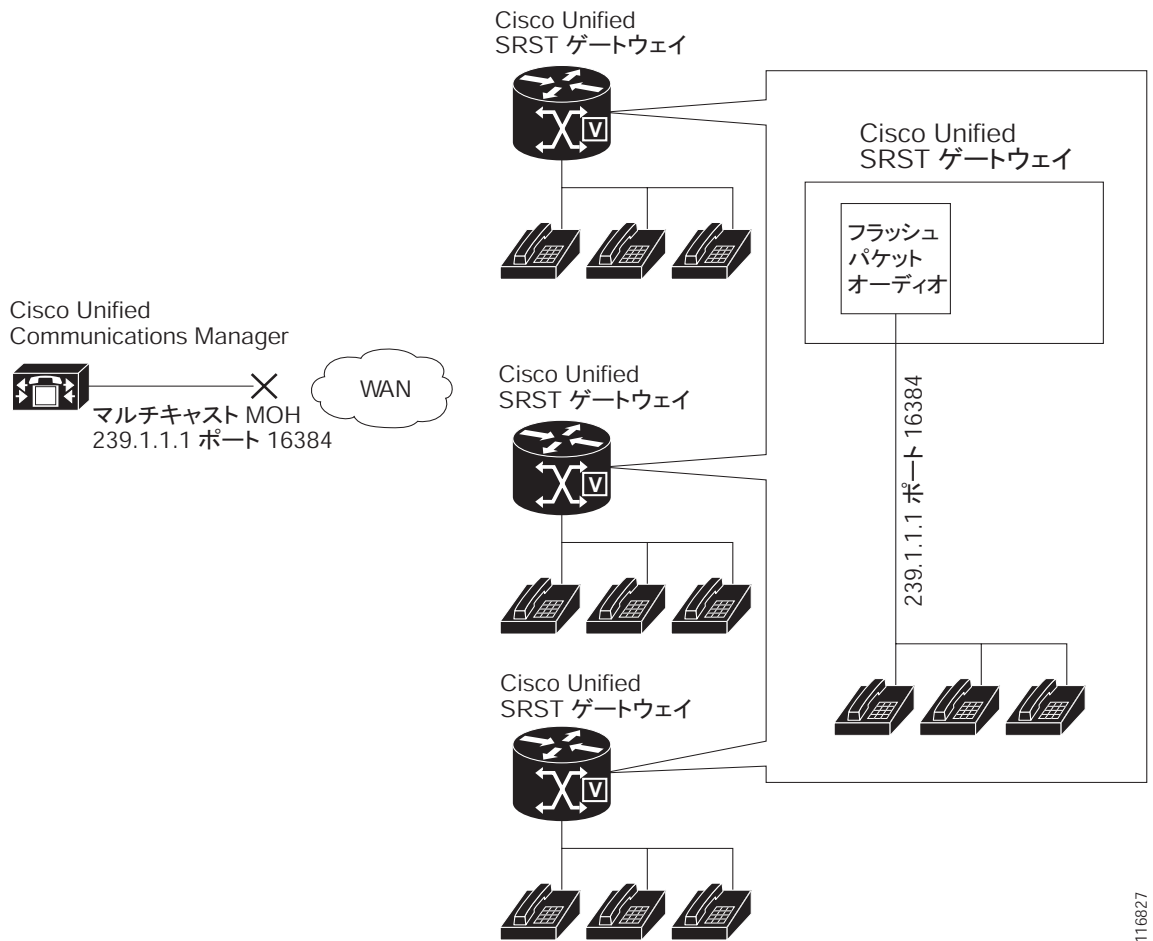
Cisco Unified SRST ルータが Cisco Unified Communications Manager の Cisco IOS 音声ゲートウェイとして使用される場合、PSTN 発信者のマルチキャスト MOH がサポートされます。この状態では、ルータの Cisco Unified SRST 機能はスタンバイモードのまま（電話機が登録されていない）、電話機およびゲートウェイのコール制御は Cisco Unified Communications Manager によって提供されます。Cisco Unified SRST ルータがフォールバックモードの場合（電話機が Cisco Unified SRST に登録されている）、この機能は適用されません。その代わりに、マルチキャストループバックインターフェイスではなく、ダイレクト内部パスを介して、PSTN 発信者に MOH が提供されます。

[図 3](#) に、すべての電話機がポート番号 16384 および IP アドレス 239.1.1.1 を介してマルチキャスト MOH を受信するように、Cisco Unified Communications Manager によって設定されている場合の設定例を示します。Cisco Unified Communications Manager はマルチキャスト MOH が WAN に到達できないように設定されており、ローカル Cisco Unified SRST ゲートウェイはフラッシュファイルからポート番号 16384 および IP アドレス 239.1.1.1 にオーディオパケットを送信するように設定されています。Cisco Unified Communications Manager および IP Phone がスプーフィングされ、Cisco Unified Communications Manager がマルチキャスト MOH を発信しているかのように動作します。



(注) セントラルサイトの電話機ユーザは、セントラルサイトからのマルチキャスト MOH を使用します。

図 3 Cisco Unified SRST フラッシュ メモリからのマルチキャスト MOH



116827

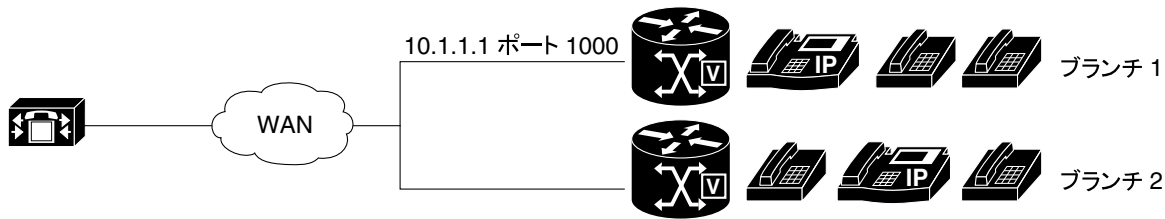
## コーデック、ポート番号、および IP アドレス

Cisco Unified SRST マルチキャスト MOH は、G.711 だけをサポートしています。図 4 に、G.711 がセントラル Cisco Unified Communications Manager および 3 つのブランチによって使用される唯一のコーデックである場合の例を示します。場合によっては、Cisco Unified Communications Manager システムが追加のコーデックを使用することもあります。たとえば、帯域幅を節約するため、Cisco Unified Communications Manager がマルチキャスト MOH に G.711 を使用し、電話の会話に G.729 を使用することがあります。

図 4 の例に示しているように、電話の会話で G.729 が使用されている場合は IP アドレス 10.1.1.1 およびポート 1000 が使用され、コールが保留にされて G.711 が使用されている場合は IP アドレス 239.1.1.1 およびポート 16384 が使用されます。

図 4 G.711 および G.729 設定での IP アドレスとポートの使用

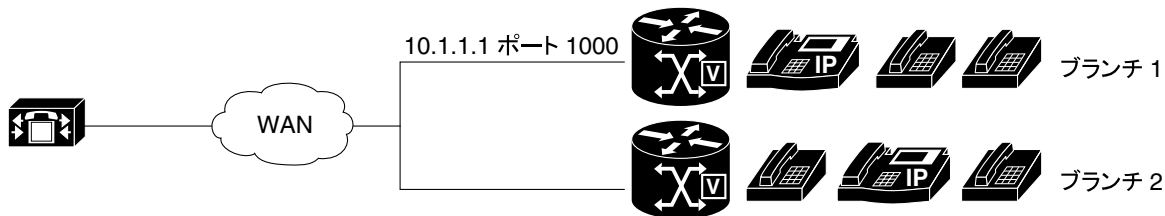
ブランチ 1 がブランチ 2 にコールを発信する (G.729 が使用される)。



ブランチ 2 がブランチ 1 を保留にする (G.711 が使用される)。



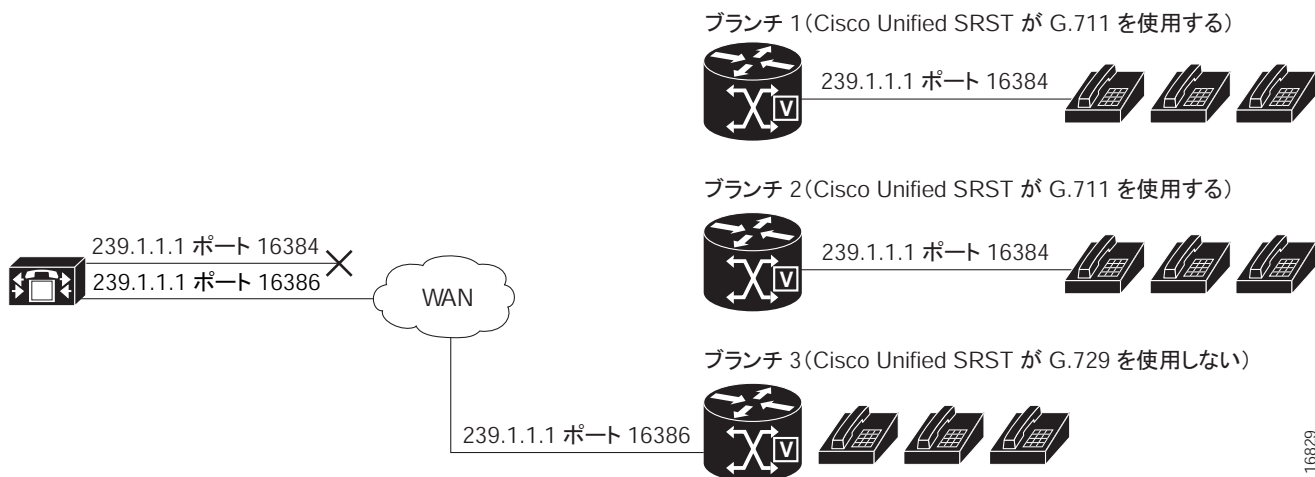
ブランチ 2 がブランチ 1 の保留を解除する (G.729 が使用される)。



116828

図 3 および図 4 では、すべてのブランチが Cisco Unified SRST マルチキャスト MOH を使用しています。図 5 では、一部のゲートウェイに Cisco Unified SRST が設定されており、他のゲートウェイには設定されていない場合を示します。セントラル サイトおよびブランチ 3 の電話機ユーザが Cisco Unified Communications Manager システム内の他の IP Phone によって保留にされた場合、Cisco Unified Communications Manager によって MOH が発信されます。ブランチ 1 およびブランチ 2 の電話機ユーザが Cisco Unified Communications Manager システム内の他の電話機ユーザによって保留にされた場合、Cisco Unified SRST ゲートウェイによって MOH が発信されます。

図 5 MOH を使用する Cisco Unified SRST IP Phone および非 Unified SRST IP Phone の MOH ソース



2 つのパスを介した MOH オーディオ パケット伝送を有効にするには、Cisco Unified Communications Manager MOH サーバに、1 つの IP アドレスと 2 つの異なるポート番号、または 1 つのポート アドレスと 2 つの異なる IP マルチキャスト アドレスを設定して、一方のブランチ セットが Cisco Unified SRST マルチキャスト MOH を使用でき、他方のブランチ セットが Cisco Unified Communications Manager マルチキャスト MOH を使用できるようにする必要があります。

## マルチキャスト MOH 伝送

図 3 のようにシステム内のすべてのブランチで Cisco Unified SRST マルチキャスト MOH がサポートされている場合は、すべてのマルチキャスト MOH オーディオ パケットが WAN に到達しないように Cisco Unified Communications Manager を設定する必要があります。図 5 のように Cisco Unified SRST を実行するブランチと実行しないブランチが混在するときには、Cisco Unified Communications Manager MOH オーディオ ファイルが WAN に到達する必要がある場合と、到達する必要のない場合があります。セントラル Cisco Unified Communications Manager からのオーディオ パケットが、WAN を通過して、Cisco Unified Communications Manager を実行するブランチに到達する必要があります。Cisco Unified SRST を実行するブランチの場合、パケットは WAN に到達する必要がありません。マルチキャスト MOH の詳細については、P.133 の「マルチキャスト MOH 用の Cisco Unified SRST の設定」を参照してください。

## Cisco Unified SRST MOH ライブ フィードのサポート

MOH ライブ フィードは、E&M または FXO ポートに接続されたオーディオ デバイスから、SRST モードの Cisco IP Phone にライブ フィード MOH ストリームを提供します。ライブ フィードの音楽はフラッシュ ファイルから読み取られるのではなく、固定のソースから取得されて MOH 再生バッファに送り続けられます。

Cisco Unified SRST には、機能拡張として **moh-live** コマンドが追加されました。**moh-live** コマンドは、E&M または FXO ポートに接続されたオーディオ デバイスから SRST モードの Cisco IP Phone に対して、ライブ フィード MOH ストリームを提供します。ライブ フィード MOH は、Cisco IP Phone に対してマルチキャストを行うこともできます。Cisco Unified SRST MOH ライブ フィードの詳細については、P.142 の「Cisco Unified SRST MOH ライブ フィード サポートの設定 (オプション)」を参照してください。

## フラッシュ ファイルからの MOH の設定

フラッシュ ファイルからの MOH マルチキャスト機能は、Cisco Unified Communications のフォールバックおよび通常の Cisco Unified Communications のサービス時に、Cisco Unified SRST ブランチ オフィス ルータのフラッシュ メモリのファイルからの MOH オーディオ フィードの継続的マルチキャストを容易にします。個々のブランチ ルータから MOH マルチキャストを行うと、セントラル オフィスからリモート ブランチに MOH オーディオを流す必要がなくなるので、WAN の帯域幅を節約できます。

フラッシュ ファイルからの MOH マルチキャスト機能は、MOH ライブ フィード機能へのバックアップ メカニズムとして動作することができます。ライブ フィード機能だけを使用するのではなく、ライブ フィードのバックアップとしてフラッシュを使用することをお勧めします。

Cisco Unified Communications Manager MOH オーディオ ファイルは、WAN に到達する必要がある場合と、到達する必要がない場合があります。セントラル Cisco Unified Communications Manager からのオーディオ パケットが、WAN を通過して、Cisco Unified Communications Manager を実行するブランチに到達する必要があります。Cisco Unified SRST を実行するブランチの場合、パケットは WAN に到達する必要がありません。



## Cisco Unified SRST ゲートウェイをマルチキャスト MOH リソースとして使用する方法

Cisco Unified SRST ゲートウェイをマルチキャスト MOH リソースとして使用するには、次の作業を行います。

- [Cisco Unified SRST マルチキャスト MOH 用の Cisco Unified Communications Manager の設定 \(P.123\)](#)
- [マルチキャスト MOH 用の Cisco Unified SRST の設定 \(P.133\)](#)
- [Cisco Unified SRST MOH ライブフィードサポートの設定 \(オプション\) \(P.142\)](#)

### Cisco Unified SRST マルチキャスト MOH 用の Cisco Unified Communications Manager の設定

次の各項では、Cisco Unified SRST マルチキャスト MOH 用の Cisco Unified Communications Manager 設定作業について説明します。

- [マルチキャストを有効にするための MOH オーディオソースの設定 \(P.124\)](#)
- [Cisco Unified Communications Manager MOH サーバでのマルチキャストの有効化およびポート番号と IP アドレスの設定 \(P.126\)](#)
- [MRG と MRGL の作成、MOH マルチキャストの有効化、およびゲートウェイの設定 \(P.129\)](#)
- [MOH サーバのリージョンの作成 \(P.130\)](#)
- [Cisco Unified Communications Manager マルチキャスト MOH の確認 \(P.132\)](#)

Cisco Unified SRST ゲートウェイをマルチキャスト MOH リソースとして使用するには、必要なブランチサイトに MOH をマルチキャストするように Cisco Unified Communications Manager を設定する必要があります。そのためには、IP アドレス、ポート番号、MOH ソース、および MOH オーディオサーバを設定する必要があります。

Cisco Unified Communications Manager を発信元とするマルチキャスト MOH が実際に WAN およびリモート電話機に到達しないように MOH ルーティングが設定されている場合でも、Cisco Unified Communications Manager は、設定されている Cisco Unified Communications Manager MOH IP ポートおよびアドレスの情報を使用して、MOH (SRST を発信元とする MOH) をリッスンするマルチキャスト IP アドレスを電話機に伝達します。

MOH サーバの設定では、オーディオソースの最大ホップ数を指定する必要があります。ホップを 1 に設定すると、Cisco Unified Communications Manager マルチキャスト MOH パケットが WAN に到達できないため、Cisco Unified Communications Manager がスプーフィングされ、Cisco Unified SRST マルチキャスト MOH パケットを Cisco Unified SRST ゲートウェイからそのコンポーネントの電話機に送信できるようになります。Cisco Unified Communications Manager マルチキャストが、Cisco Unified SRST を実行しないゲートウェイに到達する必要がある場合は、Cisco IOS の `ip multicast boundary` コマンドを使用して、マルチキャストパケットの到達先を制御します。

MOH サーバの設定後、MOH サーバをメディアリソースグループ (MRG) に追加する必要があります。その MRG をメディアリソースグループリスト (MRGL) に追加し、指定の Cisco Unified Communications Manager ブランチゲートウェイがその MRGL を使用するよう設定します。

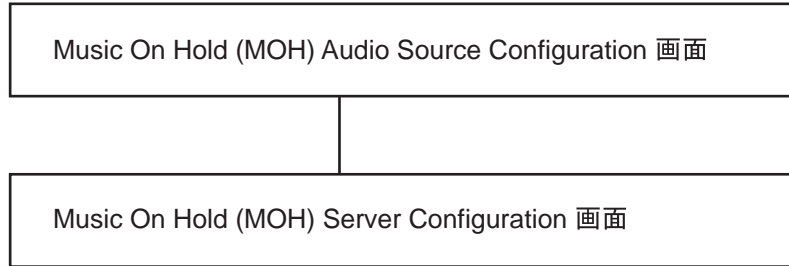
MOH サーバ、オーディオソース、MRG、MRGL、および個々のゲートウェイの設定には、5 つの Cisco Unified Communications Manager ウィンドウを使用します。図 6 に、このプロセスの概要を示します。

最後の Cisco Unified Communications Manager 設定作業では、1 つ以上のセントラルサイトおよび 1 つ以上のブランチオフィスに MOH G.711 コーデックの使用を割り当てる MOH リージョンを作成する必要があります。

リージョンは、リージョン内および既存のリージョン間のオーディオ コールとビデオ コールに使用されるコーデックを指定します。リージョンについては、『Cisco Unified Communications Manager Administration Guide』の「Region Configuration」の項を参照してください。Cisco Unified Communications Manager ドキュメント ディレクトリから **Maintain and Operate Guides** をクリックし、必要な Cisco Unified Communications Manager バージョンを選択して、ご使用のバージョンのアドミニストレーション ガイドを見つけます。

図 6 マルチキャスト MOH を設定するための Unified Communications Manager 画面

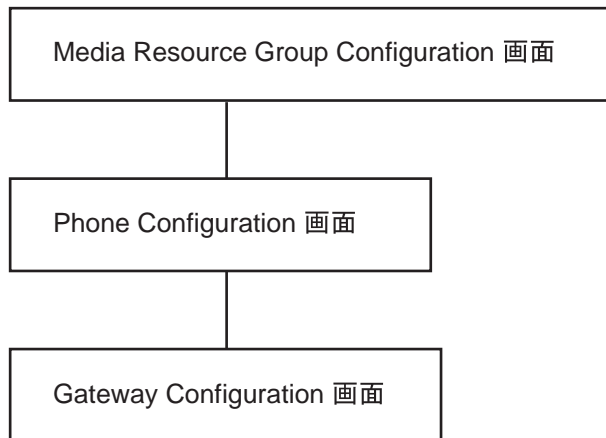
MOH サーバを設定する



サーバを追加する



MRG を追加する



146319

## マルチキャストを有効にするための MOH オーディオ ソースの設定

MOH オーディオ ソースは、Cisco Unified Communications Manager の RTP パケット送信元となるファイルです。オーディオ ファイルを作成することも、デフォルトのオーディオ ファイルを使用することもできます。Cisco Unified SRST マルチキャスト MOH では、1 つのオーディオ ソースだけを使用できます。これは、たとえば、500 のサイトのうち 1 つが Cisco Unified SRST マルチキャスト MOH を使用する場合も同様です。さらに、すべての Cisco Unified Communications Manager システムがユーザおよびネットワークの MOH に同じオーディオ ソースを使用する必要があります。これは、Cisco Unified SRST マルチキャスト MOH が 1 つのマルチキャスト IP アドレスおよびポートだけにオーディオを流すことができるためです。Cisco Unified SRST マルチキャスト MOH では、Cisco Unified Communications Manager オーディオ ソース ファイルを G.711 帯域幅用に設定する必要があります。



## ヒント

最も簡単にオーディオ ソースを作成する方法は、デフォルトのオーディオ ソースを使用することです。

デフォルトの Cisco Unified Communications Manager MOH オーディオ ソースを使用する場合でも、オーディオ ソースを作成する場合でも、Music On Hold (MOH) Audio Source Configuration ウィンドウで MOH オーディオ ソースをマルチキャスト用に設定する必要があります。

MOH Audio Source File Status セクションに、MOH オーディオ ソース ファイルが 4 つのコーデック形式用に設定されていると表示されることに注意してください。複数のコーデックを使用する場合は、オーディオ ソース ファイルがそれらのコーデックに対応していることを確認します。

MOH オーディオ ソースを作成する方法の詳細については、『*Cisco Unified Communications Manager Administration Guide*』を参照してください。[Cisco Unified Communications Manager](#) ドキュメント ディレクトリから **Maintain and Operate Guides** をクリックし、必要な Cisco Unified Communications Manager バージョンを選択します。

マルチキャストおよび継続的な再生を有効にするように MOH オーディオ ソースを設定するには、次の手順を使用します。



## (注)

次の手順では、MOH オーディオ ソース ファイルがすでに作成されていることを前提としています。

## 要約手順

1. MOH オーディオ ソースのマルチキャスト MOH を有効にします。
2. オーディオ ソースを有効にします。
3. マルチキャストを許可します。
4. すべてのマルチキャスト変更を適用します。

## 詳細手順

**ステップ 1** MOH オーディオ ソースのマルチキャスト MOH を有効にするには、**Service > Media Resources > Music On Hold Audio Source** の順に選択し、Music On Hold (MOH) Audio Source Configuration ウィンドウを表示します。

**ステップ 2** MOH Audio Sources カラムに示されている必要なオーディオ ソースをダブルクリックします。

**ステップ 3** Music On Hold (MOH) Audio Source Configuration ウィンドウで、**Allow Multicasting** をオンにします。

**ステップ 4** **Update** をクリックします。

## Cisco Unified Communications Manager MOH サーバでのマルチキャストの有効化およびポート番号と IP アドレスの設定

Music On Hold (MOH) Server Configuration ウィンドウの Multicast Audio Source Information セクションで、ベース マルチキャスト IP アドレスおよびポート番号を入力します。Cisco Unified Communications Manager マルチキャスト MOH と Cisco Unified SRST マルチキャスト MOH を使用する場合は (P.119 の「コーデック、ポート番号、および IP アドレス」および P.121 の「マルチキャスト MOH 伝送」を参照) ポート番号と IP アドレスの 2 つのセット用に設定する、ポートおよび IP アドレスの増分方式を選択する必要があります。

Increment Multicast on オプション ボタンが IP Address に設定されている場合は、MOH オーディオソースとコーデックの組み合わせごとに、異なる IP アドレスにマルチキャストされますが、同じポート番号が使用されます。このオプション ボタンが Port Number に設定されている場合は、MOH オーディオソースとコーデックの組み合わせごとに、同じ IP アドレスにマルチキャストされますが、異なる宛先ポート番号が使用されます。

表 7 に、ベース IP アドレス 239.1.1.1 およびベース ポート番号 16384 を使用した場合の IP アドレスの増分とポート番号の増分の違いを示します。また、この表では、Cisco Unified Communications Manager のオーディオソースとコーデックを IP アドレスとポート番号に対応させています。

表 7 IP アドレスの増分によるマルチキャストとポート番号の増分によるマルチキャストの違いの例

オーディオソース	コーデック	IP アドレスの増分によるマルチキャスト		ポート番号の増分によるマルチキャスト	
		宛先 IP アドレス	宛先ポート	宛先 IP アドレス	宛先ポート
1	G.711 mu-law	239.1.1.1	16384	239.1.1.1	16384
1	G.711 a-law	239.1.1.2	16384	239.1.1.1	16386
1	G.729	239.1.1.3	16384	239.1.1.1	16388
1	Wideband	239.1.1.4	16384	239.1.1.1	16390
2	G.711 mu-law	239.1.1.5	16384	239.1.1.1	16392
2	G.711 a-law	239.1.1.6	16384	239.1.1.1	16394
2	G.729	239.1.1.7	16384	239.1.1.1	16396
2	Wideband	239.1.1.8	16384	239.1.1.1	16398

増分は、コーデック使用の変更によってトリガーされます。コーデックの使用が変更されると、(選択した増分方式に応じて) 新しい IP アドレスまたはポート番号が新しいコーデック タイプに割り当てられ、その IP アドレスまたはポート番号が使用されます。元のコーデックは、その IP アドレスとポート番号を保持します。たとえば、表 7 に示しているように、ベースラインの IP アドレスおよびポート番号が G.711 mu-law コーデックに対して 239.1.1.1 および 16384 である場合、コーデックの使用が G.729 に変更されると (ポート番号の増分をトリガー) 使用される IP アドレスとポート番号が 239.1.1.1 と 16386 に変更 (増分) されます。G.711 の使用が再開されると、IP アドレスとポート番号が 239.1.1.1 と 16384 に戻ります。G.729 が再び使用されると、IP アドレスとポートが 239.1.1.1 と 16386 に戻ります (以下同様)。

Cisco Unified SRST マルチキャスト MOH に対して G.711 オーディオソースを使用する Cisco Unified Communications Manager ポート番号と IP アドレスを設定することが重要です。Cisco Unified Communications Manager マルチキャスト MOH が、Cisco Unified SRST を持たずに別のコーデック (G.729 など) を使用するゲートウェイでも使用される場合は、追加の (増分の) ポート番号または IP アドレスが Cisco Unified SRST ゲートウェイと同じオーディオソース、および必要なコーデックを使用することを確認してください。

Music On Hold (MOH) Server Configuration ウィンドウでは、MOH サーバのマルチキャスト オーディオソースも設定します。Cisco Unified SRST マルチキャスト MOH の場合、Cisco Unified Communications Manager MOH サーバは 1 つのオーディオソースだけを使用できます。オーディオソースは、オーディオソースの最大ホップ数を入力することによって選択されます。

Max Hops 設定では、オーディオソースパケットの伝送の長さを設定します。ホップ数の制限は、オーディオパケットが WAN に到達しないようにすることで Cisco Unified Communications Manager をスプーフィングし、Cisco Unified SRST が MOH をマルチキャストできるようにするための 1 つの方法です。すべてのブランチが Cisco Unified SRST を実行する場合は、小さいホップ数を使用して、オーディオソースパケットが WAN を通過しないようにします。Cisco Unified SRST を実行しないルータがシステム構成に含まれている場合は、大きいホップ数を入力して、ソースパケットが WAN を通過できるようにします。特定の IP アドレスからのリソースパケットが WAN に到達しないようにするには、`ip multicast bounder` コマンドと `access-list` コマンドを使用します。

マルチキャストを有効にしてポート番号と IP アドレスを設定するには、次の手順を使用します。

## 要約手順

1. Cisco Unified Communications Manager のマルチキャスト MOH を有効にします。
2. ベース IP アドレスとポート番号を設定します。
3. Cisco Unified Communications Manager がポート番号と IP アドレスのどちらを増分するかを選択します。
4. 最大ホップ数を入力します。
5. Cisco IOS コマンドを使用して、Cisco Unified Communications Manager の信号が WAN を通過せず、Cisco Unified SRST ゲートウェイに到達しないようにします。

## 詳細手順

**ステップ 1** Cisco Unified Communications Manager のマルチキャスト MOH を有効にします。

- a. **Service > Media Resource > Music On Hold Server** の順に選択します。
- b. Music On Hold (MOH) Server Configuration ウィンドウが表示されます。
- c. **Find** をクリックし、必要な MOH サーバをダブルクリックして、既存の MOH サーバを呼び出します。
- d. 既存の MOH サーバをアップデートする場合も、新しい MOH サーバを作成する場合も、**Enable Multicast Audio Sources on this MOH Server** をクリックします。

**ステップ 2** ベース IP アドレスとポート番号を設定します。

Music On Hold (MOH) Server Configuration ウィンドウで、Base Multicast IP Address フィールドに IP アドレスを入力し、Base Multicast Port Number フィールドにポート番号を入力します。その IP アドレスとポート番号が、必要なオーディオソースおよびコーデックを使用することを確認します。表 7 を参照してください。

**ステップ 3** Cisco Unified Communications Manager がポート番号と IP アドレスのどちらを増分するかを選択します。

ポート番号を増分して IP アドレスを変更しない場合は、Music On Hold (MOH) Server Configuration ウィンドウの Increment Multicast on フィールドで **Port Number** を選択します。IP アドレスを増分してポート番号を変更しない場合は、**IP Address** を選択します。

- すべてのブランチが Cisco Unified SRST を実行するので、MOH に G.711 を使用する場合は、増分が行われず、この選択は意味を持たないため、どちらの設定を使用してもかまいません。
- Cisco Unified SRST を実行せずに別のコーデックを使用するルータがシステム構成に含まれている場合は、増分方式を選択します。



(注) Cisco Unified SRST を実行せずに G.711 を使用するルータがブランチに含まれている場合は、個別のオーディオソース(Cisco Unified SRST を実行するルータ用に 1 つ、Cisco Unified SRST を実行しないルータ用に 1 つ)を設定してください。

#### ステップ 4 最大ホップ数を入力します。

すべてのブランチが Cisco Unified SRST を実行する場合は、Music On Hold (MOH) Server Configuration ウィンドウで、Audio Source Name フィールドの隣にある Max Hops フィールドに 1 と入力します。Cisco Unified SRST を実行しないルータがシステム構成に含まれている場合は、Max Hops フィールドに 16 と入力します。

#### ステップ 5 Cisco IOS コマンドを使用して、Cisco Unified Communications Manager の信号が WAN を通過せず、Cisco Unified SRST ゲートウェイに到達しないようにします。

すべてのブランチが Cisco Unified SRST を実行する場合は、このステップをスキップします。Cisco Unified SRST を実行せずに別のコーデックを使用するルータがシステム構成に含まれている場合は、セントラルサイトのルータでグローバル コンフィギュレーション モードから次の Cisco IOS コマンドを入力します。

**a. interface {serial | fastethernet} slot/port**

インターフェイス コンフィギュレーション モードを開始します。ここで、*slot* はスロット番号で、*port* はポート番号です。

**b. ip multicast boundary access-list-number**

管理用スコープの境界を設定します。ここで、*access-list-number* は、1 ~ 99 の数値で、この境界によって影響を受けるグループ アドレス範囲を制御するアクセス リストを表します。

**c. exit**

インターフェイス コンフィギュレーション モードを終了します。

**d. access-list access-list-number deny ip-address**

IP アドレスでフレームをフィルタリングするためのアクセス リストメカニズムを設定します。*ip-address* 引数には、WAN を通過させない MOH IP アドレスを入力します。通常、これはステップ 2 で入力したベース IP アドレスです。

次に設定例を示します。

```
Router(config)# interface serial 0/0
Router(config-if)# ip multicast boundary 1
Router(config-if)# exit
Router(config)# access-list 1 deny 239.1.1.1
```

## MRG と MRGL の作成、MOH マルチキャストの有効化、およびゲートウェイの設定

次の作業では、必要な MOH オーディオソースを保留中の IP Phone に転送できる MOH サーバを使用するように、個々のゲートウェイを設定する必要があります。これは、メディアリソースグループ (MRG) を作成することによって行います。MRG には、メディアリソース (MOH サーバなど) が含まれます。その後、MRG をメディアリソースグループリスト (MRGL) に追加し、MRGL を電話機およびゲートウェイの設定に追加します。

MRG は、Media Resource Group Configuration ウィンドウで作成します。MRGL は、Media Resource Group List Configuration ウィンドウで作成します。電話機は、Phone Configuration ウィンドウで設定します。ゲートウェイは、Gateway Configuration ウィンドウで設定します。



(注)

H.323 ゲートウェイの Gateway Configuration ウィンドウは、MGCP ゲートウェイのウィンドウに似ています。

MRGL をデバイスプール設定に追加することにより、MRGL をゲートウェイまたは IP Phone の設定に追加します。デバイスプールの詳細については、『Cisco Unified Communications Manager Administration Guide』を参照してください。[Cisco Unified Communications Manager](#) ドキュメントディレクトリから **Maintain and Operate Guides** をクリックし、必要な Cisco Unified Communications Manager バージョンを選択します。

MRG と MRGL を作成し、MOH マルチキャストを有効にし、ゲートウェイを設定するには、次の手順を使用します。

### 要約手順

1. マルチキャスト MOH メディアリソースを含む MRG を作成します。
2. 新しく作成した MRG を含む MRGL を作成します。
3. 必要な IP Phone に MRGL を追加します。
4. 必要なゲートウェイに MRGL を追加します。

### 詳細手順

**ステップ 1** マルチキャスト MOH メディアリソースを含む MRG を作成します。

- a. **Service > Media Resource > Media Resource Group** の順に選択します。
- b. ウィンドウの右上隅で、**Add a New Media Resource Group** リンクをクリックします。Media Resource Group Configuration ウィンドウが表示されます。
- c. Media Resource Group Name フィールドに値を入力します。
- d. Description フィールドに値を入力します。
- e. Available Media Resources ペインからメディアリソースを選択します。

このペインには、MRG に対して選択可能なメディアリソースが表示されます。このメディアリソースには、次のメディアリソースタイプが含まれます。

- コンファレンスブリッジ (CFB)
- メディアターミネーションポイント (MTP)
- Music On Hold サーバ (MOH)
- トランスコーダ (XCODE)
- アナウンサー (ANN)

マルチキャスト用に設定されている Music On Hold サーバには (MOH) [Multicast] というラベルが付いています。

- f. 下向き矢印をクリックして、選択したメディア リソースを Selected Media Resources ペインに移動します。
- g. **Insert** をクリックします。

## ステップ 2 新しく作成した MRG を含む MRGL を作成します。

- a. **Service > Media Resource > Media Resource Group List** の順に選択します。
- b. ウィンドウの右上隅で、**Add a New Media Resource Group List** リンクをクリックします。Media Resource Group List Configuration ウィンドウが表示されます。
- c. Media Resource Group List Name フィールドに値を入力します。
- d. Available Media Resource Groups ペインで、新しく作成した MRG を選択します。
- e. 下向き矢印をクリックして、その MRG を Selected Media Resource Groups ペインに追加します。メディア リソース グループを追加すると、その名前が Selected Media Resource Groups ペインに移動します。
- f. **Insert** をクリックします。

## ステップ 3 必要な IP Phone に MRGL を追加します。

- a. **Device > Phone** の順に選択して、Find and List Phones ウィンドウを表示します。
- b. **Find** をクリックして、電話機のリストを表示します。
- c. アップデートする電話機のデバイス名をダブルクリックします。
- d. ドロップダウン メニューから必要な MRGL を選択することで、Media Resource Group List フィールドにデータを入力します。
- e. **Update** をクリックします。

## ステップ 4 必要なゲートウェイに MRGL を追加します。

- a. **Device > Gateway** の順に選択して、Find and List Gateways ウィンドウを表示します。
- b. **Find** をクリックして、ゲートウェイのリストを表示します。
- c. アップデートするゲートウェイのデバイス名をダブルクリックします。
- d. ゲートウェイが H.323 の場合は、ドロップダウン メニューから必要な MRGL を選択することで、Media Resource Group List フィールドにデータを入力します。
- e. **Update** をクリックします。

## MOH サーバのリージョンの作成

MOH サーバが Cisco Unified SRST ゲートウェイに G.711 を使用することを保証するには、MOH サーバに個別のリージョンを作成する必要があります。コーデックの詳細については、[P.119 の「コーデック、ポート番号、および IP アドレス」](#)を参照してください。リージョンについては、『*Cisco Unified Communications Manager Administration Guide*』を参照してください。[Cisco Unified Communications Manager ドキュメント ディレクトリから Maintain and Operate Guides](#) をクリックし、必要な Cisco Unified Communications Manager バージョンを選択します。



Region Configuration ウィンドウを設定します。Cisco Unified Communications Manager システムが G.711 だけを使用する場合は、MOH リージョンでセントラル サイトとその構成ブランチのすべてを G.711 に設定する必要があります。Cisco Unified Communications Manager システムに、Cisco Unified SRST マルチキャスト MOH を実行するブランチと実行しないブランチが混在し、Cisco Unified SRST を実行しないブランチが Cisco Unified Communications Manager マルチキャスト MOH に別のコーデックを必要とする場合は、それらを適宜設定する必要があります。

「MOH Sever」リージョンが G.711 コーデックと G.729 コーデックを使用するように設定されている場合の Region Configuration ウィンドウは、たとえば次のように表示されます。

- ブランチ 1 には G.711 が使用されます。これは、ブランチ 1 のゲートウェイが、G.711 を必要とする Cisco Unified SRST マルチキャスト MOH を実行するように設定されているためです。
- ブランチ 2 には G.729 が使用されます。これは、ブランチ 2 のゲートウェイが Cisco Unified SRST を実行せず、G.729 を使用するポートおよび IP アドレスを使用するように設定されているためです。
- セントラル サイトおよび MOH Sever リージョンには G.711 が設定されます。

MOH サーバのリージョンを作成するには、次の手順を使用します。

## 要約手順

1. MOH サーバのリージョンを作成します。
2. 別のコーデックの必要性に応じて、他のリージョンを作成します。

## 詳細手順

---

### ステップ 1 MOH サーバのリージョンを作成します。

- a. **System > Region** の順に選択します。
- b. ウィンドウの右上隅で、**Add a New Region** をクリックします。Region Configuration ウィンドウが表示されます。
- c. Region Name フィールドに、新しいリージョンに割り当てる名前を入力し、**Insert** をクリックします。
- d. 他のリージョンが作成済みである場合は、リージョンのリストが表示されます。ドロップダウン リスト ボックスを使用して、新しいリージョンと既存のリージョンの間のコールに使用するオーディオコーデックを選択します。オーディオコーデックにより、圧縮のタイプ、およびコールに割り当てられる最大帯域幅が決まります。
- e. 他のリージョンに加えて、新しく作成したリージョンがリストに表示されます。ドロップダウン ボックスを使用して、新しいリージョン内で使用するコーデックを選択します。
- f. **Update** をクリックします。

### ステップ 2 別のコーデックの必要性に応じて、他のリージョンを作成します。

---

## Cisco Unified Communications Manager マルチキャスト MOH の確認

Cisco Unified SRST マルチキャスト MOH が機能するためには、Cisco Unified Communications Manager マルチキャスト MOH 設定が正しく実行される必要があります。マルチキャストが有効になっている WAN を使用する設定と、マルチキャストが無効になっている WAN を使用する設定では、Cisco Unified Communications Manager マルチキャスト MOH を確認する方法が異なります。

Cisco Unified Communications Manager マルチキャスト MOH がユニキャストではなくマルチキャストで提供されることを確認する必要があります。デフォルトではユニキャスト MOH が有効になっているため、マルチキャスト MOH が動作していない場合でも動作しているという誤った判断をしやすくなります。

### 要約手順

1. リモート ゲートウェイで Cisco Unified Communications Manager システムのマルチキャスト MOH が聞こえることを確認します。
2. Cisco Unified Communications Manager システムの MOH がユニキャストではなくマルチキャストであることを確認します。

### 詳細手順

- 
- ステップ 1** リモート ゲートウェイで Cisco Unified Communications Manager システムのマルチキャスト MOH が聞こえることを確認します。
- a. WAN でマルチキャストが有効になっている場合は、Cisco Unified Communications Manager MOH サーバに設定されているホップ数が、オーディオ パケットがリモート サイトに到達するために十分であることを確認します (P.126 の「Cisco Unified Communications Manager MOH サーバでのマルチキャストの有効化およびポート番号と IP アドレスの設定」を参照)。その後、リモート ゲートウェイ上の IP Phone にコールを発信し、そのコールを保留にして、MOH が聞こえることを確認します。
  - b. WAN でマルチキャストが無効になっている場合は、Cisco Unified Communications Manager MOH サーバと同じサブネットに IP Phone を配置し、MOH が聞こえることを確認します。IP Phone と MOH サーバが同じサブネット上にあるため、ネットワーク上のマルチキャストルーティング機能は不要です。
- ステップ 2** Cisco Unified Communications Manager システムの MOH がユニキャストではなくマルチキャストであることを確認します。
- a. Microsoft Windows で、**Start > Programs > Administrative Tools > Performance** の順に選択します。
  - b. Performance ウィンドウで、右ペインの最上部にある +( プラス ) のアイコンをクリックします。
  - c. Add Counters ウィンドウで、Cisco MOH Device を選択します。
  - d. Performance ウィンドウで、MOHMulticastResourceActive カウンタと MOHUnicastResourceActive カウンタを監視して、マルチキャスト アクティビティを確認できます。
-

## マルチキャスト MOH 用の Cisco Unified SRST の設定



(注) この項の手順は、Microsoft Windows を使用して Cisco Unified Communications Manager バージョン 4.3 以下を実行している場合にだけ使用してください。Linux オペレーティングシステム上の Cisco Unified Communications Manager 5.0 以降のバージョンで MOH アクティビティを監視するには、RTMT (Real-Time Monitoring Tool) を使用してください。RTMT の詳細については、『*Cisco Unified Communications Serviceability System Guide, Release 4.0(1)*』を参照してください。

Cisco Unified SRST をマルチキャスト MOH 用に設定するには、次の手順を使用します。

- [前提条件 \( P.133 \)](#)
- [Cisco Unified SRST ゲートウェイでのマルチキャスト MOH の有効化 \( P.134 \)](#)
- [基本的な Cisco Unified SRST マルチキャスト MOH ストリーミングの確認 \( P.136 \)](#)
- [PSTN への Cisco Unified SRST MOH の確認 \( P.138 \)](#)
- [IP Phone に対する Cisco Unified SRST マルチキャスト MOH の確認 \( P.141 \)](#)
- [トラブルシューティングに関するヒント \( P.141 \)](#)

### 前提条件

- Cisco Unified SRST ゲートウェイが Cisco IOS Release 12.2(15)ZJ2 以降のリリースを実行する必要があります。
- 各 Cisco Unified SRST ゲートウェイのフラッシュメモリに MOH オーディオファイルが格納されている必要があります。MOH ファイルは、.wav ファイル形式でも .au ファイル形式でもかまいませんが、a-law や mu-law データ形式などの 8 ビット 8-kHz データが含まれている必要があります。<http://www.cisco.com/cgi-bin/tablebuild.pl/ip-key> からダウンロードできるプログラム .zip ファイルに、実動可能な既知の MOH オーディオファイル ( music-on-hold.au ) が含まれています。または、<http://www.cisco.com/cgi-bin/tablebuild.pl/ip-iostsp> から music-on-hold.au ファイルをダウンロードして、Cisco Unified SRST ルータのフラッシュメモリにコピーできます。
- Windows 上で動作する Cisco Unified Communications Manager 4.3 以前のバージョンでは、MOH ファイルの 1 つ ( SampleAudioSource.ULAW.wav など ) を Cisco Unified Communications Manager の C:\Program Files\Cisco\MOH からコピーすることにより、MOH ファイルをダウンロードします。



(注) コピー プロセス中、各ルータのフラッシュに 4 つのファイルが自動的に追加されます。それらのファイルの 1 つが、拡張子 .ULAW.wav によって示される mu-law 形式を使用する必要があります。

- ループバック インターフェイスを設定し、その IP アドレスを Cisco Unified SRST マルチキャスト MOH 設定に含める必要があります。この設定により、ゲートウェイ上の POTS ポートでマルチキャスト MOH が聞こえるようになります。ループバック インターフェイスは、H.323 にも MGCP にもバインドする必要はありません。
- 少なくとも 1 つの ephone および Directory Number ( DN; 電話番号 ) を設定します。これは、ゲートウェイが Cisco Unified SRST に使用されない場合も同様です。ehpone と電話番号が設定されていないと、Cisco Unified SRST マルチキャスト MOH ストリーミングが開始されません。

## Cisco Unified SRST ゲートウェイでのマルチキャスト MOH の有効化

Cisco Unified SRST ゲートウェイに対するマルチキャスト MOH ルーティング設定は不要です。これは、各 Cisco Unified SRST ゲートウェイが、ネットワークからマルチキャスト MOH パケットを流すアプリケーションを実行するホストとして動作するように設定されるためです。`multicast moh` コマンドは、Cisco Unified Communications Manager マルチキャスト MOH アドレスとポート番号を宣言し、Cisco Unified SRST ゲートウェイがフラッシュメモリから最大 4 つの IP アドレスに MOH をルーティングできるようにします。ルート IP アドレスが設定されていない場合、フラッシュ MOH は、Cisco Unified SRST の `ip source-address` コマンドに設定されている IP アドレスを介して送信されます。

### 要約手順

1. `ccm-manager music-on-hold`
2. `interface loopback number`
3. `ip address ip-address mask`
4. `exit`
5. `interface fastethernet slot/port`
6. `ip address ip-address mask`
7. `exit`
8. `call-manager-fallback`
9. `ip source-address ip-address [port port]`
10. `max-ephones max-phones`
11. `max-dn max-directory-number`
12. `moh filename`
13. `multicasting-enabled`
14. `multicast moh multicast-address port port [route ip-address-list]`
15. `exit`

### 詳細手順

	コマンドまたはアクション	目的
ステップ 1	<code>ccm-manager music-on-hold</code>  例: Router(config)# <code>ccm-manager music-on-hold</code>	音声ゲートウェイでマルチキャスト MOH 機能を有効にします。
ステップ 2	<code>interface loopback number</code>  例: Router(config)# <code>interface loopback 1</code>	インターフェイス タイプを設定し、インターフェイス コンフィギュレーション モードを開始します。  • <code>number</code> : ループバック インターフェイスの番号。範囲は 0 ~ 2147483647 です。
ステップ 3	<code>ip address ip-address mask</code>  例: Router(config-if)# <code>ip address 10.1.1.1 255.255.255.255</code>	インターフェイスのプライマリ IP アドレスを設定します。  • <code>ip-address</code> : IP アドレス。 • <code>mask</code> : 関連する IP サブネットのマスク。

	コマンドまたはアクション	目的
ステップ 4	<b>exit</b>  例: Router(config-if)# exit	インターフェイス コンフィギュレーション モードを終了します。
ステップ 5	<b>interface fastethernet slot/port</b>  例: Router(config)# interface fastethernet 0/0	( <b>multicast moh</b> コマンドで <b>route</b> キーワードが使用されない場合はオプション。ステップ 9 およびステップ 13 を参照してください ) インターフェイス タイプを設定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 6	<b>ip address ip-address mask</b>  例: Router(config-if)# ip-address 172.21.51.143 255.255.255.192	( <b>multicast moh</b> コマンドで <b>route</b> キーワードが使用されない場合はオプション。ステップ 9 およびステップ 13 を参照してください ) インターフェイスのプライマリ IP アドレスを設定します。
ステップ 7	<b>exit</b>  例: Router(config-if)# exit	( <b>multicast moh</b> コマンドで <b>route</b> キーワードが使用されない場合はオプション。ステップ 9 およびステップ 13 を参照してください ) インターフェイス コンフィギュレーション モードを終了します。
ステップ 8	<b>call-manager-fallback</b>  例: Router(config)# call-manager-fallback	call-manager-fallback コンフィギュレーション モードを開始します。
ステップ 9	<b>ip source-address ip-address [port port]</b>  例: Router(config-cm-fallback)# ip source-address 172.21.51.143 port 2000	( <b>multicast moh</b> コマンドで <b>route</b> キーワードが使用されない場合はオプション。ステップ 13 を参照してください ) 指定した IP アドレスおよびポートを介してルータが Cisco Unified IP Phone からメッセージを受信できるようにします。  <ul style="list-style-type: none"> <li><b>ip-address</b> : 既存のルータの IP アドレス。通常、ルータのイーサネット ポートのアドレスの 1 つです。</li> <li><b>port port</b> : ( オプション ) Cisco Unified IP Phone からメッセージを受信するためにゲートウェイルータが接続されるポート。ポート番号の範囲は 2000 ~ 9999 です。デフォルトのポート番号は 2000 です。</li> </ul>
ステップ 10	<b>max-ephones max-phones</b>  例: Router(config-cm-fallback)# max-ephones 1	ルータがサポート可能な Cisco Unified IP Phone の最大数を設定します。  <ul style="list-style-type: none"> <li><b>max-phones</b> : ルータでサポートされる Cisco IP Phone の最大数。最大数は、プラットフォームによって異なります。デフォルトは 0 です。</li> </ul>
ステップ 11	<b>max-dn max-directory-number</b>  例: Router(config-cm-fallback)# max-dn 1	ルータがサポート可能な仮想音声ポートの最大数を設定します。  <ul style="list-style-type: none"> <li><b>max-directory-number</b> : ルータでサポートされる電話番号または仮想音声ポートの最大数。最大数は、プラットフォームによって異なります。デフォルトは 0 です。</li> </ul>
ステップ 12	<b>moh filename</b>  例: Router(config-cm-falback)# moh music-on-hold.au	MOH ファイルの使用を有効にします。  <ul style="list-style-type: none"> <li><b>filename</b> : 音楽ファイルのファイル名。音楽ファイルは、フラッシュメモリに常駐する必要があります。</li> </ul>

	コマンドまたはアクション	目的
ステップ 13	<code>multicasting-enabled</code>	Cisco Unified Communications Manager Administration GUI の Phone Configuration ページにある User Hold MOH Audio Source フィールドで、マルチキャスト対応の MOH オーディオソースを選択します。
ステップ 14	<pre>multicast moh multicast-address port port [route ip-address-list]</pre> <p>例:</p> <pre>Router(config-cm-fallback)# multicast moh 239.1.1.1 port 16386 route 239.1.1.2 239.1.1.3 239.1.1.4 239.1.1.5</pre>	<p>ブランチ オフィスのフラッシュ MOH ファイルからブランチ オフィスの IP Phone への MOH マルチキャストを有効にします。</p> <ul style="list-style-type: none"> <li><code>multicast-address</code> および <code>port port</code> : マルチキャストされる MOH パケットの IP アドレスおよびポート番号を宣言します。このマルチキャスト IP アドレスおよびポートは、Cisco Unified Communications Manager がマルチキャスト MOH に使用するように設定されている IP アドレスおよびポート番号と一致する必要があります。MOH に別のコーデックを使用する場合、これらはベース IP アドレスおよびポートではなく、増分された IP アドレスまたはポート番号となることがあります。P.124 の「<a href="#">マルチキャストを有効にするための MOH オーディオソースの設定</a>」を参照してください。Cisco Unified Communications Manager に複数のオーディオソースが設定されている場合は、オーディオソースの正しい IP アドレスおよびポート番号を使用していることを確認してください。</li> <li><code>route ip-address-list</code> : (オプション) フラッシュ MOH パケットの送信元となる IP アドレスを宣言します。最大 4 つの IP アドレス エントリを指定できます。<code>route</code> キーワードが設定されていない場合、Cisco Unified SRST システムは、Cisco Unified SRST に設定されている <code>ip source-address</code> コマンドの値を使用します。</li> </ul>
ステップ 15	<pre>exit</pre> <p>例:</p> <pre>Router(config-cm-fallback)# exit</pre>	call-manager-fallback コンフィギュレーション モードを終了します。

## 基本的な Cisco Unified SRST マルチキャスト MOH ストリーミングの確認

マルチキャスト MOH パケットが `multicast moh` コマンドで設定されていることを確認するには、次の手順を使用します。

### 要約手順

1. `debug ephone moh`
2. `show interfaces fastethernet`
3. `show ephone summary`

## 詳細手順

### ステップ 1 debug ephone moh

このコマンドは、MOH のデバッグを設定します。このコマンドを使用して、Cisco Unified SRST ゲートウェイがループバック 0 およびファスト イーサネット 0/0 から MOH をマルチキャストしていることを表示できます。

```
Router# debug ephone moh
!
MOH route If FastEthernet0/0 ETHERNET 172.21.51.143 via ARP
MOH route If Loopback0 46 172.21.51.98 via 172.21.51.98
!
```

### ステップ 2 show interfaces fastethernet

このコマンドを使用して、インターフェイス出力レートが 1 つの G.711 ストリームと一致することを確認します。一致する場合、**show interfaces fastethernet** の出力は、50 パケット / 秒および 80 kbps 以上と表示されます。

```
Router# show interfaces fastethernet 0/0
!
30 second output rate 86000 bits/sec, 50 packets/sec
!
```

### ステップ 3 show ephone summary

このコマンドを使用して、Cisco IOS ソフトウェアが MOH オーディオ ファイルを正常に読み取ることができたことを確認します。

```
Router# show ephone summary
!
File music-on-hold.au type AU Media_Payload_G.711Ulaw64k 160 bytes
!
```

## トラブルシューティングに関するヒント

**show ephone summary** の出力では、ファイル タイプが .au または .wav として表示される必要があります。INVALID と表示される場合は、エラーが存在します。

```
Router# show ephone summary
!
File music-on-hold.au type INVALID Media_Payload_G.711Ulaw64k 160 bytes651-
!
```

無効な出力は、Cisco Unified SRST 設定コマンドの入力順序が原因で発生する可能性があります。**no call-manager-fallback** コマンドを使用して、マルチキャスト MOH コマンドを再入力してください。また、リブートするとエラーがクリアされることがあります。

## PSTN への Cisco Unified SRST MOH の確認

Cisco Unified Communications Manager の MOH 制御 (WAN リンクがアップしている) を確認し、マルチキャスト MOH パケットが Public Switched Telephone Network (PSTN; 公衆電話交換網) を介して送信されることを確認するには、次の手順を使用します。



(注) この機能は、Cisco Unified SRST ルータがフォールバック モードの場合は適用されません。

### 要約手順

1. IP Phone 発信者がコールを保留にした場合に、PSTN 発信者に MOH が聞こえることを確認します。
2. `show ccm-manager music-on-hold`
3. `debug h245 asn`
4. `show call active voice`

### 詳細手順

**ステップ 1** IP Phone 発信者がコールを保留にした場合に、PSTN 発信者に MOH が聞こえることを確認します。

Cisco Unified SRST ゲートウェイの IP Phone を使用して PSTN 電話機にコールを発信し、PSTN 発信者を保留にします。PSTN 発信者に MOH が聞こえる必要があります。

**ステップ 2** `show ccm-manager music-on-hold`

Windows と Cisco Unified Communications Manager 4.3 以前のバージョンを使用している場合は、このコマンドを使用して MOH がマルチキャストされることを確認します。`show ccm-manager music-on-hold` コマンドは、保留にされている PSTN 接続の情報だけを表示することに注意してください。保留にされている IP Phone へのマルチキャスト ストリームに関する情報は表示されません。次に、`show ccm-manager music-on-hold` コマンドの出力例を示します。

```
Router# show ccm-manager music-on-hold

Current active multicast sessions : 1
Multicast      RTP port  Packets      Call   Codec   Incoming
Address        number    in/out       id     interface
=====
239.1.1.1      16384    326/326     42    G.711ulaw  Lo0
```

PSTN 発信者に MOH が聞こえ、`show ccm-manager music-on-hold` コマンドでアクティブなマルチキャスト ストリームが表示されない場合、MOH はユニキャストです。これを確認するには、[P.132 の「Cisco Unified Communications Manager マルチキャスト MOH の確認」](#)の説明に従って、MOH パフォーマンスカウンタをチェックします。

**ステップ 3** `debug h245 asn`

H.323 が使用されており、`show ccm-manager music-on-hold` コマンド出力にマルチキャスト アドレスが表示されない場合は、このコマンドを使用して、Cisco Unified Communications Manager と Cisco Unified SRST ゲートウェイの間の H.323 ハンドシェイクを確認します。PSTN 発信者が保留にされた場合、Cisco Unified Communications Manager は H.245 `closeLogicalChannel` を送信し、その後 `openLogicalChannel` を送信します。Cisco Unified Communications Manager から Cisco Unified SRST



ゲートウェイへの最後の openLogicalChannelAck に、予期していたマルチキャスト IP アドレスおよびポート番号が含まれていることを確認します。次の例では、IP アドレスが EF010101 (239.1.1.1) で、ポート番号が 16384 です。

```
Router# debug h245 asn

*Mar 1 04:20:19.227: H245 MSC INCOMING PDU ::=

value MultimediaSystemControlMessage ::= response : openLogicalChannelAck :
{
  forwardLogicalChannelNumber 6
  forwardMultiplexAckParameters h2250LogicalChannelAckParameters :
  {
    sessionID 1
    mediaChannel unicastAddress : ipAddress :
    {
      network 'EF010101'H
      tsapIdentifier 16384
    }
    mediaControlChannel unicastAddress : ipAddress :
    {
      network 'EF010101'H
      tsapIdentifier 16385
    }
  }
}
```

#### ステップ 4 show call active voice

このコマンドを `debug h245 asn` コマンドとともに使用して、Cisco Unified Communications Manager と Cisco Unified SRST ゲートウェイの間の H.323 ハンドシェイクをさらに確認します。

```
Router# show call active voice | include RemoteMedia

RemoteMediaIPAddress=239.1.1.1
RemoteMediaPort=16384
```

表示される IP アドレスおよびポート番号が、`debug h245 asn` コマンドで表示される IP アドレスおよびポート番号と一致する必要があります。RemoteMediaIPAddress フィールドに 0.0.0.0 と表示される場合は、警告 CSCdz00697 が発生した可能性があります。詳細については、Cisco [Bug ToolKit](#) および [P.117](#) の「Cisco Unified SRST ゲートウェイをマルチキャスト MOH リソースとして使用するための制限事項」を参照してください。

#### トラブルシューティングに関するヒント

- PSTN 発信者に MOH ではなく Tone On Hold (TOH; 保留時のトーン) が聞こえる場合は、次の 2 つの問題が考えられます。
  - Cisco Unified Communications Manager が MOH のアクティブ化に失敗し、フォールバックとして TOH を使用しています。これを確認するには、[P.132](#) の「Cisco Unified Communications Manager マルチキャスト MOH の確認」を参照してください。
  - Cisco Unified Communications Manager で、適切な MOH リソースが使用できません。show ccm-manager music-on-hold コマンドを使用して、MOH リソースが問題であるかどうかを確認します。



(注) `show ccm-manager music-on-hold` コマンドは、保留にされている PSTN 接続の情報だけを表示します。保留にされている IP Phone へのマルチキャスト ストリームに関する情報は表示されません。

```
Router# show ccm-manager music-on-hold

Current active multicast sessions : 1
Multicast      RTP port   Packets      Call   Codec      Incoming
Address        number     in/out       id     id         Interface
=====
239.1.1.1      16384     326/326     42    G.711ulaw  Lo0*
```

MOH ストリームが表示されない(つまり、カラムの下にデータ行がない)場合は、Cisco Unified Communications Manager が Cisco Unified SRST ゲートウェイに MOH を提供するように正しく設定されていません。設定エラーとしては、必要なコーデックが Cisco Unified Communications Manager で有効になっていない(サービスパラメータを確認してください)、ゲートウェイに MRGL が割り当てられていない、割り当てられている場合はゲートウェイのリソースが十分でない、などが考えられます。Cisco Intrusion Detection System (Cisco IDS; シスコ侵入検知システム) イベントビューアで、エラーメッセージを確認してください。

- 保留にされている POTS 発信者に音が聞こえない場合は、Cisco Unified Communications Manager が Cisco Unified SRST ゲートウェイとのマルチキャスト MOH ハンドシェイクを正常に完了していますが、ゲートウェイがローカルで生成されたマルチキャスト RTP ストリームのピックアップに失敗しています。

`show ccm-manager music-on-hold` コマンドを使用して調査します。

```
Router# show ccm-manager music-on-hold

Current active multicast sessions : 1
Multicast      RTP port   Packets      Call   Codec      Incoming
Address        number     in/out       id     id         Interface
=====
239.1.1.1      16384     326/326     42    G.711ulaw  Lo0 *
```

- MOH ストリームが表示されない場合は、Cisco Unified Communications Manager が Cisco Unified SRST ゲートウェイに MOH を提供するように正しく設定されていません。一般的なエラーとしては、Cisco Unified Communications Manager に適切な MOH リソースが設定されていないことがあります。設定エラーとしては、必要なコーデックが Cisco Unified Communications Manager で有効になっていない(サービスパラメータを確認してください)、ゲートウェイに MRGL が割り当てられていない、割り当てられている場合はゲートウェイのリソースが十分でない、などが考えられます。IDS イベントビューアでエラーメッセージを確認してください。
- `show ccm-manager music-on-hold` コマンド出力で表示されるマルチキャストアドレスおよび RTP ポート番号が、`moh multicast` コマンド設定の `multicast-address` 引数および `port` 引数と一致することを確認します。
- Packets in/out フィールドに、増分しているカウントが表示されることを確認します。`show ccm-manager music-on-hold` コマンドを繰り返し入力して、Packets in/out カウンタが増分していることを確認します。
- Codec フィールドが、Cisco Unified SRST ゲートウェイのフラッシュメモリに格納されているオーディオファイルのコーデックタイプと一致することを確認します。`show ccm-manager music-on-hold` コマンド出力に G.711 mu-law または G.711 a-law 以外のコーデック値が表示される場合は、Cisco Unified Communications Manager のリージョンでコーデック設定が正しいかどうかを確認します。P.130 の「MOH サーバのリージョンの作成」を参照してください。

- Incoming Interface フィールドには、Cisco Unified SRST ゲートウェイがマルチキャスト MOH パケットを受信する場所が表示されます。インターフェイスが表示される必要があります。このインターフェイスは、**multicast moh** コマンドに含まれるいずれかのインターフェイス、または **ip source-address** コマンドで設定されているデフォルトの IP ソース アドレスである必要があります。

詳細については、P.134 の「Cisco Unified SRST ゲートウェイでのマルチキャスト MOH の有効化」のステップ 9 を参照してください。

## IP Phone に対する Cisco Unified SRST マルチキャスト MOH の確認

Cisco Unified Communications Manager が、Cisco Unified SRST マルチキャスト MOH を正しく受信するように IP Phone にシグナリングしていることを確認するには、次の手順を実行します。

### 要約手順

1. IP Phone 発信者がコールを保留にした場合に IP Phone 発信者に MOH が聞こえることを確認します。
2. MOHMulticastResourceActive カウンタと MOHUnicastResourceActive カウンタを確認します。

### 詳細手順

---

**ステップ 1** IP Phone 発信者がコールを保留にした場合に IP Phone 発信者に MOH が聞こえることを確認します。

IP Phone を使用して別の IP Phone にコールを発信し、その IP Phone 発信者を保留にします。その発信者に MOH が聞こえる必要があります。

**ステップ 2** MOHMulticastResourceActive カウンタと MOHUnicastResourceActive カウンタを確認します。

Performance ウィンドウを使用して、Cisco MOH Device パフォーマンス オブジェクトの下にある MOHMulticastResourceActive カウンタと MOHUnicastResourceActive カウンタを確認します。

P.132 の「Cisco Unified Communications Manager マルチキャスト MOH の確認」のステップ 2 を参照してください。Cisco Unified SRST マルチキャスト MOH が機能している場合は、マルチキャスト カウンタが増分します。

---

## トラブルシューティングに関するヒント

MOH が聞こえず、Cisco Unified SRST MOH シグナリングがマルチキャストしていない場合は、IP Phone の背面にある PC ポートにスニファを接続します。IP Phone と Cisco Unified SRST ゲートウェイが同じサブネットに接続されている場合は、いつでもマルチキャスト RTP パケットが検出される必要があります。これは、IP Phone が保留にされていない場合も同様です。IP Phone と Cisco Unified SRST ゲートウェイが同じサブネットに接続されていない場合は、IP Phone が保留にされ、最も近いルータに Internet Group Management Protocol (IGMP; インターネット グループ管理プロトコル) Join を送信するときに限り、マルチキャスト RTP パケットが検出されます。

## Cisco Unified SRST MOH ライブ フィード サポートの設定 (オプション)

次の各項では、Cisco Unified SRST MOH ライブ フィードの設定作業について説明します。

- [前提条件 \(P.143\)](#)
- [制約事項 \(P.143\)](#)
- [Cisco Unified SRST ゲートウェイ上の音声ポートの設定 \(P.143\)](#)
- [Cisco Unified SRST ゲートウェイ上の電話番号の設定 \(P.144\)](#)
- [MOH フィードの確立 \(P.145\)](#)
- [Cisco Unified SRST MOH ライブ フィードの確認 \(P.147\)](#)

ライブ フィードからの MOH を設定するには、コールの音声ポートとダイヤル ピアを設定してから、「ダミー」の電話機つまり電話番号を作成します。ダミーの番号でコールを送受信できますが、この番号は物理的な電話機に割り当てられません。MOH システムが MOH フィードを確立するために、その番号を自動的にダイヤルします。

`moh-live` コマンドは、`max-dn` コマンドで作成された仮想音声ポートのプールから 1 つの仮想音声ポートを割り当てます。その仮想音声ポートはダミーの番号 (つまり、`moh-live` コマンドで指定された電話番号) にコールを発信します。MOH コールから取得されたオーディオストリームが Music On Hold オーディオストリームを提供します。

アナログ E&M ポートでは最小限の外部コンポーネントだけが必要であるため、ライブ フィード MOH 用のインターフェイスにはアナログ E&M ポートをお勧めします。回線レベルのオーディオ フィード (標準オーディオ ジャック) を E&M RJ-45 コネクタのピン 3 と 6 に直接接続します。E&M WAN Interface Card (WIC; WAN インターフェイス カード) には、外部オーディオ ソースに対して適切な電氣的遮蔽を提供する音声周波変圧器が組み込まれています (E&M ポート上のオーディオ接続には、ループ電流は必要ありません)。`signal immediate` コマンドと `auto-cut-through` コマンドは、この音声ポート上の E&M シグナリングを無効にします。G.711 オーディオ バケット ストリームは、E&M ポート上の Digital Signal Processor (DSP; デジタル シグナル プロセッサ) によって生成されます。

音声ポートに `signal loop-start live-feed` コマンドが設定されている場合は、ライブ フィード ソースを FXO ポートに直接接続できます。それ以外の場合は、バッテリー供給を行う外部のサードパーティ製アダプタを介してポートを接続する必要があります。外部アダプタは、通常の telephone company (telco; 電話会社) のバッテリー電圧に対して、FXO ポートのチップ リード線とリング リード線への正しい極性を提供する必要があります。また、外部アダプタは、外部オーディオ ソースと FXO ポートのチップ リード線およびリング リード線の間で変圧器ベースの遮断を提供する必要があります。

ライブ フィードからの音楽は、フラッシュ ファイルから読み取られるのではなく、MOH 再生バッファに送り続けられるため、通常は 2 秒の遅延が生じます。MOH 用に設定された電話番号で接続が確立されるまで、MOH ライブ フィード ソースへの発信コールが 30 秒おきに試行 (または再試行) されます。何らかの理由でライブ フィード ソースがシャットダウンされると、フラッシュ メモリ ソースが自動的にアクティブになります。

ライブ フィード MOH 接続は、自動的に接続される音声コールとして確立されます。この音声コールは、Cisco Unified SRST MOH システムによって生成されるか、またはライブ フィード MOH ポートに直接発信する外部ソースによって生成されます。MOH コールの送受信は PSTN を介して行うことができます。また、Voice Activity Detection (VAD; 音声アクティビティ検出) を無効にした状態で VoIP を介して行うこともできます。このコールは、設定時に `moh-live` コマンドで `out-call` キーワードが使用されない限り、着信コールと見なされます。

Cisco Unified SRST ルータは、コールからのオーディオ ストリームを MOH ストリームのソースとして使用し、フラッシュ ファイルから入手できるオーディオ ストリームをすべてそれに置き換えます。着信コールを介して受信される MOH ストリームの例としては、電話番号にコールを発信して Cisco Unified SRST ルータにオーディオ ストリームを配信する、H.323 ベースの外部サーバデバイスがあります。

## 前提条件

MOH ライブ フィード設定には、マルチキャスト MOH 用の Cisco Unified SRST ( P.133 の「マルチキャスト MOH 用の Cisco Unified SRST の設定」を参照 ) は不要です。ただし、MOH ライブ フィードは、マルチキャスト MOH と連携して動作するように設計されています。

## 制約事項

- バッテリ供給を行う外部のサードパーティ製アダプタが FXO ポートに用意されている場合、FXO ポートをライブ フィードに使用できます。
- FXS ポートをライブ フィードに使用することはできません。
- VoIP からのライブ フィードの場合は、VAD を無効にする必要があります。
- MOH は、PSTN および VoIP の G.711 コールに提供されます。Cisco Unified SRST の一部のバージョンでは、ローカル電話機に MOH を提供します。ローカル IP Phone への MOH をサポートしない Cisco Unified SRST の場合、発信者には保留時のトーンが繰り返し聞こえるため、まだ接続されていることを確認できます。

## Cisco Unified SRST ゲートウェイ上の音声ポートの設定

ライブ フィードからの MOH をアクティブにして、物理音声ポートを設定および接続するには、次の手順を使用します。

### 要約手順

1. `voice-port port`
2. `input gain decibels`
3. `auto-cut-through` ( E&M のみ )
4. `operation 4-wire` ( E&M のみ )
5. `signal immediate` ( E&M のみ )
6. `no shutdown`
7. `exit`

## 詳細手順

	コマンドまたはアクション	目的
ステップ 1	<code>voice-port port</code>  例: Router(config)# voice-port 1/1/0	物理音声ポートを設定するために、voice-port コンフィギュレーション モードを開始します。ご使用のルータの <i>port</i> 引数の正しい定義については、『 <a href="#">Cisco IOS Survivable Remote Site Telephony Version 3.2 Command Reference</a> 』を参照してください。
ステップ 2	<code>input gain decibels</code>  例: Router(config-voice-port)# input gain 0	インターフェイスの受信側に挿入するゲインの量をデシベルで指定します。許容値は -6 ~ 14 の整数です。
ステップ 3	<code>auto-cut-through</code>  例: Router(config-voiceport)# auto-cut-through	(E&M ポートのみ) PBX が M リード線の応答を提供しない場合のコールの完了を有効にします。MOH では、E&M ポートでこのコマンドを使用する必要があります。
ステップ 4	<code>operation 4-wire</code>  例: Router(config-voiceport)# operation 4-wire	(E&M ポートのみ) 4 線式のケーブル接続方式を選択します。MOH では、このコマンドで E&M ポートに対して 4 線式の動作を指定する必要があります。
ステップ 5	<code>signal immediate</code>  例: Router(config-voiceport)# signal immediate	(E&M ポートのみ) E&M タイ トランク インターフェイスの場合、発信側に対して、E リード線をオフフックにして回線を確認し、アドレス情報を DTMF デジタルとして送信するように指示します。
ステップ 6	<code>no shutdown</code>  例: Router(config-voiceport)# no shutdown	音声ポートをアクティブにします。
ステップ 7	<code>exit</code>  例: Router(config-voiceport)# exit	voice-port コンフィギュレーション モードを終了します。

## Cisco Unified SRST ゲートウェイ上の電話番号の設定

音声ポートの設定後、`destination-pattern` コマンドを使用して、ダイヤル ピアを作成し、音声ポートに電話番号を指定します。この電話番号は、システムが MOH へのアクセスに使用する番号です。

## 要約手順

1. `dial-peer voice tag pots`
2. `destination-pattern string`
3. `port port`
4. `exit`

## 詳細手順

	コマンドまたはアクション	目的
ステップ 1	<code>dial-peer voice tag pots</code>  例: Router(config)# dial-peer voice 7777 pots	dial-peer コンフィギュレーション モードを開始します。
ステップ 2	<code>destination-pattern string</code>  例: Router(config-dial-peer)# destination-pattern 7777	システムが Music On Hold の作成に使用する電話番号を指定します。このコマンドでは、ダイヤル ピアに使用するプレフィックスまたは完全な E.164 電話番号を指定します。
ステップ 3	<code>port port</code>  例: Router(config-dial-peer)# port 1/1/0	P.143 の「Cisco Unified SRST ゲートウェイ上の音声ポートの設定」で指定した音声ポートにダイヤル ピアを関連付けます。
ステップ 4	<code>exit</code>  例: Router(config-dial-peer)# exit	dial-peer コンフィギュレーション モードを終了します。

## MOH フィードの確立


電話番号を自動的にダイヤルすることで MOH フィードを確立して音楽ソース (CD プレーヤーなど) を接続するには、次の手順を使用します。

## 要約手順

1. `call-manager-fallback`
2. `max-dn max-directory-number`
3. `multicast moh multicast-address port port [route ip-address-list]`
4. `moh-live dn-number calling-number out-call outcall-number`
5. `exit`

## 詳細手順

	コマンドまたはアクション	目的
ステップ 1	<code>call-manager-fallback</code>  例: Router(config)# call-manager-fallback	call-manager-fallback コンフィギュレーション モードを開始します。
ステップ 2	<code>max-dn max-directory-number</code>  例: Router(config-cm-fallback)# max-dn 1	ルータがサポート可能な仮想音声ポートの最大数を設定します。 <ul style="list-style-type: none"> <li>• <code>max-directory-number</code>: ルータでサポートされる電話番号または仮想音声ポートの最大数。最大数は、プラットフォームによって異なります。デフォルトは 0 です。</li> </ul>

	コマンドまたはアクション	目的
ステップ 3	<pre>multicast moh multicast-address port port [route ip-address-list]</pre> <p>例:</p> <pre>Router(config-cm-fallback)# multicast moh 239.1.1.1 port 16386 route 239.1.1.2 239.1.1.3 239.1.1.4 239.1.1.5</pre>	<p>ブランチ オフィスのフラッシュ MOH ファイルからブランチ オフィスの IP Phone への MOH マルチキャストを有効にします。</p> <p> (注) このコマンドは、ライブフィード MOH のソースを指定して Cisco Unified Communications Manager モードをマルチキャストするために使用する必要があります。このコマンドは、厳密な SRST モードには必要ありません。</p> <ul style="list-style-type: none"> <li>• <i>multicast-address</i> および <i>port port</i> : マルチキャストされる MOH パケットの IP アドレスおよびポート番号を宣言します。このマルチキャスト IP アドレスおよびポートは、Cisco Unified Communications Manager がマルチキャスト MOH に使用するように設定されている IP アドレスおよびポート番号と一致する必要があります。MOH に別のコーデックを使用する場合、これらはベース IP アドレスおよびポートではなく、増分された IP アドレスまたはポート番号となることがあります。P.124 の「マルチキャストを有効にするための MOH オーディオソースの設定」を参照してください。Cisco Unified Communications Manager に複数のオーディオソースが設定されている場合は、オーディオソースの正しい IP アドレスおよびポート番号を使用していることを確認してください。</li> <li>• <i>route ip-address-list</i> :( オプション )フラッシュ MOH パケットの送信元となる IP アドレスを宣言します。最大 4 つの IP アドレス エントリを指定できます。<i>route</i> キーワードが設定されていない場合、Cisco Unified SRST システムは、Cisco Unified SRST に設定されている <i>ip source-address</i> コマンドの値を使用します。</li> </ul>
ステップ 4	<pre>moh-live dn-number calling-number out-call outcall-number</pre> <p>例:</p> <pre>Router(config-cm-fallback)# moh-live dn-number 3333 out-call 7777</pre>	<p>MOH ストリームのソースとなる発信コールにこの電話番号を使用することを指定します。</p> <ul style="list-style-type: none"> <li>• <i>dn-number calling-number</i> : MOH 電話番号を設定します。<i>calling-number</i> 引数は、電話番号を表す一連の数字です。</li> <li>• <i>out-call outcall-number</i> : MOH に使用されるライブフィードにルータが発信することを示し、発信先の番号を指定します。<i>outcall-number</i> 引数は、( 通常は E&amp;M ポートの ) 電話番号を表す一連の数字です。 <i>outcall</i> キーワードにより、P.143 の「Cisco Unified SRST ゲートウェイ上の音声ポートの設定」で指定したローカル ルータ音声ポートへの接続が確立されます。</li> </ul>
ステップ 5	<pre>exit</pre> <p>例:</p> <pre>Router(config-cm-fallback)# exit</pre>	<p>call-manager-fallback コンフィギュレーション モードを終了します。</p>



## Cisco Unified SRST MOH ライブ フィードの確認

MOH ライブ フィードを確認するには、P.136 の「基本的な Cisco Unified SRST マルチキャスト MOH ストリーミングの確認」で説明した `debug ephone moh` コマンドとその他のコマンドを使用します。

## Cisco Unified SRST ゲートウェイの設定例

ここでは、Cisco Unified SRST ゲートウェイの次のような設定例を示します。

- 2 つの IP アドレスにルーティングされる MOH : 例 (P.147)
- MOH ライブ フィード : 例 (P.148)

### 2 つの IP アドレスにルーティングされる MOH : 例

次の例では、Cisco Unified Communications Manager マルチキャスト MOH の IP アドレス 239.1.1.1 およびポート番号 16384 を宣言し、IP アドレス 10.1.1.1 および 172.21.51.143 が設定されているインターフェイスに `music-on-hold.au` オーディオ ファイル パケットを流します。

```
ccm-manager music-on-hold
interface Loopback0
 ip address 10.1.1.1. 255.255.255.255

interface FastEthernet0/0
 ip address 172.21.51.143 255.255.255.192

call-manager-fallback
 ip source-address 172.21.51.143 port 2000
 max-ephones 1
 max-dn 1
 moh music-on-hold.au
 multicast moh 239.1.1.1 port 16384 route 172.21.51.143 10.1.1.1
```



**(注)** このマルチキャスト IP アドレスおよびポートは、Cisco Unified Communications Manager がマルチキャスト MOH に使用するように設定されている IP アドレスおよびポート番号と一致する必要があります。MOH に別のコーデックを使用する場合、これらはベース IP アドレスおよびポートではなく、増分された IP アドレスまたはポート番号となることがあります。P.124 の「マルチキャストを有効にするための MOH オーディオ ソースの設定」を参照してください。Cisco Unified Communications Manager に複数のオーディオ ソースが設定されている場合は、オーディオ ソースの正しい IP アドレスおよびポート番号を使用していることを確認してください。

## MOH ライブフィード：例

次の例では、ライブフィードからの MOH を設定します。ダイヤルピアが `voice-port` コマンドで設定されている E&M ポートを参照すること、およびダイヤルピア番号 (7777) が `moh-live` コマンドの `out-call` キーワードで設定されている発信番号と一致することに注意してください。

```
voice-port 1/0/0
  input gain 3
  auto-cut-through
  operation 4-wire
  signal immediate
!
dial-peer voice 7777 pots
  destination-pattern 7777
  port 2/0/0
!
!
moh filename
call-manager-fallback
  max-conferences 8
  max-dn 1
  moh-live dn-number 3333 out-call 7777
!
.
.
.
```

## マルチキャスト MOH リソースとしての Cisco Unified SRST に関する機能情報

表 8 に、各バージョンにおける、マルチキャスト MOH リソース機能としての Cisco Unified SRST の拡張機能を示します。

ハードウェアおよびソフトウェアの互換性を調べるには、次の URL の Cisco Unified Communications Manager Compatibility Information ページを参照してください。

[http://www.cisco.com/en/US/products/sw/voicesw/ps556/products\\_device\\_support\\_tables\\_list.html](http://www.cisco.com/en/US/products/sw/voicesw/ps556/products_device_support_tables_list.html)

『Cisco Unified Communications Manager Documentation Roadmaps』も参照してください。このドキュメントは、次の URL から入手可能です。

[http://www.cisco.com/en/US/products/sw/voicesw/ps556/products\\_documentation\\_roadmaps\\_list.htm](http://www.cisco.com/en/US/products/sw/voicesw/ps556/products_documentation_roadmaps_list.htm)

プラットフォームおよびソフトウェア イメージのサポートに関する情報を参照するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator では、特定のソフトウェア リリース、機能セット、またはプラットフォームをサポートしている Cisco IOS ソフトウェアを確認できます。Cisco Feature Navigator にアクセスするには、<http://www.cisco.com/go/cfn> に移動してください。Cisco.com のアカウントは必要ありません。



(注)

表 8 は、所定の機能に対するサポートが導入された Cisco Unified SRST のバージョンを示しています。特に断りのない限り、その機能は以降のバージョンの Cisco Unified SRST ソフトウェアでもサポートされます。

表 8 マルチキャスト MOH リソースとしての Cisco Unified SRST に関する機能情報

機能名	リリース	機能情報
マルチキャスト MOH リソースとしての Cisco Unified SRST	3.0	MOH ライブ機能が追加されました。

## 関連情報

Cisco Unified SRST の監視および保守については、P.227 の「Cisco Unified SRST の監視と保守」を参照してください。

追加情報については、P.25 の「Cisco Unified SRST の概要」の P.40 の「その他の資料」を参照してください。



# Secure SRST の設定

---

Revised: July 11, 2008

この章では、認証、保水性、およびメディア暗号化など、新しい Secure SRST セキュリティ機能について説明します。

## 内容

- [Secure SRST を設定するための前提条件 \(P.152\)](#)
- [Secure SRST を設定する場合の制約事項 \(P.153\)](#)
- [Secure SRST の設定について \(P.154\)](#)
- [Secure SRST の設定方法 \(P.160\)](#)
- [Secure SRST の設定例 \(P.187\)](#)
- [関連情報 \(P.192\)](#)

## Secure SRST を設定するための前提条件

### 概要

- Secure SRST でサポートされている Secure Cisco Unified IP Phone には、証明書がインストールされている必要があり、暗号化が有効になっている必要があります。
- SRST ルータには、証明書が必要です。この証明書は、サードパーティまたは Cisco IOS Certificate Authority (CA; 認証局) から生成できます。Cisco IOS CA は、Cisco Unified SRST と同じゲートウェイで実行できます。
- Cisco Unified Communications Manager 4.1(2) またはそれ以降がインストールされており、セキュリティ モード (認証および暗号化モード) をサポートしている必要があります。
- Cisco Unified Communications Manager の Certificate Trust List (CTL) が有効になっている必要があります。詳細な手順については、『[Media and Signaling Authentication and Encryption Feature for Cisco IOS MGCP Gateways](#)』の「Configuring Secure IP Telephony Calls」の手順を参照してください。
- Secure SRST を実行するゲートウェイ ルータは、音声およびセキュリティ対応の Cisco IOS イメージ (「k9」暗号ソフトウェア イメージ) をサポートしている必要があります。次の 2 つのイメージがサポートされています。
  - 拡張 IP サービス。このイメージには、いくつかの拡張セキュリティ機能が含まれます。
  - 拡張エンタープライズ サービス。このイメージには、Cisco IOS ソフトウェアがすべて含まれます。

### PKI

- 手動または Network Time Protocol (NTP; ネットワーク タイム プロトコル) を使用して、クロックを設定します。クロックを設定することで、Cisco Unified Communications Manager と確実に同期を取ることができます。
- IP HTTP サーバ (Cisco IOS プロセッサ) が有効になっていない場合は、`ip http server` コマンドを使用して、IP HTTP サーバ (Cisco IOS プロセッサ) を有効にします。PKI (Public Key Infrastructure; 公開鍵インフラストラクチャ) 構成の詳細については、『[Cisco IOS Certificate Server](#)』を参照してください。
- 証明書サーバがスタートアップ コンフィギュレーションに含まれる場合、起動手順で次のメッセージが表示されることがあります。

```
% Failed to find Certificate Server's trustpoint at startup
% Failed to find Certificate Server's cert.
```

これらのメッセージは通知目的のメッセージであり、スタートアップ コンフィギュレーションがまだ完全に解析されていないので証明書サーバの設定を一時的に実行できないことを示します。このメッセージは、スタートアップ コンフィギュレーションが破損した場合のデバッグに役立ちます。

起動手順の後、`show crypto pki server` コマンドを使用して、証明書サーバのステータスを確認できます。

### SRST

- Secure SRST サービスは、Cisco Unified SRST がアクティブな間は登録できません。そのため、`no call-manager-fallback` コマンドを使用して、Cisco Unified SRST を無効にします。

### サポートされている Cisco Unified IP Phone、プラットフォーム、およびメモリの要件

- Secure SRST でサポートされている Cisco Unified IP Phone、ルータ、ネットワーク モジュール、およびコーデックのリストについては、『[Media and Signaling Authentication and Encryption Feature for Cisco IOS MGCP Gateways](#)』を参照してください。
- Cisco Unified IP Phone の最大数、電話番号 (DN) または仮想音声ポートの最大数、およびメモリ要件に関する最新情報については、『[Cisco Unified SRST 4.3 Supported Firmware, Platforms, Memory, and Voice Products](#)』を参照してください。

## Secure SRST を設定する場合の制約事項

### 概要

- 暗号ソフトウェア機能 (「k9」) は、輸出が規制されています。本製品には暗号化機能が備わっており、輸入、輸出、配布および使用に適用される米国および他の国での法律を順守するものとします。シスコの暗号化製品を譲渡された第三者は、その暗号化技術の輸入、輸出、配布、および使用を許可されたわけではありません。輸入業者、輸出業者、販売業者、およびユーザーは、米国および他の国での法律を順守する責任があります。本製品を使用するにあたっては、関係法令の順守に同意する必要があります。米国および他の国の法律を順守できない場合は、本製品を至急送り返してください。

シスコの暗号化製品に適用される米国の法律の概要については、次の URL で参照できます。  
<http://www.cisco.com/wwl/export/crypto/tool/>

ご不明な点がある場合は、[export@cisco.com](mailto:export@cisco.com) まで電子メールで連絡してください。

- Secure Real-Time Transport Protocol (SRTP) 暗号化コールは、Cisco Unified IP Phone エンドポイント間、または Cisco Unified IP Phone からゲートウェイ エンドポイントに対して行われます。IP Phone には、ロック アイコンが表示されます。ロックは、コールの IP レッグのみに対するセキュリティを示します。PSTN レッグのセキュリティは含まれていません。
- Secure SRST がサポートされるのは、1 つのルータの範囲内だけです。

### Secure SRST モードでサポートされていない内容

- 4.1(2) 以前の Cisco Unified Communications Manager バージョン
- 安全な Music On Hold (MOH; 保留音)。MOH はアクティブの状態ですが、保護されていない状態に戻ります。
- 安全な変換または会議
- Secure H.323 または SIP トランク
- SIP 電話機の相互運用性
- [Hot Standby Router Protocol \(HSRP; ホットスタンバイ ルータ プロトコル\)](#)

### Secure SRST モードでサポートされているコール

Secure SRST モードでは、音声コールだけがサポートされています。具体的には、次の音声コールがサポートされています。

- 基本的なコール
- コール転送 (打診およびブラインド)
- 自動転送 (ビジー、無応答、すべて)
- 共有回線 (IP Phone)
- 保留および再開

## Secure SRST の設定について

Secure SRST を設定するには、次の概念を理解する必要があります。

- [Secure SRST の利点 \( P.154 \)](#)
- [SRST での Cisco IP Phone のクリアテキスト フォールバック \( P.154 \)](#)
- [SRST ルータおよび TLS プロトコル \( P.155 \)](#)
- [Cisco Unified SRST ルータおよび PKI \( P.155 \)](#)
- [Secure SRST の認証および暗号化 \( P.156 \)](#)
- [Secure SRST ルータの Cisco IOS クレデンシャル サーバ \( P.158 \)](#)
- [Cisco Unified IP Phone への Secure Cisco Unified SRST の確立 \( P.158 \)](#)

## Secure SRST の利点

リモート サイトに設置され、ゲートウェイ ルータに接続されている Secure Cisco Unified IP Phone は、WAN を使用して Cisco Unified Communications Manager と安全に通信を行うことができます。ただし、WAN リンクまたは Cisco Unified Communications Manager がダウンすると、リモート電話機を使用したすべての通信が安全でなくなります。この状況を克服するために、ゲートウェイ ルータが Secure SRST モードで機能できるようになりました。このモードは、WAN リンクまたは Cisco Unified Communications Manager がダウンしたときに起動します。WAN リンクまたは Cisco Unified Communications Manager が復帰すると、Cisco Unified Communications Manager が安全なコール処理機能を再開します。

Secure SRST は、認証、保全性、およびメディア暗号化など、新しい Cisco Unified SRST セキュリティ機能を提供します。認証は、ユーザに対して、通話相手の身元が正しいことを保証します。保全性は、特定のデータがエンティティ間で変更されていないことを保証します。暗号化は機密性を意味します。つまり、対象となる受信者以外の人はデータを読み取れないということです。これらのセキュリティ機能は、Cisco Unified SRST 音声コールのプライバシーを守り、音声セキュリティ違反およびなりすまし犯罪から保護します。

SRST セキュリティが実現されるための条件は、次のとおりです。

- エンド デバイスが、証明書を使用して認証される
- シグナリングが、TCP に対する Transport Layer Security ( TLS ) を使用して認証および暗号化される
- 安全なメディア パスが、SRTP を使用して暗号化される
- 証明書が CA によって生成および配布される

## SRST での Cisco IP Phone のクリアテキスト フォールバック

12.3(14)T より以前の Cisco Unified SRST バージョンでは、安全な接続をサポートしたり、セキュリティを有効にしたりすることができませんでした。SRST ルータがフォールバック モードとして Secure SRST を実行できない場合 (つまり、Cisco Unified Communications Manager との TLS ハンドシェイクを完了できない場合)、証明書は Cisco IP Phone のコンフィギュレーション ファイルに追加されません。Cisco Unified SRST ルータの証明書がないと、Cisco Unified SRST がフォールバック モードのときに、Cisco Unified IP Phone が保護されていない (クリアテキスト) 通信を使用する原因となります。クリアテキスト モードでの検出およびフォールバックの機能は、Cisco Unified IP Phone ファームウェアに組み込まれています。クリアテキスト モードの詳細については、『[Media and Signaling Authentication and Encryption Feature for Cisco IOS MGCP Gateways](#)』を参照してください。



## SRST ルータおよび TLS プロトコル

TLS バージョン 1.0 は、Cisco Unified IP Phone、Secure Cisco Unified SRST ルータ、および Cisco Unified Communications Manager の間に Secure TCP チャンネルを提供します。TLS プロセスは、Cisco Unified Communications Manager の登録時に、Cisco Unified IP Phone が TLS 接続を確立することから始まります。Cisco Unified Communications Manager が Cisco Unified SRST にフォールバックするように設定されていると仮定すると、Cisco Unified IP Phone と Secure Cisco Unified SRST ルータ間の TLS 接続も確立されます。WAN リンクまたは Cisco Unified Communications Manager で障害が発生すると、コール制御が Cisco Unified SRST ルータに戻ります。

## Cisco Unified SRST ルータおよび PKI

Cisco Unified SRST ルータと Cisco Unified Communications Manager 間の証明書の転送は、Secure SRST 機能では必須です。PKI コマンドは、Secure Cisco Unified SRST の証明書を生成、インポート、およびエクスポートするために使用されます。表 9 に、Secure SRST 対応の Cisco Unified IP Phone および各電話機に該当する証明書を示します。P.169 の「[Secure SRST ルータへの電話機の証明書ファイル \(PEM 形式\) のインポート](#)」には、PKI コマンドを使用した証明書の生成、インポート、およびエクスポートに関する情報と設定が記載されています。




(注) 証明書のテキストは、設定によって異なる場合があります。また、Manufacturing Installed Certificate (MIC) をサポートする古い電話機では、CAP-RTP-00X または CAP-SJC-00X が必要になる場合もあります。



(注) シスコでは、MIC または Locally Significant Certificate (LSC) 証明書を使用する、Cisco IP Phone 7900 シリーズの電話機メモリを再利用した電話機をサポートしています。

表 9 サポートされている Cisco Unified IP Phone および証明書

Cisco Unified IP Phone 7940	Cisco Unified IP Phone 7960	Cisco Unified IP Phone 7970
<p>電話機は Distinguished Encoding Rules (DER) 形式の Certificate Authority Proxy Function( CAPF)から Locally Significant Certificate (LSC) を受け取ります。</p> <ul style="list-style-type: none"> <li>59fe77ccd.0</li> </ul> <p>ファイル名は、CAPF 証明書サブジェクト名および CAPF 証明書発行元に基づいて変更される場合があります。</p> <p>Cisco Unified Communications Manager がサードパーティ証明書プロバイダーを使用している場合、複数の .0 ファイルが存在する場合があります(2 ~ 10)。各 .0 証明書ファイルは、設定時に個別にインポートする必要があります。</p> <p>手動の登録だけがサポートされています。</p>	<p>電話機は Distinguished Encoding Rules (DER) 形式の Certificate Authority Proxy Function( CAPF)から Locally Significant Certificate (LSC) を受け取ります。</p> <ul style="list-style-type: none"> <li>59fe77ccd.0</li> </ul> <p>ファイル名は、CAPF 証明書サブジェクト名および CAPF 証明書発行元に基づいて変更される場合があります。</p> <p>Cisco Unified Communications Manager がサードパーティ証明書プロバイダーを使用している場合、複数の .0 ファイルが存在する場合があります(2 ~ 10)。各 .0 証明書ファイルは、設定時に個別にインポートする必要があります。</p> <p>手動の登録だけがサポートされています。</p>	<p>電話機には、デバイス認証に使用する Manufacturing Installed Certificate( MIC)が含まれています。Cisco 7970 が MIC を実装する場合、2 つの公開証明書ファイルが必要です。</p> <ul style="list-style-type: none"> <li>CiscoCA.pem( 証明書を認証するのに使用する Cisco Root CA )</li> </ul> <p> (注) MIC の名前は、設定によって異なる場合があります。</p> <ul style="list-style-type: none"> <li>a69d2e04.0. Privacy Enhanced Mail (PEM) 形式</li> </ul> <p>Cisco Unified Communications Manager がサードパーティ証明書プロバイダーを使用している場合、複数の .0 ファイルが存在する場合があります(2 ~ 10)。各 .0 証明書ファイルは、設定時に個別にインポートする必要があります。</p> <p>手動の登録だけがサポートされています。</p>

## Secure SRST の認証および暗号化

図 7 に、Secure SRST 認証および暗号化のプロセスを示します。表 10 では、プロセスの内容について説明します。

図 7 Secure Cisco Unified SRST の認証および暗号化

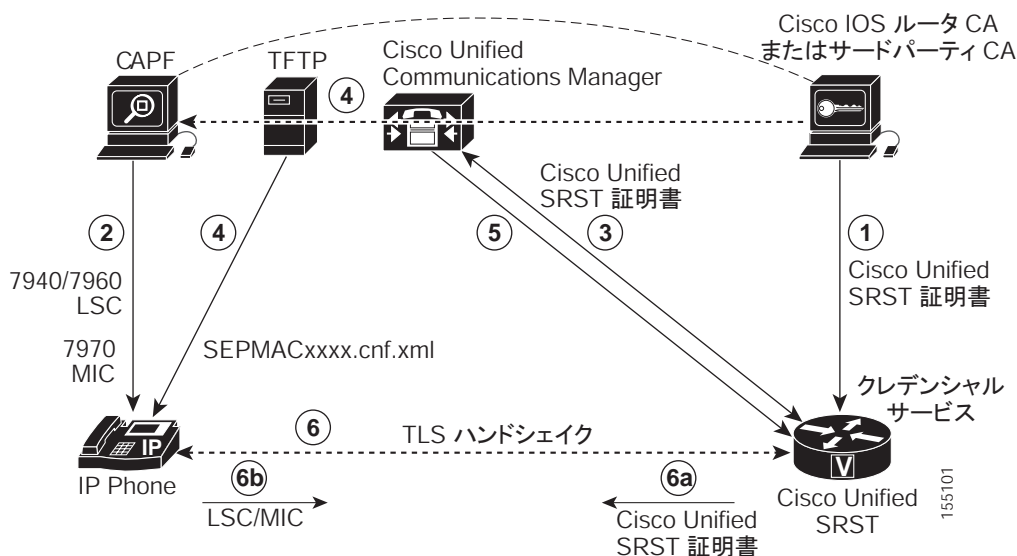


表 10 Secure SRST の認証および暗号化プロセスの概要

プロセス手順	説明または詳細
1.	<p>CA サーバが Cisco IOS ルータ CA またはサードパーティ CA であるかどうかに関わらず、CA サーバは、デバイスの証明書を SRST ゲートウェイに発行し、クレデンシャル サービスを有効にします。オプションで、Cisco IOS CA サーバを使用して SRST ルータで証明書を独自に生成することもできます。</p> <p>CA ルータは、CAPF の最終トラストポイントです。CAPF の詳細については、『<a href="#">Cisco Communications Manager Security Guide</a>』を参照してください。</p>
2.	<p>CAPF は、サポートされているデバイスが LSC を要求できるプロセスです。CAPF ユーティリティはキー ペアおよび CAPF に特有の証明書を生成し、クラスタ内のすべての Cisco Unified Communications Manager サーバにこの証明書をコピーし、LSC を Cisco Unified IP Phone に提供します。</p> <p>LSC は、MIC を持たない Cisco Unified IP Phone で必要です。Cisco 7970 には MIC が装備されているので、CAPF プロセスを行う必要はありません。</p>
3.	Cisco Unified Communications Manager はクレデンシャル サーバに SRST 証明書を要求し、クレデンシャル サーバは証明書で応答します。
4.	デバイスごとに、Cisco Unified Communications Manager は TFTP プロセスを使用し、Cisco Unified IP Phone の SEPMACxxxx.cnf.xml コンフィギュレーション ファイルに証明書を挿入します。
5.	<p>Cisco Unified Communications Manager は、電話機の証明書情報を含む PEM 形式のファイルを Cisco Unified SRST ルータに提供します。Cisco Unified SRST ルータに PEM ファイルを提供する作業は、手動で行います。詳細については、<a href="#">P.155</a> の「<a href="#">Cisco Unified SRST ルータおよび PKI</a>」を参照してください。</p> <p>Cisco Unified SRST ルータに PEM ファイルがある場合、Cisco Unified SRST ルータは IP Phone を認証して、TLS ハンドシェイクの際に IP Phone 証明書の発行元を検証できます。</p>
6.	TLS ハンドシェイクが発生すると、証明書が交換され、Cisco Unified IP Phone と Cisco Unified SRST ルータの間で相互の認証と登録が行われます。
a.	Cisco Unified SRST ルータは証明書を送信し、電話機は手順 4 で Cisco Unified Communications Manager から受信した証明書に対して証明書を検証します。
b.	Cisco Unified IP Phone は Cisco Unified SRST ルータに LSC または MIC を提供します。ルータは、手順 5 で提供された PEM 形式のファイルを使用して LSC または MIC を検証します。



(注)

電話機とルータの証明書が交換された後、メディアが自動的に暗号化され、SRST ルータとの TLS 接続が確立されます。

## Secure SRST ルータの Cisco IOS クレデンシャル サーバ

Secure SRST は、Secure SRST ルータで実行されるクレデンシャル サーバを導入しています。クライアントである Cisco Unified Communications Manager が TLS チャンネルを介して証明書を要求する場合、クレデンシャル サーバは SRST ルータの証明書を Cisco Unified Communications Manager に提供します。Cisco Unified Communications Manager は、Cisco Unified IP Phone コンフィギュレーション ファイルに SRST ルータの証明書を挿入し、電話機にコンフィギュレーション ファイルをダウンロードします。Secure Cisco Unified IP Phone は、証明書を使用して、フォールバック操作時に SRST ルータを認証します。クレデンシャル サービスは、デフォルトの TCP ポート 2445 で実行されます。

call-manager-fallback モードでクレデンシャル サーバを設定するには、次の 3 つの Cisco IOS コマンドを使用します。

- `credentials`
- `ip source-address (credentials)`
- `trustpoint (credentials)`

2 つの Cisco IOS コマンドが、クレデンシャル サーバのデバッグおよび検証機能を提供します。

- `debug credentials`
- `show credentials`

## Cisco Unified IP Phone への Secure Cisco Unified SRST の確立

図 8 および表 11 は、SRST ルータ、Cisco Unified Communications Manager、および Cisco Unified IP Phone のクレデンシャル サーバの相互作用を示し、Cisco Unified IP Phone への Secure SRST の確立について説明します。

図 8 SRST ルータ、Cisco Unified Communications Manager、および Cisco Unified IP Phone のクレデンシャル サーバの相互作用

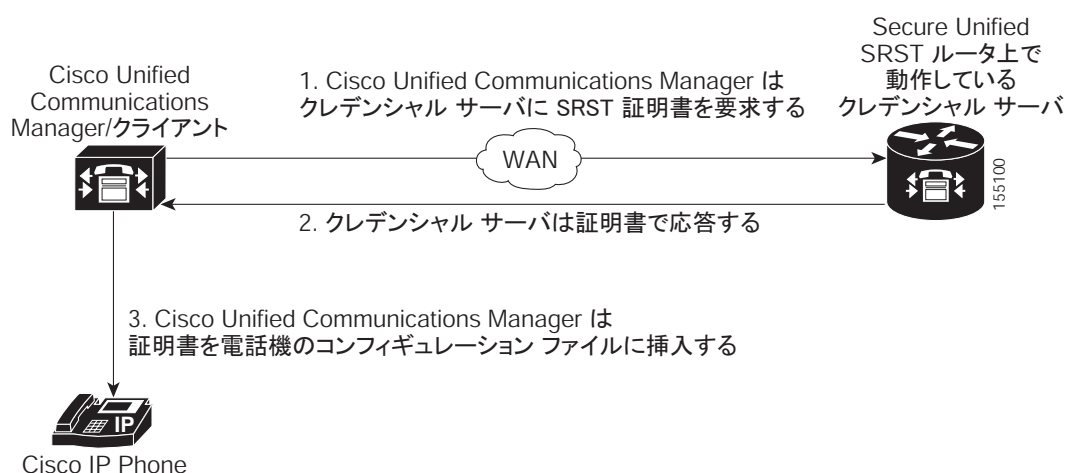


表 11 Secure SRST の確立

モード	プロセス	説明または詳細
標準モード	Cisco Unified IP Phone は DHCP を設定し、TFTP サーバのアドレスを取得します。	—
	Cisco Unified IP Phone は、TFTP サーバから CTL ファイルを取得します。	CTL ファイルには、電話機が信頼する必要がある証明書が含まれます。
	Cisco IP Phone は TLS プロトコル チャネルを開き、Cisco Unified Communications Manager に登録します。	Cisco Unified Communications Manager は、Secure Cisco Unified SRST ルータ情報および Cisco Unified SRST ルータの証明書を Cisco Unified IP Phone にエクスポートします。電話機は証明書をコンフィギュレーションに保管します。電話機に Cisco Unified SRST 証明書が保管されると、Cisco Unified SRST ルータが安全であると見なされます。 <a href="#">図 8</a> を参照してください。
	Cisco Unified IP Phone が「認証済み」または「暗号化済み」として設定されており、Cisco Unified Communications Manager が混合モードに設定されている場合、電話機はコンフィギュレーション ファイルで SRST 証明書を検索します。SRST 証明書が検出されると、デフォルトポートへのスタンバイ TLS 接続が開きます。デフォルトのポートは Cisco Unified IP Phone TCP ポートに 443 を追記した数字です。つまり、Cisco Unified SRST ルータのポート 2443 です。	セカンダリ Cisco Unified Communications Manager が存在しておらず、Cisco Unified SRST がバックアップ デバイスとして設定されていると仮定して、SRST ルータへの接続が自動的に行われます。 <a href="#">図 8</a> を参照してください。  Cisco Unified Communications Manager が、安全なモードである混合モードに設定されている必要があります。
WAN に障害が発生した場合、Cisco Unified IP Phone が Cisco Unified SRST 登録を開始します。		
SRST モード	Cisco Unified IP Phone は、安全な通信を行うためにデフォルトポートで SRST ルータに登録します。	—

## Secure SRST の設定方法

設定に関する次の項では、Secure Cisco Unified SRST ルータと Cisco Unified IP Phone が TLS ハンドシェイク時に確実に相互の認証を要求できるようにします。TLS ハンドシェイクは、WAN リンク障害の前後に関係なく、電話機が Cisco Unified SRST ルータに登録するときに行われます。

ここでは、次の内容について説明します。

- [安全に通信を行うための Cisco Unified SRST ルータの準備 \(P.160\)](#) (必須)
- [Secure SRST ルータへの電話機の証明書ファイル \(PEM 形式\) のインポート \(P.169\)](#) (必須)
- [Secure Cisco Unified SRST ルータへの Cisco Unified Communications Manager の設定 \(P.176\)](#) (必須)
- [Secure Cisco Unified SRST ルータでの SRST モードの有効化 \(P.180\)](#) (必須)
- [電話機のステータスおよび登録の確認 \(P.182\)](#) (必須)

### 安全に通信を行うための Cisco Unified SRST ルータの準備

次の作業では、安全な通信を行うために Cisco Unified SRST ルータを準備します。

- [Cisco IOS 証明書サーバへの CA サーバの設定 \(P.160\)](#) (オプション)
- [CA サーバに対する Secure Cisco Unified SRST ルータの自動登録と認証 \(P.162\)](#) (必須)
- [自動証明書登録の無効化 \(P.164\)](#) (必須)
- [証明書登録の確認 \(P.165\)](#) (オプション)
- [Secure Cisco Unified SRST ルータでのクレデンシャル サービスの有効化 \(P.167\)](#) (必須)
- [クレデンシャル設定のトラブルシューティング \(P.168\)](#) (オプション)

### Cisco IOS 証明書サーバへの CA サーバの設定

Cisco Unified SRST ルータが安全な通信を提供するためには、ネットワークのデバイス証明書を発行する CA サーバが 1 台必要です。CA サーバは、サードパーティ CA でも、Cisco IOS 証明書サーバから生成されたものでも構いません。



Cisco IOS 証明書サーバは、ネットワークにサードパーティ CA を持たないユーザに対して証明書生成オプションを提供します。Cisco IOS 証明書サーバは、SRST ルータまたは異なる Cisco IOS ルータで実行できます。

サードパーティ CA を持っていない場合、CA サーバの有効化および設定の詳細については、『[Cisco IOS Certificate Server](#)』を参照してください。次に、設定例を示します。

#### 要約手順

1. `crypto pki server cs-label`
2. `database level {minimal | names | complete}`
3. `database url root-url`
4. `issuer-name DN-string`
5. `grant auto`
6. `no shutdown`

## 詳細手順

	コマンドまたはアクション	目的
ステップ 1	<pre>crypto pki server cs-label</pre> <p>例:</p> <pre>Router (config)# crypto pki server srstcaserver</pre>	<p>証明書サーバを有効にし、certificate server コンフィギュレーション モードを開始します。</p> <p> (注) RSA キー ペアを手動で生成した場合、<i>cs-label</i> 引数がキー ペアの名前と一致する必要があります。</p> <p>証明書サーバの詳細については、『<a href="#">Cisco IOS Certificate Server</a>』を参照してください。</p>
ステップ 2	<pre>database level {minimal   names   complete}</pre> <p>例:</p> <pre>Router (cs-server)# database level complete</pre>	<p>証明書登録データベースに保存されるデータ タイプを制御します。</p> <ul style="list-style-type: none"> <li>• <i>minimal</i>: 競合を発生させずに新しい証明書を発行し続けるために、十分な情報だけを保存します。これがデフォルト値です。</li> <li>• <i>names</i>: minimal レベルで提供される情報に加えて、各証明書のシリアル番号と件名を保存します。</li> <li>• <i>complete</i>: minimal および <i>names</i> レベルで提供される情報に加えて、発行した各証明書をデータベースに書き込みます。</li> </ul> <p> (注) <i>complete</i> キーワードを指定すると、大量の情報が生成されます。このキーワードを使用する場合は、<i>database url</i> コマンドを使用して、データを保存する外部 TFTP サーバも指定する必要があります。</p>
ステップ 3	<pre>database url root-url</pre> <p>例:</p> <pre>Router (cs-server)# database url nvram</pre>	<p>証明書サーバのすべてのデータベース エントリを書き込む場所を指定します。<i>crypto pki server</i> コマンドを使用して証明書サーバを作成したら、このコマンドを使用して、発行されたすべての証明書の結合リストを指定します。<i>root-url</i> 引数は、データベース エントリを書き込む場所を指定します。</p> <ul style="list-style-type: none"> <li>• データベース エントリが書き込まれるデフォルトの場所はフラッシュですが、この作業には NVRAM が推奨されます。</li> </ul>
ステップ 4	<pre>issuer-name DN-string</pre> <p>例:</p> <pre>Router (cs-server)# issuer-name CN=srstcaserver</pre>	<p>CA 発行元名を指定した認定者名 (DN ストリング) に設定します。デフォルト値は次のとおりです。</p> <pre>issuer-name CN=cs-label</pre>
ステップ 5	<pre>grant auto</pre> <p>例:</p> <pre>Router (cs-server)# grant auto</pre>	<p>自動的な証明書がすべての要求者に発行されるようにします。</p> <ul style="list-style-type: none"> <li>• このコマンドは登録時のみに使用され、P.164 の「自動証明書登録の無効化」で削除されます。</li> </ul>
ステップ 6	<pre>no shutdown</pre> <p>例:</p> <pre>Router (cs-server)# no shutdown</pre>	<p>Cisco IOS 証明書サーバを有効にします。</p> <ul style="list-style-type: none"> <li>• このコマンドを使用できるのは、すべての証明書サーバの設定が完了してからだけです。</li> </ul>

## 例

次の例は、CA を生成する 1 つの方法を示しています。

```
Router(config)# crypto pki server srstcaserver
Router(cs-server)# database level complete
Router(cs-server)# database url nvram
Router(cs-server)# issuer-name CN=srstcaserver
Router(cs-server)# grant auto

% This will cause all certificate requests to be automatically granted.
Are you sure you want to do this? [yes/no]: y
Router(cs-server)# no shutdown
% Once you start the server, you can no longer change some of
% the configuration.
Are you sure you want to do this? [yes/no]: y
% Generating 1024 bit RSA keys ...[OK]
% Certificate Server enabled.
```

## CA サーバに対する Secure Cisco Unified SRST ルータの自動登録と認証

Secure Cisco Unified SRST ルータでは、トラストポイントを定義する必要があります。つまり、CA サーバからデバイスの証明書を取得する必要があります。この手順は、証明書の登録と呼ばれます。登録されると、Secure Cisco Unified SRST ルータは Secure SRST ルータとして Cisco Unified Communications Manager に認識されます。

CA サーバに Secure Cisco Unified SRST ルータを登録するためのオプションは、自動登録、カットアンドペースト、および TFTP の 3 つです。CA サーバが Cisco IOS 証明書サーバの場合、自動登録を使用できます。それ以外の場合は、手動の登録が必要です。手動の登録とは、カットアンドペーストまたは TFTP を指します。

自動登録に対しては、**enrollment url** コマンドを使用します。SRST ルータを認証するには、**crypto pki authenticate** コマンドを使用します。コマンドの使用方法については、『[Certification Authority Interoperability Commands](#)』を参照してください。自動登録の例は、『[Certificate Enrollment Enhancements](#)』から入手できます。P.164 の「例」に、設定例を示します。

### 要約手順

1. **crypto pki trustpoint** *name*
2. **enrollment url** *url*
3. **revocation-check** *method*
4. **exit**
5. **crypto pki authenticate** *name*
6. **crypto pki enroll** *name*



## 詳細手順

	コマンドまたはアクション	目的
ステップ 1	<pre>crypto pki trustpoint name</pre> <p>例: Router(config)# crypto pki trustpoint srstca</p>	<p>ルータが使用する必要がある CA を宣言し、ca-trustpoint コンフィギュレーション モードを開始します。</p> <ul style="list-style-type: none"> <li>指定される名前は、P.167 の「<a href="#">Secure Cisco Unified SRST ルータでのクレデンシャル サービスの有効化</a>」で宣言されるトラストポイント名と同じになります。</li> </ul>
ステップ 2	<pre>enrollment url url</pre> <p>例: Router(ca-trustpoint)# enrollment url http://10.1.1.22</p>	<p>CA の登録パラメータを指定します。</p> <ul style="list-style-type: none"> <li><code>url url</code>: ルータが証明書要求を送信する CA の URL を指定します。</li> <li>登録にシスコ独自の SCEP を使用している場合、<code>url</code> は <code>http://CA_name</code> という形式にする必要があります。ここで、<code>CA_name</code> は、Cisco IOS CA のホスト Domain Name System (DNS; ドメインネームシステム)名または IP アドレスを表します。</li> <li>P.160 の「<a href="#">Cisco IOS 証明書サーバへの CA サーバの設定</a>」に記載されている手順を使用した場合、URL は、手順 1 で設定した証明書サーバルータの IP アドレスです。サードパーティ CA が使用された場合、IP アドレスは外部 CA になります。</li> </ul>
ステップ 3	<pre>revocation-check method1</pre> <p>例: Router(ca-trustpoint)# revocation-check none</p>	<p>証明書の失効ステータスをチェックします。<code>method1</code> 引数は、ルータが証明書の失効ステータスをチェックするために使用する方法です。この作業で使用できる方法は、<code>none</code> だけです。<code>none</code> キーワードは、失効チェックが実行されず、証明書が常に受け入れられることを意味します。</p> <ul style="list-style-type: none"> <li>この作業では、<code>none</code> キーワードを使用することが必須です。</li> </ul>
ステップ 4	<pre>exit</pre> <p>例: Router(ca-trustpoint)# exit</p>	<p>ca-trustpoint コンフィギュレーション モードを終了し、global コンフィギュレーション モードに戻ります。</p>
ステップ 5	<pre>crypto pki authenticate name</pre> <p>例: Router(config)# crypto pki authenticate srstca</p>	<p>CA から証明書を取得することにより、CA を認証します。</p> <ul style="list-style-type: none"> <li>CA の名前を引数として取得します。</li> </ul>
ステップ 6	<pre>crypto pki enroll name</pre> <p>例: Router(config)# crypto pki enroll srstca</p>	<p>CA から SRST ルータの証明書を取得します。</p> <ul style="list-style-type: none"> <li>CA の名前を引数として取得します。</li> </ul>

## 例

次の例では、Cisco Unified SRST ルータを自動登録および認証します。

```
Router(config)# crypto pki trustpoint srstca
Router(ca-trustpoint)# enrollment url http://10.1.1.22
Router(ca-trustpoint)# revocation-check none
Router(ca-trustpoint)# exit
Router(config)# crypto pki authenticate srstca

Certificate has the following attributes:
Fingerprint MD5: 4C894B7D 71DBA53F 50C65FD7 75DDBFCA
Fingerprint SHA1: 5C3B6B9E EFA40927 9DF6A826 58DA618A BF39F291
% Do you accept this certificate? [yes/no]: y
Trustpoint CA certificate accepted.

Router(config)# crypto pki enroll srstca
%
% Start certificate enrollment ..
% Create a challenge password. You will need to verbally provide this
password to the CA Administrator in order to revoke your certificate.
For security reasons your password will not be saved in the configuration.
Please make a note of it.
Password:
Re-enter password:

% The fully-qualified domain name in the certificate will be: router.cisco.com
% The subject name in the certificate will be: router.cisco.com
% Include the router serial number in the subject name? [yes/no]: y
% The serial number in the certificate will be: D0B9E79C
% Include an IP address in the subject name? [no]: n
Request certificate from CA? [yes/no]: y
% Certificate request sent to Certificate Authority
% The certificate request fingerprint will be displayed.
% The 'show crypto pki certificate' command will also show the fingerprint.

Sep 29 00:41:55.427: CRYPTO_PKI: Certificate Request Fingerprint MD5: D154FB75
2524A24D 3D1F5C2B 46A7B9E4
Sep 29 00:41:55.427: CRYPTO_PKI: Certificate Request Fingerprint SHA1: 0573FBB2
98CD1AD0 F37D591A C595252D A17523C1
Sep 29 00:41:57.339: %PKI-6-CERTRET: Certificate received from Certificate Authority
```

## 自動証明書登録の無効化

**grant auto** コマンドを使用すると証明書が発行されます。このコマンドは、P.160の「Cisco IOS 証明書サーバへのCAサーバの設定」に記載されているオプションの作業でアクティブ化されます。



(注) セキュリティ上の最善策は、証明書が引き続き許可されないように、**grant auto** コマンドを無効にすることです。

## 要約手順

1. **crypto pki server *cs-label***
2. **shutdown**
3. **no grant auto**
4. **no shutdown**

## 詳細手順

	コマンドまたはアクション	目的
ステップ 1	<code>crypto pki server cs-label</code>  例: Router (config)# <code>crypto pki server srstcaserver</code>	証明書サーバを有効にし、certificate server コンフィギュレーション モードを開始します。   (注) RSA キー ペアを手動で生成した場合、 <code>cs-label</code> 引数がキー ペアの名前と一致する必要があります。
ステップ 2	<code>shutdown</code>  例: Router (cs-server)# <code>shutdown</code>	Cisco IOS 証明書サーバを無効にします。
ステップ 3	<code>no grant auto</code>  例: Router (cs-server)# <code>no grant auto</code>	自動的な証明書がすべての要求者に発行されないようにします。  • このコマンドは登録時にのみ使用するので、この作業で削除する必要があります。
ステップ 4	<code>no shutdown</code>  例: Router (cs-server)# <code>no shutdown</code>	Cisco IOS 証明書サーバを有効にします。  • このコマンドを使用できるのは、すべての証明書サーバの設定が完了してからだけです。

## 次の作業

手動の登録手順については、『[Manual Certificate Enrollment \(TFTP and Cut-and-Paste\)](#)』を参照してください。

## 証明書登録の確認

Cisco IOS 証明書サーバを CA として使用した場合、証明書登録を確認するには `show running-config` コマンドを使用し、CA サーバのステータスを確認するには `show crypto pki server` コマンドを使用します。

## 要約手順

1. `show running-config`
2. `show crypto pki server`

## 詳細手順

ステップ 1 `show running-config`

CA サーバ (01) およびデバイス (02) の証明書の作成を確認するには、`show running-config` コマンドを使用します。この例は、登録された証明書を示します。

```

Router# show running-config
.
.
.
! SRST router device certificate.
crypto pki certificate chain srstca
certificate 02
308201AD 30820116 A0030201 02020102 300D0609 2A864886 F70D0101 04050030
17311530 13060355 0403130C 73727374 63617365 72766572 301E170D 30343034
31323139 35323233 5A170D30 35303431 32313935 3232335A 30343132 300F0603
55040513 08443042 39453739 43301F06 092A8648 86F70D01 09021612 6A61736F
32363931 2E636973 636F2E63 6F6D305C 300D0609 2A864886 F70D0101 01050003
4B003048 024100D7 0CC354FB 5F7C1AE7 7A25C3F2 056E0485 22896D36 6CA70C19
C98F9BAE AE9D1F9B D4BB7A67 F3251174 193BB1A3 12946123 E5C1CCD7 A23E6155
FA2ED743 3FB8B902 03010001 A330302E 300B0603 551D0F04 04030205 A0301F06
03551D23 04183016 8014F829 CE97AD60 18D05467 FC293963 C2470691 F9BD300D
06092A86 4886F70D 01010405 00038181 007EB48E CAE9E1B3 D1E7A185 D7F0D565
CB84B17B 1151BD78 B3E39763 59EC650E 49371F6D 99CBD267 EB8ADF9D 9E43A5F2
FB2B18A0 34AF6564 11239473 41478AFC A86E6DA1 AC518E0B 8657CEBB ED2BDE8E
B586FE67 00C358D4 EFDD8D44 3F423141 C2D331D3 1EE43B6E 6CB29EE7 0B8C2752
C3AF4A66 BD007348 D013000A EA3C206D CF
quit
certificate ca 01
30820207 30820170 A0030201 02020101 300D0609 2A864886 F70D0101 04050030
17311530 13060355 0403130C 73727374 63617365 72766572 301E170D 30343034
31323139 34353136 5A170D30 37303431 32313934 3531365A 30173115 30130603
55040313 0C737273 74636173 65727665 7230819F 300D0609 2A864886 F70D0101
01050003 818D0030 81890281 8100C3AF EE1E4BB1 9922A8DA 2BB9DC8E 5B1BD332
1051C9FE 32A971B3 3C336635 74691954 98E765B1 059E24B6 32154E99 105CA989
9619993F CC72C525 7357EBAC E6335A32 2AAF9391 99325BFD 9B8355EB C10F8963
9D8FC222 EE8AC831 71ACD3A7 4E918A8F D5775159 76FBF499 5AD0849D CAA41417
DD866902 21E5DD03 C37D4B28 0FAB0203 010001A3 63306130 0F060355 1D130101
FF040530 030101FF 300E0603 551D0F01 01FF0404 03020186 301D0603 551D0E04
160414F8 29CE97AD 6018D054 67FC2939 63C24706 91F9BD30 1F060355 1D230418
30168014 F829CE97 AD6018D0 5467FC29 3963C247 0691F9BD 300D0609 2A864886
F70D0101 04050003 8181007A F71B25F9 73D74552 25DFD03A D8D1338F 6792C805
47A81019 795B5AAE 035400BB F859DABF 21892B5B E71A8283 08950414 8633A8B2
C98565A6 C09CA641 88661402 ACC424FD 36F23360 ABFF4C55 BB23C66A C80A3A57
5EE85FF8 C1B1A540 E818CE6D 58131726 BB060974 4E1A2F4B E6195522 122457F3
DEDBAAD7 3780136E B112A6
quit

```

## ステップ 2 show crypto pki server

起動手順の後に CA サーバのステータスを確認するには、**show crypto pki server** コマンドを使用します。

```

Router# show crypto pki server

Certificate Server srstcaserver:
Status: enabled
Server's configuration is locked (enter "shut" to unlock it)
Issuer name: CN=srstcaserver
CA cert fingerprint: AC9919F5 CAFE0560 92B3478A CFF5EC00
Granting mode is: auto
Last certificate issued serial number: 0x2
CA certificate expiration timer: 13:46:57 PST Dec 1 2007
CRL NextUpdate timer: 14:54:57 PST Jan 19 2005
Current storage dir: nvram
Database Level: Complete - all issued certs written as <serialnum>.cer

```

## Secure Cisco Unified SRST ルータでのクレデンシャル サービスの有効化

Cisco Unified SRST ルータが独自の証明書を取得したら、Cisco Unified Communications Manager に証明書を提供する必要があります。クレデンシャル サービスを有効にすると、Cisco Unified Communications Manager は Secure SRST デバイスの証明書を取得して、Cisco Unified IP Phone のコンフィギュレーション ファイルに保管することができます。

すべての Cisco Unified SRST ルータのクレデンシャル サービスをアクティブにします。



(注) セキュリティ上の最善策は、コントロールプレーン ポリシングを使用してクレデンシャル サービスポートを保護することです。コントロールプレーン ポリシングは、ゲートウェイを保護し、トラフィックの負荷が大きいときもパケットの転送とプロトコルの状態を維持します。コントロールプレーンの詳細については、『[Control Plane Policing](#)』を参照してください。また、[P.192](#) の「[コントロールプレーン ポリシング：例](#)」に設定例を示します。

### 要約手順

1. `credentials`
2. `ip source-address ip-address [port port]`
3. `trustpoint trustpoint-name`
4. `exit`

### 詳細手順

	コマンドまたはアクション	目的
ステップ 1	<code>credentials</code>  例： <pre>Router(config)# credentials</pre>	Cisco Unified SRST ルータの証明書を Cisco Unified Communications Manager に提供し、credentials コンフィギュレーション モードを開始します。
ステップ 2	<code>ip source-address ip-address [port port]</code>  例： <pre>Router(config-credentials)# ip source-address 10.1.1.22 port 2445</pre>	Cisco Unified SRST ルータが、指定した IP アドレスとポートを介して Cisco Unified Communications Manager からメッセージを受信できるようにします。 <ul style="list-style-type: none"> <li>• <code>ip-address</code> : IP アドレスは既存のルータの IP アドレスです。通常、ルータのイーサネットポートのアドレスの 1 つです。</li> <li>• <code>port port</code> : (オプション) Cisco Unified Communications Manager からメッセージを受信するためにゲートウェイ ルータが接続されるポート。ポート番号は 2000 ~ 9999 です。デフォルトのポート番号は 2445 です。</li> </ul>
ステップ 3	<code>trustpoint trustpoint-name</code>  例： <pre>Router(config-credentials)# trustpoint srstca</pre>	Cisco Unified SRST ルータの証明書と関連付けるトラストポイントの名前を指定します。 <code>trustpoint-name</code> 引数はトラストポイント名で、SRST デバイスの証明書に対応します。 <ul style="list-style-type: none"> <li>• トラストポイント名は、<a href="#">P.162</a> の「<a href="#">CA サーバに対する Secure Cisco Unified SRST ルータの自動登録と認証</a>」で宣言したトラストポイント名と同じにする必要があります。</li> </ul>

	コマンドまたはアクション	目的
ステップ 4	<pre>exit</pre> <p>例:</p> <pre>Router(config-credentials)# exit</pre>	credentials コンフィギュレーション モードを終了します。

## 例

```
Router(config)# credentials
Router(config-credentials)# ip source-address 10.1.1.22 port 2445
Router(config-credentials)# trustpoint srstca
Router(config-credentials)# exit
```

## クレデンシャル設定のトラブルシューティング

次の手順では、クレデンシャル設定を表示するか、Cisco Unified SRST ルータのクレデンシャル設定のデバッグを設定します。

### 要約手順

1. `show credentials`
2. `debug credentials`

### 詳細手順

#### ステップ 1 `show credentials`

Secure Cisco Unified SRST のフォールバック時に使用する Cisco Unified Communications Manager に提供される Cisco Unified SRST ルータのクレデンシャル設定を表示するには、`show credentials` コマンドを使用します。

```
Router# show credentials

Credentials IP: 10.1.1.22
Credentials PORT: 2445
Trustpoint: srstca
```

#### ステップ 2 `debug credentials`

Cisco Unified SRST ルータのクレデンシャル設定のデバッグを設定するには、`debug credentials` コマンドを使用します。

```
Router# debug credentials

Credentials server debugging is enabled
Router#
Sep 29 01:01:50.903: Credentials service: Start TLS Handshake 1 10.1.1.13 2187
Sep 29 01:01:50.903: Credentials service: TLS Handshake returns OPSSLReadWouldBlockErr
Sep 29 01:01:51.903: Credentials service: TLS Handshake returns OPSSLReadWouldBlockErr
Sep 29 01:01:52.907: Credentials service: TLS Handshake returns OPSSLReadWouldBlockErr
Sep 29 01:01:53.927: Credentials service: TLS Handshake completes.
```

### 関連コマンド

次のコマンドを使用して、証明書が見つからない（認証しようとする証明書が欠落している）かどうかを表示したり、特定の証明書が照合されたことを表示したりします（したがって、電話機の認証に使用されたルータがわかります）。

- `debug crypto pki messages`
- `debug crypto pki transactions`

## Secure SRST ルータへの電話機の証明書ファイル（PEM 形式）のインポート

この作業では、Cisco IP Unified Phone に必要な作業のプロビジョニングを完了して、Secure SRST を認証します。

### Cisco Unified Communications Manager 4.X.X およびそれ以前のバージョン

Cisco Unified Communications Manager 4.X.X およびそれ以前のバージョンを実行しているシステムの場合、Secure Cisco Unified SRST ルータは電話機の証明書を取得して、TLS ハンドシェイク時に Cisco Unified IP Phone を認証できるようにする必要があります。Cisco Unified IP Phone が異なると、異なる証明書が使用されます。表 9 (P.156) に、電話機の各タイプに必要な証明書を示します。

証明書は、Cisco Unified Communications Manager から Cisco Unified SRST ルータに手動でインポートする必要があります。証明書の数は、Cisco Unified Communications Manager の設定によって異なります。手動の登録とは、カット アンド ペーストまたは TFTP を指します。手動の登録手順については、『*Manual Certificate Enrollment (TFTP and Cut-and-Paste)*』を参照してください。各電話機または PEM ファイルに対して、登録手順を繰り返します。

### Cisco Unified Communications Manager 5.0 およびそれ以降のバージョン

Cisco Unified Communications Manager 5.0 およびそれ以降のバージョンを実行しているシステムには、表 9 に示されている要件に加えて、4 つの証明書（CAPF、CiscoCA、CiscoManufactureCA、および CiscoRootCA2048）が必要です。これらの証明書は、Cisco Unified SRST ルータにコピー アンド ペーストする必要があります。



(注)

CiscoRootCA は、CiscoRoot2048CA と呼ばれます。

### 前提条件

最後のコンフィギュレーション コマンド（`crypto pki authenticate`）が次のプロンプトを発行するときに、有効な証明書が必要になります。

```
Enter the base 64 encoded CA certificate.  
End with a blank line or the word "quit" on a line by itself
```

### Cisco Unified Communications Manager 4.X.X およびそれ以前のバージョン

Cisco Unified Communications Manager 4.X.X およびそれ以前のバージョンの場合、Cisco Unified Communications Manager のメニュー バーで、**Program Files > Cisco > Certificates** を選択することで、証明書を検索できます。

Windows Wordpad または Notepad を使用して .0 ファイルを開き、内容を SRST ルータ コンソールにコピー アンド ペーストします。次に、.pem ファイルに対して同じ手順を繰り返します。「-----BEGIN CERTIFICATE-----」と「-----END CERTIFICATE-----」の間に表示されるすべての内容をコピーします。

### Cisco Unified Communications Manager 5.0 およびそれ以降のバージョン

Cisco Unified Communications Manager 5.0 およびそれ以降のバージョンの場合、次の手順を実行します。

- 
- ステップ 1** Cisco Unified Communications Manager にログインします。
  - ステップ 2** Security > Certificate Management > Download Certificate/CTL に進みます。
  - ステップ 3** Download Trust Cert を選択し、Next をクリックします。
  - ステップ 4** CAPF-trust を選択し、Next をクリックします。
  - ステップ 5** CiscoCA を選択し、Next をクリックします。
  - ステップ 6** Continue をクリックします。
  - ステップ 7** ファイル名をクリックします。
  - ステップ 8** 「-----BEGIN CERTIFICATE-----」と「-----END CERTIFICATE-----」の間に表示されるすべての内容を、後で取得できる場所にコピーします。
  - ステップ 9** CiscoManufactureCA、CiscoRootCA2048、および CAPF に対して、手順 5 ~ 8 を繰り返します。
- 

### 制約事項

仮想 Web サーバを介した Cisco Unified Communications Manager からの HTTP 自動登録は、サポートされていません。

### 要約手順

1. `crypto pki trustpoint name`
2. `revocation-check method1`
3. `enrollment terminal`
4. `exit`
5. `crypto pki authenticate name`



## 詳細手順

	コマンドまたはアクション	目的
ステップ 1	<b>crypto pki trustpoint <i>name</i></b>  <b>例:</b> Router (config)# crypto pki trustpoint 7970	ルータが使用する必要がある CA を宣言し、ca-trustpoint コンフィギュレーション モードを開始します。 <ul style="list-style-type: none"> <li>• Cisco Unified Communications Manager 5.0 を使用している場合、4 つの <i>name</i> 引数 (CAPF、CiscoCA、CiscoManufactureCA、および CiscoRootCA2048) を個別に設定する必要があります。P.175 の「Cisco Unified Communications Manager 5.0 およびそれ以降のバージョンの例」を参照してください。</li> </ul>
ステップ 2	<b>revocation-check <i>method1</i></b>  <b>例:</b> Router(ca-trustpoint)# revocation-check none	証明書の失効ステータスをチェックします。 <i>method1</i> 引数は、ルータが証明書の失効ステータスをチェックするために使用する方法です。この作業で使用できる方法は、none だけです。none キーワードは、失効チェックが実行されず、証明書が常に受け入れられることを意味します。 <ul style="list-style-type: none"> <li>• この作業では、none キーワードを使用することが必須です。</li> </ul>
ステップ 3	<b>enrollment terminal</b>  <b>例:</b> Router(ca-trustpoint)# enrollment terminal	手動のカット アンド ペースト証明書登録を指定します。
ステップ 4	<b>exit</b>  <b>例:</b> Router(ca-trustpoint)# exit	ca-trustpoint コンフィギュレーション モードを終了し、global コンフィギュレーションに戻ります。
ステップ 5	<b>crypto pki authenticate <i>name</i></b>  <b>例:</b> Router(config)# crypto pki authenticate 7970	CA から証明書を取得することにより、CA を認証します。 <ul style="list-style-type: none"> <li>• <b>crypto pki trustpoint</b> コマンドで使用したのと同じ <i>name</i> 引数を入力します。</li> </ul>

## 例

ここでは、次の内容について説明します。

- [Cisco Unified Communications Manager 4.X.X およびそれ以前のバージョンの例 \(P.172\)](#)
- [Cisco Unified Communications Manager 5.0 およびそれ以降のバージョンの例 \(P.175\)](#)

## Cisco Unified Communications Manager 4.X.X およびそれ以前のバージョンの例

次の例は、Cisco Unified SRST ルータ (Cisco 7970、7960、PEM) にインポートされた 3 つの証明書を示しています。

```
Router(config)# crypto pki trustpoint 7970
Router(ca-trustpoint)# revocation-check none
Router(ca-trustpoint)# enrollment terminal
Router(ca-trustpoint)# exit
Router(config)# crypto pki authenticate 7970
```

```
Enter the base 64 encoded CA certificate.
End with a blank line or the word "quit" on a line by itself
MIIDQCcCApCgAwIBAgIQNT+yS9cPFKNGwfOprHJWdTANBgkqhkiG9w0BAQUFADAu
MRYwFAYDVQQKEw1DaXNjbjBTExN0ZW1zMRQwEgYDVQQDEwtdQVAtUlRQLTAwMjAe
Fw0wMzEwMTAyMDE4NDlaFw0yMzEwMTAyMDI3MzdaMC4xZjAUBGNVBAoTDUNpc2Nv
IFN5c3R1bXN5c3R1bXN5c3R1bXN5c3R1bXN5c3R1bXN5c3R1bXN5c3R1bXN5c3R1
AAOCAQ0AMIIBCAKCAQEAAxZlBK19w/2NZVVvpjCPrpW1cCY7V1q9lhZ185RZZdnQ
2M4CufgIzNa3zYxGJIAYeFfcRECNMB3f5A+x7xNiEuZB87UPvK+7S80uWCY0Uht1
AVVf5NQgZ3YDNoNXg5MmONb81T86F55EzYVacOXGne77TSIbIdejrTgYQXGP2MJx
Qhg+ZQlGFDRzbhFM84Duv2Msez+1+SqmQ080kIckqE9Nr3/XCSj1hXZNNVg8D+mv
Hth2P6KZqAKXAAStGRLSZX3jNbS8tveJ3Gi5+s9+66KKK2PD0iDwHcRkKcUhb7g
1I++U/5nswjUDIAPH715Ds2rn9ehkMGipGLF8kpuCwIBA60BwzCBwDALBgNVHQ8E
BAMCAYYwDwYDVR0TAQH/BAUwAwEB/zAdBgNVHQ4EFgQUUpIr4ojuLgmKTn5wLFal
mrTUm5YwbwYDVR0fBGgwZjBkoGKgYIYtaHR0cDovL2Nhcn1yYDhAtMDAyL0N1cnRf
bnJvbGwvQ0FQLVJUUC0wMDIuY3Jshi9maWx10i8vXFxjYXAtcnRwLTAwM1xZXXJ0
RW5yb2xsXENBUC1SVFAtMDAyLmNybnDAQBgkrBgEAAI3FQEEAwIBADANBgkqhkiG
9w0BAQUFAAOCAQEAVoOM78TaOtHqj7sVL/5u5VChlyvU168f0piJLNWip2vDRihm
E+DlXdwMS5JaquTuaSd/m/xzxpCRJm4ZRRwPq6VeaiiQGkjFuZEe5jSKiSAK7eHg
tup4HP/ZfKSwPA40DlsGSYsKNMm3OmVOCQUMH021PkS/eEQ9sIw6QS7uuHN4y4CJ
NPNRbpFRLw06hnStCZHTGpKEHnY213QOy3h/EWhbnpOMZ+hdr20FuJsi6G1+L39l
aRjed708f2fYoz9wnEpZbnt2Kzse3uhU1Ygq1D1x9yuPq388C18HWdmCj4OVTXux
V6Y47H1yv/GJM8FvdgvKlExbGTFnlHpPiaG9tQ==
```

**quit**

```
Certificate has the following attributes:
Fingerprint MD5: F7E150EA 5E6E3AC5 615FC696 66415C9F
Fingerprint SHA1: 1BE2B503 DC72EE28 0C0F6B18 798236D8 D3B18BE6
% Do you accept this certificate? [yes/no]: y
Trustpoint CA certificate accepted.
% Certificate successfully imported
```

```
Router(config)# crypto pki trustpoint 7960
Router(ca-trustpoint)# revocation-check none
Router(ca-trustpoint)# enrollment terminal
Router(ca-trustpoint)# exit
Router(config)# crypto pki authenticate 7960
```

```
Enter the base 64 encoded CA certificate.
End with a blank line or the word "quit" on a line by itself
MIICKDCCAzGgAwIBAgIC8wEwDQYJKoZIhvcNAQEFBQAwQDELMAkGA1UEBhMCVVMx
GjAYBgNVBAoTEUNpc2NvIFN5c3R1bXN5c3R1bXN5c3R1bXN5c3R1bXN5c3R1bXN5
QzAwHhcNMDQwNzE1MjIzODMyWWhcNMTkwNzEyMjIzODMxWjBAMQswCQYDVQQGEwJV
UzEaMBGGA1UEChMRQ21zY28gU31zdGVtcyBjb21xZmFATBGNVBAoTDUNpc2NvIFN5
RDBDMDCBnzANBgkqhkiG9w0BAQEFAAOBjQAwYkCgYEA0hvMOZZ9ENYWme11YGY1
it2rvE3Nk/eqhmv8P9eqBliqt+ffBeAG0WZ5b05FetdU+BCmPnddvAeSpsfr3Z+h
x+r58f0EIBRHQLgndZ+nnYH39uwXcRWWqWw1W147YHjV7M5c/R8T6daCx4B5NBo6
kdQdQNOvR3IP7kQaCShdM/kCAwEAAMxMC8wDgYDVR0PAQH/BAQDAgKEMB0GA1Ud
JQQwMBGQCcGAQUFBwMBBggrBgEFBQcDBTANBgkqhkiG9w0BAQUFAAOBGGCaNi6x
sL6M5N1DezpsB03QmUVyXMFronV2ysrSwcXzHu0gJ9MSJ8TwiQmVaJ47hST1F5a8
YVYJ0IdifXbXRo+/EEO7kkmFE8MZta5rM7UWj8bAer42iqA3RzQaDwuJgNWT9Fhh
GgfuNAlo5h1AikxsvxivmD1LdZyCMoqJJd7B2Q==
```

**quit**

```
Certificate has the following attributes:
Fingerprint MD5: 4B9636DF 0F3BA6B7 5F54BE72 24762DBC
Fingerprint SHA1: A9917775 F86BB37A 5C130ED2 3E528BB8 286E8C2D
% Do you accept this certificate? [yes/no]: y
Trustpoint CA certificate accepted.
% Certificate successfully imported
```

```
Router(config)# crypto pki trustpoint PEM
Router(ca-trustpoint)# revocation-check none
Router(ca-trustpoint)# enrollment terminal
Router(ca-trustpoint)# exit
Router(config)# crypto pki authenticate PEM
```

Enter the base 64 encoded CA certificate.

End with a blank line or the word "quit" on a line by itself

```
MIIDqDCCApCgAwIBAgIQdhL5YBU9b590QiAgMrcjVjANBgkqhkiG9w0BAQUFADAu
MRYwFAYDVQQKEw1DaXNjbyBTcXN0ZW1zMRQwEgYDVQQDEwtDQVAtU1RQLTAwMTAe
Fw0wMzAyMDYyMzI3MTNaFw0yMzAyMDYyMzI3MzRaMC4xZjAUBgNVBAAoTDUNpc2Nv
IFN5c3RlbnRlcXN0b3R5b250b3R5b250b3R5b250b3R5b250b3R5b250b3R5b250
AAOCAQ0AMIIBCAKCAQEARFW77Rjem4cJ/7yPLVCauDohwZZ/3qf0sJaWLLeAzBlq
Rj2lFlSij0ddkDtfEEo9VKmBOJsvx6xJlWJiuBwUMDhTRbsuJz+npkaGBXPOXJmN
Vd54q1pc/hQDfWlbrIFkCcYhHws7vvnPsLuy1Kw2L2cP0UXxYghSsx8H4vGqdPFQ
NnYy7aKJ43SvDFt4zn37n8jrVlRuz0x3mdbcBEdHbA825Yo7a8skl2tshMJ/YdMm
vny0pmDNZxmeHjQegV03UFUn6GVCO+K1y1dUU1qpYJNYtqLkqj7wgccGjsHdHr3a
U+bw1uLgSGSgQnxMWeMaWo8+6hMxw1ANPweufgZMaywIBA60BwzCBwDALBgNVHQ8E
BAMCAYYwDwYDVR0TAQH/BAUwAwEB/zAdBgNVHQ4EFgQU6Rexgscfz6ypG270qSac
cK4FoJowbwYDVR0fBGgwZjBkoGKgYIYtaHR0cDovL2NhcC1ydHAtMDAxL0N1cnRF
bnJvbGwvQ0FQLVJUUC0wMDEuY3Jshi9maWx1oi8vXFxjYXAtcnRwLTAwMVxZXXJ0
RW5yb2xsXENBUC1SVFAtMDAxLmNybdAQBgkrBgEEAYI3FQEEAwIBADANBgkqhkiG
9w0BAQUFAAOCAQEAg2T96/YMMtw2Dw4QX+F1+g1XSrUCrNyjx7vtFaRDHyB+kobw
dwkphfzkfTyYpJELzV1r+kMRoyuZ7oIqqccEroMDnmeApc+BRGbDJqS1Zzk4OA
c6Ea7fm53nQRlcSPmUVLjDBzKYDNbnEji zptaIC5fgB/S9S6C1q0YpTZFn5tjUjy
WXzeYSXPrxcb0UH7IQJlogpONAAUKLoPaZU7tVDSH3hD4+VjmLyysaLUhksGFrrN
phzZrsVvilk17qpqCP1lKLGAS4fSbkruq3r/6S/SpXS6/gAoljBKixP7ZW2PxcGU
1aU9cURLP095NDOFN3jBk3Sips7cVidcogowPQ==
```

**quit**

Certificate has the following attributes:

Fingerprint MD5: 233C8E33 8632EA4E 76D79FEB FFB061C6

Fingerprint SHA1: F7B40B94 5831D2AB 447AB8F2 25990732 227631BE

% Do you accept this certificate? [yes/no]: **y**

Trustpoint CA certificate accepted.

% Certificate successfully imported

登録が成功し、5 つの CA 証明書が許可されたことを表示するには、`show crypto pki trustpoint status` コマンドを使用します。5 つの証明書には、入力したばかりの 3 つの証明書、CA サーバの証明書、および SRST ルータの証明書が含まれます。

```
Router# show crypto pki trustpoint status

Trustpoint 7970:
Issuing CA certificate configured:
Subject Name:
cn=CAP-RTP-002,o=Cisco Systems
Fingerprint MD5: F7E150EA 5E6E3AC5 615FC696 66415C9F
Fingerprint SHA1: 1BE2B503 DC72EE28 0C0F6B18 798236D8 D3B18BE6
State:
Keys generated ..... Yes (General Purpose)
Issuing CA authenticated ..... Yes
Certificate request(s) ..... None

Trustpoint 7960:
Issuing CA certificate configured:
Subject Name:
cn=CAPF-508A3754,o=Cisco Systems Inc,c=US
Fingerprint MD5: 6BAE18C2 0BCE391E DAE2FE4C 5810F576
Fingerprint SHA1: B7735A2E 3A5C274F C311D7F1 3BE89942 355102DE
State:
Keys generated ..... Yes (General Purpose)
Issuing CA authenticated ..... Yes
Certificate request(s) ..... None

Trustpoint PEM:
Issuing CA certificate configured:
Subject Name:
cn=CAP-RTP-001,o=Cisco Systems
Fingerprint MD5: 233C8E33 8632EA4E 76D79FEB FFB061C6
Fingerprint SHA1: F7B40B94 5831D2AB 447AB8F2 25990732 227631BE
State:
Keys generated ..... Yes (General Purpose)
Issuing CA authenticated ..... Yes
Certificate request(s) ..... None

Trustpoint srstcaserver:
Issuing CA certificate configured:
Subject Name:
cn=srstcaserver
Fingerprint MD5: 6AF5B084 79C93F2B 76CC8FE6 8781AF5E
Fingerprint SHA1: 47D30503 38FF1524 711448B4 9763FAF6 3A8E7DCF
State:
Keys generated ..... Yes (General Purpose)
Issuing CA authenticated ..... Yes
Certificate request(s) ..... None

Trustpoint srstca:
Issuing CA certificate configured:
Subject Name:
cn=srstcaserver
Fingerprint MD5: 6AF5B084 79C93F2B 76CC8FE6 8781AF5E
Fingerprint SHA1: 47D30503 38FF1524 711448B4 9763FAF6 3A8E7DCF
Router General Purpose certificate configured:
Subject Name:
serialNumber=F3246544+hostname=c2611XM-sSRST.cisco.com
Fingerprint: 35471295 1C907EC1 45B347BC 7A9C4B86
State:
Keys generated ..... Yes (General Purpose)
Issuing CA authenticated ..... Yes
Certificate request(s) ..... Yes
```

## Cisco Unified Communications Manager 5.0 およびそれ以降のバージョンの例

次の例は、Cisco Unified Communications Manager 5.0 を実行するのに必要な 4 つの証明書 (CAPF、CiscoCA、CiscoManufactureCA、および CiscoRootCA2048) の設定を示します。

```
Router(config)# crypto pki trustpoint CAPF
Router(ca-trustpoint)# revocation-check none
Router(ca-trustpoint)# enrollment terminal
Router(ca-trustpoint)# exit
Router(config)# crypto pki authenticate CAPF
```

```
Enter the base 64 encoded CA certificate.
End with a blank line or the word "quit" on a line by itself
MIICKjCCAzoGAWIBAgIC8wEwDQYJKoZIhvcNAQEFBQAwQTELMakGA1UEBhMCVVMx
GjAYBgNVBAoTEUNpc2NvIFN5c3RlbXMGSW5jMRYwFAYDVQQDEw1DQVBGLTU4RUFE
MkQyYmB4XDTA2MDMwMTIxMjc1Ml0XDTIxMDIyNTIxMjc1MVowQTELMakGA1UEBhMC
VVMxGjAYBgNVBAoTEUNpc2NvIFN5c3RlbXMGSW5jMRYwFAYDVQQDEw1DQVBGLTU4
RUFEMkQyMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC99KgZT94qhozw4bOB
f8Z0tYwT214L++mC6403s3AshDi8xe8Y8sN/f/ZKRRhNIXBlK4SWafXnHKJBqKZn
WtSgkRjJ3Dh0XtqcWYt8VS2sC69g8sX091skK13m+TpWsr2T/mDXv6CceaKN+mch
gcrnNo8kamOOIG8OsQc4L6XzQIDAQABoZEWLzAOBGNVHQ8BAf8EBAMCAoQwHQYD
quit
Certificate has the following attributes:
Fingerprint MD5: 1951DJ4E 76D79FEB FFB061C6 233C8E33
Fingerprint SHA1: 222891BE Z7B89B94 447AB8F2 5831D2AB 25990732
% Do you accept this certificate? [yes/no]: y
Trustpoint CA certificate accepted.
% Certificate successfully imported
```

```
Router(config)# crypto pki trustpoint CiscoCA
Router(ca-trustpoint)# revocation-check none
Router(ca-trustpoint)# enrollment terminal
Router(ca-trustpoint)# exit
Router(config)# crypto pki authenticate CiscoCA
```

```
Enter the base 64 encoded CA certificate.
End with a blank line or the word "quit" on a line by itself
MIIDqDCCApCgAwIBAgIQdhlL5YBU9b590QiAgMrcjVjANBgkqhkiG9w0BAQUFADAu
MRYwFAYDVQQKEw1DaXNjbyBTeXN0ZW1zMRQwEgYDVQQDEw1DQVAtU1RQLTAwMTAe
Vd54qlpc/hQDFw1brIFkCcYhHws7vwnPsLuy1Kw2L2cP0UXxYghSsx8H4vGqdPFQ
NnYy7aKJ43SvDFt4zn37n8jrv1Ruz0x3mdbcBEedHbA825Yo7a8sk12tshMJ/YdMm
vny0pmDNZxmeHjqEgV03UFUn6GVCO+K1y1dUU1qpYJNYtqLkqj7wgccGjsHdHr3a
U+bw1uLgSGsQnxMWeMaWo8+6hMxw1ANPweufgZMaywIBA60BwzCBwDALBgNVHQ8E
c6Ea7fm53nQRlCSpmUVLjDBzKYDNbnEjiZptaIC5fgB/S9S6C1q0YpTZFn5tjUjy
WXzeYSXPrxcb0UH7IQJlogpONAAUKLoPaZU7tVDSH3hd4+VjmLyysaLUhksGFrrN
phzZrsVvllK17qpqCPl1KLGAS4fSbkruq3r/6S/SpXS6/gAoljBKixP7ZW2PxcGU
1aU9cURLP095NDOFN3jBk3Sips7cVidcogowPQ==
quit
Certificate has the following attributes:
Fingerprint MD5: 21956CBR 4B9706DF 0F3BA6B7 7P54AZ72
Fingerprint SHA1: A9917775 F86BB37A 7H130ED2 3E528BB8 286E8C2D
% Do you accept this certificate? [yes/no]: y
Trustpoint CA certificate accepted.
% Certificate successfully imported
```

```
Router(config)# crypto pki trustpoint CiscoManufactureCA
Router(ca-trustpoint)# revocation-check none
Router(ca-trustpoint)# enrollment terminal
Router(ca-trustpoint)# exit
Router(config)# crypto pki authenticate CiscoManufactureCA
```

```
Enter the base 64 encoded CA certificate.
End with a blank line or the word "quit" on a line by itself
MIIE2TCCA8GgAwIBAgIKamlnswAAAAAAZANBgkqhkiG9w0BAQUFADA1MRywFAYD
D/g2qgfEMkHFp68dGf/2c5k5WnNnYhM0DR9e1XBSZBcG7FncXNtq6jUAQQIBA6OC
AecwggHjMBIGA1UdEwEB/wQIMAYBAf8CAQAwHQYDVQ00BBYEFNFDFiarT0Zg7K4F
kcfCWtGwR/dsMASGALUdDwQEAWIBhJAQBgkrBgEEAYI3FQEEAwIBADAZBgkrBgEE
AYI3FAIEDB4KAFMADQBiAEMAQTAfBgNVHSMEGDAwBQn88gVHm6aAgkWrSugiWBF
2nsvqjBDBgNVHR8EPDA6MDIgdGQhZjodHRwOi8vd3d3LmNpc2NvLmNvbS9zZWN1
```

```

cml0eS9wa2kvY3JsL2NyY2EyMDQ4LmNybDBQBggrBgEFBQcBAQREMEIwQAYIKwYB
BQUHMAKGNGh0dHA6Ly93d3cuY2l1zY28uY29tL3N1Y3VyaXR5L3BraS9jZXJ0cy9j
cmNhMjA0OC5jZlIwXAYDVR0gBFUwUzBRBgorBgEEAQkVAQIAMEMwQQYIKwYBBQUH
I+i6itvaSN6go4cTAnPpE+rhC836WVg0ZrG2PML9d7QJwBcbx2RvdFOWFEdyeP3
OOFTC9Fovo4ipUsG4eakqjN9GnW6JvNwxmEApCn5J1unGdGTjaubEBEPH6GC/f08
S2513JNFBemvM2tnIwcGhiLa69yHz1khQhrpz3B1iOAKPV19TpY4gJfVb/Cbcdi6
YBmlsGGGrd11Zva5J6LuL2GbuqEwYf2+rDUU+bgtlwavw+9tzD0865XpgdOKXrbO
+nmka9eiV2TEP0zJ2+iC7AFm1BCIo1blPFft6QKoSJFjB6thJksaE5/k3Npf
quit
Certificate has the following attributes:
Fingerprint MD5: 0F3BA6E7 4B9636DF 5F54BE72 24762SBR
Fingerprint SHA1: L92BB37A S9919925 5C130ED2 3E528UP8 286E8C2D
% Do you accept this certificate? [yes/no]: y
Trustpoint CA certificate accepted.
% Certificate successfully imported

Router(config)# crypto pki trustpoint CiscoRootCA2048
Router(ca-trustpoint)# revocation-check none
Router(ca-trustpoint)# enrollment terminal
Router(ca-trustpoint)# exit
Router(config)# crypto pki authenticate CiscoRootCA2048

Enter the base 64 encoded CA certificate.
End with a blank line or the word "quit" on a line by itself
MIIDQzCCAiuGAWIBAgIQX/h7KctU3I1CoxW1aMmt/zANBgkqhkiG9w0BAQUFADA1
MRYwFAYDVQQKEw1DaXNjbyBTeXN0ZW1zMRswGQYDVQQDExJDhDaXNjbyBSb290IENB
IDIwNDgwHhcNMDQwNTE0MjAxNzEyWhcNMjkwNTE0MjAyNTQyWjA1MRYwFAYDVQQK
Ew1DaXNjbyBTeXN0ZW1zMRswGQYDVQQDExJDhDaXNjbyBSb290IENBIDIwNDgwggEg
MA0GCsQGSIb3DQEBAQUAA4IBDQAwggEIAoIBAQCWmrmrp68Kd6ficba0ZmKUEIhH
FR5umgIJFq0roIlgX9p7L6owEAYJKwYBBAGCNxUBBAMCAQAwDQYJKoZIhvcNAQEF
BQADggEBBAJ2dhISjQa18dwy3U8pORFbi71R803UXHOjgxxkLtv5MOhmBvrBW7hmW
Yppao2TB9k5UM8Z3/sUcuVdJcr18JOagxEu5sv4dEX+5wW4q+ffY0vhN4TauYuX
cB7w4ovXsNgOnbFp1iqRe61JT37mjpXYgyc81WhJdTsd9i7rp77rMKsSH0T81asz
Bvt9YaretIpjsJyp8qS5UwGH0GikJ3+r/+n6yUA4iGe0OcaEb1fJU9u6ju7AQ7L4
CYNu/2bPPu8Xs1gYJQk0XuPL1hS27PKSb3TkL4Eq1ZKR4OCXPDJoBYVL0fdX41Id
kxpUnwVwwEpxYB5DC2Ae/qPOgRnhCzU=
quit
Certificate has the following attributes:
Fingerprint MD5: 2G3LZ6B7 2R1995ER 6KE4WE72 3E528BB8
Fingerprint SHA1: M9912245 5C130ED2 24762JBC 3E528VF8 956E8S5H
% Do you accept this certificate? [yes/no]: y
Trustpoint CA certificate accepted.
% Certificate successfully imported

```

## Secure Cisco Unified SRST ルータへの Cisco Unified Communications Manager の設定

次の作業を Cisco Unified Communications Manager で実行します。

- [Cisco Unified Communications Manager への SRST リファレンスの追加 \(P.176\)](#) (必須)
- [Cisco Unified Communications Manager での SRST フォールバックの設定 \(P.178\)](#) (必須)
- [Cisco Unified Communications Manager への CAPF の設定 \(P.180\)](#) (必須)

### Cisco Unified Communications Manager への SRST リファレンスの追加

SRST リファレンスを Cisco Unified Communications Manager に追加する手順は、次のとおりです。

この手順に従う前に、Cisco Unified SRST ルータでクレデンシャル サービスが実行されていることを確認してください。Cisco Unified Communications Manager は、デバイスの証明書のために Cisco Unified SRST ルータに接続します。クレデンシャル サービスを有効にするには、[P.167](#) の「[Secure Cisco Unified SRST ルータでのクレデンシャル サービスの有効化](#)」を参照してください。

Cisco Unified Communications Manager に Cisco Unified SRST を追加する方法については、実行している Cisco Unified Communications Manager バージョンの「Survivable Remote Site Telephony Configuration」を参照してください。すべての Cisco Unified Communications Manager アドミニストレーション ガイドは、

[http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod\\_maintenance\\_guides\\_list.html](http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html) にあります。

## 要約手順

1. Cisco Unified Communications Manager メニュー バーの **SRST** を選択します。
2. 新しい SRST リファレンスを追加します。
3. SRST フィールドに適切な設定値を入力します。
4. **Insert** をクリックします。
5. 他の SRST リファレンスについて、手順 2 ~ 4 を繰り返します。

## 詳細手順

- 
- ステップ 1** Cisco Unified Communications Manager のメニュー バーで、**CCMAdmin > System > SRST** の順に選択します。
- ステップ 2** **Add New SRST Reference** をクリックします。
- ステップ 3** 適切な設定値を入力します。図 9 に、SRST Reference Configuration ウィンドウで使用可能なフィールドを示します。
- a. SRST ゲートウェイの名前、IP アドレス、およびポートを入力します。
  - b. SRST ゲートウェイが安全かどうかを尋ねるボックスをオンにします。
  - c. 証明書プロバイダー（クレデンシャル サービス）のポート番号を入力します。クレデンシャル サービスは、デフォルトのポート 2445 で実行されます。

図9 SRST Reference Configuration ウィンドウ

System Route Plan Service Feature Device User Application Help

Cisco CallManager Administration  
For Cisco IP Telephony Solutions

Cisco Systems

**SRST Reference Configuration** [Add New SRST Reference](#)  
[Back to Find/List SRST References](#)

SRST Reference: New  
Status: Ready

SRST Reference Name\*

IP Address\*

Port\*

Is SRST Secure?

SRST Certificate Provider Port\*

\* indicates required item

127030

**ステップ 4** 新しい SRST リファレンスを追加するには、**Insert** をクリックします。「Status: Insert completed」メッセージが表示されます。

**ステップ 5** さらに SRST リファレンスを追加するには、手順 2 ~ 4 を繰り返します。

## Cisco Unified Communications Manager での SRST フォールバックの設定

デバイス プールを SRST に割り当てることにより、Cisco Unified Communications Manager に SRST フォールバックを設定する手順は、次のとおりです。

デバイス プールを Cisco Unified Communications Manager に追加する方法については、実行している Cisco Unified Communications Manager バージョンの『Cisco Unified Communications Manager Administration Guide』の「Device Pool Configuration」を参照してください。すべての Cisco Unified Communications Manager アドミニストレーション ガイドは、

[http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod\\_maintenance\\_guides\\_list.html](http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html) にあります。

### 要約手順

1. Cisco Unified Communications Manager メニュー バーの **Device Pool** を選択します。
2. デバイス プールを追加します。
3. **Add New Device Pool** をクリックします。
4. SRST リファレンスを入力します。
5. **Update** をクリックします。



## 詳細手順

- ステップ 1** Cisco Unified Communications Manager のメニュー バーで、**CCMAdmin > System > Device Pool** の順に選択します。
- ステップ 2** デバイス プールを追加するには、次のいずれかの方法を使用します。
- 追加するデバイス プールと同様の設定を持つデバイス プールがすでに存在する場合は、設定を表示するために既存のデバイス プールを選択し、**Copy** をクリックして、必要に応じて設定を変更してください。**ステップ 4**に進みます。
  - 既存のものをコピーせずにデバイス プールを追加するには、**ステップ 3**に進みます。
- ステップ 3** ウィンドウの右上隅で、**Add New Device Pool** リンクをクリックします。Device Pool Configuration ウィンドウが表示されます ( [図 10](#) を参照 )。

**図 10** Device Pool Configuration ウィンドウ

The screenshot shows the 'Device Pool Configuration' window in Cisco CallManager Administration. The page title is 'Device Pool Configuration' and it includes a navigation bar with 'System', 'Route Plan', 'Service', 'Feature', 'Device', 'User', 'Application', and 'Help'. The main content area shows the configuration for a 'Default' device pool with 13 members. The status is 'Ready'. There are buttons for 'Copy', 'Update', 'Delete', and 'Reset Devices'. The 'Device Pool Settings' section includes the following fields:

Device Pool Name*	Default
Cisco CallManager Group*	Default
Date/Time Group*	CMLocal
Region*	Default
Softkey Template*	Standard User
SRST Reference*	jiso2691
Calling Search Space for Auto-registration	— Not Selected —
Media Resource Group List	Disable
Network Hold MOH Audio Source	Use Default Gateway
User Hold MOH Audio Source	jiso2691
Network Locale	SRST GW
	< None >
	< None >

- ステップ 4** SRST リファレンスを入力します。
- ステップ 5** **Update** をクリックして、デバイス プール情報をデータベースに保存します。

## Cisco Unified Communications Manager への CAPF の設定

CAPF プロセスでは、Cisco Unified Communications Manager などのサポート対象デバイスが、Cisco Unified IP Phone から LSC 証明書を要求できます。CAPF コーティリティは、キー ペアおよび CAPF に特有の証明書を生成し、クラスタ内のすべての Cisco Unified Communications Manager サービスにこの証明書をコピーします。

Cisco Unified Communications Manager への CAPF の設定方法については、『[Cisco IP Phone Authentication and Encryption for Cisco Communications Manager](#)』を参照してください。

## Secure Cisco Unified SRST ルータでの SRST モードの有効化

Cisco Unified IP Phone 機能をサポートするようにルータ上の Secure SRST を設定するには、global コンフィギュレーション モードを開始して、次のコマンドを使用します。

### 要約手順

1. `call-manager-fallback`
2. `secondary-dialtone digit-string`
3. `transfer-system {blind | full-blind | full-consult | local-consult}`
4. `ip source-address ip-address [port port]`
5. `max-ephones max-phones`
6. `max-dn max-directory-numbers`
7. `transfer-pattern transfer-pattern`
8. `exit`

### 詳細手順

	コマンドまたはアクション	目的
ステップ 1	<code>call-manager-fallback</code>  例: Router(config)# call-manager-fallback	call-manager-fallback コンフィギュレーション モードを開始します。
ステップ 2	<code>secondary-dialtone digit-string</code>  例: Router(config-cm-fallback)# secondary-dialtone 9	数字列がダイヤルされたときに第 2 発信音をアクティブにします。

	コマンドまたはアクション	目的
ステップ 3	<p><b>transfer-system</b> {<i>blind</i>   <i>full-blind</i>   <i>full-consult</i>   <i>local-consult</i>}</p> <p>例: Router(config-cm-fallback)# transfer-system full-consult</p>	<p>Cisco Unified SRST ルータが提供するすべての回線のコール転送方法を定義します。</p> <ul style="list-style-type: none"> <li>• <b>blind</b>: シスコ独自の方法を使用して、単一電話回線で、打診を行わずにコールを転送します。</li> <li>• <b>full-blind</b>: H.450.2 標準方式を使用して、打診を行わずにコールを転送します。</li> <li>• <b>full-consult</b>: 使用可能な 2 番目の電話回線を使用し、打診を行ってコールを転送します。2 番目の回線が使用できない場合、コールは <b>full-blind</b> にフォールバックします。</li> <li>• <b>local-consult</b>: 使用可能な 2 番目の電話回線を使用し、ローカルで打診を行ってコールを転送します。打診先または転送先がローカル以外の場合、コールは <b>blind</b> にフォールバックします。</li> </ul>
ステップ 4	<p><b>ip source-address</b> <i>ip-address</i> [<i>port port</i>]</p> <p>例: Router(config-cm-fallback)# ip source-address 10.1.1.22 port 2000</p>	<p>指定した IP アドレスを使用してルータが Cisco IP Phone からメッセージを受信できるようにし、厳密な IP アドレスの検証を提供します。デフォルトのポート番号は 2000 です。</p>
ステップ 5	<p><b>max-ephones</b> <i>max-phones</i></p> <p>例: Router(config-cm-fallback)# max-ephones 15</p>	<p>ルータがサポートできる Cisco IP Phone の最大数を設定します。最大数は、プラットフォームによって異なります。デフォルトは 0 です。詳細については、<a href="#">P.31 の「プラットフォームとメモリのサポート」</a>を参照してください。</p>
ステップ 6	<p><b>max-dn</b> <i>max-directory-numbers</i></p> <p>例: Router(config-cm-fallback)# max-dn 30</p>	<p>ルータがサポート可能な DN または仮想音声ポートの最大数を設定します。</p> <ul style="list-style-type: none"> <li>• <b>max-directory-numbers</b>: ルータでサポートされる電話番号または仮想音声ポートの最大数。最大数は、プラットフォームによって異なります。デフォルトは 0 です。詳細については、<a href="#">P.31 の「プラットフォームとメモリのサポート」</a>を参照してください。</li> </ul>
ステップ 7	<p><b>transfer-pattern</b> <i>transfer-pattern</i></p> <p>例: Router(config-cm-fallback)# transfer-pattern .....</p>	<p>Cisco Unified IP Phone による電話コールを指定の電話番号パターンに転送できるようにします。</p> <ul style="list-style-type: none"> <li>• <b>transfer-pattern</b>: 許可するコール転送の数字列。ワイルドカードが使用可能です。</li> </ul>
ステップ 8	<p><b>exit</b></p> <p>例: Router(config-cm-fallback)# exit</p>	<p>call-manager-fallback コンフィギュレーション モードを終了します。</p>

## 例

次の例では、ルータで SRST モードを有効にします。

```
Router(config)# call-manager-fallback
Router(config-cm-fallback)# secondary-dialtone 9
Router(config-cm-fallback)# transfer-system full-consult
Router(config-cm-fallback)# ip source-address 10.1.1.22 port 2000
Router(config-cm-fallback)# max-ephones 15
Router(config-cm-fallback)# max-dn 30
Router(config-cm-fallback)# transfer-pattern .....
Router(config-cm-fallback)# exit
```

## 電話機のステータスおよび登録の確認

Cisco Unified IP Phone のステータスおよび登録について、確認またはトラブルシューティングを行うには、特権 EXEC モードを開始して、次の手順を実行します。

### 要約手順

1. `show ephone`
2. `show ephone offhook`
3. `show voice call status`
4. `debug ephone register`
5. `debug ephone state`

### 詳細手順

#### ステップ 1 `show ephone`

登録された Cisco Unified IP Phone およびその機能を表示するには、このコマンドを使用します。`show ephone` コマンドは、Secure SRST に対して使用されると、認証と暗号化のステータスも表示します。この例では、TLS 接続で認証と暗号化のステータスがアクティブになっています。

```
Router# show ephone
```

```
ephone-1 Mac:1000.1111.0002 TCP socket:[5] activeLine:0 REGISTERED in SCCP ver 5  
+ Authentication + Encryption with TLS connection  
mediaActive:0 offhook:0 ringing:0 reset:0 reset_sent:0 paging 0 debug:0  
IP:10.1.1.40 32626 7970 keepalive 390 max_line 8  
button 1: dn 14 number 2002 CM Fallback CH1 IDLE
```

```
ephone-2 Mac:1000.1111.000B TCP socket:[12] activeLine:0 REGISTERED in SCCP ver  
5 + Authentication + Encryption with TLS connection  
mediaActive:0 offhook:0 ringing:0 reset:0 reset_sent:0 paging 0 debug:0  
IP:10.1.1.40 32718 7970 keepalive 390 max_line 8  
button 1: dn 21 number 2011 CM Fallback CH1 IDLE
```

```
ephone-3 Mac:1000.1111.000A TCP socket:[16] activeLine:0 REGISTERED in SCCP ver  
5 + Authentication + Encryption with TLS connection  
mediaActive:0 offhook:0 ringing:0 reset:0 reset_sent:0 paging 0 debug:0  
IP:10.1.1.40 32862 7970 keepalive 390 max_line 8  
button 1: dn 2 number 2010 CM Fallback CH1 IDLE
```

## ステップ 2 show ephone offhook

Cisco IP Phone のステータスおよびオフフック状態のすべての電話機の品質を表示するには、このコマンドを使用します。この例では、TLS 接続で認証と暗号化のステータスがアクティブで、さらにアクティブな保護されたコールが存在します。

```
Router# show ephone offhook

ephone-1 Mac:1000.1111.0002 TCP socket:[5] activeLine:1 REGISTERED in SCCP ver 5
+ Authentication + Encryption with TLS connection
mediaActive:1 offhook:1 ringing:0 reset:0 reset_sent:0 paging 0
:0
IP:10.1.1.40 32626 7970 keepalive 391 max_line 8
button 1: dn 14 number 2002 CM Fallback CH1 CONNECTED
Active Secure Call on DN 14 chan 1 :2002 10.1.1.40 29632 to 10.1.1.40 25616 via
10.1.1.40
G711Ulaw64k 160 bytes no vad
Tx Pkts 295 bytes 49468 Rx Pkts 277 bytes 46531 Lost 0
Jitter 0 Latency 0 callingDn 22 calledDn -1

ephone-2 Mac:1000.1111.000B TCP socket:[12] activeLine:1 REGISTERED in SCCP ver
5 + Authentication + Encryption with TLS connection
mediaActive:1 offhook:1 ringing:0 reset:0 reset_sent:0 paging 0 debug:0
IP:10.1.1.40 32718 7970 keepalive 391 max_line 8
button 1: dn 21 number 2011 CM Fallback CH1 CONNECTED
Active Secure Call on DN 21 chan 1 :2011 10.1.1.40 16382 to 10.1.1.40 16382 via
10.1.1.40
G711Ulaw64k 160 bytes no vad
Tx Pkts 295 bytes 49468 Rx Pkts 277 bytes 46531 Lost 0
Jitter 0 Latency 0 callingDn -1 calledDn 11
```

## ステップ 3 show voice call status

Cisco Unified SRST ルータのすべての音声ポートのコール ステータスを表示するには、このコマンドを使用します。このコマンドは、2つのPOTSダイヤルピア間のコールには適用できません。

```
Router# show voice call status

CallID CID ccVdb Port DSP/Ch Called # Codec Dial-peers
0x1164 2BFE 0x8619A460 50/0/35.0 2014 g711ulaw 20035/20027
0x1165 2BFE 0x86144B78 50/0/27.0 *2014 g711ulaw 20027/20035
0x1166 2C01 0x861043D8 50/0/21.0 2012 g711ulaw 20021/20011
0x1168 2C01 0x860984C4 50/0/11.0 *2012 g711ulaw 20011/20021
0x1167 2C04 0x8610EC7C 50/0/22.0 2002 g711ulaw 20022/20014
0x1169 2C04 0x860B8894 50/0/14.0 *2002 g711ulaw 20014/20022
0x116A 2C07 0x860A374C 50/0/12.0 2010 g711ulaw 20012/20002
0x116B 2C07 0x86039700 50/0/2.0 *2010 g711ulaw 20002/20012
0x116C 2C0A 0x86119520 50/0/23.0 2034 g711ulaw 20023/20020
0x116D 2C0A 0x860F9150 50/0/20.0 *2034 g711ulaw 20020/20023
0x116E 2C0D 0x86088DC20 50/0/10.0 2022 g711ulaw 20010/20008
0x116F 2C0D 0x86078AD8 50/0/8.0 *2022 g711ulaw 20008/20010
0x1170 2C10 0x861398F0 50/0/26.0 2016 g711ulaw 20026/20028
0x1171 2C10 0x8614F41C 50/0/28.0 *2016 g711ulaw 20028/20026
0x1172 2C13 0x86159CC0 50/0/29.0 2018 g711ulaw 20029/20004
0x1173 2C13 0x8604E848 50/0/4.0 *2018 g711ulaw 20004/20029
0x1174 2C16 0x8612F04C 50/0/25.0 2026 g711ulaw 20025/20030
0x1175 2C16 0x86164F48 50/0/30.0 *2026 g711ulaw 20030/20025
0x1176 2C19 0x860D8C64 50/0/17.0 2032 g711ulaw 20017/20018
0x1177 2C19 0x860E4A008 50/0/18.0 *2032 g711ulaw 20018/20017
0x1178 2C1C 0x860CE3C0 50/0/16.0 2004 g711ulaw 20016/20019
0x1179 2C1C 0x860EE8AC 50/0/19.0 *2004 g711ulaw 20019/20016
0x117A 2C1F 0x86043FA4 50/0/3.0 2008 g711ulaw 20003/20024
0x117B 2C1F 0x861247A8 50/0/24.0 *2008 g711ulaw 20024/20003
0x117C 2C22 0x8608337C 50/0/9.0 2020 g711ulaw 20009/20031
0x117D 2C22 0x8616F7EC 50/0/31.0 *2020 g711ulaw 20031/20009
```

```

0x117E 2C25 0x86063990 50/0/6.0 2006 g711ulaw 20006/20001
0x117F 2C25 0x85C6BE6C 50/0/1.0 *2006 g711ulaw 20001/20006
0x1180 2C28 0x860ADFF0 50/0/13.0 2029 g711ulaw 20013/20034
0x1181 2C28 0x8618FBBC 50/0/34.0 *2029 g711ulaw 20034/20013
0x1182 2C2B 0x860C3B1C 50/0/15.0 2036 g711ulaw 20015/20005
0x1183 2C2B 0x860590EC 50/0/5.0 *2036 g711ulaw 20005/20015
0x1184 2C2E 0x8617A090 50/0/32.0 2024 g711ulaw 20032/20007
0x1185 2C2E 0x8606E234 50/0/7.0 *2024 g711ulaw 20007/20032
0x1186 2C31 0x861A56E8 50/0/36.0 2030 g711ulaw 20036/20033
0x1187 2C31 0x86185318 50/0/33.0 *2030 g711ulaw 20033/20036
18 active calls found

```

#### ステップ 4 debug ephone register

Cisco IP Phone の登録のプロセスをデバッグするには、このコマンドを使用します。

```
Router# debug ephone register
```

```

EPHONE registration debugging is enabled
*Jun 29 09:16:02.180: New Skinny socket accepted [2] (0 active)
*Jun 29 09:16:02.180: sin_family 2, sin_port 51617, in_addr 10.5.43.177
*Jun 29 09:16:02.180: skinny_socket_process: secure skinny sessions = 1
*Jun 29 09:16:02.180: add_skinny_secure_socket: pid =155, new_sock=0, ip address =
10.5.43.177
*Jun 29 09:16:02.180: skinny_secure_handshake: pid =155, sock=0, args->pid=155, ip
address = 10.5.43.177
*Jun 29 09:16:02.184: Start TLS Handshake 0 10.5.43.177 51617
*Jun 29 09:16:02.184: TLS Handshake retcode OPSSLReadWouldBlockErr
*Jun 29 09:16:03.188: TLS Handshake retcode OPSSLReadWouldBlockErr
*Jun 29 09:16:04.188: TLS Handshake retcode OPSSLReadWouldBlockErr
*Jun 29 09:16:05.188: TLS Handshake retcode OPSSLReadWouldBlockErr
*Jun 29 09:16:06.188: TLS Handshake retcode OPSSLReadWouldBlockErr
*Jun 29 09:16:07.188: TLS Handshake retcode OPSSLReadWouldBlockErr
*Jun 29 09:16:08.188: CRYPTO_PKI_OPSSL - Verifying 1 Certs

*Jun 29 09:16:08.212: TLS Handshake completes

```

#### ステップ 5 debug ephone state

2つの Secure Cisco Unified IP Phone 間のコール設定を見直すには、このコマンドを使用します。**debug ephone state** トレースは、2つの電話機間の暗号化および複合化キーの生成と配布を示します。

```
Router# debug ephone state
```

```

*Jan 11 18:33:09.231:%SYS-5-CONFIG_I:Configured from console by console
*Jan 11 18:33:11.747:ephone-2[2]:OFFHOOK
*Jan 11 18:33:11.747:ephone-2[2]:---SkinnySyncPhoneDnOverlays is onhook
*Jan 11 18:33:11.747:ephone-2[2]:SIEZE on activeLine 0 activeChan 1
*Jan 11 18:33:11.747:ephone-2[2]:SetCallState line 1 DN 2(-1) chan 1 ref 6 TsOffHook
*Jan 11 18:33:11.747:ephone-2[2]:Check Plar Number
*Jan 11 18:33:11.751:DN 2 chan 1 Voice_Mode
*Jan 11 18:33:11.751:dn_tone_control DN=2 chan 1 tonetype=33:DtInsideDialTone onoff=1
pid=232
*Jan 11 18:33:15.031:dn_tone_control DN=2 chan 1 tonetype=0:DtSilence onoff=0 pid=232
*Jan 11 18:33:16.039:ephone-2[2]:Skinny-to-Skinny call DN 2 chan 1 to DN 4 chan 1
instance 1
*Jan 11 18:33:16.039:ephone-2[2]:SetCallState line 1 DN 2(-1) chan 1 ref 6 TsProceed
*Jan 11 18:33:16.039:ephone-2[2]:SetCallState line 1 DN 2(-1) chan 1 ref 6 TsRingOut
*Jan 11 18:33:16.039:ephone-2[2]:callingNumber 6000

*Jan 11 18:33:16.039:ephone-2[2]:callingParty 6000

*Jan 11 18:33:16.039:ephone-2[2]:Call Info DN 2 line 1 ref 6 call state 1 called 6001
calling 6000 origcalled

```

```
*Jan 11 18:33:16.039:ephone-2[2]:Call Info DN 2 line 1 ref 6 called 6001 calling 6000
origcalled 6001 calltype 2
*Jan 11 18:33:16.039:ephone-2[2]:Call Info for chan 1
*Jan 11 18:33:16.039:ephone-2[2]:Original Called Name 6001
*Jan 11 18:33:16.039:ephone-2[2]:6000 calling
*Jan 11 18:33:16.039:ephone-2[2]:6001
*Jan 11 18:33:16.047:ephone-3[3]:SetCallState line 1 DN 4(4) chan 1 ref 7 TsRingIn
*Jan 11 18:33:16.047:ephone-3[3]:callingNumber 6000

*Jan 11 18:33:16.047:ephone-3[3]:callingParty 6000

*Jan 11 18:33:16.047:ephone-3[3]:Call Info DN 4 line 1 ref 7 call state 7 called 6001
calling 6000 origcalled
*Jan 11 18:33:16.047:ephone-3[3]:Call Info DN 4 line 1 ref 7 called 6001 calling 6000
origcalled 6001 calltype 1
*Jan 11 18:33:16.047:ephone-3[3]:Call Info for chan 1
*Jan 11 18:33:16.047:ephone-3[3]:Original Called Name 6001
*Jan 11 18:33:16.047:ephone-3[3]:6000 calling
*Jan 11 18:33:16.047:ephone-3[3]:6001
*Jan 11 18:33:16.047:ephone-3[3]:Ringer Inside Ring On
*Jan 11 18:33:16.051:dn_tone_control DN=2 chan 1 tonetype=36:DtAlertingTone onoff=1
pid=232
*Jan 11 18:33:20.831:ephone-3[3]:OFFHOOK
*Jan 11 18:33:20.831:ephone-3[3]:---SkinnySyncPhoneDnOverlays is onhook
*Jan 11 18:33:20.831:ephone-3[3]:Ringer Off
*Jan 11 18:33:20.831:ephone-3[3]:ANSWER call
*Jan 11 18:33:20.831:ephone-3[3]:SetCallState line 1 DN 4(-1) chan 1 ref 7 TsOffHook
*Jan 11 18:33:20.831:ephone-3[3]:[SEP000DEDAB3EBF]:Answer Incoming call from ephone-(2)
DN 2 chan 1
*Jan 11 18:33:20.831:ephone-3[3]:SetCallState line 1 DN 4(-1) chan 1 ref 7 TsConnected
*Jan 11 18:33:20.831:defer_start for DN 2 chan 1 at CONNECTED
*Jan 11 18:33:20.831:ephone-2[2]:SetCallState line 1 DN 2(-1) chan 1 ref 6 TsConnected
*Jan 11 18:33:20.835:ephone-3[3]:callingNumber 6000

*Jan 11 18:33:20.835:ephone-3[3]:callingParty 6000

*Jan 11 18:33:20.835:ephone-3[3]:Call Info DN 4 line 1 ref 7 call state 4 called 6001
calling 6000 origcalled
*Jan 11 18:33:20.835:ephone-3[3]:Call Info DN 4 line 1 ref 7 called 6001 calling 6000
origcalled 6001 calltype 1
*Jan 11 18:33:20.835:ephone-3[3]:Call Info for chan 1
*Jan 11 18:33:20.835:ephone-3[3]:Original Called Name 6001
*Jan 11 18:33:20.835:ephone-3[3]:6000 calling
*Jan 11 18:33:20.835:ephone-3[3]:6001
*Jan 11 18:33:20.835:ephone-2[2]:Security Key Generation
! Ephone 2 generates a security key.

*Jan 11 18:33:20.835:ephone-2[2]:OpenReceive DN 2 chan 1 codec 4:G711Ulaw64k duration
20 ms bytes 160
*Jan 11 18:33:20.835:ephone-2[2]:Send Decryption Key
! Ephone 2 sends the decryption key.

*Jan 11 18:33:20.835:ephone-3[3]:Security Key Generation
!Ephone 3 generates its security key.

*Jan 11 18:33:20.835:ephone-3[3]:OpenReceive DN 4 chan 1 codec 4:G711Ulaw64k duration
20 ms bytes 160
*Jan 11 18:33:20.835:ephone-3[3]:Send Decryption Key
! Ephone 3 sends its decryption key.

*Jan 11 18:33:21.087:dn_tone_control DN=2 chan 1 tonetype=0:DtSilence onoff=0 pid=232
*Jan 11 18:33:21.087:DN 4 chan 1 Voice_Mode
*Jan 11 18:33:21.091:DN 2 chan 1 End Voice_Mode
*Jan 11 18:33:21.091:DN 2 chan 1 Voice_Mode
*Jan 11 18:33:21.095:ephone-2[2]:OpenReceiveChannelAck:IP 1.1.1.8, port=25552,
dn_index=2, dn=2, chan=1
*Jan 11 18:33:21.095:ephone-3[3]:StartMedia 1.1.1.8 port=25552
*Jan 11 18:33:21.095:DN 2 chan 1 codec 4:G711Ulaw64k duration 20 ms bytes 160
*Jan 11 18:33:21.095:ephone-3[3]:Send Encryption Key
```

```
! Ephone 3 sends its encryption key.

*Jan 11 18:33:21.347:ephone-3[3]:OpenReceiveChannelAck:IP 1.1.1.9, port=17520,
    dn_index=4, dn=4, chan=1
*Jan 11 18:33:21.347:ephone-2[2]:StartMedia 1.1.1.9 port=17520
*Jan 11 18:33:21.347:DN 2 chan 1 codec 4:G711Ulaw64k duration 20 ms bytes 160
*Jan 11 18:33:21.347:ephone-2[2]:Send Encryption Key
!Ephone 2 sends its encryption key.*Jan 11 18:33:21.851:ephone-2[2]::callingNumber
6000

*Jan 11 18:33:21.851:ephone-2[2]::callingParty 6000
*Jan 11 18:33:21.851:ephone-2[2]:Call Info DN 2 line 1 ref 6 call state 4 called 6001
calling 6000 origcalled
*Jan 11 18:33:21.851:ephone-2[2]:Call Info DN 2 line 1 ref 6 called 6001 calling 6000
origcalled 6001 calltype 2
*Jan 11 18:33:21.851:ephone-2[2]:Call Info for chan 1
*Jan 11 18:33:21.851:ephone-2[2]:Original Called Name 6001
*Jan 11 18:33:21.851:ephone-2[2]:6000 calling
*Jan 11 18:33:21.851:ephone-2[2]:6001
```

---



## Secure SRST の設定例

ここでは、次の設定例を示します。

- [Secure SRST : 例 \(P.187\)](#)
- [コントロールプレーン ポリシング : 例 \(P.192\)](#)



(注) この例の IP アドレスとホスト名は架空のものです。

### Secure SRST : 例

ここでは、前の項で特定された設定作業に一致する設定例を示します。この例には、サードパーティ CA の使用は含まれていません。Cisco IOS 証明書サーバを使用して、証明書を生成することを前提とします。

```
Router# show running-config
.
.
.
! Define Unified Communications Manager.
ccm-manager fallback-mgcp
ccm-manager mgcp
ccm-manager music-on-hold
ccm-manager config server 10.1.1.13
ccm-manager config
!
! Define root CA.
crypto pki server srstcaserver
  database level complete
  database url nvram
  issuer-name CN=srstcaserver
!
crypto pki trustpoint srstca
  enrollment url http://10.1.1.22:80
  revocation-check none
!
crypto pki trustpoint srstcaserver
  revocation-check none
  rsakeypair srstcaserver
!
! Define CTL/7970 trustpoint.
crypto pki trustpoint 7970
  enrollment terminal
  revocation-check none
!
crypto pki trustpoint PEM
  enrollment terminal
  revocation-check none
!
! Define CAPF/7960 trustpoint.
crypto pki trustpoint 7960
  enrollment terminal
  revocation-check none
!
! SRST router device certificate.
crypto pki certificate chain srstca
certificate 02
  308201AD 30820116 A0030201 02020102 300D0609 2A864886 F70D0101 04050030
  17311530 13060355 0403130C 73727374 63617365 72766572 301E170D 30343034
  31323139 35323233 5A170D30 35303431 32313935 32323335A 30343132 300F0603
  55040513 08443042 39453739 43301F06 092A8648 86F70D01 09021612 6A61736F
  32363931 2E636973 636F2E63 6F6D305C 300D0609 2A864886 F70D0101 01050003
```

```

4B003048 024100D7 0CC354FB 5F7C1AE7 7A25C3F2 056E0485 22896D36 6CA70C19
C98F9BAE AE9D1F9B D4BE7A67 F3251174 193BB1A3 12946123 E5C1CCD7 A23E6155
FA2ED743 3FB8B902 03010001 A330302E 300B0603 551D0F04 04030205 A0301F06
03551D23 04183016 8014F829 CE97AD60 18D05467 FC293963 C2470691 F9BD300D
06092A86 4886F70D 01010405 00038181 007EB48E CAE9E1B3 D1E7A185 D7F0D565
CB84B17B 1151BD78 B3E39763 59EC650E 49371F6D 99CBD267 EB8ADF9D 9E43A5F2
FB2B18A0 34AF6564 11239473 41478AFC A86E6DA1 AC518E0B 8657CEBB ED2BDE8E
B586FE67 00C358D4 EFDD8D44 3F423141 C2D331D3 1EE43B6E 6CB29EE7 0B8C2752
C3AF4A66 BD007348 D013000A EA3C206D CF
quit
certificate ca 01
30820207 30820170 A0030201 02020101 300D0609 2A864886 F70D0101 04050030
17311530 13060355 0403130C 73727374 63617365 72766572 301E170D 30343034
31323139 34353136 5A170D30 37303431 32313934 3531365A 30173115 30130603
55040313 0C737273 74636173 65727665 7230819F 300D0609 2A864886 F70D0101
01050003 818D0030 81890281 8100C3AF EE1E4BB1 9922A8DA 2BB9DC8E 5B1BD332
1051C9FE 32A971B3 3C336635 74691954 98E765B1 059E24B6 32154E99 105CA989
9619993F CC72C525 7357EBAC E6335A32 2AAF9391 99325BFD 9B8355EB C10F8963
9D8FC222 EE8AC831 71ACD3A7 4E918A8F D5775159 76FBF499 5AD0849D CAA41417
DD866902 21E5DD03 C37D4B28 0FAB0203 010001A3 63306130 0F060355 1D130101
FF040530 030101FF 300E0603 551D0F01 01FF0404 03020186 301D0603 551D0E04
160414F8 29CE97AD 6018D054 67FC2939 63C24706 91F9BD30 1F060355 1D230418
30168014 F829CE97 AD6018D0 5467FC29 3963C247 0691F9BD 300D0609 2A864886
F70D0101 04050003 8181007A F71B25F9 73D74552 25DFD03A D8D1338F 6792C805
47A81019 795B5AAE 035400BB F859DABF 21892B5B E71A8283 08950414 8633A8B2
C98565A6 C09CA641 88661402 ACC424FD 36F23360 ABFF4C55 BB23C66A C80A3A57
5EE85FF8 C1B1A540 E818CE6D 58131726 BB060974 4E1A2F4B E6195522 122457F3
DEDBAAD7 3780136E B112A6
quit
crypto pki certificate chain srstcaserver
certificate ca 01
30820207 30820170 A0030201 02020101 300D0609 2A864886 F70D0101 04050030
17311530 13060355 0403130C 73727374 63617365 72766572 301E170D 30343034
31323139 34353136 5A170D30 37303431 32313934 3531365A 30173115 30130603
55040313 0C737273 74636173 65727665 7230819F 300D0609 2A864886 F70D0101
01050003 818D0030 81890281 8100C3AF EE1E4BB1 9922A8DA 2BB9DC8E 5B1BD332
1051C9FE 32A971B3 3C336635 74691954 98E765B1 059E24B6 32154E99 105CA989
9619993F CC72C525 7357EBAC E6335A32 2AAF9391 99325BFD 9B8355EB C10F8963
9D8FC222 EE8AC831 71ACD3A7 4E918A8F D5775159 76FBF499 5AD0849D CAA41417
DD866902 21E5DD03 C37D4B28 0FAB0203 010001A3 63306130 0F060355 1D130101
FF040530 030101FF 300E0603 551D0F01 01FF0404 03020186 301D0603 551D0E04
160414F8 29CE97AD 6018D054 67FC2939 63C24706 91F9BD30 1F060355 1D230418
30168014 F829CE97 AD6018D0 5467FC29 3963C247 0691F9BD 300D0609 2A864886
F70D0101 04050003 8181007A F71B25F9 73D74552 25DFD03A D8D1338F 6792C805
47A81019 795B5AAE 035400BB F859DABF 21892B5B E71A8283 08950414 8633A8B2
C98565A6 C09CA641 88661402 ACC424FD 36F23360 ABFF4C55 BB23C66A C80A3A57
5EE85FF8 C1B1A540 E818CE6D 58131726 BB060974 4E1A2F4B E6195522 122457F3
DEDBAAD7 3780136E B112A6
quit
crypto pki certificate chain 7970
certificate ca 353FB24BD70F14A346C1F3A9AC725675
308203A8 30820290 A0030201 02021035 3FB24BD7 0F14A346 C1F3A9AC 72567530
0D06092A 864886F7 0D010105 0500302E 31163014 06035504 0A130D43 6973636F
20537973 74656D73 31143012 06035504 03130B43 41502D52 54502D30 3032301E
170D3033 31303130 32303138 34395A17 0D323331 30313032 30323733 375A302E
31163014 06035504 0A130D43 6973636F 20537973 74656D73 31143012 06035504
03130B43 41502D52 54502D30 30323082 0120300D 06092A86 4886F70D 01010105
00038201 0D003082 01080282 010100C4 266504AD 7DC3FD8D 65556FA6 308FAE95
B570263B 575ABD96 1CC8F394 5965D9D0 D8CE02B9 F808CCD6 B7CD8C46 24801878
57DC4440 A7301DDF E40FB1EF 136212EC C4F3B50F BCAFBB4B CD2E5826 34521B65
01555FE4 D4206776 03368357 83932638 D6FC953F 3A179E44 67255A73 45C69DEE
FB4D221B 21D7A3AD 38184171 8FD8C271 42183E65 09461434 736C77CC F380EEBF
632C7B3F A5F92AA6 A8EF3490 8724A84F 4DAF7FD7 0928F585 764D3558 3C0FE9AF
1ED8763F A299A802 970004AD 1912D265 7DE335B4 BCB6F789 DC68B9FA C8FDF85E
8A28AD8F 0F4883C0 77112A47 141DBEE0 948FBE53 FE67B308 D40C8029 87BD790E
CDAB9FD7 A190C1A2 A462C5F2 4A6E0B02 0103A381 C33081C0 300B0603 551D0F04
04030201 86300F06 03551D13 0101FF04 05300301 01FF301D 0603551D 0E041604
1452922B E288EE2E 098A4E7E 702C56A5 9AB4D49B 96306F06 03551D1F 04683066
3064A062 A060862D 68747470 3A2F2F63 61702D72 74702D30 30322F43 65727445

```

```

6E726F6C 6C2F4341 502D5254 502D3030 322E6372 6C862F66 696C653A 2F2F5C5C
6361702D 7274702D 3030325C 43657274 456E726F 6C6C5C43 41502D52 54502D30
30322E63 726C3010 06092B06 01040182 37150104 03020100 300D0609 2A864886
F70D0101 05050003 82010100 56838CEF C4DA3AD1 EA8FBFB15 2FFE6EE5 50A1972B
D4D7AF1F D298892C D5A2A76B C3462866 13E0E55D DC0C4B92 5AA94B6E 69277F9B
FC73C697 11266E19 451C0FAB A55E6A28 901A48C5 B9911EE6 348A8920 0AEDE1E0
B6EA781C FFD97CA4 B03C0E34 0E5B0649 8B0A34C9 B73A654E 09050C1F 4DA53E44
BF78443D B08C3A41 2EEEB873 78CB8089 34F9D16E 91512F0D 3A8674AD 0991ED1A
92841E76 36D7740E CB787F11 685B9E9D 0C67E85D AF6D05BA 3488E86D 7E2F7F65
6918DE0F BD3C7F67 D8A33F70 9C4A596E D9F62B3B 1EDEE854 D5882AD4 3D71F72B
8FAB7F3C 0B5F0759 D9828F83 954D7BB1 57A638EC 7D72BFF1 8933C16F 760BCA94
4C5B1931 67947A4F 89A1BDB5
quit
crypto pki certificate chain PEM
certificate ca 7612F960153D6F9F4E42202032B72356
308203A8 30820290 A0030201 02021076 12F96015 3D6F9F4E 42202032 B7235630
0D06092A 864886F7 0D010105 0500302E 31163014 06035504 0A130D43 6973636F
20537973 74656D73 31143012 06035504 03130B43 41502D52 54502D30 3031301E
170D3033 30323036 32333237 31335A17 0D323330 32303632 33333633 345A302E
31163014 06035504 0A130D43 6973636F 20537973 74656D73 31143012 06035504
03130B43 41502D52 54502D30 30313082 0120300D 06092A86 4886F70D 01010105
00038201 0D003082 01080282 010100AC 55BBED18 DE9B8709 FFC8F2D 509AB83A
21C1967F DEA7F4B0 969694B7 80CC196A 463DA516 54A28F47 5D903B5F 104A3D54
A981389B 2FC7AC49 956262B8 1C143038 5345BB2E 273FA7A6 46860573 CE5C998D
55DE78AA 5A5CFE14 037D695B AC816409 C6211F0B 3BBF09CF B0BBB2D4 AC362F67
0FD145F1 620852B3 1F07E2F1 AA74F150 367632ED A289E374 AF0C5B78 CE7DFB9F
C8EBBE54 6ECF4C77 99D6DC04 47476C0F 36E58A3B 6BCB24D7 6B6C84C2 7F61D326
BE7CB4A6 60CD6579 9E1E3A84 8153B750 5527E865 423BE2B5 CB575453 5AA96093
58B6A2E4 AA3EF081 C7068EC1 DD1EBDDA 53E6F0D6 E2E0486B 109F1316 78C696A3
CFBA84CC 7094034F C1EB9F81 931ACB02 0103A381 C33081C0 300B0603 551D0F04
04030201 86300F06 03551D13 0101FF04 05300301 01FF301D 0603551D 0E041604
14E917B1 82C71FCF ACA91B6E F4A9269C 70AE05A0 9A306F06 03551D1F 04683066
3064A062 A060862D 68747470 3A2F2F63 61702D72 74702D30 30312F43 65727445
6E726F6C 6C2F4341 502D5254 502D3030 312E6372 6C862F66 696C653A 2F2F5C5C
6361702D 7274702D 3030315C 43657274 456E726F 6C6C5C43 41502D52 54502D30
30312E63 726C3010 06092B06 01040182 37150104 03020100 300D0609 2A864886
F70D0101 05050003 82010100 AB64FDEB F60C32DC 360F0E10 5FE175FA 0D574AB5
02ACDCA3 C7BBED15 A4431F20 7E9286F0 770929A2 17E4CDF4 F2629244 2F3575AF
E90C468C AE67BA08 AAA71C12 BA0C0E79 E6780A5C F814466C 326A4B56 73938380
73A11AED F9B9DE74 1195C48F 99454B8C 30732980 CD6E7123 8B3A6D68 80B97E00
7F4BD4BA 0B5AB462 94D9167E 6D8D48F2 597CDE61 25CFADCC 5BD141FB 210275A2
0A4E3400 1428BA0F 69953BB5 50D21F78 43E3E563 98BCB2B1 A2D4864B 0616BACD
A61CD9AE C5558A52 B5EEAA6A 08F96528 B1804B87 D26E4AEE AB7AFFE9 2FD2A574
BAFE0028 96304A8B 13FB656D 8FC60094 D5A53D71 444B3CEF 79343385 3778C193
74A2A6CE DC56275C A20A303D
quit
crypto pki certificate chain 7960
certificate ca F301
308201F7 30820160 A0030201 020202F3 01300D06 092A8648 86F70D01 01050500
3041310B 30090603 55040613 02555331 1A301806 0355040A 13114369 73636F20
53797374 656D7320 496E6331 16301406 03550403 130D4341 50462D33 35453038
33333230 1E170D30 34303430 39323035 3530325A 170D3139 30343036 32303535
30315A30 41310B30 09060355 04061302 5553311A 30180603 55040A13 11436973
636F2053 79737465 6D732049 6E633116 30140603 55040313 0D434150 462D3335
45303833 33323081 9F300D06 092A8648 86F70D01 01010500 03818D00 30818902
818100C8 BD9B6035 366B44E8 0F693A47 250FF865 D76C35F7 89B1C4FD 1D122CE0
F5E5CDFF A4A87EFF 41AD936F E5C93163 3E55D11A AF82A5F6 D563E21C EB89EBFA
F5271423 C3E875DC E0E07967 6E1AAB4F D3823E12 53547480 23BA1A09 295179B6
85A0E83A 77DD0633 B9710A88 0890CD4D DB55ADD0 964369BA 489043BB B667E60F
93954B02 03010001 300D0609 2A864886 F70D0101 05050003 81810056 60FD3AB3
6F98D2AD 40C309E2 C05B841C 5189271F 01D864E8 98BCE665 2AFBCC8C 54007A84
8F772C67 E3047A6C C62F6508 B36A6174 B68C1D78 C2228FEA A89ECEFB CC8BA9FC
0F30E151 431670F9 918514D9 868D1235 18137F1E 50DFD32E 1DC29CB7 95EF4096
421AF22F 5C1D5804 B83F8E8E 95B04F45 86563BFE DF976C5B FB490A
quit
!
!
no crypto isakmp enable
!
```

```

! Enable IPsec.
crypto isakmp policy 1
  authentication pre-share
  lifetime 28800
crypto isakmp key cisco123 address 10.1.1.13
! The crypto key should match the key configured on Cisco Unified Communications
Manager.
!
! The crypto IPsec configuration should match your Cisco Unified Communications
Manager configuration.

crypto ipsec transform-set rtpset esp-des esp-md5-hmac
!
!
crypto map rtp 1 ipsec-isakmp
  set peer 10.1.1.13
  set transform-set rtpset
  match address 116
!
!
interface FastEthernet0/0
  ip address 10.1.1.22 255.255.255.0
  duplex auto
  speed auto
  crypto map rtp
!
interface FastEthernet0/1
  no ip address
  shutdown
  duplex auto
  speed auto
!
ip classless
!
ip http server
no ip http secure-server
!
!
! Define traffic to be encrypted by IPsec.
access-list 116 permit ip host 10.1.1.22 host 10.1.1.13
!
!
control-plane
!
!
call application alternate DEFAULT
!
!
voice-port 1/0/0
!
voice-port 1/0/1
!
voice-port 1/0/2
!
voice-port 1/0/3
!
voice-port 1/1/0
  timing hookflash-out 50
!
voice-port 1/1/1
!
voice-port 1/1/2
!
voice-port 1/1/3
!
! Enable MGCP voice protocol.
mgcp
mgcp call-agent 10.1.1.13 2427 service-type mgcp version 0.1
mgcp dtmf-relay voip codec all mode out-of-band

```

```
mgcp rtp unreachable timeout 1000 action notify
mgcp package-capability rtp-package
mgcp package-capability sst-package
no mgcp package-capability fxr-package
no mgcp timer receive-rtcp
mgcp sdp simple
mgcp fax t38 inhibit
mgcp rtp payload-type g726r16 static
!
mgcp profile default
!
!
dial-peer voice 81235 pots
  application mgcpapp
  destination-pattern 81235
  port 1/1/0
  forward-digits all
!
dial-peer voice 81234 pots
  application mgcpapp
  destination-pattern 81234
  port 1/0/0
!
dial-peer voice 999100 pots
  application mgcpapp
  port 1/0/0
!
dial-peer voice 999110 pots
  application mgcpapp
  port 1/1/0
!
!
! Enable credentials service on the gateway.
credentials
  ip source-address 10.1.1.22 port 2445
  trustpoint srstca
!
!
! Enable SRST mode.
call-manager-fallback
  secondary-dialtone 9
  transfer-system full-consult
  ip source-address 10.1.1.22 port 2000
  max-ephones 15
  max-dn 30
  transfer-pattern .....
.
.
.
```

## コントロールプレーン ポリシング : 例

ここでは、コントロールプレーン ポリシングを使用してクレデンシャル サービスを保護するための、セキュリティ上の最善策の設定例を示します。コントロールプレーン ポリシングは、ゲートウェイを保護し、トラフィックの負荷が大きいたともパケットの転送とプロトコルの状態を維持します。コントロールプレーンの詳細については、『[Control Plane Policing](#)』を参照してください。

```
Router# show running-config
.
.
.
! Allow trusted host traffic.
access-list 140 deny tcp host 10.1.1.11 any eq 2445

! Rate-limit all other traffic.
access-list 140 permit tcp any any eq 2445
access-list 140 deny ip any any

! Define class-map "sccp-class."
class-map match-all sccp-class
match access-group 140

policy-map control-plane-policy
class sccp-class
police 8000 1500 1500 conform-action drop exceed-action drop

! Define aggregate control plane service for the active Route Processor.
control-plane
service-policy input control-plane-policy
.
.
.
```

## 関連情報

ボイスメールが必要な場合、ボイスメールの設定方法について、P.193 の「[Cisco Unified SRST へのボイスメールの統合](#)」を参照してください。P.227 の「[Cisco Unified SRST の監視と保守](#)」も参照してください。

追加情報については、P.25 の「[Cisco Unified SRST の概要](#)」の P.40 の「[その他の資料](#)」を参照してください。



# Cisco Unified SRST へのボイスメールの統合

---

Revised: July 11, 2008

この章では、Cisco Unified Communications Manager のフォールバック時に Cisco Unified (SRST) ルータに接続された電話機で、既存のボイスメール システムを実行する方法について説明します。

## 内容

- [Cisco Unified SRST へのボイスメールの統合について \(P.194\)](#)
- [Cisco Unified SRST へのボイスメールの統合方法 \(P.196\)](#)
- [設定例 \(P.207\)](#)
- [関連情報 \(P.210\)](#)

## Cisco Unified SRST へのボイスメールの統合について

Cisco Unified SRST は、Cisco Unified Communications Manager のフォールバック時に Cisco Unity と他のボイスメール システムからのボイスメール メッセージを送受信できます。WAN がダウンしたとき、BRI または PRI を介して Cisco Unified SRST システムにアクセスするボイスメール システムでは、ISDN シグナリングが使用されます (図 11 を参照)。Foreign Exchange Office (FXO) または Foreign Exchange Station (FXS) を介してアクセスするシステムは PSTN に接続し、インバンド Dual Tone Multifrequency (DTMF) シグナリングを使用します (図 12 を参照)。

図 11 BRI または PRI を使用する Cisco Unified Communications Manager のフォールバック

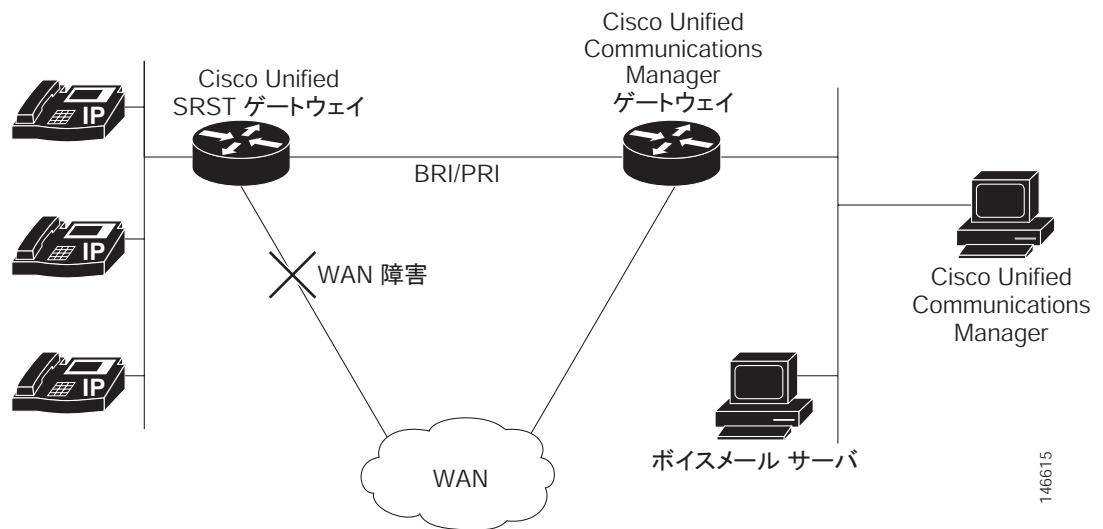
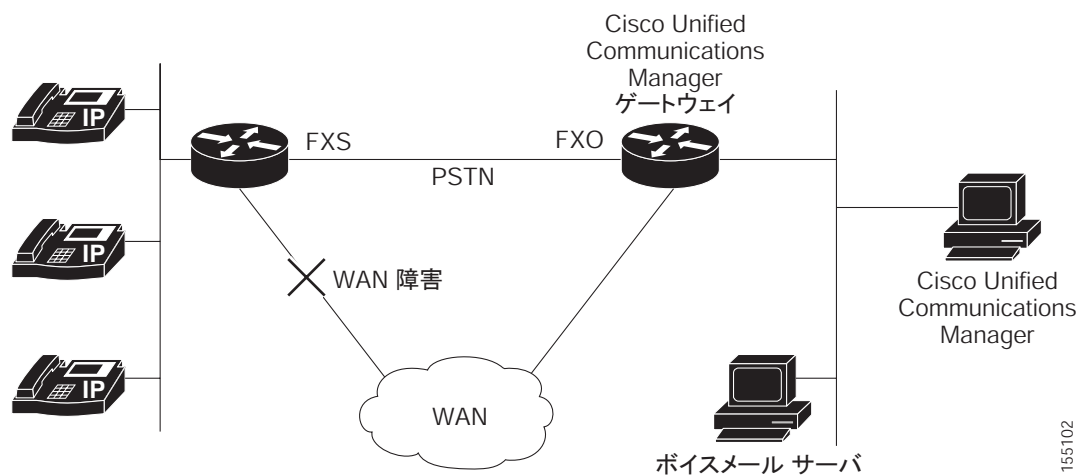


図 12 PSTN を使用する Cisco Unified Communications Manager のフォールバック



両方の設定では、電話機のメッセージ ボタンをアクティブの状態に保つことができ、ビジーまたは無応答の番号へのコールを、ダイヤルされた番号のメールボックスに転送できます。



ビジー信号に達するコール、無応答のコール、およびメッセージ ボタンが押されて発生したコールは、ボイスメール システムに転送されます。これを行うためには、ダイヤル ピアからボイスメール システムへのアクセスを設定し、ビジー コールと無応答コールのため、およびメッセージ ボタンのためにボイスメール システムへのルーティングを確立する必要があります。

FXO または FXS を介してボイスメール システムのアクセスが行われる場合、正しいボイスメール システムのメールボックスにアクセスできるように、ボイスメール システムに対する指示 (DTMF パターン) を設定する必要があります。BRI または PRI を介してボイスメール システムのアクセスが行われる場合、ボイスメール システムは発信側の電話機のメールボックスに直接ログインできるため、指示は必要ありません。

## Cisco Unified SRST へのボイスメールの統合方法

ここでは、次の作業について説明します。

- [ボイスメールへのダイレクト アクセスの設定 \(P.196\)](#) (必須)
- [メッセージ ボタンの設定 \(P.199\)](#) (必須)
- [Cisco Unified Communications Manager ゲートウェイへのリダイレクト \(P.201\)](#) (BRI または PRI の場合は必須)
- [ボイスメールへのコール転送の設定 \(P.201\)](#) (FXO または FXS の場合は必須)
- [MWI の設定 \(P.205\)](#) (オプション)

### ボイスメールへのダイレクト アクセスの設定

FXO または FXS アクセスを使用してボイスメール メッセージにアクセスするには、ボイスメール システムの番号と一致する宛先パターンが設定された、POTS ダイアル ピアが必要です。また、ボイスメール システムのアクセスが行われるポートにダイアル ピアを関連付ける必要があります。

両方の一連の設定は、global コンフィギュレーション モードと dial-peer コンフィギュレーション モードで実行されます。以下の要約手順および詳細手順には、この作業を実行するのに必要な基本的なコマンドだけが含まれます。特定のダイアル ピア設定で、追加のコマンドが必要になる場合があります。

#### 要約手順


1. `dial-peer voice tag {pots | voatm | vofr | voip}`
2. `destination-pattern [+] string [T]`
3. `port {slot-number/subunit-number/port | slot/port:ds0-group-no}`
4. `forward-digits {num-digit | all | extra}`
5. `exit`

## 詳細手順

	コマンドまたはアクション	目的
ステップ 1	<p><code>dial-peer voice tag {pots   voatm   vofr   voip}</code></p> <p>例: Router(config)# <code>dial-peer voice 1002 pots</code></p>	<p>(FXO/FXS および BRI/PRI) 特定のダイヤル ピアを定義し、音声カプセル化の方法を指定し、<code>dial-peer</code> コンフィギュレーション モードを開始します。<code>dial-peer</code> コマンドは、個々のルータに対して異なる構文を提供します。この例は、Cisco 3600 シリーズルータの構文です。</p> <ul style="list-style-type: none"> <li>• <code>tag</code>: 特定のダイヤル ピアを定義する数字。範囲は 1 ~ 2147483647 です。</li> <li>• <code>pots</code>: IP バックボーンで VoIP カプセル化を使用する POTS ダイヤル ピアであることを示します。</li> <li>• <code>voatm</code>: ATM バックボーン ネットワークでリアルタイム AAL5 音声カプセル化を使用する VoATM ダイヤル ピアであることを指定します。</li> <li>• <code>vofr</code>: フレームリレー バックボーン ネットワークで FRF.11 カプセル化を使用する VoFR ダイヤル ピアであることを指定します。</li> <li>• <code>voip</code>: POTS ネットワークで音声カプセル化を使用する VoIP ダイヤル ピアであることを示します。</li> </ul>
ステップ 2	<p><code>destination-pattern [+] string [T]</code></p> <p>例: Router(config-dial-peer)# <code>destination-pattern 1100T</code></p>	<p>(FXO/FXS および BRI/PRI) ダイヤル ピアにプレフィックスまたは完全な E.164 電話番号 (ダイヤルプランに応じて) を使用することを指定します。</p> <ul style="list-style-type: none"> <li>• <code>+</code>: (オプション) E.164 標準番号を示す文字。</li> <li>• <code>string</code>: 表 12 を参照してください。</li> <li>• <code>T</code>: (オプション) <code>destination-pattern</code> 値が可変長ダイヤル文字列であることを示す制御文字。</li> </ul>
ステップ 3	<p><code>port {slot-number/subunit-number/port   slot/port:ds0-group-no}</code></p> <p>例: Router(config-dial-peer)# <code>port 1/1/1</code></p>	<p>(FXO/FXS および BRI/PRI) Cisco 3600 シリーズルータの特定の音声ポートにダイヤル ピアを関連付けます。</p> <ul style="list-style-type: none"> <li>• <code>slot-number</code>: 音声インターフェイスカード (VIC) が設置されたルータのスロット番号。有効なエントリは 0 ~ 3 です。設置先のスロットによって異なります。</li> <li>• <code>subunit-number</code>: 音声ポートがある VIC のサブユニット。有効なエントリは 0 または 1 です。</li> <li>• <code>port</code>: 音声ポート番号。有効なエントリは 0 および 1 です。</li> <li>• <code>ds0-group-no</code>: DS0 グループ番号を指定します。定義される各 DS0 グループ番号は、別個の音声ポートで表されます。これにより、デジタル T1/E1 カードの個々の DS0 を定義できます。</li> </ul>

	コマンドまたはアクション	目的
ステップ 4	<p><code>forward-digits {num-digit   all   extra}</code></p> <p>例: Router(config-dial-peer)# <code>forward-digits all</code></p>	<p>(FXO または FXS のオプション) 音声コールに転送する数字を指定します。</p> <ul style="list-style-type: none"> <li><i>num-digit</i> : 転送する桁数。桁数が宛先の電話番号より長い場合、宛先番号の長さが使用されます。範囲は 0 ~ 32 です。この値を 0 に設定すると、<code>no forward-digits</code> コマンドを入力するのと同じこととなります。</li> <li><i>all</i> : すべての数字を転送します。all を入力した場合、宛先パターンのすべての長さが使用されます。</li> <li><i>extra</i> : ダイヤルした数字列がダイヤル ピアの宛先パターンの長さより長い場合、右揃えした追加の数字が転送されます。ただし、ダイヤル ピアの宛先パターンが可変長で、「T」の文字（たとえば、T、123T、123...T）で終わる場合、追加の数字は転送されません。</li> </ul>
ステップ 5	<p><code>exit</code></p> <p>例: Router(config-dial-peer)# <code>exit</code></p>	<p>(FXO/FXS および BRI/PRI) dial-peer コンフィギュレーション モードを終了します。</p>

表 12 destination-pattern コマンドの string 引数の有効エン트리

エン트리	説明
0 ~ 9 の数字	—
A ~ D の文字	—
アスタリスク(*)およびポンド記号(#)	標準の押しボタン式ダイヤルパッドに表示されます。
カンマ(,)	数字の間にポーズを挿入します。
ピリオド(.)	入力された任意の数字と一致します (この文字は、ワイルドカードとして使用されます)。
パーセント記号(%)	先行する数字が 0 回またはそれ以上の回数発生することを示します。ワイルドカードの使用方法与類似しています。
プラス記号(+)	先行する数字が 1 回以上発生することを示します。
	 <p><b>(注)</b> 数字列として使用されるプラス記号は、E.164 標準番号であることを示すために数字列の前に使用することができるプラス記号とは異なります。</p>
曲折アクセント記号(^)	文字列の先頭との一致を示します。
	パターンを示すカッコ(( ))は、標準の表現ルールと同じ内容になります。
ドル記号(\$)	入力文字列の末尾のヌル文字列と一致します。
バックスラッシュ記号(\)	単一文字の前に置かれ、その文字と一致します。特に意味を持たない単一文字に対して使用できます (その文字に一致します)。
疑問符(?)	先行する数字が 0 回または 1 回発生することを示します。
角カッコ([ ])	範囲を示します。範囲は、角カッコに囲まれた一連の文字です。範囲では 0 ~ 9 の数字だけを使用できます。

## 例

次の FXO と FXS の例では、1102 という POTS ダイアル ピアを設定し、ダイアル ピア 1102 をボイスメール内線の 1101 と照合して、ボイスメールシステムが接続された音声ポート 1/1/1 にダイアル ピア 1102 を割り当てます。他のダイアル ピアは、ボイスメールへのダイレクト アクセス用に設定されます。

```
voice-port 1/1/1
  timing digit 250
  timing inter-digit 250

dial-peer voice 1102 pots
  destination-pattern 1101
  port 1/1/1
  forward-digits all

dial-peer voice 1103 pots
  destination-pattern 1101
  port 1/1/1
  forward-digits all

dial-peer voice 1104 pots
  destination-pattern 1101
  port 1/1/1
  forward-digits all
```

次の例では、1102 という名前の POTS ダイアル ピアが、ポート 2/0:23 から 1101 に直接アクセスするように設定します。

```
controller T1 2/0
  framing esf
  clock source line primary
  linecode b8zs
  cablelength short 133
  pri-group timeslots 21-24

interface Serial2/0:23
  no ip address
  no logging event link-status
  isdn switch-type primary-net5
  isdn incoming-voice voice
  isdn T309-enable
  no cdp enable

voice-port 2/0:23

dial-peer voice 1102 pots
  destination-pattern 1101T
  port 2/0:23
```

## メッセージ ボタンの設定

Cisco Unified Communications Manager のフォールバック時に Cisco Unified SRST ルータに接続された Cisco Unified IP Phone のメッセージ ボタンをアクティブにするには、ボイスメールシステムで短縮ダイアル番号をプログラミングする必要があります。短縮ダイアル番号は、Cisco Unified Communications Manager のフォールバック時に、Cisco Unified SRST ルータに接続された電話機のメッセージ ボタンが押されたときにダイヤルされます。また、自動転送を設定して、ビジーおよび無応答の番号へのコールがボイスメール番号に送信されるようにする必要があります。

この設定は、FXO/FXS および BRI/PRI に必要です。

## 要約手順

1. `call-manager-fallback`
2. `voicemail phone-number`
3. `call-forward busy directory-number`
4. `call-forward noan directory-number timeout seconds`
5. `exit`

## 詳細手順

	コマンドまたはアクション	目的
ステップ 1	<code>call-manager-fallback</code>  例: Router(config)# <code>call-manager-fallback</code>	<code>call-manager-fallback</code> コンフィギュレーション モードを開始します。
ステップ 2	<code>voicemail phone-number</code>  例: Router(config-cm-fallback)# <code>voicemail 5550100</code>	Cisco Unified IP Phone のメッセージ ボタンが押されたときにダイヤルされる電話番号を設定します。  <ul style="list-style-type: none"> <li>• <code>phone-number</code> : メッセージを取得するための短縮ダイヤル番号として設定される電話番号。</li> </ul>
ステップ 3	<code>call-forward busy directory-number</code>  例: Router(config-cm-fallback)# <code>call-forward busy 2000</code>	Cisco IP Phone が通話中の場合に別の番号に自動転送するように設定します。  <ul style="list-style-type: none"> <li>• <code>directory-number</code> : 選択された電話番号。完全修飾 E.164 番号を表します。この番号には、内線電話番号の右揃えの数字に対応する「.」ワイルドカード文字を含めることができます。</li> </ul>
ステップ 4	<code>call-forward noan directory-number timeout seconds</code>  例: Router(config-cm-fallback)# <code>call-forward noan 2000 timeout 10</code>	Cisco IP Phone からの応答が受信されない場合に別の番号に自動転送するように設定します。  <ul style="list-style-type: none"> <li>• <code>directory-number</code> : 選択された電話番号。完全修飾 E.164 番号を表します。この番号には、内線電話番号の右揃えの数字に対応する「.」ワイルドカード文字を含めることができます。</li> <li>• <code>timeout seconds</code> : コールを別の電話機に自動転送するまでの待機時間を秒単位で設定します。<code>seconds</code> の範囲は 3 ~ 60000 です。</li> </ul>
ステップ 5	<code>exit</code>  例: Router(config-cm-fallback)# <code>exit</code>	<code>call-manager-fallback</code> コンフィギュレーション モードを終了します。

## 例

次の例では、Cisco Unified SRST ルータに接続されている Cisco Unified IP Phone でメッセージ ボタンが押されたときに発行される短縮ダイヤル番号として 1101 を指定します。すべてのビジー コールおよび無応答のコールは、ボイスメール番号 (1101) に転送されるように設定されます。

```
call-manager-fallback
voicemail 1101
call-forward busy 1101
call-forward noan 1101 timeout 3
```

## Cisco Unified Communications Manager ゲートウェイへのリダイレクト



(注) BRI または PRI アクセスを使用するボイスメール システムでは、次の作業が必要です。

Cisco Unified SRST では、個人メッセージを取得するためのメッセージ ボタンがサポートされていますが、ビジーおよび無応答の番号へのコールを自動的にボイスメール システムに転送することもできます。BRI または PRI アクセスを使用するボイスメール システムは、直接発信側の電話機のメールボックスにログインできます。これを実現するためには、Cisco Unified Communications Manager のいくつかの設定が推奨されます。ご使用のボイスメール システムが Redirected Dialed Number Identification Service( RDNIS )をサポートしている場合、Cisco Unified Communications Manager への発信 SETUP メッセージに RDNIS を含め、設定済みのデバイスおよびアプリケーションに対して送受信された、最後にリダイレクトされた番号と最初にダイヤルされた番号を宣言する必要があります。

- ステップ 1** Cisco Unified Communications Manager の任意のページで、**Device** および **Gateway** をクリックします。
- ステップ 2** Find and List Gateways ページで、**Find** をクリックします。
- ステップ 3** Find and List Gateways ページで、デバイス名を選択します。
- ステップ 4** Gateway Configuration ページで、**Redirecting Number IE Delivery - Outgoing** をオンにします。

## ボイスメールへのコール転送の設定



(注) FXO または FXS アクセスを使用するボイスメール システムでは、次の作業が必要です。

Cisco Unified SRST では、個人メッセージを取得するためのメッセージ ボタンがサポートされていますが、ビジーまたは無応答の番号へのコールを自動的にボイスメール システムに転送することもできます。転送されたコールは、ボイスメール システムのほとんどすべての場所にルーティングできます。通常、コールは、発信者がメッセージを残すことができる着信番号のメールボックス内の場所に転送されます。

## DTMF デジタル パターンを使用したコール ルーティング指示

転送されたコールが正しいボイスメールボックスに送信されるようにするには、Cisco Unified SRST コールルーティング指示が必要です。これらの指示は、特定のボイスメールの場所への到達にボイスメール システムが必要とするダイヤル シーケンスに一致するパターンで設定された DTMF デジタルで構成されます。たとえば、発信者が次の内容を実行してメッセージを残すように、ボイスメール システムを設計することができます。

1. セントラル ボイスメール番号 (1101) をダイヤルして、# を押します。
2. 内線番号 (6000) をダイヤルして、# を押します。

3. 2 をダイヤルして、内線番号のメールボックスにメッセージを残すためのメニュー オプションを選択します。

ビジラーまたは無応答の番号へのコールを Cisco Unified SRST が内線 6000 のメールボックスに転送するためには、1101#6000#2 のシーケンスを発行するように Cisco Unified SRST がプログラミングされている必要があります。図 13 に示すように、この処理は `voicemail` および `pattern` コマンドで実行されます。

図 13 Cisco Unified SRST でボイスメール ダイヤル シーケンス 1101#6000#2 が設定される方法

```
call-manager-fallback
  voicemail 1101
    1101
      #6000#2
        call-manager-fallback
          pattern ext-to-ext busy # cgn #2
          pattern ext-to-ext busy # cdn #2
          pattern ext-to-ext busy # fdn #2
          pattern ext-to-ext no-answer # cgn #2
          pattern ext-to-ext no-answer # cdn #2
          pattern ext-to-ext no-answer # fdn #2
          pattern trunk-to-ext busy # cgn #2
          pattern trunk-to-ext busy # cdn #2
          pattern trunk-to-ext busy # fdn #2
          pattern trunk-to-ext no-answer # cgn #2
          pattern trunk-to-ext no-answer # cdn #2
          pattern trunk-to-ext no-answer # fdn #2
```

図 13 に示す `pattern` コマンドの `# cgn #2`、`# cdn #2`、および `# fdn #2` の部分が、DTMF デジタルパターンです。これらのパターンは、タグとトークンで構成されています。タグは、DTMF トーンを表す文字のセットです。トークンは、ボイスメールにコール転送された着信コールの状態を表す 3 つのコマンド キーワード (`cgn`、`cdn`、および `fdn`) で構成されます。

タグは、DTMF トーン セット (A ~ D、0 ~ 9、# および \*) で最大 3 つの文字にすることができます。ボイスメール システムは、制限された DTMF トーン セットを使用できます。たとえば、Cisco Unity は A ~ D を除くすべての DTMF トーンを使用します。トーンは、複数の方法で定義できます。たとえば、星 (\*) をトークンの前に単独で置くと、「後続のトークン番号をダイヤルする」という意味になります。星 (\*) をトークンの末尾に置くと、トークン番号の末尾を表します。アスタリスクが他のタグ文字間にある場合は、\* をダイヤルするという意味になります。タグの使用方法は、ボイスメール システムで DTMF トーンが定義されている方法によって異なります。

トークンは、自動転送チェーンのどの電話番号をそのパターンで使用するかを Cisco Unified SRST に伝達します。図 14 に示すように、ボイスメール転送時に発生する可能性のある 3 つのコール状態に対応する、3 つのトークン タイプがあります。

図 14 番号がトークンから抽出される方法



```
pattern ext-to-ext busy # cdn # 2 = pattern ext-to-ext busy # 3000 # 2
pattern ext-to-ext busy # fdn # 2 = pattern ext-to-ext busy # 2000 # 2
pattern ext-to-ext busy # cgn # 2 = pattern ext-to-ext busy # 1000 # 2
```

88979



タグとトークンのセット、またはパターンが、ボイスメールシステムをアクティブにするための条件は、次のとおりです。

- ユーザが電話機のメッセージ ボタンを押す場合 ( `pattern direct` コマンド )
- 内線がビジーな状態の内線への接続を試み、コールがボイスメールに転送される場合 ( `pattern ext-to-ext busy` コマンド )
- 内線が内線への接続に失敗し、コールがボイスメールに転送される場合 ( `pattern ext-to-ext no-answer` コマンド )
- 外部トランク コールがビジーな状態の内線に到達し、コールがボイスメールに転送される場合 ( `pattern trunk-to-ext busy` コマンド )
- 外部トランク コールが無応答の内線に到達し、コールがボイスメールに転送される場合 ( `pattern trunk-to-ext no-answer` コマンド )

## 前提条件

- ボイスメールシステムへの FXO へアピン転送コールには、セントラル オフィスからの接続解除の監視が必要です。詳細については、『[FXO Answer and Disconnect Supervision](#)』を参照してください。
- ご使用のボイスメールシステムが正しく解釈するパターンを設定するには、システムがボイスメール コールをルーティングして、DTMF トーンを解釈する方法を理解する必要があります ( P.201 の「[DTMF デジット パターンを使用したコール ルーティング指示](#)」を参照 )。

Cisco Unity がボイスメール コールを処理する方法については、『[How to Transfer a Caller Directly into a Cisco Unity Mailbox](#)』を参照してください。他のコール処理については、任意の [Cisco Unity システム アドミニストレーション ガイド](#) の「Subscriber and Operator Orientation」の章を参照してください。

他のボイスメール システムについては、アナログ ボイスメール統合コンフィギュレーション ガイドまたはシステムのコール処理に関する情報を参照してください。

## 要約手順

1. `vm-integration`
2. `pattern direct tag1 {CGN | CDN | FDN} [tag2 {CGN | CDN | FDN}] [tag3 {CGN | CDN | FDN}] [last-tag]`
3. `pattern ext-to-ext busy tag1 {CGN | CDN | FDN} [tag2 {CGN | CDN | FDN}] [tag3 {CGN | CDN | FDN}] [last-tag]`
4. `pattern ext-to-ext no-answer tag1 {CGN | CDN | FDN} [tag2 {CGN | CDN | FDN}] [tag3 {CGN | CDN | FDN}] [last-tag]`
5. `pattern trunk-to-ext busy tag1 {CGN | CDN | FDN} [tag2 {CGN | CDN | FDN}] [tag3 {CGN | CDN | FDN}] [last-tag]`
6. `pattern trunk-to-ext no-answer tag1 {CGN | CDN | FDN} [tag2 {CGN | CDN | FDN}] [tag3 {CGN | CDN | FDN}] [last-tag]`

## 詳細手順

	コマンドまたはアクション	目的
ステップ 1	<code>vm-integration</code>  例: <code>Router(config)# vm-integration</code>	ボイスメール統合モードを開始して、DTMF およびアナログ ボイスメール システムとのボイスメール統合を可能にします。

	コマンドまたはアクション	目的
ステップ 2	<pre>pattern direct tag1 {CGN   CDN   FDN} [tag2 {CGN   CDN   FDN}] [tag3 {CGN   CDN   FDN}] [last-tag]</pre> <p><b>例:</b> Router(config-vm-int)# pattern direct 2 CGN *</p>	<p>ユーザが電話機のメッセージ ボタンを押したときに、ボイスメールシステムをアクティブにするために必要な DTMF デジット パターンを設定します。</p> <ul style="list-style-type: none"> <li>• <i>tag1</i>: 長さが DTMF デジット 4 桁未満の英数字文字列。英数字の文字列は、4 つの文字 (A、B、C、および D)、2 つの記号 (* および #) および 10 個の数字 (0 ~ 9) の組み合わせで構成されます。タグ番号は、ボイスメールシステムの統合ファイルで、発信番号、着信番号、転送番号のいずれかの直前に定義された番号と一致します。</li> <li>• <i>tag2</i> および <i>tag3</i>: (オプション) <i>tag1</i> を参照してください。</li> <li>• <i>last-tag</i>: <i>tag1</i> を参照してください。このタグは、パターンの最後を示します。</li> <li>• <b>CGN</b>: ボイスメールシステムに送信される発信番号 (CGN) 情報</li> <li>• <b>CDN</b>: ボイスメールシステムに送信される着信番号 (CDN) 情報</li> <li>• <b>FDN</b>: ボイスメールシステムに送信される転送番号 (FDN) 情報</li> </ul>
ステップ 3	<pre>pattern ext-to-ext busy tag1 {CGN   CDN   FDN} [tag2 {CGN   CDN   FDN}] [tag3 {CGN   CDN   FDN}] [last-tag]</pre> <p><b>例:</b> Router(config-vm-int)# pattern ext-to-ext busy 7 FDN * CGN *</p>	<p>内線がビジーな内線への接続を試み、コールがボイスメールに転送されたときに、ボイスメールシステムをアクティブにするのに必要な DTMF デジット パターンの転送を設定します。引数とキーワードの情報については、<a href="#">ステップ 2</a> を参照してください。</p>
ステップ 4	<pre>pattern ext-to-ext no-answer tag1 {CGN   CDN   FDN} [tag2 {CGN   CDN   FDN}] [tag3 {CGN   CDN   FDN}] [last-tag]</pre> <p><b>例:</b> Router(config-vm-int)# pattern ext-to-ext no-answer 5 FDN * CGN *</p>	<p>内線が内線への接続に失敗し、コールがボイスメールに転送されたときに、ボイスメールシステムをアクティブにするのに必要な DTMF デジット パターンの転送を設定します。引数とキーワードの情報については、<a href="#">ステップ 2</a> を参照してください。</p>
ステップ 5	<pre>pattern trunk-to-ext busy tag1 {CGN   CDN   FDN} [tag2 {CGN   CDN   FDN}] [tag3 {CGN   CDN   FDN}] [last-tag]</pre> <p><b>例:</b> Router(config-vm-int)# pattern trunk-to-ext busy 6 FDN * CGN *</p>	<p>外部トランク コールがビジーな内線に到達し、コールがボイスメールに転送されたときに、ボイスメールシステムをアクティブにするのに必要な DTMF デジット パターンの転送を設定します。引数とキーワードの情報については、<a href="#">ステップ 2</a> を参照してください。</p>
ステップ 6	<pre>pattern trunk-to-ext no-answer tag1 {CGN   CDN   FDN} [tag2 {CGN   CDN   FDN}] [tag3 {CGN   CDN   FDN}] [last-tag]</pre> <p><b>例:</b> Router(config-vm-int)# pattern trunk-to-ext no-answer 4 FDN * CGN *</p>	<p>外部トランク コールが無応答の内線に到達し、コールがボイスメールに転送されたときに、ボイスメールシステムをアクティブにするのに必要な DTMF デジット パターンの転送を設定します。引数とキーワードの情報については、<a href="#">ステップ 2</a> を参照してください。</p>

## 例

次の設定では、ボイスメール番号が 1101 で、3001 がメッセージ ボタン付き電話機の場合、3001 メッセージ ボタンが押されると 1101\*3001 が自動的にダイヤルされるようになります。このような状況では、3001 が発信番号または着信コール番号と見なされます。

```
vm-integration
pattern direct * CGN
```

次の設定では、3001 が 3006 をコールし、3006 が応答しない場合、SRST ルータが 3001 をボイスメール システム (1101) に転送し、DTMF パターン # 3006 #2 がボイスメール システムに送信されます。このパターンは、ボイスメールボックス番号 3006 (3006 のボイスメールボックス) を選択することを目的にしています。このパターンが送信されるようにするには、3001 が転送番号である必要があります。

```
vm-integration
pattern ext-to-ext no-answer # FDN #2
```

次の設定では、3006 がビジーな状態で、3001 が 3006 をコールし、SRST ルータが 3001 をボイスメール システム (1101) に転送し、DTMF パターン # 3006 #2 がボイスメール システムに送信されます。このパターンは、ボイスメールボックス番号 3006 (3006 のボイスメールボックス) を選択することを目的にしています。このパターンが送信されるようにするには、3001 が転送番号である必要があります。

```
vm-integration
pattern ext-to-ext busy # FDN #2
```

## MWI の設定

Message Waiting Indication (MWI) リレー メカニズムは、リモート ボイスメール メッセージ システムに誰かがボイスメール メッセージを残した後に開始します。MWI リレーは、1 つの Cisco Unity Voice Mail システムを複数の Cisco Unified SRST ルータで共有する場合に必要です。SRST ルータは、MWI に対して SIP Subscribe および Notify 方式を使用します。SIP MWI、Subscribe 方式、および Notify 方式の詳細については、『[Configuring Cisco IOS SIP Configuration Guide](#)』を参照してください。SIP MWI リレー サーバである SRST ルータは、SIP ノーティファイヤとして動作します。他のリモート ルータは、SIP 登録者として動作します。

### 要約手順

1. `call-manager-fallback`
2. `mwi relay`
3. `mwi reg-e164`
4. `exit`
5. `sip-ua`
6. `mwi-server {ipv4:destination-address | dns:host-name} [expires seconds] [port port] [transport {tcp | udp}] [unsolicited]`
7. `exit`

## 詳細手順

	コマンド	目的
ステップ 1	<code>call-manager-fallback</code>  例: Router(config)# call-manager-fallback	call-manager-fallback コンフィギュレーション モードを開始します。
ステップ 2	<code>mwi relay</code>  例: Router(config-cm-fallback)# mwi relay	SRST ルータがリモート Cisco IP Phone に MWI 情報をリレーするようにします。
ステップ 3	<code>mwi reg-e164</code>  例: Router(config-cm-fallback)# mwi reg-e164	SIP プロキシまたはレジストラを使用した内線番号ではなく、E.164 番号を登録します。
ステップ 4	<code>exit</code>  例: Router(config-cm-fallback)# exit	call-manager-fallback コンフィギュレーション モードを終了します。
ステップ 5	<code>sip-ua</code>  例: Router(config)# sip-ua	SIP user-agent コンフィギュレーション モードを開始します。
ステップ 6	<code>mwi-server {ipv4:destination-address   dns:host-name} [expires seconds] [port port] [transport {tcp   udp}] [unsolicited]</code>  例: Router(config-sip-ua)# mwi-server ipv4:10.0.2.254	音声ゲートウェイまたはユーザ エージェントのボイスメール サーバの設定値を設定します。SIP ベースの MWI サーバの IP アドレスとポートは、ボイスメール サーバと同じ LAN にある必要があります。MWI サーバは、Cisco Unified SRST ルータです。キーワードと引数は、次のとおりです。 <ul style="list-style-type: none"> <li>• <code>ipv4:destination-address</code> : ボイスメール サーバの IP アドレス。</li> <li>• <code>dns:host-name</code> : ボイスメール サーバの名前を解決するドメイン名サーバを収容するホスト デバイス。引数には、ターゲット アドレスに関連付けられた完全なホスト名が含まれている必要があります (例: <code>dns:test.cisco.com</code>) 。</li> <li>• <code>expires seconds</code> : サブスクリプションの有効期限 (秒単位)。範囲は 1 ~ 999999 です。デフォルトは、3600 です。</li> <li>• <code>port port</code> : ボイスメール サーバ上のポート番号。デフォルトは、5060 です。</li> <li>• <code>transport</code> : ボイスメール サーバへの転送プロトコル。有効値は tcp および udp です。デフォルトは UDP です。</li> <li>• <code>unsolicited</code>: メールボックス ステータスが変化したときに、ボイスメール サーバが音声ゲートウェイまたは UA に SIP 通知メッセージを送信するように要求します。MWI サービスに対する音声ゲートウェイ登録の要件を削除します。</li> </ul>
ステップ 7	<code>exit</code>  例: Router(config-sip-ua)# exit	SIP user-agent コンフィギュレーション モードを終了します。

## 設定例

ここでは、次の設定例を示します。

- ローカル ボイスメール システムの設定 (FXO および FXS): 例 (P.207)
- セントラル ロケーションのボイスメール システムの設定 (FXO および FXS): 例 (P.207)
- FXO および FXS を介したボイスメール アクセスの設定: 例 (P.208)
- BRI および PRI を介したボイスメール アクセスの設定: 例 (P.209)

### ローカル ボイスメール システムの設定 (FXO および FXS): 例

次の例の「Dial-Peer Configuration for Integration of Voice-Mail with Cisco Unified SRST」セクションは、ローカル ボイスメール システムの従来型のダイヤル ピア設定を示しています。「Cisco Unified SRST Voice-Mail Integration Pattern Configuration」セクションは、使用しているボイスメール システムの設定に適合している必要があります。

```
! Dial-Peer Configuration for Integration of Voice-Mail with Cisco Unified SRST
!
dial-peer voice 101 pots
 destination-pattern 14011
 port 3/0/0
!
dial-peer voice 102 pots
 preference 1
 destination-pattern 14011
 port 3/0/1
!
dial-peer voice 103 pots
 preference 2
 destination-pattern 14011
 port 3/1/0
!
dial-peer voice 104 pots
 destination-pattern 14011
 port 3/1/1
!
! Cisco Unified SRST configuration
!
call-manager-fallback
 max-ephones 24
 max-dn 144
 ip source-address 1.4.214.104 port 2000
 voicemail 14011
 call-forward busy 14011
 call-forward noan 14011 timeout 3

! Cisco Unified SRST Voice-Mail Integration Pattern Configuration
!
vm-integration
 pattern direct 2 CGN *
 pattern ext-to-ext no-answer 5 FDN * CGN *
 pattern ext-to-ext busy 7 FDN * CGN *
 pattern trunk-to-ext no-answer 4 FDN * CGN *
 pattern trunk-to-ext busy 6 FDN * CGN *
```

### セントラル ロケーションのボイスメール システムの設定 (FXO および FXS): 例

例の「Dial-Peer Configuration for Integration of Voice-Mail with Cisco Unified SRST in Central Location」セクションは、セントラル ボイスメール システムの従来型のダイヤル ピア設定を示しています。「Cisco Unified SRST Voice-Mail Integration Pattern Configuration」セクションは、使用しているボイスメール システムの設定に適合している必要があります。



(注) MWI 統合は、セントラル ロケーションのボイスメール システムへの PSTN アクセスではサポートされていません。

```

! Dial-Peer Configuration for Integration of Voice-Mail with Cisco Unified SRST in
Central
! Location
!
dial-peer voice 101 pots
 destination-pattern 14011
 port 3/0/0
!
! Cisco Unified SRST configuration
!
call-manager-fallback
 max-ephones 24
 max-dn 144
 ip source-address 1.4.214.104 port 2000
 voicemail 14011
 call-forward busy 14011
 call-forward noan 14011 timeout 3
!
! Cisco Unified SRST Voice-Mail Integration Pattern Configuration
!
vm-integration
 pattern direct 2 CGN *
 pattern ext-to-ext no-answer 5 FDN * CGN *
 pattern ext-to-ext busy 7 FDN * CGN *
 pattern trunk-to-ext no-answer 4 FDN * CGN *
 pattern trunk-to-ext busy 6 FDN * CGN *

```

## FXO および FXS を介したボイスメール アクセスの設定 : 例

次の例は、無応答のコールをボイスメールに転送するように Cisco Unified SRST ルータを設定する方法を示しています。この例では、ボイスメール番号は 1101 で、ボイスメール システムは FXS 音声ポート 1/1/1 に接続され、ボイスメールボックスの番号は 3001、3002、および 3006 です。

```

voice-port 1/1/1
 timing digit 250
 timing inter-digit 250

dial-peer voice 1102 pots
 destination-pattern 1101T
 port 1/1/1

call-manager-fallback
 timeouts interdigit 5
 ip source-address 1.6.0.199 port 2000
 max-ephones 24
 max-dn 24
 transfer-pattern 3...
 voicemail 1101
 call-forward busy 1101
 call-forward noan 1101 timeout 3
 moh minuet.au

vm-integration
 pattern direct * CGN
 pattern ext-to-ext no-answer # FDN #2
 pattern ext-to-ext busy # FDN #2
 pattern trunk-to-ext no-answer # FDN #2
 pattern trunk-to-ext busy # FDN #2

```

## BRI および PRI を介したボイスメール アクセスの設定：例

次の例は、無応答のコールをボイスメールに転送するように Cisco Unified SRST ルータを設定する方法を示しています。この例では、ボイスメール番号は 1101 で、ボイスメールシステムは BRI または PRI 音声ポートに接続され、ボイスメールボックスの番号は 3001、3002、および 3006 です。

```
controller T1 2/0
  framing esf
  clock source line primary
  linecode b8zs
  cablelength short 133
  pri-group timeslots 21-24

interface Serial2/0:23
  no ip address
  no logging event link-status
  isdn switch-type primary-net5
  isdn incoming-voice voice
  isdn T309-enable
  no cdp enable

voice-port 2/0:23

dial-peer voice 1102 pots
  destination-pattern 1101T
  direct-inward-dial
  port 2/0:23

call-manager-fallback
  timeouts interdigit 5
  ip source-address 1.6.0.199 port 2000
  max-ephones 24
  max-dn 24
  transfer-pattern 3...
  voicemail 1101
  call-forward busy 1101
  call-forward noan 1101 timeout 3
  moh minuet.au
```

## 関連情報

Cisco Unified SRST の監視および保守については、P.227 の「Cisco Unified SRST の監視と保守」に進んでください。

追加情報については、P.25 の「Cisco Unified SRST の概要」の P.40 の「その他の資料」を参照してください。





# ビデオ パラメータの設定

---

**Revised: July 11, 2008**

この章では、Cisco Unified Survivable Remote Site Telephony (SRST) ルータのビデオ パラメータを設定する方法について説明します。

## 内容

- [ビデオ パラメータを設定するための前提条件 \(P.212\)](#)
- [ビデオ パラメータの設定に関する制約事項 \(P.213\)](#)
- [ビデオ パラメータの設定について \(P.214\)](#)
- [Cisco Unified SRST のビデオ パラメータの設定方法 \(P.217\)](#)
- [Cisco Unified SRST のビデオのトラブルシューティング \(P.226\)](#)
- [関連情報 \(P.226\)](#)

## ビデオパラメータを設定するための前提条件

- Cisco Unified SRST 4.0 またはそれ以降のバージョンを使用していることを確認します。
- Cisco Unified Communications Manager 4.0 またはそれ以降のバージョンを使用していることを確認します。
- Cisco Unified SRST ルータに Cisco IP Phone が登録されていることを確認します。ephone の登録を確認するには、**show ephone registered** コマンドを使用します。
- Cisco Unified Video Advantage アプリケーションと Cisco Unified IP Phone 間の接続が正常に機能していることを確認します。

Cisco Unified Video Advantage 1.02 またはそれ以降のバージョンがインストールされた PC では、Cisco Unified Video Advantage と Cisco Unified IP Phone 間の回線がグリーンであることを確認してください。詳細については、『[Cisco Unified Video Advantage End User Guides](#)』を参照してください。

- 正しいビデオファームウェアが Cisco Unified IP Phone にインストールされていることを確認します。現在の ephone ファームウェアを表示するには、**show ephone phone-load** コマンドを使用します。ビデオに対応している最小限の Cisco Unified IP Phone のファームウェアバージョンは、次のとおりです。
  - Cisco Unified IP Phone 7940G バージョン 6.0(4)
  - Cisco Unified IP Phone 7960G バージョン 6.0(4)
  - Cisco Unified IP Phone 7970G バージョン 6.0(2)
- 基本的な Cisco Unified SRST の設定を実行します。詳細については、『[Cisco Unified SRST V4.0: Setting Up the Network](#)』を参照してください。
- 基本的な ephone の設定を実行します。詳細については、『[Cisco Unified SRST V4.0: Setting Up Cisco Unified IP Phones](#)』を参照してください。

## ビデオパラメータの設定に関する制約事項

- この機能がサポートしているのは、次のビデオコーデックに限られます。
  - H.261
  - H.263
- この機能がサポートしているのは、次のビデオ形式に限られます。
  - Common Intermediate Format (CIF) : 解像度 352x288
  - One-Quarter Common Intermediate Format (QCIF) : 解像度 176x144
  - Sub QIF (SQCIF) : 解像度 128x96
  - 4CIF : 解像度 704x576
  - 16CIF : 解像度 1408x1152
- **call start fast** 機能は、H.323 ビデオ接続ではサポートされません。H.323 ビデオには、**call start slow** を設定する必要があります。
- ビデオ機能は、回線ごとでなく、ephone ごとに設定されます。
- コール機能制御（ミュートや保留など）は、すべてオーディオコールとビデオコールの両方に適用されます（適用可能な場合）。
- この機能では、次の項目はサポートされていません。
  - ビデオ機能の動的な追加：ビデオ接続を利用するには、コール設定を開始する前に、ビデオ機能が存在している必要があります。
  - 2つのSCCPエンドポイントの間のT-120データ接続
  - ビデオのセキュリティ
  - SCCPエンドポイントでのFar-End Camera Control (FECC)
  - ビデオコーデックの再ネゴシエーション:ネゴシエートされたビデオコーデックと一致している必要があります。一致していない場合、コールはオーディオ専用でフォールバックします。新しいコールでは、既存コールでネゴシエートされたコーデックを使用できます。
  - ビデオコーデックの変換
- ビデオ対応のエンドポイントをオーディオ専用のエンドポイントに接続した場合、コールはオーディオ専用でフォールバックします。オーディオ専用のコールでは、ビデオメッセージはスキップされます。

## ビデオパラメータの設定について

この機能を使用すると、Cisco Unified SRST が Cisco Unified Communications Manager と同等の機能を保持するように、ビデオパラメータを設定できます。Cisco Unified SRST を有効にすると、すべての ephone が Cisco Unified Communications Manager で使用される同じ設定を保持するため、Cisco Unified IP Phone をビデオ機能用に再設定する必要はありません。ただし、call-manager-fallback コンフィギュレーションモードを開始して、Cisco Unified SRST のビデオパラメータを設定する必要があります。ビデオ用の機能セットは、Cisco Unified SRST オーディオコールの場合と同じです。

ビデオパラメータを設定するには、次の概念を理解する必要があります。

- [エンドポイント機能の一致 \(P.214\)](#)
- [ビデオコーデック情報の取得 \(P.214\)](#)
- [オーディオ専用のコールのフォールバック \(P.214\)](#)
- [ビデオエンドポイントでのコール設定 \(P.215\)](#)
- [RTP ビデオストリームの流れ \(P.216\)](#)

### エンドポイント機能の一致

エンドポイント機能は、電話機の登録時に Cisco Unified SRST に格納されます。これらの機能は、コール設定時に他のエンドポイントと照合するために使用されます。エンドポイントはいつでもアップデートできます。ただし、ルータがエンドポイントの機能の変更を認識するのは、コール設定時だけです。電話機にビデオ機能を追加した場合、その情報はルータの内部データ構造ではアップデートされますが、次にコールが発生するまで有効になりません。ビデオ機能が削除された場合、ルータは、コールが終了するまでは引き続きビデオ機能を認識しますが、2つのエンドポイント間でビデオストリームは交換されません。



(注) エンドポイント機能の照合は、新しいコールが設定されるか、既存のコールが再開されるたびに実行されます。

### ビデオコーデック情報の取得

音声ゲートウェイは、ダイヤルピア設定を使用してオーディオコーデックのコーデック情報を取得します。ビデオコーデックの選択は、エンドポイントによって実行されます。ダイヤルピアまたはその他の設定を通じて、H.323 Service Provider Interface (SPI) によって制御されることはありません。ビデオコーデックの情報は、コール設定時に機能要求を使用して SCCP エンドポイントから取得されます。

### オーディオ専用のコールのフォールバック

ビデオ対応のエンドポイントをオーディオ専用のエンドポイントに接続した場合、コールはオーディオ専用の接続にフォールバックします。また、会議などの特定の機能についても、ビデオサポートを使用できない場合、コールはオーディオ専用のコールにフォールバックします。

Cisco Unified SRST ルータは、コールがビデオ対応またはオーディオ専用のどちらであるかをコールタイプフラグを使用して示します。ビデオ機能が一致した場合、コールタイプフラグは video に設定されます。オーディオ専用の TDM またはオーディオ専用の SIP エンドポイントに接続している場合は、audio-only に設定されます。



(注) オーディオ専用での接続中は、ビデオ関連のすべてのメディアメッセージがスキップされます。

## ビデオエンドポイントでのコール設定

SCCP ビデオ エンドポイントを処理するプロセスは、SCCP オーディオ エンドポイントを処理する場合と同じです。ビデオ コールは、オーディオ コールの一部である必要があります。オーディオ コールの設定に失敗すると、ビデオ コールは失敗します。

ビデオ コールを設定するときに、メディアの設定処理によって、ビデオメディア パスが必要かどうかを判別されます。必要だと判別された場合は、対応するビデオメディア パス設定アクションが実行されます。

- SCCP エンドポイントの場合、ビデオメディア パスの設定には、エンドポイントにメッセージを送信してマルチメディア パスを開き、マルチメディアの伝送を開始することが含まれます。
- H.323 エンドポイントの場合、ビデオメディア パスの設定には、ビデオ ストリーム用の論理チャンネルを開くためにエンドポイント間で情報を交換することが含まれます。

コールタイプ フラグが設定されるのは、エンドポイント機能の照合に基づいてコールを設定するときです。コールが設定されると、追加のビデオメディア パスが必要かどうかをコールタイプ フラグを使用して判別されます。コールのシグナリングは Cisco Unified CME ルータによって管理され、同じルータ上の 2 つのビデオ対応 SCCP エンドポイント間でメディア ストリームが直接接続されます。ビデオ関連のコマンドおよびフロー制御メッセージは、他方のエンドポイントに転送されません。ルータはこれらのメッセージを解釈しません。

## 2 つのローカル SCCP エンドポイント間でのコール設定

同じルータ上に存在する 2 つのローカル SCCP エンドポイントの相互動作では、ビデオ コールの設定に、既存のすべてのオーディオ コール設定処理が使用されます (メディアの設定時を除く)。メディアの設定時には、ビデオメディア パスを確立するためのメッセージが送信されます。エンドポイントが応答すると、ビデオメディア パスが確立され、start-multimedia-transmission 関数が呼び出されます。

## SCCP エンドポイントと H.323 エンドポイント間でのコール設定

SCCP エンドポイントと H.323 エンドポイントの間のコール設定は、SCCP エンドポイント間のコール設定とほぼ同じです。唯一の違いは、ビデオ機能が選択されている場合、ビデオ Open Logical Channel (OLC) を要求するイベントが H.323 コール レッグに送信され、ゲートウェイがビデオ チャネル用の OLC を生成することです。ルータはメディア ストリームの終点と始点の両方になる必要があるため、コールの設定を開始する前に、ルータ上でビデオを有効にしておく必要があります。

## H.323 ネットワークを介した 2 つの SCCP エンドポイント間でのコール設定

SCCP エンドポイント間で H.323 ネットワークを経由してコールを設定する場合は、前の 2 つの項で示したプロセスを組み合わせることでコールを設定します。ルータは、2 つのエンドポイント間のビデオメディアの設定を制御し、ゲートウェイが OLC を生成できるようにイベントは H.323 コール レッグに送信されます。

## RTP ビデオ ストリームの流れ

2つのローカル SCCP エンドポイント間のビデオ ストリームの場合、Real-Time Transport Protocol (RTP) ストリームはフローアラウンド モードになります。SCCP エンドポイントと H.323 エンドポイントの間、またはそれぞれ別の Cisco Unified CME ルータ上にある 2 つの SCCP エンドポイントの間で発生するビデオ ストリームの場合、RTP ストリームはフロースルー モードになります。

- メディア フローアラウンド モードでは、ゲートウェイに関係なく、RTP パケットを VoIP コールのエンドポイント間で直接伝送できます。デフォルトでは、ゲートウェイは着信メディアを受信し、コールを終了して、発信コール レッグ上で再発信します。フローアラウンド モードの場合は、シグナリング データだけがゲートウェイに渡されるため、スケーラビリティとパフォーマンスが向上します。
- メディア フロースルー モードでは、オーディオ コールの場合と同じビデオメディア パスが関係しています。メディア パケットはゲートウェイを通過するので、ネットワークはどちらからも隠されます。

ローカルおよびリモート エンドポイントの発信者 ID 番号、IP アドレス、ポートなど、RTP 名前付きイベント パケットの情報を表示するには、`show voip rtp connection` コマンドを使用します。次に、出力の例を示します。

```
Router# show voip rtp connections
```

```
VoIP RTP active connections :
```

No.	CallId	dstCallId	LocalRTP	RmtRTP	LocalIP	RemoteIP
1	102	103	18714	18158	10.1.1.1	192.168.1.1
2	105	104	17252	19088	10.1.1.1	192.168.1.1

```
Found 2 active RTP connections
```

```
=====
```

## Cisco Unified SRST のビデオパラメータの設定方法

Cisco Unified SRST を有効にすると、すべての ephone が Cisco Unified Communications Manager で使用される同じ設定を保持するため、Cisco Unified IP Phone をビデオ機能用に再設定する必要はありません。ただし、Cisco Unified SRST のビデオパラメータは設定できます。

Cisco Unified SRST のビデオパラメータの設定には、次の作業が含まれます。

- [低速接続手順の設定 \(P.217\)](#)
- [Cisco Unified SRST の確認 \(P.218\)](#)
- [Cisco Unified SRST のビデオパラメータの設定 \(P.224\)](#)

### 低速接続手順の設定

ビデオストリームには、Cisco Unified SRST 用の低速接続手順が必要です。H.323 エンドポイントでも、接続メッセージの後にエンドポイント機能の一致が確認されるので、低速接続手順が必要です。



(注) 低速接続手順の詳細については、『[Configuring Quality of Service for Voice](#)』を参照してください。

低速接続手順を設定するには、次の手順を使用します。

#### 要約手順

1. `enable`
2. `configure terminal`
3. `voice service voip`
4. `h323`
5. `call start slow`

#### 詳細手順

	コマンドまたはアクション	目的
ステップ 1	<code>enable</code>  例: Router> enable	特権 EXEC モードを有効にします。  • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	<code>configure terminal</code>  例: Router# configure terminal	global コンフィギュレーション モードを開始します。
ステップ 3	<code>voice service voip</code>  例: Router(config)# voice service voip	voice-service コンフィギュレーション モードを開始します。
ステップ 4	<code>h323</code>  例: Router(config-voi-serv)# h323	H.323 voice-service コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 5	<pre>call start slow</pre> <p>例:</p> <pre>Router(config-serv-h323)# call start slow</pre>	H.323 ゲートウェイで、すべての VoIP コールに低速接続手順を強制的に使用します。

## Cisco Unified SRST の確認

Cisco Unified SRST 機能が有効であることと、Cisco Unified IP Phone の設定値を確認するには、次の手順を使用します。

### 要約手順

1. `enable`
2. `show running config`
3. `show call-manager-fallback all`

### 詳細手順

	コマンドまたはアクション	目的
ステップ 1	<pre>enable</pre> <p>例:</p> <pre>Router&gt; enable</pre>	特権 EXEC モードを有効にします。 <ul style="list-style-type: none"> <li>• プロンプトが表示されたら、パスワードを入力します。</li> </ul>
ステップ 2	<pre>show running config</pre> <p>例:</p> <pre>Router# show running config</pre>	実行コンフィギュレーション ファイルの内容をすべて表示します。
ステップ 3	<pre>show call-manager-fallback all</pre> <p>例:</p> <pre>Router# show call-manager-fallback all</pre>	フォールバック モード時のネットワーク内のすべての Cisco Unified IP Phone、電話番号、音声ポート、およびダイヤルピアの詳細な設定を表示します。



(注) 電話機のデフォルトのルータ IP アドレスが Cisco Unified SRST ルータの IP アドレスと一致することを確認するには、ネットワーク内の Cisco Unified IP Phone の *Settings* 表示を使用してください。



## 例

次に、**show call-manager-fallback all** コマンドの出力例を示します。

```
Router# show call-manager-fallback all

CONFIG (Version=3.3)
=====
Version 3.3
For on-line documentation please see:
www.cisco.com/univercd/cc/td/doc/product/access/ip_ph/ip_ks/index.htm

ip source-address 10.1.1.1 port 2000
max-video-bit-rate 384(kbps)
max-ephones 52
max-dn 110
max-conferences 16 gain -6
dspfarm units 0
dspfarm transcode sessions 0
huntstop
dialplan-pattern 1 4084442... extension-length 4
voicemail 6001
moh music-on-hold.au
time-format 24
date-format dd-mm-yy
timezone 0 Greenwich Standard Time
call-forward busy 6001
call-forward noan 6001 timeout 8
call-forward pattern .T
transfer-pattern .T
keepalive 45
timeout interdigit 10
timeout busy 10
timeout ringing 180
caller-id name-only: enable
Limit number of DNS per phone:
  7910: 34
  7935: 34
  7936: 34
  7940: 34
  7960: 34
  7970: 34
Log (table parameters):
  max-size: 150
  retain-timer: 15
transfer-system full-consult
local directory service: enabled.

ephone-dn 1
number 1001
name 1001
description 1001
label 1001
preference 0 secondary 9
huntstop
call-forward busy 6001
call-forward noan 6001 timeout 8
call-waiting beep

ephone-dn 2
number 1002
name 1002
description 1002
preference 0 secondary 9
huntstop
call-forward busy 6001
call-forward noan 6001 timeout 8
call-waiting beep

ephone-dn 3
```

```
preference 0 secondary 9  
huntstop  
call-waiting beep
```

```
ephone-dn 4  
preference 0 secondary 9  
huntstop  
call-waiting beep
```

```
ephone-dn 5  
preference 0 secondary 9  
huntstop  
call-waiting beep
```

```
ephone-dn 6  
preference 0 secondary 9  
huntstop  
call-waiting beep
```

```
ephone-dn 7  
preference 0 secondary 9  
huntstop  
call-waiting beep
```

```
ephone-dn 8  
preference 0 secondary 9  
huntstop  
call-waiting beep
```

```
ephone-dn 9  
preference 0 secondary 9  
huntstop  
call-waiting beep
```

```
ephone-dn 10  
preference 0 secondary 9  
huntstop  
call-waiting beep
```

```
ephone-dn 11  
preference 0 secondary 9  
huntstop  
call-waiting beep
```

```
ephone-dn 12  
preference 0 secondary 9  
huntstop  
call-waiting beep
```

```
ephone-dn 13  
preference 0 secondary 9  
huntstop  
call-waiting beep
```

```
ephone-dn 14  
preference 0 secondary 9  
huntstop  
call-waiting beep
```

```
ephone-dn 15  
preference 0 secondary 9  
huntstop  
call-waiting beep
```

```
ephone-dn 16  
preference 0 secondary 9  
huntstop  
call-waiting beep
```

```
ephone-dn 17  
preference 0 secondary 9
```

```
huntstop
call-waiting beep

ephone-dn 18
preference 0 secondary 9
huntstop
call-waiting beep

ephone-dn 19
preference 0 secondary 9
huntstop
call-waiting beep

ephone-dn 20
preference 0 secondary 9
huntstop
call-waiting beep

Number of Configured ephones 0 (Registered 2)

voice-port 50/0/1
station-id number 1001
station-id name 1001
timeout ringing 8
!
voice-port 50/0/2
station-id number 1002
station-id name 1002
timeout ringing 8
!
voice-port 50/0/3
!
voice-port 50/0/4
!
voice-port 50/0/5
!
voice-port 50/0/6
!
voice-port 50/0/7
!
voice-port 50/0/8
!
voice-port 50/0/9
!
voice-port 50/0/10
!
voice-port 50/0/11
!
voice-port 50/0/12
!
voice-port 50/0/13
!
voice-port 50/0/14
!
voice-port 50/0/15
!
voice-port 50/0/16
!
voice-port 50/0/17
!
voice-port 50/0/18
!
voice-port 50/0/19
!
voice-port 50/0/20
!

dial-peer voice 20055 pots
destination-pattern 1001
huntstop
```

```
call-forward busy 6001
call-forward noan 6001
progress_ind setup enable 3
port 50/0/1

dial-peer voice 20056 pots
destination-pattern 1002
huntstop
call-forward busy 6001
call-forward noan 6001
progress_ind setup enable 3
port 50/0/2

dial-peer voice 20057 pots
huntstop
progress_ind setup enable 3
port 50/0/3

dial-peer voice 20058 pots
huntstop
progress_ind setup enable 3
port 50/0/4

dial-peer voice 20059 pots
huntstop
progress_ind setup enable 3
port 50/0/5

dial-peer voice 20060 pots
huntstop
progress_ind setup enable 3
port 50/0/6

dial-peer voice 20061 pots
huntstop
progress_ind setup enable 3
port 50/0/7

dial-peer voice 20062 pots
huntstop
progress_ind setup enable 3
port 50/0/8

dial-peer voice 20063 pots
huntstop
progress_ind setup enable 3
port 50/0/9

dial-peer voice 20064 pots
huntstop
progress_ind setup enable 3
port 50/0/10

dial-peer voice 20065 pots
huntstop
progress_ind setup enable 3
port 50/0/11

dial-peer voice 20066 pots
huntstop
progress_ind setup enable 3
port 50/0/12

dial-peer voice 20067 pots
huntstop
progress_ind setup enable 3
port 50/0/13

dial-peer voice 20068 pots
huntstop
progress_ind setup enable 3
```

```
port 50/0/14

dial-peer voice 20069 pots
  huntstop
  progress_ind setup enable 3
port 50/0/15

dial-peer voice 20070 pots
  huntstop
  progress_ind setup enable 3
port 50/0/16

dial-peer voice 20071 pots
  huntstop
  progress_ind setup enable 3
port 50/0/17

dial-peer voice 20072 pots
  huntstop
  progress_ind setup enable 3
port 50/0/18

dial-peer voice 20073 pots
  huntstop
  progress_ind setup enable 3
port 50/0/19

dial-peer voice 20074 pots
  huntstop
  progress_ind setup enable 3
port 50/0/20

tftp-server system:/its/SEPDEFAULT.cnf
tftp-server system:/its/SEPDEFAULT.cnf alias SEPDefault.cnf
tftp-server system:/its/XMLDefault.cnf.xml alias XMLDefault.cnf.xml
tftp-server system:/its/ATADefault.cnf.xml
tftp-server system:/its/united_states/7960-tones.xml alias
United_States/7960-tones.xml
tftp-server system:/its/united_states/7960-font.xml alias
English_United_States/7960-font.xml
tftp-server system:/its/united_states/7960-dictionary.xml alias
English_United_States/7960-dictionary.xml
tftp-server system:/its/united_states/7960-kate.xml alias
English_United_States/7960-kate.xml
tftp-server system:/its/united_states/SCCP-dictionary.xml alias
English_United_States/SCCP-dictionary.xml
tftp-server system:/its/XMLDefault7960.cnf.xml alias SEP003094C2772E.cnf.xml
tftp-server system:/its/XMLDefault7960.cnf.xml alias SEP001201372DD1.cnf.xml
tftp-server system:/its/XMLDefault7960.cnf.xml alias SEPFFDD00000001.cnf.xml
tftp-server system:/its/XMLDefault7960.cnf.xml alias SEPFFDD00000002.cnf.xml
tftp-server system:/its/XMLDefault7960.cnf.xml alias SEPFFDD00000003.cnf.xml
tftp-server system:/its/XMLDefault7960.cnf.xml alias SEPFFDD00000004.cnf.xml
tftp-server system:/its/XMLDefault7960.cnf.xml alias SEPFFDD00000005.cnf.xml
tftp-server system:/its/XMLDefault7960.cnf.xml alias SEPFFDD00000006.cnf.xml
tftp-server system:/its/XMLDefault7960.cnf.xml alias SEPFFDD00000007.cnf.xml
tftp-server system:/its/XMLDefault7960.cnf.xml alias SEPFFDD00000008.cnf.xml
tftp-server system:/its/XMLDefault7960.cnf.xml alias SEPFFDD00000009.cnf.xml
tftp-server system:/its/XMLDefault7960.cnf.xml alias SEPFFDD0000000A.cnf.xml
tftp-server system:/its/XMLDefault7960.cnf.xml alias SEPFFDD0000000B.cnf.xml
tftp-server system:/its/XMLDefault7960.cnf.xml alias SEPFFDD0000000C.cnf.xml
tftp-server system:/its/XMLDefault7960.cnf.xml alias SEPFFDD0000000D.cnf.xml
tftp-server system:/its/XMLDefault7960.cnf.xml alias SEPFFDD0000000E.cnf.xml
tftp-server system:/its/XMLDefault7960.cnf.xml alias SEPFFDD0000000F.cnf.xml
tftp-server system:/its/XMLDefault7960.cnf.xml alias SEPFFDD00000010.cnf.xml
tftp-server system:/its/XMLDefault7960.cnf.xml alias SEPFFDD00000011.cnf.xml
tftp-server system:/its/XMLDefault7960.cnf.xml alias SEPFFDD00000012.cnf.xml
```

## Cisco Unified SRST のビデオパラメータの設定

Cisco Unified SRST システムのすべてのビデオ対応電話機の最高ビット レートを設定するには、次の手順を使用します。

### 要約手順

1. `enable`
2. `configure terminal`
3. `call-manager-fallback`
4. `video`
5. `maximum bit-rate value`

### 詳細手順

	コマンドまたはアクション	目的
ステップ 1	<code>enable</code>  例: Router> enable	特権 EXEC モードを有効にします。  • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	<code>configure terminal</code>  例: Router# configure terminal	global コンフィギュレーション モードを開始します。
ステップ 3	<code>call-manager-fallback</code>  例: Router(config)# call-manager-fallback	call-manager-fallback コンフィギュレーション モードを開始します。
ステップ 4	<code>video</code>  例: Router(config-call-manager-fallback)# video	call-manager-fallback video コンフィギュレーション モードを開始します。
ステップ 5	<code>maximum bit-rate value</code>  例: Router(conf-cm-fallback-video)# maximum bit-rate 256	IP Phone のビデオの最大帯域幅を Kbps 単位で設定します。範囲は 0 ~ 10000000 です。デフォルトは 10000000 です。

## 例

次の例では、Cisco Unified SRST のビデオに対する設定を示します。

```
call-manager-fallback
  video
    maximum bit-rate 384
max-conferences 2 gain -6
transfer-system full-consult
ip source-address 10.0.1.1 port 2000
max-ephones 52
max-dn 110
dialplan-pattern 1 4084442... extension-length 4
transfer-pattern .T
keepalive 45
voicemail 6001
call-forward pattern .T
call-forward busy 6001
call-forward noan 6001 timeout 3
moh music-on-hold.au
time-format 24
date-format dd-mm-yy
!
```

## Cisco Unified SRST のビデオのトラブルシューティング

Cisco Unified SRST のビデオのトラブルシューティングを行うには、次のコマンドを使用します。

- SCCP エンドポイントのトラブルシューティングを行うには、次の **debug** コマンドを使用します。
  - **debug cch323 video** : H.323 SPI のビデオ デバッグ トレースを有効にします。
  - **debug ephone detail** : ルータに登録されているすべての Cisco Unified IP Phone をデバッグし、エラーと状態レベルを表示します。
  - **debug h225 asn1** : 送信または受信された H.225 メッセージの Abstract Syntax Notation One (ASN.1) の内容を表示します。
  - **debug h245 asn1** : 送信または受信された H.245 メッセージの ASN.1 の内容を表示します。
  - **debug voip ccapi inout** : Call-Control-Application Programming Interface (CCAPI) を通じた実行パスを表示します。
- ephone のトラブルシューティングを行うには、次の **debug** コマンドを使用します。
  - **debug ephone message** : Cisco ephone 間のメッセージのトレースを有効にします。
  - **debug ephone register** : ephone の登録のデバッグを設定します。
  - **debug ephone video** : ephone のビデオのトレースを設定します。これらのトレースは、ビデオ機能の選択、起動、停止を含む、コールに関する各種のビデオ状態情報を提供します。
- 基本的なビデオ対ビデオ コールを検証するには、次の **show** コマンドを使用します。
  - **show call active video** : 進行中の SCCP ビデオ コールのコール情報を表示します。
  - **show ephone offhook** : 受話器がオフフックの状態になっている ephone の情報およびパケット数を表示します。
  - **show ephone registered** : 登録済みの ephone のステータスを表示します。
  - **show voip rtp connections** : ローカルおよびリモート エンドポイントの発信者 ID 番号、IP アドレス、ポートなど、RTP 名前付きイベント パケットの情報を表示します。

## 関連情報

これらのコマンドの詳細については、『[Cisco Unified SRST and Cisco Unified SIP SRST Command Reference \(All Versions\)](#)』を参照してください。

追加情報については、P.25 の「Cisco Unified SRST の概要」の P.40 の「その他の資料」を参照してください。





# Cisco Unified SRST の監視と保守

Revised: July 11, 2008

Cisco Unified Survivable Remote Site Telephony (SRST) の監視と保守を行うには、特権 EXEC モードで次のコマンドを使用します。

コマンド	目的
Router# <b>show running-config</b>	設定を表示します。
Router# <b>show call-manager-fallback all</b>	Cisco Unified IP Phone、音声ポート、および Cisco Unified SRST ルータのダイヤル ピアの詳細情報を表示します。
Router# <b>show call-manager-fallback dial-peer</b>	Cisco Unified SRST ルータのダイヤル ピアの出力を表示します。
Router# <b>show call-manager-fallback ephone-dn</b>	CallManager フォールバック モードの Cisco Unified IP Phone の宛先電話番号を表示します。
Router# <b>show call-manager-fallback voice-port</b>	音声ポートの出力を表示します。
Router# <b>show ephone phone</b>	Cisco Unified IP Phone のステータスを表示します。
Router# <b>show ephone offhook</b>	オフフックの状態になっているすべての電話機に関する Cisco Unified IP Phone のステータスを表示します。
Router# <b>show ephone registered</b>	現在登録されているすべての電話機に関する Cisco Unified IP Phone のステータスを表示します。
Router# <b>show ephone remote</b>	ローカル以外のすべての電話機 (アドレス解決プロトコル (ARP) のエントリがない電話機) に関する Cisco Unified IP Phone のステータスを表示します。
Router# <b>show ephone ringing</b>	呼び出し音が鳴っている電話機に関する Cisco Unified IP Phone のステータスを表示します。
Router# <b>show ephone summary</b>	すべての Cisco Unified IP Phone に関する要約を表示します。
Router# <b>show ephone telephone-number phone-number</b>	特定の電話番号に関する Unified IP Phone のステータスを表示します。
Router# <b>show ephone unregistered</b>	登録されていないすべての電話機に関する Unified IP Phone のステータスを表示します。
Router# <b>show ephone-dn tag</b>	Unified IP Phone の宛先の電話番号を表示します。
Router# <b>show ephone-dn summary</b>	すべての Cisco Unified IP Phone の宛先電話番号に関する要約を表示します。
Router# <b>show ephone-dn loopback</b>	ループバック モードの Cisco Unified IP Phone の宛先電話番号を表示します。

コマンド	目的
Router# <code>show voice port summary</code>	すべての音声ポートに関する要約を表示します。
Router# <code>show dial-peer voice summary</code>	すべての音声ダイヤルピアに関する要約を表示します。

## 関連情報

これらのコマンドの詳細については、『[Cisco Unified SRST and Cisco Unified SIP SRST Command Reference \(All Versions\)](#)』を参照してください。

追加情報については、P.25 の「[Cisco Unified SRST の概要](#)」の P.40 の「[その他の資料](#)」を参照してください。



# E911 サービス

---

**Revised: July 11, 2008**

この章では、Enhanced 911 (E911) サービス機能について説明します。

## この章の機能情報について

お使いの Cisco Unified SRST バージョンによっては、この章に記載されている機能の一部または全部がサポートされていない場合があります。各機能をサポートしているバージョンのリストについては、[P.264 の「E911 サービスの機能情報」](#)を参照してください。

## 内容

- [前提条件 \(P.230\)](#)
- [制約事項 \(P.230\)](#)
- [E911 サービスについて \(P.231\)](#)
- [E911 サービスの設定 \(P.242\)](#)
- [E911 サービスの設定例 \(P.258\)](#)
- [E911 サービスの機能情報 \(P.264\)](#)
- [関連情報 \(P.264\)](#)

## 前提条件

- Cisco Unified SRST 4.1 以降のバージョン。
- SCCP 電話機または SIP 電話機が Cisco Unified SRST サーバに登録されていること。
- 911 サービス プロバイダーの Public Safety Answering Point (PSAP) ごとに、最低 1 つの CAMA トランクまたは ISDN トランクが、Cisco Unified SRST から設定されていること。
- お客様の音声ネットワークごとに 1 つの E911 ネットワークが設計されていること。
- Cisco Unified SRST で FXS、FXO、SIP、または H.323 のトランク インターフェイスを使用できること。

## 制約事項

- Cisco Unified SRST の E911 サービスは、Cisco Emergency Responder とインターフェイスしません。
- 911 を最後にコールした電話機に関する情報は、Cisco Unified SRST のリポート後は保持されません。
- Cisco Unified Wireless IP Phone 7920 および 7921 の場合、発信者のロケーションは、システム管理者が設定した静的（固定）情報でのみ決定されます。詳細については、[P.236 の「携帯電話に関する注意事項」](#)を参照してください。
- 911 発信者の内線番号の変換先となる番号は、Emergency Response Location (ERL; 緊急応答ロケーション) ごとに 2 つの Emergency Location Identification Number (ELIN; 緊急ロケーション識別番号) に限られます。詳細については、[P.231 の「概要」](#)を参照してください。
- ELIN を複数の目的に使用すると、既存の Cisco Unified SRST 機能との間に予期しない相互作用が引き起こされる可能性があります。このような ELIN の多重使用の例には、ELIN を実際の電話番号 (ephone-dn、voice register dn、または FXS destination-pattern)、コール ピックアップ番号、またはエイリアス再ルーティング番号として使用するように設定することなどがあります。詳細については、[P.239 の「ELIN の複数の用途」](#)を参照してください。
- E911 サービスの設定によっては、既存の Cisco Unified SRST 機能と相互作用して、予期しない動作の原因になることがあります。E911 サービスと既存の Cisco Unified SRST 機能との相互作用の詳細については、[P.238 の「既存の Cisco Unified SRST 機能との相互作用」](#)を参照してください。

## E911 サービスについて

ここでは、E911 サービスに関する次の情報について説明します。

- [概要 \(P.231\)](#)
- [コール処理 \(P.233\)](#)
- [バージョン 4.2\(1\) の新機能 \(P.236\)](#)
- [携帯電話に関する注意事項 \(P.236\)](#)
- [E911 サービスの実装の計画 \(P.236\)](#)
- [既存の Cisco Unified SRST 機能との相互作用 \(P.238\)](#)

### 概要

Cisco Unified SRST の E911 サービスを使用すると、911 オペレータは次のことを実行できます。

- 発信番号に基づいて、911 発信者のロケーションをすばやく正確に特定する
- 接続解除が発生した場合、911 発信者にコールバックする

この機能が導入されるまでは、Cisco Unified SRST では 911 への発信コールしかサポートされていませんでした。911 の基本機能では、コールは単に Public Safety Answering Point (PSAP) にルーティングされるだけでした。PSAP では、911 オペレータが発信者から口頭で緊急情報とロケーションを確認したうえで、救急車サービス、消防署、または警察から応答チームを派遣する必要がありました。また、カバーする管轄地区に基づいて、別の PSAP にコールをルーティングすることもできませんでした。

E911 サービスの場合、911 コールは、発信者のロケーションに基づいて、最も近い PSAP に選択的にルーティングされます。また、発信者の電話番号と住所が PSAP の端末に自動的に表示されます。このため、PSAP では、発信者がロケーションを伝えられなくても、すばやく緊急救助を派遣できます。また、発信者が途中で接続解除した場合でも、911 発信者への連絡に必要な情報は PSAP に残ります。

E911 サービスを使用するには、Cisco Unified SRST でサポートされるすべての電話機をカバーするのに必要な管轄地区ごとの緊急応答ロケーション (ERL) を定義する必要があります。ERL の管轄地区は、地域法によって決定されます。たとえば、ERL の最大床面積が 7,000 平方フィート未満であるために、ERL を建物のフロアごとに定義する必要があるとします。ERL は既知で特定のロケーションを定義するので、この情報は PSAP のデータベースにアップロードされます。911 の通信指令係は、この情報を使用して、緊急応答チームがすばやく発信者の位置を確認できるようにします。

PSAP では、911 発信者に割り当てられている ERL を特定するために、発信者の固有の電話番号を使用します。この番号は、緊急ロケーション識別番号 (ELIN) とも呼ばれます。E911 サービスを使用するには、まず、各 ERL の ELIN と番地のリストを PSAP に提供する必要があります。この情報は、PSAP の ALI (Automatic Location Identification; 自動ロケーション識別) データベースに保存されます。通常は、電話システムをインストールしたときに、この情報を PSAP に提供します。

PSAP では、ALI データベースの住所情報を使用して、発信者のロケーションを検索できます。また、ELIN を使用して、指定の期限内に 911 発信者にコールバックできます。この期限は、Last Caller テーブルに適用されます。Last Caller テーブルは、PSAP に 911 発信者の ELIN を提供します。Last Caller テーブルに期限が指定されていない場合、デフォルトの有効期限は 3 時間です。

コール情報を一時的な Last Caller テーブルに保存するだけでなく、永続的な呼詳細レコードを設定することもできます。このようなレコードのアトリビュートは、RADIUS アカウンティング、syslog サービス、または CLI show コマンドから表示できます。

必要に応じて、各 ERL に設定する ELIN の数を、0、1、2 の中から選択できます。2 つの ELIN を設定した場合、ラウンドロビンのアルゴリズムを使用して、PSAP に送信される ELIN が選択されます。ERL の ELIN が定義されていない場合、PSAP では発信番号が表示されます。Cisco Unified SRST でダイヤルイン番号が使用されている場合や、コールが別の Cisco 音声ゲートウェイからのもので、すでに内線番号が ELIN に変換されている場合は、ELIN を定義しなくてもかまいません。

オプションで、911 発信者の IP Phone のアドレスがどのゾーンのどのロケーションの IP サブネットとも一致しない場合に PSAP が使用できるデフォルトの ELIN を定義します。このデフォルトの ELIN は、いずれかの ERL にすでに定義されている既存の ELIN でも、固有の ELIN でもかまいません。デフォルトの ELIN が定義されておらず、911 発信者の IP アドレスがどの ERL の IP サブネットとも一致しない場合は、デフォルトの ELIN が定義されていないことを示す syslog メッセージが発行され、元の ANI がそのままの状態となります。

タイムアウトの発生またはシステムの再起動により Last Caller テーブル内のコールバック情報が失われた場合、または他の何らかの理由で PSAP が発信者の ELIN またはデフォルト ELIN で 911 発信者に到達できない場合に使用される、指定コールバック番号を定義することもできます。

Last Caller テーブル内のデータの有効期限を指定したり、すべての緊急コールを通知する syslog メッセージを有効にしたりすることで、さらにシステムをカスタマイズできます。

大規模なインストレーションでは、オプションで、特定の ERL からのコールが特定の PSAP にルーティングされるように指定できます。これを行うには、緊急応答ゾーンを設定します。緊急応答ゾーンは、各ゾーン内の ERL のリストを示します。この ERL リストには、ロケーションのランキングも含まれます。このランキングは、複数の PSAP が存在する場合に ERL 検索順序を制御します。システム上のすべての 911 コールが 1 つの PSAP にルーティングされる場合は、緊急応答ゾーンを設定する必要はありません。

1 つ以上の ERL を 1 つのゾーンにグループ化できます。ゾーンは、PSAP のサービス対象領域に相当します。緊急コールが発信されると、設定されている緊急応答ゾーンで、任意の順序で ERL のサブセットを検索できます。ERL を必要な順序でランキングできます。

また、異なる PSAP に 911 コールを選択的にルーティングするためにゾーンが使用されます。選択的なルーティングを設定するには、固有のロケーションのリストでゾーンを作成し、各ゾーンを別の発信ダイヤル ピアに割り当てます。この場合、ゾーンは発信者の ERL に基づいてコールをルーティングします。緊急コールが発信されると、着信番号に一致する各ダイヤル ピアは、ゾーンのロケーション リストを使用して、発信電話機の IP アドレスに一致する IP サブネットを見つけます。ERL と ELIN が見つかった場合、ダイヤル ピアのインターフェイスを使用してコールがルーティングされます。ERL または ELIN が見つからない場合、次に一致するダイヤル ピアがそのゾーンをチェックします。



**(注)** 発信者の IP アドレスが、そのダイヤル ピアのゾーンのどのロケーションとも一致しない場合、最後に一致したダイヤル ピアがルーティングに使用され、デフォルトの ELIN が使用されます。

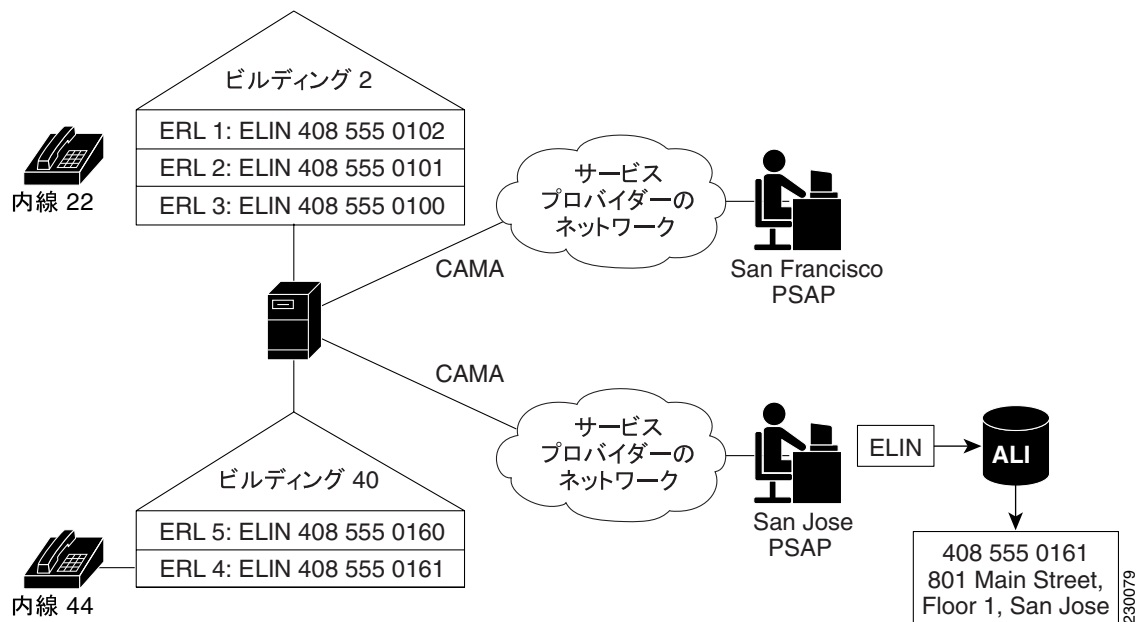
同じ宛先パターン (911) の複数のダイヤル ピアが存在し、ゾーンが異なる場合、特定の電話機からの 911 コールが必ず同じダイヤル ピアを使用するためには、プリファレンス フィールドを設定することにより、優先するダイヤル ピアの優先順位が最も高くなるように設定する必要があります。

同じゾーンでは、重複したロケーション タグを使用できません。ただし、複数のゾーンに同じロケーション タグを定義できます。同じゾーンに、重複したロケーション優先順位を入力できます。ただし、その場合は、既存のロケーションの優先順位が 1 つ大きい数値になります。たとえば、「location 36 priority 5」を設定してから、「location 19 priority 5」を設定すると、ロケーション 19 の

優先順位は 5 ですが、ロケーション 36 は優先順位 6 になります。また、2 つのロケーションに優先順位 100 が割り当てられた場合、最初のロケーションは、優先順位 101 になるのではなく、優先順位のない最初のロケーションになります。

図 15 に、911 サービスの設定例を示します。この例では、電話システムが複数の建物の複数のフロアからのコールを処理します。5 つの ERL が定義されており、ERL ごとに ELIN が 1 つ定義されています。PSAP では、ELIN は発信者の物理的な住所を ALI データベースで検索するのに使用されます。この例では、ビルディング 2 が San Francisco の PSAP の近くにあり、ビルディング 40 が San Jose の PSAP の近くにあります。したがって、この場合は、2 つの緊急応答ゾーンを設定して、911 コールが発信者に最も近い PSAP にルーティングされるようにすることをお勧めします。この例では、ビルディング 2 のすべての ERL を含む緊急応答ゾーンと、ビルディング 40 の ERL を含む別のゾーンを設定できます。緊急応答ゾーンを設定しない場合、911 コールは、発信ダイヤル ピアに設定されている宛先番号との一致に基づいてルーティングされます。

図 15 E911 の実装



## コール処理

Cisco Unified SRST で 911 コールが受信されたとき、最初は他のコールと同じように処理されます。Cisco Unified SRST では、着信番号を取得し、その着信番号にコールをルーティングするのに使用できるダイヤル ピアを検索します。

E911 機能を使用すると、発信ダイヤル ピアの宛先が PSAP かどうかを分析することもできます。発信ダイヤル ピアが **emergency response zone** コマンドで設定されている場合、コールが E911 処理を必要とすることがシステムに通知されます。発信ダイヤル ピアが **emergency response zone** コマンドで設定されていない場合、E911 機能はアクティブにならず、発信者の番号は ELIN に変換されません。

E911 機能がアクティブな場合、E911 処理の最初の手順として、発信者に割り当てられる ERL が決定されます。発信者の ERL は、次のいずれかの方法で決定されます。

- 明示的な割り当て：ERL が割り当てられている着信ダイヤル ピアに 911 コールが到着した場合、この ERL は自動的に発信者のロケーションとして使用されます。
- 暗黙的な割り当て：911 コールが IP Phone から到着した場合は、その IP アドレスが特定されません。E911 では、ERL で設定されている IP サブネットの 1 つで、発信者の電話機の IP アドレスが検索されます。ERL はタグ番号に従って順序リストとして格納され、各サブネットはリスト順に発信者の IP アドレスと比較されます。

発信者の ERL が特定された後、発信者の電話番号がその ERL の ELIN に変換されます。特定のコールに対して明示的にも暗黙的にも ERL が割り当てられていない場合は、IP Phone のデフォルトの ERL を定義できます。このデフォルトの ERL は、IP Phone 以外のエンドポイント（VoIP トランクや FXS/FXO トランクの電話機など）には適用されません。

コールの ELIN が決定された後、次の情報が Last Caller テーブルに保存されます。

- 発信者の ELIN
- 発信者の内線番号
- コールが発信された時間

Last Caller テーブルには、各 ERL からの最後の緊急コールの発信者についての情報が格納されます。発信者の情報は、コールが発信されてから指定の有効期限が経過すると、テーブルから消去されます。期限が指定されていない場合、デフォルトの有効期限は 3 時間です。

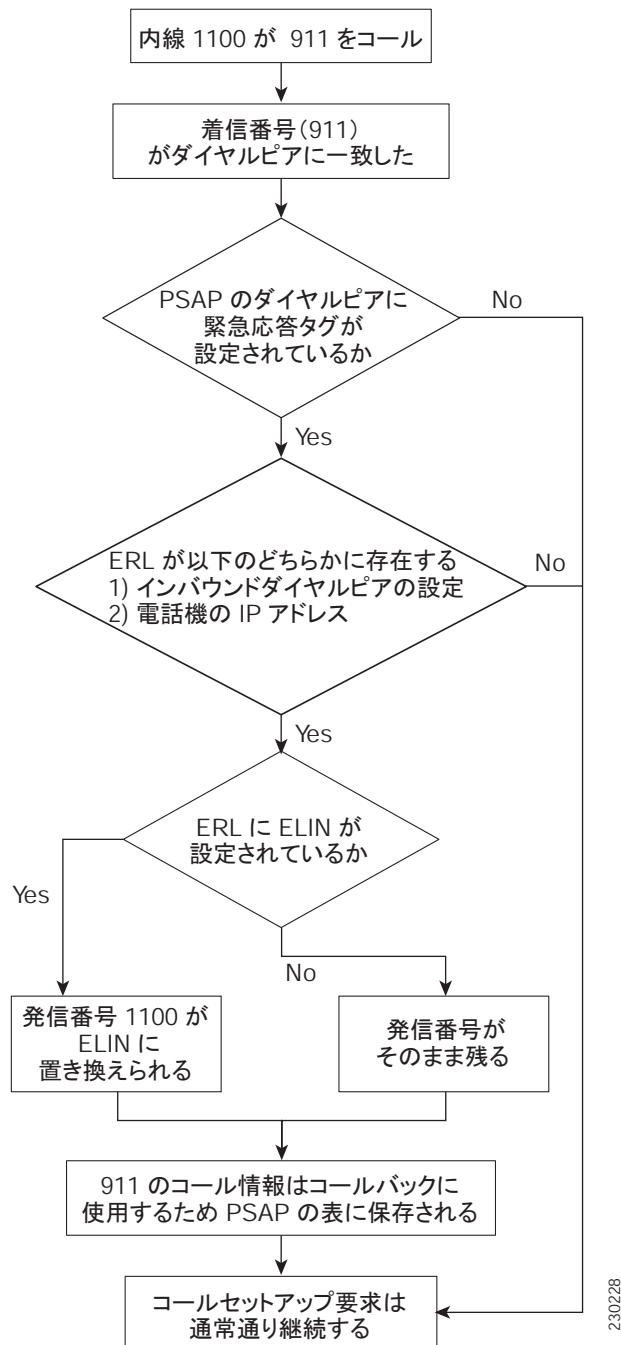
911 コール情報が Last Caller テーブルに保存された後、システムは、発信者の ERL を含む緊急応答ゾーンが設定されているかどうか調べます。発信者の ERL を含む緊急応答ゾーンが設定されていない場合は、発信者の IP アドレスと照合するためにすべての ERL が順次検索され、適切な PSAP に 911 コールがルーティングされます。ERL がゾーンに含まれている場合は、そのゾーンに関連付けられている PSAP に 911 コールがルーティングされます。

適切な PSAP に 911 コールがルーティングされたら、E911 処理は完了です。その後、コール処理は基本コールの場合と同様に進行しますが、発信設定要求の際は発信番号が ELIN に置き換えられます。

図 16 は、911 コール処理の手順をまとめたものです。



図 16 911 コールの処理



ルータがリポートされるか、コールが発信されてから指定の有効期限（デフォルトでは 3 時間）が経過すると、911 オペレータは Last Caller テーブルでコールに関する情報を見つけることができません。その場合は、911 オペレータにリオーダー トーンが再生されます。このトーンが 911 オペレータに再生されないようにするには、P.245 の「E911 サービスの発信ダイヤルピアの設定」の説明に従ってデフォルトのコールバックを設定します。また、ダイヤルピアでコール自動転送番号を設定して、オペレータが業務の窓口に転送されるようにします。

911 コールバック機能は最後の発信者とその内線番号で追跡するので、911 コールと 911 コールバックの間および有効期限内に ephone-dn の設定を変更すると、PSAP が最後の 911 発信者に正常に連絡できないことがあります。

2 つの 911 コールが同じ ERL の異なる電話機から短時間に発信された場合、Last Caller テーブルの最初の発信者の情報は、2 番目の発信者の情報で上書きされます。テーブルには 1 つの ERL につき 1 人の発信者の情報しか格納されないため、911 オペレータには最初の発信者への連絡に必要な情報が残りません。

ほとんどの場合、Cisco Emergency Responder が設定されていれば、Cisco Emergency Responder と同じ ELIN と ERL のデータを使用して、E911 サービスを設定する必要があります。

## バージョン 4.2(1) の新機能

E911 サービスのバージョン 4.2(1) には、次の新機能が備わっています。

- ゾーンへの ERL の割り当てによる、発信者に最も近い PSAP へのルーティングの有効化
- E911 のカスタマイズ ( デフォルト ELIN の定義、コールバック時に 911 発信者に到達できない場合の指定番号の設定、Last Caller テーブル内のデータの有効期限の指定、およびすべての緊急コールを通知する syslog メッセージの有効化 )
- E911 ロケーション情報の拡張による名前およびアドレスの追加
- 新しい永続的な呼詳細レコードの追加
- トラブルシューティングのための新しいコマンドの追加

## 携帯電話に関する注意事項

地域保安当局は、プライマリ サイトから離れている電話機からの緊急コールに応答しない可能性があります。IP Phone が、最初に設定されたサイトから離れている場合は、IP Phone を緊急コールに使用しないでください。携帯電話のユーザには、下記のようなポリシーへの同意を求めるとをお勧めします。

在宅勤務、遠隔オフィス、旅行などの場合の緊急コールには、ローカル側で設定されているホテル、オフィス、または自宅の固定電話を使用する必要があります。設定済みのサイトから離れているときに、リモートの IP 電話を緊急コールに使用する必要がある場合は、緊急応答機関やセキュリティオペレーションセンターの担当者に、ロケーション ( 国、市、州、番地など ) についての特定情報を伝える必要があります。

このポリシーへの同意をもって、携帯電話ユーザは次のことを確認します。

- この注意事項を理解していること
- 設定済みのサイトから離れているときは、リモートの IP Phone を緊急コールに使用しないよう注意することに同意していること

このポリシーへの応答や同意がない場合、携帯電話ユーザは、自分に関連付けられたすべての IP Phone が接続解除され、サービス継続の要望も実現されないことを承知したと見なされます。

## E911 サービスの実装の計画

Cisco Unified SRST の E911 サービスを設定する前に、次の手順に従ってインストレーションを計画してください。



(注)

この手順で説明する機能の中には、Cisco Unified SRST の一部のバージョンでしか使用できないものがあります。ご使用のバージョンで機能を使用できるかどうかを調べるには、[P.236 の「バージョン 4.2\(1\) の新機能」](#)を参照してください。

**ステップ 1** Cisco Unified SRST のサービスの対象となるサイト、および各サイトにサービスを提供する PSAP のリストを作成します。

各 PSAP への接続には CAMA または PRI インターフェイスを使用する必要があります。表 13 は、収集する必要のある情報の例を示しています。

**表 13 サイトと PSAP の情報**

建物の名前と住所	担当する PSAP	コールがルーティングされるインターフェイス
Building 2, 201 Maple Street, San Francisco	San Francisco, CA	ポート 1/0:D
Building 40, 801 Main Street, San Jose	San Jose, CA	ポート 1/1:D

**ステップ 2** 地域法を使用して、設定に必要な ERL の数を決定します。

National Emergency Number Association (NENA) のモデル法に従って、緊急応答チームがそのロケーション内で発信者の位置をすばやく確認できるほど明確にロケーションを指定します。表 14 に例を示します。

**表 14 ERL の計算**

建物	床面積(平方フィート)	フロア数	必要な ERL の数
Building 2	200,000	3	3
Building 40	7000	2	1

**ステップ 3** (オプション) ERL ごとに 1 つまたは 2 つの ELIN を割り当てます。

電話サービス プロバイダーに連絡して、ELIN として指定される電話番号を要求する必要があります。

**ステップ 4** (オプション) 各 ERL を緊急応答ゾーンに割り当て、発信者に一番近い PSAP に 911 コールをルーティングできるようにします。voice emergency response zone コマンドを使用します。

**ステップ 5** emergency response zone コマンドを使用して、911 発信者用に 1 つ以上のダイヤル ピアを設定します。

宛先パターンが異なる場合は、それに応じて複数のダイヤル ピアを設定する必要があります。

**ステップ 6** emergency response callback コマンドを使用して、PSAP の 911 コールバック用に 1 つ以上のダイヤル ピアを設定します。

**ステップ 7** 各 ERL に電話機を割り当てるのに使用する方法を決定します。

次のいずれかを選択します。

- 同じサブネットにある電話機のグループの場合、ERL に IP サブネットを作成して、各電話機の IP アドレスを割り当てます。ERL ごとに 1 つまたは 2 つの固有の IP サブネットを作成できます。これが最も簡単に設定できるオプションです。表 15 に例を示します。

表 15 ERL、説明、IP サブネット アドレス、および ELIN の設定例

ERL 番号	説明	IP アドレスの割り当て	ELIN
1	Building 2, 1st floor	10.5.124.xxx	408 555-0142
2	Building 2, 2nd floor	10.7.xxx.xxx	408 555-0143
3 & 4	Building 2, 3rd floor	10.8.xxx.xxx および 10.9.xxx.xxx	408 555-0144 および 408 555-0145

- ephone テンプレートおよび音声レジスタ テンプレートの設定を使用して、ERL を電話機のグループに明示的に割り当てることができます。同じ機能セットを複数の ephone または SIP 電話機に適用する場合は、電話機に ERL を個々に割り当ててのではなく、これらのテンプレートを使用して時間を節約できます。
- 電話機に ERL を個々に割り当てることができます。ご使用の電話機のタイプに応じて、3 つの方法のいずれかを使用できます。ERL を電話機の次の設定に割り当てることができます。
  - ephone 設定
  - ダイヤル ピア設定
  - 音声レジスタ プール設定

表 16 に、これらの各オプションの例を示します。

表 16 電話機ごとの明示的な ERL の割り当て

電話機の設定	ERL
Ephone 100	3
Dial-peer voice 213 pots	3
Dial-peer voice 214 voip	4
Voice register pool 1	2

**ステップ 8** (オプション) 911 発信者の IP Phone のアドレスがどのゾーンのどのロケーションの IP サブネットとも一致しない場合に PSAP に送信されるデフォルトの ELIN を定義します。

**ステップ 9** (オプション) タイムアウトの発生またはシステムの再起動によりコールバック情報が Last Caller テーブルから削除された場合に使用される指定コールバック番号を定義します。

**ステップ 10** (オプション) Last Caller テーブル内のデータの有効期限をデフォルトの 3 時間から変更します。

**ステップ 11** (オプション) RADIUS アカウンティングまたは syslog サービスが永続的に呼詳細レコードを記録できるようにします。

## 既存の Cisco Unified SRST 機能との相互作用

E911 サービスは、既存の Cisco Unified SRST 機能の一部と相互に作用します。次の各機能との相互作用については、次の個別の項で説明します。



**(注)** ご使用の Cisco Unified SRST のバージョンによっては、次の機能の一部または全部がサポートされていない場合があります。

- [ELIN の複数の用途 \( P.239 \)](#)
- [番号の変換 \( P.239 \)](#)
- [コール転送 \( P.240 \)](#)
- [自動転送 \( P.240 \)](#)
- [コール ロッキング機能 \( P.240 \)](#)
- [コール ウェイティング \( P.240 \)](#)
- [3 者間会議 \( P.240 \)](#)
- [ダイヤル ピアのロータリー \( P.240 \)](#)
- [ダイヤル プラン パターン \( P.241 \)](#)
- [発信者 ID のブロック \( P.241 \)](#)
- [共有回線 \( P.241 \)](#)

## ELIN の複数の用途



### 注意

その他の目的で ELIN を使用すると、既存の Cisco Unified SRST 機能との間に予期しない相互作用が引き起こされる可能性があるため、避けることをお勧めします。

その他の目的で ELIN を使用する例としては、ELIN を実際の電話番号 ( ephone-dn、voice register dn、または FXS destination-pattern )、コール ピックアップ番号、またはエイリアス再ルーティング番号として使用するよう設定することなどがあります。

ELIN を実際の電話番号として使用すると、その番号に発信されたときに問題が発生します。911 コールが発生し、最後の発信者の情報が Last Caller テーブルに残っている場合、外部の発信者は、実際の電話機ではなく、最後の 911 発信者に到達します。ELIN に使用されている電話番号を、実際の電話機と共有しないようにお勧めします。

ELIN と実際の電話機で同じ電話番号を使用していても、発信 911 コールには影響ありません。

## 番号の変換

E911 機能では、発信 911 コールの際に発信番号が ELIN に変換され、911 コールバックの間 ( PSAP から 911 発信者にコールバックしたとき ) に着信番号が最後の発信者の内線番号に変換されます。番号の変換に別の方法を使用すると、E911 ソフトウェアによる次のような変換と矛盾する可能性があります。

- dialplan-pattern : telephony-service モードで設定された内線番号にプレフィックス パターンを指定します。
- num-exp : 内線番号を完全な E.164 番号に拡張します。
- 着信番号と発信番号の voice-port 変換。
- ダイヤル ピアの発信番号の変換。
- ダイヤル ピアの translation-profile。
- ダイヤル ピア、音声ポート、POTS 音声サービス、トランク グループ、トランク グループのメンバー、音声ソース グループ、call-manager-fallback、および ephone-dn に対して行われた音声変換プロファイル。
- ephone-dn の変換。
- voice register dn の発信変換。

上記の変換機能を設定すると、ELIN のパターンの一部となるようなパターンを変換した場合に、E911 機能に影響が及びます。発信 911 コールの場合、それらの機能によって、E911 の ELIN が別の電話番号に変換され、ALI データベースで検索できない電話番号が PSAP に伝えられる可能性があります。911 コールバックの電話番号 (ELIN) が、E911 コールバック処理の前に変換された場合、E911 機能では最後の発信者の履歴を検索できません。

## コール転送

Cisco Unified SRST 環境の電話機で、別の ERL にある別の電話機を含む PSAP への半在席転送または打診転送が実行された場合、PSAP では誤った ELIN が使用されます。PSAP には、転送されたユーザではなく、転送したユーザの ELIN が表示されます。

911 コールバック (PSAP から 911 発信者へのコールバック) や PSAP による転送への影響はありません。

正当な理由がある場合、911 発信者は PSAP を別のユーザに転送できます。そうでなければ、911 発信者を PSAP に接続しておくことをお勧めします。

## 自動転送

IP Phone のユーザが、PSAP への自動転送が設定された別の電話機にコールを発信した場合は、何の影響もありません。

自動転送を有効にした電話機を使用している 911 発信者に PSAP からコールバックした場合、PSAP はその 911 発信者以外のユーザにリダイレクトされます。

## コール ブロッキング機能

営業時間外のコール ブロッキングなどの機能が有効な場合、システム管理者が 911 コールの例外を作成しない限り、発信 911 コールはブロックされます。

電話機にブロッキング機能 (Do Not Disturb など) が設定されている場合、911 コールバックは 911 発信者に到達しません。

## コール ウェイティング

PSAP との 911 コールが確立された後、コール ウェイティングによってコールが中断されることがあります。911 発信者には、オペレータを保留にするという選択肢もあります。保留操作は禁止されていませんが、911 発信者は、コールが終了するまで PSAP に接続したままにしておくことをお勧めします。

## 3 者間会議

911 発信者が PSAP と話すときに 3 者間会議を開始することは可能ですが、コールが終了するまで単独で PSAP に接続しておくことをお勧めします。

## ダイヤル ピアのロータリー

911 発信者がダイヤル式の電話機を使用している場合は、**emergency response zone** コマンドを使用して、コールが E911 コールとして処理されるように、それぞれのダイヤル ピアを設定する必要があります。そうしないと、E911 機能用に設定されていないダイヤル ピアで受信されたコールは通常のコールとして扱われ、ELIN の変換も行われません。

同じ宛先パターンを使用して2つのダイヤル ピアを別々の PSAP にルーティングするように設定しないでください。発信者の電話番号は2つの異なる ELIN には変換されないため、2つのダイヤル ピアは別々の PSAP にルーティングされません。ただし、異なる宛先パターン(9911 と 95105558911 など)を使用してダイヤル ピアを設定すれば、コールを別々の PSAP にルーティングできます。サービス プロバイダーが特定の着信番号を要求する場合は、電話番号の変換機能を使用するか、プレフィックス番号や転送番号を追加して、2番目のダイヤル ピア用に 95105558911 を 9911 に変更する必要があります。

**ヒント**

emergency response zone コマンドと emergency response callback コマンドの両方を使用して同じダイヤル ピアを設定しないことをお勧めします。

## ダイヤル プラン パターン

ダイヤル プラン パターンを使用すると、発信者の内線番号が完全修飾された E.164 番号に拡張されます。911 発信者の ERL が見つかった場合、拡張された番号が ELIN に変換されます。

911 コールバックの場合は、着信番号が 911 発信者の拡張された番号に変換されます。

## 発信者 ID のブロック

ephone または voice-port の設定で発信者 ID のブロック機能を設定すると、遠端ゲートウェイ デバイスで発信側情報の表示がブロックされます。PSAP で ELIN (発信側情報) を受け取る必要があるため、E911 コールが発信されるとこの機能は無効になります。

発信者 ID のブロック機能は、コールバックには影響しません。

## 共有回線

共有回線機能を使用すると、複数の電話機で同じ電話番号を共有できます。共有回線で着信コールが受信されると、それぞれの電話機で呼び出し音が鳴ります。最初にコールに回答したユーザだけが発信者に接続されます。

共有回線機能は、発信 911 コールには影響しません。

911 コールバックの場合は、その電話番号を共有するすべての電話機で呼び出し音が鳴ります。このため、911 発信者以外のユーザが電話に回答して PSAP に接続される場合があります。PSAP が 911 発信者だけと話す必要がある場合は、これが混乱の原因になる可能性があります。

## E911 サービスの設定

ここでは、次の内容について説明します。

- 緊急応答ロケーションの設定 (P.242)(必須)
- 緊急応答ゾーン内のロケーションの設定 (P.244)(オプション)
- E911 サービスの発信ダイヤル ピアの設定 (P.245)(必須)
- PSAP からのコールバック用のダイヤル ピアの設定 (P.247)(必須)
- 電話機への ERL の割り当て (P.248)(必須)
- カスタマイズ設定値の設定 (P.251)(オプション)
- 2 つの ELIN に対する address コマンドの使用 (P.253)(オプション)
- 呼詳細レコードの有効化 (P.254)(オプション)
- E911 設定の確認 (P.255)(オプション)

### 緊急応答ロケーションの設定

ERL には、0、1、または 2 つの ELIN を定義できます。ELIN が 1 つ定義されている場合、この ERL からコールを発信する電話機には、この ELIN が常に使用されます。ELIN を 2 つ定義した場合は、この ERL からコールを発信する電話機に、2 つの ELIN が交互に使用されます。ELIN を 1 つも定義しない場合、この ERL を使用する電話機からコールが発信されても、発信番号は変換されません。PSAP では、このような 911 コールの発信番号が表示されます。

複数の ERL が作成されている場合、E911 ソフトウェアでは ERL のタグ番号に従って使用する ELIN が決定されます。E911 ソフトウェアは、タグ 1 ~ 2147483647 の範囲で ERL を順番に検索します。ELIN の変換には、発信者の IP アドレスを含むサブネット マスクを持つ最初の ERL が使用されます。



(注)

voice emergency response location コマンドは、2 つの新しいオプションの ERL フィールド **name** および **address** を含むように拡張されました。**name** フィールドでは、管理目的で ERL の情報または説明を指定します。たとえば、**name Bldg 20 3rd floor** では、ERL 設定の目的を説明しています。**address** フィールドは、ERL の住所のカンマ区切りテキスト エントリです。この住所は、E911 ERL 設定の一部として保存されます。**show voice emergency addresses** コマンドとともに使用すると、住所情報をテキスト ファイルに保存できます。

### 前提条件

- P.236 の「E911 サービスの実装の計画」の説明に従って 911 設定を計画します。
- Cisco Unified SRST バージョン 4.2(1) またはバージョン 4.1 がインストールされている必要があります。
- P.230 の「前提条件」に記載されている前提条件を参照してください。

### 制約事項

Cisco Unified SRST バージョン 4.1 では、**name** フィールドおよび **address** フィールドを使用できません。



## 要約手順

1. `enable`
2. `configure terminal`
3. `voice emergency response location tag`
4. `elin [1 | 2] E.164 number`
5. `address address`
6. `name name`
7. `end`

## 詳細手順

	コマンドまたはアクション	目的
ステップ 1	<code>enable</code>  例: Router> enable	特権 EXEC モードを有効にします。  • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	<code>configure terminal</code>  例: Router# configure terminal	global コンフィギュレーション モードを開始します。
ステップ 3	<code>voice emergency response location tag</code>  例: Router(config)# voice emergency response location 4	ERL のパラメータを定義するために、emergency response location コンフィギュレーション モードを開始します。
ステップ 4	<code>elin [1   2] E.164 number</code>  例: Router(cfg-emrgncy-resp-location)# elin 1 4085550100	(オプション) 発信者の内線番号に代わる E.164 PSTN 番号である ELIN を指定します。この番号は、PSAP の端末に表示され、PSAP では ALI データベースを検索して発信者の位置を確認するのに使用されます。また、PSAP ではコールバックにも使用されます。オプションの <code>elin 2</code> コマンドを使用して、2 番目の ELIN を定義できます。ERL の ELIN が定義されていない場合、PSAP では発信番号が表示されません。
ステップ 5	<code>address address</code>  例: Router(cfg-emrgncy-resp-location)# address I,604,5550100, ,184 ,Main St,Kansas City,KS,1,	(オプション) 発信者の住所の Automatic Location Identification (ALI) データベース アップロードに使用される文字列を定義します。この文字列は、サービス プロバイダーが要求するレコード形式に従う必要があります。文字列は最大 247 文字です。
ステップ 6	<code>name name</code>  例: Router(cfg-emrgncy-resp-location)# name Bldg C, Floor 2	(オプション) 緊急応答ロケーションを識別または説明するために内部で使用される 30 文字の文字列を定義します。
ステップ 7	<code>end</code>  例: Router(cfg-emrgncy-resp-location)# end	特権 EXEC モードに戻ります。

## 緊急応答ゾーン内のロケーションの設定

緊急応答ゾーンの設定では、ロケーション タグを使用してゾーン内のロケーションのリストを作成します。ゾーン設定では、ロケーションのランキングが可能です。このランキングは、複数の PSAP が存在する場合に ERL 検索順序を制御します。システム上のすべての 911 コールが 1 つの PSAP にルーティングされる場合、`zone` コマンドは使用されません。

### 前提条件

- P.242 の「緊急応答ロケーションの設定」の説明に従って、ERL を定義します。
- Cisco Unified SRST バージョン 4.2(1) がインストールされている必要があります。

### 制約事項

Cisco Unified SRST バージョン 4.1 では、この機能を使用できません。

### 要約手順

1. `enable`
2. `configure terminal`
3. `voice emergency response zone tag`
4. `location location-tag [priority 1-100]`
5. `end`

### 詳細手順

	コマンドまたはアクション	目的
ステップ 1	<code>enable</code>  例: Router> enable	特権 EXEC モードを有効にします。  • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	<code>configure terminal</code>  例: Router# configure terminal	global コンフィギュレーション モードを開始します。
ステップ 3	<code>voice emergency response zone tag</code>  例: Router(config)# voice emergency response zone 10	緊急応答ゾーンのパラメータを定義するために、 <code>voice emergency response zone</code> コンフィギュレーション モードを開始します。範囲は 1 ~ 100 です。
ステップ 4	<code>location location-tag [priority 1-100]</code>  例: Router (cfg-emrgncy-resp-zone)# location 8 priority 2	各ロケーション タグは、 <code>voice emergency response location</code> コマンドで作成したロケーション タグに対応する必要があります。ゾーンに含めるロケーションごとに、このコマンドを繰り返します。priority(オプション)では、ゾーン リスト内のロケーションをランク付けします。最も高い優先順位は 1 です。
ステップ 5	<code>end</code>  例: Router (config)# end	特権 EXEC モードに戻ります。

## E911 サービスの発信ダイヤル ピアの設定

P.236 の「E911 サービスの実装の計画」の説明に従って 911 設定を計画したときに、緊急応答ゾーンを設定すると決定したかどうかに応じて、次のいずれかの手順を使用します。

- ゾーンを使用しないと決定した場合は、P.245 の「E911 サービスの発信ダイヤル ピアの設定」を参照してください。
- ゾーンを使用すると決定した場合は、P.246 の「緊急応答ゾーン用のダイヤル ピアの設定」を参照してください。



(注) Cisco Unified SRST バージョン 4.1 では、ゾーンを使用できません。

## 緊急コール用のダイヤル ピアの設定

PSAP への緊急コール用のダイヤル ピアを作成する手順は、次のとおりです。このダイヤル ピアの宛先パターンは、通常、911 の変形 (9911 など) になります。このダイヤル ピアでは、CAMA または PRI ネットワーク インターフェイス カードのポート番号が使用されます。新しい **emergency response zone** コマンドを使用すると、このダイヤル ピアで ELIN へのすべての発信コールの発信番号が変換されます。

### 前提条件

Cisco Unified SRST バージョン 4.2(1) またはバージョン 4.1 がインストールされている必要があります。

### 要約手順

1. **enable**
2. **configure terminal**
3. **dial-peer voice *number* pots**
4. **destination-pattern *n911***
5. **prefix *number***
6. **emergency response zone**
7. **end**

### 詳細手順

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b>  例: Router> enable	特権 EXEC モードを有効にします。  • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	<b>configure terminal</b>  例: Router# configure terminal	global コンフィギュレーション モードを開始します。
ステップ 3	<b>dial-peer voice <i>number</i> pots</b>  例: Router(config)# dial-peer voice 911 pots	個々のダイヤル ピアのパラメータを定義するために、dial-peer コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 4	<code>destination-pattern n911</code>  例: Router(config-dial-peer)# destination-pattern 9911	ダイヤルされた番号をテレフォニー デバイスと突き合わせます。このコマンドで指定する番号は、E.164 またはプライベート ダイヤリング プランの電話番号です。E911 サービスの場合、通常、番号は 911 の変形になります。
ステップ 5	<code>prefix number</code>  例: Router(config-dial-peer)# prefix 911	(オプション)ダイヤル文字列がテレフォニー インターフェイスに渡される前に、文字列の先頭に自動的に追加されるプレフィックスを指定します。E911 サービスの場合、ダイヤル文字列は 911 の変形になります。
ステップ 6	<code>emergency response zone</code>  例: Router(config-dial-peer)# emergency response zone	システムで定義されているすべての ERL を PSAP にルーティングするのに使用されるように、このダイヤル ピアを定義します。
ステップ 7	<code>end</code>  例: Router(config-dial-peer)# end	特権 EXEC モードに戻ります。

## 緊急応答ゾーン用のダイヤル ピアの設定

Cisco Unified SRST では、ダイヤル ピアに異なるゾーンを割り当てることにより、ERL に基づいて 911 コールを選択的にルーティングできます。`emergency response zone` コマンドでは、911 コールをルーティングするダイヤル ピアおよび使用する音声インターフェイスを指定します。このコマンドのゾーン タグにより、そのゾーンに定義されている ERL だけを、そのダイヤル ピアでルーティングできるようになります。同じ緊急番号をダイヤルしている発信者が、その ERL を含むゾーンに基づいて、別の音声インターフェイスにルーティングされます。

### 前提条件

- 次の説明に従って、ERL および緊急応答ゾーンを定義します。
  - [緊急応答ロケーションの設定 \(P.242\)](#)
  - [緊急応答ゾーン内のロケーションの設定 \(P.244\)](#)
- Cisco Unified SRST バージョン 4.2(1) がインストールされている必要があります。

### 制約事項

Cisco Unified SRST バージョン 4.1 では、この機能を使用できません。

### 要約手順

- enable
- configure terminal
- dial-peer voice *number* pots
- destination-pattern *n911*
- prefix *number*
- emergency response zone *tag*
- end

## 詳細手順

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b>  例: Router> enable	特権 EXEC モードを有効にします。  • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	<b>configure terminal</b>  例: Router# configure terminal	global コンフィギュレーション モードを開始します。
ステップ 3	<b>dial-peer voice <i>number</i> pots</b>  例: Router(config)# dial-peer voice 911 pots	個々のダイヤル ピアのパラメータを定義するために、dial-peer コンフィギュレーション モードを開始します。
ステップ 4	<b>destination-pattern <i>n911</i></b>  例: Router(config-dial-peer)# destination-pattern 9111	ダイヤルされた番号をテレフォニー デバイスと突き合わせます。このコマンドで指定する番号は、E.164 またはプライベート ダイヤリング プランの電話番号です。E911 サービスの場合、通常、番号は 911 の変形になります。
ステップ 5	<b>prefix <i>number</i></b>  例: Router(config-dial-peer)# prefix 911	(オプション) ダイヤル文字列がテレフォニー インターフェイスに渡される前に、文字列の先頭に自動的に追加されるプレフィックスを指定します。E911 サービスの場合、ダイヤル文字列は 911 の変形になります。
ステップ 6	<b>emergency response zone <i>tag</i></b>  例: Router(config-dial-peer)# emergency response zone 10	そのゾーンに定義されている ERL をルーティングするために使用されるように、このダイヤル ピアを定義します。  tag は、既存の設定済みゾーンを示します。範囲は 1 ~ 100 です。
ステップ 7	<b>end</b>  例: Router(config-dial-peer)# end	特権 EXEC モードに戻ります。

## PSAP からのコールバック用のダイヤル ピアの設定

PSAP からの 911 コールバック用のダイヤル ピアを作成する手順は、次のとおりです。このダイヤル ピアを使用すると、PSAP から ELIN を使用してコールバックできるようになります。このダイヤル ピアに適合するコールが到着すると、**emergency response callback** コマンドによって、ELIN を最後に使用した発信者が検索され、着信コールの宛先電話番号が最後の発信者の内線番号に変換されます。

## 要約手順

1. **enable**
2. **configure terminal**
3. **dial-peer voice *number* pots**
4. **incoming called-number *number***

5. `direct-inward-dial`
6. `emergency response callback`
7. `end`

## 詳細手順

	コマンドまたはアクション	目的
ステップ 1	<code>enable</code>  例: Router> enable	特権 EXEC モードを有効にします。  • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	<code>configure terminal</code>  例: Router# configure terminal	global コンフィギュレーション モードを開始します。
ステップ 3	<code>dial-peer voice number pots</code>  例: Router(config)# dial-peer voice 100 pots	個々のダイヤル ピアのパラメータを定義するために、 <code>dial-peer</code> コンフィギュレーション モードを開始します。
ステップ 4	<code>incoming called-number number</code>  例: Router(config-dial-peer)# incoming called-number 4085550100	(オプション) 着信番号に基づいて着信ダイヤル ピアを選択し、最後の発信者を識別します。この番号が ELIN です。
ステップ 5	<code>direct-inward-dial</code>  例: Router(config-dial-peer)# direct-inward-dial	(オプション) 着信番号に対して、ダイヤルイン (DID) 方式のコール処理を有効にします。詳細については、『 <a href="#">Cisco Voice, Video, and Fax Configuration Guide</a> 』を参照してください。
ステップ 6	<code>emergency response callback</code>  例: Router(config-dial-peer)# emergency response callback	ダイヤル ピアを ELIN のダイヤル ピアとして識別します。
ステップ 7	<code>end</code>  例: Router(config-dial-peer)# end	特権 EXEC モードに戻ります。

## 電話機への ERL の割り当て

Cisco Unified SRST のバージョン 4.2(1) でもバージョン 4.1 でも、同じ手順で ERL を電話機に割り当てることができます。所有する電話機のタイプに応じて、次のどの方法を使用するかが決まります。P.236 の「E911 サービスの実装の計画」のステップ 7 を参照してください。次のいずれかの手順を使用します。

- ERL を IP サブネットに割り当てるには、P.249 の「電話機の IP サブネットへの ERL の割り当て」を参照してください。
- ERL を電話機の `ephone` に割り当てるには、P.250 の「電話機の `ephone` への ERL の割り当て」を参照してください。
- ERL を電話機のダイヤル ピアに割り当てるには、P.250 の「ダイヤル ピアへの ERL の割り当て」を参照してください。

## 前提条件

- P.242 の「緊急応答ロケーションの設定」の説明に従って、ERL および緊急応答ゾーンを定義します。
- Cisco Unified SRST バージョン 4.2(1) またはバージョン 4.1 がインストールされている必要があります。

## 電話機の IP サブネットへの ERL の割り当て

通常、この手順は、電話機のグループが同じサブネットにある場合に使用します。1 つの ERL を 1 つまたは 2 つの固有の IP サブネットに関連付けることができます。したがって、この ERL で定義された ELIN が、特定のサブネットに含まれるすべての IP Phone で使用されるように、E911 ソフトウェアを設定できます。

## 要約手順

1. `enable`
2. `configure terminal`
3. `voice emergency response location tag`
4. `subnet [1 | 2] IPaddress mask`
5. `end`

## 詳細手順

	コマンドまたはアクション	目的
ステップ 1	<code>enable</code>  例: Router> enable	特権 EXEC モードを有効にします。  • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	<code>configure terminal</code>  例: Router# configure terminal	global コンフィギュレーション モードを開始します。
ステップ 3	<code>voice emergency response location tag</code>  例: Router(config)# voice emergency response location 4	ERL のパラメータを定義するために、emergency response location コンフィギュレーション モードを開始します。
ステップ 4	<code>subnet [1   2] IPaddress mask</code>  例: Router(cfg-emrgncy-resp-location)# subnet 1 192.168.0.0 255.255.0.0	このロケーションに含まれる IP Phone のグループを定義します。最大 2 個の異なるサブネットを指定できます。  すべての IP Phone を 1 つの ERL に含めるには、 <code>subnet 1 0.0.0.0 0.0.0.0</code> コマンドを使用して、デフォルトのサブネットを設定します。このサブネットは、IP Phone 以外のエンドポイント (VoIP トランクや FXS/FXO トランクの電話機など) には適用されません。
ステップ 5	<code>end</code>  例: Router(cfg-emrgncy-resp-location)# end	特権 EXEC モードに戻ります。

## 電話機の ephone への ERL の割り当て

ERL を IP サブネットに関連付けるのではなく、ERL を電話機の ephone に割り当てる場合は、次の手順を実行します。詳細については、P.236 の「E911 サービスの実装の計画」のステップ 7 を参照してください。



(注) この ERL 割り当て方法は、Cisco Unified SRST だけで使用でき、Cisco Unified SIP SRST では使用できません。

### 要約手順

1. `enable`
2. `configure terminal`
3. `ephone tag`
4. `emergency response location tag`
5. `end`

### 詳細手順

	コマンドまたはアクション	目的
ステップ 1	<code>enable</code>  例: Router> enable	特権 EXEC モードを有効にします。  • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	<code>configure terminal</code>  例: Router# configure terminal	global コンフィギュレーション モードを開始します。
ステップ 3	<code>ephone tag</code>  例: Router(config)# ephone 224	個々の ephone のパラメータを定義するために、ephone コンフィギュレーション モードを開始します。
ステップ 4	<code>emergency response location tag</code>  例: Router(config-ephone)# emergency response location 12	ERL のタグを使用して、電話機の ephone 設定に ERL を割り当てます。タグは 1 ~ 2147483647 の範囲の整数です。ERL のタグが設定済みのタグではない場合、電話機は ERL に関連付けられず、包括的な ERL のサブネットの検索に電話機の IP アドレスがデフォルトで使用されます。
ステップ 5	<code>end</code>  例: Router(config-ephone)# end	特権 EXEC モードに戻ります。

## ダイヤル ピアへの ERL の割り当て

FXS/FXO または VoIP のダイヤル ピアに ERL を割り当てる手順は、次のとおりです。これらのインターフェイスには IP アドレスが関連付けられていないので、ERL を IP サブネットに関連付けるように設定する代わりに、次の手順を使用する必要があります。詳細については、P.236 の「E911 サービスの実装の計画」のステップ 7 を参照してください。



## 要約手順

1. `enable`
2. `configure terminal`
3. `dial-peer voice tag type`
4. `emergency response location tag`
5. `end`

## 詳細手順

	コマンドまたはアクション	目的
ステップ 1	<code>enable</code>  例: Router> enable	特権 EXEC モードを有効にします。  • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	<code>configure terminal</code>  例: Router# configure terminal	global コンフィギュレーション モードを開始します。
ステップ 3	<code>dial-peer voice tag type</code>  例: Router(config)# dial-peer voice 100 pots	個々のダイヤル ピアのパラメータを定義するために、dial-peer コンフィギュレーション モードを開始します。
ステップ 4	<code>emergency response location tag</code>  例: Router(config-dial-peer)# emergency response location 12	ERL のタグを使用して、電話機のダイヤル ピア設定に ERL を割り当てます。タグは 1 ~ 2147483647 の範囲の整数です。ERL のタグが設定済みのタグではない場合、変換は行われず、E911 の情報は Last Caller テーブルに保存されません。
ステップ 5	<code>end</code>  例: Router(config-dial-peer)# end	特権 EXEC モードに戻ります。

## カスタマイズ設定値の設定

カスタマイズできる E911 設定は、次のとおりです。

- **Elin** : デフォルトの ELIN。911 発信者の IP Phone アドレスがどのゾーンのどのロケーションのサブネットとも一致しない場合は、デフォルトの ELIN を使用して元の Automatic Number Identification (ANI; 自動番号識別) が置き換えられます。デフォルトの ELIN は、いずれかの ERL にすでに定義されているものでも、固有のものでもかまいません。デフォルトの ELIN が定義されておらず、911 発信者の IP アドレスが一致しない場合、PSAP はコールバックするために ANI を参照します。デフォルトの ELIN を要求する syslog メッセージが送信され、PSAP は発信者のロケーション情報を入手できません。
- **Expiry** : 911 オペレータからのコールバックに備えて 911 コールが ELIN に関連付けられている時間 (分単位)。コールバックの有効期限は、デフォルトでは 3 時間ですが、2 分 ~ 48 時間の範囲で任意の時間に変更することができます。911 コールが PSAP に送信された時点でタイマーが起動します。この有効期限内に、PSAP は ELIN にコールバックし、最後の発信者に到達できます。
- **Callback** : 911 コールバックの際に Last Caller テーブルから最後の 911 発信者を見つけることができない場合に連絡するデフォルトの電話番号。このような状況が発生するのは、ルータのレポート後または有効期限の経過後にコールバックが実行された場合です。

- **Logging** : 緊急コールが発信されるたびに syslog 情報メッセージがコンソールに出力されます。このようなメッセージは、サードパーティのアプリケーションが社内の緊急管理者に電子メール送信またはページングを行うために必要です。これはデフォルトの機能で、**no logging** コマンドを使用して無効にできます。次に、syslog 通知メッセージの例を示します。

```
%E911-5-EMERGENCY_CALL_PLACED: calling #[4085550100] called
#[911] ELIN [4085550199]
```

## 前提条件

Cisco Unified SRST バージョン 4.2(1) がインストールされている必要があります。

## 制約事項

Cisco Unified SRST バージョン 4.1 では、この機能を使用できません。

## 要約手順

1. **enable**
2. **configure terminal**
3. **voice emergency response settings**
4. **expiry time**
5. **callback number**
6. **logging**
7. **elin number**
8. **end**

## 詳細手順

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b>  例: Router> enable	特権 EXEC モードを有効にします。  • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	<b>configure terminal</b>  例: Router# configure terminal	global コンフィギュレーション モードを開始します。
ステップ 3	<b>voice emergency response settings</b>  例: Router(config)# voice emergency response settings	E911 コールのカスタマイズ可能な設定を定義するために、voice emergency response settings モードを開始します。
ステップ 4	<b>expiry time</b>  例: Router(cfg-emrgncy-resp-settings)# expiry 300	(オプション) 各 ELIN の緊急コールの発信者の履歴情報が Last Caller テーブルに格納される期間 (分単位) を定義します。この期間は、2 ~ 2880 分の範囲の整数です。デフォルト値は 180 分です。

	コマンドまたはアクション	目的
ステップ 5	<b>callback</b> <i>number</i>  <b>例:</b> Router(cfg-emrgncy-resp-settings)# callback 7500	(オプション) 911 コールバックの際に ELIN に関連付けられている最後の発信者を見つけることができない場合の E.164 コールバック番号 (たとえば、会社のオペレータやメイン ヘルプ デスク) を定義します。
ステップ 6	<b>logging</b>  <b>例:</b> Router(cfg-emrgncy-resp-settings)# no logging	(オプション) すべての緊急コールを通知する syslog メッセージを有効にします。syslog メッセージを追跡して、社内のサポート番号にポケットベルまたは電子メールの通知を送信できます。デフォルトでは、ロギングが有効になっています。ロギングを無効にするには、このコマンドの <b>no</b> 形式を使用します。
ステップ 7	<b>elin</b> <i>number</i>  <b>例:</b> Router(cfg-emrgncy-resp-settings)# elin 4085550100	どの ERL にも、現在の 911 発信者の IP Phone アドレスに一致するサブネット マスクがない場合にデフォルトの ELIN として使用する E.164 番号を指定します。
ステップ 8	<b>end</b>  <b>例:</b> Router (cfg-emrgncy-resp-settings)# end	特権 EXEC モードに戻ります。

## 2 つの ELIN に対する address コマンドの使用



(注) Cisco Unified SRST バージョン 4.1 では、この機能を使用できません。

2 つの ELIN が定義されている ERL の場合、1 つの **address** フィールドだけを使用して、ALI データベース内の各 ELIN の 2 つの住所エントリを指定することができません。特定の電話番号を入力するのではなく、キーフレーズを入力して各 ELIN を表します。**show voice emergency address** コマンドでは、キーフレーズを ELIN 情報に置き換える出力が生成され、2 つの住所行が表示されます。

式を定義するには、キーワード *elin* (文脈に依存しない) を使用し、それに続けてピリオド、使用する ELIN の開始位置、およびもう 1 つのピリオドを入力して、最後に ELIN の終了位置を入力します。次の例を参考にしてください。

```
address I,ELIN.1.3,ELIN.4.7,678 ,Alder Drive ,Milpitas ,CA,95035
```

この例では、I に続く **address** の 2 番目のパラメータは各 ELIN の番号 1-3 です。3 番目のパラメータは各 ELIN の番号 4-7 です。**show voice emergency address** コマンドを入力すると、出力ではキーフレーズが置き換えられ、次のように表示されます。

```
I,408,5550101,678,Alder Drive ,Milpitas ,CA,95035
I,408,5550190,678,Alder Drive ,Milpitas ,CA,95035
```

## 呼詳細レコードの有効化



(注) Cisco Unified SRST バージョン 4.1 では、この機能を使用できません。

内部ポリシーまたは外部規則に従うために、次の情報を含む 911 コール履歴データを保存することが必要になる場合があります。

- 発信者の内線番号
- ELIN 情報
- ERL 情報（整数タグおよびテキスト名）
- 発信者の電話機の IP アドレス

これらのアトリビュートは、RADIUS アカウンティング サーバおよび syslog サーバの出力から、または `show call history voice` コマンドを使用して表示できます。



(注) RADIUS サーバまたは syslog サーバがこれらの詳細を表示できるようにする必要があります。RADIUS サーバまたは syslog サーバのマニュアルを参照してください。

## RADIUS アカウンティング サーバからの出力

RADIUS アカウンティングの場合、緊急コール情報は `feature-vsa` レコードの中にあります。各フィールドは、次のとおりです。

- EMR：緊急コール
- CGN：発信番号
- ELIN：緊急回線識別番号（変換された番号）
- CDN：着信番号
- ERL：緊急応答ロケーションのタグ番号
- ERLN：緊急応答ロケーションの名前（ERI が存在する場合は、ERI に対して入力された名前）
- CIP：発信者の IP アドレス（暗黙的な ERL 割り当ての場合はゼロ以外）
- ETAG：ERL タグ（明示的な ERL 割り当ての場合はゼロ以外）

次に、RADIUS サーバからの出力例を示します。

```
*Jul 18 15:37:43.691: RADIUS: Cisco AVpair [1] 202 "feature-vsa=fn:EMR
,ft:07/18/2007 15:37:32.227,frs:0,fid:6,fcid:A2444CAF347B11DC8822F63A1B4078DE,
legID:57EC,cgn:6045550101,elin:6045550199,cdn:911,erl:2,erln:Fisco,cip:1.5.6.200,etag:0"
```

## syslog サーバからの出力

ゲートウェイ アカウンティングが syslog サーバに誘導された場合、`VOIP_FEAT_HISTORY` システム メッセージが表示されます。`feature-vsa` のパラメータは、RADIUS アカウンティングで説明したものと同じです。

次に、syslog サーバの出力例を示します。

```
*Jul 18 15:37:43.675: %VOIPAAA-5-VOIP_FEAT_HISTORY: FEAT_VSA=fn:EMR,ft:07/18/2007
15:37:32.227,frs:0,fid:6,fcid:A2444CAF347B11DC8822F63A1B4078DE,legID:57EC,cgn:6045550199,
elin:6045550100,cdn:911,erl:2,erln:ABCDEFGHIJKLMNQPQRSTUVWXYZ123,cip:1.5.6.200,etag:0,
bguid:A23F6AD7347B11DC881DF63A1B4078DE
```

## show call history voice コマンドからの出力

`show call active voice` および `show call history voice` を使用して、ゲートウェイで緊急コール情報を表示します。一部の緊急コール情報は、既存のフィールドにすでに含まれています。発信者の番号は、*OriginalCallingNumber* の下にあります。ELIN は *TranslatedCallingNumber* にあります。4 つの新しいフィールドは、ERL、ERL 名、発信側の電話機の IP アドレス、および明示的な ERL 割り当てです。これらのフィールドは、ELIN 変換が行われた場合にだけ表示されます。たとえば、ELIN が定義されていない ERL からの 911 コールの場合、`show call` コマンドで 4 つの緊急フィールドは出力されません。どの ERL も発信側の電話機に一致せず、デフォルトの ELIN が使用された場合、ERL フィールドには *No Match* と表示されます。

次に、`show call history voice` コマンドを使用した場合の出力例を示します。

```
EmergencyResponseLocation=3 (Cisco Systems 3)
ERLAssignment=3
DeviceIPAddress=1.5.6.202
```

## E911 設定の確認

### バージョン 4.2(1) のみ

E911 の設定または用途を表示するための新しい `show` コマンドが導入されました。

- 各 ERL の IP アドレス、サブネット マスク、および ELIN を表示するには、`show voice emergency` コマンドを使用します。

```
Router# show voice emergency
```

```
EMERGENCY RESPONSE LOCATIONS
```

ERL	ELIN 1	ELIN2	SUBNET 1	SUBNET 2
1	6045550101		10.0.0.0	255.0.0.0
2	6045550102	6045550106	192.168.0.0	255.255.0.0
3		6045550107	172.16.0.0	255.255.0.0
4	6045550103		192.168.0.0	255.255.0.0
5	6045550105		209.165.200.224	255.0.0.0
6 6045550198		6045550109	209.165.201.0	255.255.255.224

- 各 ERL の住所情報を表示するには、`show voice emergency addresses` コマンドを使用します。

```
Router# show voice emergency addresses
```

```
3850 Zanker Rd, San Jose,604,5550101
225 W Tasman Dr, San Jose,604,5550102
275 W Tasman Dr, San Jose,604,5550103
518 Bellew Dr,Milpitas,604,5550104
400 Tasman Dr,San Jose,604,5550105
3675 Cisco Way,San Jose,604,5550106
```

- すべての ERL 情報を表示するには、**show voice emergency all** コマンドを使用します。

```
Router# show voice emergency all

VOICE EMERGENCY RESPONSE SETTINGS
  Callback Number: 6045550103
  Emergency Line ID Number: 6045550155
  Expiry: 2 minutes
  Logging Enabled

EMERGENCY RESPONSE LOCATION 1
  Name: Cisco Systems 1
  Address: 3850 Zanker Rd, San Jose,elin.1.3,elin.4.10
  IP Address 1: 209.165.200.226 IP mask 1: 255.255.255.254
  IP Address 2: 209.165.202.129 IP mask 2: 255.255.0.0
  Emergency Line ID 1: 6045550180
  Emergency Line ID 2:
  Last Caller: 6045550188 [Jan 30 2007 16:05.52 PM]
  Next ELIN For Emergency Call: 6045550166

EMERGENCY RESPONSE LOCATION 3
  Name: Cisco Systems 3
  Address: 225 W Tasman Dr, San Jose,elin.1.3,elin.4.10
  IP Address 1: 209.165.202.133 IP mask 1: 255.255.0.0
  IP Address 2: 209.165.202.130 IP mask 2: 255.0.0.0
  Emergency Line ID 1:
  Emergency Line ID 2: 6045550150
  Last Caller:
  Next ELIN For Emergency Call: 6045550151
```

- 各ゾーンのロケーションを優先順位順に示したリストを表示するには、**show voice emergency zone** コマンドを使用します。

```
Router# show voice emergency zone

EMERGENCY RESPONSE ZONES
  zone 90
    location 4
    location 5
    location 6
    location 7
    location 2147483647
  zone 100
    location 1 priority 1
    location 2 priority 2
    location 3 priority 3
```

## バージョン 4.1 およびバージョン 4.2(1)

発信 911 コールで行われた変換を確認するには、**show voice emergency callers** コマンドを使用します。このコマンドを実行すると、911 コールごとに発信番号、使用された ELIN、および時間が表示されます。この履歴は、コールの発信後 3 時間のみ有効です。有効期限を過ぎたコールは、この出力に表示されません。

```
router# show voice emergency callers
EMERGENCY CALLS CALL BACK TABLE
ELIN                               | CALLER                               | TIME
6045550100                         | 6045550150                           | Oct 12 2006 03:59:43
6045550110                         | 8155550124                           | Oct 12 2006 04:05:21
```

## E911 サービスのトラブルシューティング

**ステップ 1** `debug voice application error` コマンドおよび `debug voice application callsetup` コマンドを使用します。これらは既存のコマンドで、デフォルト セッションまたは TCL アプリケーションを使用して発信されたコールに対応します。

この例は、コールが 911 に発信されたときのデバッグ出力例を示しています。

```
router# debug voice application error
router# debug voice application callsetup

Nov 10 23:49:05.855: //emrgncy_resp_xlate_callingNum: InDialPeer[20001],
OutDialPeer[911] callingNum[6046692003]
Nov 10 23:49:05.855: //ER_HistTbl_Find_CallHistory: 6046699100
Nov 10 23:49:05.855: //59//Dest:/DestProcessEmergencyCall: Emergency Call detected:
Using ELIN 6046699100
```

この例は、PSAP から緊急コールの発信者にコールバックしたときのデバッグ出力例を示していません。

```
router# debug voice application error
router# debug voice application callsetup

Nov 10 23:49:37.279: //emrgncy_resp_xlate_calledNum: calledNum[6046699100],
dpeerTag[6046699]
Nov 10 23:49:37.279: //ER_HistTbl_Find_CallHistory: 6046699100
Nov 10 23:49:37.279: //HasERHistoryExpired: elapsedTime[10 minutes]
Nov 10 23:49:37.279: //67//Dest:/DestProcessEmergencyCallback: Emergency Response
Callback: Forward to 6046692003.
Nov 10 23:49:37.279: //67//Dest:/DestCaptureCallForward: forwarded to 6046692003
reason 1
```

## エラー メッセージ

E911 機能には、新しいシステム エラー メッセージが導入されています。次のエラー メッセージは、911 コールバックが最後の 911 発信者にルーティングされない場合に表示されます。保存された履歴が、リポート、エントリの有効期限切れ、またはソフトウェア エラーによって消失したことが原因です。

```
%E911_NO_CALLER: Unable to contact last 911 caller.
```

## E911 サービスの設定例

### バージョン 4.2(1) のみ

この例では、緊急応答が次のように設定されています。

- ELIN の一致が見つからない場合のデフォルト ELIN : 604 555-0120
- Last Caller テーブルの情報の有効期限 : 180 分
- PSAP オペレータが 911 発信者にコールバックする必要があり、コールバック履歴の有効期限が切れていた場合のコールバック番号 : 604 555-0199

ゾーン 1 には 1、2、3、4 という 4 つのロケーション含まれ、各ロケーションの名前、住所、および ELIN が定義されています。4 つのロケーションにはそれぞれ、優先順位が割り当てられています。この例では、ロケーション 4 に最も高い優先順位が割り当てられているので、911 発信者の電話機に割り当てられている ELIN を識別するために IP サブネットの一致を検索する場合、ロケーション 4 が最初に検索されます。911 コールを PSAP にルーティングするようにダイヤル ピアが設定されています (音声ポート 1/0/0)。コールバック ダイヤル ピアも設定されています。

```
voice emergency response settings
elin 6045550120
expiry 180
callback 6045550199

voice emergency response location 1
name Bldg C, Floor 1
address I,604,5550135, ,184 ,Main St,Kansas City,KS,1,
elin 1 6045550125
subnet 1 172.16.0.0 255.255.0.0
!
voice emergency response location 2
name Bldg C, Floor 2
address I,elin.1.3,elin.4.7, ,184 ,Main St,Kansas City,KS,2,
elin 1 6045550126
elin 2 6045550127
subnet 1 192.168.0.0 255.255.0.0
!
voice emergency response location 3
name Bldg C, Floor 3
address I,604,5550138, ,184 ,Main St,Kansas City,KS,3,
elin 2 6045550128
subnet 1 209.165.200.225 255.255.0.0
subnet 2 209.165.200.240 255.255.0.0
!
voice emergency response location 4
name Bldg D
address I,604,5550139, ,192 ,Main St,Kansas City,KS,
elin 1 6045550129
subnet 1 209.165.200.231 255.255.0.0
!
voice emergency response zone 1
location 4 priority 1
location 3 priority 2
location 2 priority 3
location 1 priority 4
!
dial-peer voice 911 pots
description Public Safety Answering Point
emergency response zone 1
destination-pattern 911
port 1/0/0
!
dial-peer voice 6045550 voip
emergency response callback
destination-pattern 6045550...
```



```
session target loopback:rtp
codec g711ulaw
!
dial-peer voice 1222 pots
emergency response location 4
destination-pattern 6045550130
port 1/0/1
!
dial-peer voice 5550144 voip
emergency response callback
session target ipv4:1.5.6.10
incoming called-number 604555....
codec g711ulaw
!
```

## バージョン 4.1 およびバージョン 4.2(1)

この例では、E911 サービスが次の対象に ERL を割り当てるように設定されています。

- IP サブネット 10.20.20.0
- 2 つのダイヤル ピア
- 1 台の SIP 電話機

Router#**show running-config**

```
Building configuration...

Current configuration : 6241 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
!
hostname rm-uut3-2821
!
boot-start-marker
boot-end-marker
!
no aaa new-model
network-clock-participate wic 1
network-clock-participate wic 2
no network-clock-participate wic 3
!
!
ip cef
no ip dhcp use vrf connected
!
ip dhcp pool sccp-7912-phone1
 host 10.20.20.122 255.255.0.0
 client-identifier 0100.1200.3482.cd
 default-router 10.20.20.3
 option 150 ip 10.21.20.218
!
ip dhcp pool sccp-7960-phone2
 host 10.20.20.123 255.255.0.0
 client-identifier 0100.131a.a67d.cf
 default-router 10.20.20.3
 option 150 ip 10.21.20.218
 dns-server 10.20.20.3
!
ip dhcp pool sip-phone1
 host 10.20.20.121 255.255.0.0
 client-identifier 0100.15f9.b38b.a6
 default-router 10.20.20.3
 option 150 ip 10.21.20.218
```

```

!
ip dhcp pool sccp-7960-phone1
  host 10.20.20.124 255.255.0.0
  client-identifier 0100.14f2.37e0.00
  default-router 10.20.20.3
  option 150 ip 10.21.20.218
  dns-server 10.20.20.3
!
!
no ip domain lookup
ip host rm-ut3-c2821 10.20.20.3
ip host RescuMe01 10.21.20.218
multilink bundle-name authenticated
!
isdn switch-type basic-net3
!
!
voice service voip
  allow-connections h323 to h323
  allow-connections h323 to sip
  allow-connections sip to h323
  allow-connections sip to sip
  supplementary-service h450.12
  sip
    registrar server
!
!
voice register global
  system message RM-SIP-SRST
  max-dn 192
  max-pool 48
!
voice register dn 1
  number 32101
!
voice register dn 185
  number 38301
!
voice register dn 190
  number 38201
!
voice register dn 191
  number 38202
!
voice register dn 192
  number 38204
!
voice register pool 1
  id mac DCC0.2222.0001
  number 1 dn 1
  emergency response location 2100
!
voice register pool 45
  id mac 0015.F9B3.8BA6
  number 1 dn 185
!
voice emergency response location 1
  elin 1 22222
  subnet 1 10.20.20.0 255.255.255.0
!
voice emergency response location 2
  elin 1 21111
  elin 2 21112
!
!
voice-card 0
  no dspfarm
!
!

```

```
archive
  log config
  hidekeys
!
!
controller T1 0/1/0
  framing esf
  linecode b8zs
  pri-group timeslots 8,24
!
controller T1 0/1/1
  framing esf
  linecode b8zs
  pri-group timeslots 2,24
!
controller T1 0/2/0
  framing esf
  clock source internal
  linecode b8zs
  ds0-group 1 timeslots 2 type e&m-immediate-start !
controller T1 0/2/1
  framing esf
  linecode b8zs
  pri-group timeslots 2,24
!
!
translation-rule 5
  Rule 0 ^37103 1
!
!
translation-rule 6
  Rule 6 ^2 911
!
!
interface GigabitEthernet0/0
  ip address 31.20.0.3 255.255.0.0
  duplex auto
  speed auto
!
interface GigabitEthernet0/1
  ip address 10.20.20.3 255.255.0.0
  duplex auto
  speed auto
!
interface Serial0/1/0:23
  no ip address
  encapsulation hdlc
  isdn switch-type primary-5ess
  isdn incoming-voice voice
  no cdp enable
!
interface Serial0/1/1:23
  no ip address
  encapsulation hdlc
  isdn switch-type primary-net5
  isdn incoming-voice voice
  no cdp enable
!
interface Serial0/2/1:23
  no ip address
  encapsulation hdlc
  isdn switch-type primary-net5
  isdn incoming-voice voice
  no cdp enable
!
interface BRI0/3/0
  no ip address
  isdn switch-type basic-5ess
  isdn twait-disable
```

```

    isdn point-to-point-setup
    isdn autodetect
    isdn incoming-voice voice
    no keepalive
!
interface BRI0/3/1
    no ip address
    isdn switch-type basic-5ess
    isdn point-to-point-setup
!
!
ip http server
!
!
voice-port 0/0/0
!
voice-port 0/0/1
!
voice-port 0/1/0:23
!
voice-port 0/2/0:1
!
voice-port 0/1/1:23
!
voice-port 0/2/1:23
!
voice-port 0/3/0
!
voice-port 0/3/1
!
!
dial-peer voice 2002 pots
    shutdown
    destination-pattern 2....
    port 0/2/0:1
    forward-digits all
!
dial-peer voice 2005 pots
    description for-cme2-408-pri
    emergency response location 2000
    shutdown
    incoming called-number 911
    direct-inward-dial
    port 0/2/1:23
    forward-digits all
!
dial-peer voice 2004 voip
    description for-cme2-408-thru-ip
    emergency response location 2000
    shutdown
    session target loopback:rtp
    incoming called-number 911
!
dial-peer voice 1052 pots
    description 911callbackto-cme2-3
    shutdown
    incoming called-number .....
    direct-inward-dial
    port 0/1/1:23
    forward-digits all
!
dial-peer voice 1013 pots
    description for-analog
    destination-pattern 39101
    port 0/0/0
    forward-digits all
!
dial-peer voice 1014 pots
    description for-analog-2

```

```
destination-pattern 39201
port 0/0/1
forward-digits all
!
dial-peer voice 3111 pots
emergency response Zone
destination-pattern 9....
port 0/1/0:23
forward-digits all
!
dial-peer voice 3121 pots
emergency response callback
incoming called-number 2....
direct-inward-dial
port 0/1/0:23
forward-digits all
!
!
call-manager-fallback
max-conferences 8 gain -6
transfer-system full-consult
ip source-address 10.20.20.3 port 2000
max-ephones 3
max-dn 3 dual-line preference 1
system message primary SRST-UUT3-2851
keepalive 45
!
!
line con 0
exec-timeout 0 0
line aux 0
line vty 0 4
login
!
scheduler allocate 20000 1000
!
end

rm-uut3-2821#$
```

## E911 サービスの機能情報

表 17 は、各バージョンにおける E911 サービスの機能拡張を示しています。

特定の Cisco Unified SRST バージョンをサポートする正確な Cisco IOS リリースを確認するには、『Cisco Unified Communications Manager Compatibility Matrix』を参照してください。このドキュメントは、次の URL から入手可能です。

[http://www.cisco.com/en/US/docs/voice\\_ip\\_comm/cucm/docguide/6\\_1\\_2/dg612.html#wp1028473](http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/docguide/6_1_2/dg612.html#wp1028473)

プラットフォームおよびソフトウェア イメージのサポートに関する情報を参照するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator では、特定のソフトウェア リリース、機能セット、またはプラットフォームをサポートしている Cisco IOS ソフトウェアを確認できます。Cisco Feature Navigator にアクセスするには、<http://www.cisco.com/go/cfn> に移動してください。Cisco.com のアカウントは必要ありません。



(注) 表 17 は、所定の機能に対するサポートが導入された Cisco Unified SRST のバージョンを示しています。特に断りのない限り、その機能は以降のバージョンの Cisco Unified SRST ソフトウェアでもサポートされます。

表 17 E911 サービスの機能情報

機能名	リリース	機能情報
E911 サービスのアップデート	4.2(1)	<ul style="list-style-type: none"> <li>ゾーンへの ERL の割り当て</li> <li>デフォルト ELIN の定義、指定コールバック番号の追加、Last Caller テーブル内のデータの有効期限の変更、緊急コールを通知する syslog メッセージの有効化</li> <li>911 発信者データへの名前および住所の追加</li> <li>新しい呼詳細レコードの追加</li> <li>トラブルシューティングのための新しいコマンドの追加</li> </ul>
E911 サービス	4.1	E911 サービスが導入されました。

## 関連情報

Cisco Unified SRST の監視および保守については、P.227 の「Cisco Unified SRST の監視と保守」に進んでください。

追加情報については、P.25 の「Cisco Unified SRST の概要」の P.40 の「その他の資料」を参照してください。



# 付録 A : SIP 用の Cisco Unified SRST サポートの準備

---

Revised: July 11, 2008

Cisco Unified Survivable Remote Site Telephony (SRST) は、Cisco Unified IP Phone とルータ音声ゲートウェイ音声ポートの間における Session Initiation Protocol (SIP) を使用した着信コールおよび発信コールをサポートしています。しかし、Cisco Unified SRST への SIP 電話機の直接取り付けはサポートしていません。SIP は、Cisco Unified SRST ルータが PSTN ゲートウェイから離れていて、SRST ゲートウェイと PSTN ゲートウェイが (H.323 ではなく) SIP によってリンクされている状況で使用することができます。

この付録では、SIP コールをサポートするための特別な設定について説明します。SIP の詳細については、『[Cisco IOS SIP Configuration Guide](#)』を参照してください。

## 内容

- [SIP アプリケーション用 DTMF リレーとボイスメール \(P.266\)](#)
- [関連情報 \(P.270\)](#)

## SIP アプリケーション用 DTMF リレーとボイスメール

SIP アプリケーション用 DTMF リレーは、次の 2 つのボイスメール環境で使用できます。

- SIP RFC 2833 を使用した DTMF リレー (P.266)
- SIP Notify (非標準) を使用した DTMF リレー (P.267)

### SIP RFC 2833 を使用した DTMF リレー

Cisco Unified Skinny Client Control Protocol (SCCP) を使用している電話機 (Cisco Unified SRST システムの電話機など) は、アウトオブバンド DTMF デジット表示のみをサポートします。リモートにある SIP ベースの IVR アプリケーションおよびボイスメール アプリケーションに SCCP 電話機からデジット情報を送信できるようにするには、Cisco SRST 3.2 以降のバージョンの機能を使用して、アウトオブバンド SCCP デジット表示を DTMF リレー用 SIP 標準 (RFC 2833) に変換します。この方式を選択するには、SIP VoIP ダイアルピアで `dtmf-relay rtp-nte` コマンドを使用します。

SIP DTMF リレー方式は、次の場合に必要です。

- リモートにある SIP ベースの IVR アプリケーションまたはボイスメール アプリケーション (Cisco Unity など) と Cisco Unified SRST システムとの接続に SIP が使用されている場合
- リモートにある SIP-PSTN 音声ゲートウェイ (PSTN を経由してボイスメール アプリケーションまたは IVR アプリケーションまで) と Cisco Unified SRST システムとの接続に SIP が使用されている場合



(注) アウトオブバンド DTMF リレーの変換を行う必要があるのは、SCCP 電話機だけです。SIP 電話機は、RFC 2833 で指定されているアウトオブバンド DTMF リレーを初めからサポートしています。

RFC 2833 を使用した SIP DTMF リレーを有効にするには、この項で説明するコマンドを発側ゲートウェイと着側ゲートウェイの両方で使用する必要があります。

#### 要約手順

1. `dial-peer voice tag voip`
2. `dtmf-relay rtp-nte`
3. `exit`
4. `sip-ua`
5. `notify telephone-event max-duration time`
6. `exit`

#### 詳細手順

	コマンドまたはアクション	目的
ステップ 1	<code>dial-peer voice tag voip</code>  例: Router(config)# dial-peer voice 2 voip	dial-peer コンフィギュレーション モードを開始します。
ステップ 2	<code>dtmf-relay rtp-nte</code>  例: Router(config-dial-peer)# dtmf-relay rtp-nte	Real-Time Transport Protocol (RTP) を使用して、Named Telephone Event (NTE) ペイロード タイプで DTMF トーンを転送します。



	コマンドまたはアクション	目的
ステップ 3	<b>exit</b>  例: Router(config-dial-peer)# exit	dial-peer コンフィギュレーション モードを終了します。
ステップ 4	<b>sip-ua</b>  例: Router(config)# sip-ua	SIP user-agent コンフィギュレーション モードを開始します。
ステップ 5	<b>notify telephone-event max-duration time</b>  例: Router(config-sip-ua)# notify telephone-event max-duration 2000	単一の DTMF イベントに関する NOTIFY メッセージを 2 つ連続して送信するときの、時間間隔の最大値を設定します。  <ul style="list-style-type: none"> <li>• <b>max-duration time</b> : 単一の DTMF イベントに関する NOTIFY メッセージを連続して送信するときの時間間隔 (ミリ秒)。範囲は 500 ~ 3000 です。デフォルトは 2000 です。</li> </ul>
ステップ 6	<b>exit</b>  例: Router(config-sip-ua)# exit	SIP user-agent コンフィギュレーション モードを終了します。

## トラブルシューティングに関するヒント

DTMF リレーを設定すると、**show running-config** コマンド出力の dial-peer セクションに、DTMF リレー ステータスが表示されます。この抜粋を次に示します。

```
dial-peer voice 123 voip
 destination-pattern [12]...
 monitor probe icmp-ping
 session protocol sipv2
 session target ipv4:10.8.17.42
 dtmf-relay rtp-nte
```

## SIP Notify (非標準) を使用した DTMF リレー

Cisco Unity Express システムに接続している SIP ネットワーク上のボイスメールを使用するには、非標準の SIP Notify 形式を使用します。Notify 形式を設定するには、**dtmf-relay** コマンドで **sip-notify** キーワードを使用します。**sip-notify** キーワードの使用は、Cisco SRST 3.0 および 3.1 との下位互換性のために必要になる場合があります。

### 要約手順

1. **dial-peer voice tag voip**
2. **dtmf-relay sip-notify**
3. **exit**
4. **sip-ua**
5. **notify telephone-event max-duration time**
6. **exit**

## ■ SIP アプリケーション用 DTMF リレーとボイスメール

## 詳細手順

	コマンドまたはアクション	目的
ステップ 1	<code>dial-peer voice tag voip</code>  例: Router(config)# dial-peer voice 2 voip	dial-peer コンフィギュレーション モードを開始します。
ステップ 2	<code>dtmf-relay sip-notify</code>  例: Router(config-dial-peer)# dtmf-relay sip-notify	SIP NOTIFY メッセージを使用して DTMF トーンを転送します。
ステップ 3	<code>exit</code>  例: Router(config-dial-peer)# exit	dial-peer コンフィギュレーション モードを終了します。
ステップ 4	<code>sip-ua</code>  例: Router(config)# sip-ua	SIP user-agent コンフィギュレーション モードを開始します。
ステップ 5	<code>notify telephone-event max-duration time</code>  例: Router(config-sip-ua)# notify telephone-event max-duration 2000	単一の DTMF イベントに関する NOTIFY メッセージを 2 つ連続して送信するときの、時間間隔の最大値を設定します。  • <b>max-duration time</b> : 単一の DTMF イベントに関する NOTIFY メッセージを連続して送信するときの時間間隔 (ミリ秒)。範囲は 500 ~ 3000 です。デフォルトは 2000 です。
ステップ 6	<code>exit</code>  例: Router(config-sip-ua)# exit	SIP user-agent コンフィギュレーション モードを終了します。

## トラブルシューティングに関するヒント

`show sip-ua status` コマンド出力に、電話イベントに関する NOTIFY メッセージを連続的に送信するときの時間間隔が表示されます。次の例では、時間間隔は 2000 ミリ秒です。

```
Router# show sip-ua status

SIP User Agent Status
SIP User Agent for UDP :ENABLED
SIP User Agent for TCP :ENABLED
SIP User Agent bind status(signaling):DISABLED
SIP User Agent bind status(media):DISABLED
SIP early-media for 180 responses with SDP:ENABLED
SIP max-forwards :6
SIP DNS SRV version:2 (rfc 2782)
NAT Settings for the SIP-UA
Role in SDP:NONE
Check media source packets:DISABLED
Maximum duration for a telephone-event in NOTIFYs:2000 ms
SIP support for ISDN SUSPEND/RESUME:ENABLED
Redirection (3xx) message handling:ENABLED

SDP application configuration:
Version line (v=) required
Owner line (o=) required
Timespec line (t=) required
Media supported:audio image
Network types supported:IN
Address types supported:IP4
Transport types supported:RTP/AVP udpt1
```

## 関連情報

Cisco Unified SRST の監視および保守については、P.227 の「Cisco Unified SRST の監視と保守」に進んでください。

追加情報については、P.25 の「Cisco Unified SRST の概要」の P.40 の「その他の資料」を参照してください。



## INDEX

- A**
- after-hours block pattern コマンド 107
  - after-hours date コマンド 108
  - after-hours day コマンド 108
  - alias コマンド
    - コールの再ルーティング用の 76
  - ANI ( Answer Number Indication )
    - ~の数字変換規則 85
  - application コマンド 98
  - auto-cut-through コマンド 144
- B**
- BRI ( Basic Rate Interface )
    - ボイスメールの設定 194
  - BRI/PRI アクセスを使用するボイスメールの CallManager ゲートウェイへのリダイレクト 201
- C**
- call application alternate コマンド 47
  - call application voice コマンド 97, 98
  - call start slow コマンド 213
  - call-forward busy コマンド 74, 200
  - call-forward noan コマンド 74, 200
  - call-forward pattern コマンド 94
  - CallManager ゲートウェイ
    - ボイスメールへのリダイレクト 201
  - ccm-manager fallback-mgcp コマンド 47, 48
  - cdn ( 着信番号 )
    - pattern direct コマンドの 204
    - 説明 202
  - cgn ( 発信番号 )
    - pattern direct コマンドの 204
    - 説明 202
  - CIF ( Common Intermediate Format ) 213
  - Cisco CallManager
    - Cisco SRST でサポートされるバージョン 32
    - WAN がダウンした場合の動作 26
    - インストレーション 34
    - ビデオでサポートされているバージョン 212
  - Cisco CallManager への SETUP メッセージ 201
  - Cisco IOS 証明書サーバへの CA サーバの設定 160
  - Cisco IOS ソフトウェア イメージ
    - Cisco SRST でサポートされる 32
  - Cisco IP Phone
    - Cisco SRST と連携させるための設定 61
    - 各 SRST バージョンでサポートされる システム メッセージ 30
    - システム メッセージ 16
  - Cisco IP Phone 7902G
    - 説明 20
  - Cisco IP Phone 7905G
    - 説明 20
  - Cisco IP Phone 7910
    - システム メッセージ 27
  - Cisco IP Phone 7912G
    - 説明 20
  - Cisco IP Phone 7914 拡張モジュール
    - 説明 21
  - Cisco IP Phone 7940
    - 言語表示 63
  - Cisco IP Phone 7940G
    - システム メッセージ 27
  - Cisco IP Phone 7941G および Cisco IP Phone 7941GE 8
  - Cisco IP Phone 7960
    - 言語表示 63
  - Cisco IP Phone 7960G
    - システム メッセージ 27
  - Cisco IP Phone 7961G および Cisco IP Phone 7961GE 9
  - Cisco IP Phone Conference Station 7935
    - 制約事項 98
    - 説明 21
  - Cisco IP Phone に表示されるインサービスの静的なテキスト メッセージ 65
  - Cisco IP Phone に表示される静的なテキスト メッセージ 65

- Cisco IP Phone への Secure SRST の確立 158
- Cisco Unified IP Phone 212
- Cisco Unified Video Advantage 212
- Cisco Unity 194, 203
- Common Intermediate Format、「CIF」を参照 213
- cor コマンド 103
- COR (制限クラス)
  - 設定 103
  
- D
  
- debug cch323 video コマンド 226
- debug ephone detail コマンド 226
- debug ephone message コマンド 226
- debug ephone register コマンド 226
- debug ephone video コマンド 226
- debug h225 asn1 コマンド 226
- debug h245 asn1 コマンド 226
- debug voip ccapi inout コマンド 226
- default-router コマンド 51, 52
- destination-pattern コマンド 196
- DHCP (Dynamic Host Configuration Protocol)
  - DHCP リレー サーバを定義する 53
  - オプション 150 51
  - 各 Cisco IP Phone に対する個別の DHCP IP アドレスプールを定義する 52
  - 設定 51
  - 単一の DHCP IP アドレスプールを定義する 51
- dial-peer voice コマンド 98, 196
- dialplan-pattern コマンド
  - Cisco SRST V2.1 の機能拡張 21
  - 省略された内線番号を E.164 番号に変換するための 83
- DNIS (着信番号識別サービス)
  - ~の数字変換規則 85
- DTMF (Dual Tone Multifrequency)
  - ボイスメール 194, 201, 203
- DTMF リレー、SIP RFC 2833 を使用 266
- dtmf-relay コマンド
  - SIP ネットワーク 266, 268
  
- E
  
- E.164 74, 76
  - destination-pattern コマンドの 197
  
- ephone ファームウェア 212
- ephone-dn コマンド 69, 83
  
- F
  
- Far-End Camera Control、「FECC」を参照 213
- fdn (転送番号)
  - pattern direct コマンドの 204
  - 説明 202
- FECC (Far-End Camera Control) 213
- forward-digits コマンド 196
- full-blind
  - コール転送 95
- full-consult
  - コール転送 95
- FXO
  - ヘアピン転送コール 203
- FXO (Foreign Exchange Office)
  - ボイスメール 194
- FXS (Foreign Exchange Station)
  - ボイスメール 194
  
- G
  
- G.711
  - 3 者間 Ad Hoc 会議 112
  
- H
  
- H.261 ビデオコーデック 213
- H.263 ビデオコーデック 213
- H.323 VoIP コールのコールプリザベーション 109
- H.323 エンドポイント 215
- h323 コマンド 94
- h450 h450-2 timeout コマンド 94
- H.450.12 94
- H.450.2
  - ~を使用したアナログ転送 97
  - ~を使用した打診コール転送および自動転送 93
- H.450.2 を使用した打診コール転送および自動転送 93
- host コマンド 52
- huntstop
  - コマンド 89
- huntstop channel コマンド 70

- I
- input gain コマンド 144
  - interface コマンド 53
  - ip dhcp pool コマンド 51, 52
  - ip helper-address コマンド 53
  - ip source-address コマンド 55
  - IP ルーティング
    - 有効化 46
  - ISDN ( Integrated Services Digital Network )
    - ボイスメール 194
- L
- limit-dn コマンド 55
- M
- max-conferences コマンド 112
  - max-dn コマンド 16, 55, 66
  - max-ephones コマンド 55
  - maximum bit-rate コマンド 224
  - MIB ( 管理情報ベース )
    - Cisco SRST でサポートされる 41
  - moh ( ephone-dn ) コマンド 146
  - MOH ( music on hold )
    - フラッシュ ファイルから 122
    - ライブ フィードから 143
- N
- network コマンド 51
  - notify telephone-event コマンド 267, 268
- O
- OLC ( Open Logical Channel ) 215
  - One-Quarter Common Intermediate Format, 「QCIF」を参照 213
  - operation コマンド 144
  - option 150 ip コマンド 51, 52
- P
- pattern direct コマンド 203
  - pattern ext-to-ext busy コマンド 203
  - pattern ext-to-ext no-answer コマンド 203
  - pattern trunk-to-ext busy コマンド 203
  - pattern trunk-to-ext no-answer コマンド 203
  - pattern コマンド 202
  - PBX ( 構内交換機 ) 97
  - port コマンド 196
  - POTS ( Plain Old Telephone Service )
    - ボイスメールへのダイレクト アクセスの設定 196
  - PRI ( Primary Rate Interface )
    - ボイスメールの設定 194
  - PSTN ( 公衆電話交換網 )
    - ボイスメール 194
- Q
- QCIF ( One-Quarter Common Intermediate Format ) 213
- R
- RDNIS ( Redirected Dialed Number Identification Service )
    - ボイスメール サポート 201
  - RFC 2833、SIP と SRST 266
  - RTP ( Real-Time Transport Protocol ) ストリーム 216
- S
- SCCP エンドポイント 215
  - Secure SRST 152
  - Secure SRST の設定 160
  - Secure SRST の認証および暗号化 156
  - Secure SRST ルータでのクレデンシャル サービスの有効化 167
  - Secure SRST ルータの Cisco IOS クレデンシャル サーバ 158
  - service dhcp コマンド 53
  - show call active video コマンド 226
  - show call-manager-fallback all コマンド 219, 227
  - show call-manager-fallback dial-peer コマンド 227
  - show call-manager-fallback ephone-dn コマンド 227
  - show call-manager-fallback voice-port コマンド 227
  - show dial-peer voice summary コマンド 228
  - show ephone offhook コマンド 226, 227
  - show ephone phone-load コマンド 212
  - show ephone registered コマンド 212, 226, 227

show ephone remote コマンド 227  
 show ephone ringing コマンド 227  
 show ephone summary コマンド 227  
 show ephone telephone-number コマンド 227  
 show ephone unregistered コマンド 227  
 show ephone コマンド 227  
 show ephone-dn loopback コマンド 227  
 show ephone-dn summary コマンド 227  
 show ephone-dn コマンド 227  
 show running-config コマンド 227  
 show sip-ua status コマンド 269  
 show translation-rule コマンド 85  
 show voice port summary コマンド 228  
 show voip rtp connection コマンド 216  
 show voip rtp connections コマンド 226  
 signal immediate コマンド 144  
 SIP サポート 265  
 SRTP ( Secure Real-Time Transport Protocol ) 154  
 SRST ルータおよび PKI 155  
 system message コマンド  
     Cisco IP Phone の表示用にカスタマイズされたシス  
     テム メッセージを設定するための 65

## T

timeouts busy コマンド 91  
 timeouts-ringing コマンド 91  
 transfer-pattern コマンド 92, 94  
 transfer-system コマンド 94  
 translate コマンド 85  
 translation-profile コマンド 87  
 Transport Layer Security ( TLS ) 154

## U

Unity、Cisco 194  
 user-local コマンド 63

## V

vm-integration コマンド 203  
 voice service voip コマンド 94  
 voicemail コマンド 200, 202

## W

## WAN

WAN 接続がダウンした場合 26, 45

## X

xmlschema コマンド 113

## あ

## アクセス コード

トランク 101

## い

## インストレーション

Cisco CallManager 34  
 Cisco SRST 34

## え

営業時間後のコール ブロッキング 107  
 エリア コードとプレフィックス コード 85  
 エンドポイント、ビデオの 214, 215

## お

オーディオ フォールバック 214

## か

## 会議

3 者間 G.711 Ad Hoc 112  
 二重回線電話機での有効化 66

解像度、ビデオの 213

## 確認

Cisco SRST が有効になっていること 57

監視、Cisco SRST 227

監視、自動転送と接続解除 91

## き

## キーブアライブ

キーブアライブ インターバルの設定 54



## 規則

- 再ルーティング 76
- 数字変換 85
- プリファレンス 76

## く

## 国コード

- デフォルト 63
- グローバルプレフィックス  
設定 83

## け

## 言語

- Cisco IP Phone の表示の設定 63

## こ

- コーデック、ビデオの 214
- コール ウェイティング
  - 二重回線電話機での有効化 66
- コール設定、ビデオの 215
- コールタイプ フラグ 215
- コール転送
  - blind 95
  - full-blind 95
  - full-consult 95
  - H.450.2 標準を使用した打診 15
  - local-consult 95
  - アナログ電話機 97
  - 打診 93
  - 二重回線電話機での有効化 66
  - フックフラッシュの使用 97
  - リモート 92

## さ

- 再ルーティング規則 76

## し

## 時刻形式

- Cisco IP Phone の表示の設定 62
- 時刻と日付に基づいたコール ブロッキング 107

- システム ログ メッセージ 18

## 自動転送 93

- ビジー信号の受信時または無応答時 74
- ボイスメールに対する 201

- 自動転送と接続解除の監視 91

## 資料

- 参考 40

## す

- 数字変換規則 85

## せ

## 制約事項

- 各 Cisco SRST バージョンの 37

## 設定

- Cisco SRST、作業の順序 39
- COR (制限クラス) 103
- DHCP (Dynamic Host Configuration Protocol) 51
- カスタマイズされたシステム メッセージ 65
- グローバルプレフィックス 83
- 自動転送 74
- トランク アクセス コード 101
- 二重回線電話機 66
- 発信コール 92
- ボイスメールのメッセージ ボタン 199
- ボイスメールへのダイレクト アクセス 196
- 呼び出しタイムアウトのデフォルト 91
- 例
  - セントラル ロケーションのボイスメール システム FXO/FXS 207
  - ローカル ボイスメール システム FXO/FXS 207
- ローカルおよびリモートのコール転送 92

## た

## タイムゾーン

- Cisco IP Phone の表示の設定 62

## ダイヤルピア

- COR (制限クラス) 103
- POTS (Plain Old Telephone Service) 196
- 最長一致規則 76
- ハンティング 89
- ボイスメール 195

- ダイヤルされた番号、～への追加 タグ 202 85
- ち
- 着信番号
  - 数字変換規則 85
- て
- 低速接続手順 217
- 転送パターン 92
- 電話番号
  - call-forward busy コマンド内の 75
  - 転送先としての 92
- と
- 統合
  - Cisco SRST と Cisco CallManager 35
  - Cisco SRST とボイスメール 193
- トークン 202
- ツールバー 107
- トランク アクセス コード 101
- に
- 二重回線電話機
  - 3 者間 G.711 Ad Hoc 会議 112
  - 設定 66
- 二重回線モード
  - 説明 16
- ね
- ネットワーク
  - 設定について 45
- は
- バージョン、ビデオの 212
- 発信コール
  - 設定 92
- 発信番号
  - 数字変換規則 85
- ハンティング
  - ダイヤル ピア 89
- ハントストップ
  - 規則 76
- ひ
- 日付形式
  - Cisco IP Phone の表示の設定 62
- ビット レート、ビデオの 224
- ビデオ
  - エンドポイント 214
  - コール設定 215
  - サポートされている形式 213
  - サポートされているコーデック 213
  - 帯域幅の設定値 224
  - トラブルシューティング 226
  - ファームウェア バージョン 212
  - メディア パス 216
- ビデオ コーデック 214
- ビデオ サポート 211
- 標準規格
  - Cisco SRST でサポートされる 41
- ふ
- ファームウェア、ビデオの 212
- フォールバック、オーディオへの 214
- フックフラッシュ
  - ～を使用したアナログ転送 97
- ブラインド コール転送 93, 95
- プラットフォーム
  - 各 SRST バージョンでサポートされる 31
- プリザベーション、H.323 VoIP のコール プリザベーション 109
- プリファレンス規則 76
- プレフィックス コードとエリア コード 85
- フローアラウンド モード 216
- フロースルー モード 216
- へ
- ヘアピン転送コール、FXO 203
- 変換規則、数字 85
- 変換プロファイル 86

## ほ

## ボイスメール

- Cisco SRST の処理方法 194
  - コールのルーティング 195
  - 自動転送 201
  - ダイレクト アクセスの設定 196
- 保守、Cisco SRST 227

## め

## メッセージ ボタン

- ボイスメールでの設定 199
- メディア パス、ビデオの 215
- メディア フローアラウンド モード 216
- メディア フロースルー モード 216

## よ

## 呼び出しタイムアウトのデフォルト

- 設定 91
- 説明 18

## り

- リモート コール転送 92

## る

## ルーティング

- IP ルーティングの有効化 46
- ボイスメール コールの 195

## ろ

## ローカル コール転送

- 設定 92

## ローカルでの打診

- 設定 95